JPCERT-IR-2008-0002

発行日: 2008-10-09

JPCERT/CC インシデントハンドリング業務報告
[2008 年 7 月 1 日 ～ 2008 年 9 月 30 日]

JPCERT/CC が 2008 年 7 月 1 日から 2008 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）に関する届出は 1348 件でした。実際に届出を受けたメール及び FAX の数は、延べ 1786 通（*1）で、インシデントの件数を IP アドレス別に集計すると 1493 アドレスになります。

*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、届出件数とメール及び FAX の数が異なっています。

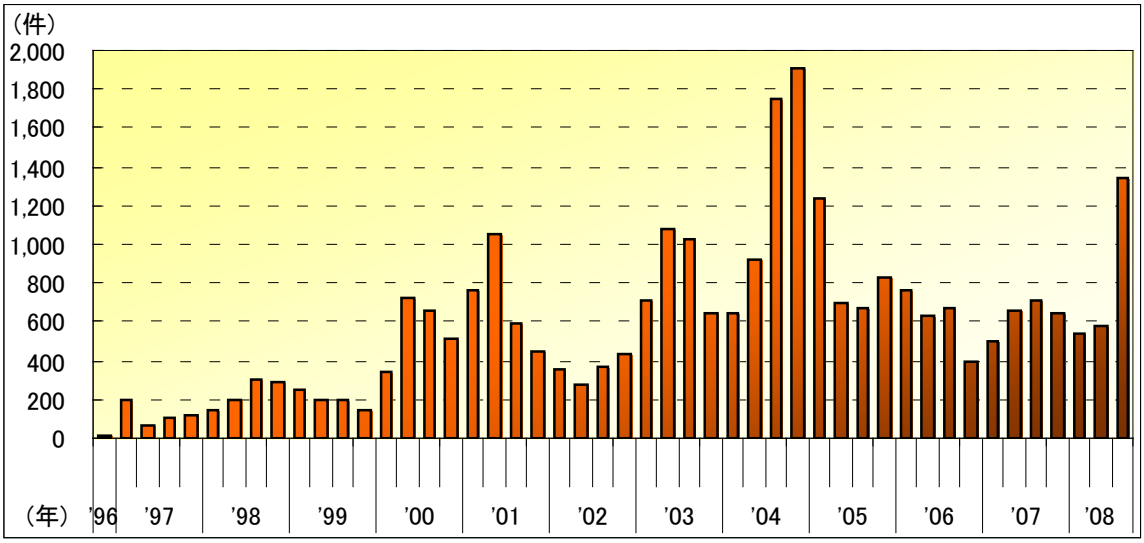


図 1「インシデント件数の推移」

インシデントの届出分類、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をトップレベルドメインで分類したもののうち、件数の多いドメインは、以下のとおりです。今四半期は、特に国内からのインシデントの届出が増えました。

.jp	1028 件
.com	389 件
.org	187 件
.br	67 件
.pl	20 件

【参考】前四半期（2008 年 4 月 1 日から 6 月 30 日）の送信元件数

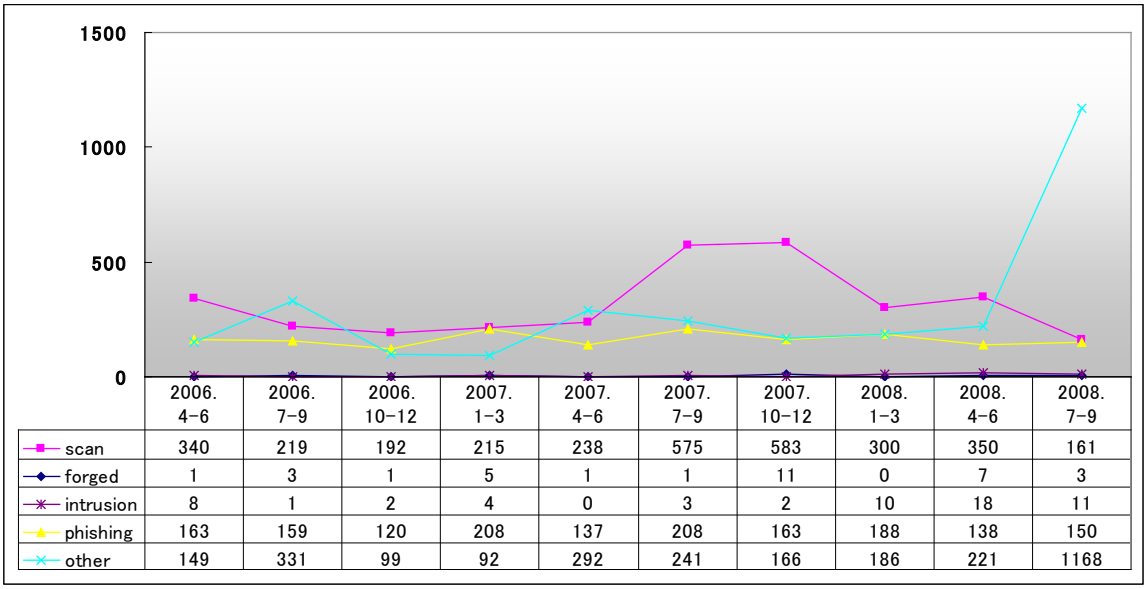
.jp	169件
.com	119件
.net	75件
.de	13件
.cn	11 件

- **インシデントの届出より派生した通知連絡**

JPCERT/CC が国内外の関連するサイトに通知連絡した件数は 444 件です。この「通知連絡」とは、連絡仲介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 や iframe のスクリプトタグ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、マルウエアに感染した後に別のマルウエアを取得する為にアクセスする先のサイト、「scan」のアクセス元等の管理者及び関係協力組織に対し、調査対応依頼の連絡を行ったものです。

- **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の推移は、以下の図のとおりです。インシデントの傾向としては、「other」に含まれる「マルウエア情報に関する届出」が増加しました。逆に、「scan」に関するインシデントの届出が減少しています。



	2006. 4-6	2006. 7-9	2006. 10-12	2007. 1-3	2007. 4-6	2007. 7-9	2007. 10-12	2008. 1-3	2008. 4-6	2008. 7-9
scan	340	219	192	215	238	575	583	300	350	161
forged	1	3	1	5	1	1	11	0	7	3
intrusion	8	1	2	4	0	3	2	10	18	11
phishing	163	159	120	208	137	208	163	188	138	150
other	149	331	99	92	292	241	166	186	221	1168

図 2「インシデントタイプ別報告件数推移」

（1）プローブ、スキャン、その他不審なアクセス（scan）

防御に成功したアタックや、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、または無視できるアクセスについての届出は 161 件でした。
このようなアクセスは、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。セキュリティ対策を施さずにホストを放置していると、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。

80（http）	68 件
22（ssh）	58 件
5554 (sgi-esphttp)	4 件
1023	4 件
445 (microsoft-ds)	3 件
110 (POP3)	2 件

（2） 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についての届出は 3 件でした。この 3 件は、メールのヘッダを詐称して不特定多数に広告メールを送信するインシデントでした。

（3） システムへの侵入（intrusion）

管理者権限の盗用が認められる場合を含むシステムへの侵入についての届出は 11 件でした。Web サイトの改ざんが多数を占めました（11 件中 10 件）。改ざんされた Web サイトのページには主に、他のサイトへ誘導する JavaScript や iframe のスクリプトタグが埋め込まれています。結果として、そのサイトを閲覧したユーザのコンピュータ上で不正なスクリプトが実行され、マルウエアがインストールされる可能性があります。

JPCERT/CC では、SQL インジェクションを行っている IP アドレスの管理者に対し、攻撃の停止を目的とする調査対応依頼を行っています。また、SQL インジェクション攻撃により改ざんされた Web サイトの管理者に対する調査対応依頼や、改ざんされた Web サイトから誘導される先の Web サイトの管理者に対する「マルウエア配布の停止等」を目的とする調査対応依頼も行っています。

さらに、10 月に入り、新しい手法による SQL インジェクション攻撃に関する届出を受けています。SQL インジェクション攻撃は、依然として継続していますのでご注意ください。

（4）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「フィッシング行為」についての届出は 150 件でした。

フィッシングサイトに使用する Web ページを構築するために、システムに侵入する、もしくはドメインを乗っ取る等の行為があります。

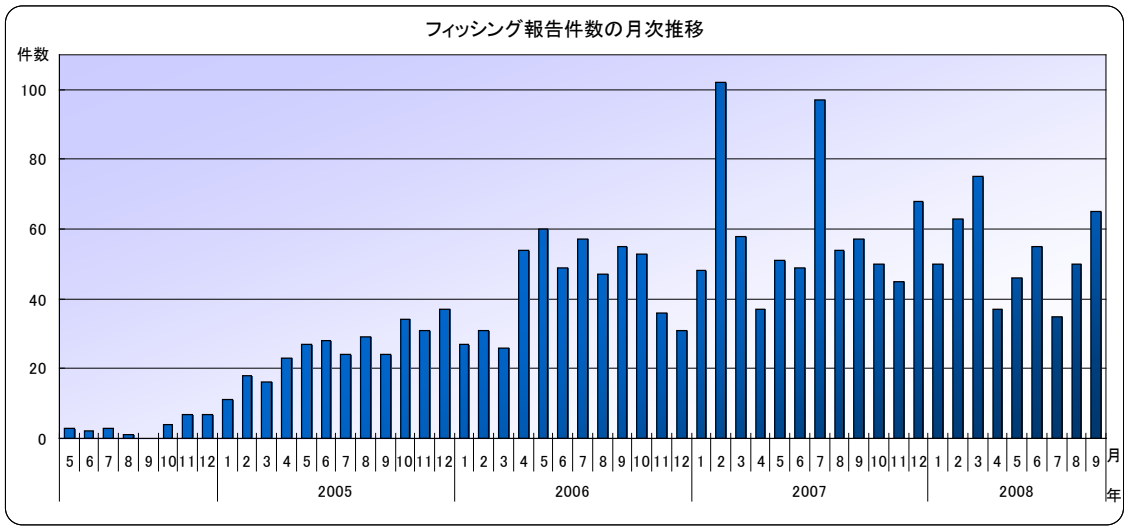


図 3「フィッシング報告件数推移」

以下は、装われたサイトの国内・国外別の件数を示しています。

国内のサイトを装ったフィッシングサイトの届出件数:　8 件 / 150 件 (*2)
国外のサイトを装ったフィッシングサイトの届出件数:138 件 / 150 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届出件数が 4 件ありました。

最近徐々に国内のサイトを装ったフィッシングサイトの届出が増えつつあります。今後もさらに国内サイトのフィッシングサイトが増えることが懸念されますので、オンラインサービスを利用する際は、個人情報を入力する前に、入力するサイトが正規のサイトであるかを確認することを推奨します。

【参考】前四半期（2008 年 4 月 1 日から 6 月 30 日）の国内・国外別の件数

国内のサイトを装ったフィッシングサイトの届出件数: 7件 / 138件
国外のサイトを装ったフィッシングサイトの届出件数: 122件 / 138件

（5）その他（other）

上記（1）から（4）に含まれないインシデント（サービス運用妨害"DoS"、コンピュータウイルス、マルウエアの情報等）の届出は 1168 件でした。今四半期は、マルウエア及び不審

なサイトに誘導するメールに関する届出が増えています。

「other」に含まれるインシデントのうち、特筆すべき事案としては、以下のものがあります。
2008 年 7 月下旬に海外組織から、日本国内の多数の学術系組織のシステム（52 組織 91 システム）がボットに感染している旨の情報提供を受け、それぞれの関係組織に対して、通知を行いしました。脆弱性が存在するテストサーバ等をそのまま放置したり、簡易なパスワードを設定したりすると攻撃者に侵入され、そのサーバにボットが設置されるケースもあります。ネットワークに接続するサーバを設置する場合は、侵入攻撃を受けること前提にして、可能な限り適切な対策を行うこと、ネットワークに接続されているサーバの状況の把握を継続することを推奨します。

届出を受けた「マルウエア情報」については、JPCERT/CC において、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は、対策に関する情報提供を行っています。また、解析によって明らかになった情報を基に、攻撃元 IP アドレスの管理者に対して「攻撃の停止」を目的とする調査対応依頼を行ったり、マルウエアの配布を行っているサイトの管理者に対して「マルウエア配布の停止等」を目的とする調査対応依頼も行ったりするなど、マルウエアによる被害の拡大を抑止するためのコーディネーション活動を行っています。
JPCERT/CC に対してマルウエア情報に関する報告を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コーディネーション活動につなげることが可能となり、他のユーザへの被害拡大を抑止することが可能となります。

● インシデント以外の報告について

JPCERT/CC では、インシデント対応方法等に関する質問や相談、APCERT 事務局窓口に対するインシデント報告等も寄せられており、その件数は 36 件でした。

● 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以下の URL をご参照ください。

JPCERT CC®

インシデント報告の届出
http://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。以下の URL から入手できます。

公開鍵
https://www.jpcert.or.jp/jpcert.asc

PGP Fingerprint：
BA F4 D9 FA B8 FB F0 73 57 EE 3C 2B 13 F0 48 B8

本文書を転載する際には JPCERT/CC(office@jpcert.or.jp)まで確認のご連絡をお願いします。
最新情報については JPCERT/CC の Web サイトを参照してください。
JPCERT コーディネーションセンター（JPCERT/CC）
http://www.jpcert.or.jp/