JPCERT/CC®

JPCERT-IR-2010-0001
発行日: 2010-01-12

# JPCERT/CC インシデントハンドリング業務報告
## [2009 年 10 月 1 日 ～ 2009 年 12 月 31 日]

JPCERT/CC が 2009 年 10 月 1 日から 2009 年 12 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) | 2048 件(2414 通) |
| インシデント対象 IP アドレス数 | 2229 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。

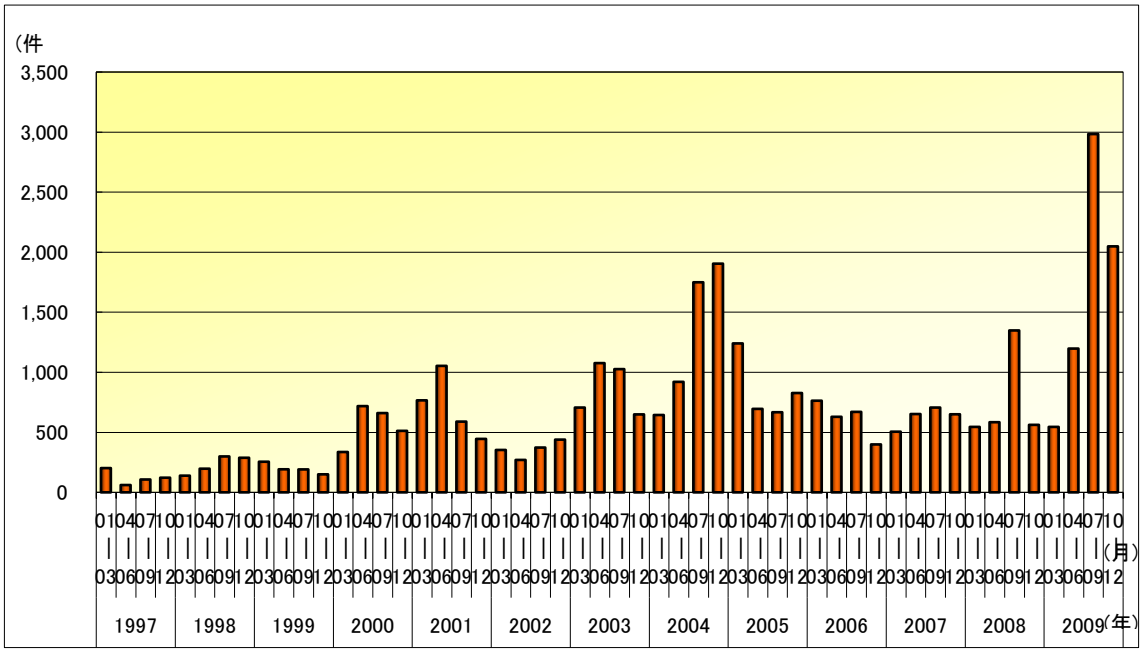


図 1：インシデント報告件数の推移

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、2009 年 5 月から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す。

表 1:インシデント報告の上位ドメイン

| 本四半期<br>(2009 年 10 月～12 月) | | 前四半期<br>(2009 年 7 月～9 月) | |
|---|---|---|---|
| .my(マレーシア) | 1) 1103 件 | .my(マレーシア) | 1) 2061 件 |
| .jp | 2) 802 件 | .jp | 2) 605 件 |
| .com | 3) 180 件 | .org | 3) 172 件 |
| .br(ブラジル) | 4) 127 件 | .com | 4) 165 件 |
| .org | 5) 124 件 | .br(ブラジル) | 5) 156 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 576 件でした。ここでいう「調整」とは、インシデントの届出に記載された攻撃元などに対する連絡調整等の依頼に基づいて、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。

● 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約 5 割を占めています。また、前四半期と比較して、phishing と intrusion の届出が増加しました。

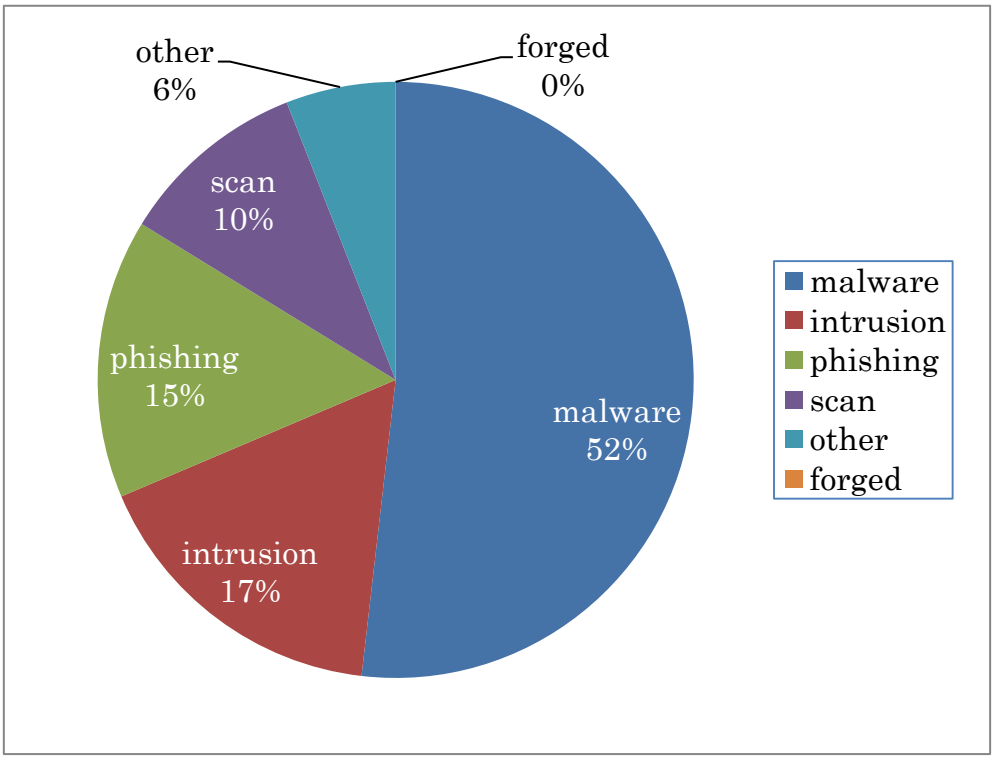


図 2：タイプ別インシデント件数割合

(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」の件数は、336 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 104 件から、141 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報告されたためです。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が広く流通している可能性があります。

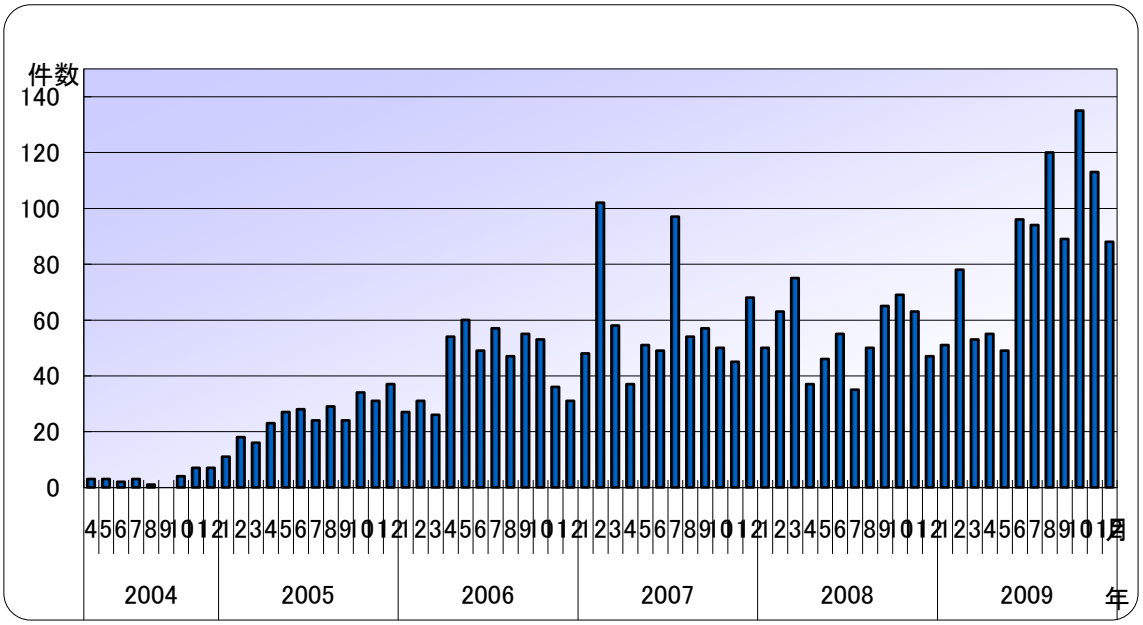


図 3：フィッシング件数推移

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: 141 件 (*2)
国外組織を装ったフィッシングサイトの件数: 185 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 10 件ありました。

JPCERT/CC では、届出に基づき、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」を依頼する調整を行っています。

Web サイトで ID,パスワード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 ID,パスワード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 7 月 1 日から 9 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: 104 件 (*3)

国外組織を装ったフィッシングサイトの件数: 192 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 7 件ありました。

(2) システムへの侵入(intrusion)

本四半期は Intrusion の報告が前四半期の 28 件から 372 件に大幅に増加しました。この大半は、前々四半期(2009 年 4 月 1 日から 2009 年 6 月 30 日)にも多数発生した JSRedir-R/Gumblar(以下「Gumblar」といいます。)による攻撃がさらに高度化・複雑化した事例です。この攻撃による事例では、不正なスクリプトを埋め込まれた Web ページ(以下「改ざんサイト」といいます。)をユーザが閲覧し、マルウエアを配布するサイトに誘導された場合、ユーザの PC 等がマルウエアに感染する可能性があります。

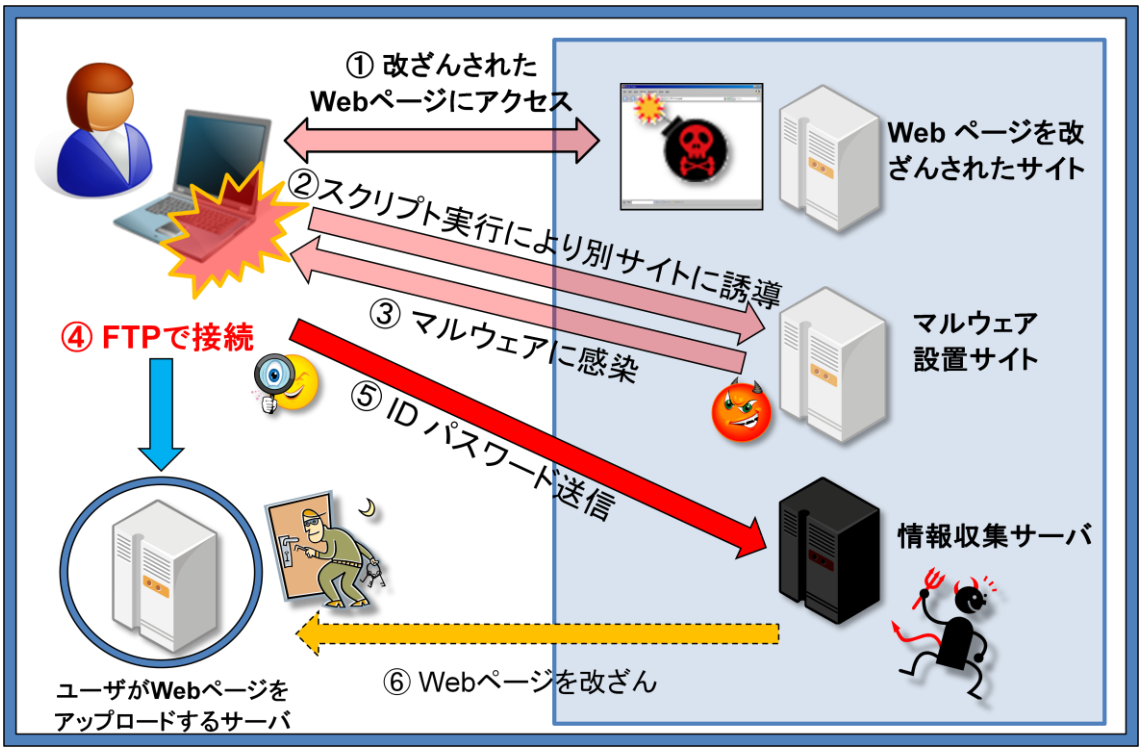


図 4: Gumblar によるインシデント

本四半期に多く報告された攻撃は、一見、前々四半期の Gumblar による攻撃に類似しているようにみえるものの、攻撃メカニズムが大きく変化しています。

表 2 :FTP アカウント盗用攻撃の比較

| | 2009 年 9 月以前 | 2009 年 10 月以降 |
|---|---|---|
| Web ページを改ざんされたサイト | 数百サイト | 数百サイト |
| マルウエア配布サイト | 数サイト | 数百サイト |
| 情報収集サイト | 不明 | 数サイト |

Gumblar をはじめとする FTP アカウント盗用攻撃によるインシデントでは、攻撃者は、まず、マルウエアに感染した PC から FTP のアカウント(ユーザ ID、パスワード)情報を窃取します。次に、窃取したアカウント情報を使って、Web サーバで公開されているページを改ざんすることで、その Web サイトを新たな攻撃用のサイトとして使用します。攻撃者は、このように攻撃用の改ざんサイトの数を徐々に増やして、被害を拡大させるという手法を取りました。前々四半期の事例では、改ざんサイトから誘導されるマルウエア配布サイトの数が比較的限定されていたため、JPCERT/CC では、その誘導先のマルウエア配布サイトを停止させる調整を行いました。

一方、本四半期の攻撃では、改ざんサイトから誘導されるマルウエア配布サイトの数が大幅に増加し、また、その構成が複雑化したため、攻撃の実態把握及びマルウエア配布サイトの停止等の調整が困難になりました。

そのため、本四半期は、外部組織からの届出情報や独自に調査した結果に基づき、マルウエアに感染した PC からアカウント情報が送信される先のサーバ(図 1 でいう情報収集サーバ)が比較的少数にとどまっていると考えられることに着目し、これらの情報収集サーバの特定のための調査および停止に向けた調整を優先して行いました。被害の拡大を抑止するためには、このように、攻撃手法の変化に応じた、より効率的な調整活動を行うことが重要であり、適切な調整先の発見のためには、関連する情報をインシデント報告等によりご提供いただくことが必要です。今後とも、インシデント報告へのご協力をお願いします。

今後、さらに攻撃のメカニズムが変化することが予測されます。また、12 月には、大手企業の Web サイトが改ざんされる事例がたて続けに発生しました。Web ページのアップロードに FTP を使用している場合はもちろん、それ以外の場合においても、今一度、管理している Web ページが改ざん(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)されていないか確認してください。また、Web ページのアップロードに使用するコンピュータについては、OS を含む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、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。

仮に、管理する Web ページの改ざんを発見した場合やウイルス対策ソフトにより Gumblar その他の類似のマルウエアを検知した場合は、すでに FTP のアカウント情報が盗まれている可能性がありますので、ウイルス対策ソフト等でマルウエアの駆除を行うとともに、FTP のパスワードを変更してください。なお、Gumblar 等のマルウエアを駆除していない状態でパスワードを変更しても、再度パスワードが盗まれてしまう可能性がありますので、ご注意ください。

また、攻撃方法の変化等により脅威の内容や有効な対策に変化が生じた場合には、随時、注意喚起等の情報発信を行いますので、JPCERT/CC からの発信情報も継続的にご確認ください。

注意喚起 － Web サイト経由でのマルウエア感染拡大に関する注意喚起
http://www.jpcert.or.jp/at/2009/at090023.txt

注意喚起 － Adobe Reader 及び Acrobat の未修正の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2009/at090027.txt

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

JPCERT/CC からのお知らせ － 冬期の長期休暇を控えて Vol.2
http://www.jpcert.or.jp/pr/2009/pr090008.txt

(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関連は 1149 件でした。前四半期の 2154 件から減少しました。これは、マレーシアのセキュリティ対応機関からの届出が減少したためです。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、関係組織に対して通知を行っています。

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。)の届出は 228 件でした。

届出を受けた Scan では、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。

JPCERT/CC では、届出者から調整の依頼がある場合は、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。

(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届出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届出は 144 件でした。
「other」に含まれるインシデントでは特筆すべきインシデントはありませんでした。

● 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、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/

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