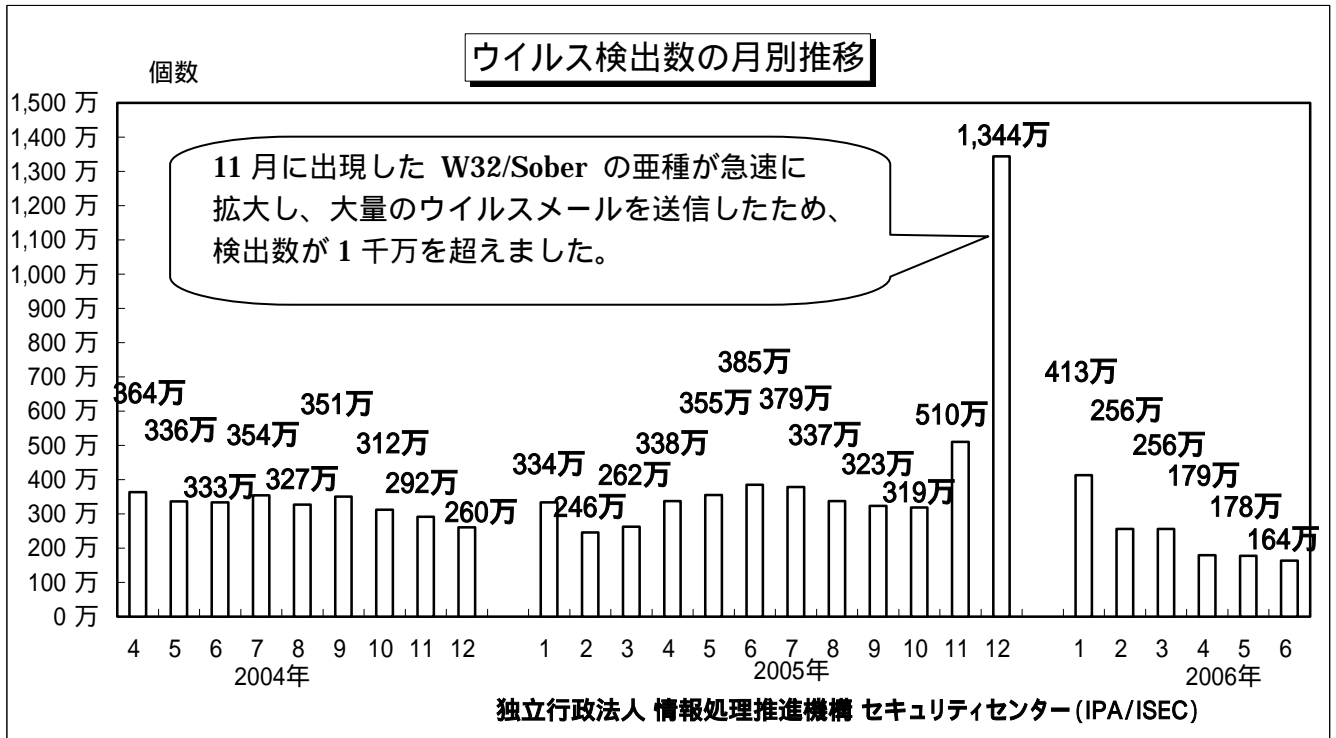


コンピュータウイルスの届出状況 [2006年6月分] について

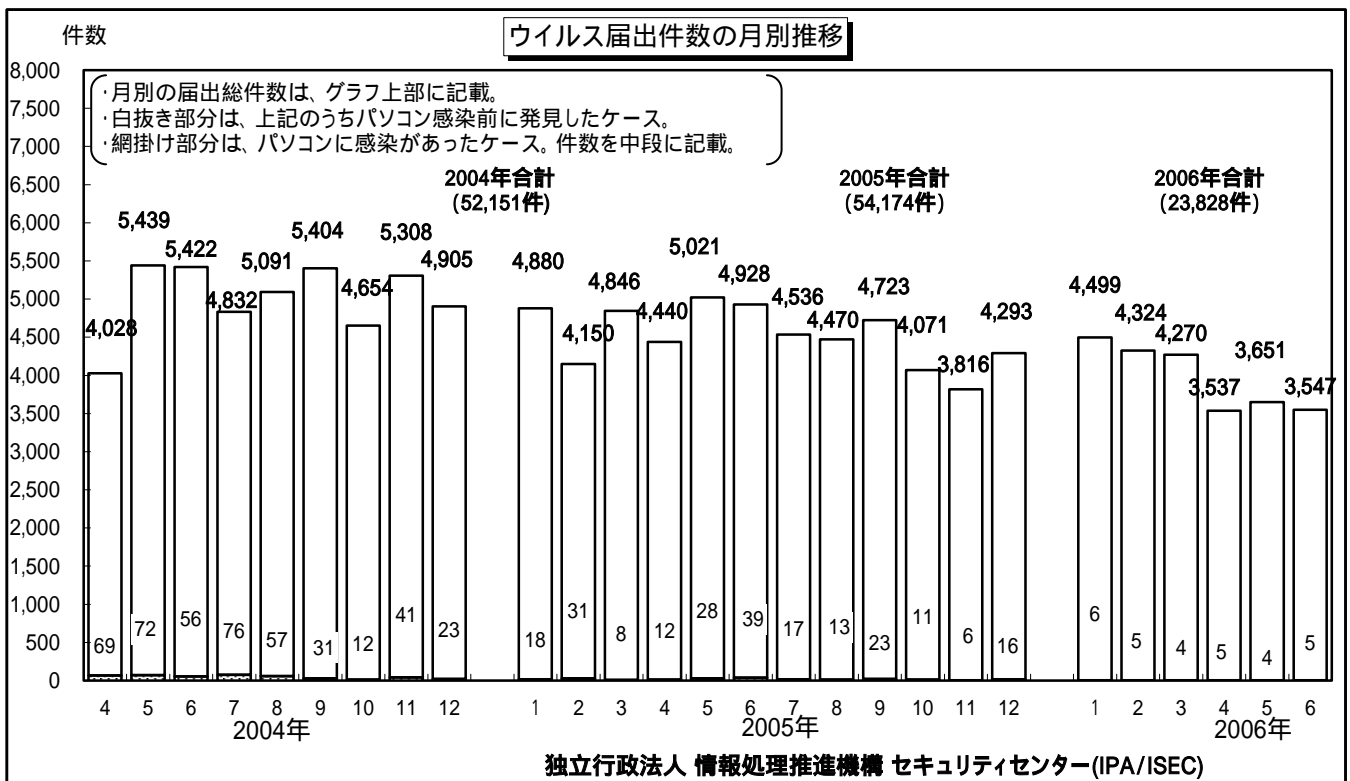
・ウイルス届出の詳細

1. ウイルス検出数の月別推移

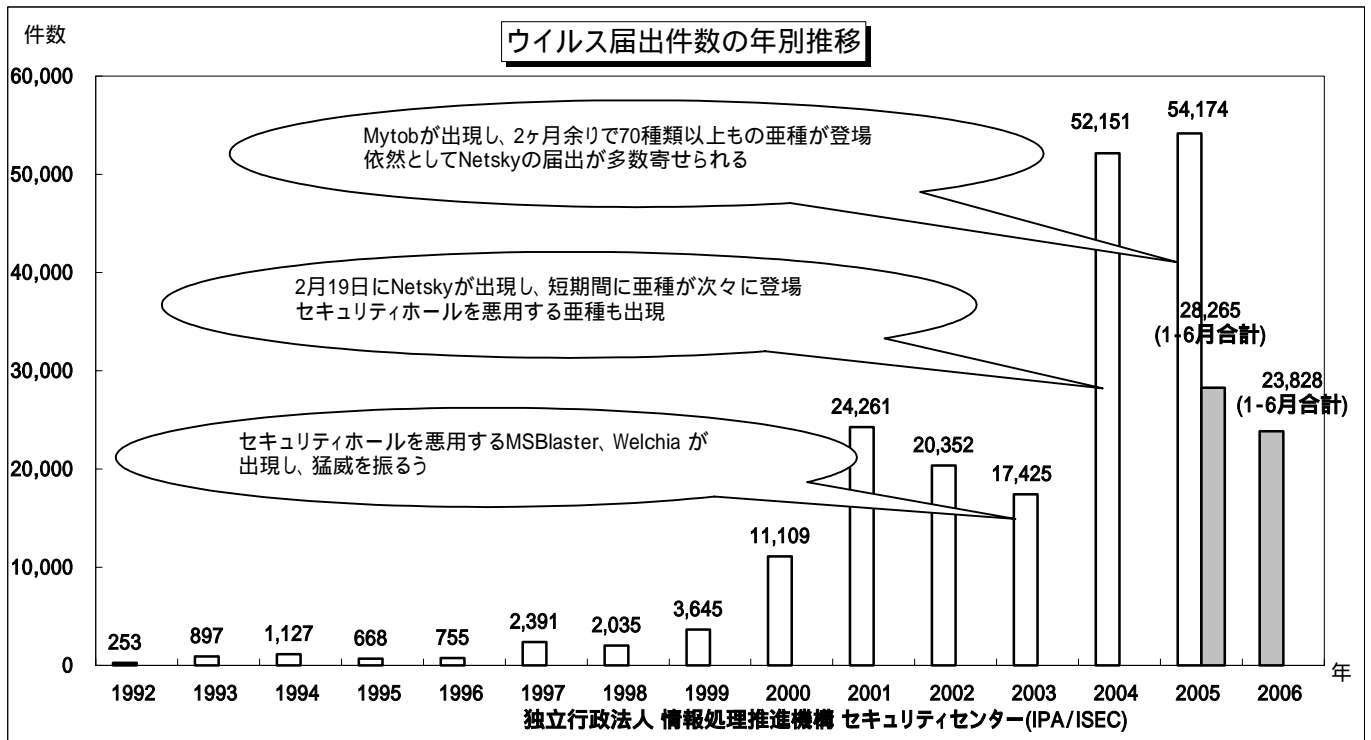


検出数は2004年4月より集計を開始

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



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 | MSEXCEL95、97 (ExcelMacro の略) |
| WM | MSWORD95、97 (WordMacro の略) |
| W97M | MSWORD97 (Word97Macro の略) |
| X97M | MSEXCEL97 (Excel97Macro の略) |
| VBS | VisualBasicScript で記述 |
| Wscript | WindowsScriptingHost 環境下で動作 (VBS を除く) |
| JS | JavaScript で記述 |
| XF | MSEXCEL95、97 で動作するウイルス。(ExcelFormula の略) |
| Linux | Linux 環境下で動作 |
| FreeBSD | FreeBSD 環境下で動作 |
| Perl | Perl で記述 |
| OSX | Macintosh OS X 環境下で動作 |

5. 6月にIPAに初めて届出のあったウイルスの概要

(1) W32/Ranchneg (ランチネグ)

このウイルスは、メールの添付ファイルを介して感染を拡大します。

感染すると、Windows のシステムフォルダに自分自身のコピーを作成します。また、パソコン起動時にウイルスが動作するように、レジストリを改ざんします。

その後、パソコン内に保存されているアドレス帳や文書ファイルなどからメールアドレスを収集し、取得できたアドレス宛に、自分自身を添付したウイルスメールを送信し、感染を拡大します。さらに、バックドアを作成し、外部からの指令を受け取るように設定します。

(2) W32/Looked (ルックド)

このウイルスは、ネットワーク共有を介して感染を拡大します。

感染すると、Windows フォルダに自分自身のコピーを作成します。また、パソコン起動時にウイルスが動作するように、レジストリを改ざんします。

その後、パソコン内の拡張子が「.exe」のファイルに自分自身を追記することで感染します。また、ネットワーク共有でアクセスできる「.exe」ファイルにも感染します。さらに、特定のセキュリティ対策製品の動作を強制終了させます。

(3) W32/Sixem (シゼム)

このウイルスは、メールの添付ファイルを介して感染を拡大します。

感染すると、Windows のシステムフォルダに自分自身のコピーを作成します。また、パソコン起動時にウイルスが動作するように、レジストリを改ざんします。

その後、パソコン内に保存されているアドレス帳などからメールアドレスを収集し、取得できたアドレス宛に、自分自身を添付したウイルスメールを送信し、感染を拡大します。さらに、セキュリティ対策製品を含む、複数のプロセスを停止させます。

(4) W32/Bacterra (バクテッラ)

このウイルスは、ファイル交換ソフト「eDonkey2000」を介して感染を拡大します。

感染すると、パソコン内の特定のフォルダに自分自身のコピーを作成します。作成後、そのフォルダが共有されるように、eDonkey2000 の設定ファイルを変更し、ファイル交換ソフトのユーザがダウンロードできるようにすることで、感染を拡大します。

(5) JS/Yamanner (ヤマナー)

このウイルスは、Yahoo! Mail サービスのセキュリティホールを悪用することで、感染を拡大します。

感染すると、Yahoo! Mail で送受信したメールからメールアドレスを収集し、取得できたアドレス宛に、自分自身を添付したウイルスメールを送信し、感染を拡大します。また、収集したアドレスを特定のサイトに送信します。

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92%を占めています。

| 届出者 | 届出件数 | | | | | |
|---------|---------|-------|-------------|-------|---------------|-------|
| | 2006年6月 | | 2006年5月(前月) | | 2005年6月(前年同月) | |
| 一般法人ユーザ | 3,270 | 92.2% | 3,408 | 93.3% | 4,461 | 90.5% |
| 個人ユーザ | 70 | 2.0% | 49 | 1.3% | 168 | 3.4% |
| 教育機関 | 207 | 5.8% | 194 | 5.3% | 299 | 6.1% |
| 合計 | 3,547 | | 3,651 | | 4,928 | |

7. 感染経路別件数

メールにより感染したケースが最も多く、届出件数の約98%を占めています。

| 感染経路 | 届出件数 | | | | | |
|-----------|---------|-------|-------------|-------|---------------|-------|
| | 2006年6月 | | 2006年5月(前月) | | 2005年6月(前年同月) | |
| メール | 3,460 | 97.5% | 3,552 | 97.3% | 4,850 | 98.4% |
| ダウンロード() | 2 | 0.1% | 0 | 0.0% | 9 | 0.2% |
| 外部からの媒体 | 1 | 0.0% | 0 | 0.0% | 4 | 0.1% |
| ネットワーク | 80 | 2.3% | 98 | 2.7% | 57 | 1.2% |
| 不明・その他 | 4 | 0.1% | 1 | 0.0% | 8 | 0.2% |
| 合計 | 3,547 | | 3,651 | | 4,928 | |

()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 | | | | | |
|-------------|---------|-------|-------------|-------|---------------|-------|
| | 2006年6月 | | 2006年5月(前月) | | 2005年6月(前年同月) | |
| 0台 | 3,542 | 99.9% | 3,647 | 99.9% | 4,889 | 99.2% |
| 1台 | 5 | 0.1% | 2 | 0.1% | 29 | 0.6% |
| 2台以上 5台未満 | 0 | 0.0% | 2 | 0.1% | 5 | 0.1% |
| 5台以上 10台未満 | 0 | 0.0% | 0 | 0.0% | 2 | 0.0% |
| 10台以上 20台未満 | 0 | 0.0% | 0 | 0.0% | 2 | 0.0% |
| 20台以上 50台未満 | 0 | 0.0% | 0 | 0.0% | 1 | 0.0% |
| 50台以上 | 0 | 0.0% | 0 | 0.0% | 0 | 0.0% |
| 合計 | 3,547 | | 3,651 | | 4,928 | |

・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って、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

独立行政法人 情報処理推進機構 セキュリティセンター

花村 / 加賀谷 / 宮本

Tel:03-5978-7527 Fax:03-5978-7518 E-mail:isec-info@ipa.go.jp