

# Information Security 情報セキュリティレポート Report

2007年1月

Vol.3 | No.1

## 情報セキュリティに関する インターネット利用者意識 2006

Rev. 1.01

---

情報セキュリティに関する  
インターネット利用者意識

2006

---

## はじめに

NRIセキュアテクノロジーズ株式会社（以下「NRIセキュア」）は、全国のインターネット利用者（2,321名）に対し、2006年11月にインターネットアンケート調査を行い、その結果を「情報セキュリティに関するインターネット利用者意識 2006」としてレポートにまとめました。約半数の企業において、社員の私物パソコンがLANに接続されることを明示的に禁止しておらず、また、自宅で仕事をしている会社員も少なくないことが明らかになりました。企業の情報セキュリティ対策におけるパソコンの接続ルールや、社外での業務活動に関する管理体制の整備などに、今後の注目が高まると考えられます。

現在、個人情報保護に関する意識が高まり、情報セキュリティは生活者にも身近な問題となってきた一方で、企業の内部統制がIT分野でも大きな関心事となっています。このような背景から、今回の調査は、NRIセキュアが2003年よりインターネット利用者を対象に毎年実施してきた「個人情報に関する消費者意識調査」の内容を継承するとともに、対象のうち、会社員に対しては、勤務先以外での内部情報の利用・管理の実態を明らかにするための設問を追加し、結果を分析しています。

本報告書が情報セキュリティ全般に関する理解を深め、情報セキュリティ対応の施策の一助になれば幸いです。

- |   |
|---|
| <ul style="list-style-type: none"><li>■ 本アンケート調査は、NRIセキュアテクノロジーズ株式会社が、企業や公的機関におけるセキュリティ対策の推進のために、自主的な活動として行っているものです。</li><li>■ 本アンケート調査の生データの提供には応じておりません。</li><li>■ 本報告書の著作権は、NRIセキュアテクノロジーズ株式会社が保有します。内容の一部を転載、引用する場合には、出所として弊社名および調査名称「情報セキュリティに関するインターネット利用者意識 2006」を併記してください。なお、転載・引用の際には弊社までご一報下さい。</li><li>■ 以下の行為は禁止いたします。<ul style="list-style-type: none"><li>● データの一部、または全部を改変すること</li><li>● 本報告書を販売、出版すること</li><li>● 出所を併記せずに転載、引用を行うこと</li></ul></li></ul> |
|---|

---

## 目 次

アンケート調査まとめ.....	4
調査概要.....	6
<b>1. インターネット上で経験したトラブル.....</b>	<b>12</b>
1.1 インターネット上で経験したトラブル.....	12
1.2 インターネット上で経験した金銭的な被害.....	13
<b>2. 個人情報保護に関する意識.....</b>	<b>14</b>
2.1 WEB サイトへ入力するのに抵抗を感じる情報.....	14
2.2 WEB サイトへの情報入力に抵抗感がある理由.....	15
2.3 自分の個人情報が漏洩された経験とその後の対応.....	16
2.4 最近の個人情報の漏洩事件に対する所感.....	18
<b>3. 家庭にあるパソコンのセキュリティ.....</b>	<b>19</b>
3.1 セキュリティ対策への意識.....	19
3.2 セキュリティ対策を図る上での問題点.....	21
3.3 セキュリティ対策への支出額と支払意思額の比較.....	22
3.4 情報セキュリティの知識の情報源.....	23
3.5 行政機関、非営利団体のホームページへのアクセス頻度.....	24
3.6 情報セキュリティ教育に対する考え方.....	25
<b>4. ビジネスパーソンの情報セキュリティ意識調査（特別集計）.....</b>	<b>26</b>
4.1 業務の部門.....	26
4.2 業務でのノート型パソコンの利用の状況.....	27
4.3 自宅でパソコンを使った仕事の実施状況と企業ルールの遵守状況.....	28
4.4 自宅で仕事をするときの利用媒体、手段.....	29
4.5 会社のパソコンの持ち出しルールの遵守状況.....	30
4.6 仕事で使うノート型パソコンのセキュリティ対策.....	31
4.7 会社の LAN への接続ルールとその遵守状況.....	32
4.8 会社所有のノート型パソコンに関するトラブル.....	33
4.9 勤め先の情報管理の状況.....	34
4.10 企業内の情報管理を徹底させる方策.....	35

---

## アンケート調査まとめ

### (1) インターネット上で経験したトラブル

- インターネット上でのトラブルがないという回答は 36.0%にとどまり、残りの人は何らかのトラブルに遭っている。特に多い項目は、『見知らぬ人からの電子メールでの迷惑なダイレクトメール（スパムメール）』に約半数が遭遇している。
- また、回答者の 3.0%がインターネット利用で、架空請求や詐欺などの金銭上のトラブルを経験している。また、個人情報を漏洩されたという人も 5.6%いる。

### (2) 個人情報保護に関する認識

- WEB サイトへ入力するのに抵抗を感じる情報としては、『顔写真』、『クレジットカード番号』、『銀行の口座番号』など。いずれも機微な情報であると考えている人が多いことが推察される。
- 個人情報を漏洩されたことがあると回答した人（回答者全体の 5.6%）に対し、その後の対応を質問したところ、『サービスの利用を中止した』という人が 43.1%と 4 割強を占めている。
- 実際に個人情報を漏洩されたという回答は 5.6%で、20 人に 1 人を越える割合で情報漏洩の被害者となっているが、この数値は 2004 年（20.2%）、2005 年（12%）と継続して減少傾向にあり、個人情報保護法の効果が現れている可能性を示唆する。
- 最近の個人情報の漏洩事件に対する所感としては、『有料であるからには、基本的な情報であっても絶対に漏洩はして欲しくない』という項目について、『そう思う』との回答が 64.6%を占め、2005 年調査結果（56.5%）より上昇した。法律上の個人情報の定義に関わらず、依然、情報管理の厳格な実施を求める声は高いと言える。

### (3) 家庭にあるパソコンのセキュリティ

- 自宅のパソコンについて、『ウイルス対策ソフト』を導入している人は約 8 割に達している。
- セキュリティ対策として利用しているものの上位は、『ウイルス対策ソフト』、『パーソナルファイアウォール』、『スパイウェア対策ソフト』などが挙げられる。しかし、これらの対策を利用している人の約半数は『セキュリティ対策が不十分である』と感じている。
- セキュリティ対策として実施しているものの上位は、『不審な電子メールの添付ファイルは開けないようにしている』、『怪しげなサイトへアクセスしないようにしている』、『セキュリティのパッチ当てを実施している』などが挙げられる。先のセキュリティ対策の利用の設問と同様に、これらの対策を実施している人の約半数は『セキュリティ対策が不十分である』と感じている。
- 自宅のパソコンのセキュリティ対策を行う上で問題となることとして、全体の 69.6%の人が『お金がかかること』と回答している。
- 1 年間のパソコンのセキュリティ対策の支出額を試算したところ平均で 4,000 円となった。一方、支払意思額（実際にセキュリティ対策上支払ってもよいと考える金額）は、平均で

---

4,238 円となっており、実際には支払っていないものの情報セキュリティ対策にお金をかけても良いと考える層が存在することが明らかにされた。

- 情報セキュリティ知識を得るための情報源としては、『ウイルス対策メーカーのホームページやメール』(52.4%)、『インターネットのニュース』(49.2%)を挙げる人が多い。一方、『行政機関・非営利団体のホームページ』はわずか 3.0%にとどまっていることが明らかになった。
- 情報セキュリティ教育については、『企業の社員の情報セキュリティ教育をきちんと行うべきである』(57.7%)、『情報セキュリティ教育の研修の機会をもっと増やすべきである』(39.5%)、『学校教育の一環で情報セキュリティ教育を行うべきである』(35.0%)などが上位に挙がっている。

#### (4) ビジネスパーソン（会社員）の情報セキュリティ意識調査（特別集計）

- 『自宅でパソコンを使った仕事の実施状況と企業ルールの遵守状況』についての設問については、『自宅で仕事することを禁じられていないので、自宅で仕事をすることもある』(30.6%)、『自宅で仕事することを会社は推奨している』(2.9%)という回答が合わせて3分の1となり、ユビキタス環境や成果主義の導入といった要因が、会社の内部情報を利用して自宅で業務を行うケースに結びついている可能性をうかがわせる。『自宅で仕事することが禁じられているが、自宅で仕事をすることがある』(7.4%)も含めると、オフィスの物理的範囲にとどまらずに業務が行われているケースが4割を越えている。
- 個人所有のノート型パソコンの会社 LAN への接続に関しては、『個人のパソコンを会社の LAN につなげることを禁じていないが、個人のパソコンをネットワークにつなげたことはない』(34.3%)、『個人のパソコンを会社の LAN につなげることを禁じていないため、個人のパソコンをネットワークにつなげたことがある』(11.2%)など、接続ルール自体の不備をうかがわせる回答が半数近くに達している。また、『個人のパソコンを会社の LAN につなげることを禁じられているが、個人のパソコンをネットワークにつなげたことがある』(1.4%)という回答もごく少数ながら寄せられており、接続禁止のルールはあるがそれを強制する手段までは採られていない場合は、社員がルールを犯していることを知りつつ私物のパソコンを接続するケースが現実にあることが判明した。
- 『企業内の情報管理を徹底させる方策』についての設問では、『社員の情報セキュリティ教育の実施』(66.3%)、『社内の情報管理ルールの明確化』(58.1%)、『ウイルス対策ソフトやパッチ対策などのネットワークセキュリティの強化』(53.1%)、『社内情報のアクセス権限の厳格化』(40.1%)などが上位に挙がっている。
- 今回のビジネスパーソンの情報セキュリティ意識調査結果全般から、企業の情報セキュリティ対策の徹底や内部統制構築を確実に進めるためには、社員行動の規範となるルールの整備とともに会社外での社員の行動をコントロールするための方策や経営層の積極的な関与が必要であるということが確認された。

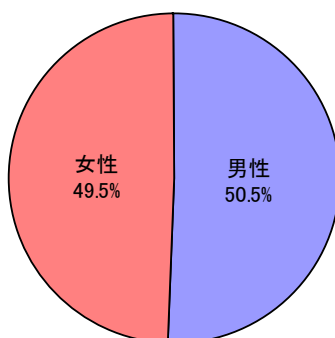
## 調査概要

- 1) 実施時期：2006年11月17日～11月21日
- 2) 調査方法：WEB アンケート<sup>1</sup>
- 3) 調査対象：インターネットを利用する消費者（16歳以上）  
『インターネット白書 2006』<sup>2</sup>データを基に、性別年代別にインターネットを利用するユーザ割合に一致するようにサンプルを抽出した。
- 4) 回収サンプル数：2,321（うちビジネスパーソン 1,266）
- 5) 質問数 40 問
- 6) 回答者像の把握

本アンケート調査の回答者の基本属性を以下に示す。

### (1) 性別

図1 性別



[ N=2,321 ]

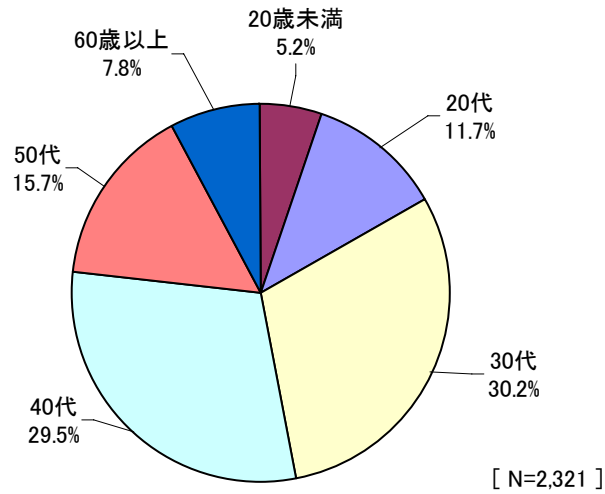
あなたの性別をお答えください。(回答は1つ)

<sup>1</sup> 本アンケートは、Yahoo!リサーチに委託して実施しました

<sup>2</sup> 出所 『インターネット白書 2006』 監修：財団法人インターネット協会 インプレス 2006年6月発刊

(2) 年齢

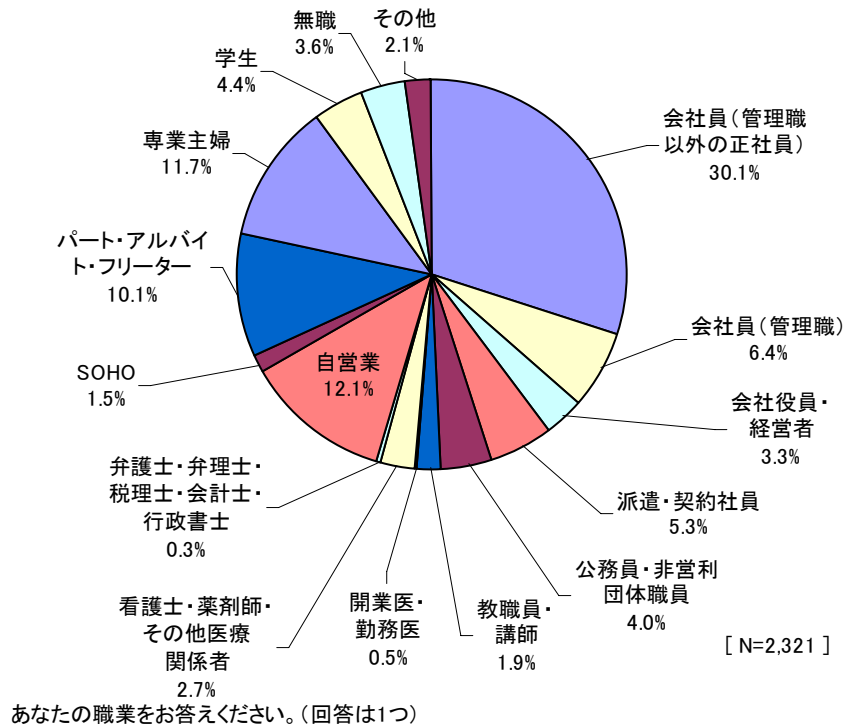
図2 年齢(年代)



あなたの年齢をお答えください。

(3) 職業

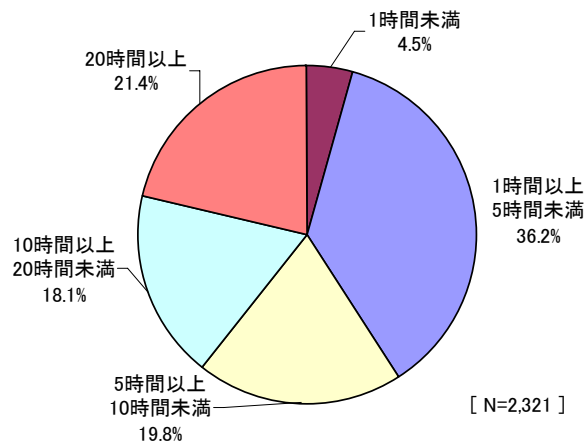
図3 職業



#### (4) インターネットの利用時間

インターネットの利用時間の傾向を下図に示す。『1週間あたり 20 時間以上』と回答した割合は 21.4%、『1週間あたり 10 時間以上 20 時間未満』と回答した割合は 18.1%に上る。合わせて、1週間に 10 時間以上利用していると回答する割合は約 4 割に達している。

図 4 インターネットの利用時間

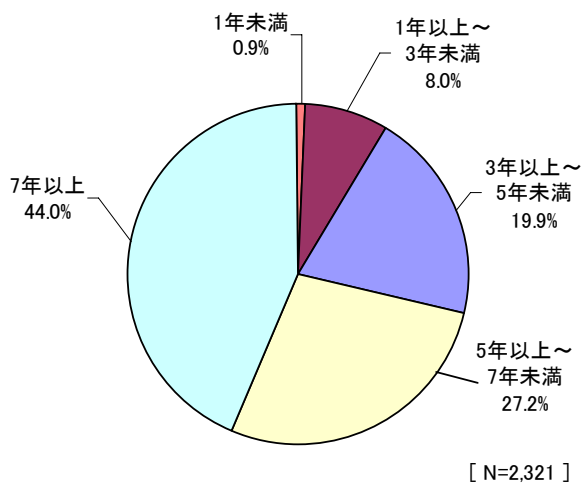


あなたは、1週間に平均何時間くらいインターネットを利用しますか。  
(回答は1つ)

#### (5) インターネットの利用経験

インターネットの利用経験を下図に示す。回答者中 44.0%が『インターネット利用経験 7年以上』と答えている。

図 5 インターネットの利用経験

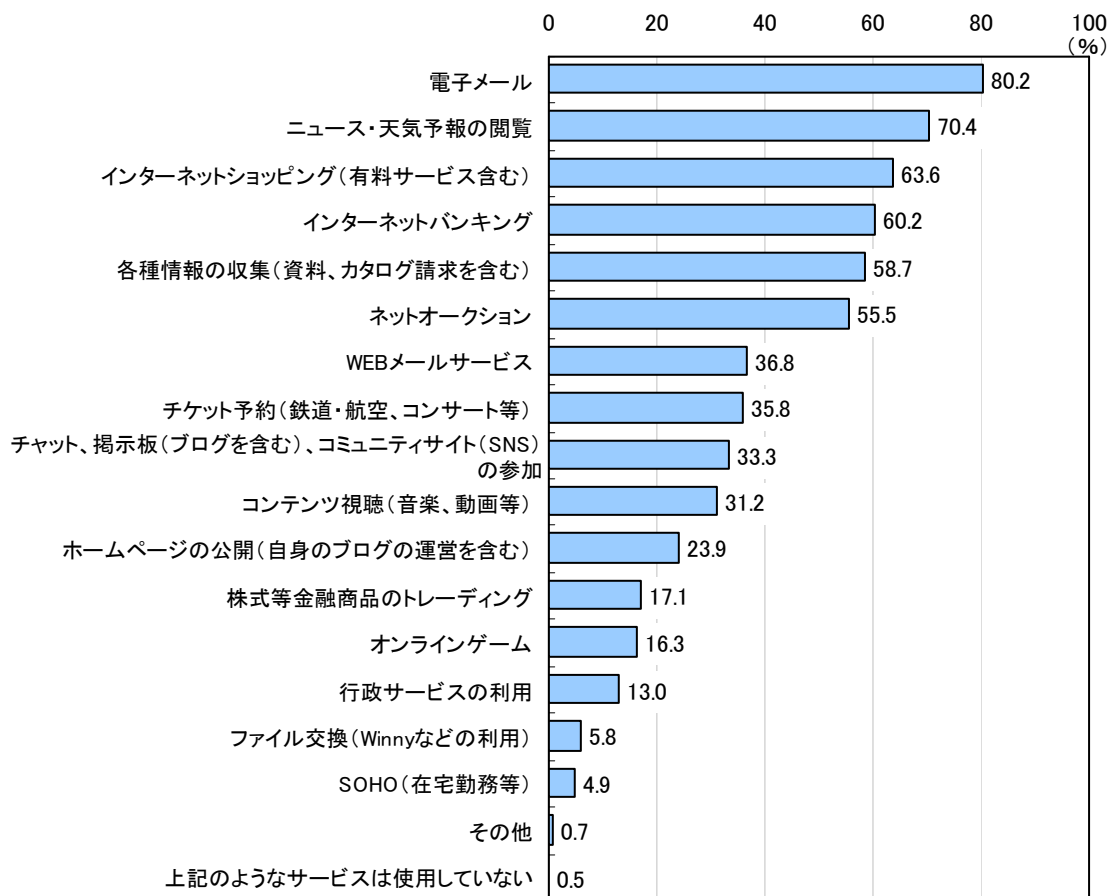


あなたのインターネット利用歴をお答えください。(回答は1つ)

(6) インターネット利用状況

インターネットの利用目的は『電子メール』と答える割合が最も多く 80.2%となった。続いて、『ニュース・天気予報の閲覧』(70.4%)、『インターネットショッピング(有料サービス含む)』(63.6%)、『インターネットバンキング』(60.2%)、『各種情報の収集(資料、カタログ請求含む)』(58.7%)、『ネットオークション』(55.5%) などとなっている。

図6 インターネット利用状況



[ N=2,321 ]

あなたは、どのような目的でインターネットを利用しますか。(回答はいくつでも)

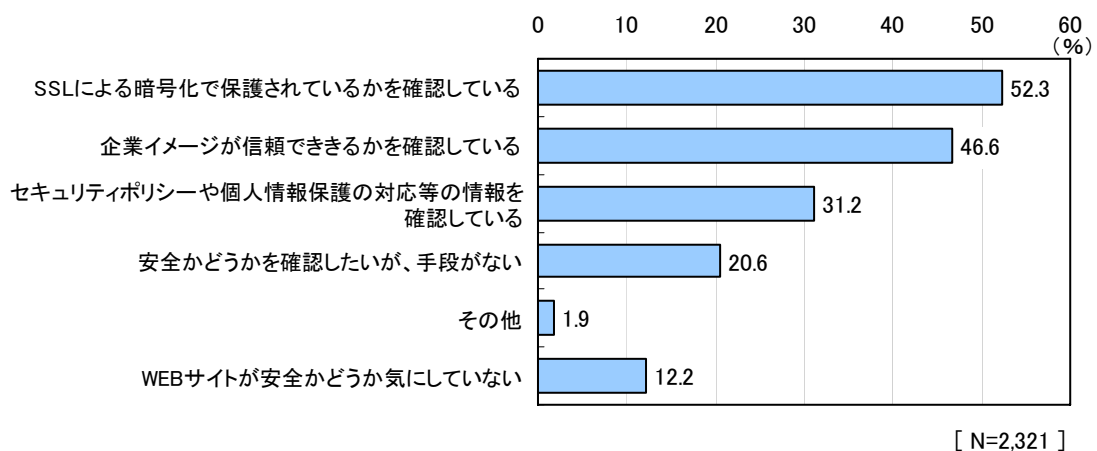
## (7) アクセスしている WEB サイトの安全性の判断

アクセスしている WEB の安全性の判断について、『SSL による暗号化で保護されているかを確認している』が 52.3%、『企業イメージが信頼できるかを確認している』が 46.6%などとなっていた。

一方、『WEB サイトが安全かどうか気にしていない』という回答も 12.2%あった。

また、『安全かどうか確認したいが、手段がない』という回答も 20.6%あり、危険なサイトかどうかの判断がつかないと考えている人もいることがわかる。この背景には、ワンクリック詐欺やフィッシング詐欺などの増加も影響しているものと考えられる。

図 7 アクセスしている WEB サイトの安全性の判断



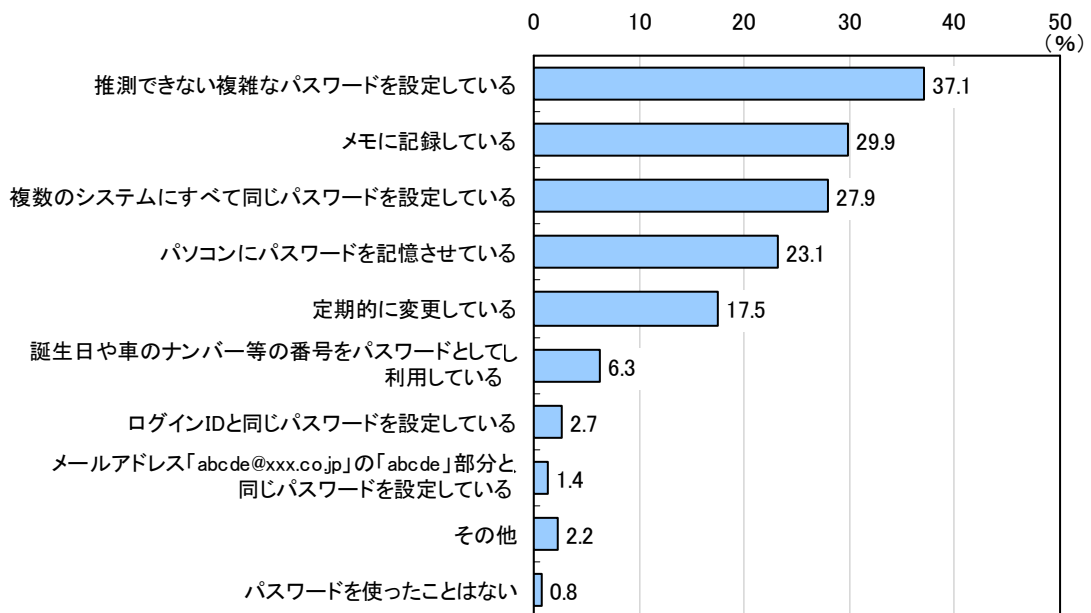
あなたがアクセスしているWEBサイトが安全かどうか、どのように判断していますか。(回答はいくつでも)

## (8) インターネット利用におけるパスワードの使い方

インターネット利用におけるパスワードの使い方としては、『推測できない複雑なパスワードを設定している』が 37.1%、『定期的に変更している』が 17.5%と情報セキュリティ対策を考慮した対応を実施していることが明らかになった。

一方、『メモに記録している』が 29.9%、『複数のシステムにすべて同じパスワードを設定している』が 27.9%、『パソコンにパスワードを記憶させている』が 23.1%などとなっており、情報セキュリティ対策の観点から問題の多い使い方をしてている人が多いことも全体の 2~3 割程度いることが明らかになった。

図 8 インターネット利用におけるパスワードの使い方



[ N=2,321 ]

あなたは、パスワードをどのようにインターネットの利用で使われていますか。(回答はいくつでも)

# 1. インターネット上で経験したトラブル

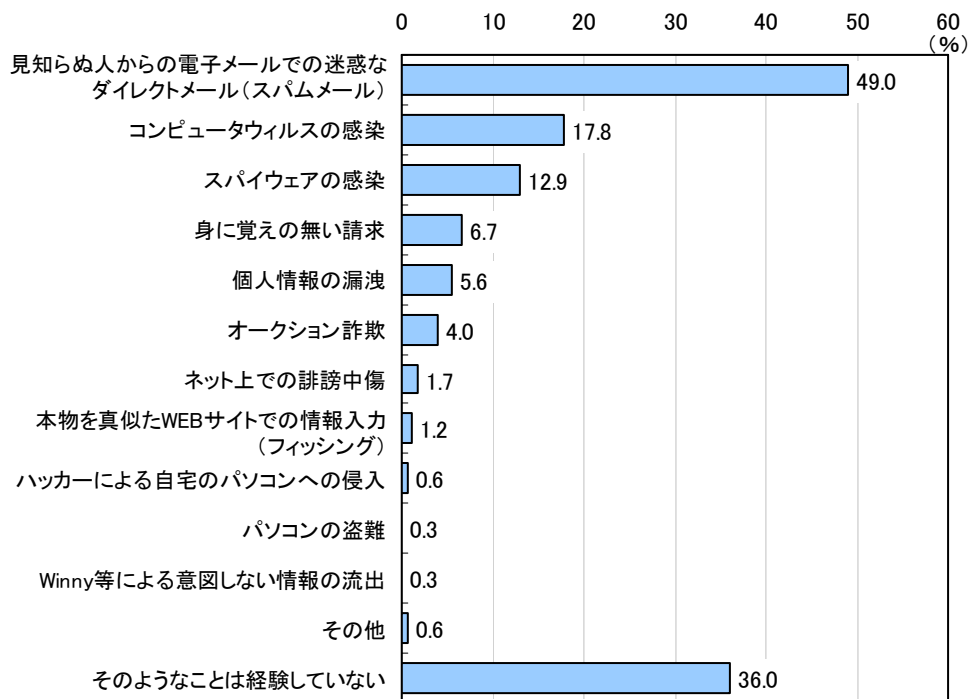
## 1.1 インターネット上で経験したトラブル

インターネット利用でトラブルに遭遇したことがないという回答は36.0%にとどまり、残りは何らかのトラブルに遭っている。また、実際に個人情報を漏洩されたという回答は5.6%で、20人に1人を越える割合で情報漏洩の被害者となっているが、この数値は2004年(20.2%)、2005年(12%)と継続して減少傾向にあり、個人情報保護法の効果が現れている可能性を示唆する。

また、『見知らぬ人からの電子メールでの迷惑なダイレクトメール』と答えた回答者は49.0%とほぼ半数を占めている。また、『コンピュータウィルスの感染』は回答者全体の17.8%、『スパイウェアの感染』が12.9%などとなっている。

その他の項目では、『身に覚えのない請求』(6.7%)、『個人情報の漏洩』(5.6%)、『オークション詐欺』(4.0%)などが続いている。

図1-1 インターネット上で経験したトラブル



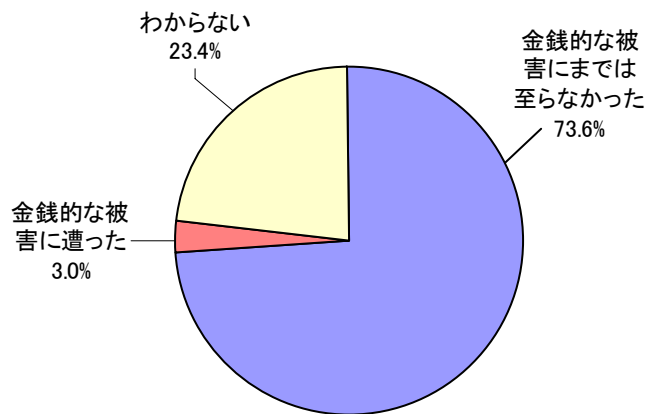
[ N=2,321 ]

あなたは、過去1年間でパソコンやインターネットを利用して以下のようなトラブルに遭ったことはありますか。(回答はいくつでも)

## 1.2 インターネット上で経験した金銭的な被害

インターネット上での、架空請求や詐欺など金銭な被害の経験の有無については、『金銭的な被害にまでは至らなかった』が73.6%であるのに対し、『金銭的な被害に遭った』という回答も3.0%あった。

図 1-2 インターネット上での金銭的な被害



[ N=2,321 ]

架空の請求や詐欺などによって金銭的な被害はありましたか。  
(回答は1つ)

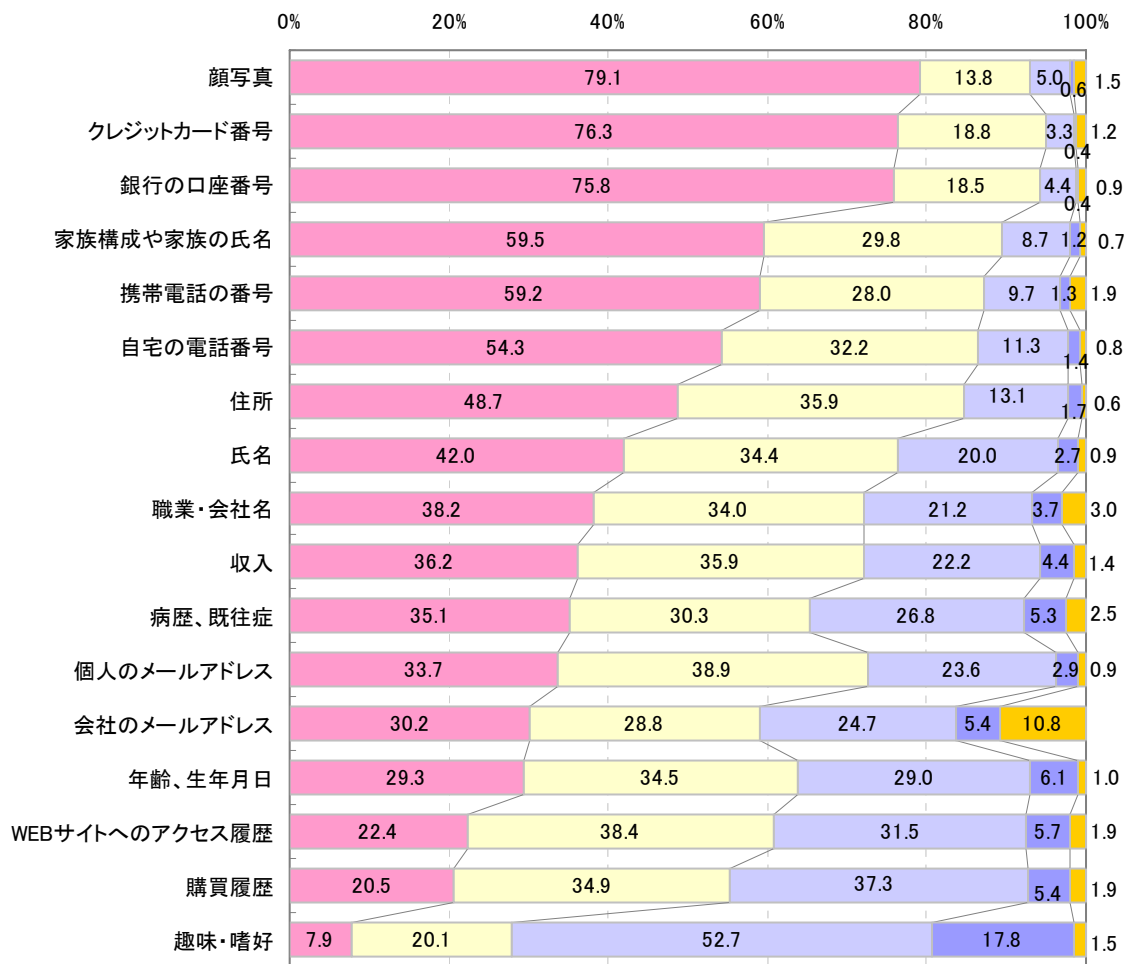
## 2. 個人情報保護に関する意識

### 2.1 WEB サイトへ入力するのに抵抗を感じる情報

2005年4月の個人情報保護法の全面施行以降、消費者の間にも個人情報の扱いについては留意する傾向が強くなったと考えられる。

WEB サイトへ入力するのに抵抗のある情報についての設問では、『顔写真』(79.1%)、『クレジットカード番号』(76.3%)、『銀行の口座番号』(75.8%)などがかなり抵抗を感じる情報として挙げている。

図 2-1 WEB サイトへ入力するのに抵抗を感じる情報



[ N=2,321 ]

■ かなり抵抗を感じる    ■ やや抵抗を感じる    ■それほど抵抗を感じない    ■ まったく抵抗を感じない    ■ わからない

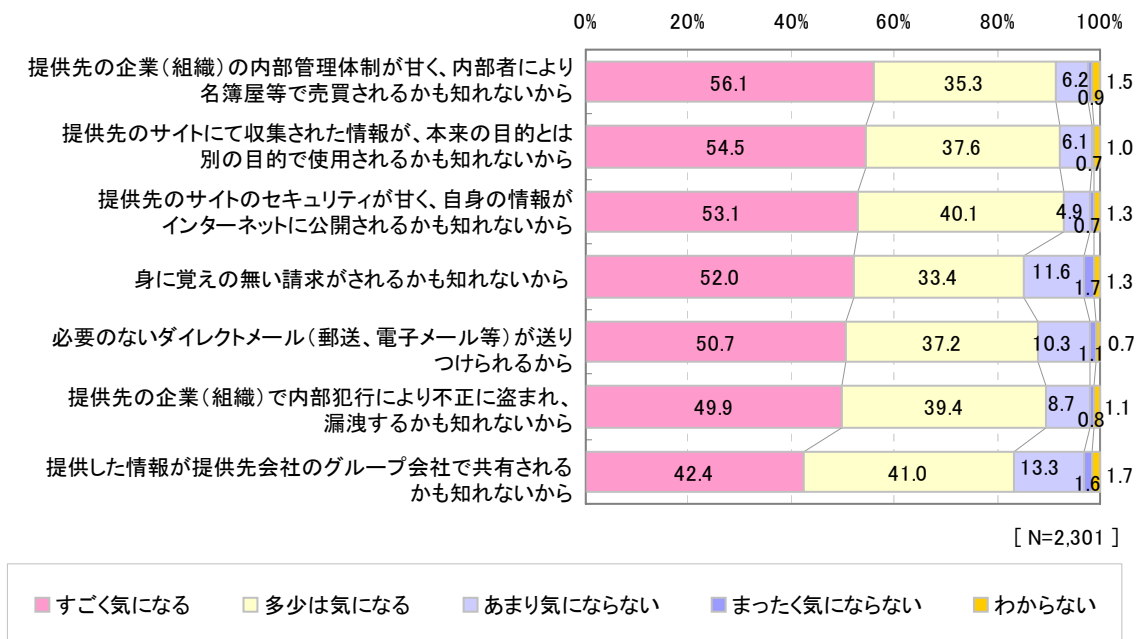
あなたは、WEBサイトに以下の情報を提供する際に、抵抗を感じますか。それぞれの項目であてはまるものをお選びください。(回答は横の行ごとに1つずつ)

## 2.2 WEB サイトへの情報入力に抵抗感がある理由

WEB サイトへの情報入力に抵抗感がある理由として、『提供先の企業（組織）の内部管理体制が甘く、内部者により名簿屋などで売買されるかもしれないから』（56.1%）、『提供先のサイトにて収集された情報が、本来の目的とは別のところで使用されるかもしれないから』（54.5%）、『提供先の企業（組織）の内部管理体制が甘く、自身の情報がインターネットに公開されるかも知れないから』（53.1%）、『身に覚えのない請求がされるかもしれないから』（52.0%）などが『情報提供に際し、すごく気になる』という回答として上位に挙げられた。

いずれも、回答者自身の入力する個人情報を提供先がどのように扱うかについて不安を感じている傾向がうかがえる。

図 2-2 WEB サイトへの情報入力に抵抗感がある理由



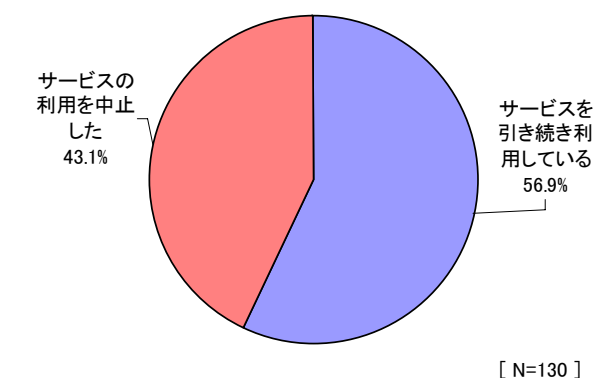
WEBサイトに情報を提供する際の抵抗感はどのようなことから感じますか。それぞれの項目であてはまるものをお選びください。（回答は横の行ごとに1つずつ）

## 2.3 自分の個人情報が漏洩された経験とその後の対応

本アンケートでは、『過去1年間で個人情報漏洩を経験した』と回答した130名に対して、その後、情報を漏洩させたサービスの利用を続けたかどうかを質問した。

『サービスの利用を中止した』という回答が43.1%あり、個人情報の漏洩は企業にとって、利用者離れを生じさせる影響があることがうかがえる。

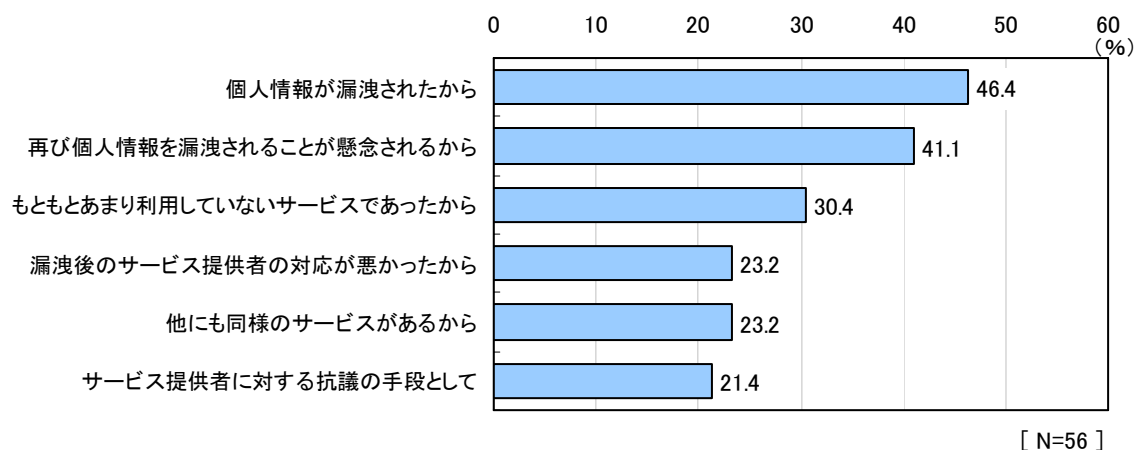
図 2-3 個人情報漏洩を経験した時の対応



個人情報漏洩された後、漏洩の原因となったサービスの利用を継続していますか。(回答は1つ)

図 2-4 は、『サービスの利用を中止した理由』を示している。上位に挙げられた理由として、『個人情報が漏洩されたから』(46.4%)、『再び個人情報を漏洩されることが懸念されるから』(41.1%)などとなっている。

図 2-4 サービスの利用を中止した理由



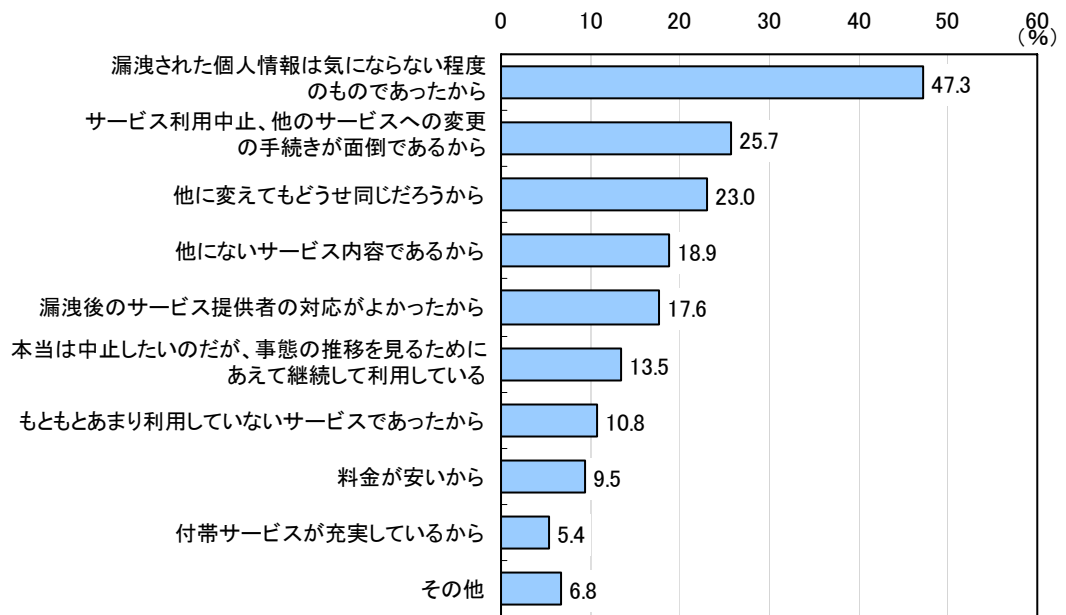
サービスの利用を中止した理由はどのようなものですか。(回答はいくつでも)

一方、個人情報を漏洩されても、そのサービスを使い続けたと回答した消費者に対して、サービスの利用を中止しなかった理由について、図 2-5 に示した。

サービスの利用を中止しなかった理由として、『漏洩された個人情報は気にならない程度のものであったから』(47.3%)、『サービス利用中止、他のサービスへの変更の手続きが面倒であるから』(25.7%)、『他に替えてもどうせ同じだろうから』(23.0%) などが上位に挙がっている。

サービス利用を中止したという回答層に比べると、サービスの利用を中止しなかった層の場合は、個人情報の漏洩の程度が軽微であった可能性も考えられる。

図 2-5 サービスの利用を中止しなかった理由



[ N=74 ]

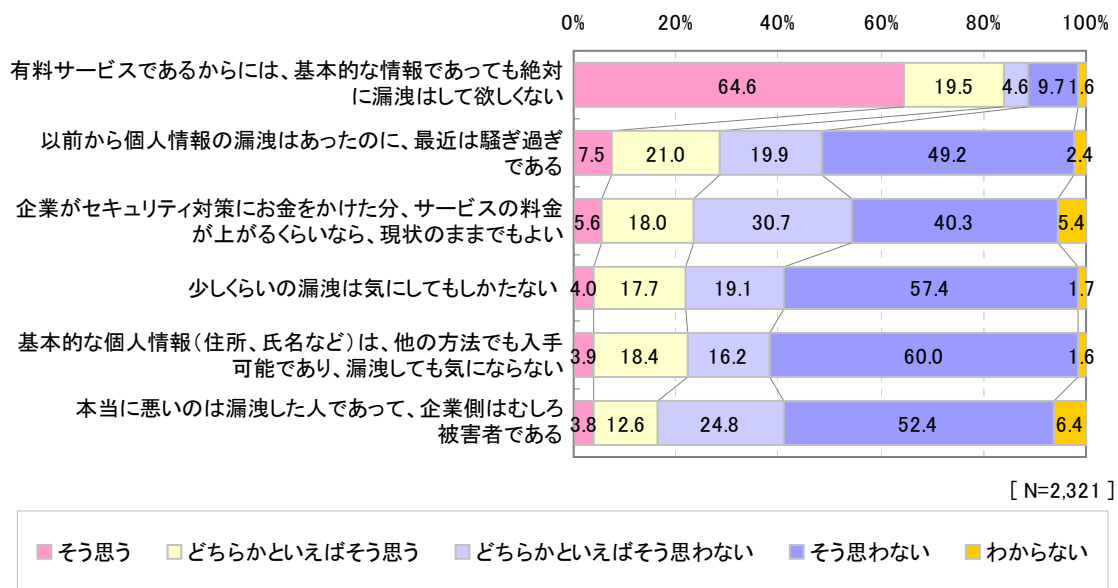
サービスの利用を中止しなかった理由はどのようなものですか。(回答はいくつでも)

## 2.4 最近の個人情報の漏洩事件に対する所感

最近の個人情報の漏洩事件に対する所感についての設問では、『有料であるからには、基本的な情報であっても絶対に漏洩はして欲しくない』という項目について、『そう思う』との回答が 64.6%を占め、2005年調査結果（56.5%）より上昇した。法律上の個人情報の定義に関わらず、依然、情報管理の厳格な実施を求める声は高いと言える。

一方、『そう思わない』という回答が多かった項目は、『基本的な個人情報（住所、氏名など）は、他の方法でも入手可能であり、漏洩しても気にならない』（60.0%）、『少しくらいの漏洩は気にしてもしかたない』（57.4%）、『本当に悪いには漏洩した人であって、企業側はむしろ被害者である』（52.4%）などとなっている。

図 2-3 個人情報の漏洩事件に対する所感



最近の個人情報の漏洩事件について、以下のように思うことはありますか。あてはまるもの全てをお選びください。（回答は横の行ごとに1つずつ）

### 3. 家庭にあるパソコンのセキュリティ

#### 3.1 セキュリティ対策への意識

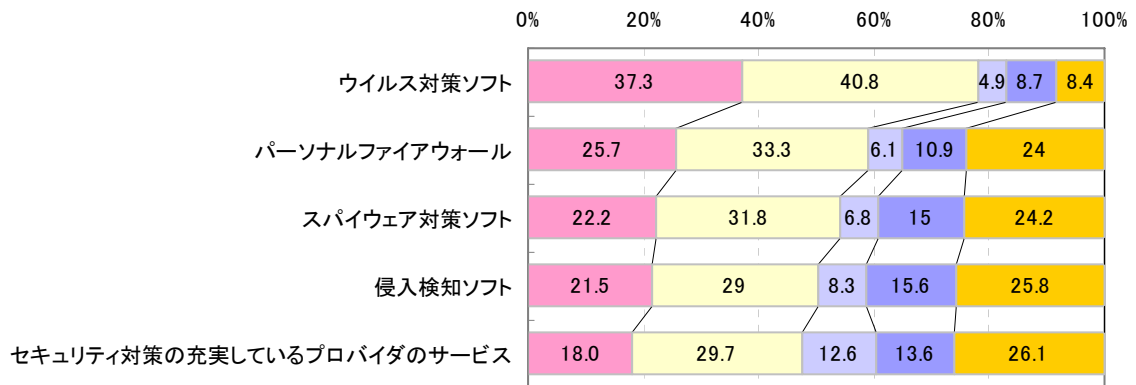
今回のアンケート調査では「現在の自宅パソコン・ネットワークのセキュリティに対する自己評価」を明らかにする質問を行った。

図 3-1 にセキュリティ対策として利用しているものとその自己評価結果を示した。個人のパソコンでは、ウイルス対策ソフトの利用率が約 8 割に達していることがわかる。

自己評価として、『利用しているためセキュリティ対策が十分であると感じている』という回答の多かった項目は、『ウイルス対策ソフト』(37.3%)、『パーソナルファイアウォール』(25.7%)、『スパイウェア対策ソフト』(22.2%) などである。

一方、『利用しているがセキュリティ対策が不十分であると感じている』という回答の多かった項目は、『ウイルス対策ソフト』(40.8%)、『パーソナルファイアウォール』が (33.3%)、『スパイウェア対策ソフト』(31.8%) などである。

図 3-1 セキュリティ対策として利用しているものとその自己評価



[ N=2,321 ]

- 利用しているため、セキュリティ対策は十分であると感じている
- 利用しているが、セキュリティ対策は不十分であると感じている
- 利用していないが、セキュリティ対策は十分であると感じている
- 利用していないため、セキュリティ対策は不十分であると感じている
- わからない

現在、あなたの個人所有のパソコンや自宅のネットワークのセキュリティ対策として利用しているものとその感想をお選びください。(回答は横の行ごとに1つずつ)

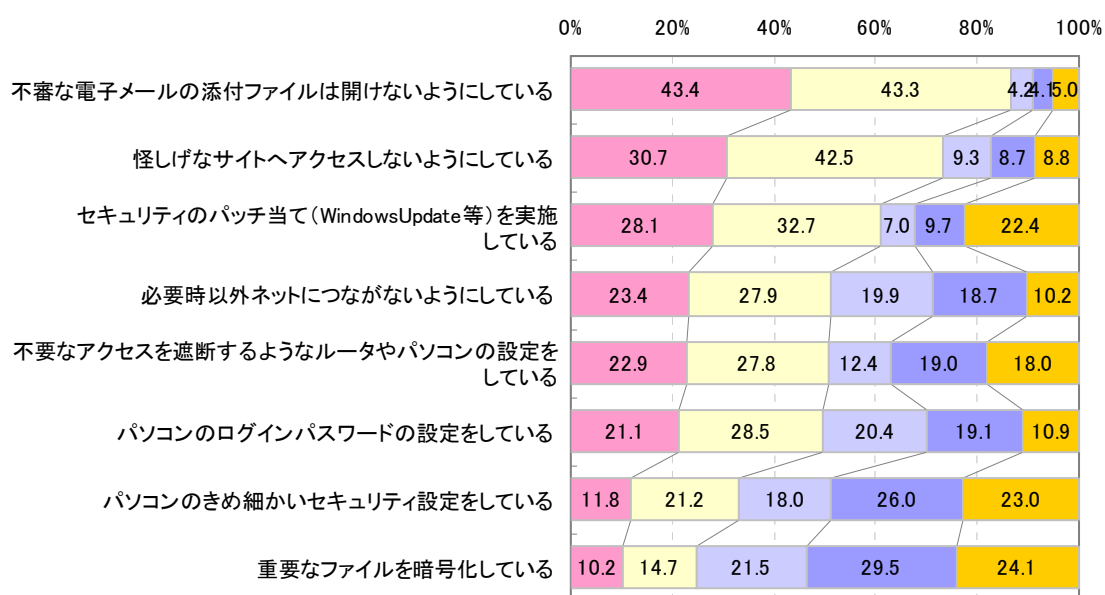
次に、セキュリティ対策への取り組み状況と自己評価結果を図 3-2 に示した。

自己評価として、『実施しているためセキュリティ対策が十分であると感じている』という回答の多かった項目は、『不審な電子メールの添付ファイルは開けないようにしている』(43.4%)、『怪しげなサイトへアクセスしないようにしている』(30.7%)、『セキュリティのパッチ当て (Windows Update など) を実施している』(28.1%) などである。

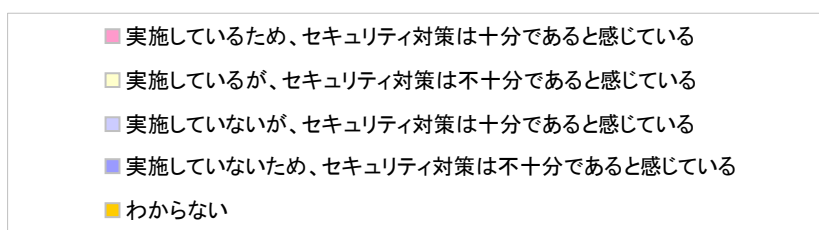
一方、『実施しているがセキュリティ対策が不十分であると感じている』という回答の多かった項目は、『不審な電子メールの添付ファイルは開けないようにしている』(43.3%)、『怪しげなサイトへアクセスしないようにしている』が(42.5%)、『セキュリティのパッチ当て (Windows Update など) を実施している』(32.7%) などである。

回答者の多くは、上記の 3 項目についてはセキュリティ対策上を実施しているものの、インターネット利用時におけるセキュリティを図る上での脅威を感じていることがうかがえる結果となった。

図 3-2 セキュリティ対策の取り組み状況とその自己評価



[ N=2,321 ]



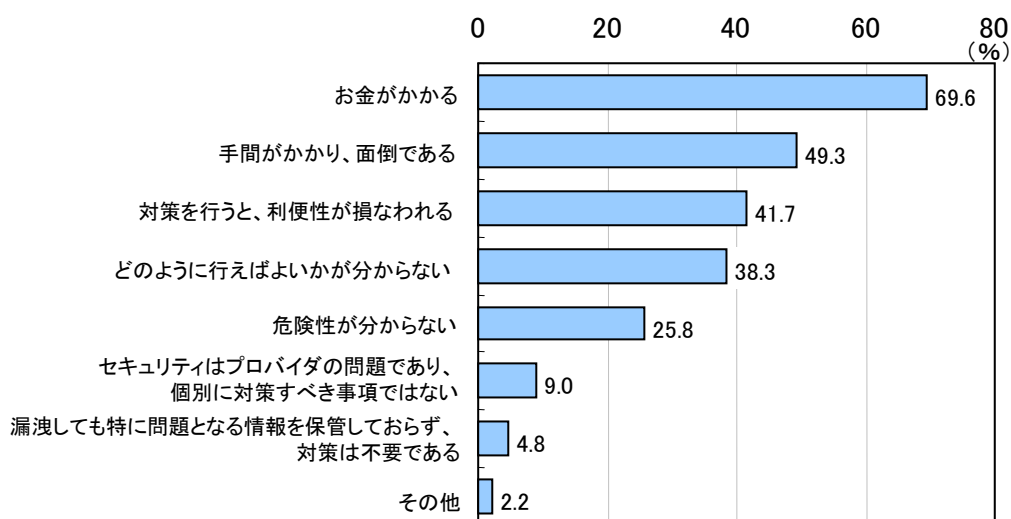
現在、あなたの個人所有のパソコンや自宅のネットワークのセキュリティ対策として実施しているものとその感想をお選びください。(回答は横の行ごとに1つずつ)

### 3.2 セキュリティ対策を図る上での問題点

個人のパソコンのセキュリティ対策を実施する上で問題となることについての設問では、『お金がかかる』(69.6%)、『手間がかかり面倒である』(49.3%)、『対策を行うと、利便性が損なわれる』(41.7%)などが上位に挙げられた。

ウイルス対策ソフトをはじめとするセキュリティ製品の価格やセキュリティパッチに代表されるような作業の手間を問題だと考えている人が多いことが確認された。

図 3-3 パソコンのセキュリティ対策を行う上で問題となること



[ N=2,321 ]

個人のパソコンのセキュリティ対策を行う上で問題となるのはどのようなことですか。(回答はいくつでも)

### 3.3 セキュリティ対策への支出額と支払意思額の比較

個人のパソコンのセキュリティ対策として、1年間の支出額はどのくらいかという設問では、『5,000円程度』（24.3%）、『3,000円程度』（21.4%）などとなっており、『1～5,000円程度』までの層で全体の約6割を占めている。また、「支払っていない」という回答も22.7%あった。

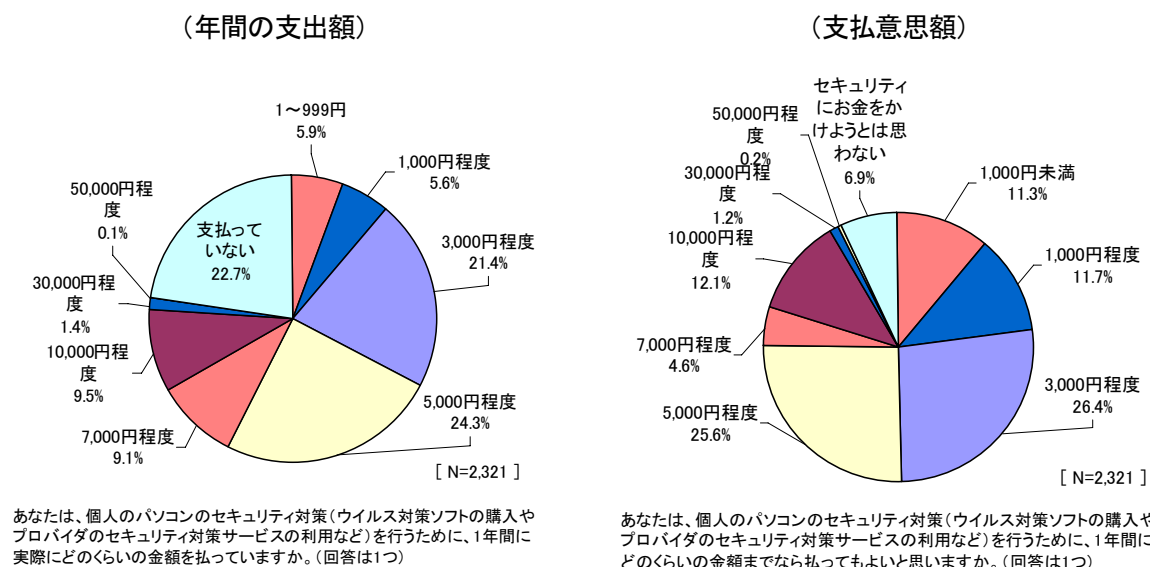
1人あたりの平均支出額を試算すると、4,000円となる。

一方、1年間の支払意思額については、「5,000円程度」が25.6%、「3,000円程度」が26.4%などとなっており、『1～5,000円程度』までの層で全体の約4分の3を占めている。

1人あたりの平均支払意思額を試算すると、4,238円となった。

セキュリティ対策についての支払意思額が実際の支出額を若干上回っていることから、セキュリティ対策についてお金をかけても良いと考えていて、実際は支払っていない層が存在することがうかがえる。

図 3-4 パソコンのセキュリティ対策の年間支出額と支払意思額



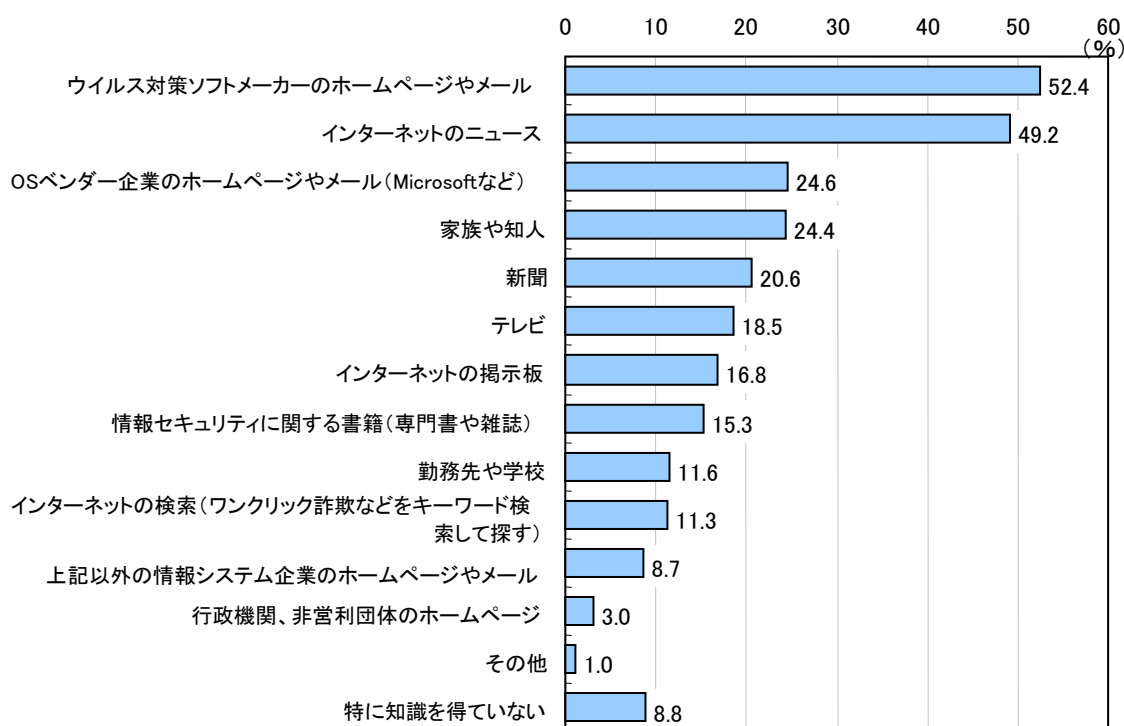
### 3.4 情報セキュリティの知識の情報源

『セキュアジャパン 2006』などの国家的な情報セキュリティ戦略において、国民のセキュリティ教育についての検討が行われている点をふまえ、本アンケートでは、情報セキュリティについての知識をどこから得るかという設問をおいた。

回答が多かった項目は、『ウイルス対策ソフトメーカーのホームページやメール』(52.4%)、『インターネットのニュース』(49.2%)などである。これらの項目がともにほぼ半数を占めているのに対し、『行政機関、非営利団体のホームページ』は3.0%にとどまっている。

情報セキュリティ対策上、ウイルスなどの情報は即時性が求められるため、専門の企業(ウイルス対策ソフトメーカーやOSベンダー企業)から情報を収集する人が多いことが確認された。

図 3-5 情報セキュリティの知識の情報源



[ N=2,321 ]

あなたは、情報セキュリティについての知識をどこから得ていますか。(回答はいくつでも)

### 3.5 行政機関、非営利団体のホームページへのアクセス頻度

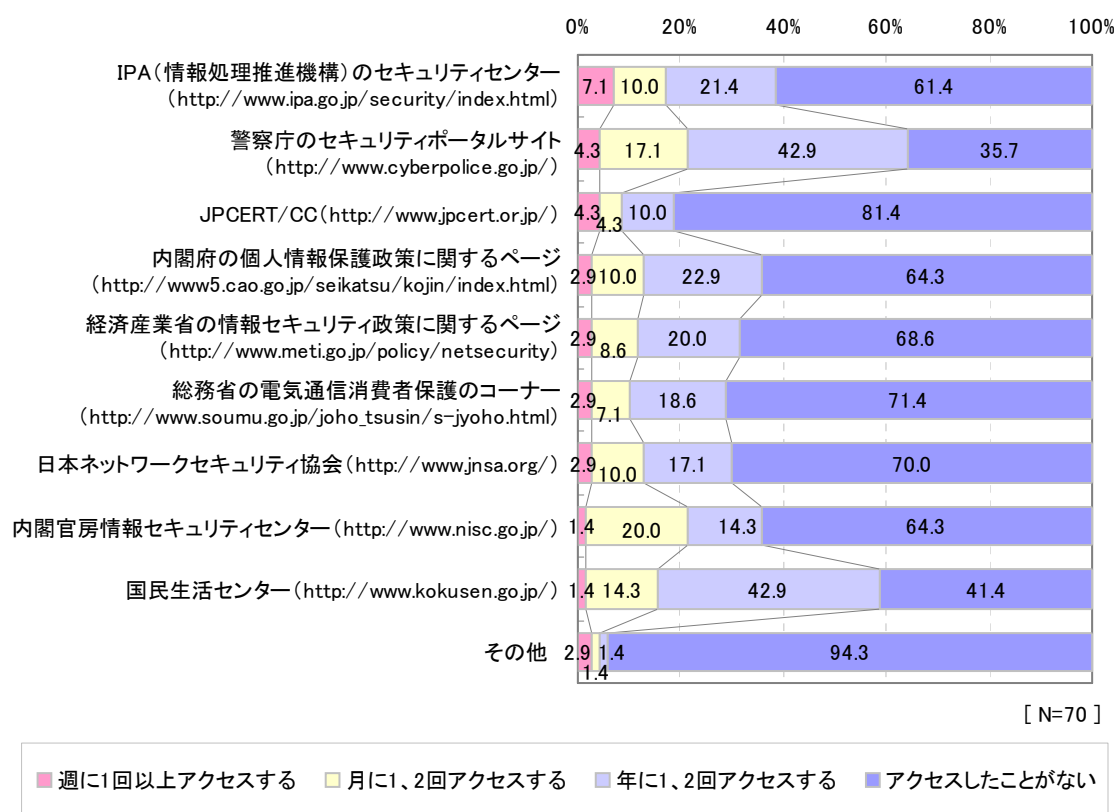
先の設問で、『行政機関、非営利団体のホームページ』からの情報収集をしている人は少数派であることが確認された。

次に、こうしたホームページから情報を収集しているという回答者の各ホームページへのアクセス頻度について質問した。

『週に1回以上アクセスする』という回答が多かったところとしては、『IPA（情報処理推進機構）のセキュリティセンター』（7.1%）、『警察庁のセキュリティポータルサイト』、『JPCERT/CC』がともに4.3%ずつなどとなっている。

『行政機関、非営利団体のホームページ』のホームページにおいても、情報セキュリティ対策に関する情報発信は積極的に実施されているが、利用実態はそれほど活発でないことが明らかになった。今後、さらなるアクセスの向上を図る施策を実施することも重要であると考えられる。

図 3-6 行政機関、非営利団体のホームページへのアクセス頻度



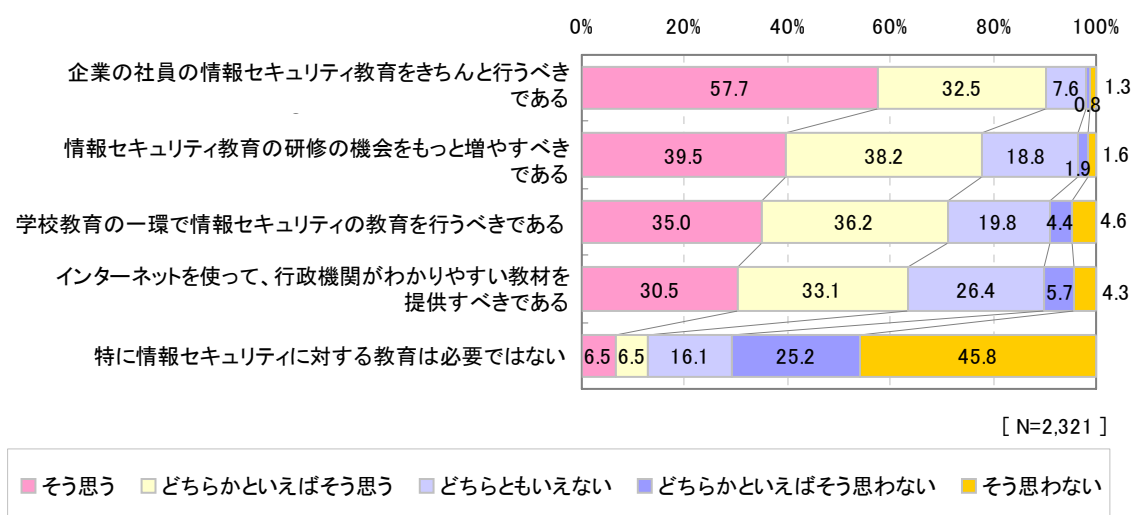
情報セキュリティについての知識を「行政機関、非営利団体のホームページ」から得ているとお答えの方におうかがいします。どのような行政機関のホームページをご覧になりましたか。(回答は横の行ごとに1つずつ)

### 3.6 情報セキュリティ教育に対する考え方

情報セキュリティ教育に対する考え方についての設問で、『そう思う』という回答が多かった項目は、『企業の社員の情報セキュリティ教育をきちんと行うべきである』(57.7%)、『情報セキュリティ教育の研修の機会をもっと増やすべきである』(39.5%)、『学校教育の一環で情報セキュリティ教育を行うべきである』(35.0%) などである。

一方、『そう思わない』という回答が最も多かったのは、『特に情報セキュリティに対する教育は必要ではない』(45.8%) であり、『どちらかといえばそう思わない』(25.2%) を加えると、約7割以上の人が何らかの情報セキュリティ教育を実施していく必要性を感じていることがうかがえる。

図 3-7 情報セキュリティ教育に対する考え方



情報セキュリティの教育についてどうお考えですか。(回答は横の行ごとに1つずつ)

## 4. ビジネスパーソンの情報セキュリティ意識調査(特別集計)

2006年は企業における内部統制が大いに注目を集め、IT業界は、新会社法や金融商品取引法（いわゆる日本版SOX法）への対応ソリューションを活発に提案した時期でもあった。

しかし、企業が内部統制を推進している活動とは裏腹に、社員がそうした企業内の情報セキュリティのルールを遵守しているのか否かについての実態、すなわち、社員の行動から見た情報セキュリティ管理の実態は、既存の調査からは必ずしも明らかになっていないのが実情である。

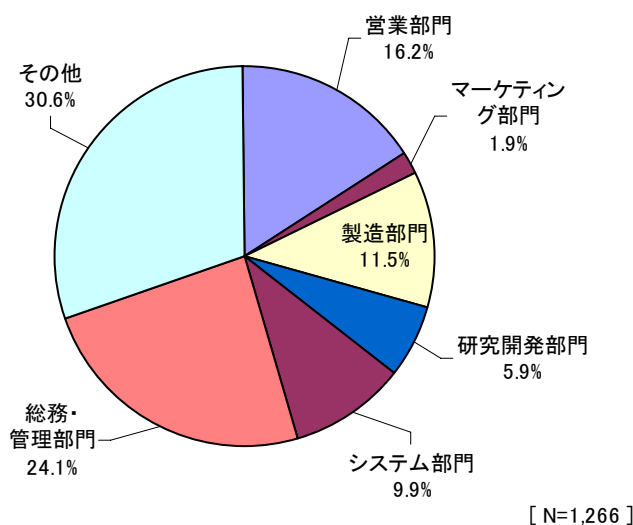
そこで、本調査の回答者のうち、会社員（ビジネスパーソン）1,266人を対象に、自社の情報セキュリティルールの遵守状況と自宅での業務実施の有無などについて質問した。

本章はその特別集計の結果をまとめたものである。

### 4.1 業務の部門

回答者の業務部門は、『総務・管理部門』（24.1%）、『営業部門』（16.2%）、『製造部門』（11.5%）などとなっている。

図 4-1 業務の部門



あなたのお仕事の部門は、この中のどれにあたりますか。  
(回答は1つ)

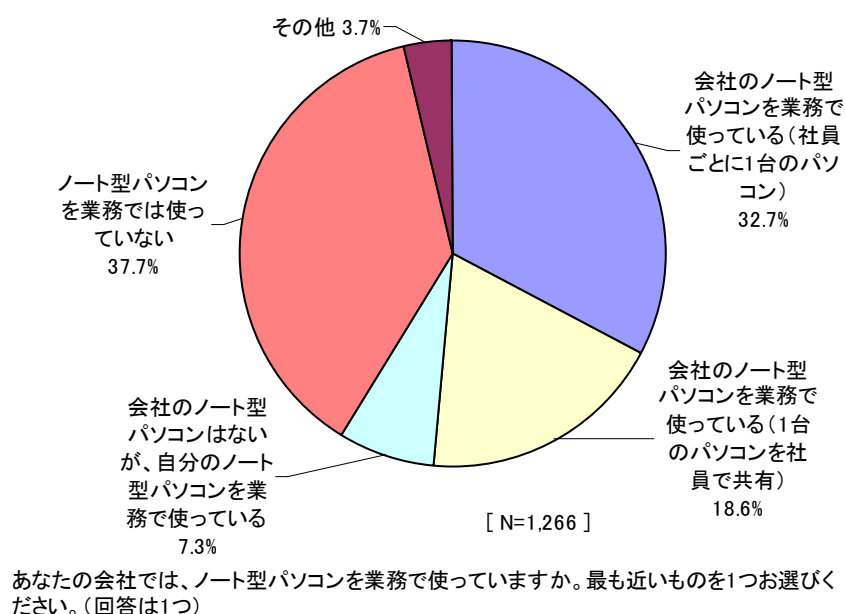
## 4.2 業務でのノート型パソコンの利用の状況

自社の業務でのノート型パソコンの利用状況について質問した。

『会社のノート型パソコンを業務で使っている（社員ごとに1台のパソコン）』（32.7%）、『会社のノート型パソコンを業務で使っている（1台のパソコンを社員で共有）』（18.6%）となっており、半数以上の企業では、会社のノート型パソコンを業務で利用しているという回答が得られた。

一方、『会社のノート型パソコンはないが、自分のノート型パソコンを業務で使っている』（7.3%）という回答も1割弱見られる。

図 4-2 業務でのノート型パソコンの利用の状況

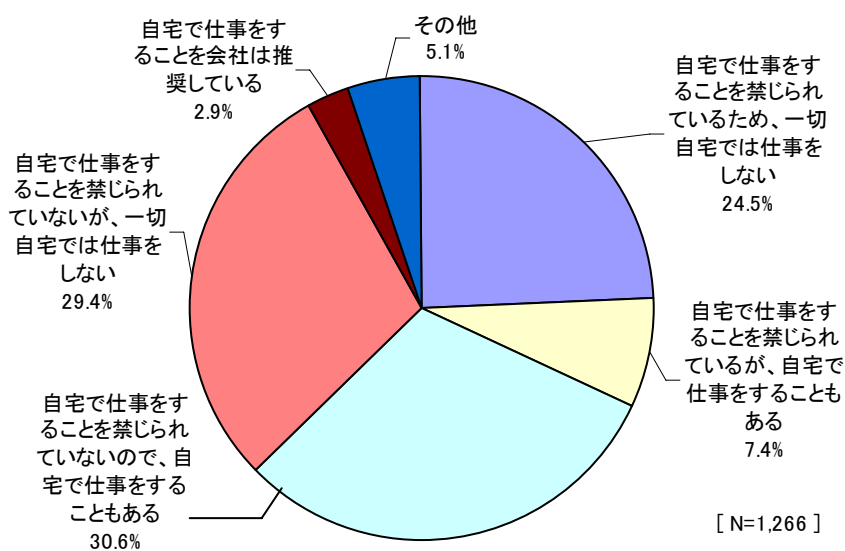


### 4.3 自宅でのパソコンを使った仕事の実施状況と企業ルールの遵守状況

次に、自宅でのパソコンを使った仕事の実施状況と企業ルールの遵守状況について質問した。

『自宅でパソコンを使った仕事の実施状況と企業ルールの遵守状況』についての設問については、『自宅で仕事をするのを禁じられていないので、自宅で仕事をすることもある』(30.6%)、『自宅で仕事をするのを会社は推奨している』(2.9%) という回答が合わせて3分の1となり、ユビキタス環境や成果主義の導入といった要因が、会社の内部情報を利用して自宅で業務を行うケースに結びついている可能性をうかがわせる。『自宅で仕事をするのが禁じられているが、自宅で仕事をすることがある』(7.4%) も含めると、オフィスの物理的範囲にとどまらずに業務が行われているケースが4割を越えている。

図 4-2 自宅でのパソコンを使った仕事の実施状況と企業ルールの遵守状況



あなたの会社では、自宅でパソコンを使って仕事をするのを禁じていますか。(回答は1つ)

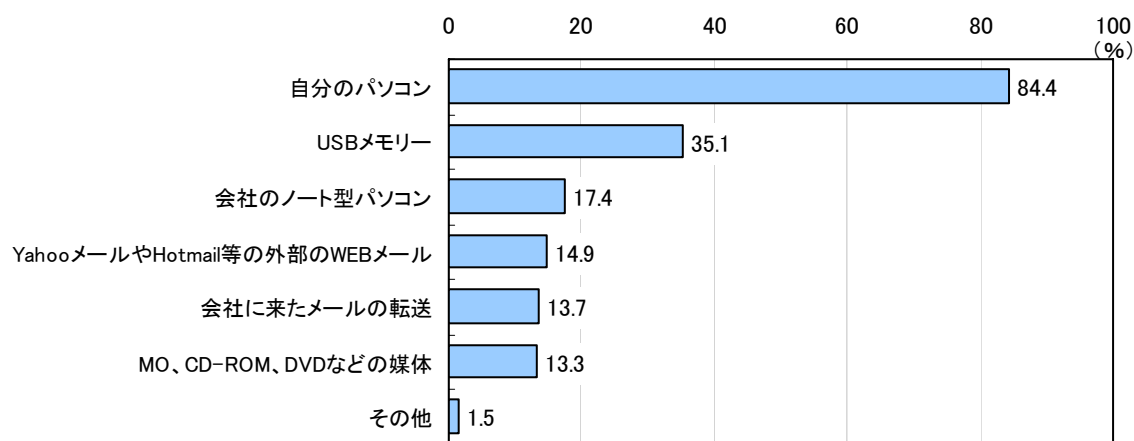
#### 4.4 自宅で仕事をするときの利用媒体、手段

『自宅でパソコンを使って仕事をしたことがある』という回答者に対して、どのような媒体、手段で仕事を行っているかを質問した。

『自分のパソコン』(84.4%)、『USBメモリ』(35.1%)、『会社のノート型パソコン』(17.4%) などとなっている。

回答のあった手段、媒体の中では、USBメモリの利用が少なくないといえるが、過去に発生した情報漏洩事件でもUSBメモリなどの容易に持ち運べる媒体の盗難により発生している事例があることから、こうした媒体の利用についても何らかの対策を講ずる必要があると考えられる。

図 4-3 自宅で仕事をするときの利用媒体、手段



[ N=482 ]

「自宅で仕事することを禁じられているが、自宅で仕事することもある」「自宅で仕事することを禁じられていないので、自宅で仕事することもある」とお答えの方におうかがいします。自宅での仕事にはどのような媒体、手段を利用していますか。(回答はいくつでも)

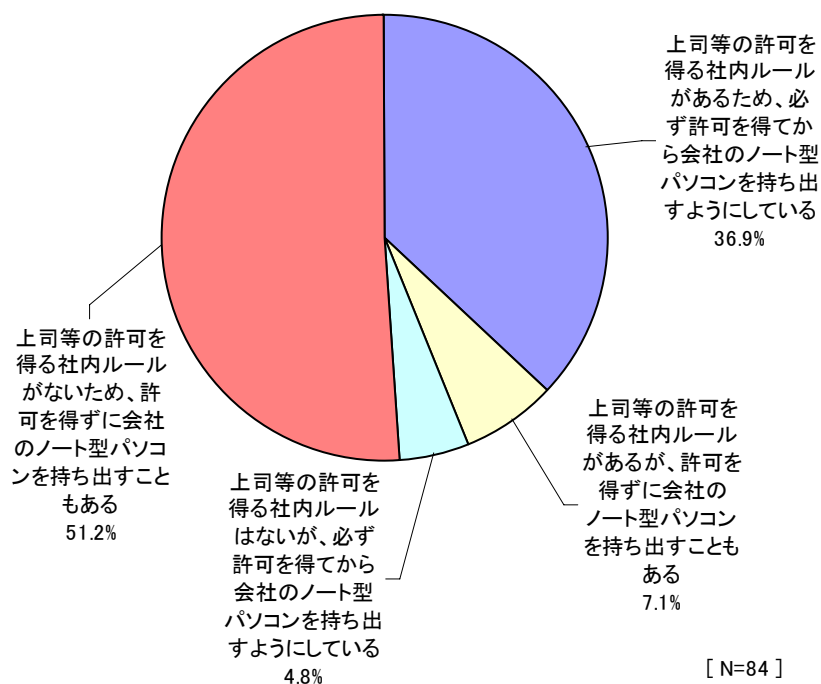
## 4.5 会社のパソコンの持ち出しルールの遵守状況

会社のパソコンの持ち出しルールの遵守状況についての設問では、『上司等の許可を得る社内ルールがあるため、必ず許可を得てから会社のノート型パソコンを持ち出すようにしている』(36.9%)、『上司等の許可を得るルールがあるが、許可を得ずに会社のノート型パソコンを持ち出すこともある』(7.1%)、『上司等の許可を得る社内ルールはないが、必ず許可を得てから会社のノート型パソコンを持ち出すようにしている』(4.8%)、『上司等の許可を得る社内ルールがないため、許可を得ずに会社のノート型パソコンを持ち出すこともある』(51.2%)という結果となった。

この結果から情報セキュリティ対策上問題になるのは、『上司等の許可を得るルールがあるが、許可を得ずに会社のノート型パソコンを持ち出すこともある』という回答で、社内のルールを遵守していない社員が存在するということが確認された。

また、『上司等の許可を得る社内ルールがないため、許可を得ずに会社のノート型パソコンを持ち出すこともある』という回答が約半数を占めていることから、自社のパソコンの持ち出しルールについても、自社で扱う情報資産の大きさを考慮しながら、適切なルールを策定することが望まれる。

図 4-4 会社のパソコンの持ち出しルールの遵守状況



会社のノート型パソコンを社外に持ち出す際の社内ルールがありますか。(回答は1つ)

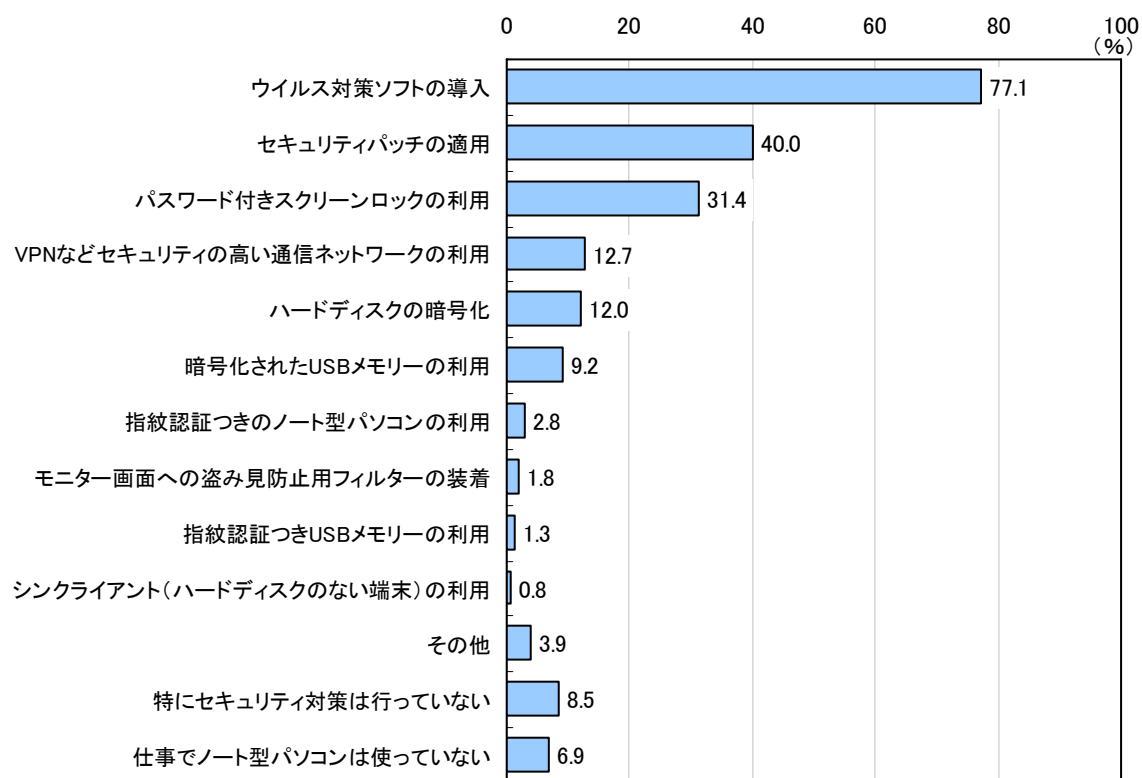
## 4.6 仕事で使うノート型パソコンのセキュリティ対策

仕事で使うノート型パソコンのセキュリティ対策についての設問では、『特にセキュリティ対策は行っていない』(8.5%)、『仕事でノート型パソコンは使っていない』(6.9%)という回答が少数ながら見られた。

一方、実際のセキュリティ対策として回答の多かった項目として、『ウイルス対策ソフトの導入』(77.1%)、『セキュリティパッチの適用』(40.0%)、『パスワード付きスクリーンロックの適用』(31.4%)などとなっている。

また、『VPNなどセキュリティの高い通信ネットワークの利用』(12.7%)、『ハードディスクの暗号化』(12.0%)、『暗号化されたUSBメモリの利用』(9.2%)など、より高いレベルのセキュリティ対策を講じているという回答はそれぞれ1割ずつ程度しか見られない。

図 4-5 仕事で使うノート型パソコンのセキュリティ対策



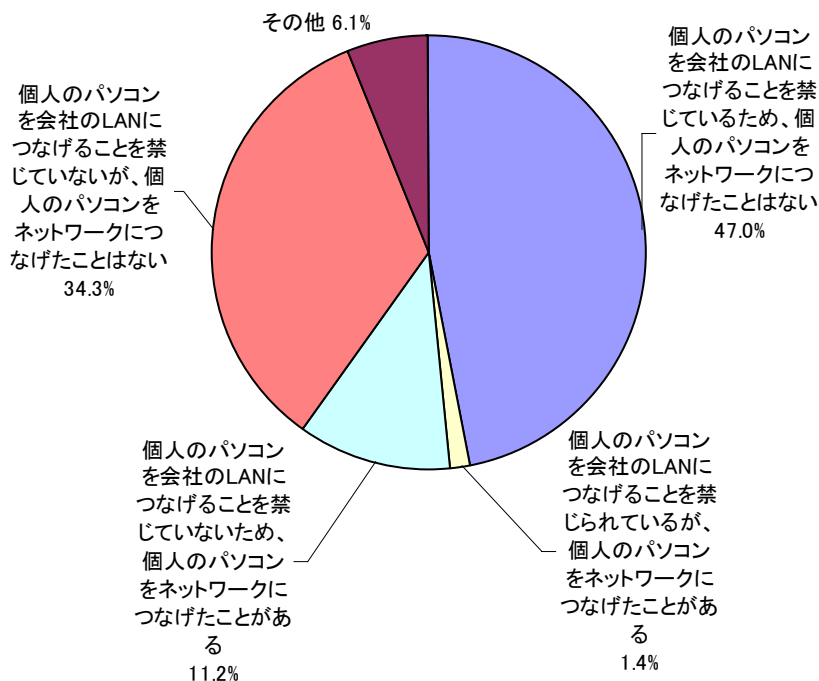
仕事でノート型パソコンを利用の方へおうかがいします。ノート型パソコンについて、セキュリティ上、どのような対策をしていますか。(回答はいくつでも)

## 4.7 会社の LAN への接続ルールとその遵守状況

会社の LAN へ、自分のノート型パソコンを接続したことがあるかについて質問した。

個人所有のノート型パソコンの会社 LAN への接続に関しては、『個人のパソコンを会社の LAN につなげることを禁じていないが、個人のパソコンをネットワークにつなげたことはない』(34.3%)、『個人のパソコンを会社の LAN につなげることを禁じていないため、個人のパソコンをネットワークにつなげたことがある』(11.2%) など、接続ルール自体の不備をうかがわせる回答が半数近くに達している。また、『個人のパソコンを会社の LAN につなげることを禁じられているが、個人のパソコンをネットワークにつなげたことがある』(1.4%) という回答もごく少数ながら寄せられており、接続禁止のルールはあるがそれを強制する手段までは採られていない場合は、社員がルールを犯していることを知りつつ私物のパソコンを接続するケースが現実にあることが判明した。

図 4-6 会社の LAN への接続ルールとその遵守状況



[ N=1,266 ]

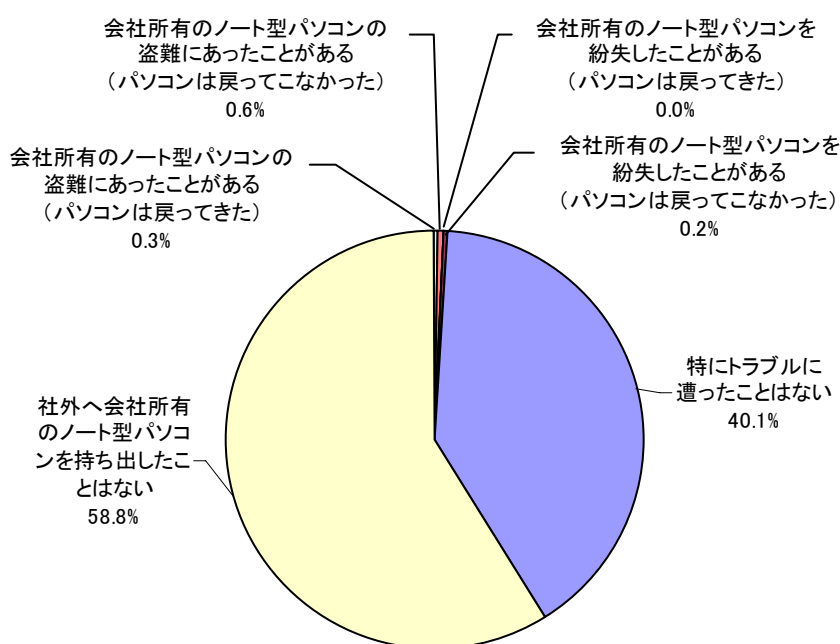
個人のパソコンを会社のLANにつなげることを禁じていますか。(回答は1つ)

## 4.8 会社所有のノート型パソコンに関するトラブル

会社所有のノート型パソコンに関するトラブルについての設問では、『特にトラブルに遭ったことはない』(40.1%)、『社外へ会社所有のノート型パソコンを持ち出したことはない』(58.8%)とを合わせると全体の98.9%を占めており、何らかのトラブルに巻き込まれた経験のある人はごく少数であることがわかる。

なお、回答数が少ないため傾向を論じることは適切ではないが、少なくとも今回の調査で得られた結果では、『会社所有のノート型パソコンを盗難、紛失して、パソコンは戻ってこなかった』という回答0.8%に対し、『会社所有のノート型パソコンを盗難、紛失して、パソコンは戻ってきた』という回答はわずか0.3%にとどまっており、社外へ持ち出したパソコンの情報管理についても、企業側として有効な対策を検討していく必要があるものと考えられる。

図 4-7 会社所有のノート型パソコンに関するトラブル



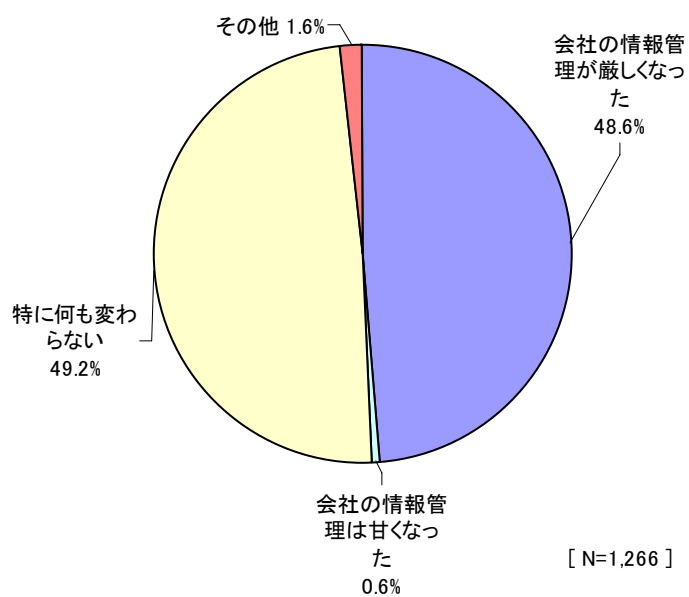
[ N=1,266 ]

あなたは社外へ会社所有のノート型パソコンを持ち出したとき、事故に遭遇したことはありませんか。最も近いものを1つお選びください。(回答は1つ)

## 4.9 勤め先の情報管理の状況

勤め先の情報管理の状況を1年前と比べてどのように感じるかという設問では、『特に何も変わらない』(49.2%)という回答と『会社の情報管理が厳しくなった』(48.6%)という回答がほぼ半数ずつを占めている。

図 4-8 勤め先の情報管理の状況



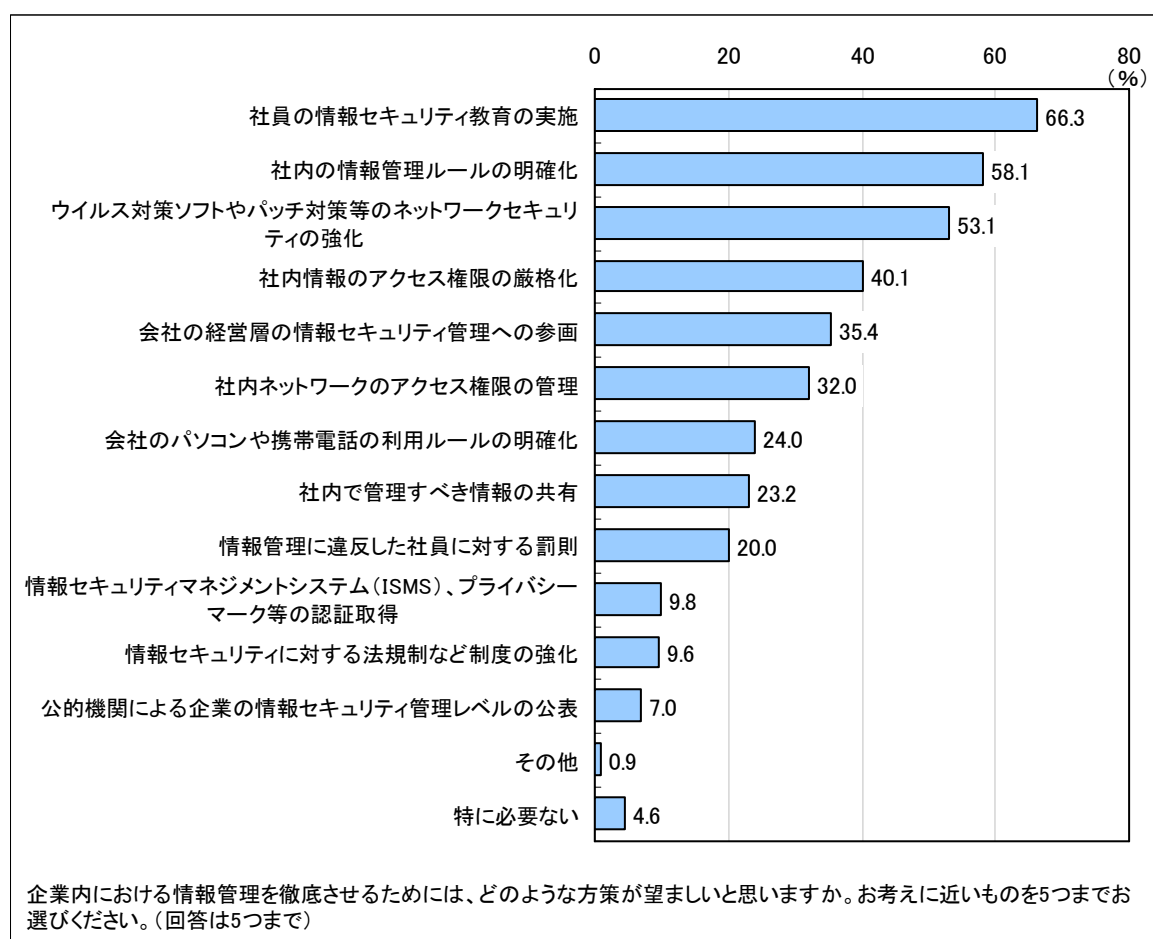
ここ1年ほどの間に、あなたの勤め先での情報管理はどのように変わったとお感じですか。(回答は1つ)

## 4.10 企業内の情報管理を徹底させる方策

企業内の情報管理を徹底させる方策についての設問では、『社員の情報セキュリティ教育の実施』(66.3%)、『社内の情報管理ルールの明確化』(58.1%)、『ウイルス対策ソフトやパッチ対策などのネットワークセキュリティの強化』(53.1%)、『社内情報のアクセス権限の厳格化』(40.1%)などが上位に挙がっている。

いずれも企業が情報セキュリティ対策を構ずる上では、必要不可欠な項目である。今回の回答結果から、『会社の経営層の情報セキュリティへの参画』、『情報管理に違反した社員に対する罰則』などの項目よりも、自社のセキュリティ教育の実施や社内の情報管理ルールを明確にすることなどを上位に挙げる声が社員の間では強いことが確認された。

図 4-9 企業内の情報管理を徹底させる方策





## NRIセキュアテクノロジーズ株式会社

〒100-0005 東京都千代田区丸の内1-6-5 丸の内北口ビル  
Tel : 03-5220-2022 Fax : 03-5220-2039  
ホームページ <http://www.nri-secure.co.jp/>  
メールアドレス [info@nri-secure.co.jp](mailto:info@nri-secure.co.jp)