

# 2007年 国内における 情報セキュリティ事象被害状況調査

- 報告書 -

2008年4月

**IPA**<sup>®</sup> 独立行政法人 情報処理推進機構  
セキュリティセンター

## 目 次

|  |    |
|--|----|
| 1. 調査概要                                    | 1  |
| 1.1. 調査目的                                  | 1  |
| 1.2. 調査対象                                  | 2  |
| 1.3. 調査期間                                  | 2  |
| 1.4. 調査方法                                  | 3  |
| 1.5. 回収結果                                  | 3  |
| 1.6. 調査項目                                  | 3  |
| 2. 調査結果                                    | 4  |
| 2.1. 回答企業・自治体の概要                           | 4  |
| 2.1.1. 業種                                  | 4  |
| 2.1.2. 総従業員数                               | 5  |
| 2.1.3. 総売上高（単体）                            | 6  |
| 2.1.4. 経営利益（単体）                            | 7  |
| 2.1.5. 規程年間営業日数および1日の営業時間                  | 8  |
| 2.1.6. IT関連の支出総額                           | 10 |
| 2.1.7. 利用しているパソコンのOSと台数                    | 11 |
| 2.1.8. LANやWAN等のネットワークの構築状況                | 14 |
| 2.2. 情報セキュリティ対策の現状                         | 15 |
| 2.2.1. 情報セキュリティ対策管理の社内体制                   | 15 |
| 2.2.2. セキュリティ対策ソフト導入状況                     | 17 |
| 2.2.3. 2007年のセキュリティ対策ソフトの導入・更新および装置の導入費用   | 26 |
| 2.2.4. 2008年のセキュリティ対策への投資額                 | 28 |
| 2.2.5. 情報セキュリティ関連製品やソリューションの導入             | 30 |
| 2.2.6. 情報セキュリティ被害防止のための組織・運用面の対策           | 32 |
| 2.2.7. セキュリティパッチの適用                        | 34 |
| 2.2.8. セキュリティパッチを導入しなかった理由                 | 36 |
| 2.2.9. Windows 98 / Me がインストールされているパソコンの割合 | 38 |
| 2.2.10. 情報セキュリティ対策教育の実施状況                  | 39 |
| 2.3. コンピュータウイルス対策に対する意識                    | 41 |
| 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         | 41 |
| 2.3.2. 「コンピュータウイルス対策基準」の認知度                | 43 |
| 2.3.3. 被害届出について                            | 44 |
| 2.4. コンピュータウイルスによる被害状況                     | 47 |
| 2.4.1. コンピュータウイルス遭遇（感染または発見）経験             | 47 |

|         |                                   |     |
|---------|-----------------------------------|-----|
| 2.4.2.  | 感染・発見したウイルスの名称                    | 50  |
| 2.4.3.  | ウイルスの感染件数                         | 53  |
| 2.4.4.  | ウイルスに感染したパソコン・サーバの台数              | 54  |
| 2.4.5.  | ウイルスの直接的な被害                       | 57  |
| 2.4.6.  | 電子商取引（EC）業務                       | 59  |
| 2.4.7.  | EC サーバ以外の業務遂行上重要なサーバ停止の影響         | 62  |
| 2.4.8.  | 2007年1年間の情報管理部門が行った復旧作業人日         | 65  |
| 2.4.9.  | 2007年1年間のシステム復旧に関して新たに購入した代替機器の費用 | 66  |
| 2.4.10. | システム復旧に関して外部に発注した業務の費用            | 68  |
| 2.4.11. | 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         | 69  |
| 2.4.12. | 復旧以外の対応                           | 71  |
| 2.4.13. | 復旧時の復旧以外の対応による外部発注費用              | 76  |
| 2.4.14. | 影響の最も大きかったウイルス                    | 77  |
| 2.5.    | ファイル共有ソフトを介した情報漏えい                | 84  |
| 2.5.1.  | 個人情報、業務情報流出被害経験の有無                | 84  |
| 2.5.2.  | 流出情報の種類                           | 85  |
| 2.5.3.  | 対応延べ人日                            | 86  |
| 2.5.4.  | 対応内容                              | 87  |
| 2.6.    | 標的型攻撃による被害について                    | 92  |
| 2.6.1.  | 標的型攻撃の電子メールの有無                    | 92  |
| 2.7.    | その他の脅威について                        | 93  |
| 2.7.1.  | スパイウェアの被害の有無                      | 93  |
| 2.7.2.  | 発見されたスパイウェアの侵入経路                  | 94  |
| 2.8.    | 情報セキュリティ事象に関する間接的被害について           | 95  |
| 2.8.1.  | ウイルス、スパイウェアによる間接的な被害              | 95  |
| 2.8.2.  | 情報漏えいによる間接的な被害                    | 97  |
| 3.      | 考察                                | 98  |
| 4.      | 情報漏えいに関する被害事例調査                   | 100 |
| 4.1.    | 調査目的                              | 100 |
| 4.2.    | 被害事例調査（ヒアリング）                     | 101 |
| 4.2.1.  | 不正アクセスによる情報漏えいの被害実態               | 101 |
| 4.2.2.  | Winnyのウイルス感染による情報漏えいの被害実態         | 106 |
| 4.2.3.  | 内部犯行による情報漏えいの被害実態                 | 111 |
| 4.3.    | 情報漏えい等に関するグループインタビュー調査            | 115 |
| 4.3.1.  | 情報管理の考え方                          | 115 |
| 4.3.2.  | 経営的観点から見た情報漏えい等の被害・影響             | 117 |
| 4.3.3.  | 考察                                | 119 |

## 1. 調査概要

### 1.1. 調査目的

ネットワークを軸とする IT（情報技術）は、わが国の社会・経済の基盤を支える極めて重要な社会インフラを担っている。そのため、情報セキュリティ事象（コンピュータウイルス、不正アクセス、情報漏えい等）が発生すると、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<sup>1</sup>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。さらに、取引先や提供サービスのエンドユーザへの感染拡大、トラフィックの急増によるネットワーク障害といった IT 社会への悪影響も発生する可能性がある。

つまり、情報セキュリティ対策は、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る。したがって、政府は、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、その背中を押す適切な施策の実施を通じて、企業の情報セキュリティ対策を促進することが求められている。

しかし、情報セキュリティ対策の実施にはコストを要するため、企業が十分な予算を確保するのに有効な客観的データが必要である。企業が適切な対策レベルを模索するためには、最新の情報セキュリティ事象の被害実態及び対策の実施状況を把握する必要がある。IPA では、これまで継続的な実態調査を実施してきたが、これらの精度をさらに安定的に高めるとともに、情報セキュリティ事象によって企業に何が起こるのかを具体的に示すことによって、説得力のある啓発効果が期待できる。

そこで、本調査においては以下の目的を設定する。

- ・ 国内における情報セキュリティ事象の被害状況や対策状況に係る実態の定量的把握
- ・ 不正アクセス、情報漏えい等の情報セキュリティ事象による被害や対応の具体事例の収集と集約

---

<sup>1</sup> P2P ソフトのウイルスによる機密情報の流出事故は 2007 年に入っても引き続き頻発している。また海外では、米企業の社内ネットワークに不正アクセスして未公開情報を盗み出し、その情報をもとに株式市場で不正に利益を上げたとして、2007 年 2 月、米国証券取引委員会が香港の企業等を告訴している。

## 1.2. 調査対象

本調査は、全国の企業及び自治体 11,000 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 10,000 件、及び全国の自治体 1,000 件となっている。

|      | 内容  |
|------|---|
| 標本数  | 11,000 件<br>(うち、企業 10,000 件、自治体 1,000 件)  |
| 標本台帳 | (1)企業<br>・「情報処理実態調査」対象機関<br>・四季報<br>(上記の抽出機関の補足)<br>(2)自治体<br>・財団法人地方自治情報センター   |
| 抽出方法 | (1)企業：<br>業種別、就業者規模別無作為抽出<br>(2)自治体：<br>・東京特別区 23<br>・政令指定都市 17<br>・中核市 35<br>・上記以外の県庁所在地 13<br>・その他、人口を軸とする層別抽出(比例割当法) |

なお、企業対象の調査結果は、業種や企業規模による回収のばらつきにより精度が低下する可能性がある。そこで、

- ・ 業種や企業規模によって、業務の IT 化や対策の取組み度合いが異なること
- ・ 従業員一人当たりの PC 保有台数が多いほど、ウイルス等の情報セキュリティ事象被害が発生する可能性が高いと考えられること

を考慮し、本調査では次の 2 つの軸を設定し、それぞれの軸に沿ってサンプリングを行った。

軸 1 : パソコンの従業員一人当たり保有台数が 平均(0.9)<sup>2</sup> 以上の企業 → 企業群  
平均(0.9) 未満の企業 → 企業群

軸 2 : 従業員数が 300 人以上 / 300 人未満

## 1.3. 調査期間

調査実施期間 : 2008 年 1 月

調査対象期間 : 2007 年 1 月 ~ 12 月

---

<sup>2</sup> 経済産業省「平成 17 年度情報処理実態調査結果」による。ただし、「不動産業」「飲食店、宿泊業」「医療・福祉」「教育、学習支援業」については、「その他の非製造業」の値で代替した。

#### 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 11,000 件に対し、2,280 件の有効回収があり、有効回収率は 20.7%であった。企業、自治体別の内訳は下表の通りである。

|                 | 発送数    | 回収数   | 回収率   |
|-----------------|--------|-------|-------|
| 全体              | 11,000 | 2,280 | 20.7% |
| (企業 / 自治体別 内訳)  |        |       |       |
| 企業              | 10,000 | 1,859 | 18.6% |
| 自治体             | 1,000  | 421   | 42.1% |
| (企業業種・規模別 内訳)   |        |       |       |
| 企業群 ・ 300 人以上企業 | 2,500  | 416   | 16.6% |
| 企業群 ・ 300 人未満企業 | 2,500  | 461   | 18.4% |
| 企業群 ・ 300 人以上企業 | 2,500  | 385   | 15.4% |
| 企業群 ・ 300 人未満企業 | 2,500  | 597   | 23.9% |

#### 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
- ( 6 ) その他のセキュリティ事象に関する発見と被害状況

## 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」(18.5%)を除くと「他の製造業」(17.6%)、「他のサービス業」(14.2%)が多く、次いで「情報通信業」(9.3%)、「卸売業」(7.4%)、「建設業」(7.0%)と続く。

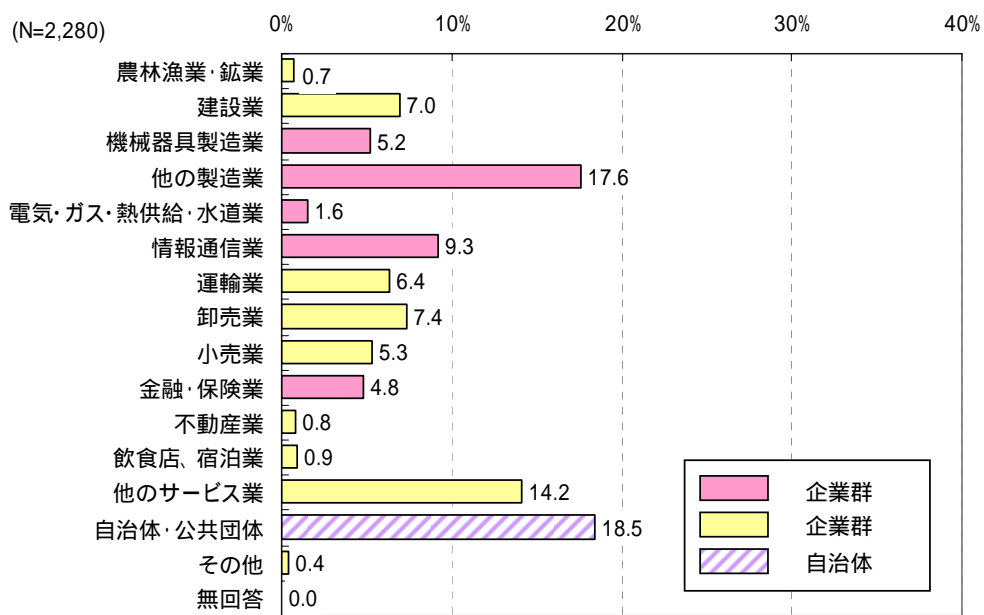


図 2.1-1 業種

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」に含めた。

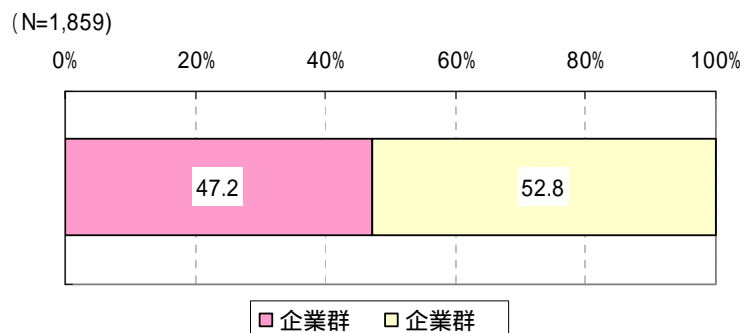


図 2.1-2 業種 (企業群別)

### 2.1.2. 総従業員数

企業・自治体全体で見た総従業員数は「300 人未満」で半数強であるが、自治体は「300 人未満」が 4 割以下に留まる一方「1,000 人以上」が 3 割近くに達する。平均をみても、企業の平均が 965 人、自治体が 2,012 人、全体平均が 1,154 人であることから、自治体の規模は企業と比較して大きい傾向にあると言える。

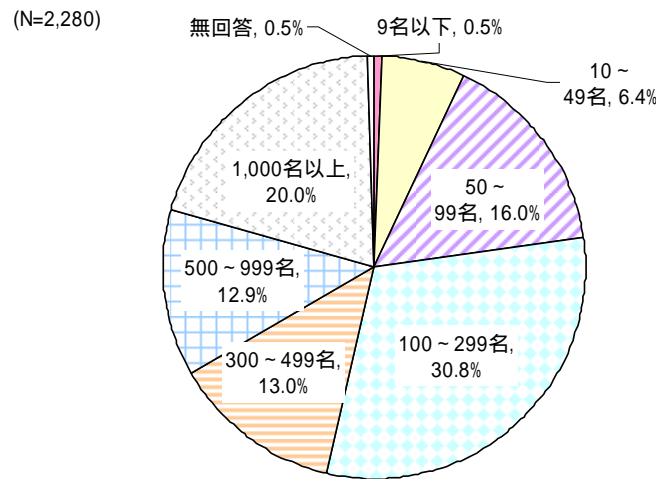


図 2.1-3 総従業員数

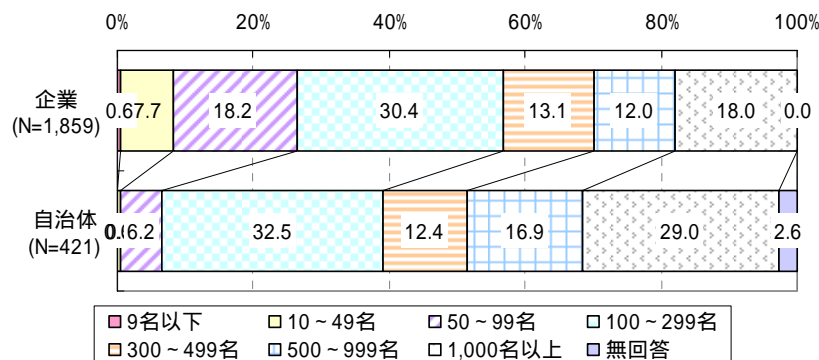


図 2.1-4 総従業員数（企業 / 自治体別）

### 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」が約半数である。全体平均は751.4億円である。

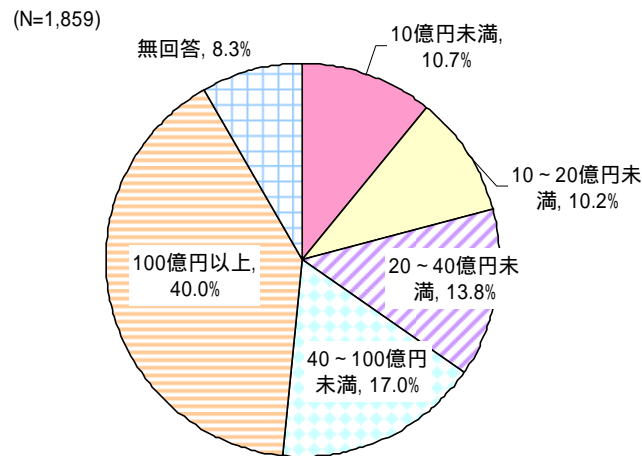


図 2.1-5 総売上高（単体、企業のみ）

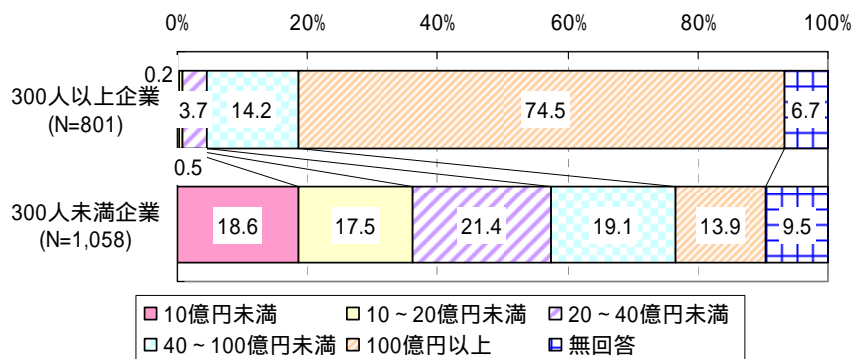


図 2.1-6 総売上高（企業、就業者規模別）

表 2.1-1 総売上高平均（企業）

| 全体      | 300人以上企業  | 300人未満企業 | 企業群     | 企業群     |
|---------|-----------|----------|---------|---------|
| 751.4億円 | 1,625.9億円 | 68.7億円   | 866.8億円 | 645.1億円 |

#### 2.1.4. 経営利益（単体）

經常利益は4億円未満が半数程度である。全体平均は38.7億円である。

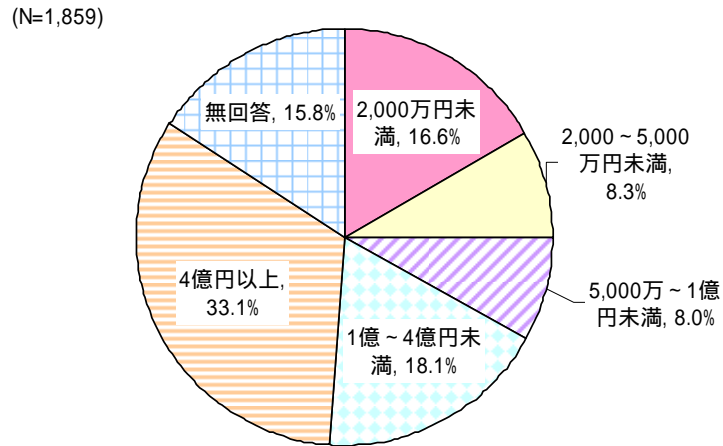


図 2.1-7 経営利益（単体、企業のみ）

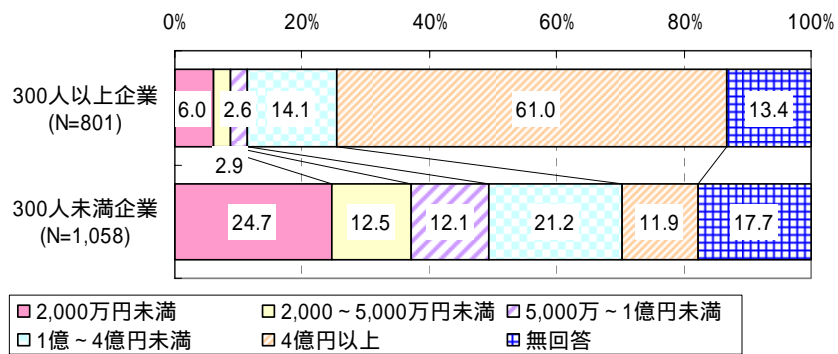


図 2.1-8 経営利益（企業、就業者規模別）

表 2.1-2 経営利益平均（企業）

| 全体     | 300人以上企業 | 300人未満企業 | 企業群    | 企業群    |
|--------|----------|----------|--------|--------|
| 38.7億円 | 84.3億円   | 2.4億円    | 52.9億円 | 25.2億円 |

### 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45.4%で最も多く、「250～299日」が26.9%で続く。自治体と比較して企業の方が営業日数が多い。また、就業者規模別では、300人未満企業の方が営業日数が多い傾向にある。

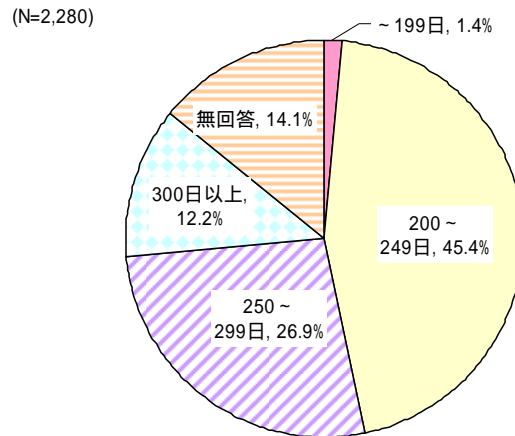


図 2.1-9 規程年間営業日数

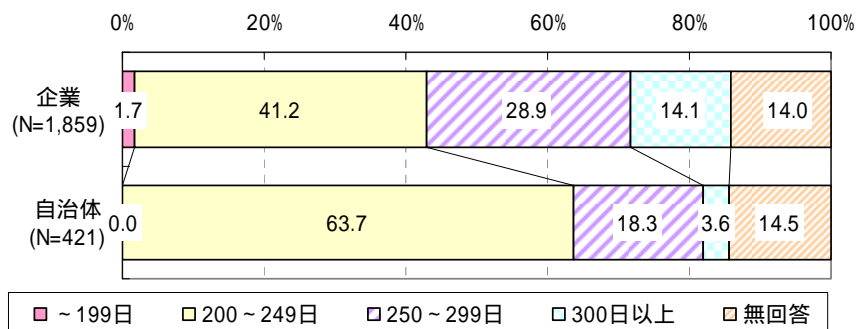


図 2.1-10 規程年間営業日数 (企業 / 自治体別)

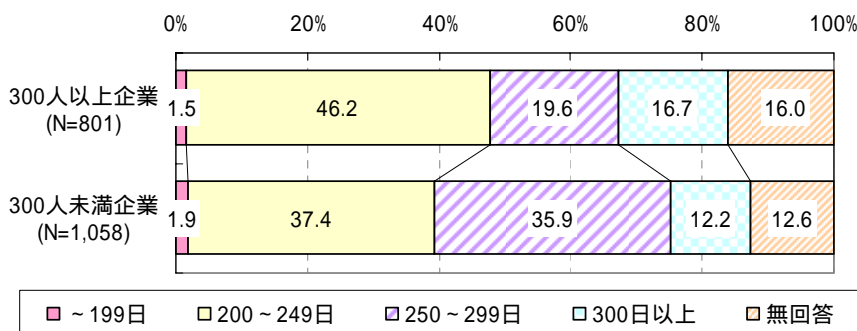


図 2.1-11 規程年間営業日数 (就業者規模別)

1日の営業時間は約半数が「8時間」であり、特に自治体の8割近くが「8時間」と回答している。就業者規模別に見ると、「8時間未満」と営業時間が短い回答は300人以上企業の方が多く、「8時間」は300人未満企業の方が多い。

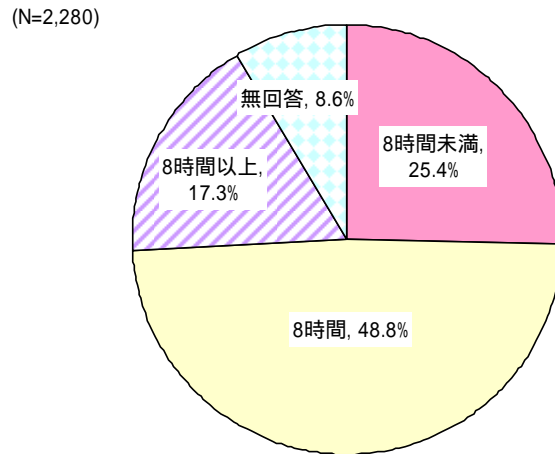


図 2.1-12 1日の営業時間

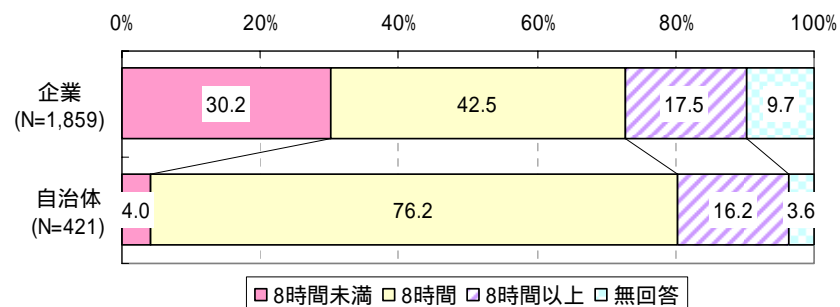


図 2.1-13 1日の営業時間（企業／自治体別）

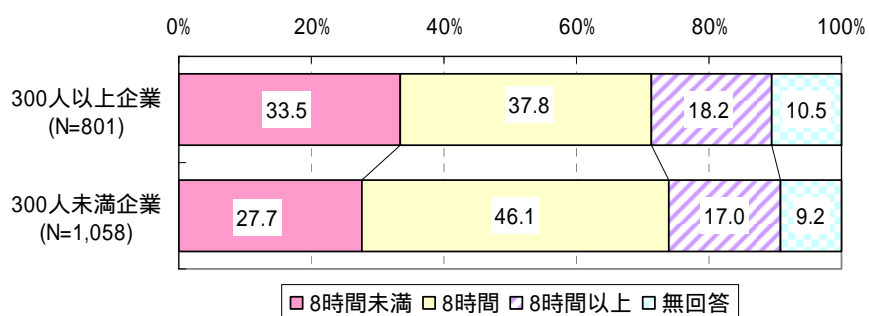


図 2.1-14 1日の営業時間（従業員別）

### 2.1.6. IT 関連の支出総額

IT 関連の支出総額は、「2,000 万円未満」が最も多く 3 割を超える。300 人未満企業の 6 割近くは「2,000 万円未満」であるが、300 人以上企業の半数以上は 1 億円以上である。企業群別に見ると、「4 億円以上」において企業群 より企業群 の方が約 10 ポイント高く、IT 活用度の高い企業の方が、IT 投資も積極的であることが示されている。

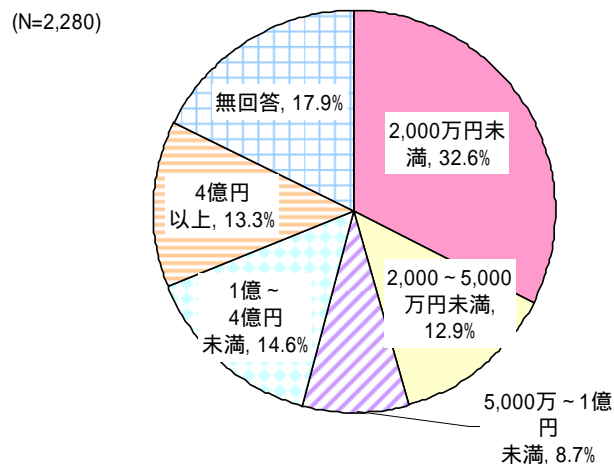


図 2.1-15 IT 関連の支出総額

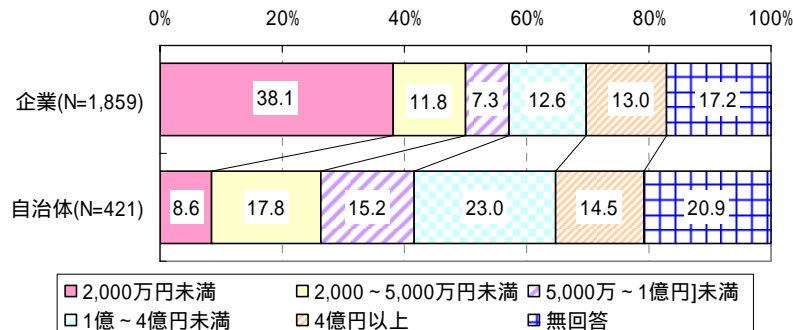


図 2.1-16 IT 関連の支出総額（企業 / 自治体別）

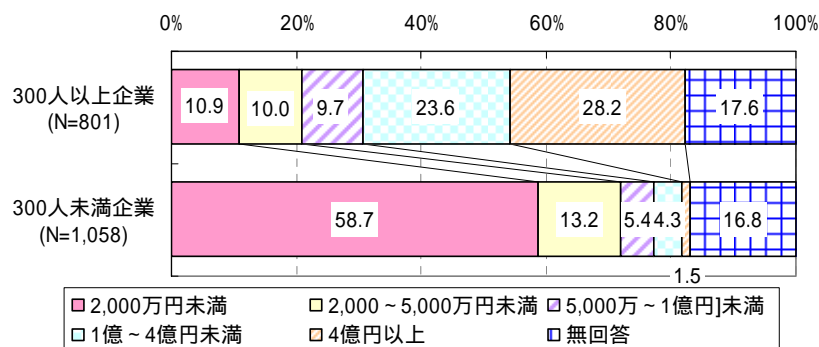


図 2.1-17 IT 関連の支出総額（就業者規模別）

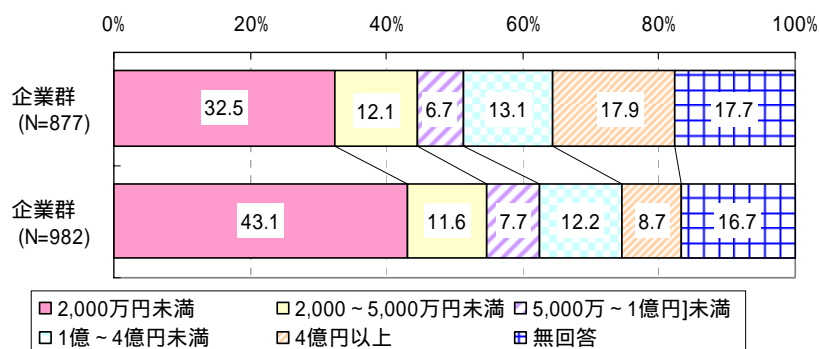


図 2.1-18 IT 関連の支出総額（企業群別）

### 2.1.7. 利用しているパソコンのOSと台数

ほぼ全ての組織が Windows 系のパソコンを利用しており、そのうち 6 割が 100 台以上を保有している。Macintosh 系、Unix・Linux 系のパソコンを 1 台でも利用している組織はいずれも 2 割弱に留まる。

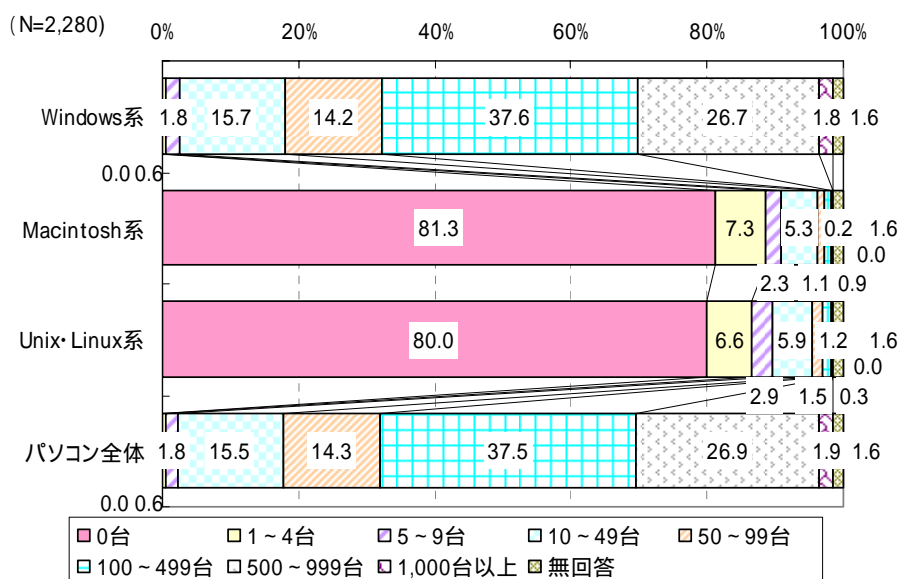
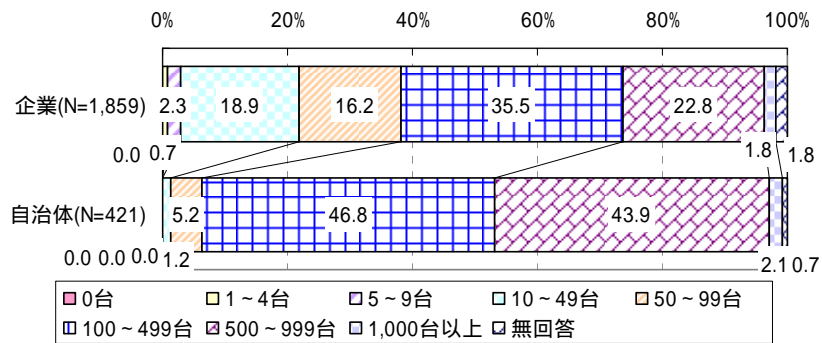
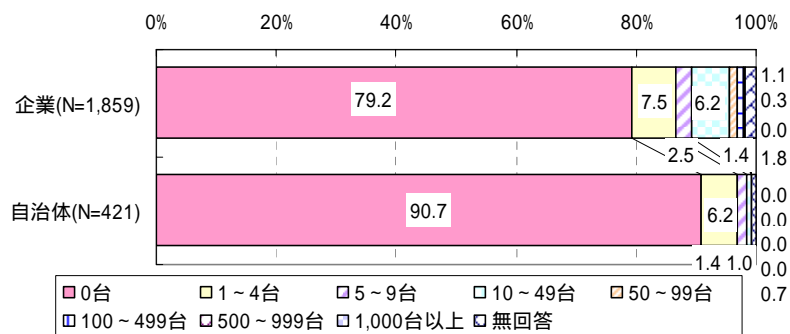


図 2.1-19 利用しているパソコンのOSと台数

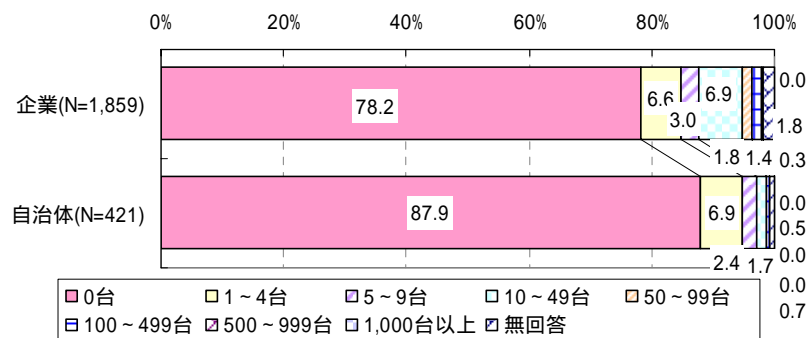
< Windows 系 >



< Macintosh 系 >



< Unix・Linux 系 >



< 全体 >

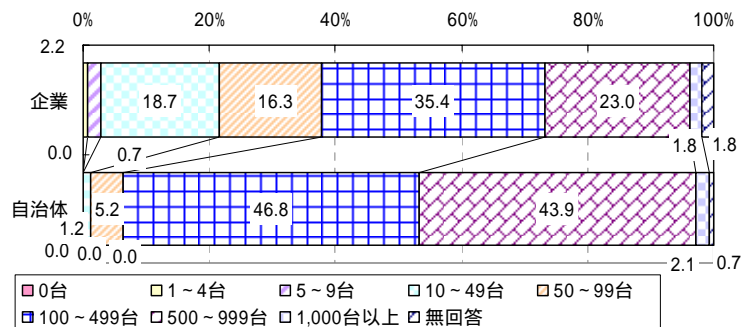
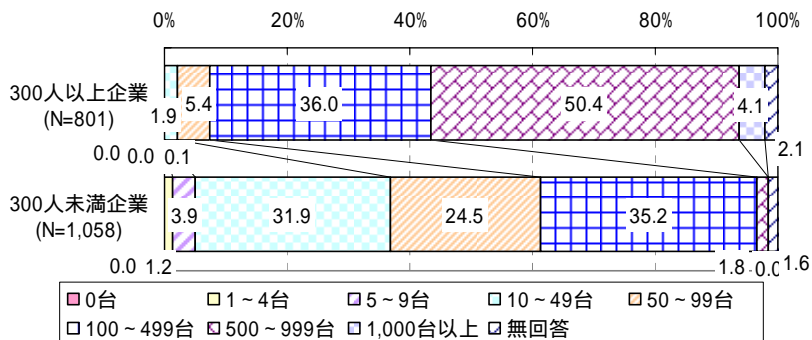
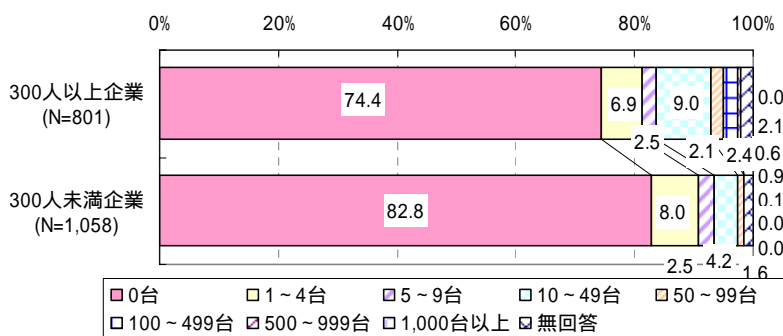


図 2.1-20 利用しているパソコンのOSと台数（企業／自治体別）

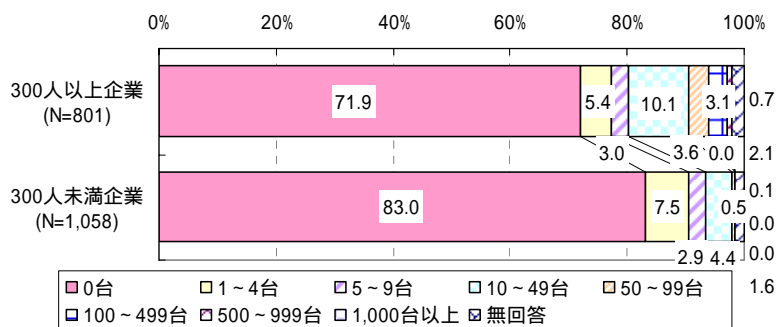
< Windows 系 >



< Macintosh 系 >



< Unix・Linux 系 >



< 全体 >

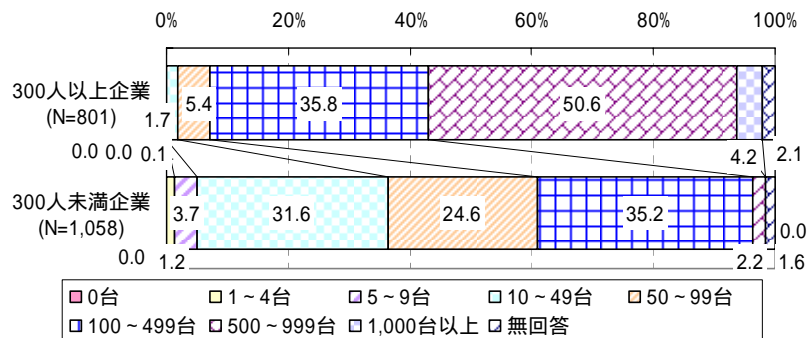


図 2.1-21 利用しているパソコンのOSと台数（就業者規模別）

### 2.1.8. LAN や WAN 等のネットワークの構築状況

全体の 6 割が「機関内の事業所間ネットワークまで構築」しているが、企業と比較すると自治体の方が広範囲のネットワークを構築している傾向にある。また、300 人以上企業の 2 割が「外部の機関とのネットワークまで構築」しているが、300 人未満企業では 1 割以下に留まる。

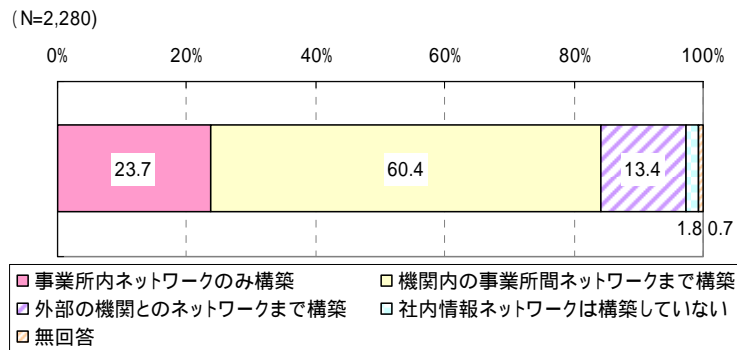


図 2.1-22 LAN や WAN 等のネットワークの構築状況

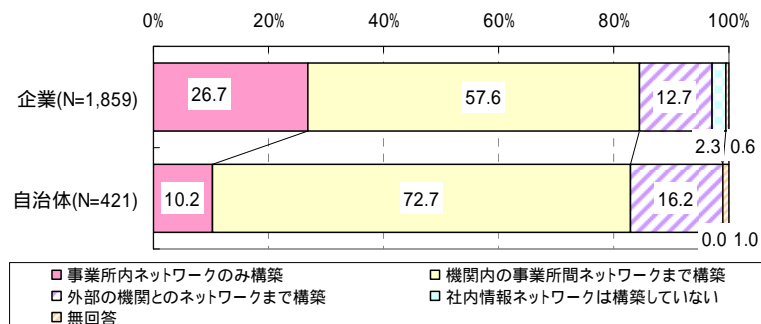


図 2.1-23 LAN や WAN 等のネットワークの構築状況（企業 / 自治体別）

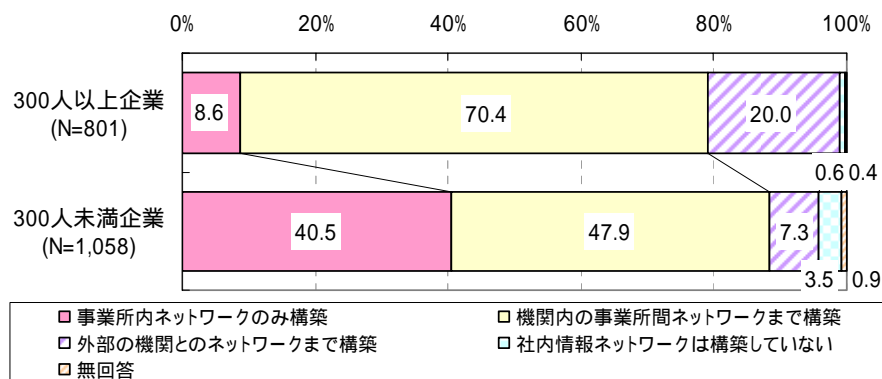


図 2.1-24 LAN や WAN 等のネットワークの構築状況（就業者規模別）

## 2.2. 情報セキュリティ対策の現状

### 2.2.1. 情報セキュリティ対策管理の社内体制

専門あるいは兼務を問わず、情報セキュリティ専門部署や専門担当が設置されている組織は7割を超える。企業より自治体、300人未満企業より300人以上の企業、企業群より企業群の方が、専門部署や専門担当が設置し、情報セキュリティ対策管理体制を整備している傾向が強い。

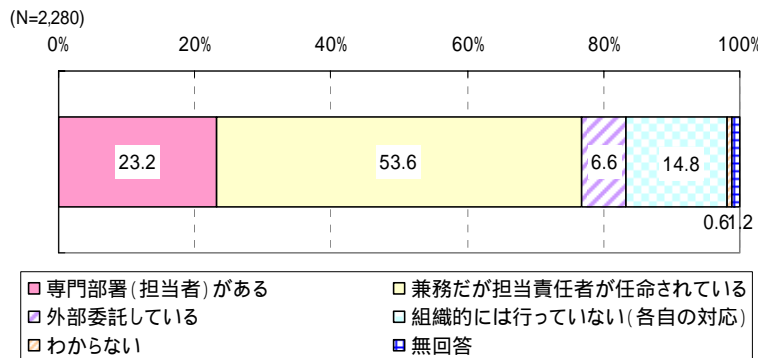


図 2.2-1 情報セキュリティ対策管理の社内体制

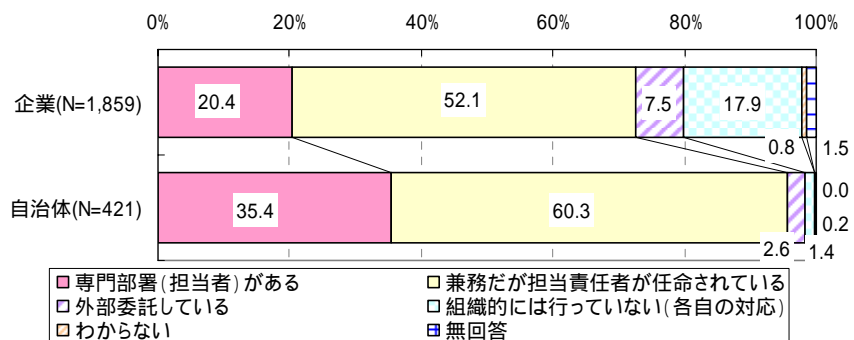


図 2.2-2 情報セキュリティ対策管理の社内体制(企業/自治体別)

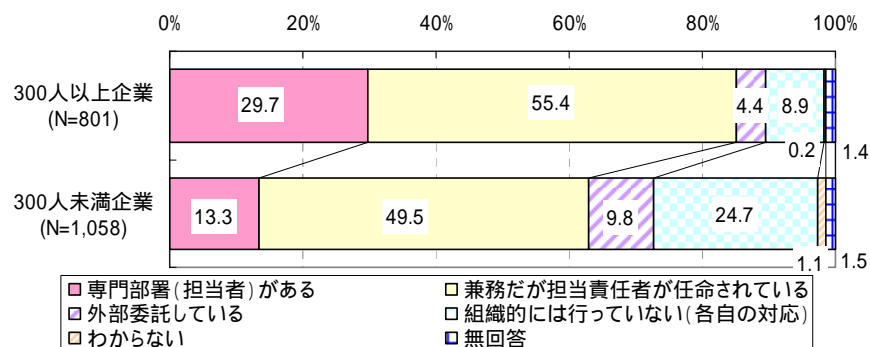


図 2.2-3 情報セキュリティ対策管理の社内体制(就業者規模別)

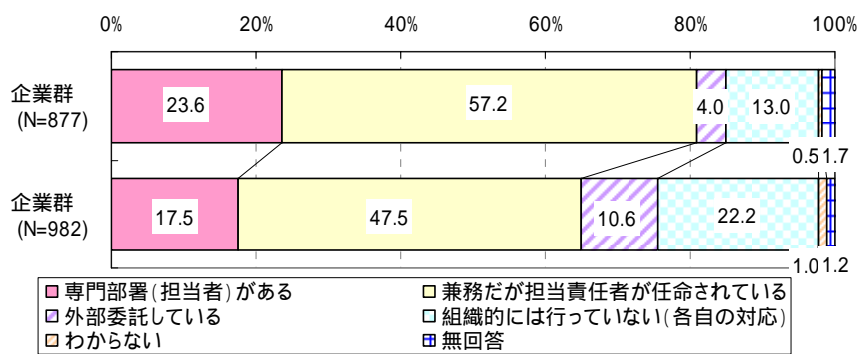


図 2.2-4 情報セキュリティ対策管理の社内体制（企業群別）

### 2.2.2. セキュリティ対策ソフト導入状況

#### (1) 各自クライアント（パソコン）への導入

クライアント（PC）のセキュリティ対策ソフト導入状況を見ると、組織の「9割以上に導入済み」である比率は、「ウイルス対策ソフト」が9割、「スパイウェア対策ソフト」が5割、「パーソナルファイアウォール」が4割、「スパムメール対策」「P2Pソフトウェア等のインストール状況チェック」が3割である。

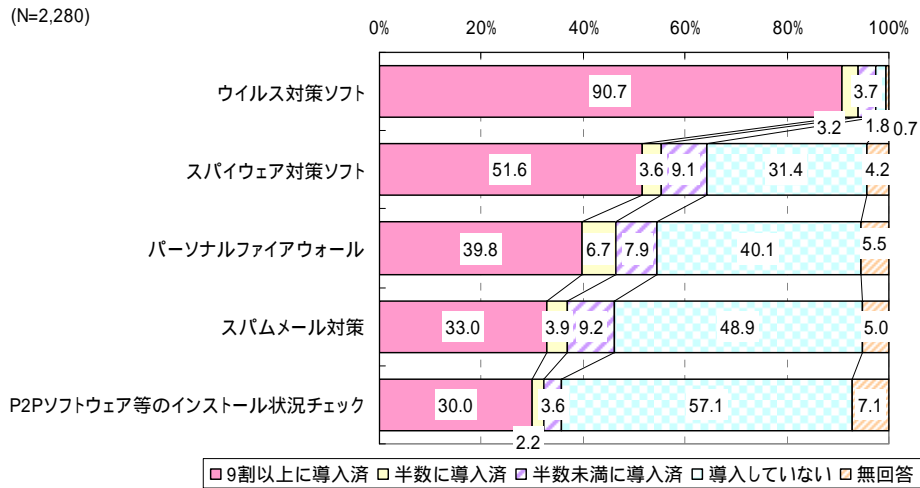
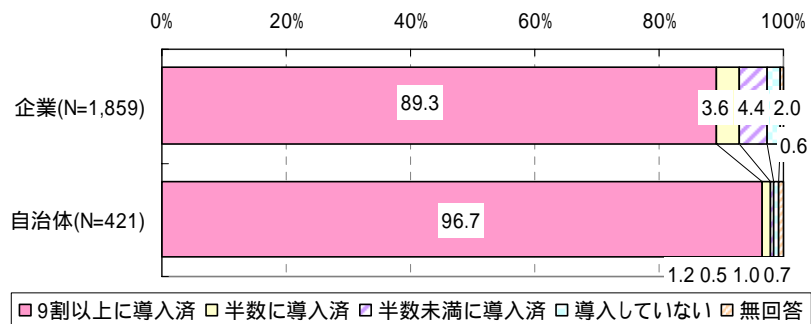
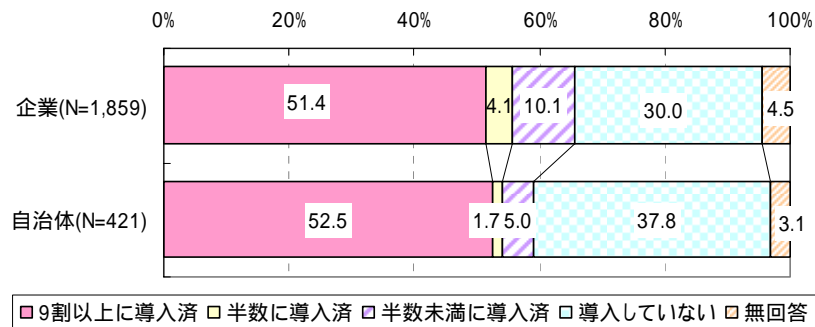


図 2.2-5 各自クライアント（パソコン）への導入

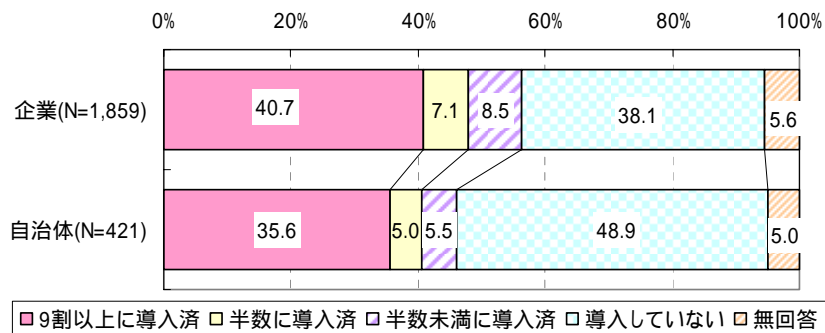
#### < ウイルス対策ソフト >



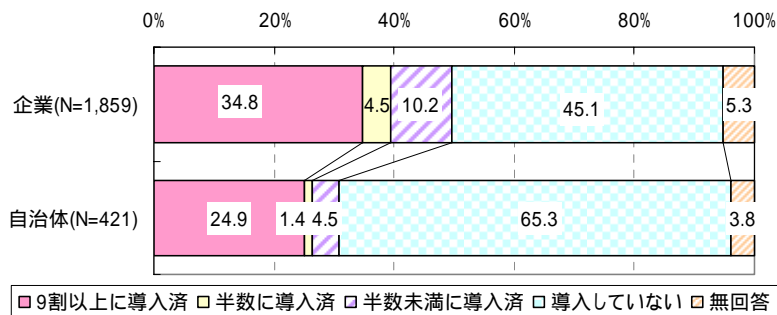
< スパイウェア対策ソフト >



< パーソナルファイアウォール >



< スпамメール対策 >



< P2P ソフトウェア等のインストール状況チェック >

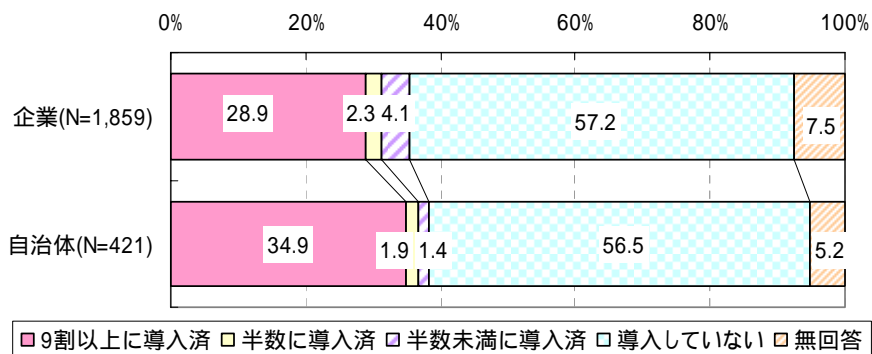
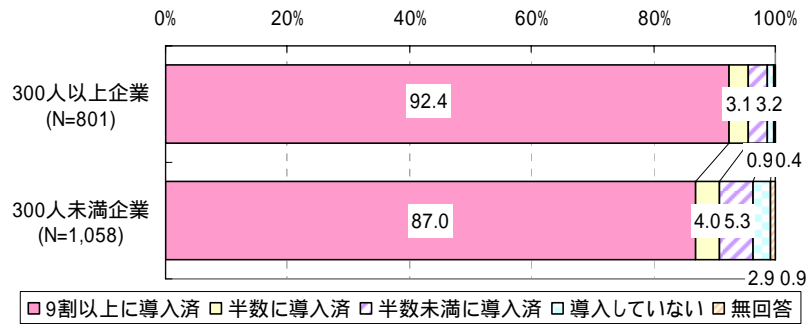
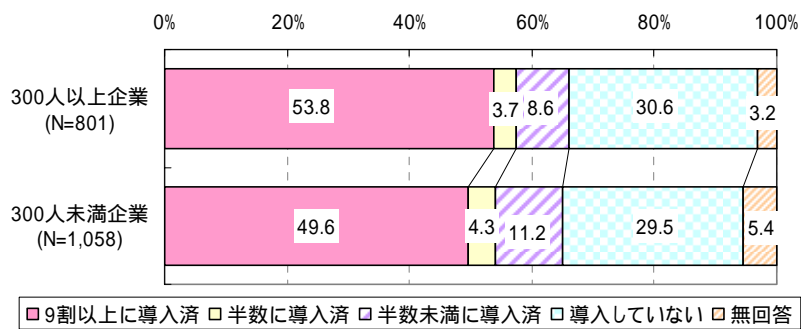


図 2.2-6 各自クライアント（パソコン）への導入（企業／自治体別）

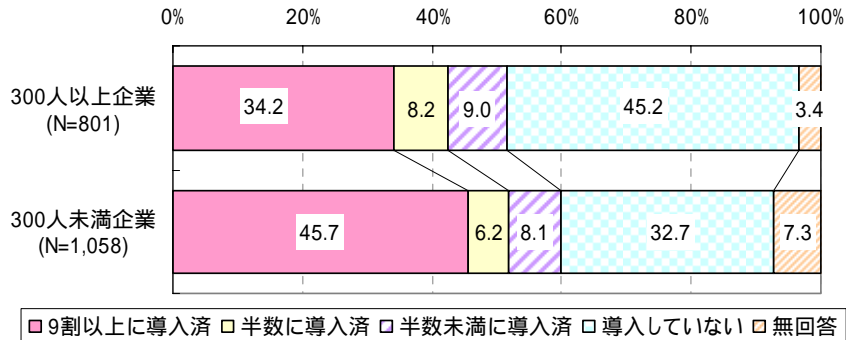
< ウイルス対策ソフト >



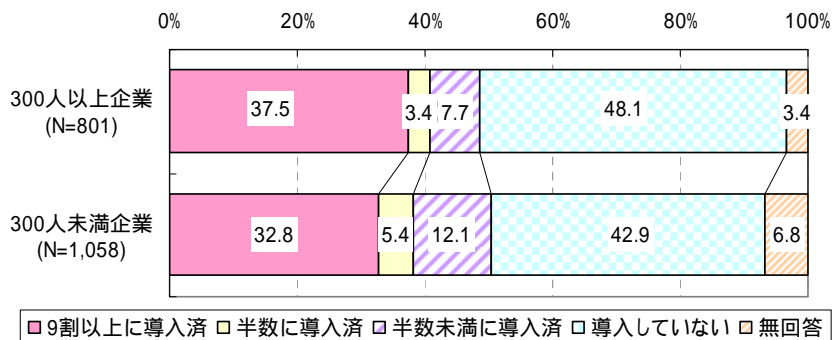
< スパイウェア対策ソフト >



< パーソナルファイアウォール >



< スпамメール対策 >



< P2P ソフトウェア等のインストール状況チェック >

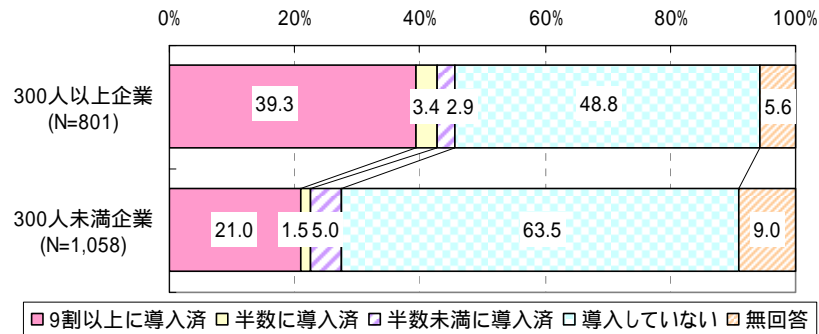


図 2.2-7 各自クライアント（パソコン）への導入（就業者規模別）

(2) ネットワークサーバ（メールサーバ、Webサーバなど）への導入

ネットワークサーバに対し、ウイルス対策ソフトは、約8割の組織において「9割以上に導入済」である。「9割以上に導入済み」である比率は、「スパイウェア対策ソフト」および「スパムメール対策」は約5割である。

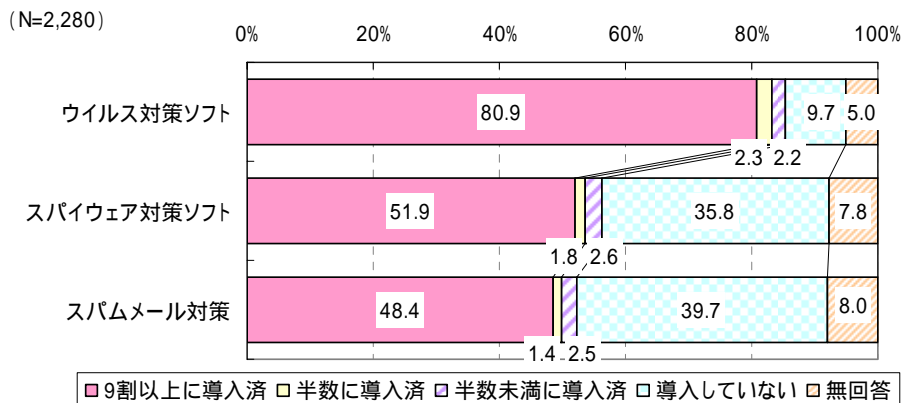
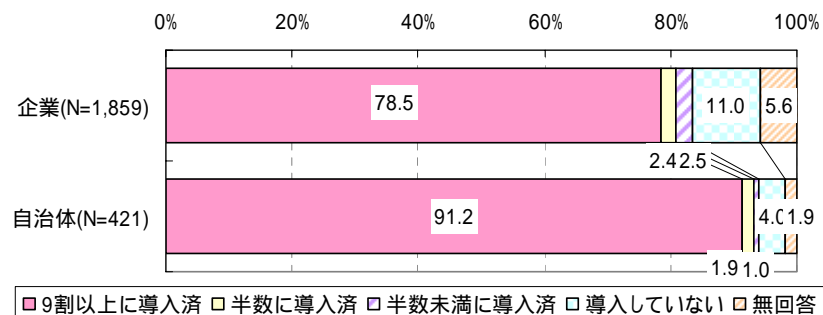
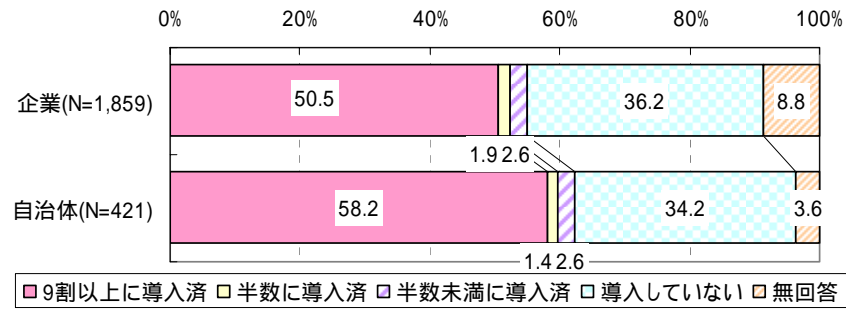


図 2.2-8 ネットワークサーバ（メールサーバ、Webサーバなど）への導入

< ウイルス対策ソフト >



< スパイウェア対策ソフト >



< スпамメール対策 >

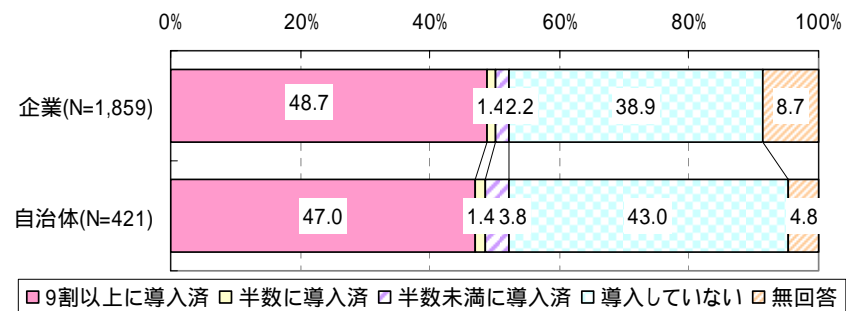
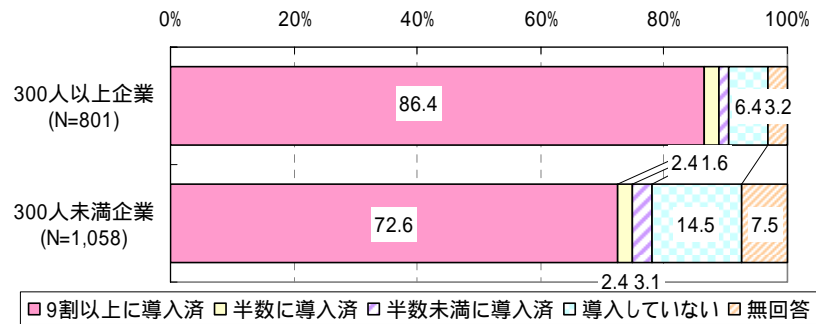
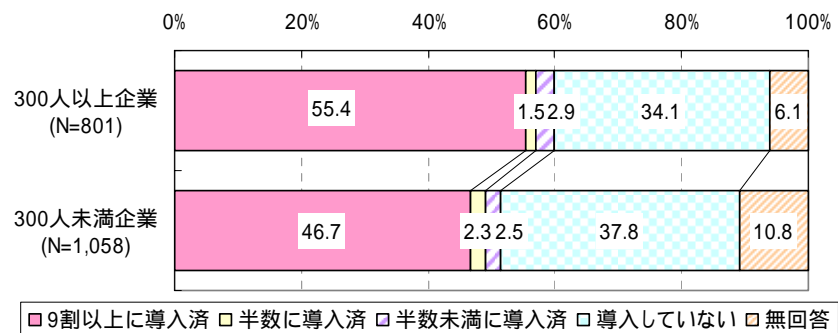


図 2.2-9 ネットワークサーバ（メールサーバ、Webサーバなど）への導入（企業／自治体別）

< ウイルス対策ソフト >



< スパイウェア対策ソフト >



< スпамメール対策 >

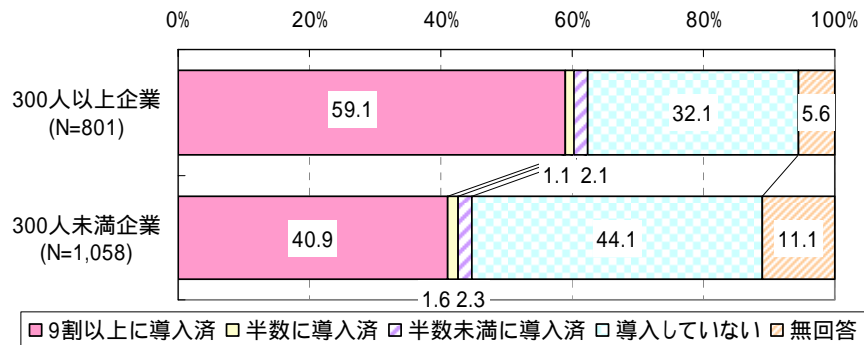


図 2.2-10 ネットワークサーバ（メールサーバ、Webサーバなど）への導入（就業者規模別）

(3) ローカルサーバ（ファイルサーバ、プリントサーバなど）への導入

ローカルサーバに対し、ウイルス対策ソフトは約7割、「スパイウェア対策ソフト」は約4割の組織が「9割以上に導入済」である。

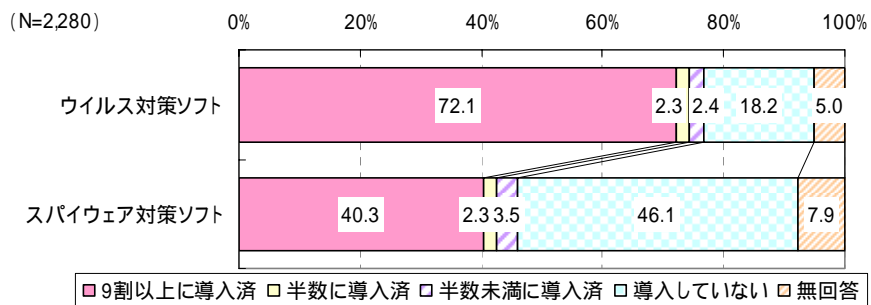
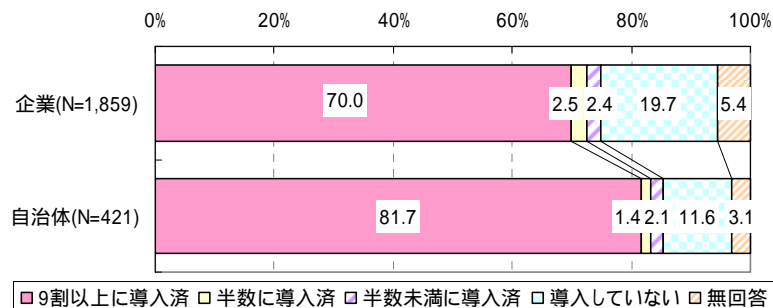


図 2.2-11 ローカルサーバ（ファイルサーバ、プリントサーバなど）への導入

< ウィルス対策ソフト >



<スパイウェア対策ソフト>

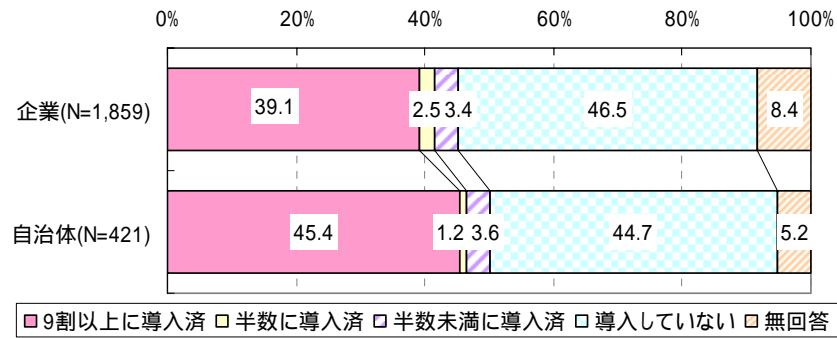
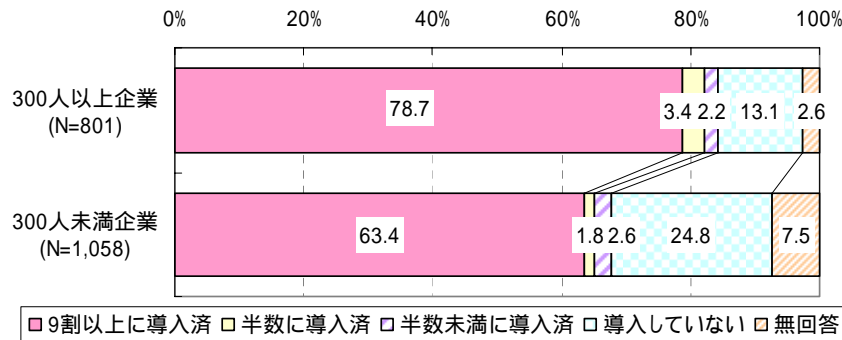


図 2.2-1 ローカルサーバ(ファイルサーバ、プリントサーバなど)への導入(企業/自治体別)

<ウイルス対策ソフト>



<スパイウェア対策ソフト>

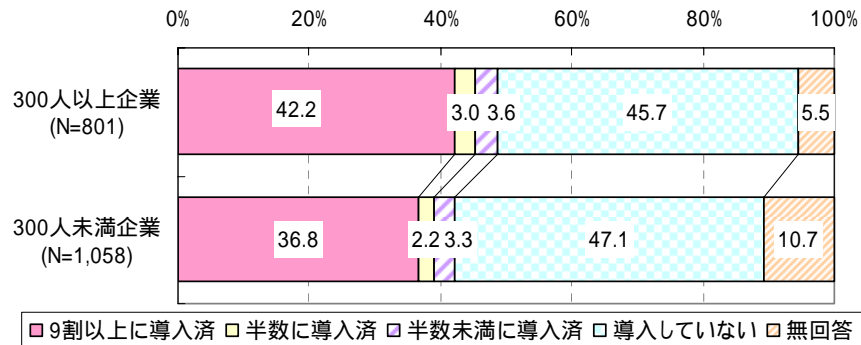


図 2.2-2 ローカルサーバ(ファイルサーバ、プリントサーバなど)への導入(就業者規模別)

(4)その他

その他のパソコン・サーバ等に対し、「9割以上に導入済」であるのは、「ファイアウォール」が7割、「IDS/IPSによる侵入検知」及び「プロバイダによるウイルスチェックサービス」が約3割である。

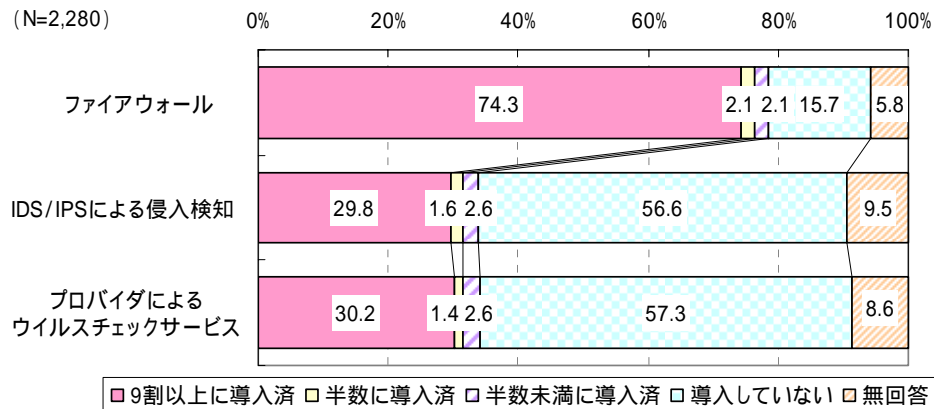
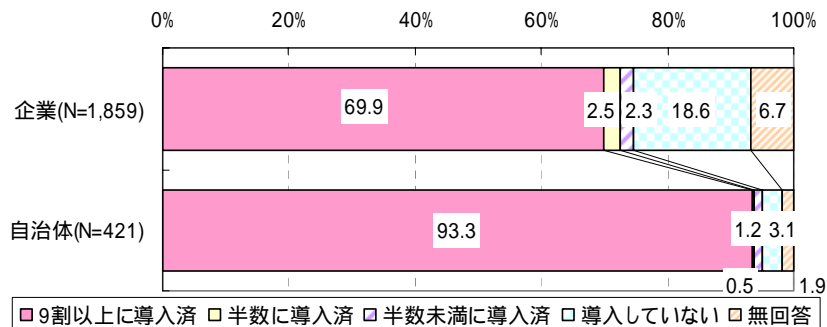
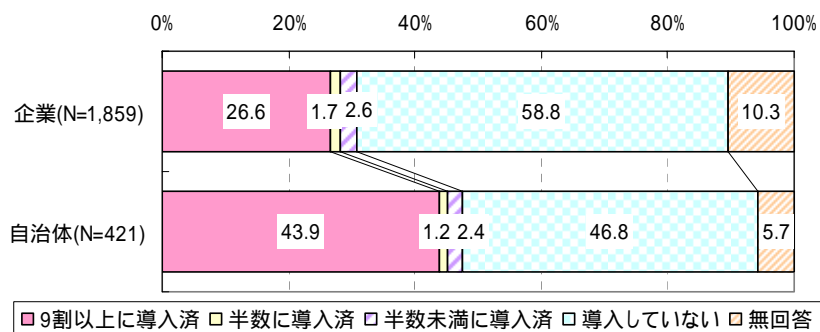


図 2.2-12 その他のパソコン・サーバに対する導入

<ファイアウォール>



<IDS/IPSによる侵入検知>



< プロバイダによるウイルスチェックサービス >

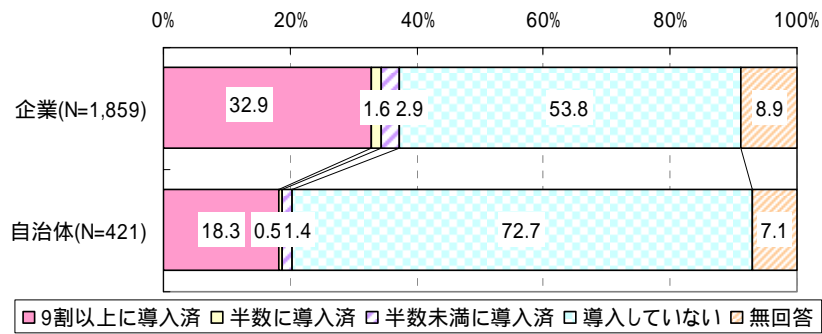
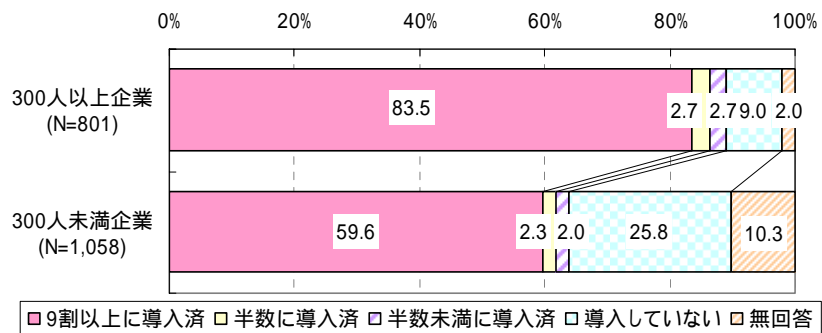
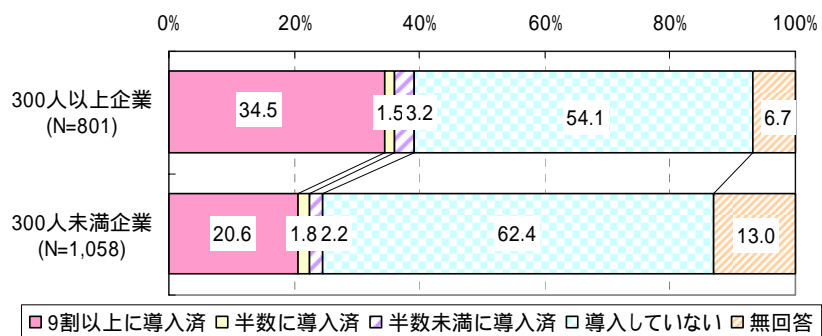


図 2.2-13 その他のパソコン・サーバに対する導入（企業／自治体別）

< ファイアウォール >



< IDS/IPS による侵入検知 >



<プロバイダによるウイルスチェックサービス>

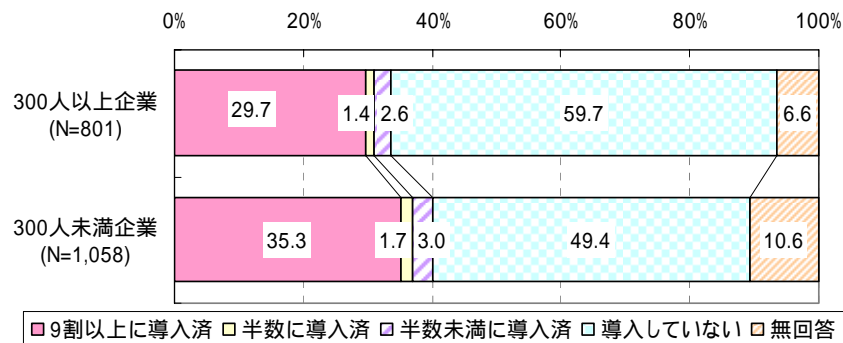


図 2.2-14 その他のパソコン・サーバに対する導入（就業者規模別）

2.2.3. 2007年のセキュリティ対策ソフトの導入・更新および装置の導入費用

2007年にウイルス対策ソフトの導入・更新にかけた費用は「0万円」が12.5%、「100万円未満」が34.9%、「100万円以上」が41.5%である。企業と自治体を比較すると、自治体の方が費用が高い傾向にある。また、300人未満企業の4割近くが「1万～49万円」に留まるのに対し、300人以上企業の半数近くが「200万円以上」である。企業群でも3割以上が「200万円以上」であるが、企業群では3割以上が「1万～49万円」である。

(N=2,280)

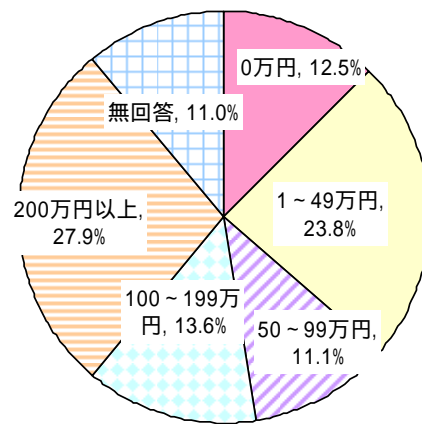


図 2.2-15 ウイルス対策ソフトの導入・更新費用

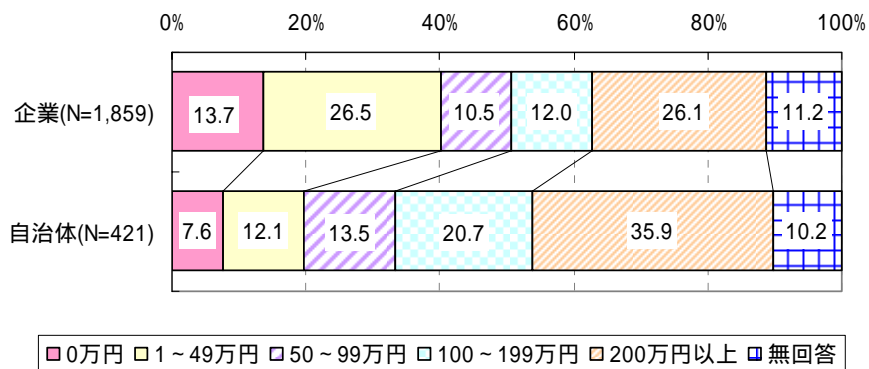


図 2.2-16 ウイルス対策ソフトの導入・更新費用（企業／自治体別）

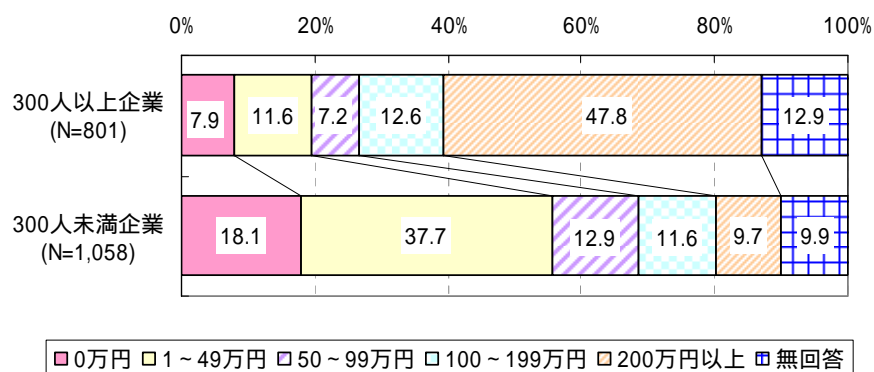


図 2.2-17 ウイルス対策ソフトの導入・更新費用（就業者規模別）

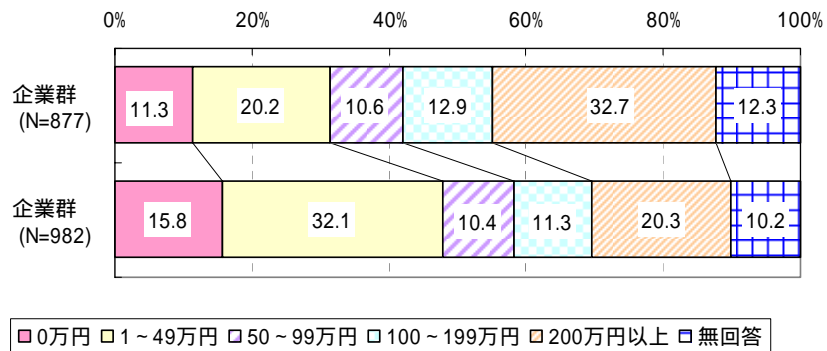


図 2.2-18 ウイルス対策ソフトの導入・更新費用（企業群別）

### 2.2.4. 2008年のセキュリティ対策への投資額

2008年のセキュリティ対策への投資額は「2007年と同程度」が6割を超え最も多い。

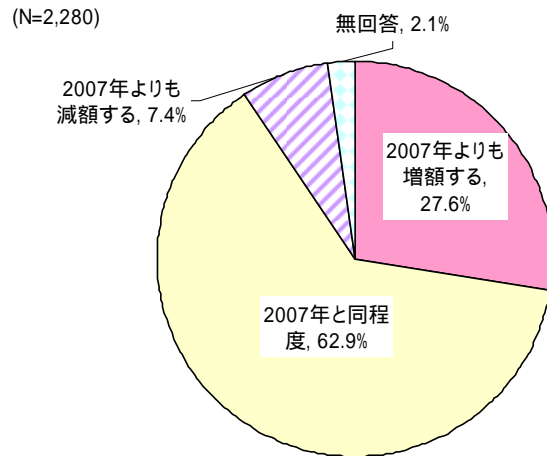


図 2.2-19 来年1年間（2008年）のセキュリティ対策への投資額

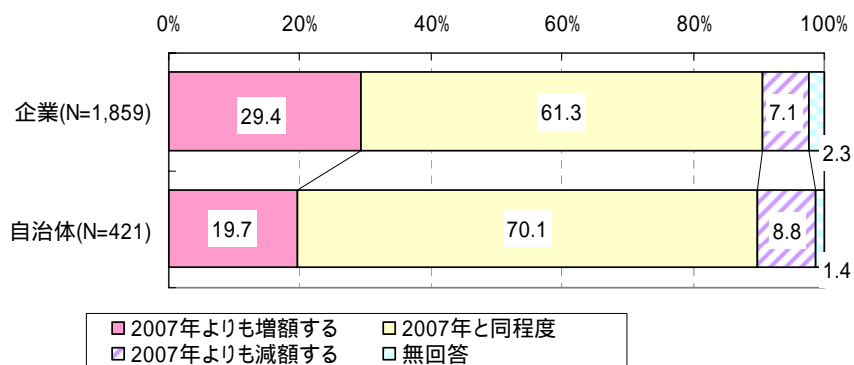


図 2.2-20 来年1年間（2008年）のセキュリティ対策への投資額（企業/自治体別）

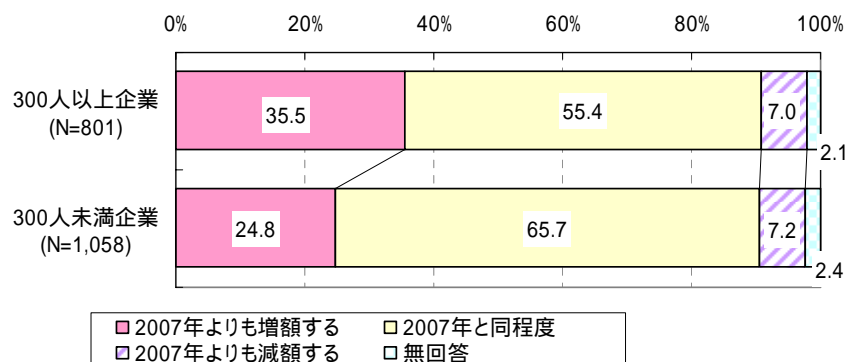


図 2.2-21 来年1年間（2008年）のセキュリティ対策への投資額（就業者規模別）

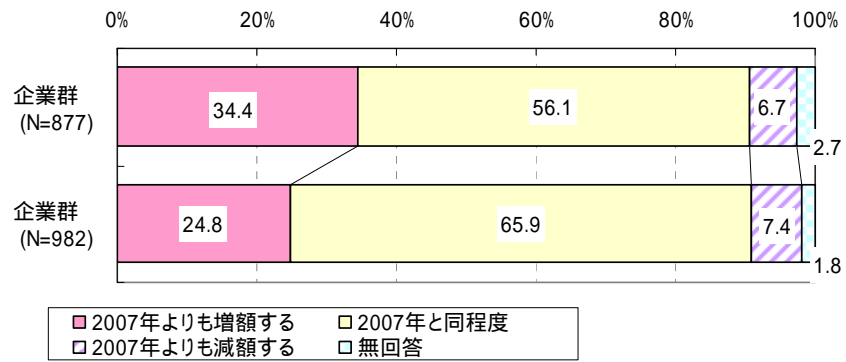


図 2.2-22 来年 1 年間 (2008 年) のセキュリティ対策への投資額 (企業群別)

### 2.2.5. 情報セキュリティ関連製品やソリューションの導入

情報セキュリティ関連製品やソリューションの導入状況を見ると、「VPN」が最も多く 44.0%、「ウェブ閲覧のフィルタリング」が次いで 36.5%でこの 2 対策が 3 割を超えている。その他、「顧客情報等の暗号化」( 14.8% )、「電子署名」( 10.1% ) が 1 割を超えている。一方、「特にない」との回答も 3 割を超える。

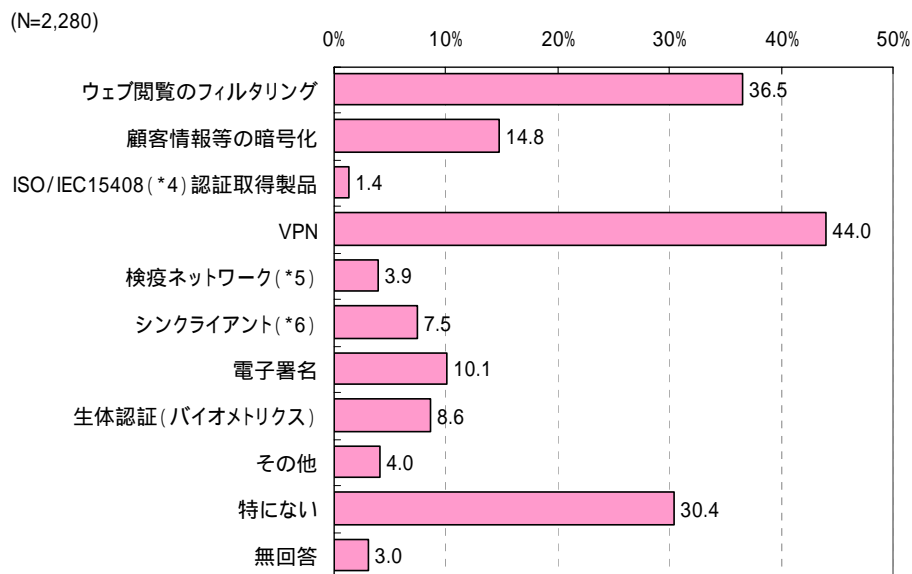


図 2.2-23 情報セキュリティ関連製品やソリューションの導入

企業 / 自治体別に見ると、特に「ウェブ閲覧のフィルタリング」の導入率について、自治体の方が約 30 ポイント高いことが特徴的である。

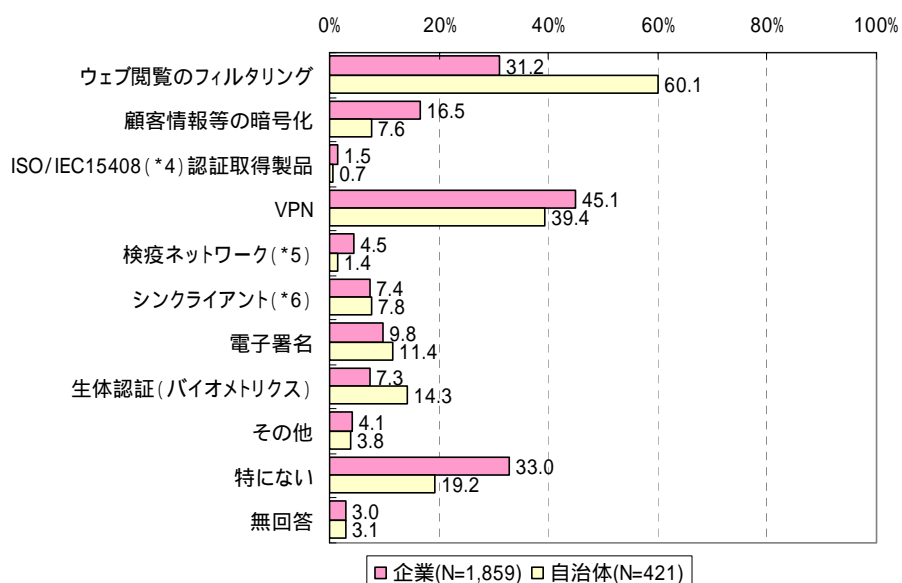


図 2.2-24 情報セキュリティ関連製品やソリューションの導入 (企業 / 自治体別)

就業者規模別に見ると、全ての項目において300人以上企業の導入率が上回っている。特に「ウェブ閲覧のフィルタリング」「VPN」ではその差が顕著である。300人未満企業においては、「特にない」との回答も半数近くに達する。

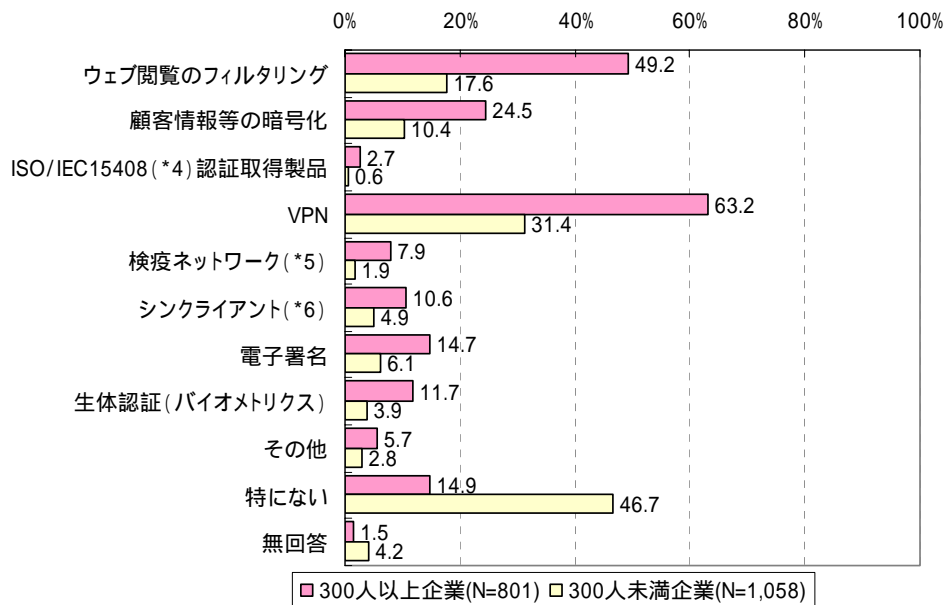


図 2.2-25 情報セキュリティ関連製品やソリューションの導入（就業者規模別）

企業群別に見ても、全ての項目においてIT活用度の高い企業の導入率が上回っている。

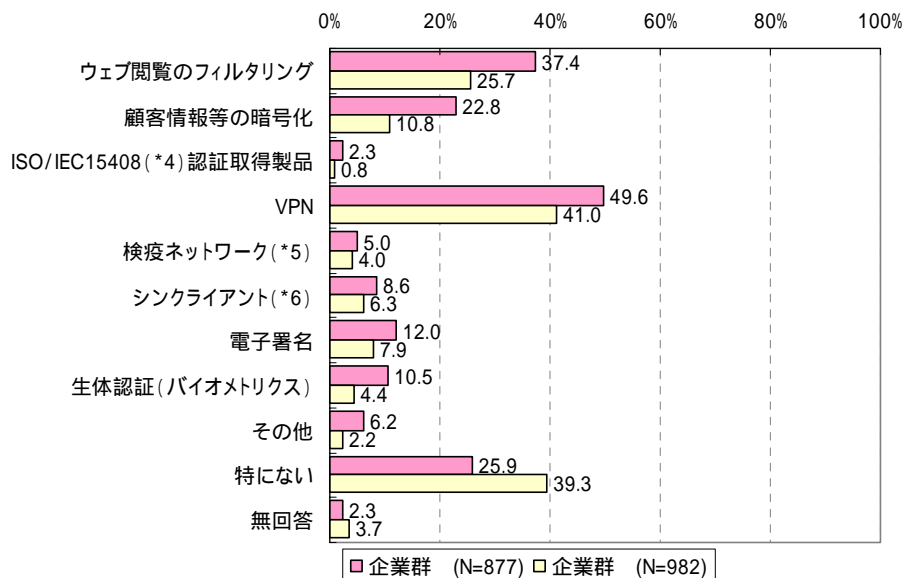


図 2.2-26 情報セキュリティ関連製品やソリューションの導入（企業群別）

### 2.2.6.情報セキュリティ被害防止のための組織・運用面の対策

情報セキュリティ被害防止のための組織・運用面での対策は、「重要なシステム・データのバックアップ」が76.9%で最も多く、「ID・パスワード、アクセス権限管理の強化」(64.9%)、「ハードディスク等の廃棄時の破壊」(61.3%)が続く。

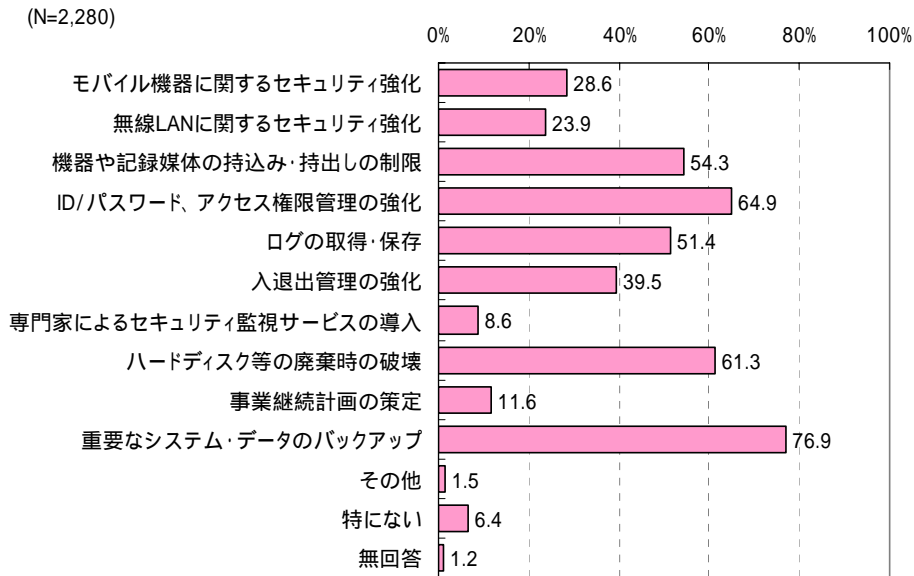


図 2.2-27 情報セキュリティ被害防止のための組織・運用面の対策

企業/自治体別に見ると、多くの項目について自治体の方が対策状況が進展している。ただし、「モバイル機器に関するセキュリティ強化」では、企業の方が約20ポイント対策率が高いことが特徴的である。

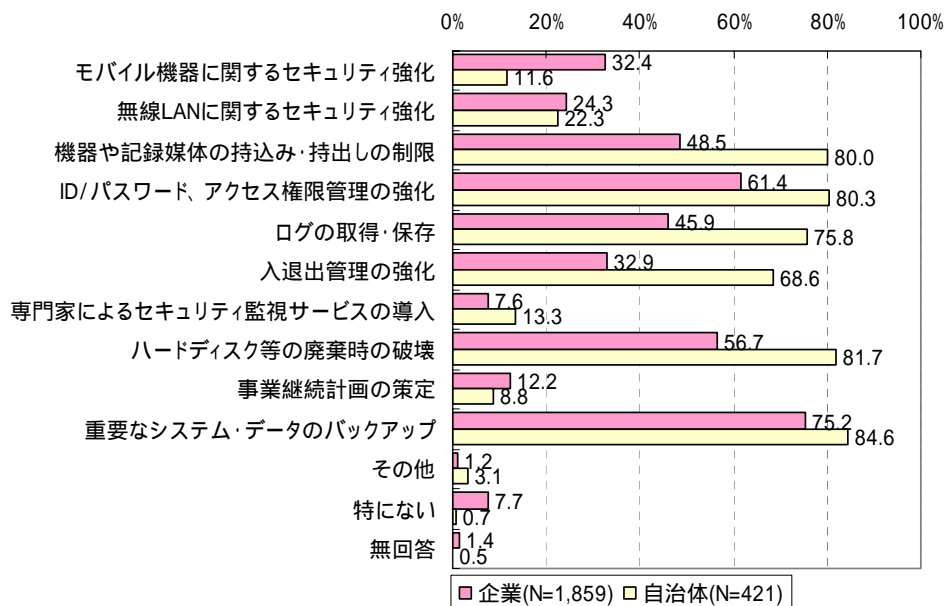


図 2.2-28 情報セキュリティ被害防止のための組織・運用面の対策（企業/自治体別）

就業者規模別に見ると、300人以上企業の方がいずれの項目においても対策状況が進展している。

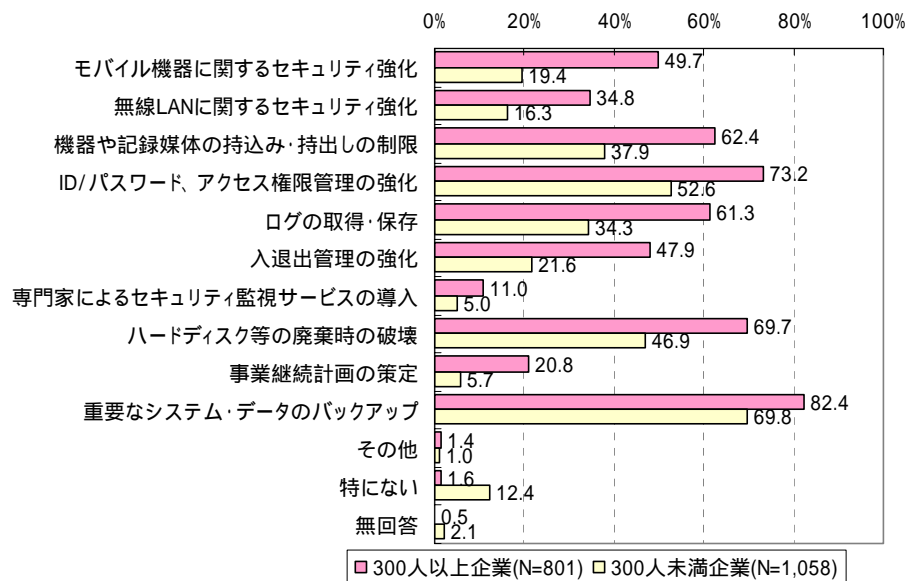


図 2.2-29 情報セキュリティ被害防止のための組織・運用面の対策（就業者規模別）

企業群別に見ると、企業群の方が対策状況が進展している傾向にある。

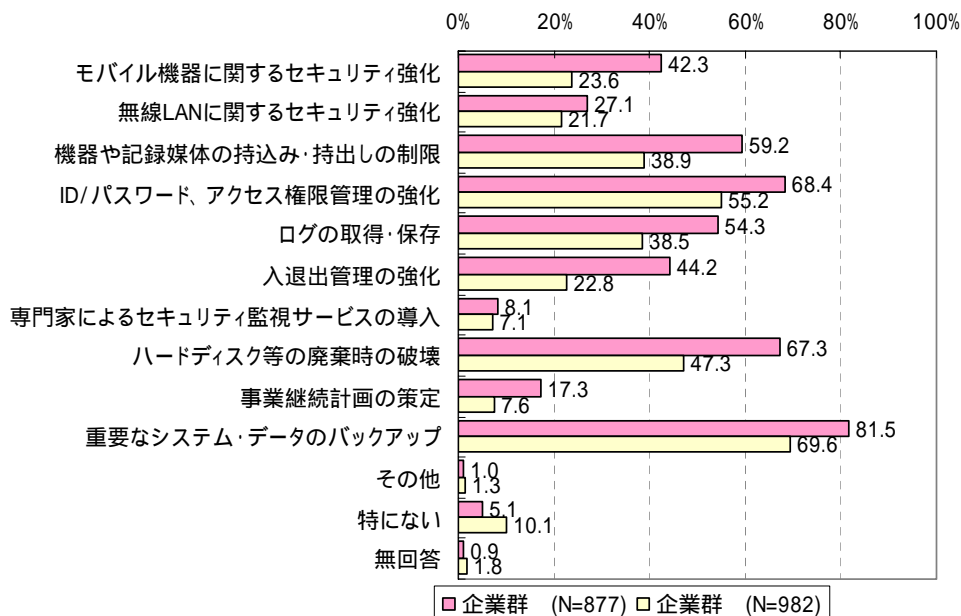


図 2.2-30 情報セキュリティ被害防止のための組織・運用面の対策（企業群別）

### 2.2.7. セキュリティパッチの適用

セキュリティパッチの適用について、「常に適用し、適用状況も把握している」のは、ネットワークサーバ(44.2%)、ローカルサーバ(38.2%)が約4割だが、クライアントパソコンでは33.8%と最も低い。クライアントパソコンでは、「常に適用する方針・設定だが、実際の適用状況は不明」(29.3%)が他の機器よりも高く、管理状況を把握するのが困難であることが示されている。

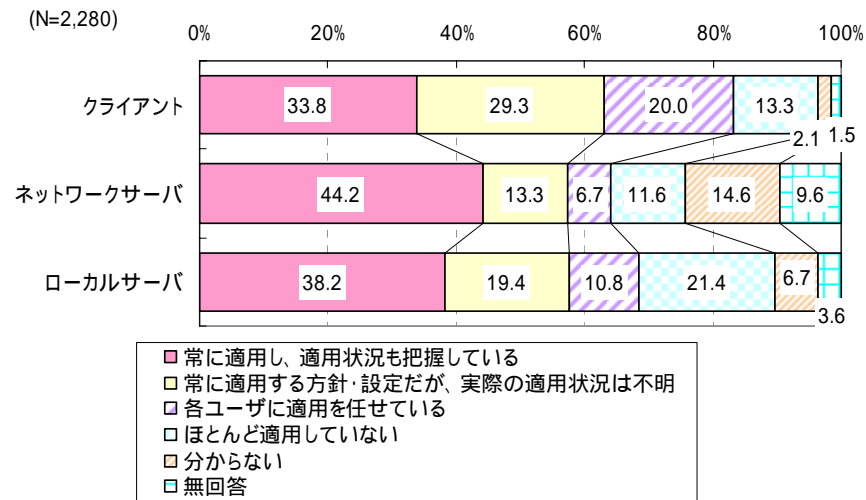
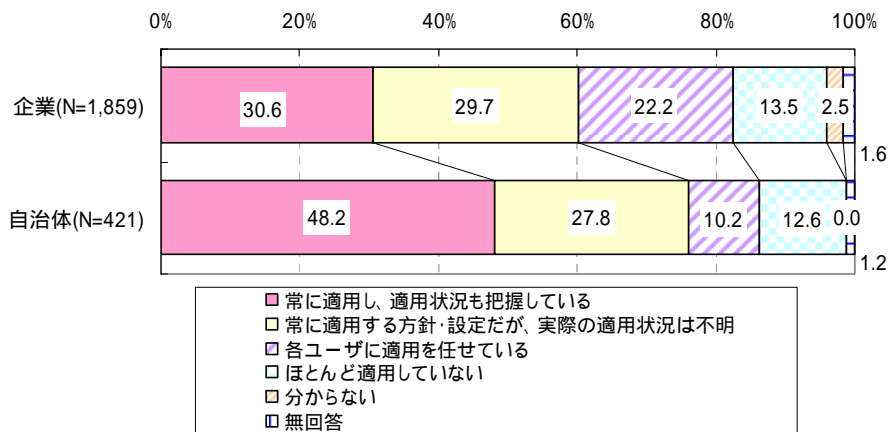
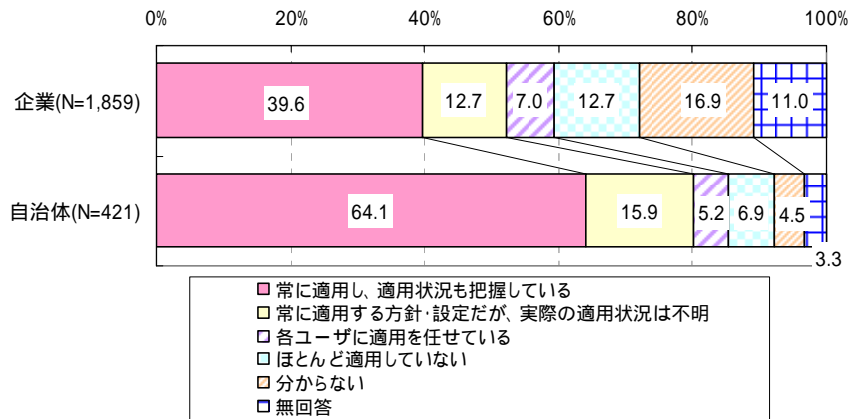


図 2.2-31 セキュリティパッチの適用

#### <クライアント>



< ネットワークサーバ >



< ローカルサーバ >

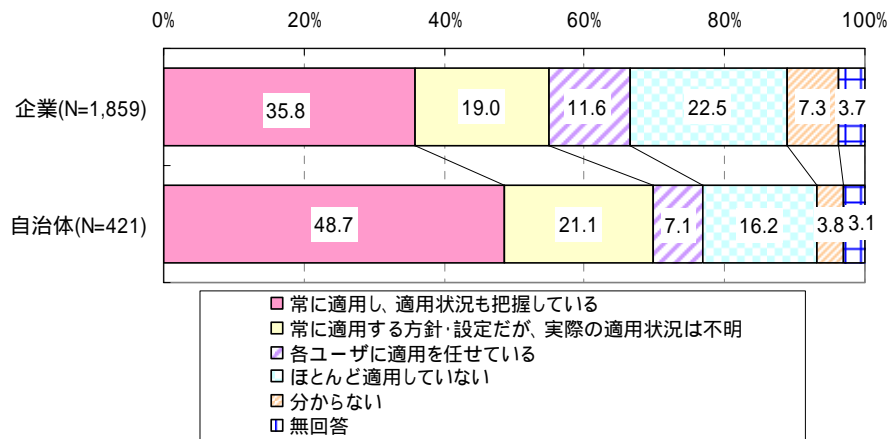
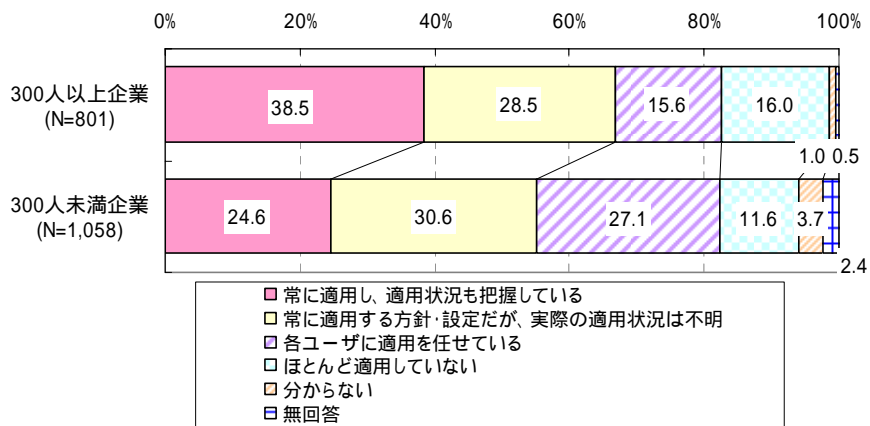
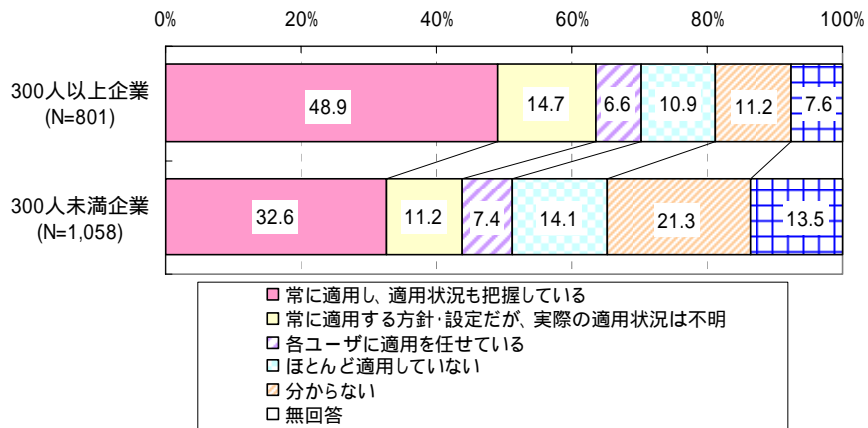


図 2.2-32 セキュリティパッチの適用（企業／自治体別）

< クライアント >



< ネットワークサーバ >



< ローカルサーバ >

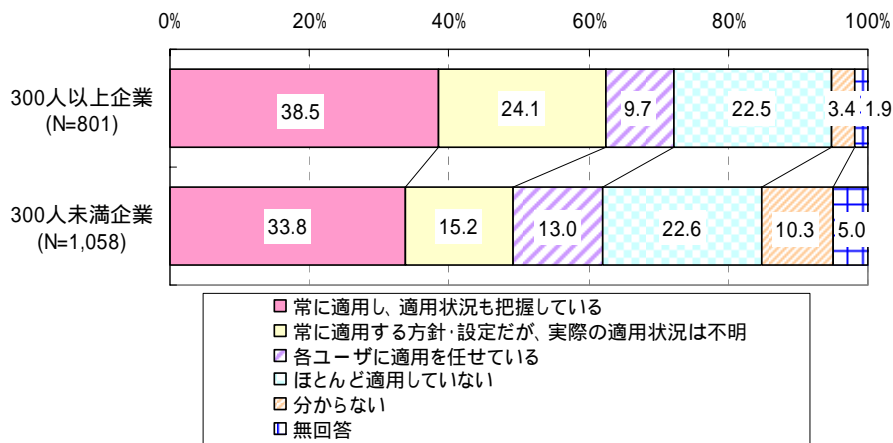


図 2.2-33 セキュリティパッチの適用（就業者規模別）

2.2.8. セキュリティパッチを導入しなかった理由

セキュリティパッチを導入しなかった理由は「既存のシステム/サービスの動作を重視し、パッチの適用により生じる悪影響や改修作業を避けた」が37.2%で最も多い。

(N=2,280)

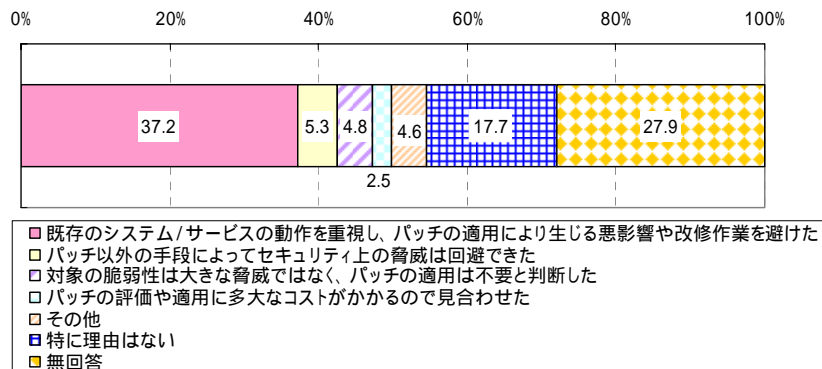


図 2.2-34 セキュリティパッチを導入しなかった理由

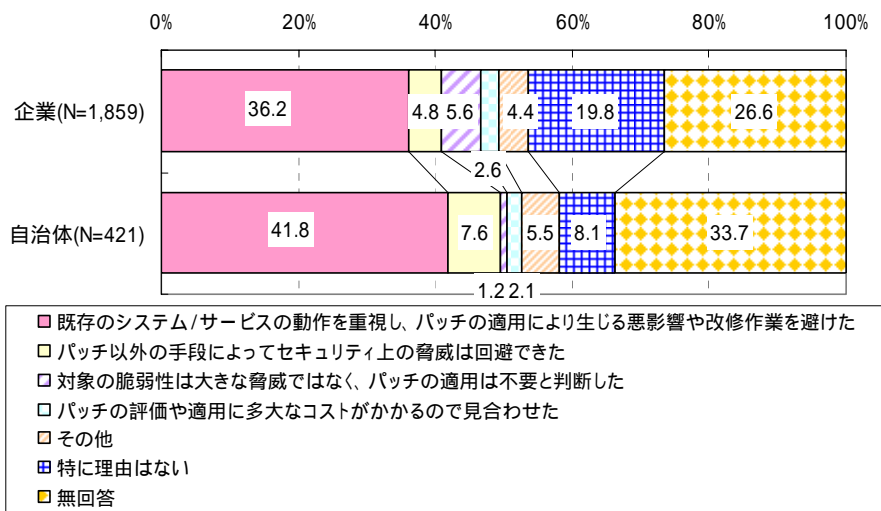


図 2.2-35 セキュリティパッチを導入しなかった理由（企業 / 自治体別）

就業者規模別では、「既存のシステム / サービスの動作を重視し、パッチの適用により生じる悪影響や改修作業を避けた」について 300 人以上企業の方が約 20 ポイント高く、300 人未満企業では、半数が「特に理由はない」もしくは「無回答」である。

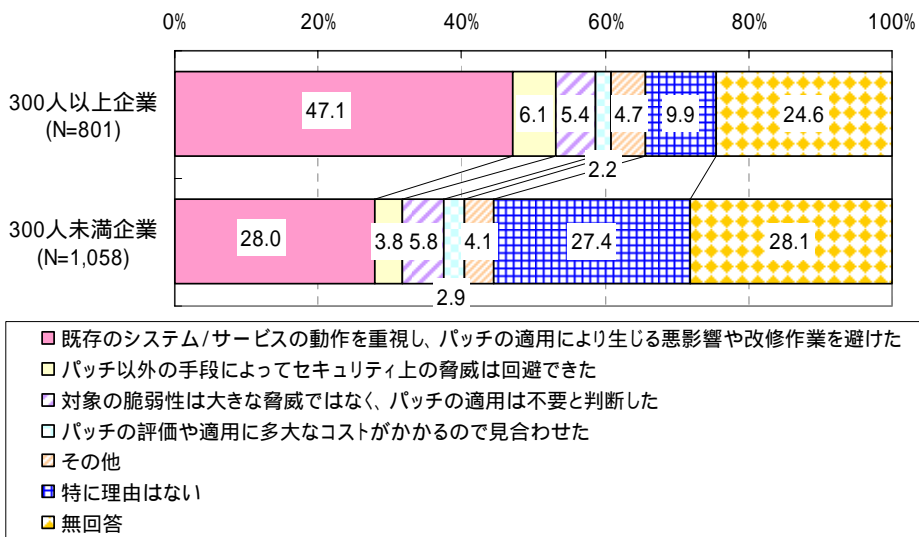


図 2.2-36 セキュリティパッチを導入しなかった理由（就業者規模別）

### 2.2.9. Windows 98 / Me がインストールされているパソコンの割合

Windows98/Me がインストールされている PC を保有するのは約 3 割である。

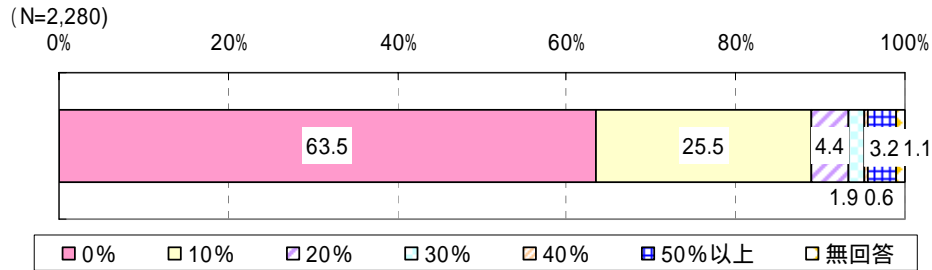


図 2.2-37 Windows 98 / Me がインストールされているパソコンの割合

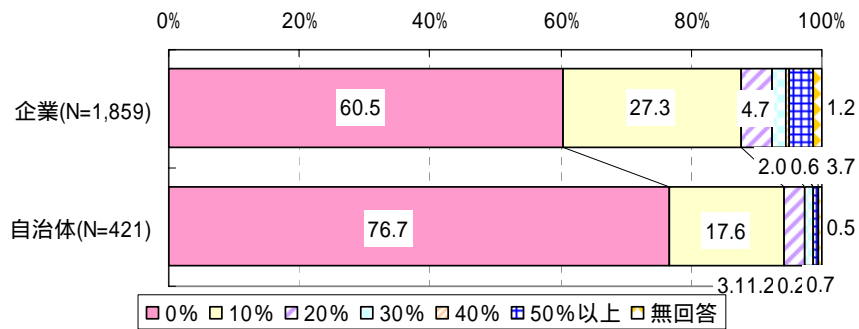


図 2.2-38 Windows 98 / Me がインストールされているパソコンの割合（企業 / 自治体別）

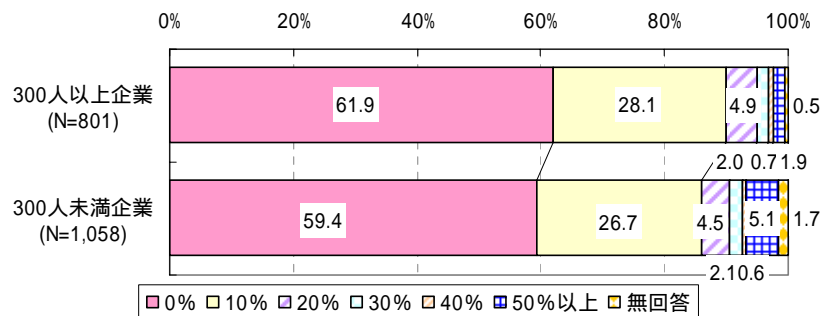


図 2.2-39 Windows 98 / Me がインストールされているパソコンの割合（就業者規模別）

### 2.2.10. 情報セキュリティ対策教育の実施状況

情報セキュリティ対策教育の実施率は、「正社員・正職員」が最も高く7割を超える。いずれの職種においても企業より自治体の方がセキュリティ対策教育の実施率が高いが、準社員・準職員・アルバイトにおける「eラーニング」の実施率は自治体より企業の方が高い。

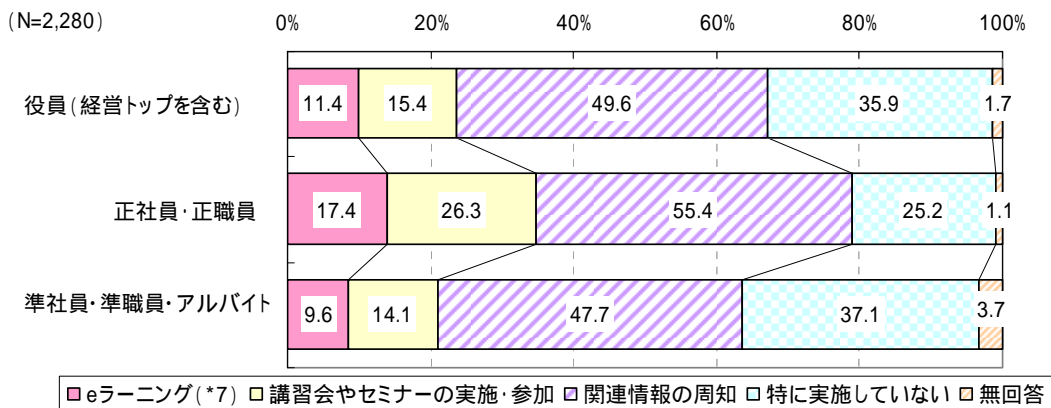
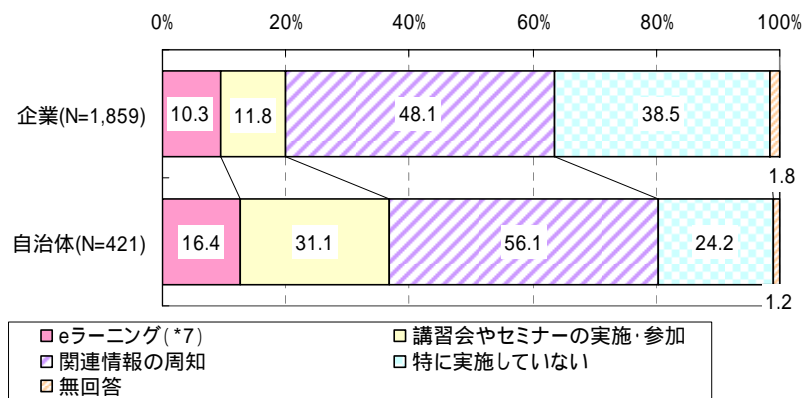
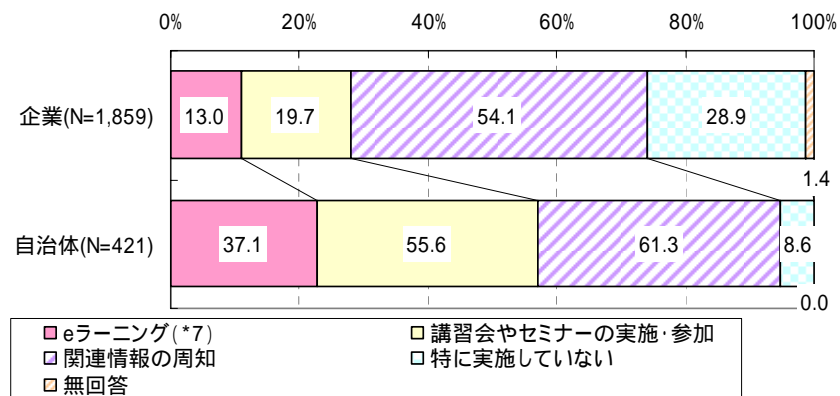


図 2.2-40 情報セキュリティ対策教育の実施状況

< 役員 >



< 正社員・正職員 >



< 準社員・準職員・アルバイト >

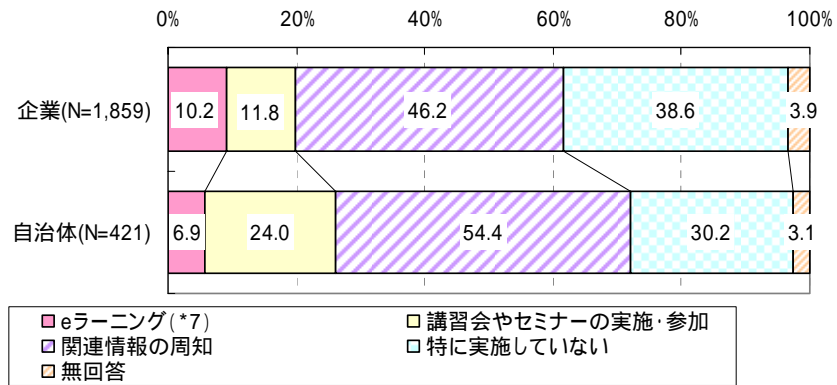
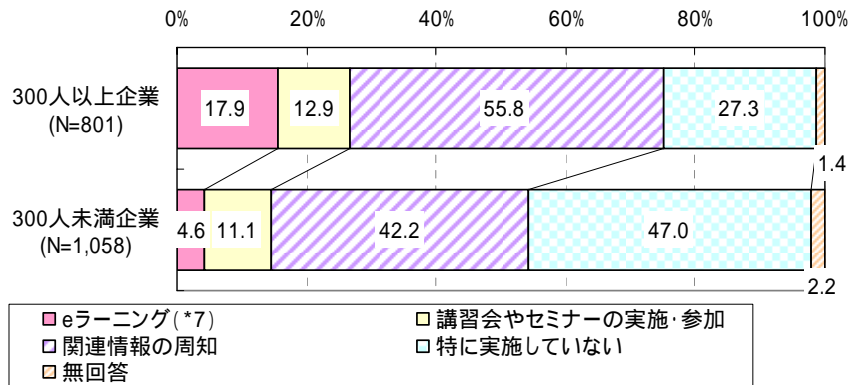


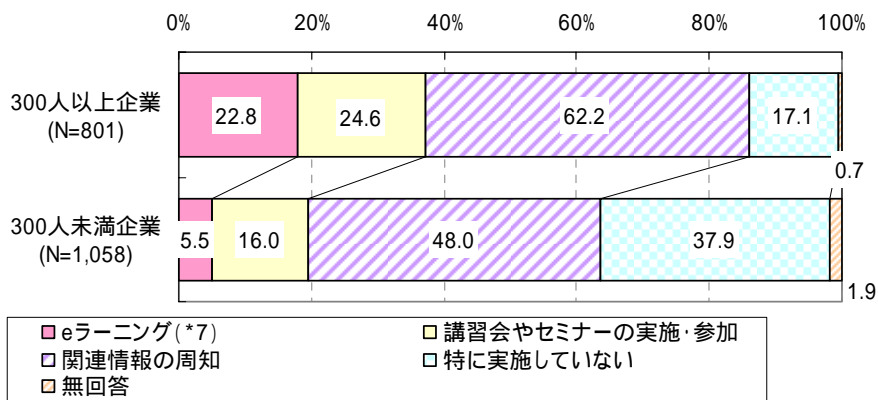
図 2.2-41 情報セキュリティ対策教育の実施状況（企業／自治体別）

就業者規模別に見ても、300人未満企業より300人以上企業の方がセキュリティ対策教育の実施率が高い。

< 役員 >



< 正社員・正職員 >



< 準社員・準職員・アルバイト >

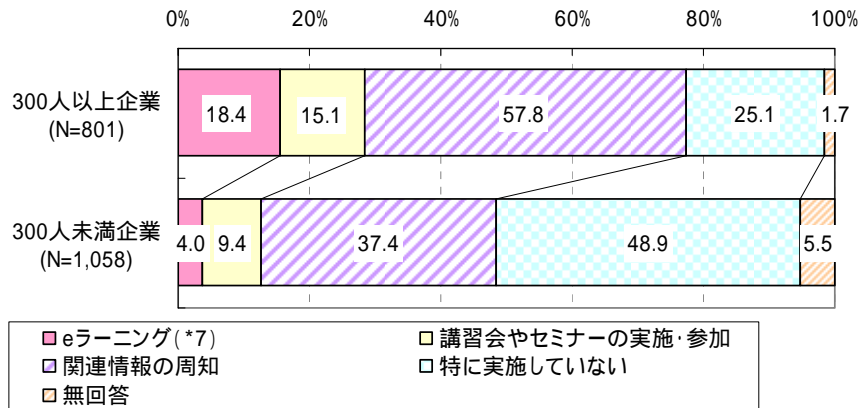


図 2.2-42 情報セキュリティ対策教育の実施状況 (就業者規模別)

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

コンピュータウイルスに関連して知りたいと思う情報は「情報漏えいが発生した場合の対処方法」が 45.1%、「不正アクセスを受けた際の対処方法」が 43.8%で、この 2 項目が 4 割を超える。その他、「情報セキュリティ対策の導入・運用に関する基準やガイドライン」( 39.3%)、「他社における各種情報セキュリティ対策の導入状況」( 38.8%)、「ウイルス感染時の復旧方法」( 38.7%)、「新種ウイルス、要注意ウイルスの警戒情報」( 34.4%) が 3 割を超えている。

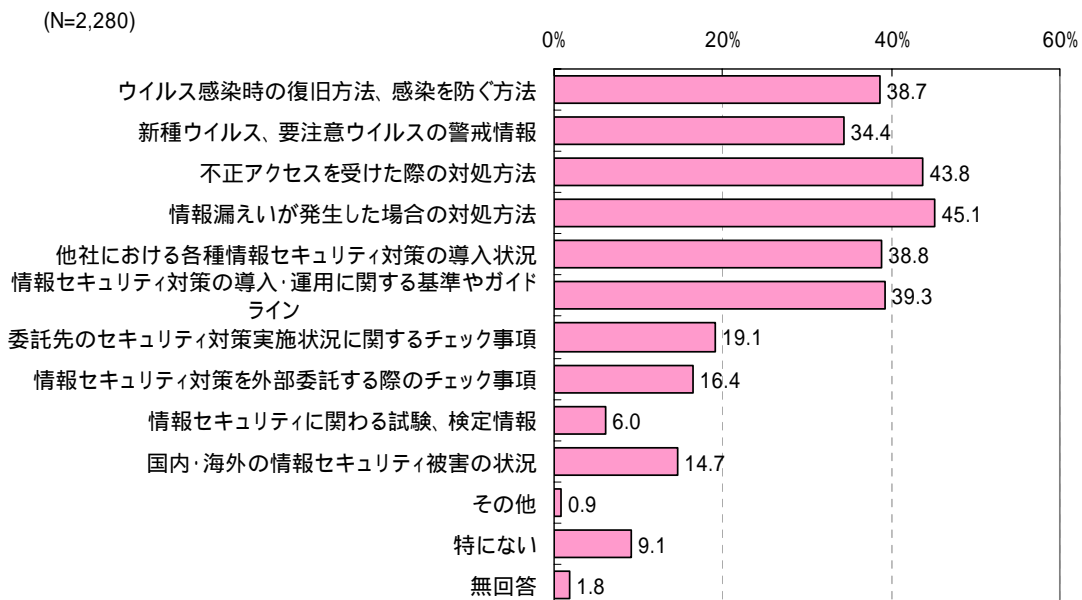


図 2.3-1 コンピュータウイルスに関連して知りたいと思っている情報

企業 / 自治体の比較では、自治体の方が多くの項目において回答率が高い傾向にある。ただし、「他社における各種情報セキュリティ対策の導入状況」や「情報セキュリティ対策の導入・運用

に関する基準やガイドライン」等、日常的な情報セキュリティ対策方法に関する情報については、企業・自治体とも知りたいと思う率が同程度である。また、300人未満企業の方が、ウイルス感染・不正アクセス・情報漏えい発生時等の対処方法を知りたいと思い、300人以上企業の方が日常的な対策方法について知りたいと思う傾向にある。

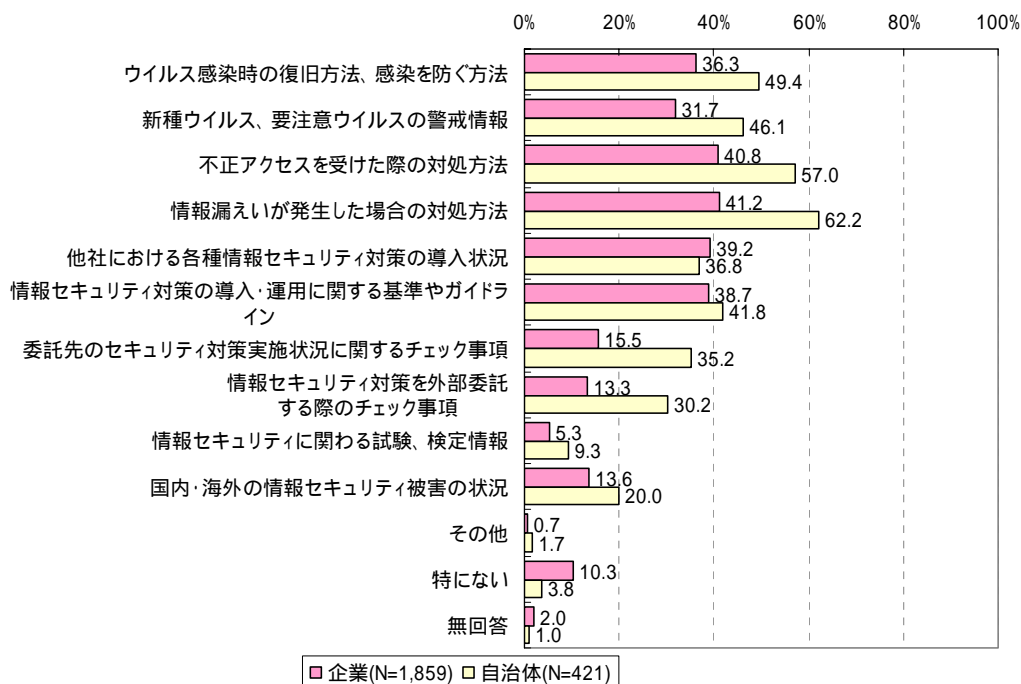


図 2.3-2 コンピュータウイルスに関連して知りたいと思っている情報（企業／自治体別）

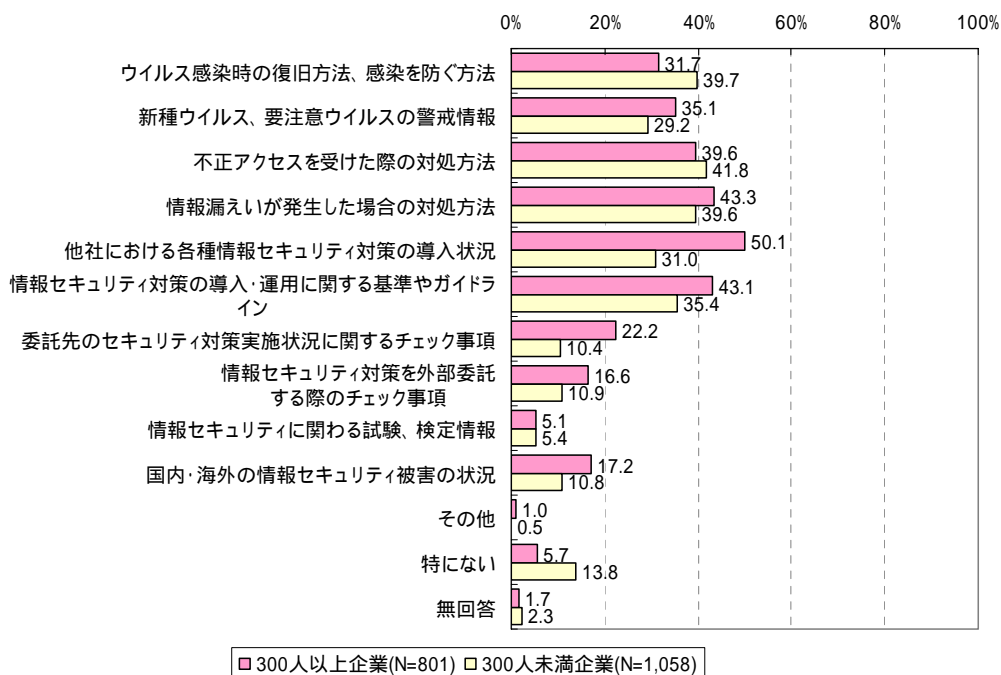


図 2.3-3 コンピュータウイルスに関連して知りたいと思っている情報（就業者規模別）

### 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」の認知度は6割強に達するが、うち半数は「存在を知っている」に留まり、内容を理解しているのは1割にも満たない。

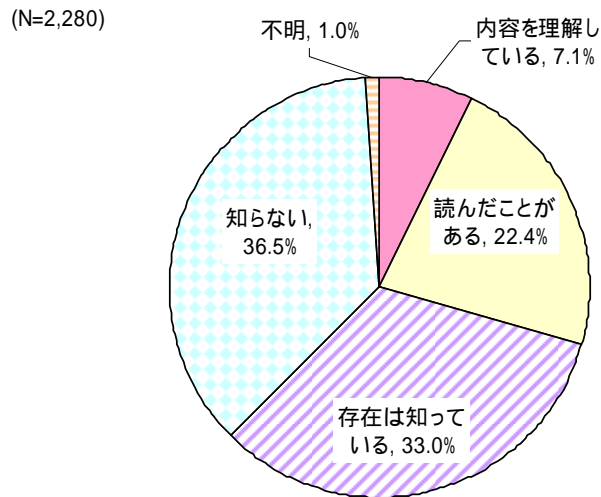


図 2.3-4 「コンピュータウイルス対策基準」の認知度

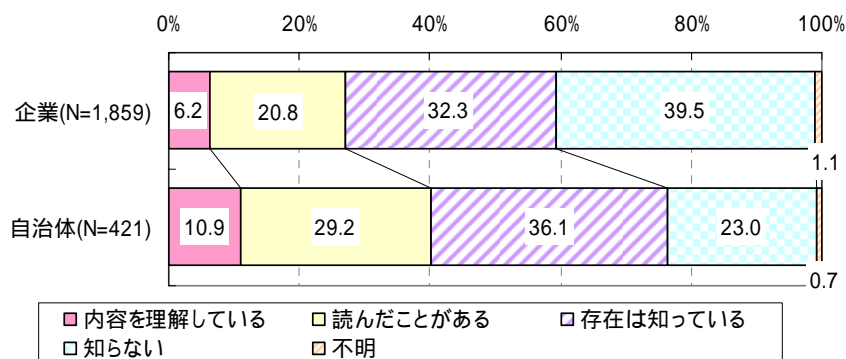


図 2.3-5 「コンピュータウイルス対策基準」の認知度（企業/自治体別）

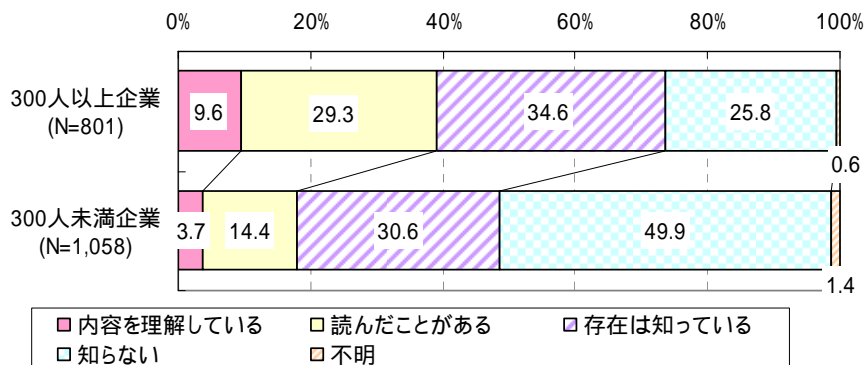


図 2.3-6 「コンピュータウイルス対策基準」の認知度（就業者規模別）

### 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

被害届出機関としてのIPAを認知しているのは約半数である。企業より自治体の方が約12ポイント、300人未満企業より300人以上企業の方が約29ポイント「知っている」との回答が多い。

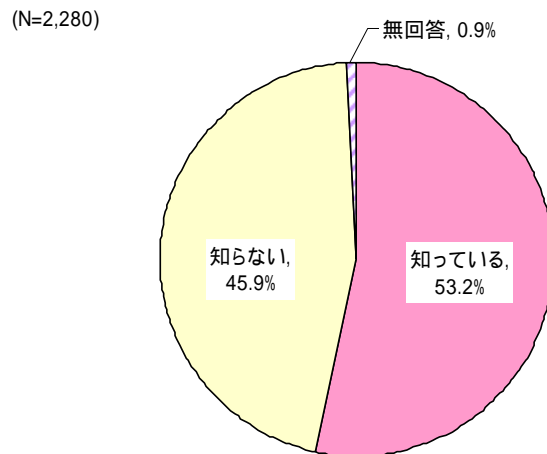


図 2.3-7 届出機関としてのIPA の認知度

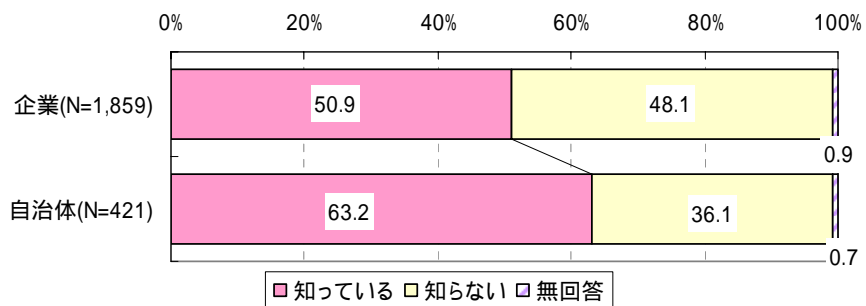


図 2.3-8 届出機関としてのIPA の認知度（企業 / 自治体別）

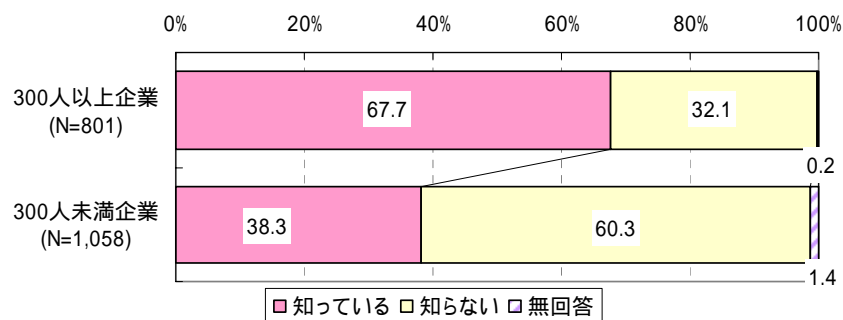


図 2.3-9 届出機関としてのIPA の認知度（就業者規模別）

(2)届出の実施

感染が発見された際、実際に届出を行うと回答したのは3割に留まる。企業より自治体の方が届出を行うとする回答が18ポイント高いが、企業における就業者規模による違いはほとんど無い。

(N=2,280)

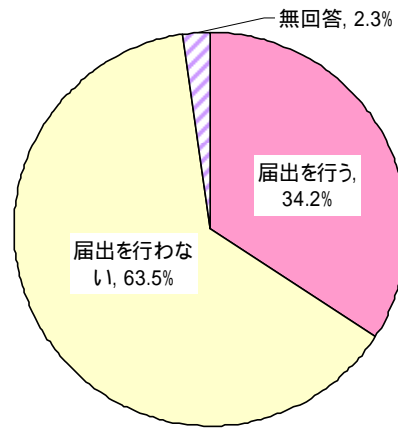


図 2.3-10 届出の実施

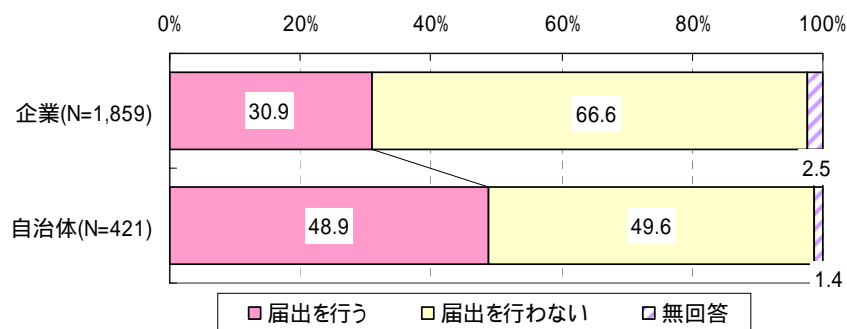


図 2.3-11 届出の実施（企業／自治体別）

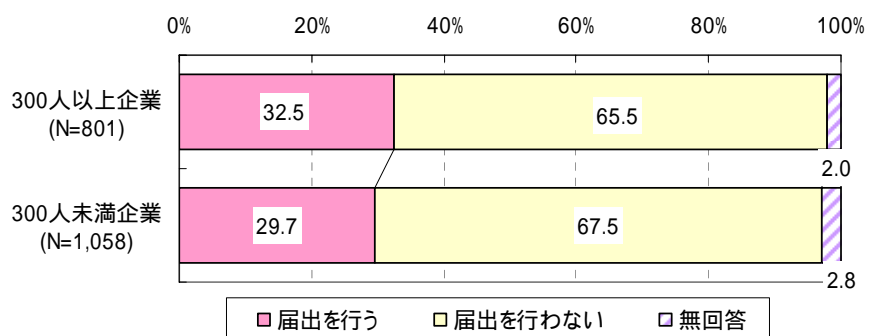


図 2.3-12 届出の実施（就業者規模別）

### (3)届け出を行わない理由

届け出を行わない理由は「被害が大きければ届出する」が47.2%で最も大きく、次いで「届け出方法が不明なため」が37.9%で続く。企業では、自治体と比較して「届出方法が不明なため」が約10ポイント、「届出に手間がかかる」が約9ポイント高い一方、自治体では、企業と比較して「被害が大きければ届出する」が約11ポイント高く、自治体は届出制度の問題で届出を行わないのではなく、被害の大きさに届出の実施を判断していると言える。また、就業者規模別で見ると、300人未満企業では「届出方法が不明なため」(45.5%)が300人以上企業より約14ポイント高く、規模の小さな企業に対しては届出方法の周知が不足していると考えられる。

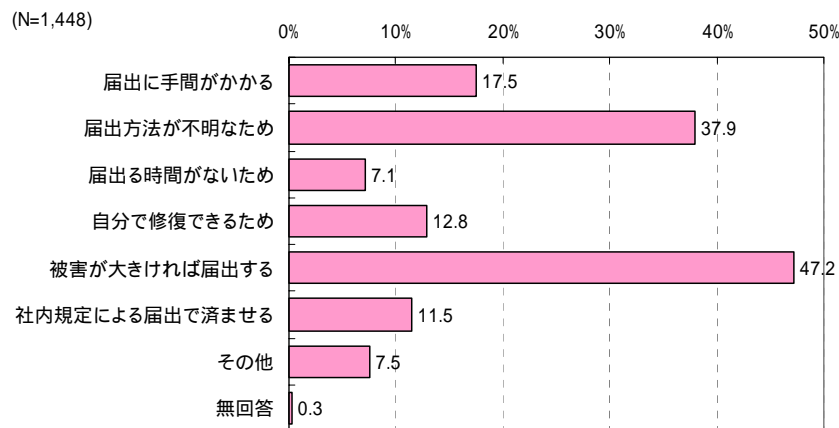


図 2.3-13 届出を行わない理由

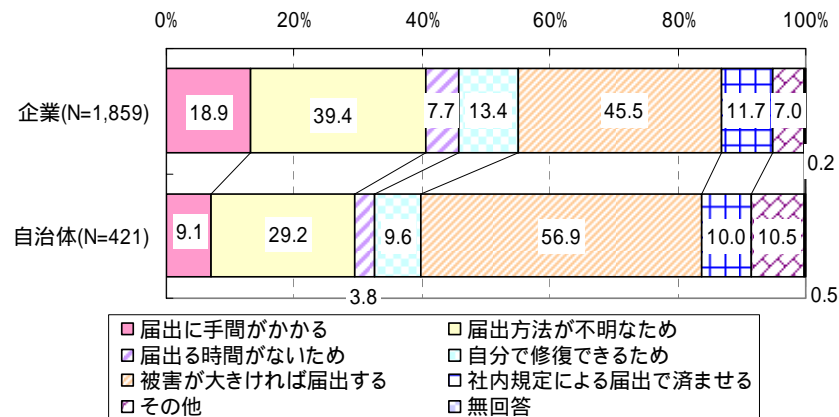


図 2.3-14 届出を行わない理由（企業／自治体別）

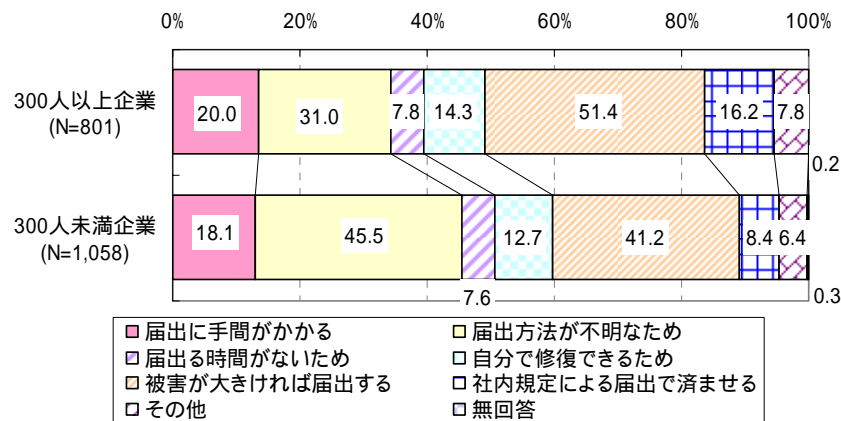


図 2.3-15 届出を行わない理由（就業者規模別）

## 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

コンピュータウイルスに感染したのは約 1 割であり、4 割が遭遇（感染も発見も）していない。企業 / 自治体別に見ると、企業より自治体の方が遭遇率が低く、「ウイルスを発見したが、感染には至らなかった」は約 15 ポイント高い。さらに、感染率（ウイルスに遭遇したうち、実際に感染した比率）は、企業より自治体の方が 7 ポイント低い。

就業者規模別では、300 人以上企業の遭遇率が約 7 割に達するのに対し、300 人未満企業の遭遇率は 5 割にも満たず、感染率も 300 人以上企業の方が約 12 ポイント高い。

企業群別では、企業群 の遭遇率が企業群 よりも約 10 ポイント高いが、感染率はほぼ同じである。

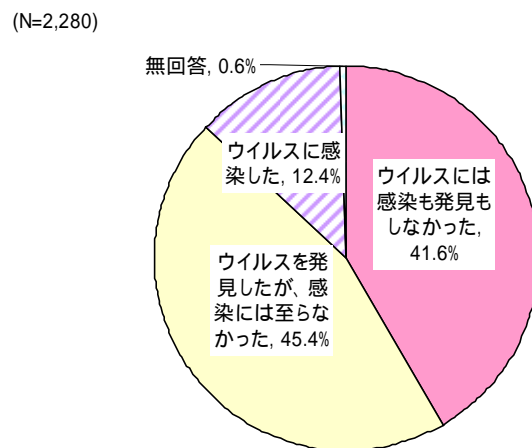


図 2.4-1 コンピュータウイルス遭遇（感染または発見）経験

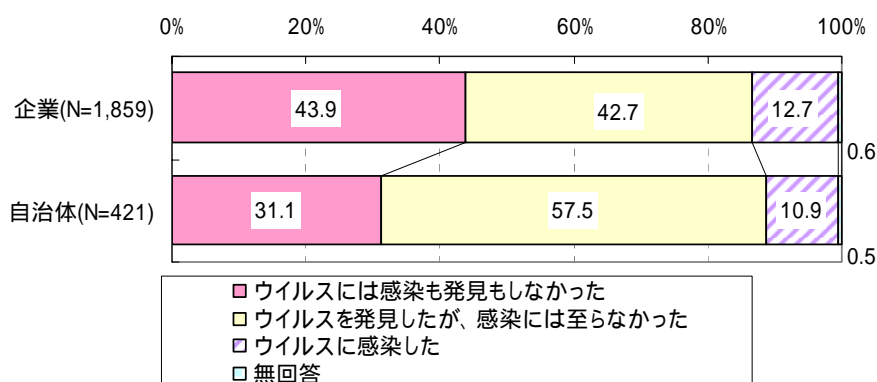


図 2.4-2 コンピュータウイルス遭遇（感染または発見）経験（企業／自治体別）

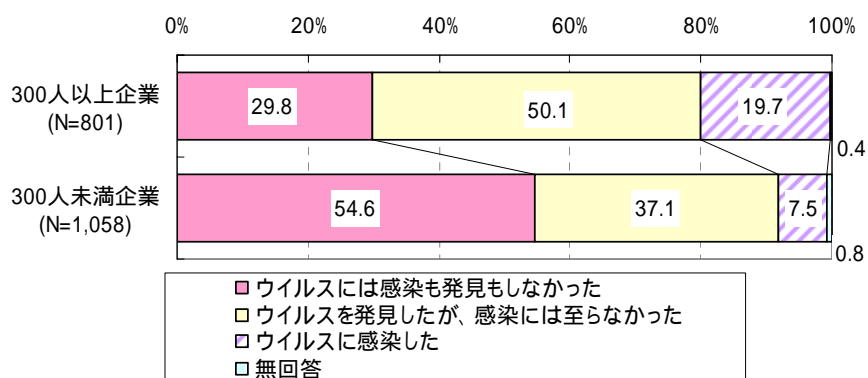


図 2.4-3 コンピュータウイルス遭遇（感染または発見）経験（就業者規模別）

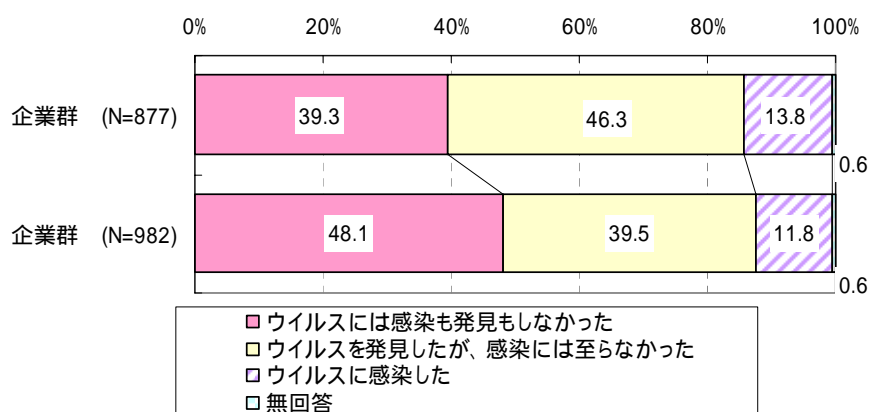


図 2.4-4 コンピュータウイルス遭遇（感染または発見）経験（企業群別）

表 2.4-1 感染率（ウイルスに遭遇したうち、実際に感染した比率）

| 全体    | 企業    | 自治体   | 300人以上<br>企業 | 300人未満<br>企業 | 企業群   | 企業群   |
|-------|-------|-------|--------------|--------------|-------|-------|
| 21.5% | 23.0% | 16.0% | 28.3%        | 16.7%        | 23.0% | 23.0% |

時系列でみると、ウイルスの遭遇率は2002年をピークとし、2003～2005年では横ばいを続けたが、2006年、2007年と連続して減少している。

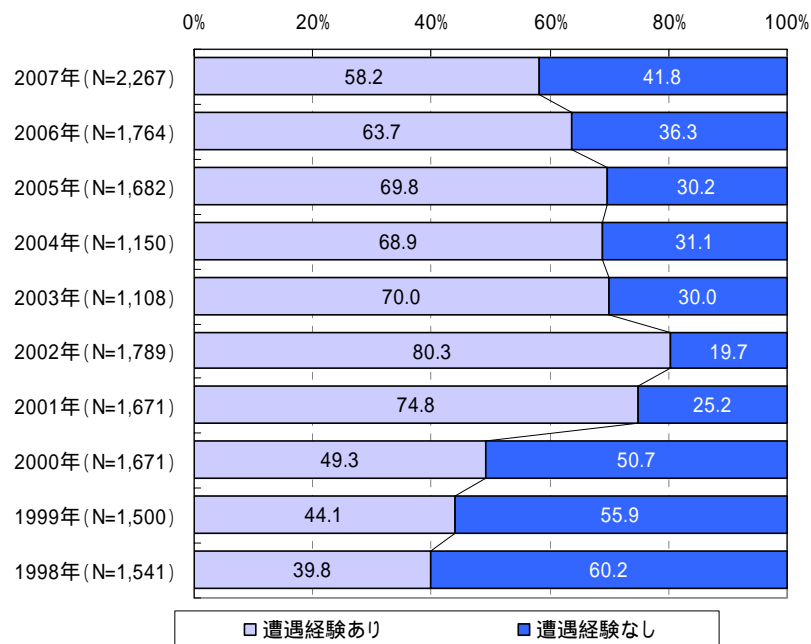


図 2.4-5 コンピュータウイルス遭遇（感染または発見）経験（時系列）

注1)「遭遇経験あり」とは、「感染した」と「ウイルスを発見したが、感染には至らなかった」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、2006年の値を再集計しており、前頁および前図の比率と異なる。

### 2.4.2. 感染・発見したウイルスの名称

感染したウイルスは「W32/Netsky」が最も多く 20.5%である。また、「W32/Bagle」「W32/Mytob」「W32/Klez」「W32/Mydoom」「W32/Stration」は約 7~8%が感染している。一方、「その他」も半数近くに達しているが、特に「トロイの木馬」(131件)、「受動型攻撃コード」(58件)、「マクロウイルス」(21件)等の記載が多い。

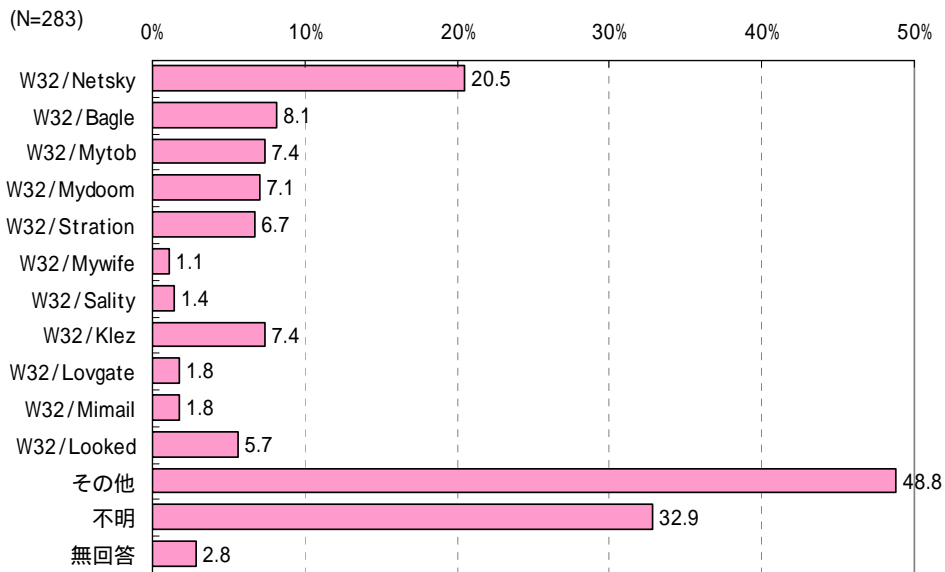


図 2.4-6 感染したウイルスの名称

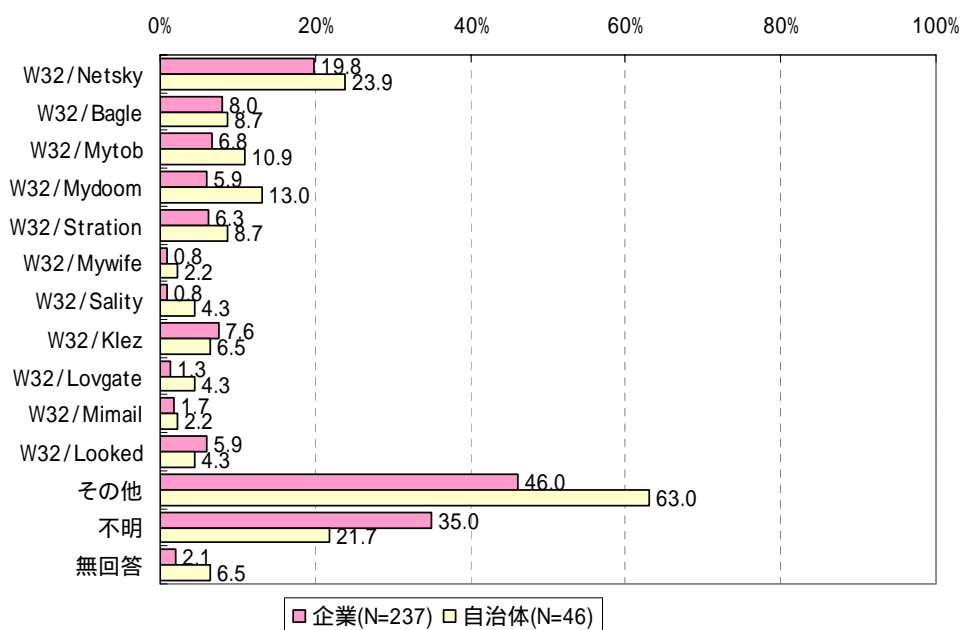


図 2.4-7 感染したウイルスの名称 (企業 / 自治体別)

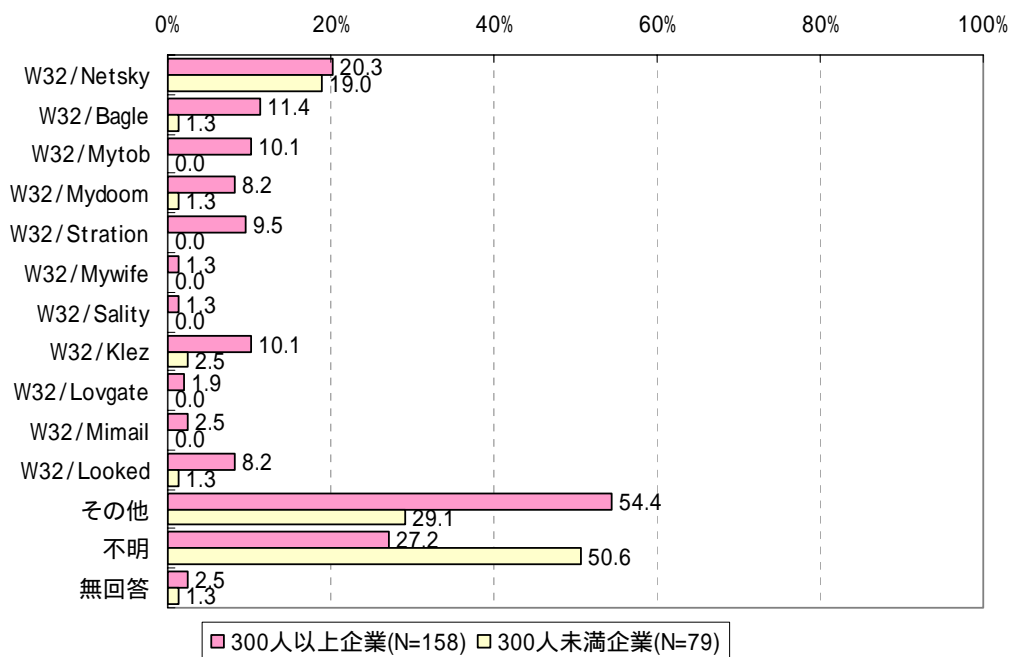


図 2.4-8 感染したウイルスの名称（就業者規模別）

また、発見のみのウイルスも「W32/Netsky」が最も多く 31.8%である。また、「W32/Klez」「W32/Mydoom」は、10%以上が発見している。

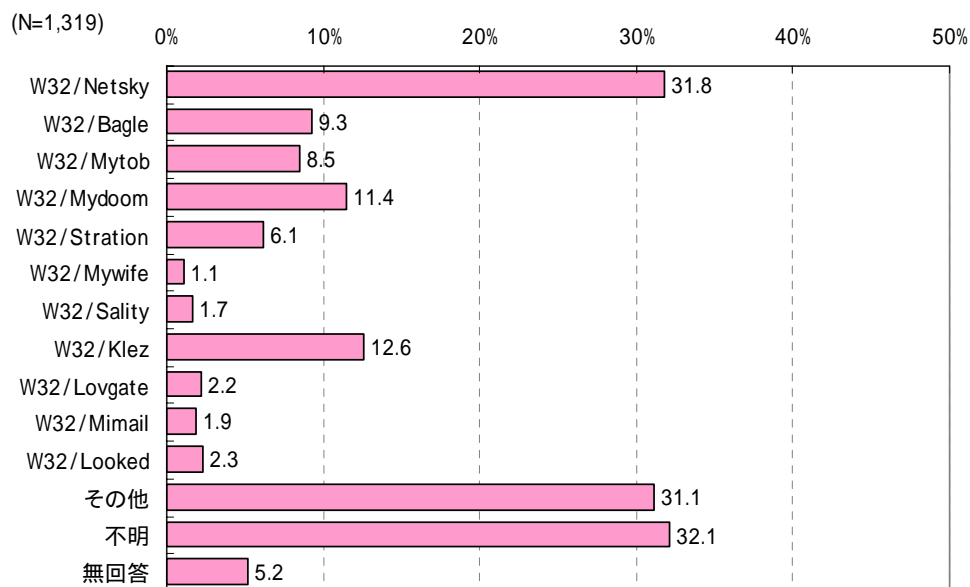


図 2.4-9 発見したウイルスの名称

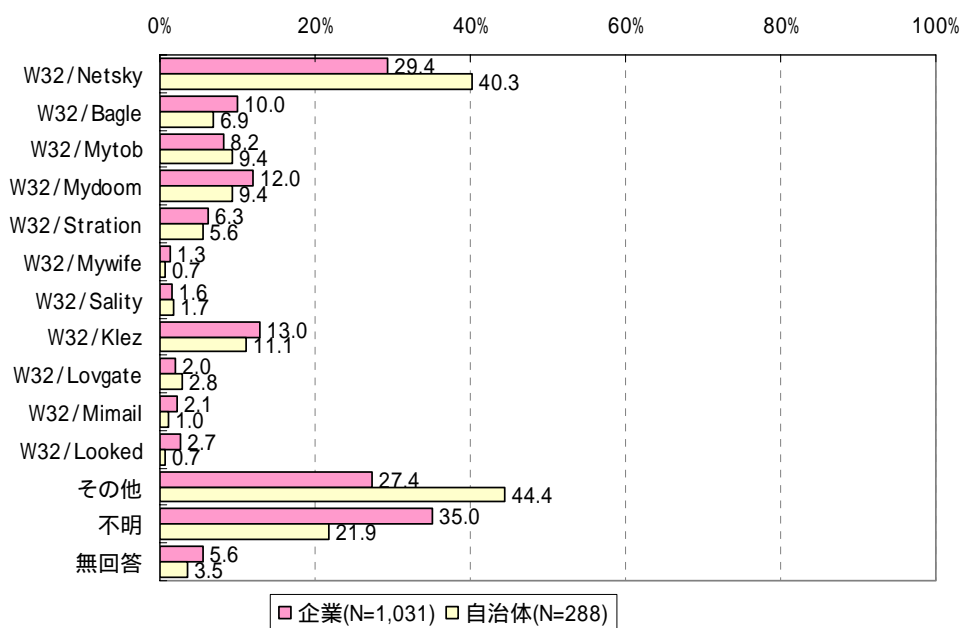


図 2.4-10 発見したウイルスの名称（企業 / 自治体別）

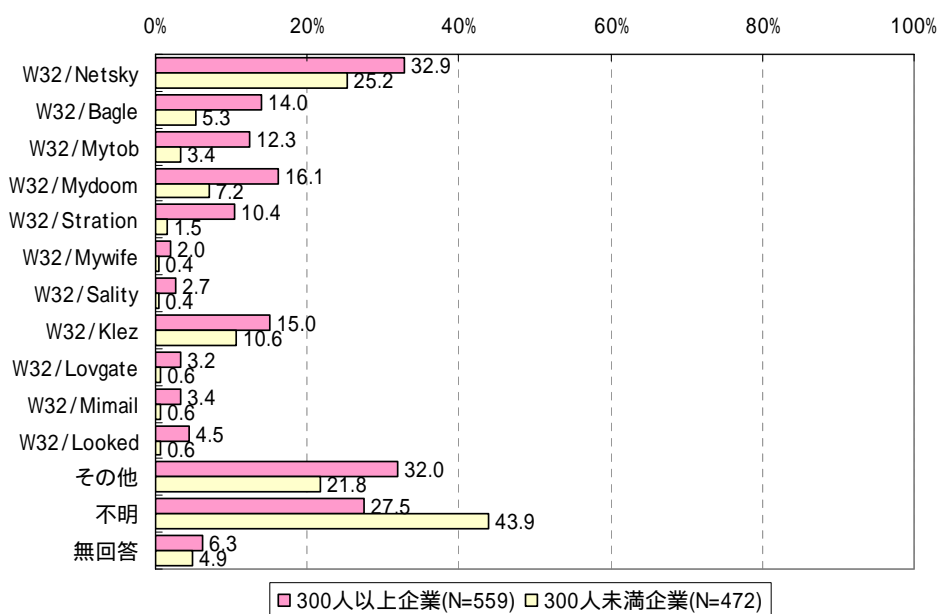


図 2.4-11 発見したウイルスの名称（就業者規模別）

### 2.4.3. ウイルスの感染件数

ウイルスの感染件数は「1件」が最も多く 36.7%であるが、「5件以上」も 30.0%ある。

企業/自治体別でみると、自治体は「1件」が半数を超え、企業より感染件数が少ない傾向にある。また、就業者規模別では、300人以上企業は 39.9%が「5件以上」であるが、300人未満企業は「1件」が 44.3%であり、感染件数は企業規模に応じて増えると言える。さらに、企業群では、「5件以上」の回答は、IT活用度の高い企業群の方が企業群より約 15ポイント高い。

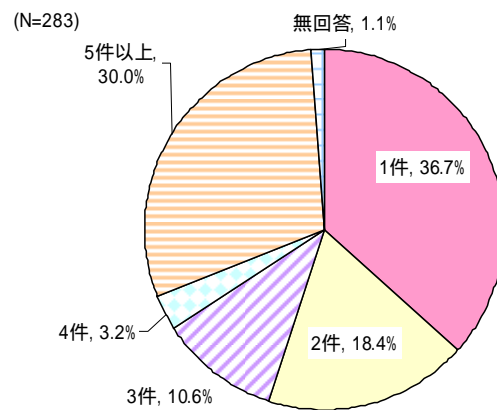


図 2.4-12 ウイルスの感染件数

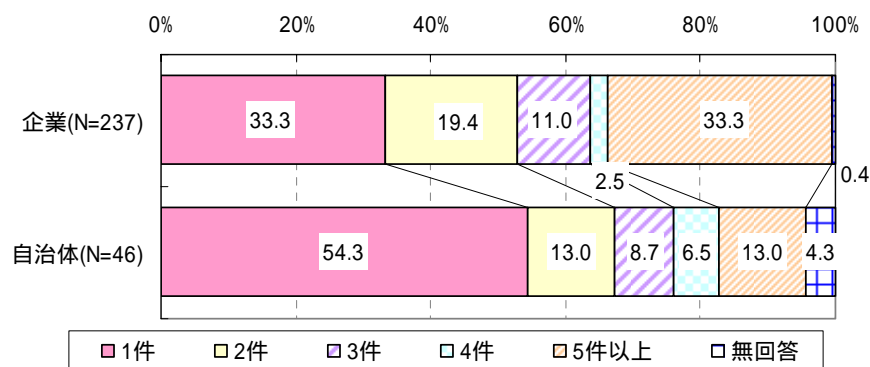


図 2.4-13 ウイルスの感染件数 (企業/自治体別)

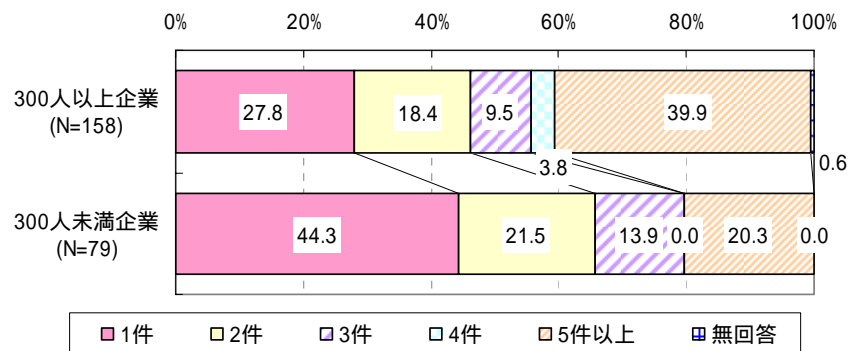


図 2.4-14 ウイルスの感染件数（就業者規模別）

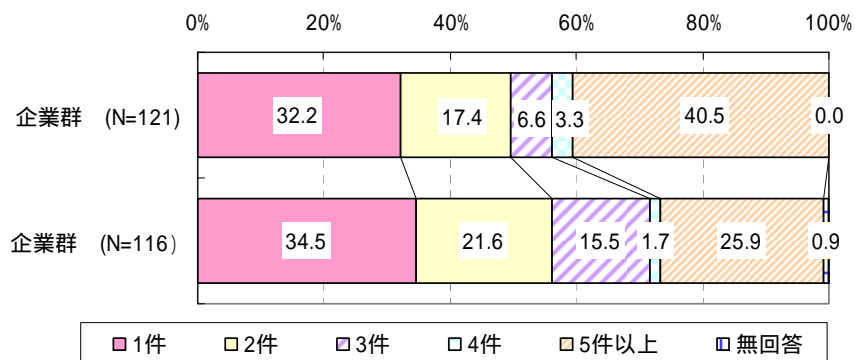


図 2.4-15 ウイルスの感染件数（企業群別）

#### 2.4.4. ウイルスに感染したパソコン・サーバの台数

ウイルスに感染したパソコンは「1～4台が」46.3%、サーバは「0台」が71.0%である。

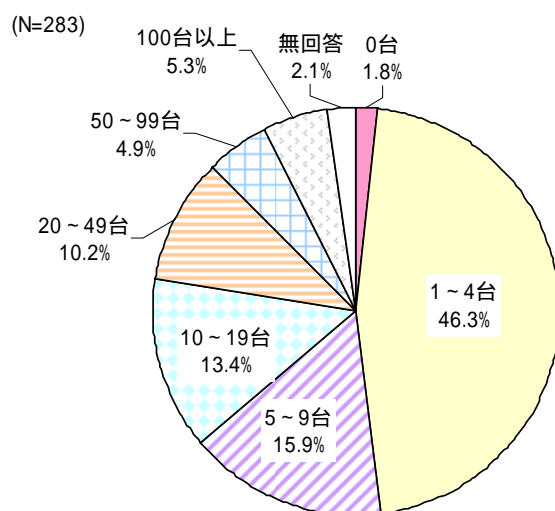


図 2.4-16 ウイルスに感染したパソコンの台数

企業 / 自治体別では、「1～4台」の回答は自治体の方が約 23 ポイント高いなど、自治体の方が感染台数が少ない傾向にある。

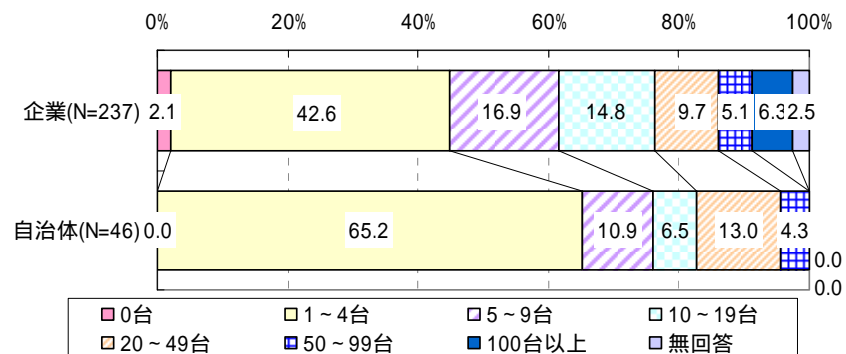


図 2.4-17 ウイルスに感染したパソコンの台数（企業 / 自治体別）

300 人未満企業の 7 割近くの感染パソコン台数は「1～4台」である。

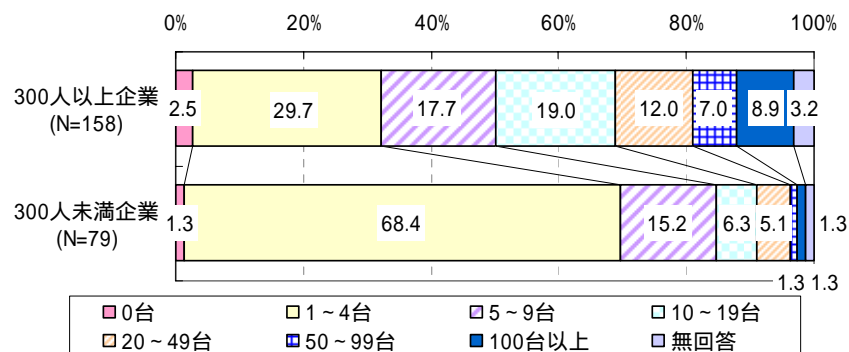


図 2.4-18 ウイルスに感染したパソコンの台数（就業者規模別）

感染サーバ台数は「0台」が7割を超える。企業 / 自治体別では、パソコンと同様、自治体の感染台数が少ない傾向にあるが、300人未満企業では300人以上企業に対して「0台」が約6ポイント少ないのに加え、「1～4台」が300人以上企業より約9ポイント高く、規模が小さな企業ではサーバ自体が感染するケースが多いことが考えられる。

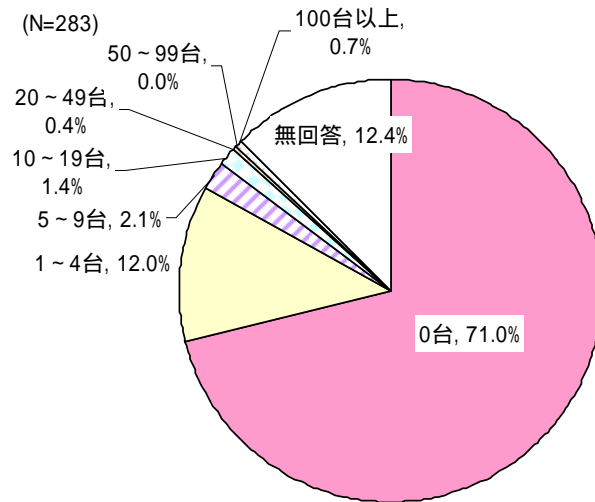


図 2.4-19 ウイルスに感染したサーバの台数

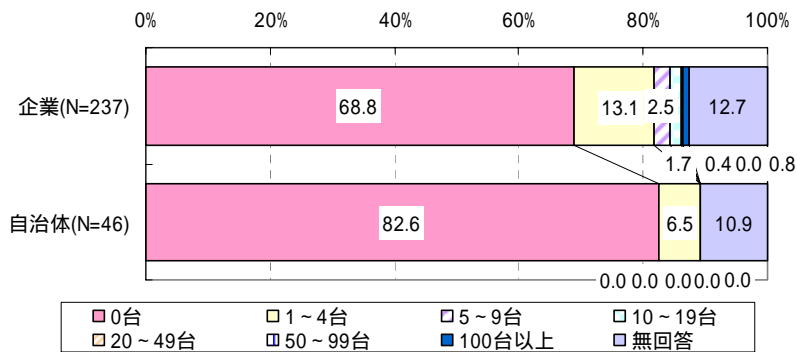


図 2.4-20 ウイルスに感染したサーバの台数 (企業/自治体別)

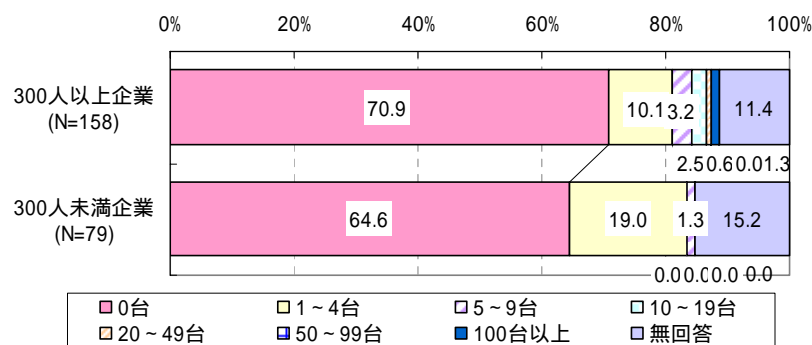


図 2.4-21 ウイルスに感染したサーバの台数 (就業者規模別)

#### 2.4.5. ウイルスの直接的な被害

ウイルスの直接的な被害は「個人の業務停滞」が 41.7%で最も多く、次いで「パソコン単体の停止」が 35.0%で続く。直接的な被害は企業の方が強く感じており、自治体では被害が「特になし」との回答が、企業より約 18 ポイント高い。

就業者規模別では、300 人以上企業の方が全般的に直接的な被害を感じる傾向にあるが、「情報破壊」「情報流出」「ウイルスメール等の発信」など、情報に係わる直接的な被害については、300 人以上企業よりも 300 人未満企業の方が被害と認識している。

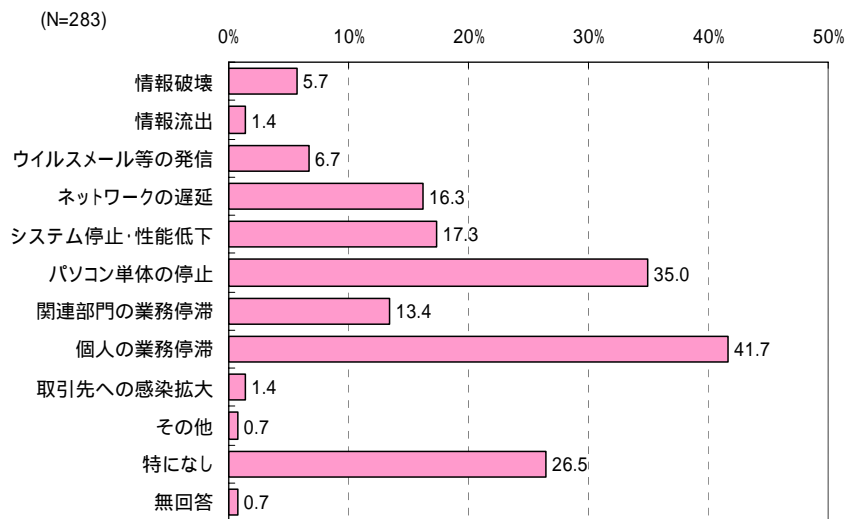


図 2.4-22 ウイルスの直接的な被害の有無

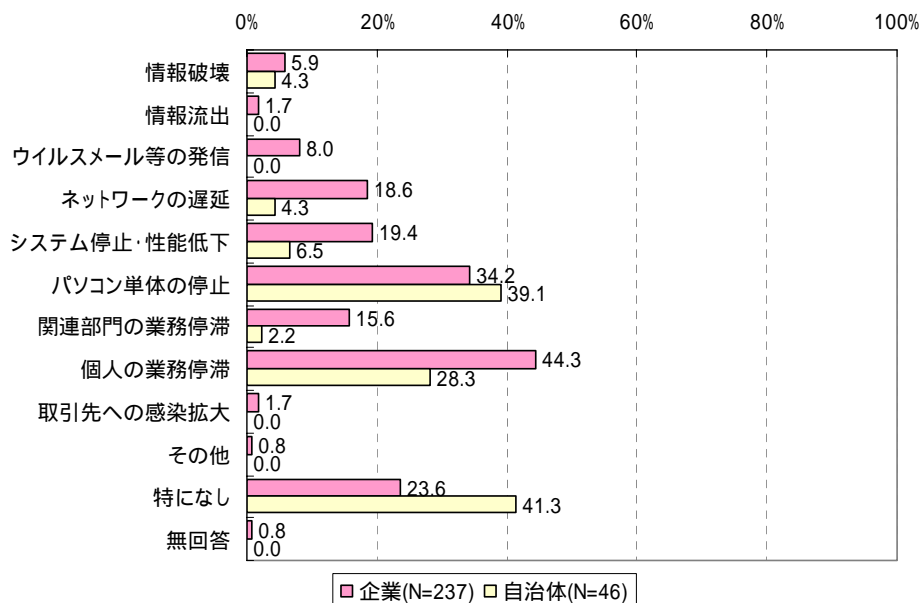


図 2.4-23 ウイルスの直接的な被害の有無（企業 / 自治体別）

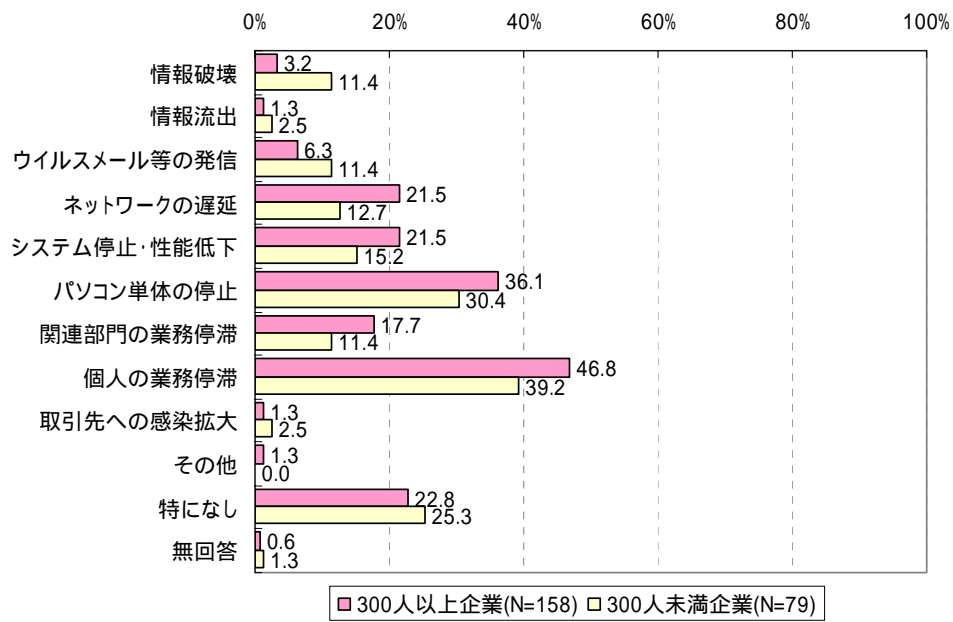


図 2.4-24 ウイルスの直接的な被害の有無（就業者規模別）

### 2.4.6. 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の売上に占める割合は、「0%」が2割である。

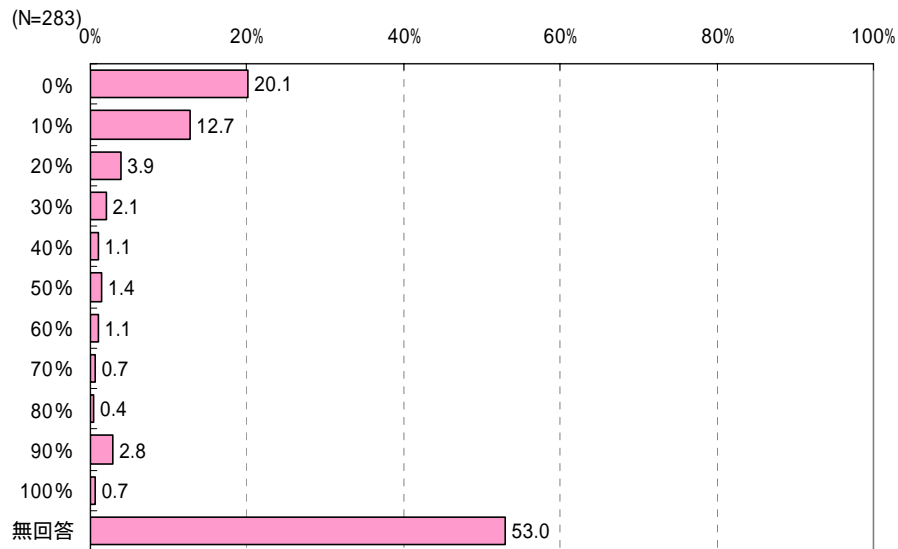


図 2.4-25 電子取引業務の売上が全体の売上に占める割合

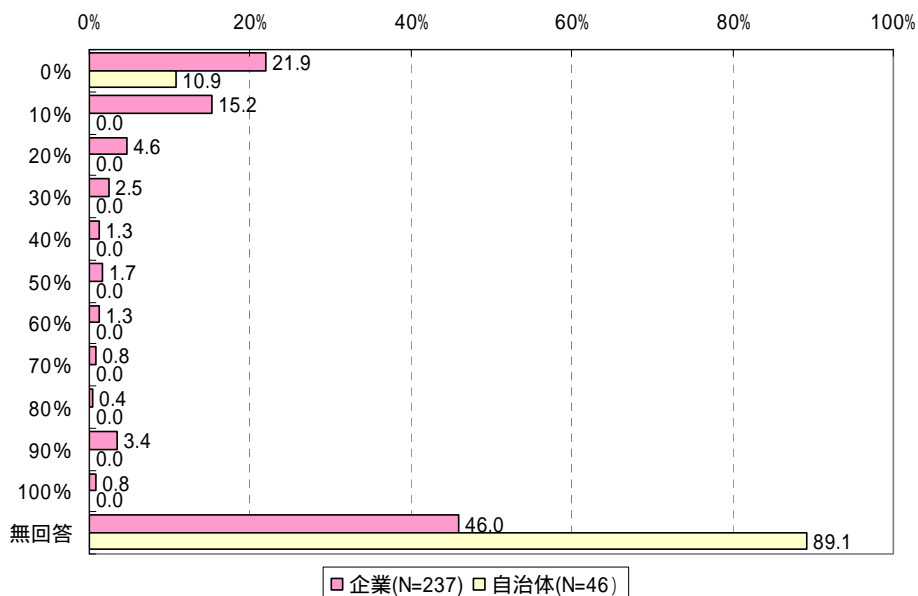


図 2.4-26 電子取引業務の売上が全体の売上に占める割合（企業 / 自治体別）

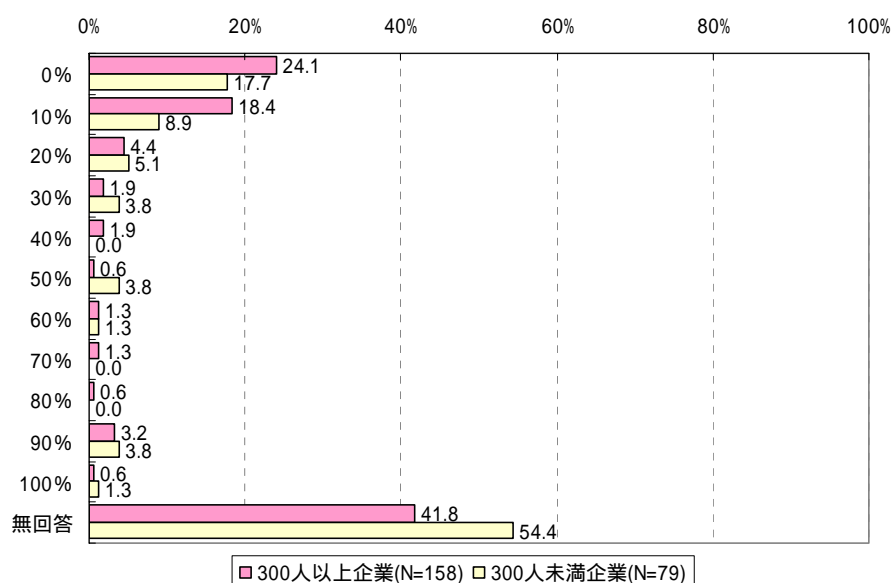


図 2.4-27 電子取引業務の売上が全体の売上に占める割合（就業者規模別）

(2) 電子商取引業務が停止した年間の延べ日数

電子商取引業務が停止した年間延べ日数は「0日」が40.3%である。

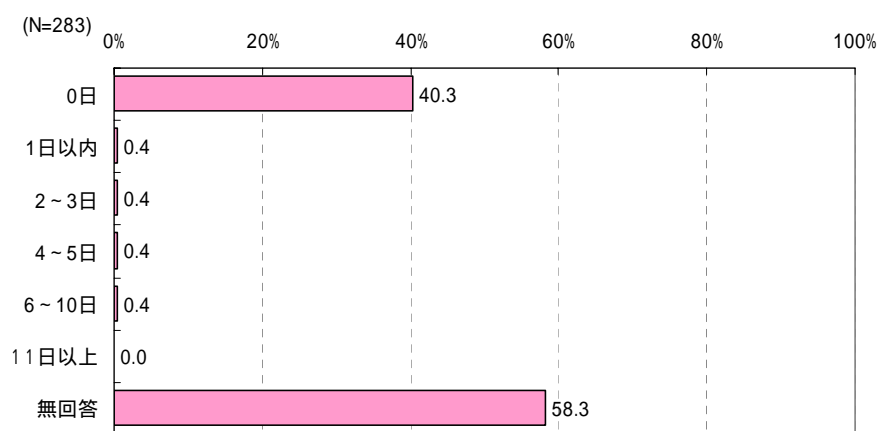


図 2.4-28 電子商取引業務が停止した年間延べ日数（ウイルス感染経験あり）

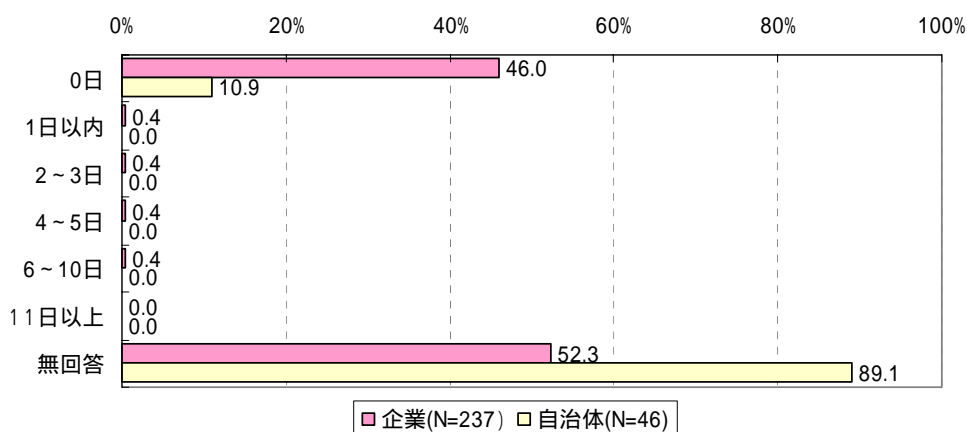


図 2.4-29 電子商取引業務が停止した年間延べ日数  
(ウイルス感染経験あり、企業/自治体別)

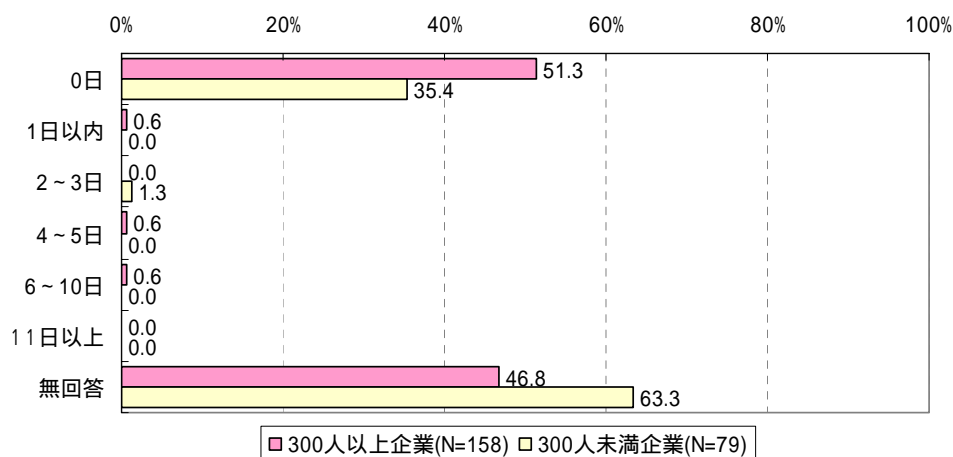


図 2.4-30 電子商取引業務が停止した年間延べ日数  
(ウイルス感染経験あり、就業者規模別)

### 2.4.7. EC サーバ以外の業務遂行上重要なサーバ停止の影響

#### (1) EC サーバ以外の業務遂行上重要なサーバ停止の年間延べ日数

EC サーバ以外の重要なサーバがが停止した年間延べ日数は「0日」が65.4%である。

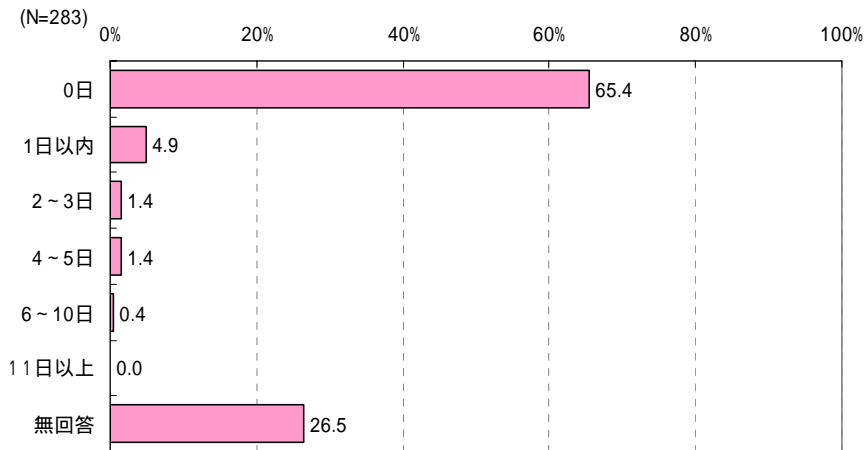


図 2.4-31 EC サーバ以外の業務遂行上重要なサーバ停止の年間延べ日数

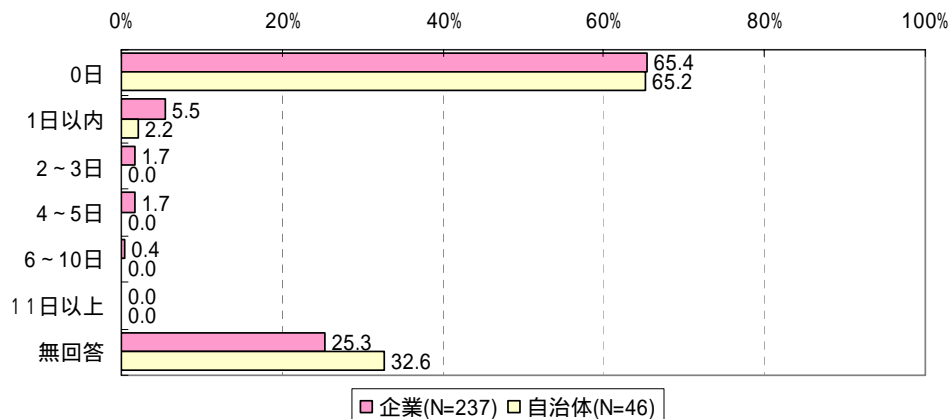


図 2.4-32 EC サーバ以外の業務遂行上重要なサーバ停止の年間延べ日数（企業 / 自治体別）

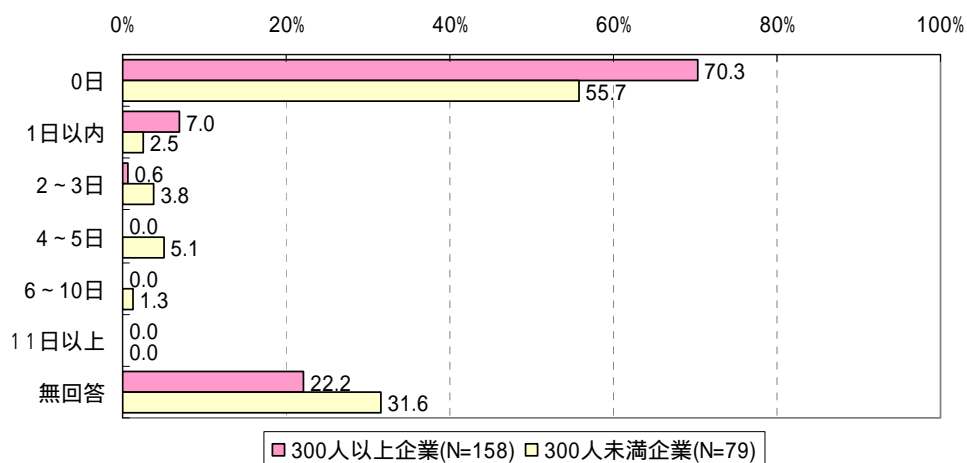


図 2.4-33 EC サーバ以外の業務遂行上重要なサーバ停止の年間延べ日数（就業者規模別）

(2)EC サーバ以外の業務遂行上重要なサーバ停止による売上への影響

EC サーバ以外の重要なサーバ停止による売上への影響は「0%」が73.9%である。

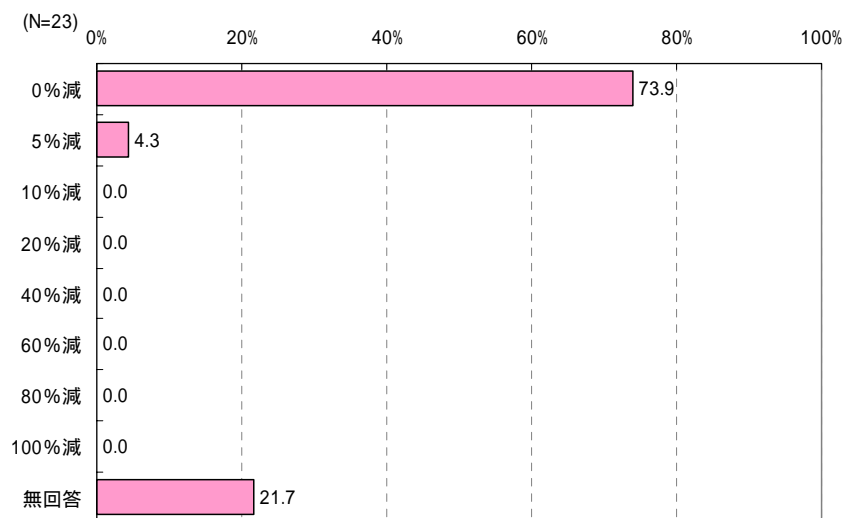


図 2.4-34 EC サーバ以外の業務遂行上重要なサーバ停止による売上への影響

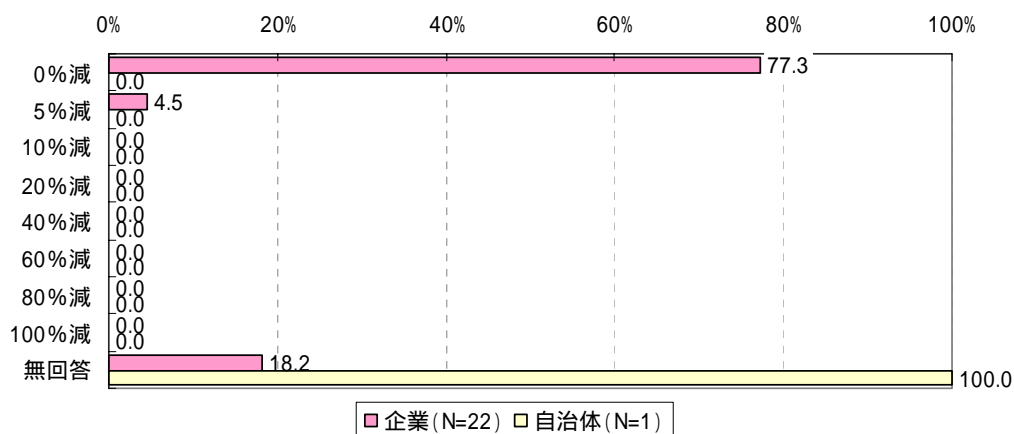


図 2.4-35 EC サーバ以外の業務遂行上重要なサーバ停止による売上への影響（企業／自治体別）

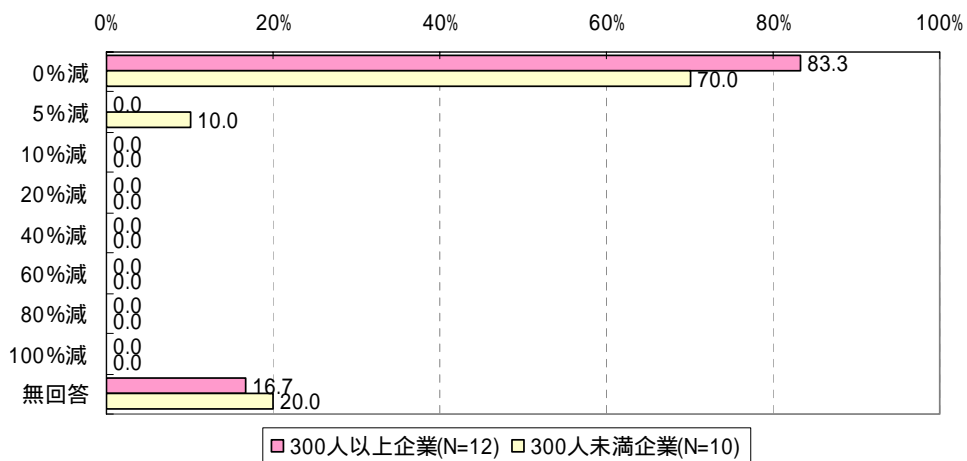


図 2.4-36 EC サーバ以外の業務遂行上重要なサーバ停止による売上への影響（就業者規模別）

2.4.8. 2007年1年間の情報管理部門が行った復旧作業人日

2007年1年間に情報管理部門が行った復旧作業人日は「0～1人・日」が33.9%である。

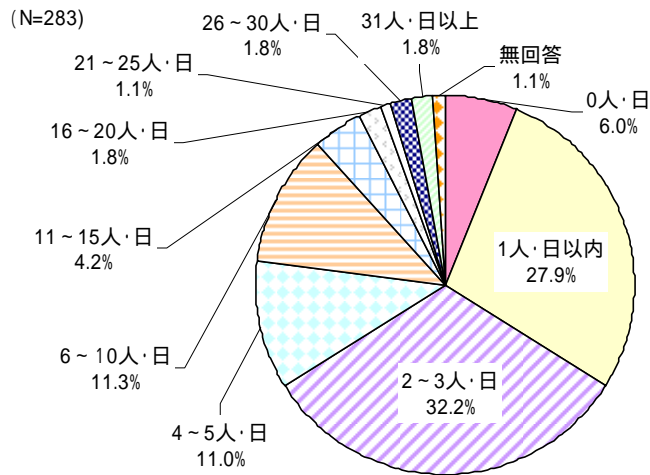


図 2.4-37 2007年1年間のウイルス感染からの復旧作業延べ人日

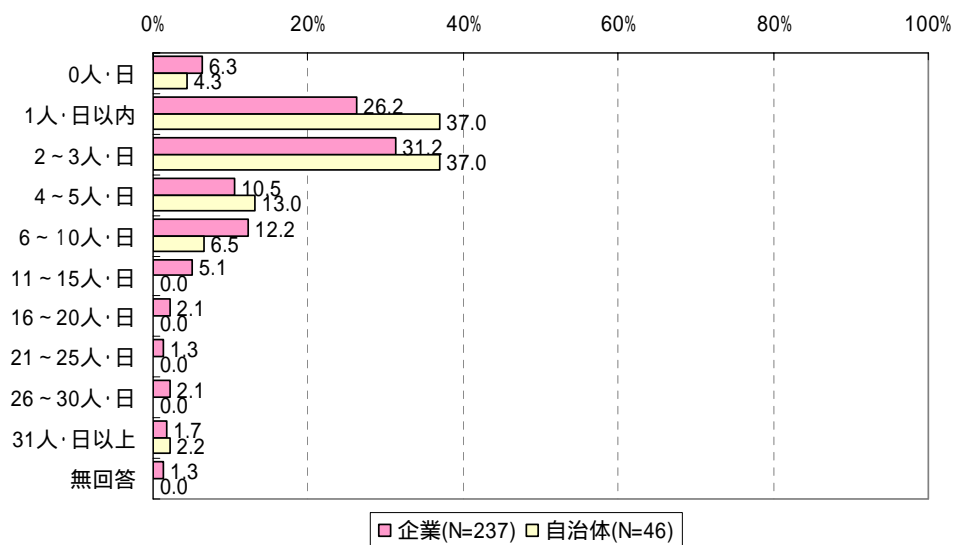


図 2.4-38 2007年1年間のウイルス感染からの復旧作業延べ人日 (企業/自治体別)

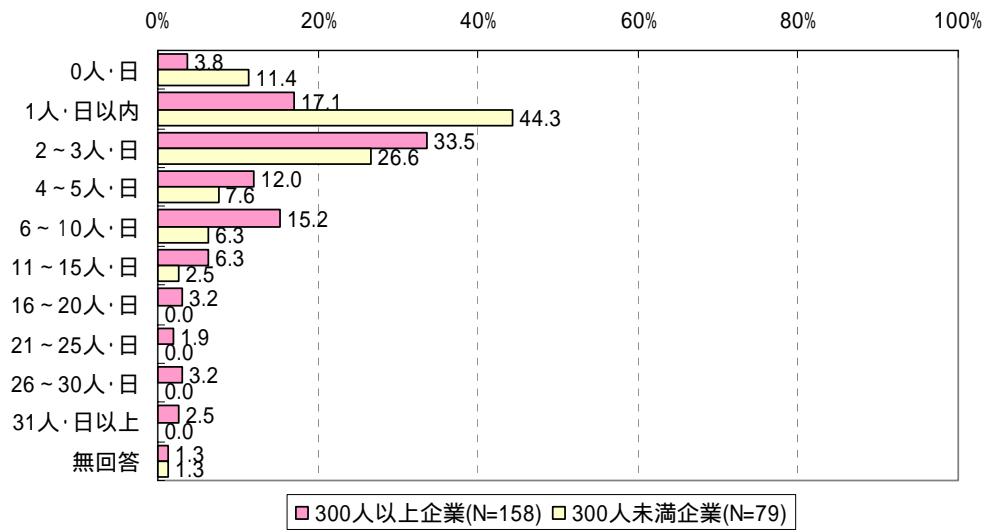


図 2.4-39 2007年1年間のウイルス感染からの復旧作業延べ人日（就業者規模別）

2.4.9. 2007年1年間のシステム復旧に関して新たに購入した代替機器の費用

1年間の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、「0円」が81.6%である。

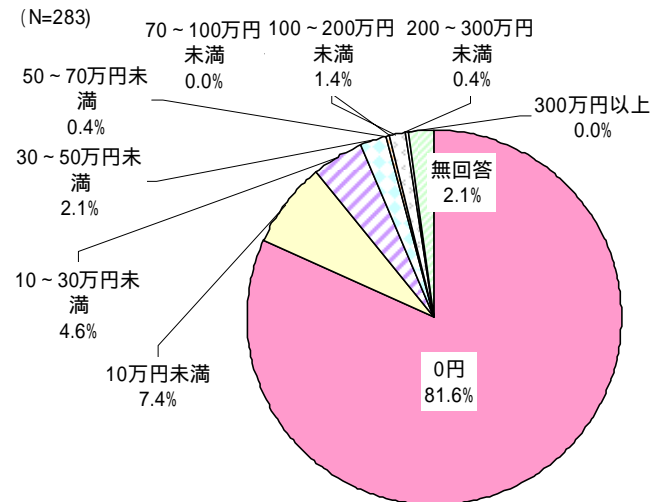


図 2.4-40 2007年1年間のシステム復旧に関して新たに購入した代替機器の費用

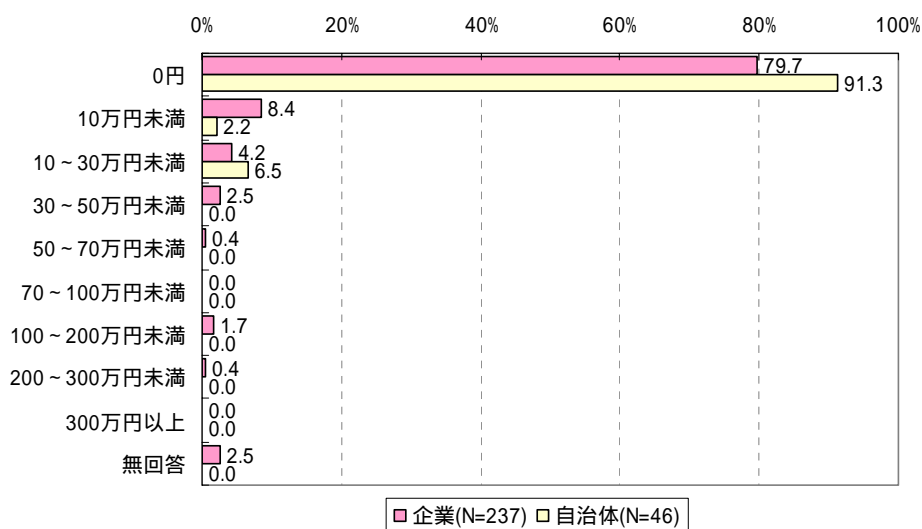


図 2.4-41 2007年1年間のシステム復旧に関して新たに購入した代替機器の費用  
(企業/自治体別)

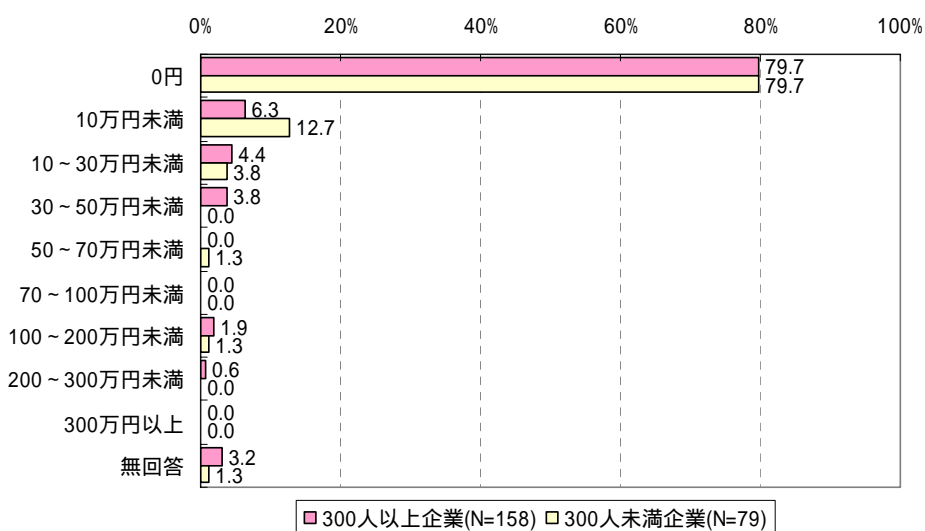


図 2.4-42 2007年1年間のシステム復旧に関して新たに購入した代替機器の費用  
(就業者規模別)

2.4.10. システム復旧に関して外部に発注した業務の費用

システム復旧に関して新たに外部に発生した業務の費用は、「0円」が83.4%である。

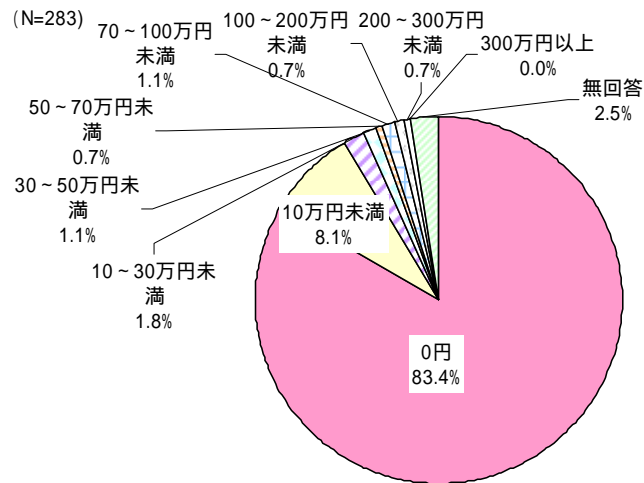


図 2.4-43 2007年1年間にシステム復旧に関して外部に発注した業務の費用

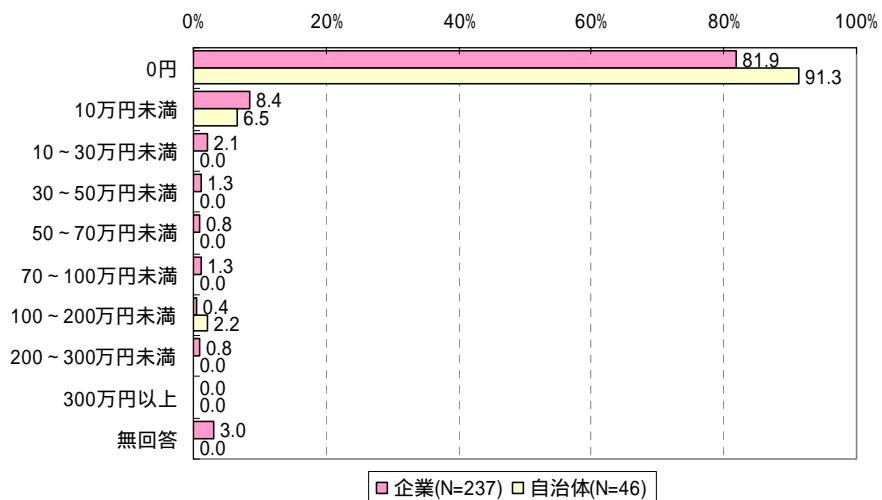


図 2.4-44 2007年1年間にシステム復旧に関して外部に発注した業務の費用(企業/自治体別)

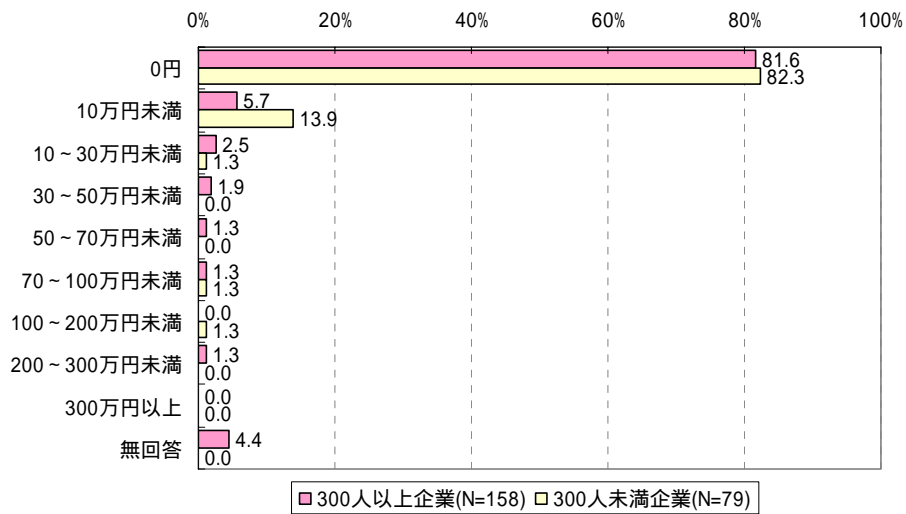


図 2.4-45 2007年1年間にシステム復旧に関して外部に発注した業務の費用（従業員規模）

2.4.11. 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

ウイルス感染が原因で発生した追加データ処理作業人日は、「0人・日」が73.5%である。

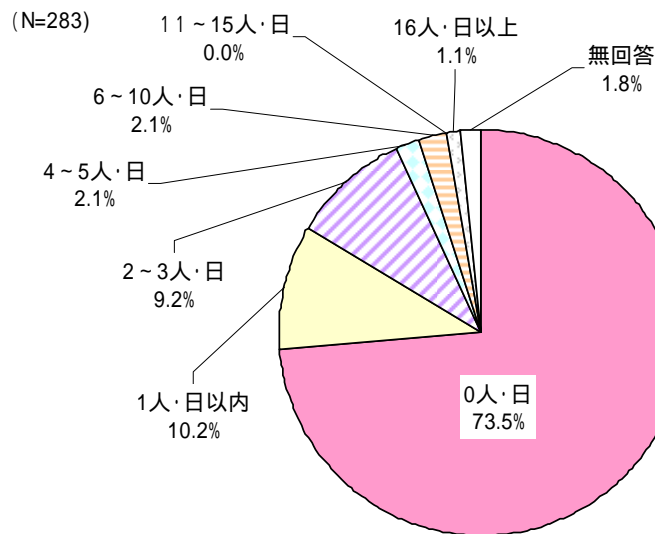


図 2.4-46 ウイルス感染が原因で発生した追加データ処理作業人日

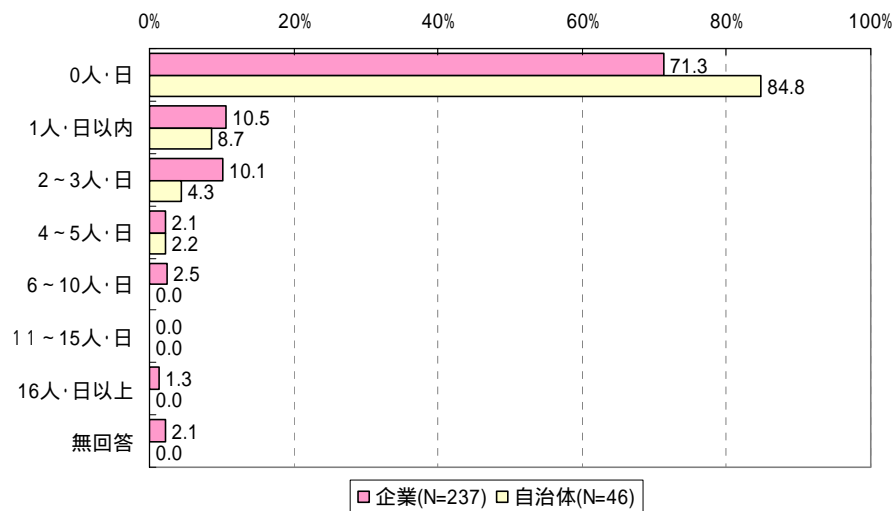


図 2.4-47 ウイルス感染が原因で発生した追加データ処理作業人日（企業／自治体別）

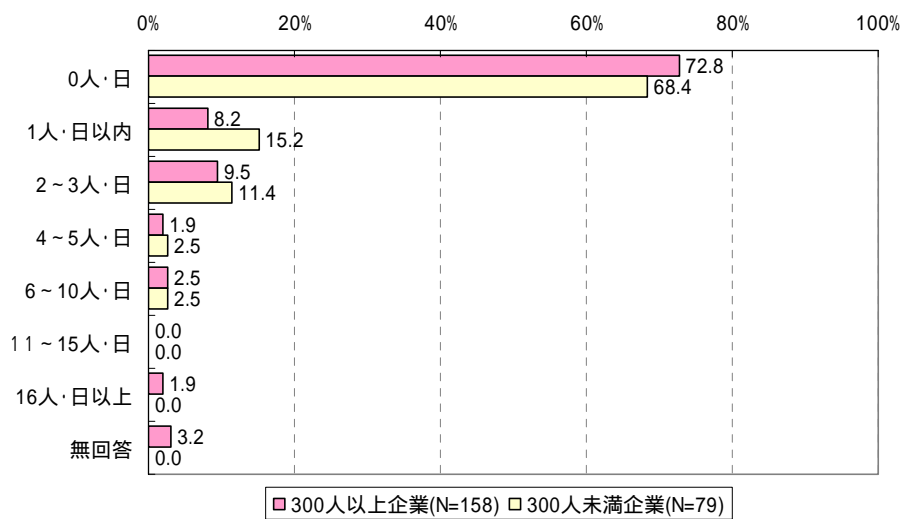


図 2.4-48 ウイルス感染が原因で発生した追加データ処理作業人日（就業者規模別）

## 2.4.12. 復旧以外の対応

### (1) 作業内容

復旧以外の対応は、「原因追求・影響範囲特定のための外部調査」が最も多く 18.7%だが、「特に実施していない」が 54.8%にも達する。

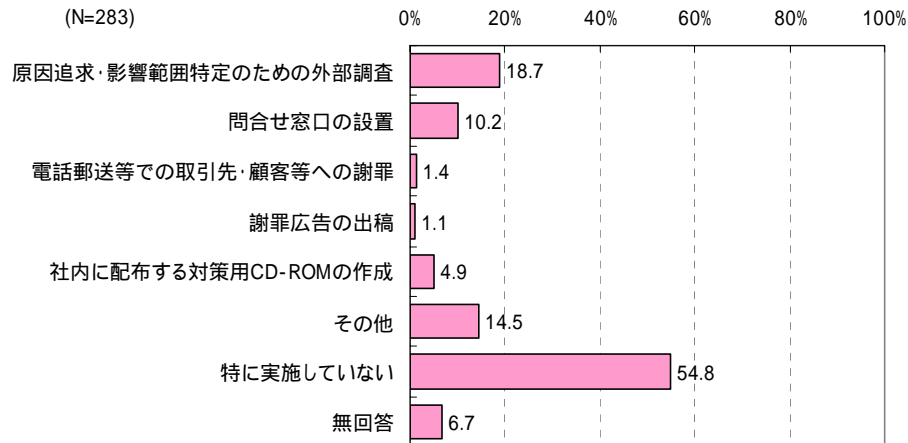


図 2.4-49 復旧以外の対応作業内容

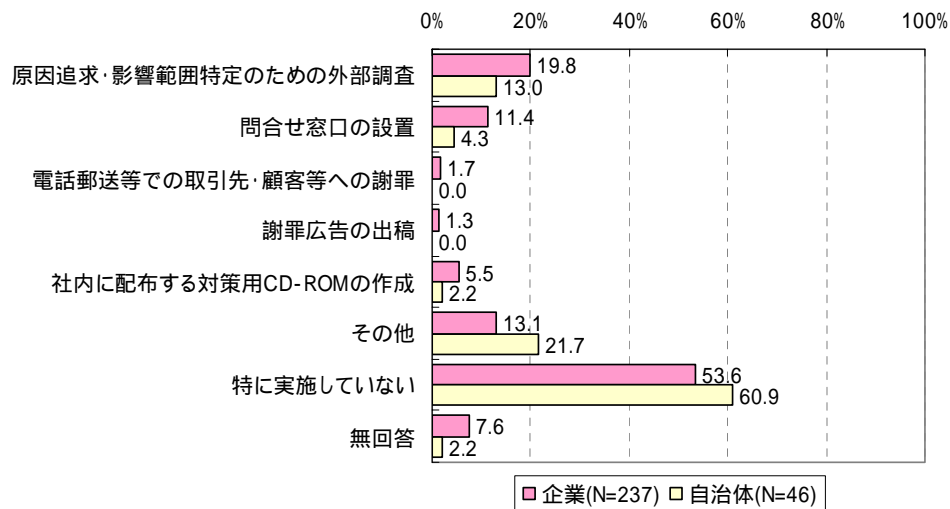


図 2.4-50 復旧以外の対応作業内容（企業 / 自治体別）

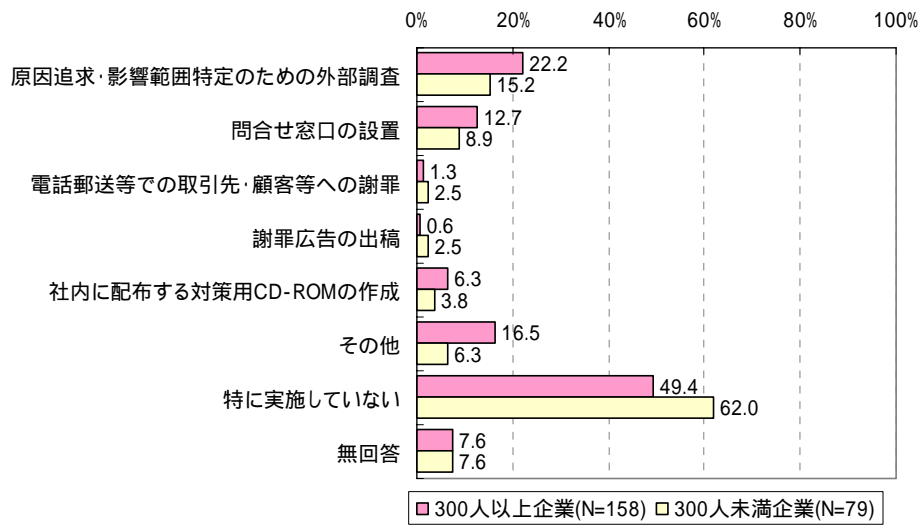


図 2.4-51 復旧以外の対応作業内容（就業者規模別）

(2)作業人日

作業人日は、ほぼ全ての作業においても「1人・日」が最も多い。

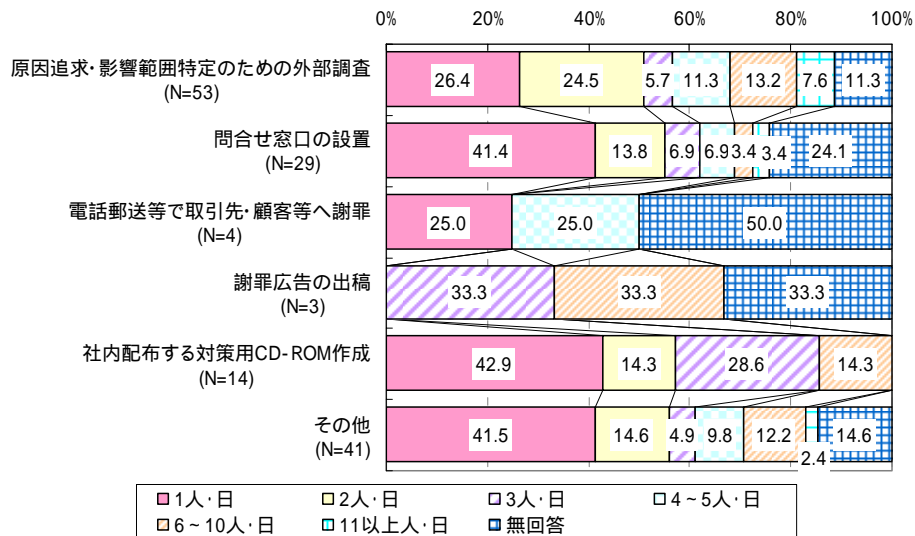
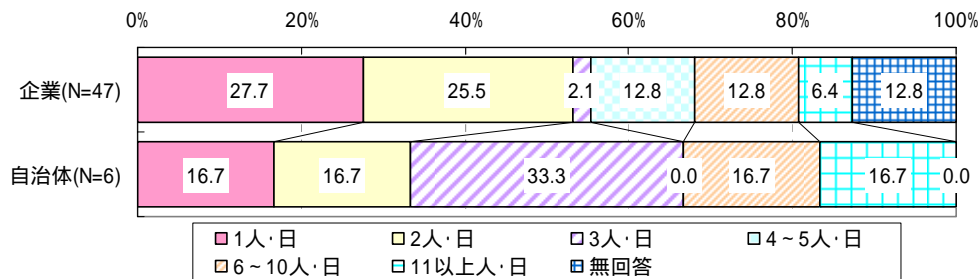
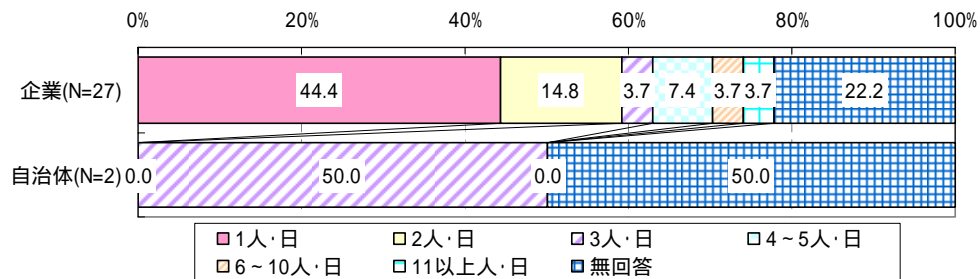


図 2.4-52 作業人日

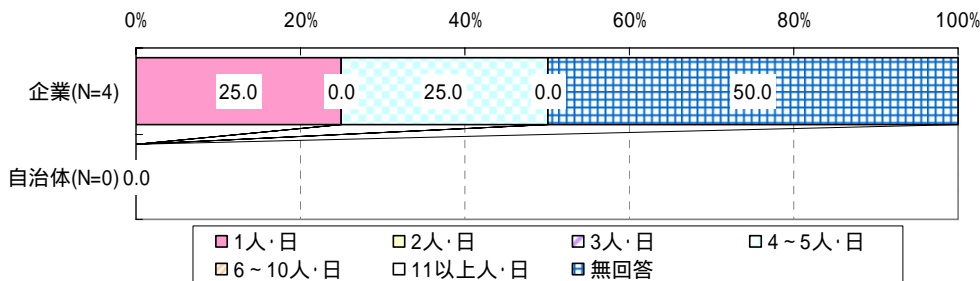
< 原因追及・影響範囲特定のための外部調査 >



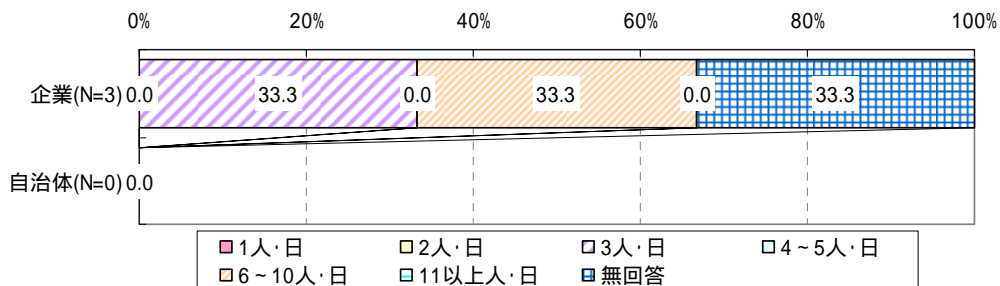
< 問合せ窓口の設置 >



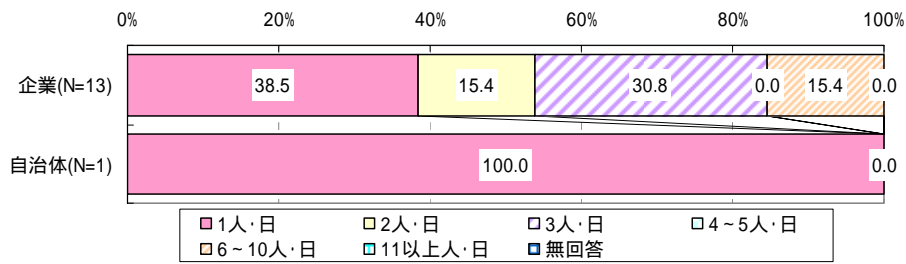
< 電話郵送等で取引先・顧客等へ謝罪 >



< 謝罪広告の出稿 >



< 社内配布する対策用 CD-ROM 作成 >



< その他 >

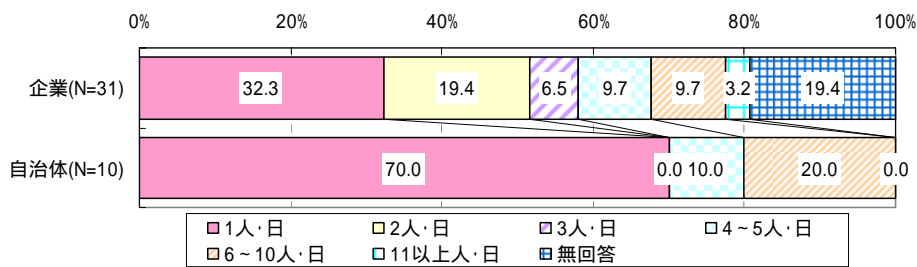
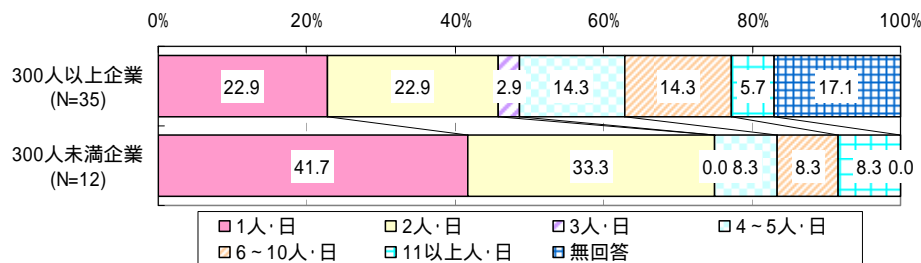
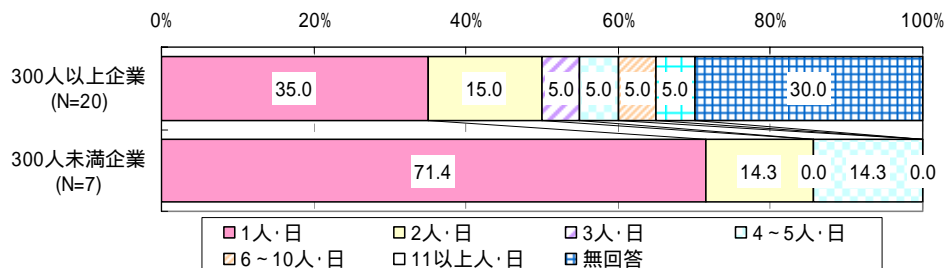


図 2.4-53 作業人日（企業 / 自治体別）

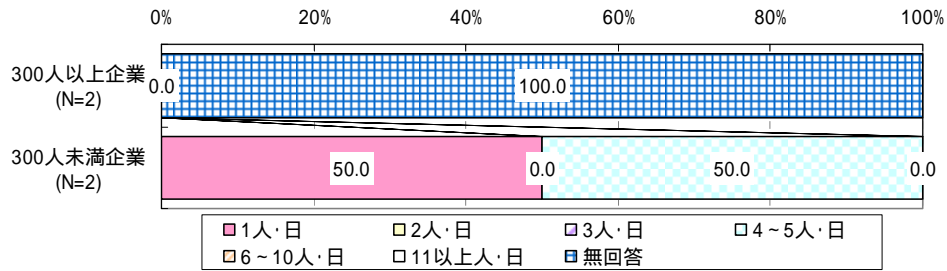
< 原因追及・影響範囲特定のための外部調査 >



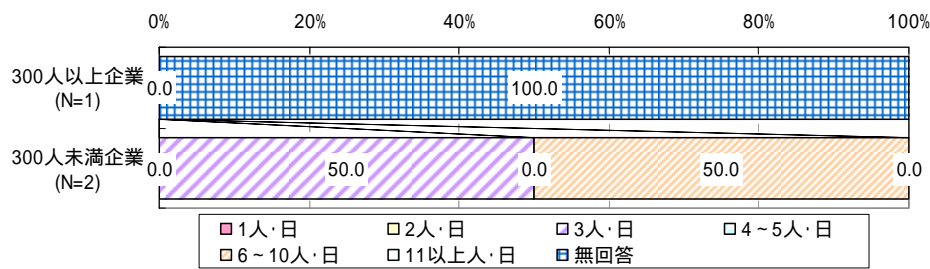
< 問合せ窓口の設置 >



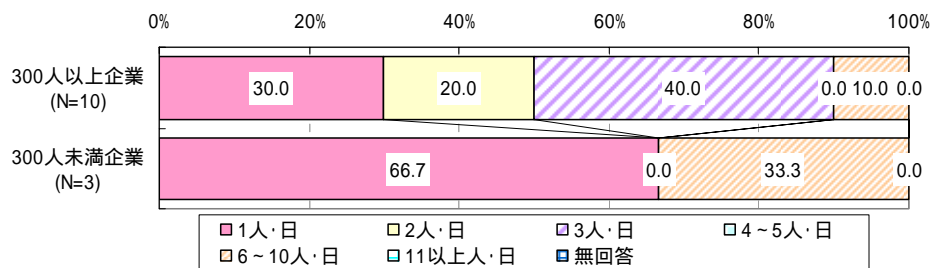
< 電話郵送等で取引先・顧客等へ謝罪 >



< 謝罪広告の出稿 >



< 社内配布する対策用 CD-ROM 作成 >



< その他 >

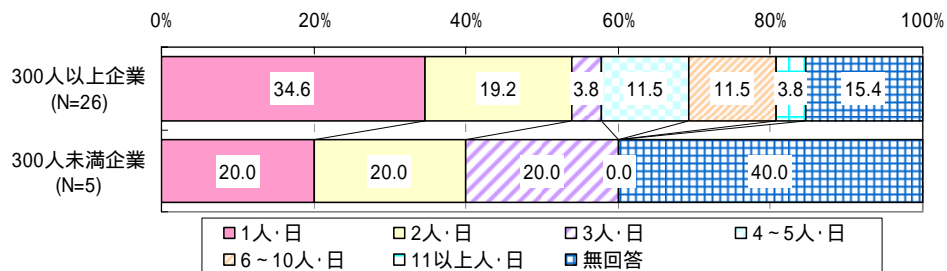


図 2.4-54 作業人日（就業者規模別）

### 2.4.13. 復旧時の復旧以外の対応による外部発注費用

復旧時の復旧以外の対応による外部発注費用は、「0円」が81.3%である。

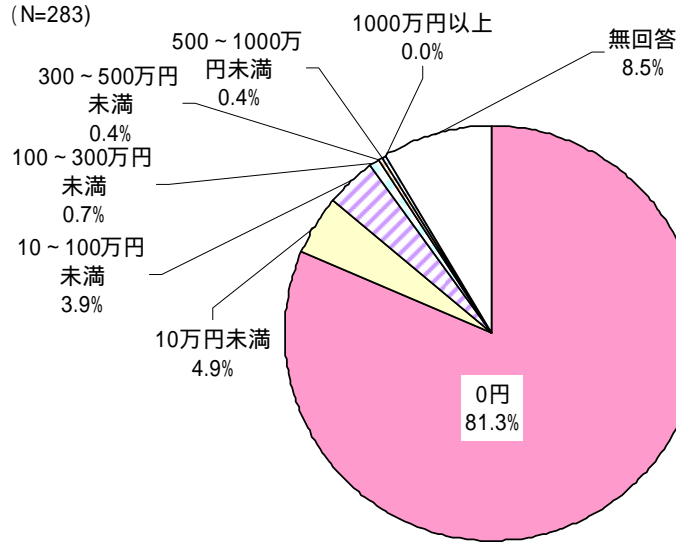


図 2.4-55 復旧以外の対応による外部発注費用

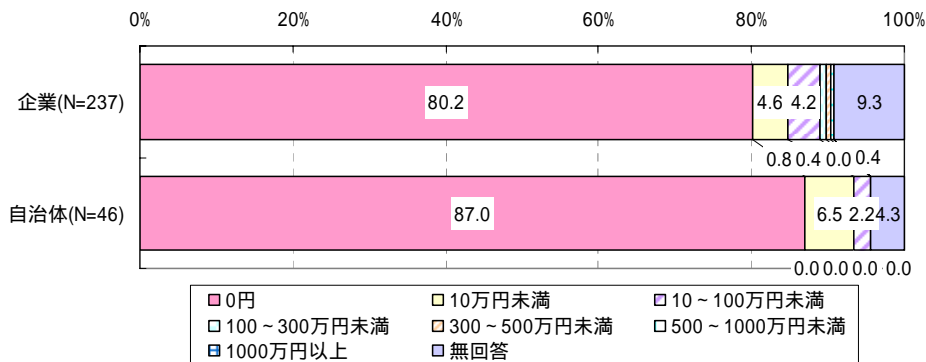


図 2.4-56 復旧以外の対応による外部発注費用 (企業 / 自治体別)

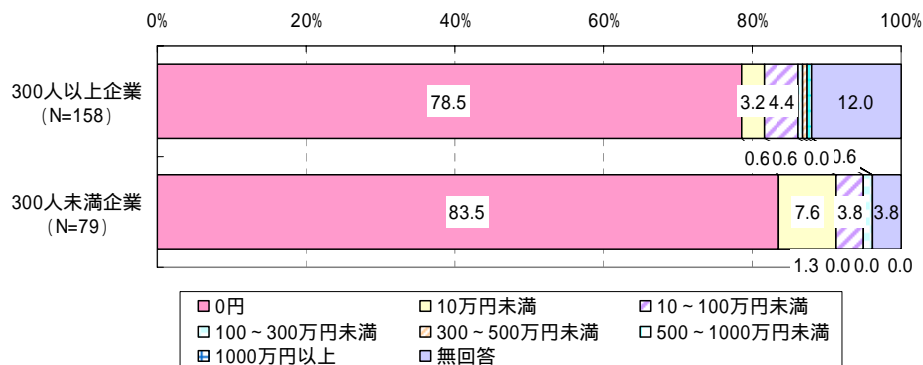


図 2.4-57 復旧以外の対応による外部発注費用 (就業者規模別)

## 2.4.14. 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

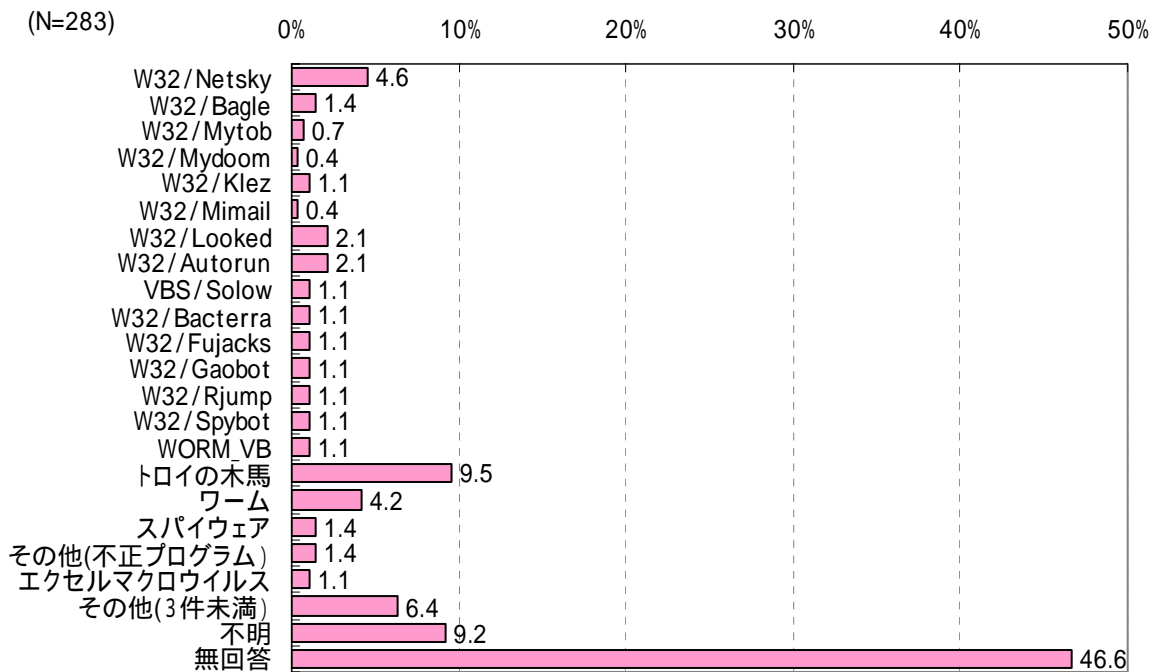


図 2.4-58 被害の最も大きかったウイルス名

ウイルス感染・発見月は 2007 年後半が若干多い傾向にある。

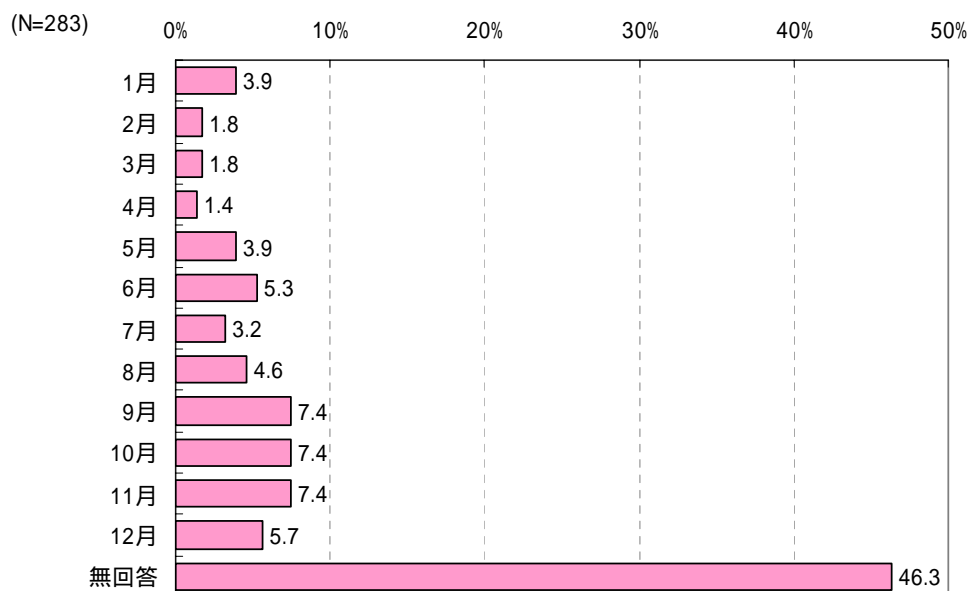


図 2.4-59 被害の最も大きかったウイルス発見月

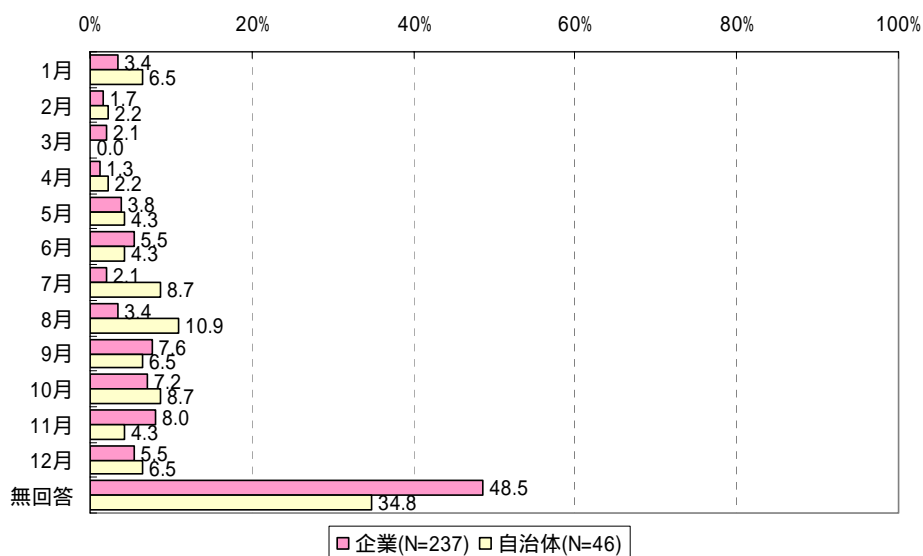


図 2.4-60 被害の最も大きかったウイルス発見月（企業／自治体別）

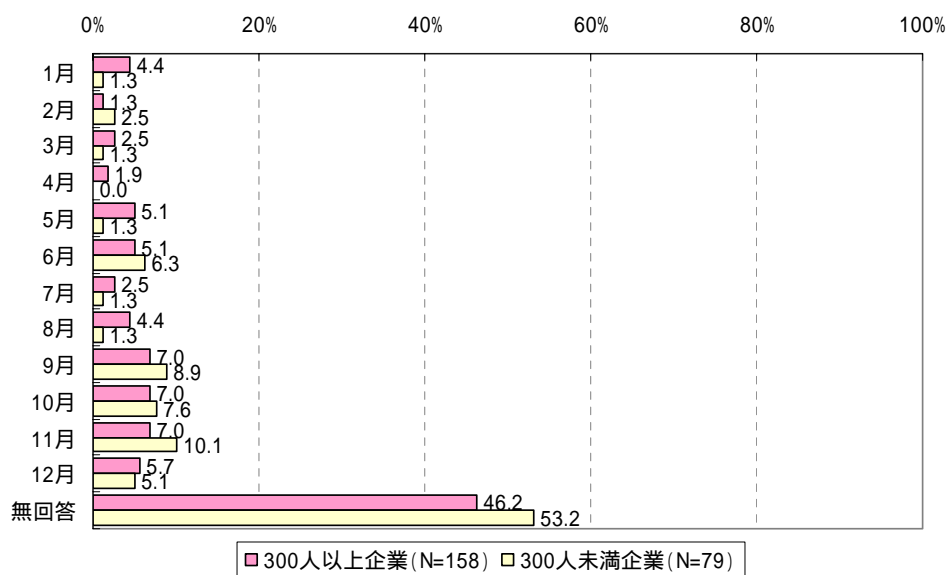


図 2.4-61 被害の最も大きかったウイルス発見月（就業者規模別）

(2) ウイルス発見の経緯

ウイルス感染・発見の経緯は「クライアント対策ソフト」が68.9%で最も多い。

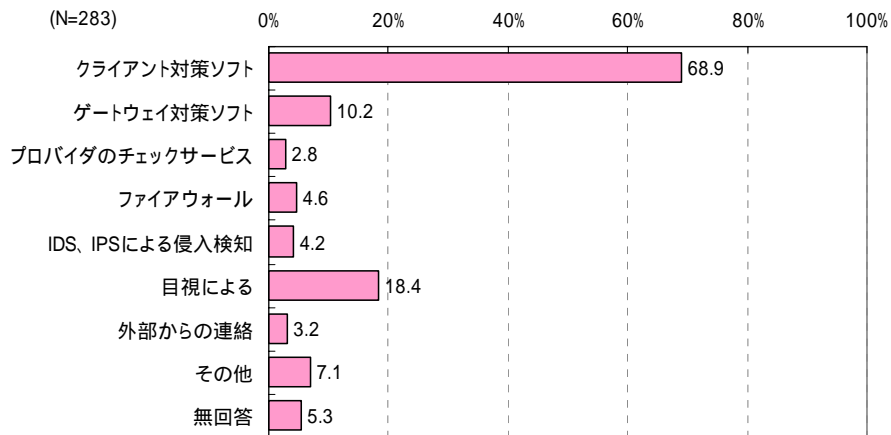


図 2.4-62 ウイルス発見の経緯

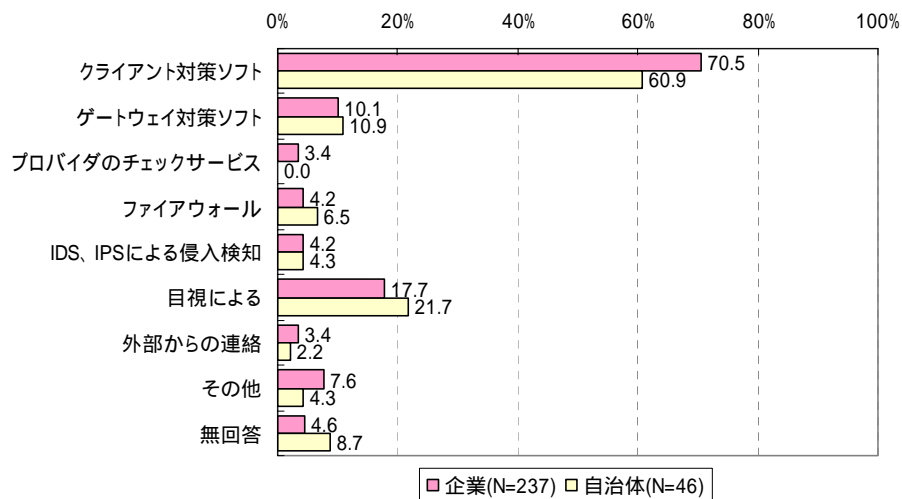


図 2.4-63 ウイルス発見の経緯（企業 / 自治体別）

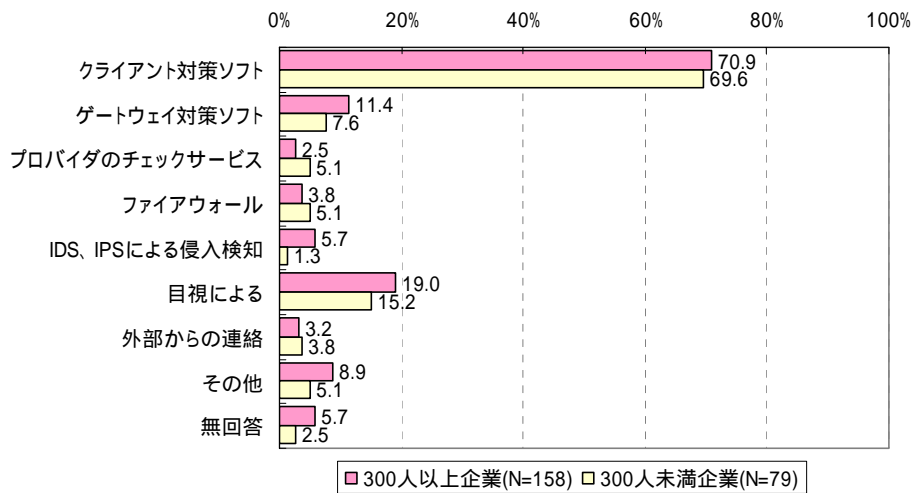


図 2.4-64 ウイルス発見の経緯（就業者規模別）

(3) 想定されるコンピュータウイルスの感染経路

想定されるコンピュータウイルスの感染経路は「インターネット接続」「外部媒体、持ち込みクライアント」が2割を超える。自治体では、特に「インターネット接続」が多い。また、300人未満企業では「電子メール」が増える。

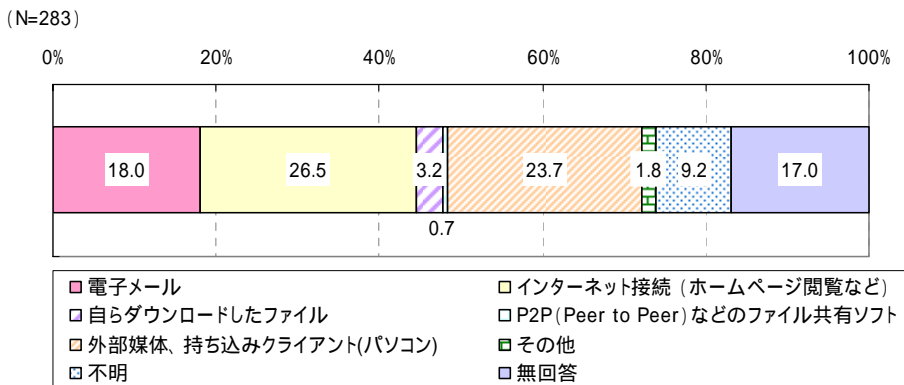


図 2.4-65 想定されるコンピュータウイルスの感染経路

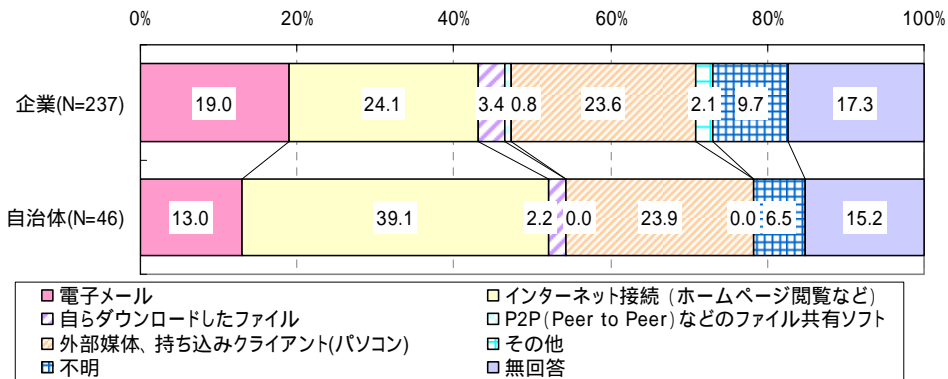


図 2.4-66 想定されるコンピュータウイルスの感染経路（企業／自治体別）

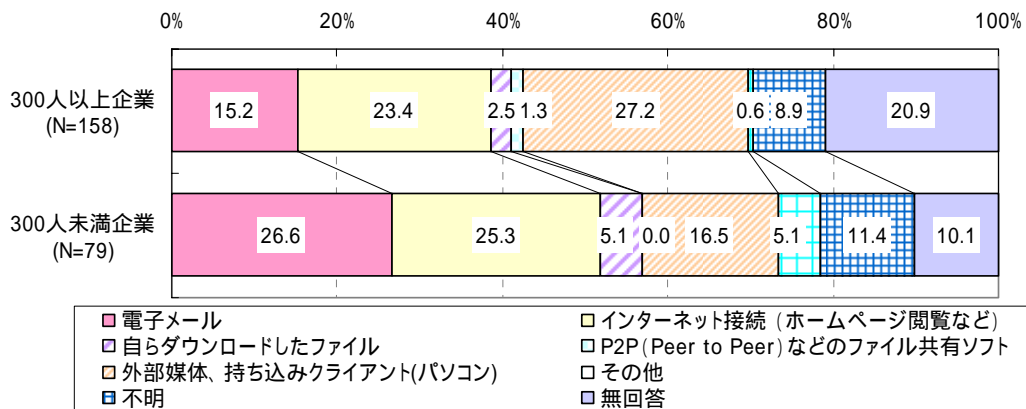


図 2.4-67 想定されるコンピュータウイルスの感染経路（就業者規模別）

(4) 感染したパソコンのOSと台数

感染したパソコンのOSはWindows系で「4台以下」が半数である。

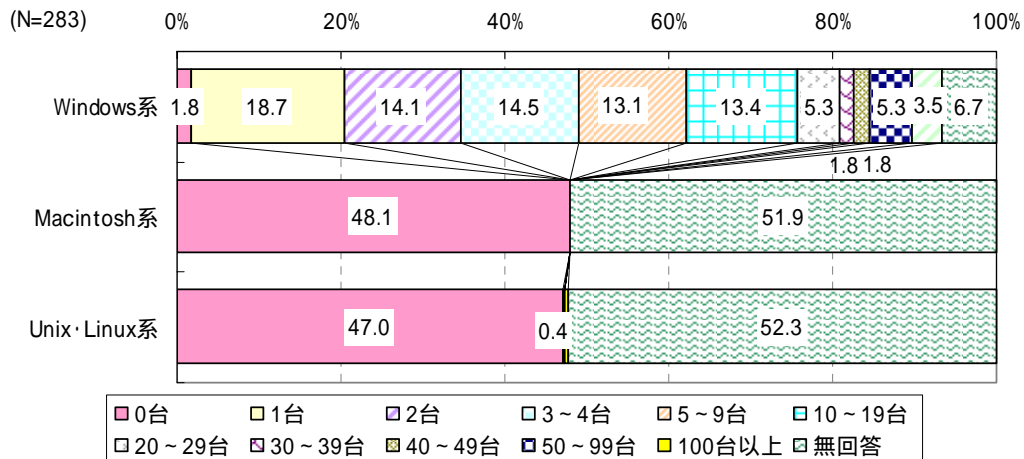
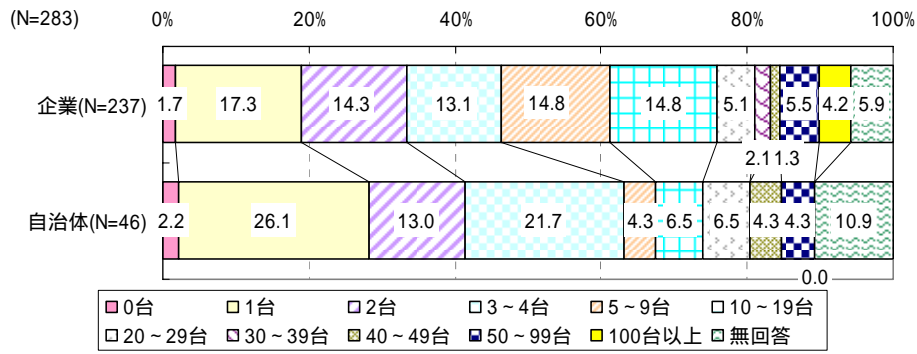
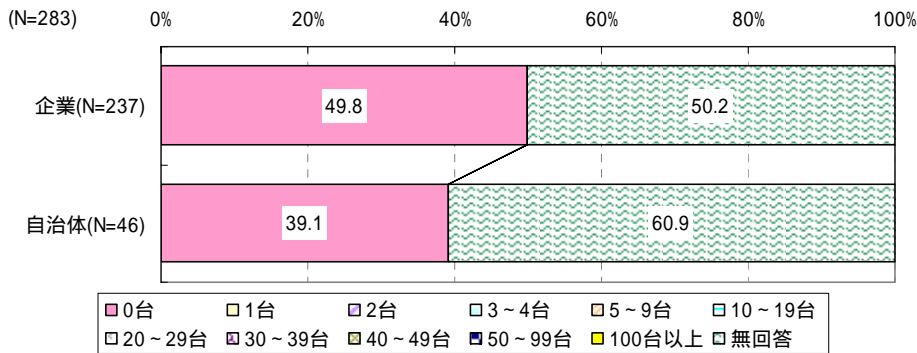


図 2.4-68 感染したパソコンのOSと台数

< Windows 系 >



< Macintosh 系 >



< Unix・Linux 系 >

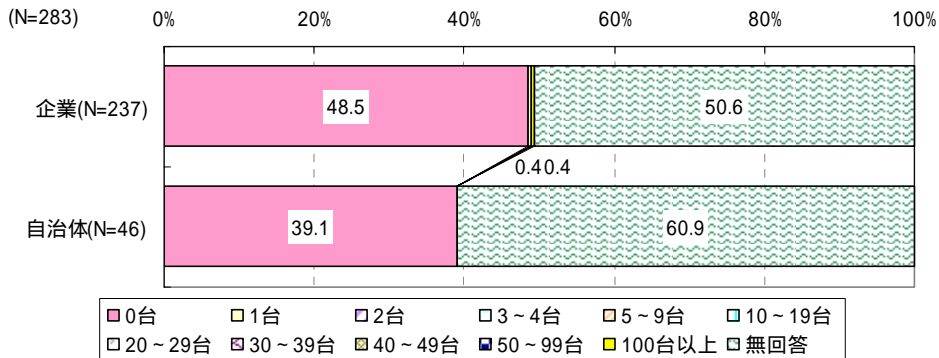
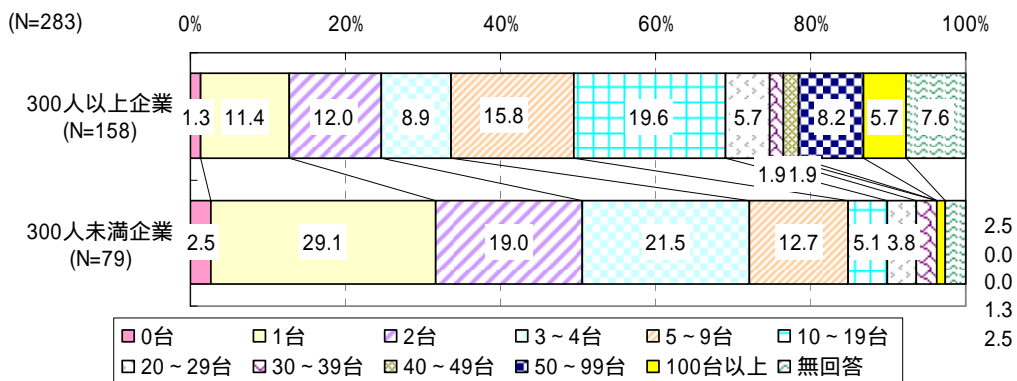
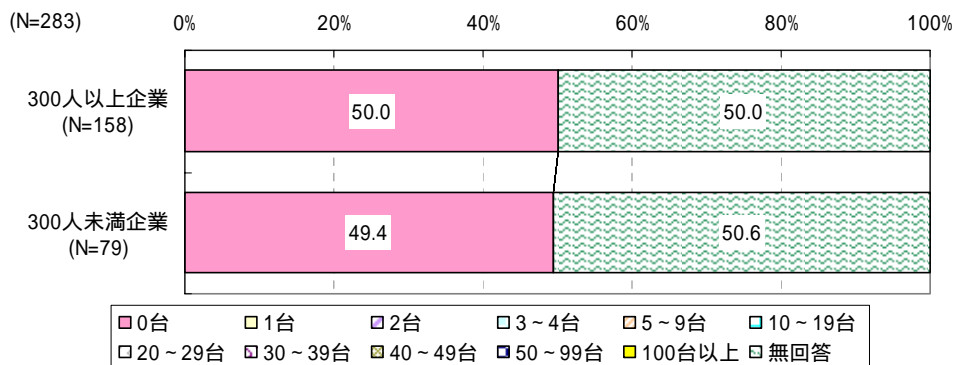


図 2.4-69 感染したパソコンのOSと台数（企業／自治体別）

< Windows 系 >



< Macintosh 系 >



< Unix・Linux 系 >

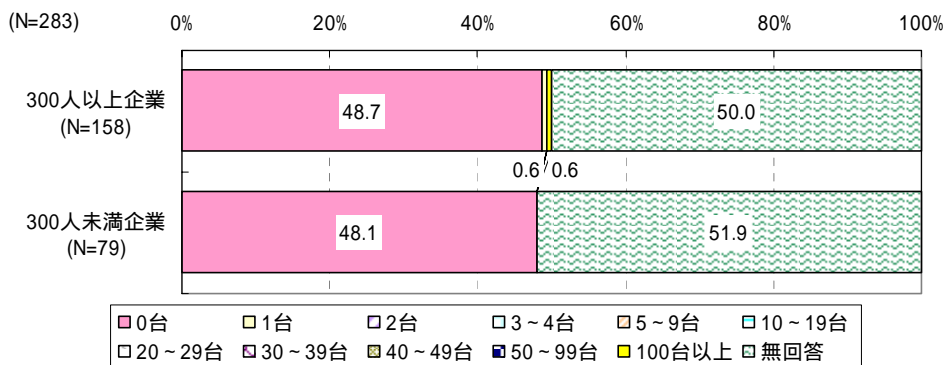


図 2.4-70 感染したパソコンのOSと台数（就業者規模別）

## 2.5. ファイル共有ソフトを介した情報漏えい

### 2.5.1. 個人情報、業務情報流出被害経験の有無

ファイル共有ソフトを介した情報漏えいについて「被害経験がある」としたのは2.2%である。

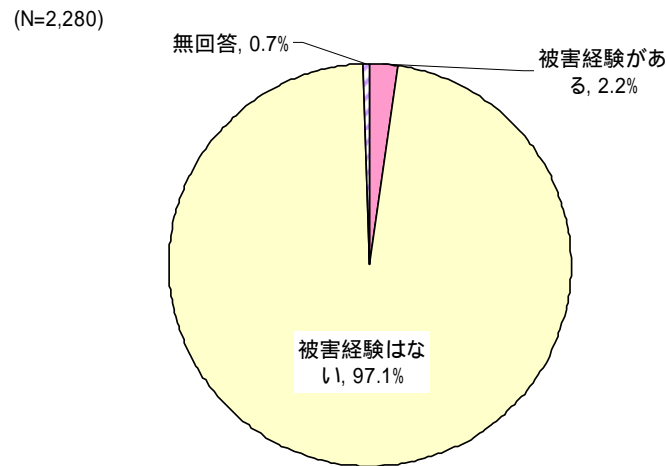


図 2.5-1 個人情報、業務情報流出被害経験の有無

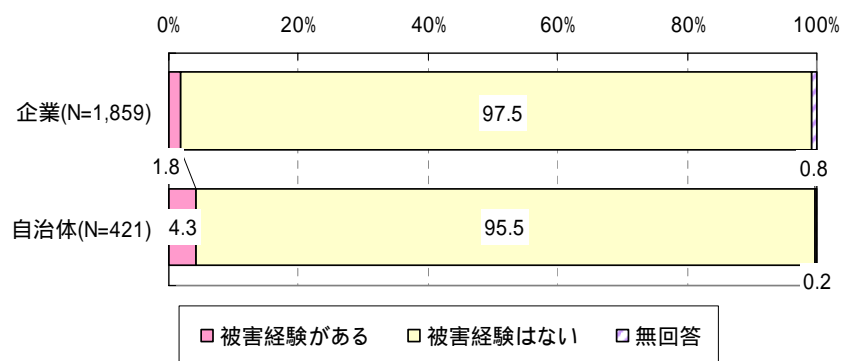


図 2.5-2 個人情報、業務情報流出被害経験の有無（企業／自治体別）

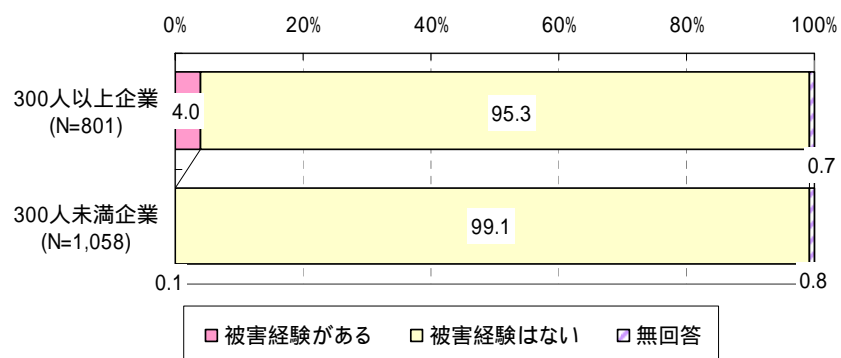


図 2.5-3 個人情報、業務情報流出被害経験の有無（就業者規模別）

### 2.5.2. 流出情報の種類

流出した情報は、「社内の業務情報」および「顧客（個人）情報」がいずれも約半数であるが、自治体は7割近くが「顧客（個人）情報」である。

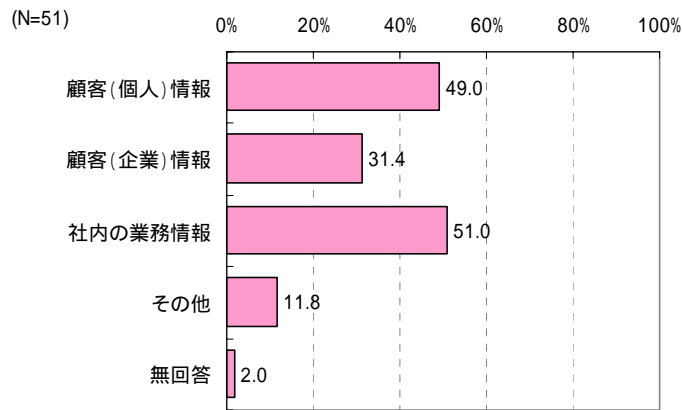


図 2.5-4 流出情報の種類

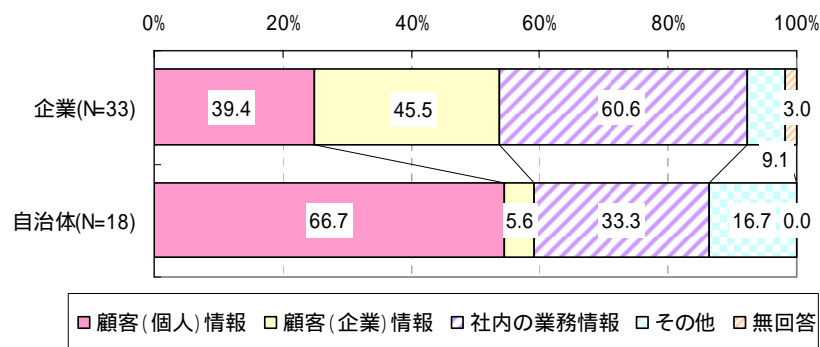


図 2.5-5 流出情報の種類（企業 / 自治体別）

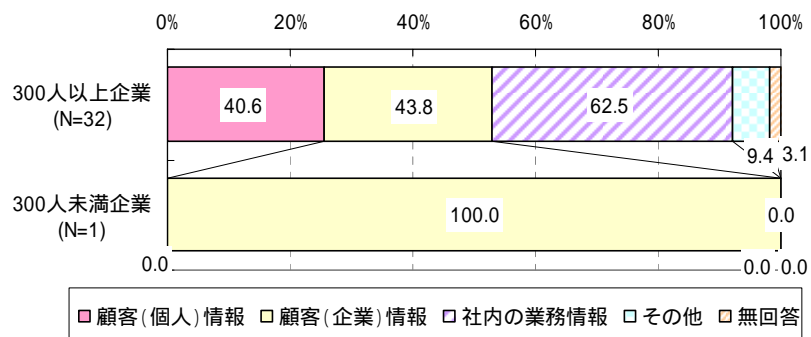


図 2.5-6 流出情報の種類（就業者規模別）

### 2.5.3. 対応延べ人日

情報漏えいに対する対応延べ人日は、「16人・日以上」が31.4%で最も大きい。

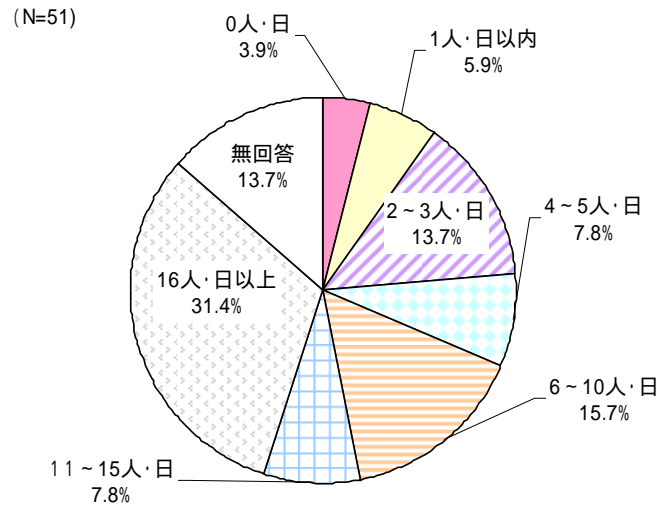


図 2.5-7 対応延べ人日

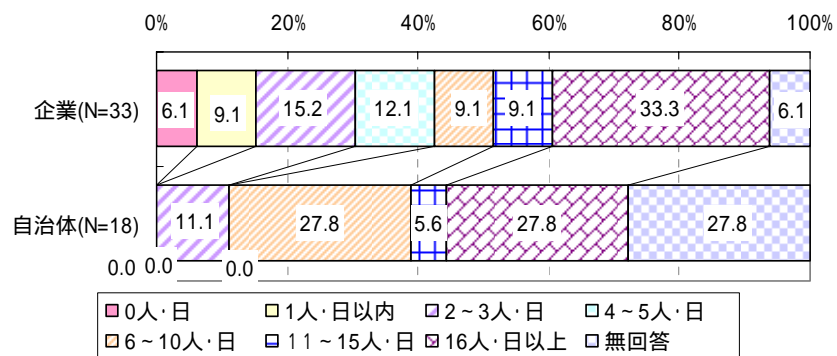


図 2.5-8 対応延べ人日 (企業 / 自治体別)

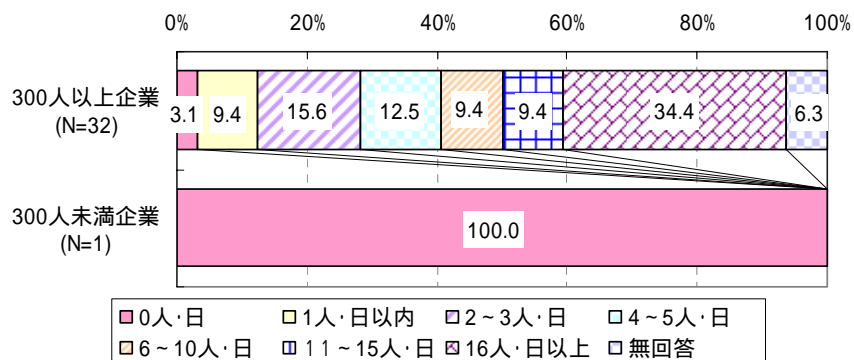


図 2.5-9 対応延べ人日 (就業者規模別)

### 2.5.4. 対応内容

対応内容は、「原因追及・影響範囲特定のための外部調査」が60.8%で最も多い。

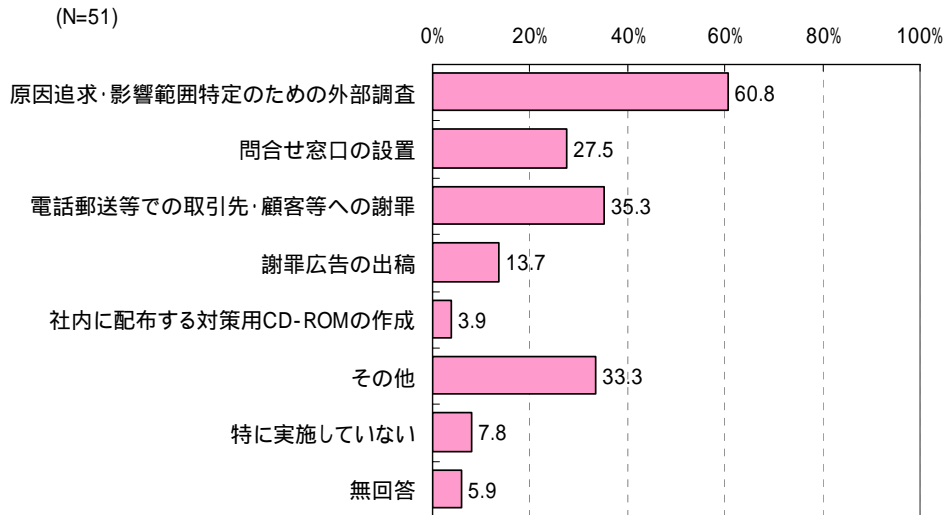


図 2.5-10 対応内容

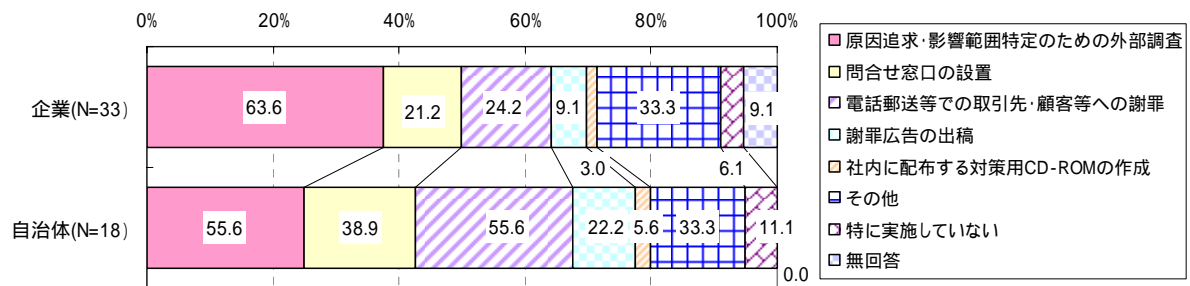


図 2.5-11 対応内容（企業／自治体別）

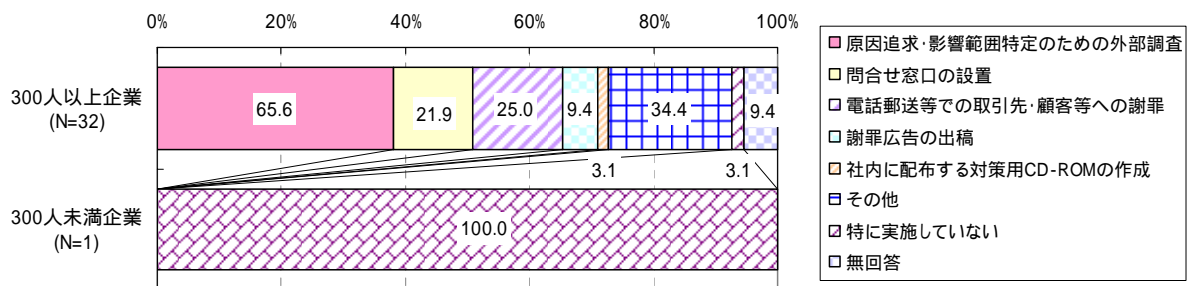


図 2.5-12 対応内容（就業者規模別）

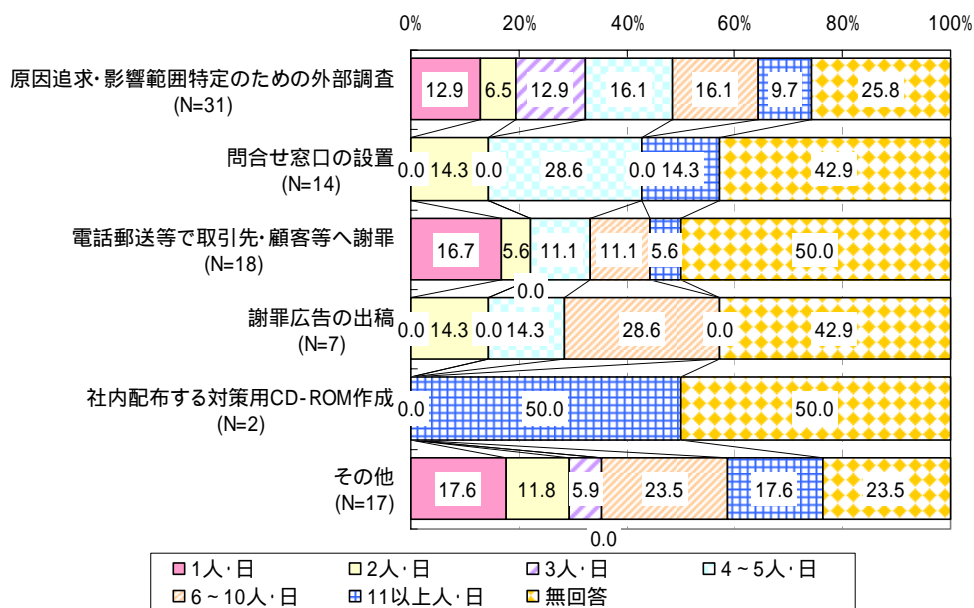
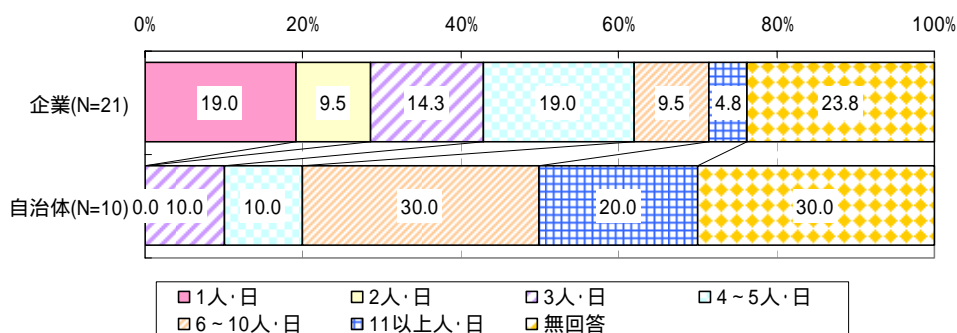
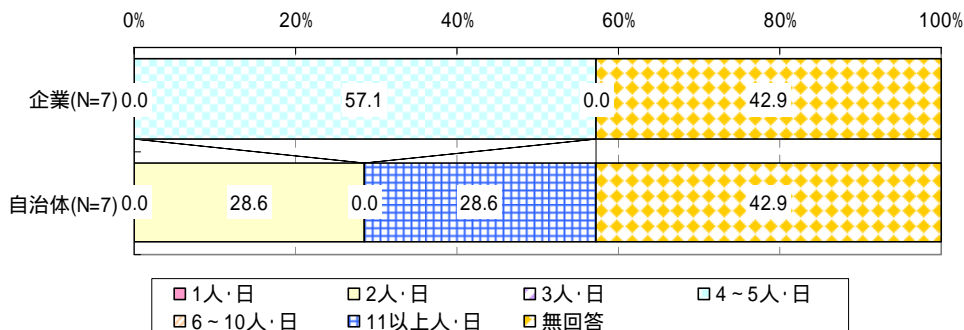


図 2.5-13 対応に要した人員

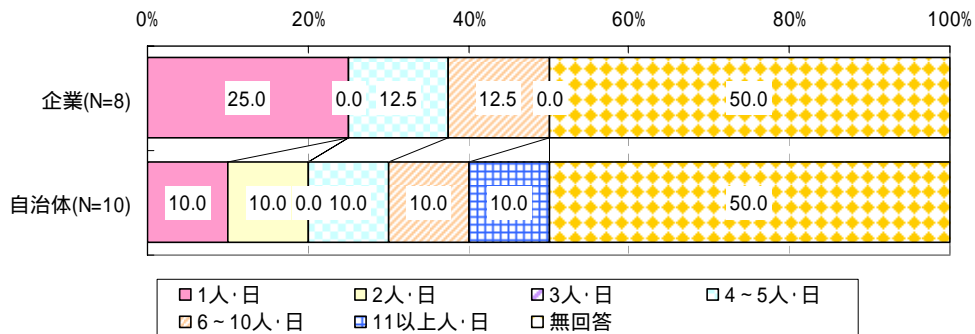
< 原因追求・影響範囲特定のための外部調査 >



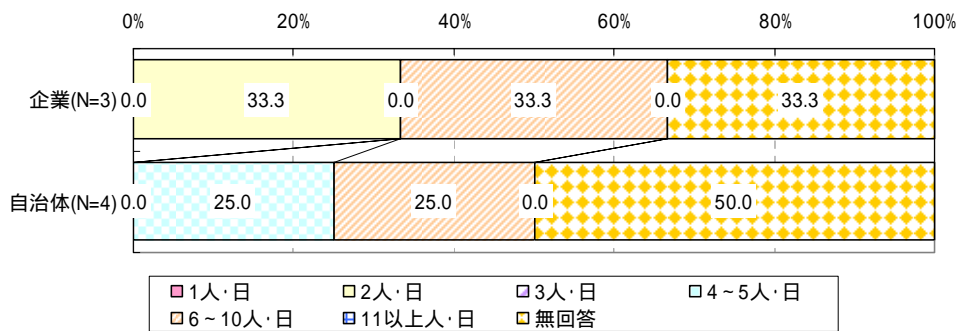
< 問合せ窓口の設置 >



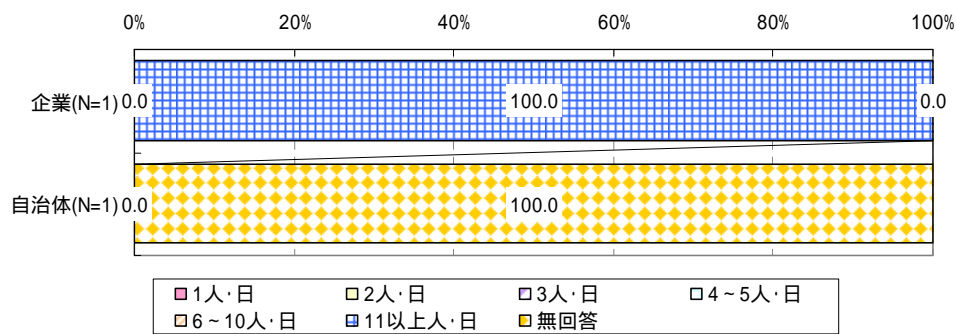
< 電話郵送等で取引先・顧客等へ謝罪 >



< 謝罪広告の出稿 >



< 社内配布する対策用 CD-ROM 作成 >



< その他 >

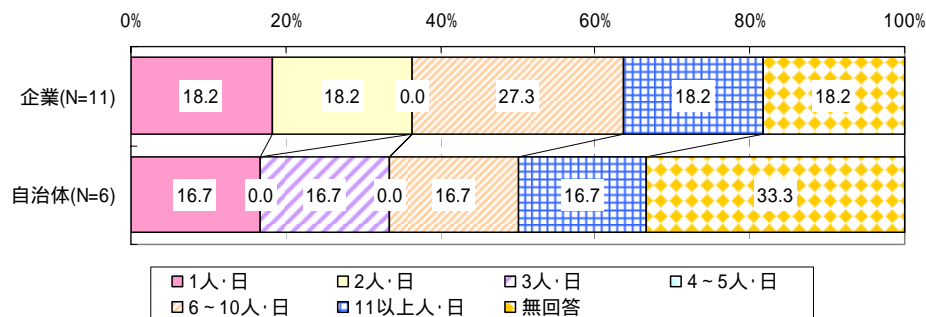
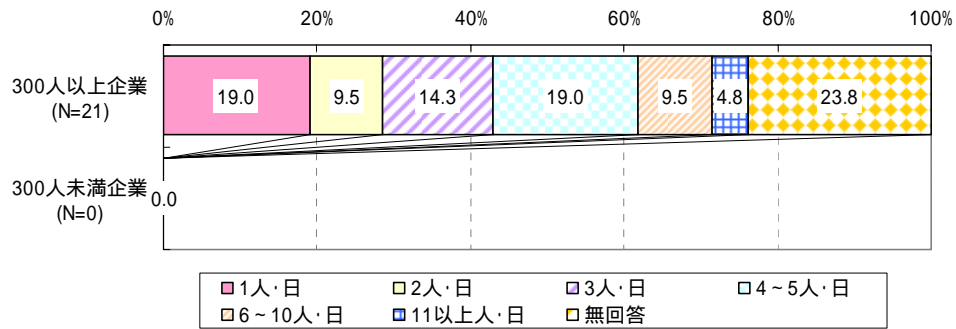
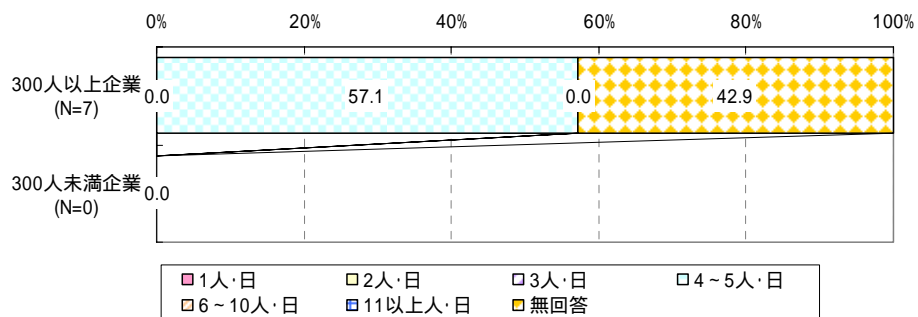


図 2.5-14 対応に要した人員（企業／自治体別）

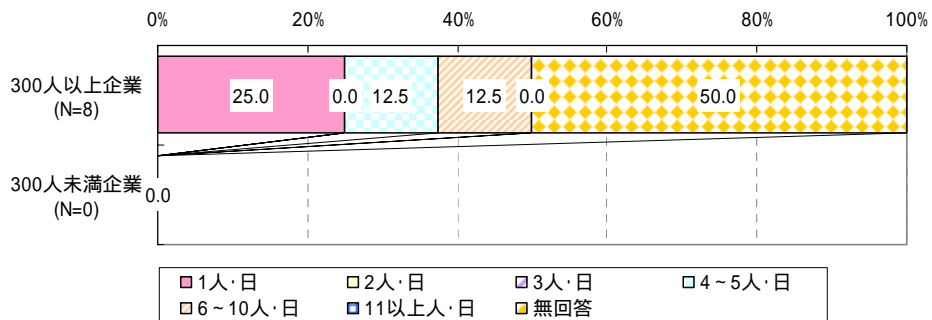
< 原因追求・影響範囲特定のための外部調査 >



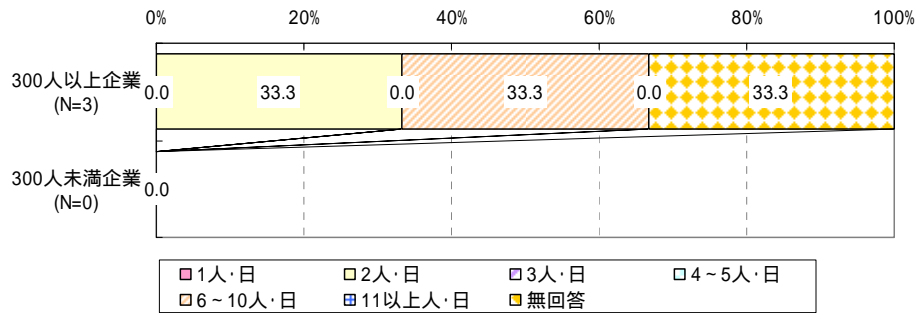
< 問合せ窓口の設置 >



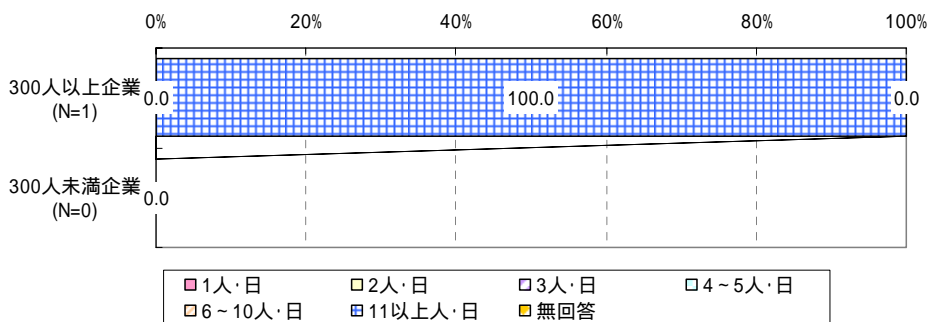
< 電話郵送等で取引先・顧客等へ謝罪 >



< 謝罪広告の出稿 >



< 社内配布する対策用 CD-ROM 作成 >



< その他 >

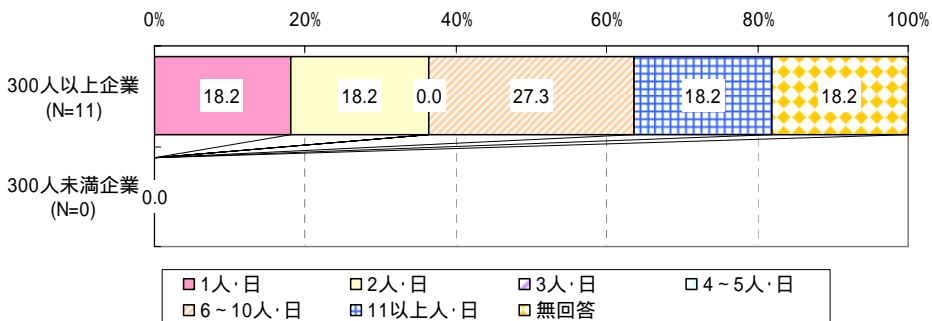


図 2.5-15 対応に要した人員（就業者規模別）

## 2.6. 標的型攻撃による被害について

### 2.6.1. 標的型攻撃の電子メールの有無

標的型攻撃の電子メールで被害を受けた経験があるのは 0.2% である。

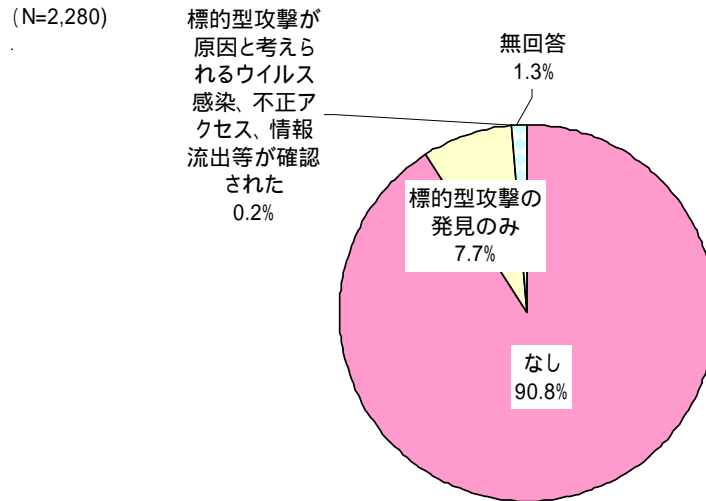


図 2.6-1 標的型攻撃の電子メールの有無

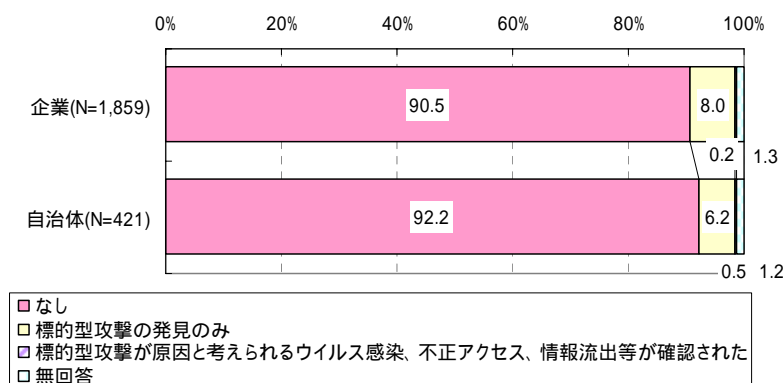


図 2.6-2 標的型攻撃の電子メールの有無（企業 / 自治体別）

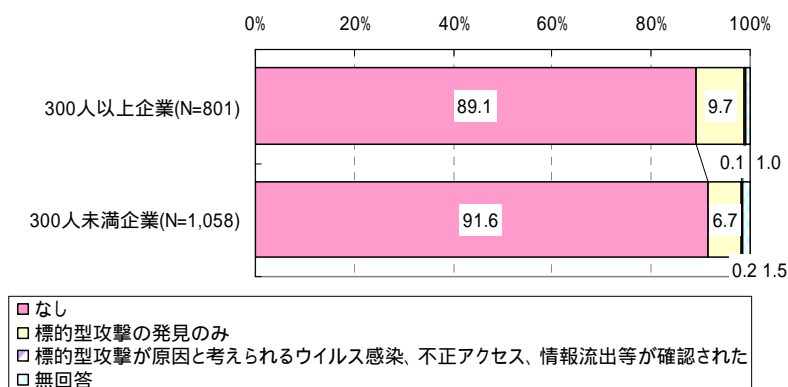


図 2.6-3 標的型攻撃の電子メールの有無（就業者規模別）

## 2.7. その他の脅威について

### 2.7.1. スパイウェアの被害の有無

スパイウェアによる被害経験はあったとする回答はなく、被害が「なし」が76.2%、「発見のみ」が23.0%である。

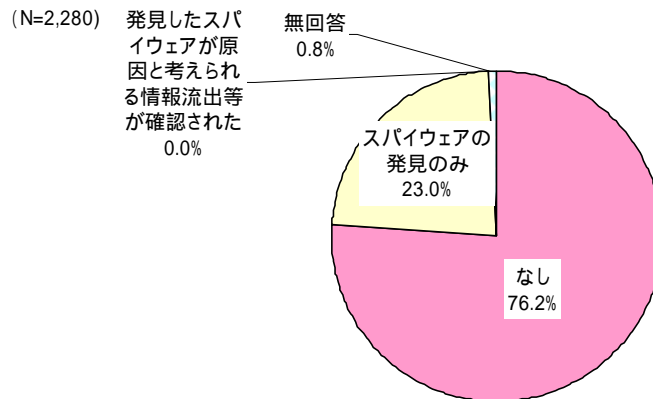


図 2.7-1 スパイウェアの被害の有無

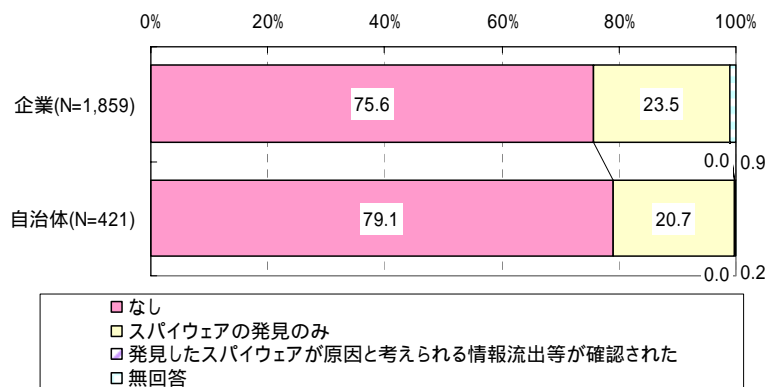


図 2.7-2 スパイウェアの被害の有無（企業／自治体別）

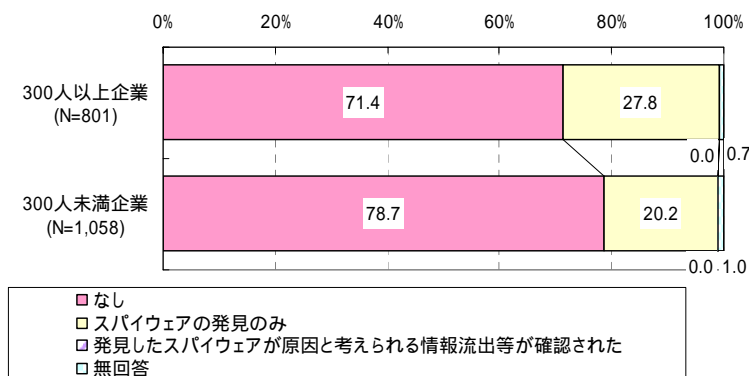


図 2.7-3 スパイウェアの被害の有無（就業者規模別）

### 2.7.2. 発見されたスパイウェアの侵入経路

発見されたスパイウェアの侵入経路は「インターネット接続」が60.7%で最も多い。

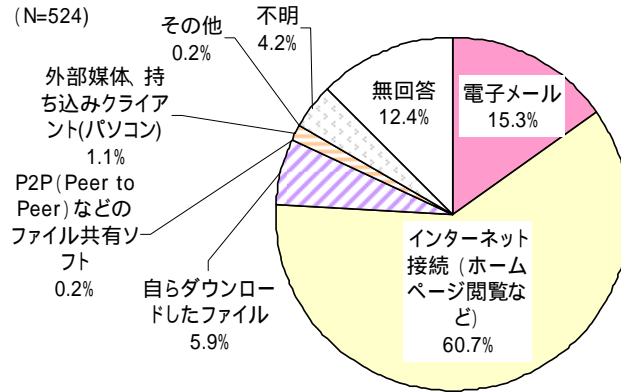


図 2.7-4 スパイウェアの侵入経路

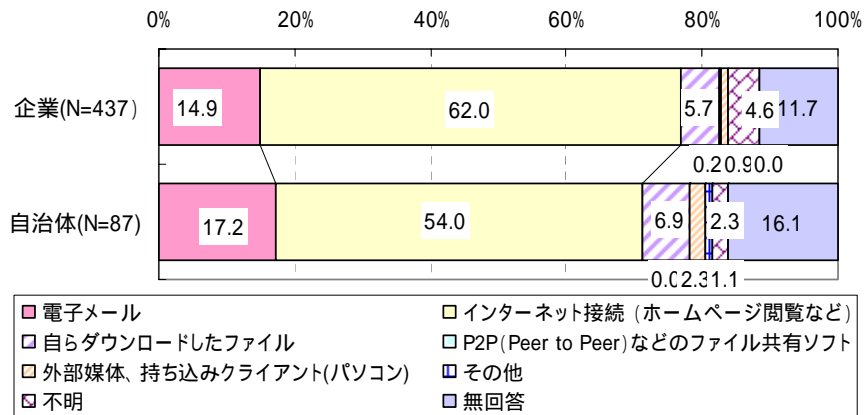


図 2.7-5 スパイウェアの侵入経路 (企業/自治体別)

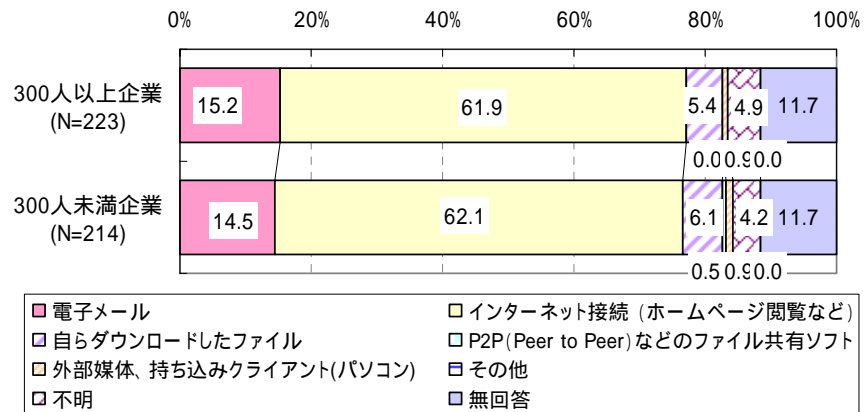


図 2.7-6 スパイウェアの侵入経路 (就業者規模別)

## 2.8. 情報セキュリティ事象に関する間接的被害について

### 2.8.1. ウイルス、スパイウェアによる間接的な被害

ウイルス・スパイウェアによる間接的な被害を受けているのは、被害を受けた組織のうち 1.8% である。

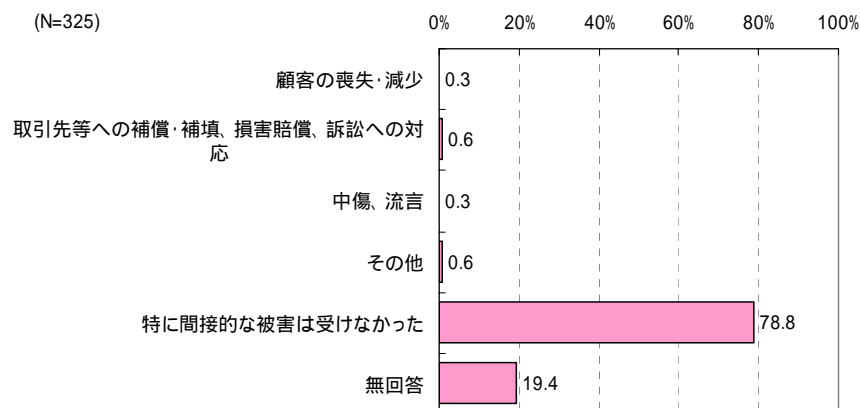


図 2.8-1 ウイルス、スパイウェアによる間接的被害の有無  
(ウイルス、スパイウェアの被害を受けた組織のみ)

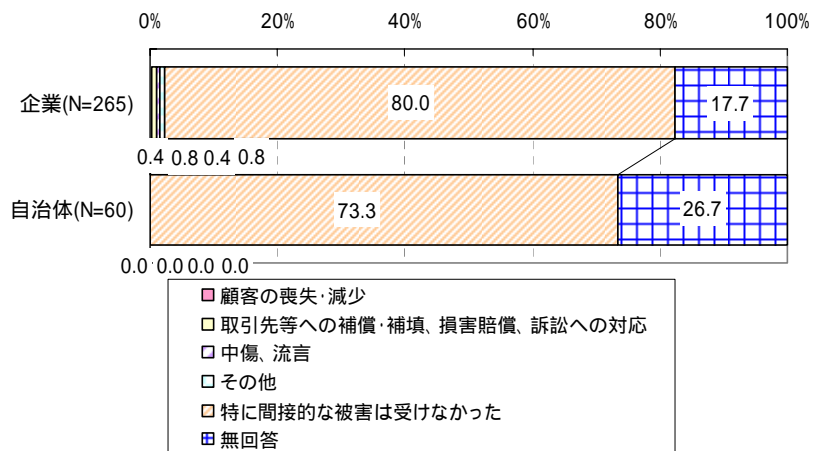


図 2.8-2 ウイルス、スパイウェアによる間接的被害の有無 (企業/自治体別)  
(ウイルス、スパイウェアの被害を受けた組織のみ)

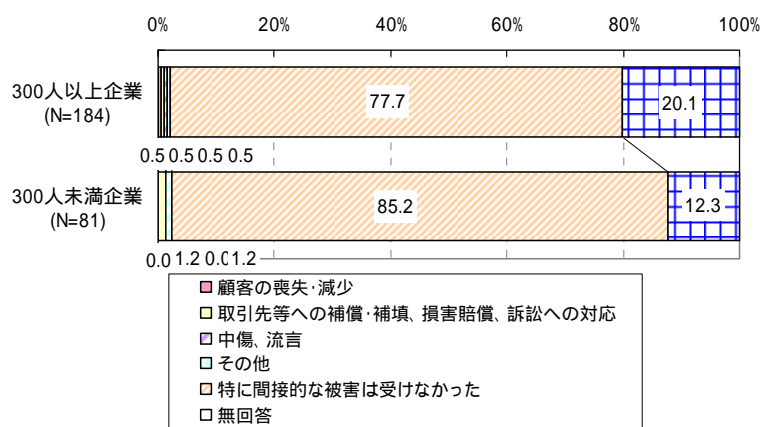


図 2.8-3 ウイルス、スパイウェアによる間接的被害の有無（就業者規模別）  
（ウイルス、スパイウェアの被害を受けた組織のみ）

### 2.8.2. 情報漏えいによる間接的な被害

情報漏えいによる間接的な被害を受けているのは、情報漏えいを経験した組織の 4.7%である。

(N=325)

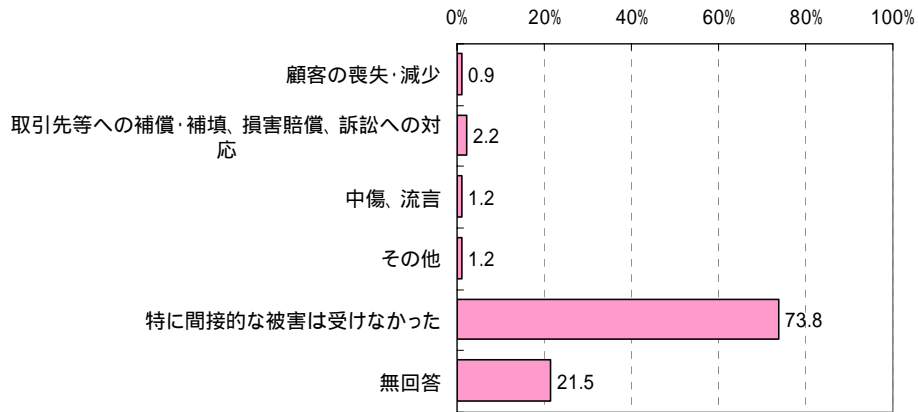


図 2.8-4 情報漏えいによる間接的被害の有無  
(情報漏えいを経験した組織のみ)

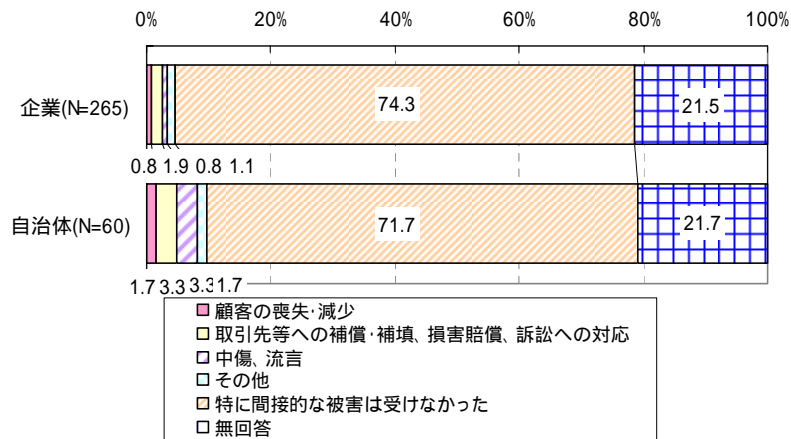


図 2.8-5 情報漏えいによる間接的被害の有無(企業/自治体別)  
(情報漏えいを経験した組織のみ)

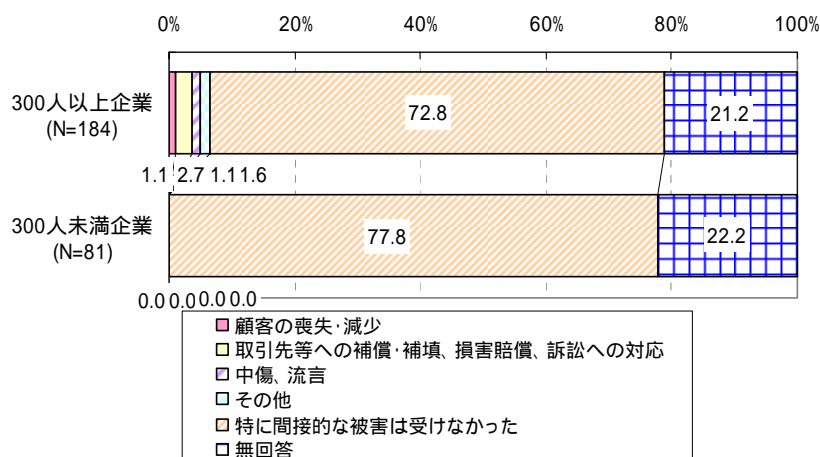


図 2.8-6 情報漏えいによる間接的被害の有無（就業者規模別）  
（情報漏えいを経験した組織のみ）

### 3. 考察

#### (1) ウイルス対策・スパイウェア対策はさらに進展、スパム対策は今後の課題

クライアントパソコンに対するウイルス対策ソフトの導入率は、9割以上のパソコンに導入済みである組織が2005年度調査で約9割に達し、2007年度も同程度の水準であった。ネットワークサーバやローカルサーバに対するウイルス対策ソフトの導入率は、2006年度調査よりもさらに向上している。また、スパイウェア対策ソフトについても、組織の9割以上に導入済みであるのは、クライアントパソコン・ネットワークサーバで5割、ローカルサーバで4割を超え、2006年度調査より1~2割も導入率が向上した。

一方、2007年度より調査を開始したスパムメール対策については、未導入がクライアントパソコンで約5割、ネットワークサーバで約4割にも達している。

以上より、パソコン・サーバにおけるウイルス対策・スパイウェア対策はますます進展している一方、スパムメール対策は今後の課題となっていることが示された。

#### (2) ウイルス遭遇経験は減少傾向にあり、被害も減少

ウイルス遭遇率は、ここ2年間で連続して減少している。また、1組織あたりのウイルス感染件数は1件のみの場合も5件以上の場合も多く二極化の傾向にあると言えるが、感染したパソコン台数は1~4台の回答が最も多いなど感染規模は小さく、直接的な被害は業務停滞やパソコン単体の停止等に留まる。情報管理部門における感染からの復旧作業についても、半数以上の組織が3人・日未満としており、被害の際に外部に支払った費用も0円との回答は多い。さらには、情報セキュリティ事象による顧客の喪失、取引先への損害賠償など、間接的被害についてもほとんどないという結果が示された。

2007年は、前年に引き続き大規模な感染活動を引き起こす新たなウイルスは発生しておらず、組織において遭遇するウイルスの種類も多岐に渡っている。このようなウイルスの発生状況と、

前述した組織におけるウイルス対策が進展した背景もあり、ウイルス感染による被害は軽減されつつあるといえる。

### (3)大・中堅企業や IT 活用度の高い業種におけるセキュリティ対策が進展

VPN やウェブ閲覧のフィルタリング等の情報セキュリティ関連製品やソリューションの導入、情報セキュリティ被害防止のための組織・運用面の対策については、大・中堅企業や IT 活用度の高い業種において実施率が高くなっている。

特に、大・中堅企業（300人以上）においては、重要なシステム・データのバックアップや ID/パスワード、アクセス権限管理の強化、ハードディスク等の廃棄時の破壊など、保有するシステムやデータの管理策について約 7～8 割が実施している。このように、ウイルス感染等の情報セキュリティ被害防止については、大・中堅企業や IT 活用度の高い業種が先行して対策を進めていると言える。

### (4)P2P ソフトウェア等を通じた情報漏えい対策が必要

ファイル共有ソフトを介した情報漏えいの被害経験は 2.2%に留まったが、情報漏えいに対する対応として、原因追及・影響範囲特定のための外部調査、取引先・顧客等への謝罪・問い合わせ窓口の設置等、対応のための延べ人日は 16 人・日以上との回答が 3 割を超えた。また、情報漏えいを経験した組織の 4.7%が、取引先への補償・訴訟対応や、中小・流言、顧客の喪失・減少等の間接的な被害を受けており、情報漏えいが一度発生した場合の損害は非常に大きいものになるといえる。

一方、組織における P2P ソフトウェア等のインストール状況チェックは 6 割近くが未対応であり、顧客情報等の暗号化や検疫ネットワーク等、対応可能な製品の導入率も 1 割程度に留まる。組織においては、P2P ソフトウェア等を通じた情報漏えい対策についても検討することが求められる。

## 4. 情報漏えいに関する被害事例調査

### 4.1. 調査目的

前章までに、アンケートを通じて、情報セキュリティ事象の動向を定量的に把握し、現状の大きな流れを明らかにすることに取り組んだ。

その一方、情報セキュリティ事象が発生した際、個別の原因や起こる事象、必要な対応策、課題など、具体的な内容については、アンケート調査では把握することが困難である。

そこで、情報セキュリティ事象が発生した場合の出来事や対応策、課題等について個別ケースから紐解くため、情報セキュリティ事象の代表例である情報漏えいの被害事例に関するヒアリング調査を実施した。

その際、トラブルシューティングを巡る一連の動きについては現場レベルの観点から把握する必要があるが、被害・影響や体外的な説明を含む対処策については経営的観点からの捉え方が重要と考えられる。そこで、以下の2つのアプローチで調査を実施した。

- (1) 被害発生企業のシステム管理者を対象としたヒアリング調査
- (2) 被害経験のある企業の CIO/CISO 等を対象としたグループインタビュー

(1)については、報道等を通じて、2007 年中に情報漏えいの被害が発生もしくは発覚・公表された企業を抽出し、計 10 社からご協力いただいた。抽出には、以下の視点を設定した。

[ 被害モデル 1 ] 不正アクセスによる情報漏えい

[ 被害モデル 2 ] P2P ウイルスによる情報漏えい

[ 被害モデル 3 ] 内部犯行による情報漏えい

被害モデル 1・2 については各 4 社、被害モデル 3 については 2 社から情報を得た。

(2)については、通常のヒアリング調査では接触が難しい CIO/CISO もしくはその補佐役の層から幅広い意見を得るため、信頼のおける場に同様の立場の人が集まり、匿名を前提に自由に語り合うような形(グループインタビュー)を設定することとし、社団法人情報システム・ユーザー協会(JUAS)の協力を得て、JUAS 主催で会員企業の CIO やその補佐等の層が匿名で参加できる場を開催していただいた。

- ・対 象：被害経験のある国内大手企業 12 社の CIO、CISO、およびその補佐( IT 部門長など)  
第一回(5名)、第二回(7名)の計 2 回開催
- ・方 法：グループインタビュー調査(匿名の座談会)

## 4.2.被害事例調査（ヒアリング）

以下に、被害事例に関するヒアリング調査の結果を示す。

### 4.2.1.不正アクセスによる情報漏えいの被害実態

#### （1）不正アクセスによる情報漏えい時の対応

##### 不正アクセスの顕在化・初動対応

不正アクセスの発覚はインターネット上のサービスを利用する顧客や取引先、関連部署から指摘を受ける場合と、情報システム担当者が定期点検の際にアクセスログの異常に気付く場合の2つのケースがあった。顧客等による指摘の場合、情報システム部門において該当システムのアクセスログを解析し、指摘された不正アクセスが確認された場合、責任者へ報告を行う。情報システム部門における発覚の場合、不正アクセスがあったと確認された時点で責任者に報告する。不正アクセスを受けたことが情報システム部門から報告され次第、被害の拡大を抑えるため、責任者の決定によってサービスを停止する。

##### 被害状況調査

情報システム部門においてアクセスログを調査し、攻撃の詳細（攻撃の種類、攻撃の行われた時間）および不正アクセスを受けたシステムで照会されたデータの種類と範囲を特定する。

特に不正アクセスによって個人情報漏えいした場合は、顧客ごとに漏えいした情報（氏名、住所、電話番号、性別、口座情報、クレジットカード情報など）の組み合わせを明確にして、それに応じた顧客への対応策を、対策委員会で検討する。特にクレジットカード情報、口座情報などが不正に照会された場合は、顧客からの問い合わせが増えることが予想され、カードの切り替えなどの対応についても検討する。不正に入手されたIDやパスワードによってなりすましが行われた場合、該当するIDの持ち主を特定し、本人の協力の下IDの流出経緯を調査する。ヒアリング事例では、個人所有のPCがウイルスに感染したことでID、パスワードが盗まれたというケースがあった。現在、多くの企業においては個人所有のPCで業務ファイルを使用することを認めない方針をとっているが、こうした規定が履行されているか、個人所有のPCに対して確認することは難しく、業種によっては個人所有のPC上での業務を禁止すること自体が難しい場合もある。不正アクセス元や経路、手法など専門的な知識が必要な調査については、警察や情報セキュリティ調査会社などの協力を得て実施する。

##### システム復旧対応

#### （a）実施体制

情報システム部門から不正アクセスの事実が報告され次第、担当役員、関連部門の責任者をメンバーとした対策委員会を組織する。社内の情報セキュリティ規定によりインシデントの対策委員会が既に組織されている場合もあるが、不正アクセス発生時に緊急的に組

織されるケースが多い。対策委員会では情報システム部門からの報告を踏まえ、今後の対応の方針について協議する。

対策委員会の協議と並行して情報システム部門において、初動対応から継続して被害の調査およびシステム復旧対応を行う。技術的な対応については、迅速性を優先して情報システム部門の責任者が対策委員会から決定権を委任されるケースが多い。また中小企業などにおいて、情報システム担当が少人数で対応しきれない場合には、外部の専門機関に対応を委託するケースもある。

#### (b) システム復旧作業

##### ・アクセスの遮断

攻撃が行われた IP アドレスからのアクセスを遮断する。

##### ・脆弱性対策

不正アクセスを受けたコンテンツの修正作業を行う。必要に応じて第三者によるペネトレーションテストを実施する。

##### ・ログインルールの変更

ログイン情報が不正に入手された場合は、既存のログインシステムやルールについて対策委員会で検討を行い、必要に応じて変更を行う。ID、パスワードは一度全てリセットし、全ユーザに不正アクセスの経緯や ID・パスワードの再設定を通知する。

### 対外説明

#### (a) プレスリリース、顧客への説明文書

ヒアリングした企業では、プレスリリースや顧客説明などの対外説明は、できる限り早い段階で、ありのままの状況を報告するという共通した方針をとっている。これらの企業においては、情報を隠したことで事態が悪化した前例もあり、積極的な情報公開が後のリスクを下げるという意識が浸透している。

対策委員会が中心となってプレスリリースの公表、顧客への状況説明について検討を行う。プレスリリースや郵送する説明文書の内容は広報グループを中心に自社で作成し、取締役がレビューした上で確定させる。プレスリリースや説明文書の内容には不正アクセスの経緯と漏えいした情報の件数などを含める。サイトに不正なコード等が含まれていた場合には、不正コードが含まれていたページと期間を公表し、閲覧者に対しウイルス感染の確認や対処を依頼する。不正アクセスを警察に通報している場合、捜査への影響を考慮し、公開する情報の範囲を警察と協議する。混乱を避けるため、ウェブサイト上でのプレスリリースの公開と顧客への説明文書の発送はできる限り同じタイミングとし、内容に関しても整合性を測る。また会員制のサービスの場合、メールマガジンやメーリングリストなどを活用してより迅速な顧客説明を実施する。個人情報漏えいした顧客に対しては説明文書に見舞いとして金券を同封するケースもあった。

#### (b) 問い合わせ対応

顧客や関係者からの問い合わせ対応窓口を設置する。問い合わせはメール及び電話で受け付ける。電話による問い合わせには専用のフリーダイヤルを設置し、被害範囲が大きい場合には専門のオペレータを配置する。問い合わせ窓口の電話番号、メールアドレスはプレスリリースや顧客への説明文書の中で指定する。問い合わせへの回答をオペレータ内で統一させるため、想定問答集を作成する。想定されていない問い合わせがあった場合には、広報で対応を協議する。個別に決定された対応は随時、想定問答集に反映させる。個人情報漏えいした場合、問い合わせの大半は自分の個人情報（特に信用情報）が漏えいしたかについてであるため、問い合わせ窓口において顧客と漏えい情報のリストを共有する。

(c) 指定報告機関への報告

所轄官庁、各種指定報告機関及び警察に事情説明を行い、今後の対応について協議する。不正アクセスの犯人捜査のために、必要に応じてアクセスログなどの参考資料を提供する。

(d) 報道対応

報道機関への対応については、対策委員会で方針を定め、広報において実対応を行う。被害の影響が大きい場合、必要に応じて記者会見を開き、責任者から事実関係を説明する。

(e) 社内説明

対外説明を行う前に、社員に対して不正アクセスの事実関係および会社の今後の方針について説明し情報を共有する。

### 再発防止策

情報システム部門及び対策委員会において、再発防止のために必要な情報セキュリティ対策を検討する。社内で判断しにくい部分については、情報セキュリティ事業者に協力を要請する。システムの構築、管理を外部に委託していた場合、委託業者の適正を改めて協議し、必要に応じて一度契約を解消し新たな業者の選定を行う。

意図的に夜間や休日などを狙った不正アクセスが多く発生しているため、不正アクセス検知システム(IDS)を強化し、異常なアクセスを検知した場合にはリアルタイムに情報システム部門及び担当者にアラートが発せられる仕組みを導入する。公表されている危険な IP アドレスについて情報を収集し、適宜アクセスを遮断する。

DDoS 攻撃に対しては障害検知ツールの導入や帯域を増やすなどの措置をとる。サーバの管理を外部のデータセンター等に委託している場合、不正アクセス発生時に、迅速にアクセスの遮断などの対応をとれるように、データセンター側とインシデント対応を共有する。

ログイン ID およびパスワードの管理に問題があった場合にはワンタイムパスワード、接続時の検疫機能等の対策を導入する。ID、パスワードの管理方法についても社内ルールを周知、徹底する。

## (2) 不正アクセスによる情報漏えい時の対応にかかる費用

### 不正アクセスの顕在化・初動対応

外部からの指摘、アクセスログの異常の検知を受け、情報システム部門において不正アクセス

の状況を確認する。不正アクセスが確認された時点で責任者に状況を報告し、サービスの停止などの措置をとる。人員はサービスの規模や不正アクセスが行われた範囲によっても異なるが、人・日で換算すると0.5～2人・日を要する。

$$0.5 \sim 2 \text{ 人} \cdot \text{日} \times 22,000^{\text{a}} \text{ 円/人} \cdot \text{日} = 11,000 \sim 44,000 \text{ 円}$$

(<sup>a</sup>大企業情報管理部門の件費単価。厚生労働省「平成18年賃金構造基本統計調査(全国)結果より算出)

不正アクセスを受けたサービスの規模が大きかったため、多くの人員が対応にあたり50人・日を要したケースもあった。

$$50 \text{ 人} \cdot \text{日} \times 22,000^{\text{a}} \text{ 円/人} \cdot \text{日} = 1,100,000 \text{ 円}$$

#### 被害状況調査・システム復旧対応

情報システム部門によって不正アクセスの詳細及び漏えい情報について調査を行う。規模の大きいサービスを運営している場合、常駐している外注業者も対応に加わる。被害状況の調査と並行して、情報システム部門を中心にシステム復旧に必要な作業を行う。ヒアリングの事例では、攻撃が行われたIPアドレスからのアクセスの遮断、漏えいした情報の調査、コンテンツの修正、ログインシステムのリセット、ID・パスワードの再設定などの作業が発生した。作業担当人員は不正アクセスの種類によって、システム復旧に要する時間は異なるが、ヒアリングの事例では人・日換算で6人・日を要したケースがあった。

$$6 \text{ 人} \cdot \text{日} \times 22,000^{\text{a}} \text{ 円/人} \cdot \text{日} = 132,000 \text{ 円}$$

社内の情報システム部門のみで対応しきれない場合は、外部の情報セキュリティ調査会社に調査を依頼する。ヒアリングの事例では、調査会社への外注費は200～300万円程度であった。

#### 対外説明

情報公開を迅速に行うため、プレスリリース、説明文書の公開は、不正アクセス発覚から2～3日以内で行われる。プレスリリース、顧客への説明文書の内容は対策委員会が中心となり、広報部門が協議して決定する。個人情報の漏えいが発生した場合、対象者へ個別に説明文書を送付する必要がある。

$$\text{印刷代} + \text{個人情報漏えい件数} \times 80 \text{ 円}$$

漏えいした情報にクレジットカード情報などが含まれる場合、見舞いとして1,000円相当の金券を同封するケースがあった。

$$\text{個人情報漏えい件数} \times 1,000 \text{ 円}$$

個人情報などの漏えいがない場合、メールマガジンやメーリングリストを使って情報を公開する

ことが多い。問い合わせ窓口としてフリーダイヤル等を開設した場合、設置費および通話料の等費用が発生する。またオペレータを配置した場合、その分の人件費が発生する。

問い合わせ窓口のオペレータの人数×231,697円<sup>b)</sup>/人・ヶ月

(<sup>b)</sup> 1人1ヶ月平均派遣労働者受け入れ関係費用。厚生労働省「平成18年就労条件総合調査結果より算出)

#### 再発防止策

サービスの規模にもよるが、ネットワーク監視ツール、障害検知ツールの導入には1,000万円程度の費用が発生する。DDoS攻撃への対策の場合、対策機器の導入に1,200～1,300万円、帯域の確保に200～300万円/月、DNSサーバの切り替えに100万円程度などの費用が必要となる。またログインシステムに脆弱性があった場合、システムを再構築する必要があり、ヒアリング事例の中では800万円程度の費用を要したケースもある。

#### (3) 考察

不正アクセスの手法は年々巧妙化し、今回のヒアリングの事例においても企業側が想定していない隙を突く犯行が多く見受けられた。休日や夜間を狙われたり、複数のサービスを提供する企業の比較的規模の小さいサービスが狙われたりすることによって発覚が遅れるケースや、システムの管理・運営を外部業者に任せられた結果、長期間にわたって不正アクセスに気付かないケースもあった。昔構築されたまま、メンテナンスが行われていないシステムなど、潜在的に攻撃を受けている事例がかなりあると考えられる。

不正アクセスの場合、攻撃側を抜本的に抑え込むことは難しいため、企業側には十分な防衛策が必要となる。具体的にはネットワークの監視ツールの強化、コンテンツの作りこみといった技術的な対策に加え、社内の体制や組織に問題がある場合には社内ルールを再検討する必要がある。

実際にはこうした対策を事前に行うことが望ましいが、情報セキュリティツール等の導入にはまとまった投資が必要である。情報システム部門が不正アクセスの危険性を認識していても、実際の被害がない状態で、経営者に情報セキュリティ対策費の必要性を納得させることは難しい。今回のヒアリングの事例でも、不正アクセスの被害が起こって初めて情報セキュリティ対策費用が計上されたケースがあった。情報システム部門自体もシステムを動かすための最小限の人員が確保されているだけでは、監視や緊急時の対応を十分に行うことはむずかしい。実際に不正アクセスの対応において、情報システム部門にかなりの負担がかかっている現状が見受けられた。企業が提供するサービスの規模および抱えるリスクと情報セキュリティ体制のバランスがとれていない点が不正アクセス対策のボトルネックになっている。

#### 4.2.2. Winny のウイルス感染による情報漏えいの被害実態

##### ( 1 ) Winny のウイルス感染による情報漏えい時の対応

###### 情報流出の顕在化・初動対応

Winny ネットワークへの情報流出は、社外からの指摘、社内のインシデント情報収集・監視体制からの発見報告により発覚する。ほぼ同時に両方の経路から情報が得られた場合もある。情報を寄せる組織・機関としては、取引先、情報セキュリティ関連インシデント等を取り扱う組織、関係官庁等が挙げられる。

情報収集には、ウェブサイト等を対象としてネットワーク上の情報について収集・検索を行うシステムが用いられる。

漏えいさせた者を特定したら、漏えい元の PC をネットワークから切り離し、そこに保存されているファイルを確認して流出した情報の範囲を明確化する。漏えい元が個人所有 PC である場合には調査および被害拡大防止への協力を所有者に求める。

対応実施体制については、意思決定のための組織として担当役員、広報部門、人事部門、情報セキュリティ関連部門、法務部門等に流出元部門が含まれる少人数の対応チームが組まれている。事後の対策についても基本的にはこのチームで一貫して検討にあたる。

調査作業を担当するチームは意思決定のチームとは別に作られる。IT に強いシステム担当部門や外部ベンダの数十名が集められ、人手が必要な調査作業を集中的に行う。

対外的に公表するタイミングまでは漏えいに関する情報は上記の関係者限りとされる。

###### 被害状況調査

流出した全データについて、セキュリティ関連部門を中心にした調査作業担当者らが精査にあたり、含まれている個人情報を特定する（氏名、住所、電話番号、電子メールアドレス等の種別および数を明確化する）。さらに他のデータベースや名刺情報等と照合しながら連絡先リストを作成する。ヒアリング対象事例では数万点のファイルについて社から持ち出した情報に該当するかを確認の上で個人情報を抽出した場合もあった。

漏えいの原因として、個人情報を含むデータを持ち帰り、自宅で個人が所有する PC に保存した後に Winny を利用し、ウイルスに感染することにより情報が漏えいするケースが多く見られる。個人情報に関する取扱・対策を強化する以前に持ち帰られたデータが漏えいしている事例が複数あるが、効果的な対策は難しい。

漏えい情報については、住所録のように個人情報のみが集積されたファイルではなく、個人情報が断片的に含まれる業務日誌や、公開企業情報を整理して作成した営業用情報の漏えいが報告されている。これらから個人情報を抽出し明確化するためには多大な労力が費やされている。

###### 対外説明

対外説明は対応チームが決定したスケジュールに沿って行う。これは漏えいした相手への謝罪

と説明、取引先や顧客への説明、問い合わせ対応、ホームページへの掲載、プレスリリース、関係省庁やセキュリティ関連団体等の届出先への連絡と事情説明が含まれる（ただし第一報の通報がこれらから寄せられた場合には状況連絡を公表前に行うこともある）。対応と直接関係が無い社内部署に対する説明も対外説明と同時に行う。

可能な限り迅速に事実関係を示すことが望ましいが、一方で、公表によって新たな関心を集め、漏えい情報が Winny でより多くダウンロードされる危険性もある。さらなる被害を誘発しないよう最善と思われる措置を取る。また、事実関係の調査、公表後の対応の準備および緊急対策の状況を踏まえてスケジュールを調整する必要もある。

メッセージする内容としては、お詫び、確認した事実の説明、対応状況についてであり、伝達内容を揃えるために広報部門が全公表情報の作成・確認にあたる。情報が流出した相手への謝罪と事実説明の方法は、流出した情報の種類や数、流出元の業態により異なる。顧客・取引先への説明についても対応に割く人員や内容には幅が見られる。

営業情報が流出した場合には、含まれる情報が取引の無い企業や個人の情報である場合もある。また、古いデータが漏えいした場合には連絡先等が既に無効であることもある。これらの場合でも可能な範囲で対応を行う。

問い合わせに対応するためのフリーダイヤル等の設置は、漏えいの実態に合わせて考慮される。漏えいを起こした地方支社の現地状況に詳しいスタッフを説明にあてる場合もある。想定問答集、責任者が呼び出された場合のエスカレーション等についても事前準備が必要となる。

#### 再発防止策

対外説明と同時期に再発防止のための緊急的な対策を実施し外部にも公表する。また、その後、より長期的視点に基づいて従業員教育や IT 基盤の整備といった対策を実施する。

全従業員あるいは対策強化が必要とみなされる一部の従業員に対しては、社内で使用する PC への Winny 等のファイル共有ソフトウェアを利用しないことを徹底するため、インストール状況の確認（検索）と削除を行うソフトウェアの適用を求める。

持ち出された情報が個人所有 PC に保存され漏えい元となるため、この点に関して複数の対策が複合的に実施される。

企業が保持する個人情報の見直し、個人情報の持出しの禁止や制限、個人所有 PC への業務情報（個人情報）の保存の禁止等のルールを改めて明確化し、従業員に徹底を促す。

個人所有 PC の業務利用を禁止する場合もある。ヒアリング事例では禁止だけでなく、適切な作業環境を整えることを重視し、従業員にノート PC 等を新たに支給している場合もあった。

個人所有の PC に保存された個人情報については、検出 / 削除ツールを全従業員に CD-ROM 等で配布して自宅での実行を求める場合もある。より強い要請を従業員に行う場合としては、自宅で業務に用いる PC からのファイル共有ソフトウェアの削除（使用停止）を求めるケースもある。

社員教育については、個人情報および情報システムの取扱いに関する既存のルールの再確認と遵守徹底が促される。長期的な視点からはファイル共有ソフトウェア等の利用に伴う危険性等情報リテラシおよびモラル向上に関する教育も行われる。

この他、ヒアリング事例に見られた対策を以下に示す。

- ・ 社から提供する PC においてファイル共有ソフトウェアを利用しない旨や、不適切な PC 利用を行わない旨を記した誓約書の提出を従業員に求める。
- ・ DVD-R や USB 等の外部記録媒体の利用制限・禁止を行う（許可制とする場合や、利用時に自動的に警告や記録を行うシステムを導入する場合がある）。
- ・ 個人情報の持出状況の把握やセキュリティ対策の徹底を考慮し、シンクライアントの導入を長期的な PC 整備計画の一環として検討する

また、対策方針および具体的対策を定めるにあたり、外部の専門家を含む諮問委員会を作り、事件の分析と対策検討を行う場合もあった。

## （ 2 ） Winny のウイルス感染による情報漏えい時の対応にかかる費用

### 情報流出の顕在化・初動対応

外部からの指摘、自社の監視体制からの報告を基に、情報システム部門において漏えい事実の確認と流出元の特定を行う。可能であれば流出元となった PC で流出した情報を正確に把握する。

流出したデータに個人を特定可能な情報がどの程度含まれるか、社内システムに保存された情報との比較対照が可能か等によって、流出元特定に要する時間には 3 時間から約 1 日まで幅が生じる。ある事例では流出元の特定までに約 1.5 人・日を要していた。

$$1.5 \text{ [人・日]} \times 22,000^{\text{a}} \text{ [円/(人・日)]} = 33,000 \text{ [円]}$$

（<sup>a</sup> 大企業情報管理部門の件数単価。厚生労働省「平成 18 年賃金構造基本統計調査（全国）結果より算出）

### 被害状況調査

情報システム部門等から集められた人員が、流出データに含まれる個人情報の精査と通知先リスト作成の作業を行う。また、並行して対外公表に関する準備作業と緊急対策が行われる。

個人情報の精査に必要な作業量は、流出したデータの性質や量によって異なる。ヒアリングの事例では、人・日換算で 15 人・日を要したケースがあった。

$$15 \text{ [人・日]} \times 22,000^{\text{a}} \text{ [円/(人・日)]} = 330,000 \text{ [円]}$$

業務日誌のようなデータが流出した場合には抽出と確認作業により多くの手間がかかる。また、業種・業態によっては確認に慎重を期すため多くのコストをかけている。ヒアリング事例には、40 名体制で 1 日半の作業で調査にあたった事例もあった。

$$60 \text{ [人・日]} \times 22,000^{\text{a}} \text{ [円/(人・日)]} = 1,320,000 \text{ [円]}$$

対外公表の準備や緊急対策のために、対応チームが活動にあたる。ヒアリング事例には、およそ 5 名の管理職が 3 日ほどの作業にあたった場合があった。

$$15 \text{ [人・日]} \times 42,000^b \text{ [円/(人・日)]} = 630,000 \text{ [円]}$$

(<sup>b</sup> 部長以上の人件費単価。厚生労働省「平成 18 年賃金構造基本統計調査(全国)結果」より算出。)

#### 対外説明

謝罪および説明のための訪問に要するコストは、漏えい件数、取引先の件数にもより幅が生じうる。ヒアリング対象の事例では、およそ 40~70 人・日を費やしていた(1 件の訪問対応に 0.3 人・日が必要となるとみなして導出)。以下に営業職等の一般社員が対応にあたる場合の試算を示す。幹部社員が対応する場合には数倍となる可能性がある。

$$40 \sim 70 \text{ [人・日]} \times 22,000^a \text{ [円/(人・日)]} = 800,000 \sim 1,400,000 \text{ [円]}$$

郵送による説明とお詫びについては、お詫び、再発防止策の概要などを順次報告する場合には 3 回程の連絡となる。また、件数に応じた印刷費も必要となる。

$$\begin{aligned} \text{対象者数 [件]} \times 80 \text{ [円]} \times 1 \sim 3 \text{ [回]} + \text{印刷費用 [円]} \\ = \text{対象者数 [件]} \times 80 \sim 240 \text{ [円]} + \text{印刷費用 [円]} \end{aligned}$$

問合せ対応電話としてフリーダイヤル等を設置する場合にはその費用が発生する。漏えい元の部署や広報部門が担当する場合が多い。ヒアリング事例では、漏えい元の関連部署が 20 人体制で 2 週間の対応にあっていた。

$$20 \text{ [人]} \times 14 \text{ [日]} \times 22,000^a \text{ [円/(人・日)]} = 5,600,000 \text{ [円]}$$

この他にお詫びとして漏えいの対象者に金券等を配布する企業もある。

#### 再発防止策

個人所有の PC へのデータの持ち帰りに関する対策としては、ルールの再確認と徹底を求める他に、持ち帰られた個人情報等を検索し削除するツールを配布する対策が挙げられる。従業員数に応じた配布数の準備が必要だが、ヒアリング対象の事例では 10,000 枚の CD-ROM を作成するために 80 万~90 万円の費用をかけていた。

自ら私用のアカウントに宛てて添付ファイル付きのメールを送ることで情報を持ち出す場合があるため、社内から社外へのメールを監視・記録する対策も有効である。100 ライセンス規模のメールフィルタリングソフトウェアは約 100 万円の費用がかかる。

ネットワークへの情報流出を検出するために自社関連情報の流通を常時監視するチームとシステムを新たに備える場合にもコストが必要となる。情報セキュリティ部門あるいは関連会社の数名で構成する。ヒアリング事例では 2~3 名体制で常時監視を行っている場合があった。

$$2 \sim 3 \text{ [人]} \times 365 \text{ [日/年]} \times 22,000^a \text{ [円/(人・日)]} = 16,060,000 \sim 24,090,000 \text{ [円/年]}$$

### (3) 考察

Winny を介した情報漏えい被害が幾度となく報道され、そのリスクも十分に周知されつつあると思われるが、依然として同様のトラブルの公表が続いている。企業内の情報システムへの Winny 対策が進み、社内でのウイルス感染による漏えい事件の発生は抑制されつつあると考えられるが、ヒアリングでは、過去に持ち出され個人所有の PC に保存された情報が Winny の利用を契機に漏えいするケースが見られた。したがって対策としては、情報持ち出しの監視・制限等の対策を実施するだけでなく、ヒアリング事例のように、個人所有 PC から業務に関する古い情報を削除するよう従業員に協力を求め、必要に応じて持ち帰られた個人情報等を検索・削除するツールを配布するなどの対策が望まれる。

また、ヒアリング事例のように、個人所有 PC の使用禁止に合わせ新たな PC を支給する形も考えられるが、それがコスト的に難しい場合には、個人所有 PC を用いて業務が行われている実態を企業の経営層が直視し、セキュリティ上のリスクを認識した上で、個人所有 PC の業務利用について自社の方針を明示し、その順守を従業員に促すことが重要である。

さらに、ヒアリングでは、シンクライアントの導入、社内から社外へのメールの監視・記録、自社関連情報の流通の常時監視などの手段が挙げられているが、これらの採用には企業の IT 利活用の成熟度が高いことが望ましい。

#### 4.2.3. 内部犯行による情報漏えいの被害実態

##### (1) 内部犯行による情報漏えい時の対応

###### 内部犯行の顕在化・初動対応

内部犯行か否かによらず、個人情報の場合、不正取得された個人情報が流通したり悪用されることをきっかけとして社外から問い合わせがなされ、問題発覚につながることも多いと見られる。ヒアリング先のケースでも、通報をもとに所管省庁が報告を求めたことが発端となっていた。一方、営業秘密（研究開発データ、設計情報、製法ノウハウ等）の場合には、競合企業で秘密裏に活用されるため、漏えいの事実が発覚する可能性はより少ないと考えられる。

ヒアリング先のケースの場合、従業員が付与された、もしくは本来は与えられていないはずのアクセス権を悪用して、機密情報にアクセスし、不正に情報を取得した形である。いずれのケースも、まず漏えいした情報を照会し、それが自社の機密情報である事実を確認した上で、社内の機密情報に関するアクセスログの分析とヒアリング調査を行うことにより、不正行為の実態を明らかにしている。

危機管理体制は、意思決定を行う役員中心の本部と、問題の性格に合わせて割り付けられる実務担当メンバー（社員）で構成される。

危機管理体制の発動はポリシーによって異なる。具体的には、情報漏えいの可能性があることがわかった時点ですぐに危機管理本部を召集し、対応方針を検討するパターンと、まず現場レベルで調査を行い、問題が発生していることが判明した時点で危機管理本部を設置するパターンがある。

###### 被害状況調査

まず、漏えい情報が自社のものであるかどうかを検証する。個人情報の場合、個人データのリスト構成、また、個人データに割り付けられている ID 番号や属性情報の構成、記載内容、表現等について、自社の保有する個人情報と比較して判断することになる。

漏えいした情報が自社の機密情報であることが判明した場合、事実関係の把握に取り組む。具体的には、自社の機密情報に関するアクセスログの分析を行い、不正行為を行った人物とその経緯を特定する。対象者をある程度絞り込んだ段階で、法務担当、人事担当、セキュリティ担当など危機管理の実務スタッフが本人や周辺に対するヒアリング調査を行い、不正行為を行った人物を特定する。

不正行為を行った従業員は、雇用契約に基づき、懲戒解雇または契約解除する。そのためには、そうした違反行為と懲罰の明文化、ならびにその周知が重要である。

###### 対外説明

###### (a) 指定通報機関への報告

判明した事実に応じて、警察や所管省庁、認証機関（プライバシーマーク取得企業の場合

合)等に届け出る。事件性がある場合には、捜査のために必要に応じてアクセスログなどの参考資料を提供する。ただし、情報のみ持ち出されたため、現行法では立件できないケースもありうる。

また、所管省庁からの報告要請があった場合には、調査結果を踏まえた事実関係について報告し、その後の対応について協議することになる。

#### (b) 本人への通知

個人情報漏えいの場合には、個人情報保護法ガイドラインに基づき、該当する顧客本人に漏えい事実を通知する。特に内部犯行においては、不正な持ち出しの目的が明確であり、二次被害の危険性が高い点に留意すべきである。

#### (c) 公表・問合せ対応

個人情報漏えいの場合、公表のあり方については事業者の自主的な判断に委ねられており、社会的影響や顧客への周知の徹底、事件性等を鑑み適切な判断がなされることが望まれる。

プレスリリースを行う場合には、同時に、フリーダイヤル等の専用の対応窓口を設置し、問合せを受け付ける体制を整える。ヒアリング先の場合、ピーク時の問合せは数百件に達したが、その大半は自分が情報漏えいの被害者に該当するかどうかを確認する顧客で、訴訟に至るケースは見られなかった。

### 再発防止策

再発防止策としてまず重要なのは、アクセス管理の整備と運用である。たとえば、コンテンツ単位で所属部署や役職によるアクセス権限を設定し、従業員からの参照要請に対し、その可否を従業員のIDから判断するしくみを導入する。また、組織の改編や人事異動、離職等に対応して適切なタイミングで設定変更を行うよう、運用時のメンテナンス体制を確立しておく必要がある。

また、従業員が正規のアクセス権を保有している場合、技術的対策だけで不正目的のアクセスを防ぐことは難しい。したがって、アクセスする情報を書面で事前申請しログと付き合わせる、機密情報へのアクセスを常時モニタリングし適切と判断されたアクセス以外のケースについて適宜確認するなど、作業手続の面での対策を強化することも重要である。加えて、社員教育の強化、アクセス権を有する従業員やアクセス可能な端末の絞込みも有効である。

なお、個人情報の場合、アクセス管理等の適切な情報セキュリティ対策を実施し、安全な環境を確保していなければ法律違反となる(個人情報保護法の安全管理措置義務)。また、営業秘密を持ち出し競合他社に渡す等の不正行為から守るためには、営業秘密として認められる要件を満たす必要がある(不正競争防止法)、そのための秘密管理性の確保が前提となる。

### (2) 内部犯行による情報漏えい時の対応にかかる費用

#### 内部犯行の顕在化・初動対応及び被害状況調査

流出したデータと社内の機密情報との比較作業、および社内のヒアリング調査等について、事例では約200人・日を要していた。

200 [人・日] × 22,000<sup>a</sup> [円/(人・日)] = 4,400,000 [円]

(<sup>a</sup> 大企業情報管理部門の件費単価。厚生労働省「平成 18 年賃金構造基本統計調査(全国)結果より算出)

また、ヒアリング先では情報の突合せ作業に数千名程度が関わり、膨大な件費を要したケースもある。

#### 対外説明

情報漏えいの対象者への詫び状などの送付のほか、問い合わせ窓口としてフリーダイヤル等を開設した場合、設置費および通話料の等費用が発生する。ヒアリング先では約 1 ヶ月間窓口を開設していた。

またオペレータを配置した場合、その分の件費が発生する。

問い合わせ窓口のオペレータの人数 × 231,697 円<sup>b</sup>/人・ヶ月

(<sup>b</sup> 1 人 1 ヶ月平均派遣労働者受け入れ関係費用。厚生労働省「平成 18 年就労条件総合調査結果より算出)

#### 再発防止策

ヒアリング先では、内部犯行を防ぐためのアクセス管理の強化策として、機密情報へのアクセスの適切性を自動判定するための環境を数千万円で構築することを検討しているケースがあった。

#### (3) 考察

外部からの攻撃にはツールを活用して防御を固めることが重要であるが、内部犯行による情報漏えいについては通常業務の遂行上単純な防御策が適用困難である。ヒアリング事例では、アクセス権の徹底(従業員・端末)や従業員へのモラル教育によるリスク抑制といった従来型的手段に加え、業務処理プロセスにおいて不正行為が困難な構造(アクセス対象についての事前申請とログチェック、アクセスの適切性の自動判定装置等)を整備するなど、これまでとは異なる観点の対策を適用することを選択している。

ヒアリング事例では派遣社員による犯行のケースを扱ったが、ヒアリング先からは「正社員と派遣社員・アルバイトの間でモラルに格差があるという見方は一方的」との意見も得られた。違反行為と懲罰を明文化し、雇用契約に盛り込むとともに従業員に周知徹底するといった取組みが重要と考えられるが、悪意のある従業員の犯行をどこまで抑制できるかは疑問が残る。今のところ、どのような形で統制を効かせるべきか、明確な成功事例が乏しく、各社が最適解を模索している状況といえる。また、内部犯行の場合、被害者(企業)と被疑者(従業員)の関係や捜査上の制約から情報開示が進みにくいため、経験・知見を共有することが難しいという問題もある。

なお、今回のヒアリング調査では明らかにすることができなかったが、営業秘密の管理は現場の運用ルールに任されていて、厳格なアクセス管理やアクセスログの保全がなされていないケースも少なくないと推測される。この場合、情報を不正に持ち出されてもそれを発見することは困

難で、発見できたとしても不正競争防止法を適用できない可能性があることから、企業は重要情報について社内横断的なたな卸しを行い、その種類や量、管理状況の把握に着手すべきであろう。

#### 4.3. 情報漏えい等に関するグループインタビュー調査

以下に、情報漏えい等に関するグループインタビュー調査の結果を示す。

##### 4.3.1. 情報管理の考え方

###### (1) 情報資産の分類

- ・ 何のために情報を守るのかをまず考えている。営業機密は持っていかれて同じことをされたら自分たちの会社が困るから守る。個人情報と漏れると人に迷惑をかけるので守る。守る目的によって仕分けも啓発の仕方も違ってくると認識している。
- ・ 個人情報も営業秘密も両方とも大事である。やり方は違ってくるが、漏えいした結果は同じである。個人情報は漏えいするとその人に迷惑を掛けるのだが、営業秘密は「漏らしました」と言った途端に自分たちの損害になる。
- ・ 漏えいした情報がお客様のものではないものとしても、「あの会社が」ということで不信感を持たれ、信頼感をなくし、「大事な自分の情報を預けているのに」と不安にさせてしまう。最終的には会社の情報も顧客の情報も同じである。
- ・ 個人情報のなかで大きいものは社員の給与情報・人事情報である。会社の生産のノウハウが漏れることはあっても、情報漏えいによって第三者に直接迷惑を掛けることは少ないと認識している。
- ・ 機密情報とは会社の機密であり、経営管理情報である。問題は重要情報で、部門間で差がある。各部門が重要だと思ったものが重要情報であるということに対応している。
- ・ 情報漏えいが発生したら、会社の名前が出てしまうという意味で、どんな情報でもすべてが重要な情報と社員には説明している。紙1枚でもだめということになっている。協力会社については、「協力会社に渡すときに意識して渡し、取り扱う」という意味で重要情報を決めている。何が重要情報であるかということについては、仕事をする部門に決めさせている。IT部門が決めるものではない。

###### (2) 情報管理体制・方針

- ・ 社内的には、規定 - 規則 - 基準という体系である。情報管理規定は経営企画部門が策定していて、紙文書と紙以外に分かれている。IT部門は情報セキュリティ基準（いわゆる電子データの管理規則を作成していて、その下にITセキュリティ基準があり、そのなかで情報セキュリティを管理している。情報には、機密情報（企業情報いわゆる経営管理情報）、一般的な重要な情報、個人情報の3種類があるという形である。
- ・ われわれは、個人情報を持っている会社や顧客から情報を扱ってデータをプロセッシングする業種とは違うから、身の丈にあった情報セキュリティをしていけばよいと考えている。

- ・ BtoC のビジネスがほとんどなので、社内では情報セキュリティと個人情報保護がほとんど同義になっている。
- ・ BtoC の取引が多いことから、個人情報には特に厳密に対応している。CPO (チーフプライバシーオフィサー) を設置している。個人情報に関しては紙情報であろうと電子情報であろうと、何かあれば CPO に報告する。監督官庁への報告等も CPO が行う。これだけは徹底している。これとは別に、全般のリスクマネジメントは CRO (チーフリスクマネジメントオフィサー) が行うが、CRO の下に法務や内部統制の部門があるので、CIO の責任がだいぶ分散されている。
- ・ 情報セキュリティの組織を強化しているが、個人情報への対応が中心で、技術情報が今後の課題である。本来はもっと早く行うべきだったが、なかなか手が付けられなかったという状況である。
- ・ 情報漏えいは IT の問題ではなく、情報の問題である。情報管理規定は IT の規定ではなく、経営企画部門すなわち中枢部門が管理すべき。情報のなかには電子情報と文書がある。電子情報の管理についてはわれわれ IT が担当するが、情報がどこかで漏れたら IT 部門が対処するということはあり得ない。
- ・ 紙媒体は総務が管理している。電子データは IT 部門が管理する。
- ・ 情報セキュリティの管理規定は IT 部門が見ている。紙媒体による情報を紛失した場合も含めて IT 部門が最終的には責任をとる。
- ・ IT 部門が紙媒体も含めて管理している。ただし、情報資産の所有者は各部門であり、各部門が責任をとることになっているのだが、その意識が定着しなくて苦労している。
- ・ 現場とタイアップはするが、監督官庁への報告などはすべて IT 部門が行う。これまで、事故が起きた際は、IT 部門が全社に対して号令をかけて対策を呼びかけている。

#### 4.3.2. 経営的観点から見た情報漏えい等の被害・影響

##### (1) 情報セキュリティについての基本的な考え方、方針

- ・ 人は善いとか悪いとか決め付けられるものではないが、弱い人がそれをしようと思えばできるという状態にしておくほうが悪い。できないように手立てを講ずることが、会社として情報を守るということと同時に、結果としてその人を守ることになる。
- ・ 個人情報ばかりが注目されている。ただ、当社は個人情報の塊であり、個人情報の漏えいは死活問題であるため、個人情報の情報管理の強化を進めている。
- ・ 内部の人間に対しては従来考えられていた対策だけでは守れないが、どこまで行うかは情報の種類によって異なる。どこまで行うにしても、確かに内部の人間の不正を防ぐためには、それだけの対策を講じなくてはならないのだが、結局はあなたを守ることになるという考え方を理解してもらう必要がある。対策は継続させなくてはならない。無理なことは続かない。納得が得られなくては続かない。考え方を納得してもらえるように常に改善していく必要がある。
- ・ セキュリティの教育は繰り返し行っているが、最後は人間に頼るしかない。「皆さんの倫理観・責任感が頼りである」という言い方でモチベーションを上げてもらうしかないというのが正直なところである。そうしなければ業務として成り立たない。

##### (2) 情報漏えい等の発覚から再発防止策まで

- ・ イベントの企画・運営を行う子会社で情報漏えいが発生した。出入りしていた委託先の社員が、データのやりとりのため個人名義でサービスプロバイダのサーバを借りて仕事をしていて、そこから情報が漏えいした。外部のサービス利用を禁止すると、仕事が進まないため隠れて利用するようになるので、現在は申告制にしている。ただし、子会社に入出入りする委託先の社員には強制できない。子会社にどのように守ってもらうか、さらにその委託先をどう管理するかが課題。
- ・ 中国で事務員の PC がウイルスに感染した影響で、日本の工場の在庫管理システムが停止した。弱いところに影響が出てしまう。海外は対応が難しい。
- ・ 一旦発生すると、被害は甚大。社内のネットワーク全体、さらに得意先にも影響する。
- ・ ウイルス対策を徹底していても毎日 1 件ぐらいは事故が起きているが、ウイルス対策をサーバで管理するようになって以前のように二次感染はしなくなった。
- ・ ホームページ上で顧客のデータを削除してしまったという事故に対して、業務プロセスを変更することで再発を防いでいる。
- ・ 携帯型 PC を年に数台ほど盗まれることが続き、事業所が携帯型の PC を持ち歩くことを禁止するようになってきた。本社は許可すると言っているのだが事業所が嫌がっている。携帯

電話のメールだけが見られるようにしている。

- ・ まじめな社員が金曜日の夜に、仕事が終わらなくて、仕事を自宅でしようと思って PC を車に乗せて持ち帰り、駐車場に置いているうちに窓ガラスを割られて PC を盗まれた。持って帰ること自体が問題だが、悪気でやったことではない。まじめに仕事をしようとして持って帰るような人を悪者にしないために、見える管理をするという考え方を進めている。
- ・ 再発しないよう改善しなければ会社が生存できなくなるということで、有無を言わず行った。外部の専門会社に見てもらったところ、厳しい意見を頂戴した。社内の人間だけで考えていても、自社の弱点や不足している点は見えにくい。厳しく言ってくれる人が、ここまでやるならいいと認めてくれるところまで行く。ここは妥協できない。
- ・ 過去複数回の個人情報の漏えいがあった際、担当者が過剰反応してしまい、研修等を徹底した結果、現場が情報セキュリティに背を向けてしまい、「うちは個人情報を扱っていないので関係ない」と営業部門以外はほとんど逃げてしまうという事態が起きてしまった。その意識を改めてもらうのが大変だった。
- ・ 完璧ではないが、漏えい起きると即座に分かるようにしている。専用の連絡先を設け、そこに連絡させる。紙を含めて漏えいしたら即座に報告する。ある一定時間（数時間）を超えて報告が遅れたものは解雇もあるというルールになっていて、その理由で解雇した者もある。
- ・ 大きな事故を起こした後では対策については有無を言わず行うしかないが、それですべてができるわけではない。今後、どういう基準で実施するのが課題である。
- ・ 社内の罰則を強化したいが、人事との調整が難しい。

### (3) 問題意識

- ・ 情報セキュリティには神経質に取り組んできていて、ISMS に代表される情報セキュリティの規格に沿った取り組みは進めてきている。特に、人やシステムの管理はそれなりに行ってきているつもりである。しかし、セキュリティ事故はなくなる。今後、どう進めていけば根源的になくせるのかという「人との戦い」に悩んでいる。
- ・ 米国では、その事象によってどれだけの実被害があったのかということを尺度に議論する。日本は情報セキュリティ事象に過剰反応する。PC が盗まれても実質的に情報漏えいの被害がなければよいという考え方をしてはどうか。
- ・ グループ会社全体を見渡してみると規模が全く異なる会社が多いので、どこまで情報セキュリティを統一するかに悩んでいる。本社と比べると売上規模が 10 分の 1 以下の会社もあるので、情報セキュリティに投資せよといっても難しい。
- ・ ホールディング化したので、多様な会社がグループに入ってきた。売上規模の差が 1000 倍

もある。脆弱性を修正する指摘を行うと、そのための月額 2 万円の費用が捻出できないとなきつかれるケースもある。

- ・ 協力会社の孫会社から当社の業務情報が流出したケースについても、監督責任を問われる。どのように根絶していけばよいのか。
- ・ モバイル型の勤務形態を奨励しているため、会社と同じ業務を自宅や出先で行う人が増えている。印刷等もできるようにすると心配が増える。また、SNS やブログなどで自ら情報発信する社員も増えている。余計なことは言わないように注意はしているが、戸は立てられない。
- ・ 海外の事故については把握できていない。自分たちの情報が漏えいしていてもわからない。国内でも、情報の持ち出しの記録はとっているが、その記録を見て事故かどうかを判定するノウハウまで高まっていない。

#### 4.3.3. 考察

情報資産の分類や情報管理体制について、参加者の考え方は様々で、それこそが情報管理の難しさを物語っている。たとえば、紙情報と電子情報の管理は、前者を総務部門や経営企画部門、後者を IT 部門が担うケースもあれば、IT 部門が一元的に担うケースもある。さらに、個人情報問題はすべて CPO に一元化されているケースも見られる。

また、情報セキュリティ対策における人の管理の重要性が、複数の参加者から指摘された。実際に情報漏えい等に遭遇したケースでは、自社だけでなく子会社の委託先や海外事業所でのトラブルなど、本社からの統制が困難なケースのほか、社員が悪意なく仕事のために持ち出した PC が盗難に遭うケースなども挙がっている。

こうしたトラブルを契機として、業務プロセスの変更やトラブル発生時の報告制度を含む積極的な対策の導入・改善が行われているが、その一方、担当者の過剰反応で現場との軋轢が生じたり、罰則の導入で人事との調整が難航するケースも見られ、バランスの難しさが伺える。

さらに、問題意識としては、規模の異なるグループ会社にどうやって横断的に情報セキュリティを適用するか、特に対策費用の確保が困難な小規模の事業者をどうすべきかといったグループ経営上の情報セキュリティ確保、また、企業のグローバル化や勤務形態の多様化、個人の情報発信の環境などの変化により、リスクが高まりつつあることへの懸念が指摘されている。