JPCERT CC®

JPCERT-IR-2010-0004
発行日: 2010-10-07

JPCERT/CC インシデント報告対応レポート
[2010 年 7 月 1 日 ～ 2010 年 9 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 7 月 1 日から 2010 年 9 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、正当な権限を持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は次のとおりでした。

[表 1　インシデント報告関連件数]

	7 月	8 月	9 月	合計
報告件数(注 2)	739	872	830	2441
インシデント件数（注 3）	844	939	978	2761
調整件数（注 4）	283	214	204	701

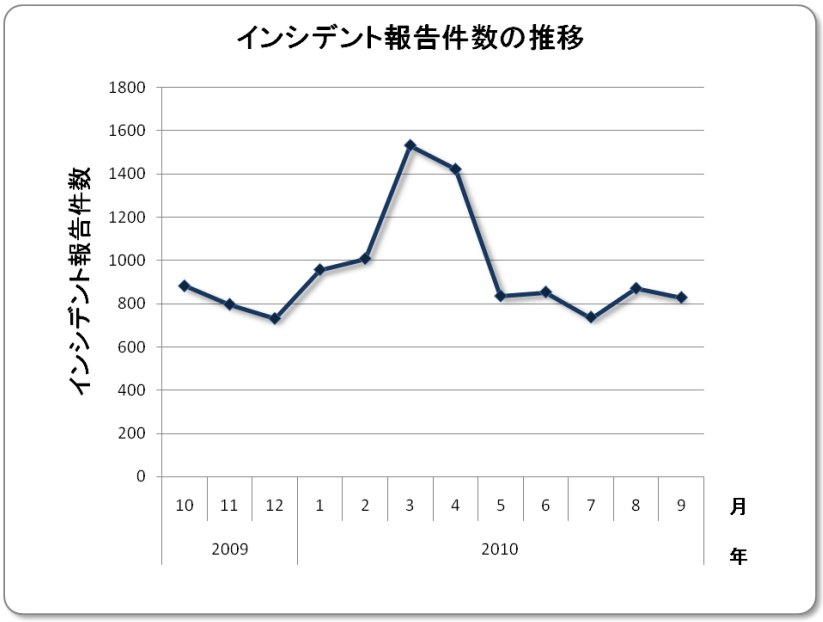
【注 2】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。

【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。

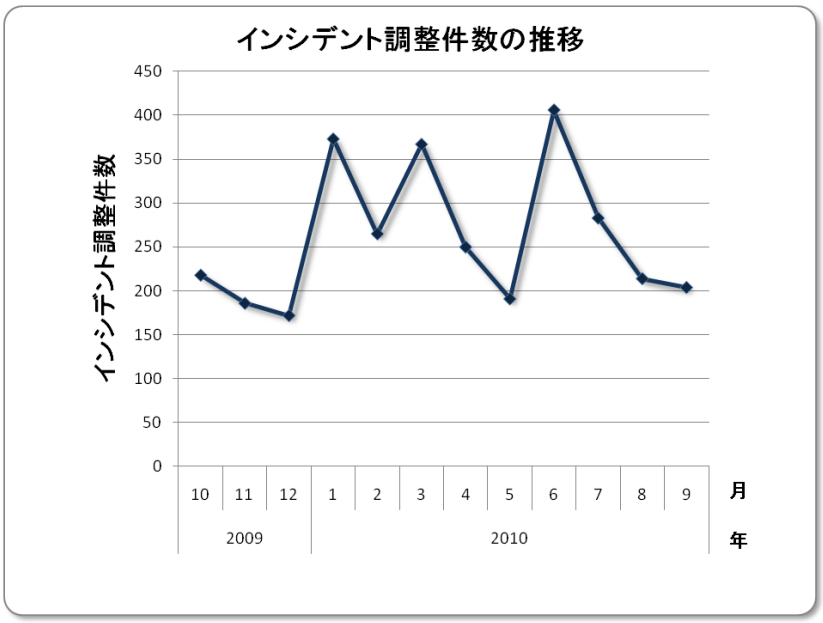
【注 4】「調整件数」とは、インシデントの拡大防止のため、サイトの管理者などに対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、2,441 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 701 件でした。前四半期の 847 件と比較して約 17%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]



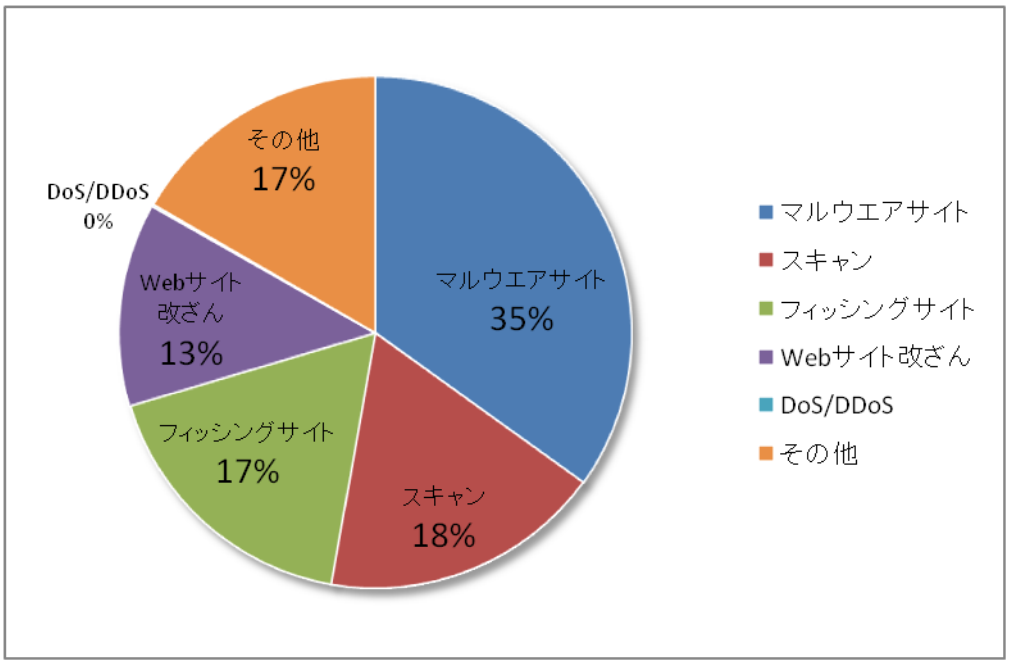
[図 2　インシデント調整件数の推移]

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]

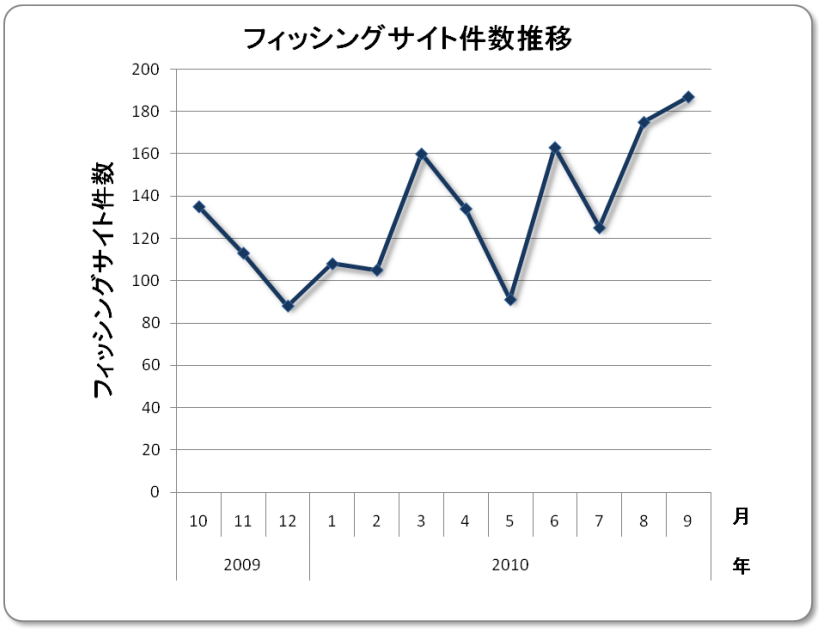
インシデント	7 月	8 月	9 月	合計
フィッシングサイト	125	175	187	487
Web サイト改ざん	85	162	106	353
マルウエアサイト	385	332	248	965
スキャン	99	115	278	492
DoS/DDoS	0	3	2	5
その他	150	152	157	459

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 35%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 13%でした。

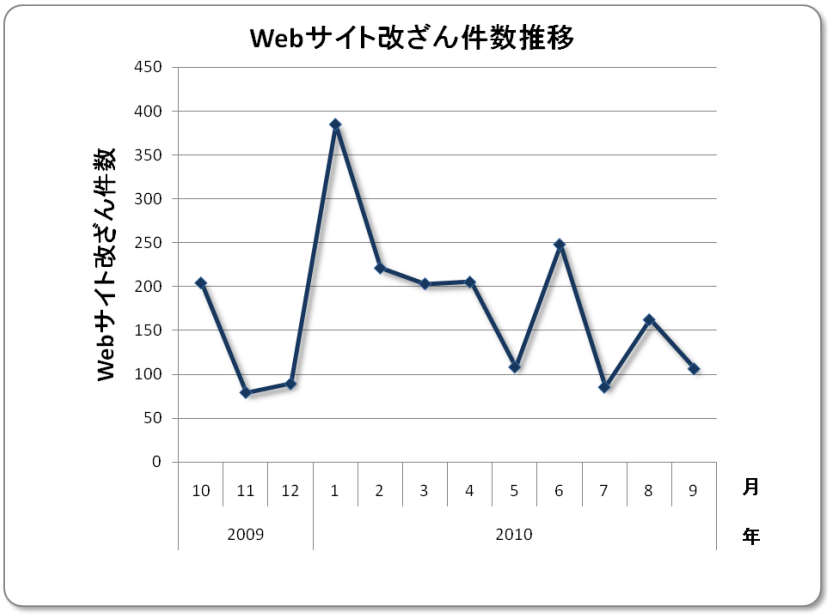


[図 3　インシデントのタイプ別割合]

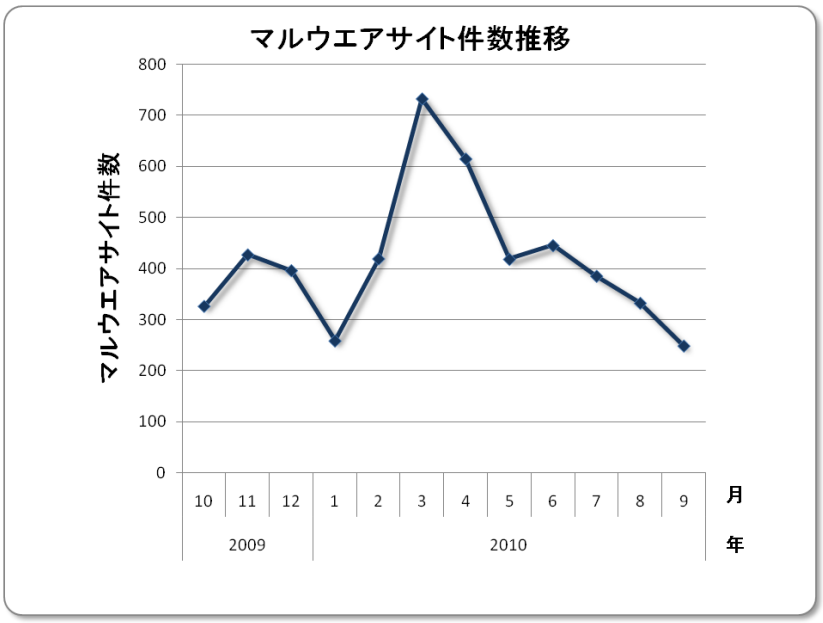
[図 4]から[図 7]に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



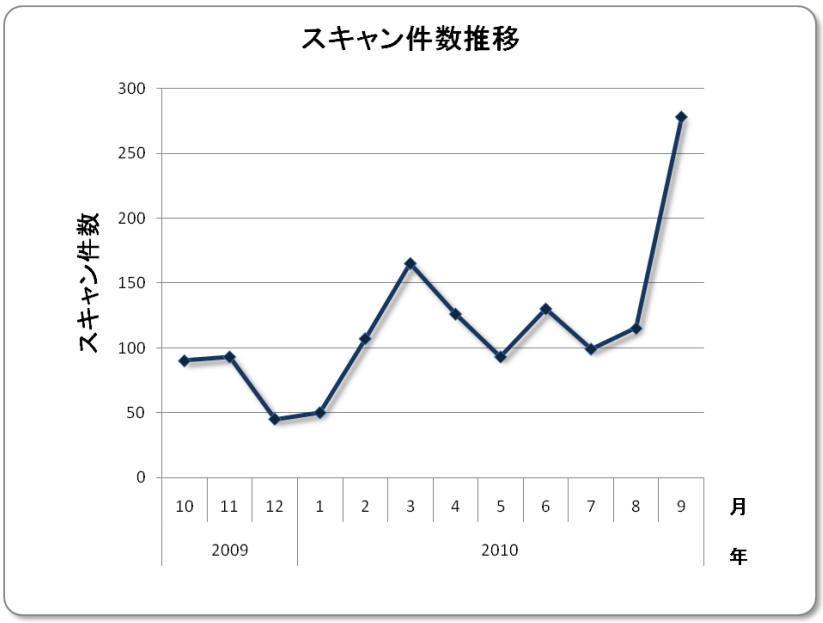
[図 4　フィッシングサイト件数推移]



[図 5　Web サイト改ざん件数推移]

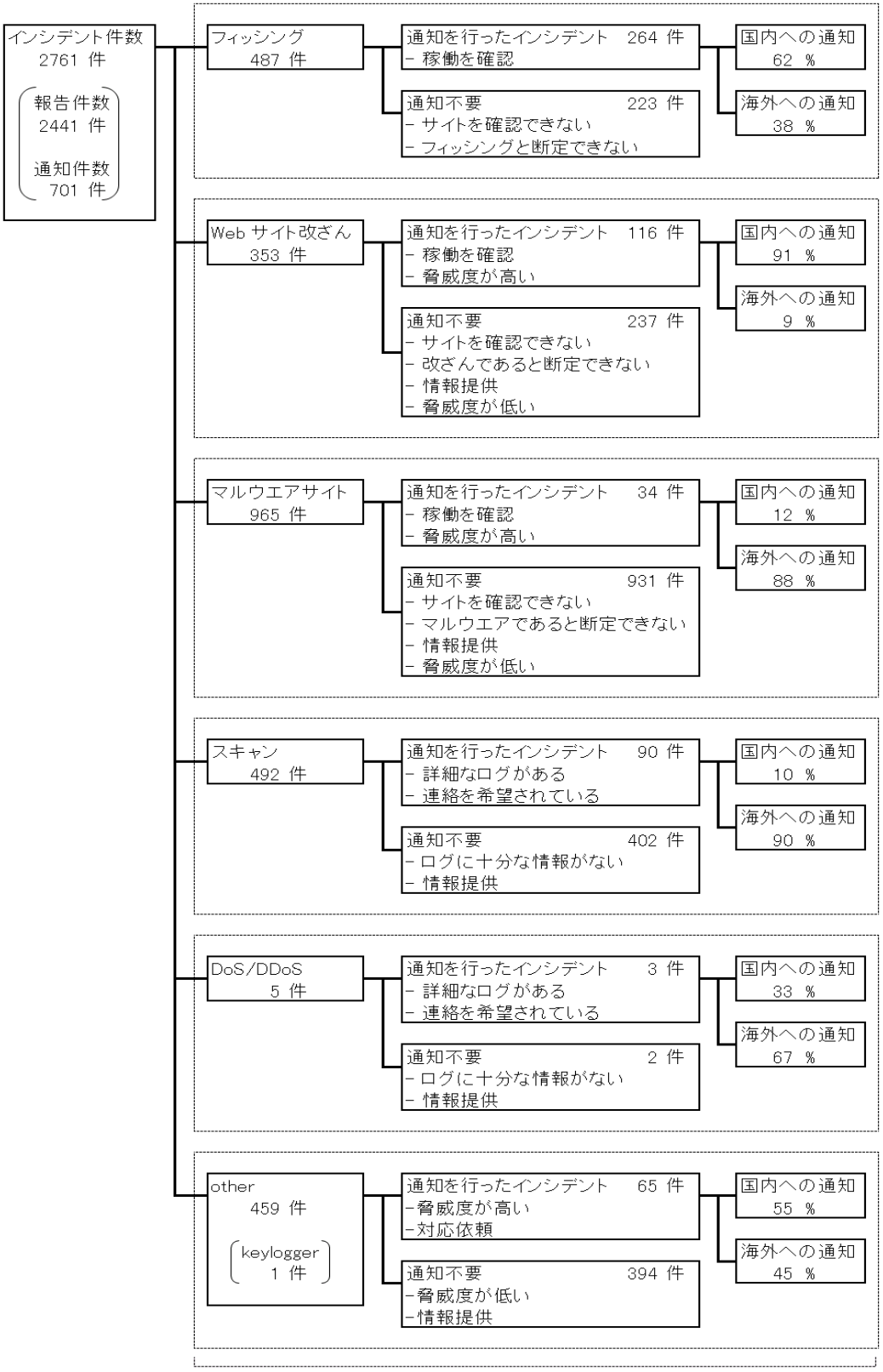


[図 6　マルウエアサイト件数推移]


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

[図 7　スキャン件数推移]

[図 8] 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 8　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。**

本四半期は、「フィッシングサイト」の報告が多く寄せられました。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、487 件で、前四半期の 388 件から約 25%増加しました。また、前年度同四半期（303 件）との比較では、約 61%の増加となっています。これらフィッシングサイトの国内・国外ブランド別の内訳を[表 3] に示します。

[表 3　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	7 月	8 月	9 月	国内外別合計（割合）
国内ブランド	74	101	103	278 (57%)
国外ブランド	38	44	41	123 (25%)
国内外の別不明	13	30	43	86 (18%)
月別合計	125	175	187	487(100%)

本四半期は、国内ブランドを装ったフィッシングサイトの件数が 278 件と、前四半期の 157 件から大幅に増加しました。この増加は、国内のポータルサイトを装ったフィッシングサイトの増加によるものです。なお、国外のブランドを装ったフィッシングサイトの件数は、123 件と、前四半期の 186 件から減少しています。

本四半期のフィッシングサイトにおける調整先については、国内が 62%、国外が 38%でした。前四半期の割合（国内 55%、国外 45%）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、前述の国内ポータルサイトを装った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、353 件でした。前四半期の 561 件から約 37%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減少したためですが、前年度同四半期（2009 年 7 月から 9 月）における Web 改ざんの報告件数が 28 件であったことに鑑みれば、いまだに多数の報告が寄せられている状況にあります。このことからも、Web サイト改ざんの攻撃が常態化していると考えられますので、引き続き OS やアプリケーションの修正プログラムの適用を励行してください。

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、965 件でした。前四半期の 1473 件から約 35%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よ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、492 件でした。前四半期の 349 件から約 41%増加しています。これは、2010 年 9 月以降、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増加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 4]に示します。

[表 4　ポート別のスキャン件数]

スキャン	7 月	8 月	9 月	合計
80	42	52	65	159
445	0	0	111	111
22	41	36	34	111
25	11	19	35	65
5060	0	2	0	2
1433	0	1	1	2
21	0	1	1	2
23	0	0	2	2
5900	1	0	0	1
3127	0	1	0	1
不明	4	3	29	36
月別合計	99	115	278	492

スキャンの対象となったポートは、http（80/tcp)、smb（445/tcp）、ssh（22/tcp)の順に多く確認しています。http に対するスキャンは、Web アプリケーションの脆弱性を攻撃する RFI（リモート・ファイル・インクルード）攻撃を多く確認しています。smb に対するスキャンは、Windows の脆弱性を狙う攻撃を多く確認しています。また、ssh に対するスキャンは、サーバに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。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）探索を行うスキャンが常態化しているため、サーバ管理者は注意が必要です。

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。

【フィッシングサイト】
2010 年 8 月、海外 CSIRT から、海外金融機関 A 社を騙るフィッシングサイトが国内企業のサーバ上で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、国内 ISP を通じて当該国内企業にフィッシングサイトの停止を依頼し、同日にフィッシングサイトが停止した事を確認しました。

【DoS/DDoS】
2010 年 8 月、国内の企業から、DDoS 攻撃を受けているとの報告を受領しました。JPCERT/CC では、提供されたログ情報をもとにアクセス元の IP アドレスを管理するアメリカ、イギリスの ISP に対し、アクセスの停止を求める対応の依頼を行いました。その後、報告者から DDoS 攻撃が JPCERT/CC への相談の翌々日に停止したとの連絡をいただきました。

【その他】
2010 年 9 月、海外の CSIRT から、キーロガー機能を持つマルウエアによって窃取され、海外に送信された日本のユーザのアカウント情報についての報告を受領しました。JPCERT/CC では、受領したアカウント情報から、そのアカウントが利用されるサービスの提供事業者を特定し、そのうちの情報の受領意思のある事業者に対して情報提供を行いました。

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、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。