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 2 四半期（4 月～6 月)]

本レポートでは、2014 年 4 月 1 日から 2014 年 6 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 7 月 25 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 2 四半期に寄せられたウイルスの検出数 (*1) は、2014 年第 1 四半期 26,086 個より 8,612 個（約 33%）少ない 17,474 個でした（図 1-2 参照）。また、2014 年第 2 四半期の不正プログラム (*2) 検出数は 2014 年第 1 四半期 118,767 個から 45,026 個（約 38%）少ない 73,741 個でした（図 1-3 参照）。

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の Bancos で 16,086 個でした。しかし同時に検出数の減少も顕著で前四半期の 41,113 個から約 6 割減少しました。これは前四半期の検出が突出して多かったためで、依然多く検出されています。

ウイルスと不正プログラムの総検出数 91,215 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 59,201 個で全体の約 65%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 17,396 個、全体の約 19%でした（表 1-4 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が 1 件寄せられました。
下記の表 1-1 は、その時に感染した「W32/Burnwoo（バーンウー）」というウイルスの被害の詳細です。

表 1-1. ウイルス感染被害届出詳細

届出元	一般企業
感染被害対象	3 台の社内パソコン
セキュリティソフトの利用	あり（パターンファイルを最新にしながら利用）
感染経路	外部記憶媒体（デジカメ用 SD メモリカード）
被害状況	感染パソコンからは、ファイルの改ざんや破壊、情報漏えい等の実被害は確認されなかった。（感染パソコンから不審なウェブサイトへの接続痕跡があったが、感染当時は既に当該ウェブサイトが閉鎖していたため、実害発生に至らなかった。）
発見方法	インターネット接続ログの解析により社内の 3 台のパソコンが、不審なウェブサイトにアクセスしている痕跡が発見された。 その 3 台のパソコンを調査した所、いずれのパソコンでも、特定のデジカメ用 SD メモリカードを使用していたことが判明した。 そのため SD メモリカードを調査した所、W32/Burnwoo に感染していたことが判明した。

(*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

感染原因	ウイルスに感染していることに気が付かないままデジカメ用 SD メモリカードをパソコンに接続し、SD メモリカード内にある画像フォルダにあったファイルを実行したため感染。このファイルはアイコンがフォルダに偽装されていたため、開封してしまったと考えられる。この SD メモリカードへの感染は、自社で管理していない第三者のパソコンと写真のやりとりを行った際に SD メモリカードを使用したためと考えられる。 また、感染パソコンにインストールされていたセキュリティソフトは、最新の状態であったにもかかわらず、W32/Burnwoo を検知しなかった。
対　処	インターネット接続ログから感染パソコンを割り出し、当該パソコンを即座にネットワークから切り離した。その後、パソコンを初期化しウイルスの駆除を実施。 感染した SD メモリカードも、初期化しウイルスの駆除を実施。

W32/Burnwoo は、主に USB メモリ等の外部記憶媒体に自分自身をコピーすることで感染を拡大するウイルスです（1-7.（3）参照）。本事例では、W32/Burnwoo に感染していた SD メモリカード内のファイルがフォルダに偽装されており、それを開封したことでパソコンにウイルスを感染させてしまいました。

また、感染パソコンではセキュリティソフトを最新の状態で使用していましたが、感染当時（2014 年 3 月頃）W32/Burnwoo は出現したばかりだったため [(*3)]、セキュリティソフトで検出されませんでした。

セキュリティソフトであってもウイルス検出用の定義ファイル（パターンファイル）が新種のウイルスに対応していないと検出できません。本事例は定義ファイルのアップデートよりもウイルスの侵入が早かったために感染してしまった事例です。

W32/Burnwoo に感染したパソコンは、不審なウェブサイトへのアクセスを試みて、アクセスが成功すればさらに他のウイルスや不正プログラムを、パソコン利用者に気づかれないようにダウンロードします。しかし本届出では、接続先ウェブサイトが既に何らかの理由で接続不可になっていたため、更なるウイルスの感染被害には遭わずに済みました。

外部記憶媒体を経由したパソコンのウイルス感染には、“接続しただけで”感染する場合と、“接続後、パソコン利用者が外部記憶媒体内のファイルを実行して”感染する場合があります。前者は

・自動実行（オートラン）無効化

・パソコン内の脆弱性の解消

によってほとんど防止できますが、後者はいくらパソコン上で対策をしていても、パソコン利用者が自身で実行してしまうことでウイルスに感染してしまう恐れがあります。

(*3) トレンドマイクロ:
http://about-threats.trendmicro.com/malware.aspx?language=jp&name=WORM_BURNWOO.A
SOPHOS:
http://www.sophos.com/ja-jp/threat-center/threat-analyses/viruses-and-spyware/W32~Burnwoo-A.aspx
マイクロソフト:
http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Worm:Win32/Burnwoo.A#tab=2

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 2 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 2014 年第 1 四半期から約 29%（2014 年第 2 四半期：8,354 件、2014 年第 1 四半期：6,452 件）増加しました。反対に W32/Mydoom [(*5)] の検出数は、2014 年第 1 四半期から約 45%（2014 年第 2 四半期：6,203 件、2014 年第 1 四半期：14,691 件）の減少となりました。（図 1-2 参照）。

一方最も多く検出された不正プログラムは、インターネットバンキングのログイン情報を窃取する Bancos でした。しかしその検出数は 2014 年第 1 四半期から約 6 割も減少（2014 年第 2 四半期：16,086 件、2014 年第 1 四半期：41,113 件）しました（図 1-3 参照）。

これは前四半期の検出数が突出して多かったためで、依然多くが検出されています。

1-3. 届出件数

2014 年第 2 四半期（4 月～6 月）の届出件数は 1,292 件でした。そのうち被害があったものは 1 件でした。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 1 四半期の 1,414 件から 122 件の減少となりました。

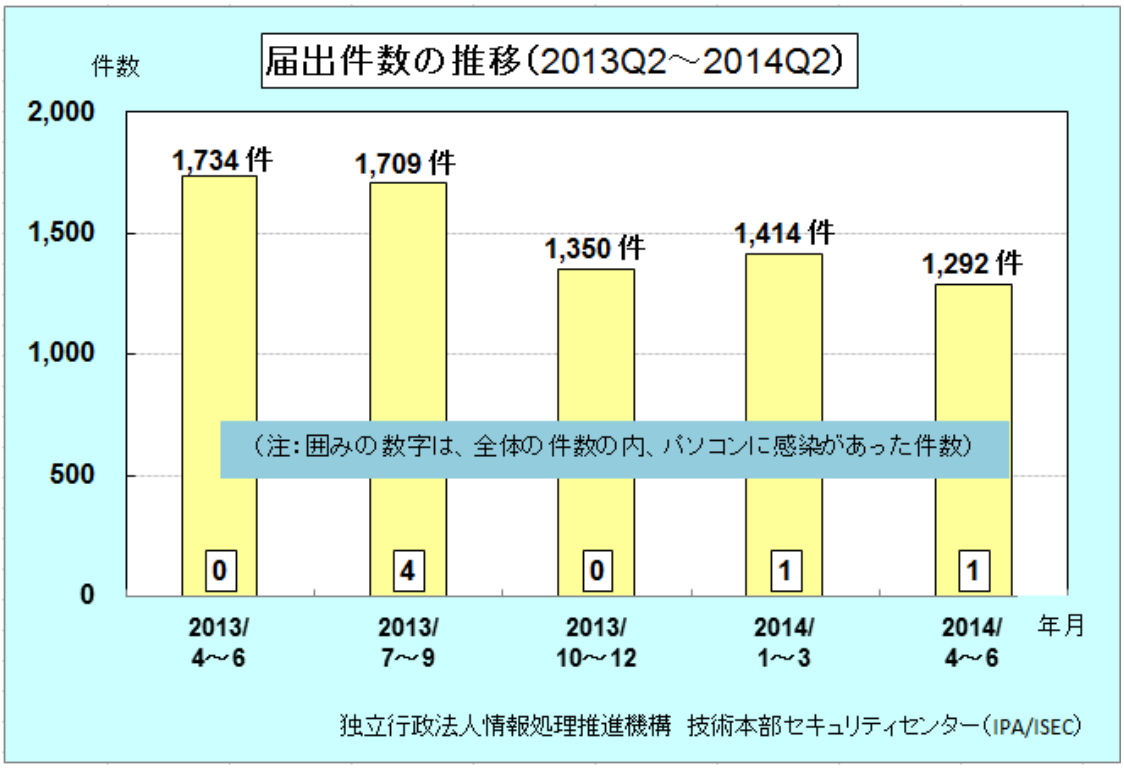


図 1-1. 届出件数の四半期別推移

(*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、いわゆるマスメール型ウイルス。

(*5) W32/Mydoom: W32/Netsky と同様、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。

1-4. ウイルス検出数

2014 年第 2 四半期のウイルス検出数は 17,474 個と、2014 年第 1 四半期の 26,086 個から 8,612 個（約 33%）の減少となりました（図 1-2 参照）。

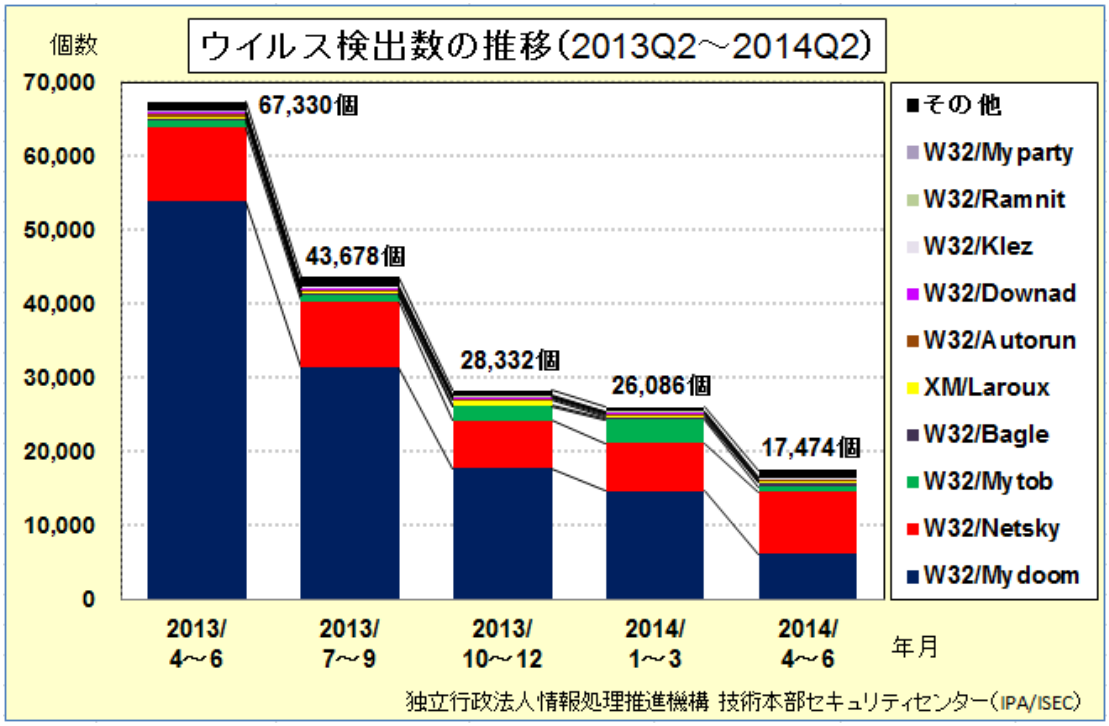


図 1-2. ウイルス検出数の推移

1-5. 不正プログラム検出数

2014 年第 2 四半期の不正プログラム上位 10 個の検出数は 41,021 個と、2014 年第 1 四半期の 73,112 個から、32,091 個（約 44%）の減少となりました（図 1-3 参照）。

Bancos の検出が 25,027 個減少したことが主因です。

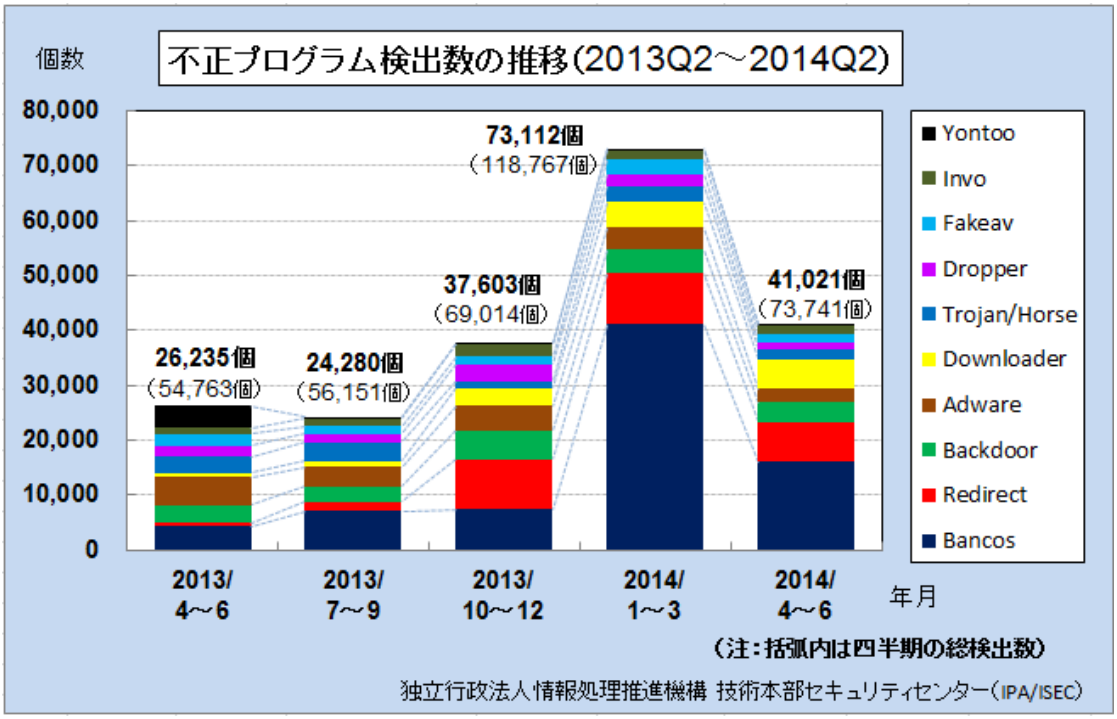


図 1-3. 不正プログラム検出数の推移

1-6. 2014 年第 2 四半期の検出ウイルス

ウイルスの種類は 74 種類、検出数は、Windows/DOS ウイルス 17,275 個 (*6)、スクリプトウイルス及びマクロウイルス 192 個、携帯端末ウイルス 7 個でした。

表 1-2. 2014 年第 2 四半期の検出ウイルス　　(※) 印は 2014 年第 2 四半期の新規届出ウイルス

i) Windows/DOS ウイルス	検出数
W32/Netsky	8,354
W32/Mydoom	6,203
W32/Mytob	752
W32/Bagle	513
W32/Autorun	218
W32/Rontokbro	210
W32/Klez	178
W32/Ramnit	115
W32/Downad	89
W32/Sality	81
W32/Magistr	71
W32/Traxg	49
W32/Virut	40
W32/Dorkbot	38
W32/Koobface	32
W32/Prettypark	32
W32/Sircam	26
W32/Sobig	24
W32/Badtrans	23
W32/Fakerecy	23
W32/Parite	20
W32/Gammima	15
W32/Chir	14
W32/Gibe	12
W32/Palevo	11
W32/Mumu	10
W32/Antinny	9
W32/Inor	8
W32/Nimda	8
W32/Fbound	6
W32/Frethem	6
W32/Fujacks	6
W32/Myparty	6
W32/Winevar	6
W32/Almanahe	5
W32/Lovgate	5
W32/Mywife	5
W32/Bacterra	4
W32/Changeup	4
W32/Hybris	4
W32/IRCbot	4

i) Windows/DOS ウイルス	検出数
W32/Sober	4
Wscript/Fortnight	4
W32/Bugbear	3
W32/Dotex	3
W32/Oror	3
W32/Imaut	2
W32/Mabezat	2
W32/Wapomi	2
W32/Zoher	2
Anti-CMOS	1
W32/Burnwoo (※)	1
W32/Manzon (※)	1
W32/Mota	1
W32/Nuwar	1
W32/Piggi	1
W32/Remadm	1
W32/Sohanad	1
W32/Spyrat	1
W32/Stration	1
Wscript/Kakworm	1
小計　(49 種類)	17,275

スクリプトウイルス	検出数
VBS/Freelink	59
VBS/LOVELETTER	11
VBS/Solow	3
VBS/SST	2
小計　(4 種類)	75

マクロウイルス	検出数
XM/Laroux	77
XM/Mailcab	17
WM/Cap	15
W97M/Melissa	5
W97M/Locale	2
W97M/Marker	1
小計　(6 種類)	117

(*6) 件数には亜種の届出を含む。

ii)携帯端末ウイルス	検出数
AndroidOS/Adware	4
AndroidOS/Fakeinst	2
AndroidOS/Boxer（※）	1
小計　(3 種類)	7

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	Windows32 ビット環境下で動作
XM	Microsoft Excel95、97（ExcelMacro の略）
WM	Microsoft Word95、97（WordMacro の略）
W97M	Microsoft Word97（Word97Macro の略）
X97M	Microsoft Excel97（Excel97Macro の略）
VBS	VisualBasicScript で記述
Wscript	WindowsScriptingHost 環境下で動作（VBS を除く）
AndroidOS	AndroidOS 環境下で動作
SymbOS	SymbianOS 環境下で動作
XF	Microsoft Excel95、97 で動作するウイルス。（ExcelFormula の略）

1-7. 2014 年第 2 四半期に IPA に初めて届出のあったウイルスの概要

（1）AndroidOS/Boxer（ボクサー）　届出時期：2014 年 4 月

モバイル端末用の Android OS を感染対象としたウイルスです。例えば本ウイルスが添付されたメールを Android OS の端末で受信し、その添付ファイルを開封すると感染します。

感染すると、事前にウイルス内に設定された番号に SMS でショートメッセージの送信を試みます。この場合、その番号はプレミアム SMS (*7) と呼ばれるサービスの番号になっており、端末所有者はそれとは知らずに、SMS の送信先に「送金」してしまうことになります。

（2）W32/Manzon（マンゾン）　届出時期：2014 年 4 月

このウイルスは、COM (*8)、EXE ファイルに寄生して感染を広げる、常駐型です。

また、セキュリティソフトからの検出を回避するために、ウイルスプログラムコードを二重に暗

(*7) 主に海外で利用されているショートメッセージサービス。SMS の送信により送信先に送金できるサービス。
(*8) 実行ファイルの 1 種。実行ファイルには他に BIN ファイル、BAT ファイルなどがあり、“パソコン利用者がダブルクリックすると、プログラムとして記述された内容が実行される”という共通点を持つ。

号化しています（ポリモルフィック暗号型）。

（3）W32/Burnwoo（バーンウー）　届出時期：2014 年 6 月

このウイルスは、USB メモリ等の外部記憶媒体を介して感染を広げます。その感染には、次の 2 つの場合があります。

・パソコンの自動実行機能によって、外部記憶媒体内のウイルスがパソコン内にコピーされる。
・パソコン利用者が外部記憶媒体内の偽装ファイルをダブルクリックすることで、ウイルスがパソコン内にコピーされる。

また、感染すると“〇〇〇.exe”（〇〇〇は不規則な英数字の羅列）というファイルが生成され、パソコンを起動するたびにこのファイルが実行されるように環境が設定されます。また、不正なウェブサイトにアクセスをして、他のウイルスや不正プログラムをダウンロードしようとします。

1-8. ウイルス届出者構成及び感染経路

2014 年第 2 四半期の届出者属性は、過去の傾向と同じく、ほとんどを一般法人が占めています。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 1-3. ウイルス届出者別件数

	2013/ 4～6	2013/ 7～9	2013/ 10～12	2014/ 1～3	2014/ 4～6
一般法人	1,656	1,675	1,308	1,404	1,269
	(95.5%)	(98.0%)	(96.9%)	(99.3%)	(98.2%)
個人	0	0	0	0	0
	(0.0%)	(0.0%)	(0.0%)	(0.0%)	(0.0%)
教育機関	78	34	42	10	23
	(4.5%)	(2.0%)	(3.1%)	(0.7%)	(1.8%)
合計	1,734	1,709	1,350	1,414	1,292

表 1-4. 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/ 4～6	2013/ 7～9	2013/ 10～12	2014/ 1～3	2014/ 4～6
メール	67,118	42,952	28,098	25,927	17,396
	(57.0%)	(43.0%)	(28.9%)	(17.9%)	(19.1%)
ダウンロード ファイル	46,629	44,409	51,787	90,861	59,201
	(39.6%)	(44.5%)	(53.2%)	(62.7%)	(64.9%)
外部記憶 媒体	4	6	65	1	41
	(0.003%)	(0.006%)	(0.067%)	(0.001%)	(0.045%)
ネット ワーク	279	667	249	250	125
	(0.2%)	(0.7%)	(0.3%)	(0.2%)	(0.1%)
不明・その他	3,800	11,795	17,147	27,814	14,452
	(3.2%)	(11.82%)	(17.6%)	(19.2%)	(15.8%)
合計	117,830	99,829	97,346	144,853	91,215

・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 2 四半期（2014 年 4 月～6 月）のコンピュータ不正アクセス届出の総数は 37 件（2014 年 1 月～3 月 : 28 件）でした（図 2-1）。そのうち『なりすまし』の届出が 12 件（同 : 10 件）、『DoS』の届出が 6 件（同 : 7 件）、『不正プログラム埋め込み』の届出が 5 件（同 : 2 件）などでした（表 2-1）。

前四半期では DoS の届出に、NTP の脆弱性を悪用したものが複数ありましたが、**本四半期では chargen (*9) サービスを悪用した DoS 攻撃の届出が 2 件ありました。**いずれも chargen サービスが外部から接続され、他組織への踏み台として悪用されてしまったものでした。

chargen サービスは外部から不正に接続されると、サーバーの CPU やメモリを消費し、サーバー機能が低下します。更に、“IP スプーフィング (*10) によって送信元 IP アドレスを偽装” した上で、“特定のサーバーに大量のパケットを送りつけ”、その結果“受信サーバーは偽装された IP アドレスに大量のパケットを返信” してしまう、いわゆる「リフレクター攻撃」(*11) の踏み台として悪用されてしまいます。

chargen サービスの主な用途は通信試験や通信用プログラムの動作確認であるため、通常、運用中のシステム上で chargen サービスを有効にする必要はありません。前述の 2 件の届出の原因は、chargen サービスが有効な状態のままとなっていたこと、通信フィルターの設定不備によるものでした。リフレクター攻撃の踏み台にならないために、“不要なサービスは無効にする”、“不特定多数への公開が不要なサービスについてはアクセスを制限する”などの適切な設定が必要です。

また、本四半期は OpenSSL や Apache Struts2 などサーバー用プログラム等の脆弱性公表が目立ちました。IPA にも、**OpenSSL の脆弱性を狙った通信（被害なし）の届出が 4 件寄せられました。**

前四半期と同様、引き続き**『なりすまし』の届出件数が多い状況が続いています**（表 2-1 参照）。その内訳は、『オンラインショッピング』が 4 件、『ウェブメール』が 4 件、『自組織が運用するメール』が 3 件、『動画サイト』が 1 件でした。

そのうち、『動画サイト』のなりすましは初めて届出されたものです。その内容は、登録したパスワードで動画サイトにログインができないというものでした。届出当時、当該サイトは不正アクセスを受け、ID・パスワードの漏えい被害が発生したとの報道がありました。このことから、第三者が ID・パスワードを不正に入手し、本人になりすましてログインし、パスワードを変更したと考えられます。

(*9) chargen： 接続すると任意の文字を送信する、試験やデバッグを目的としたプロトコル。

(*10) IP スプーフィング： 任意の IP アドレスを送信元として設定することで、実際の送信元とは異なる IP アドレスに詐称して身元を詐称する手法。

(*11) リフレクター攻撃： UDP を利用するプロトコルを悪用する各種リフレクター攻撃に対する注意喚起について（警察庁） http://www.npa.go.jp/cyberpolice/detect/pdf/20140711.pdf

2-2. 被害事例

（i）不正ログインにより身に覚えのない購入手続きが行われていた

被害の概要	・普段利用しているショッピングサイトから突然、身に覚えのない決済連絡メールが届いた。 ・初めはスパムメールかと思ったが、記載されたクレジットカード番号の一部が一致していたため、ショッピングサイトにログインして履歴を確認した。 ・確認の結果、見覚えのないアプリが勝手に購入され、決済が完了していることが判明した。またログイン履歴を確認すると、自分のものではない IP アドレスから複数回のアクセスがあったことも判明した。 ・すぐに購入のキャンセル手続きを行い、パスワードも変更した。
解説・対策	知らない間に第三者にショッピングサイトにログインされ、購入手続きが行われてしまった事例です。幸い、決済連絡メールによりすぐに異変に気付き、適切な対応ができたことで、金銭的被害には遭わずに済みました。 アクセスの履歴情報からも、第三者によるアクセスは確認できましたが、ログイン成功の手口は判明していません。**パスワード管理の基本として、“強固なパスワードにする”、“他のサイトとは異なるパスワードにする（使い回しをしない）”を守ってください。** また、万が一、同様の被害に遭ってしまった場合には、すぐに購入元およびクレジットカード会社へ問い合わせる、パスワードを変更するなど、被害の拡大を防止するための対策を実施してください。

（ii）古いバージョンのプログラムの脆弱性を悪用されて、バックドアを埋め込まれた

被害の概要	・ウェブサーバーのログ内に異常を発見したため、調べたところ、管理者が認識していないプログラムファイルが存在することを確認した。 ・被害状況把握および対策のため、当該ウェブサーバーを即座に停止して調査を開始した。 ・調査の結果、WordPress の脆弱性を悪用してウェブサーバーに不正ログインされ、バックドアが埋め込まれていたことが判明した。
解説・対策	WordPress のバージョンアップ作業を先延ばしし、脆弱性が残ったままになっていたことで、被害に遭ってしまった事例です。 バージョンアップ作業は、サービス停止や他のサービスへの影響などを考慮する余り早急な対応を敬遠しがちです。しかし、**脆弱性対策の遅れは、本来、防げたはずの被害に遭う可能性を高めることを意味します。** サーバー管理者は、自分が管理しているサーバーに**インストールされているソフトウェアのバージョンを把握するとともに、それらのソフトウェアの脆弱性情報を常に収集し、万が一、深刻な脆弱性が発見された場合には、早急に解決策や回避策を講じる必要があります。**

2-3. 届出件数

2014 年第 2 四半期（4 月～6 月）の届出件数は合計 37 件（前四半期から 32%増加）であり、そのうち被害があった件数は 29 件（前四半期から 37%増加）となりました。

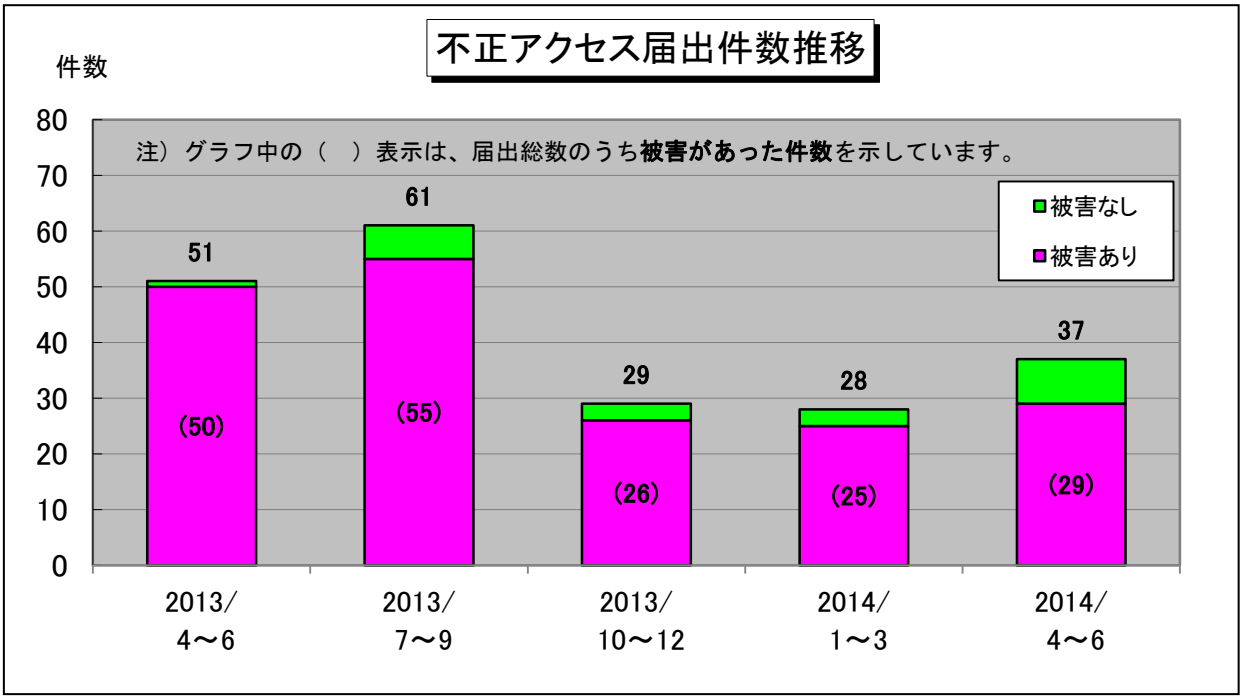


図 2-1. 不正アクセス届出件数の推移

2-4. 届出種別

IPA に届けられた 37 件（前四半期 28 件）のうち、実際に被害があった届出は 29 件（前四半期 25 件）と全体の約 78%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。

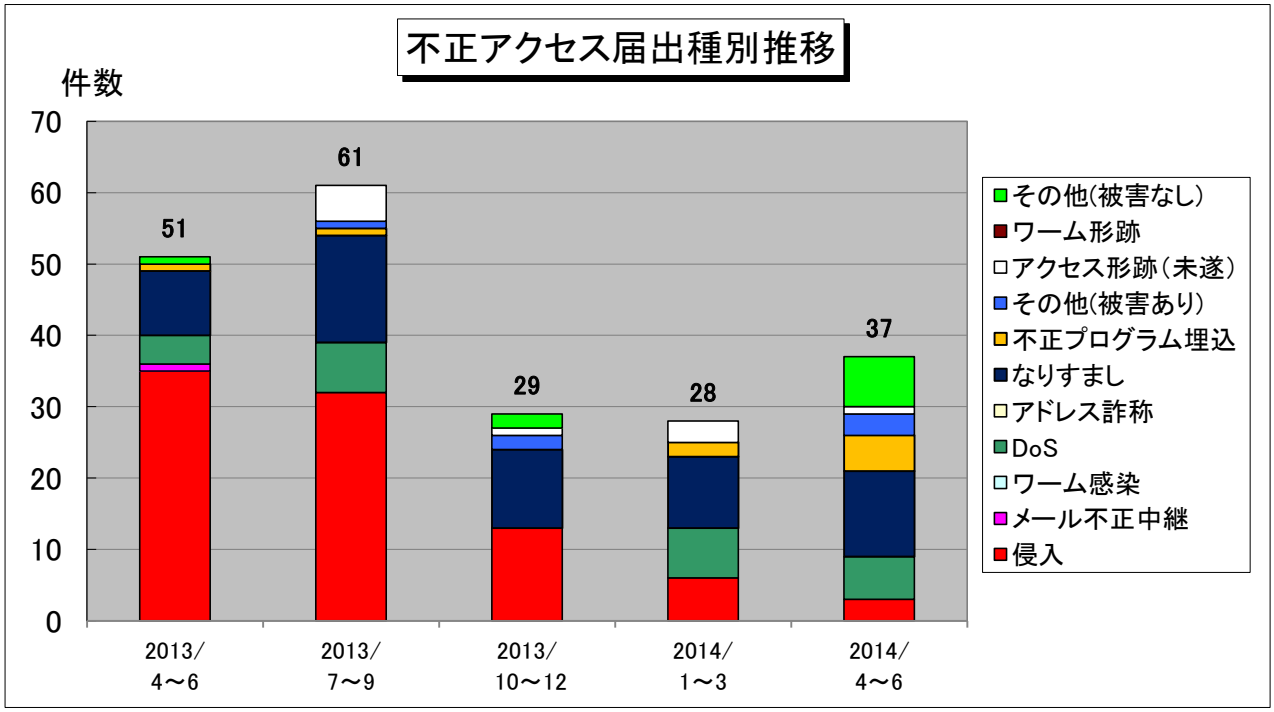


図 2-2. 不正アクセス届出種別の推移

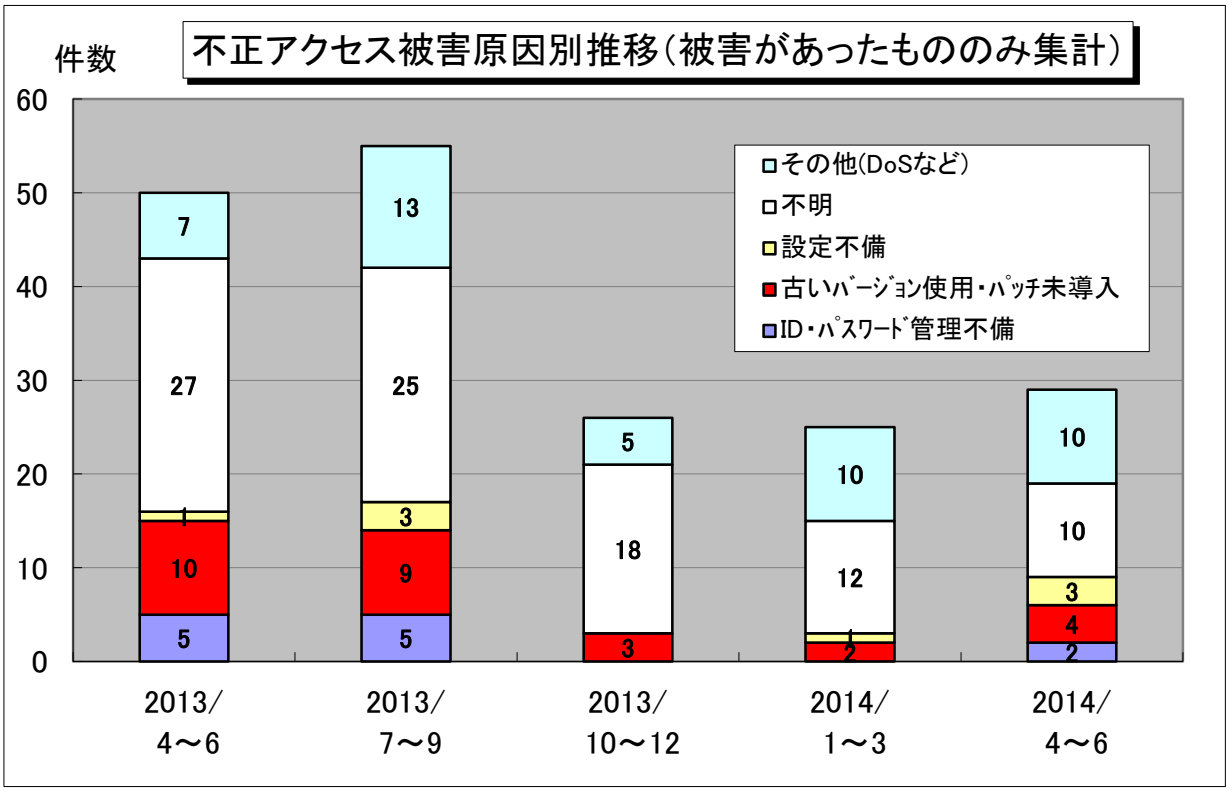
表 2-1. 不正アクセス届出種別の四半期推移

	2013年 第2四半期		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	
侵入	35	68.6%	32	52.5%	13	44.8%	6	21.4%	3	8.1%
メール不正中継	1	2.0%	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	4	7.8%	7	11.5%	0	0.0%	7	25.0%	6	16.2%
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	9	17.6%	15	24.6%	11	37.9%	10	35.7%	12	32.4%
不正プログラム埋込	1	2.0%	1	1.6%	0	0.0%	2	7.1%	5	13.5%
その他（被害あり）	0	0.0%	1	1.6%	2	6.9%	0	0.0%	3	8.1%
アクセス形跡（未遂）	0	0.0%	5	8.2%	1	3.4%	3	10.7%	1	2.7%
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）	1	2.0%	0	0.0%	2	6.9%	0	0.0%	7	18.9%
合　計（件）	**51**		**61**		**29**		**28**		**37**	

注）網掛け部分は、今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（29 件）のうち、原因が判明しているものは**古いバージョン使用・パッチ未導入が 4 件、設定不備が 3 件、 ID・パスワード管理不備が 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。

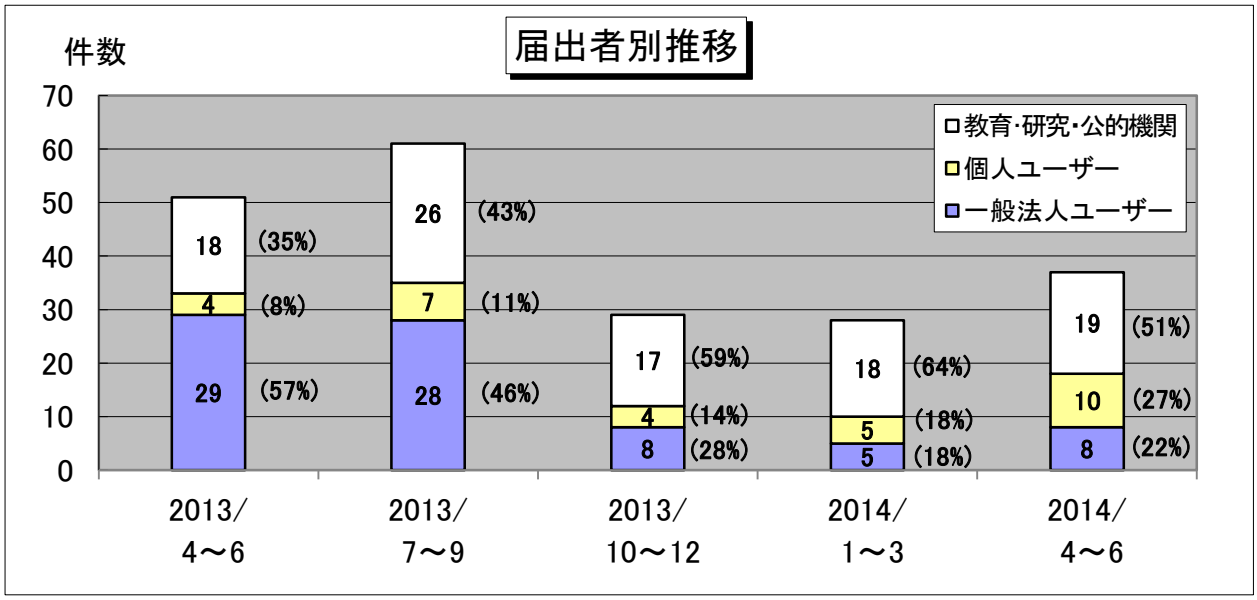


図 2-4. 届出者別推移

・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. 相談受付状況

3-1. 四半期総括

2014 年第 1 四半期（2014 年 4 月～6 月）のウイルス・不正アクセス関連の相談総件数は **4,426 件**でした（2014 年 1 月～3 月：3,585 件）。相談員による対応の中で最も多かったのが**『ワンクリック請求』**に関する相談で **937 件**（同 706 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を入力させる手口』**に関する相談が **182 件**（同 177 件）、**『スマートフォン』**に関する相談が **298 件**（同 217 件）などでした（図 3-3、図 3-4、図 3-5 参照）。

前四半期の相談総件数と比べて、今四半期は 23.5%増となりました（図 3-1 参照）。

『インターネットバンキング』に関する相談は **67 件**と、前四半期の 69 件とほぼ変らず横ばいでした。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 44 件で、前四半期の 49 件から約 10%減少しました（図 3-6 参照）。また、グラフはありませんが身代金型ウイルス**『ランサムウェア』**は今四半期 **14 件**で、前四半期の 13 件とほぼ同等でした。

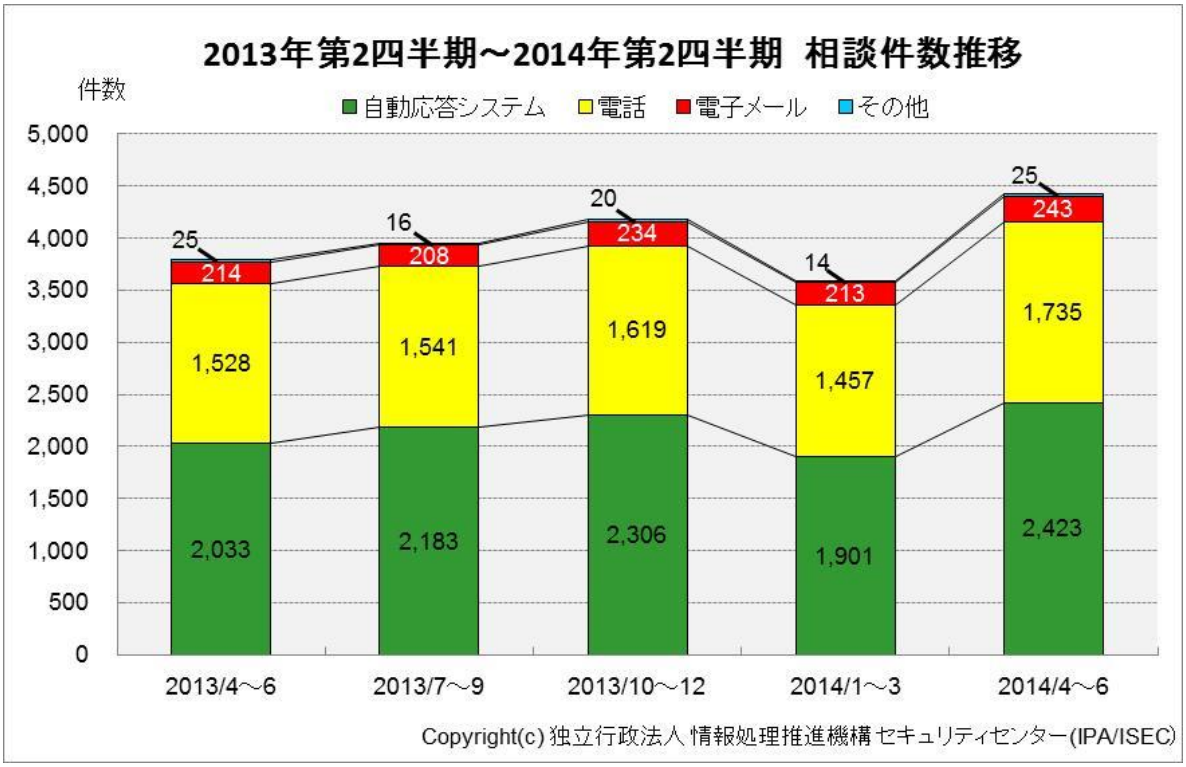


図 3-1. ウイルス・不正アクセス関連の相談件数

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/ 4～6		2013/ 7～9		2013/ 10～12		2014/ 1～3		2014/ 4～6	
合計	3,800		3,948		4,179		3,585		4,426	
自動応答システム	2,033	53.5%	2,183	55.3%	2,306	55.2%	1,901	53.0%	2,423	54.7%
電話	1,528	40.2%	1,541	39.0%	1,619	38.7%	1,457	40.6%	1,735	39.2%
電子メール	214	5.6%	208	5.3%	234	5.6%	213	6.0%	243	5.5%
その他	25	0.7%	16	0.4%	20	0.5%	14	0.4%	25	0.6%

3-2. 相談事例

（i）LINE のアカウントが乗っ取られた。

相談	・LINE のアカウントを第三者に使用されて、見覚えのない内容のメッセージを友人へ次々と送信しているようだ。友人から連絡を受け、気づいた。 ・メッセージ送信を止めたいが、アカウントにログインできないために自分ではどうにもできず、友人へのメッセージの送信を止めることができない。 ・Apple ID と mixi のアカウントも同じ ID とパスワードにしている。
回答	他のサービスのパスワードを使い回していたために、ID・パスワードリスト型攻撃に遭ってしまったと考えられます。 LINE におけるアカウント乗っ取り被害が多発しており、金銭被害に遭ったとの報道もあります。 **被害発生を受けて事業者が 2014 年 7 月 7 日にシステム上での対処を行いました**[(*12)]。しかしパスワードの使い回しを続けていると、他のサービスで乗っ取り被害を受ける可能性があります。**利用しているネットサービスすべてで異なるパスワードを設定することが必要です**。

（ii）yahoo メールアドレスを不正利用にされた。

相談	・銀行になりすました内容のメールが自分の yahoo のメールアドレスから勝手に発信されている。 ・2、3 分間隔で送信され、今まで 100 件以上送信されている。 ・宛先不明のメールに関しては、自分のメールアドレス宛に送信エラーが返ってくる。 ・yahoo メールアドレスのパスワードを変更したら、その後送信されなくなった。 ・他に何か対策はした方がよいですか。
回答	自身のメールアカウントが不正ログインに遭った後、パスワードを変更したことにより、銀行になりすましたメールを勝手に送信される事象は収まりました。これで問題が解決したように思われますが、まだ対策が不足しています。 もしパソコンのウイルス感染が原因でパスワードを窃取されてしまった場合、パスワードを変更しても、パソコン内のウイルスによって変更後のパスワードが再度窃取されて、メールアカウントに再度不正ログインされる恐れがあります。そのためパソコン内のウイルスチェックをする必要があります。 フリーメールのアドレスに不正ログインされて、銀行を騙ったフィッシングメールを自分のアドレス帳の知り合い宛に勝手に送信される被害相談が複数寄せられています。メールアドレスが不正ログインに遭って乗っ取られると、自分が被害を受けるだけでなく、アドレス帳内の知り合いにも被害を及ぼす可能性があります。**自分のパソコンやアカウントが攻撃に悪用されないためにも、パソコンのセキュリティ対策をしっかり行ってください。**

(*12) PC 版 LINE のセキュリティ強化のため「認証番号」の入力が必要になりました
http://official-blog.line.me/ja/archives/1005593400.html

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 937 件寄せられました。前四半期では一旦相談数が落ち着きましたが、今四半期は約 33%（231 件）増加しました。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 236 件で、前四半期の 135 件から約 75%（101 件）増加しました。

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。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！ ～
http://www.ipa.go.jp/security/txt/2014/06outline.html

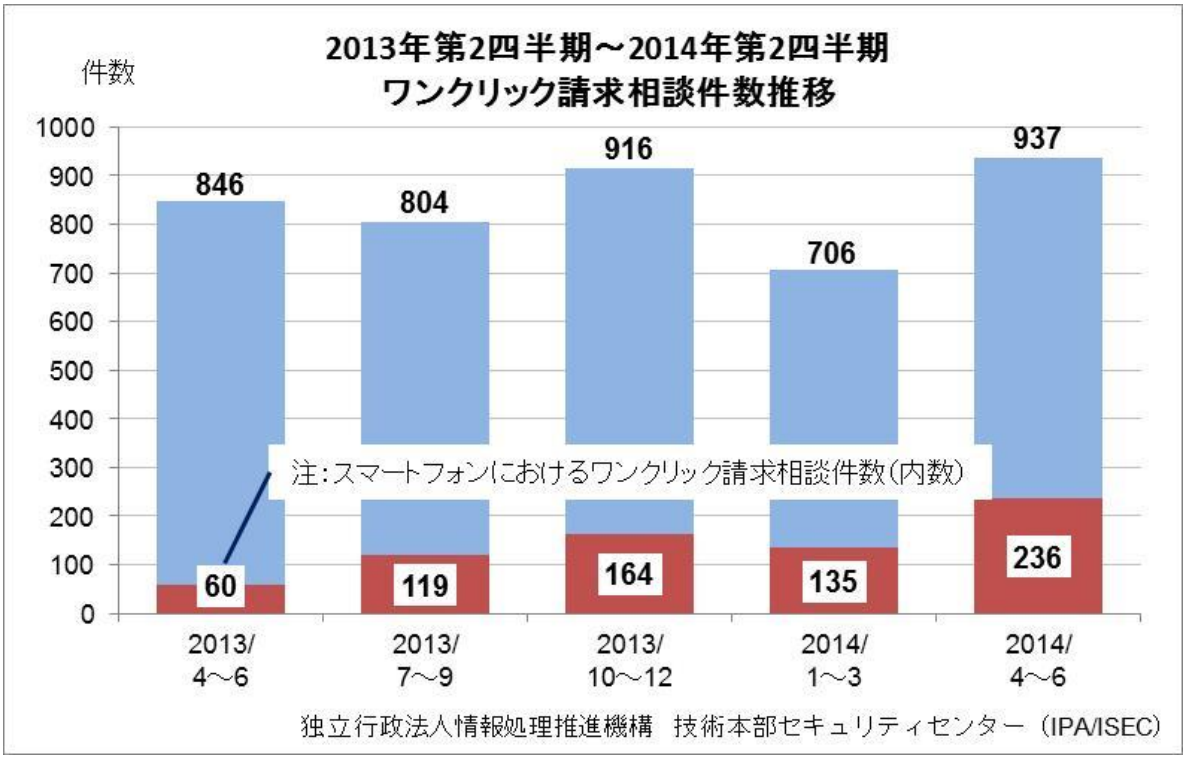


図 3-3.『ワンクリック請求』相談件数推移、および
『スマートフォン』における『ワンクリック請求』相談件数推移

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

今四半期の相談は 182 件寄せられました。前四半期から約 3%（5 件）の微増でした。

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が急減（今四半期 0 件、前四半期 19 件） 金銭窃取の手口に変化が

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”（0 件）、“ランサムウェア”（14 件）、“Bancos”（インターネットバンキングのログイン情報を窃取するウイルス、44 件）等が一般的です。これらウイルスを使った手口の中では“ランサムウェア”や“Bancos”の方が感染パソコン 1 台あたりの窃取金額が、多く見込め[(*13)]ます。そのため偽セキュリティソフト以外の手口に移行しつつあることが伺え、相談件数が急減したと考えられます。

ウイルス感染ではありませんが、ウェブブラウザ上に「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」等と表示される広告があります。中には利用者の不安をあおる意図で赤い点滅で警告メッセージを表示しているものもあります。こうした広告は、クレジットカード番号を入力させるため、利用者に問題解決のためのソフトウェアの購入を促していると考えられます。

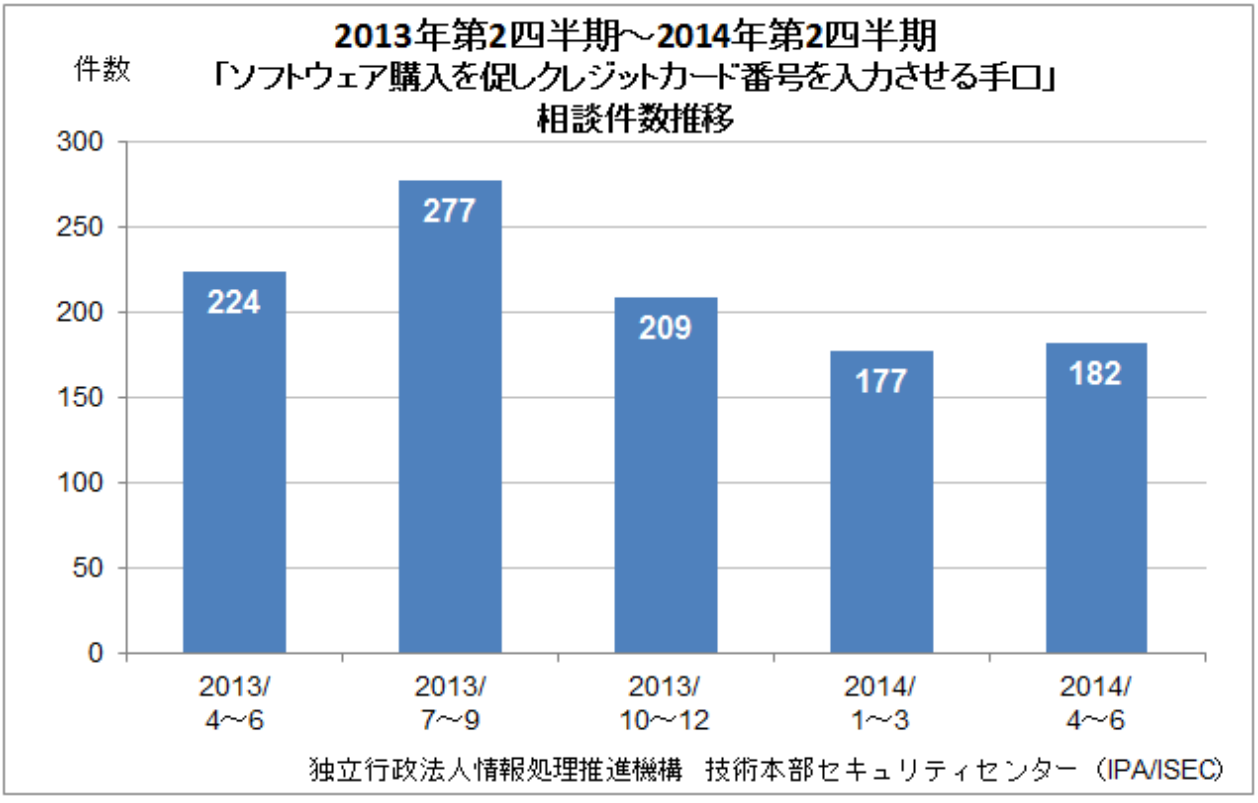


図 3-4.『ソフトウェアの購入を促しクレジットカード番号を入力させる手口』相談件数推移

(*13) “偽セキュリティソフト”で請求されるのは 1 人 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 298 件寄せられました。前四半期からは約 37%（81 件）の増加でした。

『スマートフォン』に関する相談のうち、『ワンクリック請求』以外の件数は 62 件でした。その多くは“ウイルス感染”や“不正アクセス”を疑っただけの相談でした。不安を覚えた場合はまず以下の項目にある、スマートフォンなどの利用における情報セキュリティ対策を実行しているかを確認してください。

・スマートフォンを使用しない時は操作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
・ID とパスワードを使用するウェブサイトの情報が第三者に知られていないか
・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や、実際に不審な画面が表示された場合は、写真や画像のハードコピー等を証拠として残し、当機構の安心相談窓口（03-5978-7509）にご相談下さい。

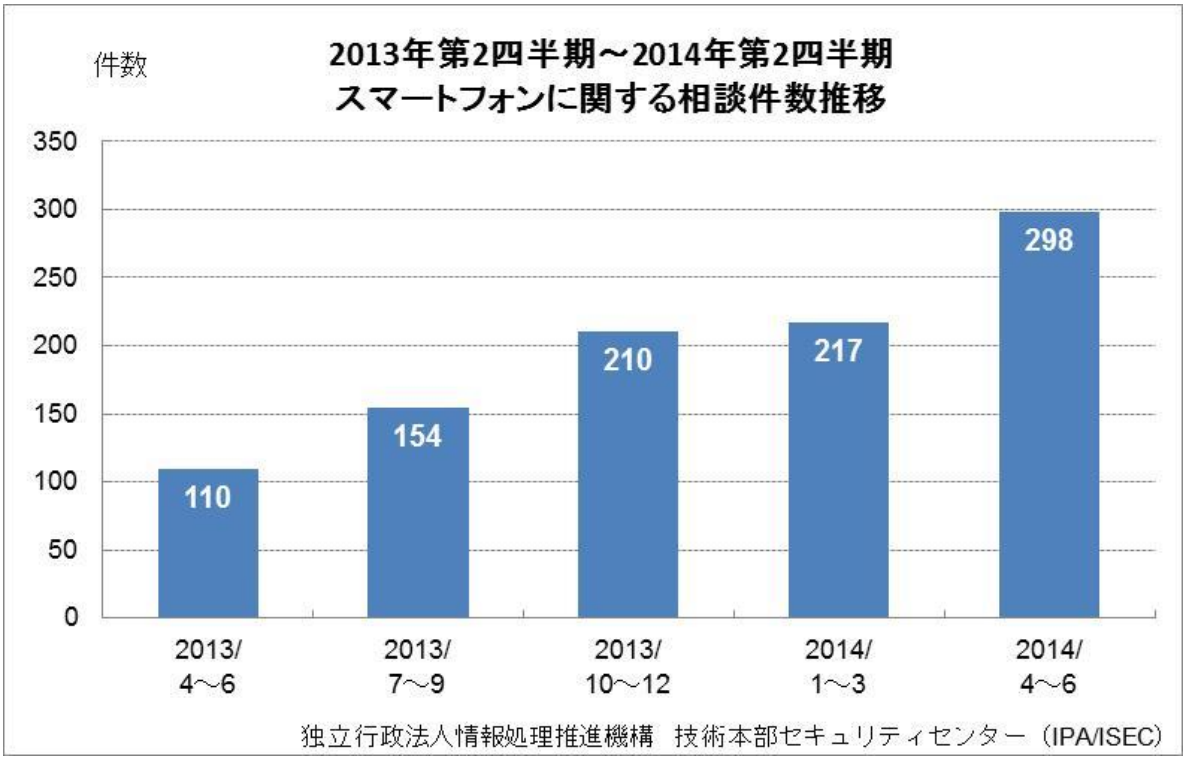


図 3-5.『スマートフォン』に関する相談件数推移

（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 67 件寄せられました。前四半期からは約 3%（2 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 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 11 件、その他が 12 件でした。

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、以下のような偽の画面が表示されます。

（IPA に寄せられた相談事例）

・インターネットバンキングにログイン直後、普段表示されない認証画面が表示された。
・振込みの際にパスワードを入力したらエラーが表示された。
・送金画面の途中で「メンテナンス中」と表示された。

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、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！」
http://www.ipa.go.jp/security/txt/2014/07outline.html

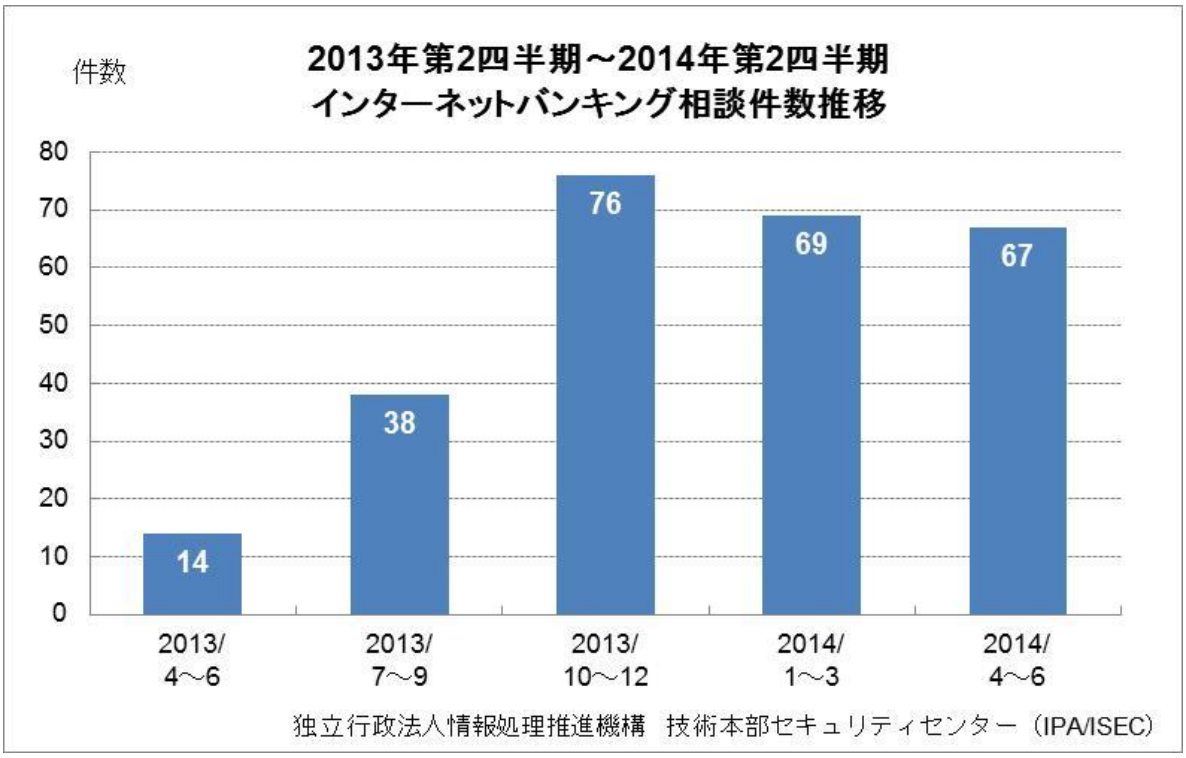


図 3-6.『インターネットバンキング』相談件数推移