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 1 四半期（1 月～3 月)]

本レポートでは、2014 年 1 月 1 日から 2014 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

2014 年 4 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 1 四半期に寄せられたウイルスの検出数 (*1) は、2013 年第 4 四半期 28,332 個より 2,246 個（約 7.9%）少ない 26,086 個でした（図 1-2 参照）。また、2014 年第 1 四半期の不正プログラム (*2) 検出数は 2013 年第 4 四半期 69,014 個から 49,753 個（約 72%）多い 118,767 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、検出数の増加がもっとも顕著だったの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、約 5.5 倍に増加しました（2013 年第 4 四半期 7,378 件、2014 年第 1 四半期 41,113 件）。2013 年は国内のインターネットバンキングを狙った不正送金事件の被害が増加しましたが(*3)、いまだ多くの利用者に感染させるため、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。

ウイルスと不正プログラムの総検出数 144,853 件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 90,861 件で全体の約 63%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 25,927 件、全体の約 18%でした（表 1-4 参照）。これらは 1 件の例外を除いて、感染する前にパソコン上のセキュリティソフトや企業におけるウイルスゲートウェイで駆除されていました。

下記の表 1-1 は、「CryptoLocker」というランサムウェア (*4) の感染被害事例です。

表 1-1. ウイルス感染被害届出詳細

届出元	一般企業
セキュリティソフトの利用	あり
感染経路	不明
被害状況	・パソコンの被害： 赤い警告画面がデスクトップ上に表示され、パソコン内のファイルも暗号化されているため、使用できなくなった。 ・ファイルサーバーの被害： 業務に必要なファイルが暗号化されてしまったため、会社としての業務影響が発生。
発見方法	ファイルサーバー上の共有フォルダのファイルの暗号化と思われる文字化けを正常なパソコンからの接続で発見、その後、感染パソコンを特定した。
感染原因	クライアントパソコンでの Windows Update や Java（JRE）のアップデートの未実施によるものと推察。
対　処	・感染パソコンの対処： 廃棄。 ・ファイルサーバーの対処： 別途バックアップしておいたサーバー内の正常なファイルをサーバーに戻して復旧させた。

(*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) 2014 年 1 月 30 日付　警察庁広報資料 「平成 25 年中のインターネットバンキングに係る不正送金事犯の発生状況等について」：http://www.npa.go.jp/cyber/pdf/H260131_banking.pdf

(*4) ランサムウェア： パソコン内のデータを暗号化し、ファイル等の利用を不可能にし、その暗号化したファイルの暗号解除を名目に身代金を要求するウイルス

CryptoLocker は、感染したパソコンに保存されたファイルを暗号化した後、デスクトップに赤い警告画面を表示し、暗号化されたファイルの暗号化解除を名目に身代金を要求するウイルスです。このCryptoLocker は本来パソコン内のファイルを暗号化するウイルスですが、本事例ではパソコンが接続するファイルサーバー上のファイルまでもが暗号化されてしまった例です。

本事例では当初、ファイルサーバー上の共有フォルダ内のファイルにおいて異常があることが確認されました。その後ウイルス感染の疑いを持った担当者が、当該ファイルサーバーに接続するパソコンを順次確認する中で CryptoLocker に感染したパソコンを 1 台発見しました。この CryptoLocker に感染したパソコンは、デスクトップに特徴的な赤い警告画面が出ているので容易に識別できます。

本事例では、感染したパソコンは Windows の「ネットワークドライブの割り当て」機能を利用して、ファイルサーバー上の共有フォルダを、C ドライブや D ドライブなどと同様にパソコン上のドライブの一つとして扱える設定をしていました。このため実際にはファイルサーバー上のデータであってもパソコン内のデータと論理的に同様の扱いとなります。その結果、CryptoLocker にとっては、パソコン上のファイルのみならず、ファイルサーバー上の共有フォルダ内のファイルも暗号化されてしまい、被害が拡大してしまいました。

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 1 四半期、最も多く検出されたウイルスは、W32/Mydoom [(*5)] でした。検出数は 2013 年第 4 四半期から約 17%（2014 年第 1 四半期：14,691 件、2013 年第 4 四半期：17,701 件）減少しており、2013 年第 2 四半期をピークに減少傾向にあります。（図 1-2 参照）。

一方、最も多く検出された不正プログラムは Bancos でした。検出数は 2013 年第 4 四半期から約 5.5 倍に増加（2014 年第 1 四半期：41,113 件、2013 年第 4 四半期：7,378 件）しました（図 1-3 参照）。

1-3. 届出件数

2014 年第 1 四半期（1 月～3 月）届出件数は 1,414 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、IPA が受け付けた四半期（3 ヶ月）ごとの届出件数の推移を示したものです。届出件数は 2013 年第 4 四半期の 1,350 件から 64 件の増加となりました。

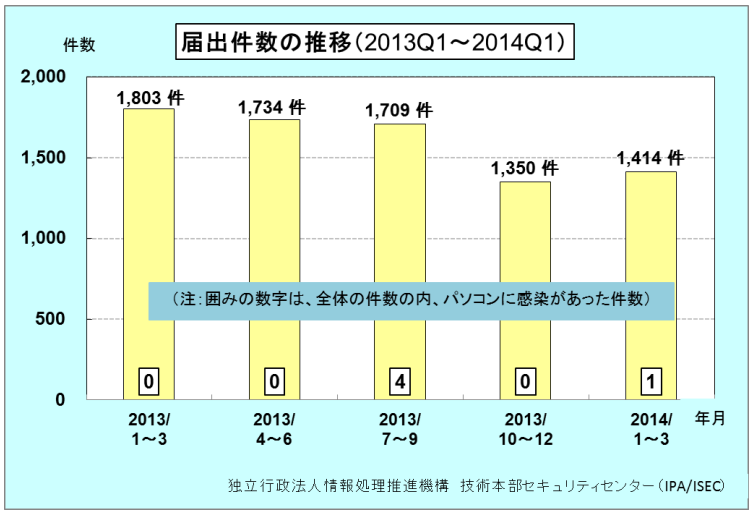


図 1-1. 届出件数の四半期別推移

(*5) W32/Mydoom： 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。

1-4. ウイルス検出数

2014 年第 1 四半期のウイルス検出数は 26,086 個と、2013 年第 4 四半期の 28,332 個から 2,246 個の減少となりました（図 1-2 参照）。

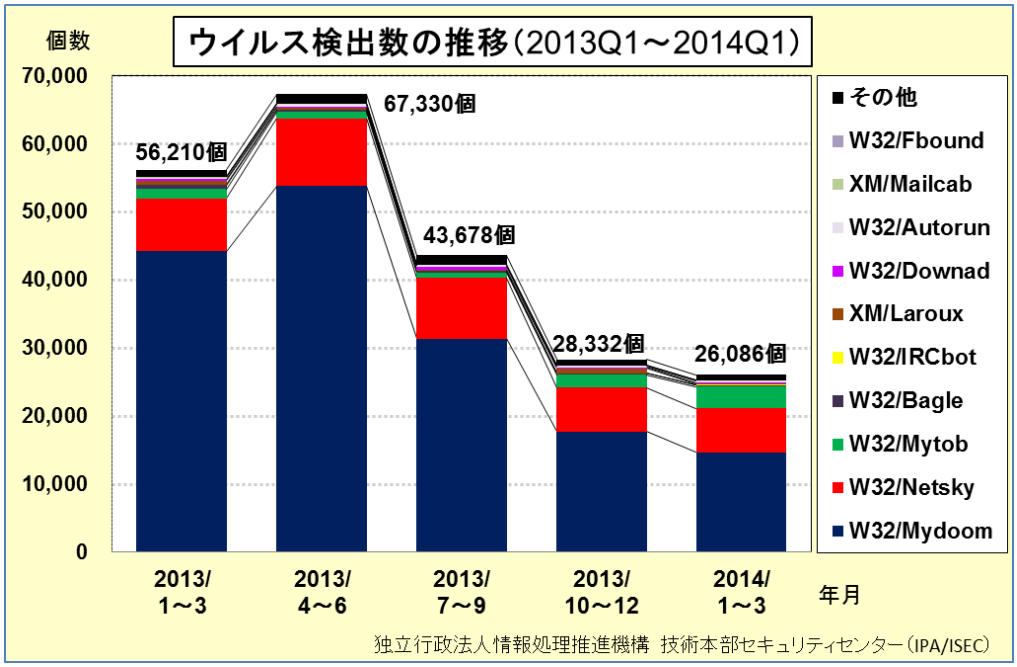


図 1-2. ウイルス検出数の推移

1-5. 不正プログラム検出数

2014 年第 1 四半期の不正プログラム上位 10 個の検出数は 63,872 個と、2013 年第 4 四半期の 28,616 個から、35,256 個の増加となりました（図 1-3 参照）。

Bancos が 33,735 個増加しており、不正プログラム検出数増加の主因です。

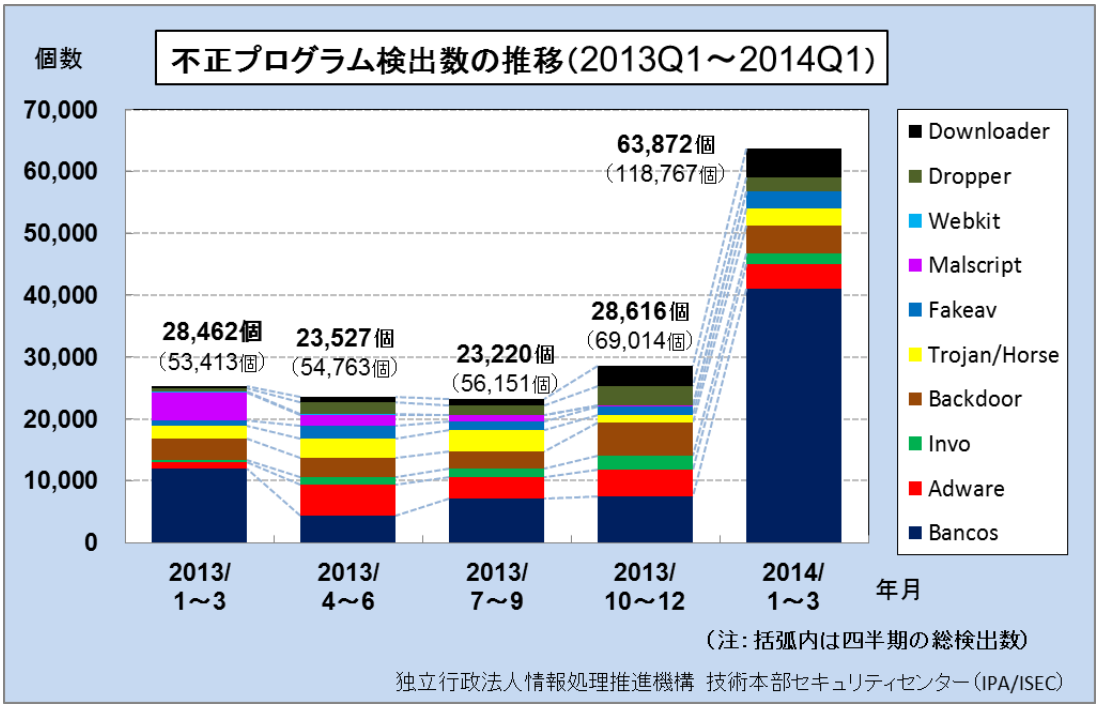


図 1-3. 不正プログラム検出数の推移

1-6. 2014 年第 1 四半期の検出ウイルス

ウイルスの種類は 63 種類、検出数は、Windows/DOS ウイルス 25,821 個 (*6)、スクリプトウイルス及びマクロウイルス 260 個、携帯端末ウイルス 5 個でした。

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

i) Windows/DOS ウイルス	検出数
W32/Mydoom	14,691
W32/Netsky	6,452
W32/Mytob	3,216
W32/Autorun	318
W32/Bagle	238
W32/Ramnit	204
W32/Downad	144
W32/Koobface	57
W32/Stration	43
W32/Chir	41
W32/Gaobot	41
W32/IRCbot	35
W32/Klez	32
W32/Gammima	27
W32/Myparty	27
W32/Fakerecy	26
W32/Rontokbro	24
W32/Sobig	24
W32/Traxg	19
W32/Badtrans	18
W32/Mumu	17
W32/Virut	15
W32/Antinny	13
W32/Nimda	13
W32/Parite	12
W32/Bacterra	9
W32/Almanahe	8
W32/Sober	6
Diskkiller	5
W32/Magistr	5
W32/Harakit	4
W32/Looked	4
W32/Morto	4
W32/Allaple	3
W32/Fujacks	3
W32/Palevo	3
W32/Swen	3
W32/Bugbear	2
W32/Mabezat	2
W32/Sality	2
W32/Sircam	2

i) Windows/DOS ウイルス	検出数
W32/Whybo	2
Stoned	1
W32/Cryptolocker(※)	1
W32/Dorkbot	1
W32/Dotex	1
W32/Funlove	1
W32/Imaut	1
W32/Wukill	1
小計　(49 種類)	25,821

スクリプトウイルス	検出数
VBS/DUNIHI(※)	2
VBS/Solow	2
VBS/Freelink	1
VBS/LOVELETTER	1
小計　(4 種類)	6

マクロウイルス	検出数
XM/Laroux	144
XM/Mailcab	82
WM/Cap	14
WM/Wazzu	6
W97M/Relax	3
W97M/Marker	3
W97M/X97M/Toraja	1
XF/Helpopy	1
小計　(8 種類)	254

ii)携帯端末ウイルス	検出数
SymbOS.Kiazha(※)	3
AndroidOS/Lotoor	2
小計　(2 種類)	5

iii) Macintosh	検出数
なし	

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

(*6) 件数には亜種の届出を含む。

（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 1 四半期に IPA に初めて届出のあったウイルスの概要

（1）W32/Cryptolocker（クリプトロッカー）　届出時期：2014 年 3 月

このウイルスは、パソコン版身代金型ウイルスで、感染したパソコンのファイルを暗号化し、デスクトップ上に赤い警告画面を表示させ、暗号化したファイルの暗号解除を名目に身代金を要求します。

（2）VBS/DUNIHI（デュニヒ）　届出時期：2014 年 1 月

このウイルスは、主に電子メールの添付ファイルとしてパソコン内に入り込み、その後 USB メモリなどの外部記憶媒体に自身のコピーを作成します。その際、ウイルスは外部記憶媒体内の既存のファイル名を借用し、ウイルス自身がそのファイル名になりすまします。そうするとウイルスに感染する前の外部記憶媒体内の元ファイルはファイル名を横取りされたことになり、自動的に別ファイル名で保存されます。しかし、パソコン利用者が覚えの無いファイル名を怪しむ可能性があります。そこで別ファイル名で保存された元ファイルを USB メモリー内で目に見えないよう隠してしまうこと（隠し属性設定）が特徴です。その結果、パソコン利用者は外部記憶媒体内の既存のファイルをウイルスであることに気がつけず、実行しこのウイルス（VBS/DUNIHI）に感染してしまいます。

また、このウイルスは感染したパソコンから外部のサーバーと通信を行い、パソコン内の情報を窃取したり、別のウイルスや不正プログラムを取り込んだりします。

（3）SymbOS.Kiazha（キアザ）　届出時期：2014 年 3 月

このウイルスは、携帯電話版身代金型ウイルスで、Symbian OS を搭載した携帯電話に感染します。感染すると画面にメッセージを表示させ、暗号化したファイルの暗号解除を名目に人民元で身代金を要求します。

1-8. ウイルス届出者構成及び感染経路

2014 年第 1 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/ 1～3	2013/ 4～6	2013/ 7～9	2013/ 10～12	2014/ 1～3
一般法人	1,769	1,656	1,675	1,308	1,404
	(98.1%)	(95.5%)	(98.0%)	(96.9%)	(99.3%)
個人	0	0	0	0	0
	(0.0%)	(0.0%)	(0.0%)	(0.0%)	(0.0%)
教育機関	34	78	34	42	10
	(1.9%)	(4.5%)	(2.0%)	(3.1%)	(0.7%)
合計	1,803	1,734	1,709	1,350	1,414

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/ 1～3	2013/ 4～6	2013/ 7～9	2013/ 10～12	2014/ 1～3
メール	55,933	67,118	42,952	28,098	25,927
	(51.0%)	(57.0%)	(43.0%)	(28.9%)	(17.9%)
ダウンロード ファイル	41,755	46,629	44,409	51,787	90,861
	(38.0%)	(39.6%)	(44.5%)	(53.2%)	(62.7%)
外部記憶媒体	6	4	6	65	1
	(0.01%)	(0.003%)	(0.01%)	(0.1%)	(0.001%)
ネットワーク	441	279	667	249	250
	(0.4%)	(0.2%)	(0.7%)	(0.3%)	(0.2%)
不明・その他	11,488	3,800	11,795	17,147	27,814
	(10.5%)	(3.2%)	(11.8%)	(17.6%)	(19.2%)
合計	109,623	117,830	99,829	97,346	144,853

・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 1 四半期（2014 年 1 月～3 月）のコンピュータ不正アクセス届出の総数は 28 件（2013 年 10 月～12 月：29 件）でした（図 2-1 参照）。そのうち『なりすまし』の届出が 10 件（同：11 件）、『DoS』の届出が 7 件（同：0 件）、『侵入』の届出が 6 件（同：13 件）などでした（表 2-1 参照）。

本四半期は『DoS』の届出件数の増加が顕著でした。7 件の『DoS』の届出のうち、6 件は NTP (*7) という仕組みに関するもので、不正な通信が発生していました。被害の多くは次の 2 つのケースに大別されます。

・大量の NTP 通信を受けた結果、サービス低下に陥った。

・NTP サービスが DoS 攻撃の踏み台として悪用されてしまった。

後者については、攻撃者の目的はあくまで NTP サービスを DoS 攻撃の踏み台として悪用することでしたが、通信量が急増した結果、踏み台にされたサーバー自身の動作が遅くなるなど DoS 攻撃を受けた場合と同じ状態となっていました。

NTP を悪用した DoS に関する届出が急増した背景として、2014 年 1 月に NTP に関する脆弱性が公開されたことが挙げられます (*8)。当該脆弱性が存在することで、NTP リクエスト (*9) の数十倍のパケット量の NTP レスポンス (*10) を返してしまうため、DoS 攻撃を行う際の攻撃の増幅器として悪用されてしまいました。

また、前四半期と同様に**『なりすまし』の件数が多い**状況が続いています。

具体的な被害内容は、大部分がメールアカウントのなりすましによる大量のスパムメール送信の被害でした。なりすましに遭った実際の原因の大半は不明ですが、原因が特定できたものについては、前四半期から引き続き発生している Active! Mail の管理者を装ったフィッシングメールを用いてフィッシングサイトに誘導し、ID やパスワードの入力を求めるというものでした (*11)。

（参考）

「大学などで使用されている Web メール（Active! Mail）アカウントを狙うフィッシング」
https://www.antiphishing.jp/news/alert/20131212activemail.html

これまでと同様に不正アクセスの原因は不明が大半です（図 2-3 参照）。“現状復帰を優先させるため、あまり詳細な調査は行わず初期化などによる復旧を行った”、“早期にサービスを再開させることを優先した”というコメントが添えられた届出もありましたが、再発防止のためにも、やはり原因を特定した上で復旧及び対策を行うことが重要です。

不正アクセスの手口は様々ですが、被害を防止するための基本的な対策は以下のとおりで、従来から変わりありません。

(*7) NTP（Network Time Protocol）：ネットワーク機器やサーバーなどの機器の時刻をネットワーク経由で同期するためのプロトコル

(*8) 「NTP が DDoS 攻撃の踏み台として使用される問題」
http://jvn.jp/vu/JVNVU96176042/index.html

(*9) NTP リクエスト：NTP サーバーに対して時刻を問い合わせること。またはその問い合わせ内容。

(*10) NTP レスポンス：NTP リクエストに対して応答すること。またはその応答内容。時刻情報などが含まれる。

(*11) トランスウエア社「Active! mail のメールアカウント不正使用にご注意ください！」
http://www.transware.co.jp/news/2014/02/25_1406.html

システム管理者向け対策

- **OS、CMS [*12] などのアップデートを行い、サーバープログラムの脆弱性を解消する**
- **複雑なパスワードにする、アカウントを共有しないなど、アカウント管理を見直す**
- **アクセス元 IP アドレスによる接続制限を行う、不要なサービスは停止するなど、インターネットへは必要最小限のサービスのみを公開する**

パソコン上での対策

- **OS、各種プログラム（Java、Flash Player、Adobe Reader）のアップデートを行う**
- **セキュリティ対策ソフトを、最新の状態にしながら利用する**

[*12] 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。

被害事例

（i）アプライアンス機器上で NTP 用プログラムが動作していることを管理者が把握していなかったため、脆弱性対策が至らず、アプライアンス機器が DoS 攻撃の踏み台に悪用された

被害の概要	・インターネット経由で顧客に提供しているクラウドサービスに動作遅延が発生した。 ・クラウドサービスを提供しているサーバーには異常がなかったが、ネットワークの負荷を確認したところ、ネットワーク機器であるアプライアンス (*13) のトラフィックが急増していることが判明した。 ・トラフィックの詳細を調査したところ、当該アプライアンス機器から大量の NTP パケットが外部へ送信されており、送信パケットと受信パケットの通信量に大きな乖離があったことから、NTP サービスが DoS 攻撃の踏み台に悪用されていることが判明した。
解説・対策	アプライアンス機器に NTP 用プログラムが初めから動作していることを管理者が把握していなかったため、必要な脆弱性対策を行っていなかったことが原因です。その結果 NTP 用プログラムが DoS 攻撃に悪用されてしまった事例です。ネットワーク遅延によって自社サービスに悪影響が発生したのみならず、他組織への DoS 攻撃の踏み台として悪用されていました。 「2.1 四半期総括」で紹介した NTP の脆弱性は、一般的なサーバーだけではなく、今回の事例のようにアプライアンス機器にまで影響が及びます。 本事例のように、攻撃が発生すると自組織への影響のみならず、他組織にも攻撃を仕掛けてしまう場合があります。インターネットに接続している機器についてはサーバー、アプライアンス機器に関わらず動作しているプログラムをすべて把握した上で、必要最小限のプログラムを動作させるようにしてください。

（ii）SQL インジェクションによりデータベースに保存していた情報が流出した

被害の概要	・ネットワーク監視部門から攻撃を検知したとの連絡が入った。 ・アクセスログを確認したところ、自社で運営しているウェブサイトの会員情報を管理しているデータベースへの不正なアクセスが確認された。 ・詳細な調査を行ったところ、SQL インジェクションによりウェブサイトの登録情報として自社で管理していた会員のメールアドレスとパスワードが漏えいしたことが判明した。
解説・対策	SQL インジェクションにより、情報漏えいが発生してしまった事例です。漏えいした情報にパスワードが含まれていましたが、ハッシュ値 (*14) で保存されていたため、データベースから漏えいした情報をそのまま他の攻撃に悪用することは難しいと言えます。 IPA では、安全なウェブサイトの作り方の指南書として以下を公開しています。SQL インジェクションなどの脆弱性の技術的解説と解決策を解説していますので、活用してください。 ・安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/websecurity.html

(*13) アプライアンス：特定の機能に特化した機器のことで、専用のサーバーソフトが初めから組み込まれている。ファイアウォール、ウイルス検知、SSL 通信復号、IPv4・Ipv6 変換、など様々なアプライアンスが存在する。

(*14) ハッシュ値：あるデータから、ハッシュ関数という特定の計算式を用いて得られた数値のこと。逆にハッシュ値から元データを得ることは極めて困難であるため、パスワードのハッシュ値を窃取された場合、パスワードそのものを窃取された場合よりも、悪用される危険性が低い。

2-2. 届出件数

2014 年第 1 四半期（1 月～3 月）の届出件数は合計 28 件（前四半期比 97%）であり、そのうち被害があった件数は 25 件（前四半期比 96%）となりました。

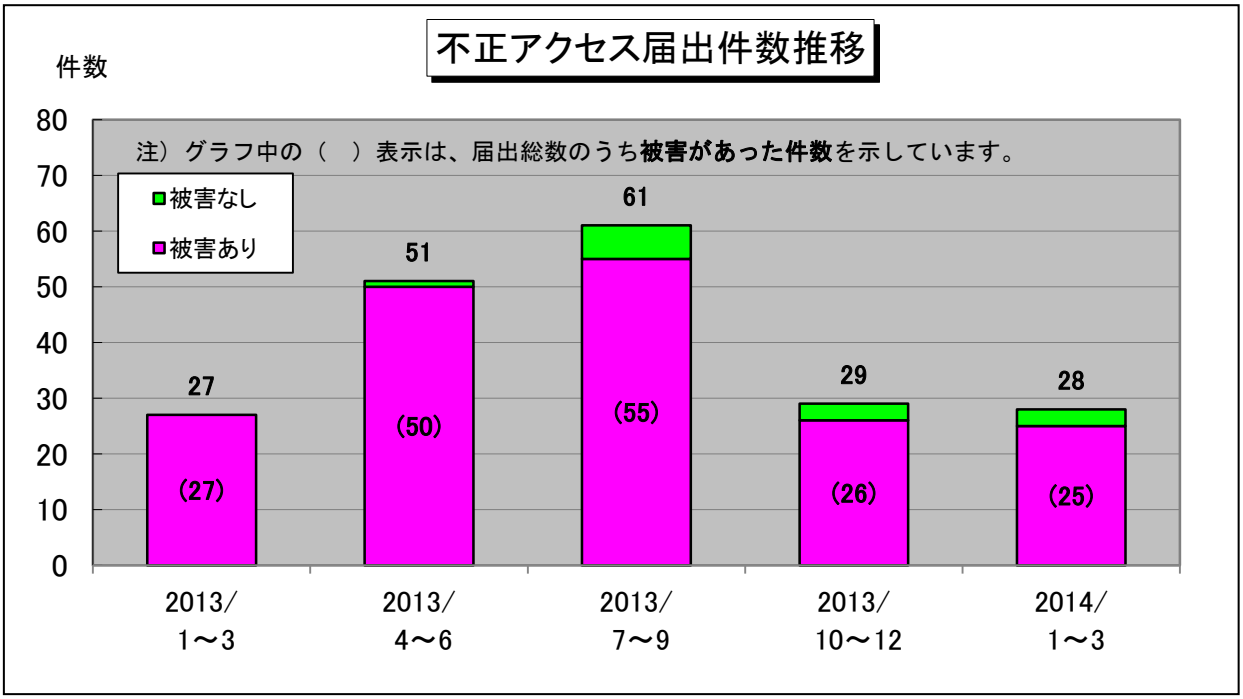


図 2-1. 不正アクセス届出件数の推移

2-3. 届出種別

IPA に届けられた 28 件（前四半期 29 件）のうち、実際に被害があった届出は 25 件（前四半期 26 件）と全体の約 89%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。

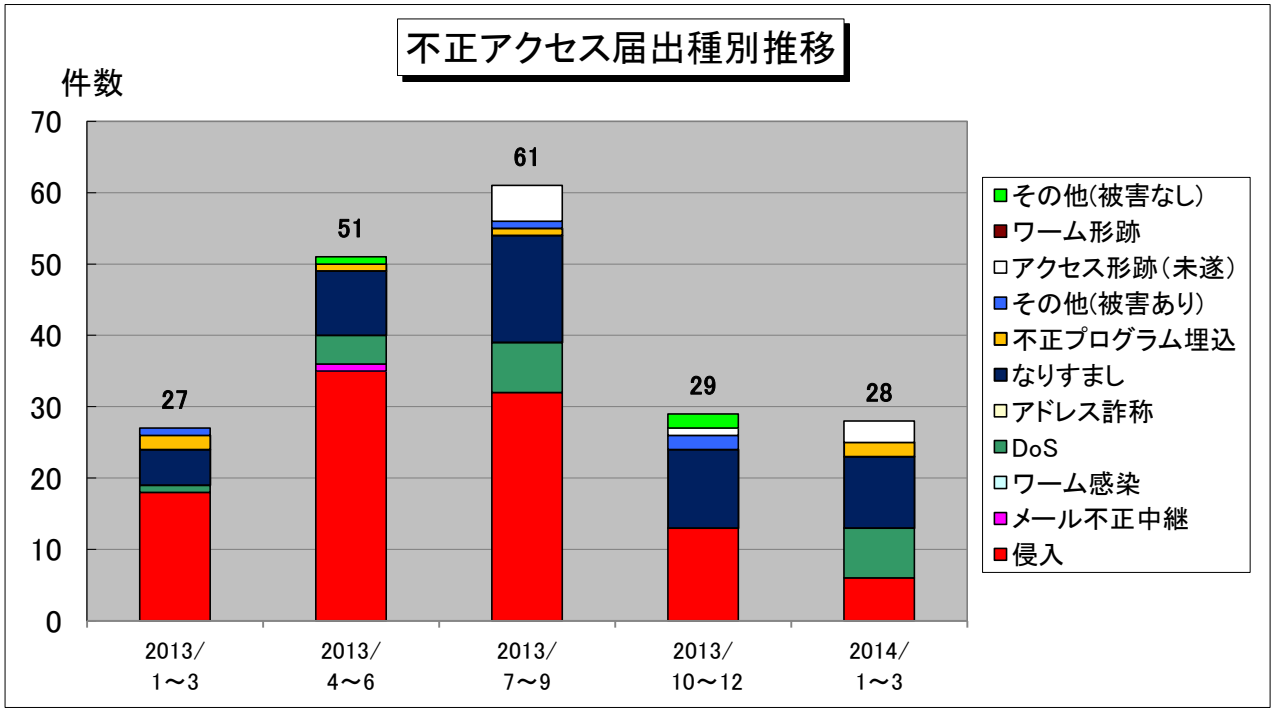


図 2-2. 不正アクセス届出種別の推移

表 2-1. 不正アクセス届出種別の四半期推移

	2013年 第1四半期		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	
侵入	18	66.7%	35	68.6%	32	52.5%	13	44.8%	6	21.4%
メール不正中継	0	0.0%	1	2.0%	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	1	3.7%	4	7.8%	7	11.5%	0	0.0%	7	25.0%
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	5	18.5%	9	17.6%	15	24.6%	11	37.9%	10	35.7%
不正プログラム埋込	2	7.4%	1	2.0%	1	1.6%	0	0.0%	2	7.1%
その他（被害あり）	1	3.7%	0	0.0%	1	1.6%	2	6.9%	0	0.0%
アクセス形跡（未遂）	0	0.0%	0	0.0%	5	8.2%	1	3.4%	3	10.7%
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）	0	0.0%	1	2.0%	0	0.0%	2	6.9%	0	0.0%
合　計（件）	**27**		**51**		**61**		**29**		**28**	

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。

2-4. 被害原因

実際に被害があった届出（25 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 2 件、設定不備が 1 件、**などでした。

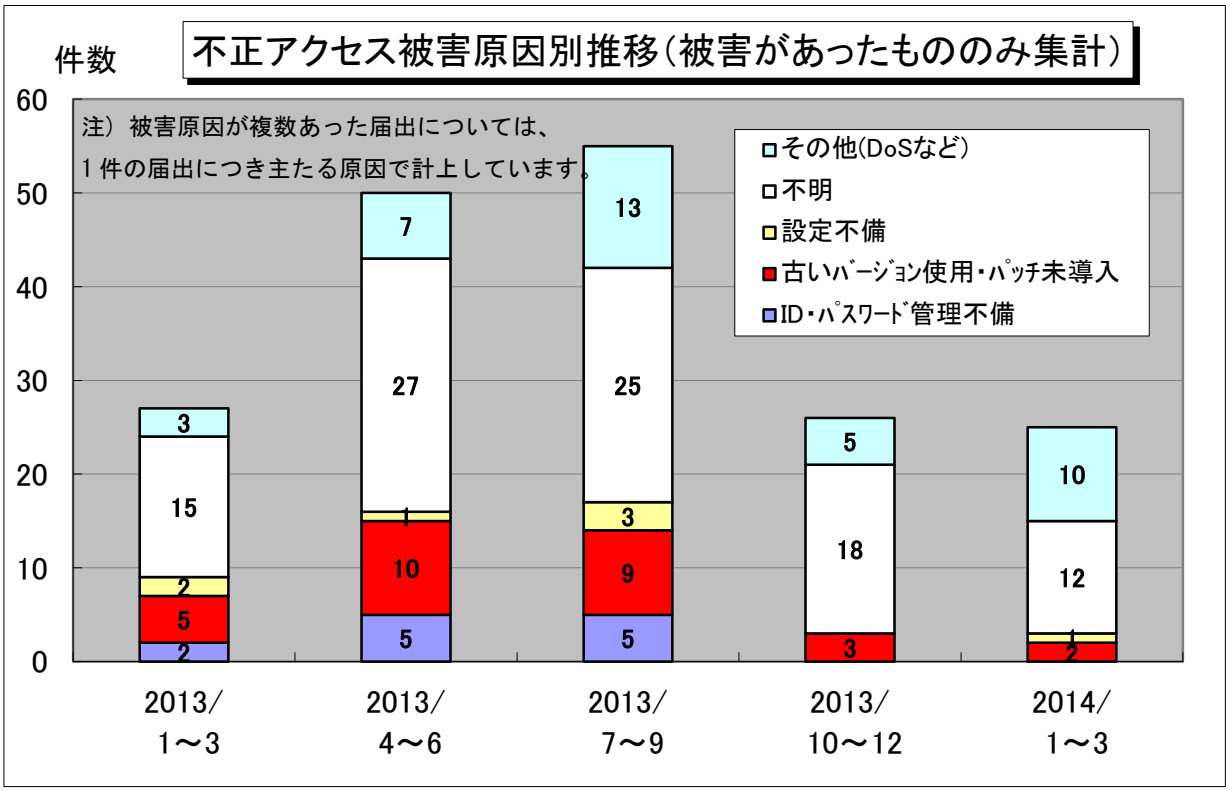


図 2-3. 不正アクセス被害原因別推移

2-5. 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。

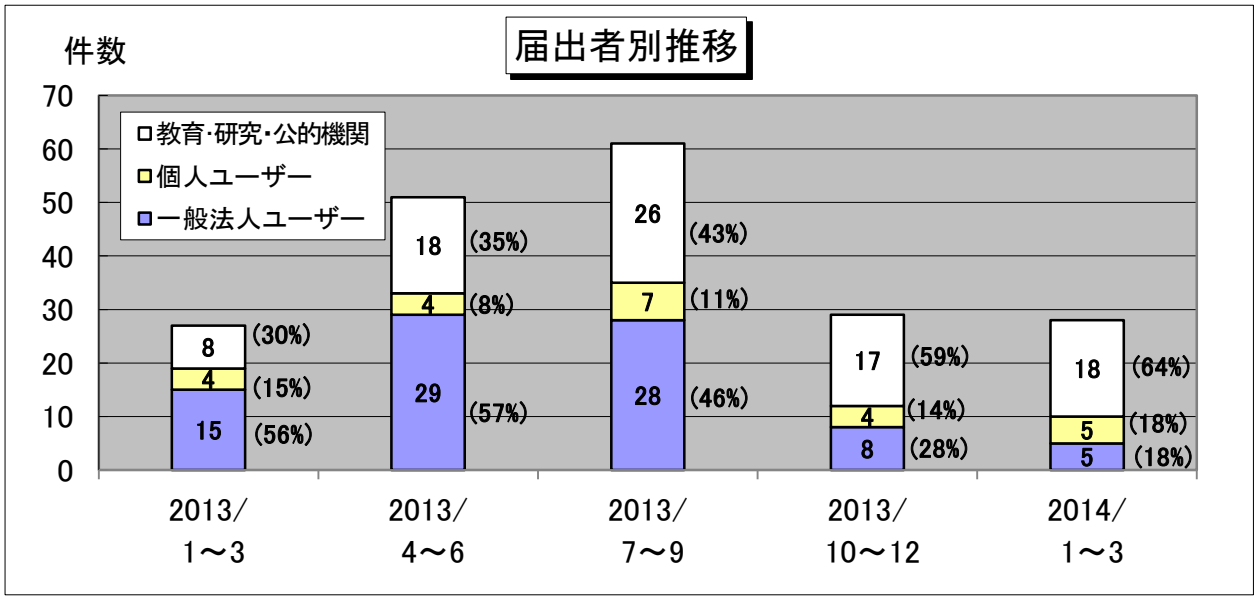


図 2-4. 届出者別推移

・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 1 月～3 月）のウイルス・不正アクセス関連の相談総件数は **3,585 件**でした（2013 年 10 月～12 月 : 4,179 件）。そのうち**『ワンクリック請求』**に関する相談が **706 件**（同 916 件）、**『偽セキュリティソフト等』**に関する相談が **177 件**（同 209 件）、**『スマートフォン』**に関する相談が **217 件**（同 210 件）などでした（図 3-3、図 3-4、図 3-5 参照）。

相談総件数を四半期ごとの推移で見ると、今期は前期と比べて 14.2%減となりました（図 3-1 参照）。

2013 年に国内過去最悪の不正送金被害をもたらした**『インターネットバンキング』**に関する相談は **69 件**と、前期の 76 件よりは減少したものの、いまだに感染被害は続いていると考えられます（図 3-6 参照）。また、グラフに記載はありませんが身代金型ウイルス**『ランサムウェア』**は、今期 **13 件**と前期の 8 件から増加しました。こちらも感染被害は続いていると言えます。

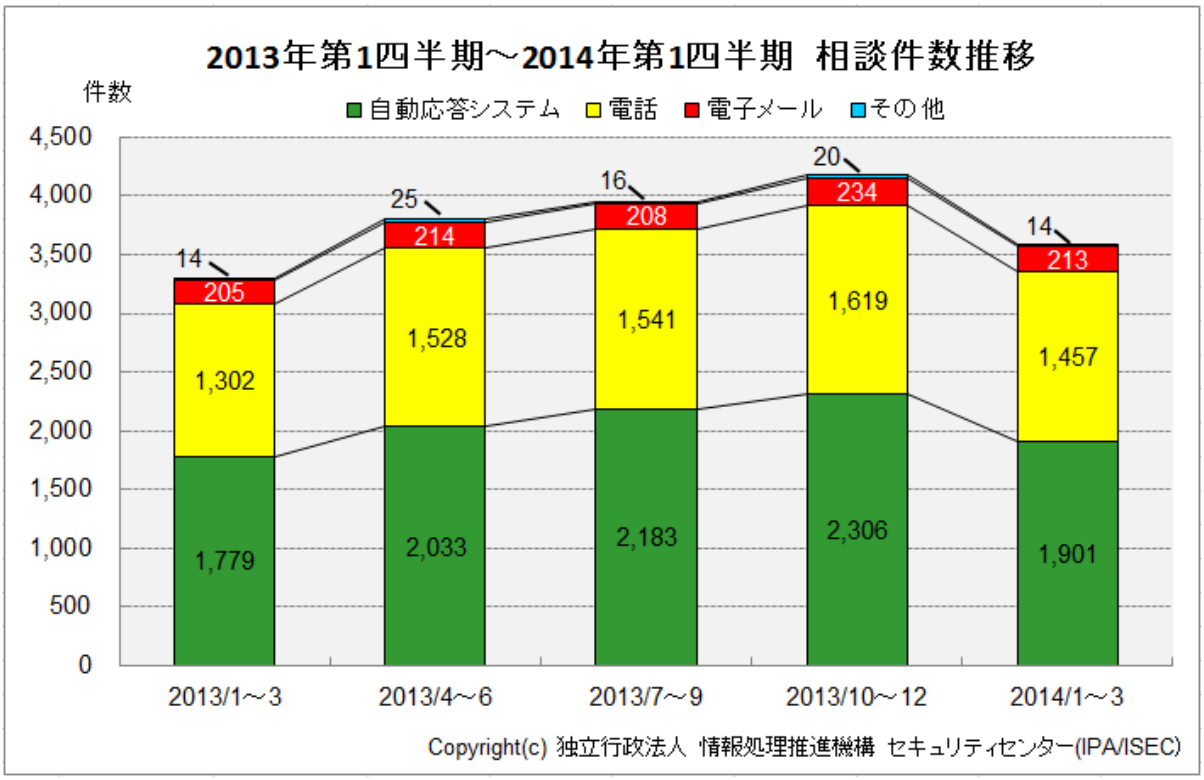


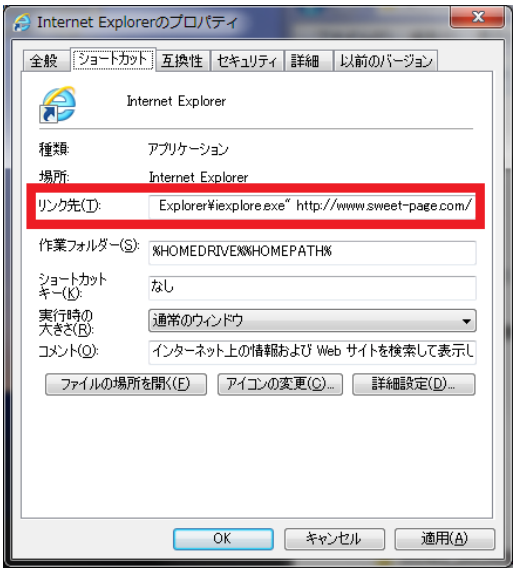
図 3-1. ウイルス・不正アクセス関連の相談件数

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/ 1～3		2013/ 4～6		2013/ 7～9		2013/ 10～12		2014/ 1～3	
合計	3,300		3,800		3,948		4,179		3,585	
自動応答システム	1,779	53.9%	2,033	53.5%	2,183	55.3%	2,306	55.2%	1,901	53.0%
電話	1,302	39.5%	1,528	40.2%	1,541	39.0%	1,619	38.7%	1,457	40.6%
電子メール	205	6.2%	214	5.6%	208	5.3%	234	5.6%	213	6.0%
その他	14	0.4%	25	0.7%	16	0.4%	20	0.5%	14	0.4%

3-2. 相談事例

（i）ブラウザのスタートページが”Sweet Page”になってしまって元に戻らない

相談	・無料のソフトウェアをダウンロードし、インストールした。それ以降ブラウザを起動すると、”Sweet Page”というページが表示されるようになった。 ・［コントロールパネループログラムのアンインストール］から、その時にインストールしたソフトウェアをアンインストールしたが、相変わらず表示される。 ・ブラウザの設定でスタートページを変更したが、ブラウザ起動直後に表示されるのは”Sweet Page”で変わらない。 ・セキュリティソフトでパソコンをスキャンしても何も見つからない。元に戻すにはどうしたらよいか。
回答	”Sweet Page”はいわゆる検索サイトで、他の検索サイトと同様にインターネット検索を利用できます。しかし「ディスクの空き容量低下」「エラー修正が必要」などという広告が表示されることがあり、最終的に何らかの製品を購入させることが目的と考えられます。 ”Sweet Page”に関する相談は、今四半期 30 件（1 月 18 件、2 月 10 件、3 月 2 件）あり、相談者全員が上述の被害に遭いました。 **相談者が、インターネットから何かしらフリーのソフトウェアをインストールした際、”Sweet Page”をブラウザのスタートページに表示するという設定に気がつかずインストールしてしまったものと考えられます。** **”Sweet Page”は、ブラウザの起動ショートカットのリンク先に”http://www.sweet-page.com”を追加（図 3-2）することで、ブラウザを起動する度に、”Sweet Page”のサイトページを最初に表示させます。** **そのため、ブラウザの「ホームページ」の設定を変更しても、”Sweet Page”が最初のページとして表示されてしまいます。** このようになってしまった場合、起動ショートカットのリンク先に追加されてしまった箇所を削除すれば、”Sweet Page”が最初に表示されることはなくなります。 起動ショートカットの修正がわからない場合は、起動ショートカットそのものを削除して、再度作り直して下さい。 方法がわからない時は、パソコンが操作できる状態で安心相談窓口までご連絡下さい（安心相談窓口：03-5978-7509）。  図 3-2. IE のショートカットプロパティ画面

（ii）Windows XP に関する相談について

相談	Q1. Windows XP のサポートが 4 月 9 日で終了すると聞いたが、終了してからも Windows XP を使い続けるとどうなりますか？ Q2. セキュリティソフトが入っているので使い続けても大丈夫ですか？ Q3. インターネットをしなければ大丈夫ですか？ Q4. 盗まれたり壊されたりして困る情報をパソコンに保存していないので、このまま Windows XP を使い続けたい。 Q5. 4 月 9 日以降、急に Windows XP パソコンが危険になるのでしょうか？
回答	A1. サポート終了後も Windows XP を使い続けると、ウイルス感染や不正アクセスを受ける可能性が高くなります。 A2. たとえセキュリティソフトを最新の状態で使用してもその脅威は拭えません。 パソコンのセキュリティ対策は、以下 2 点の両方が必要です。 1. OS と各種プログラムの脆弱性の解消 2. セキュリティソフトを常に最新の状態で使うこと Windows XP のサポート終了後は上記 1.を実施できないため、セキュリティ対策として不十分です。 A3. インターネットに接続しなければ大丈夫とは言えません。インターネットのみならず、LAN などのネットワークにも接続しないことが必要です。具体的には“他のパソコンとは接続をしない”、“USB メモリなどの外部記憶媒体にも接続しない”といったことを守る必要があります。他のパソコンや USB メモリからウイルスに感染する場合があるからです。 A4. 盗まれて困るようなデータがパソコンに保存されていなくても、ウイルスに感染すると迷惑メールの発信元として悪用されたり、他のパソコンへの攻撃に悪用される恐れがあります。その状態で Windows XP を使い続けていると、プロバイダーから警告のメールが届くことがあり、それも無視し続けるとプロバイダーから一方的に接続を止められてしまう場合があります。 また遠隔操作ウイルスに感染すると、自分のパソコンを拠点として、犯罪予告などを掲示板に書き込む行為に加担させられる恐れもあります。 A5. 4 月 9 日から急にパソコンが危険になる、ということではありません。しかし 2014 年 5 月にマイクロソフト社から Windows 8、Windows 7 などの月例パッチが公表されると、その修正に関する脆弱性情報が Windows XP パソコンへの攻撃のヒントになる可能性があります。 （参考） 「あなたのパソコンは 4 月 9 日以降、大丈夫？」 ～使用中パソコンの判別方法、乗り換えプランを紹介～ http://www.ipa.go.jp/security/txt/2014/04outline.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 706 件寄せられました。前四半期は過去 1 年間で件数が最多でしたが、今四半期では約 23%（210 件）減少しました。一方、『ワンクリック請求』に関する相談のうち、スマートフォンにおける『ワンクリック請求』に関する相談は 135 件で、前四半期の 164 件から約 18%（29 件）減少しました。

今四半期の相談件数は減少しましたが、長期的に見ると決して減少していると言えない状況です。

『ワンクリック請求』は、数分おきに料金請求画面をパソコンに表示して利用者を心理的に追い込みます。その料金請求画面は、動画などを装ったプログラムをパソコン利用者が自分で実行することで表示されます。ウェブサイト閲覧中にプログラムの実行が繰り返し表示されても、安易に実行しないことが重要です。

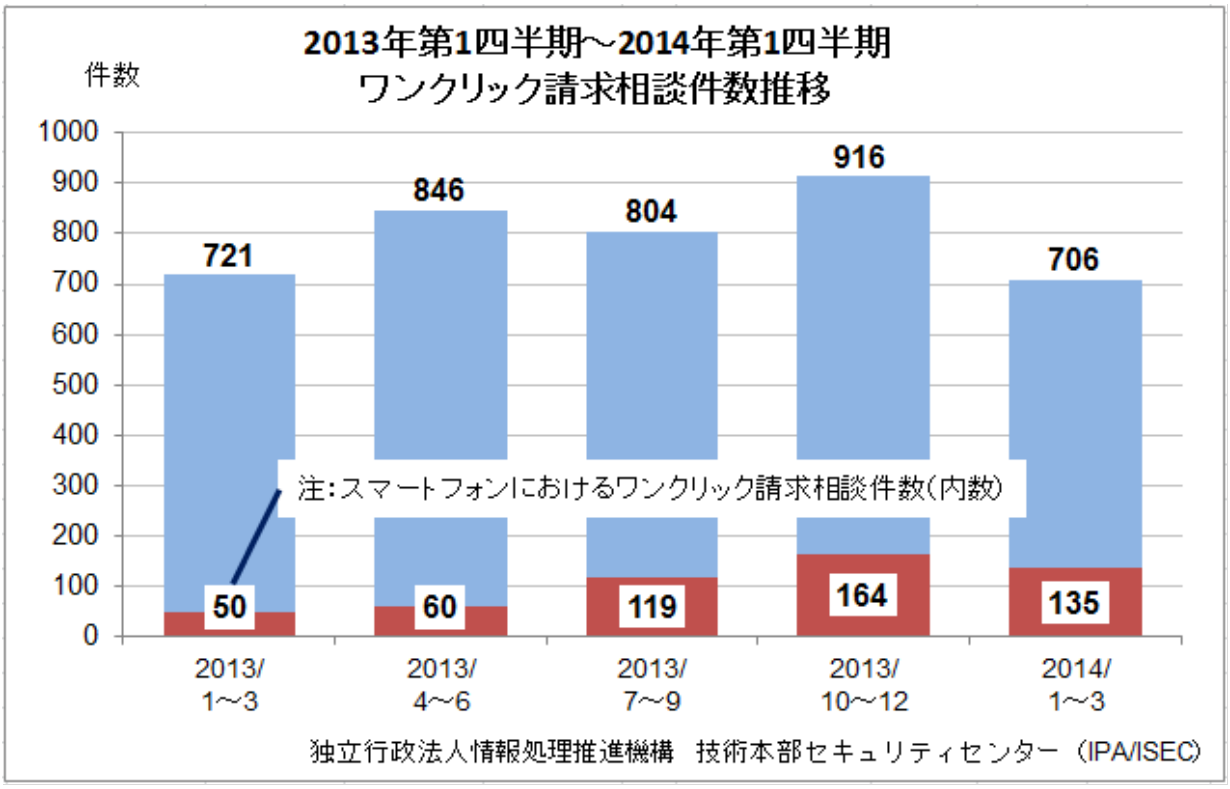


図 3-3.『ワンクリック請求』相談件数推移、および
『スマートフォン』における『ワンクリック請求』相談件数推移

(ii)『偽セキュリティソフト等』に関する相談

『偽セキュリティソフト等』に関する相談は、今四半期 177 件寄せられました。前四半期から約 15%（32 件）減少しました。

最近の『偽セキュリティソフト等』の感染手口は、パソコンの脆弱性を悪用し、利用者の知らない間に勝手にインストールされてしまうものから、“お使いの PC がクラッシュ寸前です！”、“お使いのパソコンの性能が低下しています！”などの警告を表示し、その広告をクリックさせて利用者にダウンロード・インストールを促すものなど多様化しています。**利用者は、OS や各種ソフトウェアを常に最新の状態で使用するなどの基本的な対策だけでなく、自分がどんなセキュリティソフトを使っているのかを確認してください。またセキュリティソフトを使用しているのであればこうした広告が表示されても鵜呑みにして、安易にクリックせず、無視して下さい。**

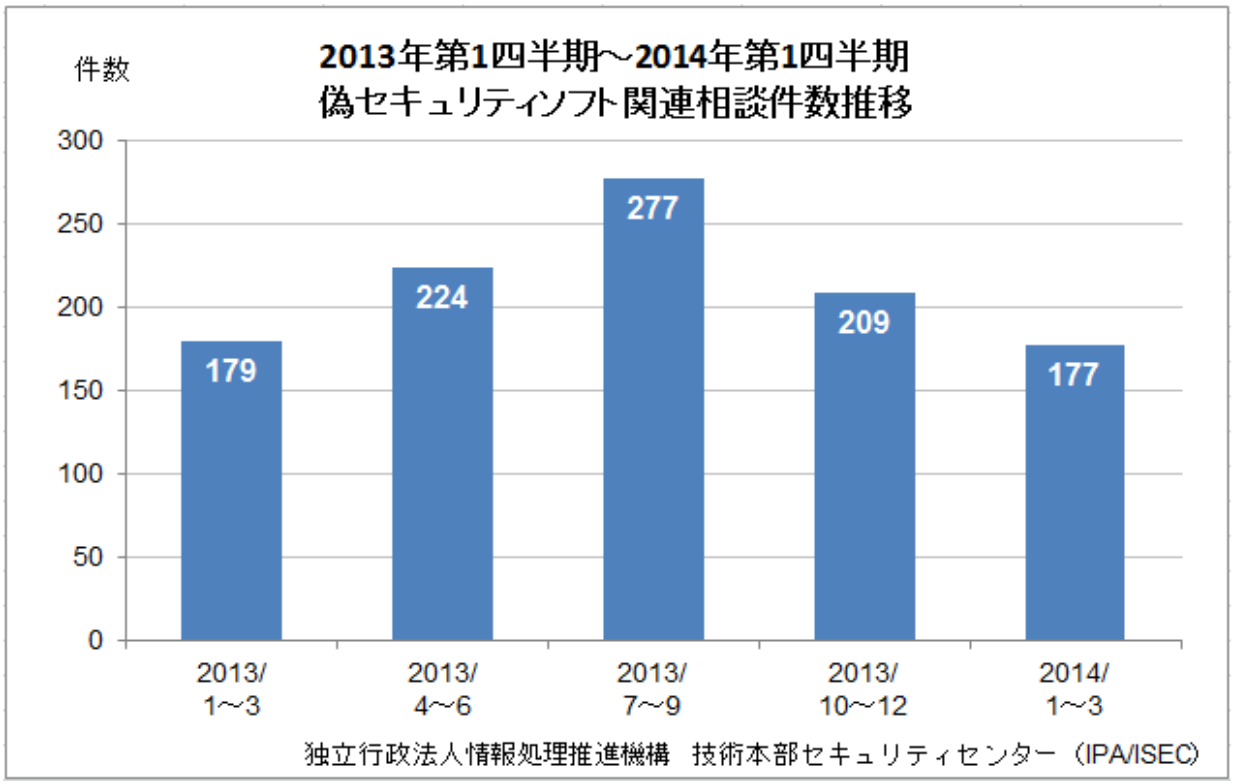


図 3-4.『偽セキュリティソフト』関連相談件数推移

(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 217 件寄せられました。前四半期から約 3%（7 件）増加しました。

『スマートフォン』に関する相談のうち、『ワンクリック請求』に関する相談以外の件数は 82 件ありました。その多くは“ウイルス感染”や“不正アクセス”の疑いについての相談でした。確固たる証拠がなく、またスマートフォンそのものではなくスマートフォンを通じて利用するクラウドサービスに関する相談もあり、その多くは原因の切り分けが困難なものでした。

そのような疑いを持った場合は、

- **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**
- **アカウント／パスワードを使用するウェブサイトの情報が誰か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**
- **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**

などを確認して下さい。また、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撮影し、それを元にまずは当機構の安心相談窓口（03-5978-7509）にご相談下さい。

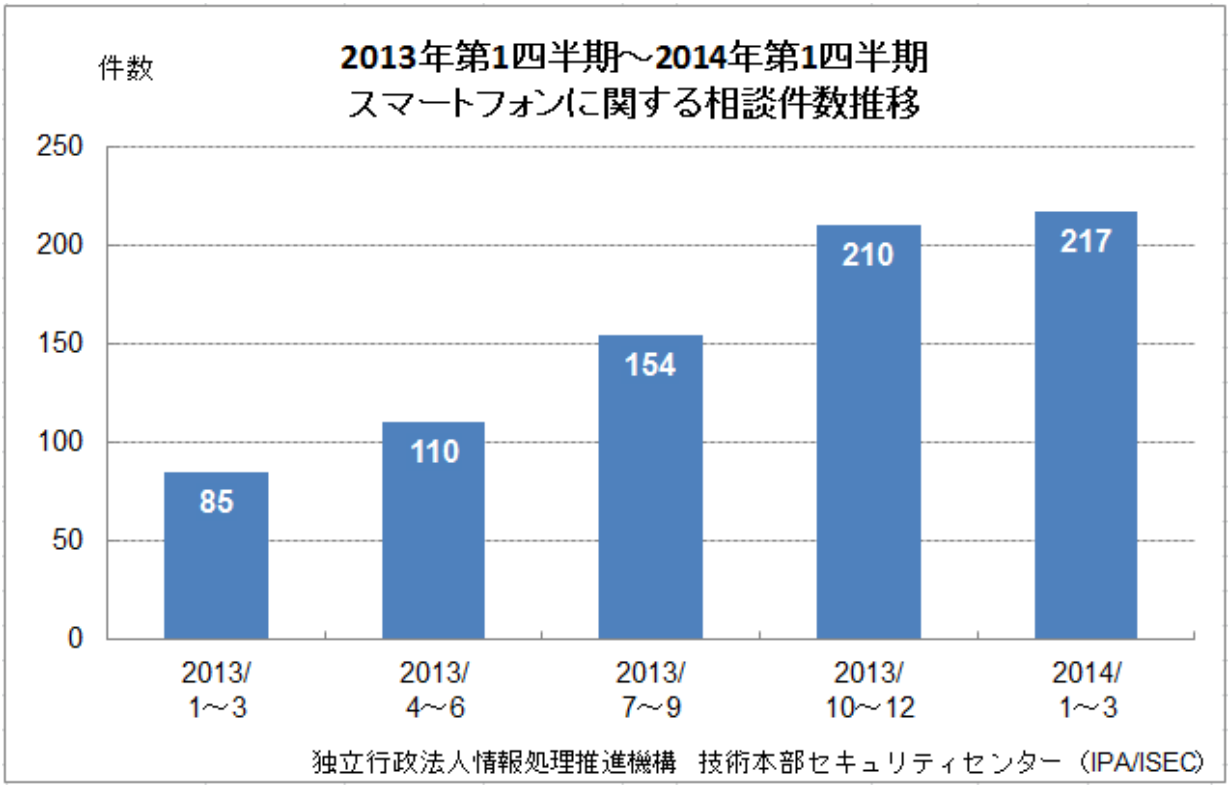


図 3-5.『スマートフォン』に関する相談件数推移

（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 69 件寄せられました。前四半期からは約 9%（7 件）減少しました。内訳は、銀行を騙ったフィッシングメールについての相談内容が 12 件、**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内容が 49 件**、その他が 8 件でした。

不正画面の表示については、暗証番号や乱数表、合言葉の情報を詐取するウイルスに感染したことが原因です。この場合、**セキュリティソフトを使用して感染したウイルスを全て駆除する必要がありますが、セキュリティソフトを使ってもウイルスが見つからない場合、パソコンを購入した時点まで戻す初期化（リカバリ）処理をお勧めします。**

ウイルス感染の相談内容の中には、「インターネットバンキングが使えない」旨の相談内容がありました。これは、**相談者が先に当該銀行に問合せしたところ、既にウイルスによって相談者の情報が盗まれていることを銀行側で把握していたため、当該相談者のインターネットバンキングの利用を停止していたことがわかりました。**サービス利用を再開するためには、パソコン内のウイルスを駆除するかパソコンを初期化した後で、サービス停止解除の依頼を銀行側に行う必要があります。

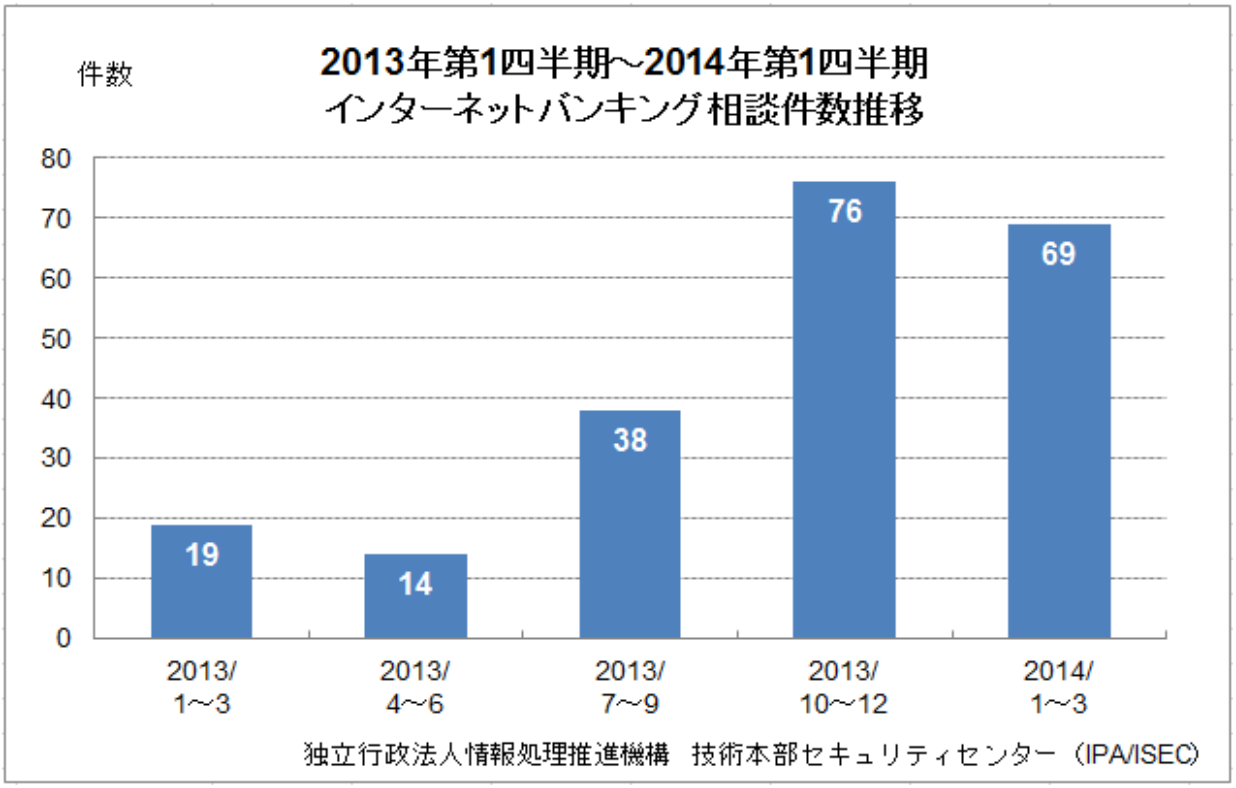


図 3-6.『インターネットバンキング』相談件数推移