# 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 2 四半期（4 月～6 月）］

本レポートでは、2015 年 4 月 1 日から 2015 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

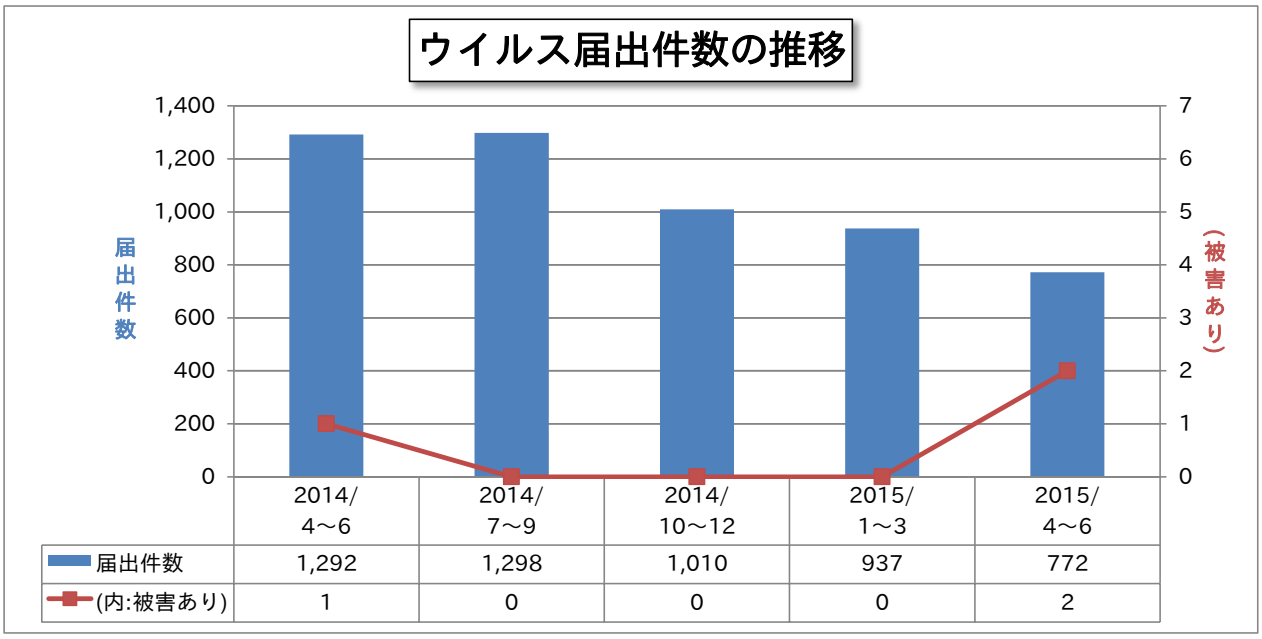
2015 年 7 月 24 日

**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 4 月～6 月）のウイルス届出件数は 772 件で、そのうちウイルス感染被害があった届出は 2 件でした。




| | 2014/4～6 | 2014/7～9 | 2014/10～12 | 2015/1～3 | 2015/4～6 |
|---|---|---|---|---|---|
| 届出件数 | 1,292 | 1,298 | 1,010 | 937 | 772 |
| (内:被害あり) | 1 | 0 | 0 | 0 | 2 |

図 1-1：ウイルス届出件数の推移

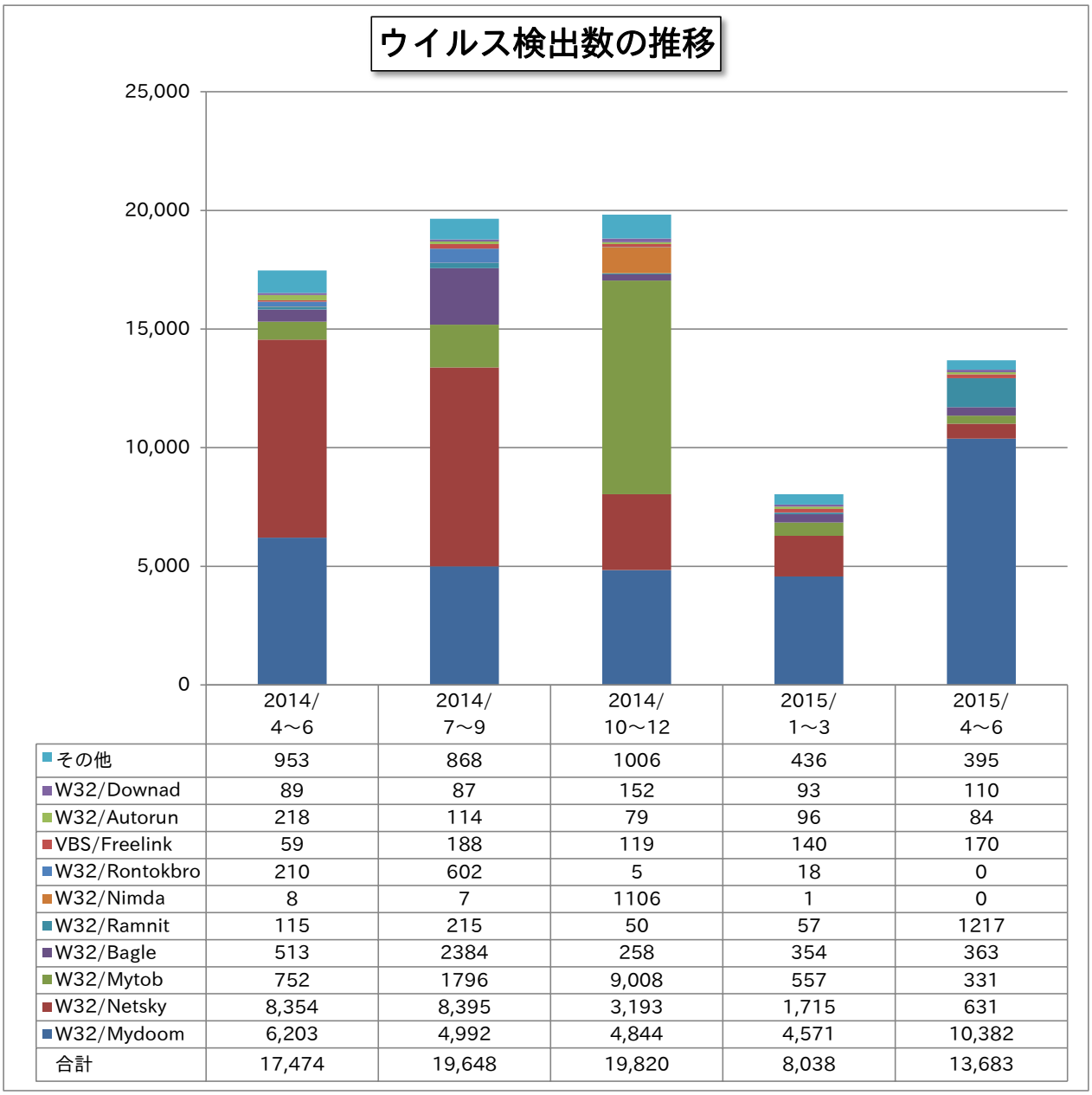
被害にあった届出のうち 1 つは、2015 年 5 月に届出された W32/Cryptolocker は「ランサムウェア [*1]」と呼ばれるタイプのウイルスでした。感染するとパソコンに保存していたファイルが暗号化されるとともに、暗号化されたファイルの暗号化解除を名目に身代金を要求する警告画面が表示されます。

同ウイルスは、2014 年 3 月にも感染被害の届出がされており、今後も感染被害が発生することが懸念されます。

[*1] 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化解除を名目に身代金を要求するウイルス。

## 1-2. ウイルス検出数

今四半期のウイルス検出数 (*2) は 13,683 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、前四半期までは検出数がほぼ横ばいでしたが、今四半期は全体の約 75.9%を占め、急増しました。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 0.7%だった W32/Ramnit が今四半期は約 8.9%と急増しました。W32/Netsky は、2014 年第 4 四半期に検出数が大きく減少し、それ以降は減少傾向となっています。



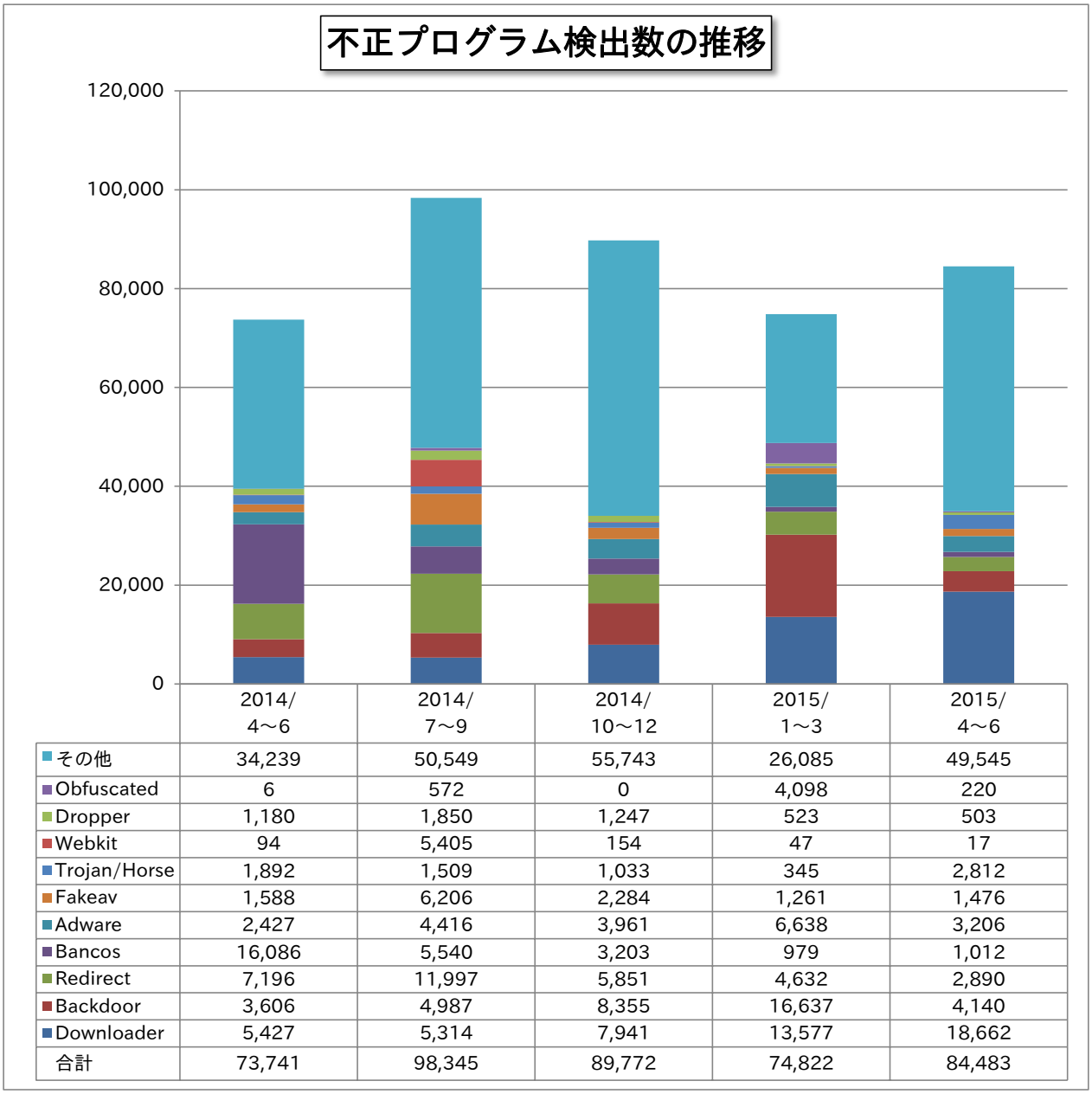

| | 2014/4～6 | 2014/7～9 | 2014/10～12 | 2015/1～3 | 2015/4～6 |
|---|---|---|---|---|---|
| その他 | 953 | 868 | 1006 | 436 | 395 |
| W32/Downad | 89 | 87 | 152 | 93 | 110 |
| W32/Autorun | 218 | 114 | 79 | 96 | 84 |
| VBS/Freelink | 59 | 188 | 119 | 140 | 170 |
| W32/Rontokbro | 210 | 602 | 5 | 18 | 0 |
| W32/Nimda | 8 | 7 | 1106 | 1 | 0 |
| W32/Ramnit | 115 | 215 | 50 | 57 | 1217 |
| W32/Bagle | 513 | 2384 | 258 | 354 | 363 |
| W32/Mytob | 752 | 1796 | 9,008 | 557 | 331 |
| W32/Netsky | 8,354 | 8,395 | 3,193 | 1,715 | 631 |
| W32/Mydoom | 6,203 | 4,992 | 4,844 | 4,571 | 10,382 |
| 合計 | 17,474 | 19,648 | 19,820 | 8,038 | 13,683 |

図 1-2：ウイルス検出数の推移

(*2) 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 (*3) は 84,483 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 2014 年第 4 四半期の約 2.35 倍、前四半期の約 37.5%増となっています。Backdoor は前四半期まで増加が続いていましたが、今四半期は大幅に減少し前期の約 75.1%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となっています。Trojan/Horse も減少傾向が続いていましたが、今四半期に急増し、前期の約 8.15 倍の検出がありました。




| | 2014/4～6 | 2014/7～9 | 2014/10～12 | 2015/1～3 | 2015/4～6 |
|---|---|---|---|---|---|
| その他 | 34,239 | 50,549 | 55,743 | 26,085 | 49,545 |
| Obfuscated | 6 | 572 | 0 | 4,098 | 220 |
| Dropper | 1,180 | 1,850 | 1,247 | 523 | 503 |
| Webkit | 94 | 5,405 | 154 | 47 | 17 |
| Trojan/Horse | 1,892 | 1,509 | 1,033 | 345 | 2,812 |
| Fakeav | 1,588 | 6,206 | 2,284 | 1,261 | 1,476 |
| Adware | 2,427 | 4,416 | 3,961 | 6,638 | 3,206 |
| Bancos | 16,086 | 5,540 | 3,203 | 979 | 1,012 |
| Redirect | 7,196 | 11,997 | 5,851 | 4,632 | 2,890 |
| Backdoor | 3,606 | 4,987 | 8,355 | 16,637 | 4,140 |
| Downloader | 5,427 | 5,314 | 7,941 | 13,577 | 18,662 |
| 合計 | 73,741 | 98,345 | 89,772 | 74,822 | 84,483 |

図 1-3：不正プログラム検出数の推移

(*3) 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 2 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 51 種類、検出数は Windows/DOS ウイルス 13,393 個、スクリプトウイルス及びマクロウイルス 243 個、携帯端末ウイルス 47 個でした。

表 1-1：2015 年第 2 四半期の検出ウイルス

| i) Windows/DOS ウイルス | 検出数 |
|---|---|
| W32/Mydoom | 10,382 |
| W32/Ramnit | 1,217 |
| W32/Netsky | 631 |
| W32/Bagle | 363 |
| W32/Mytob | 331 |
| W32/Downad | 110 |
| W32/Autorun | 84 |
| W32/Magistr | 43 |
| W32/Fujacks | 22 |
| W32/klez | 20 |
| W32/Fakerecy | 18 |
| W32/Lovgate | 17 |
| W32/Sality | 17 |
| W32/CIH | 16 |
| W32/IRCbot | 14 |
| W32/Mumu | 14 |
| W32/Looked | 12 |
| W32/Myparty | 12 |
| W32/Fbound | 9 |
| W32/Parite | 9 |
| W32/Antinny | 8 |
| W32/Gammima | 8 |
| W32/Almanahe | 6 |
| W32/Bacterra | 4 |
| W32/Fanbot | 4 |
| W32/Remadm | 4 |
| W32/Mywife | 3 |
| W32/Badtrans | 2 |
| W32/Dorkbot | 2 |
| W32/Frethem | 2 |
| W32/Zafi | 2 |
| W32/Bugbear | 1 |
| W32/Cryptolocker | 1 |
| W32/Harakit | 1 |
| W32/Licum | 1 |
| W32/Nuwar | 1 |
| W32/Stration | 1 |
| W32/Wapomi | 1 |
| 小計　(38 種類) | 13,393 |

| スクリプトウイルス | 検出数 |
|---|---|
| VBS/Freelink | 170 |
| VBS/Redlof | 2 |
| VBS/LOVELETTER | 2 |
| VBS/DUNIHI | 1 |
| 小計　(4 種類) | 175 |

| マクロウイルス | 検出数 |
|---|---|
| XM/Laroux | 36 |
| W97M/Class | 12 |
| WM/Cap | 8 |
| W97M/Marker | 4 |
| W97M/Relax | 4 |
| W97M/Melissa | 2 |
| WM/Concept | 1 |
| XM/Mailcab | 1 |
| 小計　(8 種類) | 68 |

| ii) 携帯端末ウイルス | 検出数 |
|---|---|
| AndroidOS/Lotoor | 47 |
| 小計　(1 種類) | 47 |

| iii) Macintosh | 検出数 |
|---|---|
| なし | |

| iv) OSS<br>Linux・BSD を含む | 検出数 |
|---|---|
| なし | |

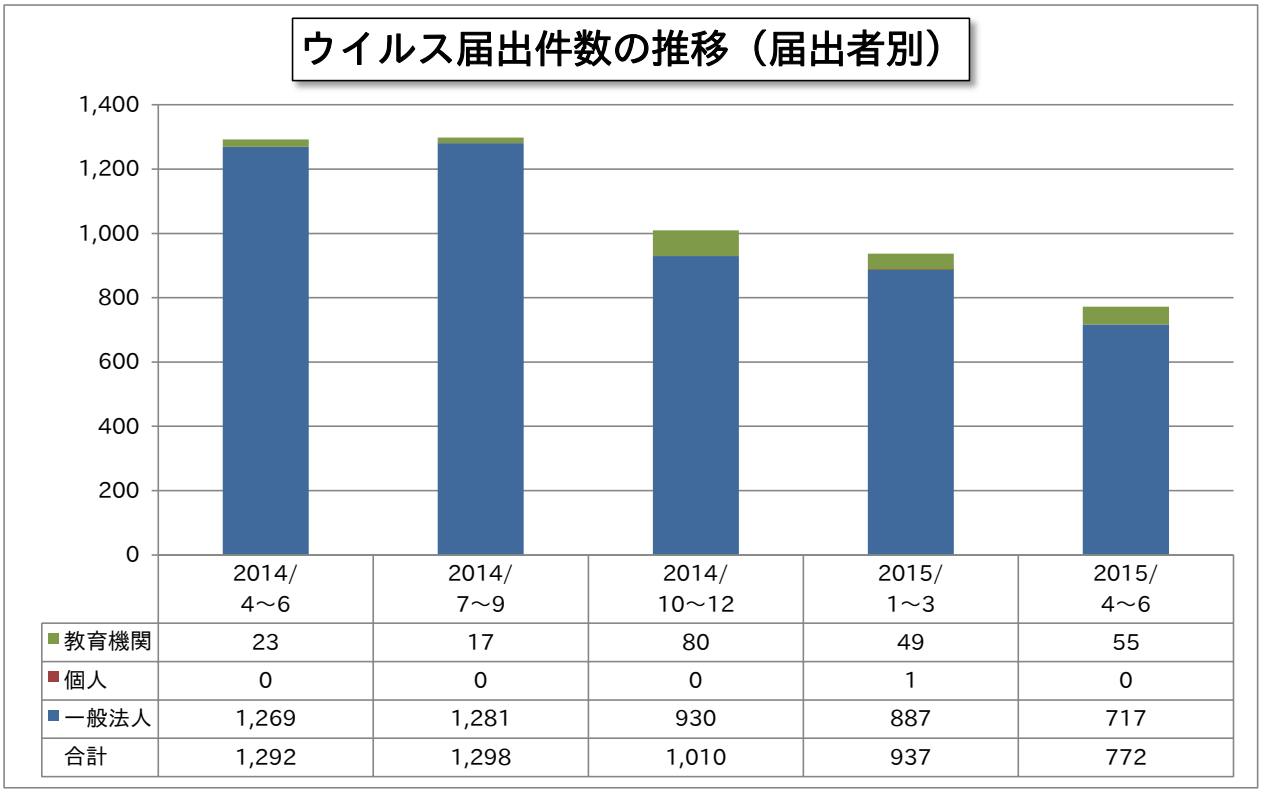
（参考）
・Windows/DOS ウイルス … Windows、MS-DOS 環境下で動作するウイルス。
・マクロウイルス … Microsoft Word や Microsoft Excel などのマクロ機能を悪用するウイルス。
・スクリプトウイルス … 機械語への変換作業を省略して実行できるようにした簡易プログラムで記述されたウイルス。
・携帯端末ウイルス … 携帯電話やタブレットなどの環境下で動作するウイルス。

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 | 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 92.9%を占めました。

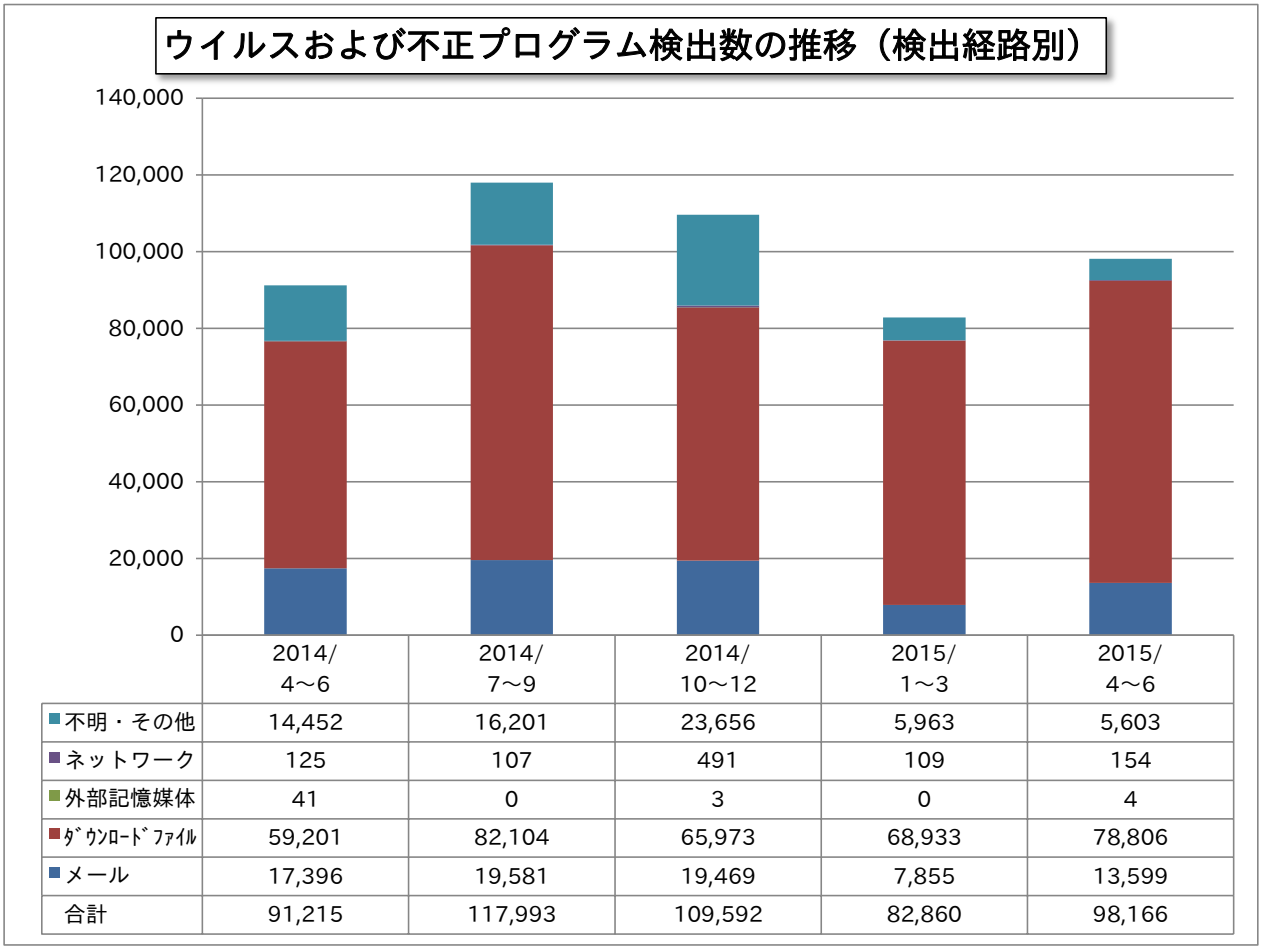



| | 2014/4～6 | 2014/7～9 | 2014/10～12 | 2015/1～3 | 2015/4～6 |
|---|---|---|---|---|---|
| 教育機関 | 23 | 17 | 80 | 49 | 55 |
| 個人 | 0 | 0 | 0 | 1 | 0 |
| 一般法人 | 1,269 | 1,281 | 930 | 887 | 717 |
| 合計 | 1,292 | 1,298 | 1,010 | 937 | 772 |

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「メール」の約 13.9%でした。




| | 2014/ 4～6 | 2014/ 7～9 | 2014/ 10～12 | 2015/ 1～3 | 2015/ 4～6 |
|---|---|---|---|---|---|
| 不明・その他 | 14,452 | 16,201 | 23,656 | 5,963 | 5,603 |
| ネットワーク | 125 | 107 | 491 | 109 | 154 |
| 外部記憶媒体 | 41 | 0 | 3 | 0 | 4 |
| ﾀﾞｳﾝﾛｰﾄﾞﾌｧｲﾙ | 59,201 | 82,104 | 65,973 | 68,933 | 78,806 |
| メール | 17,396 | 19,581 | 19,469 | 7,855 | 13,599 |
| 合計 | 91,215 | 117,993 | 109,592 | 82,860 | 98,166 |

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。

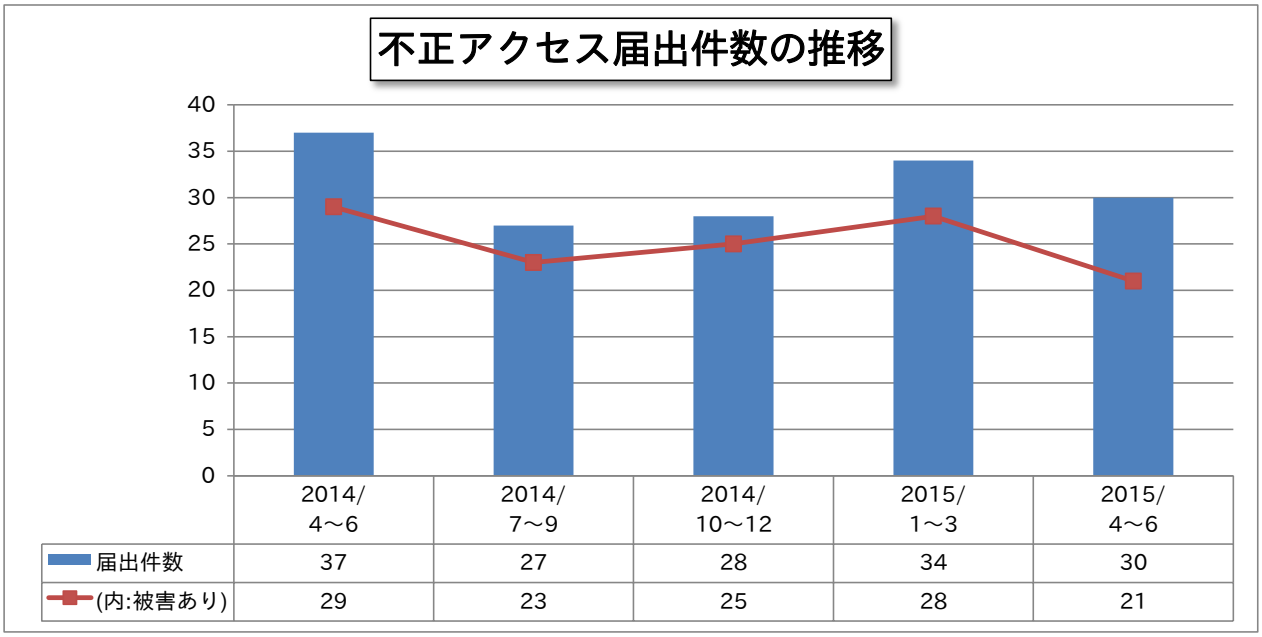
IPA では、個別に届出者への対応を行っていますが、同時に受理した届出等を基に、コンピュータウイルス対策を検討しています。また受理した届出は、届出者のプライバシーを侵害することがないように配慮した上で、被害等の状況を分析し、検討結果を定期的に公表しています。

○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 30 件で、そのうち被害があったのは 21 件でした。

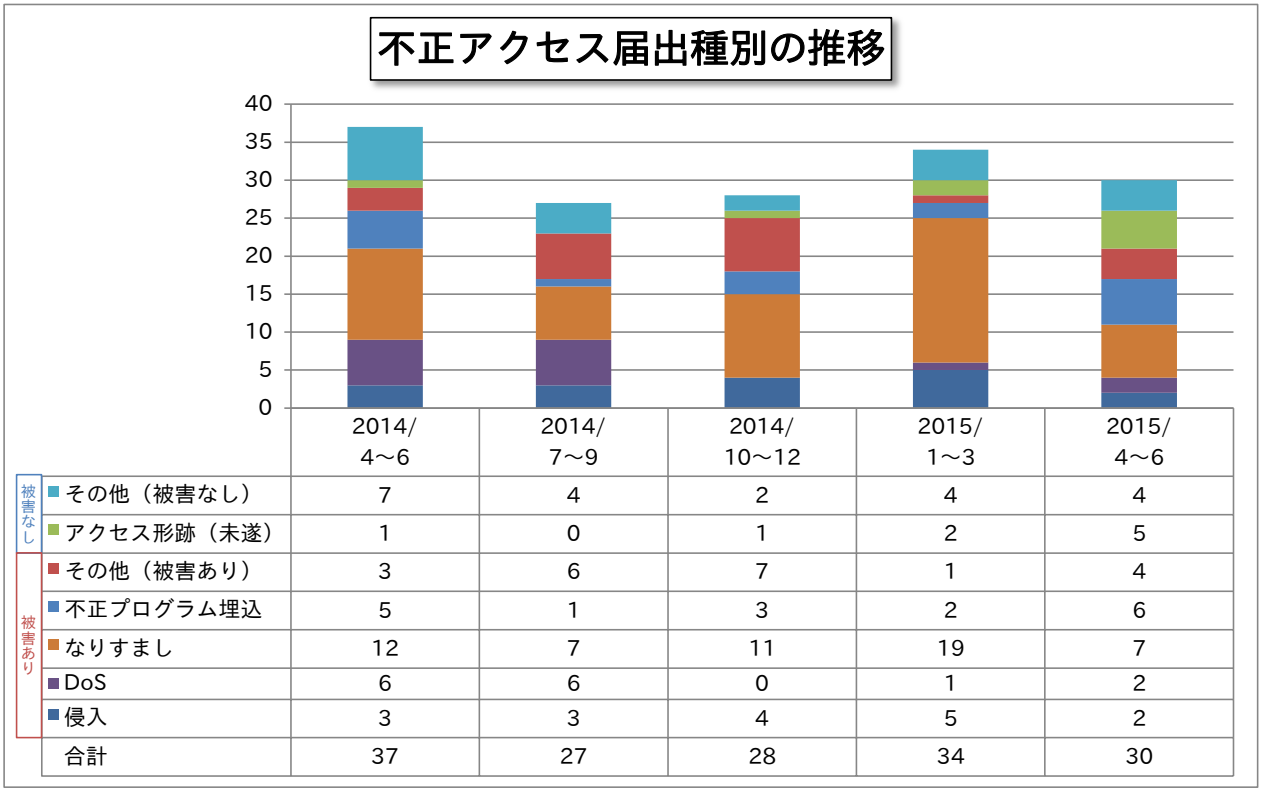



| | 2014/4～6 | 2014/7～9 | 2014/10～12 | 2015/1～3 | 2015/4～6 |
|---|---|---|---|---|---|
| 届出件数 | 37 | 27 | 28 | 34 | 30 |
| (内:被害あり) | 29 | 23 | 25 | 28 | 21 |

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 7 件、「不正プログラム埋込」が 6 件、「侵入」が 2 件、「DoS」が 2 件、「その他（被害あり）」が 4 件でした。前四半期と比較して「なりすまし」の届出が全体の約 55.9%から約 23.3%に減少し、「不正プログラム埋込」が約 5.9%から 20%に増加しました。

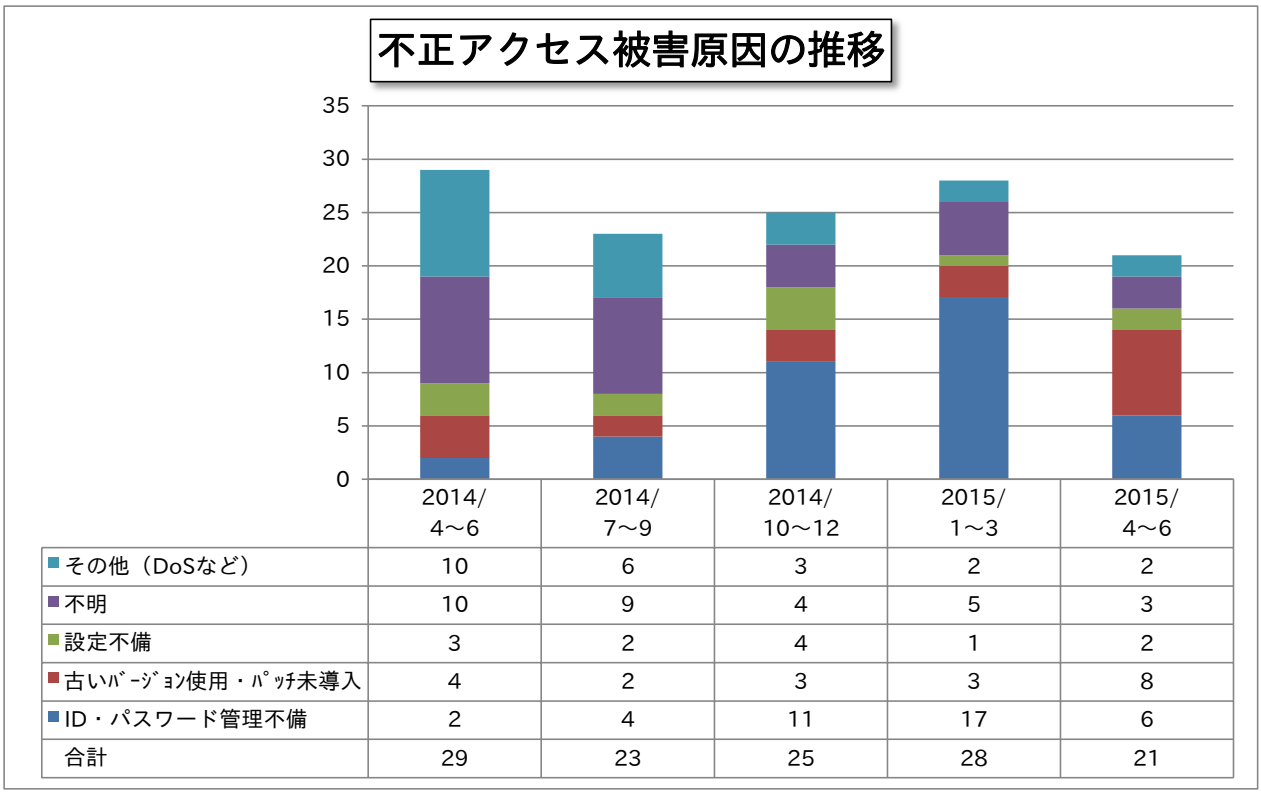



| | | 2014/4～6 | 2014/7～9 | 2014/10～12 | 2015/1～3 | 2015/4～6 |
|---|---|---|---|---|---|---|
| 被害なし | その他（被害なし） | 7 | 4 | 2 | 4 | 4 |
| 被害なし | アクセス形跡（未遂） | 1 | 0 | 1 | 2 | 5 |
| 被害あり | その他（被害あり） | 3 | 6 | 7 | 1 | 4 |
| 被害あり | 不正プログラム埋込 | 5 | 1 | 3 | 2 | 6 |
| 被害あり | なりすまし | 12 | 7 | 11 | 19 | 7 |
| 被害あり | DoS | 6 | 6 | 0 | 1 | 2 |
| 被害あり | 侵入 | 3 | 3 | 4 | 5 | 2 |
| | 合計 | 37 | 27 | 28 | 34 | 30 |

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「古いバージョン使用・パッチ未導入」が 8 件、「ID・パスワード管理不備」が 6 件、「設定不備」が 2 件等でした。前四半期と比較して「ID・パスワード管理不備」が全体の約 60.7%から約 28.6%に減少し、「古いバージョン使用・パッチ未導入」は全体の約 10.7%から約 38.1%に増加しました。

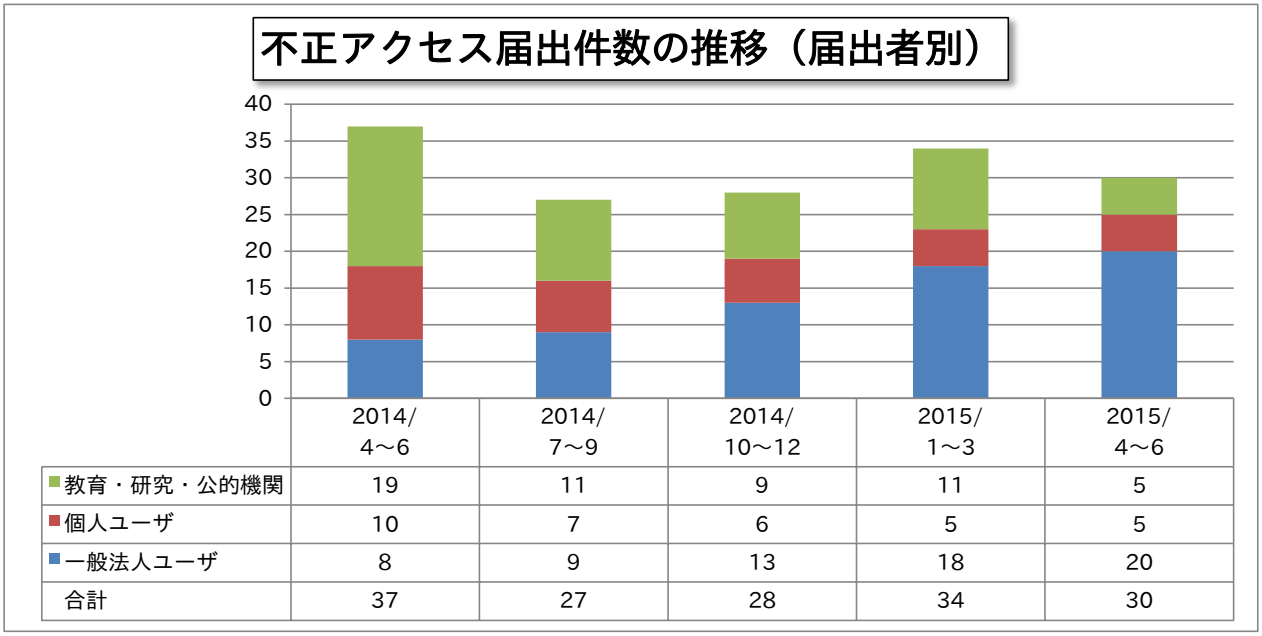



| | 2014/4～6 | 2014/7～9 | 2014/10～12 | 2015/1～3 | 2015/4～6 |
|---|---|---|---|---|---|
| その他（DoSなど） | 10 | 6 | 3 | 2 | 2 |
| 不明 | 10 | 9 | 4 | 5 | 3 |
| 設定不備 | 3 | 2 | 4 | 1 | 2 |
| 古いﾊﾞｰｼﾞｮﾝ使用・ﾊﾟｯﾁ未導入 | 4 | 2 | 3 | 3 | 8 |
| ID・パスワード管理不備 | 2 | 4 | 11 | 17 | 6 |
| 合計 | 29 | 23 | 25 | 28 | 21 |

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 20 件、「個人ユーザ」が 5 件、「教育・研究・公的機関」が 5 件でした。




| | 2014/4～6 | 2014/7～9 | 2014/10～12 | 2015/1～3 | 2015/4～6 |
|---|---|---|---|---|---|
| 教育・研究・公的機関 | 19 | 11 | 9 | 11 | 5 |
| 個人ユーザ | 10 | 7 | 6 | 5 | 5 |
| 一般法人ユーザ | 8 | 9 | 13 | 18 | 20 |
| 合計 | 37 | 27 | 28 | 34 | 30 |

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）DNS キャッシュポイズニング(*4)によって不正なサイトに誘導された。

| | |
|---|---|
| **被害の概要** | ・パソコンでウェブサイトを閲覧中、セキュリティソフトによる警告が表示された。<br>・職場のほとんどのパソコンで、同じ警告画面が表示されていることが確認できた。<br>・インターネット接続を一時中断し、DNS サーバのキャッシュ情報を確認すると不正な情報に書き換えられていることが確認できた。<br>・具体的な手口は判明していないが、ネットワークシステム構成のセキュリティ上の問題が確認でき、当該 DNS サーバに社外からアクセスが可能であったことが主な要因であったと推測される。 |
| **解説・対策** | 社内で利用している DNS サーバの情報を本来とは異なる名前解決の結果に書き換えられてしまい、不正なサイトに誘導されてしまった事例です。<br>職場のパソコンはセキュリティソフトを導入していたため、誘導先の不正なサイトを検知し、警告画面が表示されました。そのため、一時的な業務停止を余儀なくされたものの、それ以上の被害はありませんでした。<br>DNS キャッシュポイズニングの被害を受けると、ブラウザで事前に登録しておいたお気に入り（ブックマーク）からアクセスした場合でも、本来とは異なる不正なサイトへ誘導されてしまうことになります。そのため、不正なサイトに接続されても利用者が気付かず、その結果としてウイルスに感染してしまうなどの恐れがあります。<br>今回の事例では、ネットワークシステム構成に不備があったことで DNS サーバへの攻撃は許してしまったものの、パソコンにセキュリティソフトを導入していたことですぐに異変に気付くことができ、幸いにも被害を最小限に抑えることができています。<br>万が一の被害に備えて、攻撃対象となりやすいサーバへの対策はもちろんのこと、サーバへの接続を許可するパソコンについてもセキュリティソフトの導入やインストールしているソフトウェアのバージョンアップ（脆弱性の解消）といった、基本的なセキュリティ対策の実施を推奨します。 |

**・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。

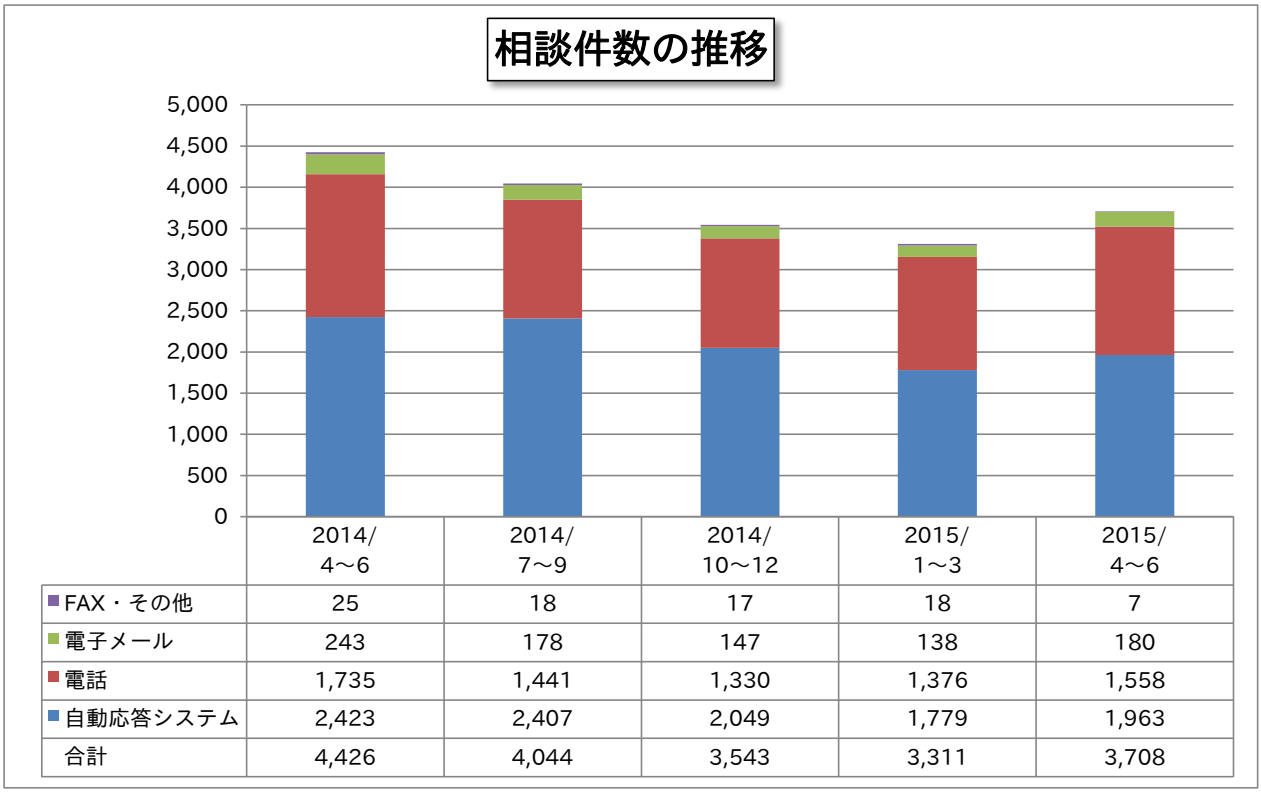
○コンピュータ不正アクセス対策基準
　平成 8 年 8 月 8 日（通商産業省告示 第 362 号）（制定）
　平成 9 年 9 月 24 日（通商産業省告示 第 534 号）（改定）
　平成 12 年 12 月 28 日（通商産業省告示 第 950 号）（最終改定）
○経済産業大臣が別に指定する者
　平成 16 年 1 月 5 日（経済産業省告示 第 3 号）

(*4) DNS キャッシュポイズニング：ドメイン名と IP アドレスとの対応を偽の情報に書き換えることで、目的のサイトへ到達できないようにしたり、本来とは異なるサイトへ誘導したりする攻撃のこと。

## 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 12%増の 3,708 件でした。



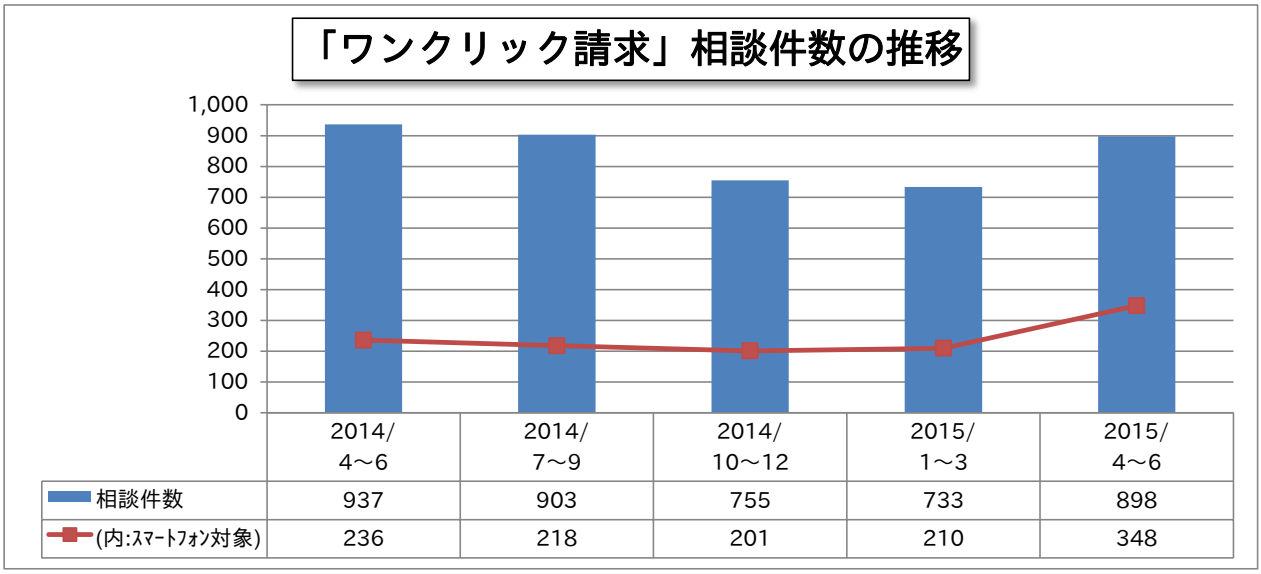

| | 2014/4～6 | 2014/7～9 | 2014/10～12 | 2015/1～3 | 2015/4～6 |
|---|---|---|---|---|---|
| FAX・その他 | 25 | 18 | 17 | 18 | 7 |
| 電子メール | 243 | 178 | 147 | 138 | 180 |
| 電話 | 1,735 | 1,441 | 1,330 | 1,376 | 1,558 |
| 自動応答システム | 2,423 | 2,407 | 2,049 | 1,779 | 1,963 |
| 合計 | 4,426 | 4,044 | 3,543 | 3,311 | 3,708 |

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 898 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 65.7%増の 348 件で過去最多でした。




| | 2014/4～6 | 2014/7～9 | 2014/10～12 | 2015/1～3 | 2015/4～6 |
|---|---|---|---|---|---|
| 相談件数 | 937 | 903 | 755 | 733 | 898 |
| (内:ｽﾏｰﾄﾌｫﾝ対象) | 236 | 218 | 201 | 210 | 348 |

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 30 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 27 件でした。

2014 年第 3 四半期（7 月～9 月）は、警察庁、総務省、JPCERT/CC 等が連携した「国際的なボットネットのテイクダウン作戦」[*5] によりウイルス感染端末が減少したと考えられ、その結果、相談件数が激減しました。しかし、その後徐々に相談件数が増加し、テイクダウン作戦前の 5 割近くまで戻っています。

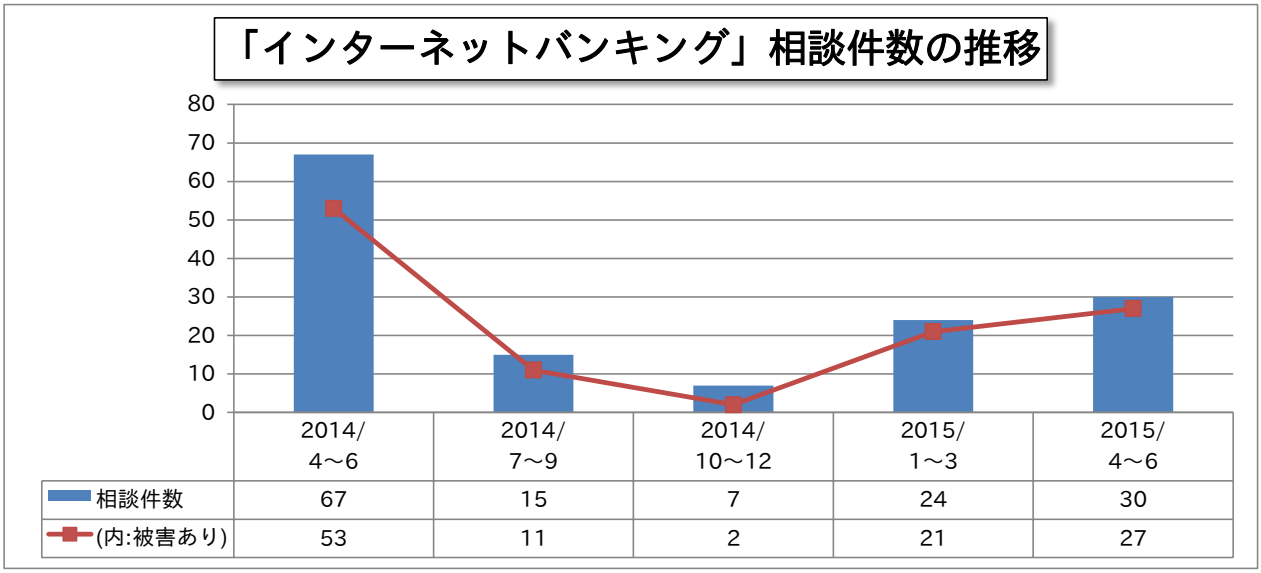



図 3-3：「インターネットバンキング」相談件数の推移

### (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の 5 倍強にあたる 31 件寄せられました。同相談のうち、実際にランサムウェアに感染していたのは全体の約 9 割の 27 件でした。

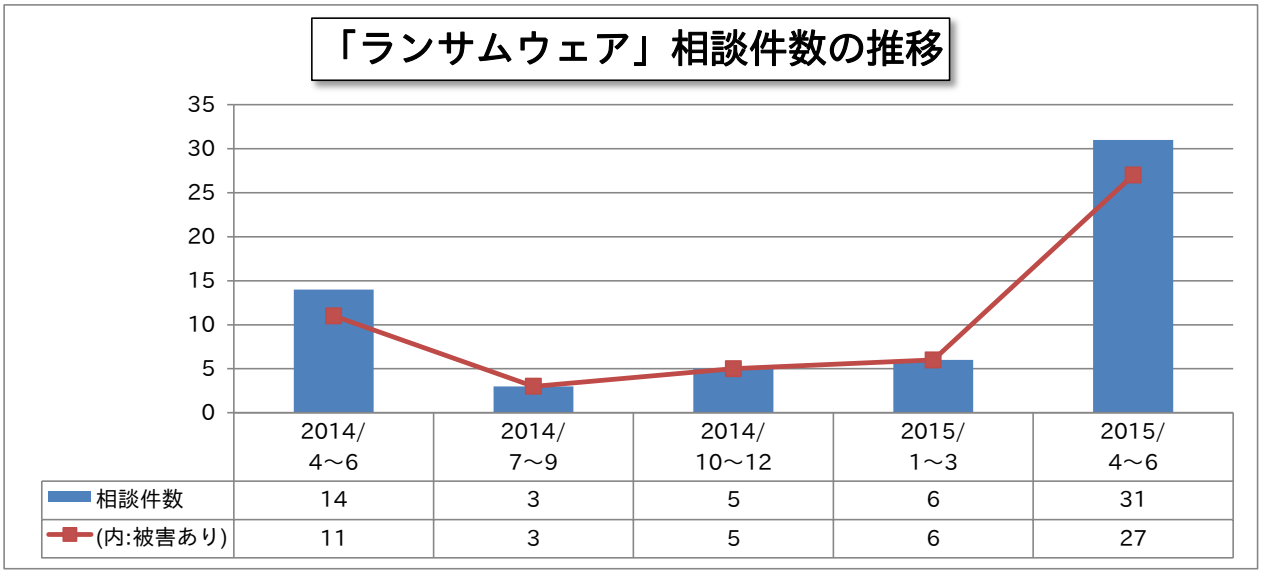



図 3-4：「ランサムウェア」相談件数の推移

[*5] 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/

### 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）パソコンで、ウイルス感染を警告する画面が出現すると同時に、音声による警告が流れてきた。**

| | |
|---|---|
| **相談の概要** | ・パソコンでウェブサイト閲覧中にあるリンクをクリックしたら、「あなたのコンピュータでウイルスが見つかりました」というウェブ画面が突然表示された。同時に、女性の音声が急に流れてきて驚いた。<br>・音声の内容は「あなたのコンピュータでウイルスが検出されました」「あなたの個人情報が危険に晒されています」「電話していただくとウイルス駆除のアドバイスをします」等といったもの。<br>・ウェブ画面上には、連絡先と思われる電話番号も表示されていた（東京地域の 03 で始まる電話番号）。<br>・表示された電話番号に電話をかけると、ウイルス駆除と称してパソコンの操作を色々と指示された。最終的には、パソコンを遠隔操作してウイルスを駆除してくれたようだ。<br>・電話の最後に、あるソフトウェアの購入を勧められたが断った。 |
| **回答** | 「ウイルスに感染した」という偽の警告画面を表示するだけでなく、音声でもメッセージを流してパソコン利用者を驚かせて電話をかけさせ、最終的にソフトウェア購入を持ちかける新しい手口です。<br>このウェブ画面で表示されるメッセージや音声による警告は、端末がウイルスに感染していなくても出現する事を確認しており、偽のメッセージと言えます。音声が聞こえても慌てる必要はなく、表示された電話場号に連絡する必要はありません。<br><br>今後も新たな手口が現れるかもしれませんが、異変や見慣れない警告を示す画面が現れても、焦ってクリックしたり連絡したりせずに冷静になることで、被害を防げる場合があります。また、セキュリティソフトを利用する事も自衛の助けになります。 |