2. コンピュータ不正アクセス届出状況

（1） 四半期総括

2013 年第 1 四半期（2013 年 1 月～3 月）のコンピュータ不正アクセス届出の総数は **27 件**でした（2012 年 10 月～12 月：36 件）。そのうち**『侵入』の届出**が **18 件**（同：14 件）、**『なりすまし』の届出**が **5 件**（同：12 件）、**『不正プログラムの埋め込み』の届出**が **2 件**（同：3 件）などでした。

『侵入』18 件のうち、その多くは『ウェブ改ざん』の被害を受けたもので、15 件の届出がありました。

2010 年第 1 四半期にはいわゆる「ガンブラー」の流行※1、2012 年第 3 四半期には一部島しょの領有権に関する近隣国からの抗議行動の一環によるものと推測される改ざんが多く、届出件数の増加に繋がりました。本四半期ではその時期と異なり、“特定のウイルスによる感染が流行する”、“ウェブサーバに関する深刻な脆弱性が発見される”といった特徴的な原因は見受けられませんでしたが、これらの時期に迫る件数の届出がありました。

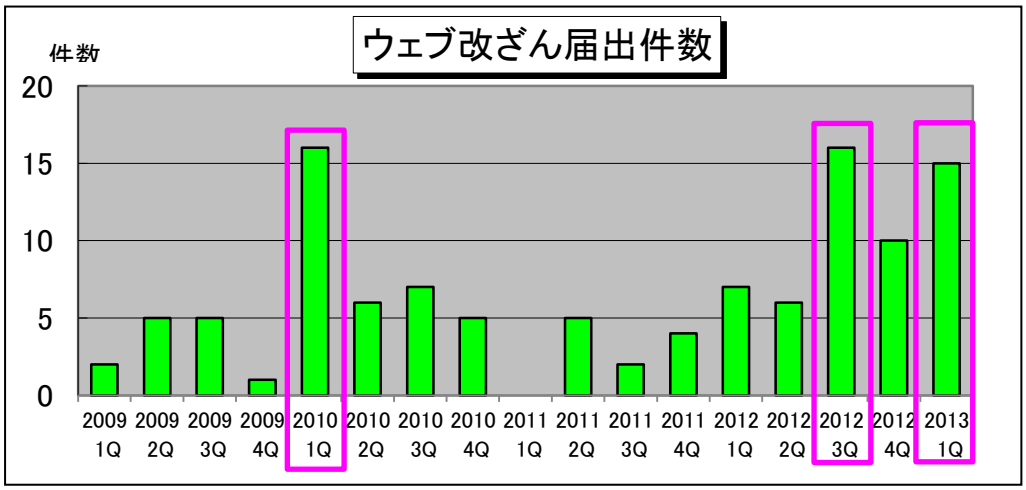

図 2-1：ウェブ改ざん届出件数の推移

ウェブを改ざんされた原因としては**「原因不明」が大半**を占めていますが（図 2-4 参照）、原因が特定できたものとしては、**管理者権限アカウントに対するブルートフォース攻撃、CMS※2 やサーバー管理ツールの脆弱性の悪用など、多岐**にわたります。また FTP アカウントを窃取されたことによる改ざん被害もあり、2010 年第 1 四半期に流行した「ガンブラー」と同様の手口がいまだに継続して行われていると推測されます。

また JPCERT/CC が、「Parallels Plesk Panel」というサーバー管理ツールを利用しているウェブサイトへの改ざんに対する注意喚起を発表しております※3。IPA にも、「Parallels Plesk Panel」を利用しているウェブサイトに不正な Apache モジュールを設置された被害の届出や相談が寄せられています。「Parallels Plesk Panel」が原因とは断定できませんが、同ツールの利用サイトは、念のためツールを最新版にバージョンアップするなどの対策を実施することを推奨します。

ウェブを改ざんされた場合については、前四半期までは、近隣国からの抗議行動の一環と推測されるような内容にページが改ざんされるといった内容が届出られていましたが、本四半期はそういった届出は一切なく、**“ウイルス配布サイトに改ざんされた”という被害内容の届出が半数**を占めており、ウェブ利用者への直接攻撃以外にも、正規のサイトを改ざんすることで間接的にウェブ閲覧者を攻撃する攻撃手法が目立ってきていると言えます。

ウェブ改ざんへの対策として、**システム管理者によるサーバー側での対策はもちろん**ですが、万が一、改ざんされたウェブページを閲覧してしまった場合に備える事前の対策として、**パソコン側での対策も忘れずに実施**してください。

なお、対策としては、以下に挙げる基本的なセキュリティ対策が効果的であることに変わりありませ

ん。各項目についてしっかりと対策が行われているか、改めて対策状況を確認してください。

サーバー側での対策（システム管理者向け対策）
・ID やパスワードの厳重な管理及び設定
・セキュリティホールの解消（パッチ適用不可の場合は、運用による回避策も含む）
・ルータやファイアウォールなどの設定やアクセス制御設定
・アクセスログのこまめなチェック

パソコン側での対策（個人向け対策）
・ウイルス対策ソフトを、常に最新の状態にしながら利用
・Windows Update や Office Update など､OS やアプリケーションソフトのアップデート
・パスワードの設定と管理（複雑化、安易に他人に教えない、使い回しをしない、など）
・ルータやパーソナルファイアウォールの活用
・無線 LAN の暗号化設定確認（WEP は使用せず、できる限り WPA2 を使用する）

※1　『ドライブ・バイ・ダウンロード攻撃により閲覧者のパソコンをウイルスに感染させ』､『そのウイルスで FTP のアカウントを盗み』､『そのアカウントで更に別のウェブサイトを改ざんし、ドライブ・バイ・ダウンロード攻撃により感染を拡大させる』という一連の手口。
※2　CMS（Content Management System）：ウェブサイトのコンテンツ（テキストや画像など）を統合的に管理するためのウェブアプリケーションソフト。
※3　JPCERT/CC「旧バージョンの Parallels Plesk Panel の利用に関する注意喚起」
https://www.jpcert.or.jp/at/2013/at130018.html

（2） 被害事例

（i）サーバーから大量の通信が発生しており、他組織に迷惑をかけている

事例	・当社が利用しているホスティングサービス会社から､「内部向け、外部向け両方において大量の通信が発生している。特に外部向けの通信量が異常に多い」との連絡を受けた。 ・その外部向け通信の内容は､当社の DNS サーバーから出ているもので､宛先も DNS が通常使用する UDP53 番ポートを宛先ポートとする通信であった。 ・それらの通信は、当然ながら当社が意図する通信ではない。 ・ホスティングサービス会社に調査を依頼したが、原因不明との調査結果であった。
解説・対策	本事例のような「自社の DNS サーバーが DoS 攻撃並みの通信を受けると同時に、他の組織に対しても意図しない DoS 攻撃が発生している」といった相談や届出が IPA に複数寄せられています。 これは「**DNS Amp 攻撃**」※4 という攻撃を受けた時の典型的症状です。 不適切な設定で、かつ脆弱性を抱えている DNS キャッシュサーバー※4 は、本事例のように知らぬ間に他組織への DoS 攻撃に加担してしまう恐れがあります。 ・DNS 問い合わせを受け付ける範囲を限定する ・IP アドレスなりすまし（IP スプーフィング）対策を行う ・DNS キャッシュポイズニング対策を行う DNS キャッシュサーバーにおいては上記 3 点の対策を行うことを推奨します。 （ご参考） IPA – DNS サーバーの脆弱性に関する再度の注意喚起 ～DNS サーバーを管理するウェブサイト運営者は 早急に DNS サーバーのパッチ適用や設定変更を!～ http://www.ipa.go.jp/security/vuln/documents/2008/200812_DNS.html

※4　「DNS Amplification 攻撃」「DNS 増幅攻撃」などと呼ばれることもある。
※5　DNS キャッシュサーバー：自組織内のクライアント（パソコンなど）に代わって、外部の DNS サーバーに DNS 問い合わせを行う DNS サーバー。

（3）届出件数

2013 年第 1 四半期［1 月～3 月］の届出件数は合計 27 件（前四半期比約 75%）**であり、**そのうち被害があった件数は 27 件（前四半期比 79%）となりました。

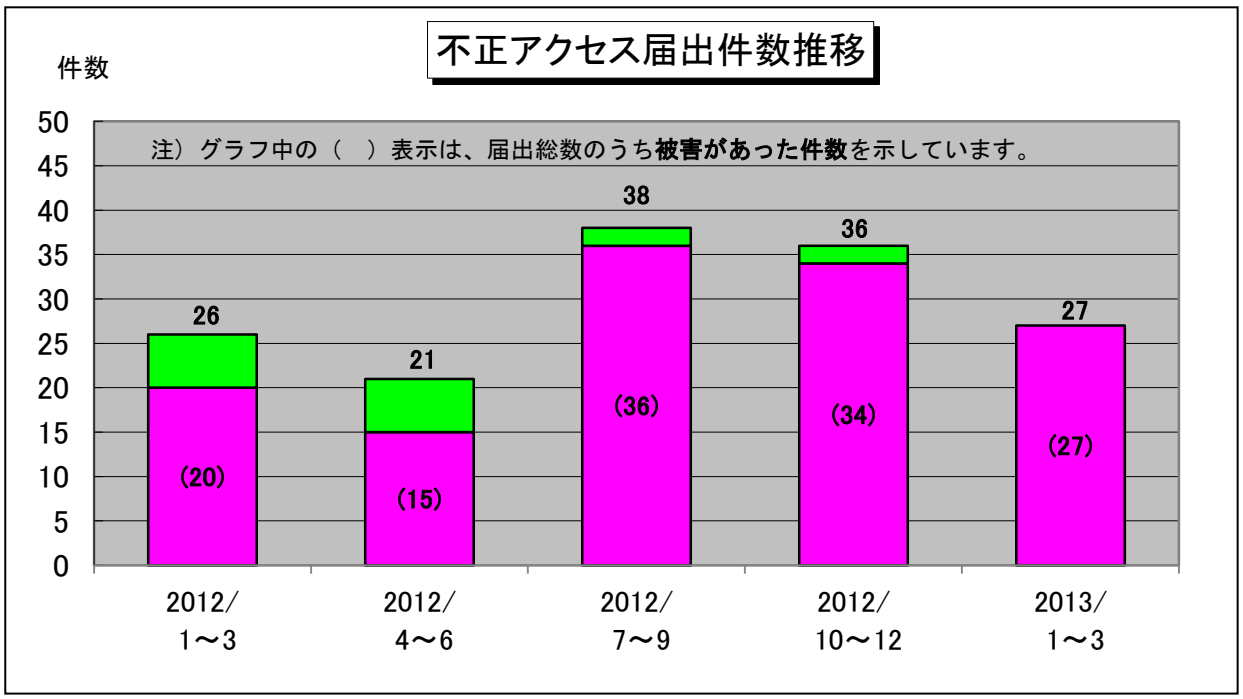

図 2-2：不正アクセス届出件数の推移

（4）届出種別

IPA に届けられた 27 件（先期 36 件）のうち、実際に被害があった届出は 27 件（先期 34 件）と全体の 100%を占めました。実際に被害に遭った届出とは「侵入」「メール不正中継」「ワーム感染」「DoS」「アドレス詐称」「なりすまし」「不正プログラム埋込」「その他（被害あり）」の合計です。

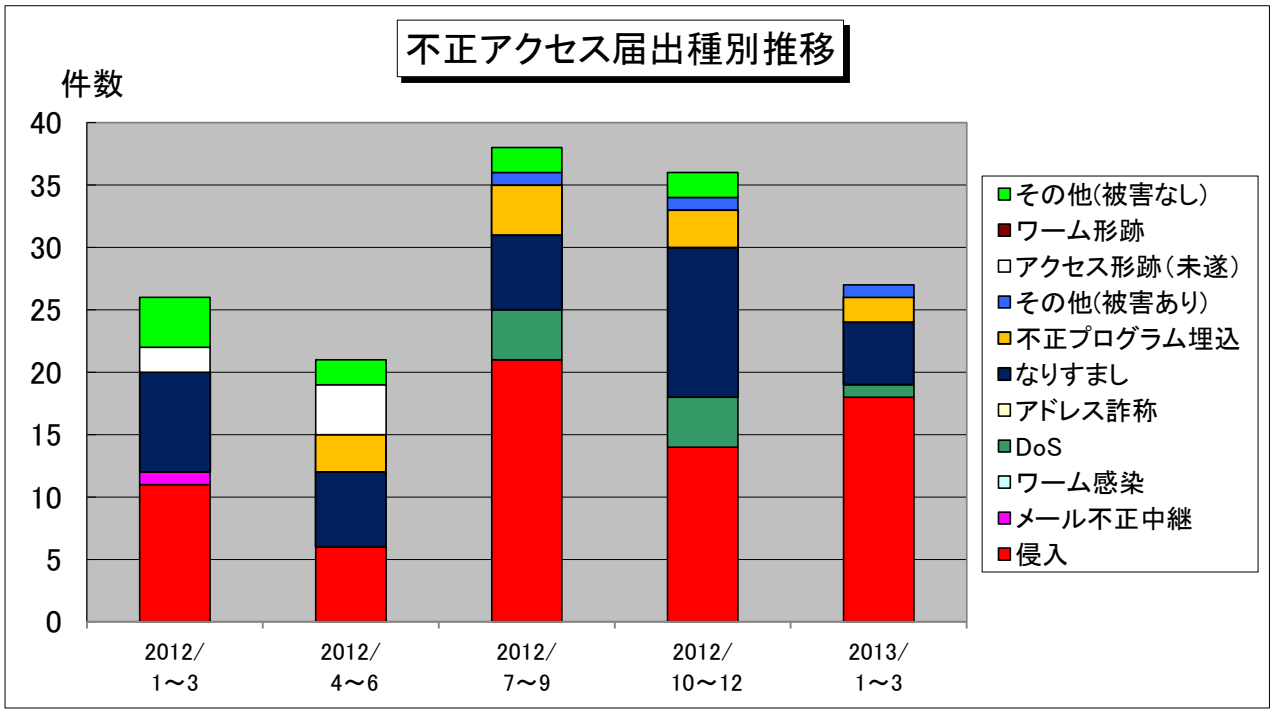

図 2-3：不正アクセス届出種別推移

表 2-1　不正アクセス届出件数の推移（項目別）

	2012年 第1四半期		2012年 第2四半期		2012年 第3四半期		2012年 第4四半期		2013年 第1四半期	
侵入	11	42.3%	6	28.6%	21	55.3%	14	38.9%	18	66.7%
メール不正中継	1	3.8%	0	0.0%	0	0.0%	0	0.0%	0	0.0%
ワーム感染	0	0.0%	0	0.0%	0	0.0%	0	0.0%	0	0.0%
DoS	0	0.0%	0	0.0%	4	10.5%	4	11.1%	1	3.7%
アドレス詐称	0	0.0%	0	0.0%	0	0.0%	0	0.0%	0	0.0%
なりすまし	8	30.8%	6	28.6%	6	15.8%	12	33.3%	5	18.5%
不正プログラム埋込	0	0.0%	3	14.3%	4	10.5%	3	8.3%	2	7.4%
その他（被害あり）	0	0.0%	0	0.0%	1	2.6%	1	2.8%	1	3.7%
アクセス形跡（未遂）	2	7.7%	4	19.0%	0	0.0%	0	0.0%	0	0.0%
ワーム形跡	0	0.0%	0	0.0%	0	0.0%	0	0.0%	0	0.0%
その他（被害なし）	4	15.4%	2	9.5%	2	5.3%	2	5.6%	0	0.0%
合　計（件）	**26**		**21**		**38**		**36**		**27**	

注）網掛け部分は、**被害があった**届出種類を示しています。
割合の数字は小数点第二位を四捨五入していますので、合計が100%ちょうどにならない場合があります。

（5）被害原因

実際に被害があった届出（36 件）のうち、原因の内訳は**古いバージョン使用・パッチ未導入が 5 件、ID・パスワード管理不備が 2 件、設定不備が 2 件、**などでした。

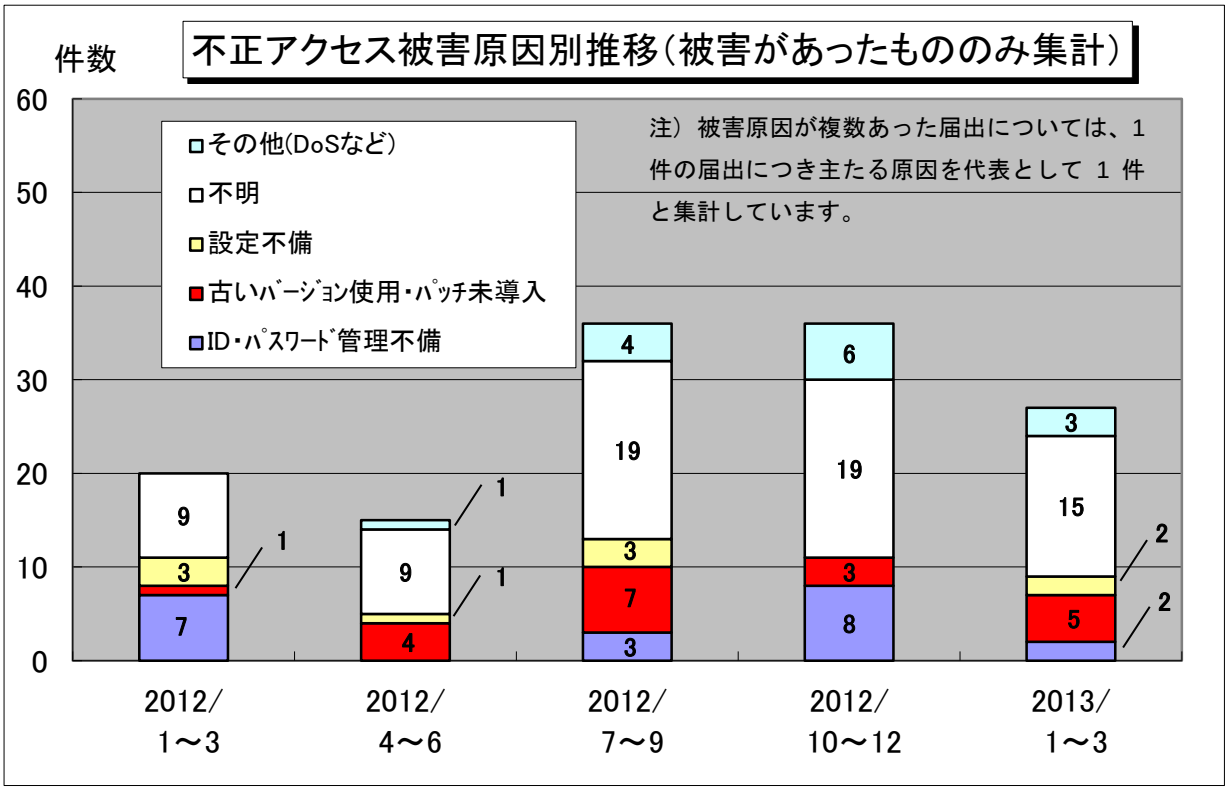

図 2-4：不正アクセス被害原因別推移

（6）届出者の分類

届出者別の内訳は、以下のようになっています。

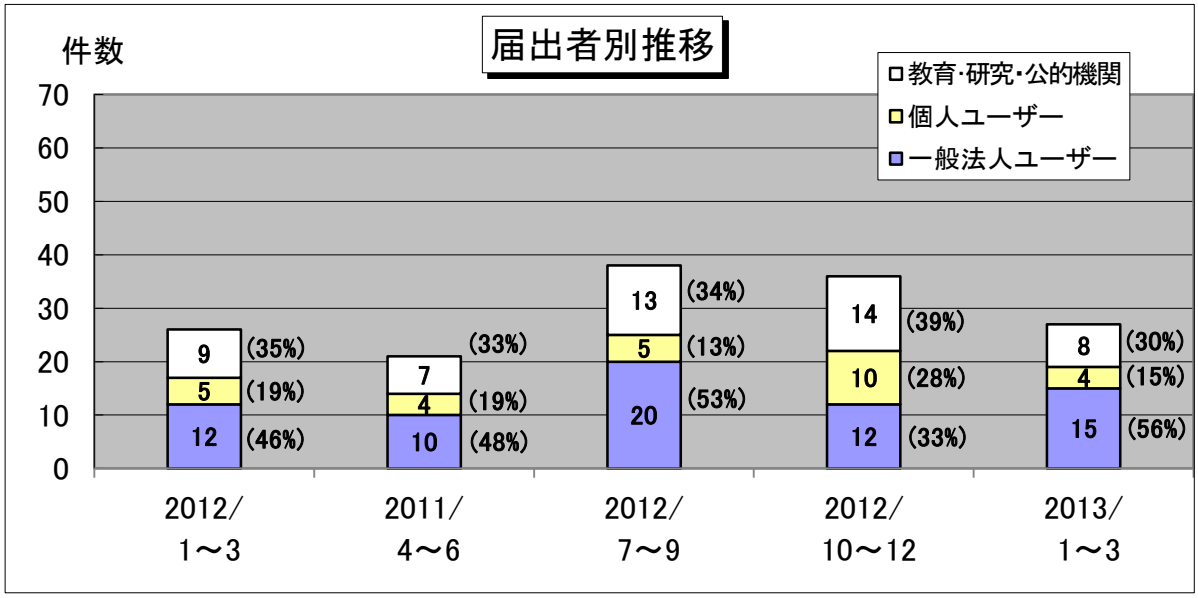

図 2-5：届出者別推移

・コンピュータ不正アクセス被害の届出制度について

コンピュータ不正アクセス被害の届出制度は、経済産業省のコンピュータ不正アクセス対策基準に基づき、'96 年 8 月にスタートした制度であり、同基準において、コンピュータ不正アクセスの被害を受けた者は、被害の拡大と再発を防ぐために必要な情報を IPA に届け出ることとされています。

IPA では、個別に届出者への対応を行っていますが、同時に受理した届出等を基に、コンピュータ不正アクセス対策を検討しています。また受理した届出は、届出者のプライバシーを侵害することがないように配慮した上で、被害等の状況を分析し、検討結果を定期的に公表しています。

〇コンピュータ不正アクセス対策基準
平成 8 年 8 月 8 日（通商産業省告示第 362 号）（制定）
平成 9 年 9 月 24 日（通商産業省告示第 534 号）（改定）
平成 12 年 12 月 28 日（通商産業省告示 第 950 号）（最終改定）

〇経済産業大臣が別に指定する者
平成 16 年 1 月 5 日（経済産業省告示 第 3 号）