資料　30－1－1

サイバーセキュリティに関する
インターネット利用者の意識調査結果について

令和3年4月7日

サイバーセキュリティタスクフォース事務局

目次

調査趣旨・概要

■調査の趣旨

- 情報通信技術（ＩＣＴ）の進展により、様々な分野においてＩＣＴの利活用が進んでいる一方、サイバー攻撃は巧妙化・複雑化し、攻撃の種類も多様化していることから、サイバーセキュリティ上の脅威は増大している。このような状況のもと、サイバーセキュリティ上の脅威をインターネット利用者が自ら認識し対応していくための普及啓発が不可欠となっている。
- サイバーセキュリティに関する普及啓発の推進については、総務省として取り組むべき課題として、「IoT・5G セキュリティ総合対策 2020」(2020年7月)に提言されているところである。本調査はサイバーセキュリティに関する普及啓発の検討に資するため、インターネット利用者に対してサイバーセキュリティに関する意識調査を実施するものである。

■調査の概要

調査手法	ウェブアンケート（アンケート調査会社の登録モニターから対象者を抽出）
調査対象者	● 18歳から69歳の男女。 ● 学業や仕事の利用以外にインターネットサービスを利用する人。
サンプル数	2,000件
実施期間	2021年3月2日（火）～3月3日（水）
調査地域	日本全国（47都道府県）

調査ポイント1（なりすまし被害防止）

■ 本調査の調査結果から、なりすまし被害防止のための対策に関して今後期待される方向性は以下の通り。

		調査結果の概要	今後期待される方向性
なりすまし被害防止のための対策	フィッシング被害防止	• 「フィッシングメール・SMSの送信元の確認(54.1%）」「メールリンク先サイトのURLの確認（49.2%）」については、利用者のほぼ２人中１人しか確認していない。（P11, 12）	フィッシング被害防止のため、送信元やリンク先URLをよく確認することの重要性を周知すべきではないか。
		• フィッシングメール・SMS、フィッシングサイトによる被害防止のための有効な対策については、「ユーザ自身がもっと心掛けるべき（69.7%)」を選択した利用者が一番多いほか、「サイト運営者による対策強化（55.9%)」「ISPや携帯事業者による対策強化（47.8%)」を選択した利用者も比較的多かった。(P15)	ISPや携帯電話事業者に対して、フィッシング被害防止に向けた十分な対策の実施を働きかけるべきではないか。
	多要素認証の重要性	• 多要素認証の活用について「多要素認証が提供されている場合には、多要素認証を活用するようにしている（20.4%)」を選択した利用者が少ない。(P12) • 多要素認証の導入について、「面倒に感じることはあるがやむを得ない(45.8%)」、「必要なことではあるが工夫してもらいたい(17.3%)」及び「面倒に感じる(9.0%)」との回答があわせて72.1%に上っている。(P13)	ウェブサイト運営者等に対して、使い勝手の良い方法の工夫を働きかけるべきではないか。
		• 多要素認証を導入すべきサービスとして回答が特に多いのが「キャッシュレス決済サービスなど（81.0%)」「オンラインショッピング（65.1%)」である。(P14)	特にキャッスレス決済サービスやオンラインショッピングサイトで多要素認証の導入に対するニーズが高いことを関係者に共有していくことが適当ではないか。

調査ポイント2（マルウェア感染防止・周知の媒体）

■ 本調査の調査結果から、マルウェア感染防止のための対策及び周知の媒体に関して今後期待される方向性は以下の通り。

		調査結果の概要	今後期待される方向性
マルウェア感染防止のための対策	事業者によるセキュリティ水準の確保	• マルウェア感染防止のための有効な対策については、「ISPや携帯事業者等による十分なセキュリティ水準の確保（50.9%）」と過半数の利用者がISPや携帯事業者による十分なセキュリティ水準の確保を求めている。(P19)	ISPや携帯事業者によるマルウェア感染等の被害防止のためのセキュリティ対策が引き続き必要ではないか。
	アップデートの必要性の周知	• 「OSのアップデートを行うようにしている（27.7%）」及び「ルータ等のファームウェアのアップデートを行うようにしている（14.8%）」を選択した利用者が少ない。(P18)	OSアップデート、ルータ等のファームウェアアップデートの必要性について周知すべきではないか。
	サイバー攻撃の踏み台になるケースの周知	• サイバー攻撃の踏み台になるケースがあることについて「知っている（47.7%）」とあり、フィッシングについて「知っている（74.8%）」やマルウェア感染するおそれについて「知っている（73.7%）」の認知度より低い。(P10, 16, 17)	サイバー攻撃の踏み台になるケースは、ユーザ自身のこととして捉えづらいため、事業者側の取組(NOTICE等)の推進も重要ではないか。
周知の媒体	注意喚起情報の伝達手法	• セキュリティに関する注意喚起の情報を知る媒体について、「動画サイトやSNSなどで表示されるWeb公告(47.9%)」が多く、次いで「政府機関やセキュリティ機関などのTwitterやFacebookなどのSNS(31.2%)」、「政府機関やセキュリティ機関などのホームページ(28.7%)」と続く。(P20) • 政府機関の注意喚起情報の適切な伝達手法については、「動画サイトやSNSなどで表示されるWeb公告(58.8%)」多く、次いで「街中や駅・電車等に掲示されている公告(41.9%)」、「政府機関のTwitterやFacebookなどのSNS(38.7%)」と続く。(P21)	オンラインでの周知に注力しつつ、効果的な周知手法を検討すべきではないか。

調査方法

調査手法

ウェブアンケート（アンケート調査会社の登録モニターから対象者を抽出）

調査対象者

- 18歳から69歳の男女。
- 学業や仕事の利用以外にインターネットサービスを利用する人。

サンプル数

回収標本数：2,000件

	18～29歳	30～39歳	40～49歳	50～59歳	60～69歳
男性	200	200	200	200	200
女性	200	200	200	200	200

補正後の標本数：2,000件　（補正の詳細については備考を参照）

	18～29歳	30～39歳	40～49歳	50～59歳	60～69歳
男性	196	185	237	205	185
女性	184	179	231	204	193

※補正後の標本数は整数でなく、表では小数点第1位を四捨五入して表記しており、件数を合算した件数が全体の件数と一致しない場合がある。

実施期間

2021年3月2日（火）～3月3日（水）

調査地域

日本全国（47都道府県）

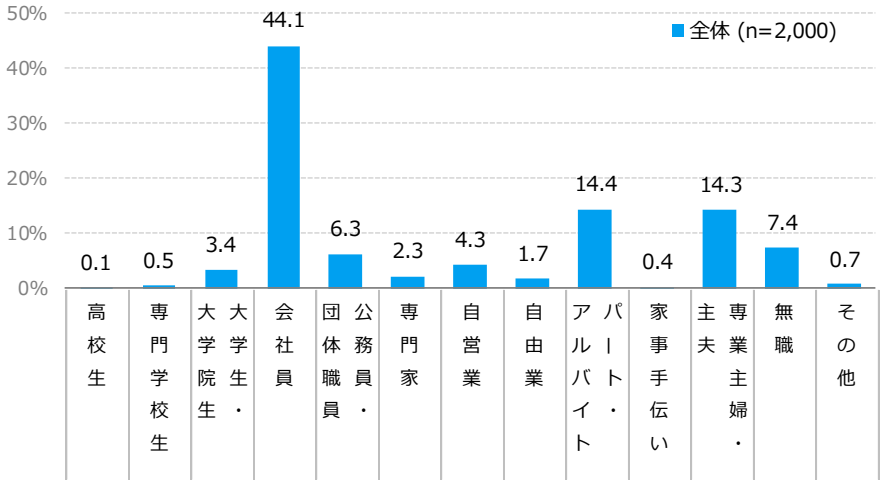
備考

- 集計時に、調査対象者の構成比率をインターネット利用率に合わせるように補正を行った。その方法は以下の通りである。
- 地域別、男女別、年齢別人口※1に、インターネット利用率※2を掛け合わせてインターネット人口を算出した。その際に、インターネット利用率は各地域同率として算出した。
- 算出したインターネット利用者数から構成比率を算出し、調査対象者の構成比率が算出した構成比率になるように補正を行った。

※１　出典：総務省統計局「人口推計」2019年10月1日現在人口（2020年4月14日発表）
※２　出典：総務省「通信利用動向調査」、図表5-2-1-5 属性別インターネット利用率（2019年）

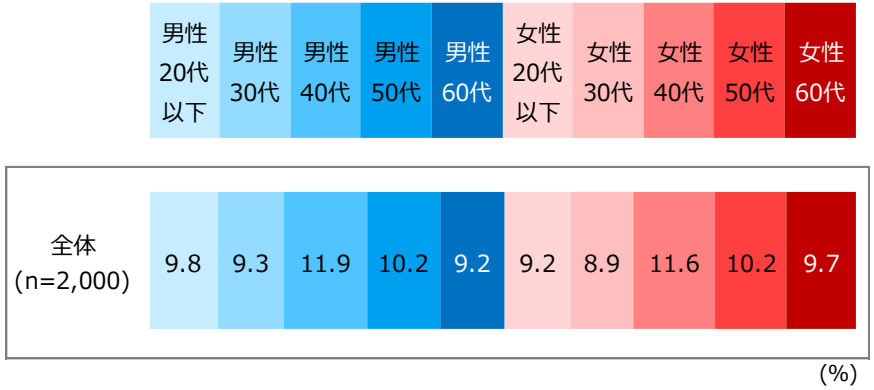
調査対象者の属性

職業



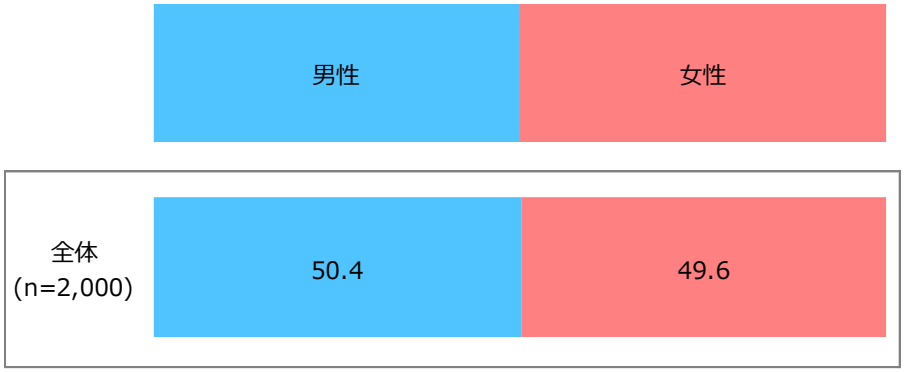
※ 専門家：医師、弁護士、会計士など

性年代



(%)

性別



(%)

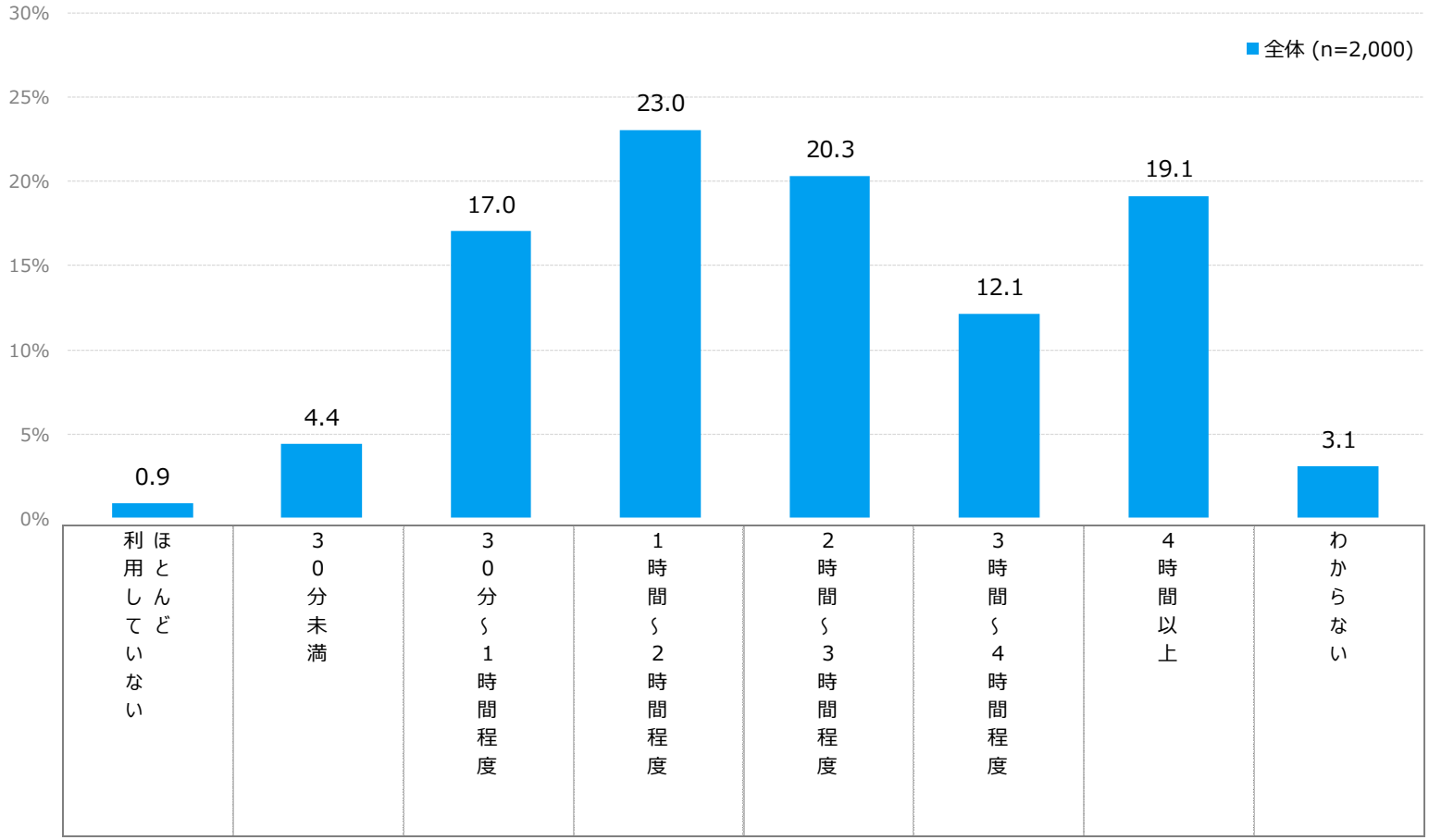
年代

【平均年齢：44.67歳】(%)

インターネットサービスの１日当たり平均使用時間

■ インターネットサービスの１日当たり平均使用時間をみると、「1時間～2時間程度」が23.0%と高く、次いで「2時間～3時間程度」20.3%、「4時間以上」19.1%、「30分～1時間程度」17.0%と続いている。

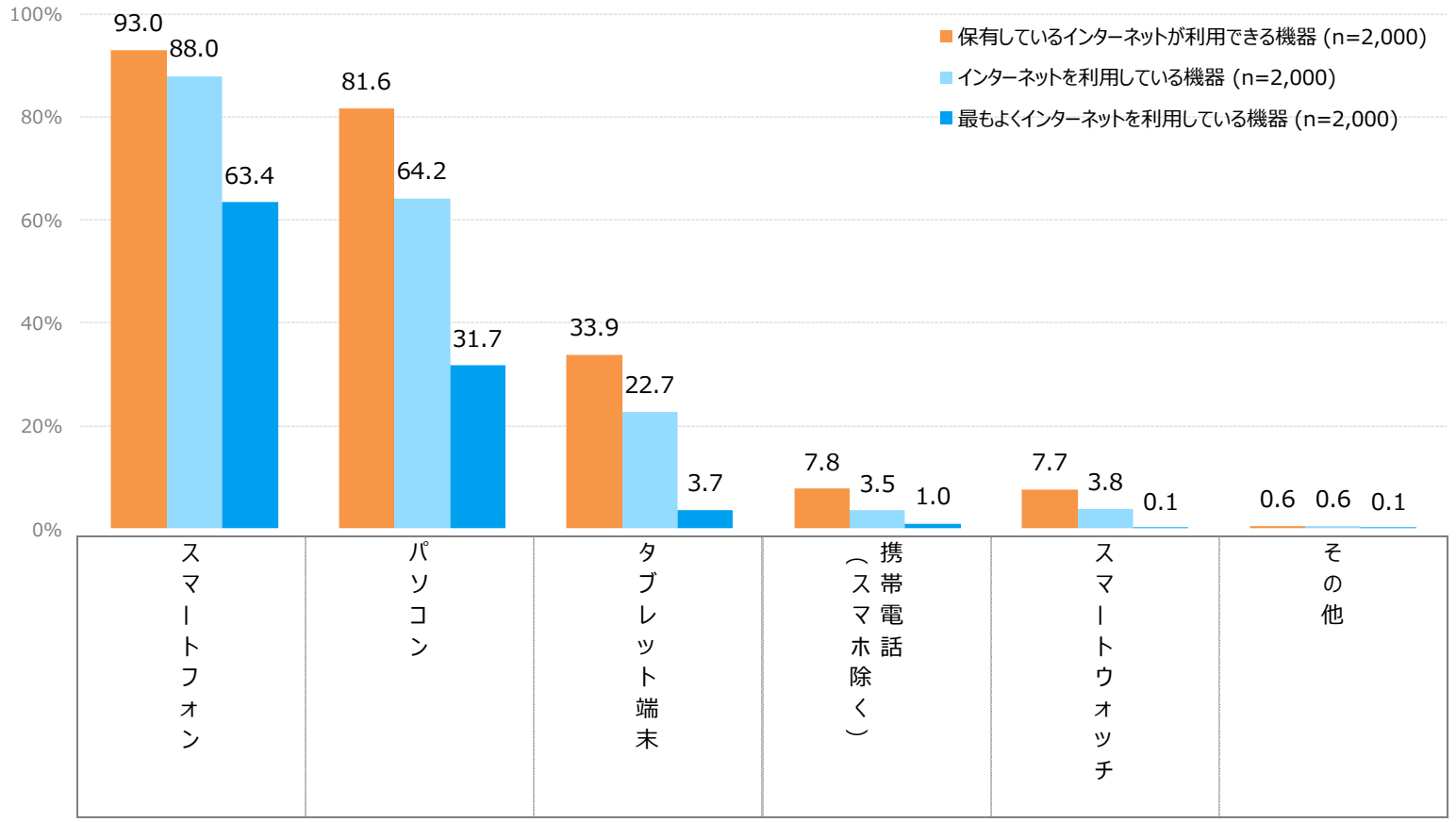
（対象者）全数
SC3.直近の1ヶ月の間で、あなたは1日の間にインターネットのサービスを平均してどれくらいの時間利用していますか。※学業や仕事で利用している時間は除きます。



保有しているインターネットが利用できる機器／利用している機器

■「スマートフォン」(保有93.0%、利用88.0%、最利用63.4)がすべてにおいて高く、次いで「パソコン」(保有81.6%、利用64.2%、最利用31.7%)、「タブレット端末」(保有33.9%、利用22.7%、最利用3.7%)と続いている。

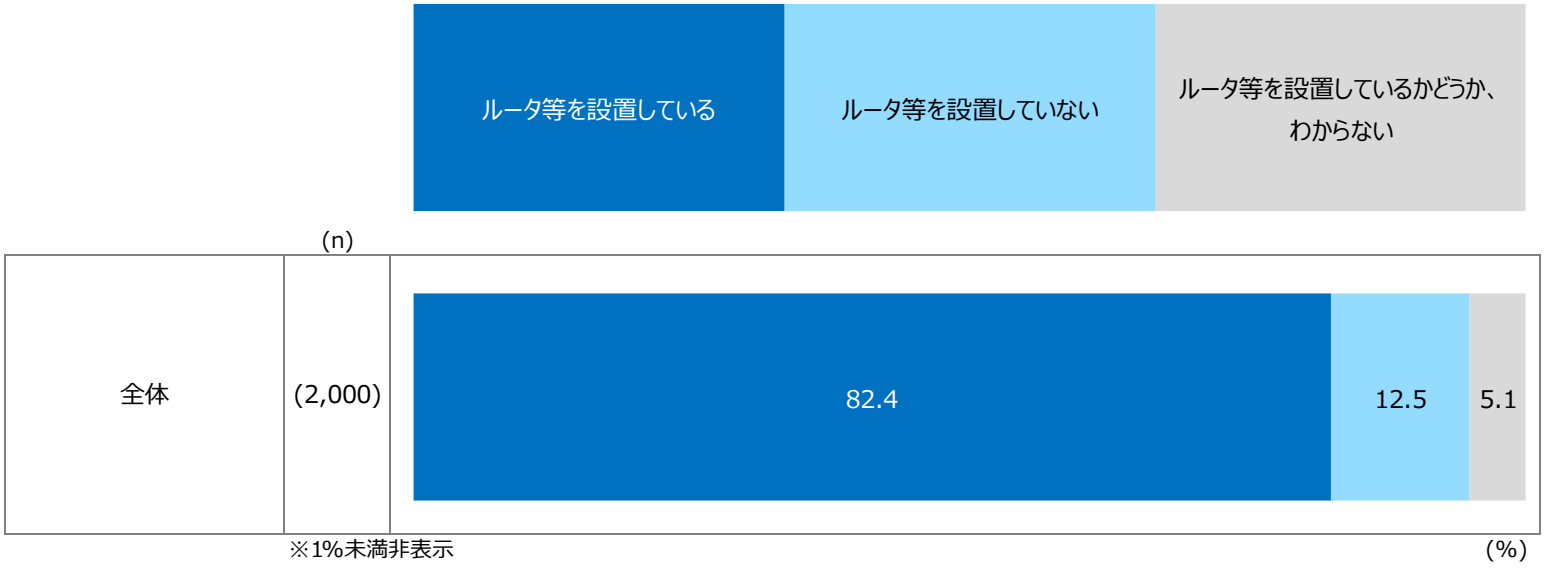
（対象者）全数
Q1.あなたは、インターネットを利用できる端末として、何を保有していますか。その中から、普段、学業や仕事以外で、インターネットを利用している端末、最もよく利用している端末をお選びください。



自宅でのルータ等の設置

■ 自宅でのルータ等の設置をみると、全体では「ルータ等を設置している」が82.4%、「ルータ等を設置していない」が12.5%となっている。

（対象者）全数
Q2.あなたは、ご自宅でインターネットを利用するためにルータ等を設置していますか。

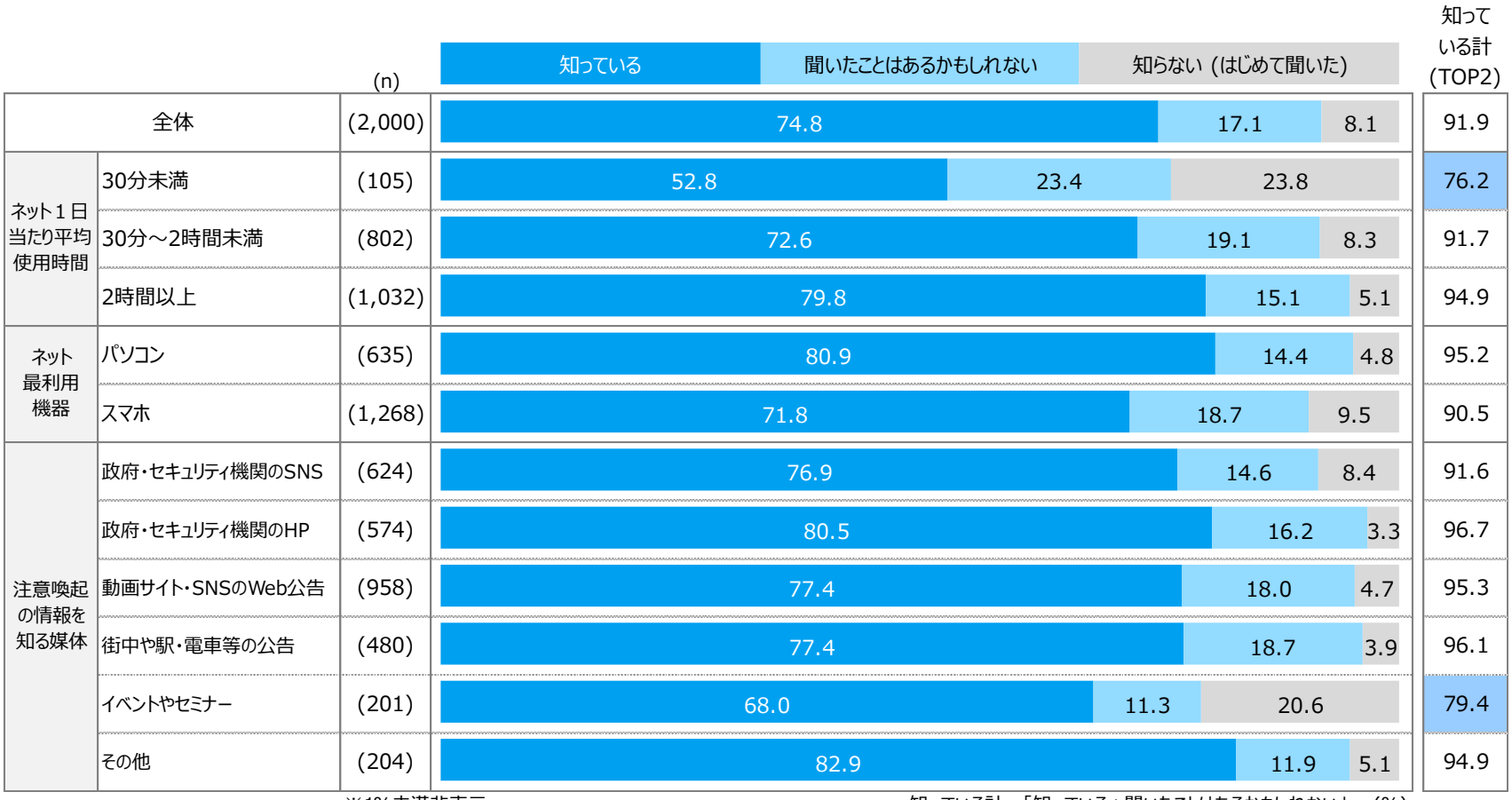


フィッシングに対する認知度

- フィッシングに対する認知度をみると、「知っている」74.8%、「聞いたことはあるかもしれない」17.1%となっており、合わせた認知計で91.9%を占めている。
- ネット使用時間別では、[30分未満]の認知計が76.2%と低くなっている。
- ネット最利用機器別では、[パソコン]の認知が[スマホ]よりもやや高くなっている。
- 注意喚起の情報を知る媒別体では、[イベントやセミナー]の認知が8割弱と低くなっている。

（対象者）全数

Q3.あなたは、「フィッシングメール」や「フィッシングショートメール（SMS）」から誘導された「フィッシングサイト」で、ID・パスワード、口座番号、住所・氏名等の個人情報の入力をすることで、第三者にこれらの情報を窃取される事例があることを知っていますか。



※1%未満非表示

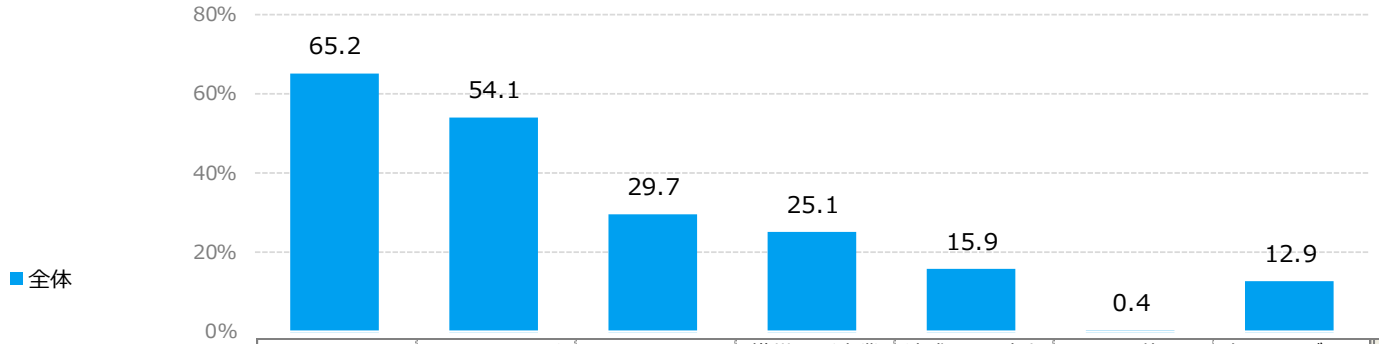
知っている計：「知っている+聞いたことはあるかもしれない」 (%)

電子メールやショートメール(SMS)を受信する際に気をつけていること

- メール受信時に気をつけていることをみると、「リンクをむやみにクリックせず、安全と思った場合にクリックすることにしている」が65.2%と最も高く、いずれかに気をつけていると回答した人（気をつけている計）が87.1%を占める。
- ネット使用時間別では、使用時間が長いほど総じてスコアが高い傾向となっている。
- ネット最利用機器別では、[パソコン]で「リンクをクリックせず、ブックマークしてあるURLや検索結果からアクセス」「迷惑メール防止ソフトを購入して利用している」がやや高い。

（対象者）全数

Q4.あなたは、スマートフォンやパソコン等で電子メールやショートメール（SMS）を受信する際には、どのようなことに気をつけていますか。（いくつでも）



※数表内の網掛け

- 全体値より10%以上高いもの
- 全体値より5%以上高いもの
- 全体値より5%以上低いもの
- 全体値より10%以上低いもの

		n	電子メールやショートメールの本文中に記載のあるリンクをむやみにクリックせず、安全と思った場合にクリックすることにしている	電子メールの発信元アドレスやショートメールの発信元電話番号を確認するようにしている	電子メールやショートメールの本文中に記載のあるリンクをクリックせず、ブックマークしてあるURLや検索結果からアクセスすることにしている	携帯電話事業者やインターネット接続サービスプロバイダが提供する迷惑メール防止サービス等に加入するようにしている	迷惑メール防止ソフトを購入して利用している	その他	左記のいずれもしていない	気をつけている計
全体		(2,000)	65.2	54.1	29.7	25.1	15.9	0.4	12.9	87.1
ネット１日当たり平均使用時間	30分未満	(105)	40.3	32.4	11.9	18.5	14.9	3.0	27.6	72.4
	30分～2時間未満	(802)	63.2	51.5	30.6	25.2	17.2	0.4	13.2	86.8
	2時間以上	(1,032)	70.8	59.8	31.6	26.2	15.9	0.2	9.6	90.4
ネット最利用機器	パソコン	(635)	65.5	53.9	36.5	28.6	22.3	0.3	11.0	89.0
	スマホ	(1,268)	65.7	54.9	26.2	23.0	12.8	0.4	13.3	86.7

※全体で降順ソート

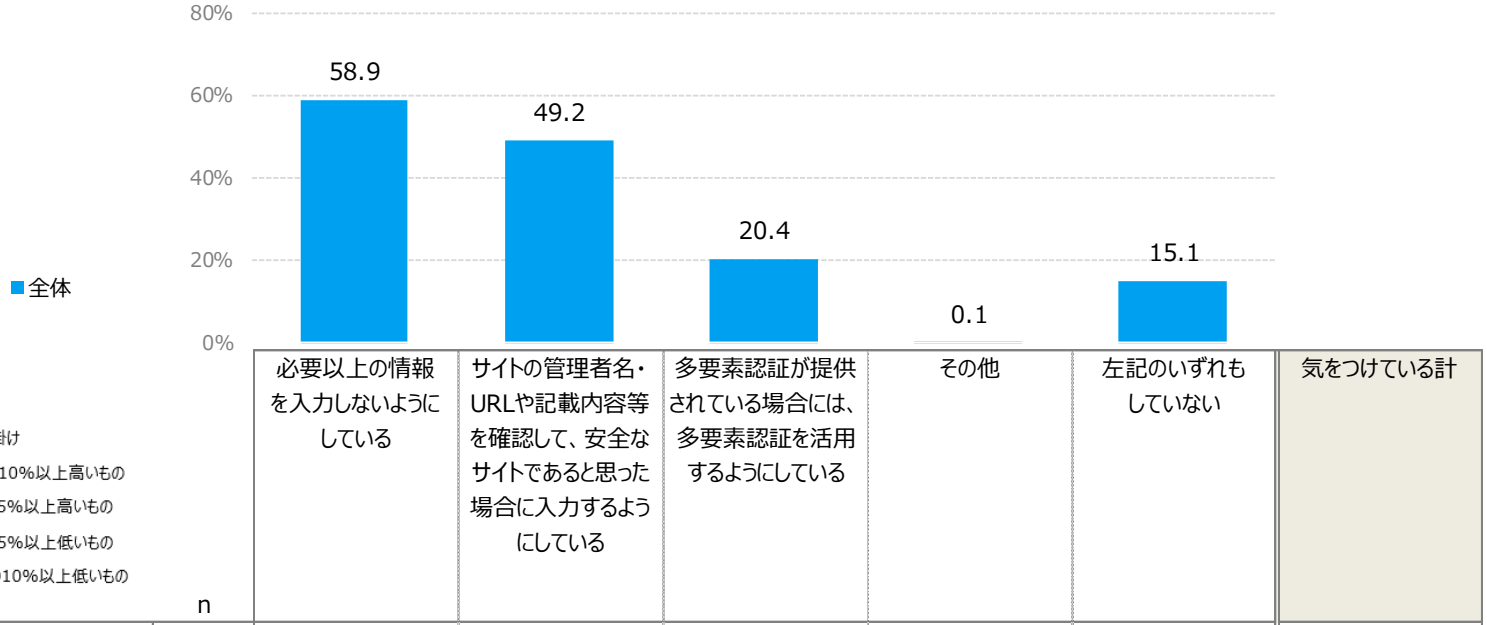
(%)

ウェブサイトにID・パスワードを入力する際に気をつけていること

- ID・パスワードを入力する際に気をつけていることをみると、「必要以上の情報を入力しないようにしている」が58.9%と高く、次いで「サイトの管理者名・URLや記載内容等を確認して、安全なサイトであると思った場合に入力するようにしている」が49.2%で続いている。いずれかに気をつけていると回答した人（気をつけている計）は84.9%。
- ネット使用時間別では、[30分未満]では総じてスコアが低くなっている。
- ネット最利用機器別では、[パソコン]で「安全なサイトであると思った場合に入力」がやや高い。

（対象者）全数

Q6.あなたは、ウェブサイトにアクセスしてID・パスワードの入力を求められる際、どのようなことに気をつけていますか。（いくつでも）



※数表内の網掛け

- 全体値より10%以上高いもの
- 全体値より5%以上高いもの
- 全体値より5%以上低いもの
- 全体値より10%以上低いもの

		n	必要以上の情報を入力しないようにしている	サイトの管理者名・URLや記載内容等を確認して、安全なサイトであると思った場合に入力するようにしている	多要素認証が提供されている場合には、多要素認証を活用するようにしている	その他	左記のいずれもしていない	気をつけている計
全体		(2,000)	58.9	49.2	20.4	0.1	15.1	84.9
ネット1日当たり平均使用時間	30分未満	(105)	47.9	26.5	8.9	-	34.4	65.6
	30分～2時間未満	(802)	60.6	48.0	19.1	0.2	13.6	86.4
	2時間以上	(1,032)	59.5	54.1	23.4	0.0	12.9	87.1
ネット最利用機器	パソコン	(635)	61.5	54.6	21.5	-	12.7	87.3
	スマホ	(1,268)	57.2	47.0	19.6	0.2	16.1	83.9

※全体で降順ソート

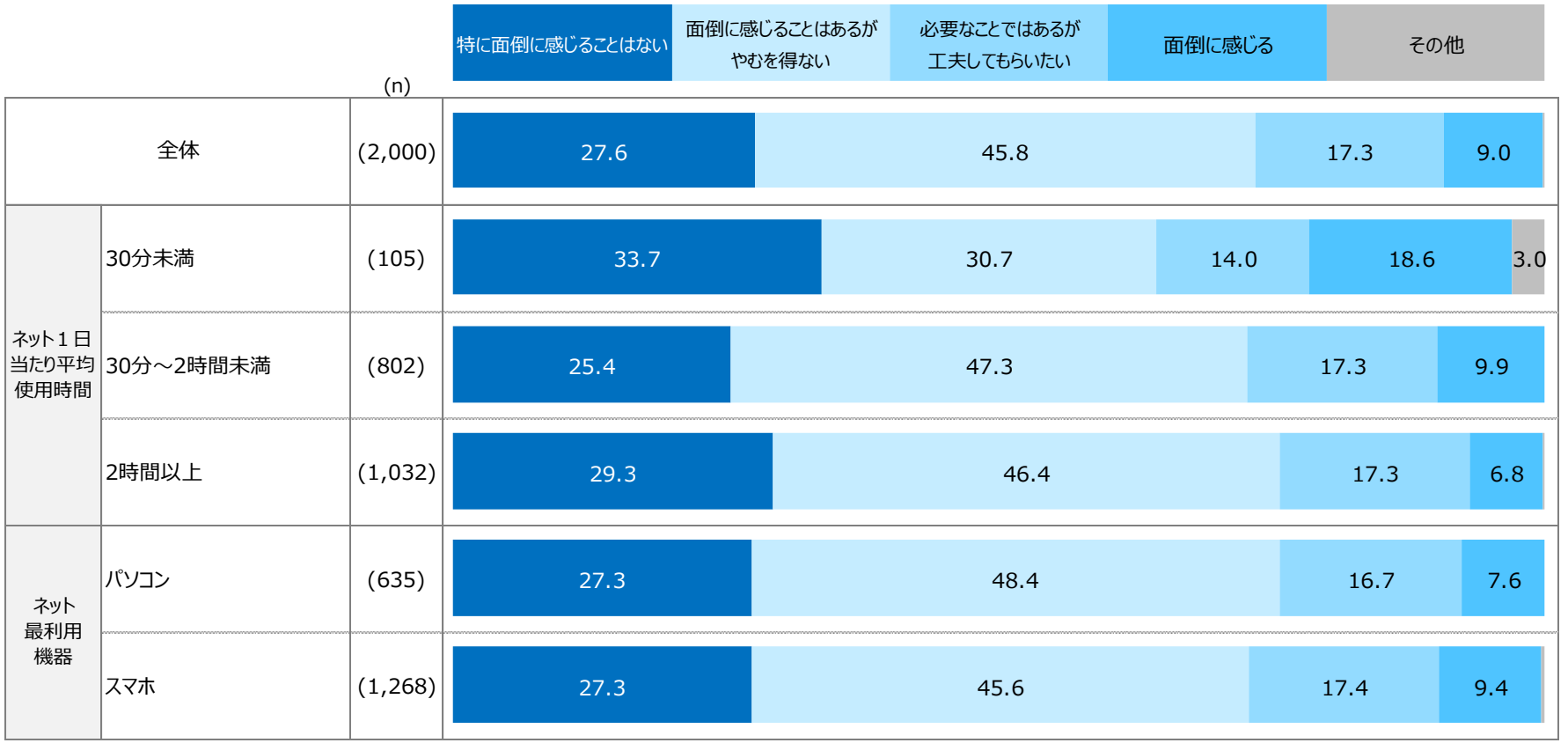
(%)

多要素認証の導入について

■ 多要素認証の導入をみると、「面倒に感じることはあるがやむを得ない」が45.8%と高く、次いで「特に面倒に感じることはない」27.6%、「必要なことではあるが工夫してもらいたい」17.3%と続いている。
■ ネット使用時間別では、[30分未満]で「特に面倒に感じることはない」が3割以上と高くなっている。
■ ネット最利用機器別では、[パソコン]と［スマホ］とで違いは見られない。

（対象者）全数
Q7.オンラインサービスの提供に当たって、正しいユーザであるかどうかの認証のために、多要素認証を導入する企業が増えていますが、これについてどう思いますか。

「特に面倒に感じることはない」：なりすまし等の被害のリスクを低減させるために必要なことであり、特に面倒に感じることはない
「面倒に感じることはあるがやむを得ない」：面倒に感じることはあるが、なりすまし等の被害のリスクを低減させるために必要なことであり、やむを得ない
「必要なことではあるが工夫してもらいない」：なりすまし等の被害のリスクを低減させるために必要なことではあるが、面倒に感じることもあるので、使い勝手のいい方法を工夫してもらいたい
「面倒に感じる」：面倒に感じる(なりすまし等の被害のリスクを低減させるために必要とは思わない)



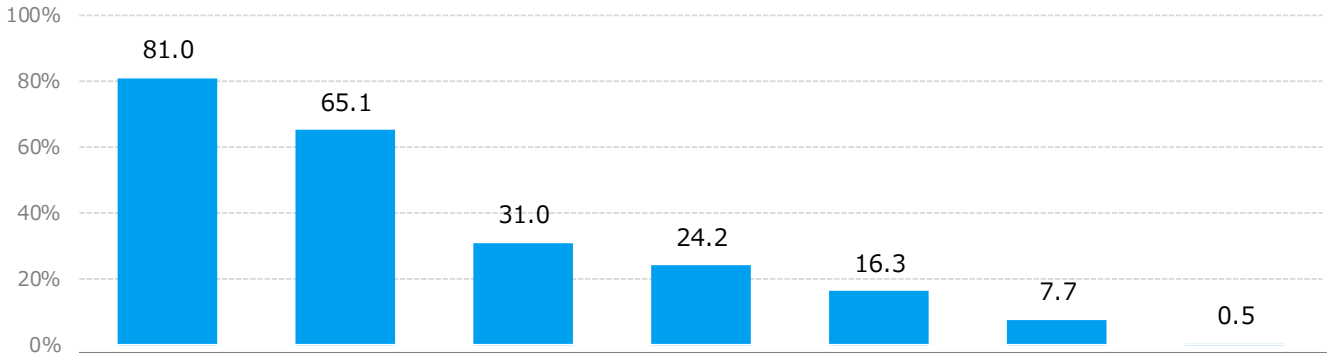
※1%未満非表示

(%)

多要素認証の導入が望ましいサービス

■ 多要素認証の導入が望ましいサービスをみると、「キャッシュレス決済サービスなどの金銭のやり取りを伴うサービス」が81.0%と高く、次いで「オンラインショッピング」が65.1%で続いている。
■ ネット使用時間別では、[2時間以上]で「オンラインショッピング」が7割とやや高い。また、[30分未満]では「キャッシュレス決済サービスなどの金銭のやり取りを伴うサービス」「オンラインショッピング」が低い。
■ ネット最利用機器別では、[パソコン]で「SNS、メールなどのコミュニケーションサービス」がやや低い。

（対象者）全数
Q8.あなたは、特にどのようなオンラインサービスにおいて多要素認証を導入すべき、または、導入しても構わないと思いますか。（いくつでも）



※数表内の網掛け
全体値より10%以上高いもの
全体値より5%以上高いもの
全体値より5%以上低いもの
全体値より10%以上低いもの

		n	キャッシュレス決済サービスなどの金銭のやり取りを伴うサービス	オンラインショッピング	SNS、メールなどのコミュニケーションサービス	ポイントサービス	音楽定額配信などのサブスクリプション	ゲーム	その他
全体		(2,000)	81.0	65.1	31.0	24.2	16.3	7.7	0.5
ネット１日当たり平均使用時間	30分未満	(105)	65.8	43.7	29.7	28.3	8.9	9.8	1.3
	30分～2時間未満	(802)	80.5	61.1	29.1	23.5	13.7	5.7	0.4
	2時間以上	(1,032)	84.2	71.7	32.9	24.1	19.6	8.7	0.6
ネット最利用機器	パソコン	(635)	81.8	69.9	23.6	26.2	15.9	6.1	1.1
	スマホ	(1,268)	81.4	62.5	34.7	23.0	17.0	8.1	0.1

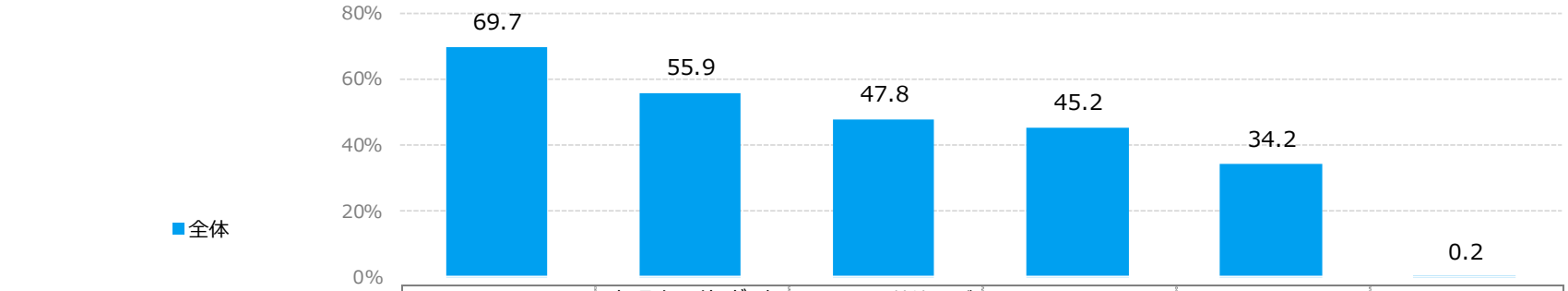
※全体で降順ソート

(%)

フィッシング詐欺等の被害を防ぐ有効な対策

■ フィッシング詐欺等の被害を防ぐ有効な対策をみると、「ユーザ自身が、被害に遭わないように、もっと心掛けるべきである」が69.7%と高く、次いで「オンラインでサービスを提供するサイト運営者が、多要素認証を導入するなどなりすましによるユーザの被害を防止するための対策に努めるべきである」が55.9%で続いている。
■ ネット使用時間別では、使用時間が長いほど総じてスコアが高い傾向となっている。
■ フィッシング認知度別では、[知っている]層で全体的にスコアが高くなっている。

（対象者）全数
Q9.あなたは、フィッシングメールやフィッシングサイトによる詐欺等の被害を防ぐための対策として、どのようなことが有効だと思いますか。（いくつでも）



※数表内の網掛け
全体値より10%以上高いもの
全体値より5%以上高いもの
全体値より5%以上低いもの
全体値より10%以上低いもの

		n	ユーザ自身が、被害に遭わないように、もっと心掛けるべきである	オンラインでサービスを提供するサイト運営者が、多要素認証を導入するなどなりすましによるユーザの被害を防止するための対策に努めるべきである	インターネット接続サービス事業者(ISP)や携帯電話事業者が、不審なメールの受信や不審なサイトへのアクセスをしようとするユーザを守るための対策に努めるべきである	犯罪に該当するケースはしっかり取り締まるべきである	政府や企業等が、ユーザに対して、わかりやすい周知に努めるべきである	その他
全体		(2,000)	69.7	55.9	47.8	45.2	34.2	0.2
ネット１日当たり平均使用時間	30分未満	(105)	44.9	44.9	43.7	38.0	26.5	1.3
	30分～2時間未満	(802)	67.5	56.2	45.7	43.8	31.6	0.1
	2時間以上	(1,032)	75.0	58.0	50.6	46.5	37.8	0.1
ネット最利用機器	パソコン	(635)	70.3	57.6	48.8	44.0	35.2	0.0
	スマホ	(1,268)	70.3	55.3	47.7	45.2	34.4	0.3
フィッシング認知度	知っている	(1,496)	74.5	61.2	52.3	46.2	35.9	0.1
	聞いたことはある	(343)	59.4	49.9	43.2	40.0	35.6	0.5
	知らない	(162)	47.6	19.4	16.0	47.6	15.3	0.2

※全体で降順ソート

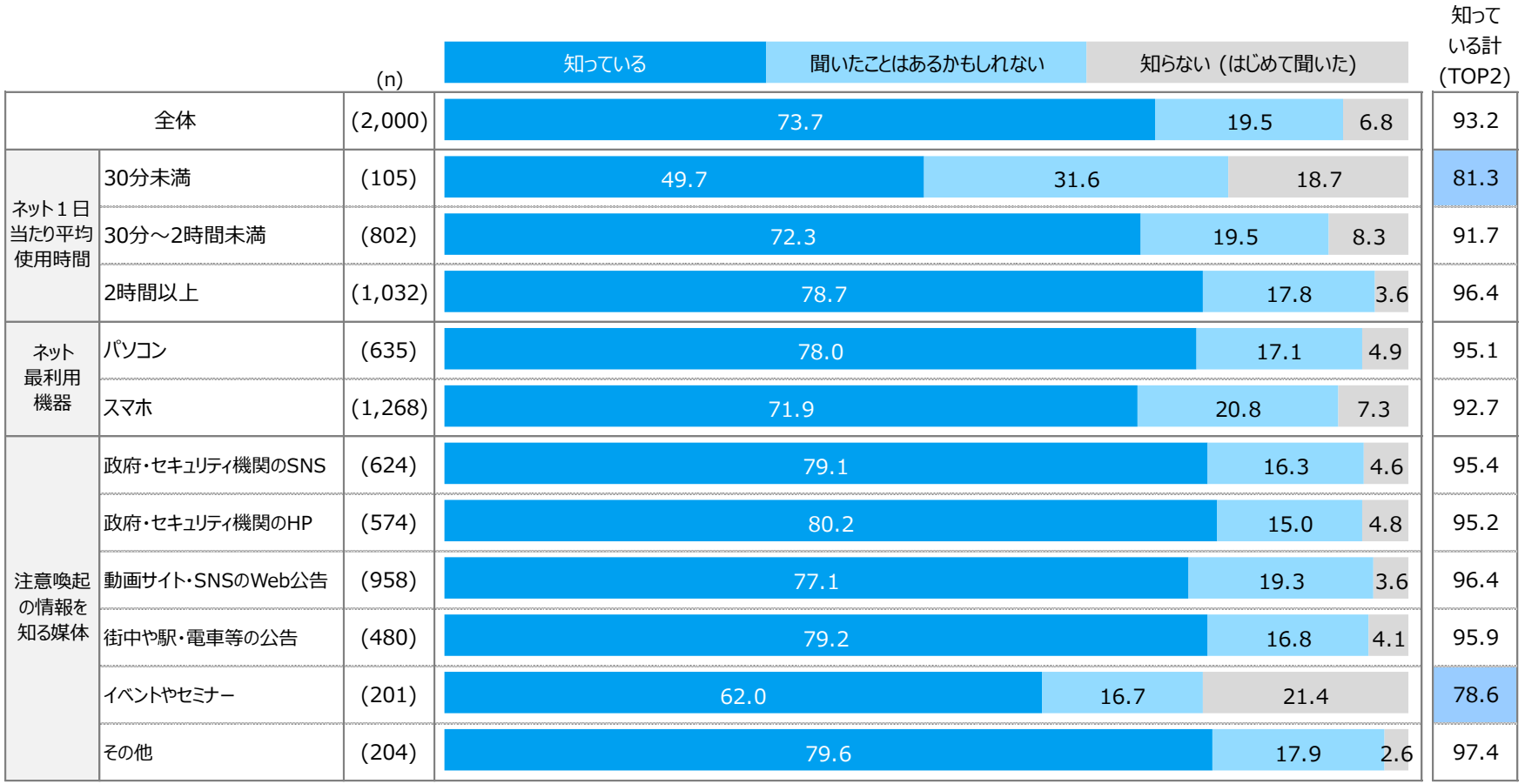
(%)

マルウェア感染の認知度

- マルウェア感染の認知度をみると、「知っている」73.7%、「聞いたことはあるかもしれない」19.5%となっており、合わせた認知計で93.2%を占めている。
- ネット使用時間別では、[30分未満]の認知計が81.3%と低く、使用時間が長いほど認知が高い傾向。
- ネット最利用機器別では、[パソコン]の認知が[スマホ]よりもやや高くなっている。
- 注意喚起の情報を知る媒体別では、[イベントやセミナー]の認知が8割弱と低くなっている。

（対象者）全数

Q10.あなたは、パソコン等で不審なメールの添付ファイルを開いたり、不審なサイトから不正なプログラムをダウンロードすることで、気づかないうちにパソコンやルータ等がコンピュータウイルスに感染するケースがあることを知っていますか。



※1%未満非表示

知っている計：「知っている+聞いたことはあるかもしれない」　(%)

サイバー攻撃の踏み台となるおそれの認知度

- サイバー攻撃の踏み台となるおそれの認知度をみると、「知っている」47.7%、「聞いたことはあるかもしれない」31.2%となっており、合わせた認知計で78.9%を占めている。
- ネット使用時間別では、[30分未満]の認知計が60.3%と低く、使用時間が長いほど認知が高い傾向。
- ネット最利用機器別では、[パソコン]の認知が[スマホ]よりもやや高くなっている。
- 注意喚起の情報を知る媒体別では、[政府・セキュリティ機関のHP]がやや高い。

（対象者）全数

Q11.あなたは、パソコンやルータ等、また、家庭内でネットにつないだ監視カメラ等のIoT機器がコンピュータウイルスに感染した場合、気づかないうちに、これらの機器が他への攻撃元になる（サイバー攻撃の「踏み台」になる）ケースがあることを知っていますか。

		(n)	知っている	聞いたことはあるかもしれない	知らない (はじめて聞いた)	知っている計 (TOP2)
全体		(2,000)	47.7	31.2	21.1	78.9
ネット1日当たり平均使用時間	30分未満	(105)	30.7	29.6	39.7	60.3
	30分～2時間未満	(802)	43.3	35.6	21.1	78.9
	2時間以上	(1,032)	54.1	27.7	18.2	81.8
ネット最利用機器	パソコン	(635)	55.5	29.2	15.3	84.7
	スマホ	(1,268)	43.4	32.9	23.6	76.4
注意喚起の情報を知る媒体	政府・セキュリティ機関のSNS	(624)	52.3	31.5	16.3	83.7
	政府・セキュリティ機関のHP	(574)	57.7	28.3	14.1	85.9
	動画サイト・SNSのWeb公告	(958)	49.0	32.3	18.7	81.3
	街中や駅・電車等の公告	(480)	51.1	31.0	17.9	82.1
	イベントやセミナー	(201)	45.7	24.4	29.9	70.1
	その他	(204)	48.4	28.8	22.9	77.1

※1%未満非表示

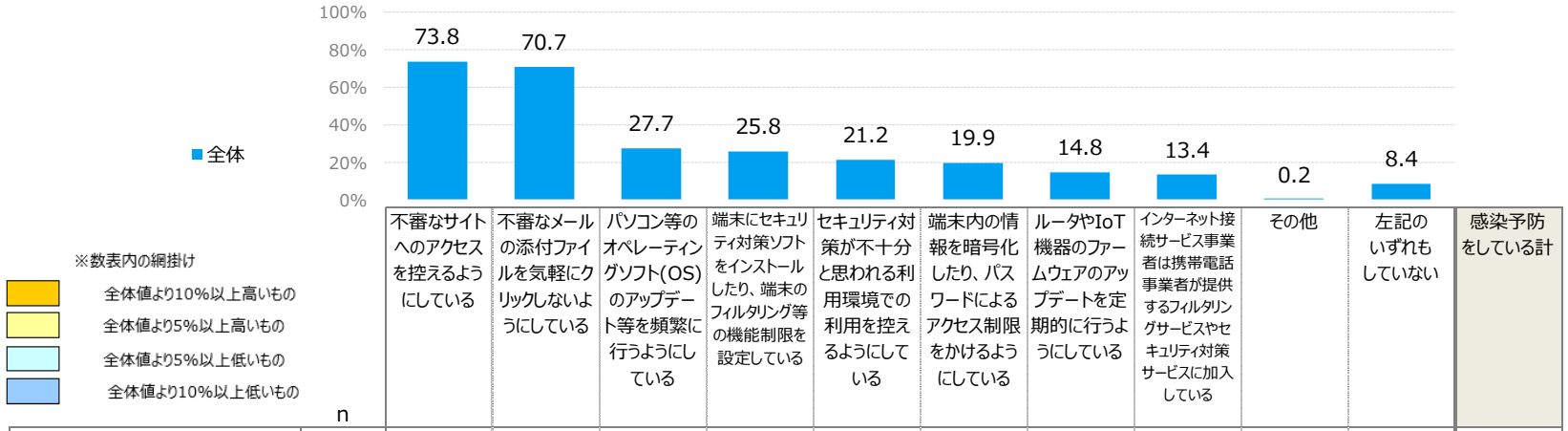
知っている計：「知っている+聞いたことはあるかもしれない」 (%)

コンピュータウイルス感染防止のために気をつけていること

- コンピュータウイルス感染防止のために気をつけていることをみると、「不審なサイトへのアクセスを控えるようにしている」が73.8%と高く、次いで「不審なメールの添付ファイルを気軽にクリックしないようにしている」が70.7%で続く。
- ネット使用時間別では、総じて使用時間が長いほどスコアが高い傾向。
- ネット最利用機器別では、[パソコン]で「OSのアップデート等を頻繁に行うようにしている」が高い。
- マルウェア感染認知別およびサイバー攻撃踏み台認知別では、共に[知っている]層のスコアが総じて高くなっている。
- ルーター等を設置している人のうち「ルータやIoT機器のファームウェアのアップデートを定期的に行うようにしている」は16.8%であり、ルーター等のアップデートによる対策は十分ではない。

（対象者）全数

Q12.あなたは、ご自分のパソコンやルータ等、また、家庭内でネットにつないだ監視カメラ等のIoT機器がコンピュータウイルスに感染しないようにするために、どのようなことに気をつけていますか。（いくつでも）



		n	不審なサイトへのアクセスを控えるようにしている	不審なメールの添付ファイルを気軽にクリックしないようにしている	パソコン等のオペレーティングソフト(OS)のアップデート等を頻繁に行うようにしている	端末にセキュリティ対策ソフトをインストールしたり、端末のフィルタリング等の機能制限を設定している	セキュリティ対策が不十分と思われる利用環境での利用を控えるようにしている	端末内の情報を暗号化したり、パスワードによるアクセス制限をかけるようにしている	ルータやIoT機器のファームウェアのアップデートを定期的に行うようにしている	インターネット接続サービス事業者は携帯電話事業者が提供するフィルタリングサービスやセキュリティ対策サービスに加入している	その他	左記のいずれもしていない	感染予防をしている計
全体		(2,000)	73.8	70.7	27.7	25.8	21.2	19.9	14.8	13.4	0.2	8.4	91.6
ネット１日当たり平均使用時間	30分未満	(105)	57.6	53.3	17.1	18.8	13.7	9.8	10.4	8.6	-	17.8	82.2
	30分～2時間未満	(802)	73.9	69.8	24.8	24.5	17.8	18.3	12.2	14.4	0.2	8.8	91.2
	2時間以上	(1,032)	76.3	74.3	32.1	28.7	25.1	22.6	17.9	13.7	0.2	6.0	94.0
ネット最利用機器	パソコン	(635)	76.0	72.5	39.4	34.1	22.1	20.0	18.0	15.9	0.1	6.6	93.4
	スマホ	(1,268)	73.0	70.0	21.8	21.6	21.3	19.6	13.0	12.3	0.1	8.9	91.1
マルウェア感染認知度	知っている	(1,475)	80.4	78.5	33.4	31.7	25.7	22.8	17.5	16.3	0.1	4.6	95.4
	聞いたことはある	(390)	62.9	57.5	12.2	11.5	10.3	14.1	8.2	5.8	0.4	9.2	90.8
	知らない	(136)	33.2	23.9	8.9	2.9	3.6	5.0	5.1	4.1	-	48.1	51.9
サイバー攻撃踏み台認知度	知っている	(954)	82.8	78.5	40.6	36.6	27.1	26.9	23.0	18.0	-	2.7	97.3
	聞いたことはある	(624)	70.7	69.9	19.2	18.5	18.6	17.9	8.3	10.9	0.3	7.1	92.9
	知らない	(422)	58.0	54.3	10.8	12.5	11.8	6.9	5.9	6.7	0.5	23.5	76.5
ルーター等	設置している	(1,648)	76.8	73.9	30.4	28.4	22.8	21.2	16.8	14.5	0.2	6.3	93.7

※全体で降順ソート

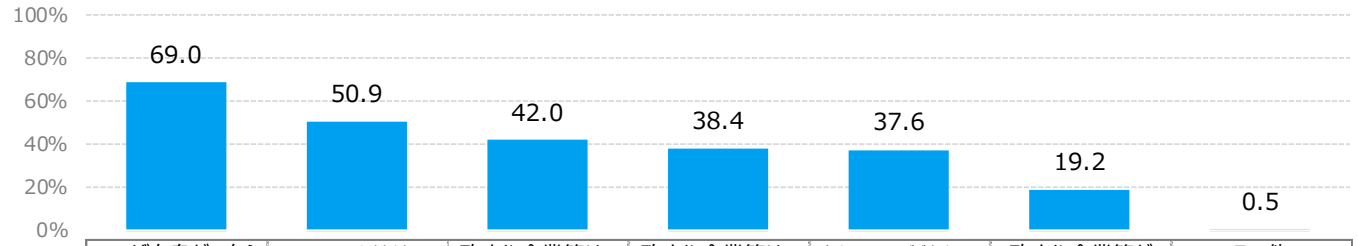
(%)

コンピュータウイルス感染を防ぐ有効な対策

- コンピュータウイルス感染を防ぐ有効な対策をみると、「ユーザ自身が、自らの保有する機器がコンピュータウイルスに感染しないように、もっと心掛けるべきである」が69.0%と高い。
- ネット使用時間別では、総じて使用時間が長いほどスコアが高い傾向。
- マルウェア感染認知別およびサイバー攻撃踏み台認知別では、共に[知っている]層のスコアが総じて高くなっている。

（対象者）全数

Q13.あなたは、パソコンやルータ等、また、家庭内でネットにつないだ監視カメラ等のIoT機器がコンピュータウイルスに感染するなどの被害を防ぐための対策として、どのようなことが有効だと思いますか。（いくつでも）



※数表内の網掛け

- 全体値より10%以上高いもの
- 全体値より5%以上高いもの
- 全体値より5%以上低いもの
- 全体値より10%以上低いもの

		n	ユーザ自身が、自らの保有する機器がコンピュータウイルスに感染しないように、もっと心掛けるべきである	インターネット接続サービスを提供するISPや携帯電話事業者、また、WiFi設置者等は、ユーザが安心してネットを利用できるよう、十分なセキュリティ水準を確保するよう努めるべきである	政府や企業等は、ユーザに対して、特に基本的なセキュリティ対策について、わかりやすい周知啓発に努めるべきである	政府や企業等は、ユーザに対して、高度なセキュリティ対策も含めて、周知啓発に努めるべきである	政府は、ユーザが安心してネットを利用できるよう、インターネット接続サービスを提供するISPや携帯電話事業者、また、WiFi設置者等に対して、わかりやすい指針等を示すなどにより、十分なセキュリティ水準が確保されるように努めるべきである	政府や企業等がユーザに対して周知啓発を行っても感染防止の効果には限界があり、周知啓発の必要性はあまり高くない	その他
全体		(2,000)	69.0	50.9	42.0	38.4	37.6	19.2	0.5
ネット１日当たり平均使用時間	30分未満	(105)	49.6	37.1	36.5	29.5	39.7	18.2	0.5
	30分～2時間未満	(802)	65.1	50.6	38.9	33.9	38.4	17.0	0.4
	2時間以上	(1,032)	74.5	53.2	45.7	43.9	36.3	21.6	0.5
ネット最利用機器	パソコン	(635)	70.8	49.9	41.1	38.4	35.7	18.7	0.6
	スマホ	(1,268)	68.5	51.7	42.6	38.6	38.5	19.8	0.3
マルウェア感染認知度	知っている	(1,475)	75.7	56.2	44.6	42.0	39.0	19.7	0.3
	聞いたことはある	(390)	55.0	41.3	39.9	32.5	29.5	18.9	0.9
	知らない	(136)	37.0	19.9	19.7	16.3	45.9	14.1	0.2
サイバー攻撃踏み台認知度	知っている	(954)	80.8	54.6	45.5	43.4	36.0	20.1	0.4
	聞いたことはある	(624)	60.3	47.9	40.3	35.0	34.5	17.8	0.6
	知らない	(422)	55.1	46.7	36.3	32.0	46.0	19.1	0.4

※全体で降順ソート

(%)

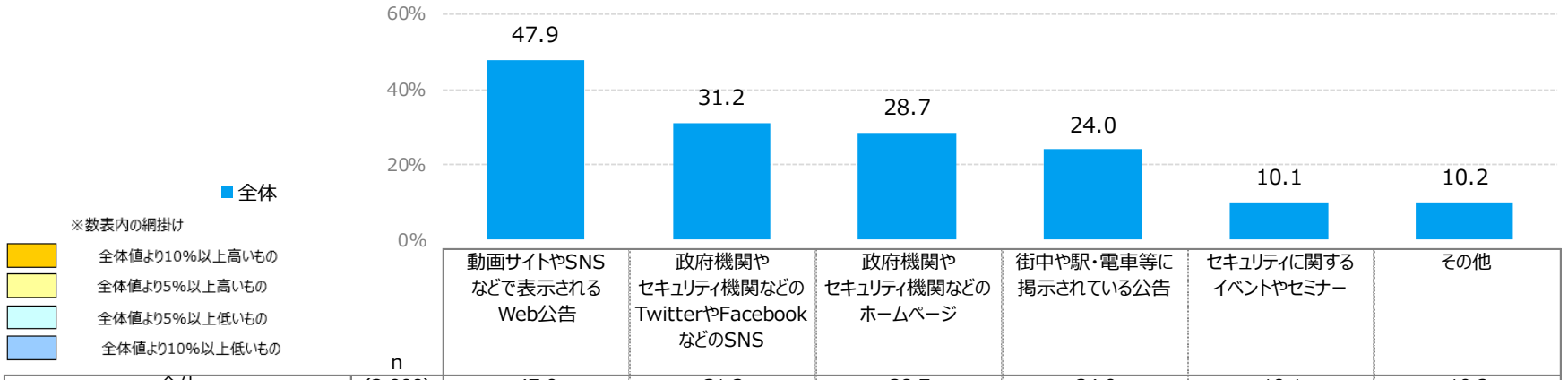
注意喚起の情報を知る媒体

- 注意喚起の情報を知る媒体をみると、「動画サイトやSNSなどで表示されるWeb公告」が47.9%と高く、次いで「政府機関やセキュリティ機関などのTwitterやFacebookなどのSNS」31.2%、「政府機関やセキュリティ機関などのホームページ」28.7%と続く。
- 職業別では、大学生・大学院生および専門家※で「街中や駅・電車等に掲示されている公告」が顕著。
- ネット使用時間別では、概ね使用時間が長いほどスコアが高い傾向。
- ネット最利用機器別では、[パソコン]で「政府機関やセキュリティ機関などのホームページ」がやや高い。

※ 専門家：医師、弁護士、会計士など

（対象者）全数

Q14.あなたは、セキュリティに関する注意喚起の情報を、どのような形で知ることが多いですか。（いくつでも）



		n	動画サイトやSNSなどで表示されるWeb公告	政府機関やセキュリティ機関などのTwitterやFacebookなどのSNS	政府機関やセキュリティ機関などのホームページ	街中や駅・電車等に掲示されている公告	セキュリティに関するイベントやセミナー	その他
全体		(2,000)	47.9	31.2	28.7	24.0	10.1	10.2
職業	高校生	(3)	29.9	38.8	-	54.6	12.4	-
	専門学校生	(11)	73.3	16.4	10.3	10.3	10.3	57.7
	大学生・大学院生	(69)	43.0	37.5	21.0	45.8	11.8	8.2
	会社員	(882)	51.3	33.8	28.2	24.8	10.9	7.5
	公務員・団体職員	(126)	39.7	34.4	34.2	15.8	9.0	8.0
	専門家	(45)	46.8	17.2	23.7	47.5	0.9	11.6
	自営業	(87)	51.9	29.7	30.4	23.9	6.5	8.1
	自由業	(35)	45.0	24.5	35.8	21.2	18.2	13.6
	パート・アルバイト	(288)	45.7	29.2	25.2	22.9	10.0	10.0
	家事手伝い	(7)	24.8	15.9	34.7	37.3	3.3	15.3
	専業主婦・主夫	(286)	45.7	30.5	30.8	20.0	6.5	15.0
	無職	(148)	44.3	22.7	32.2	20.0	15.4	16.1
	その他	(14)	43.1	44.4	46.2	15.4	9.8	17.4
ネット１日当たり平均使用時間	30分未満	(105)	33.8	19.9	17.8	16.3	14.2	17.6
	30分～2時間未満	(802)	46.7	29.2	28.1	26.8	9.7	8.1
	2時間以上	(1,032)	50.7	33.6	31.3	23.0	9.6	11.2
ネット最利用機器	パソコン	(635)	45.3	28.5	37.2	18.7	11.0	10.9
	スマホ	(1,268)	49.2	33.1	24.6	27.1	8.9	9.7

※全体で降順ソート

※ 灰色の網がけについてはサンプル数が少ないため参考値

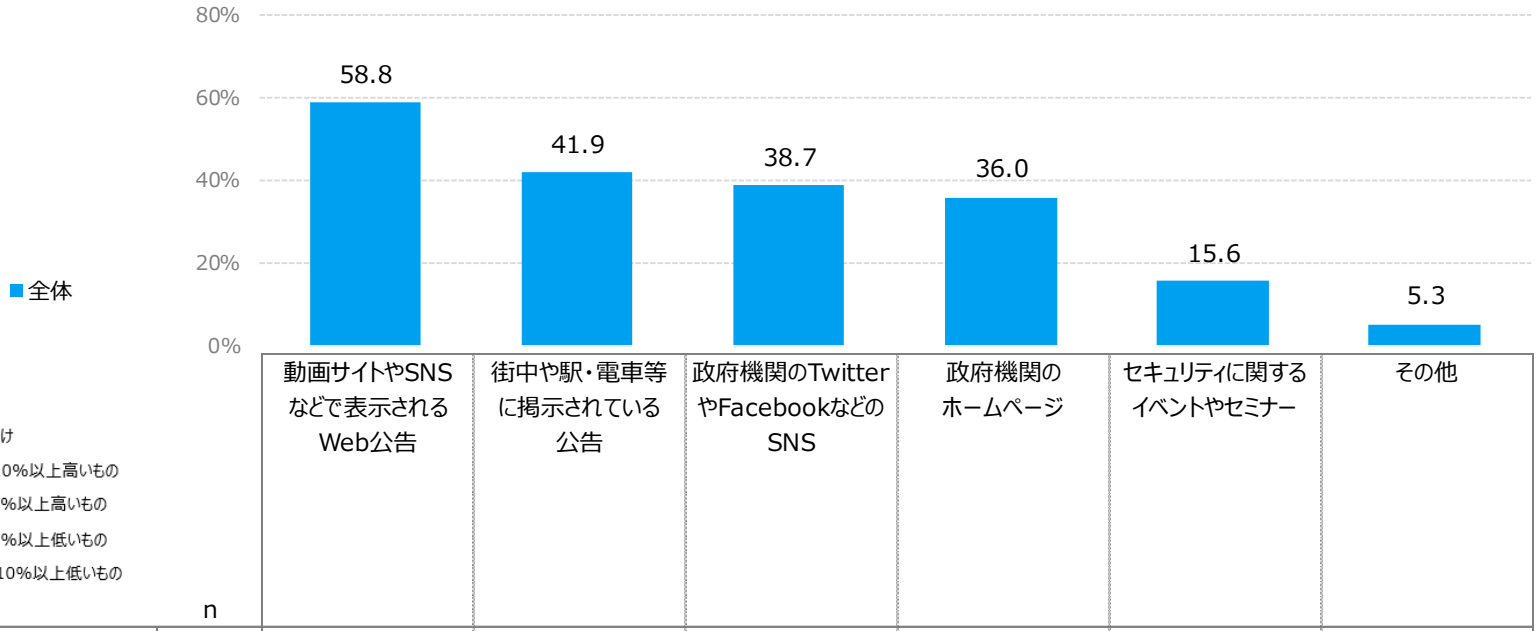
(%)

政府機関の注意喚起情報の適切な伝達手法

- 政府機関の注意喚起情報の適切な伝達手法をみると、「動画サイトやSNSなどで表示されるWeb公告」が58.8%と高く、次いで「街中や駅・電車等に掲示されている公告」41.9%、「政府機関のTwitterやFacebookなどのSNS」38.7%と続く。
- ネット使用時間別では、概ね使用時間が長いほどスコアが高い傾向。
- ネット最利用機器別では、[パソコン]で「動画サイトやSNSなどで表示されるWeb公告」「街中や駅・電車等に掲示されている公告」がやや低い。

（対象者）全数

Q15.あなたは、政府機関からの注意喚起情報の伝達手法として、どのような形が適切だと思いますか。（いくつでも）



※数表内の網掛け

- 全体値より10%以上高いもの
- 全体値より5%以上高いもの
- 全体値より5%以上低いもの
- 全体値より10%以上低いもの

		n	動画サイトやSNSなどで表示されるWeb公告	街中や駅・電車等に掲示されている公告	政府機関のTwitterやFacebookなどのSNS	政府機関のホームページ	セキュリティに関するイベントやセミナー	その他
全体		(2,000)	58.8	41.9	38.7	36.0	15.6	5.3
ネット１日当たり平均使用時間	30分未満	(105)	42.9	31.1	22.9	31.8	20.3	11.2
	30分～2時間未満	(802)	57.4	41.2	33.7	36.2	16.3	3.5
	2時間以上	(1,032)	62.6	44.5	44.2	37.1	13.7	6.2
ネット最利用機器	パソコン	(635)	53.4	34.5	38.5	38.7	15.4	6.0
	スマホ	(1,268)	62.1	46.3	39.4	34.0	15.7	4.8

※全体で降順ソート

(%)