



INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

# 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

---

2006 年 11 月

独立行政法人 情報処理推進機構

## 目 次

1. 調査概要	1
1.1. 調査目的	1
1.2. 調査対象	1
1.3. 調査期間	1
1.4. 調査方法	2
1.5. 回収結果	2
1.6. 調査項目	2
2. 調査結果	3
2.1. 回答企業・自治体の概要	3
2.1.1. 業種	3
2.1.2. 総従業員数	4
2.1.3. 総売上高（単体）	5
2.1.4. 経営利益（単体）	5
2.1.5. 規程年間営業日数および1日の営業時間	6
2.1.6. 利用しているパソコンのOSと台数	7
2.1.7. LANやWAN等のネットワークの構築状況	8
2.2. コンピュータウイルス対策の現状	9
2.2.1. パソコンへのウイルス対策ソフトの導入状況	9
2.2.2. 外部公開ネットワークサーバへのウイルス対策ソフトの導入状況	10
2.2.3. 内部利用ローカルサーバへのウイルス対策ソフトの導入状況	11
2.2.4. ウイルス対策ソフトの導入・更新費用	12
2.2.5. ウイルス対策に関するユーザ教育	13
2.2.6. ウイルス対策に関する社内体制	14
2.2.7. セキュリティパッチ（Windows Update など）の適用	15
2.3. コンピュータウイルス対策に対する意識	16
2.3.1. コンピュータウイルスに関連して知りたいと思っている情報	16
2.3.2. 「コンピュータウイルス対策基準」の認知度	18
2.3.3. 被害届出について	20
2.4. コンピュータウイルスによる被害状況	27
2.4.1. コンピュータウイルス遭遇（感染または発見）経験	27
2.4.2. 遭遇したウイルスの種類数	30
2.4.3. 遭遇したウイルスの名称	31
2.4.4. ウイルスの感染件数	32
2.4.5. ウイルスに感染したパソコンの台数	33

2.4.6. ウイルスの直接的な被害	34
2.4.7. ウイルスの間接的な被害	35
2.4.8. 電子商取引（EC）業務	36
2.4.9. インターネット公開の業務遂行上重要なサーバが停止した年間延べ日数	37
2.4.10. 事業所内のネットワークや社内の重要なサーバの利用が困難になった年間延べ日数	38
2.4.11. 2005年1年間のウイルス感染からの復旧作業延べ人日	39
2.4.12. 2005年1年間にウイルス感染が原因で発生した追加データ処理作業人日	40
2.4.13. システム復旧に関して新たに購入した代替機器の費用	41
2.4.14. システム復旧に関して外部に発注した業務の費用	41
2.4.15. システム復旧に関してその他に発生した費用	41
2.4.16. 影響の最も大きかったウイルス	42
2.5. 新しい脅威について	48
2.5.1. スパイウェアの被害の有無	48
2.5.2. スパイウェア対策ツールの有無	49
2.5.3. 発見されたスパイウェアの侵入経路	50
3. 考察	51

付録 コンピュータウイルスに関する被害状況調査票

## 1. 調査概要

### 1.1. 調査目的

近年、ネットワークを軸とする IT（情報技術）は、わが国の社会・経済における極めて重要な社会インフラとなっており、IT システムにおけるコンピュータウイルス等の感染は、単に従業員やグループの業務に支障を来すだけでなく、個人情報をはじめとする機密情報の流出事故や、全社あるいは取引先を含むバリューチェーン全体の事業中断をも招きかねない状況となっている。コンピュータウイルス対策は、企業の事業継続性確保や果たすべき社会的責任の遂行に不可欠な取組みの一つと言え、政府においても、企業に対策実施の動機を与える定量的なデータの提供と、適切な施策の実施を通じて、企業のコンピュータウイルス対策を促進することが求められている。

このような背景の下、独立行政法人情報処理推進機構（以下、「IPA」という）では、従前から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、今後企業が適切な対策レベルを設定するための有益な手法に関して検討することを目的として、企業・自治体に対してアンケート調査を行っている。

### 1.2. 調査対象

本調査は、全国の企業及び自治体 6,561 件を調査対象として実施した。その内訳は、無作為に抽出した全国の企業 5,500 件、及び無作為に抽出した全国の自治体 1,061 件となっている。

	内容
標本数	6,561 件 (うち、企業 5,500 件、自治体 1,061 件)
標本台帳	①企業 ・「情報処理実態調査」対象機関 ・株式会社 東京商工リサーチ (上記の抽出機関の補足) ②自治体 ・財団法人地方自治情報センター
抽出方法	①企業： 業種別、従業員規模別無作為抽出 ②自治体： 都道府県（47 都道府県） 特別区（東京 23 区） 市町村 人口規模別無作為抽出

### 1.3. 調査期間

調査実施期間：2006 年 3 月

調査対象期間：2005 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 6,561 件に対し、1,701 件の回収があり、回収率は 25.9%であった。企業、自治体別の内訳は下表の通りである。なお、後述するが、本調査における企業と自治体の比較においては、自治体でも比較的規模が大きな自治体の回答値であることに留意いただきたい。

	発送数	回収数	回収率
全体	6,561	1,701	25.9%
企業	5,500	1,206	21.9%
自治体	1,061	495	46.7%

#### 1.6. 調査項目

調査の主な設問項目は下記の通りである。民間企業及び自治体も基本的に共通の設問である。

<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対策
- (3) コンピュータウイルスの発見と被害状況
- (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. 回答企業・自治体の概要

#### 2.1.1. 業種

回答企業・自治体の業種については、「自治体・公共団体」（29.1%）を除くと「他の製造業」（13.5%）が最も多く、次いで「情報通信業」（12.1%）、「他のサービス業」（10.1%）、「金融・保険業」（7.5%）の順となっている。

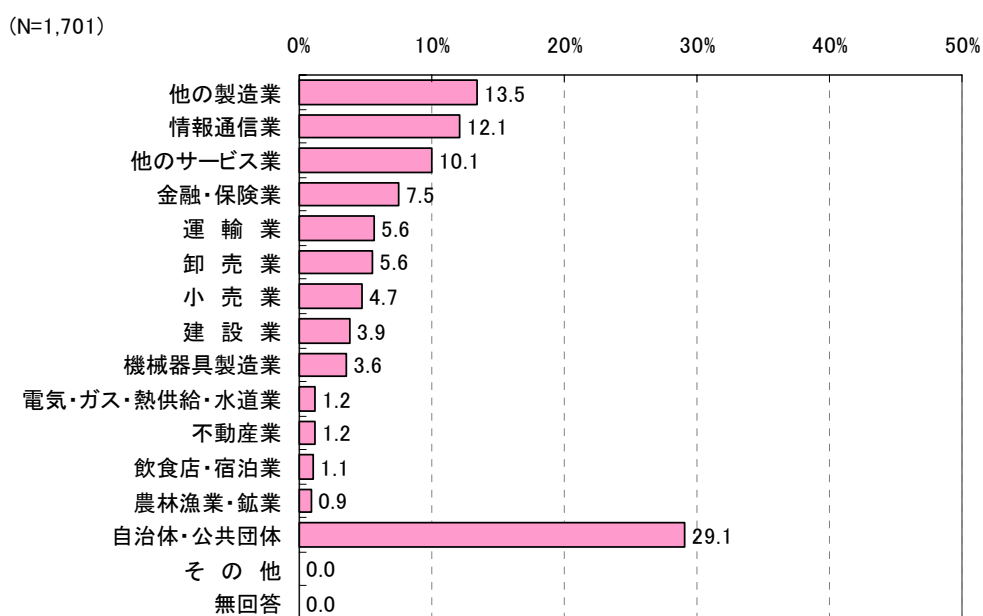


図 2.1-1 業種

注1) 「他のサービス業」「その他」の回答、および無回答の回収票については、適切な業種へ振り分けを行った。

注2) 標準産業分類に準じ、「情報サービス業」は「情報通信業」に含まれる。

### 2.1.2. 総従業員数

全体で見た総従業員数は「300 人未満」で半数弱であるが、地方自治体の総従業員数が多い傾向にあり、地方自治体だけでは「300 人以上」がほぼ 8 割に上る。これは、市町村合併が急速に進展していることから、規模が大きい地方自治体が増えていることも背景にある。本調査における企業と自治体の比較においては、自治体でも比較的規模が大きな自治体の回答値であることに留意いただきたい。

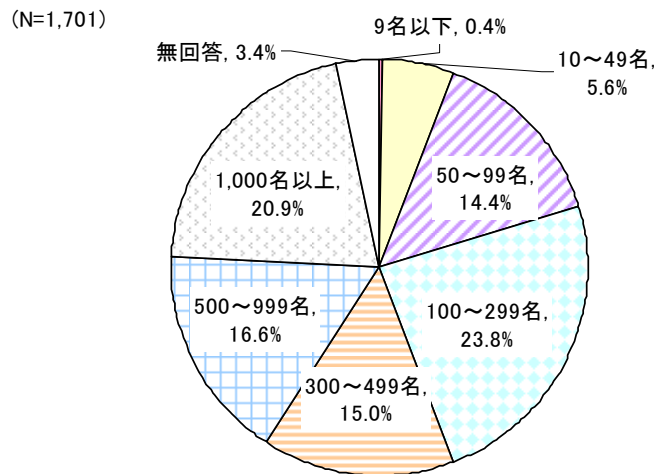


図 2.1-2 総従業員数

表 2.1-1 総従業員数（自治体との比較）

	N	9名以下	10~49名	50~99名	100~299名	300~499名	500~999名	1,000名以上	無回答
全体	1,701	0.4	5.6	14.4	23.8	15.0	16.6	20.9	3.4
企業	1,206	0.5	7.6	20.1	27.6	13.3	12.1	15.8	2.8
地方自治体	495	0.0	0.6	0.4	14.3	19.2	27.5	33.1	4.8

(%)

### 2.1.3. 総売上高（単体）

企業における直近年度の総売上高は「100 億円未満」が半数程度である。平均は、売上規模の大きな一部企業が引き上げたことで、527.3 億円であった。

(N=1,206)

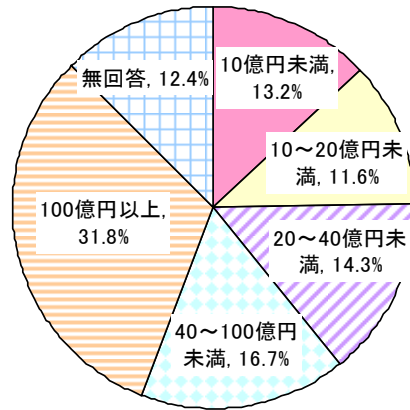


図 2.1-3 総売上高（単体、企業のみ）

### 2.1.4. 経営利益（単体）

経常利益は 4 億円未満が半数程度であり、平均は 30.6 億円であった。

(N=1,206)

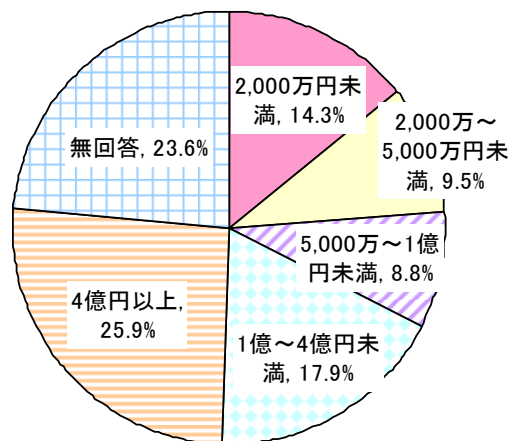


図 2.1-4 経営利益（単体、企業のみ）

### 2.1.5. 規程年間営業日数および1日の営業時間

規程年間営業日数は、「200～249日」が4割強、「250～300日」が3割程度であり、自治体と比較すると企業の方が多傾向にある。1日の営業時間は半数以上が「8時間」であり、特に地方自治体の7割以上が「8時間」と回答している。

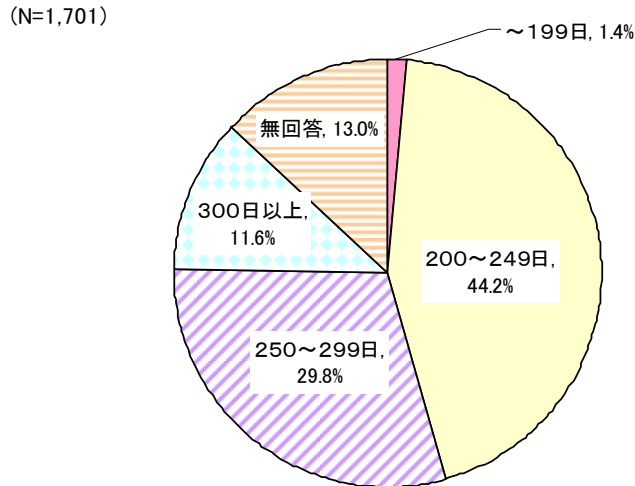


図 2.1-5 規程年間営業日数

表 2.1-2 規程年間営業日数（自治体との比較）

	N	～199日	200～249日	250～299日	300日以上	無回答
全体	1,701	1.4	44.2	29.8	11.6	13.0
企業	1,206	2.0	40.6	30.3	14.3	12.8
地方自治体	495	0.0	52.7	28.7	5.1	13.5

(%)

(N=1,701)

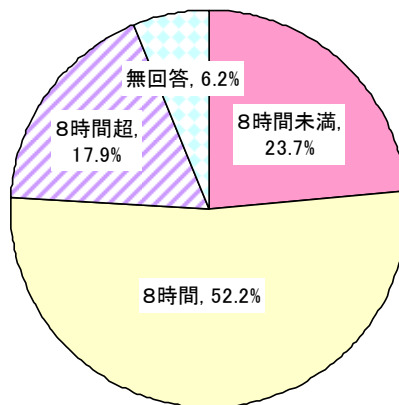


図 2.1-6 1日の営業時間

表 2.1-3 1日の営業時間（自治体との比較）

	N	8時間未満	8時間	8時間超	無回答
全体	1,701	23.7	52.2	17.9	6.2
企業	1,206	31.2	42.5	19.6	6.8
地方自治体	495	5.5	76.0	13.7	4.8

(%)

2.1.6. 利用しているパソコンのOSと台数

9割以上の組織がWindows系のパソコンを利用しており、そのうち半数以上が100台以上を保有している。Macintosh系のパソコンを1台でも利用しているのは約2割、Unix・Linux系のパソコンを1台でも利用しているのは約3割である。

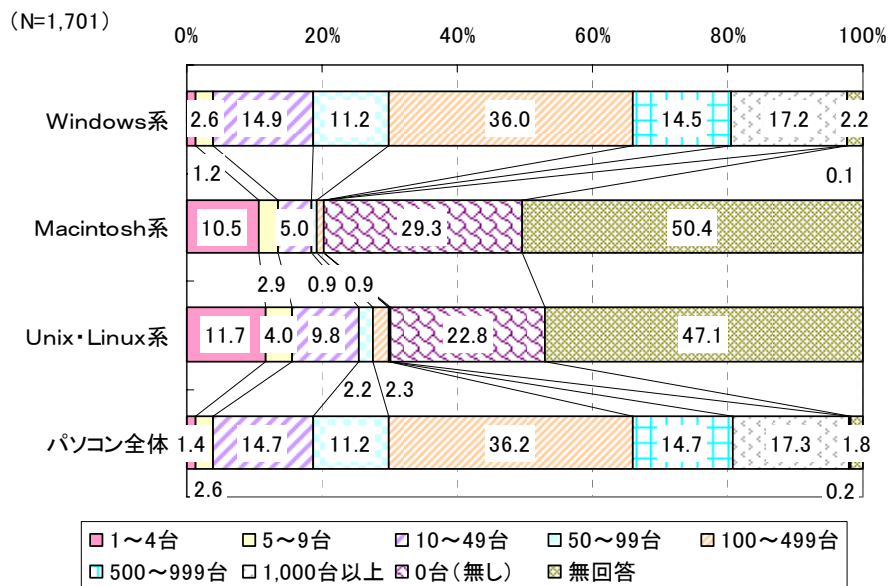


図 2.1-7 利用しているパソコンのOSと台数

表 2.1-4 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	1,701	1.2	2.6	14.9	11.2	36.0	14.5	17.2	0.1	2.2
企業	1,206	1.7	3.4	20.8	15.8	32.9	9.9	13.4	0.1	2.0
地方自治体	495	0.0	0.6	0.4	0.2	43.6	25.9	26.5	0.0	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	1,701	10.5	2.9	5.0	0.9	0.9	0.0	0.0	29.3	50.4
企業	1,206	9.9	2.9	6.6	1.3	1.3	0.0	0.0	31.5	46.5
地方自治体	495	12.1	2.8	1.2	0.0	0.0	0.0	0.0	24.0	59.8
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	1,701	11.7	4.0	9.8	2.2	2.3	0.0	0.2	22.8	47.1
企業	1,206	11.0	3.2	10.9	3.0	2.7	0.0	0.2	24.8	44.2
地方自治体	495	13.3	6.1	7.1	0.2	1.2	0.0	0.0	18.0	54.1
パソコン全体 (%)										
	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	1,701	1.4	2.6	14.7	11.2	36.2	14.7	17.3	0.2	1.8
企業	1,206	1.9	3.4	20.6	15.7	33.0	10.1	13.6	0.2	1.5
地方自治体	495	0.0	0.6	0.2	0.2	43.8	25.9	26.5	0.2	2.6

### 2.1.7. LAN や WAN 等のネットワークの構築状況

企業の6割強、地方自治体の約9割が、「事業所内だけではなく、機関内の事業所間ネットワーク（WAN）まで構築」「外部の機関とのネットワークまで構築」等、何らかの形態で事業所外とのネットワークが構築されている。

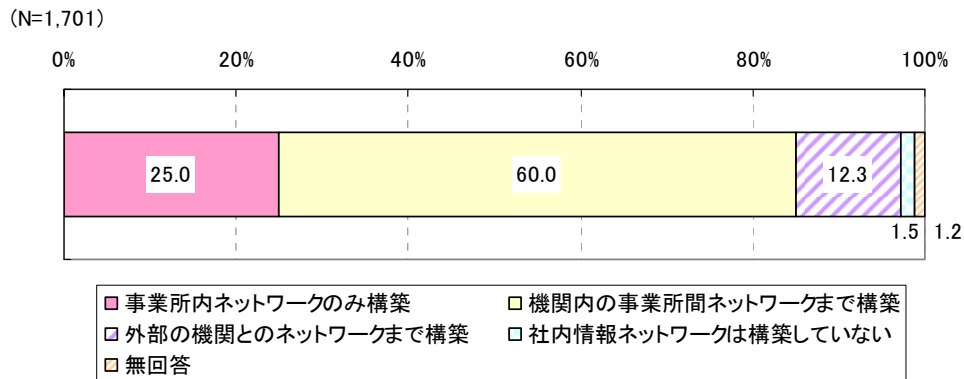


図 2.1-8 LAN や WAN 等のネットワークの構築状況

表 2.1-5 LAN や WAN 等の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	機関内の事業所間ネットワークまで構築	外部の機関とのネットワークまで構築	社内情報ネットワークは構築していない	無回答
全体	1,701	25.0	60.0	12.3	1.5	1.2
企業	1,206	31.4	53.9	11.2	2.1	1.4
地方自治体	495	9.5	74.7	14.9	0.2	0.6

(%)

## 2.2. コンピュータウイルス対策の現状

### 2.2.1. パソコンへのウイルス対策ソフトの導入状況

ウイルス対策ソフトは、「9割以上のパソコンに導入済み」が9割近くに達し、導入していないのは2.4%に過ぎない。

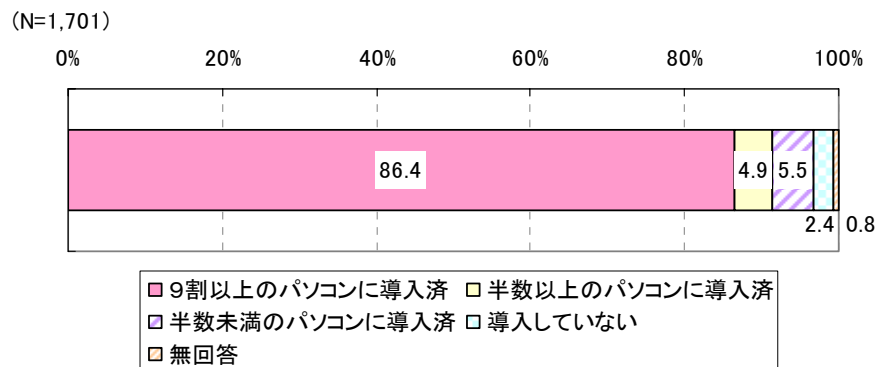


図 2.2-1 パソコンへのウイルス対策ソフトの導入状況

表 2.2-1 パソコンへのウイルス対策ソフトの導入状況（自治体との比較）

(%)

	N	9割以上のパソコンに導入済み	半数以上のパソコンに導入済み	半数未満のパソコンに導入済み	導入していない	無回答
全体	1,701	86.4	4.9	5.5	2.4	0.8
企業	1,206	82.3	6.4	7.2	3.2	0.9
地方自治体	495	96.6	1.4	1.4	0.2	0.4

### 2.2.2. 外部公開ネットワークサーバへのウイルス対策ソフトの導入状況

ウイルス対策ソフトが「9割以上のネットワークサーバに導入済み」であるのは約7割であるが、パソコン向けウイルス対策と異なり、導入していない事業所も14.9%ある。

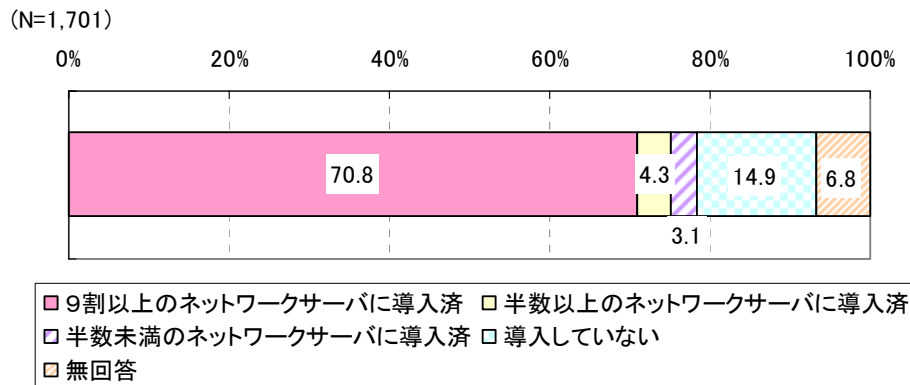


図 2.2-2 外部公開ネットワークサーバへのウイルス対策ソフトの導入状況

表 2.2-2 外部公開ネットワークサーバへのウイルス対策ソフトの導入状況（自治体との比較）

(%)						
	N	9割以上のネットワークサーバに導入済	半数以上のネットワークサーバに導入済	半数未満のネットワークサーバに導入済	導入していない	無回答
全体	1,701	70.8	4.3	3.1	14.9	6.8
企業	1,206	65.5	4.1	3.3	18.5	8.6
地方自治体	495	83.8	4.8	2.6	6.3	2.4

### 2.2.3. 内部利用ローカルサーバへのウイルス対策ソフトの導入状況

ウイルス対策ソフトが「9割以上のローカルサーバに導入済み」であるのは7割強だが、パソコン向けウイルス対策と異なり、導入していない事業所も11.8%ある。

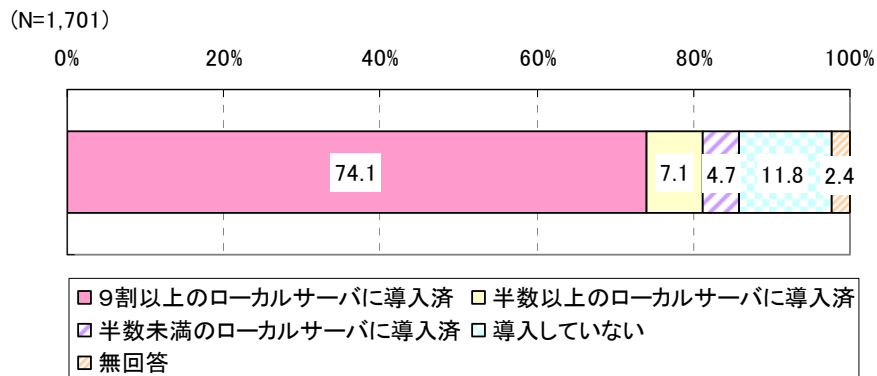


図 2.2-3 内部利用ローカルサーバへのウイルス対策ソフトの導入状況

表 2.2-3 内部利用ローカルサーバへのウイルス対策ソフトの導入状況（自治体との比較）

	N	9割以上のローカルサーバに導入済	半数以上のローカルサーバに導入済	半数未満のローカルサーバに導入済	導入していない	無回答
全体	1,701	74.1	7.1	4.7	11.8	2.4
企業	1,206	69.7	7.2	4.8	15.6	2.7
地方自治体	495	84.8	6.9	4.4	2.4	1.4

(%)

#### 2.2.4. ウイルス対策ソフトの導入・更新費用

ウイルス対策ソフトの導入・更新にかけた費用は3割が「1万～49万円」で最も多く、次いで「200万円～」(18.1%)、「100万～199万円」(16.6%)、「50万～99万」(15.1%)であった。企業においては業種群Ⅰ／業種群Ⅱの違いはほとんど見られない。なお、回答企業・自治体全体の平均は、142.5万円であったが、自治体の方が平均は高かった。総従業員別に見ると、導入・更新費用は導入ライセンス数に拠るため、総従業員数が多いほどウイルス対策ソフトの導入・更新費用は高い傾向にある。自治体の平均が高いのは、総従業員数の平均の差異によると推測される。

(N=1,701)

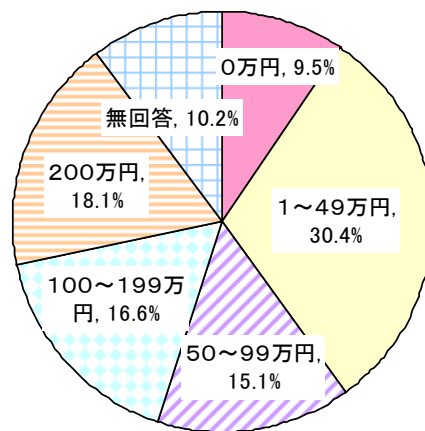


図 2.2-4 ウイルス対策ソフトの導入・更新費用

表 2.2-4 ウイルス対策ソフトの導入・更新費用（自治体との比較）

	N	0万円	1～49万円	50～99万円	100～199万円	200万円～	無回答
全体	1,701	9.5	30.4	15.1	16.6	18.1	10.2
企業	1,206	11.1	39.6	12.4	12.9	13.7	10.3
地方自治体	495	5.7	7.9	21.6	25.9	28.9	10.1

表 2.2-5 ウイルス対策ソフトの導入・更新費用の平均（総従業員による比較）

	N	更新費用平均 (万円)	パソコン台数平均 (台)	(参考)N パソコン台数 記入者
99名以下	316	316.0	50.2	342
100～299名	362	362.0	182.5	393
300～999名	496	496.0	465.9	530
1,000名以上	308	308.0	2877.9	344

### 2.2.5. 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、「特に実施していない」3割を除くと、約7割がなんらかの形で実施していると考えられる。しかし、最も多いのは「情報を収集・配布」(59.1%)と簡易なものであり、「社内でセミナー等を開催」や「外部の教育機関・セミナー等を利用」等、積極的な教育を行っているのはそれぞれ21.5%、6.6%と少ない。今回の回答自治体は規模が大きいため、「社内でセミナー等を開催」しているのは4割を超え、企業と比較すると非常に高い。

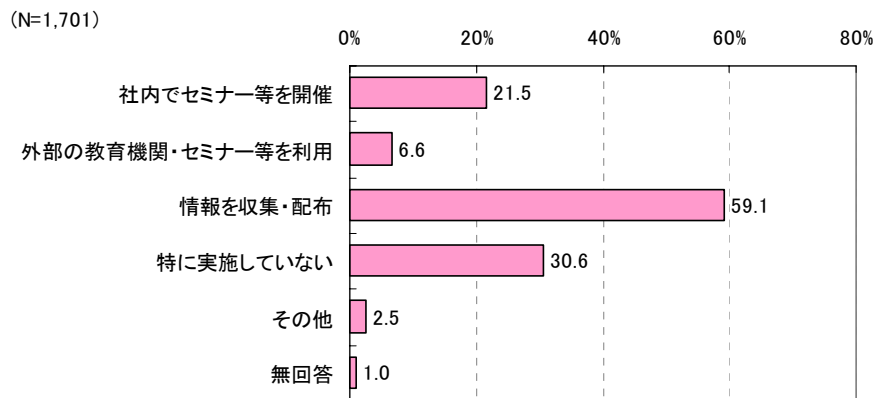


図 2.2-5 ウイルス対策に関するユーザ教育

表 2.2-6 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	情報を収集・配布	特に実施していない	その他	無回答
全体	1,701	21.5	6.6	59.1	30.6	2.5	1.0
企業	1,206	13.4	3.2	55.1	37.5	2.7	1.2
地方自治体	495	41.0	14.9	68.9	13.7	1.8	0.6

表 2.2-7 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別）

	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	情報を収集・配布	特に実施していない	その他	無回答
全体	1,701	21.5	6.6	59.1	30.6	2.5	1.0
感染した	265	22.3	4.9	63.4	27.5	3.4	1.1
ウイルスを発見したが、感染には至らなかった	909	25.1	7.7	65.3	24.8	2.6	0.6
感染も発見もしなかった	508	15.2	5.9	46.7	42.5	1.8	0.4
無回答	19	5.3	0.0	31.6	31.6	0.0	36.8

### 2.2.6. ウイルス対策に関する社内体制

専任・兼任を問わず、組織内にウイルス対策の専門部署（担当者）が設置されているのは7割を超える。自治体では「専門部署（担当者）がある」のが半数を超える。

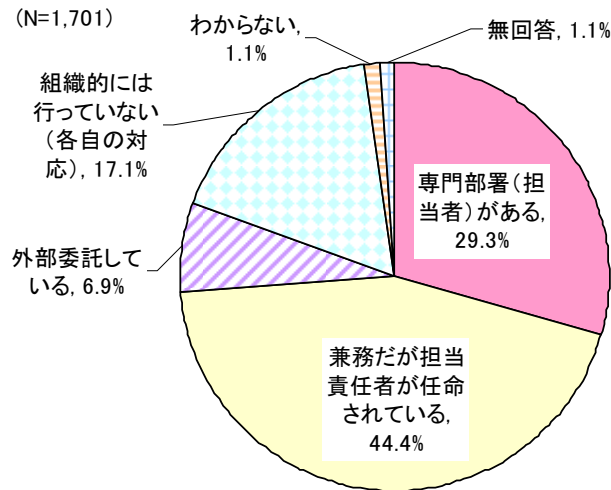


図 2.2-6 ウイルス対策に関する社内体制

表 2.2-8 ウイルス対策に関する社内体制（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されている	外部委託している	組織的には行っていない(各自の対応)	わからない	無回答
全体	1,701	29.3	44.4	6.9	17.1	1.1	1.1
企業	1,206	20.1	47.0	7.6	22.7	1.4	1.2
地方自治体	495	51.9	38.2	5.3	3.4	0.4	0.8

### 2.2.7. セキュリティパッチ（Windows Update など）の適用

クライアント、ネットワークサーバは3割以上が、ローカルサーバは4分の1程度が、「常に最新のパッチを適用」している。

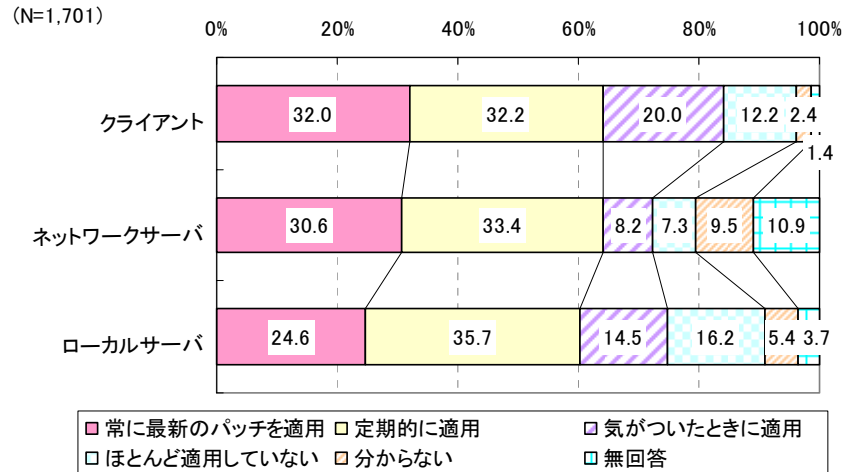


図 2.2-7 セキュリティパッチ（Windows Update など）の適用

表 2.2-9 セキュリティパッチ（Windows Update など）の適用（自治体との比較）

クライアント (%)

	N	常に最新のパッチを適用	定期的に応用	気がついたときに適用	ほとんど適用していない	分からない	無回答
全体	1,701	32.0	32.2	20.0	12.2	2.4	1.4
企業	1,206	32.2	27.6	23.1	12.4	3.0	1.7
地方自治体	495	31.5	43.2	12.3	11.5	0.8	0.6

ネットワークサーバ (%)

	N	常に最新のパッチを適用	定期的に応用	気がついたときに適用	ほとんど適用していない	分からない	無回答
全体	1,701	30.6	33.4	8.2	7.3	9.5	10.9
企業	1,206	29.6	27.7	8.3	8.3	12.4	13.7
地方自治体	495	33.1	47.3	8.1	4.8	2.4	4.2

ローカルサーバ (%)

	N	常に最新のパッチを適用	定期的に応用	気がついたときに適用	ほとんど適用していない	分からない	無回答
全体	1,701	24.6	35.7	14.5	16.2	5.4	3.7
企業	1,206	24.5	30.6	16.0	17.7	6.5	4.7
地方自治体	495	24.6	48.1	10.7	12.5	2.8	1.2

## 2.3. コンピュータウイルス対策に対する意識

### 2.3.1. コンピュータウイルスに関連して知りたいと思っている情報

ウイルスに関して知りたいと思っている情報は「感染した時の復旧方法」(60.4%)と「感染しないための方法や対策」(57.7%)の2項目の割合が企業・自治体とも高い。

また、「その他」を除いた全ての情報において、企業より自治体のほうが知りたいと思う率が高く、特に「ウイルスが悪用する脆弱性の情報」を知りたいと思うのは、自治体の方が20.8ポイントも高い。

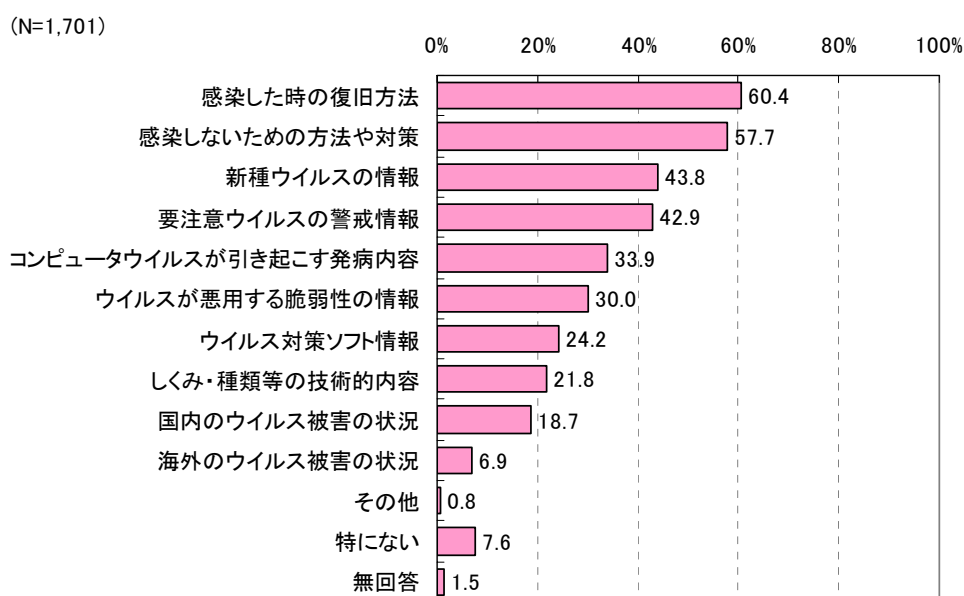


図 2.3-1 コンピュータウイルスに関連して知りたいと思っている情報

表 2.3-1 コンピュータウイルスに関連して知りたいと思っている情報（自治体との比較）

	N	感染した時の復旧方法	感染しないための方法や対策	新種ウイルスの情報	要注意ウイルスの警戒情報	コンピュータウイルスが引き起こす発病内容	ウイルスが悪用する脆弱性の情報	ウイルス対策ソフト情報
全体	1,701	60.4	57.7	43.8	42.9	33.9	30.0	24.2
企業	1,206	57.7	53.7	39.2	38.6	30.3	24.0	22.4
地方自治体	495	66.9	67.5	54.9	53.1	42.6	44.8	28.5

(%)

	N	しくみ・種類等の技術的内容	国内のウイルス被害の状況	海外のウイルス被害の状況	その他	特になし	無回答
全体	1,701	21.8	18.7	6.9	0.8	7.6	1.5
企業	1,206	18.0	15.9	6.4	1.1	9.9	1.8
地方自治体	495	31.1	25.5	8.1	0.2	2.2	0.8

(%)

時系列で見ると、回答の多い「感染した時の復旧方法」や「感染しないための方法や対策」の比率は落ち着きつつある反面、「新種ウイルスの情報」や「要注意ウイルスの警戒情報」の比率は2005年に若干上がっており、新たなタイプのウイルスや経済的利益を得ることを目的とした悪質なウイルスが増加していることが背景にあるとも推測される。

ウイルス対策に関する社内体制別に見ると、ウイルス対策に関する体制が整備されていない組織は、「新種ウイルスの情報」や「要注意ウイルスの警戒情報」より「感染しないための方法や対策」を知りたいと思う率が高い。

表 2.3-2 コンピュータウイルスに関連して知りたいと思っている情報（時系列）

	(%)						
	1999年 (N=1,505)	2000年 (N=1,674)	2001年 (N=1,755)	2002年 (N=1,791)	2003年 (N=1,115)	2004年 (N=1,124)	2005年 (N=1,675)
しくみ・種類等の技術的内容	31.6	26.8	26.7	25.4	25.4	23.8	22.1
感染した時の復旧方法	68.5	64.8	68.1	64.3	63.3	62.1	61.3
感染しないための方法や対策	62.7	57.8	66.0	60.4	61.9	61.0	58.6
ウイルス対策ソフト情報	46.9	38.2	38.7	27.0	22.9	21.1	24.5
コンピュータウイルスが引き起こす発病内容	48.0	37.6	41.6	34.8	31.5	28.6	34.4
国内のウイルス被害の状況	33.2	22.4	18.7	19.5	15.8	15.7	19.0
海外のウイルス被害の状況	16.4	12.8	11.3	8.4	5.7	6.7	7.0
ウイルスが悪用する脆弱性の情報	-	-	-	-	-	-	30.5
要注意ウイルスの警戒情報	-	48.9	54.4	50.7	39.7	39.9	43.5
新種ウイルスの情報	-	49.2	54.9	53.0	45.7	40.2	44.5
その他	1.9	1.1	1.5	0.8	1.3	0.5	0.8
特にない	6.4	5.0	4.2	5.8	9.4	10.6	7.8

注) 時系列結果の比較のため、無回答を除いて2004年、2005年の値を再集計しており、前頁および前表の比率と異なる。

表 2.3-3 コンピュータウイルスに関連して知りたいと思っている情報  
(ウイルス対策に関する社内体制別)

	(%)					
	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	コンピュータ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
専門部署(担当者)がある(N=499)	28.3	60.9	57.1	26.3	39.1	23.8
兼務だが担当責任者が任命されている(N=756)	21.4	62.0	57.5	23.3	34.8	17.5
外部委託している(N=118)	12.7	50.0	55.1	19.5	26.3	12.7
組織的には行っていない(各自の対応)(N=291)	16.2	62.5	61.2	26.8	27.8	16.5
わからない(N=19)	15.8	42.1	63.2	5.3	26.3	15.8
無回答(N=18)	16.7	27.8	38.9	11.1	11.1	5.6

	(%)					
	海外のウイルス被害の状況	要注意ウイルスの警戒情報	ウイルスが悪用する脆弱性の情報	新種ウイルスの情報	その他	特にない
専門部署(担当者)がある(N=499)	8.6	52.5	39.7	57.1	0.4	5.4
兼務だが担当責任者が任命されている(N=756)	7.5	44.6	32.1	43.8	1.1	6.0
外部委託している(N=118)	4.2	30.5	13.6	33.1	0.0	11.9
組織的には行っていない(各自の対応)(N=291)	3.4	28.9	16.5	28.2	1.4	12.7
わからない(N=19)	5.3	21.1	10.5	26.3	0.0	26.3
無回答(N=18)	5.6	33.3	22.2	16.7	0.0	11.1

### 2.3.2. 「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」を何らかの形で認知しているのは約6割であるが、そのうち約半数は「存在は知っている」程度に留まる。

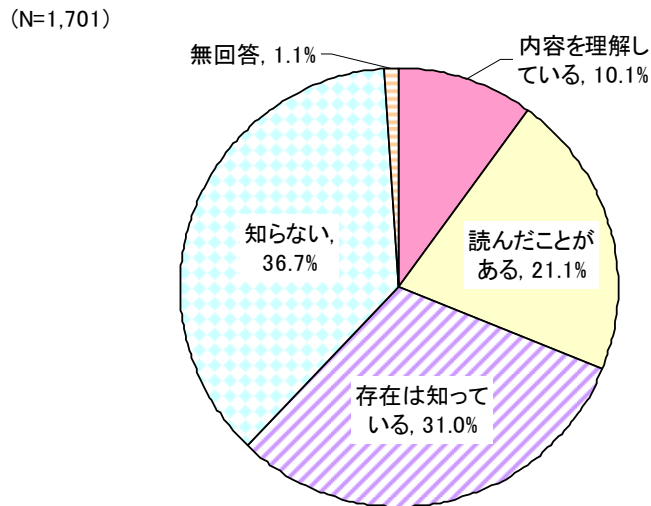


図 2.3-2 「コンピュータウイルス対策基準」の認知度

表 2.3-4 「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	1,701	10.1	21.1	31.0	36.7	1.1
企業	1,206	8.0	17.6	29.4	43.6	1.4
地方自治体	495	15.4	29.7	34.7	19.8	0.4

時系列で見ると、2003年、2004年の認知度はいったん下がっているが、2005年は2002年の水準とほぼ同程度に回復している。

就業者規模別では、総就業者が多いほど「内容を理解している」「読んだことがある」比率が高く、結果的に認知度も高まっている。

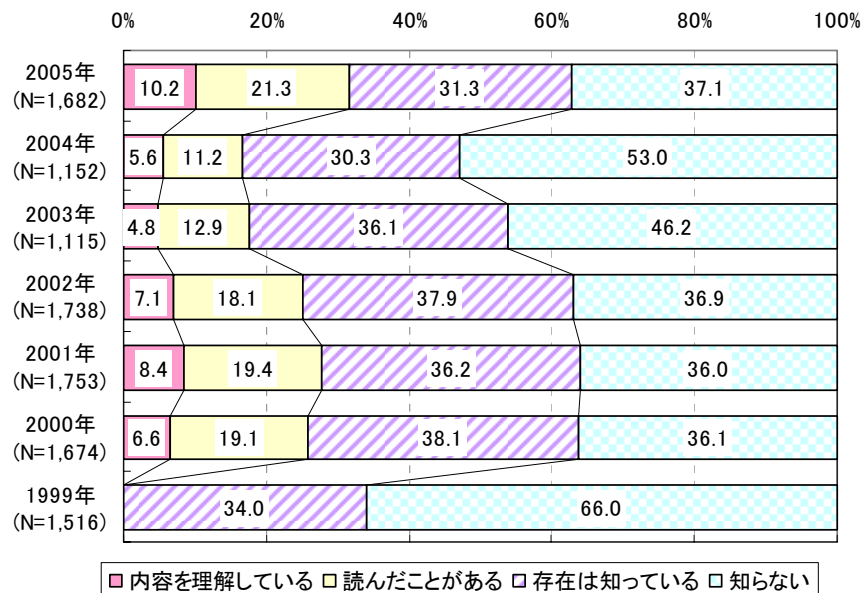


図 2.3-3 「コンピュータウイルス対策基準」の認知度の推移（時系列）

注1) 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2004年、2005年の値を再集計しており、前頁および前表の比率と異なる。

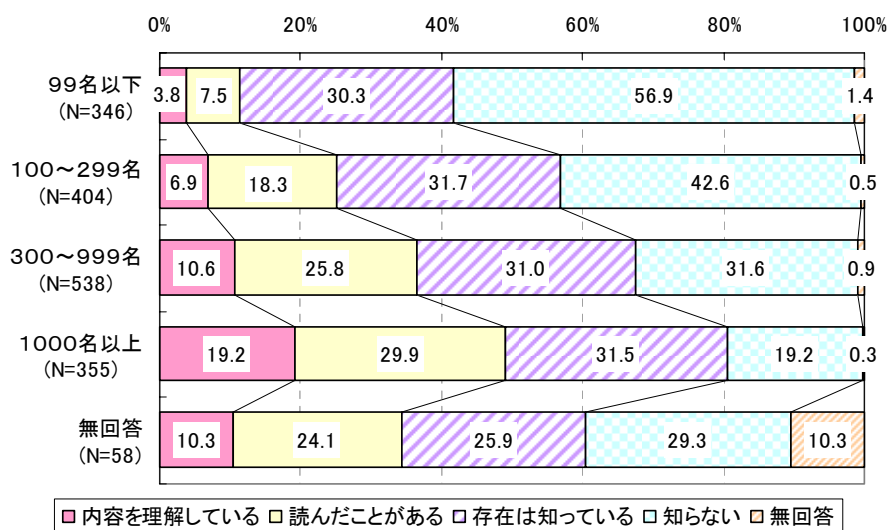


図 2.3-4 「コンピュータウイルス対策基準」の認知度（就業者規模別）

### 2.3.3. 被害届出について

#### (1)届出機関としてのIPA の認知度

コンピュータウイルス被害の拡大と再発防止のために、IPA がウイルスに関する届出を受け付ける指定機関になっていることを知っているのは半数強である。地方自治体では、7割近くが届出機関であることを知っている。

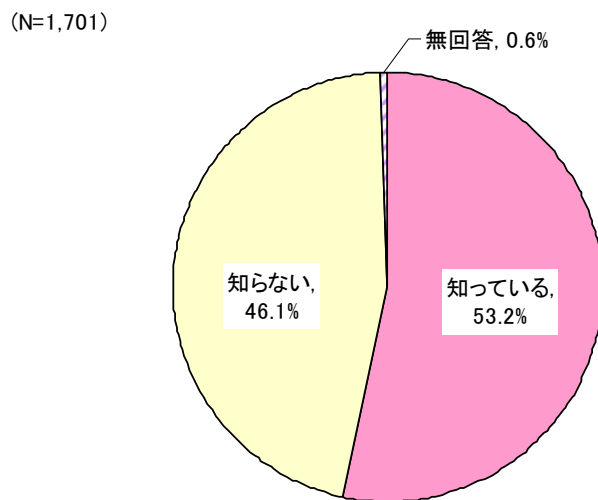


図 2.3-5 届出機関としてのIPA の認知度

表 2.3-5 届出機関としてのIPA の認知度（自治体との比較）

	N	認知度 (%)		
		知っている	知らない	無回答
全体	1,701	53.2	46.1	0.6
企業	1,206	46.4	52.7	0.8
地方自治体	495	69.7	30.1	0.2

時系列で見ると、2003年、2004年は認知度が大きく下がっているが、2005年は2002年の水準に近づいている。就業者規模別では、総就業者が多いほど認知度が高い。また、ウイルス対策に係わる社内体制別では、専門部署（担当者）がある方が認知度が高い。

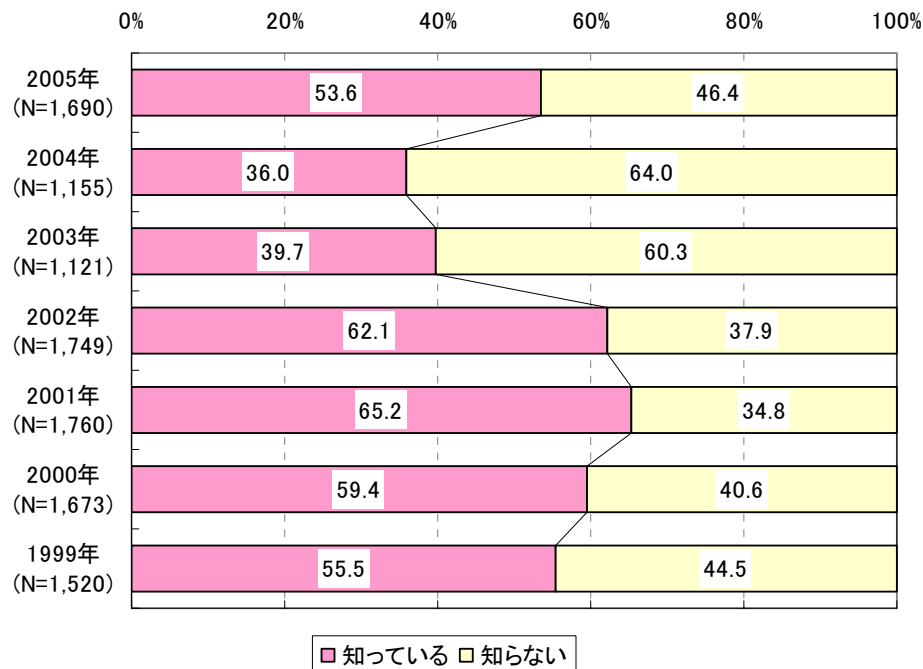


図 2.3-6 届出機関としてのIPAの認知度推移（時系列）

注）時系列結果の比較のため、無回答を除いて2004年、2005年の値を再集計しており、前頁および前表の比率と異なる。

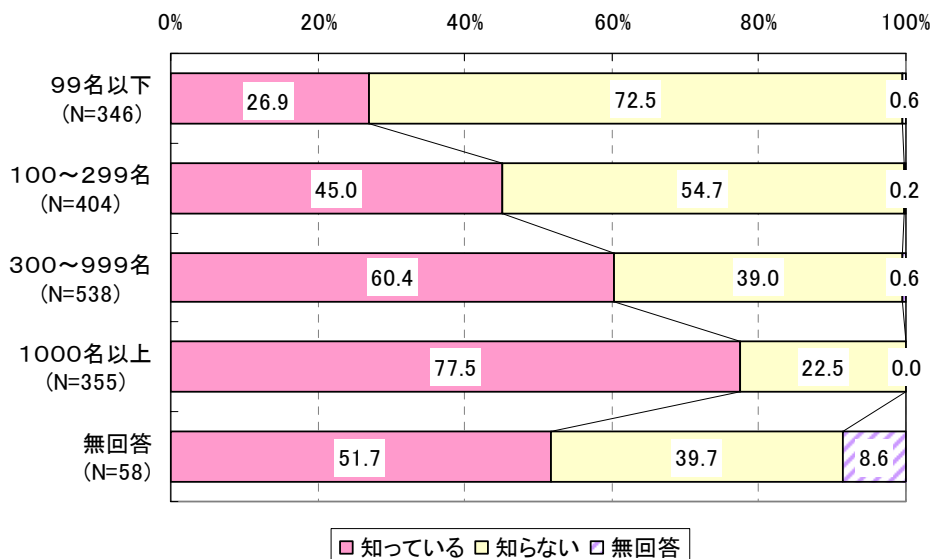


図 2.3-7 届出機関としてのIPAの認知度（就業者規模別）

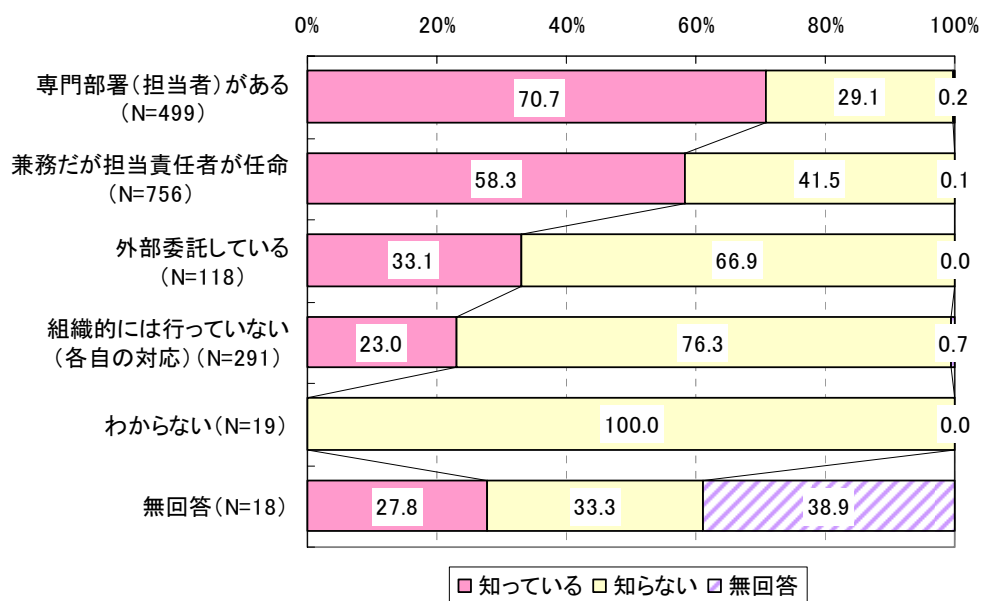


図 2.3-8 届出機関としてのIPA の認知度 (ウイルス対策に関する社内体制別)

## (2)届出の実施

今後感染が発見された際に、IPAへ届け出る意向があるのは全体で3割強に留まるが、地方自治体では半数を超える。

(N=1,701)

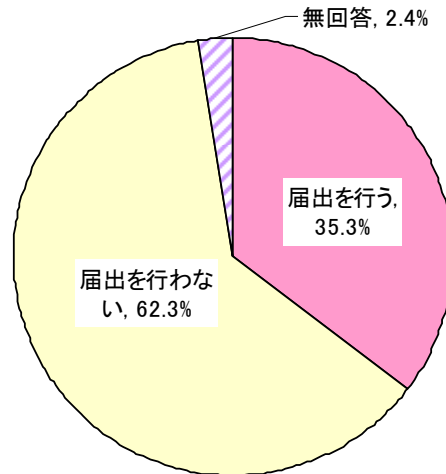


図 2.3-9 届出の実施

表 2.3-6 届出の実施（自治体との比較）

	N	届出を行う	届出を行わない	無回答
全体	1,701	35.3	62.3	2.4
企業	1,206	27.4	69.8	2.8
地方自治体	495	54.7	44.0	1.2

時系列で見ると、「届出を行う」率は2002年以降減少を続けている。IPAを届出機関として知っている企業・地方自治体については、今後感染が感染されたときIPAに届出を行おうとするのが半数近くに達するが、2004年は知っている場合に届出を行うと回答したのは61.5%であり、2004年度の結果と比較すると、低い水準に留まっている。

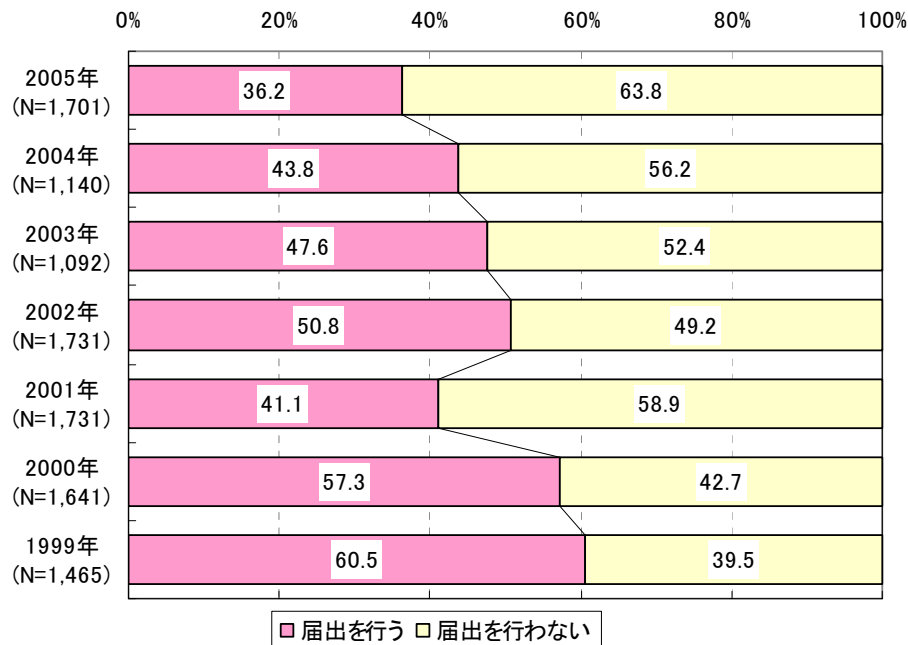


図 2.3-10 届出の実施推移（時系列）

注) 時系列結果の比較のため、無回答を除いて2004年、2005年の値を再集計しており、前頁および前表の比率と異なる。

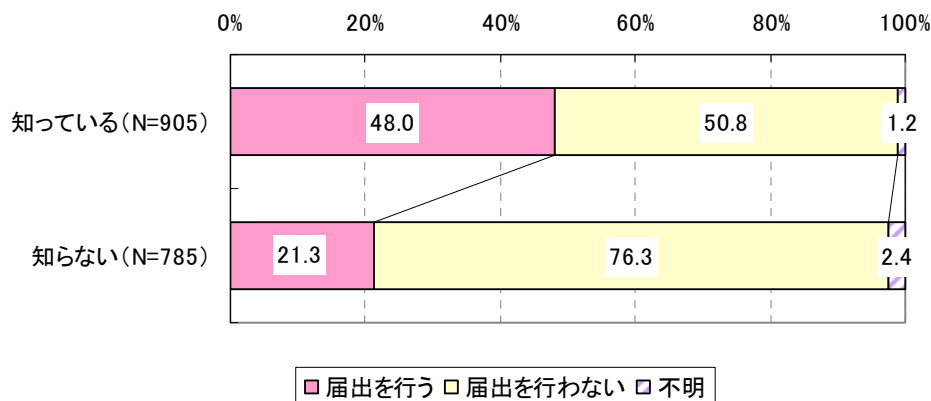


図 2.3-11 届出の実施（被害届出機関としてのIPAの認知度別）

### (3) 届け出を行わない理由

IPA への届出を行わない理由については、「被害が大きければ届出する」(45.6%)、「届出方法が不明なため」(39.4%)の回答が多い。しかし、企業では「届出方法が不明なため」(42.4%)の回答が「被害が大きければ届出する」(41.8%)を上回る。

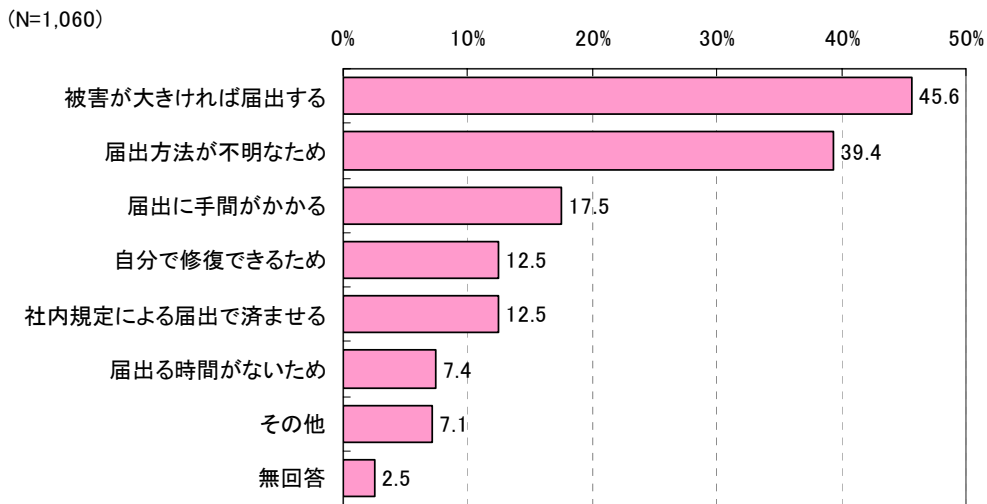


図 2.3-12 届出を行わない理由

表 2.3-7 届出を行わない理由（自治体との比較）

(%)

	N	被害が大きければ届出する	届出方法が不明なため	届出に手間がかかる	自分で修復できるため	社内規定による届出で済ませる	届出る時間がないため	その他	無回答
全体	1,060	45.6	39.4	17.5	12.5	12.5	7.4	7.1	2.5
企業	842	41.8	42.2	18.9	13.9	11.9	8.4	7.1	2.3
地方自治体	218	60.1	28.9	11.9	7.3	14.7	3.2	6.9	3.2

2004年調査と比較すると、「被害が大きければ届出する」が大きく15.9ポイント増加し、「届出方法が不明なため」が13.2ポイント減少していることが特徴的である。「IPAに届出しない」とした回答者における企業の割合は、2004年調査では76.8%、2005年調査では79.4%とほぼ変わりはないため、比較は妥当と考えられる。

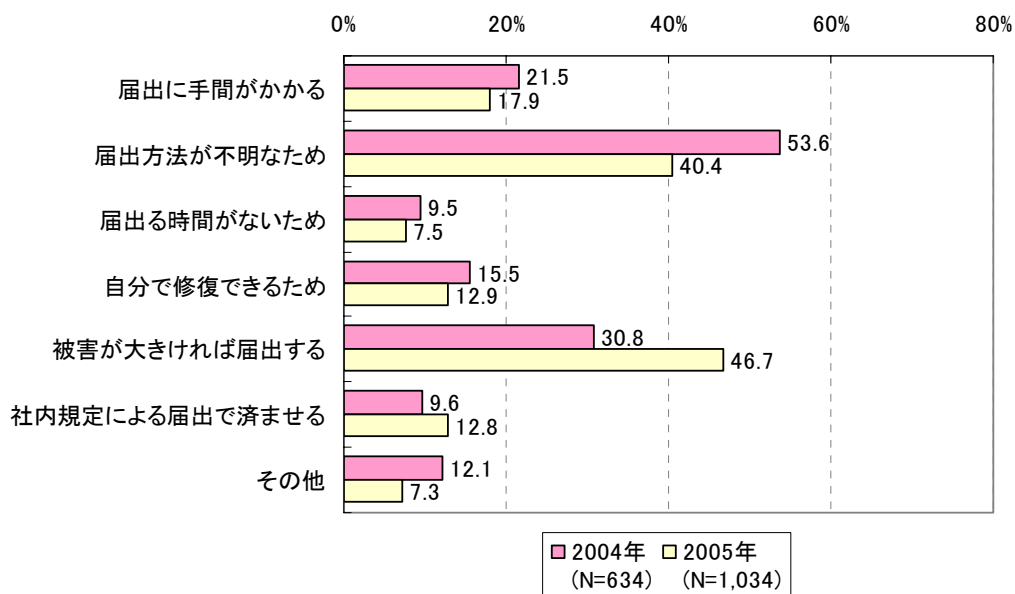


図 2.3-13 届出を行わない理由（時系列）

## 2.4. コンピュータウイルスによる被害状況

### 2.4.1. コンピュータウイルス遭遇（感染または発見）経験

2005年1月から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53.4%となっており、「感染したことがある」（15.6%）と合わせると、69.0%が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。

(N=1,701)

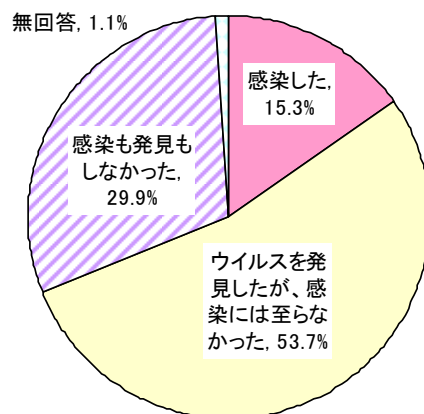


図 2.4-1 コンピュータウイルス遭遇（感染または発見）経験

表 2.4-1 コンピュータウイルス遭遇（感染または発見）経験（自治体との比較）

	N	感染した	ウイルスを発見したが、感染には至らなかった	感染も発見もしなかった	無回答
全体	1,701	15.3	53.7	29.9	1.1
企業	1,206	17.6	47.9	33.2	1.3
地方自治体	495	9.7	67.9	21.8	0.6

(%)

時系列で見ると、コンピュータウイルスの遭遇率は2002年で最大となったものの、2003年に10ポイント程度減少した後はほぼ横ばいとなっている。

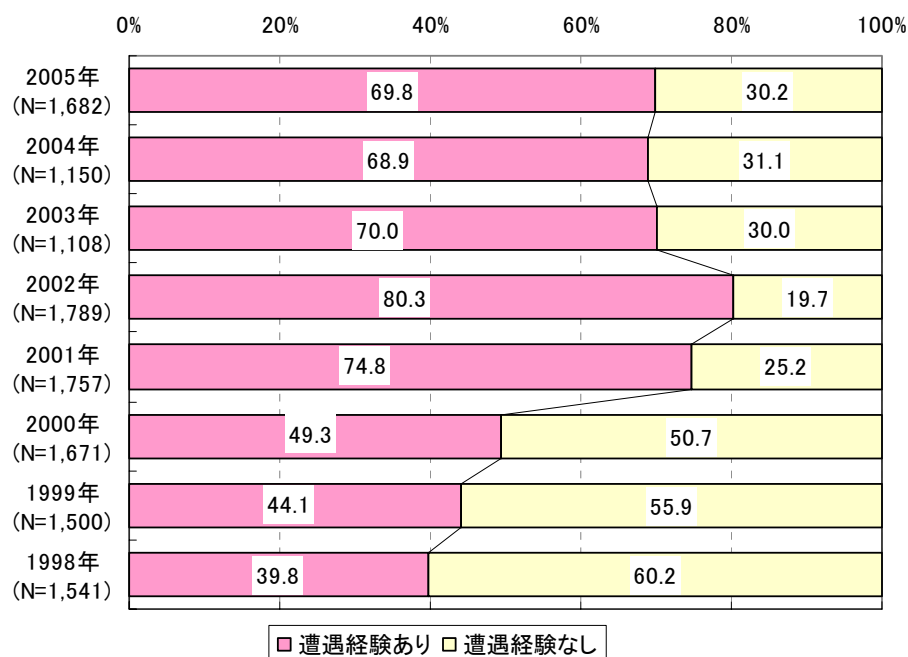


図 2.4-2 コンピュータウイルス遭遇（感染または発見）経験の推移（時系列）

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2004年、2005年の値を再集計しており、前頁および前表の比率と異なる。

表 2.4-2 コンピュータウイルス遭遇（感染または発見）経験（業種別）

	N	遭遇率 (%)	うち感染率 (%)
全体	1,701	69.0	22.2
農林漁業・鉱業	16	43.8	42.9
建設業	66	63.7	26.2
機械器具製造業	61	73.8	44.4
他の製造業	229	69.0	25.9
電気・ガス・熱供給・水道業	21	71.4	20.0
情報通信業	205	76.6	31.2
運輸業	96	60.5	19.0
卸売業	95	74.7	25.3
小売業	80	65.1	17.4
金融・保険業	127	44.8	8.7
不動産業	20	70.0	14.3
飲食店・宿泊業	19	52.6	30.0
他のサービス業	171	60.8	35.5
自治体・公共団体	495	77.6	12.5

業種別に遭遇経験を見ると、遭遇率（「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」比率の合計）は「地方自治体」が77.6%で最も多く、「情報通信業」（76.6%）、「卸売業」（74.7%）、「機械器具製造業」（73.8%）、「電気・ガス・熱供給・水道業」（71.4%）と続く。しかし感染率（遭遇したうち、一度でも感染した比率）では、「機械器具製造業」が44.4%で最も高く、次いで「農林漁業・鉱業」（42.9%）、「他のサービス業」（35.5%）である。遭遇率と感染率の関係では、遭遇率は高いが感染率が低いのが「電気・ガス・水道・熱供給」および「地方自治体」の公的サービスを提供する重要インフラ事業者である。同じ重要インフラ事業者でも「金融・保険業」は遭遇率・感染率ともに低いのが特徴的である。また、重要インフラ事業者でも、情報通信業のみ感染率が平均より高く、情報通信業のサービス内容そのものが、他の業種より脅威にさらされていることが理由と考えられる。一方、「農林漁業・鉱業」「他のサービス業」「飲食店・宿泊業」など、コンピュータやインターネットへの依存度が低い業種においては、遭遇率は低いが感染率は高くなっている。就業者規模別では、総就業者数が多いほど遭遇率が高い。

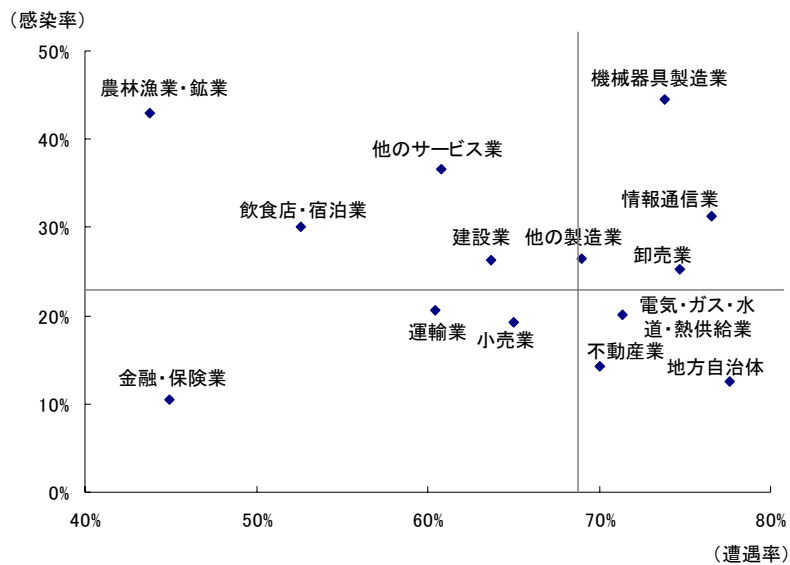


図 2.4-3 コンピュータウイルス遭遇（感染または発見）経験（業種別）

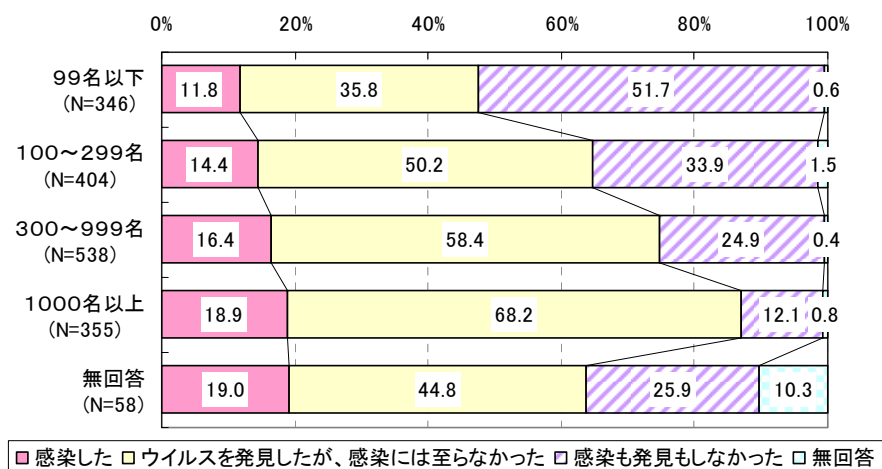


図 2.4-4 コンピュータウイルス遭遇（感染または発見）経験（就業者規模別）

### 2.4.2. 遭遇したウイルスの種類数

感染・発見したウイルスの種類数は、「5種類以上」が約4割で最も多い。時系列で見ても、「5種類以上」の割合はここ5年間で最も高い。

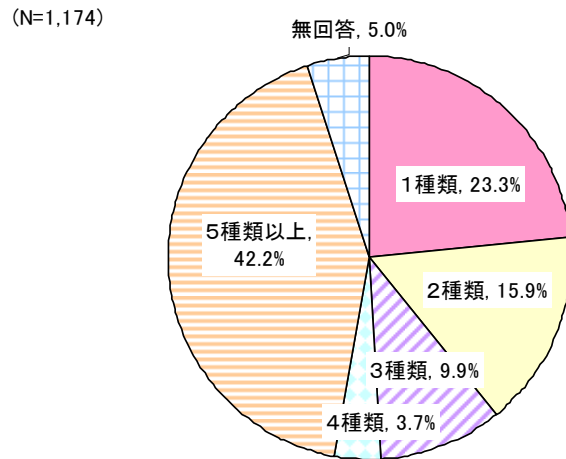


図 2.4-5 遭遇したウイルスの種類数

表 2.4-3 遭遇したウイルスの種類数（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	1,174	23.3	15.9	9.9	3.7	42.2	5.0
企業	790	27.0	17.6	10.9	3.3	36.5	4.8
地方自治体	384	15.6	12.5	7.8	4.7	53.9	5.5

(%)

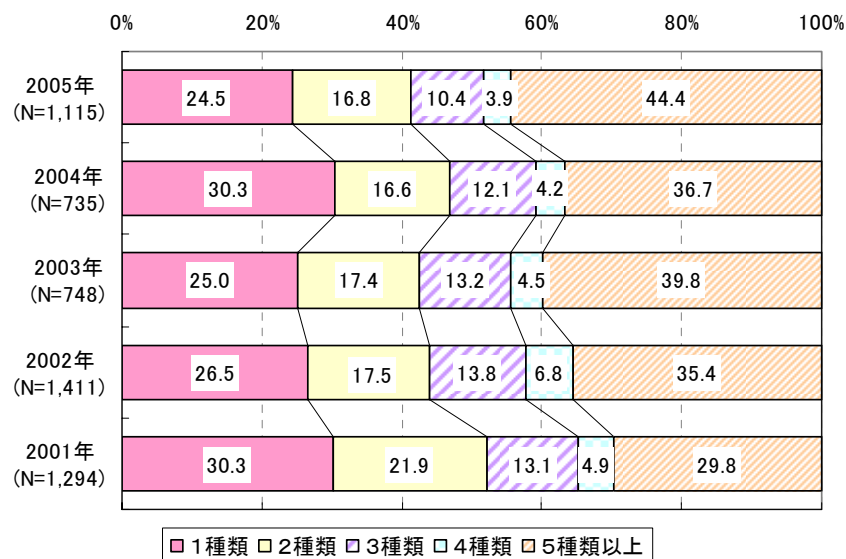


図 2.4-6 遭遇したウイルスの種類数（時系列）

注) 時系列結果の比較のため、無回答を除いて2004年、2005年の値を再集計しており、前表の比率と異なる。

### 2.4.3. 遭遇したウイルスの名称

2005年に感染・発見したウイルスは「W32/Netsky」が群を抜いて高く6割近くに達する。その他、「W32/Klez」（30.2%）、「W32/Mydoom」（27.2%）、「W32/Bagle」（25.1%）、「W32/Mytob」（24.4%）、「W32/Sober」（20.7%）等が2割を超えている。

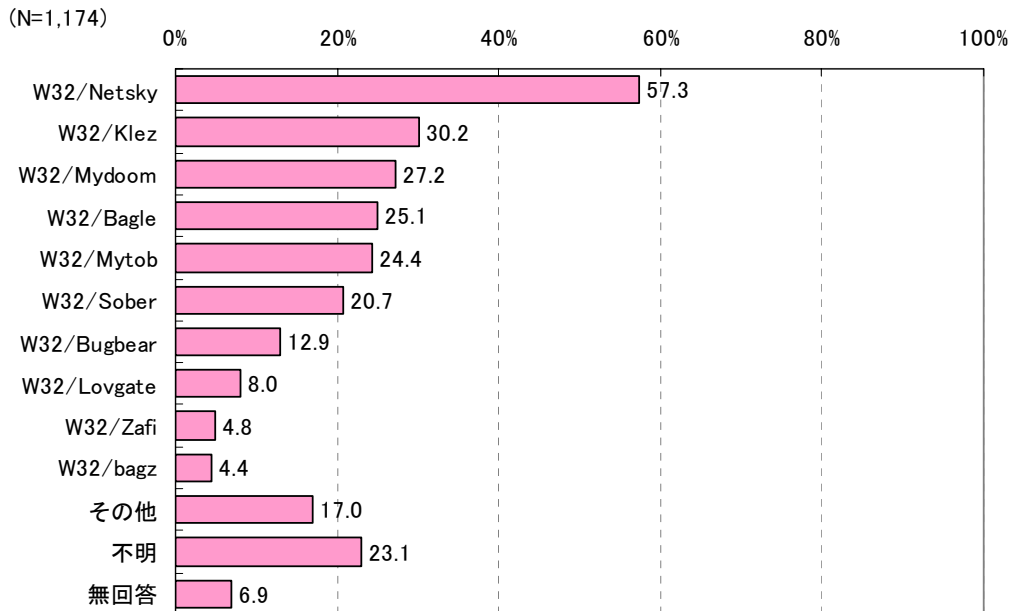


図 2.4-7 遭遇したウイルスの名称

表 2.4-4 遭遇したウイルスの名称（自治体との比較）

	N	W32/ Netsky	W32/ Klez	W32/ Mydoom	W32/ Bagle	W32/ Mytob	W32/ Sober	W32/ Bugbear
全体	1,174	57.3	30.2	27.2	25.1	24.4	20.7	12.9
企業	790	51.5	25.1	25.2	23.7	21.8	20.5	12.8
地方自治体	384	69.3	40.9	31.3	28.1	29.7	21.1	13.3

	N	W32/ Lovgate	W32/ Zafi	W32/ Bagz	その他	不明	無回答
全体	1,174	8.0	4.8	4.4	17.0	23.1	6.9
企業	790	7.1	4.4	4.7	11.6	29.0	6.3
地方自治体	384	9.9	5.5	3.9	28.1	10.9	8.1

#### 2.4.4. ウイルスの感染件数

2005年にウイルスに感染したのは「1件」が4割弱である。なお、本設問は2004年調査と異なり、コンピュータウイルスに「感染したことがある」と回答した15.6%（260件）の回答者を対象として集計しており、「発見したが、感染には至らなかった」のは914件である。

(N=260)

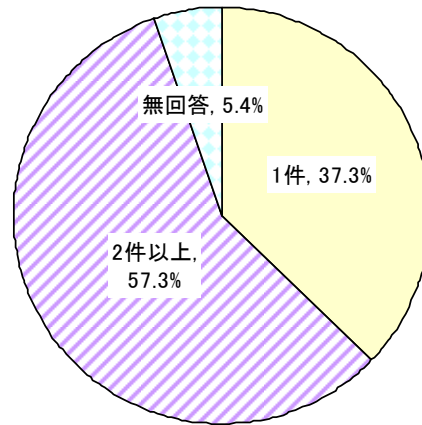


図 2.4-8 ウイルスの感染件数

表 2.4-5 ウイルスの感染件数（自治体との比較）

	N	1件	2件～	無回答
全体	260	37.3	57.3	5.4
企業	212	39.6	57.5	2.8
地方自治体	48	27.1	56.3	16.7

### 2.4.5. ウイルスに感染したパソコンの台数

感染したパソコンの年間延べ台数は「1～4台」が5割強であり、被害は小規模であると言える。なお、企業・自治体全体の平均は10.9台である。

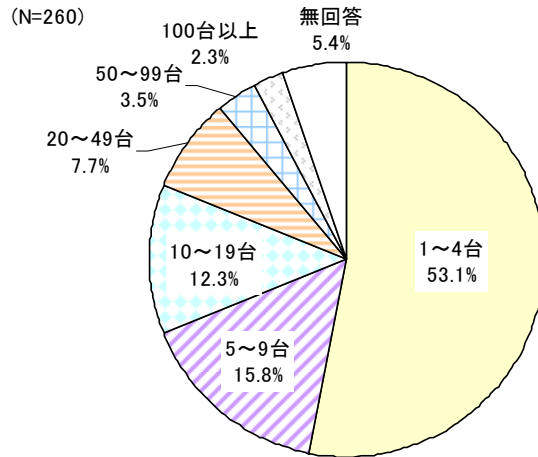


図 2.4-9 ウイルスに感染したパソコンの台数

表 2.4-6 ウイルスに感染したパソコンの台数（自治体との比較）

	N	1～4台	5～9台	10～19台	20～49台	50～99台	100台以上	無回答
全体	260	53.1	15.8	12.3	7.7	3.5	2.3	5.4
企業	212	54.7	16.0	11.8	8.0	2.8	2.4	4.2
地方自治体	48	45.8	14.6	14.6	6.3	6.3	2.1	10.4

#### 2.4.6. ウイルスの直接的な被害

ウイルス感染による直接的な被害は「システム停止・性能低下」が6割近くで最も多い。「その他」の内容は、「被害無し」が6割程度であったが、被害内容で最も多かったのは、担当部門の業務停滞に関するものであった。

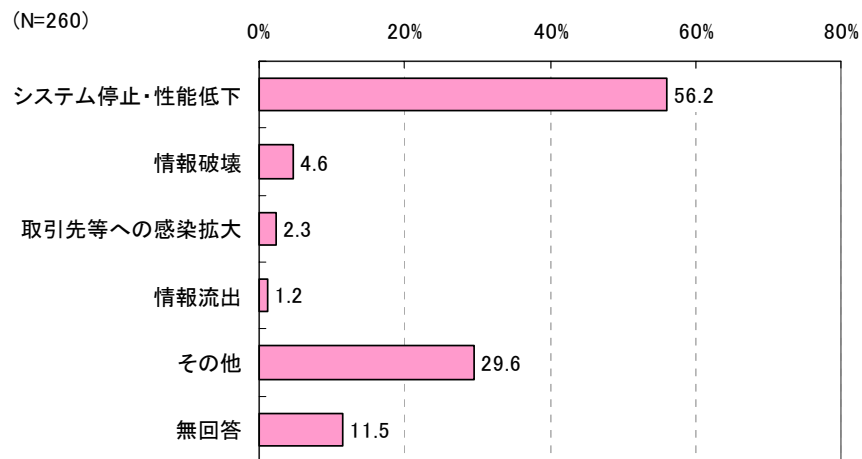


図 2.4-10 ウイルスの直接的な被害の有無

表 2.4-7 ウイルスの直接的な被害の有無（自治体との比較）

	N	システム停止・性能低下	情報破壊	取引先等への感染拡大	情報流出	その他	無回答
全体	260	56.2	4.6	2.3	1.2	29.6	11.5
企業	212	60.4	5.2	2.8	1.4	26.9	9.9
地方自治体	48	37.5	2.1	0.0	0.0	41.7	18.8

その他：被害無し（46件）、担当部門の業務停滞（12件）、スパム等メールの発信（8件）、パソコンの停止・性能低下（5件）、メール遅延（2件） ※2件以上の回答

#### 2.4.7. ウイルスの間接的な被害

ウイルス感染による間接的な被害は「その他」が4割を超え、その9割近くは「特に無し」との回答であった。風評等による企業価値の低下や損害賠償・広告への出稿等による実費負担に関しては、ほとんど懸念されていないことが示された。

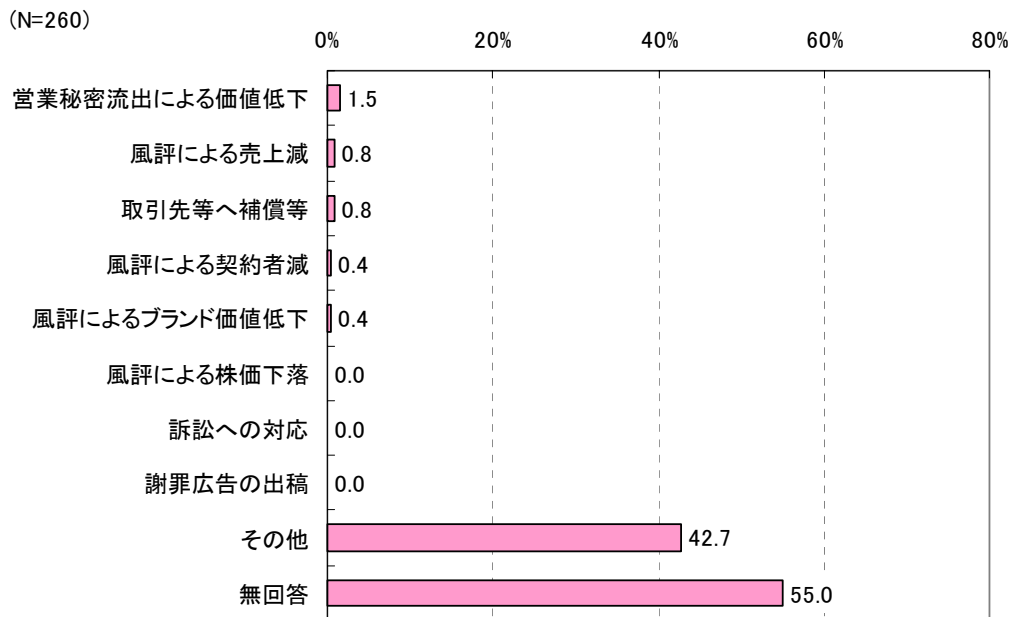


図 2.4-11 ウイルスの間接的被害の有無

表 2.4-8 ウイルスの間接的な被害の有無（自治体との比較）

	N	営業秘密流出による価値低下	風評による売上減	取引先等へ補償等	風評による契約者減	風評によるブランド価値低下	風評による株価下落	訴訟への対応	謝罪広告の出稿	その他	無回答
全体	260	1.5	0.8	0.8	0.4	0.4	0.0	0.0	0.0	42.7	55.0
企業	212	1.9	0.9	0.9	0.5	0.0	0.0	0.0	0.0	41.0	56.1
地方自治体	48	0.0	0.0	2.1	0.0	0.0	0.0	0.0	0.0	50.0	50.0

その他：被害無し（99件）、復旧作業・業務停滞・代替機器購入費用などの直接被害（18件）、取引先への謝罪、補償要求、取引先への信用低下など取引先に関する被害（3件）  
※2件以上の回答

## 2.4.8. 電子商取引（EC）業務

### (1) 電子取引業務の売上が全体の売上に占める割合

電子商取引業務の売上が全体売上額に与える影響は「なし」とする回答が7割近くで最も多い。

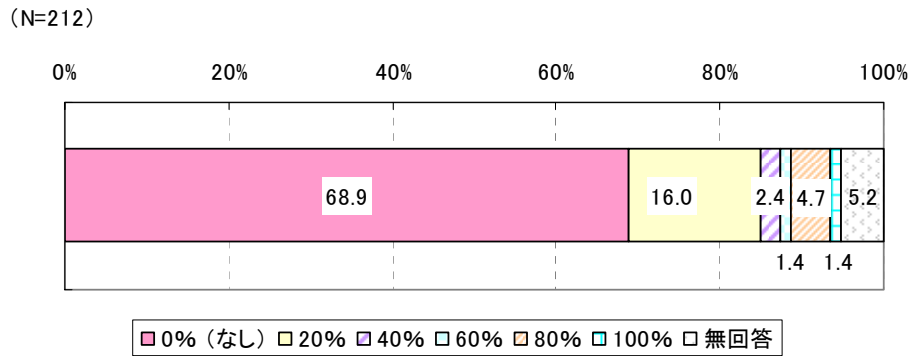


図 2.4-12 電子商取引（EC）業務の売上が全体の売上に占める割合  
（ウイルス感染経験あり、企業のみ）

### (2) 電子商取引業務が停止した年間の延べ日数

ウイルス感染は電子商取引に影響しなかったとする回答が9割近くに達する。

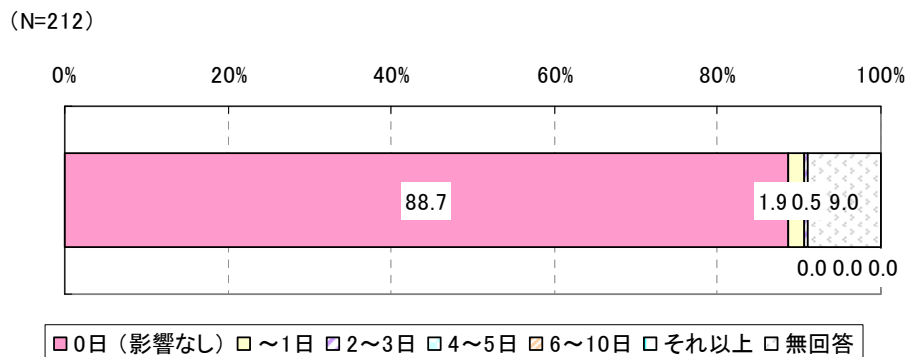


図 2.4-13 電子商取引業務が停止した年間延べ日数  
（ウイルス感染経験あり、企業のみ）

#### 2.4.9. インターネット公開の業務遂行上重要なサーバが停止した年間延べ日数

ウイルス感染は、インターネット公開の業務遂行上重要なサーバに影響しなかったとする企業・自治体が多い。

(N=260)

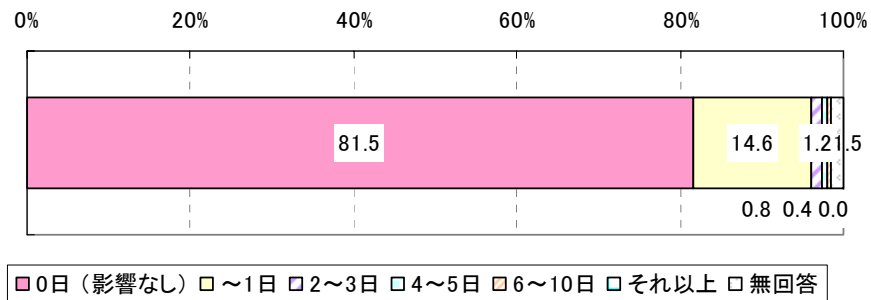


図 2.4-14 インターネット公開の業務遂行上重要なサーバが停止した年間延べ日数

表 2.4-9 インターネット公開の業務遂行上重要なサーバが停止した年間延べ日数  
(自治体との比較)

	N	0日(影響なし)	~1日	2~3日	4~5日	6~10日	それ以上	無回答
全体	260	81.5	14.6	1.2	0.8	0.4	0.0	1.5
企業	212	80.2	16.5	1.4	0.9	0.5	0.0	0.5
地方自治体	48	87.5	6.3	0.0	0.0	0.0	0.0	6.3

2.4.10. 事業所内のネットワークや社内の重要なサーバの利用が困難になった年間延べ日数  
 ウイルス感染は、事業所内のネットワークや社内の重要なサーバの利用に影響しなかったとする企業・自治体が8割近くに達する。

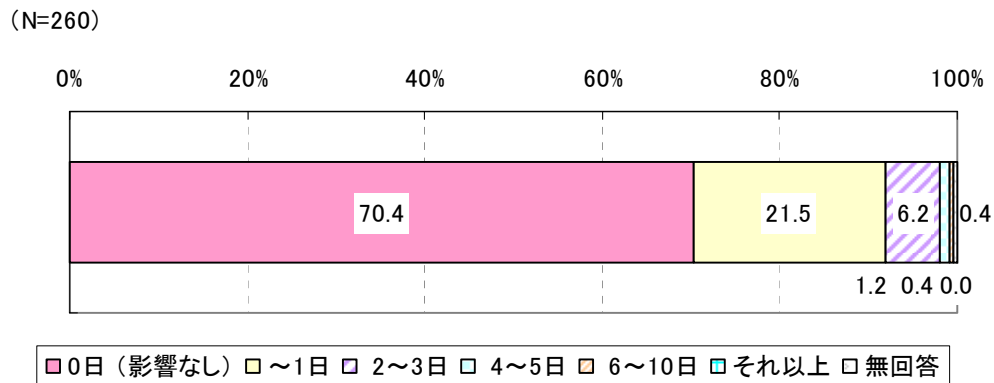


図 2.4-15 事業所内のネットワークや社内の重要なサーバの利用が困難になった年間延べ日数

表 2.4-10 事業所内のネットワークや社内の重要なサーバの利用が困難になった年間延べ日数  
 (自治体との比較)

	N	0日(影響なし)	~1日	2~3日	4~5日	6~10日	それ以上	無回答
全体	260	70.4	21.5	6.2	1.2	0.4	0.0	0.4
企業	212	66.5	24.1	7.1	1.4	0.5	0.0	0.5
地方自治体	48	87.5	10.4	2.1	0.0	0.0	0.0	0.0

#### 2.4.11. 2005年1年間のウイルス感染からの復旧作業延べ人日

情報管理部門が行ったウイルス感染からの復旧作業は、「0～1人・日」が最も多く4割強、次いで「2～3人・日」(31.3%)となっている。

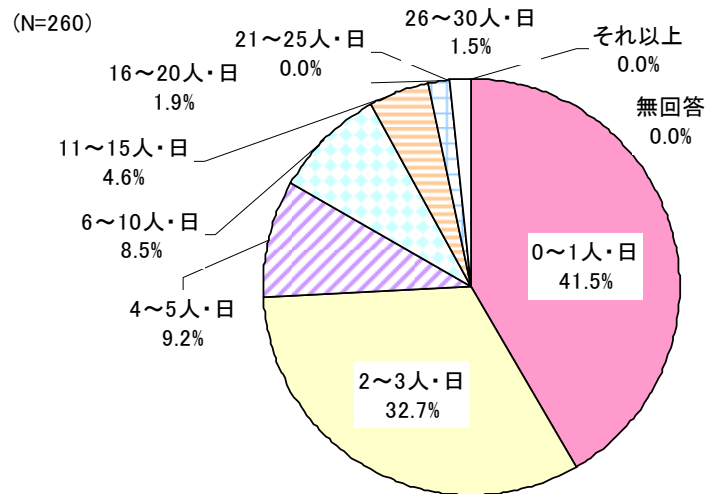


図 2.4-16 2005年1年間のウイルス感染からの復旧作業延べ人日

表 2.4-11 2005年1年間のウイルス感染からの復旧作業延べ人日  
(自治体との比較)

	N	0～1人・日	2～3人・日	4～5人・日	6～10人・日	11～15人・日	16～20人・日	21～25人・日	26～30人・日	それ以上	無回答
全体	260	41.5	32.7	9.2	8.5	4.6	1.9	0.0	1.5	0.0	1.5
企業	212	41.5	32.5	9.4	9.4	4.7	0.9	0.0	1.4	0.0	1.8
地方自治体	48	41.7	33.3	8.3	4.2	4.2	6.3	0.0	2.1	0.0	0.0

### 2.4.12. 2005年1年間にウイルス感染が原因で発生した追加データ処理作業人日

ウイルス感染によって業務部門が行った追加データ処理に要した年間延べ人日は、「0～1人・日」が8割を超える。

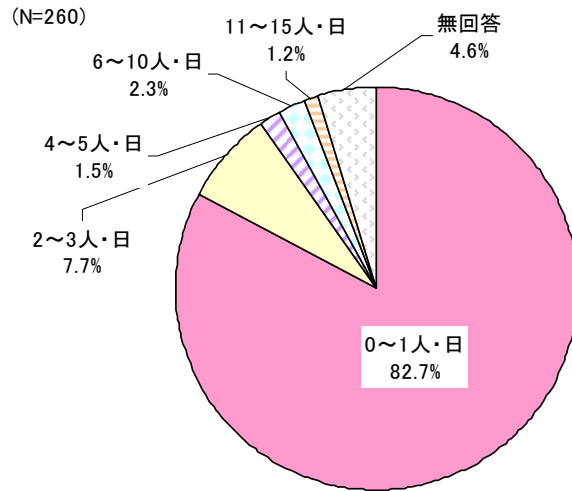


図 2.4-17 2005年1年間にウイルス感染が原因で発生した追加データ処理作業人日

表 2.4-12 2005年1年間に感染が原因で発生した追加データ処理作業人日  
(自治体との比較)

	N	0～ 1人・日	2～ 3人・日	4～ 5人・日	6～ 10人・日	11～ 15人・日	それ以上	無回答
全体	260	82.7	7.7	1.5	2.3	1.2	0.0	4.6
企業	212	81.6	9.0	1.9	2.4	1.4	0.0	3.8
地方自治体	48	87.5	2.1	0.0	2.1	0.0	0.0	8.3

#### 2.4.13. システム復旧に関して新たに購入した代替機器の費用

2005年の1年間にシステム復旧に関して新たに購入した代替機器の費用は、9割以上が「0百万円未満（なしを含む）」である。

**表 2.4-13 2005年1年間にシステム復旧に関して新たに購入した代替機器の費用  
(全体、自治体との比較)**

(百万円/年)					(%)				
	N	平均	最小値	最大値		N	0百万円未満 (なしを含む)	1百万円以上	無回答
全体	253	0.1	0.0	3.0	全体	253	93.2	4.2	2.6
企業	207	0.1	0.0	3.0	企業	207	92.6	5.1	2.3
地方自治体	46	0.0	0.0	0.0	地方自治体	46	95.8	0.0	4.2

#### 2.4.14. システム復旧に関して外部に発注した業務の費用

2005年の1年間にシステム復旧に関して外部に発注した費用は、9割以上が「0百万円未満（なしを含む）」である。

**表 2.4-14 2005年1年間にシステム復旧に関して外部に発注した業務の費用  
(全体、自治体との比較)**

(百万円/年)					(%)				
	N	平均	最小値	最大値		N	0百万円未満 (なしを含む)	1百万円以上	無回答
全体	251	0.0	0.0	3.0	全体	251	95.8	0.8	3.4
企業	206	0.0	0.0	3.0	企業	206	96.8	0.5	2.8
地方自治体	45	0.0	0.0	1.0	地方自治体	45	91.7	2.1	6.3

#### 2.4.15. システム復旧に関してその他に発生した費用

2005年の1年間にシステム復旧に関してその他に発生した費用は、9割以上が「0百万円未満（なしを含む）」である。

**表 2.4-15 2005年1年間にシステム復旧に関してその他に発生した費用  
(全体、自治体との比較)**

(百万円/年)					(%)				
	N	平均	最小値	最大値		N	0百万円未満 (なしを含む)	1百万円以上	無回答
全体	249	0.0	0.0	2.0	全体	249	94.7	1.1	4.2
企業	203	0.0	0.0	1.0	企業	203	94.9	0.9	4.1
地方自治体	46	0.0	0.0	2.0	地方自治体	46	93.8	2.1	4.2

## 2.4.16. 影響の最も大きかったウイルス

### (1) ウイルス名及び発見月

影響が最も大きかったウイルスは「W32/Netsky」との回答が17.0%で最も多かった。

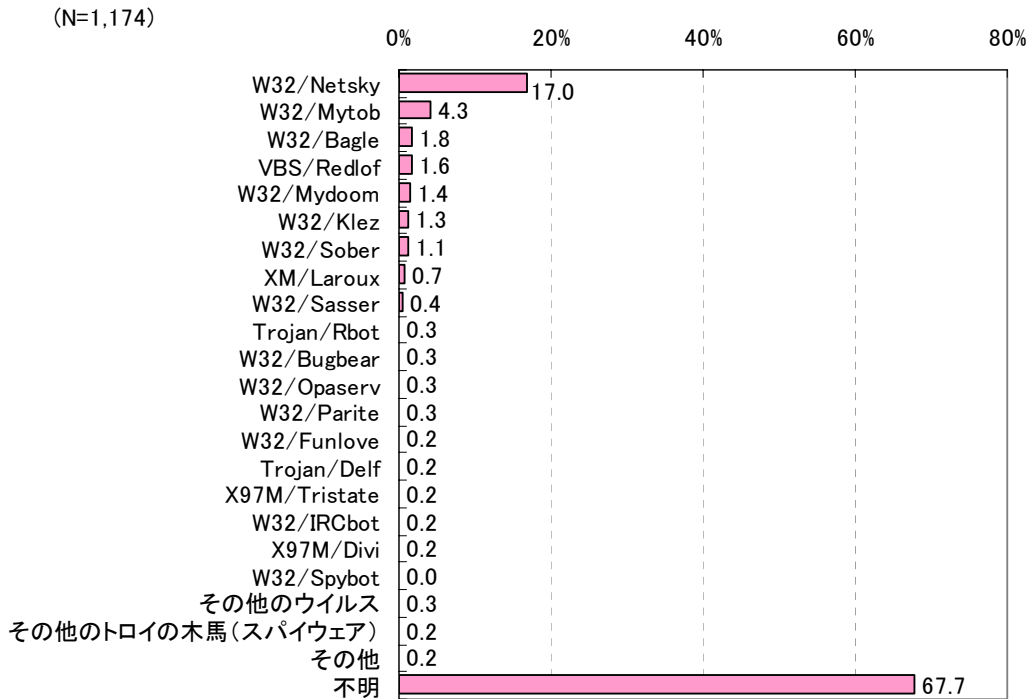


図 2.4-18 影響の最も大きかったウイルス名

表 2.4-16 影響の最も大きかったウイルス名（自治体との比較）

	N	W32/ Netsky	W32/ Mytob	W32/ Bagle	VBS/ Redlof	W32/ Mydoom	W32/ Klez	W32/ Sober	XM/ Laroux
全体	1,174	17.0	4.3	1.8	1.6	1.4	1.3	1.1	0.7
企業	790	13.8	4.7	1.9	0.5	1.8	1.6	1.6	0.0
地方自治体	384	23.4	3.4	1.6	3.9	0.5	0.5	0.0	2.1

	N	W32/ Sasser	Trojan/ Rbot	W32/ Bugbear	W32/ Opaserv	W32/ Parite	W32/ Funlove	Trojan/ Delf	X97M/ Tristate
全体	1,174	0.4	0.3	0.3	0.3	0.3	0.2	0.2	0.2
企業	790	0.4	0.5	0.5	0.4	0.3	0.3	0.1	0.0
地方自治体	384	1.0	0.3	0.0	0.0	0.0	0.0	0.0	0.3

	N	W32/ IRCbot	X97M/ Divi	W32/ Spybot	その他の ウイルス	その他の トロイの木馬 (スパイ ウェア)	その他	無回答
全体	1,174	0.2	0.2	0.0	0.3	0.2	0.2	67.7
企業	790	0.0	0.3	0.0	0.5	0.0	0.3	70.5
地方自治体	384	0.5	0.0	0.0	0.0	0.5	0.0	62.0

(N=1,174)

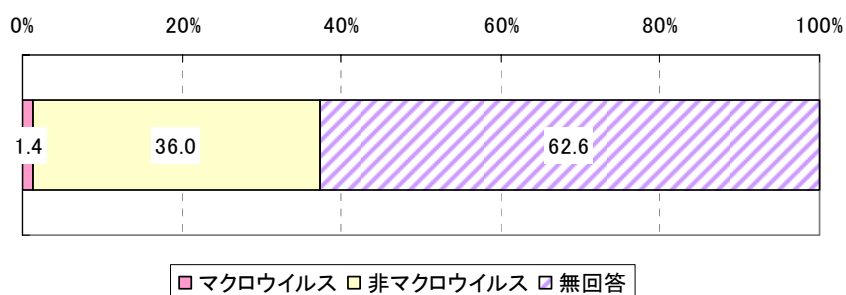


図 2.4-19 影響の最も大きかったウイルスのタイプ

ウイルス感染・発見月に大きな差異はない。

(N=1,174)

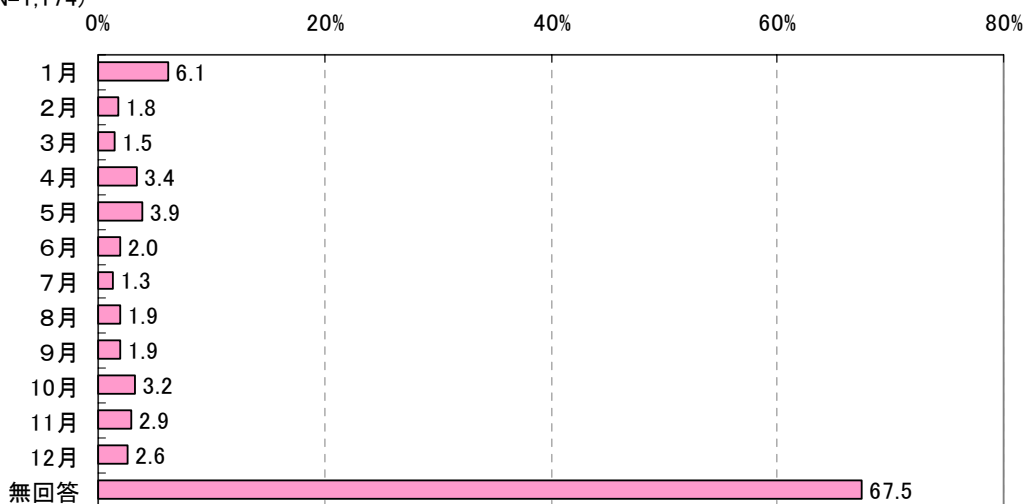


図 2.4-20 影響の最も大きかったウイルス発見月

表 2.4-17 影響の最も大きかったウイルス発見月

	N	(%)						
		1月	2月	3月	4月	5月	6月	
全体	1,174	6.1	1.8	1.5	3.4	3.9	2.0	
企業	790	4.8	1.9	1.4	2.4	3.8	2.4	
地方自治体	384	8.9	1.6	1.8	5.5	4.2	1.0	

	N	(%)						
		7月	8月	9月	10月	11月	12月	無回答
全体	1,174	1.3	1.9	1.9	3.2	2.9	2.6	67.5
企業	790	1.1	2.4	1.6	4.2	3.5	2.2	68.2
地方自治体	384	1.6	0.8	2.3	1.3	1.6	3.6	65.9

## (2) ウイルス発見の経緯

ウイルス感染・発見の経緯は「ウイルス対策ソフト」が8割で最も多い。「ウイルス対策ソフト」での発見は地方自治体の方が多く、企業では「目視による」発見や「外部からの連絡」による発見も見られる。

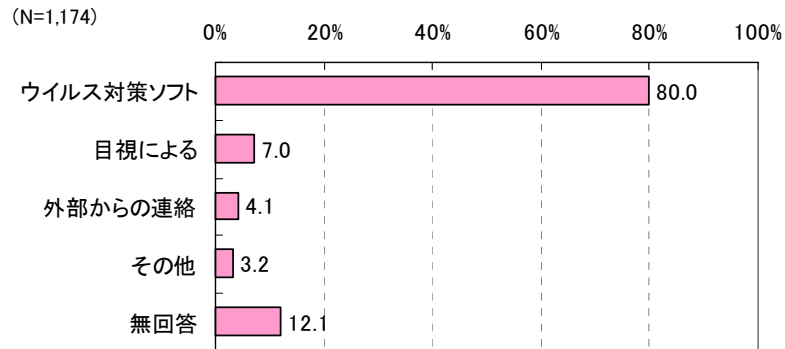


図 2.4-21 ウイルス発見の経緯

表 2.4-18 ウイルス発見の経緯（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	1,174	80.0	7.0	4.1	3.2	12.1
企業	790	77.5	9.1	5.8	4.2	11.6
地方自治体	384	85.2	2.6	0.5	1.3	13.0

(%)

### (3) 発見に使用したウイルス対策ソフト

ウイルス発見に使用したウイルス対策ソフトは「ウイルスバスター」が半数近くに達し、最も多い。その他、「Symantec Norton Internet Security」「Mcafee VirusScan」「InterScan VirusWall」等は1～2割程度の回答があった。同じベンダの製品である「ウイルスバスター」と「InterScan VirusWall」は企業より地方自治体での利用率が高い。

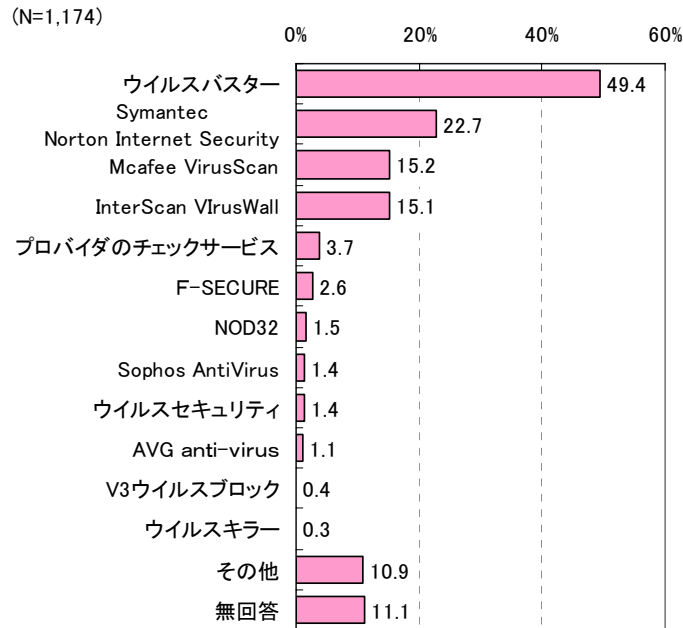


図 2.4-22 発見に使用したウイルス対策ソフト

表 2.4-19 発見に使用したウイルス対策ソフト（自治体との比較）

	N	ウイルスバスター	Symantec Norton Internet Security	Mcafee VirusScan	InterScan VirusWall	プロバイダのチェックサービス	F-SECURE	NOD32
全体	1,174	49.4	22.7	15.2	15.1	3.7	2.6	1.5
企業	790	45.9	25.6	17.3	10.5	4.9	2.7	1.8
地方自治体	384	56.5	16.9	10.9	24.5	1.3	2.6	1.0

	N	Sophos AntiVirus	ウイルスセキュリティ	AVG anti-virus	V3ウイルスブロック	ウイルスキラー	その他	無回答
全体	1,174	1.4	1.4	1.1	0.4	0.3	10.9	11.1
企業	790	1.6	2.0	1.3	0.6	0.5	10.6	10.3
地方自治体	384	1.0	0.0	0.8	0.0	0.0	11.5	12.8

#### (4) 想定されるコンピュータウイルスの感染経路

想定されるウイルス感染・発見経路は「電子メール」が最も多く 4 割を超える。自治体では、「外部媒体、持ち込みパソコン」の比率が企業より若干多い。

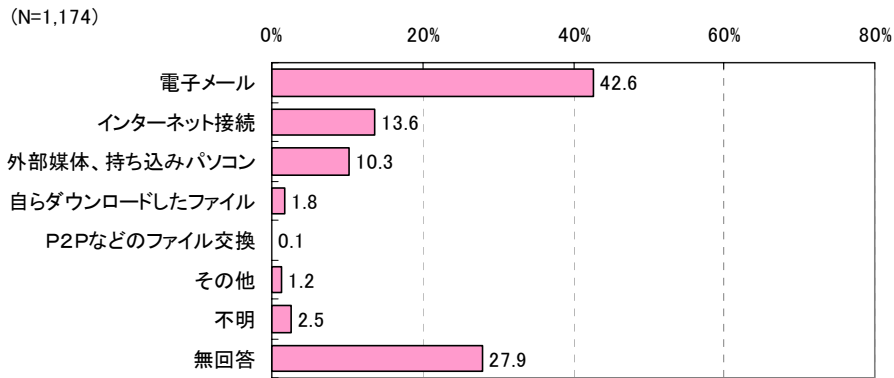


図 2.4-23 想定されるコンピュータウイルスの感染経路

表 2.4-20 想定されるコンピュータウイルスの感染経路（自治体との比較）

(%)

	N	電子メール	インターネット接続	外部媒体、持ち込みパソコン	自らダウンロードしたファイル	P2Pなどのファイル交換	その他	不明	無回答
全体	1,174	42.6	13.6	10.3	1.8	0.1	1.2	2.5	27.9
企業	790	44.8	14.3	8.7	1.8	0.1	1.1	3.3	25.8
地方自治体	384	38.0	12.2	13.5	1.8	0.0	1.3	0.8	32.3

### (5) 感染したパソコンのOSと台数

ウイルスに感染したパソコン台数は、「0台(ない)」を除くと、Windows系では「1~4台」が約2割で最も多い。Macintosh系やUnix・Linux系では、ほとんど感染は見られないため、パソコン全体で見ても、感染したパソコン台数は「1~4台」が約2割で最も多い。

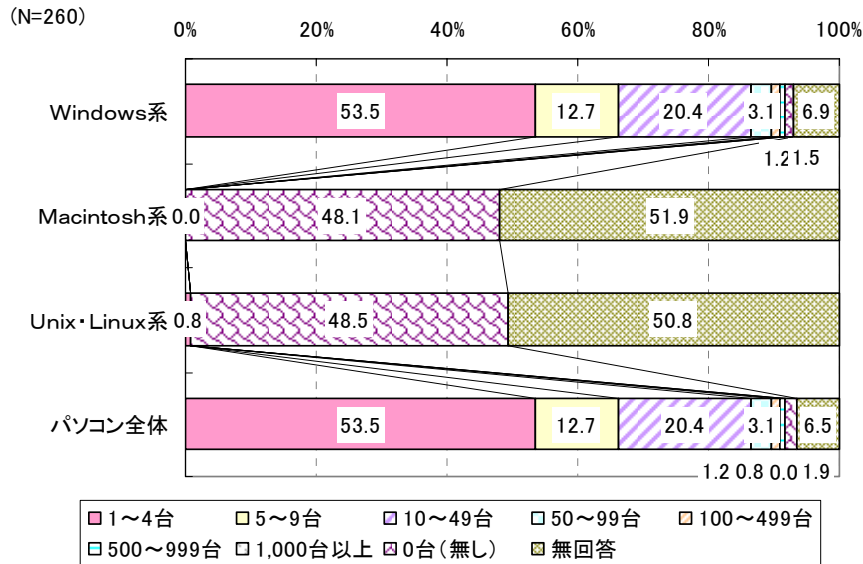


図 2.4-24 感染したパソコンのOSと台数

表 2.4-21 感染したパソコンのOSと台数（自治体との比較）

	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	260	53.5	12.7	20.4	3.1	1.2	0.8	0.0	1.5	6.9
企業	212	56.1	12.7	19.3	2.8	1.4	0.9	0.0	1.4	5.2
地方自治体	48	41.7	12.5	25.0	4.2	0.0	0.0	0.0	2.1	14.6

	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	260	0.0	0.0	0.0	0.0	0.0	0.0	0.0	48.1	51.9
企業	212	0.0	0.0	0.0	0.0	0.0	0.0	0.0	50.9	49.1
地方自治体	48	0.0	0.0	0.0	0.0	0.0	0.0	0.0	35.4	64.6

	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	260	0.8	0.0	0.0	0.0	0.0	0.0	0.0	48.5	50.8
企業	212	0.9	0.0	0.0	0.0	0.0	0.0	0.0	50.9	48.1
地方自治体	48	0.0	0.0	0.0	0.0	0.0	0.0	0.0	37.5	62.5

	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	260	53.5	12.7	20.4	3.1	1.2	0.8	0.0	1.9	6.5
企業	212	56.1	12.7	19.3	2.8	1.4	0.9	0.0	1.4	5.2
地方自治体	48	41.7	12.5	25.0	4.2	0.0	0.0	0.0	4.2	12.5

## 2.5. 新しい脅威について

### 2.5.1. スパイウェアの被害の有無

「スパイウェアの侵入を受けた、スパイウェアが実行された」のは1割未満に留まるが、発見のみも含めた遭遇率は約3割である。ウイルスの遭遇率は約7割であることから、新しい脅威を認識している組織はウイルスの半分以下と言える。企業および地方自治体で有意な差は見られない。

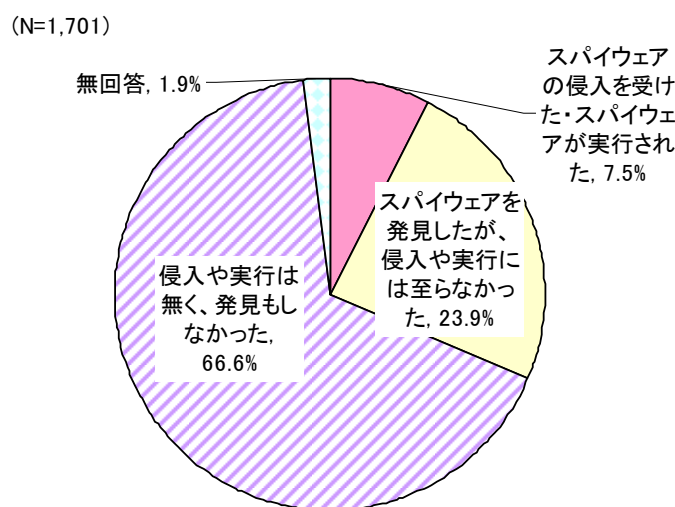


図 2.5-1 スパイウェアの被害の有無

表 2.5-1 スパイウェアの被害の有無（自治体との比較）

(%)

	N	スパイウェアの侵入を受けた・スパイウェアが実行された	スパイウェアを発見したが、侵入や実行には至らなかった	侵入や実行は無く、発見もなかった	無回答
全体	1,701	7.5	23.9	66.6	1.9
企業	1,206	8.3	23.5	66.4	1.8
地方自治体	495	5.7	25.1	67.1	2.2

### 2.5.2. スパイウェア対策ツールの有無

スパイウェア対策では、専用ツールを導入している組織は1割にも満たず、半数程度が「ウイルス対策ソフト等が機能拡張したものを利用している」。また導入していない組織も3割を超える。企業および地方自治体で有意な差は見られない。

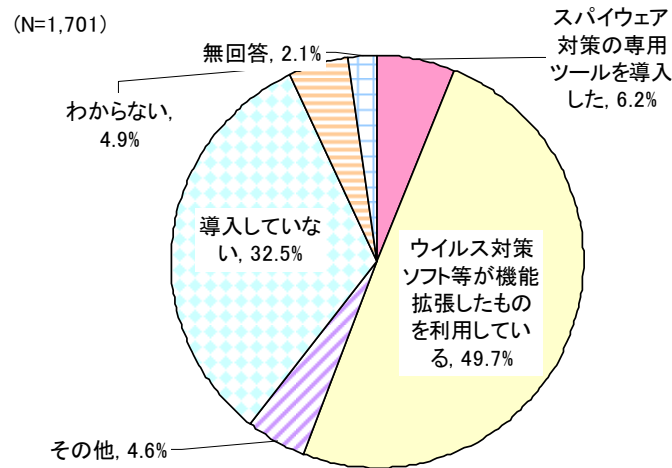


図 2.5-2 スパイウェアの対策ツールの有無

表 2.5-2 スパイウェアの対策ツール有無（自治体との比較）

	N	スパイウェア対策の専用ツールを導入した	ウイルス対策ソフト等が機能拡張したものを利用している	その他	導入していない	わからない	無回答
全体	1,701	6.2	49.7	4.6	32.5	4.9	2.1
企業	1,206	7.0	47.6	5.2	31.9	6.4	1.8
地方自治体	495	4.2	54.9	3.2	33.7	1.2	2.6

### 2.5.3. 発見されたスパイウェアの侵入経路

想定されるスパイウェアの侵入経路は6割以上が「インターネット接続」である。

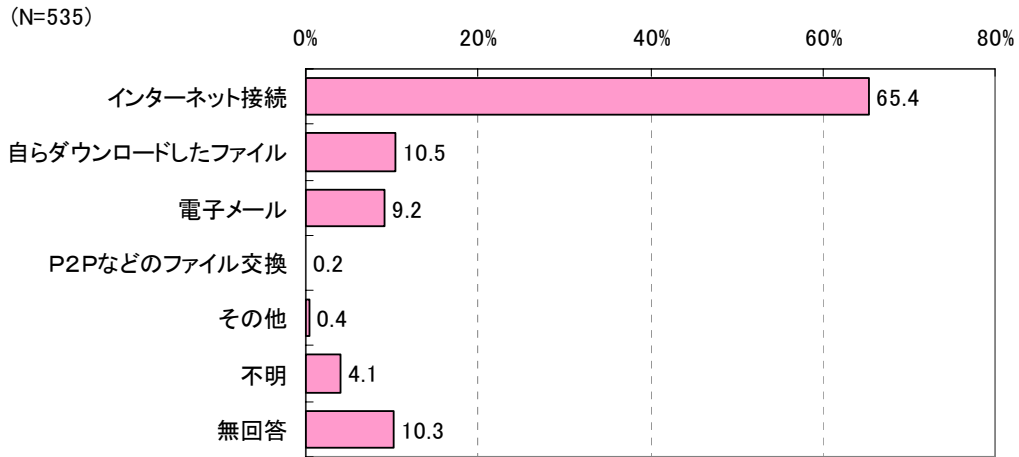


図 2.5-3 スパイウェアの侵入経路

表 2.5-3 スパイウェアの侵入経路（自治体との比較）

(%)

	N	インターネット接続	自らダウンロードしたファイル	電子メール	P2Pなどのファイル交換	その他	不明	無回答
全体	535	65.4	10.5	9.2	0.2	0.4	4.1	10.3
企業	383	63.2	11.0	11.0	0.3	0.5	5.5	8.6
地方自治体	152	71.1	9.2	4.6	0.0	0.0	0.7	14.5

### 3. 考察

#### (1) ウイルス対策が大きく進展

クライアントパソコンへのウイルス対策ソフトの導入状況を見ると、9割以上のパソコンに導入している組織が9割程度に達し、2005年と比較するとその導入率が大きく高まっている。同様に、ネットワークサーバや内部ローカルサーバのウイルス対策ソフトの導入率は、クライアントパソコンより高くはないものの、過去の調査よりはいずれも上がっており、パソコンにおけるウイルス対策ソフトの導入は大きく進展したと言える。

また、ウイルス対策ソフトの導入・更新に対する費用は、情報化の進展度と関連なく、いずれの業種においても総従業員数に応じて支払われており、ウイルス対策は業種を問わず企業・自治体において幅広く実施されていることが示された。

#### (2) ウイルス遭遇経験は横ばいだが、被害は減少

ウイルスに感染または発見したウイルス遭遇経験は、2003年以降ほぼ7割程度で横ばいである。しかし、感染台数は少なく、直接的な被害は「システム停止・性能低下」のみで間接的な被害はほとんどない。「システム停止・性能低下」の復旧作業のためにもほとんど工数がかけられていないことから、2005年のウイルス被害は従来と比較して大きくなかったと言える。これは、2005年に特に大きな被害を与えた悪質なウイルスが発生しなかったことも背景にあるが、(1)で示したように、ウイルス対策が広く普及したことも被害が軽減された大きな理由であると考えられる。

#### (3) コンピュータやインターネットへの依存度が低いほど高い感染率

ウイルスの遭遇（発見または感染した）率と感染率の関係を見ると、遭遇率は高いが感染率が低いのが「電気・ガス・水道・熱供給」および「地方自治体」の公的サービスを提供する重要インフラ事業者である。同じ重要インフラ事業者でも「金融・保険業」は遭遇率・感染率ともに低いのが特徴的であり、他業種よりウイルスの脅威にさらされる確率の高い情報通信業を除き、重要インフラ事業者は、感染率が低い傾向にある。しかし、「農林漁業・鉱業」「他のサービス業」「飲食店・宿泊業」など、コンピュータやインターネットへの依存度が低い業種においては、遭遇率は低いが感染率は高い傾向にあり、これらの業種に対しては定期的なパッチの適用など、感染を防ぐためのより効果的な対策が求められる。

#### (4) ウイルス被害が小さく、IPAへは届け出ないケースも

ウイルス感染時にIPAへ届け出る比率は年々低下している。しかし、「被害が大きければ届け出る」とする率が前回調査より大きく増加していることから、回答者はウイルス被害があまり大きくないと捉えているため、IPAへも届け出る必要がないと認識していると思われる。

ただし、企業では届出をしない理由を「届出方法が不明なため」との回答も多いことから、より有意な統計値の取得のためには、企業に対してIPAへの届出方法の認知を図ることも必要である。

#### **(5) 新たなウイルスに対しては危機感も**

ウイルスに関連して知りたい情報では、依然「感染した時の復旧方法」や「感染しないための方法や対策」の比率は高いものの、時系列で見るとその数値は落ち着きつつある。しかし、「新種ウイルスの情報」や「要注意ウイルスの警戒情報」を知りたいと思う比率は上がっており、新たなタイプのウイルスや経済的利益を得ることを目的とした悪質なウイルスの増加に対して危機感を持つ組織も多いと推測される。

#### **(6) スパイウェアの脅威はまだ小さく、既存ツールの拡張機能で対応**

スパイウェアの被害経験はまだ1割未満であり、対策としても専用ツールの導入よりウイルス対策ソフト等が機能拡張したものを利用している割合が多い。現状、スパイウェアについては大きな被害は報告されていないが、今後、スパイウェアの脅威が大きくなるにつれ、より強固な対策が必要となると予想される。

# コンピュータウイルスに関する被害状況調査票

独立行政法人 情報処理推進機構  
セキュリティセンター

## ご記入にあたってのお願い

- ◎ 本調査は、貴企業の「コンピュータの情報セキュリティの管理者（責任者・担当者）の方がご回答ください。貴方がそれ以外の方の場合は、お手数ですが、該当する方にお渡しくださいますようお願い申し上げます。
- ◎ 情報処理推進機構セキュリティセンターでは、国内の企業における「コンピュータウイルスに関する状況を捉える」ことを目的としたアンケートを実施しております。今回調査の結果は、2006年6月頃、情報処理推進機構セキュリティセンターのホームページにて公開する予定です。ただし、ご回答の内容についてはすべて統計数値として集計いたしますので、会社名や個人名などが公表されることは一切ございません。
- ◎ この調査の実施、取り纏めにつきましては、株式会社三菱総合研究所に委託しております。
- ◎ お答えは、特に説明のないかぎり、あてはまる項目をお選びになって、該当する番号に○をおつけください。また、お答えが「その他（ ）」にあてはまる場合は、お手数ですが（ ）の中にその内容を具体的にご記入ください。
- ◎ お答えの内容によっては設問の進み先が飛ぶ場合がありますので、矢印にご注意ください。
- ◎ ご記入いただいた用紙は、同封の返信用封筒（切手不要）に入れ、**3月24日（金）まで**にご投函くださいますようお願い申し上げます。
- ◎ このアンケートについてご不明な点がございましたら、下記までお問合せください。

### 【調査主旨に関するお問合せ先】



独立行政法人 情報処理推進機構  
セキュリティセンター

E-mail: [isec-survey2@ipa.go.jp](mailto:isec-survey2@ipa.go.jp)

URL: <http://www.ipa.go.jp/security/>

### 【調査実施に関するお問合せ先】

株式会社三菱総合研究所  
情報セキュリティ研究グループ

担当：川口、井上

電話：03-3277-0519

E-mail: [virus-survey-05@mri.co.jp](mailto:virus-survey-05@mri.co.jp)

\* 三菱総合研究所はプライバシーマーク取得企業です

**この調査は、企業・団体の単位でお答えください**

**I. 貴企業(当該企業・当該自治体)についてお伺いします。**

**問1 貴企業の主な業種をお答えください。(○は1つ)**

- |            |                 |            |
|------------|-----------------|------------|
| 1 農林漁業・鉱業  | 2 建設業           | 3 機械器具製造業  |
| 4 他の製造業    | 5 電気・ガス・熱供給・水道業 | 6 情報通信業    |
| 7 運輸業      | 8 卸売業           | 9 小売業      |
| 10 金融・保険業  | 11 不動産業         | 12 飲食店、宿泊業 |
| 13 他のサービス業 | 14 自治体・公共団体     | 15 その他 ( ) |

**問2 貴企業の総従業員数(有給役員、正社員、準社員、アルバイト等を含む)をお答えください。**

十万	万	千	百	十	一

人

常時従業員の総数。有給役員及び常時雇用者(正社員、準社員、アルバイト等、1ヶ月を超える雇用契約者)とし、人材派遣業者からの派遣従業員は含めません。

**問3 貴企業の直近年度の総売上高(単体)をお答えください。(自治体の方は問5へ)**

兆	千億	百億	十億	億	千万	百万

百万円

学校、組合団体など営業活動を行わない組織の場合は、当該年度における収入高とします。

**問4 貴企業の直近年度の経常利益(単体)をお答えください。(自治体の方は問5へ)**

兆	千億	百億	十億	億	千万	百万

百万円

**問5 貴企業の規程年間営業日数および1日の営業時間をお答えください。**

年間営業日数 \_\_\_\_\_日/年      1日あたり営業時間 \_\_\_\_\_時間/日

**問6 貴企業で利用されているパソコンの台数をご記入ください。**

Windows系 約 \_\_\_\_\_台      Macintosh系 約 \_\_\_\_\_台      Unix・Linux系 約 \_\_\_\_\_台

**問7 貴企業におけるLANやWAN等のネットワークの構築状況は、下記のどれに該当しますか。**

(○は1つ)

- 1 事業所内ネットワーク(LAN)のみ構築
- 2 事業所内だけではなく、機関内の事業所間ネットワーク(WAN:本社と支社・工場間等)まで構築
- 3 機関内だけではなく、外部の機関とのネットワーク(例:サプライチェーン)まで構築
- 4 社内情報ネットワークは構築していない

II. 貴社におけるコンピュータウイルス対策に関してお伺いします。

問8 貴社では、各自のパソコンにウイルス対策ソフトを導入していますか。(○は1つ)

- |                 |                 |
|-----------------|-----------------|
| 1 9割以上のパソコンに導入済 | 2 半数以上のパソコンに導入済 |
| 3 半数未満のパソコンに導入済 | 4 導入していない       |

問9 貴社では、外部に公開しているネットワークサーバ(メールサーバ、Webサーバなど)にウイルス対策ソフトを導入していますか。(○は1つ)

- |                      |                      |
|----------------------|----------------------|
| 1 9割以上のネットワークサーバに導入済 | 2 半数以上のネットワークサーバに導入済 |
| 3 半数未満のネットワークサーバに導入済 | 4 導入していない            |

問10 貴社では、内部で利用しているローカルサーバ(ファイルサーバ、プリントサーバなど)にウイルス対策ソフトを導入していますか。(○は1つ)

- |                    |                    |
|--------------------|--------------------|
| 1 9割以上のローカルサーバに導入済 | 2 半数以上のローカルサーバに導入済 |
| 3 半数未満のローカルサーバに導入済 | 4 導入していない          |

問11 問8～問10に挙げたウイルス対策ソフトの導入・更新(バージョンアップ、パターンファイル更新)について、昨年1年間(2005年1月～12月)にかけた費用(\*1)を、概算でお答えください。

\_\_\_\_\_ 万円 / 年 (購入・更新なしなら「0円」と記入)

(\*1) ウイルス対策用のソフトもしくは装置の費用を指します。導入や更新にかかる人件費は含めなくてください。

問12 貴社では、ウイルス対策に関するユーザ教育はどのようにされていますか。(○はいくつでも)

- 1 社内でセミナー等を開催
- 2 外部の教育機関・セミナー等を利用
- 3 情報を収集・配布(Web掲載、メール配布、社内通達等を含む)
- 4 特に実施していない
- 5 その他 ( \_\_\_\_\_ )

問13 貴社では、ウイルス対策の管理を組織的に行っていますか。(○は1つ)

- |                |                      |
|----------------|----------------------|
| 1 専門部署(担当者)がある | 2 兼務だが担当責任者が任命されている  |
| 3 外部委託している     | 4 組織的には行っていない(各自の対応) |
| 5 わからない        |                      |

問14 貴社ではセキュリティパッチ(Windows Update など)を適用していますか。(それぞれ○は1つ)

・クライアント(パソコン)

- |               |          |              |
|---------------|----------|--------------|
| 1 常に最新のパッチを適用 | 2 定期的に適用 | 3 気がついたときに適用 |
| 4 ほとんど適用していない | 5 分からない  |              |

・外部に公開しているネットワークサーバ(メールサーバ、Webサーバ)

- |               |          |              |
|---------------|----------|--------------|
| 1 常に最新のパッチを適用 | 2 定期的に適用 | 3 気がついたときに適用 |
| 4 ほとんど適用していない | 5 分からない  |              |

・内部で利用しているローカルサーバ(ファイルサーバ、プリントサーバ)

- |               |          |              |
|---------------|----------|--------------|
| 1 常に最新のパッチを適用 | 2 定期的に適用 | 3 気がついたときに適用 |
| 4 ほとんど適用していない | 5 分からない  |              |

問15 現在、コンピュータウイルスに関連して知りたいと思っている情報として、該当するものを下記よりすべてお選びください。(○はいくつでも)

- |                        |                |
|------------------------|----------------|
| 1 しくみ・種類等の技術的内容        | 2 感染した時の復旧方法   |
| 3 感染しないための方法や対策        | 4 ウイルス対策ソフト情報  |
| 5 コンピュータウイルスが引き起こす発病内容 | 6 国内のウイルス被害の状況 |
| 7 海外のウイルス被害の状況         | 8 要注意ウイルスの警戒情報 |
| 9 ウイルスが悪用する脆弱性の情報      | 10 新種ウイルスの情報   |
| 11 その他( )              | 12 特になし        |

問16 経済産業省告示の「コンピュータウイルス対策基準」をご存知ですか。(○は1つ)

- |             |            |
|-------------|------------|
| 1 内容を理解している | 2 読んだことがある |
| 3 存在は知っている  | 4 知らない     |

問17 コンピュータウイルス被害の拡大と再発防止のために、情報処理推進機構がウイルスに関する届出を受け付ける指定機関になっていることをご存知ですか。(○は1つ)

- |         |        |
|---------|--------|
| 1 知っている | 2 知らない |
|---------|--------|

問18 今後感染が発見されたとき、情報処理推進機構に届出を行いますか。(○は1つ)

- |                            |                  |
|----------------------------|------------------|
| 1 届出を行う                    |                  |
| 2 届出を行わない → その理由 (○はいくつでも) |                  |
| a 届出に手間がかかる                | b 届出方法が不明なため     |
| c 届出る時間がないため               | d 自分で修復できるため     |
| e 被害が大きければ届出する             | f 社内規定による届出で済ませる |
| g その他( )                   |                  |

Ⅲ. コンピュータウイルスの発見と感染に関してお伺いします。

用語等ご不明の点は、「対策情報 ウイルス対策」(<http://www.ipa.go.jp/security/isg/virus.html>)をご参照ください。

問19 貴社では、昨年1年間(2005年1月～12月)に、コンピュータウイルスに感染したこと、または感染には至らないが発見したことがありますか。一度でもあればお答えください。(○は1つ)

- 1 感染した(発見のみで感染しなかった場合は2を選択)
- 2 ウイルスを発見したが、感染には至らなかった
- 3 感染も発見もしなかった → 8ページにお進みください

問20 感染または発見したウイルスは、合計何種類ですか。亜種は一種類と数えて下さい。(○は1つ)

- 1 1種類
- 2 2種類
- 3 3種類
- 4 4種類
- 5 5種類以上

問21 感染または発見したウイルスの具体的な名称として、該当するものを下記よりすべてお選びください。(○はいくつでも)

- |               |                |
|---------------|----------------|
| 1 W32/Netsky  | 2 W32/Sober    |
| 3 W32/Mytob   | 4 W32/Bagle    |
| 5 W32/Lovgate | 6 W32/Mydoom   |
| 7 W32/Zafi    | 8 W32/Bagz     |
| 9 W32/Klez    | 10 W32/Bugbear |
| 11 その他(名称: )  | 12 不明          |

問22 昨年1年間(2005年1月～12月)のコンピュータウイルスへの感染件数をお答えください。同時期に報告された同種・同感染元と想定される場合をまとめて1件と数えます。(感染なしなら「0件」と記入)

\_\_\_\_\_件 / 年

問23 ウイルスに感染したパソコンの台数は年間延べ何台ですか。(○は1つ)

- |            |          |          |          |
|------------|----------|----------|----------|
| 1 0台(発見のみ) | 2 1～4台   | 3 5～9台   | 4 10～19台 |
| 5 20～49台   | 6 50～99台 | 7 100台以上 |          |

問24 ウイルスに感染した影響で生じた直接的な被害の有無についてお答えください。(○はいくつでも)

- |               |          |        |
|---------------|----------|--------|
| 1 システム停止・性能低下 | 2 情報破壊   | 3 情報流出 |
| 4 取引先等への感染拡大  | 5 その他( ) |        |

問25 ウイルス感染が原因で発生した間接的な被害の有無についてお答えください。(○はいくつでも)

- |                     |                   |
|---------------------|-------------------|
| 1 風評による売上減          | 2 風評による契約者減       |
| 3 風評による株価下落         | 4 風評によるブランド価値の低下  |
| 5 取引先等への補償、補填、損害賠償等 | 6 訴訟への対応          |
| 7 謝罪広告の出稿           | 8 営業秘密の流出による価値の低下 |
| 9 その他( )            |                   |

問26 貴社において、電子商取引(EC)業務(\*2)の売上が、全体の売上に占める割合をお答えください。(○は1つ)

- |   |         |   |     |   |      |
|---|---------|---|-----|---|------|
| 1 | 0% (なし) | 2 | 20% | 3 | 40%  |
| 4 | 60%     | 5 | 80% | 6 | 100% |

(\*2) ここではEC業務として、物流(物流手配、出荷、輸送管理)、顧客から対価を受取るサービスの提供、販売(見積・商談、販売計画、販売促進、受注管理、顧客情報管理、請求、決済)。金融分野における決済代行、振込・送金、預金獲得、融資、保険契約等の、売上げに直結する業務を想定します。

問27 ウイルスに感染した影響によって、電子商取引(EC)業務が停止した期間は年間延べ何日ですか。(○は1つ)

- |   |           |   |       |   |           |
|---|-----------|---|-------|---|-----------|
| 1 | 0日 (影響なし) | 2 | ～1日   | 3 | 2～3日      |
| 4 | 4～5日      | 5 | 6～10日 | 6 | それ以上 ( )日 |

問28 ウイルスに感染した影響によって、インターネットに公開している業務遂行上重要なサーバ(メールサーバやウェブサーバ、前問のECサーバは除く)が停止した期間は年間延べ何日ですか。(○は1つ)

- |   |           |   |       |   |           |
|---|-----------|---|-------|---|-----------|
| 1 | 0日 (影響なし) | 2 | ～1日   | 3 | 2～3日      |
| 4 | 4～5日      | 5 | 6～10日 | 6 | それ以上 ( )日 |

問29 ウイルスに感染した影響によって、事業所内のネットワークの利用が困難となったり、社内の重要なサーバの利用が困難となったりした期間は年間延べ何日ですか。(○は1つ)

- |   |           |   |       |   |           |
|---|-----------|---|-------|---|-----------|
| 1 | 0日 (影響なし) | 2 | ～1日   | 3 | 2～3日      |
| 4 | 4～5日      | 5 | 6～10日 | 6 | それ以上 ( )日 |

問30 昨年1年間(2005年1月～12月)に、情報管理部門が行ったウイルス感染からの復旧作業(\*3)は年間延べ何人日ですか。(○は1つ)

- |   |          |   |          |   |             |
|---|----------|---|----------|---|-------------|
| 1 | 0～1人・日   | 2 | 2～3人・日   | 3 | 4～5人・日      |
| 4 | 6～10人・日  | 5 | 11～15人・日 | 6 | 16～20人・日    |
| 7 | 21～25人・日 | 8 | 26～30人・日 | 9 | それ以上 ( )人・日 |

(\*3) ここでは、ウイルス感染を確認後に、駆除や再インストール等を行い、システムを停止状態から稼働常態に戻して、システム機能を回復させるまでの作業を指します。

問31 昨年1年間(2005年1月～12月)について、システム復旧に関して新たに購入した代替機器の費用(\*4)をお答えください。(購入なしなら「0円」と記入)

\_\_\_\_\_ 百万円 / 年

(\*4) 一時的に利用するために事後に購入したハードウェアやソフトウェアの費用のみを指します。恒久的な対策強化を目的に購入した機器の費用は含めないでください。

問32 昨年1年間(2005年1月～12月)について、システム復旧に関し外部に発注した業務の費用をお答えください。(発注なしなら「0円」と記入)

\_\_\_\_\_ 百万円 / 年

問33 昨年1年間(2005年1月～12月)について、システム復旧に関して、その他に発生した費用(\*5)があれば、その金額と費目をお答えください。(特になら「0円」と記入)

\_\_\_\_\_百万円 / 年 費目(\_\_\_\_\_)

(\*5) 社内に配布する対策用CD-ROMの作成費等

問34 昨年1年間(2005年1月～12月)に、業務部門が行ったウイルス感染が原因で発生した追加のデータ処理作業(\*6)は年間延べ何人日ですか。(○は1つ)

- 1 0～1人・日                      2 2～3人・日                      3 4～5人・日  
4 6～10人・日                      5 11～15人・日                      6 それ以上(                      人・日)

(\*6) ここでは、消失したデータの再登録や、一時的に手作業等で作成したデータのシステムへの登録などの作業を指します。

【 以後の設問は、影響が最も大きかったウイルスについてお答えください。 】

問35 貴社において、昨年1年間(2005年1月～12月)に感染または発見したコンピュータウイルスのうち影響が最も大きかったウイルスの名称と発見時期をご記入ください。

ウイルス名 \_\_\_\_\_ 発見日 \_\_\_\_\_ 2005年 \_\_\_\_\_ 月 \_\_\_\_\_

問36 コンピュータウイルスを発見した経緯について、該当するものを下記よりすべてお選びください。(○はいくつでも)

- 1 ウイルス対策ソフト                      2 目視による  
3 外部からの連絡                      4 その他(                      )

問37 コンピュータウイルスを発見するのに使用したウイルス対策ソフトはどれですか。該当するものを下記よりすべてお選びください。(○はいくつでも)

- 1 AVG anti-virus                      2 F-SECURE  
3 InterScan VirusWall                      4 Mcafee VirusScan  
5 NOD32                      6 Sophos AntiVirus  
7 Symantec Norton Internet Security                      8 V3 ウイルスブロック  
9 ウイルスキラー                      10 ウイルスセキュリティ  
11 ウイルスバスター                      12 プロバイダのチェックサービス(                      )  
13 その他(                      )

問38 想定されるコンピュータウイルスの感染経路は、下記のどれに該当しますか。(○は1つ)  
※発見のみの場合も想定される経路を選択してください。

- 1 電子メール                      2 インターネット接続 (ホームページ閲覧など)  
3 自らダウンロードしたファイル                      4 P2P(Peer to Peer)などのファイル交換  
5 外部媒体、持ち込みパソコン                      6 その他(                      )  
7 不明

問39 コンピュータウイルスに感染したパソコンの台数をご記入ください。(感染なしなら「0台」と記入)

Windows系 約 \_\_\_\_\_ 台    Macintosh系 約 \_\_\_\_\_ 台    Unix・Linux系 約 \_\_\_\_\_ 台

**IV. 新しい脅威(スパイウェア)についてお伺いします。**

スパイウェアとは、利用者や管理者の意図に反してインストールされ、利用者の個人情報やアクセス履歴などの情報を収集するプログラム等のことを指します。

**問40 貴社では、昨年1年間(2005年1月～12月)にスパイウェアの被害に遭いましたか。(○は1つ)**

- 1 スパイウェアの侵入を受けた、または、スパイウェアが実行されていた
- 2 スパイウェアを発見したが、侵入や実行には至らなかった
- 3 侵入や実行は無く、発見もしなかった

**問41 貴社では、スパイウェア対策ツールを導入していますか。(○は1つ)**

- 1 スパイウェア対策の専用ツールを導入した
- 2 ウイルス対策ソフト等が機能拡張したものを利用している
- 3 その他( )
- 4 導入していない
- 5 わからない

**問42 発見されたスパイウェアの侵入経路は、どのように想定されますか。(○は1つ)**

- 1 電子メール
- 2 インターネット接続(ホームページ閲覧など)
- 3 自らダウンロードしたファイル
- 4 P2P(Peer to Peer)などのファイル交換
- 5 その他( )
- 6 不明

貴社・貴事業所名			
お名前		所属部署・役職	
ご住所	〒  TEL:		
E-mail アドレス			

ご回答くださった方には、調査結果概要版をメールにてご送付させていただきます。

**ご協力ありがとうございました**