IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

2003 情財第 0314 号

国内･海外におけるコンピュータウイルス被害状況調査

国内におけるコンピュータウイルス被害状況調査　報告書

2004 年 4 月

独立行政法人 情報処理推進機構

(空白ページ)

目　次

1. 調査概要

1.1 調査目的

コンピュータウイルスによる被害が、社会に大きな影響を及ぼすことが予想される中、被害に対する防止策の充実は、喫緊の課題となってきている。

このような状況において、経済産業省（当時、通商産業省）は、平成 2 年 4 月に策定された「コンピュータウイルス対策基準」の改訂を平成 16 年 1 月 5 日（経済産業省告示第 2 号）に行った。この基準に基づき、独立行政法人情報処理推進機構は被害の届出機関の指定を受け、被害の拡大および再発防止のための様々な活動を実施している。

本調査は、こうした活動の一環として、最新のコンピュータウイルス関連の被害実態及びコンピュータウイルス対策の実施状況を把握し、コンピュータウイルス対策を推進していくための基礎資料を得ることを目的とし、実施するものであり、1989 年から行っている調査の 15 回目となる。

昨年より、特に自治体を取りあげ、民間企業と比較をすることにより、情報セキュリティ体制や意識の官民の差異を合わせてみていくこととした。

1.2 調査対象

本調査は、全国の事業所及び自治体 5,000 件を調査対象として実施した。その内訳は、全国の事業所から無作為に抽出した 4,000 件、及び無作為に抽出した全国の自治体 1,000 件となっている。

	内　容
標本数	5,000 件 （うち、事業所 4,000 件、自治体 1,000 件）
標本台帳	①事業所・企業統計調査名簿（平成 13 年度） ②自治体名簿
抽出方法	①事業所：業種別、従業員規模別無作為抽出 ②自治体：人口規模別無作為抽出

1.3　調査期間

調査実施期間：2004 年 2 月
調査対象期間：2003 年 1 月～12 月

1.4　調査方法

郵送調査法（郵送留置、郵送回収）

1.5　回収結果

発送総数 5,000 件に対し、1,128 件の回収があり、回収率は 22.6%となっている。事業所、自治体別の内訳は下表の通りとなっている。

	発送数	回収数	回収率
全体	5,000	1,128	22.6%
事業所	4,000	663	16.6%
自治体	1,000	465	46.5%

1.6　調査項目

調査の設問項目は下記の通りとなっている。民間事業所及び自治体は共通の設問となっている。

＜設問項目＞

（1） 属性及びパソコン利用環境
（2） コンピュータウイルスに対する意識
（3） コンピュータウイルスによる被害状況
（4） コンピュータウイルス対策の現状
（5） コンピュータウイルス対策の課題

2. 調査結果

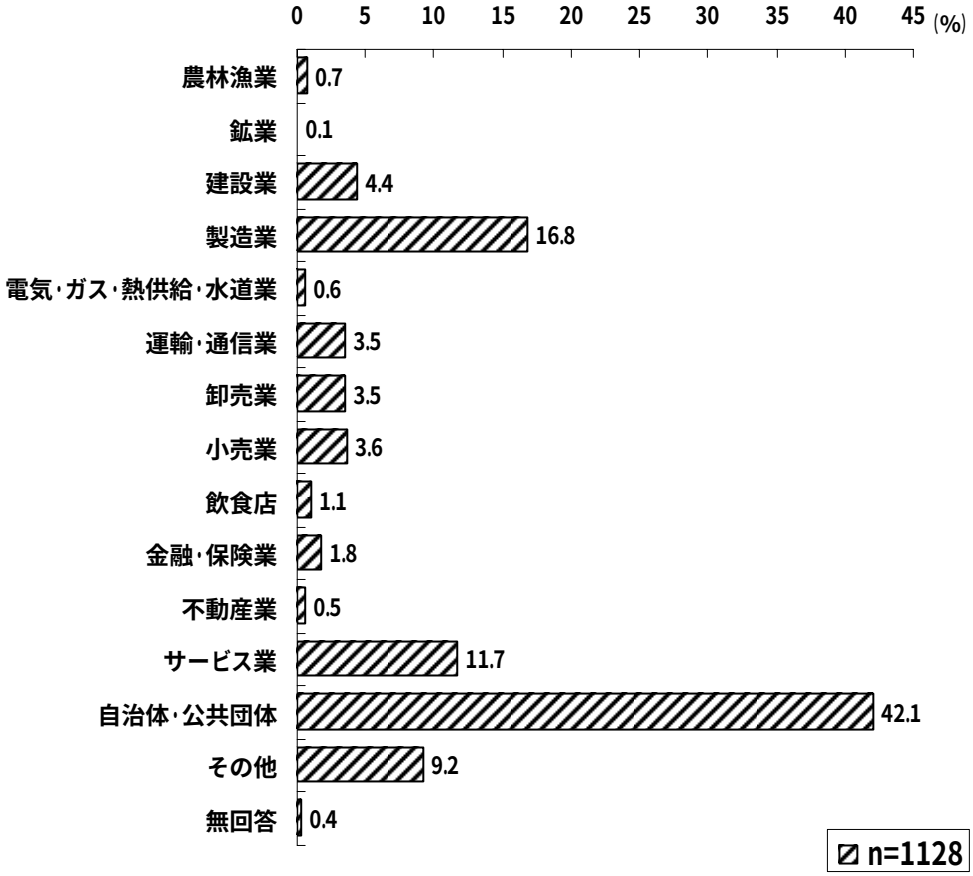
2. 1　回答事業所の概要

2. 1. 1　業種

回答事業所の業種については、「製造業」が 16.8%と最も多く、次いで「サービス業」（11.7%）、「建設業」（4.4%）、「小売業」（3.6%）、「運輸・通信業」・「卸売業」（ともに 3.5%）の順となっている。

なお「自治体・公共団体」は 42.1%となっている。

図表 2.1.1　**業種**

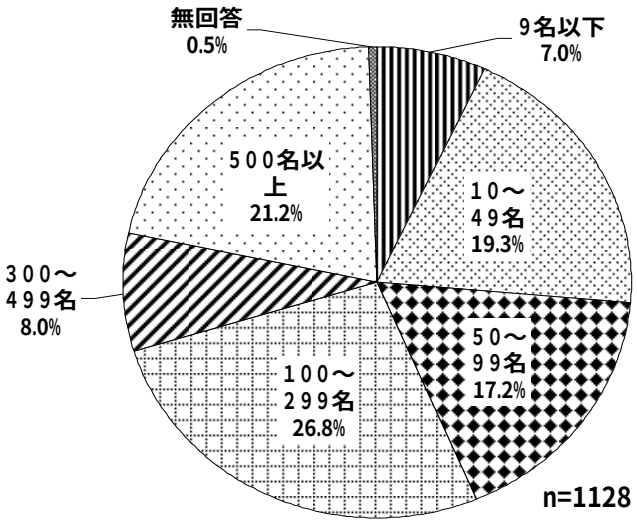


2. 1. 2　就業者数

回答事業所の就業者については、「100～299 名」が 26.8%と最も多く、次いで「500 名以上」が 21.2%、「10～49 名」が 19.3%、「50～99 名」が 17.2%の順となっている。

民間企業と自治体を比較すると、自治体では、「500 名以上」（40.4%）の割合が最も高いのに対して、民間企業では、就業者規模の小さな事業所の比率が高くなっている。

図表 2.1.2-a　**就業者数**



図表 2.1.2-b　**就業者数（自治体との比較）**

(%)

	n	9名以下	10～49名	50～99名	100～299名	300～499名	500名以上	無回答
全体	1128	7.0	19.3	17.2	26.8	8.0	21.2	0.5
民間企業	663	11.9	32.1	21.6	22.0	4.4	7.7	0.3
自治体	465	-	1.1	11.0	33.5	13.1	40.4	0.9

2. 1. 3　利用しているパソコンのＯＳと台数

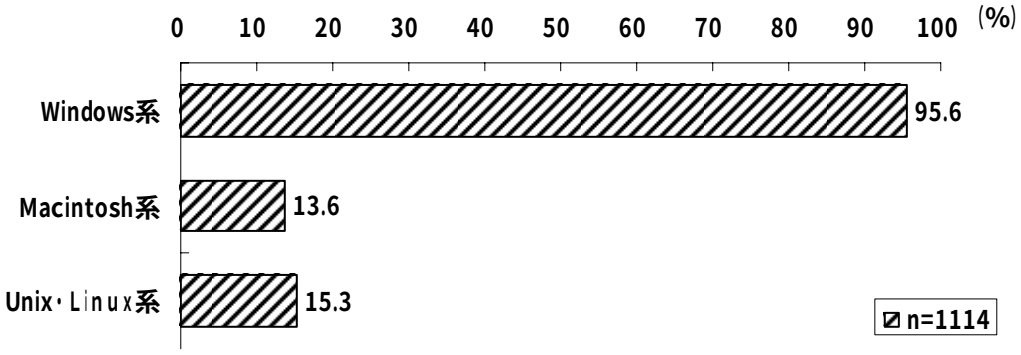
利用しているパソコンのＯＳをみると、「Windows 系」（95.6%）は大半の事業所が利用している。次いで、「Unix・Linux 系」が 15.3%、「Macintosh 系」が 13.6%となっている。

利用しているパソコンの台数をみると、全体では、「100～499 台」が 28.9%と最も多く、次いで「10～49 台」が 20.9%、「１～４台」が 12.3%の順となっている。

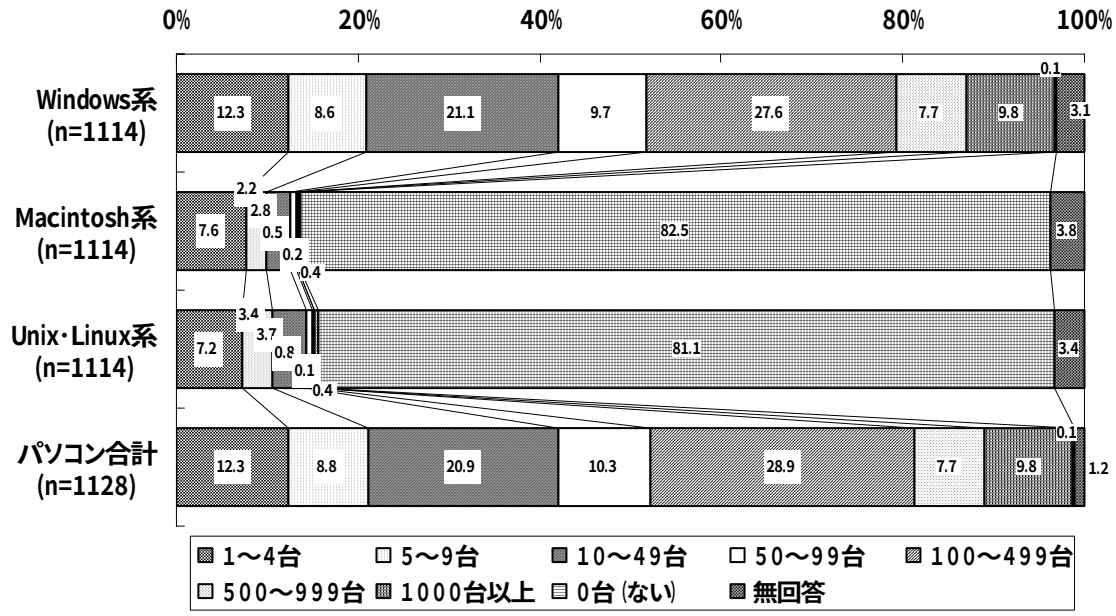
利用しているパソコンのＯＳ別台数をみると、「Windows 系」は、パソコン全体とほぼ同様の傾向を示しているのに対して、「Macintosh 系」や「Unix・Linux 系」については、利用台数の少ない事業所が多い。

民間企業と自治体それぞれのパソコンの台数は以下のとおりとなっている。

図表 2.1.3-a　**利用しているパソコンのＯＳ**



図表 2.1.3-b　利用しているパソコンのＯＳと台数



図表 2.1.3-c　利用しているパソコンのＯＳと台数（自治体との比較）

〔Windows系〕

(%)

	n	1～4台	5～9台	10～49台	50～99台	100～499台	500～999台	1000台以上	0台（ない）	無回答
全体	1114	12.3	8.6	21.1	9.7	27.6	7.7	9.8	0.1	3.1
民間企業	663	20.9	14.7	34.6	8.9	13.6	1.8	2.0	0.2	3.4
自治体	465	-	-	2.0	10.9	47.4	16.1	20.9	-	2.8

〔Macintosh系〕

(%)

	n	1～4台	5～9台	10～49台	50～99台	100～499台	500～999台	1000台以上	0台（ない）	無回答
全体	1114	7.6	2.2	2.8	0.5	0.2	-	0.4	82.5	3.8
民間企業	654	6.9	2.6	3.1	0.6	0.3	-	-	82.3	4.3
自治体	460	8.7	1.7	2.4	0.4	-	-	0.9	82.8	3.0

〔Unix／Linux系〕

(%)

	n	1～4台	5～9台	10～49台	50～99台	100～499台	500～999台	1000台以上	0台（ない）	無回答
全体	1114	7.2	3.4	3.7	0.8	0.1	-	0.4	81.1	3.4
民間企業	654	6.1	2.6	2.4	0.3	0.2	-	-	84.4	4.0
自治体	460	8.7	4.6	5.4	1.5	-	-	0.9	76.3	2.6

〔パソコン合計〕

(%)

	n	1～4台	5～9台	10～49台	50～99台	100～499台	500～999台	1000台以上	0台（ない）	無回答
全体	1128	12.3	8.8	20.9	10.3	28.9	7.7	9.8	0.1	1.2
民間企業	663	21.0	14.9	34.2	9.8	14.8	1.5	2.4	0.2	1.2
自治体	465	-	-	1.9	11.0	49.0	16.6	20.4	-	1.1

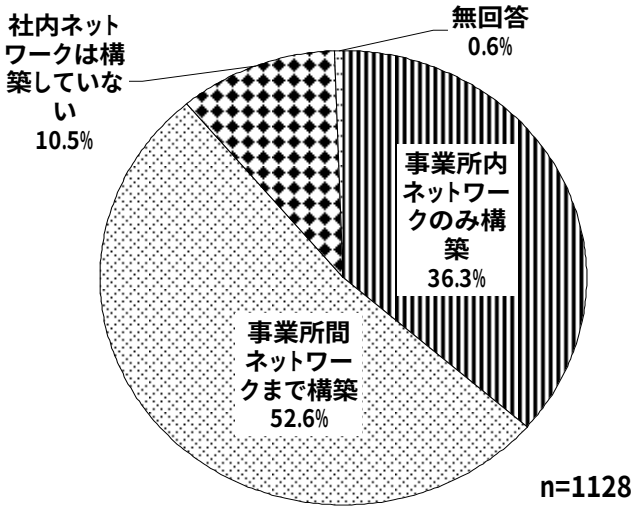
2. 1. 4　社内情報ネットワークの構築状況

社内情報ネットワークの構築状況については、「事業所間ネットワーク(WAN)まで構築」が 52.6%と半数以上を占めており、「事業所内ネットワーク(LAN)のみ構築」の 36.3%と合わせると 88.9%が情報ネットワークを構築している。

一方、「社内ネットワークは構築していない」の比率は 10.5%となっている。

民間企業と自治体を比較すると、情報ネットワーク構築比率（「事業所内ネットワーク(LAN)のみ構築」＋「事業所間ネットワーク(WAN)まで構築」）は、自治体（98.3%）が民間企業（82.2%）を上回っている。逆に、「社内ネットワークは構築していない」の比率は、民間企業が自治体より 15.7 ポイント高くなっている。

図表 2.1.4-a　**社内情報ネットワークの構築状況**



図表 2.1.4-b　**社内情報ネットワークの構築状況（自治体との比較）**

(%)

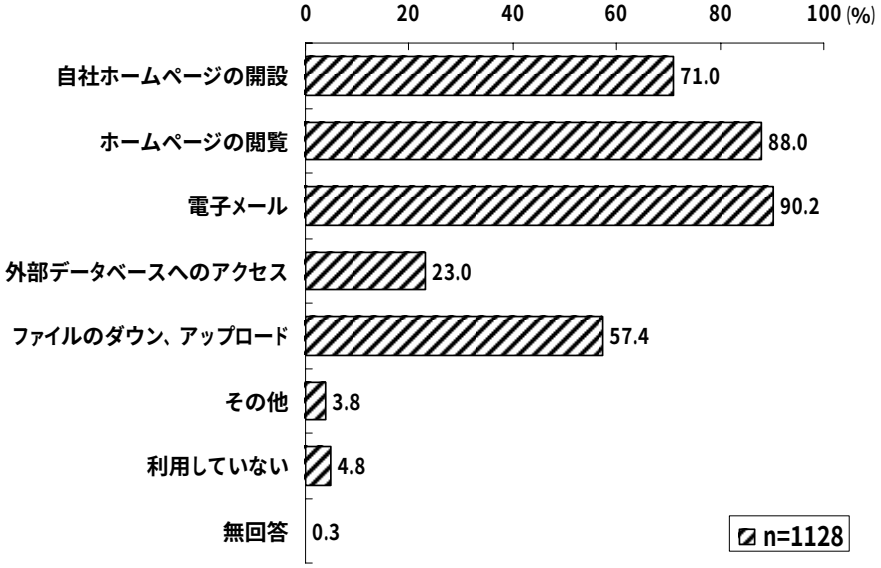
	n	事業所内ネットワークのみ構築	事業所間ネットワークまで構築	社内ネットワークは構築していない	無回答
全体	1128	36.3	52.6	10.5	0.6
民間企業	663	45.1	37.1	17.0	0.8
自治体	465	23.7	74.6	1.3	0.4

2.1.5　インターネットの利用状況

インターネットの利用状況については、「電子メール」が 90.2%と最も多く、次いで「ホームページの閲覧」（88.0%）、「自社ホームページの開設」（71.0%）、「ファイルのダウン・アップロード」（57.4%）、「外部データベースへのアクセス」（23.0%）の順となっている。

民間企業と自治体を比較すると、自治体では、「自社ホームページの開設」（93.1%）の割合が民間企業より 37.6 ポイントも高くなっている。さらに、「ホームページの閲覧」、「電子メール」において、それぞれ 12 ポイント程度、民間企業を上回っている。

図表 2.1.5-a　**インターネット利用状況**



※複数回答設問

その他　：　VPN（7 件）、EDI（6 件）、
　　電子商取引（5 件）、など

図表 2.1.5-b　**インターネットの利用状況（自治体との比較）**

(%)

	n	自社ホームページの開設	ホームページの閲覧	電子メール	外部データベースへのアクセス	ファイルのダウン、アップロード	その他	利用していない	無回答
全体	1128	71.0	88.0	90.2	23.0	57.4	3.8	4.8	0.3
民間企業	663	55.5	83.0	85.2	24.9	54.9	5.0	7.7	0.3
自治体	465	93.1	95.3	97.2	20.4	61.1	2.2	0.6	0.2

※複数回答設問

2. 1. 6　**マクロの利用状況**（MS-Word、MS-Excel）

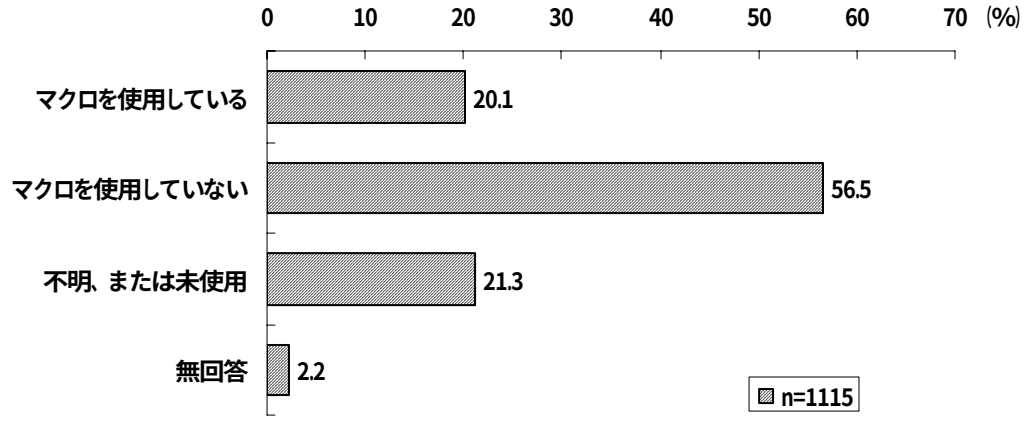
「MS-Word」の業務上でのマクロの使用状況については、「マクロを使用している」が 20.1%、「マクロを使用していない」が 56.5%となっている。

これに対し、「MS-Excel」では結果が逆転し、「マクロを使用している」が 63.0%、「マクロを使用していない」が 22.9%となっている。

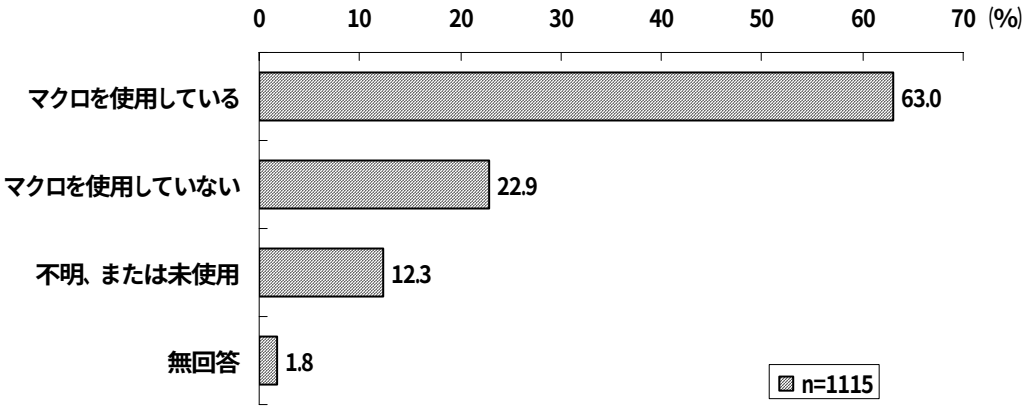
民間企業と自治体を比較すると、「マクロを使用している」の割合は、自治体の方が高く、「MS-Word」で 8.1 ポイント、「MS-Excel」で 14.2 ポイント、それぞれ民間企業を上回っている。

図表 2.1.6-a　**マクロの利用状況**

①MS-Word



②MS-Excel



図表 2.1.6-b　マクロの利用状況（自治体との比較）

①MS-Word

(%)

	n	Wordでマクロ使用している	Wordでマクロ使用していない	不明、またはWord未使用	無回答
全体	1115	20.1	56.5	21.3	2.2
民間企業	651	16.7	60.4	20.0	2.9
自治体	464	24.8	51.1	23.1	1.1

②MS-Excel

(%)

	n	Excelでマクロ使用している	Excelでマクロ使用していない	不明、またはExcel未使用	無回答
全体	1115	63.0	22.9	12.3	1.8
民間企業	651	57.1	27.8	12.4	2.6
自治体	464	71.3	15.9	12.1	0.6

2. 2　コンピュータウイルスに対する意識

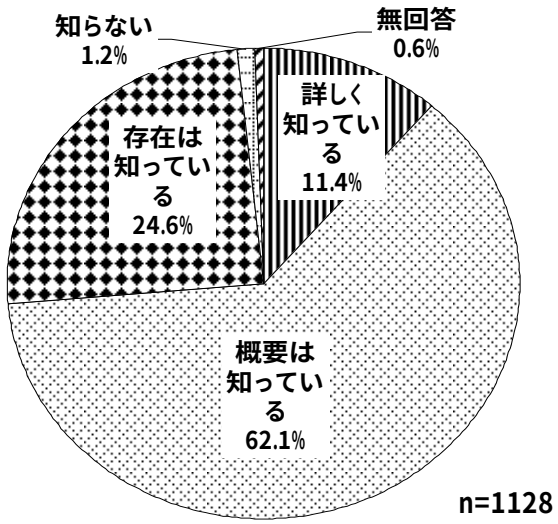
2. 2. 1　コンピュータウイルスの認知度

コンピュータウイルスに対する認知度については、「概要は知っている」が 62.1%と最も多く、次いで「存在は知っている」（24.6%）、「詳しく知っている」（11.4%）の順となっており、「知らない」は、わずか 1.2%であった。

民間企業と自治体とを比較すると、自治体では「概要は知っている」の割合が 77.8%と高く、「詳しく知っている」と合わせると、自治体の 9 割がコンピュータウイルスに対する何らかの知識を有している。これに対して、民間企業では、「存在は知っている」（35.9%）の比率が自治体に比べて高くなっている。

過去からの推移をみると、「詳しく知っている」と「概要は知っている」の比率は、ともに 2001 年まで年々増加したが、2002 年から減少傾向に転じている。今回の調査では、「詳しく知っている」の割合が、過去 6 年間で最も低くなった。

図表 2.2.1-a　**コンピュータウイルスの認知度**

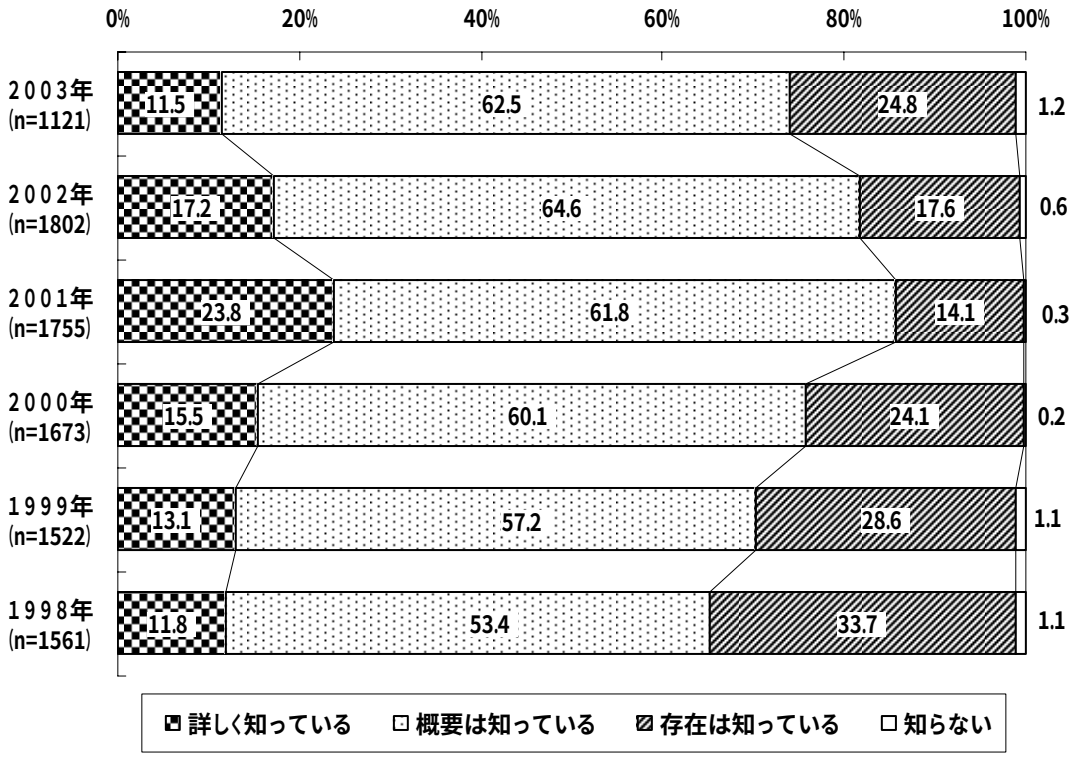


図表 2.2.1-b　**コンピュータウイルスの認知度（自治体との比較）**

(%)

	n	詳しく（専門的に）知っている	概要（種類、名称など）は知っている	存在は知っている	知らない	無回答
全体	1128	11.4	62.1	24.6	1.2	0.6
民間企業	663	10.4	51.1	35.9	1.8	0.8
自治体	465	12.9	77.8	8.6	0.2	0.4

図表 2.2.1-c　**コンピュータウイルスの認知度（時系列）**

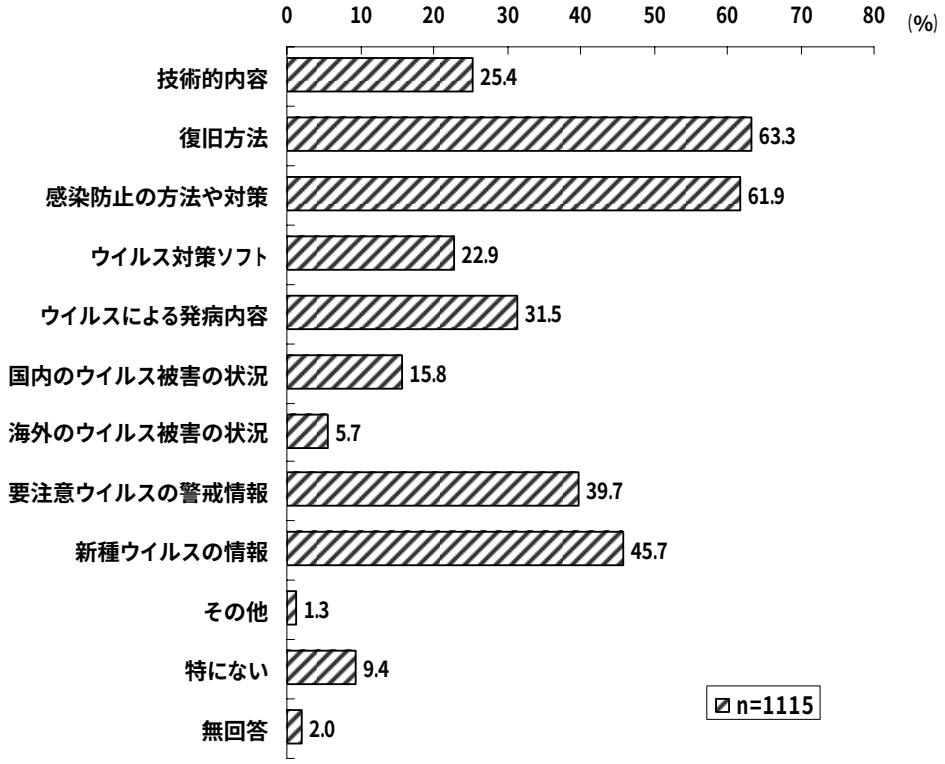


注）　時系列結果の比較のため、無回答を除いて 2003 年の値を再集計しており、前頁の比率と異なる。

2. 2. 2　コンピュータウイルスに関して知りたい情報

コンピュータウイルスに関連して知りたい情報については、「感染したときの復旧方法」が 63.3%と最も多く、次いで「感染防止の方法や対策」（61.9%）、「新種ウイルスの情報」（45.7%）、「要注意ウイルスの警戒情報」（39.7%）、「ウイルスによる発病内容」（31.5%）の順となっている。

図表 2.2.2-a　**コンピュータウイルスに関して知りたい情報**



※複数回答設問

その他　：　作者の追及対策（国際的な）、 ウイルスの作成方法の勉強、
ウイルスによる金額的損失の事例、 ISP 等でのフィルタ状況、
ウイルスの体験交流、　など

全体的に民間企業より自治体の回答比率が高くなっており、特に、「新種ウイルスの情報」で 22.0 ポイント、「要注意ウイルスの警戒情報」で 18.6 ポイント、「ウイルスが引き起こす発病内容」で 14.4 ポイントそれぞれ自治体が民間企業を上回っている。

過去からの推移をみると、「ウイルス対策ソフト情報」は減少傾向にあり、基本的なソフトに関する情報はかなり普及したことが推察される。一方、「感染した時の復旧方法」や、「感染しないための方法や対策」、「新種ウイルスの情報」などの項目は、高比率で経年的な変化があまりなく、次々と出てくる新種ウイルスや、ウイルス個別の対応方策など、より具体的な情報は常に求められていることがわかる。

図表 2.2.2-b　**コンピュータウイルスに関して知りたい情報（自治体との比較）**

(%)

	n	しくみ･種類等の技術的内容	感染した時の復旧方法	感染しないための方法や対策	ウイルス対策ソフト情報	ウイルスが引き起こす発病内容	国内のウイルス被害の状況
全体	1115	25.4	63.3	61.9	22.9	31.5	15.8
民間企業	651	21.5	61.1	57.9	21.8	25.5	11.1
自治体	464	30.8	66.4	67.5	24.4	39.9	22.4

	n	海外のウイルス被害の状況	要注意ウイルスの警戒情報	新種ウイルスの情報	その他	特にない	無回答
全体	1115	5.7	39.7	45.7	1.3	9.4	2.0
民間企業	651	4.6	32.0	36.6	1.2	12.0	2.9
自治体	464	7.1	50.6	58.6	1.3	5.8	0.6

※複数回答設問

図表 2.2.2-c　**コンピュータウイルスに関して知りたい情報の推移（時系列）**

（%）

	1998年 (n=1543)	1999年 (n=1505)	2000年 (n=1674)	2001年 (n=1755)	2002年 (n=1791)	2003年 (n=1115)
しくみ･種類等の技術的内容	37.1	31.6	26.8	26.7	25.4	25.4
感染した時の復旧方法	63.1	68.5	64.8	68.1	64.3	63.3
感染しないための方法や対策	60.5	62.7	57.8	66.0	60.4	61.9
ウイルス対策ソフト情報	47.4	46.9	38.2	38.7	27.0	22.9
コンピュータウイルスが引き起こす発病内容	47.8	48.0	37.6	41.6	34.8	31.5
国内のウイルス被害の状況	36.6	33.2	22.4	18.7	19.5	15.8
海外のウイルス被害の状況	20.1	16.4	12.8	11.3	8.4	5.7
要注意ウイルスの警戒情報	-	-	48.9	54.4	50.7	39.7
新種ウイルスの情報	-	-	49.2	54.9	53.0	45.7
その他	1.8	1.9	1.1	1.5	0.8	1.3
特にない	7.0	6.4	5.0	4.2	5.8	9.4

※複数回答設問

2. 3　コンピュータウイルスによる被害状況

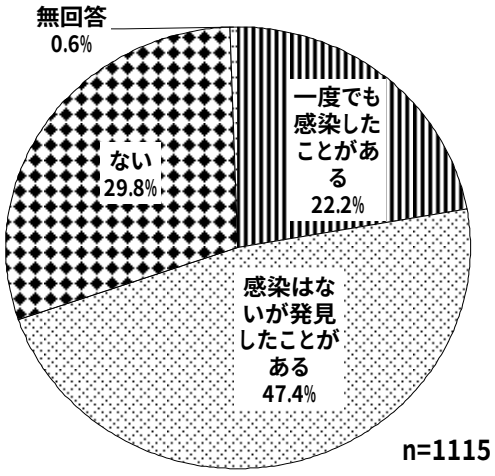
2. 3. 1　コンピュータウイルス遭遇（感染または発見）経験

2003 年 1 月から 2003 年 12 月の 1 年間におけるコンピュータウイルス遭遇経験の有無については、「感染はないが発見したことがある」が 47.4%となっており、「一度でも感染したことがある」（22.2%）と合わせると、69.6%の事業所でコンピュータウイルスに遭遇（発見・感染）した経験があることとなる。

民間企業と自治体の比較をみると、コンピュータウイルス遭遇率（「一度でも感染したことがある」＋「感染はないが発見したことがある」）は、自治体（87.5%）が民間企業（56.9%）よりも 30 ポイント以上高くなっている。

過去からの推移をみると、1997 年から増加が続いていたコンピュータウイルス遭遇率が、今回の調査では 10 ポイント以上減少した。

図表 2.3.1-a　**コンピュータウイルス遭遇経験**

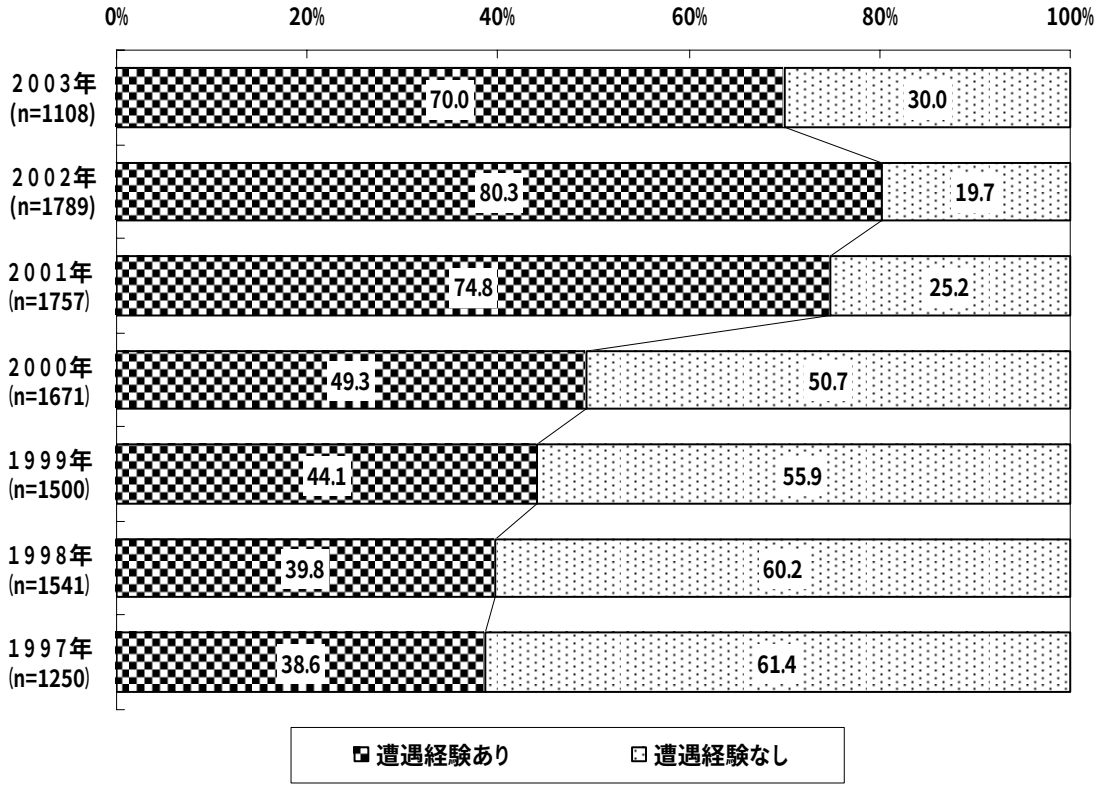


図表 2.3.1-b　**コンピュータウイルス遭遇経験（自治体との比較）**

(%)

	n	一度でも感染したことがある	感染はないが発見したことがある	ない	無回答
全体	1115	22.2	47.4	29.8	0.6
民間企業	651	21.4	35.5	42.4	0.8
自治体	464	23.3	64.2	12.1	0.4

図表 2.3.1-c　**コンピュータウイルス遭遇経験の推移（時系列）**



注１）「遭遇経験あり」とは、「一度でも感染したことがある」と「感染はないが発見したことがある」の合計を示す。

注２）時系列結果の比較のため、無回答を除いて 2003 年の値を再集計しており、前頁の比率と異なる。

遭遇経験を業種別にみると、「自治体・公共団体」における遭遇発生率が 86.9%と最も高く、次いで「製造業」（66.5%）、「建設業」（59.6%）などが続いている。

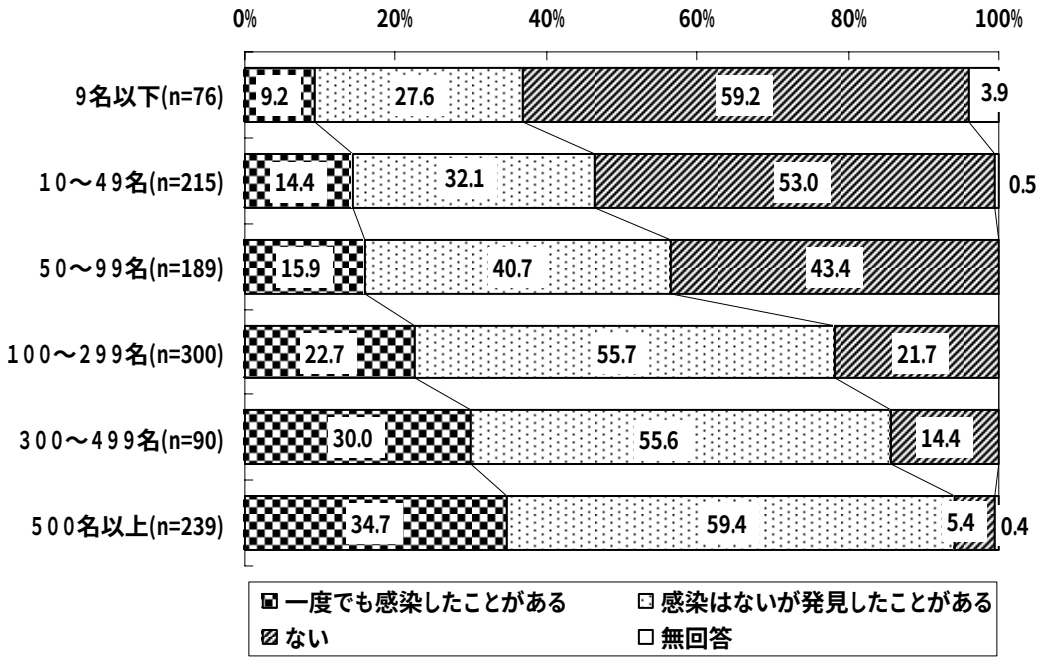
「遭遇」の内訳をみると、「自治体・公共団体」では、遭遇発生率の高さに対し、感染率は 23.4%と低くなっており、感染を未然に防いでいる様子がうかがえる。これに対し、「製造業」などでは、遭遇に占める感染の比率が比較的高くなっている。

図表 2.3.1-d　**コンピュータウイルス遭遇経験（業種別）**

業種	回答事業所数（件）	遭遇発生率(%)	うち感染率(%)
農林漁業･鉱業	9	11.1	0.0
建設業	47	59.6	21.3
製造業	188	66.5	23.9
運輸･通信業	39	41.0	20.5
卸売･小売業･飲食店	89	58.4	22.5
金融･保険･不動産業	26	34.6	3.8
サービス業	129	53.5	20.2
電気･ガス･熱供給･水道･その他	110	56.4	21.8
自治体･公共団体	474	86.9	23.4
無回答	4	50.0	50.0
総計	1115	69.6	22.2

さらに、遭遇経験を就業者規模別にみると、事業所の規模が大きい程、コンピュータウイルスを発見した比率及び感染率が高くなっている。

図表 2.3.1-e　**コンピュータウイルス遭遇経験（就業者規模別）**



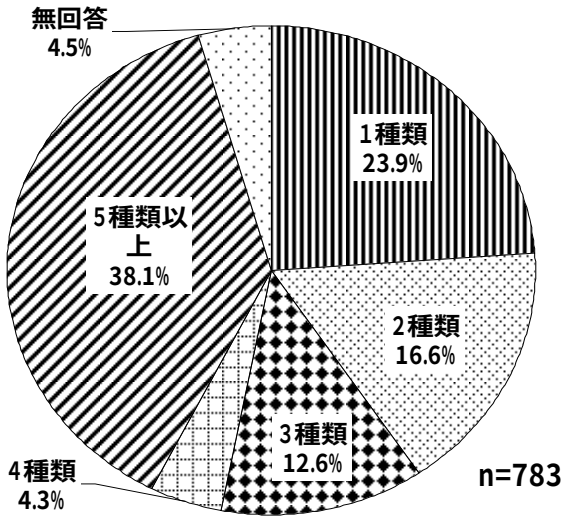
2. 3. 2　遭遇したウイルスの種類数

感染または発見したウイルスの種類数については、「5 種類以上」が 38.1%と最も多く、次いで「1 種類」（23.9%）、「2 種類」（16.6%）、「3 種類」（12.6%）の順となっている。

自治体と民間企業を比較すると、自治体では、「5 種類以上」が過半数を占め、民間企業より遭遇したウイルスは多種類となっている。

また、過去からの推移をみると、「1 種類」が年々減少しているのに対して、「5 種類以上」は年々増加している。

図表 2.3.2-a　**遭遇したウイルスの種類**

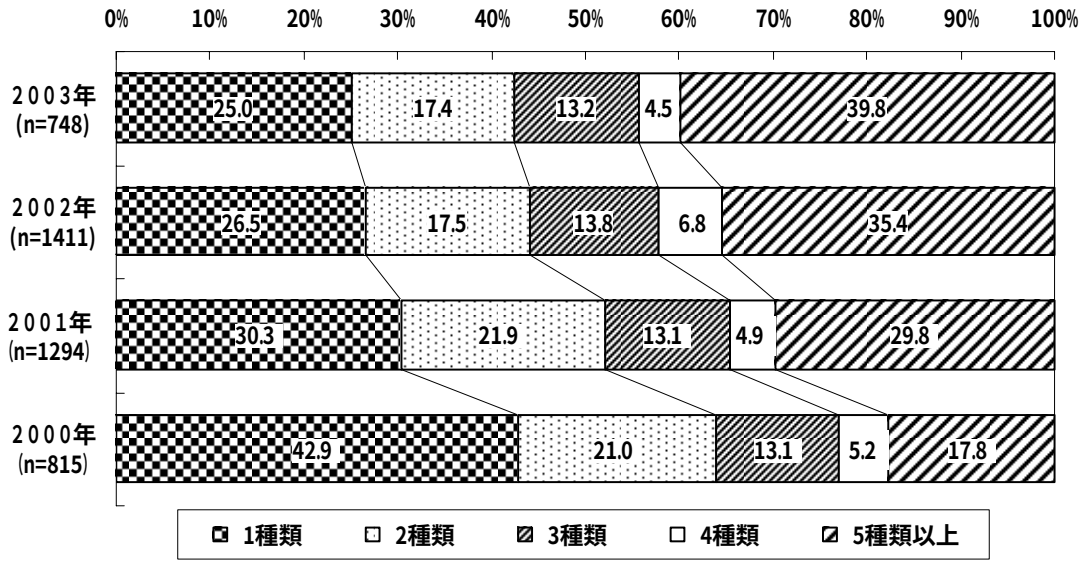


図表 2.3.2-b　**遭遇したウイルスの種類（自治体との比較）**

(%)

	n	1種類	2種類	3種類	4種類	5種類以上	無回答
全体	783	23.9	16.6	12.6	4.3	38.1	4.5
民間企業	375	29.9	22.9	13.1	3.2	24.3	6.7
自治体	408	18.4	10.8	12.3	5.4	50.7	2.5

図表 2.3.2-c　**遭遇したウイルスの種類の推移（時系列）**



注）　時系列結果の比較のため、無回答を除いて 2003 年の値を再集計しており、前頁の比率と異なる。

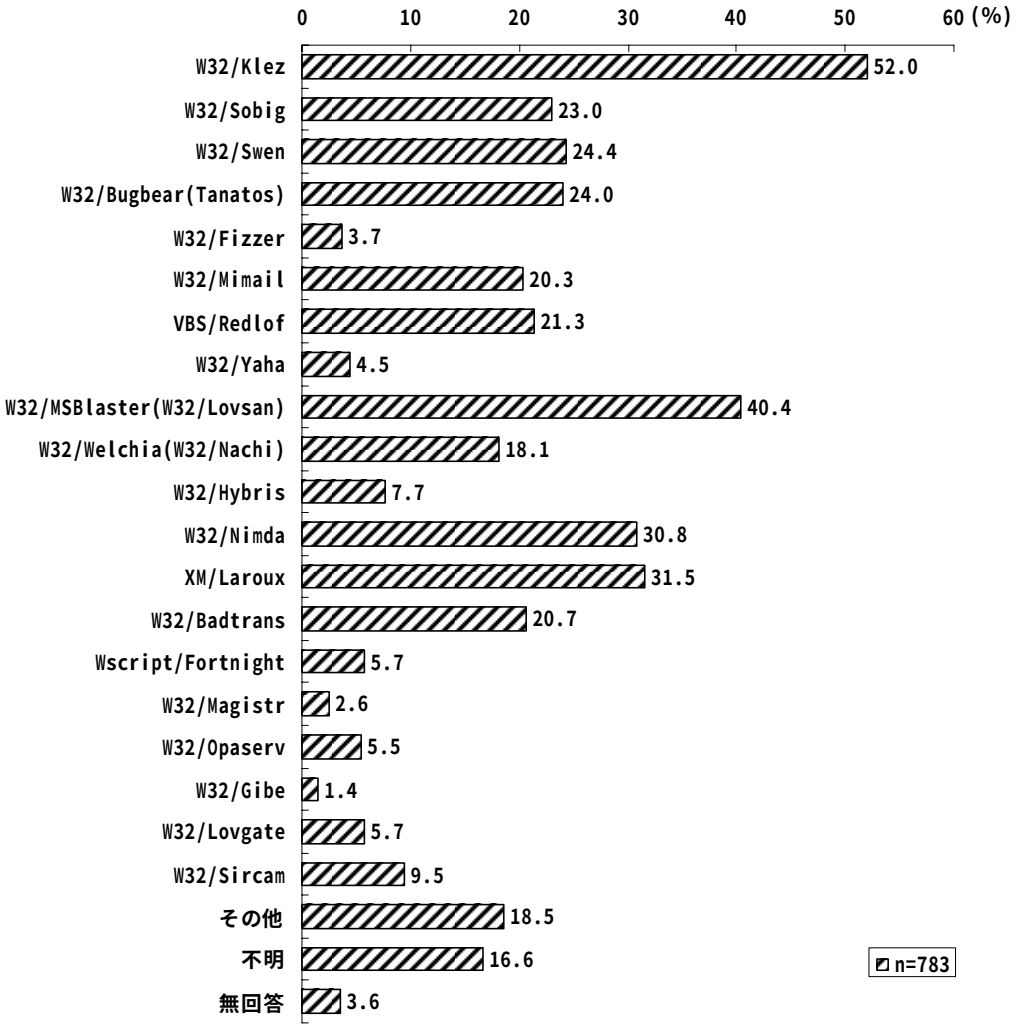
2. 3. 3　遭遇したウイルスの名称

感染または発見したコンピュータウイルスの名称については、「W32/Klez」が 52.0%と最も多く、次いで「W32/MSBlaster(W32/Lovsan)」（40.4%）、「XM/Laroux」（31.5%）、「W32/Nimda」（30.8%）、「W32/Swen」（24.4%）、「W32/Bugbear(Tanatos)」（24.0%）の順となっている。

上位にのぼっているのは、メール機能を悪用するタイプ（W32/Klez 等）や、感染するとバックドアをインストールするタイプ（W32/Bugbear 等）などである。

民間企業と自治体を比較すると、全体的に自治体の方がウイルスに遭遇した割合が高くなっている。自治体が民間企業を大きく上回っているものには、「XM/Laroux」（30.4 ポイント）、「VBS/Redlof」（28.6 ポイント）、「W32/Swen」（23.8 ポイント）などがある。

図表 2.3.3-a　**遭遇したウイルスの名称**



※複数回答設問

その他　：　JAVA/BYTVERIFY.A（9 件）、X97M/Divi（7 件）、
JS/Exception（6 件）、W32/Funlove（5 件）、
VBS/Haptime（5 件）、VBS/LOVELETTER（4 件）、
X97M/Tracker（3 件）、W32/Gaobot（3 件）、
W32/Inor（3 件）、JS/Noclose（3 件）、JS/CBASE（3 件）、
W32/Slammer（2 件）、W32/Frethem（2 件）、
JS/Seeker（2 件）、など

図表 2.3.3-b　**遭遇したウイルスの名称（自治体との比較）**

(%)

	n	W32/ Klez	W32/ Sobig	W32/ Swen	W32/ Bugbear (Tanatos)	W32/ Fizzer	W32/ Mimail	VBS/ Redlof	W32/ Yaha
全体	783	52.0	23.0	24.4	24.0	3.7	20.3	21.3	4.5
民間企業	375	41.9	13.3	12.0	17.6	3.2	13.1	6.4	3.2
自治体	408	61.3	31.9	35.8	29.9	4.2	27.0	35.0	5.6

	n	W32/ MSBlaster (W32/ Lovsan)	W32/ Welchia (W32/ Nachi)	W32/ Hybris	W32/ Nimda	XM/ Laroux	W32/ Badtrans	Wscript/ Fortnight	W32/ Magistr
全体	783	40.4	18.1	7.7	30.8	31.5	20.7	5.7	2.6
民間企業	375	34.7	13.1	5.3	32.5	15.7	12.8	2.7	1.6
自治体	408	45.6	22.8	9.8	29.2	46.1	27.9	8.6	3.4

	n	W32/ Opaserv	W32/ Gibe	W32/ Lovgate	W32/ Sircam	その他	不明	無回答
全体	783	5.5	1.4	5.7	9.5	18.5	16.6	3.6
民間企業	375	5.1	0.3	4.3	6.7	13.9	22.7	5.6
自治体	408	5.9	2.5	7.1	12.0	22.8	11.0	1.7

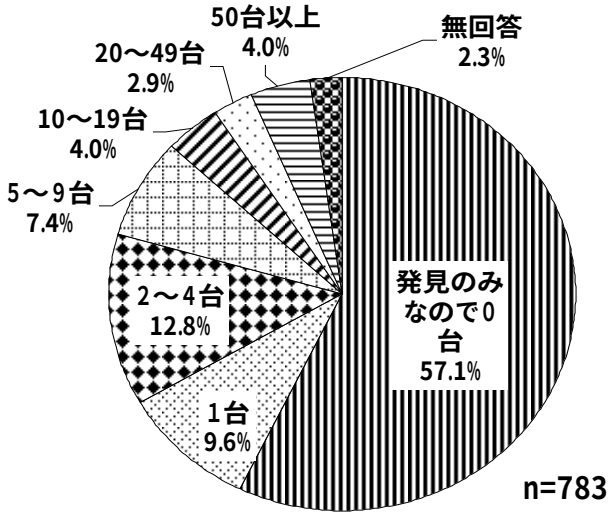
※複数回答設問

2. 3. 4　感染したパソコンの台数

ウイルスに感染したパソコンの台数については、「発見のみなので 0 台」が 57.1%と半数以上を占め、次いで「2～4 台」（12.8%）、「1 台」（9.6%）、「5～9 台」（7.4%）、「10～19 台」・「50 台以上」（ともに 4.0%）の順となっている。

企業と自治体を比較すると、「発見のみなので 0 台」については、自治体が民間企業より 22.0 ポイント高く、未然に感染を防いでいる様子がうかがえる。

図表 2.3.4-a　**感染したパソコン台数**



図表 2.3.4-b　**感染したパソコン台数（自治体との比較）**

(%)

	n	発見のみなので0台	1台	2～4台	5～9台	10～19台	20～49台	50台以上	無回答
全体	783	57.1	9.6	12.8	7.4	4.0	2.9	4.0	2.3
民間企業	375	45.6	13.9	16.8	9.9	3.5	2.9	4.0	3.5
自治体	408	67.6	5.6	9.1	5.1	4.4	2.9	3.9	1.2

2.3.5　被害の最も大きかったウイルス

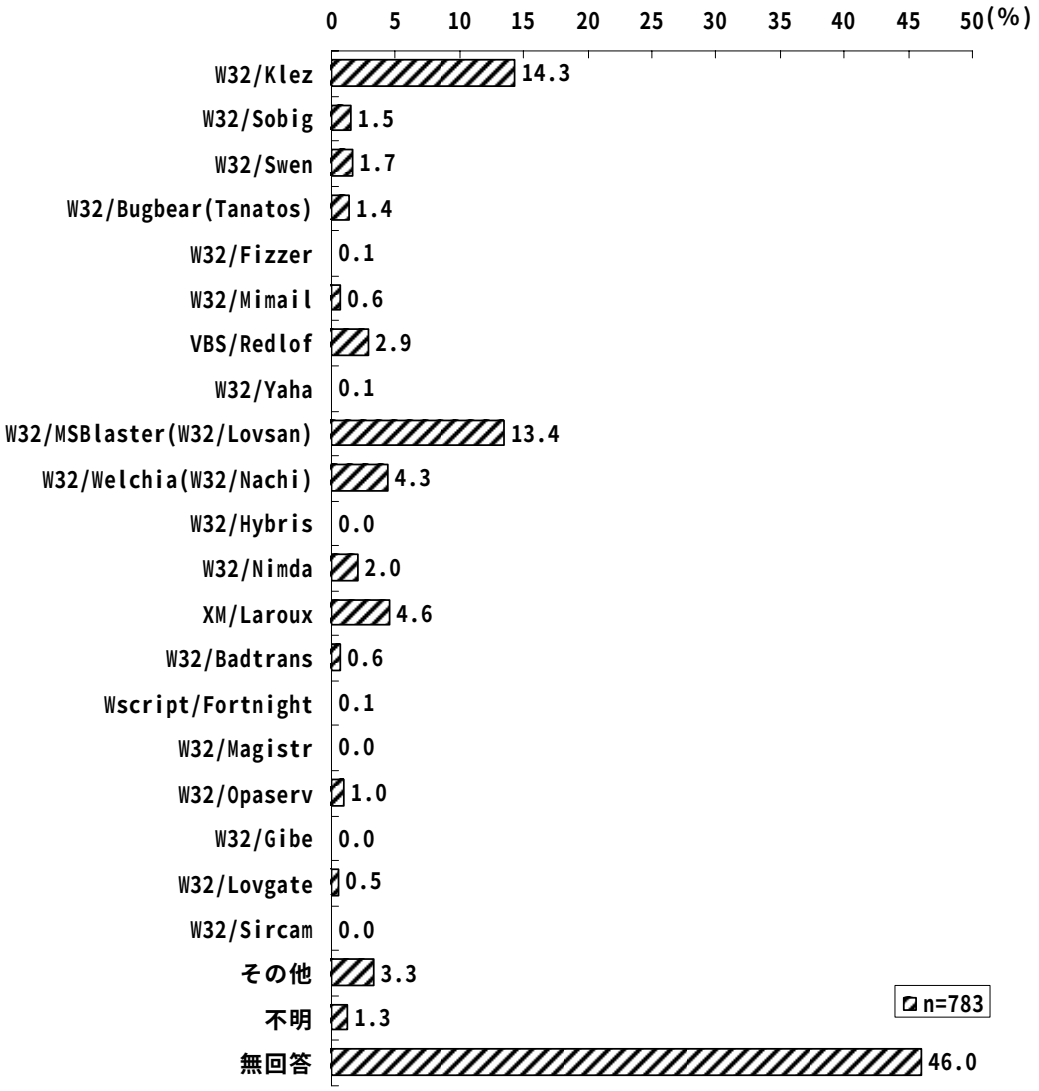
①　ウイルス名及び発見日

過去 1 年間で感染･発見した中で被害の最も大きかったウイルスについては､「W32/Klez」（14.3%）と「W32/MSBlaster(W32/Lovsan)」（13.4%）が多くなっている。次いで、「XM/Laroux」（4.6%)、「W32/Welchia(W32/Nachi)」（4.3%)、「VBS/Redlof」（2.9%）の順となっている。

民間企業と自治体に大きな差はみられない。

ウイルスの発見日については、「W32/MSBlaster(W32/Lovsan)」などが出現した「2003 年 7 月～9 月」（20.8%）が最も多くなっている。

図表 2.3.5_①-a　**被害最大のウイルス名**



図表 2.3.5_①-b　被害最大のウイルス名（自治体との比較）

[ウイルス名]

(%)

	n	W32/ Klez	W32/ Sobig	W32/ Swen	W32/ Bugbear (Tanatos)	W32/ Fizzer	W32/ Mimail	VBS/ Redlof	W32/ Yaha
全体	783	14.3	1.5	1.7	1.4	0.1	0.6	2.9	0.1
民間企業	375	10.9	0.8	0.8	2.4	0.3	0.3	0.5	-
自治体	408	17.4	2.2	2.5	0.5	-	1.0	5.1	0.2

	n	W32/ MSBlaster (W32/ Lovsan)	W32/ Welchia (W32/ Nachi)	W32/ Hybris	W32/ Nimda	XM/ Laroux	W32/ Badtrans	Wscript/ Fortnight	W32/ Magistr
全体	783	13.4	4.3	-	2.0	4.6	0.6	0.1	-
民間企業	375	14.9	2.9	-	3.7	2.9	0.8	-	-
自治体	408	12.0	5.6	-	0.5	6.1	0.5	0.2	-

	n	W32/ Opaserv	W32/ Gibe	W32/ Lovgate	W32/ Sircam	その他	不明	無回答
全体	783	1.0	-	0.5	-	3.3	1.3	46.0
民間企業	375	1.3	-	0.5	-	2.4	1.3	53.1
自治体	408	0.7	-	0.5	-	4.2	1.2	39.5

図表 2.3.5_①-c　被害最大のウイルス発見日

[発見日]

(%)

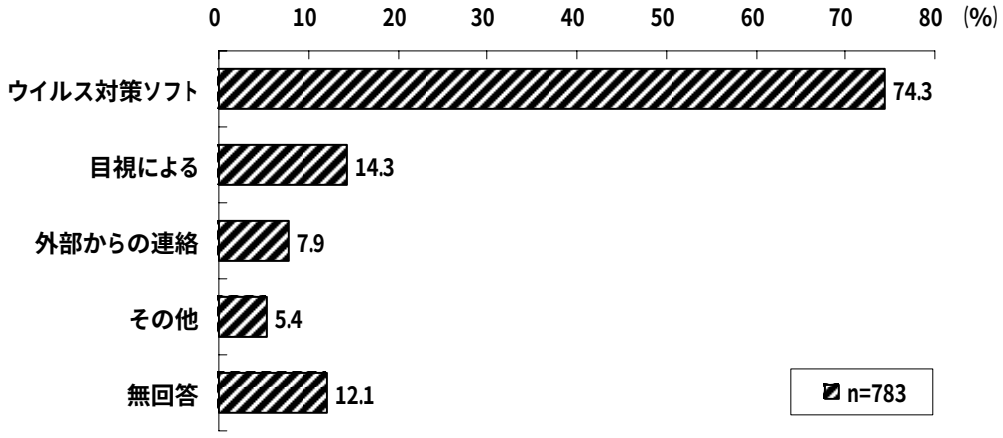
2003年 1月～3月	2003年 4月～6月	2003年 7月～9月	2003年 10月～12月	無回答
7.5	7.7	20.8	11.1	52.9

② ウイルス発見の経緯

ウイルス発見の経緯については、「ウイルス対策ソフト」が 74.3%と最も多く、次いで「目視による」（14.3%）、「外部からの連絡」（7.9%）の順となっている。

民間企業と自治体を比較すると、自治体では「ウイルス対策ソフト」において、民間企業を 12.1 ポイント上回っており、ウイルス対策がより整備されている様子がうかがえる。一方、民間企業では、「目視による」、「外部からの連絡」の割合が自治体よりも高くなっている。

図表 2.3.5_②-a **発見の経緯**



※ 複数回答設問

その他 ： パソコンの動作不良（12 件）、内部からの連絡（5 件）
プロバイダのウイルスチェックサービス（5 件）、 など

図表 2.3.5_②-b **発見の経緯（自治体との比較）**

(%)

	n	ウイルス対策ソフト	目視による	外部からの連絡	その他	無回答
全体	783	74.3	14.3	7.9	5.4	12.1
民間企業	375	68.0	16.8	10.4	8.0	12.5
自治体	408	80.1	12.0	5.6	2.9	11.8

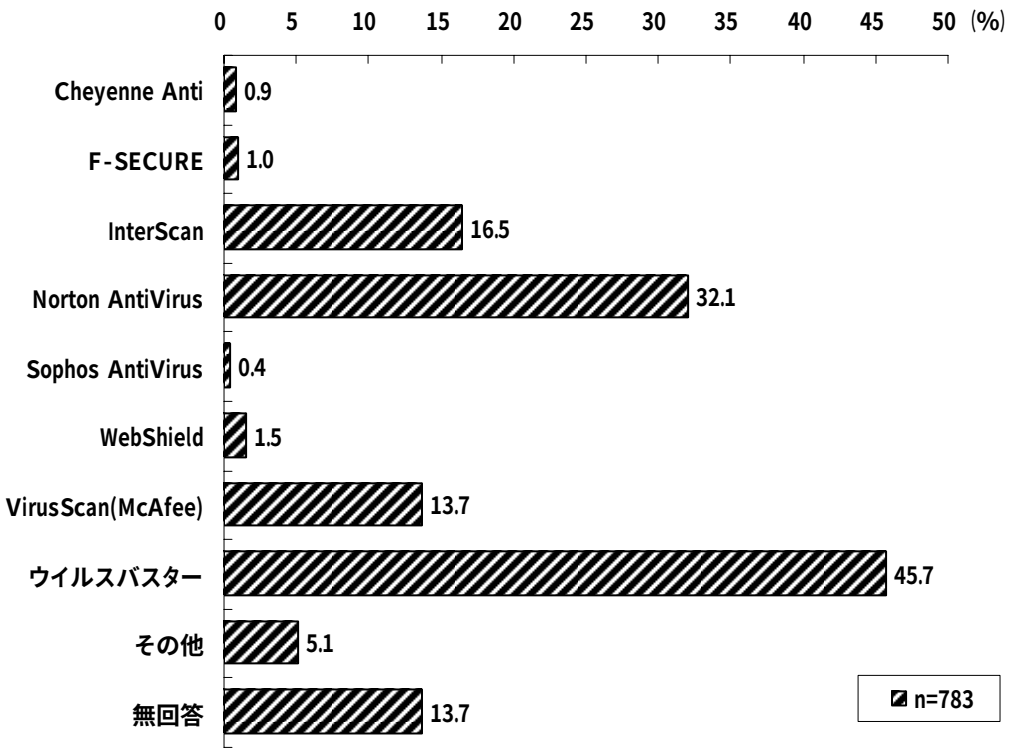
※複数回答設問

③　発見に使用したウイルス対策ソフト

発見に使用したウイルス対策ソフトについては、「ウイルスバスター」が 45.7%と最も多く、次いで「Norton AntiVirus」（32.1%）となっており、これら２つのソフトのシェアが高くなっている。以下、「InterScan」（16.5%）、「VirusScan(McAfee)」（13.7%）等が続いている。

民間企業と自治体を比較すると、自治体では、「ウイルスバスター」に次いで「InterScan」（24.3%）の割合が高くなっているのに対して、民間企業では、「Norton AntiVirus」（37.1%）を採用する比率が高い。

図表 2.3.5_③-a　**発見に使用したウイルス対策ソフト**



※複数回答設問

その他　：　AVG（6 件）、サーバープロテクト（5 件）、
Janisvirus Scan（2 件）、　など

図表 2.3.5_③-b　**発見に使用したウイルス対策ソフト（自治体との比較）**

(%)

	n	Cheyenne Antivirus	F－SECURE	InterScan	Norton AntiVirus	Sophos AntiVirus
全体	783	0.9	1.0	16.5	32.1	0.4
民間企業	375	0.8	0.8	8.0	37.1	-
自治体	408	1.0	1.2	24.3	27.5	0.7

	n	WebShield	VirusScan (McAfee)	ウイルスバスター	その他	無回答
全体	783	1.5	13.7	45.7	5.1	13.7
民間企業	375	0.8	13.9	42.7	4.8	15.2
自治体	408	2.2	13.5	48.5	5.4	12.3

※複数回答設問

④　感染したパソコンのＯＳと台数

感染・発見したウイルスの中で、被害の最も大きかったウイルスについて、感染・発見したパソコンの台数を尋ねたところ、「感染前に駆除したため被害なし」が 51.2%と過半数を占め、感染に至った事業所は 31.4%となっている。

民間企業と自治体を比較すると、「感染前に駆除したため被害なし」の割合は、民間企業より自治体の方が 17.9 ポイント高く、逆に、「パソコンに感染」では、民間企業が自治体より 11.3 ポイント高い。

感染のあったパソコンのＯＳについては、「Windows 系」が 97.1%、「Unix・Linux 系」が 0.4%となっており、「Macintosh 系」への感染はみられなかった。

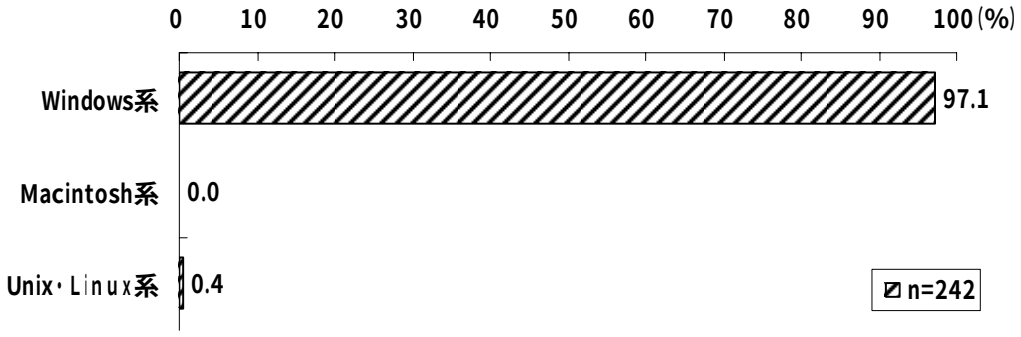
感染台数については、「１～４台」が 54.5%と最も多くなっており、次いで「10～49 台」（18.3%）、「5～9 台」（14.2%）などとなっている。

図表 2.3.5_④-a　被害の最も大きかったウイルスのパソコンへの感染状況

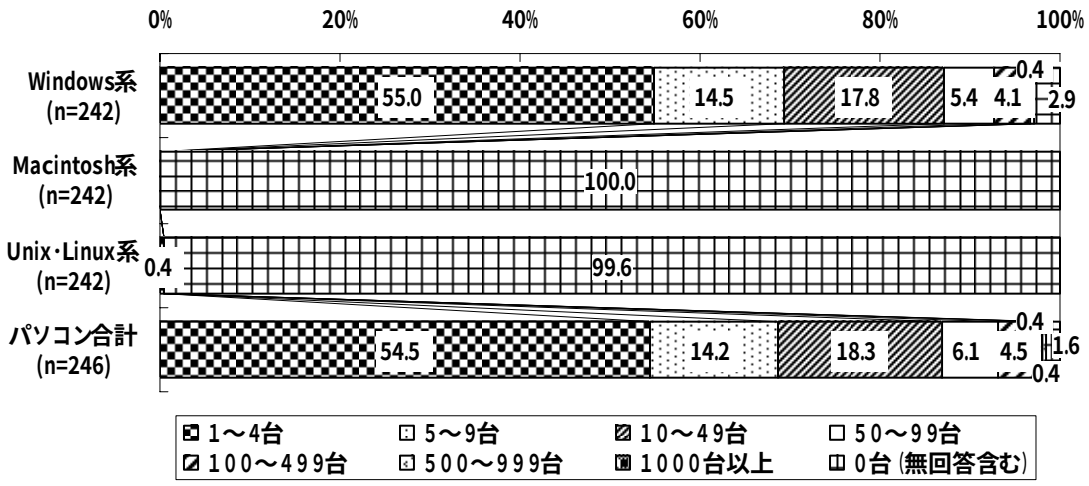
(%)

	n	感染前に駆除したため被害なし	パソコンに感染	無回答
全体	783	51.2	31.4	17.4
民間企業	375	41.9	37.3	20.8
自治体	408	59.8	26.0	14.2

図表 2.3.5_④-b　感染したパソコンのＯＳ



図表 2.3.5_④-c　感染したパソコンのＯＳと台数



図表 2.3.5_④-d　感染したパソコンのＯＳと台数（自治体との比較）

(Windows系)

(%)

	n	1～4台	5～9台	10～49台	50～99台	100～499台	500～999台	1000台以上	0台 (無回答含む)
全体	242	55.0	14.5	17.8	5.4	4.1	0.4	-	2.9
民間企業	136	59.6	14.7	15.4	5.9	2.2	-	-	2.2
自治体	106	49.1	14.2	20.8	4.7	6.6	0.9	-	3.8

(Macintosh系)

(%)

	n	1～4台	5～9台	10～49台	50～99台	100～499台	500～999台	1000台以上	0台 (無回答含む)
全体	242	-	-	-	-	-	-	-	100.0
民間企業	136	-	-	-	-	-	-	-	100.0
自治体	106	-	-	-	-	-	-	-	100.0

(Unix／Linux系)

(%)

	n	1～4台	5～9台	10～49台	50～99台	100～499台	500～999台	1000台以上	0台 (無回答含む)
全体	242	0.4	-	-	-	-	-	-	99.6
民間企業	136	-	-	-	-	-	-	-	100.0
自治体	106	0.9	-	-	-	-	-	-	99.1

(パソコン合計)

(%)

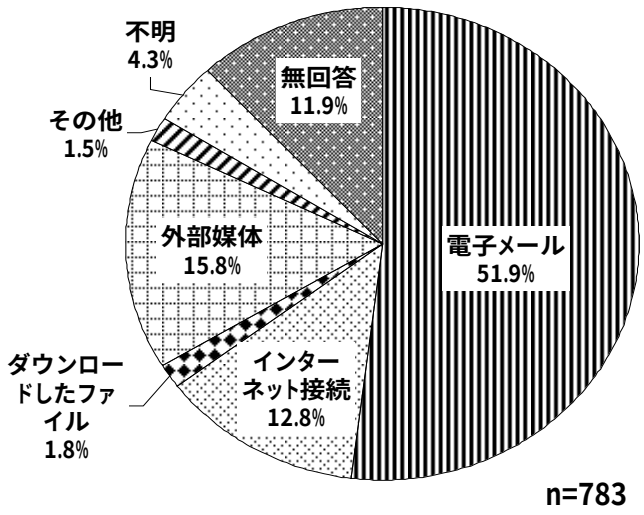
	n	1～4台	5～9台	10～49台	50～99台	100～499台	500～999台	1000台以上	0台 (無回答含む)
全体	246	54.5	14.2	18.3	6.1	4.5	0.4	0.4	1.6
民間企業	140	57.9	13.6	15.7	7.1	2.1	-	0.7	2.9
自治体	106	50.0	15.1	21.7	4.7	7.5	0.9	-	-

⑤　感染・発見経路

感染・発見経路については、「電子メール」が 51.9%と半数以上を占めており、次いで「外部媒体」（15.8%）、「インターネット接続」（12.8%）、「ダウンロードしたファイル」（1.8%）の順となっている。

民間企業と自治体を比較すると、民間企業では、「電子メール」に次いで「インターネット接続」の割合が高くなっているのに対して、自治体では、「外部媒体」からの感染や発見が多いのが特徴的である。

図表 2.3.5_⑤-a　**感染・発見経路**



その他　：　社内ネットワーク（5 件）、　など

図表 2.3.5_⑤-b　**感染・発見経路（自治体との比較）**

(%)

	n	電子メール	インターネット接続	ダウンロードしたファイル	外部媒体	その他	不明	無回答
全体	783	51.9	12.8	1.8	15.8	1.5	4.3	11.9
民間企業	375	53.6	16.0	2.9	9.3	0.5	5.6	12.0
自治体	408	50.2	9.8	0.7	21.8	2.5	3.2	11.8

2. 4　コンピュータウイルス対策の現状

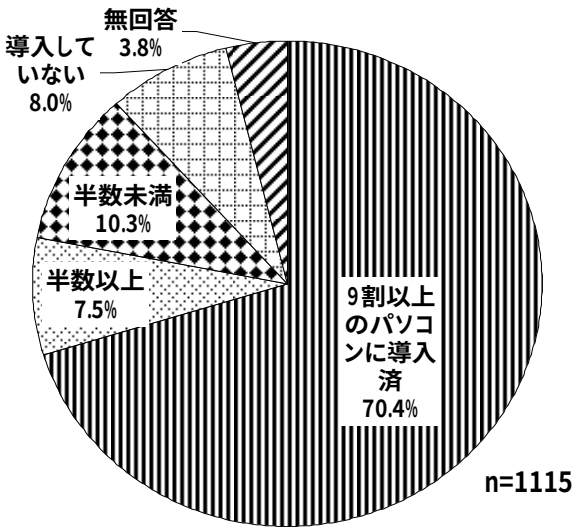
2. 4. 1　ウイルス対策ソフトの導入状況

①　クライアントマシン

クライアントマシンへのウイルス対策ソフト導入状況については、「9 割以上のパソコンに導入」が 70.4%を占め、次いで、「半数未満のパソコンに導入」（10.3%）、「導入していない」（8.0%）、「半数以上のパソコンに導入」（7.5%）の順となっている。

民間企業と自治体を比較すると、自治体では、「9 割以上のパソコンに導入」の割合がほぼ 9 割に達し、民間企業より 32.6 ポイントも高くなっている。

図表 2.4.1_①-a　**クライアントマシン**



図表 2.4.1_①-b　**クライアントマシン（自治体との比較）**

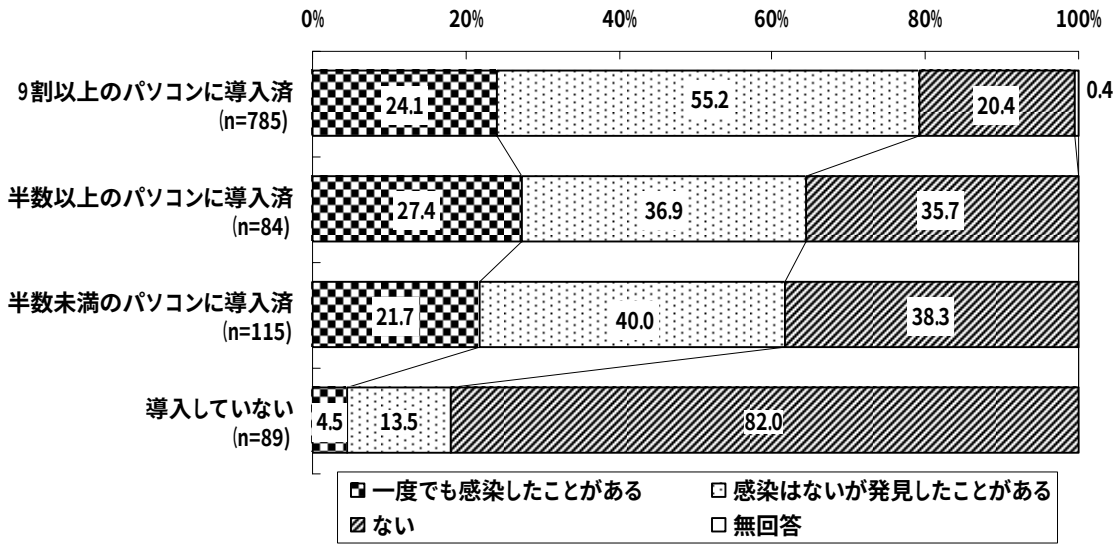
(%)

	n	9割以上のパソコンに導入済	半数以上のパソコンに導入済	半数未満のパソコンに導入済	導入していない	無回答
全体	1115	70.4	7.5	10.3	8.0	3.8
民間企業	651	56.8	10.1	14.0	12.6	6.5
自治体	464	89.4	3.9	5.2	1.5	-

クライアントマシンへのウイルス対策ソフト導入状況と、コンピュータウイルス遭遇経験とのクロス結果をみると、遭遇率（「一度でも感染したことがある」＋「感染はないが発見したことがある」）が高い程、ソフトの導入率が高くなる傾向がみられる。

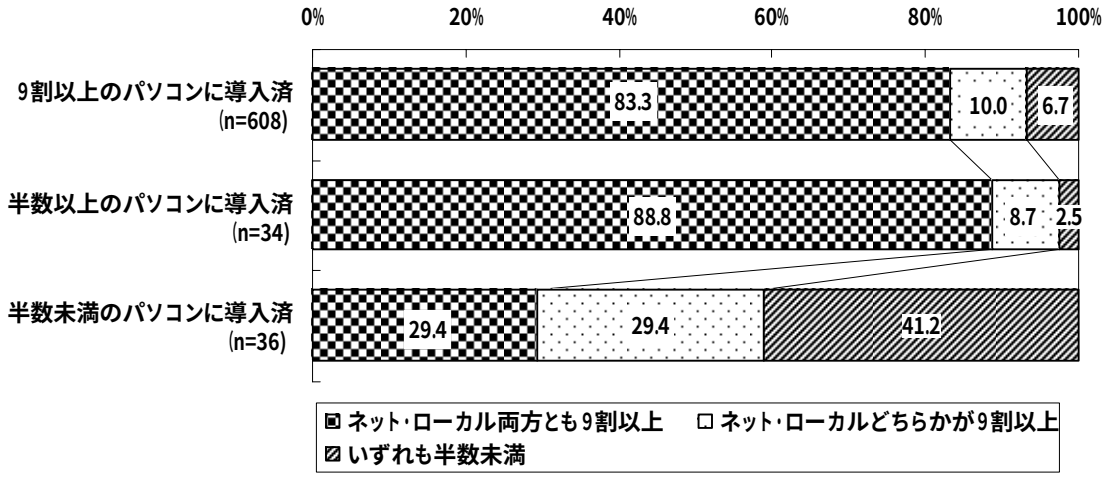
「９割以上のパソコンに導入済」では、「感染はないが発見したことがある」が過半数を占めており、クライアントマシンへのウイルスソフト導入が、感染を未然に防ぐため有効であることを示唆している。

図表 2.4.1_①-c　**クライアントマシン**
（コンピュータウイルス遭遇経験の有無別）



クライアントマシンへのウイルス対策導入状況と、ネットワークサーバー、ローカルサーバーへのウイルス対策ソフト導入状況とのクロス結果をみると、「９割以上のパソコンに導入済」、「半数以上のパソコンに導入済」では、「ネット・ローカル両方とも 9 割以上」が 8 割を超えている。これに対して、「半数未満のパソコンに導入済」では、「ネット・ローカル両方とも 9 割以上」が３割に満たず、「いずれも半数未満」の比率が最も高くなっている。

図表 2.4.1_①-d　**クライアントマシン**
（ネットワークサーバー、ローカルサーバーへの対策ソフト導入別）

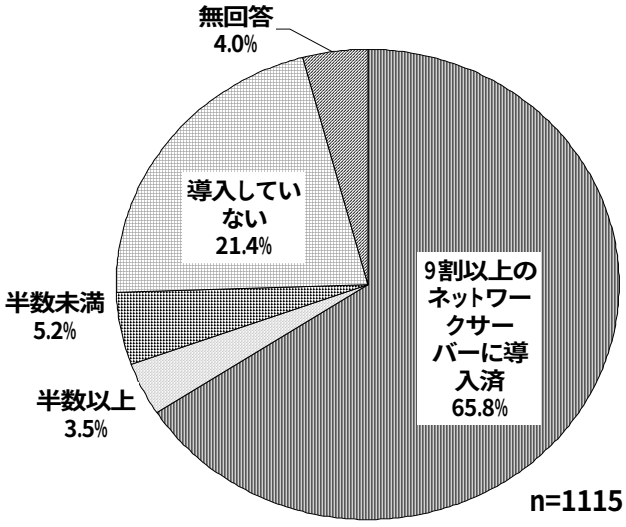


②　ネットワークサーバー

ネットワークサーバーへのウイルス対策ソフト導入状況については、「9 割以上のネットワークサーバーに導入済」が 65.8％を占め最も多くなっているが、「導入していない」（21.4％）も２割を超えている。

民間企業と自治体を比較すると、「9 割以上のネットワークサーバーに導入」の比率は、自治体が民間企業を約 30 ポイント上回っている。一方、民間企業では、「導入していない」が 3 割を超えており、ウイルス対策ソフトの導入状況については、自治体との間に差がみられる。

図表 2.4.1_②-a　**ネットワークサーバー**



図表 2.4.1_②-b　**ネットワークサーバー（自治体との比較）**

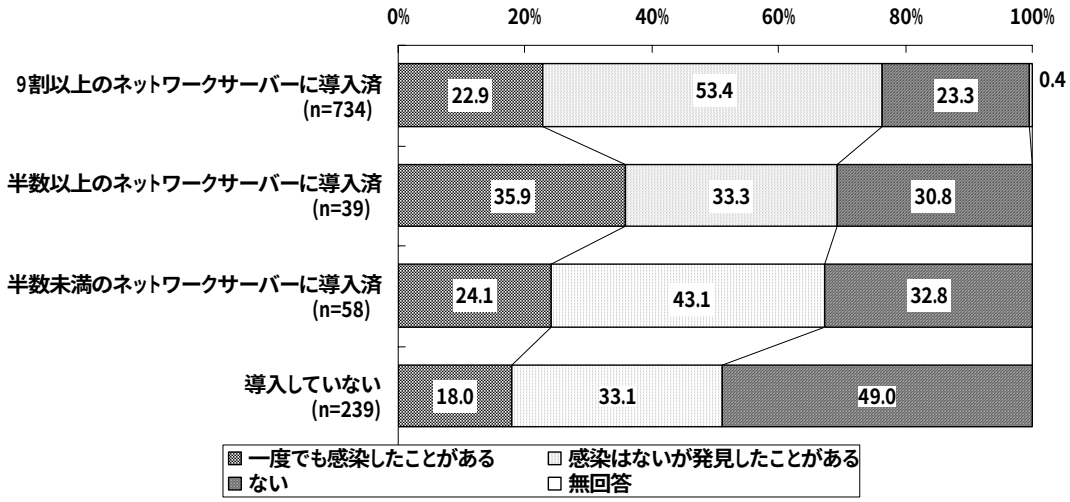
(%)

	n	9割以上のネットワークサーバーに導入済	半数以上のネットワークサーバーに導入済	半数未満のネットワークサーバーに導入済	導入していない	無回答
全体	1115	65.8	3.5	5.2	21.4	4.0
民間企業	651	53.1	3.4	6.9	31.6	4.9
自治体	464	83.6	3.7	2.8	7.1	2.8

ネットワークサーバーへのウイルス対策ソフト導入状況と、コンピュータウイルス遭遇経験とのクロス結果をみると、遭遇率（「一度でも感染したことがある」＋「感染はないが発見したことがある」）が高い程、ソフトの導入率が高くなる傾向がみられる。

また、「９割以上のネットワークサーバーに導入済」では、「感染はないが発見したことがある」が過半数を占めており、ネットワークサーバーへのウイルスソフト導入が、感染を未然に防ぐため有効であることを示唆している。

図表 2.4.1_②-c　**ネットワークサーバー**
（コンピュータウイルス遭遇経験の有無別）

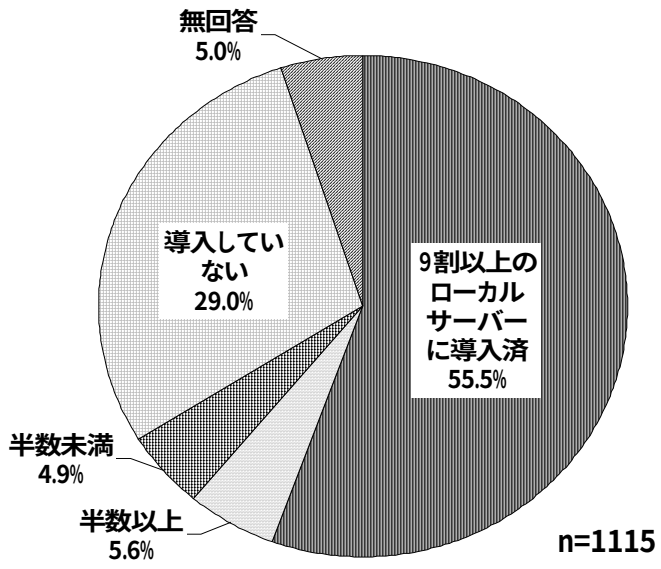


③　ローカルサーバー

ローカルサーバーへのウイルス対策ソフト導入状況については、「9 割以上のローカルサーバーに導入済」（55.5%）が半数以上を占めたものの、「導入していない」（29.0%）が３割近くにのぼった。

民間企業と自治体を比較すると、「9 割以上のローカルサーバーに導入」は、自治体が７割を占めているのに対して、民間企業では半数に満たない。また、民間企業では、「導入していない」がほぼ４割に達しており、ウイルス対策ソフトの導入については、自治体との間に差がみられる。

図表 2.4.1_③-a　**ローカルサーバー**



図表 2.4.1_③-b　**ローカルサーバー（自治体との比較）**

(%)

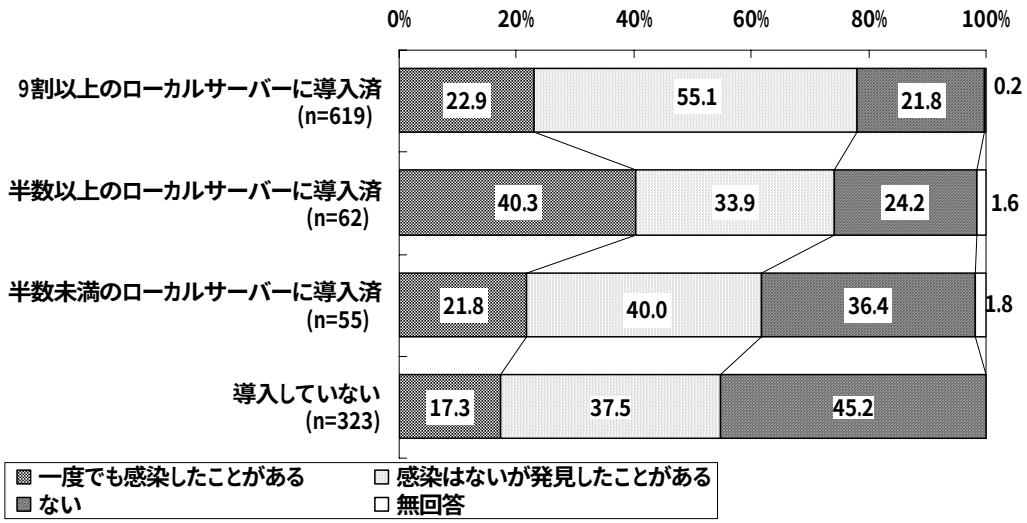
	n	9割以上のローカルサーバーに導入済	半数以上のローカルサーバーに導入済	半数未満のローカルサーバーに導入済	導入していない	無回答
全体	1115	55.5	5.6	4.9	29.0	5.0
民間企業	651	44.5	4.8	5.7	39.3	5.7
自治体	464	70.9	6.7	3.9	14.4	4.1

ローカルサーバーへのウイルス対策ソフト導入状況と、コンピュータウイルス遭遇経験とのクロス結果をみると、遭遇率（「一度でも感染したことがある」＋「感染はないが発見したことがある」）が高い程、ソフトの導入率が高くなる傾向がみられる。

「半数以上のローカルサーバーに導入済」では、「一度でも感染したことがある」が４割にのぼり、他に比べ感染率が高くなっている。

また、「９割以上のローカルサーバーに導入済」では、「感染はないが発見したことがある」が過半数を占めており、ローカルサーバーへのウイルスソフト導入が、感染を未然に防ぐため有効であることを示唆している。

図表 2.4.1_③-c　**ローカルサーバー**
（コンピュータウイルス遭遇経験の有無別）



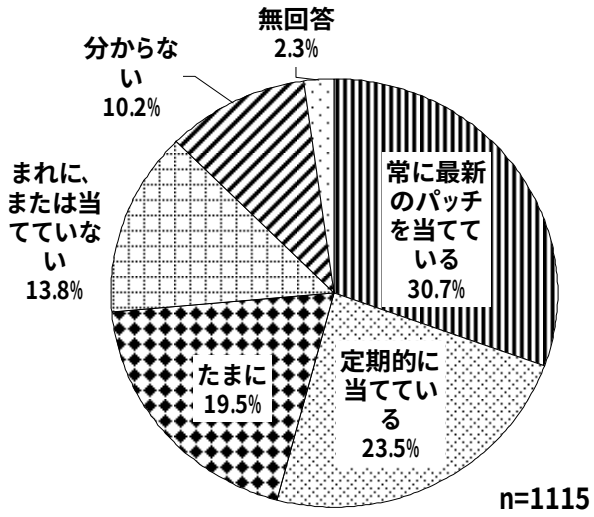
2. 4. 2　セキュリティパッチの適用頻度

①　クライアントマシン

クライアントマシンについては、「常に最新のパッチを当てている」が 30.7%と最も多く、次いで「定期的に当てている」（23.5%）、「たまに」（19.5%）、「まれに、または当てていない」（13.8%）の順となっている。

民間企業と自治体を比較すると、自治体では、「常に最新のパッチを当てている」と「定期的に当てている」とを合わせた比率が６割を占め、民間企業を 10.5 ポイント上回っている。

図表 2.4.2_①-a　**クライアントマシン**



図表 2.4.2_①-b　**クライアントマシン（自治体との比較）**

(%)

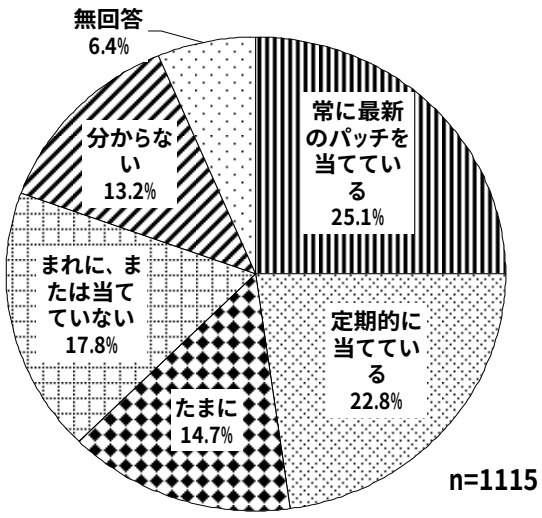
	n	常に最新のパッチを当てている	定期的に当てている	たまに	まれに、または当てていない	分からない	無回答
全体	1115	30.7	23.5	19.5	13.8	10.2	2.3
民間企業	651	28.6	21.2	17.2	14.6	15.1	3.4
自治体	464	33.6	26.7	22.6	12.7	3.4	0.9

② ローカルサーバー

ローカルサーバーについては、「常に最新のパッチを当てている」が 25.1%と最も多く、次いで「定期的に当てている」（22.8%）、「まれに、または当てていない」（17.8%）、「たまに」（14.7%）の順となっている。

民間企業と自治体を比較すると、自治体では、「常に最新のパッチを当てている」と「定期的に当てている」とを合わせた比率が６割を占め、民間企業より 22.0 ポイント高くなっている。

図表 2.4.2_②-a **ローカルサーバー**



図表 2.4.2_②-b **ローカルサーバー（自治体との比較）**

(%)

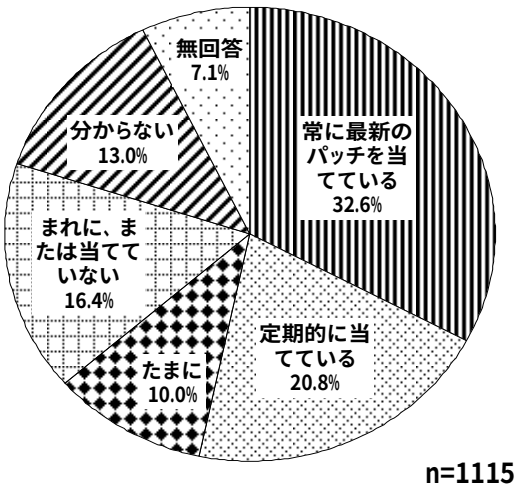
	n	常に最新のパッチを当てている	定期的に当てている	たまに	まれに、または当てていない	分からない	無回答
全体	1115	25.1	22.8	14.7	17.8	13.2	6.4
民間企業	651	21.8	16.9	14.1	20.4	18.9	7.8
自治体	464	29.7	31.0	15.5	14.2	5.2	4.3

③　ネットワークサーバー

ネットワークサーバーについては、「常に最新のパッチを当てている」が 32.6%と最も多く、次いで「定期的に当てている」（20.8%）、「まれに、または当てていない」（16.4%）、「たまに」（10.0%）の順となっている。

民間企業と自治体を比較すると、自治体では、「常に最新のパッチを当てている」と「定期的に当てている」とを合わせた割合が 76.0%を占め、民間企業を 38.7 ポイント上回っている。一方、民間企業では、「まれに、または当てていない」が 23.0%と高くなっている。

図表 2.4.2_③-a　**ネットワークサーバー**



図表 2.4.2_③-b　**ネットワークサーバー（自治体との比較）**

(%)

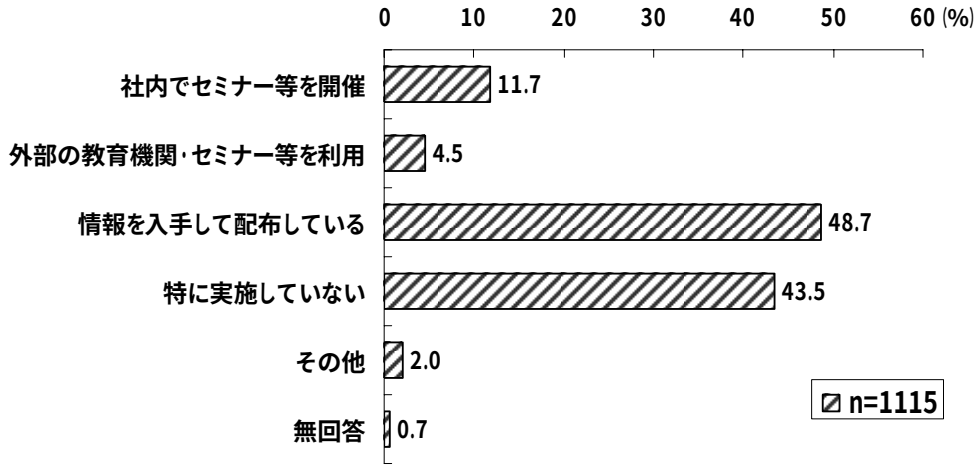
	n	常に最新のパッチを当てている	定期的に当てている	たまに	まれに、または当てていない	分からない	無回答
全体	1115	32.6	20.8	10.0	16.4	13.0	7.1
民間企業	651	24.9	12.4	9.8	23.0	20.6	9.2
自治体	464	43.5	32.5	10.3	7.1	2.4	4.1

2.4.3　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については、「情報を入手して配布している」が 48.7%と最も多く、次いで、「特に実施していない」(43.5%)、「社内でセミナー等を開催」(11.7%)、「外部の教育機関・セミナー等を利用」(4.5%)が続いている。

民間企業と自治体を比較すると、自治体では、特に、「情報を入手して配布している」(64.4%)、「社内でセミナー等を開催」(23.3%)の比率が民間企業より高くなっており、積極的にユーザ教育を行っている様子がうかがえる。逆に、民間企業では、「特に実施していない」(57.0%)の比率が高くなっている。

図表 2.4.3-a　ウイルス対策に関するユーザ教育



※複数回答設問

その他　：　適宜、口頭などで（6 件)、随時に通達（2 件)、
ウイルス対策ソフトのインストール（2 件)、　など

図表 2.4.3-b　ウイルス対策に関するユーザ教育（自治体との比較）

(%)

	n	社内でセミナー等を開催	外部の教育機関･セミナー等を利用	情報を入手して配布している	特に実施していない	その他	無回答
全体	1115	11.7	4.5	48.7	43.5	2.0	0.7
民間企業	651	3.5	1.1	37.5	57.0	2.3	1.2
自治体	464	23.3	9.3	64.4	24.6	1.5	-

※複数回答設問

ユーザ教育とコンピュータウイルスの遭遇経験とのクロスをみると、「一度でも感染したことがある」では、「情報を入手して配布している」（63.2%）が他より高いのに対して、「感染はないが発見したことがある」では、「社内でセミナー等を開催」（16.3%）、「外部の教育機関・セミナー等を利用」（6.2%）が他よりも高くなっている。

また、コンピュータウイルスの遭遇経験が「ない」事業所では、「特に実施していない」が約７割に達している。

図表 2.4.3-c　**ウイルス対策に関するユーザ教育**
（コンピュータウイルス遭遇経験の有無とのクロス）

(%)

	n	社内でセミナー等を開催	外部の教育機関・セミナー等	情報を入手して配布している	特に実施していない	その他	無回答
全体	1115	11.7	4.5	48.7	43.5	2.0	0.7
一度でも感染したことがある	247	15.0	2.8	63.2	30.8	1.6	0.0
感染はないが発見したことがある	529	16.3	6.2	57.5	33.5	2.1	0.0
ない	332	2.1	3.0	24.4	69.6	2.1	1.5

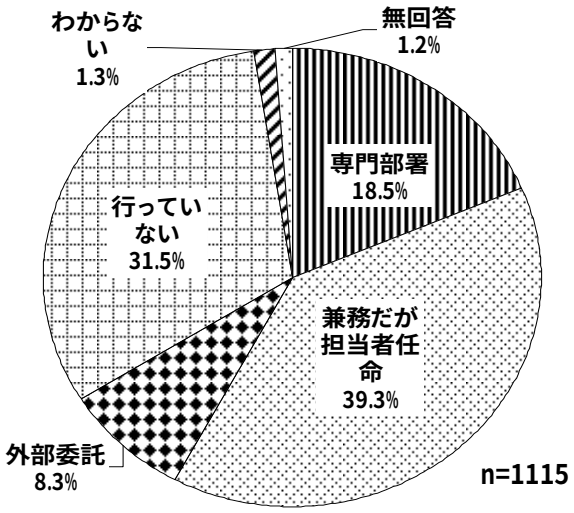
※複数回答設問

2. 4. 4　ウイルス対策の管理体制

ウイルス対策の管理体制については、「兼務だが担当者が任命されている」が 39.3%と最も高く、「専門部署（担当者）がある」（18.5%）と合わせると 57.8%が組織的な管理を実施している。一方、「行っていない」は 31.5%となっている。

民間企業と自治体を比較すると、組織的な管理を実施している（「専門部署（担当者）がある」＋「兼務だが担当者が任命されている」）割合は、自治体（77.8%）が民間企業（43.5%）より 34.3 ポイント高くなっている。

図表 2.4.4-a　**ウイルス対策の管理体制**



図表 2.4.4-b　**ウイルス対策の管理体制（自治体との比較）**

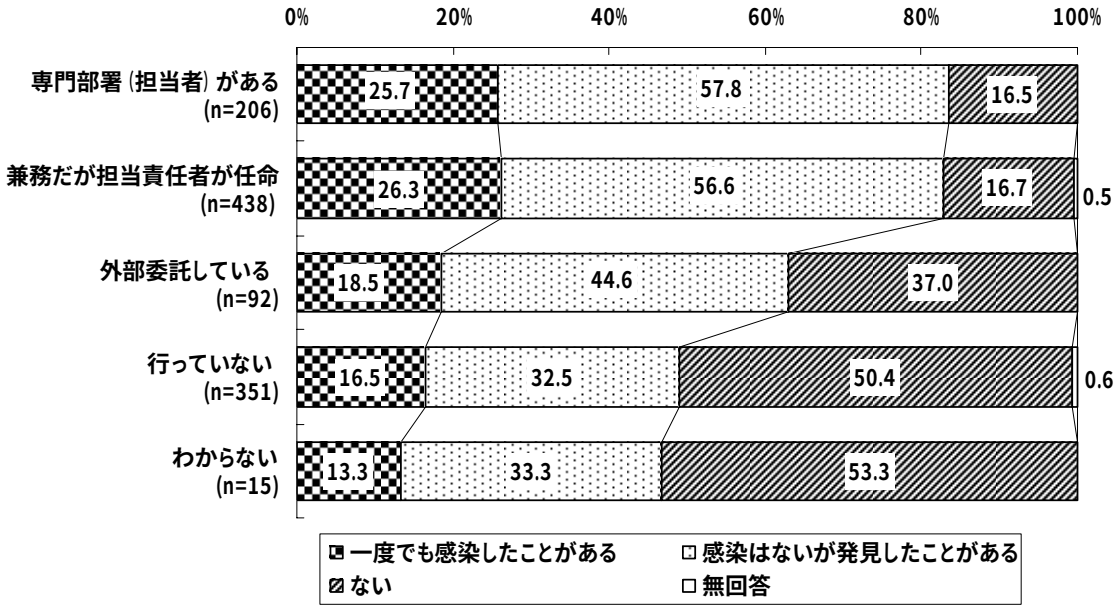
(%)

	n	専門部署（担当者）がある	兼務だが担当責任者が任命	外部委託している	行っていない	わからない	無回答
全体	1115	18.5	39.3	8.3	31.5	1.3	1.2
民間企業	651	12.0	31.5	8.6	44.4	1.7	1.8
自治体	464	27.6	50.2	7.8	13.4	0.9	0.2

ウイルス対策管理体制とコンピュータウイルスの遭遇経験とのクロス結果をみると、遭遇率（「一度でも感染したことがある」＋「感染はないが発見したことがある」）が高い程、ウイルス対策管理体制が整備されている。

また、「専門部署（担当者）がある」、「兼務だが担当者が任命されている」では、「感染はないが発見したことがある」の割合が半数以上を占めており、ウイルス対策管理体制の整備が、感染を未然に防ぐため有効であることを示唆している。

図表 2.4.4-c　ウイルス対策管理体制（コンピュータウイルス遭遇経験別）



ウイルス対策の管理体制と、コンピュータウイルスに関して知りたい情報のクロス結果をみると、「専門部署（担当者）がある」や「兼務だが担当責任者が任命されている」では、「外部委託している」や「行っていない」と比べて、「しくみ・種類等の技術的内容」、「ウイルスが引き起こす発病内容」、「国内のウイルス被害の状況」、「新種ウイルスの情報」など、より実際的な情報についての比率が高くなっている。

図表 2.4.4-d　**ウイルス対策の管理体制**
（コンピュータウイルスに関して知りたい情報別）

(%)

	n	しくみ・種類等の技術的内容	感染した時の復旧方法	感染しないための方法や対策	ウイルス対策ソフト情報	ウイルスが引き起こす発病内容	国内のウイルス被害の状況
全体	1115	25.4	63.3	61.9	22.9	31.5	15.8
専門部署（担当者）がある	206	25.7	57.8	59.7	26.2	35.0	18.4
兼務だが担当責任者が任命	438	27.6	63.5	60.5	22.6	33.6	19.2
外部委託している	92	23.9	63.0	65.2	13.0	28.3	16.3
行っていない	351	23.4	66.4	65.0	24.8	27.6	10.0
わからない	15	20.0	86.7	60.0	20.0	40.0	26.7

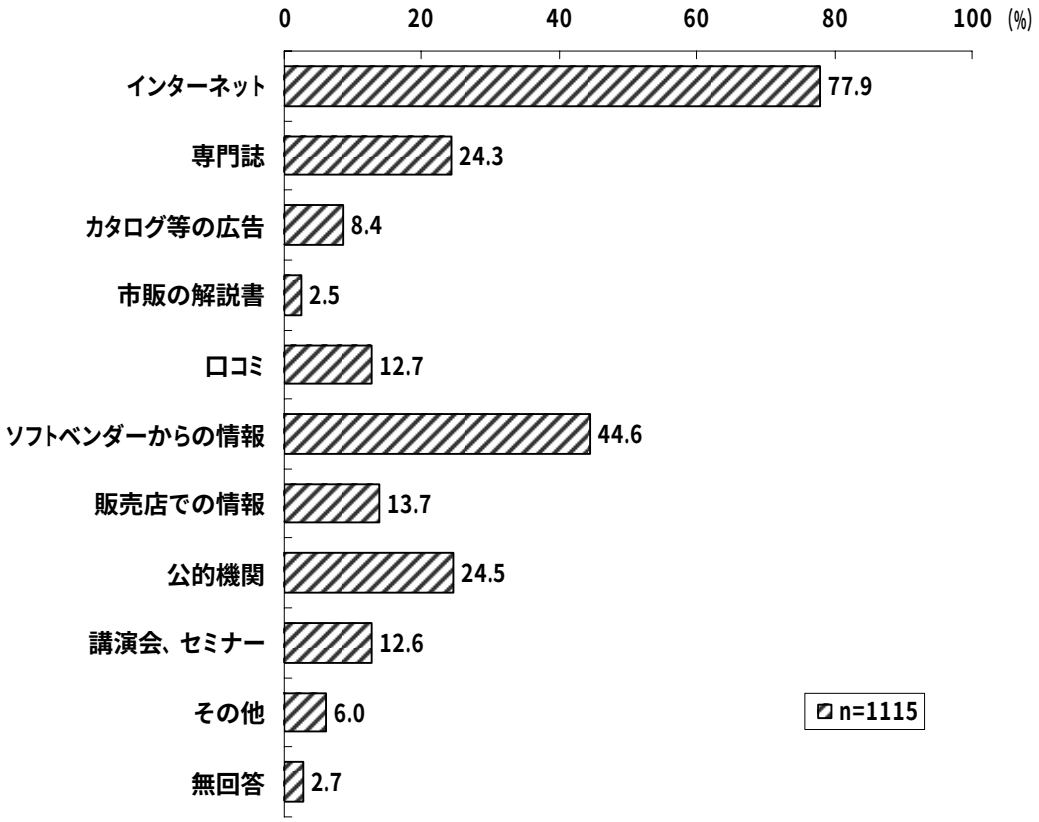
	n	海外のウイルス被害の状況	要注意ウイルスの警戒情報	新種ウイルスの情報	その他	特にない	無回答
全体	1115	5.7	39.7	45.7	1.3	9.4	2.0
専門部署（担当者）がある	206	7.3	47.1	54.9	2.9	10.2	1.5
兼務だが担当責任者が任命	438	6.8	45.0	55.5	1.8	6.2	0.7
外部委託している	92	6.5	45.7	43.5	-	12.0	2.2
行っていない	351	3.1	28.8	30.5	-	12.8	2.0
わからない	15	6.7	20.0	33.3	-	-	6.7

2.4.5　ウイルス対策ソフトに関する情報源

ウイルス対策ソフトに関する情報源については、「インターネット」が 77.9%と最も多く、次いで「ソフトベンダーからの情報」（44.6%）、「公的機関」（24.5%）、「専門誌」（24.3%）、「販売店での情報」（13.7%）などが続いている。

民間企業と自治体を比較すると、「公的機関」、「ソフトベンダーからの情報」において自治体が民間企業を大きく上回っている。これに対して、民間企業では、「口コミ」、「販売店での情報」の割合が自治体よりも高くなっている。

図表　2.4.5-a　ウイルス対策ソフトに関する情報源



※複数回答設問

その他　：　本社・本庁より（13 件）、社内の他部署より（10 件）、
外部業者・関連機関より（10 件）、
テレビ・新聞などのマスコミより（4 件）、　など

図表　2.4.5-b　ウイルス対策ソフトに関する情報源（自治体との比較）

(%)

	n	インターネット	専門誌	カタログ等の広告	市販の解説書	口コミ	ソフトベンダーからの情報
全体	1115	77.9	24.3	8.4	2.5	12.7	44.6
民間企業	651	71.0	22.7	7.1	2.6	17.1	30.4
自治体	464	87.7	26.5	10.3	2.4	6.7	64.4

	n	販売店での情報	公的機関	講演会、セミナー	その他	無回答
全体	1115	13.7	24.5	12.6	6.0	2.7
民間企業	651	16.4	6.9	9.1	8.6	4.0
自治体	464	9.9	49.1	17.7	2.4	0.9

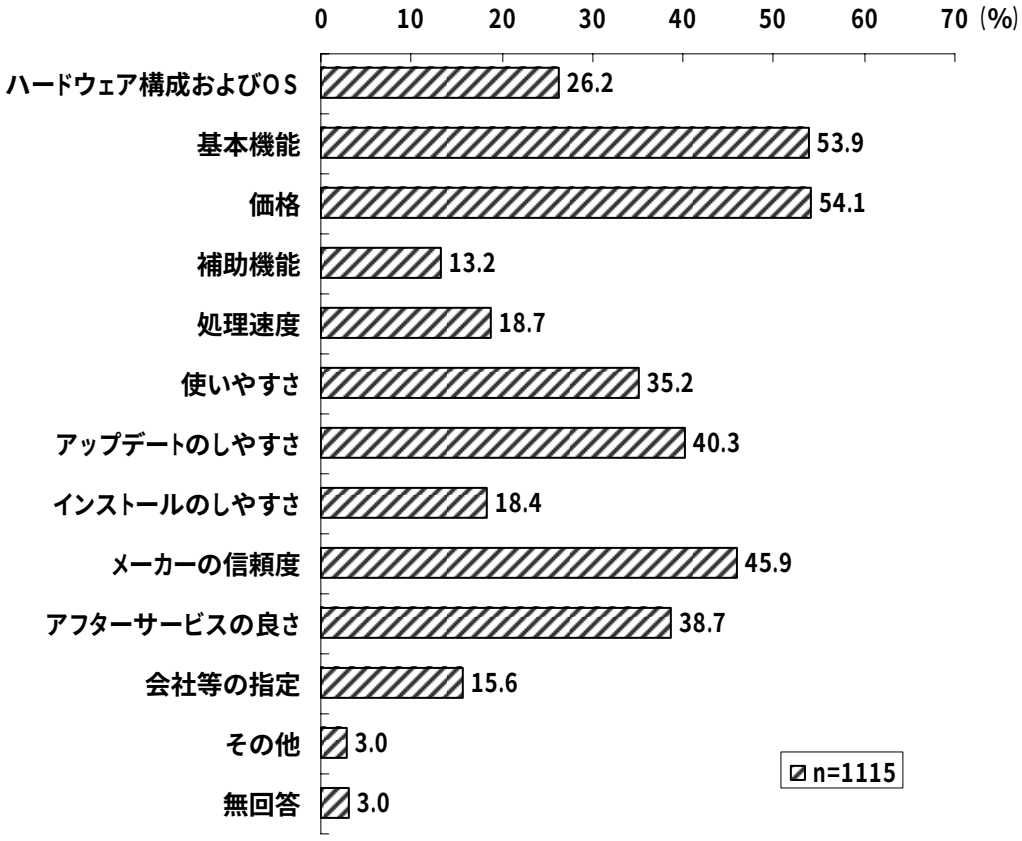
※複数回答設問

2.4.6　ウイルス対策ソフトの選択基準

ウイルス対策ソフトの選択基準については、「価格」（54.1%）が最も多く、次いで、「基本機能（予防、発見、修復）」（53.9%）、「メーカーの信頼度」（45.9%）、「アップデートのしやすさ」（40.3%）、「アフターサービスの良さ」（38.7%）の順となっている。

民間企業と自治体を比較すると、特に、「アップデートのしやすさ」、「メーカーの信頼度」において、大きく民間企業を上回っている。また民間企業に比べ自治体の方が、大半の選択基準で高い。

図表 2.4.6-a　ウイルス対策ソフトの選択基準



※複数回答設問

その他　：　販売店や保守業務の推奨（9 件）、システムの安定度（4 件）、
管理のしやすさ（2 件）、本社の指定（2 件）　など

図表 2.4.6-b　ウイルス対策ソフトの選択基準（自治体との比較）

(%)

	n	ハードウェア構成およびOS	基本機能（予防、発見、修復）	価格	補助機能（履歴、ウイルス情報）	処理速度の速さ	使いやすさ	アップデートのしやすさ
全体	1115	26.2	53.9	54.1	13.2	18.7	35.2	40.3
民間企業	651	20.9	46.9	47.9	8.0	16.7	30.7	30.6
自治体	464	33.6	63.8	62.7	20.5	21.6	41.4	53.9

	n	インストールのしやすさ	メーカーの信頼度	アフターサービスの良さ	本社またはグループ会社等の指定	その他	無回答
全体	1115	18.4	45.9	38.7	15.6	3.0	3.0
民間企業	651	16.1	37.9	34.1	18.4	3.2	4.9
自治体	464	21.6	57.1	45.0	11.6	2.6	0.4

※複数回答設問

2. 4. 7　ウイルス対策ソフトの導入・管理体制の強化

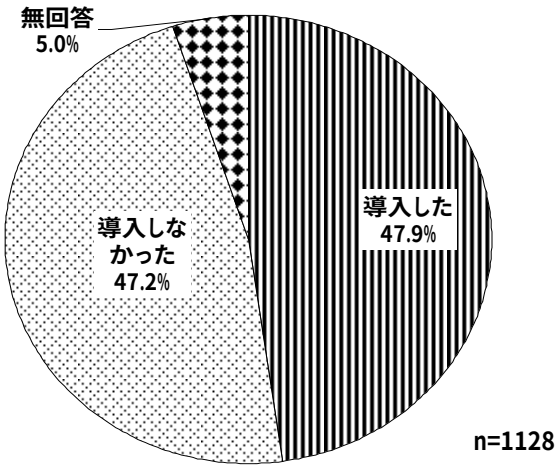
国内で新型ウイルス「W32/MSBlaster(W32/Lovsan)」が猛威を振るった 2003 年 8 月以降、ウイルス対策ソフトの導入や管理体制の強化を行ったかどうかを尋ねた。

①　ウイルス対策ソフトの導入

ウイルス対策ソフトの導入については､「導入した」が 47.9%､「導入しなかった」が 47.2%となっており、ほぼ半々の結果となった。

民間企業と自治体を比較すると、「導入した」の割合は、自治体（52.0%）が民間企業（44.9%）より 7.1 ポイント高くなっている。

図表 2.4.7_①-a　**ウイルス対策ソフトの導入**



図表 2.4.7_①-b　**ウイルス対策ソフトの導入（自治体との比較）**

(%)

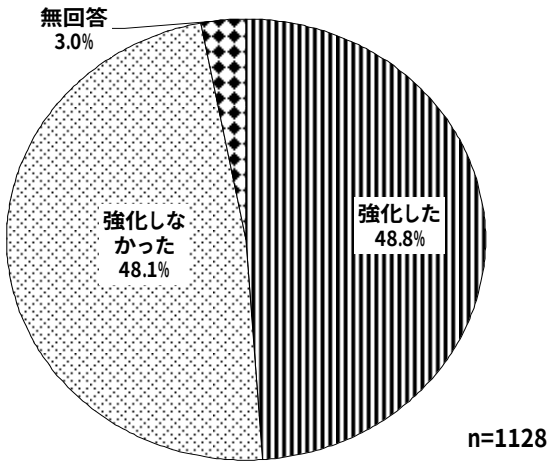
	n	導入した	導入しなかった	無回答
全体	1128	47.9	47.2	5.0
民間企業	663	44.9	50.7	4.4
自治体	465	52.0	42.2	5.8

②　管理体制の強化

管理体制の強化については、「強化した」が 48.8%、「強化しなかった」が 48.1%とほぼ等しくなっている。

民間企業と自治体を比較すると、自治体では「強化した」がほぼ６割を占めているのに対して、民間企業では４割程度となっている。

図表 2.4.7_②-a　**管理体制の強化**



図表 2.4.7_②-b　**管理体制の強化（自治体との比較）**

(%)

	n	強化した	強化しなかった	無回答
全体	1128	48.8	48.1	3.0
民間企業	663	41.2	55.4	3.5
自治体	465	59.8	37.8	2.4

2. 5　コンピュータウイルス対策の課題

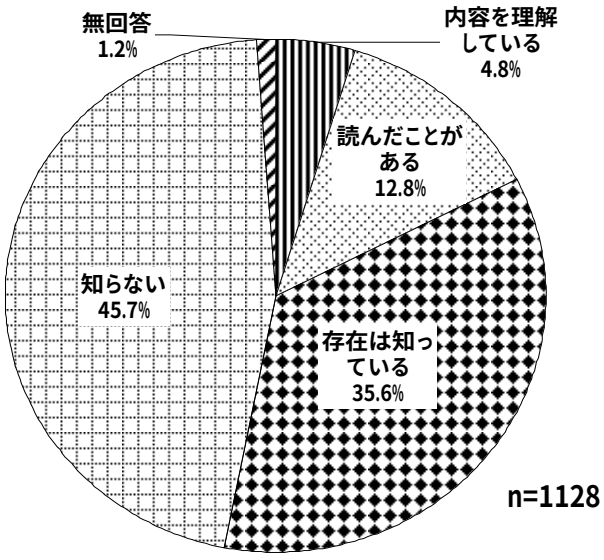
2. 5. 1　「コンピュータウイルス対策基準」の認知度

「コンピュータウイルス対策基準」の認知度については、「知らない」が 45.7%と最も多く、次いで、「存在は知っている」（35.6%）、「読んだことがある」（12.8%）、「内容を理解している」（4.8%）の順となっている。

自治体と民間企業を比較すると、民間企業で「知らない」の割合が 6 割に達しており、自治体に比べて 36.3 ポイント高くなっている。

過去からの推移をみると、前回調査に比べて「内容を理解している」、「読んだことがある」の比率が減少した。逆に、「知らない」の比率は 9.3 ポイント増加しており、「コンピュータウイルス対策基準」についてより一層の啓発活動が求められる。

図表 2.5.1-a　**「コンピュータウイルス対策基準」の認知度**

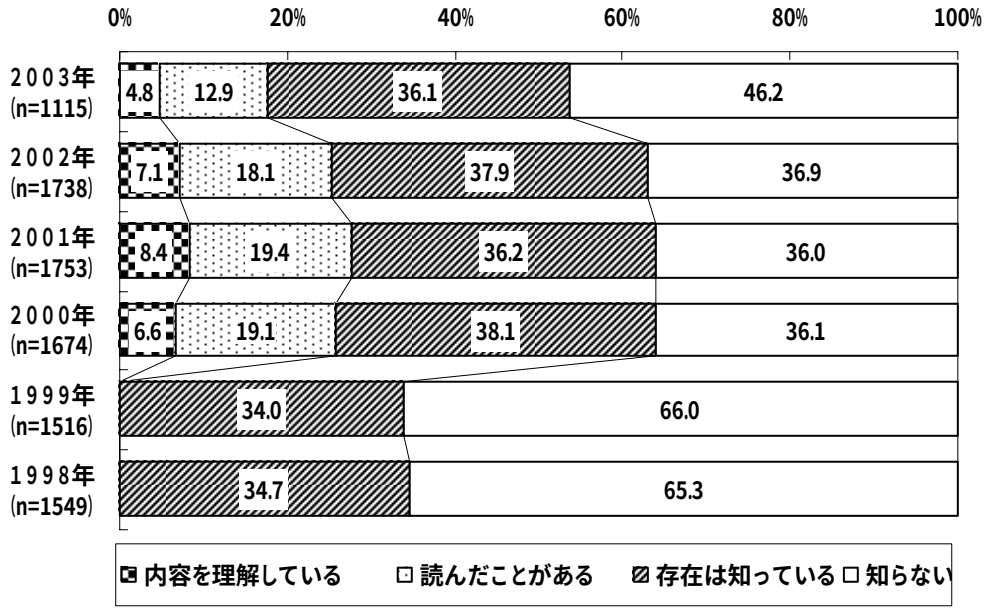


図表 2.5.1-b　**「コンピュータウイルス対策基準」の認知度（自治体との比較）**

(%)

	n	内容を理解している	読んだことがある	存在は知っている	知らない	無回答
全体	1128	4.8	12.8	35.6	45.7	1.2
民間企業	663	2.3	5.3	30.6	60.6	1.2
自治体	465	8.4	23.4	42.8	24.3	1.1

図表 2.5.1-c **「コンピュータウイルス対策基準」の認知度の推移（時系列）**

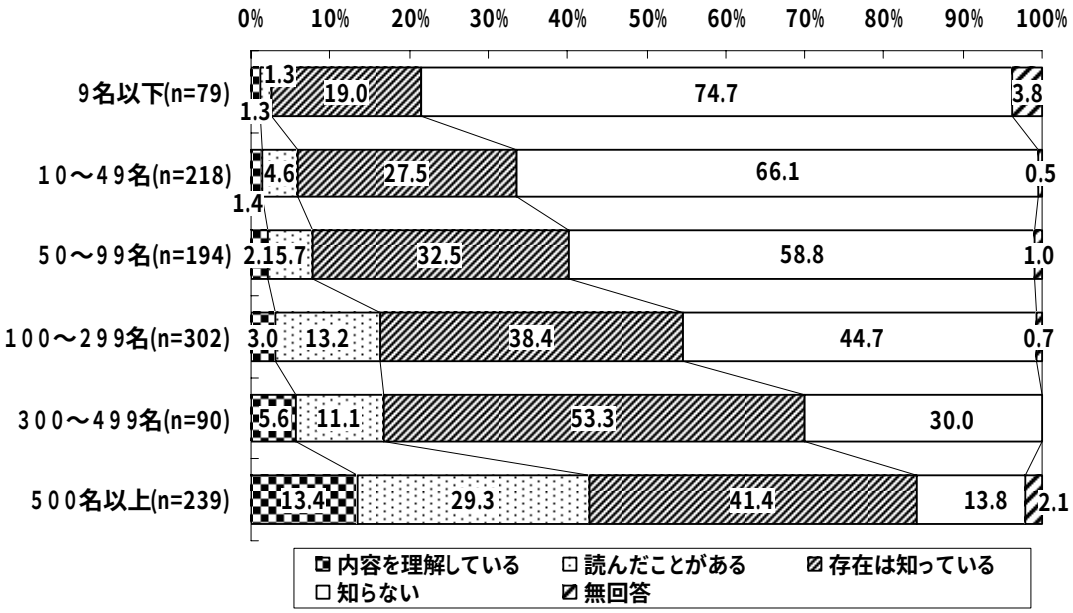


注１）1998 年～1999 年は、選択肢が「存在は知っている」「知らない」の 2 つであり、2000 年以降、選択肢が上記 4 つに細分化されている。

注２）時系列結果の比較のため、無回答を除いて 2003 年の値を再集計しており、前頁の比率と異なる。

就業者規模別にみると、「内容を理解している」の比率は、規模が大きくなる程高くなっている。また、「読んだことがある」、「存在は知っている」についてもほぼ同様の傾向がみられ、規模が大きい程、認知度も理解度も高くなっていることがわかる。逆に、「知らない」の割合は、事業所の規模が小さい程高くなっている。

図表 2.5.1-d**「コンピュータウイルス対策基準」の認知度（就業者規模別）**



2. 5. 2　被害届出について

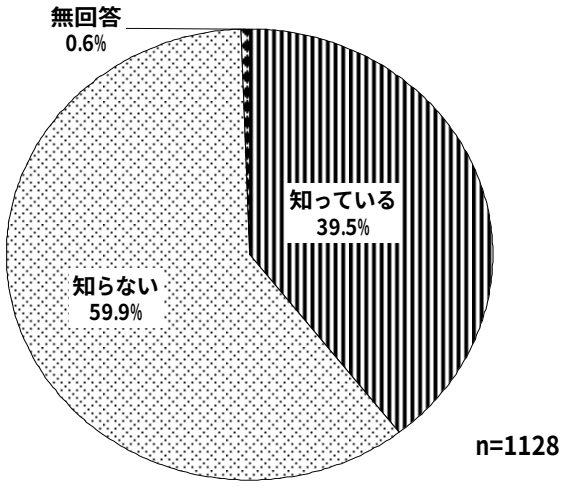
①　届出機関としての IPA の認知度

情報処理推進機構が経済産業省認定のコンピュータウイルス被害の届出機関となっていることに対する認知度については、「知らない」（59.9%）が約６割を占め、「知っている」（39.5%）が約４割となっている。

民間企業と自治体を比較すると、自治体では６割以上が「知っている」と回答しているのに対して、民間企業では「知らない」が７割を超えている。

過去からの推移をみると、「知っている」の割合は、2001 年まで増加が続いたが、前回調査から減少傾向に転じ、今回の調査では前回より 22.4 ポイント減少した。

図表 2.5.2_①-a　届出機関としての IPA の認知度

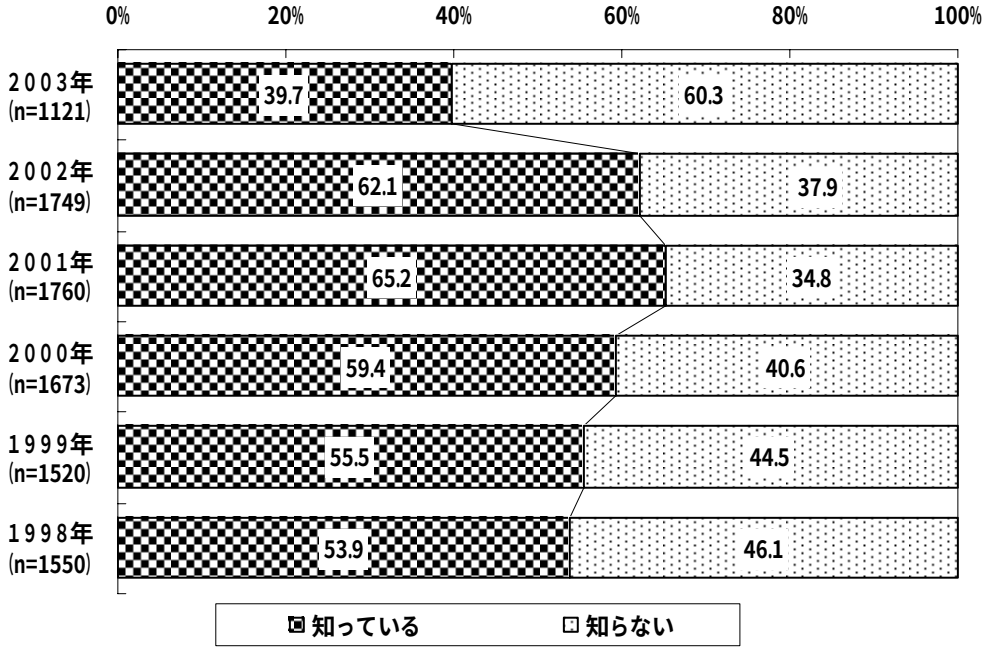


図表 2.5.2_①-b　届出機関としての IPA の認知度の推移（自治体との比較）

(%)

	n	知っている	知らない	無回答
全体	1128	39.5	59.9	0.6
民間企業	663	23.5	75.6	0.9
自治体	465	62.2	37.6	0.2

図表 2.5.2_①-c　届出機関としての IPA の認知度の推移（時系列）

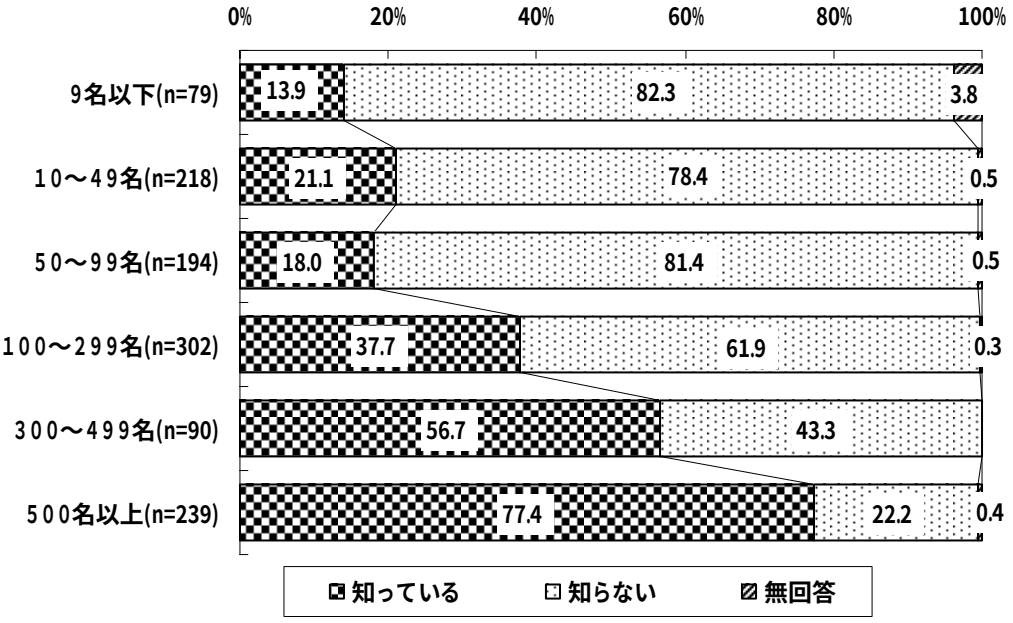


注）　時系列結果の比較のため、無回答を除いて 2003 年の値を再集計しており、前頁の比率と異なる。

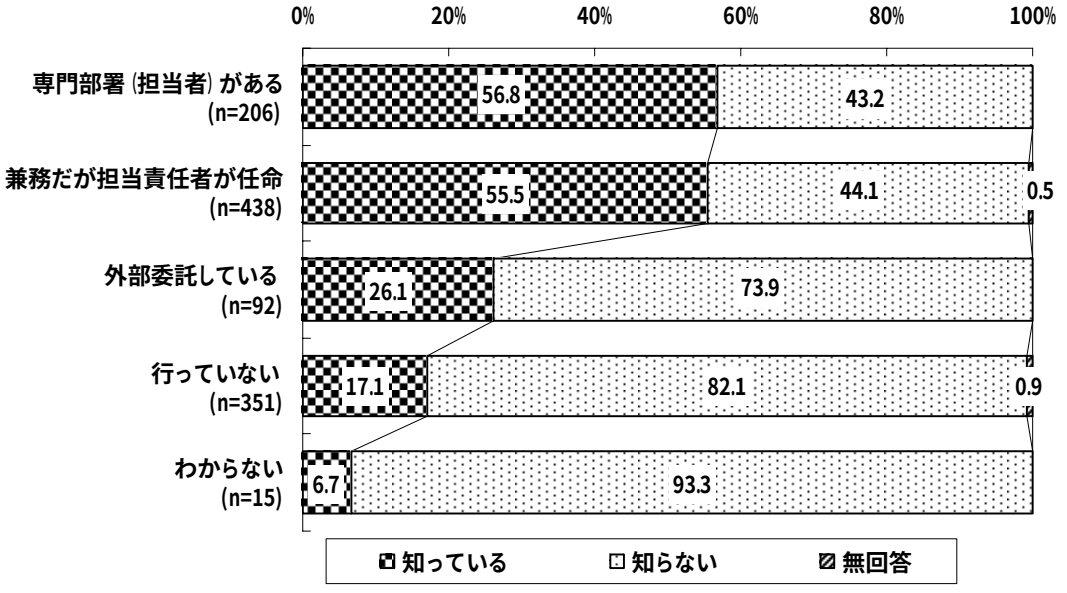
就業者規模別にみると、「10～49 人」において、「知っている」の比率がやや高いほかは、事業所の規模が大きくなる程、「知っている」の比率は高くなっている。

また、管理体制別にみると、「専門部署（担当者）がある」や「兼務だが担当責任者が任命されている」では、「知っている」が半数以上を占めており、他よりも認知度が高くなっている。

図表 2.5.2_①-d　届出機関としての IPA の認知度の推移（就業者規模別）



図表 2.5.2_①-e　届出機関としての IPA の認知度（ウイルス対策の管理体制別）



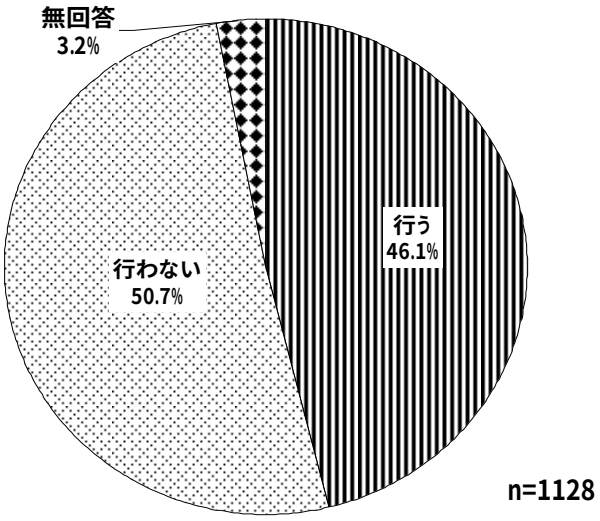
② 届出の実施

コンピュータウイルスの被害にあった際に届出を行うかどうかについては、「行う」が 46.1%、「行わない」が 50.7%であった。

民間企業では「行わない」が 57.8%を占めているのに対して、自治体では「行う」が 57.2%となっており、自治体においてより積極的な姿勢がみられる。

過去からの推移をみると、「行う」の比率は、前回調査に比べて 3.2 ポイント低くなった。

図表 2.5.2_②-a **届出の実施**

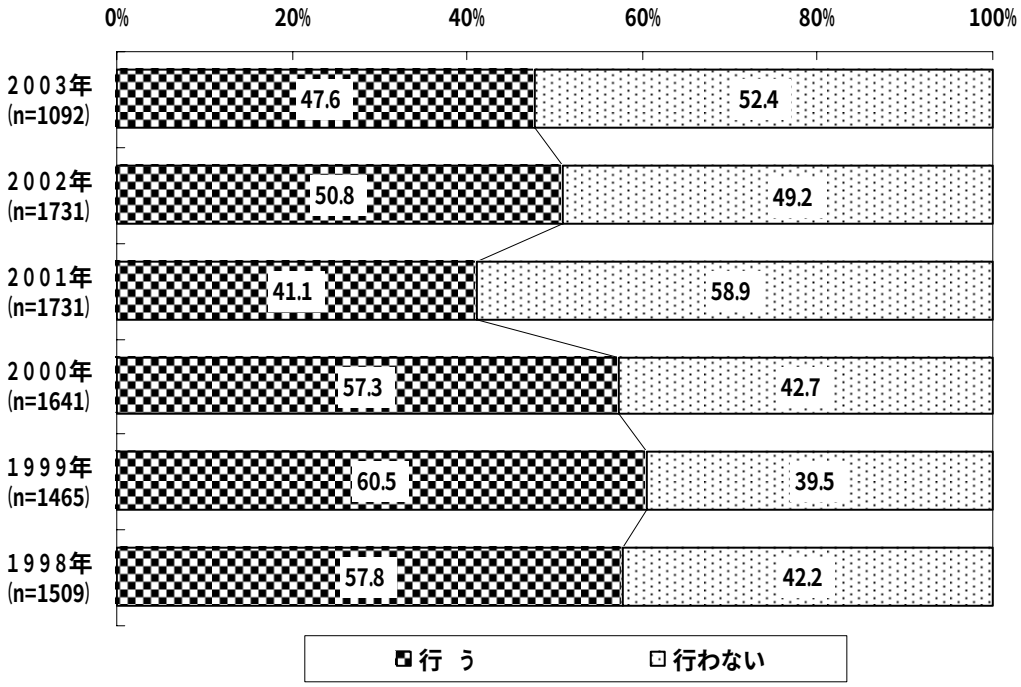


図表 2.5.2_②-b **届出の実施（自治体との比較）**

(%)

	n	行う	行わない	無回答
全体	1128	46.1	50.7	3.2
民間企業	663	38.3	57.8	3.9
自治体	465	57.2	40.6	2.2

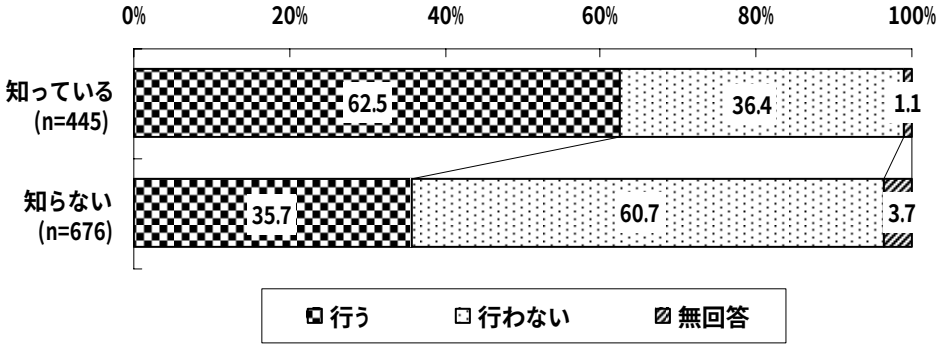
図表 2.5.2_②-c　**届出の実施（時系列）**



注）　時系列結果の比較のため、無回答を除いて 2003 年の値を再集計しており、前頁の比率と異なる。

IPA の認知度と、届出の意思のクロス結果をみると、IPA を被害届出機関と「知っている」場合、６割以上が届出を「行う」と回答している。これに対して、IPA を被害届出機関と「知らない」場合、「行う」の割合は 35.7%であり、逆に「行わない」が６割に達している。

図表 2.5.2_②-d　届出の実施（被害届出機関としての IPA の認知度とのクロス）



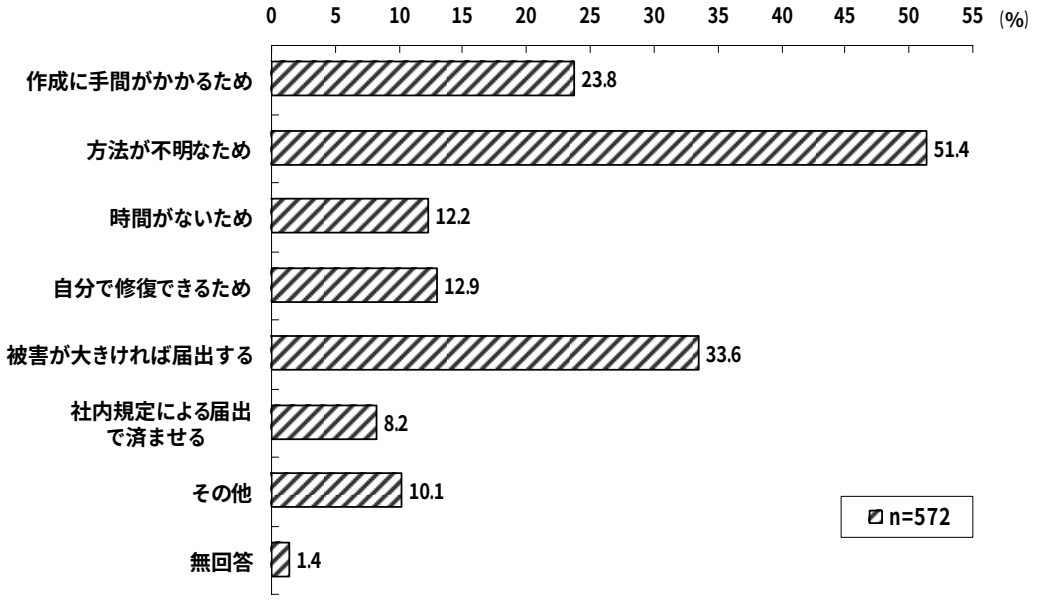
③　届出を行わない理由

IPA への届出を行わない理由については、「届出方法が不明なため」が 51.4%と最も多く、次いで「被害が大きければ届出する」（33.6%）、「届出を作成するのに手間がかかるため」（23.8%）、「自分で修復できるため」（12.9%）などが続いている。

自治体では、「被害が大きければ届出する」が最も多くなっているのに対して、民間企業では、「届出方法が不明なため」が自治体より 20 ポイント以上高くなっている。

2002 年の結果と比べて大きな変化はみられないが、「方法が不明なため」が増加し、「作成に手間がかかるため」、「被害が大きければ届出する」などが減少している。

図表 2.5.2_③-a　**届出を行わない理由**



※複数回答設問

その他　：　届出目的が不明なため（7 件）、県に報告しているため（6 件）、
本社対応のため（5 件）、届出の効果が不明（3 件）、　など

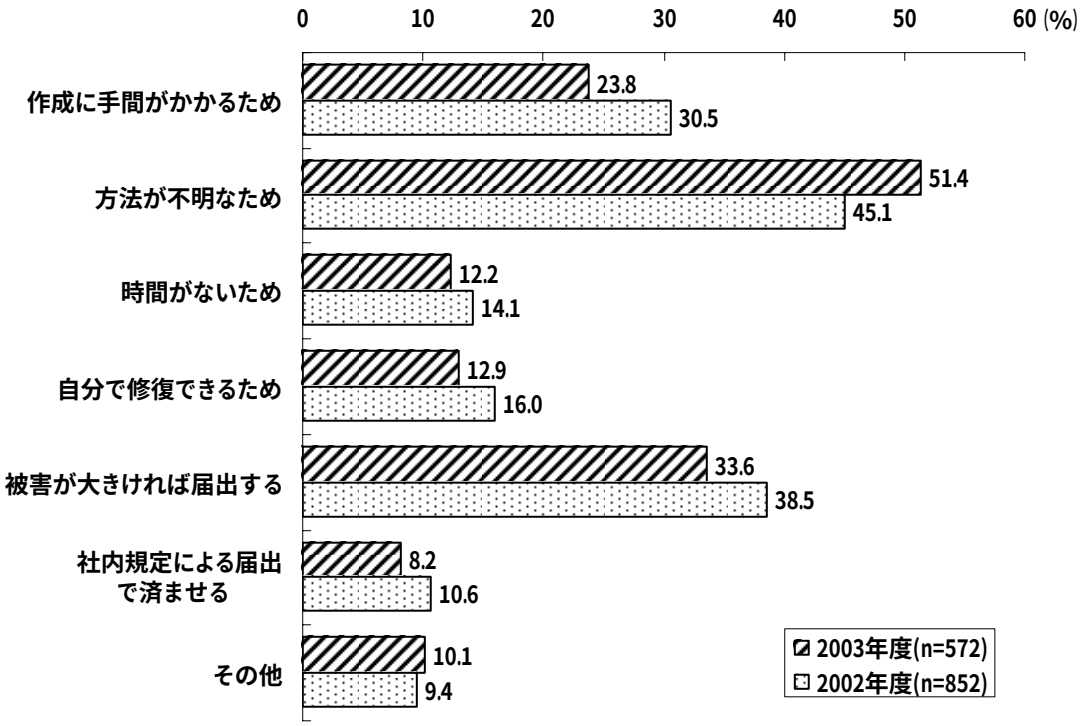
図表 2.5.2_③-b　**届出を行わない理由（自治体との比較）**

(%)

	n	届出を作成するのに手間がかかるため	届出方法が不明なため	届出る時間がないため	自分で修復できるため	被害が大きければ届出する	社内規定による届出で済ませる	その他	無回答
全体	572	23.8	51.4	12.2	12.9	33.6	8.2	10.1	1.4
民間企業	383	27.2	58.5	14.6	12.5	25.8	8.9	8.9	1.8
自治体	189	16.9	37.0	7.4	13.8	49.2	6.9	12.7	0.5

※複数回答設問

図表 2.5.2_③-c　届出を行わない理由の推移（2002 年との比較）



※複数回答設問

3. まとめ

①コンピュータウイルスの認知度は定着している

大半の事業所がコンピュータウイルスの存在を認知しており、詳しく知っているとの回答も 11.4%あった。過去からの推移をみると、認知度の上昇に伴い、コンピュータウイルスに関して知りたい情報も、基礎的知識から、より実用的なものへと移行している。

②コンピュータウイルスの遭遇経験は若干減少したが、ウイルスの種類は増加傾向にあり、また、多様化・高度化している

遭遇経験（発見および感染、以下同様）は年々増加してきたが、今年は昨年に比べ 10 ポイント少ない約 70%の事業所で遭遇経験を有する結果となった。

遭遇したウイルスの種類は年々増加する傾向にあり、今年は、2000 年以来、最も多かった「１種類」を抜いて、「５種類以上」のウイルスに感染したとの比率が 39.8%で最上位となっている。

遭遇したウイルスの性質については、メール機能を悪用するタイプ（W32/Klez 等）が、52.0％と最も多く、パスワードなどの重要情報を詐取する危険性の高いウイルス（W32/Badtrans、W32/Bugbear）も遭遇の上位にのぼっている。また、昨年夏に猛威を振るった新型ウイルス W32/MSBlaster（W32/Lovsan）は 40.4%で 2 位となっている。

③コンピュータウイルスの対策実施度に応じて被害も未然に防がれている

ウイルスの発見経緯は、ウイルス対策ソフトが 74.3%で最も多い。感染経路は、「電子メール」が 51.9%で最も多い。発見に使用されたソフトは、「ウイルスバスター」45.7%及び「Norton AntiVirus」32.1%と高い比率を占めている。

クライアントマシン、ネットワークサーバー、ローカルサーバーのいずれもウイルス対策ソフト導入率が高いほど、「感染はないが発見したことがある」との比率が高く、これらソフト導入の重要性が示唆された。

また、ウイルス対策・管理の専門部署や担当責任者が設置されているほど、発見比率が高い。ユーザ教育についても実施しているほど発見比率が高く、これら対策の有効性が示唆された。

④コンピュータウイルスの課題

「コンピュータウイルス対策基準」の認知度や、被害届出機関としての IPA の認知度はここ数年、ほとんど進展していない。届出機関として認知している場合でも、実際に届け出るとの事業所は約半数強の 62.5%に留まっている。届出方法の認知度の低さ、手続きの煩雑さ等が障壁となっている。

⑤企業と自治体との比較

自治体のほうが企業よりもコンピュータウイルス遭遇比率は 30 ポイント程度高い。管理専門部署の設置状況、セキュリティパッチ適用頻度、ユーザ教育実施状況など、感染対策に係わる多くの項目に関して企業よりも実施比率が高く、コンピュータウイルス感染に対する各種防御策に対する意識及び取り組みが進んでおり、感染が未然に防がれる傾向にある。また、自治体においては、住民基本台帳ネットワークシステムの稼動にともなう管理体制が、強化の進んだ要因のひとつと思われる。

付．コンピュータウイルス対策に関するヒアリング調査結果

○調査目的

本調査は以下の抽出基準が示すように、コンピュータウイルス対策を十分に行っている事業所において、対策実施上の工夫や実施しているにもかかわらずコンピュータウイルスに感染した理由、その対策として抱えている課題等を明らかにし、今後の対策に資することを目的として実施するものである。

○調査対象及び調査手法

- 抽出基準：
  対策ソフト導入割合　　：9 割以上
  セキュリティパッチ状況：常時最新パッチ
  組織的管理の有無　　：専門部署（担当者）設置

- 調査事業所：
  大規模企業（従業員規模 500 名）
  中規模企業（従業員規模 80 名）
  小規模企業（従業員規模 50 名）

- 調査手法
  インタビュー調査

● 大規模事業所

企業概要 （2004 年 1 月現在）	業種：情報サービス業（外資系ＤＴＰ製造メーカー子会社） 従業員規模分類：大企業（約 500 名） 所在地：東京都
システム環境	パソコン保有台数　：約 400 台（Windows 系） ネットワーク状況　：事業所間ネットワーク（ＷＡＮ）構築
対策状況等	対策ソフト導入割合：9 割以上 セキュリティパッチ：常時最新パッチ 組織的管理の有無　：専門部署（担当者）設置 ウイルス感染有無　：有

ポイント

○ 同社では、外部からのコンピュータウイルスの侵入に対しては万全のセキュリティ対策がとられていたが、社員が持ち込んだパソコンを通じて内部に持ち込まれた場合の対策は必ずしも十分ではなく結果的に防止できなかった。社員のさらなるモラル、リスクに対する意識向上に向け徹底した教育と被害を最小に抑えるための体制強化を図りつつある。

○ 同社では、これまでにもコンピュータウイルスへの対処方法を説明したビデオを配布するなど、社員教育に力を注いできた。今回のコンピュータウイルスへの感染経験を契機として、模擬環境で感染疑似体験を社員に経験させるといった教育プログラムを用意するとしている。社員の情報リテラシー、モラルの向上が期待できる実用性の高い教育方法である。

○ グループ企業全社でウイルスに関する最新情報を一元管理。効率良く低コストで最新且つ均一のとれた情報提供は、実用性の高い工夫のひとつである。また単に一元管理、掲載するのではなく、掲載されている情報からいつも最新情報を電子メールで一人一人の社員に送付し必ず読ませるといった配慮、工夫をしている。

○ 大企業ならではであるが、技術力の高い専門集団による一元集中監視体制を敷き、最新情報、管理規定マニュアル、被害時の報告フォーマット等もすべて統一的に整備し、教育、システム運用・管理を現場と連携して行っている。現場の負荷を考慮した効率の良い運用方法である。

1．事業所のコンピュータウイルス対策への取り組みの現状について

(1)　組織･体制に関して

- ✧ コンピュータ管理は同社本部に情報システム管理グループを設置、専属で 2 名を、各部署およそ 20 名程度に 1 名の割合で社員の中でもコンピュータリテラシーの高い管理担当者を兼業形態で配置している。さらに親会社には、グループ企業全体を管理する数十名の専任技術者で構成される情報管理部門が設置されている。
- ✧ 同社は社員教育として、ビデオ教材等を親会社の情報システム部門が用意し、社員がいつでも学習できるような環境を整備している。親会社が情報システム製品を扱う外資系でもあることから、情報システムを重要視する意識が高く、それ故にリスクに対する意識も高く、社員のリテラシーをいろいろな角度から先進的な取り組みを交えて高めようという努力が伺える。
- ✧ 併せて、コンピュータウイルスに関する全情報を親会社のデータベース上で一元管理しており、イントラネットに接続されたグループ企業の社員であれば誰もが検索し、最新の情報を入手できる仕組みとなっている。一元管理されているので、情報更新の運用負荷も低く、且ついつでも最新の情報を直ぐに入手できるようになっている。
- ✧ 親会社は、グループ企業各社のシステム構成、各種情報システム管理規定、文書管理規定、セキュリティ対策に関する規定、ウイルス対策手順等をすべて一元的に企画・作成・運用している。グループ企業各社は、その企画に則りシステム運用を行っている点で、グループ企業各社の運用負荷が低く抑えられている。

(2)　情報システムに関して

- ✧ 同社は外資系大手ＤＴＰ機器製造メーカー子会社で、親会社が構築する大規模ＷＡＮの１ノードとしてクライアント約 400 台を接続、運用している。クライアントは、すべて Windows で可搬型のパソコンをほぼ社員一人１台の割合で提供している。機種、搭載アプリケーション等は全て親会社のシステム部門が決定し、全クライアント情報について一元管理できる仕組みを構築している。
- ✧ 新種ウイルス等が発生した場合、親会社の情報システム管理者が警戒情報を社内用ＨＰに掲載するとともに、子会社の専属管理者が、社員各位に注意を喚起するために社内メールで最新情報を都度送信している点で、必ず社員一人一人が最新情報を認識するようきめ細かな対応を行っている。

(3)　その他（ウイルス対策、セキュリティ確保にむけて配慮している事など）

- ✧ 社員の間でコンピュータウイルスに対する専門的知識や具体的な対処方法、さらに情報システム全般への情報リテラシーの有無が明らかになっており、各部に配置されているシステム管理者の業務負担もやや高まりつつある。
- ✧ こうした状況を受けて、情報システムグループでは、さらに興味深い教育方法の実施を予定している。そのひとつは、本番環境から切り離した模擬環境を構築し、その中でコンピュータウイルスを発生させ、社員に体験してもらうというものである。そうした体験を通じて実際の対処方法などを会得してもらうとしている。
- ✧ また、情報リテラシーの低い社員を集め、集中的にリテラシー教育を施すといった教育方法も検討しているとのこと。誰もができる簡単な対処方法の教育、日頃の注意を徹底させるだけでもかなりの効果が期待される。

2．事業所のコンピュータウイルス対策への取り組みの経緯について

- ✧ 同社は、もともと親会社が扱う製品がネットワーク型のハードウェアであったため、一般企業と比べいち早くネットワーク環境を構築していた。また米国親会社の情報リテラシーが高かったという経緯もあり、ネットワークウイルス対策もいち早い対応がとられてきた。

3．ウイルス遭遇時の対応（対応策）について

- ✧ 徹底した体制、対応をとっている同社ではあるが、昨年もコンピュータウイルス感染の被害にあっている。この経験を通じて体制の弱みと強みを顕在化することができたとされる。
- ✧ 今回感染したルートは、社員が提供されている可搬型パソコンからであった。週末等に持ち帰り、家庭内の比較的手薄なウイルス対策環境で感染し、そのまま会社に持ち込み、感染が広がるといったケースであった。
- ✧ 同社のウイルス対策のための体制は外部からの感染に対して十分な配慮がなされている一方で、内部で持ち込まれた場合にその対策が十分ではないことが明らかとなった。各自への徹底したモラル再教育が必要であり、今後の課題となっている。
- ✧ その一方で感染した場合の「対応の迅速さ」という強みも明らかとなった。同社の親会社のシステム部門は常時監視体制でＬＡＮの状況を見守っており、万が一感染し異常なデータ量が発生した場合は、即座にルー

タから対象ノードの引き離しをおこない、被害がグループ各社に及ばないように対処を行った。実際の被害も数台のパソコン被害に留めることができた。

4．今後の課題

✧ 上記で述べたとおり、同社のウイルス対策の体制は外部からの侵入に対して十分な配慮がなされている一方で、内部で持ち込まれた場合にその対策が十分ではないことが明らかとなった。各自への徹底したモラル再教育が必要であり、今後の課題となっている。

✧ また、すでに確認できているウイルスに対しては、すべて外部から侵入した瞬間に自動的にファイル削除が行われているが、新規に発生したウイルスに対しては防止の手立てがないため、感染してしまうことになる。これも一人一人の注意深さが重要となる問題で、如何に意識を高めるかが今後の課題となっている。

● 中規模事業所

企業概要 （2004 年 1 月現在）	業種：情報サービス業 従業員規模分類：中事業所（約７０名：本社約 800 名） 所在地：東京都
システム環境	パソコン保有台数　：約 100 台（Windows 系） ネットワーク状況　：事業所間ネットワーク（ＷＡＮ）構築
対策状況等	対策ソフト導入割合：9 割以上 セキュリティパッチ：常時最新パッチ 組織的管理の有無　：専門担当者設置 ウイルス感染有無　：有

ポイント

○ 同事業所には、事業所内のパソコンの調達・ＬＡＮ管理・システム保守、および各種手続きなど、社員の情報システムの効率化やセキュリティを図るために事業所独自の判断で『IT 委員会』が組織されており、本社が規定するテクニカルガイドライン、ルール、ポリシーなどに準じて、システム運用を行っている。

○ 同事業所は中規模事業所であるため、『IT 委員会』による全パソコンの一括管理が難しいこと、情報サービス業であることから、社員一人一人に徹底した教育を行っている。また、社員のリテラシー向上のために、新ルール適用の度にメールで告知し、イントラネット経由で WBT(Web Based Training)を実施してもらい、テストを行っている。

○ 同事業所では、一人１台のパソコン環境が整っており、個人のパソコンの環境整備は、『IT 委員会』による指導のもと、個人の責任に任せられている。個人の持ち込みパソコンに関しても、社内 LAN に接続する場合には、『IT 委員会』への申請が義務付けられており、ウイルス対策ソフトなどをインストールしない限りは接続してはいけないことになっている。

○ ウイルス対策ソフトの定義ファイルは個人パソコンについては個人が毎日更新し、パソコン内を１週間に１回スキャンするルールを策定している。これらの実施は個人に任せられているが、実行しない人は強制的に社内 LAN から切り離すなどの処置を施している。また、ウイルスメールやセキュリティ事故が発生した場合のために、『IT 委員会』が手順等を詳細に決め、冊子やポータルサイト、メール等で告知しており、徹底して社員に認識してもらっている。

1．事業所のコンピュータウイルス対策への取り組みの現状について

(1)　組織･体制に関して

- ✧ 同事業所には、事業所内のパソコンの調達・ＬＡＮ管理・システム保守、および各種手続きなど、社員の情報システムの効率化やセキュリティを図るために『IT 委員会』を設置している。
- ✧ 『IT 委員会』は、本社が規定するテクニカルガイドライン、ルール、ポリシーなどに準じて、システム運用を行っている。
- ✧ 『IT 委員会』のメンバーは６人で構成され、３年の任期制となっている。専任ではないため、定期的に月２回程度の会議を開催し、情報交換やルール策定を行っている。イベント発生時（セキュリティ事故、ウイルス発見など）には臨時の委員会を開き、検討・対応を行っている。
- ✧ 『IT 委員会』はウイルス情報を定期的に収集しており、新種のウイルスが発生したり、またそれに伴う OS のアップデートの必要性が生じたりした場合、ウイルスの危険性について、社員全員にメールで注意を呼びかけている。

(2)　情報システムに関して

- ✧ 同事業所では、一人 1 台のパソコン環境が整っており、個人のパソコンの環境整備は、『IT 委員会』による指導のもと、個人の責任に任せられている。またアルバイト専用のパソコンも数台あり、それらは基本的には『IT 委員会』が管理している。
- ✧ 同事業所では、インターネットには社内 LAN で本社を経由して接続されており、セキュリティを確保するためにファイヤーウォールを設置している。
- ✧ フィルタリングソフトを導入しており、全社的に有害コンテンツの排除、エージェント侵入の防御を施している。このため、一部のサービスの利用やコンテンツへのアクセス等が制限されており、電子メールについても、外部メーリングリストの利用は禁止されている。また、転送指定や容量についても制限を設けている。
- ✧ 同事業所のファイルサーバーは、セキュリティの観点から、直接外部には（本社にも）繋げていない。
- ✧ メールサーバーは本社と共有しており、２種類のメーカーのウイルス対策ソフトを導入し、事前の防止につとめている。
- ✧ 本社とは別に、同事業所独自のウイルス対策方法として、シマンテック社の Norton Antivirus を事業所の全パソコンにインストールしている。ウイルス対策ソフトの定義ファイルは個人パソコンについては個人が毎

日更新することを義務付け、またパソコン内を 1 週間に 1 回スキャンするルールを策定している。

- ✧ 持ち込みパソコンに関しても、社内 LAN に接続する場合には、『IT 委員会』への申請が義務付けられており、ウイルス対策ソフトなどをインストールしない限りは接続してはいけないことになっている。

(3) その他 (ウイルス対策、セキュリティ確保にむけて配慮している事など)

- ✧ パソコンには 1 台 1 台、ユーザ管理（ＩＤを設ける）を行っており、社員以外の人がパソコンにログインできないように管理している。
- ✧ 社員教育に関しては、LAN 利用基準マニュアルを作成し、事業所内のポータルサイト上で公開している。
- ✧ 社員のリテラシー向上のために、新ルール適用の度にメールで告知し、イントラネット経由で WBT を実施してもらい、テストを行っている。

2. 事業所のコンピュータウイルス対策への取り組みの経緯について

(1) 組織･体制に関して

- ✧ 本社には、情報システムの導入・保守・管理・運用を行っている専門部署があり、全社的なセキュリティールールの策定や、サーバー管理などを行っている。
- ✧ 同社には事業所単位では、そのような体制を作ることは決められていない。しかし、同事業所は個人情報データを取り扱うことも頻繁にあり、電子ファイルでやり取りを行う業務等も多く発生するため、事業所独自の判断により、『IT 委員会』を組織した。

(2) 情報システムに関して

- ✧ 過去、いくつかのウイルス対策ソフトを使用したが、結局シマンテック社のソフトに落ち着いた。理由としては、全社的に購入していることと、比較的安くて、最新ウイルスへの対応が早いといった利点からである。
- ✧ ウイルス対策ソフトによるパソコンのスキャンの実施は個人に任せているが、実行しない人は強制的に LAN から切り離すなどの処置を施していた。結果的に、対策を実施しない人の数は減ってきている。

3. ウイルス遭遇時の対応 (対応策) について

- ✧ 昨年は 8 月に、W32/Welchia に４～５台（約 100 台中）が感染した。感染

したパソコンはウイルス対策を怠っていた（最新のパッチを当てていなかった、または定義ファイルを更新していなかった）パソコンである。

- ✧ 事象所内のパソコンからウイルスメールが発見された場合は、ファイヤーウォールの設定の変更などを『IT 委員会』が行っている。
- ✧ ウイルスメールを発見した時は以下の手順を踏むように、社員にはポータルサイトやメール、冊子等で告知している。
    - ① 感染したパソコンの利用を停止し、LAN ケーブルを抜き、スタンドアローン状態にする。
    - ② ウイルス対策ソフトの定義ファイルを更新し、検出されたウイルスを排除する。
    - ③ ウイルス発生パソコンのウイルス対策ソフトの「ウイルス定義の更新」の頻度および定時スキャンの設定を確認し、全ローカルディスクのスキャンを実施する。
    - ④ 特定可能な範囲で次の情報を記録し、直ちに『IT 委員会』のメンバーに報告する。
        - (ア)発見されたウイルスの名称
        - (イ)ウイルスに感染されたファイルの格納場所、ファイル名、更新日時
        - (ウ)(イ)の情報より推定される感染源
        - (エ)(イ)の情報より推定される感染先
    - ⑤ 『IT 委員会』は臨時召集し、社員全員にメールし、注意を呼びかける。

4．今後の課題

- ✧ 『IT 委員会』は事業所独自の組織であり、他の業務と兼務で担当している為、より専任的な人材を確保する必要がある。
- ✧ ウイルス対策は、より早期なウイルス情報の入手、そして社員への徹底した告知が必要である。
- ✧ パソコンのウイルス対策ソフトの定義ファイルの更新や、OS のアップデート等を行い、常にパソコン環境を最新に保つような社員教育が必要である。
- ✧ 基本的なセキュリティールールに関する知識を全員に植え付ける必要がある。
- ✧ ルールを厳守しない社員に対しては、時には強制的な措置が必要である。

● 小規模事業所

企業概要 （2004年1月現在）	業種：外資系金融業 従業員規模分類：小企業（50人（当該事業所のみ）） 所在地：東京都
システム環境	パソコン保有台数　：約48台（Windows系） ネットワーク状況　：事業所間ネットワーク（ＷＡＮ）構築
対策状況等	対策ソフト導入割合：9割以上 セキュリティパッチ：常時最新パッチ 組織的管理の有無　：兼務担当者 ウイルス感染有無　：無

ポイント

○ 同事業所には、本社の情報システム部とは別に、事業所内のパソコンの調達・保守・運用・管理などのシステム業務を専任しているITの知識・常識に長けた『IT担当者』がいる。

○ 同事業所では、事業所全体のシステム管理から、個人パソコンの管理までを、すべて『IT担当者』が一任しており、その『IT担当者』により事前にセキュリティ事故やウイルス感染への対策が講じられている。

○ 同事業所のシステムは、全てのＯＳ、アプリケーションを統一し、サーバー上から常時監視、一括管理できるような仕組みになっている。また、ファイヤーウォール、ウイルス対策ソフト、メール専用の対策ソフトを導入し、個人のパソコンにインストールされているアプリケーションを含め、アップデートや最新のパッチ等もサーバーから自動的に更新されるようになっている。

○ ウイルスの発見時などには、『IT担当者』以外の人が勝手にパソコンを触らないように義務付けており、また、もしもの時のために、最新のウイルスパッチを当てたパソコンの予備となる代替マシンを常時確保しており、感染時などにはすぐに差し替え、誤操作による被害が拡大しないように、事前に気をつけている。

1．事業所のコンピュータウイルス対策への取り組みの現状について

(1)　組織･体制に関して

- ✧ 同事業所には、本社の情報システム部とは別に、事業所内のパソコンの調達・保守・運用・管理などのシステム業務を専任している IT の知識・常識に長けた『IT 担当者』がいる。但し、担当者は一人である。
- ✧ ウイルス対策は『IT 担当者』が一括して管理しており、執り行っている。

(2)　情報システムに関して

- ✧ 管理対策サーバーなどにより、何段階にも分けたセキュリティ対策を実施しており、ネットワークのトラフィックやログ等の常時監視、ウイルス対策ソフトによるチェックを行っているので、事故発生などの異常が発見された場合には、即座に対応できるシステム作りを行っている。
- ✧ 同事業所は、金融業ということもあり、個人情報を取り扱う業務も多いことから、ファイヤーウォール(Cyberguard)のセキュリティレベルを厳しく高度な位置に設定している。Cyberguard は、価格が高いものの、信頼性の高いソフトだという認識のもと、『IT 担当者』の判断で導入した。
- ✧ 基本的なパッケージの導入は、本社指示に従っているが、事業所内のパソコンやシステムの保守・管理・運用は各事業所単位に任されている。
- ✧ ウイルス対策ソフトとして、サーバー・クライアントに Norton Antivirus を導入している。また、メールサーバーにはメール専用の対策ソフト TrendMicro Scanmail を導入している。
- ✧ ウイルス対策ソフトの定義ファイルや OS のセキュリティパッチは、サーバーで一括管理して自動的にアップデートされるシステムを構築している。

(3)　その他(ウイルス対策、セキュリティ確保にむけて配慮している事など)

- ✧ セキュリティポリシーは本社で規定されており、同事業所でもそれに準じて規定している。
- ✧ その他の情報システムに関するルール（LAN 接続、モバイルパソコンの持ち込み、インストールアプリケーション等）は事業所独自のガイドラインを作成し、社員に通達している。
- ✧ 社員には、パソコンへのログインパスワードを頻繁に変更するよう指示をしており、また推測されにくいパスワード設定を義務付けている。
- ✧ 自分のモバイルパソコンを事業所内に持ち込む事は許可しているが、それを社内 LAN に接続することなどはいかなる場合も堅く禁止しており、持ち込みパソコン等による感染を事前に防いでいる。

2．事業所のコンピュータウイルス対策への取り組みの経緯について

（1） 組織･体制に関して

✧ 同事業所では、社員教育を数年前まで実施していたが、現在は行っていない。社員教育のための金銭的な余裕がないためであるが、現在は社内メールやパンフレットなどを用いてウイルスの危険性などについて通達し、適宜重要性を啓蒙している。

（2） 情報システムに関して

✧ 同事業所内では、一括して管理する為にパソコン毎にインストールされる OS やウイルス対策ソフトなどのアプリケーションを統一して導入している。

✧ 同事業所では、事象所内の IT 化が比較的遅かったため、逆に最新の性能の良いセキュリティシステムの構築を行っている。

✧ 導入時のフレームワーク作りが大切であると考えており、初期投資が高くついたものの、事業所内全パソコンを一括管理できるようにシステムを構築してきた。

3．ウイルス遭遇時の対応（対応策）について

✧ 上記したようなシステムを構築してきたため、過去 3 年間、ウイルスによる感染・被害は全く無い。

✧ ウイルス感染・発見時には、必ず『IT 担当者』へ連絡が来るような体制を作っており、もしウイルスが発見された時には『ＩＴ担当者』自身がウイルス駆除処理を行っている。

✧ ウイルスの発見時などには、『IT 担当者』以外の人が勝手にパソコンを触らないように義務付けており、また、もしもの時のために、最新のウイルスパッチを当てたパソコンの予備となる代替マシンを常時確保しており、感染時などにはすぐに差し替え、誤操作による被害が拡大しないように、事前に気をつけている。

4．今後の課題

✧ 社員一人一人の IT リテラシーやウイルス被害に対する意識が弱くて、薄いため、いくら IT 担当者が頑張っても、しばしば限界を感じることがある。

✧ ウイルスに感染することは、自分が被害者である一方で加害者にもなっ

てしまうという不安があるということを社員一人一人に自覚させる必要がある。

- ✧ ウイルス対策ソフトを導入すると、ウイルス対策に対しては安心であるが、逆にこれにより、処理速度が遅くなったり、またシステムが不安定になったりするという問題点が時々発生する。
- ✧ 日々ウイルス対策に追われ苦労しなくてもいいように、コストが少々高くついても、IT 環境導入初期時に（または、導入した後も適宜)、最新のフレームワークをしっかりと作り込む必要がある。
- ✧ 小規模事業者などにとっては、セキュリティ担当の人材育成や、そのためのシステム導入などは予算的にも困難であるが、ウイルス対策には、それなりの投資が必要であり、少々高くついても、やるべきことであるということを経営者自らが認識する必要がある。
- ✧ 事業所には、セキュリティ担当者という専任の相談相手をおき、社員の IT スキル、IT リテラシーが多少低くても、ウイルス遭遇時やセキュリティ事故時などにおいて、即座に充分対応できるような体制を作る必要がある。また、情報システムを一括して監視するシステムを構築する必要がある。
- ✧ ウイルス対策などは、通常必ず施さないといけない措置であるため、IT のベンダーなどがパソコンを出荷する時に、高度なセキュリティを標準仕様にするべきではないだろうか。