JPCERT-IR-2009-0002
発行日: 2009-04-07

JPCERT/CC インシデントハンドリング業務報告
[2009 年 1 月 1 日 ～ 2009 年 3 月 31 日]

JPCERT/CC が 2009 年 1 月 1 日から 2009 年 3 月 31 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）	564 件（946 通）
インシデント対象 IP アドレス数	684 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。

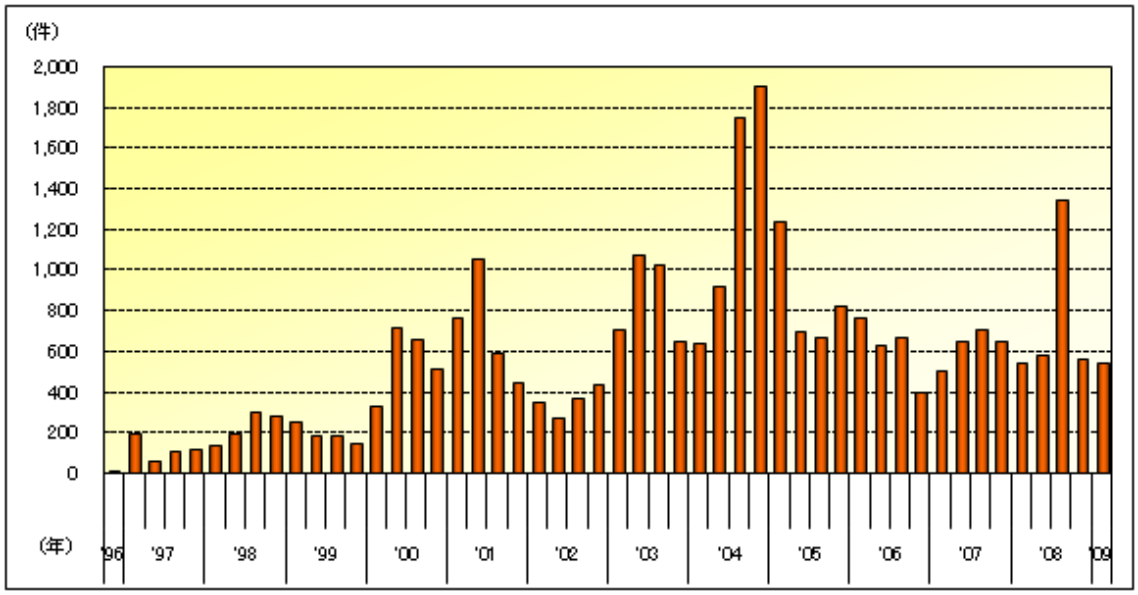


図 1：インシデント報告件数の推移

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、次のとおりです。

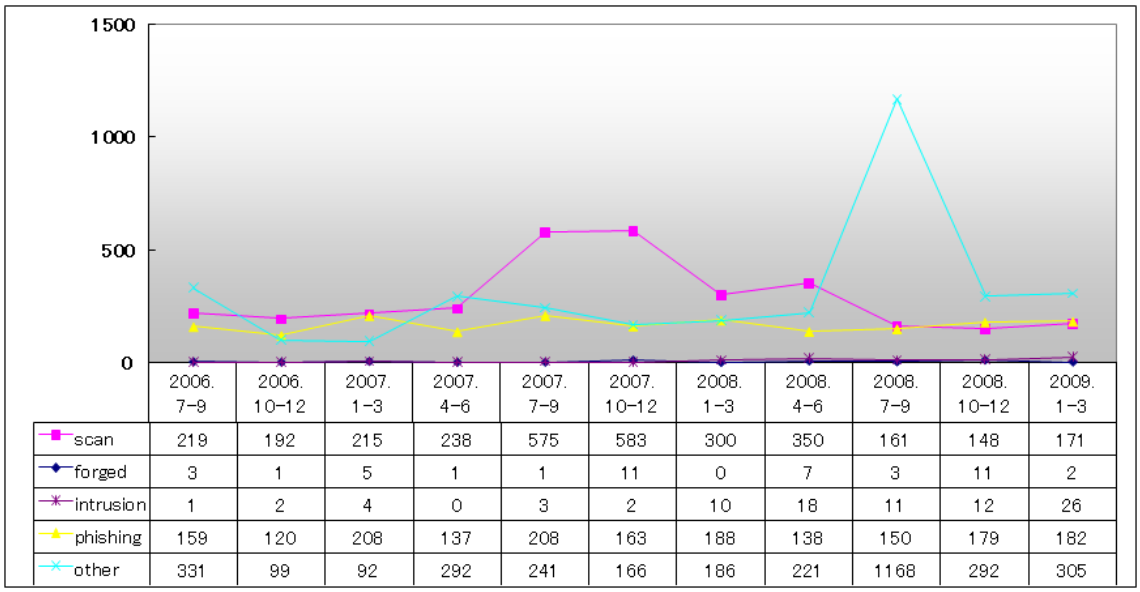
当四半期 (2009 年 1 月～3 月)		前四半期 (2008 年 10 月～12 月)	
.jp	1) 321 件	.jp	1) 283 件
.org	2) 209 件	.org	2) 240 件
.com	3) 189 件	.com	3) 199 件
.br（ブラジル）	4)　84 件	.br（ブラジル）	4)　61 件
.de（ドイツ）	5)　36 件	.pl（ポルトガル）	5)　49 件

- **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 388 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 や iframe が埋め込まれているサイト、ウイルス等のマルウェアが設置されたサイト、マルウェアに感染した後に別のマルウェ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、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の推移は、図 2 のとおりです。フィッシングの報告が若干増えました。



	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	2008. 10-12	2009. 1-3
scan	219	192	215	238	575	583	300	350	161	148	171
forged	3	1	5	1	1	11	0	7	3	11	2
intrusion	1	2	4	0	3	2	10	18	11	12	26
phishing	159	120	208	137	208	163	188	138	150	179	182
other	331	99	92	292	241	166	186	221	1168	292	305

図 2：タイプ別インシデント件数推移

（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、または特別な対応を要しないアクセス(本項では「scan」と称します。)についての届出は 171 件でした。

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、対応の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。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）	89 件
22（ssh）	58 件
1434 (ms-sql-m)	15 件
6667 (ircd)	1 件
110 (pop3)	1 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 2 件でした。電子メールのヘッダを詐称したメールが配送されたインシデントです。

（3） 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についての届出は 26 件でした。Web サイトの改ざんが多数を占めました（26 件中 20 件）。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 JavaScript や iframe のスクリプトタグが埋め込まれているケースが少なくありません。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、マルウェアがインストールされる可能性があります。

被害拡大の抑止を目的として、JPCERT/CC では、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を行っています。また、改ざんされたサイトから誘導されるマルウェアの公開サイトの管理者に対しても調査対応依頼を行っています。

フィッシングや SQL インジェクションなど、Web サイト、Web アプリケーションに関連するインシデントが定常的に報告されています。また、正規サイトであっても改ざんされている可能性がありますので、一般ユーザにおかれましては、いかがわしいサイトにはアクセスしないからと油断せず、OS や Web ブラウザを最新に保つ、ウイルス対策ソフトを導入し、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覧ください。

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

システム管理者におかれては、自分が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ェアなどに脆弱性が無いかなど定期的に確認されるよう推奨します。

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」
http://www.ipa.go.jp/security/vuln/websecurity.html

SQL インジェクションによる Web サイト改ざんに関する注意喚起
http://www.jpcert.or.jp/at/2008/at080005.txt

（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 182 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のリソースを獲得するために、先行して、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なされている場合あります。

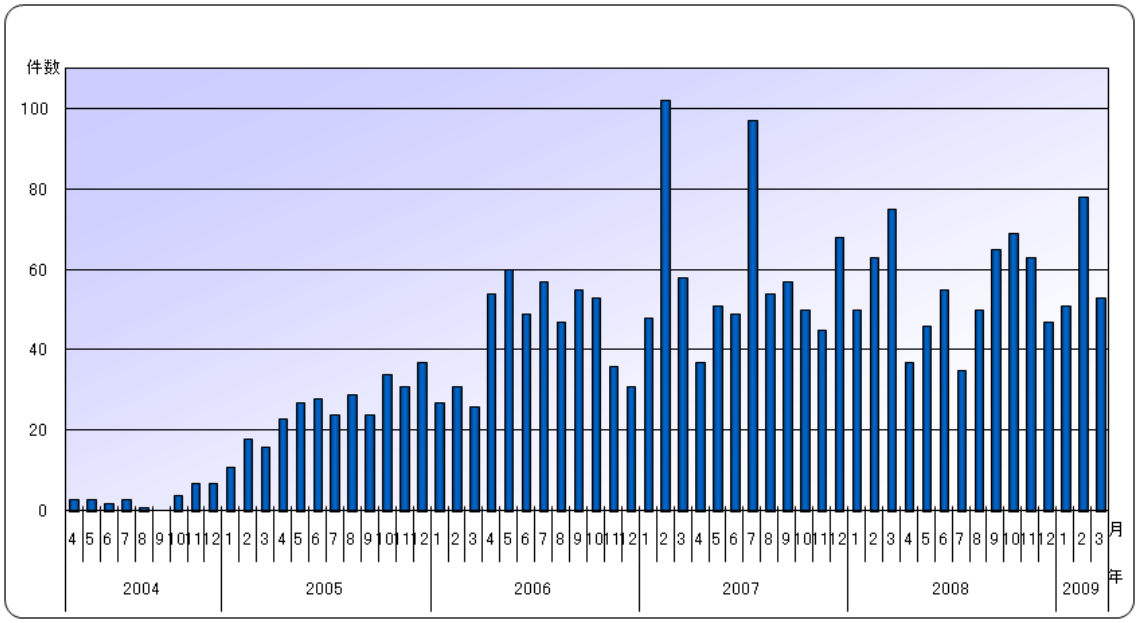


図 3：フィッシング件数推移

次の数は、装われたサイトの国内・国外別の件数を示しています。

国内のサイトを装ったフィッシングサイトの届出件数:　25 件 / 182 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: 143 件 / 182 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 14 件ありました。

国内のサイトを装ったフィッシングサイトの届出が、前四半期の 10 件から、今期は 25 件に増えています。オンラインサービスにおいて個人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されるよう推奨します。

もし、フィッシングサイトに個人情報等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（2008 年 10 月 1 日から 12 月 31 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:　10 件 / 179 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: 155 件 / 179 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、マルウェアの情報等；以下「other」といいます。）の届出は 303 件でした。

「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、次のものがあります。

海外 CSIRT より、キーロガーにより抜き取られたとみられる ID、パスワード、その他の個人情報など、日本で提供するサービスの利用に関連した情報の提供があり、JPCERT/CC では、該当するサービス提供事業者への情報提供を行いました。金融機関、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を優先し、適切な情報の利用等に関する認識が共有できた組織に対し、情報提供を行っています。なお、提供する情報の利用の方法（顧客に対する注意喚起において参照する等）については、各組織のポリシーに依存する問題であることから、情報の具体的な利用方法は、情報提供先であるサービス提供事業者に全面的に委ねています。

また、届出を受けた「マルウェア情報」については、JPCERT/CC において、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。解析によって明らかになった情報をもとに、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、マルウェアの配布を行っているサイトの管理者に対して「マルウェア配布の停止等」を目的とする調査対応依頼も行ったりするなど、マルウェアによる被害の拡大を抑止するための調整（コーディネーション）活

動を行っています。

JPCERT/CC に対してマルウェア情報に関する報告をいただくことにより、マルウェ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 33 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下記の 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/

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/jpcert.asc

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