

# 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 4 四半期 (10 月～12 月)]

本レポートでは、2015 年 10 月 1 日から 2015 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。

## 目次

1. コンピュータウイルス届出状況 .....	- 1 -
1-1. 2015 年総括 .....	- 1 -
1-2. ウイルス届出件数 .....	- 2 -
1-3. 不正プログラム検出数 .....	- 3 -
1-4. ウイルス検出数 .....	- 4 -
1-5. 2015 年第 4 四半期の検出ウイルスの種類 .....	- 5 -
1-6. ウイルス届出者 .....	- 6 -
1-7. ウイルスおよび不正プログラムの検出経路 .....	- 7 -
2. コンピュータ不正アクセス届出状況 .....	- 8 -
2-1. 2015 年総括 .....	- 8 -
2-2. 不正アクセス届出件数 .....	- 9 -
2-3. 不正アクセス届出種別 .....	- 9 -
2-4. 不正アクセス被害原因 .....	- 10 -
2-5. 不正アクセス届出者 .....	- 10 -
2-6. 不正アクセス被害事例 .....	- 11 -
3. 情報セキュリティ安心相談窓口の相談状況 .....	- 12 -
3-1. 2015 年総括 .....	- 12 -
3-2. 相談件数 .....	- 13 -
3-3. 主な手口における相談員の対応件数 .....	- 13 -
3-4. 相談事例 .....	- 15 -

# 1. コンピュータウイルス届出状況

## 1-1. 2015 年総括

2015 年に寄せられたウイルス届出件数は、前年の 5,014 件より 2,056 件（約 41.0%）少ない 2,958 件となりました。

また、2015 年に寄せられたウイルスの検出数は、前年の 83,028 個より 55,457 個（約 66.8%）少ない 27,571 個、不正プログラム検出数は前年の 380,625 個より 42,889 個（約 11.3%）少ない 337,736 個でした。いずれにおいても減少傾向となっています。

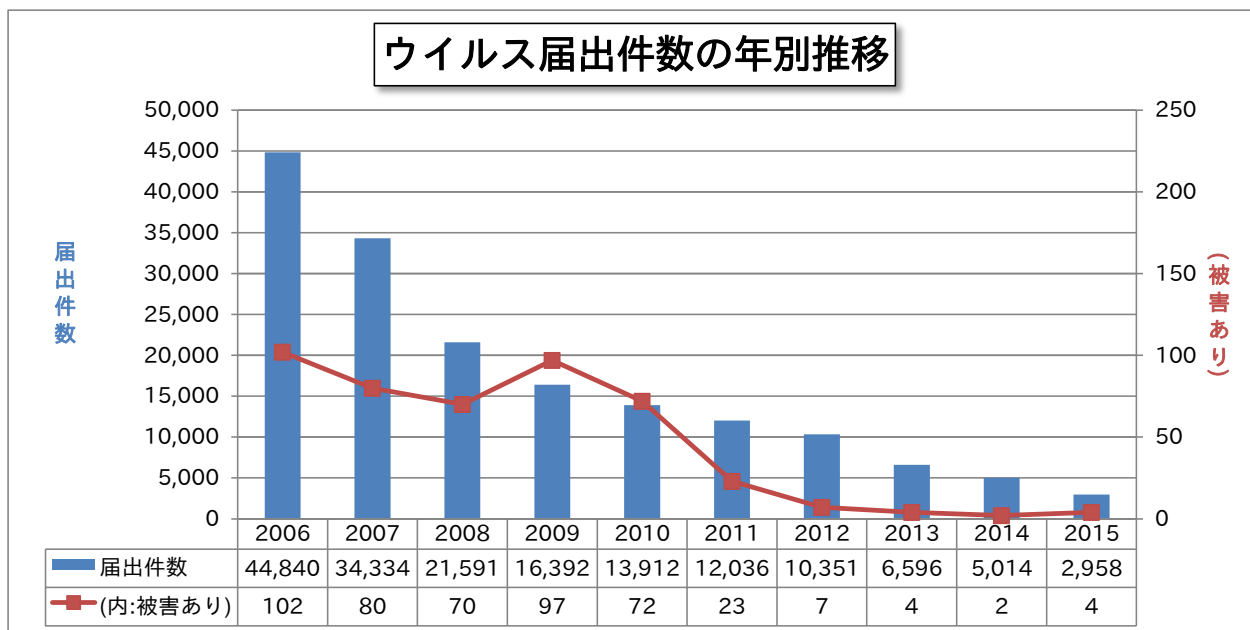


図 1-1：ウイルス届出件数の年別推移

## 1-2. ウイルス届出件数

今四半期（2015年10月～12月）のウイルス届出件数は564件で、ウイルス感染被害があった届出は2件でした。

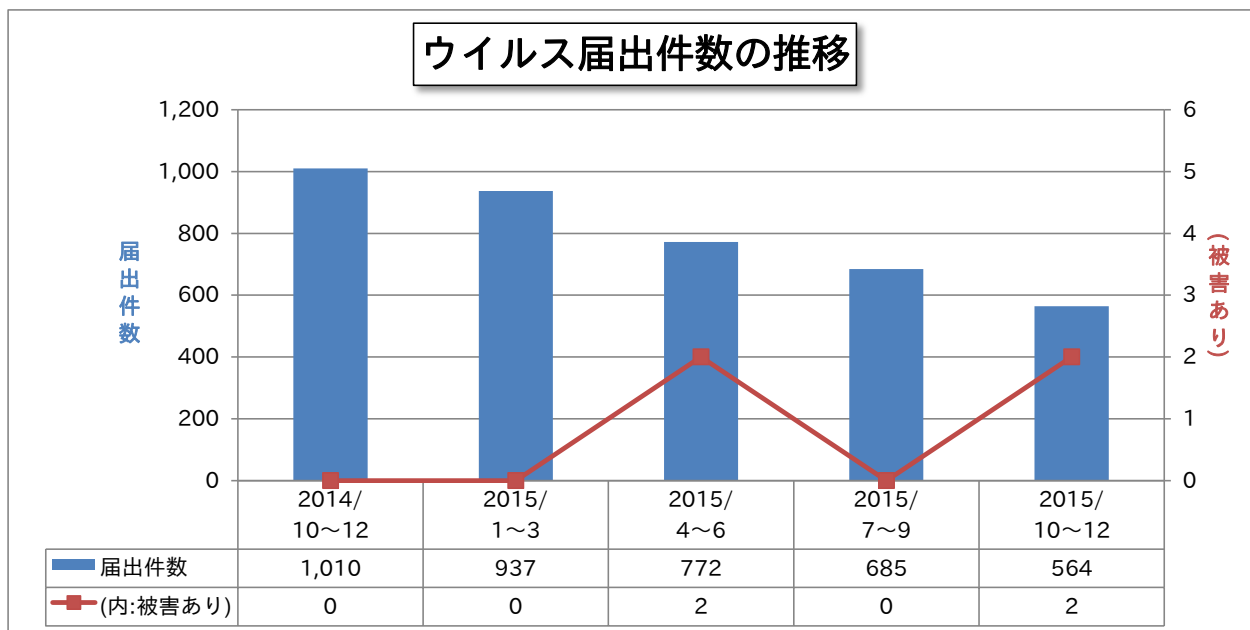


図 1-2：ウイルス届出件数の推移

### 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<sup>(\*)</sup>は120,019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。検出数は全体の約48.3%を占め、前四半期の20,650個に比べ約2.8倍となる57,932個となっています。また、今四半期に最も検出数増加の割合が多かったのはBancosで、前四半期の488個に比べ約14.1倍の6,903個となっています。Backdoorは2015年第2四半期から検出数の減少傾向が続いています。

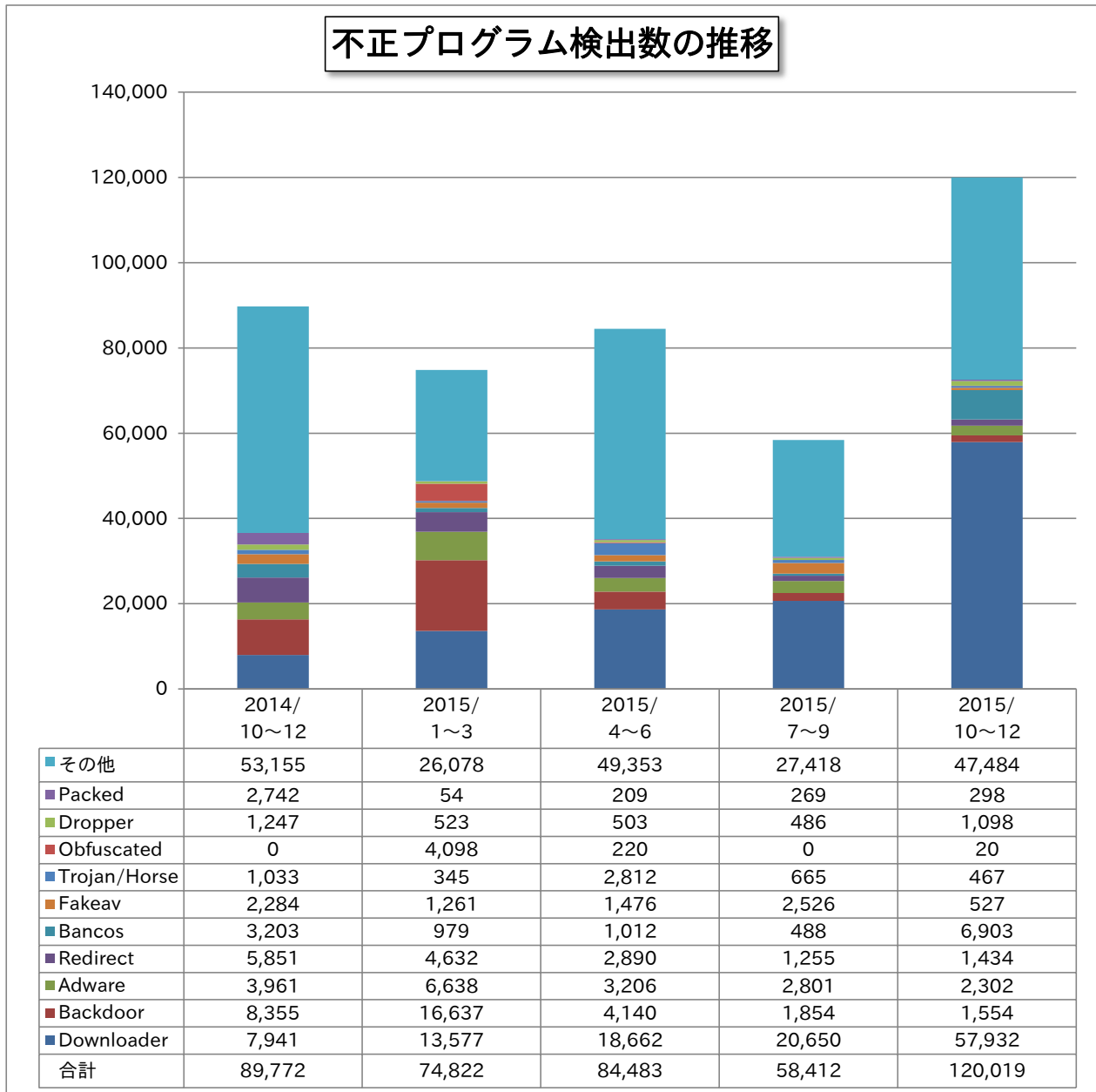


図 1-3 : 不正プログラム検出数の推移

(\*) 不正プログラム検出数：届出された「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の。

#### 1-4. ウイルス検出数

今四半期のウイルス検出数<sup>(\*)</sup>は 2,080 個でした。今四半期に最も多く検出されたウイルスは W32/Virut で、前四半期の 4 個に比べ 616 個と大きく増加しました。また、W32/Mydoom は前四半期の 2,069 個に比べ 483 個と大きく減少しました。W32/Netsky は、2014 年第 4 四半期以降、減少傾向が続いています。

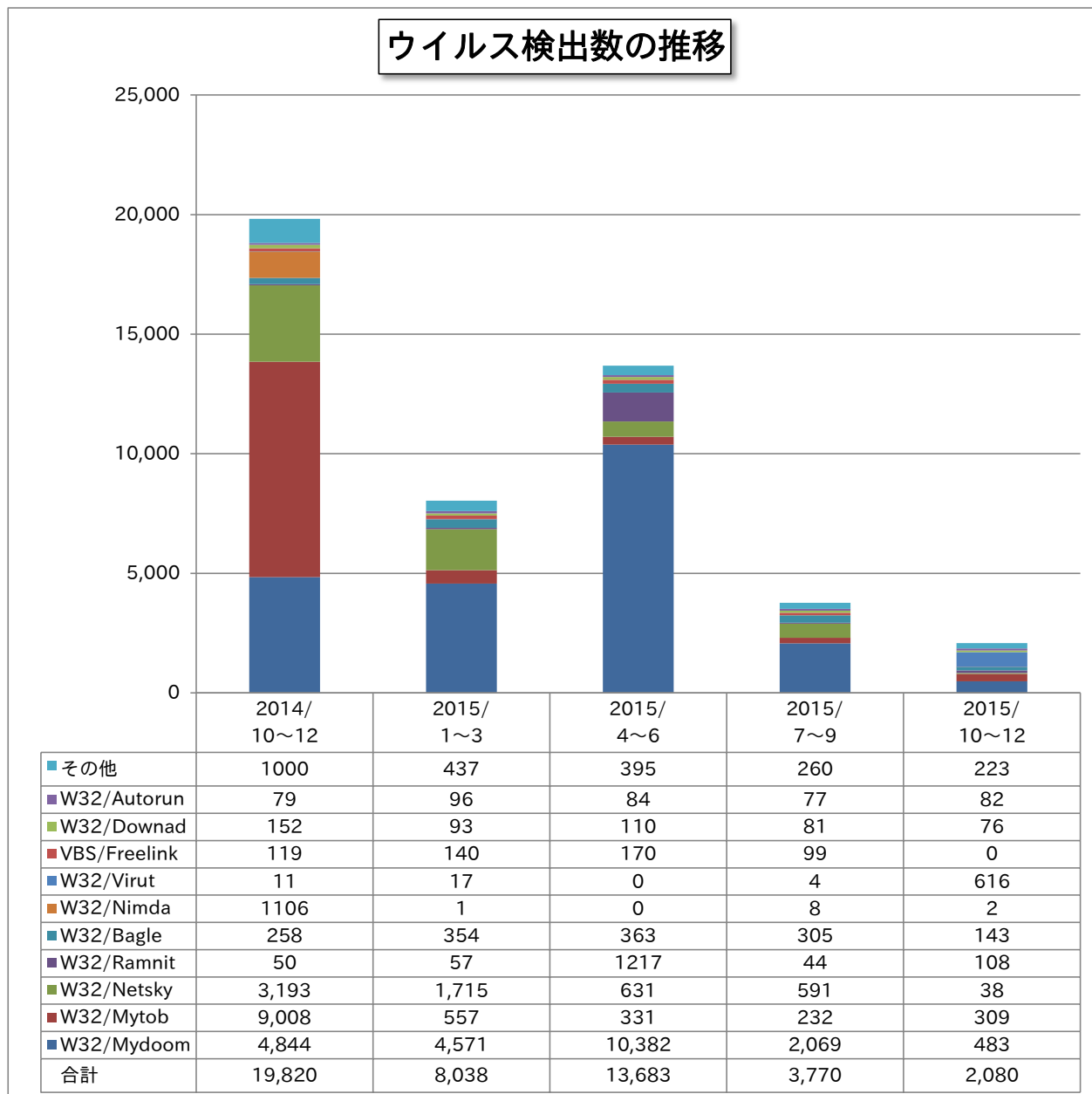


図 1-4：ウイルス検出数の推移

<sup>(\*)</sup> 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の。

### 1-5. 2015 年第 4 四半期の検出ウイルスの種類

今四半期に届出されたウイルスの種類は 41 種類、検出数は Windows/DOS ウイルス 1,996 個、スクリプトウイルス及びマクロウイルス 73 個、携帯端末ウイルス 11 個、OSS (Open Source Software) /Linux・BSD を含むウイルスはありませんでした。

表 1-1 : 2015 年第 4 四半期の検出ウイルス

i) Windows/DOS ウイルス	検出数	スクリプトウイルス	検出数
W32/Virut	616	VBS/DUNIH1	4
W32/Mydoom	483	VBS/Solow	2
W32/Netsky	309	VBS/LOVELETTER	1
W32/Ramnit	143	VBS/Redlof	1
W32/Bagle	108	小計 (4 種類)	8
W32/Downad	82		
W32/Autorun	76	マクロウイルス	検出数
W32/Sality	49	XM/Laroux	27
W32/Mytob	38	WM/Concept	12
W32/Mumu	22	XM/Mailcab	8
W32/Klez	17	W97M/Marker	8
W32/Antinny	14	X97M/Divi	3
W32/Fakerecy	7	W97M/Ethan	3
W32/Wapomi	7	W97M/Relax	2
W32/Rontokbro	4	W97M/Chack	2
W32/Gammima	3	小計 (8 種類)	65
W32/Lovgate	3		
W32/Nimda	2	ii) 携帯端末ウイルス	検出数
WM/Cap	2	AndroidOS/Lotoor	10
W32/Looked	2	AndroidOS/Adware	1
W32/Zafi	2	小計 (2 種類)	11
Stoned	2		
W32/Expiro	1	iii) Macintosh	検出数
W32/Sohanad	1	なし	
W32/Cryptolocker	1		
W32/Dorkbot	1	iv) OSS(Open Source Software)	検出数
Dropper	1	Linux・BSD を含む	
小計 (27 種類)	1,996	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)

### 1-6. 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 82.3%を占めました。

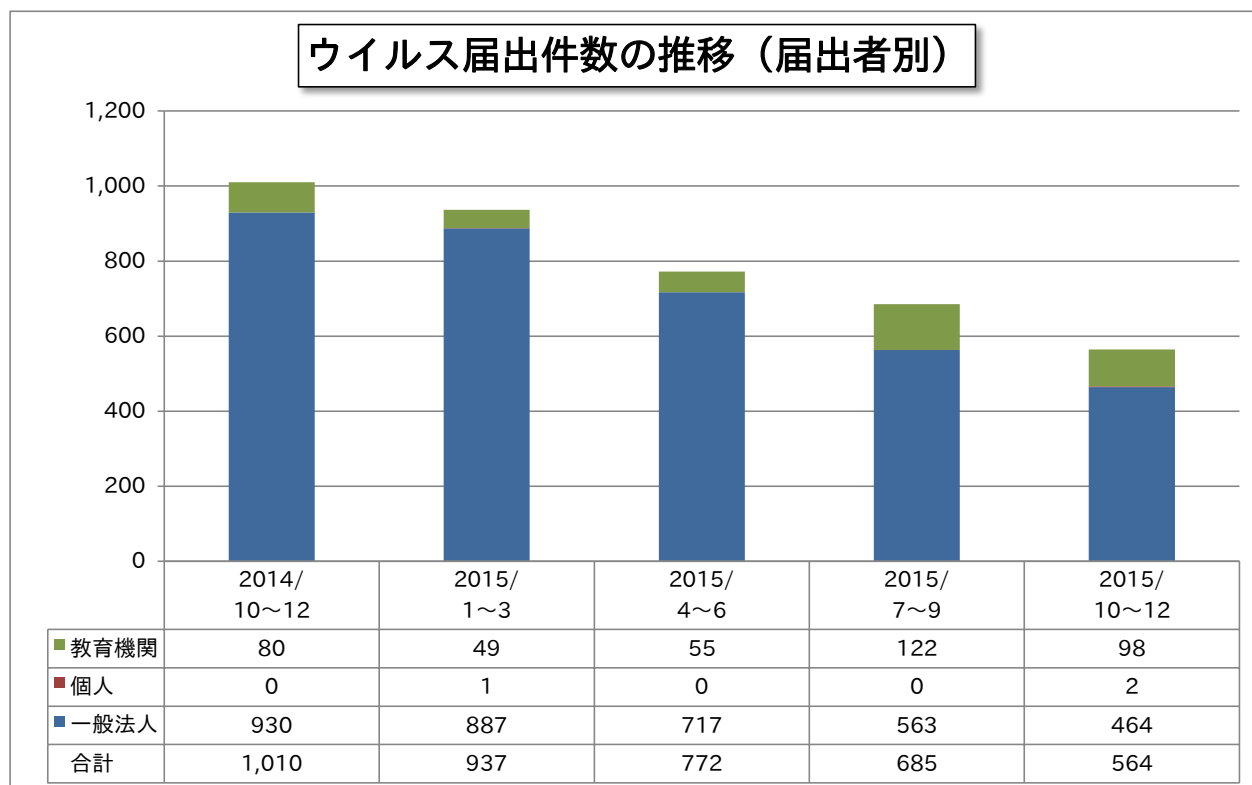


図 1-5 : ウイルス届出件数の推移 (届出者別)



### 1-7. 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」の割合が最も多く全体の約 89.5%を占め、次いで「不明・その他」が約 8.7%でした。

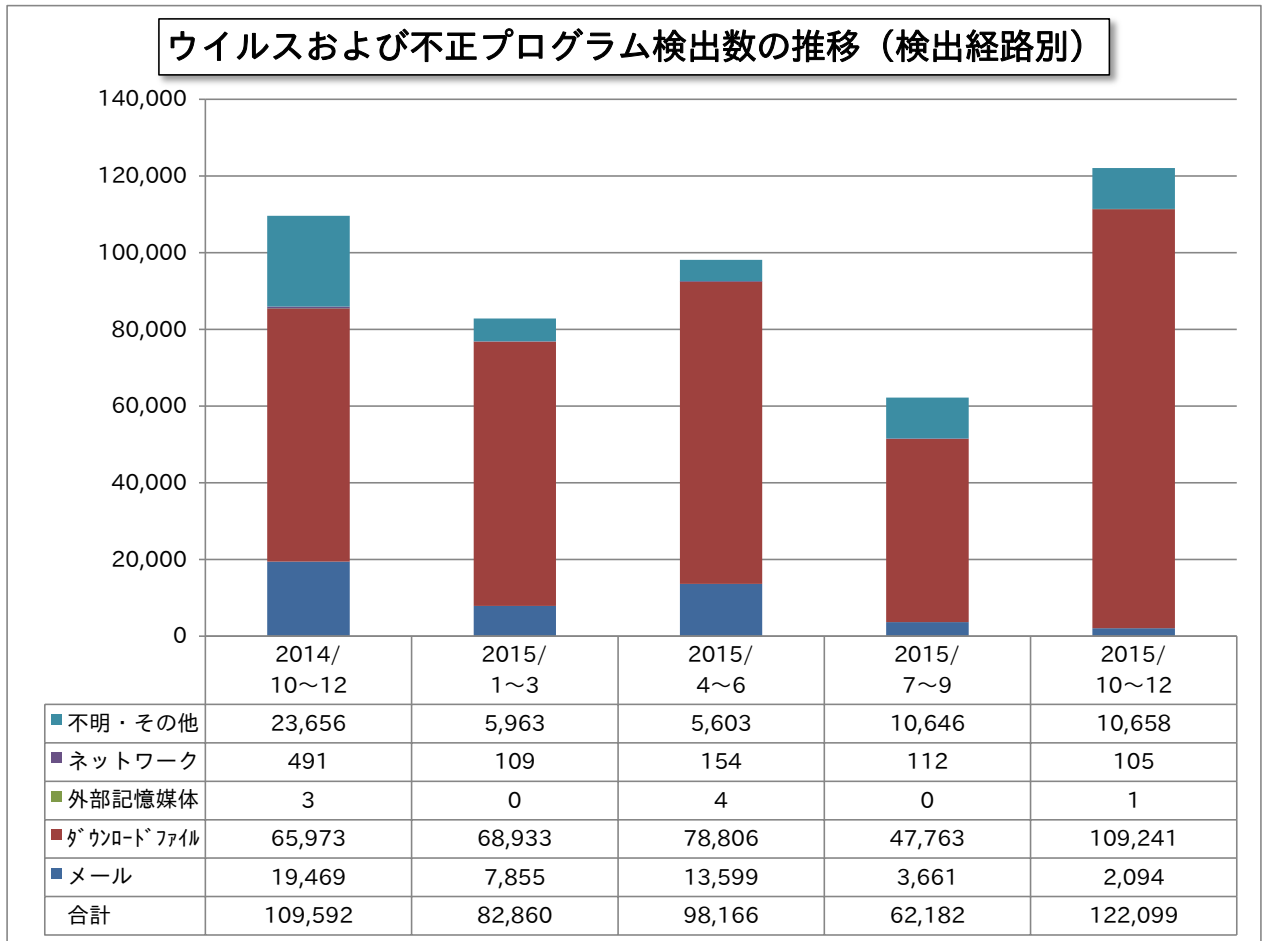


図 1-6：ウイルスおよび不正プログラム検出数の推移（検出経路別）

#### ・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. 2015 年総括

2015年に寄せられた不正アクセス届出件数は、前年の120件より10件（約8.3%）少ない110件となりました。そのうち、被害のあった届出は88件で全体の80.0%を占めています。

被害のあった届出の割合は、2013年が約94.0%、2014年が85.0%と2013年以降、減少傾向が見られます。

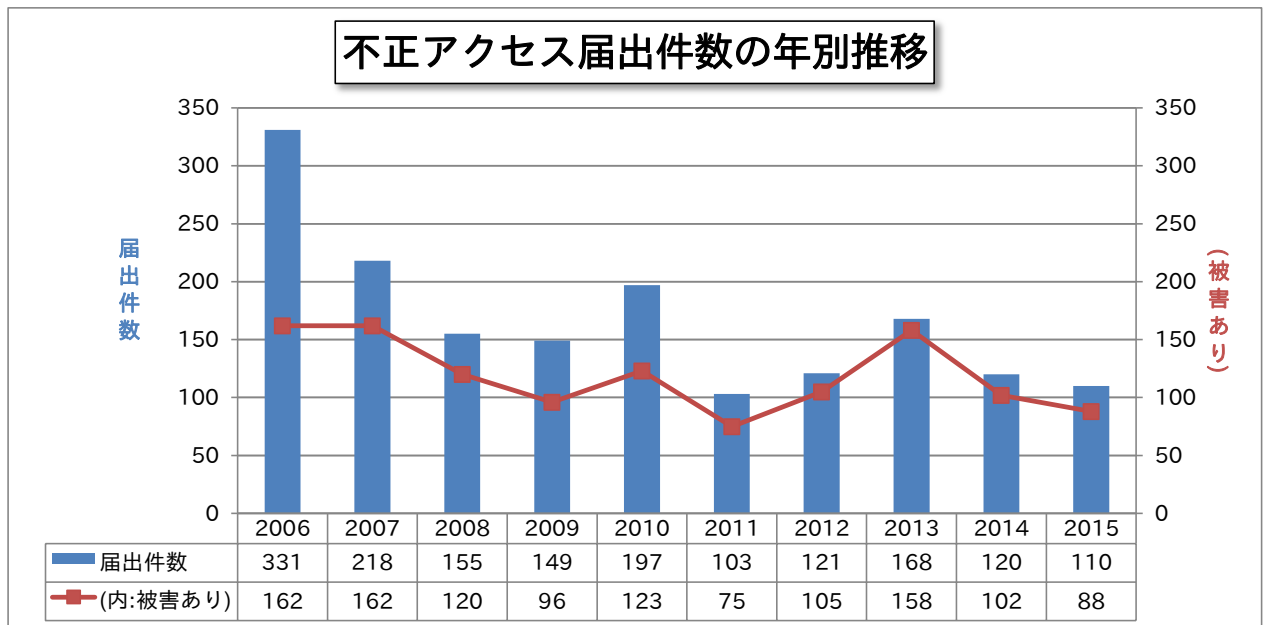


図 2-1：不正アクセス届出件数の年別推移

## 2-2. 不正アクセス届出件数

今四半期の届出件数は 28 件で、そのうち被害があったのは 24 件でした。

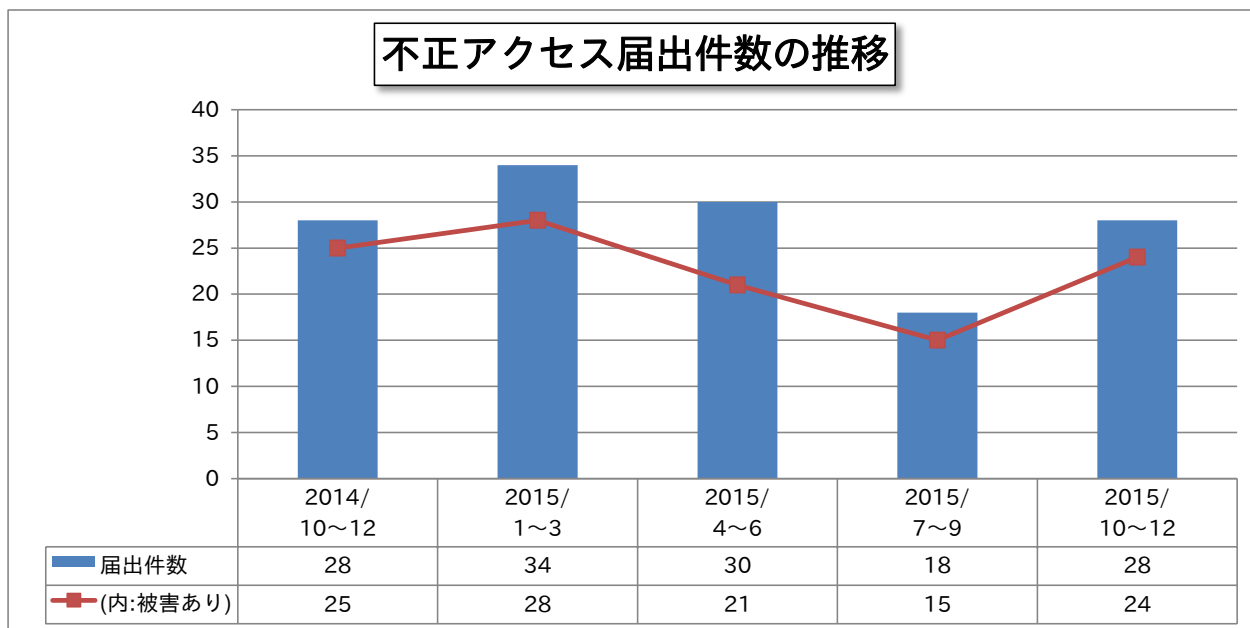


図 2-2 : 不正アクセス届出件数の推移

## 2-3. 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 13 件、「DoS」が 5 件、「侵入」が 1 件、「その他（被害あり）」が 5 件でした。前四半期と比較して「なりすまし」が全体の約 27.8%から約 46.4%に増加しました。また「不正プログラム埋込」の届出は前四半期に引き続き 0 件でした。

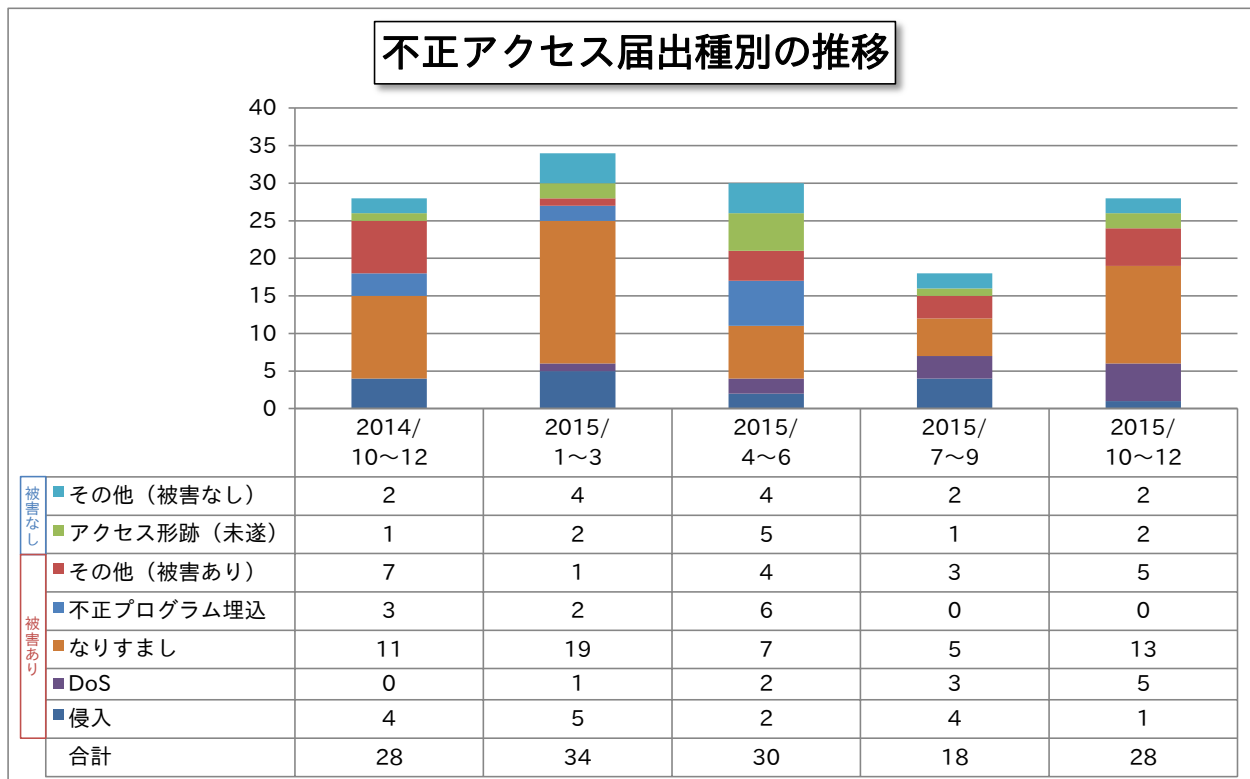


図 2-3 : 不正アクセス届出種別の推移

## 2-4. 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9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件等でした。前四半期と比較して「ID・パスワード管理不備」の割合が全体の20%から37.5%に増加しました。

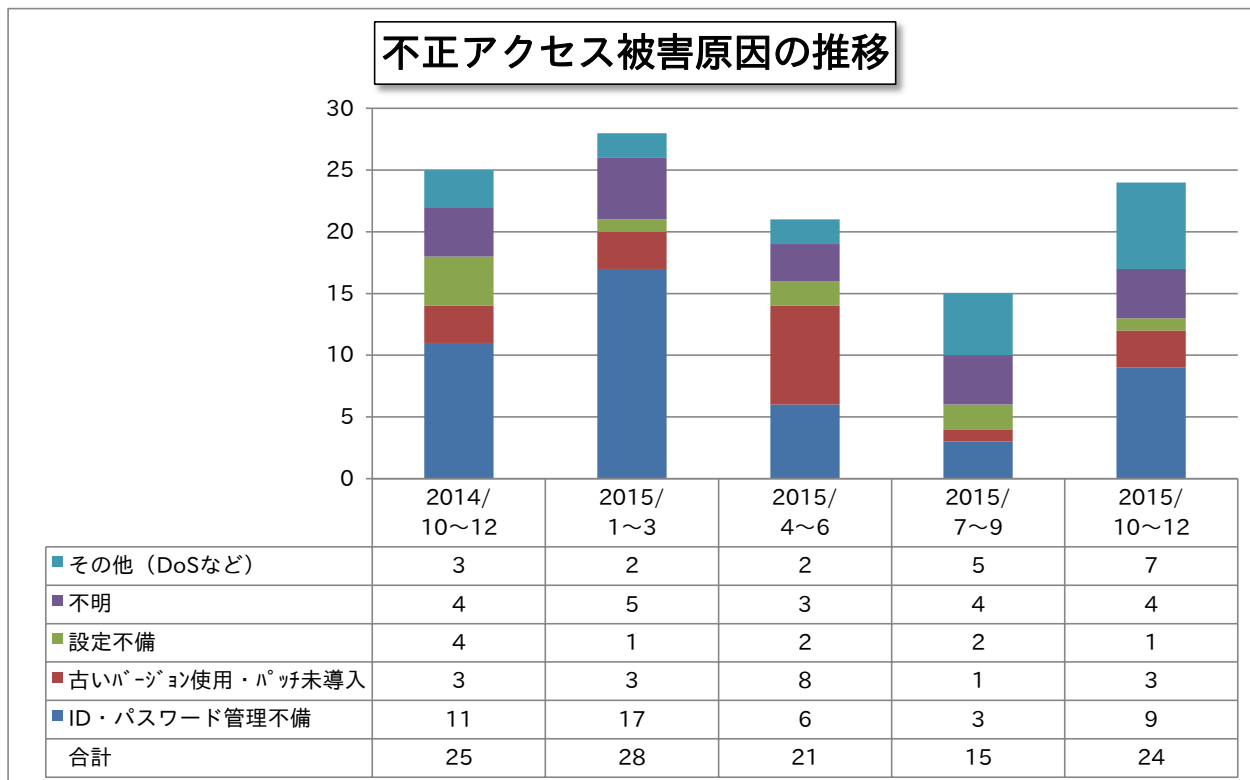


図 2-4：不正アクセス被害原因の推移

## 2-5. 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5件、「個人ユーザ」が15件、「教育・研究・公的機関」が8件でした。

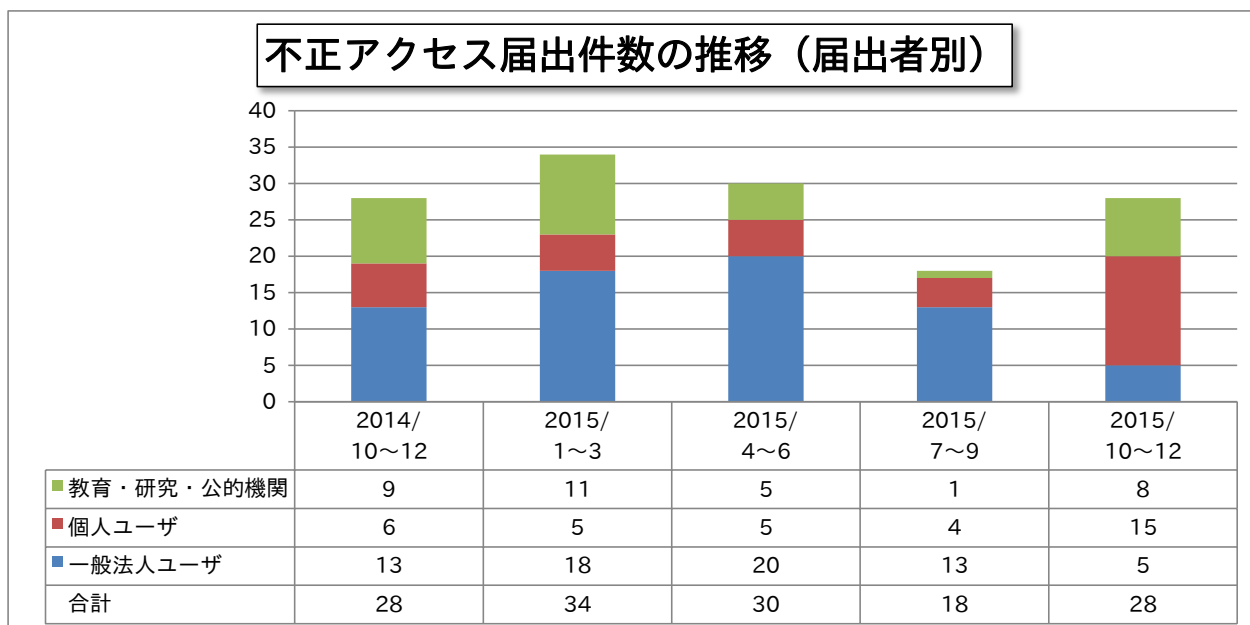


図 2-5：不正アクセス届出件数の推移（届出者別）

## 2-6. 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) ショッピングサイトで不正購入の手続きをされてしまった。

<b>被害の概要</b>	<ul style="list-style-type: none"><li>・ 高額商品を複数点購入していることに不審を抱いたとして、利用しているショッピングサイトから注文内容を確認したいという連絡があった。</li><li>・ 確認をすると、ウェブメールの受信トレイに本来届くべきはずの注文確認メールは見当たらなかったが、ショッピングサイトの記録では身に覚えのない商品を購入したことになっていた。</li><li>・ さらに調べたところ、ウェブメールに第三者がログインした痕跡が確認でき、見当たらなかった注文確認メールは削除されてしまったと考えられる。</li><li>・ ウェブメールおよびショッピングサイトにはどちらも同じパスワードを設定していて、またパスワードは安易な内容であった。</li></ul>
<b>解説・対策</b>	<p>ウェブメールおよびショッピングサイトのアカウントに不正ログインされてしまった事例です。</p> <p>被害者はウェブメールをパソコンでのみ利用していたため、不正購入されたこと（身に覚えのない注文確認メールの受信）にすぐ気づくことができませんでした。ただし、商品発送前にショッピングサイトから注文内容確認の連絡があり、その時点で購入をキャンセルできたため、幸いにも金銭被害には至りませんでした。</p> <p>この事例では、パスワードが安易な内容だけでなく、同じパスワードを使い回していたことで、ウェブメールとショッピングサイトの複数のサービスに不正ログインされてしまったと考えられます。</p> <p>なお、ウェブメールに不正ログインされてしまった場合は、メールボックスの内容から利用しているサービスを特定されてしまい被害が拡大する恐れがあります。対策として、利用するサービスすべてのパスワードを、可能な限り長く、複雑な内容に設定し、使い回さないことが肝要です。また、二段階認証機能が提供されている場合、積極的に利用することを推奨します。</p>

#### ・ 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. 2015 年総括

2015年に「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年から約6.0%減の14,657件でした。

2015年5月には、「インターネット閲覧中に突然"ウイルスを検出した"と音声 flowed」という相談がはじめて寄せられました。これはウイルスを検出したという偽の警告画面や音声で不安を煽り、指定の番号に電話をかけさせてサポート契約やソフトウェア購入に誘導するという新しい手口です。この相談は計105件寄せられました。

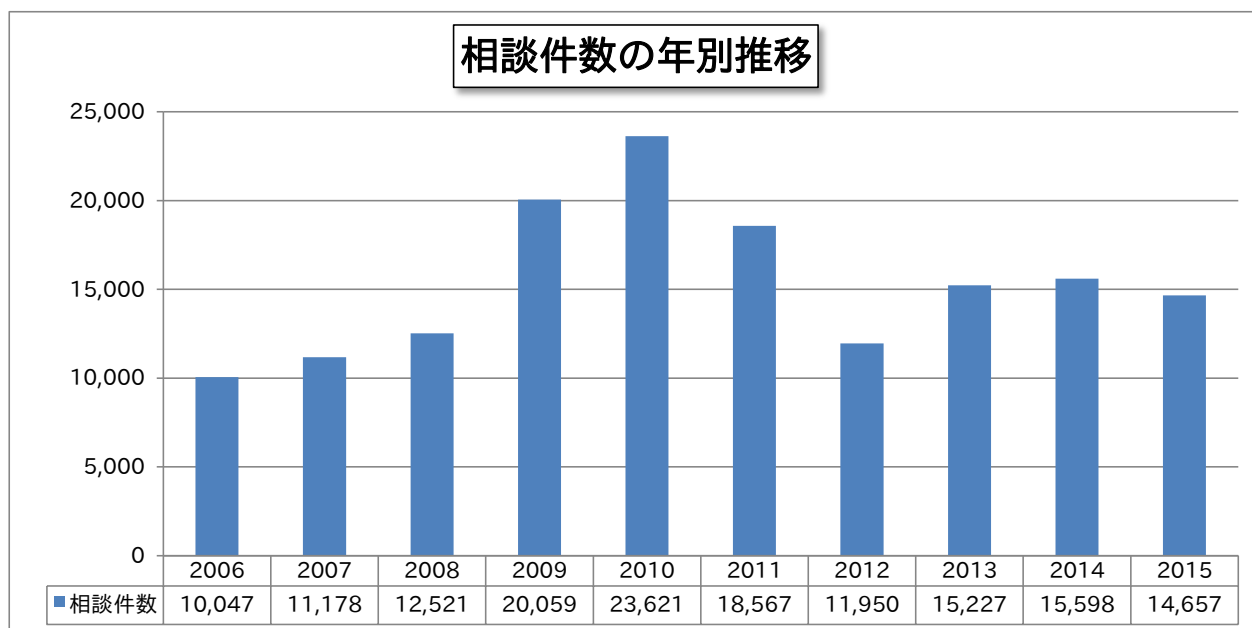


図 3-1：相談件数の年別推移

### 3-2. 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 8.2%増の 3,970 件でした。そのうち、相談員による対応件数は 1,892 件でした。

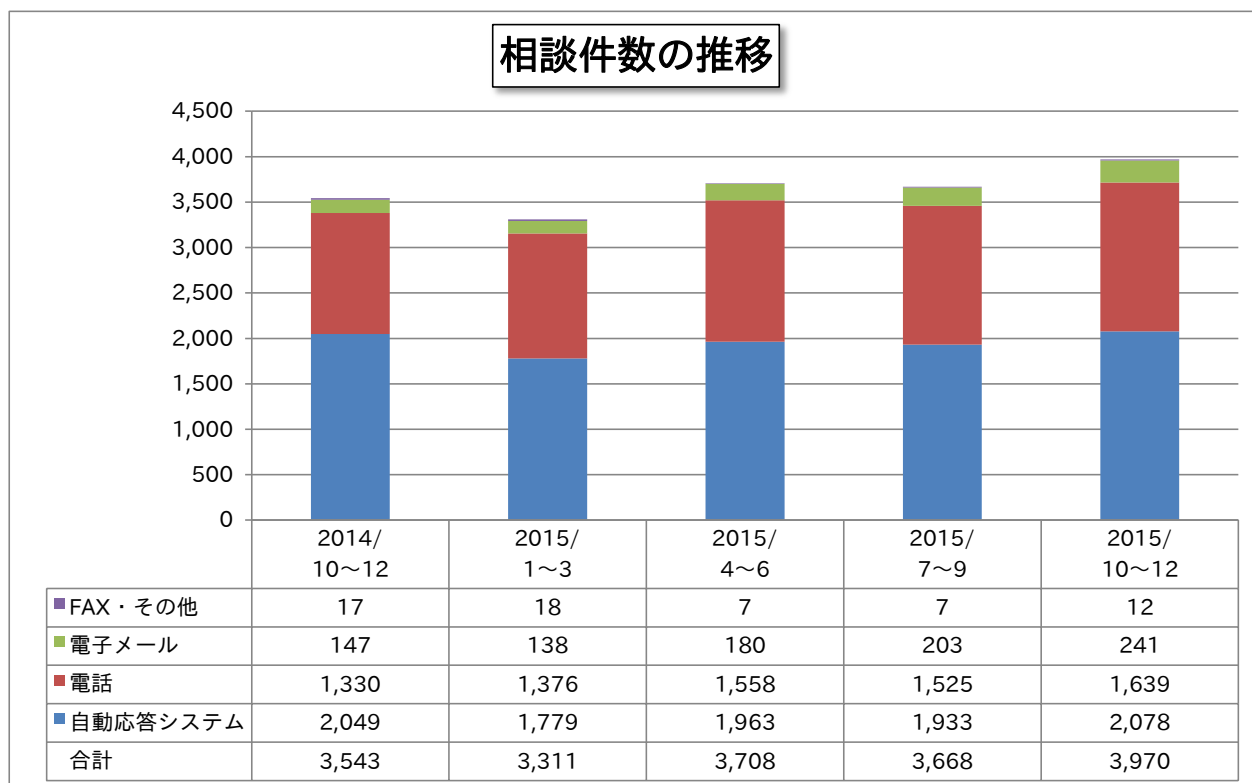


図 3-2 : 相談件数の推移

### 3-3. 主な手口における相談員の対応件数

#### (i) 「ワンクリック請求」

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」に関する相談が前四半期から約 17.7%減の 679 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 22.8%減の 311 件で、いずれの相談も減少しました。

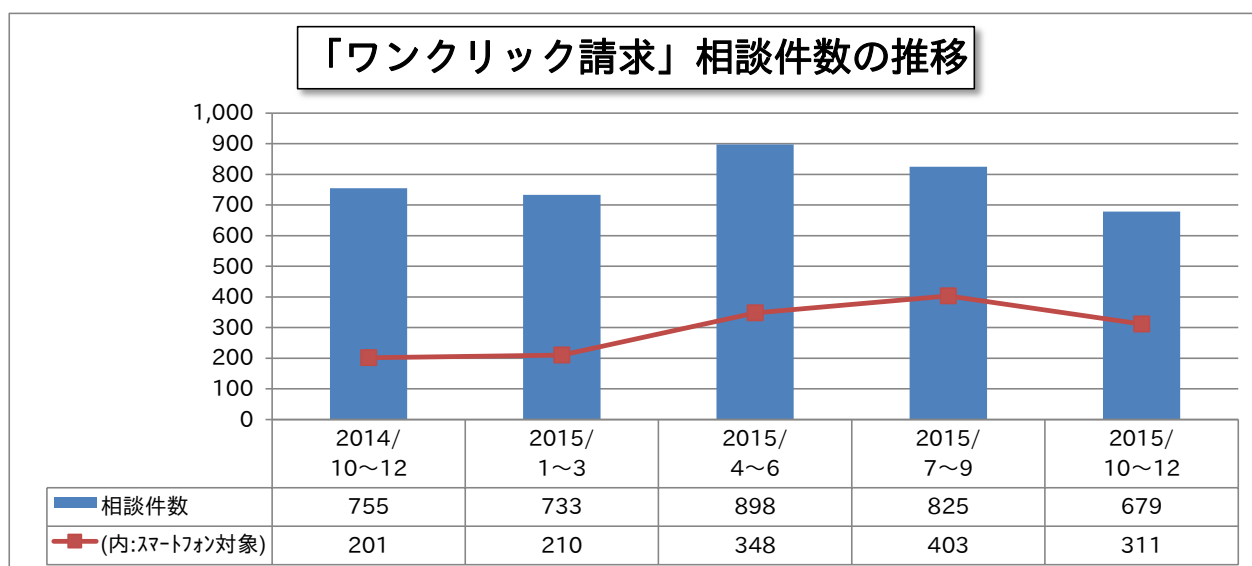


図 3-3 : 「ワンクリック請求」相談件数の推移

## (ii) 「ウイルス検出の偽警告」

ウイルスを検出したという偽の警告画面や音声で不安を煽り、指定の番号に電話をかけさせてサポート契約やソフトウェア購入に誘導する「ウイルス検出の偽警告」に関する相談が今四半期は 57 件寄せられました。

はじめて相談が寄せられた 2015 年 5 月以降、相談件数の増加は顕著です。

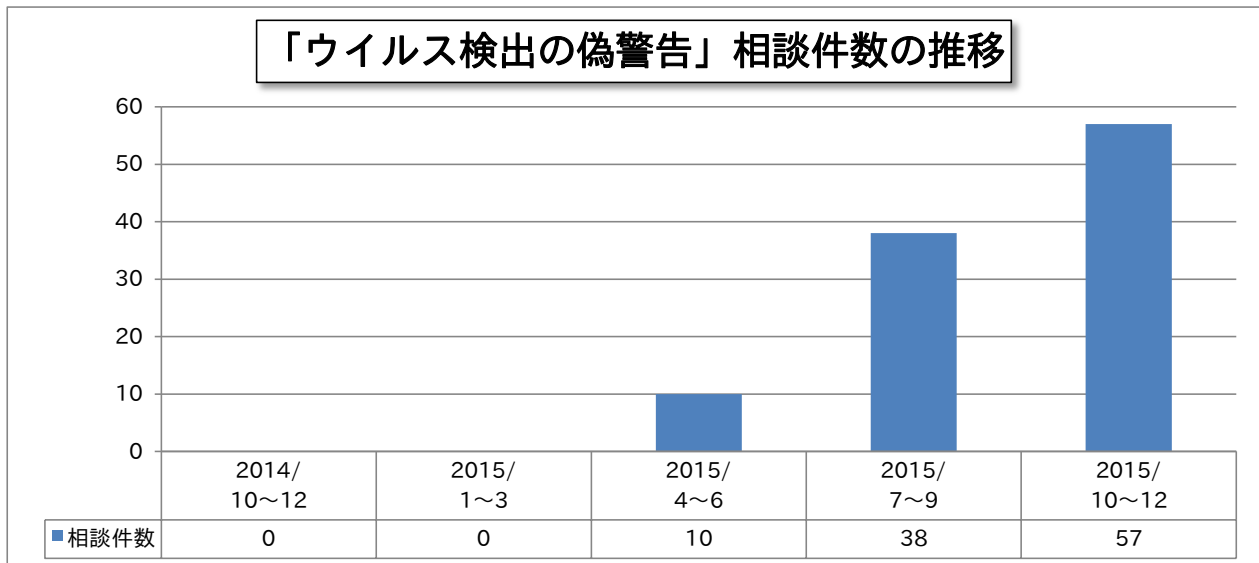


図 3-4 : 「ウイルス検出の偽警告」相談件数の推移

## (iii) 「ランサムウェア」

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約 35.3%増の 46 件寄せられました。

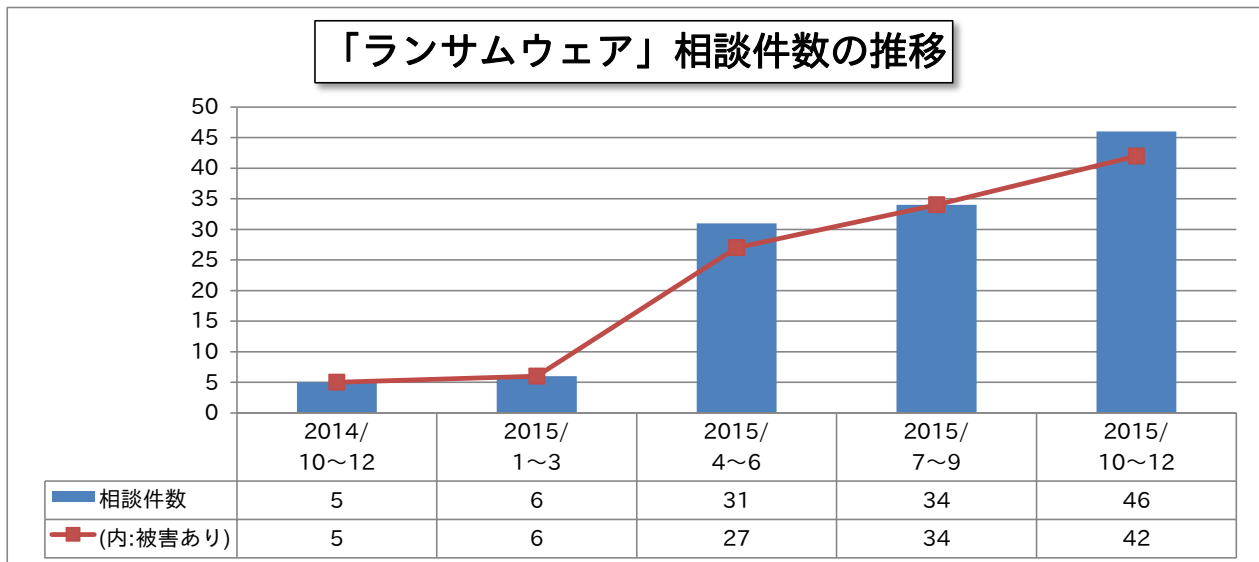


図 3-5 : 「ランサムウェア」相談件数の推移



### 3-4. 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) 突然、ブラウザに青い画面でウイルスを検出したといった警告が表示された。

<b>相談の概要</b>	<ul style="list-style-type: none"><li>・ Internet Explorer でインターネットを閲覧中、突然、青い画面に「感染 ID」や「停止：0x0000007E」といった白い文字が表示された。</li><li>・ 内容はよく覚えていないが、その際、英語の音声も流れていた気がする。</li><li>・ 青い画面には、「指定の電話番号に至急電話をかけるように」という案内の記載があったが、日本語に不自然な点を感じ、不審を抱き電話はかけていない。</li><li>・ ただし、青い画面を閉じようと思っても、タブもブラウザも閉じることができない。</li><li>・ 本当にウイルスに感染してしまっているのか。</li></ul>
<b>回答</b>	<p>ウイルスを検出したという偽の警告で不安を煽る手口の一つであり、実際のウイルス感染はないと考えられます。表示されたメッセージをよく読んで、不自然な点に気づいて電話をかけなかったというのは正しい判断であり、適切な行動です。</p> <p>ブラウザが閉じられないという事象は、ウイルスによるものではなくポップアップメッセージが繰り返し表示される仕掛けによるものです。</p> <p>この場合、×印をクリックしても画面を閉じることができないため、タスクマネージャーから終了（[タスクマネージャー] を起動し、Internet Explorer を選択して [タスクの終了] をクリック）させる、またはパソコンを再起動させるといった方法でブラウザを終了させます。</p> <p>なお、同様の相談では、指定の電話番号に電話をかけると外国人と思われる担当者が出て、ウイルス感染の有無を確認する等として、遠隔操作を持ちかけられたり、有償のサポート契約やソフトウェア購入を勧められたりするといった事例が確認できています。</p> <p>もし慌てて電話をかけ、サポート契約またはソフトウェア購入をしてしまった場合、解約の相談は、消費生活センターにご連絡ください。</p> <p>（ご参考） 「ウイルスを検出したと音声で警告してくるウェブサイトにご注意！」 <a href="https://www.ipa.go.jp/security/txt/2015/08outline.html">https://www.ipa.go.jp/security/txt/2015/08outline.html</a> 全国の消費生活センター等 <a href="http://www.kokusen.go.jp/map/">http://www.kokusen.go.jp/map/</a></p>