JPCERT Coordination Center

JPCERT/CC 活動概要

2019 年 1 月 1 日 ～ 2019 年 3 月 31 日

一般社団法人 JPCERT コーディネーションセンター

2019 年 4 月 11 日

JPCERT CC®

活動概要トピックス

ートピック 1ー「2018 年度 中南米 CSIRT 動向調査」を公開

JPCERT/CC は、中南米各国の CSIRT やサイバーセキュリティに関わる体制等について公開文献と現地でのヒアリングにより調査した結果をまとめた「**2018 年度 中南米 CSIRT 動向調査**」を公開しました。

サイバー攻撃は国境に関係なく発生し、海外のネットワークから日本のユーザを狙って攻撃されるケースも、逆に日本国内のネットワークから海外が攻撃されるケースもあります。こうした国際的な事案の調整・解決にあたって、国の窓口となる CSIRT 間での情報共有や協力が不可欠となっています。そのために JPCERT/CC では国際的な CSIRT のコミュニティである FIRST や APCERT 等への参加や、海外各国の CSIRT との連携強化を通じて、国をまたいだ協力が必要な事案へスムーズに対応できる体制を構築しています。しかしながら、海外の中で距離的にも遠い中南米地域については、これまでインシデント事案に伴う情報共有はあったものの、各国の CSIRT やサイバーセキュリティに関わる体制等については、日本語で体系的にまとめられた文書も少なく、実態が十分には分かっていませんでした。

本書は、中南米地域で OAS (米州機構)や LACNIC(Latin America and Caribbean Network Information Centre)が主導している CSIRT 間連携の現状、および、この地域でもっともサイバーセキュリティに関する取組みが進んでいるメキシコとブラジル両国の窓口 CSIRT の活動状況と彼らが直面するサイバー脅威の実態について、公開文献と現地でのヒアリングにより調査した結果をまとめたものです。

海外におけるサイバーセキュリティの取組みに関心のある組織、また中南米地域でビジネスを展開している組織において、現状の把握のための参考資料としてご活用ください。

2018 年度　中南米 CSIRT 動向調査
https://www.jpcert.or.jp/research/LACSIRT-survey.html

ートピック2ー　Japan Security Analyst Conference 2019 を開催

2019 年 1 月 18 日、御茶ノ水ソラシティカンファレンスセンターにおいて「Japan Security Analyst Conference 2019 （JSAC2019）」を開催しました。本カンファレンスは、サイバー攻撃によるインシデントの分析・対応を行っているセキュリティアナリストの技術力向上に資するために、刻々と変化する攻撃の手口や新たな分析手法について情報を共有することを目的としています。2 回目の開催となる今回は、297 名のセキュリティアナリストに参加いただきました。講演募集（CFP）に 18 件(国内: 12 件、海外: 6 件)の応募をいただき、その中から選定されたマルウエア分析やインシデント対応事例といったインシデント分析・対応に関する技術に関して、講演者独自の新し

い技術的な知見や、分析手法など 8 件について講演が行われました。また、前回も海外からの参加をいただいていましたが、今回は海外のアナリストによる講演もあり、JSAC の国際化が一段と進みました。

なお、JSAC2019 の講演資料は一部の講演を除いて公開しており、講演の様子を JPCERT/CC Eyes でも紹介しています。JPCERT/CC では、今後も引き続きインシデント分析・対応を行う技術者に有益な情報発信や活動を実施してまいります。

Japan Security Analyst Conference 2019
https://jsac.jpcert.or.jp/
Japan Security Analyst Conference 2019 開催レポート～前編～
https://blogs.jpcert.or.jp/ja/2019/01/jsac2019report1.html
Japan Security Analyst Conference 2019 開催レポート～後編～
https://blogs.jpcert.or.jp/ja/2019/02/jsac2019report2.html

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 2019」を開催

2019 年 2 月 15 日（金）に東京浅草橋で「制御システムセキュリティカンファレンス 2019」を開催しました。事前に参加登録した約 300 名の方々にご来場いただき、その内訳は、アセットオーナが 30%、制御システム機器ベンダが 11%、制御システムベンダが 15%、制御システムエンジニアリング会社が 11%、研究者が 5%でした。カンファレンスを始めた 10 年前は、制御システムベンダが参加者の多くを占めていましたが、近年はアセットオーナの占める割合が増えており、サイバーセキュリティリスクを認識し、自社の事業を安全に継続するための情報収集および対策を進めることの重要性が広く理解されてきていると思われます。本カンファレンスでは、講演募集(CFP)に応募いただいた 2 件を含む、7 件の講演が行われました。講演では、最新の制御システムセキュリティに関する脅威情報や想定すべきシナリオ、海事・鉄道・保険分野におけるガイドライン・標準化の動向およびサイバー・セキュリティへの取組み、機能安全の体系でサイバーセキュリティを扱う手法、産業用 IoT 導入のためのセキュリティ対策ガイド等についてお話いただきました。

制御システムセキュリティカンファレンス 2019
https://www.jpcert.or.jp/event/ics-conference2019.html
制御システムセキュリティカンファレンス 2019 講演資料
https://www.jpcert.or.jp/present/#year2019

JPCERT CC®

目次

本活動は、経済産業省より委託を受け、「平成 30 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。

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 4,433 件、インシデント件数ベースでは 4,972 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 2,916 件でした。前四半期の 2,579 件と比較して 13%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/2019/IR_Report20190411.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

本四半期に報告が寄せられたフィッシングサイトの件数は 1,753 件で、前四半期の 1,560 件から 12%増加しました。また、前年度同期（924 件）との比較では、65%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	98	72	88	258(15%)
国外ブランド	301	430	467	1,198(68%)
ブランド不明 (注 5)	107	89	101	297(17%)
全ブランド合計	506	591	656	1,753(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。

E コマースサイトを装ったフィッシングサイトに関する報告は前四半期よりも多く寄せられています。中でも特定の国外ブランドのフィッシングサイトの報告数が一年前と比較して倍増し、全体の半数以上を占めるに到りました。
国外ブランドのフィッシングサイトに使われるドメインは約半数が.com ドメインで中には日本語ドメインや日本語 TLD の「.コム」ドメインを使用したものもありました。
また、短縮 URL サービスを利用してフィッシングサイトへ転送されるケースも多く報告があり、中には複数の短縮 URL サービスを経由した後にフィッシングサイトへ転送されるケースもありました。

国内ブランドのフィッシングサイトでは SNS を装ったフィッシングサイトが前四半期に比べて減少しましたが、金融機関や通信事業者を装ったフィッシングサイトについては増加傾向にありました。

金融機関を装ったフィッシングサイトについてはブランド名の後ろに co や cojp などの文字列を加えたものに.com, .org.などの gTLD や.eu, .it, .za などの ccTLD など様々な TLD を組み合わせたドメインが使用されていました。
また、中には定期的にサイトの稼働と停止を繰り返すものもありました。

通信事業者を装ったフィッシングサイトについては大半が台湾の IP アドレス上で稼働しており、ドメイン名については正規サイトと似た紛らわしい.com ドメインを使用したものが多く、そのほとんどが中国のレジストラで取得されたものでした。

フィッシングサイトの調整先の割合は、国内が 21%、国外が 79%であり、前四半期（国内が 28%、国外が 72%）と比べて国外への通知の割合が増加しました。

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、229 件でした。前四半期の 242 件から 5%減少しています。

2 月頃から、改ざんされた Web サイトから次のような URL の Web ページを経由し、不審なサイトに転送されるといった報告が複数寄せられています。

```
https[:]//somelandingpage[.]com/3gGykjDJ?frm=script&#038;
```

上記 URL の Web ページへの転送は、改ざんされたページの至る所に埋め込まれた JavaScript によって行われ、約 50 もの同一の改ざんコードが挿入されているページも確認しました。改ざんされていた HTML ソースの例を［図 1-1］に示します。

［図 1-1　改ざんされた Web ページの HTML ソースに埋め込まれた JavaScript］

改ざんされた Web サイトからの転送先として、不審なブログサイトや、不審なソフトウエアをダウンロードさせる Web サイトなどを確認しています。この不正な転送は、次のような.tk ドメインの URL をもつものを含む、複数の Web サイトを経由する特徴があります。

```
http://<ドメイン名>.tk/index/?<数字の列>
```

1.1.1.3. その他

標的型攻撃に分類されるインシデントの件数は、6 件でした。前四半期の 4 件から 50%増加しています。本四半期に対応を依頼した組織は 3 組織でした。次に、確認されたインシデントを紹介します。

(1) 資産管理ソフトウエアの脆弱性を悪用した新たなマルウエアの感染を試みる標的型攻撃
2018 年 3 月以前から、資産管理ソフトウエアの脆弱性を悪用して xxmm や Datper と呼ばれるマルウエアに感染させる攻撃がありましたが、2019 年 1 月に、JavaScript で作成された新たなマルウエアに感染させる攻撃の報告が寄せられました。このマルウエアは Node.js を使って動作し、HTTP で C&C サーバと通信します。C&C サーバから受信する命令により、任意のコマンドの実行や、ファイルのアップロード・ダウンロード、感染した端末の情報を送信する可能性があります。

(2) DNS の A レコードを利用して通信を行う Cobalt Strike
ペネトレーションテストツール Cobalt Strike を悪用した攻撃の報告が 2019 年 2 月に寄せられました。Cobalt Strike は HTTP,HTTPS の他、DNS プロトコルを利用して C&C サーバと通信する機能を持っており、今回の攻撃では DNS の A レコードの問合せと応答を用いて C&C サーバと通信を行っていました。

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 CISTA（Collective Intelligence Station for Trusted Advocates）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。

発行件数：0 件

1.2.1.2. 注意喚起

深刻かつ影響範囲の広い脆弱性等が公表された場合には、「注意喚起」と呼ばれる情報を発行し、利用者に対して広く対策を呼びかけています。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：14 件（うち 2 件は更新情報）　https://www.jpcert.or.jp/at/

2019-01-04　Adobe Acrobat および Reader の脆弱性 (APSB19-02) に関する注意喚起 (公開)
2019-01-09　2019 年 1 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)
2019-01-16　2019 年 1 月 Oracle 製品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)
2019-02-13　Adobe Acrobat および Reader の脆弱性 (APSB19-07) に関する注意喚起 (公開)
2019-02-13　Adobe Flash Player の脆弱性 (APSB19-06) に関する注意喚起 (公開)
2019-02-13　2019 年 2 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)
2019-02-14　runc の権限昇格の脆弱性 (CVE-2019-5736) に関する注意喚起 (公開)
2019-02-22　Adobe Acrobat および Reader の脆弱性 (APSB19-13) に関する注意喚起 (公開)
2019-02-22　ISC BIND 9 に対する複数の脆弱性 (CVE-2018-5744, CVE-2018-5745, CVE-2019-6465) に関する注意喚起 (公開)
2019-02-26　Drupal の脆弱性 (CVE-2019-6340) に関する注意喚起 (公開)

2019-02-26　ISC BIND 9 に対する複数の脆弱性 (CVE-2018-5744, CVE-2018-5745, CVE-2019-6465) に関する注意喚起 (更新)
2019-03-04　Adobe ColdFusion の脆弱性 (APSB19-14) に関する注意喚起 (公開)
2019-03-08　Adobe ColdFusion の脆弱性 (APSB19-14) に関する注意喚起 (更新)
2019-03-13　2019 年 3 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)

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：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 63 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。

2019-01-09　Microsoft 製品における複数の脆弱性 (CVE-2018-8611、CVE-2018-8626) について
2019-01-17　複数の Microsoft 社製品が 2020 年にサポート終了
2019-01-23　NISC が「インターネットの安全・安心ハンドブック Ver.4.00」を公開
2019-01-30　SysmonSearch を用いて不審な挙動を調査
2019-02-06　IPA が「情報セキュリティ 10 大脅威 2019」を発表
2019-02-14　Japan Security Analyst Conference 2019 開催レポートを公開
2019-02-20　総務省および NICT IoT 機器の調査及び利用者への注意喚起を行う「NOTICE」を実施
2019-02-27　フィッシング対策協議会、サイバー犯罪被害防止啓発キャンペーンを開始
2019-03-06　日本スマートフォンセキュリティ協会、「IoT セキュリティチェックシート 第二版」を公開
2019-03-13　2018 年度 中南米 CSIRT 動向調査
2019-03-20　JNSA が「セキュリティ知識分野（SecBoK）人材スキルマップ 2019 年版」を公開
2019-03-27　IPA が「中小企業の情報セキュリティ対策ガイドライン」の第 3 版を公開

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 では、脆弱性やマルウエア、サイバー攻撃などに関する最新情報を、タイムリーにお届けしています。注意喚起とは異なり、発行時点では注意喚起の基準に満たない脆弱性の情報やセキュリティアップデート予告なども含まれます。本四半期に公表した CyberNewsFlash は次のとおりです。

発行件数：8 件　https://www.jpcert.or.jp/newsflash/

2019-01-09　複数の Adobe 製品のアップデートについて
2019-01-23　複数の Adobe 製品のアップデートについて
2019-02-12　Docker 等で使用する runc の権限昇格に関する脆弱性 (CVE-2019-5736) について
2019-02-13　複数の Adobe 製品のアップデートについて
2019-02-15　QNAP 社製 NAS に影響を与えるマルウエアに関する情報について
2019-02-27　OpenSSL の脆弱性 (CVE-2019-1559) について
2019-03-13　複数の Adobe 製品のアップデートについて
2019-03-26　Apache Tomcat の脆弱性 (CVE-2019-0199) 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) runc の権限昇格の脆弱性 (CVE-2019-5736) に関する情報発信

2019 年 2 月 12 日 (米国時間) 、Docker 等で使用されているコンテナランタイム runc に関する脆弱性 (CVE-2019-5736) が公開されました。本脆弱性を悪用して細工されたコンテナをユーザが実行した場合、ホスト上の runc バイナリが意図せず上書きされます。結果として、コンテナが起動しているホスト上で任意のコマンドが root 権限で実行される可能性があります。本脆弱性は 2019 年

2 月 12 日時点で提供されている runc のすべてのバージョンに内在し、また脆弱性の実証コードの公開を 2019 年 2 月 18 日に予定しているとの記載があったことから、JPCERT/CC では、CyberNewsFlash を通じて早期の情報発信を行いました。その後、2019 年 2 月 13 日に本脆弱性に関する実証コードが公開され、JPCERT/CC では、公開された実証コードによる脆弱性の悪用が可能なことを確認したため、注意喚起および早期警戒情報を発行し、広く注意を呼びかけました。

Docker 等で使用する runc の権限昇格に関する脆弱性 (CVE-2019-5736) について
https://www.jpcert.or.jp/newsflash/2019021201.html

runc の権限昇格の脆弱性 (CVE-2019-5736) に関する注意喚起
https://www.jpcert.or.jp/at/2019/at190007.html

(2) QNAP 社製 NAS に影響を与えるマルウエアに関する情報発信

2019 年 2 月 13 日、QNAP 社が、同社製 NAS に関するアドバイザリ (NAS-201902-13) を公開しました。QNAP 社では、同社製 NAS に影響を与えるとされるマルウエアに関する情報を受け取っており、詳細について調査を行っているとのことですが、マルウエアの詳細には言及していません。一方で、QNAP 社のフォーラムサイトや海外の IT 情報サイトには、機器内のファイルが書き換えられるとともにアップデートが阻害される等の現象を一部のユーザが報告しているとの記載がありました。JPCERT/CC では、同社製 NAS が個人用、法人用問わず広く利用されていることから、CyberNewsFlash にて、同社からのアップデート等に関する情報に注目するよう利用者に呼びかけました。

QNAP 社製 NAS に影響を与えるマルウエアに関する情報について
https://www.jpcert.or.jp/newsflash/2019021501.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。

2019 年 3 月末時点で、海外の 21 の経済地域の 27 組織に観測用センサーを設置させていただいています。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、海外の 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

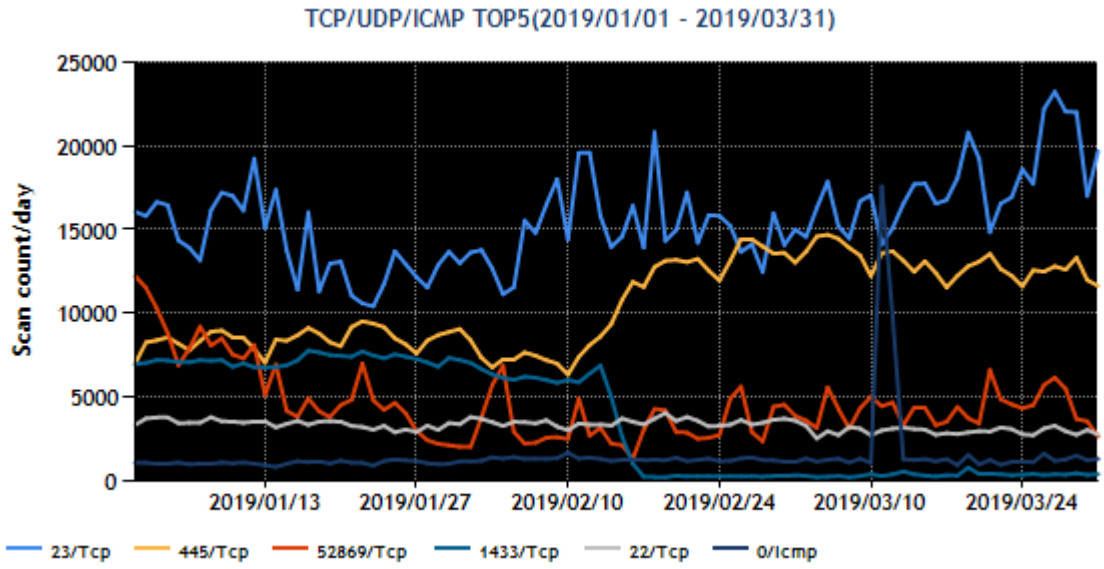
1.3.1. インターネット定点観測システム TSUBAME の観測データの活用

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、2018 年 10 月から 12 月分のレポートを 2019 年 1 月 16 日に公開しました。

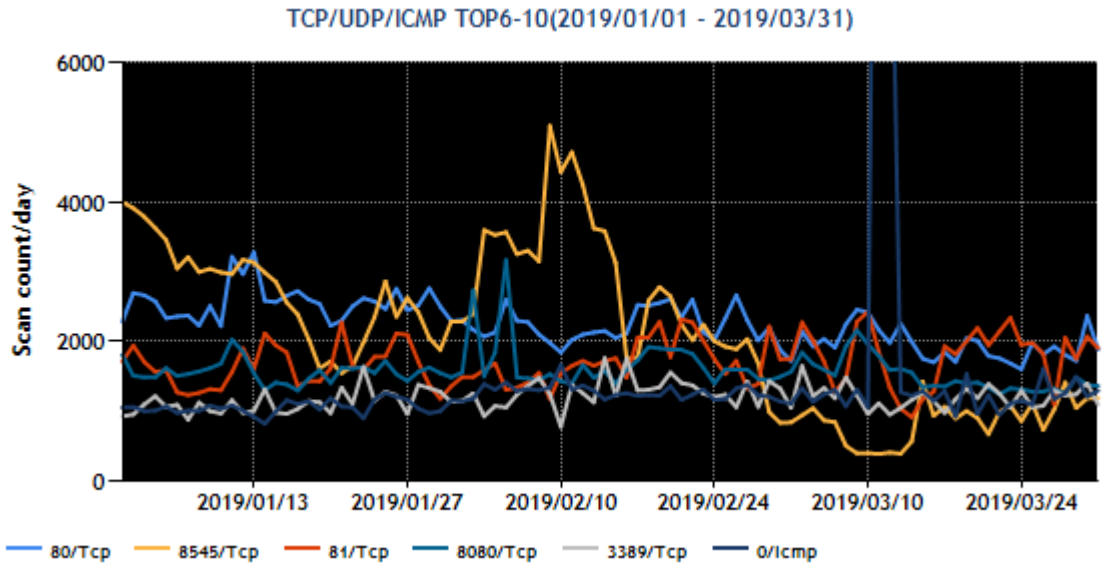
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples
インターネット定点観測レポート（2018 年 10～12 月）
https://www.jpcert.or.jp/tsubame/report/report201810-12.html

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 1-2］と［図 1-3］に示します。

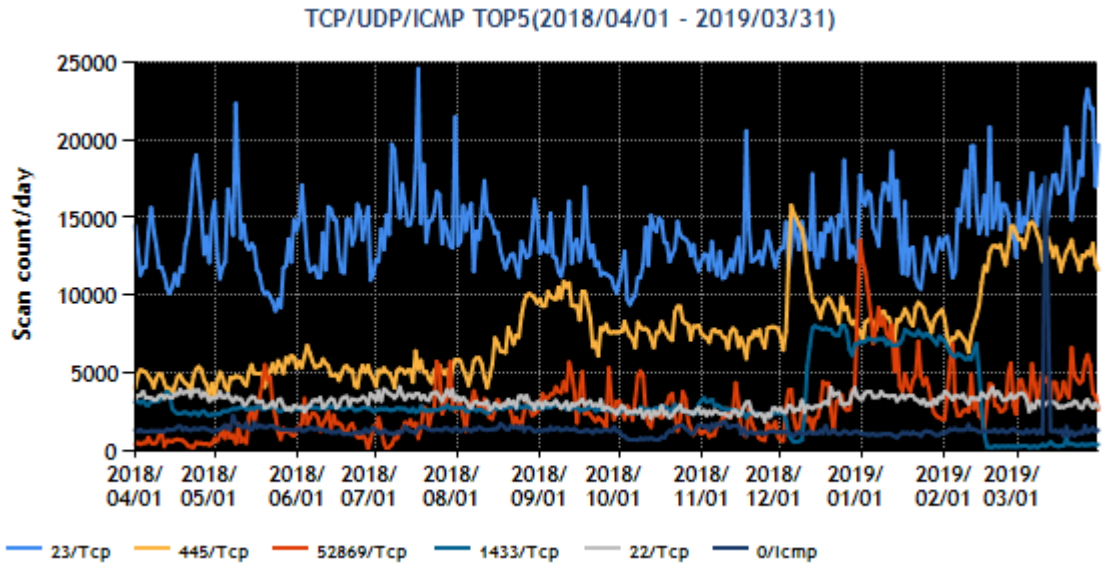


［図 1-2 宛先ポート別グラフ トップ 1-5（2019 年 1 月 1 日-3 月 31 日）］

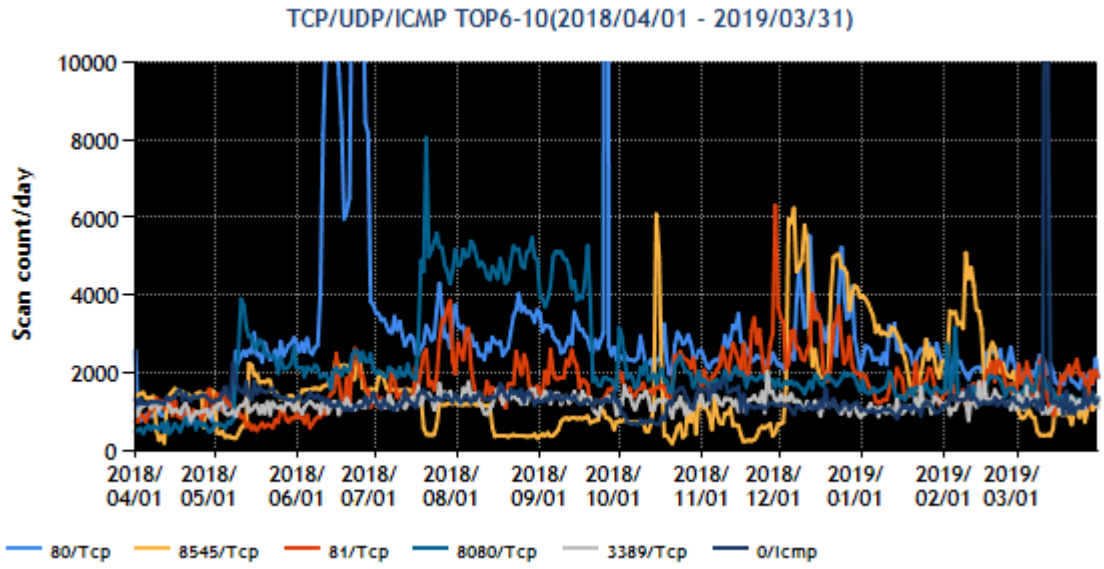


［図 1-3 宛先ポート別グラフ トップ 6-10（2019 年 1 月 1 日-3 月 31 日）］

また、過去 1 年間（2018 年 4 月 1 日-2019 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 1-4］と［図 1-5］に示します。



［図 1-4 宛先ポート別グラフ トップ 1-5（2018 年 4 月 1 日-2019 年 3 月 31 日)］



［図 1-5　宛先ポート別グラフ トップ 6-10（2018 年 4 月 1 日-2019 年 3 月 31 日)］

本四半期も、23/TCP(telnet)宛のパケット数が最も多く、1 月 27 日頃からは徐々に増加しました。送信元を調査したところ、その一部でルータや監視カメラ、レコーダー等の機器が設置されていることが分かりました。これらの機器に関しては、すでに脆弱性情報や攻撃用コードが公開されています。また、攻撃用コードによるものと見られるパケット数の一時的増加も観測されていました。攻撃者がこれらの機器

で脆弱なまま放置されているものを攻撃するパケットを送り付け、その結果、マルウエアに感染した機器が 23/TCP(telnet)宛のパケットを送信し始めたものと考えられます。
次に多かった 445/TCP(microsoft-ds)宛のパケットも本四半期の後半に向けてに増加しました。送信元を調査したところ、一部で Windows OS とみられる環境が確認されています。Windows OS のバージョンは様々でした。古いバージョンを含む Windows OS の既知の脆弱性や弱いパスワードを狙って攻撃するパケットが送り付けられ、その結果として Windows 環境がマルウエアに感染し 445/TCP(microsoft-ds)宛のパケットを送信し始めたものと考えられます。3 番目に多かった 1433/TCP(ms-sql)宛のパケットは 2 月 15 日以降減少しています。

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、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、送信元 IP アドレスの管理者に連絡する等の対応を行っています。本四半期における主な対応事例として、1.1.2 でも言及した 445/TCP(microsoft-ds)宛のパケットを送信するインシデントについて次に述べます。

2019 年 12 月から 445/TCP(microsoft-ds)宛のパケットが観測され、送信元を調べると国内の複数の IP アドレスのいずれかであることを確認しました。本四半期もその現象は増加し、パケット数で増加しています。フィードバックを期待して、それぞれの送信元ホストの IP アドレスの管理者にメールで連絡を行ったところ、複数の管理者から返信がありました。返信内容は様々で、不審な挙動がみられたため仮想サーバを削除しましたという返信もあれば、マルウエアを検出した旨の返信もありました。しかしながら、複数のマルウエアが検出されるケースも多く、パケットを送信しているマルウエアを特定できていません。

JPCERT/CC では、継続して観測したパケットの分析等を行い、必要に応じて管理者への情報提供や、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等の対策に努めています。

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。

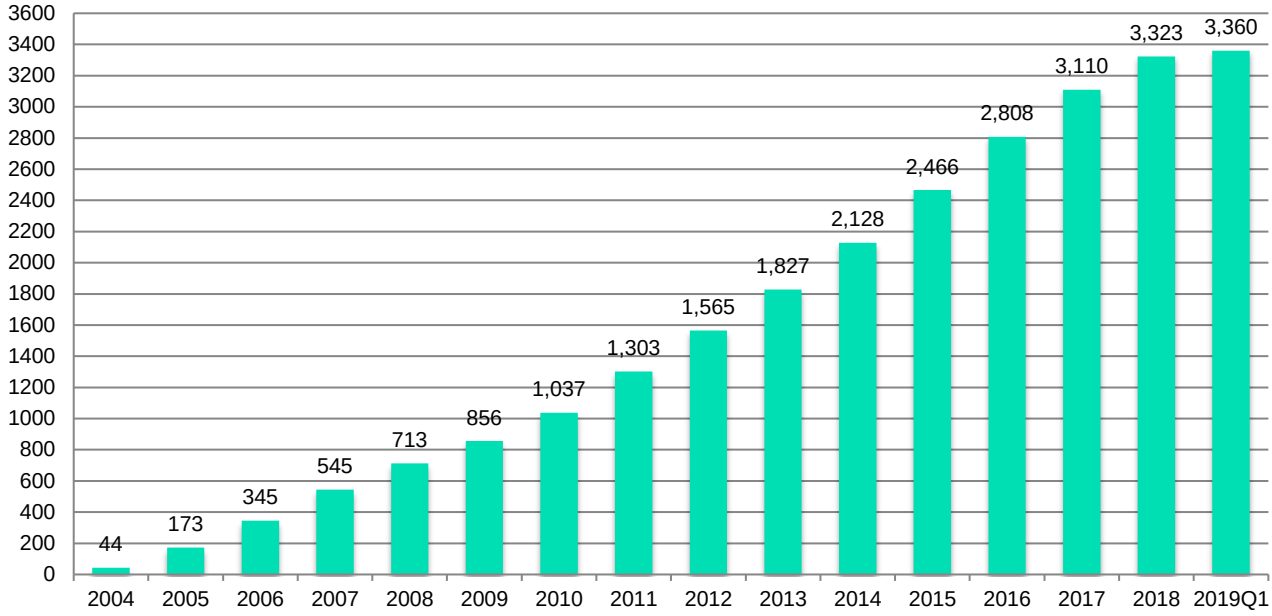
独立行政法人情報処理推進機構（IPA）脆弱性対策
https://www.ipa.go.jp/security/vuln/

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 37 件（累計 3,360 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/



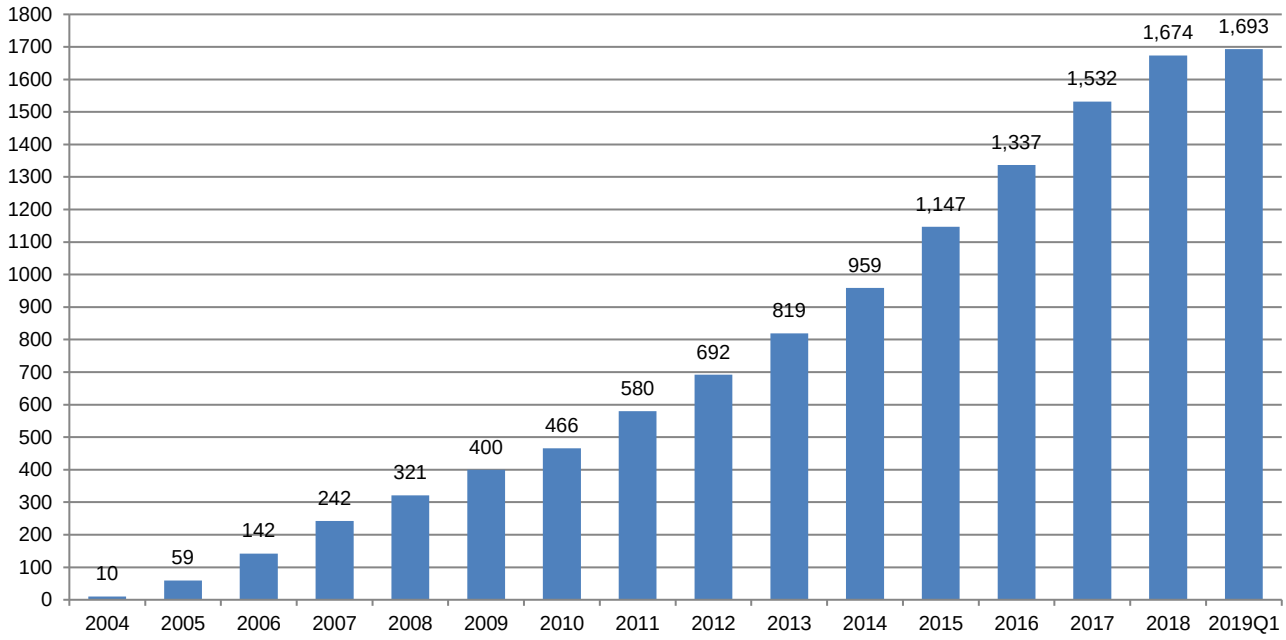
［図 2-1 JVN 公表累積件数］

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 19 件（累計 1,693 件）で、累計の推移は［図 2-2］に示すとおりです。本四半期に公表した 19 件の内訳は、国内の単一の製品開発者の製品に影響を及ぼすものが 10 件、海外の単一の製品開発者の製品に影響を及ぼすものが 8 件、国内の複数の製品開発者の製品に影響を及ぼすものが 1 件ありました。19 件うち 2 件が自社製品の届出によるものでした。自社製品における脆弱性の届出は年々増加しており、毎四半期に一定数の届出があります。

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の内訳は、［表 2-1］のとおりです。本四半期は前四半期同様に、Windows アプリケーションが 4 件と最も多く、2017 年第 2 四半期から継続して多数公表されています。これは、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」と同類の脆弱性をもつ Windows アプリケーションがあると考えた特定の発見者が、2017 年以降多数の Windows アプリケーションで検証を行い、脆弱性が確認されたものを順次届出たことに起因しています。
次いで本四半期の公表で多数を占めた製品カテゴリは、iOS アプリケーション（3 件）とプラグイン（3 件）でした。本四半期に iOS アプリケーションの公表が比較的多いのは、特定の発見者が、iOS アプリケーション作成に使用している特定の共通プラグインの脆弱性を発見し、複数製品に影響を受けるとして届出をしてきたことによるものです。また、プラグインに関しては、複数の発見者により WordPress で使用される複数のプラグインにおける脆弱性が探索されており、順次届け出ている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	4
プラグイン	3
iOS アプリケーション	3
ライブラリ	2
グループウエア	2
マルチプラットフォームアプリケーション	1
制御系製品	1
組込系	1
ウェブアプリケーションフレームワーク	1
CMS	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 18 件（累計 1,667 件）で、累計の推移は［図 2-3］に示すとおりです。

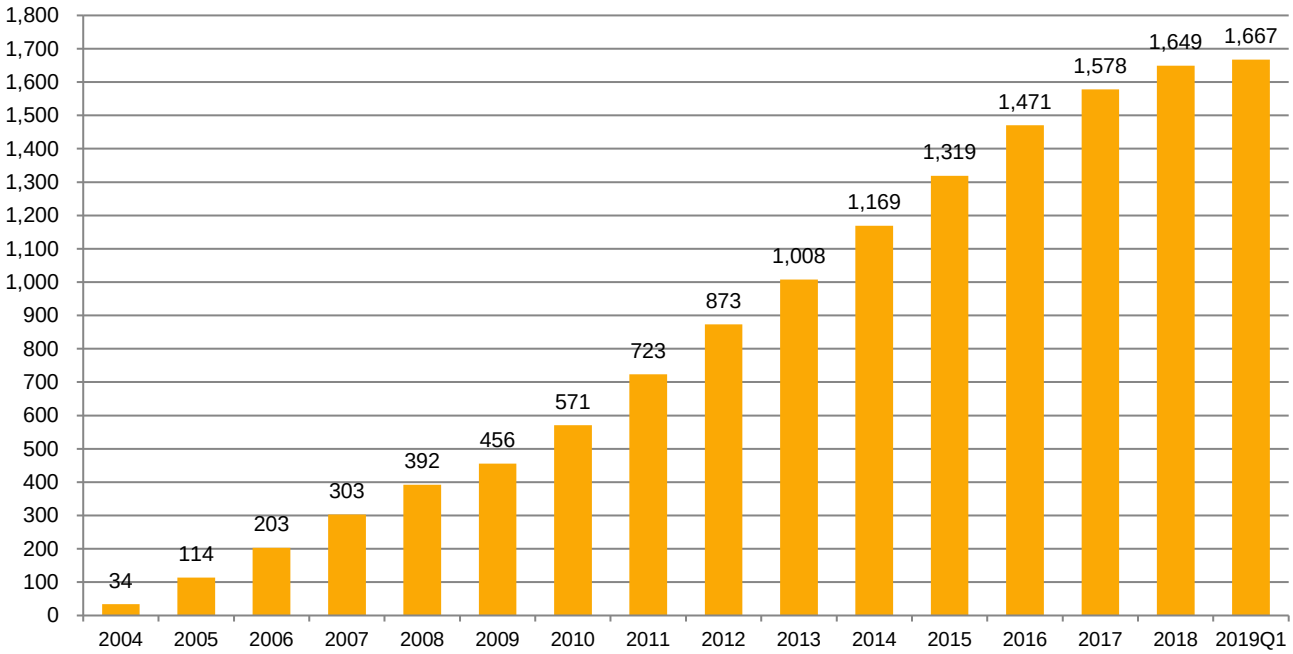
本四半期に公表した脆弱性の影響を受けた製品のカテゴリ内訳は、［表 2-2］のとおりです。本四半期の

公表で多数を占めた製品カテゴリは、マルチプラットフォームアプリケーション（4 件）と組込系（4 件）でした。組込系 4 件のうち 3 件は、製品開発者による自社製品の脆弱性情報を JVN での公表を目的に通知を受けたもので、残り 1 件は、CERT/CC が発行した注意喚起を、JPCERT/CC が翻訳し JVN にて注意喚起を行ったものです。また。4 件のマルチプラットフォームアプリケーションの公表も、製品開発者による自社製品の脆弱性情報を JVN より広くユーザに注意喚起を促すことを目的に届出られたものです。次いで多かったのは、macOS アプリケーションに関する脆弱性が 3 件、制御系製品に関する脆弱性が 3 件でした。制御系製品に関する 3 件の公表の内訳は、米国 ICS-CERT からの国際展開および調整依頼を受け、国内製品開発者との調整を行い公表に至ったものが 2 件、制御系製品を開発する製品開発者が、自社製品に関する脆弱性情報を JVN で広く情報発信することを目的としたものが 1 件でした。

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、製品開発者自身からの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］

製品分類	件数
マルチプラットフォームアプリケーション	4
組込系	4
macOS アプリケーション	3
制御系製品	3
Windows カーネル	1
DNS	1
Windows アプリケーション	1
サーバ製品	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、48 件（製品開発者数で 28 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 203 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。これまでに、公表判定委員会での審議を経て 11 件（製品開発者数で 8 件）を、JVN の「Japan Vulnerability Notes JP（連絡不能）一覧」に掲載しています。

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に、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 NCSC-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 24 件の制御システム用製品の脆弱性情報を公表しています。

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 24 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会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。

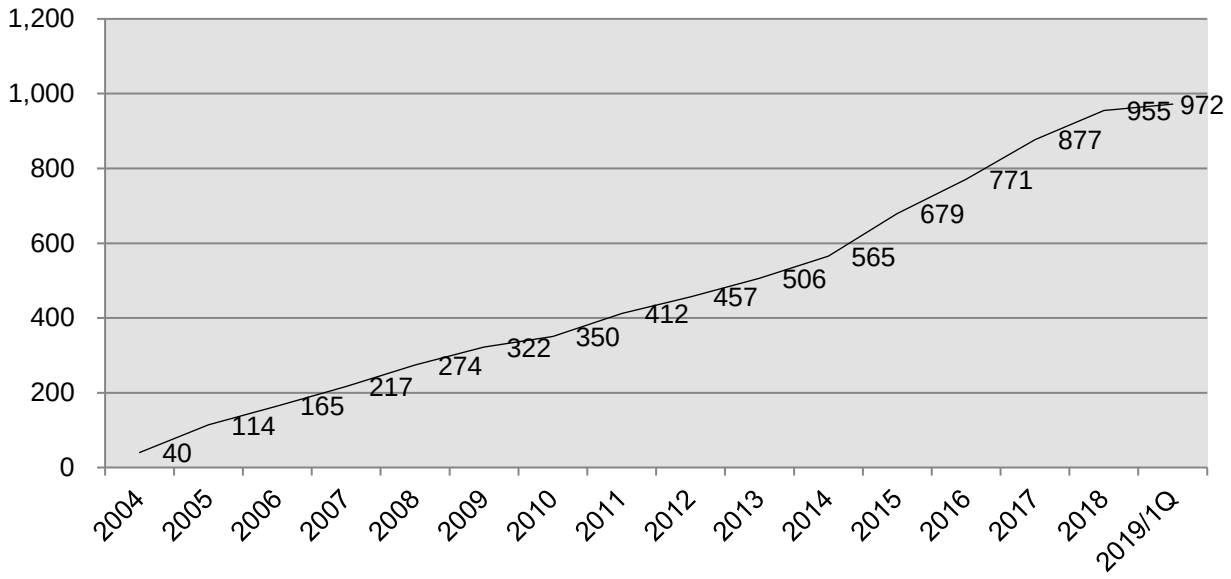
脆弱性情報取扱体制
http://www.meti.go.jp/policy/netsecurity/vulhandlingG.html
脆弱性情報コーディネーション概要
https://www.jpcert.or.jp/vh/

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）
https://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、2019 年 3 月 31 日現在で 972 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
https://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。2019 年 3 月 20 日に開催したミーティングでは、今年度の脆弱性情報取扱制度の運用状況、製品開発者の PSIRT 活動事例、脆弱なコンポーネントやソフトウエア設定の利用実態と改善の取組みなどの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

脆弱性コーディネーショングループでは、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。

講演日時: 2 月 25 日
講演タイトル: Android Secure Coding Workshop
イベント名: Everybody Can Hack #2

インドネシアの情報工学系単科大学である Sekolah Tinggi Teknologi Terpadu Nurul Fikri（STT-NF）の学内 CSIRT 立ち上げイベント Everybody Can Hack #2 において、ゲストスピーカーとして Android アプリのセキュアコーディングワークショップを行いました。本講演は ID-SIRTII/CC の Rudi Lumanto 氏の招待により実現したもので、イベントに参加したインドネシアのアプリ開発者に向けて、Android アプリの

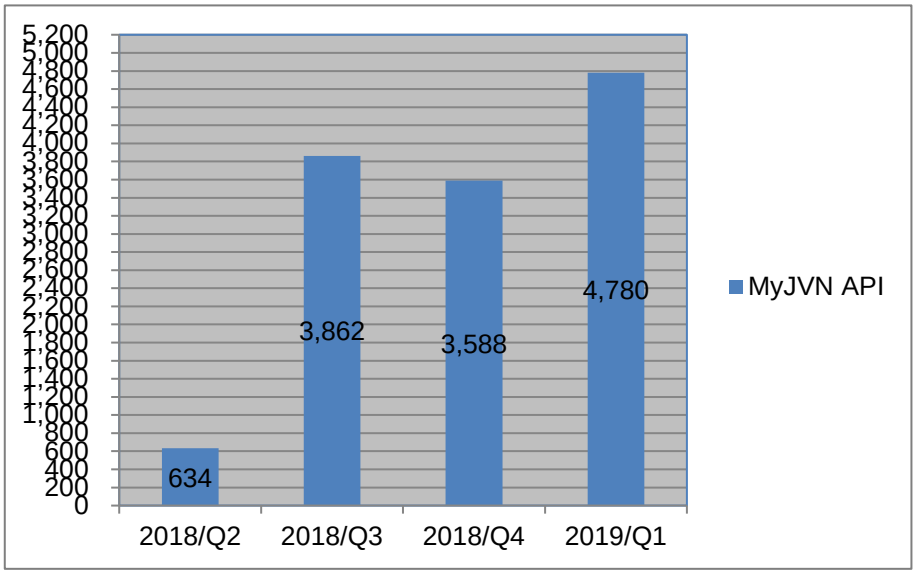
セキュア開発について解説しました。

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、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。

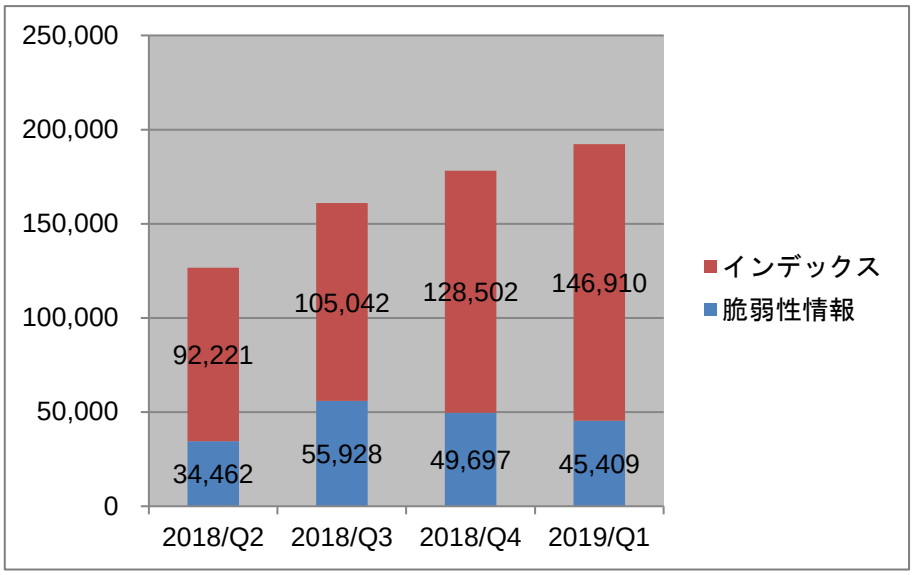
VRDA フィード 脆弱性脅威分析用情報の定型データ配信
https://www.jpcert.or.jp/vrdafeed/index.html

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 2-7］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。



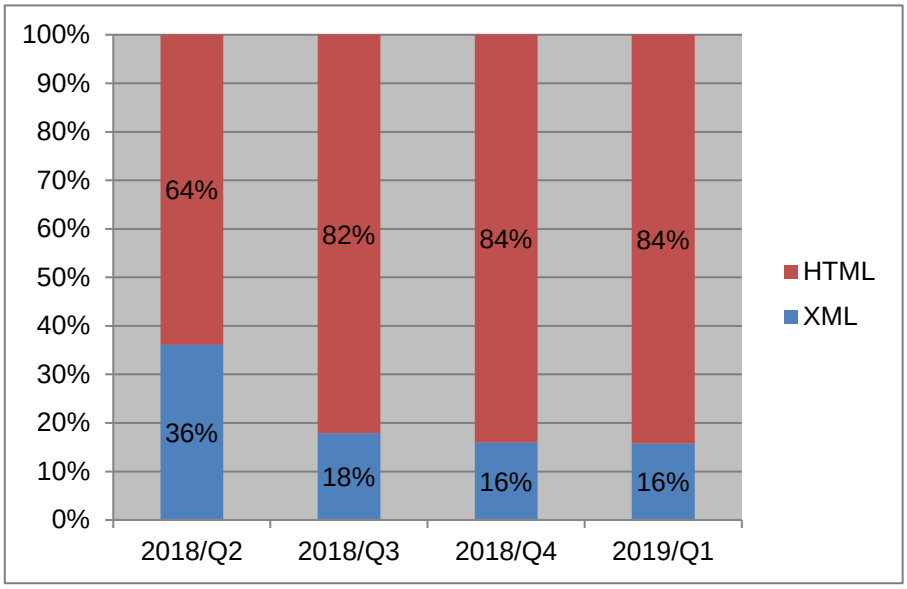
［図 2-6　VRDA フィード配信件数］

VRDA フィード配信件数については、2018 年第 2 四半期の配信件数の少なさが他の四半期と比較して目立ちますが、これは同四半期に VRDA フィード配信用システムの一部改訂作業が実施され、その際にデータ更新が一時的に停止したことが原因です。



［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 14%増加しました。脆弱性情報の利用数については、約 9%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、大きな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 366 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 4 件でした。

2019/02/04 【参考情報】IDenticard 社の PremiSys の複数の脆弱性について
2019/02/06 【参考情報】セキュリティ違反を繰り返した米電力事業者に関する記事のご紹介
2019/02/22 【参考情報】地下鉄車両調達時のサイバーセキュリティ要件強化に関する記事のご紹介
2018/02/25 【参考情報】船舶業界のサイバーセキュリティに関する記事のご紹介

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。

2019/01/11 制御システムセキュリティニュースレター 2018-0012
2019/02/06 制御システムセキュリティニュースレター 2019-0001
2019/03/08 制御システムセキュリティニュースレター 2019-0002

制御システムセキュリティ情報共有コミュニティでは、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 のサービスを設けており、メーリングリストには現在 992 名の方にご登録いただいています。今後も両サービスの充実を図り、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活動として、インシデント報告の受付と、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を行っています。本四半期における活動は次のとおりでした。

(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で公開されている情報を分析し、インターネット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が含まれていないかを調査しています。本四半期に発見したシステムの情報（64IP アドレス）を、それぞれのシステムを保有する国内の組織に対して提供しました。

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 4 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 270 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 制御システムセキュリティアセスメントサービス トライアル開始

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のトライアルを開始しました。
本四半期においては、実施に向けた調整と事前説明を行い、1 組織に対して、サイトアセスメントを実施しました。その他にも実施を希望する組織があり、当該組織との調整によっては、本四半期に事前説明を行い、2019 年度 1Q にアセスメントを実施する予定です。なお、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、制御システム利用者に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 2019 の開催

2019 年 2 月 15 日（金）に浅草橋ヒューリックホールで、300 名を超える方々にご来場いただき、「制御システムセキュリティカンファレンス 2019」［図 3-1］を開催しました。本カンファレンスは 2009 年 2 月から毎年開催しており、今回で 11 回目を迎えました。昨年に続き、講演の一部を公募いたしました。また、プログラムの構成［表 3-1］については、国内外の制御システムにおける脅威の現状を紹介しつつ、船舶分野の取組み、保険の活用、鉄道分野における対策の考察、セキュア機能に関する講演を配置して、各組織での更なるセキュリティ強化に向けた取組みの一助となるような情報提供を行いました。今回のカンファレスでは各講演後の質疑応答が活発に行われ、これまで以上に聴講された方々との交流が盛んに行われました。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 2019
https://www.jpcert.or.jp/event/ics-conference2019.html
制御システムセキュリティカンファレンス 2019 講演資料
https://www.jpcert.or.jp/present/#year2019

［図 3-1 制御システムセキュリティカンファレンス 2019 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)「海事分野におけるサイバーセキュリティ対策に関する取り組み」 東京大学大学院新領域創成科学研究科 准教授 稗方 和夫
(2)「制御システムセキュリティの現在と展望～この 1 年間を振り返って～」 JPCERT/CC 技術顧問 宮地 利雄
(3)「今後の日本におけるサイバー環境の変化に伴い、新たに想定すべき「制御システムにおけるサイバー脅威シナリオ」」 株式会社サイバーディフェンス研究所 専務理事／上級分析官 Nihon Cyber Defence Director 名和 利男
(4)「鉄道分野における制御システムセキュリティ対策の検討」 産業サイバーセキュリティセンター 中核人材育成プログラム受講生 別所 佑樹
(5)「Connected 時代のセキュア機能安全」 株式会社日立製作所 研究開発グループ システムイノベーションセンタ セキュリティ研究部 主任研究員 甲斐 賢
(6)「製造現場に産業用 IoT を導入する際のセキュリティ対策の手始め」 JPCERT/CC 制御システムセキュリティ対策グループ リーダ 河野 一之
(7)「制御システムにおけるサイバーリスクと保険の活用」 東京海上日動火災保険株式会社 企業商品業務部 担当課長 教学 大介

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。

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（1 月 30 日）

JPCERT/CC は、カンボジア、インドネシア、ラオス、ミャンマー、フィリピン、タイ、ベトナムの 7 ヶ国の National CSIRT や関係組織の IT 担当者 14 名を対象に、独立行政法人国際協力機構（JICA）が開催した「ASEAN 地域のサイバー セキュリティ対策強化のための政策能力向上」の実施に協力し、JPCERT/CC の活動や、海外重要インフラ防護や標的型攻撃への取組み、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. JICA サイバー防護演習における講演（2 月 26 日）

JPCERT/CC は、カンボジア、インドネシア、イラン、イラク、ラオス、マレーシア、フィリピン、ジンバブエ、タイ、ベトナム、ミャンマーの 11 ヶ国の National CSIRT や関係組織の IT 担当者 21 名を対象に、独立行政法人国際協力機構（JICA）が開催した「サイバー攻撃防御演習」の実施に協力し、JPCERT/CC が参加する国内および海外 CSIRT コミュニティでの活動や、CSIRT 構築支援の取組み等について講義しました。

4.2. 国際 CSIRT 間連携

国境をまたいで発生する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、APCERT について 2003 年 2 月の発足時から継続して Steering Committee（運営委員会）のメンバーに選出されており、また、その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、APRICOT 2019 の開催にあわせて 2 月 24 日に韓国のデジョンで会議を行い、今後の APCERT の運営方針等について議論しました。JPCERT/CC は Steering Committee メンバ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。

4.2.2. 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。本四半期は、JPCERT/CC が支援したベトナムの VNCERT が FIRST に加盟を果たしました。
FIRST 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. FIRST Regional Symposium Europe

TF-CSIRT は欧州における CSIRT 間連携の要となる団体であり、その会合と併催する形で FIRST Regional Symposium Europe が 2019 年 1 月 21-23 日にエストニアのタリンで開かれ、多数の CSIRT 関係者が参加し、様々な報告と提案を行いました。
NATO の担当者は、NATO のサイバーセキュリティ対応演習について、大規模で広い内容をもち、時間をかけた訓練の様子を印象的に報告しました。また、日本 CSIRT 協議会の担当者は、欧州が提案した CSIRT Maturity Framework を適用して同協議会のメンバーの成熟度を評価した実験について報告しました。

4.3. CyberGreen

国際的なプロジェクトである CyberGreen は、指標を用いて各国／地域インターネット全体の健全性を評価して比較し、各国の CSIRT や ISP、セキュリティベンダーが、関連する指標値を向上させる施策についてグッド・プラクティスを学びあい、目標を明確化することを通じて、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。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、前四半期に続き本四半期においても継続して提案を行いました。

CyberGreen Institute
https://www.cybergreen.net/

4.3.1. インターネットリスク可視化サービス Mejiro

Mejiro は、2018 年 1 月にリリースを行った後もユーザの操作向上や指標の追加などを目的とした機能強化を行っています。本四半期には、次の項目の機能を追加するとともに、画面表示レスポンスの向上とレイアウトの変更を行った新しい版を 2019 年 3 月 18 日にサービスインしました。

・CyberGreen Institute からのデータ取込
・Censys から SMB プロトコルのデータを Mejiro 指標に追加
・SHODAN から CHARGEN プロトコルのデータを Mejiro 指標に追加
・指標時系列グラフ追加対応

実証実験:インターネットリスク可視化サービス―Mejiro―
https://www.jpcert.or.jp/mejiro/
Demonstration Test: Internet Risk Visualization Service -Mejiro-
https://www.jpcert.or.jp/english/mejiro/

4.4. その他国際会議への参加

4.4.1. IHAP (Incident Handling Automation Project)

インシデントハンドリングの自動化について検討する会合 IHAP が 2019 年 1 月 24,25 日にエストニアのタリンで開かれ、これに参加しました。
各国がそれぞれの取組みの状況を報告し、JPCERT/CC も、Shodan の詳細データのうち日本に関係する部分をデータベース化する取組みや、このデータベースから時系列データを取り出し、統計手法によって異常値を検出した時に警報を発する仕組みについて報告しました。

インシデントハンドリングの自動化やその周辺の取組みについて自由に議論するハッカソンである IHAP が 2019 年 1 月 24,25 日にエストニアのタリンで開かれ、これに参加しました。
各参加者がそれぞれの取組みの状況を報告し、JPCERT/CC も Shodan の詳細データのうち日本に関係する部分をデータベース化して時系列上の変化検出を行い自動的に通報する仕組みを作ろうとする取組みについて報告しました。

4.4.2. The Global Commission on the Stability of Cyberspace（GCSC）への参加

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 2017 年 3 月に立ち上がりました。その中に技術、法律、インターネットガバナンスなどの分野ごとにオープンな議論を行うことを目的とする 4 つのワーキンググループが設けられています。技術ワーキンググループではメーリングリストでの議論や調査の仕様作成などを行っており、JPCERT/CC の小宮山が副議長としてこれに関与しています。
本四半期は 2019 年 3 月 9-10 日に神戸で開催された GCSC の委員会に参加するとともに、メーリングリストでの議論などに参加しました。

Global Commission Introduces Six Critical Norms Towards Cyber Stability
https://cyberstability.org/news/global-commission-introduces-six-critical-norms-towards-cyber-stability/

4.4.3. 海外 CSIRT 等の来訪および往訪

4.4.3.1. オーストラリア AusCERT 往訪（2 月 20 日）

オーストラリアの AusCERT（オーストラリアコンピュータ緊急対応チーム）を訪問し、活動の状況についてヒアリングを行うとともに、今後の協力について意見交換を行いました。

4.4.3.2. オーストラリア ACSC 往訪（2 月 20 日）

オーストラリアの ACSC（オーストラリアサイバーセキュリティセンター）を訪問し、活動の状況についてヒアリングを行うとともに、今後の協力について意見交換を行いました。

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。
脆弱性関連のうち、脆弱性の取扱手順（ISO/IEC 30111）については 10 月 31 日から 2019 年 1 月 23 日まで国際標準草案(DIS；Draft of international standard)が国際投票に付されました。SC27 事務局の開票報告によれば、国際標準として発行するに十分な賛成票がありましたが、日英米の 3 国がコメントを付して投票しており、2019 年 4 月に予定されている次の SC27 国際会議で取扱いが審議されることになっています。

4.6. 中南米 CSIRT 動向調査

国境に関係なく発生する国際的なサイバー攻撃事案の調整・解決にあたっては、国の窓口となる CSIRT 間での情報共有や協力が不可欠となっており、JPCERT/CC では国際的な CSIRT のコミュニティである FIRST や APCERT 等への参加や、海外各国の CSIRT との連携強化を通じて、国をまたいだ協力が必要な事案へスムーズに対応できる体制を構築しています。これまで、インシデント事案に伴う情報共有は時々あったものの、中南米地域では個別に MOU を結んでいる CSIRT もなく、直接来訪・往訪して意見交換をする機会もほとんどありませんでした。また、サイバーセキュリティに関わる体制等について日本語で体系的にまとめられた文書が少なく、実態についての理解があまり進んでいませんでした。そこで、中南米地域の CSIRT 間の連携や、個別の CSIRT の取り組みについて理解を深めるための調査プロジェクト「中南米 CSIRT 動向調査」をアビームコンサルティング株式会社の協力のもと実施し、この調査の結果についてまとめた報告書を 3 月 7 日に公表しました。特にメキシコとブラジルに焦点を当て、National CSIRT の活動やサイバーセキュリティ関連の法整備の状況、また各国が直面するサイバー脅威の概要、また中南米地域での CSIRT 間連携の仕組み等についてまとめています。

2018 年度中南米 CSIRT 動向調査
https://www.jpcert.or.jp/research/LACSIRT-survey.html

5. 日本シーサート協議会（NCA）事務局運営

5.1. 概況

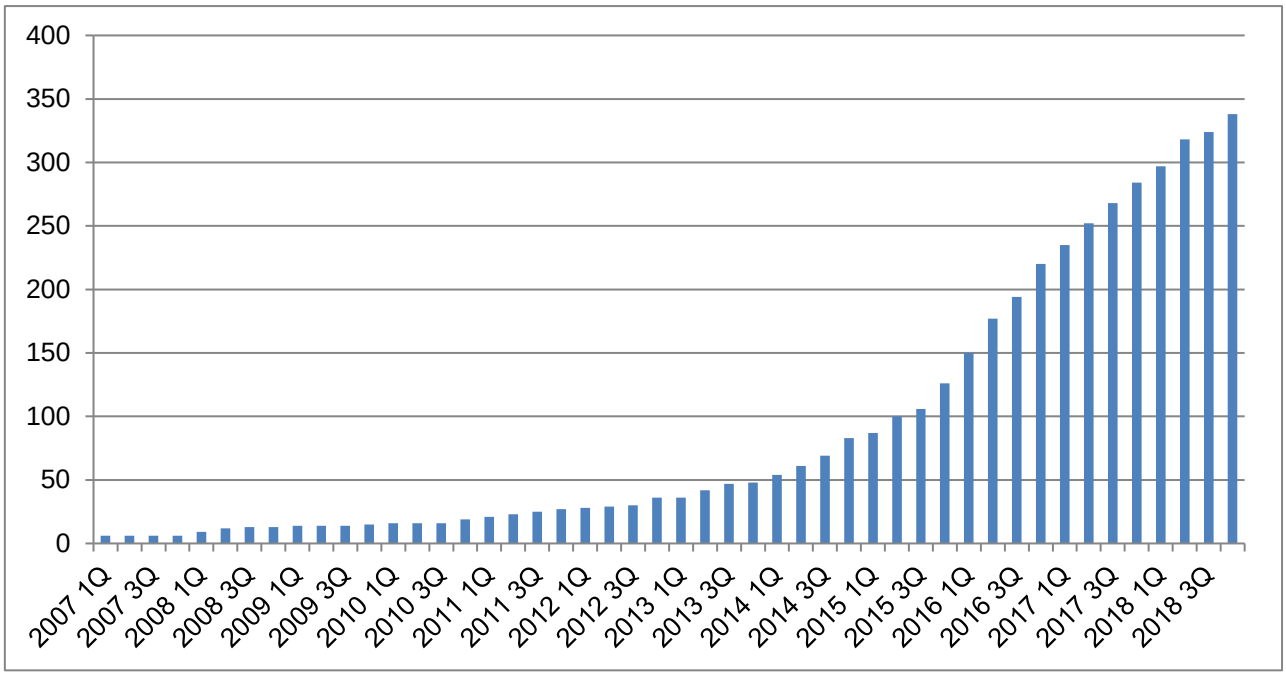
日本シーサート協議会（NCA：Nippon CSIRT Association；本節の以下において「協議会」）は、国内のシーサート（CSIRT：Computer Security Incident Response Team）組織が互いに協調し、連携して共通の問題を解決する場として 2007 年に設立されました。その事務局として、JPCERT/CC は、NCA の Web サイトの管理や更新を通じた広報活動、協議会の問合せ窓口やメーリングリストを含む会員情報の管理、加盟のためのガイダンスの実施および手続きの運用を担当するとともに、自らも会員として協議会の活動に参加しています。

本四半期には、次の 14 組織（括弧内はシーサート名称）が新規に NCA の一般会員となりました。

国立大学法人　大阪大学 (OU-CSIRT)
日本レコード・キーピング・ネットワーク株式会社 (NRK-CSIRT)
日本無線株式会社 (JRC-CSIRT)
TOTO 株式会社 (TOTO-CSIRT)
株式会社ジュピターテレコム (JCOM-CSIRT)
株式会社三菱ケミカルホールディングス (MCHC-CSIRT)
大阪ガス株式会社 (Daigas Group-CSIRT)
国立大学法人静岡大学 (SU-CSIRT)
不二製油グループ本社株式会社 (FUJIOIL-CSIRT)
コインチェック株式会社 (CC-CSIRT)
株式会社 USEN-NEXT HOLDINGS (Usirt)
株式会社カプコン (CAPCOM-CSIRT)
メタウォーター株式会社 (WBCSIRT)
株式会社村田製作所 (muRata CSIRT)

本四半期末時点で※338（一般会員 336、協力会員 2）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。

※集計は協議会 Web の掲載時期をもとに実施。実際の加盟承認時期と若干のタイムラグが生じる場合があります。



［図 5-1　日本シーサート協議会 加盟組織数の推移］

5.2.　第 15 回臨時総会&第 24 回シーサートワーキンググループ会

第 15 回総会 とそれに続けて第 24 回シーサートワーキンググループ会が次のとおり開催されました。JPCERT/CC は事務局としてこの開催のための各種サポートを行いました。

日時：2019 年 3 月 25 日（月)
場所：大崎ブライトコアホール

総会では、運営委員会から一般社団法人化に向けての今後の運営体制に関して説明と、地区活動委員会、チームトレーニング委員会、そして各タスクフォースからの活動についての報告がありました。
また、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。この日の会合では、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が行われました。

5.3.　日本シーサート協議会　運営委員会

本四半期は、次のとおり計 3 回の運営委員会と 1 回の臨時運営委員会を開催しました。

第 140 回運営委員会

開催日時：2019 年 1 月 23 日（水）16:00 - 18:00

開催場所：NTT Com-SIRT

臨時運営委員会

開催日時：2019 年 2 月 6 日（水）16:00 - 18:00

開催場所：JPCERT/CC

第 141 回運営委員会

開催日時：2019 年 2 月 20 日（水）16:00 - 18:00

開催場所：MBSD-SIRT

第 142 回運営委員会

開催日時：2019 年 3 月 20 日（水）16:00 - 18:00

開催場所：HIRT

5.4. 日本シーサート協議会　コンテンツの海外展開支援

NCA の人材ワーキンググループでは、日本国内での CSIRT の普及を目的として「CSIRT 人材の定義と確保」を作成し、以下の Web ページに公開しています。

CSIRT 人材の定義と確保 Ver.1.5
https://www.nca.gr.jp/activity/imgs/recruit-hr20170313.pdf

本文書は、日本国内にある組織内 CSIRT において、CSIRT の役割や必要な人材を定義すること等に活用されてきましたが、今般、この文書を日本企業の海外支部や子会社でも活用できるようにすべく、JPCERT/CC は本文書の英語翻訳を担当しました。NCA 内でのレビューを経て、3 月 29 日に以下の Web ページに公開されました。

NCA Publications / Definition of Roles Required for CSIRT (Ver.1.5) / English Version
https://www.nca.gr.jp/en/activity/index.html

日本シーサート協議会の活動の詳細については、次の Web ページをご参照ください。

日本シーサート協議会
http://www.nca.gr.jp/

6. フィッシング対策協議会事務局の運営

JPCERT/CC は、フィッシング対策協議会（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。また、協議会は報告を受けたフィッシングサイトについて JPCERT/CC に報告しており、これを受けて JPCERT/CC が、サイトを停止するための調整をインシデント対応支援活動の一環として行っています。

6.1. 情報収集 / 発信の実績

6.1.1. フィッシングの動向等に関する情報発信

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計 14 件（ニュース：5 件、緊急情報：9 件）発信しました。
本四半期は前四半期と同様に、Amazon と Apple をかたるフィッシングの報告が多く、特に Amazon をかたるフィッシングメールは何度も大量配信が行われました。その他、クレジットカード会社や金融機関をかたるフィッシングについても多数報告がありました。

利用者数が多く、影響範囲も大きい報告については、緊急情報を Web サイトに適宜掲載し、広く注意を喚起しました。その件数と内訳は次のとおりです。

Amazon をかたるフィッシング：3 件
PayPal をかたるフィッシング：1 件
ゆうちょ銀行をかたるフィッシング：1 件
VJA (Vpass) をかたるフィッシング：1 件
三井住友カードをかたるフィッシング：1 件
三井住友銀行をかたるフィッシング：1 件
LINE をかたるフィッシング：1 件

本四半期の特筆すべきフィッシング事案として、Amazon をかたるフィッシングがありました（[図 6-1] 参照）。何度も大量配信が行われたことから、Web ページに緊急情報を 3 回掲載するとともに、フィッシングメールが経由する設備を管理している事業者に対しても、状況の調査や問題解決のための対応を依頼しました。
また、LINE をかたるフィッシングでは、フィッシングサイトが短時間で停止と稼働を繰り返している状況が確認されました。JPCERT/CC やセキュリティベンダ等の対策組織が、フィッシングの報告を確認したタイミングでフィッシングサイトが稼働していない場合、当該サイトの閉鎖調整やフィルタリングが

難しくなります。同一のフィッシングサイトが長期に渡って残りつづける可能性があるため、注意が必要です。

［図 6-1　Amazon をかたるフィッシングメールとフィッシングサイト ］

https://www.antiphishing.jp/news/alert/_amazon_20190304.html

6.1.2. 定期報告

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/
2019 年 1 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201901.html
2019 年 2 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201902.html
2019 年 3 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201903.html

6.1.3. フィッシングサイト URL 情報の提供

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やフィッシングに関する研究を行っている学術機関等に該当する協議会の会員に対し、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。これは、フィッシング対策製品の強化や、関連研究の促進を目的としたものです。本四半期末の時点で 40 組織に対し URL 情報を提供しており、今後も要望に応じて提供を拡充する予定です。

6.1.4. フィッシング対策ガイドライン等改訂に向けた会合

協議会の「技術・制度検討ワーキンググループ」の会合を開催し、「フィッシング対策ガイドライン」（事業者と一般消費者向け）および「フィッシングレポート」の 2019 年 6 月の公開を目指して改訂を進めました。

技術・制度検討ワーキンググループ会合
日時：2019 年 1 月 30 日 15:00 - 17:00
場所：JPCERT/CC

技術・制度検討ワーキンググループ会合
日時：2019 年 3 月 13 日 14:00 - 17:00
場所：山王パークタワー

7. フィッシング対策協議会の会員組織向け活動

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独自の活動を、運営委員会の決定に基づいて行っています。ここでは本四半期における会員組織向けの活動の一部について記載します。

7.1. 運営委員会開催

本四半期においては、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。

第 67 回運営委員会
日時：2019 年 2 月 15 日 15:00-17:30、2 月 16 日 9:00-12:00
場所：レクトーレ熱海桃山

第 68 回運営委員会
日時：2019 年 3 月 15 日 16:00-18:00
場所：JPCERT/CC

7.2. ワーキンググループ会合等 開催支援

本四半期においては、次のとおり開催された協議会のワーキンググループ等の会合の開催の支援と参加を行いました。

学術研究プロジェクト会合
日時：2019 年 2 月 8 日 10:00 - 12:00
場所：ソースネクスト

証明書普及促進ワーキンググループ会合
日時：2019 年 3 月 27 日 16:00 - 18:00
場所：JPCERT/CC

認証方法調査・推進ワーキンググループ会合
日時：2019 年 3 月 29 日 15:00 - 17:00
場所：アルプス電気本社ビル

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。

ソフトウェア等の脆弱性関連情報に関する届出状況 [2018 年第 4 四半期 (10 月～12 月)]（2019 年 1 月 24 日）
https://www.jpcert.or.jp/press/2018/vulnREPORT_2018q4.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[2018 年 10～12 月]（2019 年 1 月 16 日）
https://www.jpcert.or.jp/tsubame/report/report201810-12.html
https://www.jpcert.or.jp/tsubame/report/TSUBAMEReport2018Q3.pdf

8.3. JPCERT/CC Eyes～JPCERT コーディネーションセンター公式ブログ～

JPCERT コーディネーションセンター公式ブログ 「JPCERT/CC Eyes」は、JPCERT/CC が分析・調査した内容、TSUBAME（インターネット定点観測システム）で観測された動向や国内外のイベントやカンファレンスの様子などをいち早くお届けする情報提供サービスです。
JPCERT/CC Web ページにおいて公開していた「分析センターだより」、「インシデントレスポンスだより」、「コラム」の各コンテンツも「JPCERT/CC Eyes」に集約しました。
本四半期においては次の 9 件の記事を公開しました。

日本語版発行件数：5 件　https://blogs.jpcert.or.jp/ja/

2019-01-21	SysmonSearch を用いて不審な挙動を調査
2019-01-31	Japan Security Analyst Conference 2019 開催レポート～前編～
2019-02-07	Japan Security Analyst Conference 2019 開催レポート～後編～
2019-02-14	世界の CSIRT から ～ベトナム(VNCERT, AIS)～
2019-02-19	攻撃グループ Tick による日本の組織をターゲットにした攻撃活動

英語版発行件数：4 件 https://blogs.jpcert.or.jp/en/

2019-01-07	Supporting CSIRT Activities for Africa (in Tunisia)
2019-02-08	Investigate Suspicious Account Behaviour Using SysmonSearch
2019-02-13	Japan Security Analyst Conference 2019 -Part 1-
2019-02-18	Japan Security Analyst Conference 2019 -Part 2-

9. 主な講演活動

(1) 洞田 慎一（早期警戒グループ マネージャー）：
「KIIS セキュリティ人材育成プログラム CSIRT 構築・運営」
平成 30 年 KIIS サイバーセキュリティ研究会/人材育成プログラム，2019 年 1 月 11 日

(2) 宮地 利雄(技術顧問)：
「製造業・重要インフラのサイバーセキュリティの脅威と対策の近況」
ARC プロセス・ユーザ・グループ SIG, 2019 年 1 月 24 日

(3) 河野 一之（制御システムセキュリティグループ）：
「JPCERT／CC の制御システムセキュリティに関する支援活動とサービス紹介」
ARC プロセス・ユーザ・グループ SIG, 2019 年 1 月 24 日

(4) 洞田 慎一（早期警戒グループ マネージャー）：
「Mejiro 指標と DDoS 攻撃」
大学共同利用機関法人等におけるセキュリティーワークショップ，2019 年 2 月 7 日

(5) 佐々木 勇人（早期警戒グループ）：
「Web サイトを狙うサイバー攻撃の脅威　～情報漏洩だけじゃない、最近の攻撃動向～」
イーコマースフェア 2019　EC サイト対策セミナー, 2019 年 2 月 8 日

(6) 米澤 詩歩乃（早期警戒グループ）：
「最新のインシデント事例、不審メール対策について」
自治体 CSIRT 協議会　技術講習会, 2019 年 2 月 8 日

(7) 内田 有香子（国際）：
「JPCERT/CC Activities」
JICA プロジェクト「サイバー攻撃防御演習」, 2019 年 2 月 26 日

(8) 小宮山 功一朗（国際）：
「The Internet under threat」
IGF2018 報告会, 2019 年 2 月 27 日

(9) 真鍋 敬士（理事・最高技術責任者）：
「情報漏えいを取り巻く最新のサイバーセキュリティ動向」
認定個人情報保護団体シンポジウム, 2019 年 3 月 6 日

(10) 河野 一之（制御システムセキュリティグループ）：
「製造現場に産業用 IoT を導入する際のセキュリティ対策の第一歩　企業が工場でセキュアに産業用 IoT を活用するために」
Security Days Spring 2019 -Tokyo-, 2019 年 3 月 7 日

(11) 河野 一之（制御システムセキュリティグループ）：
「産業用 IoT 導入時のセキュリティ対策」
新時代のものづくり研究会, 2019 年 3 月 14 日

(12) 河野 一之（制御システムセキュリティグループ）：
「製造現場に産業用 IoT を導入する際のセキュリティ対策の第一歩　企業が工場でセキュアに産業用 IoT を活用するために」
JUAS 会員向けミニセミナー,2019 年 3 月 20 日

(13) 奥石 隆（早期警戒グループ）：
「サイバーセキュリティの観点から見る IoT-『IoT セキュリティチェックリスト』のご紹介
JUAS 会員向けミニセミナー, 2019 年 3 月 20 日

(14) 洞田 慎一（早期警戒グループ マネージャー）：
「脅威から身を守るために～高等教育・研究機関にて注意したいサイバーセキュリティ～」
公益財団法人高輝度光科学研究センター (JASRI), 2019 年 3 月 28 日

10. 主な執筆活動

(1) 森崎 樹弥（早期警戒グループ）：
「2018 年の情報セキュリティ動向」
株式会社インプレス R&D インターネット白書 2019,2019 年 1 月 31 日

(2) 洞田 慎一（早期警戒グループ マネージャー）：
「放送が狙われている！～サイバー攻撃に立ち向かうために～放送に対するサイバー攻撃を考える」
兼六館出版株式会社　放送技術 3 月号,2019 年 3 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) 第三回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
開催日：2019年2月21日

(2) Security Days Spring 2019
主　催：株式会社ナノ・オプトメディア
開催日：2019年2月22日～3月8日

(3) セキュリティフォーラム2019
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
一般社団法人セキュアIoTプラットフォーム協議会
開催日：2019年3月14日

(4) 第14回IPAひろげよう情報モラル・セキュリティコンクール2018
主　催：IPA 独立行政法人 情報処理推進機構
開催日：2018年6月1日～2019年3月31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　：secure-coding@jpcert.or.jp
■公開資料、講演依頼、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