JPCERT/CC 活動四半期レポート

2020 年 10 月 1 日 ～ 2020 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

2021 年 1 月 21 日

活動四半期レポートトピックス

ートピック 1ー リモートワーク環境下で利用が進む VPN 製品の脆弱性への取り組み

2020 年 4 月以降、新型コロナウイルス感染症（COVID-19）対策の一環として VPN システムの利用場面が増え、その重要性が高まっています。その一方で、2019 年から 2020 年にかけて SSL-VPN 機能を持つ複数の製品において、すでに公表された脆弱性が修正されないまま運用されている機器が少なからず存在し、それらを狙った攻撃で実際に被害が発生しています。こうした状況の中で、JPCERT/CC では脆弱性情報の公表や注意喚起後、あらためて各機器の管理者へ個別の通知を進めるなど追加の取り組みを進めています。

そうした事例の一つとして本四半期には Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性に関する対応を行いました。この脆弱性は 2019 年 5 月に公表されたもので、JPCERT/CC からも 2019 年 9 月に注意喚起を行いましたが、1 年以上経った本四半期になっても、対策がとられず脆弱性をもったままの多数のシステムが稼働しています。2020 年 11 月にそうしたシステムのリストがフォーラムなどで公開されました。攻撃者が脆弱性を悪用可能であることを確認した上で作成したものとみられ、ホストの IP アドレスに加え、SSL VPN 接続を利用するユーザーアカウント名や平文のパスワードなどの情報が含まれていました。JPCERT/CC では、こうした状況に関して CyberNewsFlash で広く注意を呼びかけるとともに、公開された情報に含まれていた国内の対象組織へ直接または ISP やベンダーなどの関係組織を通じて情報を提供し早期の対処をお願いしました。

新型コロナウイルス感染症（COVID-19）流行という環境下において、リモートワーク中心の業務形態はさらに広がり、VPN システムをはじめとしたインターネット経由で接続するシステムの増加が考えられます。こうした状況を突いた攻撃に対する対策を強化するため、今後、JPCERT/CC では、すでに公表済み、注意喚起済みの情報についても、関連する攻撃動向などとあわせて、各四半期末にあらためて注意が必要なものについて取りまとめ、お知らせを公開していく予定です。

CyberNewsFlash「Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性 (CVE-2018-13379) の影響を受けるホストに関する情報の公開について」
https://www.jpcert.or.jp/newsflash/2020112701.html

CyberNewsFlash「2020 年 9 月から 12 月を振り返って」
https://www.jpcert.or.jp/newsflash/2020122301.html

ートピック 2ー 脆弱性情報のグローバルな流通基盤体制整備のための JPCERT/CC の活動と国内における新 CNA の誕生

脆弱性情報の識別に欠かせない CVE (Common Vulnerabilities and Exposures)識別子を付与する機関が CNA (CVE Numbering Authority)です。制度の発足当初は米国の MITRE 社が唯一の CNA でしたが、流通する脆弱性情報の増加に対応できるよう現在では複数の CNA が認定され、分散的に CVE の採番を行う体制に移行しています。CNA のうち、他の CNA の管轄や必要な調整の役割を担っている機関は「Root CNA」と呼ばれ、現在は MITRE 社と JPCERT/CC、米国政府の CISA の 3 つの機関がその任に当たっています。

JPCERT/CC は、複数 CNA 体制となった直後から CNA としての活動を開始し、さらに、Root CNA が設置されることなった 2018 年からは、CNA の枠組みの整備と推進に MITRE 社と協力しながら努めてきました。日本国内でも複数の CNA による分散的な CVE 採番の体制を目指そうと、新たに CNA になる組織のための研修資料の邦訳にも協力しています。

こうした活動が実を結び、2020 年 12 月 4 日に LINE 株式会社と三菱電機株式会社が、JPCERT/CC を Root CNA とする初の CNA として登録されました。

JPCERT/CC Eyes「CNA 活動レポート ～日本の 2 組織が新たに CNA に参加～」
https://blogs.jpcert.or.jp/ja/2020/12/cna-2cna.html

現在グローバルには 152 組織が CNA として登録されており、さらに多くの日本の組織が CNA として登録されることが期待されています。JPCERT/CC では、脆弱性情報の一層の迅速かつ効果的な流通をめざすとともに、国内外の CNA との連携協力や体制の整備に努めてまいります。

目次

本活動は、経済産業省より委託を受け、「令和２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、「6.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」、「8.主な講演活動」、「9.主な執筆」、「10.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ー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 13,066 件、インシデント件数ベースでは 7,429 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 4,220 件でした。前四半期の 4,807 件と比較して 6%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ェ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_Report20210121.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 5,015 件で、前四半期の 5,845 件から 14%減少しました。また、前年度同期（3,700 件）との比較では、36%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	931	777	927	2,635(53%)
国外ブランド	697	385	547	1,629(32%)
ブランド不明 (注 5)	274	223	254	751(15%)
全ブランド合計	1,902	1,385	1,728	5,015

（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。

国外ブランドは特定の通販サイトを装ったフィッシングサイトが多い状況は前四半期と同じですが、国内ブランドは金融機関のサイトを装ったフィッシングサイトが急増しています。

また、本四半期には新型コロナウイルス感染症対策における特別定額給付金の給付を騙ったフィッシングサイトの報告が多数寄せられました。これは特別給付金に関する特別サイトが開設されたという内容のメールでフィッシングサイトへ誘導し、個人情報やクレジットカード情報を入力させるだけではなく、運転免許証やパスポートなどの本人確認書類のコピーをアップロードさせようとするものでした。

このフィッシングサイトの URL には総務省の Web サイトに似せた kyufukin.soumu.go.jp や soumu-go-jp などの文字列が使われ、一見しただけでは偽物かどうかの判断に迷うようなものが多く見受けられました。

［図 1-1：特別定額給付金の給付を騙ったフィッシングサイト］

フィッシングサイトの調整先の割合は、国内が 23%、国外が 77%であり、前四半期（国内が 29%、国外が 71%）と比べて国外への調整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、404 件でした。前四半期の 374 件から 8%増加しています。

本四半期は、改ざんされた Web サイトから、特定ブランドを扱う E コマースサイトに誘導される事例が複数寄せられました。改ざんされた Web サイトには不正な JavaScript ファイルが設置されており、［図 1-2］のようなスクリプトタグでブラウザーに読み込まれるようになっていました。

```
<html>
<script type="text/javascript" src="promk.js"></script>
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8" />
<title>[redacted]</title>
<meta name="keywords" content="[redacted]" />
<meta name="description" content="[redacted]
<meta name="viewport" content="width=device-width, user-scalable=yes, initial-scale=1, minimum-scale=1, maximum-scale=3">
<meta property="og:title" content="[redacted]
<meta property="og:type" content="website">
<meta property="og:url" content="#">
<meta property="og:image" content="[redacted]" />
<meta property="og:description" content="[redacted]
<meta property="fb:app_id" content="[redacted]">
<base href="[redacted]" />
<script type="text/javascript" src="http://[redacted]/jss/promk1.js"></script>
<link href="/common/css/base.css" rel="stylesheet" type="text/css" media="screen, print" />
```

［図 1-2：不正な JavaScript ファイルが埋め込まれたページ］

また、［図 1-3］、［図 1-4］および［図 1-5］は設置された不正な JavaScript ファイルの例です。JavaScript の難読化アルゴリズムの違いによって見かけは異なっていますが、いずれも Referrer の値をチェックし、検索エンジンからのアクセスの場合のみ、E コマースサイトに誘導するようになっています。

```
var s = document.referrer;
if (s.indexOf("google") > 0 || s.indexOf("bing") > 0 || s.indexOf("yahoo") > 0 || s.indexOf("aol") > 0) {
        window.location.href = 'http://[redacted]'
}
```

［図 1-3：不正な JavaScript ファイル例 1］

```
var PCeWEea$1$ = ["[redacted]",
"\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 n$$E2$fXU2 = PCeWEea$1$[0];var JeZaGj3$msV3 = PCeWEea$1$[1];var b4 = window[PCeWEea$1$[2]]
[PCeWEea$1$[3]];if (b4) {      var orOebziI5 = JeZaGj3$msV3[PCeWEea$1$[4]](PCeWEea$1$[5]);     for (i = 0x0; i < orOebziI5[PCeWEea$1$[6]]; i++) {
if (b4[PCeWEea$1$[7]](orOebziI5[i]) > 0x0) {                  top[PCeWEea$1$[8]][PCeWEea$1$[9]] = n$$E2$fXU2          }       }}
```

［図 1-4：不正な JavaScript ファイル例 2］

```
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|[redacted]|referrer'.split('|'),0,{}))
```

［図 1-5：不正な JavaScript ファイル例 3］

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、10 件でした。前四半期の 16 件から 38%減少しています。次に、確認されたインシデントを紹介します。

(1) Lazarus グループによる攻撃

本四半期も Lazarus（別名 Hidden Cobra）と呼ばれる攻撃グループによる国内組織を狙った標的型攻撃の報告が引き続き寄せられました。確認された攻撃は、SNS 経由で対象組織の個人を標的にマルウェアに感染させようとする不正なリンクを送信するものでした。組織のネットワーク内への直接的な攻撃ではなく、個人が使用する SNS から侵入することで、標的とする組織に気づかれないように組織内ネットワークに侵入しようとする意図が感じられます。

Lazarus が使用するマルウェアについては、JPCERT/CC Eyes で詳細を解説しています。

攻撃グループ Lazarus がネットワーク侵入後に使用するマルウェア
https://blogs.jpcert.or.jp/ja/2020/08/Lazarus_malware.html

攻撃グループ Lazarus が使用するマルウェア BLINDINGCAN
https://blogs.jpcert.or.jp/ja/2020/09/BLINDINGCAN.html

(2) SSL-VPN 製品の脆弱性を突いた攻撃

本四半期に報告された標的型攻撃の中には、SSL-VPN 製品の脆弱性を突いて侵入した事案が含まれていました。攻撃者は、国内組織の海外拠点に設置された SSL-VPN 製品の脆弱性を侵入経路とし、SigLoader(1)と呼ばれる新種のマルウェアを使用して、攻撃を行っていました。

2019 年より、様々な SSL-VPN 製品の脆弱性が公表されており、これらを狙った攻撃が引き続き活発に行われています。標的型攻撃だけでなく、金銭目的のランサムウェア攻撃にも悪用されており、この傾向は今後も続くと考えられます。パッチ管理の徹底とログの確認を推奨します。

Pulse Connect Secure の脆弱性を狙った過去の攻撃事案については JPCERT/CC Eyes で詳細を解説しています。

Pulse Connect Secure の脆弱性を狙った攻撃事案
https://blogs.jpcert.or.jp/ja/2020/03/pulse-connect-secure.html

1.1.2. インシデントに関する情報提供のお願い

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

等の情報発信を行います。

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

1.2. 情報収集・分析

JPCERT/CC では、国内の企業ユーザーが利用するソフトウェア製品の脆弱性情報、国内のインターネットユーザーが影響を受ける可能性のあるコンピューターウイルス、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、あわ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：17 件（うち更新情報が 5 件）　https://www.jpcert.or.jp/at/

2020-10-14　2020 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)
2020-10-14　Adobe Flash Player の脆弱性 (APSB20-58) に関する注意喚起 (公開)
2020-10-21　2020 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)
2020-11-04　Adobe Acrobat および Reader の脆弱性 (APSB20-67) に関する注意喚起 (公開)

2020-11-04　2020 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 (更新)
2020-11-11　2020 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)
2020-11-18　Cisco Security Manager の複数の脆弱性に関する注意喚起 (公開)
2020-12-02　ファイル・データ転送アプライアンス FileZen に関する注意喚起 (公開)
2020-12-04　Apache Tomcat の脆弱性 (CVE-2020-17527) に関する注意喚起 (公開)
2020-12-09　Cisco Security Manager の複数の脆弱性に関する注意喚起 (更新)
2020-12-09　Apache Struts 2 の脆弱性 (S2-061) に関する注意喚起 (公開)
2020-12-09　2020 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)
2020-12-09　OpenSSL の脆弱性 (CVE-2020-1971) に関する注意喚起 (公開)
2020-12-10　Adobe Acrobat および Reader の脆弱性 (APSB20-75) に関する注意喚起 (公開)
2020-12-11　ファイル・データ転送アプライアンス FileZen に関する注意喚起 (更新)
2020-12-17　2020 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 (更新)
2020-12-21　Apache Struts 2 の脆弱性 (S2-061) 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 94 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。

2020-10-07　経済産業省が『サイバーセキュリティ体制構築・人材確保の手引き』(第 1 版)を公開
2020-10-14　警察庁が「令和 2 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
2020-10-21　総務省が「特別定額給付金の給付を騙ったメールに対する注意喚起」を公開
2020-10-28　IPA が「情報セキュリティ安心相談窓口の相談状況［ 2020 年第 3 四半期 (7 月～9 月) ］」を公開
2020-11-05　IPA が「サイバー情報共有イニシアティブ（J-CSIP）運用状況［2020 年 7 月～9 月］」を公開
2020-11-11　JPCERT／CC がイベントログ分析支援ツール「LogonTracer v1.5.0」を公開
2020-11-18　攻撃グループ BlackTech が使用する Linux 版マルウェア（ELF_PLEAD）について
2020-11-26　JASA が「サイバーセキュリティ対策マネジメントガイドライン Ver2.0」を公開
2020-12-02　NISC が「ランサムウエアによるサイバー攻撃について【注意喚起】」を公開
2020-12-09　JPCERT/CC 「QuasarRAT analysis tools and research report」を公開

2020-12-16　JPCERT/CC Eyes 「Quasar Family による攻撃活動」を公開
2020-12-23　制御システムセキュリティカンファレンス 2021 参加登録開始のお知らせ

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、脆弱性やマルウェア、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：15 件（うち更新情報が 2 件）　https://www.jpcert.or.jp/newsflash/

2020-10-13　Acronis 製バックアップソフトウェアの複数の脆弱性について
2020-10-14　Intel 製品に関する複数の脆弱性について
2020-10-15　DDoS 攻撃を示唆して仮想通貨による送金を要求する脅迫行為 (DDoS 脅迫) について (更新)
2020-10-16　Magento に関するアップデート (APSB20-59) について
2020-10-21　複数の Adobe 製品のアップデートについて
2020-10-30　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
2020-11-11　複数の Adobe 製品のアップデートについて
2020-11-11　Intel 製品に関する複数の脆弱性について
2020-11-27　Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性 (CVE-2018-13379) の影響を受けるホストに関する情報の公開について
2020-12-09　複数の Adobe 製品のアップデートや予告について
2020-12-15　SolarWinds 社製 SolarWinds Orion Platform ソフトウェアのアップデートについて
2020-12-22　Emotet などのマルウェア感染に繋がるメールに引き続き警戒を
2020-12-23　2020 年 9 月から 12 月を振り返って

2020-12-25　複数のバックアップソフトウェアの脆弱性について
2020-12-28　SolarWinds 社製 SolarWinds Orion Platform ソフトウェアのアップデートについて (更新)

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) Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性（CVE-2018-13379）の影響を受けるホストに関する情報発信

JPCERT/CC は、Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性の影響を受けるホストに関する情報が 2020 年 11 月 19 日頃にフォーラムなどで公開されたことを確認しています。この情報には、FortiOS の任意のファイル読み取りの脆弱性（CVE-2018-13379）の影響を受けるとみられるホストの一覧に加え、SSL VPN 接続を利用するユーザーアカウント名や、平文のパスワードなどの認証情報が含まれています。当該製品を使用しており、SSL VPN サービスを有効にした状態で脆弱性の影響を受けるバージョンを稼働させている場合、公開されている認証情報や脆弱性を悪用した攻撃を受ける可能性があります。JPCERT/CC は、公開されたホストの一覧に、日本の IP アドレスが含まれていることを確認しており、11 月 27 日の CyberNewsFlash で、脆弱性の詳細や想定される影響、対策についての情報を公開し、広く注意を呼びかけました。また、連絡可能な該当するホストの管理者に情報提供を行い、侵害有無の確認と対策を早急に行うよう呼びかけました。

CyberNewsFlash 「Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性 (CVE-2018-13379) の影響を受けるホストに関する情報の公開について」
https://www.jpcert.or.jp/newsflash/2020112701.html

(2) DDoS 攻撃をすると脅して仮想通貨による送金を要求する脅迫行為（DDoS 脅迫）に関する情報発信

JPCERT/CC は 2020 年 9 月に、DDoS 攻撃をすると脅して仮想通貨による送金を要求する脅迫行為に関する情報を CyberNewsFlash で公開しました。その後、10 月に入り、本攻撃による被害の報告が複数の国内組織から寄せられました。多くのケースでは、脅迫メールが送られた後すぐに、攻撃能力を示す目的からか、標的のシステムに対して数十 Gbps から 100Gbps の規模の DDoS 攻撃が 30 分から 60 分間ほど行われたことが確認されています。また、複数の IP アドレスやシステムを対象とした攻撃が行われる場合もあり、DNS コンテンツサーバーを標的とするようなケースも確認されています。JPCERT/CC が確認している限りでは、攻撃は情報・通信系の組織に対して多く行われている傾向があります。これらの状況を踏まえて、JPCERT/CC は、10 月 15 日に CyberNewsFlash を更新し、国内の組織に対して改めて注意を呼びかけました。

CyberNewsFlash 「DDoS 攻撃を示唆して仮想通貨による送金を要求する脅迫行為 (DDoS 脅迫) について」
https://www.jpcert.or.jp/newsflash/2020090701.html

(3) Cisco Security Manager の複数の脆弱性に関する情報発信

2020 年 11 月 16 日（米国時間）、Cisco は Cisco Security Manager の複数の脆弱性（CVE-2020-27125、CVE-2020-27130、CVE-2020-27131）に関する情報を公開しました。公開された情報によると、本脆弱性を悪用された場合、遠隔の第三者が当該製品上から任意のファイルをダウンロードしたり、当該製品上で任意の Java コードを管理者権限で実行したりする可能性があります。JPCERT/CC は、本脆弱性に関連する実証コードが Web 上に公開されていることを確認しており、脆弱性を悪用する攻撃が行われる可能性があることから、2020 年 11 月 18 日に注意喚起および早期警戒情報を発行し、早期のアップデートを呼びかけました。また、2020 年 12 月 7 日（米国時間）に、一部の脆弱性に対する修正バージョンが公開されたことから、JPCERT/CC も後日情報を更新しました。

Cisco Security Manager の複数の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2020/at200043.html

1.3. インターネット上でリスク源となり得るノードの状態と活動を示す観測データの収集および分析

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ー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、サイバー空間全体の健全性を次の 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」）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ー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 —

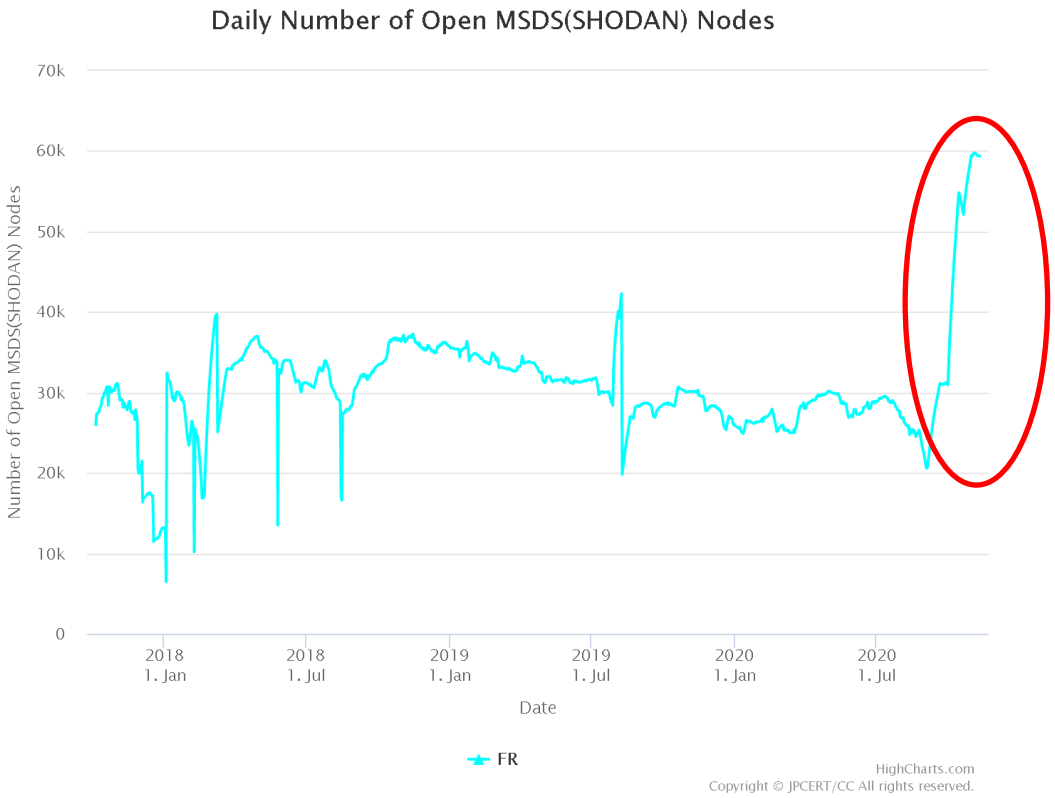
インターネットリスク可視化サービス Mejiro では、次のポートがインターネットに対して開いているノードを DoS リフレクション攻撃（DRDoS）に悪用される恐れのあるインターネット上のリスク要因と見なし、国や地域ごとにその分布状況を分析しています。

・19/udp（CHARGEN）
・53/udp（DNS）
・123/udp（NTP）
・161/udp（SNMP）
・445/tcp（MSDS）
・1900/udp（SSDP）
・5060/udp（SIP）

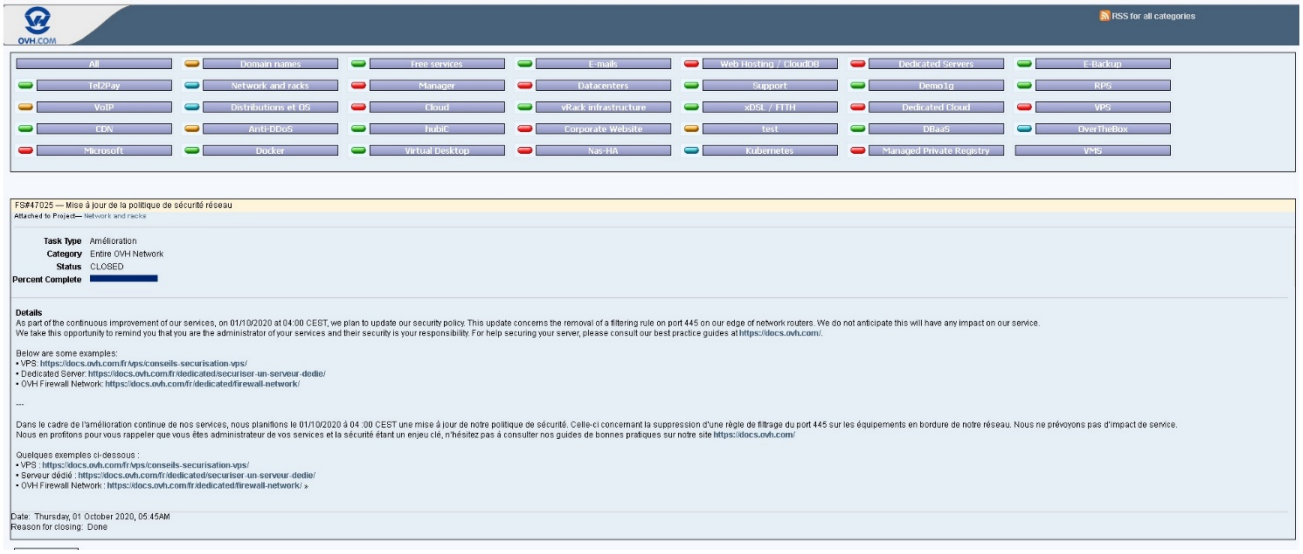
それらのノードの IP アドレスをもとにノードが設置された国・地域を判別して、リスク要因の分布状況を調べます。さらに、国・地域ごとのリスク要因となるノード数から、Mejiro 指標と呼ばれる指標値を算出します。各国・地域の Mejiro 指標の値を比較することで、それぞれの国・地域の相対的な特徴を明らかにして、対策の必要性や方向性を判断する参考にできると期待し、一般に公表しています。各国・地域の Mejiro 指標の値を比較することで、それぞれの国・地域の相対的な特徴を明らかにして、対策の必要性や方向性を判断する参考にできると期待しています。

1.3.1.2. フランス（FR）におけるポート 445/TCP の開放ついて

2020 年 10 月初旬ごろからフランス(FR ; Mejiro での ccTLD の分類による）で Port 445/TCP が解放されているノードが増加し、Mejiro 指標も悪化していることが認められました。



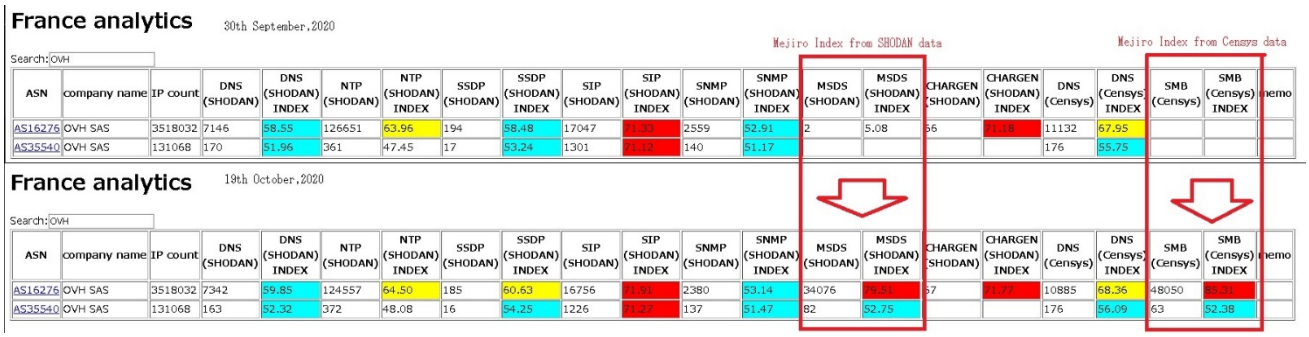
［図 1-6：FR の Port 445/TCP が解放されている端末の状況］



［図 1-7：OVH 社のポリシー変更について］

この増加の背景を調べてみると、2020 年 10 月 1 日 4:00(CEST)にフランスのクラウド事業者である OVH 社が、セキュリティポリシーの変更を行い、Port 445/TCP のフィルターを解除したことによる影響とみられます。Mejiro では、ASN 別に指標の分析を行っており、FR に分類する各 ASN での指標の変化を確

認したところ、OVH 社に割り当てられた ASN の Mejiro 指標が最も大きく悪化していました。



France analytics 30th September,2020

Search:OVH

Mejiro Index from SHODAN data　　Mejiro Index from Censys data

ASN	company name	IP count	DNS (SHODAN)	DNS (SHODAN) INDEX	NTP (SHODAN)	NTP (SHODAN) INDEX	SSDP (SHODAN)	SSDP (SHODAN) INDEX	SIP (SHODAN)	SIP (SHODAN) INDEX	SNMP (SHODAN)	SNMP (SHODAN) INDEX	MSDS (SHODAN)	MSDS (SHODAN) INDEX	CHARGEN (SHODAN)	CHARGEN (SHODAN) INDEX	DNS (Censys)	DNS (Censys) INDEX	SMB (Censys)	SMB (Censys) INDEX	memo
AS16276	OVH SAS	3518032	7146	58.55	126651	63.96	194	58.48	17047	71.33	2559	52.91	2	5.08	56	71.18	11132	67.95			
AS35540	OVH SAS	131068	170	51.96	361	47.45	17	53.24	1301	71.12	140	51.17					176	55.75			

France analytics 19th October,2020

Search:OVH

ASN	company name	IP count	DNS (SHODAN)	DNS (SHODAN) INDEX	NTP (SHODAN)	NTP (SHODAN) INDEX	SSDP (SHODAN)	SSDP (SHODAN) INDEX	SIP (SHODAN)	SIP (SHODAN) INDEX	SNMP (SHODAN)	SNMP (SHODAN) INDEX	MSDS (SHODAN)	MSDS (SHODAN) INDEX	CHARGEN (SHODAN)	CHARGEN (SHODAN) INDEX	DNS (Censys)	DNS (Censys) INDEX	SMB (Censys)	SMB (Censys) INDEX	memo
AS16276	OVH SAS	3518032	7342	59.85	124557	64.50	185	60.63	16756	71.91	2380	53.14	34076	79.51	67	71.77	10885	68.36	48050	85.31	
AS35540	OVH SAS	131068	163	52.32	372	48.08	16	54.25	1226	71.27	137	51.47	82	52.75			176	56.09	63	52.38	

［図 1-8：OVH 社の Mejiro 指標］

445/TCP を通じて感染拡大活動をするワームが存在し、445/TCP のポートがインターネットに対して開いているとそうしたワームに感染する可能性があります。そうした懸念を CERT FR に伝えるとともに、JPCERT/CC では今後の推移を注意深く見守ることにしています。

ただ、これまでのところ、定点観測システム TSUBAME が捕捉したフランスからのスキャンに大きな変化は見られず、ワームへの感染の拡大には直結していないようです。OS が適切にアップデートされているなどの対策により適切に防御されているためと考えられます。

本件からの学びとして、クラウド上の仮想サーバーの利用にあたっては、クラウド事業者のネットワーク・ポリシーが変更される可能性を考慮して基本的な対策を取っておくことや，事業者においてもセキュリティに配慮したフィルターやテンプレートの提供の重要性を挙げることができます。

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/

OVH Tasks
http://travaux.ovh.net/?do=details&id=47025&edit=yep

1.3.2. 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

1.3.2.1. 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ーを開発し、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」）を構築し運用しています。TSUBAME から得られる情報を、すでに公開されている脆弱性情報やマルウェア、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付くことがあります。
観測用センサーの設置に協力した 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

1.3.2.2. TSUBAME の観測データの活用

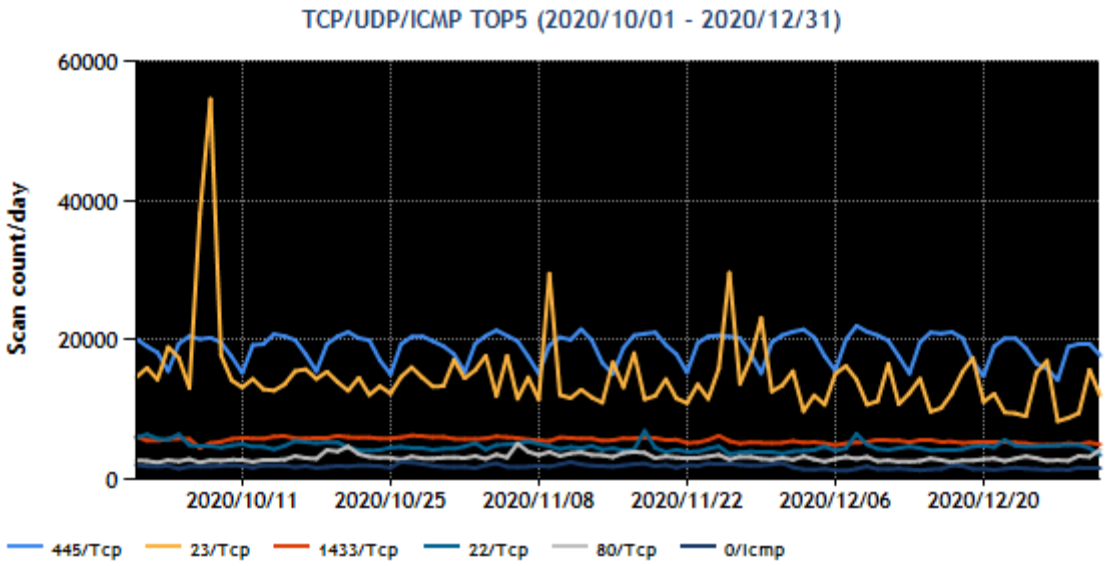
JPCERT/CC では、主に日本企業のシステム管理者の方々に、自組織のネットワークに届くパケットの傾向と比較していただけるよう、日本国内の TSUBAME のセンサーで受信したパケットを宛先ポート別に集計してグラフ化し、毎週月曜日に JPCERT/CC の Web ページで公開しています。また、四半期ごとに観測傾向や注目される現象を紹介する「インターネット定点観測レポート」を公開しており、2020 年 7 月から 9 月分のレポートを 2020 年 10 月 29 日に公開しました。

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

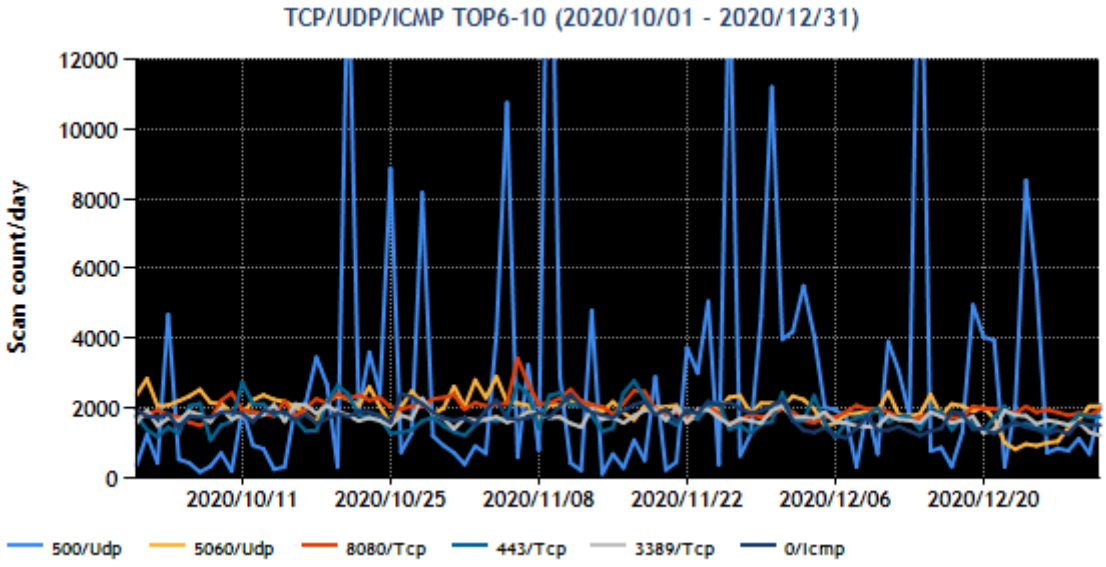
インターネット定点観測レポート（2020 年 7～9 月）
https://www.jpcert.or.jp/tsubame/report/report202007-09.html

1.3.2.3. 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 1-9］と［図 1-10］に示します。

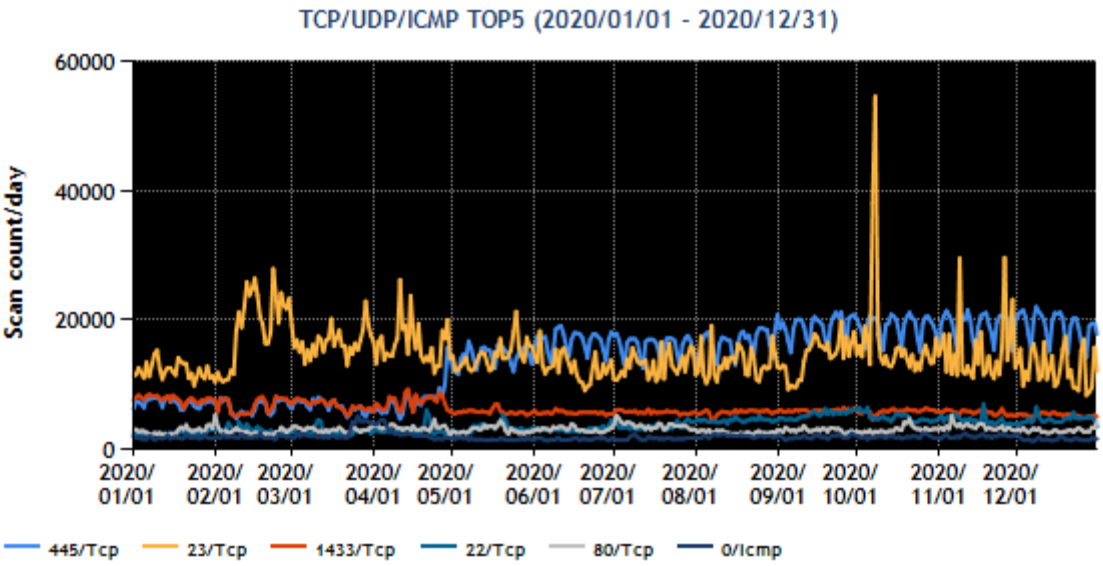


［図 1-9：宛先ポート別グラフ トップ 1-5（2020 年 10 月 1 日-12 月 31 日)］

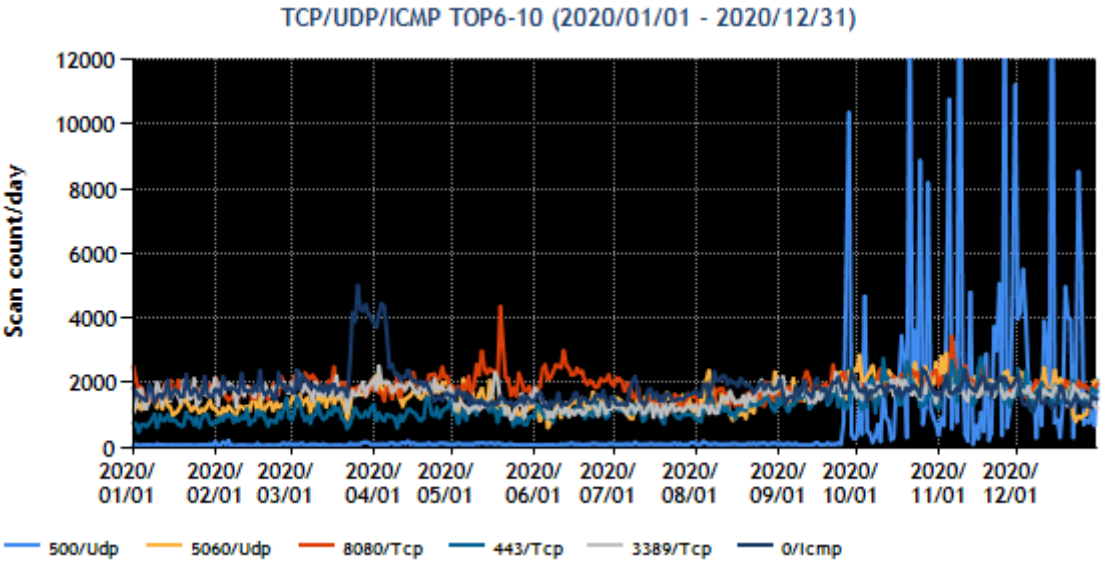


［図 1-10：宛先ポート別グラフ トップ 6-10（2020 年 10 月 1 日- 12 月 31 日)］

また、過去 1 年間（2029 年 10 月 1 日-2020 年 9 月 30 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 1-11］と［図 1-12］に示します。



［図 1-11：宛先ポート別グラフ トップ 1-5（2020 年 1 月 1 日-12 月 31 日）］



［図 1-12：宛先ポート別グラフ トップ 6-10（2020 年 1 月 1 日-12 月 31 日）］

本四半期に最も多く観測されたパケットは 445/TCP（microsoft-ds）宛のものでした。インターネットリスク可視化サービス Mejiro の節で、フランス OVH のネットワーク・ポリシーの変更に触れました

が、観測傾向から、その影響で多くのパケットが観測されたとは言えません。観測結果をもとに通知した国内のネットワーク管理者からは、不正アクセスが行われていた形跡や、マイニングを行うマルウェアへの感染が見つかったとの情報提供がありました。ブルートフォースや脆弱性などの攻撃によって不

正アクセスを受け、マルウェアに感染した結果と考えられますが、攻撃の全容が解明できていないことから、利用者は OS のアップデートやファイアウォールの利用、強固なパスワードの使用など注意することが望まれます。
また、国内の組織を対象とした DDoS 攻撃が目的とみられるパケットを観測しました。観測されたパケットから DDoS 攻撃の手法を複数確認できました。攻撃対象となった組織に対して、情報を提供しました。

1.3.2.4. 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、スキャン活動を TSUBAME によって観測することに加えて、スキャンに応答した場合に始まる攻撃のための通信内容を低対話型ハニーポットにより観測するための試作システムを用意して、その有効性を確認するための試験運用を行っています。試験運用では、簡単なシステムを構築して HTTP リクエストを収集し、それを分析しています。

2020 年 10 月 28 日以降、Oracle WebLogic Server の脆弱性（CVE-2020-14882）の悪用を試みる通信を観測しています。この通信は、Weblogic が動作するサーバーに細工されたパケットを送信することで、サーバー上で任意のコードを実行させるもの考えられます。脆弱性（CVE-2020-14882）は、2020 年 10 月のクリティカルアップデートで修正されています。JPCERT/CC では、観測した内容に基づき注意喚起の更新や、早期警戒情報の提供を行いました。

2020 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
https://www.jpcert.or.jp/at/2020/at200040.html

また、HTTP プロトコル以外のプロトコルによる攻撃も観測できるような複数のハニーポットプログラムの試験を実施しています。本四半期の試験では、6 種類のハニーポットで、SSH プロトコルや RDP プロトコルによる攻撃を観測でき、対応策の検討のための参考情報と役立つ情報を収集できることが確認できました。なお，今回観測された攻撃については、収集した情報に基づいて、関係者に対策を促すための通知をする準備を進めています。

2. 脆弱性関連情報流通促進活動

JPCERT/CC は、ソフトウェ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 から届け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け出状況については、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/

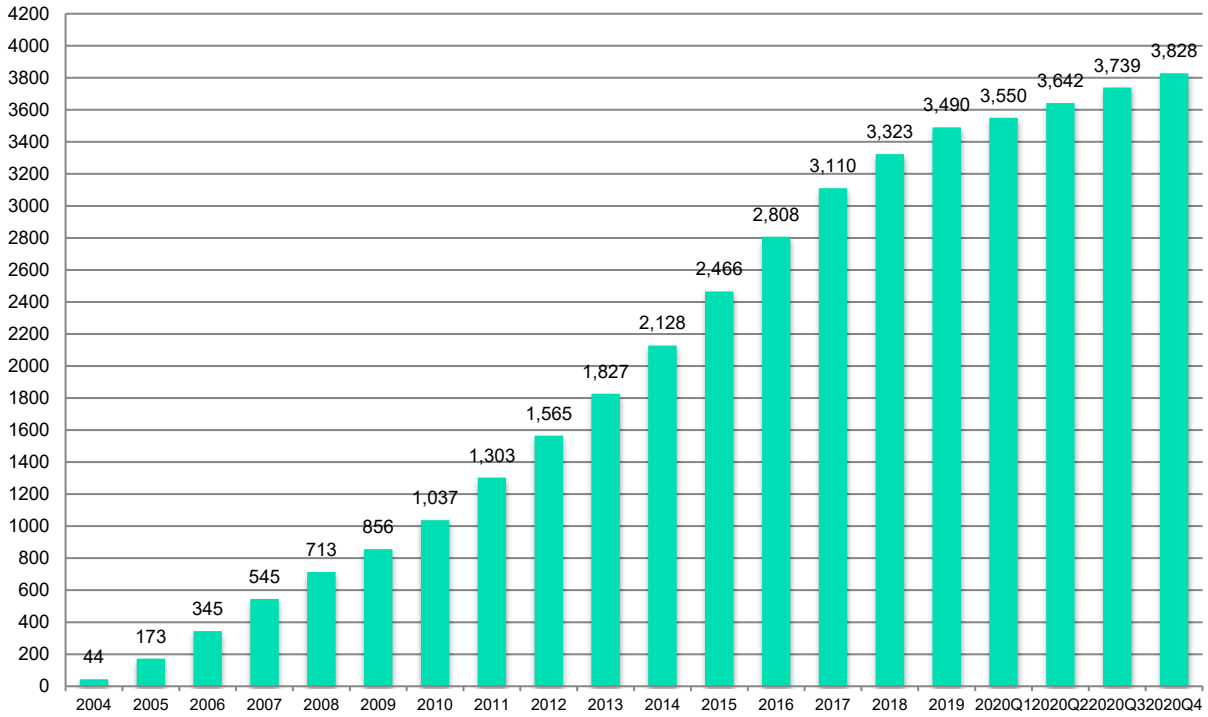
2.1.2. Japan Vulnerability Notes（JVN）において公表した脆弱性情報および対応状況

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 CISA ICS 、NCSC-NL、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等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 89 件（累計 3,828 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/



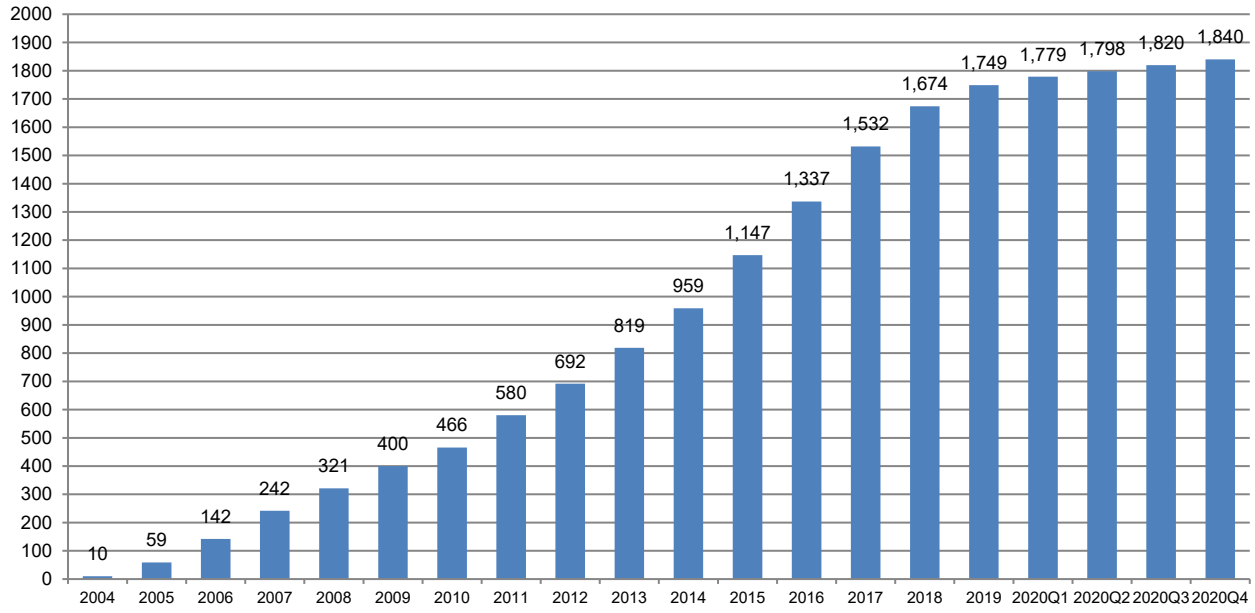
［図 2-1：JVN 公表累積件数］

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 20 件（累計 1,840 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 20 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 15 件（このうち自社製品の届け出によるものが 5 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 2 件、国内外の複数の製品開発者の製品に影響を及ぼすものが 3 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ーごとの内訳は、［表 2-1］のとおりです。本四半期は、CMS と組込系製品がそれぞれ 4 件と最も多く、次いでプラグインが 3 件、続いて Windows アプリケーション、グループウェアが 2 件、アプライアンス、アプリケーションフレームワーク、スマートフォンアプリケーション、制御系製品、ライブラリがそれぞれ 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ー内訳］

製品分類	件数
CMS	4
組込系製品	4
プラグイン	3
Windows アプリケーション	2
グループウェア	2
アプライアンス	1
アプリケーションフレームワーク	1
スマートフォンアプリケーション	1
制御系製品	1
ライブラリ	1



［図 2-2：公表を行った国内取扱脆弱性情報の累積件数］

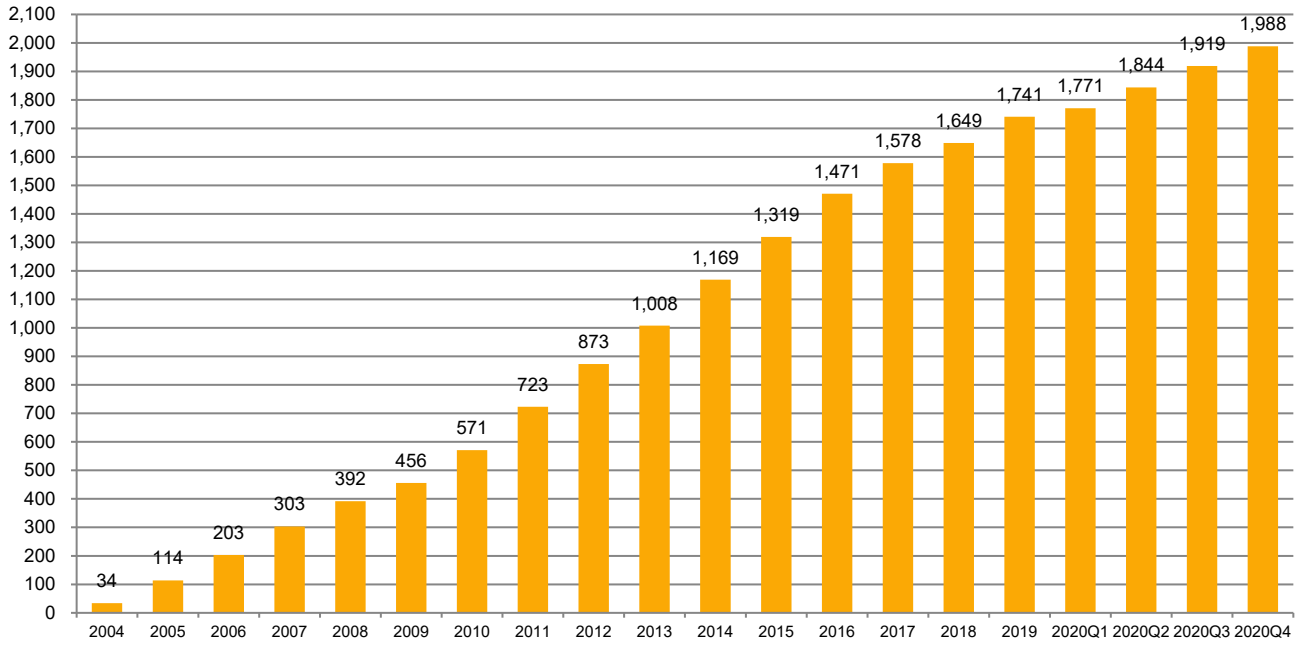
本四半期に公表した国際取扱脆弱性情報は 69 件（累計 1,988 件）で、累計の推移は［図 2-3］に示すとおりです。69 件のうち 68 件はアドバイザリとして公表したもので、1 件は発見者と JPCERT/CC で共同執筆し Technical Alert として公表したものでした。69 件のアドバイザリおよび Technical Alert のうち、海外調整機関や製品開発者等からの届け出によるものおよび製品開発者による脆弱性情報公開の事前通知によるものは 21 件、国内外の発見者からの届け出によるものは 3 件でした。

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ー内訳は、［表 2-2］のとおりです。本四半期は、制御系製品が 39 件と最も多く、次いで医療機器が 4 件、CMS、Windows アプリケーション、アンチウイルス製品、組込系製品、プロトコルに関するものがそれぞれ 3 件、macOS、macOS アプリケーション、ウェブサーブレットコンテナ―、マルチプラットフォームアプリケーションがそれぞれ 2 件、IT 資産管理ツール、サーバー製品、その他がそれぞれ 1 件でした。

本四半期も、国際取扱脆弱性情報において、製品開発者自身による届け出や、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。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、調整および公開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ー内訳］

製品分類	件数
制御系製品	39
医療機器	4
CMS	3
Windows アプリケーション	3
アンチウイルス製品	3
組込系製品	3
プロトコル	3
macOS	2
macOS アプリケーション	2
Web サーブレットコンテナ―	2
マルチプラットフォームアプリケーション	2
IT 資産管理ツール	1
サーバー製品	1
その他	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。

連絡不能開発者一覧
https://jvn.jp/reply/index.html

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 および CISA ICS、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。

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 では、2008 年 5 月以降 JVN 英語版サイトの公開を機に CVE 採番を行っており、Primary CNA である 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 番号を付与しています。本四半期には、JVN で公表したもののうち国内で届け出られた脆弱性情報に 49 個の CVE 番号を付与しました。

最初は CVE 番号の付与を、MITRE 社から番号プールの提供を受けて、その中から採番することにより実施していましたが、2010 年 6 月には CNA（CVE Numbering Authorities）として CVE 番号を付与し始めました。さらに 2018 年には Root CNA に指定され、新しい CNA の勧誘やトレーニングなどの活動も行っています。こうした活動の結果として、本四半期においては、三菱電機株式会社と株式会社 LINE の 2 社が、JPCERT/CC を Root とする CNA として新たに登録されました。

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

JPCERT/CC Eyes
CNA 活動レポート ～日本の 2 組織が新たに CNA に参加～
https://blogs.jpcert.or.jp/ja/2020/12/cna-2cna.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/

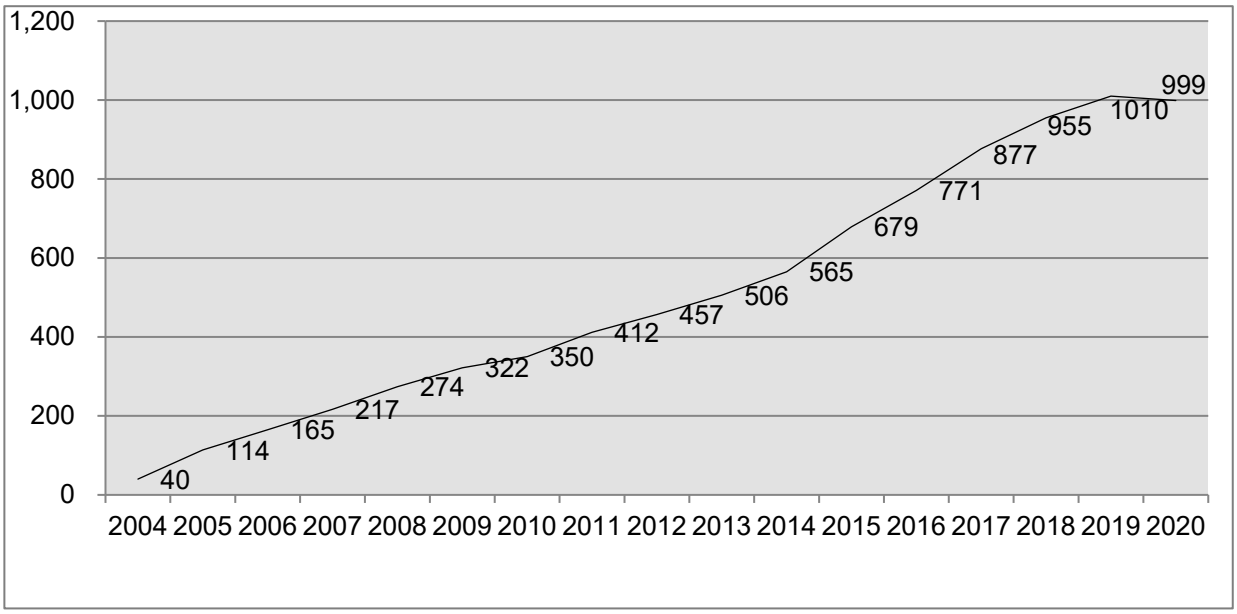
情報セキュリティ早期警戒パートナーシップガイドライン（2019 年版）
https://www.jpcert.or.jp/vh/partnership_guideline2019.pdf

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 12 月 31 日現在で 999 となっています。なお、これまでの製品開発者リストには、廃業や活動終了等のため今後の脆弱性対応を期待できない製品開発者も含まれていましたが、本四半期の調査で該当すると判明した者の登録を抹消しました。上記の登録数にはこの登録抹消に伴う減少分を反映しています。
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。
昨今の新型コロナウイルスの流行のため 3 月のミーティング開催を延期としてから現在に至るまで一堂に集合しての開催が困難であることや、拠点が東京から遠い製品開発者も参加しやすくなることに鑑み、新しい試みとしてオンライン形式でミーティングを開催することとし、本四半期には 2 回のミーティングを開催しました。10 月 16 日に開催した第 1 回は脆弱性事例と対策に関する議論と産業用ロボットのセキュリティに関する情報共有、12 月 18 日に開催した第 2 回は CWE と CVSS に関する勉強会や PSIRT 実態調査に関する報告などのプログラム構成で、参加者との意見交換を行いました。

2.3. 脆弱性の低減方策の研究・開発および普及啓発

早期警戒グループでは、脆弱なソフトウェ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ェア開発者の方々に伝えるための活動を行っています。

本四半期に次の 1 件の講演を行いました。

(1) 早稲田大学基幹理工学部「サイバー攻撃対策技術の基礎」: 2020 年 11 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、JPCERT/CC の活動を紹介する講演を行いました。セキュリティインシデントと CSIRT の概念を紹介するとともに、脆弱性関連情報の調整業務について詳しく説明しました。

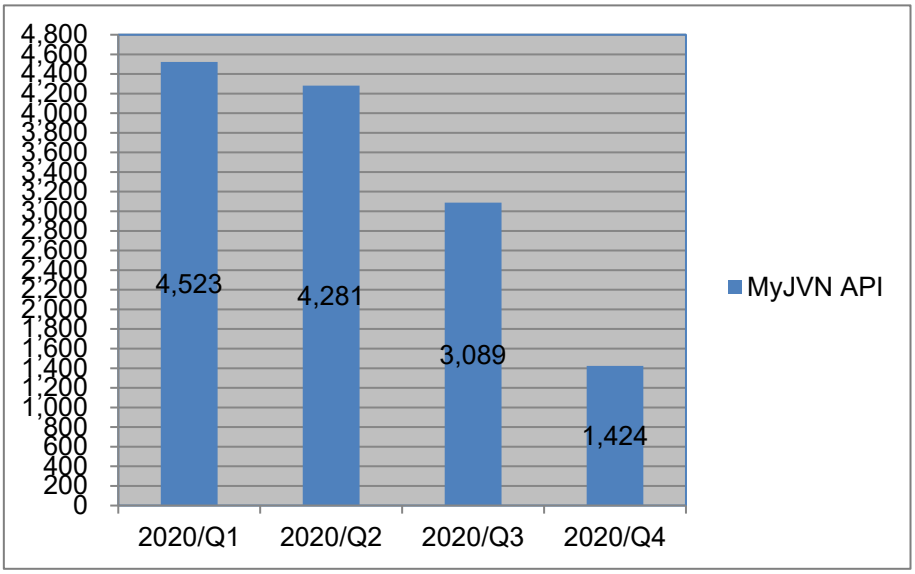
2.4. VRDA フィードによる脆弱性情報の配信

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

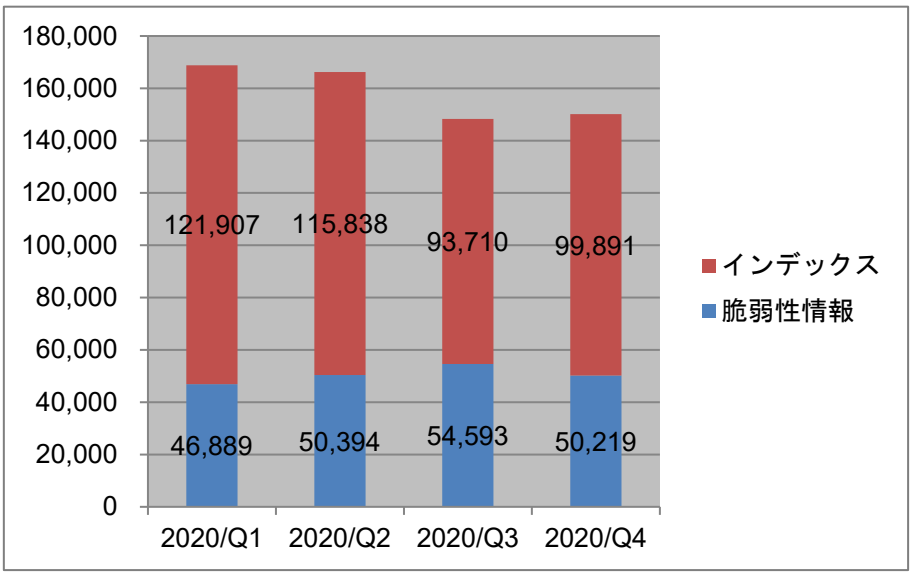
VRDA フィード 脆弱性脅威分析用情報の定型データ配信
https://www.jpcert.or.jp/vrdafeed/index.html

四半期ごとに配信した VRDA フィード配信件数を［図 2-5］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。

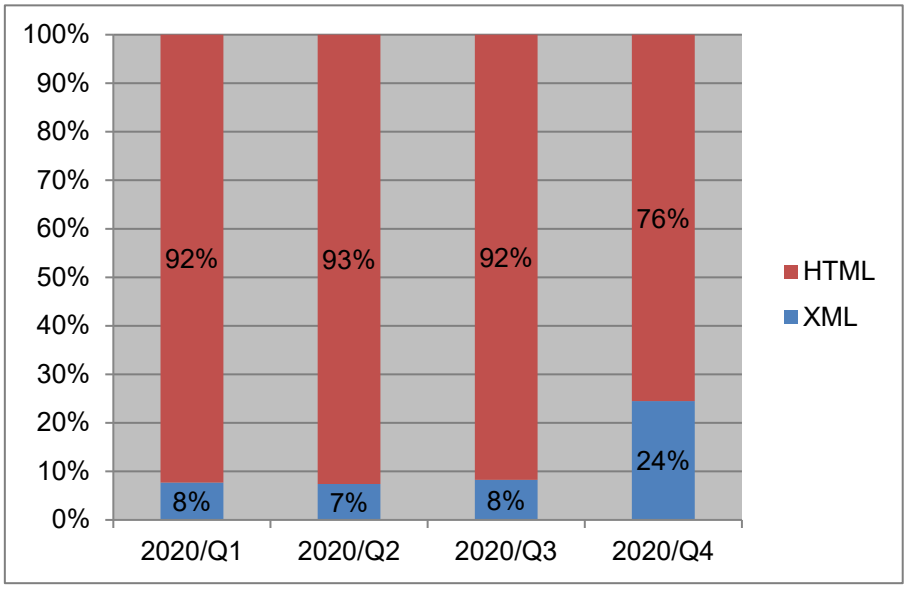


［図 2-5：VRDA フィード配信件数］



［図 2-6：VRDA フィード利用件数］

インデックスの利用数については、［図 2-6］に示したように、前四半期と比較し、約 7%増加しました。
脆弱性情報の利用数については、約 8%減少しました。



［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、XML 形式の利用割合が 16%増加しました。

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 162 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、その情報を必要とする国内組織に提供しました。

本四半期に提供した参考情報は 3 件でした。

2020/11/20 【参考情報】鉄道のサイバーセキュリティに関する ENISA の報告書について
2020/12/02 【参考情報】海事業界におけるサイバーセキュリティの課題についての情報が公表された件について
2020/12/02 【参考情報】NERC 傘下の E-ISAC の取り組みに関する情報が公表された件について

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ー (注 1) 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。

（注 1）JPCERT/CC が運営するコミュニティーで、制御システム関係者を中心に構成されています。

本四半期は計 3 件を配信しました。

2020/10/09　制御システムセキュリティニュースレター 2020-0009
2020/11/09　制御システムセキュリティニュースレター 2020-0010
2020/12/10　制御システムセキュリティニュースレター 2020-0011

制御システムセキュリティ情報共有コミュニティーでは、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 1,160 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。参加資格や申し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ー
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を行っています。本四半期における制御システムに関連するインシデントの報告件数は 0 件（0 IP アドレス）でした。

3.3. 関連団体との連携

SICE（計測自動制御学会）と JEITA（電子情報技術産業協会）、JEMIMA（日本電気計測器工業会）が定期的に開催している合同セキュリティ検討ワーキンググループに参加し、制御システムのセキュリティに関して専門家の方々と意見交換を行いました。

3.4. 制御システム向けセキュリティ自己評価ツールの提供

JPCERT/CC では、制御システムの構築と運用に関するセキュリティ上の問題項目を抽出し、バランスの良いセキュリティ対策を行っていただくことを目的として、簡便なセキュリティ自己評価ツールである日本版 SSAT（SCADA Self Assessment Tool：申し込み制）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 281 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す。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。

4. 国際連携活動関連

本四半期も引き続き、新型コロナウイルス感染症対策の観点から世界の多くの国で国外への渡航制限が敷かれ、予定されていた多くの国際会議が中止・延期ないしオンラインでの開催に変更されました。

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、アジア太平洋地域の CSIRT コミュニティーである 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、11 月 18 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. OIC-CERT 12th Annual Conference 2020 での講演（11 月 23 日～24 日）

OIC-CERT (Organisation of The Islamic Cooperation – Computer Emergency Response Teams) の年次会合が 11 月 23 日と 24 日にオンラインで開催されました。JPCERT/CC は 23 日に行われた Session 2: Technical (COVID-19 Hardening Security Operation) に APCERT の代表として参加し、OIC-CERT と APCERT のこれまでの協力関係や、新型コロナウイルス感染拡大が進む中オンラインで行われた年次会合やトレーニングなど組織内連携の取り組みについて紹介しました。

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/

4.2.2.1. 32nd FIRST Annual Conference - Virtual Edition での講演（11 月 16 日～18 日）

第 32 回 FIRST 年次会合は、6 月にカナダのモントリオールで開催される予定でしたが、新型コロナウイルス感染拡大の影響を受けて延期され、11 月 16 日から 18 日にかけてオンラインで開催されました。

JPCERT/CC は 11 月 16 日に「Bridging the Gap on SBOM: Collaborating for Software Component Transparency」と題したセッションで、脆弱性情報を取り扱う上での SBOM（Software Bill of Materials: ソフトウェア部品表）の考え方や、ソフトウェアの透明性と高める取り組みを米国の研究者とともに紹介しました。また、18 日には「Gear Up Regional CSIRT Community for More Robust Global Collaboration」と題したパネルセッションでモデレーターを務め、AfricaCERT と OIC-CERT の代表者を招いて地域的な CSIRT コミュニティーの活動について議論しました。

第 32 回 FIRST 年次会合についての詳細は、次の Web ページをご参照ください。

FIRST Annual Conference - Virtual Edition
https://www.first.org/conference/2020/

4.2.2.2. 2020 FIRST & AfricaCERT Virtual Symposium for Africa and Arab Regions での講演（10 月 21 日～23 日）

FIRST と AfricaCERT が共催する 2020 FIRST & AfricaCERT Virtual Symposium for Africa and Arab Regions が 10 月 21 日から 23 日にかけて、オンラインで行われました。JPCERT/CC は、23 日に行われたパネルセッション「Panel Discussion: Crisis Management During COVID-19」の中で、アフリカ地域の CSIRT 関係者らとともに、新型コロナウイルスに関連したサイバー攻撃やその対処事例について紹介しました。

2020 FIRST & AfricaCERT Virtual Symposium for Africa and Arab Regions
https://www.first.org/events/symposium/africa-arab-regions2020/

4.3. その他国際会議への参加

4.3.1. 国連軍縮研究所のパネルセッション「Neutrality and Peacebuilding in Cyberspace」での登壇（11 月 3 日）

ジュネーブ平和週間にあわせて国連軍縮研究所（UNIDIR）とチューリヒ工科大学が主催したパネルセッション「Neutrality and Peacebuilding in Cyberspace」が 11 月 3 日にオンラインで開催され、JPCERT/CC はパネリストとして参加しました。サイバー空間の規範に関する議論や、CERT の中立性に関して意見を述べました。

Neutrality and Peacebuilding in Cyberspace
https://unidir.org/events/neutrality-and-peacebuilding-cyberspace

4.3.2. Botconf 2020 での講演（12 月 1 日～4 日）

フランスの国際ボットネット対策連盟 Alliance internationale de lutte contre les botnets (AILB-IBFA) が主催した技術者向けのカンファレンス Botconf 2020 が 12 月 1 日から 4 日にかけてオンラインで開催されました。JPCERT/CC は 12 月 2 日に「Hunting the Quasar Family – How to Hunt a Malware Family」と題した講演を行い、Quasar RAT と呼ばれるマルウェアおよび亜種の挙動、また実際にそれらを使用した攻撃事例とその検知手法について解説しました。

Botconf 2020
https://www.botconf.eu/

4.4. 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「複数の開発者が関与する脆弱性の開示と取扱」の標準化作業と、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。

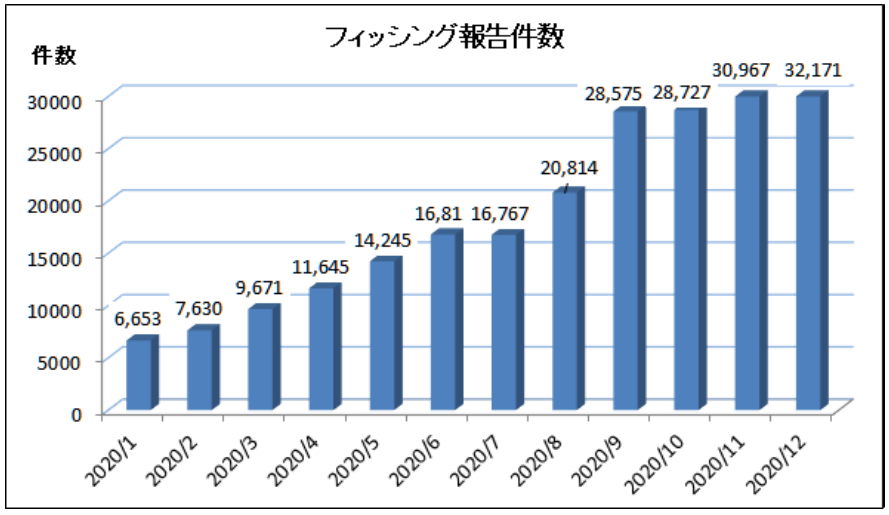
本四半期中は、「複数の開発者が関与する脆弱性の開示と取扱」に関して 9 月から開始された技術文書の作成に取り組んだほか、インシデント管理に関する標準の新しい WD：Working draft（作業原案）に対するコメントを提出しました。

5. 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・問い合せの受付、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、Web サイトを停止するための調整等を行っています。

5.1. フィッシングに関する報告・問い合わせの受付

本四半期のフィッシング報告件数は、2020 年初から毎月の報告件数が増加を続けており、2020 年 4 月には 1 万件、8 月には 2 万件を超え、さらに 11 月には年初 1 月の約 5 倍にあたる 3 万件を超える、非常に多くの報告が寄せられました。（[図 5-1]）



［図 5-1：1 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の報告が非常に多く、全体の約 54.8 %を占めています。次いで、三井住友カード、楽天、MyJCB、アプラスをかたるフィッシングの報告が多く、この 5 ブランドに関連する報告が全体の約 88.2 %を占めました。

5.2. 情報収集／発信

5.2.1. 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 15 件（ニュース：0 件、緊急情報：15 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。その内訳は次のとおりです。

- 特別定額給付金に関する通知を装うフィッシング：2 件
- MyJCB をかたるフィッシング：1 件
- 宅配便の不在通知を装うフィッシング：2 件
- UCS カードをかたるフィッシング：2 件
- アプラスをかたるフィッシング：1 件
- ポケットカードをかたるフィッシング：1 件
- 国税庁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
- オリコ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
- セディナカード・OMC カードをかたるフィッシング：1 件
- 三菱 UFJ 銀行をかたるフィッシング：1 件

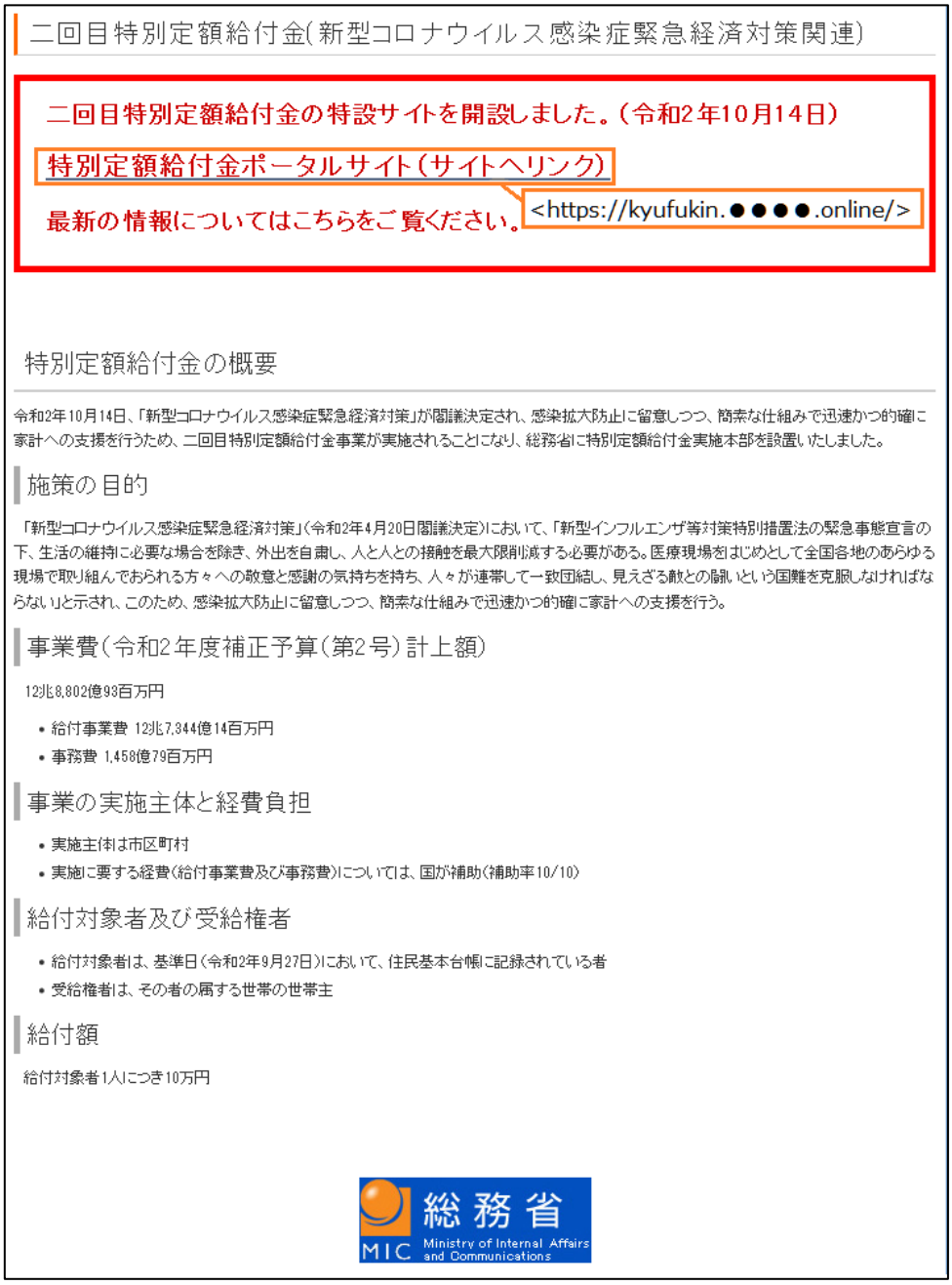
本四半期は新型コロナウイルス感染症の流行に関連して、特別定額給付金に関する通知を装うフィッシングの報告（[図 5-2：特別定額給付金に関する通知を装うフィッシングメールおよびフィッシングサイト]）が寄せられました。これは 2 回目の特別定額給付金配布の可能性についてニュースで報じられた翌日から発生し、個人情報およびクレジットカード情報等の入力を促されるものでした。他にも行政サービスをかたるフィッシングとして、国税庁の還付金申請フォームと誤認させて、個人情報およびクレジットカード情報の入力を促すフィッシングも確認されました。

その他、クレジットカードブランドをかたるフィッシングの報告が多く寄せられました。特に新規カードブランドや、しばらく報告がなかったカードブランドの報告を受領しています。これらカードブランドをかたるフィッシングの特徴として、メール文面は共通で、ブランド名（社名）の部分を変えて送られるケースが多いことを確認しています。

また、ショートメッセージサービス (SMS) を使用したフィッシングの報告が増えました。前四半期に引き続き、宅配便の不在通知を装うショートメッセージから金融機関をかたるフィッシングサイトへ誘導するケースの他、金融機関をかたるショートメッセージも確認されています。これらは、これらと同じようなショートメッセージに騙されて不正アプリ (マルウェア) をインストールしてしまった被害者の Android スマートフォンから送信されていることを確認しています。他には Amazon をかたるショートメッセージの報告が増えました。こちらは送信者が Amazon や Prime 等の文字列に設定されており、本物と誤認してフィッシングサイトへ情報を入力した、という相談が寄せられました。

2020 年 12 月に内閣府消費者委員会から「フィッシング問題への取組に関する意見」が提出されました。この中で「フィッシングメールの受信防止対策の普及促進」として「送信ドメイン認証技術の普及促進」と「迷惑メールフィルターの啓発強化」が挙げられています。国内のサービス事業者や組織における「なりすまし」フィッシングメール対策である送信ドメイン認証のさらなる普及と、利用者側における迷惑メールフィルターの利用の普及による被害抑制の効果が期待されます。

参考情報: 内閣府消費者委員会「フィッシング問題への取組に関する意見」
https://www.cao.go.jp/consumer/iinkaikouhyou/2020/1203_iken.html



二回目特別定額給付金(新型コロナウイルス感染症緊急経済対策関連)

二回目特別定額給付金の特設サイトを開設しました。(令和2年10月14日)

特別定額給付金ポータルサイト(サイトへリンク)

最新の情報についてはこちらをご覧ください。<https://kyufukin.●●●●.online/>

特別定額給付金の概要

令和2年10月14日、「新型コロナウイルス感染症緊急経済対策」が閣議決定され、感染拡大防止に留意しつつ、簡素な仕組みで迅速かつ的確に家計への支援を行うため、二回目特別定額給付金事業が実施されることになり、総務省に特別定額給付金実施本部を設置いたしました。

施策の目的

「新型コロナウイルス感染症緊急経済対策」(令和2年4月20日閣議決定)において、「新型インフルエンザ等対策特別措置法の緊急事態宣言の下、生活の維持に必要な場合を除き、外出を自粛し、人と人との接触を最大限削減する必要がある。医療現場をはじめとして全国各地のあらゆる現場で取り組んでおられる方々への敬意と感謝の気持ちを持ち、人々が連帯して一致団結し、見えざる敵との闘いという国難を克服しなければならない」と示され、このため、感染拡大防止に留意しつつ、簡素な仕組みで迅速かつ的確に家計への支援を行う。

事業費(令和2年度補正予算(第2号)計上額)

12兆8,802億93百万円

- 給付事業費 12兆7,344億14百万円
- 事務費 1,458億79百万円

事業の実施主体と経費負担

- 実施主体は市区町村
- 実施に要する経費(給付事業費及び事務費)については、国が補助(補助率10/10)

給付対象者及び受給権者

- 給付対象者は、基準日(令和2年9月27日)において、住民基本台帳に記録されている者
- 受給権者は、その者の属する世帯の世帯主

給付額

給付対象者1人につき10万円

総務省 MIC Ministry of Internal Affairs and Communications

［図 5-2：特別定額給付金に関する通知を装うフィッシングメールおよびフィッシングサイト ］

https://www.antiphishing.jp/news/alert/kyufukin_20201015.html

5.2.2. 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 10 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202010.html

2020 年 11 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202011.html

2020 月 12 日 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202012.html

5.2.3. 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アンチウイルス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 47 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。

5.2.4. フィッシング対策ガイドライン等の改定作業

「技術・制度検討ワーキンググループ」は、フィッシング対策協議会の会員等の有識者で構成される、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を作成・改訂を行う作業部会です。
今期は、2021 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 WG 会合
  日時：2020 年 10 月 28 日 10:00-12:00

- 技術・制度検討 WG 会合
  日時：2020 年 11 月 25 日 10:00-12:00

6. 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。

6.1. 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 83 回運営委員会
  日時：2020 年 10 月 20 日(火) 15:30-18:00

- 第 84 回運営委員会
  日時：2020 年 11 月 24 日(火) 15:30-18:00

- 第 85 回運営委員会
  日時：2020 年 12 月 22 日(火) 15:30-18:00

6.2. 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 10 月-12 月　毎週火曜日 11:00-11:30

- フィッシング対策セミナー2020（オンライン）
  日時：2020 年 11 月 6 日 (金) 10:00 - 15:15

※運営委員会およびワーキンググループ会合等はすべてオンライン開催

6.3. ワーキンググループ等の成果物の公開支援

本四半期においては、次のとおりワーキンググループ等の成果物の公開を支援しました。

STOP. THINK. CONNECT.普及啓発 WG

- 『第 16 回 IPA「ひろげよう情報モラル・セキュリティコンクール」2020』 の優秀賞を選出
  https://www.antiphishing.jp/news/info/20200714.html

チャレンジコイン授与

- フィッシング対策協議会よりコミュニティーにて活躍する有識者に対しチャレンジコイン贈呈を開始 (2020/12/08)
  https://www.antiphishing.jp/news/info/20201208.html

7. 公開資料

本章では JPCERT/CC が本四半期に公開した調査・研究の報告書や論文、セミナー資料を一覧にまとめています。

7.1. 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ー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。

2020-10-15 JPCERT/CC インシデント報告対応レポート [2020 年 7 月 1 日～2020 年 9 月 30 日]
https://www.jpcert.or.jp/pr/2020/IR_Report20201015.pdf

2020-12-11 JPCERT/CC Incident Handling Report [July 1, 2020 - September 30, 2020]
https://www.jpcert.or.jp/english/doc/IR_Report2020Q2_en.pdf

7.2. インターネット定点観測レポート

JPCERT/CC では、インターネット上に複数のセンサーを分散配置し、不特定多数に向けて発信されるパケットを継続して収集するインターネット定点観測システム「TSUBAME」を構築・運用しています。脆弱性情報、マルウェ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。

2020-10-29 JPCERT/CC インターネット定点観測レポート [2020 年 7 月 1 日～2020 年 9 月 30 日]
https://www.jpcert.or.jp/tsubame/report/report202007-09.html
https://www.jpcert.or.jp/tsubame/report/TSUBAMEReport2020Q2.pdf

2020-12-11 JPCERT/CC Internet Threat Monitoring Report [July 1, 2020 - September 30, 2020]
https://www.jpcert.or.jp/english/doc/TSUBAMEReport2020Q2_en.pdf

7.3. 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、ソフトウェ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。

2020-10-22　ソフトウェア等の脆弱性関連情報に関する届出状況[2020 年第 3 四半期 (7 月～9 月)]
https://www.jpcert.or.jp/press/2020/vulnREPORT_2020q2.pdf

7.4. 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、国内外のイベントやカンファレンスの様子などを JPCERT/CC のアナリストの眼をとおして、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 8 件の記事を公開しました。

日本語版発行件数：4 件　https://blogs.jpcert.or.jp/ja/

2020-10-30　LogonTracer v1.5 リリース
2020-11-10　攻撃グループ BlackTech が使用する Linux 版マルウェア（ELF_PLEAD）
2020-12-04　CNA 活動レポート ～日本の 2 組織が新たに CNA に参加～
2020-12-10　Quasar Family による攻撃活動

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

2020-10-30　LogonTracer v1.5 Released
2020-11-16　ELF_PLEAD - Linux Malware Used by BlackTech
2020-12-04　CNA activity report - 2 organizations from Japan newly added as CNAs
2020-12-10　Attack Activities by Quasar Family

8.　主な講演活動

(1) 小島 和浩（早期警戒グループ）：
「ビジネスメール詐欺の実態および対策 - #BECareful -」
JPAAWG 3rd General Meeting, JPAAWG 運営事務局, 2020 年 11 月 11 日
(2) 中井 尚子（インシデントレスポンスグループ）：
「DNS でいま起きていること」
JPAAWG 3rd General Meeting, JPAAWG 運営事務局, 2020 年 11 月 12 日
(3) 輿石 隆（早期警戒グループ）：
「サイバー攻撃 2020 - 昨今のサイバー攻撃動向とその問題 -」
Internet Week 2020, 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（JPNIC）,
2020 年 11 月 24 日

(4) 中井 尚子（インシデントレスポンスグループ）：
「ドメインハイジャック時のインシデント対応と外部機関との連携の重要性について」
Internet Week 2020, 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（JPNIC）, 2020 年 11 月 25 日

(5) 佐々木 勇人（早期警戒グループマネージャー）：
「新しい働き方」を支えるインシデント対応のポイント～2020 年のセキュリティ脅威の動向から～」
テレワーク PC、安全と言い切れますか？～専門家が語る脅威の実態と今後求められるエンドポイント対策～, アイティメディア株式会社 ＠IT 編集部,2020 年 11 月 27 日

(6) 土居 啓介（早期警戒グループ）：
「サイバー攻撃の検知、対応における Active Directory ログの重要性について」
第 17 回デジタル・フォレンジック・コミュニティ 2020 in TOKYO, 特定非営利活動法人 デジタル・フォレンジック研究会, 2020 年 12 月 7 日

(7) 小島 和浩（早期警戒グループ）：
「2020 年度 脅威動向の振り返り～被害を防ぐ為に今後できること～」
SecurityDay2020, SecurityDay 運営委員会, 2020 年 12 月 17 日

(8) 水野 哲也（インシデントレスポンスグループリーダー インシデントコーディネーター）：
パネル「リモートワーク」
SecurityDay2020, SecurityDay 運営委員会, 2020 年 12 月 17 日

9. 主な執筆活動

(1) 宮地利雄（技術顧問）
「制御システム・セキュリティの動向と展望」
月刊「計測技術」12 月号

10. 協力、後援

本四半期の行事開催に協力または後援等を行いました。

(1) SecurityDays 2020
主 催：株式会社ナノオプト・メディア
開催日：2020 年 10 月 7 日（水）～9 日（金）

(2) IAjapan 第 20 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：2020 年 11 月 11 日（水）～12 日（木）

(3) Internet Week 2020
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（JPNIC）
開催日：2020 年 11 月 17 日（火）～27 日（金）

(4) 第 16 回 IPA「ひろげよう情報モラル・セキュリティコンクール」2020
主　催：独立行政法人情報処理推進機構
開催日：2020 年 12 月 4 日（金）

(5) 第 17 回デジタル・フォレンジック・コミュニティ 2020 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：2020 年 12 月 7 日（月）～8 日（火）

(6) SecurityDay2020
主　催：SecurityDay 運営委員会
開催日：2020 年 12 月 17 日（木）

■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ーのお問い合わせ　：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