JPCERT-IR-2011-0002
発行日: 2011-04-12

JPCERT/CC インシデント報告対応レポート
[2011 年 1 月 1 日 ～ 2011 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、2011 年 1 月 1 日から 2011 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、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）	587	553	796	1936	2375
インシデント件数 （注 3）	542	522	819	1883	2638
調整件数（注 4）	195	191	210	596	731

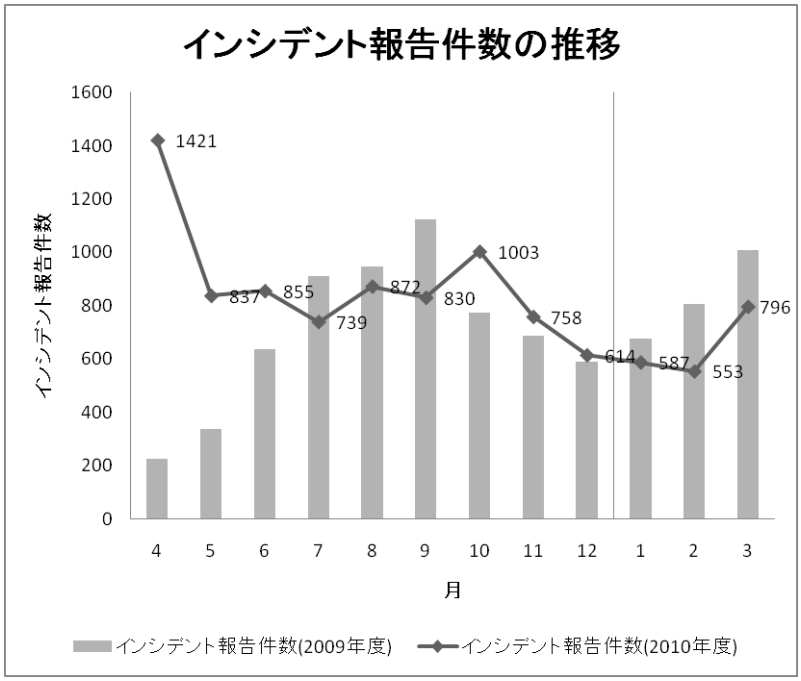
【注 2】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

【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。

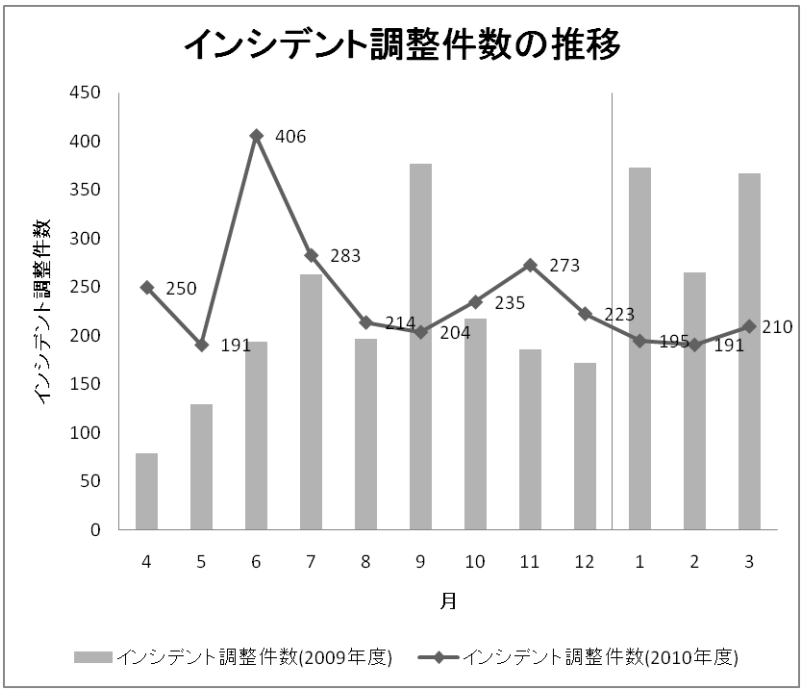
【注 4】「調整件数」とは、インシデントの拡大防止のため、サイトの管理者などに対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、1936 件でした。また、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 596 件でした。前四半期の 731 件と比較して、18%減少しています。

[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]

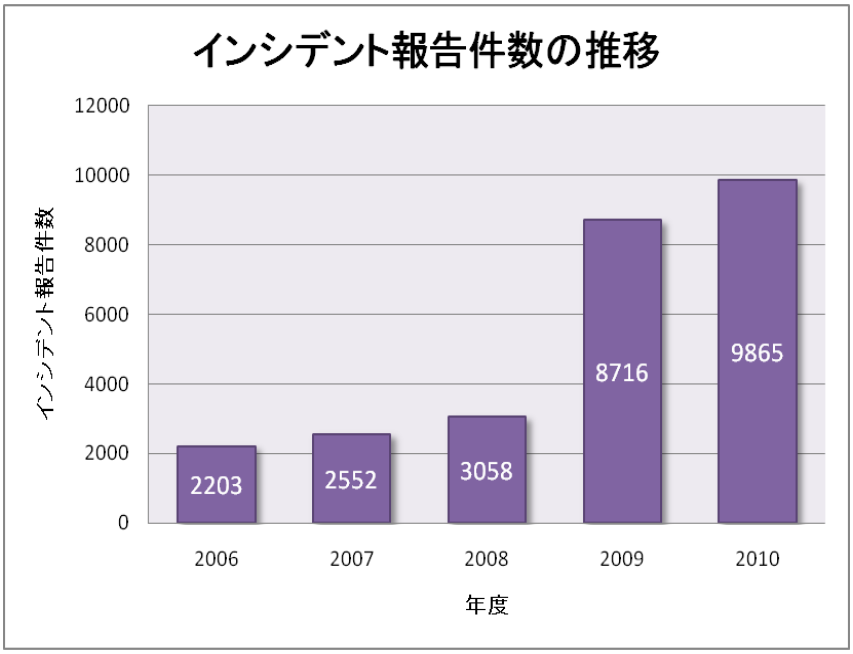
【参考】統計情報の年度比較

2010 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	2006	2007	2008	2009	2010
報告件数	2203	2552	3058	8716	9865

2010 年度に寄せられた報告件数は 9865 件でした。前年度の 8716 件と比較して、13 % 増加しています。本四半期の報告件数は減少傾向にありますが、年間の報告件数は前年度から増加となりました。[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）]

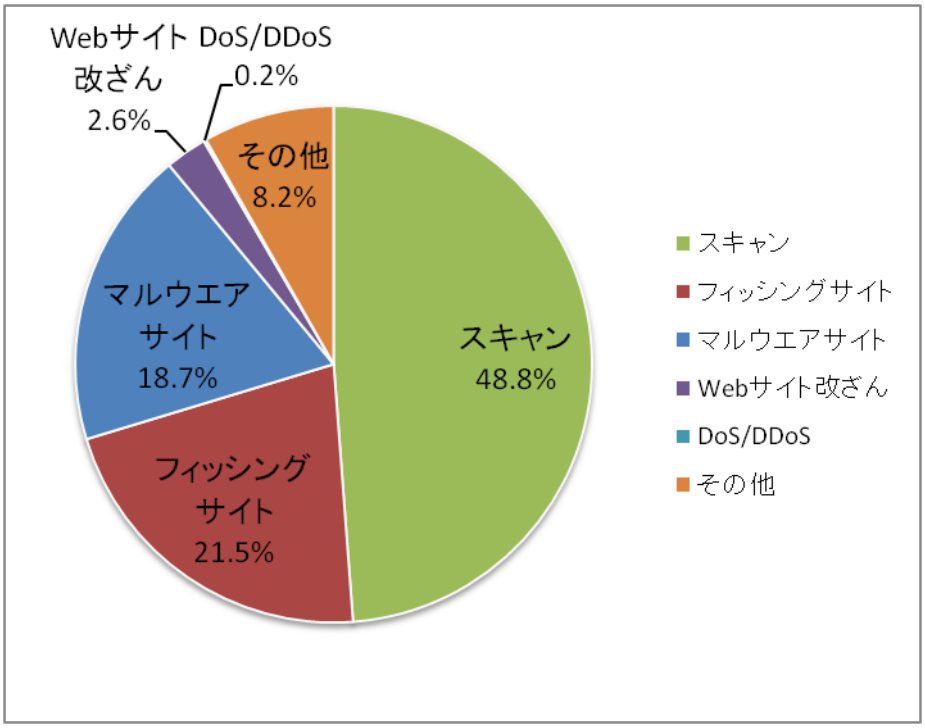
JPCERT/CC では報告を受けたインシデントをタイプ別に分類し、各インシデントタイプに応じた調整、対応を実施しています。本四半期に発生したインシデントのタイプ別件数を[表 3]に示します。

[表 3: タイプ別インシデント件数]

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	122	147	136	405	538
Web サイト改ざん	17	12	20	49	199
マルウエアサイト	131	155	66	352	572
スキャン	217	169	533	919	1128
DoS/DDoS	0	3	0	3	4
その他	55	36	64	155	197

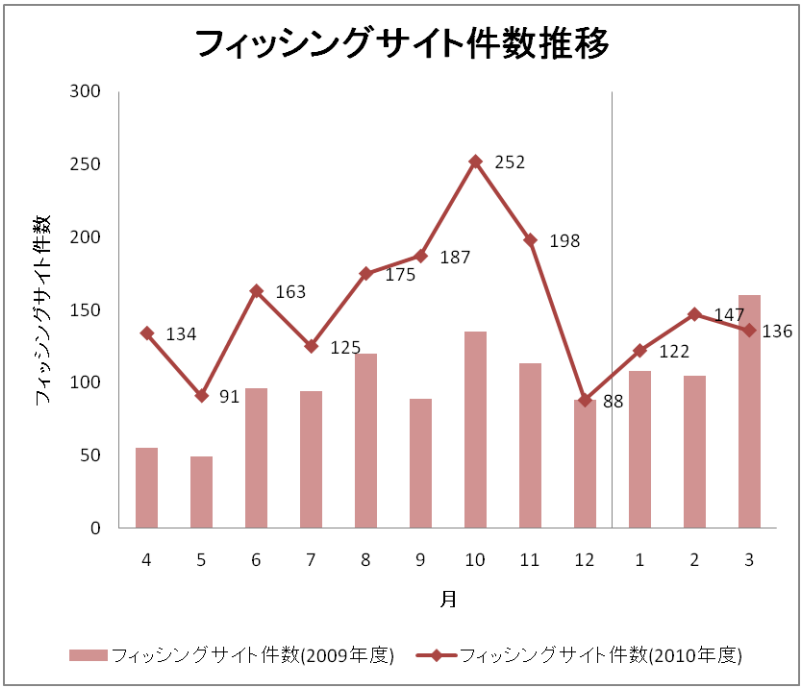
本四半期に発生したインシデントのタイプ別割合は、[図 4]のとおりです。システムの弱点を探索するスキャンに分類されるインシデントは 48.8%と大きな割合を占めています。フィッシングサイトに分類されるインシデントが 21.5%を占めています。また、Web サイト

改ざんに分類されるインシデントは 2.6%でした。
本四半期の DDoS に関する報告件数は 3 件でした。このうち、1 件は攻撃に国内のホストが関係するものであったため、JPCERT/CC では、攻撃に使用されたホストの管理者に通知を行い、対応を依頼しました。

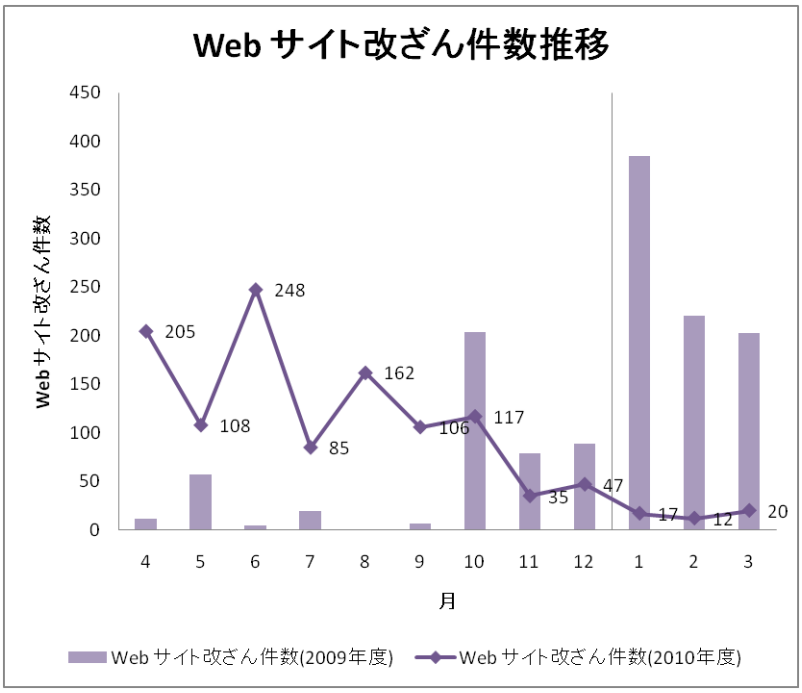


[図 4: インシデントのタイプ別割合]

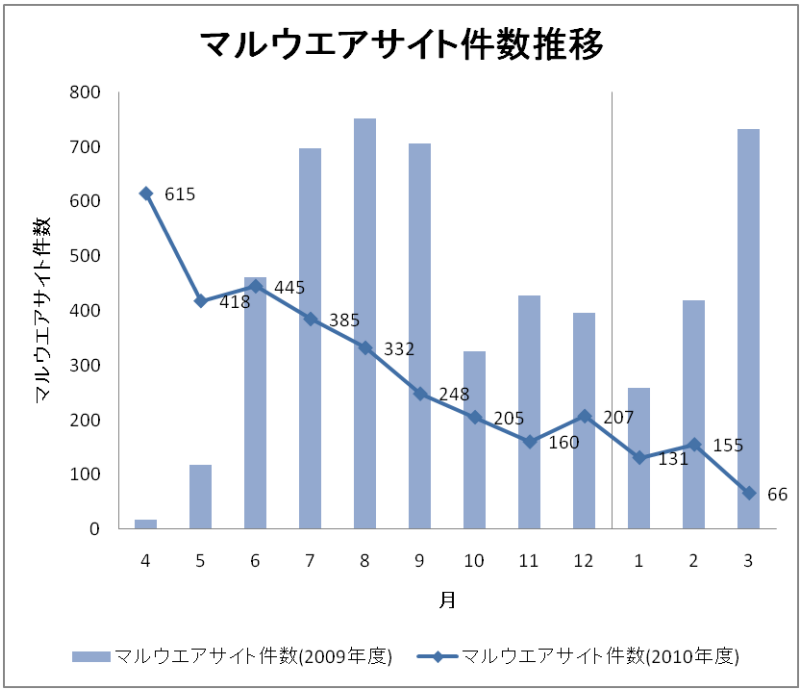
[図 5]から[図 8]に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



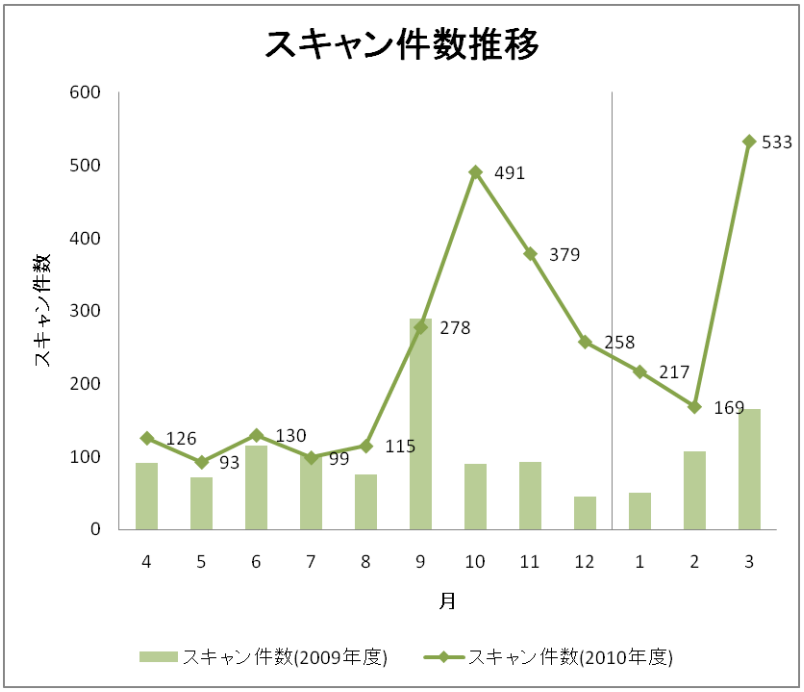
[図 5: フィッシングサイト件数推移]



[図 6: Web サイト改ざん件数推移]

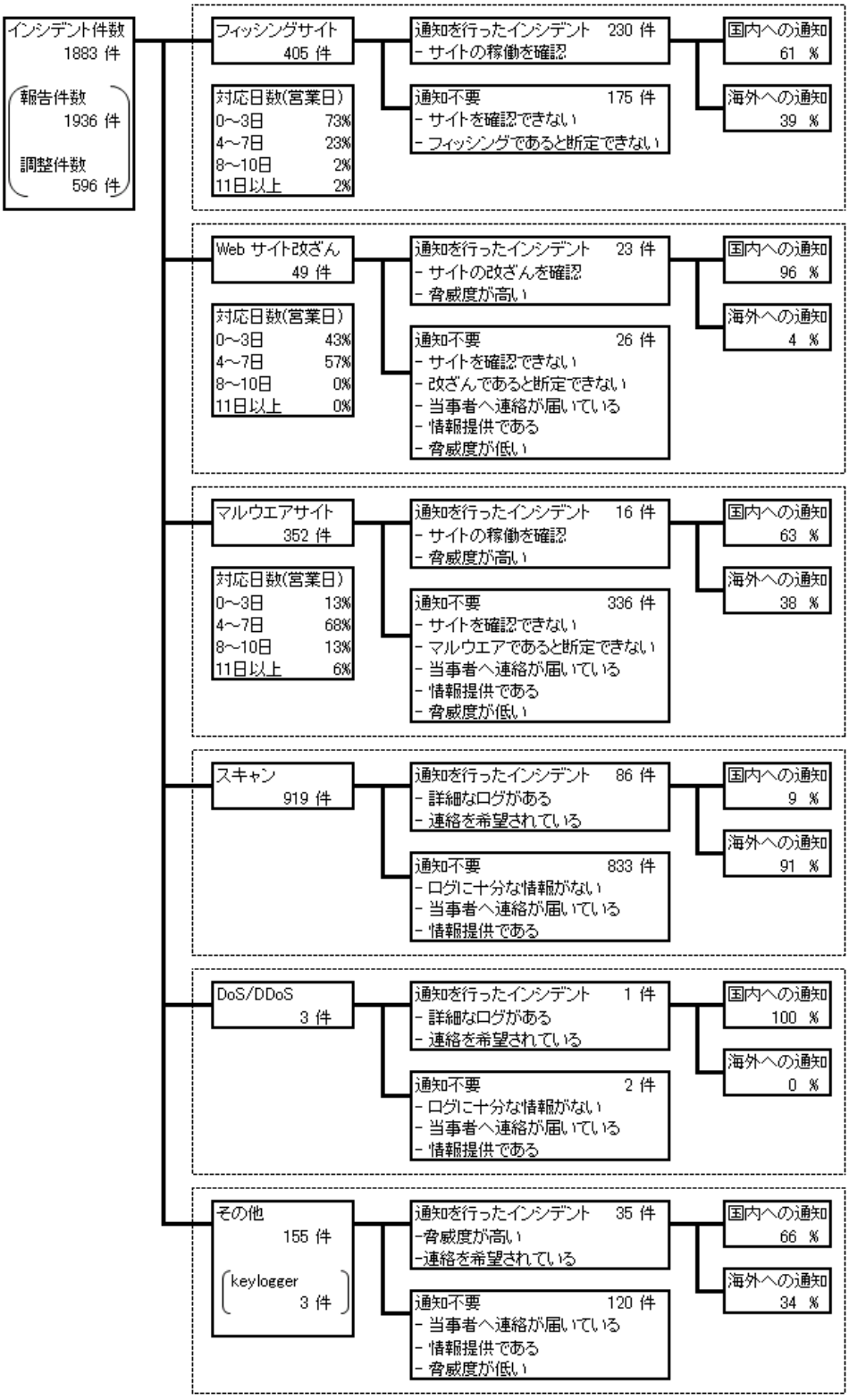


[図 **7**: マルウエアサイト件数推移]



[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。

本四半期に報告を頂いたフィッシングサイトの件数は、405 件で、前四半期の 538 件から 25%減少しました。また、前年度同四半期（373 件）との比較では、9%の増加となっています。
本四半期のフィッシングサイトが装っていたブランドの国内・国外別の内訳を[表 4] 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	24	29	31	84(21%)
国外ブランド	77	94	76	247(61%)
ブランド不明	21	24	29	74(18%)
月別合計	122	147	136	405(100%)

本四半期は、前四半期のような、特定の国内ブランドのフィッシングサイトに関する報告が多数寄せられるという状況ではなく、様々な国外ブランドのフィッシングサイトに関する報告が多数寄せられたため、国外ブランドを装ったフィッシングサイトの件数が 247 件と、前四半期の 202 件から 22 % 増加した一方で、国内のブランドを装ったフィッシングサイトの件数は、84 件と、前四半期の 284 件から大幅に減少しました。

本四半期のフィッシングサイトの調整先は、国内が 61%、国外が 39%でした。前四半期の割合（国内 53%、国外 47%）と比較して、本四半期は国内への調整が増えました。これは、前述の様々な国外ブランドのフィッシングサイトの多くが国内に設置されていたためです。

本四半期に報告が寄せられた Web サイト改ざんの件数は、49 件でした。前四半期の 199 件から 75%減少しています。これは、いわゆる Gumblar による Web サイト改ざんに関する報告が、11 月頃から減少したためです。いわゆる Gumblar の報告減少については、前四半期に引き続き一部の亜種の攻撃がおさまってきていることや、世間での注目度が下がっていることが一因になっていると考えられます。
いわゆる Gumblar については、報告件数は減少傾向にありますが、前四半期にあった Internet Explorer の未修正の脆弱性(現在は修正済み)を悪用した攻撃や、Java の脆弱性を

悪用するような脅威度の高い攻撃が引き続き発生する可能性があるため、JPCERT/CC では、攻撃の分析や動向調査を継続しています。

本四半期に報告をいただいたマルウエアサイトの件数は、352 件でした。前四半期の 572 件から 28%減少しています。これは、マレーシアのセキュリティ対応機関から定常的に寄せられていた報告が減少したためです。

本四半期に報告が寄せられたスキャンの件数は、919 件でした。前四半期の 1128 件から 19%減少しています。これも、マレーシアのセキュリティ対応機関からのスキャンに関する報告が減少していることによるものです。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	109	72	450	631
22/tcp	42	26	37	105
25/tcp	18	26	20	64
icmp	23	17	12	52
445/tcp	11	16	4	31
21/tcp	4	3	2	9
110/tcp	1	1	1	3
5900/tcp	1	0	1	2
61756/udp	1	0	0	1
4899/tcp	1	0	0	1
143/tcp	0	1	0	1
不明	9	12	6	27
月別合計	220	174	533	927

スキャンの対象となったポートは、http(80/tcp)、ssh(22/tcp)、smtp(25/tcp)の順に多く確認しています。http に対するスキャンでは、Web アプリケーションの脆弱性への攻撃を試みる RFI(リモート・ファイル・インクルード)攻撃を確認しています。また、ssh に対するスキャンは、不正侵入することを目的としたブルートフォース攻撃を多く確認しています。

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。

【 オークションサイトをかたるフィッシングサイト】
2011 年 1 月、中古自動車オークションをかたるフィッシングサイトの報告がありました。当該サイトは、主に国内外の中古車販売事業者を対象とした自動車の売買を行うサイトであり、金銭的被害が国際的に拡大する可能性が考えられました。JPCERT/CC は、本サイトで使用している米国の ISP、ドメインレジストラまた、US-CERT を含めた関係組織に連絡を行い、報告受領から 1 日で当該サイトの停止を確認しました。

【移動体通信ネットワークとダイナミック DNS を使用したフィッシングサイト】
2011 年 1 月以降、移動体通信ネットワークの IP アドレスと、ダイナミック DNS サービスで登録したホスト名を持ったサーバ上に、フィッシングサイトが設置されている例を複数確認しています。このフィッシングサイトの特徴として、フィッシングサイトは常時オンラインになってはおらず、不定期に稼働が確認されるため、サイトが実際に停止したのか判断することが困難です。
JPCERT/CC では、フィッシングサイトの存在を確認次第、移動体通信ネットワークを提供する ISP に対応を依頼しており、フィッシングサイトが順次停止していることを確認しています。

【韓国の政府系サイトを対象とする DDoS 攻撃への対応】
2011 年 3 月上旬、主に韓国の政府系サイトを対象とした DDoS 攻撃が発生しました。この攻撃は、マルウエアに感染した多数のコンピュータが指令サイトからの指令を受けて行ったものでしたが、この攻撃に使用された指令サイトやマルウエアに感染したコンピュータの一部が日本国内に存在していたため、KrCERT/CC からの依頼に基づき、関係サイトの管理者や ISP 各社に対し、攻撃の停止のための対応を依頼しました。

【震災や原発事故に乗じた標的型攻撃への対応】
2011 年 3 月 11 日の東日本大震災発生の数日後に、震災や原子力発電所の事故に関連する言葉をメールの件名や添付ファイル名に使用した標的型攻撃に関する報告を受けました。これらの攻撃の一部に、Adobe 製品の未修正の脆弱性を使用するマルウエアを確認したため、マルウエアを解析して得られた結果に基づき、マルウエアが通信する先のサイトを管理する ISP 及び関係する CSIRT に対してサイトの停止を依頼し、依頼の翌日に当該サイトの停止を確認しました。

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

6. ［付録］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２２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。