

2008年度第2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

2009年3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	10
3.1 PCインターネットの利用状況	11
3.2 情報セキュリティに関する脅威に対する被害状況	20
3.3 情報セキュリティに関する脅威に対する対策状況	28
3.4 USBメモリのセキュリティに対する対策状況	38
3.5 無線LANのセキュリティに対する対策状況	42
3.6 セキュリティ情報の入手方法	47
参考 調査票	52

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 2009年1月16日(金)～2009年1月19日(月)
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。

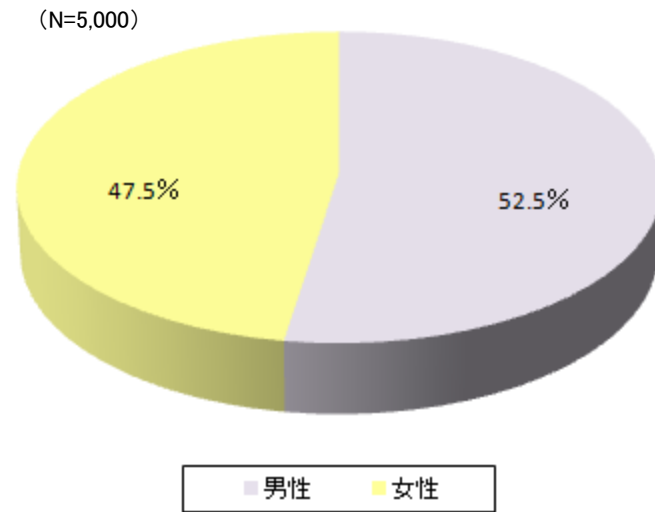
区分	男性		女性		計	
	サンプル数	構成比	サンプル数	構成比	サンプル数	構成比
15-19	215	4.3%	215	4.3%	430	8.6%
20代	530	10.6%	510	10.2%	1,040	20.8%
30代	631	12.6%	597	11.9%	1,228	24.5%
40代	472	9.4%	451	9.0%	923	18.5%
50代	493	9.9%	400	8.0%	893	17.9%
60代	284	5.7%	202	4.0%	486	9.7%
計	2,625	52.5%	2,375	47.5%	5,000	100.0%

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被害状況
 - ・セキュリティ情報の入手方法
 - ・情報セキュリティに関する脅威に対する対策状況
 - ・USBメモリのセキュリティに対する対策状況

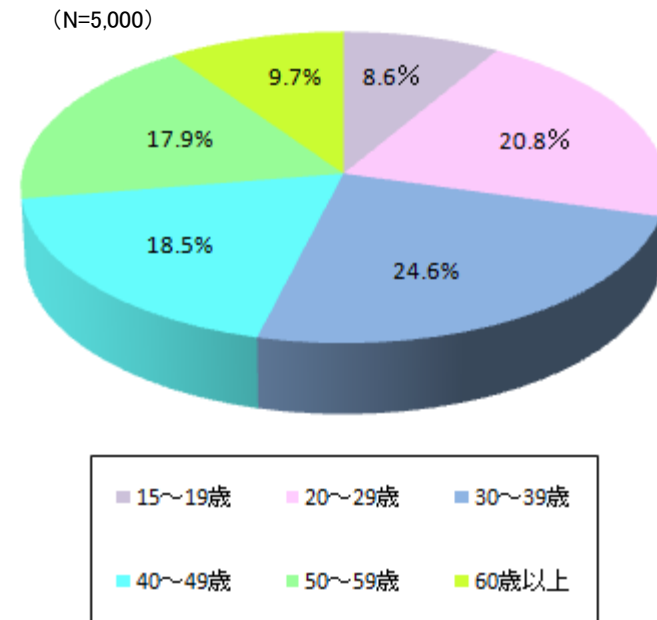
基本属性(1)

- ・ 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

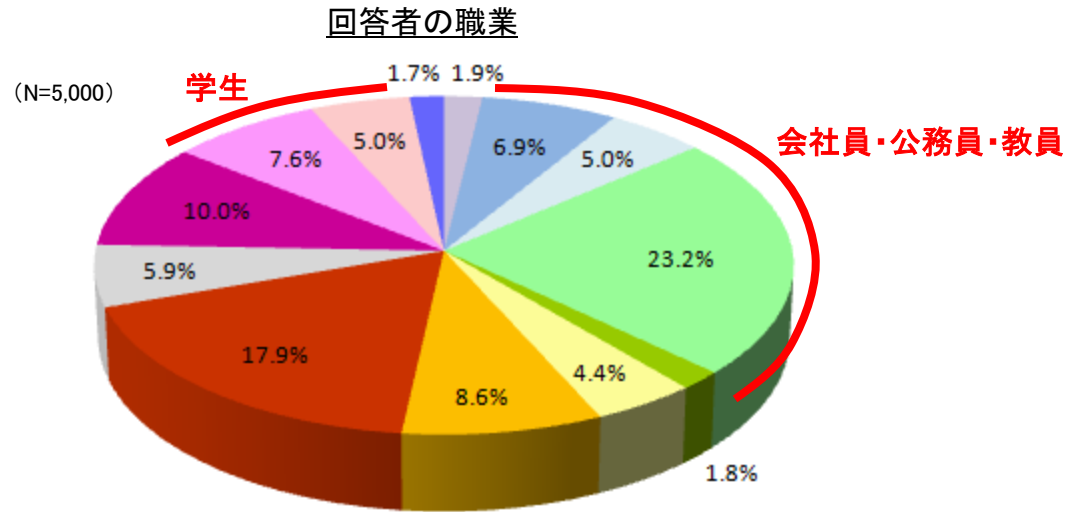


回答者の年齢構成



基本属性(2)

- ・ 回答者の職業構成は、「会社員・公務員・教員」が35.1%と最も多く、次いで、「専業主婦(17.9%)」、「パート・アルバイト(10.0%)」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7.6%、「高校生」が5.0%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

USBメモリの利用者が全体の59.2%を占め、普及の進展が見られる中で、USBメモリを介して、コンピュータに感染するウイルスが存在することや、そのような被害が広がっていることについて、詳しい内容や概要を認知しているユーザの割合は、USBメモリ利用者の53.1%にとどまっている。

- ・ ユーザの59.2%が現在、USBメモリを使用している。ユーザの12.4%は、以前はUSBメモリを使用していたが、現在は使用していない。また、ユーザの28.4%は、これまで一度もUSBメモリを使用していない。
- ・ USBメモリ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は、「詳しい内容を知っている」が14.1%、「概要をある程度知っている」が39.0%、「そのような話題があること聞いたことがある程度」が32.6%である。

3.4.1 USBメモリの使用状況 (P39) / 3.4.3 USBメモリのセキュリティに関する被害やトラブルの認知状況 (P41) 参照

USBメモリ利用者の3人に1人が、USBメモリのセキュリティ対策を実施していない状況である。勝手にウイルスが起動しないように、USBメモリの自動実行をさせないようにしているユーザ、挿入先のコンピュータにおいて、セキュリティ対策ソフトが常に最新の状態で使用されているかどうかを確認するようにしているユーザ、USBメモリ内のファイルを開く前には、必ずウイルスチェックをするようにしているユーザはいずれもUSBメモリ利用者の20%にも満たない状況である。

- ・ USBメモリのセキュリティ対策を実施しているユーザは、USBメモリ利用者の67.0%である。
- ・ USBメモリのセキュリティ対策の実施内容についてみると、「出所不明のUSBメモリや、セキュリティ面で信用できないUSBメモリを使用しないようにしている」が50.2%、「勝手にウイルスが起動しないように、USBメモリの自動実行をさせないようにしている」が18.5%、「挿入先のコンピュータにおいて、セキュリティ対策ソフトが常に最新の状態で使用されているかどうかを確認するようにしている」が18.3%、「USBメモリ内のファイルを開く前には、必ずウイルスチェックをするようにしている」が14.7%と低い水準となっている。

3.4.2 USBメモリのセキュリティ対策の実施状況 (P40) 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

無線LANのセキュリティに対しては、利用者の意識の低さが顕著である。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%が電波の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である。

- ・ 自宅で無線LANを利用しているユーザのうち、「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」や「無線LANの電波の傍受により、通信内容を盗み見られる場合がある」、「外部からの不正アクセスにより、無線LANアクセスポイントを経由して、自分のパソコンが他人に侵入される場合がある」といった事例について全く知らなかったと回答しているユーザがそれぞれ22.1%、30.2%、30.3%存在する。

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(P43)参照

無線LANの暗号方式に関しては、WEPにより暗号化された情報を瞬時に解読することができる手法が報告されており、WEPの脆弱性が指摘されているが、自宅での無線LAN利用者の21.7%が、WEPを利用している。また、より解読しにくい暗号方式として乗り換えが期待されているWPA2の利用率に関しては、自宅での無線LAN利用者の僅か6.0%にしか過ぎない状況である。

- ・ 自宅で無線LANを利用しているユーザのうち、通信の暗号化対策を実施しているユーザは58.5%である。実施率の高いものとしては、「WEPによる通信の暗号化」が21.7%、次いで、「WPAによる通信の暗号化」が7.0%、「WPA2による通信の暗号化」が6.0%となっている。また、「どのような暗号方式を利用しているまでは分からない」が23.8%に上っている。

3.5.2 無線LANのセキュリティ対策の実施状況(1)(P44)参照

通信の暗号化対策以外で、MACアドレスによる接続制限(フィルタリング)やSSIDの非通知機能(ステルス化)など何らかのセキュリティ対策を実施しているユーザの割合は、自宅での無線LAN利用者の40%にも満たない状況である。

- ・ 自宅で無線LANを利用しているユーザのうち、通信の暗号化対策以外のセキュリティ対策を実施しているユーザは39.8%にしか過ぎない状況である。実施率の最も高いものとしては、「MACアドレスによる接続制限(フィルタリング)」が26.1%、次いで、「SSIDの非通知機能(ステルス化)」が14.8%、「SSIDの「ANY」接続を拒否する設定」が13.5%となっている。

3.5.2 無線LANのセキュリティ対策の実施状況(2)(P45)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

セキュリティ対策ソフトの利用者のうち、10%強がパターンファイル(更新ファイル)を更新しているかどうか分からない、あるいはパターンファイル(更新ファイル)を更新していない状況となっている。

- ・ セキュリティ対策ソフトの利用者のうち、パターンファイル(更新ファイル)の更新について、何もしなくても新しいパターンファイル(更新ファイル)が更新されるように、自動更新機能を設定しているユーザが75.6%、自分で新しいパターンファイル(更新ファイル)をダウンロードし、手動で実行しているユーザが13.2%、パターンファイル(更新ファイル)を更新しているかどうか分からないユーザが8.5%、パターンファイル(更新ファイル)を更新していないユーザが2.7%存在する。

3.3.1 情報セキュリティ対策の実施状況(3)(P31)参照

パターンファイル(更新ファイル)を更新しているユーザにおいても、直近でパターンファイル(更新ファイル)を更新した時期が1ヶ月以上も遡るユーザや、手動で更新しているにも関わらずパターンファイル(更新ファイル)の更新時期が分からないユーザが存在しており、上記のパターンファイル(更新ファイル)を更新しているかどうか分からないユーザやパターンファイル(更新ファイル)を更新していないユーザを合わせると、パターンファイル(更新ファイル)の更新が適切ではないと考えられるユーザが、セキュリティ対策ソフトの利用者の23.3%を占める。

- ・ パターンファイル(更新ファイル)を更新しているユーザのうち、直近でのパターンファイル(更新ファイル)の更新時期について、「1ヶ月前」が3.6%、「2～3ヶ月前」が1.7%、「3ヶ月～半年前」が1.2%、「半年～1年前」が2.3%、「1年以上前」が0.1%となっており、更新時期が1ヶ月以上も遡るユーザはトータルで8.9%となっている。
- ・ 自分で新しいパターンファイル(更新ファイル)をダウンロードし、手動で実行しているユーザで、かつ、直近でのパターンファイル(更新ファイル)の更新時期が「分からない」と回答しているユーザが、パターンファイル(更新ファイル)を更新しているユーザの1.8%を占めている。

3.3.1 情報セキュリティ対策の実施状況(3)(P31)／3.3.1 情報セキュリティ対策の実施状況(4)(P32)参照

ユーザの知りたいセキュリティ情報の入手経路として、インターネットのニュース、掲示板が果たすべき役割が大きくなっているが、情報源や情報の信頼性や、情報源や情報量の過多を問題点として指摘する声も大きい。

- ・ セキュリティ情報の収集上の問題点として、「信頼できる情報源や情報であるかを見極めるのが難しい(45.2%)」、「情報源や情報量が多すぎるため、情報の取捨選択を行うのが難しい(40.3%)」が上位を占めている。

3.6.2 知りたいセキュリティ情報の入手経路(1)(P49)／3.6.3 セキュリティ情報の収集上の問題点(P51)参照

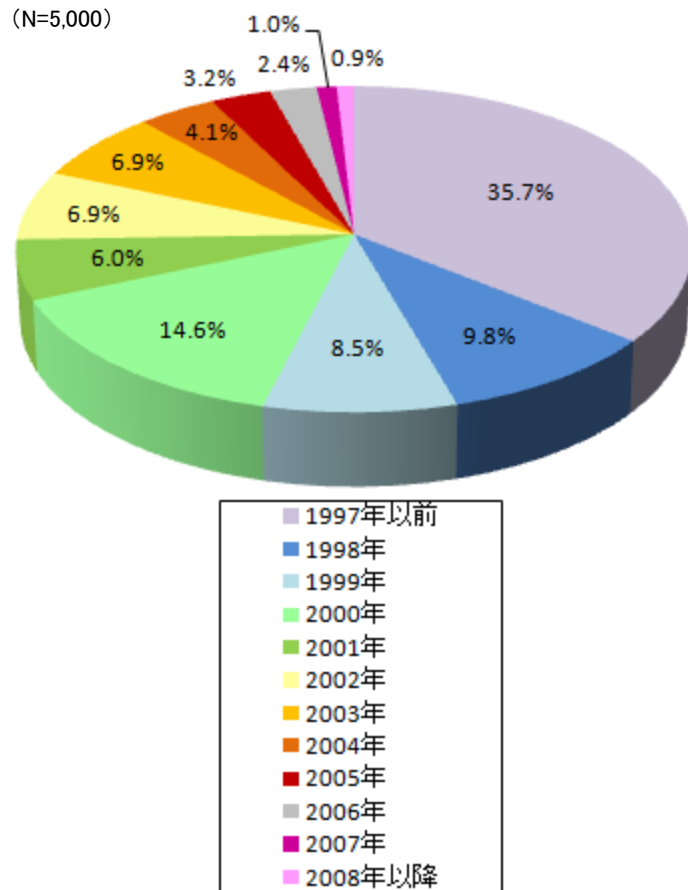
3. 調査結果

3. 1 PCインターネットの利用状況

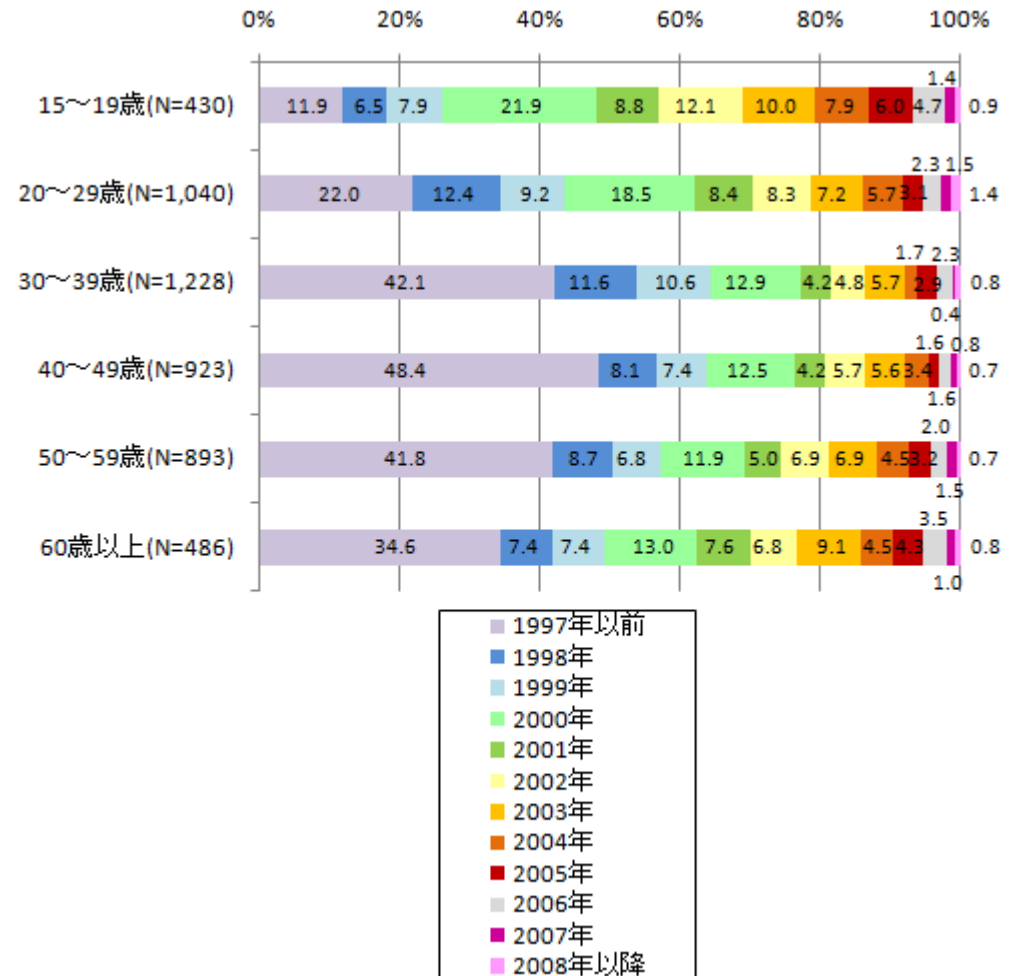
3.1.1 PCインターネットの利用開始時期

- ・ 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35.7%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81.4%を占めている。
- ・ 年代別にみると、40代では、「1997年以前」が約50%、30代、50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



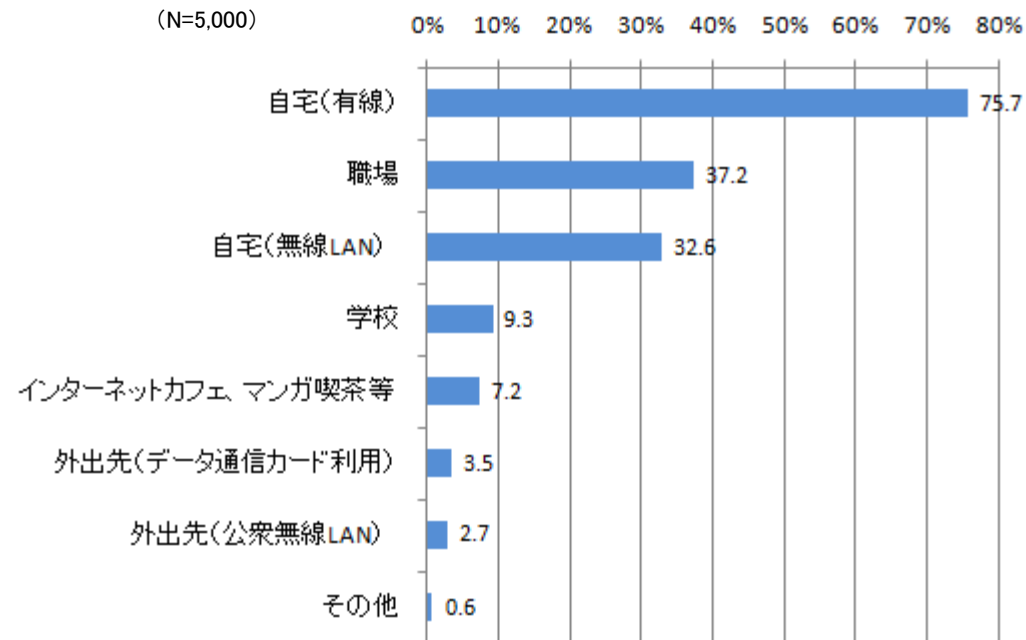
PCインターネットの利用開始時期
[年代別]



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75.7%、次いで「職場(37.2%)」、「(自宅(無線LAN)(32.6%)」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7.2%、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3.5%、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2.7%であり、僅少であった。

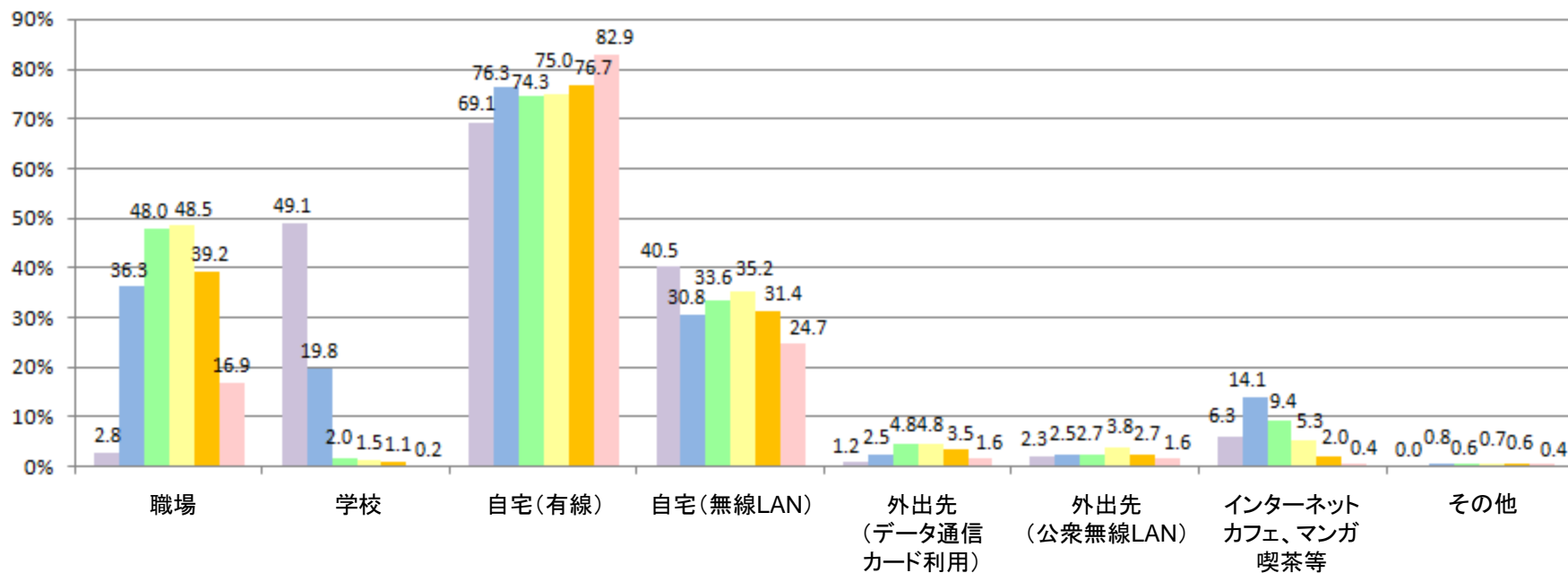
PCインターネットの利用場所



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14.1%と最も多く、次いで、30代が9.4%、10代が6.3%となっている。
- ・ 自宅(無線LAN)での利用は、10代が40.5%であり、20代から50代でも30%強となっている。

PCインターネットの利用場所
[年代別]

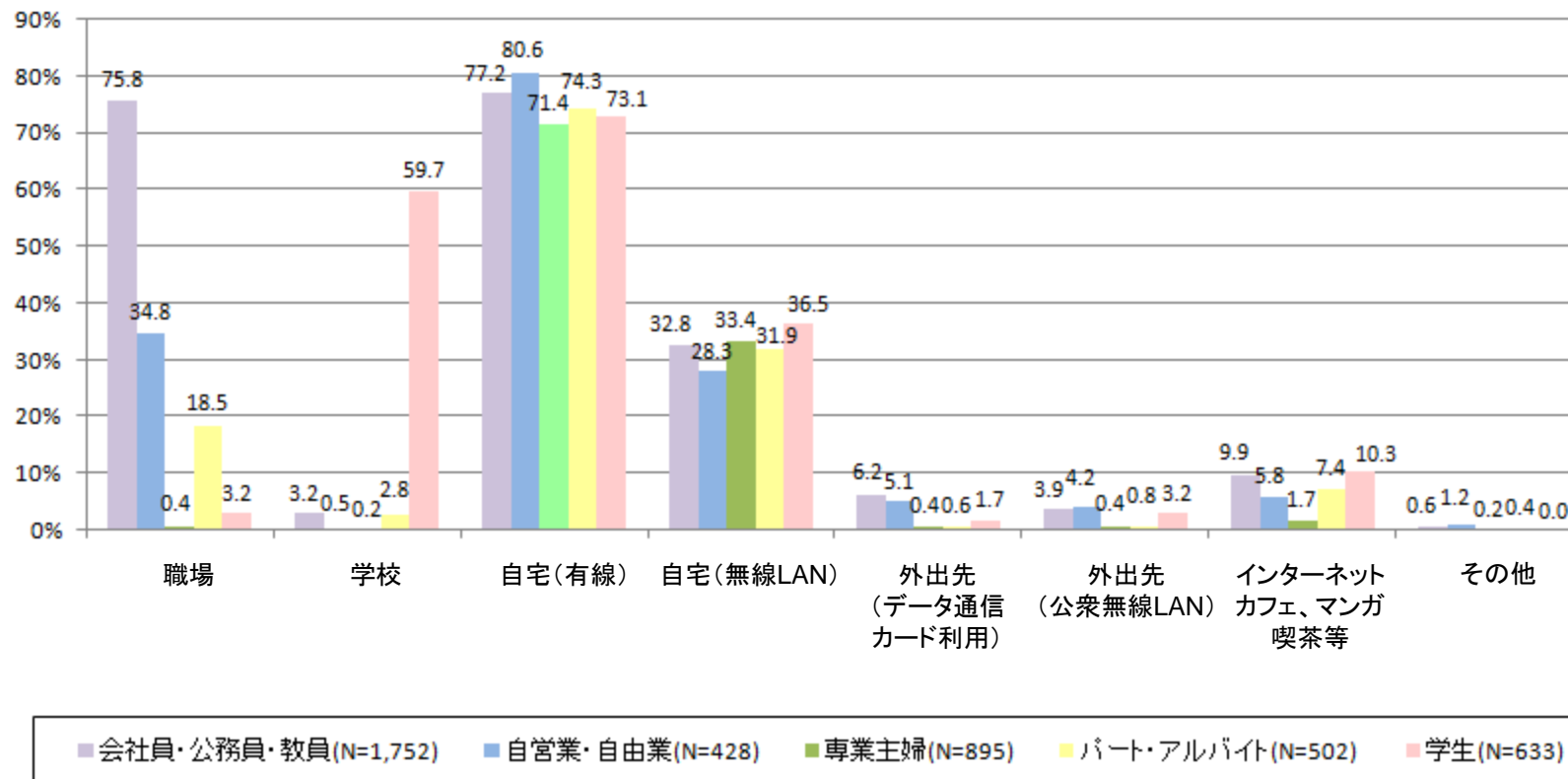


■ 15～19歳(N=430)
 ■ 20～29歳(N=1,040)
 ■ 30～39歳(N=1,228)
 ■ 40～49歳(N=923)
 ■ 50～59歳(N=893)
 ■ 60歳以上(N=486)

3.1.2 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36.5%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、学生が10.3%と最も多く、次いで会社員・公務員・教員が9.9%、パート・アルバイトが7.4%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。

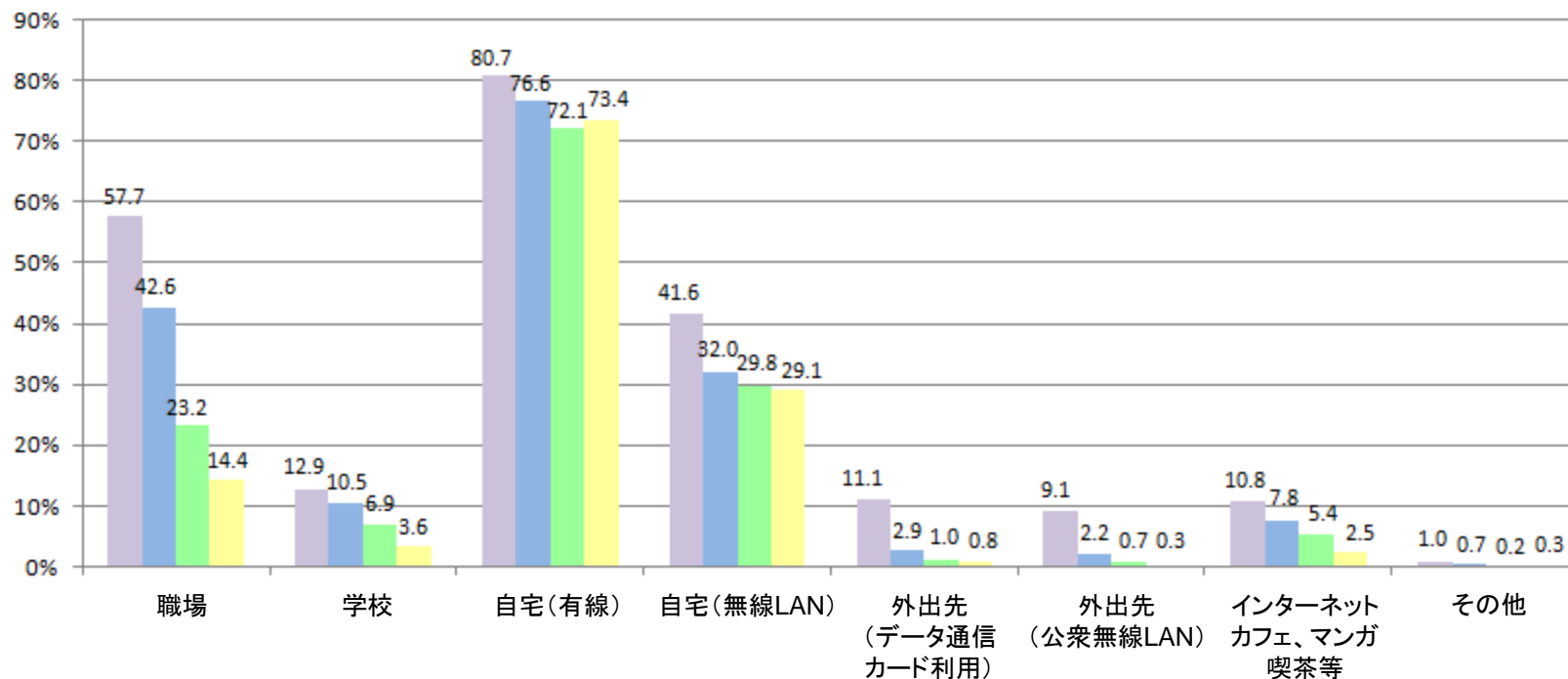
PCインターネットの利用場所
[職業別]



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]

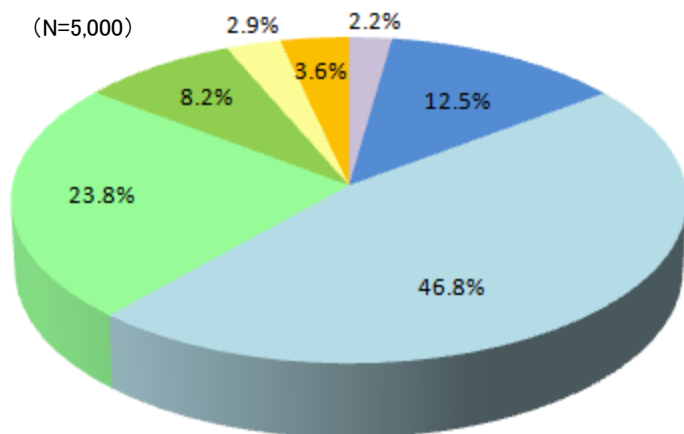


- パソコンを自分で組み立てたり、トラブルが起きても自分で解決できるレベルである(N=766)
- 必要なソフトウェアをインストールして使ったり、パソコンの設定を変えて使ったりすることができるレベルである(N=2,402)
- メールを使ったり、ホームページを閲覧したり、文章を書いたりするのに支障がないレベルである(N=1,471)
- パソコンの簡単な操作しか分からないレベルである(N=361)

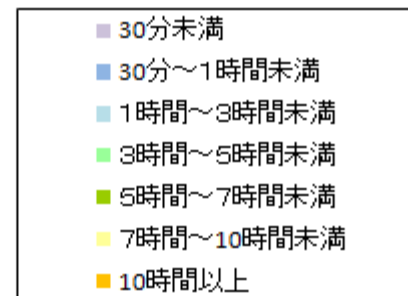
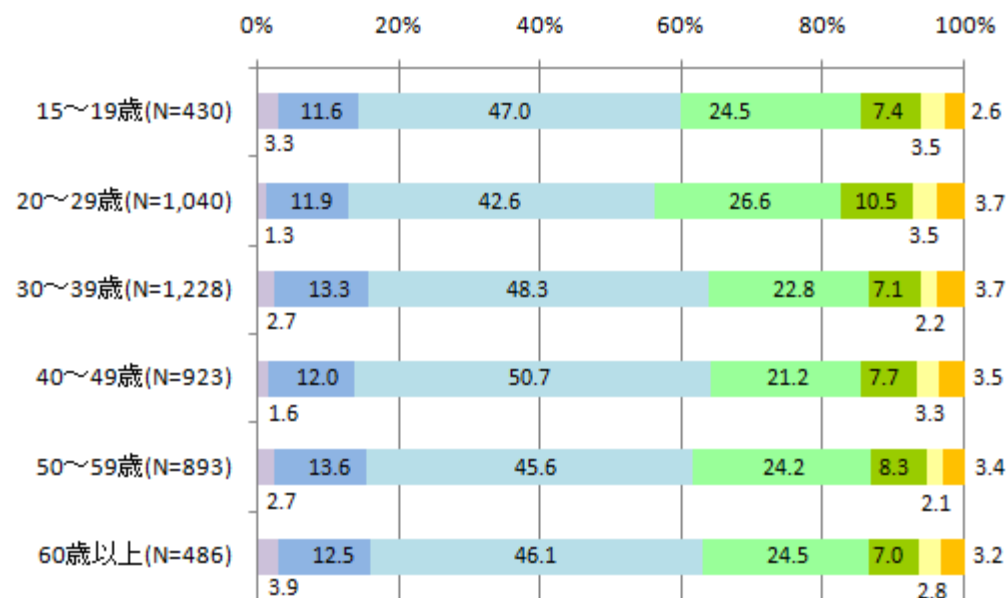
3.1.3 1日のPCインターネットの利用時間(仕事上での利用を除く)

- 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46.8%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)



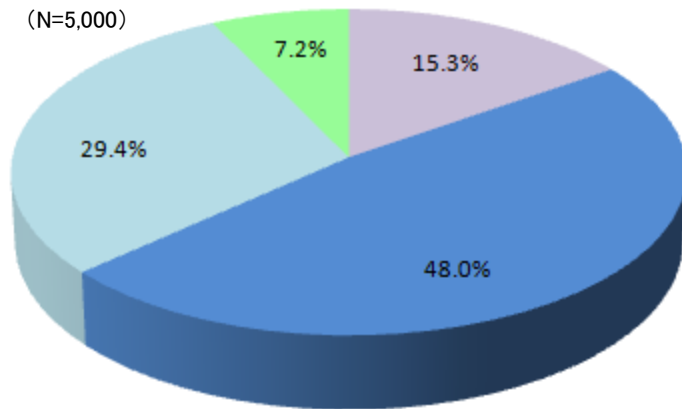
PCインターネットの利用時間(1日平均)
[年代別]



3.1.4 パソコンの習熟度(1)

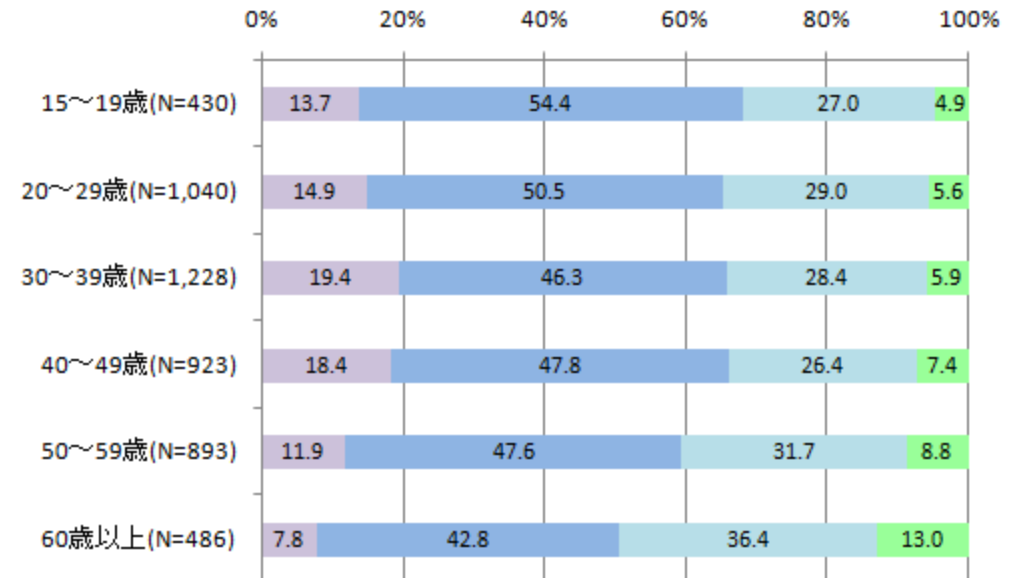
- ・ 回答者のパソコンの習熟度についてみると、最も多いのは、「必要なソフトウェアをインストールして使ったり、パソコンの設定を変えて使ったりすることができる」という上級レベルのユーザが48.0%、次いで、「メールを使ったり、ホームページを閲覧したり、文章を書いたりするのに支障がない」という中級レベルのユーザが29.4%となっている。
- ・ 「パソコンを自分で組み立てたり、トラブルが起きても自分で解決できる」という最上級レベルのユーザや、「パソコンの簡単な操作しか分からない」という初級レベルのユーザは比較的少数である。
- ・ 年代別にみると、最上級レベルのユーザが多いのは、30代である。60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



- 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

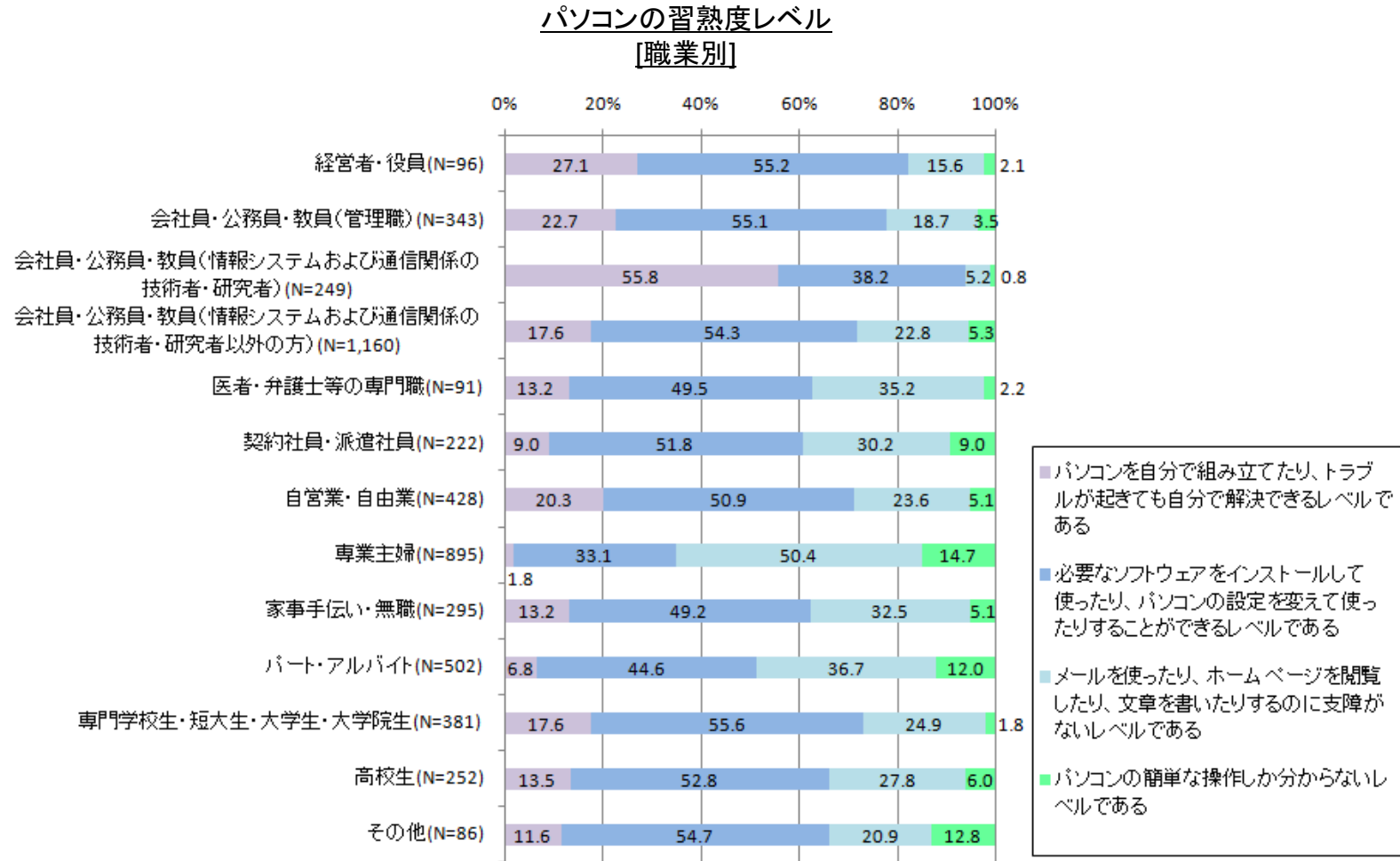
パソコンの習熟度レベル
[年代別]



- 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55.8%、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38.2%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1.8%、6.8%、上級レベルのユーザはそれぞれ33.1%、44.6%にとどまっている。

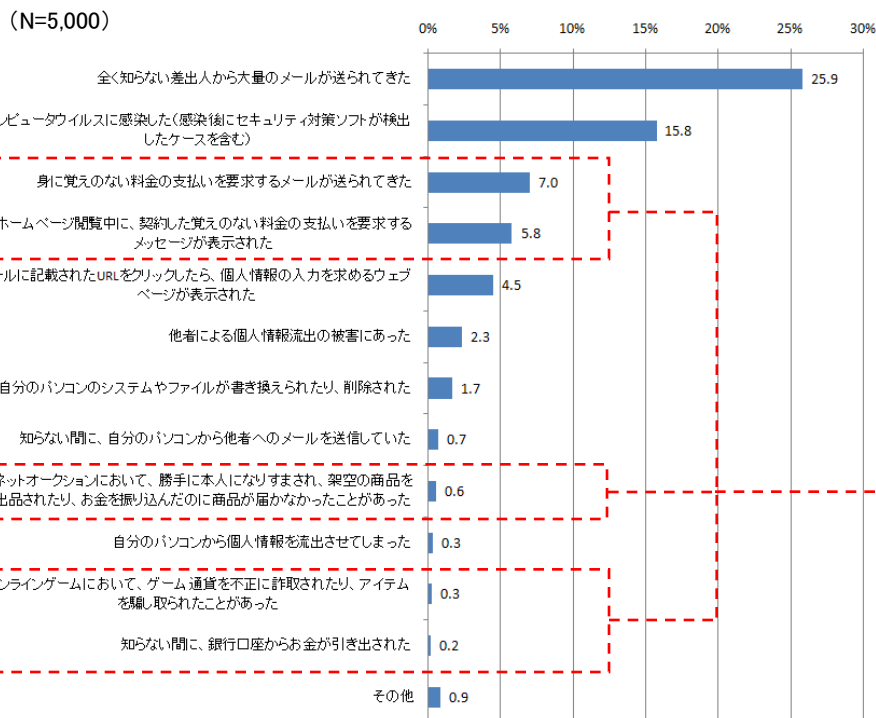


3. 2 情報セキュリティに関する脅威に対する被害状況

3.2.1 情報セキュリティに関する被害やトラブルの経験(1)

- ・ 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数は、2008年7月調査では825であったが、本調査では568にまで減少している。
- ・ その一方で、上記に示したユーザのうち、実際に金銭的な被害を被ったことがあるユーザの割合は、2008年7月調査の4.6%から、1.9ポイント上昇し、6.5%となっている。金銭的な被害につながる攻撃・脅威の手口が巧妙化していることを裏付ける結果となっている。

情報セキュリティに関する被害やトラブルの遭遇状況

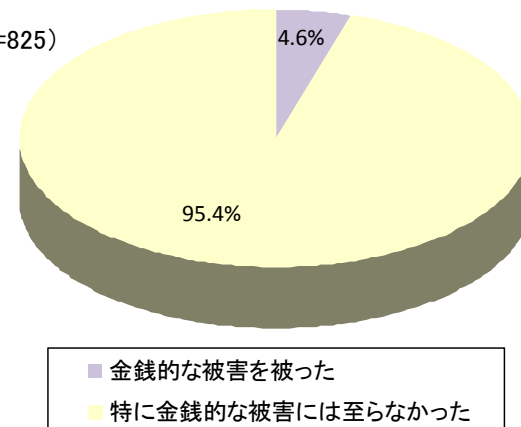


「」 金銭的な被害と関わりがある被害やトラブル

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の経験がある者]

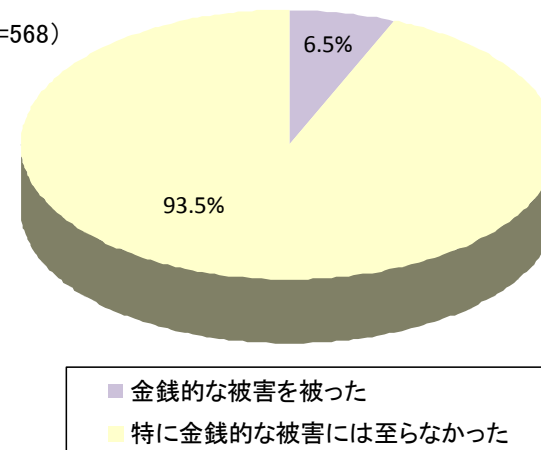
【2008年7月調査】

(N=825)



【本調査】

(N=568)

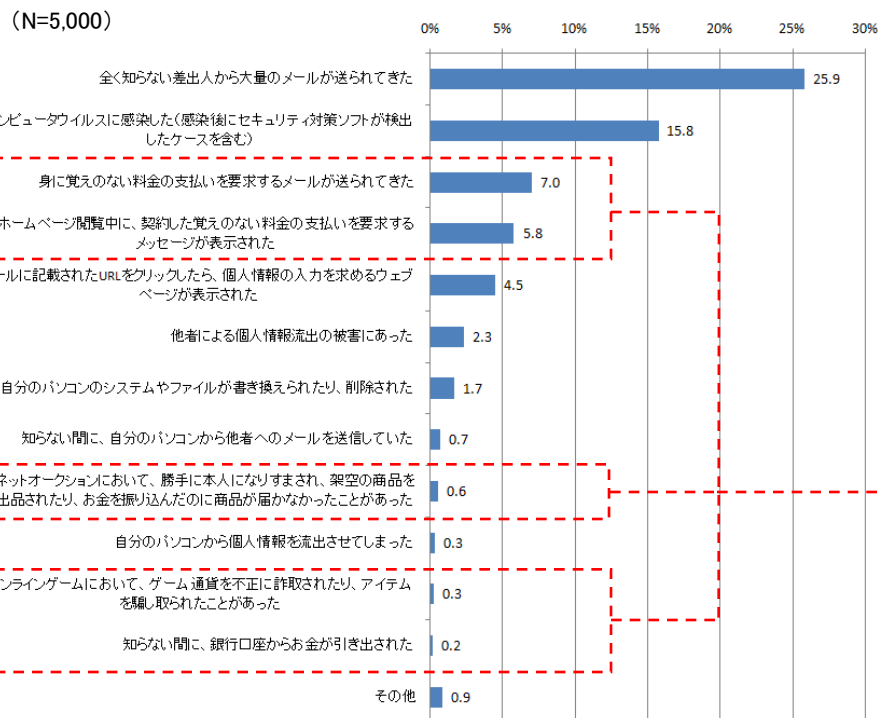


3.2.1 情報セキュリティに関する被害やトラブルの経験(2)

- 1 ユーザ当たりの被害金額は、2008年7月調査では平均被害金額約42,000円、最大被害金額500,000円であったが、本調査では平均被害金額約37,000円、最大被害金額300,000円となっている。
- 目標金額を引き下げること、ユーザが被害に遭う確率を高めようとする不正者の意図が感じられる内容となっている。

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

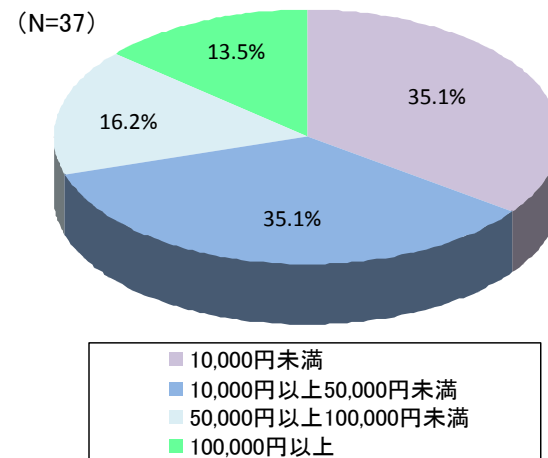
情報セキュリティに関する被害やトラブルの遭遇状況



〔 〕 金銭的な被害と関わりがある被害やトラブル

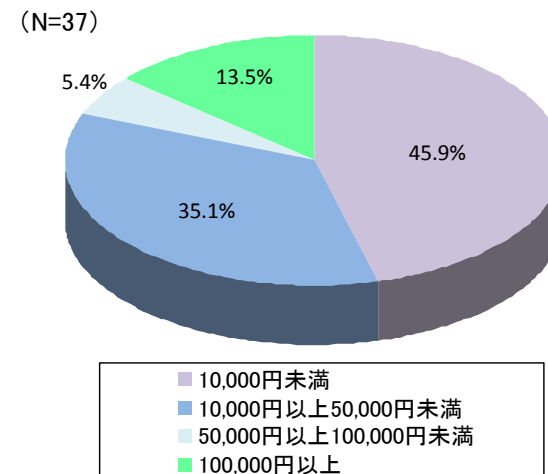
【2008年7月調査】

平均被害金額 約42,000円
最大被害金額 500,000円



【本調査】

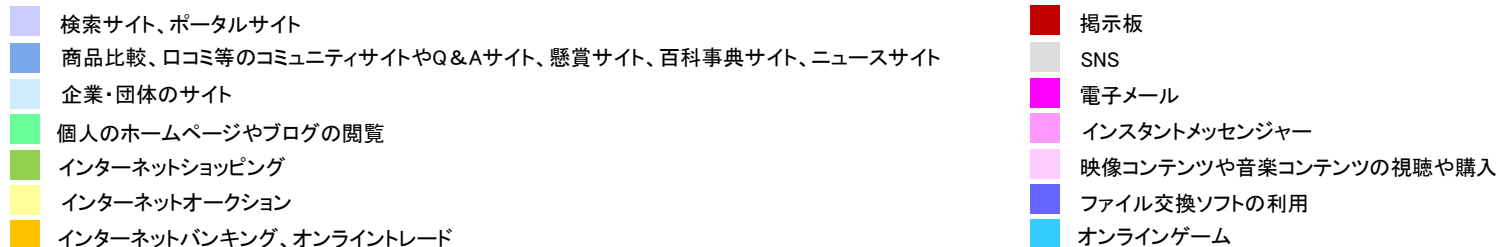
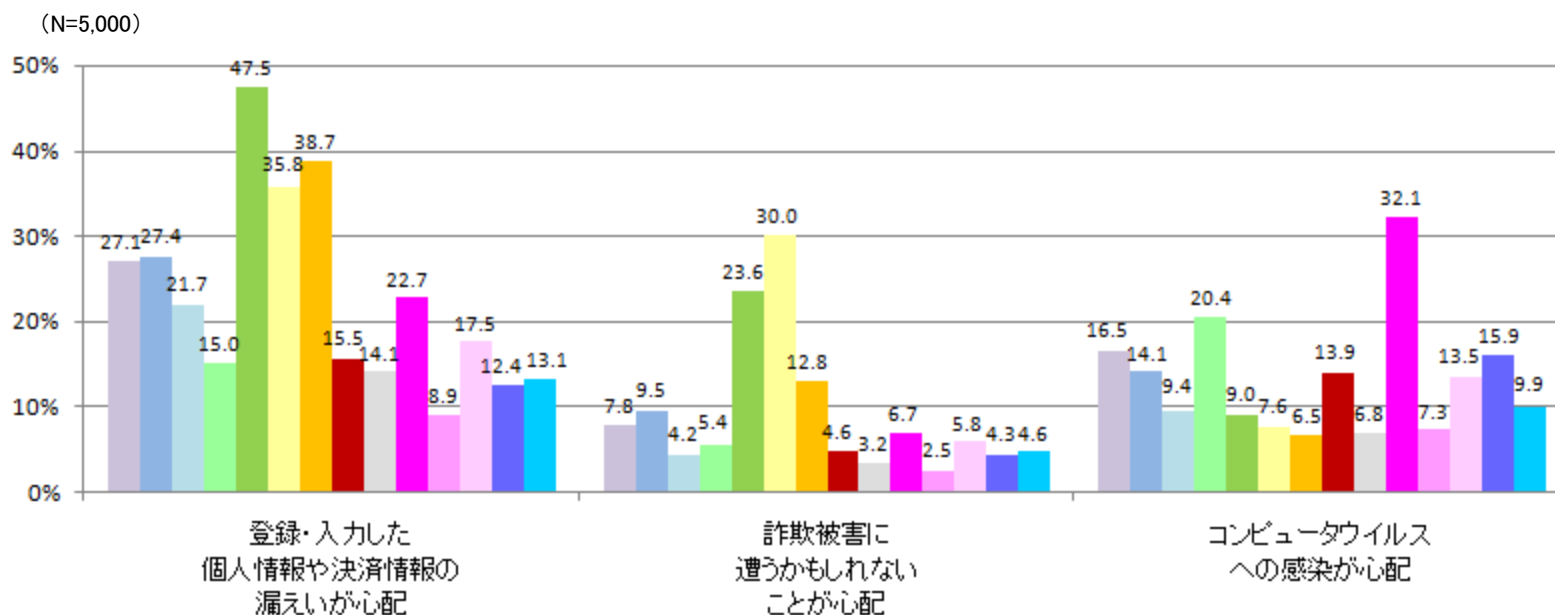
平均被害金額 約37,000円
最大被害金額 300,000円



3.2.2 サイト・サービスを利用する際のセキュリティ上の不安(1)

- ・「インターネットオークション」や「インターネットショッピング」、「インターネットバンキング、オンライントレード」については、利用する際のセキュリティ上の不安として、登録・入力した個人情報や決済情報の漏えいを心配するユーザや、詐欺被害に遭うかもしれないことを心配するユーザが多い。
- ・他方、「電子メール」や「個人のホームページやブログの閲覧」については、コンピュータウイルスへの感染が、利用する際のセキュリティ上の不安となっている。

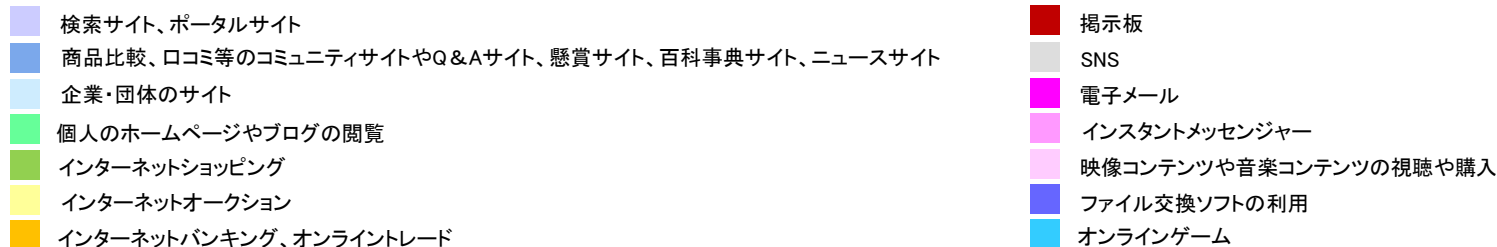
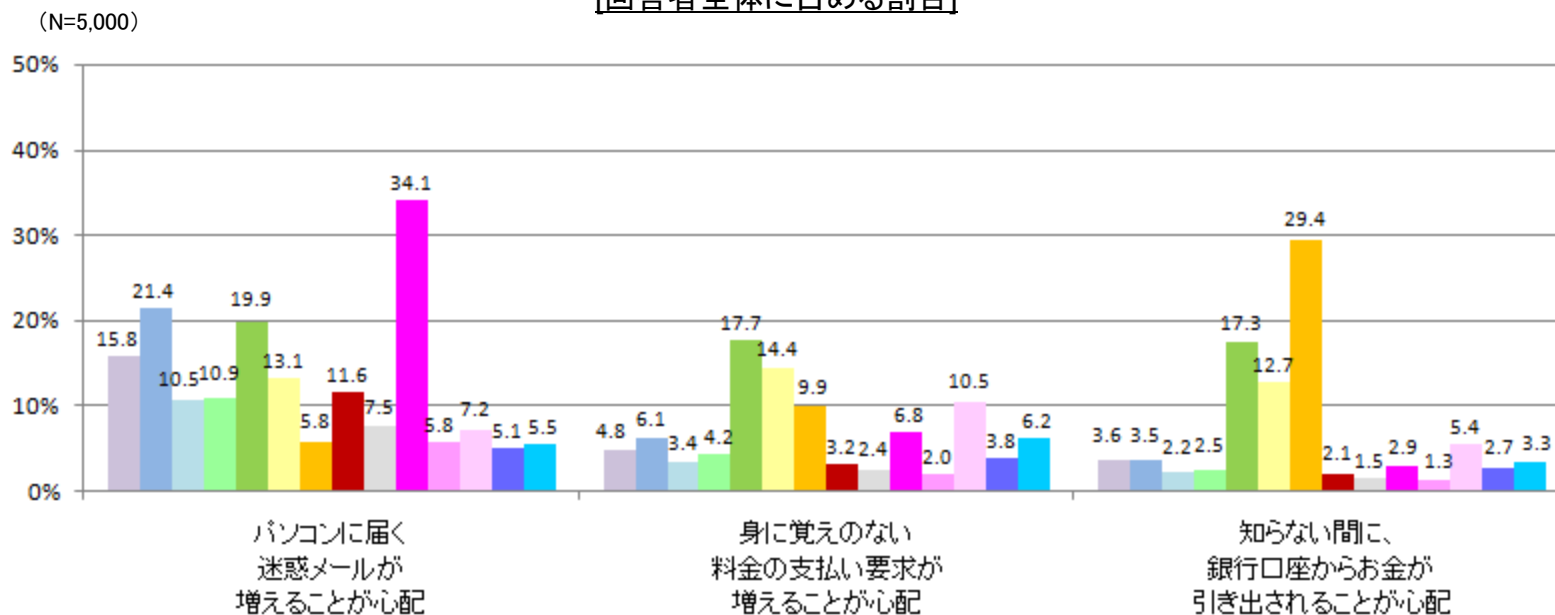
サイト・サービスを利用する際のセキュリティ上の不安
[回答者全体に占める割合]



3.2.2 サイト・サービスを利用する際のセキュリティ上の不安(2)

- ・「電子メール」の利用にあたって、パソコンに届く迷惑メールが増えることを心配しているユーザは全体の34.1%と最も多い。また、「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」や「インターネットショッピング」についても、全体の約20%のユーザが、セキュリティ上の不安として、「パソコンに届く迷惑メールが増えることが心配」を挙げている。
- ・他方、全体の約30%のユーザが、「インターネットバンキング、オンライントレード」を利用する際のセキュリティ上の不安として、「知らない間に、銀行口座からお金が引き出されることが心配」を挙げている。

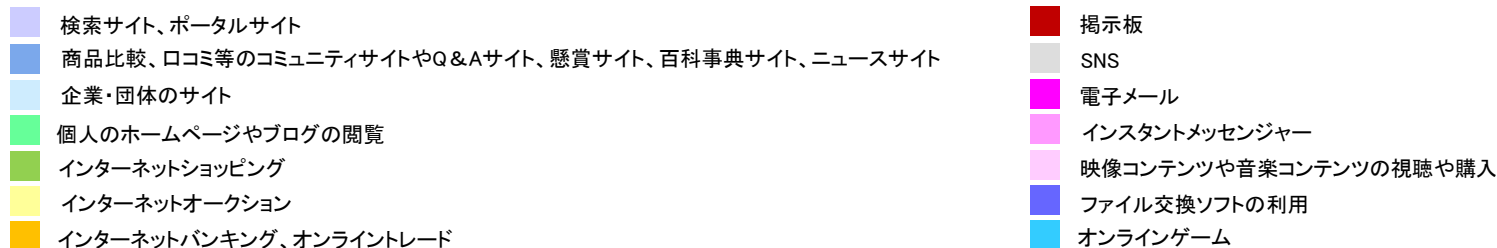
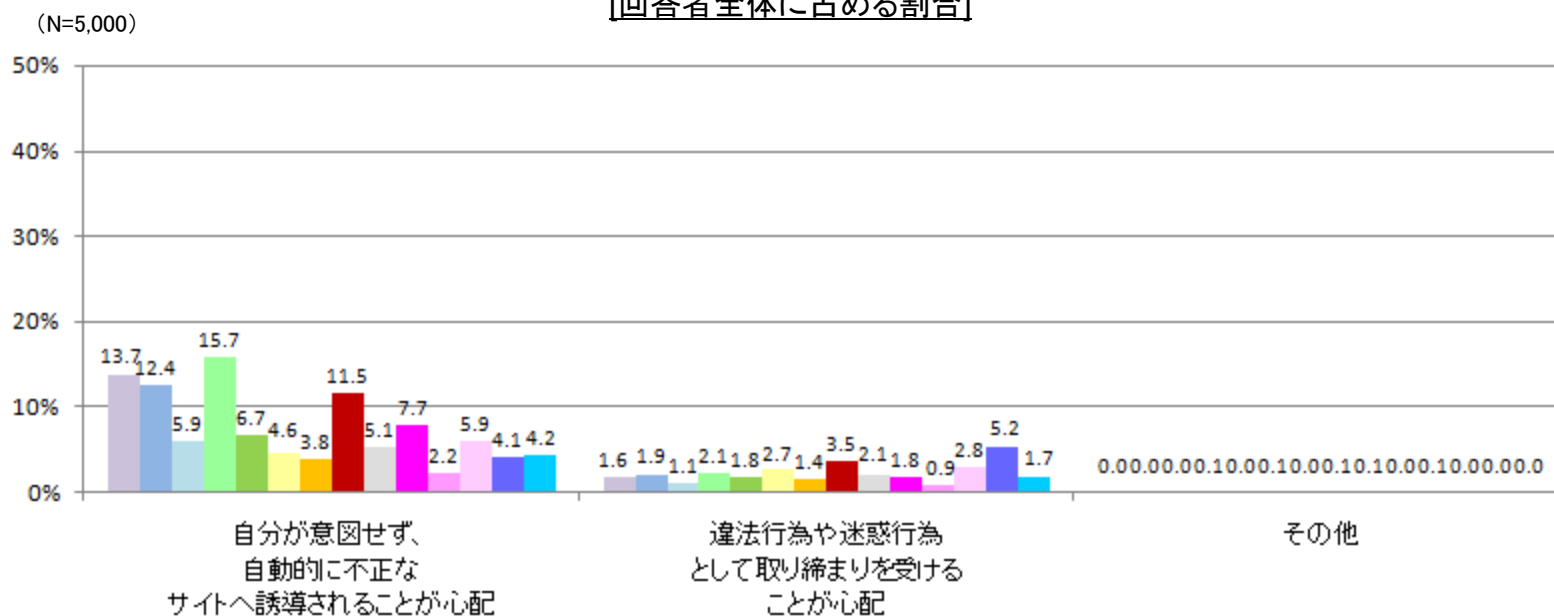
サイト・サービスを利用する際のセキュリティ上の不安
[回答者全体に占める割合]



3.2.2 サイト・サービスを利用する際のセキュリティ上の不安(3)

- ・ 自分が意図せず、自動的に不正なサイトへ誘導されることが心配なサイト・サービスとしては、「個人のホームページやブログの閲覧(15.7%)」、「検索サイト、ポータルサイト(13.7%)」、「商品比較、ロ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(12.4%)」が上位を占める。
- ・ 他方、違法行為や迷惑行為として取り締まりを受けることが心配なサイト・サービスとしては、「ファイル交換ソフトの利用」が5.2%と最も多い。

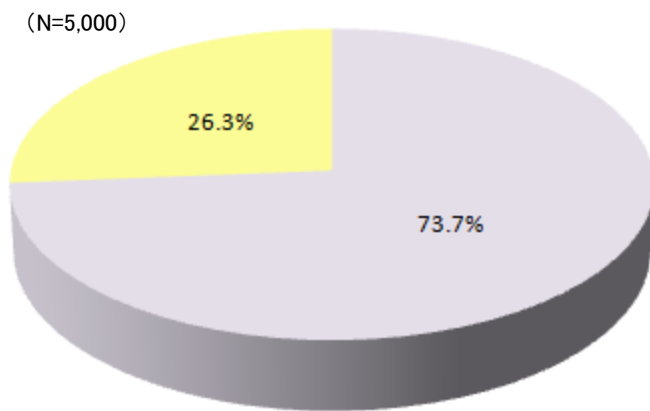
サイト・サービスを利用する際のセキュリティ上の不安
[回答者全体に占める割合]



3.2.3 スпамメールの受信状況(1)

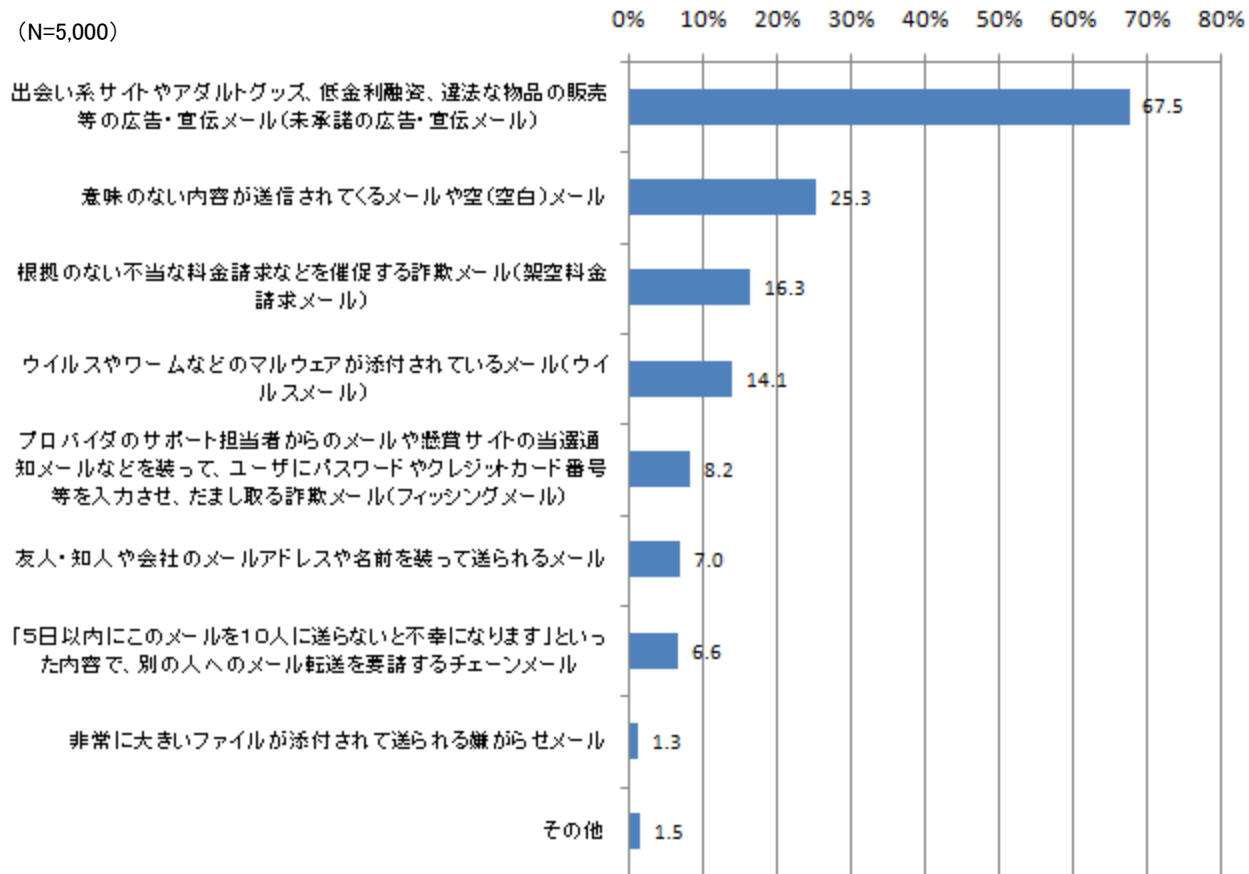
- ・ スпамメールを受信したことがあるユーザは、全体の73.7%である。なかでも特に、「出会い系サイトやアダルトグッズ、低金利融資、違法な物品の販売等の広告・宣伝メール」は、受信者の割合が67.5%と最も高い。
- ・ また、架空料金請求メール、ウイルスメール、フィッシングメールの受信者の割合は、それぞれ16.3%、14.1%、8.2%となっている。

スパムメールの受信経験の有無



- スпамメールを受け取ったことがある
- スпамメールを受け取ったことがない

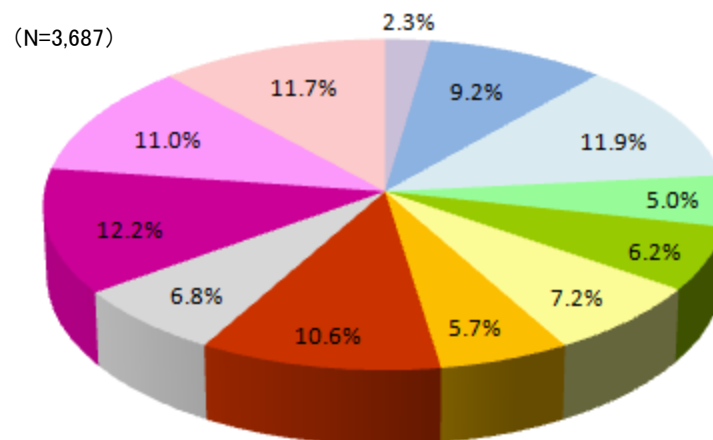
スパムメールの受信状況



3.2.3 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通以上スパムメールを受信しているユーザが全体の約4分の1を占めている。
- ・ 他方、スパムメールの受信数が比較的に少ないユーザについては、「ほとんどない(11.7%)」、「週に1～5通程度(11.0%)」、「毎日1～5通(12.2%)」を合わせると、全体の約3分の1を占めている。

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]



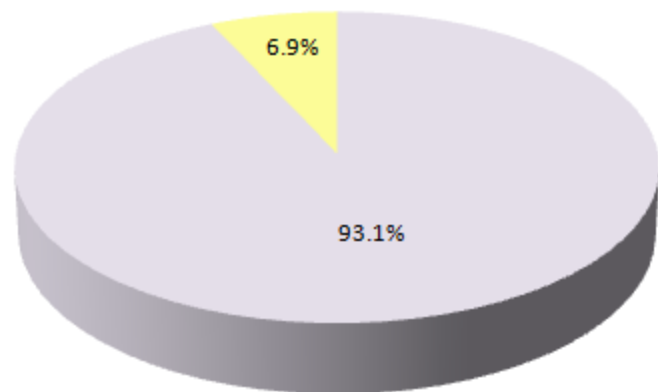
3.3 情報セキュリティに関する脅威に対する対策状況

3.3.1 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93.1%であり、残りの6.9%は対策を未着手である。
- ・ 実施率が高い情報セキュリティ対策としては、「不審な電子メールの添付ファイルは開かない(80.6%)」、「怪しいと思われるウェブサイトにはアクセスしない(80.0%)」、「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(78.0%)」といった注意行動が上位を占める。
- ・ ユーザの約4人に3人は、「セキュリティ対策ソフトの導入・活用」、「Windows Update等によるセキュリティパッチの更新」を実施しているが、依然として、約4人に1人がそれらの対策を実施していない危険なユーザとなっている。
- ・ 「パスワードの定期的な更新」を行っているユーザは、全体の約40%にとどまっている。

情報セキュリティ対策の実施の有無

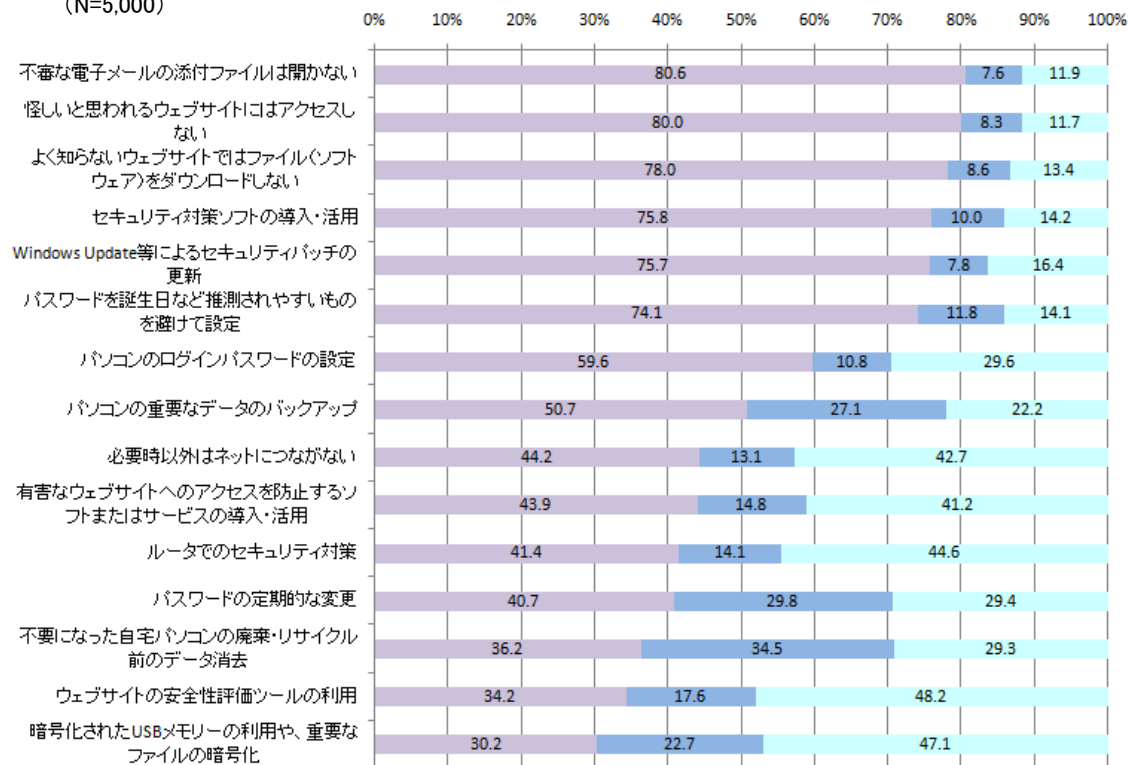
(N=5,000)



■ 実施している ■ 特に実施していない

情報セキュリティ対策の実施状況

(N=5,000)



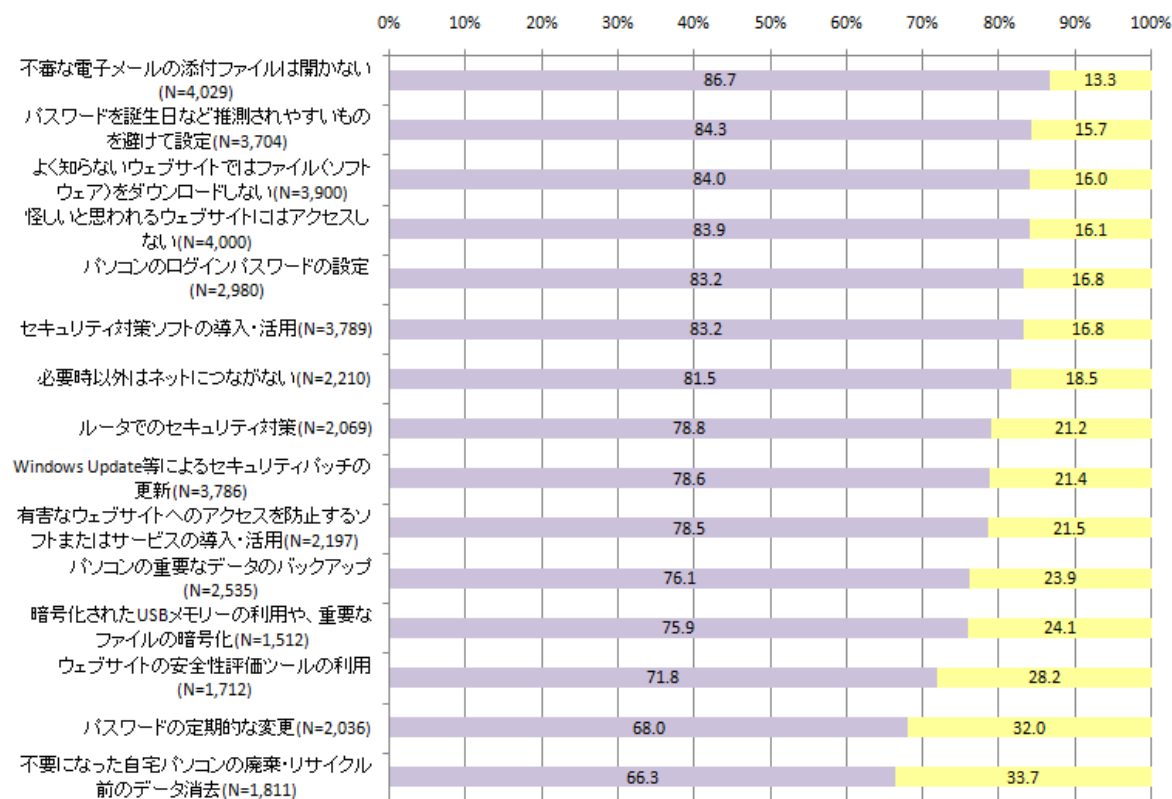
■ 実施している ■ 現在実施はしていないが、今後実施する予定である ■ 現在も、今後も実施する予定はない

3.3.1 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の満足度についてみると、「セキュリティ対策ソフトの導入・活用」、「Windows Update等によるセキュリティパッチの更新」の満足度については、それぞれ83.2%、78.6%と比較的高くなっている。
- ・ 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(66.3%)」や「パスワードの定期的な変更(68.0%)」、「ウェブサイトの安全性評価ツールの利用(71.8%)」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]



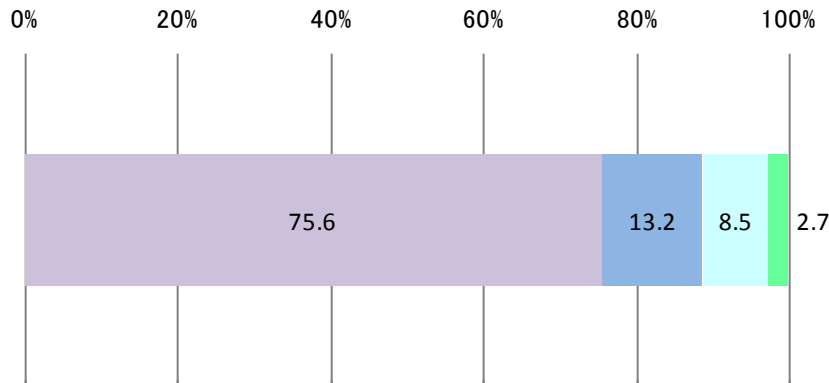
■ 満足である ■ 不満である

3.3.1 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を導入しているユーザの10%強が、パターンファイル(更新ファイル)を更新していない、もしくはパターンファイル(更新ファイル)を更新しているかどうか分からない状況である。
- ・パターンファイル(更新ファイル)の更新状況について製品版とフリー版のセキュリティ対策ユーザを比較すると、自動更新機能を設定しているユーザの割合については、フリー版の方が製品版に比べて高く、また、パターンファイル(更新ファイル)を更新していない、もしくはパターンファイル(更新ファイル)を更新しているかどうか分からないユーザの割合については、フリー版の方が製品版に比べて低くなっている。

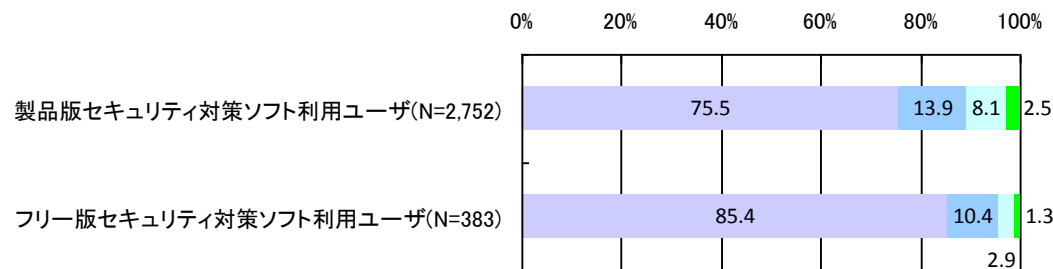
パターンファイルの更新状況
[セキュリティ対策ソフトの利用者に占める割合]

(N=3,789)



- 何もしなくても新しいパターンファイル(更新ファイル)が更新されるように、自動更新機能を設定している
- 自分で新しいパターンファイル(更新ファイル)をダウンロードし、手動で実行している
- パターンファイル(更新ファイル)を更新しているかどうか分からない
- パターンファイル(更新ファイル)を更新していない

パターンファイルの更新状況
[製品版/フリー版セキュリティ対策ソフトの利用者に占める割合]



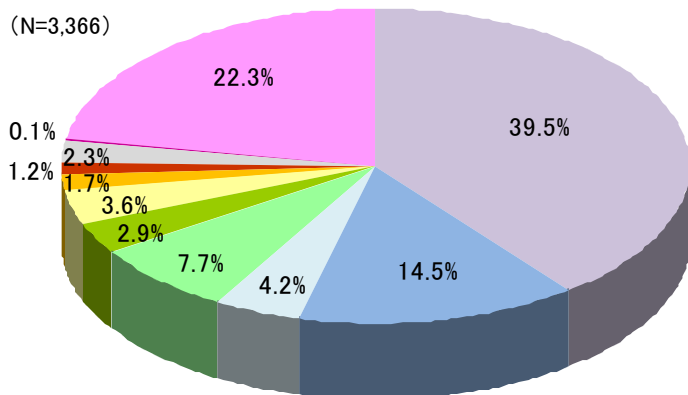
- 何もしなくても新しいパターンファイル(更新ファイル)が更新されるように、自動更新機能を設定している
- 自分で新しいパターンファイル(更新ファイル)をダウンロードし、手動で実行している
- パターンファイル(更新ファイル)を更新しているかどうか分からない
- パターンファイル(更新ファイル)を更新していない

注)「製品版セキュリティ対策ソフト」については、トレンドマイクロ、シマンテック、ソースネクスト、マカフィー、アンラボ、カスペルスキーの6社が提供元となっているセキュリティ対策ソフトを対象としている。「フリー版セキュリティ対策ソフト」については、ALWIL Software a.s.、AVG Technologies、Avira GmbHの3社が提供元となっているセキュリティ対策ソフトを対象としている。

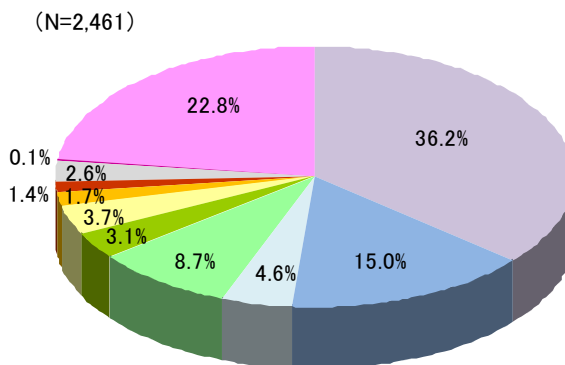
3.3.1 情報セキュリティ対策の実施状況(4)

- ・ パターンファイル(更新ファイル)を更新しているユーザのうち、直近でパターンファイル(更新ファイル)を更新した時期が1ヶ月以上も遡るユーザは8.9%、手動で更新しているにもかかわらずパターンファイル(更新ファイル)の更新時期が分からないユーザは1.8%存在している。双方を合わせて、パターンファイル(更新ファイル)の更新が適切ではないと考えられるユーザが10%強含まれている。
- ・ 直近でのパターンファイル(更新ファイル)の更新時期について製品版とフリー版のセキュリティ対策ユーザを比較すると、更新時期が1日前、もしくは2～3日前であるユーザの割合については、製品版が51.2%に対してフリー版は73.0%と20ポイント以上高くなっている。

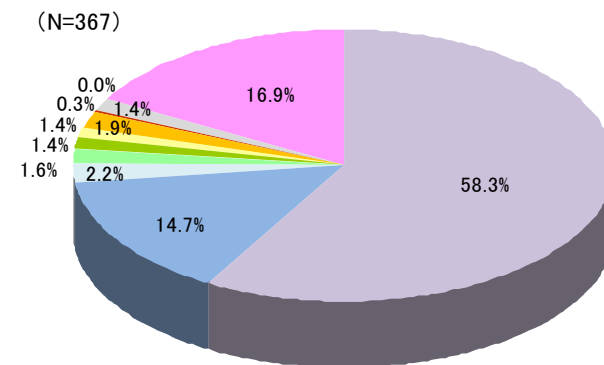
直近でのパターンファイルの更新時期
[パターンファイル(更新ファイル)の更新者に占める割合]



直近でのパターンファイルの更新時期
[製品版セキュリティ対策ソフトのパターンファイル(更新ファイル)の更新者に占める割合]



直近でのパターンファイルの更新時期
[フリー版セキュリティ対策ソフトのパターンファイル(更新ファイル)の更新者に占める割合]

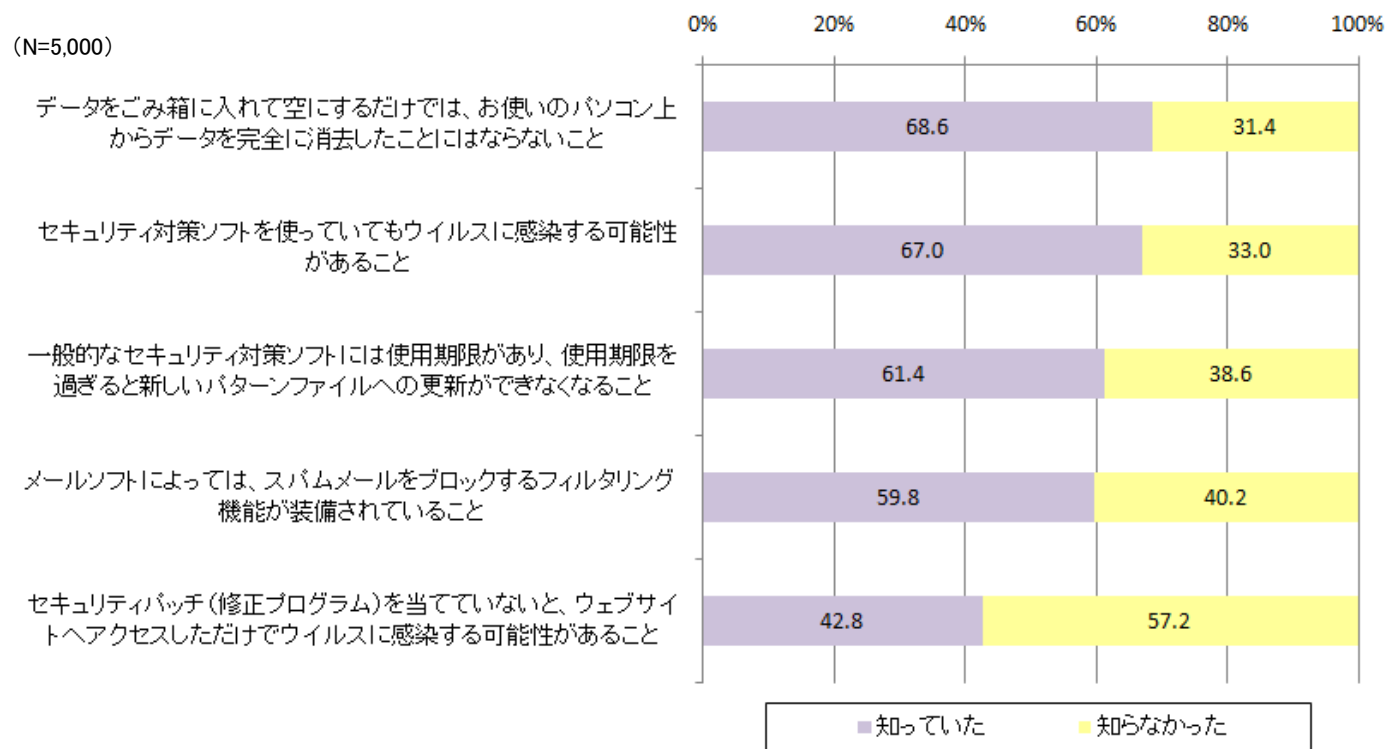


注)「製品版セキュリティ対策ソフト」については、トレンドマイクロ、シマンテック、ソースネクスト、マカフィー、アンラボ、カスペルスキーの6社が提供元となっているセキュリティ対策ソフトを対象としている。「フリー版セキュリティ対策ソフト」については、ALWIL Software a.s.、AVG Technologies、Avira GmbHの3社が提供元となっているセキュリティ対策ソフトを対象としている。

3.3.1 情報セキュリティ対策の実施状況(5)

- ・「データをごみ箱に入れて空にするだけでは、データを完全に消去したことにはならないこと」や「セキュリティ対策ソフトを使ってもウイルスに感染する可能性があること」については、ユーザの約3人に1人が認知していない。
- ・「セキュリティパッチ(修正プログラム)を当てていないと、ウェブサイトへアクセスしただけでウイルスに感染する可能性があること」について知らないユーザが、全体の半数を大きく上回っている。

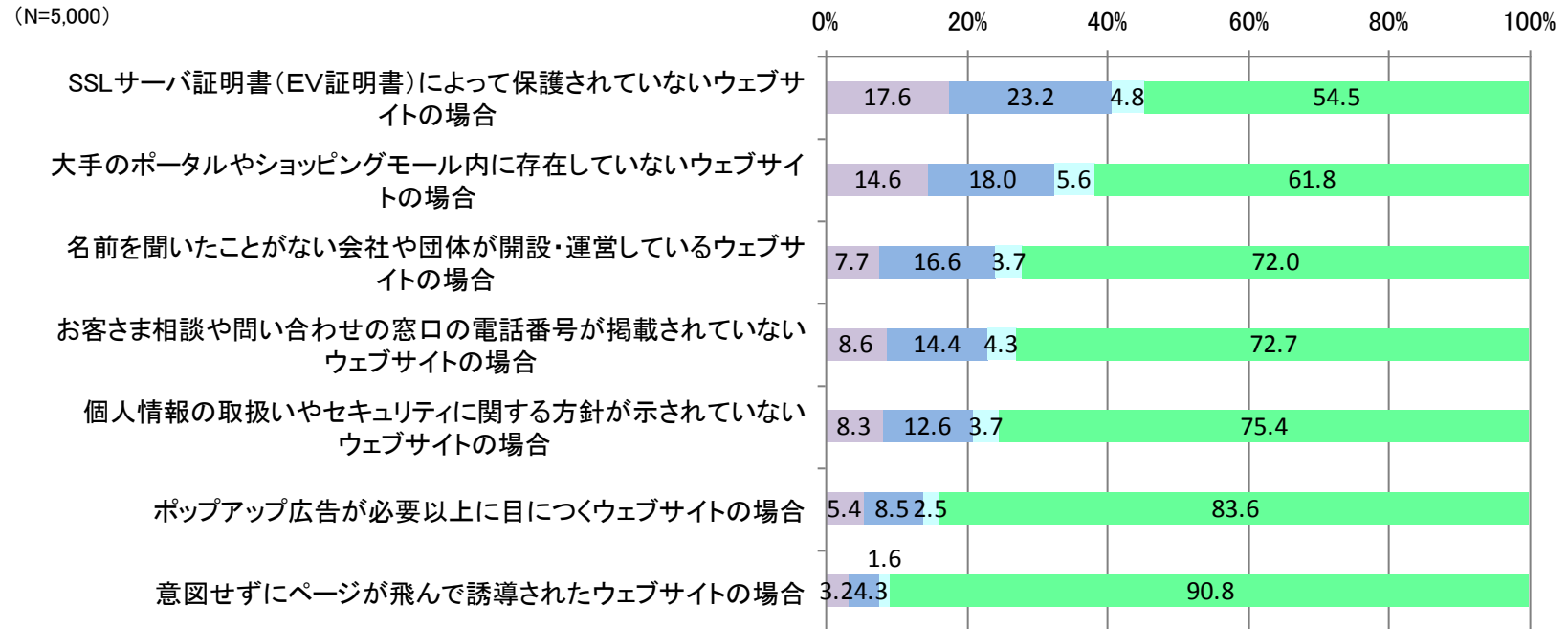
情報セキュリティ対策に関する事象の認知状況



3.3.2 ユーザ情報の管理状況(1)

- ・ ユーザが敬遠して、個人情報や決済情報について一切登録・入力を行わないウェブサイトの条件としては、「意図せずにページが飛んで誘導されたウェブサイト(90.8%)」や「ポップアップ広告が必要以上に目につくウェブサイト(83.6%)」が上位を占める。
- ・ 全体の50%弱のユーザが、SSLサーバ証明書(EV証明書)によって保護されていないウェブサイト上で、個人情報あるいは決済情報の登録・入力を行っている。

ウェブサイト上でユーザ情報(個人情報、決済情報)の登録・入力を
要請された場合の対応

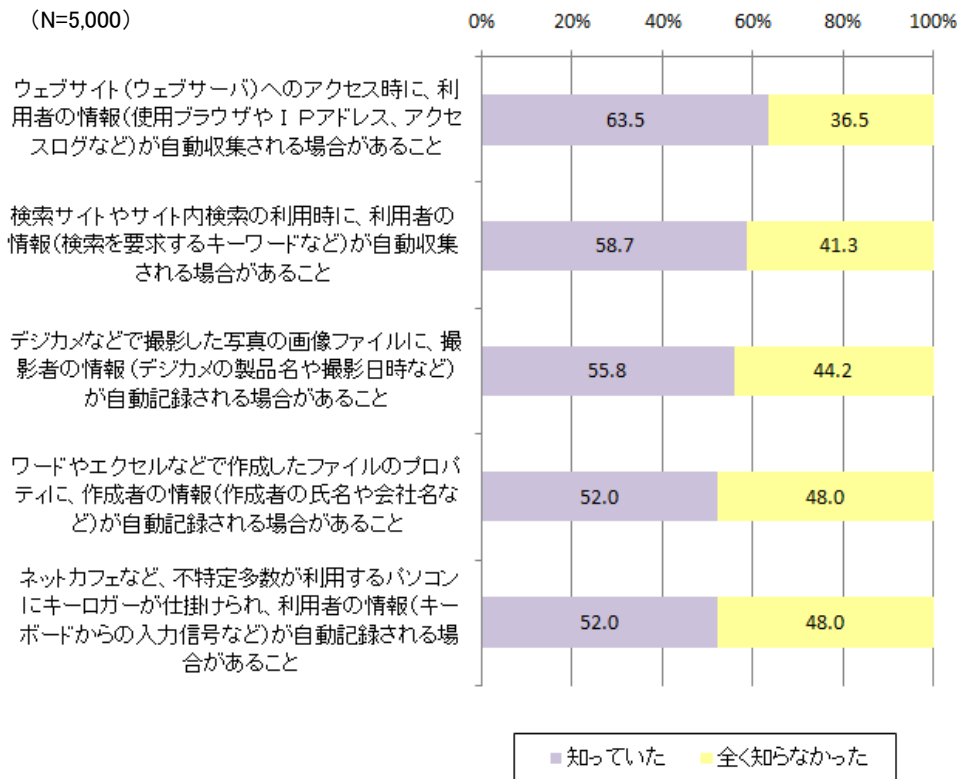


- 個人情報であるか、決済情報であるかは特に気にせず登録・入力している
- 個人情報のみ、登録・入力している
- 決済情報のみ、登録・入力している
- 一切登録・入力をしていない

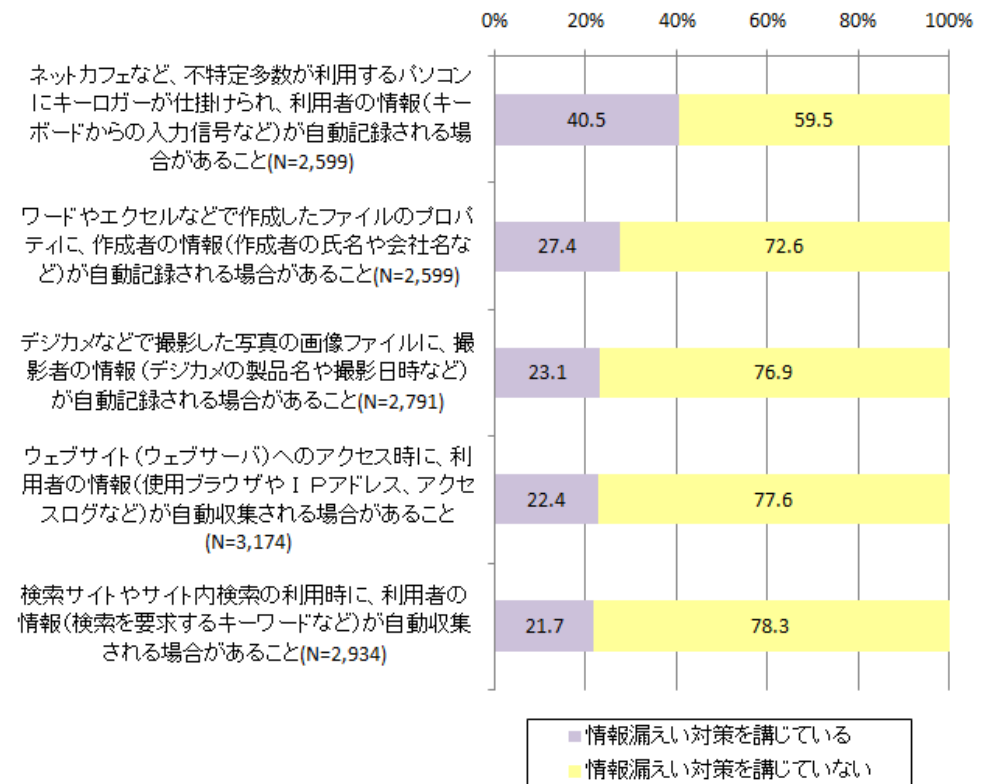
3.3.2 ユーザ情報の管理状況(2)

- 「ワードやエクセルなどで作成したファイルのプロパティに、作成者の情報が自動記録される場合があること」や「ネットカフェなど、不特定多数が利用するパソコンにキーロガーが仕掛けられ、キーボードからの入力信号などの利用者の情報が自動記録される場合があること」については、約半数のユーザに認知されていないのが現状である。
- 「検索サイトやサイト内検索の利用時に、検索を要求するキーワードなどの利用者の情報が自動収集される場合があること」についても、ユーザの約40%に知られていない。

ユーザ情報が記録・収集される箇所に対する認知状況



情報漏えいを防ぐための対策の実施状況
[ユーザ情報が記録・収集される箇所を認知していた者に占める割合]



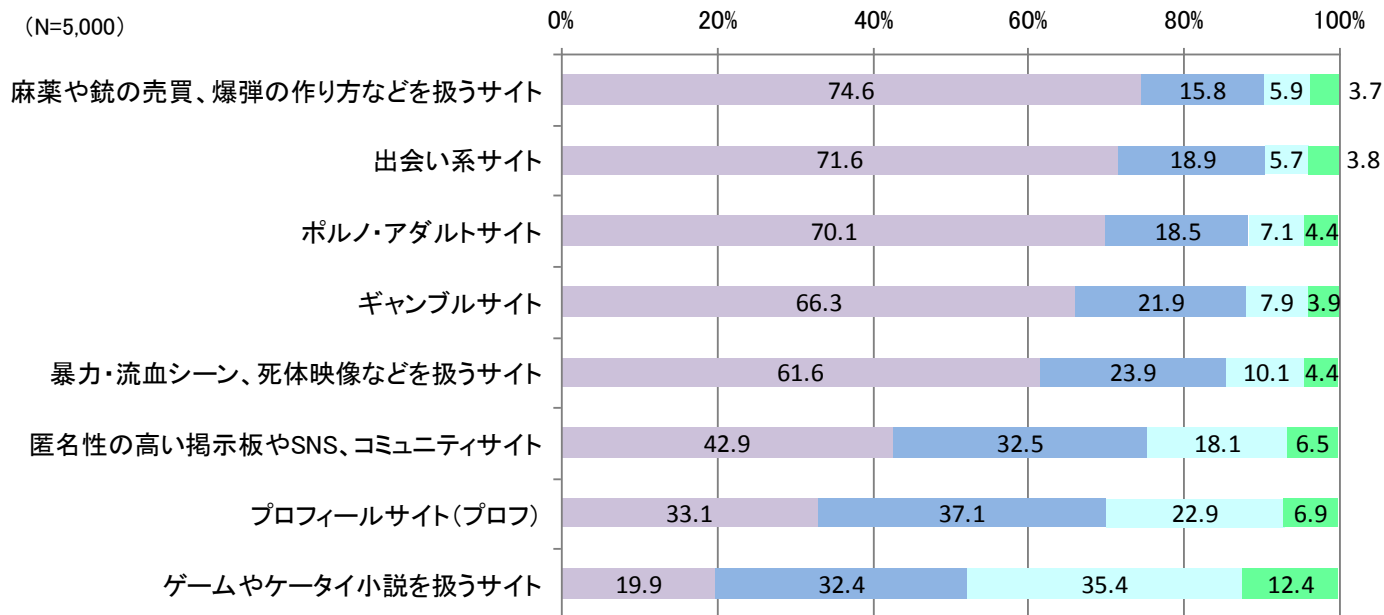
3.3.3 違法・有害サイト対策(1)

- 子どもたちに危害が及ぶことを避けるために、できる限り厳しくアクセスを制限すべきであると考えているユーザの割合(「Aの考えに近いと思う」と「どちらかといえば、Aの考えに近いと思う」を足し合わせた割合)としては、「麻薬や銃の売買、爆弾の作り方などを扱うサイト(90.4%)」や「出会い系サイト(90.5%)」、「ポルノ・アダルトサイト(88.6%)」が上位を占める。
- 「匿名性の高い掲示板やSNS、コミュニティサイト」、「プロフィールサイト(プロフ)」、「ゲームやケータイ小説を扱うサイト」についても、同割合はそれぞれ75.4%、70.2%、52.3%と比較的高い。

違法・有害サイトへの対応についての考え

【Aの考え】 子どもたちに危害が及ぶことを避けるため、できる限り厳しくアクセスを制限すべきだと思う

【Bの考え】 子どもたちがリスクについて学ぶことも重要であるため、(厳しく)アクセスを制限するべきではないと思う



- Aの考えに近いと思う
- どちらかといえば、Aの考えに近いと思う
- どちらかといえば、Bの考えに近いと思う
- Bの考えに近いと思う

3.3.3 違法・有害サイト対策(2)

- ユーザ全体と比べて、小学生未満、小学生、中学生の子どもがいるユーザでは、子どもたちに危害が及ぶことを避けるために、できる限り厳しくアクセスを制限するべきであるという意識がより強い。

違法・有害サイトへの対応についての考え

【Aの考え】 子どもたちに危害が及ぶことを避けるため、できる限り厳しくアクセスを制限するべきだと思う

【Bの考え】 子どもたちがリスクについて学ぶことも重要であるため、(厳しく)アクセスを制限するべきではないと思う

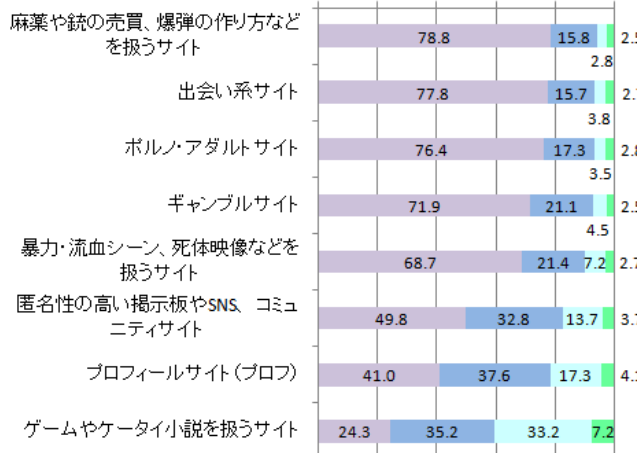
[小学生未満の子どもがいる者に占める割合]

[小学生の子どもがいる者に占める割合]

[中学生の子どもがいる者に占める割合]

(N=707)

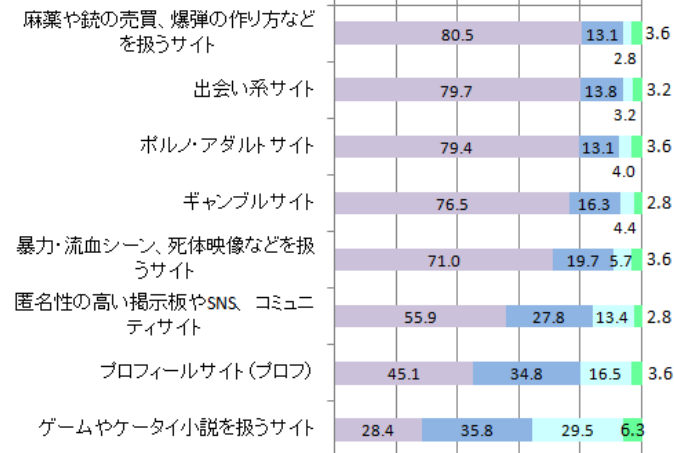
0% 20% 40% 60% 80% 100%



■ Aの考えに近いと思う
 ■ どちらかといえば、Aの考えに近いと思う
 ■ どちらかといえば、Bの考えに近いと思う
 ■ Bの考えに近いと思う

(N=528)

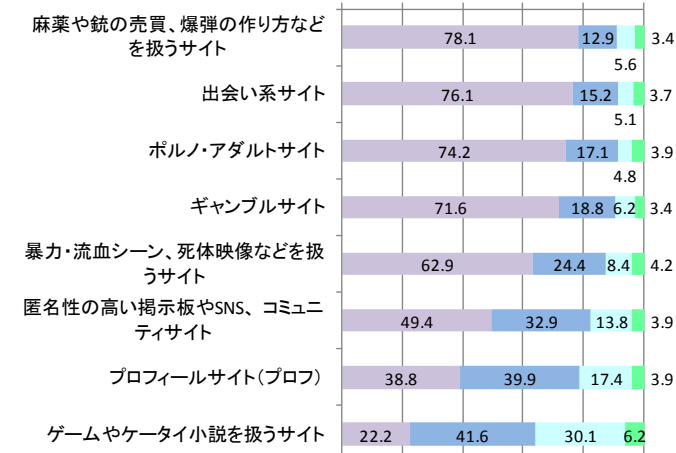
0% 20% 40% 60% 80% 100%



■ Aの考えに近いと思う
 ■ どちらかといえば、Aの考えに近いと思う
 ■ どちらかといえば、Bの考えに近いと思う
 ■ Bの考えに近いと思う

(N=356)

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



■ Aの考えに近いと思う
 ■ どちらかといえば、Aの考えに近いと思う
 ■ どちらかといえば、Bの考えに近いと思う
 ■ Bの考えに近いと思う

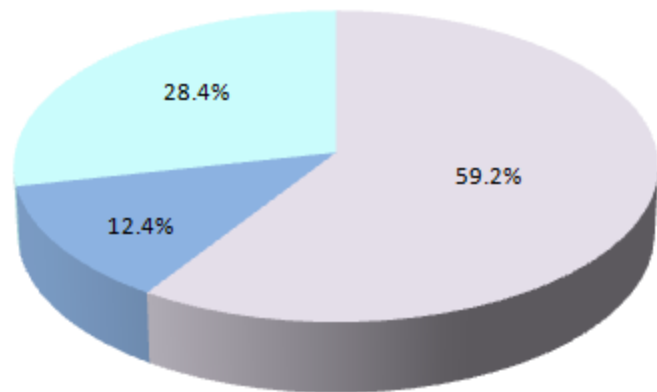
3.4 USBメモリのセキュリティに対する対策状況

3.4.1 USBメモリの使用状況

- ・ ユーザの約60%が現在、USBメモリを使用している。また、ユーザの12.4%は、以前はUSBメモリを使用していたが、現在は使用していないユーザである。
- ・ 自分のUSBメモリを自分のパソコンで使用しているユーザと、自分のUSBメモリを他人のパソコンで使用しているユーザは、USBメモリ利用者のそれぞれ94.6%、28.3%である。
- ・ USBメモリ利用者の13.8%は、他人のUSBメモリを自分のパソコンで使用している。

USBメモリの利用状況
[回答者全体に占める割合]

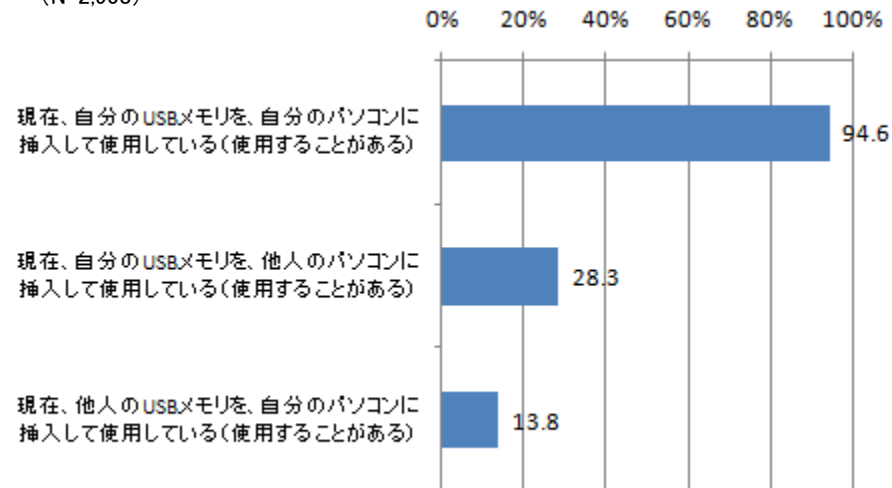
(N=5,000)



- USBメモリを使用している
- 以前はUSBメモリを使用していたが、現在は使用していない
- これまで一度もUSBメモリを使用したことがない

USBメモリの利用形態
[USBメモリ利用者に占める割合]

(N=2,958)

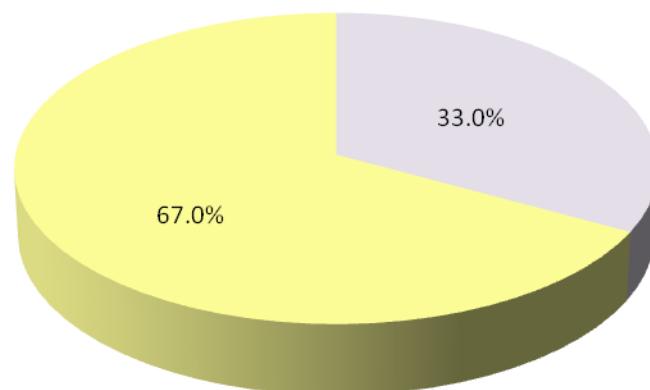


3.4.2 USBメモリのセキュリティ対策の実施状況

- ・ USBメモリ利用者の3人に1人が、USBメモリのセキュリティ対策を実施していない。
- ・ 勝手にウイルスが起動しないように、USBメモリの自動実行をさせないようにしているユーザ、USBメモリ内のファイルを開く前には、必ずウイルスチェックをするようにしているユーザはいずれもUSBメモリ利用者の20%にも満たない状況である。

USBメモリのセキュリティ対策の実施の有無
[USBメモリ利用者に占める割合]

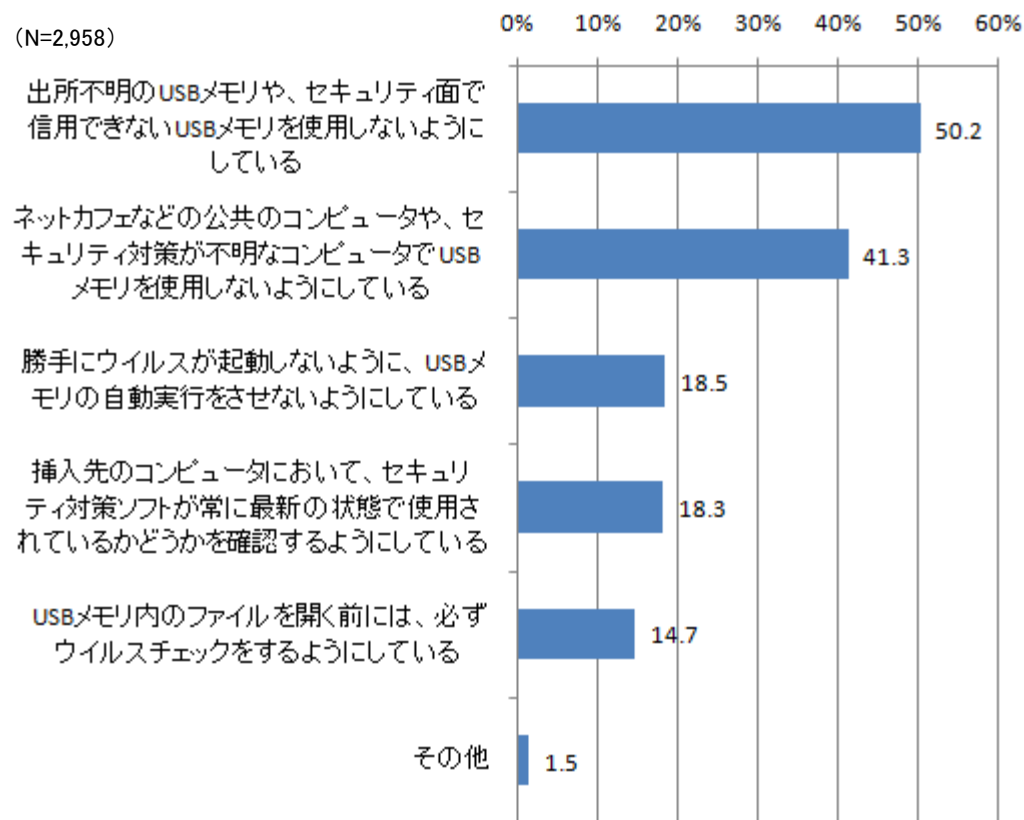
(N=2,958)



■ 対策を実施していない ■ 対策を実施している

USBメモリのセキュリティ対策の実施状況
[USBメモリ利用者に占める割合]

(N=2,958)

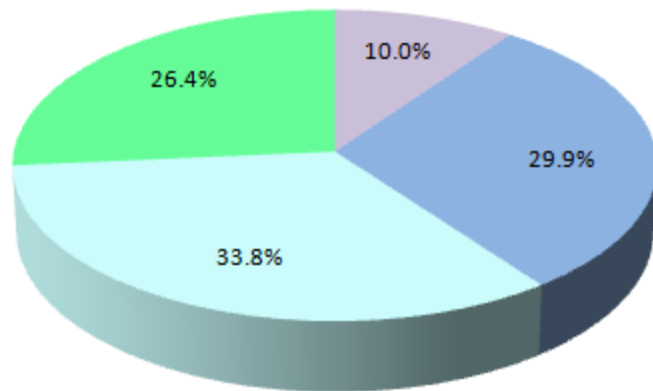


3.4.3 USBメモリのセキュリティに関する被害やトラブルの認知状況

- ・ USBメモリを介して、コンピュータに感染するウイルスが存在することや、その被害が広がっていることについて、認知しているユーザ(詳しい内容について知っているユーザと概要をある程度知っているユーザを足し合わせたユーザ)は、全体の40%にとどまっている。
- ・ また、USBメモリ利用者のうち、これらについて認知しているユーザは53.1%にとどまっている。

USBメモリのセキュリティに関する被害やトラブルに対する認知状況
[回答者全体に占める割合]

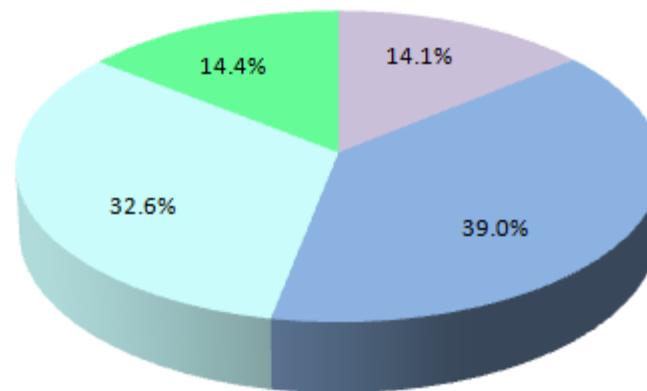
(N=5,000)



- 詳しい内容について知っている
- 概要をある程度知っている
- そのような話題があることを聞いたことがある程度である
- 全く知らなかった

USBメモリのセキュリティに関する被害やトラブルに対する認知状況
[USBメモリ利用者に占める割合]

(N=2,958)



- 詳しい内容について知っている
- 概要をある程度知っている
- そのような話題があることを聞いたことがある程度である
- 全く知らなかった

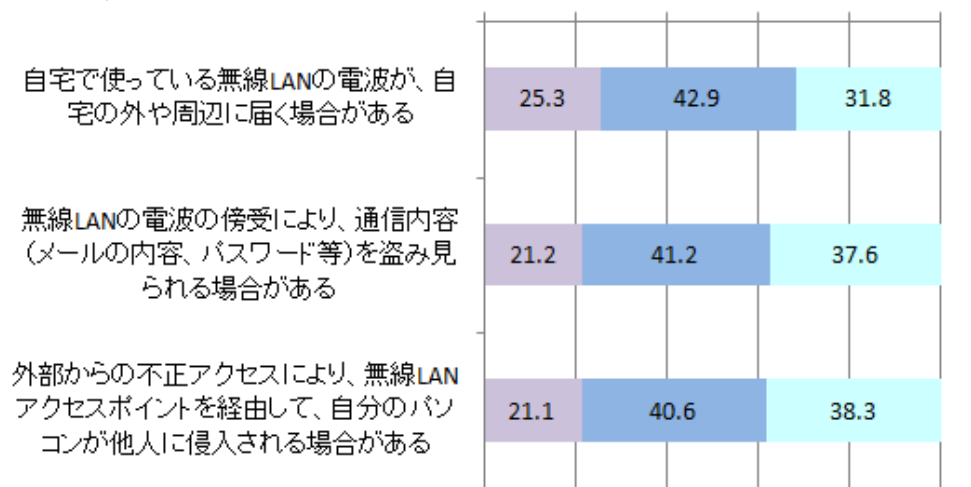
3.5 無線LANのセキュリティに対する対策状況

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%強にとどまっている。
- 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]

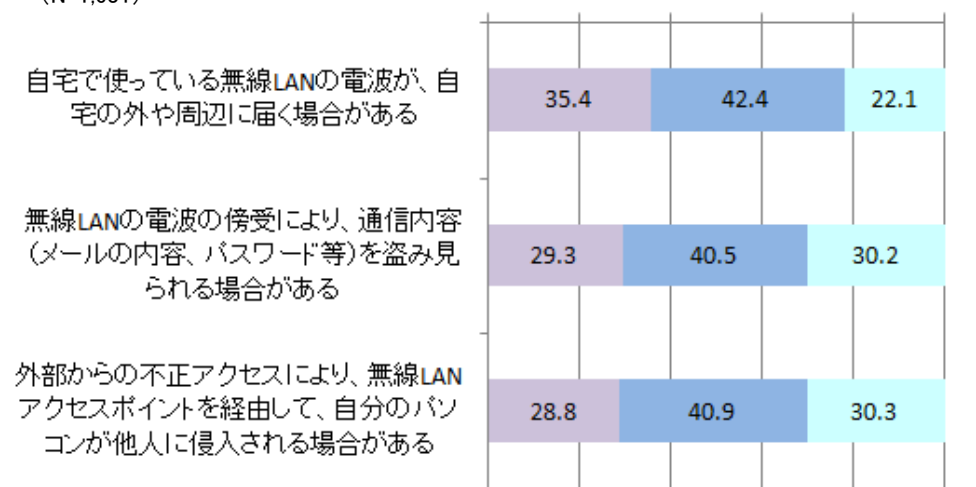
(N=5,000)



- 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全く知らなかった

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]

(N=1,631)



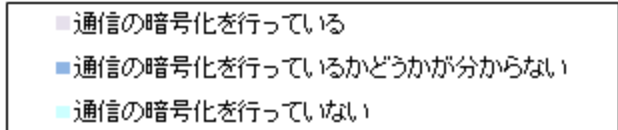
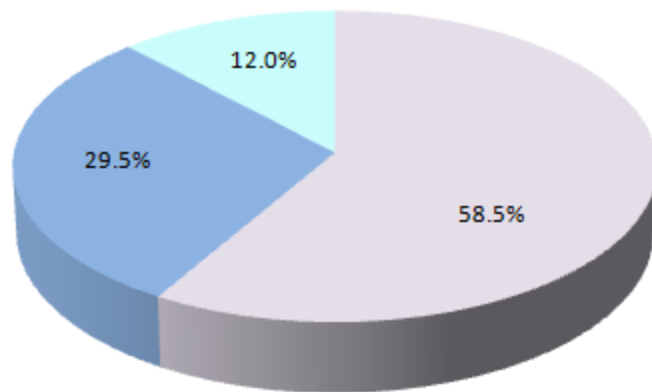
- そのような事例について、詳しい内容を知っている
- そのような事例について、概要を聞いたことがある程度である
- そのような事例について全く知らなかった

3.5.2 無線LANのセキュリティ対策の実施状況(1)

- ・ 自宅で無線LANを利用しているユーザのうち、通信の暗号化を実施しているユーザは全体の58.5%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。
- ・ 通信の暗号化のうち、実施率として最も高いものは、「WEP」で21.7%、次いで、「WPA(7.0%)」、「WPA2(6.0%)」の順となっている。

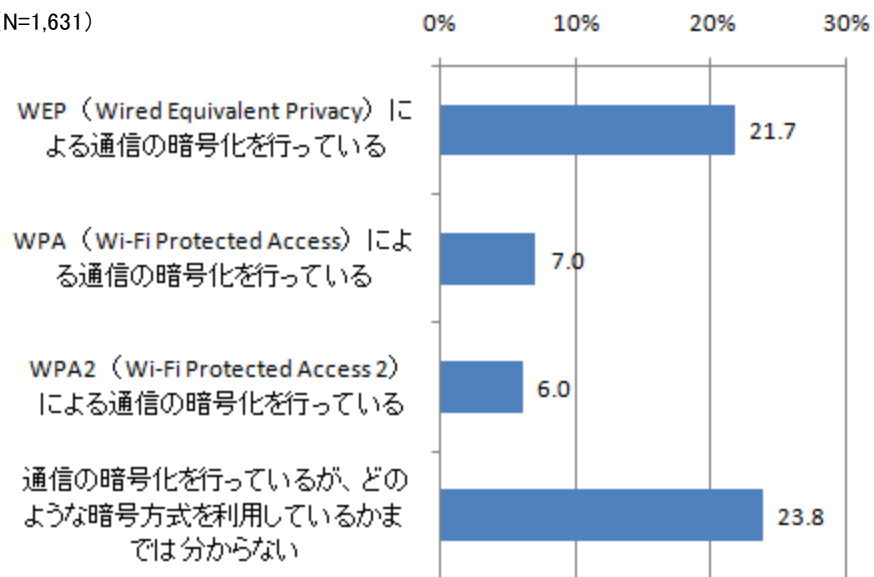
無線LANの暗号化対策の実施の有無
[自宅での無線LAN利用者に占める割合]

(N=1,631)



無線LANの暗号化対策の実施状況
[自宅での無線LAN利用者に占める割合]

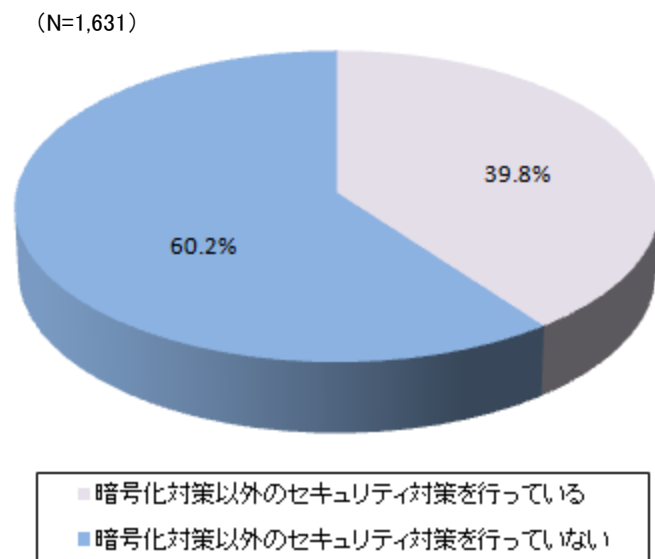
(N=1,631)



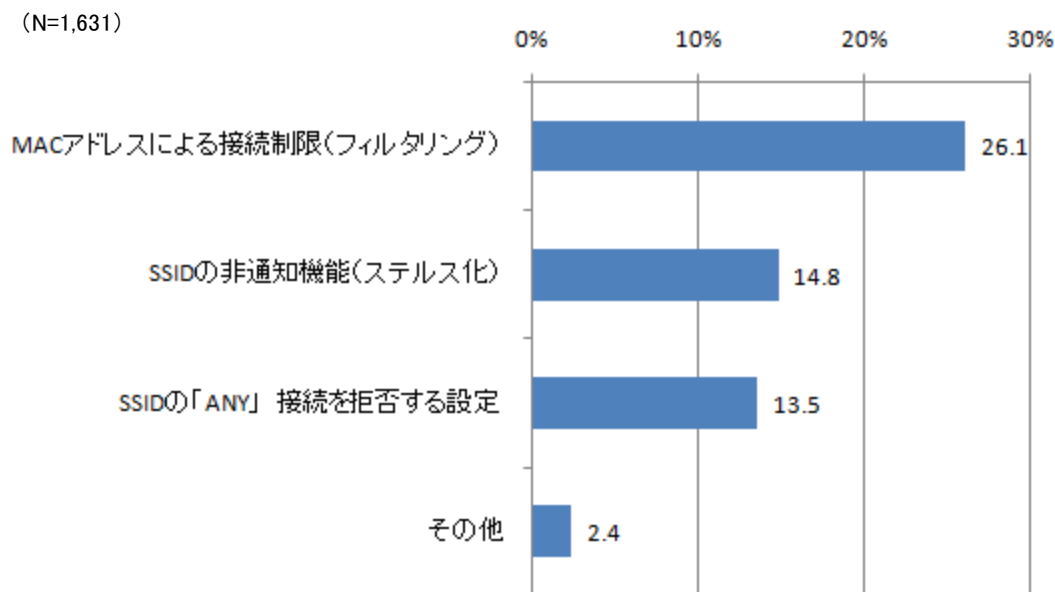
3.5.2 無線LANのセキュリティ対策の実施状況(2)

- ・ 自宅で無線LANを利用しているユーザのうち、通信の暗号化以外のセキュリティ対策を実施しているユーザは全体の40%にも満たない状況である。
- ・ 通信の暗号化以外のセキュリティ対策のうち、実施率として最も高いものは、「MACアドレスによる接続制限(フィルタリング)」で26.1%、次いで、「SSIDの非通知機能(ステルス化)(14.8%)」、「SSIDの「ANY」接続を拒否する設定(13.5%)」の順となっている。

無線LANの暗号化対策以外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]



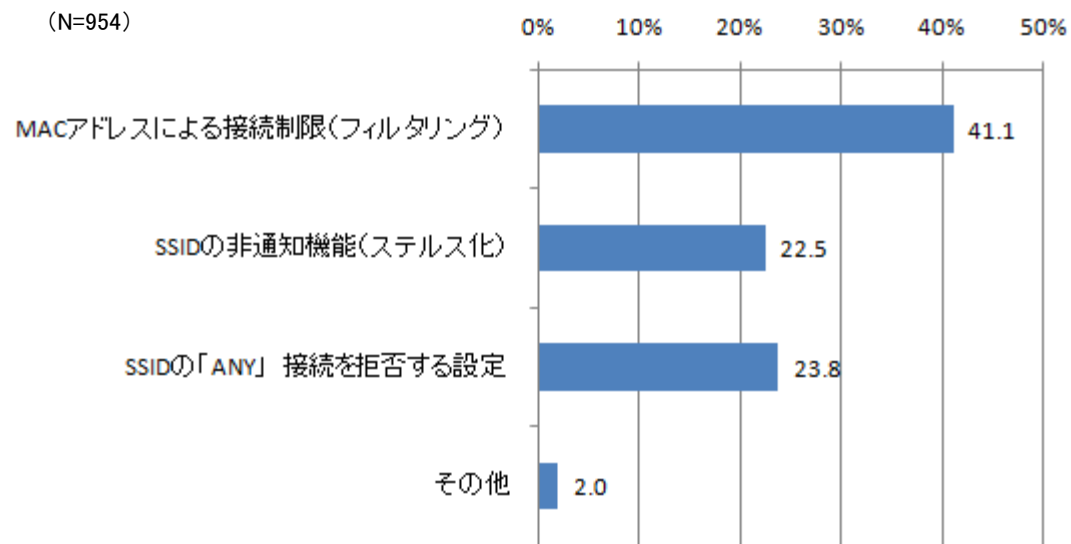
無線LANの暗号化対策以外のセキュリティ対策の実施状況
[自宅での無線LAN利用者に占める割合]



3.5.2 無線LANのセキュリティ対策の実施状況(3)

- ・ 無線LANの暗号化対策の実施状況と、無線LANの暗号化対策以外のセキュリティ対策の実施状況との関係性についてみると、自宅で無線LANを利用しているユーザで、かつ通信の暗号化対策を実施しているユーザを母数とした場合、「MACアドレスによる接続制限(フィルタリング)」の実施率は41.1%と半数を下回っている。
- ・ また、「SSIDの非通知機能(ステルス化)」、「SSIDの「ANY」接続を拒否する設定」の実施率についても、20%を若干上回る程度である。
- ・ 無線LANについては、通信の暗号化対策のみで満足し、より強固なセキュリティ対策を追求しようとするユーザが必ずしも多くないのが現状である。

無線LANの暗号化対策以外のセキュリティ対策の実施状況
[自宅での無線LAN利用者でかつ無線LANの暗号化対策を実施している者に占める割合]

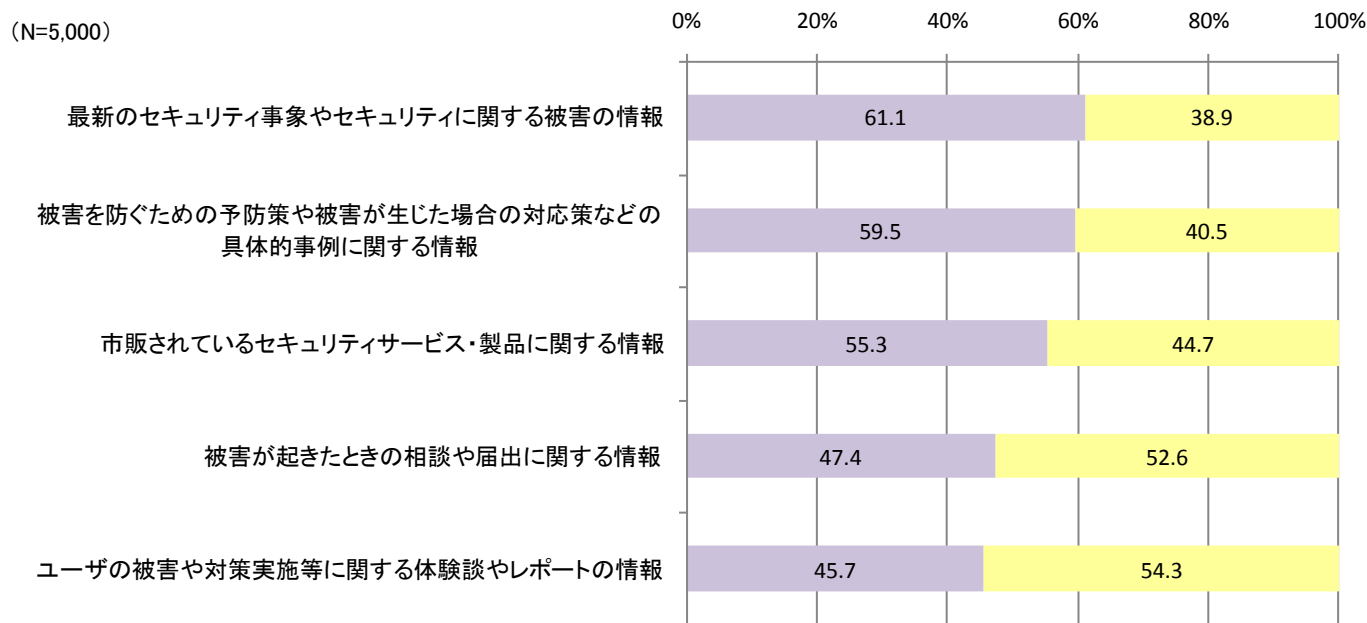


3.6 セキュリティ情報の入手方法

3.6.1 セキュリティ情報に対するニーズ

- ・ ユーザが知りたいセキュリティ情報のうち、最も入手意向が高いものは、「最新のセキュリティ事象やセキュリティに関する被害の情報」であり、60%を大きく上回る。次いで、「被害を防ぐための予防策や被害が生じた場合の対応策などの具体的事例に関する情報(59.5%)」、「市販されているセキュリティサービス・製品に関する情報(55.3%)」の順となっている。

セキュリティ情報の入手意向
[回答者全体に占める割合]

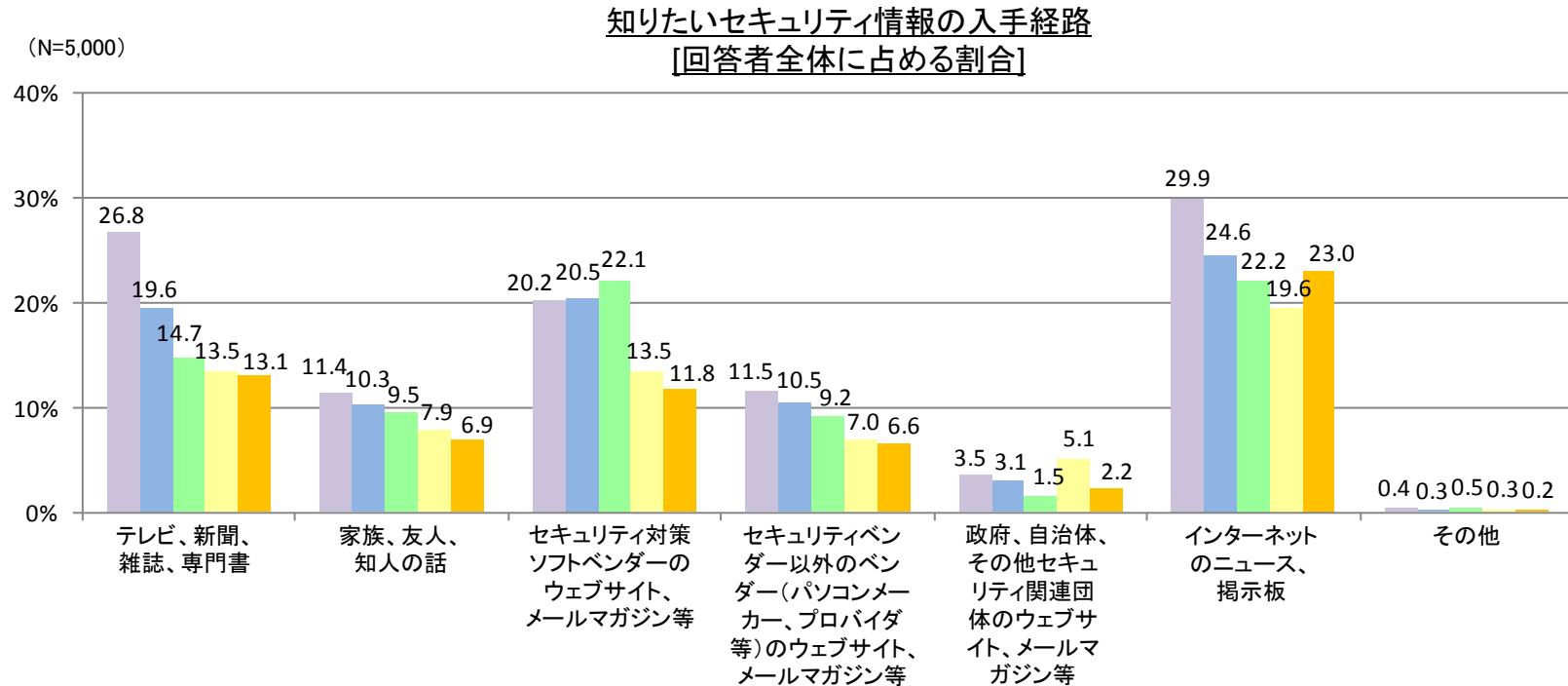


■ 知りたいと思ったことがある

■ 特に知りたいと思ったことはない

3.6.2 知りたいセキュリティ情報の入手経路(1)

- ・ 知りたいセキュリティ情報を、どのような経路で入手しているかについて尋ねた。
- ・ いずれのセキュリティ情報についても、入手経路として「インターネットのニュース、掲示板」が最も多くなっている。
- ・ ユーザの入手意向の高い「最新のセキュリティ事象やセキュリティに関する被害の情報」や「被害を防ぐための予防策や被害が生じた場合の対応策などの具体的事例に関する情報」については、「インターネットのニュース、掲示板」に加えて、「テレビ、新聞、雑誌、専門書」や「セキュリティ対策のソフトベンダーのウェブサイト、メールマガジン等」といった入手経路から情報を入手しているユーザも比較的多くなっている。

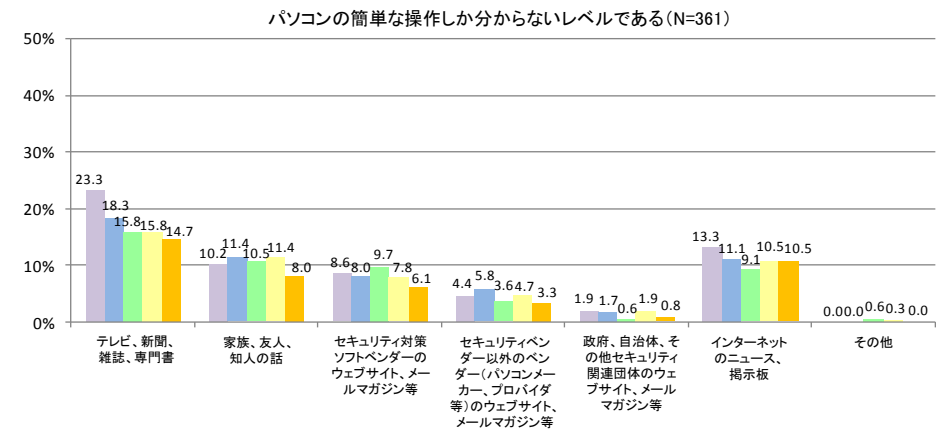
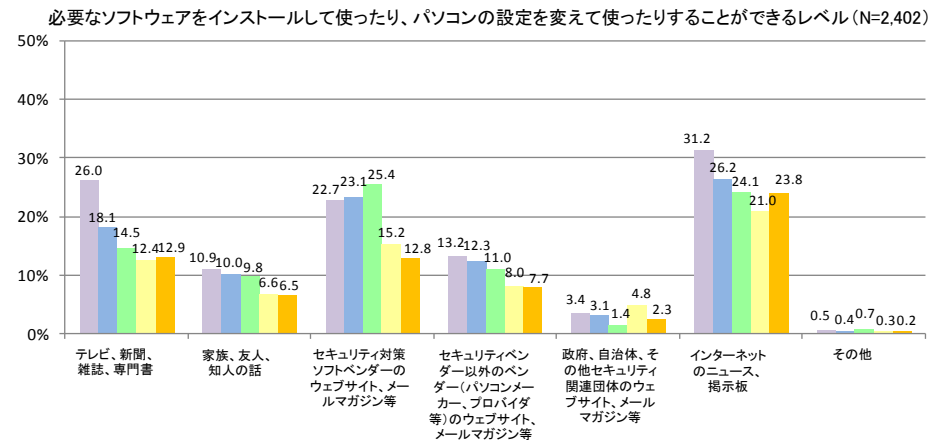
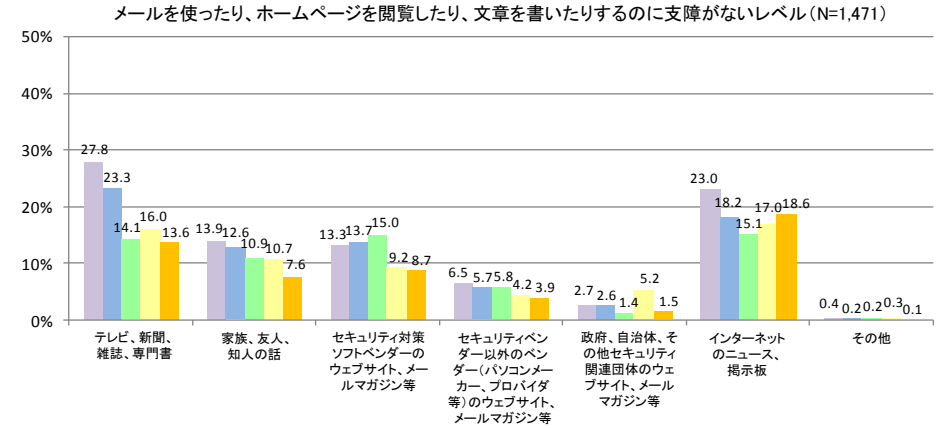
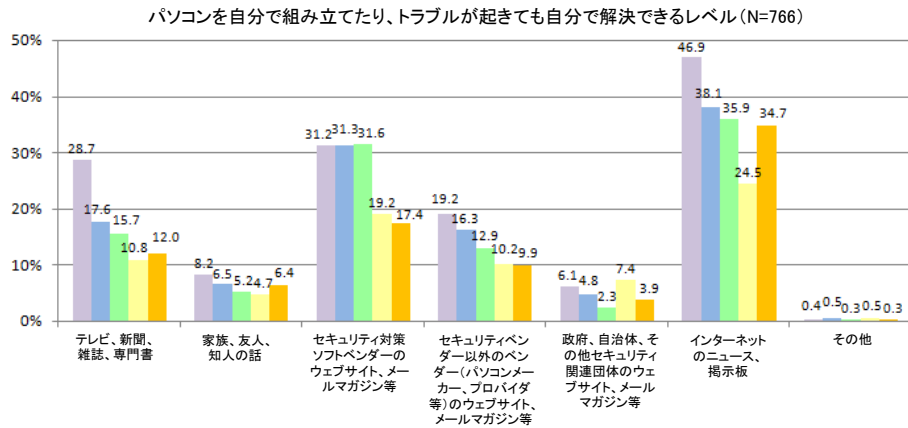


- 最新のセキュリティ事象やセキュリティに関する被害の情報
- 被害を防ぐための予防策や被害が生じた場合の対応策などの具体的事例に関する情報
- 市販されているセキュリティサービス・製品に関する情報
- 被害が起きたときの相談や届出に関する情報
- ユーザの被害や対策実施等に関する体験談やレポートの情報

3.6.2 知りたいセキュリティ情報の入手経路(2)

- セキュリティ情報の入手意向・入手経路を、回答者のパソコンの習熟度別にみると、パソコンの習熟度が高いユーザほど、セキュリティ情報の入手行動を活発に行っている様相が見受けられる。

知りたいセキュリティ情報の入手経路
[パソコンの習熟度レベル別の回答者に占める割合]

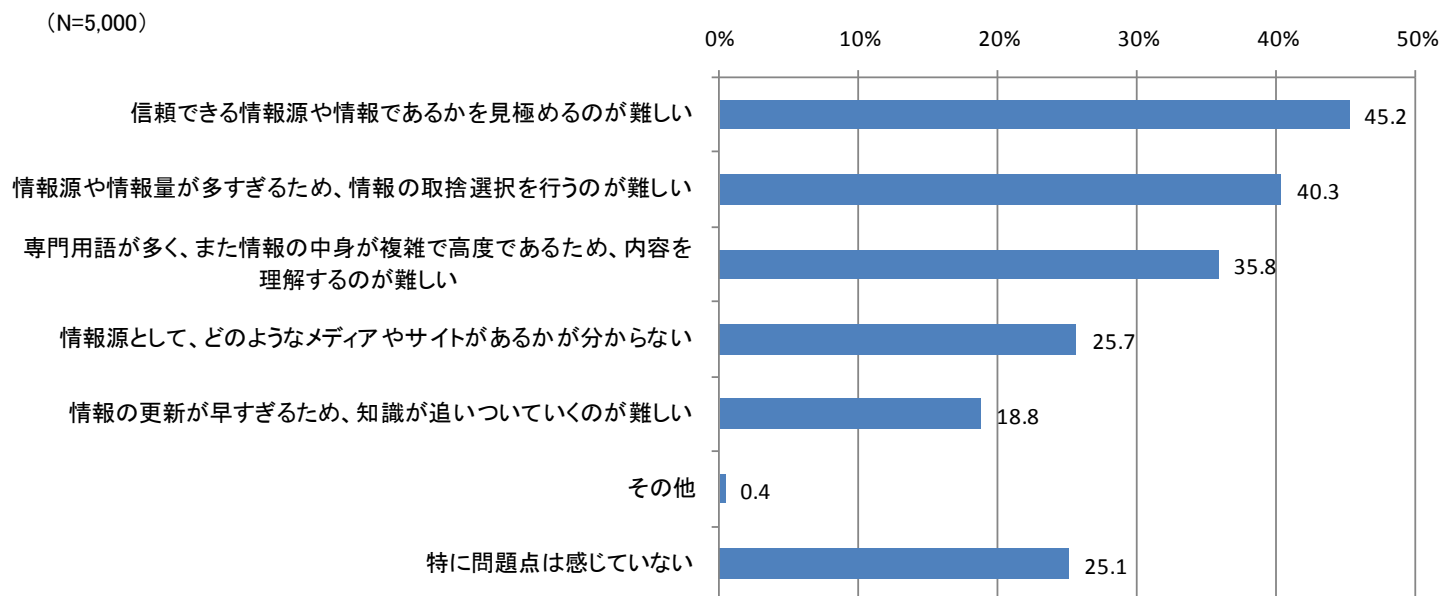


■ 最新のセキュリティ事象やセキュリティに関する被害の情報 ■ 被害を防ぐための予防策や被害が生じた場合の対応策などの具体的事例に関する情報 ■ 市販されているセキュリティサービス・製品に関する情報 ■ ユーザの被害や対策実施等に関する体験談やレポートの情報 ■ 被害が起きたときの相談や届出に関する情報

3.6.3 セキュリティ情報の収集上の問題点

- ・ セキュリティ情報の収集について、ユーザの4人に1人が特に問題点は感じていない。反対に、ユーザの4人に3人は、問題点を感じている。
- ・ セキュリティ情報の収集上の問題点として上位を占めるのが、「信頼できる情報源や情報であるかを見極めるのが難しい(45.2%)」や「情報源や情報量が多すぎるため、情報の取捨選択を行うのが難しい(40.3%)」であり、情報の入手ではなく、情報の利活用の難しさを問題点として指摘する声が多い。

セキュリティ情報の収集上の問題点
[回答者全体に占める割合]



調査票

過去1年間に於けるみなさんのセキュリティ情報の入手状況や、収集にあたっての課題点についてお尋ねします。



【Q.1】過去1年間に、あなたの知りたいと思ったセキュリティ情報は、どのようなことでしたか。また、その情報を、どのようなメディアや経路から収集しましたか。次の中から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】

セキュリティ情報	テレビ、新聞、雑誌、専門書	家族、友人、知人の助言	セキュリティ対策ソフトウェアベンダー以外のベンダーのウェブページ、メールマガジン等	セキュリティベンダー以外のベンダーのウェブページ、ブログ、YouTube、メールマガジン等	政府、自治体、その他セキュリティ関連団体等のウェブページ、メールマガジン等	インターネットのニュース、検索結果	その他	特に知りたいと思った情報はない
1. 最新のセキュリティ事案やセキュリティに関する被害の情報	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. 被害を防ぐための予防策や被害が起きた場合の対応策などの具体的な事例に関する情報	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. 公開されているセキュリティサービス製品に関する情報	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. ユーザーの被害予防策策面に関する体験談やレポートの情報	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5. 被害が起きたときの対応や原因に関する情報	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



【Q.2】あなたは、セキュリティ情報を収集するにあたって、どのような課題点を感じていますか。あてはまるものをすべて選んでお知らせください。(いくつでも)【必須】

- 1. 情報源として、どのようなメディアやサイトがあるかが分からない
- 2. 情報源や情報量が多すぎるため、情報の取捨選択を行うのが難しい
- 3. 信頼できる情報源や情報であるかを見極めるのが難しい
- 4. 専門用語が多く、また情報の中身が複雑で高度であるため、内容を理解するのが難しい
- 5. 情報の更新が早すぎるため、知識が追いついていくのが難しい
- 6. その他 (具体的に→)
- 7. 特に課題点は感じていない

インターネット上で発信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年間に於けるみなさんの被害状況をお尋ねします。



【Q.3】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. 全く知らない発着元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、個人情報を入力を求められ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
- 10. 自分のパソコンから個人情報を流出させてしまった
- 11. オンラインゲームにおいて、ゲーム通貨を不正に詐取されたり、アイテムを騙し取られたことがあった
- 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った
- 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



【Q.4】【Q.3】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が、(ひとつだけ)金銭的な被害を受けた場合は、具体的な金額をお知らせください。(未満取値)【必須】

- 1. 金銭的な被害を受けた (おおよそ) 円(くらい)未満未満で記入ください。
- 2. 特に金銭的な被害にはならなかった



【Q.5】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(乗っ取りの広告・宣伝メール)
- 2. 怪しい不審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警察サイトの当番通知メールなどを装って、ユーザIDやパスワードやクレジットカード番号を入力させ、不正に取る詐欺メール(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人に送らないと不審になります」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



【Q.6】商品やサービスの広告メールといったいわゆる迷惑メールの受信頻度は、現在どの程度ですか。あてはまるものをお知らせください。(ひとつだけ)【必須】

迷惑メールとは以下のものを含みます。
 ・水戸路の広告・宣伝メール、購読料金請求メール、フィッシングメール、ウイルスメール、詐欺メール

※ご自宅でお使いのパソコンについてお答えください。
 ※あなたが所有するパソコンに複数のパソコンを所有している場合は、それらをすべて見合わせた数でお答えください。

1. 毎日200通以上 (おおよそ _____ 通) ※平均数でご記入ください。
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8～9通
10. 毎日1～6通
11. 週に1～6通程度
12. ほとんどない

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。



【Q.7】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、現在実施しているセキュリティ対策と、実施している方はそれらに見解について、実施していない方は今後の対応について、あてはまるものをお知らせください。(それぞれひとつだけ)【必須】

セキュリティ対策	実施している		実施していない	
	満足である	不満である	現在実施はしていない現在も、今後実施する予定はある	今後実施する予定はない
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 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. 増強されたRAMメモリの利用や、重要なファイルの増強化	<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"/>
10. 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"/>
11. 不要な電子メールの送信ファイルは削除しない	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

12. 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"/>
13. 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"/>
14. パスワードの定期的な変更	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15. パスワードを誕生日など推測されやすいものを使って設定	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



【Q.8】あなたがお使いのセキュリティ対策ソフトについて、販売元の会社名と製品名をお知らせください。(具体的に)【必須】

例) シマンテック/ノートンアンチウイルス2009、トレンドマイクロ/ウイルスバスター2009 など
 会社名/製品名



【Q.9】あなたは、どのような方法でパターンファイルの更新を行っていますか。(ひとつだけ)【必須】

1. 何もしなくても新しいパターンファイル(更新ファイル)が更新されるように、自動更新機能を設定している
2. 自分で新しいパターンファイル(更新ファイル)をダウンロードし、手動で実行している
3. パターンファイル(更新ファイル)を更新しているかどうか分からない
4. パターンファイル(更新ファイル)を更新していない



【Q.10】あなたが、最近でパターンファイルを更新したのはいつですか。(ひとつだけ)【必須】

1. 1日前
2. 2～3日前
3. 4～6日前
4. 1週間前
5. 2～3週間前
6. 1ヶ月前
7. 2～3ヶ月前
8. 3ヶ月～半年前
9. 半年～1年前
10. 1年以上前 (おおよそ _____ 年前) ※平均数でご記入ください。
11. 分からない



【Q.11】セキュリティ対策に関する以下の事象について、あなたがご存知のものをお知らせください。(いくつでも)【必須】

1. メールソフトによっては、スパムメールをブロックするフィルタリング機能が設置されていること
2. データをごみ箱に入れて空にするだけでは、お使いのパソコン上からデータを完全に消去したことにはならないこと
3. 一般的なセキュリティ対策ソフトには使用期限があり、使用期限を過ぎると新しいパターンファイルへの更新ができなくなる
4. セキュリティパッチ(修正プログラム)を当てていないと、ウェブサイトへアクセスしただけでウイルスに感染する可能性があること
5. セキュリティ対策ソフトを使ってもウイルスに感染する可能性があること
6. 上記1～5のいずれも知らなかった

	の考えに近いと思う	の考えに近いと思う
1. 出会い系サイト	<input type="checkbox"/>	<input type="checkbox"/>
2. ポルノアダルトサイト	<input type="checkbox"/>	<input type="checkbox"/>
3. ギャブルサイト	<input type="checkbox"/>	<input type="checkbox"/>
4. 暴力・売血シーン、死体映像などを扱うサイト	<input type="checkbox"/>	<input type="checkbox"/>
5. 新興や飲の売買、偽造の作り方などを扱うサイト	<input type="checkbox"/>	<input type="checkbox"/>
6. 匿名性の高い掲示板やSNS、コミュニティサイト	<input type="checkbox"/>	<input type="checkbox"/>
7. プロフィールサイト(プロフィール)	<input type="checkbox"/>	<input type="checkbox"/>
8. ゲームやケータイ小説を扱うサイト	<input type="checkbox"/>	<input type="checkbox"/>



【Q16】あなたには、あなたと同居している未成年のお子さんがいらっしゃいますか。(いくつでも)【必須】

- 1. 小学生未満の子がいる
- 2. 小学生の子がいる
- 3. 中学生の子がいる
- 4. 高校生以上の子がいる
- 5. 未成年の子はいない



【Q17】以下のUSBメモリの使用形態のうち、あなたの使用形態に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. 現在、自分のUSBメモリを、自分のパソコンに挿入して使用している(使用することがある)
- 2. 現在、自分のUSBメモリを、他人のパソコンに挿入して使用している(使用することがある)
- 3. 現在、他人のUSBメモリを、自分のパソコンに挿入して使用している(使用することがある)
- 4. 以前はUSBメモリを使用していたが、現在は使用していない
- 5. これまで一度もUSBメモリを使用したことがない



【Q18】あなたは、USBメモリを介して、コンピュータに感染するウイルスが存在することや、その被害が広がっていることをご存知ですか。(ひとつだけ)【必須】

- 1. 詳しい内容について知っている
- 2. 概要がある程度知っている
- 3. そのような話題があることを聞いたことがある程度である
- 4. 全く知らなかった



【Q19】あなたは、USBメモリを利用するにあたり、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. 出所不明のUSBメモリや、セキュリティ面で使用できないUSBメモリを使用しないようにしている
- 2. ネットカフェなどの公共のコンピュータや、セキュリティ対策が不明なコンピュータでUSBメモリを使用しないようにしている

- 3. 挿入先のコンピュータにおいて、セキュリティ対策ソフトが常に最新の状態で使用されているかどうかを確認するようにしている
- 4. 勝手にウイルスが起動しないように、USBメモリの自動実行をさせないようにしている
- 5. USBメモリ内のファイルを開く前には、必ずウイルスチェックをするようにしている
- 6. その他 (具体的に)
- 7. 上記1.~6.の対策を実施していない



【Q20】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、概要を知ったことがある程度である	そのような事例について全く知らなかった
1. 自宅で行っている無線LANの電波が、自宅の外や周辺に届く被害がある	<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)を盗み見られる場合がある	<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アクセスポイントを経由して、自分のパソコンが他人に侵入される被害がある	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



【Q21】自宅の無線LANに関して、電波の検受により、通信内容を盗み見されないように、通信の暗号化を行っていますか。(ひとつだけ)【必須】

- 1. WEP(Wire Equivalent Privacy)による通信の暗号化を行っている
- 2. WPA(Wi-Fi Protected Access)による通信の暗号化を行っている
- 3. WPA2(Wi-Fi Protected Access 2)による通信の暗号化を行っている
- 4. 通信の暗号化を行っているが、どのような暗号方式を利用しているかまでは分からない
- 5. 通信の暗号化を行っているかどうか分からない
- 6. 通信の暗号化を行っていない
- 7. 無線LANを利用していない



【Q22】通信の暗号化以外で、自宅の無線LANを利用するにあたり、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. MACアドレスによる接続制限(フィルタリング)
- 2. SSIDの「ANY」接続を拒否する設定
- 3. SSIDの非通知機能(ステルス化)
- 4. その他 (具体的に)
- 5. 上記1.~4.の対策を行っていない

続いて、調査を統計的に処理するために、あなた自身のことについてお伺いします。



【Q.23】 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

【Q.24】 あなたの現在の年齢をお知らせください。(単角数値)【必須】

歳

【Q.25】 あなたが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

【Q.26】 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関連関係の技術者・研究者)
- 4. 会社員・公務員・教員(情報システムおよび関連関係の技術者・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. 高校生
- 13. その他(具体的に⇒)



【Q.27】 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



【Q.28】 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(具体的に⇒)



【Q.29】 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



【Q.30】 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

戻る