解　説

コンピュータセキュリティ対策—コンピュータウィルスを中心として—

Computer Security—Computer Virus Countermeasure by Toru NAKAMURA (Information Technology Promotion Agency Japan, Information Technology Security Center).

中　村　　達[1]

1 情報処理振興事業協会・セキュリティセンター・ウィルス対策室

1. はじめに

コンピュータの低価格化が進む中1996年のパソコン出荷台数は過去最高の700万台（日本電子工業振興会調べ）に達し，コンピュータの利用は企業を始め学校や家庭にまで広がってきている．また，国際的ネットワークであるインターネットが普及してきたことで，コンピュータとネットワークが結合されたネットワーク情報社会が形成されつつある．このような社会では，コンピュータの果たす役割は日増しに重要になってきており，コンピュータがダウンした場合の影響は計り知れないものがある．近年，ネットワークを介してコンピュータに不正侵入して，コンピュータの活動を停止させたり，プログラムやデータなどを破壊してコンピュータを動作不能にするコンピュータウィルスが社会的に大きな問題となってきた．

コンピュータウィルスの定義については，世界中でいろいろ行われているが，通商産業省で定めた「コンピュータウィルス対策基準」では次のように定めている．

(コンピュータウィルスの定義)

第3者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり

・感染機能
・潜伏機能
・発病機能

のうち1つ以上の機能を有するもの．

定義では3つの機能のうち1つの機能でももてばコンピュータウィルスとしているが，実際に発見されているコンピュータウィルスのほとんどが上記3つの機能をすべて兼ね備えている．これらコンピュータウィルスは，一度コンピュータに侵入すると自分の複製を作成しながら発病する時期を待ち発病条件が整うと一斉に被害を引き起こす．

2. 国内のコンピュータウィルスの被害状況

通商産業省では，コンピュータウィルスの拡大と再発を防ぐための「コンピュータウィルス対策基準」を1990年4月に告示しているが，この中で情報処理振興事業協会（以降IPAと記述する）を被害の届け出を受け付ける公的機関に指定した（最新の「コンピュータウィルス対策基準」は1995年7月に改定されている）．以下この届け出情報を基に，我が国でのコンピュータウィルス被害の現状をみることにする．

2.1 被害届け出件数の推移

図-1のグラフは1990年からの被害届け出件数の年別推移を表したものである．1996年12月までのコンピュータウィルスによる被害届け出件数は，累計で3771件である．内訳は，1990年が14件，1991年が57件，1992年が253件，1993年が897件と対前年に比べ大幅に伸びてきた．さらに1994年に入っても被害届け出は伸びて3月には月間の届け出が過去最高の185件を記録するとともに，年間の届け出件数が1127件と1000件を突破している．1995年は668件と前年に比べ届け出件数が約半分に減少しているが，1996年は755件と増加傾向に転換してきている．この数字からみると1995年以降の被害が急激に減少したようにみえるが，被害届け出以外の各種状況から推測するに，それほど大きく減少したとは考えられず，1994年とほぼ同じかまたは少し下回る程度でないかと考えている．

2.2 国内のコンピュータウィルスの傾向

表-1に1990年4月～1996年12月までに被害

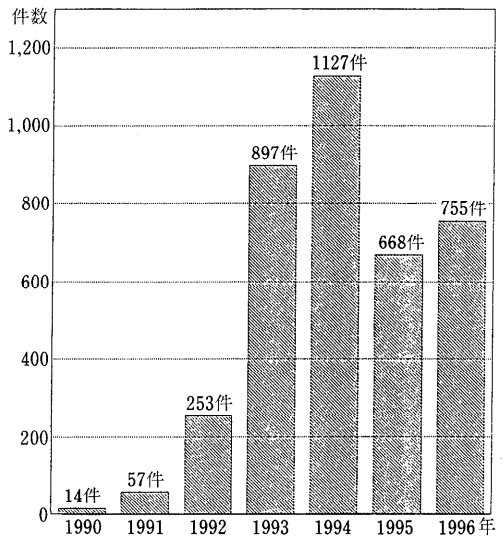


図-1 被害届け出件数の推移

届け出されたコンピュータウィルスの一覧を示す．全体で148種類のウィルスが届け出されている．そのうち，番号が1～121の121種類が海外で発見された後国内に侵入してきたコンピュータウィルスで，番号123～148の26種類が国内で最初に発見されたコンピュータウィルスである．世界的には9000種類以上のコンピュータウィルスが存在するといわれているが，国内に侵入してきているコンピュータウィルスの種類はまだ意外に少ない．その反面，国内で製造された疑いがあるコンピュータウィルスがすでに26種類も届け出されている．また，番号8～148の141種類がDOS系（WINDOWSでもそのまま動作する）のコンピュータウィルス，残りの番号1～6の6種類がマッキントッシュのコンピュータウィルス，汎用OSのコンピュータウィルスは番号7の1種類だけである．この汎用OSのコンピュータウィルスは1990年に1回届け出されているだけで以降被害届け出はない．現在のところほぼ死滅している状態と考えている．被害届け出状況から判断するに国内に広まっているコンピュータウィルスは，圧倒的にDOS系のものが多いことがわかる．またこれら被害届け出されたコンピュータウィルスの80%以上が海外から侵入してきていることもわかる．

2.3 届け出コンピュータウィルスの傾向

コンピュータウィルスを感染形態で分類するとフロッピーディスクやハードディスクのシステム領域に感染するブートセクタ感染型コンピュータウィルス，プログラムファイルに感染するファイル感染型コンピュータウィルス，前記両方に感染するファイル・ブートセクタ感染型コンピュータウィルス，各種アプリケーションプログラムで作成した添付ファイルに感染するマクロ感染型コンピュータウィルスに分類できる．

次にこれら届け出コンピュータウィルスを感染形態で分析すると，**図-2**に示すようになる．1990年～1993年はファイル感染型のコンピュータウィルスが多いが，1994年以降ブートセクタ感染型のコンピュータウィルスが増え始め1995年～1996年は半数以上を占めるようになった．反面1991年に初めて届け出された感染力が強いファイル・ブートセクタ感染型のコンピュータウィルスは，それほど増加する傾向を示さず1995年～1996年は各々1種類，4種類にとどまっている．

このような状況から推測するに，今後ブートセクタ感染型のコンピュータウィルスが増えていくことが予想される．このタイプのコンピュータウィルスは，システム起動直後にすべてのプログラムに先駆けコンピュータウィルスが動きだす点にある．動き出したコンピュータウィルスはメモリに常駐し自分自身の侵入を隠蔽するステルス機能を動作させることが多い．このため，ワクチン・ソフトウェアを使ってコンピュータウィルスを検査しても，コンピュータウィルスが検出できない．コンピュータウィルス検査を実施するにあたり確実にコンピュータウィルスが侵入していないコンピュータの使用とワクチン・ソフトウェアにコンピュータウィルスが感染していないことが重要なポイントになる．このため検査時には，どのコンピュータを使用したか，どのワクチン・ソフトウェアを使ったか，という記録を残しておくことが重要になる．

またすでに新型のマクロ感染型のコンピュータウィルスの届け出も少なからずきている（103，109番）．このコンピュータウィルスは全世界にネットワークを経由して広まりつつあり，今後最も注意が必要なものになると考えている．

2.4 感染経路

図-3に1996年（1月～12月）に被害届け出さ

表-1 被害届け出ウィルス一覧

番号	ウイルス名 海外で最初に発見された ウイルス	届出件数 '90	'91	'92	'93	'94	'95	'96	合計	備考
1	WDEF	8	7	2	2	1	0	1	21	マッキントッシュ
2	nCVIR		1	2	0	3	1	2	9	
3	CDEF			8	7	5	1	1	22	
4	iNIT29				1	0	0	0	1	
5	ANTI				2	0	0	0	2	
6	MBDF							7	7	
7	クリスマスワーム	1	0	0	0	0	0	0	1	汎用
8	ストーンド	1	6	9	13	6	5	2	42	DOS
9	ストーンドII			2	0	2	3	2	9	
10	カスケード	1	3	43	313	422	132	86	1000	
11	カスケードーB			1	0	0	0	0	1	
12	インベーダー		1	0	1	0	0	0	2	
13	ウインナー		1	0	0	2	0	0	3	
14	ジョシ		2	1	3	1	0	0	8	
15	ダークアベンジャー		2	1	3	0	0	0	6	
16	リバティ		2	2	3	4	0	0	11	
17	エルサレムB		3	3	1	0	0	0	7	
18	イスラエル型	1	0	0	0	0	0	0	1	
19	エルサレム		3	2	14	11	3	0	33	
20	キー・ブレス		2	4	4	0	1	0	11	
21	ヤンキー・ドゥードル		11	118	380	375	100	45	1029	
22	アズサ		1	0	6	3	0	0	10	
23	サンデー		3	9	21	11	2	0	46	
24	ワクシナ		3	0	1	1	0	0	5	
25	プエルト			2	0	0	0	0	2	
26	フォーム			3	42	97	70	77	289	
27	アンチテレフォニカ			4	56	63	31	22	176	
28	ミケランジェロ			8	12	16	1	2	39	
29	15715			4	1	3	1	0	11	
30	1554			1	0	0	0	0	1	
31	フリップ (2153)			1	0	2	0	0	5	
32	フリーハイ			1	0	0	0	0	1	
33	4096			2	0	2	0	0	5	
34	スロー			2	0	0	0	0	2	
35	フレアジャックス			1	0	0	0	0	1	
36	カンス			1	0	5	3	2	13	
37	フィニッシュー709			1	0	0	0	0	1	
38	スクリーム			1	0	0	0	0	1	
39	ハロウイン (1376)				1	2	0	0	3	
40	64				1	0	0	0	1	
41	エアーコップ				1	0	0	0	1	
42	テキーラ				3	2	2	0	6	
43	マミー				2	0	0	1	3	
44	SVC(3.1.5.0.6.0)				2	0	1	0	3	
45	3445				5	4	0	0	9	
46	DiーrーII					0	0	0	1	
47	ピータII				2	25	21	17	65	
48	クラッキー					0	0	0	1	
49	チャンジャ					1	0	0	2	
50	バリティブート					14	15	13	43	
51	ブラッディ					5	1	0	7	
52	シリィ					1	0	0	2	
53	シリクウイアズ					1	0	0	1	
54	スタンフォード					3	0	0	3	
55	ヨンユ					2	0	4	8	
56	モンキー			1		16	33	16	65	
57	D3					6	37	43	86	
58	アルゼンティーナ					2	0	0	2	
59	アンチシーモス					19	98	174	291	
60	ジェリー					1	0	0	1	
61	スタードット					2	0	0	2	
62	ディスクウォッシャー					3	0	0	3	
63	ブート					1	0	0	1	
64	ガニュー					1	0	0	1	
65	クレジーブート					1	0	0	2	
66	ステルスブート						3	1	4	8
67	リトルレッド						1	0	2	3
68	キープレスD						1	0	0	1
69	スイスブート						1	2	0	4
70	ワクシナ16						1	2	0	1
71	DH2						2	6	3	11
72	sPI						1	1	0	2
73	ハイドナウト						1	0	0	1
74	シリーポップ						4	1	3	8
75	WXYC						1	0	0	1
76	タイムワープ						1	1	0	2
77	ブート437						1	1	2	4
78	ホリデーB						1	1	0	2
79	BI						1	14	21	36
80	リッパー						1	16	35	52
81	JAN							1	0	1
82	ジャンキー							3	4	7
83	ノップス							2	2	4
84	Lixi							7	11	18
85	Cvex3							1	1	2
86	タイバン							5	2	7
87	ドスバー							1	0	1
88	ニューイヤー							1	0	1
89	プリントスクリーン							1	0	1
90	モンジュテュー							1	3	4
91	サンボ							17	27	44
92	ナシータ							14	13	27
93	タマンナ							1	0	1
94	ファットアベンジャー							4	1	5
95	ベイジン							5	18	23
96	DSMEコニー							1	0	1
97	V3SCAN							2	0	2
98	モンゴル							2	0	2
99	アンジェリーナ							7	12	19
100	ストーンヘンゲ							1	2	3
101	ダイナモ							1	0	1
102	トロジェクタ							1	0	1
103	WORD_MACRO コンセプト							1	48	49
104	ナタス							3	5	8
105	MCGY2803							1	0	1
106	ウォンカ							1	0	1
107	コンクール							1	0	1
108	ディーエーボーイズ							1	0	1
109	WORD_MACRO カラーズ								19	19
110	ワンハーフ								4	4
111	15イヤーズ								1	1
112	3783								1	1
113	BOOTEXE								1	1
114	HLLP.RNA.7408								1	1
115	YMA3596								1	1
116	エイズ								1	1
117	ジェネシス								1	1
118	バリティenc								1	1
119	バロッテス								1	1
120	ロシアンフラグ								1	1
121	ワーウルフ								1	1
122	ウイルス名不明		1	0	0	0	0	0	1	
	合計	12	52	239	916	1165	697	773	3854	

番号	ウイルス名 日本で最初に発見された ウイルス	届出件数 '90	'91	'92	'93	'94	'95	'96	合計	備考
123	DBf-1	1	0	0	0	0	0	0	1	DOS
124	DApm-2	1	2	6	14	8	2	0	33	
125	DBo-3		1	0	0	0	0	0	1	
126	DBh-4		1	0	1	0	0	0	2	
127	DAn-5		1	0	0	0	0	0	1	
128	DShm-6		1	0	0	0	0	0	1	
129	DApm-7		1	0	0	0	0	0	1	
130	DApm-8			2	0	0	0	0	2	
131	DSofmh-9			4	0	0	0	0	4	
132	DSofmh-10			3	0	0	0	0	3	
133	DAofp-11			1	0	0	0	0	1	
134	DApm-12			2	0	0	0	0	2	
135	DApdm-13			3	1	0	0	0	4	
136	DBmh-14			1	3	2	0	0	6	
137	DApm-15			1	0	0	0	0	1	
138	DSpdh-16				3	0	0	0	3	
139	DTd-17				1	0	0	0	1	
140	DBfs-18				1	0	0	0	1	
141	DBn-19				1	1	0	0	2	
142	DAmh-20				2	1	0	0	3	
143	DAn-21				1	0	0	0	1	
144	DAmh-22					2	0	0	2	
145	DAn-23					5	0	0	5	
146	DAn-24						1	0	1	
147	DAmh-25						1	0	1	
148	DAdmh-26							1	1	
	合計	2	7	23	28	19	4	1	84	

注) 1件の届出で複数種類のウイルスの届出も含む。 出典：情報処理振興事業協会

れた感染経路の内訳を示す．感染経路が特定できていない感染経路不明の届け出が約40%もある．コンピュータウィルスの侵入を防止するには，コンピュータの利用を管理することが重要であるにもかかわらず管理していないコンピュータが非常に多いことがわかる．コンピュータの利用者とそのとき使用する記録媒体の管理を実施していただきたい．コンピュータを管理することにより，コンピュータウィルスの侵入を防止できるだけでなく，被害が発生した場合感染範囲を早期に特定できるようになるため，被害を最小に抑えることができる．

ある程度感染経路が特定できているものでは外部からのフロッピーディスク/ハードディスクが約44%と一番多い．フロッピーディスクを外部から持ち込むとき，外部で使用したフロッピーディスクを持ち帰るときは，とくに厳重なるコンピュータウィルス検査が必要である．

このほか，1996年12月現在ではあまり被害が報告されていないが，被害が多くなることが予測されるものに電子メールによる感染がある．マクロ感染型のコンピュータウィルスには，マイクロソフト社のWORDやEXCELで作成した添付ファイルに感染するものがある．これら添付ファイルがネットワークを介して電子メールでやりとりされることで，ネットワークを介してマクロ感染型のコンピュータウィルスがコンピュータに侵入してくる．今後この新たな侵入口への対策が重要になる．

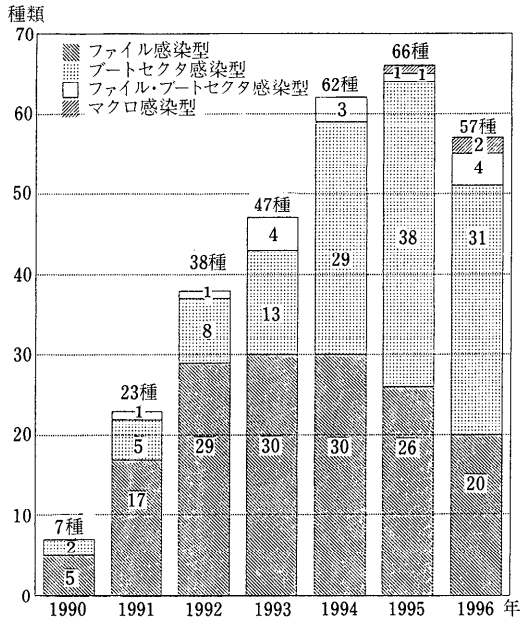


図-2 感染形態からみた傾向

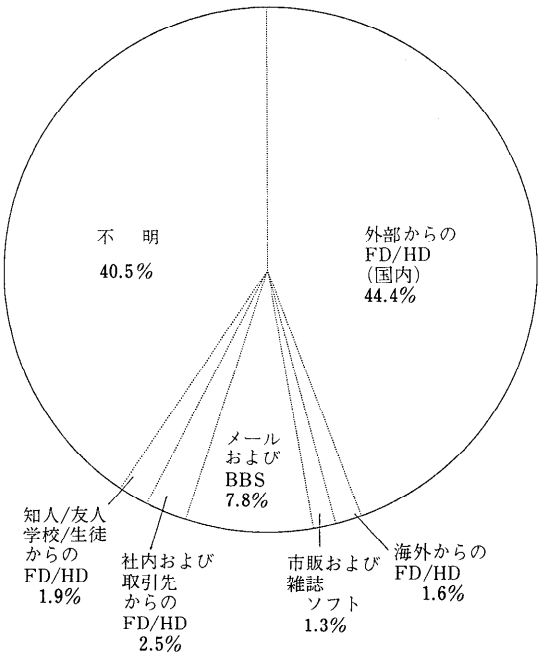
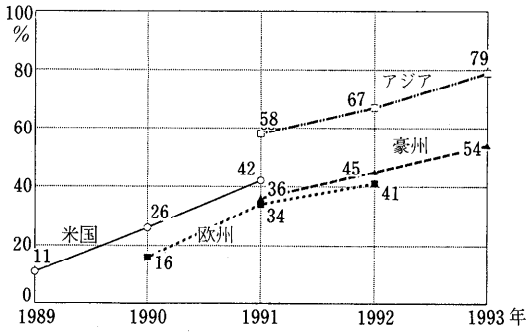


図-3 被害届け出の感染経路

3. 海外のコンピュータウィルス被害

海外では被害届け出制度のようなものを実施している国がない．そこで情報処理振興事業協会では，アンケート方式で，米国，欧州地域（イギリス，ドイツ，フランス），アジア地域（香港，シンガポール，韓国，台湾），豪州地域のコンピュータウィルス被害を調査した．ただし，調査した年が少し古いため，マクロ感染型のコンピュータウィルスの被害状況は調査できていない．

表-2 各国のコンピュータウィルス感染者



3.1 海外の被害状況の推移

表-2 に各国のコンピュータウィルス感染者の年別推移を示す．米国での被害は初年に比較して3年後には約4倍に増加しており，1991年の感染経験のある者の比率が42%に達している．また，欧州でも米国と同じように増加傾向を示し，1992年には初年度の約2.5倍の41%に達している．一方アジアでは初年度から58%と高い感染経験者率を示し，1993年には初年度の約1.5倍の79%にも達している．各国の調査年度が異なるので単純には比較できないが海外では急激にコンピュータウィルスの被害が広まっている．

3.2 コンピュータウィルスの種類

各国での主なDOS系コンピュータウィルスの被害をみると，ストーンド，エルサレム，ミケランジェロの感染被害が広まっている．次に，これら被害をコンピュータウィルスの感染形態から分類すると，米国およびアジア，豪州ではブートセクタ感染型のコンピュータウイルスによる被害が多い傾向，欧州ではファイル感染型とブートセクタ感染型による被害で2分されている傾向になっている．DOS系コンピュータウィルスの種類は世界的には非常に多くの種類が発生しているが，各国や地域ごとに数千種類ものコンピュータウィルスが流行っているのではなく，2〜3種類のコンピュータウィルス被害が集中しているのがわかる．

一方の各国のMacintoshコンピュータウィルスは，DOS系コンピュータウィルスに比較して

少なく，種類も各地域ごとで差はない．各地域ともWDEF，nVIR，CDEF，SCORESの4種類のコンピュータウィルスによる被害で占められていて国内と同じ傾向を示している．

このほかUNIXおよび汎用OSのコンピュータウィルスによる被害についても同時に調査したが，国内と同じくほとんど被害が出ていない．

4. IPAのコンピュータウィルス対策活動

IPAのコンピュータセキュリティ技術調査室ではコンピュータウィルス対策として被害の届け出の受理およびアンケートによる被害調査とコンピュータウィルスの侵入を防止するための研究を行っている．

4.1 被害届け出・相談

コンピュータウィルスの被害状況については，**2章**に記述したので，ここでは被害の届け出方法および相談方法を紹介する．

被害届け出は，被害者の連絡先・被害日時・コンピュータウィルスの種類・被害状況・侵入経路などをわかる範囲で記述し（定型用紙はIPAに備えてある），郵送・FAX・電子メール・パソコン通信などで提出するようになっている．このとき，新種のコンピュータウィルスが発見されたなどの場合，コンピュータウィルス自身の検体も提供していただくことがある．IPAではこれら提供情報を解析・分析しプライバシを守る形態で情報蓄積して，コンピュータウィルス対策に活用している．また相談時には，コンピュータウィルスに感染した場合のコンピュータウィルスの駆除方法およびシステムの復旧方法，国内の被害情報・対策情報などを提供している．いずれも無料で対応しているので，論末の連絡先に気軽に相談していただきたい．

4.2 研　　究

IPAで実施している研究は，インテグリティ検査法と呼んでいる．現状コンピュータウィルスを検出するとき，ワクチン・ソフトウェアを使うが，このワクチン・ソフトウェアは記録媒体に侵入した未知のコンピュータウィルスを発見することができないため，常に対応が後手に回っている．このような問題点を解決するために，暗号技術を応用したインテグリティ法の研究に取り組むことにした．この研究は，コンピュータウィルスがファイルおよびシステムに感染したとき，感染した場所の完全性が崩れることを利用して異常を発見する方法で，コンピュータウィルスが既知・未知の状況を問わずすべてのコンピュータウィルスを発見する．それでは実際，どのようにソフトウェアに侵入したコンピュータウィルスが発見できるかみることにする．初めにソフトウェアを販売・配布するメーカが2種類の鍵を作る．1つは，メーカ自身が販売・配布するソフトウェアに暗号技術を使ってデジタル署名するときに使用するもので，使用後秘密がほかの者に漏れないように厳重に管理する．インテグリティ検査法ではこの鍵のことを秘密鍵と呼んで，メーカだけが使用するようになっている．もう1つは，ソフトウェアの利用者が，入手したソフトウェアにコンピュータウィルスが侵入しているかどうか検証するときに使うもので，ソフトウェアを入手した利用者は，各ソフトウェアに対応した鍵を鍵管理機関などから入手して，ソフトウェアの内容が正しいことを検証する．インテグリティ検査法では，先程の秘密鍵に対して，利用者が使う鍵を公開鍵と呼んでいる．この段階において，コンピュータウィルスがソフトウェアに侵入していれば，ソフトウェアの内容がオリジナルと異なる状態になっているので，メーカが秘密鍵でソフトウェアにつけたデジタル署名とユーザが公開鍵で作成したデジタル署名が一致しなくなり，コンピュータウィルスを検出できる仕掛けになっている．

IPAではこの研究をより多くの方に利用していただくことにより，ソフトウェアの流通過程（特に通信ネットワークを介した）でのコンピュータウィルス侵入を防止できると考えている．

5. おわりに

以上コンピュータウィルス対策の方法をみてきたが，近年のインターネットを代表する通信ネットワークの普及・発展を考えるに，今後コンピュータウィルスだけではなく，ネットワークを介して他人のコンピュータに侵入して各種悪さをするコンピュータ不正アクセスが社会的に問題になってくると推測できる．IPAでは，これら行為に対する対策の研究を実施して行くためには，コンピュータウィルス対策のときと同様に現状の被害状態の把握が必須であると考える．そこでこのた

めの被害情報の収集を1995年8月よりIPAの自主事業として独自に行ってきたが，1996年8月に通産省が「コンピュータ不正アクセス対策基準」を告示したことで，正式に「コンピュータ不正アクセスの被害の届け出制度」がスタートした．これからの情報化社会をより安全にしていくためにも，前記のコンピュータウィルス被害のときと同様にコンピュータ不正アクセス被害の届け出にもご協力をお願いしたい．

[連絡先]

・住所：東京都港区芝公園3丁目1番38号
秀和芝公園3丁目ビル6F
・代表電話：03-3437-2301
・相談電話：03-3433-4844
・FAX ：03-3437-2537
・BBS ：03-3459-8944（N 81 XN）
・WWW ：http://www.ipa.go.jp/SECURITY/index-j.html
・e-mail ：virus@adm.ipa.go.jp

参考文献

1) 棟上昭男 編著：ウィルス退治，共立出版情報フロンティアシリーズ13情報処理学会編．
2) 情報処理振興事業協会コンピュータウィルス対策室編：コンピュータウィルスのおはなし，日本企画協会．
3) 通商産業省：コンピュータウィルス対策基準解説書，日本情報処理開発協会．
4) Hoffman, L. J.: Rougue Programs: Viruses, Worms, and Trojan Horses (1990).
5) Dr. Cohen, F. B.: A SHORT COURSE ON COMPUTER VIRUSES Second Edition (1994).

（平成8年10月8日受付）

中村 達（正会員）

1950年生．1972年現(株)アイネス（旧協栄計算センター）に入社．オペレーティングシステム，エキスパートシステムの研究・開発に従事．1993年情報処理振興事業協会出向．コンピュータウィルス技術調査室室長．1996年同協会セキュリティセンター・ウィルス対策室および不正アクセス対策室室長．1995年通産省告示「コンピュータウィルス対策基準」改定WGの主査．1996年通産省告示「コンピュータ不正アクセス対策基準」検討WGの主査．人工知能学会会員．