JPCERT CC®

JPCERT-IR-2009-0004
発行日: 2009-10-08

JPCERT/CC インシデントハンドリング業務報告
[2009 年 7 月 1 日 ～ 2009 年 9 月 30 日]

JPCERT/CC が 2009 年 7 月 1 日から 2009 年 9 月 30 日までの間に受け付けた届出のうち、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。）に関する届出は次のとおりでした。

届出（メール、FAX の延数*1）	2983 件（3228 通）
インシデント対象 IP アドレス数	3141 アドレス

*1:同一サイトのインシデント情報が異なる届出者の方から届けられるため、届出件数はメール及び FAX の数よりも少なくなっています。

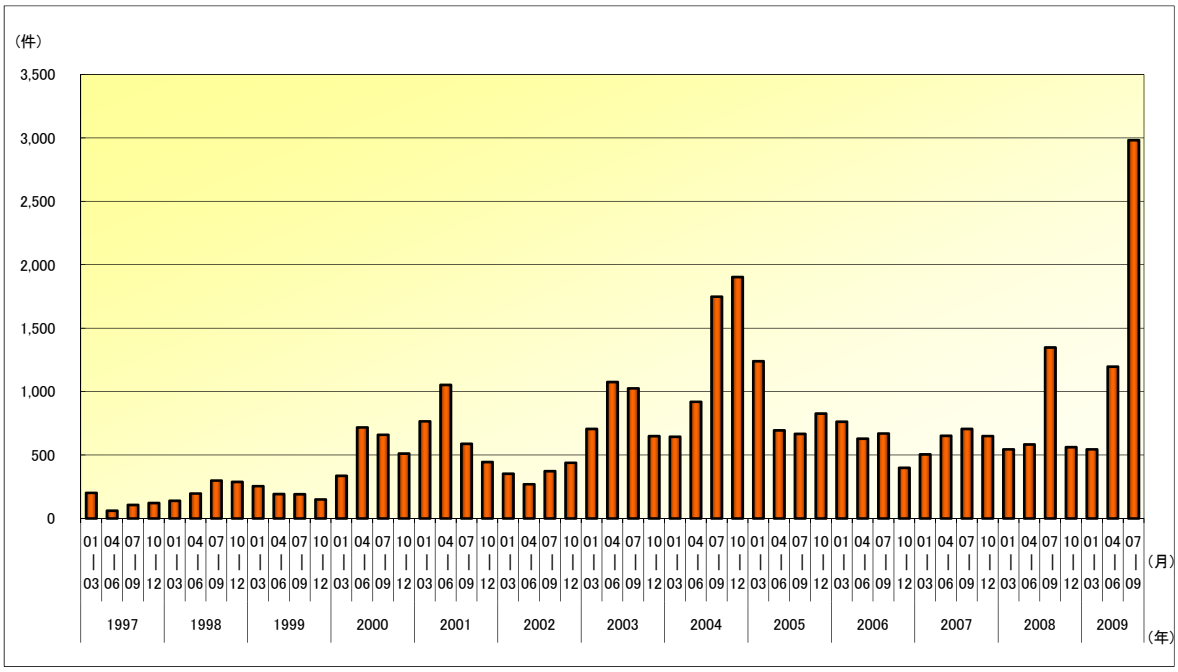

図 1：インシデント報告件数の推移

インシデント届出の分類、傾向等の詳細は、以下のとおりです。

- **インシデントの届出の送信元による分類**

JPCERT/CC が届出を受けたインシデント報告の送信元トップレベルドメインの上位 5 位までは、次のとおりです。マレーシアのドメインからの報告が他と比較して多いのは、本年 5 月以降定常的に受領している、日本国内のマルウエア設置サイトに関するマレーシアのセキュリティ対応機関からの届出が含まれているためであり、同機関からの届出件数の増加が、全体の件数の増加にも寄与しています。

当四半期 (2009 年 7 月～9 月)		前四半期 (2009 年 4 月～6 月)	
.my（マレーシア）	1) 2061 件	.my（マレーシア）	1) 713 件
.jp	2) 605 件	.jp	2) 301 件
.org	3) 172 件	.org	3) 223 件
.com	4) 165 件	.com	4) 142 件
.br	5) 156 件	.br（ブラジル）	5) 137 件

- **インシデントの届出に基づく調整件数**

JPCERT/CC がインシデントの届出に基づいて国内外の関連するサイトとの調整を行った件数は 837 件でした。ここでいう「調整」とは、インシデントの発生元に対する連絡調整等の依頼を含むインシデントの届出に基づいて、フィッシングサイトが設置されているサイトや、改ざんにより JavaScript が埋め込まれているサイト、ウイルス等のマルウエアが設置されたサイト、「scan」のアクセス元等の管理者及び関係協力組織に対し、現状の調査と善処の依頼の連絡を行うものです。

- **インシデントのタイプ別分類**

JPCERT/CC が届出を受けたインシデントのタイプ別分類割合は図 2 のとおりです。マルウエアに関連するインシデントが 7 割近くを占めています。

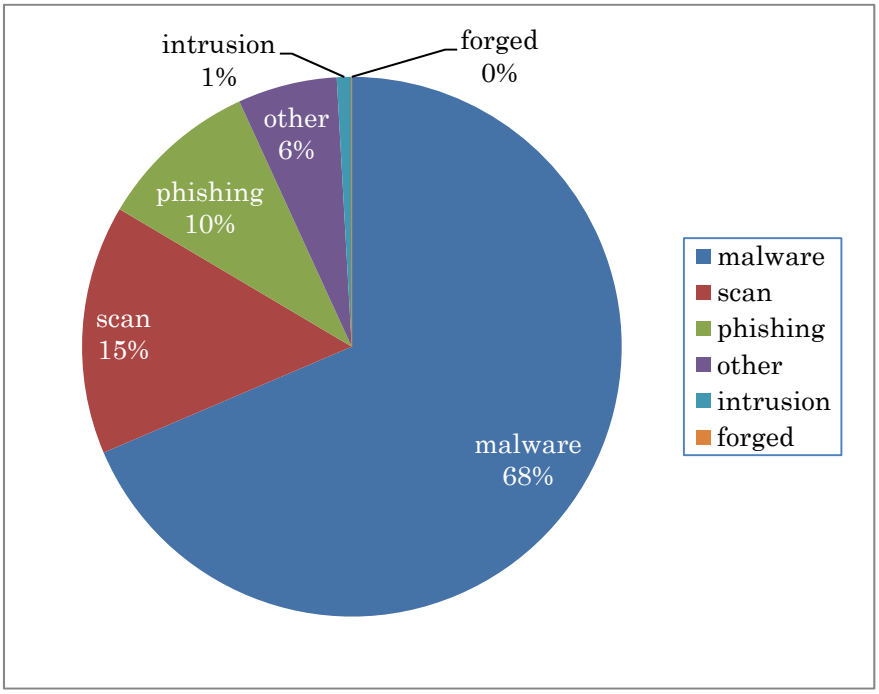

図 2：タイプ別インシデント件数割合

（1）フィッシング（phishing）

国内外の金融機関やオークションサイトなどのオンラインサービスであるかのように装いサービス利用者の ID、パスワード、口座番号、暗証番号、個人情報等の重要な情報を盗み取ろうとする「フィッシング」の件数は、303 件でした。

国内のサイトを装ったフィッシングサイトの件数が前四半期の 58 件から、101 件と増加しています。これは国内の有名ポータルサイトを装うフィッシングサイトが数多く届出されたためです。これらの事例では設置されるコンテンツやフィッシングの手口が類似しており、なんらかの攻撃ツールの流通が広く行われている可能性があります。

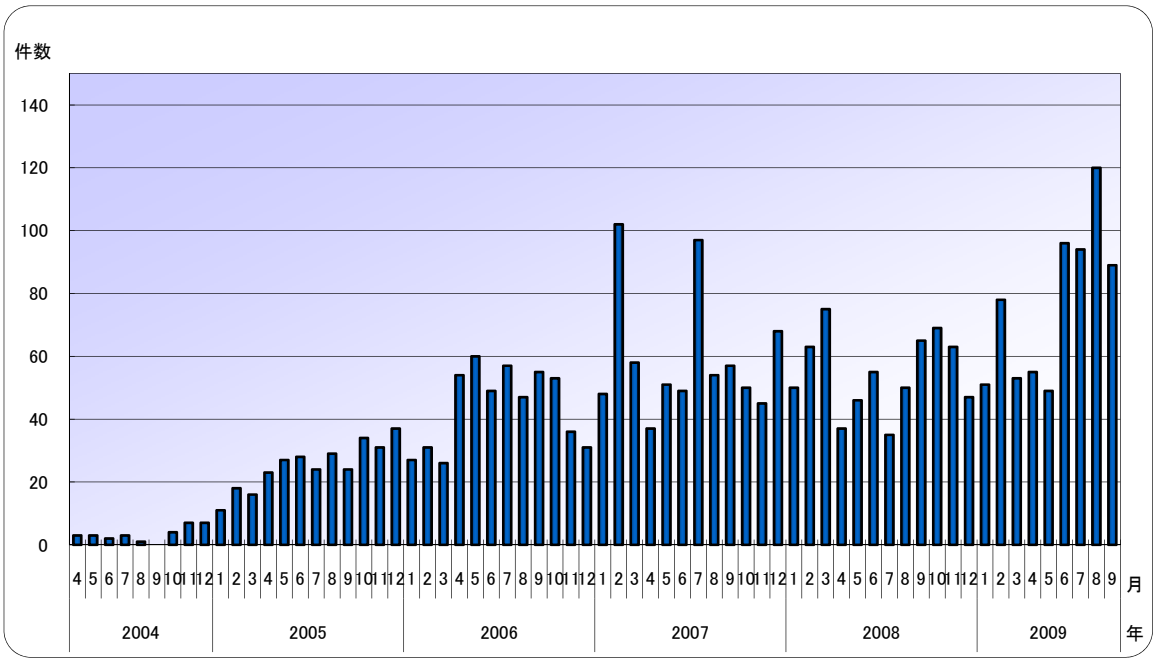

図 3：フィッシング件数推移

以下の件数は、装われたサイトの国内・国外別の件数を示しています。

国内組織を装ったフィッシングサイトの件数: 104 件 (*2)
国外組織を装ったフィッシングサイトの件数: 192 件 (*2)

*2:フィッシングサイトが装ったサイトの国内・国外の別を確認できなかった件数が 7 件ありました。

JPCERT/CC ではフィッシングサイトが設置されている国内外のサイト管理者に対して、「フィッシングサイトの停止」のための調査対応依頼を行っています。

Web サイトで個人情報等の重要な情報を入力する際には、情報を入力しようとしているサイトが、正規のサイトであることを慎重に確認してください。

もし、フィッシングサイトに個人情報等の重要な情報を入力してしまったことに気づいた場合は、速やかに正規のサービス事業者にご相談いただき、ID、パスワード等の変更手続きを行ってください。

【参考】前四半期（2009 年 4 月 1 日から 6 月 30 日）の国内・国外別の件数

国内組織を装ったフィッシングサイトの件数:　58 件 (*3)
国外組織を装ったフィッシングサイトの件数: 125 件 (*3)

*3:フィッシングサイトが装ったサイトの国内・国外の別を確認できなかったフィッシングサイトの件数が 17 件ありました。

（2）　システムへの侵入（intrusion）

管理者権限の盗用またはシステムへの侵入の件数は 28 件でした。Web サイトが改ざんされるインシデントが前四半期の 74 件から今期は 28 件に減少しました。28 件すべてが前四半期の事例と同じ JSRedir-R/Gumblar による Web サイト改ざんの事例でした。改ざんされた Web サイトのページには他のサイトへ誘導する難読化された JavaScript が埋め込まれています。このページを閲覧すると、閲覧したユーザのコンピュータ上で特定のソフトウエアの脆弱性が使用され、マルウエアがインストールされる可能性があります。このマルウエアは感染した PC から FTP アカウントの情報を詐取します。この情報を使用してユーザが管理する Web サイトをさらなる攻撃に使用します。この手順の攻撃によって改ざんサイトが多数発生しました。

JPCERT/CC では、改ざんされたサイトの管理者へ通知を行っています。

システム管理者におかれては、管理しているサイトが改ざんされていないか、使用しているソフトウエアなどに脆弱性がないかなどについて定期的に確認してください。

独立行政法人 情報処理推進機構
「安全なウェブサイトの作り方 改訂第 3 版」
https://www.ipa.go.jp/security/vuln/websecurity.html

一般ユーザにおかれては、OS や Web ブラウザだけでなく、PC にインストールされているすべてのソフトウエアを最新の状態に保つとともに、ウイルス対策ソフトを導入し、またウイルス定義ファイルを常に最新の状態に保つなどの対策を行うことをお勧めします。詳細は以下の資料をご参照ください。

技術メモ － 安全な Web ブラウザの使い方
https://www.jpcert.or.jp/ed/2008/ed080002_1104.pdf

（3）マルウエア（malware）

コンピュータウイルスやワームなどの、悪意のあるソフトウエアに関連する件数は 2154 件でした。大半がマレーシアのセキュリティ対応機関からのマルウエアに関する届出です。これは、この組織が大規模にマルウエアの設置サイトの調査を行い、その調査で得られた情報のうち、日本に関連する情報を JPCERT/CC へ提供してくれているものです。この届出も含め、マルウエアに関連して届け出られたインシデントに関係する IP アドレスの数は 2154 件に達しました。非常に多数のサイトが関連しており、マルウエアに関する脅威が潜在化して大規模に広がっている可能性があります。JPCERT/CC ではマルウエアの解析や脅威分析を行い、影響が大きいと考えられるものについて関係組織に対して通知を行っています。

JPCERT/CC に対してマルウエアに関する情報をご提供いただくことにより、マルウエアの配布元を閉鎖する等の調整が可能となります。被害拡大を抑止するためにも、早期の情報提供にご協力をお願い致します。

（4）プローブ、スキャン、その他不審なアクセス（scan）

侵入行為の試み（未遂に終わったもの）や、コンピュータやサービス、脆弱性の探査を意図したアクセス、その他の不審なアクセス等、システムへの影響が直接生じない、または特別な対応を必要としないアクセス（本稿では「scan」と称します。）の件数は 469 件でした。

届出を受けた Scan については、TCP139、TCP445 番ポートに対する OS の脆弱性を探査するアクセス、TCP80 番ポートに対する Web アプリケーションの脆弱性を探査するアクセスや、TCP22 番ポートに対する SSH サービスへのブルートフォース攻撃が依然として多数見られます。

特に届出の多かった TCP139、TCP445 番ポートに対するアクセスは、MS03-026、MS08-067 など、Windows の脆弱性を攻撃するアクセスでした。既知の脆弱性も常に狙われています。TCP139、TCP445 番ポートが、ルータや FW などの対策により、インターネットから直接アクセスすることができなくなっていても、マルウエアに感染したコンピュータをローカルネットワークに接続するとローカルネットワーク内で感染が拡大する可能性もありますので、ローカルネットワークに接続しているコンピュータであっても、OS を含む、コンピュータで使用しているすべてのソフトウエアを最新の状態に保つとともに、ウイルス対策ソフトを導入し、またウイルス定義ファイルを常に最新の状態に保つなどの

対策を行うことをお勧めします。

JPCERT/CC では、届出者から調整の依頼がある場合について、アクセス元の管理者に対し、調査対応依頼を行っています。

Scan は、一般的に自動化ツールを用いて広範囲のホストに対して行なわれています。正式リリース前のテストサーバなど、セキュリティ対策を施していないホストを不用意に設置すると、脆弱性の存在を検出され、ホストへの侵入等深刻なインシデントに繋がる可能性があります。

（5） 送信ヘッダを詐称した電子メールの配送（forged）

差出人アドレス等の送信ヘッダを詐称した電子メールの配送の事例はありませんでした。

（6）その他（other）

上記（1）から（5）に分類されないその他のインシデントの件数は 187 件でした。

「other」に含まれるインシデントのうち、特筆すべきものの一つは、キーロガーにより抜き取られたとみられる日本人向けの複数のサービスに関連した ID、パスワード、その他の個人情報などが海外 CSIRT より提供された事案です。JPCERT/CC では、該当するサービス提供事業者へ情報を提供(*4)しました。

> * 4: JPCERT/CC ではこのようなキーロガーの情報を受け取った場合、金融機関、ポータルサイト事業者、ISP、ソーシャルネットワークサービス（SNS）など、情報を悪用された場合の被害が深刻であると考えられるサービスに関する情報を優先して調整しています。また、二次被害等のトラブルを避けるため、適切に対処していただけることが確認できた組織に対してのみ情報を提供します。なお、提供した情報への対処方法（顧客への注意喚起等）については、各組織のポリシーを尊重し、情報提供先の事業者に全面的に委ねています。

他には、韓国のサイトに対して、日本の複数の IP アドレスからサービス運用妨害(*4)が行われているとの連絡を韓国 KrCERT/CC から受け、国内の管理者に対して調査対応依頼を行った事案がありました。また、国内事業者から、公開している Web サイトがサービス運用妨害を受けているとの連絡を受け、攻撃元の国外の管理者及び関係協力組織に対し、調査対応依頼を行った事案もありました。

* 4 韓国のサイトに対するサービス運用妨害の概要については、四半期報告「早期警戒 ー情報収集・分析ー【 2009 年第 3 四半期(7-9 月)の動向について】」を参照してください。

● 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・閉鎖を目的としたコーディネーションを行ったり、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、国内における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お願い致します。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。

インシデント報告の届出
https://www.jpcert.or.jp/form/

届出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ご提供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