KASPERSKY lab

あなたの「ネット常識力」はどのくらい?

リサーチサマリー

2015 年 9 月

目次

はじめに

インターネットの世界には、現実社会と同様に、危険な習慣もあれば安全な習慣もあります。たとえば、信号が青色のときに横断歩道を渡るのは安全ですが、歓楽街にあるバーの真ん中で大金を数えることは危険です。危険は物理的な世界だけではなく、オンラインにも潜んでいます。

残念なことに、誰もが安全なオンライン行動のルールを知っているわけではありません。潜在的なインターネット上の脅威を認識できないために、金銭および貴重品の損失やプライバシーの侵害など、現実社会と同様に不愉快な結果がもたらされる可能性があります。

このことを念頭に置いて、カスペルスキーはオンライン調査の形式でテストを実施し、18,000 名を超えるインターネットユーザーの「ネット常識力」を調査しました。世界 16 か国の 18 歳以上のインターネットユーザーです。このテストの目的は、回答者のオンライン習慣を知り、サイバーセキュリティについて正しい判断を下せるかどうか、脅威に直面したときにそれを認識できるかどうかを把握することにありました。

図 1:調査対象となった国とユーザー数

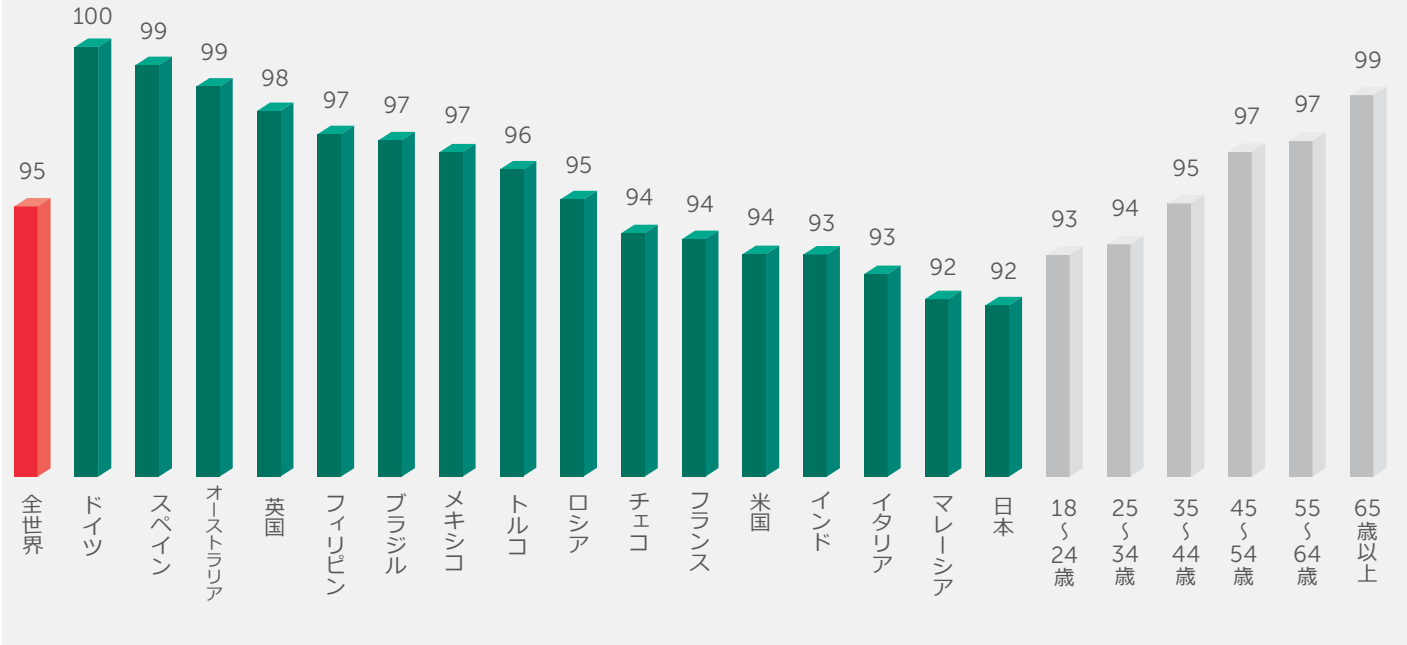
回答者は、Web サイトの閲覧やファイルのダウンロード時、SNS の利用中にインターネットで発生することの多い、危険に繋がる可能性のある状況について回答を求められました（本レポートでは、取り上げられた 8 つの状況すべてについて解説します）。

想定された各状況には複数の回答選択肢が設定されています。各回答には、一定のスコアが与えられました。選択した内容が安全であるほどスコアは高くなり、危険であるほど低くなります。ユーザーが得られる最高スコアは 150 点でした。

テスト終了後に、ユーザーには最終的なスコアと、現在の行動を続けた場合に直面する可能性のある危険のレベルが通知されました。最終スコアは、Kaspersky Lab がサイバー脅威と闘ってきた経験に基づいて、以下のとおりに分類されました。

- 137 点以上 - リスクレベルがもっとも低い、素晴らしい結果。ユーザーは安全なインターネット行動のルールを理解しており、適切な判断をしています。
- 113～137 点 - 良い結果。ユーザーはインターネット上でいくつかの危険な間違いをしていますが、全体的には注意深く安全な行動を取っています。
- 75～113 点 - 平均的なリスクレベル。ユーザーは直面するサイバー脅威の半分しか識別できていないため、リスクレベルは高いと言えます。
- 75 点未満 - 非常に危険なオンライン行動。ユーザーはサイバー脅威を認識できておらず、自分自身やデータを脅威から守ることができません。また、この問題を重視していません。

図 2:国および年齢別の平均スコア分布



また、属性（生年、性別、インターネットアクセスによく利用するデバイスなど）と回答を関連づけて観察する目的で、社会人口統計学的な質問もいくつか設けられました。

主な調査結果:

多数のユーザーが、サイバー脅威を識別できませんでした。

- 偽の Web ページを選ぶことなく、正規の Web ページを識別できたユーザーは、わずか **24** % でした。
- **34** % のユーザーが、オーディオファイルの代わりに拡張子.exeの付いたファイル(おそらくは悪意のあるプログラム)をダウンロードしようとしました。

自身を保護できていないユーザーも確認されました。

- パスワードを作るとき、より難しい新たなパスワードを考え出したのは、**38** % のユーザーにすぎず、回答者の **14** % は常に同じパスワードを使用しています。
- 回答者の **35** % が、使用可能なアプリのすべてでプライベートなやり取りを続けており、**13** % は、これを使用できるすべてのデバイスで実行していました。
- ソフトウェアをインストールする前に、ライセンス契約を注意深く読んでいたのはわずか **37** % のユーザーにすぎず、回答者の **9** % は一度も読んでいませんでした。

セキュリティについて過信するユーザーもいました。

- 回答者の **29** % が、大手企業の Web サイトは適切に保護されているためオンラインショッピングに対する安全対策は必要ない、と考えています。
- **12** % のユーザーは、SNS で進んで無差別に友達を追加しており、**26** % の回答者は友達から受け取ったリンクを疑うことなくクリックします。
- アンチウイルス製品によってプログラムのインストールが妨げられる場合、回答者の **19** % はアンチウイルス製品を無効化すると回答しました。

凡例)レポート中の図(図 1、2 以外の棒グラフ)については、特に但し書きのないかぎり、以下のように色分けされています。

- 緑 – 適切な判断と見なすことができる選択肢
- 赤 – 適切ではなく、危険にさらされる可能性のある選択肢

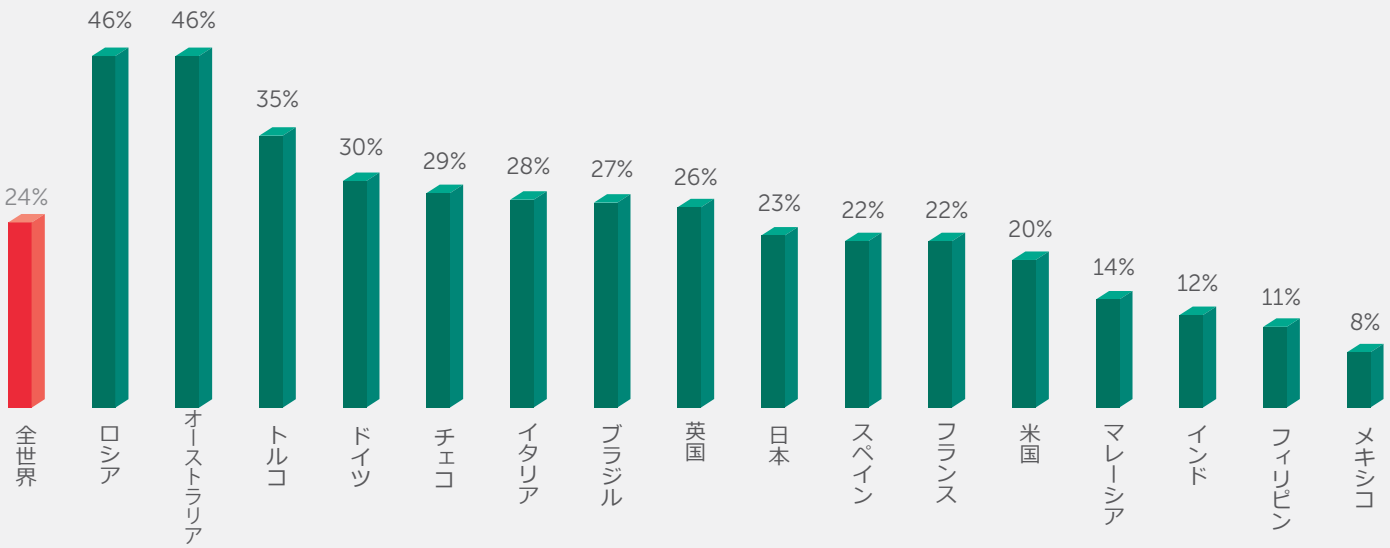
セクション 1:安全な WEB サイト閲覧

Web サイト閲覧は、ユーザーがインターネット上で行う主な活動の 1 つです。サイバー犯罪の犠牲者とならないためには、安全なページおよびファイルのみを開くようにする必要があります。

ユーザーが偽のページと本物のページを区別できるかどうかを確認するため、個人情報を入力して差し支えないと思われる Web ページを 4 つのうちから 1 つ選んでもらいました。国ごとに専用のサンプルが用意され（付録 1 を参照）、回答者は複数のページを選択できました。しかし、実は 4 つのページのうち 3 つは、Kaspersky Lab のエキスパートがインターネット上で発見したフィッシングページでした。

フィッシングページを選ぶことなく、本物のページのみを認識できたのは、わずか 24 % のユーザーでした。つまり、残りのページが危険であると判断できたインターネットユーザーは、4 人に 1 人だけでした。さらに、データを入力しても問題ない Web ページを指定する際、偽のサイトだけを挙げたユーザーは 58 % もいました。

図 3:本物のページのみを選択した回答者の割合

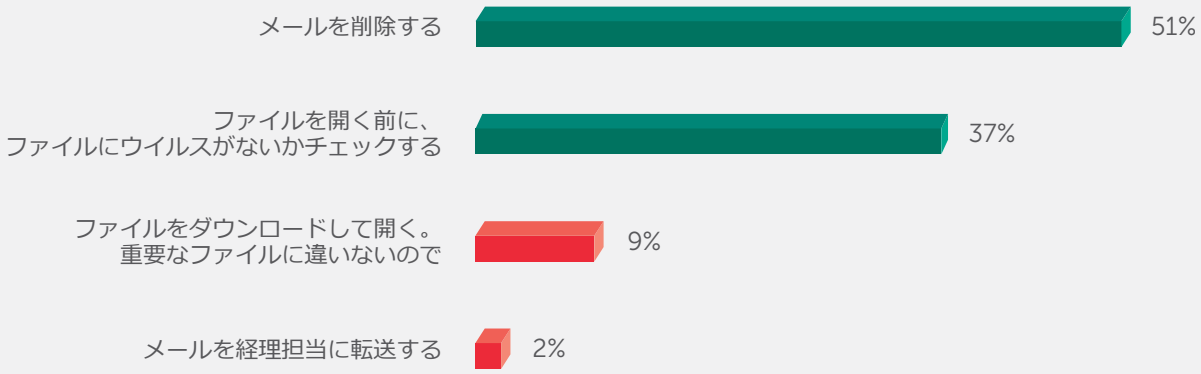


注意すべきは、フィッシングのサンプルがいずれも見分けやすいものだったという点です。アドレスバーには、標準のアドレスとは大きく異なるアドレスが表示されていました。これは、偽のページを見分ける上で一番わかりやすいサインです。しかし、Web ページのサンプルが表示されたとき、大半のユーザーは直感的にアドレスを見なかったと考えられます。

回答者に対する 2 番目のタスクは、「未払いの罰金に関する情報」という Word 文書が添付された「税務署」からのメールを受け取った場合の対処法を選ぶことです。このようなぎょっとするメールや注意を引くメールには、.txtなどの一般的で無害な形式のもとにマルウェアが隠されていることが多くあります。

大半のユーザーはこの策略には引っ掛かりませんでした。回答者の 89 % がメールを削除するか、または保護製品を使って添付ファイルをチェックするという正しい選択をしました。その一方で、**回答者の 9 % がチェックなしで添付ファイルを開き、さらに少数（2 %）は経理担当にファイルを転送**するという、感染範囲を拡大しかねない行動をとると回答しました。興味深いことに、これらの数字は若年ユーザー（18～24 歳）で若干高くなっていました（それぞれ 12 % と 3 %）。

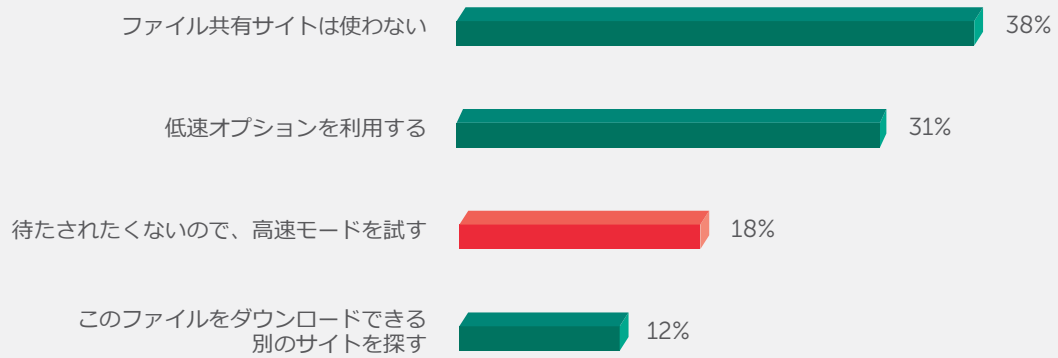
図 4:フィッシングメールに対する処理の選択肢



3 番目の状況は、ファイル共有サービスに関連するものでした。このサイトでは、ファイルをアップロードおよびダウンロードできます。多くのファイル共有サービスでは、必要なファイルを低速でダウンロードするか、または高速ダウンロードモードを選択するかという選択肢が提供されています。2番目の選択肢を選ぶと、広告リンクをクリックするか、または電話番号を入力するなどのアクションを実行するよう要求されます。こうしたアクションには、デバイスの感染や機密データの損失を招くリスクが付随します。

およそ 5 人に 1 人(18 %)の回答者が、危険を伴う高速ダウンロードを選びました。もっとも多かったのは24 歳未満の若年層であり、22 % がこの選択肢を選びました。

図 5:ファイル共有サービスからファイルをダウンロードするときの処理の選択肢



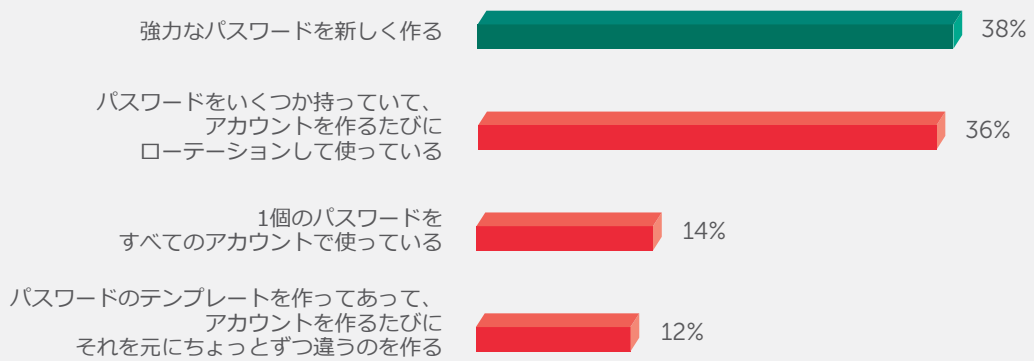
このセクションで見る限り、メールとファイルのダウンロードに対する対応では高いレベルのネット常識力があることが示されています。しかし、フィッシング Web ページと本物のページを見分ける能力に関する平均的なユーザーの対応は、良いとは言いがたいものがあります。犠牲者にならないためには、直感を鍛える必要があります。そうでない限り、ソーシャルエンジニアリングに対する耐性の欠如に詐欺師がつけ込む隙が残ります。インターネット上で行う活動の種類が増え続けるにつれ、伝統的な領域を逸脱することが増え、安全に関する直感が役に立たないことがますます多くなるでしょう。

セクション 2:デジタル ID の保護

現実社会と同様に、インターネット上でも常にユーザーは自分自身である必要があります。つまり、仮想の「自分」を保護し、メール、IM、SNS などの各種サービス用の認証情報が、別人によって使用されることのないようにする必要があります。

テスト結果によると、新規アカウントに対してパスワードを選択するとき、**より複雑な組み合わせを持つ新しいパスワードを考え出したのは、回答者の 38 %** にすぎませんでした。その一方で、回答者の 36 % は限られた数のパスワードを使用しており、12 % は同じパスワードパターンの変形を使って新しいパスワードを作成していましたが、**14 % のユーザーは常に 1 つのパスワードを使っていると回答**しました。したがって、62 % の回答者は、1 つのパスワード漏えいが複数アカウントのクラッキングにつながるリスクにさらされています。

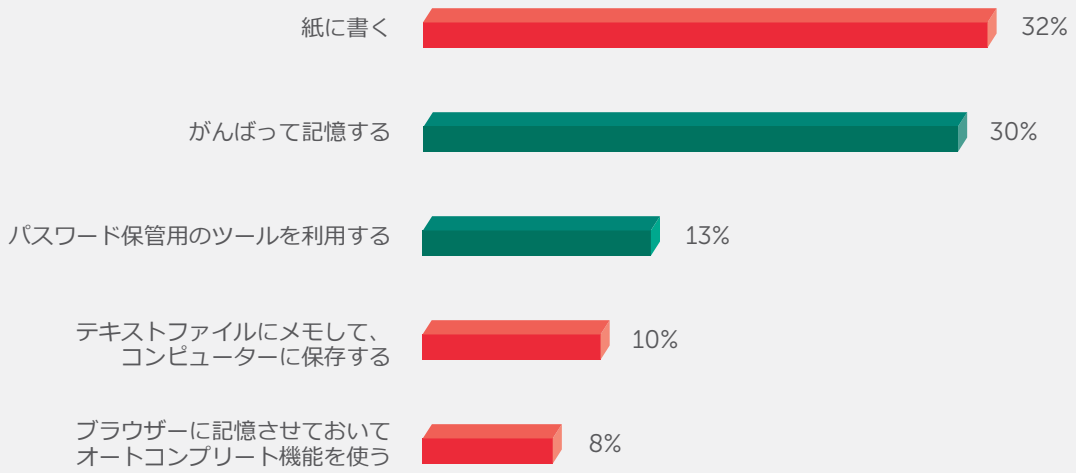
図 6:新規アカウントに対するパスワード作成方法



興味深いのは、回答者の年齢が上がるほど複雑な新規パスワードを作成する意欲が高まることです。より複雑なパスワードの作成をいとわない回答者は、若年層ではわずか 1/3 ですが、年配のユーザーでは半分を超えています。

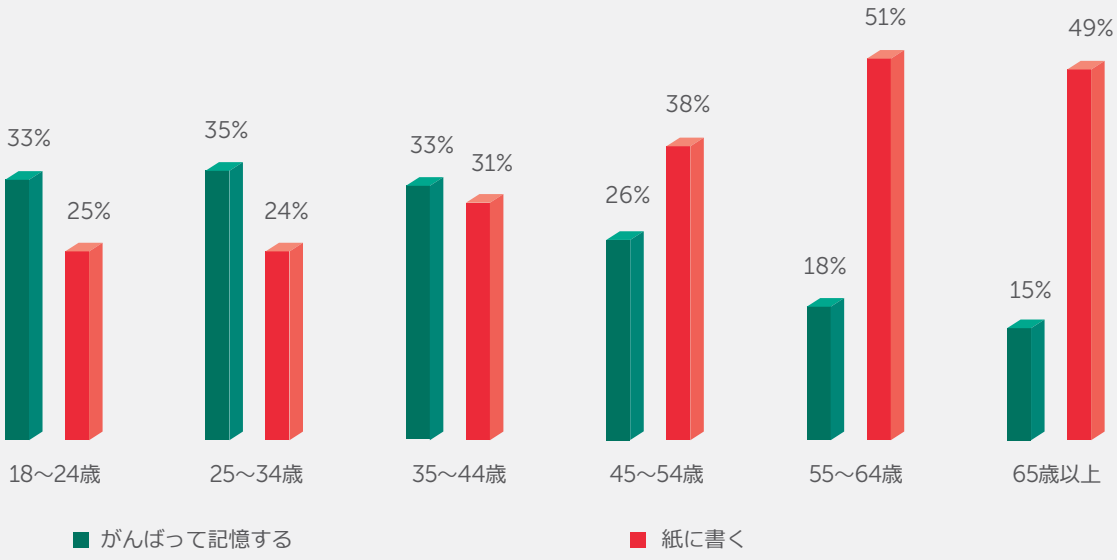
また、**57 % の回答者が安全でないパスワードの保存方法を選択**しており、紙に書いたり、ブラウザーや携帯電話に保存したりすることで、パスワードを危険にさらしています。

図 7:パスワードの保存方法



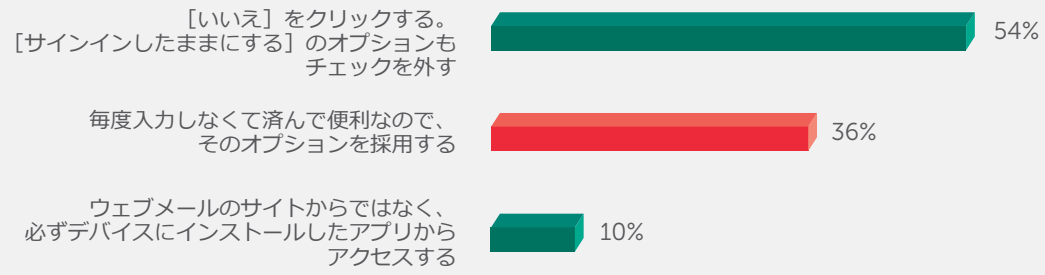
年配のユーザーは複雑なパスワードを作成する傾向にありますが、記憶しようとするユーザーは少なく、しばしば、もっとも簡単かつ危険な保存方法を選択します。

図 8:年代別のパスワード保存方法



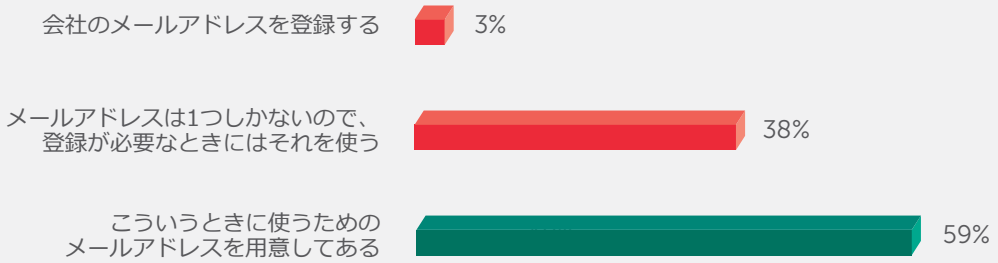
ブラウザーにログインとパスワードの保存オプションがある場合、36 % がこれを使用しており、サイバー犯罪者や卑劣な人物に付け入る隙を与え、デバイスへのアクセスを許す状況となっています。

図 9:ブラウザーに対する自動アカウント指定の選択



38 % の回答者が常に同じメールアドレスを使用しています。今回のテストの設問にあったような1度限りの宅配を注文する場合にも同じアドレスを使う、ということでもあります。回答者の大半（59 %）は、このような場合のために専用アドレスを作成して、自身を保護していますが、3 % のユーザーはこの目的のために会社のメールアドレスを指定しても構わないと考えています。

図 10:一時的な登録用に指定するメールアドレス



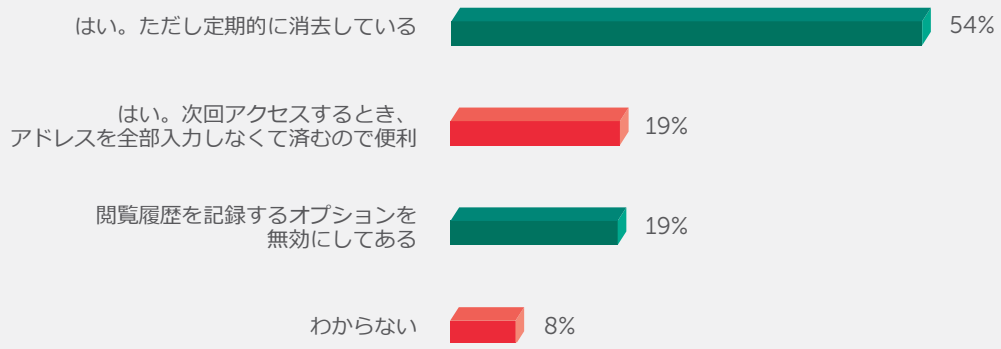
今回のテストは、多くのインターネットユーザーが、不正なアクセスからアカウントを効果的に保護していないことを示しています。複雑なパスワードを選択し、信頼性の高い方法で保存することは、高いネット常識力を持つユーザー自身とその友人のセキュリティを強化するのに貢献します。盗まれたプロファイルは、個人の追跡やデータの窃盗に悪用されたり、スパムや悪意あるファイルの送信に利用される可能性があります。

セクション 3:プライバシーの保護

インターネットが発展したことで、プライバシー保護の概念が及ぶ範囲が広がっています。現在、ユーザーが何をしているのか、何に興味を持っているのか、誰とどんなコミュニケーションを取っているのかなど、インターネットユーザーの私生活がデジタルテクノロジーに委ねられています。プライバシーの保護能力は、すべてのインターネットユーザーが習得すべき大切なスキルです。

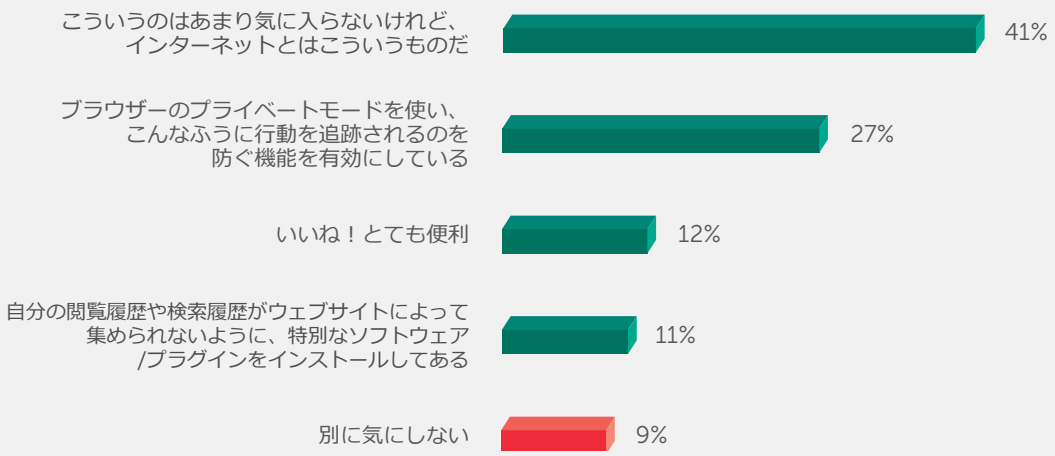
たとえば、**回答者の 8 % は Web ページの閲覧履歴がブラウザーに保存されることすら把握していません**。この情報はユーザーに対するスパイ行為に使用できます。

図 11:ブラウザーの履歴の保存



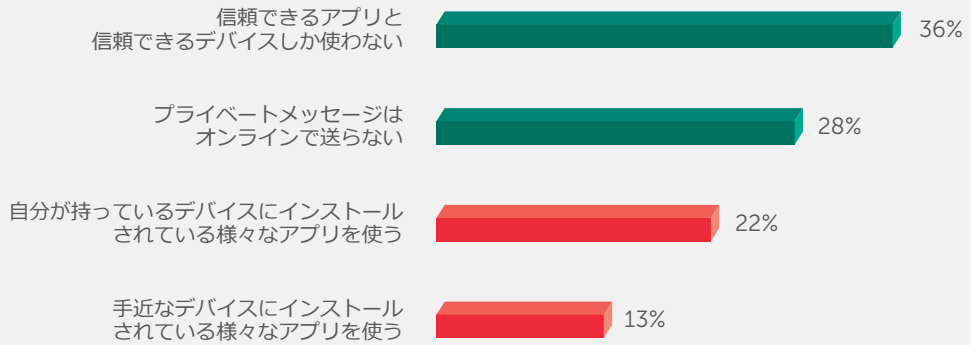
また、今回のテストから、訪問したサイトが自動的に自分の場所を特定するだけでなく、訪問サイトや検索エンジンで検索した単語に基づいて広告が表示されるとは考えもしなかったユーザーが 9 % いることが分かりました。12 % の回答者がこの方法を便利だと感じる一方で、**41 % は納得していないものの、「これがインターネットというもの」だとして、プライバシーを保護するための対策を取っていません**。

図 12:Web サイトによる追跡に対するユーザーの受け止め方



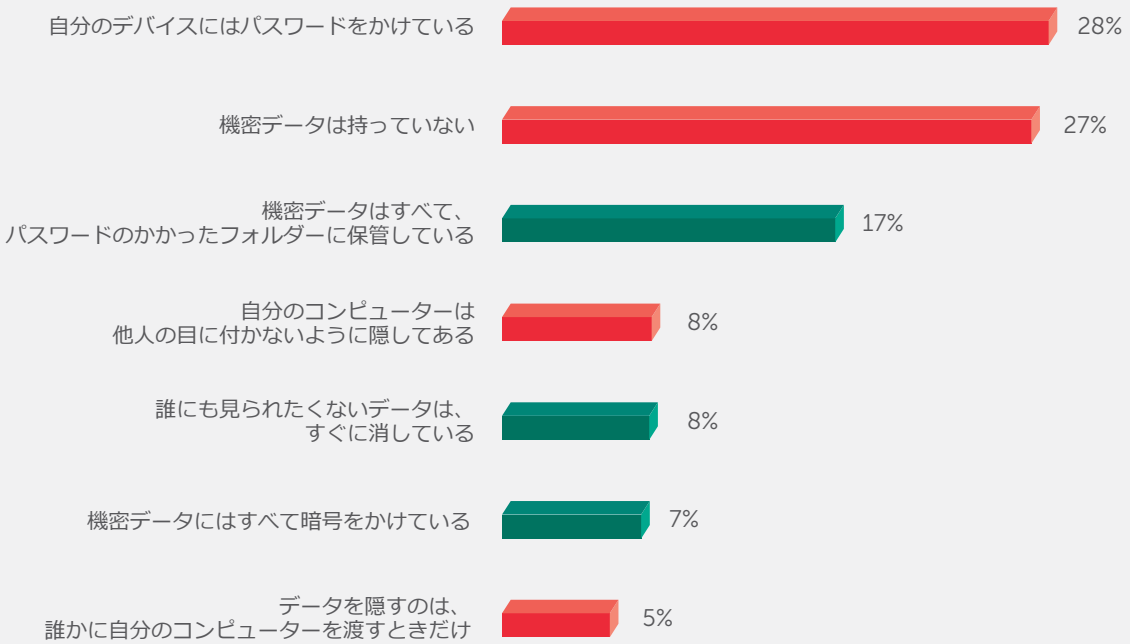
回答者の 35 % が、使用可能なアプリのすべてでプライベートなやり取りを行っており、13 % は個人用デバイスだけでなく、使用できるすべてのデバイスで実行していました。これらの通信チャネルは傍受に対して脆弱である可能性があると認識しており、オンラインで個人的な話はしない、というユーザーは 1/3 を下回りました(28 %)。

図 13:プライベートなやり取りに使用するアプリケーション



インターネットを利用する人は皆、オンライン活動の履歴や個人的な連絡先、ファイル、パスワードなど、自分自身に関する機密情報を保持しています。これらのデータすべてを、他人やサイバー犯罪者による潜在的なアクセスからさらに保護する必要があります。しかし、**27 % のユーザーは、コンピューター上に機密情報は保持していないと考えています**。

図 14:質問「他人に知られたくない情報をコンピューター上でどのように保存していますか?」に対する回答



残念ながら、デバイスをパスワードで保護したり(28 % が選択)、デバイスを他人から隠したり(8 %)しても、Wi-Fi トラフィックの傍受やマルウェアの導入などのテクニックを使った侵入からデータを保護することはできません。より信頼性の高い方法には、他人に見られたくないデータはすべて削除する(8%)、パスワードで保護したフォルダ(17 %)または暗号化フォルダ(7 %)を作成する、があります。

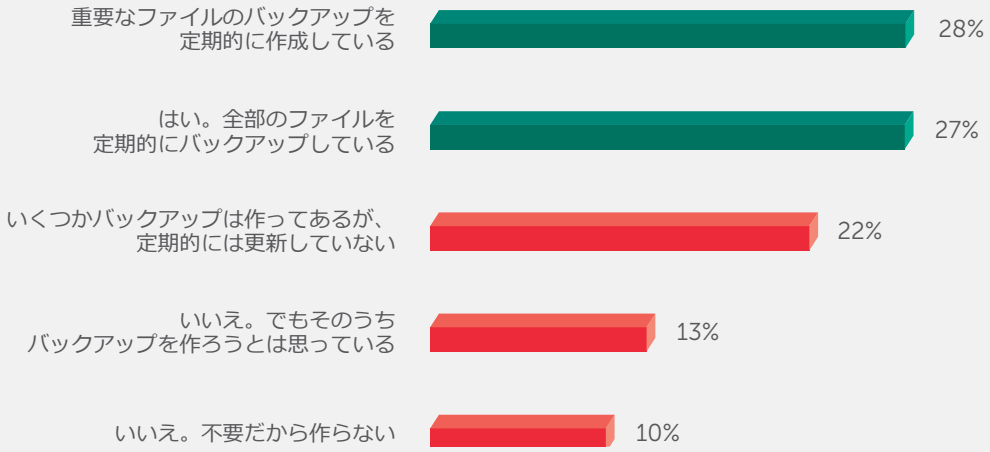
私たちは皆、インターネット上に自分の影を映しています。この影には、オンラインの認証情報、アカウント、ログインとパスワードだけでなく、私たちがどこにいて、誰で、何を行い、誰とどのようなコミュニケーションを取ったかが含まれています。インターネットユーザーは、このようなデータが存在することを全体としては理解していますが、広告主や犯罪者などの第三者にとっての価値を過小評価する傾向にあります。ネット常識力と専門ツールを使って、インターネット上の影を保護する方法を学習することが非常に重要です。これはすべてのインターネットユーザーが習得すべきスキルであるにもかかわらず、現時点でのレベルは極めて低いままです。

セクション 4:データ保護

現在、これまでになく大量のデジタルコンテンツが作り出されています。インターネットには、毎分数テラバイトのデータが新しく追加されています。インターネットユーザーのデバイスには、さまざまな種類の写真、文書、メモ書き、ビデオ、オーディオファイルが保存されています。しかし、不安定なデジタル空間では、デバイスが故障したり、サイバー犯罪者が身代金目当てでファイルを暗号化したり、後から使用するためにファイルを盗んだりします。これらの脅威に対抗するため、インターネットユーザーにはある程度の保護スキルが必要になります。

デバイスを紛失した場合に備えてファイルをバックアップしているかどうかを、回答者に質問しました。この調査によると、**23 % のユーザーがバックアップコピーをまったく作成しておらず、回答者の 10 人に 1 人はバックアップが必要だとも思っていません**。

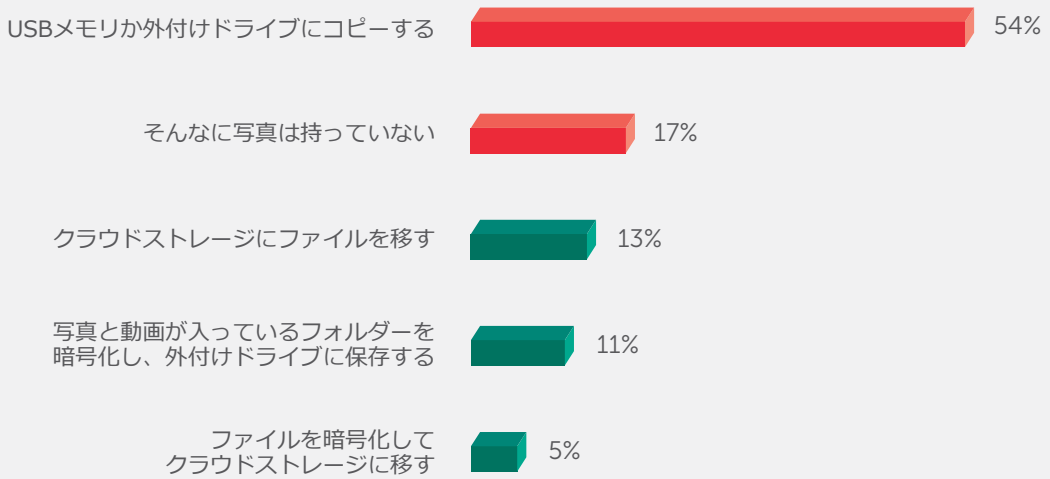
図 15:バックアップコピーの作成



仮に、写真やビデオを保存するための容量がデバイス上に不足している場合、**半分のユーザー(54 %)が外部メディアにコピーを取る**ことを選びます。しかし、外付けドライブは紛失や破損の可能性が高いため、この方法がもっとも信頼性が高いとは決して言えません。ディスクを紛失した場合、データが不適切な人間の手に渡るおそれがあります。これを避けるため、11 % の回答者はディスクにコピーする前にデータを暗号化しています。

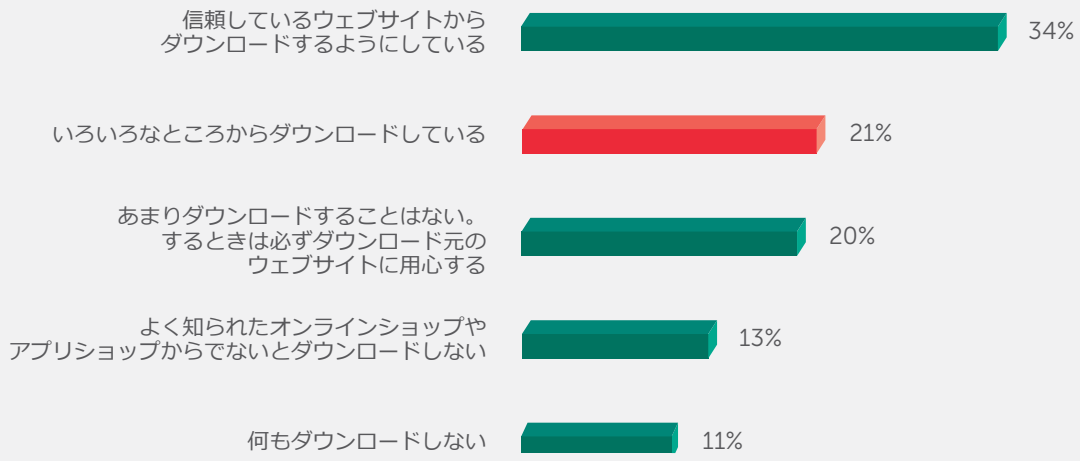
17 % のユーザーはほとんど写真を持っていないため、バックアップは不要であると考えています。しかし、写真を保存しているデバイスも外付けドライブと同様に脆弱です。このケースでの最善の解決策は、クラウドにバックアップコピーを取ることです。クラウドサービスは通常、信頼性の高いストレージシステムを装備しています。ただし、クラウドサービスによっては、データを暗号化した方が良い場合があります。この選択肢を選んだのは、回答者の 5 % にすぎませんでした。

図 16:多数の写真およびビデオファイルに関する問題の解決策



プログラム、映画、書籍、ゲームなどのファイルをダウンロードするために使用するサイトを問う質問もありました。**5 人に 1 人のユーザー(21 %)はさまざまなサイトからファイルをダウンロードしており、良心的でないサプライヤーに遭遇する危険があります**。

図 17:ファイルをダウンロードするサイト



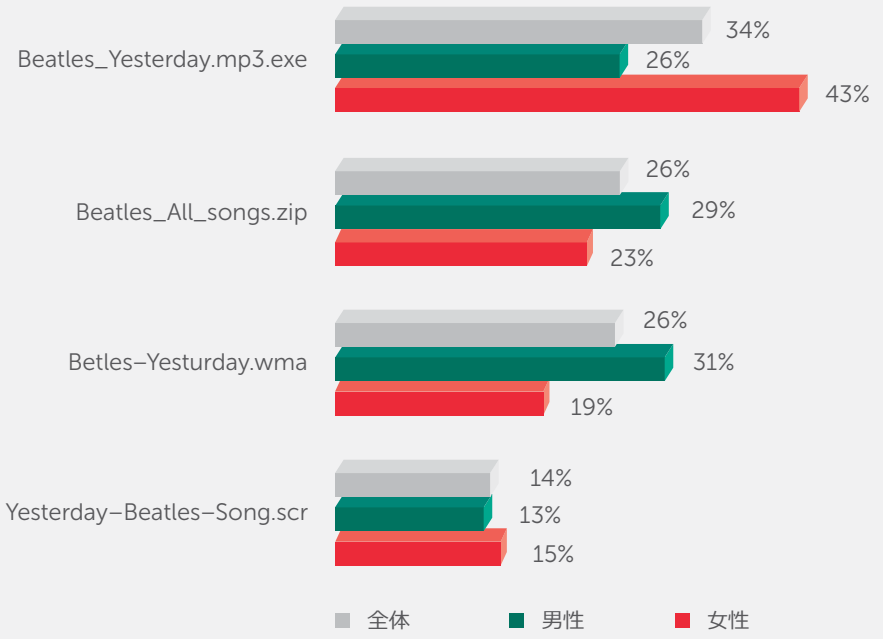
面白いことに、女性よりも男性の方がより頻繁にバックアップコピーを取り、信頼できる保存方法を選んでいます。その一方で、男性はファイルをダウンロードするサイトにはあまり注意を払っていません(男性 25 %、女性 17 %)。また、回答者が若いほど、サイトを選ぶことなくファイルをダウンロードする傾向があります(24歳未満 31 %、65歳以上 6 %)。

回答者はまた、インターネット上にあるとされるビートルズの楽曲「Yesterday」のいずれかのバージョンを、各自のデバイスにダウンロードする場合について質問を受けました。安全な拡張子が付いていたのは 4 つのファイルのうち 1 つだけであり、残り 3 つのファイルには有名な歌の代わりに危険なコンテンツが隠されている可能性がありました。このタスクの目的は、安全なファイルを見つけて、詐欺師かもしれない人物による策略を回避することでした。この質問は引っかけ問題で、唯一の安全なファイルに誤植があり、もっとも危険なファイルの名前には有名な拡張子 .mp3 が含まれていました。

その結果、拡張子 .wma（Windows Media）の付いた正しいファイルを選んだのは、わずか 26 % の参加者でした。別の 26 % はアーカイブされたzipフォルダを選びましたが、これにはオーディオデータ以外に好ましくない要素が含まれる可能性があります。14 % の回答者は拡張子 .scr の付いたファイル（オーディオデータではなくスクリーンセーバー）を選びました。これは、サイバー犯罪者が悪意のあるソフトウェアをユーザーのデバイスに送り込むために使用するファイル形式の1つです。

もっとも危険なのは、**多数（34 %）の回答者が音楽ではなく、拡張子 .exe の付いたファイルをダウンロードしようとしたことです。この実行可能ファイルは、ほぼ確実に危険なプログラムです**。この選択肢を選択したのは、主に女性でした。拡張子.scrと.exeは年配の回答者によって選ばれ、zipおよびwmaファイルは若い回答者によって選ばれる傾向にありました。

図 18:ダウンロードする楽曲の選択肢



デジタルストレージにまったく注意を払わない特徴的なユーザーも目立ちますが、回答者の大半は、デジタルストレージメディアの信頼性が高くないことを理解しており、少なくとも、もっとも重要なファイルをときどきバックアップする必要があることに気付いています。しかし、調査に使用した、ファイルをダウンロードする機会を与えられたシナリオでは、サイバー脅威に対するユーザーの認識が低いことが示されています。これは、デジタル情報を失うリスクが大きいことを意味します。

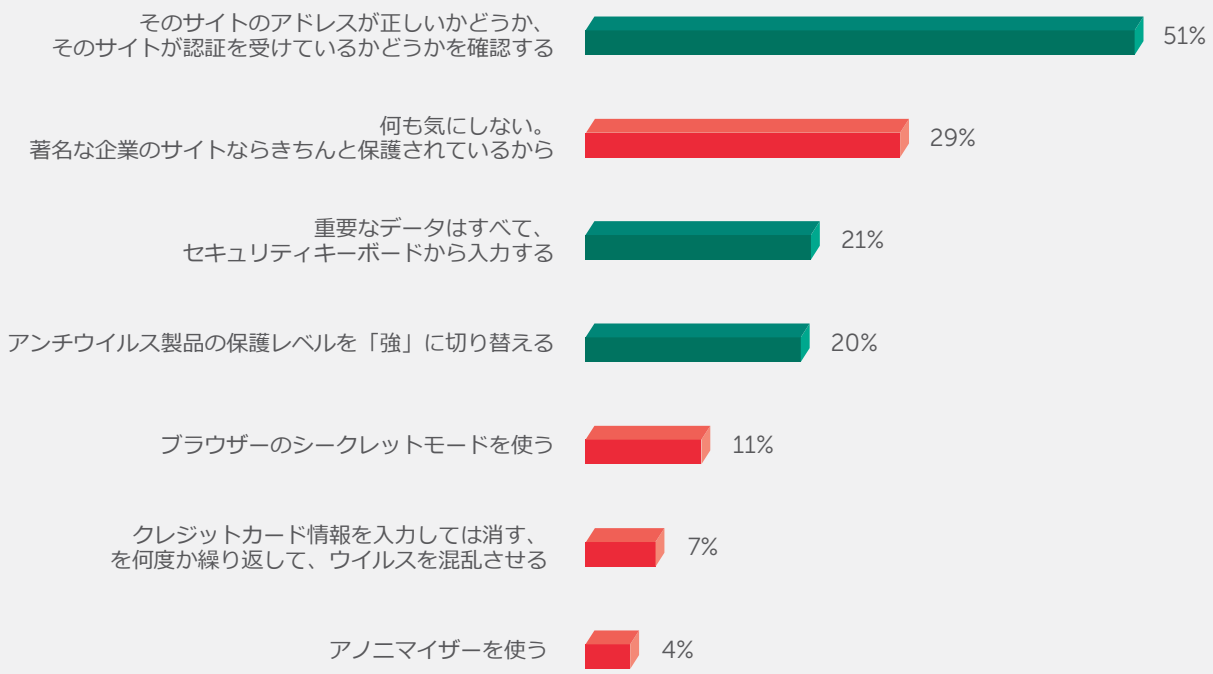
セクション 5:金銭の保護

テストの結果によると、**大半の回答者(86 %)が時折、インターネット上のオンラインショッピングで商品やサービスを購入**しています。その一方で、デジタルテクノロジーを使った金銭の盗難は、もはや SF 映画での出来事ではなく厳しい現実となっています。詐欺師から銀行口座を守るためには、金融取引の実行に安全なソリューションを使用するだけでなく、潜在的な脅威を識別できる必要があります。

この 86 % の回答者は、オンラインショッピング中にクレジットカードデータを入力する際どのような安全策をとるかたずねられ、複数回答が可能でした。回答者の半数(51 %)は念入りにサイトをチェックすると回答していますが、これは正しい選択です。セキュリティキーボードを使ってデータを入力すると回答した回答者はわずか 21 % でしたが、この方法では、コンピューターが感染している場合に特殊なマルウェアによって入力情報が傍受されるのを防ぐことができます。別の 20 % のユーザーは、セキュリティソリューションによる保護が有効化されていることを確認すると回答しました。

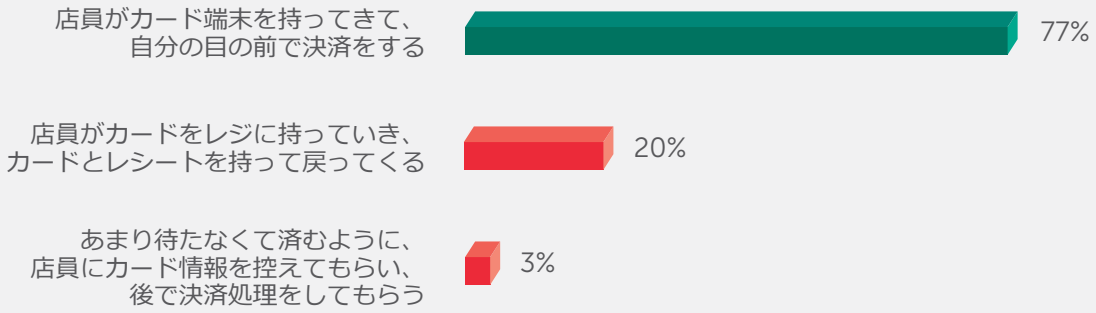
回答者の 29 % は、大手企業の Web サイトは適切に保護されているため、電子決済に対する安全対策は必要ないと考えています。しかし、サイトが保護されていても、セキュリティ侵害のあったデバイス上でデータが傍受されないとは限りません。11 % のユーザーがブラウザーの「匿名」モードを使用すると回答し、4 % の回答者がアノニマイザーを使用すると回答していますが、これらの対策を取っても傍受やマルウェアから金銭データを保護することはできません。7 % の回答者は、番号を複数回入力することでウイルスを混乱させるという、ユーモアのある回答を選びました。

図 19:オンラインショッピングで用いる安全対策



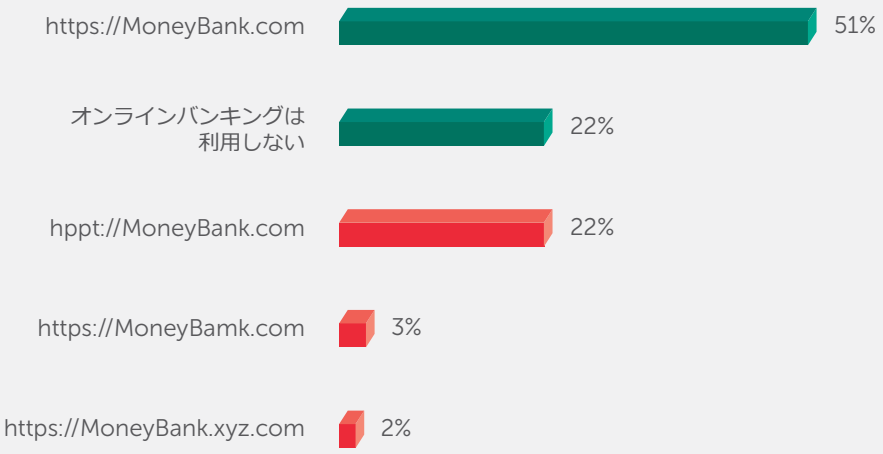
もう 1 つのよくある金銭詐欺の手法は、クレジットカードの違法コピーです。幸い、カフェでクレジットカードを使って支払いをするという仮の状況で、大半のユーザー(77 %)はクレジットカードが見える範囲にとどまることを選びました。ウエーターやウエートレスがレジまでカードを持っていくよりも、目の前で取引を処理できるように、クレジットカード端末を運んでくれることを求めています。しかし、20 % の回答者はこのようなシナリオを嫌がっておらず、3 % のユーザーはウエーターやウエートレスが金融データのコピーを取ることを了承すると回答しました。

図 20:カフェでのクレジットカードによる望ましい支払方法



この設問では、Money Bank という架空の銀行のサイトにデータを入力するために、適切な Web ページを選ぶように要求されました。正しいアドレスと必要な暗号化（http ではなく https で始まる）が指定されたもっとも安全な選択肢は、51 % の回答者によって選ばれました。しかし、**5 人に 1 人の回答者（22 %）が選んだページではトラフィックが暗号化されない**ため、傍受に対する脆弱性が潜在します。また、5 % の回答者は誤ったアドレスを持つ偽のページを選びました。

図 21:架空の銀行ページの選択肢



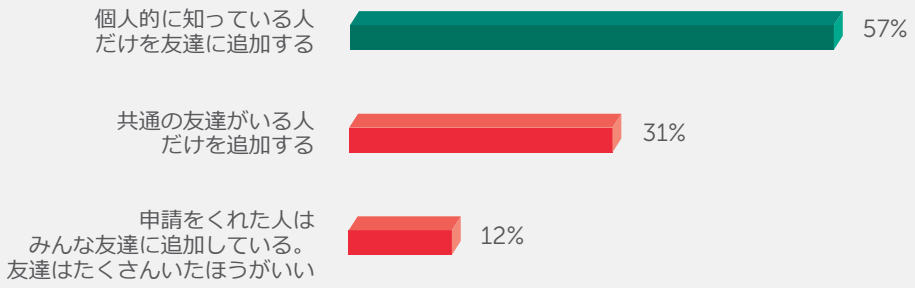
オンラインバンキングやオンラインでの買い物および金融取引は、多くの人にとって日常生活の一部となっており、このために注意が不十分になっています。私たちは大通りにある店舗を信頼するのと同じように Web サイトを信頼していますが、この信頼は他者によって悪用される可能性があります。私たちの大半は見たいものを見る傾向にあり、自分が標的となることなどなく、仮にそうなったとしても誰かが支払ってくれるだろうと考えています。
今回の結果が示すように、かなりの割合のユーザーが必要以上にインターネットを信頼しています。金融取引をしても安全なサイトを選ぶ能力や意志がないか、または効果的な保護ツールを使う準備ができていない場合、サイバー犯罪者の標的となる可能性があります。

セクション 6:SNS 活動

現代のソーシャルネットワーク(SNS)は、エンターテインメントや Web サイト閲覧を超える存在です。SNS 上のページはインターネット上の個人を公式に代表する存在であり、非常に多くの個人情報を含んでいます。**今回のテスト『あなたの「ネット常識力」はどのくらい?』の回答者のうち、78 % が SNS を使用しています。**ただし、SNS は人々を結びつけたり、情報を知らせたりするだけではなく、サイバー犯罪者にとっての便利なツールにもなります。

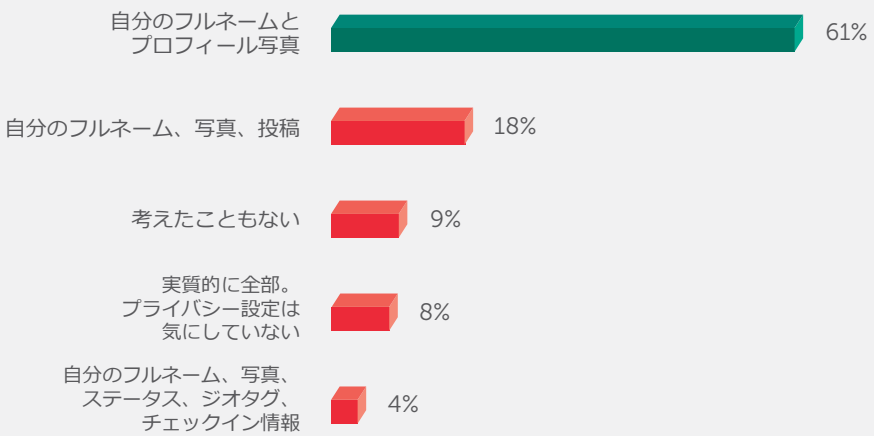
たとえば、**SNS に個人ページを持つ回答者のうちの 12 % が、ほとんど誰でも友達として追加すると回答し、31 % の回答者が共通の友達がいれば見知らぬ人でも友達として追加する**と回答しました。これらの共通の友達も、赤の他人からの招待を承認しているかもしれません。半分をわずかに上回るユーザー(57 %)が、友達として追加する相手に十分な注意を払っています。年代別に見ると、この割合は若年層の回答者では 52 % になり、年配の回答者では 77 % に上昇します。

図 22:SNS での友達の追加



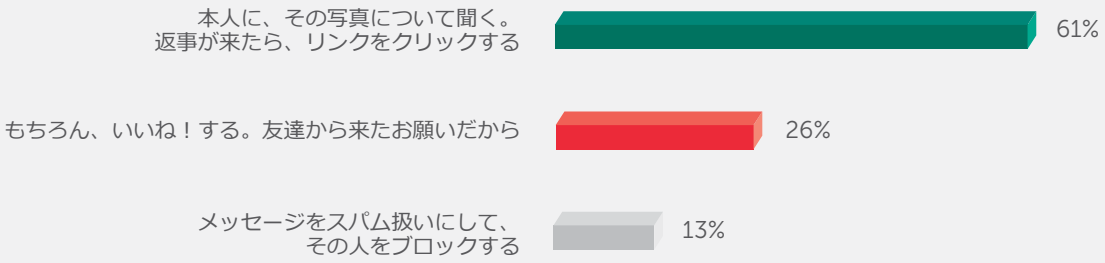
用心深いユーザーとほぼ同数のユーザー(61 %)が、名前とプロフィール写真のみを一般公開しています。**ページ所有者の 30 % は、自分の投稿や居場所などの私生活に関する情報を全員に公開しています。**さらに、9 % の回答者は他人がページ上の何を見るかについて考えてもいません。この選択肢を選んだ年配のユーザーの割合は 14 % に上ります。

図 23:SNS 上で公開している情報



写真を見るように依頼する友人からのリンクを受け取ったとき、4 人に 1 人の回答者（26 %）がまったく疑うことなくリンクをクリックします。したがって、友達のページのセキュリティが侵害されている場合、この 26 % のユーザーが悪意のあるリンクをクリックすると、おそらくはデバイスが感染することになります。スパムでないことを確認するのは回答者の 61 % のみですが、13 % の回答者は問題を根本的に解決するべくこの友人をブロックすると回答しました。

図 24:SNS 上の友達からリンクのクリックと写真のいいね!を依頼された場合の対応



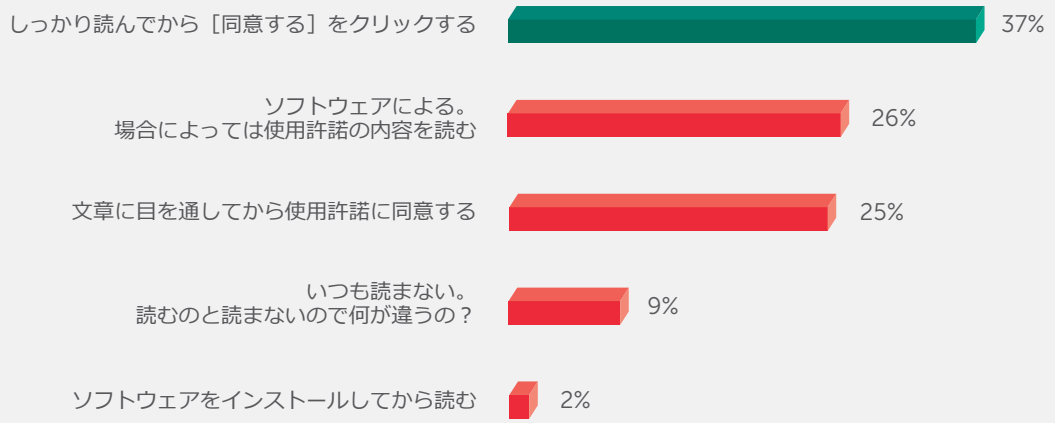
SNS は、私たちの個人情報が残る場所であり、インターネット上に投影される自分の影でもあります。ページがクラッキングされると、ページ所有者の代わりにサイバー犯罪者は広告を表示したり、その人の友達に悪意のあるリンクを送ったり、その人の個人情報を悪用したりすることができます。SNS のユーザーはこれに備えて、いくつかの簡単なルール、たとえば、次々と友達を追加しない、個人情報を過度に公開しない、友達から受け取ったリンクをすべてクリックしない、に従う必要があります。

セクション 7:ソフトウェア／アプリの使用

隠れたマルウェアではないソフトウェアが問題を引き起こす場合があります。比較的正当なソフトウェアであっても、所有者の情報を収集したり、ユーザーに気づかれることなく設定を変更したり、予想外の広告を表示したりする場合もあります。しかし、デバイスにソフトウェアをインストールするときに十分な注意を払っていれば、このようなことが行われる可能性を低減することができます。

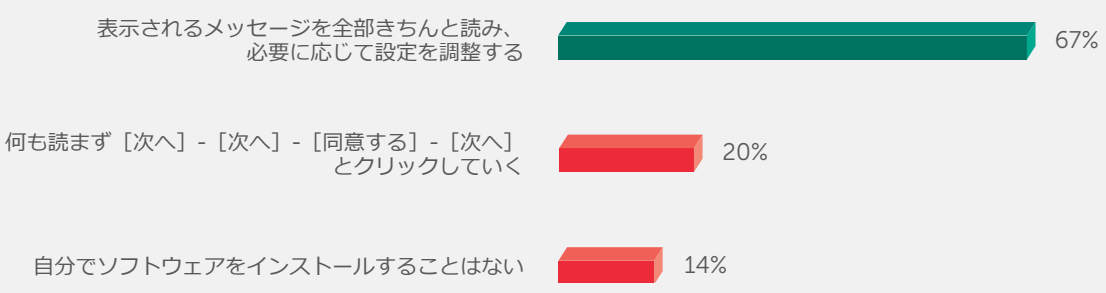
たとえば、**ソフトウェアをインストールする前に入念にライセンス契約を読むユーザーは、わずか 37 % です**。10 人に 1 人の回答者（9 %）は意味がないとして、ライセンス契約を一度も読んでいません。回答者が若いほど、ライセンス契約を読む割合が下がり、同意する割合は高くなります。

図 25:ライセンス契約の閲覧



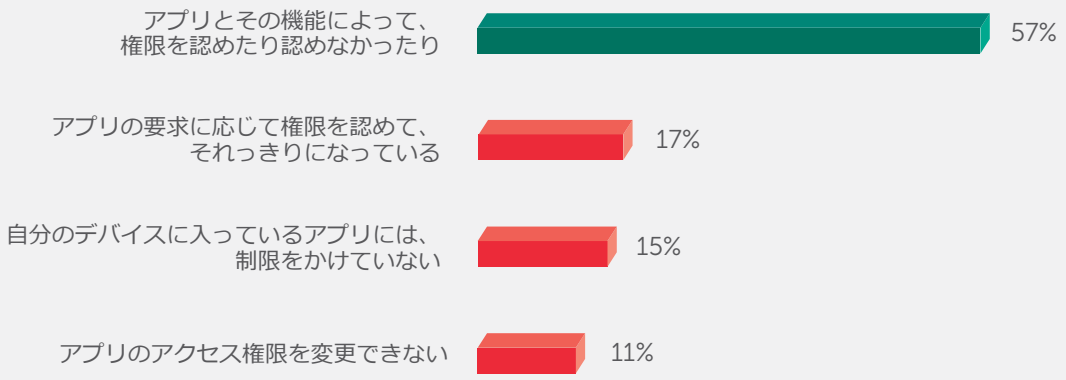
20 % のユーザーは、ソフトウェアのインストール中に表示されるインストールウィンドウの中身を注意深く読むことなく、単純に［次へ］-［次へ］-［同意する］-［次へ］とクリックしています。67 % の回答者だけが慎重にメッセージを読み、必要に応じて設定を調製することで、製造元から不要なソフトウェアが追加インストールされたり、オペレーティングシステムの設定が無断で変更されたりするのを防止しています。

図 26:ソフトウェアのインストール中の設定チェック



デバイス上のアプリに付与する権限に関する質問に対して、**17 % のユーザーが要求に応じてアクセスを付与したのち、そのことを忘れると回答しました。また、15 % の回答者はデバイス上のアプリケーションに対してアクセスを制限したことがありません。**57 % の回答者だけが、意図した目的に応じて、特定の情報へのアクセスや一定の機能の実行権限をアプリに付与しています。興味深いことに、若年層の回答者はアプリに自由な権限を与えることが多い一方で、年配層は独断で権限を変更することはできないと考える傾向にあります。

図 27:アプリに付与する権限



インストールしたアプリが不要になった場合、**37 % のユーザーはいつか役に立つときのためにデバイス上にアプリを残します**が、63 % の回答者はいったん削除して、必要になった場合は再度ダウンロードすると回答しました。正しい回答は後者です。更新されていない古いアプリは、悪意のあるアプリがソフトウェアの脆弱性を悪用してコンピューターに侵入するための「表玄関」となる可能性があります。

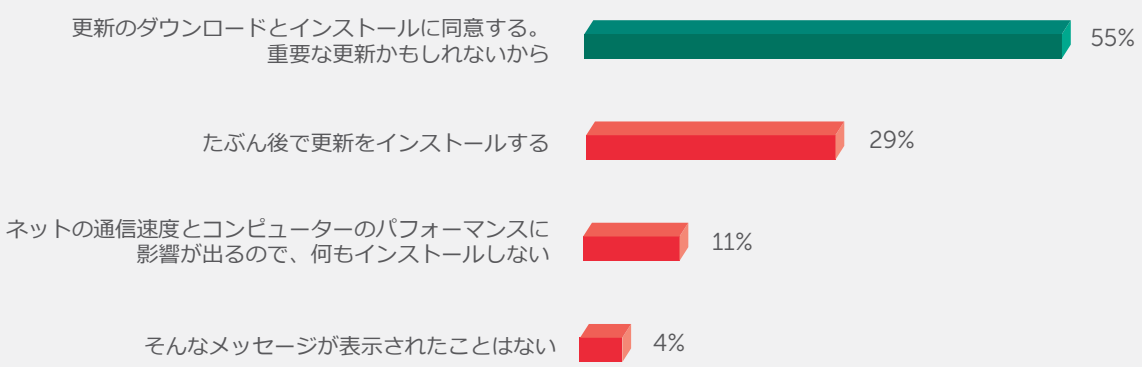
ライセンス契約を読まずに、アプリに無制限のアクセスを付与すると、アプリが何を実行しているか認識できません。忘れがちなことですが、デバイスとアプリはその内部だけでなく、外部の世界も見ることができるのです。たとえば、私たちが写真を撮るために使うカメラ機能は、個人の世界を撮るためにも利用されます。使い方を誤れば、インターネットは私たちの暮らしのもっとも個人的な部分に侵入しかねず、味方だったデバイスが敵に変わることもあります。反対に、十分なネット常識力を身につけている人は、生活を委ねているデバイス上で何が実行されているかを熱心に管理します。

セクション 8:ユーザー自身の保護

ここまでのセクションでは、インターネットユーザーがネットから得られる機会の幅が広がり続ける中で、これに対してどの程度適切に適応してきたかについての全体像を確認しました。このセクションでは、デジタルツールに対する用心深さに的を絞って確認します。ネット常識力の中には、適切なデジタルツールの使用も含まれており、これらを正しく扱うことが重要になります。

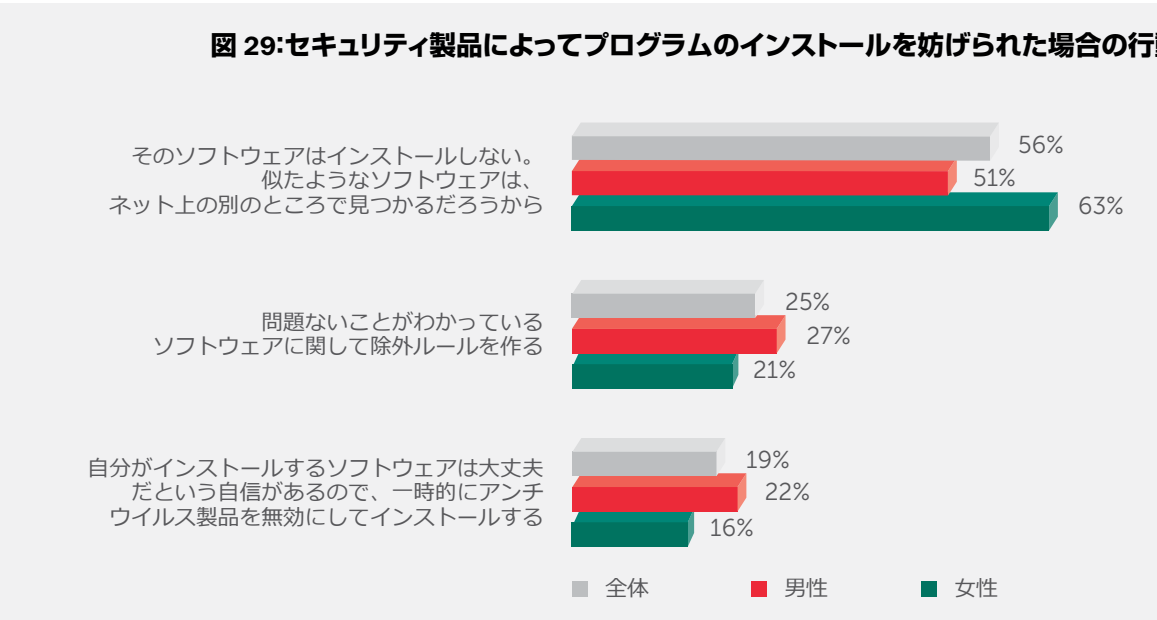
たとえば、オペレーティングシステムに重要な更新をインストールするように求められた場合、これに合意することは理にかなっています。しかし、すぐに更新する人はわずか 55 % であり、29 % の回答者は後から検討すると回答しました。また、**11 % の回答者は、デバイスの性能に影響が及ぶまでは更新をインストールしない**と回答しています。

図 28:OS の更新インストールに対する合意



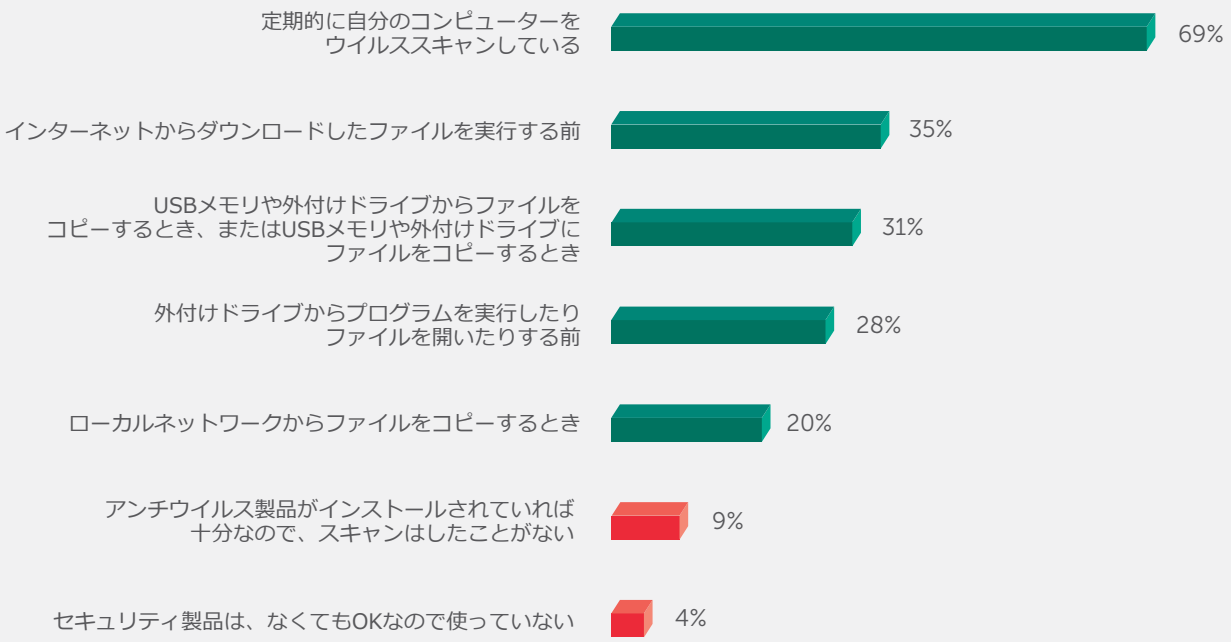
セキュリティ製品によってプログラムのインストールが妨げられた場合、**19 % の回答者はその危険性にもかかわらず、アンチウイルスソフトウェアを無効化してプログラムをインストールする**ことを選びました。若いユーザーほど確信が強く、このような状況でアンチウイルスソフトウェアを無効化するか、プログラムに対して信頼リストを設定する割合が高くなります。この傾向は、女性よりも男性によく見られます。

図 29:セキュリティ製品によってプログラムのインストールを妨げられた場合の行動



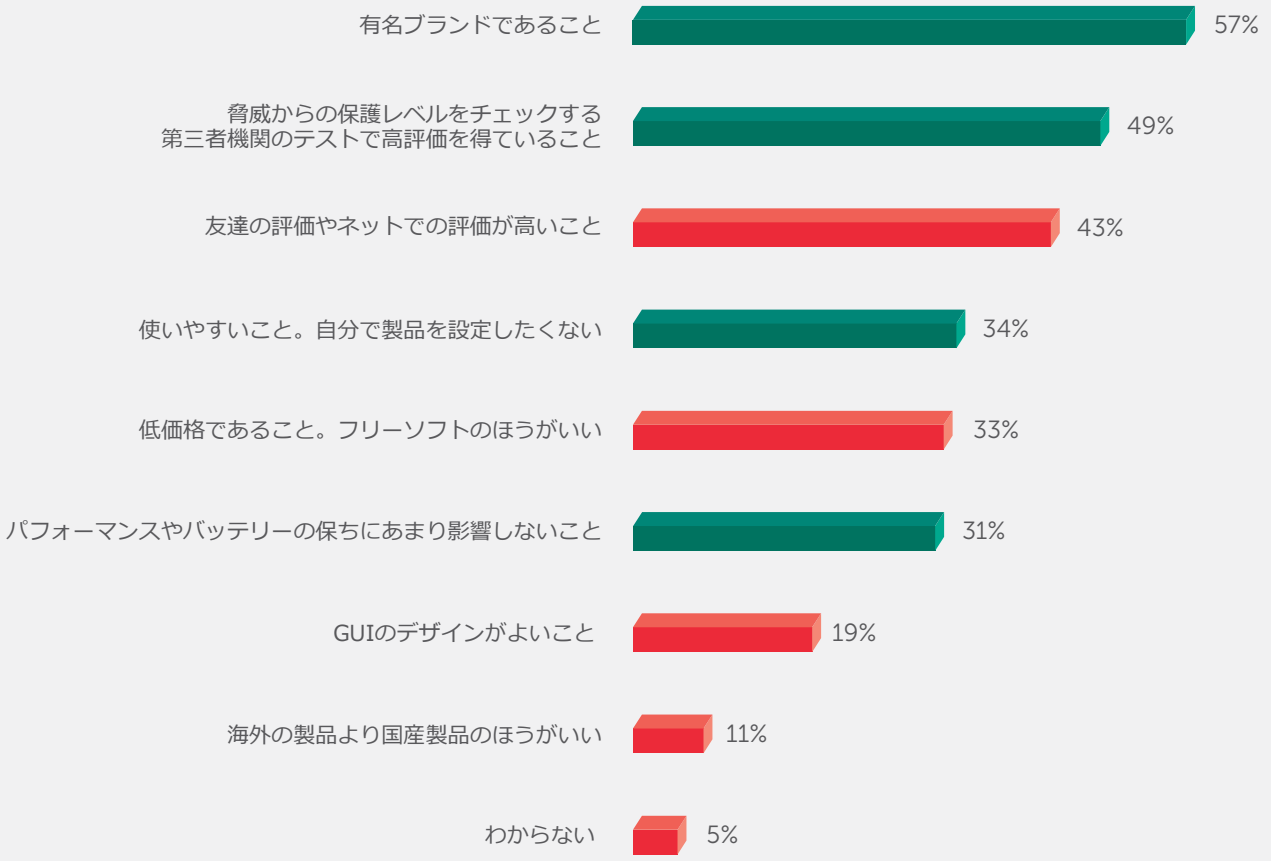
9 % の回答者が、セキュリティ製品をインストールしただけで十分であり、コンピューターのスキャンは不要だと考えています。4 % のユーザーは、セキュリティ製品なしでも安全だと感じています。69 % の回答者がデバイスを定期的にスキャンして、脅威がないかどうかを確認しているのは、良い結果です。

図 30:デバイスのスキャンによるサイバー脅威の確認



セキュリティ製品を選ぶときに複数の基準を同時に選択できる場合、33 % の回答者が低価格を選び、19 % のユーザー（女性 13 %、男性 23 %）がデザインを選ぶと回答しました。若い回答者は友人の意見やオンラインレビューに頼りやすく（24 歳未満の回答者の 51 %）、年配の回答者は自国産製品を選びました（65 歳以上の回答者の 27%）。

図 31:セキュリティ製品を選択するための重要な基準



大部分の人がデジタルツールをいったんインストールしたら後は忘れてしまう傾向にあることは、懸念すべき事態です。また、「今、この場で」実行したい状況でインターネットセキュリティ製品が障壁となると、進んでこれを無視して先に進む場合があります。サイバー空間ではセキュリティに対する従来からの直感は役に立たないことが多いため、このような心構えは甚大な損害をもたらす可能性があります。

まとめ

自己防衛本能は、生まれつきすべての人が持っています。しかし、現実社会ではなく仮想空間が問題になるとき、この本能はうまく働きません。多くの人々が、デバイスとそこに保存したデータに十分な注意を払わず、フィッシングページに個人情報を入力し、簡単すぎるパスワードを選び、表示されたリンクをむやみにクリックし、未確認のソフトウェアをダウンロードしてインストールしています。このためユーザーは無防備になり、詐欺師や犯罪者の標的になりやすくなります。

現代のデジタル空間における「ネット常識力」は、子供時代から身につける必要のあるスキルです。子供が親のタブレットを初めて手に取るとき、何が危険なのかアドバイスしてやる必要がありますし、タブレットに保護手段を講じてある状態にしておくのも重要です。

十分なネット常識力を身につけた人であれば、自身の安全に責任を負うべきであると認識しています。このような人々はインターネットの中身とぜい弱な個所を把握しており、どうすれば脅威に直面する確率を最小限に抑えられるかを理解しています。また、デバイス上に保存されたアカウントやファイルが、現実社会におけるパスポート情報や財布などと同様の価値を持つと知っています。さらに、偽の Web サイトの見分け方や、マルウェアの検知方法、損失や盗難からデータを保護する方法、目に見えない脅威から保護してくれるセキュリティ製品の選び方を知っているか、または学ぼうとする傾向があります。

ネット常識力は、新たな自己防衛本能です。今回のテストが示したとおり、現時点でこの知識を持つインターネットユーザーは圧倒的に少数です。しかし、自分自身と互いを守るためには、このままではいけません。インターネットユーザーで構成された社会全体で、これまでとは違う新しい保護本能、すなわちオンラインで働くデジタル本能を養成する必要があります。

以下のサイトで、ご自身のネット常識力をぜひ確認してみてください。
https://blog.kaspersky.co.jp/cyber-savvy-quiz/

付録 1

使用したフィッシングサンプル

オーストラリア	CommonwealthBank
ブラジル	Itau
チェコ共和国	Facebook（英語）
フランス	Orange
ドイツ	Sparkasse
イギリス	Facebook
インド	Facebook
イタリア	CartaSi
日本	GameCity
マレーシア	Facebook
メキシコ	Banamex
フィリピン	Facebook
ロシア	Vkontakte
スペイン	Banko Popular
トルコ	Facebook
アメリカ	Facebook

株式会社カスペルスキー
PR-1017-201510