別紙 1

# 1. コンピュータウイルス届出状況

## （1）四半期総括

2013 年第 1 四半期のウイルス届出件数※1 状況は、2012 年第 4 四半期から減少での推移となりました（図 1-1 参照）。

2013 年第 1 四半期のウイルス検出数※2 は、**W32/Mydoom が全体の 3/4 以上**を占めました（図 1-2 参照）。しかし、2012 年第 4 四半期と比較すると、**W32/Mydoom**、**W32/Netsky ともに減少傾向**でした。

**W32/Netsky** の届出を見ると、ウイルスコードが破損して感染活動が行えないものも多く検出されていました。よって、今後大幅に増加する可能性は低いと予想されます。

**W32/IRCbot** は、**2012 年第 4 四半期から大きく減少**しました。**W32/IRCbot** は、Windows やプログラムの脆弱性を悪用して感染活動を行うもので、標的型攻撃を行うための足掛かりとして使われることが多いですが、このウイルスを使わない攻撃に切り替わった可能性が考えられます。

**XM/Mailcab** は、メールソフトのアドレス帳を悪用して、自分自身のコピーをばら撒くマスメール型ウイルスでもあります。こうしたメールの添付ファイルを無造作に開いてしまう利用者が多いと、再び増加する恐れがあります。

2013 年第 1 四半期の不正プログラム検出数※3 は、主にインターネットバンキングの ID／パスワードを窃取する **Bancos**、パソコン内に裏口を仕掛ける **Backdoor**、悪意あるウェブサイトに誘導して、別のウイルスを感染させようとする **Webkit** が多く検出されました。しかし、**Bancos** 以外は全て減少傾向でした（図 1-3 参照）。

**Bancos** は、2013 年第 1 四半期では主に 2013 年 3 月に多く検知されています。3 月に多く検知された理由として、期が変わる繁忙の時期を狙い、メールを使って不特定多数に大量にばら撒いたと予想されます。

その他、偽セキュリティソフトの検知名である **Fakeav** が大幅に減少しました。これは、最近の偽セキュリティソフトを感染させる手口が、メールでの攻撃からウェブサイト閲覧によるドライブ・バイ・ダウンロード攻撃へと変遷しているからと考えられます。また、**韓国への大規模サイバー攻撃に使われたとされる不正プログラム Trojan/MBRKill（届出名：Trojan.Jokra［届出件数 2 件／検知件数 3 個］）の届出が 2013 年 3 月**に寄せられました。この不正プログラムに感染すると、**コンピュータのハードディスクの内容が消去される可能性**があります。

**韓国での被害発生と同時期に、日本にも同じ不正プログラムが少なからず流通**していたと推測されます。

ウイルスや不正プログラムの検出数を見ると、かなりのウイルスや不正プログラムがパソコンの手前まで届いていることがわかります。しかし、**ウイルス対策ソフト等を使用することで感染被害に遭わずに済んでいる**と言えます。

これらウイルスや不正プログラムは、そのほとんどがメールを感染経路として送られてくるものです（表 1-2 参照）。対策として、**ウイルス対策ソフト等を適切に使うことで感染はかなりの確度で防ぐ**ことができます。また、**メールの添付ファイルの開封には注意**するとともに、**身に覚えのないメールは読まずに捨てるべき**と言えます。**ドライブ・バイ・ダウンロード攻撃については、OS やアプリケーションソフトの脆弱性を悪用**するため、古いバージョンのままにしておかず、**常に最新の状態に保つことが一番の対策**になります。

※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たもの。

※2 検出数 ： 届出にあたり届出者から寄せられたウイルスの発見数（個数）。

※3 ここでいう「不正プログラム検出数」とは、IPA に届出られたものの中から「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当てはまらない不正なプログラムについて集計したものです。
コンピュータウイルス対策基準：平成 12 年 12 月 28 日（通商産業省告示 第 952 号）（最終改定）（平成 13 年 1 月 6 日より、通商産業省は経済産業省に移行しました。）

「コンピュータウイルス対策基準」（経済産業省）
http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm

## （2）ウイルス感染被害届出

2013 年第 1 四半期のウイルス感染による被害届出は 0 件でした。
パソコン利用者には、引き続きウイルス対策などでセキュリティ維持の継続をお願いいたします。

## （3）届出件数

2013 年第 1 四半期［1 月～3 月］の届出件数は **1,803 件**となりました。下記グラフ（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。

図 1-1 で示すように、届出件数は 2012 年第 4 四半期の **2,456 件**から **653 件の減少**での推移となりました。

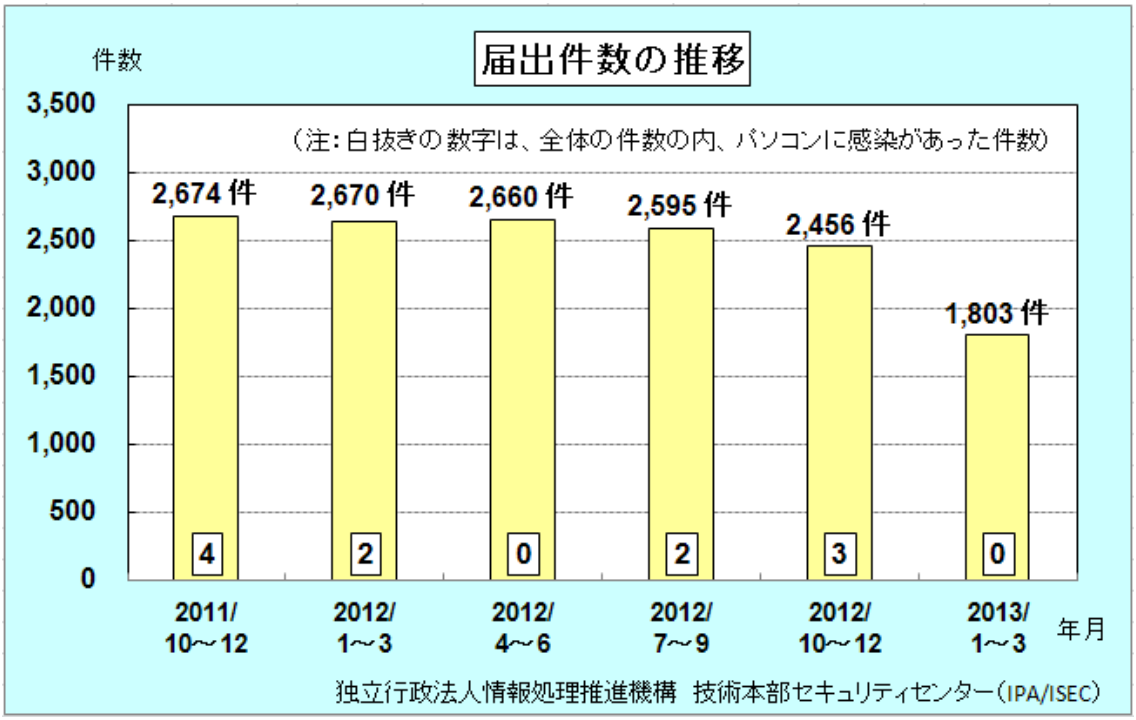


図 1-1：届出件数の四半期毎推移

### （4）ウイルス検出数

2013 年第 1 四半期のウイルス検出数は **56,210 個**と、2012 年第 4 四半期の **67,533 個**から **11,323 個の減少**での推移となりました（図 1-3 参照）。

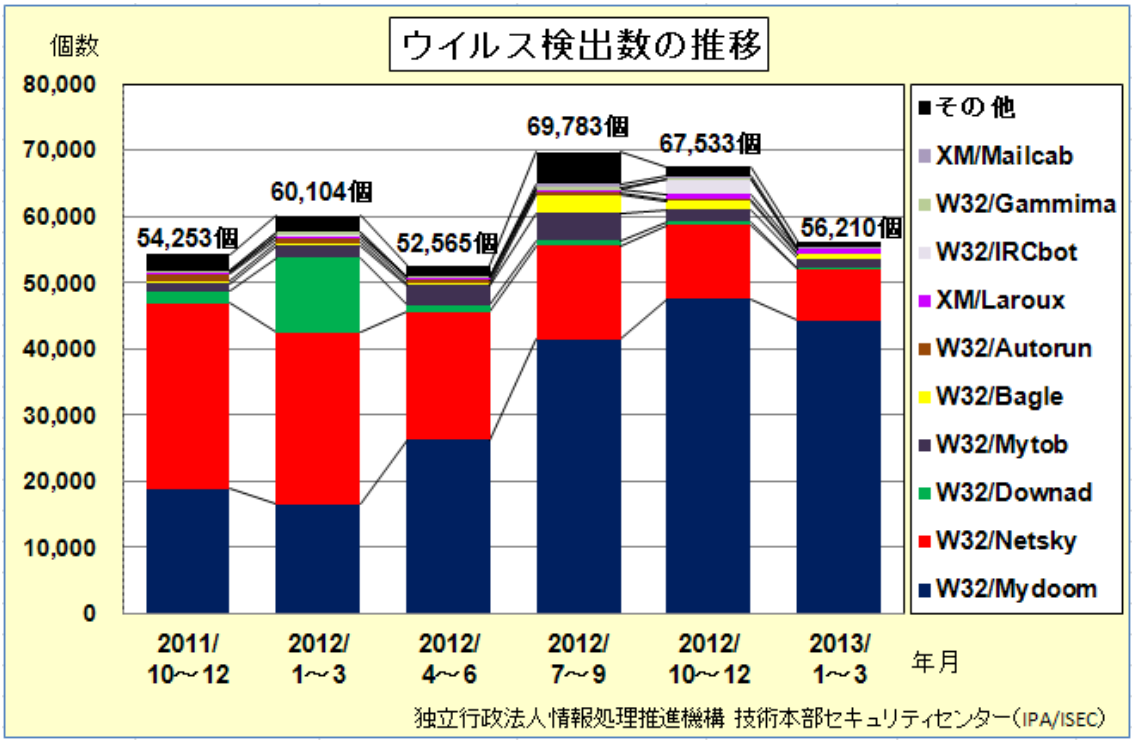


図 1-2：ウイルス検出数の推移

### （5）不正プログラム検出数

2013 年第 1 四半期の不正プログラム上位 10 個の検出数は **23,617 個**と、2012 年第 4 四半期の **37,480 個**から、**13,863 個の減少**となりました。

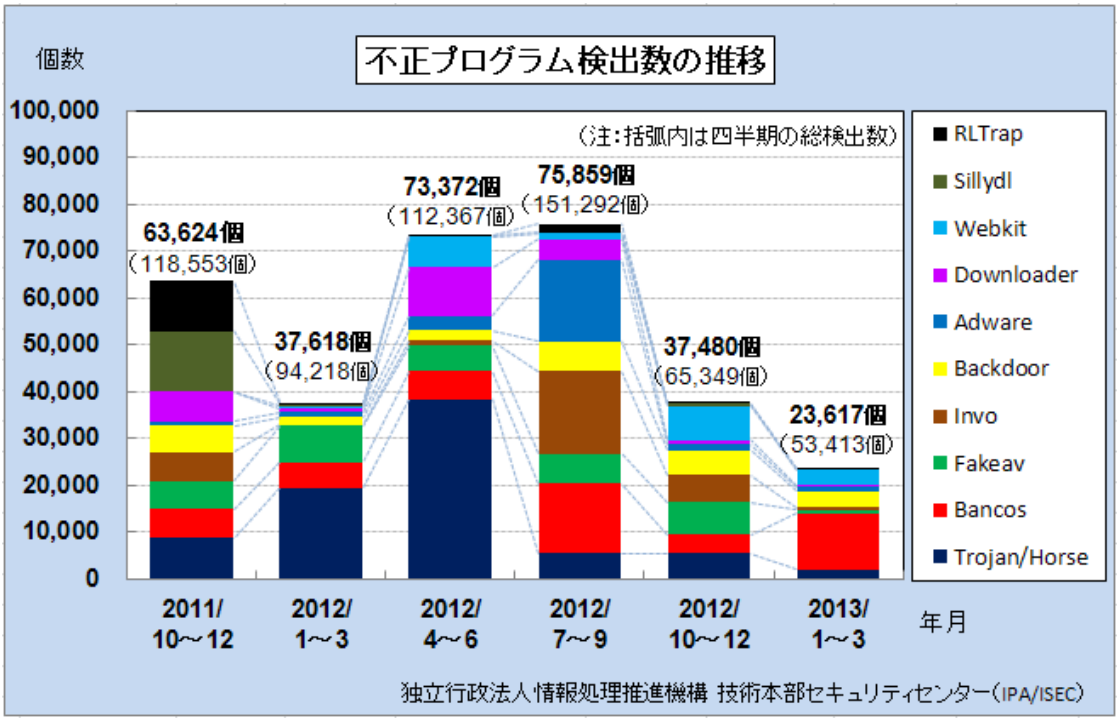


図 1-3：不正プログラム検出数の推移

## （6）2013 年第 1 四半期の届出ウイルス

ウイルスの種類は 76 種類で、Windows/DOS ウイルス 1,589 件、スクリプトウイルス及びマクロウイルス 197 件、携帯端末のウイルス 17 件でした。

※件数には亜種の届出を含む　　(※)印は 2013 年第 1 四半期の新種ウイルス

| i) Windows/DOS ウイルス | 届出件数 |
|---|---|
| W32/Netsky | 440 |
| W32/Mydoom | 367 |
| W32/Autorun | 129 |
| W32/Mytob | 125 |
| W32/Bagle | 114 |
| W32/Downad | 106 |
| W32/Klez | 58 |
| W32/Mumu | 42 |
| W32/Gammima | 23 |
| W32/Virut | 17 |
| W32/Funlove | 15 |
| W32/IRCbot | 12 |
| W32/Sality | 11 |
| Perl/Santy | 9 |
| W32/Antinny | 9 |
| W32/Lovgate | 9 |
| W32/Palevo | 9 |
| Wscript/Kakworm | 9 |
| W32/Fujacks | 8 |
| W32/Fakerecy | 5 |
| W32/Looked | 5 |
| W32/Badtrans | 4 |
| W32/Parite | 4 |
| W32/Bacterra | 3 |
| W32/Harakit | 3 |
| W32/Myparty | 3 |
| W32/Ramnit | 3 |
| W32/Stration | 3 |
| W32/Stuxnet | 3 |
| W32/Witty (※) | 3 |
| W32/Zafi | 3 |
| Stoned | 2 |
| W32/Allaple | 2 |
| W32/Imaut | 2 |
| W32/Mywife | 2 |
| W32/Sober | 2 |
| W32/Sobig | 2 |
| W32/Waledac | 2 |
| Diskkiller | 1 |
| W32/Aliz | 1 |
| W32/Brid | 1 |
| W32/CIH | 1 |
| W32/Chir | 1 |
| W32/Dorkbot | 1 |
| W32/Dupator | 1 |
| W32/Gaobot | 1 |
| W32/Hybris | 1 |
| W32/Lunalight | 1 |

| i) Windows/DOS ウイルス | 届出件数 |
|---|---|
| W32/Mabutu | 1 |
| W32/Magistr | 1 |
| W32/Nimda | 1 |
| W32/Opaserv | 1 |
| W32/Rontokbro | 1 |
| W32/Sohanad | 1 |
| W32/Traxg | 1 |
| W32/Valla | 1 |
| W32/Wapomi | 1 |
| W32/Whybo | 1 |
| W32/Xpaj (※) | 1 |
| 小計　(59 種類) | 1,589 |

| スクリプトウイルス | 届出件数 |
|---|---|
| VBS/LOVELETTER | 3 |
| VBS/SST | 3 |
| VBS/Solow | 3 |
| VBS/Freelink | 2 |
| VBS/Internal | 1 |
| VBS/Redlof | 1 |
| 小計　(6 種類) | 13 |

| マクロウイルス | 届出件数 |
|---|---|
| XM/Laroux | 100 |
| XM/Mailcab | 70 |
| XF/Sic | 5 |
| XF/Helpopy | 3 |
| W97M/Relax | 2 |
| X97M/Divi | 2 |
| W97M/Melissa | 1 |
| W97M/X97M/P97M/Tristate | 1 |
| 小計　(8 種類) | 184 |

| ii)携帯端末 | 届出件数 |
|---|---|
| AndroidOS/Lotoor | 14 |
| AndroidOS/Fakeinst | 2 |
| AndroidOS/Rootcage | 1 |
| 小計　(3 種類) | 17 |

| iii) Macintosh | 届出件数 |
|---|---|
| なし | |

| iv) OSS（OpenSourceSoftware）：Linux・BSD を含む、UNIX | 届出件数 |
|---|---|
| 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。

注）ウイルス名欄での各記号はそれぞれ下記の内容を示す。

| 記号 | 対象ウイルス |
|---|---|
| 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 |
| XF | Microsoft Excel95、97 で動作するウイルス。（ExcelFormula の略） |

## （7）2013 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/Witty（ウィティ） 2013 年 1 月

このウイルスは、ネットワークよりセキュリティソフト「BlackICE」の脆弱性を悪用して感染します。

感染すると、UDP ポート 4000 を通じてランダムな IP アドレスとポートに、自分自身のコピーを送信して感染を拡大します。

このウイルスはメモリ上だけに存在するため、コンピュータを再起動すると感染活動を中止します。

（2）W32/Xpaj（エックスピーエージェー） 2013 年 1 月

このウイルスは、リムーバブルドライブを介して感染を拡大するウイルスです。

感染すると、 自分自身を暗号化して、.dll、.exe、.scr、.sys の各ファイルに感染します。また、利用者を悪意あるウェブサイトへ誘導します。

このウイルスの亜種によっては、ハードディスクのマスターブートレコードに感染します。そのため、OS が動作する前にウイルスが起動するので、駆除が困難な場合があります。

## （8）届出者別件数（表 1-1）

| | 2011/ 10～12 | 2012/ 1～3 | 2012/ 4～6 | 2012/ 7～9 | 2012/ 10～12 | 2013/ 1～3 |
|---|---|---|---|---|---|---|
| 一般法人 | 2,524 | 2,523 | 2,580 | 2,506 | 2,367 | 1,946 |
| | (94.4%) | (95.6%) | (97.0%) | (96.6%) | (96.4%) | (97.8%) |
| 個人 | 0 | 0 | 0 | 3 | 4 | 0 |
| | (0.0%) | (0.0%) | (0.0%) | (0.1%) | (0.2%) | (0.0%) |
| 教育機関 | 150 | 117 | 80 | 86 | 85 | 43 |
| | (5.6%) | (4.4%) | (3.0%) | (3.3%) | (3.5%) | (2.2%) |
| 合計 | 2,674 | 2,640 | 2,660 | 2,595 | 2,456 | 1,989 |

### （9）感染（発見）経路別件数（表 1-2）　（※）ホームページからの感染を含む

| | 2011/ 10～12 | 2012/ 1～3 | 2012/ 4～6 | 2012/ 7～9 | 2012/ 10～12 | 2013/ 1～3 |
|---|---|---|---|---|---|---|
| メール | 2,413 | 2,391 | 2,434 | 2,336 | 2,230 | 1,796 |
| | (90.2%) | (90.6%) | (91.5%) | (90.0%) | (90.8%) | (90.3%) |
| ダウンロードファイル（※） | 29 | 26 | 14 | 23 | 29 | 23 |
| | (1.1%) | (1.0%) | (0.5%) | (0.9%) | (1.2%) | (1.2%) |
| 外部からの媒体 | 0 | 1 | 0 | 2 | 3 | 2 |
| | (0.0%) | (0.0%) | (0.0%) | (0.1%) | (0.1%) | (0.1%) |
| ネットワーク | 230 | 220 | 212 | 233 | 194 | 168 |
| | (8.6%) | (8.3%) | (8.0%) | (9.0%) | (7.9%) | (8.4%) |
| 不明・その他 | 2 | 2 | 0 | 1 | 0 | 0 |
| | (0.1%) | (0.1%) | (0.0%) | (0.0%) | (0.0%) | (0.0%) |
| 合計 | 2,674 | 2,640 | 2,660 | 2,595 | 2,456 | 1,989 |

### （10）感染台数（表 1-3）

| | 2011/ 10～12 | 2012/ 1～3 | 2012/ 4～6 | 2012/ 7～9 | 2012/ 10～12 | 2013/ 1～3 |
|---|---|---|---|---|---|---|
| 0 台 | 2,670 | 2,638 | 2,660 | 2,593 | 2,453 | 1,989 |
| | (99.9%) | (99.9%) | (100.0%) | (99.9%) | (99.9%) | (100.0%) |
| 1 台 | 2 | 1 | 0 | 1 | 2 | 0 |
| | (0.1%) | (0.0%) | (0.0%) | (0.0%) | (0.1%) | (0.0%) |
| 2～4 台 | 0 | 1 | 0 | 0 | 1 | 0 |
| | (0.0%) | (0.0%) | (0.0%) | (0.0%) | (0.0%) | (0.0%) |
| 5～9 台 | 1 | 0 | 0 | 1 | 0 | 0 |
| | (0.0%) | (0.0%) | (0.0%) | (0.0%) | (0.0%) | (0.0%) |
| 10～19 台 | 0 | 0 | 0 | 0 | 0 | 0 |
| | (0.0%) | (0.0%) | (0.0%) | (0.0%) | (0.0%) | (0.0%) |
| 20～49 台 | 1 | 0 | 0 | 0 | 0 | 0 |
| | (0.0%) | (0.0%) | (0.0%) | (0.0%) | (0.0%) | (0.0%) |
| 50～9,999 台 | 0 | 0 | 0 | 0 | 0 | 0 |
| | (0.0%) | (0.0%) | (0.0%) | (0.0%) | (0.0%) | (0.0%) |
| 10,000 台以上 | 0 | 0 | 0 | 0 | 0 | 0 |
| | (0.0%) | (0.0%) | (0.0%) | (0.0%) | (0.0%) | (0.0%) |
| 合計 | 2,674 | 2,640 | 2,660 | 2,595 | 2,456 | 1,989 |

**・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。

〇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）
〇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）