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 年年間（1 月～12 月）]

本レポートでは、2014 年 1 月 1 日から 2014 年 12 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 1 月 26 日

目次

1. コンピュータウイルス届出状況

1-1. 2014 年総括

2014 年に寄せられたウイルスの検出数は、2013 年の 195,550 個より 112,522 個（約 58%）少ない 83,028 個でした。また、2014 年の不正プログラム検出数は 2013 年の 233,341 個から 147,284 個（約 63%）多い 380,625 個でした。

同一日、同一種のウイルス報告を 1 件とカウントするなど、所定の方法で集計した 2014 年のウイルス届出件数 (*1) は 5,014 件で、2013 年の 6,596 件から 1,582 件減少しました（図 1-1）。

2014 年のウイルス感染被害については、以下の 2 件の届出がありました（表 1-1）。

表 1-1：ウイルス感染被害届出

時期	届出元	セキュリティソフトの利用	ウイルス名	感染経路	被害状況	発見詳細	感染原因	対処
2014年3月	一般法人	あり	W32/Cryptolocker	不明	パソコンおよびファイルサーバー内ファイルの暗号化	ファイルサーバー内ファイルの文字化けを発見	不明	バックアップデータを使用して復旧
2014年6月	一般法人	あり	W32/Burnwoo	外部記憶媒体（SDカード）	感染端末（3台）から外部ウェブサイトへのアクセス試行	インターネット接続ログから不審な通信を発見し、感染パソコンおよび感染経路を特定	第三者とのやり取りで使用していたSDカード内に保存されていたファイルを実行したため	パソコンおよびSDカードの初期化

2014 年 3 月に届出された 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解除を名目に身代金を要求するランサムウェア (*2) と呼ばれるタイプのウイルスです。

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。しかし、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、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。

このような事態に備えてバックアップを定期的に行うことが重要です。また、外部記憶媒体へバックアップする際には上述のファイルサーバーと同様の被害に遭わないように、“バックアップ時のみバックアップ媒体を接続する”、“バックアップ媒体を複数用意する”などの対策を行うことが重要です。

(*1) 届出件数：同じ届出者から寄せられた届出の内、同一発見日で同一種類のウイルスの検出が複数ある場合は、1 日何個検出されても届出 1 件としてカウントし集計している。

(*2) 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。

1-2. 検出数 (*3) が多かったウイルス・不正プログラム (*4)

2014 年に寄せられたウイルスの年間検出数の第 1 位は W32/Mydoom (*5) で、検出数は 2013 年の 147,197 個から約 79%減少し 30,730 個（図 1-2）でした。検出数第 2 位の W32/Netsky も W32/Mydoom と同様に、メールの添付ファイルとして拡散し感染を広げます。これらは 2013 年と比べて検出数は減少していますが、こうしたウイルスに感染しているサーバーやパソコンがいまだに多数存在していると言えます。

2014 年に寄せられた不正プログラムの年間検出数の第 1 位は Bancos (*6) で、検出数は 65,942 個（図 1-3）でした。2013 年は 30,867 個で、前年比較では倍増していますが、2014 年 5 月以降は減少しました。これは金融機関や利用者のセキュリティ対策が進んだことで、攻撃者が別の手口に移行し、当該不正プログラムの流通が減少したことがひとつの要因と考えられます。

ウイルスと不正プログラムについては、メールに添付されて送られてくるものが多数存在します。このため、メールの添付ファイルの開封には十分注意するとともに、身に覚えのないメールは開かずに削除することが有効な対策です。メール以外では、ウェブサイトにウイルスや不正プログラムを仕込み、閲覧者に感染させる手口が増加しています。

このためパソコンだけでなくスマートフォンなども利用する際は、Windows などの OS やアプリケーションソフトを最新のバージョンにして脆弱性を解消しておくとともに、ウイルス対策機能を有するセキュリティソフトを適切に使用することが重要です。

1-3. 届出件数

2014 年の届出件数は 5,014 件でした。そのうち被害があったと届出されたのは 2 件でした。下記グラフ（図 1-1）は、IPA が受け付けた年別ごとの届出件数の推移を示したものです。

図 1-1 で示すように、届出件数は 2013 年の 6,596 件から 1,582 件減少しました。2005 年以降の減少傾向は、一般利用者へのセキュリティソフトの普及や、企業でのウイルスゲートウェイ導入など、ウイルスへの対策が進んだためと推測されます。

(*3) 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）。

(*4) 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

(*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。

(*6) 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不正プログラム。

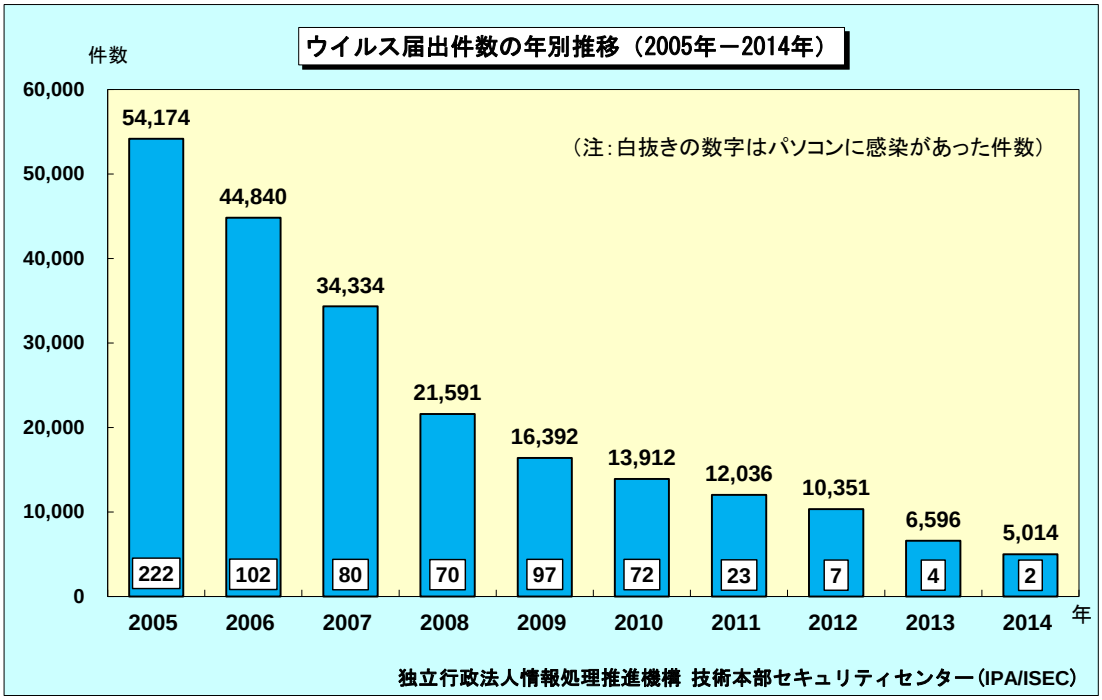


図 1-1：ウイルス届出件数の年別推移（2005 年～2014 年）

1-4. ウイルス検出数 (*7)

2014 年のウイルス検出数は 83,028 個と、2013 年の 195,550 個から 112,522 個の減少となりました

2014 年のウイルス別検出数推移は以下の通りです（図 1-2）。2 月に W32/Mydoom の検出数が急減し、その後横ばいが続いています。

(*7) 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。

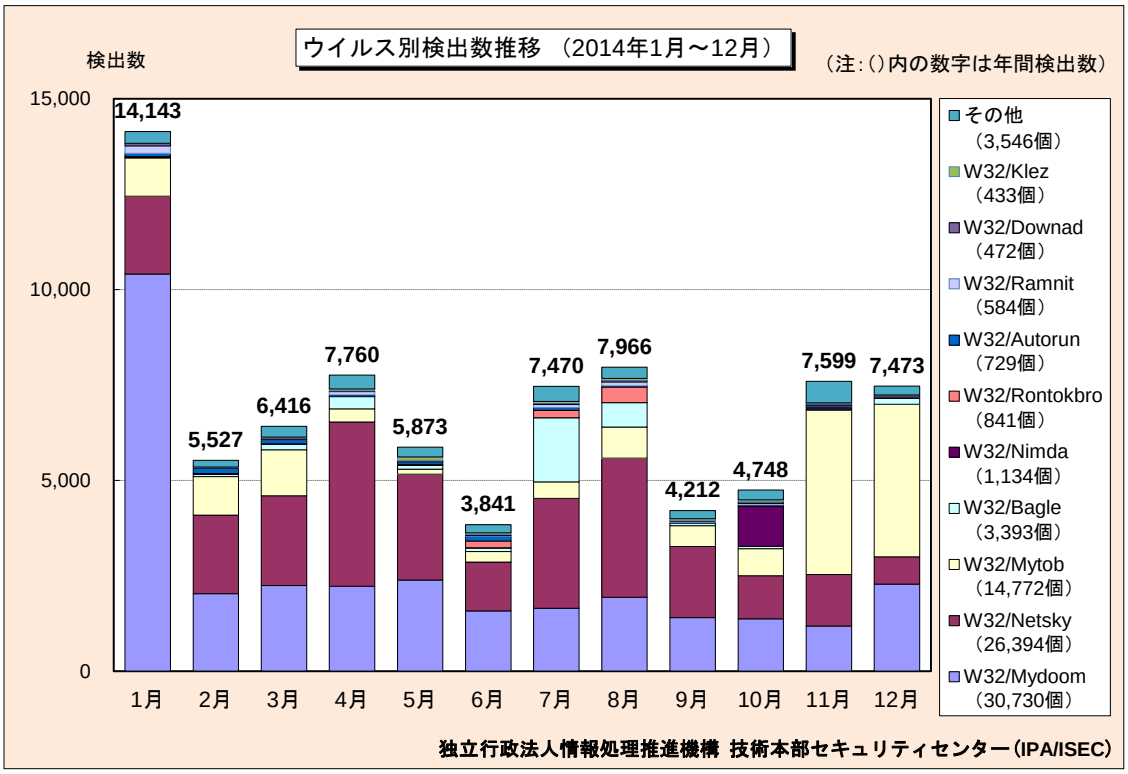


図 1-2：ウイルス検出数の推移（2014 年 1 月～12 月）

1-5. 不正プログラム検出数 (*8)

2014 年の不正プログラムの検出数は 380,625 個と、2013 年の 233,341 個から、147,284 個（63.1%）の増加となりました。

2014 年の不正プログラム別検出数推移は以下の通りです（図 1-3）。Bancos の検出数が 5 月に激減し、それ以降は低水準が続いています。

(*8) 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。

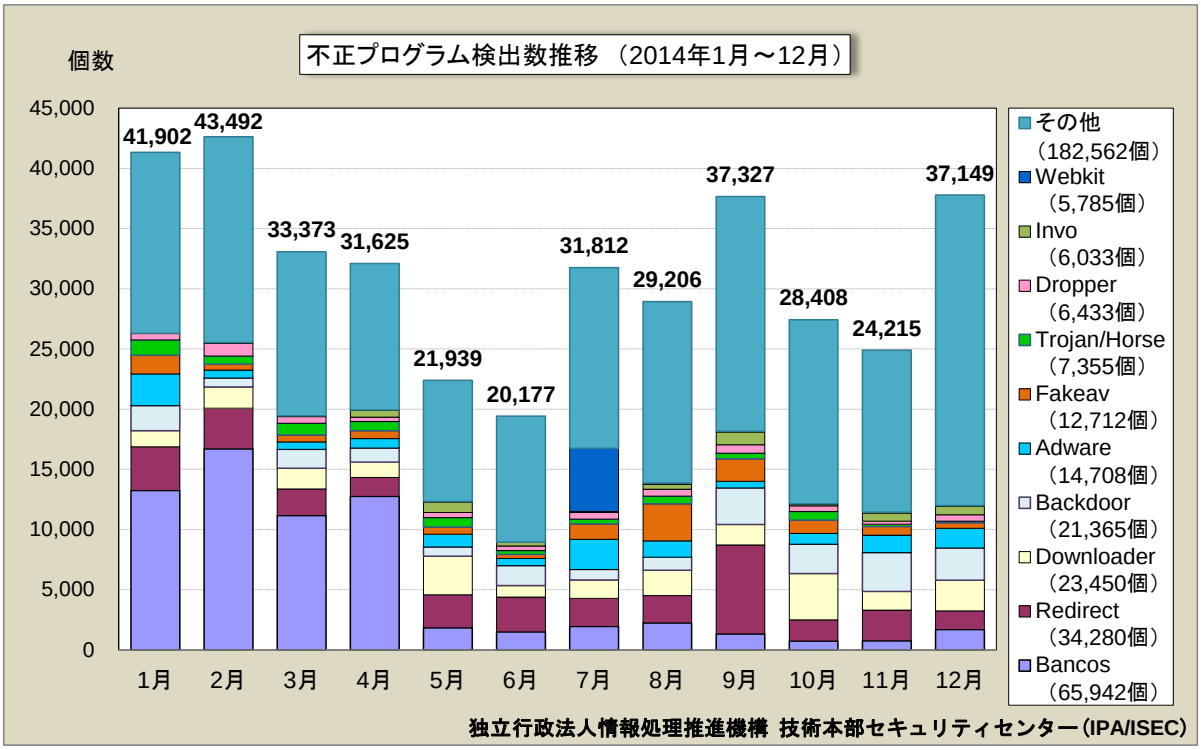


図 1-3：不正プログラム検出数の推移 (2014 年 1 月～12 月)

1-6. ウイルス届出者構成及び検出経路

2014 年の届出者属性は、ほとんど法人が占めており、2013 年と同様の傾向でした（表 1-2）。

表 1-2：ウイルス届出者別件数

届出者	2014年1月～12月	%	2013年1月～12月	%
一般法人	4,884	97.4%	6,408	97.1%
個人	0	0.0%	0	0.0%
教育機関	130	2.6%	188	2.9%
合計	5,014		6,596	

2014 年の検出経路は、2013 年と比べてメールが 111,712 個減少しましたが、ダウンロードファイルが 113,601 個増加しました（表 1-3）。理由として、組織や利用者のメールに関するセキュリティ対策が進んだことで、攻撃者の手口がダウンロードファイルへ移行したことがひとつの要因として考えられます。

表 1-3：ウイルスおよび不正プログラム検出数（検出経路別）

検出経路	2014年1月～12月	%	2013年1月～12月	%
メール	82,375	17.8%	194,087	45.3%
ダウンロードファイル	298,137	64.3%	184,536	43.0%
外部記憶媒体	45	0.0%	81	0.0%
ネットワーク	973	0.2%	1,637	0.4%
不明	29,962	6.5%	10,157	2.4%
その他	52,160	11.2%	38,340	8.9%
合計	463,652		428,838	

・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. 2014 年総括

2014 年の年間届出件数は 120 件となり、2013 年の届出件数 168 件から 48 件（約 28%）減少しました。120 件の年間届出のうち被害があった件数は 102 件で、全体の約 85%を占めました。

2014 年の届出件数のうち、『侵入』の届出数は 16 件であり、2013 年の 98 件と比較すると大きく減少しています。2013 年はウェブサイト改ざんの届出が 75 件ありましたが、2014 年はウェブサイト改ざんの届出は 15 件に留まりました。2014 年はウェブサイト改ざん被害が収束傾向にあったと考えられ、これに連動して『侵入』の届出および年間の届出件数が減少しました。

2014 年は OpenSSL の脆弱性 (*9) や bash の脆弱性 (*10) などが指摘されました。対象となる製品やサービスが多く、影響が広範囲に渡る脅威であったと言え、サーバー管理者にとっては迅速な対応が求められました。一部では適切な対策が行えなかったために、これらの脆弱性を悪用されてしまう被害もありました。しかし、対象や影響の大きさから脆弱性の存在が広く知られたことで、対策が一斉に進められたと考えられます。結果として脆弱性の対策を行ったサーバーが増えたことが、ウェブサイト改ざん届出が減少した理由の 1 つと考えられます。

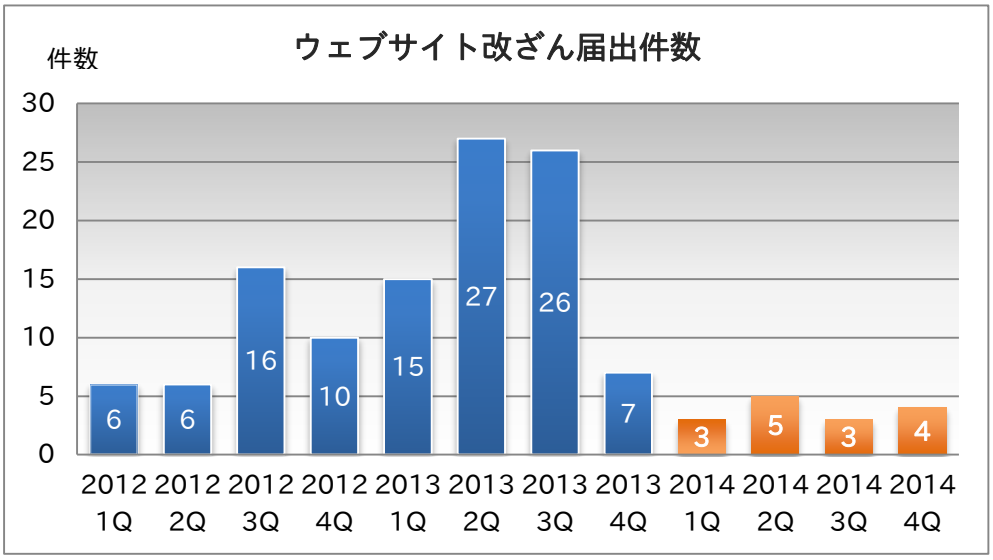


図 2-1. ウェブサイト届出件数の推移

一方で、2013 年には届出のなかったパスワードリスト攻撃の届出が 2014 年は 4 件ありました。報道された情報によるとパスワードリスト攻撃が原因と考えられる不正ログイン被害は、2013 年より継続的に発生しており、2014 年も収束の兆しがなかったことから 2014 年 9 月に IPA から被害防止に向けた注意喚起 (*11) を行いました。

(*9) OpenSSL の脆弱性対策について(CVE-2014-0160)
https://www.ipa.go.jp/security/ciadr/vul/20140408-openssl.html

(*10) 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

(*11) 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

また、パスワードリスト攻撃と同様に継続的に発生しているのが、メールアカウントが不正使用され、スパムメール送信の踏み台とされてしまう被害です。2013 年は 27 件の届出があり、2014 年は 20 件の届出がありました。ほとんどの被害でメールアカウント不正使用の原因は特定されていませんが、当該アカウントのパスワード変更により被害の再発を防げたことから、推測が容易なパスワードの利用、パスワードの使い回し、フィッシングサイトへの入力等が原因であったと考えられます。

パスワードリスト攻撃の被害、スパムメール送信の踏み台となる被害、いずれも、ウェブサイト改ざん被害のようにサーバーの脆弱性が起因するものではないため、サーバーの脆弱性を解消していても被害を防ぐことはできません。

これらの被害の防止については、ユーザーは“パスワードの使いまわしをしない”、“二段階認証などのセキュリティオプションを積極的に採用する”など、適切なアカウント管理とリスクへの対策を実施することが推奨されます。また、システム管理者向けの対策として、“ログイン通知やログイン履歴の機能を設ける”、“外部からメールサーバへ接続する際にはアカウント情報以外の認証情報を必要とする”など、不正ログインを早急に検知できるような機能追加を検討することが推奨されます。

2-2. 被害事例

(i) bash の脆弱性を悪用され不正なスクリプトを実行された

被害の概要	・突如、大量の通信が発生し、回線が輻輳（ふくそう）(*12) 状態に陥った。 ・調査を進めたところ、あるサーバー上で不正なスクリプトによる大量の通信が発生していることが確認できた。 ・bash の脆弱性を悪用されて、不正なスクリプトが特定の日時に実行されるように cron (*13) の設定が書き換えられていたことがわかった。
解説・対策	被害に遭ったサーバー上に、OS インストール時に生成される cgi（先頭に「#!/bin/sh」と記述されている）サンプルファイルが削除されていなかったことで、当該ファイルを通して bash の脆弱性を悪用されてしまった事例です。 恒久的な対策が存在しない時点で脆弱性情報が公表された場合は、暫定的であっても被害に遭わないために回避策を行うことが望まれます。 特に今回の事例のように、デフォルトで生成されるファイルや設定の初期値などをそのまま利用することは、攻撃者に不正アクセスに必要な一部の情報を提供していることと同じとも言えます。被害に遭わないためにも、変更が不可能な内容以外は、ファイル名や設定値などをそのまま利用することは避け、また利用しないファイルは削除する、利用しない設定であれば変更（削除、停止）するといった対策が必要です。

(*12)輻輳（ふくそう）：物が集中して込み合う様態。ネットワークの分野においては、回線の帯域を逼迫する量のトラフィックが発生することで通信がしにくい、応答が遅くなるといった状況を意味する。

(*13)cron（クーロン）：ジョブを自動実行するためのプログラム。設定されたスケジュールに基づき、コマンドやシェルスクリプトを自動実行する。

（ii）辞書攻撃で不正ログインされてしまい外部に大量のパケットを送出していた

被害の概要	・ファイアウォールのログ情報より、あるサーバーの送信バイト数が異常に多いという連絡を受けた。 ・当該サーバーを調査したところ心当たりのないプログラムが実行されており、外部宛に意図しない大量のパケットを送出していたので、ネットワーク回線を遮断した。 ・調査を進めたところ、root アカウントに対して SSH 接続で辞書攻撃を仕掛けられ、不正ログインされていたことが判明した。 ・辞書攻撃が開始される前には、SSH 接続を制限するフィルタリング設定がされていたが、システム移行の際に動作不良が発生したので事象解消のために解除していた。 ・実行されていたのはプログラムのコードや挙動から、DDoS 攻撃用のプログラムと推測された。
解説・対策	root アカウントのパスワードを辞書攻撃で破られてしまったことで、サーバーに不正なプログラムを設置、実行されてしまった事例です。 対策としては強固なパスワードを設定する他、root アカウントでのログインを禁止する、ログイン試行の回数制限を設定するなどの対策もあります。 なお、今回の被害では推測が容易なパスワードを設定してしまっていたことが主因ではありますが、結果として外部から当該サーバーへのアクセスを許可してしまうこととなったフィルタリング設定の解除も原因の 1 つと言えます。 フィルタリング設定を行っていた場合、システム構成の変更などにより機器の IP アドレスや通信の流れが変わると、本来許可すべき通信が制御されてしまい、システムが適切に機能しなくなることもあります。システム構成を変更する場合には同時にフィルタリング設定の見直しが必要となりますが、設定変更にあたっては変更後もシステム全体としてのセキュリティレベルが維持できるかをしっかりと確認する必要があります。仮にフィルタリング条件を緩和させなくてはならない場合には、設定変更に伴うリスクについても事前に十分に考慮、検討することが重要です。

2-3. 届出件数

2014 年の年間届出件数は 120 件となり、2013 年の届出件数 168 件から 48 件（約 28%）減少しました。なお、下記グラフは、過去 10 年間に IPA セキュリティセンターが受け付けた届出件数の推移を示したものです（図 2-2）。

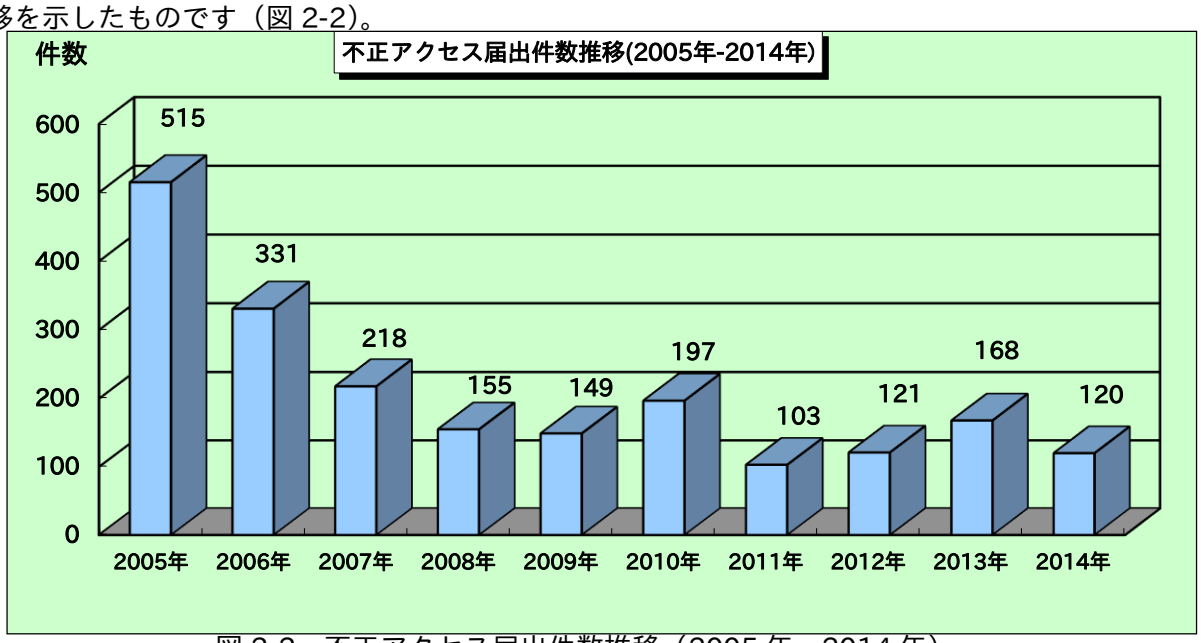
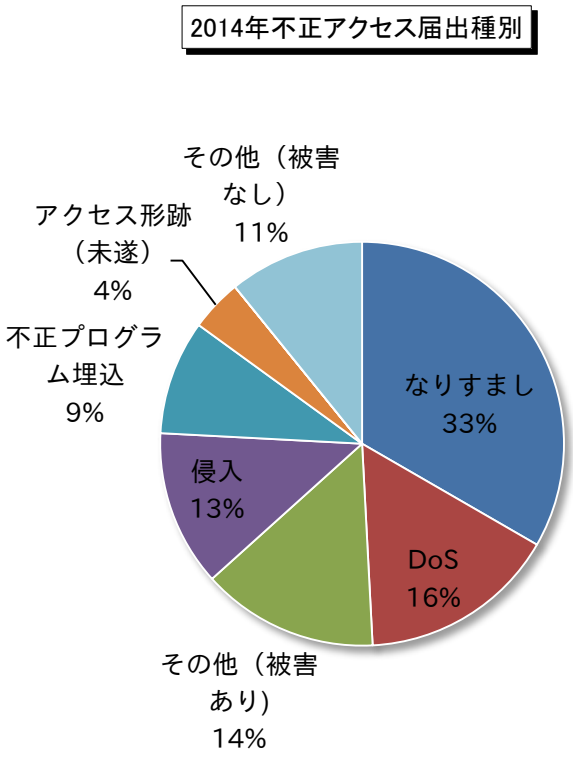


図 2-2：不正アクセス届出件数推移（2005 年～2014 年）

2-4. 届出種別

2014 年は 2013 年と比較すると「侵入」の届出数の大幅減、また「DoS（サービス妨害）」および「不正プログラム埋込」の届出数の増加が目立ちました（図 2-3）。それぞれの主だった被害内容は次の通りです。

- 「DoS（サービス妨害）」19 件のうち、6 件は「NTP を悪用した DoS [(*14)]」、2 件は「chargen [(*15)] サービスを悪用した DoS」
- 「不正プログラム埋込」11 件のうち、6 件は「ボットと推測される不正プログラム」、2 件は「Bitcon [(*16)]（ビットコイン）のマイニングプログラム [(*17)]」



届出種別		2014 年	2013 年
被害あり	侵入	16	99
	メール不正中継	0	1
	ワーム感染	0	0
	DoS(サービス妨害)	19	11
	アドレス詐称	0	0
	なりすまし	40	40
	不正プログラム埋込	11	3
	その他（被害あり）	16	4
被害なし	アクセス形跡（未遂）	5	6
	ワーム形跡	0	0
	その他（被害なし）	13	4
合計　（件）		120(102)	168(158)

※合計のカッコ内の数字は、被害ありの届出種別の合計を示しています。

図 2-3：2014 年不正アクセス届出種別

[(*14)]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

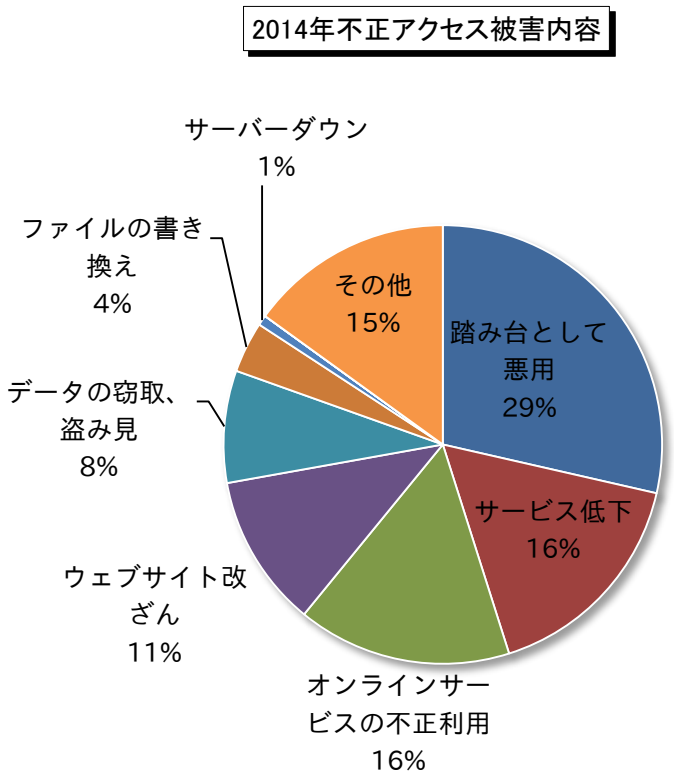
[(*15)]chargen：接続すると任意の文字を送信する、試験やデバッグを目的としたプロトコル。TCP 接続の場合、接続が閉じられるまで文字を送信し続ける。

[(*16)]ビットコイン：2009 年に誕生したインターネット上の仮想通貨。インターネット上のショッピングのみならず、ビットコイン決済に対応している現実の店舗でも利用が可能。

[(*17)]マイニングプログラム：ビットコインは既存通貨との両替以外に、「miner」という専用ソフトでマイニング（採掘）することでも入手ができる。採掘には複雑な数学的計算が必要であるため、処理能力の高いコンピュータが必要となる。

2-5. 被害内容

届出のうち実際に被害があった内容の分類です。のべ被害件数は前年から 62 件（約 32%）減少しました（図 2-4）。「**ウェブサイト改ざん**」の届出件数が 60 件減少しているのは、2014 年のウェブサイト改ざん被害減少が要因と考えられます。



被害内容	2014 年	2013 年
メール不正中継	0	1
サーバーダウン	1	0
不正アカウントの作成	0	2
ウェブサイト改ざん	15	75
パスワードファイルの盗用	0	0
サービス低下	22	22
オープンプロキシ	0	0
ファイルの書き換え	5	1
踏み台として悪用	38	50
オンラインサービスの不正利用	21	19
データの窃取、盗み見	11	12
その他	20	13
合計　（件）	**133(※)**	**195(※)**

※実被害届出 1 件に複数の被害内容が存在するケースもあるため実被害届出件数合計と一致していません。

図 2-4：2014 年不正アクセス被害内容

2-6. 不正アクセス届出者構成

2014 年は 2013 年と比較すると届出者別の内訳は「法人」からの届出件数が減少し、「個人」からの届出件数が増加しました（図 2-5)。「法人」からの届出件数の減少は、2014 年はウェブ改ざん被害が収束傾向にあったためと考えられます。「個人」からの届出件数 28 件のうち、21 件は「なりすまし」であり、ウェブメールやオンラインゲームのアカウントへの不正ログイン被害に関する届出でした。

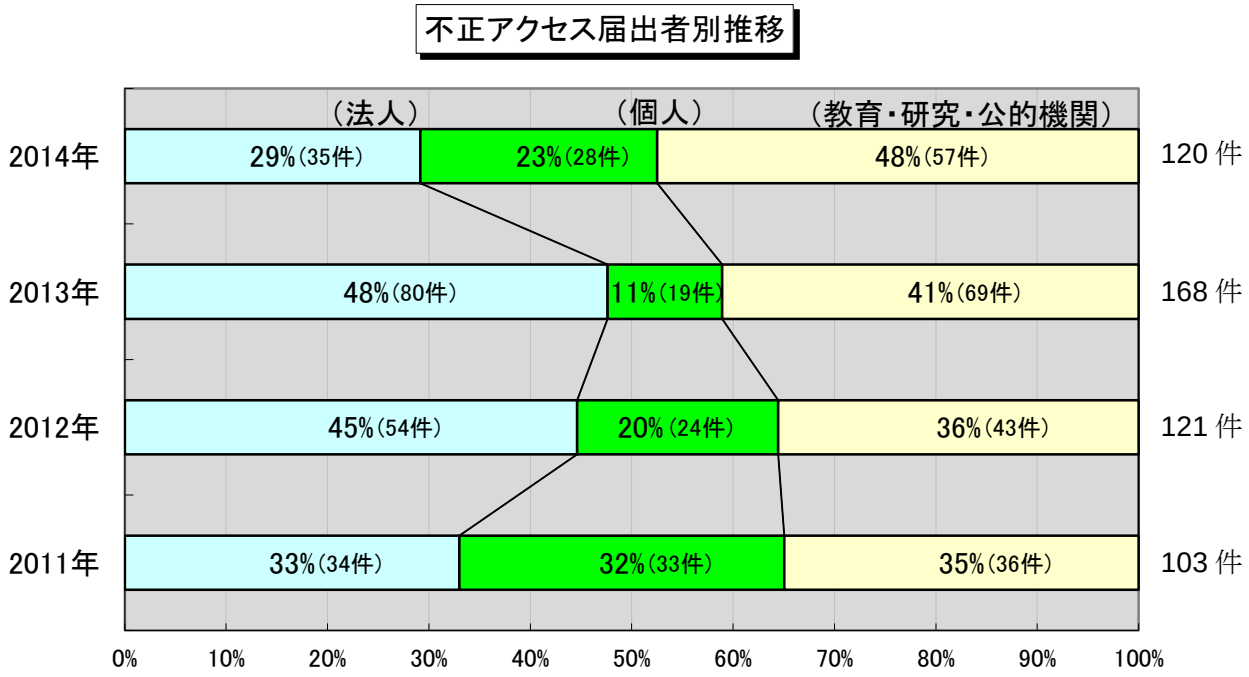
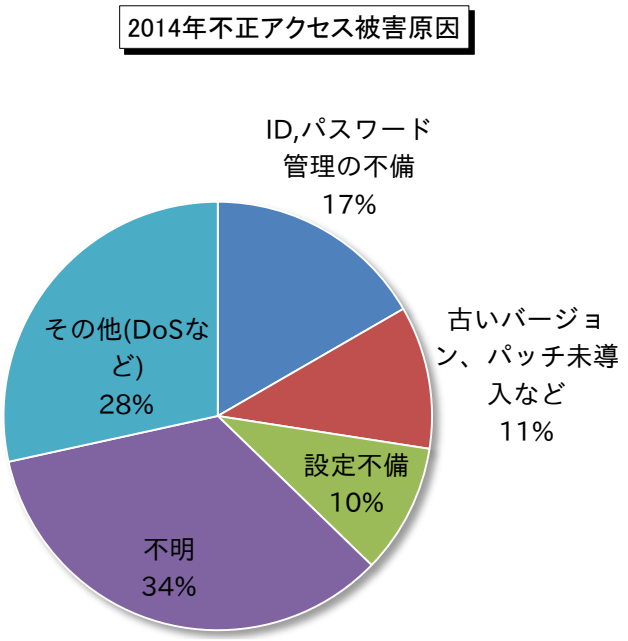


図 2-5：不正アクセス届出者別年次推移

2-7. 被害原因

実際に被害があった届出の原因の内訳は、「ID・パスワード管理の不備」が 17 件（17%）、「古いバージョン使用・パッチ未導入などが」11 件（11%）、「設定不備」が 10 件（10%）、「不明」が 35 件（34%）でした（図 2-6）。



被害原因	2014 年	2013 年
ID,パスワード管理の不備	17	12
古いバージョン使用、パッチ未導入など	11	27
設定不備	10	6
不　明	35	85
その他（DoS など）	29	28
合計　（件）	**102**	**158**

図 2-6：2014 年不正アクセス被害原因

・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. 2014 年総括

2014 年 1 月～12 月の間「安心相談窓口」に寄せられた相談件数は 15,598 件でした。2013 年の 15,227 件から 371 件（約 2.4%）増加しました（図 3-1）。月毎の件数で見ると、毎月常に 1,000 件を越す相談が寄せられました（図 3-2）。

『ワンクリック請求』に関する相談は **3,301 件**（2013 年：3,287 件）とほぼ横這いだった一方、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 **790 件**（同 393 件）の相談があり、前年比でほぼ倍増しました。昨今のスマートフォン利用者の増加に伴い、ワンクリック請求の被害者も増加していると考えられます。

その他、金銭被害に関係する相談として**『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 **624 件**（同 889 件）、**『インターネットバンキング』**に関する相談が **158 件**（同 147 件）、**『ランサムウェア』**に関する相談が **35 件**（同 22 件）、それぞれ寄せられました。

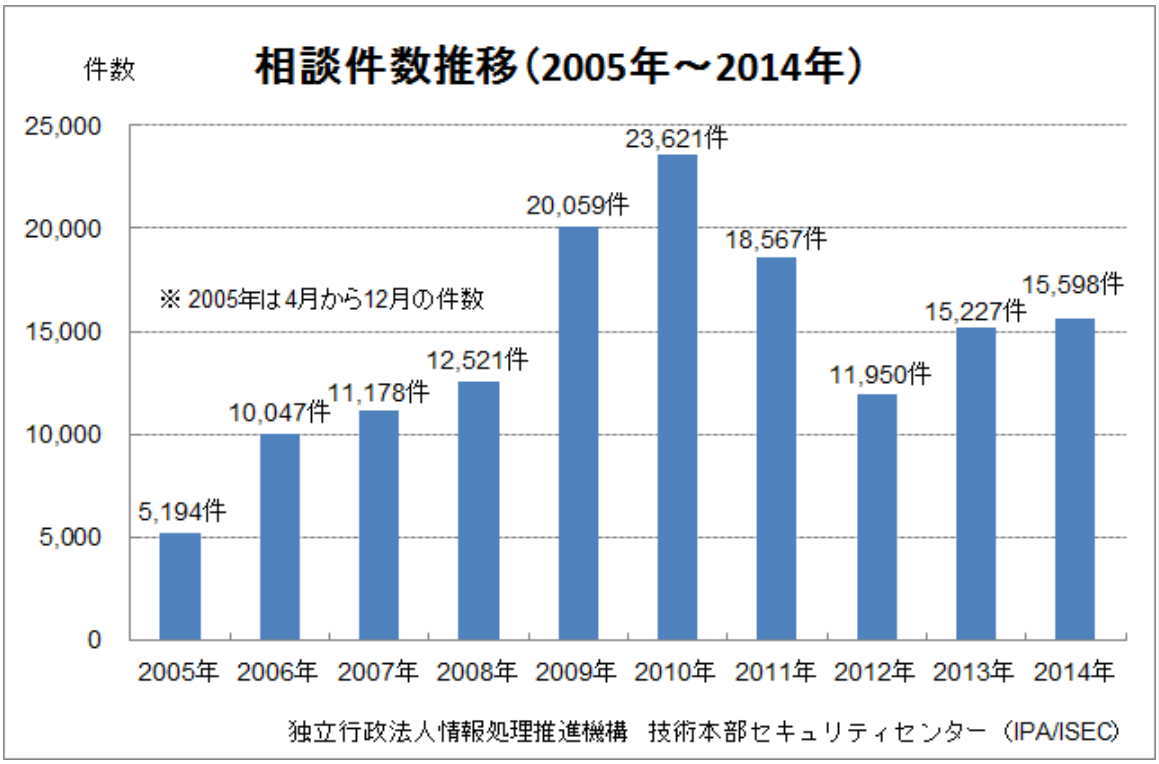


図 3-1：「安心相談窓口」における相談件数推移（2005 年～2014 年）

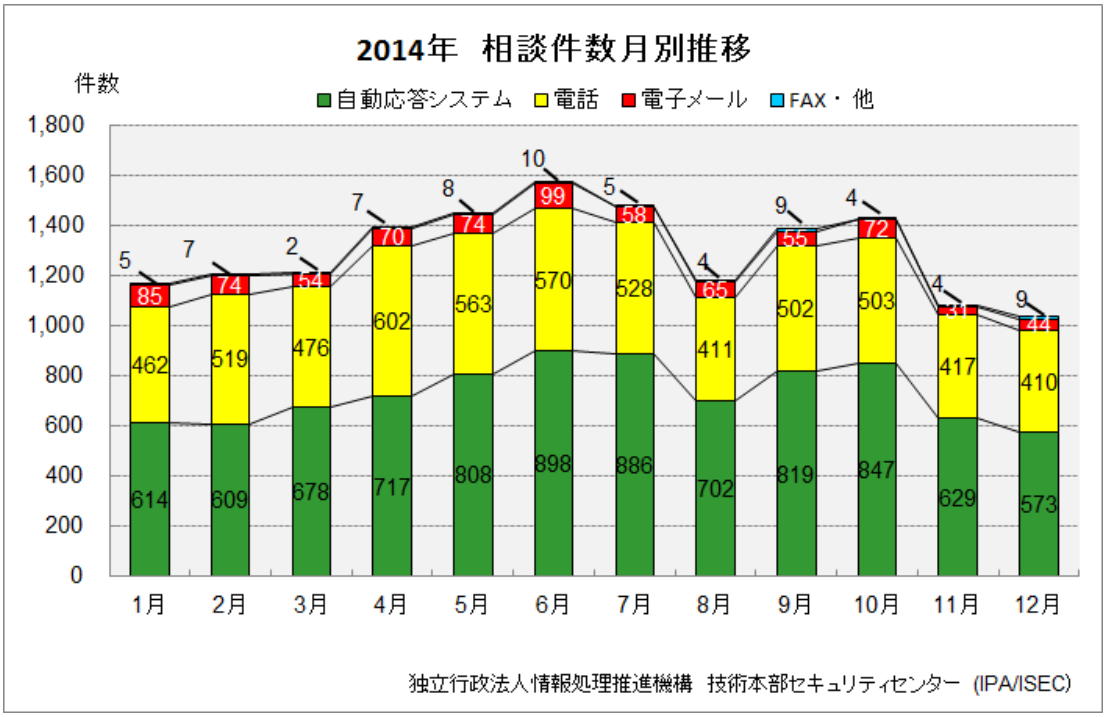


図 3-2：「安心相談窓口」における相談件数の推移

表 3-1：「安心相談窓口」における相談件数の推移（前掲 図 3-2 の詳細）

		2014 年											
		1 月	2 月	3 月	4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月	12 月
合計		15,598											
		1,166	1,209	1,210	1,396	1,453	1,577	1,477	1,182	1,385	1,426	1,081	1,036
	自動応答システム	614	609	678	717	808	898	886	702	819	847	629	573
	電話	462	519	476	602	563	570	528	411	502	503	417	410
	電子メール	85	74	54	70	74	99	58	65	55	72	31	44
	FAX・他	5	7	2	7	8	10	5	4	9	4	4	9

3-2. 相談事例

(i) ランサムウェアに感染してしまい、日本語の支払い請求文が表示される

相談	・ウェブサイトを閲覧している最中に突然、「パソコン内のファイルを暗号化した」という**日本語で書かれた警告画面**が現れた。 ・暗号化を解除してファイルを元に戻すためには、ビットコインという仮想通貨で15万円分の支払いが必要とのこと。 ・ビットコインでの支払い方法が分からないし、そもそも15万円もの大金を支払うつもりはない。暗号化されてしまったファイルはもう元に戻せないのか。
回答	ランサムウェアはパソコン内のファイルを暗号化し、ファイル復旧を条件に身代金（または罰金）の名目で金銭を要求します。**身代金を支払ったとしてもファイルが元に戻る保証はなく、たとえウイルスを駆除できたとしても、暗号化されたファイルは元に戻りません。** 普段から重要なファイルは定期的にバックアップすることを勧めます。またウイルスの感染被害に遭わないよう、セキュリティソフトの利用は当然ですが、OS（Windows、Mac OS など）や Java、Flash Player など、よく使用するプログラムを常に最新の状態にしてください。 【解説】ランサムウェアというウイルスに感染してしまったケースです。今まではイギリス警察など海外の組織を騙ったランサムウェアの相談がほとんどでしたが、**自然な日本語で書かれた警告文を伴うランサムウェアに関する相談が IPA に寄せられたのは今回が初めてです。**今後、日本語ランサムウェアによる被害が増加する事が懸念されます。

(ii) クレジットカード会社のウェブサイトにログインする時、カード番号等を入力させる見慣れない画面が現れた（ウイルス感染被害によるケース）

相談	・クレジットカードの残高を確認するために、クレジットカード会社のサイトにパソコンからログインしようとしたら、**カード番号と 3 桁のセキュリティコード**を入力させる普段見慣れない画面が現れた。 ・不審に思い、その時は何も入力しなかった。 ・試しに別のカード会社のサイトにログインを試みると、同様にカード番号等を入力させる画面が出てきた。 ・Windows の「システムの復元」機能でパソコンの状態を 3 日前に戻したら、その見慣れない画面は出てこなくなった。これでもうパソコンはいつも通り使ってもいいのか。
回答	**そのカード番号等を入力させる画面は、パソコンのウイルス感染が原因で表示される偽の画面です。**入力してしまうと第三者にカード情報が渡ってしまうため、そこで何も入力しなかったのは賢明な判断でした。 偽の画面は「システムの復元」を実施後に出てこなくなったため、偽画面を表示させるウイルスは削除されたと考えられますが、別のウイルスが侵入している可能性があるため、パソコンを一度初期化する事を勧めます。 **【解説】２０１４年はインターネットバンキングの不正送金を狙ってウイルス感染を試みる手口が横行しました。この事例のように金銭窃取を目的にカード会社のウェブサイトも標的になっていますので、注意が必要です。**

（iii） クレジットカード会社のサイトへのログイン時、普段は出ない画面が現れて、電話番号の一部と生年月を入力してしまった（問題が無かったケース）

相談	・クレジットカードの残高を確認するために、クレジットカード会社のウェブサイトにパソコンからログインしようとしたら、電話番号の一部と生年月を入力させる普段見慣れない画面が現れた。 ・不審に思い、その時は何も入力しなかった。 ・ログインしようとする時に追加で情報を聞かれる画面は危険だと聞いた。自分のパソコンはウイルスに感染しているのか。
回答	当窓口（安心相談窓口）で確認した結果、ご連絡いただいた画面は、カード会社が提供する正規の画面で、問題のないことがわかりました。 カード会社のウェブサイトに掲載されている情報によりますと、2014 年 10 月、当該サイトのログイン方法が変更されたようです。 今後も、ログイン時に不審に思った時には「これは大丈夫なのか」と一度立ち止まってみることは良いでしょう。なおウェブサービスにおけるログイン画面仕様は頻繁に変わる事も珍しくないので、**ログイン時に何か不審に思ったら、まず初めにサービス提供元の窓口に確認していただく事を勧めます。**

3-3. 主なトピックにおける相談状況

(i)『ワンクリック請求』に関する相談

2014 年は、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 3,301 件寄せられ、2013 年の 3,287 件と**ほぼ同数**でした（14 件、0.4%の増加）。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相談は 790 件で、2013 年の 393 件から**ほぼ倍増**しました（397 件、約 101%の増加）。

昨今のスマートフォン利用者の増加に伴い、興味本位でアダルトサイトなどを閲覧した結果、ワンクリック請求の被害に遭ってしまう利用者が増加していると考えられます。今後一層のスマートフォン普及に伴い、ワンクリック請求に関する被害と相談が増加することが懸念されます。

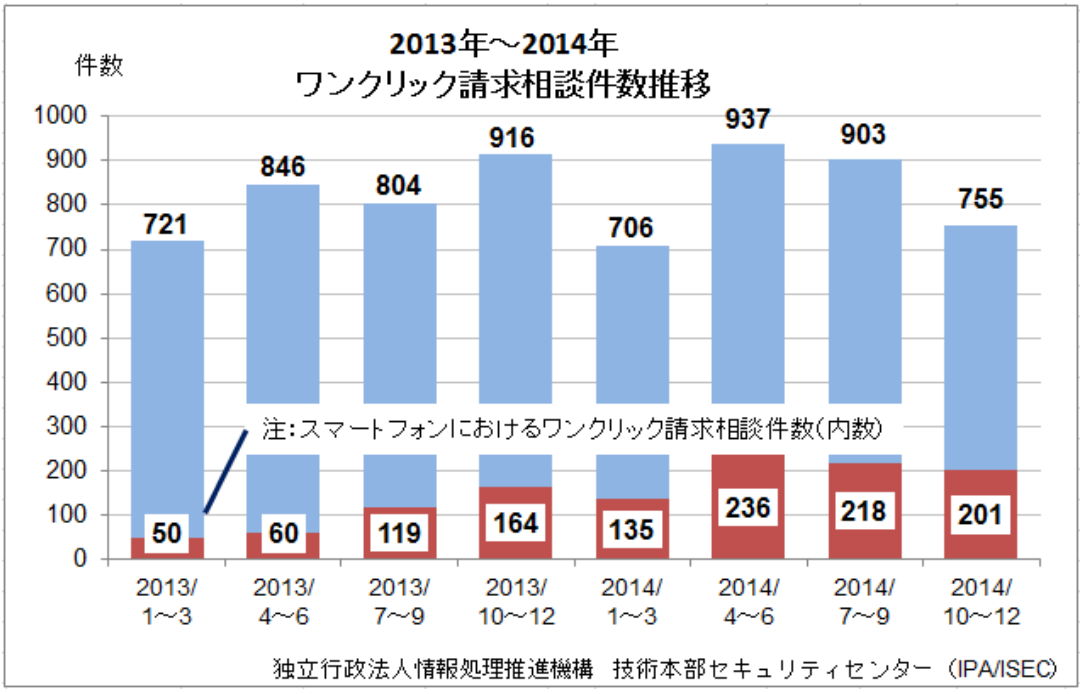


図 3-3：『ワンクリック請求』、スマートフォンにおける『ワンクリック請求』の相談件数推移

（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

2014 年は 624 件の相談が寄せられました。相談件数は 2013 年の 889 件から 265 件（約 30%）減少しました。

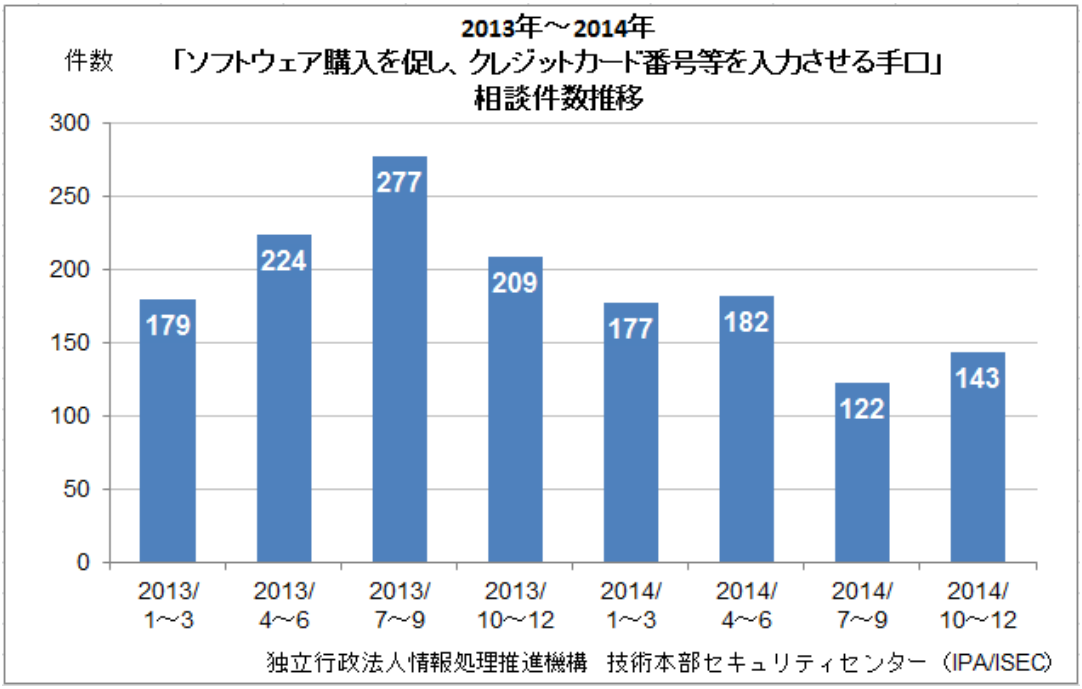


図 3-4：『ソフトウェア購入を促し、クレジットカード番号等を入力させる手口』相談件数推移

この手口は、“パソコンがウイルスに感染している”、“パソコンにエラーがある”、“ドライバーが古い”などパソコンに何か問題があるような警告画面を表示します。そして、その問題解決のためと称してソフト購入を促し、クレジットカード番号等を入力させようとする、金銭目的の手口です。

警告画面をパソコンに表示させるためには、何らかのプログラムがパソコンにインストールされていることが前提ですが、利用者にインストールさせる方法によって下記 2 タイプに大別されます。

タイプ 1

パソコンの脆弱性を悪用して、利用者の知らぬ間にパソコンに入り込むタイプ (*18)。利用者から見ると、ウェブサイト閲覧中に突然ウイルススキャンが始まったように見えます。

2013 年には「Smart Fortress」、「Live Security」、「System Progressive Protection」、「Disk Antivirus Professional」など、月替わりで新しい偽セキュリティソフトに関する相談が次々と寄せられる状況でしたが、2014 年に入ると下火になり、同年後半には 1 件相談が寄せられただけでした（図 3-5）。

金銭窃取のために悪用されるウイルスとしては、“偽セキュリティソフト”の他にも“ランサムウェア”、“Bancos”などがあり、感染パソコン 1 台からより多額の窃取が見込めるため (*19)、それらのウイルスや不正プログラムを使った手口に移行したと考えられます。

(*18) IPA ではこのタイプ 1 を“偽セキュリティソフト”と呼んでいる。

(*19) 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”の請求額は 3 万円～30 万円程度で、“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。

タイプ２

脆弱性が原因のウイルス感染ではなく、パソコン利用者自らクリックしてパソコンにインストールしてしまうタイプ。インストールに至るまでには以下のようなケースが存在します。

・「パソコンが故障寸前」「ドライバーが古い」など、パソコン利用者を驚かせるような広告を表示して、パソコン利用者にその表示された不具合を解消するためと称した対策ソフトをダウンロード、インストールさせるよう誘導します。
・ソフトウェアのインストール中に出てくる注意書きをよく読まずに進んだ結果、一緒に別のプログラムもインストールしてしまうケース。

タイプ２は年間を通じて相談が寄せられており、今後も被害と相談が継続すると推測されます（図 3-5）。

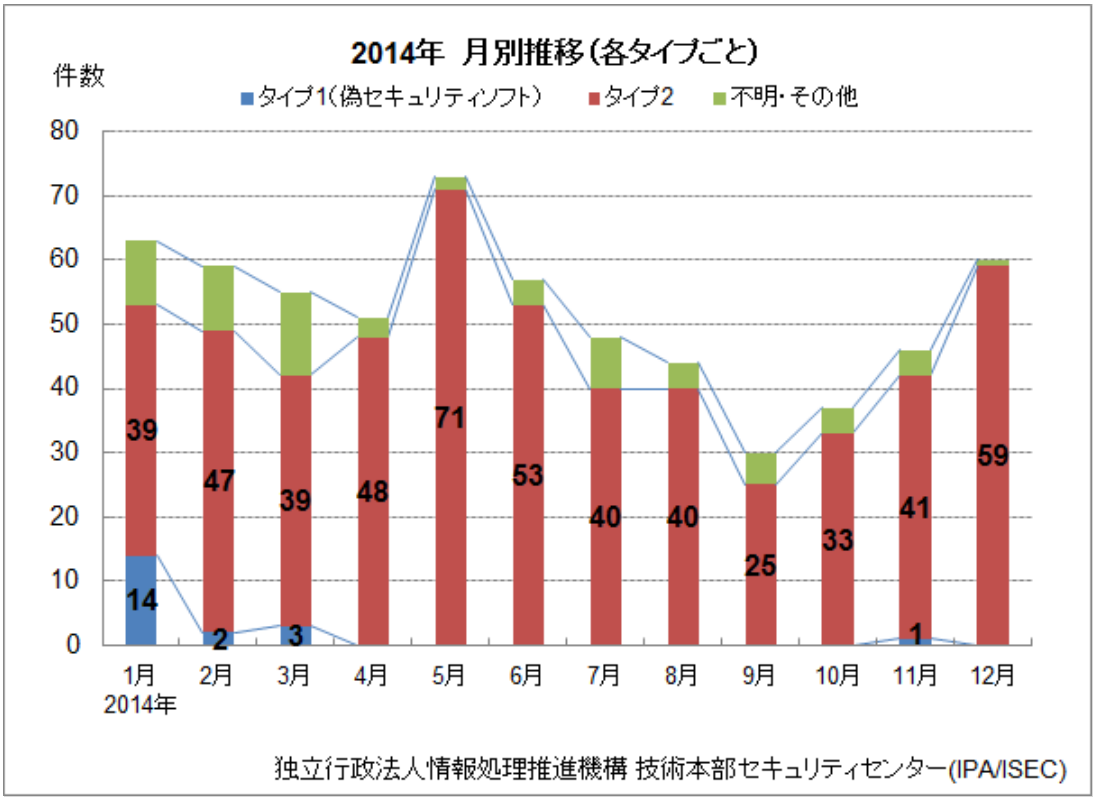


図 3-5：タイプごとの月別件数推移

（iii）『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、2014 年は 158 件寄せられました。2013 年の 147 件から 11 件（約 7.5%）増加しました。

年間件数は横這いですが、四半期ごとの推移を見ると大きく変動しています（図 3-6）。

2012 年後半には、パソコンにウイルスを感染させて、そのウイルスによって“乱数表”などの情報をすべて入力させる手口が出現しました。それに伴い IPA への相談も 2012 年 10 月から増加しました（図 3-6）。

それ以後相談が絶える事がありませんでしたが、2014 年 7 月以降相談が激減しました（図 3-6）。その理由として、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大作戦」[*20] が決行された事が挙げられます。“Bancos”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すもので、この取り組みにより“Bancos”感染パソコンが減少し、相談も減少したと考えられます。

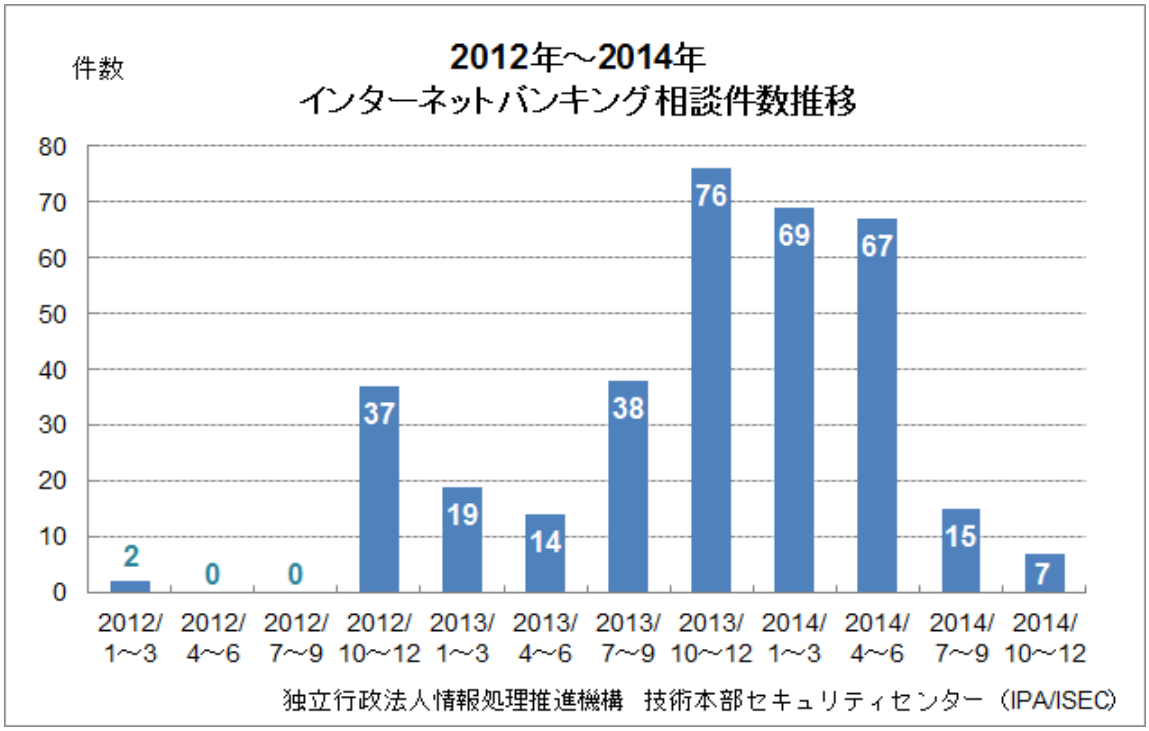


図 3-6：『インターネットバンキング』相談件数推移（四半期ごと）

[*20] 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～　https://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