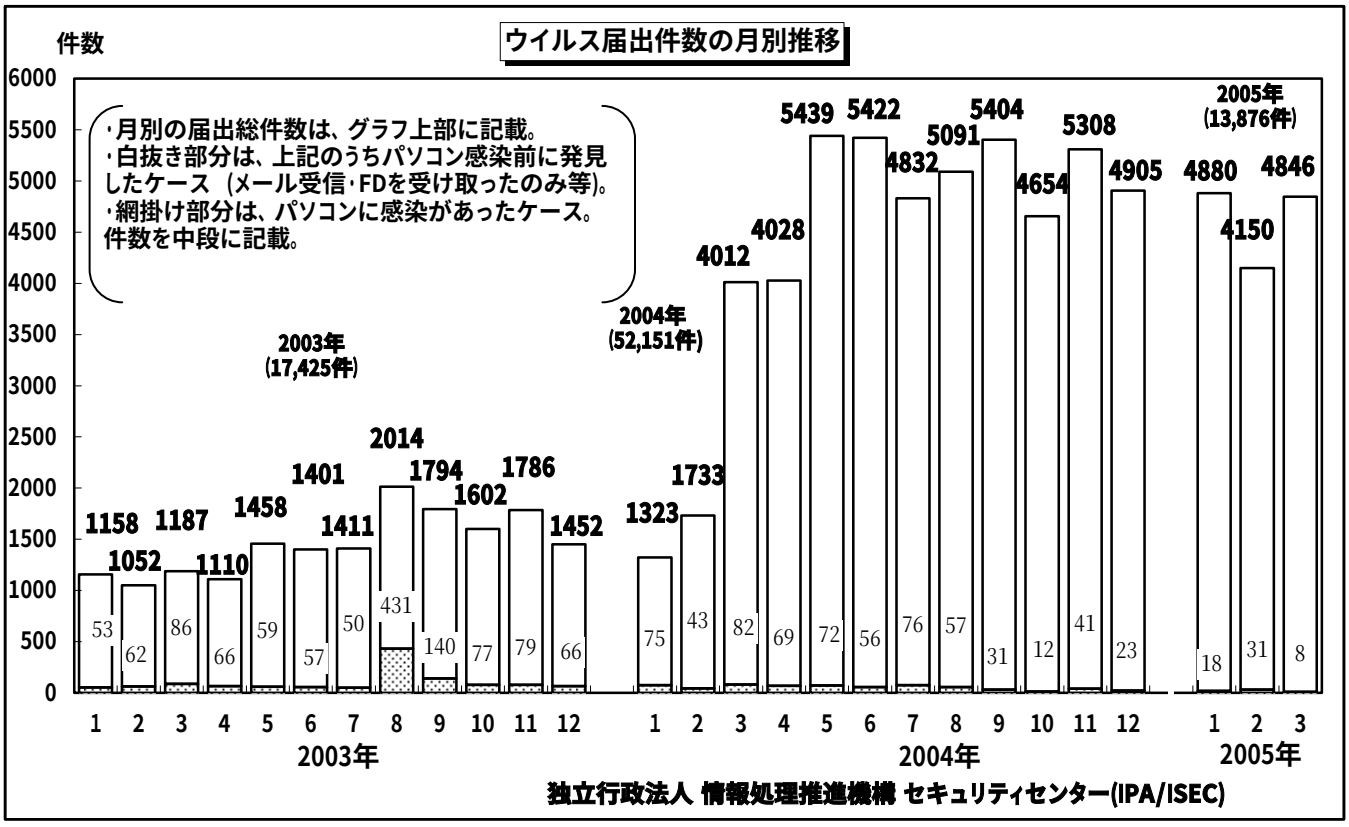
別紙 1

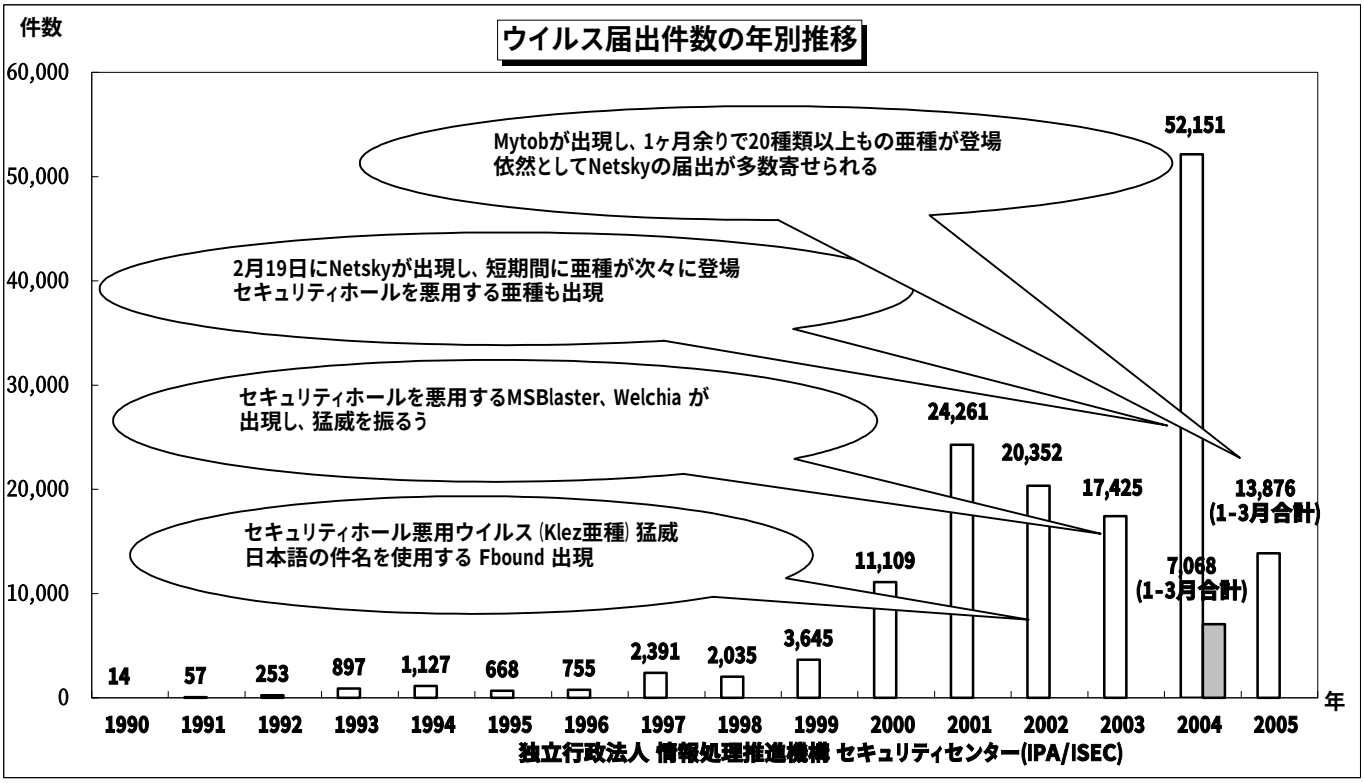
コンピュータウイルスの届出状況［2005 年 3 月分］について

・ウイルス届出の詳細

1．ウイルス届出件数の月別推移



2．ウイルス届出件数の年別推移



3．3月の届出ウイルス

ウイルスの種類は 95 種類で、Windows/DOS ウイルス 4,709 件、マクロウイルス及びスクリプトウイルス 137 件でした。（Macintosh 及び OSS のウイルスはありませんでした。）

i）Windows　　(※)印は今月の新種ウイルス

Windows/DOS ウイルス	届出件数
W32/Netsky	1,262
W32/Bagle	484
W32/Mydoom	399
W32/Lovgate	292
W32/Klez	249
W32/Zafi	192
W32/Bagz	185
W32/Mytob (※)	147
W32/Bugbear	132
W32/Mabutu	125
W32/Mimail	102
W32/Mywife	91
W32/Swen	91
W32/Sober	87
W32/Funlove	85
W32/Mota	73
W32/Fizzer	71
W32/Valla	59
W32/Parite	55
W32/Dumaru	52
W32/Yaha	52
W32/Hybris	47
W32/Tenrobot	29
W32/Sobig	26
W32/Spaces	24
W32/Magistr	21
W32/Mumu	21
W32/Welchia	21
W32/Badtrans	19
W32/Nimda	16
W32/Dupator	15
W32/Lovelorn	15
W32/Ganda	14
WYX	13
W32/CIH	13
W32/Kriz	13
W32/Conycspa (※)	10
W32/Gaobot	10
W32/Sasser	10
W32/Plexus	9
W32/Randex	9
W32/Maslan	7
W32/Sircam	6
W32/Chir	5
W32/MTX	5
W32/Antinny	4
W32/Buchon	4
W32/Evaman	3
Anti-CMOS	2
Cascade	2
Form	2
W32/Chod (※)	2
W32/Explet	2
W32/Korgo	2
W32/Myfip	2
W32/Tecata	2

Windows/DOS ウイルス	届出件数
W32/Torvil	2
W32/Aliz	1
W32/Bobax	1
W32/Bropia	1
W32/Codbot (※)	1
W32/Fatso (※)	1
W32/Frethem	1
W32/Inforyou (※)	1
W32/Inor	1
W32/Jubon	1
W32/Kobot (※)	1
W32/Lorez (※)	1
W32/Mofei	1
W32/MSBlaster	1
W32/Mugly	1
W32/Remadm	1
W32/Ska	1
W32/Zoher	1
小計	4,709

マクロウイルス	届出件数
XM/Laroux	17
W97M/Ethan	4
W97M/X97M/P97M/Tristate	4
XF/Sic	3
X97M/Squared (※)	3
W97M/Opey	2
W97M/Bablas	1
W97M/Class	1
W97M/Eight941	1
W97M/Sting (※)	1
W97M/Relax	1
X97M/Divi	1
小計	39

スクリプトウイルス	届出件数
VBS/Redlof	62
VBS/LOVELETTER	16
Wscript/Fortnight	8
VBS/Soraci	3
VBS/Freelink	2
VBS/Internal	2
VBS/SST	2
Wscript/Kakworm	2
VBS/Netlog	1
小計	98

（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
MS-WORD や MS-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。

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	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）
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

4．3月にＩＰＡに初めて届出のあったウイルスの概要

(1) W32/Mytob（マイトブ）

このウイルスは、パソコン内のアドレス帳などのファイルからメールアドレスを収集し、取得できたアドレスに対して、ウイルス自身を添付したメールを送信する活動を行います。また、アクセス可能なネットワーク共有を検索して、自分自身をコピーしたり、Windows のセキュリティホールを悪用してネットワークに接続しているパソコンに感染を拡大したりします。

感染すると、バックドアを仕掛けられ、外部からパソコン内のファイルを削除されたり、不正なプログラムを埋め込まれたりする危険があります。また、ワクチンベンダー等のセキュリティ関連サイトの閲覧を妨害するために、Hosts ファイルを改ざんします。

(2) W32/Conycspa（コニーシーエスピーエー）

このウイルスは、アドレス帳から取得できたメールアドレスに対して、自分自身を送信する活動を行います。また、レジストリを改変し、Windows の起動時にウイルスが実行されるように設定します。

送信されるメールは、セキュリティホールを悪用するための仕掛けがされており、メール本文を開いただけで不正なプログラムをダウンロードされてしまいます。

(3) X97M/Squared（スクアード）

このウイルスは、MS-Excel ファイルに感染するマクロウイルスです。感染した Excel ファイルを開くと、テンプレートが保存されているフォルダにウイルスのコピーを作成し、以後、開かれる Excel ファイルに感染します。

(4) W32/Chod（チョッド）

このウイルスは、パソコン内のアドレス帳などのファイルからメールアドレスを収集し、取得できたアドレスに対して、ウイルス自身を添付したメールを送信する活動を行います。また、MSN Messenger を介してウイルス自身を送信する活動も行います。

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。また、バックドアを仕掛け、外部から感染したパソコンを操作できるようにします。

(5) W97M/Sting（スティング）

このウイルスは、MS-Word に感染するマクロウイルスです。感染した Word ファイルを開くと、標準テンプレートファイルの Normal.dot ファイルを上書きします。また、Word の設定を改変し、特定の操作を無効にする等の活動を行います。

(6) W32/Codbot（コッドボット）

このウイルスは、ネットワーク共有フォルダに自分自身のコピーを作成して感染します。その際、ウイルス自身が持つユーザ名・パスワードリストを使用してログインを試みます。
感染すると、バックドアを作成され、外部から感染したパソコンを操作できるようになります。

(7) W32/Lorez（ロレズ）

このウイルスは、exe ファイル(プログラムファイル)に自分自身を追加することで感染します。感染すると、ファイルサイズが増加しますが、主な発病はありません。また、メールを送信する等の機能はありません。

(8) W32/Fatso（ファトソウ）

このウイルスは、MSN Messenger を介して感染を拡大するウイルスです。
感染すると、Hosts ファイルを改ざんし、セキュリティ関連サイトへのアクセスを妨害します。また、パソコンで使用しているセキュリティ対策ソフトのプロセスを停止して、検査・駆除ができないようにします。

(9) W32/Inforyou（インフォーユー）

このウイルスは、パソコン内からメールアドレスを収集し、取得できたアドレスに対して、ウイルス自身を添付したメールを送信する活動を行います。
感染すると、特定の Web サイトへの接続を試み、不正プログラムをダウンロードしようとします。また、DoS 攻撃を行うための機能も有しています。

(10) W32/Kobot（コボット）

このウイルスは、ネットワーク共有や FTP、telnet 等のサービスを検索し、ウイルス自身が持つユーザ名・パスワードリストを使用して接続を試みます。接続に成功すると、自分自身のコピーを送り込みます。
感染すると、バックドアを仕掛けたり、外部からのメールを中継したりして、リモートからパソコンを操作される危険があります。

参考：スパイウェアと不正プログラムの例

(1) Trojan/StartPage（スタートページ）

レジストリを改変することにより、ブラウザ（Internet Explorer）の起動時に表示されるスタートページを不正な Web サイトに変更します。

(2) Trojan/Websearch（ウェブサーチ）

ブラウザの設定を改変し、URL リクエストをリダイレクト(意図しないページを表示)します。これにより、特定の検索サイトにアクセスすると、意図しないページが表示されます。

(3) Trojan/Downloder（ダウンローダー）

特定のサイトへ接続して、ハッキングツールやウイルス等の不正プログラムをダウンロードします。ダウンロードが完了すると、そのプログラムを実行し、パソコンにインストールします。それにより、マシンを乗っ取ります。

(4) Trojan/Dropper（ドロッパー）

特定のサイトへ接続して、ハッキングツールやバックドアなどの不正プログラムをダウンロードします。ダウンロードが完了すると、そのプログラムを実行し、パソコンにインストールします。

(5) Trojan/PWSteal（パスワードスティール）

侵入したパソコン上から、パスワードやシステム情報を収集し、特定のメールアドレスにそれらの情報を送信します。

(6) Trojan/IRC（インターネットリレーチャット）

IRC サーバを通じて、ユーザのシステムへアクセスします。接続に成功すると、そのターゲットのシステム情報などを盗み出したり、ファイルを削除したり等の操作がリモートから可能となります。

5．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 91%を占めています。

届　出　者	届　出　件　数					
	2005 年 3 月		2005 年 2 月(前月)		2004 年 3 月(前年同月)	
一般法人ユーザ	４,３９６	90.7%	３,９９６	96.3%	３,１１５	77.6%
個人ユーザ	１８８	3.9%	１３０	3.1%	５２４	13.1%
教育機関	２６２	5.4%	２４	0.6%	３７３	9.3%

6．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99%を占めています。

感　染　経　路	届　出　件　数					
	2005 年 3 月		2005 年 2 月(前月)		2004 年 3 月(前年同月)	
メール	４,７８０	98.6%	４,１１１	99.1%	３,９５６	98.6%
ダウンロード(※)	２	0%	０	0%	１２	0.3%
外部からの媒体	２	0%	０	0%	１５	0.4%
ネットワーク	５４	1.1%	３９	0.9%	１２	0.3%
不明・その他	８	0.2%	０	0%	１７	0.4%

(※)ホームページからの感染を含む

7. 感染台数

感染台数	届出件数					
	2005年3月		2005年2月(前月)		2004年3月(前年同月)	
0台	4,838	99.8%	4,119	99.3%	3,930	98.0%
1台	4	0.1%	23	0.6%	56	1.4%
2台以上　5台未満	2	0%	4	0.1%	11	0.3%
5台以上10台未満	1	0%	2	0%	6	0.1%
10台以上20台未満	1	0%	1	0%	1	0%
20台以上50台未満	0	0%	0	0%	2	0%
50台以上	0	0%	1	0%	6	0.1%

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