JPCERT-IR-2012-01

発行日: 2012-04-12

JPCERT/CC インシデント報告対応レポート
[2012 年 1 月 1 日 ～ 2012 年 3 月 31 日]

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」といいます。）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」といいます。）の報告を受け付けています(注 1)。本レポートでは、2012 年 1 月 1 日から 2012 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及び事例について紹介します。

> 【注 1】「コンピュータセキュリティインシデント」とは、本稿では、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、できごとの全般をいいます。

JPCERT/CC は、国際的な調整・支援が必要となるインシデントについて、日本の窓口組織として、国内や国外（海外の CSIRT など）の関係機関との調整活動を行っています。この活動を通じて、各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しています。

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)	837	812	1050	2699	2501
インシデント件数 （注 3）	790	731	1014	2535	2339
調整件数（注 4）	205	237	312	754	752

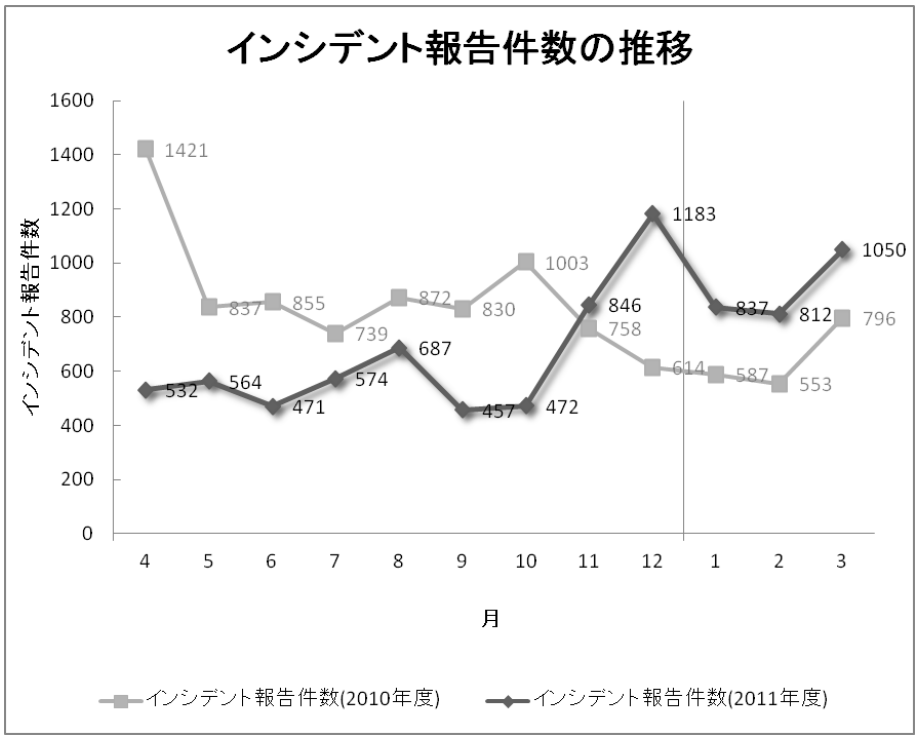
【注 2】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

【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。ただし、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は、1 件のインシデントとして扱います。

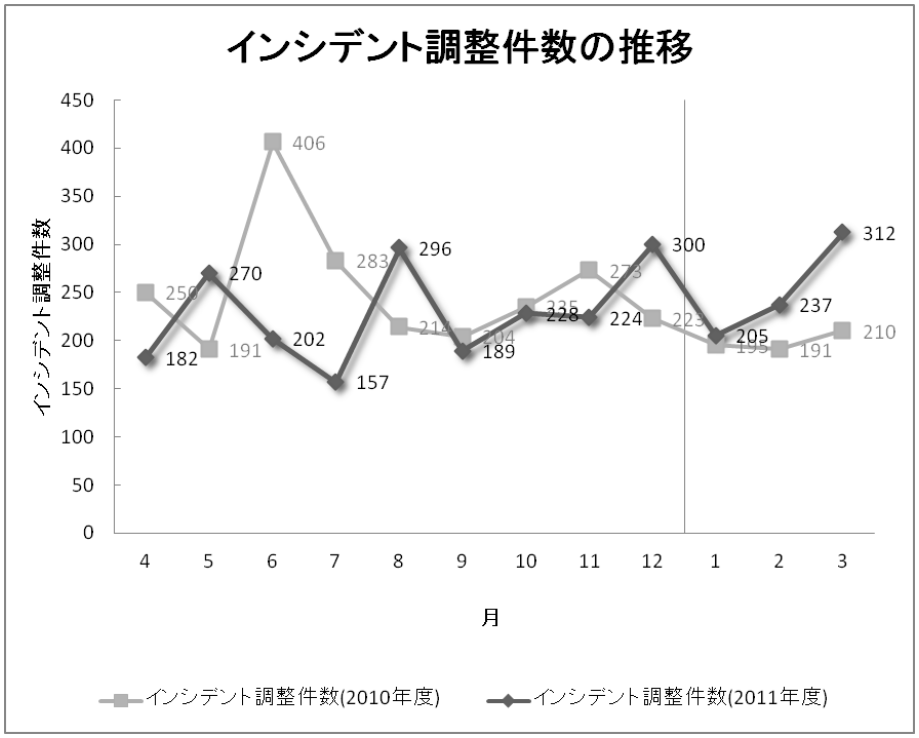
【注 4】「調整件数」とは、インシデントの拡大防止のため、サイトの管理者などに対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、2699 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 754 件でした。前四半期と比較して、総報告件数は 8%増加し、調整件数は 0.3%増加しました。また、前年同期と比較すると、総報告数で 39%増加し、調整件数は 26%増加しました。

[図 1]～[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]

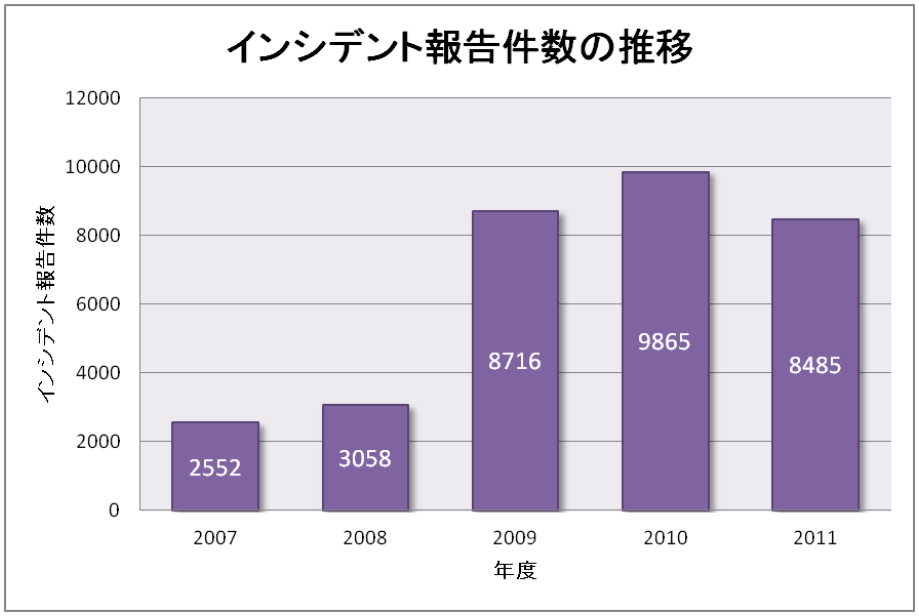
【参考】統計情報の年度比較

2011 年度を含む過去 5 年間の報告件数を表 2 に示します。なお、年度の期間は、当該年の 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	2007	2008	2009	2010	2011
報告件数	2552	3058	8716	9865	8485

2011 年度に寄せられた報告件数は 8485 件でした。前年度の 9865 件と比較して、14%減少しています。 [図 3]に過去 5 年間の年間報告件数の推移を示します。



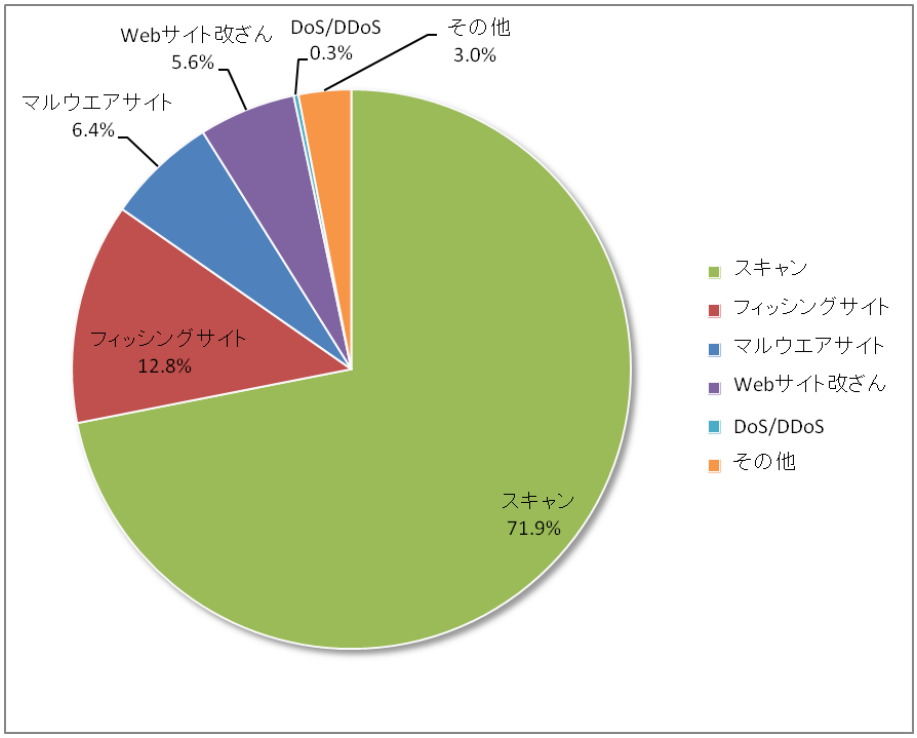
[図 3: インシデント報告件数の推移（年度比較）]

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。本四半期に報告を受けた各カテゴリのインシデント件数を [表 3]に示します。

[表 3 カテゴリ別インシデント件数]

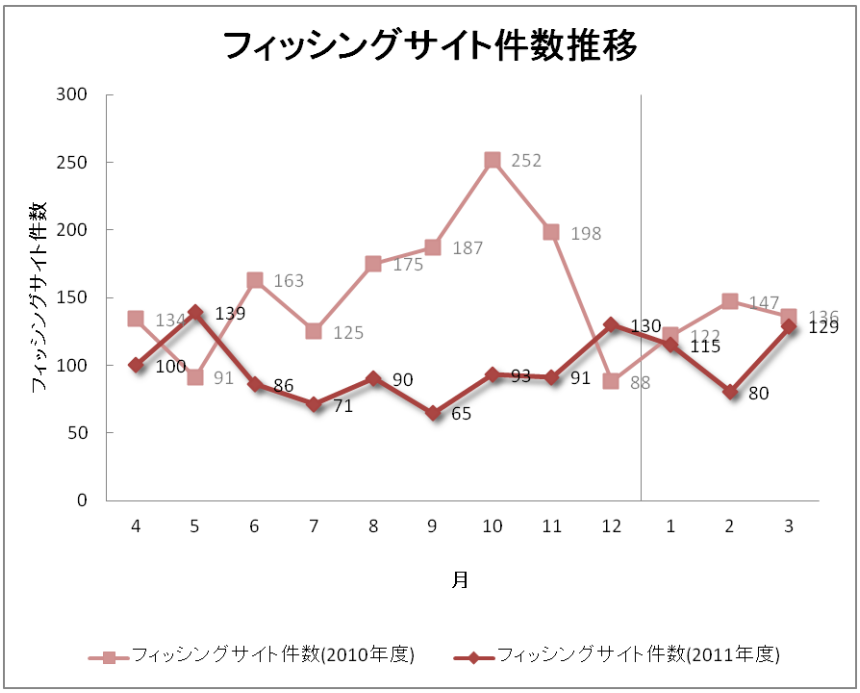
インシデントカテゴリ	1 月	2 月	3 月	合計	前四半期合計
フィッシングサイト	115	80	129	324	314
Web サイト改ざん	22	80	40	142	164
マルウエアサイト	50	50	62	162	131
スキャン	593	504	726	1823	1624
DoS/DDoS	0	1	6	7	1
その他	10	16	51	77	105

本四半期に発生したインシデントにおける各カテゴリの割合は、[図 4]のとおりです。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は 71.9%と大きな割合を占めています。フィッシングサイトに分類されるインシデントが 12.8%を占めています。また、Web サイト改ざんに分類されるインシデントは 5.6%でした。

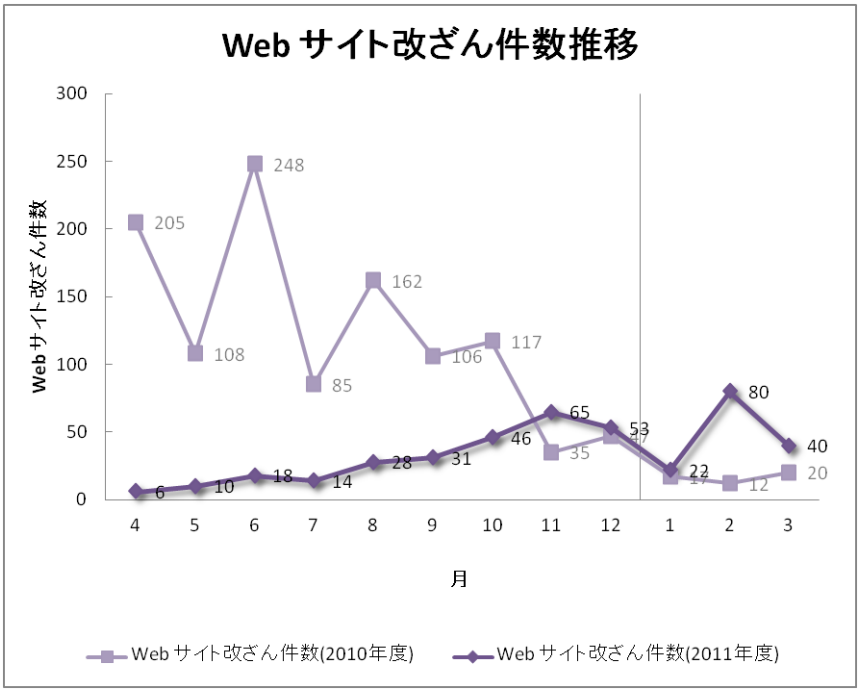


[図 4 インシデントのカテゴリ別割合]

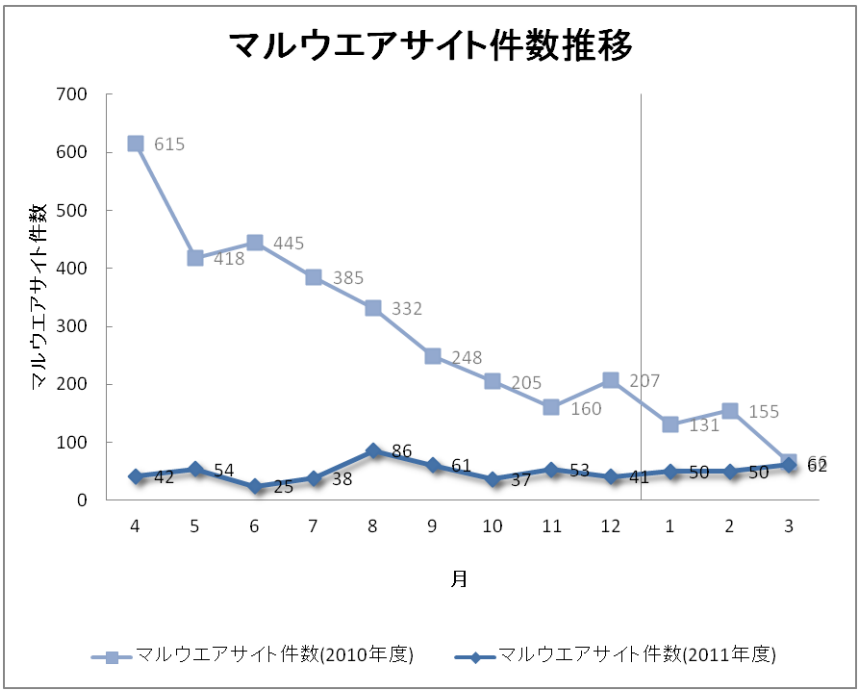
[図 5]から[図 8]に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



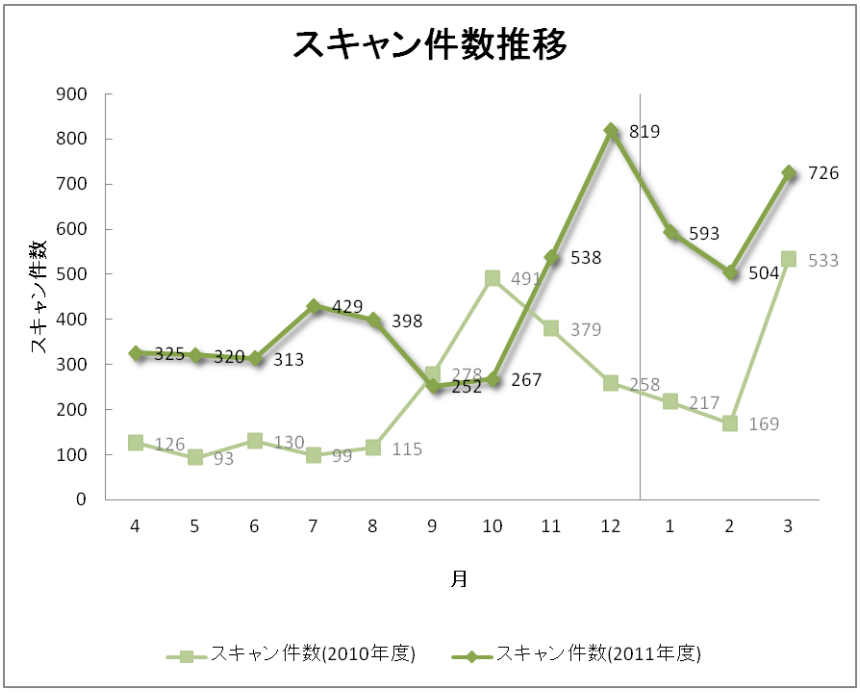
[図 5 フィッシングサイト件数推移]



[図 6 Web サイト改ざん件数推移]

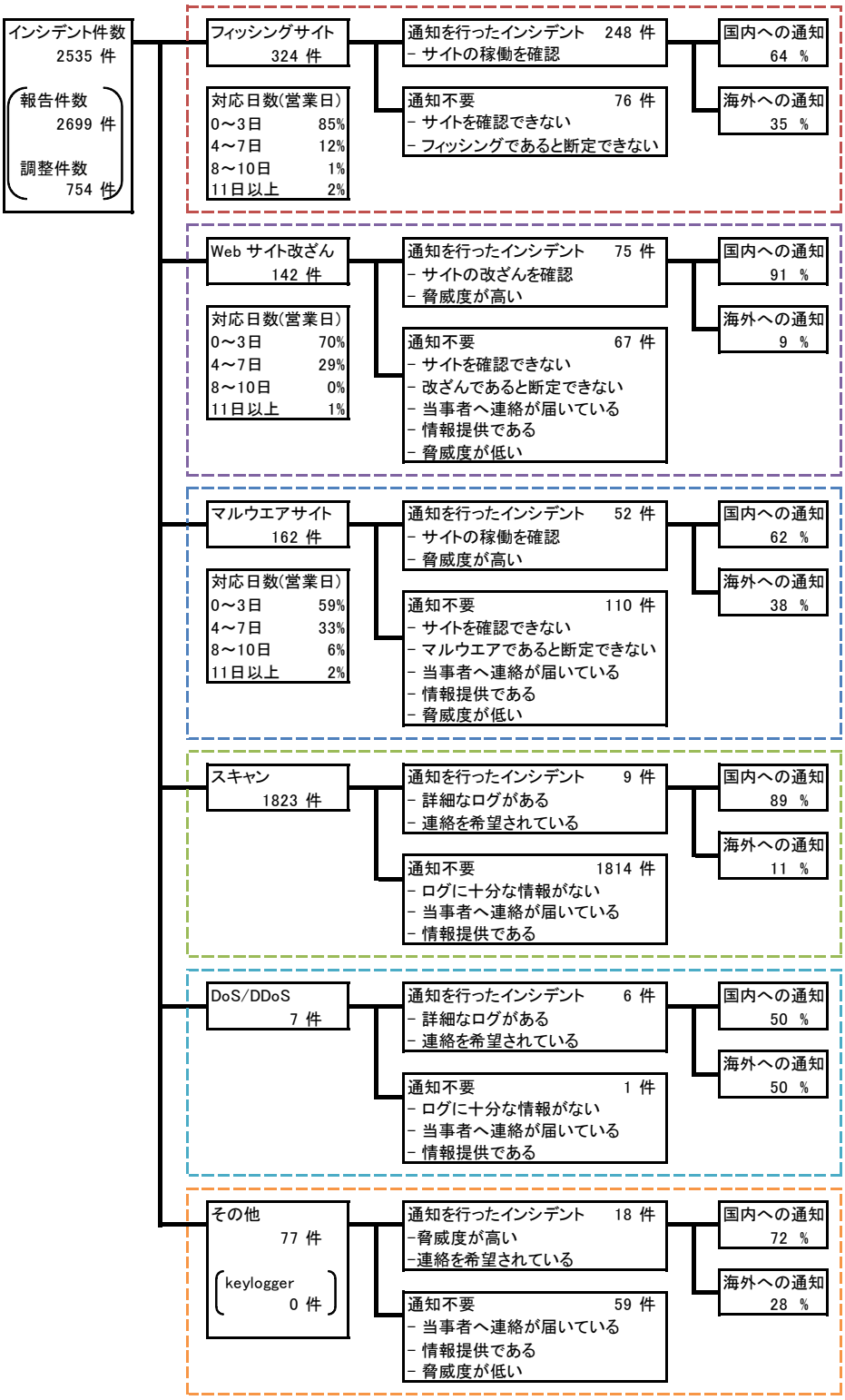


[図 7 マルウエアサイト件数推移]



[図 8 スキャン件数推移]

[図 9] にインシデントにおける調整・対応状況の内訳を示します。



[図 9 インシデントにおける調整・対応状況]

3. インシデントの傾向

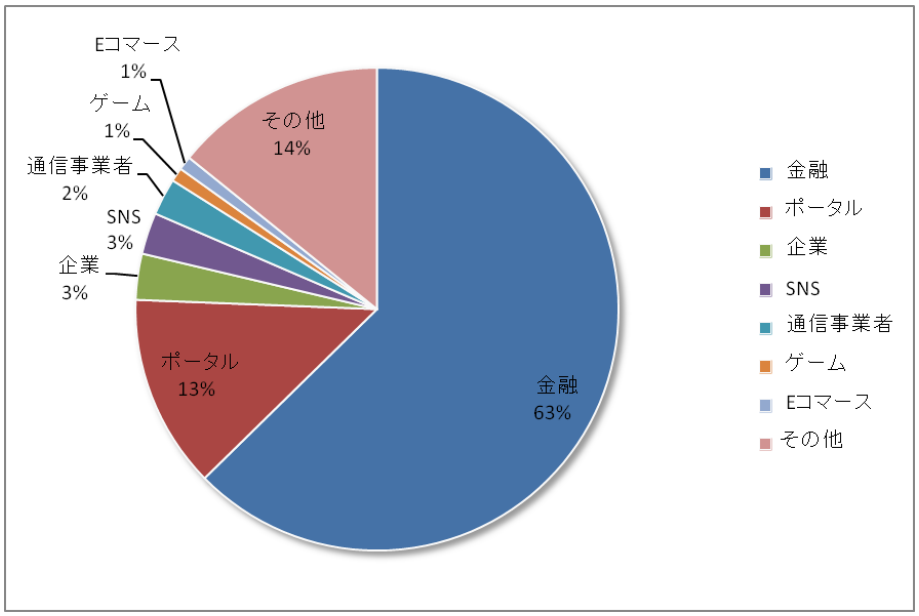
本章で説明する各インシデントの定義については、6.[付録]インシデントの分類を参照してください。

本四半期に報告が寄せられたフィッシングサイトの件数は 324 件で、前四半期の 314 件から 3%増加しました。また、前年度同期（405 件）との比較では、20%の減少となりました。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 4]、業界割合を[図 10]に示します。

[表 4 フィッシングサイトの国内・国外ブランド別の件数]

フィッシングサイト	1 月	2 月	3 月	国内外別合計（割合）
国内ブランド	30	7	21	58(18%)
国外ブランド	72	55	94	221(68%)
ブランド不明（注 5）	13	18	14	45(14%)
月別合計	115	80	129	324(100%)

【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などの理由により、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 10 フィッシングサイトのブランド種別割合]

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 58 件と、前四半期の 65 件から 11%減少しました。国外ブランドを装ったフィッシングサイトの件数は 221 件と、前四半期の 198 件から 12%増加しました。

本四半期に確認された、国内の SNS やオンラインゲームを装った複数のフィッシングサイトは、正規サイトの画像や Flash などのコンテンツを直接参照していて、見た目には正規サイトとまったく変わらないものでした。見分ける手立てはアドレス・バーに表示される URL しかありません。

WordPress で構築されたサイトについては、前四半期は改ざんされるインシデントが多くありましたが、本四半期はフィッシングサイトが設置された事例を多数確認しています。

JPCERT/CC で報告を受領したフィッシングサイトについては、金融機関のサイトを装ったものが 63%、ポータルサイトを装ったものが 13%を占めています。
国内金融機関を装ったフィッシングの報告は、昨年から続いており、3 月に報告を受領したフィッシングサイトでは、前四半期にも見られたダイナミック DNS サービスのドメインを使用していました。また、複数の国内 ISP の Web メールサービスを装ったフィッシングサイトも、前四半期に引き続き確認しています。

フィッシングサイトの調整先の割合は、国内が 64%、国外が 35%と、前四半期の割合（国内 62%、国外 38%）と比較して、国内への調整が増えました。

本四半期に報告が寄せられた Web サイト改ざんの件数は、142 件でした。前四半期の 164 件から 13%減少しています。

本四半期には、オンラインゲームの RMT (Real Money Trading: オンラインゲーム内のアイテムや通貨などを、現金で取引する行為) サイトなどへのリンクを埋め込む Web ページの改ざんの報告を受領しました。報告をもとに調査したところ、同様のリンクを埋め込む改ざん事例を国内で多数確認しました。これは、リンクが埋め込まれたサイトを大量に作り出すことで、RMT サイトの検索エンジンにおけるランキングを上昇させる、検索エンジン用の最適化 (SEO: Search Engine Optimization) を目的とした改ざんであると考えられます。

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、162 件でした。前四半期の 131 件から 24%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、1823 件でした。前四半期の 1624 件から 12%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 5]に示します。

[表 5　ポート別のスキャン件数]

ポート	1 月	2 月	3 月	合計
80/tcp	366	335	511	1212
25/tcp	122	69	122	313
22/tcp	91	90	75	256
5060/udp	4	0	0	4
443/tcp	2	1	1	4
23/tcp	2	2	0	4
143/tcp	0	0	4	4
110/tcp	1	0	3	4
/udp	3	1	0	4
8080/tcp	0	1	1	2
3389/tcp	1	1	0	2
21/tcp	0	1	1	2
17525/udp	0	0	2	2
80/udp	0	1	0	1
22/udp	0	1	0	1
/icmp	0	1	0	1
不明	4	3	5	12
月別合計	596	507	725	1828

スキャンの対象となったポートは、上位から http(80/tcp)、smtp(25/tcp)、ssh(22/tcp) の順でした。

4. インシデント対応事例

以下に、本四半期に行った対応の例を紹介します。

【コードサイニング証明書を使用したマルウエア】
JPCERT/CC では、コードサイニング証明書添付で署名された不審なソフトウエアに関する報告を受領しました。当該ソフトウエアは、標的型攻撃メールに添付されたドキュメントファイルを開いたときに Microsoft Office の脆弱性(MS10-087)を悪用して生成、実行されるもので、詳細な分析の結果、起動時における外部への通信などの不審な挙動を確認しています。JPCERT/CC では、証明書の発行元組織に対し、当該証明書の取り扱いに関し適切な対応を依頼しました。その後、証明書の発行元組織によって当該証明書が失効されたことを確認しました。

【DNS Changer に関する対応】
JPCERT/CC では、海外のセキュリティ対策組織より「PC の DNS 設定を書き換えるマルウエア(以下、DNS Changer *1)」に感染した国内の PC の情報提供を受けました。入手した情報を精査した結果、国内でも相当数の PC が DNS Changer に感染していた事に加え、DNS Changer によって書き換えられた DNS 設定上の DNS サーバが 2012 年 3 月 9 日に運用を停止する*2 ことから、個別に国内通信事業者に向けて感染 PC に関する情報提供を行うとともに、広く注意喚起を行いました。

*1)DNS Changer は、PC の DNS 設定を攻撃者が用意した不正な DNS サーバに変更することで、Web サイトを閲覧した際に別のサイトを表示させます。この不正な DNS サーバは、2011 年 11 月米国連邦捜査局(FBI)によって差し押さえられ、暫定的に正常な DNS サーバに置き換えらました。
*2)暫定的に置き換えられた DNS サーバの運用は、その後 4 ヶ月延長される事となりました。

【国内ボットを含む転送サイトを使用したマルウエアの配布】
JPCERT/CC では、サイトを閲覧した PC をマルウエア配布サイトに誘導することを目的とした複数の fast-flux 攻撃*3 の報告を受領しました。fast-flux 攻撃に使用されたドメインには、ユニークな IP アドレスが常に数千個割り当てられており、使用された IP アドレスには国内のものも多く含まれていました。JPCERT/CC では、fast-flux 攻撃に使用されたドメイン登録者に通知するとともに、最終的に転送されるマルウエア配布サイトの IP アドレス管理者に対応を依頼し、ドメインの停止とマルウエア配布サイトが停止したことを確認しました。

*3)fast-flux は、フィッシングサイトなどに使用される攻撃手法で、攻撃用ドメインに対して生存時間(TTL)を短くした IP アドレスを多量に割り当てることで、攻撃用ドメインの名前解決を行った際に返される IP アドレスを都度異なるようにして、テイクダウンに対抗しフィッシングサイトを延命化する手法です。

5. 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 URL 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/

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 URL 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おります。購読をご希望の方は、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、以下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など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など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などのサイトに似せた 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。

- Gumblar ウイルスによる不審なスクリプト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 など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など) 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無いもの) を指します。また、マルウエアなど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など)
- 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、ワームなど）による感染の試み (未遂に終わったもの)
- ssh,ftp,telnet など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など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。

- 大量の通信などにより、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 メールなど) を受信させることによるサービス妨害

○ その他

「その他」とは、上記に含まれないインシデントを指します。

JPCERT/CC では、たとえば、以下を「その他」に分類しています。

- 脆弱性などをついたシステムへの不正侵入
- ssh,ftp,telnet など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、ワームなど) の感染

本活動は、経済産業省より委託を受け、「平成２３年度コンピュータセキュリティ早期警戒体制の整備（不正アクセス行為等対策業務）」事業として実施したものです。