

平成 9 年
海外（米、欧、亜）における
コンピュータウイルス
被害状況調査報告書

平成 10 年 7 月

情報処理振興事業協会
セキュリティセンター

はじめに

本概要報告書は、情報処理振興事業協会が過去 1 年間で実施した『海外におけるコンピュータウイルス被害状況調査』の結果をとりまとめたものです。平成 9 年度に実施した調査では、米国、欧州 2 ヶ国（イギリス、ドイツ）、そして香港、シンガポールを対象として調査を行いました。

調査結果では、各国ともに非常に高いウイルス感染率が報告されています。インターネット/イントラネットの普及に伴い、社内や事業所間では、稟議書、提案書等、また取引先などの社外向けでは、価格表や見積書などのデータファイルを E-mail で送付するなどの方法が急速に普及してきており、マクロウイルス等の被害は急速に広がっています。

本調査で確認された海外における被害の実態や、防止技術や回復方法等の対策に関する方向性が、我が国におけるコンピュータウイルス等の防止策の検討に活用され、将来の被害防止に寄与できれば幸甚です。なお、今回の調査にあたり、アンケートにご協力頂いた海外の多数のご回答者、並びに調査結果のとりまとめにご尽力頂いた株式会社三菱総合研究所に感謝いたします。

1998 年 7 月

情報処理振興事業協会
セキュリティセンター

目 次

1. 調査概要

1.1 調査の目的	1
1.2 調査対象	1
1.3 調査方法	1
1.4 実施期間	1
1.5 調査項目	2
1.6 アンケート回収数(率)	3
1.7 その他	3

2. 回答者の属性

2.1 業種	4
2.2 従業員規模	6
2.3 利用しているコンピュータの種類と台数	7
2.4 ネットワーク化の状況	9
2.4.1 社内情報ネットワークの構築状況	9
2.4.2 インターネット接続状況	11
2.4.3 商用パソコン通信サービスの利用状況	12
2.4.4 商用 VAN ネットおよびその他の企業間ネットワークの接続状況	14

3. コンピュータウイルスによる被害状況

3.1 コンピュータウイルスに対する関心	15
3.1.1 コンピュータウイルスの認知度	15
3.1.2 コンピュータウイルスに対する脅威	15
3.1.3 今後の被害予想	16
3.1.4 求められている情報	18
3.2 コンピュータウイルスによる被害状況	19
3.2.1 コンピュータウイルス感染経験の有無	19
3.2.2 感染したウイルスの種類数	19
3.2.3 感染したウイルスの名称	20
3.2.4 感染したコンピュータの延べ台数	22
3.2.5 感染した FD の累計枚数	22

4. コンピュータウイルスの対策の現状と課題

4.1 セキュリティ対策実施状況	23
4.1.1 現在実施しているセキュリティ対策	23
4.1.2 今後実施予定のセキュリティ対策	24

4.1.3	ウイルス対策に関するユーザ教育	26
4.2	ワクチンソフト	27
4.2.1	情報源	27
4.2.2	導入目的	28
4.2.3	選択基準	29

5. コンピュータウイルス被害分析調査報告

5.1	感染したコンピュータの種類と台数	30
5.2	発見の経緯	32
5.3	発見に使用したワクチンソフト	33
5.4	感染経路	34
5.5	復旧方法	35
5.6	被害規模	36
5.6.1	復旧に要した期間	36
5.6.2	復旧に要した人日	37

6. まとめ

7. 資料編

7.1	調査表	39
7.2	調査結果集計一覧	46

1. 調査概要

1.1 調査の目的

本調査は、米国、欧州、アジア・豪州の3地域において、「コンピュータウイルス等被害状況調査」を行い、海外におけるウイルスの被害状況とその対策について幅広く情報を収集分析し、コンピュータウイルスに関する有効な対策技術の開発に役立てることを目的に実施した。

1.2 調査対象

(1) 調査対象国

米国、ドイツ、イギリス、香港、シンガポールの5ヶ国を対象に調査を実施した。

(2) 調査対象者

企業、大学、研究機関、ソフトハウス等のコンピュータ管理者（Information System Manager）を調査対象として抽出した。

アンケートの調査対象先の選定にあたっては、各国の調査会社に委託し、それぞれの国のコンピュータユーザ（MIS Manager and DP Manager）関連の各種データベースや、関連団体の会員リスト等を用いた。（MIS: Management Information System）

1.3 調査方法

郵送による発送回収のアンケート方法を採用した。

調査の実施にあたっては、翻訳した調査票を送付した。

1.4 実施期間

本調査は、米国、ドイツ、イギリス、香港、シンガポールの5地域に、1997年度に限り実施した。

1.5 調査項目

本調査は、以下の項目を中心に調査票を設定した。また、調査は1997年度1年間に実施した。

回答事業所属性

- (1) 主たる業種
- (2) 就業者数
- (3) 利用しているコンピュータの種類別台数
- (4) 社内情報ネットワークの構築状況
 - 社内情報ネットワークの用途
 - インターネット接続の有無
 - ホームページの有無
- (5) 商用パソコン通信サービスの利用状況
 - 利用している商用パソコン通信サービス
- (6) 商用VANネット等との接続状況

コンピュータウイルスによる被害状況

- (1) コンピュータウイルスの認知度
- (2) コンピュータウイルスへの脅威
- (3) コンピュータウイルス感染の有無
 - 感染したウイルスの種類
 - 感染したウイルスの名称
 - 感染したコンピュータの種類と台数
 - 感染したフロッピーディスクの枚数
 - 発見の経緯
 - 使用したワクチンソフト
 - 想定される感染経路
 - 復旧方法
 - 被害規模(期間・投入人日)
- (4) 現在および今後のセキュリティ対策
- (5) ウイルス対策に関するユーザ教育
- (6) ワクチンソフトの情報源
- (7) ワクチンソフトの導入目的
- (8) ワクチンソフトの選択基準
- (9) 今後の被害予測
- (10) 求める情報

1.6 アンケート回収数（率）

アンケート全体の有効回収数は1,136件、回収率は4.5%という結果になった。

国別、地域別の回収数、及び回収率は以下の通りで、それぞれの地域や国によって郵送アンケート調査の環境が異なるため、回収率はイギリス、ドイツの3.3%から、米国の6.4%まで開きがみられる。しかし、各国とも約150件以上は回収できており、国別の傾向を把握することは可能である。

表 1.6 アンケートの発送・回収結果一覧

項目 国・地域	発送数	回収数	回収率
米 国	5,000 件	318 件	6.4%
イギリス	5,000	165	3.3
ドイツ	5,000	163	3.3
香 港	5,000	216	4.3
シンガポール	5,000	274	5.5
合 計	25,000	1,136	4.5

1.7 その他

本調査は、株式会社三菱総合研究所にアンケートの準備や、海外の調査会社との業務調整等を委託して行った。

2. 回答者の属性

本調査は、コンピュータを利用している企業、大学、研究機関、ソフトハウス等を、データベースや団体会員リスト等を用いて抽出し、コンピュータ管理者宛に郵送して行われたものである。抽出の方法等は5カ国とも同じ方法を採用したが、それぞれの地域別に状況が異なるため回答者の属性比率は異なった値になっている。

地域別回答者の業種、従業員規模別の分類は以下の通りである。

2.1 業種

業種は地域によってかなりばらつきがあり、米国では、金融・保険業 12.9%、教育・研究機関 10%の順になっているが、他国では製造業が多い。

回答者の業種の割合は、それぞれの国の産業構造等によっても異なるが、全体としてはかなり広範囲な業種から回答を得ている。

表 2.1 回答者の業種別地域別分類

業種	米 国		イギリス		ドイツ		香 港		シンガポール	
	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比
農林・水産業	12 件	3.8%	1	0.6	4	2.5	2	0.9	3	1.1
鉱業	2	0.6	0	0.0	2	1.2	0	0.0	2	0.7
建設業	6	1.9	2	1.2	9	5.5	17	7.9	13	4.8
製造業	26	8.3	36	22.1	24	14.7	42	19.5	96	35.3
出版・印刷業	3	1.0	2	1.2	13	8.0	3	1.4	2	0.7
卸売・小売業	16	5.1	12	7.4	23	14.1	11	5.1	18	6.6
金融・保険業	40	12.8	13	8.0	12	7.4	24	11.2	17	6.3
不動産業	11	3.5	0	0.0	1	0.6	5	2.3	1	0.4
運輸業	9	2.9	2	1.2	4	2.5	14	6.5	12	4.4
通信業	14	4.5	1	0.6	2	1.2	9	4.2	1	0.4
電力業	8	2.6	4	2.5	9	5.5	2	0.9	5	1.8
ガス業	5	1.6	0	0.0	1	0.6	0	0.0	1	0.4
新聞・放送業	3	1.0	0	0.0	7	4.3	1	0.5	0	0.0
情報サービス業	9	2.9	5	3.1	5	3.1	7	3.3	10	3.7
物品賃貸業	2	0.6	2	1.2	1	0.6	0	0.0	2	0.7
遊興娯楽業	2	0.6	0	0.0	0	0.0	0	0.0	0	0.0
医療業	8	2.6	2	1.2	3	1.8	3	1.4	1	0.4
教育・研究機関	31	9.9	8	4.9	0	0.0	15	7.0	3	1.1
政治、経済、文化団体	1	0.3	0	0.0	1	0.6	0	0.0	0	0.0
その他サービス業	17	5.4	28	17.2	11	6.7	8	3.7	16	5.9
政府または政府関係機関	8	2.6	4	2.5	4	2.5	2	0.9	0	0.0
地方公共団体	1	0.3	1	0.6	5	3.1	0	0.0	0	0.0
その他	79	25.2	40	24.5	22	13.5	50	23.3	69	25.4
合 計	313	100.0	163	100.0	163	100.0	215	100.0	272	100.0
不 明	5		2		0		1		2	

その他：慈善団体、教会、会員制組織、個人介護、老人ホーム、リサイクル事業、宗教団体、社会福祉、ボランティア団体、ごみ焼却（エネルギー再利用）事業、水道業、など

2.2 従業員規模

回答者の属する組織の従業員規模別の構成は以下の通りである。

従業員規模別の分類もそれぞれの地域の状況によって異なるが、全体としては10名以下の小さな組織から、1万名を超える非常に大規模な組織まで幅広く含まれている。地域別には、米国が大規模な組織の回答が多く、他の国では比較的規模の小さな組織の回答が多い傾向がみられる。

回答者の属する組織の従業員規模別の構成は以下の通りである。

表 2.2 回答者の属する組織の従業員規模

従業員数	米 国		イギリス		ドイ ツ		香 港		シンガポール	
	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比
50名未満	120件	39.7%	44	26.8	41	25.2	58	27.0	84	31.1
50～99名	27	8.9	16	9.8	23	14.1	38	17.7	48	17.8
100～299名	31	10.3	28	17.1	38	23.3	33	15.3	58	21.5
300～499名	14	4.6	20	12.2	14	8.6	9	4.2	14	5.2
500～999名	18	6.0	27	16.5	16	9.8	15	7.0	16	5.9
1,000名以上	92	30.5	29	17.7	31	19.0	47	28.8	50	18.5
合 計	302	100.0	164	100.0	163	100.0	215	100.0	270	100.0
不 明	16		1		0		1		4	

2.3 利用しているコンピュータの種類と台数

利用しているコンピュータの台数を種類別に見ると、米国での「汎用機」、「ワークステーション」の台数が多いことが目立つ。

図 2.3.1 利用しているコンピュータ 汎用機

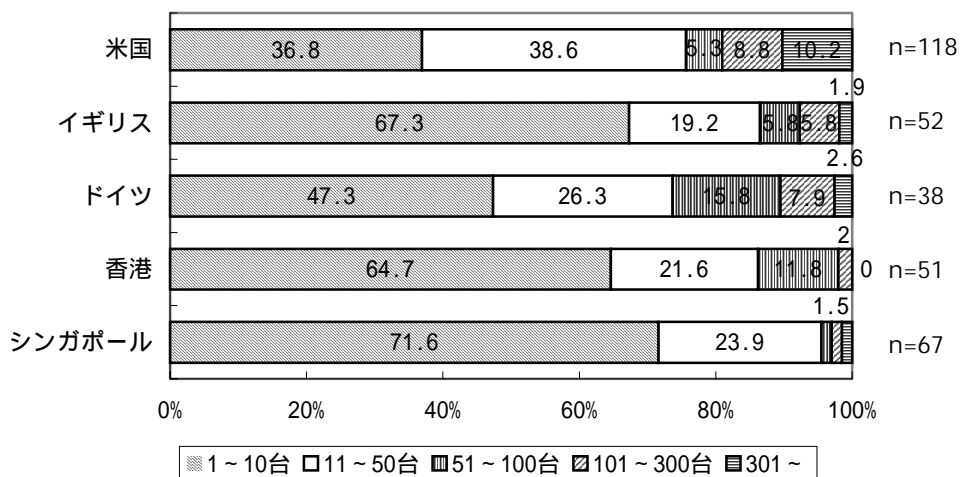


図 2.3.2 利用しているコンピュータ ワークステーション

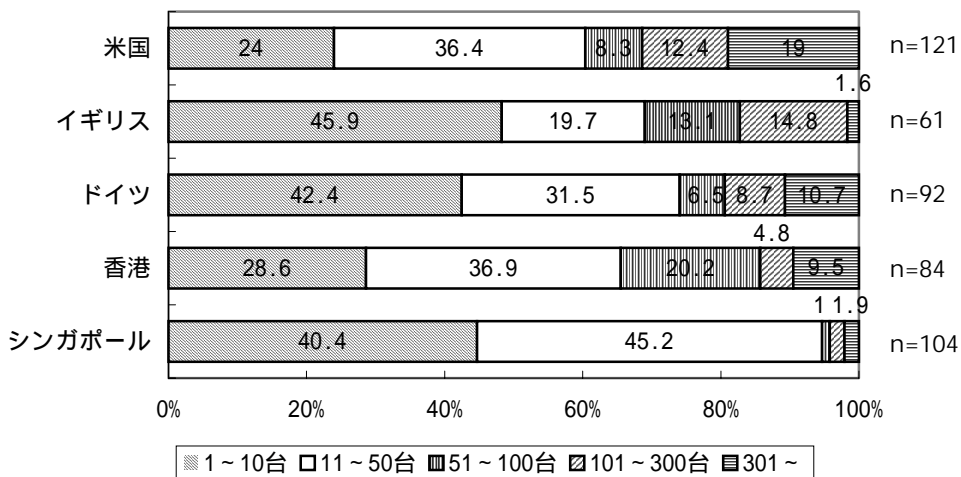


図 2.3.3 利用しているコンピュータ DOS、Windows

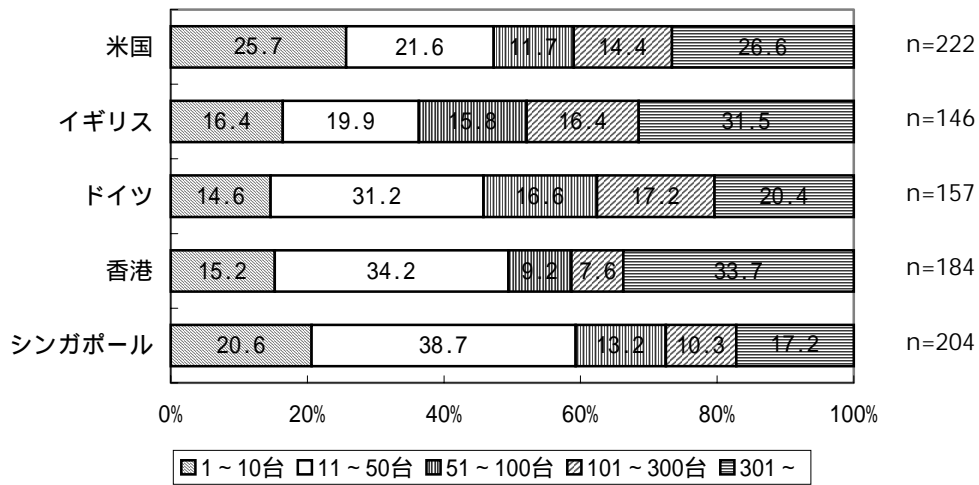
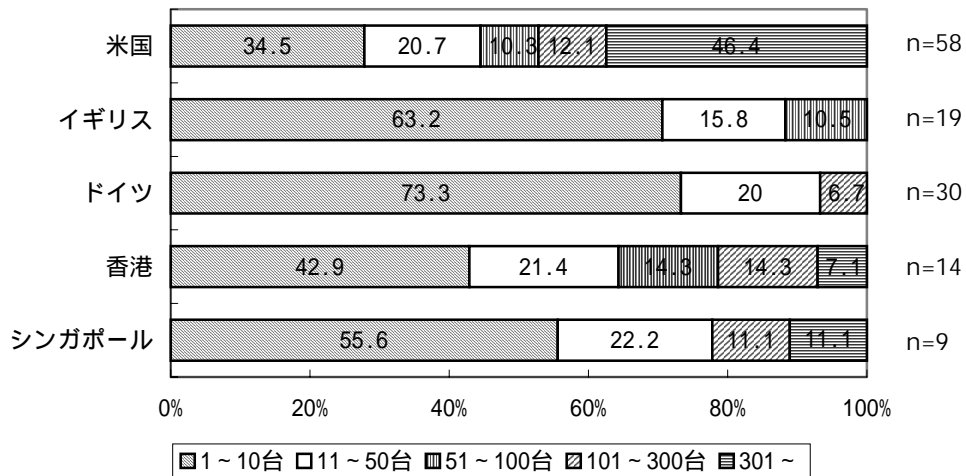


図 2.3.4 利用しているコンピュータ Macintosh



2.4 ネットワーク化の状況

2.4.1 社内情報ネットワークの構築状況

(1) 社内情報ネットワークの構築状況

社内情報ネットワークについては、各国とも 80%以上の事業所で社内情報ネットワークが構築されている。

表 2.4.1(1) 社内情報ネットワークの構築状況

ネットワーク	米 国		イギリス		ドイツ		香 港		シンガポール	
	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比
事業所内ネットワークのみ	93 件	33.2%	66	40.2	77	47.2	128	60.4	133	50.8
事業所間ネットワークまで	141	50.4	88	53.7	73	44.8	59	27.8	80	30.5
ネットワーク未構築	46	16.4	10	6.1	13	8.0	25	11.8	49	18.7
合 計	280	100.0	164	100.0	163	100.0	212	100.0	262	100.0

(2) 社内情報ネットワークの用途

社内情報ネットワークの用途としては、「電子メール」、「経理系」、「データベース検索」が各国とも10%を超えている。

表 2.4.1(2) 社内情報ネットワークの用途

用途	米 国		イギリス		ドイツ		香 港		シンガポール	
	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比
販売管理系	106件	8.8%	98	15.0	106	12.7	83	12.7	129	15.7
生産管理系	99	8.3	46	7.0	61	7.6	55	8.4	53	6.4
技術系(制御、管制等)	75	6.3	32	4.9	49	5.9	38	5.8	40	4.9
経理系	178	14.8	117	17.9	116	13.9	109	16.7	135	16.4
開発系(技術計算、CAD等)	106	8.8	53	8.1	80	1.0	49	7.5	55	6.7
信用情報	55	4.6	20	3.1	43	5.1	22	3.4	25	3.0
データベース検索	180	15.0	95	14.5	110	13.2	129	19.7	130	15.8
TSS	25	2.1	4	0.6	30	0.4	9	1.4	8	1.0
金融総合オンライン	78	7.3	39	6.0	49	5.9	30	4.6	33	4.0
警備システム	83	6.9	27	4.1	53	6.3	23	3.5	20	2.4
電子メール	180	15.0	105	16.0	116	13.9	107	16.4	177	21.5
その他	26	2.2	19	2.9	22	2.6	13	2.0	17	2.1
合 計	1200	100.0	655	100.0	835	100.0	654	100.0	822	100.0

(複数回答有り)

その他：ファイル共有、インターネット、インターネット接続教育・プログラミング情報交換、在庫管理、OA、周辺機器共有、研究開発、授業、など

2.4.2 インターネット接続状況

インターネットへの接続状況については、「接続している」事業所は各国とも 50%を超えている。

また、接続している事業所で事業所のホームページが「ある」事業所は、米国が 80%と高くなっており、香港、シンガポールも 50%を超えている。

図 2.4.2(1) インターネットへの接続状況

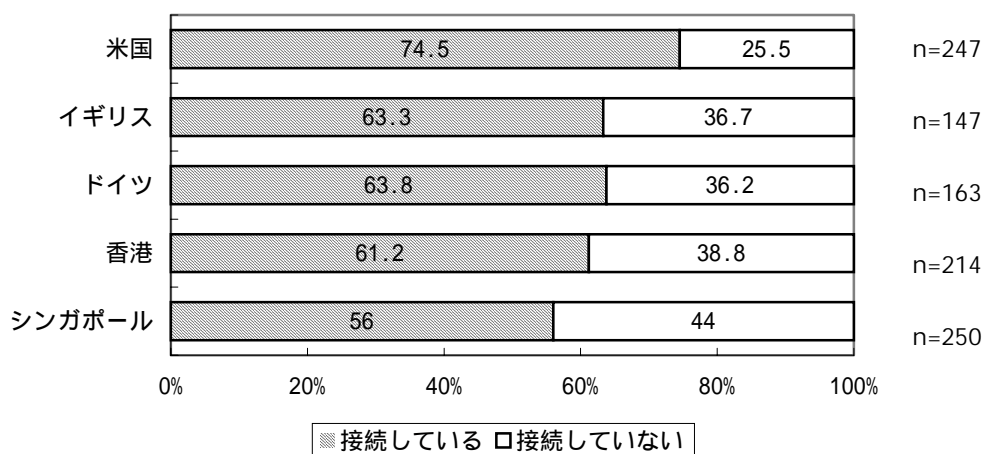
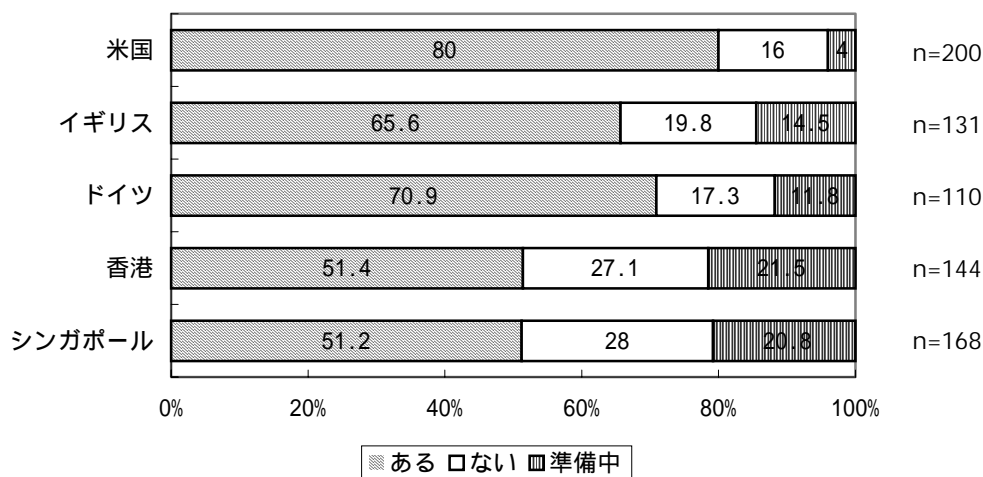


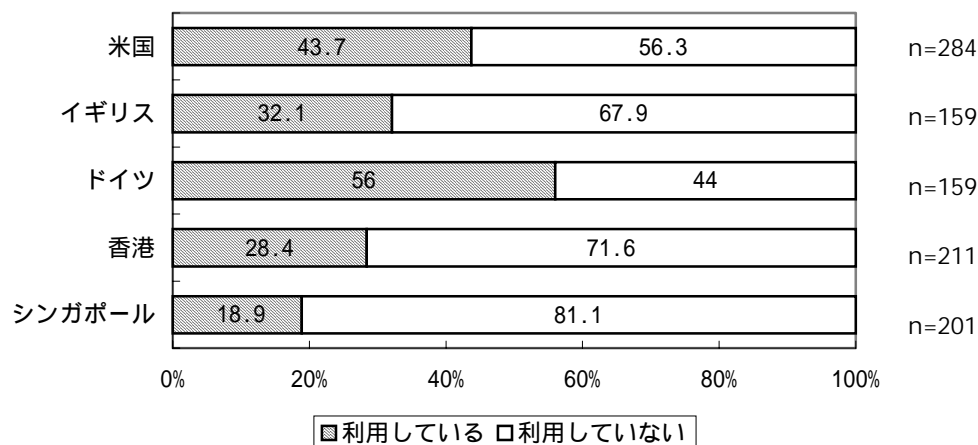
図 2.4.2(2) 自事業所ホームページの有無



2.4.3 商用パソコン通信サービスの利用状況

商用パソコン通信サービスの利用状況については、「利用している」事業所はシンガポールの18.9%から、ドイツの56%までかなりの開きが見られる。

図 2.4.3 商用パソコン通信サービスの利用状況



商用パソコン通信サービス名称：AOL、APPLE TALK、AsiaOnLine、ASTN、AT&T NET、AT&T Frame-relay、ATM、ATT、BANYAN VINES、BBN、Bloomberg、British Telecoms and IIN、BT Frame-relay、BT INTERNET、BT SMDS WAN、BT2000、COMPUSERVE、CPF OnLine、Cybercash、Cyberway、Dan & Bradstreet、DEC-NET、Delta Net、DEMON、DS3/OC-3、EARTHLINK、EDI、Electronic Commerce、FRAME RELAY、FTAM、GEIS.、Gateway、GE、GE-MARK、BLOBAL ONE、GTE Internetworking、HK Telecom、Hong Kong STAR、IBM NET、IBM ADVANTIS、IBM Global Network、INFONET、IMS NETVIGATOR、Internet、Internet & WAN links、ISA、ISDN/T1、ISP、ISP for internet access、ISP for PPP、LE-net、London Insurance Market Network、Marinet Global Messaging Services、MCI、MOTOR DRIVE、MRNET、MSN、NIL、NOVELL、NYSERNet、ONLINE BANKING、OSNAJRUECK、Pacific Internet、PACNET、PIPEX、Port Net、PSINet、QUZA、Reuter Financial News、Reuters、Reuters & Bavtech、

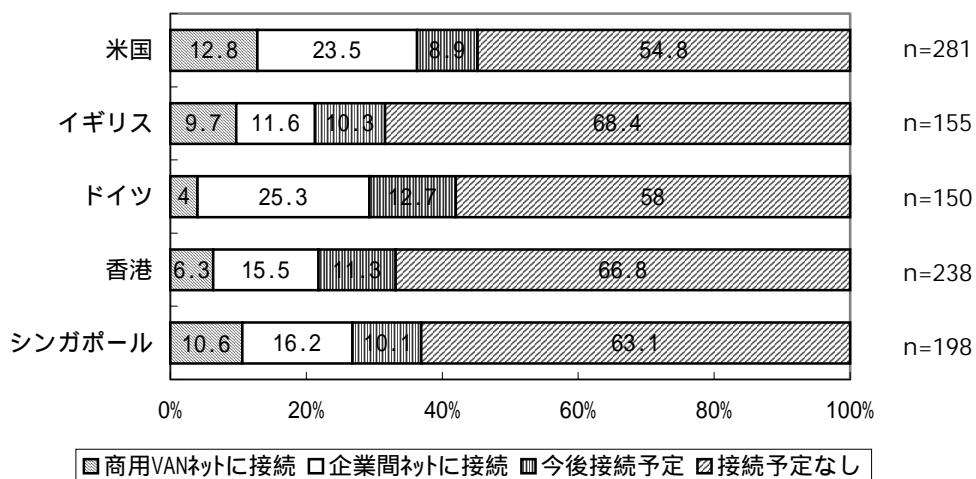
SAP、Singapore Network Services、Singnet、SITA、SNS、
Southwestern Bell、SPRINT、SPRINT Frame-relay、
SPRINT Managed Power、STAR INTERNET、
TELECOM、T-Online、Trade Net、
UU NET、
V-Online、Value added network、VAN、
WEB WORLD、WEBTRON、World Net、WORLD.COM、
X25、X-Link、
York Multimedia Network、など

2.4.4 商用 VAN ネットおよびその他の企業間ネットワークの接続状況

「商用 VAN ネットに接続している」企業については、ドイツの 4%から、米国の 12.8%まで開きがみられる。

「企業間ネットに接続している」企業は、米国、ドイツが 20%を超えている。

図 2.4.3 商用 VAN ネット接続状況



商用 VAN ネット名称：ADVANTIS、AT&T、

BT、BT SMDS、

DIAL T、DIAL PLUS、

F-PROT DISINFECT、

GE、GEIS、GE-MARK、GNS、

HK Linkage Online、

IBM Frame-relay、IBM GLOBAL、INFONET ANS、IVANS、

MCI(F/R)、

NYSERNet、

SITA、SNS、STERLING、

TMI、

W I Net、

YOB E-Banking、など

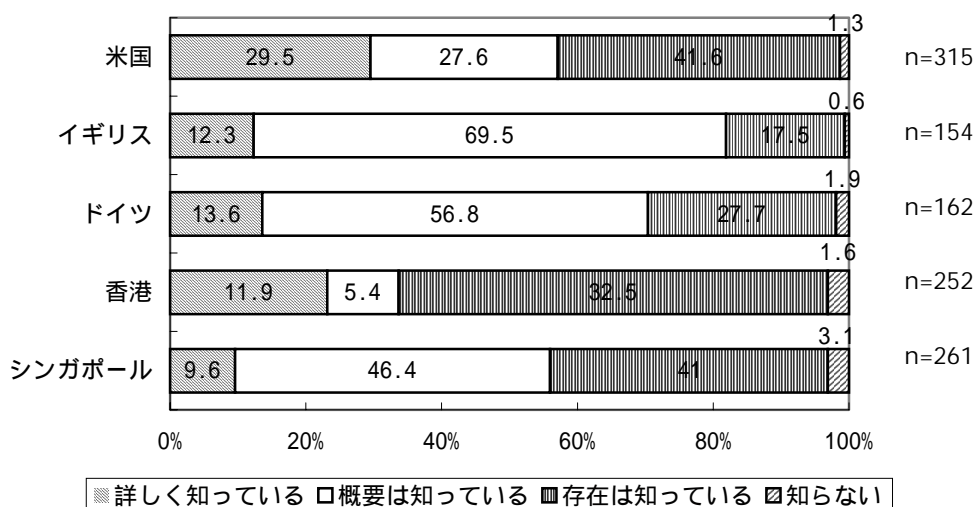
3. コンピュータウイルスによる被害状況

3.1 コンピュータウイルスに対する関心

3.1.1 コンピュータウイルスの認知度

コンピュータウイルスについて、「詳しく知っている」企業は米国で 29.5%と高くなっている。「詳しく知っている」または「概要は知っている」企業は、米国、イギリス、ドイツ、シンガポールで 50%を超えているのに対し、香港では 15%程度である。

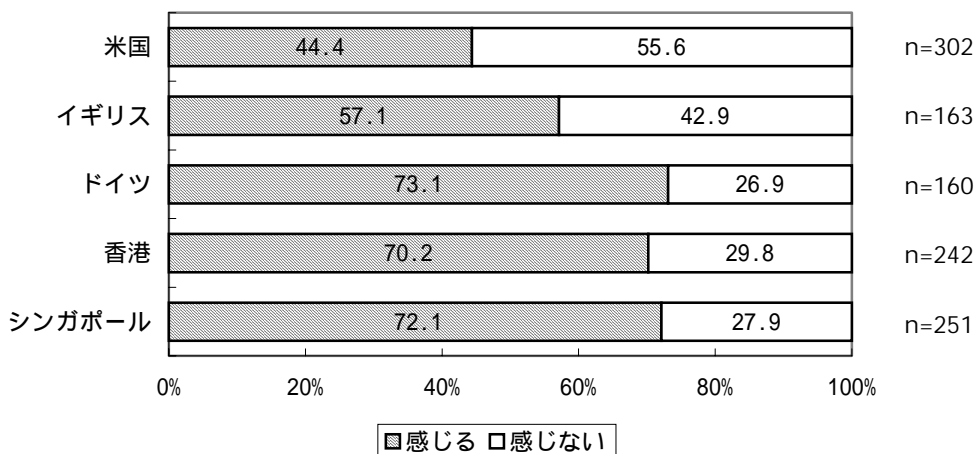
図 3.1.1 コンピュータウイルスの認知度



3.1.2 コンピュータウイルスに対する脅威

コンピュータウイルスに対する脅威については、ドイツ、香港、シンガポールでは「感じる」とする企業が多い。

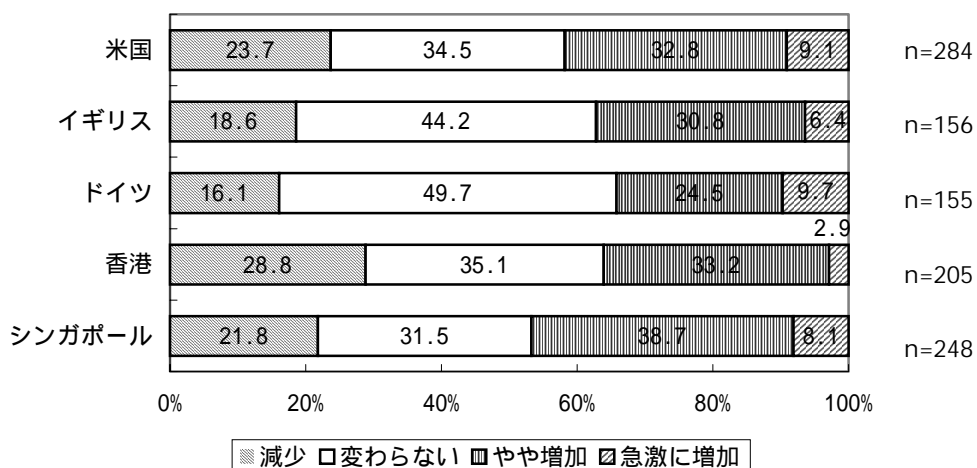
図 3.1.2 コンピュータウイルスに対する脅威



3.1.3 今後の被害予想

今後の被害については、「変わらない」又は「やや増加」とする回答が多く、各国とも今後もウイルス被害は増大すると考えている。

図 3.1.3 今後の被害予想



減少の理由：現在ほとんどのユーザはワクチンを所有している、ユーザのウイルスに対する意識が高まった、ワクチンは年間数回もアップデートされる、ウイルス検査手続きとユーザ教育は高水準となった、すべての PC にワクチンが装備される、よりよいワクチンが開発される、多種のウイルススキャナーを使用される、ネットワークセキュリティが良くなる、WWW から簡単に情報とワクチンのアップデートを入手できる、システムプロテクトコードをインストールした、大多数のシステムがプロテクトされている、など

変わらない理由：旧種がストップされるうちに、新種が出てくる、ワクチンの開発は新ウイルスに追い付く、今の状況は過去数年と変わらない、ユーザがウイルス感染ディスクを使用しないようにするのは不可能、拡散が防げる、感染したことがない - これからも頑張っていくつもり、減る理由はなにもない、プロテクトシステムの顕著な改善がみられない、ウイルスが存在しなければならない、など

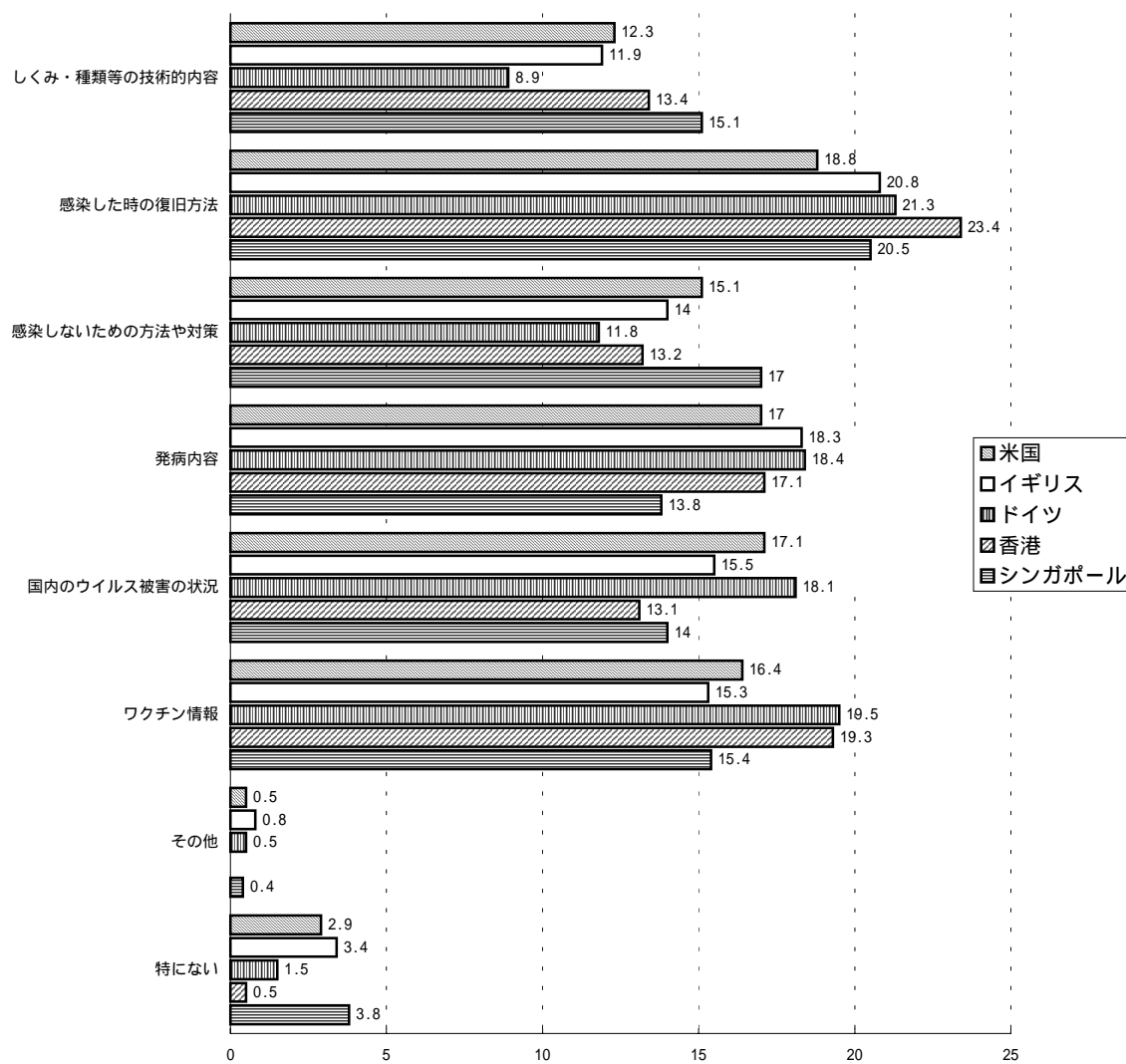
やや増加の理由：E-mail 使用の増加、新しいコンピュータの導入、ウイルスはワクチンが開発される前に開発・拡散されている、WWW への接続の増加、家庭使用率の増大、インターネットとイントラネット使用の増加、外部データソースへのアクセスの増加、ソフトのダウンロードによる感染、WAN の導入、コンピュータとネットワーク接続の増加、インターネット経由ファイルの増加、マクロウイルスの増加、オープンシステムの増加、データ交換の増加、など

急激に増加する理由：ネットワークの急激な成長、ウイルス生産の成長、ネットワーク機能の増加、コンピュータ情報使用率の増大、ユーザの無関心、ユーザが与えられたワクチンを使用しない、結局 Java + ActiveX のようなインターネット言語によってウイルスが自ら拡散していく、など

3.1.4 求められている情報

コンピュータウイルスについて、求められている情報は、「感染したときの復旧方法」が最も多く、次いで「発病の内容」となっている。

図 3.1.4 求められている情報



複数回答有り (米国 : n=1038、イギリス : n=529、ドイツ : n=609、香港 : n=627、シンガポール : n=922)

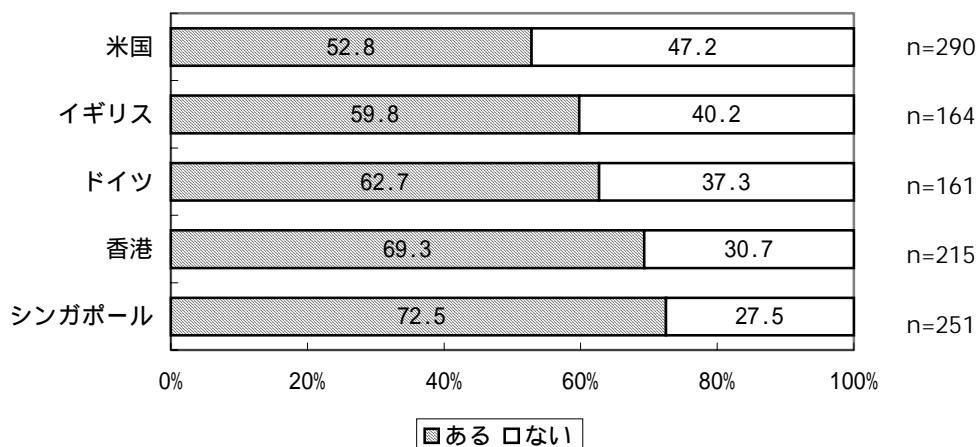
その他 : 産業へのダメージ影響、可能なウイルス源、これ以上いない、など

3.2 コンピュータウイルスによる被害状況

3.2.1 コンピュータウイルス感染経験の有無

1997年1年間の間にコンピュータウイルスに感染したことがある事業所は、各国とも50%を超えている。

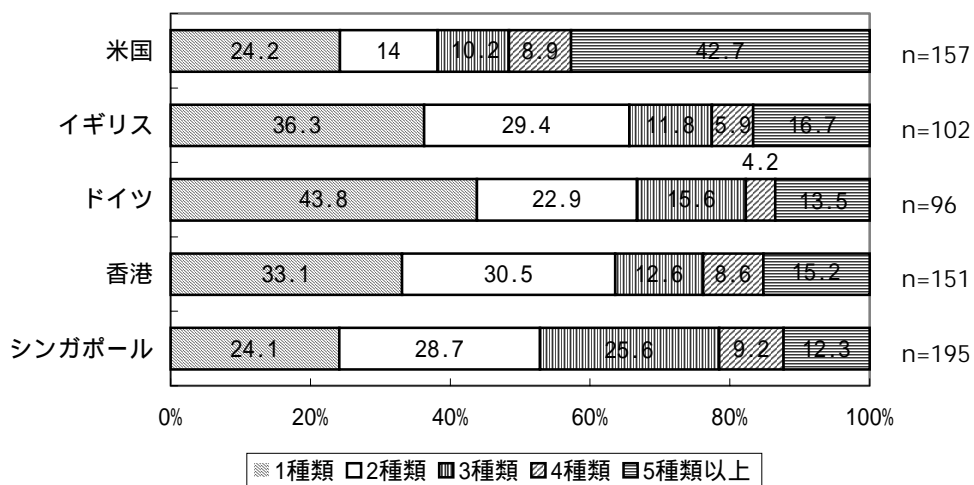
図 3.2.1 コンピュータウイルス感染経験の有無



3.2.2 感染したウイルスの種類数

感染したウイルスの種類数は、米国の約半数の事業所が5種類以上のウイルスに感染しており、複数のウイルスに感染した事業所は、各国とも50%を超えている。

図 3.2.2 感染したウイルスの種類数



(複数回答有り)

3.2.3 感染したウイルスの名称

感染したウイルスの名称としてあげられているものとしては、マクロウイルスの「Word Macro / Concept」が最も多くなっている。

全体としては、圧倒的にマクロウイルスの感染率が高く、Yankee Doodle 等のファイル型ウイルスの感染は少ない。

表 3.2.3 感染したウイルスの名称

名称	米 国		イギリス		ドイ ツ		香 港		シンガポール	
	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比
AntiCMOS	36 件	8.2%	20	8.4	5	2.7	58	22.5	56	12.4
Anti Telefonica	5	1.1	5	2.1	2	1.1	1	0.4	0	0.0
B1	24	5.5	3	1.3	5	2.7	2	0.8	1	0.2
Beijing	8	1.8	2	0.8	1	0.5	17	6.6	27	6.0
Cascade	7	1.6	2	0.8	3	1.6	10	3.9	2	0.4
D3	22	5.0	12	5.1	6	3.3	6	2.3	4	0.9
Form	23	5.2	21	8.9	35	19.1	8	3.1	3	0.7
Ripper	16	3.6	8	3.4	9	4.9	1	0.4	1	0.2
SAMPO	10	2.6	10	4.2	0	0.0	9	3.5	35	7.7
Yankee Doodle	7	1.6	3	1.3	4	2.2	1	0.4	3	0.7
Word Macro / Cap	40	9.1	29	12.2	25	13.7	33	12.8	58	12.8
Word Macro / Colors	15	3.4	9	3.8	2	1.1	0	0.0	5	1.1
Word Macro / Concept	57	13.0	37	15.6	11	6.0	38	14.7	89	19.6
Word Macro / Npad	15	3.4	12	5.1	4	2.2	8	3.1	10	2.2
Word Macro / Wazzu	40	9.1	11	4.6	4	2.2	13	5.0	18	4.0
Excel Macro / Laroux	26	5.9	25	10.5	5	2.7	10	3.9	61	13.5
MBDF	10	2.3	0	0.0	0	0.0	1	0.4	1	0.2
nVIR	11	2.5	3	1.3	1	0.5	3	1.2	2	0.4
その他	58	13.2	31	8.9	41	22.4	22	8.5	38	8.4
名称不明	9	2.1	4	1.7	20	10.9	12	4.7	39	8.6
合 計	439	100.0	237	100.0	183	100.0	258	100.0	453	100.0
不 明	22		2		2		8		9	

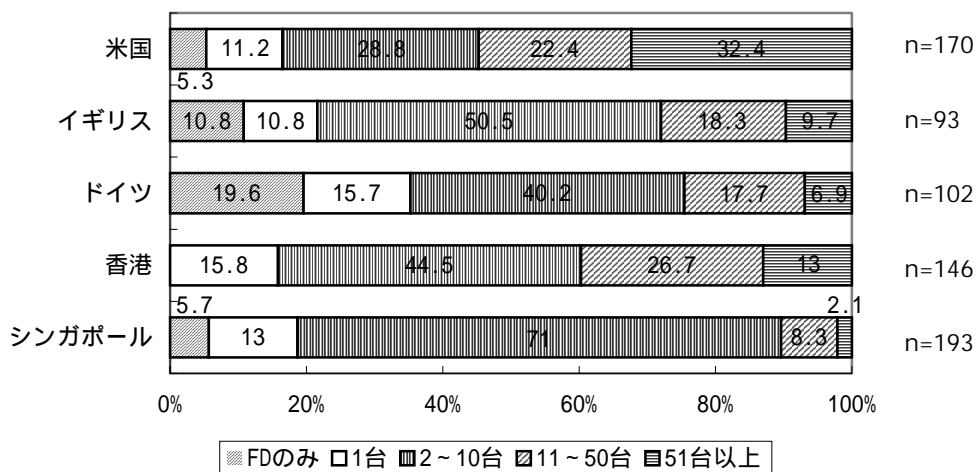
(複数回答有り)

その他 : APPDAP、APPDER、
BANDUNG、Blood、Boot、Boot 437、Bootsector、Brain、BURGLAR 1150、
CARA、Chemnitz、COMEBACK、
DelWin、Die Hard、Die Hard 2、
Form A、Frabkenstein、
Half Moon、Helper、HiAC、
IMPOSTER、
JOHNNY、Jumper、
LAROUX A、Little Girl、LUNCHBOX、
MDMA、MDMA.A、Michaelangelo、Micro Angles、Monkey、Monkey B、
Natas、NIKNAT、NOP、
One half、
Parity、Parity B、Paruty Boot B、SECURE.COM、SETMD、SETMD.A2TW、
Show off、Stealth、Stealth C、Stoned、Stoned.Empire、Sylvia 1200、
Tegma、TPVO.3783.A、
Victorian、
Word Hybrid、Word Macro/Goldfish、Word Macro/Shumann-B、など

3.2.4 感染したコンピュータの延べ台数

感染したコンピュータの延べ台数は、「2～10台」が最も多くなっている。米国では32.4%の企業が「51台以上」の大きな被害にあっている。

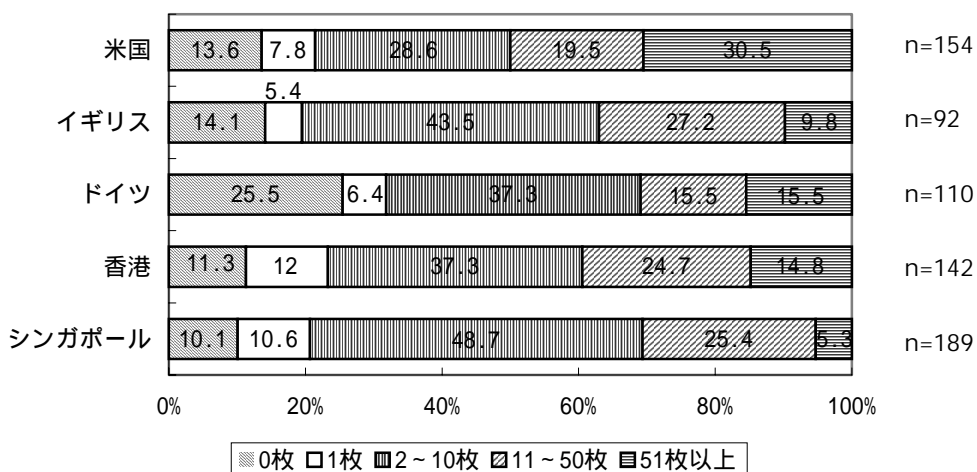
図 3.2.4 感染したコンピュータの延べ台数



3.2.5 感染したFDの累計枚数

感染したFDの累計枚数は、「2～10枚」が最も多くなっている。

図 3.2.5 感染したFDの累計枚数



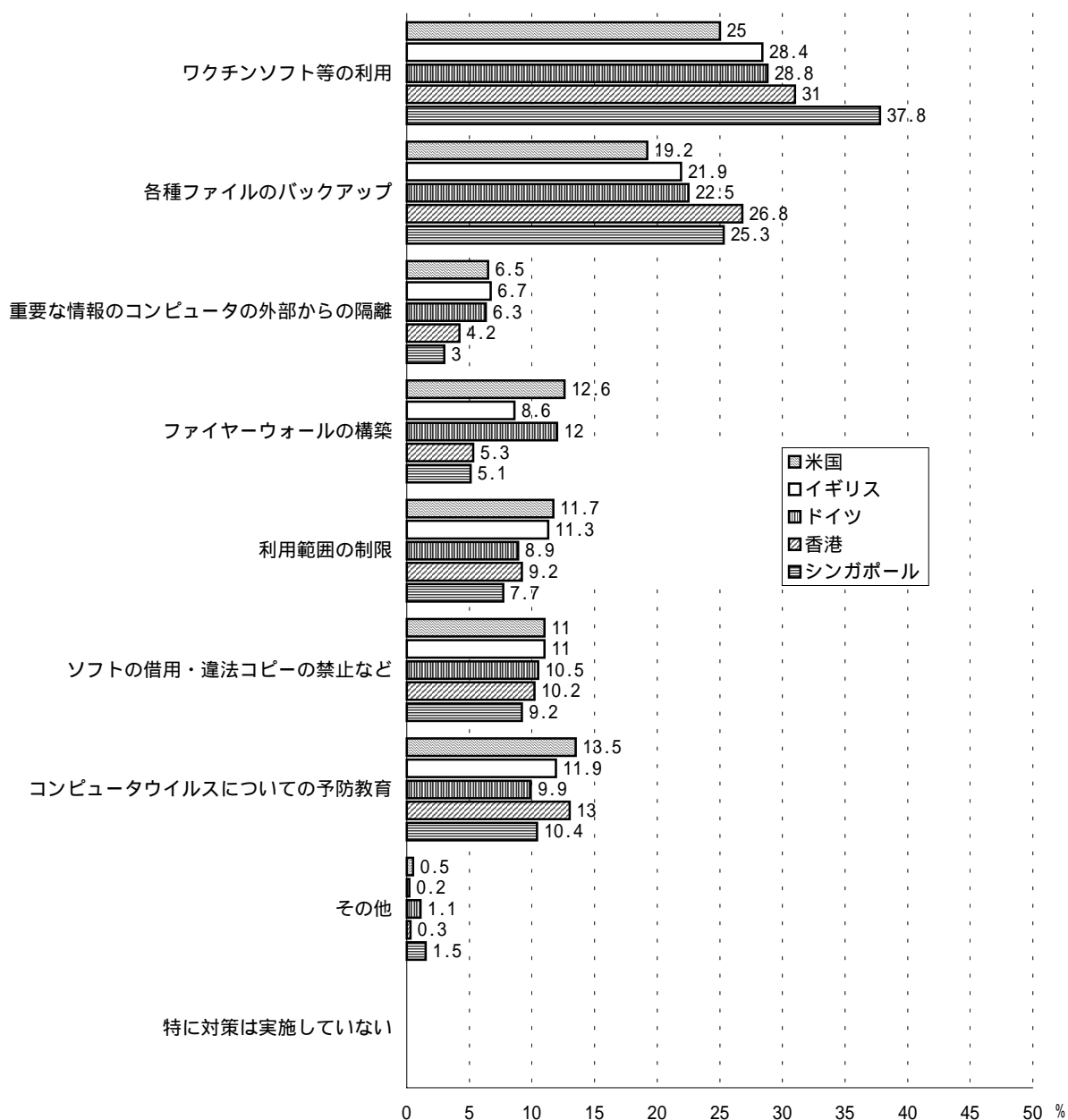
4. コンピュータウイルスの対策の現状と課題

4.1 セキュリティ対策実施状況

4.1.1 現在実施しているセキュリティ対策

コンピュータウイルスのセキュリティ対策については、各国とも100%の事業所が現在実施している。具体的な対策としては、「ワクチン等の利用」が最も多く、次いで「各種ファイルのバックアップ」となっている。

図 4.1.1 現在実施しているセキュリティ対策



複数回答有り (米国：n=987、イギリス：n=538、ドイツ：n=236、香港：n=501、シンガポール：n=565)

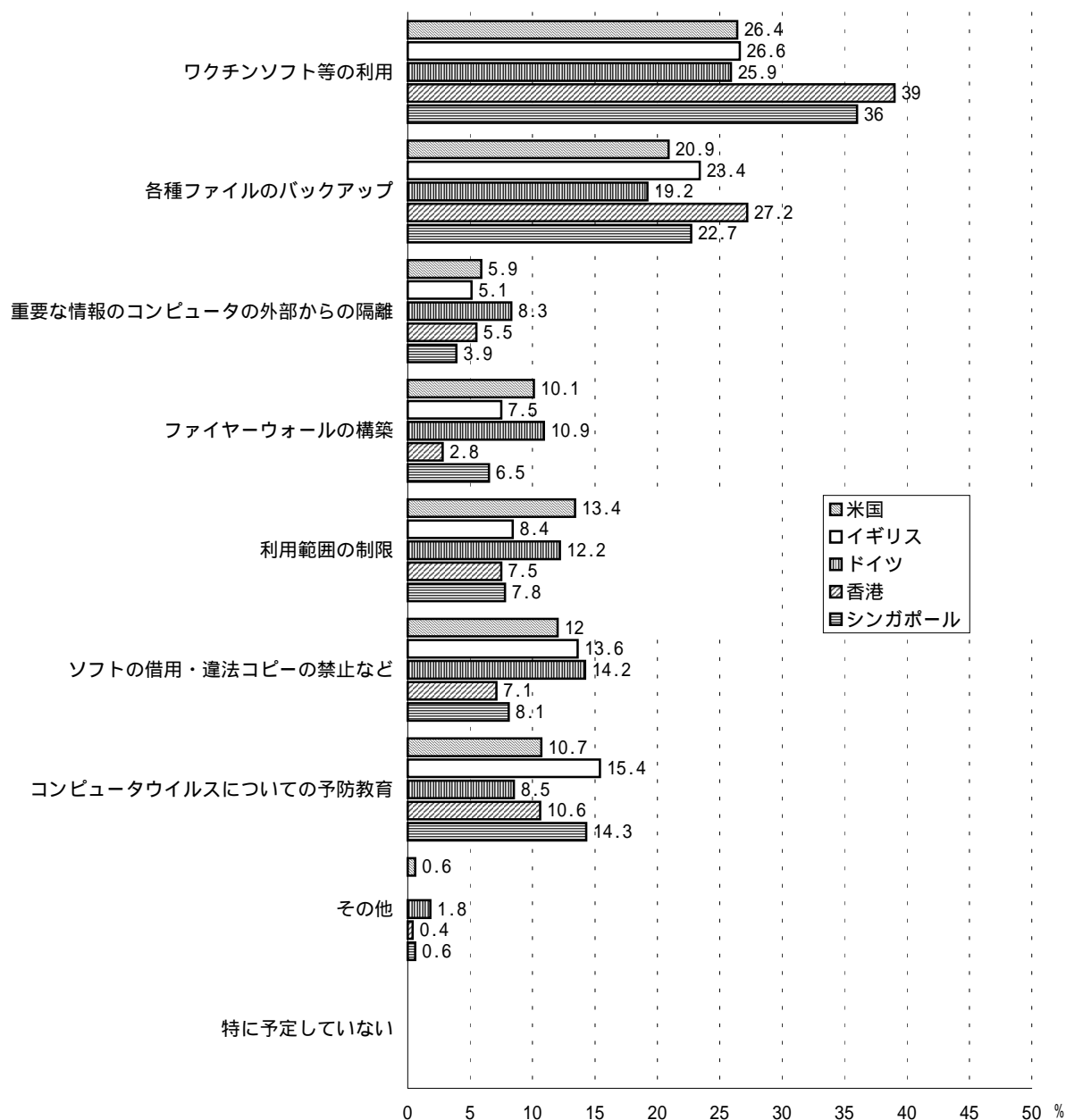
4.1.2 今後実施予定のセキュリティ対策

(1) 引き続き継続するセキュリティ対策

現在実施しているセキュリティ対策を含む、今後実施予定の対策としては、「ワクチン等の利用」が最も多く、次いで「各種ファイルのバックアップ」となっている。

現在実施されている対策に比べて、「コンピュータウイルスについての予防教育」が増加している。

図 4.1.2(1) 引き続き継続するセキュリティ対策

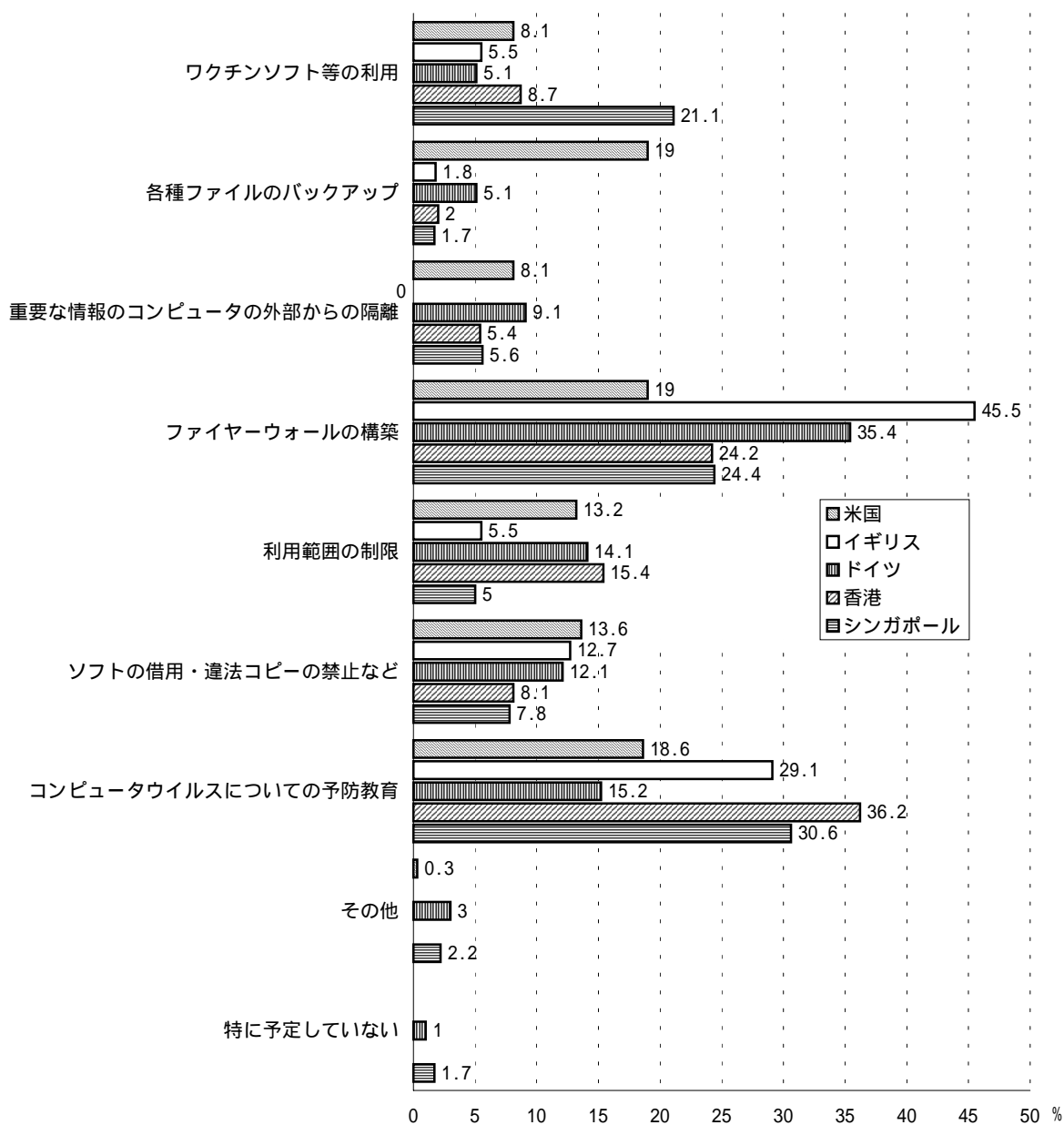


複数回答有り (米国 : n=693、イギリス : n=214、ドイツ : n=336、香港 : n=254、シンガポール : n=308)

(2) 今後の実施予定

今後の実施予定については、「ファイヤーウォールの構築」が最も多く、次いで「コンピュータウイルスについての予防教育」となっている。

図 4.1.2(2) 今後のセキュリティ対策の実施予定

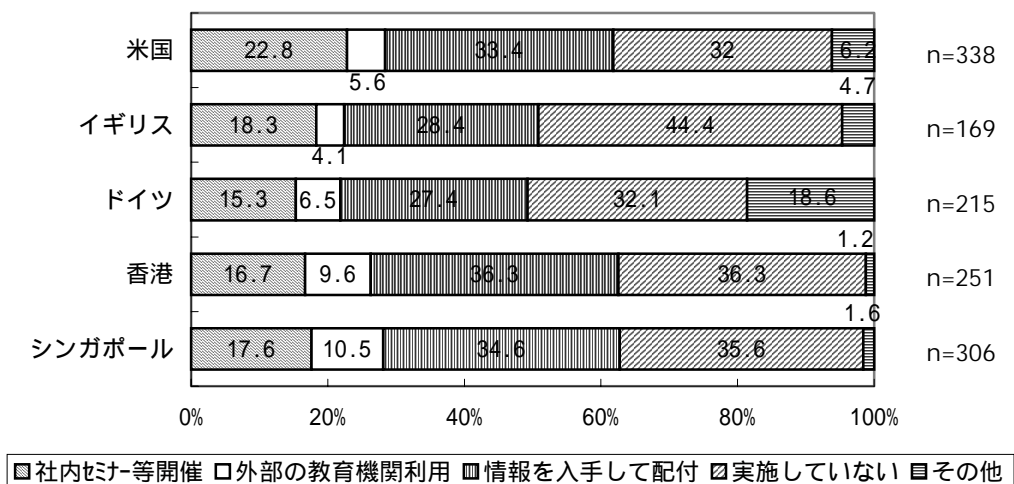


複数回答有り (米国 : n=295、イギリス : n=55、ドイツ : n=99、香港 : n=149、シンガポール : n=180)

4.1.3 ウイルス対策に関するユーザ教育

ウイルス対策に関するユーザ教育は、特に米国では70%の事業所で実施しており、各国とも半数以上の事業所で実施している。その内容としては各国とも「情報を入手して配付」が多い。

図 4.1.3 ユーザ教育の内容



(複数回答有り)

その他：雑誌や本を読む、ユーザに「もっと慎重に」と忠告、感染時にウイルス意識を高める、など

4.2 ワクチンソフト

4.2.1 情報源

ワクチンソフトの情報源としては、「ベンダーからの情報」が多く、次いで「市販の解説書」となっている。

表 4.2.1 ワクチンソフトの情報源

情報原	米 国		イギリス		ドイ ツ		香 港		シンガポール	
	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比
専門誌	27 件	5.6%	38	10.3	33	7.8	31	7.4	78	13.5
カタログ等	43	8.9	35	9.5	71	16.7	78	18.5	84	14.6
口こみ	62	12.8	29	7.9	64	15.1	22	5.2	20	3.5
市販の解説書	113	23.4	88	23.8	108	25.4	93	22.1	114	19.8
講演会、セミナー	34	7.0	23	6.2	15	3.5	38	9.0	49	8.5
ベンダーからの情報	105	21.7	79	21.4	45	10.6	92	21.9	141	24.5
販売店での情報	40	8.3	41	11.1	36	8.5	37	8.8	48	8.3
公的機関	37	7.7	16	4.3	15	3.5	19	4.5	14	2.4
その他	22	4.6	20	5.4	38	8.9	11	2.6	28	4.9
合 計	483	100.0	369	100.0	425	100.0	421	100.0	576	100.0

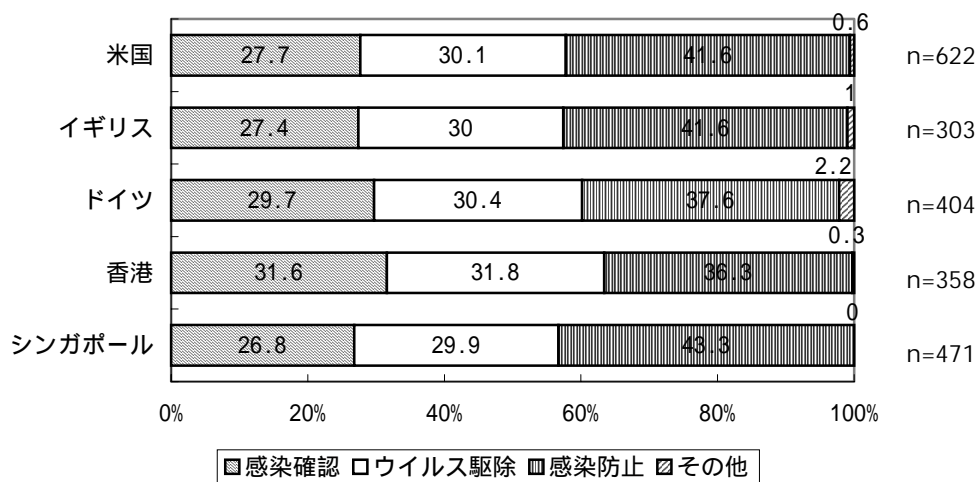
(複数回答有り)

その他：展示会、社内メーリングリスト（世界規模）、インターネット、インターネットソフトウェアライブラリ（ZD Net）、ニュースグループ（Norton）、新聞、LAN 掲示板、SARC、タスクフォース、アーカイブのあるウェブサイトを訪問、など

4.2.2 導入目的

ワクチンソフトの導入目的としては、「感染防止」が最も多い。

表 4.2.2 ワクチンソフトの導入目的



(複数回答有り)

その他：セキュリティ

4.2.3 選択基準

ワクチンソフトの選択基準として重視しているものとしては、「基本機能」が最も多く、次いで「ハード構成・OS」、「メーカーの信頼度」、「アフターサービス」となっている。

表 4.2.3 ワクチンソフトの選択基準

選択基準	米 国		イギリス		ドイ ツ		香 港		シンガポール	
	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比
ハードウェア構成及び OS	173件	13.9%	97	14.7	88	13.1	88	13.1	178	15.8
基本機能	189	15.2	123	18.7	135	20.1	135	20.1	196	17.4
価格	137	11.0	75	11.4	90	13.4	90	13.4	170	15.1
補助機能	50	4.0	8	1.2	25	3.7	25	3.7	24	2.1
処理速度の速さ	99	8.0	35	5.3	34	5.1	34	5.1	73	6.5
使いやすさ	128	10.3	61	9.3	103	15.3	103	15.3	122	10.8
インストールのし易さ	132	10.6	61	9.3	58	8.6	58	8.6	120	10.7
メーカーの信頼度	173	13.9	96	14.6	65	9.7	65	9.7	111	9.9
アフターサービスの良さ	151	12.2	94	14.3	72	10.7	72	10.7	117	10.4
その他	10	0.8	9	1.4	3	0.4	3	0.4	14	1.2
合 計	1242	100.0	659	100.0	673	100.0	673	100.0	1125	100.0

(複数回答有り)

その他：多言語システム環境の適用度、監視の継続性、アップデートの頻度（少なくとも年 4 回）、アップデートのし易さ（インターネット経由）、世界的な製品、質の良さ、ウイルスのを見つける範囲、信頼性、報告されたウイルス検査と駆除の正確さ、新しいウイルスへの対応、など

5. コンピュータウイルス被害分析調査報告

5.1 感染したコンピュータの種類と台数

ウイルスに感染したコンピュータの台数をみると、1～10台が圧倒的に多い。

図 5.1(1) 感染したコンピュータの種類と台数 汎用機

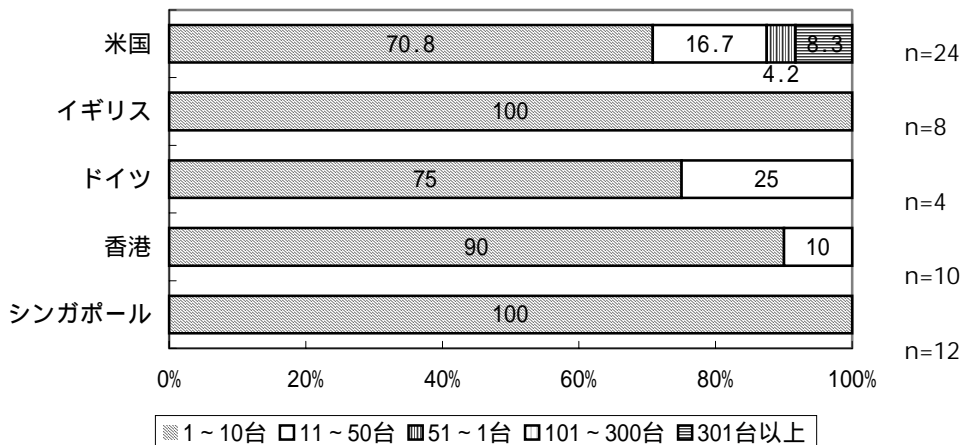


図 5.1(2) 感染したコンピュータの種類と台数 ワークステーション

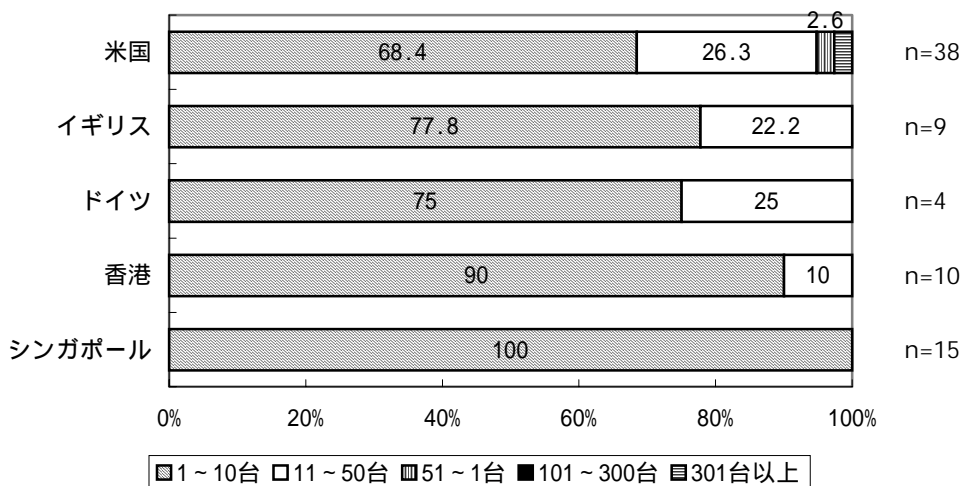


図 5.1(3) 感染したコンピュータの種類と台数 DOS、Windows

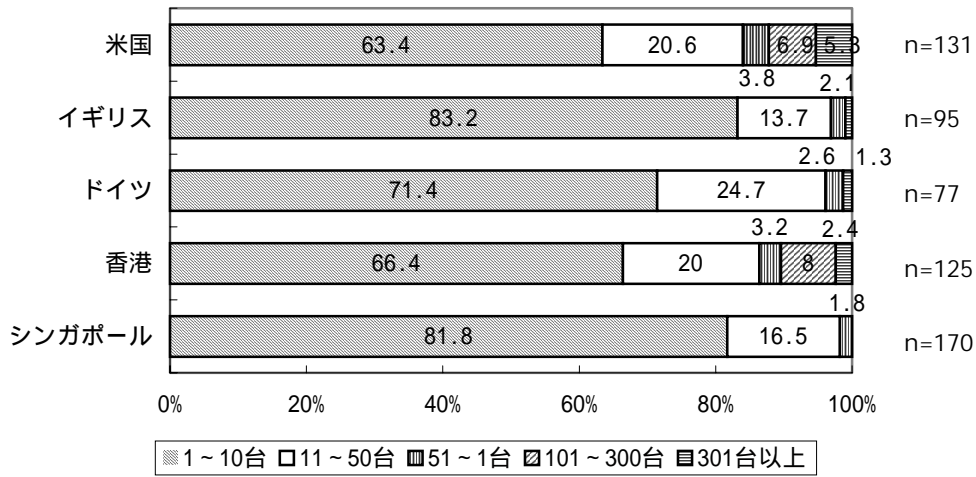
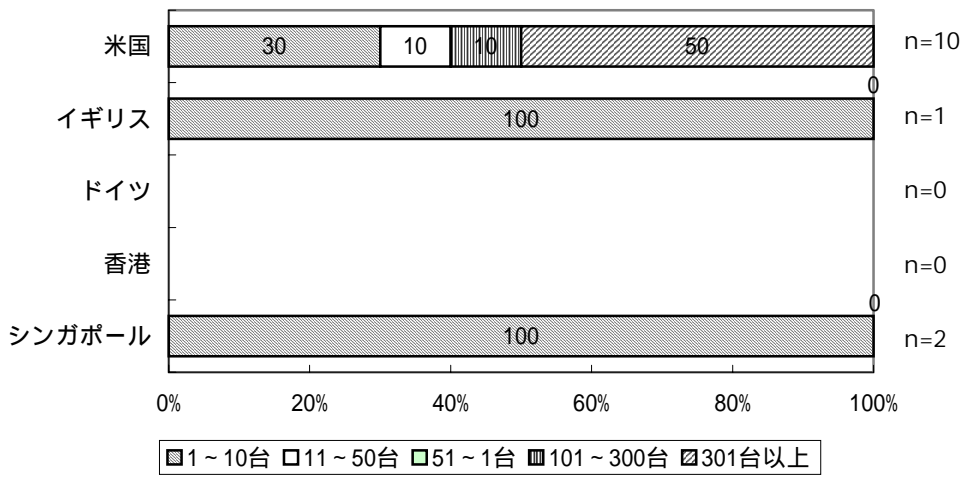


図 5.1(4) 感染したコンピュータの種類と台数 Macintosh



5.2 発見の経緯

ウイルス発見の経緯としては、「ワクチンソフトによる定期検査」が最も多く、次いで「ファイル内容読み取り不可」、「ディスプレイメッセージ」となっている。

表 5.2 ウイルス発見の経緯

内容	米 国		イギリス		ドイツ		香 港		シンガポール	
	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比
起動できなくなった	35 件	12.5%	15	9.5	6	4.2	45	19.7	19	6.1
処理速度の低下	19	6.8	9	5.7	8	5.6	12	5.3	26	8.4
ファイル内容読み取り不可	40	14.3	30	19.0	16	11.2	34	14.9	78	25.1
FD 内容破壊	17	6.1	9	5.7	3	2.1	10	4.4	20	6.4
HDD 内容破壊	9	3.2	5	3.2	2	1.4	13	5.7	22	7.1
システムダウン	18	6.4	9	5.7	13	9.1	10	4.4	25	8.0
意味不明のファイル	3	1.1	1	0.6	6	4.2	5	2.2	3	1.0
ディスプレイメッセージ	36	12.9	17	10.8	16	11.2	12	5.3	30	9.6
ファイルのサイズ等が変化	14	5.0	8	5.1	3	2.1	11	4.8	18	5.8
音楽の演奏	1	0.4	0	0.0	0	0.0	0	0.0	0	0.0
ソフトウェアによる定期検査	71	25.4	44	27.8	58	40.6	67	29.0	56	18.0
発病無し	17	6.1	11	7.0	12	8.4	9	3.9	14	4.5
合 計	280	100.0	158	100.0	143	100.0	228	100.0	311	100.0

(複数回答有り)

5.3 発見に使用したワクチンソフト

感染したウイルスを発見するのに使用したワクチンソフトとして最も多くあげられているのは、イギリスを除いて「VirusScan」で、各国とも20%以上の事業所が使用している。イギリスでは「Anti-Virus Toolkit」が43.9%と高い比率になっている。

表 5.3 発見に使用したワクチンソフト

ワクチン名	米 国		イギリス		ドイ ツ		香 港		シンガポール	
	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比
Anti-Virus Toolkit	24 件	10.0%	61	43.9	20	16.7	11	5.3	25	9.8
F-PROT	19	7.9	13	9.4	13	10.8	54	26.1	23	9.0
IBM Antivirus	17	7.1	0	0.0	6	5.0	7	3.4	5	2.0
InocuLAN	11	4.6	6	4.3	4	3.3	6	2.9	10	3.9
Inter Scan	1	0.4	0	0.0	0	0.0	4	1.9	0	0.0
Norton Antivirus	61	25.5	10	7.2	10	8.3	53	25.6	69	27.1
VirusScan	81	33.9	36	25.9	35	29.2	58	28.0	103	40.4
XLSCAN.XLA	1	0.4	1	0.7	1	0.8	0	0.0	22	0.8
VirusBuster	0	0.0	2	1.4	1	0.8	0	0.0	5	2.0
ScanVakzin	1	0.4	0	0.0	0	0.0	0	0.0	0	0.0
Disinfectant	3	1.3	0	0.0	5	4.2	0	0.0	0	0.0
SAM	4	1.7	1	0.7	0	0.0	0	0.0	1	0.4
OS 添付ソフト	1	0.4	2	1.4	1	0.8	0	0.0	2	0.8
その他	15	6.3	7	5.0	24	20.0	0	0.0	10	3.9
合 計	239	100.0	139	100.0	120	100.0	207	100.0	255	100.0

(複数回答有り)

その他：CAP、Central Point Anti Virus、Emergency Anti Virus、
Intel Virus Protect、INVIRCINBLE、Landesk Virus Protect - VSCAND、
Macro Virus Buster Eval、Managewise Vprotect、MSAV、Nash Pack、
Novell Managewise、PC-cillin(97)、SCAN、SCANPROTECT、
SAR(Hong Kong) developed software、SOPHOS(SWEEP & INTERCHECK)、
SSCAN、Stest、Thunder Byte Anti-Virus、Turbo Anti-Virus、Virex for Macintosh、
Virusafe 95、VNT AntiVirus、VTHUNT、W Protect、など

5.4 感染経路

ウイルスの感染経路としては、「取引先からのFD」、「他部署からのFD」が、各国とも高い数値となっており、FDを経由した感染が多いことがわかる。

表 5.4 感染経路

経路	米 国		イギリス		ドイ ツ		香 港		シンガポール	
	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比
シェアウェアやサンプルソフト	20 件	8.6%	5	3.4	4	3.5	16	8.3	19	6.8
ネットワークによる外部からの侵入	27	11.6	11	7.6	1	0.9	6	3.1	18	6.4
知人から借用、コピーしたソフト	22	9.5	18	12.4	4	3.5	25	13.0	40	14.2
市販ソフト、雑誌	3	1.3	4	2.8	2	1.8	7	3.6	1	0.4
他部署からのFD	44	19.0	28	19.3	28	24.6	48	25.0	82	29.2
取引先からのFD	56	24.1	46	31.7	53	46.5	54	28.1	75	26.7
メーカーのサービス時	1	0.4	4	2.8	0	0.0	14	7.3	3	1.1
その他	42	18.1	21	14.5	17	14.9	12	6.3	17	6.0
不明	17	7.3	8	5.5	5	4.4	10	5.2	18	6.4
合 計	232	100.0	145	100.0	114	100.0	192	100.0	281	100.0

その他：海外オフィスからの添付ファイル、文書共有、インターネットからのダウンロード、E-mail（添付ファイル）、ファイル交換、他国（親会社）からのファイル転送、コンサルタントからのFD、プロバイダーからのFD、ベンダーからのFD、など

5.5 復旧方法

ウイルスに感染した際の復旧方法としては、「自分で対応した」が高い数値となっており、「各種ツールの使用」、「社内の技術者に相談」が続いている。

表 5.5 復旧方法

復旧方法	米 国		イギリス		ドイ ツ		香 港		シンガポール	
	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比
自分で対応	97 件	29.4%	68	43.6	65	41.1	79	31.6	81	29.9
社内の技術者に相談	82	24.8	21	13.5	24	15.2	26	10.4	30	11.1
外部の機関に相談	5	1.5	6	3.8	5	3.2	19	7.6	16	5.9
各種ツール使用	76	23.0	36	23.1	42	26.6	57	22.8	71	26.2
ソフトウェアの再購入	11	3.3	0	0.0	2	1.3	2	0.8	1	0.4
データの再入力	18	5.5	4	2.6	3	1.9	19	7.6	25	9.2
バックアップ 再ロード	12	3.6	9	5.8	6	3.8	26	10.4	28	10.3
ワケソフト独自開発	13	3.9	1	0.6	5	3.2	11	4.4	4	1.5
その他	16	4.8	11	7.1	6	3.8	11	4.4	15	5.5
合 計	330	100.0	156	100.0	158	100.0	250	100.0	271	100.0

(複数回答有り)

その他：ハードディスクのフォーマット

5.6 被害規模

5.6.1 復旧に要した期間

復旧に要した期間としては、「1日未満」が最も多く、次いで「1～3日」、「1週間程」と、各国とも比較的短い日数で復旧できている。シンガポールでは「復旧不可能」が1件ある。

表 5.6.1 期間

期間	米 国		イギリス		ドイ ツ		香 港		シンガポール	
	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比
1日未満	151件	78.2%	96	83.5	77	82.8	100	71.4	155	79.5
1～3日程度	31	16.1	11	9.6	7	7.5	23	16.4	27	13.8
1週間程度	7	3.6	5	4.3	7	7.5	4	2.9	7	3.6
1～2週間程度	3	1.6	3	2.6	1	1.1	6	4.3	3	1.5
1ヵ月程度	1	0.5	0	0.0	1	1.1	4	2.9	1	0.5
3ヵ月程度	0	0.0	0	0.0	0	0.0	2	1.4	0	0.0
6ヵ月程度	0	0.0	0	0.0	0	0.0	1	0.7	0	0.0
6ヵ月以上	0	0.0	0	0.0	0	0.0	0	0.0	1	0.5
復旧不可能	0	0.0	0	0.0	0	0.0	0	0.0	1	0.5
合 計	193	100.0	115	100.0	93	100.0	140	100.0	195	100.0

5.6.2 復旧に要した人日

復旧に要した人日についても短いものが多く、各国とも「1人日未満」、「1～5人日」が大半となっている。

表 5.6.2 復旧に要した人日

期間 \ 国名	米 国		イギリス		ドイ ツ		香 港		シンガポール	
	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比	回答数	構成比
1人日未満	145件	78.8%	84	73.7	30	68.2	105	77.8	138	81.2
1～5人日	35	19.0	27	23.7	12	27.3	22	16.3	27	15.9
6～10人日	1	0.5	3	2.6	2	4.5	4	3.0	3	1.8
11～20人日	1	0.5	0	0.0	0	0.0	2	1.5	1	0.6
21～30人日	1	0.5	0	0.0	0	0.0	2	1.5	1	0.6
31～50人日	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
51～100人日	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0
101人日以上	1	0.5	0	0.0	0	0.0	0	0.0	0	0.0
合 計	184	100.0	114	100.0	44	100.0	135	100.0	170	100.0

6.まとめ

1章の調査概要で示した様に、本調査は平成9年度1年間にわたって米国、欧州(イギリス、ドイツ)、香港、シンガポールの主要5カ国について被害実態の調査を行ったものである。アンケートを送付した件数は約2万5千件で、合計1,120件のコンピュータユーザから回答を入手している。また、コンピュータウイルスの被害状況や防止技術に関しては、海外諸国の実情から日本の今後の対策について学ぶべき点も多い。本章では調査全体として特徴的な事項を記載する。

(1) ウイルス感染の状況

過去1年間にウイルスに感染した経験のある事業所は、各国とも50%を超えており、地域による差は感じられない。これは、インターネット/イントラネットの普及により、コンピュータの使用形態が世界中で均一化してきているためと考えられる。

また、ウイルス感染を受けた機種は、PCからワークステーション、汎用機に広がっており、Macintoshの被害はほとんど無かった。

(2) 感染ウイルスの種類

感染ウイルスの種類としては、圧倒的にマクロウイルスが多いが、古くから被害報告のあるAntiCMOS、Formの感染も多い。マクロウイルスの被害の増加は、E-mailの利用の普及によって文書ファイルのやり取りによる感染が増えているためと考えられるが、Bootセクタ型(システム感染型)ウイルス被害が無くならないのは、依然としてFDによるデータの受け渡しが一般的なためである。

(3) ウイルス感染対応策

感染源で多いのは、「他部署からのFD」や「取引先からのFD」が主体で、「借用、コピーしたソフト」がこれに続いている。

また、感染したことを検出する方法としては、ワクチンソフトの使用が最も多く、ファイルの読み取り不可、ディスプレイメッセージの発生時点が続いている。そして、感染後の回復手段としてもワクチンソフトが多く使われており、バックアップからの再ロードや、データの再入力率を大きく上回っている。

今後のセキュリティ対策として、各国とも「ファイアーウォールの構築」が上位となっているが、これは、更なるネットワーク化の普及とともに、各国ともにネットワーク経由でのウイルス感染が増大すると予想しているためと考えられる。

以上、1年間の海外調査の結果を記載したが、同様の国内調査と比較してみると、日本はウイルス対策に関するユーザー教育の実施率が低く、またセキュリティ対策として各種ファイルのバックアップが上位を占めており、ウイルス対策に対する対応が遅れている。

今後、日本でも欧米諸国を見習い、ウイルス対策教育の徹底、予防としてのワクチンソフトの導入が重要な課題といえる。

7. 資料編

7.1	調査表	40
7.2	調査結果集計一覧	46
7.3	送付先一覧	78
7.3.1	米国	79
7.3.2	イギリス	90
7.3.3	ドイツ	101
7.3.4	香港	112
7.3.5	シンガポール	123
7.4	回答先一覧	134
7.4.1	米国	135
7.4.2	イギリス	144
7.4.3	ドイツ	152
7.4.4	香港	158
7.4.5	シンガポール	167
7.5	コンピュータウイルス個別表	177
	米国、イギリス、ドイツ、香港、シンガポール	
7.6	調査表原表	別冊
	米国、イギリス、ドイツ、香港、シンガポール(3冊)	

7.1 調査表

調査依頼書	41
調査説明書	42
調査表	43
コンピュータウイルス個別表	45

7.2 調査結果集計一覧

回答事業所属性

1. 主たる業種	47	
2. 就業者数	48	
3. 利用しているコンピュータの種類別台数	49	
4. 社内情報ネットワークの構築状況	50	
4 - 1. 社内情報ネットワークの用途	51	
4 - 2. インターネット接続の有無	52	
4 - 3. ホームページの有無	53	
5. 商用パソコン通信サービスの利用状況	54	
5 - 1. 利用している商用パソコン通信サービス	55	55
6. 商用 VAN ネット等との接続状況	56	

コンピュータウイルスによる被害状況

7. コンピュータウイルスの認知度	57	
8. コンピュータウイルスへの脅威	58	
9. コンピュータウイルス感染の有無	59	
10. 感染したウイルスの種類	60	
11. 感染したウイルスの名称	61	
12. 感染したコンピュータの延べ台数	62	
13. 感染したフロッピーディスクの枚数	63	
14. 現在および今後のセキュリティ対策	64	
15. ウイルス対策に関するユーザ教育	65	
16. ワクチンソフトの情報源	66	
17. ワクチンソフトの導入目的	67	
18. ワクチンソフトの選択基準	68	
19. 今後の被害予測	69	
20. 求める情報	70	

コンピュータウイルス個別表

1. ウイルス名称と発見日	71	
2. 発見の経緯	72	
3. 使用したワクチンソフト	73	
4. 感染したコンピュータの種類と台数	74	
5. 想定される感染経路	75	
6. 復旧方法	76	
7. 被害規模（期間・投入人日）	77	

回答事業所属性

1. 主たる業種

業種	米 国	イ ン	ド ン	香 港	シ ン ガ ポ ー ル
農 林 水 産 業	12	1	4	2	3
鉱 業	2	0	2	0	2
建 設 業	6	2	9	17	13
製 造 業	26	36	24	42	96
出 版 印 刷 業	3	2	13	3	2
卸 売 小 売 業	16	12	23	11	18
金 融 保 険 業	40	13	12	24	17
不 動 産 業	11	0	1	5	1
運 輸 業	9	2	4	14	12
通 信 業	14	1	2	9	1
電 力 業	8	4	9	2	5
ガ ス 業	5	0	1	0	1
新 聞 放 送 業	3	0	7	1	0
情 報 サ ー ビ ス 業	9	5	5	7	10
物 品 賃 貸 業	2	2	1	0	2
遊 興 娯 楽 業	2	0	0	0	0
医 療 業	8	2	3	3	1
教 育 研 究 機 関	31	8	0	15	3
政 治 、 経 済 、 文 化 団 体	1	0	1	0	0
そ の 他 サ ー ビ ス 業	17	28	11	8	16
政 府 ま た は 政 府 関 係 機 関	8	4	4	2	0
地 方 公 共 団 体	1	1	5	0	0
そ の 他	79	40	22	50	69
合 計	313	163	163	215	272
不 明	5	2	0	1	2

2. 就業者数

従業員数	米 国	イ ン	ド イツ	香 港	シンガポール
50名未満	120	44	41	58	84
50～99名	27	16	23	38	48
100～299名	31	28	38	33	58
300～499名	14	20	14	9	14
500～999名	18	27	16	15	16
1,000名以上	92	29	31	47	50
合 計	302	164	163	215	270
不 明	16	1	0	1	4

3. 利用しているコンピュータの種類別台数

(1) 汎用機

利用台数	1～10台	11～50台	51～100台	101～300台	301台～
米国	52	37	10	7	12
イギリス	35	10	3	3	1
ドイツ	18	10	6	3	1
香港	33	11	2	0	0
シンガポール	48	16	1	1	1

(2) ワークステーション

利用台数	1～10台	11～50台	51～100台	101～300台	301台～
米国	29	44	10	15	23
イギリス	28	12	8	9	4
ドイツ	39	29	6	8	10
香港	24	31	17	4	8
シンガポール	42	47	11	2	2

(3) DOS、Windows 系

利用台数	1～10台	11～50台	51～100台	101～300台	301台～
米国	57	48	26	32	59
イギリス	24	29	23	24	46
ドイツ	23	49	26	27	32
香港	28	63	17	14	51
シンガポール	42	79	27	21	35

(4) Macintosh 系

利用台数	1～10台	11～50台	51～100台	101～300台	301台～
米国	20	12	6	7	13
イギリス	12	3	2	0	2
ドイツ	22	6	0	2	0
香港	6	3	2	2	1
シンガポール	5	2	0	1	1

4. 社内情報ネットワークの構築状況

ネットワーク	米 国	イ ン	ド ン	香 港	シンガポール
事業所内 ネットワーク	93	66	77	128	133
事業所間 ネットワーク	141	88	73	59	80
ネットワーク 構築	46	10	13	25	49
合 計	280	164	163	212	262

4 - 1 . 社内情報ネットワークの用途

用途	米 国	イ ン	ド ン	香 港	シンガポール
販売管理系	106	98	106	83	129
生産管理系	99	46	61	55	53
技術系 (制御、管制等)	75	32	49	38	40
経理系	178	117	116	109	135
開発系 (技術計算、CAD等)	106	53	80	49	55
信用情報	55	20	43	22	25
データベース検索	180	95	110	129	130
TSS	25	4	30	9	8
金融総合オンライン	78	39	49	30	33
警備システム	83	27	53	23	20
電子メール	180	105	116	107	177
その他	26	19	22	13	17
合 計	1200	691	835	654	822

4 - 2 . インターネット接続の有無

インターネット接続	接続している	接続していない
米国	184	63
イタ	93	54
ドツ	104	59
香港	131	83
シンガポール	140	110

4 - 3 . ホームページの有無

ホームページ	ある	ない	準備中
米国	160	32	8
イギリス	86	26	19
ドイツ	78	19	13
香港	74	39	31
シンガポール	86	47	35

5. 商用パソコン通信サービスの利用状況

商用サービス	利用している	利用していない
米国	124	160
イタ	51	108
ドイツ	89	70
香港	60	151
シンガポール	38	163

5 - 1 . 利用している商用パソコン通信サービス

利用している商用パソコン通信サービスは、

AOL

BT Frame-Relay

COMPUSERVE

DEC-NET

FTAM

Internet Provider

Local Internet Provider

TELECOM

T-Online

X-Link

V-Online

などがある。

6 . 商用 VAN ネット等との接続状況

商用ネット	商用VANネットに接続	企業間ネットに接続	今後接続予定	接続予定なし
米国	36	66	25	154
イタ	15	18	16	106
ドイツ	6	38	19	87
香港	15	37	27	159
シンガポール	21	32	20	125

コンピュータウイルスによる被害状況

7. コンピュータウイルスの認知度

認知度	詳しく知っている	概要は知っている	存在は知っている	知らない
米国	93	87	131	4
イギリス	19	107	27	1
ドイツ	22	92	45	3
香港	30	136	82	4
シンガポール	25	121	107	8

8 . コンピュータウイルスへの脅威

脅威	感じる	感じない
米国	134	168
イタ	93	70
ドイツ	117	43
香港	170	72
シンガポール	181	70

9 . コンピュータウイルス感染の有無

感染経験	ある	ない
米国	153	137
イギリス	98	66
ドイツ	101	60
香港	149	66
シンガポール	182	69

10 . 感染したウイルスの種類

感染種類	1種類	2種類	3種類	4種類	5種類以上
米国	38	22	16	14	67
イタ	37	30	12	6	17
ドイツ	42	22	15	4	13
香港	50	46	19	13	23
シンガポール	47	56	50	18	24

1 1 . 感染したウイルスの名称

感染名称	米 国	イタ	日 本	香 港	シンガポール
AntiCMOS	36	20	5	58	56
Anti Telefonica	5	5	2	1	0
B1	24	3	5	2	1
Beijing	8	2	1	17	27
Cascade	7	2	3	10	2
D3	22	12	6	6	4
Form	23	21	35	8	3
Ripper	16	8	9	1	1
SAMPO	10	10	0	9	35
Yankee Doodle	7	3	4	1	3
Word Macro / Cap	40	29	25	33	58
Word Macro / Colors	15	9	2	0	5
Word Macro / Concept	57	37	11	38	89
Word Macro / Npad	15	12	4	8	10
Word Macro / Wazzu	40	11	4	13	18
Excel Macro / Laroux	26	25	5	10	61
MBDF	10	0	0	1	1
nVIR	11	3	1	3	2
その他	58	31	41	22	38
名称不明	9	4	20	12	39
合 計	439	237	183	258	453
不 明	22	2	2	8	9

12. 感染したコンピュータの延べ台数

感染延べ台数	FDのみ	1台	2～10台	11～50台	51台以上
米国	9	19	49	38	55
イタ	10	10	47	17	9
ドイツ	20	16	41	18	7
香港	0	23	65	39	19
シンガポール	11	25	137	16	4

13. 感染したフロッピーディスクの枚数

感染FD数	0枚	1枚	2～10枚	11～50枚	51枚以上
米国	21	12	44	30	47
イタ	13	5	40	25	9
ドイツ	28	7	41	17	17
香港	16	17	53	35	21
シンガポール	19	20	92	48	10

14. 現在および今後のセキュリティ対策

現在対策	米国	イギリス	ドイツ	香港	シンガポール
ワクチンソフト等の利用	259	153	67	78	215
各種ファイルのバックアップ	198	118	51	141	139
重要な情報のコンピュータの外部からの隔離	67	36	13	28	24
ファイヤーウォールの構築	103	46	29	19	35
利用範囲の制限	127	61	24	43	42
ソフトの借用・違法コピーの禁止など	114	59	26	48	48
コンピュータウイルスについての予防教育	111	64	23	55	57
その他	8	1	3	1	5
特に対策は実施していない	3	0	0	0	0

継続対策	米国	イギリス	ドイツ	香港	シンガポール
ワクチンソフト等の利用	183	57	100	99	111
各種ファイルのバックアップ	145	50	74	69	70
重要な情報のコンピュータの外部からの隔離	41	11	28	14	12
ファイヤーウォールの構築	70	16	42	7	20
利用範囲の制限	93	18	47	19	24
ソフトの借用・違法コピーの禁止など	83	29	55	18	25
コンピュータウイルスについての予防教育	74	33	33	27	44
その他	4	0	7	1	2
特に予定していない	0	0	0	0	0

将来対策	米国	イギリス	ドイツ	香港	シンガポール
ワクチンソフト等の利用	24	3	5	13	38
各種ファイルのバックアップ	56	1	5	3	3
重要な情報のコンピュータの外部からの隔離	24	0	9	8	10
ファイヤーウォールの構築	56	25	35	36	44
利用範囲の制限	39	3	14	23	9
ソフトの借用・違法コピーの禁止など	40	7	12	12	14
コンピュータウイルスについての予防教育	55	16	15	54	55
その他	1	0	3	0	4
特に予定していない	0	0	1	0	3

15 . ウイルス対策に関するユーザ教育

ユーザ教育	社内セミナー等 開催	外部の教育機関 利用	情報入手して 配付	実施していない	その他
米国	77	19	113	108	21
イタ	31	7	48	75	8
ドツ	33	14	59	69	40
香港	42	24	91	91	3
シンガポール	54	32	106	109	5

16. ワクチンソフトの情報源

ワクチン情報源	米 国	イギリス	日 本	香 港	シンガポール
専門誌	27	38	33	31	78
カタログ等	43	35	71	78	84
口こみ	62	29	64	22	20
市販の解説書	113	88	108	93	114
講演会セミナー	34	23	15	38	49
ベンダーからの情報	105	79	45	92	141
販売店での情報	40	41	36	37	48
公的機関	37	16	15	19	14
その他	22	20	38	11	28
合 計	483	369	425	421	576

17. ワクチンソフトの導入目的

ワクチン導入目的	感染確認	ウイルス駆除	感染防止	その他
米国	172	187	259	4
イギリス	83	91	126	3
ドイツ	120	123	152	9
香港	113	114	130	1
シンガポール	126	141	204	0

18. ワクチンソフトの選択基準

ワクチン選択基準	米 国	イタリ	ドイツ	香 港	シンガポール
ハードウェア構成及びOS	173	97	88	88	178
基本機能	189	123	135	135	196
価格	137	75	90	90	170
補助機能	50	8	25	25	24
処理速度の速さ	99	35	34	34	73
使いやすさ	128	61	103	103	122
インストールのし易さ	132	61	58	58	120
メーカーの信頼度	173	96	65	65	111
アフターサービスの良さ	151	94	72	72	117
その他	10	9	3	3	14
合 計	1242	659	673	673	1125

19. 今後の被害予測

被害予想	減少	変わらない	やや増加	急激に増加
米国	68	99	94	26
イタ	29	69	48	10
ドイツ	25	77	38	15
香港	59	72	68	6
シンガポール	54	78	96	20

20. 求める情報

求められている情報	米国	イタ	ドツ	香港	シンガポール
しみ種類等の技術的内容	128	63	54	84	139
感染した時の復旧方法	195	110	130	147	189
感染しないための方法や対策	157	74	72	83	157
発病内容	176	97	112	107	127
国内のウイルス被害の状況	177	82	110	82	129
ワクチン情報	170	81	119	121	142
その他	5	4	3	0	4
特になし	30	18	9	3	35

コンピュータウイルス個別表

1 . ウイルス名称と発見日

7.5 節を参照してください。

2. 発見の経緯

発見経緯	米 国	イ 州	日 本	香 港	シンガポール
起動できなくなった	35	15	6	45	19
処理速度の低下	19	9	8	12	26
ファイル内容読み取り不可	40	30	16	34	78
FD内容破壊	17	9	3	10	20
HDD内容破壊	9	5	2	13	22
システムダウン	18	9	13	10	25
意味不明のファイル	3	1	6	5	3
ディスプレイメッセージ	36	17	16	12	30
ファイルのサイズ等が変化	14	8	3	11	18
音楽の演奏	1	0	0	0	0
ワケソフによる定期検査	71	44	58	67	56
その他	17	11	12	9	14
合 計	280	158	143	228	311

3 . 使用したワクチンソフト

使用ワクチン	米 国	イ ン ン	日 本	香 港	シンガポール
Anti-Virus Toolkit	24	61	20	11	25
F-PROT	19	13	13	54	23
IBM Antivirus	17	0	6	7	5
InocuLAN	11	6	4	6	10
Inter Scan	1	0	0	4	0
Norton Antivirus	61	10	10	53	69
VirusScan	81	36	35	58	103
XLSCAN.XLA	1	1	1	0	22
ウイルスバスター	0	2	1	0	5
スキャンワクチン	1	0	0	0	0
Disinfectant	3	0	5	0	0
SAM	4	1	0	0	1
OS添付ソフト	1	2	1	0	2
その他	15	7	24	0	10
合 計	239	139	120	207	255

4. 感染したコンピュータの種類と台数 (%)

(1) 汎用機

利用台数	1～10台	11～50台	51～100台	101～300台	301台～
米国	17	4	1	0	2
イタ	8	0	0	0	0
ドイツ	3	1	0	0	0
香港	9	1	0	0	0
シンガポール	12	0	0	0	0

(2) ワークステーション

利用台数	1～10台	11～50台	51～100台	101～300台	301台～
米国	26	10	1	0	1
イタ	7	2	0	0	0
ドイツ	14	3	0	0	1
香港	16	4	0	0	0
シンガポール	15	0	0	0	0

(3) DOS、Windows 系

利用台数	1～10台	11～50台	51～100台	101～300台	301台～
米国	83	27	5	9	7
イタ	79	13	2	0	1
ドイツ	55	19	2	0	1
香港	83	25	4	10	3
シンガポール	139	28	3	0	0

(4) Macintosh 系

利用台数	1～10台	11～50台	51～100台	101～300台	301台～
米国	3	1	0	1	5
イタ	1	0	0	0	1
ドイツ	0	0	0	0	0
香港	0	0	0	0	0
シンガポール	2	0	0	0	0

5 . 想定される感染経路

感染経路	米 国	イタリ	日 本	香 港	シンガポール
シェアウェア サンプルソフト	20	5	4	16	19
ネットワークによる外部からの侵入	27	11	1	6	18
知人から借用、コピーしたソフト	22	18	4	25	40
市販ソフト雑誌	3	4	2	7	1
他部署からのFD	44	28	28	48	82
取引先からのFD	56	46	53	54	75
メーカーのサービス時	1	4	0	14	3
その他	42	21	17	12	17
不明	17	8	5	10	18
合 計	232	145	114	192	281

6 . 復旧方法

復旧方法	米 国	イ ン	ド ン	香 港	シ ン
自分で対応	97	68	65	79	81
社内〇技術者に相談	82	21	24	26	30
外部〇機関に相談	5	6	5	19	16
各種ツール使用	76	36	42	57	71
ソフトウェア〇再購入	11	0	2	2	1
データ〇再入力	18	4	3	19	25
バックアップ再ロード	12	9	6	26	28
ワチソフ独自開発	13	1	5	11	4
そ〇他	16	11	6	11	15
合 計	330	156	158	250	271

7. 被害規模（期間・投入人日）

復旧期間	米 国	イ ン	ド ン	香 港	シンガポール
1日未満	151	96	77	100	155
1～3日程度	31	11	7	23	27
1週間程度	7	5	7	4	7
1～2週間程度	3	3	1	6	3
1ヵ月程度	1	0	1	4	1
3ヵ月程度	0	0	0	2	0
6ヵ月程度	0	0	0	1	0
6ヵ月以上	0	0	0	0	1
復旧不可能	0	0	0	0	1
合 計	193	115	93	140	195

復旧人日	米 国	イ ン	ド ン	香 港	シンガポール
1人日未満	145	84	30	105	138
1～5人日	35	27	12	22	27
6～10人日	1	3	2	4	3
11～20人日	1	0	0	2	1
21～30人日	1	0	0	2	1
31～50人日	0	0	0	0	0
51～100人日	0	0	0	0	0
101人日以上	1	0	0	0	0
合 計	184	114	44	135	170