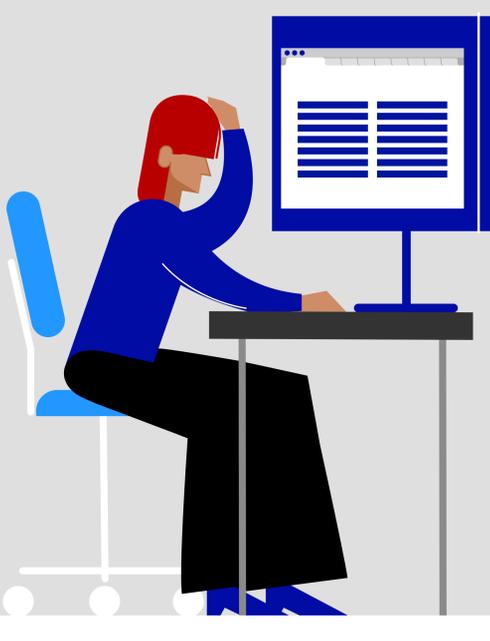


# デジタル不安の時代

リモートワークにおける、サイバーセキュリティやプライバシーに関する『デジタル不安』の高まり



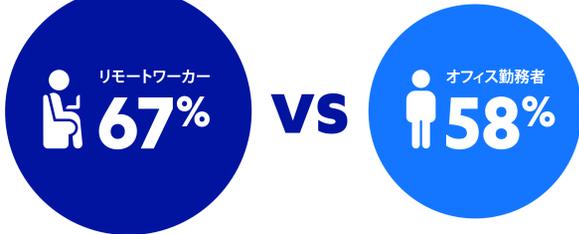
2021年に6月にエフセキュアが実施した調査で、以前より自宅での勤務が増えたと回答した人のうち、79%がセキュリティリスクに対する懸念が高まったと答えています。



リモートワーカーは、実際には何も問題がない場合でも、オンライン上のセキュリティやプライバシーに関する不安を感じる人が多いようです。

実際には何も問題がない場合でも、オンライン上のセキュリティやプライバシーに関して不安を感じる。

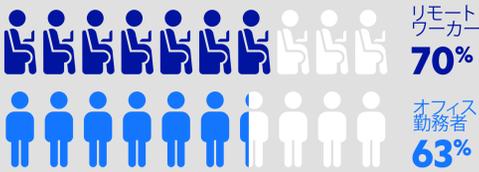
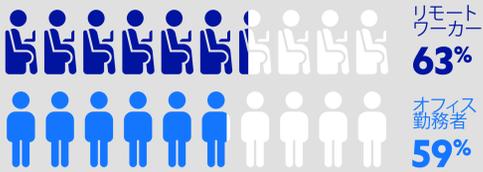
オンライン上のセキュリティやプライバシーに関する懸念は珍しいものではありません。しかし、最近の調査では、リモートワーカーは次から次へと様々な問題について不安を抱くようになってきていることがわかりました。



## 不安に感じること

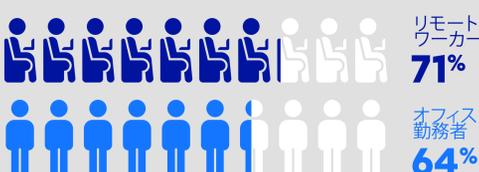
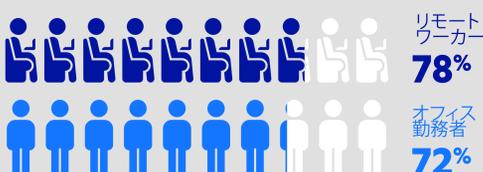
ネット接続されている自分の全てのデバイスのセキュリティを管理することは、ほぼ不可能な作業だと感じている。

セキュリティ上のリスクを考えると、公共のWi-Fiに接続することにより強い抵抗を感じるようになった。



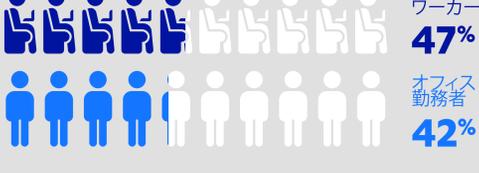
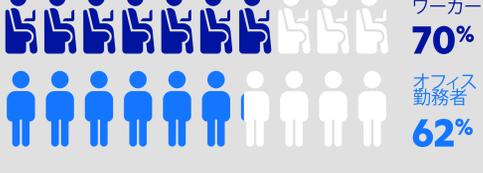
オンラインサービスの登録時やオンラインショッピング時に提供する個人情報の量を減らすようになった。

ネット接続している自分のデバイスが、ウイルスやマルウェアに感染したり、ハッキングされたりしないか不安だ。



ネット接続された自分の新しいデバイスが、自分のプライバシーを侵害するのではないかと心配だ。

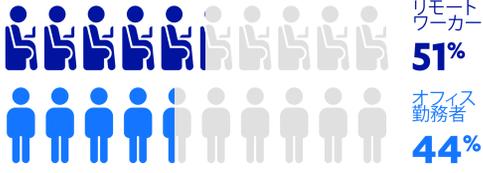
過去12ヶ月の間に、パスワードの管理がより難しくなったと感じる。



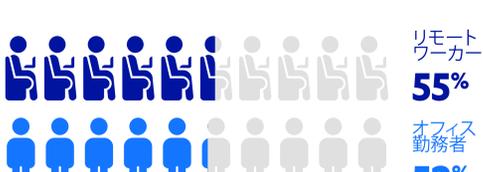
## 安全性や個人情報

十分な安全性が確保されているかどうか確信が持てなかったため、ネット接続デバイスの購入を延期、または購入そのものを見送ったことがある。

自分の個人情報の収集について不安があり、スマートデバイスやサービス (Alexa, Google home, Siriなど) の購入を延期したり、購入そのものを見送ったことがある。



収集される個人情報の量が心配になり、スマートサービス (Siriなど) を利用しないことにした。



## 習慣の変更

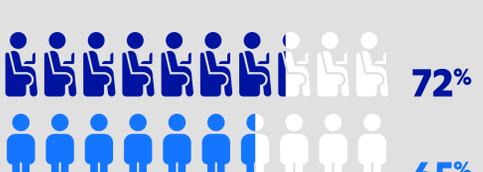
最近数ヶ月でデータのプライバシーに関する懸念が高まり、インターネット利用における習慣を変えた。

インターネットがより危険な場所になってきていると感じ、インターネット利用における習慣を変えた。



ハッカーに個人情報を盗まれたり、デバイスが感染したりすることが心配で、公共のWi-Fiは使わないようにしている。

カメラの使用や連絡先リストへのアクセスなど、不要と思える許可を求めるアプリはインストールしないようにしている。



Source: F-Secure Consumer Survey Wave 4 (2021), nine countries (USA, UK, Germany, France, Brazil, The Netherlands, Mexico, Sweden, Japan), sample size 800/country, total 7200 respondents.

## 不安を解消する方法

基本的なオンラインセキュリティとプライバシー対策は、仕事や遊びでデバイスを使用する際のリスク管理に役立ちます。また、スマートな習慣を身につけることで、ネット上で何をしても、安全にプライベートを保護することができます。

- 1.1** オンライン会議では、自分の背景 (部屋の内部など) を必要以上に共有しないようにしましょう。必要に応じて、ぼかしやバーチャル背景を使用しましょう。
- 1.2** VPNでプライバシーを保護しましょう。
- 1.3** 不要なデバイスのプラグは抜き、Wi-Fiとルーターに強力でユニークなパスワードを使用することで、ホームネットワークを保護しましょう。
- 1.4** 業務用/個人用の全てのデバイスで、システム/プログラム/セキュリティソフトウェアが最新の状態でアップデートされていることを確認しましょう。
- 1.5** 不審なメール/メッセージ/電話の着信/その他の通信を所属企業に報告しましょう。

しかし、これらのステップだけでは、デジタルへの不安を解消できない場合があります。何も問題がない時に起こる不安を解消するには、仕事と個人のデバイス使用を明確に切り分ける必要があるかもしれません。

- 2.1** 業務用のデバイスやホームオフィスを、個人的な作業や趣味のために使用しない。
- 2.2** 仕事とそれ以外に明確な境界線を設定します。これは、勤務時間外に業務用のデバイスやメールをチェックしないようにすることです。
- 2.3** 会社のメールアドレスを個人的な用途のために使用することは避けましょう。

## エフセキュアについて

最も優れたセキュリティコンサルタント、何百万台ものデバイスに搭載された数多くの受賞歴を誇るソフトウェア、進化し続ける革新的なセキュリティ対策に関するAIテクノロジー、そして「検知と対応」。これらの橋渡しをするのがエフセキュアです。当社は、大手銀行機関、航空会社、そして世界中の多くのエンタープライズから、「世界で最も強力な脅威に打ち勝つ」という私たちのコミットメントに対する信頼を勝ち取っています。グローバルなトップクラスのチャネルパートナー、200社以上のサービスプロバイダーにより構成されるネットワークと共にエンタープライズクラスのサイバーセキュリティを提供すること、それがエフセキュアの使命です。

エフセキュアは本社をフィンランド・ヘルシンキに、日本法人であるエフセキュア株式会社を東京都港区に置いています。また、NASDAQヘルシンキに上場しています。詳細は以下のページをご覧ください。  
<https://www.f-secure.com/en/welcome> (英語)  
[https://www.f-secure.com/ja\\_JP/](https://www.f-secure.com/ja_JP/) (日本語)

また、Twitter @FSECUREBLOG でも情報の配信をおこなっています。

[f-secure.com/business](https://f-secure.com/business) | [twitter.com/fsecure](https://twitter.com/fsecure) | [linkedin.com/f-secure](https://linkedin.com/f-secure)

エフセキュア株式会社  
 〒105-0004 東京都港区新橋2丁目2番9号 KDX新橋ビル 2階  
 Tel: 03-4578-7710 / E-mail: japan@f-secure.co.jp  
[https://www.f-secure.com/ja\\_JP/](https://www.f-secure.com/ja_JP/)

2022.02.JP

