解　説

# 我が国におけるコンピュータウィルスの現状と対策†

岡本栄司††　山田忠直†††　湯藤典夫†††

## 1. はじめに

高度情報化によるコンピュータ利用の拡大は，ネットワークなどによるコンピュータ利用範囲の拡大，情報ベースへのアクセス機会の増大，さらにはコンピュータ利用・運用の多様化をもたらしている．これにともなって，情報保護の重要性が高まってきている．しかしながら，情報セキュリティの確保は必ずしも十分とは言えず，さまざまなセキュリティ問題が起きている．中でもコンピュータウィルスの被害は徐々に広まりつつある．

コンピュータウィルスは外国，特にアメリカやヨーロッパで深刻化しており，最近ではアジア地区の被害も目だっている．日本でも，1989年に初めてコンピュータウィルス被害が報道されて以来，かなり報告されるようになってきた．コンピュータウィルスは情報化社会の健全な発展を阻害する恐れが十分にあるため，早期の対策が望まれている．それに対して，我が国では，組織，個人のレベルでさまざまな対策が施されるようになってきた．

そこで本解説は，通産省，警察庁，情報処理振興事業協会（IPA，通産省の特別認可法人），企業，個人における対策を，制度，運用，技術の面から解説し，これによってコンピュータウィルスの防止に役だてることを目的とする．

まず，平成2年および3年にIPAが行った我が国のコンピュータウィルス被害調査の結果を示す．また，IPAは通産省告示により，ウィルス被害時の届出先に指定されているが，今までに届けられたウィルスの被害統計概要も示す．これらにより，我が国におけるコンピュータウィルスの被害状況および増加傾向が明らかになろう．

それに対する対策として，まず制度面から，官公庁のガイドラインである，警察庁による不正プログラムに対する安全指針，通産省による対策基準を述べる．また，情報処理振興事業協会への届出制度，同協会によるコンピュータウィルス対策パソコンネットワークの運営についても言及する．さらに，ウィルス対策は各企業や組織による活動も不可欠であるため，企業における対策活動例をあげる．

一方，技術的対策では，コンピュータウィルス防御ツールが重要になる．ここでは，1例としてIPAによるウィルス検知ツールについて述べる．

## 2. コンピュータウィルスとは

コンピュータウィルスの定義にはいろいろあるが，ここでは通産省による定義に従う[Ts90]．

コンピュータウィルスとは，第三者のプログラムやデータベースに対して意図的になんらかの被害を及ぼすように作られたプログラムであり，次の機能の一つ以上を有するもの．

1) 自己伝染機能：自らの機能によって他のプログラムに自らをコピーしまたはシステム機能を利用して自らを他のシステムにコピーすることにより，他のシステムに伝染する機能

2) 潜伏機能：発病するための特定時刻，一定時間，処理回数などの条件を記憶させて，発病するまで症状を出さない機能

3) 発病機能：プログラムやデータなどのファイルの破壊を行ったり，設計者の意図しない動作をするなどの機能

図-1に，コンピュータウィルスの感染の様子を示す．

† Computer Viruses and Anti-viral Activities in Japan by Eiji OKAMOTO (Japan Advanced Institute of Science and Technology, East), Tadanao YAMADA and Norio YUTOH (Software Technology Center, Information-technology Promotion Agency).

†† 北陸先端科学技術大学院大学情報科学研究科
††† 情報処理振興事業協会技術センター

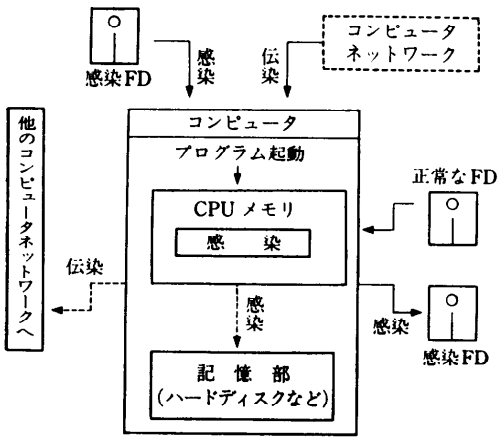


図-1　コンピュータウィルスの感染

コンピュータウィルスを広く解釈すると，狭義のコンピュータウィルスのほかに，ワーム，トロイの木馬などを含む．

(狭義) コンピュータウィルスは，自分自身の複製が他のプログラムに取り付くプログラムコードである．

ワームは，自分自身の複製が他のコンピュータに送り込まれ，そこで実行を開始する独立したプログラムである．

トロイの木馬は，良性のプログラムに忍び込ませてあり，そのプログラムを実行すると本性を現して悪事を働くプログラムコードである．

警察庁の対策指針では広義のコンピュータウィルスを不正プログラムなどと呼んでいる[Kc89]．本報告書では，主に広義の意味でコンピュータウィルスを扱う．前述のコンピュータウィルス対策基準による定義も，広義である．

コンピュータウィルスを作成する動機には，さまざまな理由があげられる．一般的には

- 自己顕示
- 反抗
- 不法コピーに対する警告
- テロの1手段
- スパイ行為

などがあるといわれている．

## 3. 我が国の被害の現状

### 3.1 アンケート調査 (平成2，3年)

IPA では，コンピュータウィルスに関する被害状況調査を，平成2年の2～3月および平成3年の2～3月にかけて，2回行った．

表-1　アンケート回答者

| | | | 第1回 | 第2回 |
|---|---|---|---|---|
| 調査対象 | 公団体など | 大　学 | 99 | 62 |
| | | その他教育機関 | 3 | 14 |
| | | 政府・政府関係機関 | 111 | 28 |
| | | 地方公共団体 | 1 | 7 |
| | | 計 | 214 | 111 |
| | 民間企業など | | 165 | 639 |
| | 合　計 | | 379 | 750 |
| 被害を被った団体 | | | 51 | 40 |
| 被害総件数 | | | 51 | 50 |

アンケートの回答総数は，第1回が379（発送数500）で，第2回が750（発送数1000）となっている．表-1に回答者の内訳を示す．

表から分かるように，被害を被った団体については，前回の51団体が40団体に減少し，被害発生率では，前回の13.4%が半分以下の5.3%になった．

この原因は，第2回の調査が被害の発生を幅広く捉えるために民間企業を中心に対象範囲をほぼ倍と広げたのに対し，第1回の調査では，実際に被害が想定される部門（大学，政府および政府関係機関などの研究・開発部門とか，情報処理部門）に的を絞っており，そうした違いによるものと判断される．

ウィルスの種類別で見ると，両調査共マッキントッシュにおけるウィスルが最も多く，ほぼ9割を占めている．ただ，感染の多いウィルスはnVIR から WDEF へシフトしていると言える（後述する届出ウィルスの状況からも分かる）．

また，数こそ少ないが，第2回ではストーンド，エルサレム，イスラエルといったIBM PC/AT系のウィルスが発見されている．

次に，一般企業を主たる対象とした第2回目の調査を基に，ウィルスの被害について関連する事柄をいくつかあげてみる．

ウィルスの「知名度」については，知らないという答えが5件あったが，全体の99.2%に当たる744人が知っていると答え，ウィルスについては，ほとんどの回答者が知っていた．詳しく知っている人は，全体の12.4%に相当する93人で状況としてはまだまだ少ないと言える．

感染経路については，ウィルスに汚染されたコンピュータで使用したフロッピィからが，50件中

表-2 ウィルス名および被害機種

| 種　類 | 第1回 | 第2回 | 対象機種 |
|---|---|---|---|
| nVIR | 29 | 11 | |
| WDEF | 3 | 24 | マッキントッシュ |
| SCORE | 2 | 0 | |
| INIT 29 | 1 | 1 | |
| ストーンド | 0 | 2 | |
| エルサレム | 0 | 1 | IBM/PC 系 |
| イスラエル | 0 | 1 | |
| メリークリスマス | 2 | 1 | 国　産 |
| X68000 FORCE | 0 | 1 | MS-DOS 機 |
| ワーム | 2 | 0 | 汎用機 |

26件と最も多く，続いて知人などから借用・コピーしたソフトウェアからが11件となっている．

復旧期間では，1日未満が33件と最も多く，続いて1～3日程度が8件となっており，比較的短期間で復旧はできている．

さらにウィルスに関する質問を，ウィルスを知っていると回答した744人に対して行った．その回答の中から主なものをいくつかあげてみる．

①ウイルスに対する脅威感

約8割の594人が脅威を感じると回答しており，多くの人がウィルスに対する恐れを抱いている．

②今後の被害予測

約8割の591人が増加すると答え，中でも17.7%にあたる132人が急激に増加すると回答しており，今後被害は増加するとの見方をする人が多い．

③セキュリティ対策

ウィルスに対し脅威を感じる，今後被害は拡大するという回答が多い中で，何も対策を行っていないが196件（割合としては，26.3%）もある．

実施している対策（複数回答が可能）としては，ファイルのバックアップが454件と最も多く，続いてコンピュータの利用管理が194件，ソフトウェアの利用管理が152件となっている．また，今後計画している対策（複数回答が可能）についても，ファイルのバックアップが299件と最も多い．対策としては，実際に行っている対策，今後計画している対策共，通常の運用管理の範疇に入るものが多く，ウィルスの知識を得たり，ワクチンの利用といった，ウィルスを特に意識した積極的な対策は，あまり多くない．

### 3.2 被害届出状況

IPAはコンピュータウィルス対策基準（後述）に基づき，平成2年4月よりコンピュータウィルスの被害を届け出る公的機関に指定されている．制度開始以来，届出件数は，平成2年20件，平成3年10カ月で45件となっており，確実に増加の傾向にある．

届出ウィルスの種類をまとめると，表-3のように24種ある．マッキントッシュのウィルスが2種16件，IBM/PC系が15種38件，国産ウィルスが6種8件，ワームが1種1件となっている．

カスケードやヤンキードゥードルのように元来IBM/PC系のウィルスにもかかわらず，国産MS-DOS機に感染したケースも報告されている．IBM/PC系のウィルスの中には，国産MS-DOS機に対して感染するものもあるため，機種が違うからと言って安心はできない．

なお，表の中に見慣れないウィルス名，たとえばDAph-2など，があるが，これはIPAにて用いているウィルスコード命名法によるウィルス名である．これについては，付録を参照のこと．

届出をしたユーザは，情報産業や大企業など，

表-3 届出ウィルスと被害機種

| No | ウィルス名 | 件数 | オリジナル機 |
|---|---|---|---|
| 1 | WDEF | 15 | マッキントッシュ |
| 2 | nVIR | 1 | 〃 |
| 3 | ヤンキードゥードル | 8 | IBM/PC 系 |
| 4 | ストーンド | 7 | 〃 |
| 5 | エルサレムB | 3 | 〃 |
| 6 | サンデー | 3 | 〃 |
| 7 | ジョシ | 2 | 〃 |
| 8 | エルサレム | 2 | 〃 |
| 9 | カスケード | 2 | 〃 |
| 10 | ダークアベンジャー | 2 | 〃 |
| 11 | リバティ | 2 | 〃 |
| 12 | ワクシナ | 2 | 〃 |
| 13 | イスラエル型 | 1 | 〃 |
| 14 | インベーダー | 1 | 〃 |
| 15 | ウインナー | 1 | 〃 |
| 16 | キー・プレス | 1 | 〃 |
| 17 | アズサ | 1 | 〃 |
| 18 | DBf-1 (X68000) | 1 | MS-DOS 機 |
| 19 | DAph-2 (メリークリスマス) | 3 | (国産) |
| 20 | DBo-3 (DB 29) | 1 | 〃 |
| 21 | DBh-4 | 1 | 〃 |
| 22 | DAn-5 | 1 | 〃 |
| 23 | DShm-6 | 1 | 〃 |
| 24 | クリスマスワーム | 1 | ワーム |
| | 不　明 | 1 | |

表-4 届出をした機関

| ユーザ | 件数 |
|---|---|
| 情報産業 | 22 |
| 一般法人ユーザ | 19 |
| 個人ユーザ | 12 |
| 大学・研究機関 | 9 |

表-5 届出ウィルスの感染経路

| 感染経路 | 件数 |
|---|---|
| 外部から持ち込んだFD | 32 |
| ネットワークから | 7 |
| 購入したソフトから | 3 |
| ショップから | 1 |
| レンタルマシンから | 1 |
| 秘匿希望 | 3 |
| 不明 | 15 |

日頃からセキュリティに関心のある部門の人が多い．ただ，一般的にはウィルスの発生の事実を隠したがる傾向があるため，実際のウィルス発生数はもっと多いことが予想される．届出を行っても企業名などは外に出ることはないので，コンピュータセキュリティに対する警鐘という意味から，積極的に届出を行うことが望まれる．

感染経路をみると外部から持ち込んだFD（フロッピィディスク）からが圧倒的に多い．外部の業者や友人が持ち込んだFD，コピーソフトなどが原因となっている．特に，海外では日本とは比較にならないほど広く蔓延しているため，海外からソフトを持ち込む場合は信頼できるところから入手し，ワクチンなどでチェックを行う必要がある．

被害についてはかなり重大な損害を被ったものも何件かあるが，大半は軽微なものである．特にマッキントッシュについては，ワクチンソフトにより被害が出る前に発見したケースが多い．しかしながら，不審な動作に対する調査やメーカへの相談といった，目に見えない形で被害を被る例もあり，一概に被害は少ないとは言えない．

## 4. コンピュータウィルス対策

コンピュータウィルス対策には，社会的対策と技術的対策がある．これらは併せて実施されることにより，はじめて十分な効果を発揮する．

社会的には教育・啓蒙が重要であるが，中でもモラルの向上が最も重要である．コンピュータウィルスの作成だけではなく，既存の無害ウィルスを改変するということも反社会的行動で，「情報犯罪」とみなすべきであろう．マスコミ報道などは，この視点の配慮が足りないように見受けられる．海外では，モラルや倫理的教育は無意味だと考えている人が多く，またウィルスコンテストを呼びかけたりする「有名人」もおり，問題視されている．

### 4.1 官庁によるガイドライン

コンピュータウィルスに関する官庁によるガイドラインは，今までに二つ公表されている．一つは，平成元年11月，警察庁によって公表された「コンピュータ・ウィルス等不正プログラム対策指針」で，もう一つは，通商産業省が，平成2年4月に告示した「コンピュータウィルス対策基準」（告示第139号）である．ここでは，この二つのガイドラインについて概観する．

#### 4.1.1 「コンピュータ・ウィルス等不正プログラム対策指針」

本指針は，昭和61年1月に公表された「情報システム安全対策指針」を策定した「コンピュータ・システム安全対策研究会」（警察庁設置の研究会）における中間報告の形をとり，不正プログラムによる被害を防止するために講ずることが望ましい事項がとりまとめられている．

指針は，具体的に実施する場合を想定し，便宜上対策実施者をコンピュータ・システムの運用者，開発業者，および行政機関の3種類に分け，それぞれが行うべき対策を示している．運用者については，さらに，対策を継続すべき性質のものと特定の場合にのみ行うべきものとに分けている．指針の内容を，**図-2**に一部抜粋の形で示した．

指針の中では，コンピュータ・システムの運用者や開発業者などが，不正プログラム対策の重要性を認識することが大切なことである（“対策実施の支援”の項）とし，そのためには，行政機関などが，啓蒙・啓発活動を行うことも重要であると述べている．さらに，開発業者および行政機関などに対しては，ワクチン・プログラムの開発，その普及の促進，コンピュータ・セキュリティに関するコンサルタント業の育成，システム監査の普及促進など，不正プログラム対策を支援する諸施策を講ずる必要があるとしている．

2　コンピュータ・システムの運用に携わる者が講ずべき対策
　2—1　継続的に講ずべき対策
　　1　アクセス管理
　　2　ファイル破壊・改ざんの防止対策
　　3　障害復旧への備え
　　4　不正プログラム対策に関する教育
　2—2　特定の場合に講ずべき対策
　　1　コンピュータ・システムの使用開始時に講ずべき対策
　　2　新しく入手したプログラムを使用する際に講ずべき措置
　　3　コンピュータ・システム使用中に講ずべき措置
　　4　不正プログラム発見時に講ずべき措置
3　コンピュータ・システムの開発業者等が講ずべき対策
　1　ワクチン・プログラムの開発
　2　不正プログラム対策実施支援システムの開発
　3　不正プログラムの被害を受けにくいコンピュータ・システムの開発
　4　コンピュータ・システムの生産，流通過程における管理
4　行政機関が講ずべき対策
　1　不正プログラム対策実施の支援
　2　不正プログラムの作成，実行等の抑止
　3　捜査技術の開発
　4　国際的な連絡協調体制の確立

図-2　コンピュータ・ウィルス等不正プログラム対策指針の抜粋

### 4.1.2 「コンピュータウィルス対策基準」

通商産業省が定めたこの対策基準は，コンピュータウィルスに対する予防，検知，事後対応などについて実効性の高い対応策を取りまとめたものである．基準の適用にあたっては，使用するコンピュータ・システムの実態に則したものとすることが必要であると述べ，その際，コンピュータ・システムの種類による相違，機種による相違，およびソフトウェアの設計による相違の三つを留意すべき事項としてあげている．

この基準は，内容的には，ユーザ基準，システム管理者基準，ソフトウェア開発管理者基準の三つの基準から構成され，59項目にわたってかなり詳細に取るべき対策が述べられている．

● ユーザ基準

コンピュータ・システム利用者のためのソフトウェア管理，運用管理，およびウィルスに汚染された場合の事後対応についての対策．全部で19項目からなる（図-3）．

● システム管理者基準

コンピュータ・システム管理者のためのソフトウェア管理，運用管理，ネットワーク管理，およびウィルスに汚染された場合の事後対応についての対策．全部で27項目からなる．

| 項目 | 対策項目 |
|---|---|
| ソフトウェア管理 | (一) ソフトウェアの販売者，又は配布責任者の連絡先，バージョン，更新情報を入手し，信頼できるソフトウェアを使用すること．<br>(二) オリジナルプログラムには，ライトプロテクトを施すこと．<br>(三) オリジナルプログラムのバックアップを確保すること．また，オリジナルプログラムは安全な場所に保管すること．<br>(四) 運用中のシステムのバックアップを定期的に行うこと．また，それを一定期間保管すること． |
| 運用管理 | (一) 他人とのファイル媒体の共用を避けること．<br>(二) システムの利用は，いったん初期状態にしてから行うこと．<br>(三) マスターファイルの管理を厳重に行うこと．<br>(四) システムの動作の変化に注意すること．<br>(五) ディレクトリを定期的に点検すること．<br>(六) ワクチンを利用すること．<br>(七) パスワードは容易に推測されないように設定し，その秘密を保つこと．<br>(八) パスワードは随時変更すること．<br>(九) 同一のユーザIDを複数のユーザで共用しないこと．<br>(十) アクセス履歴を確認すること．<br>(十一) ユーザの機密情報を格納しているファイルの管理を厳重に行うこと．<br>(十二) 入力待ちの状態で放置しないこと． |
| 事後対応 | (一) 異常が発生した場合には，その現象を記録し，システム管理者に連絡すること．<br>(二) システムディスクの復元は，オリジナルプログラムから行うこと．<br>(三) 汚染されたフロッピィディスクは破棄すること． |

図-3　ユーザ基準

● ソフトウェア開発管理者基準

ソフトウェア開発管理の責任者のための開発環境管理，製品管理，およびウィルスに汚染された場合の事後対応についての対策．全部で13項目からなる．

各対策項目は，参考しやすいものとなっており，順序なども考慮に入れながら，自社の運用に適した，無理のない対策としていくことが望まれる．

こうしたガイドラインをもとに，システムは常に危険にさらされているとの認識に立ち，自分のシステムは自分で守るといった積極的な取り組みを行うことが大切である．

### 4.2 届出制度

届出制度は，前に述べた通商産業省の「コンピュータウィルス対策基準」に基づく制度である．対策基準には，被害の拡大および再発を防止するために，必要な情報を公的機関に届けることが明記されている．この基準に基づき，届出を受ける公的機関に，通商産業大臣から平成2年4月に情報処理振興事業協会（通称 IPA）が指定され（通商産業省告示第176号），届出は IPA に対してなされることになった．

IPA への届出は，被害状況を発生時と回復時に分けてできるだけ詳しく記述し，報告するようになっている．記述した内容の中で，公表したくない項目には秘匿とするように指定ができるなど，取扱いには十分注意が払われている．届出する内容を参考までに**図-4**に示した．

IPA には，ウィルス対策のために学識経験者からなる「コンピュータウィルス対策委員会」が設けられており，届出を受けると，そのメンバの協力を得るなどして，届出内容を調査し，対策を検討するといった手順を取っている．また，広報活動の一環として被害の拡大防止を図るため，必要に応じ，随時，または定期的に結果を公表している．

以上が，届出制度ができた経緯とその概要である．

(発生時)
1. 届出者名
2. コンピュータウィルスの発見場所
○ 3. コンピュータウィルスの発見日時
○ 4. 機種名
○ 5. 使用時の OS（バージョンレベル），ソフトウェア（バージョンレベル）
○ 6. ネットワークへの加入状況（もしあれば）
○ 7. コンピュータウィルスの内容（わかればその名称）
8. 発見以前にセキュリティ対策を講じていた場合はその内容
○ 9. 推定される感染経路
10. 被害の状況（届出時点で把握できる範囲で）
11. 直ちに講じた回復等のための措置があればその内容

(回復時)
12. 回復の日時
13. 回復のためにとった措置及びその期間・投入人日
14. 被害状況（台数，枚数，被害金額）
15. 今後のセキュリティ対策（もしあれば）
16. その他，発見時届出内容に関して追加または修正があればその内容

注）○印の項目は，原則として公表を前提としている項目を示す．

**図-4** 届出内容

この制度は従来の安全対策と違い，新しい面をもつ制度である．すなわち従来の安全対策では，コンピュータウィルスなどの問題は一企業の問題として閉じた形で処されていたが，それに対し，この制度はそうした問題を届け出ることによって広く社外に公表し，同じような被害の拡大を防止していくという点で，新しい試みと言える．

制度自体は，まだ，日も浅く，世の中に広く浸透しているとは言えないが，被害は，届出状況からみる限り増加する傾向にあり，対策は急を要する課題でもある．一般の多くの利用者の方々に役に立つ，正しい情報を流していくためにも，被害にあった場合は，社会的責任を考え，積極的に届出を行っていくことが求められる．届出のために専用電話が用意されており，その番号は (03) 3433-4844 である．

### 4.3 ウイルス対策パソコンネットワーク

届出は，すでに IPA が届出機関に指定された時点からスタートしているが，法人ユーザばかりでなく，個人ユーザからも広く届出ができるように制度をより充実させる目的で，平成3年7月に，IPA では，ウィルス対策パソコンネットワーク（アクセス電話番号：03-3459-8944，MNP クラス5，ボーレート：1200 と 2400）を開設した．このパソコンネットワークには，被害の届出コーナとともに，被害届出状況，ウィルス，およびワクチンなどに関する情報提供コーナなども設けられている．運営は，24時間体制を取り，アクセスは，利用者が好きな時にいつでも利用できるようになっている．パソコンネットワークからの情報収集もウィルス対策の一環として，広く活用されることが望まれる．

### 4.4 企業における活動例

一昨年から今年にかけて，国産のパーソナルコンピュータもウィルスの被害にあった．このため，多くのコンピュータメーカは企業活動としてコンピュータウィルスの対策に本腰を入れて取り組んでいる．

ここでは，パソコンメーカの活動例を示す．通常，活動は次のような項目からなっている．

1) ウィルス対策チームの設置
2) 社内外連絡体制の確立
3) コンピュータウィルス対策マニュアルの制定・配布

4) 防御プログラムの提供

5) 教育／啓蒙

ウィルス対策チームの設置と社内外連絡体制の確立は，企業におけるウィルス対策活動の基本となるものである．ウィルス対策チームは，中央的な組織として位置づけられ，各事業所や全国代理店に設置されたウィルス対策窓口を統括している．この連絡網により，ウィルス相談を受けたり，コンピュータウィルスの早期発見／被害発生時における処置・対応を行っている．また，IPA ウィルス対策室などの公的関係組織とも緊密な連携をとり，被害発生時には被害届をすみやかに IPA に提出すること，としている．

企業では，官庁のコンピュータウィルス対策ガイドラインを基に各企業にあったマニュアルを制定し，全社に配布しているところが多い．マニュアルには，ウィルスの被害にあわないようにするための対策・管理法だけでなく，被害発生時の対処の仕方，連絡法なども規定している．パソコンユーザのためには，ウィルス対策パンフレットを作成して配布している．ウィルス被害発生後に配布したある企業のパンフレットには，次のようなことが書かれている．

コンピュータウィルスについてのお知らせ

1) 今回のウィルスの特徴

2) ウィルスへ感染の可能性が高い方

3) 今回のウィルスへの感染有無の診断方法

4) 感染の疑いが強いと判断される場合の措置

5) ワクチンのご案内

6) 問い合わせ先

また，パソコン通信サービスや企業の情報誌でもウィルスやワクチンの情報提供を行っているケースもある．

### 4.5 防御ツール

技術的対策には，予防，検知および回復の三つの機能が必要となる．具体的には，

- ワクチン
- セキュア OS
- 暗号／認証技術の応用

などによりこれらの機能が実現される．

この中ではワクチンが最もよく用いられている．手軽だが，ソフトウェアで対処するので，ウィルスに裏をかかれる可能性がないわけではない．

OS にセキュリティ機能を組み込めば，安全性は高まる．完璧を期すならば，少なくとも OS のある一部は ROM に焼き付けるか，ハード構成にしなければならない．ただし，使い勝手は多少悪くなる．

暗号／認証技術の応用は，既存のシステムに載せやすいという利点がある．従来暗号／認証技術の応用については，幾つかの提案がなされている[Ho90]．特に，RSA などのディジタル署名を用いてウィルス汚染を検知する方法は，かなり以前から知られている．ただし，RSA 署名を直接ソフトウェアに付加することにすると，だれが署名するか，あるいは公開鍵をどう公開／管理するかなどが問題になる．参考文献 [OM 90] では，ID 情報に基づく認証方式を用いることによりその問題点の解決を図っている．IPA ではすでにそれを試作している．以下に本方式の概要を示す．

[ID 情報に基づくウィルス検知方式]

ID 情報に基づくウィルス検知方式では，ID 情報としてソフトウェアベンダの名前を利用している．

本方式では，信頼できるセンタが必要となる．このセンタは，RSA 暗号系と同様に鍵 $e$, $d$, $n$ を生成し，公開鍵 $e$, $n$ を一般に公開しておく．$d$ は秘密である．ここで $e$, $d$, $n$ は約 512 ビット（あるいはそれ以上）の整数である．

本方式は，次に示す三つのフェーズに分かれている．

1) 加入フェーズ

● 各ソフトウェアメーカはセンタに加入を申し込む．

● センタは当該ソフトウェアメーカの正当性をなんらかの手段で判定した後，IC カードを渡す．その中には，

$(\mathrm{ID}_i, s_i, g, e, n)$

が記録されている．ここで，$\mathrm{ID}_i$ はそのソフトウェアメーカを示す識別子（名前など）で $s_i$ は $\mathrm{ID}_i$ を整数とみなして，

$$s_i^e \pmod n = \mathrm{ID}_i \qquad (1)$$

を満たすように作られている．このような $s_i$ は秘密鍵 $d$ を持っているセンタのみが作成できる．ここで mod $n$ は，$n$ で割った余りを示す．

2) 配送フェーズ

● ソフトウェアメーカ $\mathrm{ID}_i$ があるソフトウェ

ア $P$ を作成したとして，$P$ に $a_i$，$b_i$ を付加して，$(P, a_i, b_i)$ をユーザに配布（販売）する．ここで，$a_i$，$b_i$ は，乱数 $r$ を用いて計算した

$$a_i = g^{er} \bmod n \quad (2)$$

$$b_i = s_i g^{hr} \bmod n \quad (3)$$

であり，$h$ は，データをなんらかの変換で512ビット以下にするハッシュ関数'hash'により計算される：

$$h = \mathrm{hash}(a_i, P) \quad (4)$$

3) 検証フェーズ

● ユーザは，ソフトウェア $(P, a_i, b_i)$ を受け取る．もしそのソフトウェアの正当性を判断したければ，

$$h = \mathrm{hash}(a_i, P) \quad (5)$$

を計算し，

$$b_i{}^e / a_i{}^h \bmod n = \mathrm{ID}_i \quad (6)$$

が成立するか否かをみる．もし成立すれば，ウィルスにかかっていないと判断できる．

加入フェーズはソフトウェアメーカごとに一回だけ行えばよい．また，検証フェーズは，ユーザが心配になったときだけ行えばよい．

この方式の特徴は，ソフトウェアメーカごとにディジタル署名が異なるが，ユーザは全員同一の $e$，$n$ を用いるだけでよいことにある．

一般に，ディジタル署名を用いれば，一般ユーザは，アプリケーション・ソフトウェアにウィルスが感染した場合に，チェックモジュールを用いることにより異常を検知できる．これは，全てのウィルス，あるいは今後新たに現れるウィルスにも有効である．

ただし，次の点に注意する必要がある．

● チェックモジュールは，汚染されていないパソコンで立ちあげること．たとえば，書き込み禁止のフロッピィディスクに入れておき，そのフロッピィディスクから立ち上げる．

● ウェルス汚染からの回復はできない．アプリケーションソフトウェアがなんらかの形で改変されたことが判明するだけである．したがって，具体的なウィルス名までは分からない．

いずれの技術的対策を用いても，使いやすさなどを考慮すると完全ではない．しかし，一つ一つの対策は完全でなくても，それらを組み合わせることにより，効果的な防御策となる．たとえば，ソフトウェア製造工程の清浄化，ワクチンの使用と，ウィルス検知ツールの組み合わせなどである．こうすれば，通常はワクチンでウィルスを発見でき，もし見逃してもウィルス検知ツールで検出できることになる．

## 5. おわりに

以上，我が国におけるコンピュータウィルスの被害の現状とその対策を述べた．特に，官公庁のガイドライン，届出制度，技術的対策を重点的に示した．

最後に，繰り返しになるが，教育・啓蒙を強調しておきたい．モラルを向上するためには，情報処理教育の初期段階から，ウィルスなどの不正プログラムの作成あるいはその改変は「情報犯罪」であり，決して行ってはならないことを繰り返し述べる必要がある．これにより我が国の情報処理従事者の意識が高まることが，長い目でみれば最も有効となる．それには，まず情報処理の教育・研修を行う機会の多い読者諸兄が，教育・モラルの向上の重要性を認識していただきたい．また，情報処理の教育・講演に際しては，必ずモラルの向上を一言つけ加えていただきたい．

## 参考文献

[Ho 90] Hoffman, L. J.: Rogue programs: viruses, worms, and Trojan horses, Van Nostrand Reinhold (1990).

[Ip 90] 電子ウィルス対策の調査研究のための被害状況調査—調査報告書—，情報処理振興事業協会技術センター（平成2年8月）．

[Ke 89] コンピュータ・ウィルス等不正プログラム対策指針，警察庁（平成元年11月）．

[OF 90] 岡本，藤岡：電子ウィルスの現状とその対策，情報処理振興事業協会技術センター技術発表会予稿集（1990）．

[OM 90] OKAMOTO, E. and MASUMOTO, H.: ID-Based Authentication System for Computer Virus Detection, ELECTRONICS LETTERS, 26, 15, pp. 1169-1170 (1990).

[Ts 90] 通商産業省：コンピュータウイルス対策基準解説書，日本情報処理開発協会（1990）．

（平成3年12月16日受付）

## 付　録　ウィルスコード命名法

IPA では，国内で新規に発見され，IPA に届けられたウィルスに対して，以下の基準に従って名称を付けている．できるかぎり無機質な名称を心がけている．

ウィルスコード＝OS コード
＋感染場所コード
＋発病状況コード＋ハイフン
＋届出順通番

（1） OS コード

| | |
|---|---|
| MS-DOS (PC-DOS) | : D |
| Macintosh | : M |
| UNIX | : U |
| その他 | : T |

（2） 感染場所コード

| | |
|---|---|
| BOOT セクタ（パーティションテーブル，SRAM を含む） | : B |
| OS (IO. SYS, MS-DOS, COMMAND. COM) | : S |
| アプリケーション | : A |
| その他 | : T |

（3） 発病状況コード

| | |
|---|---|
| OS 部の破壊 | : o |
| FAT の破壊 | : f |
| プログラムの破壊 | : p |
| データ破壊 | : d |
| メッセージ表示 | : m |
| ハングアップ | : h |
| 発病なし | : n |
| その他 | : t |

（4） 届出順通番

新種ウィルスに対する通番

本命名法によると従来のウィルス X68000 とメリークリスマスのウィルス名は

X68000 ウィルス→DBf-1

メリークリスマス→DApm-2

となる．


**岡本　栄司**（正会員）

昭和 48 年東京工業大学工学部電子工学科卒業．昭和 53 年同大学院博士課程修了．同年日本電気(株)入社．平成 3 年 12 月から北陸先端科学技術大学院大学情報科学研究科教授．グラフ理論，通信理論および情報セキュリティを初めとする情報数理工学の教育・研究に従事．平成 2 年電子情報通信学会論文賞受賞．IEEE シニア会員．電子情報通信学会，情報理論とその応用学会，応用数理学会，システム監査学会，日本セキュリティ・マネジメント学会，IACR 各会員．

**山田　忠直**

1948年生．大阪府立大学工学部化学工学科修士課程修了．(株)石井鉄工所にて解析業務に従事．その後(株)バーテックスシステム創設．情報処理振興事業協会コンピュータウイルス技術調査室前室長．著書「コンピュータウイルスのおはなし」．

**湯藤　典夫**

昭和 47 年富山大学文理学部卒業．同年 4 月 (株)アイネス入社．平成 3 年 4 月情報処理振興事業協会に出向．現在，コンピュータウイルス対策業務に従事．