JPCERT CC®

JPCERT-IR-2011-0001
発行日: 2011-01-12

JPCERT/CC インシデント報告対応レポート
[2010 年 10 月 1 日 ～ 2010 年 12 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、2010 年 10 月 1 日から 2010 年 12 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は次のとおりでした。

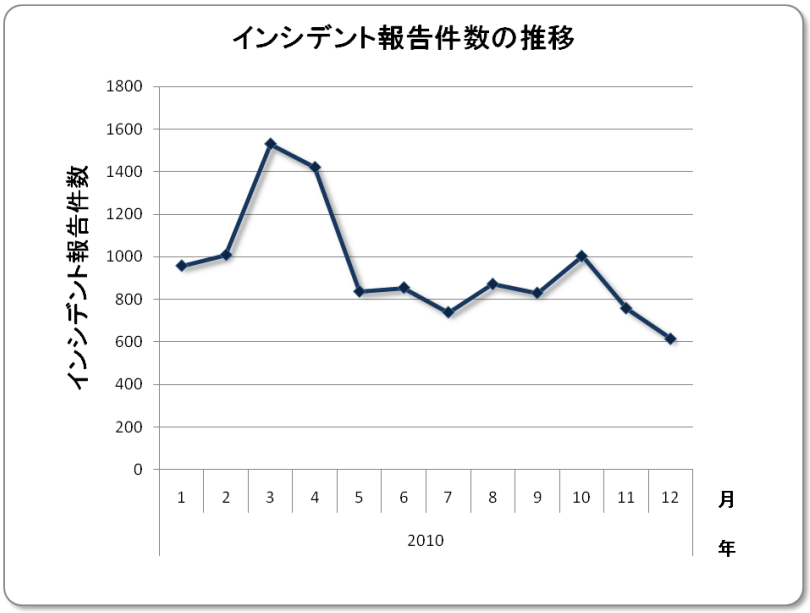
[表 1: インシデント報告関連件数]

	10 月	11 月	12 月	合計	前四半期合計
報告件数（注 2）	1003	758	614	2375	2441
インシデント件数（注 3）	1182	798	658	2638	2761
調整件数（注 4）	235	273	223	731	701

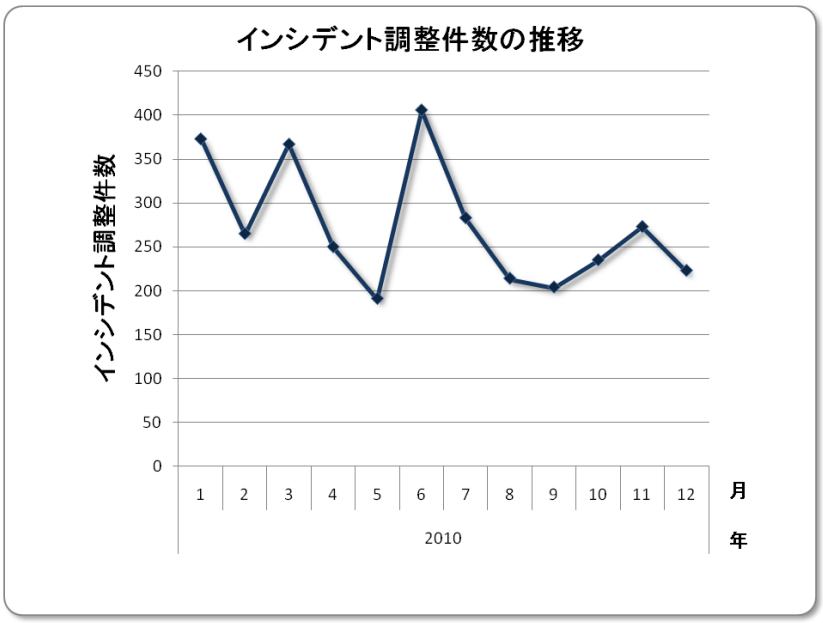
【注 2】「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。
【注 3】「インシデント件数」は、各報告に含まれるインシデント件数の合計を示します。ただし、1 つのインシデントに関して複数件の報告が寄せられた場合は、1 件のインシデントとして扱います。
【注 4】「調整件数」とは、インシデントの拡大防止のため、サイトの管理者などに対し、現状の調査と問題解決のための対応を依頼した件数を示します。

本四半期に寄せられた報告件数は、2375 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 731 件でした。前四半期と比較して、報告件数、インシデント件数ともに減少していますが、調整件数は増加しています。

[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]



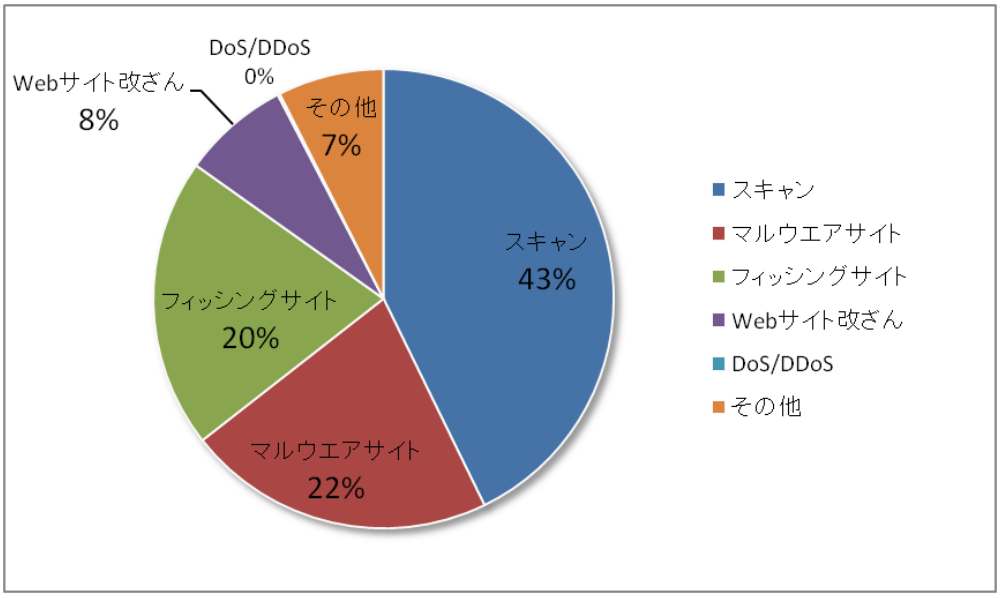
[図 2: インシデント調整件数の推移]

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]

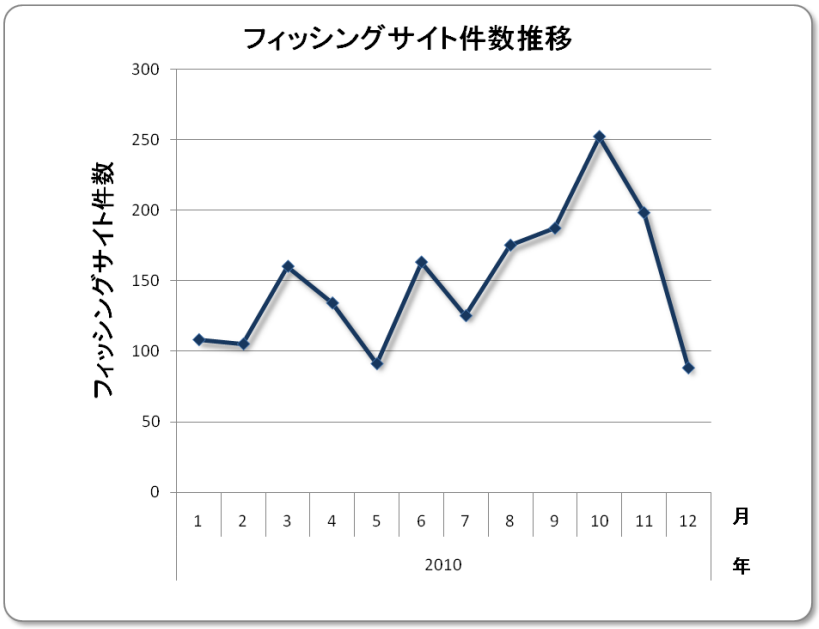
インシデント	10 月	11 月	12 月	合計
フィッシングサイト	252	198	88	538
Web サイト改ざん	117	35	47	199
マルウエアサイト	205	160	207	572
スキャン	491	379	258	1128
DoS/DDoS	4	0	0	4
その他	113	26	58	197

本四半期に発生したインシデントのタイプ別割合は、[図 3]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 42%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 22%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 8%でした。

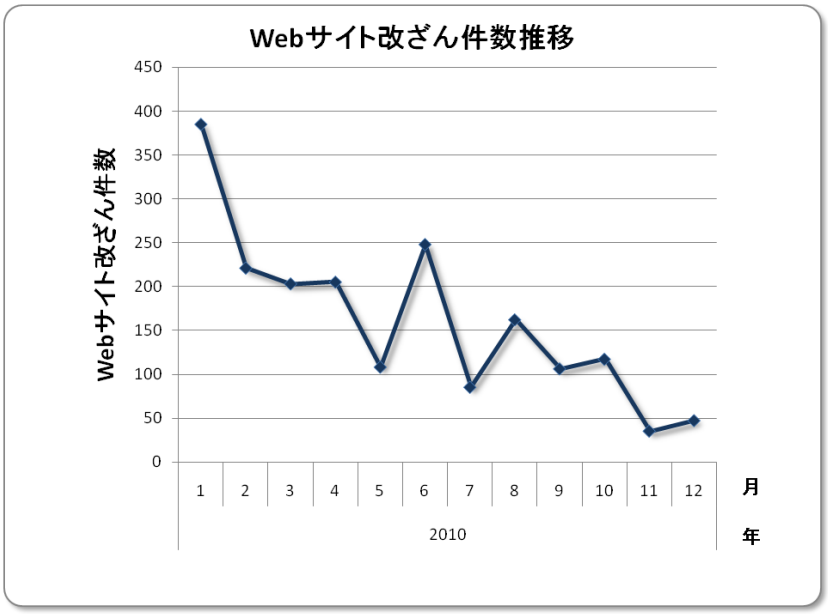


[図 3: インシデントのタイプ別割合]

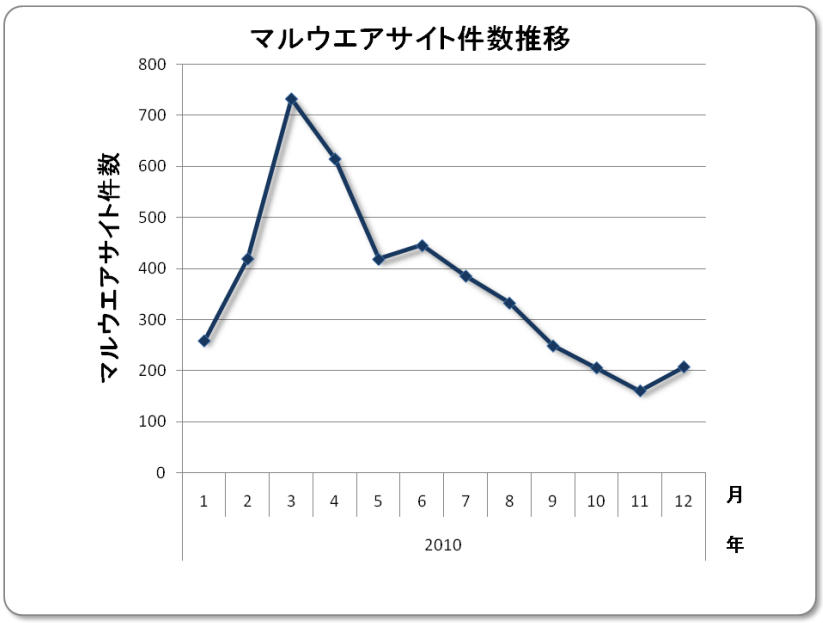
[図 4]から[図 7]に、フィッシングサイト、Web サイト改ざん、マルウエアサイト、スキャンのインシデントの過去 1 年間の月別推移を示します。



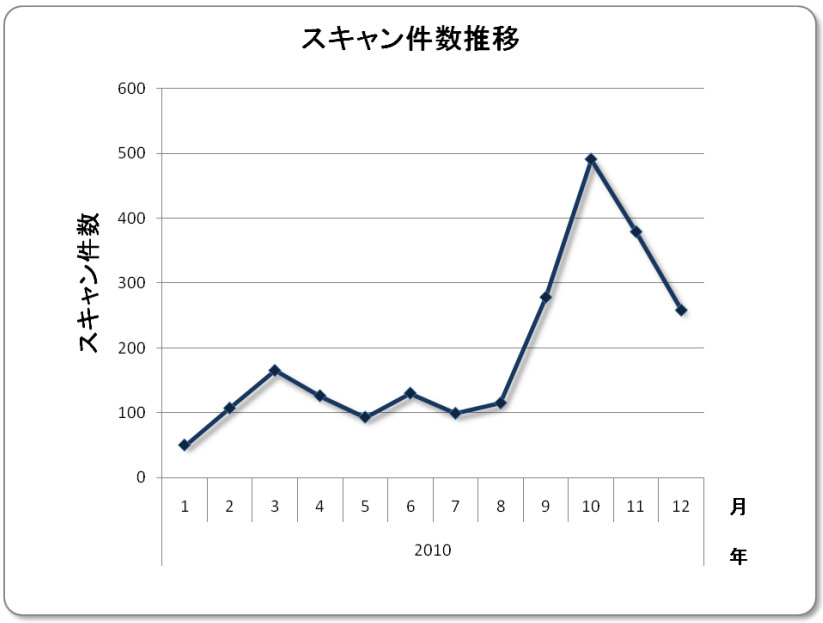
[図 4: フィッシングサイト件数推移]



[図 5:　Web サイト改ざん件数推移]

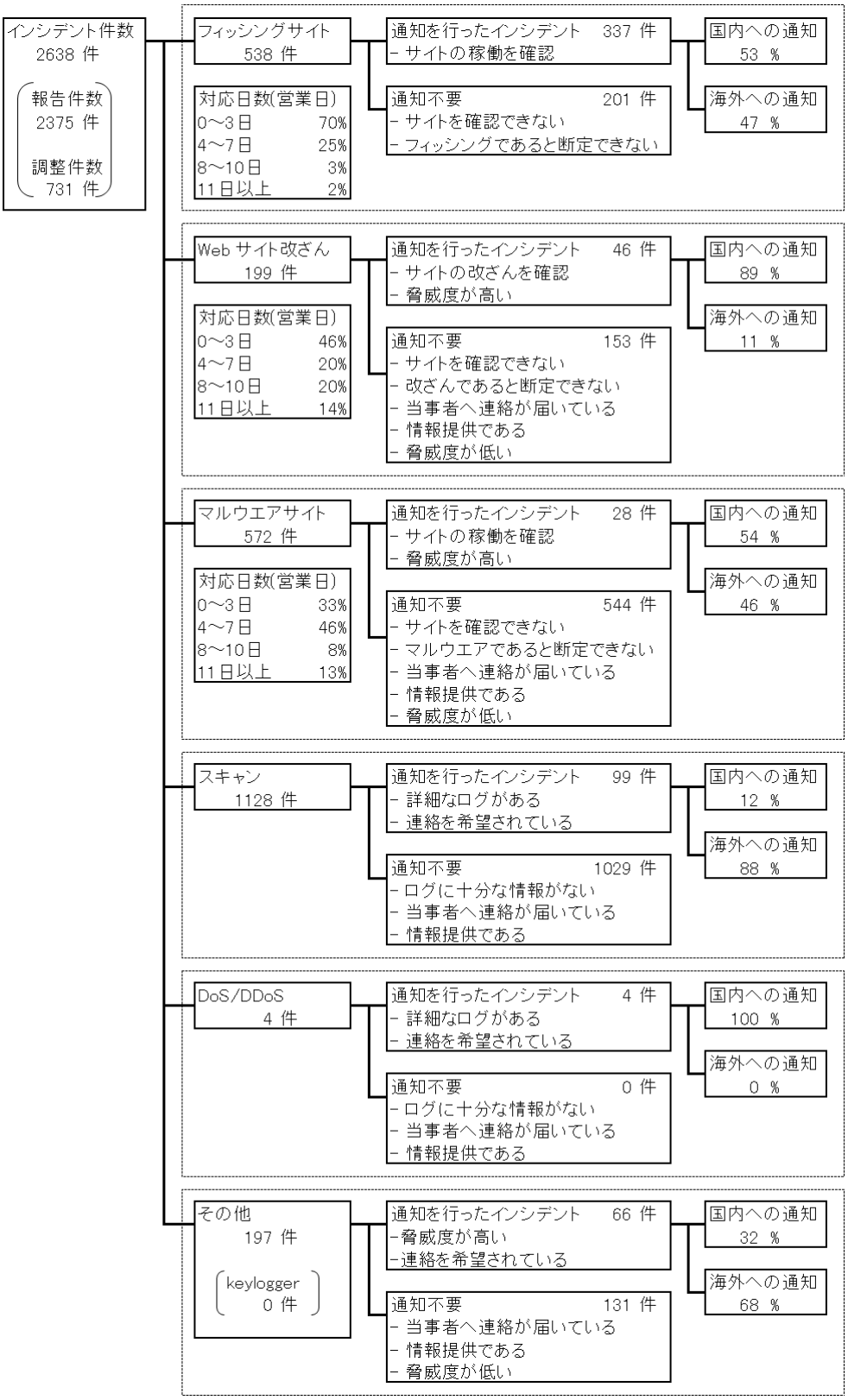


[図 6: マルウエアサイト件数推移]


スキャン件数推移
600
500
400
300
200
100
0
スキャン件数
1
2
3
4
5
6
7
8
9
10
11
12
月
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、10 月に多くの「フィッシングサイト」の報告をいただきました。本四半期に報告を頂いたフィッシングサイトの件数は、538 件で、前四半期の 487 件から約 10%増加しました。また、前年度同四半期（336 件）との比較では、約 60%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 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	10 月	11 月	12 月	国内外別合計（割合）
国内ブランド	177	88	19	284 (53%)
国外ブランド	58	91	53	202 (37%)
ブランド不明	17	19	16	52 (10%)
月別合計	252	198	88	538(100%)

本四半期は、グローバルにサービスを展開するクレジットカード会社を装ったフィッシングサイトを数多く報告いただいたため、国外ブランドを装ったフィッシングサイトの件数が 202 件と、前四半期の 123 件から約 64 % 増加しました。なお、国内のブランドを装ったフィッシングサイトの件数も、284 件と、前四半期の 278 件から増加しています。

本四半期のフィッシングサイトの調整先は、国内が 53%、国外が 47%でした。前四半期の割合（国内 62%、国外 38%）と比較して、本四半期は国外への調整が増えました。これは、前述のグローバルにサービスを展開するクレジットカード会社を装ったフィッシングサイトの多くが国外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、199 件でした。前四半期の 353 件から約 44%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 については、一部の亜種の攻撃がおさまってきており、世間での注目度が下がっていることが一因になっています。一方で 11 月ころから報告を頂いている Web サイト改ざんでは、Internet Explorer の未修正の脆弱性を悪用した攻撃や、Java の脆弱性を悪用する、より脅威度の高い攻撃が確認さ

れています。JPCERT/CC では、これらの攻撃の分析を行い、攻撃において中核となっていたサイトを停止させる対応を行っています。

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、572 件でした。前四半期の 965 件から約 41%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頂い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、1128 件でした。前四半期の 492 件から約 129%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]

ポート	10 月	11 月	12 月	合計
135/tcp	168	233	0	401
445/tcp	180	145	10	335
80/tcp	105	74	153	332
25/tcp	65	12	29	106
22/tcp	22	30	42	94
icmp	37	26	24	87
21/tcp	2	0	0	2
53/udp	1	0	0	1
110/tcp	0	1	0	1
161/udp	0	0	1	1
5900/tcp	0	0	1	1
6667/tcp	0	1	0	1
不明	1	21	6	28

スキャンの対象となったポートは、rpc(135/tcp)、smb(445/tcp)、http(80/tcp) の順に多く確認しており、rpc、smb などの Windows の脆弱性を狙う攻撃が多いといえます。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。

【Internet Explorer の未修正の脆弱性を使用した攻撃サイトへの対応】
2010 年 11 月、Internet Explorer の未修正の脆弱性を悪用した攻撃サイトの情報とそのサイトからダウンロードされるマルウエアの検体を提供いただきました。本攻撃サイトは、改ざんされた Web サイトから誘導され、アクセスしただけでマルウエアに感染させるいわゆるドライブ・バイ・ダウンロード攻撃に使用されていました。JPCERT/CC では、この攻撃の根幹となる本攻撃サイトを停止させるための対応を行い、11 月中旬に本攻撃サイトの停止を確認しました。

【住民税還付を装うなりすましメール】
2010 年 10 月、財団法人地方自治情報センターから、同組織を騙るなりすましメールが確認されたとの報告を受領しました。このメールは、件名が「住民税還付還付追加―総務省」となっており、添付ファイルとして「住民税還付 追加項目」というファイル名の PDF ファイルが添付されていました。この添付ファイルには Adobe Reader や Acrobat の脆弱性を悪用するマルウエアが埋め込まれており、このファイルを開くとマルウエアに感染し、海外のサーバと不審な通信を行うことが確認されました。
JPCERT/CC では、マルウエアの接続先サーバに対して通知を行い、11 月中旬にサーバが停止したことを確認しました。

【共用サーバのコンテンツ改ざん】
2010 年 10 月、国内ホスティング業者のホスティングサービスで提供しているサーバが不正侵入され、多数のサイトのコンテンツが改ざんされているとの報告を受領しました。サイト数は 500 以上あり、JPCERT/CC では、改ざんされたサイトを確認し、当該ホスティング事業者にサイトを確認いただくよう依頼し、該当サイトに対して継続的に状況把握・通知を行いました。

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。