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

[2015 年第 1 四半期(1 月～3 月)]

本レポートでは、2015 年 1 月 1 日から 2015 年 3 月 31 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

2015 年 4 月 24 日

目次

1. コンピュータウイルス届出状況

1-1. 四半期総括

2015 年第 1 四半期（以下、今四半期）に寄せられたウイルスの検出数 [*1] は 8,038 個で、2014 年第 4 四半期（以下、前四半期）の 19,820 個より 11,782 個（約 59%）減少しました（図 1-2）。今四半期の不正プログラム[*2]検出数は 74,822 個で、前四半期の 89,772 個より 14,950 個（約 17%）減少しました（図 1-3）。また今四半期は、ウイルス感染被害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 位はパソコン内に裏口を仕掛ける不正プログラムの総称である Backdoor（バックドア）で、検出数は 16,637 個（1 月：3,839 個、2 月：11,374 個、3 月：1,424 個）でした。四半期単位では 2014 年第 2 四半期から今四半期にいたるまで増加傾向が続いています。

ウイルスと不正プログラムの総検出数 82,860 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 68,933 個で全体の約 83%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 7,855 個、全体の約 10%でした（表 1-3）。

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

今四半期に最も多く検出されたウイルスは、W32/Mydoom でした。W32/Mydoom の検出数は 4,571 個で、前四半期の 4,844 個より 273 個減少しました。前四半期から大きく減少したウイルスは、W32/Mytob でした。W32/Mytob の検出数は 557 個で、前四半期の 9,008 個から 8,451 個（約 94%）減少しました。また、前四半期に大きく減少した W32/Netsky の検出数は 1,715 個で、前四半期の 3,193 個から更に 1,478 個（約 46%）減少しました。

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 Backdoor で、次に多く検出された不正プログラムは、Downloader（ダウンローダー）でした。Downloader も Backdoor 同様増加傾向が続いています。

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 979 個で、前四半期の 3,203 個より 2,224 個（約 69%）減少しました。

[*1] 検出数：届出として IPA に寄せられた届出者の自組織等で発見・検出したウイルスおよび不正プログラムの数（個数）。

[*2] 不正プログラム：IPA に届出られたもののうち、「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に該当しない（「(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

1-3. ウイルス届出件数

下記グラフ（図 1-1）は、IPA が受け付けた四半期ごとの届出件数の推移を示したものです。今四半期のウイルス届出件数は 937 件で、前四半期の 1,010 件から 73 件減少しました。また、感染被害があった届出はありませんでした。

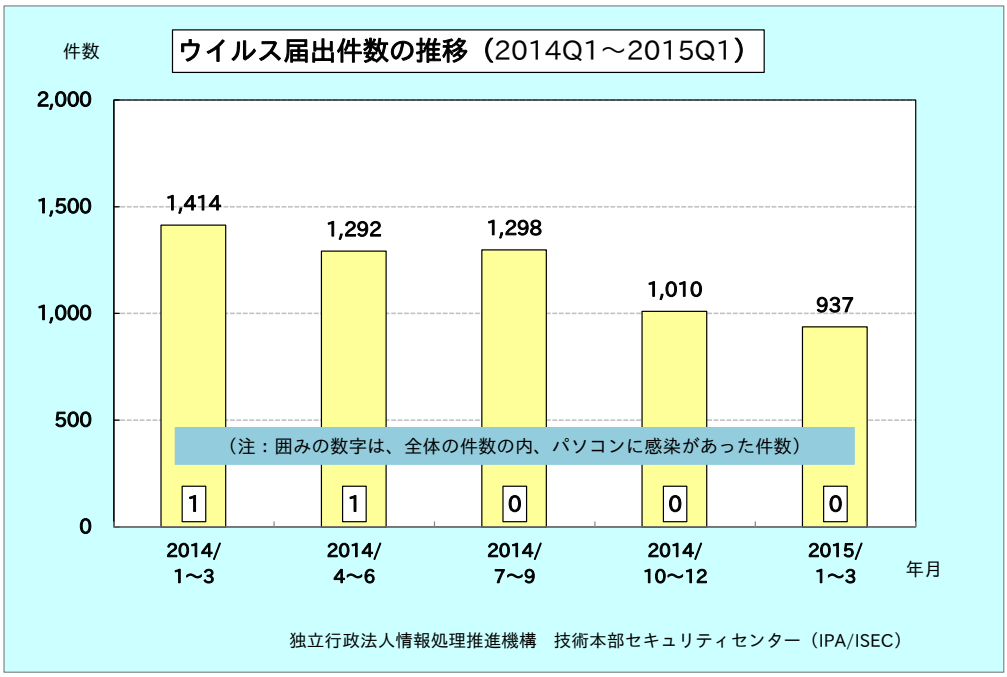


図 1-1：ウイルス届出件数の四半期別推移

1-4. ウイルス検出数

今四半期のウイルス検出数 [*3] は 8,038 個と、前四半期の 19,820 個から 11,782 個（約 59%）減少しました。前四半期に最も多く検出された W32/Mytob が大きく減少したことが主因です。

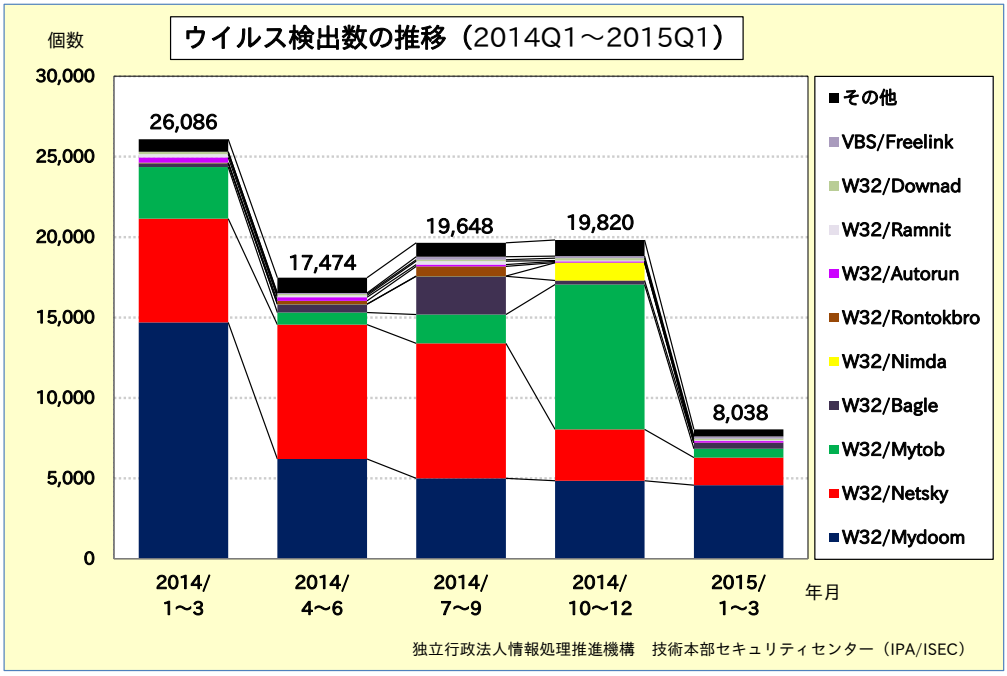


図 1-2：ウイルス検出数の推移

[*3] ウイルス検出数：届出られた「ウイルス」、「不正プログラム」のうち、「ウイルス」の総数を示したもの。

1-5. 不正プログラム検出数

今四半期の不正プログラム検出数 (*4) は 74,822 個と、前四半期の 89,772 個から、14,950 個（約 17%）減少しました。全体的な検出数は前四半期に続いて減少しましたが、Backdoor と Downloader は前四半期に引き続き増加しました。

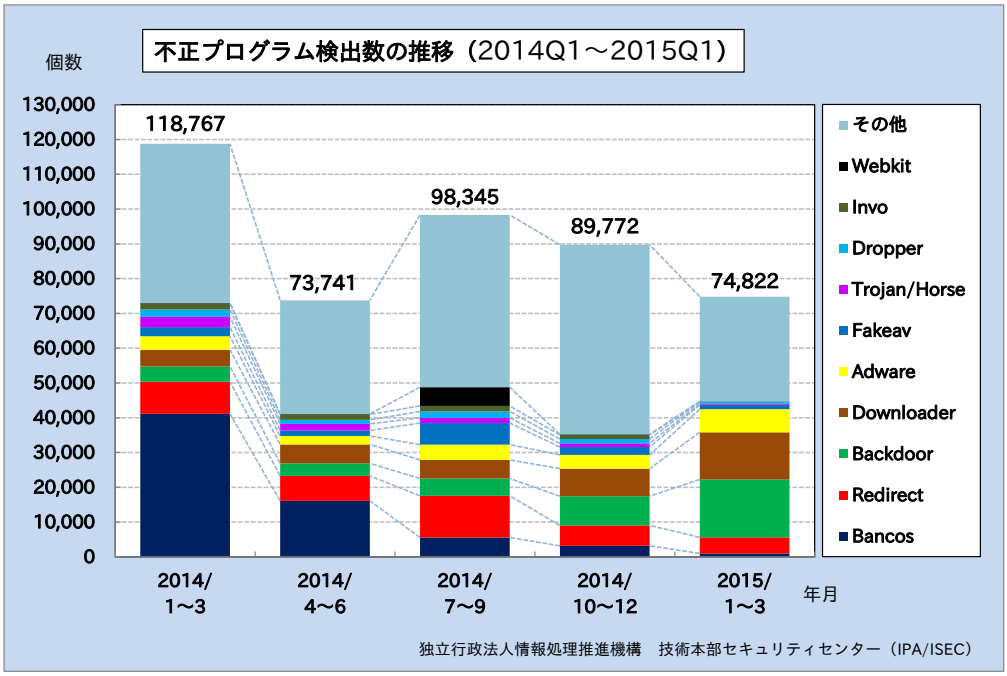


図 1-3：不正プログラム検出数の推移

(*4) 不正プログラム検出数：届出られた「ウイルス」、「不正プログラム」のうち「不正プログラム」の総数を示したもの。

1-6. 2015 年第 1 四半期の検出ウイルス

ウイルスの種類は 60 種類、検出数は Windows/DOS ウイルス 7,740 個、スクリプトウイルス及びマクロウイルス 185 個、携帯端末ウイルス 113 個でした。

表 1-1. 2015 年第 1 四半期の検出ウイルス　(※)印は 2015 年第 1 四半期の新規届出ウイルス

i) Windows/DOS ウイルス	検出数
W32/Mydoom	4571
W32/Netsky	1715
W32/Mytob	557
W32/Bagle	354
W32/Autorun	96
W32/Downad	93
W32/Ramnit	57
W32/Parite	43
W32/Magistr	36
W32/Frethem	22
W32/Klez	22
W32/Rontokbro	18
W32/Virut	17
W32/Lovgate	14
W32/Prettypark	13
W32/Looked	11
W32/Sality	10
W32/Myfip	9
W32/Badtrans	8
W32/Bugbear	7
W32/IRCbot	7
W32/Fbound	6
W32/Imaut	6
W32/Myparty	6
W32/Mumu	5
W32/Gammima	4
W32/Expiro	3
W32/Fakerecy	3
Form	2
Perl/Santy	2
W32/Aliz	2
W32/Bacterra	2
W32/Gibe	2
W32/Sircam	2
W32/Sohanad	2
W32/Stration	2
W32/Swen	2
Perl/Lexac	1
SAMPO	1
Stoned	1

i) Windows/DOS ウイルス	検出数
W32/Gaobot	1
W32/Nimda	1
W32/Nuwar	1
W32/Oror	1
W32/Spyrat	1
W32/Wapomi	1
小計　(46 種類)	7,740

スクリプトウイルス	検出数
VBS/Freelink	140
VBS/LOVELETTER	7
VBS/DUNIHI	5
VBS/Nobelman(※)	2
VBS/Solow	1
Wscript/Fortnight	1
小計　(6 種類)	156

マクロウイルス	検出数
XM/Laroux	21
W97M/Marker	2
W97M/Relax	2
WM/Wazzu	2
X97M/Divi	1
XM/Mailcab	1
小計　(6 種類)	29

ii)携帯端末ウイルス	検出数
AndroidOS/Lotoor	112
AndroidOS/Ginmaster	1
小計　(2 種類)	113

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. 2015 年第 1 四半期に IPA に初めて届出のあったウイルスの概要

（1）VBS/Nobelman　届出月：2015 年 1 月

このウイルスは、Windows OS を感染対象とした Visual Basic Script(VBS) で記述されたウイルスです。

利用者がウイルスに感染したファイルを開くと感染します。

感染すると、レジストリの情報が書き換えられ、アドレス帳に登録されているメールアドレス宛へウイルスが送信されます。

1-8. ウイルス届出者構成及び検出経路

今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。

表 1-2. ウイルス届出者別件数

	2014/ 1～3	2014/ 4～6	2014/ 7～9	2014/ 10～12	2015/ 1～3
一般法人	1,404	1,269	1,281	930	887
	(99.3%)	(98.2%)	(98.7%)	(92.1%)	(94.7%)
個人	0	0	0	0	1
	(0.0%)	(0.0%)	(0.0%)	(0.0%)	(0.1%)
教育機関	10	23	17	80	49
	(0.7%)	(1.8%)	(1.3%)	(7.9%)	(5.2%)
合計	1,414	1,292	1,298	1,010	937

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）

	2014/ 1～3	2014/ 4～6	2014/ 7～9	2014/ 10～12	2015/ 1～3
メール	25,927	17,396	19,581	19,469	7,855
	(17.9%)	(19.1%)	(16.6%)	(17.8%)	(9.5%)
ダウンロード ファイル	90,861	59,201	82,104	65,973	68,933
	(62.7%)	(64.9%)	(69.6%)	(60.2%)	(83.2%)
外部記憶 媒体	1	41	0	3	0
	(0.001%)	(0.045%)	(0.000%)	(0.003%)	(0.000%)
ネット ワーク	250	125	107	491	109
	(0.2%)	(0.1%)	(0.1%)	(0.4%)	(0.1%)
不明・その他	27,814	14,452	16,201	23,656	5,963
	(19.2%)	(15.8%)	(13.7%)	(21.6%)	(7.2%)
合計	144,853	91,215	117,993	109,592	82,860

・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

今四半期のコンピュータ不正アクセス届出の総数は 34 件で、2014 年第 4 四半期（以下、前四半期）の 28 件と比べて 6 件増加しました（図 2-1）。そのうち『なりすまし』の届出が 19 件（前四半期：11 件）、『侵入』の届出が 5 件（同：4 件）、『不正プログラム埋込』の届出が 2 件（同：3 件）、『DoS』の届出が 1 件（同：0 件）などでした（表 2-1）。

今四半期の 19 件の『なりすまし』の届出は、前四半期と比べ大きく増加しています（表 2-1）。なりすましによる具体的な不正アクセスの被害として、メールアカウントの不正利用によってスパムメール送信の踏み台とされてしまった届出が最も多く、8 件でした。その他、ショッピングサイトへの不正ログインによって身に覚えのない商品の購入手続きをされてしまった届出が 1 件、IP-PBX（IP 電話）への不正接続によって国外宛に電話発信をされてしまった届出が 1 件、オンラインゲームのアカウント情報を伝えてしまったために不正にデータ引継操作をされて乗っ取られてしまった届出が 1 件などでした。これらの届出のうち、ブルートフォースアタック (*5) や辞書攻撃、パスワードリスト攻撃、フィッシングなど、ログ情報やアカウント所有者の行動から不正ログイン（パスワード情報の漏えい）の原因が明らかな被害もありますが、19 件のうち 11 件は原因の特定に至っていません。

一方で、攻撃者による不正アクセスが失敗に終わり、被害に至らなかった『アクセス形跡（未遂）』の届出が 2 件ありました。1 件はフィルタ機能によってメールサーバへログインを試みる不審なアクセスを遮断できたことで被害に至らずに済みました。もう 1 件は、FTP サーバに対して辞書攻撃と思われる大量のログイン試行をされてしまったものの、試行された情報ではログインができなかったため被害には至らずに済みました。

前四半期に続き、今四半期でも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。利用者においては不正ログインによる SNS の乗っ取りやショッピングサイトの不正利用を防ぐため、“推測が容易となるパスワードを設定していないか”、“パスワードの使いまわしをしていないか”など、パスワード管理 (*6) における基本的な対策ができているか改めて確認してください。また、システム管理者においては利用者の対策に加え、“初期設定のユーザ ID の利用を禁止する”などアカウント情報への取り扱いにも注意が必要です。さらに、ブルートフォースアタックや辞書攻撃を想定した“ログイン試行回数制限を設定する”、“フィルタ機能で不要なアクセスを制限する”といった、システムにおける対策についても検討してください。

今四半期では、前述の『アクセス形跡（未遂）』の届出 2 件を含め、被害に至らなかった届出が 6 件ありました。その手口は SQL インジェクション (*7) や bash の脆弱性 (*8) の悪用などでした。いずれもセキュアなウェブサイト設計、稼動プログラムのバージョンアップ対応といった基本的な対策を実施していれば被害を防げるものです。システム管理者においては稼動プログラムのバージョンアップ対応をはじめとした、基本的なセキュリティ対策を確実に実施してください。

(*5) ブルートフォースアタック： 文字の組み合わせを総当たりで試行する攻撃。

(*6) パスワードーもっと強くキミを守りたいー
https://www.ipa.go.jp/security/keihatsu/munekyun-pw/index.html

(*7) SQL インジェクション攻撃に関する注意喚起
https://www.ipa.go.jp/security/vuln/documents/2008/200805_SQLinjection.html

(*8) bash の脆弱性対策について(CVE-2014-6271 等)
https://www.ipa.go.jp/security/ciadr/vul/20140926-bash.html

2-2. 被害事例

(i) FTP[(*9)]アカウントに不正ログインされ詐欺サイトを構築された

被害の概要	・ウェブサーバに大量のファイルがアップロードされていることを発見した。 ・調査の結果、FTP アカウントを悪用され、6GB を超えるブランド品の通販サイトと思われるコンテンツをアップロードされていることが確認された。しかし、元々、公開していたコンテンツへの改ざんなどは確認されなかった。 ・FTP アカウントのパスワードが安易な内容だったため、推測により不正ログインされてしまったと考えられる。
解説・対策	FTP アカウントの悪用により不正ログインされ、ウェブサーバに大量の不審なファイルをアップロードされてしまった事例です。 公開していたコンテンツの改ざんはなく、ブランド品の通販サイトと思われるコンテンツを大量にアップロードされたとのことなので、個人情報や金銭を摂取することを目的とした詐欺サイトの構築、公開に悪用されたと考えられます。 脆弱性を突くような攻撃への対策として、OS やソフトウェアのバージョンを最新に保つことも重要ですが、アカウント情報を適切に設定、管理することも同じように重要です。不正ログインされてしまう可能性が高くなるため、特に初期設定の ID や安易なパスワードは、原則として使用しないことを推奨します。 また、万が一、不正なアップロードをされてしまった場合に、早期発見、対応が行えるよう、FTP サーバへのアクセスやウェブサーバ上での操作など、不審なログに対して、アラートを出力するといったような対策も有効となります。

(ii) CMS の脆弱性を突かれて不正な PHP[(*10)]ファイルを設置された

被害の概要	・ウェブサーバへアクセスすると不正なページが表示されるようになった。 ・確認したところ、2 種類の不審な PHP ファイルが設置されていた。 ・PHP ファイルはバックドアとして機能していたようで、PHP ファイルを通じて不正なページを表示するファイルを設置されていた。 ・利用していた CMS は脆弱性が存在するバージョンで修復がされていない状態であったため、脆弱性を突かれて PHP ファイルを設置されたと推測される。 ・表示された不正なページの内容は海外で発生したテロに関するメッセージと思われるもので、ハクティビスト[(*11)]による犯行の可能性が考えられる。
解説・対策	CMS が適切にバージョン管理されていなかったことで、画像ファイルをアップロードされるというウェブ改ざん被害に遭ってしまった事例です。被害は特定の画像が表示されるように書き換えられただけに留まり、大きな被害には至りませんでした。 なお、届出はありませんでしたが、報道によると 2015 年 3 月、「Islamic State (ISIS)」と称する攻撃者により、CMS のプラグインの脆弱性を悪用したと想定されるウェブサイト改ざん被害[(*12)]が複数発生しました。 ウェブサイト管理を容易にする目的で多用される CMS ですが、CMS 自体を適切に管理していないとウェブ改ざん被害の可能性が高まります。利用している CMS の情報を把握し、常に最新のバージョンで稼動するよう、アップデートの確認からバージョンアップの実施までの具体的な作業フローを事前に確立しておく必要があります。

(*9) FTP（File Transfer Protocol）：ファイル転送を行うためのプロトコル。
(*10) PHP（PHP: Hypertext Preprocessor）：動的に HTML データを生成するスクリプト言語。
(*11) ハクティビスト ：社会的・政治的な主張を目的としたハッキング活動を行う者を指す用語。
(*12) 警察庁 ：「Islamic State（ISIS）」と称する者によるウェブサイト改ざんに係る注意喚起について
http://www.npa.go.jp/cyberpolice/detect/pdf/20150312.pdf

2-3. 届出件数

今四半期の届出件数は 34 件で、そのうち被害があったのは 28 件と全体の約 82%を占めました。

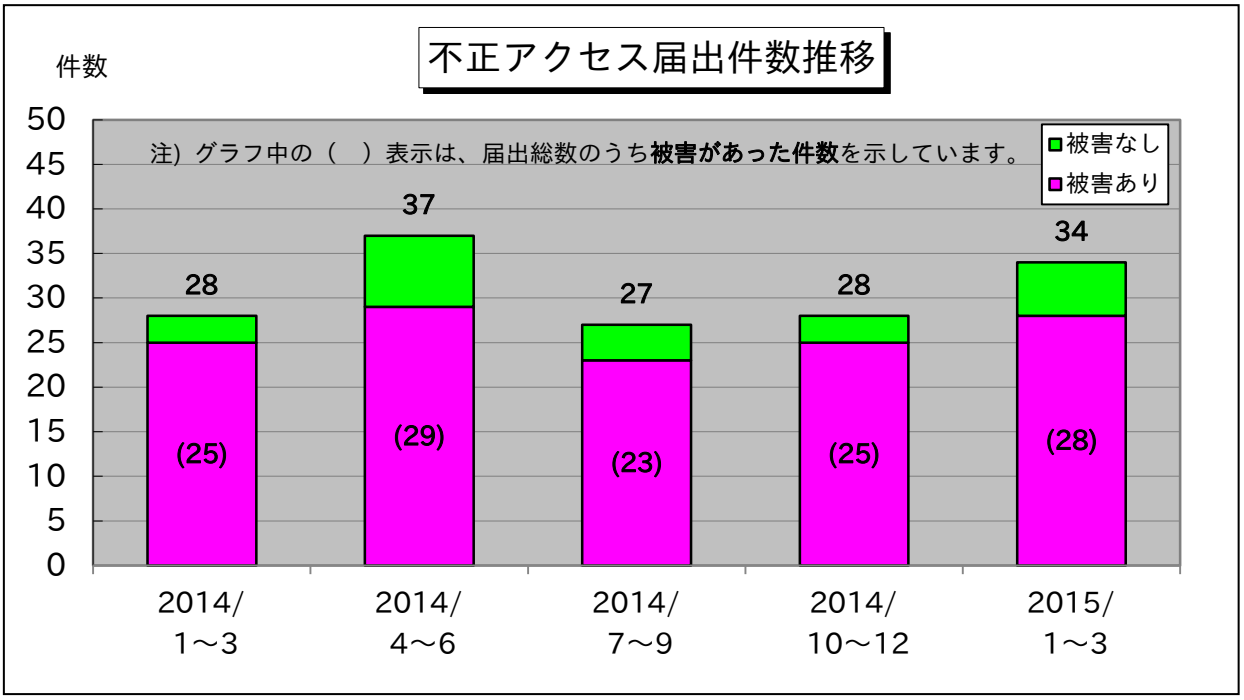


図 2-1. 不正アクセス届出件数の推移

2-4. 届出種別

前述の実際に被害に遭った届出種別には「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）」がありました。

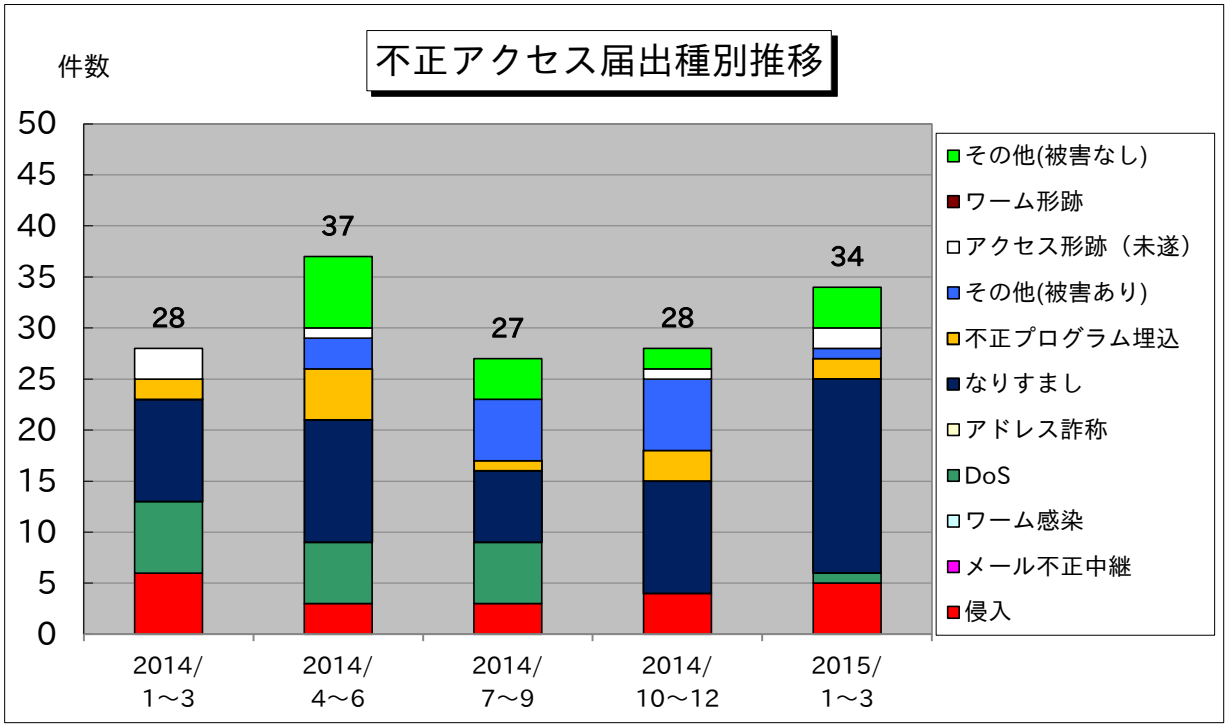


図 2-2. 不正アクセス届出種別の推移

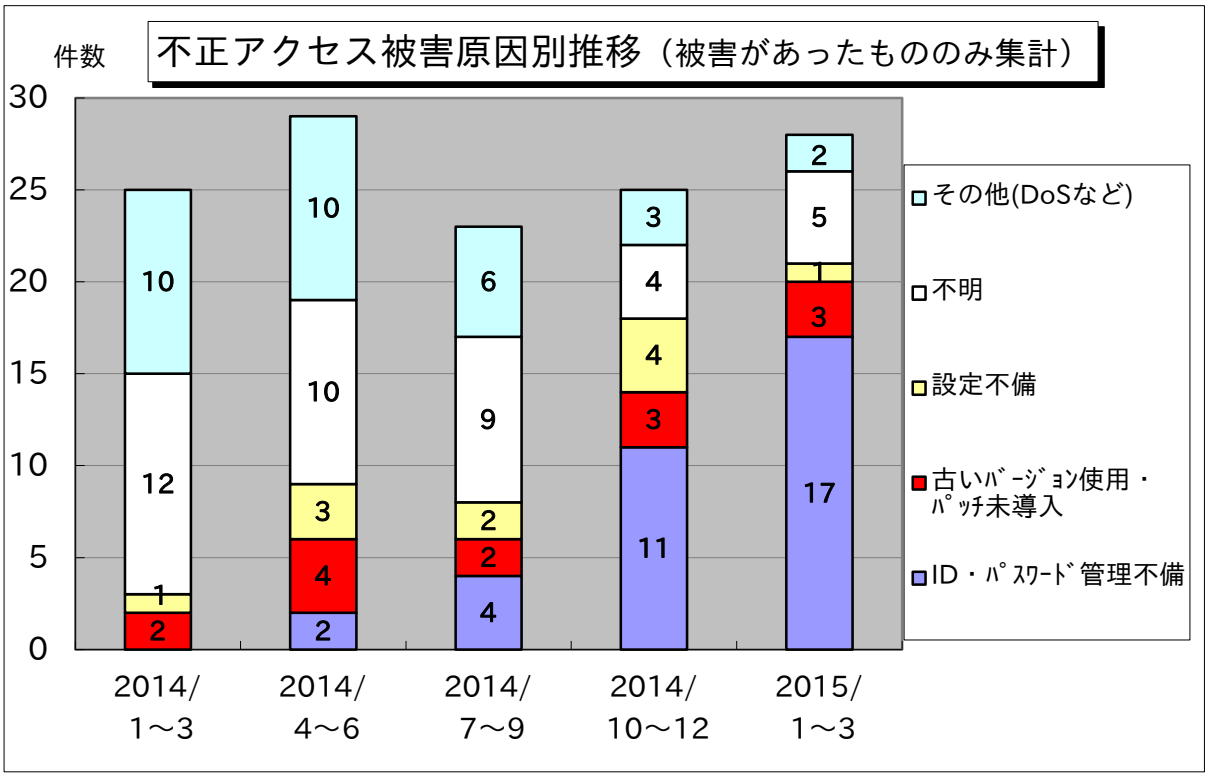
表 2-1. 不正アクセス届出種別の四半期推移

	2014年 第1四半期		2014年 第2四半期		2014年 第3四半期		2014年 第4四半期		2015年 第1四半期	
侵入	6	21.4%	3	8.1%	3	11.1%	4	14.3%	5	15.6%
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	25.0%	6	13.5%	6	22.2%	0	0.0%	1	3.1%
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	10	35.7%	12	32.4%	7	25.9%	11	39.3%	19	56.3%
不正プログラム埋込	2	7.1%	5	10.8%	1	3.7%	3	10.7%	2	3.1%
その他（被害あり）	0	0.0%	3	13.5%	6	22.2%	7	25.0%	1	3.1%
アクセス形跡（未遂）	3	10.7%	1	8.1%	0	0.0%	1	3.6%	2	6.3%
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%	7	13.5%	4	14.8%	2	7.1%	4	12.5%
合　計（件）	**28**		**37**		**27**		**28**		**34**	

注）網掛け部分は、今四半期の届出種別のうち被害があったものです。
注）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。

2-5. 被害原因

実際に被害があった届出（28 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 17 件、古いバージョン使用・パッチ未導入が 3 件、設定不備が 1 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、一般法人ユーザが 18 件、個人ユーザが 5 件、教育・研究・公的機関が 11 件でした。

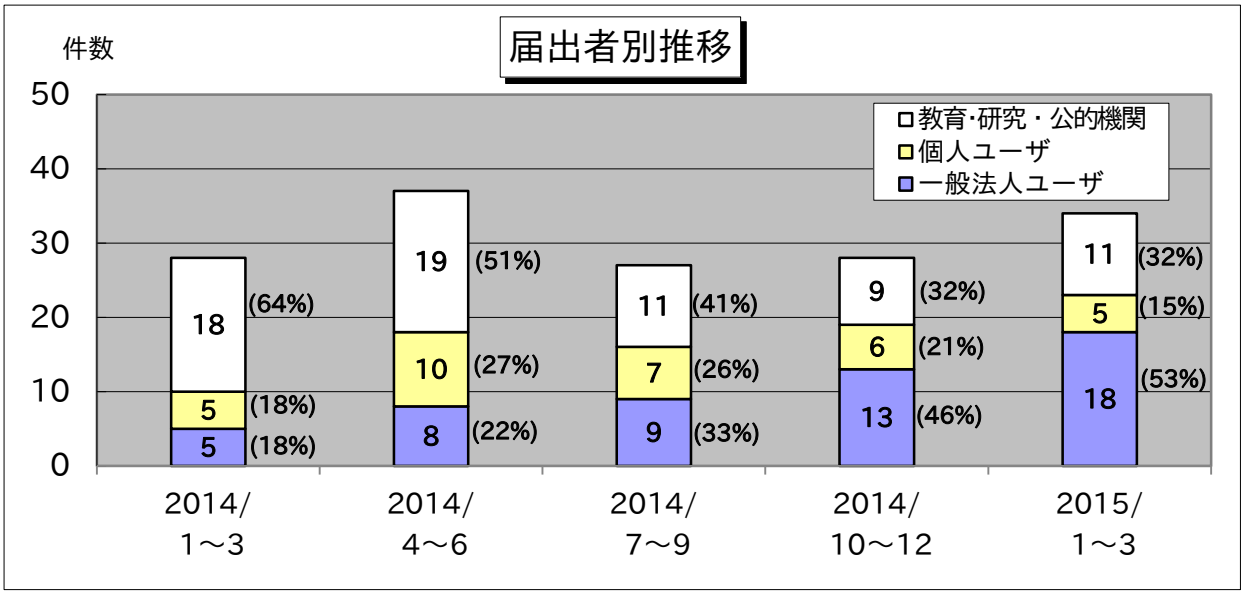


図 2-4. 届出者別推移

・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

今四半期に「情報セキュリティ安心相談窓口」に寄せられた相談件数は 3,311 件で、2014 年第 4 四半期（以下、前四半期）の 3,543 件に比べて 232 件（約 7%）減少しました（図 3-1）。

相談員による対応件数は 1,532 件で、その中で最も多かったのが約半数を占める『ワンクリック請求』で 733 件（前四半期：755 件）でした。そのうちスマートフォンにおける『ワンクリック請求』に限ると 210 件（同：201 件）で、ともに件数は前四半期から横這いでした（図 3-2）。

『インターネットバンキング』に関する相談は 24 件（同：7 件）でした。そのうち、相談者のパソコンが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に感染していたのは 21 件（同：2 件）でした。（図 3-3）。その相談件数は 2014 年第 3 四半期（7 月～9 月）にそれまでの約四分の一（15 件）に激減して以来、低水準で推移しています。しかし今四半期は 24 件と再び増加しました。

グラフは掲出していませんが、今期の身代金型ウイルス『ランサムウェア』に関する相談は 6 件（同：5 件）でした。2014 年 12 月に、日本語の脅迫文が表示されるランサムウェアの存在が指摘されましたが [(*13)]、今四半期は IPA に相談がありませんでした [(*14)]。また『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』に関する相談は 96 件（同：143 件）でした。

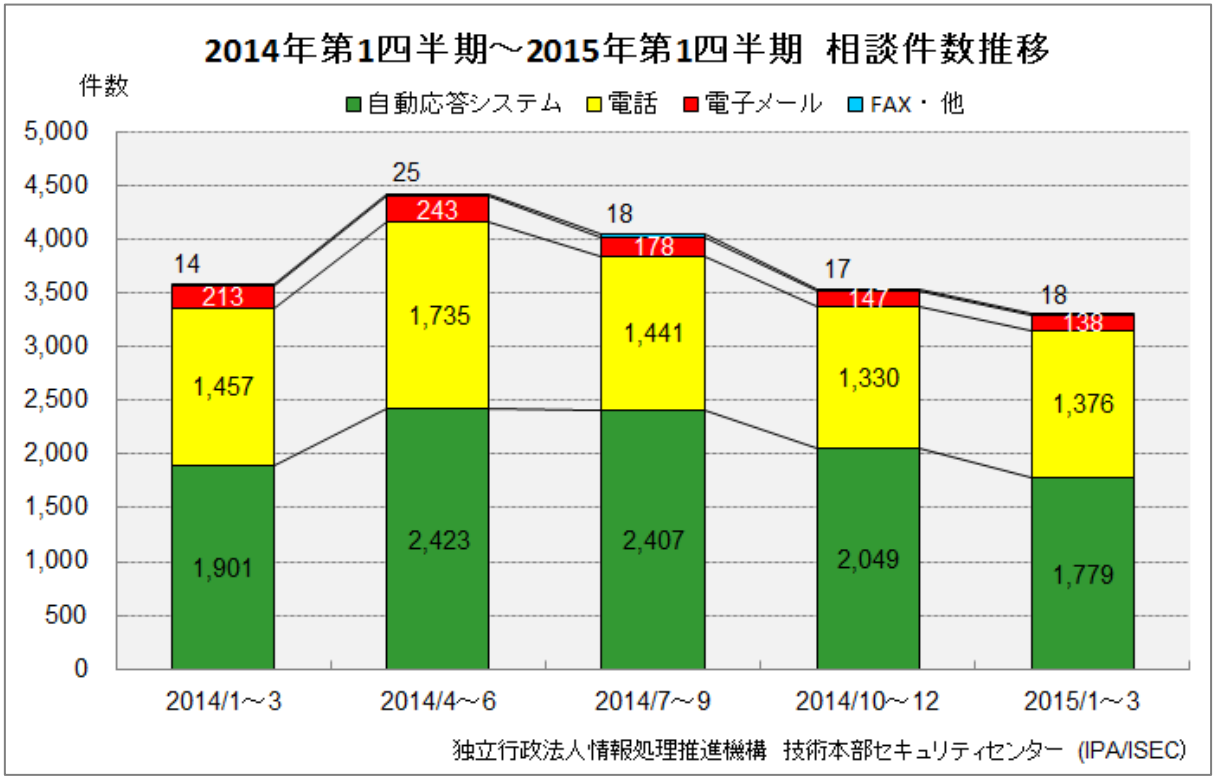


図 3-1. ウイルス・不正アクセス関連の相談件数

(*13) シマンテック：日本のユーザーを狙って設計された TorLocker ランサムウェアの亜種
http://www.symantec.com/connect/blogs/torlocker

(*14) 海外の捜査機関（FBI Cybercrime Division、Interpol など）を騙ったランサムウェアの感染被害が 4 件、ランサムウェアの種類が不明の感染被害が 2 件。

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）

	2014/ 1～3		2014/ 4～6		2014/ 7～9		2014/ 10～12		2015/ 1～3	
合計	3,585		4,426		4,044		3,543		3,311	
自動応答システム	1,901	53.0%	2,423	54.7%	2,407	59.5%	2,049	57.8%	1,779	53.7%
電話	1,457	40.6%	1,735	39.2%	1,441	35.6%	1,330	37.5%	1,376	41.6%
電子メール	213	6.0%	243	5.5%	178	4.4%	147	4.1%	138	4.2%
その他	14	0.4%	25	0.6%	18	0.4%	17	0.5%	18	0.5%

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） Android 端末で、突然画面下部にウイルス感染の警告文が出た。この警告文は信用して良いのか。

相談	・Android 端末で色々なサイトを見て回っている最中に、画面下に警告文が出てきた。 ・「この端末はウイルスに感染しました。感染を解除するには以下のアプリをインストールしてください。」という内容。 ・その警告文をタップすると、あるセキュリティアプリの Google Play ページが出てきたので、表示に従ってアプリをインストールした。 ・その後、誘導のされ方に不安を覚えたので、そのセキュリティアプリはアンインストールした。 ・最初に出た画面下部の警告文は信用して良いのか。
回答	IPA でも、画面下部に警告文が出るスマートフォン用サイトを複数確認していますが、そのような警告文は広告表示に過ぎません。また、スマートフォンはパソコンと比較して画面が小さいため、それが単なる広告表示なのか、それとも端末自体やアプリの機能によって表示されている警告なのかの区別がつきにくいのが特徴です。 この場合は不正アプリの可能性は低いと考えられますが、必ずしも全てがそうとは限りません。もし悪質な場合、端末内の情報が窃取されるなどの被害を受ける可能性があります。アプリをインストールする際には、利用者の評判やインストール時に表示されるアクセス権限（パーミッション）を確認する等、安全性について確認した上でインストールしてください。

（ii）Android 端末で LINE を使おうとしたら、突然「誰かが LINE に侵入しようとしました」という通知が現れ、カメラのシャッター音が鳴った。

相談	・Android 端末で LINE を使おうとしたら、突然「誰かが LINE に侵入しようとしました」という通知が出てきた。それとともにカメラのシャッター音が鳴った。 ・スマートフォンが誰かに乗っ取られているのではないか。 ・なお端末上では無料のセキュリティアプリを使用している。
回答	公式サイトによれば、その通知はご利用中のセキュリティアプリの仕様によるものと考えられます。LINE へのログイン回数が規定回数以上失敗すると、「誰かが LINE に侵入しようとしました」という、警告メッセージが発せられます。シャッター音もそのセキュリティアプリが実際にカメラで撮影したことによるものです。この機能は正規の利用者以外の第三者が不正にログインしようとした際のアラート機能のようなものです。 規定回数以上失敗すると、写真が撮られ、画像が端末内に保存されます。これにより正規の利用者は不正にログインしようとした人物の特定が容易になると考えられます。 何かあっても慌てずに済むよう、ご利用中のアプリ、特に“セキュリティアプリ”と“頻繁に利用するアプリ”については、事前に機能を把握しておくことを勧めます。

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 733 件寄せられました。前四半期と比較すると 22 件（約 3%）の減少でほぼ横這いです。また同相談のうち、スマートフォンにおける『ワンクリック請求』は 210 件で、前四半期の 201 件から 9 件（約 4%）の増加でした。こちらも前四半期と比較して横這いでした。

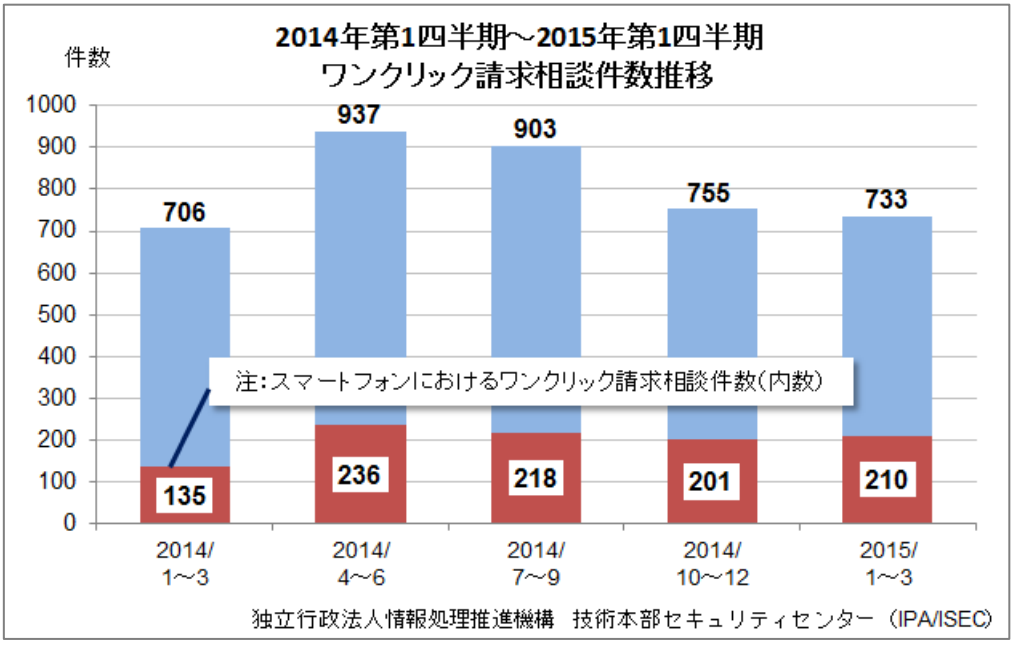


図 3-2.パソコンおよびスマートフォンにおける『ワンクリック請求』相談件数推移

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料金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起動前と同じページが表示されます。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。

2014 年 12 月以降、“料金請求画面の表示と同時に写真も撮られたようだ”という相談が寄せられるようになりました。実際にはカメラは作動しておらず、シャッター音の音楽データを再生しているだけと考えられます。利用者に“自分の写真を撮影、送信された”と誤認させ、振り込みを誘発させることを狙った手口と考えられます。

また、料金請求画面の表示につづいて、電話を発信させる画面を表示させるスマートフォン用ウェブサイトの存在も確認されています。今後も様々な手口が出現する可能性がありますが、スマートフォンの場合はワンクリック請求の料金請求画面が表示されても慌てる必要はありません。

（参考）

「スマートフォンでのワンクリック請求の新しい手口にご用心」
～ 業者への電話、メールは絶対 NG ～
https://www.ipa.go.jp/security/txt/2015/04outline.html

(ii) 『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 24 件寄せられました。前四半期からは 17 件増加しました。

相談件数は 2014 年第 3 四半期（7 月～9 月）にそれまでの約四分の一（15 件）に激減して以来、低水準で推移しています。しかし今四半期は 24 件と再び増加しました。

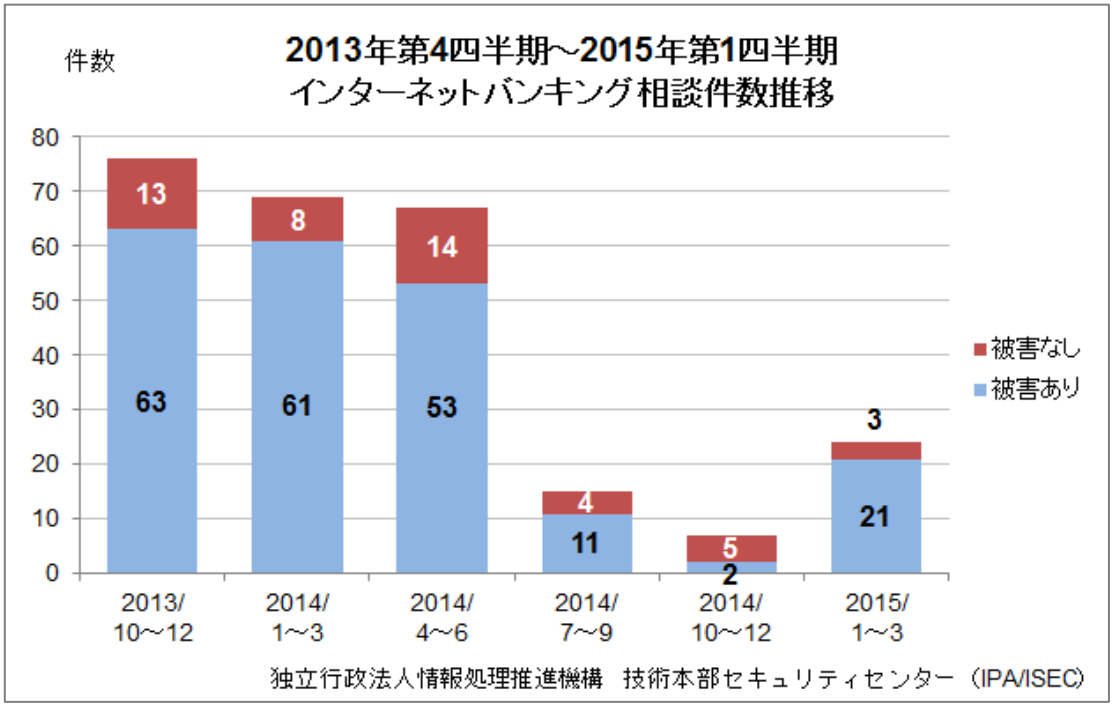


図 3-3.『インターネットバンキング』相談件数推移

今四半期の 24 件の相談中、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”が相談者のパソコンに感染していたケースが 21 件ありました。異常を察知した利用者はその現象別に次の 3 タイプに分かれます。

なおタイプ 3 の相談は今四半期に初めて寄せられたものです。

タイプ 1　金融機関の画面を装ってはいるが、ログイン画面にいつもと違う“入力項目”または“メッセージ”が出たために気付いた。

例：

・普段とは異なり、手元の乱数表の数字を全て入力させる画面が出現した。

・普段とは異なり、暗証番号を入力させる画面が出現した。

・「あなたのコンピュータをシステムが認識できませんでした。引き続き利用するためには表からコードを入力してください。」等といった普段と異なるメッセージが表示された。

タイプ 2　ログイン画面やログイン直後の画面表示が異常 (*15) なために気付いた。

例：

・数字、パーセント記号などの羅列が出現した。

・何も書かれていない真っ白な画面が出現した。

タイプ 3　ログイン時に、金融機関側からウイルス感染の警告があったために気付いた。

例：

・ログイン時に「ウイルス感染の恐れがあるためログインできません」といった内容のメッセージが表示された。金融機関に電話した確認した所、自分のパソコンがインターネットバンキングを狙ったウイルスに感染している可能性が高いと言われた。

中には“事前に何度か金融機関のサイトを見ていたおかげで、正しい画面を知っており、すぐに異変に気付いた”という相談もありました。正しい画面を認識していれば、すぐに異変に気付くことができます。各金融機関のウェブサイトではインターネットバンキング利用時の正しい画面遷移や、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、仮にウイルスに感染してしまっ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を自身で判断できない場合は、金融機関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

またタイプ 3 のように金融機関側がインターネットバンキング利用者のパソコンに対してウイルス感染の可能性を検知した場合、顧客預金保護のために自動で利用停止する仕組みを導入するケースが増えています。もしそのような警告が表示された場合、直ちに金融機関に連絡して今後の対処法を確認してください。

(*15) ウイルスの不具合や、ウイルス動作範囲外の OS など何らかの理由によって、ウイルスが正常に動作していないと考えられるケース。