JPCERT CC®

JPCERT-IR-2010-0003
発行日: 2010-07-07

JPCERT/CC インシデント報告対応レポート
[2010 年 4 月 1 日 ～ 2010 年 6 月 30 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、2010 年 4 月 1 日から 2010 年 6 月 30 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、正当な権限をもたない人がコンピュータを不正に使用するような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おいて、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

本四半期の報告のうち、インシデントに関する報告は次のとおりでした。

[表 1 インシデント報告関連件数]

	総数	4 月	5 月	6 月
報告件数 (注 2)	3113	1421	837	855
インシデント件数 (注 3)	3185	1198	846	1141
調整件数 (注 4)	847	250	191	406

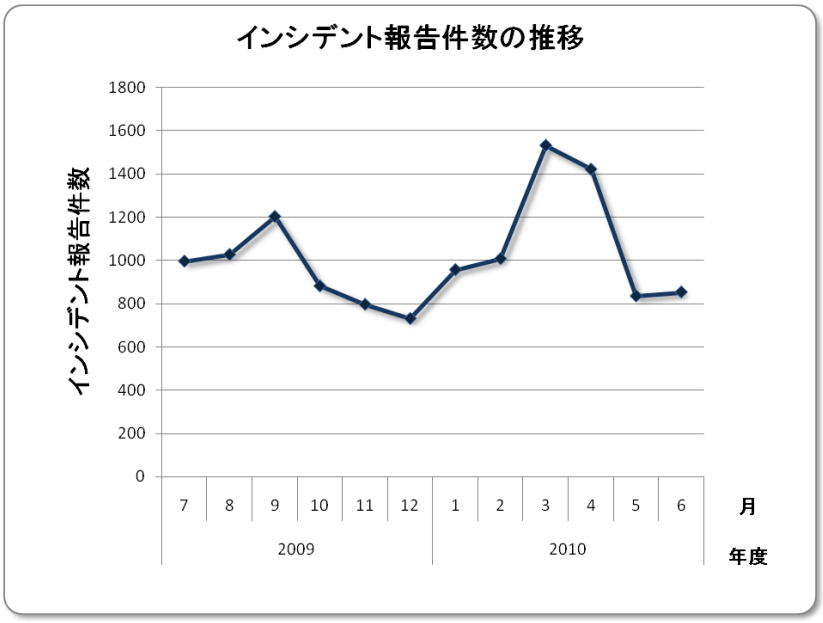
【注 2】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

【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。

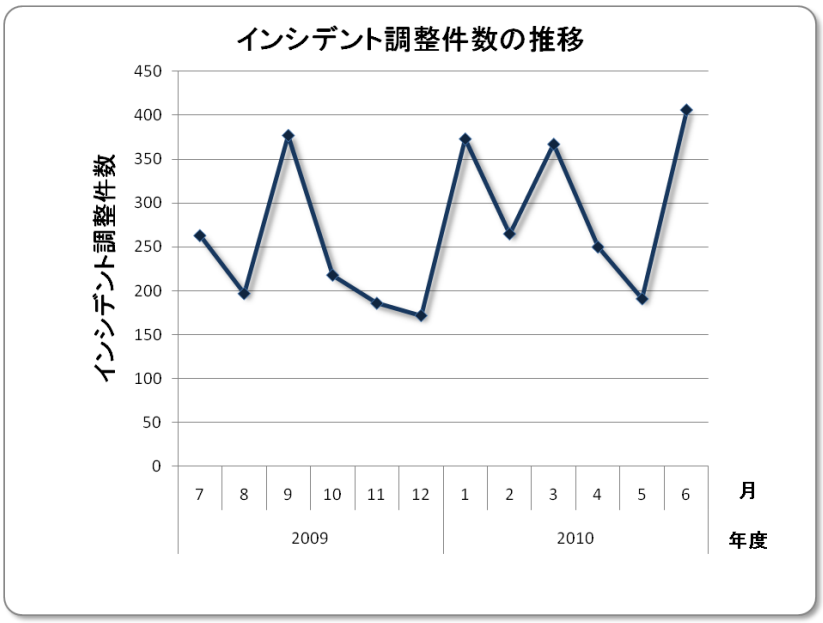
【注 4】「調整件数」とは、インシデントの拡大防止のため、サイトの管理者などに対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、3113 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 847 件でした。前四半期の 1,005 件と比較して 16%減少しています。

[図 1]～[図 2]に報告件数、及び調整件数の過去 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]



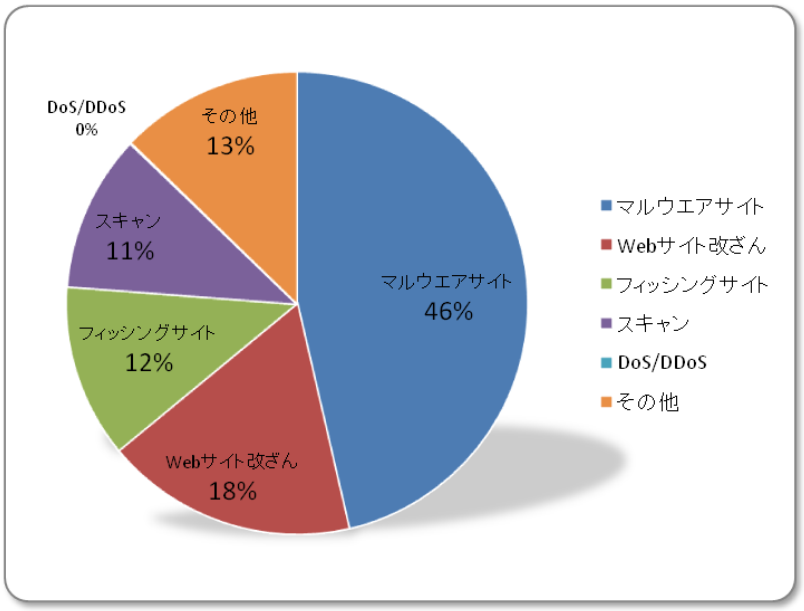
[図 2　インシデント調整件数の推移]

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 2]に示します。

[表 2 タイプ別インシデント件数]

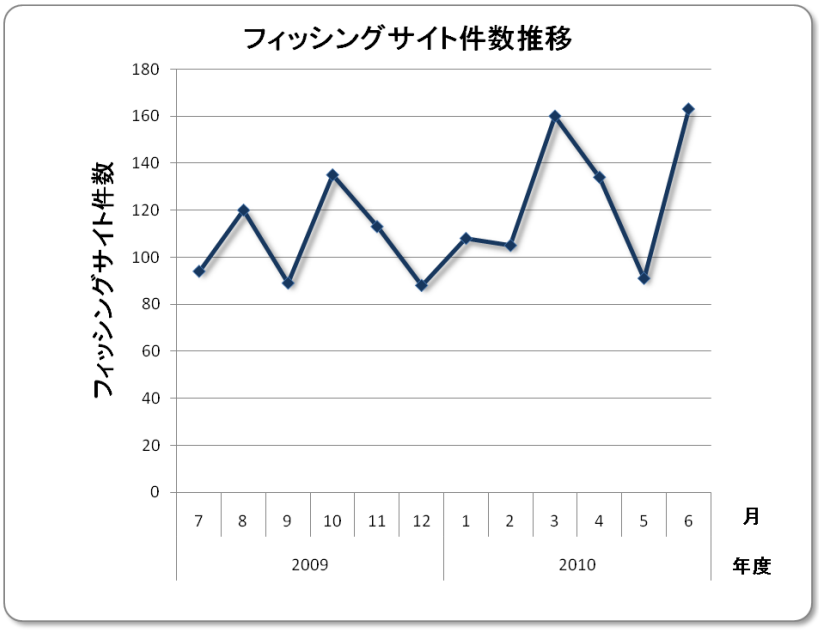
インシデント	総数	4 月	5 月	6 月
フィッシングサイト	388	134	91	163
Web サイト改ざん	561	205	108	248
マルウエアサイト	1478	615	418	445
スキャン	349	126	93	130
DoS/DDoS	2	0	0	2
その他	407	118	136	153

本四半期に発生したインシデントのタイプ別割合は、[図 3]のとおりです。マルウエアサイトに関するインシデントが 46%を占めています。また、Web サイト改ざんによるインシデントは 18%でした。

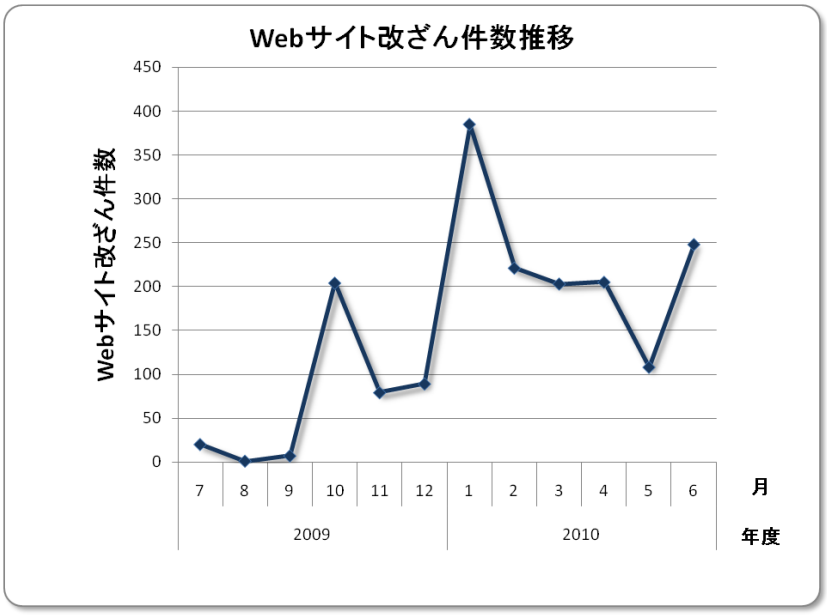


[図 3　インシデントのタイプ別割合]

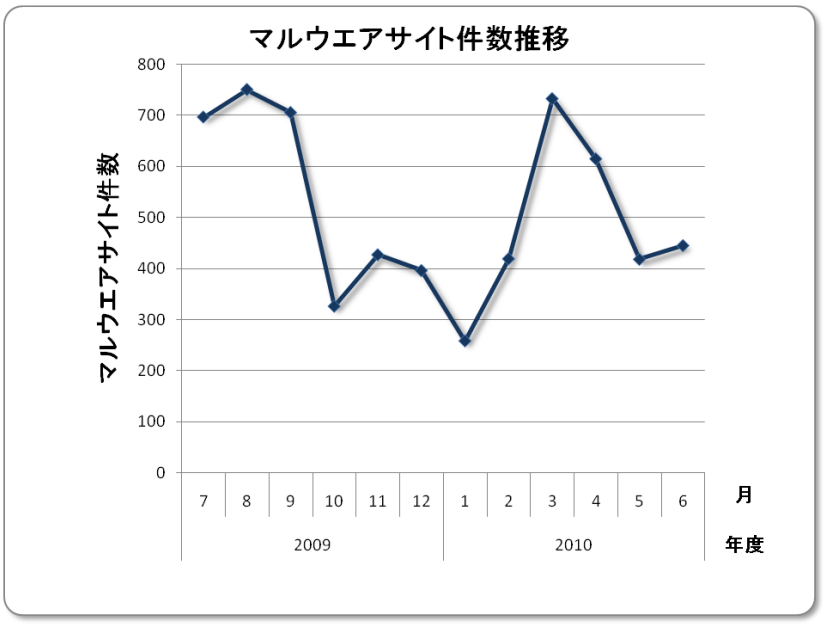
[図 4]から[図 7]に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



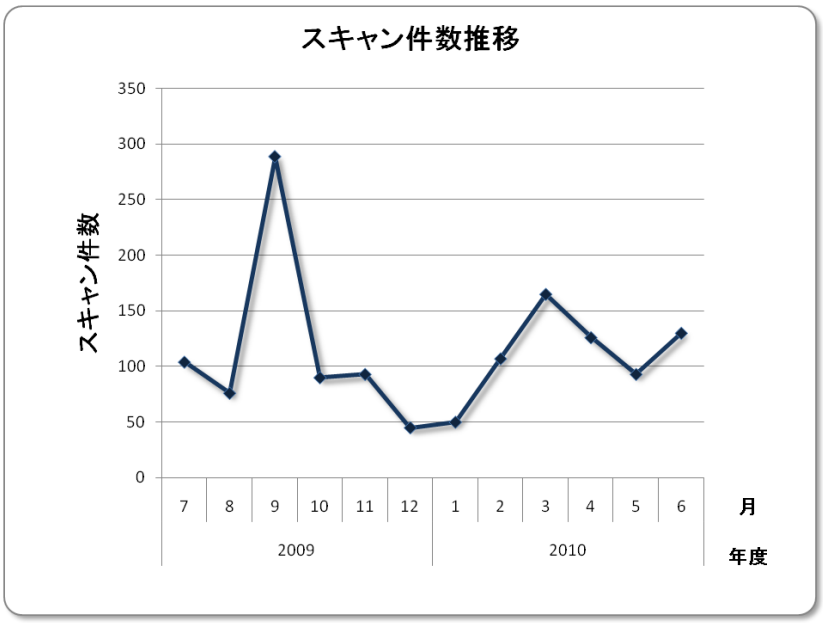
[図 4　フィッシングサイト件数推移]



[図 5　Web サイト改ざん件数推移]



[図 6　マルウエアサイト件数推移]


スキャン件数推移
スキャン件数
350
300
250
200
150
100
50
0
7
8
9
10
11
12
1
2
3
4
5
6
月
2009
2010
年度

[図 7　スキャン件数推移]

3. インシデントの傾向

本四半期は、特に国内のポータルサイトを装った「フィッシングサイト」と「Web サイト改ざん」の報告が多く寄せられました。

本四半期のフィッシングサイトのインシデント件数は、388 件でした。前四半期の 373 件から若干増加しました。このうち国内のブランドを装ったフィッシングサイトの件数は 157 件でした。前四半期の 77 件から増加しています。

以下は、フィッシングサイトの被害ブランドの国内・国外別の件数を示しています。

国内のブランドを装ったフィッシングサイトの件数: 157 件
国外のブランドを装ったフィッシングサイトの件数: 186 件
被害ブランドの国内外の別が不明な件数： 45 件

また、Web サイト改ざんのインシデント件数は、561 件でした。前四半期の 809 件から減少しています。本四半期の 561 件の大半は、いわゆる Gumblar ウイルスによる Web サイト改ざん攻撃でした。この攻撃は時とともに変化し続けており、2010 年 4 月には JDK および JRE の未修正の脆弱性を攻撃する手法が確認されました。また、この攻撃で感染するマルウエアの中に新たに DDoS 攻撃を行うものが追加されたことを確認しています。さらに、2010 年 6 月には、Windows XP/2003 に含まれる Windows のヘルプとサポート センター機能の未修正の脆弱性を攻撃する手法を確認しました。今後も新しく発見される脆弱性が組み込まれるなど攻撃が変化していく可能性があります。

Oracle Sun JDK および JRE の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2010/at100010.txt

いわゆる Gumblar ウイルスによってダウンロードされる
DDoS 攻撃を行うマルウエアに関する注意喚起
https://www.jpcert.or.jp/at/2010/at100011.txt

Windows のヘルプとサポートセンターの未修正の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2010/at100016.txt

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。

【フィッシングサイト】
2010 年 5 月、国内金融機関 A 社を騙るフィッシングサイトが公開されているとの報告を受領しました。JPCERT/CC では、フィッシングサイトの稼働を確認後、サイトを管理する米国の ISP と US-CERT に対して、フィッシングサイトの停止を依頼し、報告受領の翌日にフィッシングサイトが停止した事を確認しました。

【Web サイト改ざん】
2010 年 4 月、国内企業 B 社の Web サイトが改ざんされているとの報告を受領しました。JPCERT/CC では、当該サイトの調査を行い、いわゆる Gumblar ウイルスによる不審なスクリプトが埋め込まれていること、誘導先 Web サイトがマルウエアサイトであったことを確認し、当該 Web サイト管理者に改ざん内容の通知と所要の対応を依頼しました。また、誘導先サイトから入手したマルウエアの分析を行い、マルウエアが窃取した情報を送付する先のサイトを特定し、そのサイトを管理する ISP にサイトの停止を依頼しました。その結果、報告受領の 2 日後には改ざんされた Web サイトが修正されたこと、3 日後に情報送付先サイトが停止したことを確認しました。

【その他】
2010 年 5 月、日本語で記述されたマルウエア添付メールに関する報告を受領しました。JPCERT/CC では、メールに添付されたマルウエアの分析を行い、マルウエアがアクセスする外部サイトを特定し、サイトを管理する韓国の ISP と KrCERT/CC に対してマルウエアの配布サイトの停止を依頼しました。8 日後にマルウエアがアクセスする外部サイトが停止したことを確認しました。
また、情報収集・分析の結果、国内の複数の組織に対して、同様のメールが送られていることが確認されたことから、注意喚起情報として広く一般への情報提供も行いました。

社内 PC のマルウエア感染調査を騙るマルウエア添付メールに関する注意喚起
https://www.jpcert.or.jp/at/2010/at100013.txt

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を行ったり、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ったりする活動を通じて、インシデントによる被害の拡大・再発の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、下記の 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。下記の 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 が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、下記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（マルウエア含む）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、ユーザが閲覧すると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。

- アクセスした者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) 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。