

2008年度第1回
情報セキュリティに関する脅威に
対する意識調査 報告書

2008年9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	11
3.1 PCインターネットの利用状況	12
3.2 情報セキュリティに関する脅威に対する認知・理解状況	21
3.3 情報セキュリティに関する脅威に対する被害状況	35
3.4 情報セキュリティに関する脅威に対する対策状況	45
3.5 無線LANのセキュリティに対する対策状況	56
参考 調査票	59

1. 調査概要

調査概要

1. 調査名 「情報セキュリティに関する脅威に対する意識調査」
2. 調査目的 個人PCユーザの情報セキュリティに関する認知、理解、意識および行動の現状を把握する。その結果を基に、個人PCユーザに対するセキュリティ関連施策の効果や課題を抽出し、今後の施策検討に資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
株式会社野村総合研究所が設計・作成した調査票に基づき、同社が提供するインターネットアンケートサービス「TrueNavi」を活用して調査を実施した。
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 2008年7月18日(金)～2008年7月22日(火)
6. 有効回答数 5,000名(男性 2,625名(52.5%) 女性 2,375名(47.5%))
各性別・年代別のサンプル割付は、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2007」)の性別・年代別の構成比を基に行い、分析を行うのに十分なサンプルを確保した。

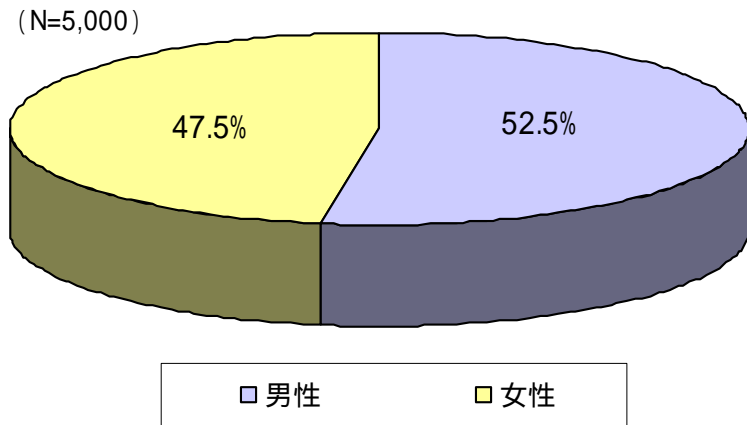
区分	男性		女性		計	
	サンプル数	構成比	サンプル数	構成比	サンプル数	構成比
15-19	215	4.3%	215	4.3%	430	8.6%
20代	530	10.6%	510	10.2%	1,040	20.8%
30代	631	12.6%	597	11.9%	1,228	24.5%
40代	472	9.4%	451	9.0%	923	18.5%
50代	493	9.9%	400	8.0%	893	17.9%
60代	284	5.7%	202	4.0%	486	9.7%
計	2,625	52.5%	2,375	47.5%	5,000	100.0%

7. 調査内容
 - ・PCインターネットの利用状況
 - ・無線LANのセキュリティに対する対策状況
 - ・情報セキュリティに関する脅威に対する認知・理解状況
 - ・情報セキュリティに関する脅威に対する被害状況
 - ・情報セキュリティに関する脅威に対する対策状況

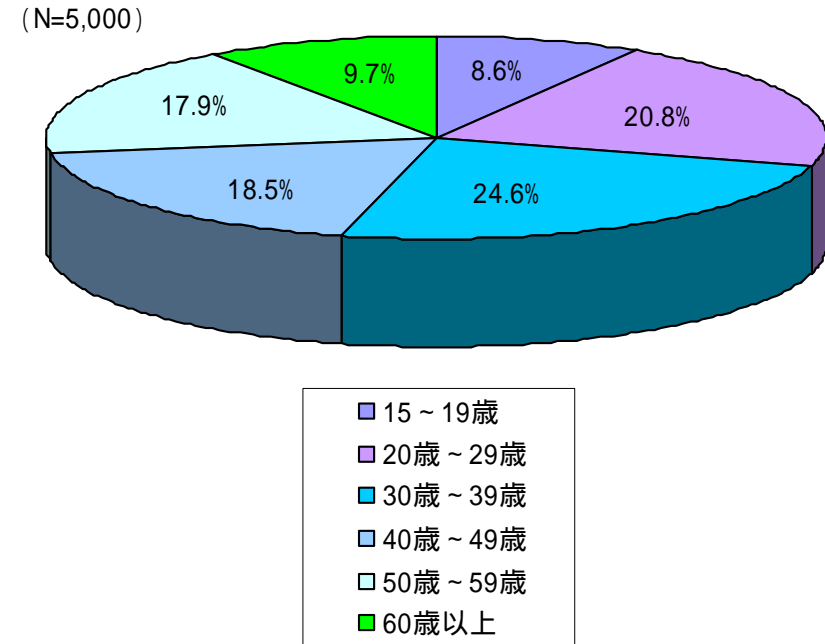
基本属性(1)

- 回答者の性別構成は、「男性」が52.5%、「女性」が47.5%である。
- 回答者の年齢構成は、「30代」をピークとし、次いで「20代」が多い。「10代」は15～19歳が対象ということもあり、全世代の中でも最も低い割合となっている。

回答者の性別

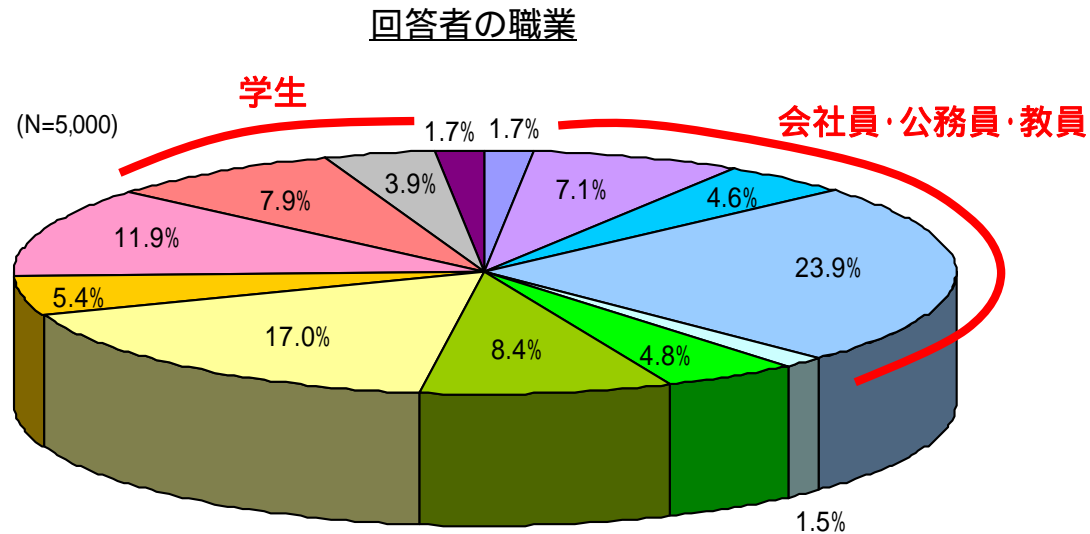


回答者の年齢構成



基本属性(2)

- 回答者の職業構成は、「会社員・公務員・教員」が35.6%と最も多く、次いで、「専業主婦(17.0%)」、「パート・アルバイト(11.9%)」の順となっている。
- 学生は、「専門学校生・短大生・大学生・大学院生」が7.9%、「高校生」が3.9%を占めており、全体の1割を上回っている。



- 経営者・役員
- 会社員・公務員・教員(管理職)
- 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)
- 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・研究者以外の方)
- 医者・弁護士等の専門職
- 契約社員・派遣社員
- 自営業・自由業
- 専業主婦
- 家事手伝い・無職
- パート・アルバイト
- 専門学校生・短大生・大学生・大学院生
- 高校生
- その他

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

最近新聞等よく使用される「ボット」や「マルウェア」といった言葉の詳しい内容や概要について分かっているユーザは全体の20%にも満たない状況である。名前を聞いたことがある程度のユーザを含めても、全体の40%に達していない。

- 「ボット」に対する認知度は、「詳しい内容を知っている」が5.5%、「概要をある程度知っている」が9.9%、「名前を聞いたことがある程度」が19.9%である。また、「マルウェア」に対する認知度は、「詳しい内容を知っている」が5.0%、「概要をある程度知っている」が8.4%、「名前を聞いたことがある程度」が18.4%である。

3.2.1 情報セキュリティに関する攻撃・脅威に対する認知状況(1)(P22)参照

「スパイウェア」といった言葉の詳しい内容や概要について知っていると回答したユーザは全体の55.6%を占めているが、それらのユーザに理解度を把握するための質問を行ったところ、正答率が5問中、4問以上でほぼ正しく理解しているユーザの構成割合は33.2%にしか過ぎない状況(正答率が5問中、3問以下のユーザの構成割合は66.8%)。ユーザがスパイウェアへの対応にあたって適切な対処方法を選択していない可能性がある。

- 正答率が5問中、4問以上を「理解度大」、3問以下を「理解度小」とした場合に、「理解度大」が「理解度小」の割合を大きく下回っているのは、「スパイウェア」以外では、「標的型攻撃」。いずれも概要や特徴がユーザに正しく理解されていない状況が見受けられる。
- 他方、「ワンクリック不正請求」や「フィッシング詐欺」は、比較的ユーザに正しく理解されている。

3.2.2 情報セキュリティに関する攻撃・脅威に対する理解状況(1)(P27)参照

パソコンの習熟度が高まると、情報セキュリティに関する攻撃・脅威を表す言葉への認知度や新たな攻撃手口への感度も高くなり、インターネット利用に対する安心感が醸成される傾向。

- 情報セキュリティに関する攻撃・脅威を表す言葉への認知度について、年代別にみると、「20代」、「30代」の認知度が相対的に高く、「50代」、「60代以上」の認知度が相対的に低い。また、職業別にみると、「会社員・公務員・教員」、「自営業・自由業」の認知度が相対的に高く、「専業主婦」、「パート・アルバイト」の認知度が相対的に低い。

3.2.1 情報セキュリティに関する攻撃・脅威に対する認知状況(5)(P26) / 3.2.3 攻撃手口の実現性に対する感度(2)(P33)参照

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

ユーザの2人に1人が、過去1年間に情報セキュリティに関する何らかの被害やトラブルに遭遇した経験がある。最も多いのは、「全く知らない差出人から大量のメールが送られてきた」の32.0%であり、1年前の調査結果よりも7.5ポイント増加している。

- 過去1年間に情報セキュリティに関する被害やトラブルにあったことがあるユーザは全体の51.0%、被害やトラブルにあっていないユーザは32.7%、被害やトラブルにあったかどうか分からないユーザは16.3%となっている。

3.3.1 情報セキュリティに関する被害やトラブルの経験(1)(P36)参照

「ホームページ閲覧中に、契約した覚えのない料金の支払いを要求するメッセージが表示された」や「身に覚えのない料金の支払いを要求するメールが送られてきた」といった架空請求に遭遇した経験があるユーザについても1年前と比べて増加傾向が顕著である。

- 「ホームページ閲覧中に、契約した覚えのない料金の支払いを要求するメッセージが表示された」ユーザは、2007年7月調査時点では8.7%であったが、本調査では1.4ポイント増加し、10.1%となっている。
- また、「身に覚えのない料金の支払いを要求するメールが送られてきた」ユーザは、2007年7月調査時点では6.3%であったが、本調査では2.8ポイント増加し、9.1%となっている。

3.3.1 情報セキュリティに関する被害やトラブルの経験(1)(P36)参照

架空請求やネットオークション詐欺、オンラインゲーム詐欺等に遭遇した経験があるユーザのうち、金銭的な被害を被ったことがあるユーザは4.5%。平均被害金額は約42,000円、最大被害金額は500,000円。

- ネットオークション利用者のうち、過去1年間に勝手に本人になりすまされ、架空の商品を出品されたり、お金を振り込んだのに商品が届かなかったことがある利用者は、1.8%存在する。
- また、オンラインゲーム利用者のうち、過去1年間にゲーム通貨を不正に搾取されたり、アイテムを騙し取られたことがある利用者も、1.6%存在する。

3.3.1 情報セキュリティに関する被害やトラブルの経験(3)(P38)参照

現在、インターネット上で提供されているサイトやサービスの利用特性についてみると、ユーザが情報セキュリティに関する被害やトラブルと関わりがあると認識し、危ないと分かっているながら利用している場合が多くみられるのが特徴である。サイトやサービスそのものの安全性がユーザに信用されておらず、サイトやサービスを安心して利用するための環境整備も不完全である様相がうかがえる。

- 当該サイト・サービスの利用者のうち、危ないと分かっているながら利用しているユーザ（「関わりがあると思う」あるいは「どちらかといえれば関わりがあると思う」と回答しているユーザ）の割合は、「ファイル交換ソフトの利用」が86.6%と最も高く、次いで、「電子メール（75.9%）」、「掲示板（70.0%）」、「SNS（63.5%）」の順となっている。

3.3.2 情報セキュリティに関する被害やトラブルと関わりがあるサイト・サービス(2) (P40) 参照

ユーザが危ないと分かっているながらサイト・サービスを利用している場合、新たな攻撃手口への感度も高くなる傾向。ユーザが一定レベルの信頼を寄せているサイト・サービスを利用している場合は、新たな攻撃手口への感度が鈍く、新たな攻撃手口による被害に対して脆弱になりがちである。

- 電子メール利用者のうち、「タイトルや文面を工夫し、あなた自身に関係があるメールであるようにみせかけることで、添付ファイルやURLをクリックされやすいようにする手口」や「ウイルスを仕込んだデータファイルをメールに添付し、クリックされやすいようにする手口」について、「すでに実現されているのを知っている」と回答している利用者はそれぞれ43.9%、41.8%となっている。
- また、SNS利用者のうち、「本人確認が必要で、かつ相手の所在の確認が容易であるような安心・安全を売り物にしたサービスを利用することで、詐欺トラブル等に遭わせやすくする手口」について、「すでに実現されているのを知っている」と回答している利用者も40.6%存在する。
- 反対に、ユーザが情報セキュリティに関する被害やトラブルとの関わりについて希薄であると感じ、一定レベルの信頼を寄せているサイト・サービスとしては、「企業・団体のサイト」や「検索サイト、ポータルサイト」、「インターネットバンキング、オンライントレード」が挙げられるが、検索サイト・ポータルサイト利用者のうち、「閲覧したいサイトのURLを正しく入力しても、勝手に別のサイトに誘導されてしまう手口」について、「すでに実現されているのを知っている」と回答している利用者は24.3%にとどまっている。

3.2.3 攻撃手口の実現性に対する感度(1) (P32) 参照

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

情報セキュリティ対策を実施しているユーザが、最も心配しているのは、自分のパソコン内の個人情報や、暗証番号、パスワード、クレジットカード番号等の利用サービス情報が、外部漏えいや削除、改ざんの危険にさらされること。

- ユーザが情報セキュリティに関する被害から守りたいと考えているパソコン内のデータやファイルの中身としては、「利用サービスに関わるもの」、「個人情報に関わるもの」が上位を占め、「会社や職場に関わるもの」、「趣味に関わるもの」は、一部のユーザを除いて、それほど重要ではないという認識。

3.4.2 情報セキュリティ対策を実施している理由(1)(P53)参照

情報セキュリティ対策を実施しているユーザの4人に1人は、情報セキュリティに関する被害やトラブルに実際に見舞われた経験が、情報セキュリティ対策を実施するきっかけになっている。ウイルスの感染等により、パソコンの動作が不安定になったことがきっかけになっている場合が多い。

- 情報セキュリティに関する被害やトラブルの遭遇経験が情報セキュリティ対策を実施するきっかけとなっているユーザのうち、「パソコンが勝手にシャットダウンしたり、新しいウィンドウやフレームが次々に開いて生成されるなど動作が不安定になった」ことが情報セキュリティ対策を実施するきっかけとなっているユーザは56.1%存在する。次いで多いのは、「パソコンのシステムが書き換えられ、パソコンが使えなくなった(23.7%)」こと。

3.4.3 情報セキュリティ対策を実施するきっかけになったもの(P55)参照

無線LANについては、利用者のセキュリティ意識の低さが対策実施上の課題となっている。自宅で使っている無線LANの電波が自宅の外や周辺に届く場合があることを、無線LAN利用者の約20%が知らない状況。また、約30%が電波傍受による通信内容の盗み見の危険性や外部からのアクセスによる侵入の危険性についても認知していない状況。無線LAN利用者の44.6%が対策を実施していない、もしくは対策を実施していることを分かっていない。

- 自宅で無線LANを利用しているユーザのうち、セキュリティ対策を実施しているユーザは55.4%にしか過ぎない状況である。セキュリティ対策の実施率の最も高いものとしては、「WPA2などによる通信の暗号化」が38.2%、次いで、「MACアドレスによる接続制限(フィルタリング)(22.7%)」、「無線LANクライアント側でSSIDを「ANY」あるいは空欄に設定しない(22.4%)」の順となっている。

3.5.1 無線LANのセキュリティに関する被害やトラブルの認知状況(P57)/3.5.2 無線LANのセキュリティ対策の実施状況(P58)参照

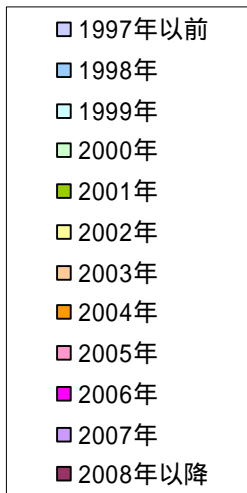
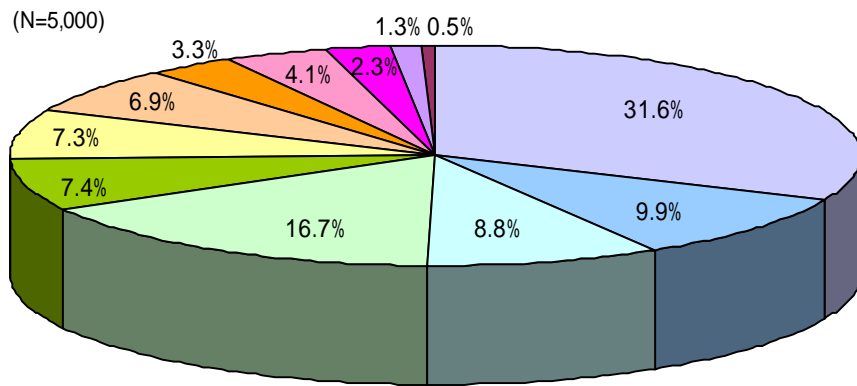
3 . 調查結果

3.1 PCインターネットの利用状況

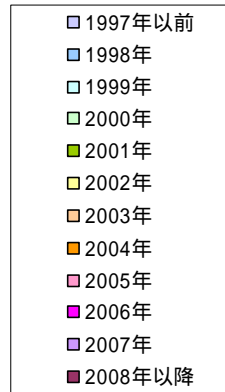
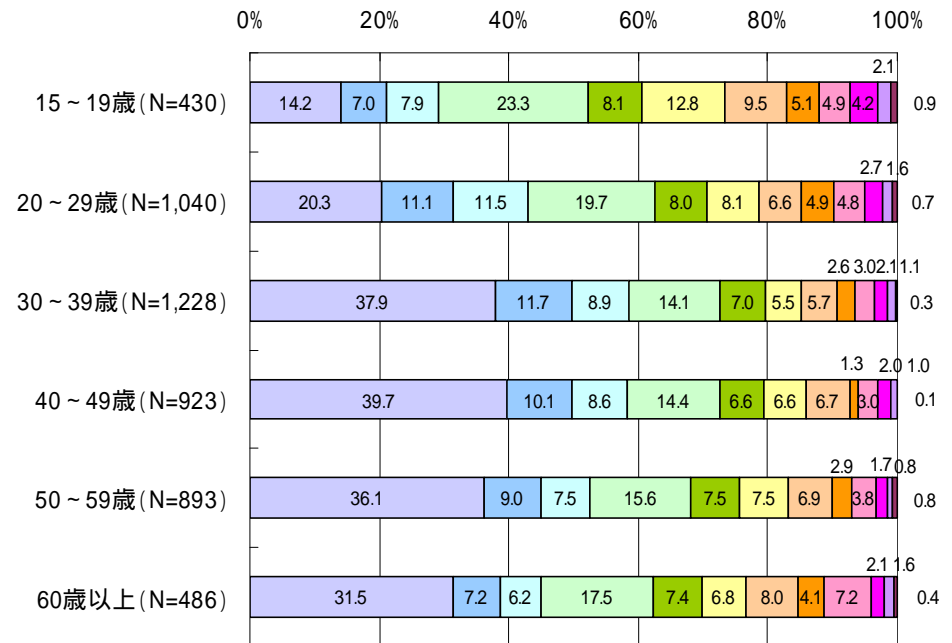
3.1.1 PCインターネットの利用開始時期

- 回答者のうち、インターネットの利用開始から10年以上を経たユーザ(利用開始時期が1997年以前のユーザ)は、全体の31.6%を占める。また、インターネットの利用開始から5年以上を経たユーザ(利用開始時期が2002年以前のユーザ)は、全体の81.7%を占めている。
- 年代別にみると、30代、40代では、「1997年以前」が約40%を占めている。

PCインターネットの利用開始時期



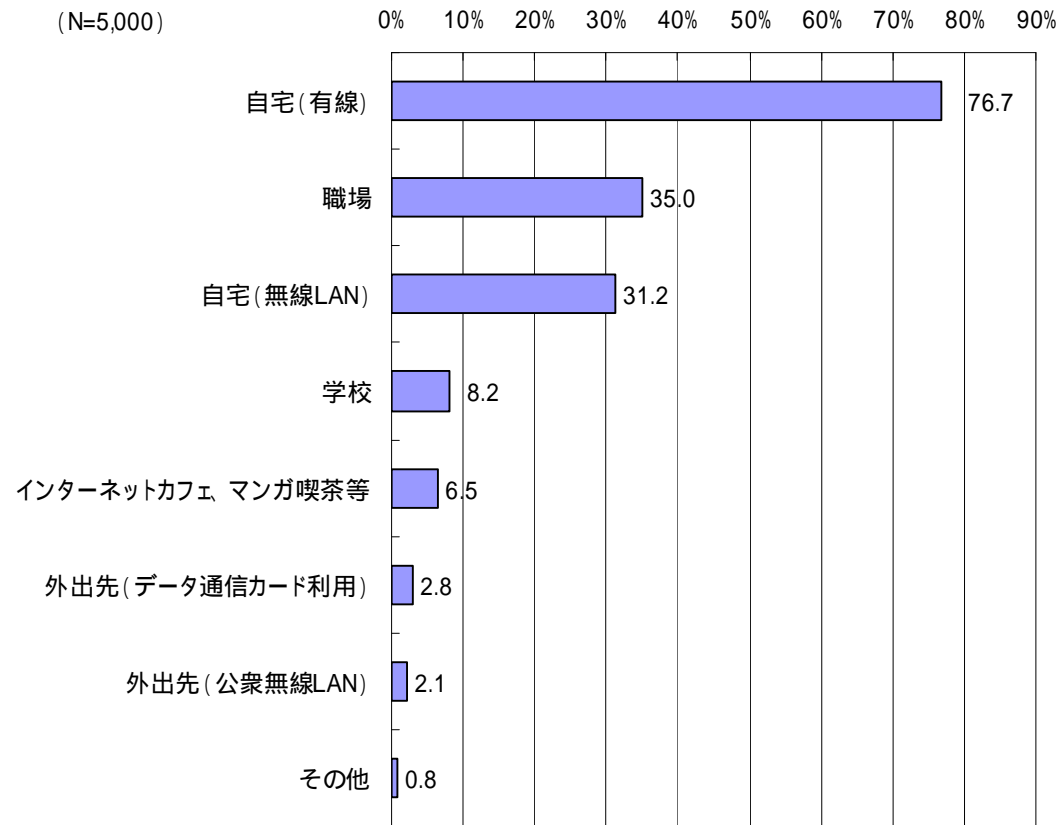
PCインターネットの利用開始時期
[年代別]



3.1.2 PCインターネットの利用場所(1)

- 回答者のインターネットの利用場所についてみると、最も多いのは、「自宅(有線)」で全体の76.7%、次いで「職場(35.0%)」、「(自宅(無線LAN)(31.2%)」の順となっている。
- 「インターネットカフェ、マンガ喫茶等」でのユーザは、全体の6.5%、外出先でデータ通信カードを利用してインターネット接続しているユーザは2.8%、公衆無線LANを利用してインターネット接続しているユーザは2.1%であり、僅少であった。

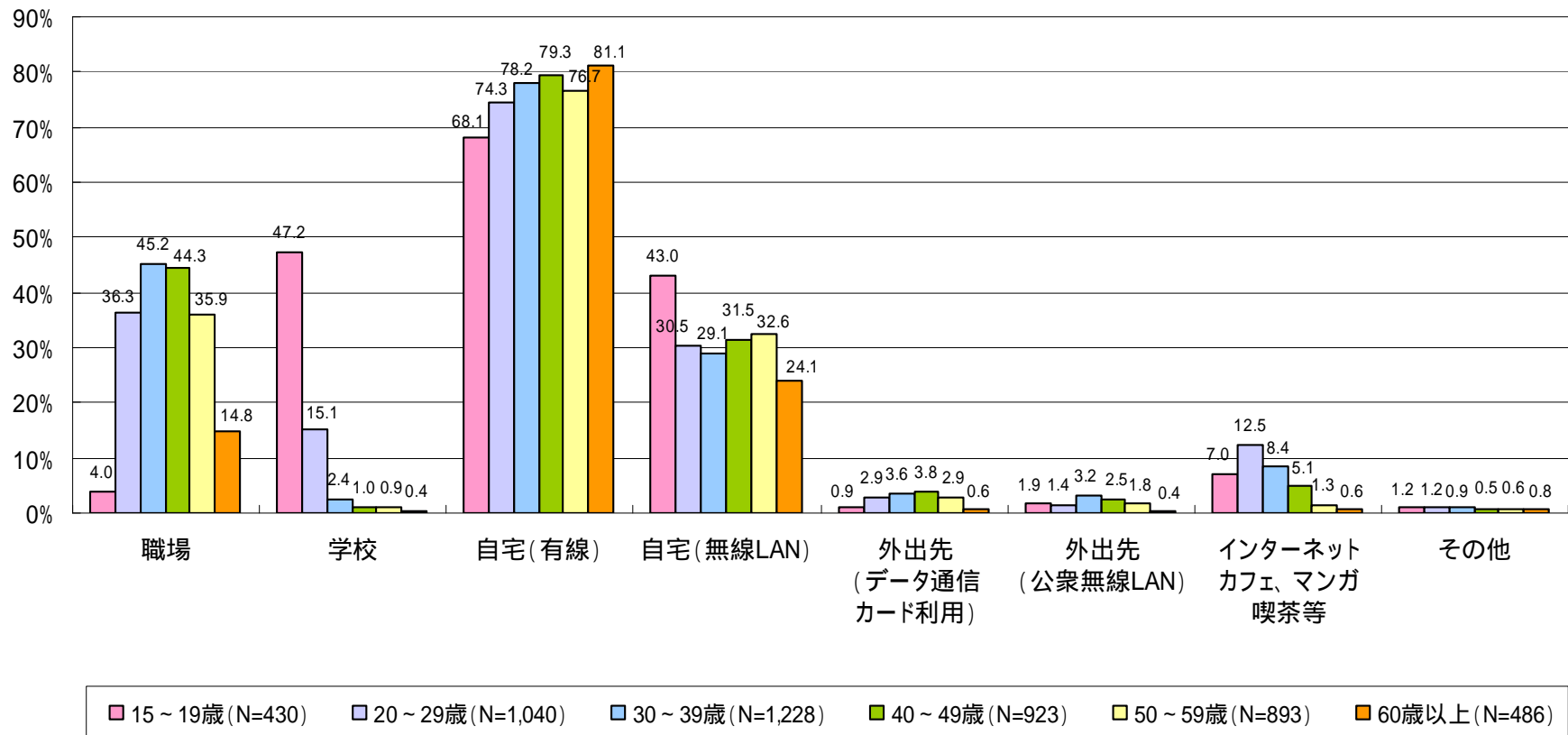
PCインターネットの利用場所



3.1.2 PCインターネットの利用場所(2)

- 年代別にみると、「インターネットカフェ、マンガ喫茶等」での利用は、20代が12.5%と最も多く、次いで、30代が8.4%、10代が7.0%となっている。
- 自宅(無線LAN)での利用は、10代が43.0%であり、他の世代に比べて10%以上多い。

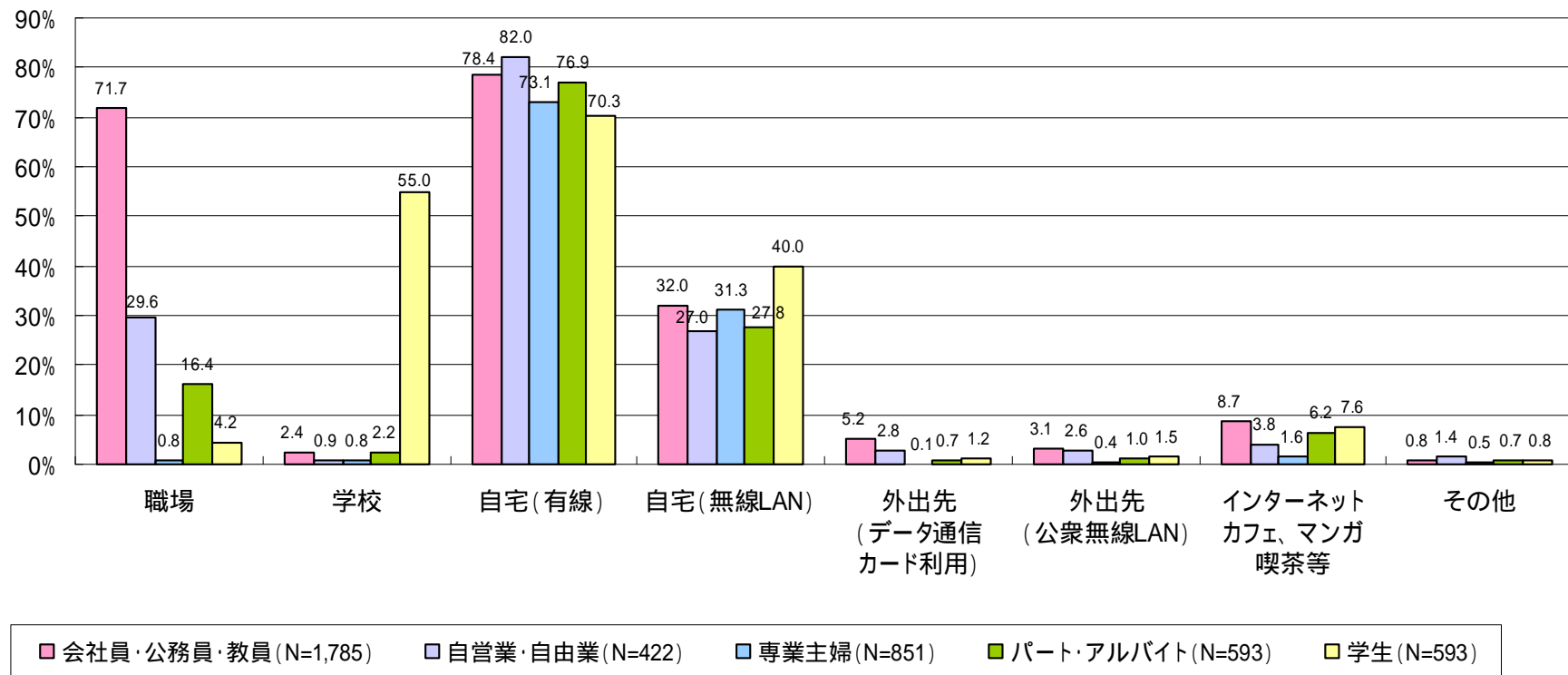
PCインターネットの利用場所
[年代別]



3.1.2 PCインターネットの利用場所(3)

- 職業別にみると、「自宅(無線LAN)」での利用は、学生が40.0%と最も多い。また、「インターネットカフェ、マンガ喫茶等」での利用は、会社員・公務員・教員が8.7%と最も多く、次いで学生が7.6%、パート・アルバイトが6.2%となっている。
- 「外出先(データ通信カード利用)」や「外出先(公衆無線LAN)」での利用が比較的多いのは、会社員・公務員・教員と自営業・自由業である。

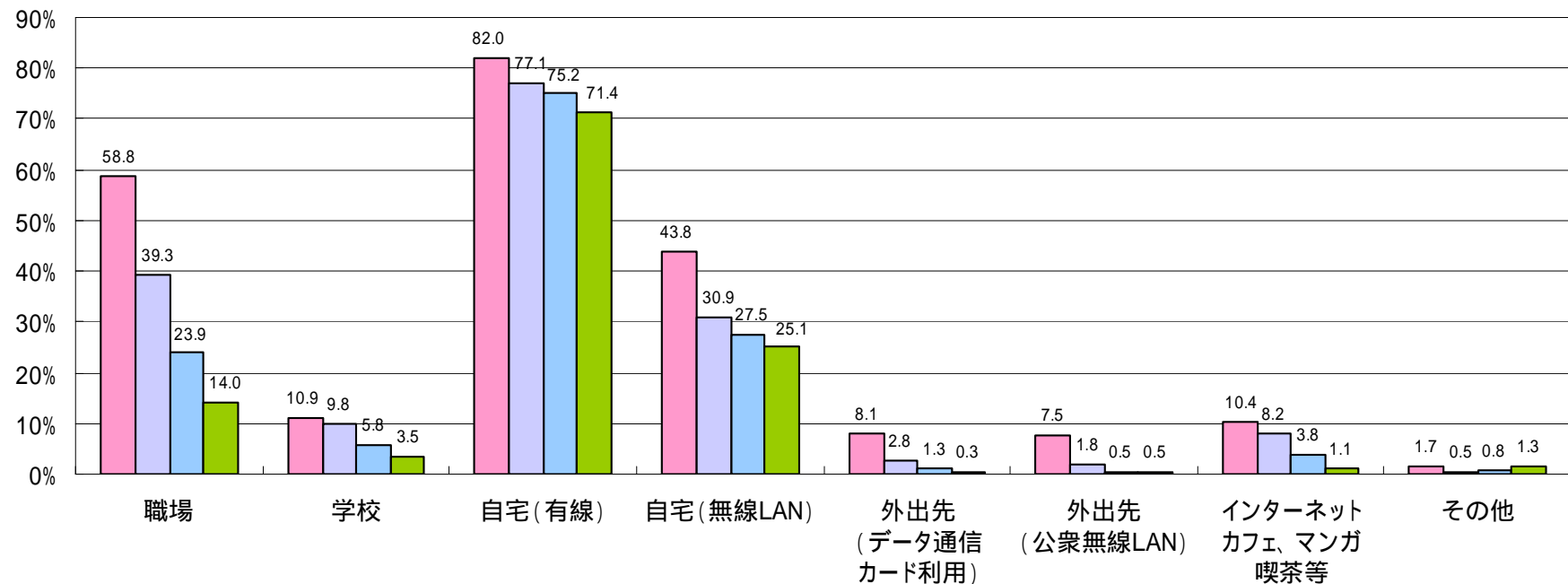
PCインターネットの利用場所
[職業別]



3.1.2 PCインターネットの利用場所(4)

- パソコンの習熟度レベル別にみると、パソコンを自分で組み立てたり、トラブルが起きても自分で解決できる最上級レベルのユーザが、「自宅(無線LAN)」や「外出先(データ通信カード利用)」、「外出先(公衆無線LAN)」での利用を牽引している様相がうかがえる。

PCインターネットの利用場所
[パソコンの習熟度レベル別]

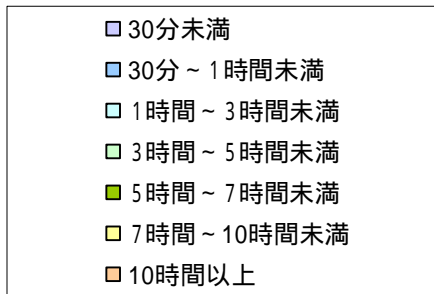
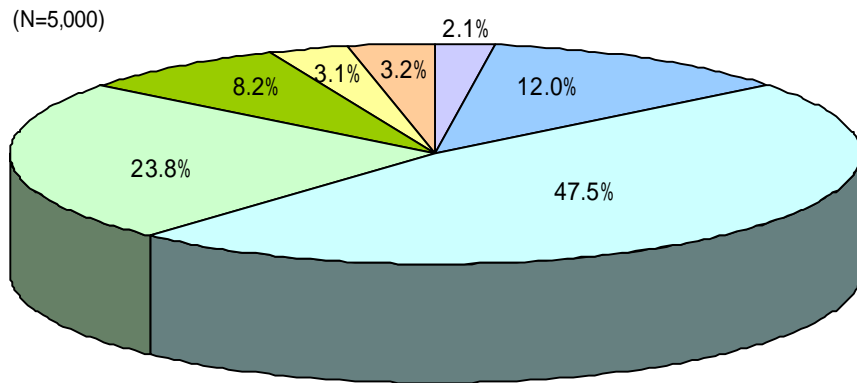


- パソコンを自分で組み立てたり、トラブルが起きても自分で解決できるレベルである (N=704)
- 必要なソフトウェアをインストールして使ったり、パソコンの設定を変えて使ったりすることができるレベルである (N=2,257)
- メールを使ったり、ホームページを閲覧したり、文章を書いたりするのに支障がないレベルである (N=1,668)
- パソコンの簡単な操作しか分からないレベルである (N=371)

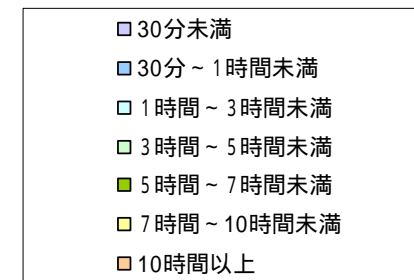
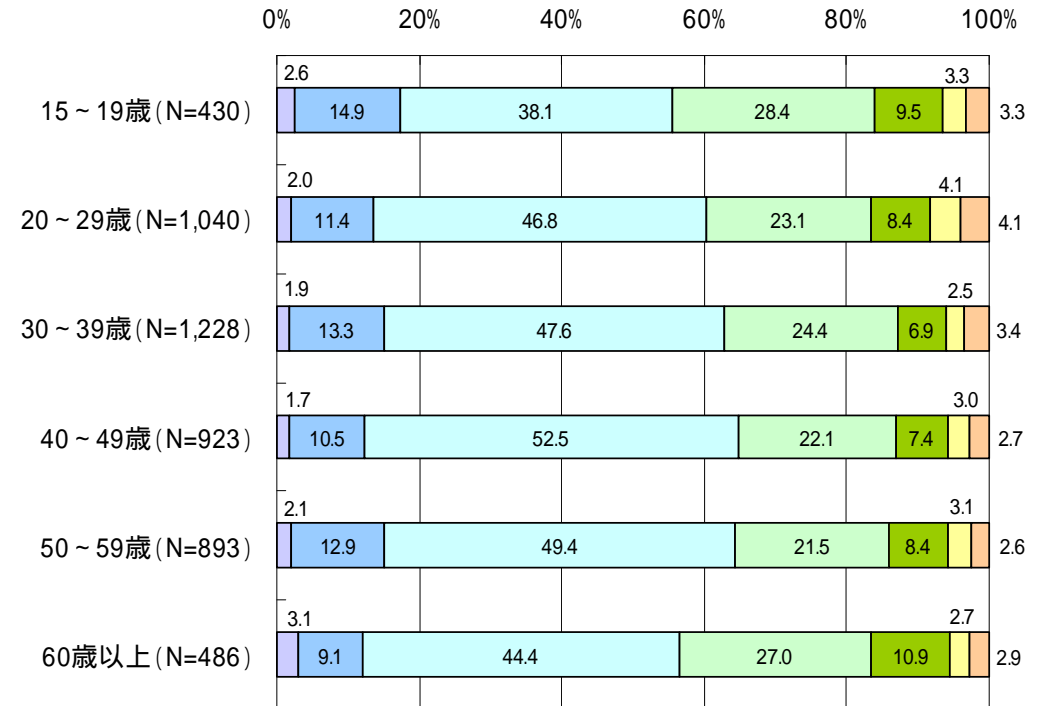
3.1.3 1日のPCインターネットの利用時間(仕事上での利用を除く)

- 仕事上でのインターネット利用を除く、1日のインターネット利用時間は、「1時間～3時間」が47.5%と半数近くを占めている。

PCインターネットの利用時間(1日平均)



PCインターネットの利用時間(1日平均)
[年代別]

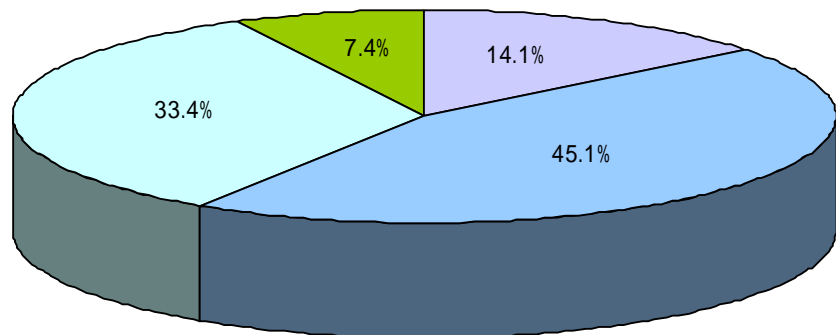


3.1.4 パソコンの習熟度(1)

- 回答者のパソコンの習熟度についてみると、最も多いのは、「必要なソフトウェアをインストールして使ったり、パソコンの設定を変えて使ったりすることができる」という上級レベルのユーザが45.1%、次いで、「メールを使ったり、ホームページを閲覧したり、文章を書いたりするのに支障がない」という中級レベルのユーザが33.4%となっている。
- 「パソコンを自分で組み立てたり、トラブルが起きても自分で解決できる」という最上級レベルのユーザや、「パソコンの簡単な操作しか分からない」という初級レベルのユーザは比較的少数である。
- 年代別にみると、最上級レベルのユーザが多いのは、30代である。60代では、初級レベルのユーザと中級レベルのユーザを合わせると、過半数を大きく上回る。

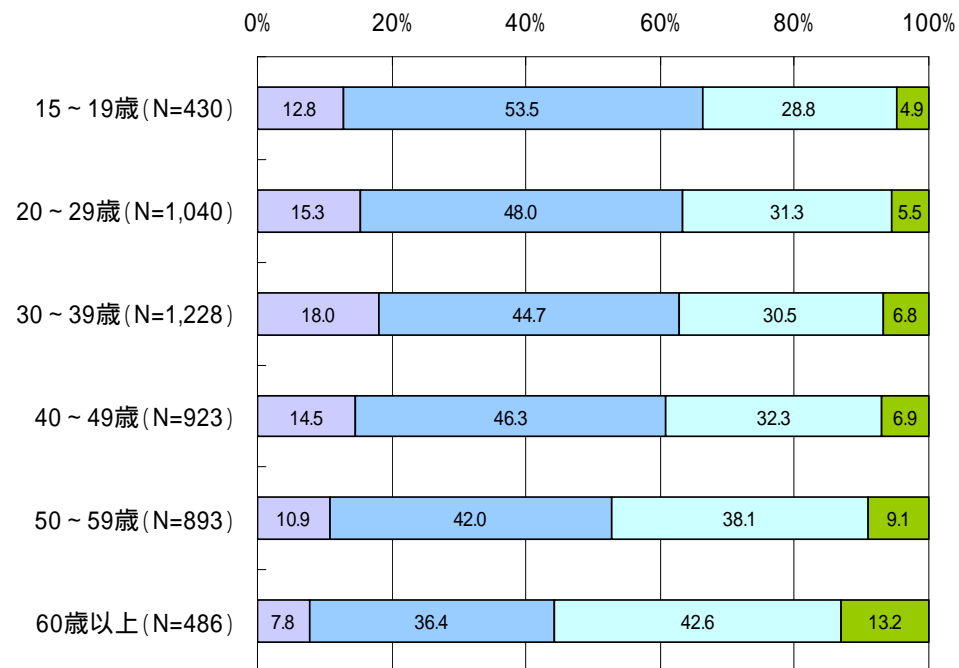
パソコンの習熟度レベル

(N=5,000)



- パソコンを自分で組み立てたり、トラブルが起きても自分で解決できるレベルである
- 必要なソフトウェアをインストールして使ったり、パソコンの設定を変えて使ったりすることができるレベルである
- メールを使ったり、ホームページを閲覧したり、文章を書いたりするのに支障がないレベルである
- パソコンの簡単な操作しか分からないレベルである

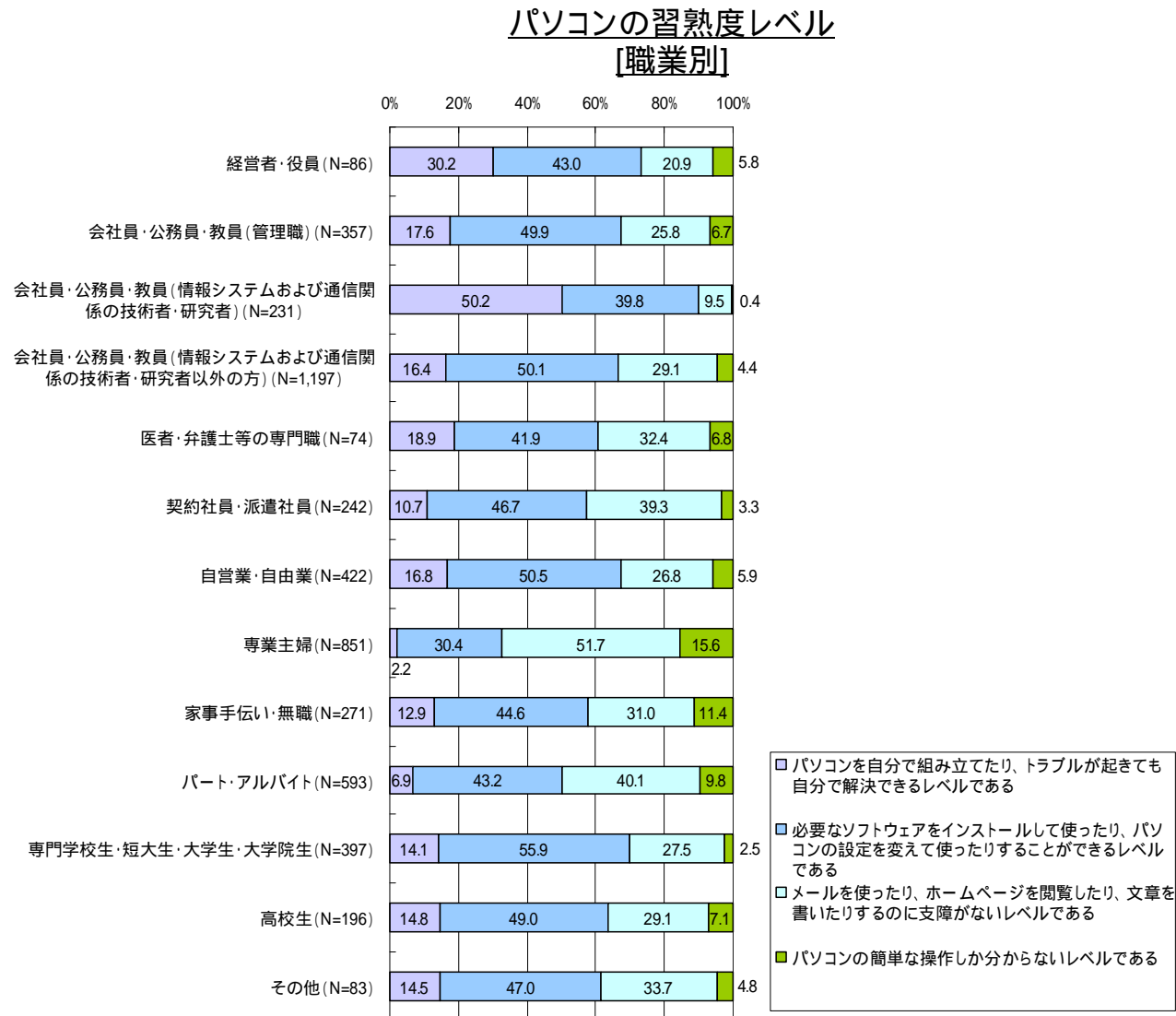
パソコンの習熟度レベル
[年代別]



- パソコンを自分で組み立てたり、トラブルが起きても自分で解決できるレベルである
- 必要なソフトウェアをインストールして使ったり、パソコンの設定を変えて使ったりすることができるレベルである
- メールを使ったり、ホームページを閲覧したり、文章を書いたりするのに支障がないレベルである
- パソコンの簡単な操作しか分からないレベルである

3.1.4 パソコンの習熟度(2)

- パソコンの習熟度が相対的に高いのは、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)であり、パソコンを自分で組み立てたり、トラブルが起きても自分で解決できる最上級レベルのユーザが約50%、必要なソフトウェアをインストールして使ったり、パソコンの設定を変えて使ったりすることができる上級レベルのユーザが約40%を占めている。
- 一方、専業主婦やパート・アルバイトはパソコンの習熟度が相対的に低く、最上級レベルのユーザはそれぞれ2.2%、6.9%、上級レベルのユーザはそれぞれ30.4%、43.2%にとどまっている。

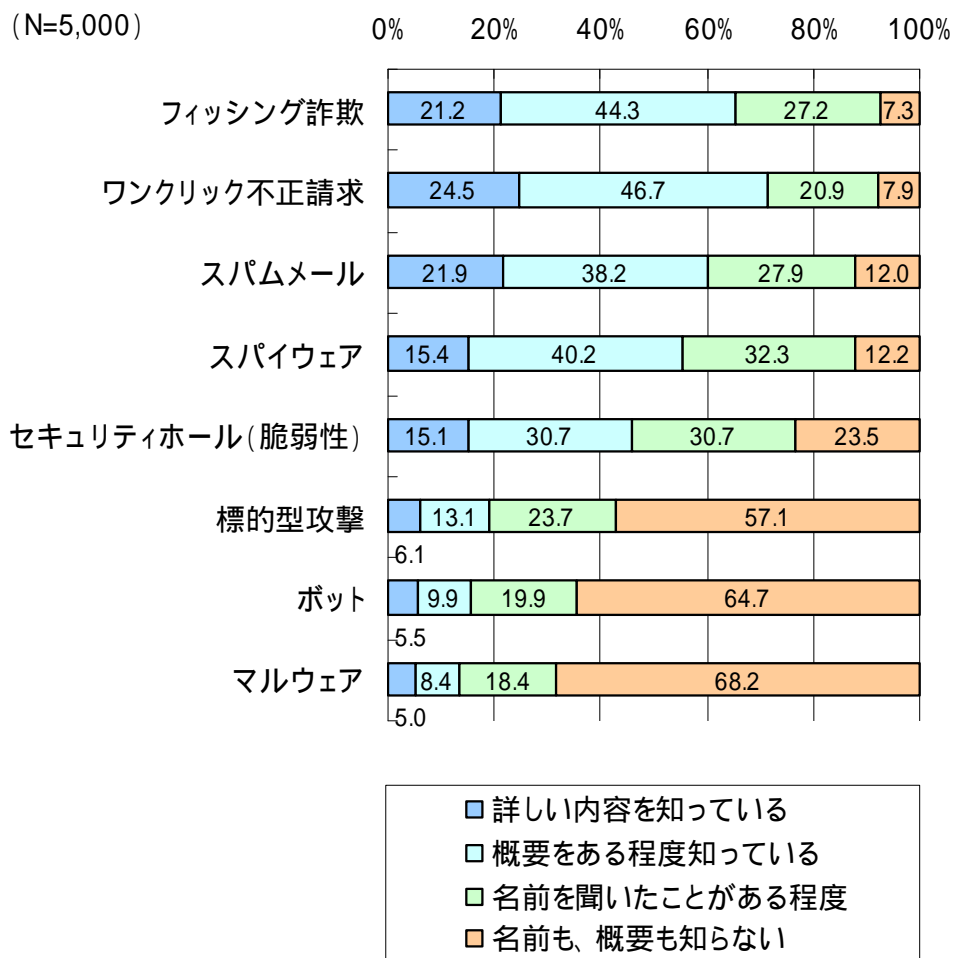


3.2 情報セキュリティに関する脅威に対する認識・理解状況

3.2.1 情報セキュリティに関する攻撃・脅威に対する認知状況(1)

- 情報セキュリティに関する攻撃・脅威を表す言葉について、聞いたことがあるか、攻撃・脅威の内容を知っているかについて尋ねた。
- 「フィッシング詐欺」、「ワンクリック不正請求」、「スパムメール」、「スパイウェア」の4つの言葉は、いずれも90%前後のユーザに、詳しい内容や概要、名前が認知されている。
- 上記の4つの攻撃・脅威のうち、「スパイウェア」については、名前を聞いたことがある程度であるユーザが比較的多い。
- 「標的型攻撃」、「ボット」、「マルウェア」については、詳しい内容や概要について知っているユーザは全体の20%を下回っている。

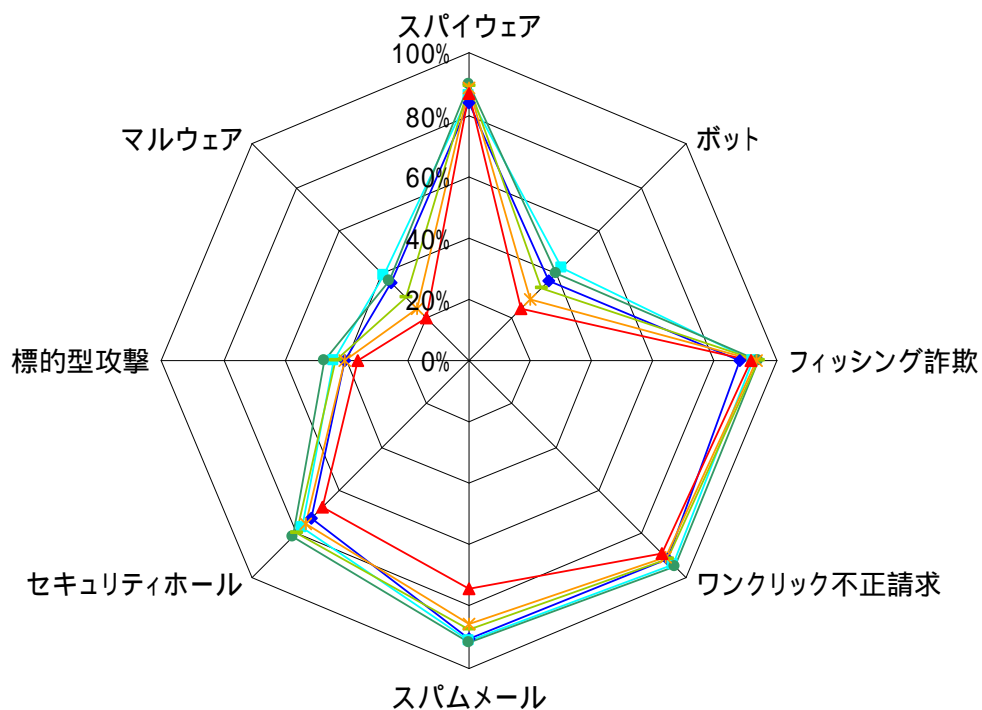
情報セキュリティに関する攻撃・脅威に対する認知状況



3.2.1 情報セキュリティに関する攻撃・脅威に対する認知状況(2)

- 情報セキュリティに関する攻撃・脅威を表す言葉の認知度を、年代別にみると、50代と60代以上の認知度が相対的に低くなっている。詳細な数値を、24～25ページに示す。

情報セキュリティに関する攻撃・脅威に対する認知度
[年代別]



認知度について

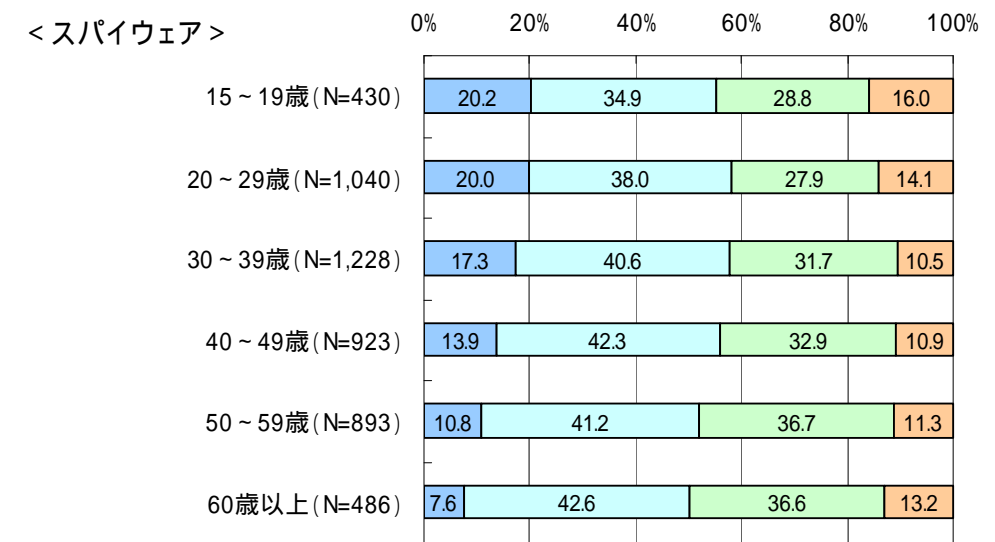
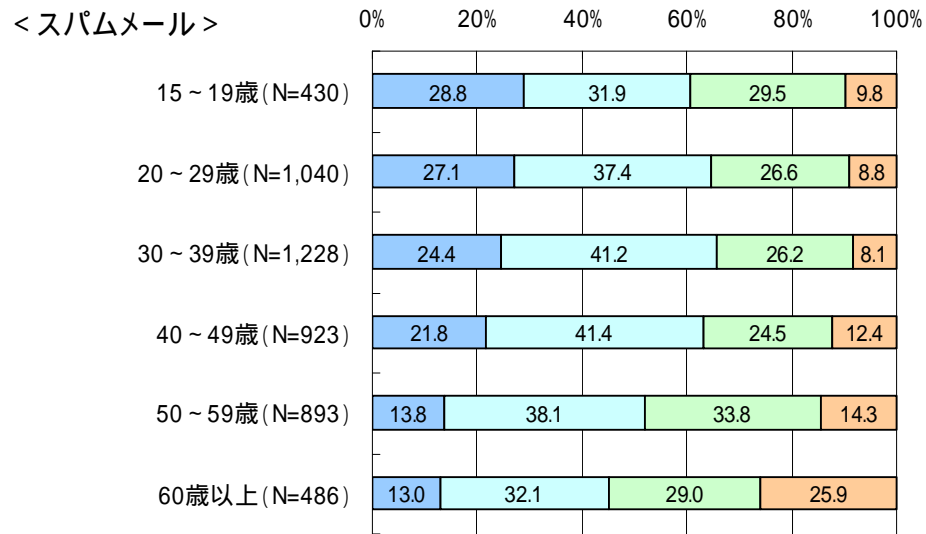
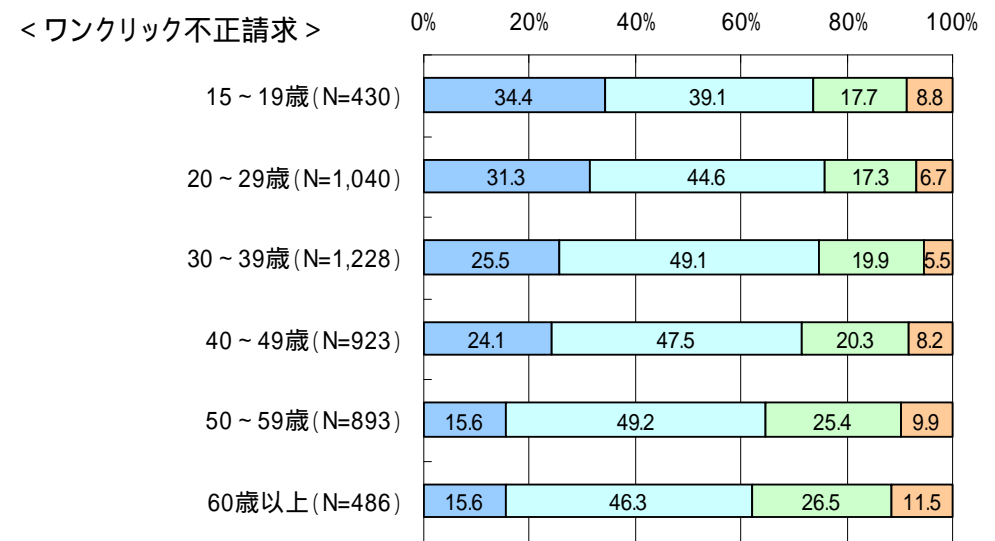
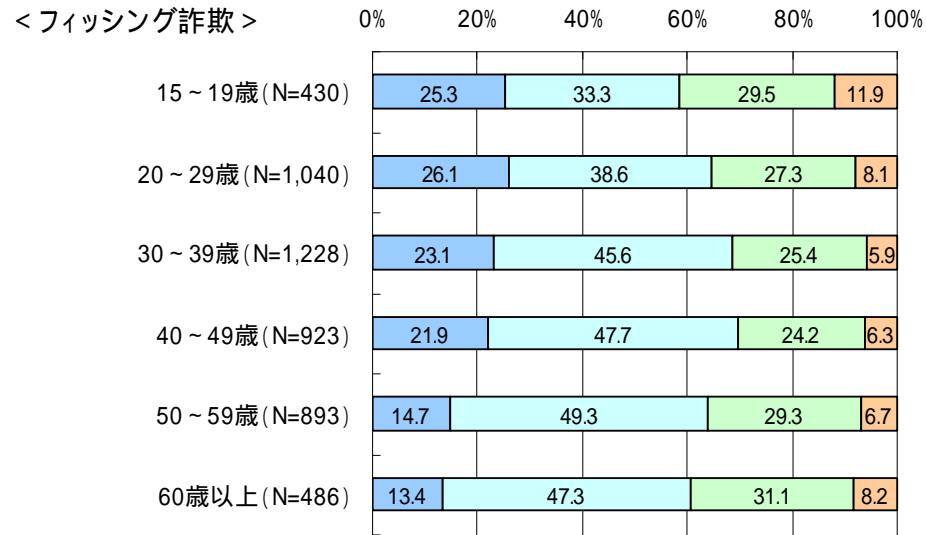
本アンケートでは、ユーザが情報セキュリティに関する攻撃・脅威を表す言葉を、どの程度知っているかについて、「詳しい内容を知っている」、「概要をある程度知っている」、「名前を聞いたことがある程度」、「名前も、概要も知らない」の4つのレベルで把握している。

このうち、「詳しい内容を知っている」、「概要をある程度知っている」、「名前を聞いたことがある程度」それぞれの回答者の割合を足し合わせた値を「認知度」と定義するものとする。

◆ 15～19歳 (N=430)	■ 20～29歳 (N=1,040)
● 30～39歳 (N=1,228)	▲ 40～49歳 (N=923)
✱ 50～59歳 (N=893)	▲ 60歳以上 (N=486)

3.2.1 情報セキュリティに関する攻撃・脅威に対する認知状況(3)

情報セキュリティに関する攻撃・脅威に対する認知状況
[年代別]



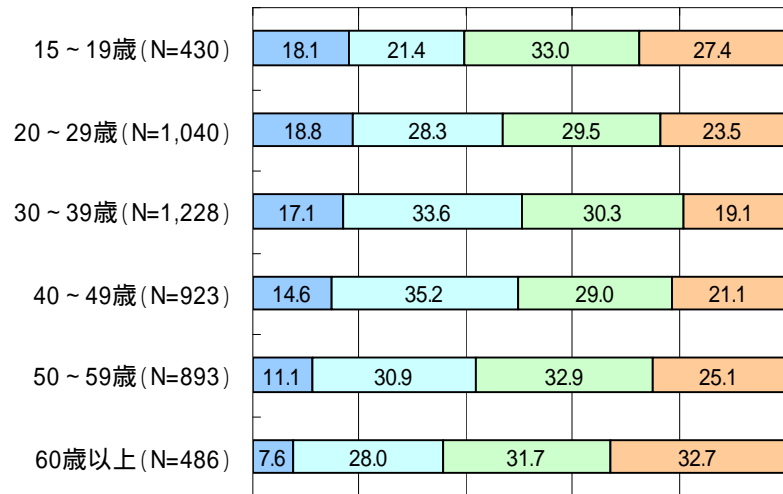
- 詳しい内容を知っている
- 概要をある程度知っている
- 名前を聞いたことがある程度
- 名前も、概要も知らない

- 詳しい内容を知っている
- 概要をある程度知っている
- 名前を聞いたことがある程度
- 名前も、概要も知らない

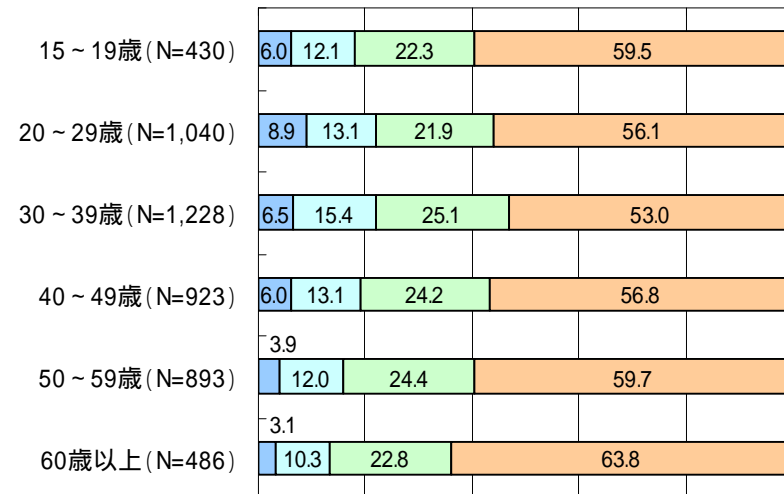
3.2.1 情報セキュリティに関する攻撃・脅威に対する認知状況(4)

情報セキュリティに関する攻撃・脅威に対する認知状況
[年代別]

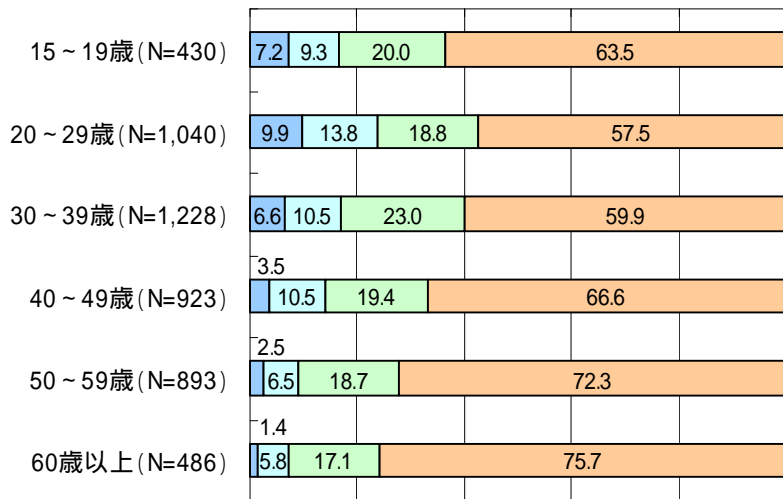
< セキュリティホール(脆弱性) > 0% 20% 40% 60% 80% 100%



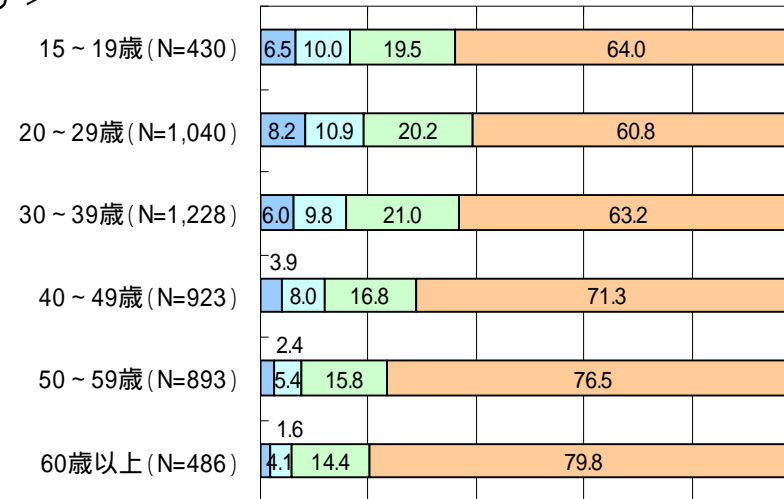
< 標的型攻撃 > 0% 20% 40% 60% 80% 100%



< ボット > 0% 20% 40% 60% 80% 100%



< マルウェア > 0% 20% 40% 60% 80% 100%



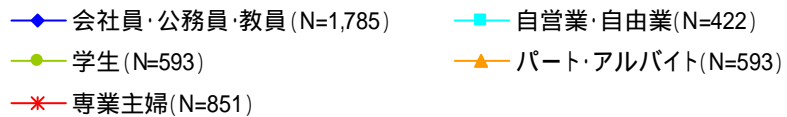
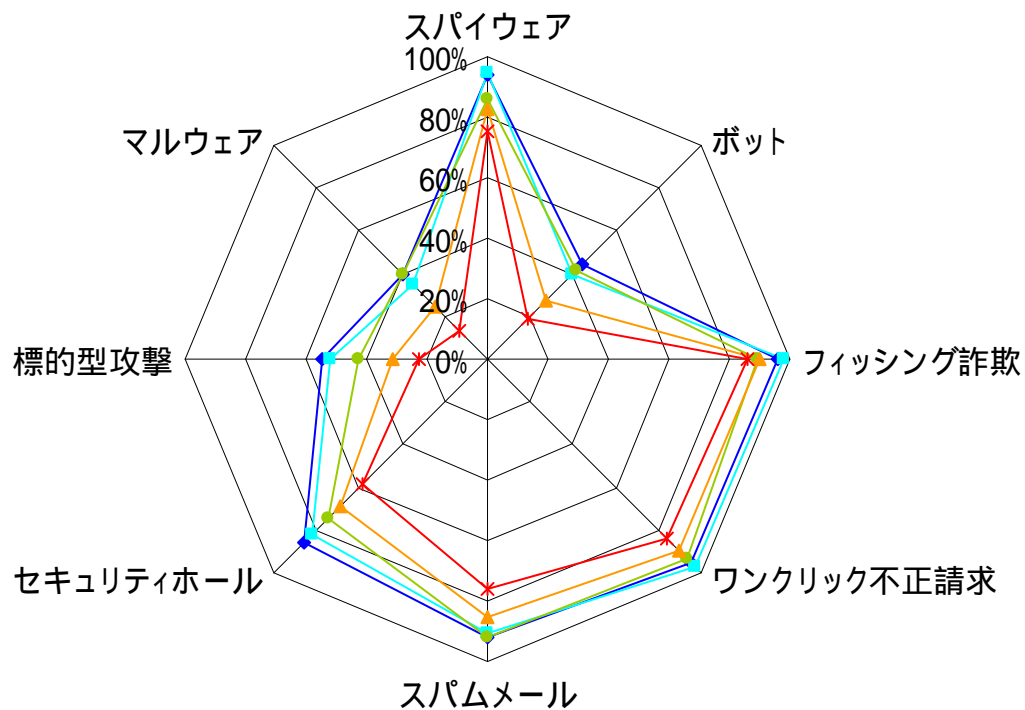
- 詳しい内容を知っている
- 概要をある程度知っている
- 名前を聞いたことがある程度
- 名前も、概要も知らない

- 詳しい内容を知っている
- 概要をある程度知っている
- 名前を聞いたことがある程度
- 名前も、概要も知らない

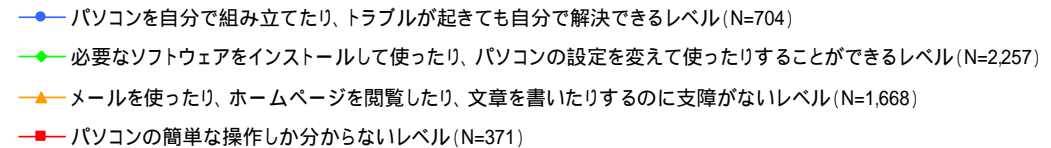
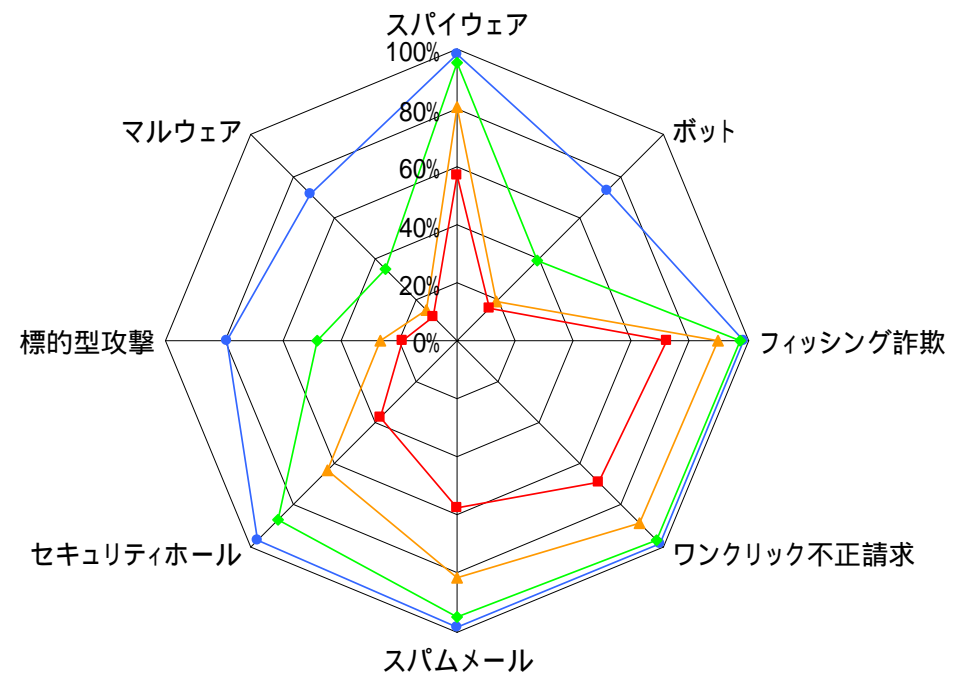
3.2.1 情報セキュリティに関する攻撃・脅威に対する認知状況(5)

- 情報セキュリティに関する攻撃・脅威を表す言葉の認知度を、職業別にみると、専業主婦やパート・アルバイトの認知度が相対的に低くなっている。
- パソコンの習熟度が高まると、情報セキュリティに関する攻撃・脅威に対する認知度も高まる傾向がみられる。

情報セキュリティに関する攻撃・脅威に対する認知度
[職業別]



情報セキュリティに関する攻撃・脅威に対する認知度
[パソコンの習熟度レベル別]

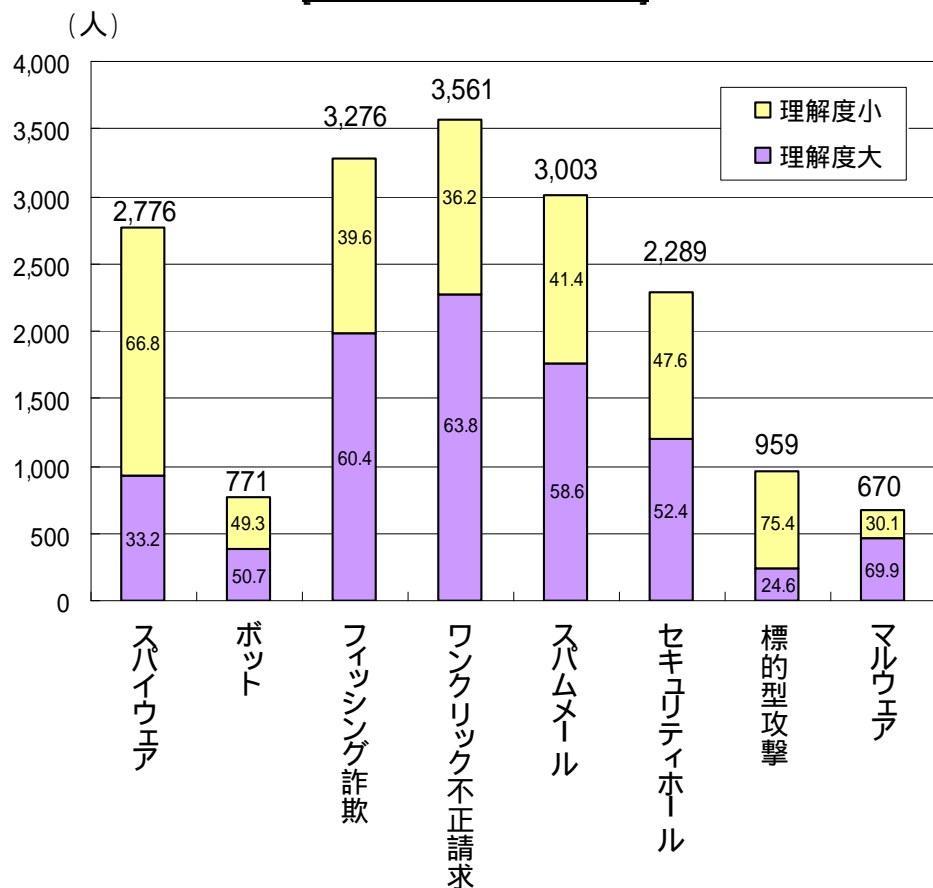


認知度は、「詳しい内容を知っている」、「概要をある程度知っている」、「名前を聞いたことがある程度である」それぞれの回答者の割合を足し合わせた値。

3.2.2 情報セキュリティに関する攻撃・脅威に対する理解状況(1)

- 「ワンクリック不正請求」や「フィッシング詐欺」、「スパムメール」については、概要や特徴について正しく理解しているユーザが多く、「理解度大」が「理解度小」の割合を大きく上回っている。
- 一方、「スパイウェア」については、「理解度大」が「理解度小」の割合を大きく下回っており、概要や特徴がユーザに正しく理解されていない状況が見受けられる。
- また、「ボット」や「標的型攻撃」、「マルウェア」については、他の攻撃・脅威に比べて、ユーザの理解が十分ではない。

情報セキュリティに関する攻撃・脅威に対する理解度
[理解している回答者数]



棒グラフ中の数字は、「理解度大」と「理解度小」の回答者の構成割合を表す。単位は%。

理解度について

本アンケートでは、情報セキュリティに関する攻撃・脅威に関して、攻撃・脅威の定義や手口、発生傾向、被害特性、有効な対策等について十分考慮しつつ、理解度を把握するための設問を5問設定している。

設問例)スパイウェア

スパイウェアについての概要や特徴に関する説明のうち、あなたが正しいと思われるものをすべてお知らせください。(いくつでも)

1. 利用者の個人情報等を収集し、外部に送信するプログラムのことを指します
2. ネットカフェなどのパソコンに仕掛けられていて、他の利用者の記録を盗むタイプがあります
3. コンピュータウイルスと同様、コンピュータ内や接続されているネットワーク内で自己増殖するタイプがあります
4. ポップアップ画面や確認メッセージにおいて、不審なメッセージが表示されたら、クリックせずに、ブラウザごと閉じることが大切です
5. セキュリティ対策ソフトをパソコンにインストールしていれば、スパイウェアの侵入を防ぐのに有効です

5問中、正解が4問以上の場合を「理解度大」、3問以下の場合を「理解度小」と定義するものとする。

3.2.2 情報セキュリティに関する攻撃・脅威に対する理解状況(2)

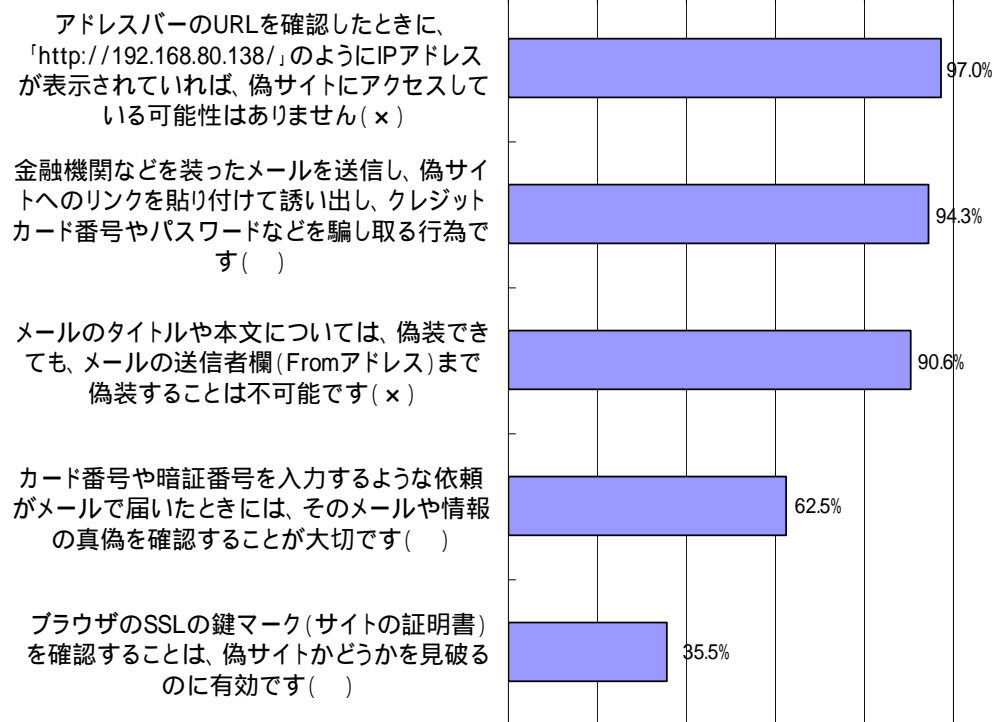
- 「フィッシング詐欺」、「ワンクリック不正請求」については、いずれも用語の定義に関する正答率はそれぞれ94.3%、94.1%と高かった。
- 一方、「フィッシング詐欺」への被害予防策についてみると、フィッシングメールで届いたときのメールや情報の真偽を確認することの重要性や、偽サイトかどうかを見破るために、ブラウザのSSLの鍵マーク(サイトの証明書)を確認することの重要性への理解が不十分であり、正答率はそれぞれ62.5%、35.5%にとどまっている。
- また、「ワンクリック不正請求」への被害予防策においても、信頼できないサイトにアクセスし、セキュリティの警告画面が表示されたときに、決して「実行」をクリックすることなく、「キャンセル」をクリックして先に進まないようにすることの重要性が十分理解されていないのが現状である。

情報セキュリティに関する攻撃・脅威に対する理解度(各設問の正答率)

< フィッシング詐欺 >

(N=3,276)

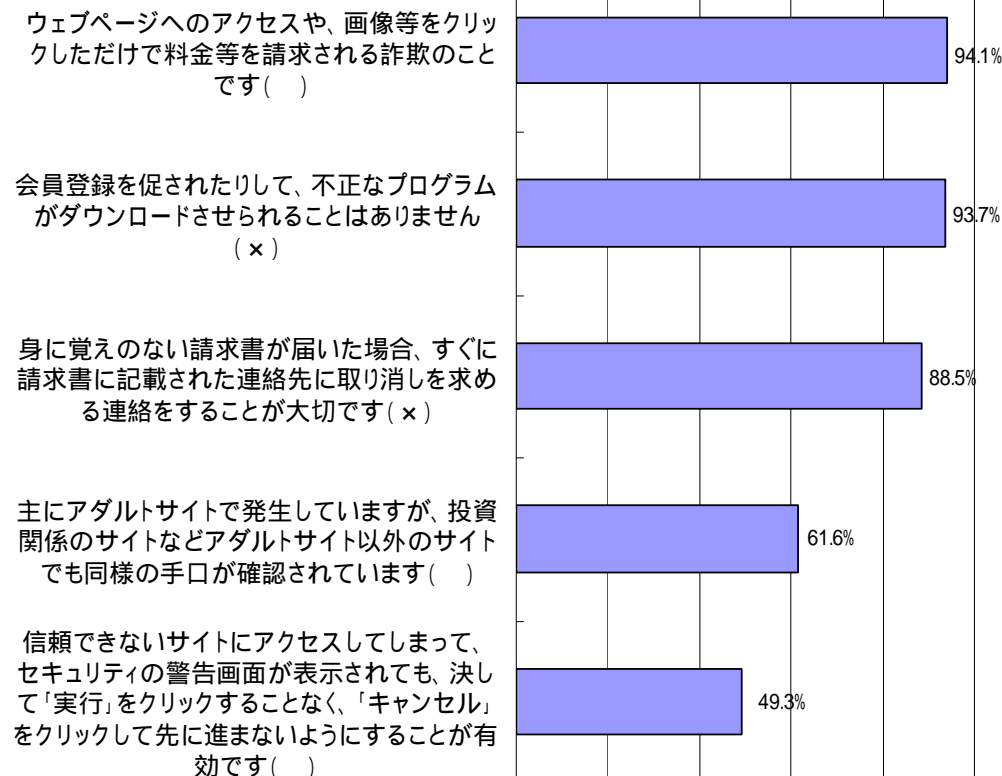
「理解度大」60.4% 「理解度小」39.6%



< ワンクリック不正請求 >

(N=3,561)

「理解度大」63.8% 「理解度小」36.2%



母数(N数)については、それぞれの情報セキュリティに関する攻撃・脅威について、「詳しい内容を知っている」あるいは「概要をある程度知っている」と回答した者を対象としている。「理解度大」、「理解度小」は、それぞれの情報セキュリティに関する攻撃・脅威について、「詳しい内容を知っている」あるいは「概要をある程度知っている」と回答した者を母数にしたときの割合である。

3.2.2 情報セキュリティに関する攻撃・脅威に対する理解状況(3)

- 「スパイウェア」、「スパムメール」については、いずれも用語の定義に関する正答率はそれぞれ83.6%、84.5%と高かった。
- 一方、「スパイウェア」への被害予防策についてみると、スパイウェアの侵入を防ぐために、セキュリティ対策ソフトをパソコンにインストールすることの重要性や、ポップアップ画面や確認メッセージで不審なメッセージが表示されたときに、クリックせずに、ブラウザを閉じることの重要性への理解が不十分であり、正答率はそれぞれ54.4%、43.5%にとどまっている。
- また、「スパムメール」への被害予防策においても、プロバイダの中に、スパムメールの送受信を防止したり、スパムメールをフィルタリングするサービスを提供している事業者があることが十分理解されておらず、正答率は64.9%と相対的に低い結果となっている。

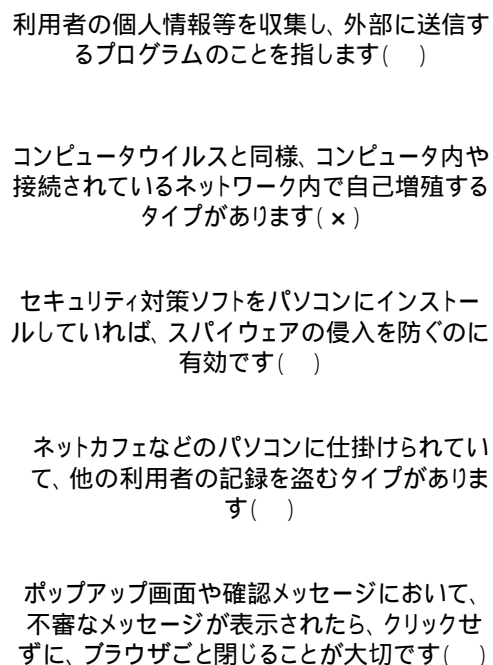
情報セキュリティに関する攻撃・脅威に対する理解度(各設問の正答率)

< スパイウェア >

「理解度大」33.2% 「理解度小」66.8%

(N=2,776)

0% 20% 40% 60% 80% 100%

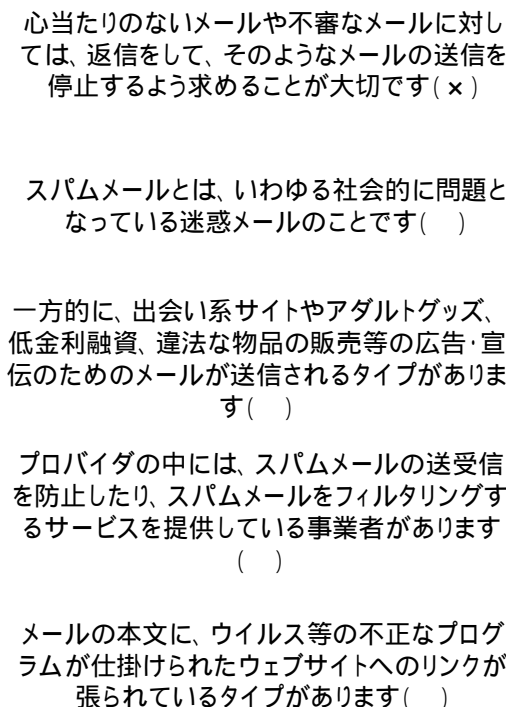


< スパムメール >

「理解度大」58.6% 「理解度小」41.4%

(N=3,003)

0% 20% 40% 60% 80% 100%



母数(N数)については、それぞれの情報セキュリティに関する攻撃・脅威について、「詳しい内容を知っている」あるいは「概要をある程度知っている」と回答した者を対象としている。「理解度大」、「理解度小」は、それぞれの情報セキュリティに関する攻撃・脅威について、「詳しい内容を知っている」あるいは「概要をある程度知っている」と回答した者を母数にしたときの割合である。

3.2.2 情報セキュリティに関する攻撃・脅威に対する理解状況(4)

- 「セキュリティホール(脆弱性)」への被害予防策において、セキュリティホール(脆弱性)を解消するために、Windows Updateなどを利用して常にパソコンを最新の状態にしておくことの重要性を理解しているユーザは、全体の68.1%にとどまっている。
- また、セキュリティホールが発見された場合に、ベンダー等から対策のための修正プログラムが無償で配布されることを理解しているユーザは46.4%であり、過半数を大きく下回っている。
- 一方、「標的型攻撃」への被害予防策として、多くの場合にセキュリティ対策ソフトで標的型攻撃を検知することができるものと誤解している。

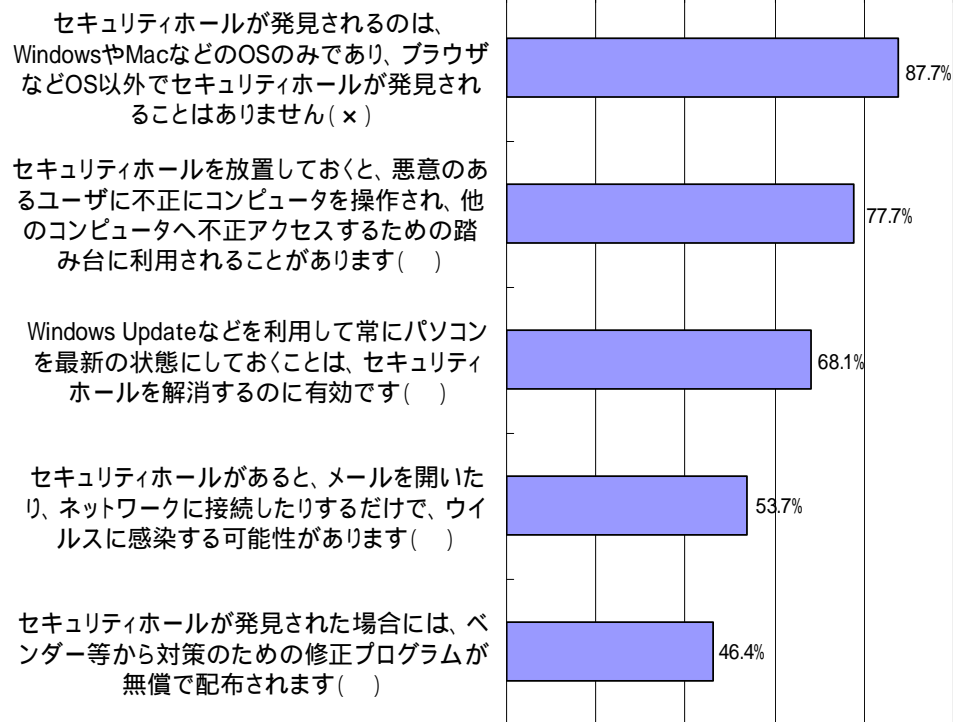
情報セキュリティに関する攻撃・脅威に対する理解度(各設問の正答率)

< セキュリティホール(脆弱性) >

「理解度大」52.4% 「理解度小」47.6%

(N=2,289)

0% 20% 40% 60% 80% 100%

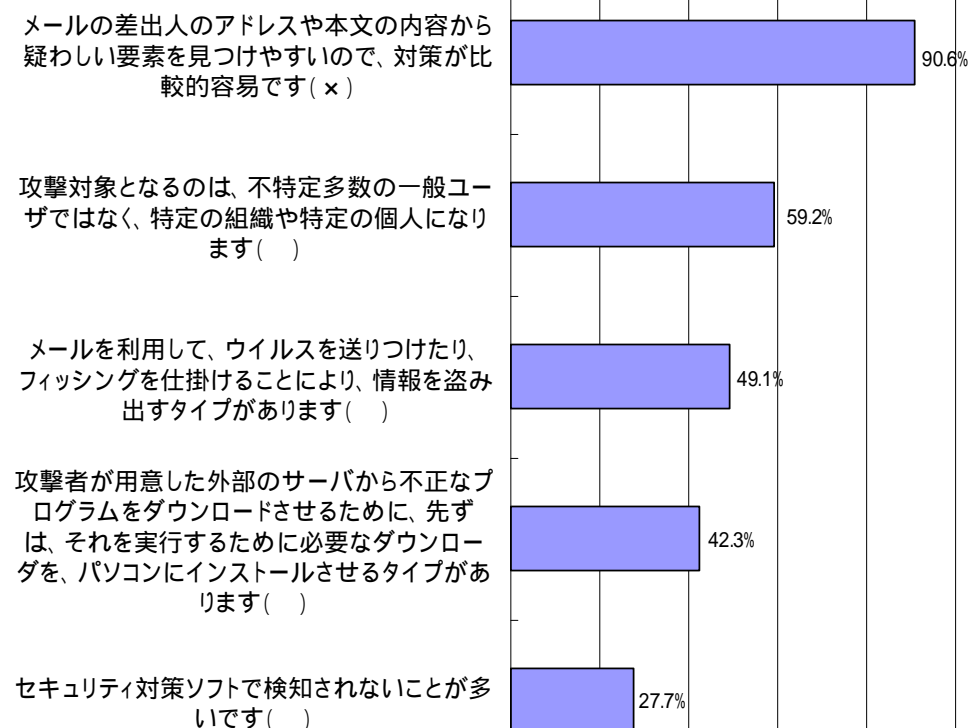


< 標的型攻撃 >

「理解度大」24.6% 「理解度小」75.4%

(N=959)

0% 20% 40% 60% 80% 100%



母数(N数)については、それぞれの情報セキュリティに関する攻撃・脅威について、「詳しい内容を知っている」あるいは「概要をある程度知っている」と回答した者を対象としている。「理解度大」、「理解度小」は、それぞれの情報セキュリティに関する攻撃・脅威について、「詳しい内容を知っている」あるいは「概要をある程度知っている」と回答した者を母数にしたときの割合である。

3.2.2 情報セキュリティに関する攻撃・脅威に対する理解状況(5)

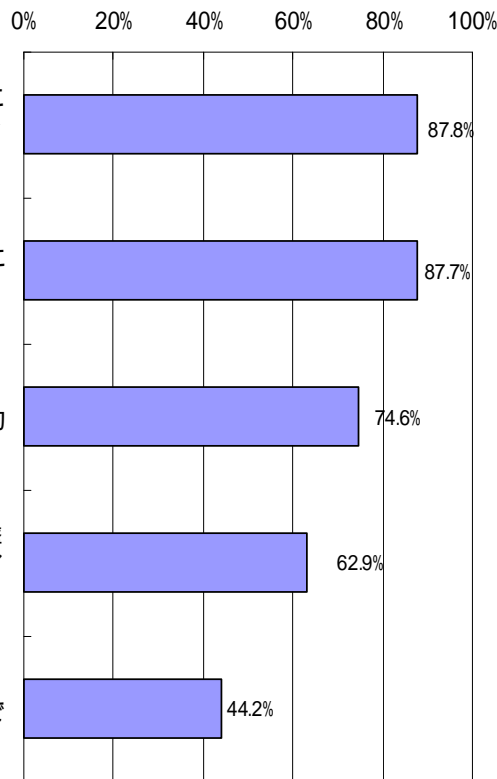
- 「ボット」、「マルウェア」については、いずれも用語の定義に関する正答率はそれぞれ74.6%、75.4%と比較的低かった。
- 一方、「ボット」への被害予防策についてみると、ボットの感染を防ぐために、セキュリティ対策ソフトをパソコンにインストールすることの重要性への理解が不十分であり、正答率は44.2%と半数を大きく下回っている。
- また、「マルウェア」については、マルウェアに、コンピュータウイルスやスパイウェア、ワーム等が含まれることが十分理解されていない。

情報セキュリティに関する攻撃・脅威に対する理解度(各設問の正答率)

<ボット>

「理解度大」50.7% 「理解度小」49.3%

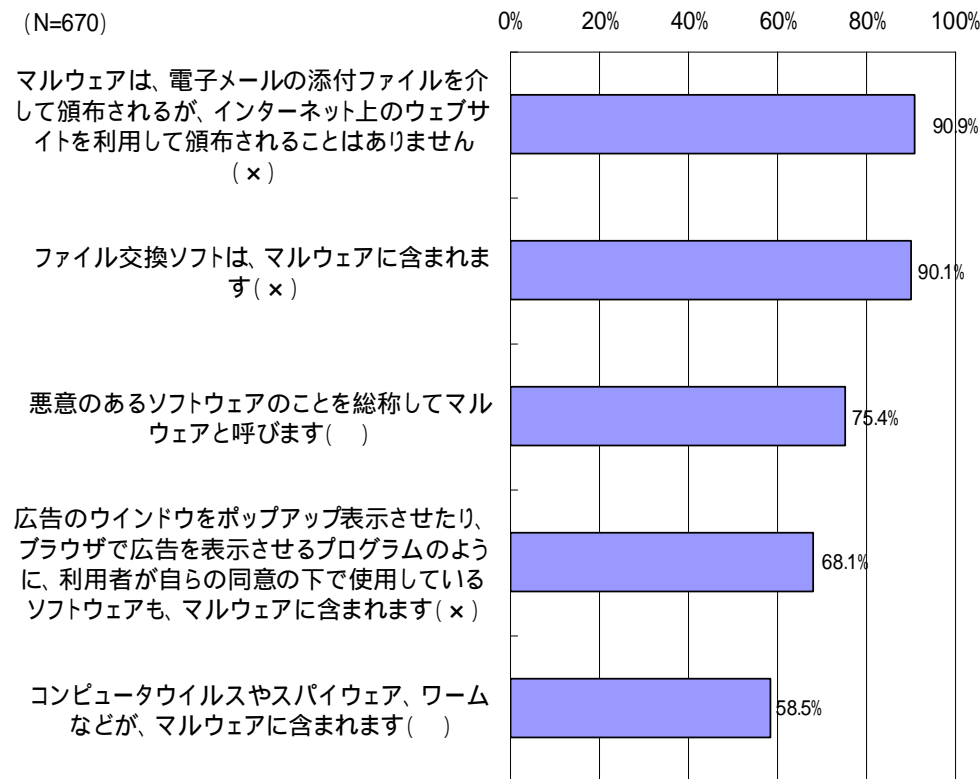
(N=771)



<マルウェア>

「理解度大」69.9% 「理解度小」30.1%

(N=670)



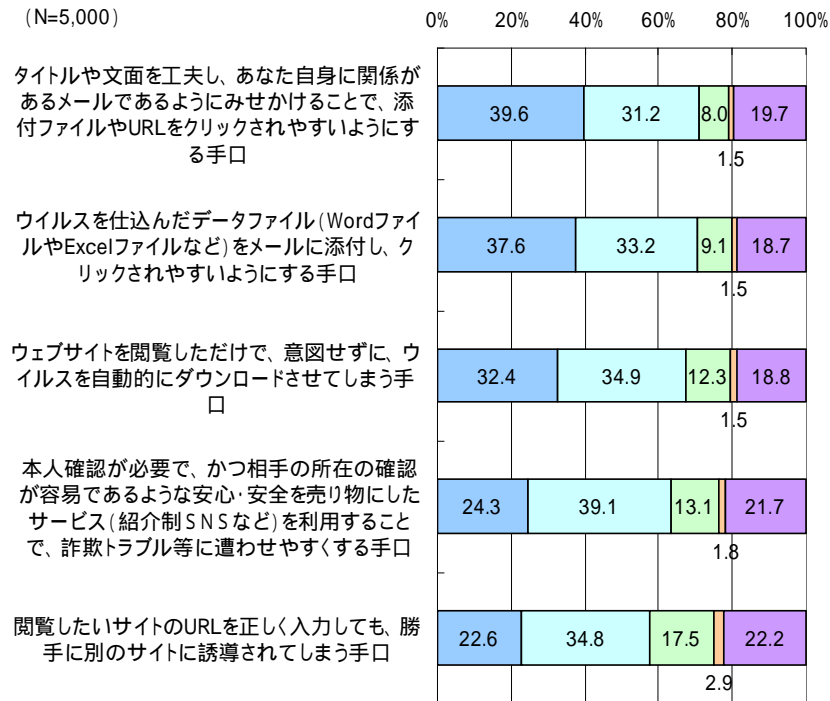
母数(N数)については、それぞれの情報セキュリティに関する攻撃・脅威について、「詳しい内容を知っている」あるいは「概要をある程度知っている」と回答した者を対象としている。「理解度大」、「理解度小」は、それぞれの情報セキュリティに関する攻撃・脅威について、「詳しい内容を知っている」あるいは「概要をある程度知っている」と回答した者を母数にしたときの割合である。

3.2.3 攻撃手口の実現性に対する感度(1)

- いずれの攻撃手口も既に実現されているものであるが、このような攻撃手口について「すでに実現されているのを知っている」と回答している感度の高いユーザはいずれも回答者全体の40%を満たない状況である。
- 回答者全体と関連サービスの利用者の攻撃手口への感度を比較すると、関連サービスの利用者は、一般ユーザである回答者全体に比べて攻撃手口への感度が高いことから、利用者は新たな攻撃手口によって被害に遭う危険性のある程度感じながら関連サービスを利用している傾向が見受けられる。
- それぞれの攻撃手口について比較すると、検索サイト・ポータルサイト利用者における「閲覧したいサイトのURLを正しく入力しても、勝手に別のサイトに誘導されてしまう手口」への感度が相対的に低く、利用者が検索サイト・ポータルサイトに対して、高い信頼を寄せている様相がうかがえる。

攻撃手口の実現性に対する感度
[回答者全体に占める割合]

攻撃手口の実現性に対する感度
[関連サービスの利用者に占める割合]



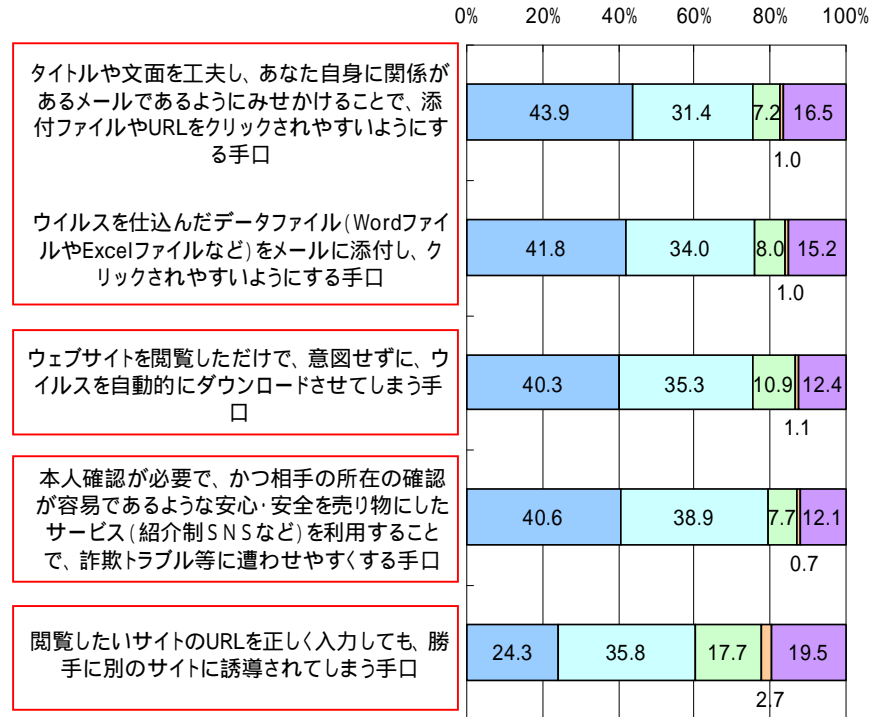
- すでに実現されているのを知っている
- 確信はないが、実現されていると思う
- 実現されていないが、今後実現される可能性があると思う
- 現在も、今後も実現される可能性はないと思う
- 分からない

電子メール利用者
(N=4,084)

個人のホームページ・ブログ閲覧者
(N=2,669)

SNS利用者
(N=1,107)

検索サイト・ポータルサイト利用者
(N=4,400)



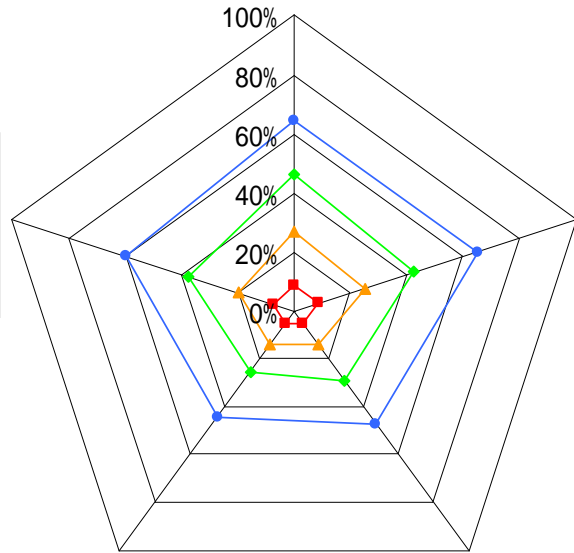
- すでに実現されているのを知っている
- 確信はないが、実現されていると思う
- 実現されていないが、今後実現される可能性があると思う
- 現在も、今後も実現される可能性はないと思う
- 分からない

3.2.3 攻撃手口の実現性に対する感度(2)

- パソコンの習熟度が高まると、様々な攻撃手口に対する感度も高まる傾向がみられる。詳細な数値を、33～34ページに示す。

攻撃手口の実現性に対する感度 [パソコンの習熟度レベル別]

タイトルや文面を工夫し、あなた自身に関係があるメールであるようにみせかけることで、添付ファイルやURLをクリックされやすいようにする手口



ウェブサイト閲覧しただけで、意図せず、ウイルスを自動的にダウンロードさせてしまう手口

ウイルスを仕込んだデータファイル (WordファイルやExcelファイルなど) をメールに添付し、クリックされやすいようにする手口

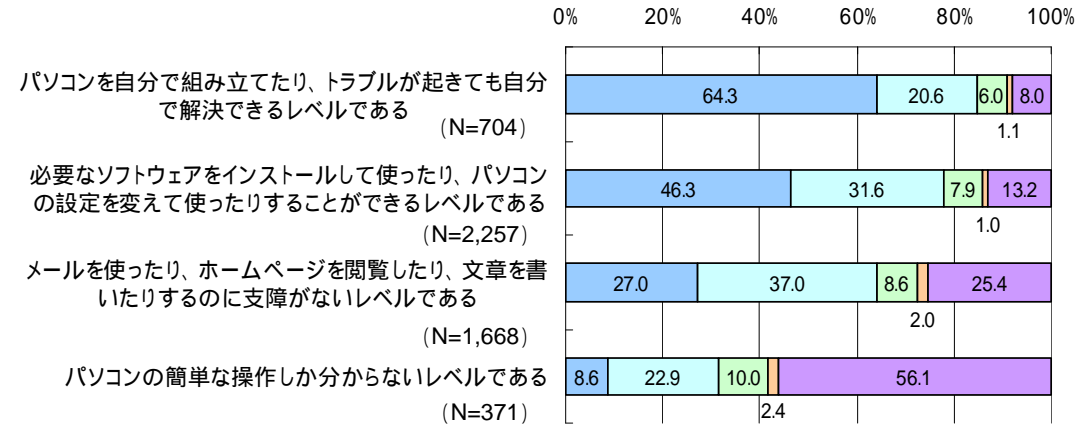
閲覧したいサイトのURLを正しく入力しても、勝手に別のサイトに誘導されてしまう手口

本人確認が必要で、かつ相手の所在の確認が容易であるような安心・安全を売り物にしたサービス (紹介制SNSなど) を利用することで、詐欺トラブル等に遭わせやすくする手口

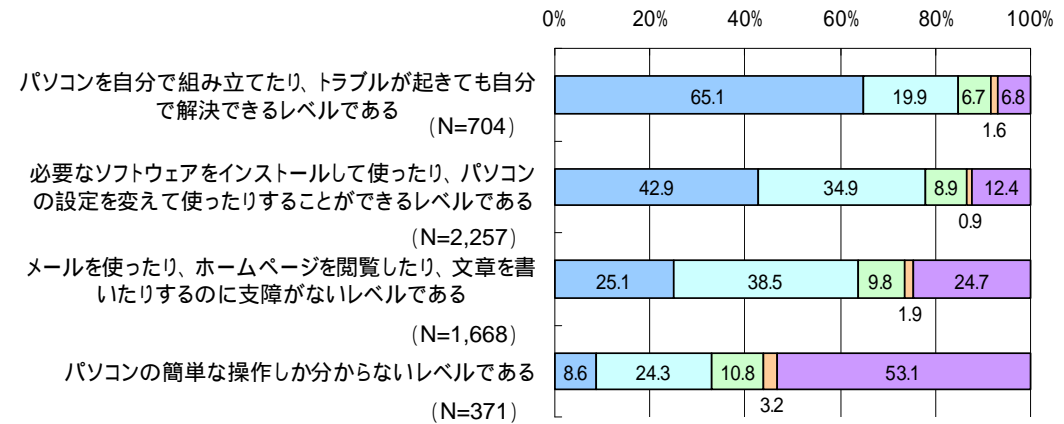
- パソコンを自分で組み立てたり、トラブルが起きても自分で解決できるレベル (N=704)
- 必要なソフトウェアをインストールして使ったり、パソコンの設定を変えて使ったりすることができるレベル (N=2,257)
- メールを使ったり、ホームページを閲覧したり、文章を書いたりするのに支障がないレベル (N=1,668)
- パソコンの簡単な操作しか分からないレベル (N=371)

感度は、「すでに実現されているのを知っている」と回答した者の割合。

タイトルや文面を工夫し、あなた自身に関係があるメールであるようにみせかけることで、添付ファイルやURLをクリックされやすいようにする手口



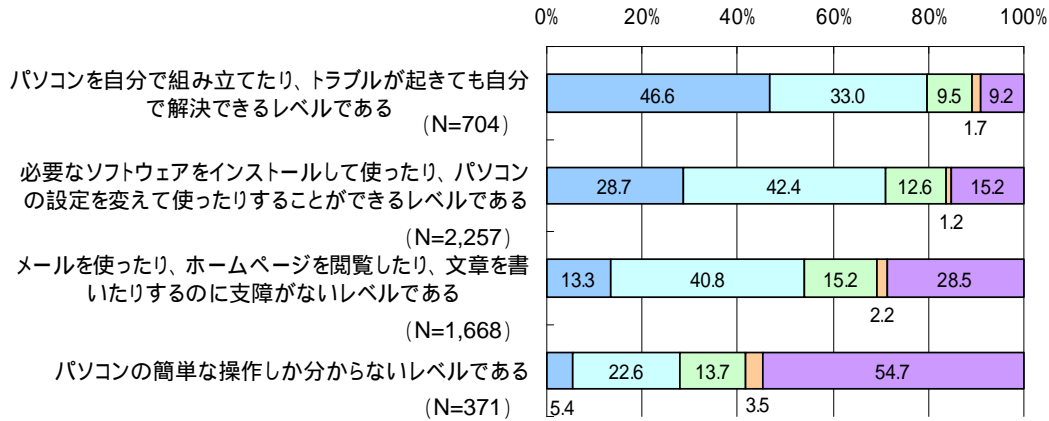
ウイルスを仕込んだデータファイル (WordファイルやExcelファイルなど) をメールに添付し、クリックされやすいようにする手口



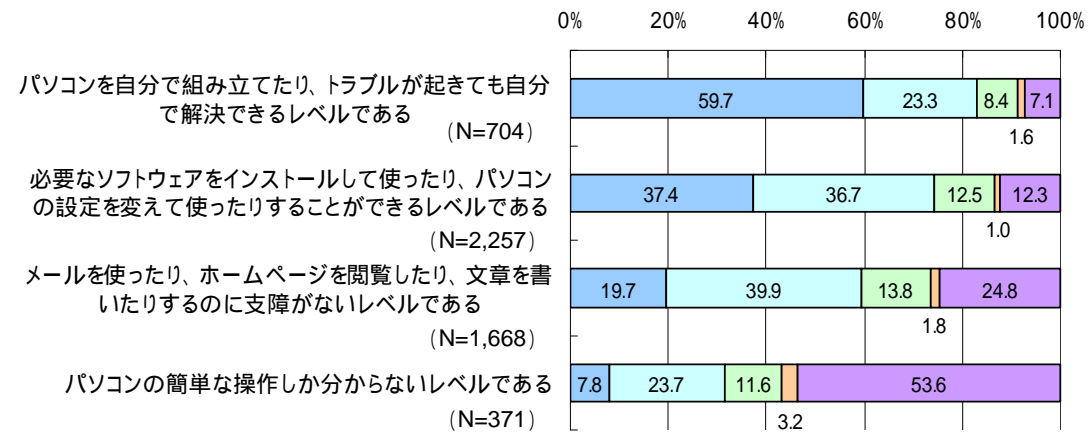
- すでに実現されているのを知っている
- 確信はないが、実現されていると思う
- 実現されていないが、今後実現される可能性があると思う
- 現在も、今後も実現される可能性はないと思う
- 分からない

3.2.3 攻撃手口の実現性に対する感度(3)

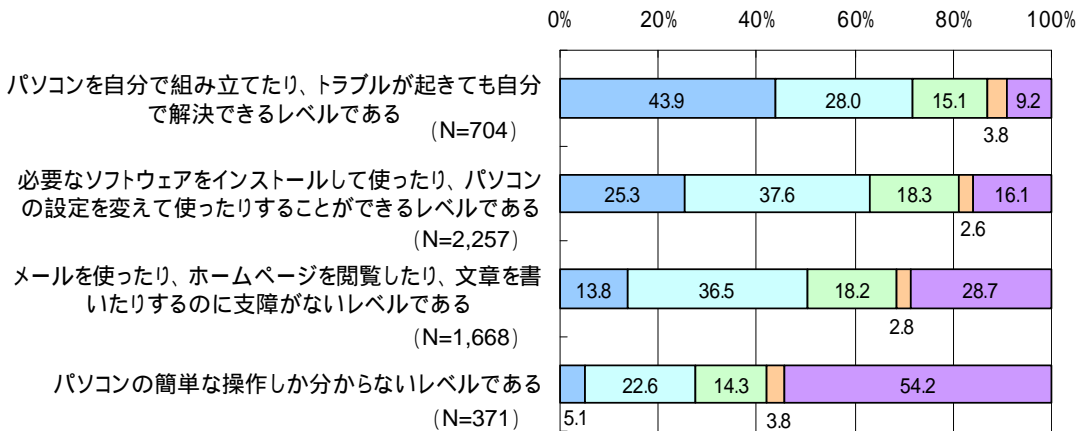
本人確認が必要で、かつ相手の所在の確認が容易であるような安心・安全を売り物にしたサービス(紹介制SNSなど)を利用することで、詐欺トラブル等に遭わせやすくする手口



ウェブサイトを閲覧しただけで、意図せずに、ウイルスを自動的にダウンロードさせてしまう手口



閲覧したいサイトのURLを正しく入力しても、勝手に別のサイトに誘導されてしまう手口



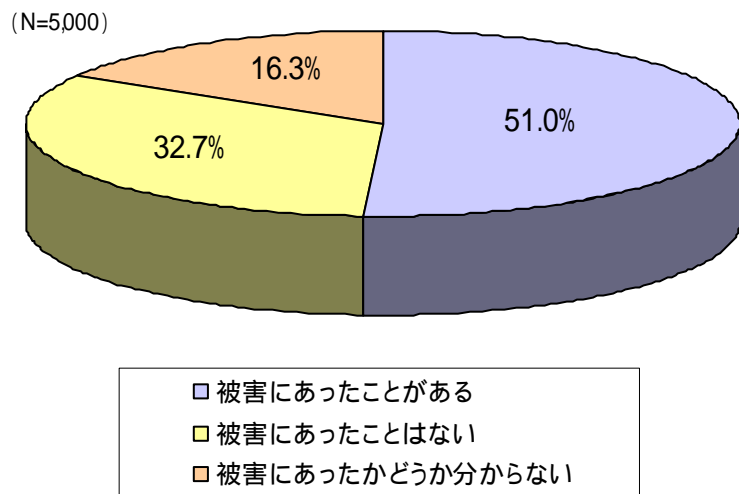
- すでに実現されているのを知っている
- 確信はないが、実現されていると思う
- 実現されていないが、今後実現される可能性があると思う
- 現在も、今後も実現される可能性はないと思う
- 分からない

3.3 情報セキュリティに関する脅威に対する被害状況

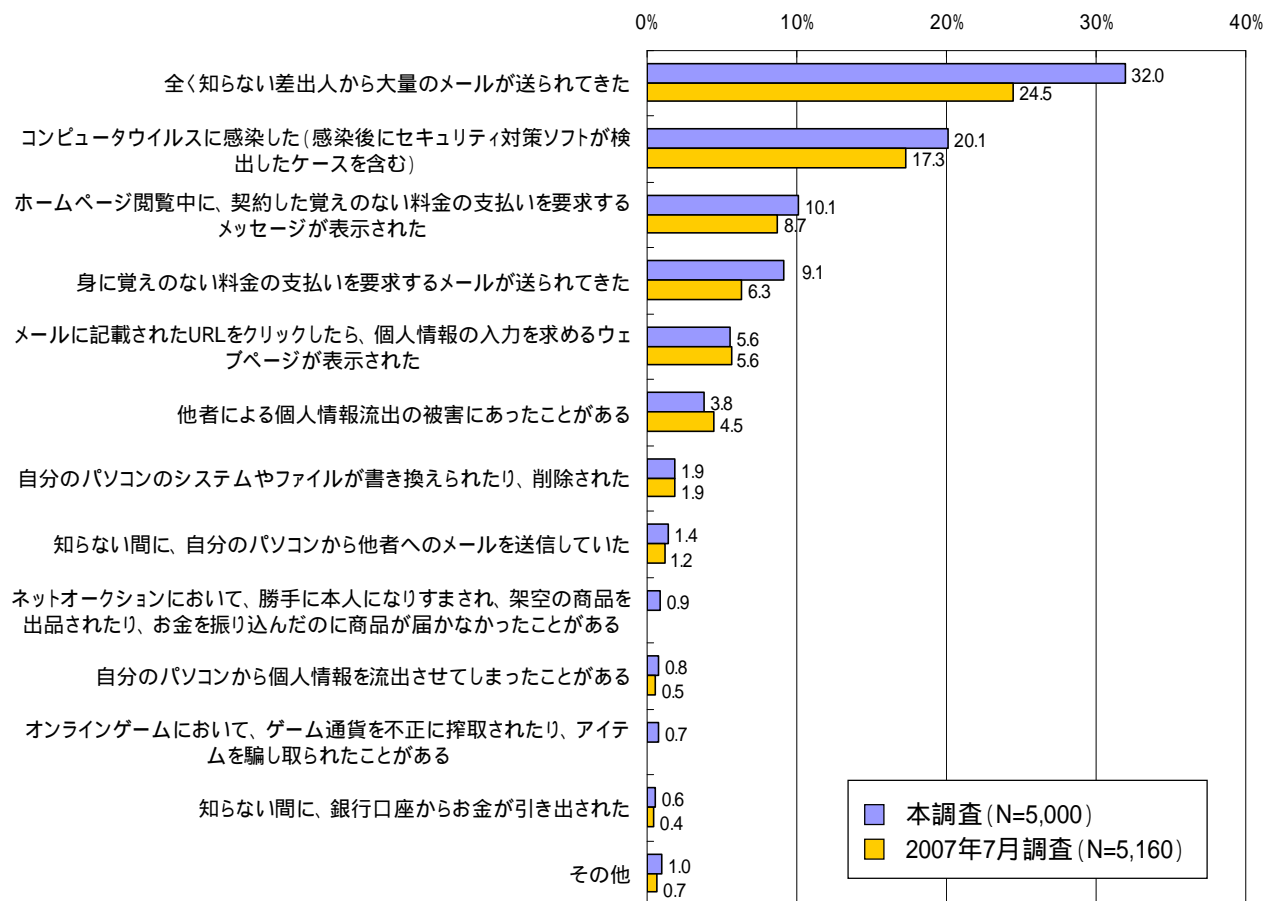
3.3.1 情報セキュリティに関する被害やトラブルの経験(1)

- 過去1年間に何らかの被害を経験したことがあるユーザは、全体の約半数に上っている。最も多いのは、「全く知らない差出人から大量のメールが送られてきた」で32.0%、次いで「コンピュータウイルスに感染した(20.1%)」、「ホームページ閲覧中に、契約した覚えのない料金の支払いを要求するメッセージが表示された(10.1%)」の順となっている。
- 本調査と2007年7月調査の結果を比較すると、「全く知らない差出人から大量のメールが送られてきた」や「コンピュータウイルスに感染した」、「ホームページ閲覧中に、契約した覚えのない料金の支払いを要求するメッセージが表示された」、「身に覚えのない料金の支払いを要求するメールが送られてきた」といった被害やトラブルに増加傾向がみられる。

情報セキュリティに関する被害やトラブルの遭遇経験の有無



情報セキュリティに関する被害やトラブルの遭遇状況
[2007年7月調査 / 本調査]

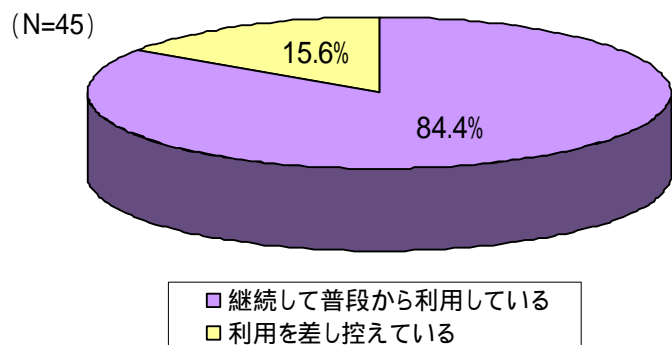


「ネットオークションにおいて、勝手に本人になりすまされ、架空の商品を出品されたり、お金を振り込んだのに商品が届かなかったことがある」、「オンラインゲームにおいて、ゲーム通貨を不正に搾取されたり、アイテムを騙し取られたことがある」については、本調査から新たに追加された選択肢であるため、2007年7月調査の結果は存在しない。

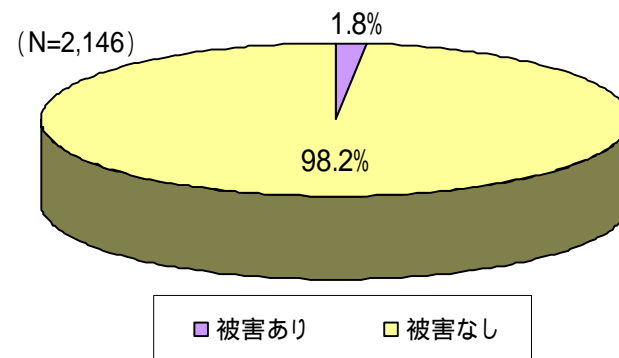
3.3.1 情報セキュリティに関する被害やトラブルの経験(2)

- 過去1年間にネットオークションに関する被害を経験したことがあるユーザの84.4%が、その後も継続して普段からよくネットオークションを利用している。
- 他方、オンラインゲームについては、過去1年間にオンラインゲームに関する被害を経験したことがあるユーザの62.2%が、その後利用を差し控えており、被害やトラブルがサービス離れに直結している様相がうかがえる。
- 利用を差し控えているユーザを除き、普段からよくネットオークションやオンラインゲームを利用しているユーザのうち、過去1年間にそれぞれのサービスに関する被害を経験したことがあるユーザは、1.8%、1.6%となっている。

ネットオークションに関する被害経験者のサービス利用の継続状況
[ネットオークションに関する被害経験者に占める割合]

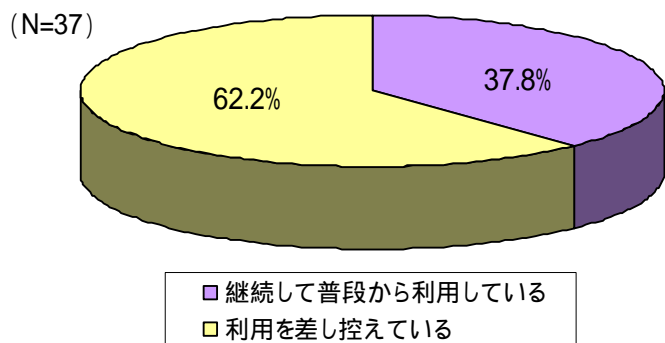


ネットオークションに関する被害やトラブルの遭遇経験の有無
[普段からよくネットオークションを利用しているユーザに占める割合]

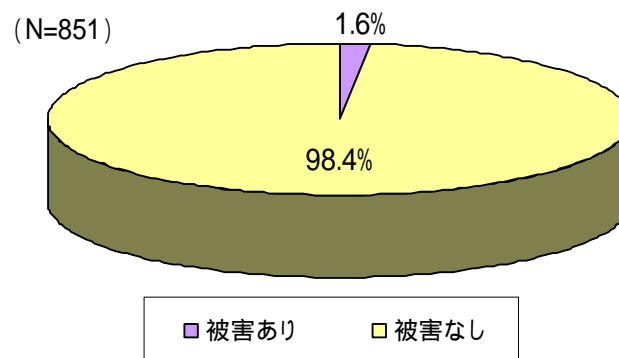


勝手に本人になりすまされ、架空の商品を出品される被害や、お金を振り込んだのに商品が届かない被害が対象

オンラインゲームに関する被害経験者のサービス利用の継続状況
[オンラインゲームに関する被害経験者に占める割合]



オンラインゲームに関する被害やトラブルの遭遇経験の有無
[普段からよくオンラインゲームを利用しているユーザに占める割合]

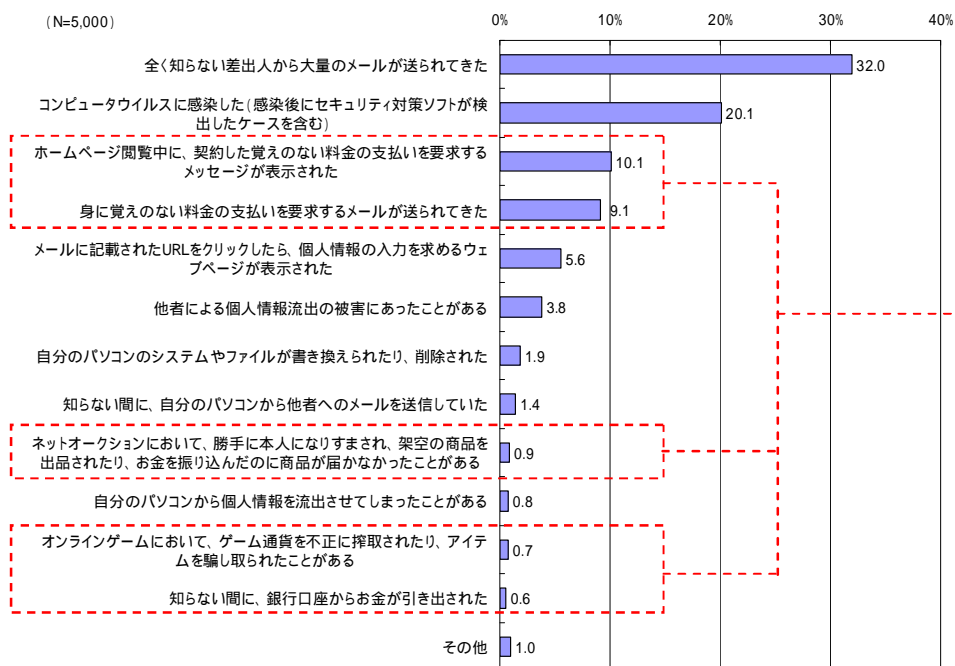


ゲーム通貨を不正に搾取される被害や、アイテムを騙し取られる被害が対象

3.3.1 情報セキュリティに関する被害やトラブルの経験(3)

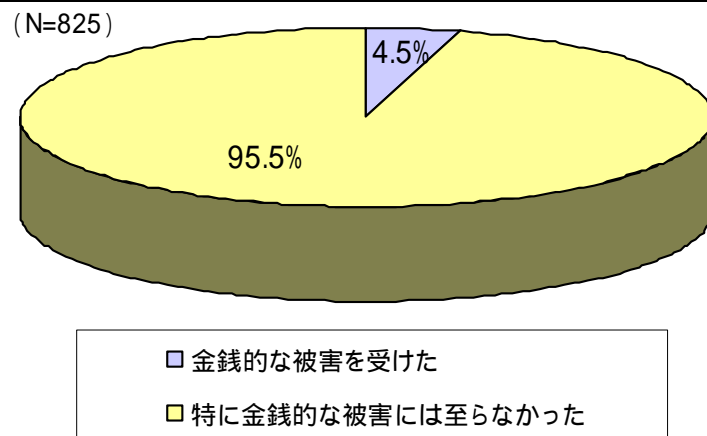
- 下記に示した金銭的な被害と関わりがある被害やトラブルを経験したユーザのうち、実際に金銭的な被害を被ったことがあるユーザは、4.5%に及んでいる。
- 1ユーザ当たりの被害金額は、「10,000円未満」、「10,000円以上50,000円未満」がともに35.1%と多く、平均被害金額は約42,000円、最大被害金額は500,000円となっている。

情報セキュリティに関する被害やトラブルの遭遇状況



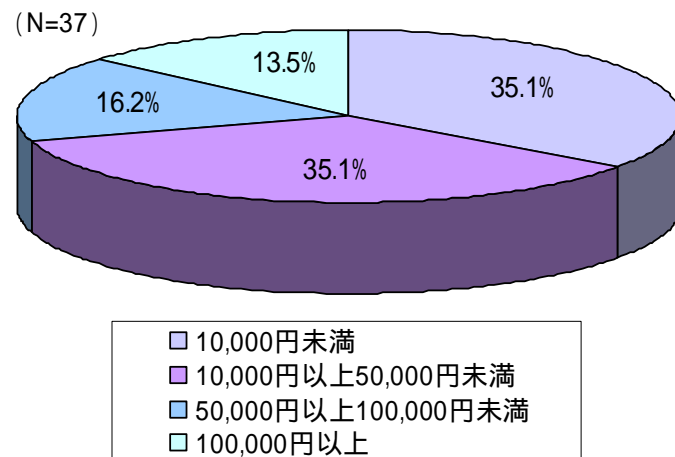
金銭的な被害と関わりがある被害やトラブル

情報セキュリティに関する被害やトラブルにおける金銭的被害の有無 [金銭的被害と関わりがある被害やトラブルに遭遇した経験がある者]



情報セキュリティに関する被害やトラブルにおける被害金額 [金銭的被害に遭遇した経験がある者]

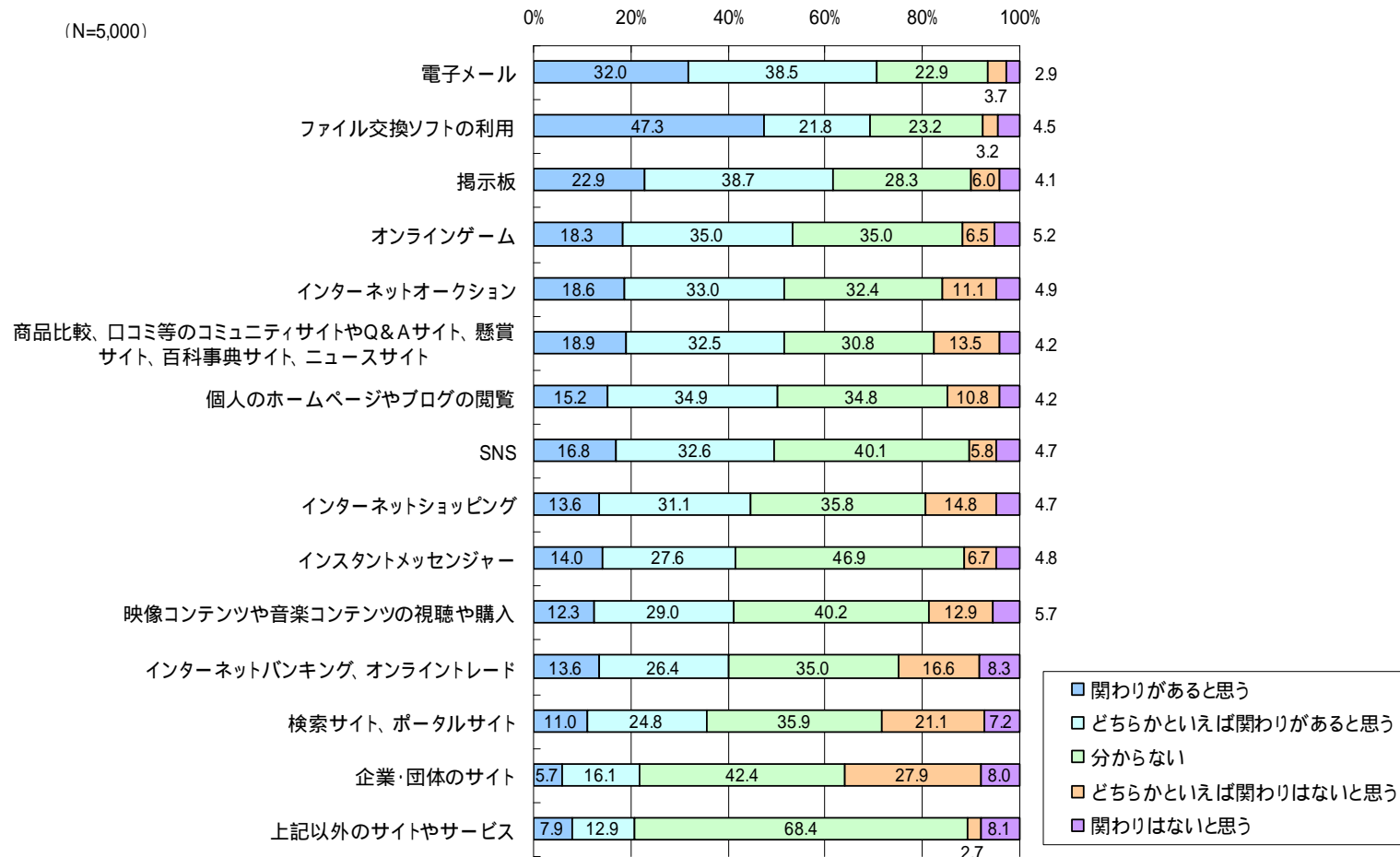
平均被害金額 約42,000円 最大被害金額 500,000円



3.3.2 情報セキュリティに関する被害やトラブルと関わりがあるサイト・サービス(1)

- ユーザが情報セキュリティに関する被害やトラブルと関わりがあると考えている(「関わりがあると思う」と「どちらかといえば関わりがあると思う」の割合を足し合わせたもの)サイト・サービスとしては、「電子メール」、「ファイル交換ソフトの利用」、「掲示板」、「オンラインゲーム」、「インターネットオークション」が上位を占める。
- 他方、ユーザが情報セキュリティに関する被害やトラブルと関わりがないと考えている(「関わりがないと思う」と「どちらかといえば関わりがないと思う」の割合を足し合わせたもの)サイト・サービスとしては、「企業・団体のサイト」、「検索サイト、ポータルサイト」、「インターネットバンキング、オンライントレード」、「映像コンテンツや音楽コンテンツの視聴や購入」、「インスタントメッセージ」が上位を占める。

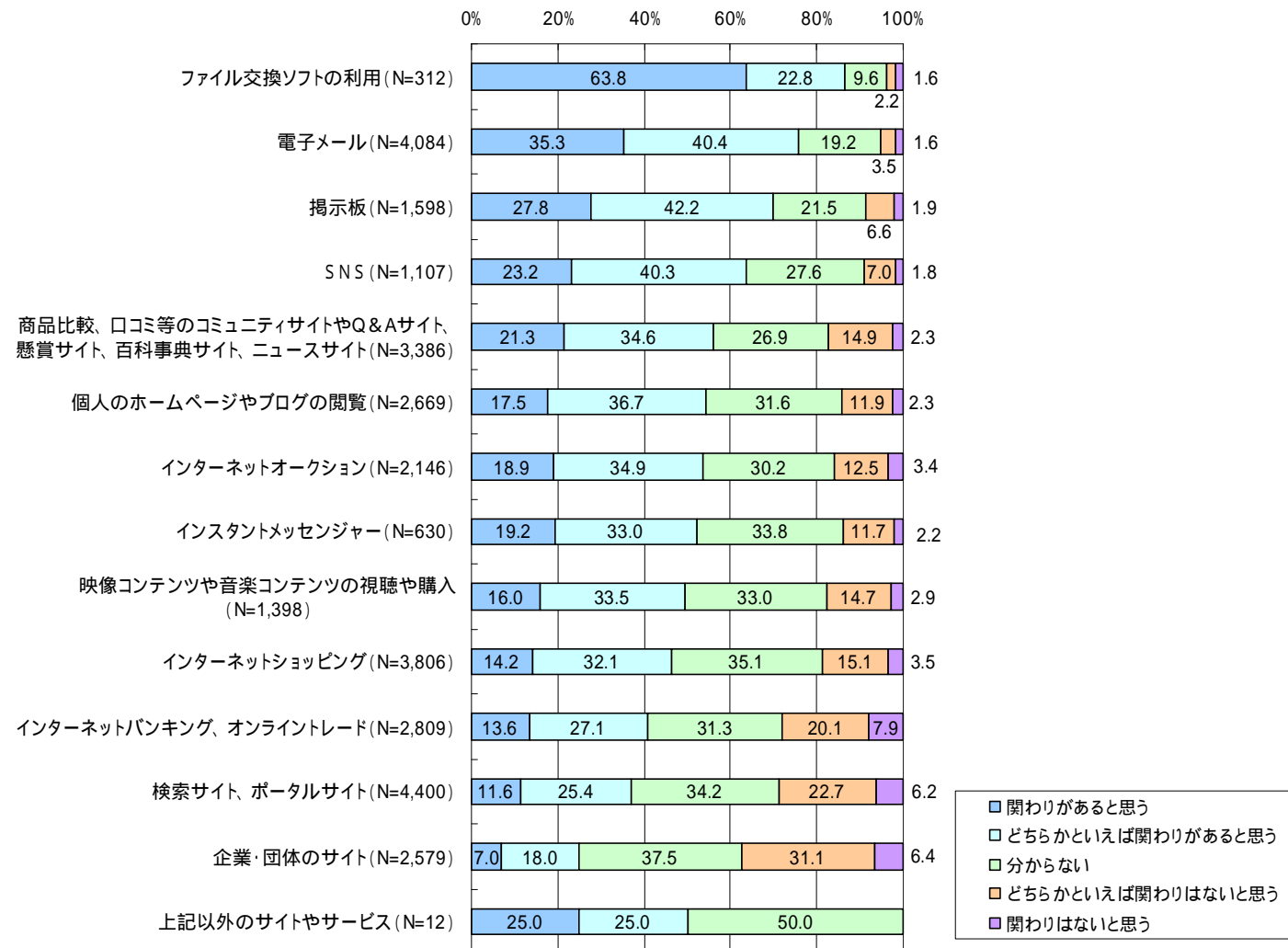
サイト・サービスと情報セキュリティに関する被害・トラブルとの関わり度合い
[回答者全体に占める割合]



3.3.2 情報セキュリティに関する被害やトラブルと関わりがあるサイト・サービス(2)

- インターネット上で提供されている各種サイト・サービスのユーザのうち、当該サイト・サービスが情報セキュリティに関する被害やトラブルと関わりがあると認識し、危ないと分かっているが利用しているユーザがどの程度の割合で存在するかについて分析を行った。
- 危ないと分かっているが利用しているユーザ(「関わりがあると思う」あるいは「どちらかといえば関わりがあると思う」と回答しているユーザ)の割合は、「ファイル交換ソフトの利用」が86.6%と最も高く、次いで、「電子メール(75.9%)」、「掲示板(70.0%)」、「SNS(63.5%)」の順となっている。

サイト・サービスと情報セキュリティに関する被害・トラブルとの関わり度合い
[当該サイト・サービスの利用者に占める割合]



3.3.2 情報セキュリティに関する被害やトラブルと関わりがあるサイト・サービス(3)

- 被害やトラブルとの関わりが高く、利用度合いが低い、右下に位置する「ファイル交換ソフトの利用」や「掲示板」、「オンラインゲーム」、「SNS」については、双方の度合いによる値がともに高い、右上に位置する「電子メール」と比べて、危険性を認知し、利用を差し控えているユーザも多く存在するものと推察される。

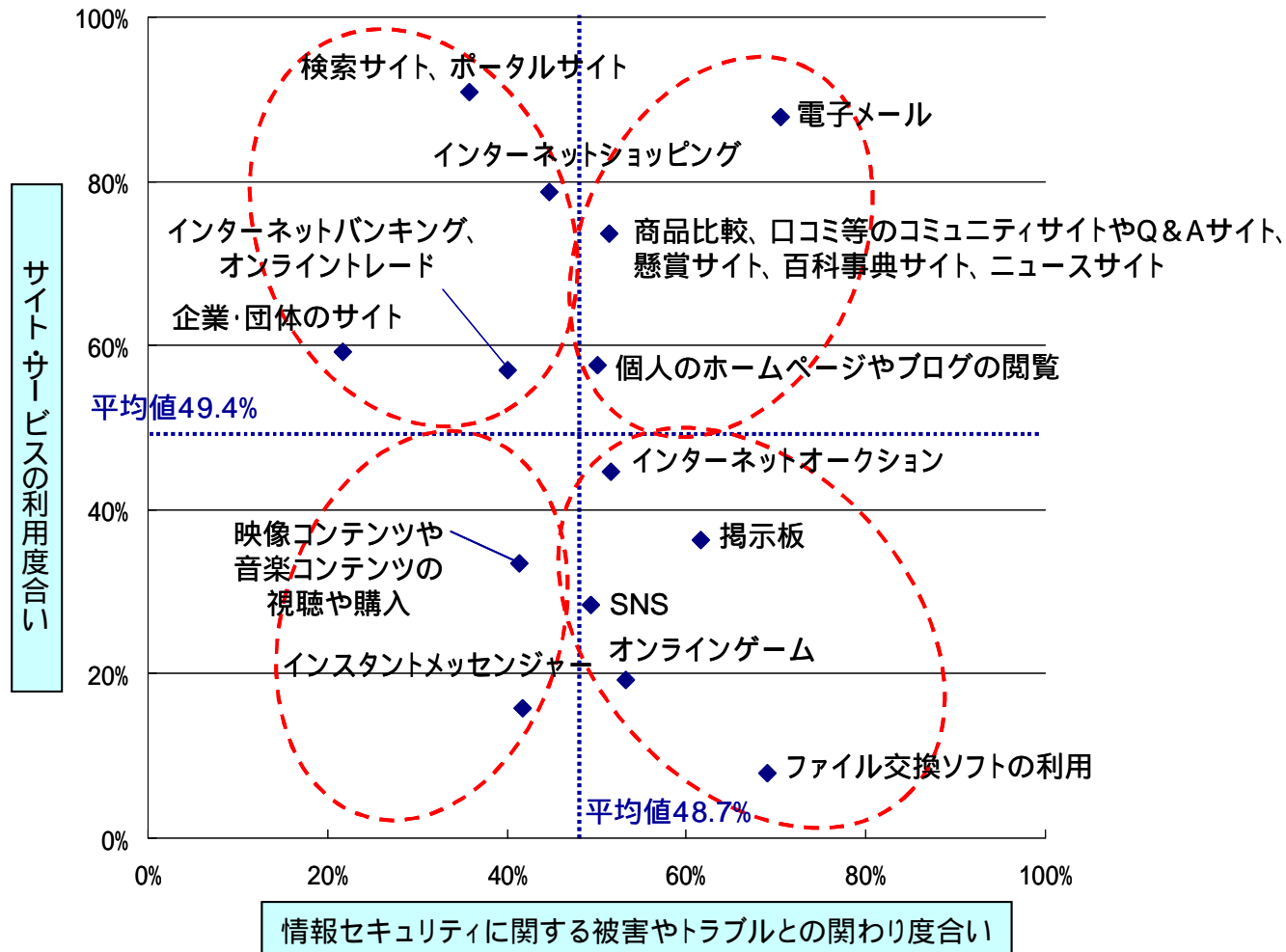
サイト・サービスの利用度合いと情報セキュリティに関する被害・トラブルとの関わり度合いとの関係

分析手法について

インターネット上のサイト・サービスにおいては、ひとたび情報セキュリティに関する被害やトラブルが発生すると、サイト・サービスの利用に重大な影響もたらされる可能性がある。本調査では、横軸に「情報セキュリティに関する被害やトラブルとの関わり度合い」、縦軸に「サイト・サービスの利用度合い」をとり、それぞれのサイト・サービスごとの値をプロットした散布図を作成する。

「情報セキュリティに関する被害やトラブルとの関わり度合い」は、情報セキュリティに関する被害やトラブルと関わりがあるかどうかについて、「関わりがあると思う」、「どちらかといえば関わりがあると思う」と回答した者の割合（回答者全体に占める割合）であり、当該サイト・サービスの危険性の認識度合いを表す。「サイト・サービスの利用度合い」は、現在、普段から利用している利用者の割合（上記の「関わりがあると思う」、「どちらかといえば関わりがあると思う」と回答した者に占める割合）である。

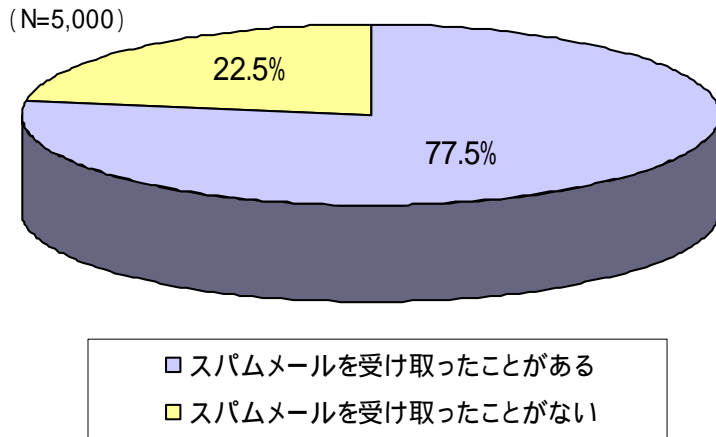
双方の度合いの関係から、当該サイト・サービスの危険性を認識し、利用を差し控えている利用者がどの程度の割合で存在するかを推量し分析するものとする。



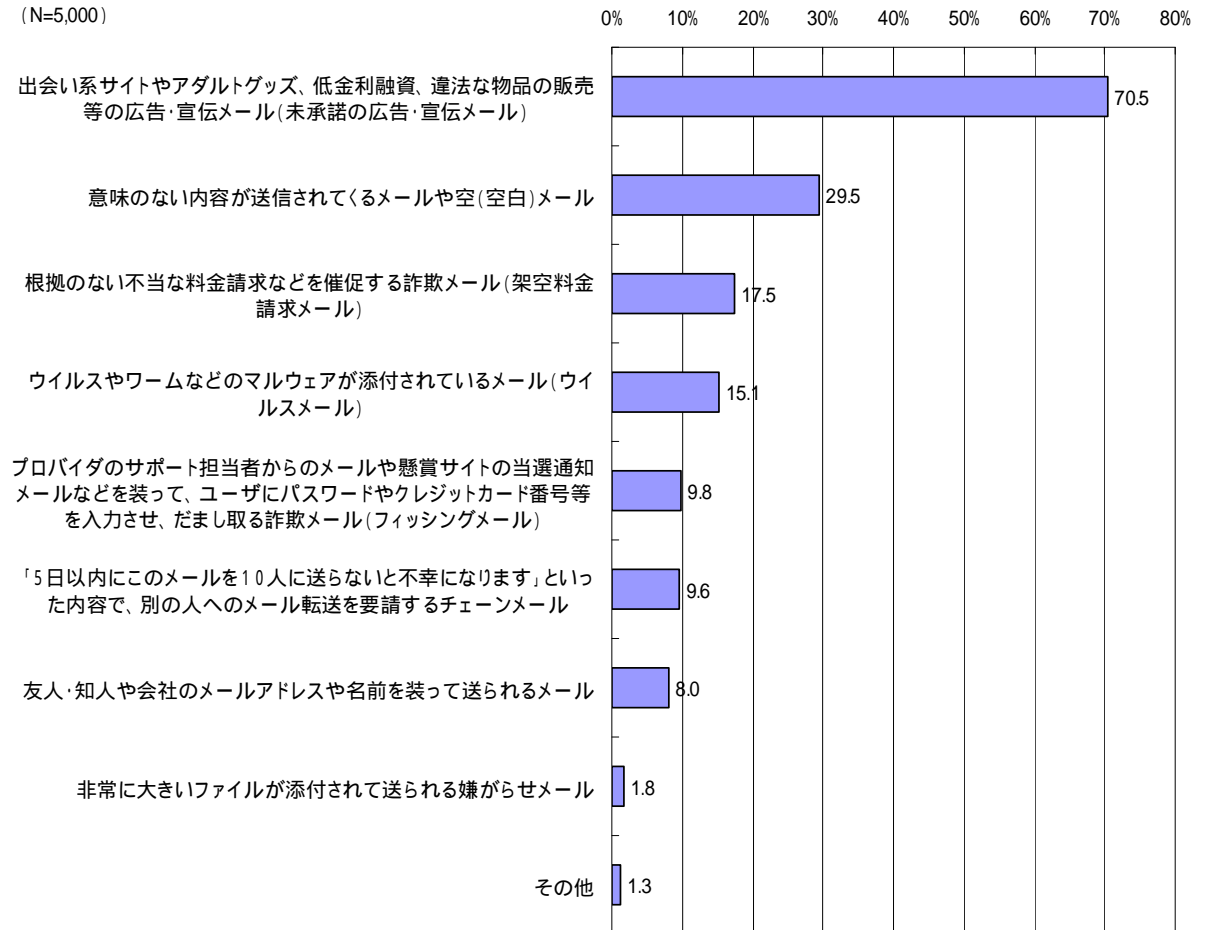
3.3.3 スпамメールの受信状況(1)

- 「上記のいずれも受け取ったことがない」を除く、スパムメールを受信したことがあるユーザは、全体の77.5%である。なかでも特に、「出会い系サイトやアダルトグッズ、低金利融資、違法な物品の販売等の広告・宣伝メール」や「意味のない内容が送信されてくるメールや空(空白)メール」は受信者の割合が相対的に高い。
- また、架空料金請求メール、ウイルスメール、フィッシングメールの受信者の割合は、それぞれ17.5%、15.1%、9.8%となっている。

スパムメールの受信経験の有無



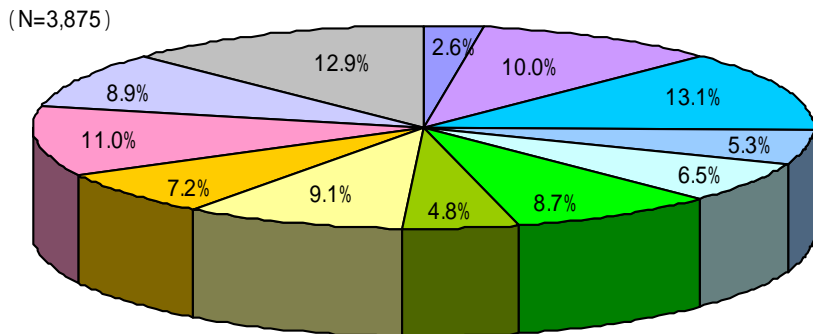
スパムメールの受信状況



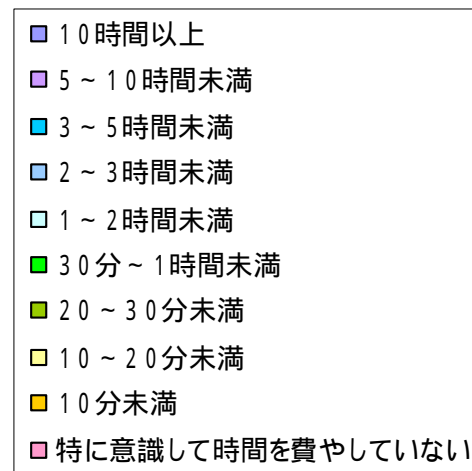
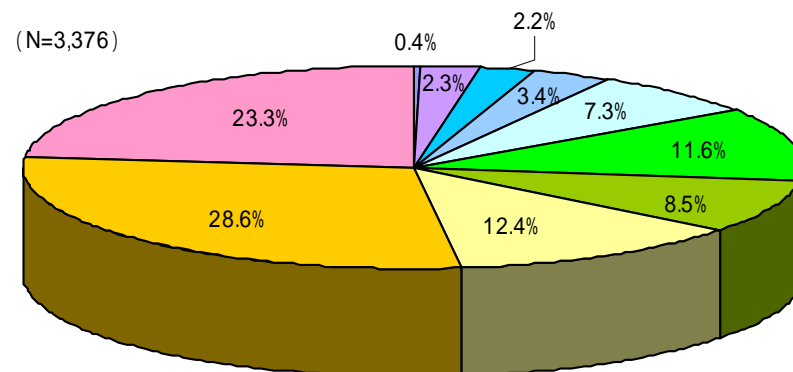
3.3.3 スпамメールの受信状況(2)

- スпамメール受信者におけるスパムメールの受信数についてみると、「毎日50～99通」が13.1%と最も高い。また、毎日100通以上スパムメールを受信しているユーザも全体の12.6%存在している。
- スпамメール受信者の15.6%が、1週間当たり1時間以上、スパムメールの受信相手や内容の確認、メール分類、ウイルスチェック、メール削除などのために時間を費やしており、過重な負担となっている。

スパムメールの受信数
[スパムメール受信者に占める割合]



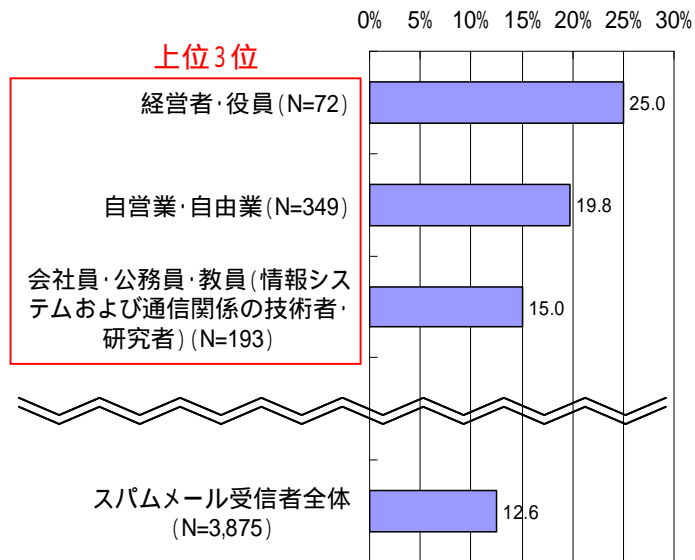
スパムメールの処理に係る時間(1週間当たり)
[スパムメール受信者(「ほとんどない」を除く)に占める割合]



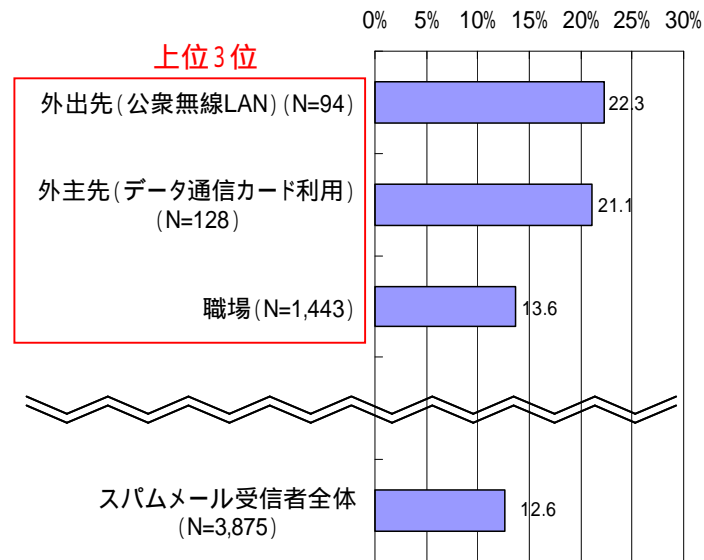
3.3.3 スпамメールの受信状況(3)

- 「経営者・役員」や「自営業・自由業」、「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)」を職業とするユーザ、「外出先(公衆無線LAN)」や「外出先(データ通信カード利用)」、「職場」をPCインターネットの利用場所とするユーザに、1日当たり100通以上のスパムメールを受信するユーザが多いという傾向がみられる。

スパムメールの受信数
1日当たり100通以上の受信者の割合
[職業別]



スパムメールの受信数
1日当たり100通以上の受信者の割合
[PCインターネットの利用場所別]

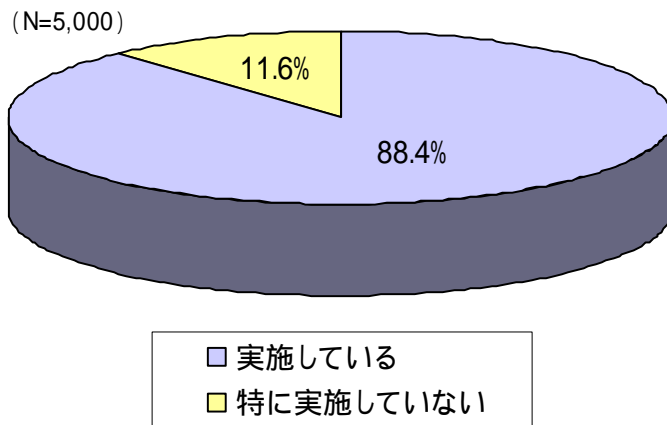


3.4 情報セキュリティに関する脅威に対する対策状況

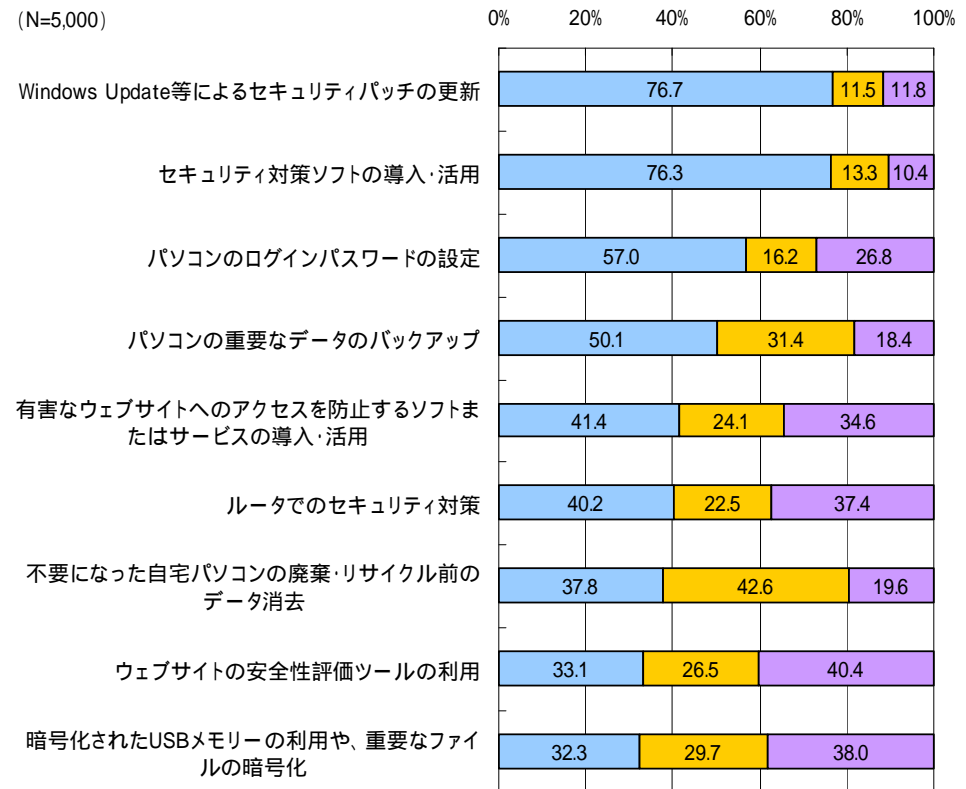
3.4.1 情報セキュリティ対策の実施状況(1)

- 情報セキュリティ対策を実施しているユーザは、全体の88.4%であり、残りの11.6%は対策を未着手である。
- 情報セキュリティ対策(技術的対策)として実施率の最も高いものは、「Windows Update等によるセキュリティパッチの更新」で76.7%となっている。次いで、「セキュリティ対策ソフトの導入・活用(76.3%)」、「パソコンのログインパスワードの設定(57.0%)」、「パソコンの重要なデータのバックアップ(50.1%)」の順となっている。
- 反対に、実施率の最も低いものは、「暗号化されたUSBメモリーの利用や、重要なファイルの暗号化」で32.3%となっている。次いで「ウェブサイトの安全性評価ツールの利用(33.1%)」、「不要になった自宅パソコンの廃棄・リサイクル前のデータ消去(37.8%)」、「ルーターでのセキュリティ対策(40.2%)」の順となっている。

情報セキュリティ対策の実施の有無



情報セキュリティ対策の実施の有無
[技術的対策別]

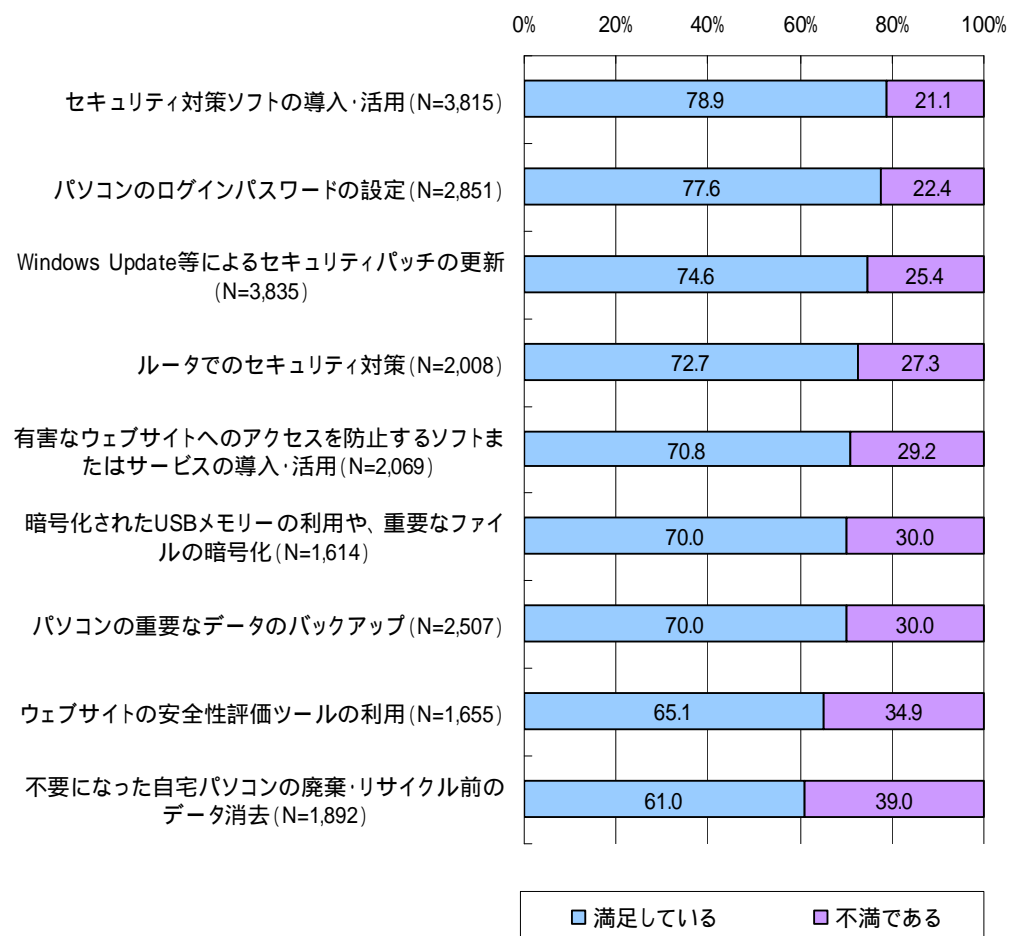


■ 実施している
■ 現在実施はしていないが、今後実施する予定である
■ 現在も、今後も実施する予定はない

3.4.1 情報セキュリティ対策の実施状況(2)

- 実施している情報セキュリティ対策(技術的対策)の満足度についてみると、満足度の高いものとして、「セキュリティ対策ソフトの導入・活用(78.9%)」や「パソコンのログインパスワードの設定(77.6%)」、「Windows Update等によるセキュリティパッチの更新(74.6%)」が挙げられる。
- 反対に、満足度が相対的に低いものとしては、「不要になった自宅パソコンの廃棄・リサイクル前のデータ消去(61.0%)」や「ウェブサイトの安全性評価ツールの利用(65.1%)」が挙げられる。

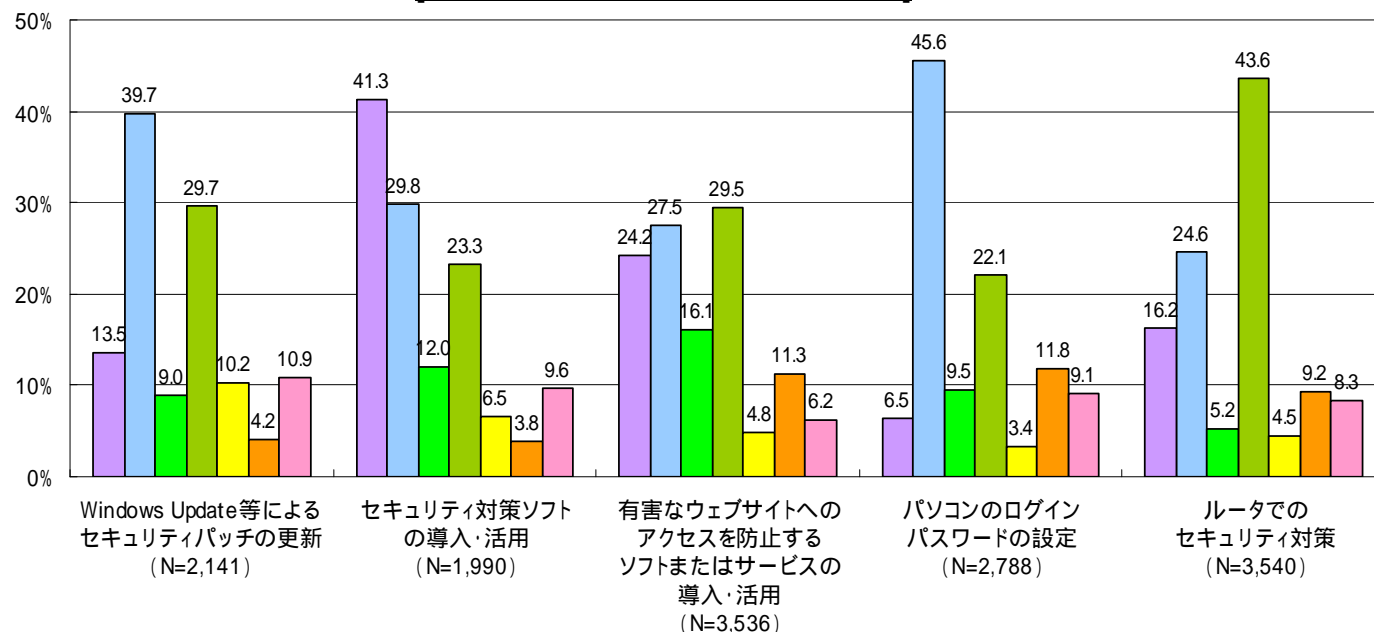
情報セキュリティ対策についての満足度
[個別の対策実施者に占める割合]



3.4.1 情報セキュリティ対策の実施状況(3)

- 「セキュリティ対策ソフトの導入・活用」は、実施上の問題点として金銭面を挙げるユーザが多く、41.3%を占めている。
- 手間や面倒臭さを、対策実施上の問題点として挙げるユーザが多いのは、「パソコンの重要なデータのバックアップ(53.3%)」や「パソコンのログインパスワードの設定(45.6%)」、「Windows Update等によるセキュリティパッチの更新(39.7%)」である。
- どのように対策を行えばよいか分かりにくい、あるいは分からないことを、対策実施上の問題点として挙げるユーザが多いのは、「ルータでのセキュリティ対策(43.6%)」や「ウェブサイトの安全性評価ツールの利用(41.6%)」である。
- 「有害なウェブサイトへのアクセスを防止するソフトまたはサービスの導入・活用」を行っているユーザのうち、16.1%が対策を行うと、サイトやサービスの利用の利便性が損なわれると考えている。

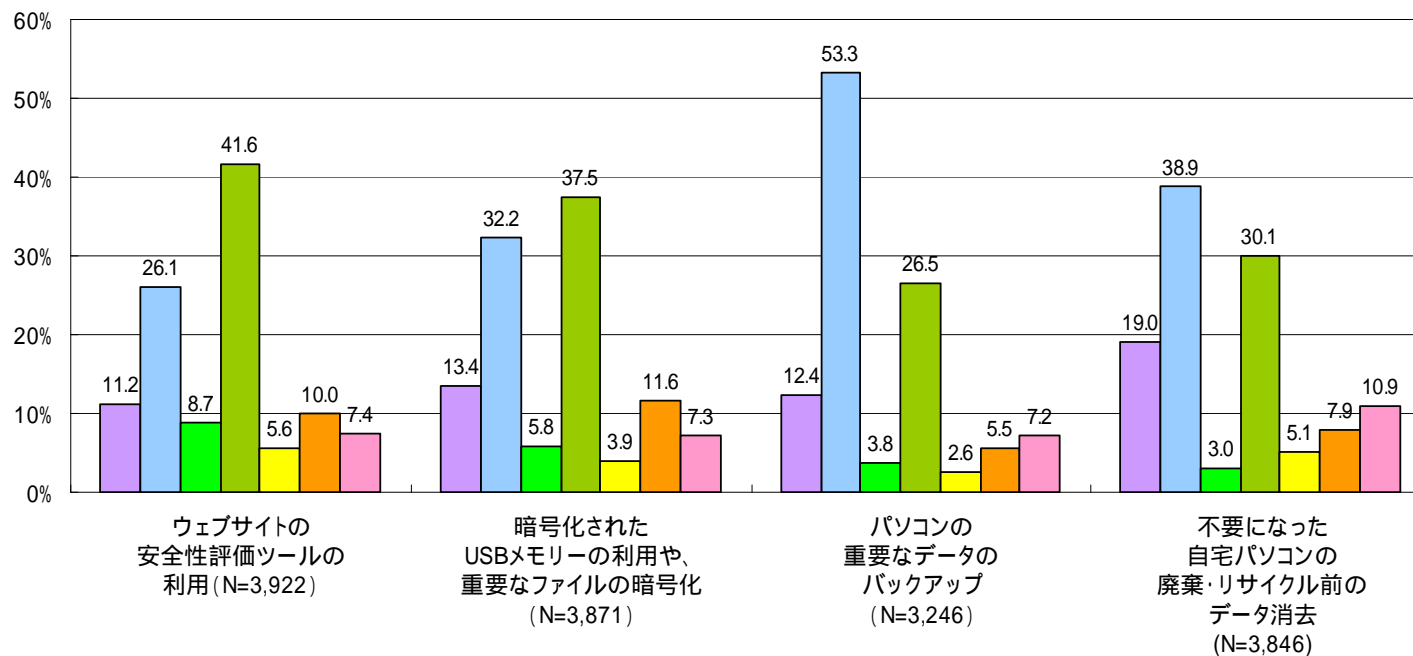
情報セキュリティ対策の実施上の問題点
[個別の対策実施者に占める割合]



- お金がかかる
- 手間がかかり、面倒である
- 対策を行うと、サイトやサービスの利用の利便性が損なわれる
- どのように行えばよいか分かりにくい、あるいは分からない
- 製品の製造・販売者から十分なサポートが得られない、あるいは得られるかどうか不安である
- 対策の必要性がない(該当するサービスを利用していない、他の対策で十分カバーできるなど)
- その他

3.4.1 情報セキュリティ対策の実施状況(4)

情報セキュリティ対策の実施上の問題点
[個別の対策実施者に占める割合]

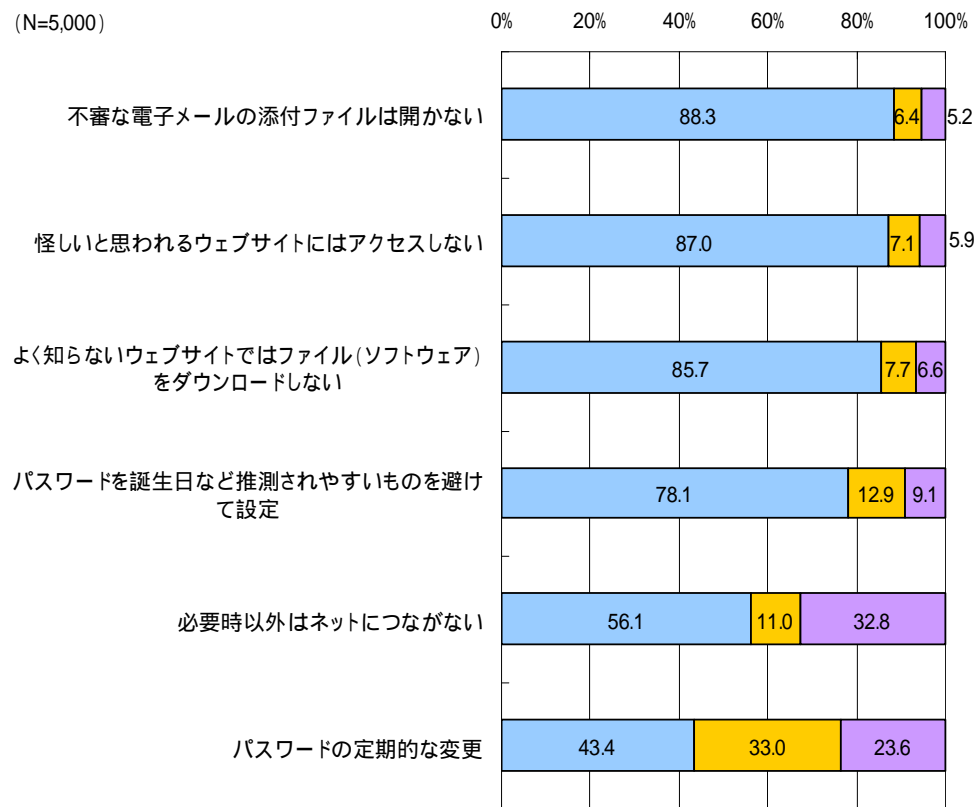


- お金がかかる
- 手間がかかり、面倒である
- 対策を行うと、サイトやサービスの利用の利便性が損なわれる
- どのように行えばよいか分かりにくい、あるいは分からない
- 製品の製造・販売者から十分なサポートが得られない、あるいは得られるかどうか不安である
- 対策の必要性がない(該当するサービスを利用していない、他の対策で十分カバーできるなど)
- その他

3.4.1 情報セキュリティ対策の実施状況(5)

- 情報セキュリティ対策(セキュリティに関する注意・安全行動)として実施率の最も高いものは、「不審な電子メールの添付ファイルは開かない」で88.3%となっている。次いで、「怪しいと思われるウェブサイトにはアクセスしない(87.0%)」、「よく知らないウェブサイトではファイル(ソフトウェア)をダウンロードしない(85.7%)」の順となっている。
- 反対に、実施率の最も低いものは、「パスワードの定期的な変更」で43.4%となっている。次いで「必要時以外はネットにつながない(56.1%)」となっている。

情報セキュリティ対策の実施の有無
[セキュリティに関する注意・安全行動別]

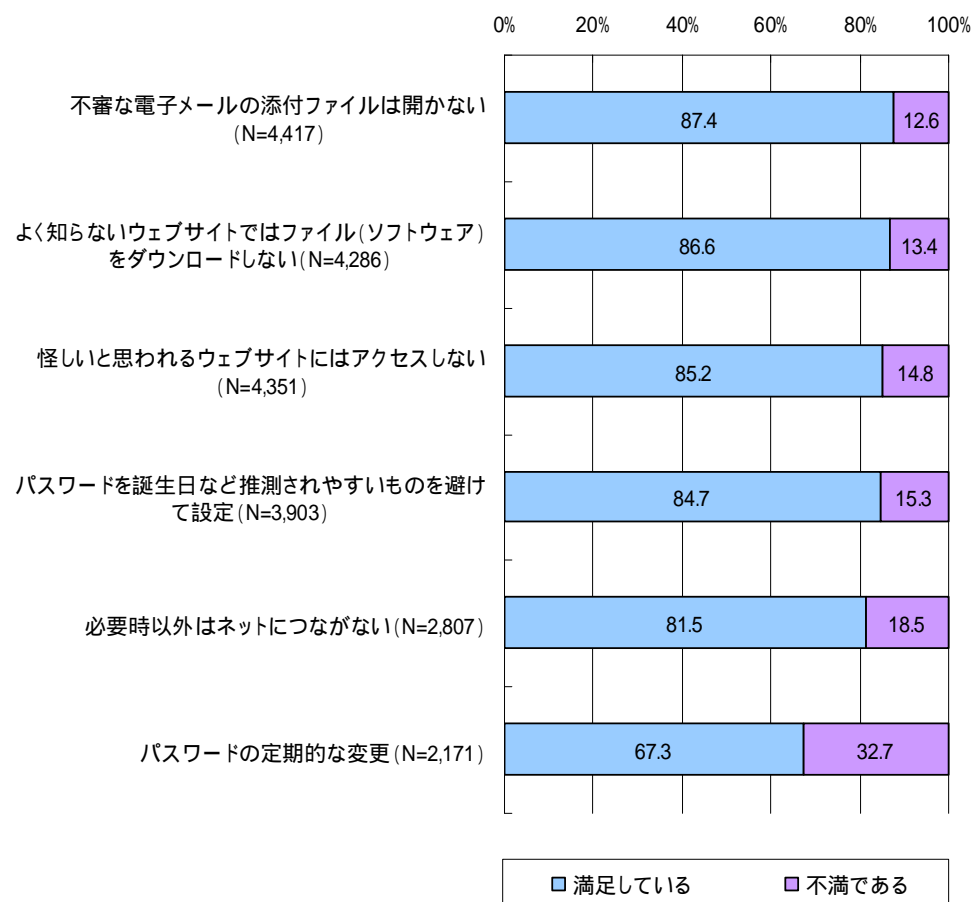


■ 実施している
■ 現在実施はしていないが、今後実施する予定である
■ 現在も、今後も実施する予定はない

3.4.1 情報セキュリティ対策の実施状況(6)

- 実施している情報セキュリティ対策(セキュリティに関する注意・安全行動)の満足度についてみると、満足度の高いものとして、「不審な電子メールの添付ファイルは開かない(87.4%)」や「よく知らないウェブサイトではファイル(ソフトウェア)をダウンロードしない(86.6%)」が挙げられる。
- 反対に、満足度が相対的に低いものとしては、「パスワードの定期的な変更(67.3%)」や「必要時以外はネットにつながらない(81.5%)」が挙げられる。

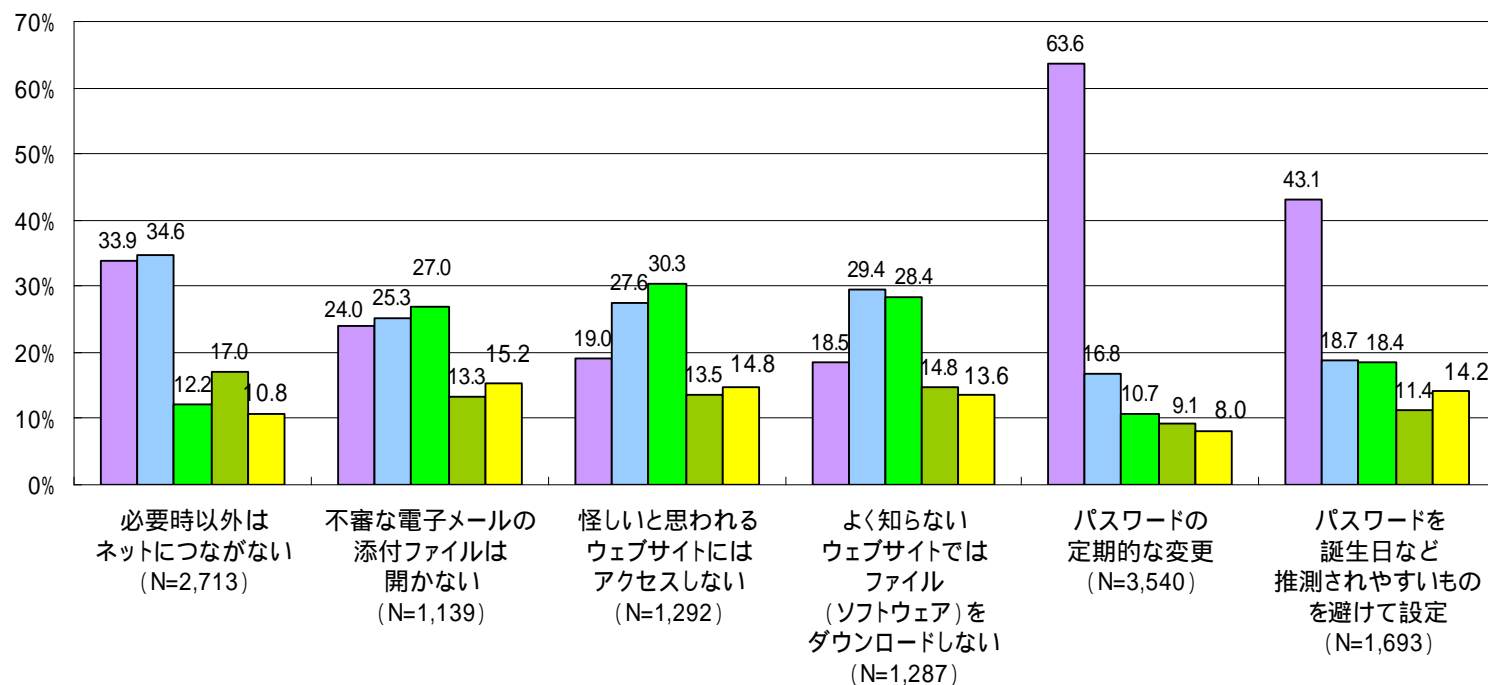
情報セキュリティ対策についての満足度
[個別の対策実施者に占める割合]



3.4.1 情報セキュリティ対策の実施状況(7)

- 手間や面倒臭さを、対策実施上の問題点として挙げるユーザが多いのは、「パスワードの定期的な変更(63.6%)」や「パスワードを誕生日など推測されやすいものを避けて設定(43.1%)」である。
- 対策を行うと、サイトやサービスの利用の利便性が損なわれることを、対策実施上の問題点として挙げるユーザが多いのは、「必要時以外はネットにつながらない(34.6%)」や「よく知らないウェブサイトではファイル(ソフトウェア)をダウンロードしない(29.4%)」である。

情報セキュリティ対策の実施上の問題点
[個別の対策実施者に占める割合]

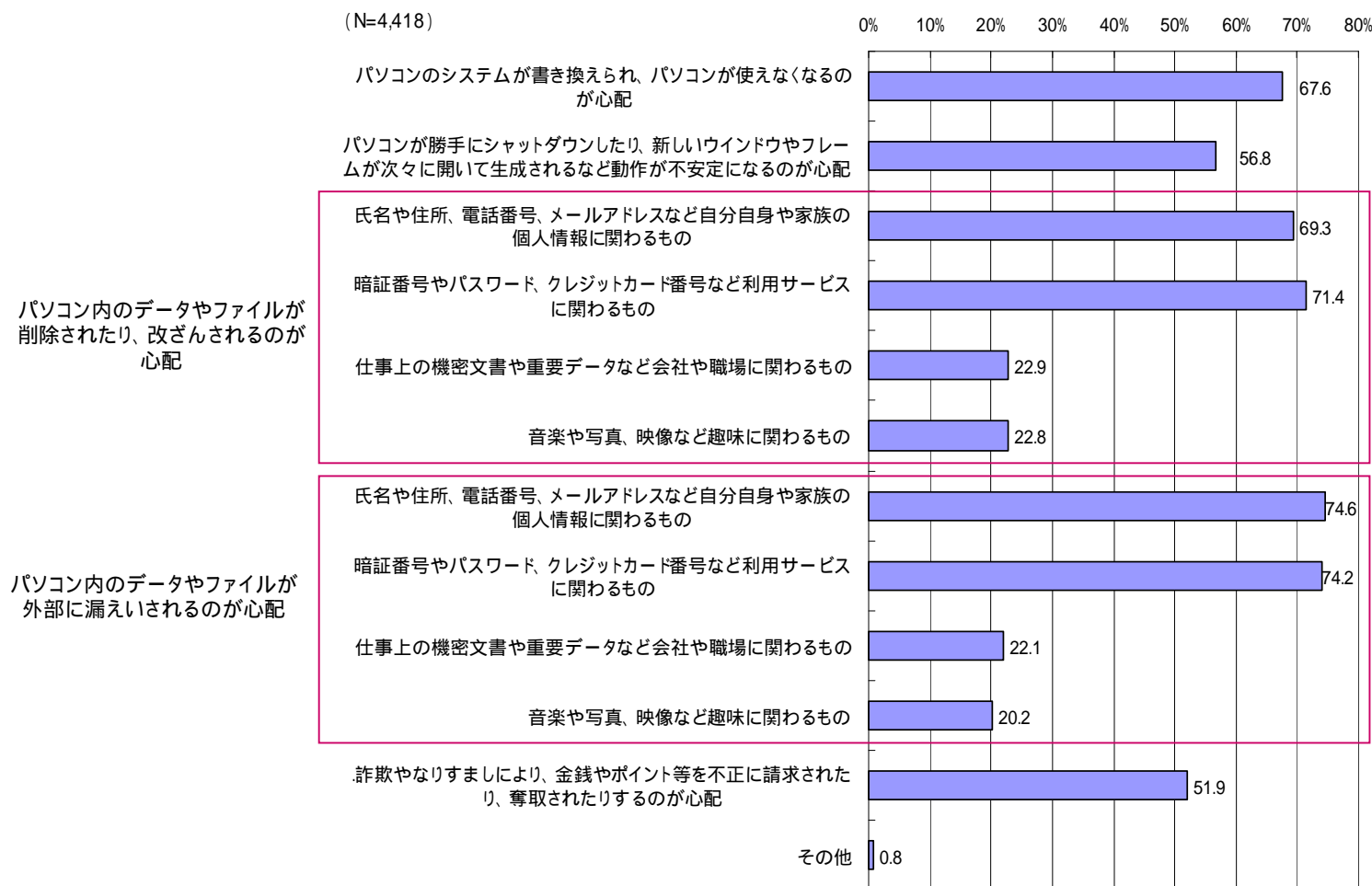


- 手間がかかり、面倒である
- 対策を行うと、サイトやサービスの利用の利便性が損なわれる
- どのように行えばよいか分かりにくい、あるいは分からない
- 対策の必要性がない(該当するサービスを利用していない、他の対策で十分カバーできるなど)
- その他

3.4.2 情報セキュリティ対策を実施している理由(1)

- 情報セキュリティ対策を実施している理由としては、「パソコン内のデータやファイルが外部に漏えいされるのが心配だから」、「パソコン内のデータやファイルが削除されたり、改ざんされるのが心配だから」が上位を占める。また、ユーザが情報セキュリティに関する被害から守りたいと考えているデータやファイルの中身としては、「氏名や住所、電話番号、メールアドレスなど自分自身や家族の個人情報に関わるもの」や「暗証番号やパスワード、クレジットカード番号など利用サービスに関わるもの」が上位を占める。
- その他、パソコンが使えなくなる心配やパソコンの動作が不安定になる心配を理由に、情報セキュリティ対策を実施しているユーザもそれぞれ67.6%、56.8%を占めている。

情報セキュリティ対策を実施している理由
[対策実施者に占める割合]

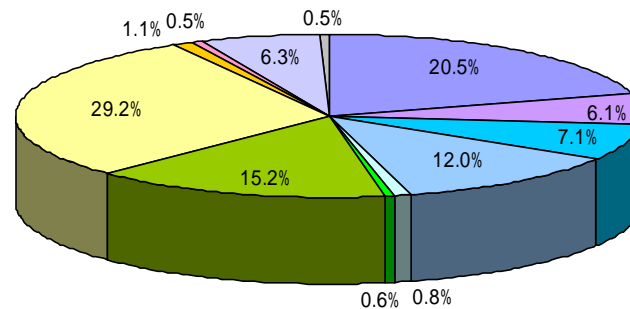


3.4.2 情報セキュリティ対策を実施している理由(2)

- 情報セキュリティ対策を実施しているユーザが最も心配している情報セキュリティに関する被害やトラブルは、パソコン内の暗証番号やパスワード、クレジットカード番号など利用サービスに関わるデータやファイルが外部に漏えいすることである。情報セキュリティ対策を実施しているユーザの約30%がこのような心配を抱えている。
- 次いで多いのは、「パソコンのシステムが書き換えられ、パソコンが使えなくなること(20.5%)」や「パソコン内の氏名や住所、電話番号、メールアドレスなど自分自身や家族の個人情報に関わるデータやファイルが外部に漏えいすること(15.2%)」である。

情報セキュリティ対策を実施している理由(主な理由)
[対策実施者に占める割合]

(N=4,418)

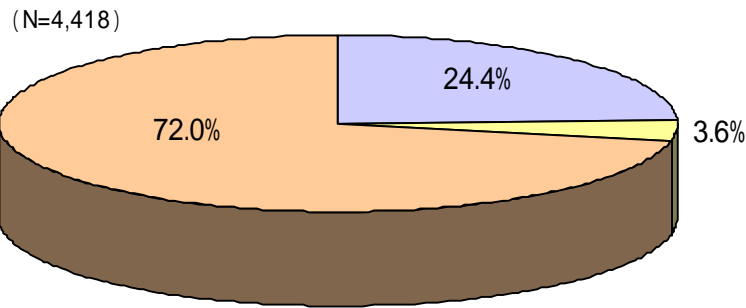


- パソコンのシステムが書き換えられ、パソコンが使えなくなるのが心配
 - パソコンが勝手にシャットダウンしたり、新しいウィンドウやフレームが次々に開いて生成されるなど動作が不安定になるのが心配
 - 氏名や住所、電話番号、メールアドレスなど自分自身や家族の個人情報に関わるもの
 - 暗証番号やパスワード、クレジットカード番号など利用サービスに関わるもの
 - 仕事上の機密文書や重要データなど会社や職場に関わるもの
 - 音楽や写真、映像など趣味に関わるもの
 - 氏名や住所、電話番号、メールアドレスなど自分自身や家族の個人情報に関わるもの
 - 暗証番号やパスワード、クレジットカード番号など利用サービスに関わるもの
 - 仕事上の機密文書や重要データなど会社や職場に関わるもの
 - 音楽や写真、映像など趣味に関わるもの
 - 詐欺やなりすましにより、金銭やポイント等を不正に請求されたり、奪取されたりするのが心配
 - その他
- パソコン内のデータやファイルが削除されたり、改ざんされるのが心配
- パソコン内のデータやファイルが外部に漏えいされるのが心配

3.4.3 情報セキュリティ対策を実施するきっかけになったもの

- 情報セキュリティ対策を実施しているユーザのうち、これまで情報セキュリティに関する被害やトラブルに実際に見舞われたことが、情報セキュリティ対策を実施するきっかけとなっているユーザは、24.4%と意外にも少数である。きっかけになった被害やトラブルとしては、「パソコンのシステムが書き換えられ、パソコンが使えなくなった」や「パソコンが勝手にシャットダウンしたり、新しいウインドウやフレームが次々に開いて生成されるなど動作が不安定になった」をあげるユーザが比較的多い。
- 残りの75.6%は、情報セキュリティに関する被害やトラブルに見舞われたことがなかったり、情報セキュリティに関する被害やトラブルが情報セキュリティ対策を実施するきっかけになっていない。

被害やトラブルの遭遇経験が
情報セキュリティ対策を実施するきっかけになったかどうか
[対策実施者に占める割合]

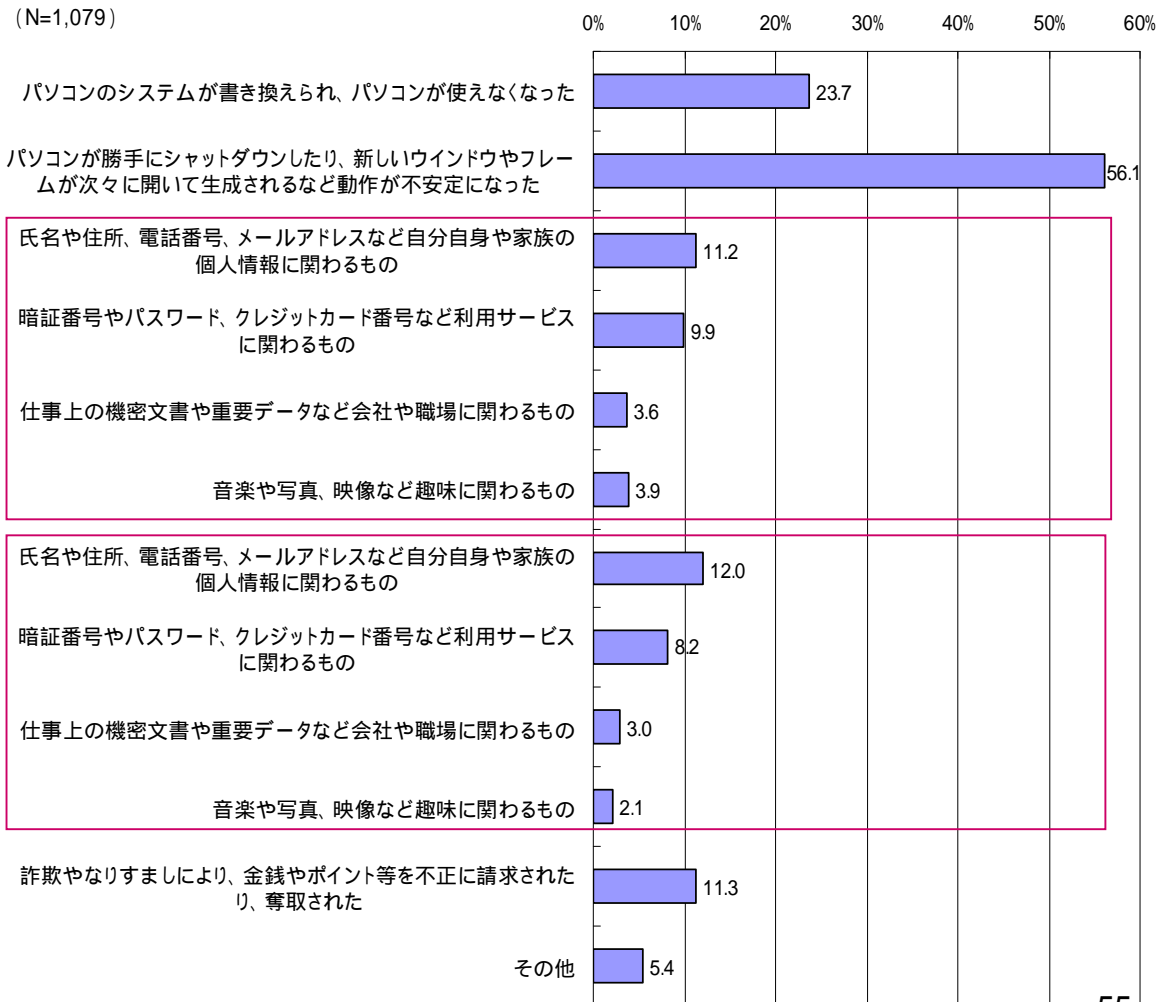


- これまで被害やトラブルに見舞われたことがあり、対策を実施するきっかけになっている
- これまで被害やトラブルに見舞われたことがあるが、対策を実施するきっかけにはなっていない
- これまで被害やトラブルに見舞われたことはない

パソコン内のデータやファイルが削除されたり、改ざんされた

パソコン内のデータやファイルが外部に漏えいされた

情報セキュリティ対策を実施するきっかけになった被害やトラブル
[被害やトラブルがきっかけになった者に占める割合]



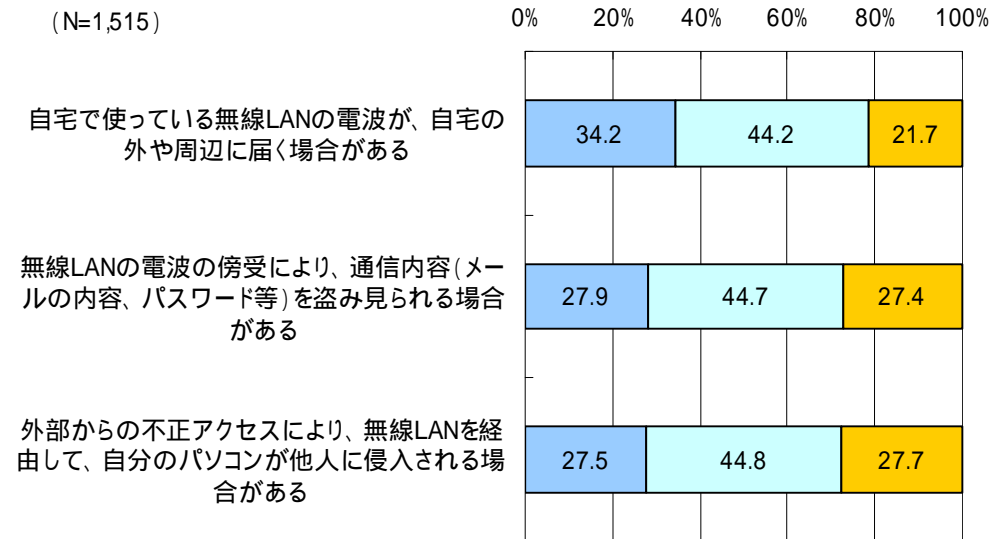
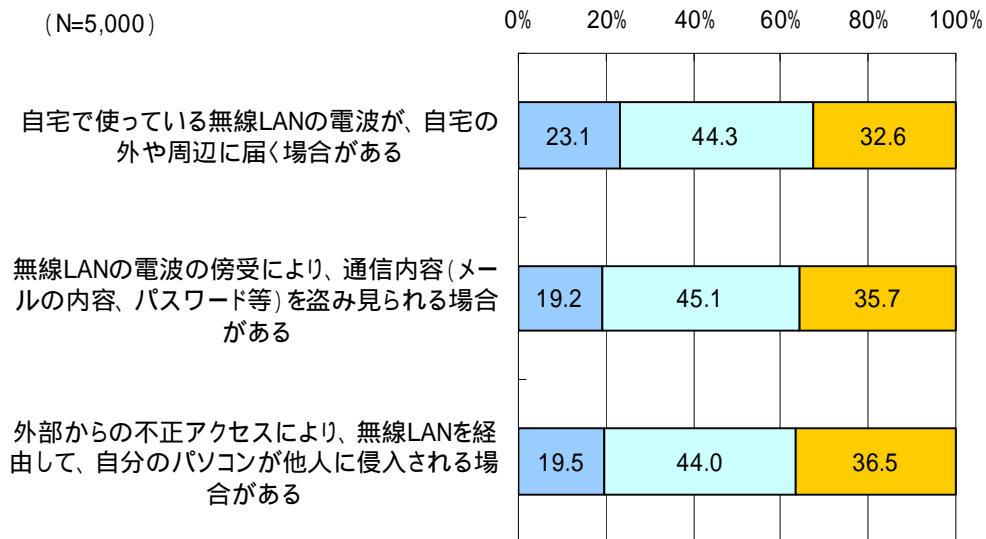
3.5 無線LANのセキュリティに対する対策状況

3.5.1 無線LANのセキュリティに関する被害やトラブルの認知状況

- 無線LANのセキュリティに関する被害やトラブルについて、聞いたことがあるか、内容を知っているかについて尋ねた。
- 自宅で使っている無線LANの電波の外部漏えいの危険性や、無線LANの電波の傍受による通信内容の盗み見の危険性、無線LAN経由での外部からの不正アクセスによるパソコンへの侵入の危険性について、詳しい内容を認知しているユーザは、いずれも20%前後にとどまっている。
- 自宅での無線LAN利用者の認知度についてみると、一般ユーザに比べて認知度がやや高いものの、自宅で使っている無線LANの電波の外部漏えいの危険性や、無線LANの電波の傍受による通信内容の盗み見の危険性、無線LAN経由での外部からの不正アクセスによるパソコンへの侵入の危険性について、詳しい内容を認知しているユーザは、いずれも30%前後にとどまっているのが現状である。

無線LANのセキュリティに関する被害やトラブルに対する認知度
[回答者全体に占める割合]

無線LANのセキュリティに関する被害やトラブルに対する認知度
[自宅での無線LAN利用者に占める割合]



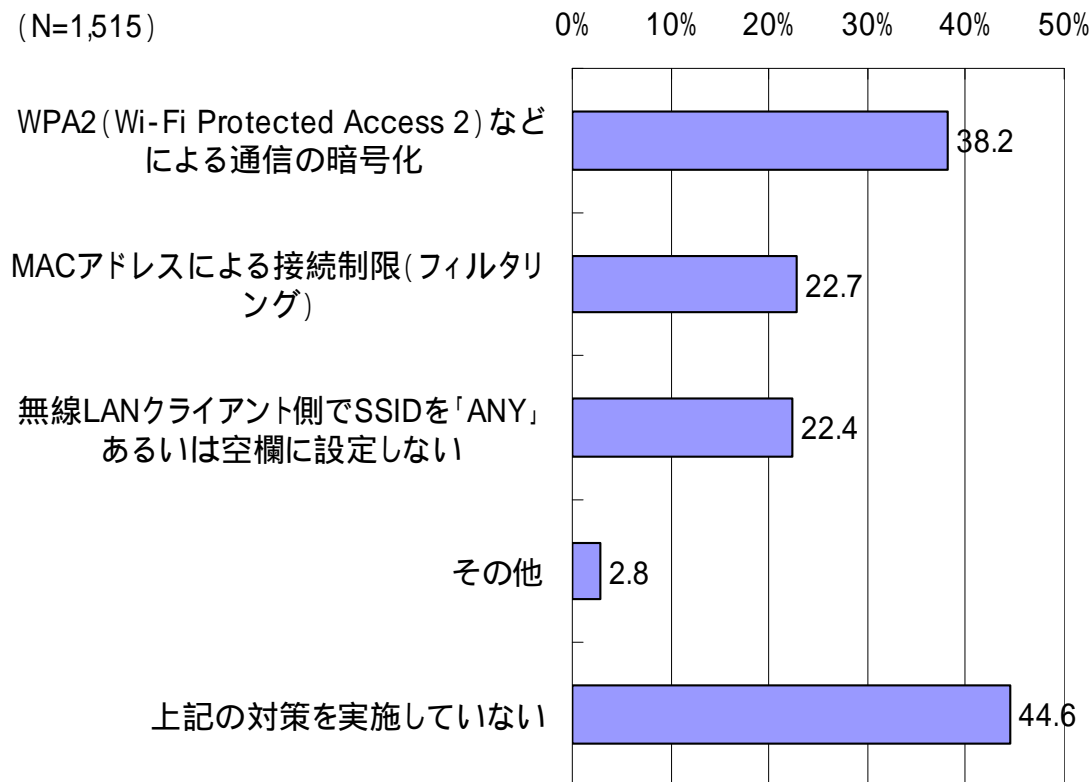
- そのような事例について、詳しい内容を知っている
- そのような事例について、概要を聞いたことがある程度である
- そのような事例について、まったく知らなかった

- そのような事例について、詳しい内容を知っている
- そのような事例について、概要を聞いたことがある程度である
- そのような事例について、まったく知らなかった

3.5.2 無線LANのセキュリティ対策の実施状況

- 自宅で無線LANを利用しているユーザのうち、セキュリティ対策を実施しているユーザは全体の55.4%にしか過ぎない状況である。無線LAN利用者のセキュリティ意識の低さが顕著である。
- セキュリティ対策の実施率として最も高いものは、「WPA2などによる通信の暗号化」で38.2%、次いで、「MACアドレスによる接続制限(フィルタリング) (22.7%)」、「無線LANクライアント側でSSIDを「ANY」あるいは空欄に設定しない(22.4%)」の順となっている。

無線LANのセキュリティ対策の実施の有無
[自宅での無線LAN利用者に占める割合]



調査票



※今、インターネット上で発生している情報セキュリティに関する脅威について、みなさんの認知状況や理解状況をお尋ねします。

【Q1】あなたは、次のようなインターネット上での攻撃・脅威に関する事例をご存知ですか。(それぞれひとつだけ)【必須】

	詳しい内容を知っている	概要をある程度知っている	名前を聞いたことがある程度	名前も、概要も知らない
1. スパイウェア	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2. ポット	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3. フィッシング詐欺	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4. ワンクリック不正請求	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5. スпамメール	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6. セキュリティホール(脆弱性)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
7. 標的型攻撃	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
8. マルウェア	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



【Q2】以下は、インターネット上の攻撃・脅威に対する理解度を確認するための設問です。

【Q2-S.1】それぞれの項目について、概要や特徴に関する説明のうち、あなたが正しいと思われるものをすべてお知らせください。(いくつでも)【必須】

ワンクリック不正請求

- 1. ウェブページへのアクセスや、画像等をクリックしただけで料金を請求される詐欺のことです
- 2. 主にアダルトサイトで発生していますが、投資関係のサイトなどアダルトサイト以外のサイトでも同様の手法が確認されています
- 3. 会員登録を促されたりして、不正なプログラムがダウンロードさせられることはありません
- 4. 身に覚えのない請求書が届いた場合、すぐに請求書に記載された連絡先に取り消しを求めると連絡をすることが大切です
- 5. 信頼できないサイトにアクセスしてしまっ、セキュリティの警告画面が表示されても、決して「実行」をクリックすることなく、「キャンセル」をクリックして先に進まないようにすることが有効です

スパイウェア

- 6. 利用者の個人情報等を収集し、外部に送信するプログラムのことを指します
- 7. ネットカフェなどのパソコンに仕掛けられていて、他の利用者の記録を盗むタイプがあります
- 8. コンピュータウイルスと同様、コンピュータ内や接続されているネットワーク内で自己増殖するタイプがあります
- 9. ポップアップ画面や確認メッセージにおいて、不審なメッセージが表示されたら、クリックせずに、ブラウザごと閉じるのが大切です
- 10. セキュリティ対策ソフトをパソコンにインストールしていれば、スパイウェアの侵入を防ぐのに有効です

ポット

- 11. コンピュータに感染し、そのコンピュータを、ネットワークを介して外部から操ることを目的としたプログラムのことを指します
- 12. 感染したかどうかは、パソコン自体が勝手に動くので、すぐに簡単に分かります
- 13. スпамメールを勝手に送信したり、DoS攻撃(特定のサイトへのサービス妨害)を行うタイプがあります
- 14. セキュリティ対策ソフトをパソコンにインストールしていれば、ポットの感染を防ぐのに有効です
- 15. ファイル交換ソフトの利用が感染経路となることが多く、メールでは感染することは少ないです

フィッシング詐欺

- 16. 金融機関などを装ったメールを送信し、偽サイトへのリンクを貼り付けて誘い出し、クレジットカード番号やパスワードなどを騙し取る行為です
- 17. メールのタイトルや本文については、偽装できても、メールの送信者欄(Fromアドレス)まで偽装することは不可能です
- 18. カード番号や暗証番号を入力するような依頼がメールで届いたときには、そのメールや情報の真偽を確認することが大切です

- 19. ブラウザのSSLの鍵マーク(サイトの証明書)を確認することは、偽サイトかどうかを見破るのに有効です
- 20. アドレスバーのURLを確認したときに、「http://192.168.80.138/」のようにIPアドレスが表示されていれば、偽サイトにアクセスしている可能性はありません



【Q2-S.2】それぞれの項目について、概要や特徴に関する説明のうち、あなたが正しいと思われるものをすべてお知らせください。(いくつでも)【必須】

標的型攻撃

- 1. 攻撃対象となるのは、不特定多数の一般ユーザーではなく、特定の組織や特定の個人になります
- 2. メールを利用して、ウイルスを送りつけたり、フィッシングを仕掛けることにより、情報を盗み出すタイプがあります
- 3. 攻撃者が用意した外部のサーバから不正なプログラムをダウンロードさせるために、先ずは、それを実行するために必要なダウンロードを、パソコンにインストールさせるタイプがあります
- 4. メール差出人のアドレスや本文の内容から疑わしい要素を見つけやすいので、対策が比較的容易です
- 5. セキュリティ対策ソフトで検知されないことが多いです

スパムメール

- 6. スпамメールとは、いわゆる社会的に問題となっている迷惑メールのことです
- 7. 一方的に、出会い系サイトやアダルトグッズ、低金利融資、違法な物品の販売等の広告・宣伝のためのメールが送信されるタイプがあります
- 8. メール本文に、ウイルス等の不正なプログラムが仕掛けられたウェブサイトへのリンクが強化されているタイプがあります
- 9. 心当たりのないメールや不審なメールに対しては、返信をして、そのようなメールの送信を停止するよう求めることが大切です
- 10. プロバイダの中には、スパムメールの送受信を防止したり、スパムメールをフィルタリングするサービスを提供している事業者があります

マルウェア

- 11. 悪意のあるソフトウェアのことを総称してマルウェアと呼びます
- 12. コンピュータウイルスやスパイウェア、ワームなどが、マルウェアに含まれます
- 13. 広告のウインドウをポップアップ表示させたり、ブラウザで広告を表示させるプログラムのように、利用者が自らの同意の下で使用しているソフトウェアも、マルウェアに含まれます
- 14. マルウェアは、電子メールの添付ファイルを介して頒布されるが、インターネット上のウェブサイトを利用して頒布されることはありません
- 15. ファイル交換ソフトは、マルウェアに含まれます

セキュリティホール(脆弱性)

- 16. セキュリティホールが発見されるのは、WindowsやMacなどのOSのみであり、ブラウザなどOS以外でセキュリティホールが発見されることはありません
- 17. セキュリティホールを放置しておく、悪意のあるユーザーに不正にコンピュータを操作され、他のコンピュータへ不正アクセスするための踏み台に利用されることがあります
- 18. セキュリティホールがあると、メールを開いたり、ネットワークに接続したりするだけで、ウイルスに感染する可能性があります
- 19. セキュリティホールが発見された場合には、ベンダー等から対策のための修正プログラムが無償で配布されます
- 20. Windows Updateなどを利用して常にパソコンを最新の状態にしておくことは、セキュリティホールを解消するのに有効です



【Q3】あなたは、インターネット上の攻撃・脅威において、次にあげる技術的な手口や心理的な手口が、現時点でどの程度実現されているかご存知ですか。(それぞれひとつだけ)【必須】

	すでに実現されているのを知っている	確信はないが、実現されていると思う	実現されていないが、今後実現される可能性があると思う	場合も、今後実現される可能性はないと思う	分からない
1. タイトルや文面を工夫し、あなた自身に関係があるメールであるようにみせかけることで、添付ファイルやURLをクリックされやすいようにする手口	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2. ウィルスや仕込んだデータファイル(WordファイルやExcelファイルなど)をメールに添付し、クリックされやすいようにする手口	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3. 本人確認が必要で、かつ相手の所在の確認が容易であるような安心・安全を売りにしたサービス(紹介SNSなど)を利用することで、詐欺トラブル等に遭わせやすくなる手口	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

4. 閲覧したいサイトのURLを正しく入力しても、勝手に別のサイトに誘導されてしまう手口
5. ウェブサイトを閲覧しただけで、意図せずに、ウイルスを自動的にダウンロードさせてしまう手口



インターネット上で発生している情報セキュリティに関する脅威について、過去1年間におけるみなさんの被害状況を専らお尋ねします。

【Q4】あなたは、過去1年間にパソコンやインターネットを利用して、以下のような情報セキュリティに関する被害やトラブルを経験したことがありますか。

あてはまるものをすべてお知らせください。(いくつでも)【必須】

- 1. コンピュータウイルスに感染した(感染後にセキュリティ対策ソフトが検出したケースを含む)
- 2. 自分のパソコンのシステムやファイルが書き換えられたり、削除された
- 3. 全く知らない差出人から大量のメールが送られてきた
- 4. メールに記載されたURLをクリックしたら、個人情報の入力を求めるウェブページが表示された
- 5. ホームページ閲覧中に、契約した覚えのない料金の支払いを要求するメッセージが表示された
- 6. 身に覚えのない料金の支払いを要求するメールが送られてきた
- 7. 知らない間に、銀行口座からお金が引き出された
- 8. 知らない間に、自分のパソコンから他者へのメールを送信していた
- 9. 他者による個人情報流出の被害にあったことがある
- 10. 自分のパソコンから個人情報を流出させてしまったことがある
- 11. オンラインゲームにおいて、ゲーム通貨を不正に搾取されたり、アイテムを騙し取られたことがある
- 12. ネットオークションにおいて、勝手に本人になりすまされ、架空の商品が出品されたり、お金を振り込んだのに商品が届かなかったことがある
- 13. その他 (具体的に⇒ _____)
- 14. 被害にあったことはない
- 15. 被害にあったかどうか分からない



【Q5】【Q4】でお答えになった被害やトラブルで、あなたは、過去1年間に金銭的な被害を被りましたか。(ひとつだけ)金銭的な被害を被った場合は、具体的な金額をお知らせください。(半角数値)【必須】

- 1. 金銭的な被害を被った (およそ _____ 円くらい)
- 2. 特に金銭的な被害には至らなかった



【Q6】あなたは、どのようなサイトやサービスを利用しているときに、情報セキュリティに関する被害やトラブルに遭う可能性が高いとお考えですか。

あなた自身の経験から、被害やトラブルと関わりがあると考えられるものについてお知らせください。(それぞれひとつだけ)【必須】

	情報セキュリティに関する被害やトラブルとの関わり			
	関わりがあると 思う	どちらかとい えば関わりが あもと思 う	分 から ない	ど ら ら か と い え ば 関 わり は な い と 思 う
1. 検索サイト、ポータルサイト	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2. 商品比較、口コミ等のコミュニティサイトやQ&Aサイト、懸賞サイト	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

1. 検索サイト、ポータルサイト
2. 商品比較、口コミ等のコミュニティサイトやQ&Aサイト、懸賞サイト

3. 企業・団体のサイト	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4. 個人のホームページやブログの閲覧	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5. インターネットショッピング	<input type="radio"/>	<input type="radio"/>	<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"/>	<input type="radio"/>	<input type="radio"/>
7. インターネットバンキング、オンライントレード	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
8. 掲示板	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
9. SNS	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
10. 電子メール	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
11. インスタントメッセージ	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
12. 映像コンテンツや音楽コンテンツの視聴や購入	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
13. ファイル交換ソフトの利用	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
14. オンラインゲーム	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
15. 上記1～14以外のサイトやサービス	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

「15.上記1～14以外のサイトやサービス」の具体的な内容をお知らせください。(具体的に)【必須】

※1～14以外のサイトやサービスが思い浮かばない方は、「なし」とお書きください。



【Q7】以下のサイトやサービスのうち、あなたが現在、普段から利用しているものはどれですか。あてはまるものをすべてお知らせください。(いくつでも)【必須】

- 1. 検索サイト、ポータルサイト
- 2. 商品比較、口コミ等のコミュニティサイトやQ&Aサイト、懸賞サイト、百科事典サイト、ニュースサイト
- 3. 企業・団体のサイト
- 4. 個人のホームページやブログの閲覧
- 5. インターネットショッピング
- 6. インターネットオークション
- 7. インターネットバンキング、オンライントレード
- 8. 掲示板
- 9. SNS
- 10. 電子メール
- 11. インスタントメッセージ
- 12. 映像コンテンツや音楽コンテンツの視聴や購入
- 13. ファイル交換ソフトの利用
- 14. オンラインゲーム
- 15. その他 (具体的に⇒ _____)
- 16. 普段から利用しているものはない



【Q8】あなたは、ご自宅でお使いのパソコンで、次のような電子メールを受け取ったことがありますか。受け取ったことがあるものをすべてお知らせください。(いくつでも)【必須】

- 1. 出会い系サイトやアダルトグッズ、低金利融資、違法な物品の販売等の広告・宣伝メール(未承諾の広告・宣伝メール)
- 2. 根拠のない不当な料金請求などを催促する詐欺メール(架空料金請求メール)
- 3. プロバイダのサポート担当者からのメールや懸賞サイトの当選通知メールなどを装って、ユーザにパスワードやクレジットカード番号等を入力させ、だまし取る詐欺メール(フィッシングメール)
- 4. ウイルスやワームなどのマルウェアが添付されているメール(ウイルスメール)
- 5. 「5日以内にこのメールを10人に送らないと不幸になります」といった内容で、別の人へのメール転送を要請するチェーンメール
- 6. 意味のない内容が送られてくるメールや空(空白)メール

- 7. 友人・知人や会社のメールアドレスや名前を装って送られるメール
- 8. 非常に大きいファイルが添付されて送られる嫌がらせメール
- 9. その他（具体的に⇒)
- 10. 上記1～9のいずれも受け取ったことがない



【Q9】【Q8】のような迷惑メールの受信頻度は、現在の程度ですか。あてはまるものをお知らせください。(ひとつだけ)【必須】

※ご自宅でお使いのパソコンについてお答えください。
 ※あなた自身が自宅に複数のパソコンを所有している場合や、電子メールのアカウントを複数所有している場合は、それらをすべて差し合せた形でお答えください。

- 1. 毎日200通以上（およそ 通）
- 2. 毎日100～199通
- 3. 毎日50～99通
- 4. 毎日40～49通
- 5. 毎日30～39通
- 6. 毎日20～29通
- 7. 毎日15～19通
- 8. 毎日10～14通
- 9. 毎日6～9通
- 10. 毎日1～5通
- 11. 週に1～5通程度
- 12. ほとんどない



【Q10】【Q9】のような迷惑メールの受信相手や内容の確認、メール分類、ウイルスチェック、メール削除などのために、あなたは、どの程度の貴重な時間を費やしていますか。1週間当たりの総時間でお知らせください。(ひとつだけ)【必須】

- 1. 10時間以上（およそ 時間）
- 2. 5～10時間未満
- 3. 3～5時間未満
- 4. 2～3時間未満
- 5. 1～2時間未満
- 6. 30分～1時間未満
- 7. 20～30分未満
- 8. 10～20分未満
- 9. 10分未満
- 10. 特に意識して時間を費やしていない



インターネット上で発生している情報セキュリティに関する脅威について、みなさんの対策状況をお尋ねします。

【Q11】あなたが、所有するパソコンや自宅のネットワークについて、現在、情報セキュリティ対策を実施している理由は何ですか。(いくつでも)【必須】

- 1. パソコンのシステムが書き換えられ、パソコンが使えなくなるのが心配
- 2. パソコンが勝手にシャットダウンしたり、新しいウィンドウやフレームが次々に開いて生成されるなど動作が不安定になるのが心配

パソコン内のデータやファイルが削除されたり、改ざんされたりするのが心配

- 3. 氏名や住所、電話番号、メールアドレスなど自分自身や家族の個人情報に関わるもの

- 4. 暗証番号やパスワード、クレジットカード番号など利用サービスに関わるもの
- 5. 仕事上の機密文書や重要データなど会社や職場に関わるもの
- 6. 音楽や写真、映像など趣味に関わるもの

パソコン内のデータやファイルが外部に漏えいされるのが心配

- 7. 氏名や住所、電話番号、メールアドレスなど自分自身や家族の個人情報に関わるもの
- 8. 暗証番号やパスワード、クレジットカード番号など利用サービスに関わるもの
- 9. 仕事上の機密文書や重要データなど会社や職場に関わるもの
- 10. 音楽や写真、映像など趣味に関わるもの

- 11. 詐欺やなりすましにより、金銭やポイント等を不正に請求されたり、奪取されたりするのが心配
- 12. その他（具体的に⇒)

- 13. 情報セキュリティ対策は特に実施していない



【Q11】【Q11】で選んだ中で、あなたが最も心配しているものをお知らせください。(ひとつだけ)【必須】

- 1. パソコンのシステムが書き換えられ、パソコンが使えなくなるのが心配
- 2. パソコンが勝手にシャットダウンしたり、新しいウィンドウやフレームが次々に開いて生成されるなど動作が不安定になるのが心配

パソコン内のデータやファイルが削除されたり、改ざんされたりするのが心配

- 3. 氏名や住所、電話番号、メールアドレスなど自分自身や家族の個人情報に関わるもの
- 4. 暗証番号やパスワード、クレジットカード番号など利用サービスに関わるもの
- 5. 仕事上の機密文書や重要データなど会社や職場に関わるもの
- 6. 音楽や写真、映像など趣味に関わるもの

パソコン内のデータやファイルが外部に漏えいされるのが心配

- 7. 氏名や住所、電話番号、メールアドレスなど自分自身や家族の個人情報に関わるもの
- 8. 暗証番号やパスワード、クレジットカード番号など利用サービスに関わるもの
- 9. 仕事上の機密文書や重要データなど会社や職場に関わるもの
- 10. 音楽や写真、映像など趣味に関わるもの

- 11. 詐欺やなりすましにより、金銭やポイント等を不正に請求されたり、奪取されたりするのが心配
- 12. 【FA】



【Q13】次のような情報セキュリティに関する被害やトラブルのうち、あなたが、実際に被害やトラブルに見舞われ、情報セキュリティ対策を実施するきっかけとなったものがありますか。あてはまるものをすべてお知らせください。(いくつでも)【必須】

- 1. パソコンのシステムが書き換えられ、パソコンが使えなくなった
- 2. パソコンが勝手にシャットダウンしたり、新しいウィンドウやフレームが次々に開いて生成されるなど動作が不安定になった

パソコン内のデータやファイルが削除されたり、改ざんされた

- 3. 氏名や住所、電話番号、メールアドレスなど自分自身や家族の個人情報に関わるもの
- 4. 暗証番号やパスワード、クレジットカード番号など利用サービスに関わるもの
- 5. 仕事上の機密文書や重要データなど会社や職場に関わるもの
- 6. 音楽や写真、映像など趣味に関わるもの

パソコン内のデータやファイルが外部に漏えいされた

- 7. 氏名や住所、電話番号、メールアドレスなど自分自身や家族の個人情報に関わるもの
- 8. 暗証番号やパスワード、クレジットカード番号など利用サービスに関わるもの
- 9. 仕事上の機密文書や重要データなど会社や職場に関わるもの
- 10. 音楽や写真、映像など趣味に関わるもの

- 11. 詐欺やなりすましにより、金銭やポイント等を不正に請求されたり、奪取された
- 12. その他 (具体的に⇒ _____)
- 13. 上記1～12について、これまでに被害やトラブルに見舞われたことがあるが、そのことが情報セキュリティ対策を実施するきっかけにはなっていない
- 14. 上記1～12について、これまでに被害やトラブルに見舞われたことはない



【Q14】あなた自身が所有するパソコンや自宅のネットワークについて、現在実施しているセキュリティの技術的対策と、実施している方はそれらの満足度についてお知らせください。(それぞれひとつだけ)【必須】

	実施している		実施していない	
	満足である	不満である	現在実施はして 現在も、今後もないが、今後実施する予定はない	現在実施はして 現在も、今後もない
1. Windows Update等によるセキュリティパッチの更新	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. セキュリティ対策ソフトの導入・活用	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. 有害なウェブサイトへのアクセスを防止するソフトまたはサービスの導入・活用	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. パソコンのログインパスワードの設定	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5. ルーターでのセキュリティ対策	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6. ウェブサイトの安全性評価ツールの利用	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7. 暗号化されたUSBメモリの利用や、重要なファイルの暗号化	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8. パソコンの重要なデータのバックアップ	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9. 不要になった自宅パソコンの廃棄・リサイクル前のデータ消去	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



【Q15】【Q14】で「不満である」、「現在実施はしていないが、今後実施する予定である」、「現在も、今後実施する予定はない」とご回答になられた方にお伺いします。セキュリティの技術的対策を実施する上で、問題となるのはどのようなことですか。あてはまるものをすべてお知らせください。(それぞれいくつでも)【必須】

	お金がかかる	手間がかかり、面倒である	対策を行うと、サイトやサービスの利用の利便性が損なわれる	どのように行えばよいか分からない、あるいは分からない	製品の製造・販売者から十分なサポートが得られない、あるいは得られるかどうか不安である	対策の必要性がない(該当するサービスを利用していない、他の対策で十分カバーできるなど)	その他
1. Windows Update等によるセキュリティパッチの更新	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. セキュリティ対策ソフトの導入・活用	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. 有害なウェブサイトへのアクセスを防止するソフトまたはサービスの導入・活用	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. パソコンのログインパスワードの設定	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5. ルーターでのセキュリティ対策	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6. ウェブサイトの安全性評価ツールの利用	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7. 暗号化されたUSBメモリの利用や、重要なファイルの暗号化	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8. パソコンの重要なデータのバックアップ	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9. 不要になった自宅パソコンの廃棄・リサイクル前のデータ消去	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



【Q16】あなた自身が所有するパソコンや自宅のネットワークについて、現在実施しているセキュリティに関する注意・安全行動と、実施している方はそれらの満足度についてお知らせください。(それぞれひとつだけ)【必須】

	実施している		実施していない	
	満足である	不満である	現在実施はして 現在も、今後もないが、今後実施する予定はある	現在実施はして 現在も、今後もない
1. 必要時以外はネットにつながらない	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. 不審な電子メールの添付ファイルは開かない	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. 怪しいと思われるウェブサイトにはアクセスしない	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. よく知らないウェブサイトではファイル(ソフトウェア)をダウンロードしない	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5. パスワードの定期的な変更	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6. パスワードを誕生日など推測されやすいものを避けて設定	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



【Q17】【Q16】で「不満である」、「現在実施はしていないが、今後実施する予定である」、「現在も、今後実施する予定はない」とご回答になられた方にお伺いします。セキュリティに関する注意・安全行動を実施する上で、問題となるのはどのようなことですか。あてはまるものをすべてお知らせください。(それぞれいくつでも)【必須】

	手間がかかり、面倒である	対策を行うと、サイトやサービスの利用の利便性が損なわれる	どのように行えばよいか分からない、あるいは分からない	対策の必要性がない(該当するサービスを利用していない、他の対策で十分カバーできるなど)	その他
1. 必要時以外はネットにつながらない	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. 不審な電子メールの添付ファイルは開かない	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. 怪しいと思われるウェブサイトにはアクセスしない	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. よく知らないウェブサイトではファイル(ソフトウェア)をダウンロードしない	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5. パスワードの定期的な変更	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6. パスワードを誕生日など推測されやすいものを避けて設定	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



【Q18】あなたは、以下のような無線LANのセキュリティに関する被害やトラブルについて、ご存知ですか。(それぞれひとつだけ)【必須】

	そのような事例について、詳しい内容を知っている	そのような事例について、概要を聞いたことがある程度である	そのような事例について、まったく知らなかった
1. 自宅で使っている無線LANの電波が、自宅の外や周辺に届く場合がある	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. 無線LANの電波の検受により、通信内容(メールの内容、パスワード等)を読み取られる場合がある	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. 外部からの不正アクセスにより、無線LANを経由して、自分のパソコンが他人に侵入される場合がある	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



【Q19】自宅の無線LANに対するセキュリティ対策として、あなたは以下のような対策を行っていますか。あてはまるものをすべてお知らせください。(いくつでも)【必須】

- 1. WPA2(Wi-Fi Protected Access 2)などによる通信の暗号化
- 2. MACアドレスによる接続制限(フィルタリング)

- 3. 無線LANクライアント側でSSIDを「ANY」あるいは空欄に設定しない
- 4. その他（具体的に⇒ _____)
- 5. 上記1～4の対策を実施していない
- 6. 無線LANを利用していない



【Q20】あなたの性別をお知らせください。(ひとつだけ)【必須】

- 1. 男性
- 2. 女性

【Q21】あなたの現在の満年齢をお知らせください。(半角数値)【必須】

歳

【Q22】あなたがお住まいの都道府県をお知らせください。(ひとつだけ)【必須】

県

【Q23】あなたの職業は、この中のどれにあたりますか。(ひとつだけ)【必須】

- 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通信関係の技術者・研究者)
- 4. 会社員・公務員・教員(情報システムおよび通信関係の技術者・研究者以外の方)
- 5. 医者・弁護士等の専門職
- 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. 専門学校生・短大生・大学生・大学院生
- 12. 中・高校生
- 13. その他（具体的に⇒ _____)



【Q24】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。(ひとつだけ)【必須】

- 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
- 11. 2007年
- 12. 2008年以降



【Q25】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。(いくつでも)【必須】

- 1. 職場

- 2. 学校
- 3. 自宅(有線)
- 4. 自宅(無線LAN)
- 5. 外出先(データ通信カード利用)
- 6. 外出先(公衆無線LAN)
- 7. インターネットカフェ、マンガ喫茶等
- 8. その他



【Q26】パソコンでインターネットを利用する時間(仕事上での利用を除く)は1日平均どれぐらいですか。(ひとつだけ)【必須】

- 1. 30分未満
- 2. 30分～1時間未満
- 3. 1時間～3時間未満
- 4. 3時間～5時間未満
- 5. 5時間～7時間未満
- 6. 7時間～10時間未満
- 7. 10時間以上



【Q27】あなたのパソコンの習熟度についてお知らせください。(ひとつだけ)【必須】

- 1. パソコンを自分で組み立てたり、トラブルが起きても自分で解決できるレベルである
- 2. 必要なソフトウェアをインストールして使ったり、パソコンの設定を変えて使ったりすることができるレベルである
- 3. メールを使ったり、ホームページを閲覧したり、文章を書いたりするのに支障がないレベルである
- 4. パソコンの簡単な操作しか分からないレベルである

閉じる