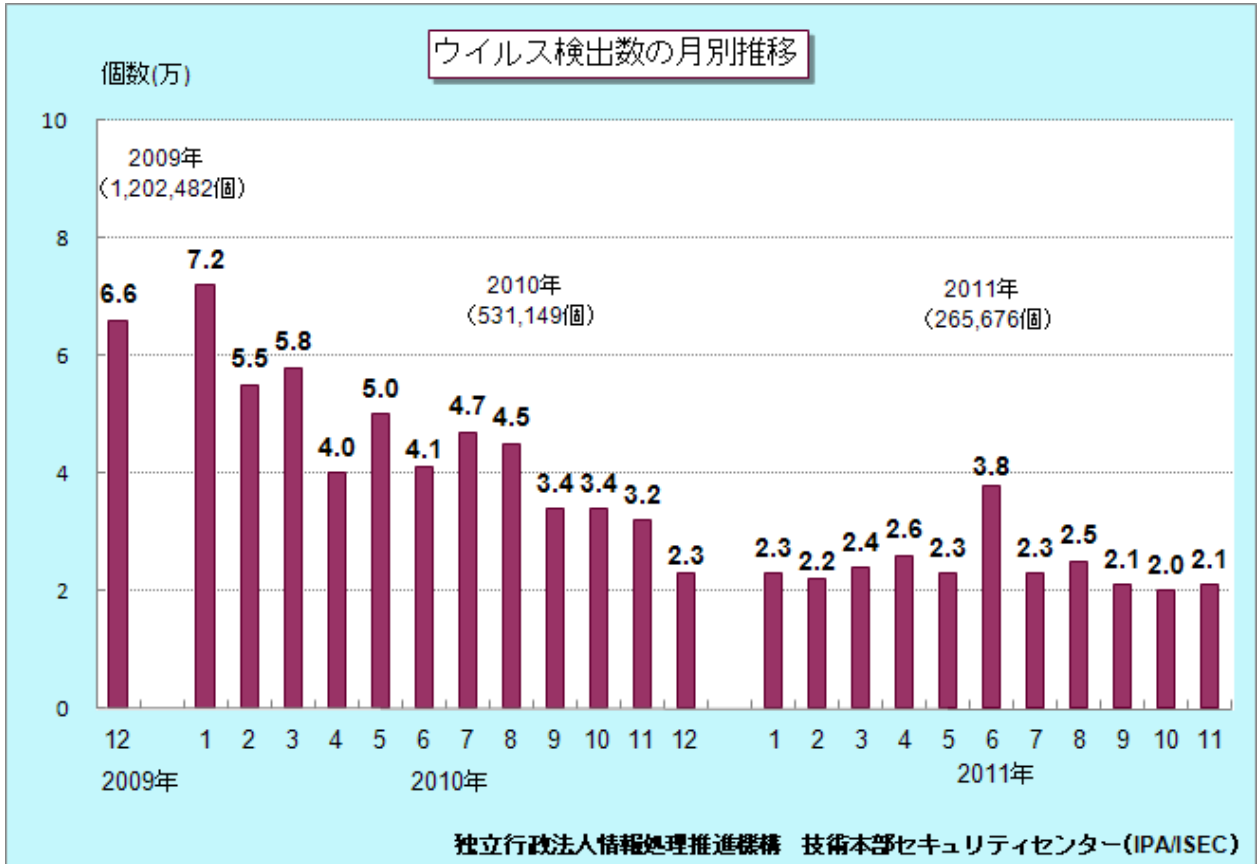
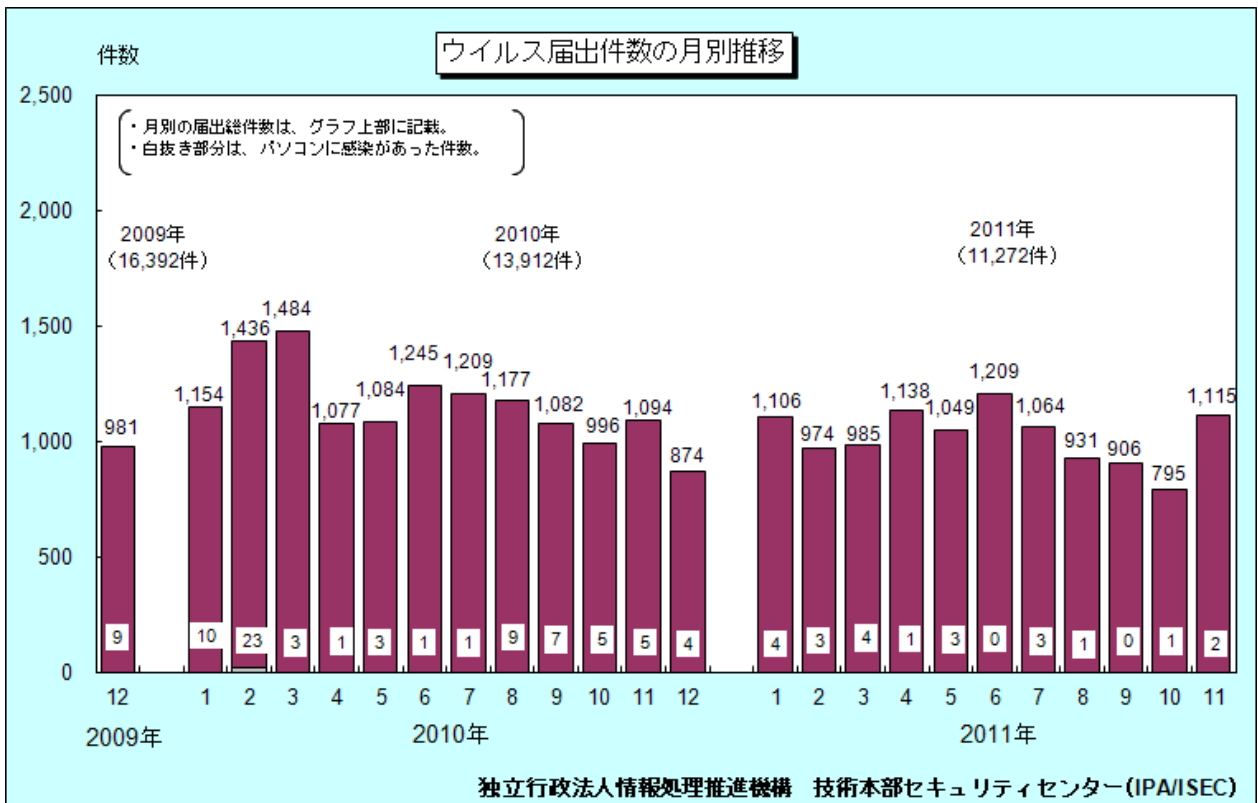


コンピュータウイルスの届出状況 [2011年11月分] について

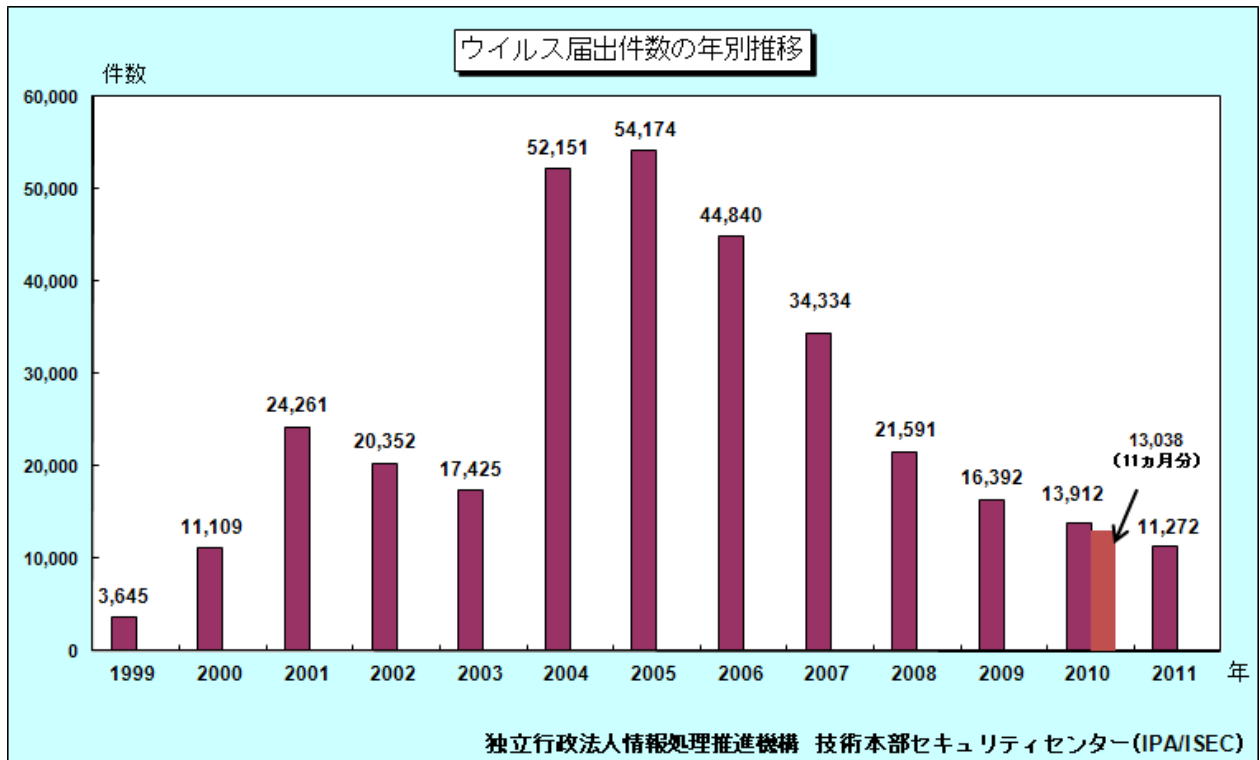
1. ウイルス検出数の月別推移



2. ウイルス届出件数の月別推移



3. ウイルス届出件数の年別推移



4. 11月の届出ウイルス

ウイルスの種類は 61 種類で、Windows/DOS ウイルス 1,003 件、スクリプトウイルス及びマクロウイルス 98 件、携帯端末のウイルス 14 件でした。

i) Windows

(※)印は今月の新種ウイルス

| Windows/DOS ウイルス | 届出件数 | Windows/DOS ウイルス | 届出件数 |
|-------------------|------|--|-------|
| W32/Mydoom | 222 | W32/Remadm | 1 |
| W32/Netsky | 216 | W32/SQLSlammer | 1 |
| W32/Autorun | 125 | W32/Whybo | 1 |
| W32/Downad | 79 | 小計 (46 種類) | 1,003 |
| W32/Bagle | 70 | | |
| W32/Mytob | 63 | スクリプトウイルス | 届出件数 |
| W32/Sality | 36 | VBS/Freelink | 6 |
| W32/Mumu | 32 | VBS/Redlof | 2 |
| W32/Lovgate | 32 | VBS/SST | 2 |
| W32/Gammima | 20 | VBS/Solow | 2 |
| W32/Virut | 19 | VBS/LOVELETTER | 1 |
| W32/Klez | 15 | 小計 (5 種類) | 13 |
| W32/Ramnit | 9 | | |
| W32/Mywife | 8 | マクロウイルス | 届出件数 |
| W32/IRCbot | 5 | XM/Laroux | 39 |
| W32/Dotex | 5 | XM/Slide | 37 |
| W32/Fakerecy | 4 | W97M/Relax | 3 |
| W32/Palevo | 4 | W97M/Melissa | 2 |
| W32/Antinny | 3 | WM/Wazzu | 1 |
| W32/Funlove | 3 | WM/Concept | 1 |
| W32/Almanahe | 2 | WM/Cap | 1 |
| W32/Nuwar | 2 | XF/Helpopy | 1 |
| W32/Stration | 2 | 小計 (8 種類) | 85 |
| W32/Fbound | 2 | | |
| W32/Fujacks | 2 | ii) 携帯端末 | 届出件数 |
| W32/Nimda | 2 | AndroidOS/Lotoor | 10 |
| W32/Allaple | 2 | AndroidOS/Rootcage (※) | 4 |
| W32/Traxg | 1 | 小計 (2 種類) | 14 |
| W32/Wapomi | 1 | | |
| W32/Morto (※) | 1 | iii) Macintosh | |
| W32/Chir | 1 | なし | |
| W32/Pykspace (※) | 1 | | |
| W32/MSBlaster | 1 | iv) OSS (OpenSourceSoftware) : Linux・BSD | |
| W32/Myparty | 1 | を含む、UNIX | |
| W32/Zafi | 1 | なし | |
| W32/Gaobot | 1 | (参考) | |
| Wscript/Fortnight | 1 | ・ Windows/DOS ウイルス | |
| W32/Areses | 1 | Windows、MS-DOS 環境下で動作するウイルス。 | |
| W32/Bacterra | 1 | ・ マクロウイルス | |
| W32/Dronzho | 1 | Microsoft Word や Microsoft Excel などのマクロ | |
| W32/Imaut | 1 | 機能を悪用するウイルス。 | |
| W32/Induc | 1 | ・ スクリプトウイルス | |
| W32/Magistr | 1 | 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。 | |

備考：件数には亜種の届出を含む

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) |

5. 11 月に IPA に初めて届出のあったウイルスの概要

(1) AndroidOS/Rootcage (ルートケージ)

このウイルスは、モバイル端末用の AndroidOS を感染対象としたウイルスです。

感染すると、モバイル端末の root 権限(※1)を取得され、モバイル端末の情報を盗み取り、外部に情報を送信します。

(※1) 管理者権限のこと。この権限を取得すると、モバイル端末のほとんどの設定が変更可能になります。

(2) W32/Morto (モート)

このウイルスは、RDP(※2)を使ってアクセス可能なパソコンに自分自身をコピーして感染を拡大します。

感染すると、tcp ポート 3389 を通じて、Windows のリモートデスクトップ機能が有効なパソコンを探します。有効なパソコンが見つかったら、パスワードクラッキングを駆使して侵入を試みます。

(※2) Remote Desktop Protocol : 遠隔でパソコンの操作をする為に使われるプロトコルのこと。

(3) W32/Pykspa (ピーワイケースパ)

このウイルスは、Skype(※3)インスタントメッセージングやリムーバブルドライブを介して感染を拡大します。

感染すると、特定のプロセスを停止したり、セキュリティ関連サイトへのアクセスを妨害するために、Hosts ファイルを改ざんしたりします。

(※3) スカイプ: 日本マイクロソフト社が提供しているインターネット電話サービス。音声通話やチャット、ファイル転送などが行えます。

6. 届出者別件数

一番多い届出は、一般法人ユーザからのもので、約 96%を占めています。

| 届出者 | 届出件数 | | | | | |
|---------|----------|-------|--------------|-------|----------------|-------|
| | 2011年11月 | | 2011年10月(前月) | | 2010年11月(前年同月) | |
| 一般法人ユーザ | 1,065 | 95.5% | 741 | 93.2% | 1,038 | 94.9% |
| 個人ユーザ | 0 | 0.0% | 0 | 0.0% | 1 | 0.1% |
| 教育機関 | 50 | 4.5% | 54 | 6.8% | 55 | 5.0% |
| 合計 | 1,115 | | 795 | | 1,094 | |

7. 感染(発見)経路別件数

メールにより感染(発見)したケースが最も多く、届出件数の約90%を占めています。

| 感染(発見)経路 | 届 出 件 数 | | | | | |
|-----------|----------|-------|--------------|-------|----------------|-------|
| | 2011年11月 | | 2011年10月(前月) | | 2010年11月(前年同月) | |
| メール | 1,006 | 90.2% | 722 | 90.8% | 1,041 | 95.2% |
| ダウンロード(※) | 15 | 1.3% | 5 | 0.6% | 0 | 0.0% |
| 外部からの媒体 | 0 | 0.0% | 0 | 0.0% | 4 | 0.4% |
| ネットワーク | 93 | 8.3% | 68 | 8.6% | 46 | 4.2% |
| 不明・その他 | 1 | 0.1% | 0 | 0.0% | 3 | 0.3% |
| 合計 | 1,115 | | 795 | | 1,094 | |

(※)ホームページからの感染を含む

8. 感染台数

| 感 染 台 数 | 届 出 件 数 | | | | | |
|-------------|----------|-------|--------------|-------|----------------|-------|
| | 2011年11月 | | 2011年10月(前月) | | 2010年11月(前年同月) | |
| 0台 | 1,113 | 99.8% | 794 | 99.9% | 1,089 | 99.5% |
| 1台 | 1 | 0.1% | 1 | 0.1% | 4 | 0.4% |
| 2台以上 5台未満 | 0 | 0.0% | 0 | 0.0% | 0 | 0.0% |
| 5台以上 10台未満 | 1 | 0.1% | 0 | 0.0% | 0 | 0.0% |
| 10台以上 20台未満 | 0 | 0.0% | 0 | 0.0% | 0 | 0.0% |
| 20台以上 50台未満 | 0 | 0.0% | 0 | 0.0% | 0 | 0.0% |
| 50台以上 | 0 | 0.0% | 0 | 0.0% | 1 | 0.1% |
| 合計 | 1,115 | | 795 | | 1,094 | |

・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

- ・通商産業省告示第139号 平成2年4月10日制定
- ・通商産業省告示第429号 平成7年7月7日改訂
- ・通商産業省告示第535号 平成9年9月24日改訂
- ・通商産業省告示第952号 平成12年12月28日改訂
- ・経済産業省告示第2号 平成16年1月5日改訂

■お問い合わせ先

IPA 技術本部 セキュリティセンター 加賀谷/宮本

Tel:03-5978-7591 Fax:03-5978-7518

E-mail: isec-info@jpa.go.jp