JPCERT CC®

JPCERT-IR-2010-0002
発行日: 2010-04-08

JPCERT/CC インシデントハンドリング業務報告
[2010 年 1 月 1 日 ～ 2010 年 3 月 31 日]

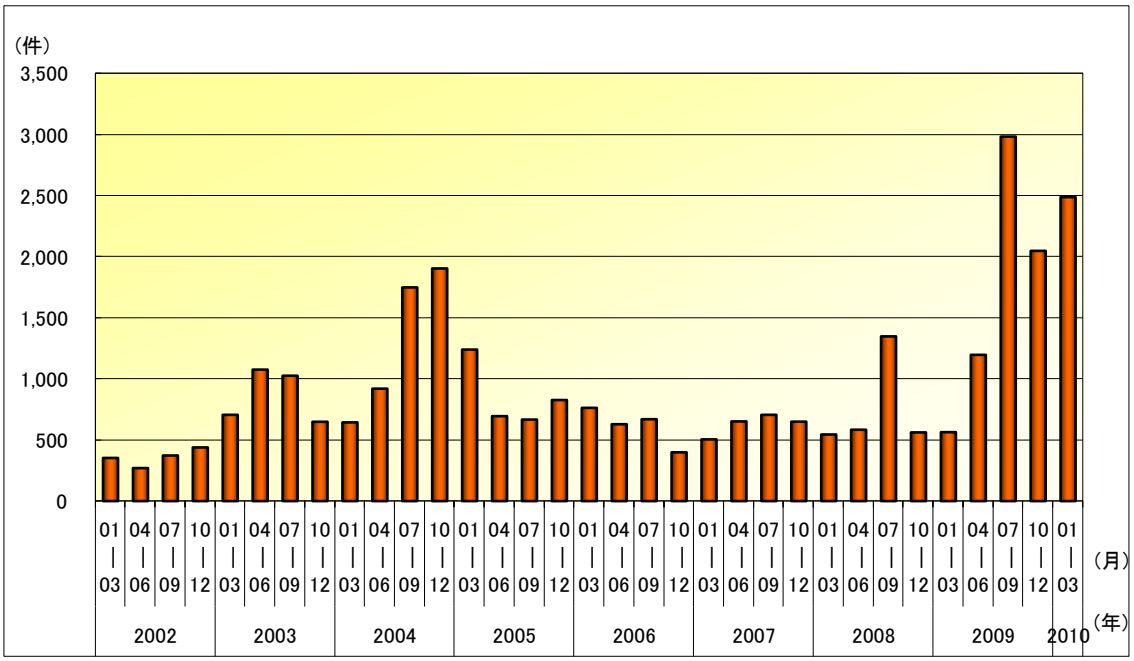
JPCERT/CC が 2010 年 1 月 1 日から 2010 年 3 月 31 日までの間に受け付けた報告のうちコンピュータセキュリティインシデント（以下「インシデント」といいます。）に関する報告は次のとおりでした。

【注】本業務報告では、インシデント「報告の件数」と「インシデントの件数」の用語を使い分けています。「報告の件数」は報告者から寄せられた Web フォーム、メール、FAX による報告の総通数のうち重複する（同一の事象に関する）ものを除いた数を示し、「インシデント件数」は報告に係るインシデントが関係している対象システムを IP アドレスベースで計上した数を示しています。

報告の件数*1	2,488 件
Web フォームメール、FAX の延数	3,498 通
インシデントの件数（インシデント対象 IP アドレス数）	3,193 アドレス

*1:同一のインシデント事象に関する情報が異なる報告者から寄せられるため、報告件数は Web フォーム、メールおよび FAX による報告の通数の合計よりも少なくなっています。

図 1 のとおり、報告件数が前四半期と比較して約 2 割増加しました。



[図 1：インシデント報告件数の推移]

インシデント報告の分類、傾向等の詳細は、以下のとおりです。

● インシデントの報告の送信元による分類

JPCERT/CC が受け付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 位は、[表 **1** のとおりです。

[表 1：インシデント報告の上位ドメイン]

本四半期 （2010 年 1 月～3 月）		前四半期 （2009 年 10 月～12 月）	
.jp（日本）	1） 1294 件	.my（マレーシア）	1） 1103 件
.my（マレーシア）	2） 1020 件	.jp	2） 802 件
.com	3） 608 件	.com	3） 180 件
.org	4） 169 件	.br（ブラジル）	4） 127 件
.br（ブラジル）	5） 150 件	.org	5） 124 件

2010 年 1 月 8 日に JPCERT/CC から「Web サイト改ざんに関する情報提供のお願い」を公開したところ、国内から多くの情報提供をいただきました。ご協力ありがとうございました。

Web サイト改ざんに関する情報提供のお願い
https://www.jpcert.or.jp/pr/2010/pr100001.txt

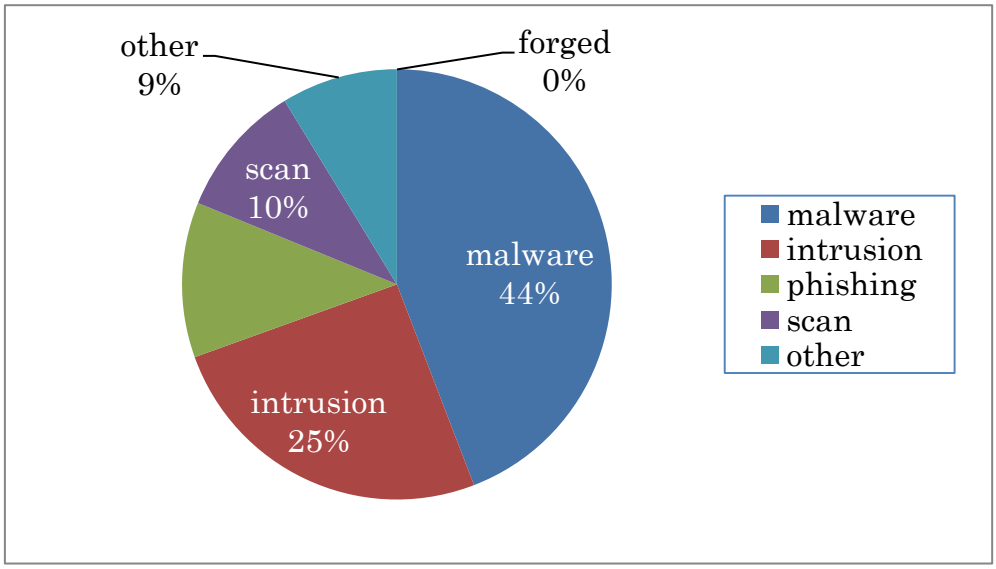
● インシデントの報告に基づく調整件数

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 1,005 件でした。前四半期と比較して約 7 割増加しています。ここでいう「調整」とは、インシデントの拡大防止のため、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および関係協力組織に対し、現状の調査と問題解決のための対応を中立的な調整機関の立場から依頼する活動です。

JPCERT/CC は、国際的な連携の元でインシデント対応の調整を行う日本の窓口組織として、インシデントの認知と解決、インシデントによる被害拡大の抑止に貢献しています。

● インシデントのタイプ別分類

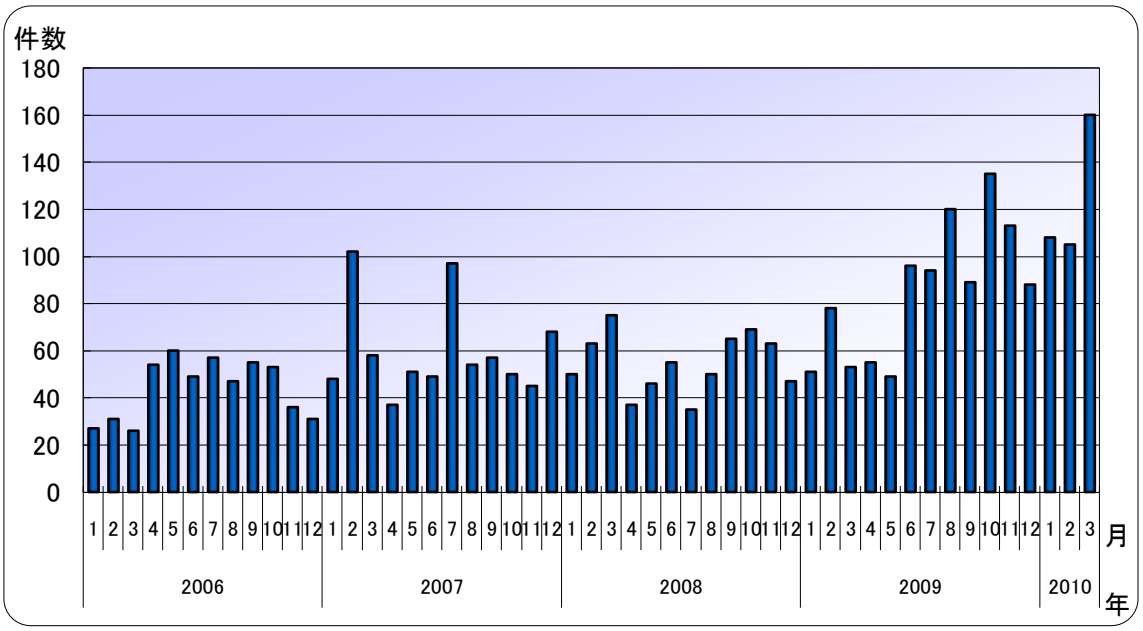
JPCERT/CC では報告を受けたインシデント（インシデントが発生している対象ホスト）をタイプ別に分類しています。本四半期におけるタイプ別分類割合は、[図 **2** のとおりです。マルウエアに関するインシデント（malware）が約 44%を占めています。また、Web 改ざんによるインシデント（intrusion）が、前四半期は 17%でしたが、本四半期は 25%に増えています。



[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を装い、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」のインシデントは、373 件でした。前四半期の 336 件から若干増加しました。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は、前四半期の 141 件から、77 件と減少しています。ただし、月別の傾向でみると 1 月 2 月は減少していましたが、3 月に入り国内ブランドを装ったフィッシングが再び増加に転じていますので、注意が必要です。図 3 は、フィッシングに関する報告の件数の 1 か月ごとの推移を示しています。



[図 3：フィッシング件数推移]

以下の件数は、フィッシングサイトの被害ブランドの国内・国外別の件数を示しています。

国内のブランドを装ったフィッシングサイトの件数:　77 件　（*3）
国外のブランドを装ったフィッシングサイトの件数: 219 件　（*3）

*3: 被害ブランドを確認できなかったフィッシングサイトの件数は 77 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の管理者に対して、「フィッシングサイトの停止」の依頼を行っています。

Web サイトでアカウント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確認してください。もし、フィッシングサイトにアカウント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相談し、ID、パスワード等の変更手続きを行ってください。

【参考】フィッシング対策

フィッシング対策ガイドライン（PDF）
https://www.antiphishing.jp/antiphishing_guide.pdf

フィッシングフィルのページ
https://www.antiphishing.jp/phil/index.html

【参考】前四半期（2009 年 10 月 1 日から 12 月 31 日）の国内・国外別の件数

国内のブランドを装ったフィッシングサイトの件数: 141 件　（*4）
国外のブランドを装ったフィッシングサイトの件数: 185 件　（*4）

*4: 被害ブランドを確認できなかったフィッシングサイトの件数は 10 件ありました。

（2） システムへの侵入（intrusion）

システムへの不正侵入に関するインシデントは、809 件でした。前四半期の 372 件から大幅に増加しました。本四半期の報告のすべてが、Web サイトで公開しているファイルに不審な JavaScript が埋め込まれる改ざんに関するものでした。これらは、前四半期から続く改ざんと同様の事例です。

JPCERT/CC では、Web サイトの管理者に対して「改ざんの修正」の依頼を行うほか、改ざんされたサイトを閲覧した利用者の PC から窃取された情報が送信される先の特定及び活動の停止に関する調整を行っています。
Web サイトの改ざんに関する報告は、2010 年 1 月をピークに徐々に減少しているものの、依然として報告され続けており、対策が広く実施されたとは言い難い状況にあります。また、改ざんされた Web サイトの修正が終了した後、そのサイトが再び改ざんされる事例もいくつか確認しています。Web サイトの改ざんへの対応に当たっては、挿入された不審なスクリプトを削除する等の表面的な対応だけではなく、改ざんを誘発した原因の追究とそ

の除去が重要です。また、管理している Web ページが改ざんされていないか（閲覧者をマルウエア配布サイトに誘導する不審なスクリプトの挿入等の形跡がないか）定期的に確認してください。

（3）マルウエア（malware）

マルウエアの配布サイトに関するインシデントは、1,410 件でした。前四半期の 1,149 件から増加しました。これは、上記(2)で説明した改ざんサイトから誘導されるマルウエア配布サイトが増加していることと、3 月後半からマレーシアのセキュリティ対応機関からの報告が増加していることによるものです。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、マルウエアを公開しているサイトの管理者に対して「マルウエアの削除」の依頼を行っています。

JPCERT/CC にマルウエアに関する情報をご提供いただくことにより、マルウエアの配布サイトを停止させ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、情報提供の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）

システムへの侵入の試み（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、サービスの運用への影響が直接生じないアクセス（本稿では「scan」と称します。）のインシデントは、322 件でした。

JPCERT/CC では、報告者から調整の依頼がある場合は、Scan のアクセス元の管理者に対して、「アクセスの原因の調査、対応」の依頼を行っています。

報告を受けた Scan に関しては、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。

Scan は、一般的にマルウエア等により広範囲のホストに対して行われています。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インターネット上に設置することは、たとえ短時間でも極めて危険です。インターネットに接続する場合は、必ず適切なセキュリティ対策を行ってください。また、サービスの運用停止等で必要が無くなったサーバについては、放置せずインターネットから切り離してください。

（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に関するインシデント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は、279 件でした。本四半期は、数組織から DDoS 攻撃に関する相談がありました。JPCERT/CC ではアクセス数の特に多いアクセス元の管理者に対して、「アクセスの原因の調査、対応」の依頼を行っています。

また、JPCERT/CC では、この DDoS 攻撃に関連しているとみられるマルウエアを入手して解析し、関係組織等に情報共有を行っています。

●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、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/

インシデントの届出（Web フォーム）
https://form.jpcert.or.jp/

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

本活動は、経済産業省より委託を受け、「平成２１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。