JPCERT/CC インシデント報告対応レポート

2022 年 1 月 1 日 ～ 2022 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

2022 年 4 月 14 日

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ー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、2022 年 1 月 1 日から 2022 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、コンピューター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)	5,306	5,822	5,060	16,188	11,870
インシデント件数 (注 3)	3,083	2,890	3,396	9,369	9,807
調整件数 (注 4)	1,723	1,632	2,203	5,558	6,554

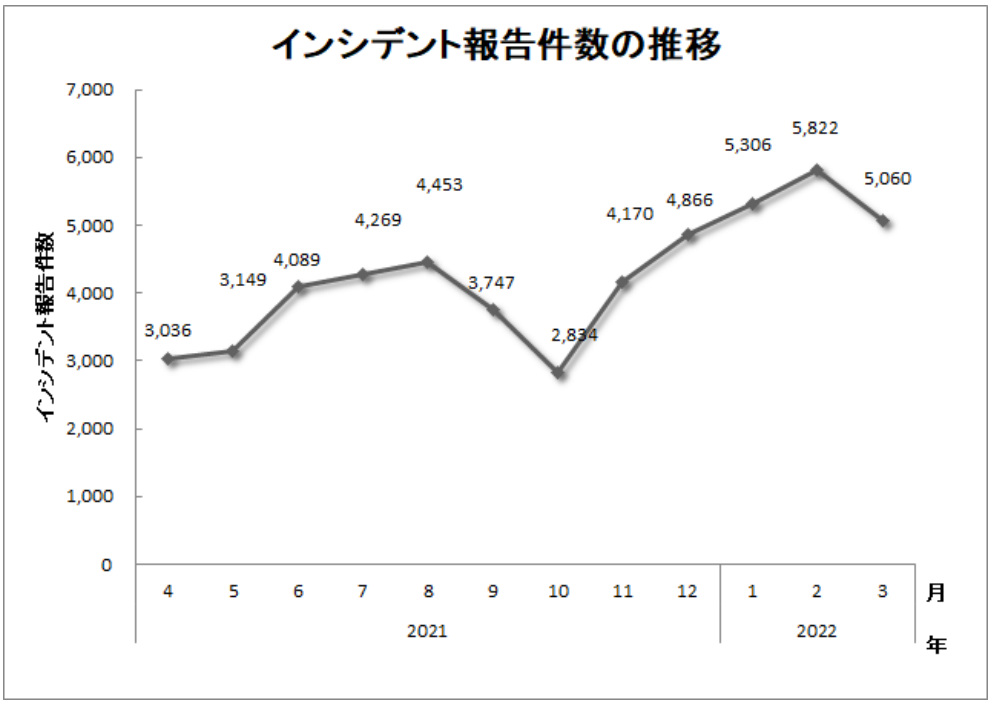
（注 2）「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

（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。

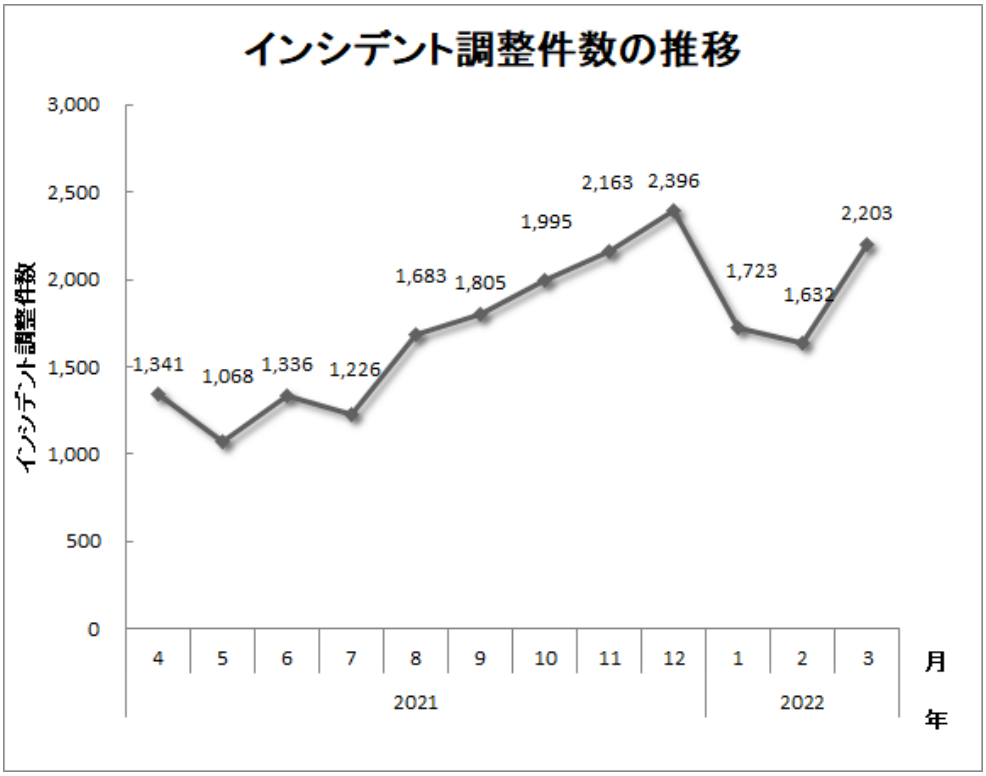
（注 4）「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、16,188 件でした。このうち、JPCERT/CC が国内外の関連する組織との調整を行った件数は 5,558 件でした。前四半期と比較して、報告件数は 36%増加し、調整件数は 15%減少しました。また、前年同期と比較すると、報告数は 68%増加し、調整件数は 39%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 年間の月次の推移を示します。



［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］

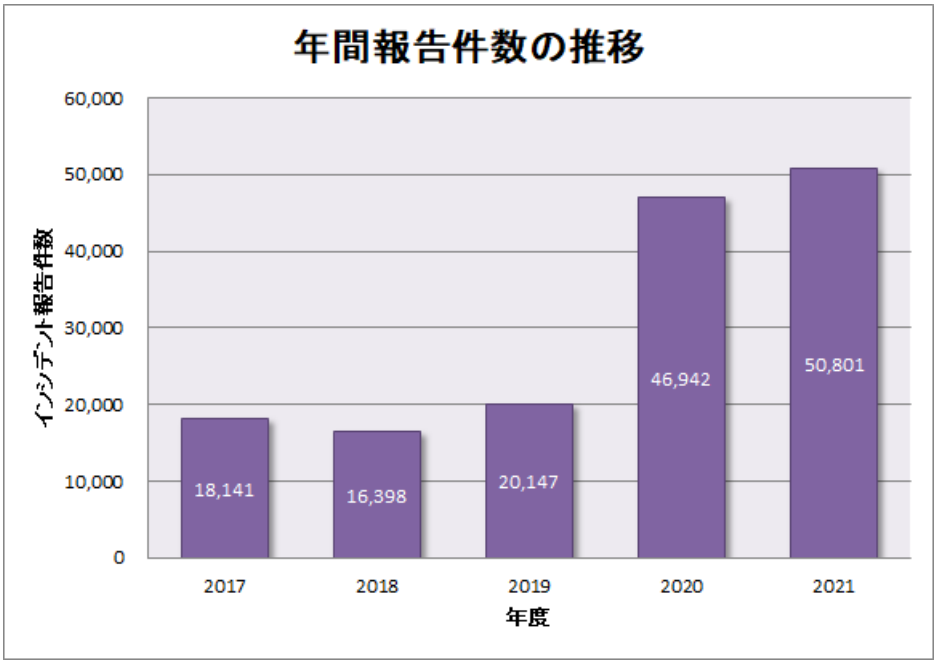
【参考】統計情報の年度比較

2021 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	2017	2018	2019	2020	2021
報告件数	18,141	16,398	20,147	46,942	50,801

2021 年度に寄せられた報告件数は 50,801 件でした。前年度の 46,942 件と比較して、8%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。



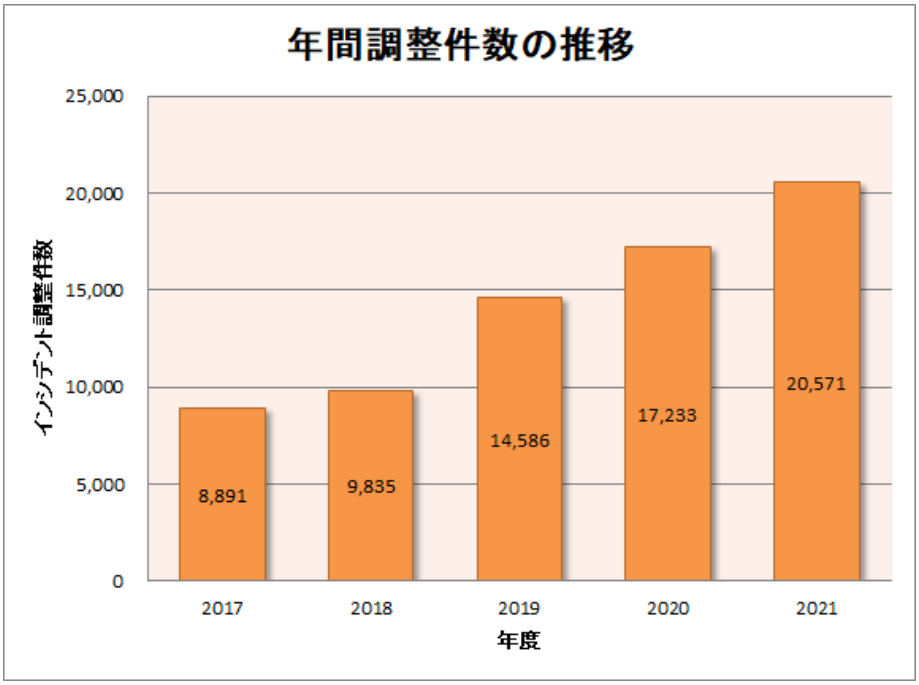
［図 3：年間報告件数の推移（年度比較）］

2021 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	2017	2018	2019	2020	2021
調整件数	8,891	9,835	14,586	17,233	20,571

2021 年度に調整を行った件数は 20,571 件でした。前年度の 17,233 件と比較して、19%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。

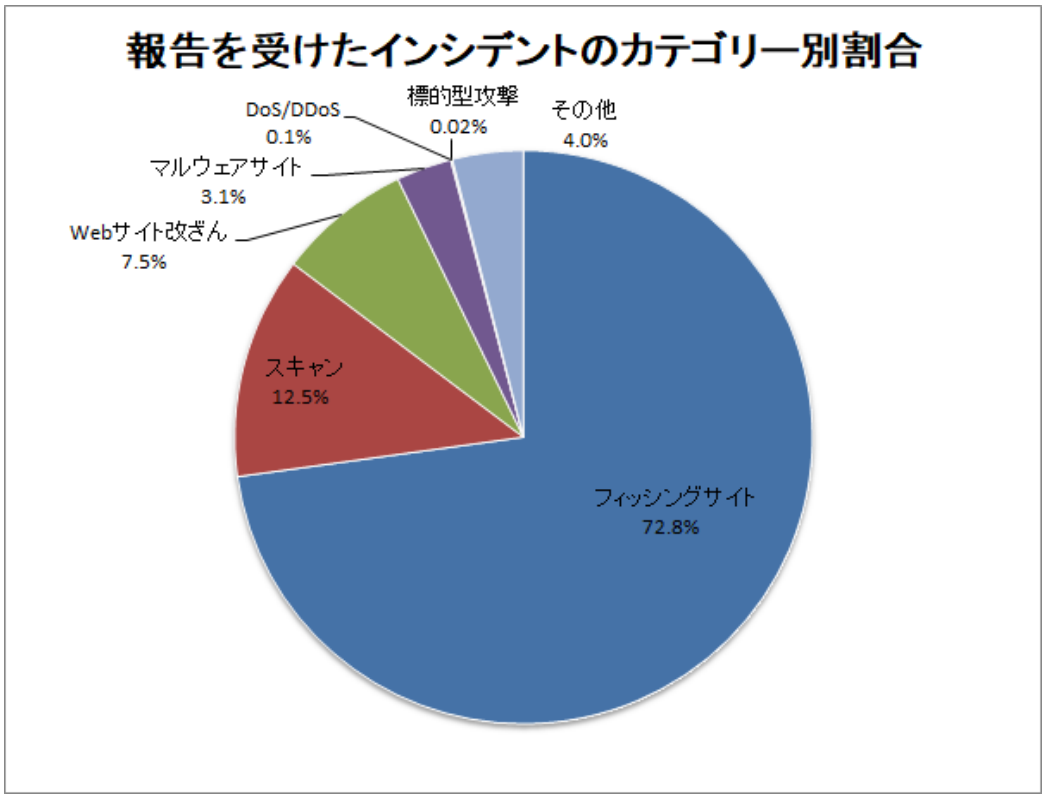


［図 4：年間調整件数の推移（年度比較）］

JPCERT/CC では、報告を受けたインシデントをカテゴリー別に分類し、各インシデントカテゴリーに応じた調整、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ーごとの内訳を［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ーごとの内訳］

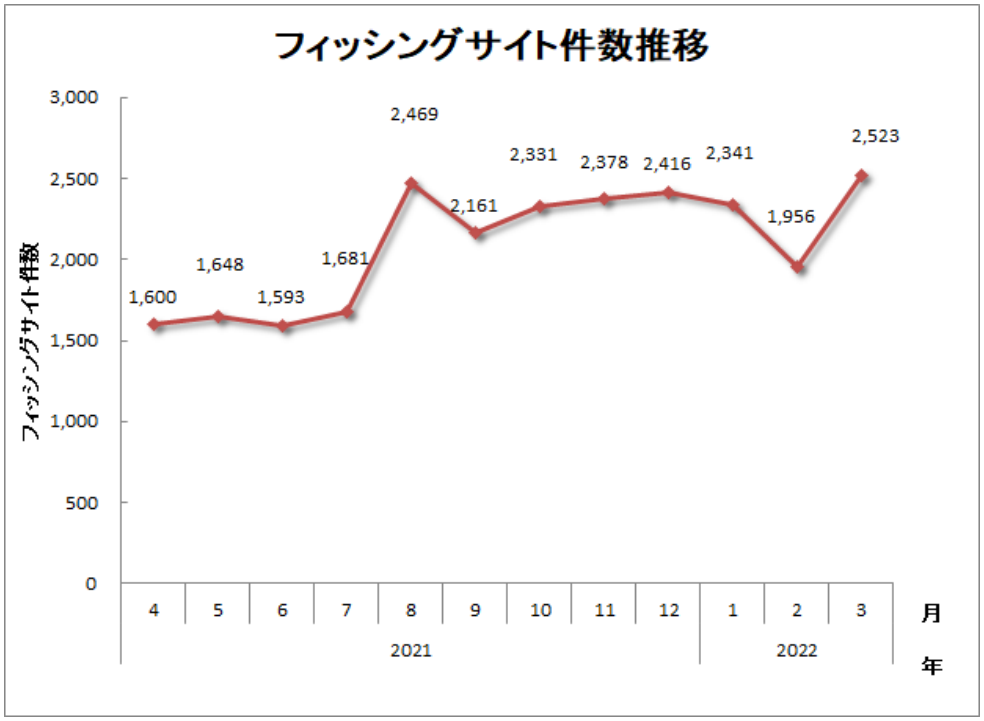
インシデント	1 月	2 月	3 月	合計	前四半期合計
フィッシングサイト	2,341	1,956	2,523	6,820	7,125
Web サイト改ざん	164	250	289	703	906
マルウェアサイト	104	80	107	291	406
スキャン	370	474	330	1,174	1,011
DoS/DDoS	0	1	6	7	16
制御システム関連	0	0	0	0	0
標的型攻撃	0	0	2	2	1
その他	104	129	139	372	342



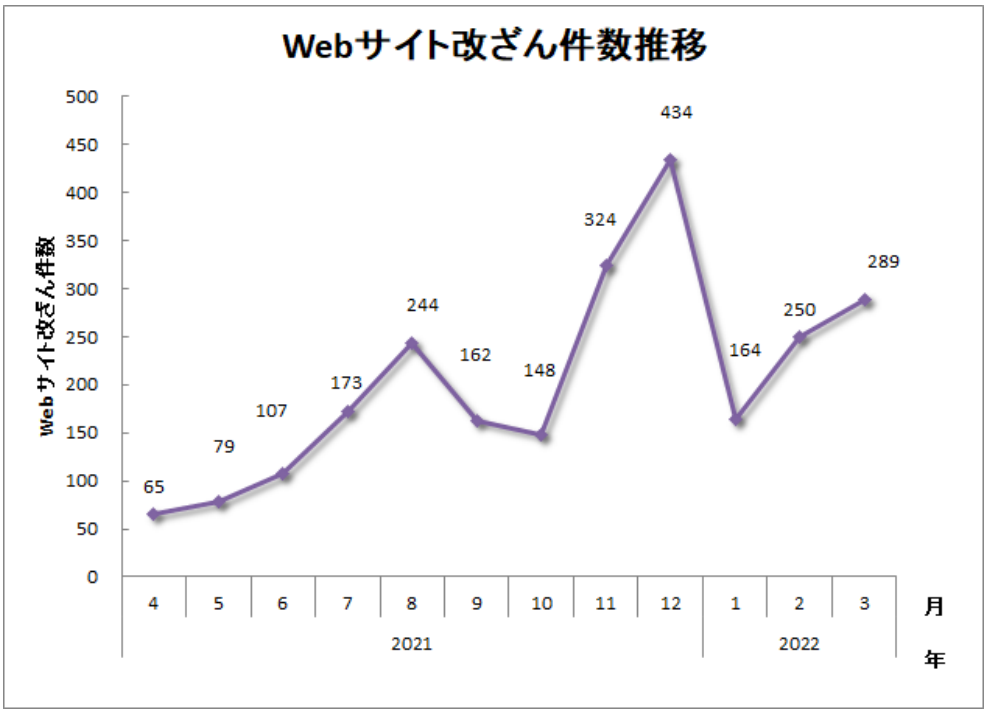
［図 5：報告を受けたインシデントのカテゴリー別割合］

フィッシングサイトに分類されるインシデントが 72.8%、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 12.5%を占めています。

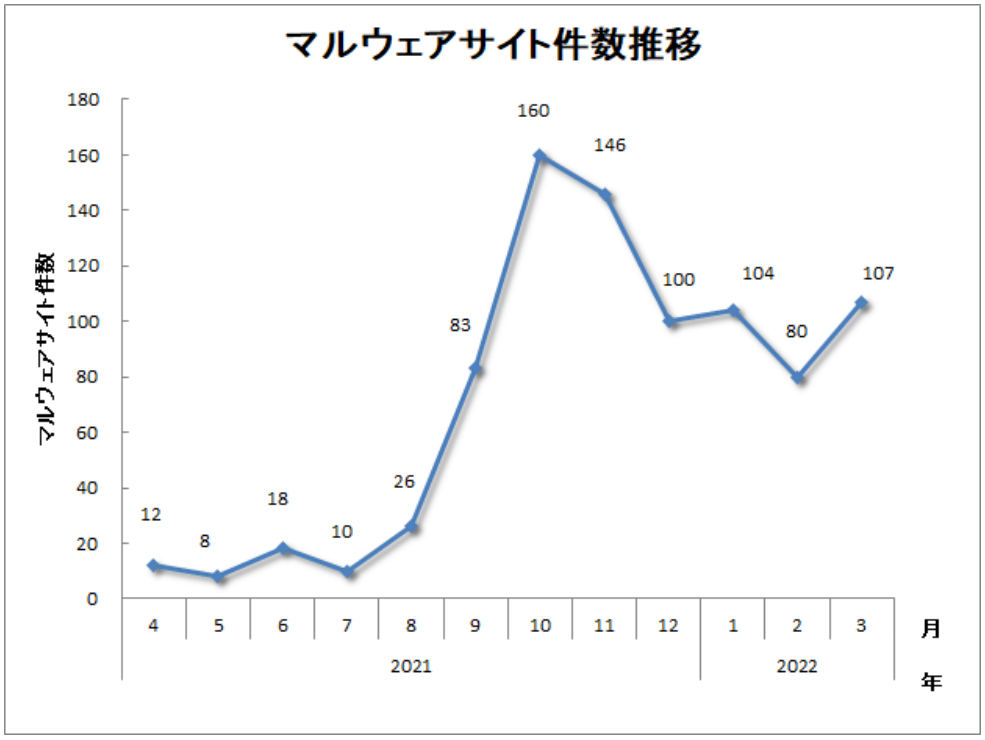
［図 6］から［図 9］に、フィッシングサイト、Web サイト改ざん、マルウェアサイト、スキャンのインシデントの過去 1 年間の月次の推移を示します。



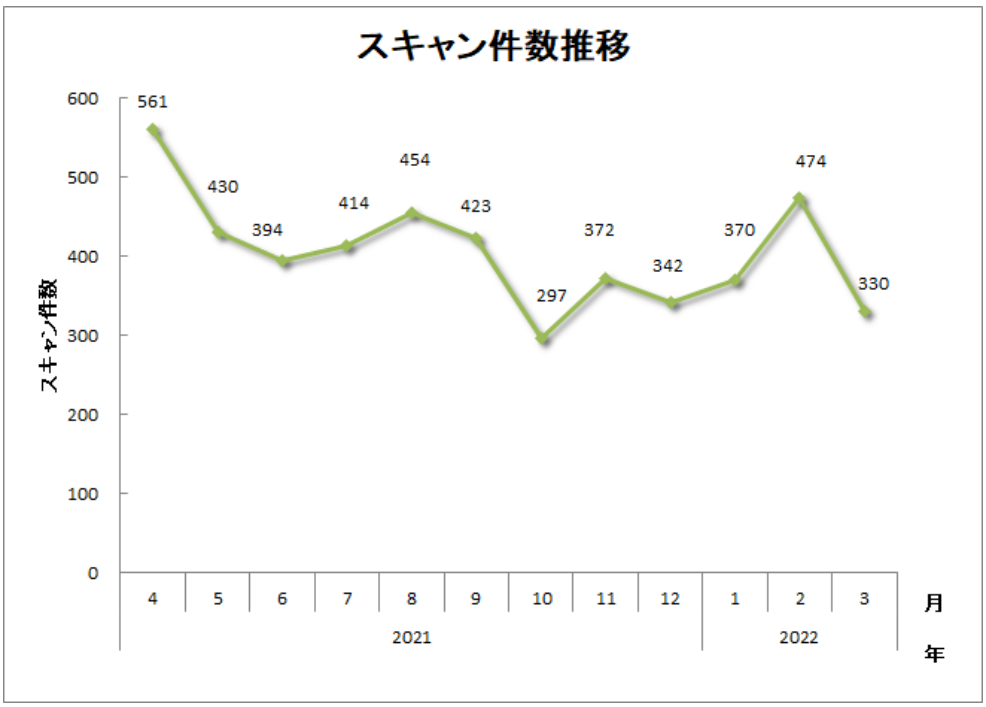
［図 6：フィッシングサイト件数の推移］



［図 7：Web サイト改ざん件数の推移］



［図 8：マルウェ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ー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ーごとの件数と調整・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

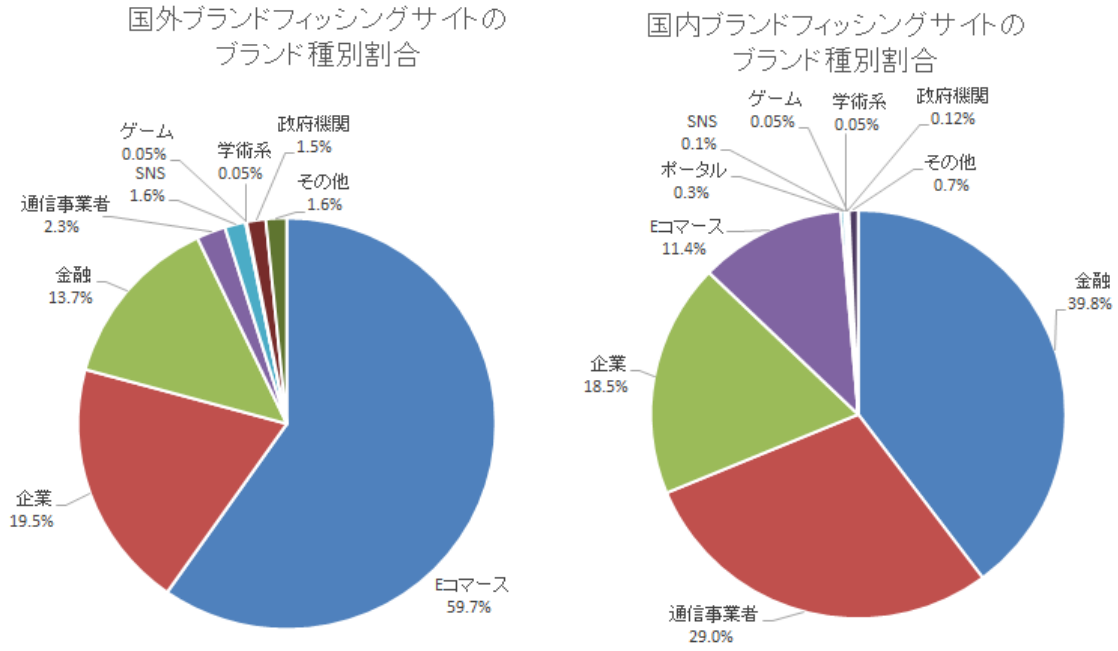
本四半期に報告が寄せられたフィッシングサイトの件数は 6,820 件で、前四半期の 7,125 件から 4%減少しました。また、前年度同期（4,831 件）との比較では、41%の増加となりました。

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 4,196 件となり、前四半期の 3,962 件から 6%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 2,043 件となり、前四半期の 2,406 件から 15%減少しました。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	1,427	1,022	1,747	4,196（62%）
国外ブランド	721	771	551	2,043（30%）
ブランド不明 (注 5)	193	163	225	581 （9%）
全ブランド合計	2,341	1,956	2,523	6,820

（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うち、国外ブランド関連の報告では E コマースサイトを装ったものが 59.7%、国内ブランド関連の報告では金融機関のサイトを装ったものが 39.8%で，それぞれ最も多くを占めました。

国内ブランドのフィッシングサイトでは、携帯キャリアのユーザーを狙ったフィッシングサイトが多くを占めました。また、前四半期に引き続き ETC の利用照会サービスや EC サイトの会員用ログインページを装ったフィッシングサイトも多く確認されました。
その他、JR 東日本が提供する Web サイト「えきねっと」を装ったフィッシングサイトの報告が 3 月に入ってから増加しました。

国外ブランドのフィッシングサイトについては、通販サイトのログインページを装ったものが半数以上占めており、ブランドや報告数は前四半期と大きな変化がありませんでした。

フィッシングサイトテイクダウンのために調整したサイトの割合は、国内が 62%、国外が 30%であり、前四半期（国内が 23%、国外が 77%）と比較し国内が増加しました。

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、703 件でした。前四半期の 906 件から 22%減少しています。

本四半期も、改ざんされた Web サイトから、不審な Web サイトへ転送される事例が複数報告されました。また、VirtualHost を使って複数の Web サイトが管理されているホスト上で、複数の Web サイトが同時に改ざんされる事象を確認しました。この改ざんは、1 つの Web サイトを改ざんしてから、次の手順で他の Web サイトにも改ざんを拡大する方法でなされた可能性があります。

改ざんの手順

1. CMS 等の脆弱性を利用し、最初の Web サイト改ざんを行い、WebShell を設置
2. WebShell を用いて、権限昇格を行うツールを設置した後にそれを起動して root 権限に昇格
3. root 権限で、同じホスト上にある複数の Web サイトを改ざん

同じホスト上に複数の Web サイトが存在している場合、1 つの Web サイト上のコンテンツに脆弱性が存在すると、同じホスト上にある別の Web サイトに対しても改ざんが行われる可能性があります。

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。
次に、確認されたインシデントを紹介します。

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

本四半期は、金融機関の社員を狙った標的型攻撃の報告が寄せられました。確認された手口では、標的の金融機関の社員に対して、乗っ取った暗号資産交換業者の社員の LinkedIn アカウントから、不正な ZIP ファイルを送信し、マルウェアを感染させようとするものでした。ZIP ファイルには不正な JavaScript をダウンロードして、実行するショートカットファイルが格納されていました。本攻撃は、弊センターのブログで公開した次の攻撃キャンペーンと類似しており、依然として攻撃活動が継続して行われていることがうかがえます。

JPCERT/CC Eyes「短縮 URL から VBScript をダウンロードさせるショートカットファイルを用いた攻撃」
https://blogs.jpcert.or.jp/ja/2019/07/shorten_url_lnk.html

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ェアサイトの数は 291 件でした。前四半期の 406 件から 28%減少しています。

本四半期に報告が寄せられたスキャン件数は 1,174 件でした。前四半期の 1,011 件から 16%増加しています。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）、Telnet （23/TCP）、143/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	102	136	119	357
23/tcp	51	186	81	318
143/tcp	112	71	51	234
80/tcp	53	29	35	117
37215/tcp	13	48	30	91
25/tcp	12	9	15	36
52869/tcp	4	15	2	21
2323/tcp	9	4	5	18
443/tcp	3	5	0	8
21/tcp	3	3	1	7
6379/tcp	3	1	2	6
3389/tcp	3	0	1	4
3306/tcp	3	0	1	4
5555/tcp	1	2	0	3
445/tcp	0	3	0	3
8081/tcp	2	0	0	2
1433/tcp	1	1	0	2
110/tcp	2	0	0	2
9443/tcp	1	0	0	1
その他	9	5	3	17
月別合計	387	518	346	1251

その他に分類されるインシデントの件数は、372 件でした。前四半期の 342 件から 9%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) 侵入型ランサムウェア攻撃に関する報告への対応

本四半期は、侵入型ランサムウェア攻撃に関する報告を複数受けました。JPCERT/CC では、報告者から被害範囲や調査状況、報告時点の対応状況などをヒアリングし、得られた情報もとに、関連するランサムウェア種別攻撃を特定し、侵入手口などの情報を対策に利用できるように提供して、対応方針をアドバイスしています。SSL-VPN 製品の脆弱性や Log4j の脆弱性を悪用して侵入されたと推定されるケースを多く確認しています。報告された侵入型ランサムウェア攻撃を行う攻撃グループとして FiveHands、Pandra、Robinhood などを確認しています。

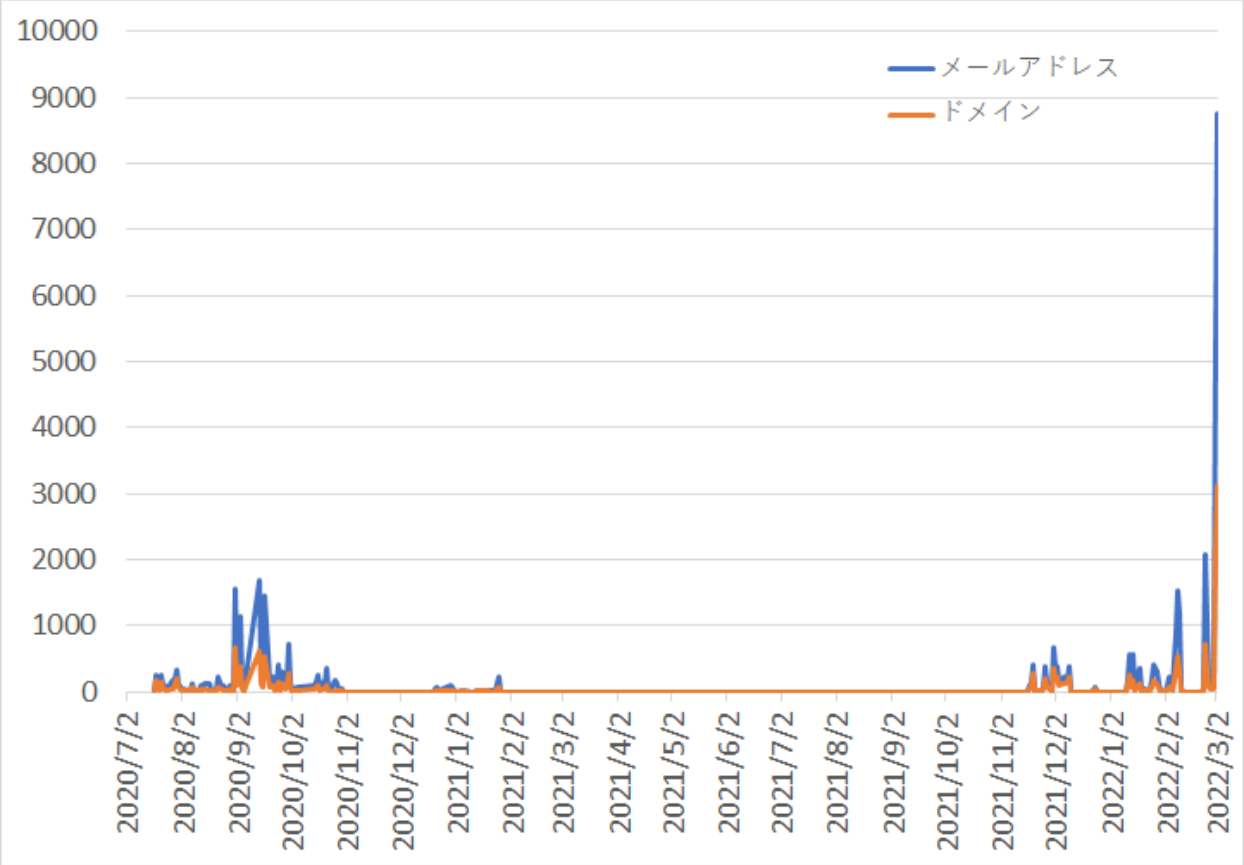
これらの対応から得られた知見を、インシデント対応の初動対応を中心にまとめ、「侵入型ランサムウェア攻撃を受けたら読む FAQ」として公開するとともに、侵入型ランサムウェア攻撃の初動対応のポイントを動画にして公開しました。

侵入型ランサムウェア攻撃を受けたら読む FAQ
https://www.jpcert.or.jp/magazine/security/ransom-faq.html

侵入型ランサムウェア攻撃の初動対応のポイント（YouTube）
https://www.youtube.com/watch?v=nDOSn_ss7zI

(2) マルウェア Emotet に関する報告への対応

本四半期は、引き続き Emotet に関する報告を多数受けました。特に 2 月以降、国内の感染端末数とともに報告数が増加しました。［図 12］に JPCET/CC に情報提供された国内の Emotet 感染端末数の推移を示します。



［図 12：日本の Emotet に感染している端末および組織数の推移］

この国内での感染拡大を受けて、次の注意喚起を発行し、また、Emotet の概要と感染確認方法を解説した動画を公開しました。

マルウェア Emotet の感染再拡大に関する注意喚起
https://www.jpcert.or.jp/at/2022/at220006.html

日本中で感染が広がるマルウェア Emotet （YouTube）
https://www.youtube.com/watch?v=wvu9sWiB2_U

Emotet 感染の確認方法と対策 （YouTube）
https://www.youtube.com/watch?v=nqxikr1x2ag

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、攻撃元や情報発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ェアによって、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。

- 攻撃者やマルウェ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

○ マルウェアサイト

「マルウェアサイト」とは、閲覧することで PC がマルウェ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ェアを公開しているサイトを指します。

JPCERT/CC では、以下を「マルウェアサイト」に分類しています。

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

○ スキャン

「スキャン」とは、サーバーや 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、マルウェ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）
- マルウェア（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ーや 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ー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ェアが通信を行うサーバー
- 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、マルウェ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、マルウェ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、マルウェ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ェアが通信を行うサーバー

○ 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ェアによる情報の窃取
- マルウェア（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、「令和３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。