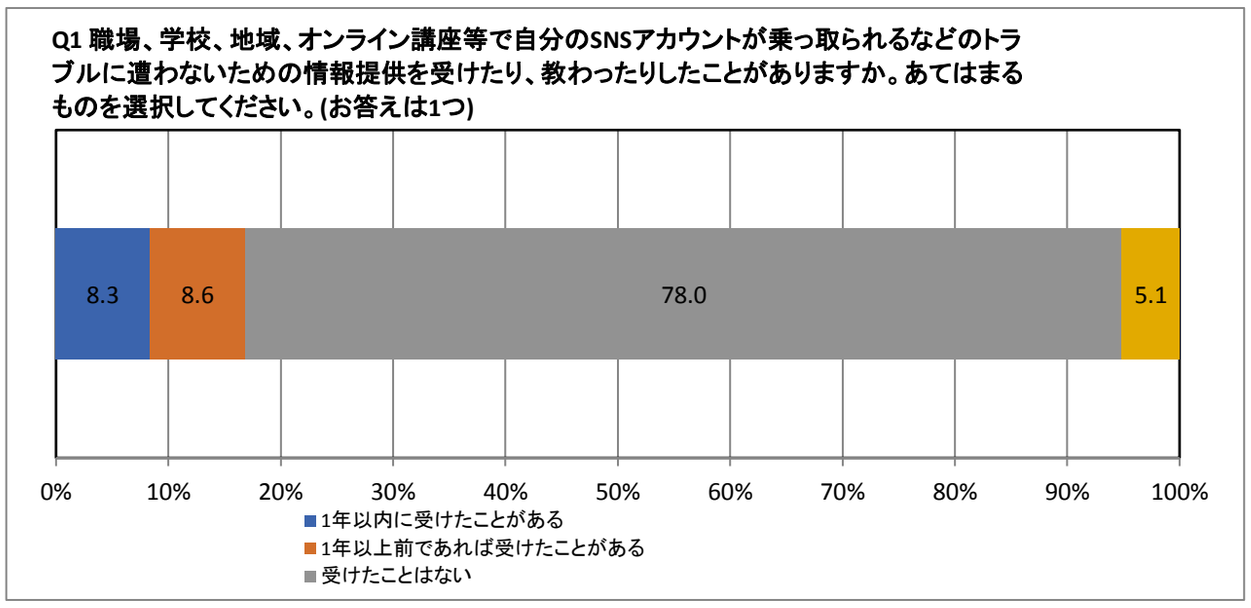
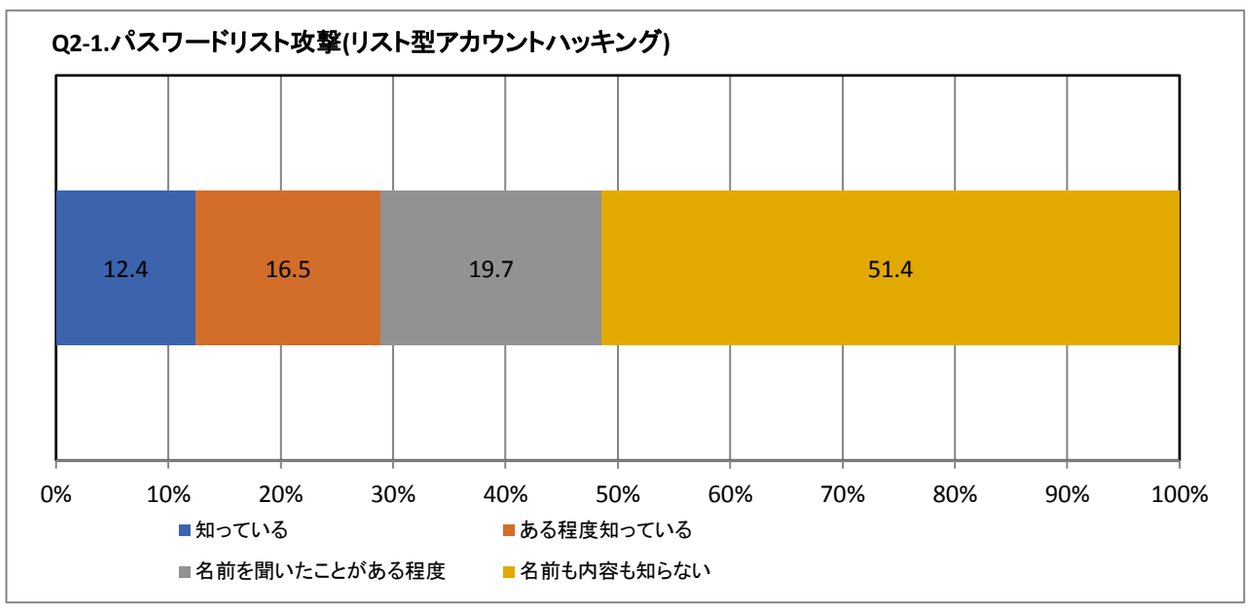
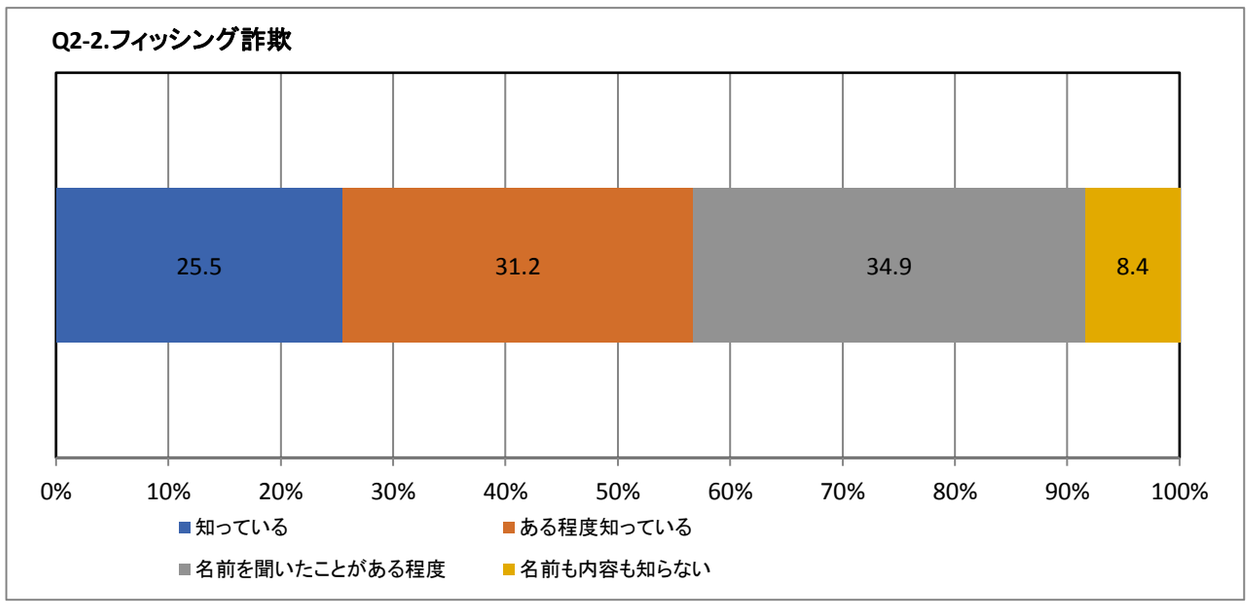
Q1 職場、学校、地域、オンライン講座等で自分のSNSアカウントが乗っ取られるなどのトラブルに遭わないための情報提供を受けたり、教わったりしたことがありますか。あてはまるものを選択してください。(お答えは1つ)	度数	%
1年以内に受けたことがある	415	8.3
1年以上前であれば受けたことがある	429	8.6
受けたことはない	3900	78.0
覚えていない	256	5.1
集計母数	5000	100.0



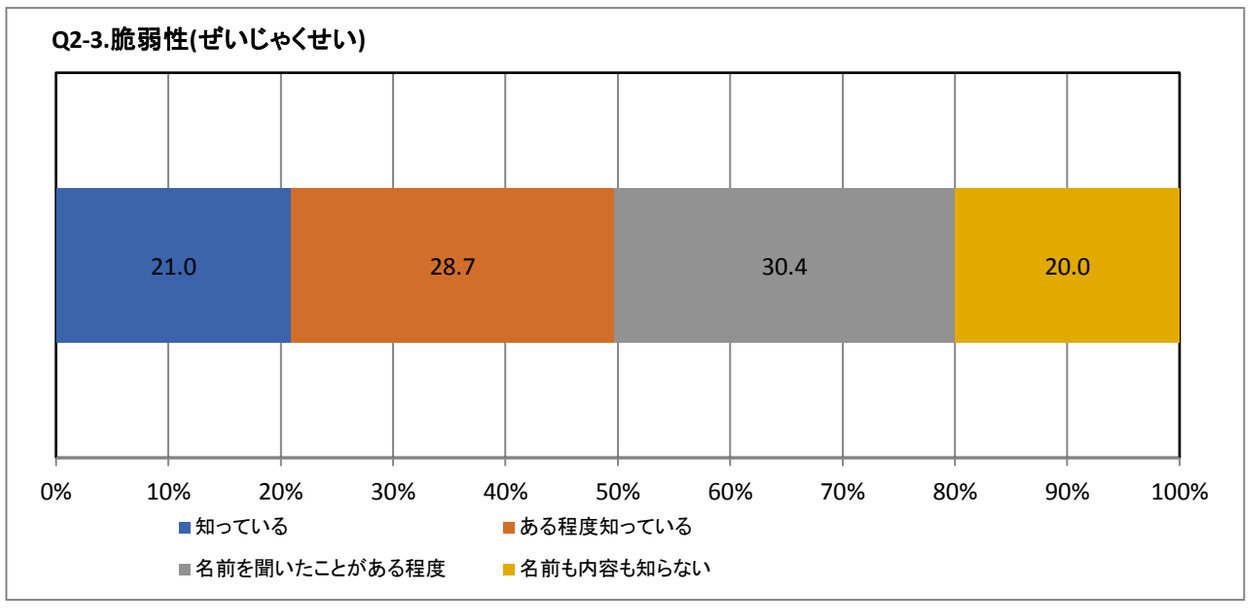
Q2 あなたは、次のようなネット上での攻撃・脅威などがどのようなものかご存知ですか。あてはまるものをそれぞれ1つずつ選択してください。(お答えはそれぞれ1つ)		
Q2-1.パスワードリスト攻撃(リスト型アカウントハッキング)	度数	%
知っている	622	12.4
ある程度知っている	823	16.5
名前を聞いたことがある程度	983	19.7
名前も内容も知らない	2572	51.4
集計母数	5000	100.0



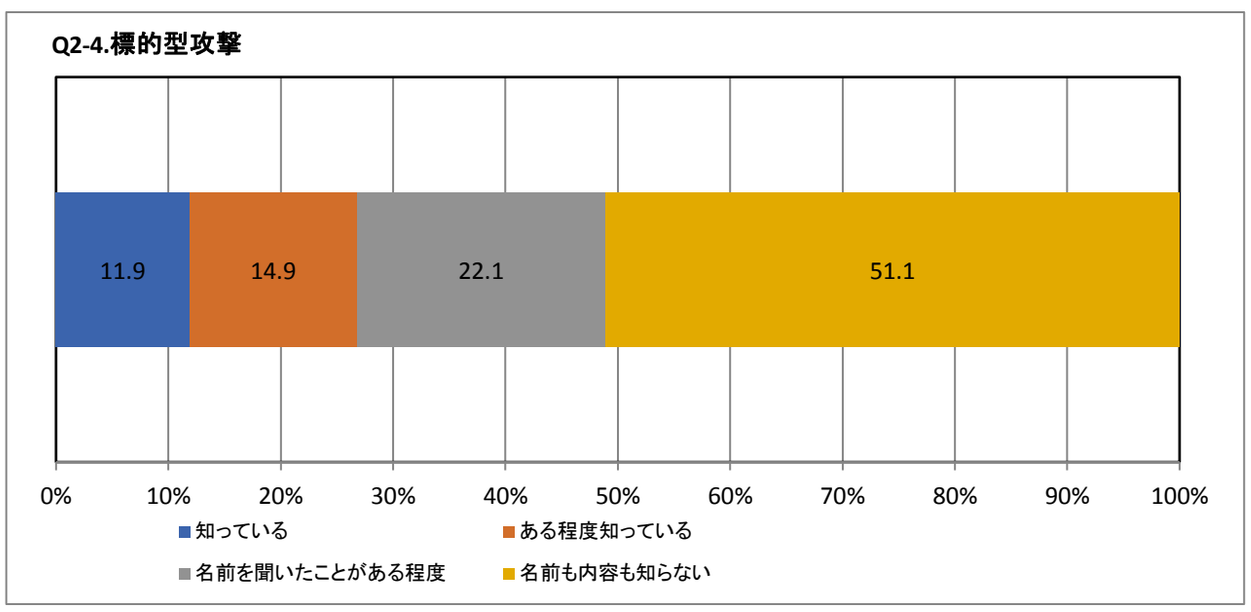
Q2-2.フィッシング詐欺	度数	%
知っている	1276	25.5
ある程度知っている	1559	31.2
名前を聞いたことがある程度	1745	34.9
名前も内容も知らない	420	8.4
集計母数	5000	100.0



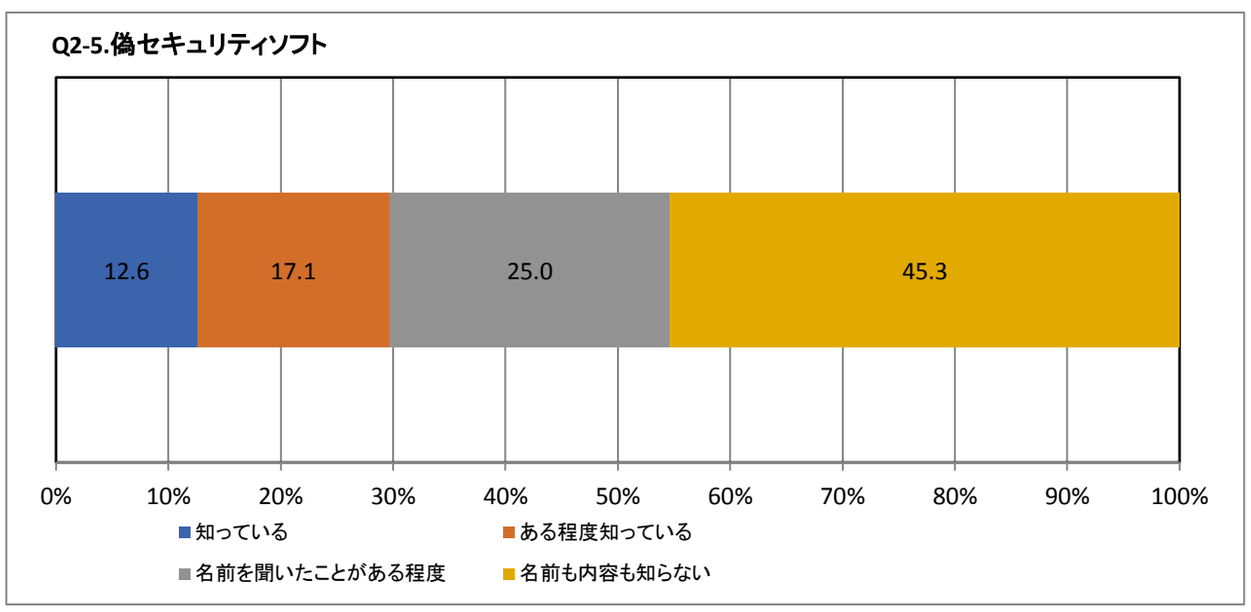
Q2-3.脆弱性(ぜいじゃくせい)	度数	%
知っている	1048	21.0
ある程度知っている	1435	28.7
名前を聞いたことがある程度	1519	30.4
名前も内容も知らない	998	20.0
集計母数	5000	100.0



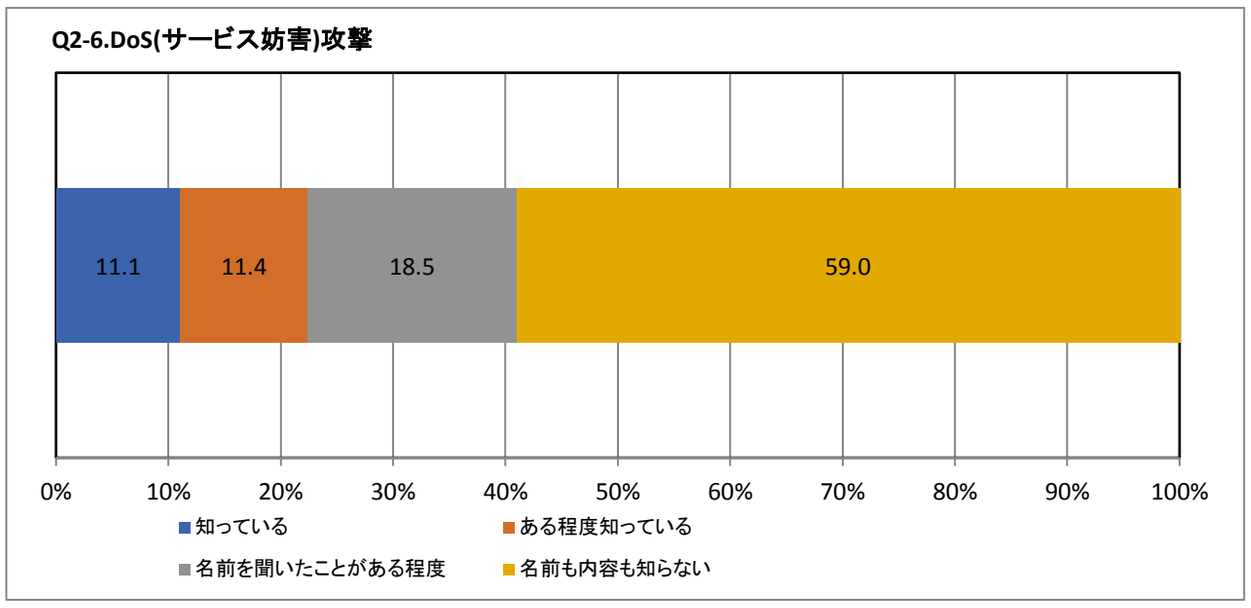
Q2-4.標的型攻撃	度数	%
知っている	594	11.9
ある程度知っている	746	14.9
名前を聞いたことがある程度	1105	22.1
名前も内容も知らない	2555	51.1
集計母数	5000	100.0



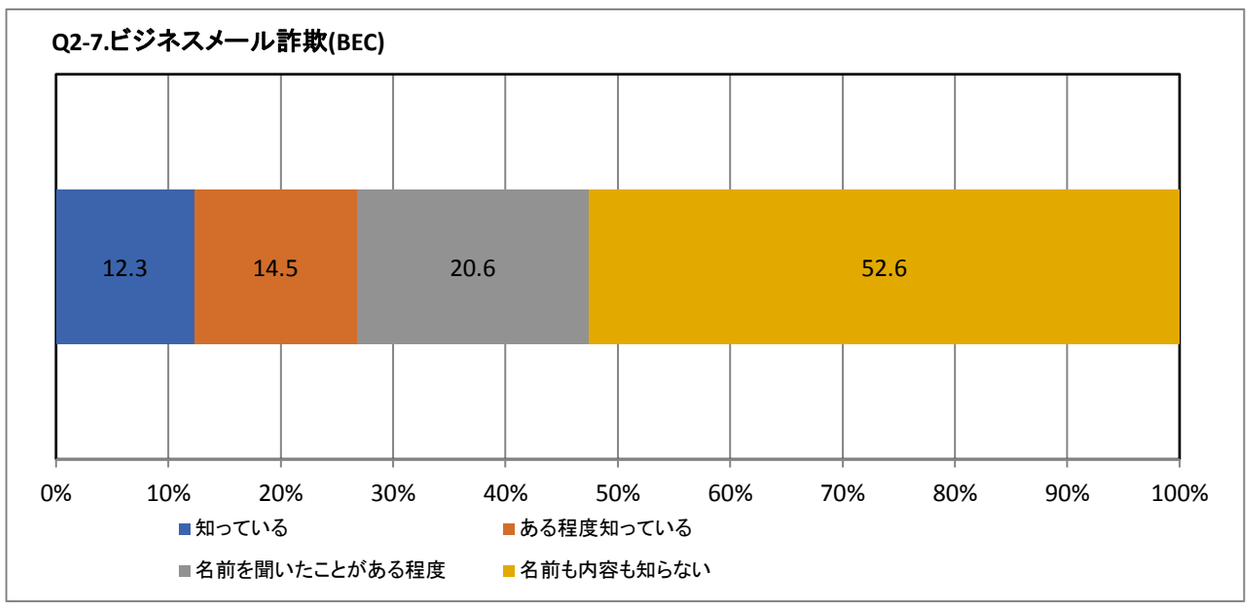
Q2-5.偽セキュリティソフト	度数	%
知っている	629	12.6
ある程度知っている	855	17.1
名前を聞いたことがある程度	1250	25.0
名前も内容も知らない	2266	45.3
集計母数	5000	100.0



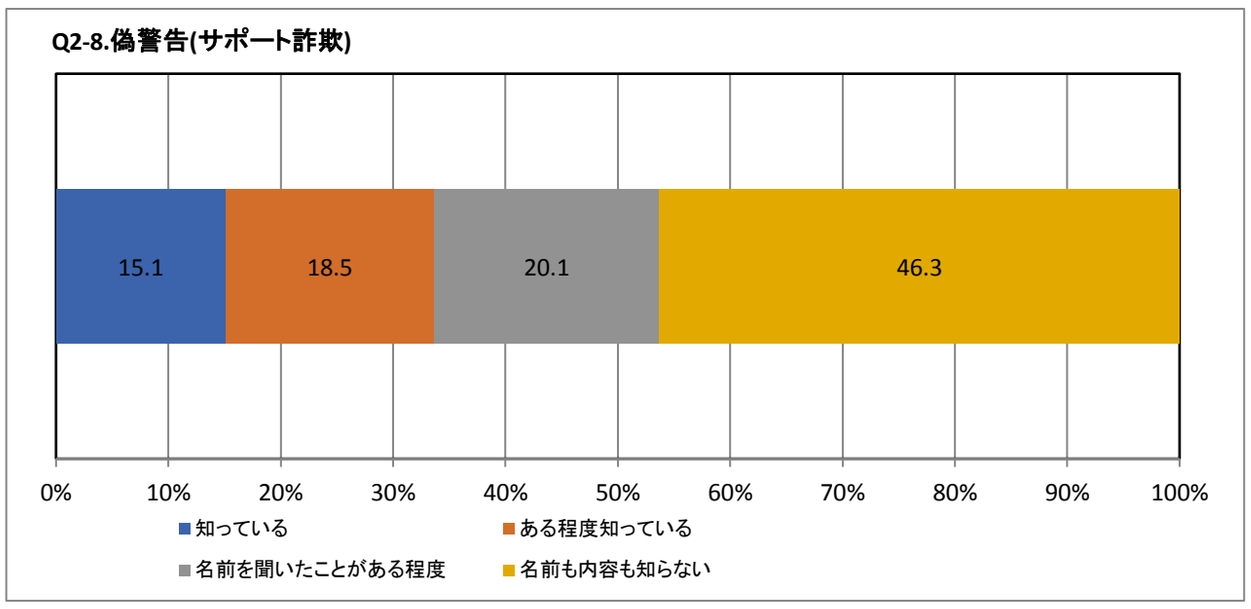
Q2-6.DoS(サービス妨害)攻撃	度数	%
知っている	553	11.1
ある程度知っている	569	11.4
名前を聞いたことがある程度	927	18.5
名前も内容も知らない	2951	59.0
集計母数	5000	100.0



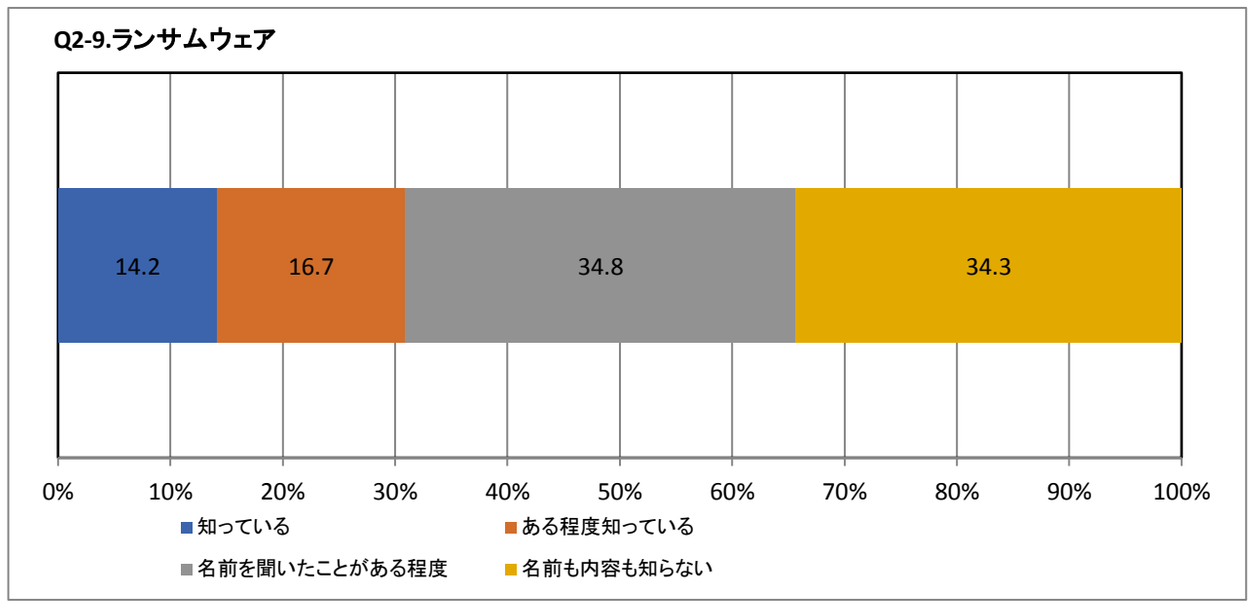
Q2-7.ビジネスメール詐欺(BEC)	度数	%
知っている	614	12.3
ある程度知っている	726	14.5
名前を聞いたことがある程度	1031	20.6
名前も内容も知らない	2629	52.6
集計母数	5000	100.0



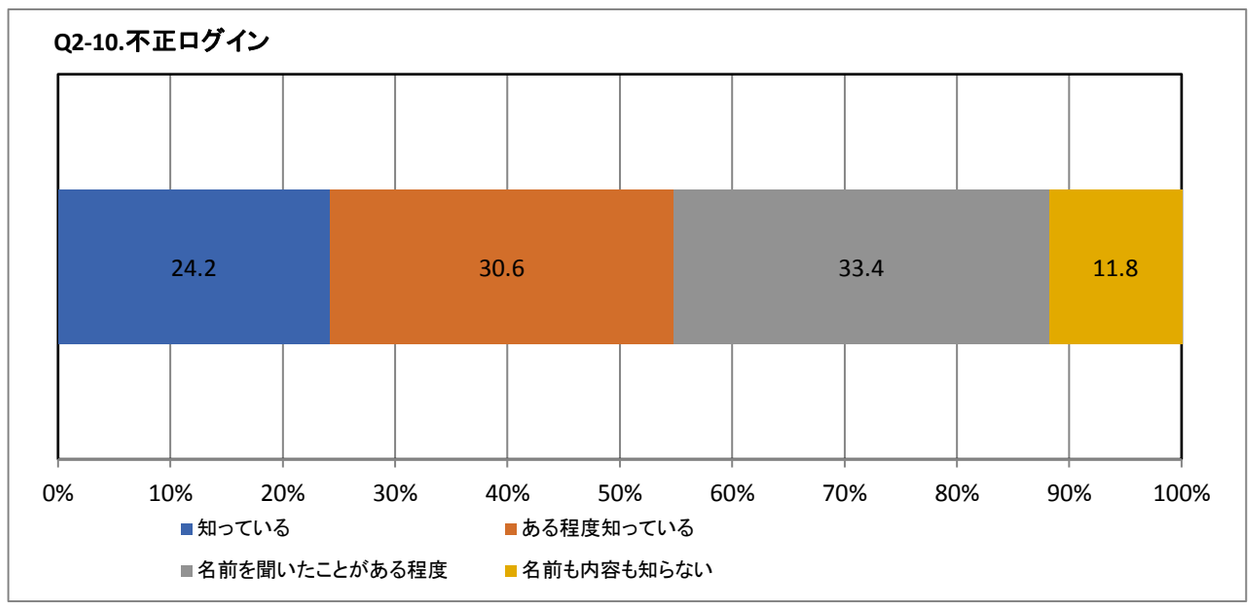
Q2-8.偽警告(サポート詐欺)	度数	%
知っている	756	15.1
ある程度知っている	926	18.5
名前を聞いたことがある程度	1004	20.1
名前も内容も知らない	2314	46.3
集計母数	5000	100.0



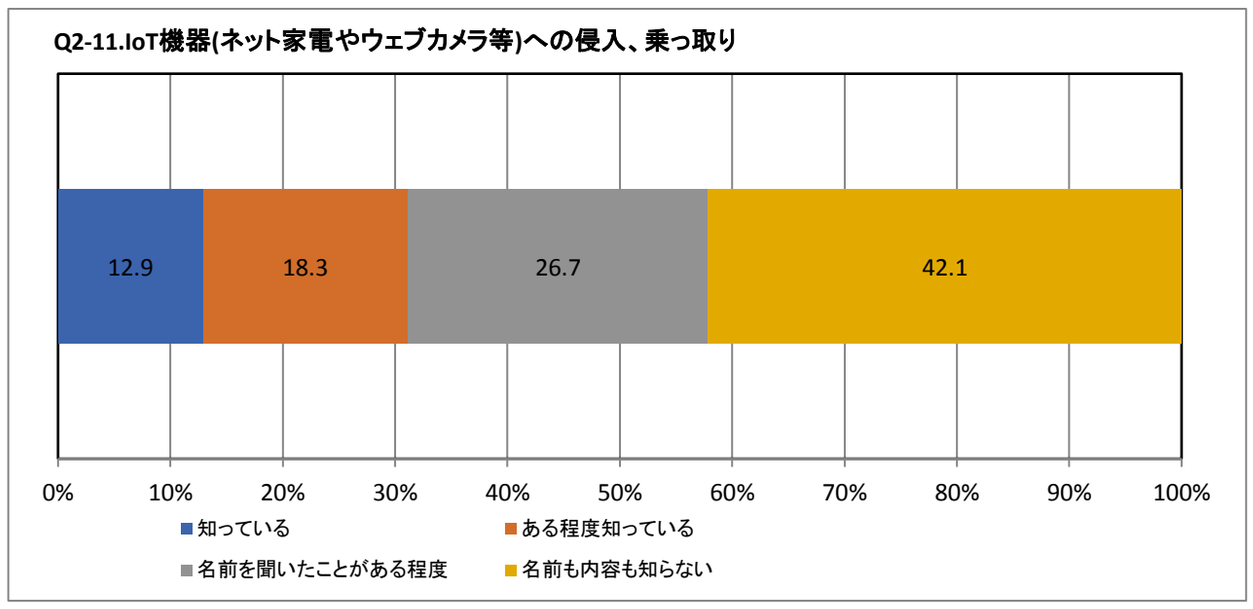
Q2-9.ランサムウェア	度数	%
知っている	710	14.2
ある程度知っている	835	16.7
名前を聞いたことがある程度	1740	34.8
名前も内容も知らない	1715	34.3
集計母数	5000	100.0



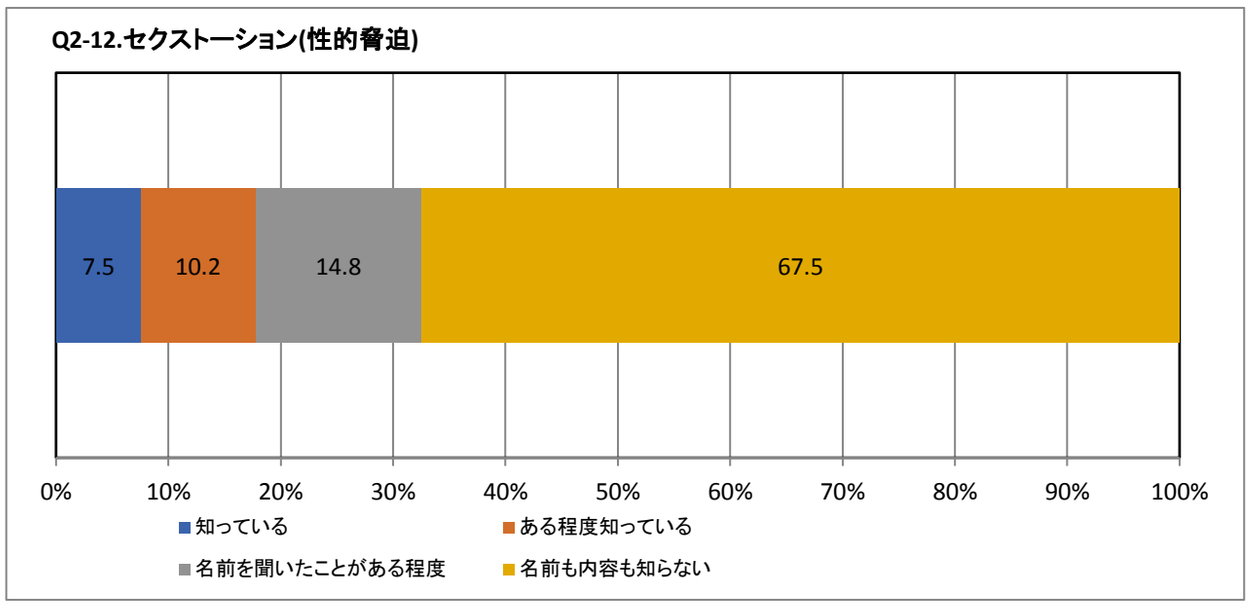
Q2-10.不正ログイン	度数	%
知っている	1210	24.2
ある程度知っている	1529	30.6
名前を聞いたことがある程度	1672	33.4
名前も内容も知らない	589	11.8
集計母数	5000	100.0



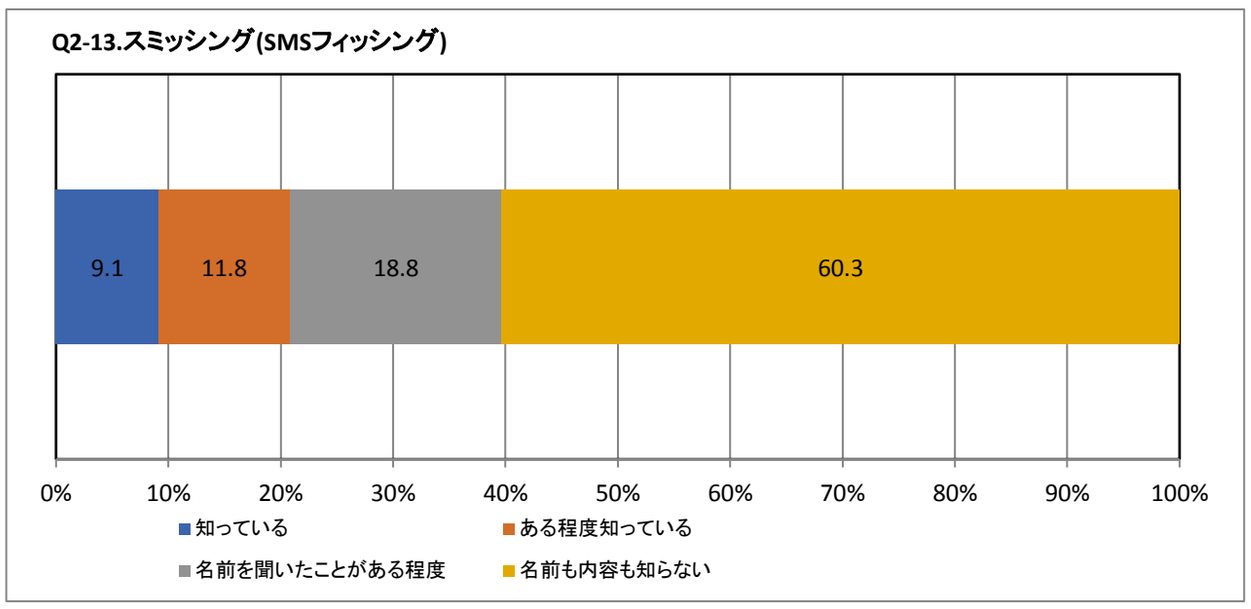
Q2-11.IoT機器(ネット家電やウェブカメラ等)への侵入、乗っ取り	度数	%
知っている	645	12.9
ある程度知っている	913	18.3
名前を聞いたことがある程度	1336	26.7
名前も内容も知らない	2106	42.1
集計母数	5000	100.0



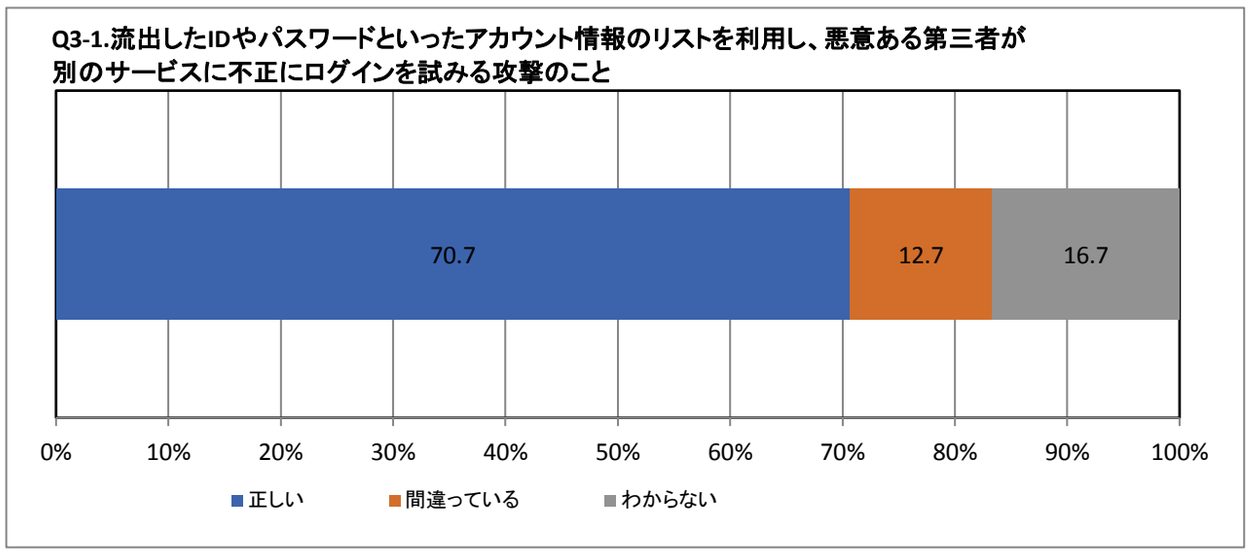
Q2-12.セクストーション(性的脅迫)	度数	%
知っている	376	7.5
ある程度知っている	512	10.2
名前を聞いたことがある程度	738	14.8
名前も内容も知らない	3374	67.5
集計母数	5000	100.0



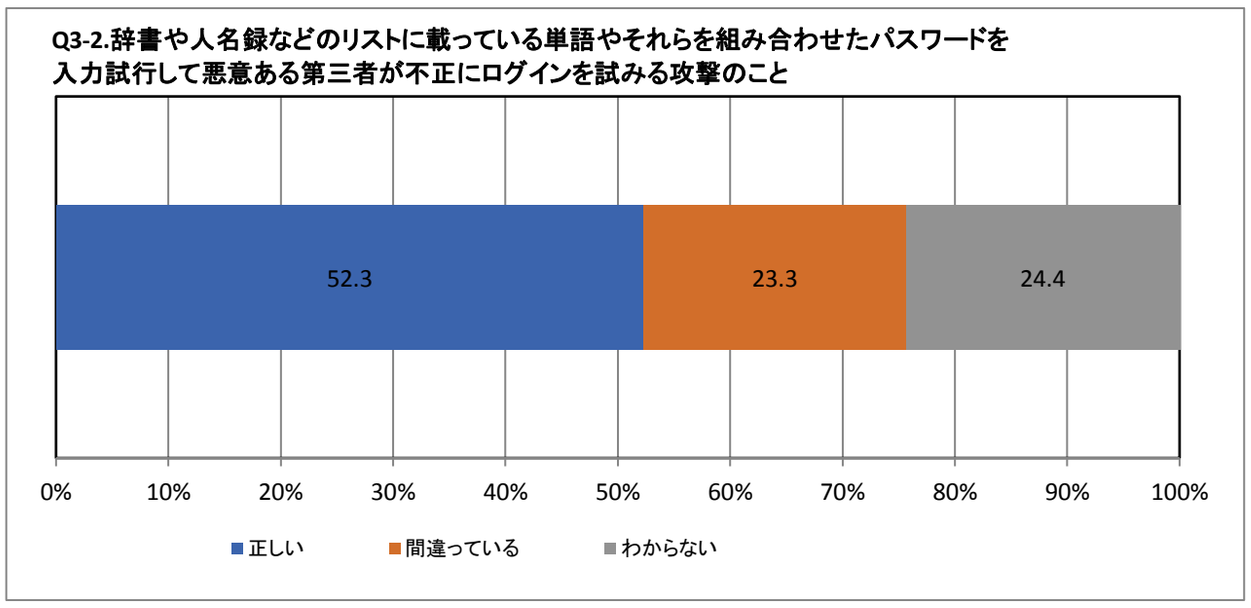
Q2-13.スミッシング(SMSフィッシング)	度数	%
知っている	455	9.1
ある程度知っている	588	11.8
名前を聞いたことがある程度	941	18.8
名前も内容も知らない	3016	60.3
集計母数	5000	100.0



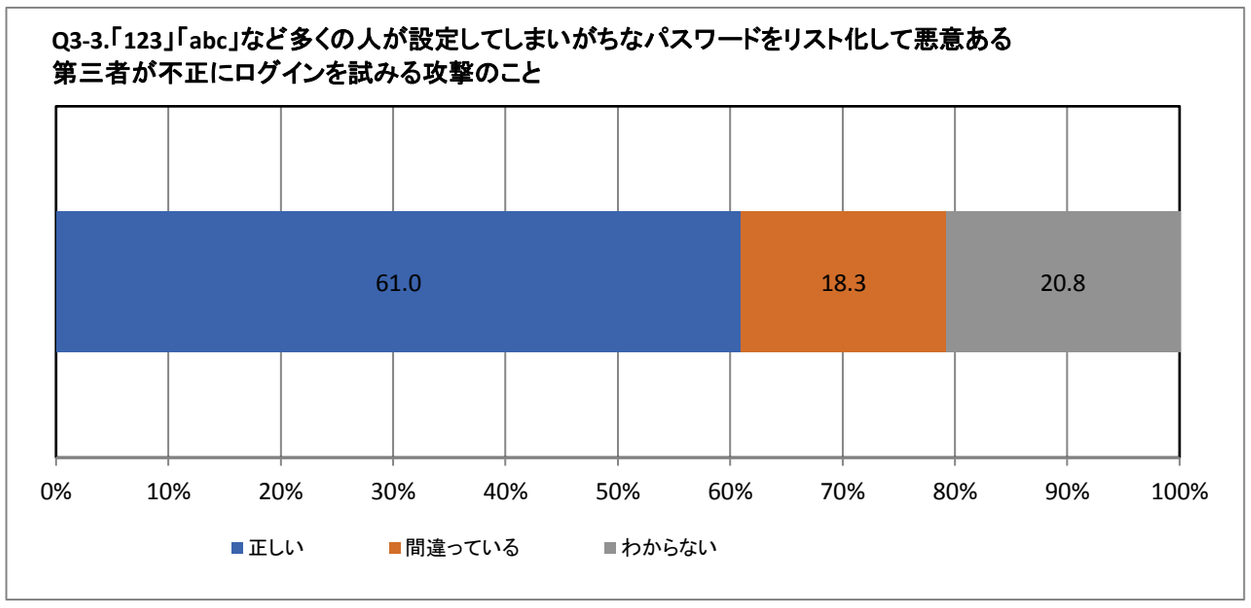
Q3 次に挙げる攻撃や脅威の手口などの概要や特徴、被害の例に関する説明の内容が「正しいか」「間違っているか」を選択してください。(お答えはそれぞれ1つ)		
Q3-1：パスワードリスト攻撃 流出したIDやパスワードといったアカウント情報のリストを利用し、悪意ある第三者が別のサービスに不正にログインを試みる攻撃のこと	度数	%
正しい	1021	70.7
間違っている	183	12.7
わからない	241	16.7
集計母数	1445	100.0



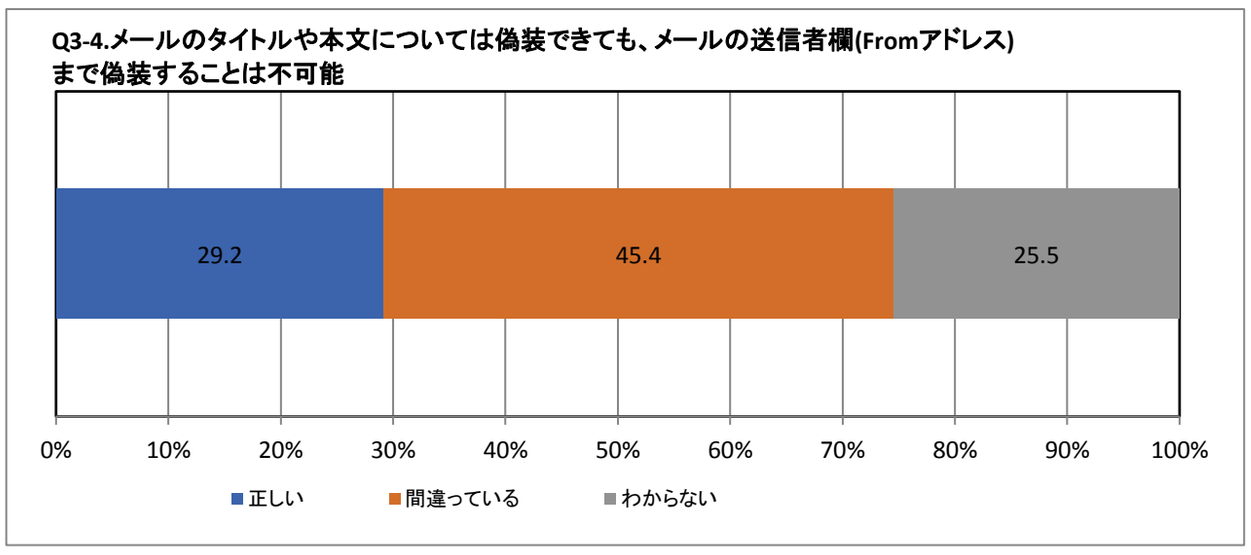
Q3-2：パスワードリスト攻撃 .辞書や人名録などのリストに載っている単語やそれらを組み合わせたパスワードを入力試行して悪意ある第三者が不正にログインを試みる攻撃のこと	度数	%
正しい	756	52.3
間違っている	337	23.3
わからない	352	24.4
集計母数	1445	100.0



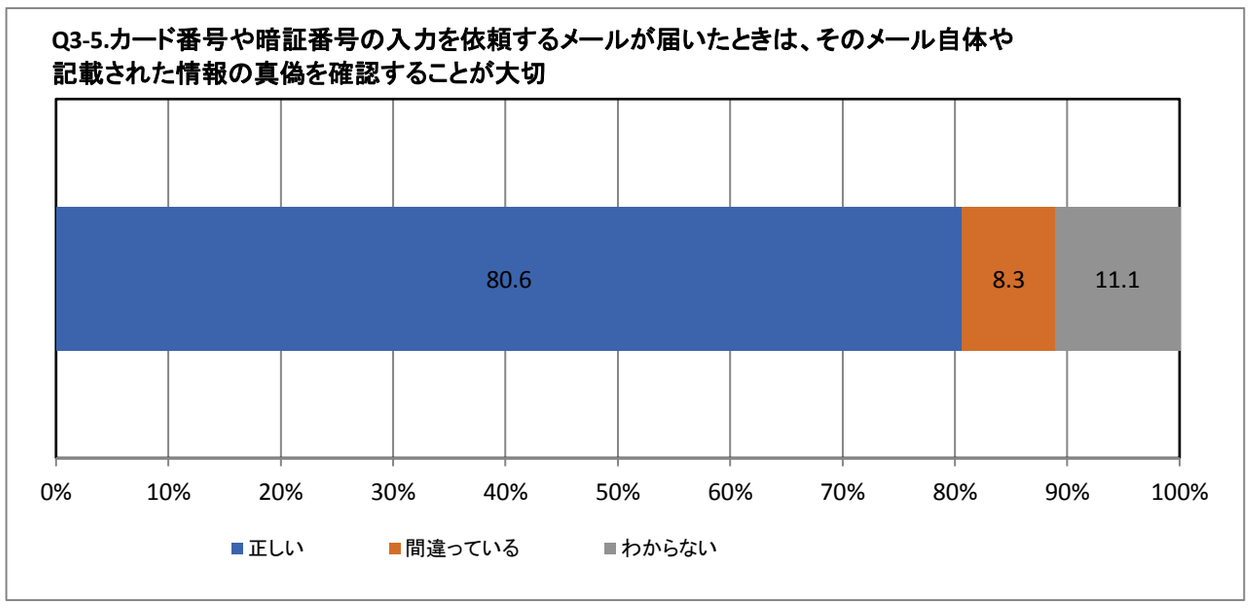
Q3-3：パスワードリスト攻撃 「123」「abc」など多くの人が設定してしまいがちなパスワードをリスト化して悪意ある第三者が不正にログインを試みる攻撃のこと	度数	%
正しい	881	61.0
間違っている	264	18.3
わからない	300	20.8
集計母数	1445	100.0



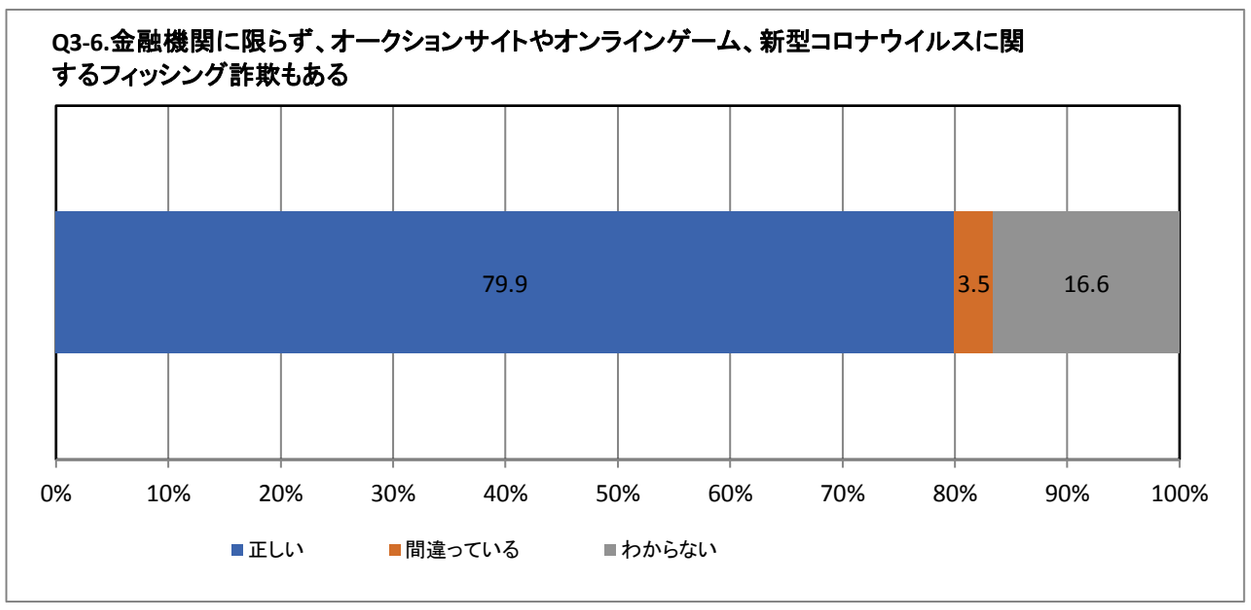
Q3-4：フィッシング詐欺 メールのタイトルや本文については偽装できても、メールの送信者欄(Fromアドレス)まで偽装することは不可能	度数	%
正しい	827	29.2
間違っている	1286	45.4
わからない	722	25.5
集計母数	2835	100.0



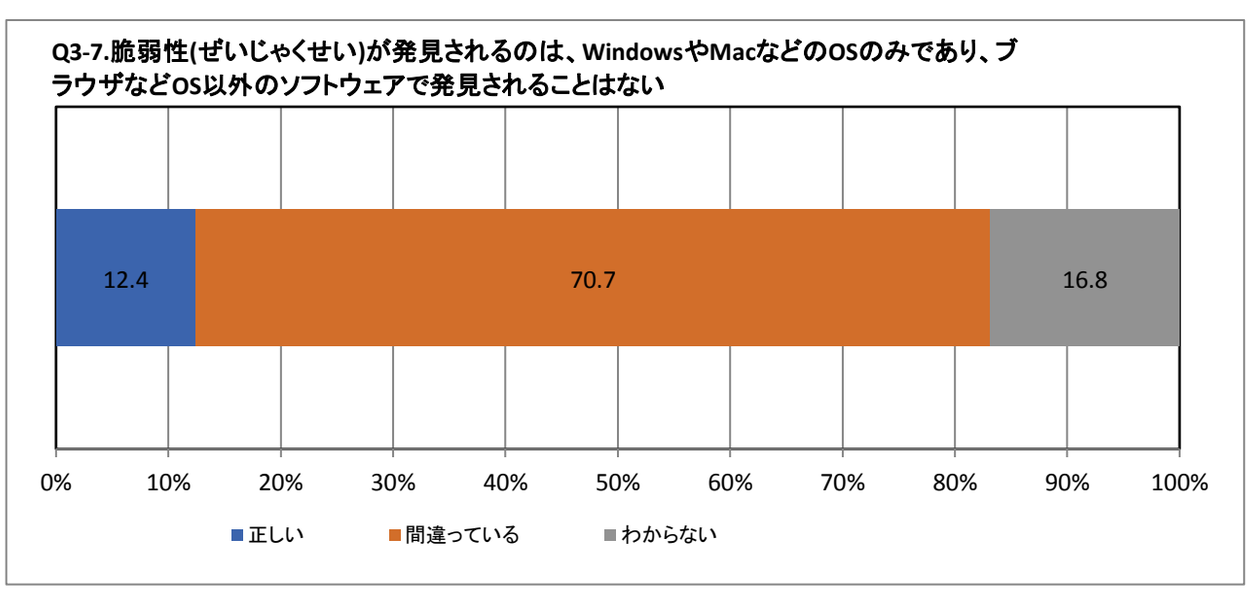
Q3-5：フィッシング詐欺 カード番号や暗証番号の入力を依頼するメールが届いたときは、そのメール自体や記載された情報の真偽を確認することが大切	度数	%
正しい	2286	80.6
間違っている	235	8.3
わからない	314	11.1
集計母数	2835	100.0



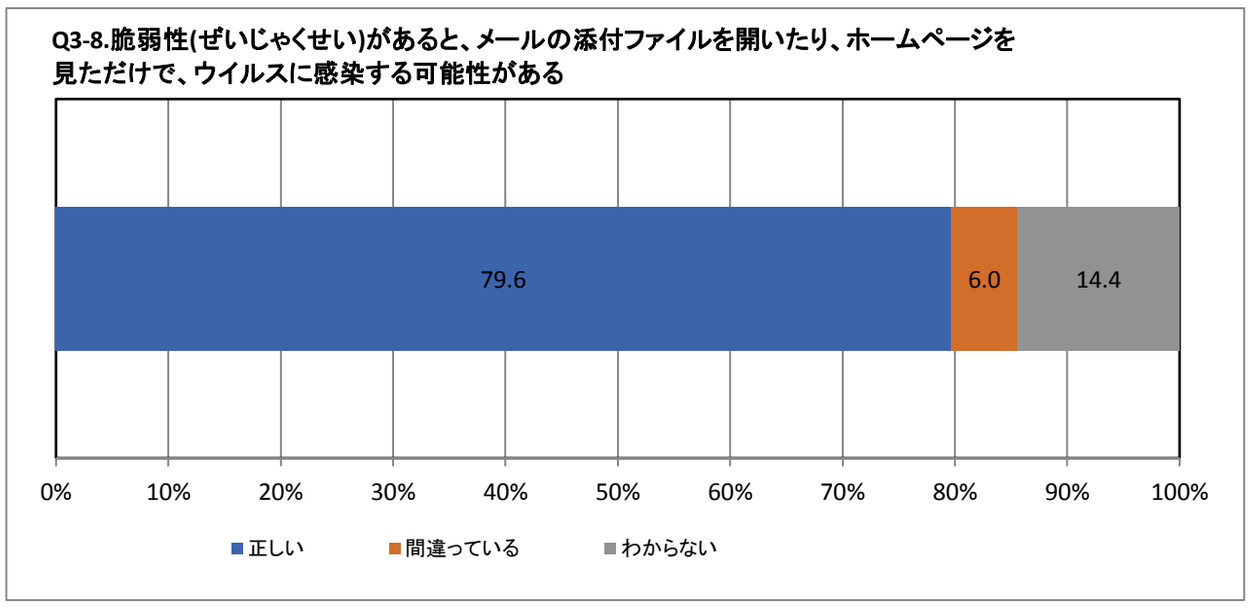
Q3-6：フィッシング詐欺 金融機関に限らず、オークションサイトやオンラインゲーム、新型コロナウイルスに関するフィッシング詐欺もある	度数	%
正しい	2265	79.9
間違っている	100	3.5
わからない	470	16.6
集計母数	2835	100.0



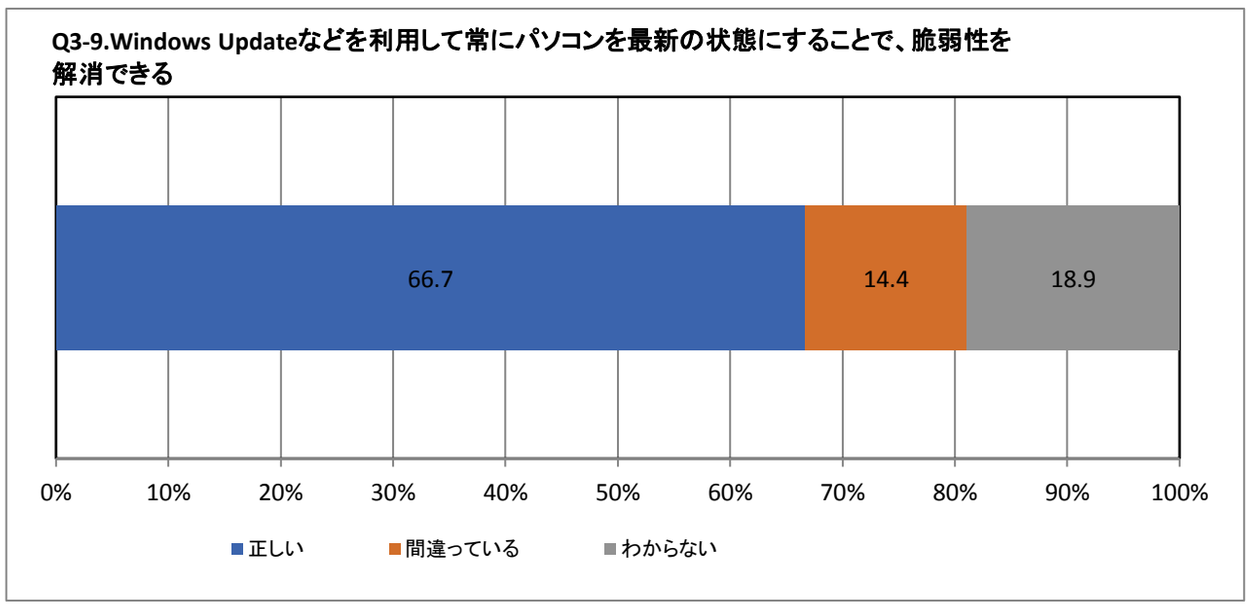
Q3-7：脆弱性 脆弱性(ぜいじゃくせい)が発見されるのは、WindowsやMacなどのOSのみであり、ブラウザなどOS以外のソフトウェアで発見されることはない	度数	%
正しい	309	12.4
間違っている	1756	70.7
わからない	418	16.8
集計母数	2483	100.0



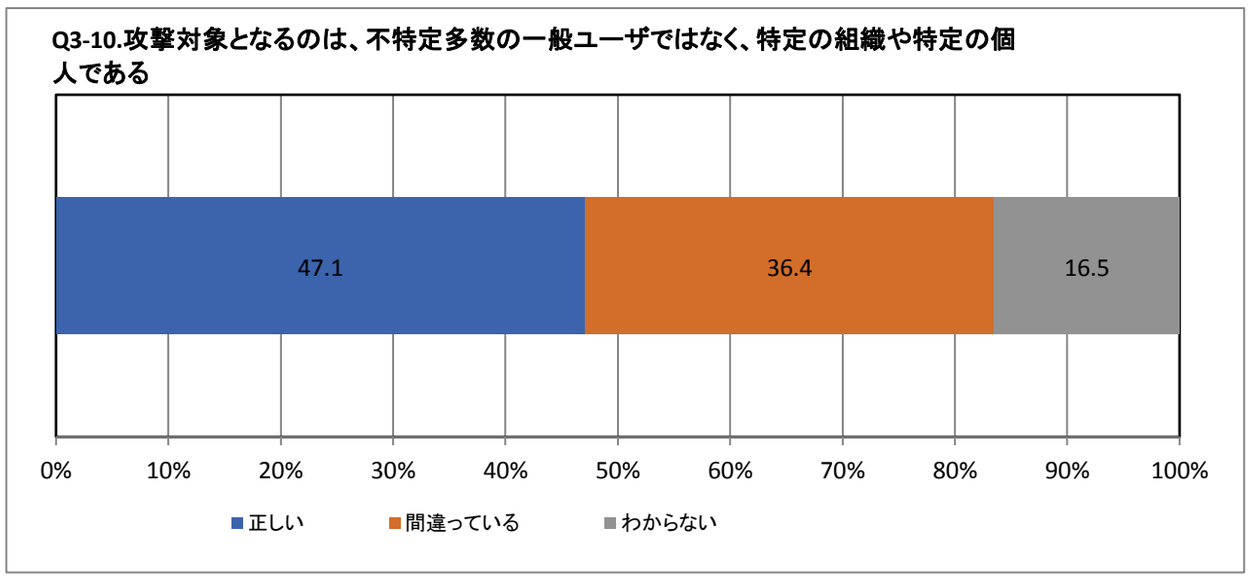
Q3-8：脆弱性 脆弱性(ぜいじゃくせい)があると、メールの添付ファイルを開いたり、ホームページを見ただけで、ウイルスに感染する可能性がある	度数	%
正しい	1977	79.6
間違っている	148	6.0
わからない	358	14.4
集計母数	2483	100.0



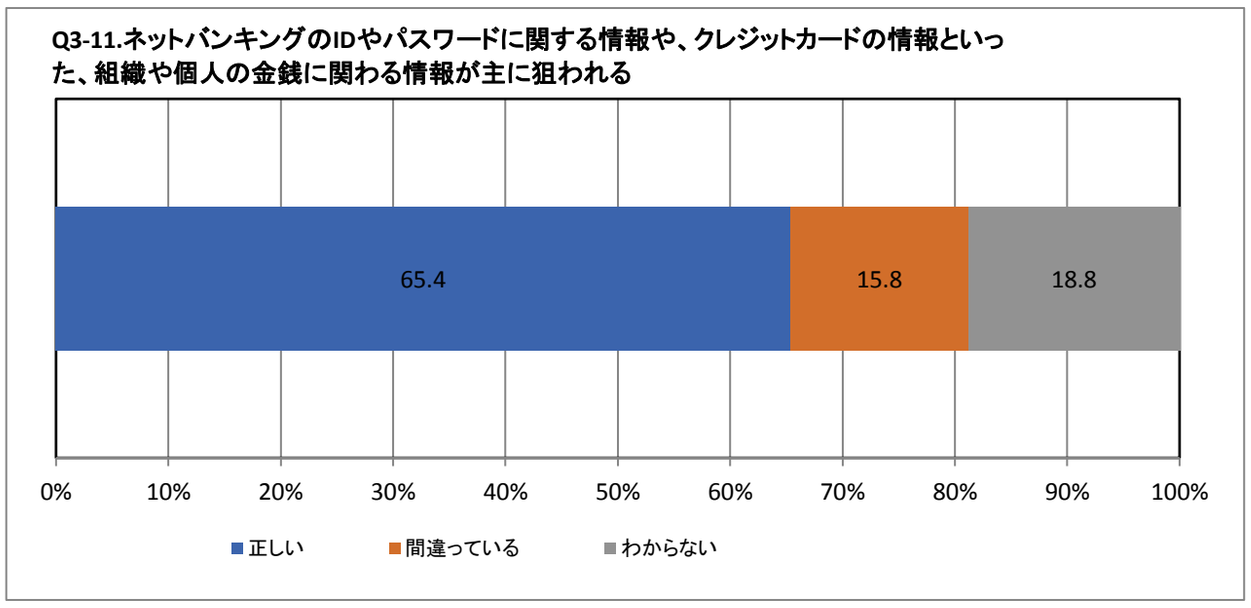
Q3-9：脆弱性 Windows Updateなどを利用して常にパソコンを最新の状態にすることで、脆弱性を解消できる	度数	%
正しい	1656	66.7
間違っている	357	14.4
わからない	470	18.9
集計母数	2483	100.0



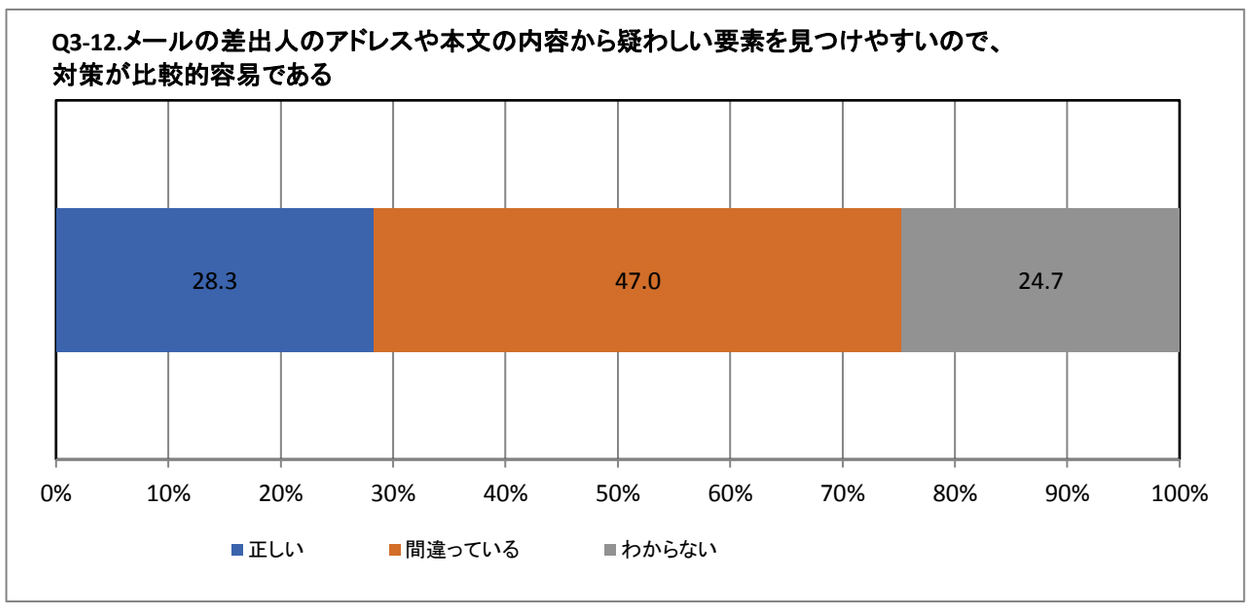
Q3-10：標的型攻撃 攻撃対象となるのは、不特定多数の一般ユーザではなく、特定の組織や特定の個人である	度数	%
正しい	631	47.1
間違っている	488	36.4
わからない	221	16.5
集計母数	1340	100.0



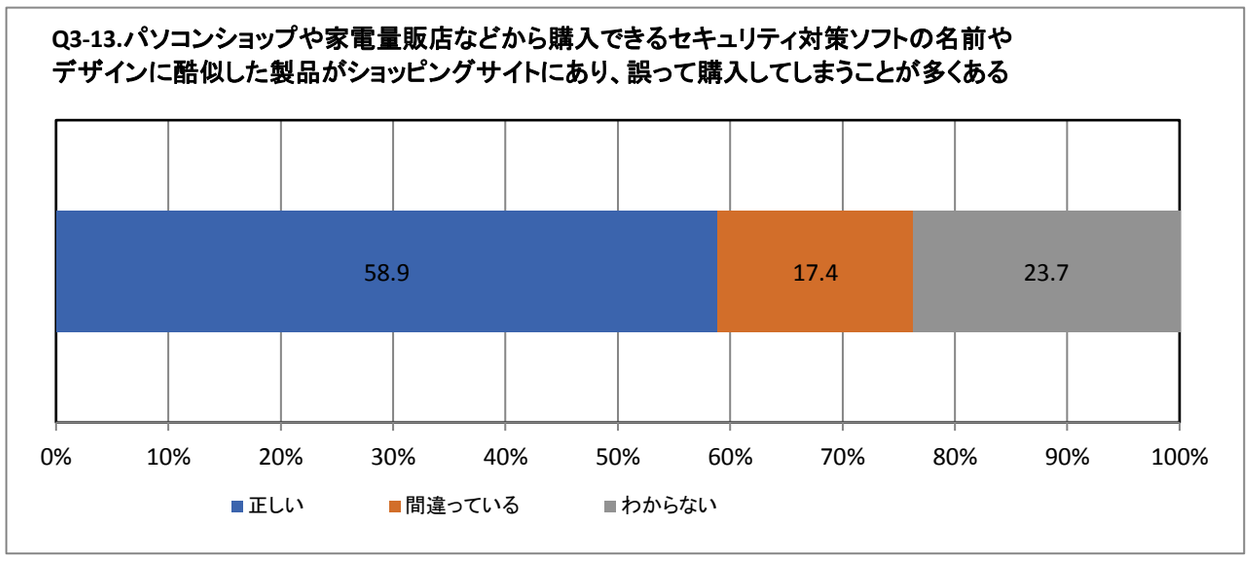
Q3-11：標的型攻撃 ネットバンキングのIDやパスワードに関する情報や、クレジットカードの情報といった、組織や個人の金銭に関わる情報が主に狙われる	度数	%
正しい	876	65.4
間違っている	212	15.8
わからない	252	18.8
集計母数	1340	100.0



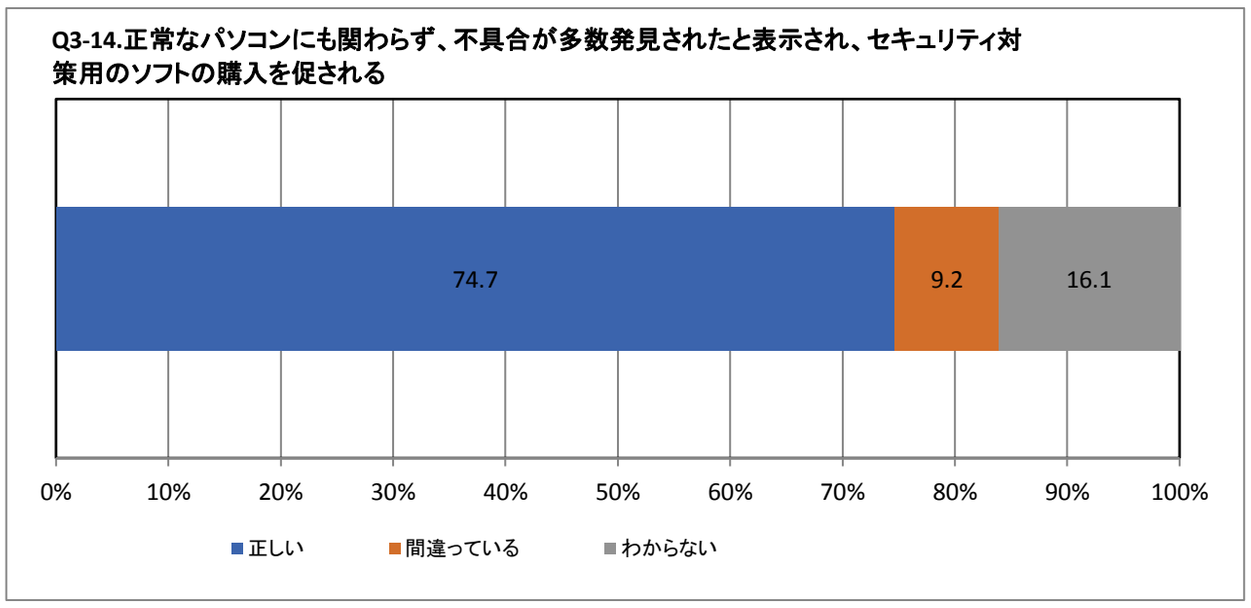
Q3-12：標的型攻撃 メールの差出人のアドレスや本文の内容から疑わしい要素を見つけやすいので、対策が比較的容易である	度数	%
正しい	379	28.3
間違っている	630	47.0
わからない	331	24.7
集計母数	1340	100.0



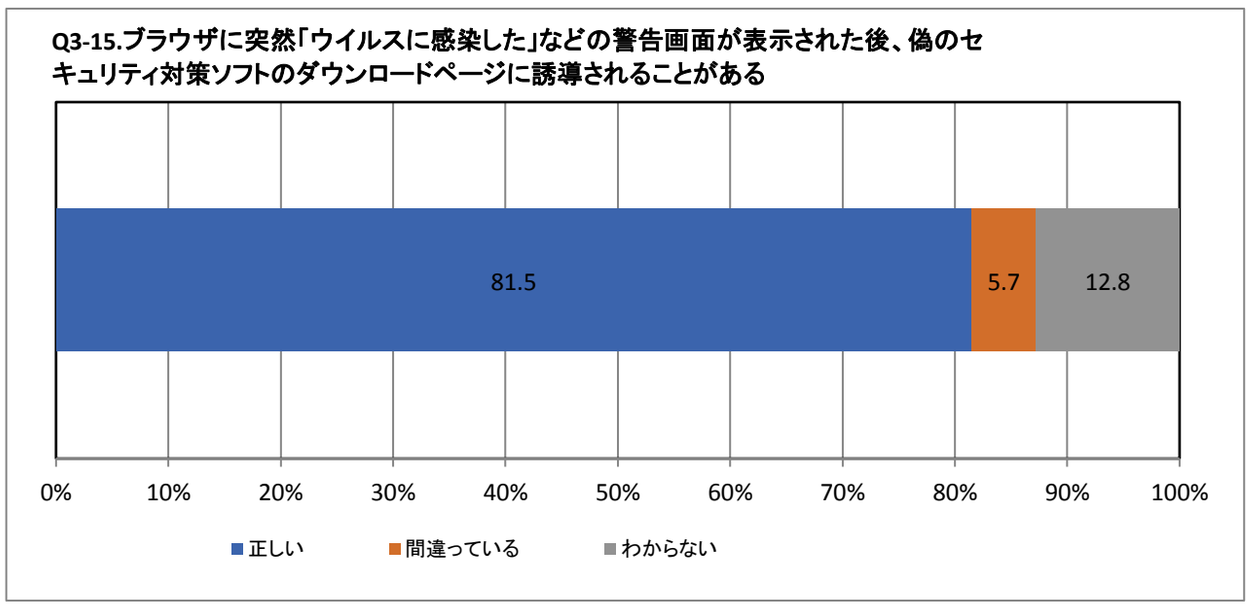
Q3-13：偽セキュリティソフト パソコンショップや家電量販店などから購入できるセキュリティ対策ソフトの名前やデザインに酷似した製品がショッピングサイトにあり、誤って購入してしまうことが多くある	度数	%
正しい	874	58.9
間違っている	258	17.4
わからない	352	23.7
集計母数	1484	100.0



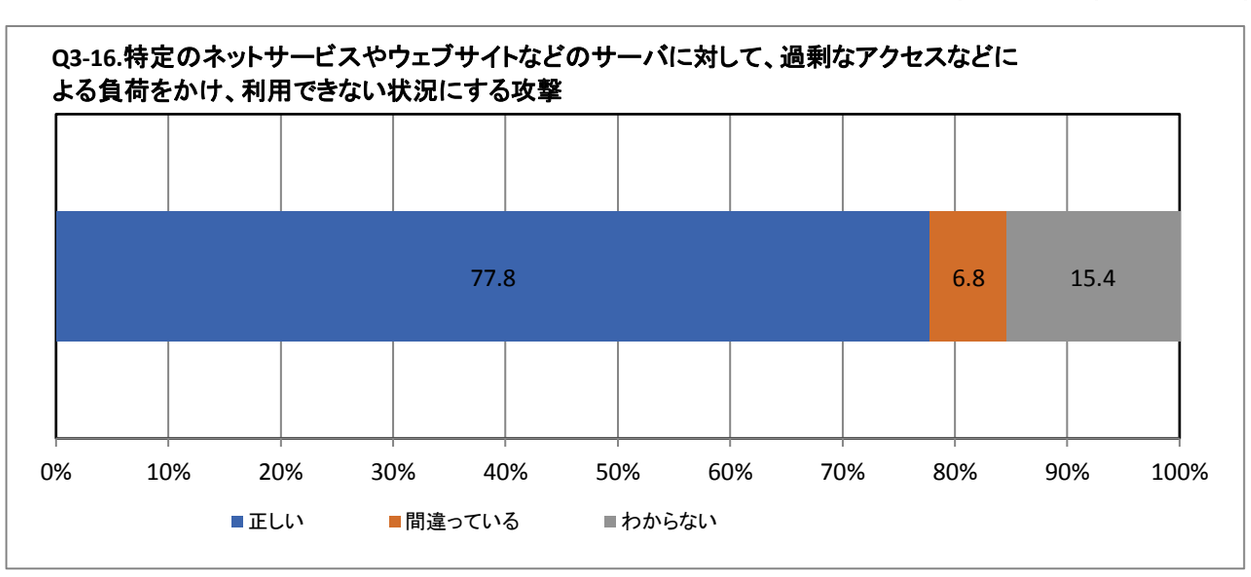
Q3-14：偽セキュリティソフト 正常なパソコンにも関わらず、不具合が多数発見されたと表示され、セキュリティ対策用のソフトの購入を促される	度数	%
正しい	1108	74.7
間違っている	137	9.2
わからない	239	16.1
集計母数	1484	100.0



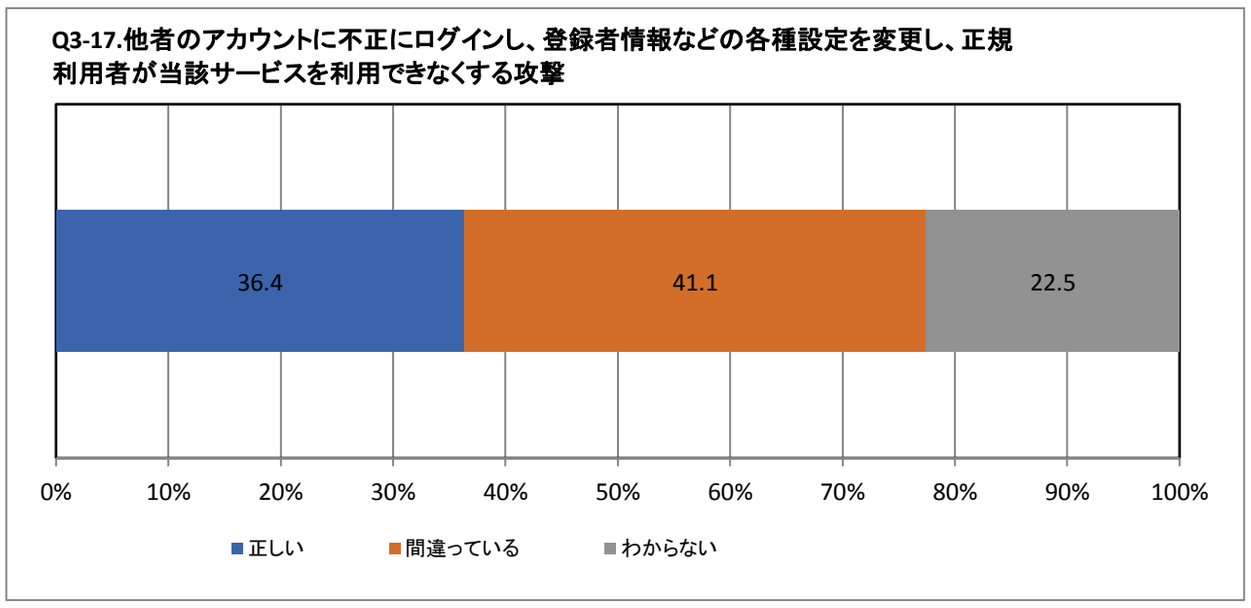
Q3-15：偽セキュリティソフト ブラウザに突然「ウイルスに感染した」などの警告画面が表示された後、偽のセキュリティ対策ソフトのダウンロードページに誘導されることがある	度数	%
正しい	1209	81.5
間違っている	85	5.7
わからない	190	12.8
集計母数	1484	100.0



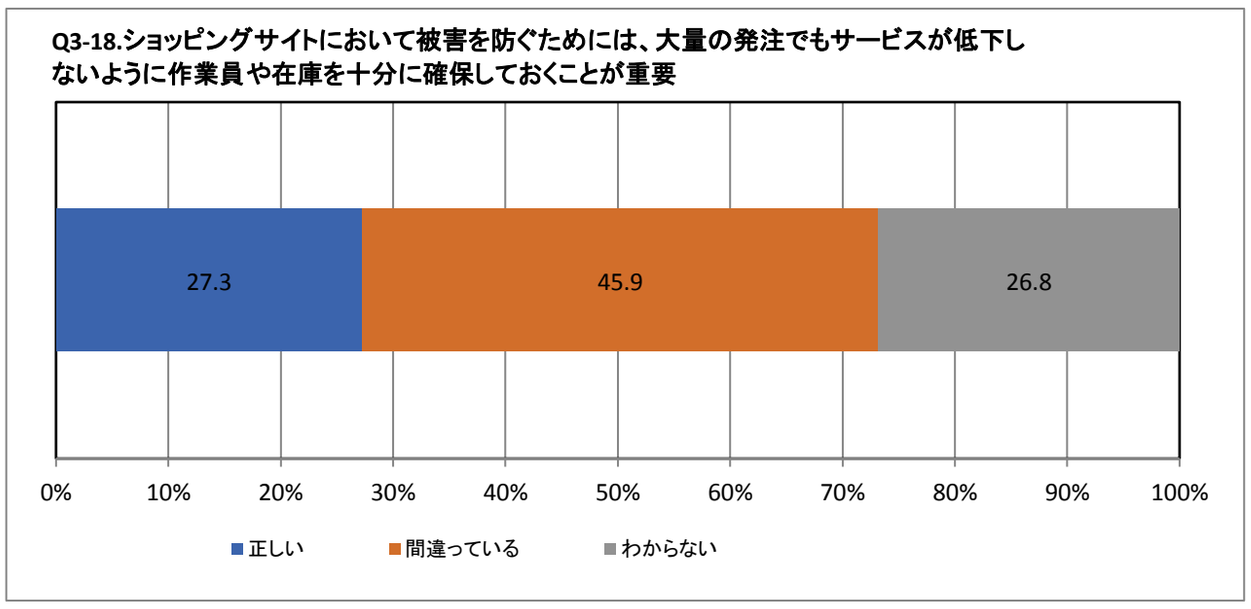
Q3-16：Dos攻撃 特定のネットサービスやウェブサイトなどのサーバに対して、過剰なアクセスなどによる負荷をかけ、利用できない状況にする攻撃	度数	%
正しい	873	77.8
間違っている	76	6.8
わからない	173	15.4
集計母数	1122	100.0



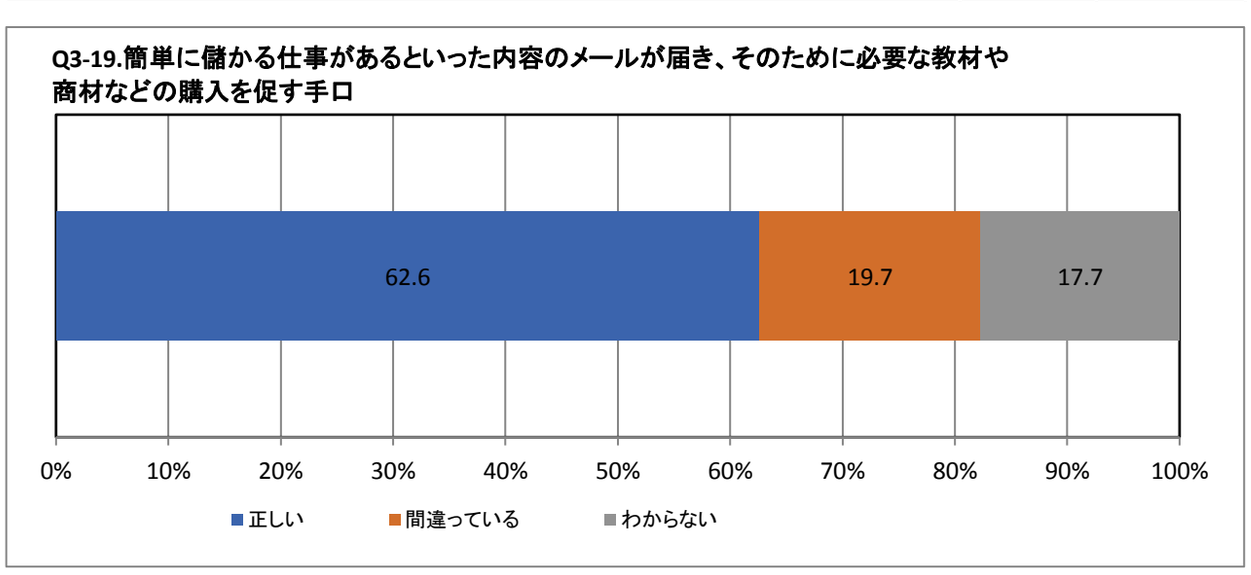
Q3-17：Dos攻撃 他者のアカウントに不正にログインし、登録者情報などの各種設定を変更し、正規利用者が当該サービスを利用できなくする攻撃	度数	%
正しい	408	36.4
間違っている	461	41.1
わからない	253	22.5
集計母数	1122	100.0



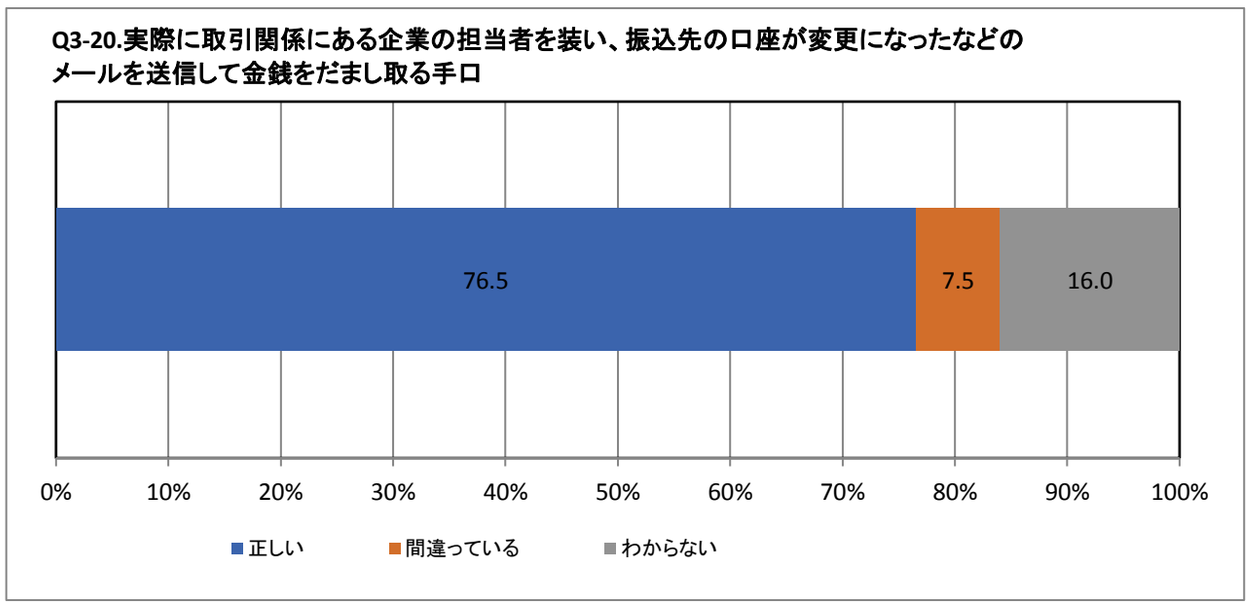
Q3-18：Dos攻撃 ショッピングサイトにおいて被害を防ぐためには、大量の発注でもサービスが低下しないように作業員や在庫を十分に確保しておくことが重要	度数	%
正しい	306	27.3
間違っている	515	45.9
わからない	301	26.8
集計母数	1122	100.0



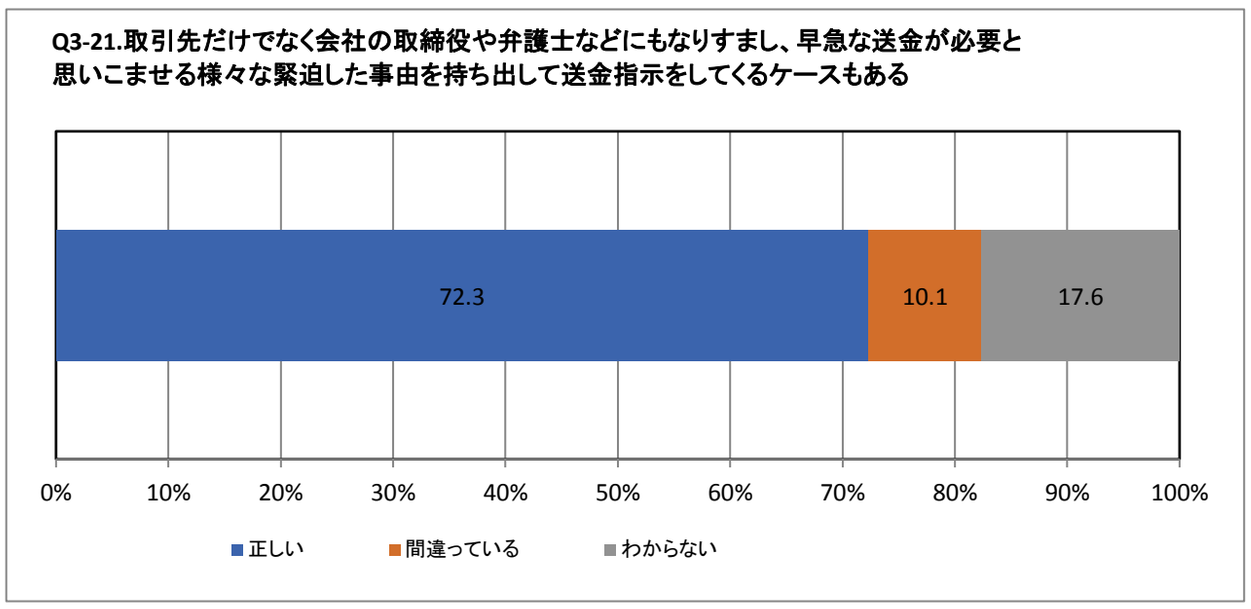
Q3-19：ビジネスメール詐欺 簡単に儲かる仕事があるといった内容のメールが届き、そのために必要な教材や商材などの購入を促す手口	度数	%
正しい	839	62.6
間違っている	264	19.7
わからない	237	17.7
集計母数	1340	100.0



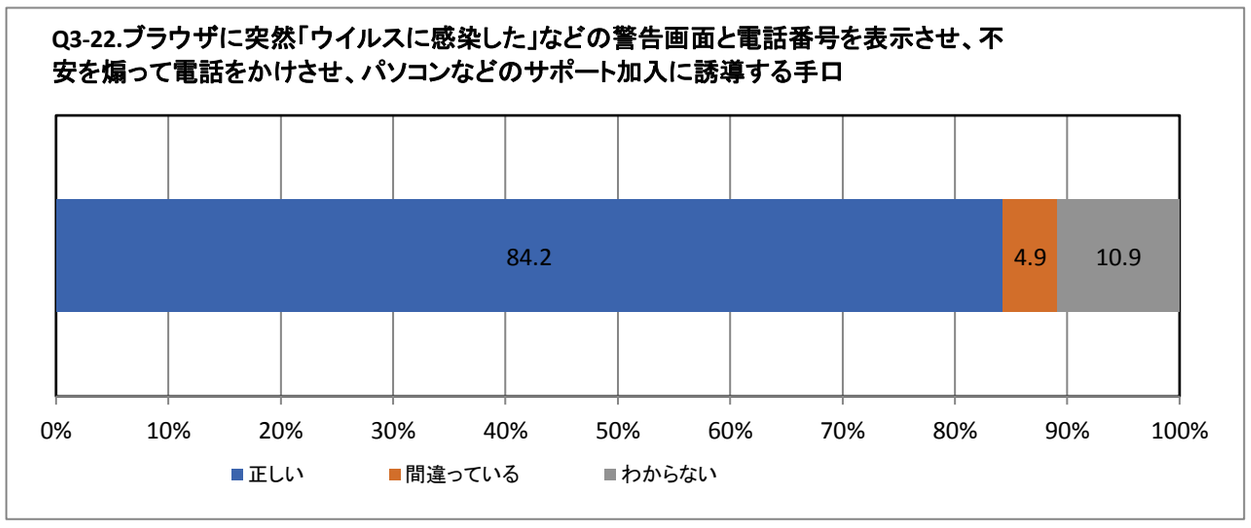
Q3-20:ビジネスメール詐欺 実際に取引関係にある企業の担当者を装い、振込先の口座が変更になったなどのメールを送信して金銭をだまし取る手口	度数	%
正しい	1025	76.5
間違っている	101	7.5
わからない	214	16.0
集計母数	1340	100.0



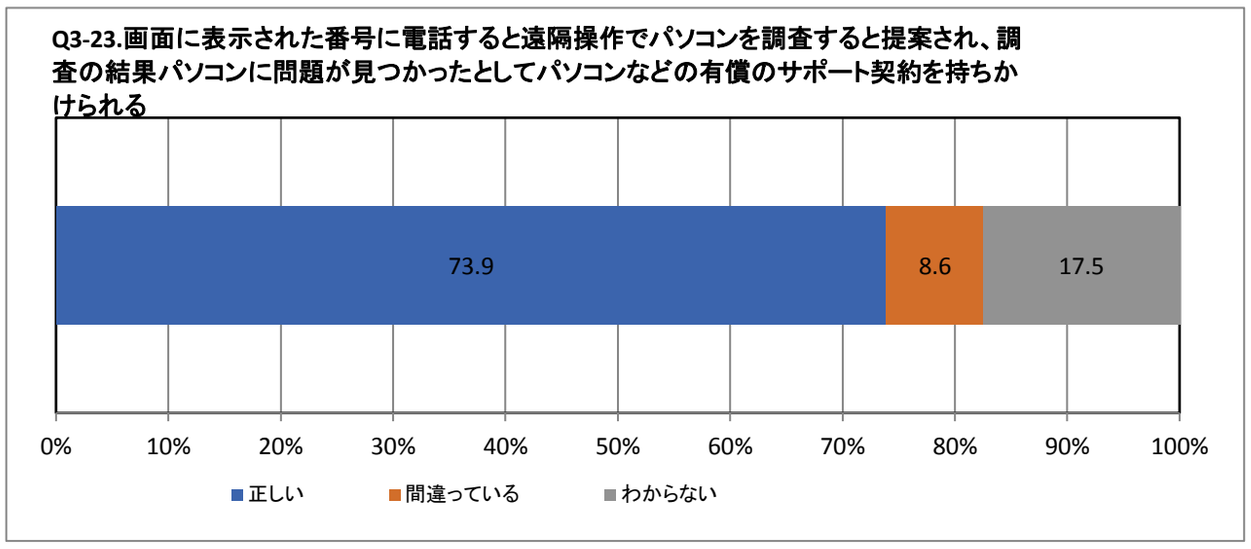
Q3-21:ビジネスメール詐欺 取引先だけでなく会社の取締役や弁護士などにもなりすまし、早急な送金が必要と思いこませる様々な緊迫した事由を持ち出して送金指示をしてくるケースもある	度数	%
正しい	969	72.3
間違っている	135	10.1
わからない	236	17.6
集計母数	1340	100.0



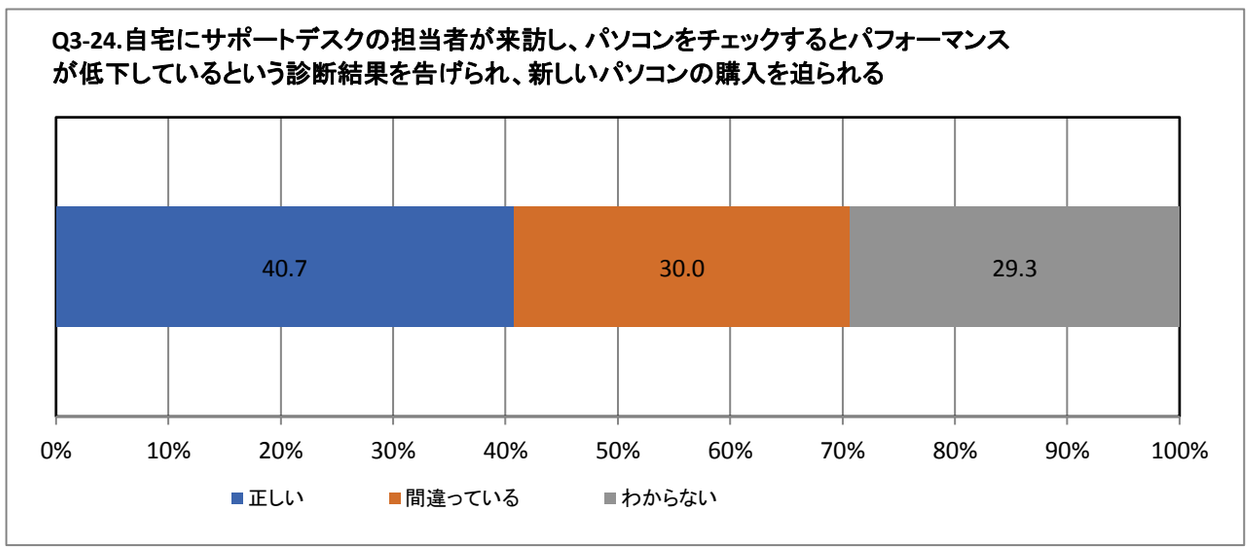
Q3-22:偽渓谷(サポート詐欺) ブラウザに突然「ウイルスに感染した」などの警告画面と電話番号を表示させ、不安を煽って電話をかけさせ、パソコンなどのサポート加入に誘導する手口	度数	%
正しい	1417	84.2
間違っている	82	4.9
わからない	183	10.9
集計母数	1682	100.0



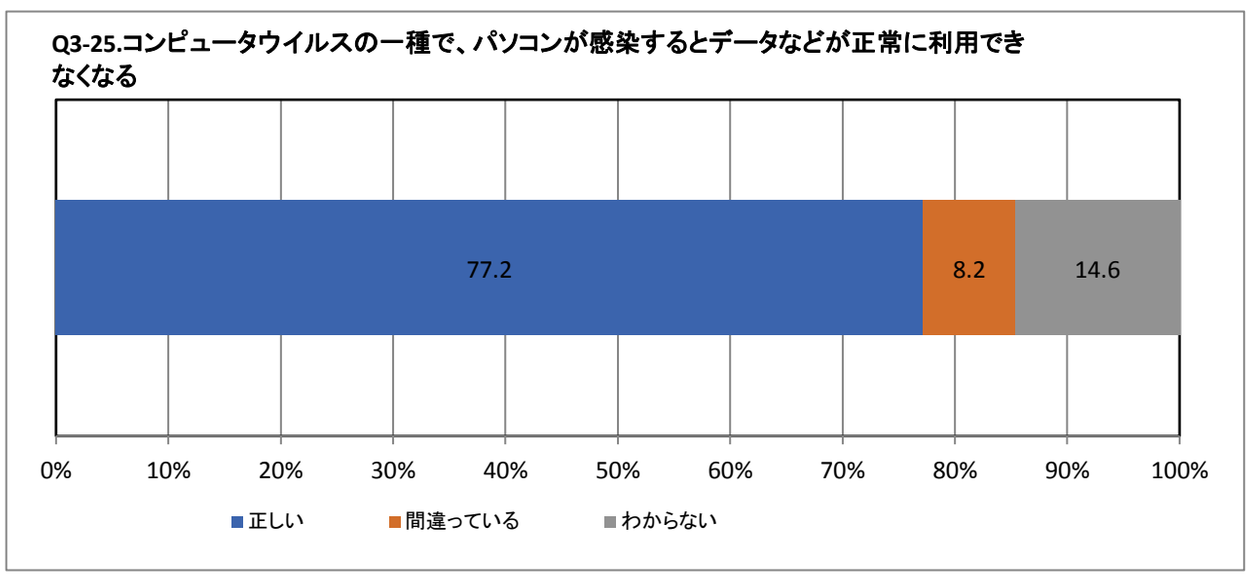
Q3-23：偽警告(サポート詐欺) 画面に表示された番号に電話すると遠隔操作でパソコンを調査すると提案され、調査の結果パソコンに問題が見つかったとしてパソコンなどの有償のサポート契約を持ちかけられる	度数	%
正しい	1243	73.9
間違っている	145	8.6
わからない	294	17.5
集計母数	1682	100.0



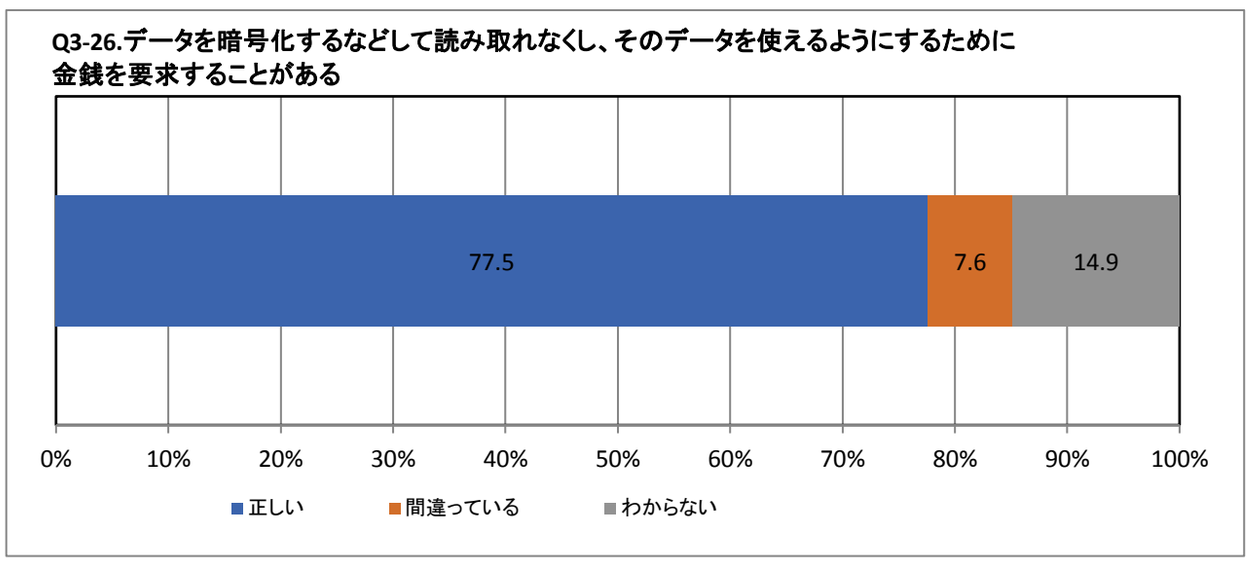
Q3-24：偽警告（サポート詐欺） 自宅にサポートデスクの担当者が来訪し、パソコンをチェックするとパフォーマンスが低下しているという診断結果を告げられ、新しいパソコンの購入を迫られる	度数	%
正しい	685	40.7
間違っている	504	30.0
わからない	493	29.3
集計母数	1682	100.0



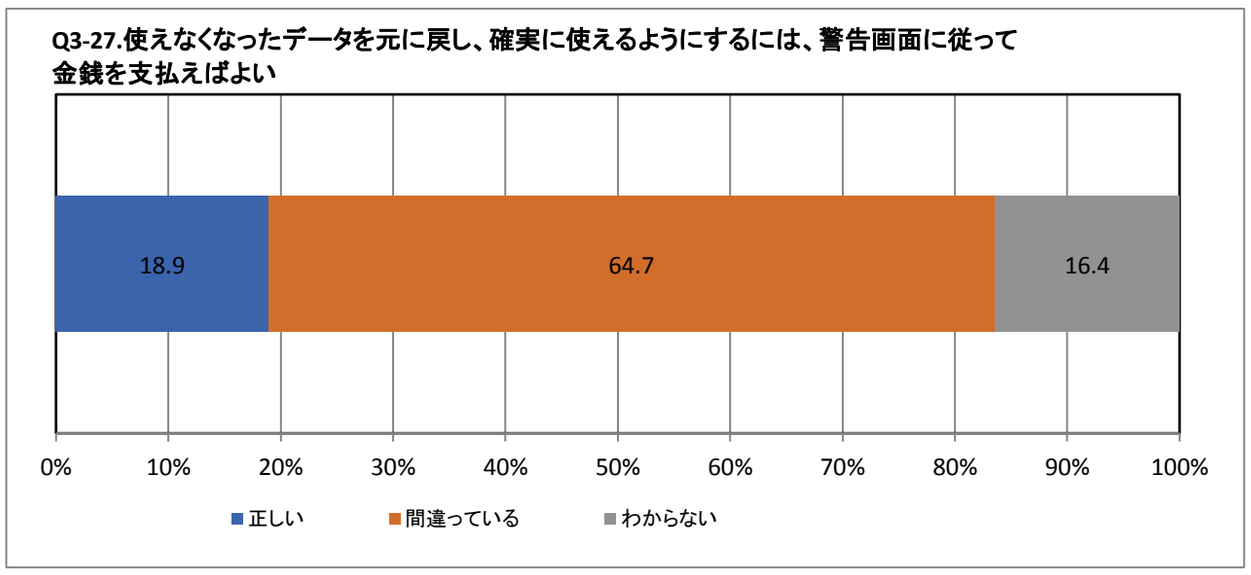
Q3-25：ランサムウェア コンピュータウイルスの一種で、パソコンが感染するとデータなどが正常に利用できなくなる	度数	%
正しい	1192	77.2
間違っている	127	8.2
わからない	226	14.6
集計母数	1545	100.0



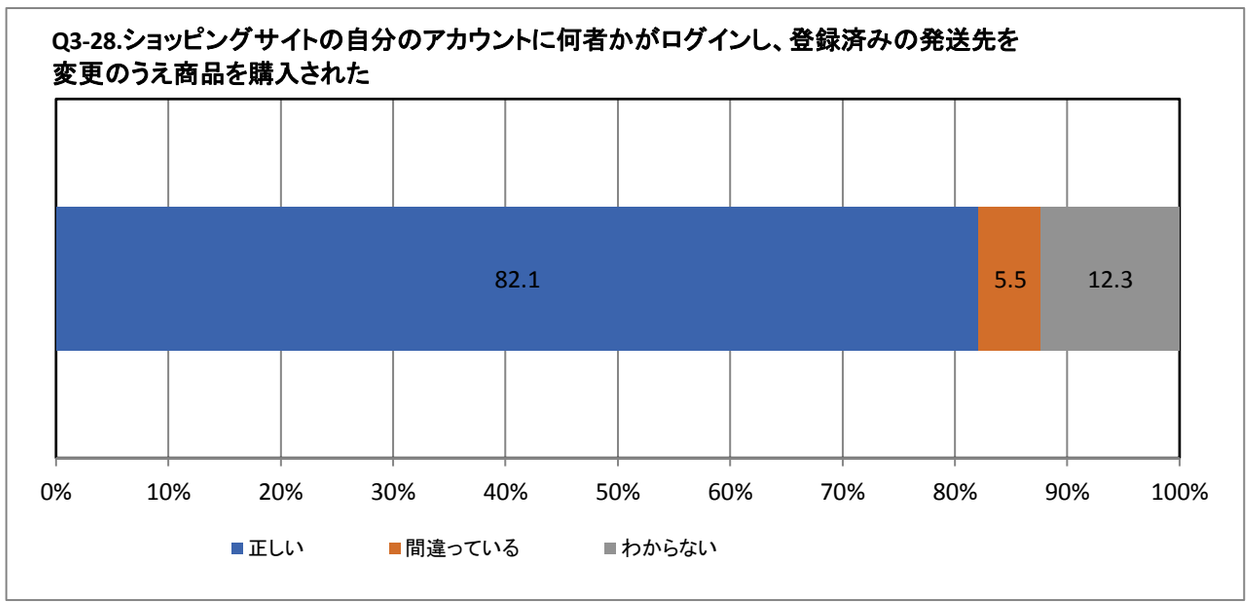
Q3-26：ランサムウェア データを暗号化するなどして読み取れなくし、そのデータを使えるようにするために金銭を要求することがある	度数	%
正しい	1198	77.5
間違っている	117	7.6
わからない	230	14.9
集計母数	1545	100.0



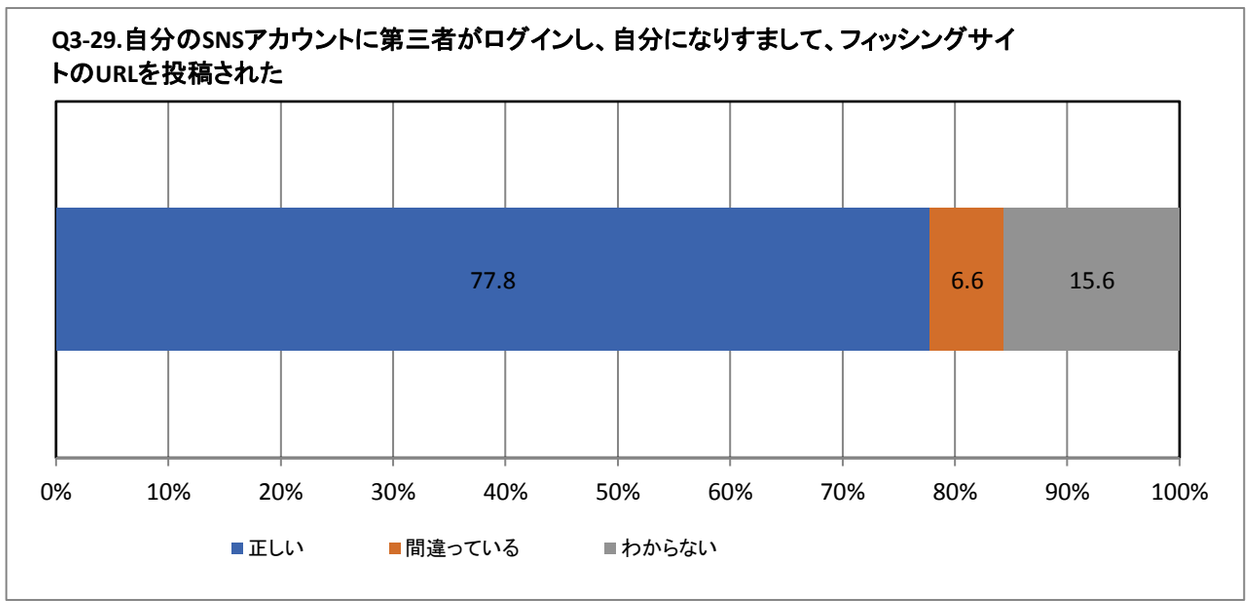
Q3-27：ランサムウェア 使えなくなったデータを元に戻し、確実に使えるようにするには、警告画面に従って金銭を支払えばよい	度数	%
正しい	292	18.9
間違っている	999	64.7
わからない	254	16.4
集計母数	1545	100.0



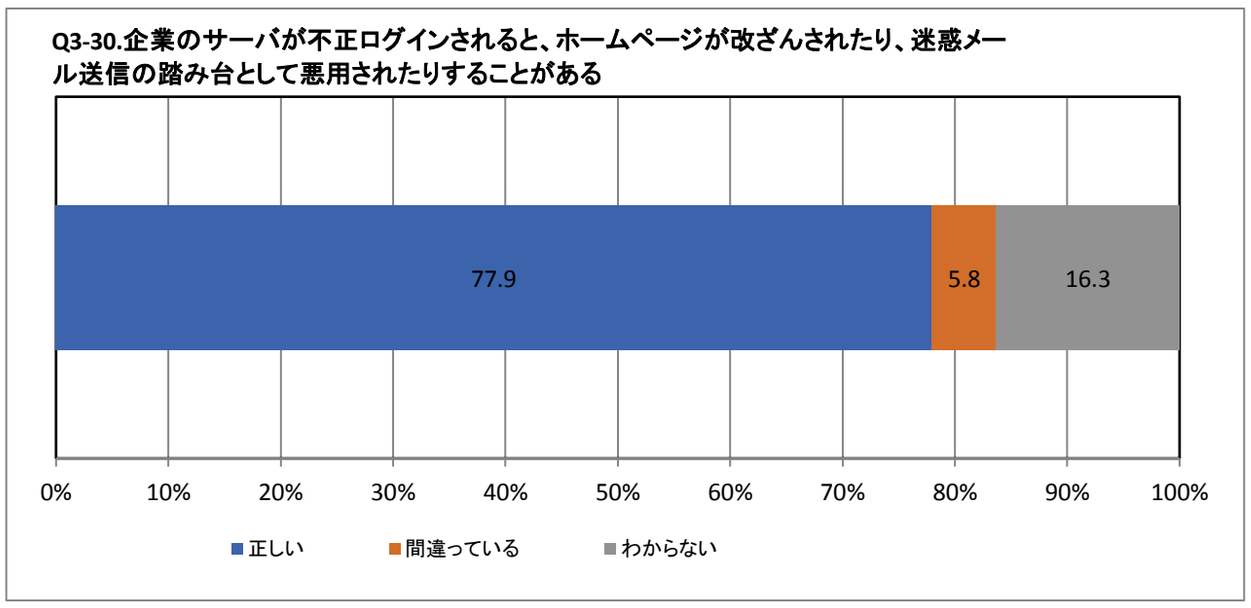
Q3-28：不正ログイン ショッピングサイトの自分のアカウントに何者かがログインし、登録済みの発送先を変更のうえ商品を購入された	度数	%
正しい	2250	82.1
間違っている	152	5.5
わからない	337	12.3
集計母数	2739	100.0



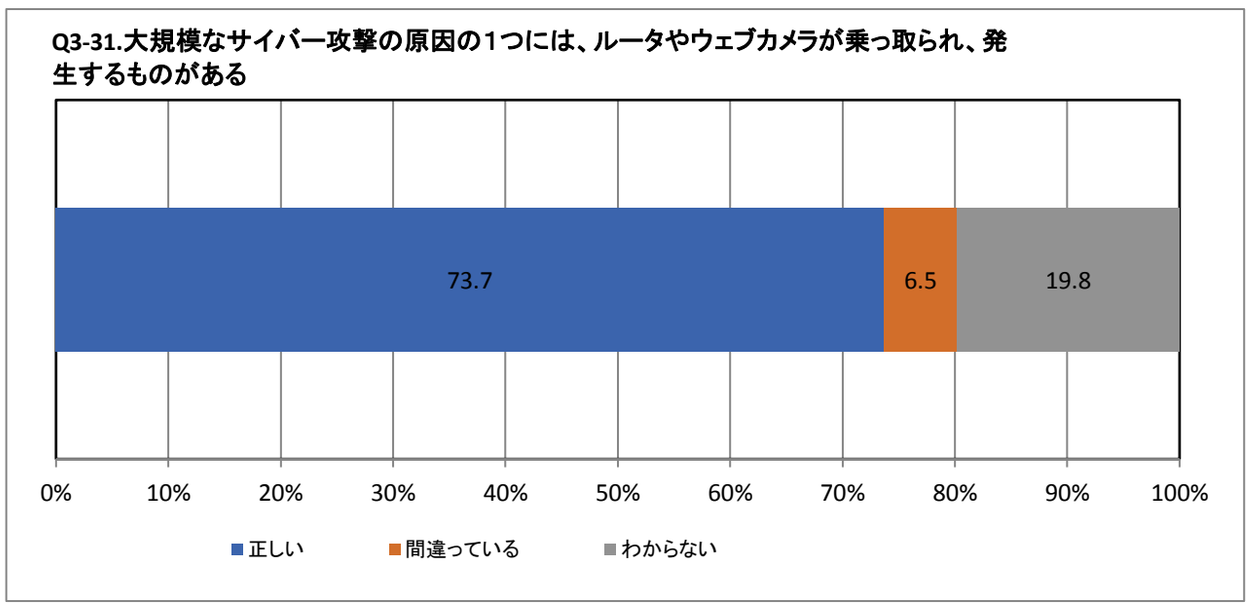
Q3-29：不正ログイン 自分のSNSアカウントに第三者がログインし、自分になりすまして、フィッシングサイトのURLを投稿された	度数	%
正しい	2131	77.8
間違っている	180	6.6
わからない	428	15.6
集計母数	2739	100.0



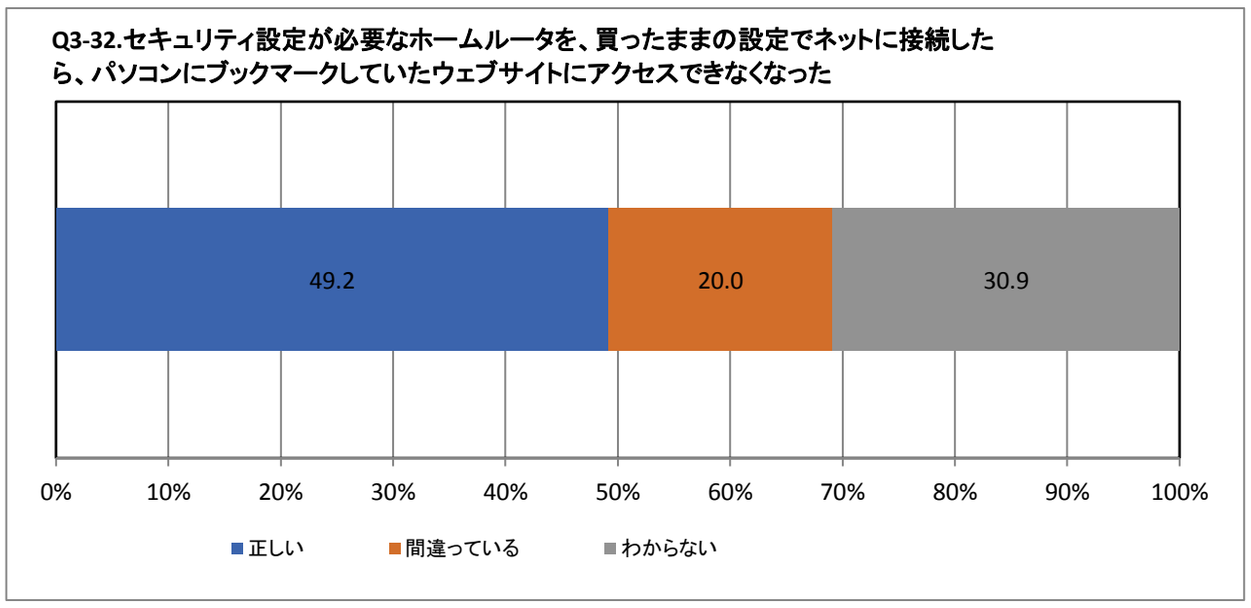
Q3-30：不正ログイン 企業のサーバが不正ログインされると、ホームページが改ざんされたり、迷惑メール送信の踏み台として悪用されたりすることがある	度数	%
正しい	2134	77.9
間違っている	159	5.8
わからない	446	16.3
集計母数	2739	100.0



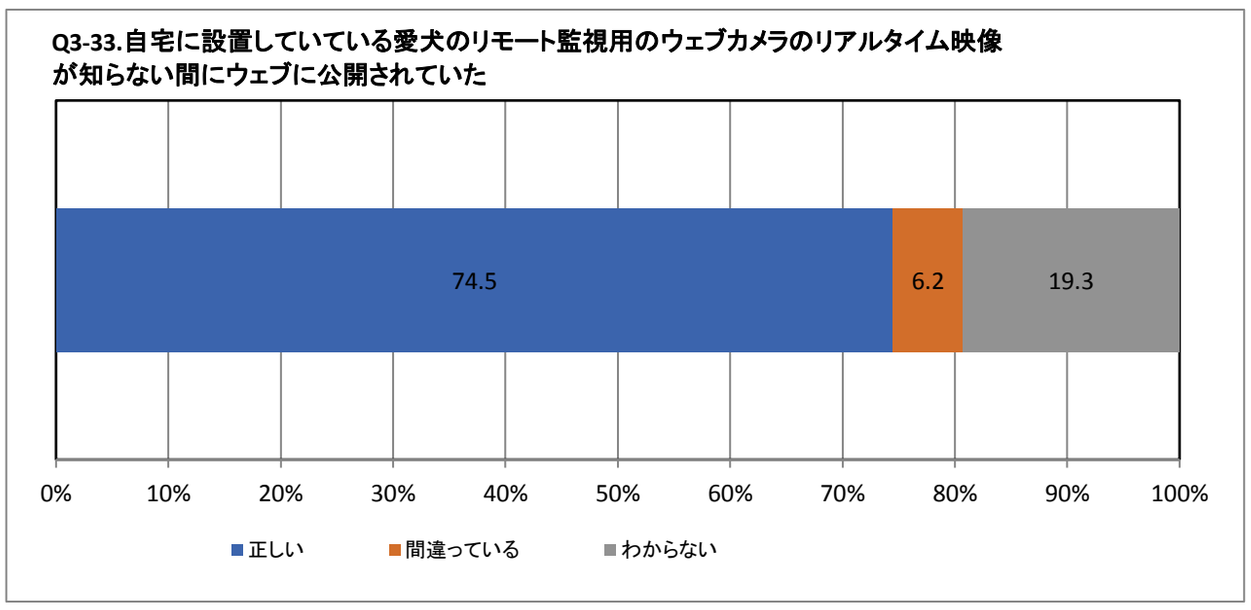
Q3-31：IoT機器への侵入、乗っ取り 大規模なサイバー攻撃の原因の1つには、ルータやウェブカメラが乗っ取られ、発生するものがある	度数	%
正しい	1148	73.7
間違っている	101	6.5
わからない	309	19.8
集計母数	1558	100.0



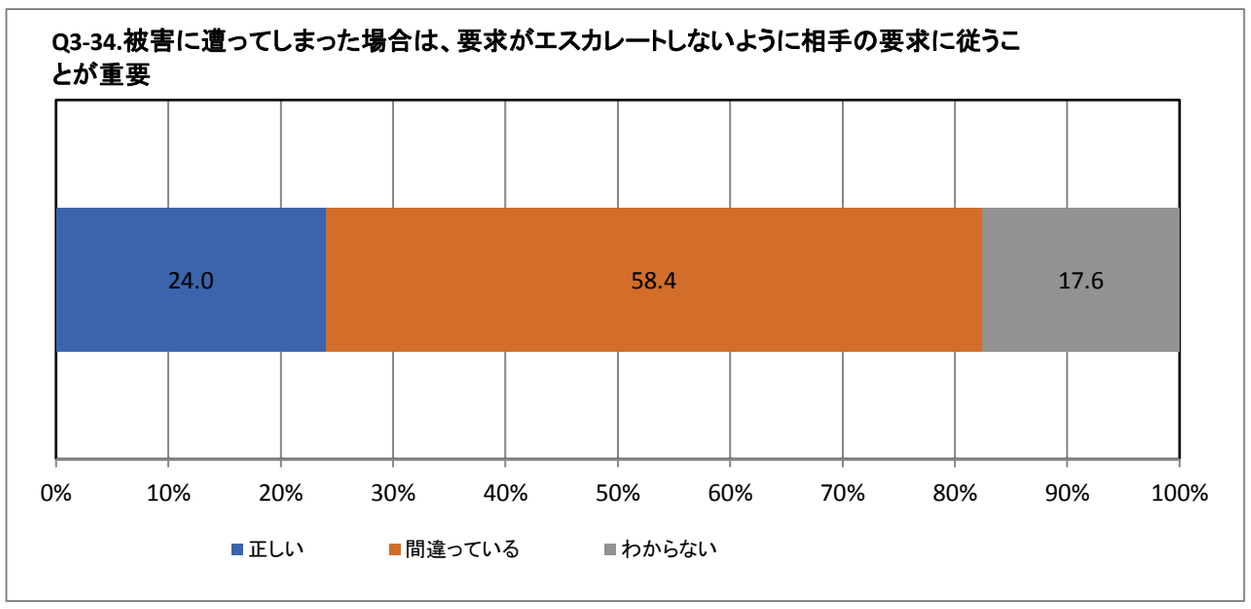
Q3-32：IoT機器への侵入、乗っ取り セキュリティ設定が必要なホームルータを、買ったままの設定でネットに接続したら、パソコンにブックマークしていたウェブサイトにアクセスできなくなった	度数	%
正しい	766	49.2
間違っている	311	20.0
わからない	481	30.9
集計母数	1558	100.0



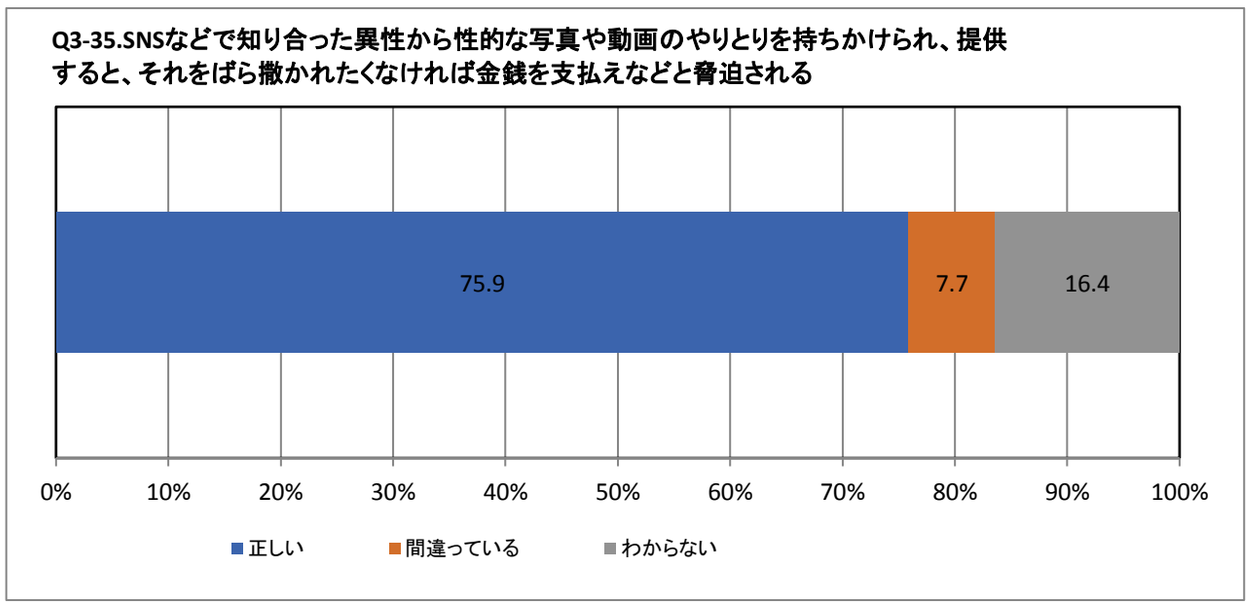
Q3-33：IoT機器への侵入、乗っ取り 自宅に設置していている愛犬のリモート監視用のウェブカメラのリアルタイム映像が知らない間にウェブに公開されていた	度数	%
正しい	1161	74.5
間違っている	96	6.2
わからない	301	19.3
集計母数	1558	100.0



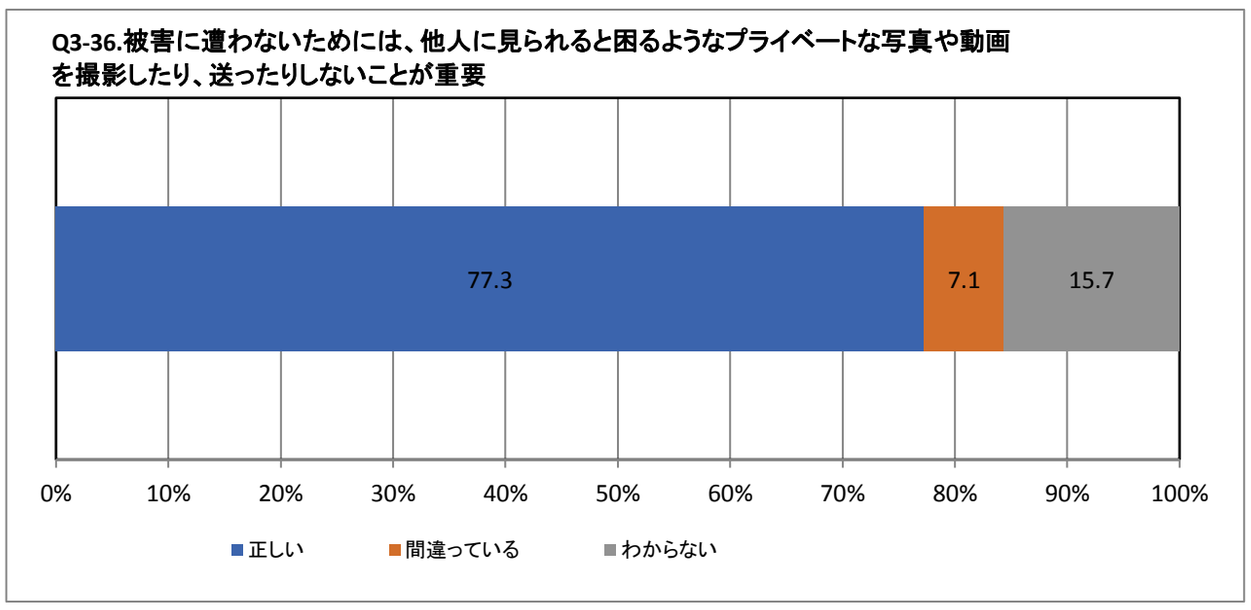
Q3-34：セクストーション(性的脅迫) 被害に遭ってしまった場合は、要求がエスカレートしないように相手の要求に従うことが重要	度数	%
正しい	213	24.0
間違っている	519	58.4
わからない	156	17.6
集計母数	888	100.0



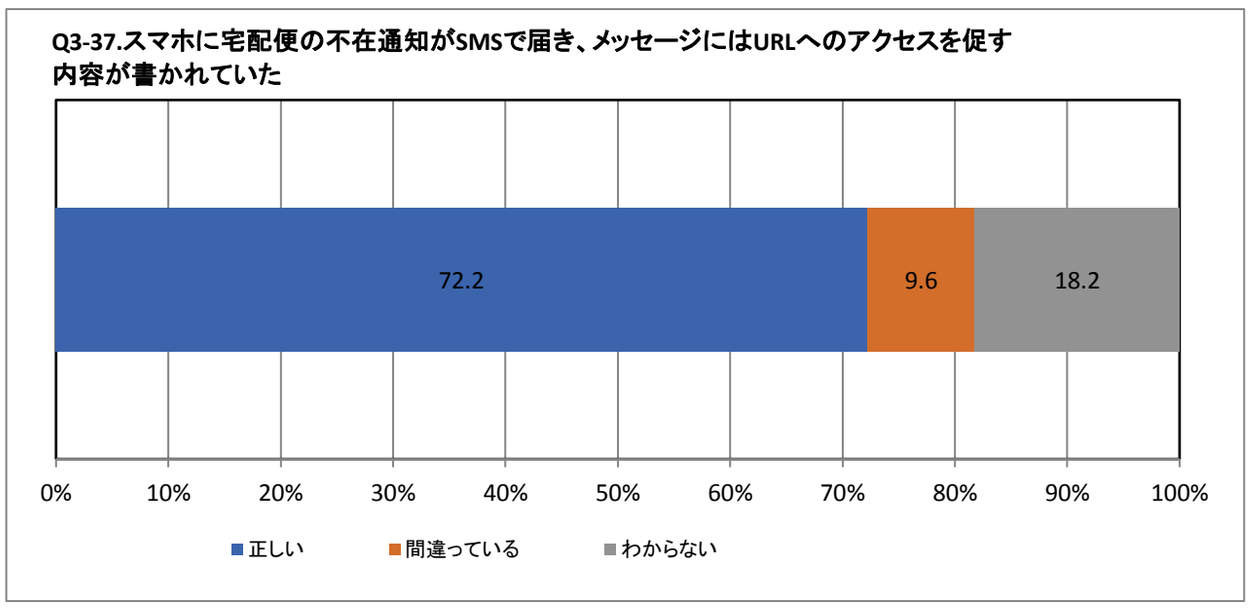
Q3-35：セクストーション(性的脅迫) SNSなどで知り合った異性から性的な写真や動画のやりとりを持ちかけられ、提供すると、それをばら撒かれたくなければ金銭を支払えなどと脅迫される	度数	%
正しい	674	75.9
間違っている	68	7.7
わからない	146	16.4
集計母数	888	100.0



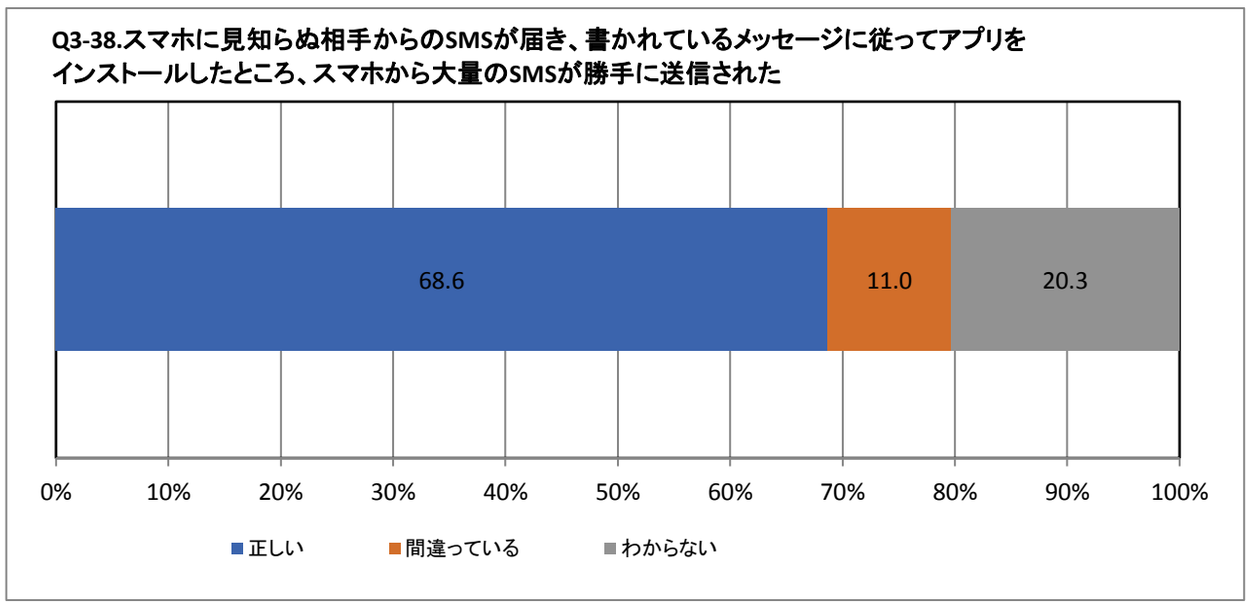
Q3-36：セクストーション（性的脅迫） 被害に遭わないためには、他人に見られると困るようなプライベートな写真や動画を撮影したり、送ったりしないことが重要	度数	%
正しい	686	77.3
間違っている	63	7.1
わからない	139	15.7
集計母数	888	100.0



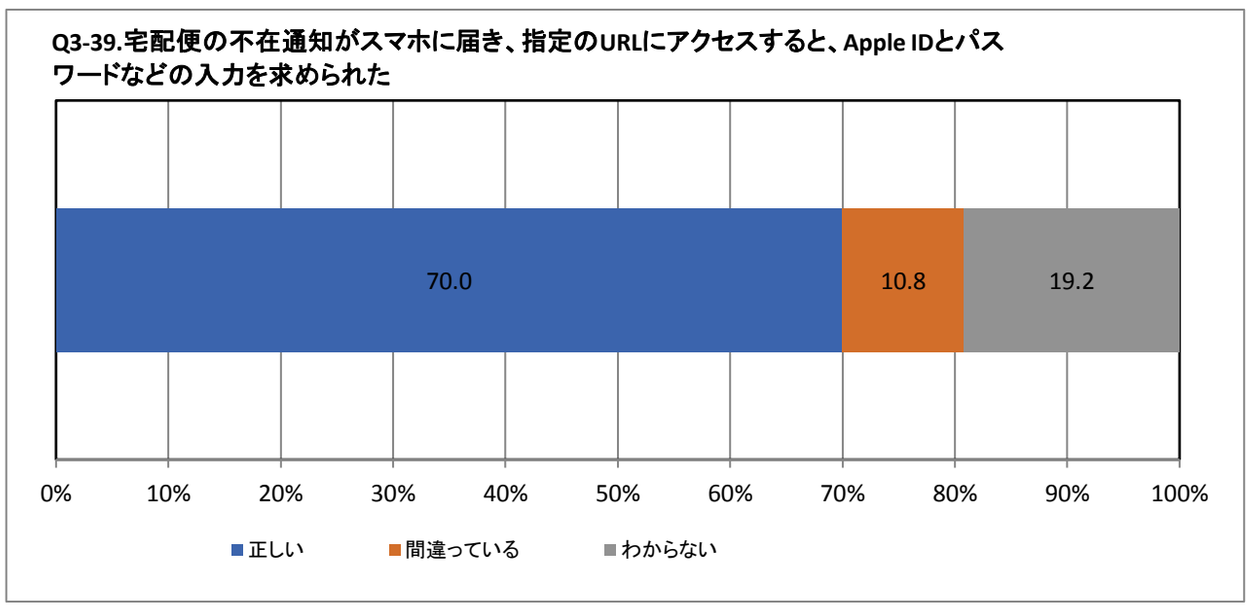
Q3-37：スミッシング(SMSフィッシング) スマホに宅配便の不在通知がSMSで届き、メッセージにはURLへのアクセスを促す内容が書かれていた	度数	%
正しい	753	72.2
間違っている	100	9.6
わからない	190	18.2
集計母数	1043	100.0



Q3-38：スミッシング（SMSフィッシング） スマホに見知らぬ相手からのSMSが届き、書かれているメッセージに従ってアプリをインストールしたところ、スマホから大量のSMSが勝手に送信された	度数	%
正しい	716	68.6
間違っている	115	11.0
わからない	212	20.3
集計母数	1043	100.0

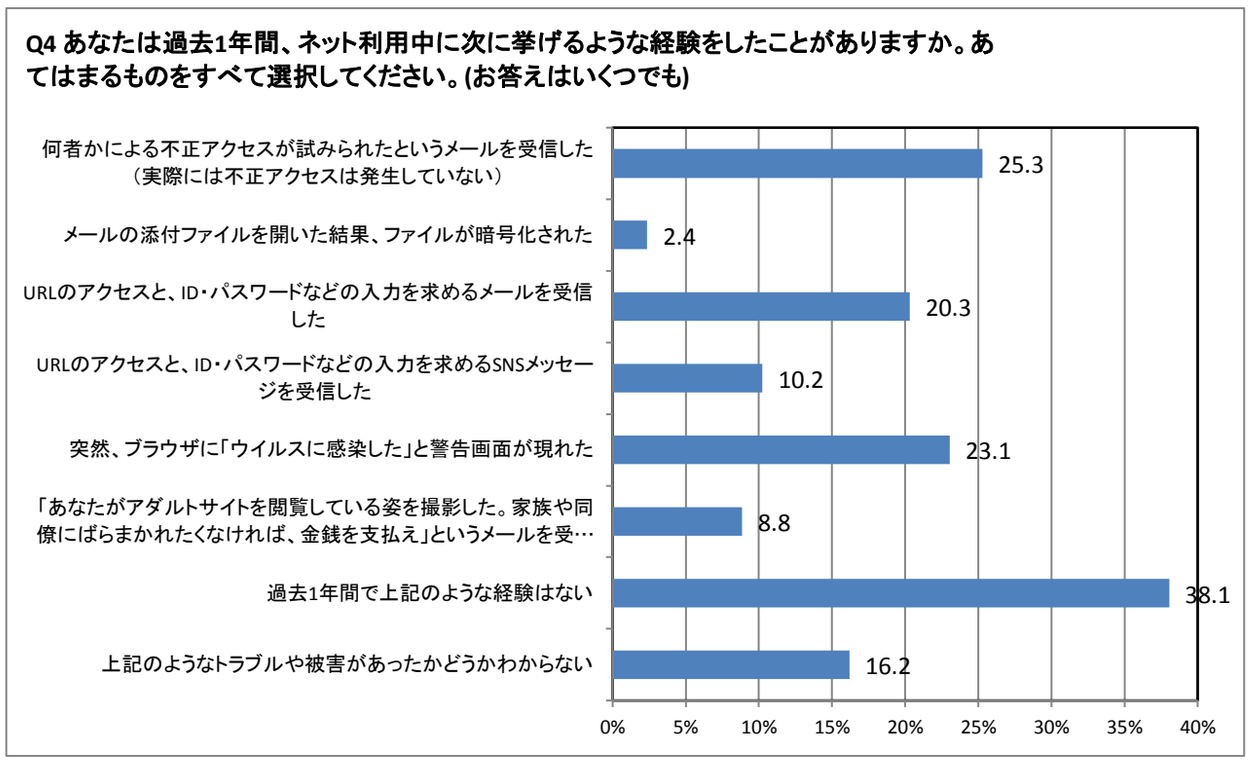


Q3-39：スミッシング（SMSフィッシング） 宅配便の不在通知がスマホに届き、指定のURLにアクセスすると、Apple IDとパスワードなどの入力を求められた	度数	%
正しい	730	70.0
間違っている	113	10.8
わからない	200	19.2
集計母数	1043	100.0



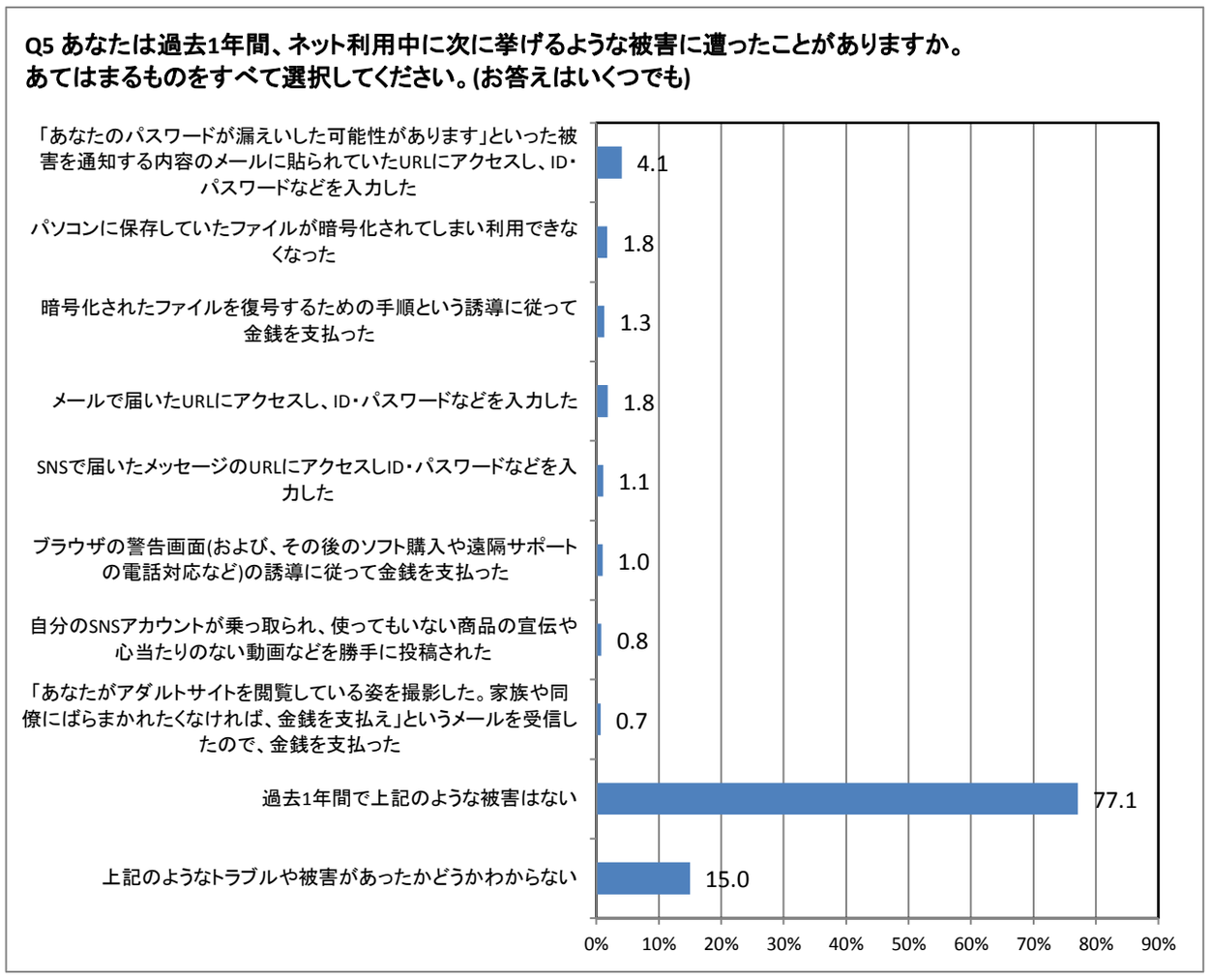
PC調査のみの設問

Q4 あなたは過去1年間、ネット利用中に次に挙げるような経験をしたことがありますか。あてはまるものをすべて選択してください。（お答えはいくつでも）	度数	%
何者かによる不正アクセスが試みられたというメールを受信した（実際には不正アクセスは発生していない）	1265	25.3
メールの添付ファイルを開いた結果、ファイルが暗号化された	118	2.4
URLのアクセスと、ID・パスワードなどの入力を求めるメールを受信した	1016	20.3
URLのアクセスと、ID・パスワードなどの入力を求めるSNSメッセージを受信した	512	10.2
突然、ブラウザに「ウイルスに感染した」と警告画面が現れた	1153	23.1
「あなたがアダルトサイトを閲覧している姿を撮影した。家族や同僚にばらまかれたくなければ、金銭を支払え」というメールを受信した	442	8.8
過去1年間で上記のような経験はない	1903	38.1
上記のようなトラブルや被害があったかどうかわからない	810	16.2
集計母数	5000	100.0

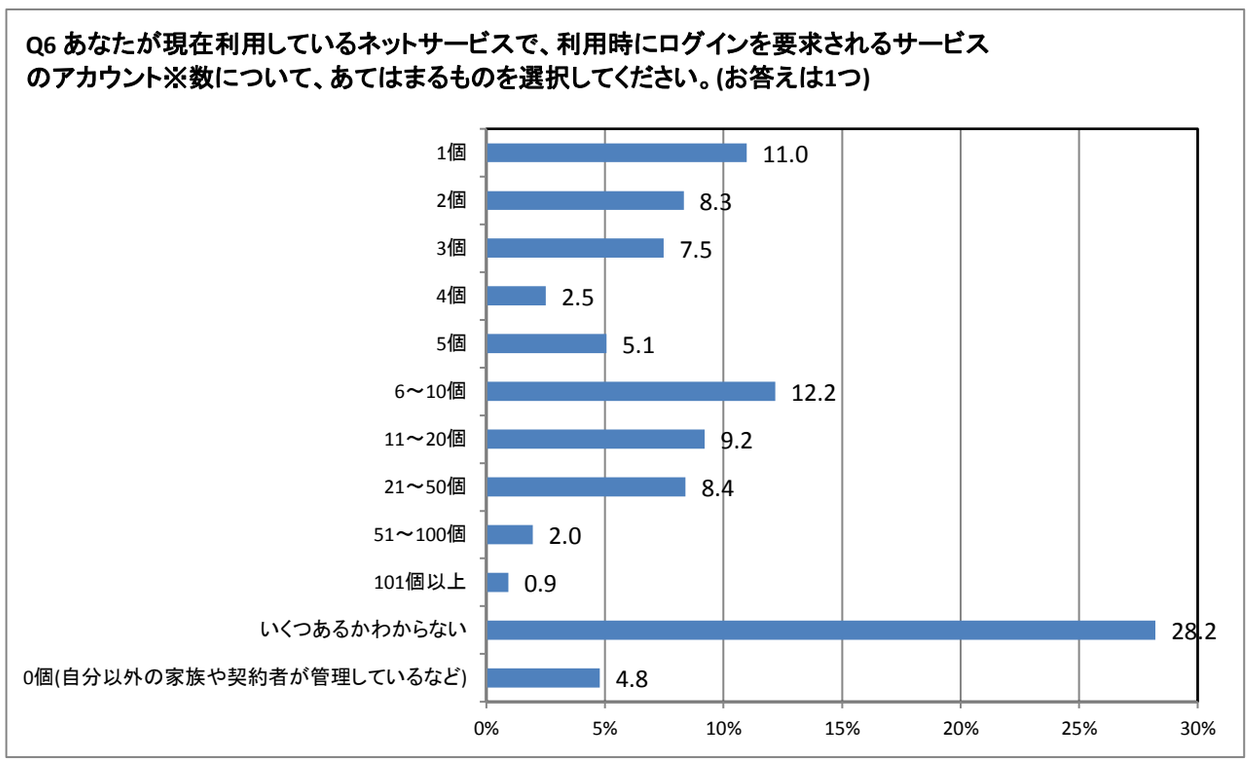


PCのみの設問

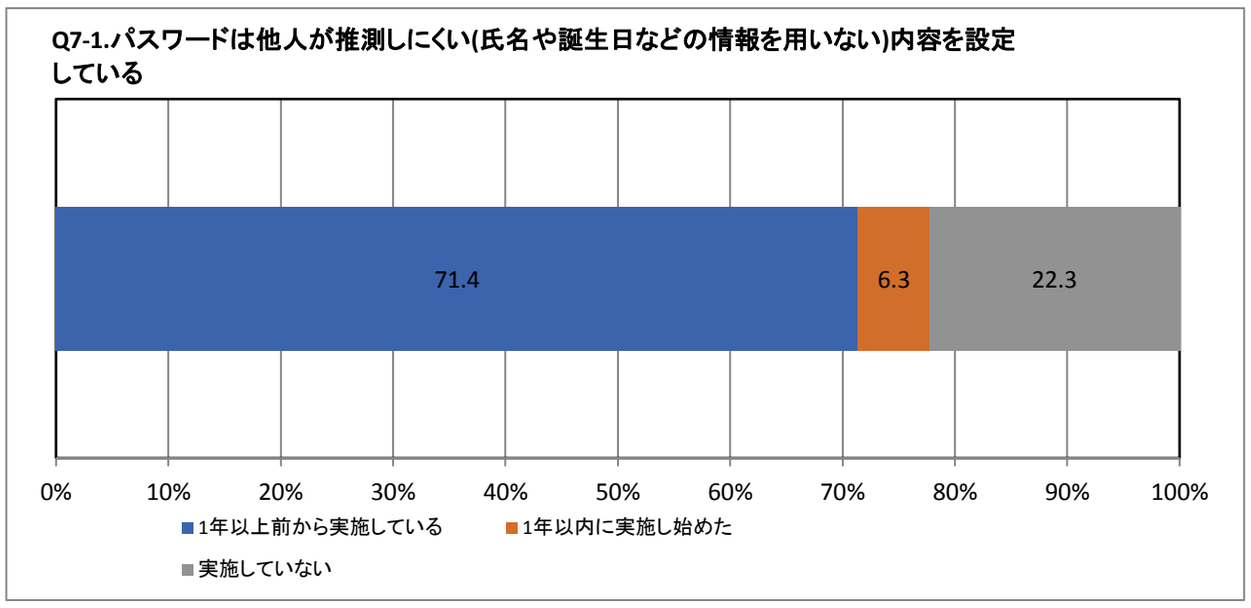
Q5 あなたは過去1年間、ネット利用中に次に挙げるような被害に遭ったことがありますか。あてはまるものをすべて選択してください。(お答えはいくつでも)	度数	%
「あなたのパスワードが漏えいした可能性があります」といった被害を通知する内容のメールに貼られていたURLにアクセスし、ID・パスワードなどを入力した	204	4.1
パソコンに保存していたファイルが暗号化されてしまい利用できなくなった	89	1.8
暗号化されたファイルを復号するための手順という誘導に従って金銭を支払った	65	1.3
メールで届いたURLにアクセスし、ID・パスワードなどを入力した	92	1.8
SNSで届いたメッセージのURLにアクセスしID・パスワードなどを入力した	54	1.1
ブラウザの警告画面(および、その後のソフト購入や遠隔サポートの電話対応など)の誘導に従って金銭を支払った	50	1.0
自分のSNSアカウントが乗っ取られ、使ってもいない商品の宣伝や心当たりのない動画などを勝手に投稿された	41	0.8
「あなたがアダルトサイトを閲覧している姿を撮影した。家族や同僚にばらまかれたくなければ、金銭を支払え」というメールを受信したので、金銭を支払った	35	0.7
過去1年間で上記のような被害はない	3854	77.1
上記のようなトラブルや被害があったかどうかわからない	750	15.0
集計母数	5000	100.0



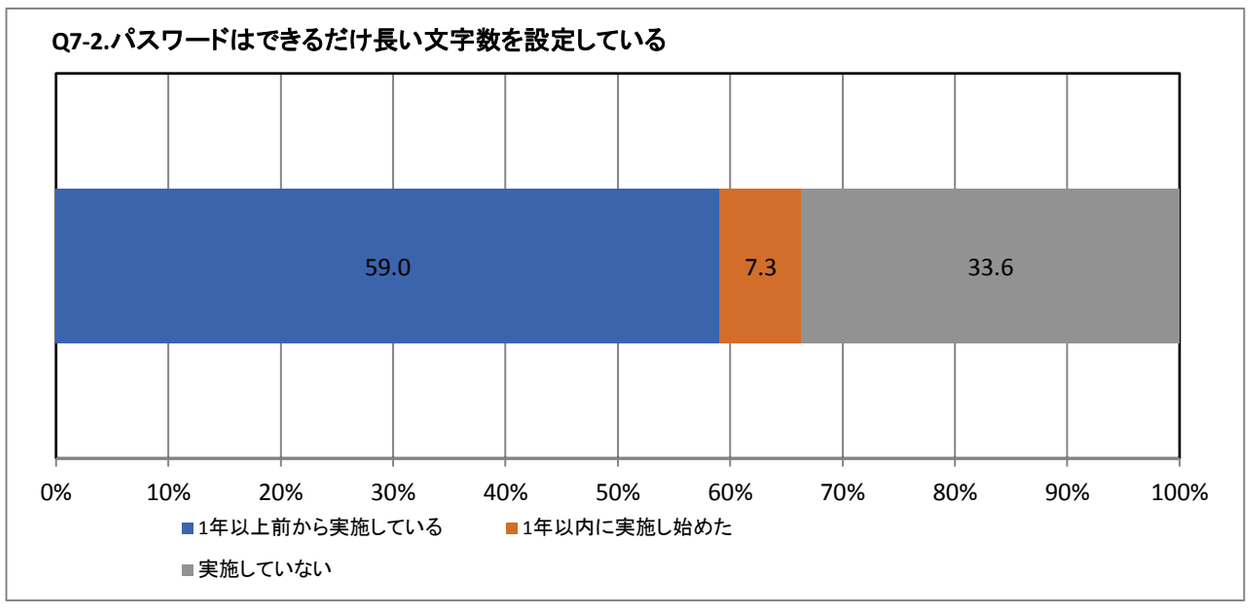
Q6 あなたが現在利用しているネットサービスで、利用時にログインを要求されるサービスのアカウント※数について、あてはまるものを選択してください。(お答えは1つ)	度数	%
1個	549	11.0
2個	416	8.3
3個	374	7.5
4個	125	2.5
5個	253	5.1
6～10個	609	12.2
11～20個	460	9.2
21～50個	420	8.4
51～100個	98	2.0
101個以上	46	0.9
いくつあるかわからない	1411	28.2
0個(自分以外の家族や契約者が管理しているなど)	239	4.8
集計母数	5000	100.0



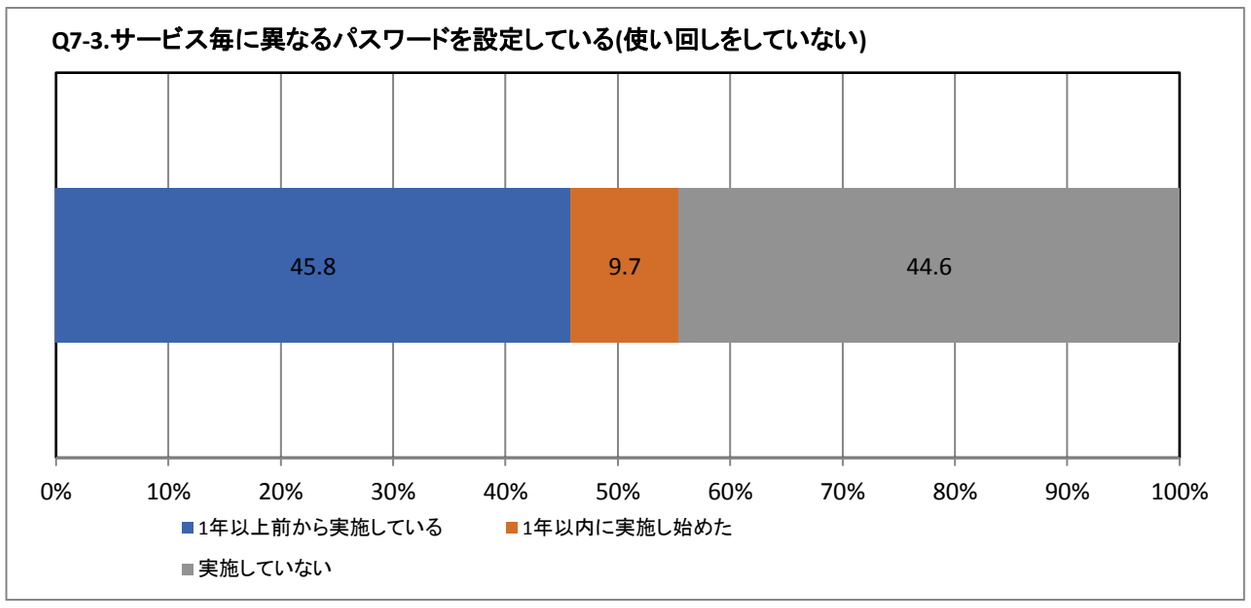
Q7 アカウントのパスワード設定における対策の実施について、あてはまるものを選択してください。(お答えはそれぞれ1つ)		
Q7-1.パスワードは他人が推測しにくい(氏名や誕生日などの情報を用いない)内容を設定している	度数	%
1年以上前から実施している	3399	71.4
1年以内に実施し始めた	302	6.3
実施していない	1060	22.3
集計母数	4761	100.0



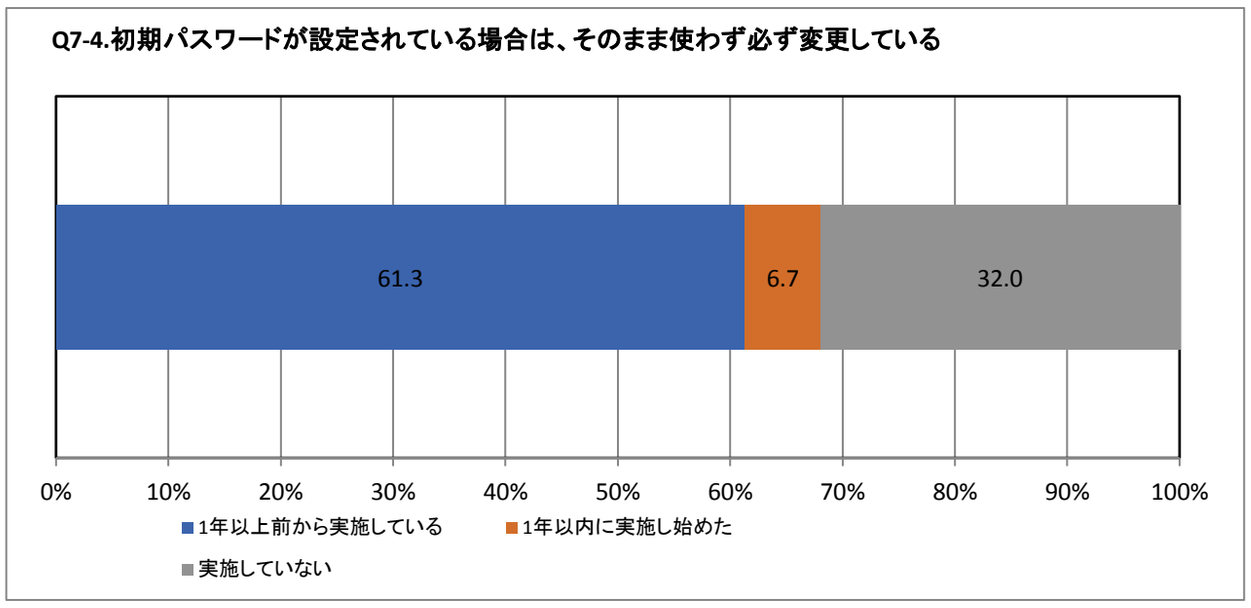
Q7-2.パスワードはできるだけ長い文字数を設定している	度数	%
1年以上前から実施している	2811	59.0
1年以内に実施し始めた	349	7.3
実施していない	1601	33.6
集計母数	4761	100.0



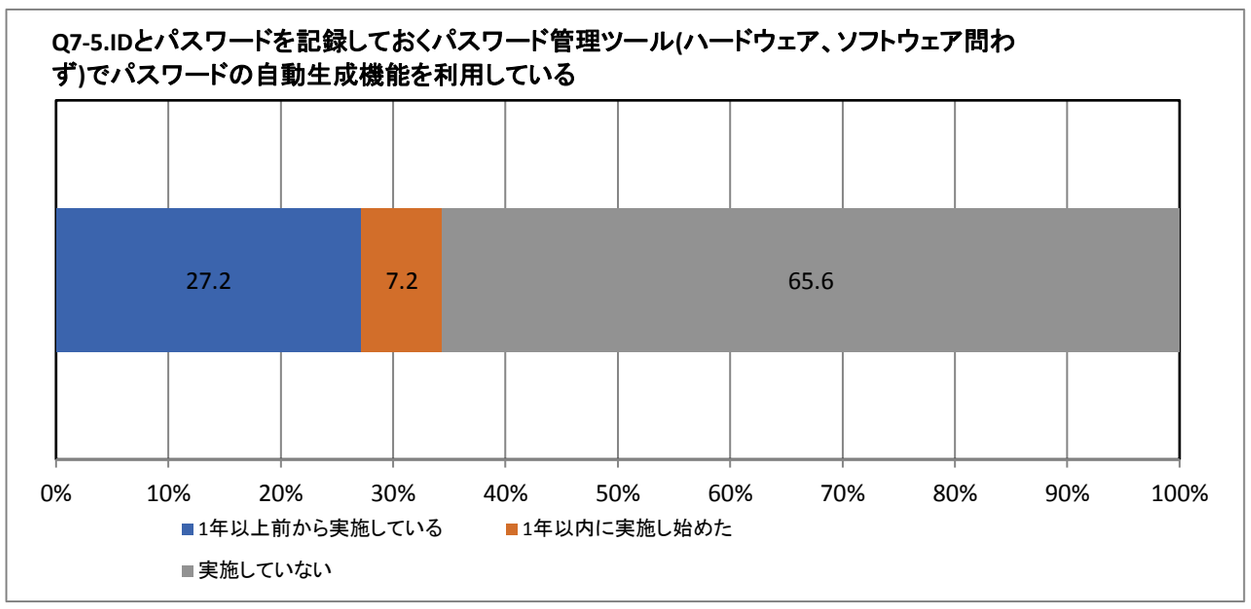
Q7-3.サービス毎に異なるパスワードを設定している(使い回しをしていない)	度数	%
1年以上前から実施している	1928	45.8
1年以内に実施し始めた	407	9.7
実施していない	1877	44.6
集計母数	4212	100.0



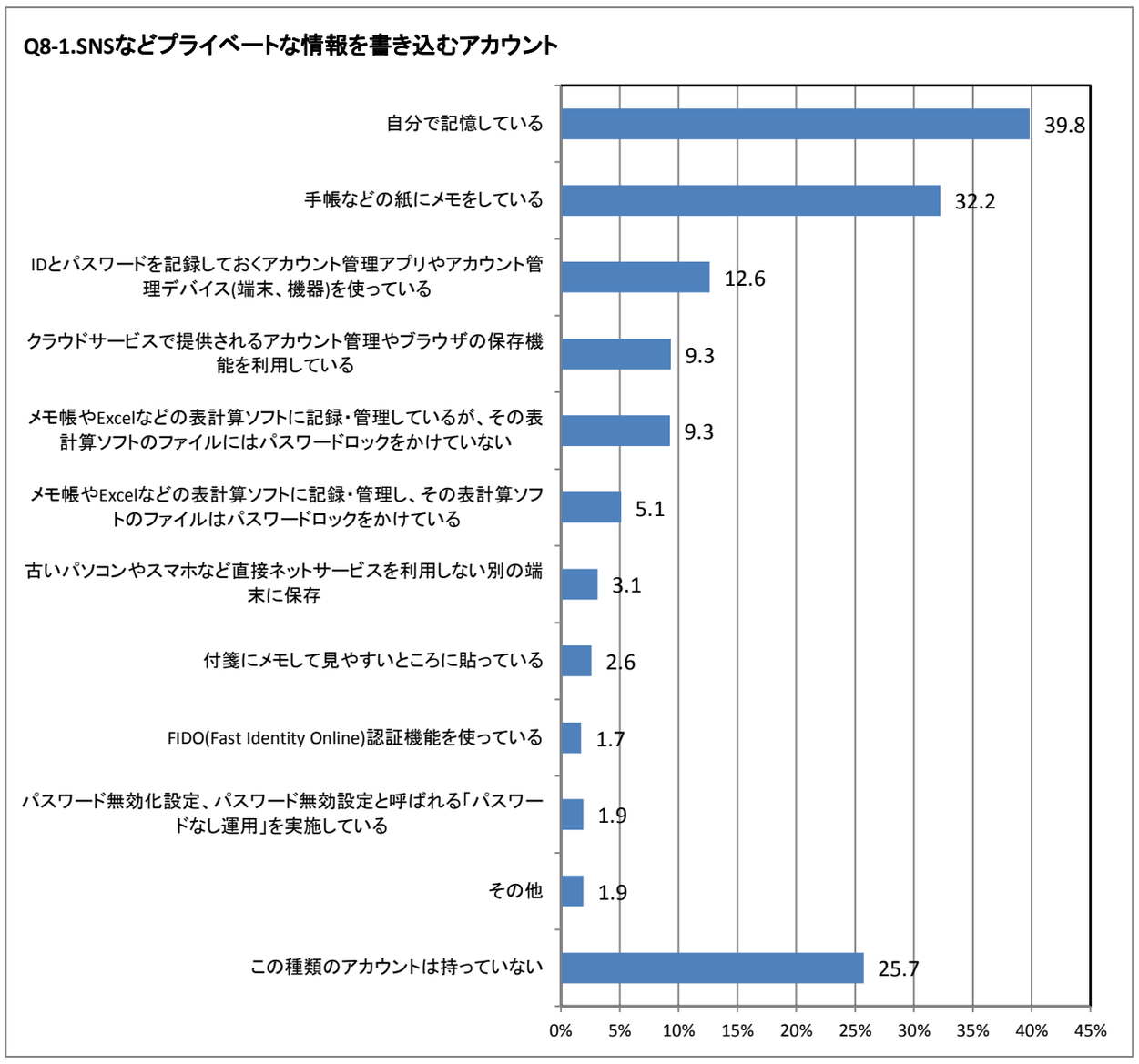
Q7-4.初期パスワードが設定されている場合は、そのまま使わず必ず変更している	度数	%
1年以上前から実施している	2919	61.3
1年以内に実施し始めた	320	6.7
実施していない	1522	32.0
集計母数	4761	100.0



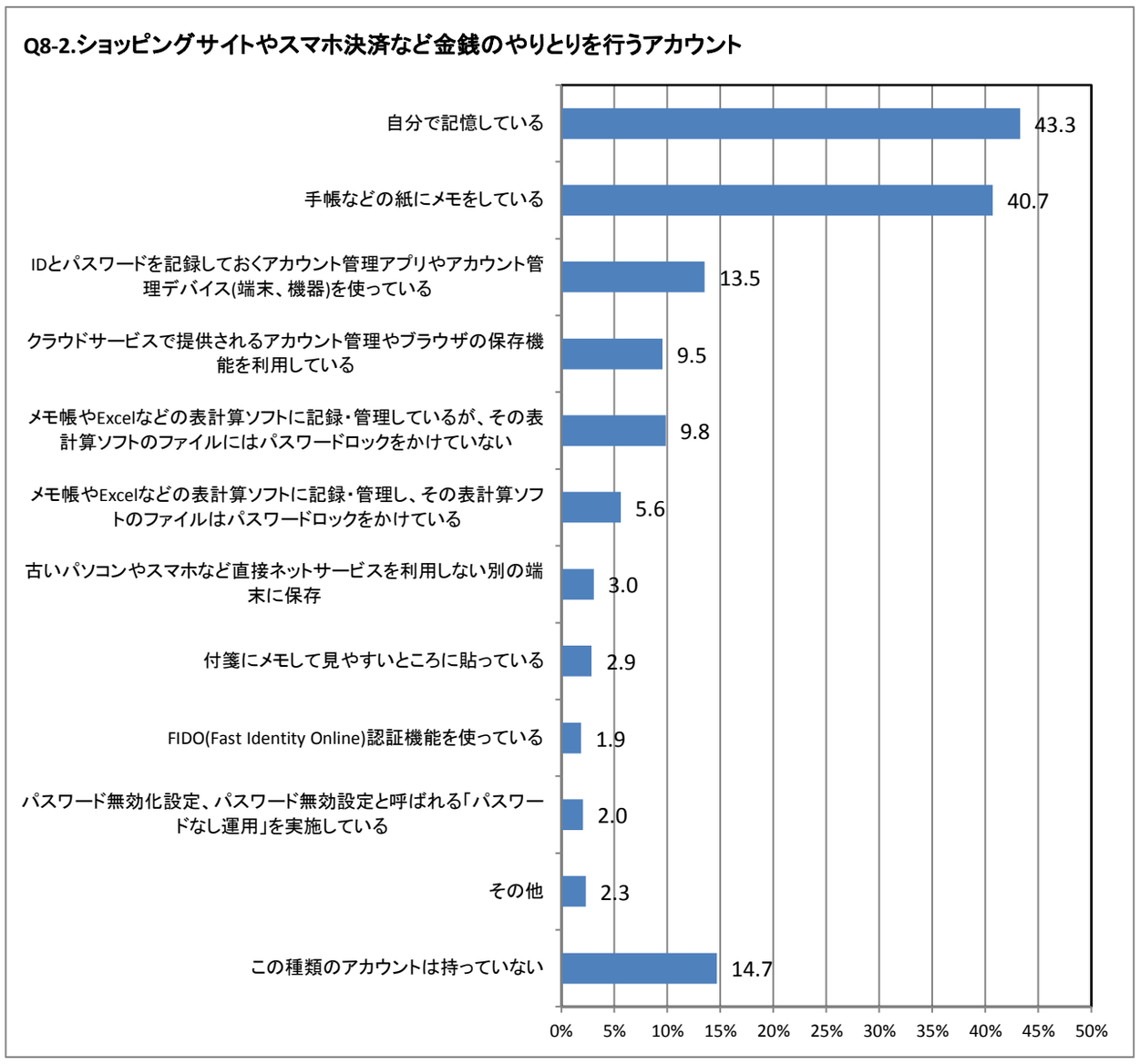
Q7-5.IDとパスワードを記録しておくパスワード管理ツール(ハードウェア、ソフトウェア問わず)でパスワードの自動生成機能を利用している	度数	%
1年以上前から実施している	1295	27.2
1年以内に実施し始めた	341	7.2
実施していない	3125	65.6
集計母数	4761	100.0



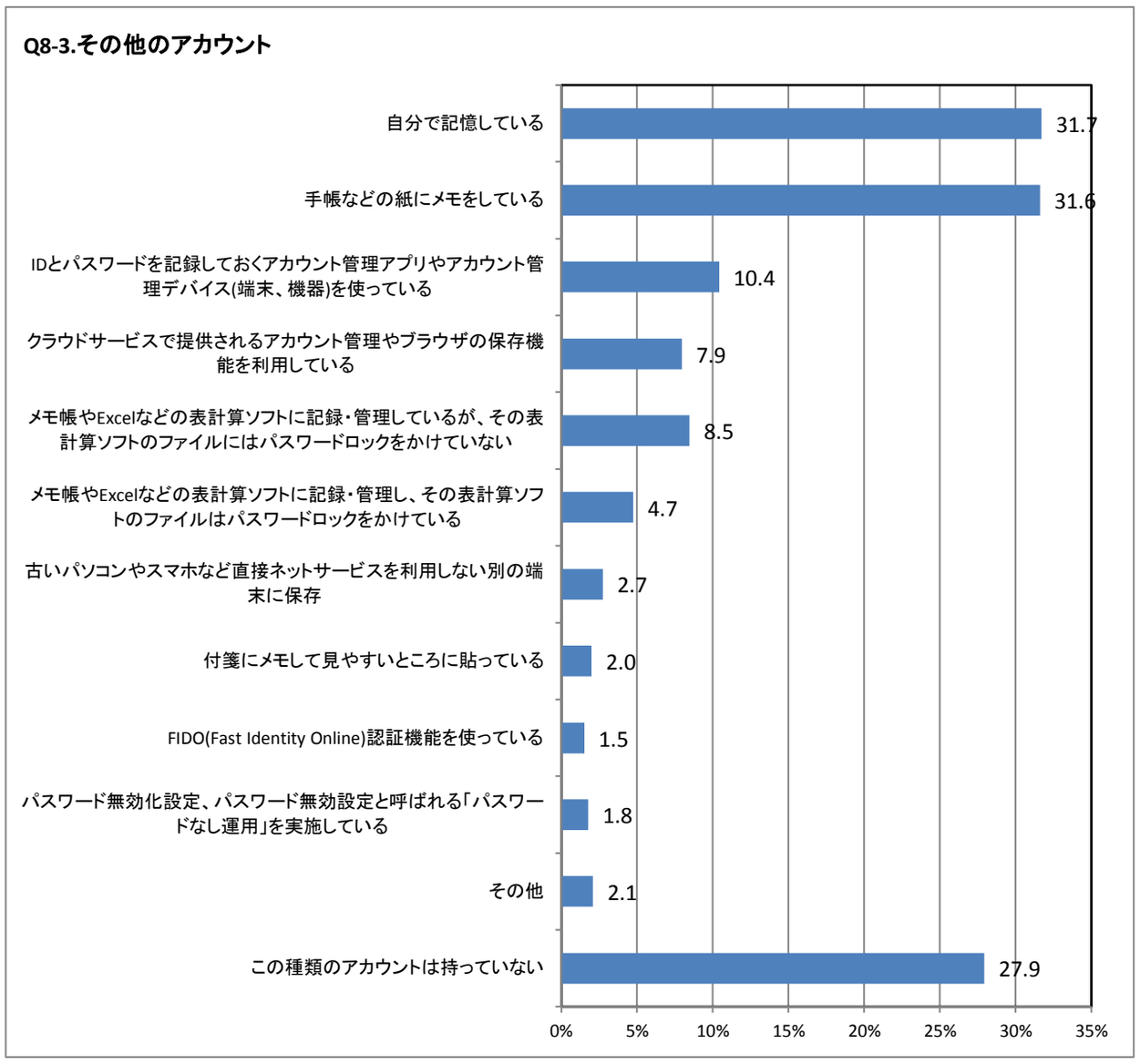
Q8 ネット上のサービスや電子メールのアカウント(IDやパスワード)の種類と管理方法について、あてはまるものを選択してください。(お答えはそれぞれいくつでも)		
Q8-1.SNSなどプライベートな情報を書き込むアカウント	度数	%
自分で記憶している	1897	39.8
手帳などの紙にメモをしている	1535	32.2
IDとパスワードを記録しておくアカウント管理アプリやアカウント管理デバイス(端末、機器)を使っている	602	12.6
クラウドサービスで提供されるアカウント管理やブラウザの保存機能を利用している	445	9.3
メモ帳やExcelなどの表計算ソフトに記録・管理しているが、その表計算ソフトのファイルにはパスワードロックをかけていない	441	9.3
メモ帳やExcelなどの表計算ソフトに記録・管理し、その表計算ソフトのファイルはパスワードロックをかけている	243	5.1
古いパソコンやスマホなど直接ネットサービスを利用しない別の端末に保存	148	3.1
付箋にメモして見やすいところに貼っている	123	2.6
FIDO(Fast Identity Online)認証機能を使っている	82	1.7
パスワード無効化設定、パスワード無効設定と呼ばれる「パスワードなし運用」を実施している	90	1.9
その他	91	1.9
この種類のアカウントは持っていない	1225	25.7
集計母数	4761	100.0



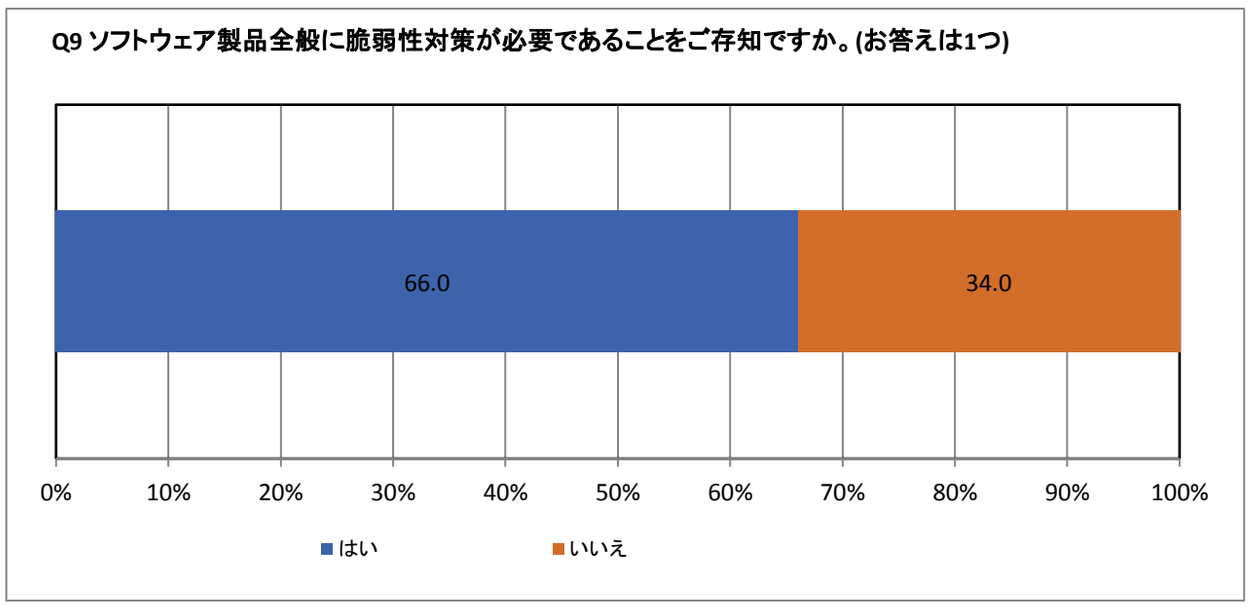
Q8-2.ショッピングサイトやスマホ決済など金銭のやりとりを行うアカウント	度数	%
自分で記憶している	2061	43.3
手帳などの紙にメモをしている	1938	40.7
IDとパスワードを記録しておくアカウント管理アプリやアカウント管理デバイス(端末、機器)を使っている	644	13.5
クラウドサービスで提供されるアカウント管理やブラウザの保存機能を利用している	454	9.5
メモ帳やExcelなどの表計算ソフトに記録・管理しているが、その表計算ソフトのファイルにはパスワードロックをかけていない	468	9.8
メモ帳やExcelなどの表計算ソフトに記録・管理し、その表計算ソフトのファイルはパスワードロックをかけている	267	5.6
古いパソコンやスマホなど直接ネットサービスを利用しない別の端末に保存	145	3.0
付箋にメモして見やすいところに貼っている	136	2.9
FIDO(Fast Identity Online)認証機能を使っている	89	1.9
パスワード無効化設定、パスワード無効設定と呼ばれる「パスワードなし運用」を実施している	97	2.0
その他	109	2.3
この種類のアカウントは持っていない	698	14.7
集計母数	4761	100.0



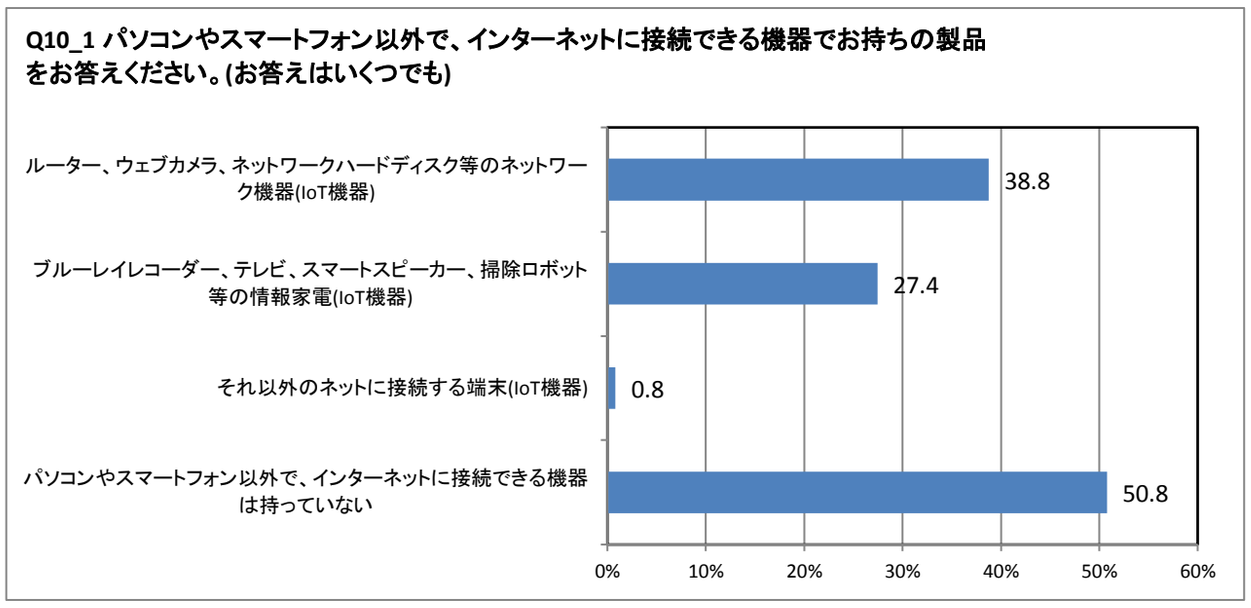
Q8-3.その他のアカウント	度数	%
自分で記憶している	1510	31.7
手帳などの紙にメモをしている	1505	31.6
IDとパスワードを記録しておくアカウント管理アプリやアカウント管理デバイス(端末、機器)を使っている	496	10.4
クラウドサービスで提供されるアカウント管理やブラウザの保存機能を利用している	378	7.9
メモ帳やExcelなどの表計算ソフトに記録・管理しているが、その表計算ソフトのファイルにはパスワードロックをかけていない	403	8.5
メモ帳やExcelなどの表計算ソフトに記録・管理し、その表計算ソフトのファイルはパスワードロックをかけている	226	4.7
古いパソコンやスマホなど直接ネットサービスを利用しない別の端末に保存	130	2.7
付箋にメモして見やすいところに貼っている	95	2.0
FIDO(Fast Identity Online)認証機能を使っている	72	1.5
パスワード無効化設定、パスワード無効設定と呼ばれる「パスワードなし運用」を実施している	84	1.8
その他	99	2.1
この種類のアカウントは持っていない	1330	27.9
集計母数	4761	100.0



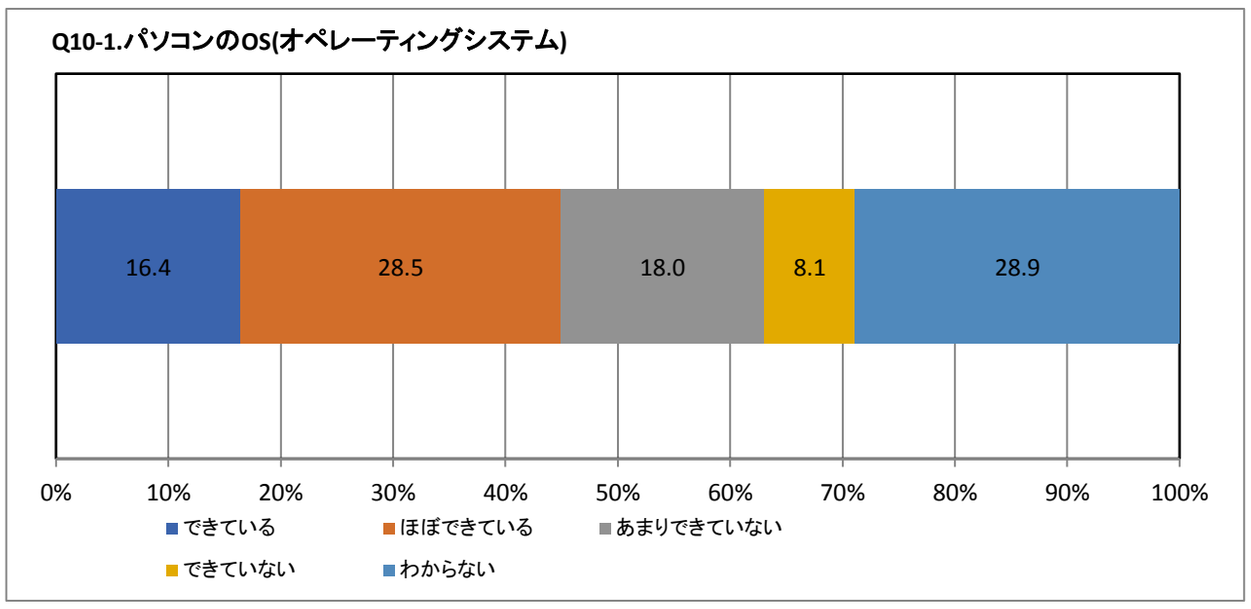
Q9 ソフトウェア製品全般に脆弱性対策が必要であることをご存知ですか。(お答えは1つ)	度数	%
はい	3302	66.0
いいえ	1698	34.0
集計母数	5000	100.0



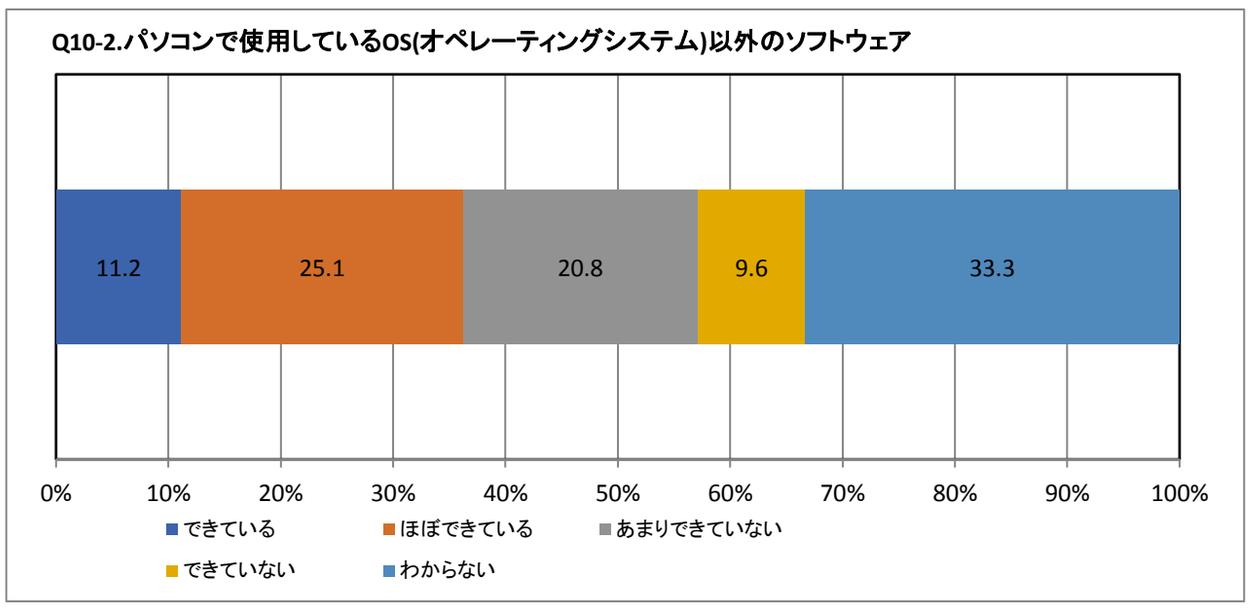
Q10_1 パソコンやスマートフォン以外で、インターネットに接続できる機器でお持ちの製品をお答えください。(お答えはいくつでも)	度数	%
ルーター、ウェブカメラ、ネットワークハードディスク等のネットワーク機器(IoT機器)	1938	38.8
ブルーレイレコーダー、テレビ、スマートスピーカー、掃除ロボット等の情報家電(IoT機器)	1372	27.4
それ以外のネットに接続する端末(IoT機器)	41	0.8
パソコンやスマートフォン以外で、インターネットに接続できる機器は持っていない	2539	50.8
集計母数	5000	100.0



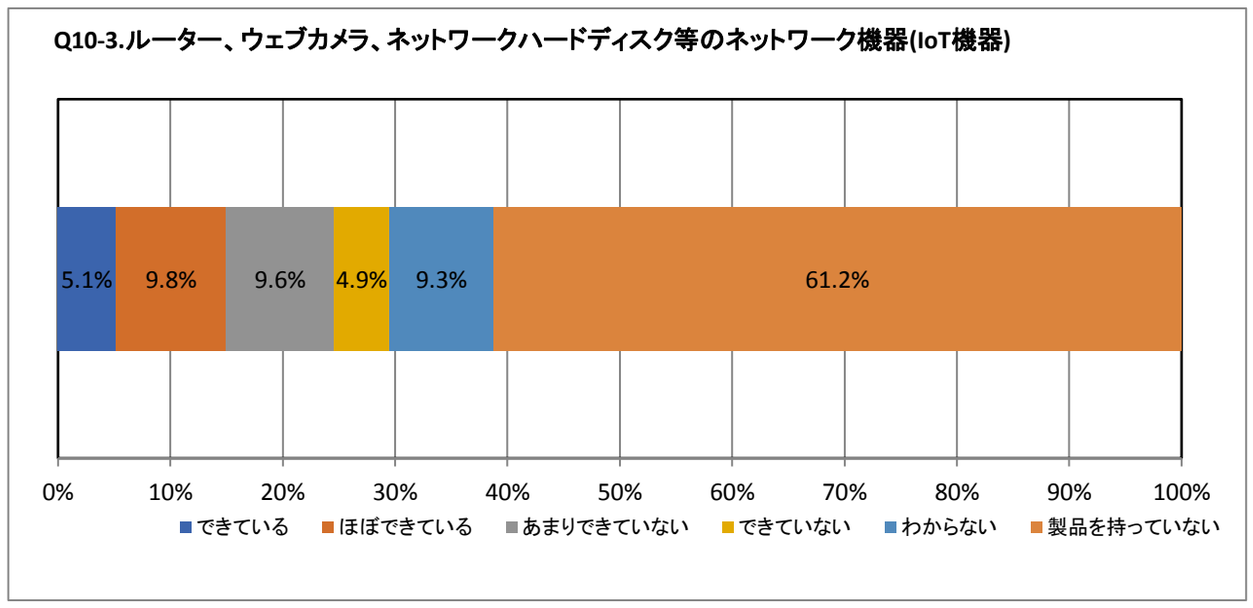
Q10_2 脆弱性対策について、あなたの実施状況に近いものを選択してください。(お答えはそれぞれ1つ)		
Q10-1.パソコンのOS(オペレーティングシステム)	度数	%
できている	821	16.4
ほぼできている	1427	28.5
あまりできていない	902	18.0
できていない	407	8.1
わからない	1443	28.9
集計母数	5000	100.0



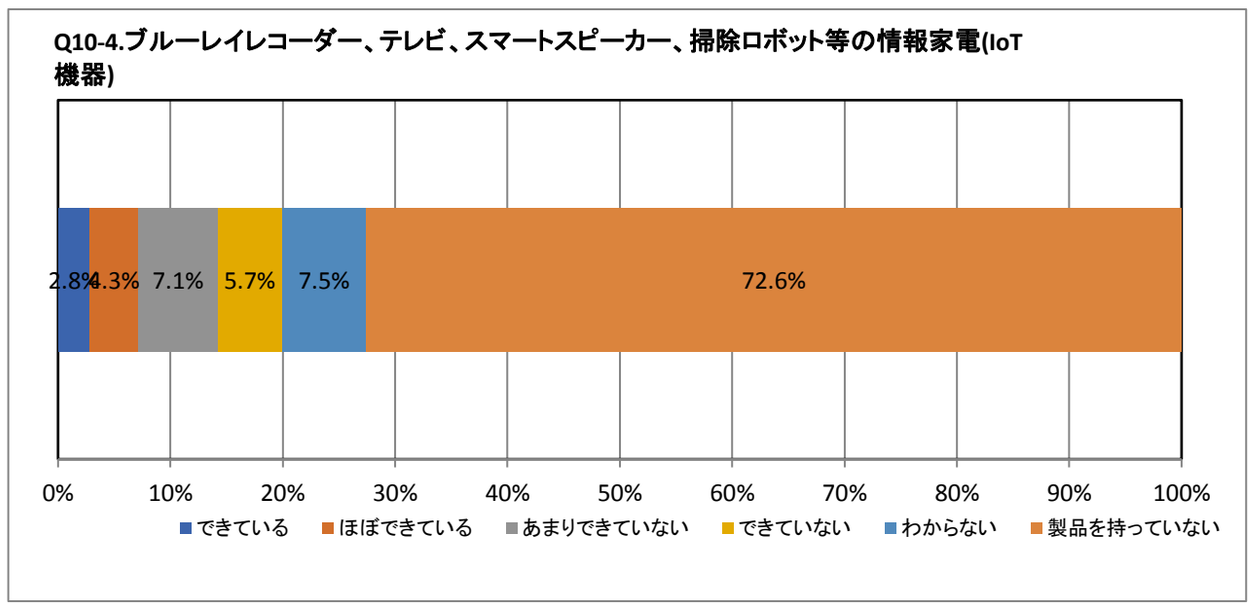
Q10-2.パソコンで使用しているOS(オペレーティングシステム)以外のソフトウェア	度数	%
できている	558	11.2
ほぼできている	1255	25.1
あまりできていない	1041	20.8
できていない	480	9.6
わからない	1666	33.3
集計母数	5000	100.0



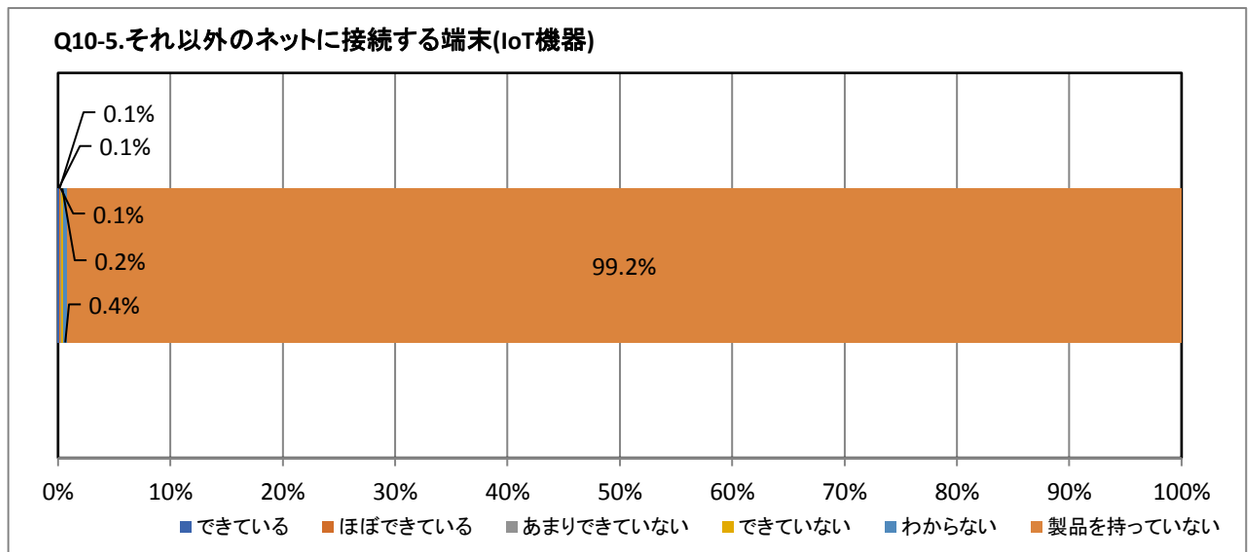
Q10-3.ルーター、ウェブカメラ、ネットワークハードディスク等のネットワーク機器(IoT機器)	度数	%
できている	257	5.1%
ほぼできている	492	9.8%
あまりできていない	479	9.6%
できていない	247	4.9%
わからない	463	9.3%
製品を持っていない	3062	61.2%
集計母数	5000	100%



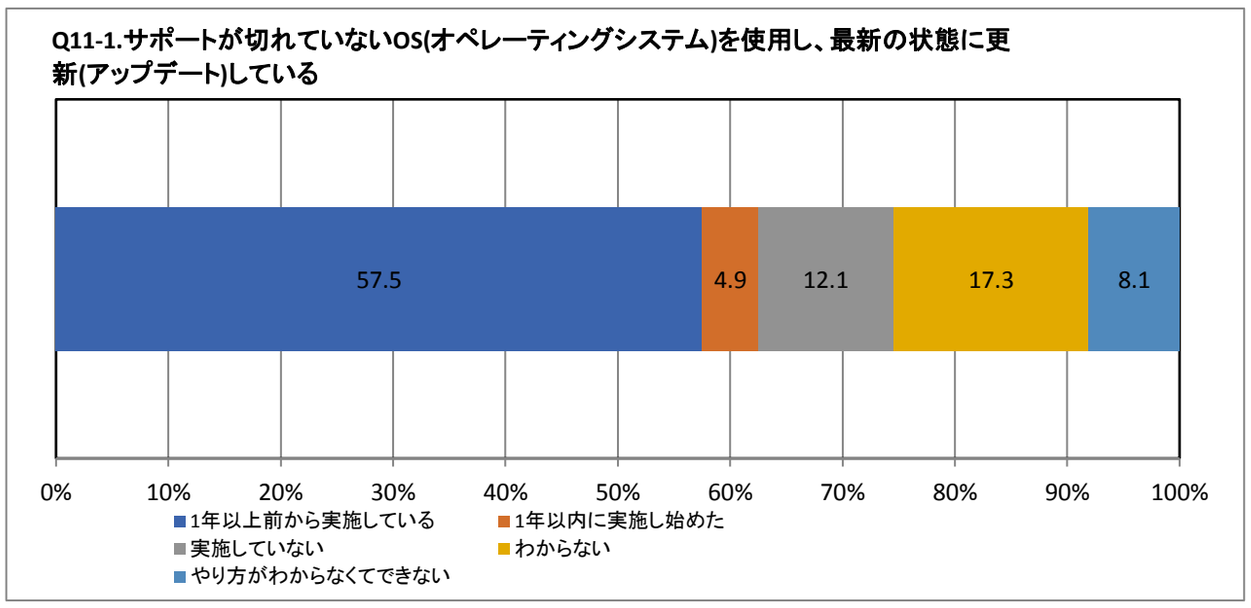
Q10-4.ブルーレイレコーダー、テレビ、スマートスピーカー、掃除ロボット等の情報家電(IoT機器)	度数	%
できている	141	2.8%
ほぼできている	216	4.3%
あまりできていない	354	7.1%
できていない	284	5.7%
わからない	377	7.5%
製品を持っていない	3628	72.6%
集計母数	5000	100%



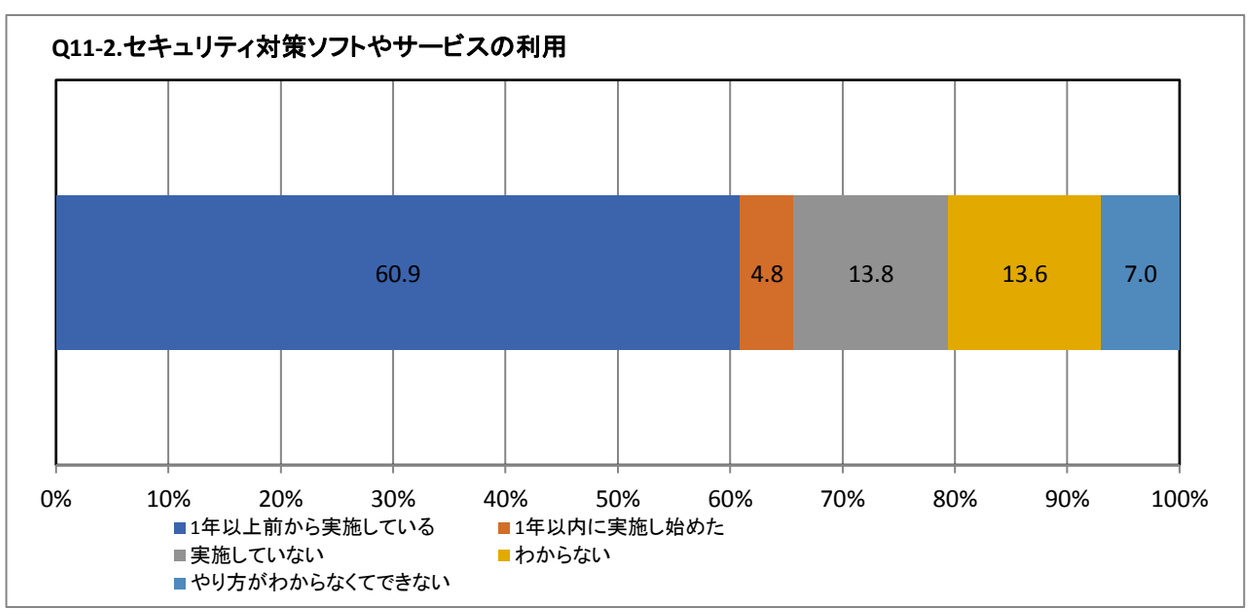
Q10-5.それ以外のネットに接続する端末(IoT機器)	度数	%
できている	5	0.1%
ほぼできている	4	0.1%
あまりできていない	6	0.1%
できていない	8	0.2%
わからない	18	0.4%
製品を持っていない	4959	99.2%
集計母数	41	100.0



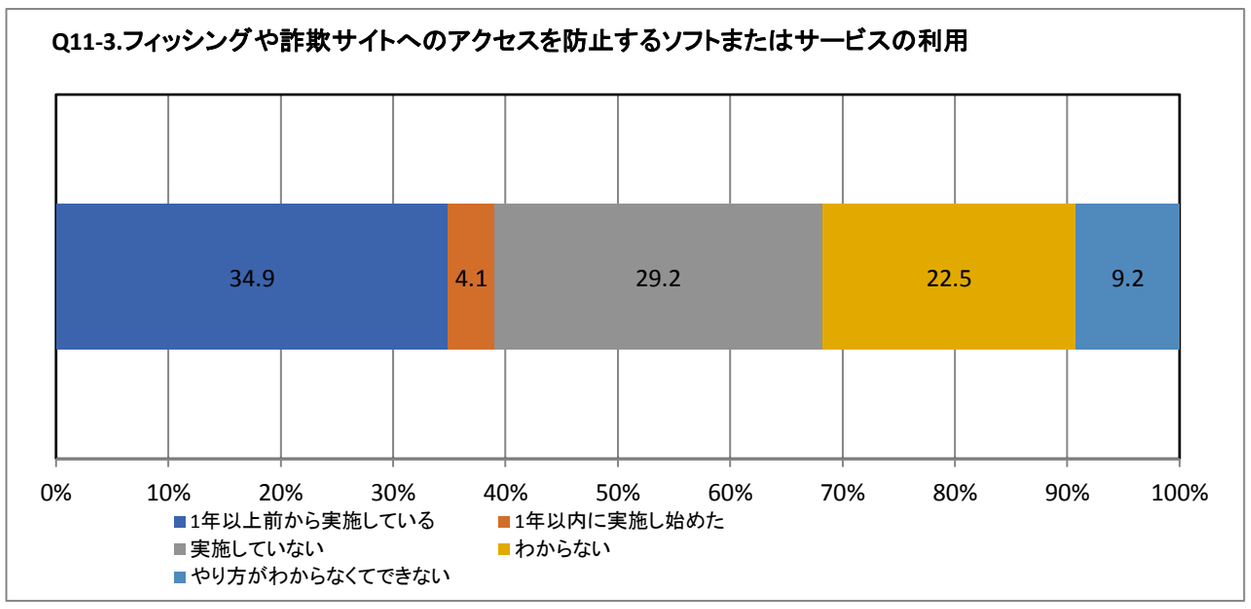
Q11 私物のパソコンや自宅のネットワークのセキュリティ対策について、実施状況としてあてはまるものを選択してください。(お答えはそれぞれ1つ)		
Q11-1.サポートが切れていないOS(オペレーティングシステム)を使用し、最新の状態に更新(アップデート)している	度数	%
1年以上前から実施している	2877	57.5
1年以内に実施し始めた	247	4.9
実施していない	605	12.1
わからない	866	17.3
やり方がわからなくてできない	405	8.1
集計母数	5000	100.0



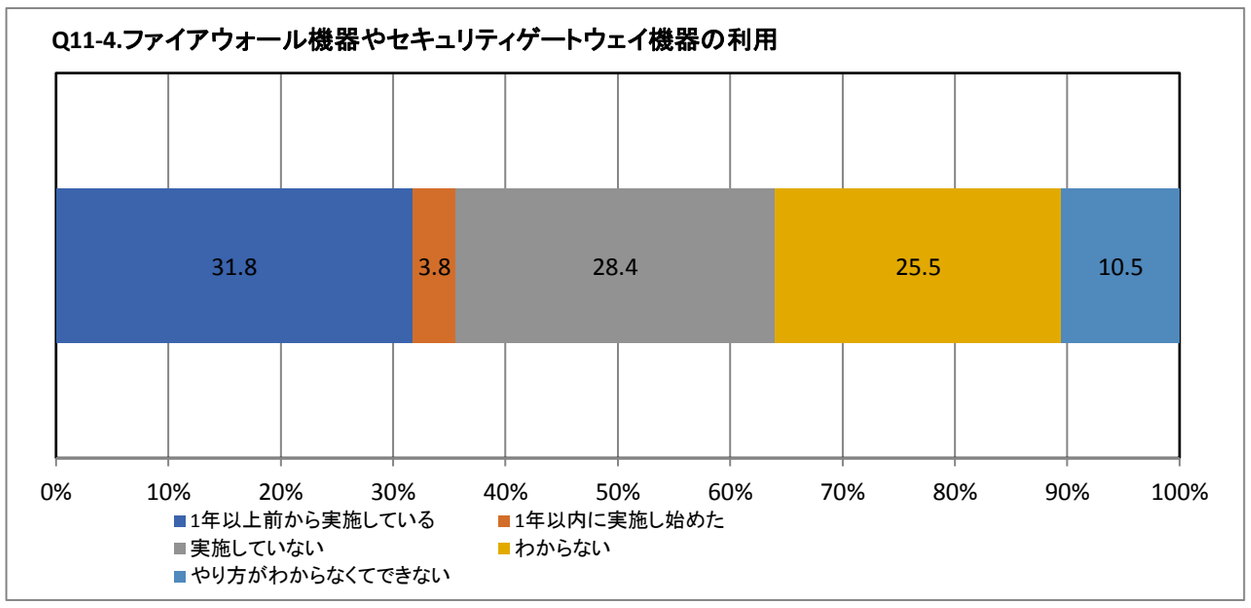
Q11-2.セキュリティ対策ソフトやサービスの利用	度数	%
1年以上前から実施している	3044	60.9
1年以内に実施し始めた	238	4.8
実施していない	689	13.8
わからない	680	13.6
やり方がわからなくてできない	349	7.0
集計母数	5000	100.0



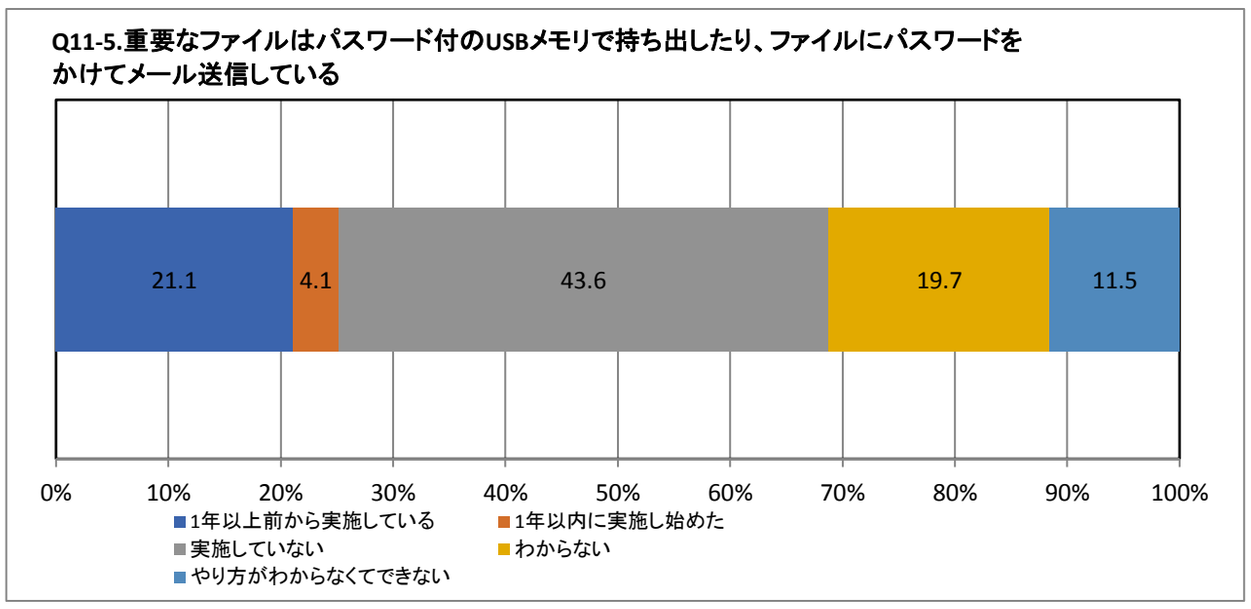
Q11-3.フィッシングや詐欺サイトへのアクセスを防止するソフトまたはサービスの利用	度数	%
1年以上前から実施している	1746	34.9
1年以内に実施し始めた	204	4.1
実施していない	1461	29.2
わからない	1127	22.5
やり方がわからなくてできない	462	9.2
集計母数	5000	100.0



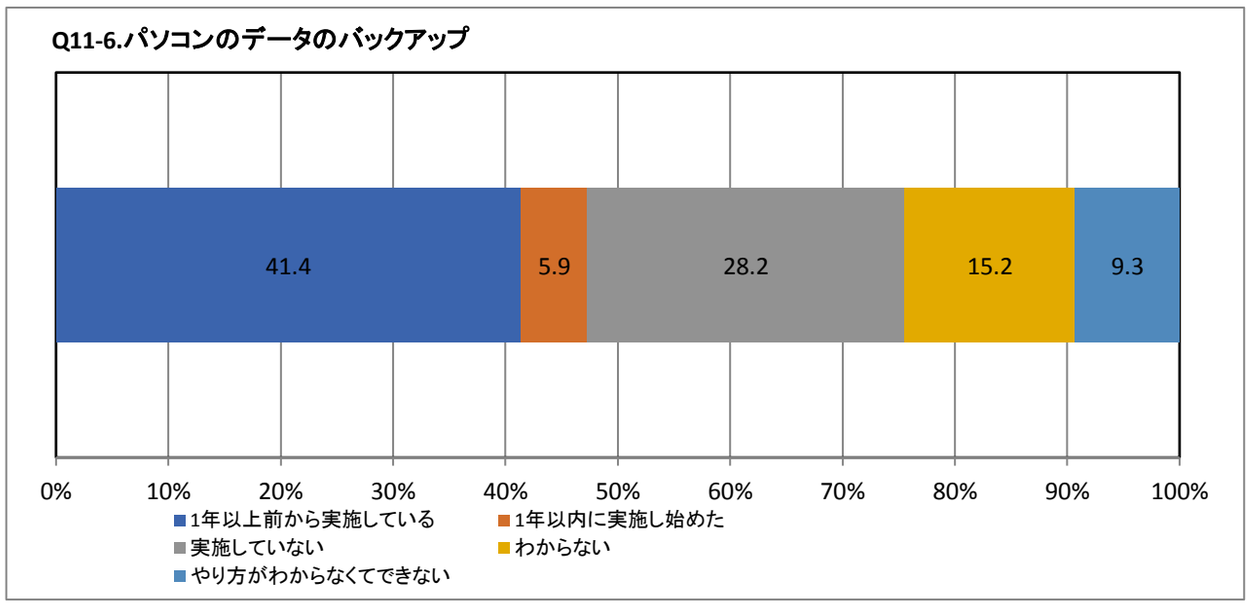
Q11-4.ファイアウォール機器やセキュリティゲートウェイ機器の利用	度数	%
1年以上前から実施している	1588	31.8
1年以内に実施し始めた	190	3.8
実施していない	1421	28.4
わからない	1276	25.5
やり方がわからなくてできない	525	10.5
集計母数	5000	100.0



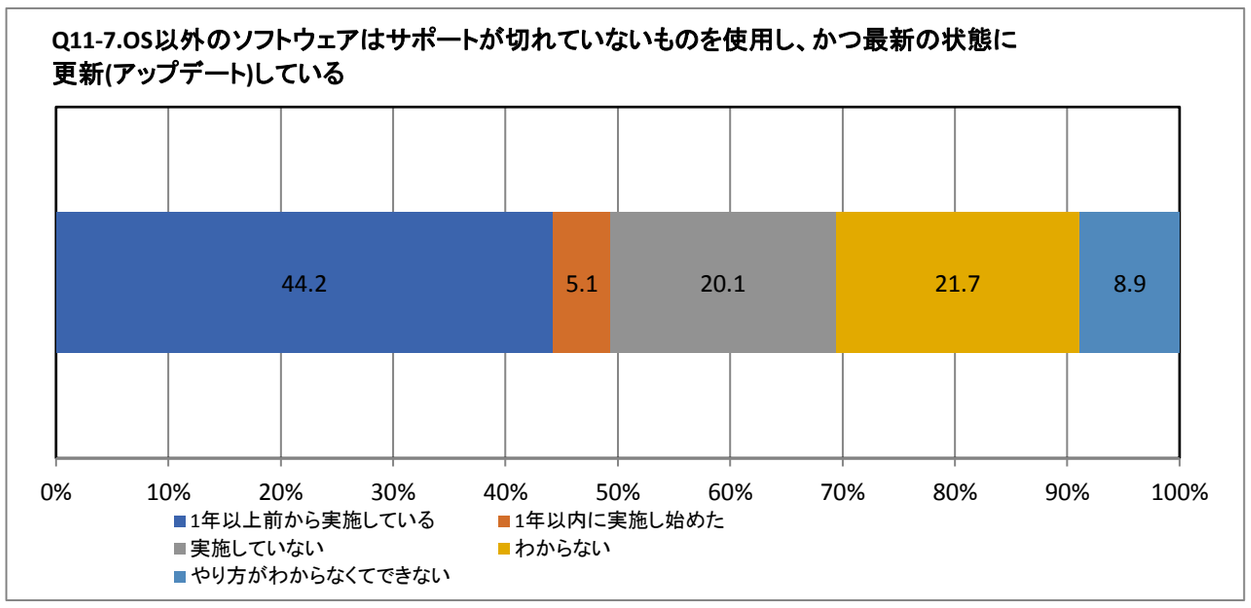
Q11-5.重要なファイルはパスワード付のUSBメモリで持ち出したり、ファイルにパスワードをかけてメール送信している	度数	%
1年以上前から実施している	1054	21.1
1年以内に実施し始めた	203	4.1
実施していない	2181	43.6
わからない	986	19.7
やり方がわからなくてできない	576	11.5
集計母数	5000	100.0



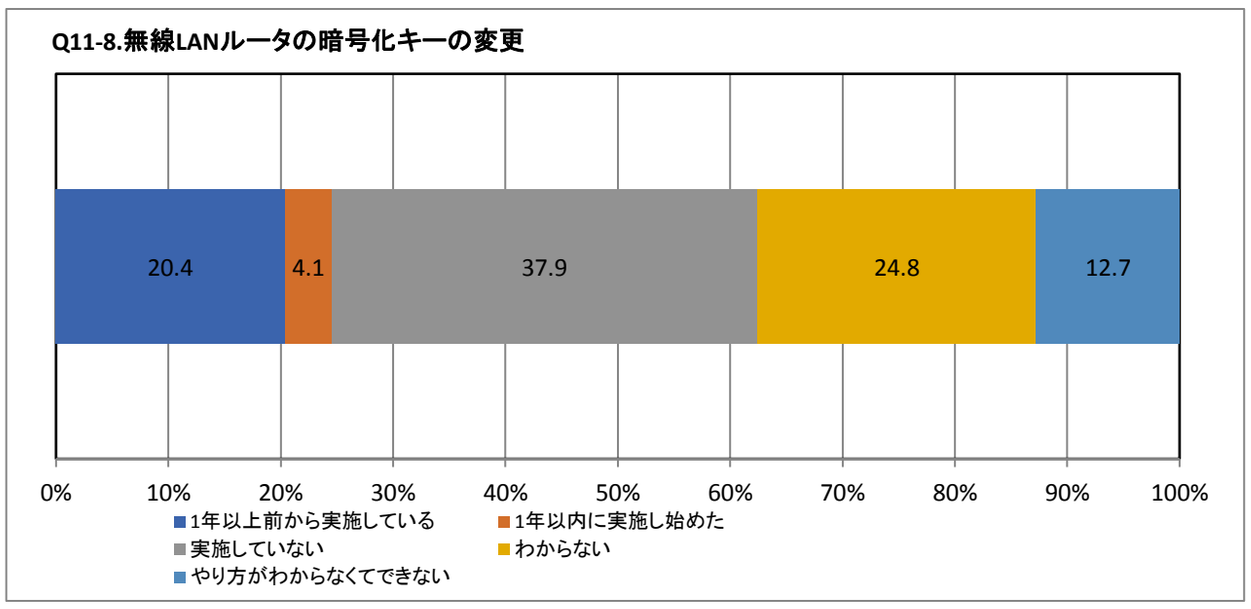
Q11-6.パソコンのデータのバックアップ	度数	%
1年以上前から実施している	2069	41.4
1年以内に実施し始めた	296	5.9
実施していない	1411	28.2
わからない	760	15.2
やり方がわからなくてできない	464	9.3
集計母数	5000	100.0



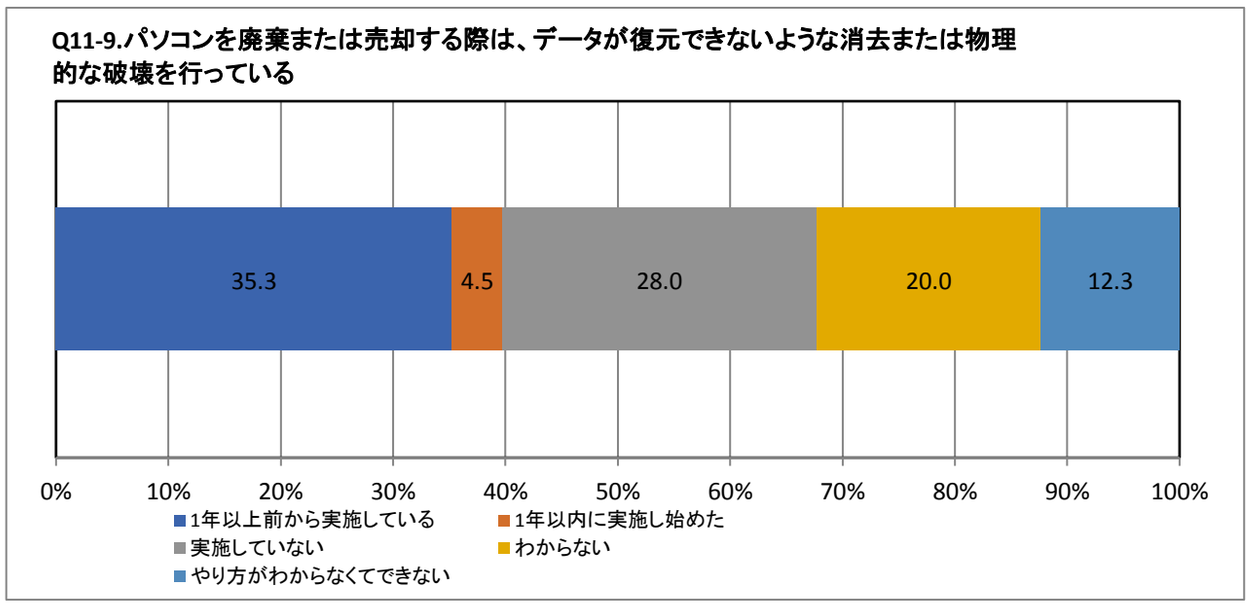
Q11-7.OS以外のソフトウェアはサポートが切れていないものを使用し、かつ最新の状態に更新(アップデート)している	度数	%
1年以上前から実施している	2212	44.2
1年以内に実施し始めた	255	5.1
実施していない	1003	20.1
わからない	1085	21.7
やり方がわからなくてできない	445	8.9
集計母数	5000	100.0



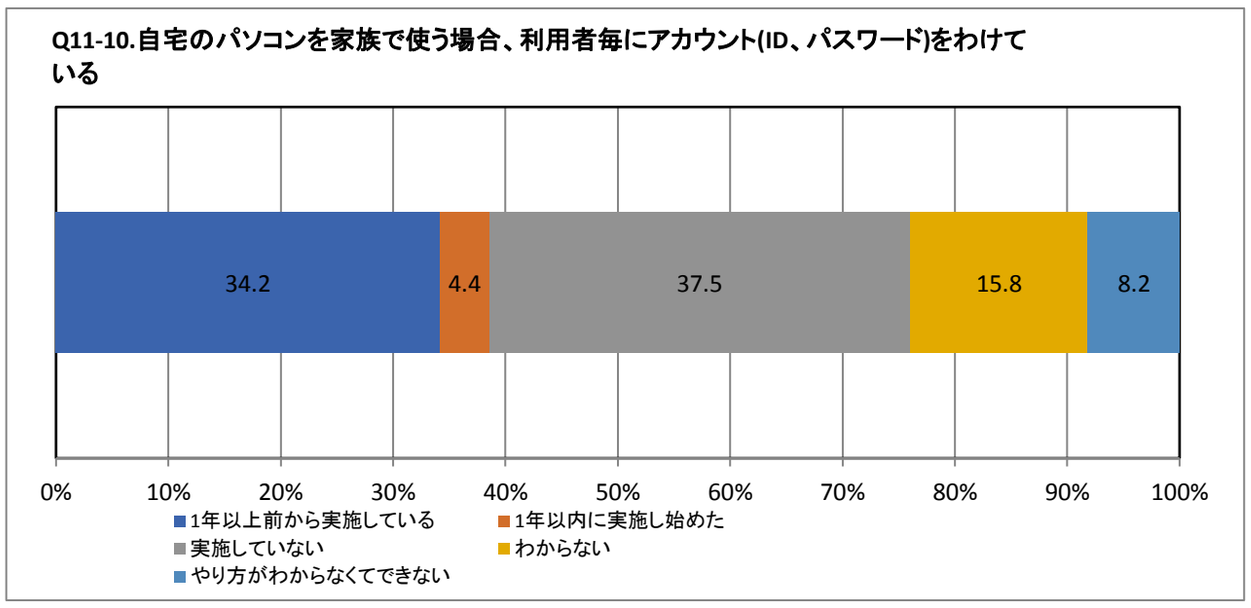
Q11-8.無線LANルータの暗号化キーの変更	度数	%
1年以上前から実施している	1019	20.4
1年以内に実施し始めた	207	4.1
実施していない	1895	37.9
わからない	1242	24.8
やり方がわからなくてできない	637	12.7
集計母数	5000	100.0



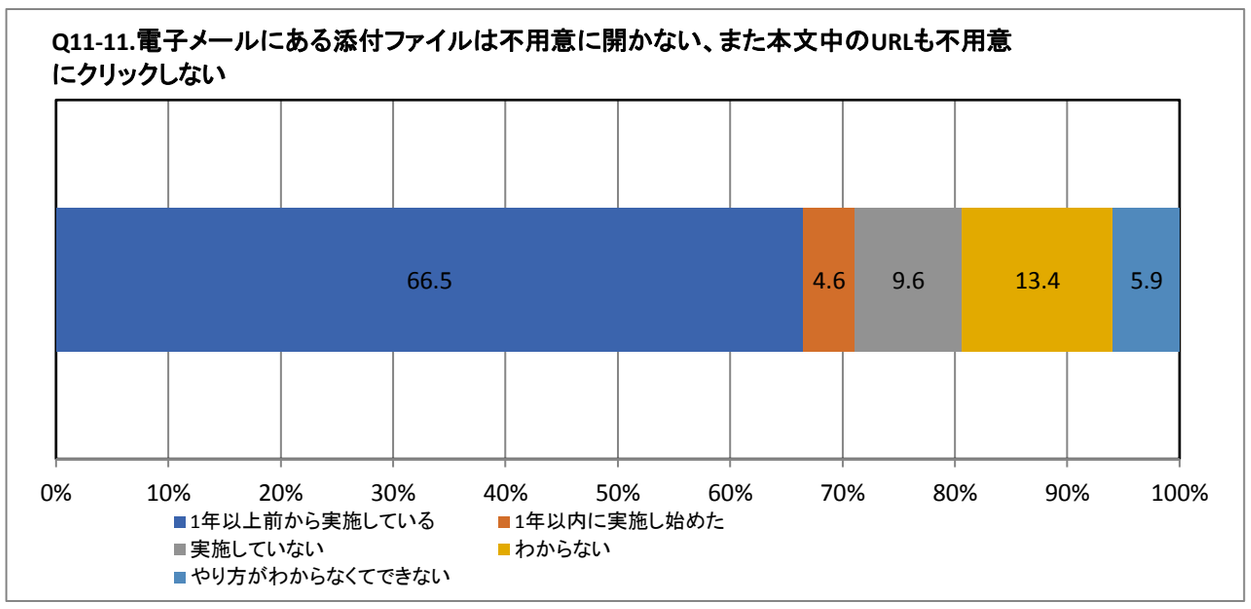
Q11-9.パソコンを廃棄または売却する際は、データが復元できないような消去または物理的な破壊を行っている	度数	%
1年以上前から実施している	1763	35.3
1年以内に実施し始めた	223	4.5
実施していない	1398	28.0
わからない	1000	20.0
やり方がわからなくてできない	616	12.3
集計母数	5000	100.0



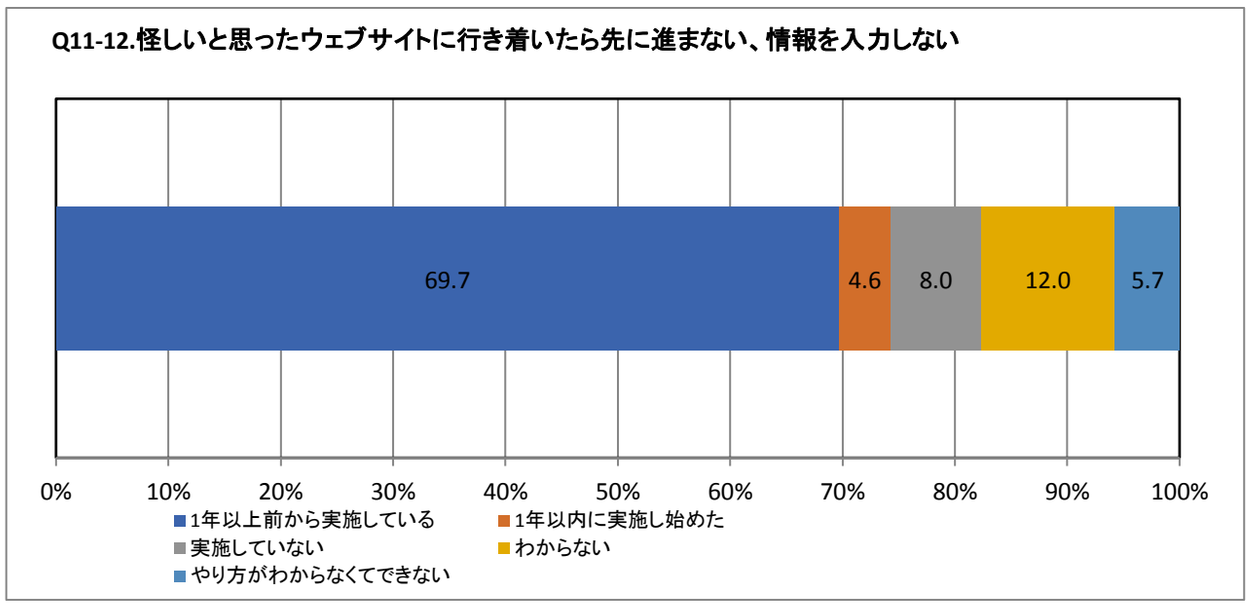
Q11-10.自宅のパソコンを家族で使う場合、利用者毎にアカウント(ID、パスワード)をわけている	度数	%
1年以上前から実施している	1708	34.2
1年以内に実施し始めた	220	4.4
実施していない	1873	37.5
わからない	791	15.8
やり方がわからなくてできない	408	8.2
集計母数	5000	100.0



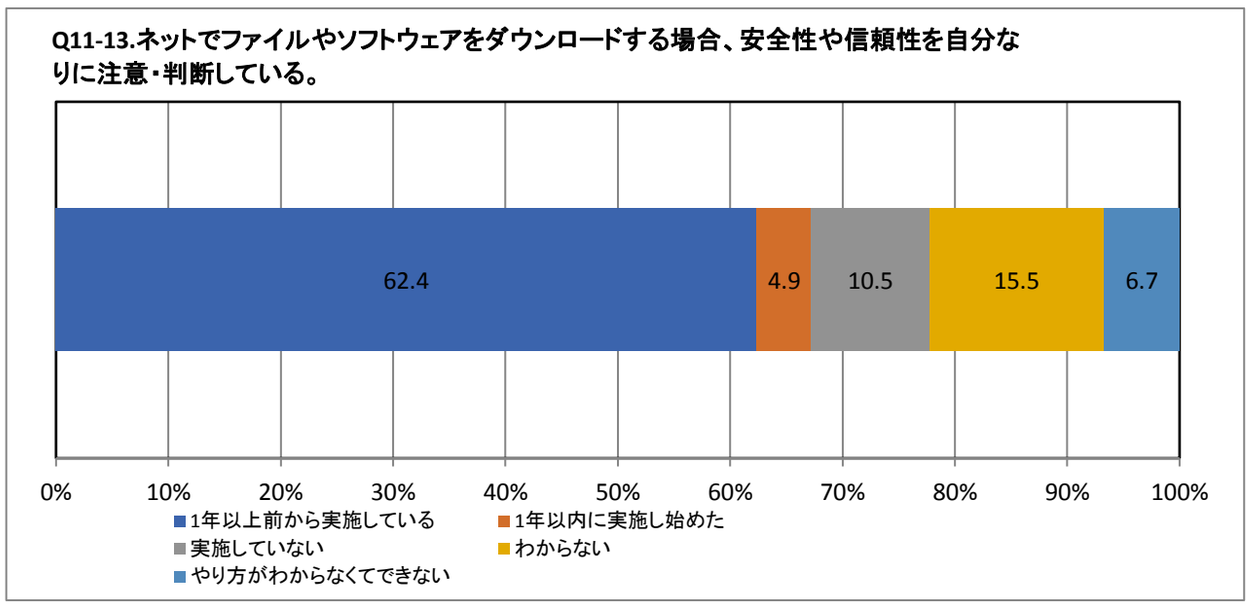
Q11-11.電子メールにある添付ファイルは不用意に開かない、また本文中のURLも不用意にクリックしない	度数	%
1年以上前から実施している	3325	66.5
1年以内に実施し始めた	228	4.6
実施していない	479	9.6
わからない	672	13.4
やり方がわからなくてできない	296	5.9
集計母数	5000	100.0



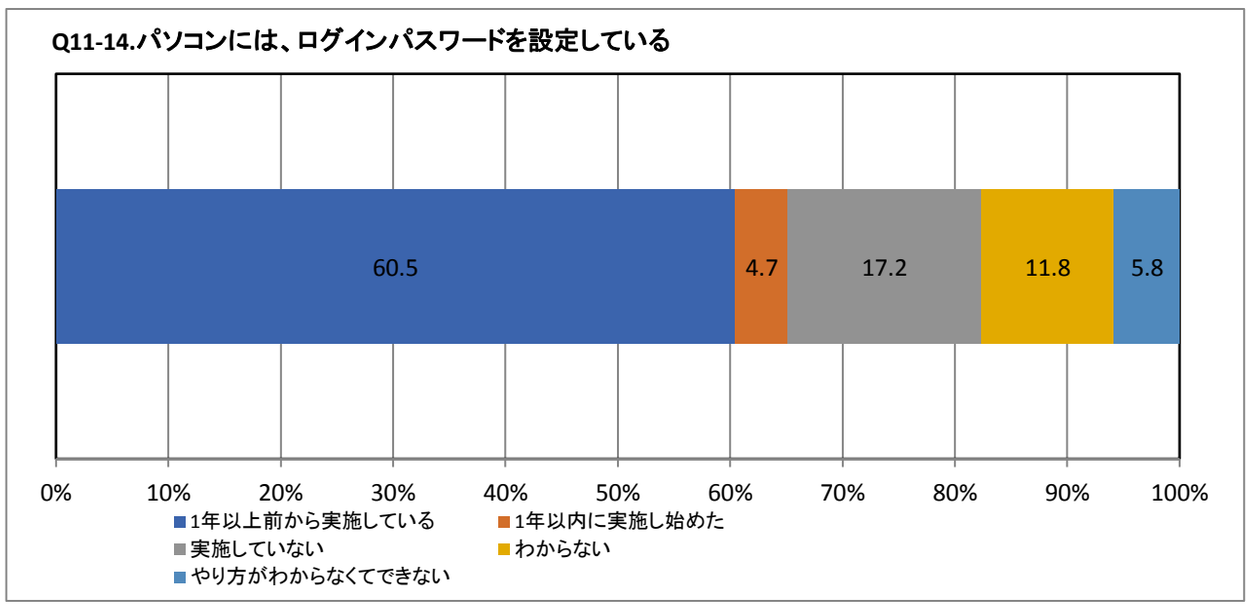
Q11-12.怪しいと思ったウェブサイトに行き着いたら先に進まない、情報を入力しない	度数	%
1年以上前から実施している	3484	69.7
1年以内に実施し始めた	229	4.6
実施していない	402	8.0
わからない	598	12.0
やり方がわからなくてできない	287	5.7
集計母数	5000	100.0



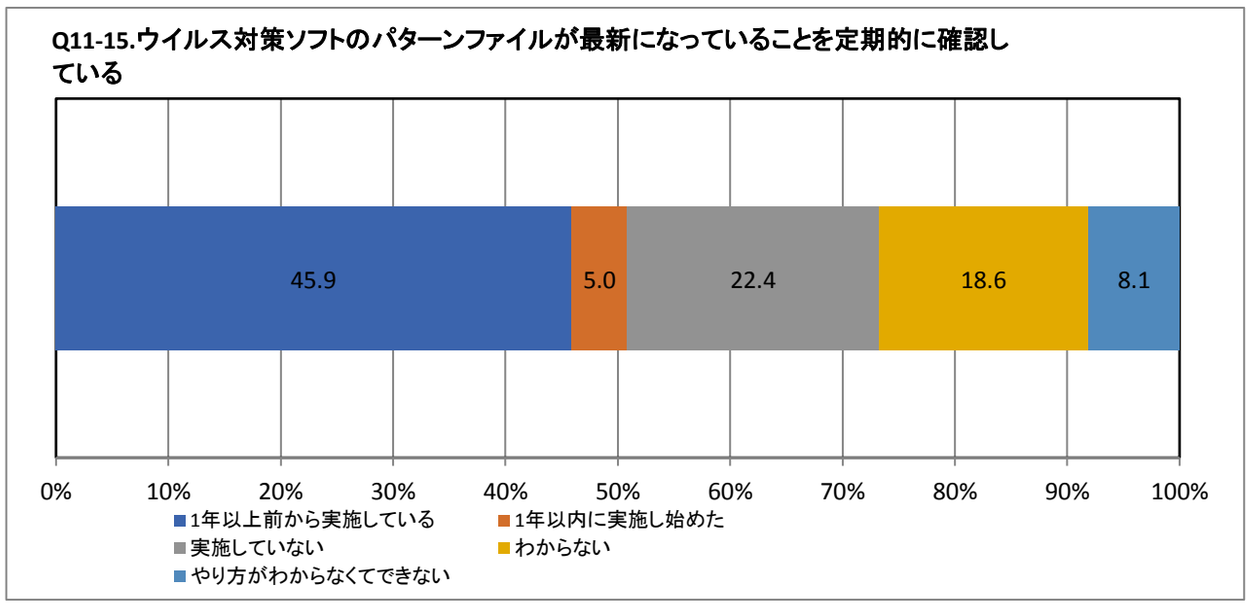
Q11-13.ネットでファイルやソフトウェアをダウンロードする場合、安全性や信頼性を自分なりに注意・判断している。	度数	%
1年以上前から実施している	3119	62.4
1年以内に実施し始めた	243	4.9
実施していない	525	10.5
わからない	776	15.5
やり方がわからなくてできない	337	6.7
集計母数	5000	100.0



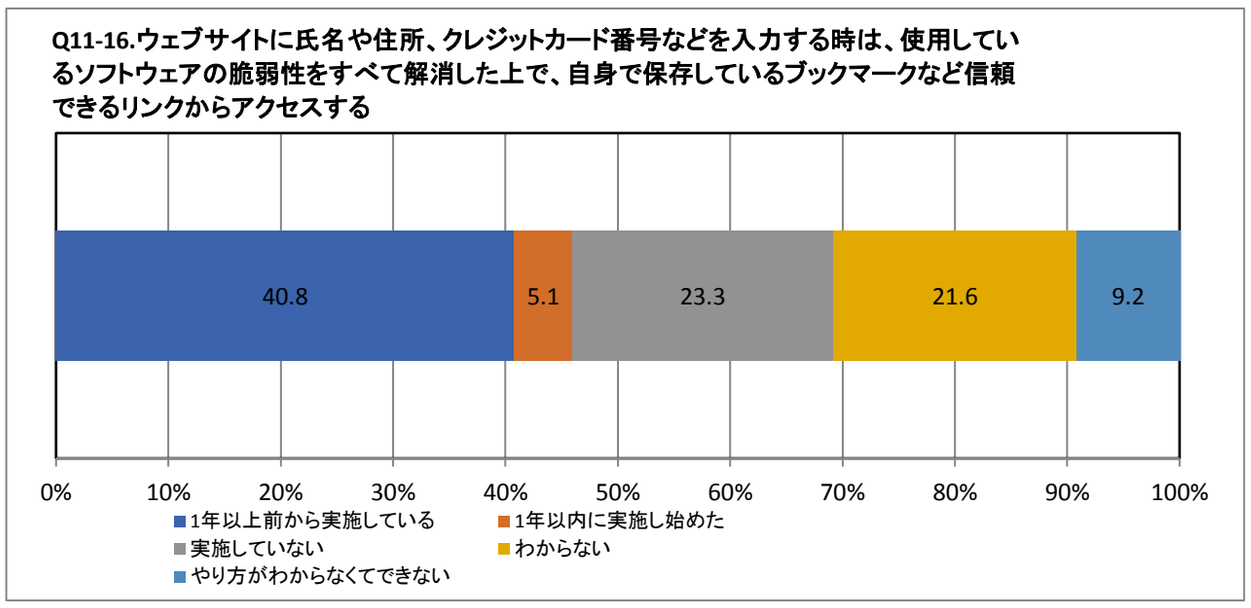
Q11-14.パソコンには、ログインパスワードを設定している	度数	%
1年以上前から実施している	3023	60.5
1年以内に実施し始めた	234	4.7
実施していない	861	17.2
わからない	592	11.8
やり方がわからなくてできない	290	5.8
集計母数	5000	100.0



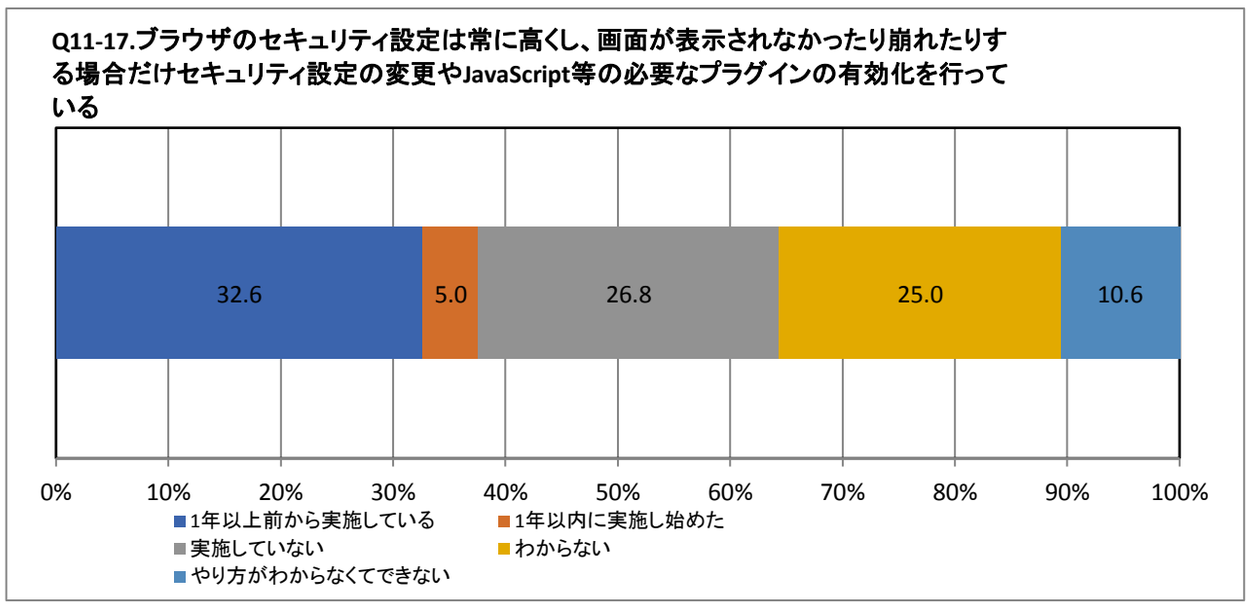
Q11-15.ウイルス対策ソフトのパターンファイルが最新になっていることを定期的に確認している	度数	%
1年以上前から実施している	2293	45.9
1年以内に実施し始めた	249	5.0
実施していない	1120	22.4
わからない	931	18.6
やり方がわからなくてできない	407	8.1
集計母数	5000	100.0



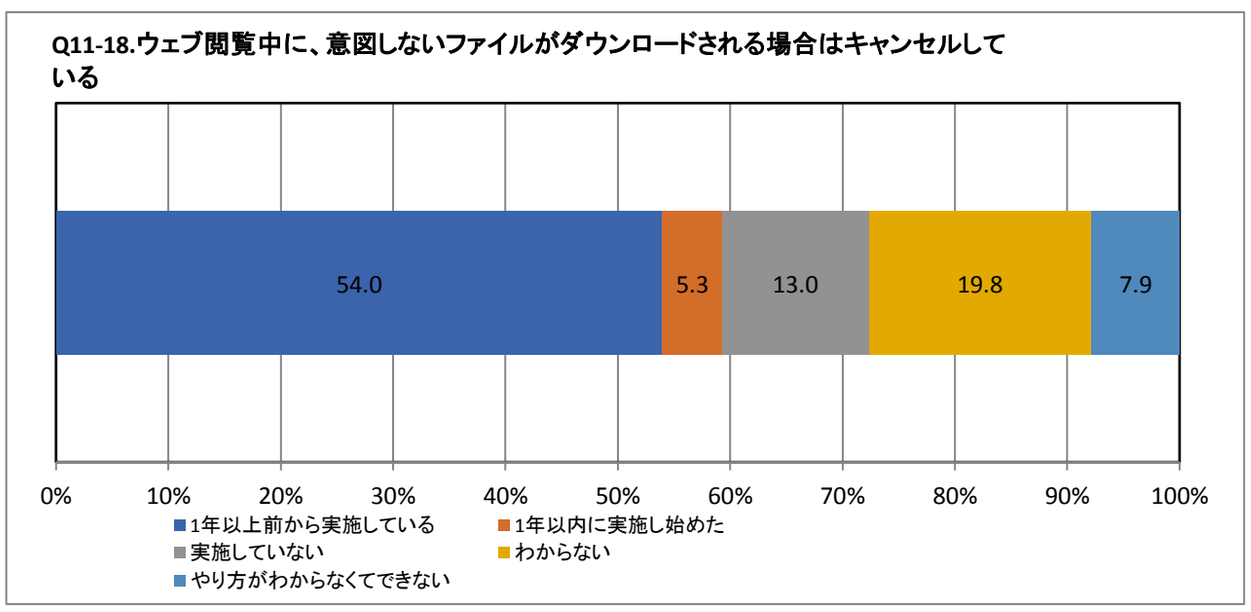
Q11-16.ウェブサイトに氏名や住所、クレジットカード番号などを入力する時は、使用しているソフトウェアの脆弱性をすべて解消した上で、自身で保存しているブックマークなど信頼できるリンクからアクセスする	度数	%
1年以上前から実施している	2040	40.8
1年以内に実施し始めた	256	5.1
実施していない	1165	23.3
わからない	1079	21.6
やり方がわからなくてできない	460	9.2
集計母数	5000	100.0



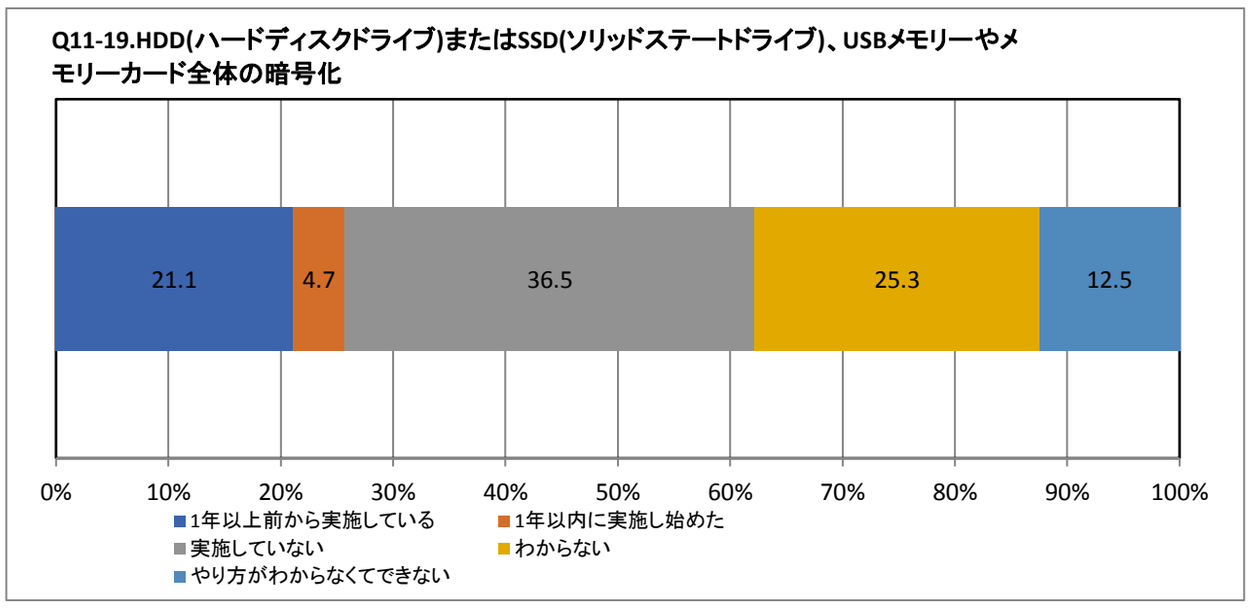
Q11-17.ブラウザのセキュリティ設定は常に高くし、画面が表示されなかったり崩れたりする場合だけセキュリティ設定の変更やJavaScript等の必要なプラグインの有効化を行っている	度数	%
1年以上前から実施している	1632	32.6
1年以内に実施し始めた	248	5.0
実施していない	1340	26.8
わからない	1252	25.0
やり方がわからなくてできない	528	10.6
集計母数	5000	100.0



Q11-18.ウェブ閲覧中に、意図しないファイルがダウンロードされる場合はキャンセルしている	度数	%
1年以上前から実施している	2698	54.0
1年以内に実施し始めた	267	5.3
実施していない	651	13.0
わからない	991	19.8
やり方がわからなくてできない	393	7.9
集計母数	5000	100.0



Q11-19.HDD(ハードディスクドライブ)またはSSD(ソリッドステートドライブ)、USBメモリーやメモリーカード全体の暗号化	度数	%
1年以上前から実施している	1053	21.1
1年以内に実施し始めた	233	4.7
実施していない	1825	36.5
わからない	1265	25.3
やり方がわからなくてできない	624	12.5
集計母数	5000	100.0



Q11-20.パスワード(知識情報)、指紋(生体情報)、ワンタイムパスワード(所有情報)などから2種類以上の要素を組み合わせた多要素認証の積極的な利用	度数	%
1年以上前から実施している	1804	36.1
1年以内に実施し始めた	377	7.5
実施していない	1352	27.0
わからない	972	19.4
やり方がわからなくてできない	495	9.9
集計母数	5000	100.0