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 3 四半期（7 月～9 月）］

本レポートでは、2015 年 7 月 1 日から 2015 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

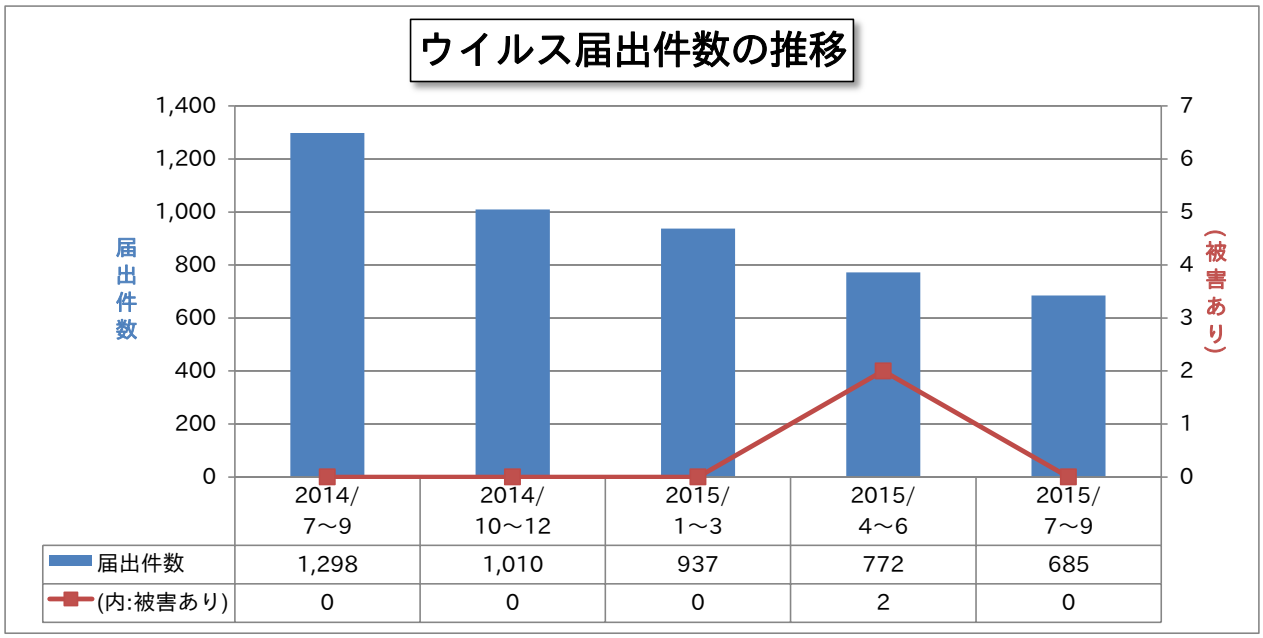
2015 年 10 月 23 日

目次

1. コンピュータウイルス届出状況

1-1. ウイルス届出件数

今四半期（2015 年 7 月～9 月）のウイルス届出件数は 685 件で、ウイルス感染被害があった届出はありませんでした。

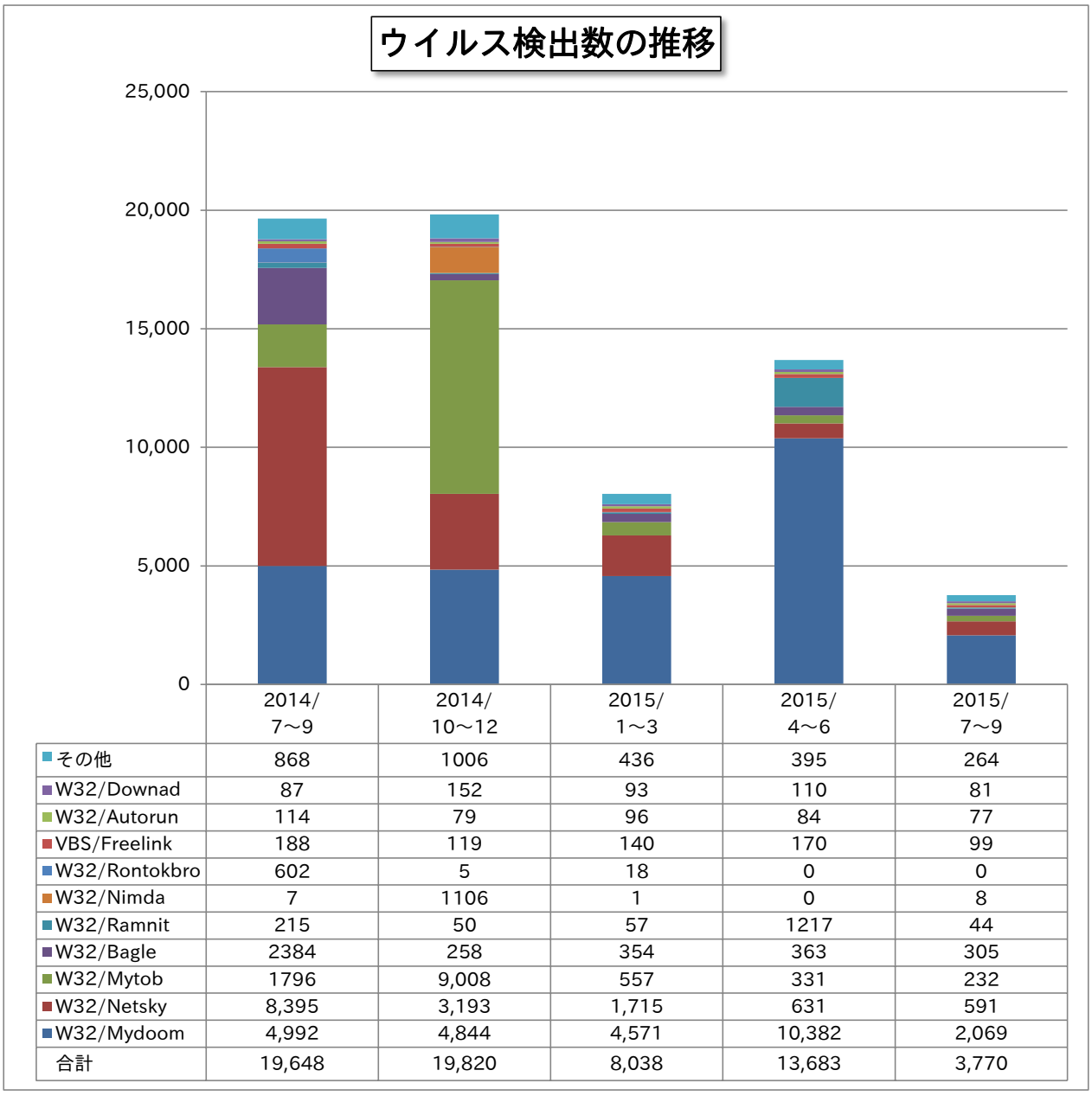


	2014/ 7～9	2014/ 10～12	2015/ 1～3	2015/ 4～6	2015/ 7～9
届出件数	1,298	1,010	937	772	685
(内:被害あり)	0	0	0	2	0

図 1-1：ウイルス届出件数の推移

1-2. ウイルス検出数

今四半期のウイルス検出数 (*1) は 3,770 個でした。今四半期に最も多く検出されたウイルスは W32/Mydoom でしたが、前四半期に比べ約 19.9%と大きく減少しました。また、全体に占める割合は大きくありませんが、前四半期が約 8.9%だった W32/Ramnit が今四半期は約 1.2%と減少しました。W32/Netsky は、2014 年第 4 四半期に検出数が大きく減少して以降、減少傾向が続いています。



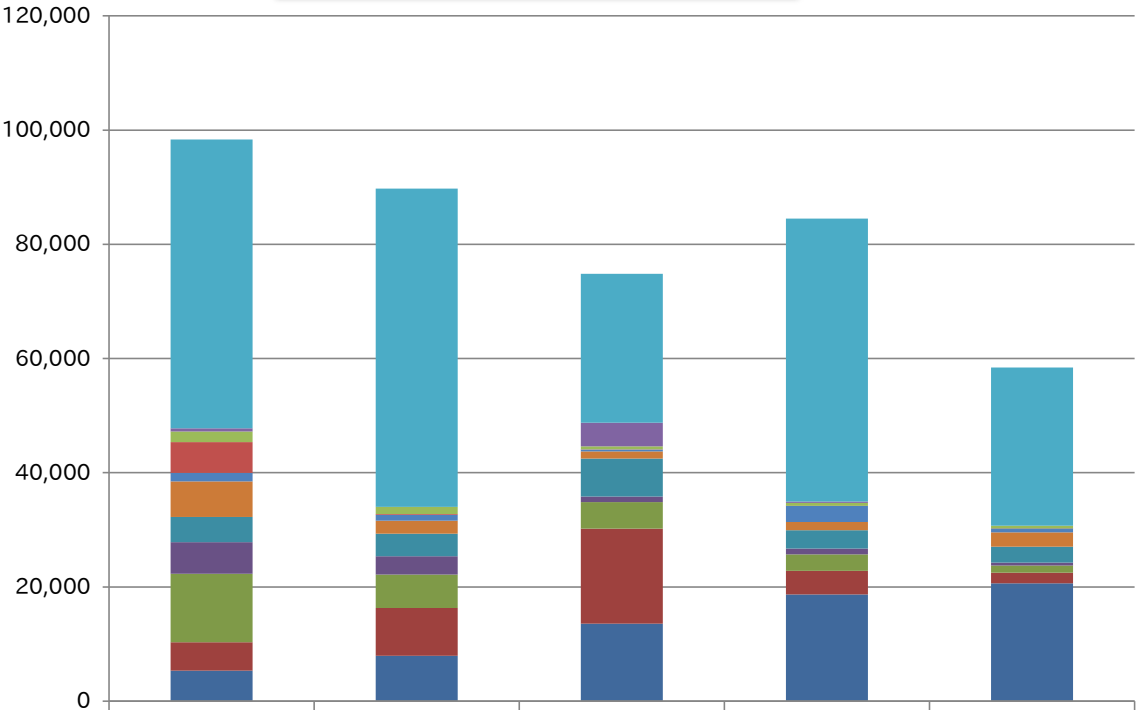
	2014/ 7～9	2014/ 10～12	2015/ 1～3	2015/ 4～6	2015/ 7～9
その他	868	1006	436	395	264
W32/Downad	87	152	93	110	81
W32/Autorun	114	79	96	84	77
VBS/Freelink	188	119	140	170	99
W32/Rontokbro	602	5	18	0	0
W32/Nimda	7	1106	1	0	8
W32/Ramnit	215	50	57	1217	44
W32/Bagle	2384	258	354	363	305
W32/Mytob	1796	9,008	557	331	232
W32/Netsky	8,395	3,193	1,715	631	591
W32/Mydoom	4,992	4,844	4,571	10,382	2,069
合計	19,648	19,820	8,038	13,683	3,770

図 1-2：ウイルス検出数の推移

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

1-3. 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 (*2) は 58,412 個でした。今四半期に最も多く検出された不正プログラムは Downloader でした。検出数は全体の 35.4%を占め、前四半期の約 10.7%増となっています。Backdoor は今四半期は大幅に減少し前期の約 55.2%減となりました。Redirect は 2014 年第 4 四半期から検出数が減少傾向が続いています。Trojan/Horse も今四半期は減少し、前期の 76.4%減となりました。



	2014/ 7～9	2014/ 10～12	2015/ 1～3	2015/ 4～6	2015/ 7～9
その他	50,549	55,743	26,085	49,545	27,673
Obfuscated	572	0	4,098	220	0
Dropper	1,850	1,247	523	503	486
Webkit	5,405	154	47	17	14
Trojan/Horse	1,509	1,033	345	2,812	665
Fakeav	6,206	2,284	1,261	1,476	2,526
Adware	4,416	3,961	6,638	3,206	2,801
Bancos	5,540	3,203	979	1,012	488
Redirect	11,997	5,851	4,632	2,890	1,255
Backdoor	4,987	8,355	16,637	4,140	1,854
Downloader	5,314	7,941	13,577	18,662	20,650
合計	98,345	89,772	74,822	84,483	58,412

図 1-3：不正プログラム検出数の推移

(*2) 不正プログラム検出数：届出られた「ウイルス」および「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。

1-4. 2015 年第 3 四半期の検出ウイルス

今四半期に届出されたウイルスの種類は 48 種類、検出数は Windows/DOS ウイルス 3,601 個、スクリプトウイルス及びマクロウイルス 144 個、携帯端末ウイルス 19 個、OSS（Open Source Software）/Linux・BSD を含むウイルス 6 個でした。

表 1-1：2015 年第 3 四半期の検出ウイルス

i) Windows/DOS ウイルス	検出数
W32/Mydoom	2,069
W32/Netsky	591
W32/Bagle	305
W32/Mytob	232
W32/Klez	90
W32/Downad	81
W32/Autorun	77
W32/Ramnit	44
W32/Fakerecy	17
W32/Fujacks	16
W32/Antinny	12
W32/Mumu	11
W32/Nimda	8
W32/Sality	6
W32/Hybris	5
W32/IRCbot	5
W32/Gammima	4
W32/Sober	4
W32/Virut	4
W32/Selex	3
W32/Bacterra	2
W32/Looked	2
W32/Lovgate	2
W32/Nuwar	2
W32/Tufik	2
Cascade	1
Perl/Lexac	1
W32/Cryptolocker	1
W32/MSBlaster	1
W32/Parite	1
W32/Stration	1
W32/Wapomi	1
小計　(32 種類)	3,601

スクリプトウイルス	検出数
VBS/Freelink	99
VBS/DUNIHI	1
VBS/SST	1
VBS/Solow	1
小計　(4 種類)	102

マクロウイルス	検出数
XM/Laroux	22
XM/VCX.A	6
X97M/Divi	5
O97M/Darksnow	2
W97M/Melissa	2
W97M/X97M/Toraja	2
W97M/Marker	1
X97M/Barisada	1
XM/Mailcab	1
小計　(9 種類)	42

ii) 携帯端末ウイルス	検出数
AndroidOS/Lotoor	17
AndroidOS/Adware	2
小計　(2 種類)	19

iii) Macintosh	検出数
なし	

iv) OSS(Open Source Software) Linux・BSD を含む	検出数
Linux/Adore	6
小計　(1 種類)	6

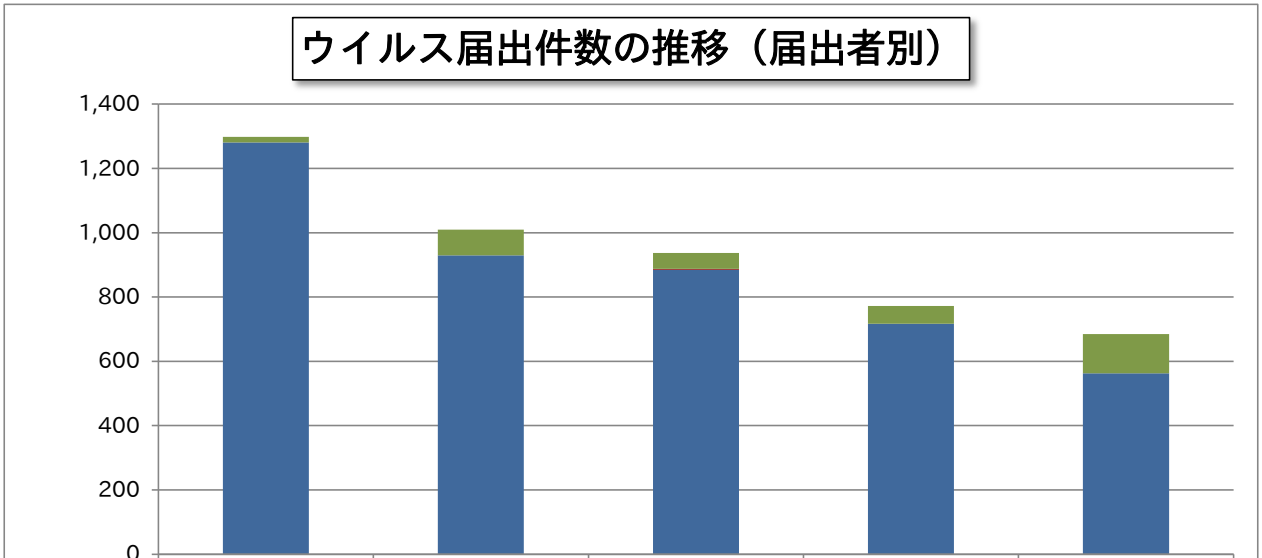
（参考）
・Windows/DOS ウイルス … Windows、MS-DOS 環境下で動作するウイルス。
・マクロウイルス … Microsoft Word や Microsoft Excel などのマクロ機能を悪用するウイルス。
・スクリプトウイルス … 機械語への変換作業を省略して実行できるようにした簡易プログラムで記述されたウイルス。
・携帯端末ウイルス … 携帯電話やタブレットなどの環境下で動作するウイルス。

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）

1-5. ウイルス届出者

今四半期の届出者は、過去の傾向と同じく一般法人がほとんどで、全体の約 82.2%を占めました。

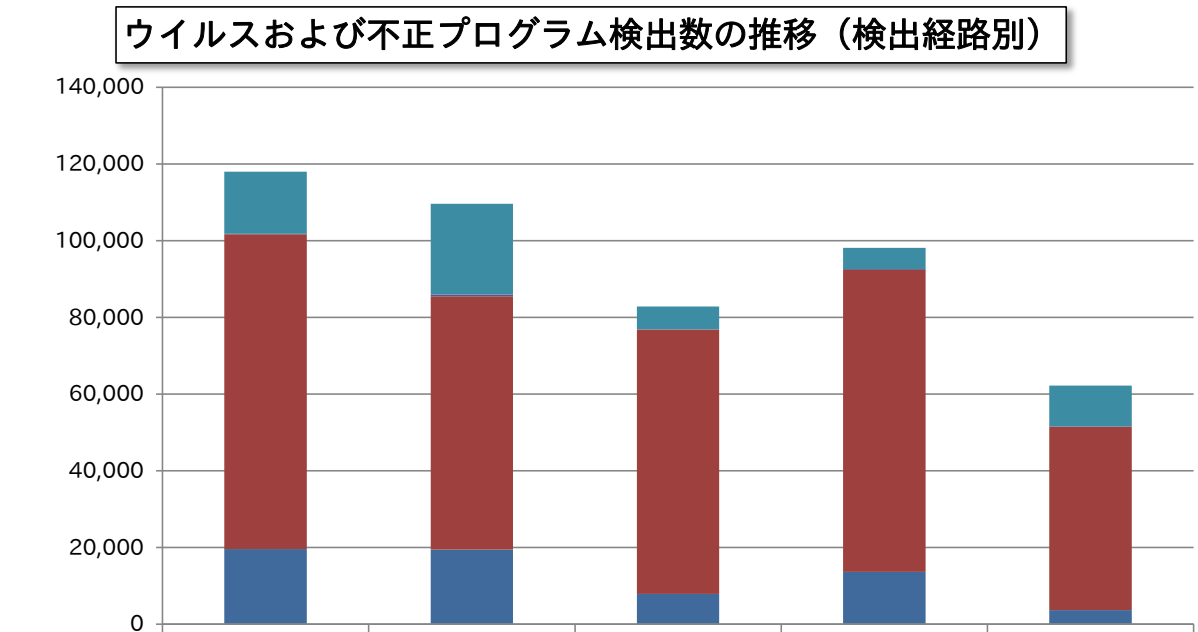


	2014/7～9	2014/10～12	2015/1～3	2015/4～6	2015/7～9
教育機関	17	80	49	55	122
個人	0	0	1	0	0
一般法人	1,281	930	887	717	563
合計	1,298	1,010	937	772	685

図 1-4：ウイルス届出件数の推移（届出者別）

1-6. ウイルスおよび不正プログラムの検出経路

今四半期のウイルスおよび不正プログラムの検出経路については、過去の傾向と同じく、「ダウンロードファイル」が最も多く全体の約８割で、次いで「不明・その他」の約 17.1%でした。



	2014/ 7～9	2014/ 10～12	2015/ 1～3	2015/ 4～6	2015/ 7～9
不明・その他	16,201	23,656	5,963	5,603	10,646
ネットワーク	107	491	109	154	112
外部記憶媒体	0	3	0	4	0
ﾀﾞｳﾝﾛｰﾄﾞﾌｧｲﾙ	82,104	65,973	68,933	78,806	47,763
メール	19,581	19,469	7,855	13,599	3,661
合計	117,993	109,592	82,860	98,166	62,182

図 1-5：ウイルスおよび不正プログラム検出数の推移（検出経路別）

・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。

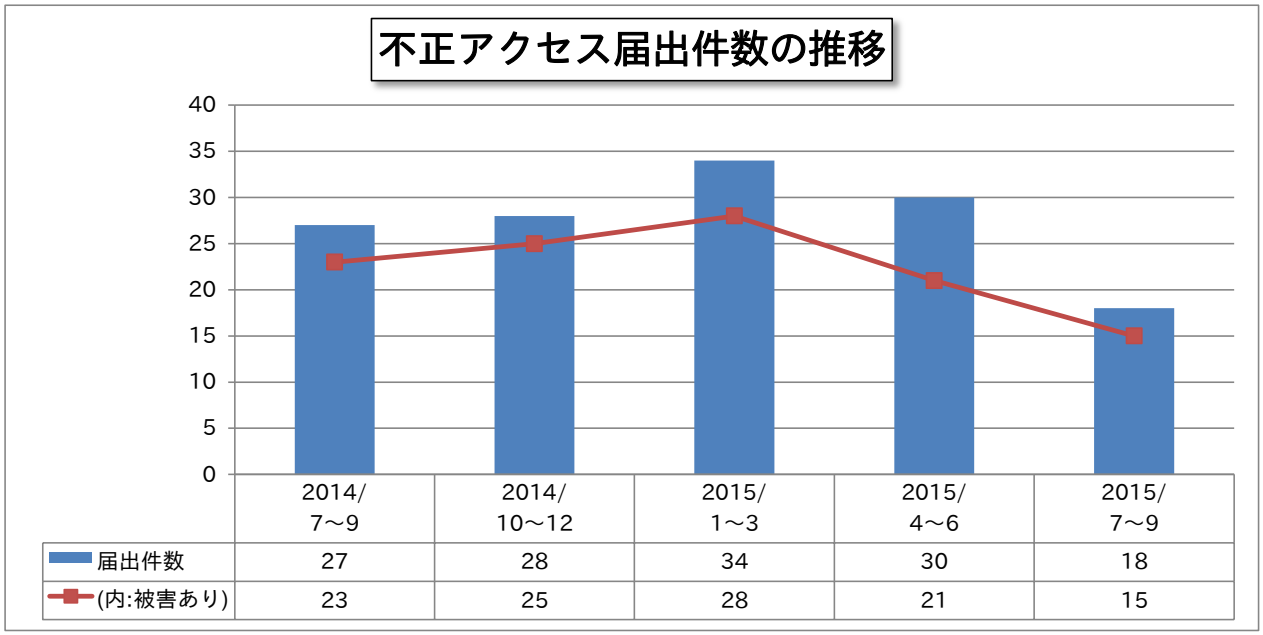
IPA では、個別に届出者への対応を行っていますが、同時に受理した届出等を基に、コンピュータウイルス対策を検討しています。また受理した届出は、届出者のプライバシーを侵害することがないように配慮した上で、被害等の状況を分析し、検討結果を定期的に公表しています。

○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. 不正アクセス届出件数

今四半期の届出件数は 18 件で、そのうち被害があったのは 15 件でした。

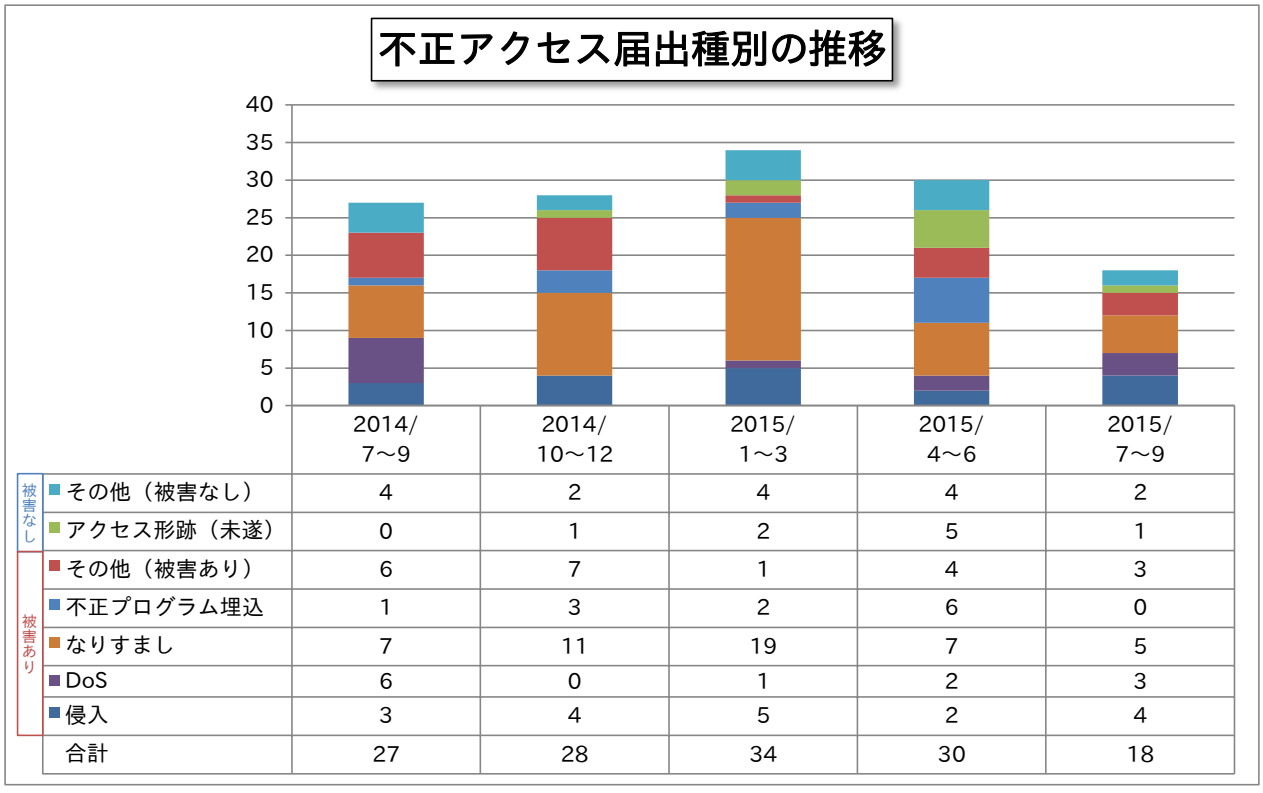


	2014/7～9	2014/10～12	2015/1～3	2015/4～6	2015/7～9
届出件数	27	28	34	30	18
(内:被害あり)	23	25	28	21	15

図 2-1：不正アクセス届出件数の推移

2-2. 不正アクセス届出種別

届出の種別としては「なりすまし」が 5 件、「侵入」が 4 件、「DoS」が 3 件、「その他（被害あり）」が 3 件でした。前四半期と比較して「侵入」が全体の約 6.7%から約 22.2%に増加しました。また「不正プログラム埋込」の届出は 0 件でした。

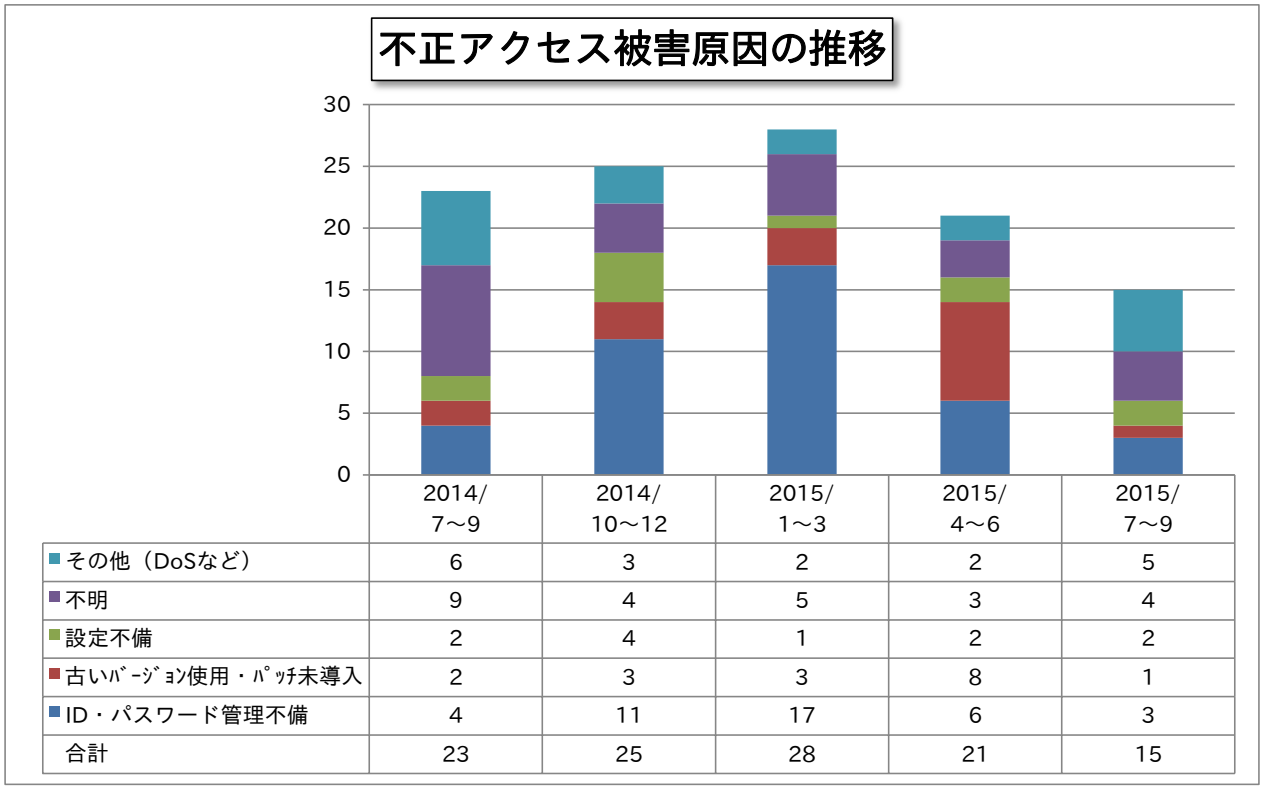


		2014/7～9	2014/10～12	2015/1～3	2015/4～6	2015/7～9
被害なし	その他（被害なし）	4	2	4	4	2
被害なし	アクセス形跡（未遂）	0	1	2	5	1
被害あり	その他（被害あり）	6	7	1	4	3
被害あり	不正プログラム埋込	1	3	2	6	0
被害あり	なりすまし	7	11	19	7	5
被害あり	DoS	6	0	1	2	3
被害あり	侵入	3	4	5	2	4
	合計	27	28	34	30	18

図 2-2：不正アクセス届出種別の推移

2-3. 不正アクセス被害原因

被害があった届出のうち、原因が判明しているものは「ID・パスワード管理不備」が 3 件、「設定不備」が 2 件、「古いバージョン使用・パッチ未導入」が 1 件等でした。前四半期と比較して「古いバージョン使用・パッチ未導入」は全体の約 38.1%から約 6.7%に減少し、「ID・パスワード管理不備」も全体の約 28.6%から 20%に減少しました。

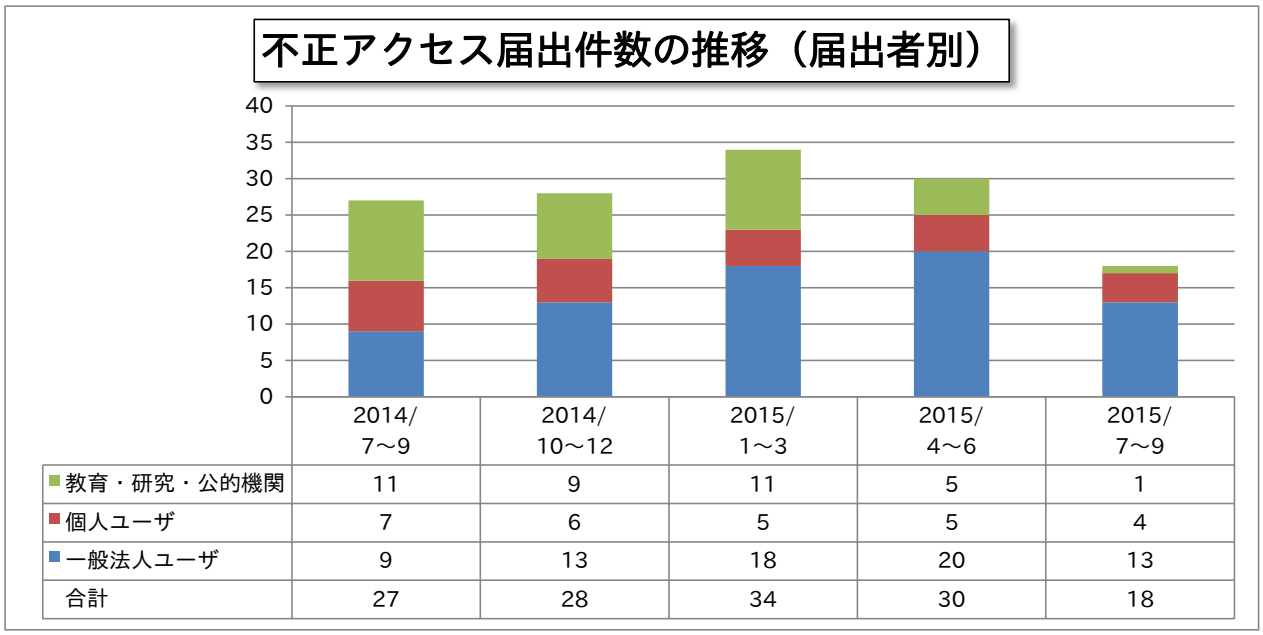


	2014/ 7～9	2014/ 10～12	2015/ 1～3	2015/ 4～6	2015/ 7～9
その他（DoSなど）	6	3	2	2	5
不明	9	4	5	3	4
設定不備	2	4	1	2	2
古いﾊﾞｰｼﾞｮﾝ使用・ﾊﾟｯﾁ未導入	2	3	3	8	1
ID・パスワード管理不備	4	11	17	6	3
合計	23	25	28	21	15

図 2-3：不正アクセス被害原因の推移

2-4. 不正アクセス届出者

届出者別の届出件数は、「一般法人ユーザ」が 13 件、「個人ユーザ」が 4 件、「教育・研究・公的機関」が 1 件でした。



	2014/ 7～9	2014/ 10～12	2015/ 1～3	2015/ 4～6	2015/ 7～9
教育・研究・公的機関	11	9	11	5	1
個人ユーザ	7	6	5	5	4
一般法人ユーザ	9	13	18	20	13
合計	27	28	34	30	18

図 2-4：不正アクセス届出件数の推移（届出者別）

2-5. 不正アクセス被害事例

今四半期に届出のあった不正アクセス被害には、下記のような事例がありました。

（i）WordPress の脆弱性を悪用されてウェブコンテンツを書き換えられた。

被害の概要	・自社のウェブサイトにアクセスしたところ、社内で設定しているフィルタリング制限によって警告が表示された。 ・原因を調べてみるとウェブサーバが改ざんされていることが確認できたため、被害拡大防止および調査のために運用を停止した。 ・調査の結果、自社サイトにアクセスしたユーザを別サイトに誘導してマルウェアに感染させることが目的と考えられる改ざんの痕跡が見つかった。 ・WordPress の脆弱性を悪用され、ウェブサーバに侵入、改ざんされたと推測される。
解説・対策	WordPress の脆弱性を悪用されたウェブ改ざんの被害に遭ってしまった事例です。 ウェブ改ざんによってアクセスしたユーザをマルウェア感染させるような不正プログラムを埋め込まれてしまいました。しかし、この不正プログラムは実際には正常に動作することはなかったようで、結果的にそれ以上の被害の拡大は免れました。 今回の事例のように、ウェブ改ざんの内容によっては改ざんの被害者であると同時に、ウェブサイトにアクセスしたユーザに被害を及ぼす加害者となってしまう可能性もあります。 ウェブサーバの運用管理にあたっては、脆弱性を悪用した攻撃への対策として OS を含めインストールしているソフトウェアについて、適時バージョンアップやセキュリティパッチを適用して脆弱性を解消する必要があります。そのため、インストールしているソフトウェアの脆弱性に関する情報を収集すること、バージョンアップが必要となる際には即時対応できる体制を整えておくことが望まれます。

・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。

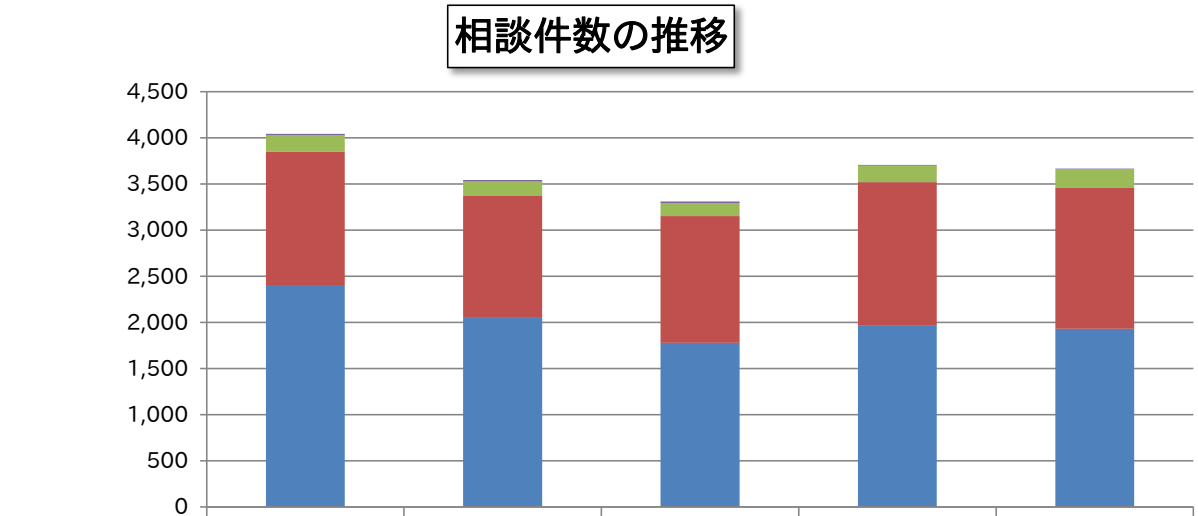
IPA では、個別に届出者への対応を行っていますが、同時に受理した届出等を基に、コンピュータ不正アクセス対策を検討しています。また受理した届出は、届出者のプライバシーを侵害することがないように配慮した上で、被害等の状況を分析し、検討結果を定期的に公表しています。

○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. 情報セキュリティ安心相談窓口の相談状況

3-1. 相談件数

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前四半期から約 1.1%減の 3,668 件でした。そのうち、相談員による対応件数は 1,735 件でした。



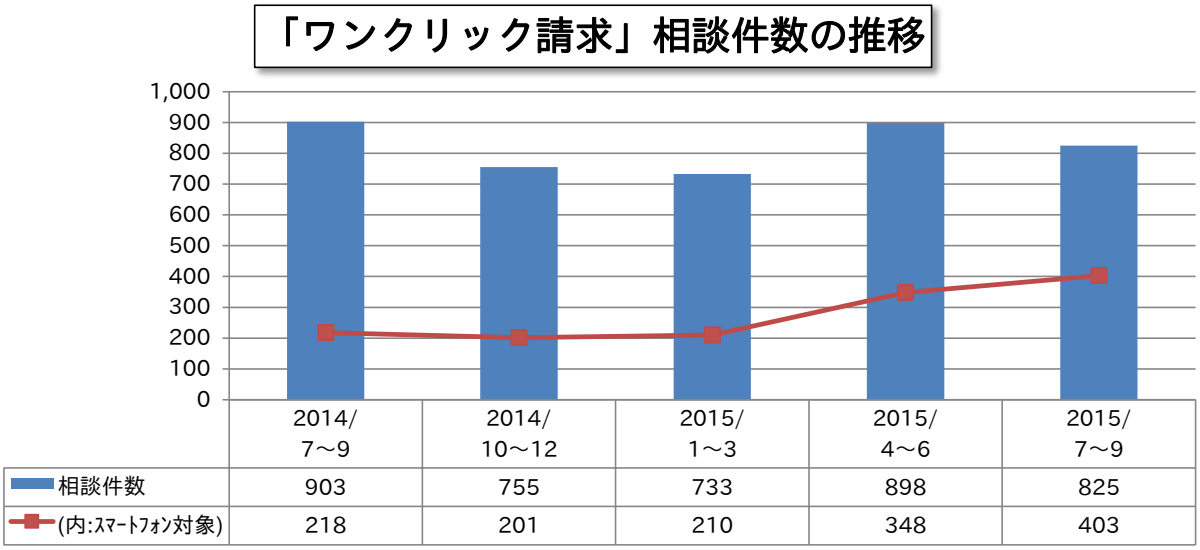
	2014/ 7～9	2014/ 10～12	2015/ 1～3	2015/ 4～6	2015/ 7～9
FAX・その他	18	17	18	7	7
電子メール	178	147	138	180	203
電話	1,441	1,330	1,376	1,558	1,525
自動応答システム	2,407	2,049	1,779	1,963	1,933
合計	4,044	3,543	3,311	3,708	3,668

図 3-1：相談件数の推移

3-2. 主なトピックの相談件数

(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 825 件寄せられました。同相談のうち、スマートフォンを対象にした相談は前四半期から約 15.8%増の 403 件で過去最多でした。



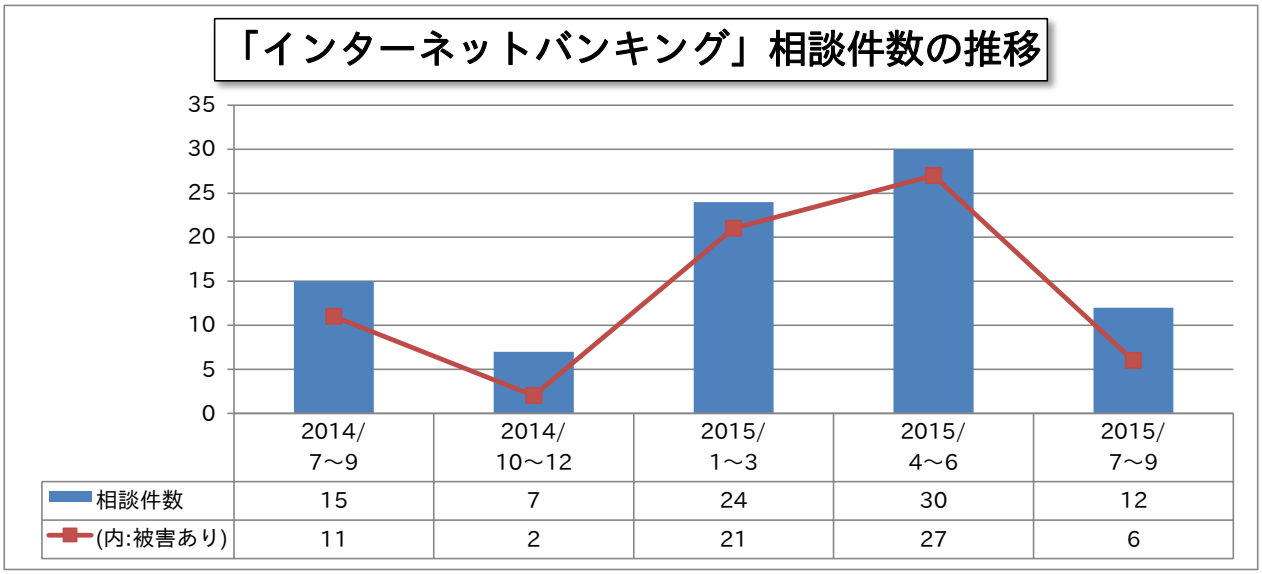
	2014/ 7～9	2014/ 10～12	2015/ 1～3	2015/ 4～6	2015/ 7～9
相談件数	903	755	733	898	825
(内:ｽﾏｰﾄﾌｫﾝ対象)	218	201	210	348	403

図 3-2：「ワンクリック請求」相談件数の推移

(ii) 「インターネットバンキング」に関する相談

今四半期は「インターネットバンキング」に関する相談が 12 件寄せられました。同相談のうち、インターネットバンキングを狙うウイルスに感染していたものは 6 件でした。

なお月単位では、2015 年 9 月の相談件数が 0 件でした。「インターネットバンキング」に関する相談が 0 件だったのは、2012 年 9 月以来 36 か月ぶりの事です。

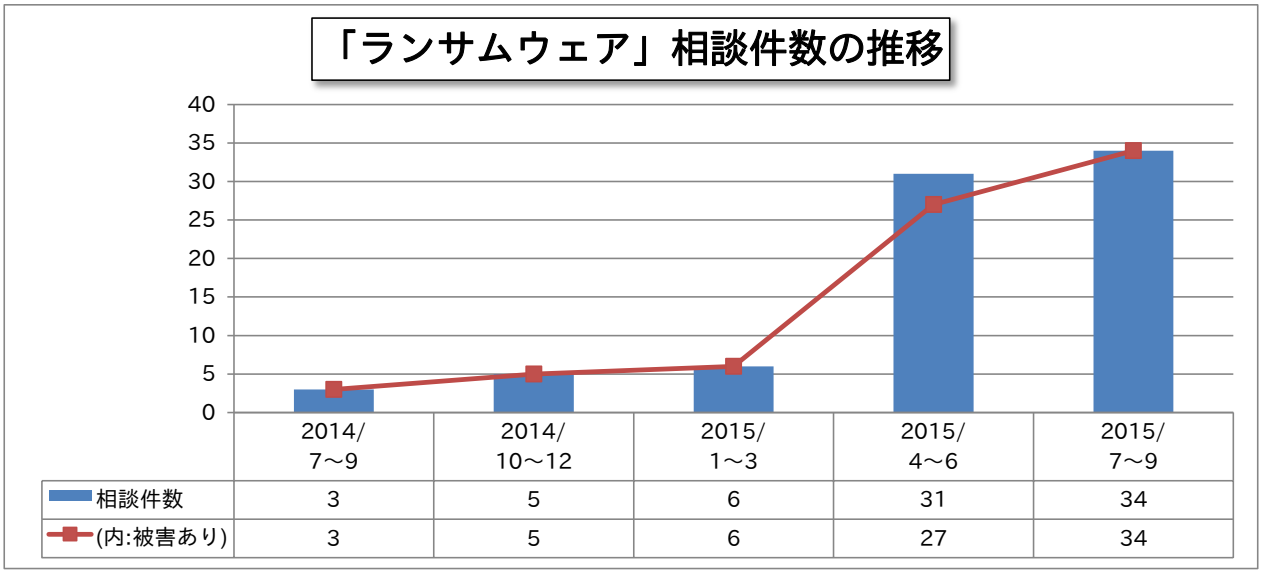


	2014/ 7～9	2014/ 10～12	2015/ 1～3	2015/ 4～6	2015/ 7～9
相談件数	15	7	24	30	12
(内:被害あり)	11	2	21	27	6

図 3-3：「インターネットバンキング」相談件数の推移

(iii) 「ランサムウェア」に関する相談

今四半期は「ランサムウェア」に関する相談が前四半期から微増して 34 件寄せられました。そのすべての相談で実際にランサムウェアに感染していました。



	2014/ 7～9	2014/ 10～12	2015/ 1～3	2015/ 4～6	2015/ 7～9
相談件数	3	5	6	31	34
(内:被害あり)	3	5	6	27	34

図 3-4：「ランサムウェア」相談件数の推移

3-3. 相談事例

今四半期の相談には、下記のような事例がありました。

（i） iPhone で、突然「iPhone 当選おめでとう」という内容のページが表示された。

相談の概要	・iPhone でインターネットを閲覧中、突然「iPhone 当選おめでとうございます」という内容のページが表示された。 ・アンケートに回答すると iPhone 6 がたった 1 ドルで買えるとの事だったので、アンケートに回答し、その後住所、氏名、メールアドレス、クレジットカード番号を入力した。 ・この事を友人に自慢しようとしたら、フィッシングの可能性を指摘された。どうしたら良いか。
回答	IPA にも類似の相談が多く寄せられています。本件もご友人の忠告の通り、フィッシングの可能性が高いと考えられます。 別の相談者のケースでは、クレジットカード情報を入力した結果、後日、動画コンテンツ名義で 6,000 円請求された、という事例もあります。 一度入力してしまった情報（住所、氏名、メールアドレス）は取り返す事ができませんが、クレジットカード利用の停止をする事で金銭被害を防ぐ事ができます。まずはクレジットカード会社に連絡して、カード停止の依頼をしてください。 今回は「iPhone 当選」を騙ったフィッシングでしたが、他にも「Apple Watch 当選」や「Apple の 1 日 CEO 権が当選」など、Apple 製品の人気に便乗していると考えられるフィッシングサイトの存在を IPA では確認しています。 うまい話を鵜呑みにせず、安易に入力をしないよう注意してください。 （ご参考） 「iPhone 人気に便乗していると考えられる手口にご注意を」 https://www.ipa.go.jp/security/txt/2015/09outline.html