平成９年

国内におけるコンピュータウイルス等被害状況調査

平成１０年６月

情報処理振興事業協会

目　　次

はじめに

Ⅰ　コンピュータウイルス等被害状況報告書

1　調査概要

1・1　調査目的 Ⅰ-2

1・2　調査内容 Ⅰ-2

1・2・1　調査期間 Ⅰ-2

1・2・2　調査方法 Ⅰ-2

1・2・3　調査対象 Ⅰ-2

1・2・4　調査項目 Ⅰ-3

1・2・5　回収結果 Ⅰ-5

2　回答事業所の概要

2・1　業　種 Ⅰ-6

2・2　就業者数 Ⅰ-7

2・3　利用しているコンピュータの種類と台数 Ⅰ-8

2・4　ネットワーク化の状況 Ⅰ-11

2・4・1　社内情報ネットワークの構築状況 Ⅰ-11

2・4・2　インターネット接続状況 Ⅰ-13

2・4・3　商用パソコン通信サービスの利用状況 Ⅰ-14

2・4・4　商用 VAN ネットおよび
その他の企業間ネットワークとの接続状況 Ⅰ-15

3　コンピュータウイルスによる被害状況

3・1　コンピュータウイルスに対する関心 Ⅰ-16

3・1・1　コンピュータウイルスの認知度 Ⅰ-16

3・1・2　コンピュータウイルスに対する脅威 Ⅰ-18

3・1・3　今後の被害予測 Ⅰ-20

3・1・4　知りたい情報 Ⅰ-22

3・2　コンピュータウイルスによる被害状況 Ⅰ-23

3・2・1　コンピュータウイルス感染経験の有無 Ⅰ-23

3・2・2　感染したウイルスの名称 Ⅰ-24

3・2・3　感染したウイルスの種類数 Ⅰ-25

3・2・4　感染したコンピュータの台数 Ⅰ-26

3・2・5　感染したフロッピーディスク（FD）の枚数 Ⅰ-27

４　コンピュータへの不正アクセスによる被害状況
４・１　コンピュータ不正アクセスに対する関心 Ⅰ-28
４・１・１　コンピュータ不正アクセスの認知度 Ⅰ-28
４・１・２　コンピュータの不正アクセスに対する脅威 Ⅰ-30
４・１・３　今後の被害予測 Ⅰ-32
４・１・４　求められている情報 Ⅰ-34
４・２　コンピュータ不正アクセス被害状況 Ⅰ-35
４・２・１　コンピュータ不正アクセス被害経験の有無 Ⅰ-35

Ⅱ　被害及び対策の現状と課題に関する報告書
１　コンピュータウイルスの被害及び対策の現状と課題
１・１　被害発生状況 Ⅱ-2
１・２　セキュリティ対策実施状況 Ⅱ-6
１・２・１　現在実施しているセキュリティ対策 Ⅱ-6
１・２・２　今後実施予定のセキュリティ対策 Ⅱ-8
１・２・３　ウイルス対策に関するユーザ教育 Ⅱ-10
１・３　ワクチンソフト Ⅱ-11
１・３・１　情報源 Ⅱ-11
１・３・２　導入目的 Ⅱ-12
１・３・３　選択基準 Ⅱ-13
１・４　コンピュータウイルス対策の課題 Ⅱ-14
１・４・１　コンピュータウイルス対策基準の認知度 Ⅱ-14
１・４・２　被害届出について Ⅱ-16
１・４・３　就業者数別セキュリティ対策実施状況 Ⅱ-19

２　コンピュータへの不正アクセスによる被害及び対策の現状と課題
２・１　被害発生状況 Ⅱ-20
２・２　セキュリティ対策実施状況 Ⅱ-22
２・２・１　現在実施しているセキュリティ対策 Ⅱ-22
２・２・２　今後実施予定のセキュリティ対策 Ⅱ-24
２・２・３　不正アクセスに関するユーザ教育 Ⅱ-26
２・３　不正アクセスに関する情報源 Ⅱ-27
２・４　コンピュータ不正アクセス対策の課題 Ⅱ-29
２・４・１　コンピュータ不正アクセス対策基準の認知度 Ⅱ-29
２・４・２　被害届出について Ⅱ-30
２・４・３　就業者数別セキュリティ対策実施状況 Ⅱ-33

Ⅲ　コンピュータウイルス被害分析調査報告書

１　コンピュータウイルスによる被害分析
１・１　感染したコンピュータの種類と台数 Ⅲ-2
１・２　発見の経緯 Ⅲ-4
１・３　発見に使用したワクチンソフト Ⅲ-5
１・４　感染経路 Ⅲ-6
１・５　復旧方法 Ⅲ-7
１・６　被害規模 Ⅲ-8
１・６・１　復旧に要した期間 Ⅲ-8
１・６・２　復旧に要した人日 Ⅲ-9

２　コンピュータへの不正アクセスの被害分析
２・１　被害を受けたコンピュータの種類とネットワーク OS Ⅲ-10
２・２　発見の経緯 Ⅲ-11
２・３　被害状況 Ⅲ-12
２・３・１　被害の内容 Ⅲ-12
２・３・２　不正利用された利用者 ID について Ⅲ-13
２・３・３　利用者 ID とパスワードが不正利用された理由 Ⅲ-14
２・４　不正アクセスした人の特定 Ⅲ-15
２・５　復旧方法 Ⅲ-16
２・６　被害規模 Ⅲ-17

Ⅳ　コンピュータウイルス感染等防止策報告書
１　コンピュータウイルス感染防止策
１・１　コンピュータウイルスに対する脅威と
セキュリティ対策の実施状況 Ⅳ-2
１・２　コンピュータウイルス感染防止策 Ⅳ-3

２　コンピュータへの不正アクセス被害防止策
２・１　コンピュータへの不正アクセスに対する脅威と
セキュリティ対策の実施状況 Ⅳ-6
２・２　コンピュータへの不正アクセス被害防止策 Ⅳ-7

資料編

Ⅰ　コンピュータウイルス等被害状況報告書

1　調査概要
2　回答事業所の概要
3　コンピュータウイルスによる被害状況
4　コンピュータへの不正アクセスによる被害状況

１　調査概要

１・１　調査目的

情報化が進展する中、コンピュータおよびコンピュータへの不正アクセスの認知度、脅威ともかなり大きくなっており、情報処理振興事業協会ではウイルス被害の届出だけでなく、不正アクセスによる被害の届出も受けることとなった。また、パソコンの急激な普及拡大や、ネットワーク化の進展、インターネットの急速な普及等により、コンピュータウイルスおよび不正アクセスによる被害は今後増加していくものと考えられる。本調査は、このような状況下、今後コンピュータウイルスおよび不正アクセスによる被害を未然にあるいは最小限に抑えられる施策をほどこすべく、事前に基礎的情報を収集するために、コンピュータウイルスおよび不正アクセスの被害状況について実態を把握することを目的として、1991 年より行っている調査の 7 回目として実施した。

１・２　調査内容

１・２・１　調査期間

１９９７年1月1日～１９９７年１２月３１日

１・２・２　調査方法

郵送発送・回収によるアンケート調査。

１・２・３　調査対象

１９９６年の調査でのアンケート回収事業所および全国の事業所から無作為に抽出した事業所の計 5,000 件を調査対象とした。

業種別アンケート発送数

業　種	発送数	業　種	発送数
農林水産業	30	電力・ガス業	18
鉱業	21	サービス業	1,072
建設業	733	教育・研究機関	334
製造業	1,041	政治、経済、文化団体	63
出版・印刷業	106	政府、政府関係機関、地方公共団体	227
卸売・小売業	1,079	その他	41
金融・保険業	98	合　計	5,000
運輸・通信業	137		

１・２・４　　調査項目

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

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

（11）「コンピュータウイルス対策基準」の認知度
（12）届出期間としての「情報処理振興事業協会」の認知度
（13）届出の実施
①届出ない理由

Ⅲ　コンピュータへの不正アクセスによる被害状況
（１）コンピュータ不正アクセスの認知度
（２）コンピュータ不正アクセスの脅威
（３）コンピュータ不正アクセスによる被害の有無
①不正アクセスされたコンピュータの機種・OS
②発見の経緯
③被害内容
④使用された利用者 ID
⑤利用者 ID およびパスワードが不正利用された理由
⑥不正アクセスを行った人の特定
⑦復旧方法
⑧被害規模（期間・投入人日）
（４）現在および今後のセキュリティ対策
（５）不正アクセス対策に関するユーザ教育
（６）不正アクセスに関する情報源
①情報源の内容
（７）今後の被害予測
（８）知りたい情報
（９）「コンピュータ不正アクセス対策基準」の認知度
（10）届出機関としての「情報処理振興事業協会」の認知度
（11）届出の実施
①届出ない理由

１・２・５　　回収結果

本調査におけるアンケートの回収結果は以下の通りである。

アンケート本票

	回　収　数	回　収　率
本　　票	1270	25.4%

個別票

	件　数	被害事業所数
ウイルス個別票	670	482
不正アクセス個別票	61	61

注記１：本票でウイルス感染被害にあったと回答した事業所数は 482 件であるが、複数の被害があった事業所で複数の個別票を提出している場合や、個別票を未送付または未記入の事業所があり、回収したウイルスの個別票は上記のように 670 件となっている。

注記２：本票で不正アクセスの被害にあったと回答した事業所数は 61 件であるが、複数の被害があった事業所で複数の個別票を提出している場合や、個別票を未送付または未記入の事業所があり、回収した不正アクセスの個別票は最終的に 61 件であった。

注記３：アンケート集計結果については、各項目とも、未記入分は集計から除外している。

２　回答事業所の概要

２・１　業　種

回答事業所の業種の内訳は、図Ⅰ－１の通りである。内訳をみると、「製造業」が 25.1%で最も多く、次いで「情報サービス業」が 19.4%、「卸売・小売業」が 12.7%、「教育・研究機関」が 9.0%となっている。

図Ⅰ－１　業種別内訳

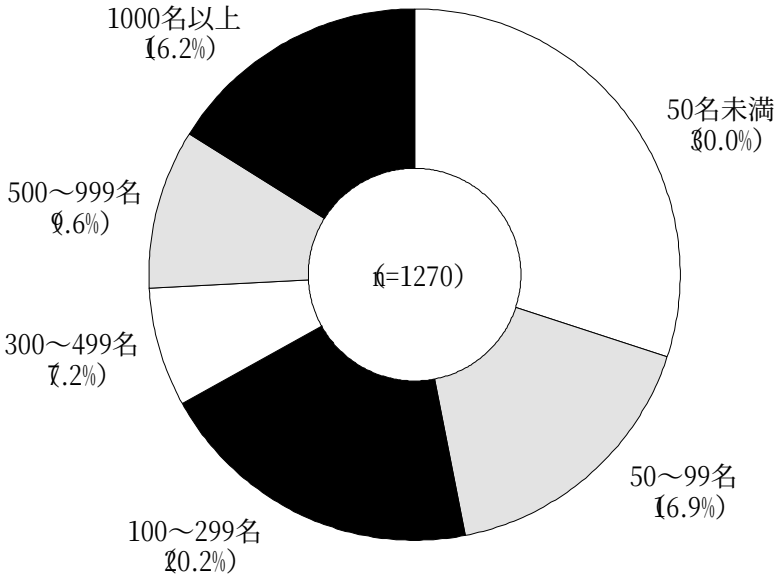
業　　種	回答数	構成比（%）	業　　種	回答数	構成比（%）
農林水産業	6	0.5	新聞・放送業	7	0.6
鉱業	5	0.4	情報サービス業	246	19.4
建設業	64	5.0	物品賃貸業	4	0.3
製造業	319	25.1	遊興娯楽業	2	0.2
出版・印刷業	20	1.6	医療業	18	1.4
卸売・小売業	161	12.7	教育・研究機関	114	9.0
金融・保険業	36	2.8	政治、経済、文化団体	26	2.0
不動産業	13	1.0	その他サービス業	85	6.7
運輸業	17	1.3	政府または政府関係機関	18	1.4
通信業	9	0.7	地方公共団体	81	6.4
電力業	2	0.2	その他	12	0.9
ガス業	5	0.4	総　　計	1270	100.0

その他：市民団体、健康保険組合、宗教法人、事業協同組合など

２・２　　就業者数

回答事業所の就業者数では、「50 名未満」が 30.0%を占めて最も多く、次いで「100～299 名」が 20.2%、「50 名～99 名」が 16.9%となっており、比較的規模の小さな事業所が多い。

図Ⅰ－２　　就業者数



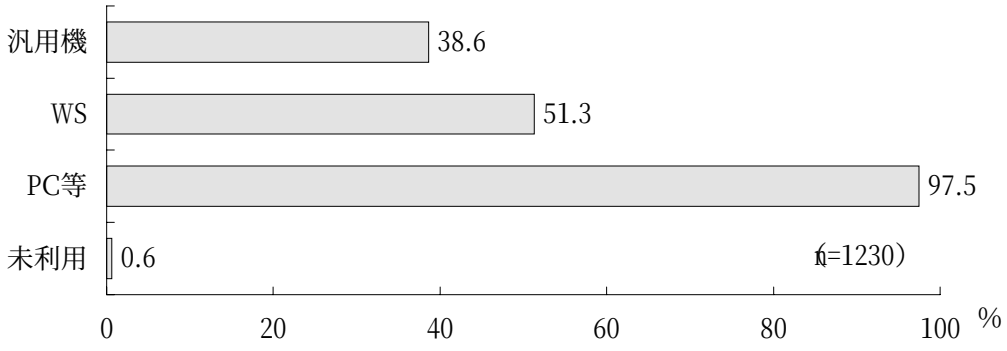
２・３　　利用しているコンピュータの種類と台数

（１）利用しているコンピュータの種類

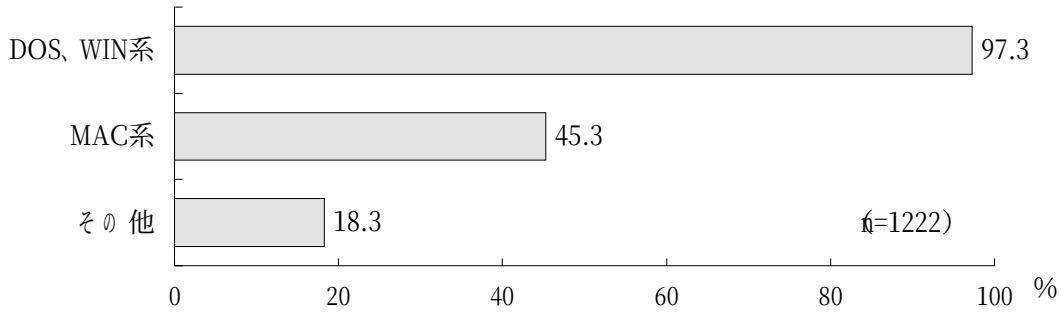
利用しているコンピュータの種類は、やはり「パソコン等」が 97.5%とほとんどの企業が利用している。次いで「ワークステーション」が 51.3%、「汎用機」が 38.6%となっている。コンピュータを「利用していない」という事業所も 0.6%あった。

また、「パソコン等」の内訳をみると最も多いのは「DOS、Windows 系」で 97.3%、「Macintosh 系」は 45.3%であった。

図表Ｉ－３　　利用しているコンピュータの種類



図表Ｉ－４　　利用しているコンピュータの種類（パソコン等内訳）



その他　：　オフコン、APCS、N5200、OS／2、等

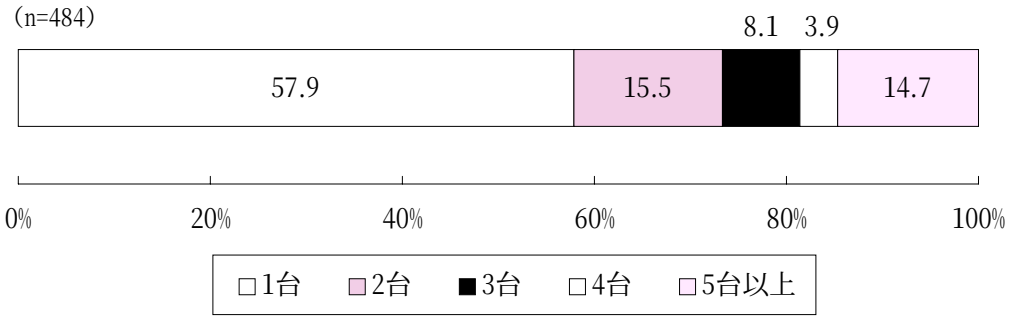
（２）利用しているコンピュータの種類別台数

利用しているコンピュータの台数を種類別にみると、「汎用機」は、全体的に台数は少なく、「1 台」が 57.9%と半数以上を占めている。

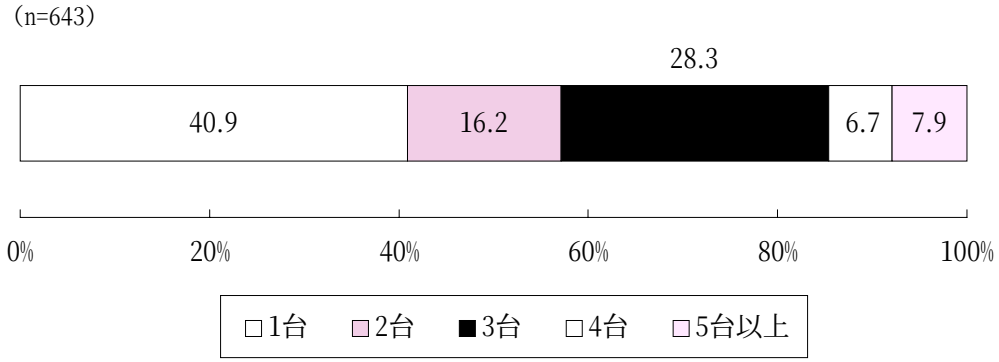
ワークステーションは、「汎用機」よりは多いが、やはり全体的に台数は少なく「1～5 台」が 40.9%で最も多くなっている。しかし、「101 台以上」とする事業所も 7.9%あった。

パソコン等では、「11～50 台」が 28.3%で最も多い。多数の台数を使用している事業所も多く「101～300」が 18.2%、「301 台以上」が 28.3%と、101 台以上のパソコン等を使用している事業所が 37.5%に達している。前回の調査では、この数字は 30.1%であったから、事業所内におけるパソコン大量利用化が進んでいることがわかる。

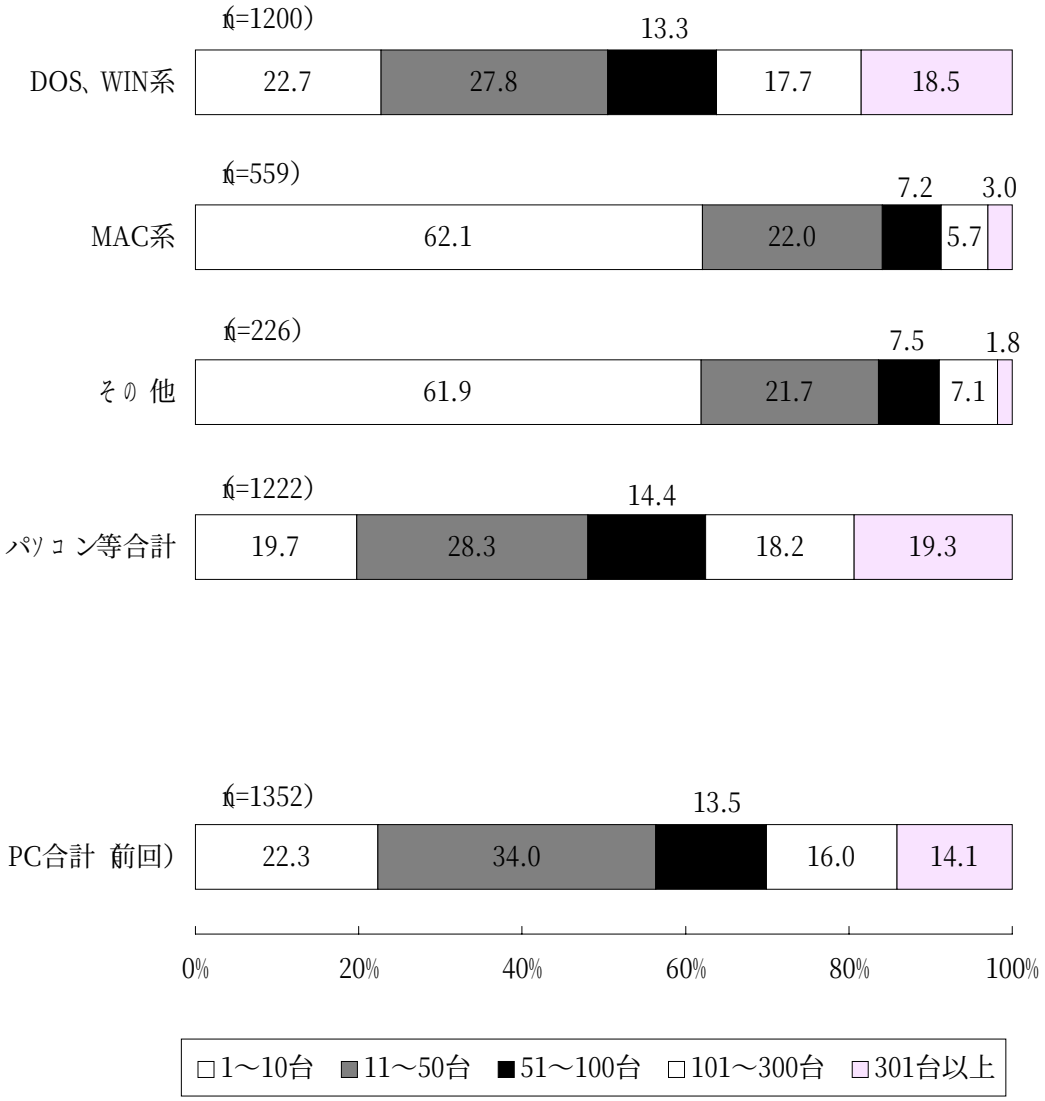
図表Ⅰ－５　利用しているコンピュータ　汎用機



図表Ⅰ－６　利用しているコンピュータ　ワークステーション



図表Ｉ－７　利用しているコンピュータ　パソコン等



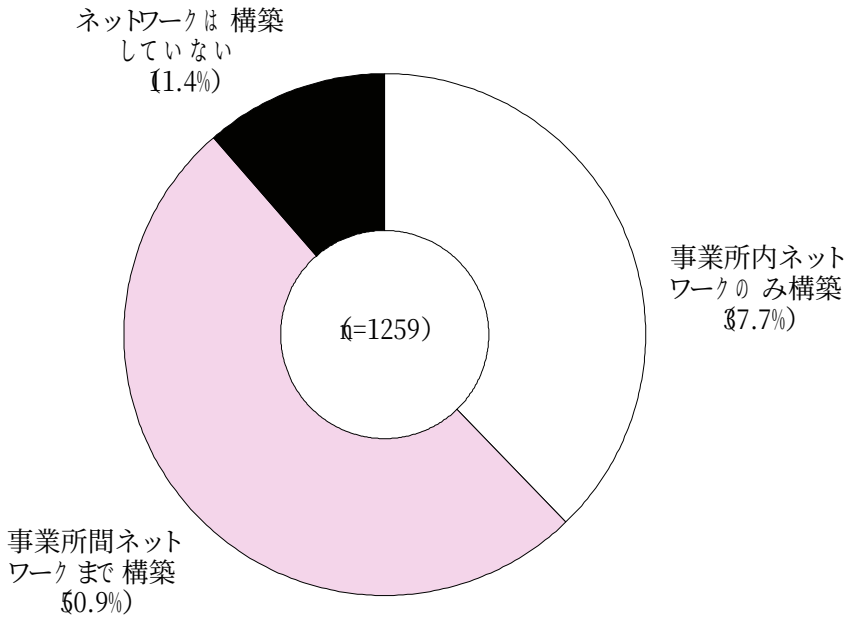
２・４　　ネットワーク化の状況

２・４・１　　社内情報ネットワークの構築状況

（１）社内情報ネットワークの構築状況

社内情報ネットワークについては、「事業所内ネットワーク（LAN）のみ構築」が 37.7%、「事業所間ネットワーク（WAN）まで構築」が 50.9%となっている。「ネットワークを構築していない」のは 11.4%で、実に 9 割近くの事業所で社内情報ネットワークが構築されている。

図表Ⅰ－８　　社内情報ネットワークの構築状況

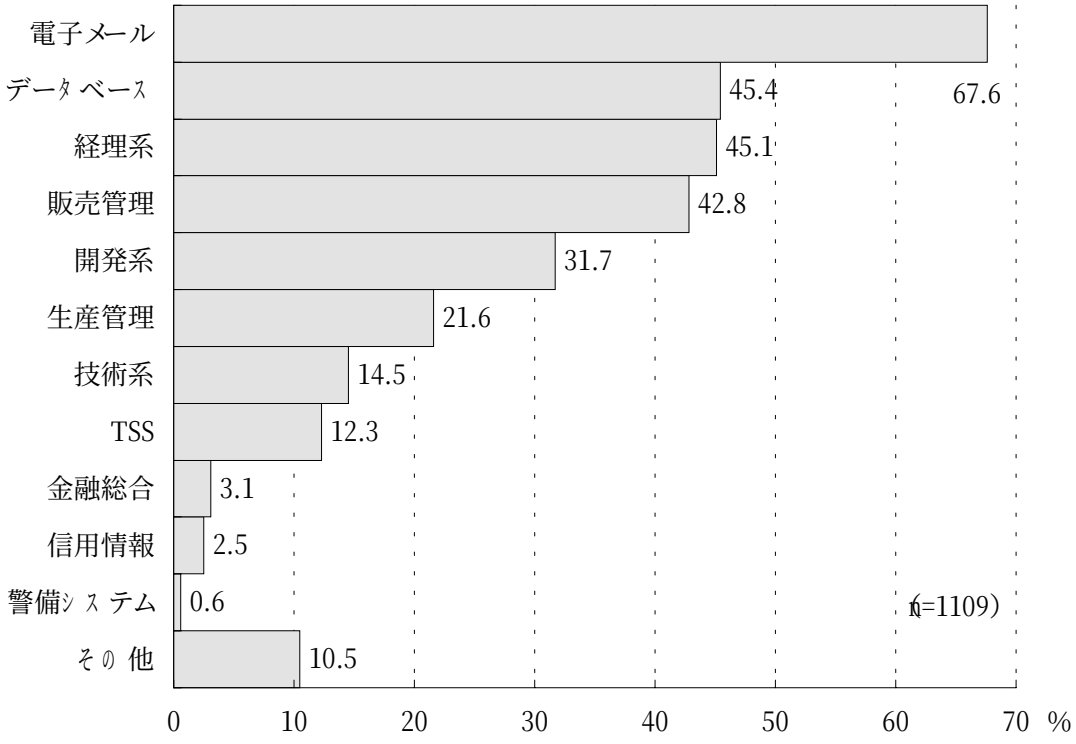


（２）社内情報ネットワークの用途

社内情報ネットワークの用途としては、「電子メール」が最も多く 67.6%、次いで「データベース検索」が 45.4%、「経理系」が 45.1%、「販売管理系」が 42.8%と続いている。

「電子メール」は前回新たに追加した回答項目であるが、前回の 59.5%からさらに 10%近く増えた。パソコン利用の拡大と共に、情報伝達ツールとして定着したことがうかがわれる。

図表Ｉ－９　社内情報ネットワークの用途



その他：グループウェア、ファイル・プリンタ共有、イントラネット、教育・研究、
人事管理、学生管理、文書管理、その他一般事務、等

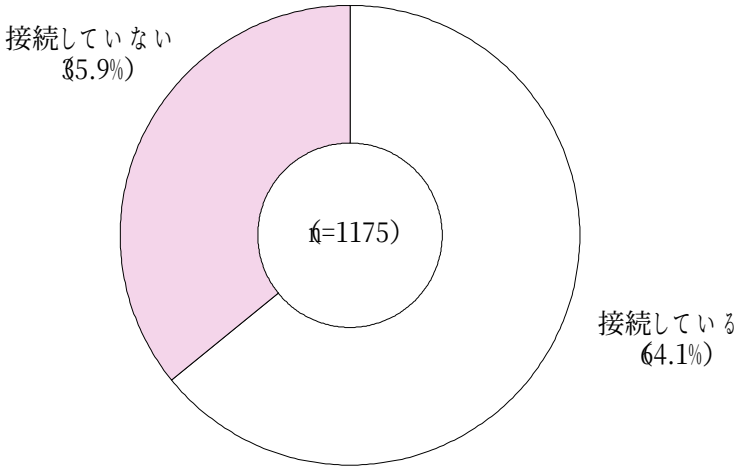
２・４・２　　インターネット接続状況

インターネットへの接続状況については、64.1%と 3 分の 2 近くの事業所が「接続している」。

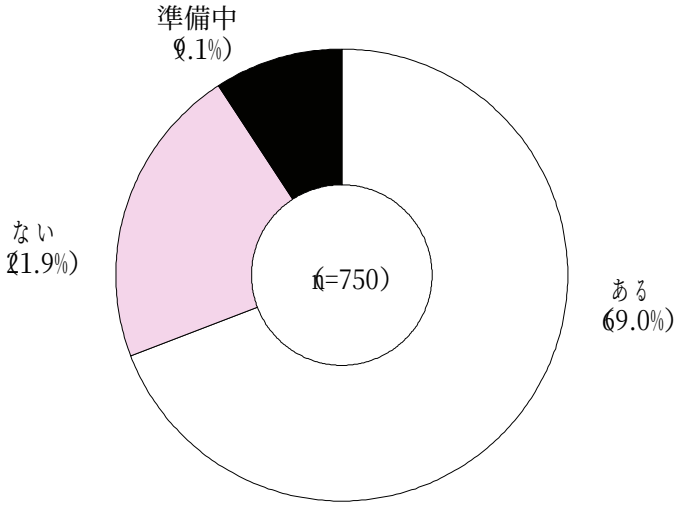
また、接続している事業所で自事業所のホームページが「ある」事業所は 69.1%で、「準備中」とする事業所が 9.1%となっている。

前回の調査と比較すると、いずれも 10%前後増えており、インターネットが一段と普及してきたことがわかる。

図表Ⅰ－10　インターネット接続状況



図表Ⅰ－11　自事業所ホームページの有無

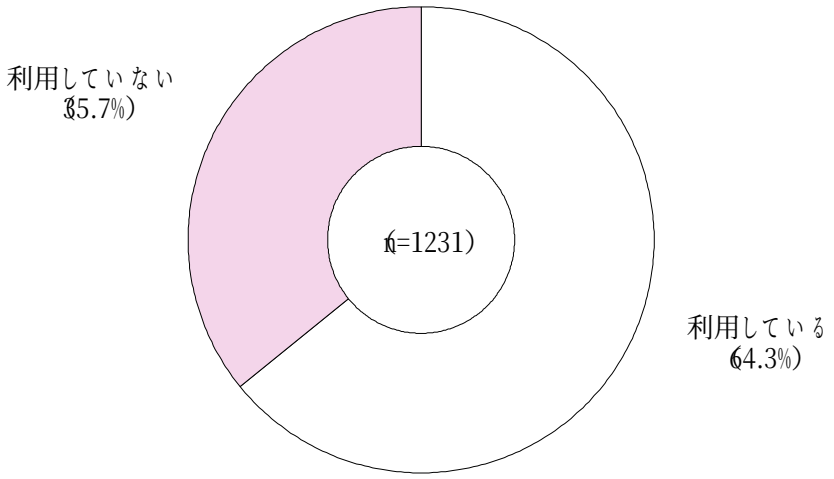


２・４・３　　商用パソコン通信サービスの利用状況

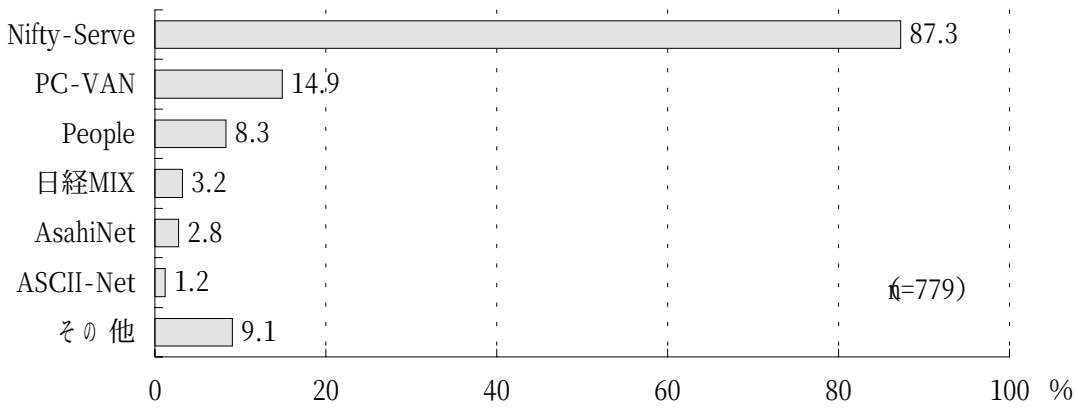
商用パソコン通信サービスの利用状況については、「利用している」とする事業所が64.3%とほぼ 3 分の 2 に達している。しかしながらこれは、前回の調査に比べてわずかながら減少している。インターネットの普及に伴って、パソコン通信が頭打ちになっていることをうかがわせる。

利用している商用パソコン通信サービスとしては、「Nifty-Serve」が圧倒的で 87.3%を占めている。

図表Ⅰ－12　商用パソコン通信サービスの利用状況



図表Ⅰ－13　商用パソコン通信サービスの利用状況



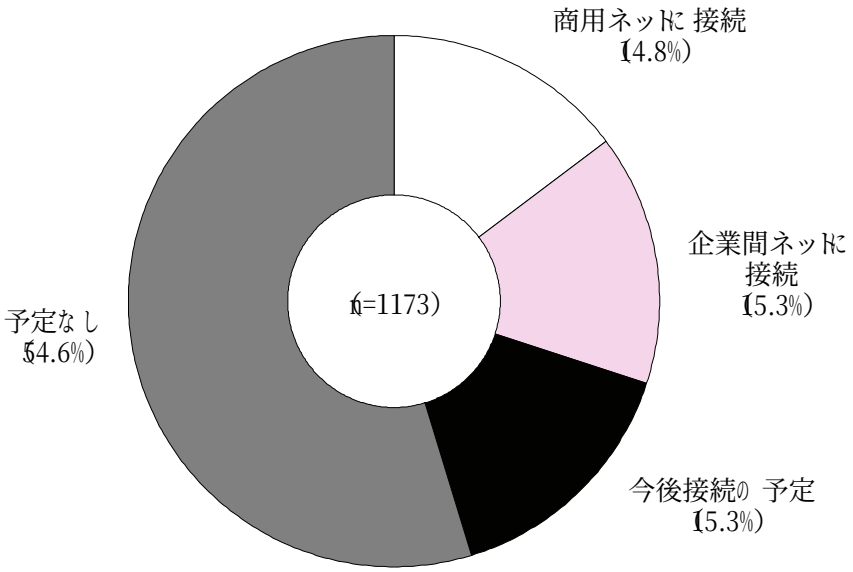
その他：日経テレコン、NTT-PC ネットワーク、JOIS、Nippon-Net、G サーチ、So-net、PATOLS、等

２・４・４　　商用VAN ネットおよびその他の企業間ネットワークとの接続状況

商用 VAN ネットおよびその他の企業間ネットワークとの接続状況については、69.9%とほぼ 7 割の事業所が「接続していない」が、その内 15.3%は「今後接続の予定」としている。

「接続している」30.1%のうち、「商用 VAN ネットに接続」している事業所は 14.8%、「その他の企業間ネットワークに接続」している事業所は 15.3%であった。

図表Ⅰ－14　商用VAN ネットの接続状況



商用 VAN ネット名称：C&C VAN、FENICS、IBM NMS、SECOM-NET、
共同 VAN、TG-VAN、プラネット、NTT-VAN、HITVAN、等

３　コンピュータウイルスによる被害状況

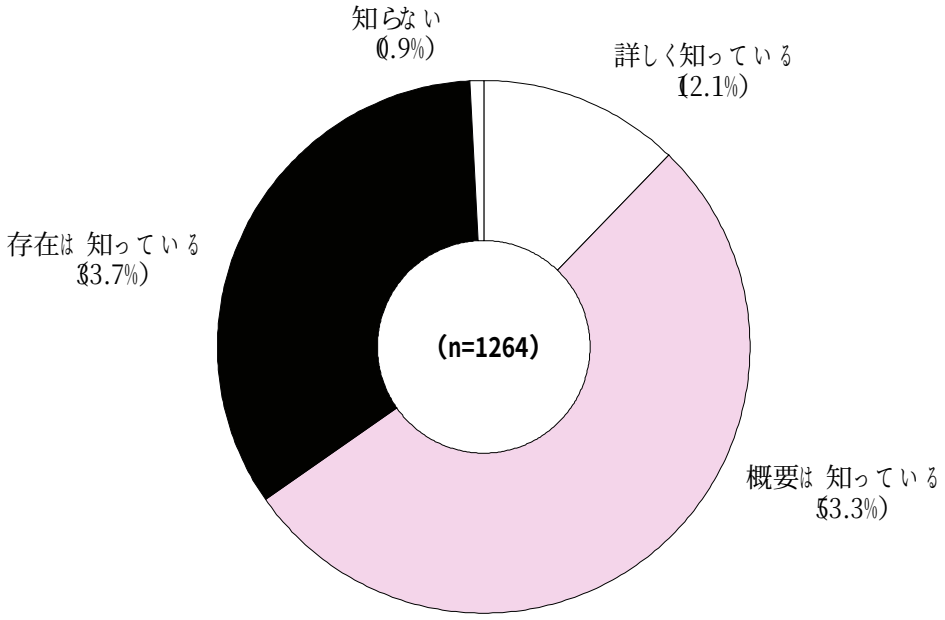
３・１　コンピュータウイルスに対する関心

３・１・１　コンピュータウイルスの認知度

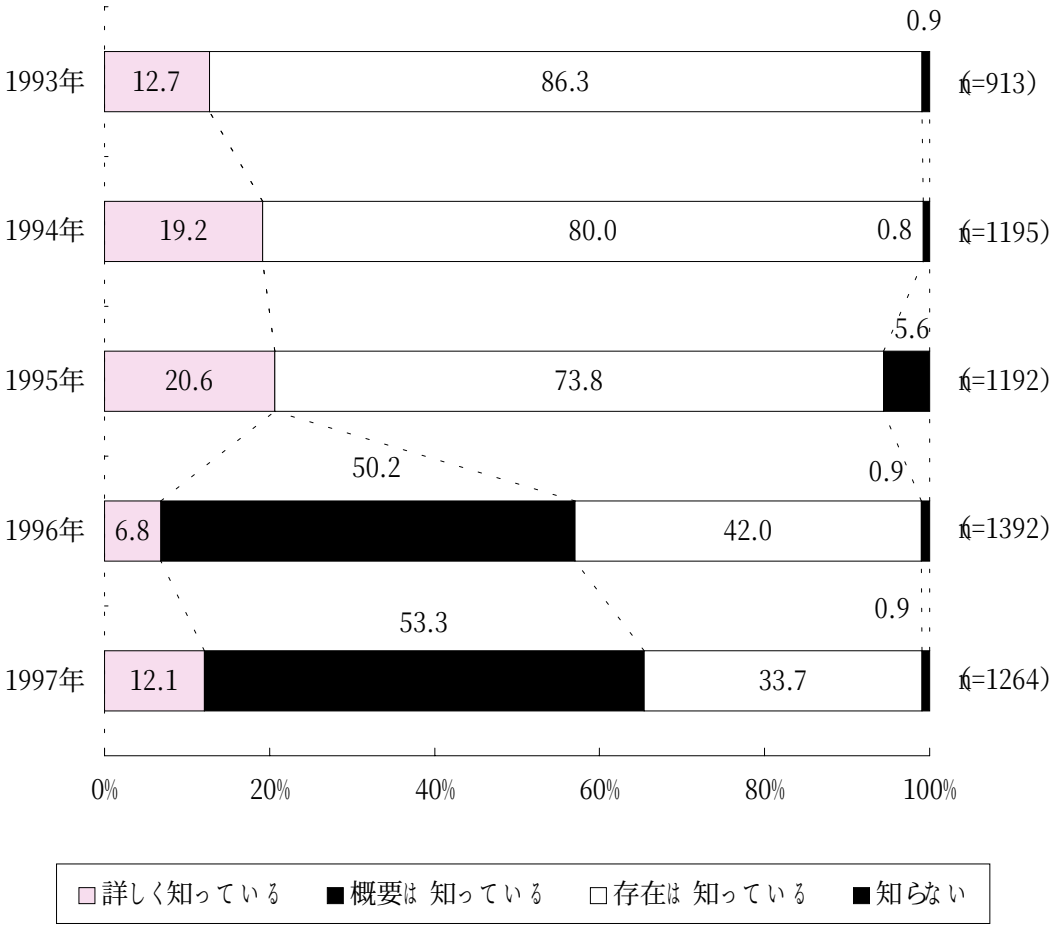
コンピュータウイルスに対する認知度を調査したところ、コンピュータウイルスについて、「詳しく知っている」とする回答は 12.1%、「概要は知っている」が 53.3%、「存在は知っている」が 33.7%で、「知らない」はわずか 0.9%であった。

前回の調査との比較で見てみると、「詳しく知っている」がほぼ倍増し、「詳しく知っている」と「概要は知っている」の合計が 57.0%から 65.4%と 10%近く増加している。言葉だけではなく、内容が伴った形で認知度は上がっているといえよう。

図表Ⅰ－15　コンピュータウイルスの認知度



図表Ⅰ－16　コンピュータウイルスの認知度の推移

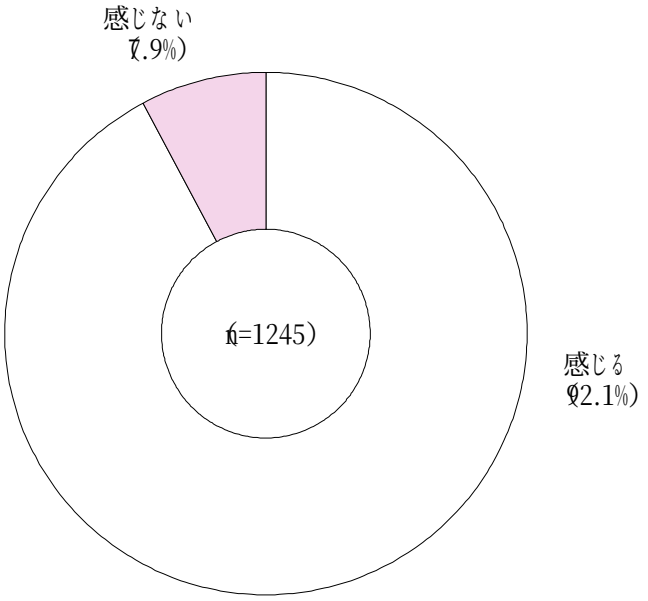


３・１・２　　コンピュータウイルスに対する脅威

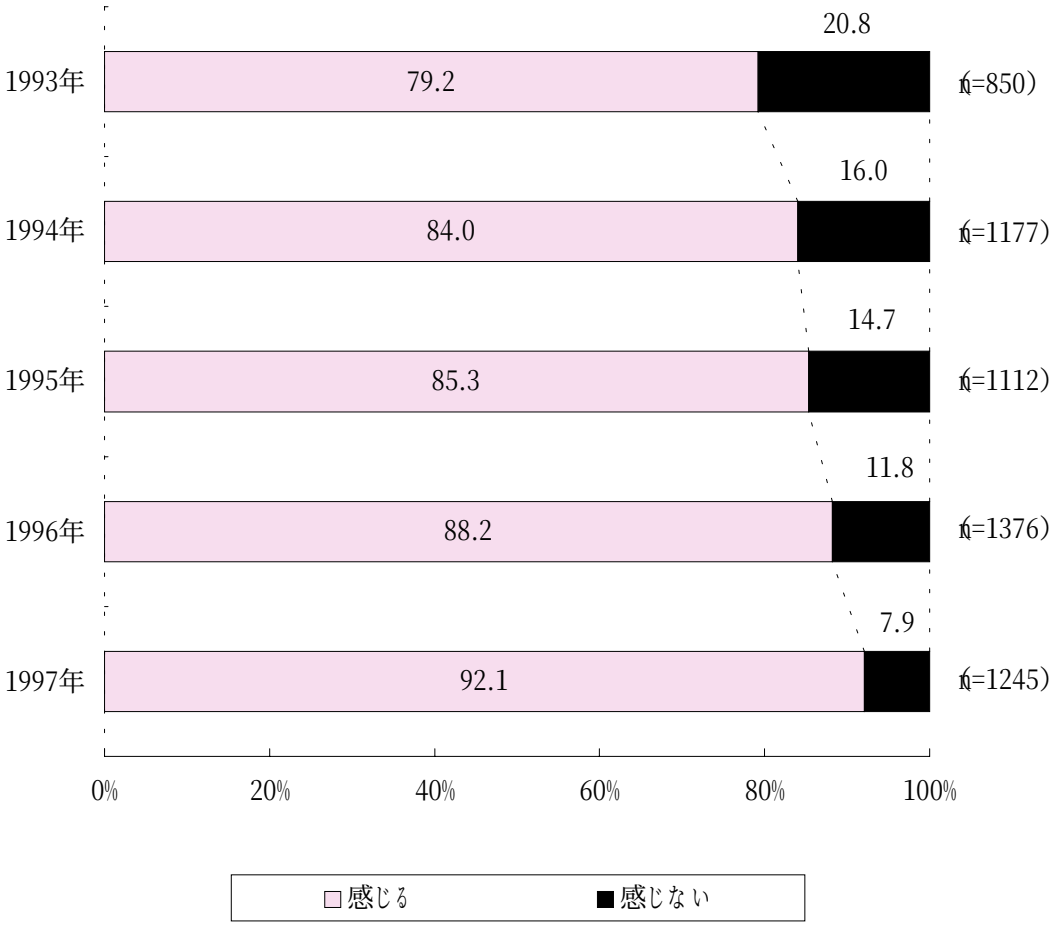
コンピュータウイルスに対する脅威については、「感じる」とする事業所が 92.1％に対して、「感じない」とする事業所は 7.9％であった。

推移をみると、脅威を「感じない」とする回答が、着実に減っており、コンピュータウイルスの認知度が上がるにつれて、コンピュータウイルスに対する知識も浸透しつつあることを示している。

図表Ⅰ－17　コンピュータウイルスに対する脅威



図表Ⅰ－18　コンピュータウイルスに対する脅威の推移

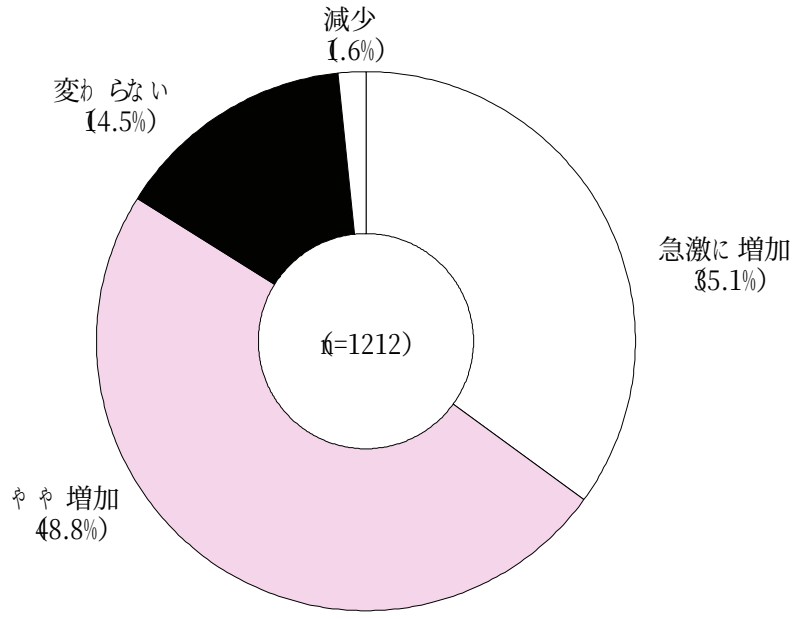


３・１・３　　今後の被害予想

コンピュータウイルスによる今後の被害予測については、「急激に増加する」とする回答が 35.1%、「やや増加する」が 48.8%と、現在より増加するという回答が 8 割以上を占めている。

推移をみると、前回の調査で減少に転じた「急激に増加する」「やや増加する」が、今回の調査結果では共に再び増加した。パソコン利用者の増加やインターネットの普及等によって今後、コンピュータウイルスの増加のスピードが、ワクチンソフトの普及やセキュリティ技術の向上を上回るとみているものと思われる。ことにマクロウイルスに対する認識が高まったためか、「急激に増加する」が大幅に増えている。

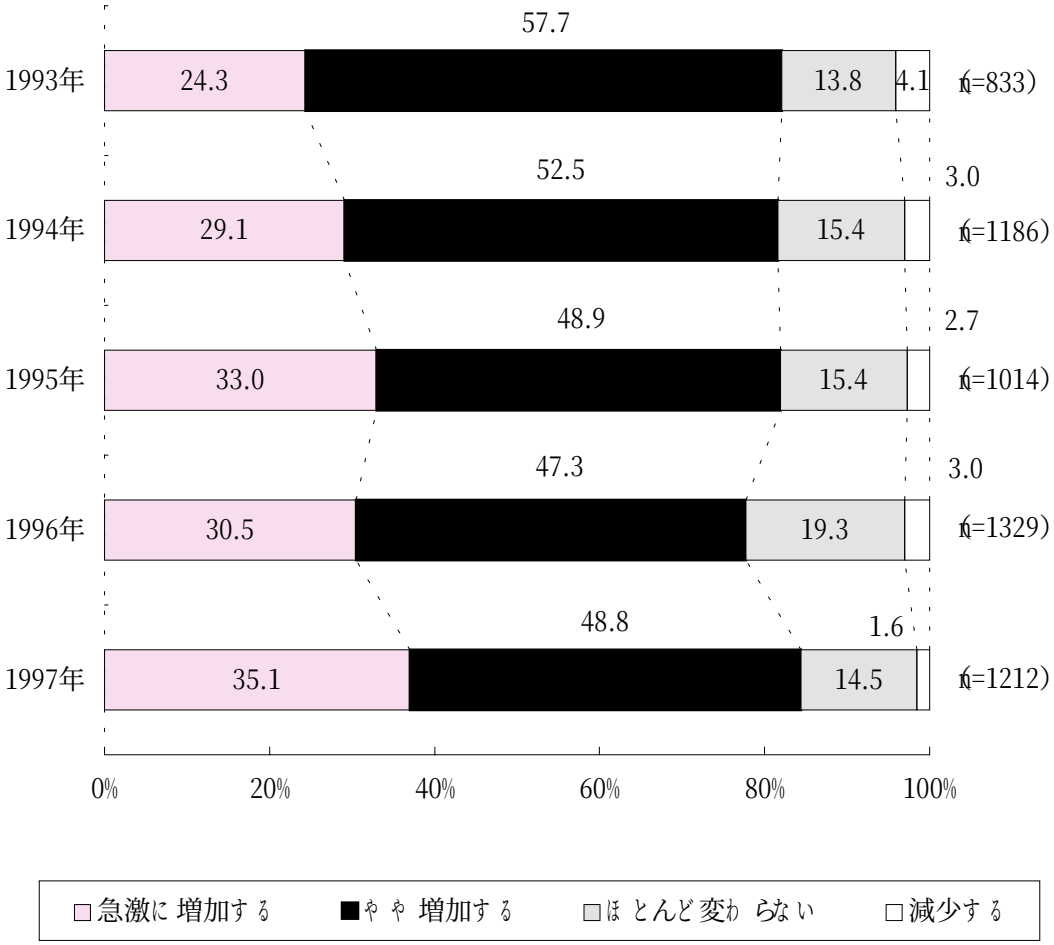
図表Ⅰ－19　今後の被害予測



増加の理由　：　パソコン利用者の拡大、ことに初心者・一般ユーザの増加、
ネットワーク化の進展、LAN およびインターネットの普及
マクロウイルスは作成容易、ウイルスとワクチンのいたちごっこ
セキュリティに対する認識の低さ、等

減少の理由　：　ワクチンソフトの普及、機能向上、
セキュリティ対策の強化、セキュリティ技術の向上
ハードメーカ、ソフトメーカの対応、
ユーザのモラルアップ、等

図表Ⅰ－20　今後の被害予測

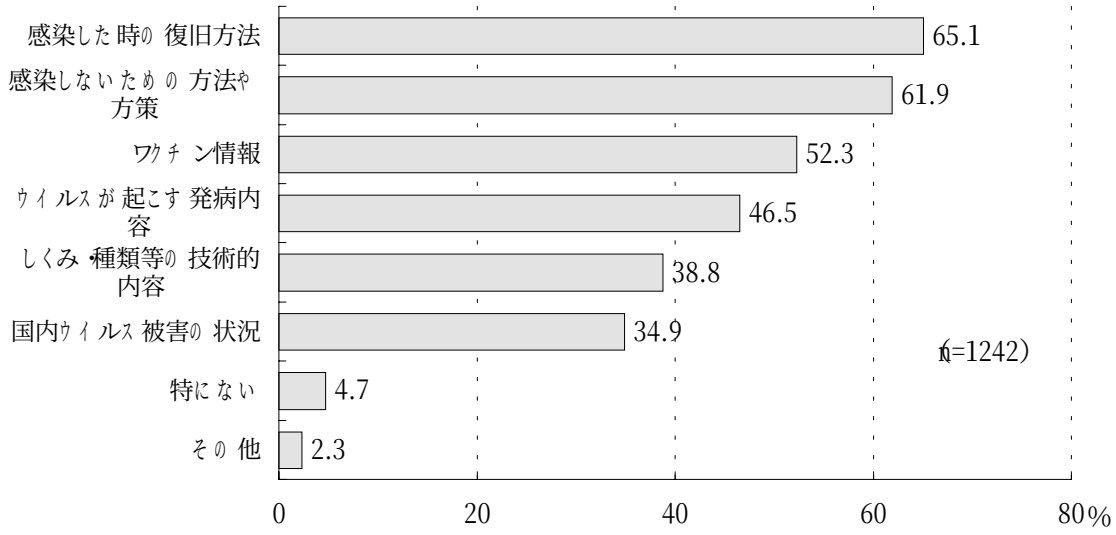


３・１・４　　知りたい情報

コンピュータウイルスに関連して知りたいと思っている情報としては、「感染したときの復旧方法」が最も多く 65.1%、次いで「感染しないための方法や方策」が 61.9%、「ワクチン情報」が 52.3%、「ウイルスが起こす発病内容」が 46.5%と続いている。

推移をみると、毎年全般的に情報ニーズは高いが、今回の調査では特に被害が大幅に増加したことを反映してか、「感染したときの復旧方法」や「ワクチン情報」など具体的な情報を求めている。

図表Ⅰ－21　求められている情報



その他　：　ワクチンソフトの性能評価および活用方法、
ウイルスに関する情報源

図表Ⅰ－22　今後求められる情報の推移

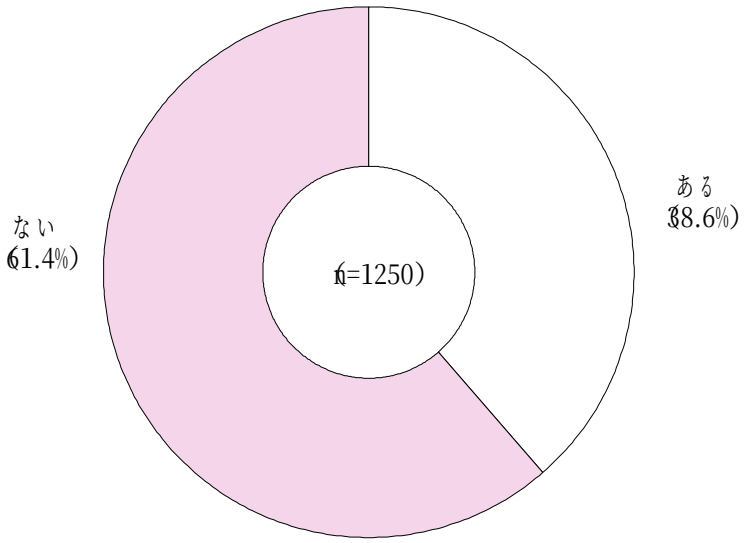
	1993年	1994年	1995年	1996年	1997年
感染したときの復旧方法	62.6	65.3	58.6	63.8	65.1
感染しないための方法や方策	69.4	65.4	60.0	64.5	61.9
ワクチン情報		34.7	39.9	44.3	52.3
ウイルスが起こす発病内容	24.6	43.6	37.9	42.4	46.5
しくみ・種類等の技術的内容	48.9	45.3	40.2	38.4	38.8
国内ウイルス被害の状況		28.7	32.4	38.6	34.9
特にない	6.0	4.7	11.5	5.0	4.7
その他	2.9	1.1	1.4	1.6	2.3
n＝	834	1160	1135	1374	1242

３・２　　コンピュータウイルスによる被害状況

３・２・１　　コンピュータウイルス感染経験の有無

1997 年 1 月から 12 月までの 1 年間にコンピュータウイルスに感染したことのある事業所は 482 件（38.6%）であった。3 分の 1 以上の事業所で、コンピュータウイルスによる感染経験があったと回答している。前回の調査では、感染を経験したことのある事業所の比率は 17.9%であったから、一挙に倍増したことになる。

図表Ⅰ－23　コンピュータウイルス感染経験の有無

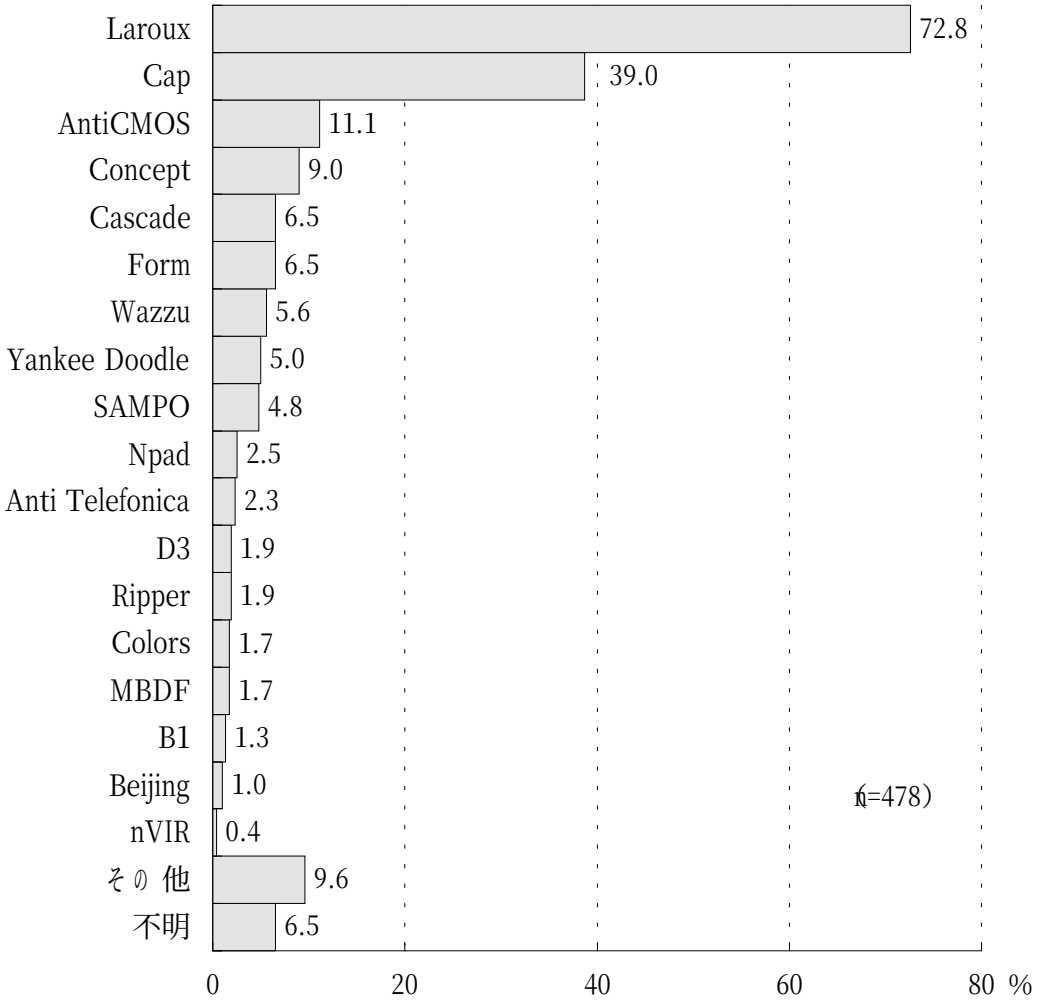


３・２・２　　感染したウイルスの名称

感染したウイルスとしては、昨年までの調査ではまだそれほど目立たなかったマクロウイルスが急激に増加したことが特筆される。実際の調査結果をみても「Excel Macro Laroux」は実に 72.8%に達しており、「Word Macro Cap」も 39.0%となっている。一方、従来多かった「AntiCMOS」「Cascade」「Form」「YankeeDoodle」はいづれも 10%前後で、前回の調査の半分あるいは 3 分に 1 以下に減少している。

その他回答項目にないものでは、新種の「Word Macro」および「Parity Boot B」等が目立っている。

図表Ⅰ－24　感染したウイルスの名 称



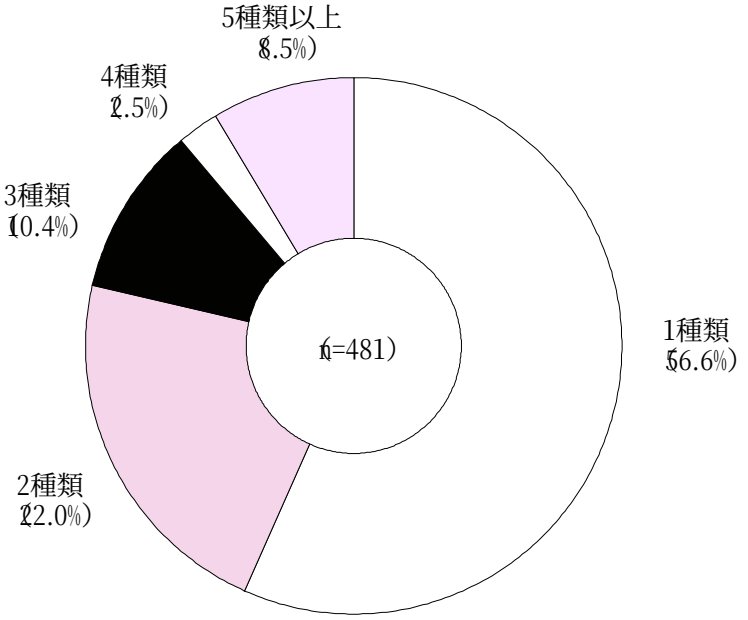
その他　：　Parity Boot、Niknat、Monkey、showoff、Lunch

３・２・３　感染したウイルスの種類数

感染したウイルスの種類数は 56.5%が「1 種類」であるが、複数の種類のウイルスに感染したとする事業所が 43.5%あった。また、「5 種類以上」の事業所も 8.5%に達している。

前回の調査と比較すると、複数感染が約 5%増加している。

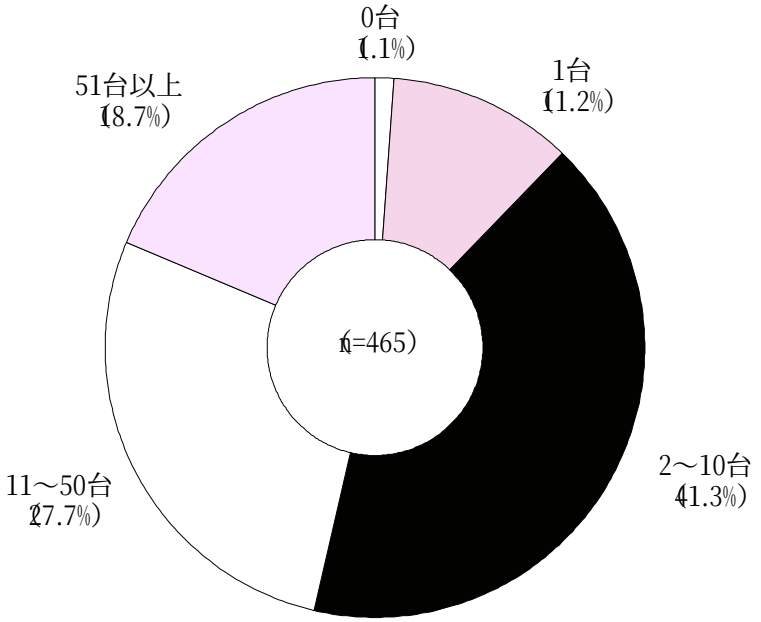
図表Ⅰ－25　感染したウイルスの種類数



３・２・４　　感染したコンピュータの台数

感染したコンピュータの台数は、「2～10 台」が最も多く 41.3%を占めている。「10 台以上」のコンピュータに感染した事業所は 46.4%であるが、これは昨年の調査結果では 21.7%に過ぎなかった。特に「51 台以上」の大規模被害が 4.1%から 18.7%と大幅に増加している。ネットワーク化の進展とマクロウイルスの増加に伴い、被害の大規模化が急激に進んできていることがわかる。

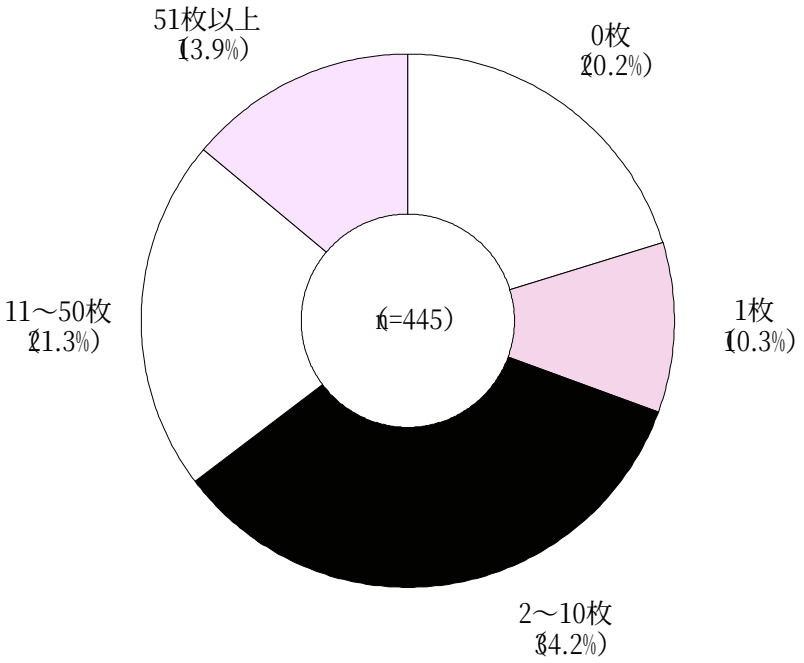
図表Ⅰ－26　感染したコンピュータの台数



３・２・５　　感染したフロッピーディスク（FD）の枚数

感染したフロッピーディスクの枚数については、「2～10 枚」が最も多く 34.2%、次いで「11～50 枚」21.2%となっている。「51 枚以上」とする事業所も 13.9%あった。

図表Ⅰ－27　感染した FD の枚数



４　コンピュータへの不正アクセスによる被害状況

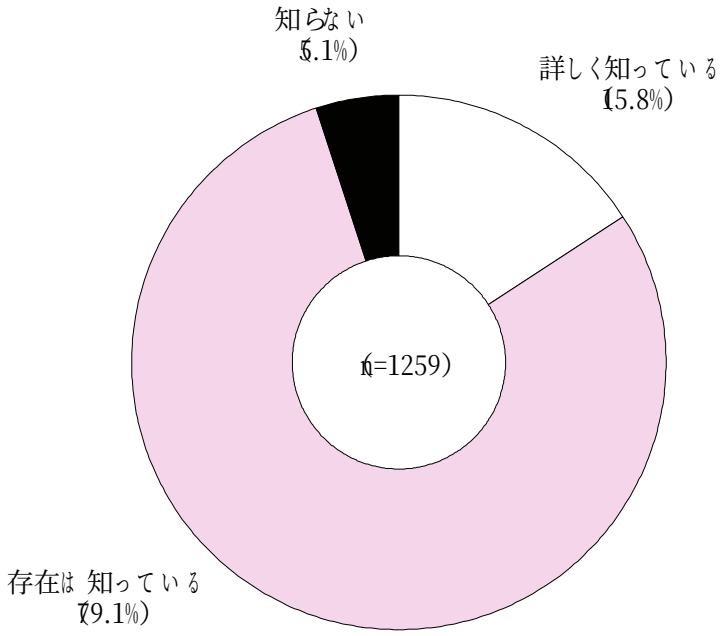
４・１　コンピュータ不正アクセスに対する関心

４・１・１　コンピュータ不正 アクセスの認知度

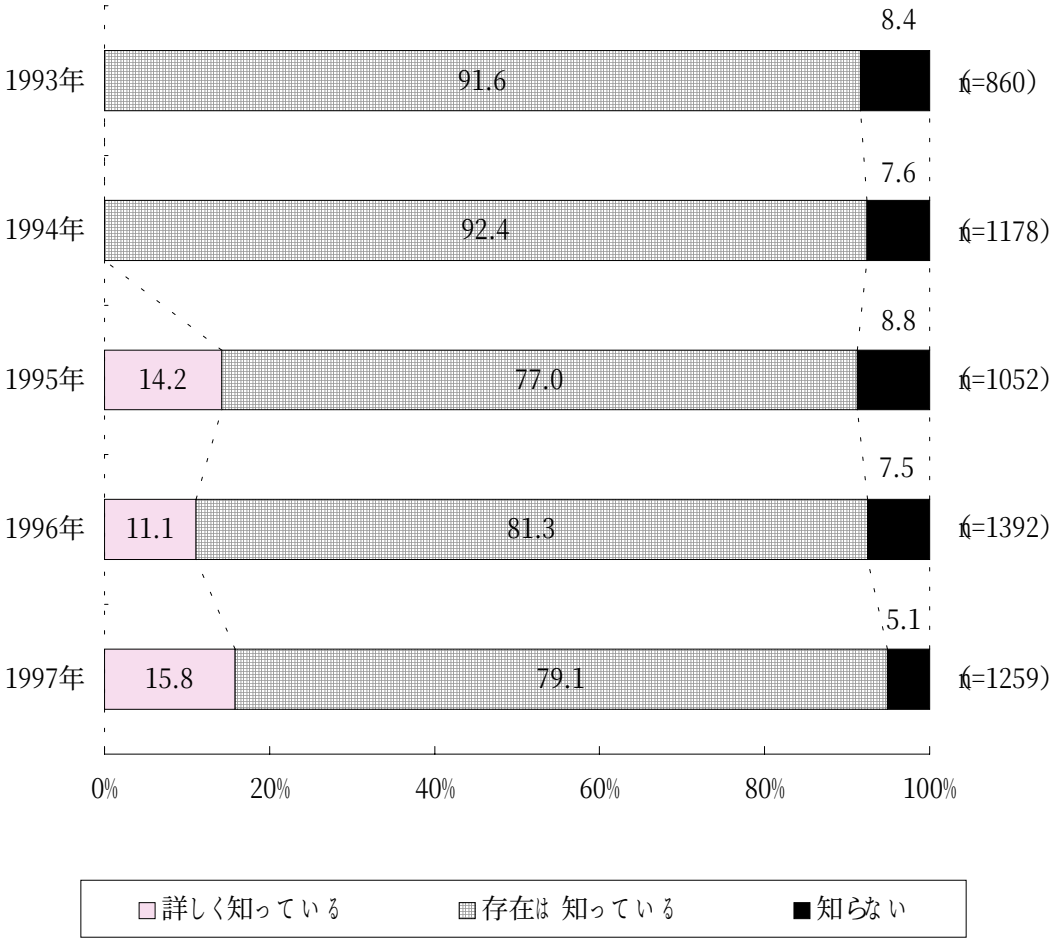
コンピュータの不正アクセスについて、「詳しく知っている」とする回答は 15.8%、「存在は知っている」が 79.1%で「知らない」は 5.1%であった。

推移をみると、認知度は着実に上がってはいるが、コンピュータウイルスよりやや低い値になっている。

図表Ⅰ－28　コンピュータの不正アクセスの認知度



図表Ⅰ－29　コンピュータの不正アクセスの認知度の推移

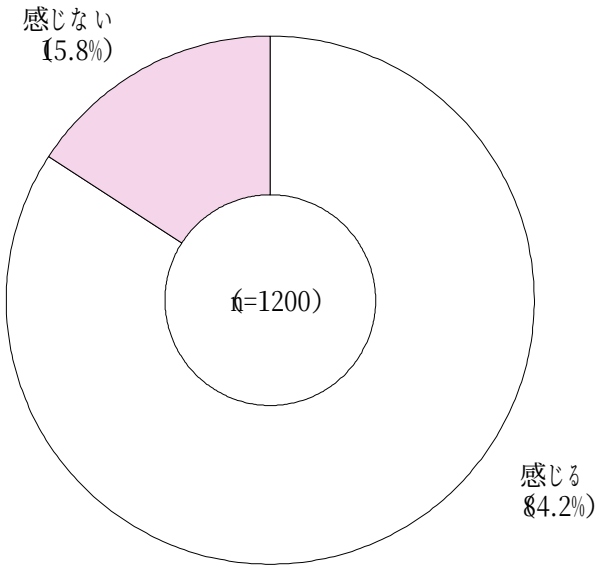


４・１・２　　コンピュータの不正アクセスに対する脅威

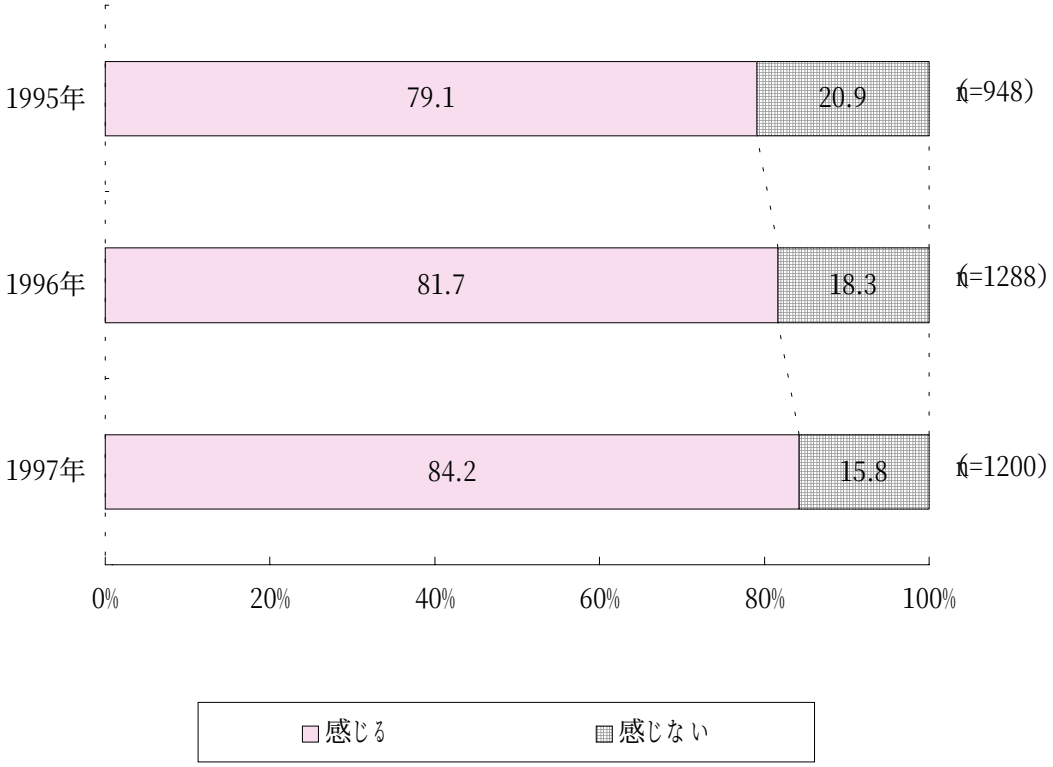
コンピュータの不正アクセスに対する脅威を「感じる」とする回答は 84.2%、「感じない」は 15.8%となっており、コンピュータウイルスに比べ「脅威を感じない」とする回答がやや多くなっている。

推移をみると、認知度の上昇に比例するように「感じる」という回答が増えている。しかしながら、不正アクセスの脅威に対する認識はまだ十分とはいえない。

図表Ⅰ－30　コンピュータの不正アクセスに対する脅威



図表Ⅰ－31　コンピュータへの不正アクセスに対する脅威の推移

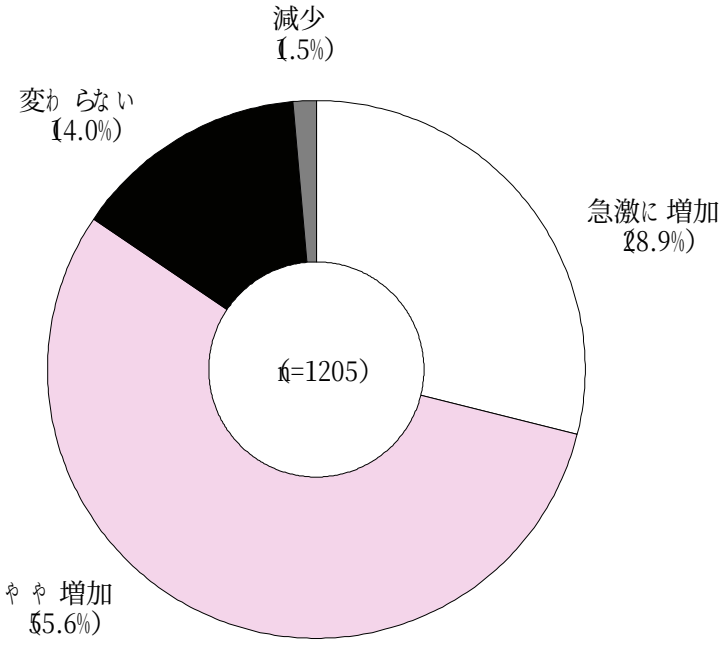


４・１・３　　今後の被害予測

コンピュータへの不正アクセスによる今後の被害予測については、「急激に増加する」という回答が 28.9%、「やや増加する」が 55.6%で、84.5%の事業所が、不正アクセスによる被害は現在より増加すると予測している。これはコンピュータウイルスとほぼ同じ割合である。

推移をみると、ほぼ横ばいであるが、「急激に増加する」が若干ながら減少している。セキュリティ技術の向上に対する期待のあらわれであろうか。

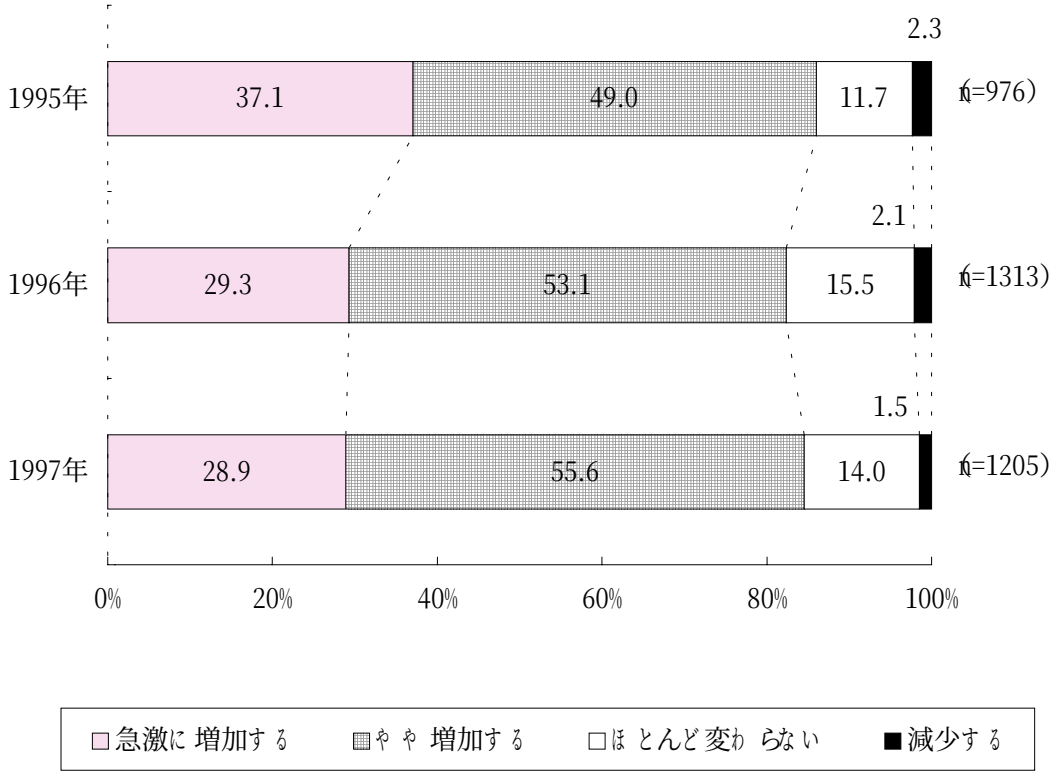
図表Ⅰ―32　今後の被害予測



増加の理由　：　ネットワークの普及・拡大、インターネットの利用者の増加、
ユーザの急激な増加、PC 台数の増加、
ハッカーを絶滅させるのは困難、危機意識の欠如、
経験不足、ネットワーク技術者の不足、等

減少の理由　：　セキュリティ技術の向上、機能の強化、
企業ユーザにおけるセキュリティ対策の強化、等

図表Ⅰ－33　今後の被害予測



４・１・４　　求められている情報

不正アクセスについて、知りたいことの情報の回答を整理すると以下のようになる。

①不正アクセス自体についての情報

・方法・手口

・具体的な事例

・内容および種類

・発見方法

②被害状況

・実態（発生状況、被害状況）

・同じ業界における被害状況

③対応策

・防止方法、対応策

・法的規制の現状および見通し

内容的には上記のように集約されるが、この項目に対する回答率は極めて高かった。不正アクセスに対する関心の高まりと、それに対する情報の不足を示すものといえよう。

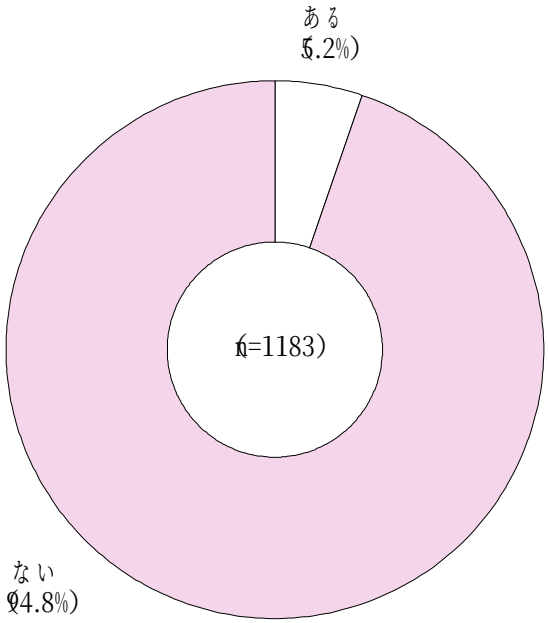
４・２　　コンピュータ不正アクセス被害状況

４・２・１　　コンピュータ不正アクセス被害経験の有無

1997 年 1 月から 12 月までの 1 年間にコンピュータへの不正アクセスによる被害を受けたことのある事業所は 61 件（5.2%）であった。

ちなみに、前回の調査では 32 件（2.5%）であったから、一挙に倍増したことになる。

図表Ⅰ－34　コンピュータの不正アクセス被害経験の有無



Ⅱ　被害及び対策の現状と課題に関する報告書

1　コンピュータウイルスの被害及び対策の現状と課題

2　コンピュータへの不正アクセスの被害及び対策の現状と課題

1　コンピュータウイルスの被害及び対策の現状と課題

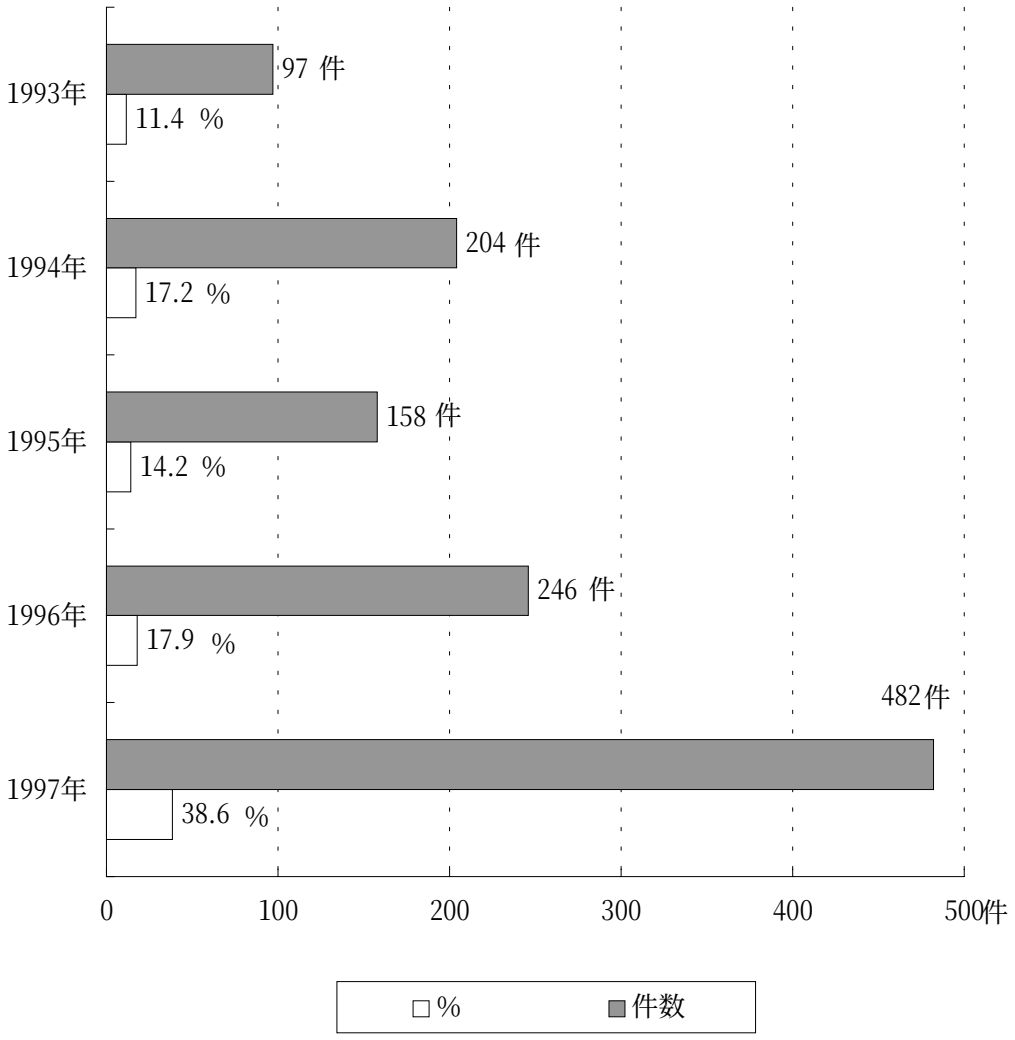
1・1　被害発生状況

（1）コンピュータウイルス感染件数の推移

「コンピュータウイルス被害状況報告」でも記したように、コンピュータウイルスの被害件数は 482 件で全体の 38.6%に達している。

感染件数の推移をみると、1995 年に一時的に減少したが、昨年の調査より著しく増加し、今回の調査結果が件数および割合共過去最高であった。

図表II－1　コンピュータウイルス感染件数の推移



（２）業種別被害発生状況

被害発生状況を業種別にみると、発送件数が多いこともあり、「製造業」と「情報サービス業」が突出しており、次いで「卸売・小売業」「その他サービス業」「教育・研究機関」「建設業」などで被害件数が多くなっている。

これを回答事業所数との割合でみると、「製造業」「情報サービス業」などで 50%以上の被害発生率となっている。

前回の調査と比較すると、すべての業種で被害発生率が大幅に増加している。ネットワーク化の進展とマクロウイルスの蔓延によるものと思われる。

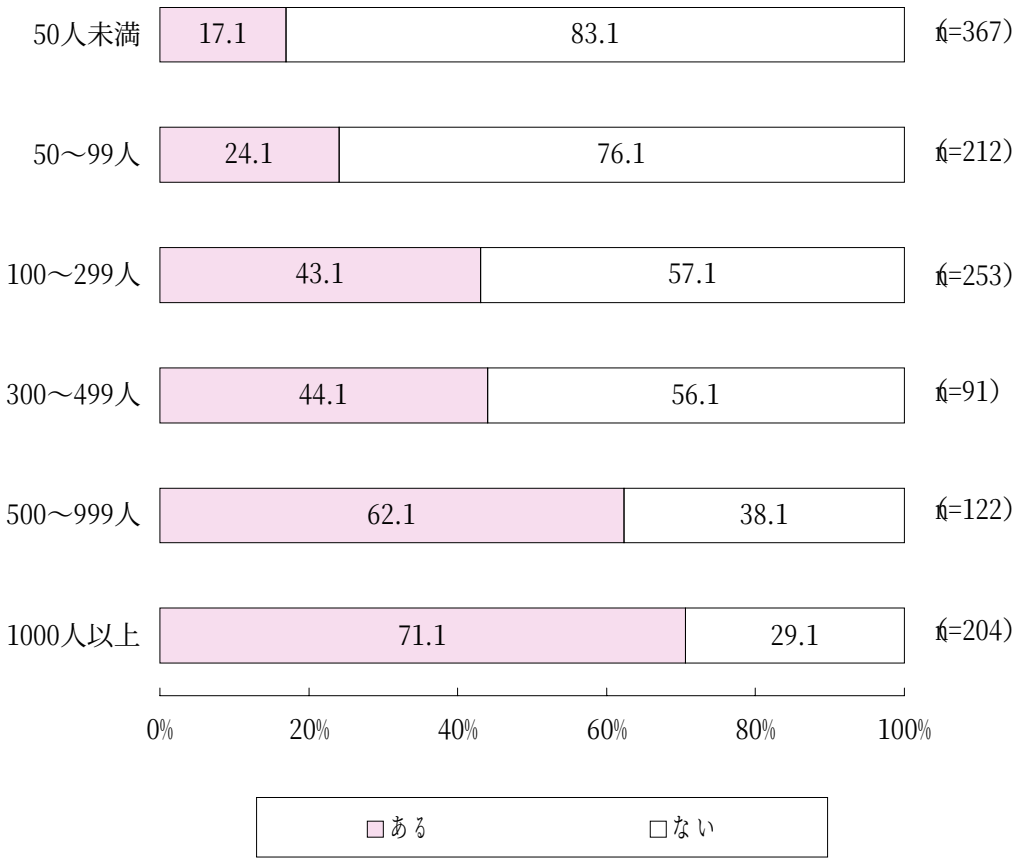
図表Ⅱ－２　　業種別被害発生状況

業　種	件数	回答数	%	業　種	件数	回答数	%
農林水産業	2	6	33.3	新聞・放送業	1	7	14.3
鉱業	2	5	40.0	情報サービス業	124	246	50.4
建設業	23	60	38.3	物品賃貸業	1	4	25.0
製造業	164	319	51.4	遊興娯楽業	1	2	50.0
出版・印刷業	8	20	40.0	医療業	6	18	33.3
卸売・小売業	42	154	27.3	教育・研究機関	25	113	22.1
金融・保険業	13	35	37.1	政治、経済、文化団体	5	24	20.8
不動産業	5	13	38.5	その他サービス業	27	81	33.3
運輸業	5	17	29.4	政府、政府関係機関	6	18	33.3
通信業	4	9	44.4	地方公共団体	15	79	19.0
電力業	1	2	50.0	その他	1	12	8.3
ガス業	1	5	20.0				

（３）就業者数別被害発生状況

就業者数別の被害状況については、規模が大きくなるにしたがって増加する傾向がはっきり現れており、「1000 名以上」の事業所では実に 71.1％と３分の 2 強に達している。これは規模の大きな企業ほどコンピュータの導入台数が多く、ネットワーク化も進み、また利用者も多いので感染の機会が多いためと考えられる。特にコンピュータに関係しない一般の企業においても、コンピュータウイルスに関するセキュリティ対策に本格的に取り組まなければならない段階に来ているといえる。

図表Ⅱ－３　　就業者数別被害発生状況



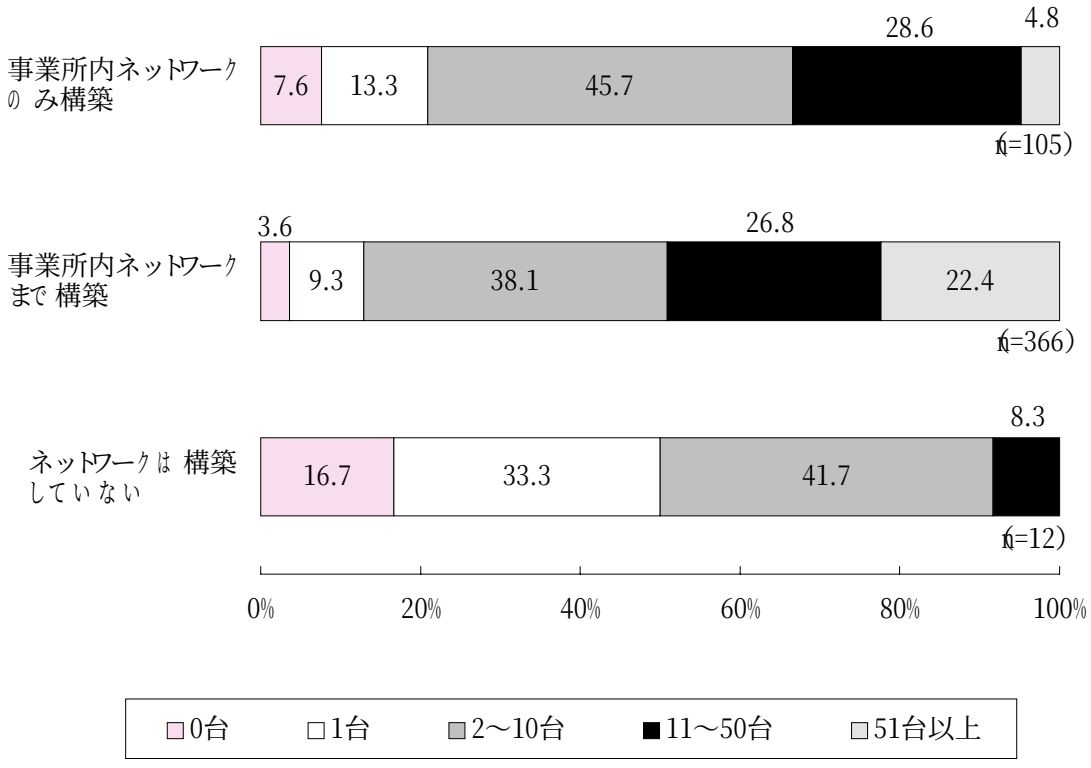
（４）ネットワーク構築状況別被害発生状況

ネットワークの構築状況別の感染したコンピュータの台数をみると、「1 台」という小規模な被害は、「ネットワークは構築していない」事業所では 33.3%だったが、「ネットワークを構築している」事業所では 10%前後であった。

「11～50 台」の比較的規模の大きな被害では、「ネットワークは構築していない」事業所が最も少なく 8.3%であったが、「ネットワークを構築している」事業所では 30%近くに達している。「ネットワークを構築していない」事業所の方が被害の規模は比較的小さい。

LAN から WAN とネットワークの規模が拡大するにつれて、被害台数も多くなっており、「事業所間ネットワークまで構築」している事業所では「51 台以上」が 22.4%に及んでいる。

図表Ⅱ－４　ネットワーク構築状況別被害発生状況



１・２　　セキュリティ対策実施状況

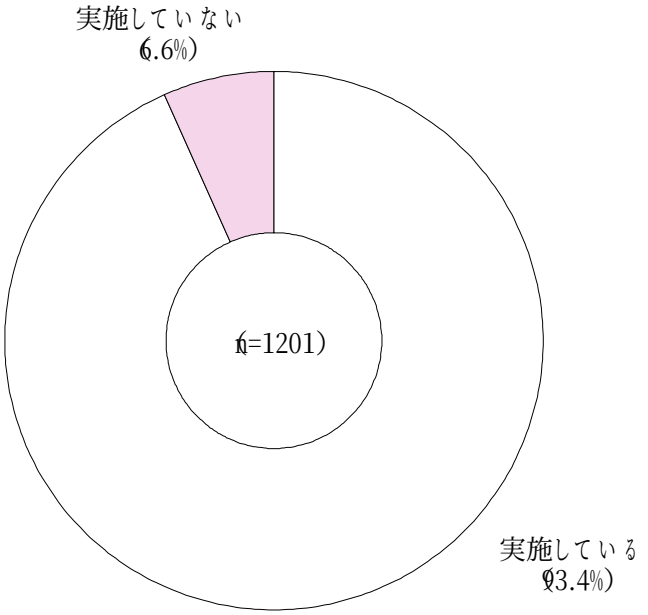
１・２・１　　現在実施しているセキュリティ対策

コンピュータウイルスに関するセキュリティ対策については、93.4%の事業所が現在「実施している」としており、「実施していない」事業所は 6.6%であった。

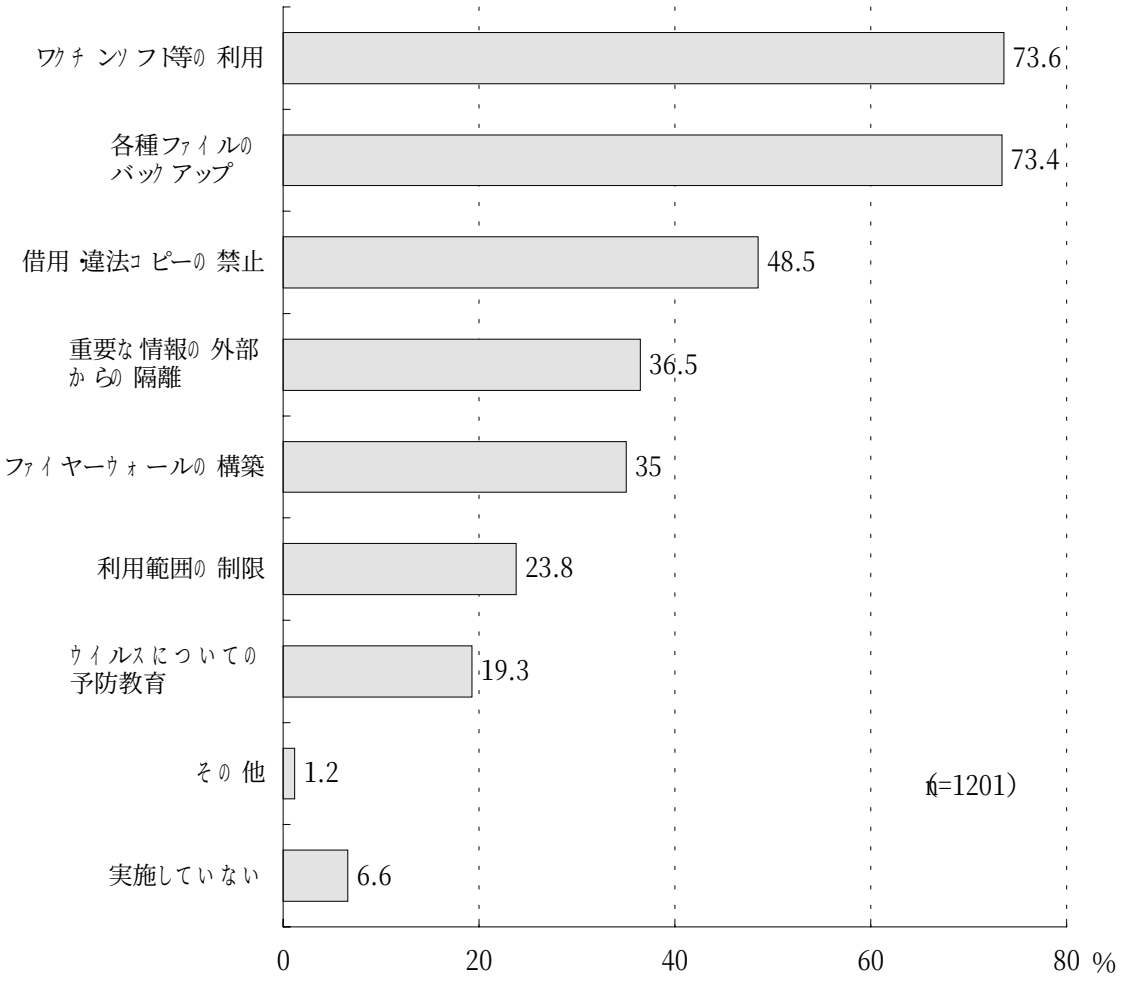
現在実施している具体的な対策としては、73.6%の「ワクチンソフト等の利用」と 73.4%の「各種ファイルのバックアップ」が突出している。以下、「借用・違法コピーの禁止」が 48.5%、「重要な情報の外部からの隔離」36.5%、「ファイヤーウォールの構築」35.0%と続いている。

前回の調査と比較すると「ワクチンソフト等の利用」が大幅に増え１位になったこと、「ファイヤーウォールの構築」および「ウイルスについての予防教育」が大幅に増加したことが目立っている。

図表Ⅱ－５　　セキュリティ対策の実施状況



図表Ⅱ－６　　現在実施しているセキュリティ対策

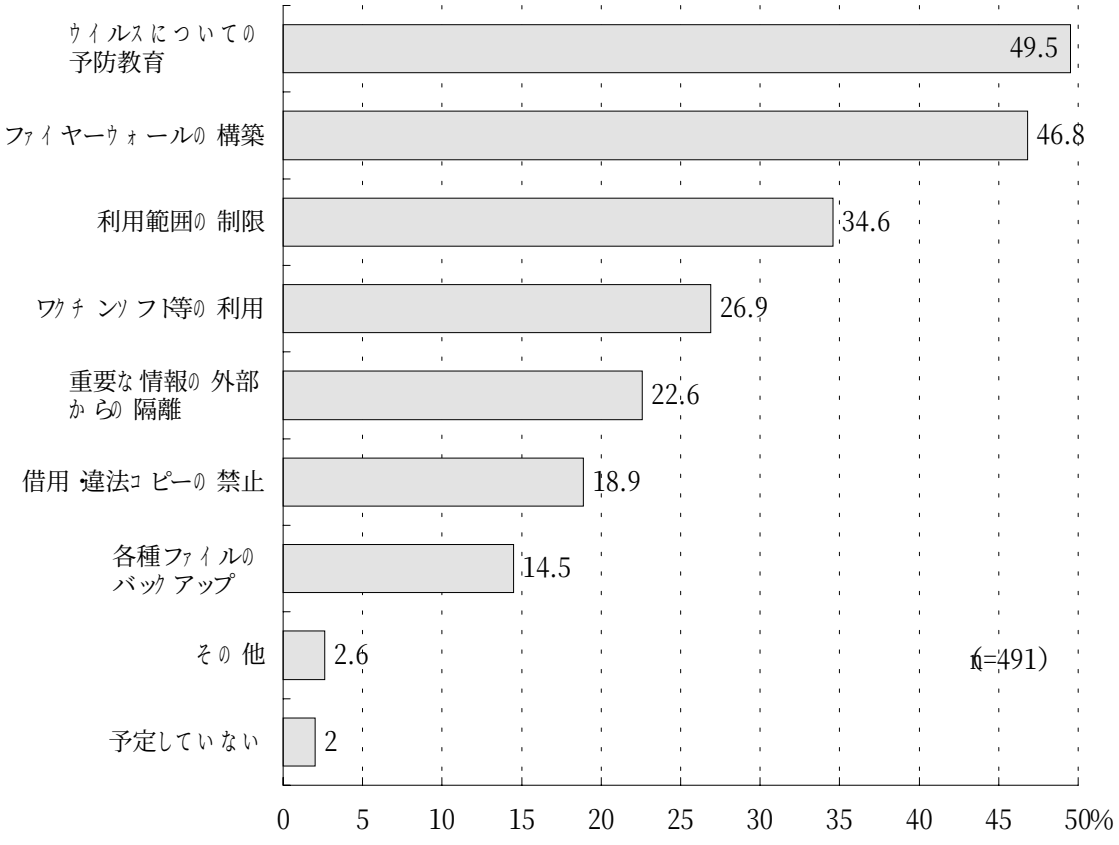


１・２・２　　今後実施予定のセキュリティ対策

（１）今後実施予定のセキュリティ対策

現在実施のセキュリティ対策の継続を含む、今後実施予定の対策としては、「コンピュータウイルスについての予防教育」が 49.5%で最も多く、次いで「ファイヤーウォールの構築」が 46.8%、「利用範囲の制限」が 34.6%となっている。ウイルス被害の増加に伴って、ユーザ教育への認識が高まり、セキュリティ対策も本格化・多様化しつつあることを示している。

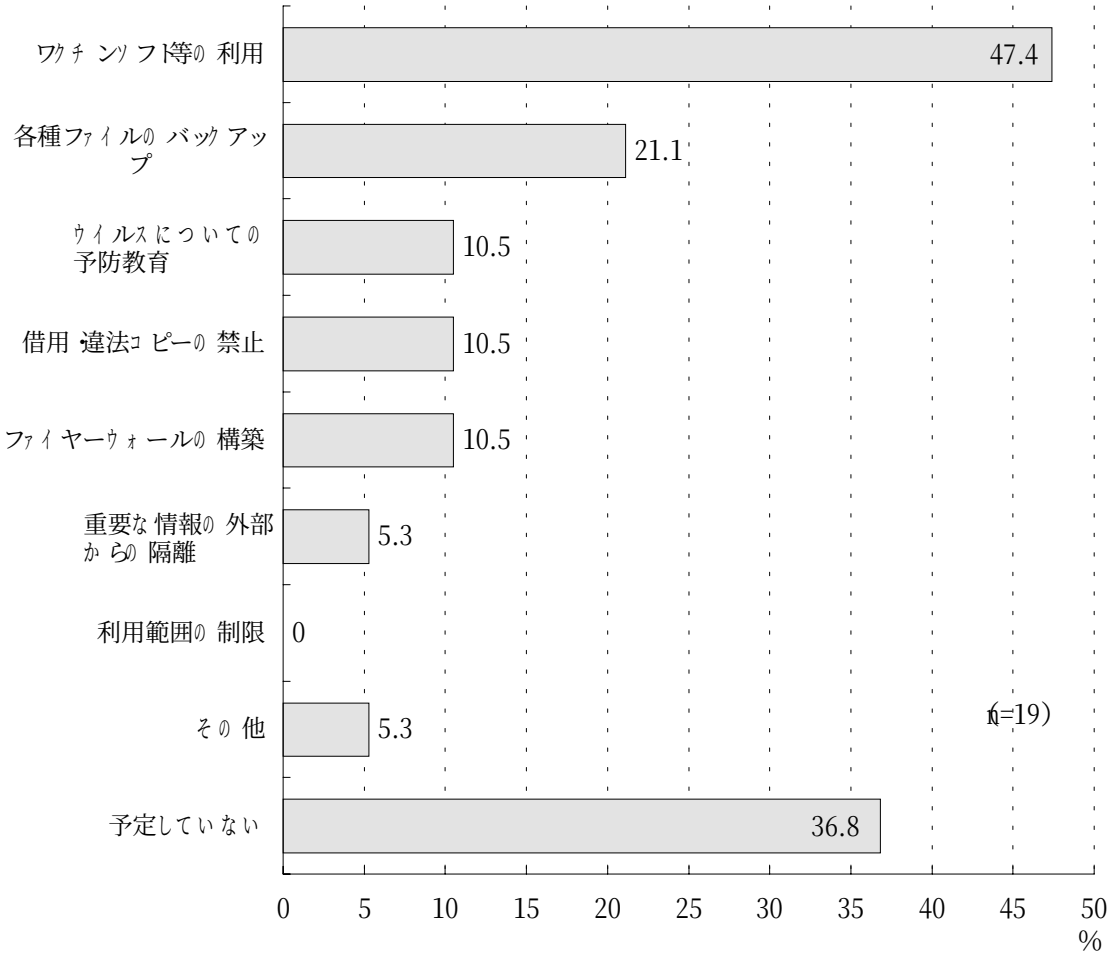
図表Ⅱ－７　　今後のセキュリティ対策の実施予定



（２）セキュリティ対策を行っていない事業所の今後の実施予定

現在、コンピュータウイルスに対するセキュリティ対策を行っていない事業所の今後の実施予定については、「ワクチンソフト等の利用」が最も多く 47.4%で、次いで「各種ファイルのバックアップ」が 21.1%となっている。また、「特に実施を予定していない」が 36.8%あり、現在実施していない事業所では、セキュリティ対策の必要性の認識が低いことを示している。

図表Ⅱ－８　　現在行っていない事業所の今後の実施予定



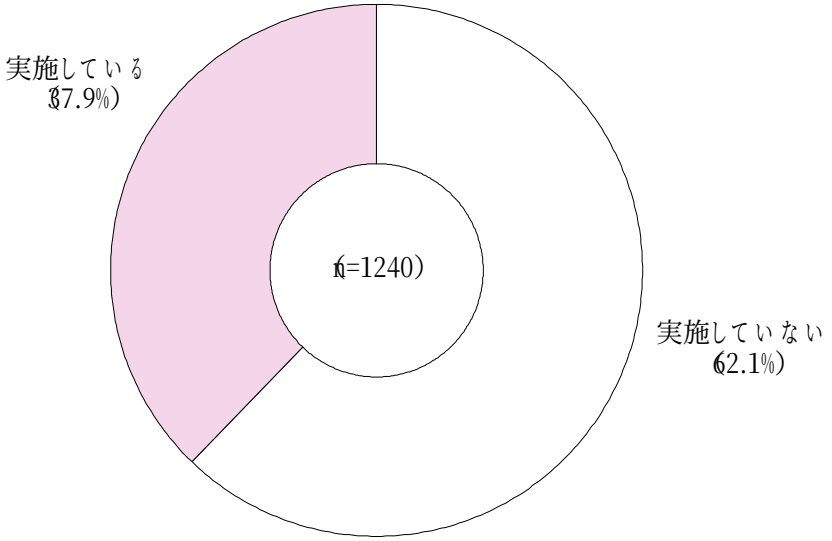
１・２・３　　ウイルス対策に関するユーザ教育

ウイルス対策に関するユーザ教育を「実施している」のは 37.9%で、「実施していない」は 62.1%であった。これは、前回新たに設けた質問項目であるが、前回の調査ではユーザ教育実施率は 23.1%であったから、大幅にアップしたといえる。

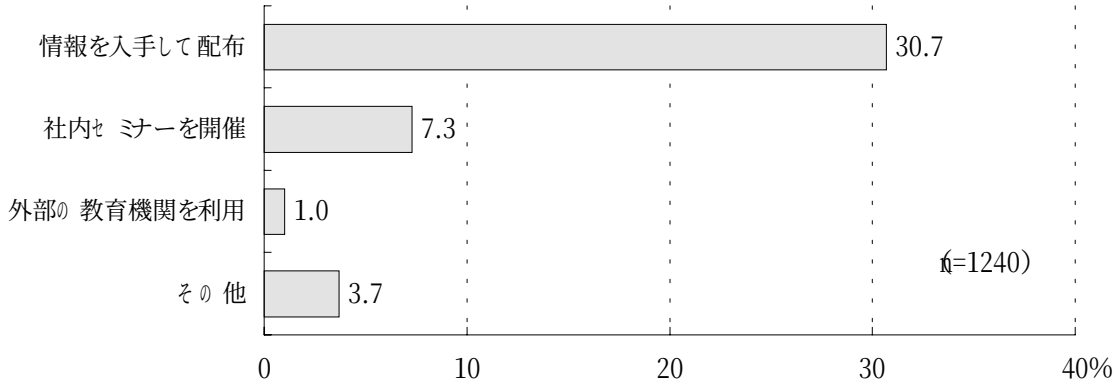
その内容については「情報を入手して配布している」が 30.7%、「社内セミナー等を開催」が 7.3%、「外部教育機関を利用している」が 1.0%となっている。

セミナーはほとんど不定期で、定期的に行っているところは極めて少ない。

図表Ⅱ－９　　ユーザ教育の実施状況



図表Ⅱ－10　ユーザ教育の内容



その他　：　社内通達・回覧、社内報、電子メール、電子掲示板、
ガイドライン・マニュアルの作成、ワクチンソフトの配布

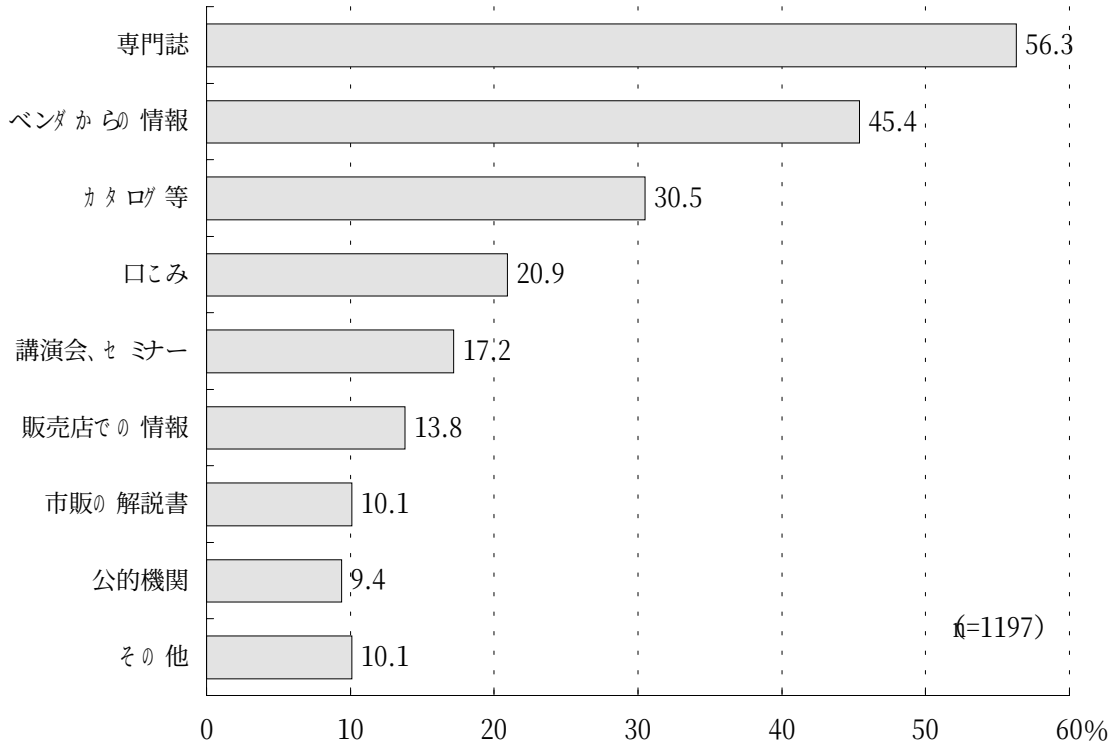
１・３　　ワクチンソフト

１・３・１　　情報源

ワクチンソフトに関する情報源としては、「専門誌」が最も多く 56.3%となっており、次いで「ソフトベンダーからの情報」が 45.4%、「カタログ等の広告」が 30.5%、「口こみ」が 20.9%となっている。前回の調査と比較すると、全般的に数字が高くなっている。ワクチンソフトに対する情報ニーズが高まっていることを示しているものと思われる。

「その他」の中では、パソコン通信およびインターネットが多い。

図表Ⅱ－11　ワクチンソフトの情報源

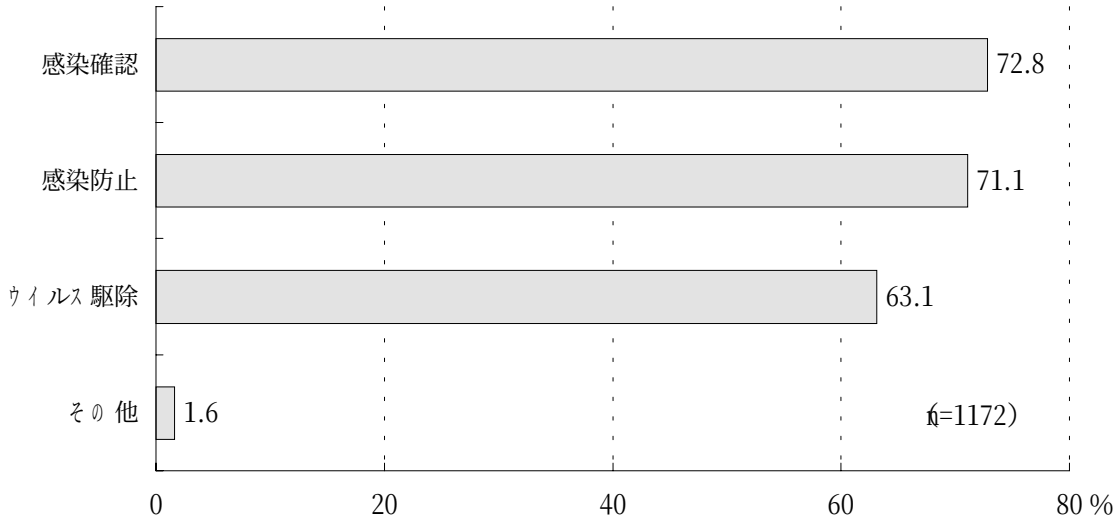


その他　：　パソコン通信、インターネット、展示会、社内情報、親会社、等

１・３・２　　導入目的

ワクチンソフトの導入目的としては、「感染の確認」が 72.8%を占めて最も多く、次いで「感染防止」が 71.1%、「駆除」が 63.1%となっている。前回調査に比べて、具体的な「感染防止」と「ウイルス駆除」のポイントが増えているのが目立っている。

図表Ⅱ－12　ワクチンソフトの導入目的



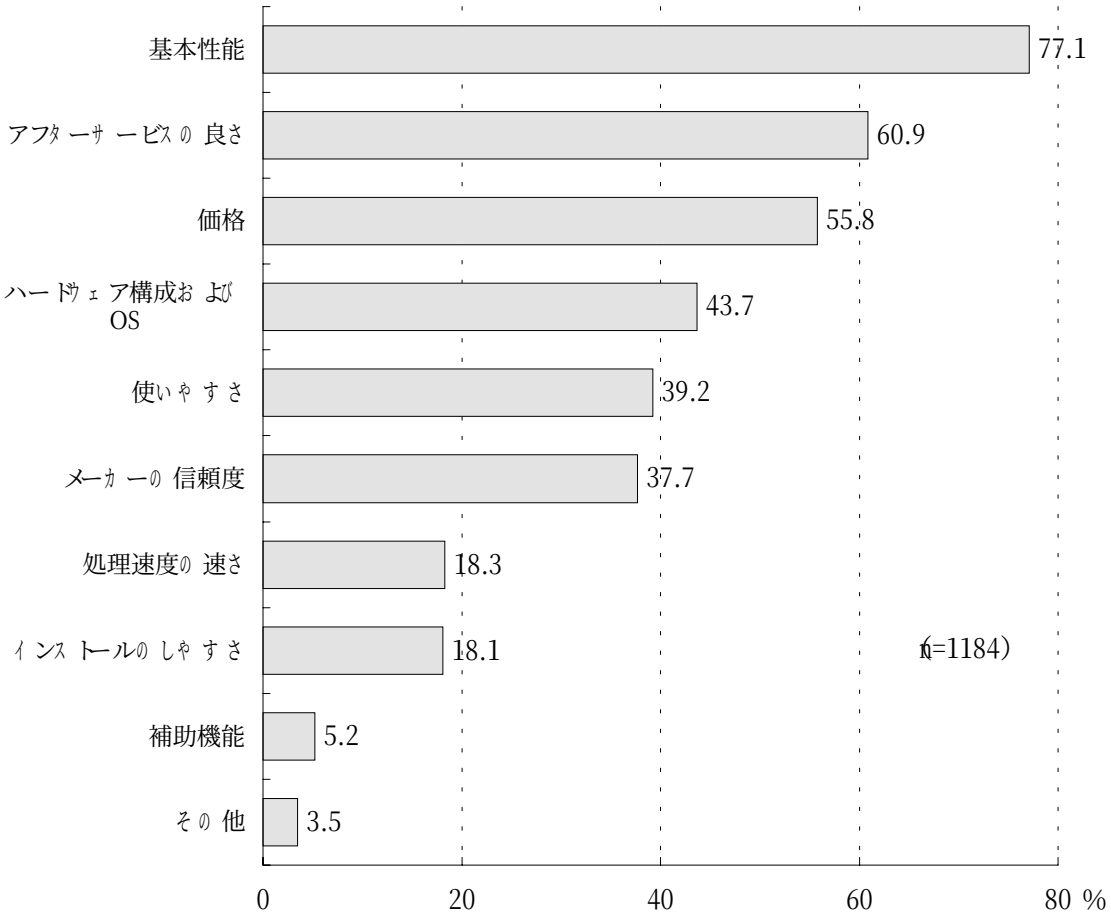
その他　：　社外へのウイルス流出防止、社内ユーザの対ウイルス意識の向上、
自社ソフトのチェック

１・３・３　　選択基準

ワクチンソフトの選択基準として重視しているものとしては、「基本機能」が77.1%で最も多く、次いで「アフターサービスの良さ」60.9%、「価格」が55.8%、「ハード構成・OS」43.7%となっている。

前回の調査と比較すると、「アフターサービスの良さ」が大幅に増えている。ワクチンソフトの導入がより進んだことを表しているものと思われる。

図表Ⅱ－13　ワクチンソフトの選択基準



その他　：　他のソフトやシステムへの影響、信頼性、世間の評価・実績
　　親会社（本社）の指定、等

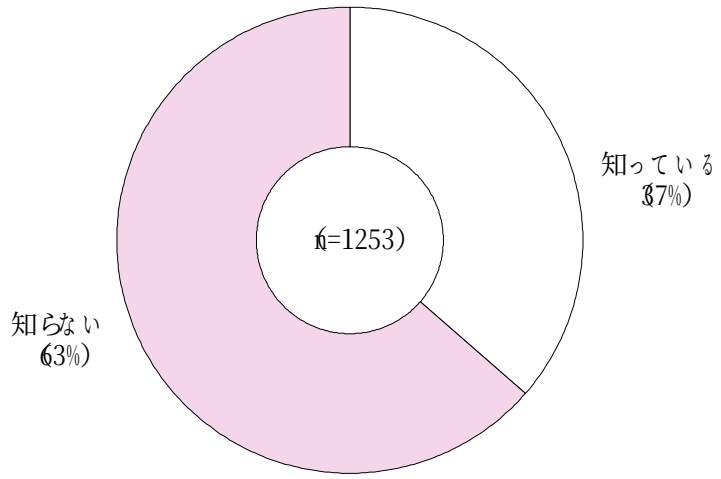
１・４　　コンピュータウイルス対策の課題

１・４・１　　コンピュータウイルス対策基準の認知度

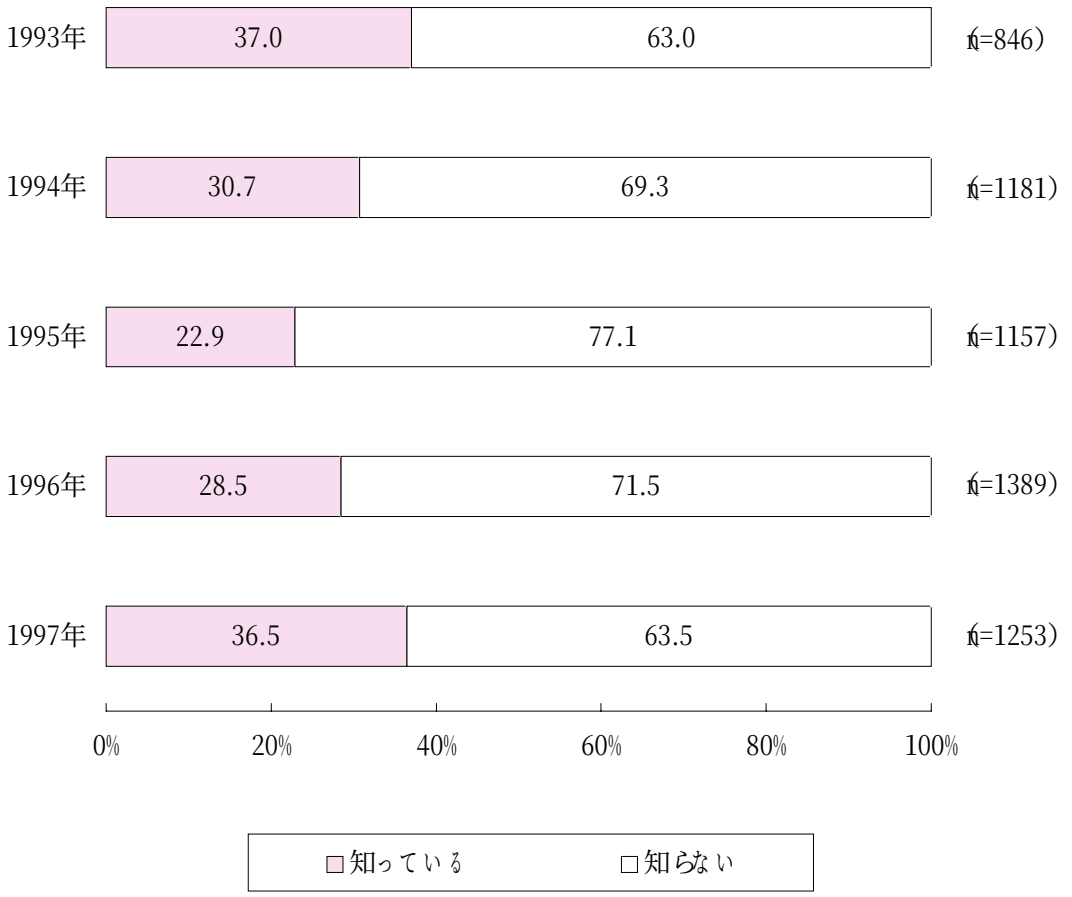
「コンピュータウイルス対策基準」の認知度については、「知っている」とする回答は36.5%で、「知らない」は63.5%であった。

認知度の推移をみると、ここ数年減少傾向にあったが、ほぼ過去の最高水準まで回復したといえる。しかしながら、対策基準の認知度は極めて低水準に止まっている。

図表Ⅱ－14　コンピュータウイルス対策基準の認知度



図表Ⅱ－15　コンピュータウイルス対策基準の認知度の推移

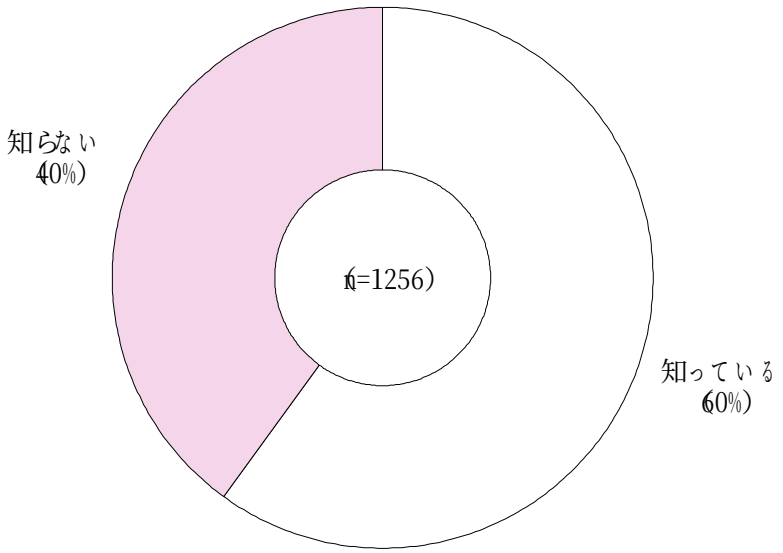


１・４・２　　被害届出について

（１）届出機関としての認知度

情報処理振興事業協会が通産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は、60.0%と前回の調査結果と比較してほぼ 10%上昇している。しかしながら依然、3 分の 1 以上が「知らない」と回答しており、さらに一層普及啓蒙活動を推進する必要がある。

図表Ⅱ－16　届出機関としての認知度

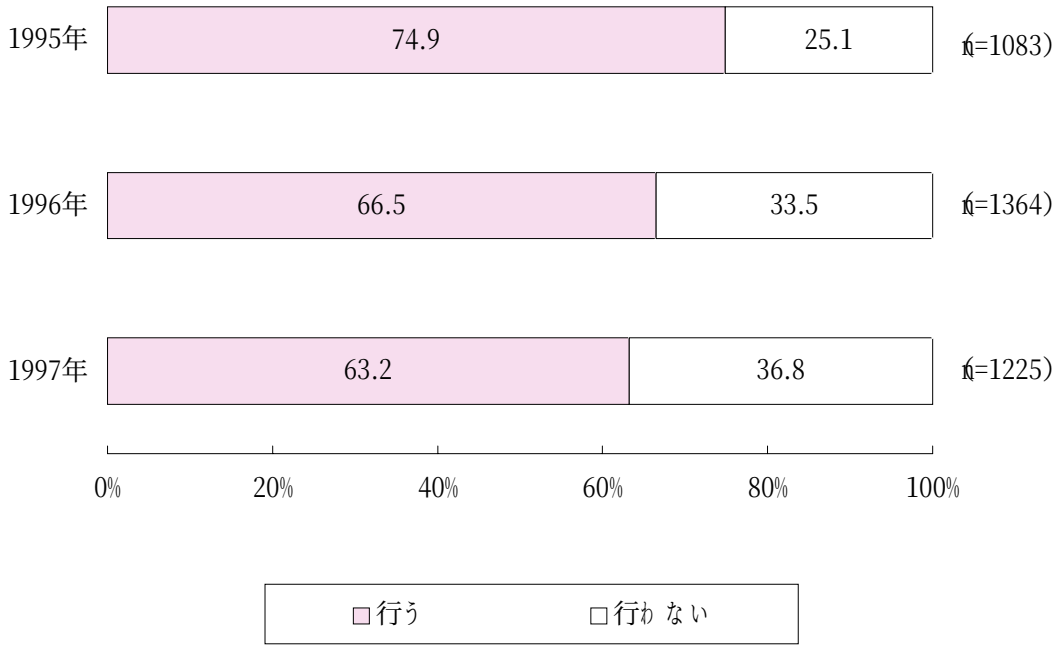


（２）届出の実施

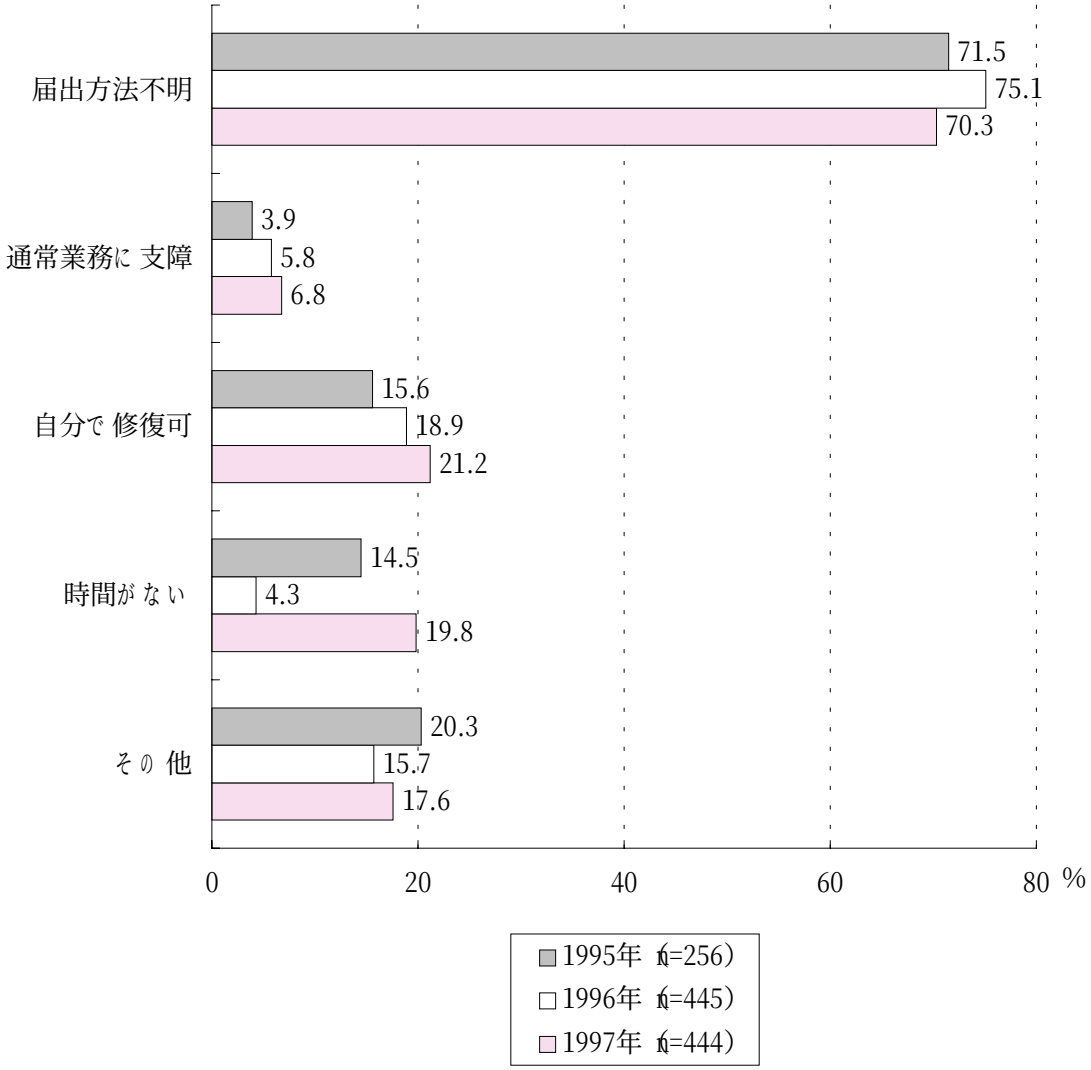
コンピュータウイルスの被害にあった際に、届出を行うかについては、「行う」とする回答が 63.2%、「行わない」が 36.8%となっている。推移をみると、「行わない」が年々増加している。

行わない理由としては、「届出方法が不明」が圧倒的に多く、70.3%であるが、その他の理由も全般的に増えている。コンピュータウイルス対策基準等の認知度を高めると同時に、さらに届出を推進するための方策が求められているといえる。

図表Ⅱ－17　今後の届出の実施



図表Ⅱ－18　届出を行わない理由



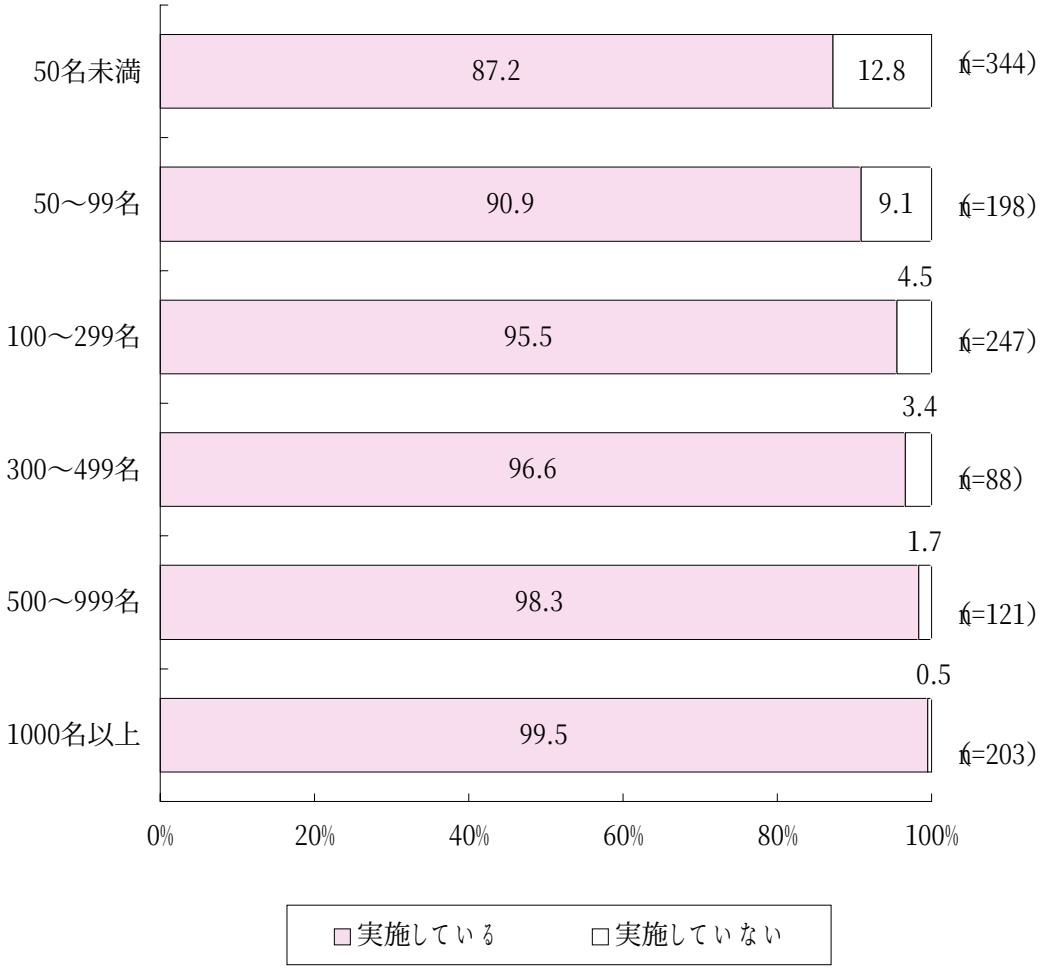
その他　：　届出をするメリットがない、届出の必要性が不明、修復が先決、本社（親会社）の指示に従う、等

１・４・３　　就業者数別セキュリティ対策実施状況

就業者数別にコンピュータウイルスに関するセキュリティ対策の実施状況をみると、就業者数が多いほど実施率が高くなる傾向にある。特に差異が大きいのは 100 名未満と以上の間で、「100 名未満」では「実施していない」事業所は 10%前後であるのに対して、100 名以上の企業はその半分以下となっており、特に「500～999 名」では、未実施はわずか 0.5%に止まっている。

前回の調査結果と比較すると、すべてのクラスの事業所でセキュリティ対策実施率は高くなっているが、さらに一層の普及活動が必要である。

図表Ⅱ－19　就業者数別セキュリティ対策実施状況



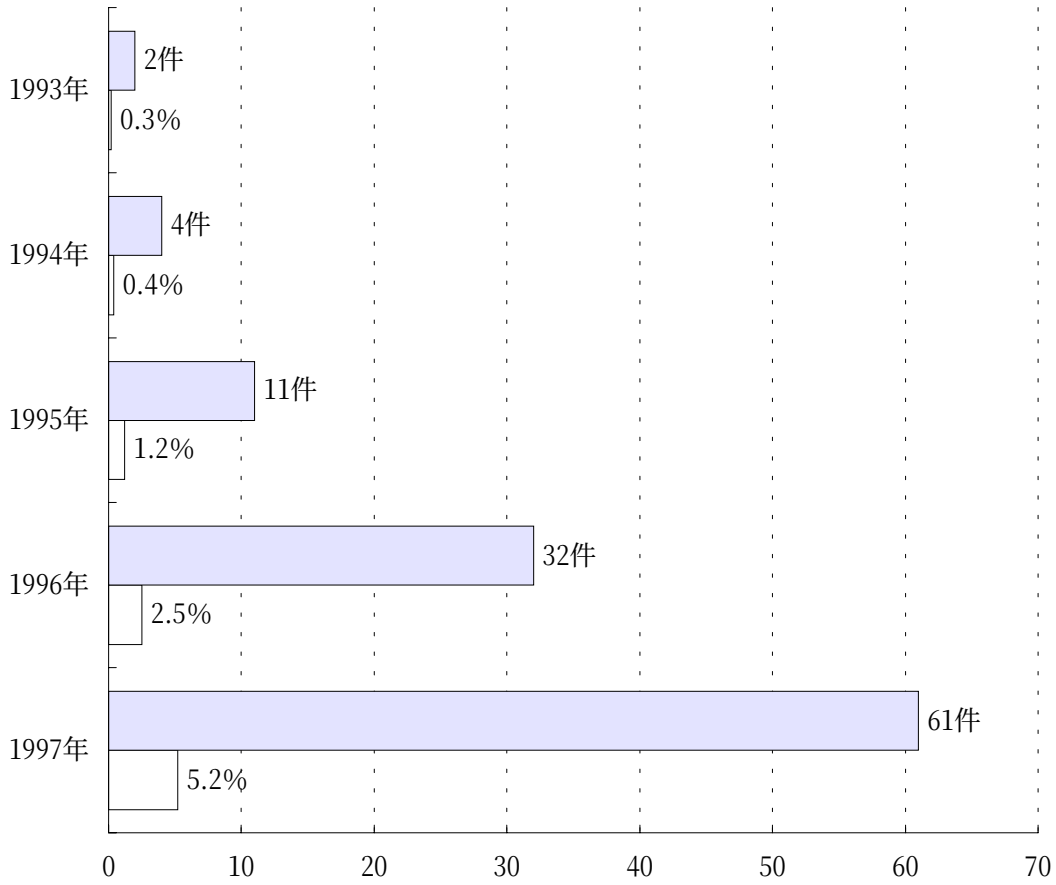
2　コンピュータへの不正アクセスによる被害及び対策の現状と課題

2・1　被害発生状況

（1）コンピュータ不正アクセス被害経験の推移

先に触れたように、コンピュータへの不正アクセスの被害件数は 61 件で、全体の 5.2%であった。コンピュータへの不正アクセスによる被害経験の推移をみると、ここ数年、前年比 3 倍近い伸びを示していたが、今年は昨年の約 2 倍であった。コンピュータの普及やネットワーク化の進展に伴って不正アクセスも確実に増えていることを示している。

図表Ⅱ－20　コンピュータ不正アクセス被害の推移



（２）業種別・就業者数別被害発生状況

業種別の不正アクセス被害発生状況をみると、「教育・研究機関」が 26 件で最も多く、次いで「情報サービス業」が 14 件、「製造業」が 5 件となっている。

就業者数別発生件数では、「1000 名以上」の大規模事業所が特に目立っている他は、ほぼ平均化している。

回答事業所数との割合でみると、「教育・研究機関」と「1000 名以上」で突出している。興味本位による不正アクセスが多いということであろうか。

図表Ⅱ－21　業種別被害発生状況

業　種	件数	%
教育・研究機関	26	23.0
情報サービス業	14	5.7
製造業	11	3.4
建設業	2	3.3
その他サービス業	2	2.5
政府または政府関係機関	2	11.1
不動産業	1	7.7
通信業	1	11.1
政治、経済、文化団体	1	4.2
地方公共団体	1	1.3

図表Ⅱ－22　就業者数別被害発生状況

就業者数	件数	%
50 名未満	12	3.3
50～99 名	6	2.8
100～299 名	8	3.2
300～499 名	9	9.9
500～999 名	4	3.3
1000 名以上	22	10.8

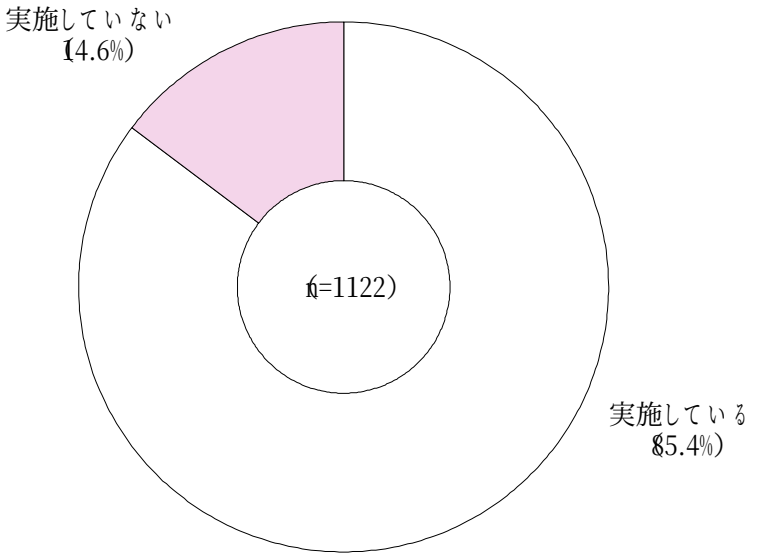
２・２　　セキュリティ対策実施状況

２・２・１　　現在実施しているセキュリティ対策

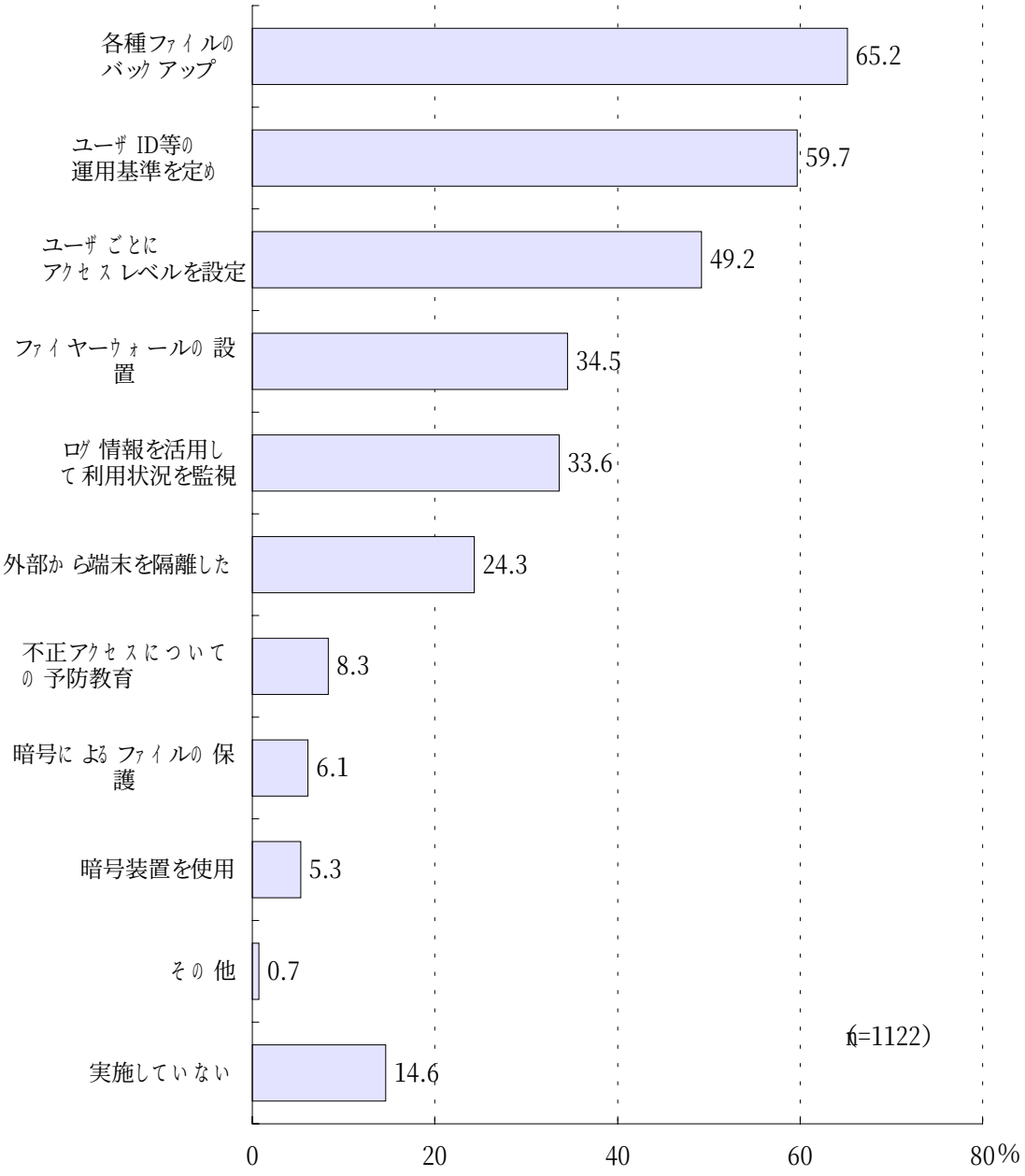
コンピュータへの不正アクセスに対処するためのセキュリティ対策については、85.4%の事業所が現在「実施している」としているが、これはコンピュータウイルスのセキュリティ対策よりも 10%程低い実施率である。

具体的な対策としては「各種ファイルのバックアップ」が最も多く 65.2%で、次いで「ユーザ ID 等運用規定を定めている」が 59.7%、「ユーザごとにアクセスレベルを設定」が 49.2%などとなっている。前回の調査と比較すると、「ファイヤーウォールの設置」および「ログ情報を活用した利用状況の監視」が共に 10%以上増加したのが目立っている。

図表Ⅱ－23　セキュリティ対策の実施状況



図表Ⅱ－24　現在実施しているセキュリティ対策

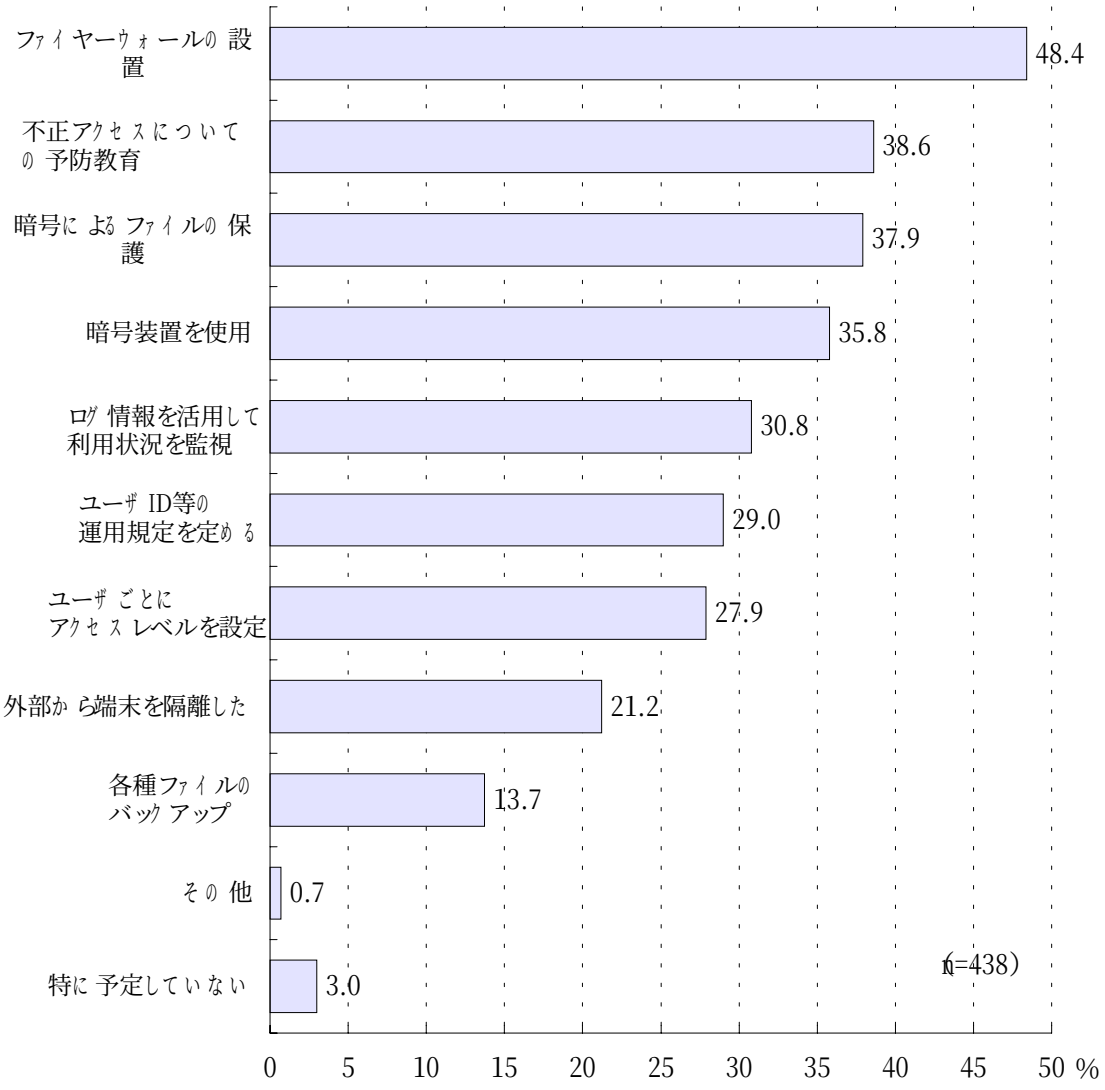


２・２・２　　今後実施予定のセキュリティ対策

（１）今後実施予定のセキュリティ対策

現在実施中のセキュリティ対策の継続も含む、今後実施予定の対策としては、「ファイヤーウォールの設置」が 48.4%で最も多く、次いで「不正アクセスについての予防教育」が 38.6%、「暗号によるファイルの保護」が 37.9%、「暗号装置等の使用」が 35.8%などとなっている。「ファイヤーウォールの設置」と「不正アクセスについての予防教育」が現在実施している対策と比較して大幅に増加している。

図表Ⅱ－25　今後のセキュリティ対策の実施予定

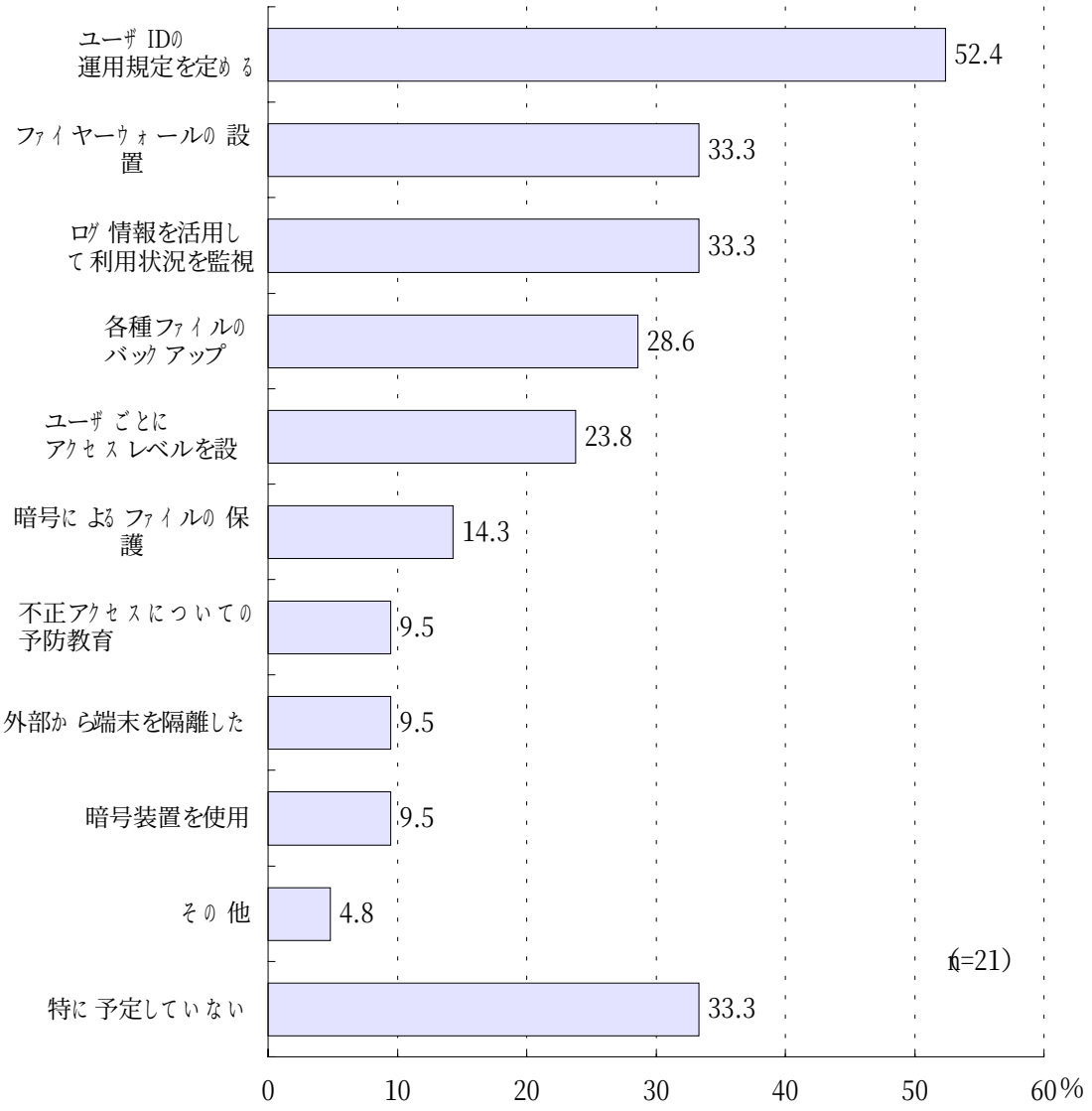


（２）セキュリティ対策を行っていない事業所の今後の実施予定

現在、不正アクセスに対するセキュリティ対策を行っていない事業所の今後の実施予定の対策については、「ユーザ ID 等運用規定を定めている」が最も多く 52.4%、次いで「ファイヤーウォールの設置」および「ログ情報を活用して利用状況の監視」が共に 33.3%、「各種ファイルのバックアップ」が 28.6%となっている。

「特に予定していない」も 33.3%と多く、コンピュータウイルスの場合と同様、現在セキュリティ対策を行っていない事業所では、セキュリティ対策の必要性の認識が低いことを示している。

図表Ⅱ－26　現在行っていない事業所の今後の実施予定

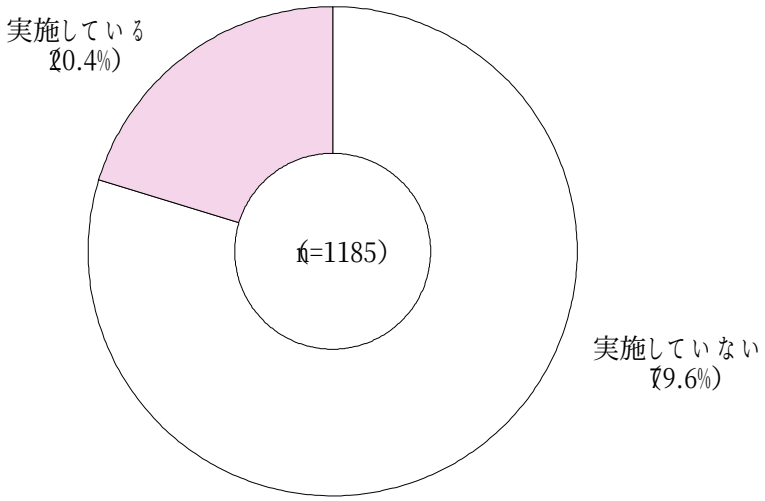


２・２・３　　不正アクセスに関するユーザ教育

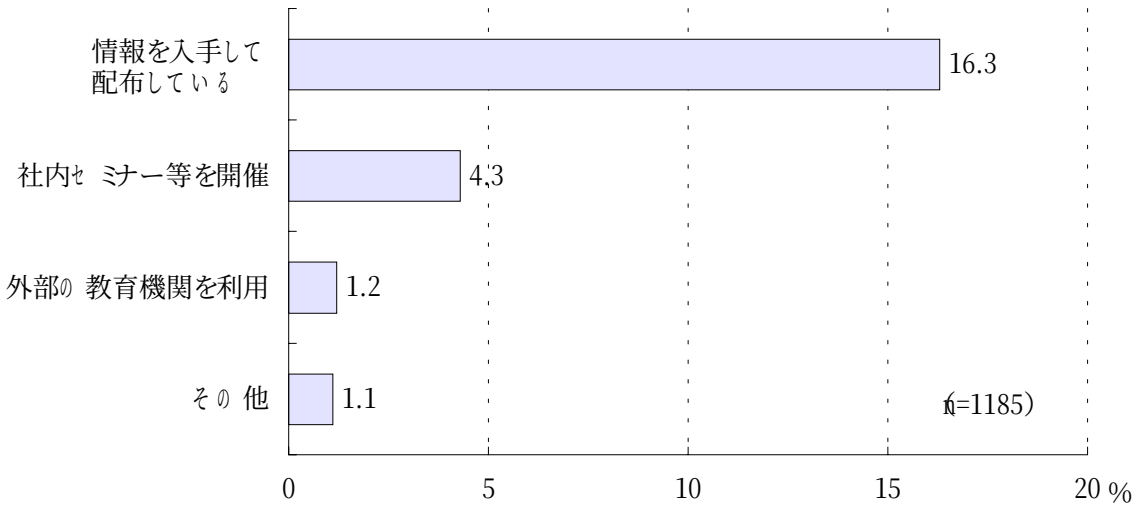
不正アクセスに関するユーザ教育を「実施している」企業はわずか 20.4%であり、「実施していない」企業は 79.6%であった。前回の調査に比べて 8%上昇しているが、ウイルス対策に関するユーザ教育の実施率の約半分に止まっている。

内容的には、「情報を入手して配布している」が 16.3%、「社内セミナー等を開催」が 4.3%、「外部の教育機関を利用」は 1.2%であった。

図表II−27　ユーザ教育の実施状況



図表II−28　ユーザ教育の内容



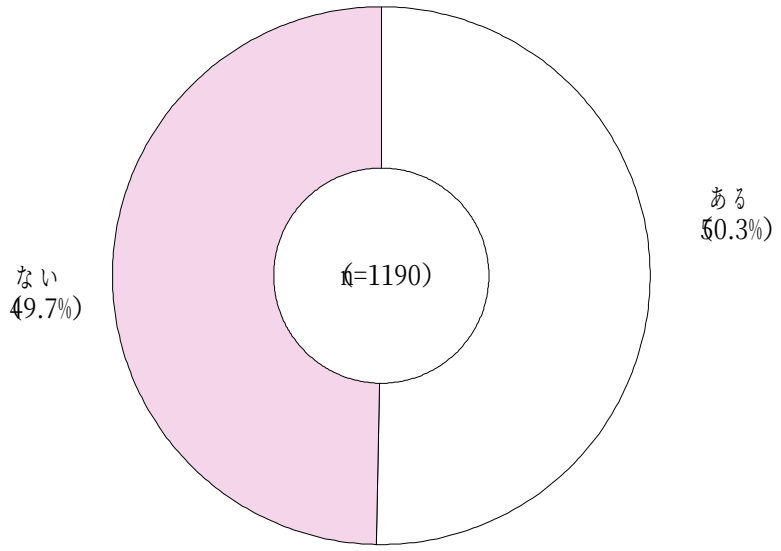
その他　：　社内通達、社内文書、相談窓口設置

２・３　　不正アクセスに関する情報源

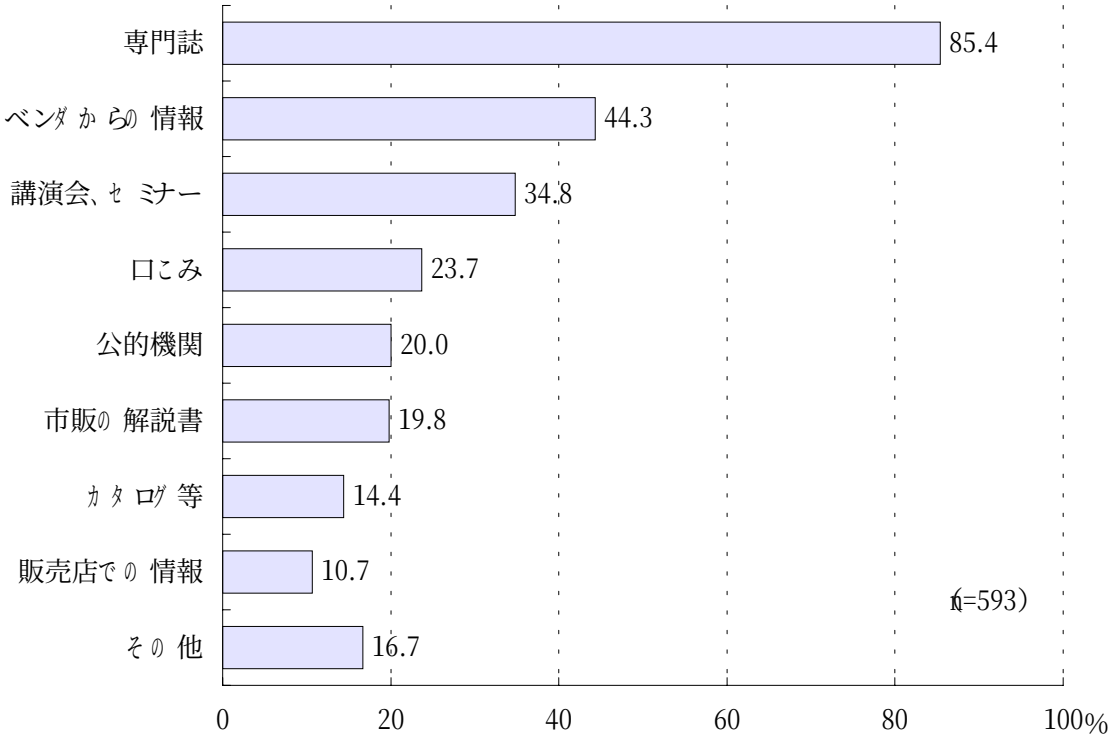
不正アクセスに対する情報源が「ある」と答えたのは 50.3%であった。約半数が情報源を持っていることになるが、ちなみに前回の調査では 36.8%であった。

不正アクセスに関する情報源としては、「専門誌」という回答が最も多く 85.4%、次いで「ソフトベンダーからの情報」が 44.3%、「講演会、セミナー」が 34.8%、「口こみ」が 23.8%などとなっている。前回の調査と比較すると、あらゆる項目で増加している。不正アクセスへの関心が高まっていることを示しているといえる。

図表Ⅱ－29　不正アクセスに関する情報源



図表Ⅱ－30　不正アクセスに関する情報源の種類



その他　：　インターネット、メール、パソコン通信、親会社、
JPCERT、等

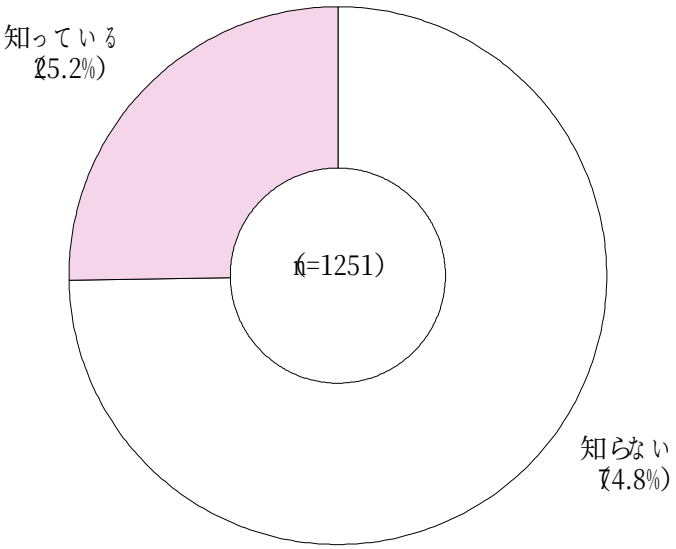
２・４　　コンピュータ不正アクセス対策の課題

２・４・１　　コンピュータ不正アクセス対策基準の認知度

「コンピュータ不正アクセス対策基準」は平成８年８月に作成されたため、今回２回目の調査であったが、「知っている」とする回答は25.2%で、「知らない」は74.8%であった。

認知度は徐々に高まっているが、まだ低水準に止まっている。今後より一層の普及活動が必要である。

図表Ⅱ－31　コンピュータ不正アクセス対策基準の認知度

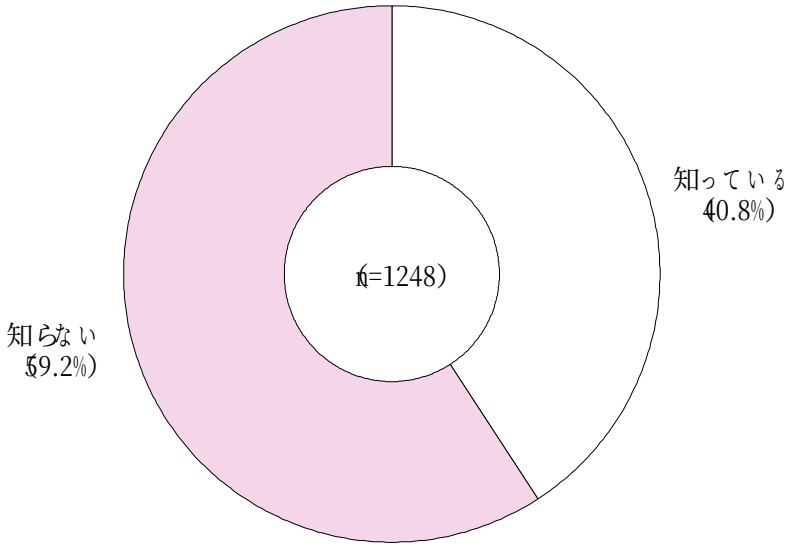


２・４・２　　被害届出について

（１）届出機関としての認知度

情報処理振興事業協会が平成 7 年から不正アクセスに関しても情報を受け付けていることについて、「知っている」という回答は 40.8%であった。前回の調査では 26.1%であったから認知度は確実に上昇しているといえるが、まだ 4 割に止まっている。「対策基準」同様、より一層の普及啓蒙活動が求められる。

図表Ⅱ－32　届出機関としての認知度

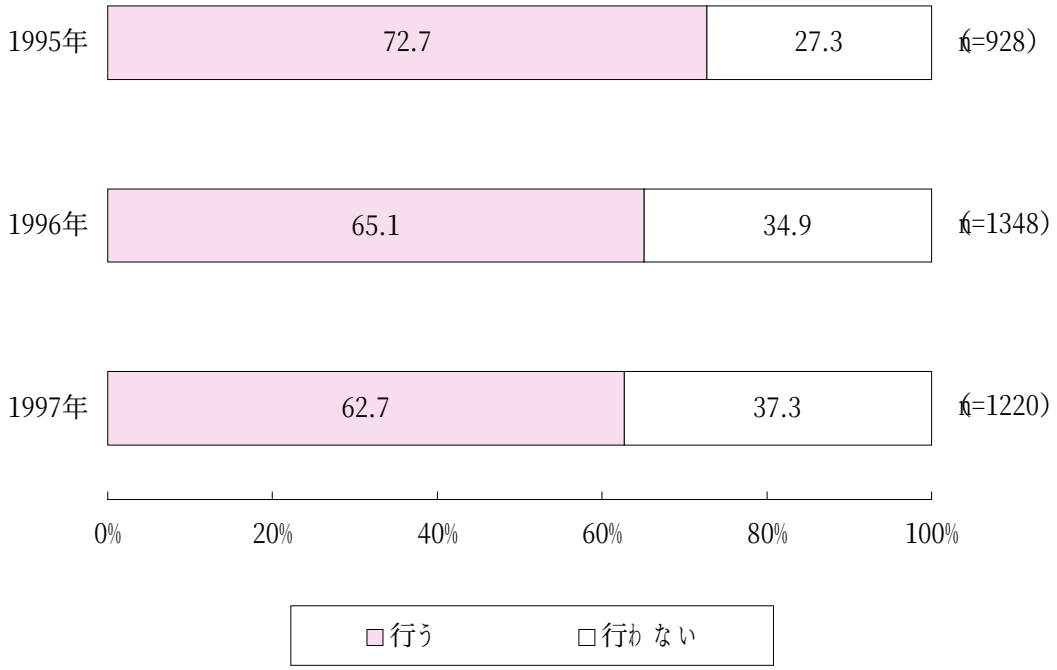


（２）届出の実施

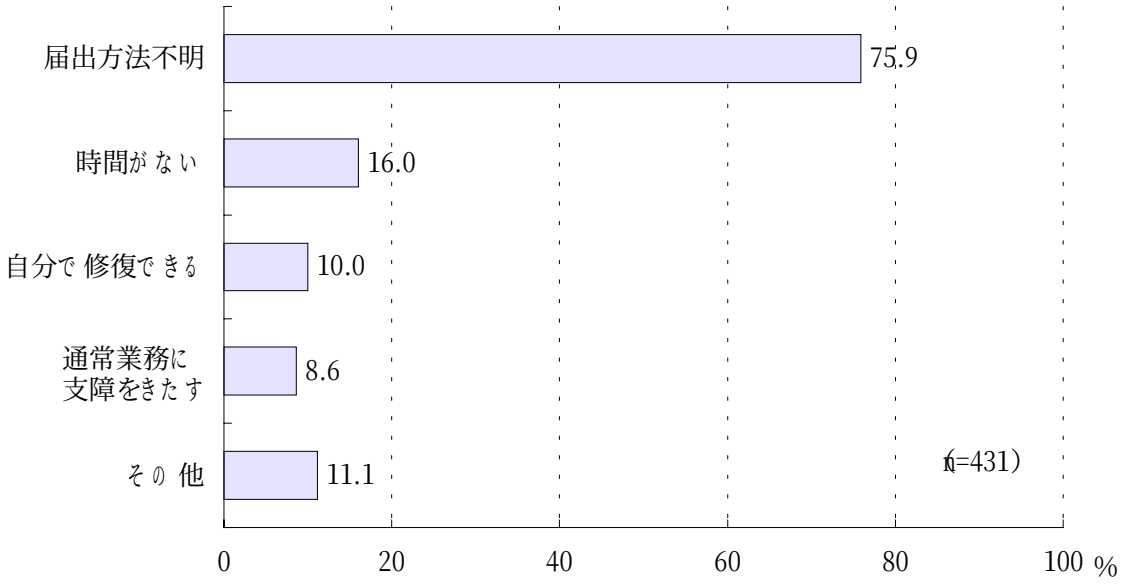
コンピュータの不正アクセスによる被害にあった際に、届出を行うかについては、「行う」とする回答が 62.7%、「行わない」が 37.3%となっている。推移をみると、コンピュータウイルス被害と同様、「行わない」が若干ながら年々増加している。

届出を行わない理由としては、「届出方法が不明」という回答が最も多く 75.9%に達している。次いで「時間がない」が 16.0%、「自分で修復できる」が 10.0%、「通常業務に支障をきたす」が 8.6%となっている。今後、より一層の認知度の向上とともに、届出率を高めるための努力が必要である。

図表Ⅱ－33　今後の届出の実施



図表Ⅱ－34　届出を行わない理由

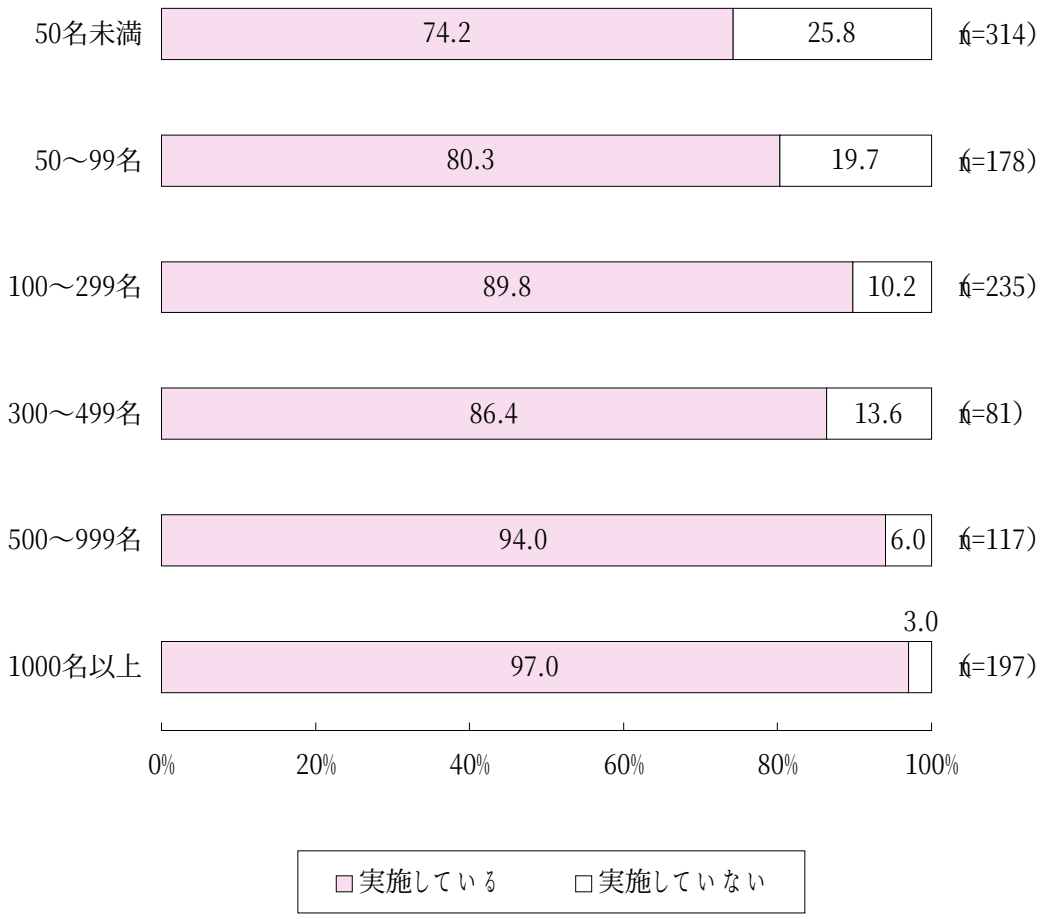


その他　：　届出の必要性が不明、メリットがない、
本社（関連会社）が一括管理している、社内規定による

２・４・３　　就業者数別セキュリティ対策実施状況

就業者数別にコンピュータへの不正アクセスに対するセキュリティ対策の実施状況をみると、ウイルスの場合と同様、就業者数が多くなるほど実施率が高くなる傾向にある。100名未満と以上およびの 500 名未満と以上の間に、セキュリティ対策実施率の大きなギャップがあるのが特徴的である。特に、小中規模事業所に対して、セキュリティ対策の重要性の認識を高める必要がある。

図表Ⅱ－35　就業者数別セキュリティ対策実施状況



Ⅲ　コンピュータウイルス等被害分析調査報告書

1　コンピュータウイルスによる被害分析

2　コンピュータへの不正アクセスによる被害分析

本報告書では、コンピュータウイルスおよび不正アクセス「個別票」にもとづいて、被害にあった事例ごとに調査分析を行っている。

１　コンピュータウイルスによる被害分析

１・１　感染したコンピュータの種類と台数

ウイルスに感染したコンピュータの種類と台数をみると、汎用機は「1 台」が比較的多く 36.0%あるが、他は「10 台」まで分散している。「50 台」という大規模被害も 1 件あった。

ワークステーションも被害台数はさまざまで分散しているが、ネットワーク接続利用が多いため総じて台数は多く、「50 台以上」が 46.0%と約半数を占めている。

パソコン等は「1～10 台」が最も多く 65.3%、次いで「11～50 台」が 19.0%、「51～100 台」が 6.1%となっている。前回調査と比較してみると、「10 台以下」が 20.%以上も減少し、50 台以上の大規模被害が昨年の 1.5%から 15.8%に大幅に増加しているのが目立っている。

図表Ⅲ－１　感染したコンピュータの種類と台数　汎用機･ ワークステーション

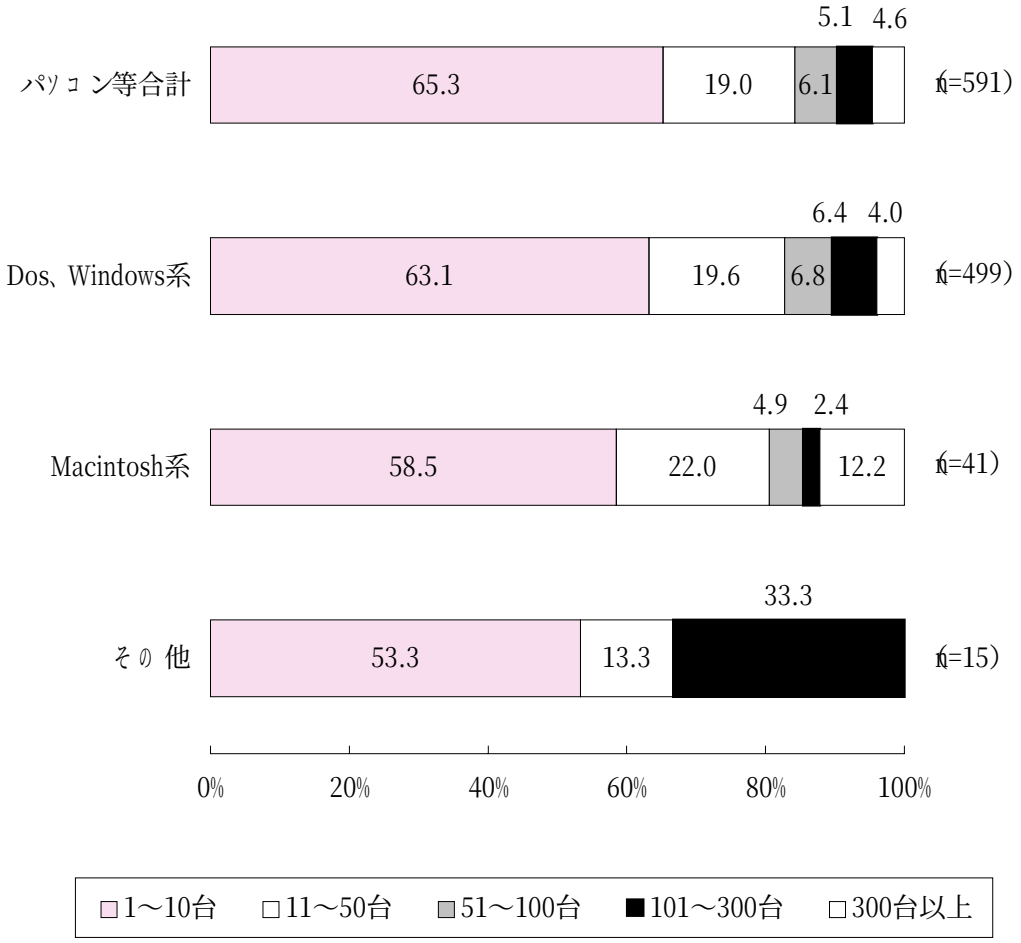
〈汎用機〉

	件数	%
1台	9	36.0
2台	3	12.0
3台	4	16.0
4台	2	8.0
5台	2	8.0
10台	4	16.0
50台	1	4.0
合　計	25	100.0

〈WS〉

	件数	%
1台	3	11.5
2台	1	3.8
10台	7	26.9
18台	1	3.8
23台	1	3.8
30台	1	3.8
50台	2	7.7
60台	1	3.8
80台	2	7.7
100台	2	7.7
130台	1	3.8
170台	1	3.8
200台	1	3.8
400台	2	7.7
合　計	26	99.6

図表Ⅲ－２　感染したコンピュータの種類と台数　パソコン等

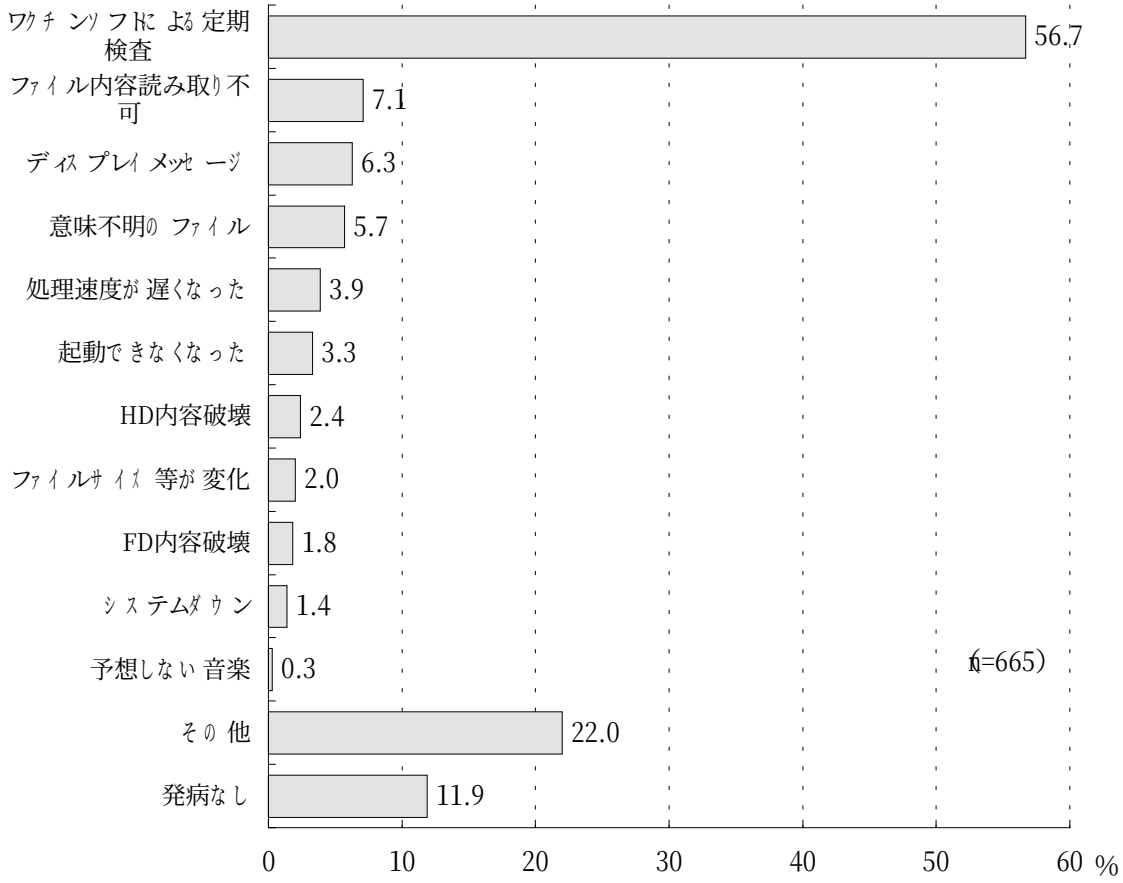


１・２　　発見の経緯

ウイルス発見の経緯としては、「ワクチンソフトによる定期検査」が圧倒的に多く 56.7%、次いで「ファイルの記録内容が読み取れなくなった」が 7.1%となっている。また、「発病なし」も 11.9%あった。

その他の中の「ワクチンソフトのインストール時」や「常駐ワクチンによる読み込み時」等を加えると、ワクチンソフトによる発見は 7 割前後に及ぶものと思われる。ワクチンソフトの普及がかなり行き渡っているといえる。

図表Ⅲ－３　　発見の経緯

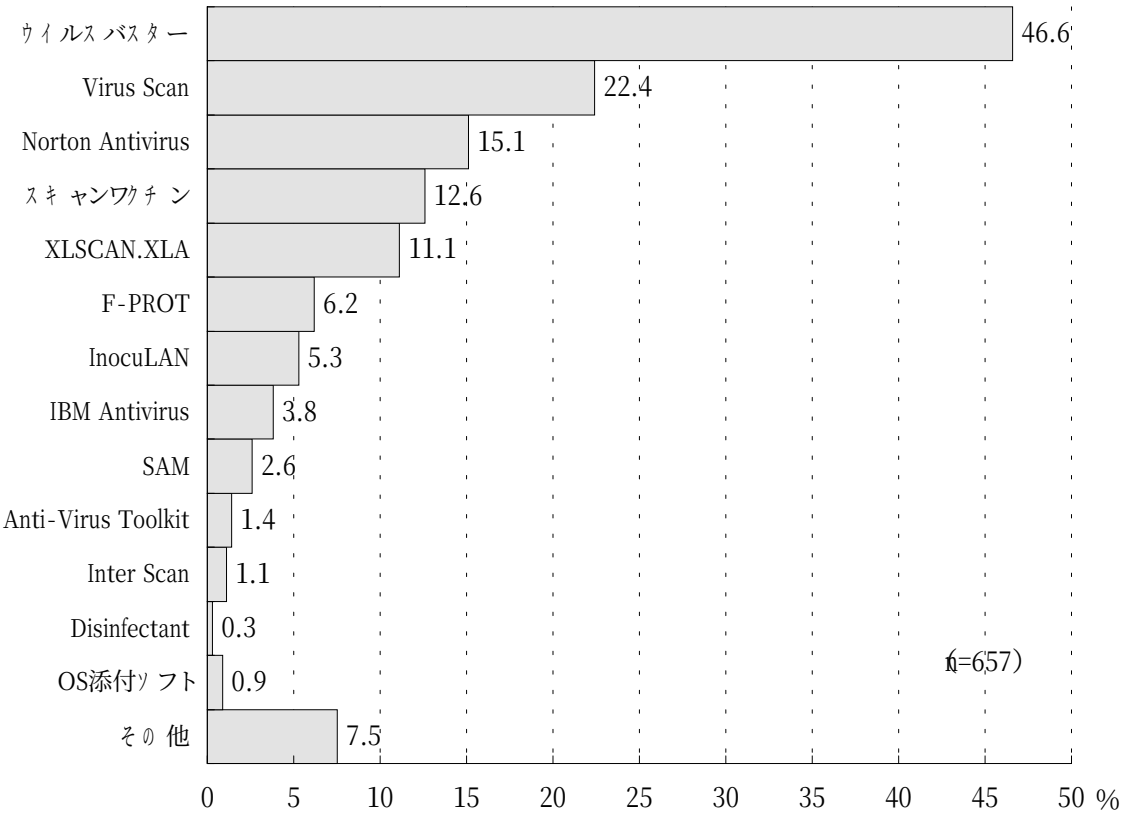


その他　：　ワクチンソフトのインストール時、
ワクチンソフトによる読み込み時（臨時検査）、
表示画面異常、アプリケーションの動作異常、ファイル保存不可、
外部（取引先、他部署）からの連絡、等

１・３　　発見に使用したワクチンソフト

感染したウイルスを発見するのに使用したワクチンソフトとして最も多くあげられているのは、「ウイルスバスター」で 46.6%と約半数の事業所が使用している。次いで「Virus Scan」が 22.4％、「Norton Antivirus」が 15.1％、「スキャンワクチン」12.6％、「XLSCAN.XLA」11.1%などとなっている。

図表Ⅲ－４　使用したワクチンソフト



OS 添付ソフト　：　SWEEP、MS-DOS

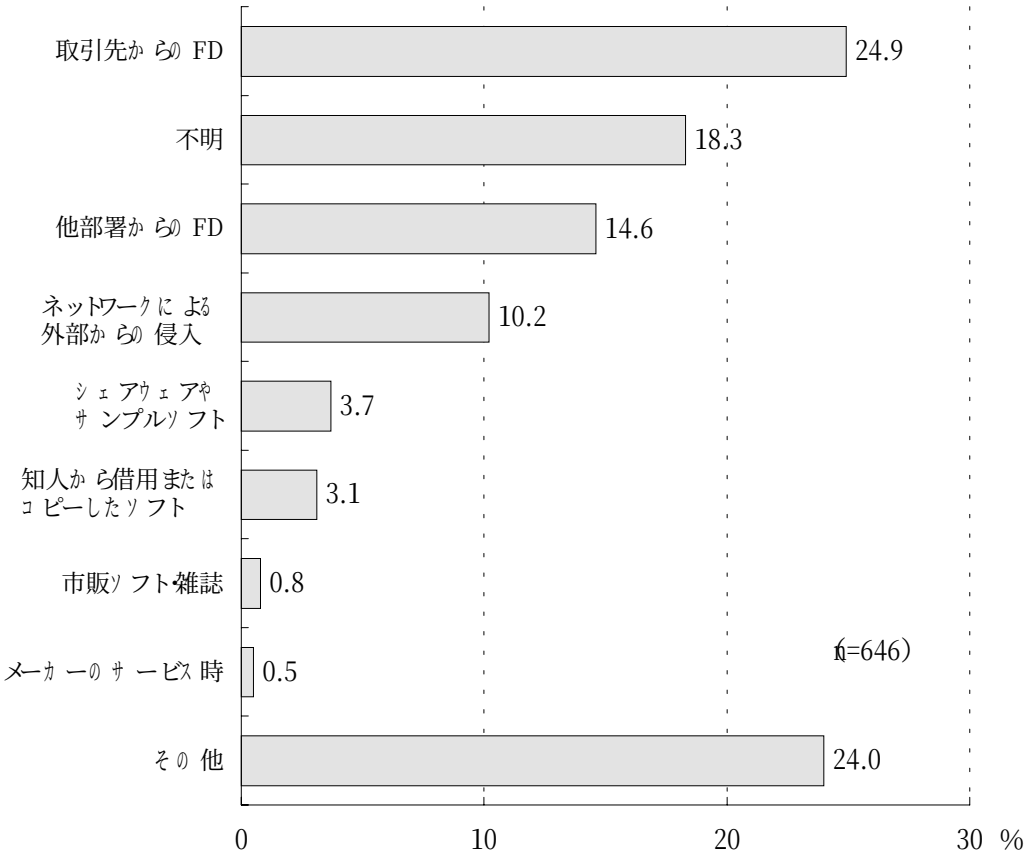
その他　：　スキャンメール、Vurus Safe、Dr.Solomon、Server Protect、等

１・４　　感染経路

ウイルスの感染経路として最も多いのが「取引先からの FD」で 24.9%、続いて「他部署からの FD」が 14.6%、「ネットワークによる外部からの侵入」10.2%となっており、FD を経由した感染が多いことがわかる。前回の調査との比較では、「ネットワークによる外部からの侵入」が大幅に増え、「不明」が逆に大幅に減ったのが特徴的である。

「その他」の中では、「メール添付ファイルによる」というのが圧倒的に多い。

図表Ⅲ－５　　感染経路

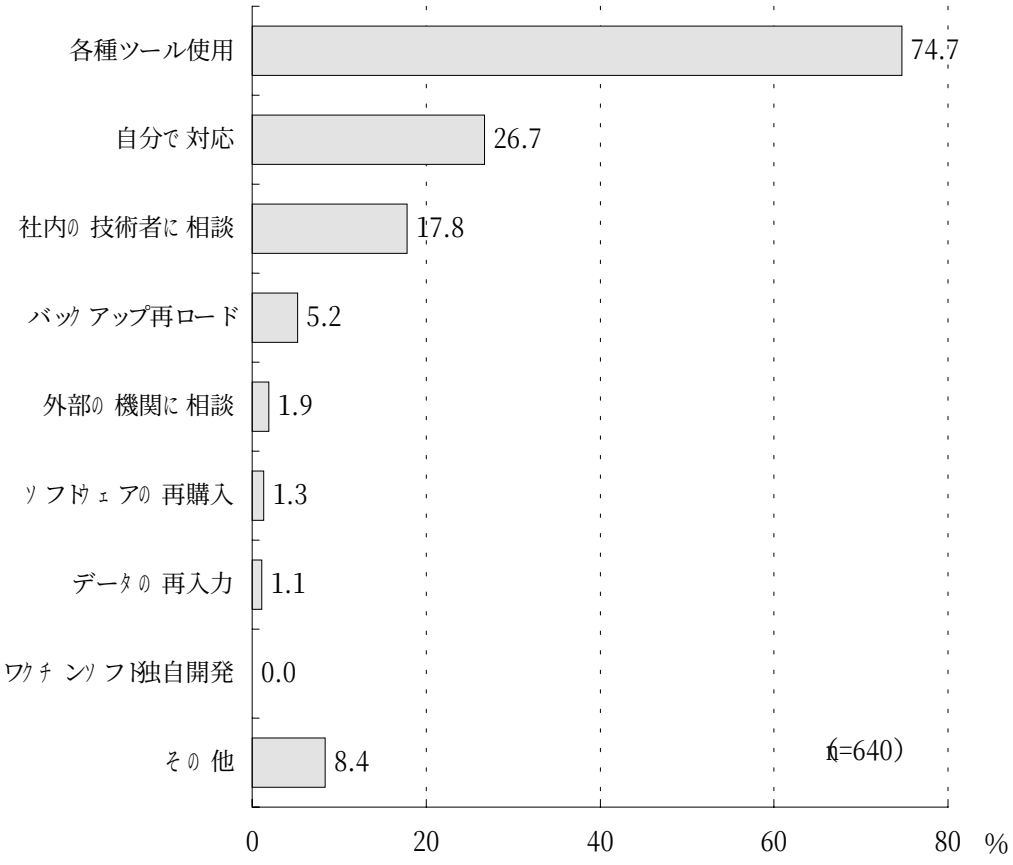


その他　：　電子メールの添付ファイル、取引先からのメール、
他部署からのメール、海外からの電子メール・ファイル、
CD-ROM、MO、等

１・５　　復旧方法

ウイルスに感染した際の復旧方法としては、「各種ツールを使用」が 74.7%と圧倒的に多くを占めている。次いで「自分で対応した」が 26.7%、「社内の技術者に相談」が 17.8%などとなっている。

図表Ⅲ－６　　復旧方法



その他　：　サーバ側のウイルス対策ソフトで自動的に駆除､データファイルの破棄、感染ファイルの削除、再インストール、再フォーマット・交換、等

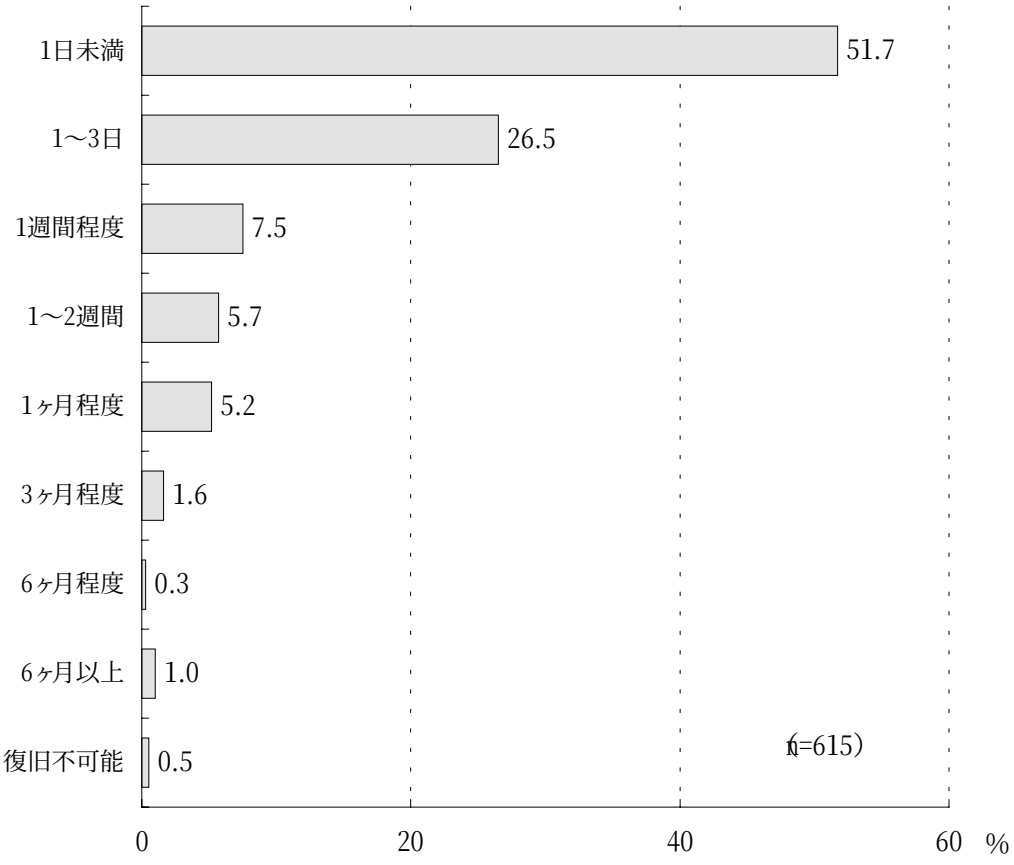
相談した外部の機関　：　ワクチンソフトメーカー、ディーラー、コンピュータメーカー、ソフトハウス

１・６　　被害規模

１・６・　１　　復旧に要した期間

ウイルス被害にあった時の復旧に要した期間としては、「1 日未満」が最も多く 51.7%、次いで「1 ～3 日」が 26.5%と比較的短い日数で復旧できているが、「1 カ月以上」という大規模被害も 8.1%あった。なお、「復旧不可能」が 0.5%あった。

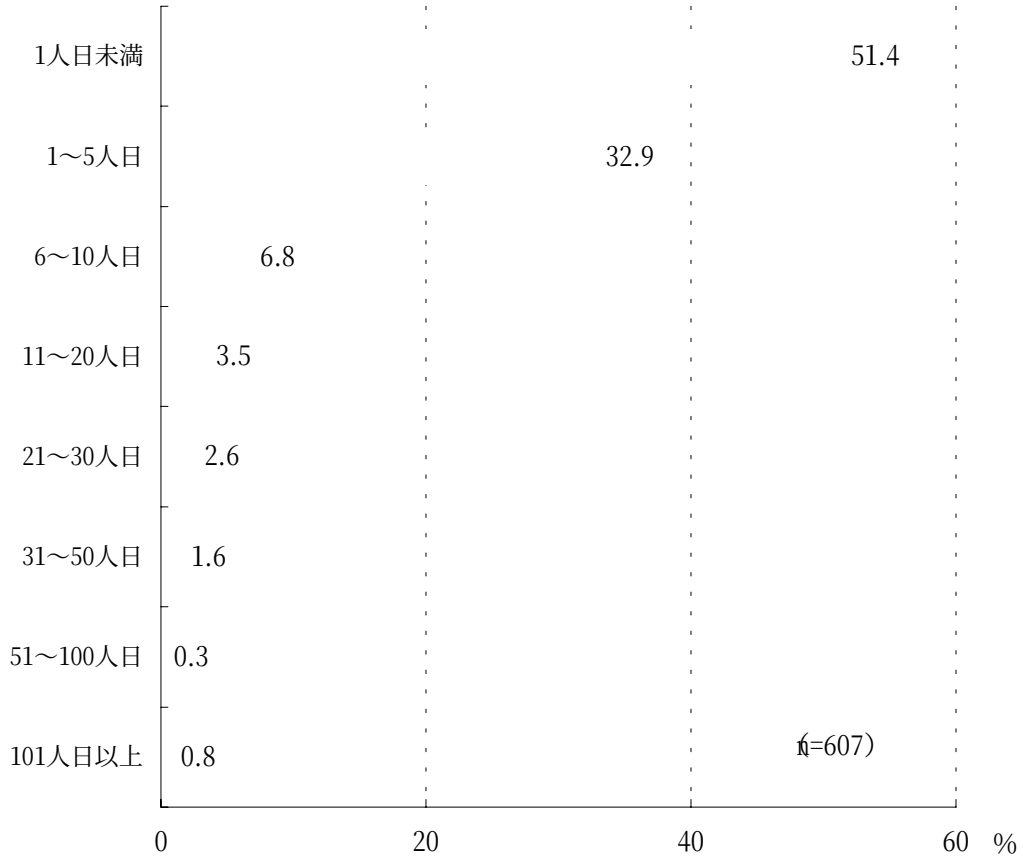
図表III－７　　復旧に要した期間



１・６・２　　復旧に要した人日

復旧に要した人日についても短いものが多く、「1人日未満」が51.4%、「1〜5人日」 が32.9%となっている。前回の調査では1.7%に過ぎなかった「11人日以上」という大きな被害が、今回は8.8%あった。ネットワーク化の進展とマクロウイルスの増加により、被害も大規模化していることをうかがわせる。

図表Ⅲ－８　　復旧に要した人日



2　コンピュータへの不正アクセスの被害分析

2・1　被害を受けたコンピュータの機種とネットワーク　OS

不正アクセスによる被害を受けたコンピュータの機種およびネットワーク OS は下表の通りである。機種は、ワークステーションが圧倒的に多い。ネットワーク OS は、「Sun OS」、「UNIX」、「Soralis」などが多い。WindowsNT は比較的少なかった。

図表Ⅲ－９　被害を受けたコンピュータの種類とネットワーク　OS

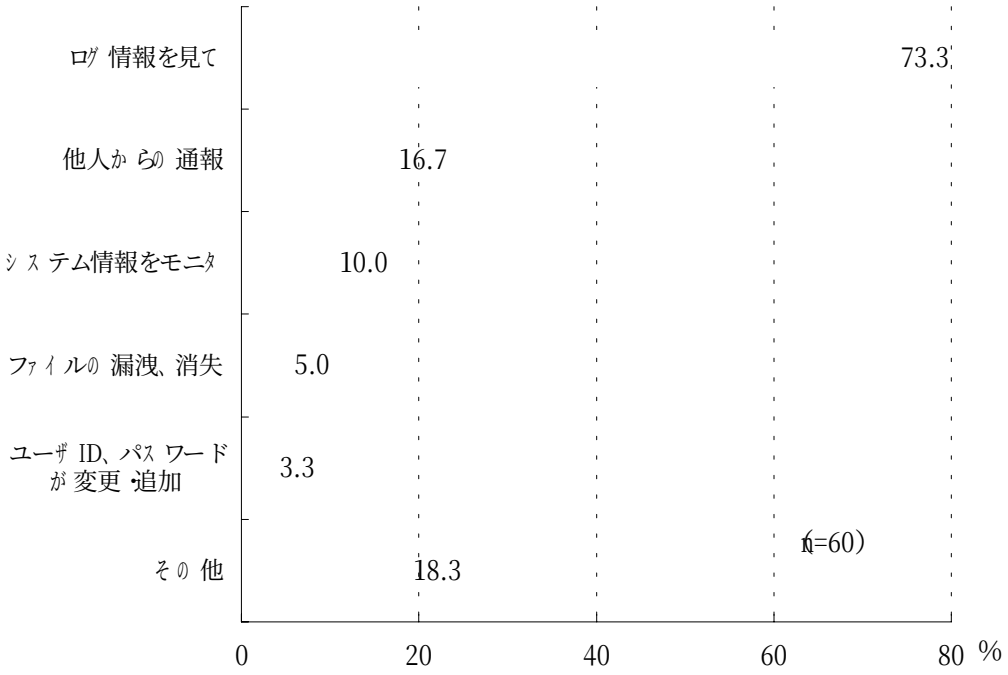
	機　種	OS
1	富士通S4/20	SUN(UNIX)
2	IBM PC-750	WindowsNT
3	PC	UNIX
4	Sun4/SS20	UNIX
5	Sun SS2	SUN OS4.1.1
6	富士通NN2X	TCP/IP
7	PC/AT互換	NT Server4.0
8	PC98V10	Windows95
9	UNIX	Soralis
10	DOS/V	Windows95
11	Sun SS5	UNIX
12	Sun SPARC	Sun OS
13	WS	Sun OS5.5.1
14	自作ｻｰﾊﾞ	WindowsNT
15	Sun	Sun OS
16	HP	HP-UX
17	PC	LINUX
18	Sun SS ELC	SUN OS4.1.4
19	Sun	Soralis
20	Sun	SUN OS4.1.3
21	EWS4800	UNIX
22	EWS4800	UNIX
23	Sun SPARC20	Sun OS
24	IBM Think Pad	Windows95
25	WS	Soralis
26	Sun	UNIX

	機　種	OS
27	UNIX	UNIX
28	UNIX	UNIX
29	Sun	UNIX
30	WS	Digital-UNIX
31	Sun	UNIX
32	Sun SS5	Soralis2.5
33	FMV	LINUX
34	Polywell	Soralis2.5X86
35	Sun	UNIX
36	Sun	UNIX
37	WS	Sun OS5
38	WS	Sun OS5
39	富士通S4/10	Sun OS4.1.4
40	WS	TCP/IP
41	Sun	Soralis1.1.2
42	Sun	Soralis1.1.2
43	富士通S4/20	Soralis1.1.2
44	Sun SS20	Soralis2.3
45	PC/AT互換	Soralis2.5.1
46	Sun	Sun OS4.1
47	Sun SPARC20	Sun OS4.1.4
48	Sun SPARC20	Sun OS4.1.4
49	Sun SPARC20	Sun OS4.1.4
50	Sun SPARC20	Sun OS4.1.4
51	SPARC Server1000	Soralis2.4
52	Gateway2000 P5-133	Net BSD 1.2G

２・２　　発見の経緯

コンピュータへの不正アクセス発見の経緯としては、「ログ情報を見て」が 73.3%で最も多く、次いで「他人からの通報」が 16.7%、「システム情報をモニターした時」が 10.0%となっている。

図表Ⅲ－10　発見の経緯



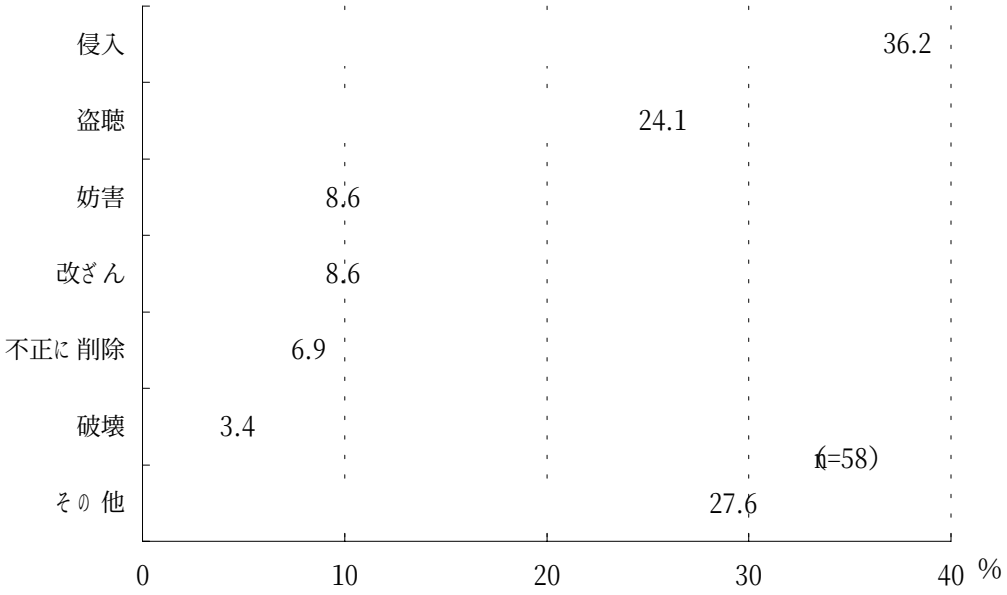
その他　：　JPCERT からのメール、加入しているプロバイダからの警告、
チェックプログラムの自動通知

２・３　　被害状況

２・３・１　　被害の内容

不正アクセスによる被害の内容については、「侵入」が最も多く 36.2%、次いで「盗聴」が 24.1%、「妨害」および「改ざん」が各 8.6%で続いている。実害なしとする回答が 4 分の 1 近くあった。

図表Ⅲ－11　被害の内容

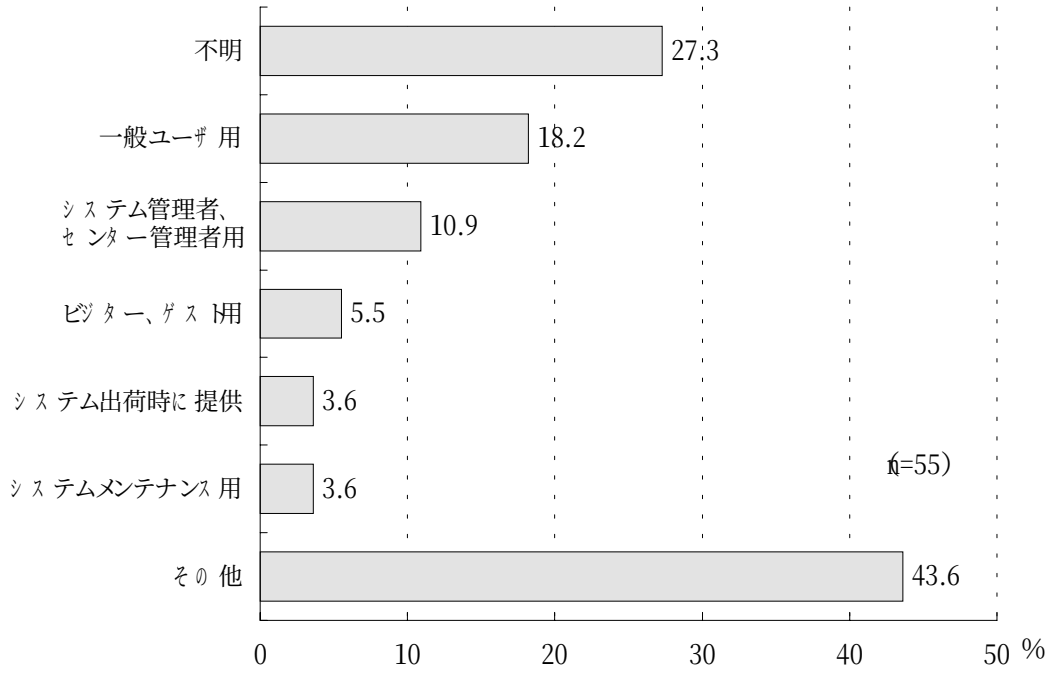


その他　：　メールの中継爆撃、パスワードファイルのコピー

２・３・２　　不正利用された利用者 ID について

不正アクセスに使用された利用者 ID については、「不明」が最も多く 27.3%、次いで「一般ユーザ用」が 18.2%、「システム管理者もしくはセンター管理者用」が 10.9%などとなっている。

図表III－12　不正利用された利用者 ID



その他　：　WWW サーバへのアクセス、
netnews のセキュリティホールをついて入ろうとした、
INN のコントロールメッセージ

２・３・３　　利用者 ID とパスワードが不正利用された理由

利用者 ID およびパスワードが不正に利用された理由としては、「不明」が 44.4%で最も多かった。「パスワードがなかった」という回答が 3 件であったが、「その他」の中に安易なパスワード、ID を指摘するものが数件あった。

図表Ⅲ－13　利用者 ID とパスワードが不正利用された理由

	件　数	%
パスワードがなかった	3	8.3
不　明	16	44.4
その他	17	47.2

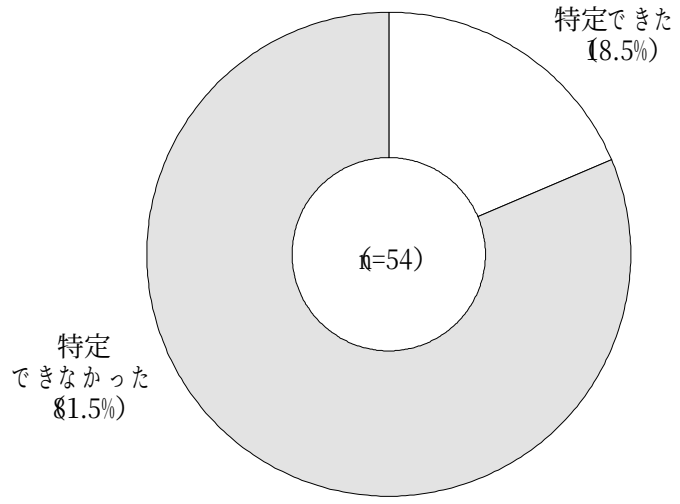
（n=36）

その他　：　INN のセキュリティホール、予想できるものだった、
Crack／Tapping、サーバのバグ

２・４　　不正アクセスした人の特定

不正アクセスした人が「特定できた」という回答は 18.5%であった。「特定できなかった」は 81.5%と非常に多かったが、実害はほとんどなかったので追求しなかったという回答もかなりあった。

図表Ⅲ－14　不正アクセスした人の特定



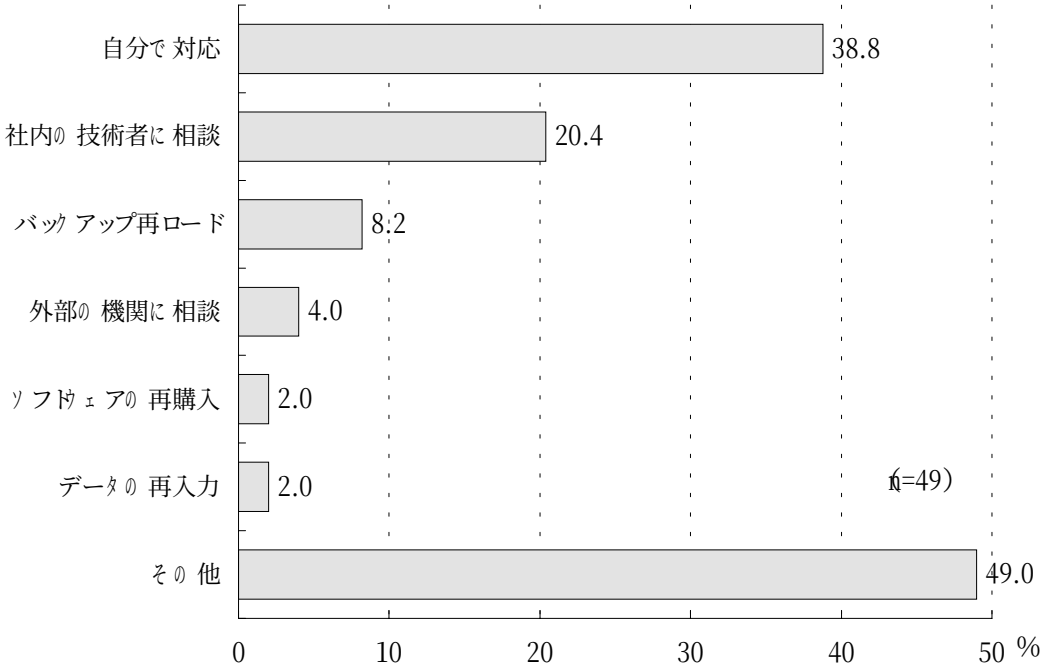
特定できた理由　：　メールアドレスが書かれていた、
プロバイダで特定してもらった

特定できなかった理由　：　詳細なアクセスログは手元にはない、個人までは無理、
不特定多数のアクセスあり

２・５　　復旧方法

不正アクセスの被害にあった時の復旧方法としては、「自分で対応した」が最も多く38.8%、次いで「社内の技術者に相談した」が20.4%、「バックアップしていたファイルを再ロードした」8.2%などとなっている。「その他」の中に「被害なし、必要なし」とする回答が２割程度あった。

図表Ⅲ－15　復旧方法



その他　：　INNのバージョンアップ、パスワードの変更、OSの再インストール

相談した外部の機関　：　ディーラー

２・６　　被害規模

復旧に要した期間は「1 日未満」が最も多く 45.9%、次いで「1～3 日」が 32.4%であった。

復旧に要した人日は「1 人日未満」、「1～5 人日」が共に 43.2%で、この２つで約 9 割を占めている。

復旧に要した期間・人日共、比較的軽微で済んでいるものが多かったが、復旧に要した期間が 1 ヶ月以上に及ぶ大規模被害が 10.8%あった。。

図表Ⅲ－16　復旧に要した期間・人日

〈期　間〉

	件数	%
1日未満	17	45.9
1～3日	12	32.4
1週間程度	3	8.1
1～2週間	1	2.7
1ヶ月程度	3	8.1
3ヶ月程度	0	0.0
6ヶ月程度	0	0.0
6ヶ月以上	1	2.7
復旧不可能	0	0.0
合　計	37	100.0

〈投入人日〉

	件数	%
1人日未満	16	43.2
1～5人日	16	43.2
6～10人日	3	8.1
11～20人日	1	2.7
21～30人日	1	2.7
31～50人日	0	0.0
51～100人日	0	0.0
101人日以上	0	0.0
合　計	37	100.0

Ⅳ　コンピュータウイルス感染等防止策報告書

1　コンピュータウイルス感染防止策

2　コンピュータへの不正アクセス被害防止策

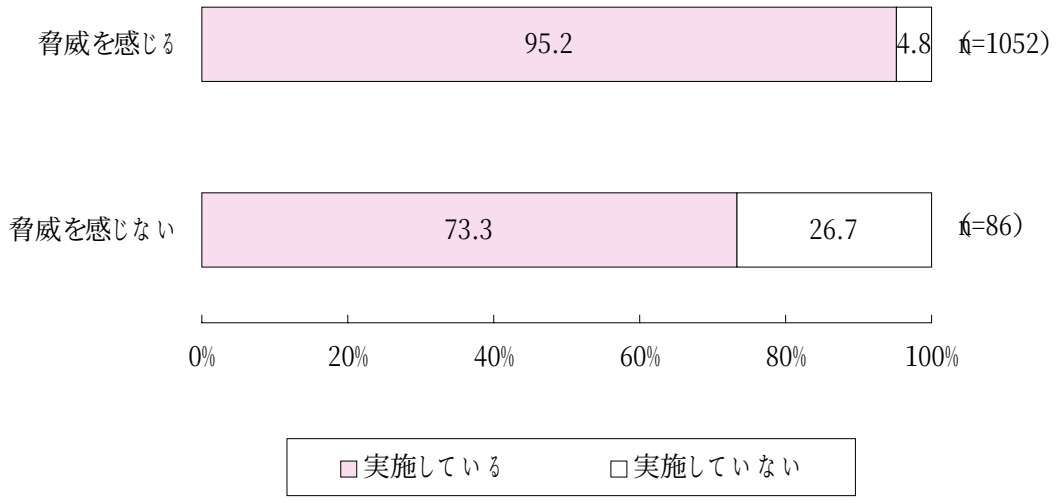
１　コンピュータウイルス感染防止策

１・１　コンピュータウイルスに対する脅威とセキュリティ対策の実施状況

コンピュータウイルスに対する脅威の認識度とセキュリティ対策の実施状況をみると、脅威を「感じる」とする事業所の 95.2%が何らかのセキュリティ対策を実施しているのに対して、脅威を「感じない」とする事業所では、73.3%と約 20%以上も低い実施率となっている。

前回の調査の、「感じない」事業所の実施率は 71.3%であったから、ほぼ頭打ちになったとみることができる。コンピュータウイルスの脅威およびセキュリティ対策の重要性に対する啓蒙活動の新たな展開が求められている。

図表Ⅳ－１　コンピュータウイルスに対する脅威とセキュリティ対策の実施状況

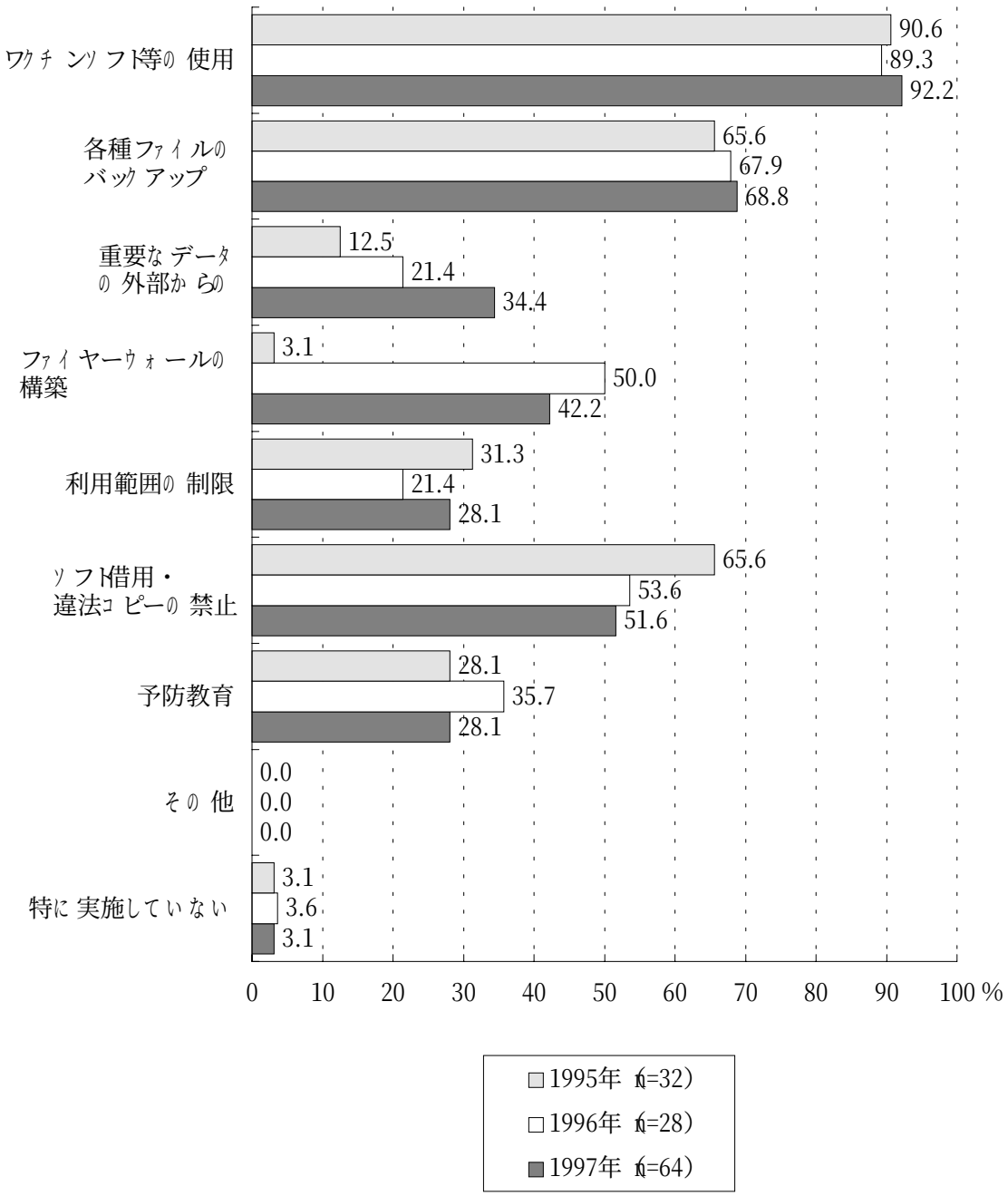


１・２　　コンピュータウイルス感染防止策

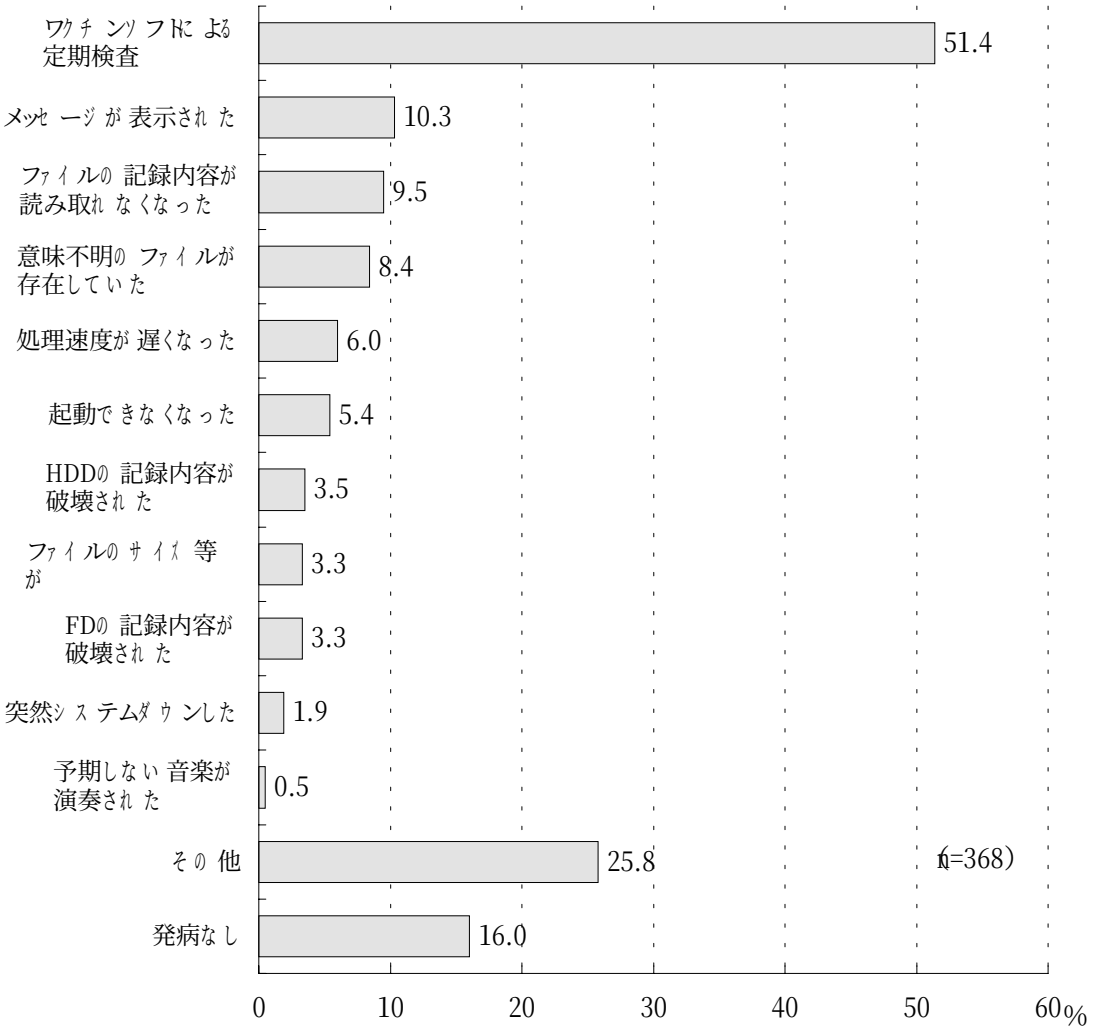
コンピュータウイルス発見の経緯で「発病なし」と回答している事業所について、現在実施しているセキュリティ対策をみると、「ワクチンソフト等の利用」が 92.2%を占めており、ワクチンソフトの導入が、ウイルスに感染した際に被害を受けないために有効であることがわかる。その他、主なセキュリティ対策としては、「各種ファイルのバックアップ」68.8%、「ソフトの借用・違法コピーの禁止」51.6%、「ファイヤーウォールの構築」42.2%などがあげられる。従来の調査結果と比較すると、「重要データの外部からの隔離」が大幅に増加したのが目立っている。

「ワクチンソフト等の利用」を実施している事業所のコンピュータウイルス発見の経緯をみると、「ワクチンソフトの定期検査」が 50%以上を占めており、ワクチンソフトの有効性がうかがえる。しかし、「ワクチンソフト等を利用」していても、「コンピュータウイルスと思われるメッセージが表示された」10.3%、「ファイルの記録内容が読み取れなくなった」9.5%、「意味不明のファイルが存在していた」8.4%などのさまざまな被害を受けている。被害を最小限に抑えるためには、ワクチンソフトの使用だけに止まらず、ネットワーク管理者だけでなくユーザも含めた総合的なセキュリティ対策が必要である。

図表Ⅳ－２　　発見の経緯「発病なし」の現在実施しているセキュリティ対策



図表Ⅳ－３　「ワクチンソフト等の利用」実施事業所の
コンピュータウイルス発見の経緯



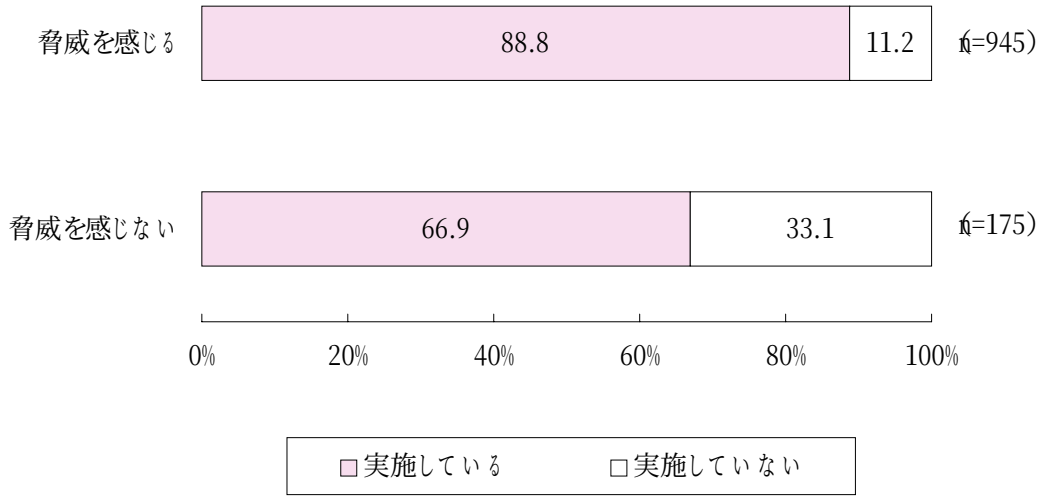
2　コンピュータへの不正アクセス被害防止策

2・1　コンピュータへの不正アクセスに対する脅威とセキュリティ対策の実施状況

コンピュータへの不正アクセスに対する脅威の認識度とセキュリティ対策の実施状況をみると、脅威を「感じる」とする事業所では 88.8%が何らかのセキュリティ対策を実施しているのに対して、「感じない」とする事業所の実施率は 66.9%と 20%以上の差があった。

コンピュータウイルスの場合と同様、ユーザのコンピュータの不正アクセスに対する意識を高め、セキュリティ対策実施の重要性を認識させる必要があると考えられる。

図表Ⅳ－４　コンピュータの不正アクセスに対する脅威と
セキュリティ対策の実施状況



２・２　　コンピュータへの不正アクセス被害防止策

コンピュータへの不正アクセスによる被害状況をみると、発見の経緯としては、「ログ情報を見て」という回答が非常に多く、ログ情報の記録とそのチェックが重要なことがわかる。

コンピュータへの不正アクセス被害は、昨年から急激に増加している。今回のアンケート結果をみても、不正アクセスに対する関心が急速に高まっているのがわかる。

現在のところ被害規模も比較的小さく実害がほとんどないというケースも多いが、コンピュータウイルスと同様に、知識に普及に伴って犯罪が増えるという側面をもっている。関心が高まっている今こそ、不正アクセスに対する適切な情報、対処方法、防止策などの総合的な普及啓蒙活動が切望される。