



INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

2006情財第687号

2006年度第2回  
情報セキュリティに関する新たな  
脅威に対する意識調査 報告書

2007年7月

独立行政法人 情報処理推進機構

# 目次

1. 調査概要	2
調査概要	3
基本属性	4
2. 調査結果の概要	6
3. 調査結果	8
3.1. 新しいセキュリティ上の脅威に対する認識	9
3.2. 情報セキュリティに対する行動実態	31
3.3. インターネットの利用状況	54

参考 調査票

## 1. 調査概要

## 調査概要

- (1) 調査名 「インターネット利用と情報セキュリティに関するアンケート」
- (2) 調査目的 PCインターネット利用者への情報セキュリティ対策の普及啓発を実施するにあたり、情報セキュリティ関連の新たな脅威に対する認識をどの程度深めているかがひとつの目安となり、脅威への対策方法を作成するための有効なデータとして活用が期待できる。そのため、本調査を実施し、今後必要とされる対策を提供できるようにすることを目的とする。
- (3) 調査方法 ウェブアンケート調査
- 株式会社三菱総合研究所が調査設計・作成した調査票に基づき、株式会社マクロミルがリサーチモニターを対象に調査を実施した。
- (4) 調査対象 15歳以上のPCインターネット利用者
- (5) 調査期間 2007年3月30日(金)～2007年3月31日(土)
- (6) 有効回答数

5,316名(男性 50.0%・女性 50.0%、平均年齢 39.7歳)

各性別・年代別に分析を行うのに十分なサンプルを確保するために、性別・年代別に割付回収を行い、インターネット利用者数(「インプレス社「インターネット白書2006」」)に応じてウェイトバック集計を行った。

		母集団	母集団 (%)	回収数	ウェイト値	規正 標本数	規正 標本数(%)
男性	10代	3,284	6.0%	443	0.72	317	6.0%
	20代	5,306	9.6%	443	1.16	513	9.6%
	30代	5,631	10.2%	443	1.23	544	10.2%
	40代	5,596	10.2%	443	1.22	541	10.2%
	50代	4,958	9.0%	443	1.08	479	9.0%
	60代	3,896	7.1%	443	0.85	376	7.1%
女性	10代	3,507	6.4%	443	0.76	339	6.4%
	20代	5,683	10.3%	443	1.24	549	10.3%
	30代	5,989	10.9%	443	1.31	579	10.9%
	40代	5,442	9.9%	443	1.19	526	9.9%
	50代	3,671	6.7%	443	0.80	355	6.7%
	60代	2,055	3.7%	443	0.45	198	3.7%
合計		55,018	100.0%	5,316		5,316	100.0%

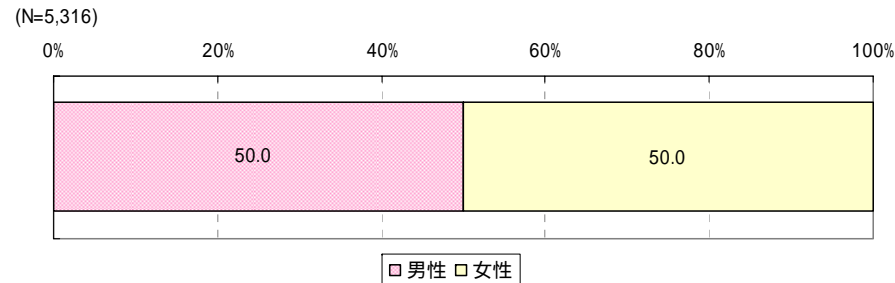
なお、「インターネット白書2006」の10代(15～19歳)のデータは、「13～15歳」及び「16～19歳」という区分になるため、平成18年国勢調査の人口比に基づき、15～19歳のデータを推計した。

- (7) 調査内容
- ・情報セキュリティ上の新たな脅威に対する認識、理解状況
  - ・情報セキュリティ上の新たな脅威の遭遇・被害経験
  - ・PC、インターネットの利用状況
  - ・情報セキュリティに関する対策状況
  - ・組織における情報セキュリティ対策の実施状況

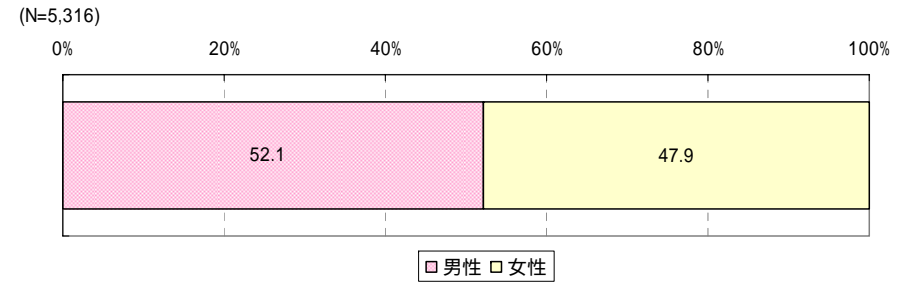
## 基本属性(1)

- ウェイトバック後の性別構成は、「男性」が52.1%、「女性」が47.9%である。
- ウェイトバック後の年齢構成は、「30代」をピークとする山形に分布し、「20代」「30代」「40代」が2割、「10代」および「60代」が1割強程度である。

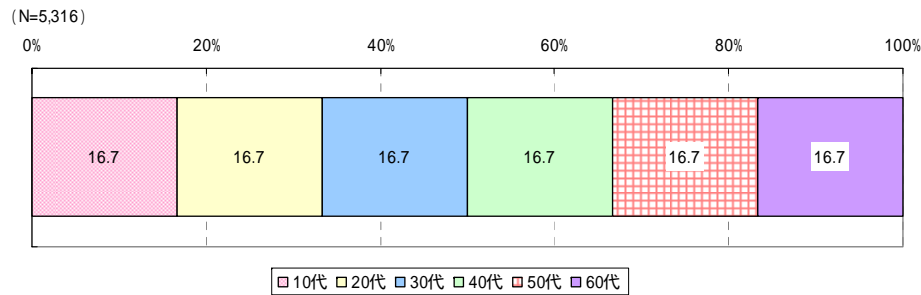
性別 [回答者全体]  
(ウェイトバック前)



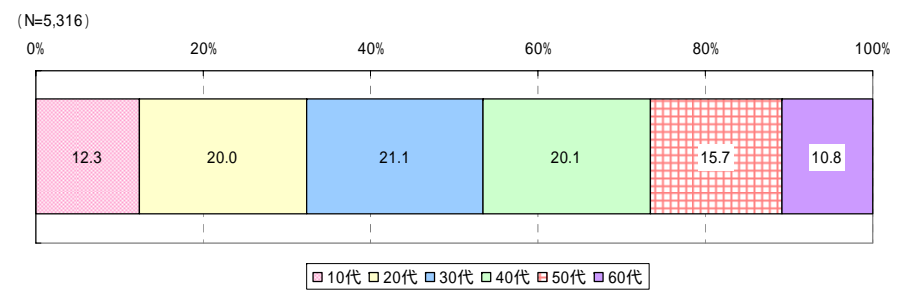
性別 [回答者全体]  
(ウェイトバック後)



年齢構成 [回答者全体]  
(ウェイトバック前)



年齢構成 [回答者全体]  
(ウェイトバック後)

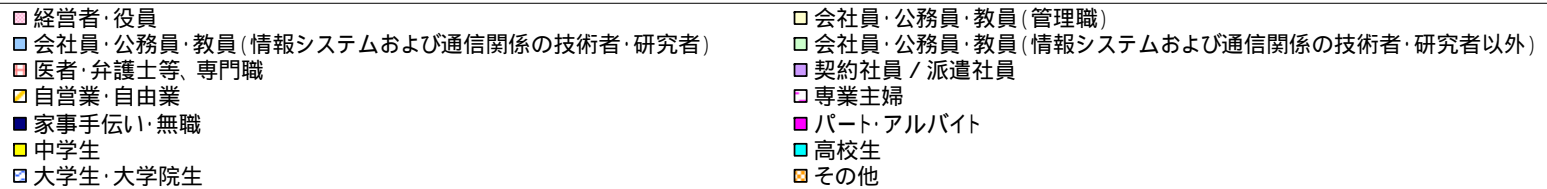
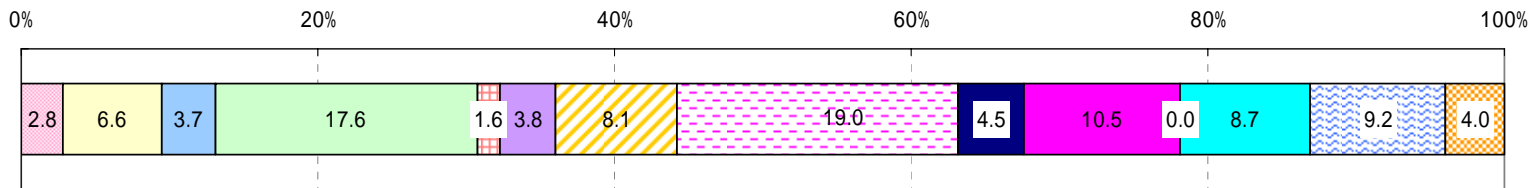


## 基本属性(2)

- ウェイトバック後の職業構成は、「会社員・公務員・教員」が最も多く32.2%、次いで専業主婦が17.7%である。

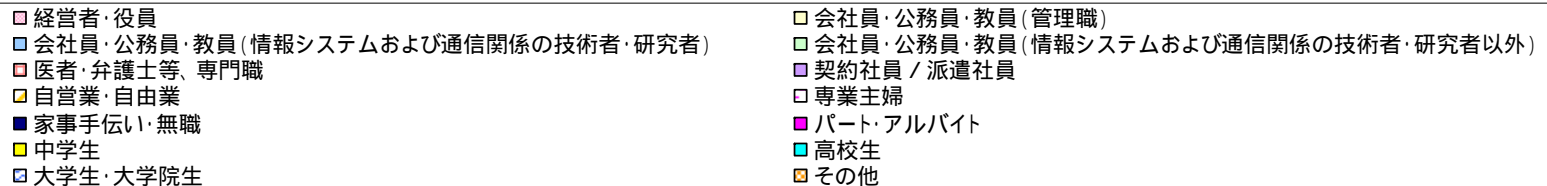
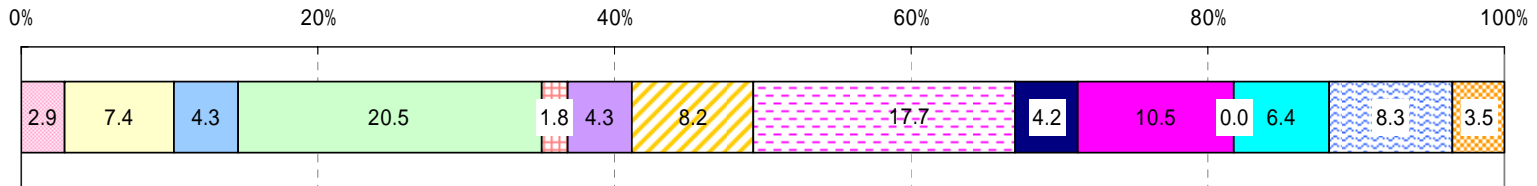
### 職業 [回答者全体] (ウェイトバック前)

(N=5,316)



### 職業 [回答者全体] (ウェイトバック後)

(N=5,316)



## 2. 調査結果の概要

## 情報セキュリティに関する新たな脅威に対する意識調査

**情報セキュリティに関して何らかの被害を受けているが、  
原因がわからない、提示された脅威以外の原因を選択している人が多い。**

原因不明・提示脅威以外との回答が、「知らない人からのメール受信」(22.8%)、  
「パソコンの起動異常やシステムの不調」(14.9%)、「個人情報流出」(7.9%)存在する。  
被害時の適切な対処のためにも、被害や対応の正しい理解を促すことが必要である。

「3.2.1. 情報セキュリティに関する被害状況(1)～(7)」(P32-38)参照

**実施率が全体的に低い対策は、メールの送信、ネットワーク接続に関わる対策、  
実施率がやや低い対策は、パスワード、OSに関わる対策である。**

「メール送信」「ネットワーク接続」「パスワード」「OS」等の対策の実施率は低く、  
特に、重点的に普及啓発を行う必要がある。

また、「定義ファイルの更新を行っている」「パッチをあてて最新の状態にしておく」といった対策は、  
自動更新機能があるため、あまり意識的に行われていない可能性がある。  
技術の発達によって実質的なセキュリティレベルが向上する反面、被害時や未知の脅威への適切な対処のためには、  
セキュリティに関わる脅威と対策に関する最低限の知識の提供を、継続的に行うべきである。

「3.2.2 情報セキュリティ対策の実施状況(1)～(9)」(P39-47)参照

**組織の情報セキュリティに関する規定は6割以上が策定、うち8割以上が遵守。  
しかし、「経営者・役員」「契約社員・派遣社員」は、情報セキュリティを「非常に重要である」  
とする回答率が低く、属する組織の規定について「未策定」や「わからない」との回答が多い。**

組織の情報セキュリティ関連規定に対して、「経営者・役員」が属する組織では「策定されていない」(38.2%)が多く、  
「契約社員・派遣社員」では「わからない」(43.1%)が多い。

「経営者・役員」「契約社員・派遣社員」は情報セキュリティに対して「非常に重要である」との回答も少ない。  
企業においては、「経営者・役員」や「契約社員・派遣社員」に対する意識啓発が有効である。

「3.1.3 情報セキュリティに対する考え(2)」(P29)、

「3.2.3 組織における情報セキュリティ対策の実施状況(1)」(P50)参照

### 3. 調査結果

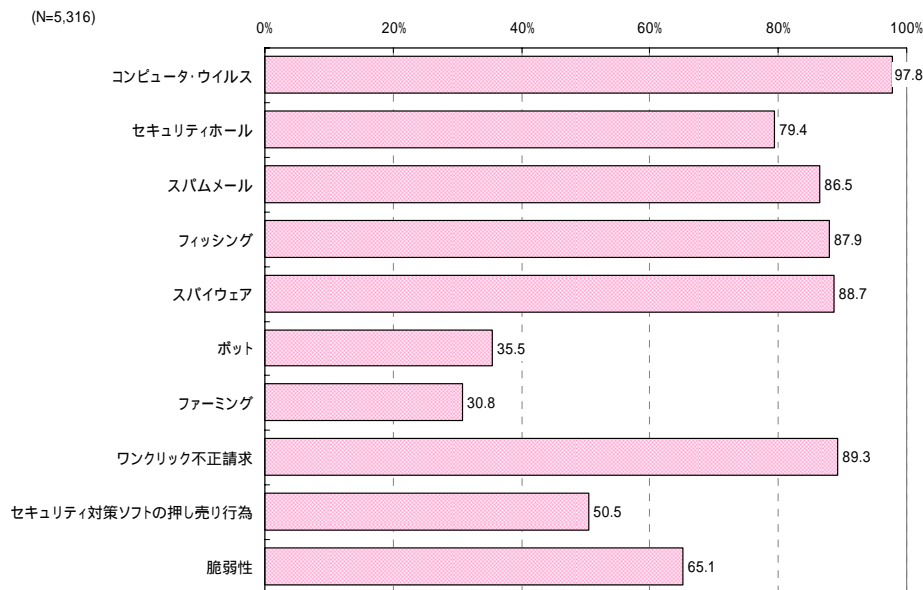
パーセンテージ数値は小数点第2位以下を四捨五入しているため、個々の数値の合計値は100%にならない場合がある。

### 3.1. 新しいセキュリティ上の脅威に対する認識

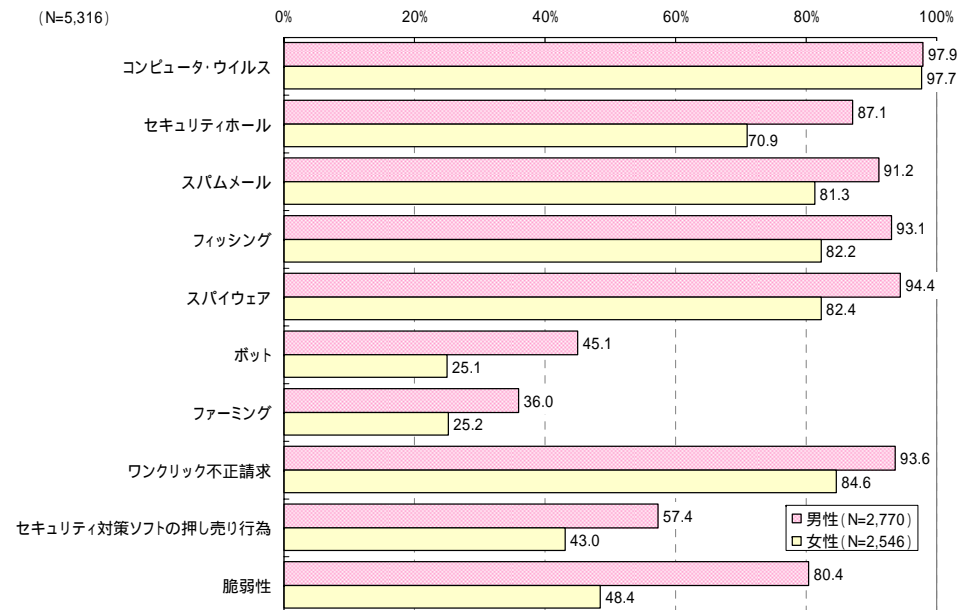
### 3.1.1. 情報セキュリティに関する言葉の認知度(1)

- 回答者全員に情報セキュリティに関する言葉について、聞いたことがあるか、事象を知っているかを選んでもらった。
- 「言葉を聞いたことがある」とした認知度が最も高いものは「コンピュータ・ウイルス」で、次いで「ワンクリック不正請求」、「スパイウェア」、「フィッシング」、「スパムメール」、「脆弱性」が続き、いずれも60%を超えている。「ボット」、「ファームング」は認知度が低い。
- [性別]では、言葉の認知度は総じて男性のほうが高い。特に、「ボット」「ファームング」の女性の認知度は、約25%に留まる。

情報セキュリティに関する言葉の認知度 [回答者全体]  
(複数回答)



情報セキュリティに関する言葉の認知度 [性別]  
(複数回答)

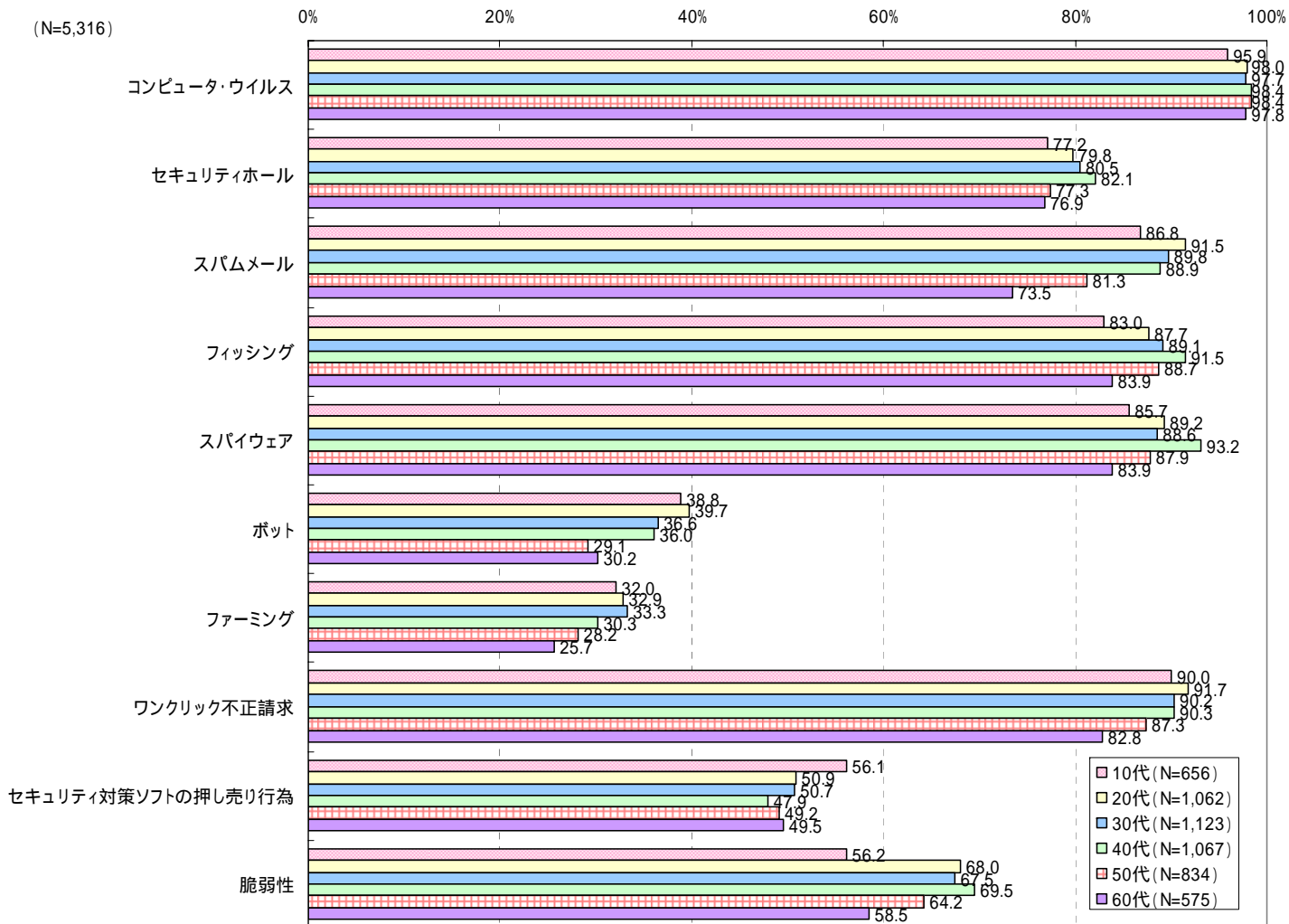


### 3.1.1. 情報セキュリティに関する言葉の認知度(2)

- 回答者全員に情報セキュリティに関する言葉について、聞いたことがあるか、事象を知っているかを選んでもらった。
- [年代別]では、20代～40代の認知度が高い傾向にあるが、言葉によって最も認知度が高い年代は異なる。

情報セキュリティに関する言葉の認知度 [年代別]

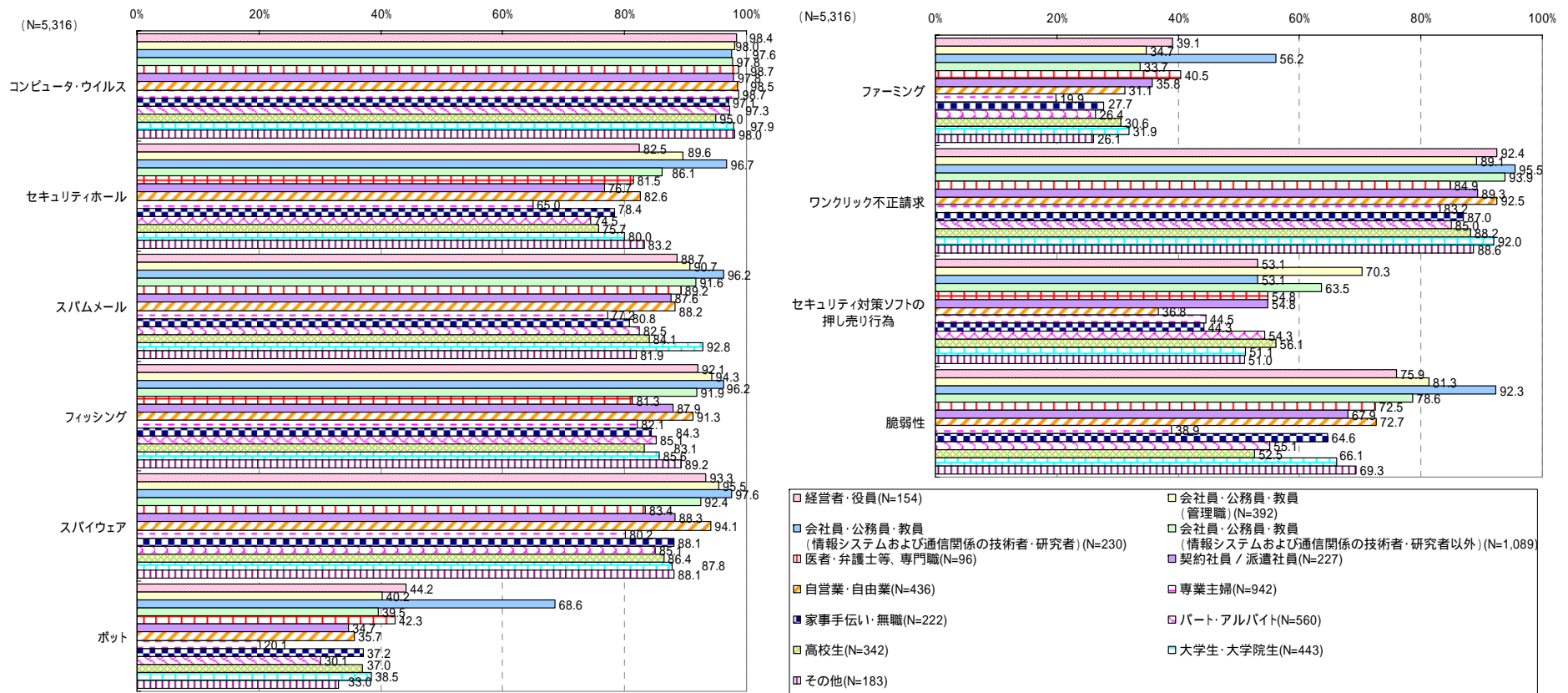
(複数回答)



### 3.1.1. 情報セキュリティに関する言葉の認知度(3)

- 回答者全員に情報セキュリティに関する言葉について、聞いたことがあるか、事象を知っているかを選んでもらった。
- [職業別]では、「コンピュータ・ウイルス」「ワンクリック不正請求」などの言葉は職業別の差異はなく全体的に認知度は高いが、「ボット」や「ファームング」など全体的に認知度の低い言葉については、「会社員・公務員・教員(情報システムおよび通信関係の技術者・研究者)」以外にほとんど認知されていない。

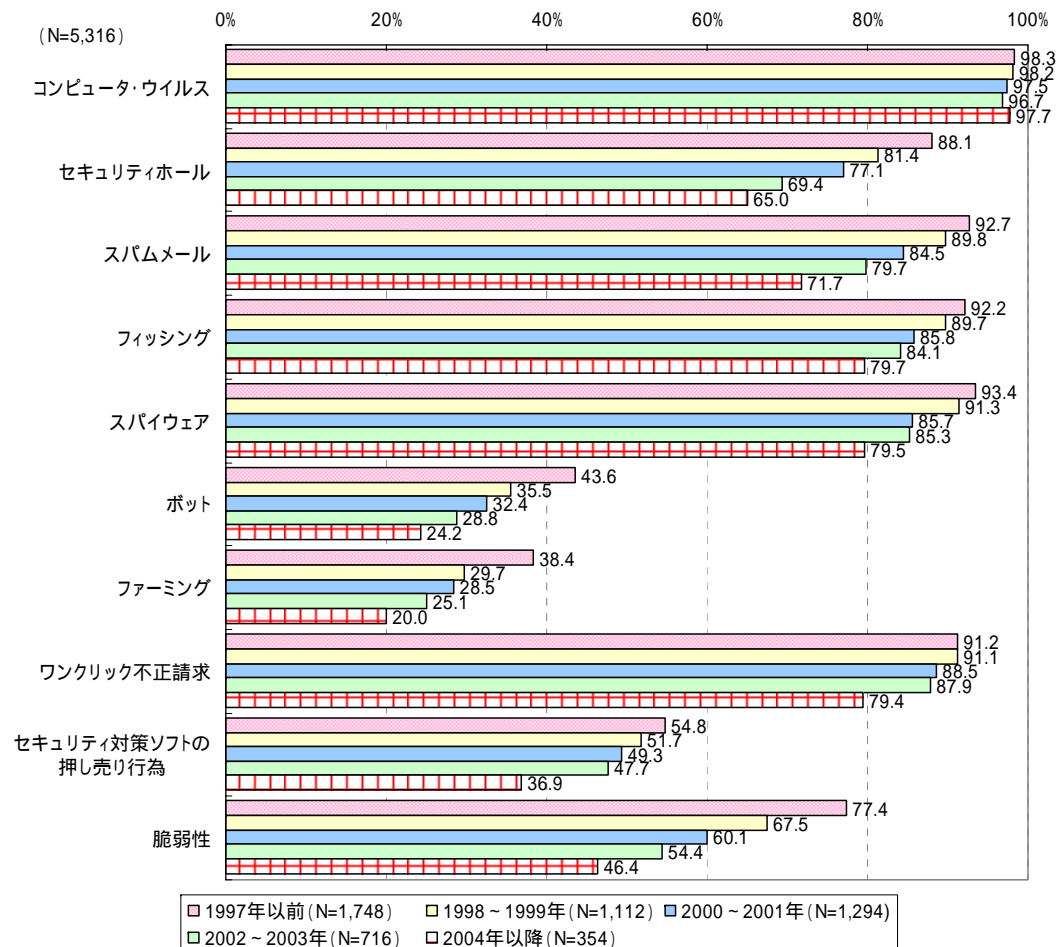
情報セキュリティに関する言葉の認知度 [職業別]  
(複数回答)



### 3.1.1. 情報セキュリティに関する言葉の認知度(4)

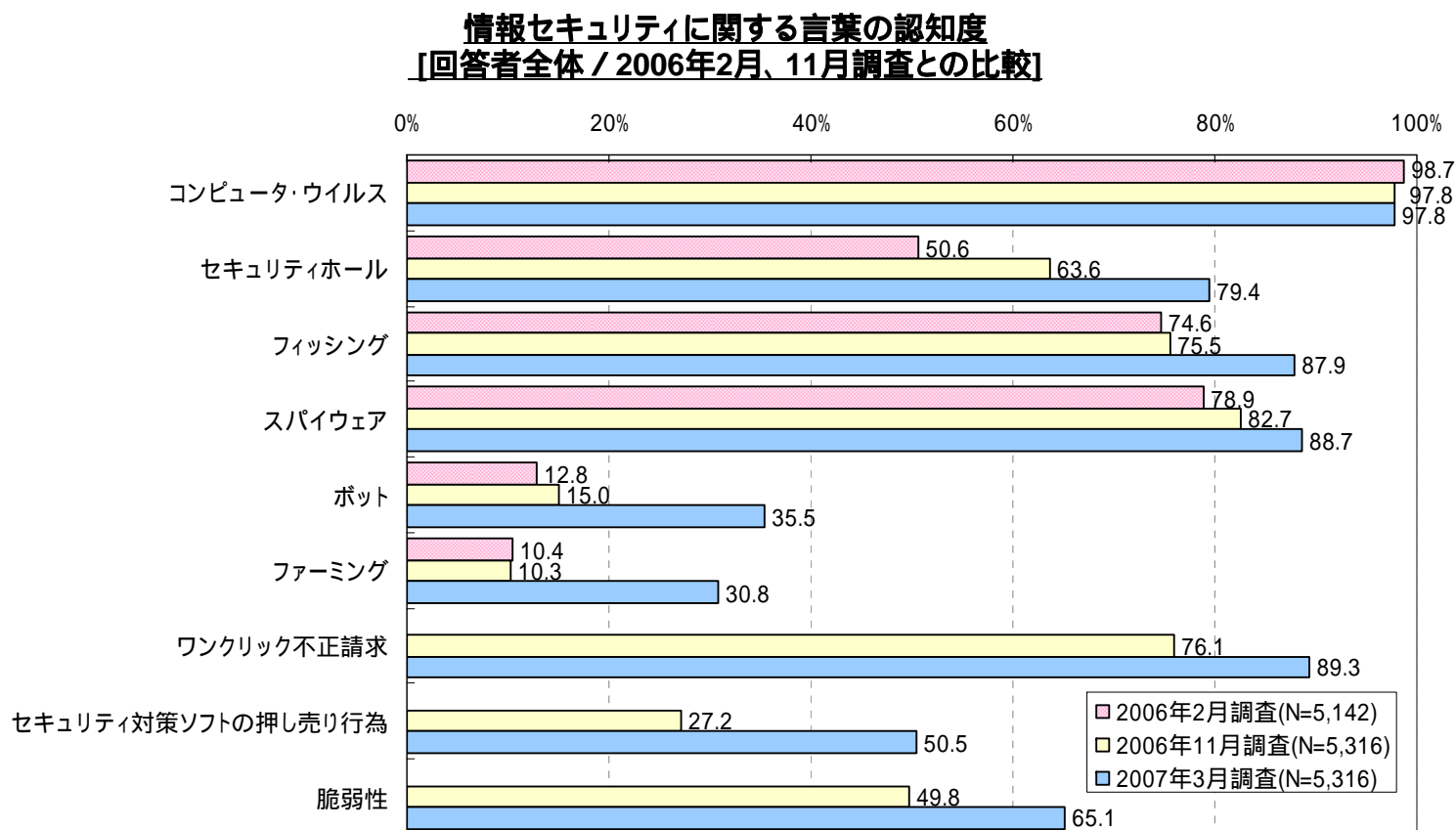
- 回答者全員に情報セキュリティに関する言葉について、聞いたことがあるか、事象を知っているかを選んでもらった。
- [インターネット開始時期別]では、「コンピュータ・ウイルス」については開始時期の差異はなく全体的に認知度は高いが、その他の言葉については、インターネット利用年数が長いほど、認知度が高い傾向にある。

情報セキュリティに関する言葉の認知度 [インターネット利用開始時期別]  
(複数回答)



### 3.1.1. 情報セキュリティに関する言葉の認知度(5)

- 情報セキュリティに関する言葉の認知度について、前回、前々回調査の類似設問と参考比較を行った。
- 「コンピュータ・ウイルス」については、既に言葉の認知度が高いため前回・前々回調査と認知度の違いは見られない。しかし、その他の言葉については、前回・前々回調査の認知度より10～20ポイントの上昇が見られ、設問形式の違いによって認知度が高めに表れた可能性が考えられる。

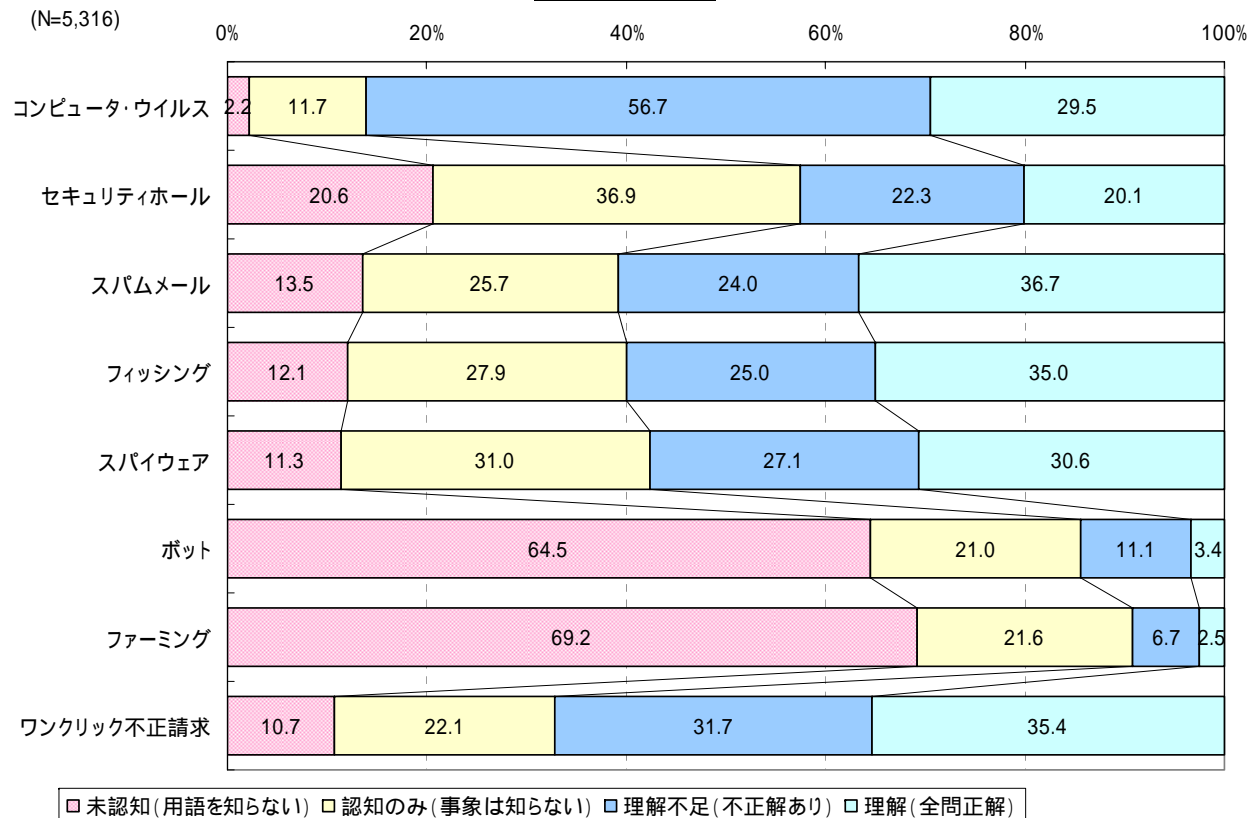


2006年実施した2回の調査と設問形式を変更したため、参考比較である

### 3.1.2 情報セキュリティに関する事象の理解度(1)

- 情報セキュリティに関する8つの事象のうち、言葉の認知、事象の認知、および正誤問題の正当数にもとづいて全回答者の理解度を4分類した。
- 情報セキュリティの新たな脅威に対する認知・理解状況を尋ねたところ、「コンピュータ・ウイルス」に関しては、ほぼ100%が言葉を認知していたが、事象の正しい理解度は設問の難易度が若干高かったことも有り、3割に留まった。
- 「スパムメール」「フィッシング」「スパイウェア」「ワンクリック不正請求」に関しては、8割以上が言葉を認知しており、事象の正しい理解度は3割を超える。
- 「ボット」「ファームング」に関しては、言葉の認知度自体が4割以下に留まった。

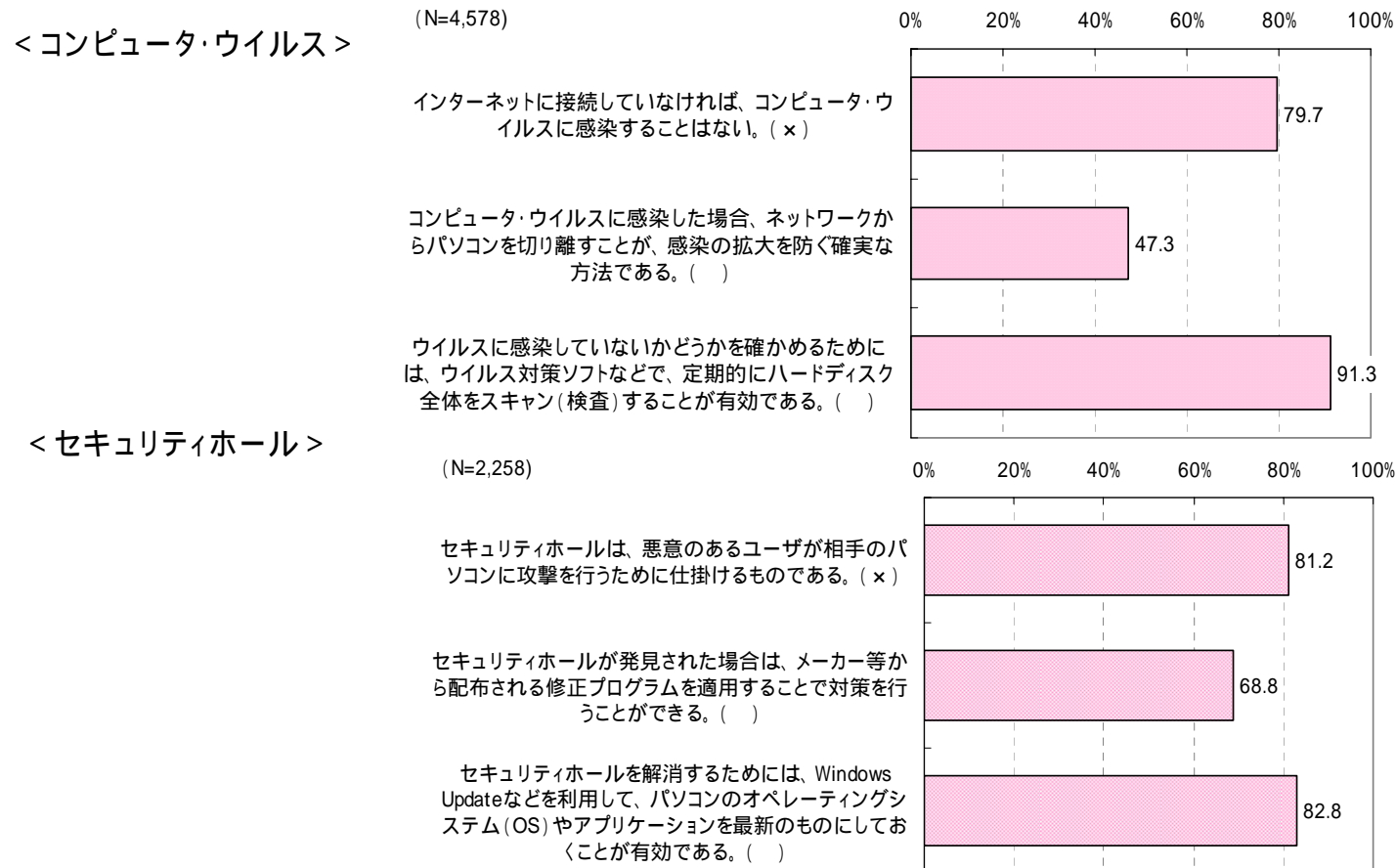
情報セキュリティに関する事象の理解度  
[回答者全体]



## 3.1.2 情報セキュリティに関する事象の理解度(2)

- 情報セキュリティに関する各事象について、「知っている」と答えた人にその事象に関連する記述を3つ示して正誤判定をしてもらった。各記述の正答率は以下のとおり。文末の( ) (×)は正誤の回答を示す。
- 「コンピュータ・ウイルス」については、1問正答率が低い設問があり、正しい理解度は結果的に低くなった。
- 「セキュリティホール」に関しては、2問の正答率が8割を超えたが、発見時の対応に関する正答率が7割を下回った。

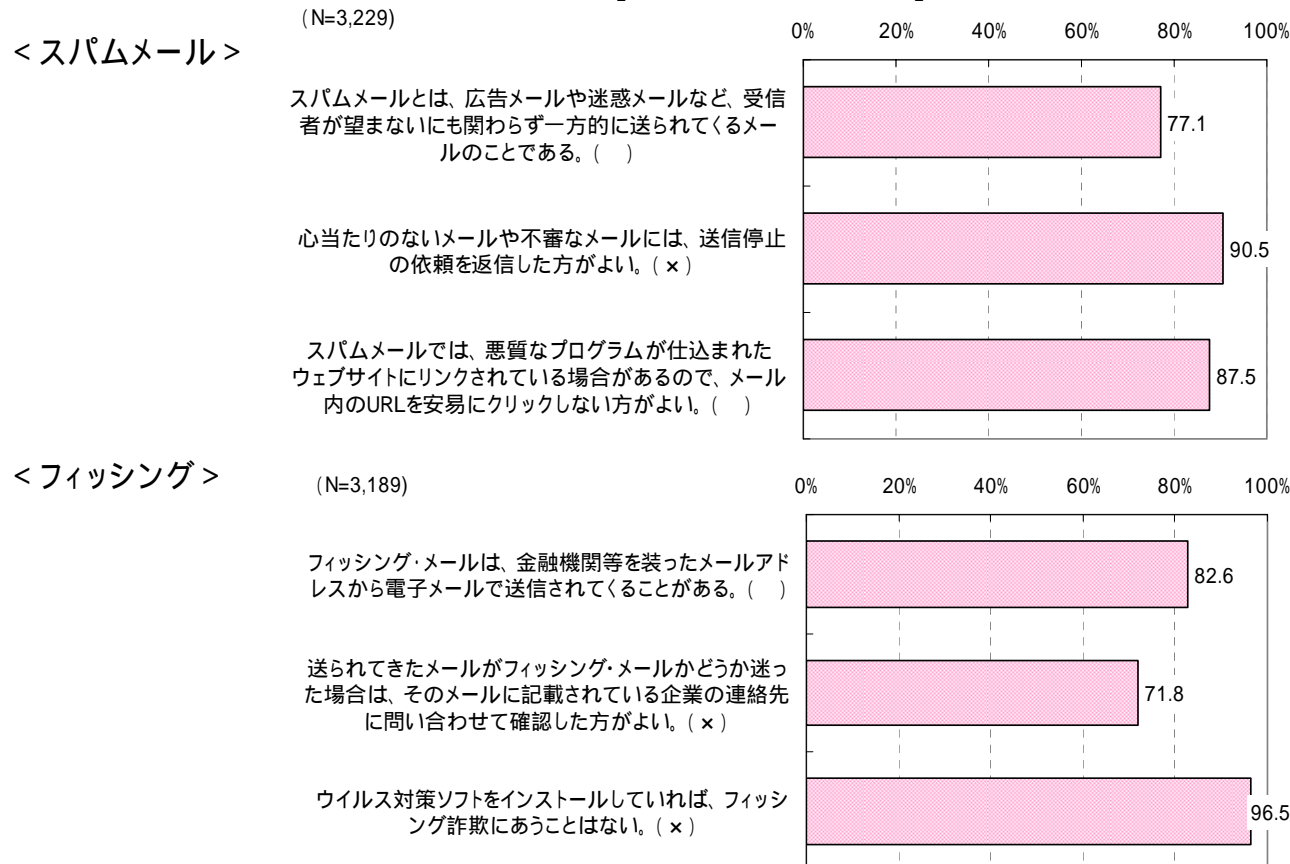
### 情報セキュリティに関する事象の理解度 - 正誤問題の正答率 [各事象の認知者全体]



## 3.1.2 情報セキュリティに関する事象の理解度(3)

- 情報セキュリティに関する各事象について、「知っている」と答えた人にその事象に関連する記述を3つ示して正誤判定をしてもらった。各記述の正答率は以下のとおり。文末の( ) (×)は正誤の回答を示す。
- 「スパムメール」に関しては、定義に関する設問の正答率が8割を下回ったが、発見時の対応に関する設問の正答率は9割程度に達した。
- 「フィッシング」に関しては、ソフトの対策だけでは有効でない点に言及する設問の正答率が高かった。

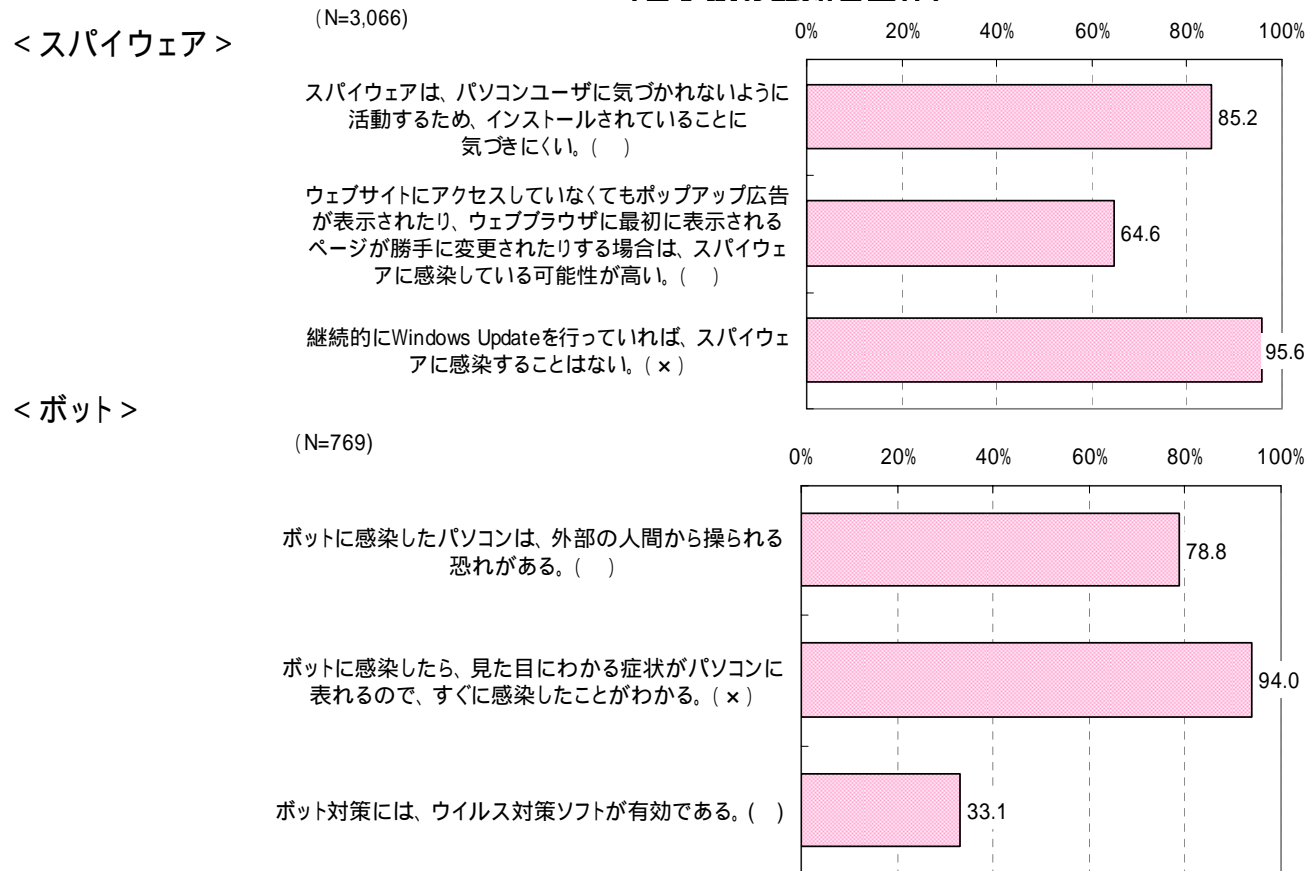
### 情報セキュリティに関する事象の理解度 - 正誤問題の正答率 [各事象の認知者全体]



## 3.1.2 情報セキュリティに関する事象の理解度(4)

- 情報セキュリティに関する各事象について、「知っている」と答えた人にその事象に関連する記述を3つ示して正誤判定をしてもらった。各記述の正答率は以下のとおり。文末の( ) (×)は正誤の回答を示す。
- 「スパイウェア」に関しては、感染予防のための対策の正答率は高い一方、スパイウェアに感染した場合の現象に関する正答率は低い。
- 「ボット」に関しては、感染時の現象についての正答率は高いが、有効な対策方法に関する設問の正答率は3割と低い。

### 情報セキュリティに関する事象の理解度 - 正誤問題の正答率 「各事象の認知者全体」



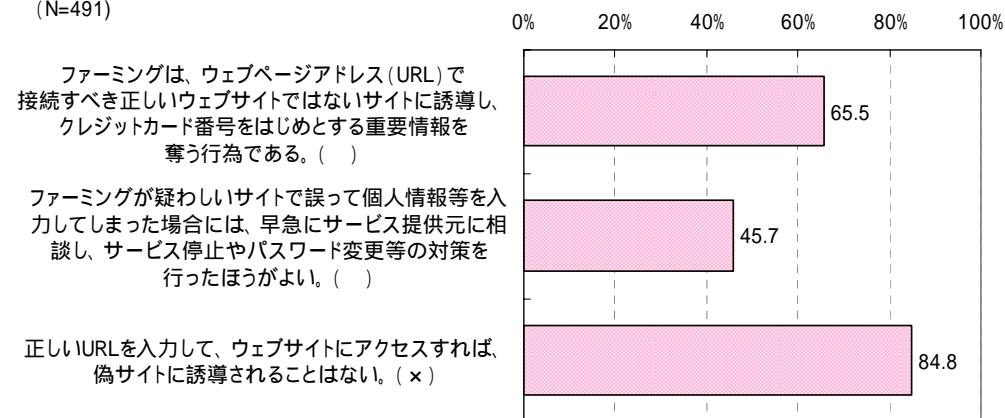
## 3.1.2 情報セキュリティに関する事象の理解度(5)

- 情報セキュリティに関する各事象について、「知っている」と答えた人にその事象に関連する記述を3つ示して正誤判定をしてもらった。各記述の正答率は以下のとおり。文末の( ) (×)は正誤の回答を示す。
- 「ファームング」に関しては、予防策に関する正答率が高いが、疑わしい場合の対応に関する正答率は5割を下回る。
- 「ワンクリック不正請求」に関しては、定義と予防策に関しては正答率が8割を超えたが、盗まれた個人情報の内容に関する設問の正答率が若干低かった。

### 情報セキュリティに関する事象の理解度 - 正誤問題の正答率 [各事象の認知者全体]

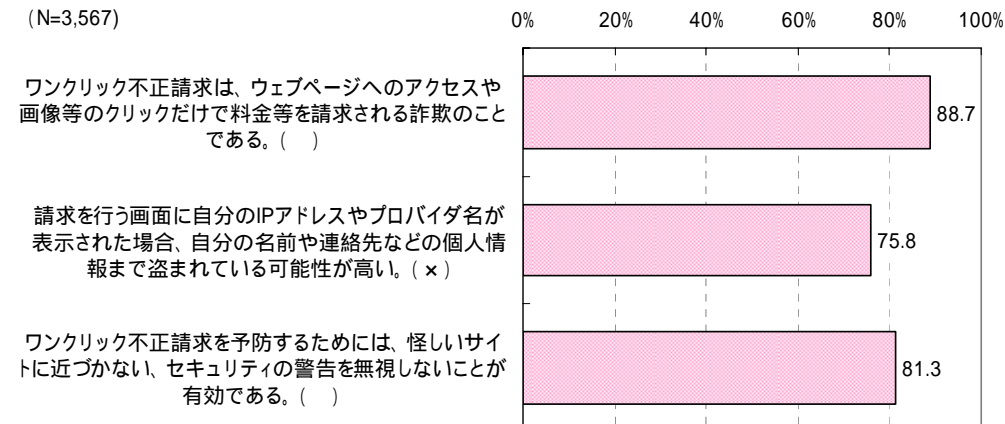
#### < ファームング >

(N=491)



#### < ワンクリック不正請求 >

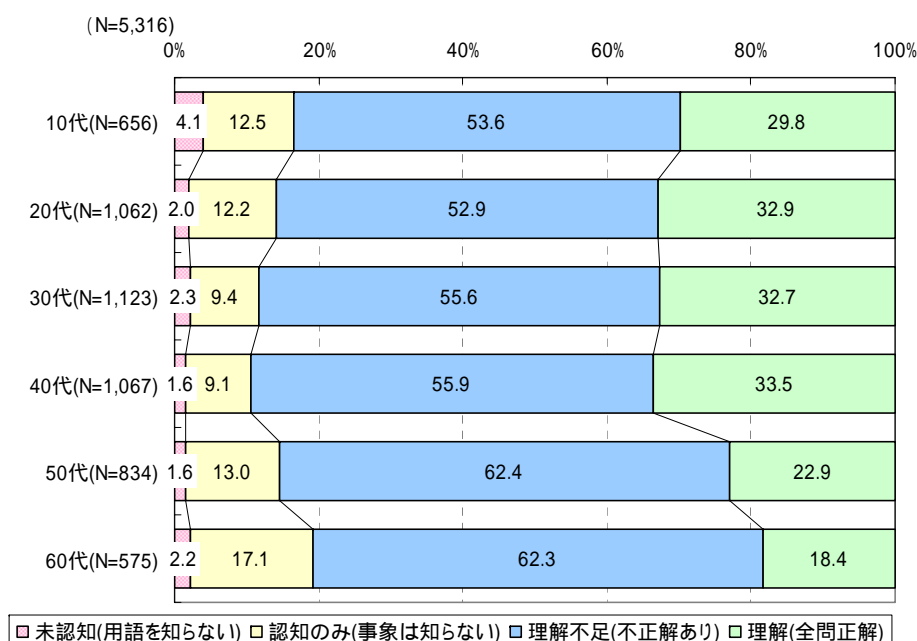
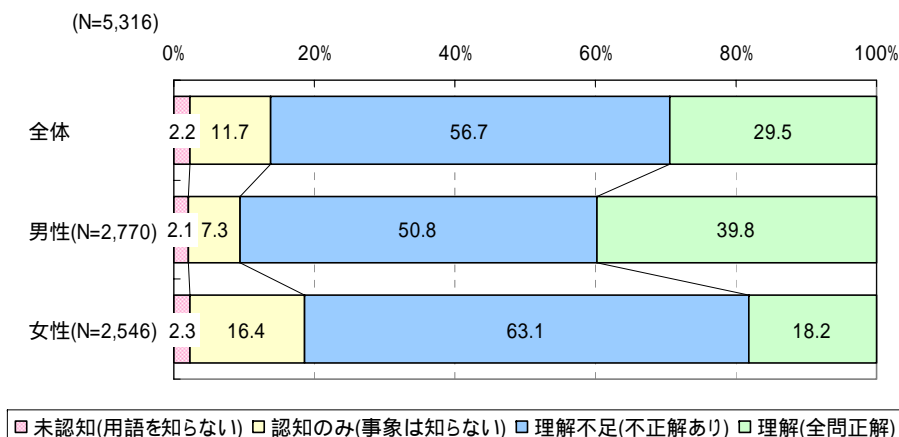
(N=3,567)



### 3.1.2 情報セキュリティに関する事象の理解度(6) - コンピュータ・ウイルス

- 「コンピュータウイルス」に関しては、ほぼ全ての回答者が言葉を認知しているが、設問の難易度の関係もあり、3問正解は3割程度であった。
- [性別]で見ると、言葉の認知率にあまり差はないが、3問正答率は男性で4割、女性で2割と正しい理解度に差がある。
- [年代別]でも、言葉の認知率はいずれの年代も9割を超える。3問正答率は50代と60代でやや低いがその他の年代は3割前後である。

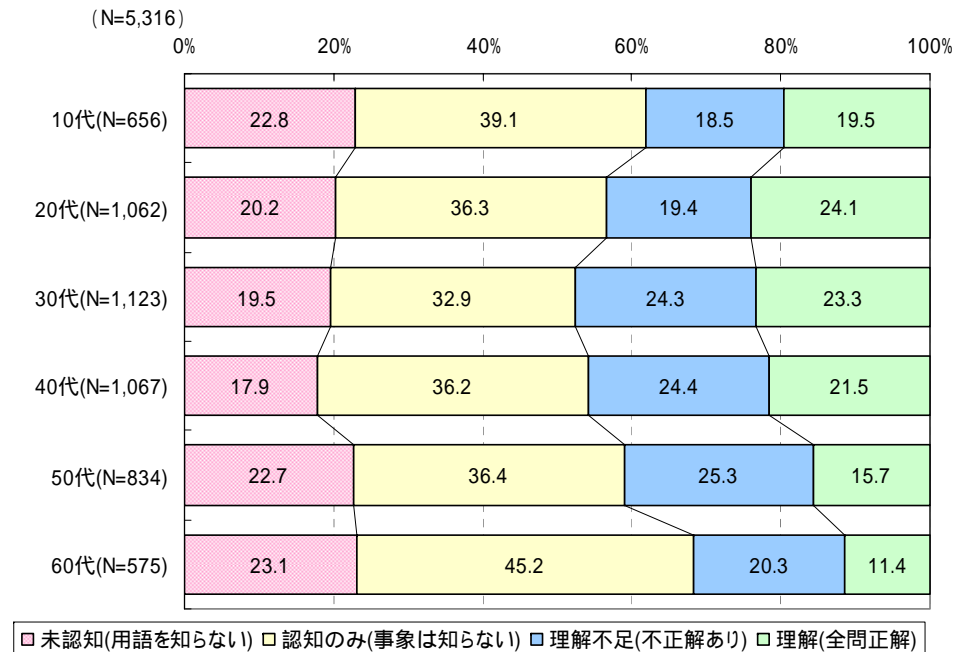
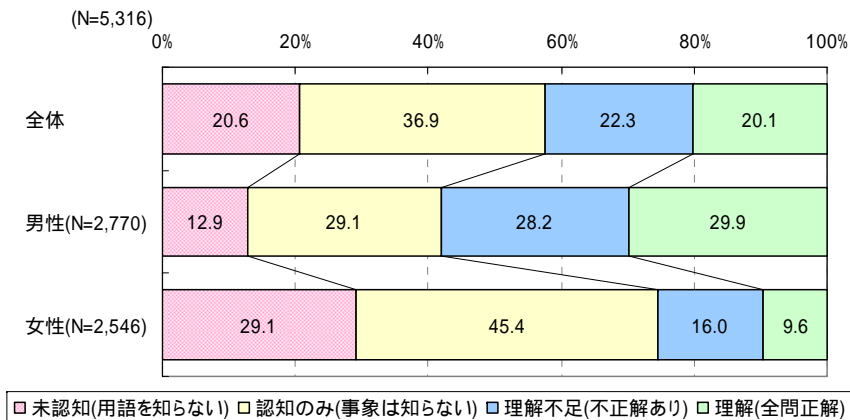
情報セキュリティに関する事象の理解度 - 正誤問題の正答数  
<コンピュータ・ウイルス>



### 3.1.2 情報セキュリティに関する事象の理解度(7) - セキュリティホール

- 「セキュリティホール」に関しては、8割程度が言葉を認知しているが、事象のみしか認知していない層が4割程度であり、3問正答の回答者も約2割である。
- [性別]で見ると、言葉の認知率が男性約9割、女性約7割である。3問正答率でも、男性で約3割、女性で1割弱と差がある。
- [年代別]では、認知率に大きな差はないが、3問正答率は50代・60代で低い。

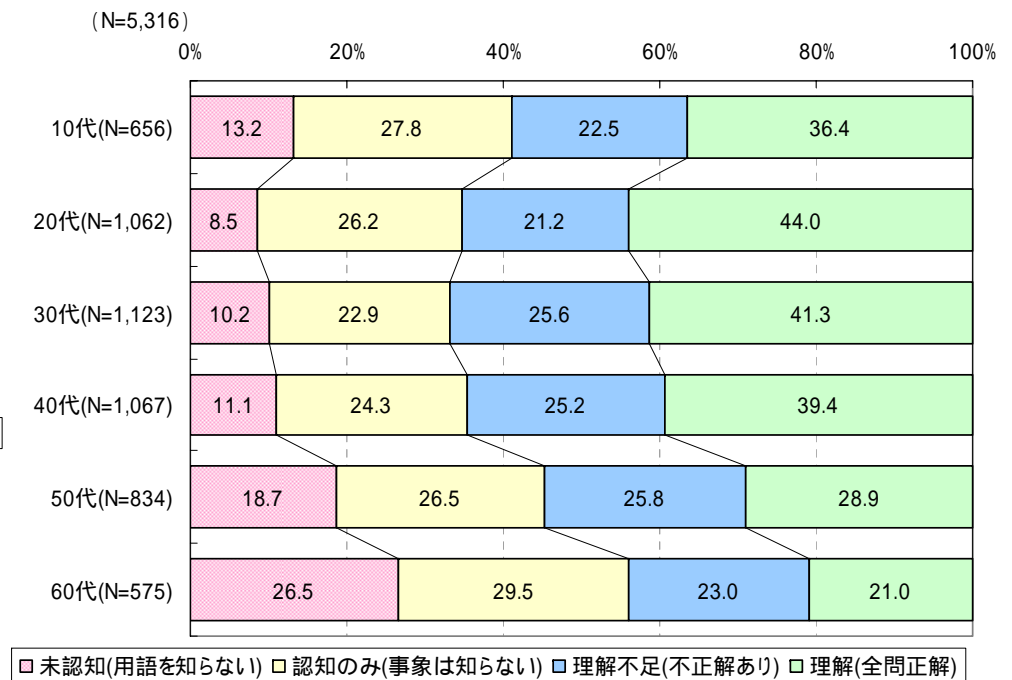
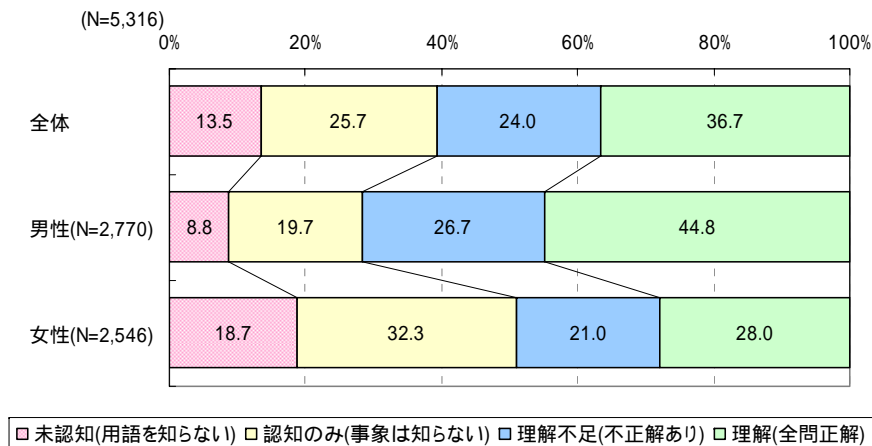
情報セキュリティに関する事象の理解度 - 正誤問題の正答数  
<セキュリティホール>



### 3.1.2 情報セキュリティに関する事象の理解度(8) - スпамメール

- 「スパムメール」に関しては、8割以上が言葉を認知しており、3問正答の回答者も4割近くに達する。
- [性別]で見ると、言葉の認知率が男性9割超、女性8割超と差がある。3問正答率では、男性で5割弱、女性で3割弱とその差はさらに開く。
- [年代別]では、50～60代にかけて、言葉の認知率・3問正答率が低下する。

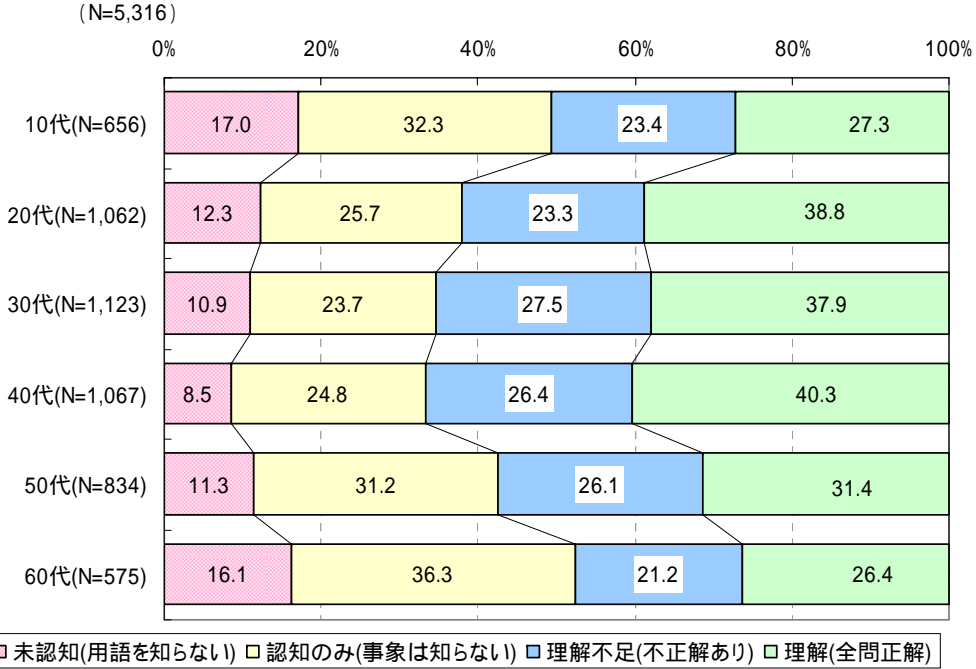
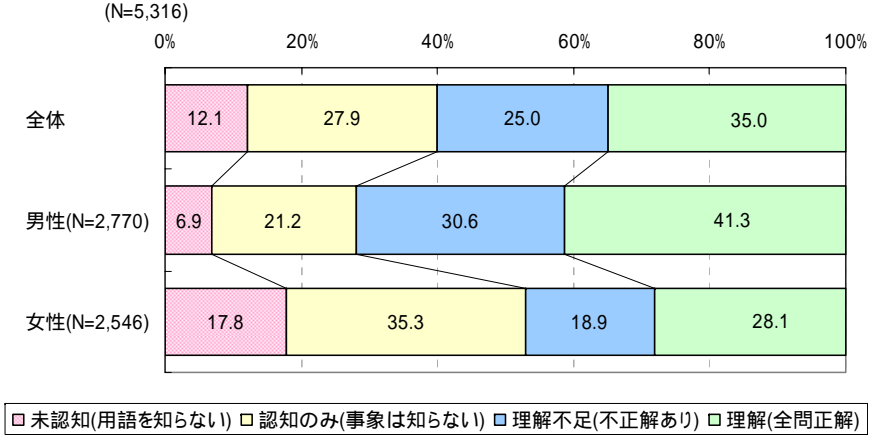
情報セキュリティに関する事象の理解度 - 正誤問題の正答数  
<スパムメール>



# 3.1.2 情報セキュリティに関する事象の理解度(9) - フィッシング

- 「フィッシング」に関しては、9割近くが言葉を認知しており、3問正答の回答者も3割を超える。
- [性別]で見ると、言葉の認知率が男性9割超、女性8割超と差がある。3問正答率でも、男性で4割強、女性で3割弱とその差が開く。
- [年代別]では、10代および60代の言葉の認知率・3問正答率が低い。

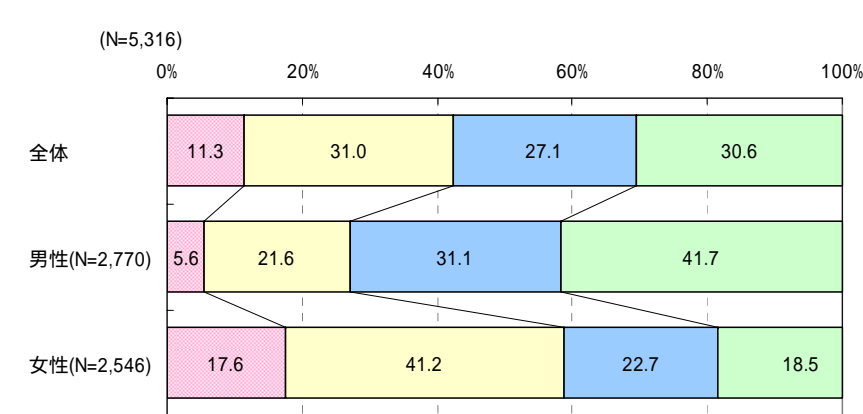
情報セキュリティに関する事象の理解度 - 正誤問題の正答数  
<フィッシング>



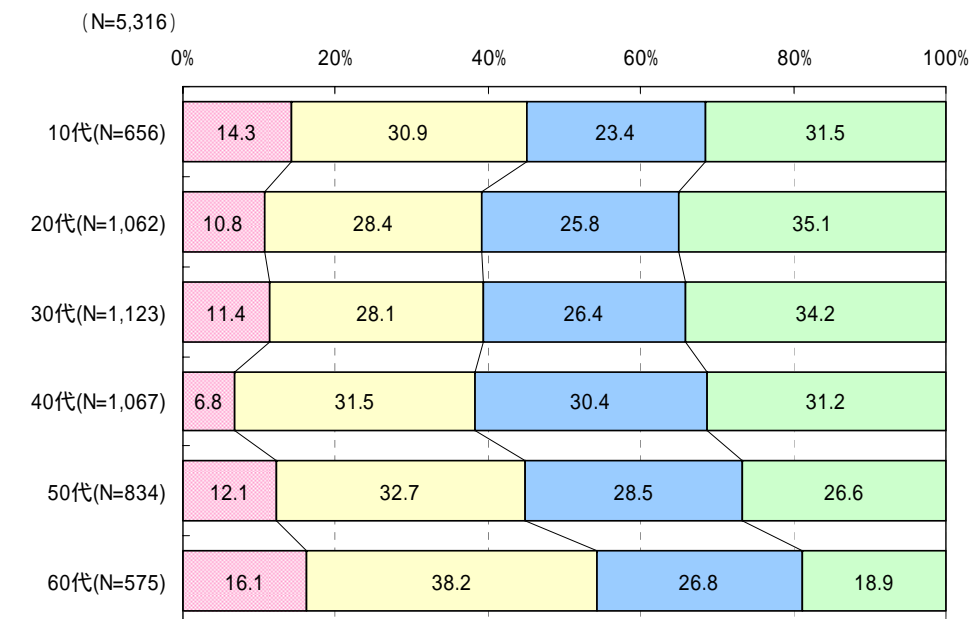
### 3.1.2 情報セキュリティに関する事象の理解度(10) - スパイウェア

- 「スパイウェア」に関しては、ほぼ9割が言葉を認知しており、3問正答率も3割に達する。
- [性別]で見ると、言葉の認知率が男性9割超、女性8割超と差がある。3問正答率は男性で約4割、女性で2割弱と大きく差が開く
- [年代別]では、10代および60代の言葉の認知率がやや低く、3問正答率は60代が最も低い。

情報セキュリティに関する事象の理解度 - 正誤問題の正答数  
<スパイウェア>



□ 未認知(用語を知らない) □ 認知のみ(事象は知らない) □ 理解不足(不正解あり) □ 理解(全問正解)

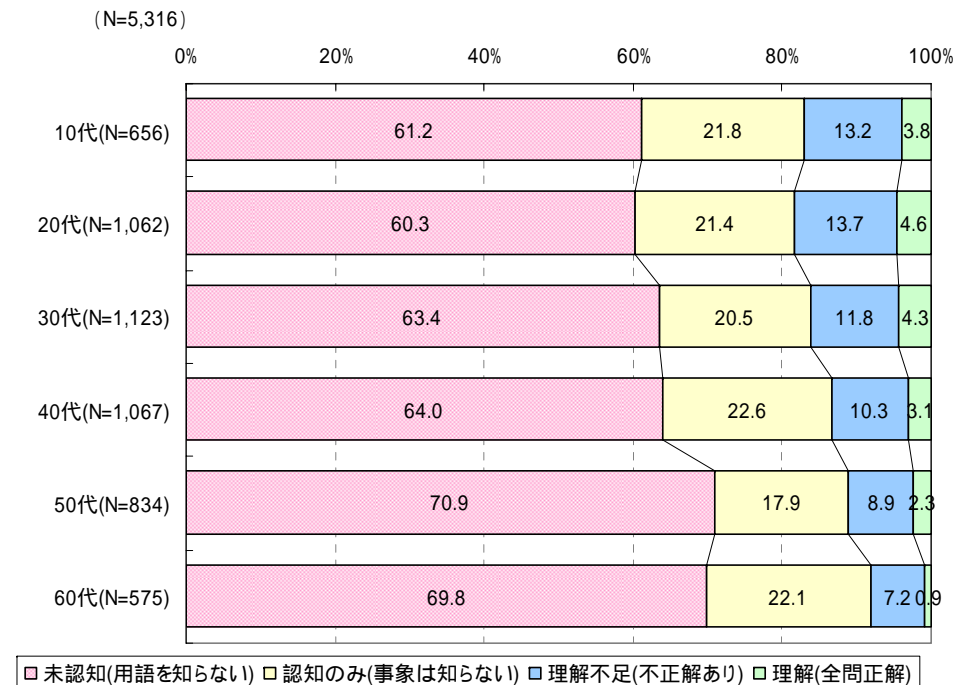
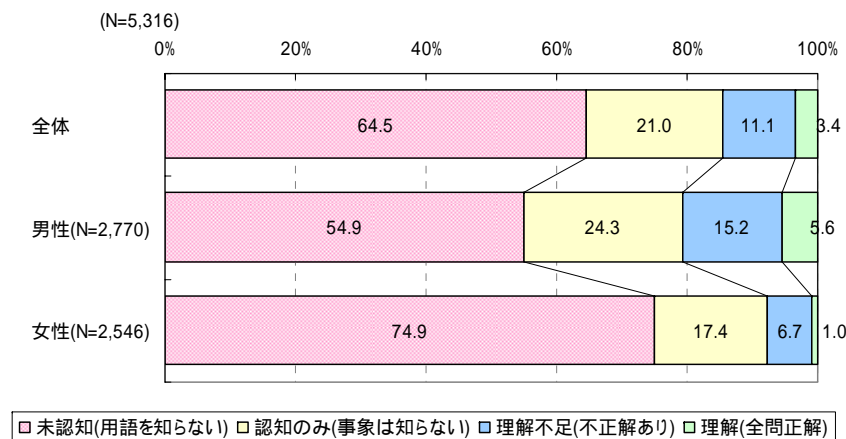


□ 未認知(用語を知らない) □ 認知のみ(事象は知らない) □ 理解不足(不正解あり) □ 理解(全問正解)

## 3.1.2 情報セキュリティに関する事象の理解度(11) - ボット

- 「ボット」に関しては、3割超しか言葉を認知しておらず、3問正答の回答者も1割未満と極わずかに留まる。
- [性別]で見ると、言葉の認知率が男性4割超、女性3割未満と差は見られるが、いずれも低く、3問正答率もいずれも1割に満たない。
- [年代別]では、全体的に認知度・3問正答率とも非常に低い。

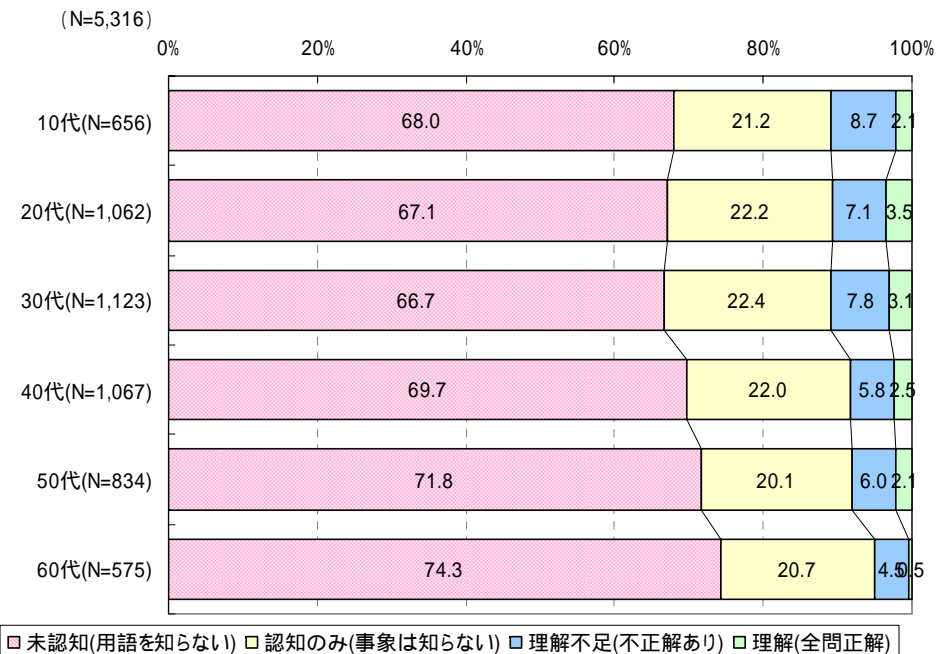
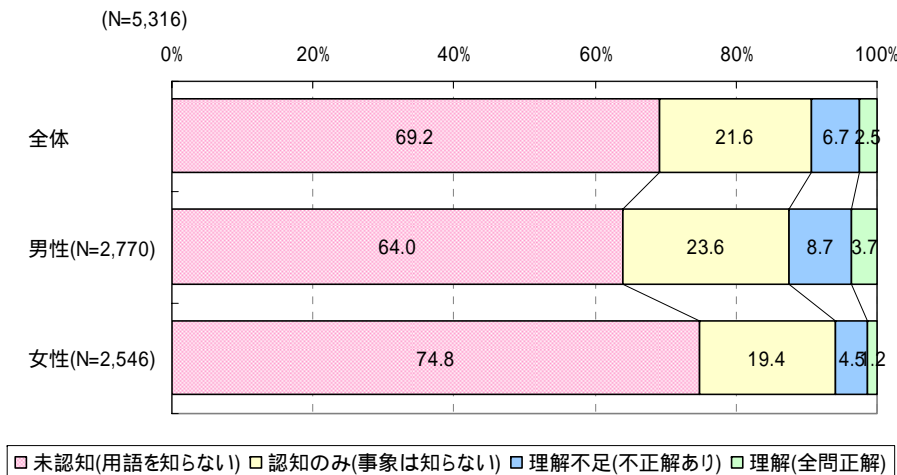
情報セキュリティに関する事象の理解度 - 正誤問題の正答数  
<ボット>



### 3.1.2 情報セキュリティに関する事象の理解度(12) - ファーミング

- 「ファーミング」に関しては、約3割しか言葉を認知しておらず、3問正答の回答者は1割未満と極わずかに留まる。
- [性別]で見ると、言葉の認知率が男性3割超、女性2割超と差は見られるが、いずれも低い。
- [年代別]でも、全体的に認知度・3問正答率とも非常に低い。

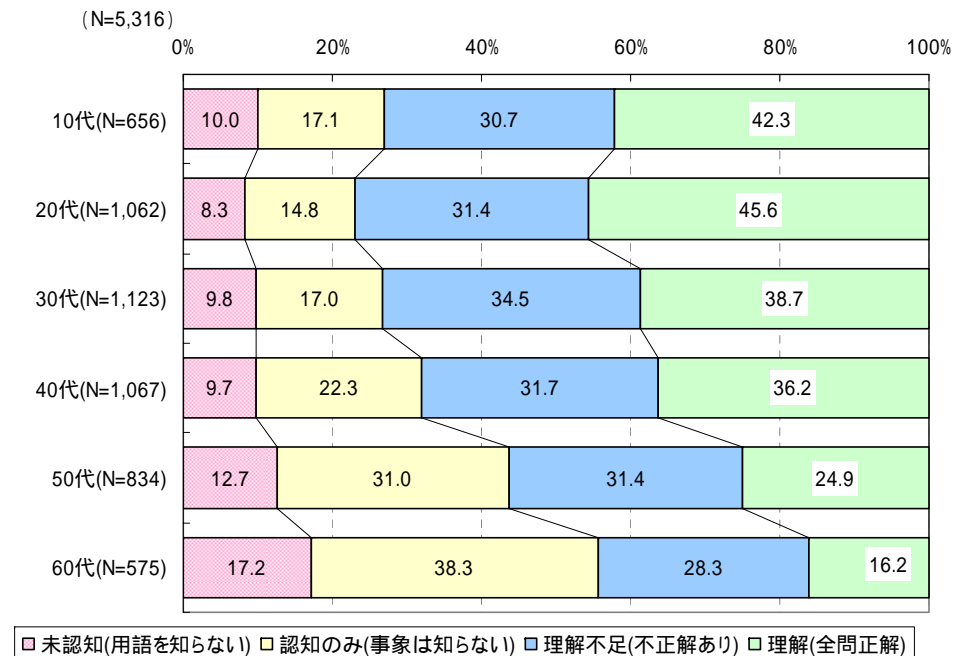
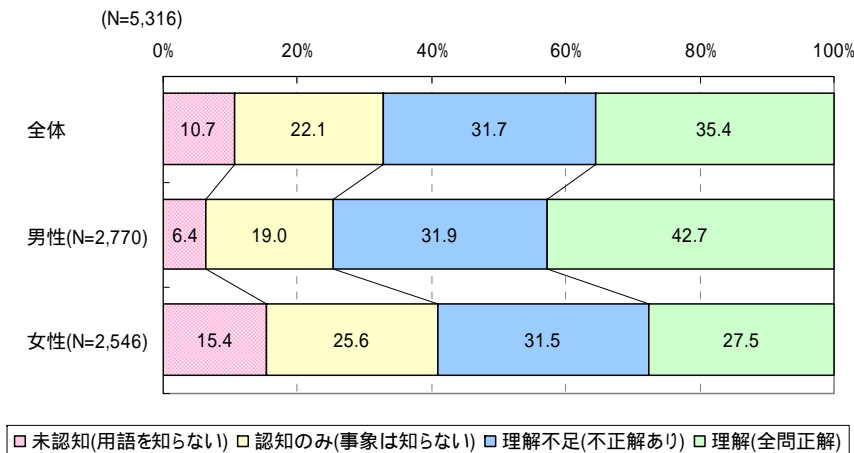
情報セキュリティに関する事象の理解度 - 正誤問題の正答数  
<ファーミング>



### 3.1.2 情報セキュリティに関する事象の理解度(13) - ワンクリック不正請求

- 「ワンクリック不正請求」に関しては、約9割が言葉を認知しており、3問正答の回答者は3割を超える。
- [性別]で見ると、言葉の認知率が男性9割超、女性8割超である。3問正答率では、男性で4割超、女性で3割弱である。
- [年代別]では、20代をピークに、認知度・3問正答率とも、年代が上がるに従って低下する傾向にある。

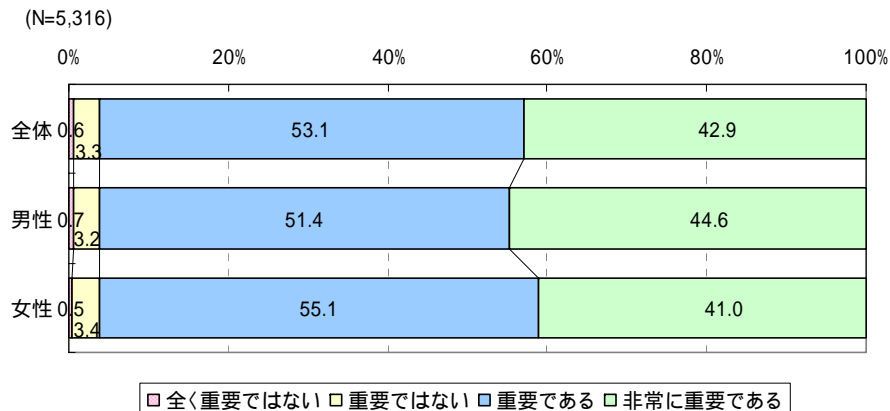
情報セキュリティに関する事象の理解度 - 正誤問題の正答数  
 <ワンクリック不正請求>



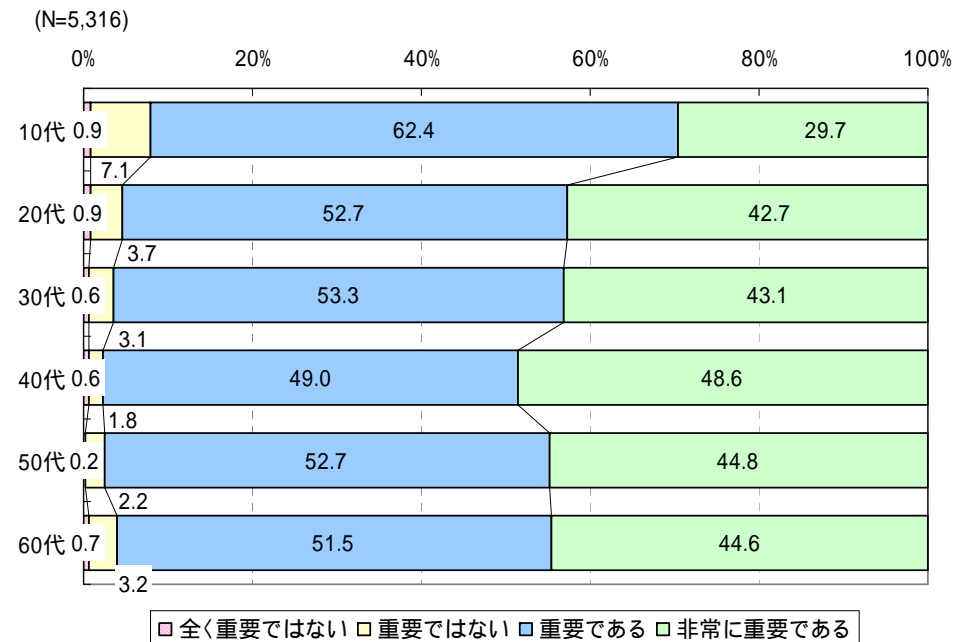
### 3.1.3 情報セキュリティに対する考え(1)

- 情報セキュリティに関する考えについて回答してもらった。
- 情報セキュリティに対して「重要である」とするのが約5割で最も多く、次いで「非常に重要である」とするのが約4割である。「重要でない」「全く重要でない」とするのは1割にも満たない。
- [年代別]では、10代で約10ポイント他の年代と比較して「非常に重要である」の回答が少ないが、その他の年代では概ね同様の傾向を示している。

情報セキュリティに対する意識  
[回答者全体 / 性別]

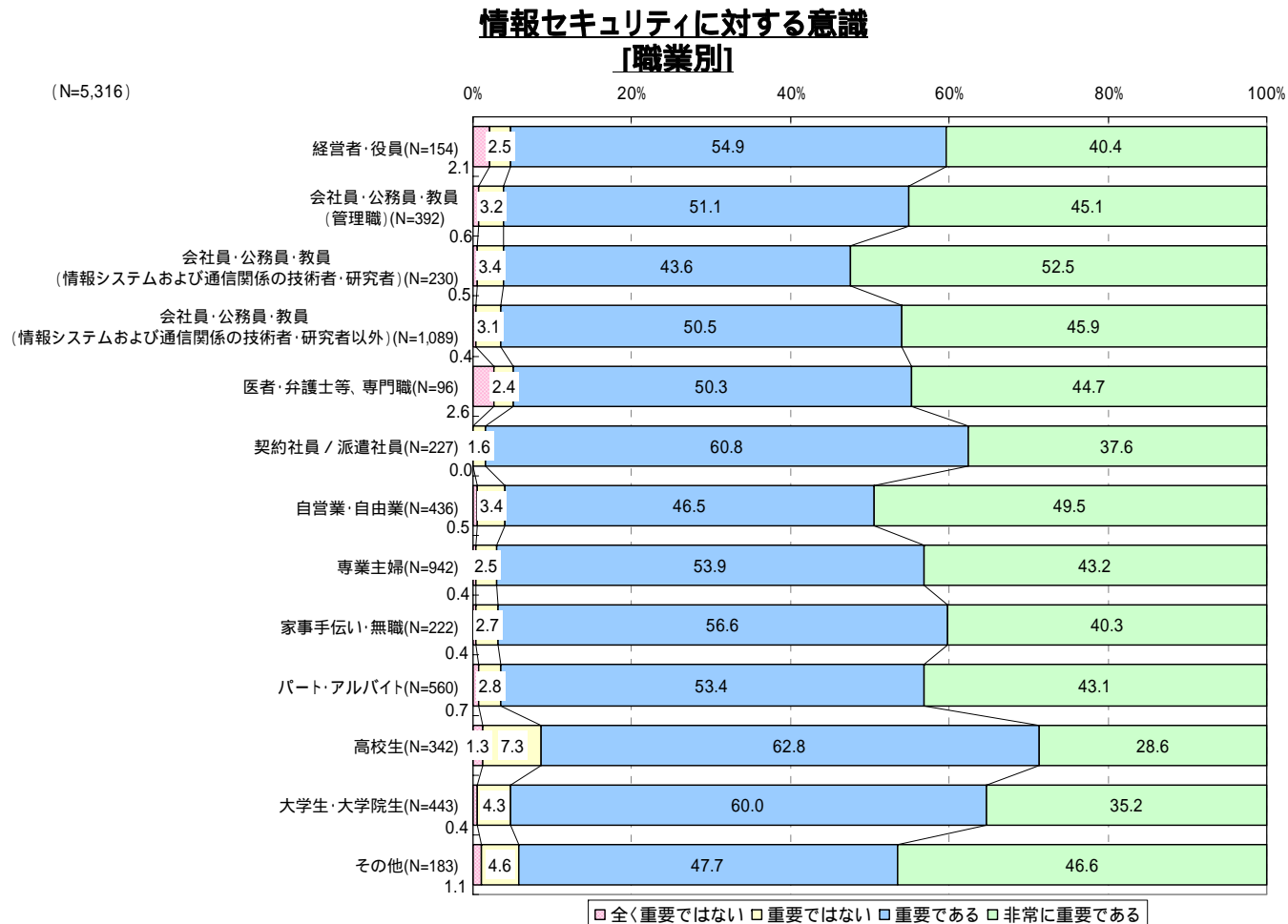


情報セキュリティに対する意識  
[年代別]



### 3.1.3 情報セキュリティに対する考え(2)

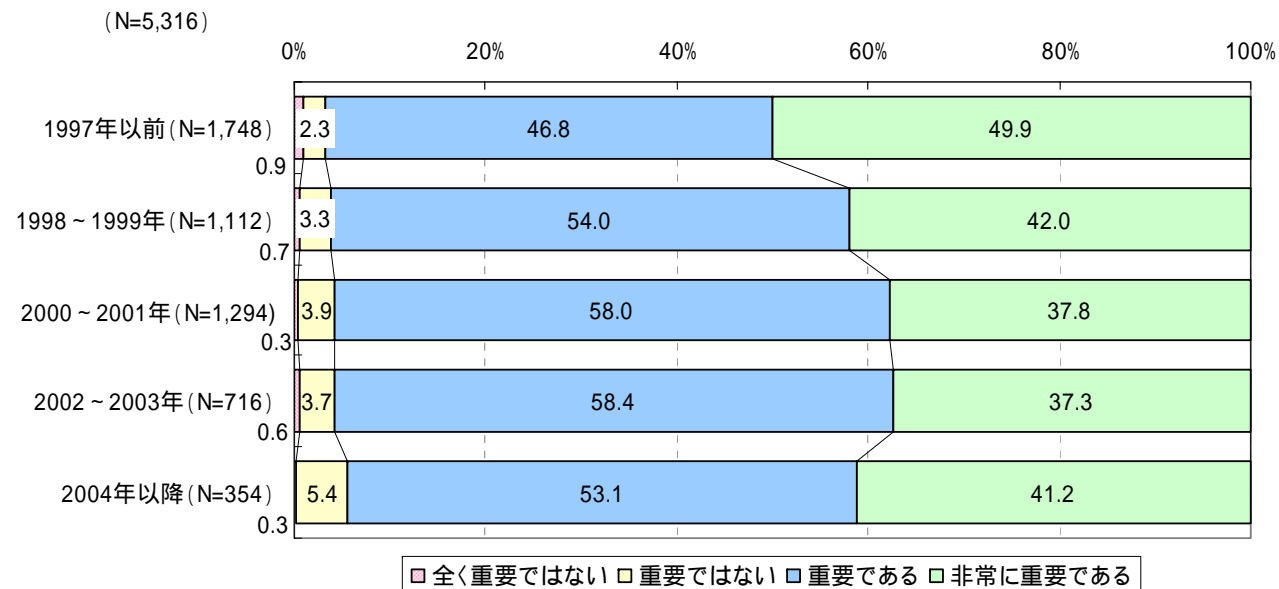
- 情報セキュリティに関する考えについて回答してもらった。
- [職業別]では、「会社員・公務員・教員(情報システムおよび通信関係の技術者・研究者)」および「自営業・自由業」の情報セキュリティに対する意識が高い。一方で、「高校生」「大学生・大学院生」等学生や「家事手伝い・無職」「専業主婦」等、家庭での利用が中心となる層では「非常に重要である」が低めの傾向にある。また、「契約社員/派遣社員」についても、「非常に重要である」が低めの傾向にある。
- 「経営者・役員」の情報セキュリティ意識は「会社・公務員・教員」と比較して低めの傾向にある。



### 3.1.3 情報セキュリティに対する考え(3)

- 情報セキュリティに関する考えについて回答してもらった。
- [インターネット利用開始時期別]では、「1997年以前」から利用している層の方が情報セキュリティに対して「非常に重要である」とする回答が多い。
- 「2004年以降」に利用を開始した層は、「全く重要ではない」「重要ではない」の回答が古くから利用している層と比較して多い傾向にあるが、一方で「非常に重要である」との回答もやや多い。

情報セキュリティに対する意識  
[インターネット利用開始時期別]

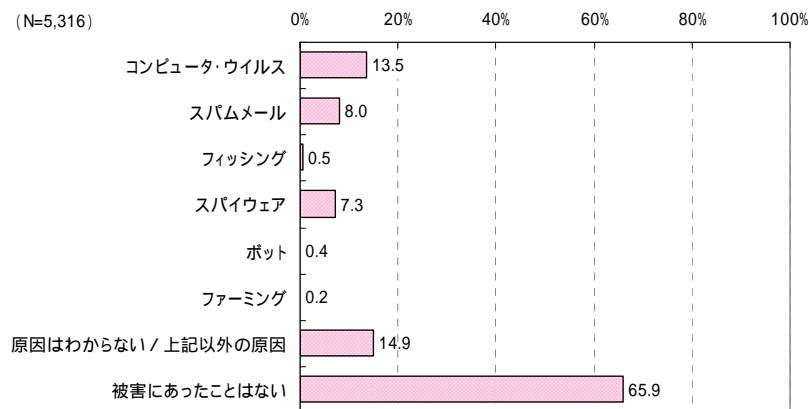


## 3.2. 情報セキュリティに対する行動実態

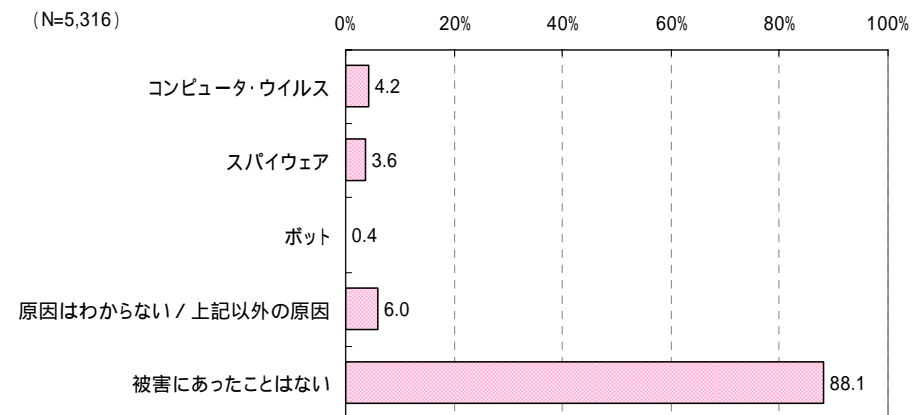
## 3.2.1. 情報セキュリティに関する被害状況(1)

- パソコンの起動異常やシステムの不調の被害にあったことがあるのは3割程度である。そのうち1/3以上がその原因を「コンピュータ・ウイルス」と捉えている。「原因はわからない/上記以外の原因」としたのは14.9%と、原因として示した各脅威よりも多い。
- 不正アクセスの被害にあったことがあるのは1割未満である。「原因はわからない/上記以外の原因」としたのは6.0%と、原因として示した各脅威よりも多い。

**情報セキュリティに関する被害状況  
(パソコンの起動異常やシステムの不調)**  
[回答者全体]



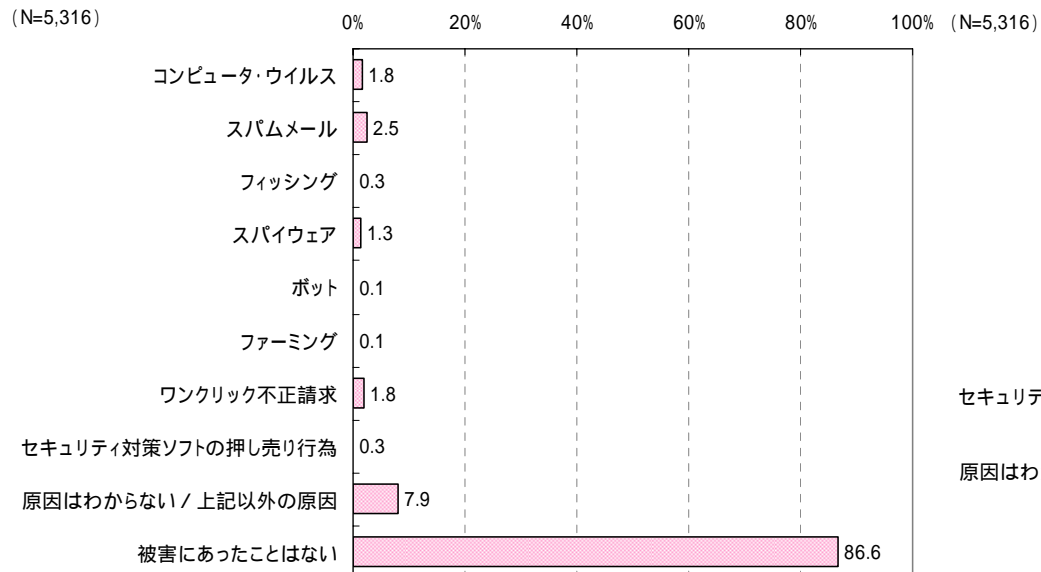
**情報セキュリティに関する被害状況  
(不正アクセス)**  
[回答者全体]



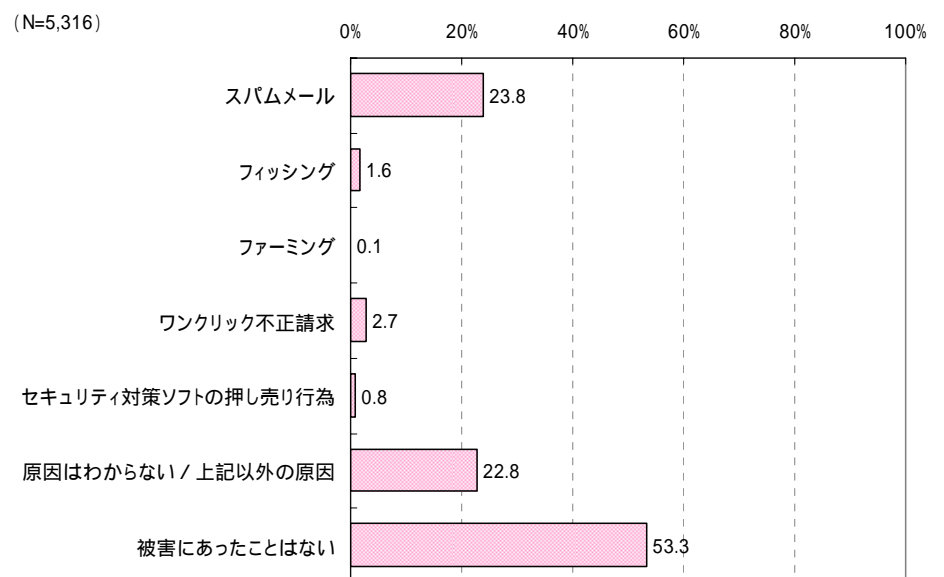
## 3.2.1. 情報セキュリティに関する被害状況(2)

- 個人情報の流出の被害にあったのは1割超である。「原因はわからない/上記以外の原因」としたのは7.9%である。
- 知らない人からのメールの受信を経験しているのは5割近くに達し、その原因は「スパムメール」と捉える人が2割を超え最も多い。一方、「原因はわからない/上記以外の原因」としたのも2割を超えている。

情報セキュリティに関する被害状況  
(個人情報の流出)  
[回答者全体]



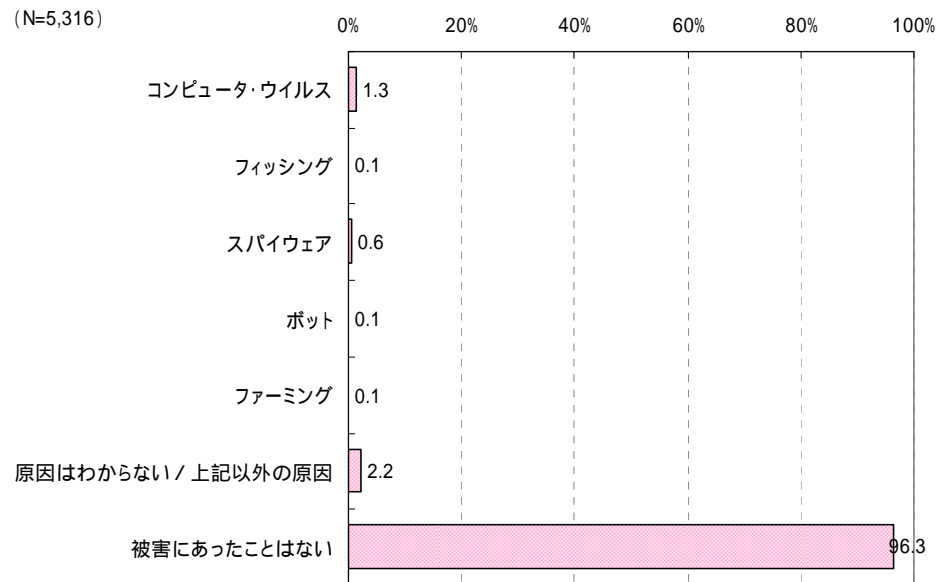
情報セキュリティに関する被害状況  
(知らない人からのメールの受信)  
[回答者全体]



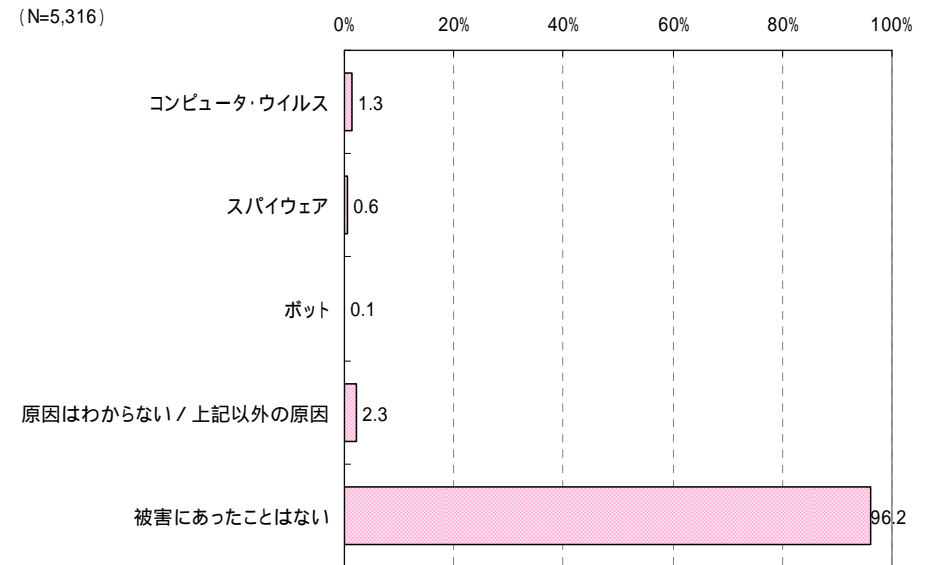
### 3.2.1. 情報セキュリティに関する被害状況(3)

- データの消失や改ざん被害や、知らない間の他者へのメール送信の被害にあったのは、1割未満に留まる。

情報セキュリティに関する被害状況  
(データの消失や改ざん)  
[回答者全体]



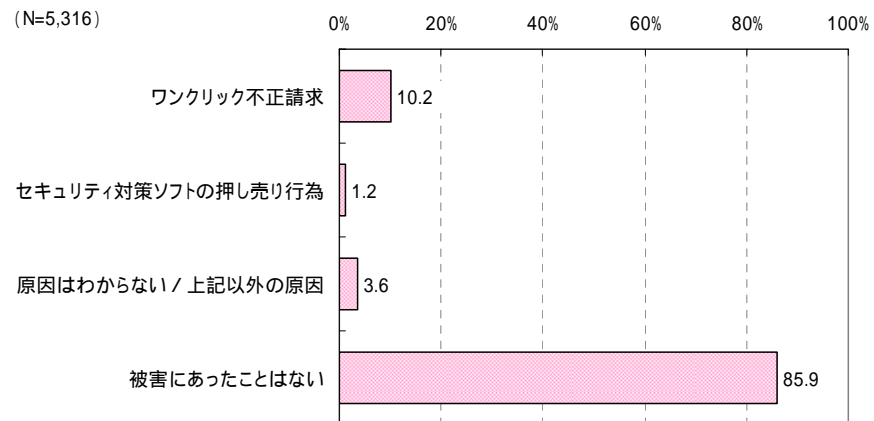
情報セキュリティに関する被害状況  
(知らない間の他者へのメール送信)  
[回答者全体]



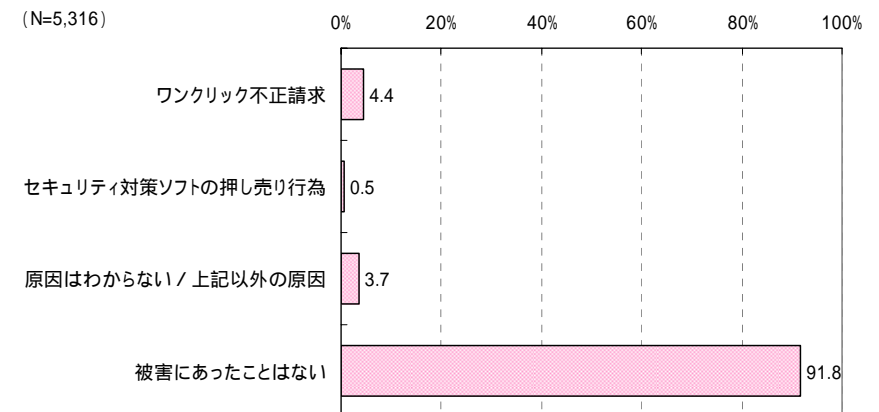
### 3.2.1. 情報セキュリティに関する被害状況(4)

- パソコンの画面に料金の支払いメッセージ表示は約15%に経験があり、そのうちほとんどが、「ワンクリック不正請求」が原因としている。
- 覚えのない料金支払い要求メールの受信の被害にあったのは、1割未満に留まる。

情報セキュリティに関する被害状況  
(パソコンの画面に料金の支払いメッセージ表示)  
[回答者全体]



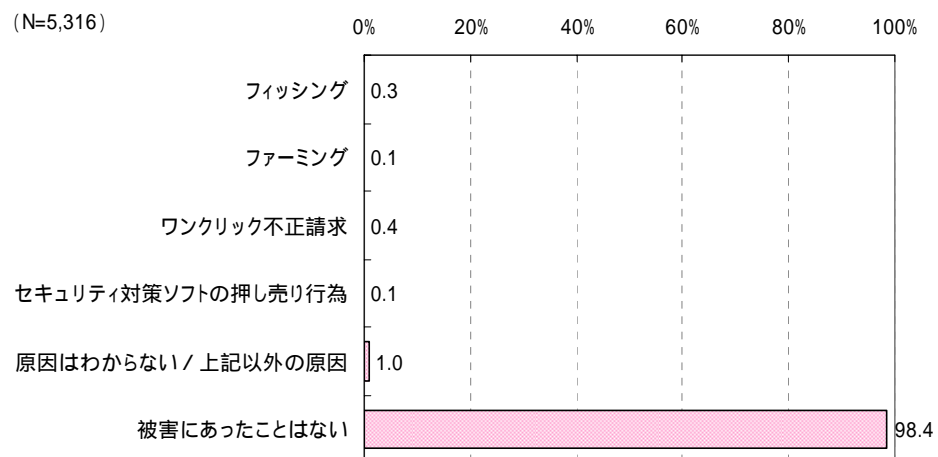
情報セキュリティに関する被害状況  
(覚えのない料金支払い要求メールの受信)  
[回答者全体]



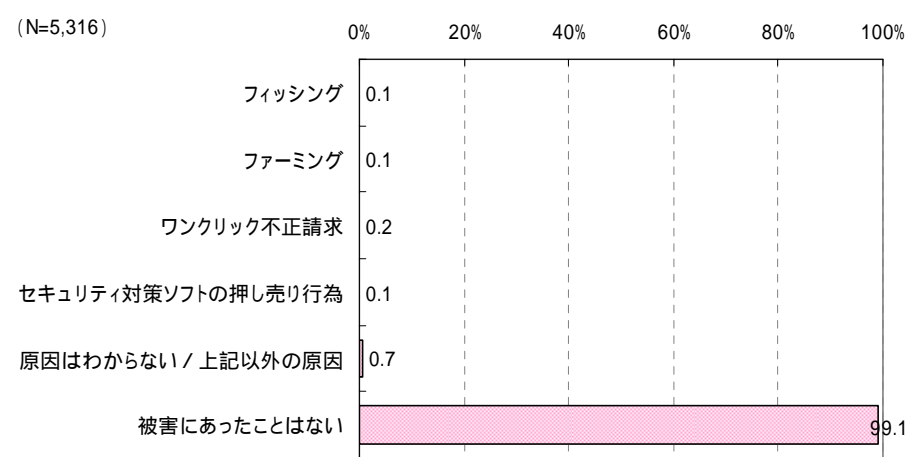
### 3.2.1. 情報セキュリティに関する被害状況(5)

- クレジットカードの不正使用や、覚えのない銀行口座の引き落としの被害にあったのは、2%未満と極わずかに留まる。

情報セキュリティに関する被害状況  
(クレジットカードの不正使用)  
[回答者全体]



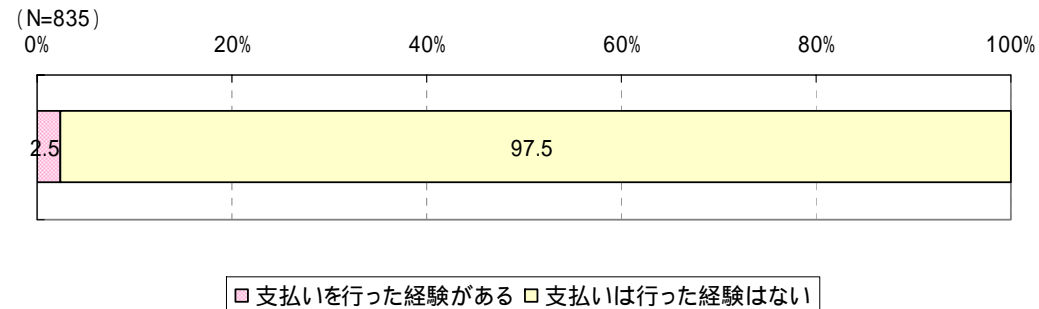
情報セキュリティに関する被害状況  
(覚えのない銀行口座の引き落とし)  
[回答者全体]



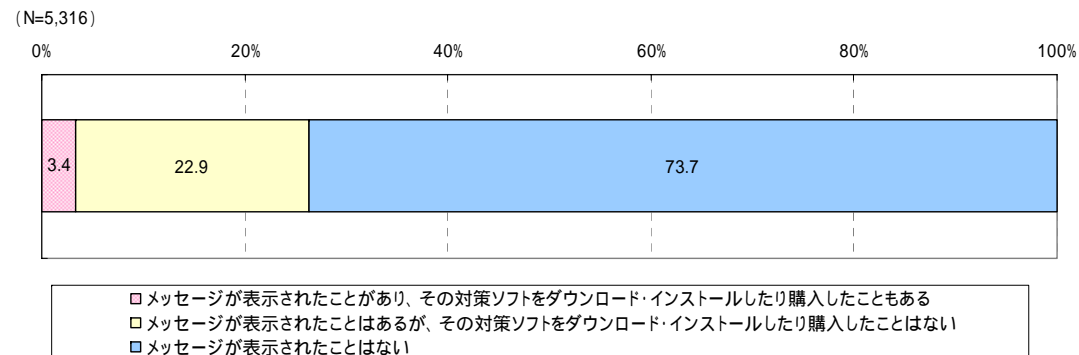
## 3.2.1. 情報セキュリティに関する被害状況(6)

- 「パソコンの画面に料金の支払いを要求するメッセージの表示」または「覚えのない料金の支払いを要求するメールの受信」を経験し、実際に支払いを行った経験があるのは2.5%である。
- セキュリティ対策ソフトのダウンロード・インストールを促すメッセージに応じた経験があるのは、3.4%である。

情報セキュリティに関する被害状況  
(料金請求のメッセージやメールに対し、実際に支払った経験)  
[回答者全体]



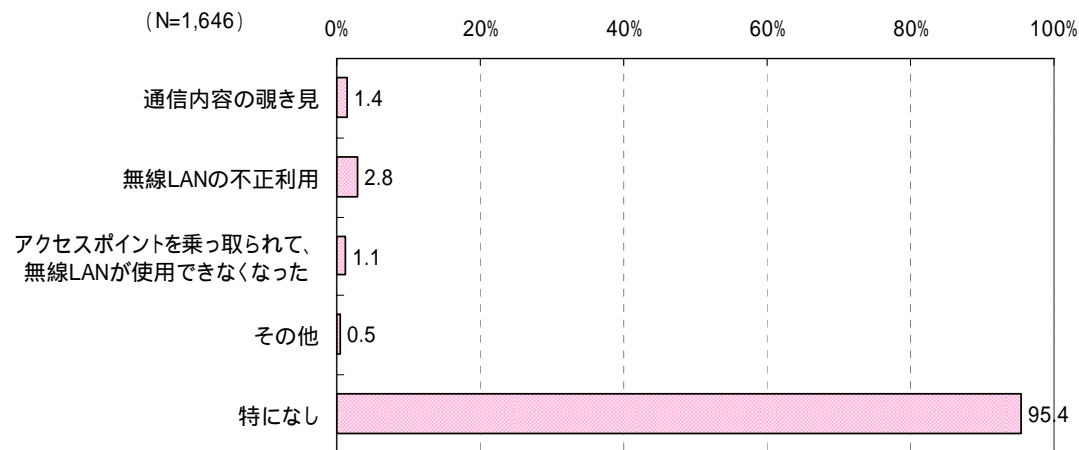
情報セキュリティに関する被害状況  
(セキュリティ対策ソフトのダウンロード・インストールを促すメッセージに応じた経験)  
[回答者全体]



### 3.2.1. 情報セキュリティに関する被害状況(7)

- 自宅で無線LANを利用して被害にあったことがあるか答えてもらった。
- 被害経験は「特になし」との回答が95%を超え、被害経験があるのは4.6%に留まった。

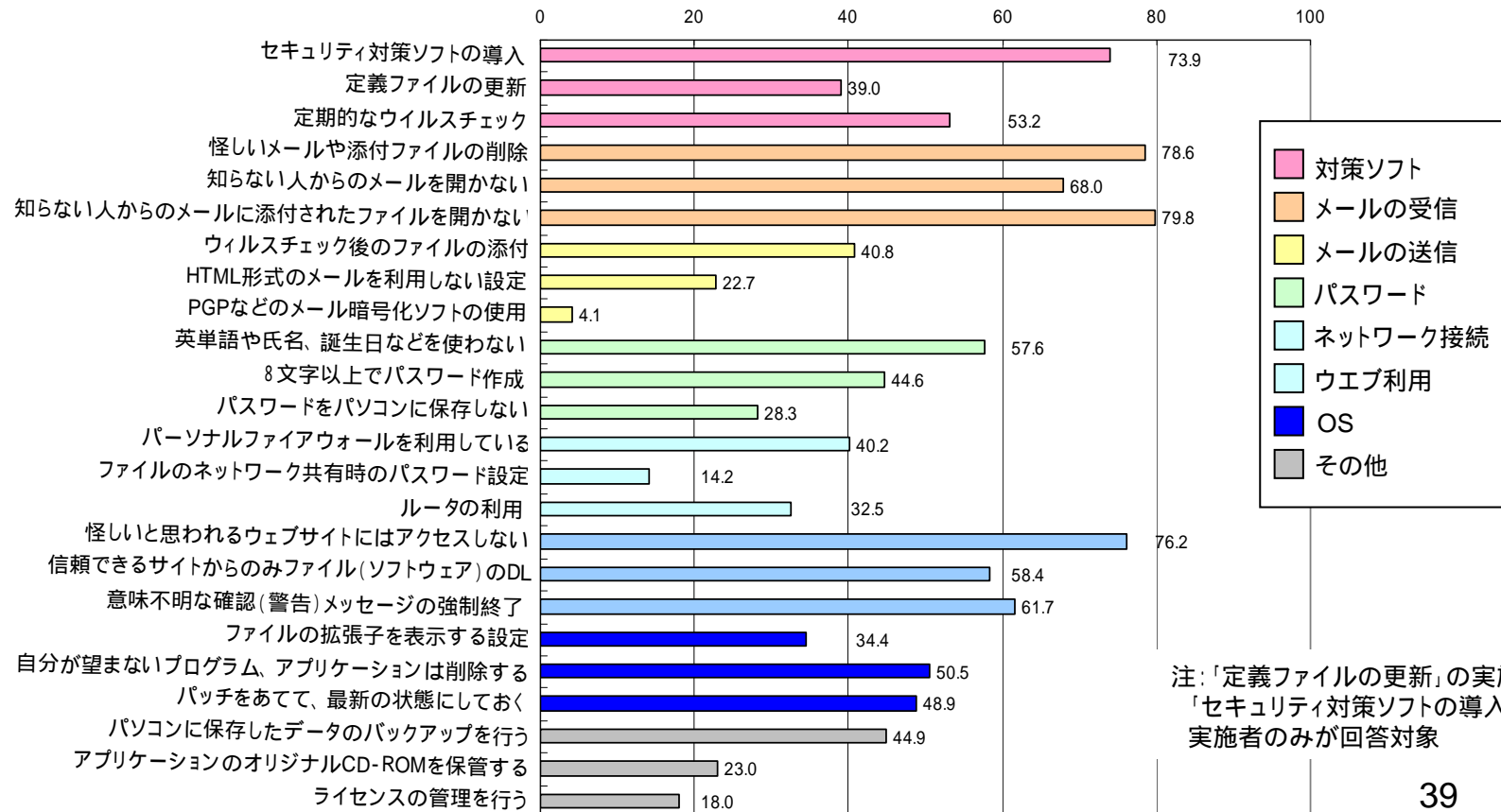
自宅での無線LAN利用時の被害経験(複数回答)  
[回答者全体]



## 3.2.2 情報セキュリティ対策の実施状況(1)

- メールの送信、ネットワーク接続、その他に関する対策はあまり実施されていない傾向にあり、パスワード、OSに係わる対策の実施傾向はやや低い。
- 個別の対策項目としては、「パスワードをパソコンに保存しない」「HTML形式のメールを利用しない設定にしている」「アプリケーションのオリジナルCD-ROMを保管する」「ライセンスの管理を行う」という対策はあまり実施されていない。
- 「定義ファイルの更新を行っている」「パッチをあてて最新の状態にしておく」といった対策は、自動更新機能があるため、あまり意識的に行われていない可能性がある。

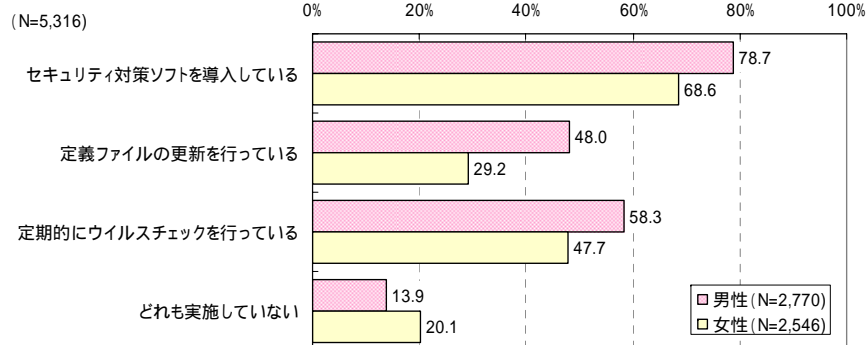
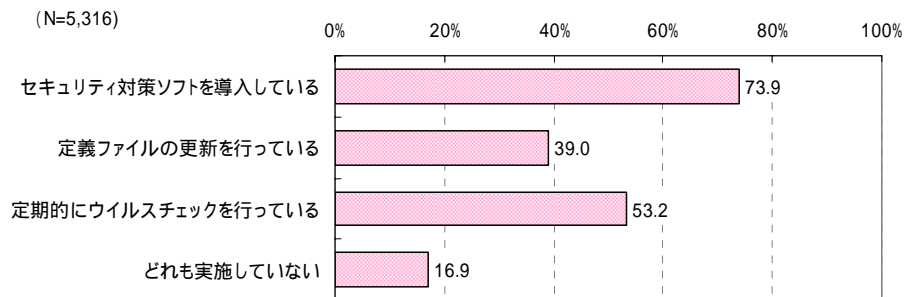
情報セキュリティ対策の実施状況(複数回答)



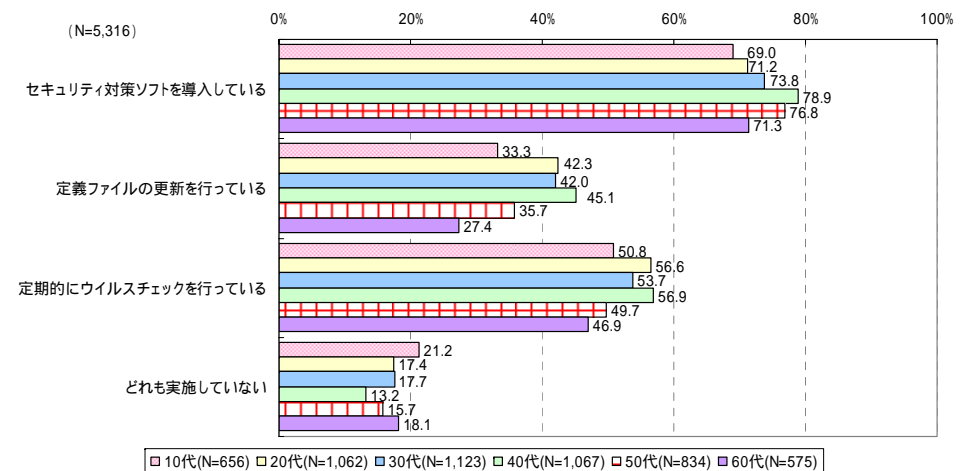
## 3.2.2 情報セキュリティ対策の実施状況(2) - 対策ソフトの利用状況

- セキュリティ対策ソフトに関わる対策状況を答えてもらった。
- セキュリティ対策ソフトを導入しているのは7割を超え、そのうち6割近くは定義ファイルの更新を行っている。また、定期的にウイルスチェックを行っているのも5割を超える。
- [性別]で見ると、いずれの対策においても男性の方が実施率が高い。

情報セキュリティ対策の実施状況 - 対策ソフトの利用状況  
(複数回答) [回答者全体 / 性別]



情報セキュリティ対策の実施状況 - 対策ソフトの利用状況  
(複数回答) [年代別]

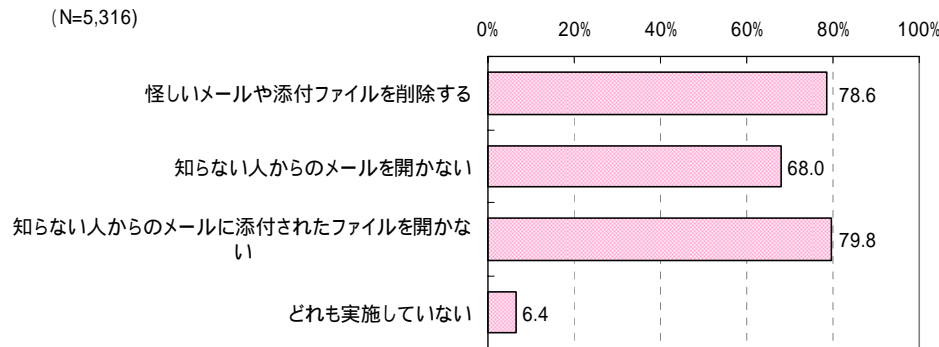


注: 「定義ファイルの更新」の実施は  
「セキュリティ対策ソフトの導入」  
実施者のみが回答対象

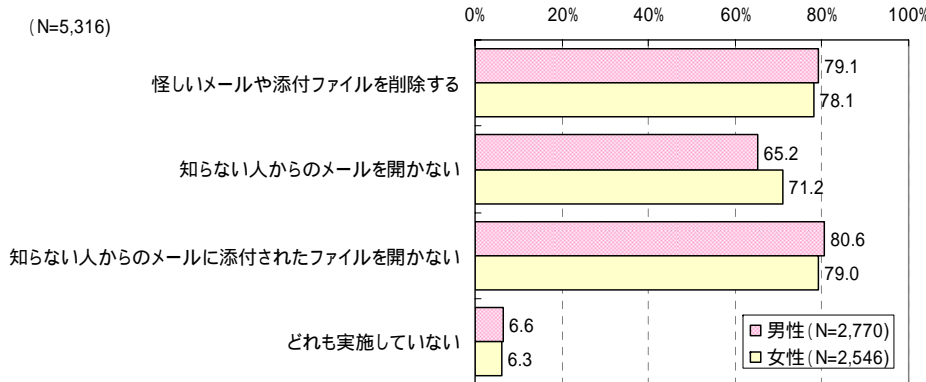
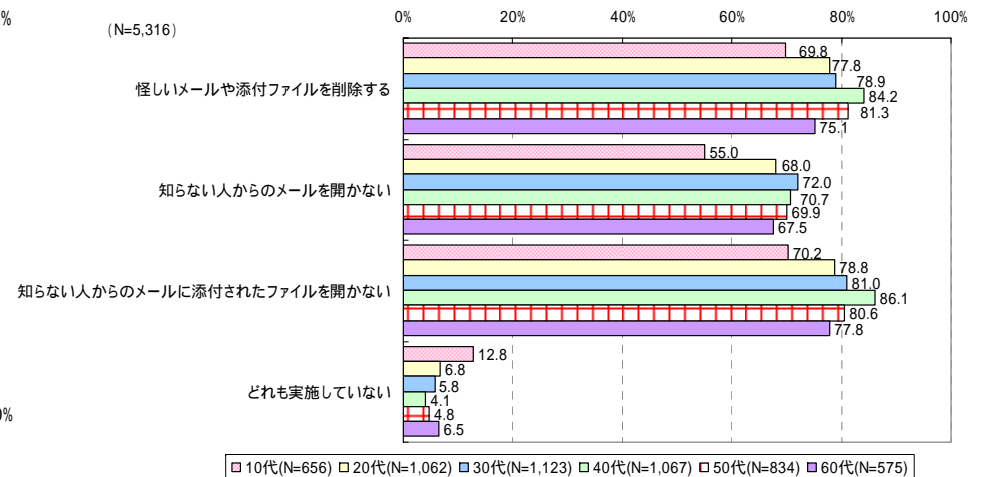
## 3.2.2 情報セキュリティ対策の実施状況(3) - 受信メールの扱い

- 受信メールの扱いに関わる対策状況を答えてもらった。
- いずれの対策においても7割弱～8割程度の実施率であり、「どれも実施していない」のは1割未満に留まる。
- [性別]で見ると、「知らない人からのメールを開かない」のみ女性の方が6ポイント高いのが特徴的である。

**情報セキュリティ対策の実施状況 - 受信メールの扱い**  
(複数回答) [回答者全体 / 性別]



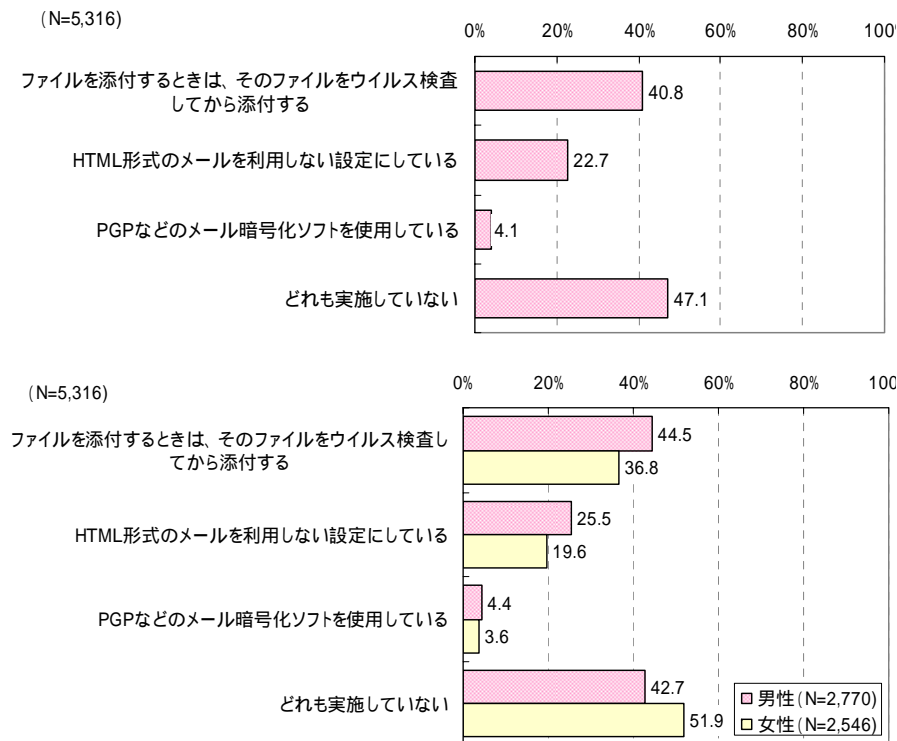
**情報セキュリティ対策の実施状況 - 受信メールの扱い**  
(複数回答) [年代別]



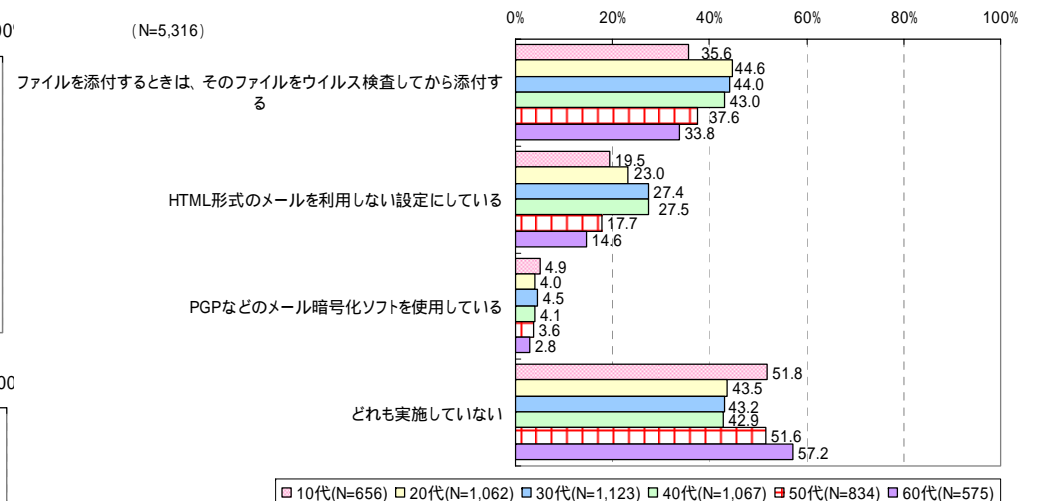
## 3.2.2 情報セキュリティ対策の実施状況(4) - 送信メールの扱い

- 送信メールの扱いに関わる対策状況を答えてもらった。
- いずれの対策においても実施率は低めの傾向にあり、「どれも実施していない」も5割近くに達する。
- [性別]ではいずれの対策も男性の方が実施率が高い。

情報セキュリティ対策の実施状況 - 送信メールの扱い  
(複数回答) [回答者全体 / 性別]



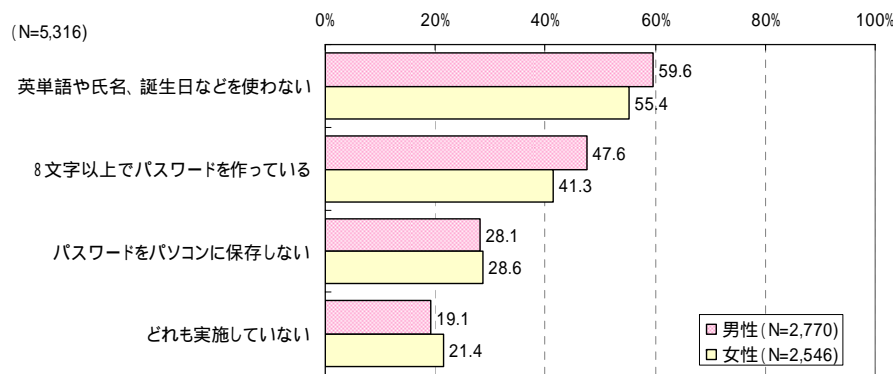
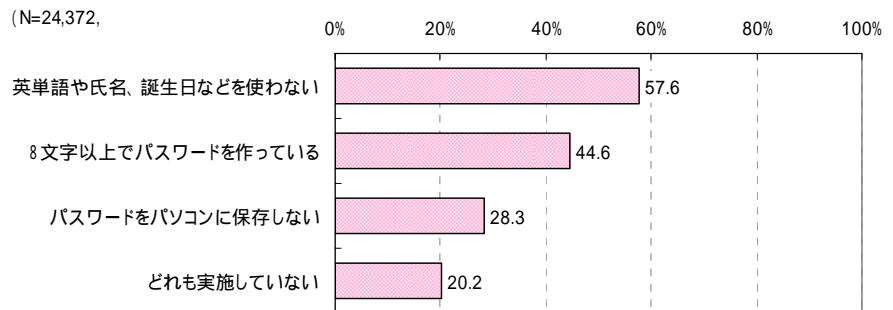
情報セキュリティ対策の実施状況 - 送信メールの扱い  
(複数回答) [年代別]



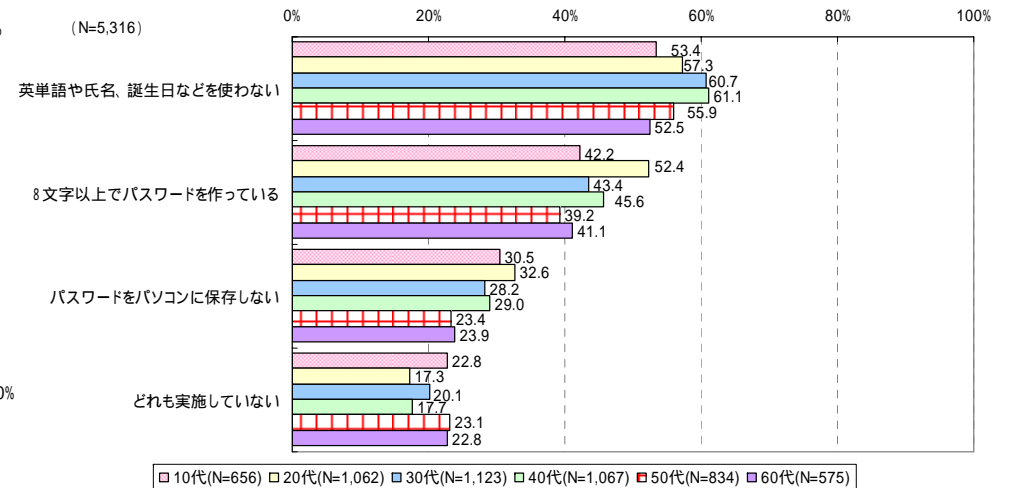
## 3.2.2 情報セキュリティ対策の実施状況(5) - パスワード

- パスワードに関わる対策状況を答えてもらった。
- いずれの対策も技術的に困難なものではないが、実施率は低めの傾向にあった。
- [性別]では、男性の方がやや実施率が高めにあるが、「パスワードをパソコンに保存しない」の実施率は、男女ともほぼ同率である。

**情報セキュリティ対策の実施状況 - パスワード**  
(複数回答) [回答者全体 / 性別]



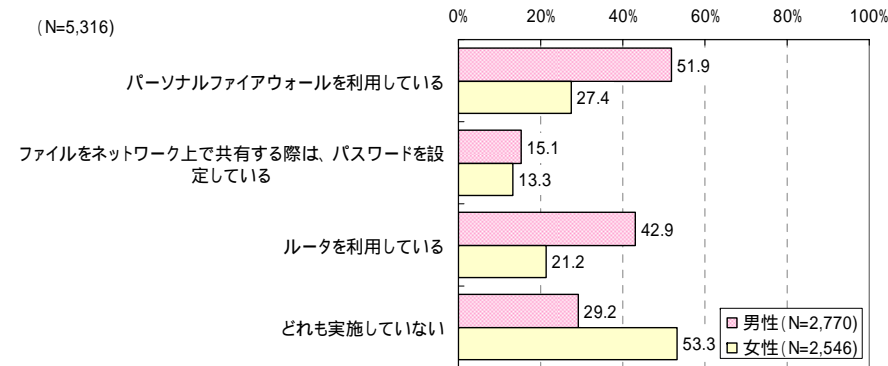
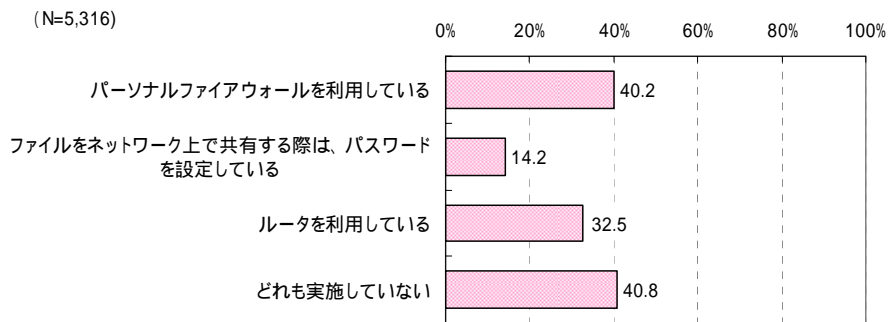
**情報セキュリティ対策の実施状況 - パスワード**  
(複数回答) [年代別]



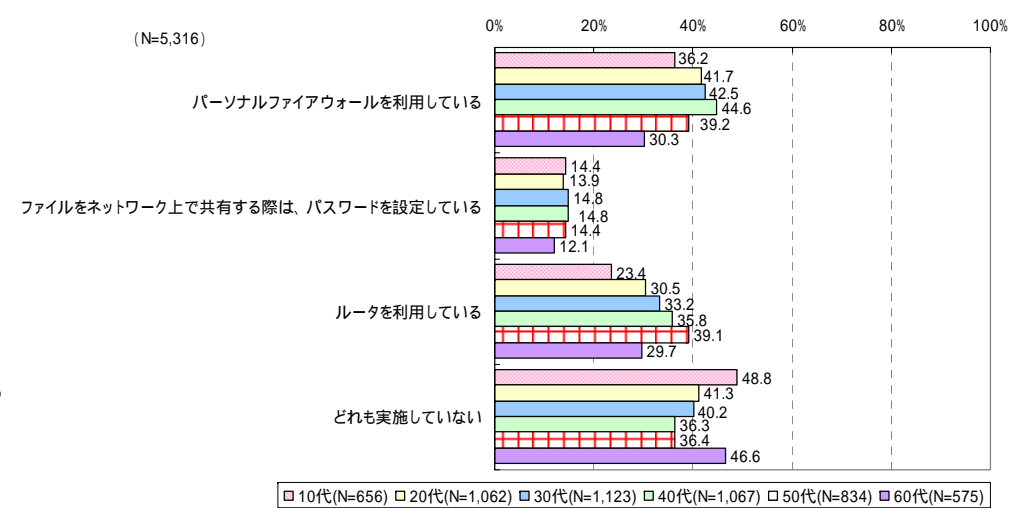
## 3.2.2 情報セキュリティ対策の実施状況(6) - インターネット接続

- インターネット接続に関わる対策状況を答えてもらった。
- 「パーソナルファイアウォールの利用」が4割、「ルータの利用」が3割強であり、[性別]では、いずれの対策も男性の方が実施率が20ポイント程度高い。

**情報セキュリティ対策の実施状況 - インターネット接続**  
(複数回答) [回答者全体 / 性別]



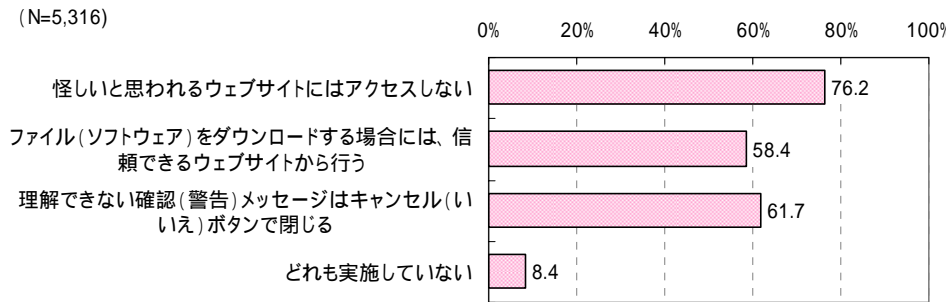
**情報セキュリティ対策の実施状況 - インターネット接続**  
(複数回答) [年代別]



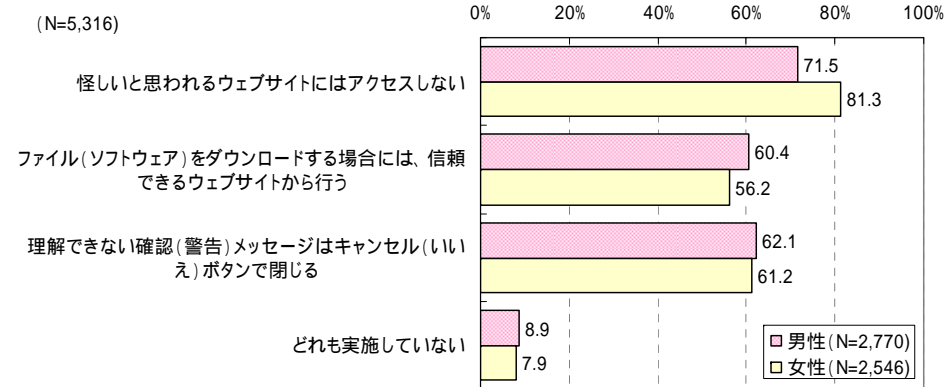
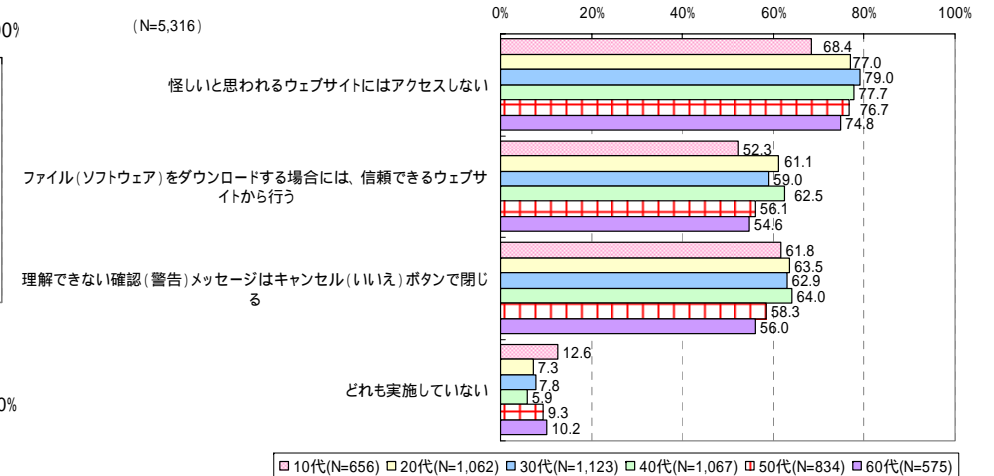
## 3.2.2 情報セキュリティ対策の実施状況(7) - ウェブページ閲覧

- ウェブページ閲覧に関わる対策状況を答えてもらった。
- いずれの対策も実施率が高めの傾向にある。
- [性別]でも、他の対策ほど男女差は見られず、「怪しいと思われるウェブサイトにはアクセスしない」は女性の方が10ポイント実施率が高い。

**情報セキュリティ対策の実施状況 - ウェブページ閲覧**  
(複数回答) [回答者全体 / 性別]



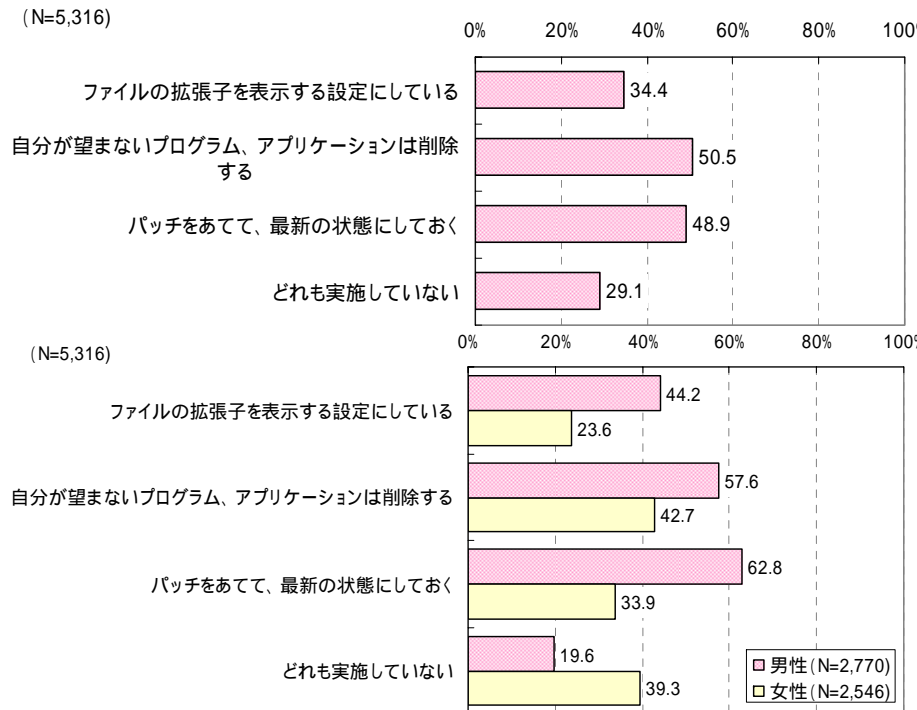
**情報セキュリティ対策の実施状況 - ウェブページ閲覧**  
(複数回答) [年代別]



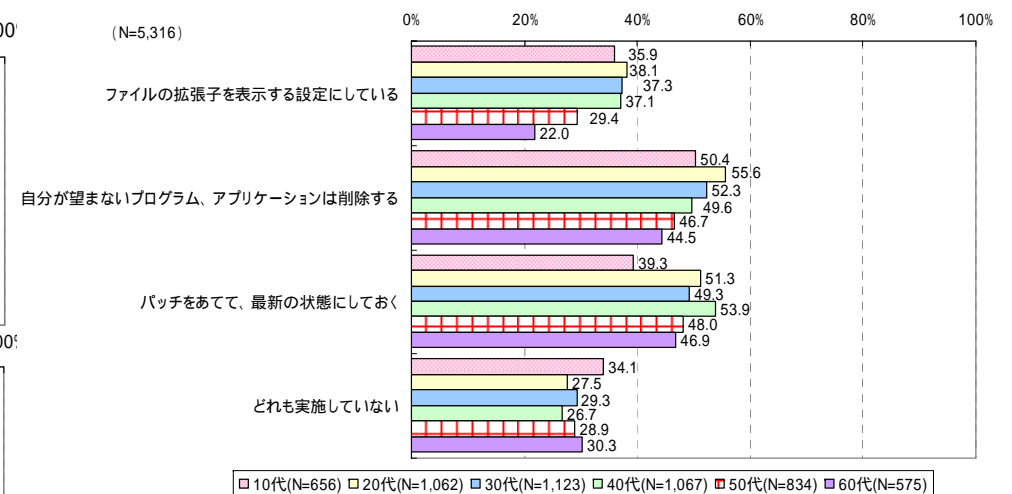
## 3.2.2 情報セキュリティ対策の実施状況(8) - オペレーティングシステム

- オペレーティングシステムに関わる対策状況を答えてもらった。
- 「望まないプログラム・アプリケーションの削除」「パッチをあてて、最新の状態にする」対策は約半数が実施している。
- [性別]では、男性の実施率の方が総じて15～30ポイント高く、女性では「どれも実施していない」のが4割近くに達する。

情報セキュリティ対策の実施状況 - オペレーティングシステム  
(複数回答) [回答者全体 / 性別]



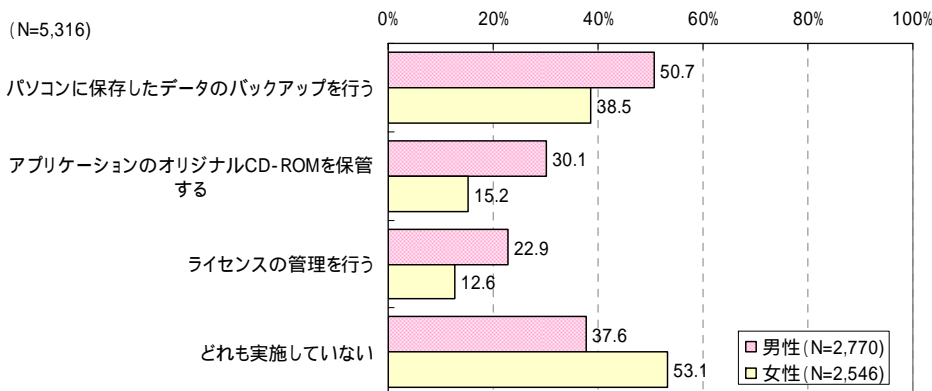
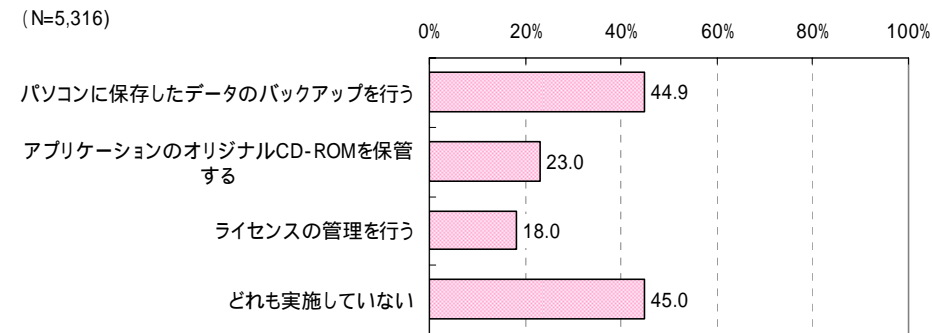
情報セキュリティ対策の実施状況 - オペレーティングシステム  
(複数回答) [年代別]



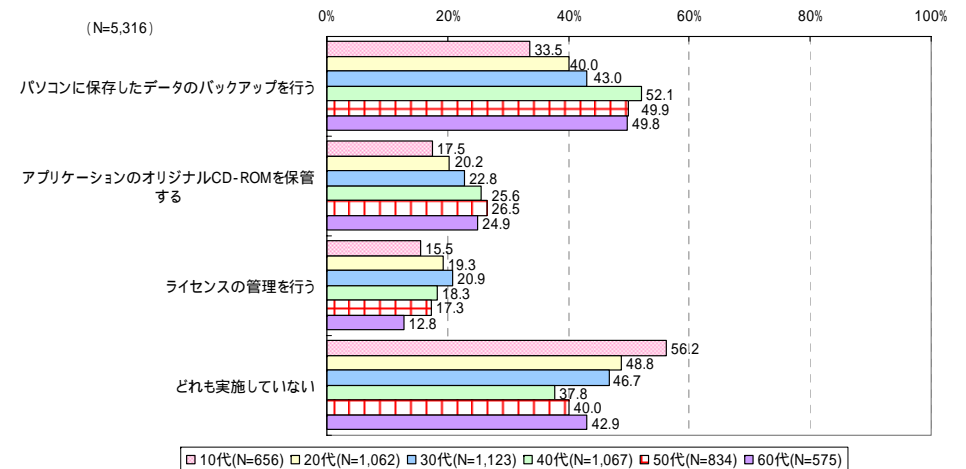
## 3.2.2 情報セキュリティ対策の実施状況(9) - その他

- これまでの設問以外に関する対策状況を答えてもらった。
- 「パソコンに保存したデータのバックアップ」の実施率は4割を超えるが、「アプリケーションのオリジナルCD-ROMを保管する」「ライセンスの管理を行う」は2割程度に留まる。
- [性別]でも、男性の実施率の方が総じて10～15ポイント高く、女性では「どれも実施していない」のが5割を超える。

情報セキュリティ対策の実施状況 - その他  
(複数回答) [回答者全体 / 性別]



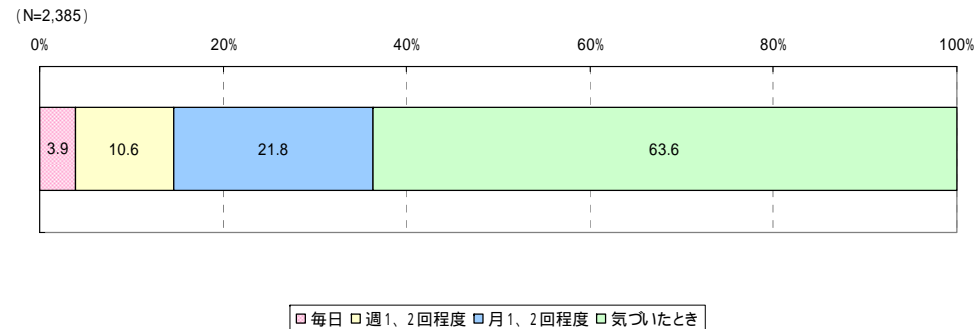
情報セキュリティ対策の実施状況 - その他  
(複数回答) [年代別]



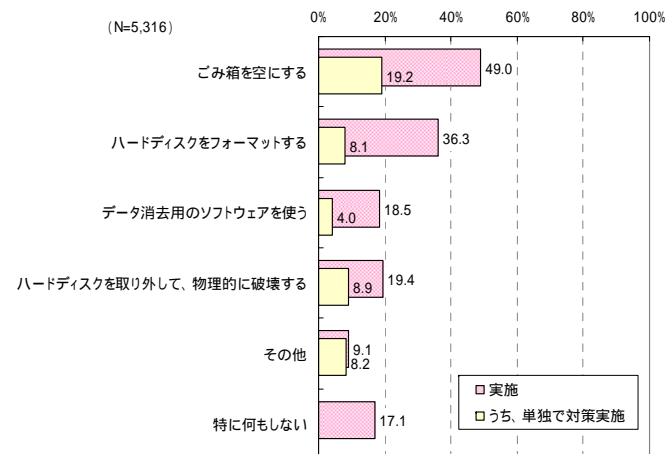
## 3.2.2 情報セキュリティ対策の実施状況(10)

- バックアップは4割強が実施しているが、そのうち6割以上が「気づいたとき」しか実施していない。
- パソコンの処分やリサイクル時のデータ消去方法は、「ゴミ箱を空にする」のが5割程度、次いで「ハードディスクのフォーマット」(36.3%)と続く。「物理的な破壊」(19.4%)、「データ消去用ソフトの利用」(18.9%)等、手間のかかる手法でも2割近い実施率に達する。一方、「ゴミ箱を空にする」のみ(19.2%)、もしくは「特に何もしない」(17.1%)等、合わせて3割以上は、データ消去方法が不十分であると言える。

### バックアップの実施頻度



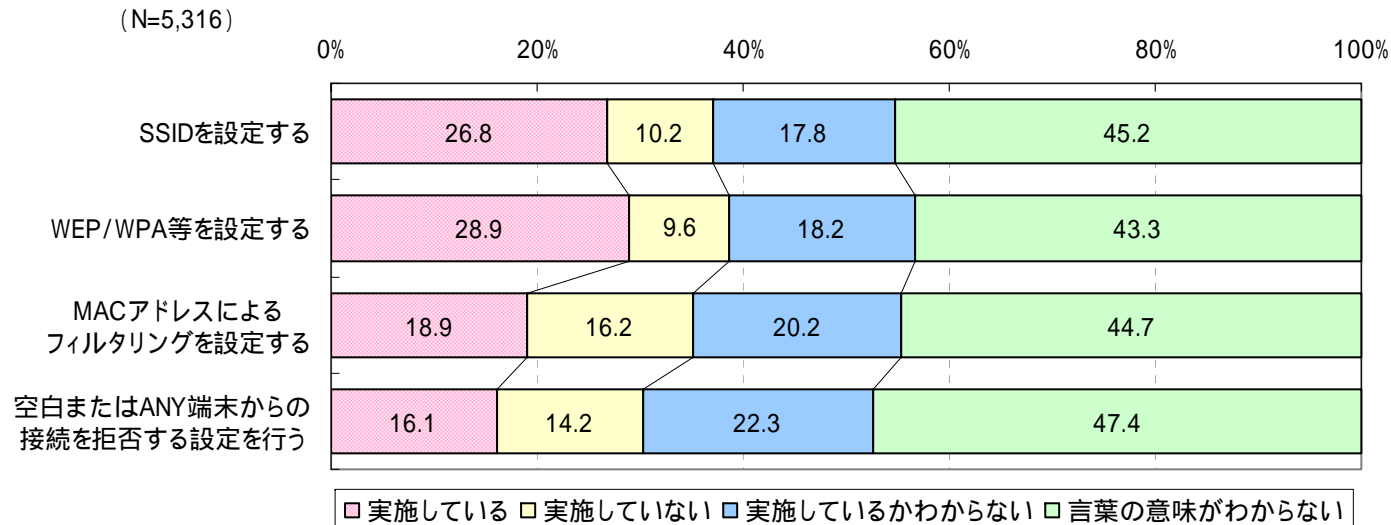
### パソコンの処分やリサイクル時のデータ消去方法(複数回答)



## 3.2.2 情報セキュリティ対策の実施状況(11)

- 自宅での無線LANの設定において、実施しているものを選んでもらった。
- 「SSIDの設定」や「WEP/WPA等の設定」は3割近くが実施しているが、「MACアドレスによるフィルタリング設定」や「空白・ANY端末からの接続拒否」については、実施率が2割を下回る。
- いずれの対策においても、「実施しているかわからない」との回答が2割前後に上り、「言葉の意味がわからない」との回答も5割近くに達する。

無線LANの設定における対策の実施状況  
[回答者全体]



(注)

SSID:無線LANのネットワークの識別子。アクセスポイントと同一のSSIDを設定した無線LANのクライアントのみが通信可能となる。

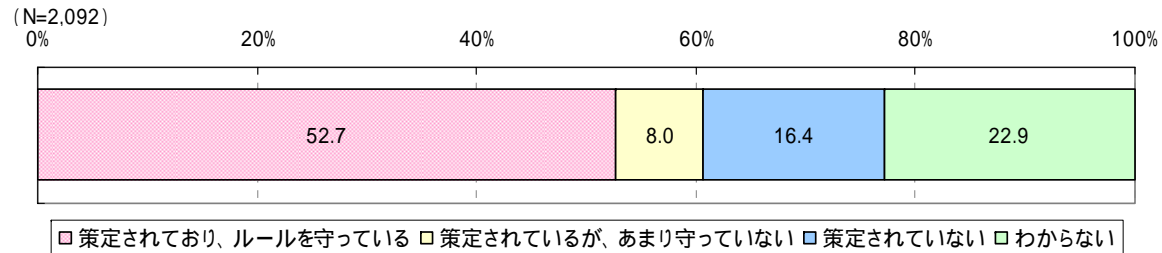
WEP/WPA:無線区間でデータを暗号化する機能。WEPよりWPAの方がセキュリティ強度が高い。

MACアドレス:アクセスポイントにクライアントのMACアドレスを登録しておくことにより、無線LANへの接続を許可するクライアントを制限できる機能。

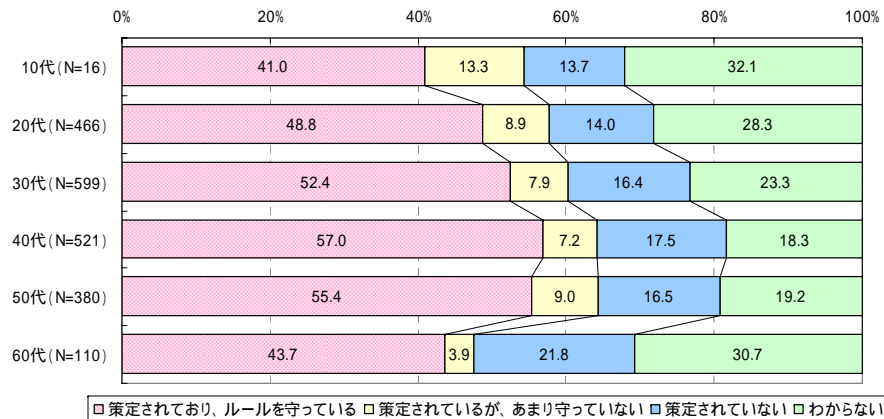
### 3.2.3 組織における情報セキュリティ対策の実施状況(1)

- 「経営者・役員」「会社員・公務員・教員」「契約社員／派遣社員」の企業勤務者に、回答者が勤める企業・組織における情報セキュリティ関連規定の策定・遵守状況を答えてもらった。
- 情報セキュリティ関連規定が策定されているのは約6割であり、そのうち9割近くが「ルールを守っている」と回答している。
- [職業別]に見ると、「会社員・公務員・教員(情報システムおよび通信関係の技術者・研究者)」が属する組織のルール策定率は高い一方、「経営者・役員」が経営する組織のルール策定率は低く、「契約社員／派遣社員」は属する組織のルール策定状況を「わからない」とする率が半数近くに達する。

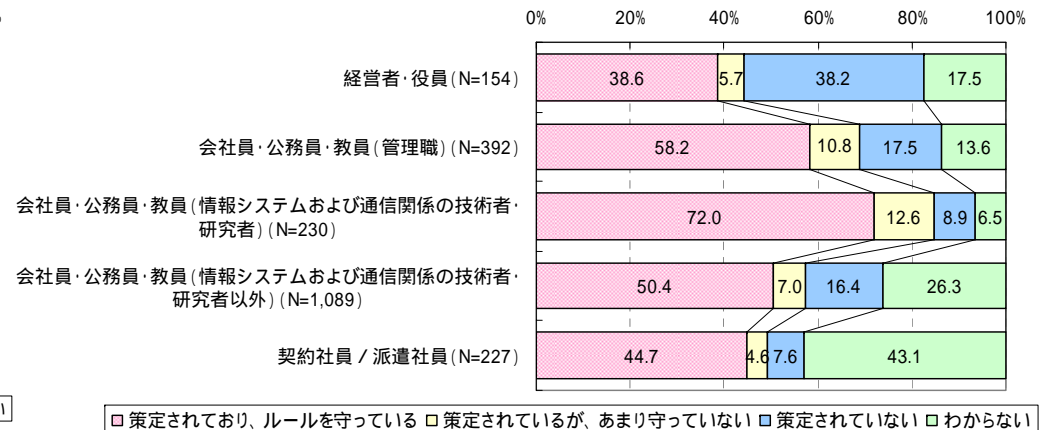
組織における情報セキュリティ関連規定の策定・遵守状況  
[企業勤務者のみ]



組織における情報セキュリティ関連規定の策定・遵守状況  
[年代別]



組織における情報セキュリティ関連規定の策定・遵守状況  
[職業別]

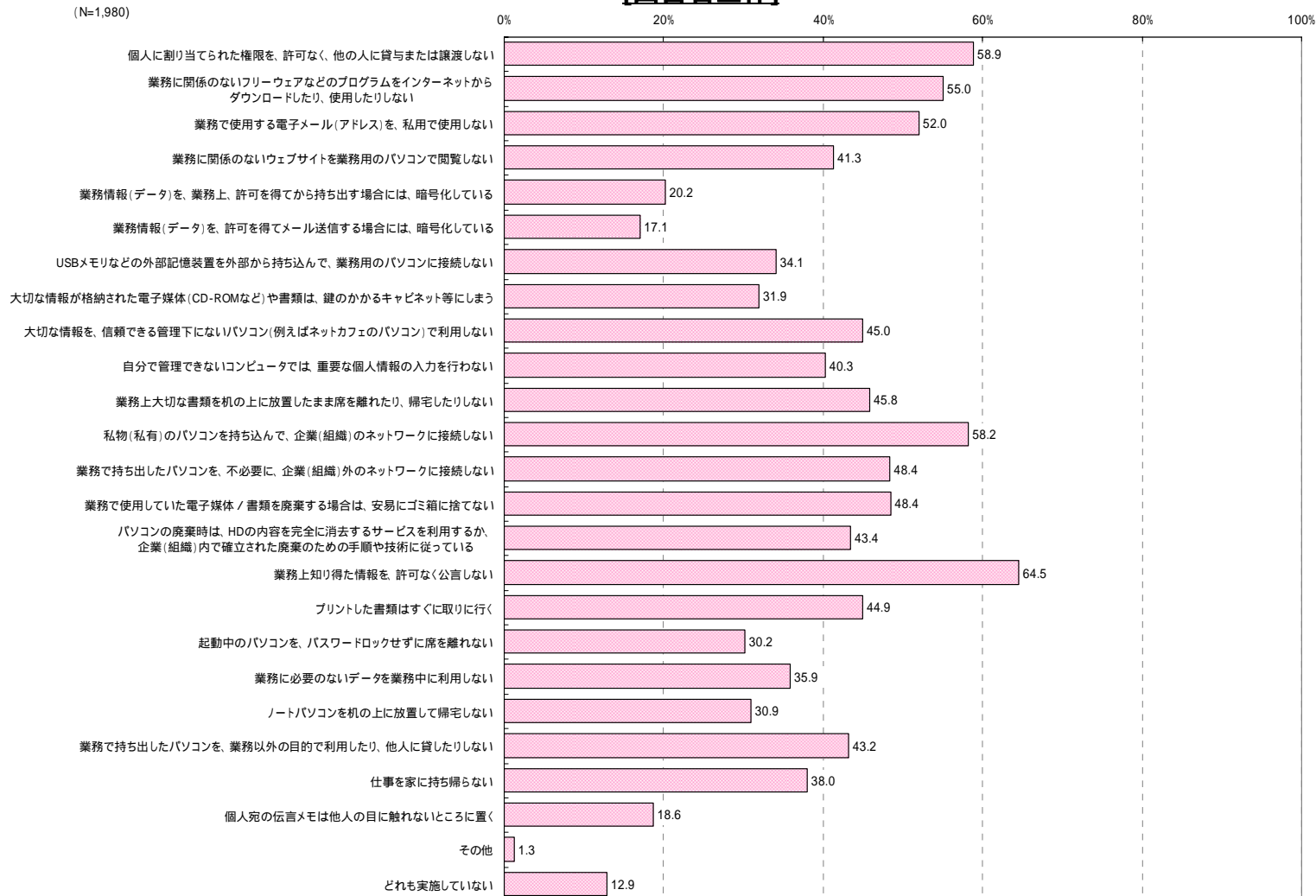


### 3.2.3 組織における情報セキュリティ対策の実施状況(2)

- 組織における情報セキュリティ対策の実施では、「業務上知りえた情報を許可なく公言しない」「私物のパソコンを持ち込んで企業のネットワークに接続しない」「個人に割り当てられた権限を許可なく他の人に貸与または譲渡しない」「業務に関係ないフリーウェアなどのプログラムをインターネットからダウンロードしたり使用したりしない」「業務で使用する電子メールアドレスを私用で使用しない」等の実施率が5割を超えている。

#### 組織における情報セキュリティ対策の実施状況(複数回答)

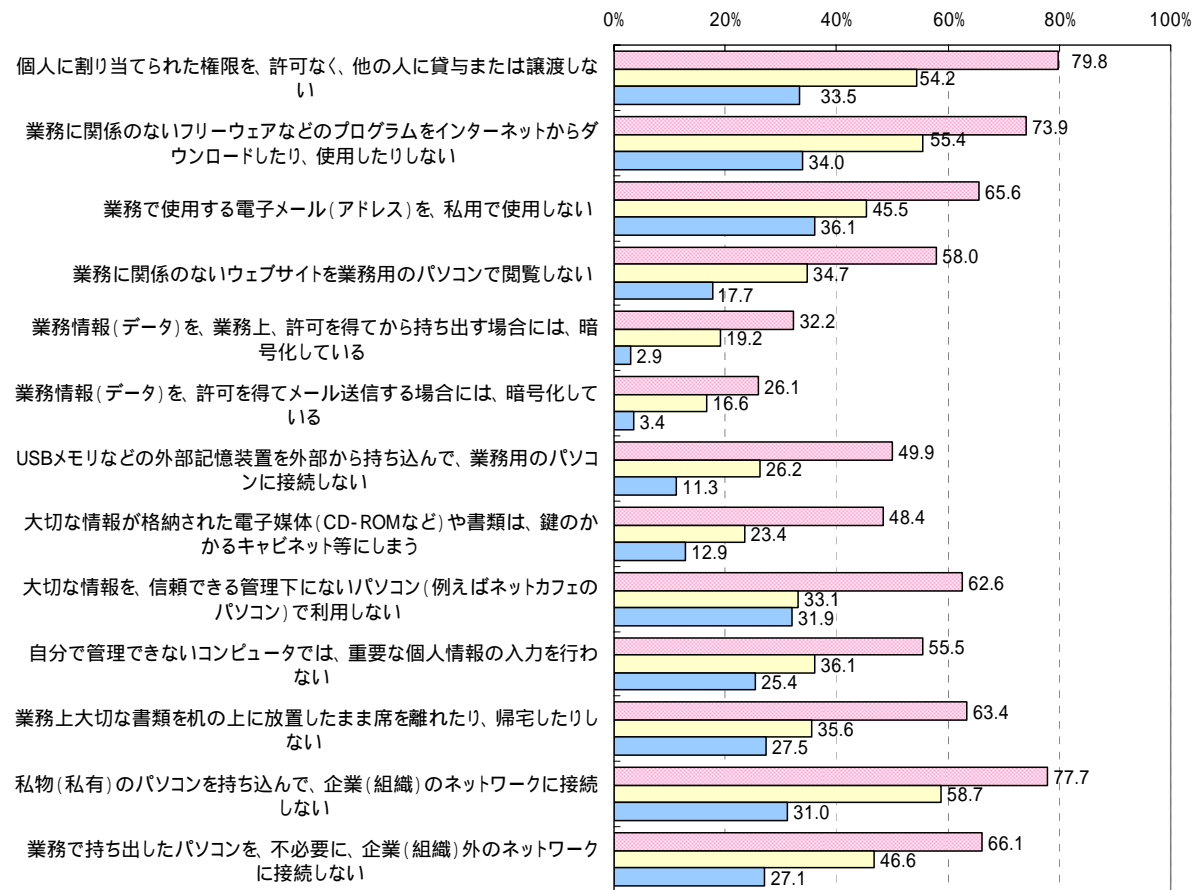
【回答者全体】



### 3.2.3 組織における情報セキュリティ対策の実施状況(3)

- 組織における情報セキュリティ関連規定の策定・遵守状況別に組織の対策実施状況を見ると、いずれの対策においても、規定が策定されている組織の方が対策の実施率が高い。

組織における情報セキュリティ対策の実施状況(複数回答) - 1  
[組織の情報セキュリティ関連規定策定・遵守状況別]



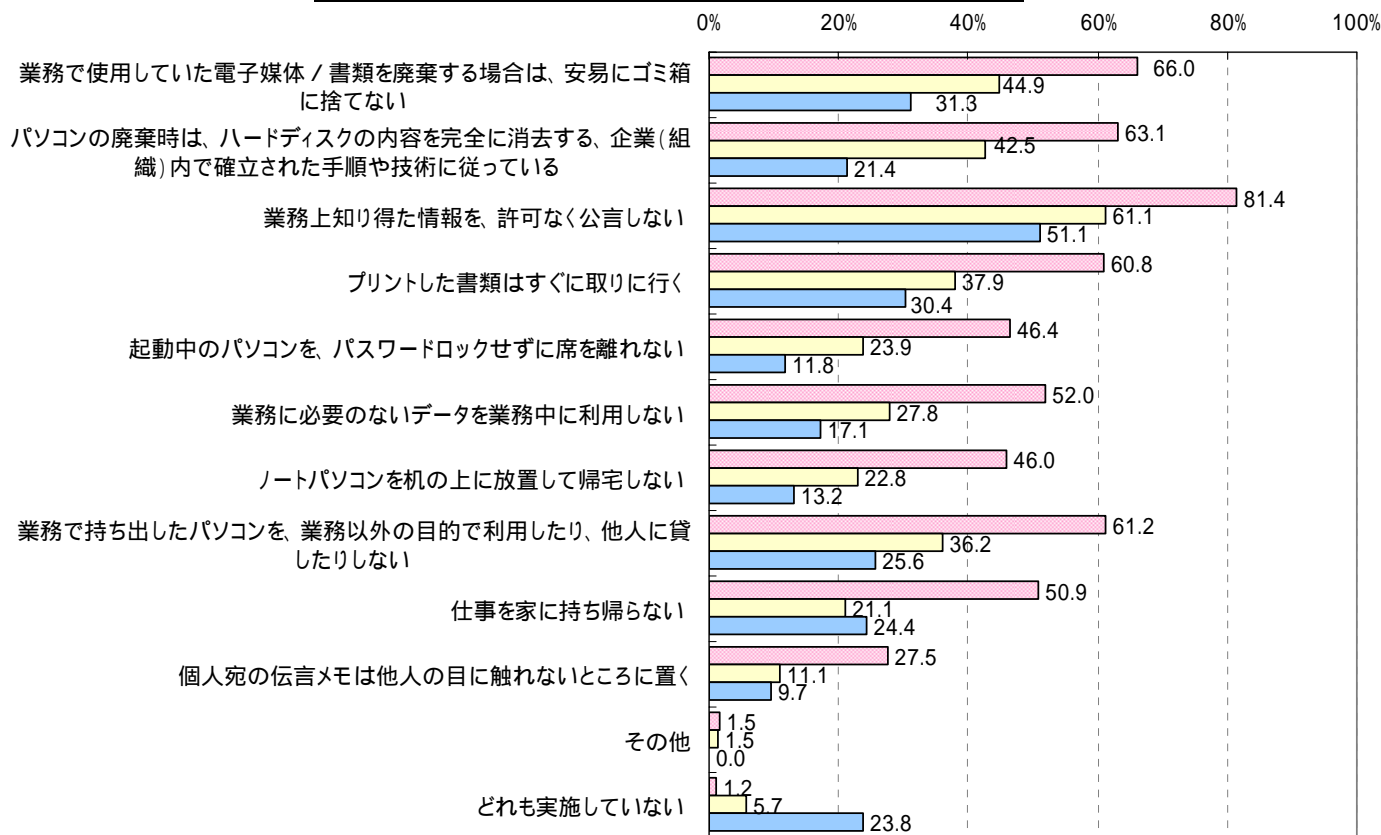
□ 策定されており、ルールを守っている(N=1,103) □ 策定されているが、あまり守っていない(N=167) □ 策定されていない(N=343)

見易さのため、企業の情報セキュリティ関連規定策定・遵守状況が「わからない」とする回答を除いて表示した。

### 3.2.3 組織における情報セキュリティ対策の実施状況(4)

- 組織における情報セキュリティ関連規定の策定・遵守状況別に組織の対策実施状況を見ると、いずれの対策においても、規定が策定されている組織の方が対策の実施率が高い。

組織における情報セキュリティ対策の実施状況(複数回答) - 2  
 [組織の情報セキュリティ関連規定策定・遵守状況別]



□ 策定されており、ルールを守っている(N=1,103) □ 策定されているが、あまり守っていない(N=167) □ 策定されていない(N=343)

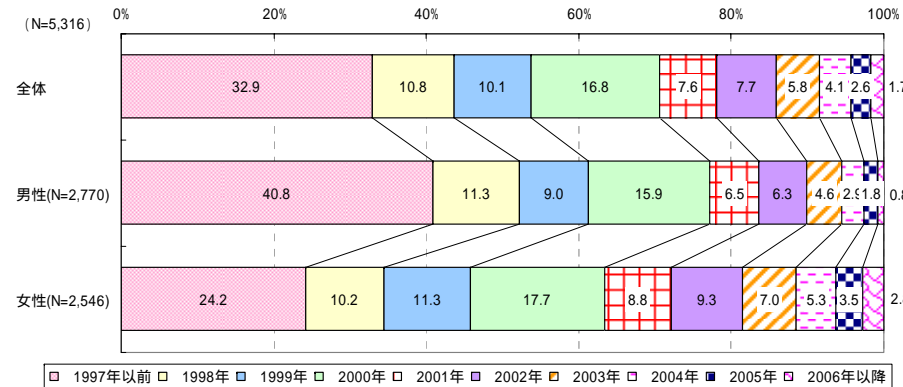
見易さのため、企業の情報セキュリティ関連規定策定・遵守状況が「わからない」とする回答を除いて表示した。

### 3.3. インターネットの利用状況

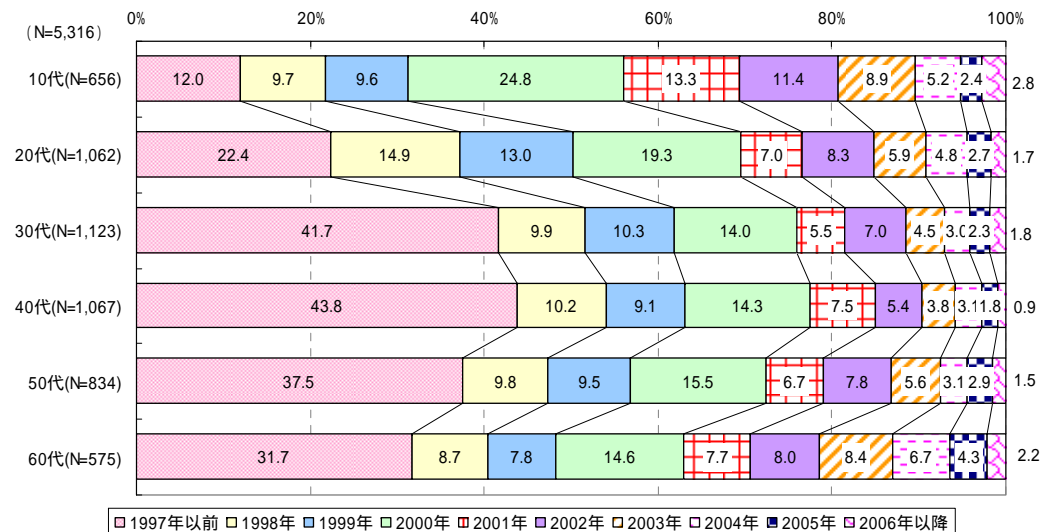
### 3.3.1. インターネット利用開始時期

- 回答者全員にインターネットの開始時期について尋ねた。
- 最も多いのは1997年以前で32.9%、ついで2000年と続く。
- [性別]では、男性の1997年以前が4割を超える。[年代別]では、30代と40代が1997年以前に集中している。

インターネットの利用開始時期  
[回答者全体 / 性別]



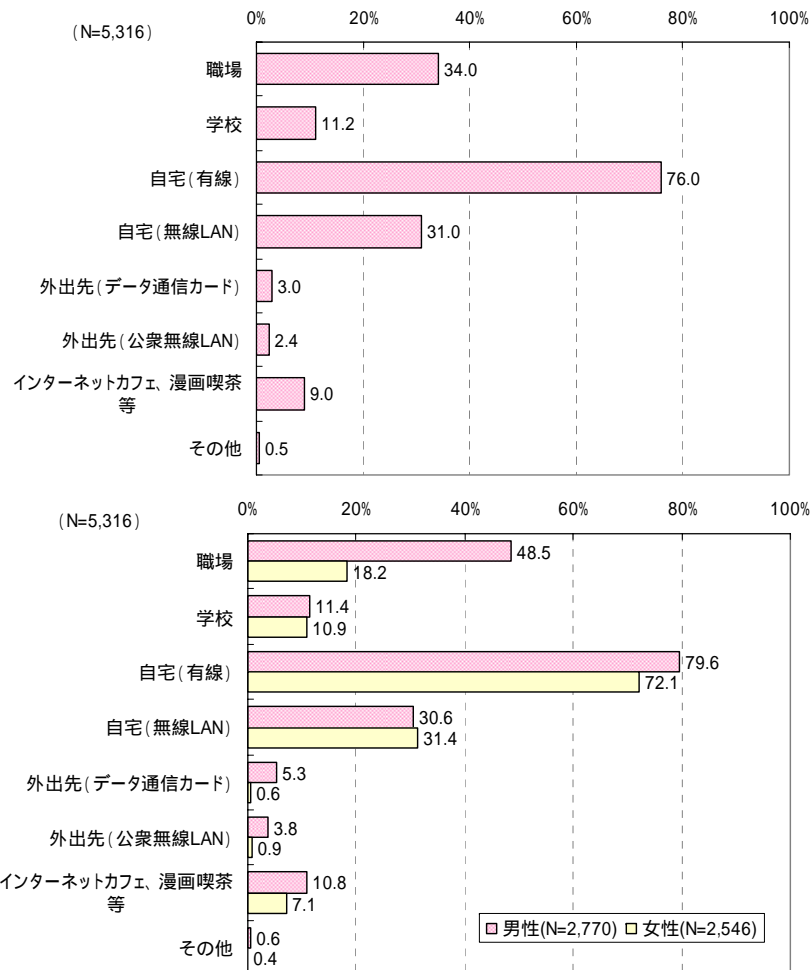
インターネットの利用開始時期  
[年代別]



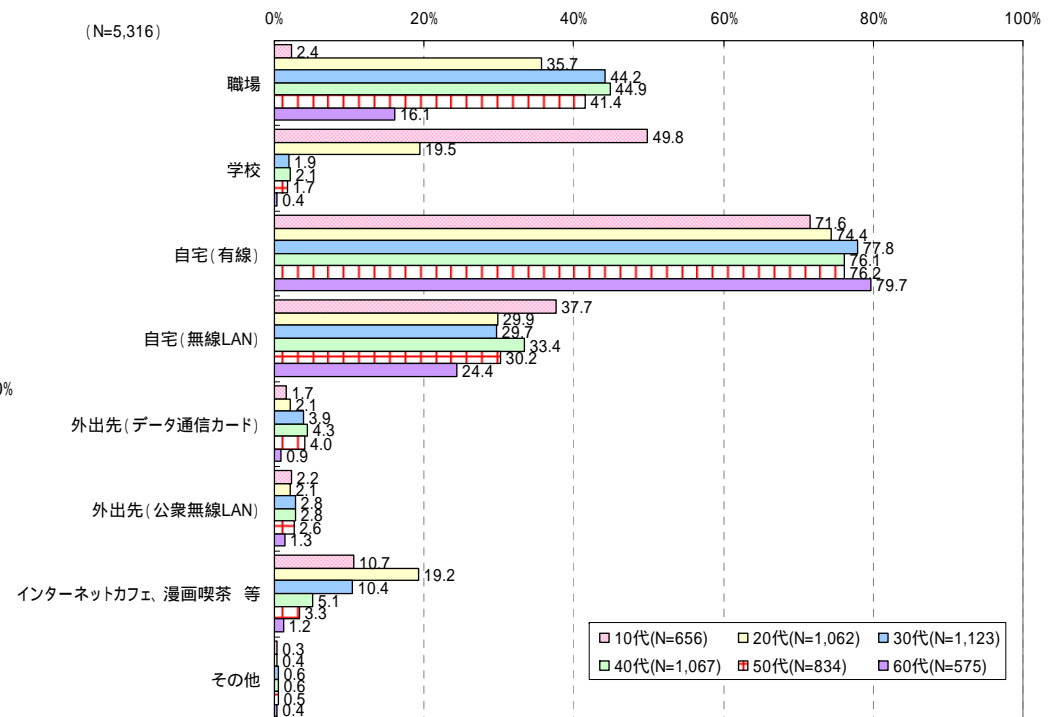
## 3.3.2. インターネット利用場所

- 回答者全員にインターネット利用場所について尋ねた。
- 全体では、「自宅(有線)」で利用しているのが8割近く最も多く、次いで「職場」「自宅(無線)」が約3割で続く。
- [性別]では、男性の5割近くが職場利用しており、女性の職場での利用は2割未満にとどまる。
- [年代別]では、「職場」での利用率は30～50代がいずれも4割を超える。

インターネット利用場所 [回答者全体 / 性別]

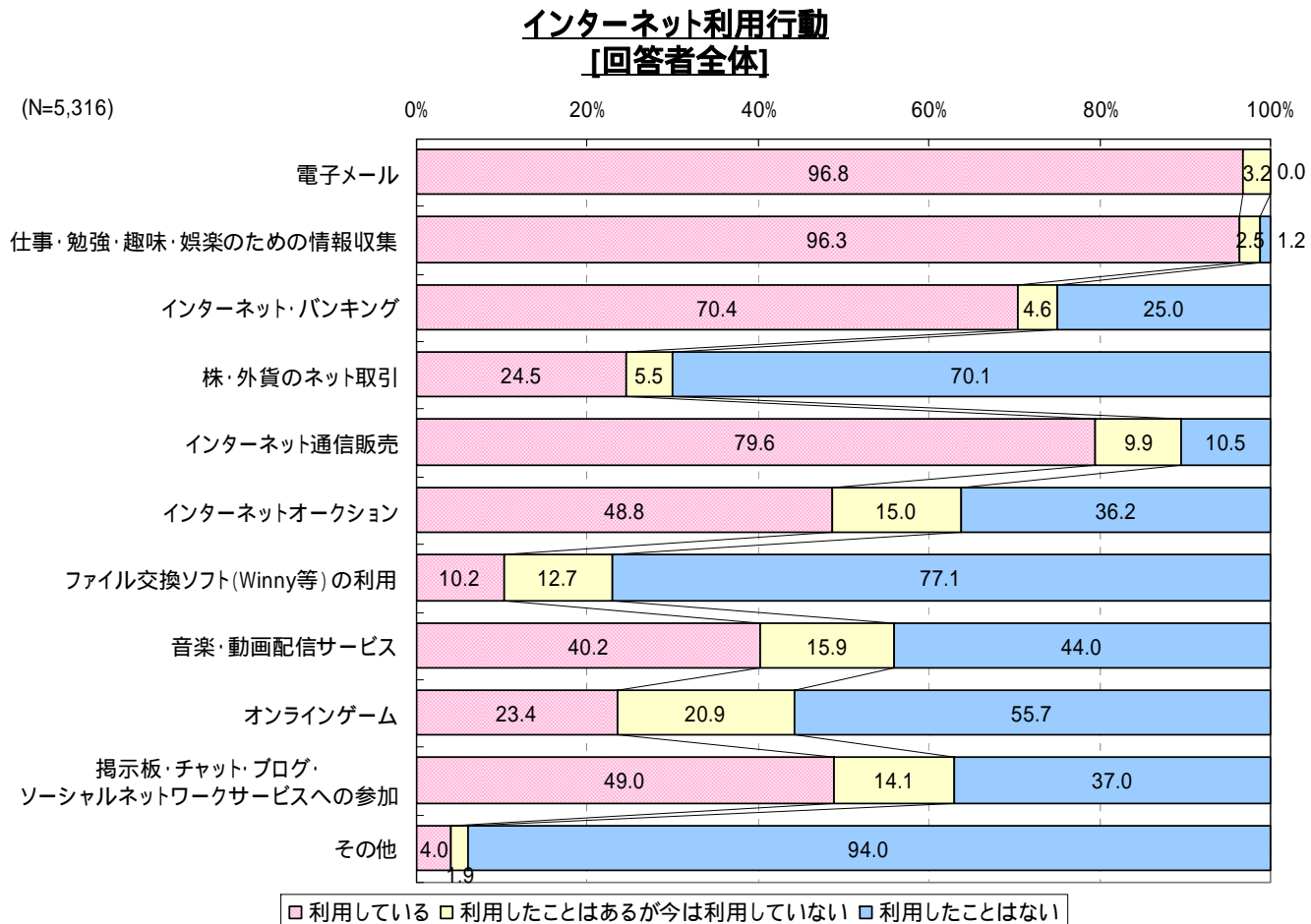


インターネット利用場所(複数回答) [年代別]



### 3.3.3. インターネット利用行動

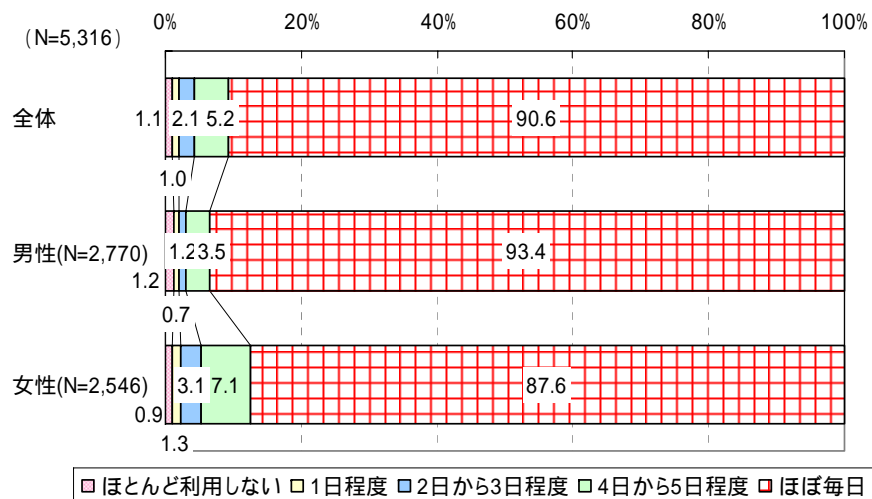
- 回答者全員にインターネット利用行動について尋ねた。
- 「電子メール」および「仕事・勉強・趣味・娯楽のための情報収集」はほぼ全ての回答者が利用している。「インターネット通信販売」は8割近く、「インターネット・バンキング」も7割が利用している。近年利用者が増えている「掲示板・チャット・ブログ・ソーシャルネットワークサービスへの参加」が5割程度、「音楽・動画配信サービス」が4割程度が利用している。情報漏えい等でも問題になった「ファイル交換ソフト(Winny等)の利用」は1割程度である。



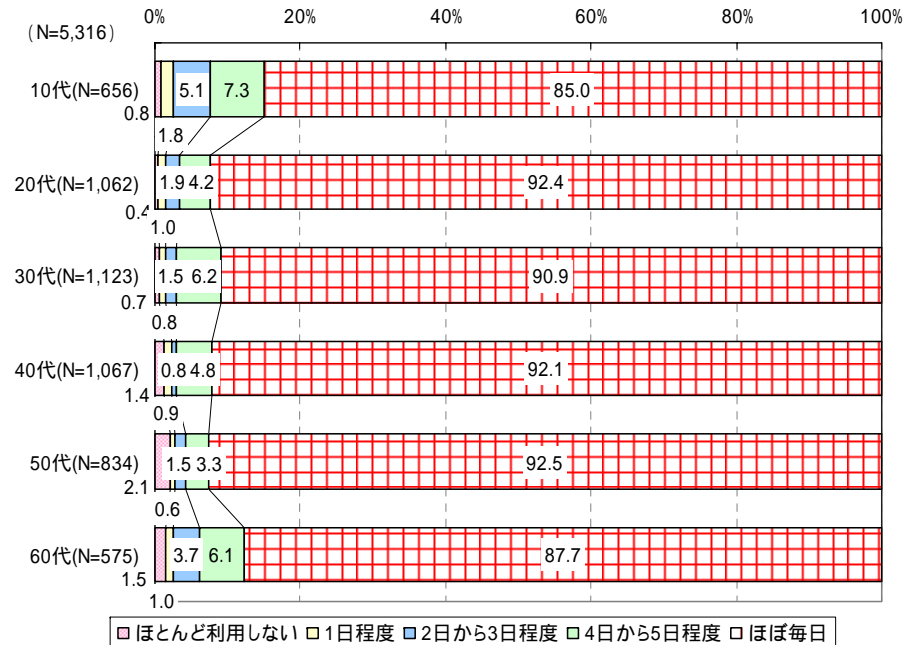
### 3.3.4. インターネット利用頻度

- 回答者全員に1週間のインターネット利用頻度について尋ねた。
- 回答者の約9割が「ほぼ毎日」インターネットを利用している。
- [性別]では、「男性」の方が「ほぼ毎日」利用する率がやや高い。
- [年代別]では、「60代」の「ほぼ毎日」利用する率がやや低いが、その他の年代の傾向に特に大きな差はない。

インターネット利用頻度  
[回答者全体 / 性別]



インターネット利用頻度  
[年代別]



調査票

## インターネット利用と情報セキュリティに関するアンケート

本アンケートは、[独立行政法人情報処理推進機構 (IPA)] が実施します。

下記アンケートにご協力をお願いします。

当アンケートの回答者の管理をお願いします

マクロミルモニタの管理にはモニタ規約にて「調査についての守秘義務」の趣意をお願いします。

当アンケートの内容および当アンケートで知り得た情報については、決して第三者に口外しないよう（掲示板やホームページへの書き込みを含む）、ご協力をお願いします。

Q1 あなたの職業を以下からひとつ選んでください。

【必須入力】

- 1. 経営者・役員
- 2. 会社員・公務員・教員（管理職）
- 3. 会社員・公務員・教員（情報システムおよび連携関係の技術者・研究者）
- 4. 会社員・公務員・教員（情報システムおよび連携関係の技術者・研究者以外）
- 5. 医者・弁護士等、専門職
- 6. 契約社員/派遣社員
- 7. 自営業・自由業
- 8. 専業主婦
- 9. 家事手伝い・無職
- 10. パート・アルバイト
- 11. 中学生
- 12. 高校生
- 13. 大学生・大学院生
- 14. その他

Q2 あなたが、パソコンでインターネットを利用し始めた時期はいつですか。

【必須入力】

- 1. 1997年以前
- 2. 1998年
- 3. 1999年
- 4. 2000年
- 5. 2001年
- 6. 2002年
- 7. 2003年
- 8. 2004年
- 9. 2005年
- 10. 2006年以降

Q3 あなたがパソコンでインターネットを利用する場所はどこですか。（複数回答可）

【必須入力】

- 1. 職場
- 2. 学校
- 3. 自宅（有線）
- 4. 自宅（無線LAN）
- 5. 外出先（データ通信カード）
- 6. 外出先（公衆無線LAN）
- 7. インターネットカフェ、漫画喫茶 等
- 8. その他

Q4 プライベートおよび仕事を問わず、パソコンでインターネットを利用する頻度は一週間でどれくらいですか。

【必須入力】

- 1. ほとんど利用しない
- 2. 1日程度
- 3. 2日から3日程度
- 4. 4日から5日程度
- 5. ほぼ毎日

Q5 プライベートにおいて、パソコンでインターネットをどのようなことに利用していますか。

※ 「11. その他」が特になければ、「利用したことはない」を選択ください。

【必須入力】

	1 利用している	2 利用したことはあるが 今は利用していない	3 利用したことはない
1. 電子メール	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2. 仕事・勉強・趣味・娯楽のための情報収集	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3. インターネット・バンキング	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4. 株・外貨のネット取引	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5. インターネット通信販売	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6. インターネットオークション	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
7. ファイル交換ソフト (Winny等) の利用	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
8. 音楽・動画配信サービス	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
9. オンラインゲーム	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
10. 掲示板・チャット・ブログ・ソーシャルネット ワークサービス (SNS) への参加	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
11. その他 <input style="width: 100px;" type="text"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- 06 あなたは普段インターネットを利用する際、情報セキュリティに対してどのようにお考えですか。  
【必須入力】

1 全く重要ではない	2 重要ではない	3 重要である	4 非常に重要である
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- 07 パソコンやインターネットを安全に利用するための情報セキュリティに関してお尋ねします。  
次の言葉を聞いたことはありますか。  
ある場合は、どのようなことが生じるか（事象）を知っていますか。  
【必須入力】

	1 聞いたことはない	2 聞いたことはあるが 事象は知らない	3 聞いたこともあり 事象も知っている
1. コンピュータ・ウイルス	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2. セキュリティホール	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3. スпамメール	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4. フィッシング	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5. スパイウェア	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6. ボット	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
7. ファーミング	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
8. ワンクリック不正請求	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
9. セキュリティ対策ソフトの押し売り行為	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
10. 脆弱性	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- 08 コンピュータ・ウイルスに関する説明で、正しいと思われるものを全て選んでください。（複数選択可能）  
【必須入力】

1. インターネットに接続していなければ、コンピュータ・ウイルスに感染することはない。
2. コンピュータ・ウイルスに感染した場合、ネットワークからパソコンを切り離すことが、感染の拡大を防ぐ確実な方法である。
3. ウイルスに感染していないかどうかを確認するためには、ウイルス対策ソフトなどで、定期的にハードディスク全体をスキャン（検査）することが有効である。
4. 正しいものがない

- 09 セキュリティホールに関する説明で、正しいと思われるものを全て選んでください。（複数選択可能）  
【必須入力】

1. セキュリティホールは、悪意のあるユーザが相手のパソコンに攻撃を行うために仕掛けるものである。
2. セキュリティホールが発見された場合は、メーカー等から配布される修正プログラムを適用することで対策を行うことができる。
3. セキュリティホールを解消するためには、Windows Updateなどを利用して、パソコンのオペレーティングシステム（OS）やアプリケーションを最新のものにしておくことが有効である。
4. 正しいものがない

- 010 スпамメールに関する説明で、正しいと思われるものを全て選んでください。（複数選択可能）  
【必須入力】

1. スпамメールとは、広告メールや迷惑メールなど、受信者が望まないにも関わらず一方的に送られてくるメールのことである。
2. 心当たりのないメールや不審なメールには、送信停止の依頼を送信した方がよい。
3. スпамメールでは、悪質なプログラムが仕込まれたウェブサイトへリンクされている場合があるので、メール内のURLを安易にクリックしない方がよい。
4. 正しいものがない

- 011 フィッシングに関する説明で、正しいと思われるものを全て選んでください。（複数選択可能）  
【必須入力】

1. フィッシング・メールは、金融機関等を持ったメールアドレスから電子メールで送信されてくることがある。
2. 送られてきたメールがフィッシング・メールかどうか迷った場合は、そのメールに記載されている企業の連絡先に関心合わせて確認した方がよい。
3. ウイルス対策ソフトをインストールしていれば、フィッシング詐欺にあうことはない。
4. 正しいものがない

- 012 スパイウェアに関する説明で、正しいと思われるものを全て選んでください。（複数回答可）  
【必須入力】

1. スパイウェアは、パソコンユーザが気づかれないように活動するため、インストールされていることに気づきにくい。
2. ウェブサイトにアクセスしてなくてもポップアップ広告が表示されたり、ウェブブラウザに最初に表示されるページが勝手に変更されたりする場合は、スパイウェアに感染している可能性が高い。
3. 継続的にWindows Updateを行っていれば、スパイウェアに感染することはない。
4. 正しいものがない

- 013 ボットに関する説明で、正しいと思われるものを全て選んでください。（複数回答可）  
【必須入力】

1. ボットに感染したパソコンは、外部の人間から操られる恐れがある。
2. ボットに感染したら、見た目にはわかる症状がパソコンに表れるので、すぐに感染したことがわかる。
3. ボット対策には、ウイルス対策ソフトが有効である。
4. 正しいものがない

Q14 ファーミングに関する説明で、正しいと思われるものを全て選んでください。(複数回答可)

【必須入力】

1. ファーミングは、ウェブページアドレス (URL) で接続すべき正しいウェブサイトではないサイトに誘導し、クレジットカード号をはじめとする重要情報を奪う行為である。
2. ファーミングが疑わしいサイトで購読した個人情報を入力してしまった場合には、早急にサービス提供元に連絡し、サービス停止やパスワード変更等の対策を行ったほうがよい。
3. 正しいURLを入力して、ウェブサイトへアクセスすれば、偽サイトに誘導されることはない。
4. 正しいものがない

Q15 ワンクリック不正請求に関する説明で、正しいと思われるものを全て選んでください。(複数回答可)

【必須入力】

1. ワンクリック不正請求は、ウェブページへのアクセスや画像等のクリックだけで料金等を請求される詐欺のことである。
2. 請求を行う画面に自分のIPアドレスやプロバイダ名が表示された場合、自分の名前や連絡先などの個人情報まで盗まれる可能性がある。
3. ワンクリック不正請求を予防するためには、怪しいサイトに近づかない、セキュリティの警告を無視しないことが有効である。
4. 正しいものがない

Q16 あなたは、インターネットを利用して、この1年(2006年4月～2007年3月)の間に、パソコンの起動遅延やシステムの不調の被害にあったことはありますか。

また、被害にあったことがある場合に、その原因と思われるものをお選びください。(複数選択可能)

【必須入力】

1. コンピュータ・ウイルス
2. スパムメール
3. フィッシング
4. スパイウェア
5. ボット
6. ファーミング
7. 被害にあったが、原因はわからない/上記以外の原因
8. 被害にあったことはない

Q17 あなたは、インターネットを利用して、この1年(2006年4月～2007年3月)の間に、不正アクセスの被害にあったことはありますか。

また、被害にあったことがある場合に、その原因と思われるものをお選びください。(複数選択可能)

【必須入力】

1. コンピュータ・ウイルス
2. スパイウェア
3. ボット
4. 被害にあったが、原因はわからない/上記以外の原因
5. 被害にあったことはない

Q18 あなたは、インターネットを利用して、この1年(2006年4月～2007年3月)の間に、個人情報の流出の被害にあったことはありますか。

また、被害にあったことがある場合に、その原因と思われるものをお選びください。(複数選択可能)

【必須入力】

1. コンピュータ・ウイルス
2. スパムメール
3. フィッシング
4. スパイウェア
5. ボット
6. ファーミング
7. ワンクリック不正請求
8. セキュリティ対策ソフトの押し売り行為
9. 被害にあったが、原因はわからない/上記以外の原因
10. 被害にあったことはない

Q19 あなたは、インターネットを利用して、この1年(2006年4月～2007年3月)の間に、知らない人からのメールの受信の被害にあったことはありますか。

また、被害にあったことがある場合に、その原因と思われるものをお選びください。(複数選択可能)

【必須入力】

1. スパムメール
2. フィッシング
3. ファーミング
4. ワンクリック不正請求
5. セキュリティ対策ソフトの押し売り行為
6. 被害にあったが、原因はわからない/上記以外の原因
7. 被害にあったことはない

Q20 あなたは、インターネットを利用して、この1年(2006年4月～2007年3月)の間に、データの盗失や盗用の被害にあったことはありますか。

また、被害にあったことがある場合に、その原因と思われるものをお選びください。(複数選択可能)

【必須入力】

1. コンピュータ・ウイルス
2. フィッシング
3. スパイウェア
4. ボット
5. ファーミング
6. 被害にあったが、原因はわからない/上記以外の原因
7. 被害にあったことはない

121

あなたは、インターネットを利用して、この1年（2006年4月～2007年3月）の間に、知らない間に迷惑メールを受信していた被害にあったことはありますか。

また、被害にあったことがある場合に、その原因と思われるものをお選びください。（複数選択可能）

【必須入力】

- 1. コンピュータ・ウイルス
- 2. スパイウェア
- 3. ボット
- 4. 被害にあったが、原因はわからない/上記以外の原因
- 5. 被害にあったことはない

122

あなたは、インターネットを利用して、この1年（2006年4月～2007年3月）の間に、パソコンの画面に料金の支払いを要求するメッセージの表示の被害にあったことはありますか。

また、被害にあったことがある場合に、その原因と思われるものをお選びください。（複数選択可能）

【必須入力】

- 1. ワンクリック不正請求
- 2. セキュリティ対策ソフトの押し売り行為
- 3. 被害にあったが、原因はわからない/上記以外の原因
- 4. 被害にあったことはない

123

あなたは、インターネットを利用して、この1年（2006年4月～2007年3月）の間に、覚えのない料金の支払いを要求するメールの受信の被害にあったことはありますか。

また、被害にあったことがある場合に、その原因と思われるものをお選びください。（複数選択可能）

【必須入力】

- 1. ワンクリック不正請求
- 2. セキュリティ対策ソフトの押し売り行為
- 3. 被害にあったが、原因はわからない/上記以外の原因
- 4. 被害にあったことはない

124

あなたは、インターネットを利用して、この1年（2006年4月～2007年3月）の間に、クレジットカードの不正利用の被害にあったことはありますか。

また、被害にあったことがある場合に、その原因と思われるものをお選びください。（複数選択可能）

【必須入力】

- 1. フィッシング
- 2. ファーミング
- 3. ワンクリック不正請求
- 4. セキュリティ対策ソフトの押し売り行為
- 5. 被害にあったが、原因はわからない/上記以外の原因
- 6. 被害にあったことはない

125

あなたは、インターネットを利用して、この1年（2006年4月～2007年3月）の間に、覚えのない銀行口座の引落しの被害にあったことはありますか。

また、被害にあったことがある場合に、その原因と思われるものをお選びください。（複数選択可能）

【必須入力】

- 1. フィッシング
- 2. ファーミング
- 3. ワンクリック不正請求
- 4. セキュリティ対策ソフトの押し売り行為
- 5. 被害にあったが、原因はわからない/上記以外の原因
- 6. 被害にあったことはない

126

Q22～Q23において、「パソコンの画面に料金の支払いを要求するメッセージの表示」または「覚えのない料金の支払いを要求するメールの受信」を経験されたとお答えの方にお尋ねします。

そのようなメッセージやメールを受け取った際に、実際に支払いを行ってしまった経験はありますか。

【必須入力】

- 1. 支払いを行った経験がある
- 2. 支払いを行った経験はない

127

インターネット利用中に、「貴方のパソコンがウイルスに感染しているため、セキュリティ対策ソフトをダウンロードすることをお勧めします。」または、「パソコンにエラーが発生していますので、セキュリティ対策ソフトをダウンロードすることをお勧めします。」といった内容のメッセージが表示されたことがありますか。

ある場合は、その対策ソフトをダウンロード・インストールしたり、クレジットカード番号を入力して購入したことがありますか。

【必須入力】

- 1. メッセージが表示されたことがあり、その対策ソフトをダウンロード・インストールしたり購入したこともある
- 2. メッセージが表示されたことはあるが、その対策ソフトをダウンロード・インストールしたり購入したことはない
- 3. メッセージが表示されたことはない

128

ご自宅のパソコンでのセキュリティ対策ソフトの利用状況について、以下にあげるもののうち、実施しているものはどれですか。（複数選択可能）

【必須入力】

- 1. セキュリティ対策ソフトを導入している
- 2. 定義ファイルの更新を行っている
- 3. 定期的にウイルスチェックを行っている
- 4. どれも実施していない

Q29 プライベートで受信したメールの扱いについて、以下にあげるもののうち、実施しているものはどれですか。(複数選択可能)  
【必須入力】

- 1. 怪しいメールや添付ファイルを削除する
- 2. 知らない人からのメールを開かない
- 3. 知らない人からのメールに添付されたファイルを開かない
- 4. どれも実施していない

Q30 プライベートでメールを送信するときに、以下にあげるもののうち、実施しているものはどれですか。(複数選択可能)  
【必須入力】

- 1. ファイルを添付するときは、そのファイルをウイルス検査してから添付する(ウイルス対策ソフトで、送信メールのウイルスチェックを行うような設定にしている)
- 2. HTML形式のメール(ウェブページのように文字の大きさを変えたり、色を変えたり、写真を貼り付けたりできるメール)を利用しない設定にしている
- 3. PGP (Pretty Good Privacy) などのメール暗号化ソフトを使用している
- 4. どれも実施していない

Q31 プライベートで利用しているパスワードについて、以下にあげるもののうち、実施しているものはどれですか。(複数選択可能)  
【必須入力】

- 1. 英数字や氏名、誕生日などを使わない
- 2. 8文字以上でパスワードを作っている
- 3. パスワードをパソコンに保存しない
- 4. どれも実施していない

Q32 プライベートでインターネットに接続する際に、以下にあげるもののうち、実施しているものはどれですか。(複数選択可能)  
【必須入力】

- 1. パーソナルファイアウォールを利用している
- 2. ファイルをネットワーク上で共有する際は、パスワードを設定している
- 3. ルータを利用している
- 4. どれも実施していない

Q33 プライベートでウェブページを利用する際に、以下にあげるもののうち、注意しているものはどれですか。(複数選択可能)  
【必須入力】

- 1. 怪しいと思われるウェブサイトにはアクセスしない
- 2. ファイル(ソフトウェア)をダウンロードする場合には、信頼できるウェブサイトから行う
- 3. 理解できない確認(警告)メッセージは、キャンセル(いいえ)ボタンで閉じる
- 4. どれも実施していない

Q34 プライベートで使用するパソコンのオペレーティングシステム(OS)について、以下にあげるもののうち、実施しているものはどれですか。(複数選択可能)  
【必須入力】

- 1. ファイルの拡張子を表示する設定にしている
- 2. 自分が望まないプログラム、アプリケーションは削除する
- 3. パッチをあてて、最新の状態にしておく(Windows UpdateまたはMicrosoft Updateの定期的更新)
- 4. どれも実施していない

Q35 プライベートでパソコンを利用する際に、以下にあげるもののうち、実施しているものはどれですか。(複数選択可能)  
【必須入力】

- 1. パソコンに保存したデータのバックアップを行う
- 2. アプリケーションのオリジナルCD-ROMを保管する
- 3. ライセンスの管理を行う
- 4. どれも実施していない

【この質問はQ35で「パソコンに保存したデータのバックアップを行う」と答えた方にお問合せします】

Q36 バックアップの頻度はどのくらいですか、最も近いものをひとつ選んでください。  
【必須入力】

- 1. 毎日
- 2. 週1、2回程度
- 3. 月1、2回程度
- 4. 気づいたとき

Q37 プライベートで使っていたパソコンを処分したり、リサイクルをする際、どのようにデータを消去していますか。(複数選択可能)

【必須入力】

1. ゴミ箱を空にする
2. ハードディスクをフォーマットする
3. データ消去用のソフトウェアを使う
4. ハードディスクを取り外して、物理的に破壊する
5. その他
6. 特に何もしない

Q38 ご自宅での無線LANの設定において、以下にあげるものうち、実施しているものはどれですか。

【必須入力】

	1	2	3	4
	実施している	実施していない	実施しているか言葉の意味がわからない	わからない
1. SSIDを設定する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2. WEP/WPA等を設定する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3. MACアドレスによるフィルタリングを設定する	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4. 空白またはANY端末からの接続を拒否する設定を行う	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q39 無線LANをご自宅で利用していて、以下の被害にあったことはありますか。(複数選択可能)

【必須入力】

1. 通信内容の覗き見
2. 無線LANの不正利用
3. アクセスポイントを奪取られて、無線LANが使用できなくなった
4. その他
5. 特になし

<企業等にお勧めの方にお伺いします>

Q40 あなたが所属する企業等の組織では、情報セキュリティに関する規程などのルールは制定されていますか。また、制定されている場合、あなたはそのルールを守っていますか。

【必須入力】

1. 制定されており、ルールを守っている
2. 制定されているが、あまり守っていない
3. 制定されていない
4. わからない

<企業等にお勧めの方にお伺いします>

Q41 所属する企業等の組織で、情報漏えい対策として、あなたが実施しているものは以下のうちどれですか。(複数選択可能)

【必須入力】

<業務用パソコンの設定>

1. 個人に割り当てられた権限を、許可なく、他の人に貸与または譲渡しない
2. 業務に関係のないフリーウェアなどのプログラムをインターネットからダウンロードしたり、使用したりしない
3. 業務で使用する電子メール（アドレス）を、私用に使用しない

<情報資産の入手・移送>

4. 業務に関係のないウェブサイトを業務用のパソコンで閲覧しない
5. 業務情報（データ）を、業務上、許可を得てから持ち出す場合には、暗号化している
6. 業務情報（データ）を、許可を得てメール送信する場合には、暗号化している
7. USBメモリなどの外部記憶装置を外部から持ち込んで、業務用のパソコンに接続しない

<情報資産の保管・管理>

8. 大切な情報が格納された電子媒体（CD-ROMなど）や書類は、鍵のかかるキャビネット等にしよう
9. 大切な情報を、信頼できる管理下でないパソコン（例えばネットカフェのパソコン）で利用しない
10. 自分で管理できないコンピュータでは、重要な個人情報の入力を行わない
11. 業務上大切な書類を机の上に放置したまま席を離れたり、帰宅したりしない

<ネットワークへの接続>

12. 私物（私有）のパソコンを持ち込んで、企業（組織）のネットワークに接続しない
13. 業務で持ち出したパソコンを、不要時に、企業（組織）外のネットワークに接続しない

<情報の廃棄>

14. 業務で使用していた電子媒体／書類を廃棄する場合は、安易にゴミ箱に捨てない
15. パソコンの廃棄時は、ハードディスクの内容を完全に消去するサービスを利用するか、企業（組織）内で確立された廃棄のための手順や技術に従っている

<その他>

16. 業務上知り得た情報を、許可なく公表しない
17. プリントした書類はすぐに取りに行く
18. 起動中のパソコンを、パスワードロックせずに席を離れない
19. 業務に必要のないデータを業務中に利用しない
20. ノートパソコンを机の上に放置して帰宅しない
21. 業務で持ち出したパソコンを、業務以外の目的で利用したり、他人に貸したりしない
22. 仕事を家に持ち帰らない
23. 個人用の伝言メモは他人の目に触れないところに置く
24. その他
25. どれも実施していない