日本版
ネット常識力
レポート
2016

サイバーセキュリティ：日本ユーザーの
意識、知識、行動に関する調査

内容

本調査の実施理由

プロアクティブなマルウェア検出技術のパイオニアであるESETは、日本のインターネットユーザーのネット常識力を把握するアンケート調査を2016年1月に実施しました。サイバーセキュリティに関する日本のネットユーザーの意識や知識レベルを把握することが目的で、その意識や知識がオンラインでどのような行動につながり、どのような対策に結び付いているかも調査しています。

ESETがネット常識力の調査を開始したのは2015年。香港、インド、インドネシア、マレーシア、シンガポール、タイのユーザー1,800人を対象に同様のアンケートを実施しました。アジア版のネット常識力レポートはこちらからダウンロードできます。

ベトナム版のレポートも2015年11月に作成しました。ダウンロードはこちらからお願いします。

調査方法

「ESET日本版ネット常識力レポート2016」のオンラインアンケートは、第三者の調査会社により2016年1月に実施されました。回答者は日本全国のインターネットユーザー1,033人。対象年齢は18～55歳で、男女比は均等です。

要点

- 日本では、セキュリティ対策に対するユーザーの意識と実際の対応に大きなギャップが存在します。セキュリティ対策に消極的な日本のユーザーは、サイバー攻撃の被害に遭う可能性があります。

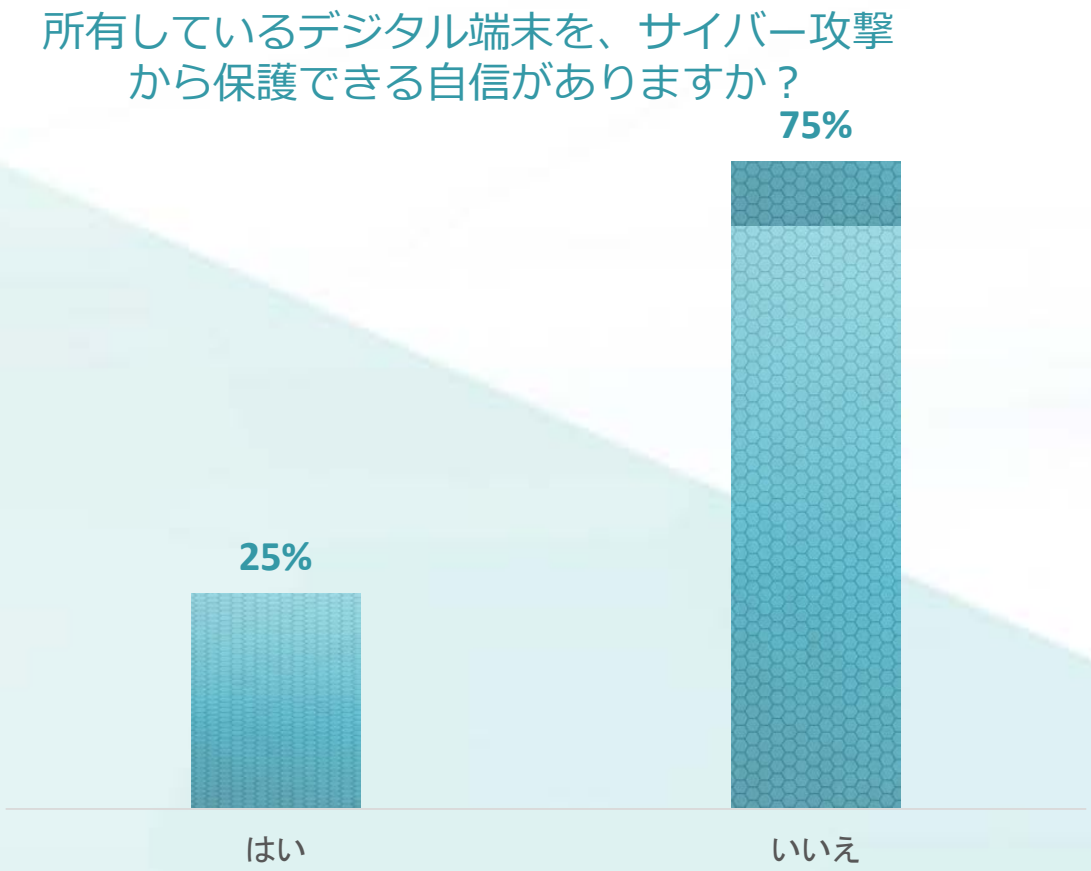
- 日本のユーザーのネット常識力はアジア太平洋地域でもトップクラスにあり、2位以降はマレーシア、シンガポール、インド、タイ、香港、インドネシア、ベトナムと続いています。ネット常識力は攻撃を受けやすい行動、Web上での危険な行為、被害を未然に防ぐ対策に関するユーザーの知識や理解力などを見て評価します。

- アンケートの回答者の70%以上がサイバーセキュリティに関する正式な教育を受けていませんが、80%以上が基本的な質問に正しく答えています。日本のユーザーのこの分野の知識はアジア太平洋地域でも群を抜いており、世代間の知識格差もありません。

- 日本のネットユーザーの多くが、セキュリティリスクにつながる行為を意識的に回避しています。ほとんどの回答者（86%）が、セキュリティ侵害を受けた端末のインターネット接続はすぐに切断すべきだと理解しており、71%は知らない送信者から送られてきたメールの添付ファイルを開かないよう気を付けています。

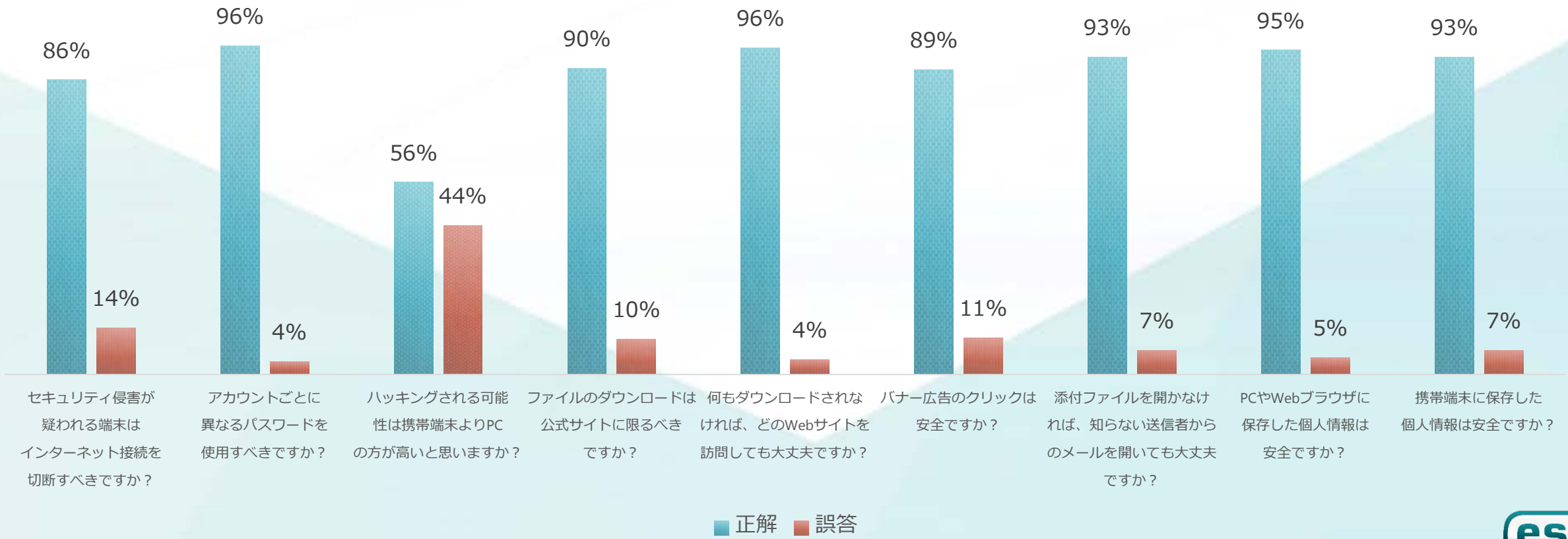
セキュリティ対策に対するユーザーの自信

半数以上のアンケート回答者がセキュリティ侵害を受ける可能性に不安を感じています。また、実に75%の回答者がサイバー攻撃への対策に自信がないと答えています。



サイバーセキュリティに関する知識

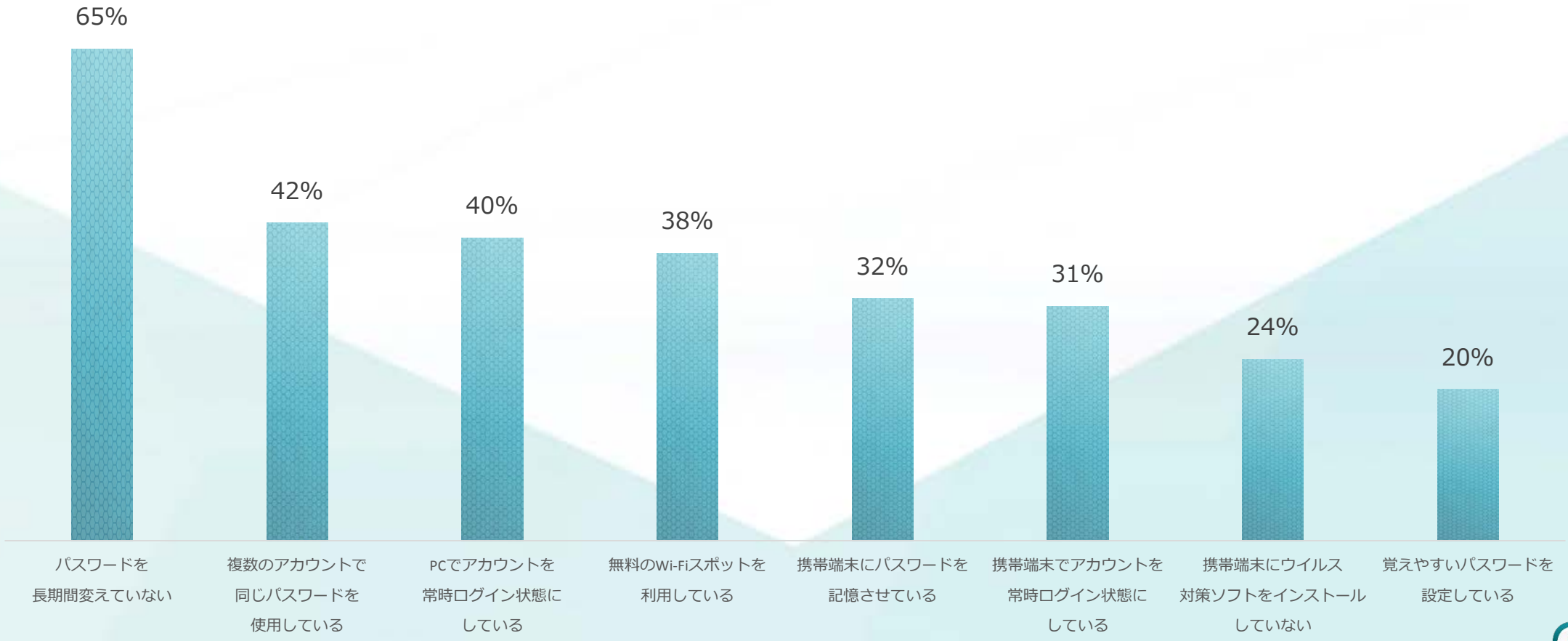
日本のユーザーの多くはサイバーセキュリティの基本事項を理解しており、バナー広告のクリックや、パソコン/Webブラウザに個人情報を保存する危険性も知っていますが、他のアジア諸国と同じように、携帯端末を狙ったサイバー攻撃が増えている事実は把握できていません。



*サイバーセキュリティ関連の質問に正解した、または正解できなかったユーザーの割合

日本のユーザーの問題点

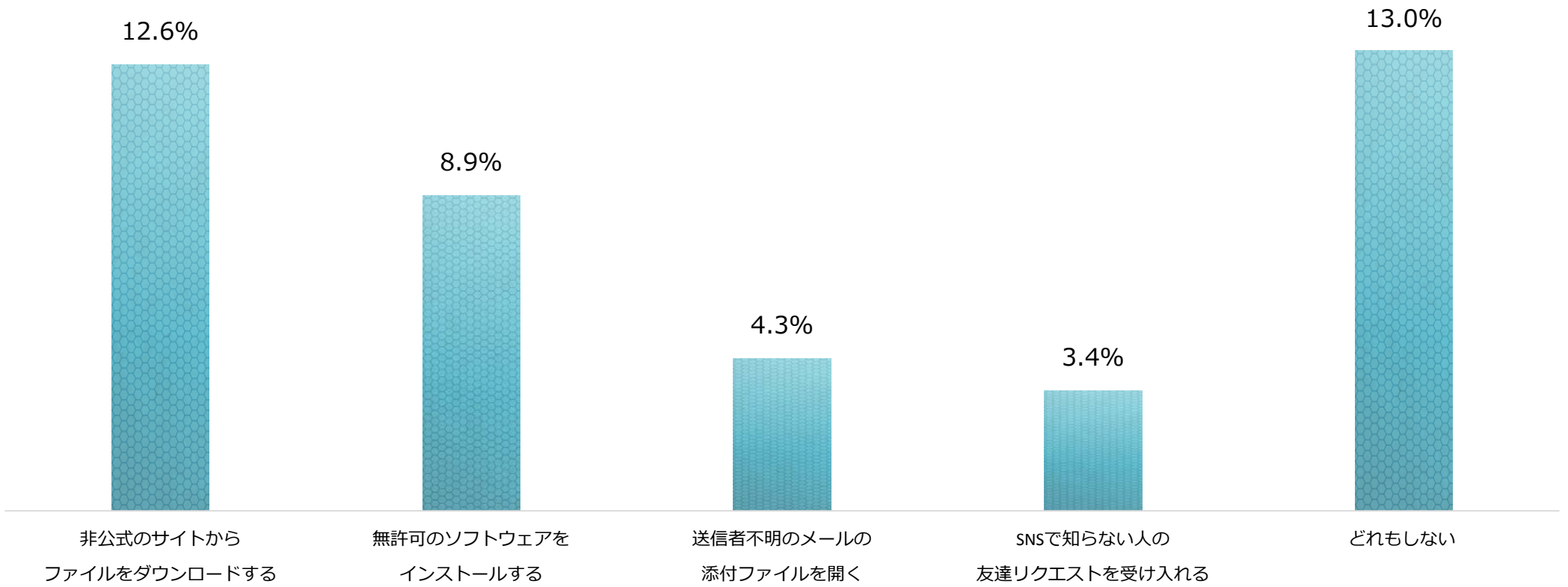
日本のインターネットユーザーの多くは、セキュリティリスクにつながるような行為を控えています（次のスライドを参照）。しかし、パスワードやアカウントの管理が貧弱という特徴があるため、日本のユーザーには的を絞った啓蒙活動が必要です。



*リスクの高い行動を取っているユーザーの割合

日本のユーザーの問題点

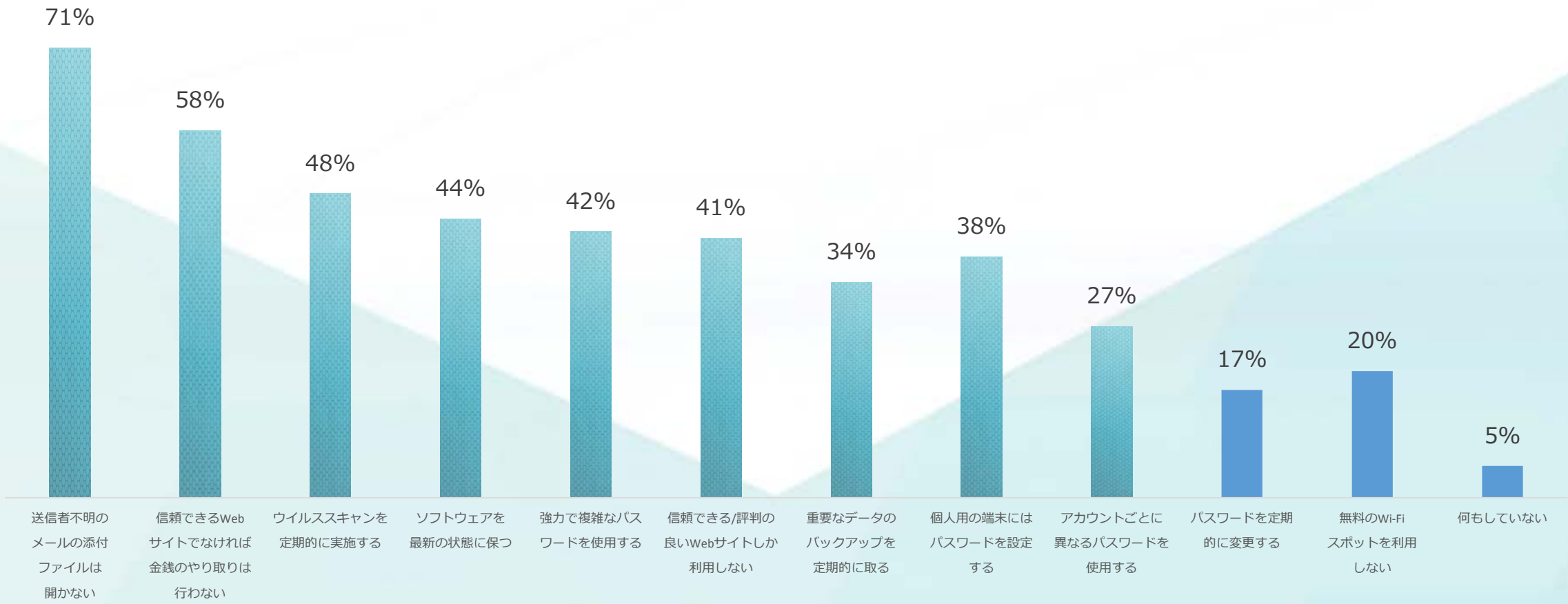
日本のインターネットユーザーは、セキュリティリスクにつながるような行為を控えています。安全に配慮してインターネットを利用し、情報の取り扱いにも注意を払っています。



*リスクの高い行動を取っているユーザーの割合

サイバー攻撃への対策

日本のユーザーはセキュリティ対策にあまり積極的ではありません。調査したほとんどの対策について、定期的に行っていると答えた回答者は50%を下回っていました。



*セキュリティ対策を行っているユーザーの割合

他のアジア太平洋諸国との比較


1. 日本


2. マレーシア


3. シンガポール


4. インド


5. タイ


6. 香港


7. インドネシア

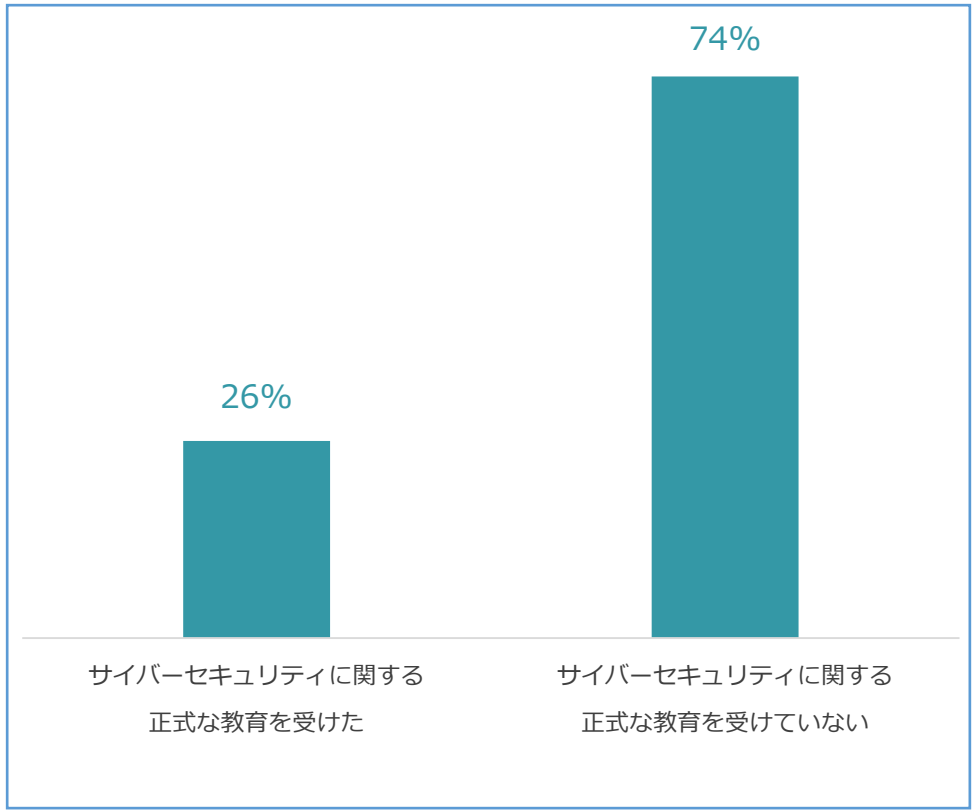

8. ベトナム

ネット常識力に関しては、これまでに調査したアジア太平洋諸国の中では日本が群を抜いており、2位以下はマレーシア、シンガポール、インド、タイ、香港、インドネシア、ベトナムと続いています。

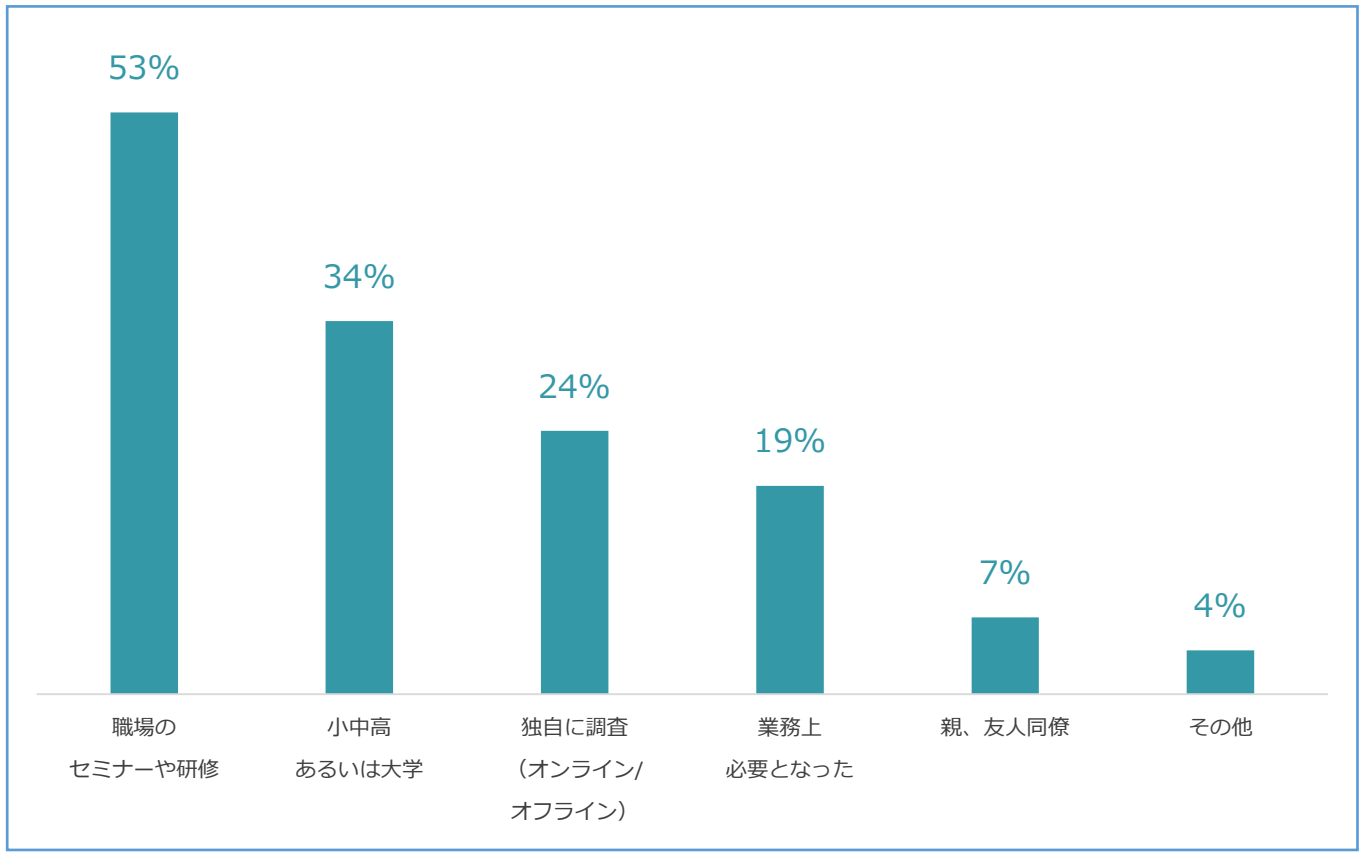
ネット常識力は攻撃を受けやすい行動、Web上での危険な行為、被害を未然に防ぐ対策に関するユーザーの知識や理解力などを見て評価します。

サイバーセキュリティに関する教育

サイバーセキュリティに関する正式な教育を受けたことがありますか？



サイバーセキュリティに関する知識をどこで/どのように獲得しましたか？



結論

日本のインターネットユーザーはサイバーセキュリティに関する知識がありながら、それを活かせず攻撃を受けるリスクを抱えています。日本のユーザーは知識としてセキュリティの基本事項を押さえており、危険な行動は控えるよう注意していますが、安心してインターネットを利用するにはさらなる対策が必要です。

技術水準の高い日本であっても、サイバーセキュリティ対策には改善すべき点があります。日本のユーザーが様々な技術を安心して利用できるようにするためにも、サイバー犯罪を防止する具体的な対策の実施をユーザーに徹底する取り組みが急務と考えられます。

安全を確保するヒント

- **強力なパスワードを使用**: アカウントごとに異なる複数のパスワードを設定し、簡単に推測可能な誕生日や名字などの使用は避けます。文字と数字を組み合わせてパスワードを作成し、3～6か月ごとに変更します。
- **セキュリティの設定を有効化**: ソフトウェアやアプリケーションに組み込まれているセキュリティ機能を、できるだけ利用します。2要素認証を有効にすれば、ネットショッピングなどのセキュリティを強化できます。ブラウザは設定を更新してセキュリティを強化し、ポップアップのブロックも有効にします。
- **セキュリティソフトウェアを使用**: 信頼できるセキュリティソリューションを導入し、あらゆる機能とファイアウォールを有効にします。ソフトウェアの更新も定期的に行います。
- **携帯端末を保護**: パスワード等を設定して携帯端末を保護します。アプリは公式のアプリストアなど、信頼できるサイトからダウンロードしてください。機密データや重要情報は携帯端末に保存しないように心がけます。
- **慎重に行動**: ネット詐欺に遭わないよう万全の対策を講じます。不審なメールには注意し、必ず送信元を確認してください。ネットショッピングを利用する場合は、偽装サイトではないことを確認します。
- **情報の取り扱いに注意:** 個人情報や金融関係の情報を求めてくるメールには返信しないようにします。信頼できる送信元であっても、フィッシング詐欺の恐れがあります。

ESETについて

企業または個人ユーザー向けセキュリティソリューションのグローバルプロバイダであるESET®は、プロアクティブなマルウェア検出技術のパイオニアであり、26年間にわたって業界をリードし続けています。開発したESET NOD32®技術は1998年のテスト開始以来、実際に感染報告のある、いわゆる「In-the-Wild」ワームやウイルスをすべて検出しており、見逃したことがありません。この技術は2013年6月に通算80回目の『Virus Bulletin』誌VB100アワードを獲得し、現在、受賞回数の最多記録を保持しています。

ESET NOD32技術はVB100 アワード連続受賞の最長記録も保持しています。また、ESETはAV-ComparativesやAV-TESTなどの第三者テスト機関からも、幾度となく高い評価を受けてきました。ESET NOD32®アンチウイルス、ESET Smart Security®、ESET Cyber Security® （Mac向け）、ESET® Mobile Security、およびIT Security for Businessはすべて、数百万のユーザーに支持されている世界有数の推奨セキュリティソリューションです。