コンピュータウイルス・不正アクセスの届出状況および相談状況

[2014 年第 3 四半期（7 月～9 月）]

本レポートでは、2014 年 7 月 1 日から 2014 年 9 月 30 日までの間にセキュリティセンターで受理した、コンピュータウイルスと不正アクセスに関する「届出」と「相談」の統計及び事例について紹介しています。

独立行政法人情報処理推進機構 技術本部 セキュリティセンター

2014 年 10 月 24 日

目次

1. コンピュータウイルスおよび不正プログラムの検出数

1-1. 四半期総括

2014 年第 3 四半期に寄せられたウイルスの検出数 (*1) は、2014 年第 2 四半期 17,474 個より 2,174 個（約 12%）多い 19,648 個でした（図 1-2 参照）。また、2014 年第 3 四半期の不正プログラム (*2) 検出数は 2014 年第 2 四半期 73,741 個から 24,604 個（約 33%）多い 98,345 個でした（図 1-3 参照）。また本四半期は、実際にウイルスに感染してしまった旨の届出はありませんでした。

個別のウイルス、不正プログラムに着目すると、検出数の第 1 位は不正なウェブサイトにリダイレクト（移動）させる不正プログラムの総称である Redirect (*3) で 11,997 個（7 月：2,334 個、8 月：2,270 個、9 月：7,393 個）でした。今期は 2014 年 9 月の検出数だけで前四半期の検出数を上回り、前四半期の 7,196 個から約 67%（4,801 個）増加しました。急増の理由は不明ですが、Redirect を使って不正なウェブサイトに誘導し、さらに別のウイルスに感染させることが目的と考えられます。

ウイルスと不正プログラムの総検出数117,993個のうちパソコン利用者のダウンロード行為またはウイルスによってパソコンにダウンロードされた数は 82,104 個で全体の約 70%でした。次に多かったのは受け取ったメールに添付されていたものを検出したもので 19,581 個、全体の約 17%でした（表 1-3 参照）。

1-2. 検出数に顕著な変化が見られたウイルス・不正プログラム

2014 年第 3 四半期に最も多く検出されたウイルスは、W32/Netsky (*4) でした。検出数は前四半期の 8,354 個より 41 個多い、8,395 個でした。また、前四半期からの増加率が大きいウイルスは、W32/Bagle (*5) と W32/Mytob (*6) の 2 種類でした。W32/Bagle の検出数は前四半期から約 365%（2014 年第 3 四半期：2,384 個、2014 年第 2 四半期：513 個）増加、W32/Mytob の検出数は前四半期から約 139%（2014 年第 3 四半期：1,796 個、2014 年第 2 四半期：752 個）増加しました。メールを使って大量にばら撒かれているものと考えられます。

一方、最も多く検出された不正プログラムは、前述のとおり Redirect で、次に多く検出された不正プログラムは、偽セキュリティソフトの Fakeav (*7) でした。検出数は前四半期から約 291%（2014 年第 3 四半期：6,206 個、2014 年第 2 四半期：1,588 個）増加しました。

前四半期に最も多く検出されたインターネットバンキングのログイン情報を窃取する不正プログラム、“Bancos”の検出数は前四半期から約 66%（2014 年第 3 四半期：5,540 個、2014 年第 2 四半期：16,086 個）減少しました。

(*1) 検出数： 届出者の自組織等で発見・検出したウイルスの数（個数）

(*2) 不正プログラム：「コンピュータウイルス対策基準」におけるウイルスの定義「(1)自己伝染機能」、「(2)潜伏機能」、「(3)発病機能」の、どの機能も持たないもの。
「コンピュータウイルス対策基準」：http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm

(*3) Redirect： 不正なウェブサイトにリダイレクト（移動）させる不正プログラムの総称。移動先のウェブサイトから、別のウイルスや不正プログラムをダウンロードして感染させようとする。

(*4) W32/Netsky： 自身の複製をメールの添付ファイルとして拡散するマスメール型ウイルス。

(*5) W32/Bagle： 自身の複製をメールの添付ファイルとして拡散するマスメール型ウイルス。

(*6) W32/Mytob： パソコン内のアドレス帳からメールアドレスを取得しウイルス自身を添付したメールを送信するウイルス。

(*7) Fakeav： 金銭を騙し取るオンライン詐欺を目的とした不正プログラム。

1-3. 届出件数

2014 年第 3 四半期（7 月～9 月）の届出件数は 1,298 件で、感染被害があった届出はありませんでした。下記図 1-1 は、四半期ごとの届出件数の推移を示したものです。届出件数は 2014 年第 2 四半期の 1,292 件より 6 件増えました。

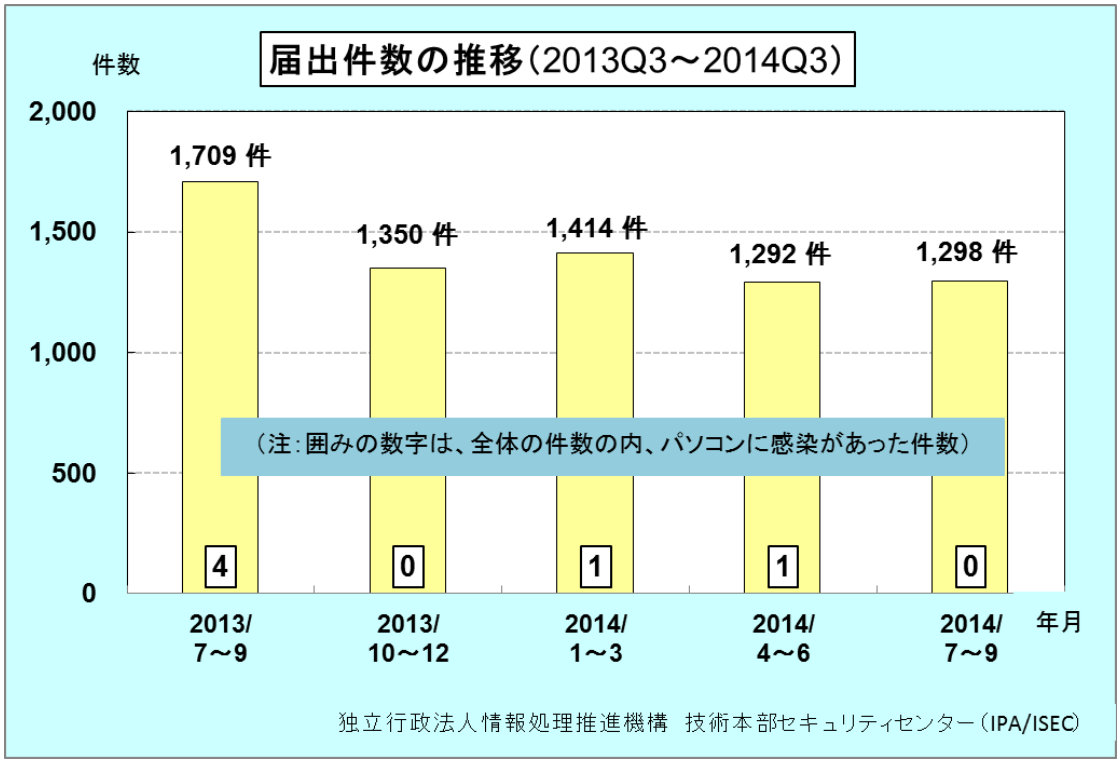


図 1-1. 届出件数の四半期別推移

1-4. ウイルス検出数

2014 年第 3 四半期のウイルス検出数は 19,648 個と、前期の 17,474 個から 2,174 個（約 12%）の増加となりました（図 1-2 参照）。

W32/Bagle が 1,871 個、W32/Mytob が 1,044 個、検出数が増加したことが主因です。

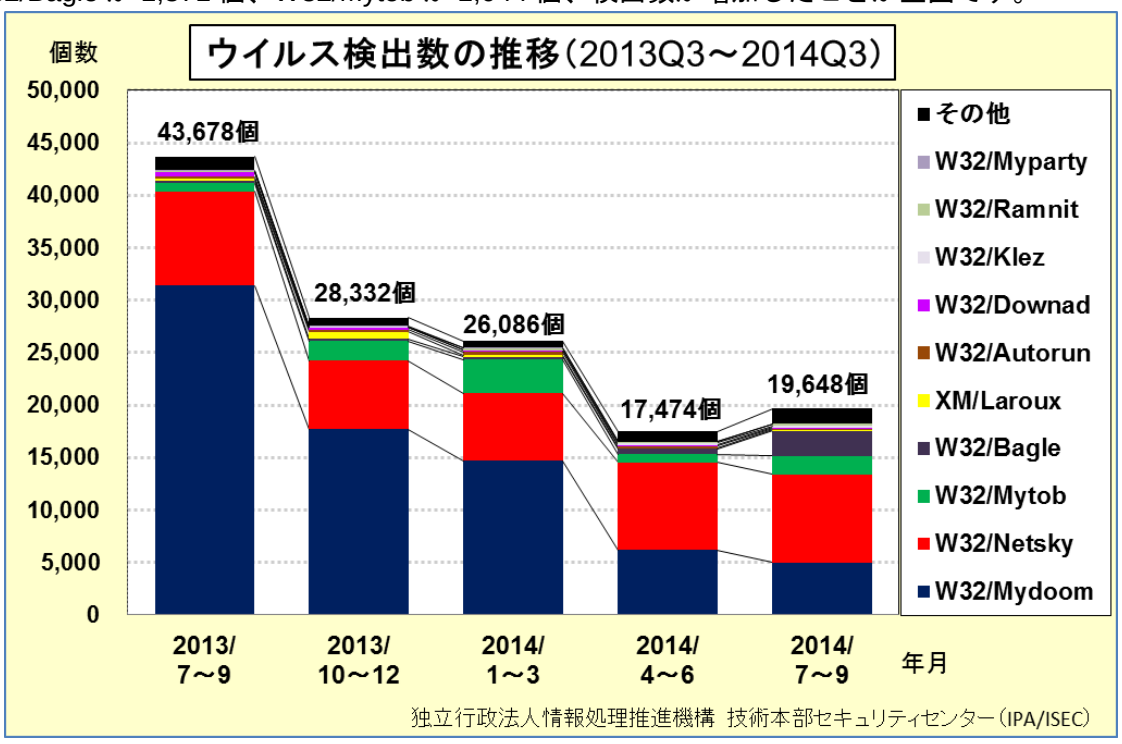


図 1-2. ウイルス検出数の推移

1-5. 不正プログラム検出数

2014 年第 3 四半期の不正プログラム検出数は 98,345 個と、前期の 73,741 個から、24,604 個（約 33%）増加しました（図 1-3 参照）。

検出数増加の主な要因は前四半期の 7,196 個から 4,801 個増加し 11,997 個検出された Redirect と、検出数が 4,618 個増加した Fakeav です。

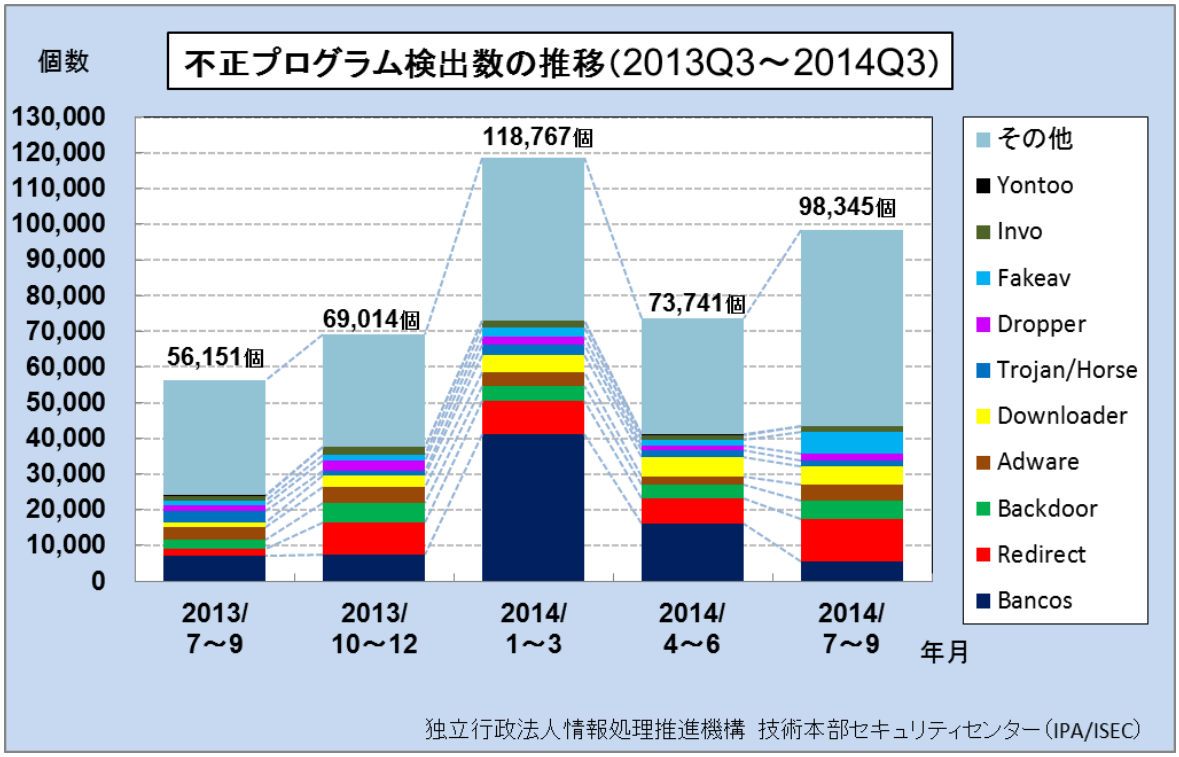


図 1-3. 不正プログラム検出数の推移

1-6. 2014 年第 3 四半期の検出ウイルス

ウイルスの種類は 54 種類、検出数は、Windows/DOS ウイルス 19,258 個、スクリプトウイルス及びマクロウイルス 380 個、携帯端末ウイルス 10 個でした。

表 1-1. 2014 年第 3 四半期の検出ウイルス　　(※)印は 2014 年第 3 四半期の新規届出ウイルス

i) Windows/DOS ウイルス	検出数
W32/Netsky	8,395
W32/Mydoom	4,992
W32/Bagle	2,384
W32/Mytob	1,796
W32/Rontokbro	602
W32/Ramnit	215
W32/Klez	148
W32/Autorun	114
W32/Chir	88
W32/Downad	87
W32/Virut	80
W32/Magistr	65
W32/Fujacks	50
W32/Prettypark	37
Wscript/Kakworm	29
W32/Sircam	26
W32/Parite	18
W32/Sobig	16
W32/Badtrans	12
W32/Imaut	12
W32/Inor	11
W32/Gammima	9
W32/IRCbot	9
W32/Fakerecy	8
W32/Nimda	7
W32/Sality	7
W32/Spyrat	6
W32/Almanahe	5
W32/Mumu	5
W32/Sober	4
W32/Antinny	3
W32/Mywife	3
W32/Neeris	2
W32/Nuwar	2
Anti-CMOS	1
W32/Dotex	1
W32/Frethem	1
W32/Gaobot	1
W32/Lovgate	1
W32/Mota	1
W32/Remadm	1

i) Windows/DOS ウイルス	検出数
W32/Sohanad	1
W32/Tenga	1
W32/Vbsclick	1
W32/Whybo	1
小計　(45 種類)	19,258

スクリプトウイルス	検出数
VBS/Freelink	188
VBS/DUNIHI	77
VBS/Solow	3
VBS/LOVELETTER	2
小計　(4 種類)	270

マクロウイルス	検出数
XM/Laroux	85
XM/Mailcab	22
W97M/Marker	1
W97M/Relax	1
O97M/Darksnow(※)	1
小計　(5 種類)	110

ii)携帯端末ウイルス	検出数
AndroidOS/Lotoor	7
AndroidOS/Fakeflash	1
AndroidOS/SmsSpy(※)	1
AndroidOS/Smssend	1
小計　(4 種類)	10

iii) Macintosh	検出数
なし	

iv) OSS（OpenSourceSoftware）: Linux･BSD を含む	検出数
なし	

（参考）
・Windows/DOS ウイルス … Windows、MS-DOS 環境下で動作するウイルス。
・マクロウイルス … Microsoft Word や Microsoft Excel などのマクロ機能を悪用するウイルス。
・スクリプトウイルス … 機械語への変換作業を省略して実行できるようにした簡易プログラムで記述されたウイルス。
・携帯端末ウイルス … 携帯電話やタブレットなどの環境下で動作するウイルス。

注）ウイルス名欄での各記号の用語説明は以下の通り。

記号	用語説明
W32	Windows 32 ビット環境下で動作
XM	Microsoft Excel95、97（Excel Macro の略）
WM	Microsoft Word95、97（Word Macro の略）
W97M	Microsoft Word97（Word 97 Macro の略）
X97M	Microsoft Excel97（Excel 97 Macro の略）
O97M	Microsoft Office97（Office 97 Macro の略）
VBS	Visual Basic Script で記述
Wscript	Windows Scripting Host 環境下で動作（VBS を除く）
AndroidOS	Android OS 環境下で動作
SymbOS	Symbian OS 環境下で動作
XF	Microsoft Excel95、97 で動作するウイルス（Excel Formula の略）

1-7. 2014 年第 3 四半期に IPA に初めて届出のあったウイルスの概要

（1）AndroidOS/SmsSpy (エスエムエススパイ)　届出月：2014 年 9 月

このウイルスは、モバイル端末用の AndroidOS を感染対象としたウイルスです。
ウイルス感染したファイルを入手しユーザーがインストールすると感染します。
感染すると、電話番号・受信した SMS (*8) メッセージなどの情報を外部に送信します。

（2）O97M/Darksnow (ダークスノー)　届出月：2014 年 9 月

このウイルスは、Microsoft Word ファイル および Microsoft Excel ファイルに感染するマクロウイルスです。
利用者がウイルスに感染したファイルを開くと感染し、感染したパソコンから情報を窃取します。

1-8. ウイルス届出者構成及び感染経路

2014 年第 3 四半期の届出者属性は、過去の傾向と同じく、一般法人がほとんどを占めています。ウイルスと不正プログラムの検出経路については、「ダウンロード」が最も多く、次いで「メール」が多い状況です。

(*8) 携帯端末同士で、短い文章のメールを送受信できるサービス。

表 1-2. ウイルス届出者別件数

	2013/ 7～9	2013/ 10～12	2014/ 1～3	2014/ 4～6	2014/ 7～9
一般法人	1,675	1,308	1,404	1,269	1,281
	(98.0%)	(96.9%)	(99.3%)	(98.2%)	(98.7%)
個人	0	0	0	0	0
	(0.0%)	(0.0%)	(0.0%)	(0.0%)	(0.0%)
教育機関	34	42	10	23	17
	(2.0%)	(3.1%)	(0.7%)	(1.8%)	(1.3%)
合計	1,709	1,350	1,414	1,292	1,298

表 1-3. ウイルス検出数および不正プログラム検出数（検出経路別）

	2013/ 7～9	2013/ 10～12	2014/ 1～3	2014/ 4～6	2014/ 7～9
メール	42,952	28,098	25,927	17,396	19,581
	(43.0%)	(28.9%)	(17.9%)	(19.1%)	(16.6%)
ダウンロード ファイル	44,409	51,787	90,861	59,201	82,104
	(44.5%)	(53.2%)	(62.7%)	(64.9%)	(69.6%)
外部記憶 媒体	6	65	1	41	0
	(0.006%)	(0.067%)	(0.001%)	(0.045%)	(0.000%)
ネット ワーク	667	249	250	125	107
	(0.7%)	(0.3%)	(0.2%)	(0.1%)	(0.1%)
不明・その他	11,795	17,147	27,814	14,452	16,201
	(11.8%)	(17.61%)	(19.2%)	(15.8%)	(13.7%)
合計	99,829	97,346	144,853	91,215	117,993

・コンピュータウイルスに関する届出制度について

コンピュータウイルスに関する届出制度は、経済産業省のコンピュータウイルス対策基準に基づき、平成 2 年 4 月にスタートした制度であり、コンピュータウイルスを発見したもの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、コンピュータウイル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。

○コンピュータウイルス対策基準
平成 7 年 7 月 7 日（通商産業省告示第 429 号）（制定）
平成 9 年 9 月 24 日（通商産業省告示第 535 号）（改定）
平成 12 年 12 月 28 日（通商産業省告示 第 952 号）（最終改定）

○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 2 号）

2. コンピュータ不正アクセス届出状況

2-1. 四半期総括

2014 年第 3 四半期（2014 年 7 月～9 月）のコンピュータ不正アクセス届出の総数は 27 件（2014 年第 2 四半期：37 件）でした（図 2-1）。そのうち『DoS』の届出が 6 件（同：6 件）、『なりすまし』の届出が 7 件（同：12 件）、『侵入』の届出が 3 件（同：3 件）『不正プログラム埋込』の届出が 1 件（同：5 件）などでした（表 2-1）。

本四半期の『なりすまし』の届出件数は 7 件で、前四半期から減少しています（表 2-1）。そのうち 2 件の詳細はオンラインゲームへの不正なログインで、そのうち 1 件ではゲーム内の課金アイテムを不正購入されていました。前四半期と同様、金銭被害を伴う不正ログインが発生しており、原因はパスワードの使いまわしが考えられます。

オンラインゲームに限らず、パスワードの使いまわしは様々なサービスで不正ログインのリスクが高まります。特にショッピングサイトのようなクレジットカード情報を登録するサイトにおいて、利用者は“パスワードを使いまわさない[(*9)]”、“二段階認証などのセキュリティオプションを積極的に利用する”ことが推奨されます。一方、事業者においても“二段階認証”のような安全な仕組みを採用することが求められます。

また、本四半期では、スパムメール送信の踏み台とされてしまう被害が 5 件ありました。内訳はアカウント情報の不正利用による被害が 3 件（届出『なりすまし』）、メーリングリストやウェブコンテンツの管理システムの脆弱性悪用による被害が 2 件（届出『その他（被害あり）』）です（表 2-1）。

前述のアカウント情報の不正利用による被害では、推測が容易なパスワードの利用またはフィッシングによる情報窃取が原因と考えられます。このようなアカウント情報の不正利用による被害を防ぐためには、パスワードの適切な設定および管理が重要です。例えば、複雑で強固なパスワードを設定した場合でも、ウイルス感染やフィッシングにより、パスワードは強度に関係なく窃取されてしまう可能性があります。

また、事業者の場合、パスワードの適切な管理・設定の他、万が一、アカウント情報が流出した場合でも被害を受けないように、不用意に SMTP サービスを外部に公開しない対応が必要です。外部に SMTP サービスを公開している場合は、外部からのアクセスを一度 VPN に経由させ内部ネットワークに接続してから SMTP サービスを利用するなどの代替案の適用可否を検討してください。

その他、基本的な脆弱性対策を含め、システムの構成に応じた多角的な対策の検討、実施が必要です。

その他、ウェブ改ざんの被害やパスワードリスト攻撃の被害についての届出もありましたが、いずれも原因は不正ログインと考えられます。このように、本四半期ではパスワード管理の隙を狙われた被害が散見されています。繰り返しとなりますが、“推測が容易となるパスワードを設定していないか”、“パスワードを使いまわしていないか”など、いま一度パスワードの適切な設定と管理方法を確認することを推奨します。

(*9) パスワードリスト攻撃による不正ログイン防止に向けた呼びかけ
https://www.ipa.go.jp/about/press/20140917.html

2-2. 被害事例

（i）ウェブサーバーの“.bash_history”(*10) ファイルを窃取された

被害の概要	・管理しているウェブサーバーに対して、「GET /.bash_history HTTP/1.1」のリクエストを送信され、.bash_history ファイルを窃取された。 ・当該.bash_history ファイルには、サーバー内の設定やパスワード等、管理上重要な内容に関わる情報は含まれていなかった。
解説・対策	ファイルに対するアクセス権限の設定不備が原因の情報窃取の事例です。（2014 年 9 月 24 日に US-CERT が発表(*11) した Bash の脆弱性の影響によるものではありません） 幸いにして今回窃取されてしまったファイルには、悪用される恐れがあるパスワードのような情報は含まれていませんでした。 .bash_history ファイルには、入力されたコマンドの履歴が記録されます。そのため、例えば、疎通確認のために ping コマンドを実行していた場合には、疎通対象となった端末の IP アドレスが知られてしまいます。また、サービスの設定を実行していた場合には、稼働しているサービスや設定内容などを知られてしまい、次の攻撃に悪用される恐れがあります。 まずは機密性を確保するためにも、それぞれのファイルに対するアクセス権限をしっかりと見極め、適切に設定することが重要です。また、ユーザーのログアウト時に.bash_history ファイルを削除する設定を追加するなど、不用意に重要な情報が流出しないような対策も併用すると、より効果的と言えます。

（ii）アンケート入力フォームに大量の不正入力が行われた

被害の概要	・アンケート入力ページの運用テスト実施中に、アンケートに入力された情報を通知する 1,700 通あまりのメールを受信した。 ・受信したメールの内容（攻撃者が入力した情報）には、コマンド・インジェクションを試行したと思われる記述があった。 ・運用テスト実施中の事象であること、およびコマンド・インジェクションへの対策もできていたことから、業務上の実被害は特になかった。
解説・対策	REFERER (*12) チェック機能およびコマンド・インジェクション対策の有効性や重要性が確認できる事例です。 今回の被害では運用テスト実施のため、という突発的かつ短時間の状況にも関わらず、REFERER チェック機能が無効となっていることを悪用され、コマンド・インジェクションを試行されてしまいましたが、その他のセキュリティ対策がしっかりなされていたために二次被害もなく、業務上の影響は生じませんでした。 このように現在管理しているシステムが、いつ、どのような攻撃の対象となるかはわかりません。そのため、セキュリティレベルの高いシステム設計、構築はもちろん、日頃からセキュリティを意識した多層的な運用、管理が重要と言えます。

(*10) .bash_history ： 入力したコマンドの履歴（ヒストリーリスト）が保存されるファイル。
(*11) US-CERT： Bourne-Again Shell (Bash) Remote Code Execution Vulnerability
https://www.us-cert.gov/ncas/current-activity/2014/09/24/Bourne-Again-Shell-Bash-Remote-Code-Execution-Vulnerability
(*12) REFERER ： 特定のウェブページを参照している、元の URL 情報。REFERER の情報をチェックすることで、リンク元を条件としたアクセス制限が可能となるため、CSRF の対策として利用される。

2-3. 届出件数

2014 年第 3 四半期（7 月～9 月）の届出件数は合計 27 件（前四半期比 73%）であり、そのうち被害があった件数は 23 件（前四半期比 79%）となりました。

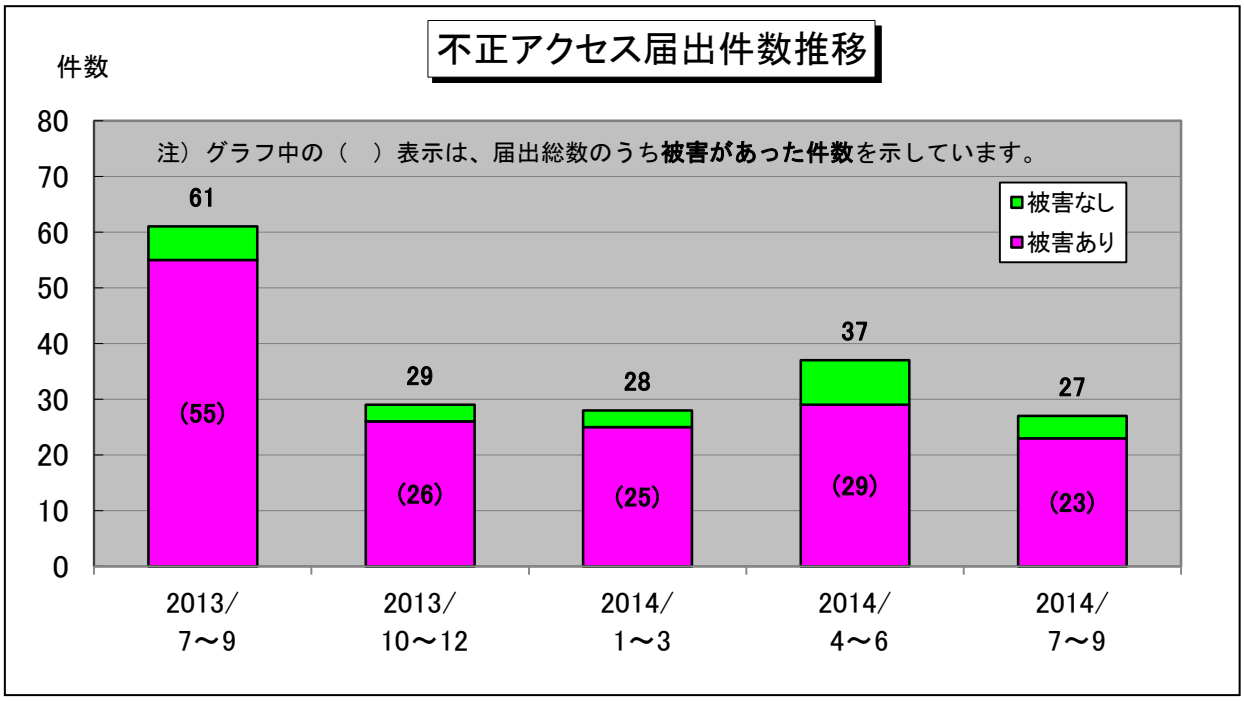


図 2-1. 不正アクセス届出件数の推移

2-4. 届出種別

IPA に届けられた 27 件（前四半期 37 件）のうち、実際に被害があった届出は 23 件（前四半期 29 件）と全体の約 85%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。

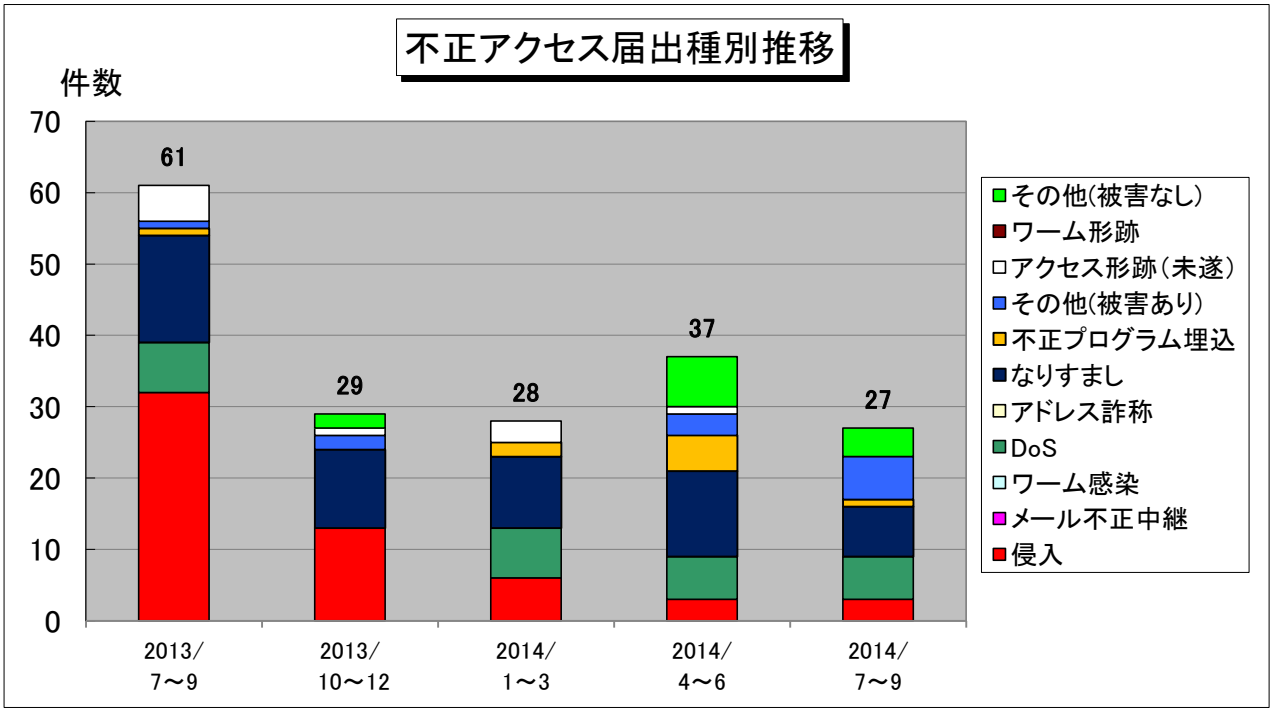


図 2-2. 不正アクセス届出種別の推移

表 2-1. 不正アクセス届出種別の四半期推移

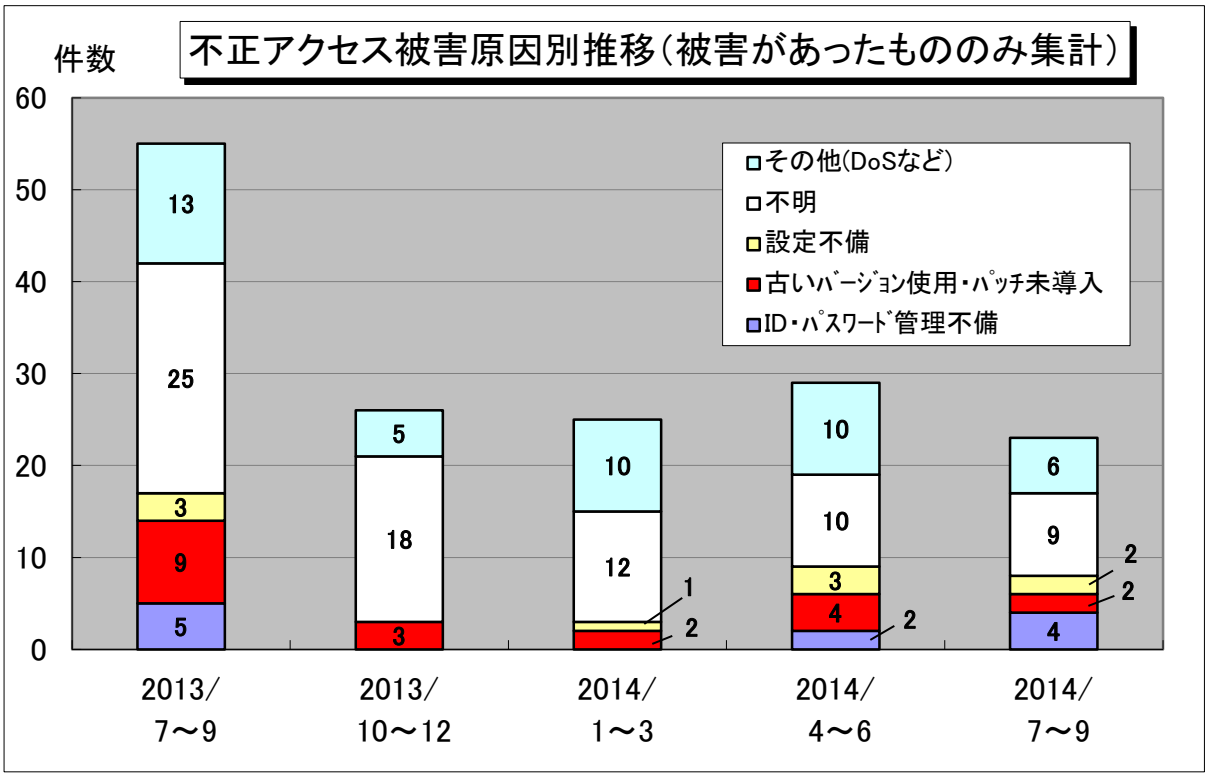
	2013年 第3四半期		2013年 第4四半期		2014年 第1四半期		2014年 第2四半期		2014年 第3四半期	
侵入	32	52.5%	13	44.8%	6	21.4%	3	8.1%	3	11.1%
メール不正中継	0	0.0%	0	0.0%	0	0.0%	0	0.0%	0	0.0%
ワーム感染	0	0.0%	0	0.0%	0	0.0%	0	0.0%	0	0.0%
DoS	7	11.5%	0	0.0%	7	25.0%	6	16.2%	6	22.2%
アドレス詐称	0	0.0%	0	0.0%	0	0.0%	0	0.0%	0	0.0%
なりすまし	15	24.6%	11	37.9%	10	35.7%	12	32.4%	7	25.9%
不正プログラム埋込	1	1.6%	0	0.0%	2	7.1%	5	13.5%	1	3.7%
その他（被害あり）	1	1.6%	2	6.9%	0	0.0%	3	8.1%	6	22.2%
アクセス形跡（未遂）	5	8.2%	1	3.4%	3	10.7%	1	2.7%	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）	0	0.0%	2	6.9%	0	0.0%	7	18.9%	4	14.8%
合　計（件）	**61**		**29**		**28**		**37**		**27**	

注）網掛け部分は**被害があった届出**です。

注）割合の数値は小数点第二位を四捨五入しており、合計が 100%にならない場合があります。

2-5. 被害原因

実際に被害があった届出（23 件）のうち、原因が判明しているものは **ID・パスワード管理不備が 4 件、古いバージョン使用・パッチ未導入が 2 件、設定不備が 2 件、**などでした。



注）被害原因が複数あった届出については、1 件の届出につき主たる原因で計上しています。

図 2-3. 不正アクセス被害原因別推移

2-6. 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。

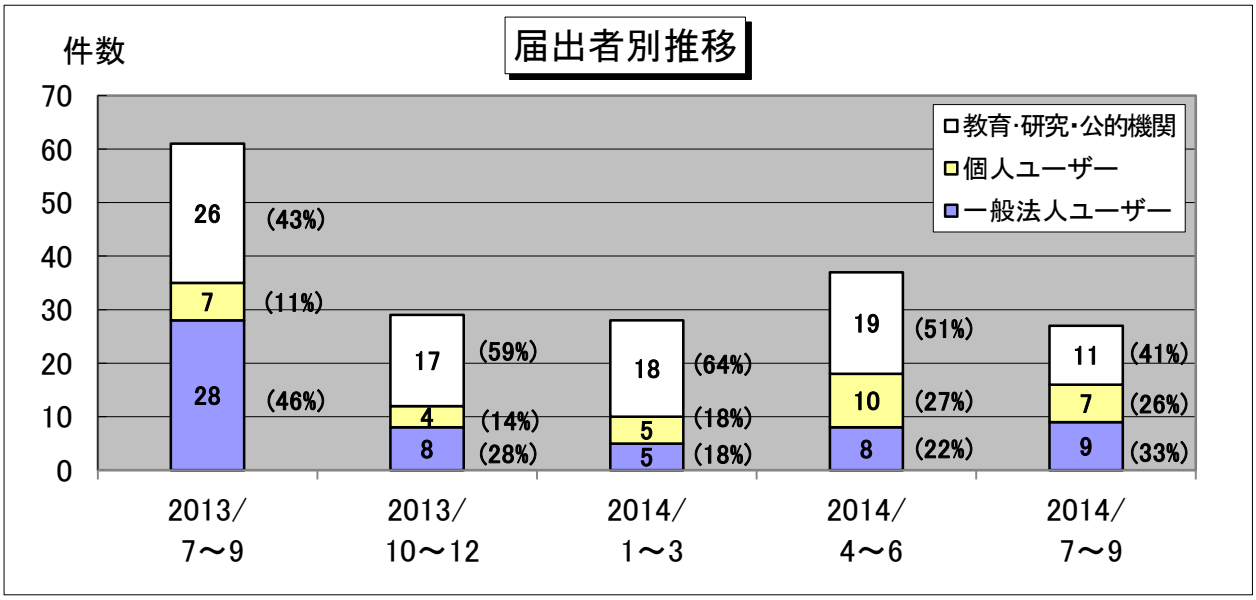


図 2-4. 届出者別推移

・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。

○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）

○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）

3. 相談状況

3-1. 四半期総括

2014 年第 3 四半期（2014 年 7 月～9 月）の相談件数は **4,044 件**でした（2014 年第 2 四半期 : 4,426 件）。前四半期の相談総件数と比べて、今四半期は約 9%減となりました（図 3-1 参照）。

そのうち相談員による対応件数は 1,637 件で、その中で最も多かったのが**『ワンクリック請求』**で **903 件**（同 937 件）でした。そのほか主だったものは**『ソフトウェア購入を促し、クレジットカード番号等を入力させる手口』**に関する相談が **122 件**（同 182 件）、**『スマートフォン』**に関する相談が **272 件**（同 298 件）などでした（図 3-2、図 3-3、図 3-4 参照）。

『インターネットバンキング』に関する相談は **15 件**と、前四半期の 67 件から大幅に減少しました（図 3-5 参照）。グラフは掲出していませんが、そのうち暗証番号や乱数表の入力を求める不正画面を表示するウイルス感染に関する相談は 9 件で、前四半期の 44 件から約 80%減少しました。また、身代金型ウイルス**『ランサムウェア』**は今四半期 **3 件**で、前四半期の 14 件から減少しました。

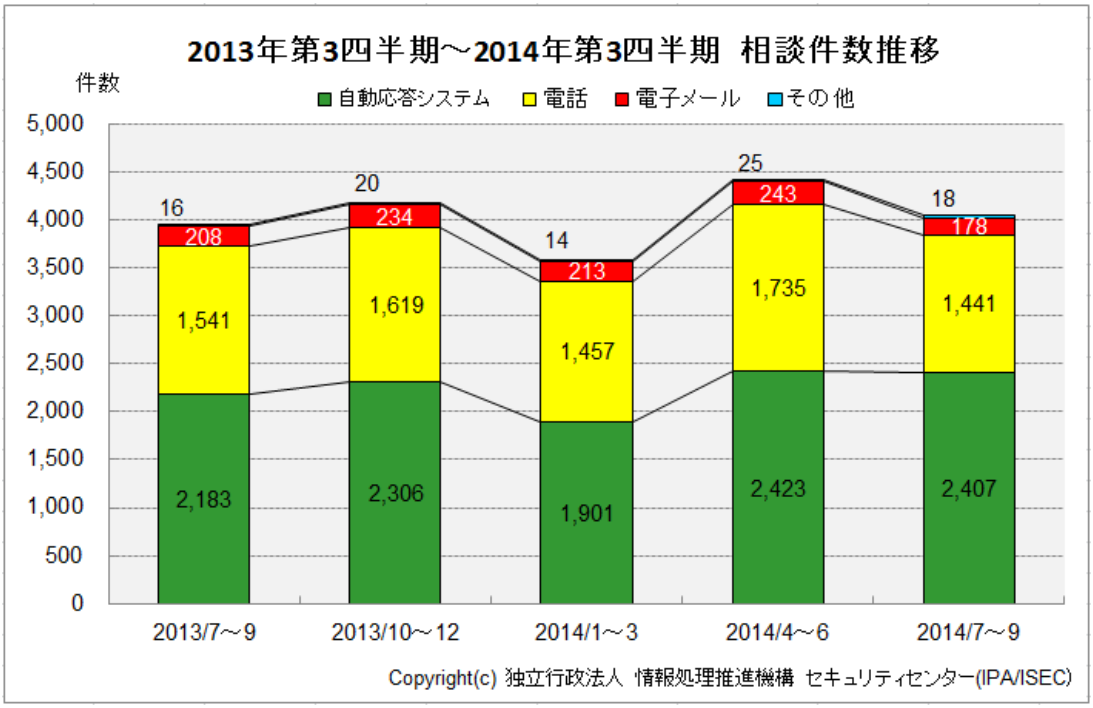


図 3-1. ウイルス・不正アクセス関連の相談件数

表 3-1. ウイルス・不正アクセス関連の相談件数（前掲 図 3-1. の詳細）

	2013/ 7～9		2013/ 10～12		2014/ 1～3		2014/ 4～6		2014/ 7～9	
合計	3,948		4,179		3,585		4,426		4,044	
自動応答システム	2,183	55.3%	2,306	55.2%	1,901	53.0%	2,423	54.7%	2,407	59.5%
電話	1,541	39.0%	1,619	38.7%	1,457	40.6%	1,735	39.2%	1,441	35.6%
電子メール	208	5.3%	234	5.6%	213	6.0%	243	5.5%	178	4.4%
その他	16	0.4%	20	0.5%	14	0.4%	25	0.6%	18	0.4%

注）割合の数値は小数点第二位を四捨五入しており、合計が 100%にならない場合があります。

3-2. 相談事例

（i） プロバイダー変更を勧められ、業者に言われるまま、遠隔操作ツールをパソコンにインストールしてしまって不安。

相談	・利用中のプロバイダーとは異なる事業者から、プロバイダー変更を勧誘する電話があった。 ・事業者に電話越しで言われるまま、よく理解せずにパソコンを操作していたら、いつの間にか遠隔操作ツールのようなソフトウェアをダウンロードし、パソコンに入ってしまったようだ。その事業者は自分のパソコンを遠隔操作して、勝手にプロバイダー変更を設定してしまった。 ・その後プロバイダーは元に戻したが、事業者が引き続き遠隔操作していないか心配。 ・こういったソフトは、セキュリティソフトが入っていれば検出してくれるのか。
回答	**■第三者に遠隔操作させることの危険性について** 遠隔操作によるサポートは、パソコン初心者にとっては便利なサービスです。しかし、自分のパソコンを第三者に自由に操作させることになるため、もし相手に悪意があるとパソコンに何をされるか分かりません。例えばパソコンに格納された情報を盗み見されたり、迷惑メール送信の踏み台にされたりする恐れがあります。そのため、**パソコンを遠隔操作させる時は、信頼できる相手に限定してください**。 また、自分で理解せずに第三者の言われるままにファイルをダウンロードすることは、出所不明なファイルをダウンロードすることと同じで危険です。必ずしも全てが悪質とは限りませんが、もし悪質な場合、パソコンがウイルスに感染するなどの被害を受けてしまいます。 （ご参考） IPA　2012 年 11 月の呼びかけ 「濡れ衣を着せられないよう自己防衛を！」～踏み台として悪用されないために～ https://www.ipa.go.jp/security/txt/2012/11outline.html **■遠隔操作ツールのセキュリティソフトでの検知について** 遠隔操作ツールの中には市販されている正規の製品もあり、必ずしもウイルスとして検知されるわけではありません。 しかしウイルスではない正規の遠隔操作ツールであっても、遠隔操作者に悪意があれば、自分のパソコンに何をされるか分からず危険と言えます。繰り返しとなりますが**パソコンを遠隔操作させる時は、信頼できる相手に限定してください**。

（ii） クレジットカード会社の偽画面に、カード情報を入力してしまった。今後が心配。

相談	・クレジットカード会社のサイトにアクセスした際、身元確認と称した入力画面が現れて、カード番号とセキュリティコードを入力してしまった。 ・それが偽の入力画面であることは、事後にカード会社から連絡が来て判明した。クレジットカードもその時停止してもらった。 ・当時、パソコンにはセキュリティソフトをインストールしていなかった。 ・今後はどうしたら良いか。

回答	パソコンがウイルスに感染し、そのウイルスによって偽画面が表示され、その画面を偽物と気付かずに情報を入力してしまった事例です。 もしセキュリティソフトを導入していれば、パソコンのウイルス感染を防止できた可能性があります。現在は**インターネットバンキングやクレジットカードの情報を盗み取るウイルスが多く、セキュリティソフトを導入していないパソコンでインターネットを利用することは非常に危険**です。セキュリティソフトをパソコンに導入し、常にパターンファイル（ウイルス定義ファイル）を最新の状態に保って利用してください。 クレジットカード会社の会員専用サイトでは、クレジットカード番号・有効期限等利用者情報の入力を求めることは通常ありません。 通常利用する時と異なる入力の要求があった場合は、入力せずに、サービス提供元に確認をしてください。

3-3. 相談内容の詳細分析

(i) 『ワンクリック請求』に関する相談

今四半期は、パソコンとスマートフォンを合わせた『ワンクリック請求』に関する相談が 903 件寄せられました。前四半期と比較すると約 4%（34 件）減少しましたが、直近 1 年間の件数は高止まりしています。また相談のうち、スマートフォンにおける『ワンクリック請求』は 218 件で、前四半期の 236 件から約 8%（18 件）減少しました。

スマートフォンにおける手口の多くはウェブブラウザで請求画面を表示しているだけです。スマートフォンでは前回表示した URL が端末内に保持されるため、ブラウザの再起動時に同じサイトが表示されます。この現象を悪意ある手口と誤解し脅威に感じる利用者が、解決のために請求金額を振り込んでしまっていると考えられます。現状、スマートフォンの場合ワンクリック請求の登録画面が表示されても、慌てる必要はありません。

（参考）

「登録完了画面が現れても、あわてないで！」

～ スマートフォンでのワンクリック請求に注意！ ～

https://www.ipa.go.jp/security/txt/2014/06outline.html

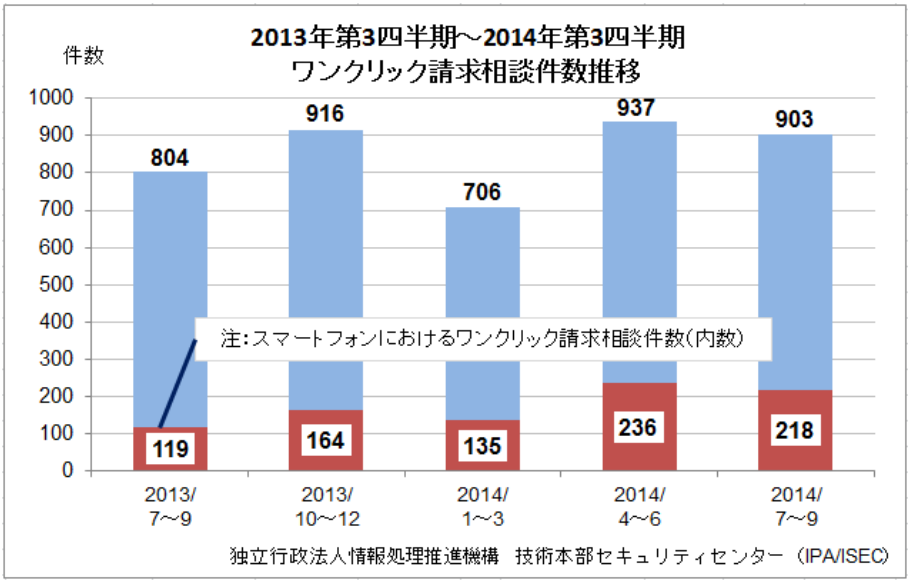


図 3-2.パソコンおよびスマートフォンにおける『ワンクリック請求』相談件数推移

(ii) 『ソフトウェア購入を促し、クレジットカード番号等を入力させる手口』に関する相談

今四半期の相談は 122 件寄せられました。前四半期から約 33%（60 件）の減少でした。

この相談の手口は 2 つに大別されます。パソコンの脆弱性を悪用しウイルスに感染している等、偽の検査結果を画面に表示させ“偽セキュリティソフト”の購入を促す手口と、ウェブブラウザ上の広告表示をパソコン利用者にクリックさせて製品購入を促す手口です。いずれも製品の購入時にクレジットカード番号等を入力させ、入力した番号を窃取するのが目的です。

“偽セキュリティソフト”の相談は、前四半期と同様に今四半期も 0 件でした（前々四半期 19 件）。6 か月相談がなく、**“偽セキュリティソフト”は金銭窃取の手口としては下火になった**と考えられます。個人のパソコンにウイルスを感染させて金銭を要求する手口に使われるウイルスは“偽セキュリティソフト”の他にも“ランサムウェア”、“Bancos”があり[(*13)]、感染パソコン 1 台からより多額の窃取金額が見込めます。“偽セキュリティソフト”が下火になったのは、より効率良く金銭窃取ができる他のウイルスに移行したためと考えられます。

多くの相談は、前述の“偽セキュリティソフト”のようなウイルス感染によるものではなく、自分で URL やウェブブラウザに表示される画像をクリックしたことによって結果的に製品購入を促す画面が表示されてしまうものでした。

中には利用者が自ら望んでそういったソフトウェアをインストールしたケースや、ウェブブラウザ上に表示される「パソコンが危険な状態にある」などの不安を煽るような広告を見て、怖くなりインストールしてしまったケースがありました。その他「パソコンの性能を上げるソフト」「バックアップをしてデータを保護するソフト」などの類似する相談がありました。

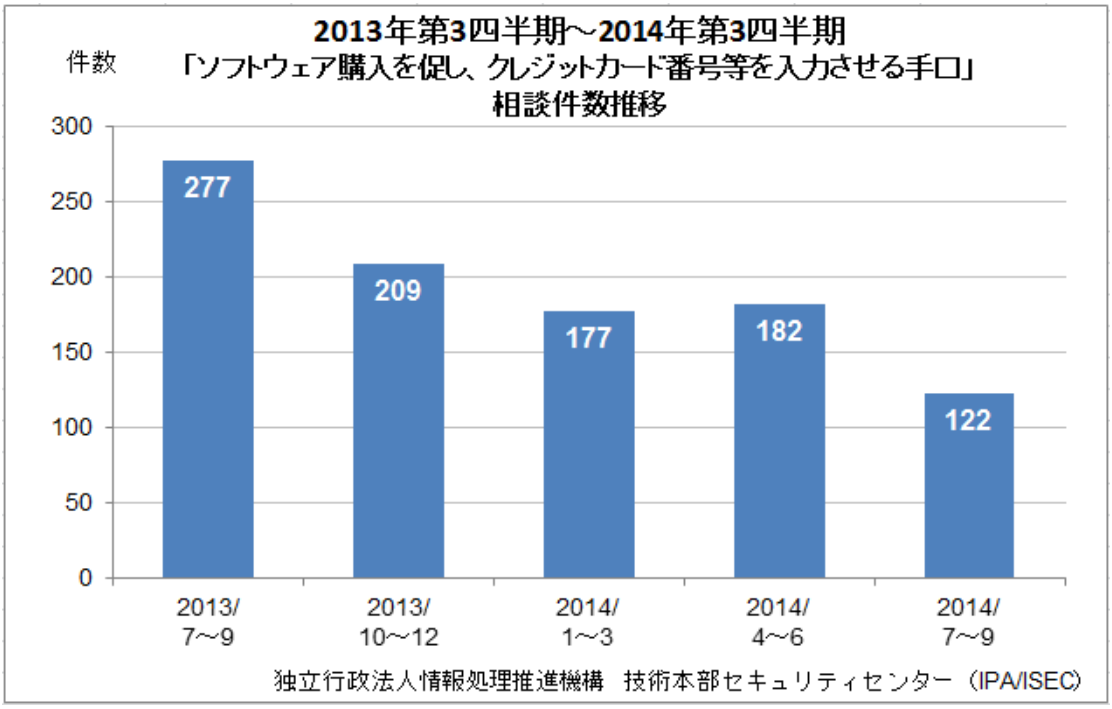


図 3-3.『ソフトウェア購入を促し、クレジットカード番号等を入力させる手口』相談件数推移

(*13) 現時点で確認されているのは“偽セキュリティソフト”による請求額は 1 回 1 万円程度。それに対して“ランサムウェア”では 3 万円～5 万円程度、“Bancos”では最悪の場合、預金残高すべてが窃取される恐れがある。

（iii）『スマートフォン』に関する相談

『スマートフォン』に関する相談は、今四半期 272 件寄せられました。前四半期からは約 9%（26 件）の減少でした。

『スマートフォン』に関する相談のうち、『ワンクリック請求』以外は 54 件でした。その多くは“ウイルス感染”や“不正アクセス”を疑っただけで、被害の無かった相談でした。不安を覚えた場合はまず以下の事柄を確認してください。

- **スマートフォンを使用しない時はパスワードロックをかけているか**
- **インストールしたアプリに問題はないか**
- **身に覚えのないアプリがインストールされていないか**
- **SNS 等に自分の情報を必要以上に公開していないか**
- **スマートフォンを誰かに触らせていないか**
- **スマートフォンを自分の目が届かない所に置くことはないか**

それでも不安が残る場合は、当機構の安心相談窓口（03-5978-7509）にご相談下さい。

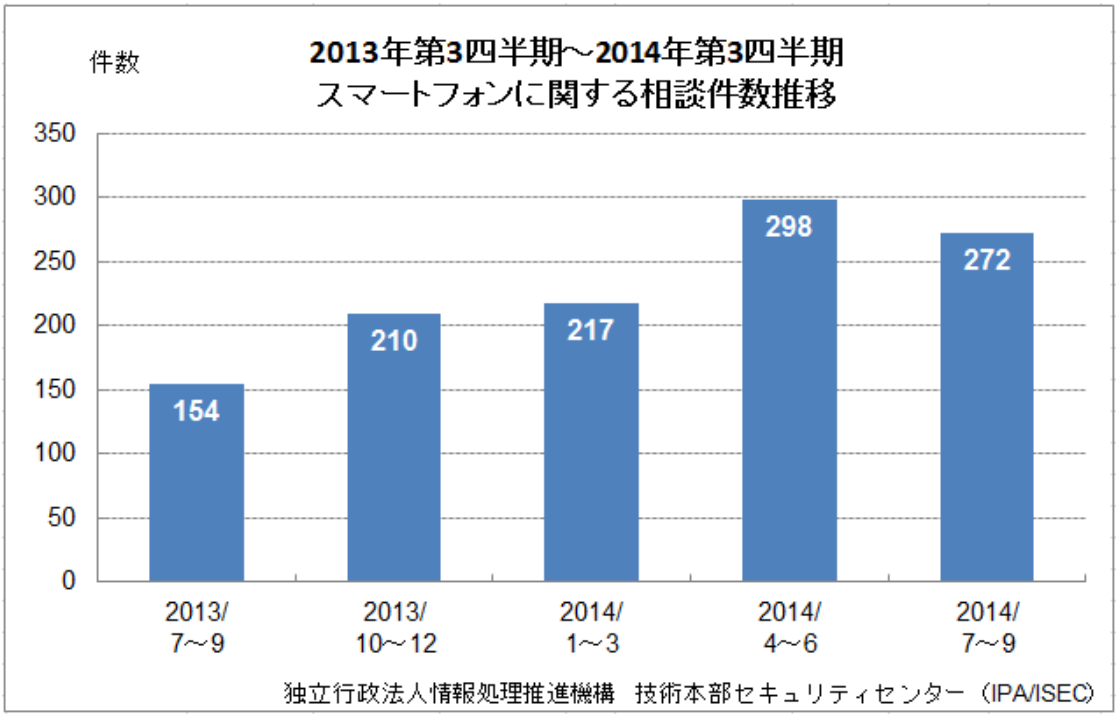


図 3-4.『スマートフォン』に関する相談件数推移

（iv）『インターネットバンキング』に関する相談

『インターネットバンキング』に関する相談は、今四半期 15 件寄せられました。**前四半期からは約 78%（52 件）減少**しました。内訳は、暗証番号や乱数表の入力を求める不正画面を表示するウイルス感染の相談が 9 件（前四半期 44 件）、銀行を騙ったフィッシングメールについての相談が 2 件（前四半期 11 件）、その他が 4 件でした。

相談件数が大幅に減少した理由のひとつとして、2014 年 7 月に警察庁、総務省、JPCERT/CC などが連携して「国際的なボットネットのテイクダウン作戦」(*14) が決行されたことが挙げられます。これは特定された“Bancos”ウイルスの感染パソコンの利用者に対して、プロバイダー等を通じてウイルス駆除を促し、感染端末を減少させる取り組みです。この取り組みにより“Bancos”の感染端末が減少した結果、相談も減少したと考えられます。

“Bancos”ウイルスに感染しているパソコンでインターネットバンキングを利用しようとすると、偽の認証画面が表示されます。そこにパスワードや送金に必要な情報を入力してしまうと、それらの情報が悪意ある第三者に渡り、結果として不正送金の被害に遭ってしまいます。

しかし**正しい画面を知っていれば、すぐに異変に気付くことができます。**各銀行のウェブサイトにインターネットバンキング利用時の正しい画面遷移についての案内や不正送金の被害に遭わないための対策方法が記載されています。これらを事前に確認していれば、もしウイルスに感染していても金銭被害に遭う前に気付くことができます。また、正規の画面かどうか自身で判断できない場合は、銀行に電話で問い合わせすることをお勧めします。

（参考）

「オンラインバンキングの正しい画面を知って、金銭被害から身を守りましょう！」

https://www.ipa.go.jp/security/txt/2014/07outline.html

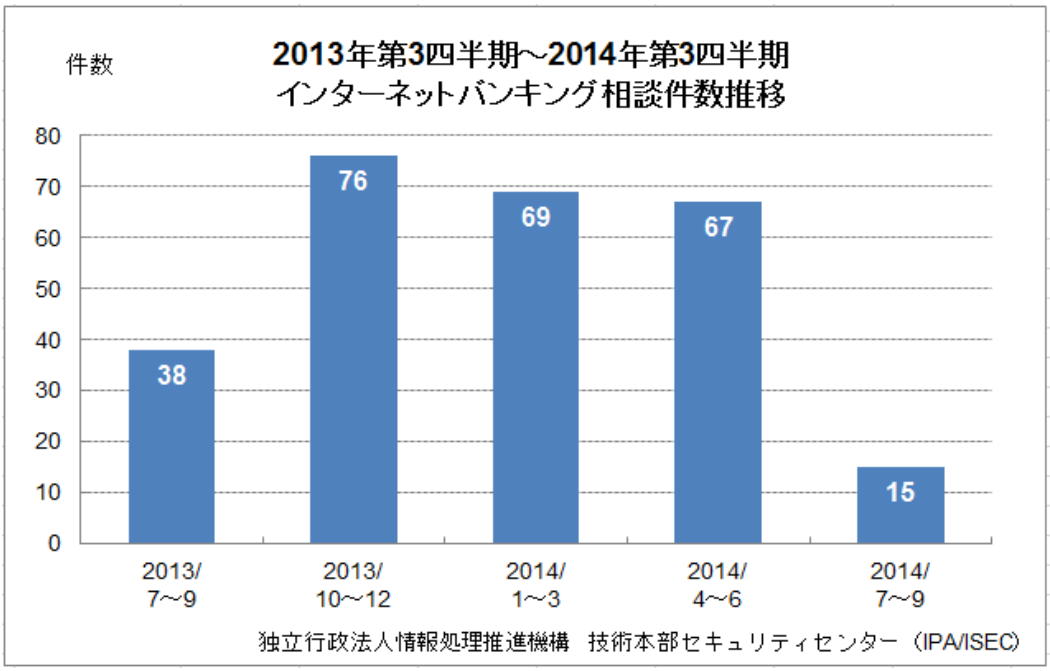


図 3-5.『インターネットバンキング』相談件数推移

(*14) 警察庁： インターネットバンキングに係る不正送金事犯に関連する不正プログラム等の感染端末の特定及びその駆除について ～国際的なボットネットのテイクダウン作戦～
http://www.npa.go.jp/cyber/goz/
JPCERT/CC： JPCERT/CC、「インターネットバンキングに係わる不正送金事犯に関連する不正プログラム等の感染端末の特定及びその駆除について～国際的なボットネットのテイクダウン作戦～」に協力
https://www.jpcert.or.jp/pr/2014/pr140002.html