JPCERT-IR-2008-0001
発行日: 2008-07-07

JPCERT/CC インシデントハンドリング業務報告
[2008 年 4 月 1 日 ～ 2008 年 6 月 30 日]

JPCERT/CC が 2008 年 4 月 1 日から 2008 年 6 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 584 件です。実際に届出を受けたメール、FAX の数は、延べ 768 通（*1）で、インシデントの件数を IP アドレス別に計上すると 734 アドレスです。

*1: 届出のメール、FAX には異なる届出者の方から同一サイトのインシデント情報が含まれるため、届出件数とメール、FAX の総数が異なっています。

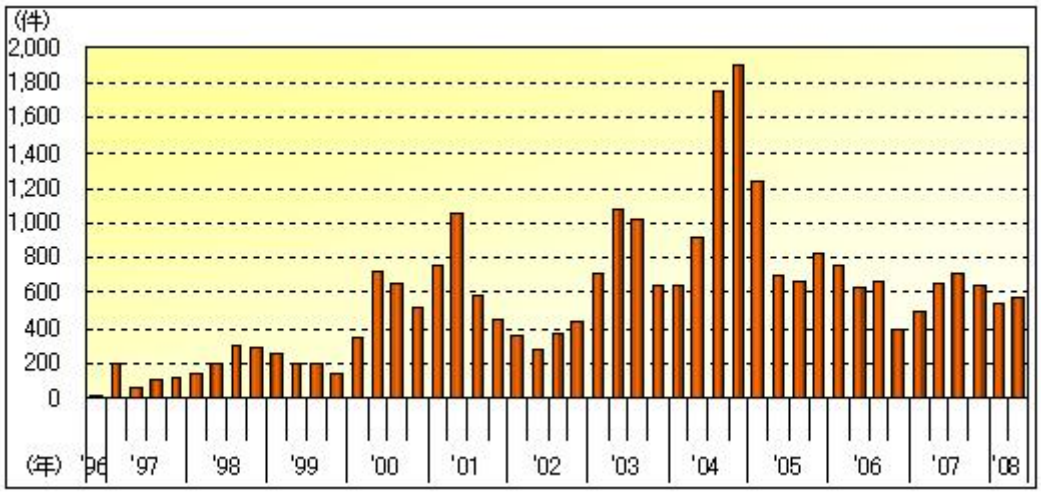


図 1「インシデント件数の推移」

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、件数の多いものは、以下の通りです。

.jp	169 件
.com	119 件

.net　　75 件
.de　　13 件
.cn　　11 件

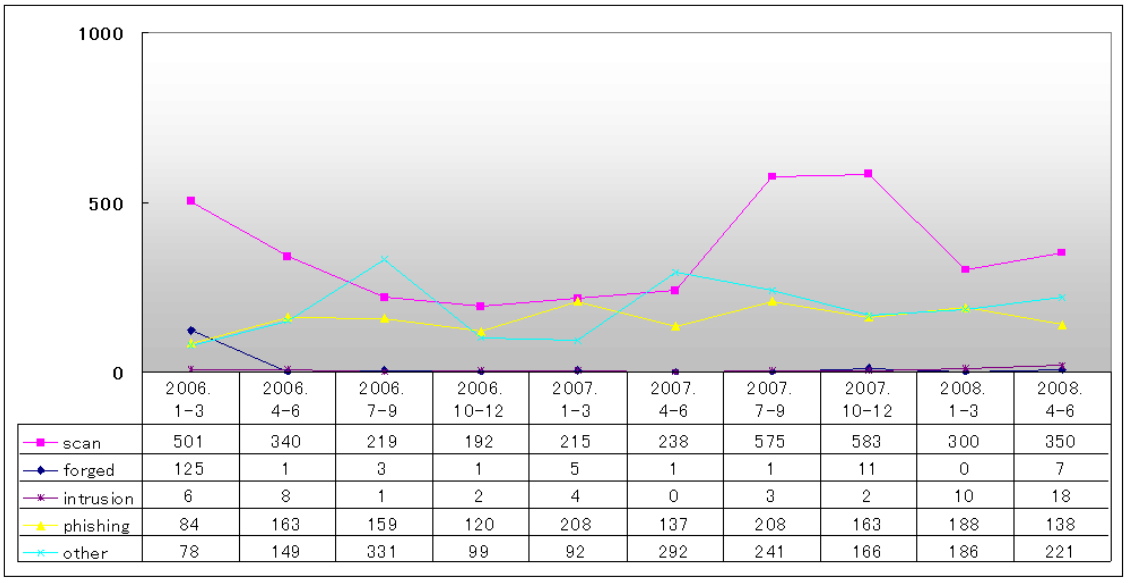
● インシデントの届出より派生した通知連絡

JPCERT/CC が国内外の関連するサイトに通知連絡した件数は 465 件です。この通知連絡の件数はフィッシングサイトが設置されているサイトや、有害なサイトへ誘導するコードを埋め込まれた改ざんされたサイト、悪意のあるウイルス等マルウェアが置かれたサイト、Scan のアクセス元等の管理者及び関係協力組織への連絡仲介依頼を含むインシデントの届出に基づいて行ったものです。

● 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となります。インシデントの傾向としては SQL インジェクションに関する届出の増加による「intrusion」の増加があります。また、「phishing」では、若干減少傾向にあるものの国内外の金融機関のフィッシングサイトが引き続き多くあります。

なお、フィッシングは多くの場合、サーバへの侵入「intrusion」を伴います。フィッシングの加害者とならないためにも、サーバ管理者の方は侵入へのセキュリティ対策を心がけてください。



	2006. 1-3	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
scan	501	340	219	192	215	238	575	583	300	350
forged	125	1	3	1	5	1	1	11	0	7
intrusion	6	8	1	2	4	0	3	2	10	18
phishing	84	163	159	120	208	137	208	163	188	138
other	78	149	331	99	92	292	241	166	186	221

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生じない、または無視できるアクセスについての届出は 350 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）	222 件（*2）
22（ssh）	114 件（*2）
5900（vnc-server）	5 件（*2）
21（ftp）	4 件（*2）
139	4 件
10000（ndmp）	1 件（*2）

*2: ワームによる感染の試みやワーム等によって設置されたバックドアからの侵入の試みと思われるアクセスが報告されています。

（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 7 件でした。中には、アドレスを詐称した広告メールを不特定多数に送り、その中で存在しないメールアドレスに対して送信した結果、大量のエラーメールが差出人に配送される例もあります。

（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 18 件でした。侵入方法としては、次のような事例が報告されています。

脆弱なパスワードを総当り攻撃、辞書攻撃で解読され侵入される
SQL インジェクション攻撃
Web のアクセス解析ツールの脆弱性を利用して侵入

また、今回受領した届出において侵入後に行なわれた操作のうち、主なものを以下に紹介します。

システムの改ざん（ファイルの置き換え、ログの改ざん、Web ページの改ざん等）
メール送信ツールの設置とメールの送信

（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、国内 ISP 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 138 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。以下は、届出において国内・国外のサイトを装ったそれぞれ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:　7 件 / 138 件 (*3)
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 (*3)

*3: 装うサイトがわからない届出件数が 9 件ありました。

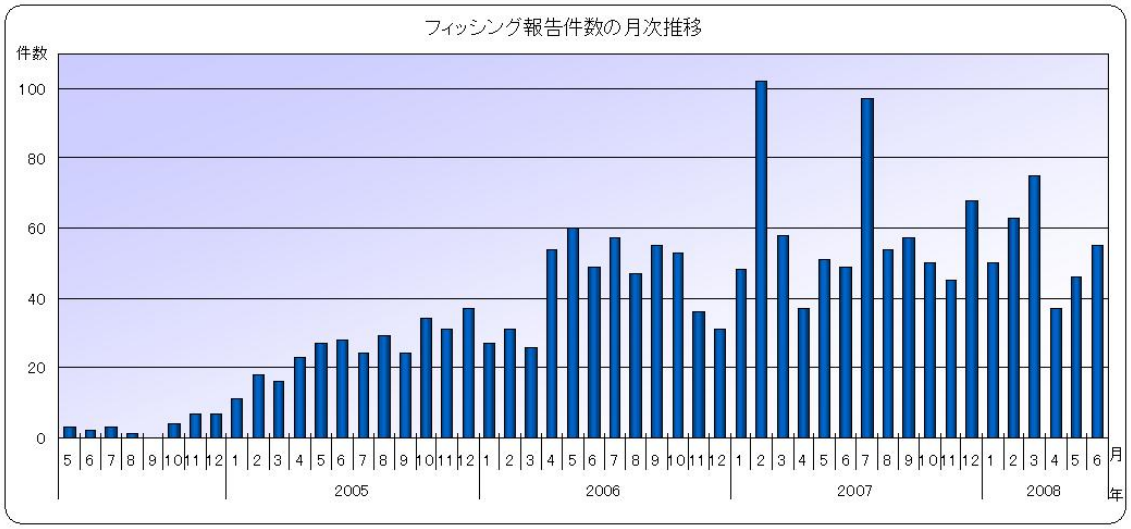


図 3「フィッシング報告件数推移」

（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、マルウェアの情報等）の届出は 221 件でした。

マルウェア情報については影響が大きいと考えられるものや分析依頼を受けているものについて分析を実施して、対策に関する情報提供を行っています。また、マルウェアが設置されているサイトへ確認と削除依頼も実施しています。

● 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何らかの対応が必要な相談、の届出は 19 件でした。一部を以下で紹介します。

国外のインシデント事例に関する情報提供
APCERT 事務局窓口宛に来たインシデント報告の対応
JPCERT/CC が関連する事業に関しての問い合わせ

インシデントによる被害の拡大・再発防止のため、今後とも JPCERT/CC への情報提供にご協力お願い致します。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。

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

JPCERT/CC の PGP 公開鍵は、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/