JPCERT-PR-2018-01
発行日：2018-1-16

JPCERT/CC 活動概要 [2017 年 10 月 1 日 ～ 2017 年 12 月 31 日]

活動概要トピックス

ートピック1ー　攻撃行動の痕跡を調査するための文書およびツールを公開

組織のさまざまな情報システムが侵害されるサイバー攻撃をはじめとしたインシデントの調査は、調査対象が多数になるため、重要な手がかりを見落とすことなく迅速に調査することが難しいのが現状です。そのため、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法やそれを支援するツールが求められています。

JPCERT/CC では、そうした期待に応えて、近年のインシデント対応や調査等に幅広く役立てていただくことを目的として、攻撃行動によって組織内の機器に残る痕跡を調査するための報告書（「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」）の第 2 版と、イベントログを可視化するツール「LogonTracer」を公開しました。

「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」は、攻撃に使われることの多いツールを実行した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調査しまとめたものです。2016 年 6 月に公表した初版から内容を大幅に見直して、調査対象のツールの入れ替えや拡充、痕跡を確認する OS 環境のアップデート、レポートの形式の変更などを行った第 2 版は、最新の攻撃の痕跡の調査を行う場合のガイドとしてより活用しやすい報告書となっています。

なお、本報告書に記載している痕跡の調査については、2017 年 11 月 9 日の CODE BLUE 2017 において「攻撃者の行動を追跡せよ -行動パターンに基づく横断的侵害の把握と調査-」と題した講演を、2017 年 12 月 8 日の Botconf 2017 において「Hunting Attacker Activities - Methods for Discovering and Detecting Lateral Movements」と題した講演を行うとともに、報告書の公開とあわせて、「分析センターだより」および英語ブログにて報告書の内容を紹介しました。

イベントログを可視化するツール「LogonTracer」は、ログオンに関連するイベントログに含まれるホスト名（または IP アドレス）とアカウント名を関連付けて可視化（グラフ表示）でき、インシデント調査に欠かせないイベントログの分析を視覚的に行えるようになっていることから、多くの方から好意的なフィードバックをいただいています。

なお、2015 年 11 月 29 日の Internet Week 2017 におけるハンズオン「インシデント対応ハンズオン 2017」でもツールを実際に活用したトレーニングを実施するとともに、ツールの公開に合わせて、ツールを紹介する「分析センターだより」の公開も行いました。

なお、ツールの公開は、ソフトウエア開発プロジェクトのための共有ウェブサービスの GitHub で行うとともに、実行環境を事前にセットアップした Docker イメージを Docker Hub で公開しています。

■「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」関連資料

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
http://www.jpcert.or.jp/research/ir_research.html

分析センターだより「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（第 2 版）公開（2017-11-09）」
http://www.jpcert.or.jp/magazine/acreport-ir_research2.html

Research Report Released: Detecting Lateral Movement through Tracking Event Logs (Version 2)
http://blog.jpcert.or.jp/2017/12/research-report-released-detecting-lateral-movement-through-tracking-event-logs-version-2.html

■「LogonTracer」関連資料

JPCERTCC/LogonTracer - GitHub
https://github.com/JPCERTCC/LogonTracer

jpcertcc/docker-logontracer - DockerHub
https://hub.docker.com/r/jpcertcc/docker-logontracer/

分析センターだより「イベントログを可視化して不正使用されたアカウントを調査 ~LogonTracer~（2017-11-28）」
http://www.jpcert.or.jp/magazine/acreport-logontracer.html

ートピック2ー　ランサムウエア対策特設サイトを公開

ランサムウエアは、感染した PC に特定の制限をかけ、その制限の解除と引き換えに金銭を要求するマルウエアの一種です。その起源は 1989 年に遡りますが、2012 年前後から数多くのランサムウエアが出現するようになりました。さらに、仮想通貨の普及を背景に、2015 年頃からは、法人組織での被害が深刻化し、2016 年には日本国内における被害報告の件数が過去最多となりました。2017 年には自己増殖性をもった「WannaCrypt」や「NotPetya」などのマルウエアが猛威を振るい、その被害が広く報道されました。今やランサムウエアは最も深刻なサイバー脅威の一つとも言われています。

このような状況から、JPCERT/CC は、ユーザの意識啓発を促進することを目的として、ランサムウエア対策に必要となる情報を集約したランサムウエア対策特設サイトを 2017 年 10 月 26 日に公開しました。 同サイトでは、JPCERT/CC が国内において確認している代表的なランサムウエアについて紹介するとともに、ランサムウエアの被害低減策や予防策、感染した場合の対処法を説明しています。

また、JPCERT/CC は、ランサムウエア撲滅に向けて取り組む国際的なプロジェクト「No More Ransom」に参加しており、国内外の関連機関と連携して、ランサムウエアの対策を進めています。同サイトでは、国内外における JPCERT/CC の活動方針も説明しておりますので、ご参照ください。

ランサムウエア対策特設サイト
https://www.jpcert.or.jp/magazine/security/nomore-ransom.html

本活動は、経済産業省より委託を受け、「平成 29 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」、「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 4,530 件、インシデント件数ベースでは 4,735 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 1,901 件でした。前四半期の 2,234 件と比較して 15%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/2018/IR_Report20180116.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 852 件で、前四半期の 1,011 件から 16%減少しました。また、前年度同期（521 件）との比較では、64%の増加となりました。

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

［表 1-1 フィッシングサイトの国内・国外ブランド別の件数］

フィッシングサイト	10 月	11 月	12 月	国内外別合計（割合）
国内ブランド	42	32	43	117(14%)
国外ブランド	192	216	191	599(70%)
ブランド不明 (注 5)	31	53	52	136(16%)
全ブランド合計	265	301	286	852(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。

フィッシングサイトが装ったブランドの国内、海外の内訳では、海外ブランドが 70%を占め、国内ブランドの割合は 14%でした。海外ブランドの割合が多いのは、特定の海外ブランドを装ったフィッシングメールが広く出回っており、多数の報告が寄せられていることが原因です。それらのフィッシングメールから誘導される特定ブランドを装ったサイトの一部を JPCERT/CC が確認したところ、ブラウザの言語設定が日本語の場合にだけフィッシングサイトとして機能し、それ以外の場合には「サイトが停止している」と表示されました。これらは日本語を使うユーザだけを標的にしていると見られます。

国内ブランドを装ったフィッシングサイトについては、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と、SNS を装った.cn ドメインのフィッシングサイトに関する報告が多く寄せられています。国内通信事業者の複数のブランドや国内の大学の Web メールサービスを装ったフィッシングサイト等、Web メールサービスのアカウントを窃取するフィッシングサイトの構築に、Web サイトを簡易に開設できる海外の無料サービスがしばしば使用されていることを確認しています。

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 24%、国外 76%）に比べ、国内への調整の割合が増加しています。

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、276 件でした。前四半期の 254 件から 9%増加しています。

Web サイトに不正に埋め込まれたスクリプトによって、マルウエア感染の警告を表示して偽のサポートへの電話を促す詐欺サイトや、不審なツールのダウンロードを促すサイトなどに転送される事例を多く確認しています。また、ブログページや、現在使用されていないドメインへのアクセスがあった場合に広告が表示されるドメインパーキングからも、サポート詐欺サイトなどに転送される事例を確認しています。不審なサイトへの転送は、正規のブログパーツや広告から呼び出されるページの転送設定やスクリプトに

よって行われており、広告配信ネットワークが悪用されている可能性があります。

10 月初めごろから、仮想通貨に関連した演算処理（マイニング）をサイト閲覧者の端末上で実行させるスクリプトが埋め込まれた Web サイトに関する報告が寄せられています。このようなサイトには、改ざんされてスクリプトを埋め込まれたと見られるサイトがある一方で、サイト管理者が意図してスクリプトを使用していると見られる例もありました。

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、9 件でした。前四半期の 7 件から 29%増加しています。本四半期は、対応を依頼した組織は 7 件でした。

10 月末から 11 月初めにかけて、標的型攻撃と見られるなりすましメールで、Microsoft Office ドキュメントの DDE（Dynamic Data Exchange）プロトコルを悪用するファイルが添付された事例を確認しました。10 月末に報告が寄せられたなりすましメールには、DDE フィールドが埋め込まれた docx 形式の文書ファイルが添付されており、この文書ファイルを開いた際に表示されるダイアログでアプリケーションの起動を許可すると、C&C サーバへの通信が発生する仕組みになっていました。また、11 月初めに寄せられた報告では、なりすましメールに DDE を悪用する msg ファイルが添付されていました。ファイルを開いた際に表示されるダイアログで許可を意味する応答を返すと、C&C サーバから HTTP ボットが取得され、実行されます。これにより、攻撃者は HTTP ボットに感染した端末で任意の機能を実行することができる仕組みとなっていました。DDE を悪用してマルウエアに感染させる攻撃手法は、標的型攻撃に限らず確認されており、11 月上旬には、Microsoft 社が「DDE フィールドを含む Microsoft Office ドキュメントを安全に開く方法」のセキュリティアドバイザリ(*1)を公開しています。

前四半期に引き続き、添付ファイル内のショートカットファイル（LNK ファイル）を実行させてマルウエアに感染させる攻撃手法を確認しています。10 月後半に寄せられた報告では、なりすましメールに添付された ZIP ファイル内に LNK ファイルが含まれていました。LNK ファイルを実行すると、Powershell スクリプトなどがダウンロードされた後、実行され、最終的に遠隔操作型のマルウエア PlugX に感染することを確認しました。

また、11 月半ばに報告が寄せられたなりすましメールでは、標的組織が受け取った正規のメールについての情報を入手した攻撃者が、その再送を装い、攻撃用のファイルをダウンロードさせるリンクを含むメールを標的組織に送信していました。リンクをクリックするとダウンロードされる ZIP ファイルは、Powershell スクリプトを実行する LNK ファイルを含んでおり、この LNK ファイルを実行すると、遠隔からの指令に従ってファイルのアップロード・ダウンロードや、コマンドの実行を行うマルウエアに感染することが確認されました。

1.1.1.4. 参考文献

(1) マイクロソフト セキュリティ アドバイザリ 4053440
https://technet.microsoft.com/ja-jp/library/security/4053440.aspx

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 34,000 名の登録者を擁するメーリングリスト、早期警戒情報の提供用ポータルサイト WAISE（Watch and Warning Analysis Information for Security Experts）等を通じて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「お知らせ」としてまとめ公表しています。本四半期には次のようなお知らせを発行しました。

発行件数：2 件　https://www.jpcert.or.jp/update/2017.html

2017-10-26　ランサムウエア対策特設サイトを公開
2017-12-18　長期休暇に備えて 2017/12

1.2.1.2. 注意喚起

注意喚起は深刻かつ影響範囲の広い脆弱性等について公表する情報です。本四半期は次のような注意喚起を発行しました。

発行件数：16 件（うち 5 件更新）　https://www.jpcert.or.jp/at/

2017-10-04　Apache Tomcat における脆弱性に関する注意喚起 (更新)
2017-10-05　Apache Tomcat における脆弱性に関する注意喚起 (更新)
2017-10-11　2017 年 10 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)
2017-10-17　Adobe Flash Player の脆弱性 (APSB17-32) に関する注意喚起 (公開)
2017-10-18　Adobe Flash Player の脆弱性 (APSB17-32) に関する注意喚起 (更新)
2017-10-18　2017 年 10 月 Oracle Java SE のクリティカルパッチアップデートに関する注意喚起 (公開)
2017-11-15　Adobe Flash Player の脆弱性 (APSB17-33) に関する注意喚起 (公開)
2017-11-15　Adobe Reader および Acrobat の脆弱性 (APSB17-36) に関する注意喚起 (公開)
2017-11-15　2017 年 11 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)
2017-11-29　macOS High Sierra の設定に関する注意喚起 (公開)
2017-11-30　macOS High Sierra の設定に関する注意喚起 (更新)
2017-11-30　2017 年 11 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (更新)
2017-12-07　Microsoft Malware Protection Engine のリモートでコードが実行される脆弱性（CVE-2017-11937）に関する注意喚起 (公開)
2017-12-13　Adobe Flash Player の脆弱性 (APSB17-42) に関する注意喚起 (公開)
2017-12-13　2017 年 12 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)
2017-12-19　Mirai 亜種の感染活動に関する注意喚起 (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も掲載しています。本四半期における発行は次のとおりです。

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。

2017-10-04　マルウエア Datper の痕跡を調査するためのログ分析ツール活用方法
2017-10-12　10 月は「サイバーセキュリティ国際キャンペーン」
2017-10-18　「CODE BLUE」開催
2017-10-25　Wi-Fi Protected Access II (WPA2) に関する脆弱性が公開
2017-11-01　JPCERT/CC が「ランサムウエア対策特設サイト」を開設
2017-11-08　Japan Security Analyst Conference 2018 参加登録開始
2017-11-15　JPCERT/CC が「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（第 2 版）」を公開
2017-11-22　経済産業省と IPA が「サイバーセキュリティ経営ガイドライン Ver2.0」を公開
2017-11-29　CSA ジャパンが「クラウドコンピューティングのためのセキュリティガイダンス v4.0」を公開
2017-12-06　JPCERT/CC が「イベントログを可視化して不正使用されたアカウントを調査 ~LogonTracer~」を公開
2017-12-13　NICT が実践的サイバー演習「サイバーコロッセオ」の実施を発表
2017-12-20　長期休暇に備えて 2017/12
2017-12-27　Mirai 亜種の感染活動に関する注意喚起

1.2.1.4. 早期警戒情報

JPCERT/CC では、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/

1.2.1.5. CyberNewsFlash

CyberNewsFlash は、情報収集・分析・情報発信を行っている早期警戒グループのメンバーが、最新のインシデント情報、対策情報、情報の読み方などをタイムリーにお届けする情報です。本四半期に公表した CyberNewsFlash は次のとおりです。

発行件数：2 件　https://www.jpcert.or.jp/newsflash/

2017-10-25　新たなランサムウエア「Bad Rabbit」について
2017-12-07　送信者を偽装できる脆弱性「Mailsploit」について

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。

(1) ランサムウエア特設サイト開設について
世界中で猛威を振るうランサムウエアは、今やインターネット利用者にとって、深刻な脅威のひとつとなっています。JPCERT/CC は、ユーザの意識啓発を促進することを目的として、ランサムウエア特設ページを 2017 年 10 月 26 日に開設しました。同サイトでは、ランサムウエアの被害低減策や予防策、感染した場合の対処法を紹介しています。 また、JPCERT/CC は、ランサムウエア撲滅に向けて取り組む国際的なプロジェクト「No More Ransom」にも参加しており、国内の関連機関と連携して、ランサムウエア対策を進めています。同サイトでは、このような JPCERT/CC の活動の紹介も行いました。

ランサムウエア対策特設サイト
https://www.jpcert.or.jp/magazine/security/nomore-ransom.html

(2) Apache Tomcat の脆弱性に関する情報発信
Apache Software Foundation から Apache Tomcat の脆弱性 (CVE-2017-12615) に関する情報が 2017 年 9 月 19 日（現地時間）に公開されました。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、Windows で動作している Apache Tomcat において任意のコードが実行できることを確認したため、9 月 20 日に注意喚起を公開しました。
その後、Windows 以外の OS で動作する Apache Tomcat においても本脆弱性と類似した影響を受けるという情報が Web サイト上で公開され、Apache Software Foundation からは、10 月 4 日から 5 日にかけて、脆弱性 (CVE-2017-12617) に関する情報が新たに公開されました。この脆弱性は、Apache Tomcat 7 系から 9 系までの広い範囲に影響が及んでいたことから、JPCERT/CC では注意喚起を更新し、早期の対策を呼びかけました。

Apache Tomcat における脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2017/at170038.html

(3) macOS High Sierra の脆弱性に関する情報発信
「macOS High Sierra 10.13.1」にて、「ルートユーザを無効にする」という設定にしている場合、脆弱性を悪用されることで、ログイン画面でユーザ名を「root」と入力すると、パスワードなしで認証が通る場合があります。脆弱性を実証する手法に関する情報も公開されており、JPCERT/CC でも、この手法を用いることで脆弱性が実証できることを確認したことから、2017 年 11 月 29 日に、macOS High Sierra の脆弱性 (CVE-2017-13872) に関する注意喚起を公開し、早期の対策を呼びかけました。

macOS High Sierra の設定に関する注意喚起
https://www.jpcert.or.jp/at/2017/at170045.html

1.3. インターネット定点観測

JPCERT/CC では、インターネット上に複数の観測用センサーを分散配置し、不特定多数に向けて発信されるパケットを収集するインターネット定点観測システム「TSUBAME」を構築し、運用しています。TSUBAME から得られる情報を、既に公開されている脆弱性情報やマルウエア、攻撃ツールの情報などと対比して分析することで、攻撃活動や攻撃の準備活動等の把握に努めています。
2007 年以降、TSUBAME の観測用センサーは、海外の National CSIRT 等の協力のもと、国外にも設置しています。JPCERT/CC はセンサーを設置した海外の National CSIRT 等と、国内外の観測データを共同で分析する「TSUBAME プロジェクト」を推進しています。
2017 年 12 月末時点で、海外の 20 の経済地域の 25 組織の協力のもとで観測用センサーが設置されています。さらなるセンサー設置地域の拡大と共同分析の深化を目指して、未参加の海外 National CSIRT 等に対して TSUBAME 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

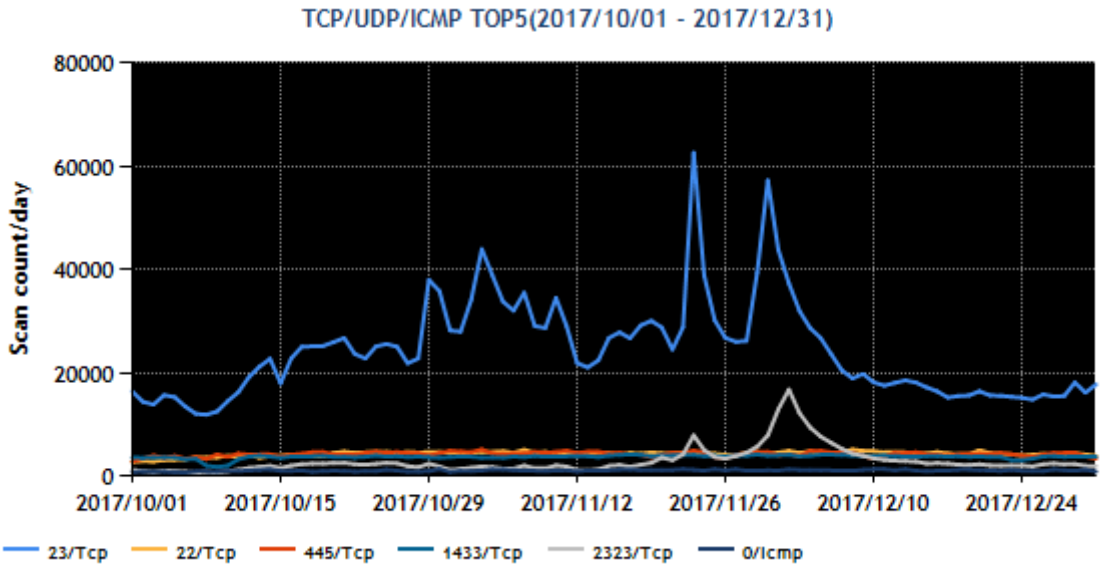
1.3.1. インターネット定点観測システム TSUBAME の観測データの活用

JPCERT/CC では、主に日本企業のシステム管理者の方々に、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 TSUBAME 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、2017 年 7 月から 9 月分のレポートを 2017 年 11 月 30 日に公開しました。

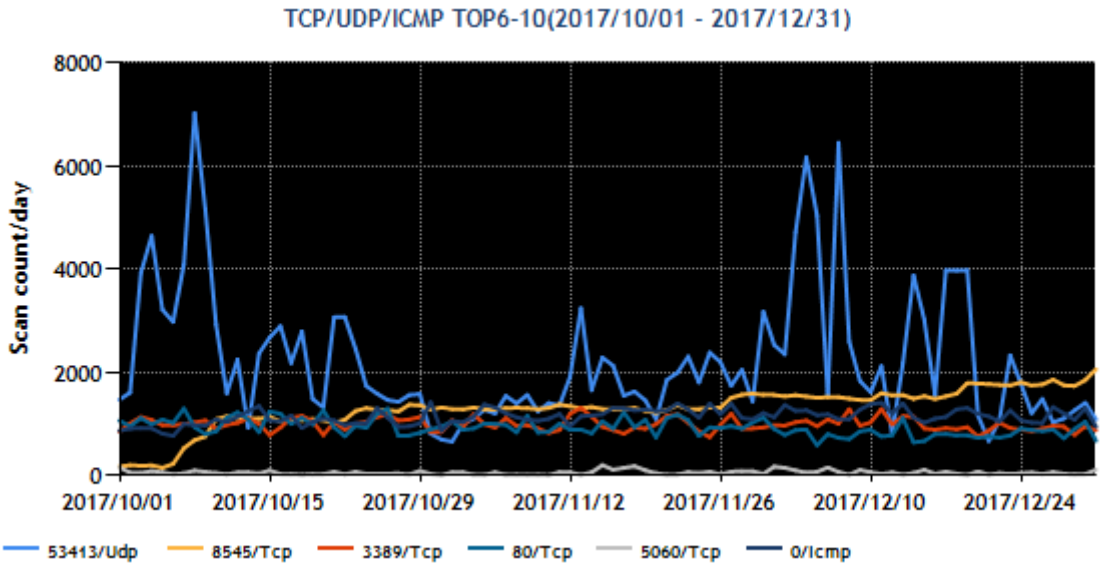
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples
インターネット定点観測レポート（2017 年 7～9 月）
http://www.jpcert.or.jp/tsubame/report/report201707-09.html

1.3.2. 観測動向

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。

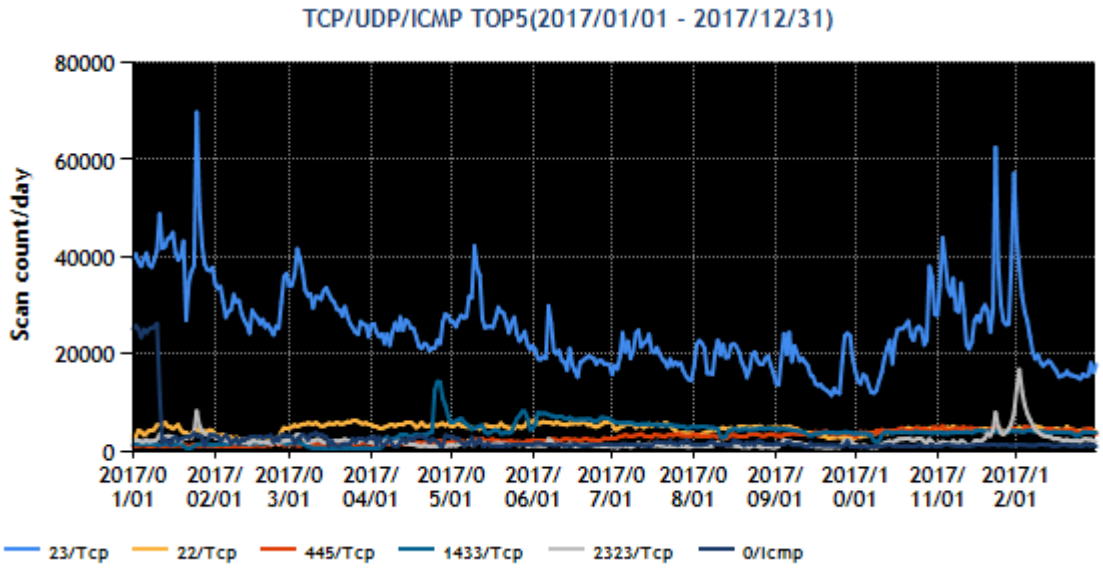


［図 1-1 宛先ポート別グラフ トップ 1-5（2017 年 10 月 1 日-12 月 31 日）］

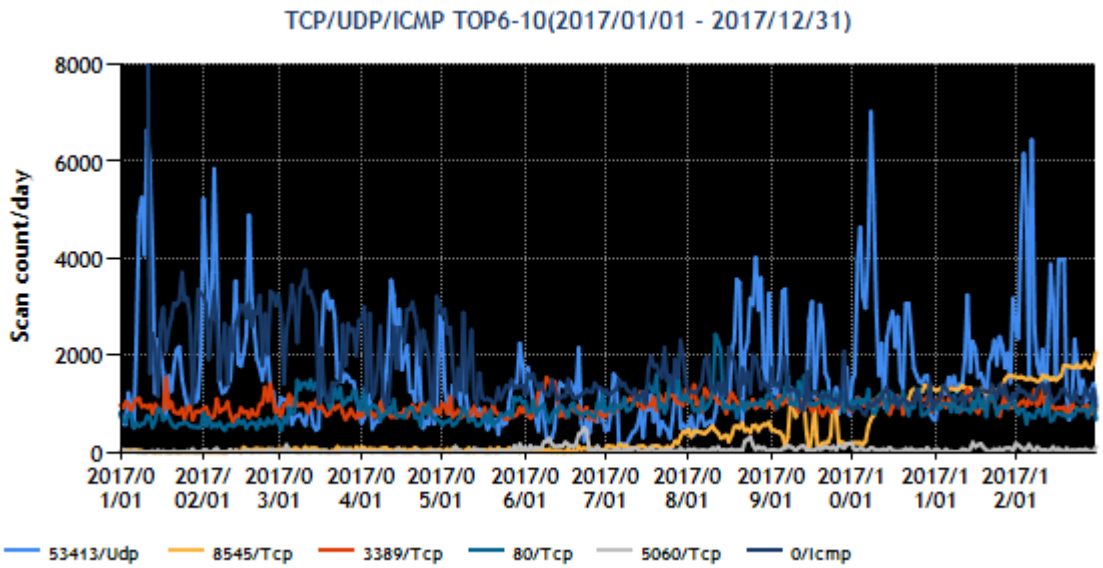


［図 1-2 宛先ポート別グラフ トップ 6-10（2017 年 10 月 1 日-12 月 31 日）］

また、過去 1 年間（2017 年 1 月 1 日-12 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（2017 年 1 月 1 日-12 月 31 日）］



［図 1-4 宛先ポート別グラフ トップ 6-10（2017 年 1 月 1 日-12 月 31 日）］

本四半期は、23/TCP や 22/TCP のパケットが多く観測されました。11 月以降は、一時的に著しく増加し、その後、減少する現象が複数回観測されました。これらのパケットは、調査の結果、Mirai 等のマルウエアに感染した監視カメラやルータ、NAS といった専用機器から送信されていたことが判明しました。こうしたパケットは以前から観測されており、送信元の機器は変わったものの、ほぼ同水準の数のパケットの送信が本四半期も続きました。その他、WannaCrypt やその亜種に感染した PC から送信されているとみられるパケットも観測されました。

1.3.3. 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。本四半期における事例として、日本国内を送信元とし Port 23/TCP を宛先とするパケットが観測されたことに端を発して明らかになったインシデントについて次に述べます。

10 月 31 日頃から、TSUBAME において、日本国内の IP アドレスを送信元とし、Port23/TCP を宛先とするパケットが観測されました。これらのパケットは、日本国内のさまざまな ISP に割り当てられている IP アドレスから送信されていました。

異常なパケットを出している旨の連絡を送信元の機器の管理者に対して行う等の対応を行いつつ、詳細な調査を進めたところ、国内ベンダ製の複数のルータに脆弱性があることがわかりました。JPCERT/CC では観測したパケットの分析等を行い、必要に応じて送信元の機器の管理者へ情報を提供して調査を依頼するなど、感染した機器の発見やマルウエアの駆除、対策の実施に努めています。

1.3.4. TSUBAME WORKSHOP 2017 の開催（2017 年 11 月 13 日）

2017 年 11 月の APCERT 年次総会の期間内に、TSUBAME Workshop 2017 を開催しました。本ワークショップは、各受講者が所属する CSIRT のインシデント対応において、TSUBAME を効果的に活用できるようになることを目的に開催し、TSUBAME プロジェクトのメンバーを中心に、約 30 名が参加しました。

本ワークショップは大きく分けて、「JPCERT/CC からの観測報告」と「ハンズオン演習」という構成で行いました。

観測報告では、本年度 TSUBAME にて観測されたパケット数の推移や攻撃の傾向の変化、また、パケットを分析した結果について共有しました。具体的には、WannaCrypt や Mirai 亜種に感染した端末からのスキャン動向等について紹介しました。

ハンズオン演習では、受講者は、上述の事例について TSUBAME のポータルや関連ウェブサイトにアクセスし、実際にデータの分析を体験しました。また、TSUBAME の蓄積されたデータをローカル PC 上で処理し、分析や可視化を行う新しいツール「pytsubame」の使い方について学習しました。

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り扱い状況

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。

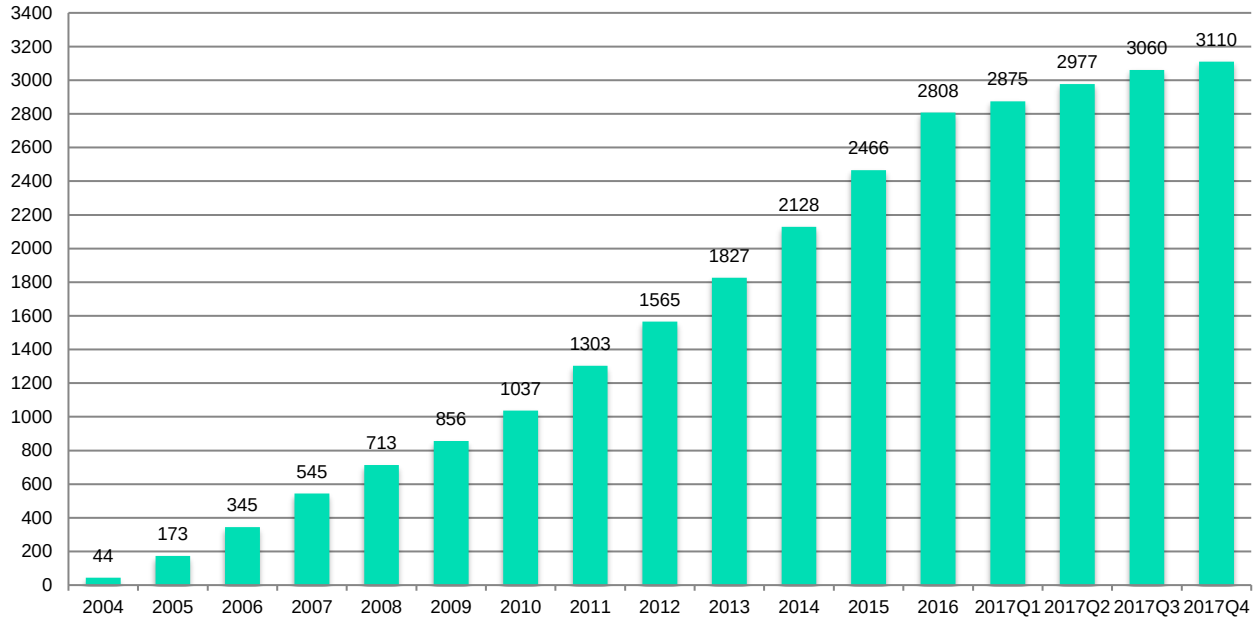
独立行政法人情報処理推進機構（IPA）脆弱性対策
https://www.ipa.go.jp/security/vuln/

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（以下「国内取扱脆弱性情報」:「JVN#」に続く 8 桁の数字の形式の識別子［例えば、JVN#12345678 等］を付与している）と、それ以外の脆弱性に関するもの（以下「国際取扱脆弱性情報」:「JVNVU#」に続く 8 桁の数字の形式の識別子［例えば、JVNVU#12345678 等］を付与している）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 50 件（累計 3,110）で、累計の推移は［図 2-1］に示すとおりです。本四半期に公表された個々の脆弱性情報に関しては、次の Web ページをご参照ください。

JVN(Japan Vulnerability Notes)
https://jvn.jp/



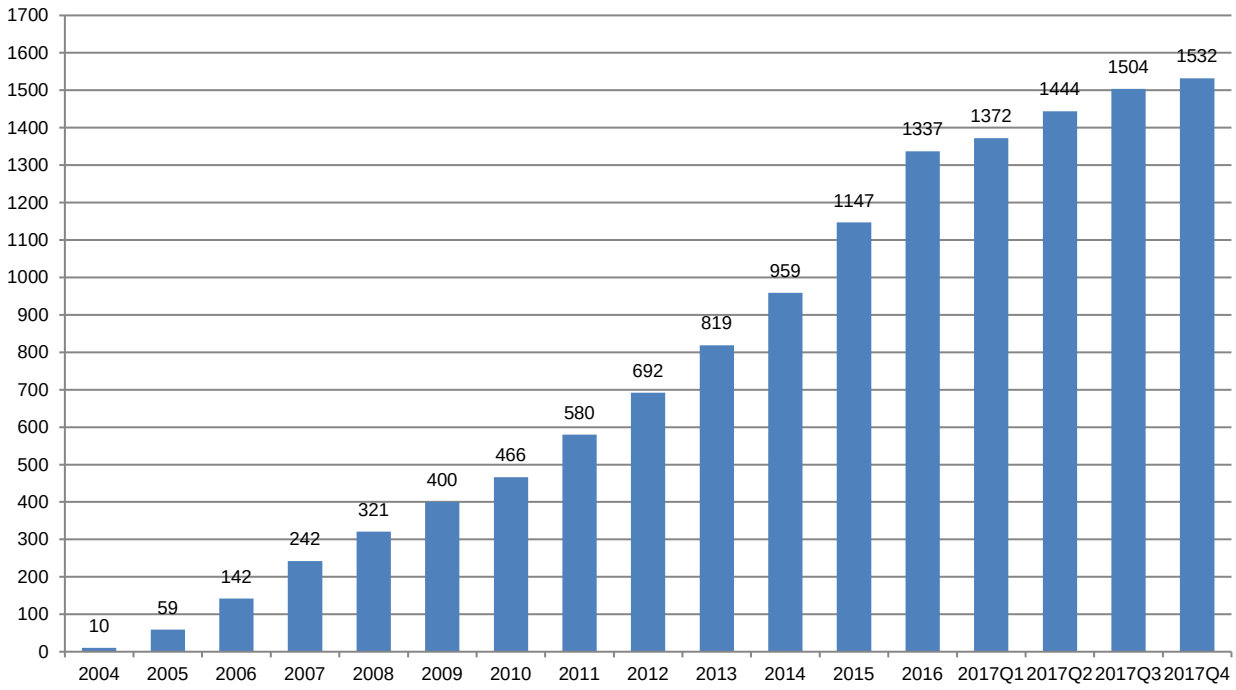
［図 2-1 JVN 公表累積件数］

本四半期において公表に至った脆弱性情報のうち、国内取扱脆弱性情報は 28 件（累計 1,532 件）で、累計の推移は［図 2-2］に示すとおりです。28 件のうち、27 件は単一の製品開発者の製品だけに影響を及ぼすもので、うち 23 件が国内製品開発者に係るもの、4 件が海外の製品開発者にかかわるものでした。また、28 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の影響を受けた製品のカテゴリの内訳は、［表 2-1］のとおりでした。本四半期は前四半期同様に、Windows アプリケーションが 10 件と多く、次いで無線 LAN ルータやネットワークカメラ、IoT 家電等の組込み系製品が 7 件でした。Windows アプリケーションに関する公表は、2017 年第 2 四半期から非常に多く、2010 年に公表された「Windows アプリケーションにおける任意の DLL 読込みの脆弱性」と同じ機序で起こる Windows アプリケーションの脆弱性が多数みられました。これは、特定の発見者が、さまざまな Windows アプリケーションに対し同一の脆弱性が存在しないかを検証し、再現が確認されたものが順次届け出られたことによるものです。

［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内訳］

製品分類	件数
Windows アプリケーション	10
組込系	7
CMS	2
アプリケーションフレームワーク	2
プラグイン	2
ライブラリ	2
グループウエア	1
サーバ製品	1
マルチプラットフォームアプリケーション	1
計	28



［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 22 件（累計 1,578 件）で、累計の推移は［図 2-3］に示すとおりです。

本四半期に公表した脆弱性の影響を受けた製品のカテゴリ内訳は、［表 2-2］のとおりでした。本四半期には、さまざまな OS で起動するアプリケーションの脆弱性を 9 件（表 2-2 No.1,2,4）と多く公表しました。また、前四半期に続き、ライブラリやサーバ製品、プロトコル実装といった製品開発に使用されるソフトウエアやその実装に関する脆弱性の公表も 3 件（表 2-2 No.9,10,12）ありました。

本四半期において特に目立った脆弱性は、米国 CERT/CC が主導となり、フィンランド NCSC-FI、オランダ NCSC-NL、そして JPCERT/CC への国際展開および調整依頼を受け、10 月 16 日に公表に至った WPA2 の脆弱性で、この脆弱性の影響を受ける製品が広範囲に及ぶことから、公表後、国内外問わず非常に注目されました。

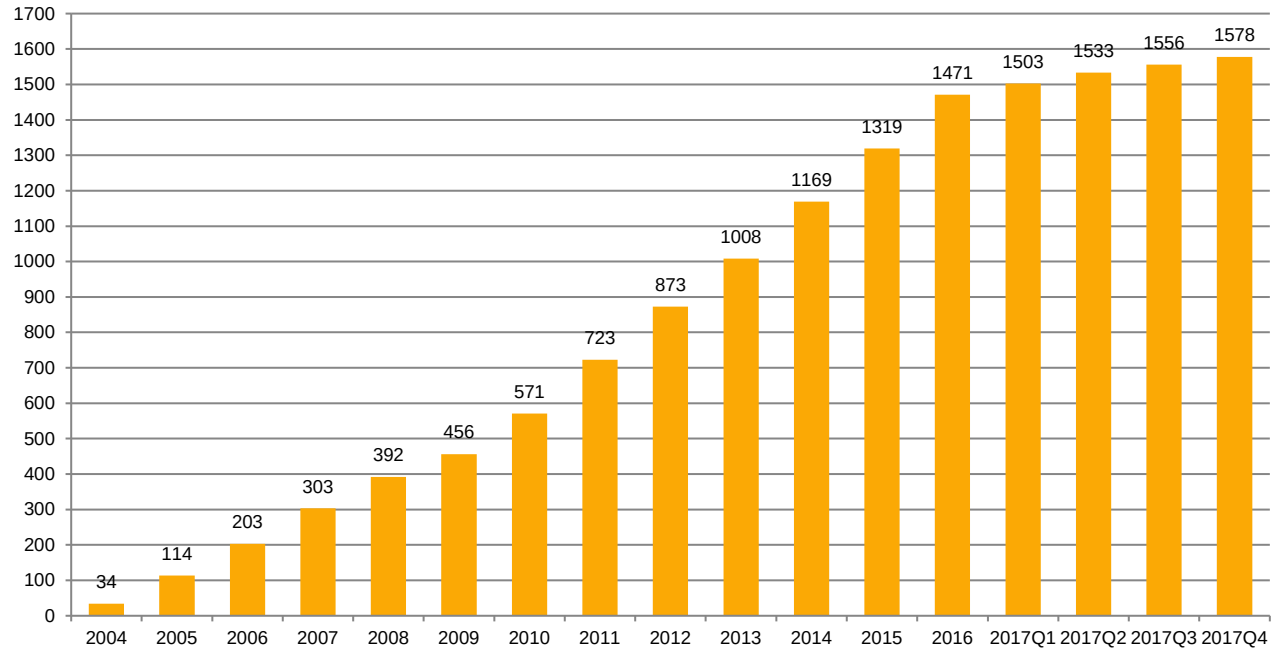
22 件中 3 件は、製品開発者自身による自社製品に関する脆弱性情報の公表依頼に基づくものでした。

また本四半期には、発見者から直接 JPCERT/CC に届け出が行われた脆弱性情報を 5 件公表しました。

このように、JPCERT/CC では、米国 CERT/CC をはじめとする海外調整機関に届け出られた脆弱性情報の日本国内への展開や調整、海外発見者から直接届出られる脆弱性情報の受付や調整、製品開発者自身か告知を目的とした公表依頼の受付など、脆弱性情報の流通、調整および公表を幅広く行っています。

［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内訳］

No.	製品分類	件数
1	macOS アプリケーション	3
2	Windows アプリケーション	3
3	サーバ製品	3
4	マルチプラットフォームアプリケーション	3
5	アンチウィルス製品	2
6	macOS	1
7	Windows OS	1
8	OS(その他)	1
9	プロトコル	1
10	プロトコル実装	1
11	メディアプレイヤー	1
12	ライブラリ	1
13	その他	1
計		22



［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。

本四半期に連絡不能開発者一覧に新たに掲載した案件はありませんでした。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場合、IPA が招集する公表判定委員会が妥当と判断すれば、公表できることに 2014 年から制度が改正されました。既に前年度までに 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きました。2017 年度においては、12 月に開催された公表判定委員会で 4 件が審議され、すべて公表すべきと判定されました。前年度までの 5 件と今年度の 4 件を合わせた全 9 件を、本年度末までに公表するべく IPA とともに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 など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 46 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。

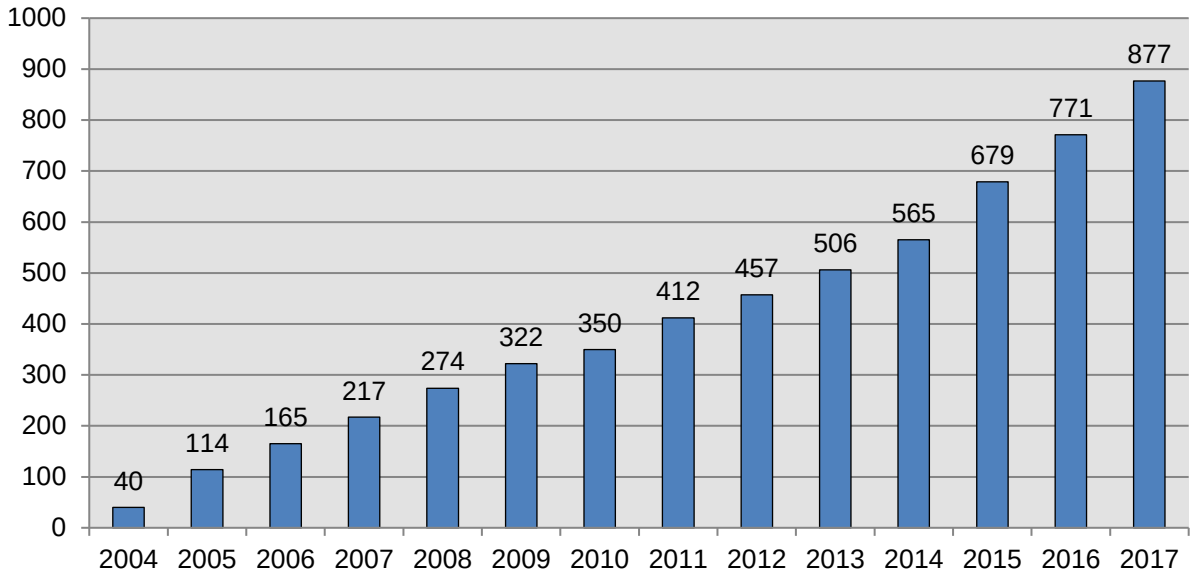
脆弱性情報取扱体制
http://www.meti.go.jp/policy/netsecurity/vulhandlingG.html
脆弱性情報コーディネーション概要
https://www.jpcert.or.jp/vh/

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（2017 年版）
https://www.jpcert.or.jp/vh/partnership_guideline2017.pdf
JPCERT/CC 脆弱性情報取扱いガイドライン（2017 年版）
http://www.jpcert.or.jp/vh/vul-guideline2017.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 12 月 31 日現在で 877 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。

製品開発者登録
http://www.jpcert.or.jp/vh/regist.html



［図 2-4 累計製品開発者登録数］

2.2.2. 製品開発者との定期ミーティングの実施

JPCERT/CC では、技術情報やセキュリティ・脆弱性の動向などの情報交換や、脆弱性情報ハンドリング業務に関する製品開発者との意見交換、また、製品開発者間の情報交換を目的として、脆弱性情報ハンドリングにご協力いただいている製品開発者の皆さまとのミーティングを定期的に開催しています。
2017 年 10 月 31 日に開催したミーティングは、最近の脆弱性事例をもとにした対策手法の研究成果や脆弱性管理の省力化・自動化ツールの紹介、脆弱性診断する側から製品開発者への提言、脆弱性情報の記述法に関する提案など、技術的なトピックを中心にプログラムを構成し、各テーマについて講演と意見交換

を行いました。

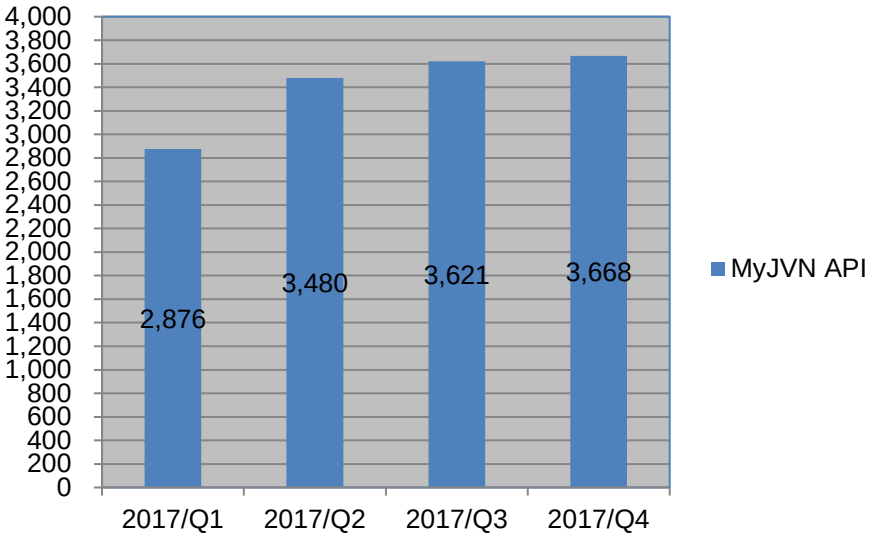
［図 2-5 製品開発者との定期ミーティングの様子］

2.3. VRDA フィードによる脆弱性情報の配信

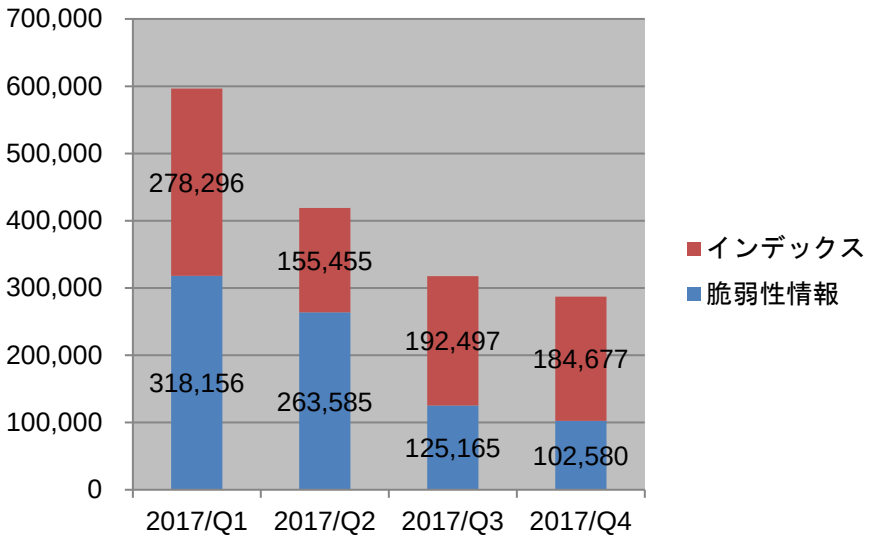
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、KENGINE 等のツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API を外部データソースとして利用した、VRDA（Vulnerability Response Decision Assistance）フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情報は、次の Web ページを参照ください。

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

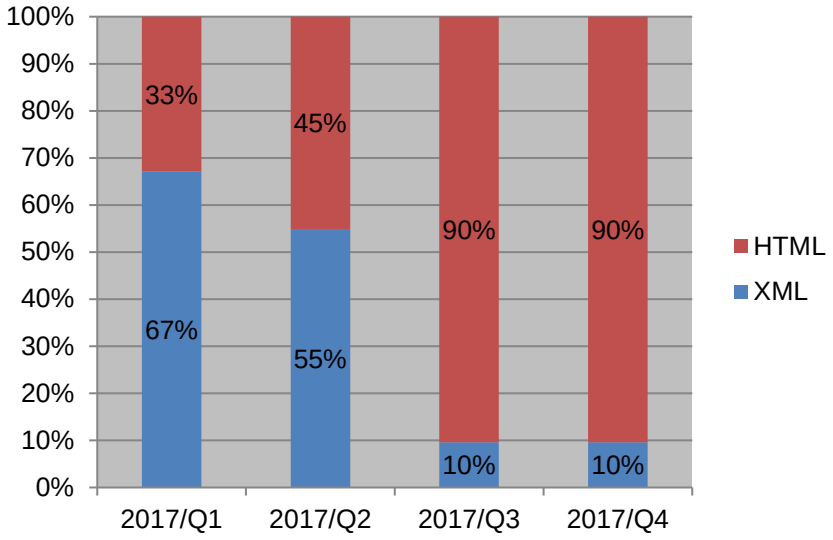


［図 2-6 VRDA フィード配信件数］



［図 2-7 VRDA フィード利用件数］

インデックスの利用数については、［図 2-7］に示したように、前四半期と比較し、約 4%減少しました。脆弱性情報の利用数についても、約 18%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］

脆弱性情報のデータ形式別利用傾向については、［図 2-8］に示したように、前四半期と比較し、変化は有りませんでした。

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。本四半期に収集・分析した情報は 409 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 7 件でした。

2017/10/06 【参考情報】電力用スマートメータの脆弱性情報について
2017/10/13 【参考情報】Siemens 社製 BACnet Field Panel の脆弱性情報について
2017/10/17 【参考情報】スウェーデンで発生した通信事業者へのサイバー攻撃による列車運行への影響について
2017/10/19 無線 LAN の WPA2 における複数の脆弱性に関する注意喚起
2017/10/24 【参考情報】米国エネルギー業界などを標的とした高度サイバー攻撃 (APT) 活動について (TA17-293A)

2017/12/15　CODESYS に関する情報提供
2017/12/20　【参考情報】Schneider Electric 社製の安全計装コントローラ Triconex を標的にしたマルウエアに関する情報

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。

2017/10/11　制御システムセキュリティニュースレター 2017-0009
2017/11/13　制御システムセキュリティニュースレター 2017-0010
2017/12/07　制御システムセキュリティニュースレター 2017-0011

制御システムセキュリティ情報共有コミュニティには、制御システムセキュリティ情報提供用メーリングリストと制御システムセキュリティ情報共有ポータルサイト ConPaS があり、メーリングリストには現在 774 名の方にご登録いただいています。今後も各サービスの内容の充実を図り、さらなる利用を促進していく予定です。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

JPCERT/CC は、制御システム関連のインシデント対応の分野で、インシデント報告の受付、およびインターネットからアクセスできる可能性がある制御システムの探索とそれら制御システムを保有している国内の組織に対する情報提供の 2 つの活動を展開しています。本四半期における活動は次のとおりです。

(1) インシデント報告の受付
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（0 IP アドレス）でした。

(2) インシデント未然防止活動
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発見したため、そのシステムを保有する国内の組織に対してインターネットからアクセスできる可能性があるという情報を 20 件（68IP アドレス）提供しました。

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 5 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 247 件となりました。

日本版 SSAT(SCADA Self Assessment Tool)
https://www.jpcert.or.jp/ics/ssat.html

制御システムセキュリティ自己評価ツール(J-CLICS)
https://www.jpcert.or.jp/ics/jclics.html

3.5 海外カンファレンス出張報告会の開催

JPCERT/CC では、制御システム・セキュリティに関する国内外の最新動向の情報を入手して分析し、種々の対策活動の計画立案や具体的な進め方を判断する際の参考情報をして役立てるとともに、収集した情報を国内の関係者にお知らせする活動を行っています。
本四半期においては、次の 2 つの海外カンファレンスを聴講し、欧米における技術動向に関する情報を収集しました。

CS3sthlm（今回から改称；前年までの会議名は 4SICS）
(Cyber Security in Control Systems for Critical Societal Functions (CS3) in STHLM, Sweden)
開催地： ストックホルム市（スウェーデン）
開催日： 10 月 25～26 日

Industrial Control Systems (ICS) Cyber Security Conference
開催地：アトランタ市（アメリカ）
開催日：10 月 23～26 日

また、国内の関係者に呼びかけて 12 月 22 日に報告会を催し、これらの会議の概要を共有しました。アセット・オーナーを中心に制御システムに関わっている 29 名の方々が参加されました。

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、研修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。本四半期は新規の研修教材の開発を進めました。

4.2. 国際 CSIRT 間連携

国境をまたぐインシデントへのスムーズな対応等を目的に、JPCERT/CC は海外 CSIRT との連携強化を進めています。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）のメンバーに選出されており、事務局も担当しています。APCERT の詳細および APCERT における JPCERT/CC の役割については、次の Web ページをご参照ください。

JPCERT/CC within APCERT
https://www.jpcert.or.jp/english/apcert/

4.2.1.1. APCERT Steering Committee 会議の実施

Steering Committee は 11 月 1 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 メンバー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 年次総会 2017 への参加（11 月 12 日 - 15 日）

アジア太平洋地域の CSIRT コミュニティである APCERT の年次総会がインドのデリーで開催されました。APCERT の主要メンバーであるオペレーショナルメンバー（全 30 チーム）から、JPCERT/CC を含む 22 チームが参加しました。
APCERT 年次総会は、各経済地域における最近のインターネットセキュリティ動向、インシデント対応の事例、調査・研究活動等を共有することを目的に、毎年開催されています。今年のテーマは”Building Trust in Digital Economy”でした。開催概要は次のとおりです。

(1) 日程：

11/12（日）	午前：APCERT ワーキンググループ会合
	午後：APCERT チームビルディングイベント
11/13（月）	午前：TSUBAME ワークショップ
	午後：APCERT Steering Committee 会議
11/14（火）	午前：メンバー向けカンファレンス（Closed Conference）
	午後：APCERT 年次総会（Annual General Meeting）
11/15（水）	終日：一般公開講演（Open Conference）

(2) 会場：Hotel The Ashok, Delhi, India

(3) 主な決定事項等：

APCERT Steering Committee および年次総会では、APCERT の運営上の規約をまとめた Operational Framework の文書の見直しが行われました。

メンバー向けカンファレンスにおいては、マルウエア分析の事例や、モバイル端末に特化したインシデントの対応事例、ボットネット・クリーンアップセンターの立ち上げや近隣諸国への能力向上支援のプロジェクトなど、各チームで行っている取り組みについて紹介しました。

一般公開講演においては、こうした CSIRT レベルの取組みの紹介に加えて、大学や民間企業の専門家よりフィンテックやインダストリアルインターネットなど、新しい分野に係るサイバー脅威や、人工知能や機械学習を用いたサイバー脅威観測の事例紹介などがありました。

Steering Committee の選挙では、JPCERT/CC と MyCERT（マレーシアコンピュータ緊急対応チーム）が再選されるとともに、CERT-In（インドコンピュータ緊急対応チーム）が初めて選出されました。さらに、APCERT 議長チームおよび副議長チームの改選が行われ、CERT Australia（オーストラリアコンピュータ緊急対応チーム）が議長チームとして、MyCERT が副議長チームとしてそれぞれ再選されるとともに、JPCERT/CC が事務局に再選されました。JPCERT/CC は、引き続き APCERT の主要メンバーとしてさまざまな活動をリードしてまいります。

［図 4-1　APCERT 年次総会集合写真］

APCERT 年次総会についての詳細は、次の Web ページをご参照ください。

APCERT Annual General Meeting & Conference 2017
https://apcert2017.in/index.html

4.2.2. FIRST（Forum of Incident Response and Security Teams）

JPCERT/CC は、1998 年の加盟以来、FIRST の活動に積極的に参加しています。現在は JPCERT/CC の国際部シニアアナリスト 小宮山功一朗が FIRST の理事を務めており、本四半期は 10 月 1 日から 4 日にかけてモントリオール（カナダ）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。また四半期に一度開催されるシンポジウムの準備調整を進めました。FIRST と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

4.2.3. CERT-Ro 年次会合参加（10 月 30 日-11 月 1 日）

ルーマニアの National CSIRT である CERT-Ro が毎年開催している年次会合「CERT-Ro Conference」に出席しました。JPCERT/CC は、欧州やアジア等の CSIRT が参加するセッションにおいて、日本の標的

型攻撃の状況や JPCERT/CC の脅威分析への取り組み等を紹介しました。また、サイバーセキュリティの政策面や脅威分析等を議論するパネルディスカッションを聴講しました。

4.2.4. 米 US-CERT-JPCERT/CC 年次定例会合（11 月 29 日）及び第 13 回日米重要インフラ防護フォーラム（11 月 30 日-12 月 1 日）参加

JPCERT/CC は、インシデント対応で協力関係にある米国の US-CERT、ICS-CERT との年次会合を 12 月 1 日にワシントン D.C.で行いました。それぞれの組織の活動状況や、日米におけるインシデント動向およびインシデント対応における連携等について情報共有および意見交換を行い、今後も密な連携を維持していくことを確認しました。
また、11 月 30 日および 12 月 1 日に開催された、第 13 回日米重要インフラ防護フォーラムを聴講し、情報収集を行いました。

4.3. CyberGreen

国際的なプロジェクトである CyberGreen は、インターネット全体の健全性とリスクを評価する指標を用いて各国／地域間で比較を行い、各国の CSIRT や ISP、セキュリティベンダーといった技術パートナーが、それぞれの担当領域の指標値を向上させる施策に努めることを通じて、より効率的に健全なサイバー空間を実現することを目的としています。2015 年 11 月に設立された日本発の国際 NPO である CyberGreen Institute がプロジェクトの中心を担っています。前四半期より、JPCERT/CC は、CyberGreen Institute が収集したデータに対し、検索条件や抽出方法の改善などデータを利用する立場から提案を行っていますが、本四半期においても継続して提案を行いました。

CyberGreen Institute については、次の Web ページをご参照ください。
https://www.cybergreen.net/

4.4. その他国際会議への参加

4.4.1. The Global Commission on the Stability of Cyberspace（GCSC）会合への参加（11 月 20 日-11 月 21 日）

2017 年 3 月にサイバー空間における規範を議論する場として The Global Commission on the Stability of Cyberspace (GCSC) が発足しました。その中に設けられた、複数の分野ごとにオープンな議論を行うことを目的とするワーキンググループの副議長に JPCERT/CC の小宮山が就任しております。
11 月 20 日と 21 日に、インドのニューデリーで当該分野の専門家を集めた GCSC の会合が開かれ、小宮山が意見発表などを行いました。また本会合以外にも調査プロジェクトのサポートを日頃から行っています。

GCSC の詳細は、次の Web ページをご参照ください。

The Global Commission on the Stability of Cyberspace (GCSC)
https://cyberstability.org/

4.4.2. Global Conference on Cyber Space 2017 への参加（11 月 23 日-11 月 24 日）

11 月 23 日から 24 日にかけて、インドのニューデリーにおいて行われた Global Conference on Cyber Space 2017（サイバー空間に関するニューデリー会議、略称 GCCS2017）に出席しました。GCCS2017 は、2011 年のサイバー空間に関するロンドン会議、2012 年の同ブダペスト会議、2013 年の同ソウル会議、2015 年の同ハーグ会議に続く第 5 回目になります。政府、民間企業、市民社会を代表するサイバーセキュリティの有識者が集い、サイバー空間について議論しました。JPCERT/CC はこの会議に出席し、CSIRT に期待される役割を確認し、また各国関係者と意見交換を行いました。
GCCS2017 の詳細は、次の Web ページをご参照ください。

GCCS2017
https://gccs2017.in/

4.4.3. APEC TEL 56 への参加（12 月 11 日-12 月 15 日）

12 月 11 日から 15 日にかけてタイのバンコクで開催された APEC TEL (APEC Telecommunications and Information Working Group) 56 に参加しました。APEC TEL は、APEC に参加しているエコノミーにおいて情報電気通信分野を担当する政府機関を中核とする会合です。
JPCERT/CC は APEC TEL56 内のワークショップにおいて、日本のサイバー演習の取り組みについての講演をおこないました。

4.5. 国際標準化活動

IT セキュリティ分野の標準化を行うための組織 ISO/IEC JTC-1/SC27 で進められている標準化活動のうち、作業部会 WG3（セキュリティの評価・試験・仕様）で検討されている脆弱性の開示と取り扱いに関する標準の改定と、WG4（セキュリティコントロールとサービス）で検討されているインシデント管理に関する標準の改定に、情報処理学会の情報規格調査会を通じて参加しています。

今四半期は、10 月 30 日から 11 月 3 日にかけてベルリンで開催された標準化会議に参加し、脆弱性の開示(ISO/IEC 29147)と脆弱性の取扱手順(ISO/IEC 30111)の改定草案に対して事前に各国から提出されていたコメントの取り扱いを関係者と協議しました。

4.6. 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。

Visualise Event Logs to Identify Compromised Accounts - LogonTracer -（11 月 30 日）
http://blog.jpcert.or.jp/2017/11/visualise-event-logs-to-identify-compromised-accounts---logontracer-.html

Research Report Released: Detecting Lateral Movement through Tracking Event Logs (Version 2)（12 月 5 日）
http://blog.jpcert.or.jp/2017/12/research-report-released-detecting-lateral-movement-through-tracking-event-logs-version-2.html

5. 日本シーサート協議会（NCA）事務局運営

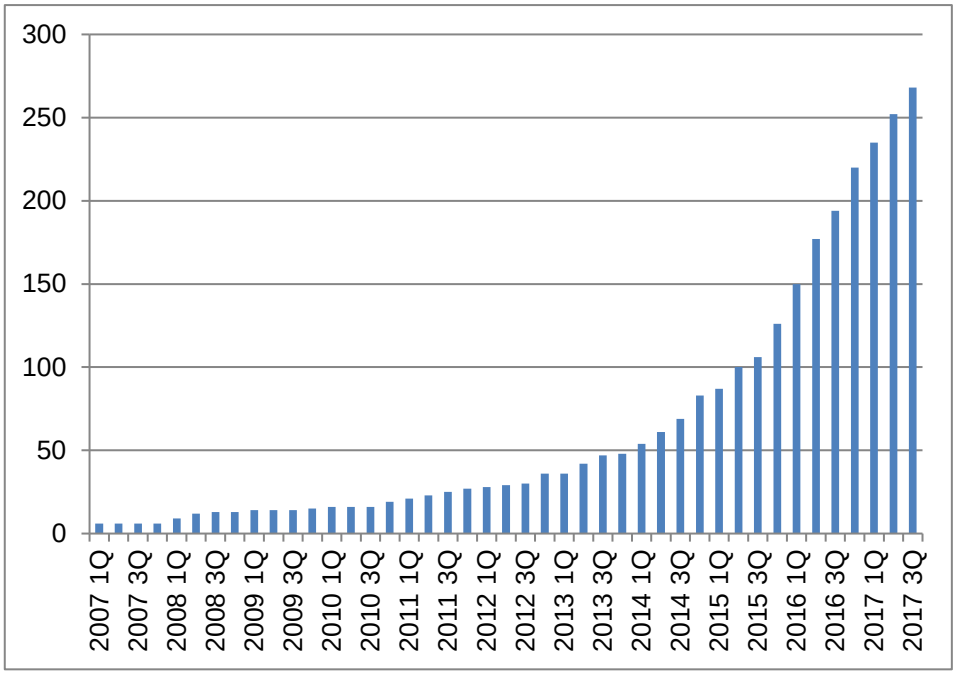
5.1. 概況

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 16 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。

株式会社日清製粉グループ本社 (NISSHIN-CSIRT)
freee 株式会社 (freee-CSIRT)
株式会社 MC データプラス (MCDP-CSIRT)
エムオーテックス株式会社 (MOTEX-CSIRT)
エキサイト株式会社 (ExSIRT)
株式会社テプコシステムズ (TEPSYS－SIRT)
デジタル・アドバタイジング・コンソーシアム株式会社 (DAC-CSIRT)
NTT アドバンステクノロジ株式会社 (AT-CSIRT)
ネオファースト生命保険株式会社 (NFL-CSIRT)
株式会社オウケイウェイヴ (OKWAVE-CSIRT)
株式会社　セガホールディングス (S2SIRT)
藤田観光株式会社 (FK-SIRT)

本四半期末時点で 268 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 19 回シーサートワーキンググループ会

第 19 回シーサートワーキンググループ会を次のとおり開催しました。

日時：2017 年 12 月 4 日
場所：TDU-CSIRT (東京電機大学)

第 19 回シーサートワーキンググループ会は、NCA の会員および NCA 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組織が参加する会合です。会合では、各ワーキンググループからの活動報告や、新しく加盟した 17 チームによる自組織のシーサートの概要紹介に加えて、次の 2 つの講演がおこなわれました。

講演 1
「メールセキュリティについて」
一般財団法人日本情報経済社会推進協会（JIPDEC）　高倉　万記子氏

講演 2
「身近にある法制度面の課題」
萩原 健太氏（日本シーサート協議会　副運営委員長）

5.3. 日本シーサート協議会　運営委員会

本四半期は、次のとおり 3 回の運営委員会を開催しました。

第 125 回運営委員会
日時：2017 年 10 月 30 日（月）16:00 - 18:00
場所：OKI-SIRT

第 126 回運営委員会
日時：2017 年 11 月 29 日（水）16:00 - 18:00
場所：TM-SIRT

第 127 回運営委員会
日時：2017 年 12 月 20 日（水）16:00 - 18:00
場所：JPCERT/CC

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（本節の以下において「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、一般消費者からのフィッシングに関する報告・問い合わせの受付、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

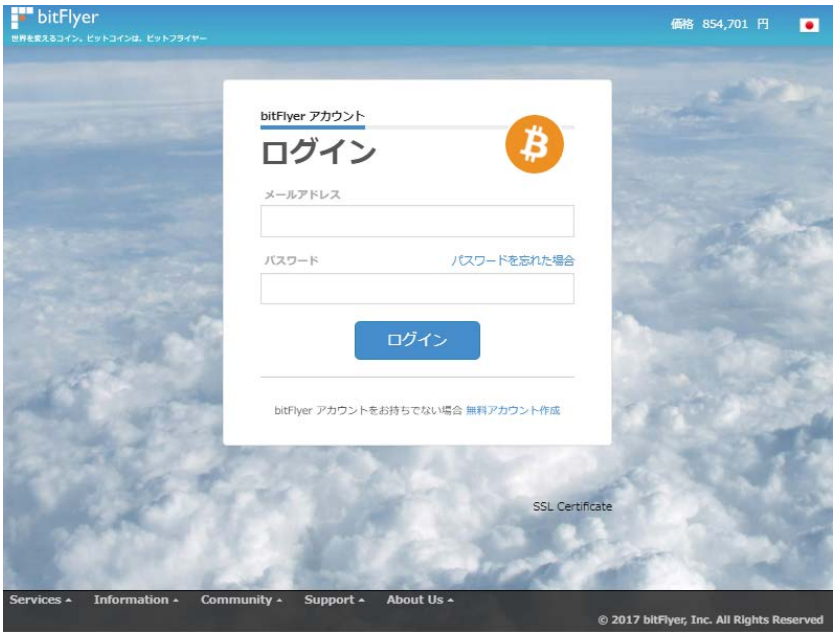
本四半期は、協議会 Web サイトや会員向けメーリングリストを通じて、フィッシングに関するニュースや緊急情報を 14 件発信しました。

本四半期も前四半期に引き続き、Amazon、Apple 等の E コマースサイトをかたりクレジットカード情報を不正に詐取するフィッシング、および LINE をかたりアカウント情報を詐取するフィッシングについて、多くの報告が寄せられました。これらのサービスは利用者数も多く、影響範囲も大きいため、緊急情報を発行し注意を促しました。また、仮想通貨関連サービス事業者の大手である bitFlyer をかたるフィッシングの報告についても多くの報告が寄せられたため、緊急情報を発行しました。

本四半期は、7 件の緊急情報を協議会 Web サイト上に掲載し、広く注意を喚起しました。その内訳は次のとおりです。

ライセンス更新をかたるフィッシング関連：0 件
SNS サービスをかたるフィッシング関連：1 件
クレジットカード会社をかたるフィッシング関連：1 件
E コマースサイトをかたるフィッシング関連：4 件
仮想通貨関連サービスをかたるフィッシング関連：1 件

仮想通貨関連サービスをかたるフィッシングの例として、［図 6-1］に bitFlyer をかたるフィッシング (2017/11/06) の注意喚起に掲載したフィッシングサイト画像を示します。



［図 6-1 bitFlyer をかたるフィッシングサイト ］
https://www.antiphishing.jp/news/alert/bitflyer_20171106.html

これらのフィッシングサイトについて、JPCERT/CC のインシデント対応支援活動を通じて、サイトを停止するための調整を行いました。

6.2. フィッシングサイト URL 情報の提供

協議会の会員のうち、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 を集めたリストを提供しています。この URL 情報の提供は、各社の製品においてブラックリストに登録する等、ユーザ保護に向けた取り組みへの活用や、研究教育機関における関連研究への利用を目的としています。本四半期末の時点で 37 組織に対し URL 情報を提供しており、今後も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の動向を紹介し、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。

(1) 駒場 一民（エンタープライズサポートグループ　情報セキュリティアナリスト）
「フィッシングの現状と対策 2017」フィッシング対策セミナー2017 , 2017 年 11 月 10 日
「フィッシングの現状と対策 2017」北海道地域情報セキュリティセミナー，2017 年 11 月 22 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 10 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201710.html
フィッシング対策協議会 2017 年 11 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201711.html
フィッシング対策協議会 2017 年 12 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201712.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のほかに、協議会の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 55 回運営委員会
日時：2017 年 10 月 13 日 16:00 - 18:00
場所：JPCERT/CC

フィッシング対策協議会 第 56 回運営委員会
日時：2017 年 11 月 2 日 16:00 - 18:00
場所：NTT コミュニケーションズ株式会社

フィッシング対策協議会 第 54 回運営委員会
日時：2017 年 12 月 8 日 16:00 - 18:00
場所：トレンドマイクロ株式会社

7.2. フィッシング対策セミナー 2017 開催

フィッシング対策ガイドライン実践セミナー 2017 を次のとおり開催しました。

フィッシング対策セミナー 2017
日時：2017 年 11 月 10 日 13:00 - 18:00
場所：大崎ブライトコアホール（JR 大崎駅 新東口）
東京都品川区北品川 5 丁目 5 番 15 号 大崎ブライトコア 3 階
講演内容：
講演 1：「フィッシング対策に求められる科学的・工学的アプローチ」
講演者：国立大学法人奈良先端科学技術大学院大学 教授 門林 雄基氏
講演 2：「最近のサイバー犯罪の発生状況」
講演者 2：警察庁生活安全局情報技術犯罪対策課 官民連携推進官 高尾 健一氏
講演 3：「フィッシングの現状と対策 2017」
講演者 3：フィッシング対策協議会 (JPCERT/CC) 駒場 一民氏
講演 4：「セブン銀行口座における不正利用対策への取組みについて」

講演者 4：株式会社セブン銀行 金融犯罪対策部 7BK-CSIRT 次長 安田 貴紀氏
講演 5：「LINE をかたるフィッシングサイトを実際に調査してわかったこと」
講演者 5：LINE 株式会社 中村 智史氏

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、それぞれ受付機関および調整機関として、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）等に基づく脆弱性関連情報流通制度の運用の一端を 2004 年 7 月から担っています。
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。

ソフトウエア等の脆弱性関連情報に関する届出状況[2017 年第 3 四半期（7 月～9 月）]
（2017 年 10 月 25 日）
https://www.jpcert.or.jp/press/2017/vulnREPORT_2017q3.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(2017 年 7～9 月)
（2017 年 11 月 30 日）
https://www.jpcert.or.jp/tsubame/report/report201707-09.html
https://www.jpcert.or.jp/tsubame/report/TSUBAMEReport2017Q2.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 2 件の記事を公開しました。

(1) 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（第 2 版） (2017-11-09)
JPCERT/CC では、攻撃者がネットワーク内に侵入した後に利用する可能性が高いツールやコマンドを調査し、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た結果をまとめたレポート「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」の第 2 版を 2017 年 11 月に公開しました。第 2 版では、調査対象とするツールやコマンド、OS の更新、並びにツール分析結果の追加を行っています。また、HTML 形式の「ツール分析結果シート」も報告書と同時に公開しました。合わせてご活用ください。

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（第 2 版） (2017-11-09)
https://www.jpcert.or.jp/magazine/acreport-ir_research2.html

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 日公開）
https://www.jpcert.or.jp/research/ir_research.html

(2) イベントログを可視化して不正使用されたアカウントを調査 ~LogonTracer~（2017-11-28）
イベントログの分析はセキュリティインシデントの調査において欠かせない作業である一方、環境によっては膨大になるイベントログの分析に多くの時間が必要となります。本記事では、こうした状況を改善する一助として JPCERT/CC が作成したイベントログの分析をサポートするツール「LogonTracer」を紹介しています。「LogonTracer」を用いることで、ログオンに関連するイベントログに含まれるホスト名（または IP アドレス）とアカウント名を関連付けて可視化（グラフ表示）でき、比較的簡単にイベントログの分析を行うことが可能になります。

イベントログを可視化して不正使用されたアカウントを調査 ~LogonTracer~（2017-11-28）
https://www.jpcert.or.jp/magazine/acreport-logontracer.html

9. 主な講演活動

(1) 中村 祐（分析センター）：
「アーティファクト分析とサイバー攻撃対応」
警察大学校研修,2017 年 10 月 2 日

(2) 宮地 利雄 (技術顧問)：
「最近の海外でのサイバー攻撃によるインフラ被害 ～制御システムを中心に～」
明治大学国際総合研究所 第 4 回サイバーセキュリティ政策に関する研究会，2017 年 10 月 5 日

(3) 真鍋 敬士（理事・最高技術責任者）:
「つながるインシデント vs つなげる対応」
情報セキュリティワークショップ in 越後湯沢 2017, 2017 年 10 月 6 日

(4) 戸田 洋三（情報流通対策グループ）、久保正樹（情報流通対策グループ マネージャー）:
「セキュアプログラミング Web アプリケーション（演習）」
東京電機大学 国際化サイバーセキュリティ学特別コース(CySec)「セキュアシステム設計・開発」, 2017 年 10 月 7 日

(5) 洞田 慎一（早期警戒グループ マネージャー）:
「IoT をとりまくセキュリティの現状と課題」
第 9 回 TCG 日本支部公開ワークショップ,2017 年 11 月 20 日

(6) 川居 裕人（早期警戒グループ）:
「サイバー攻撃の最新動向と対応」
大日本印刷グループ社内セミナー, 2017 年 11 月 21 日

(7) 村上 晃（経営企画室、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その対処」
京都府サイバーテロ対策連絡会総会, 2017 年 11 月 22 日

(8) 真鍋 敬士（理事・最高技術責任者）:
「日本が直面しているセキュリティ・リスク、そして、求められる取り組み」
CheckPoint Experience Japan, 2017 年 11 月 28 日

(9) 戸田 洋三（情報流通対策グループ）:
「インターネットとセキュリティと JPCERT/CC」
早稲田大学 「サイバー攻撃対策技術の基礎」ゲスト講演, 2017 年 12 月 8 日

10. 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) Hardening Project 2017
主　催：Hardening Project実行委員会
開催日：2017年6月23日～11月25日

(2) 第13回IPAひろげよう情報モラル・セキュリティコンクール2017
主　催：IPA（独立行政法人情報処理推進機構）
開催日：2017年6月1日～2018年3月31日

(3)情報セキュリティワークショップ in 越後湯沢 2017
主　催：INPO新潟情報セキュリティ協会（ANISec）/ 情報セキュリティワークショップin越後湯沢実行委員会
開催日：2017年10月6日～10月7日

(4) Cyber3 Conference Tokyo 2017

主　催：日本経済新聞社、日経BP社

開催日：2017年10月5日～10月6日

(5) CODE BLUE2017

主　催：CODE BLUE実行委員会

開催日：2017年11月7日～11月10日

(6) 第9回TCG日本支部公開ワークショップ

主　催：TCG日本支部

開催日：2017年11月20日

(7) Internet Week2017

主　催：一般社団法人日本ネットワークインフォメーションセンター

開催日：2017年11月28日～12月1日

(8) 第14回デジタル・フォレンジック・コミュニティ2017inTOKYO

主　催：特定非営利活動法人デジタル・フォレンジック研究会、デジタル・フォレンジック・コミュニティ2017実行委員会

開催日：2017年12月11日～12月12日

(9) SecurityDay2017

主　催：SecurityDay運営委員会

開催日：2017年12月14日～12月15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