

調査報告書

IoT セキュリティガイドラインに対する
一般利用者の意識の実態調査（その3）

2022 年 3 月 31 日

モバイルコンピューティング推進コンソーシアム
セキュリティ委員会

目 次

はじめに.....	2
1 調査概要.....	4
1.1 調査の目的	4
1.2 調査内容	5
2 IoTセキュリティガイドラインに対する一般利用者の意識の実態調査	6
3 考察.....	7
3.1 セキュリティ対策全般に対する意識	7
3.2 一般利用者のためのルールと利用者意識の現状	8
3.3 セキュリティ対策意識の向上に向けて	10
4 アンケート調査結果.....	11

はじめに

モバイルコンピューティング推進コンソーシアム（MCPC、会長 安田靖彦）は、過去 2 回 IoT セキュリティに関する調査報告をしました。

今回、IoT セキュリティ意識の浸透度合いを 2018 年度に引き続き実施しましたので、前回の調査と比較しまとめた結果をお知らせします。今後サービス提供社が実施すべき対応の一助となりましたら幸いです。

＜調査の背景＞

モバイル PC、スマートフォンに続く潮流として、あらゆるものが繋がる IoT 時代になりセキュリティに関する懸念が増加しています。

この状況下、

- 1) 総務省及び経済産業省では「IoT 推進コンソーシアム IoT セキュリティワーキンググループ」を開催、「IoT セキュリティガイドライン」としてまとめ、公表
- 2) 総務省では「IoT セキュリティ総合対策」を策定し進捗状況を「IoT セキュリティ総合対策プログレスレポート」としてまとめ、2018 年より毎年公表

を行っています。

昨今の IoT のセキュリティ脅威の多様化に伴い、政府並びに民間の取り組み施策が多数公表されています。

MCPC では、2016 年と 2018 年に「IoT セキュリティ」に関する一般利用者の意識調査を行いました。

2016 年：一般消費者の意識がどのような実体なのか、「IoT セキュリティガイドライン」に記載されている「一般利用者のためのルール」をもとに身近な Web カメラを事例として調査を行いました。

2018 年：Wi-Fi ルーターを事例とし、IoT 機器の安心・安全な普及に向け、セキュリティ意識の実態、啓蒙による意識の変化、対策に対するコスト負担の許容範囲等を調査しました。

今回、IoT 機器の浸透に伴い、特定機器を事例とせず、IoT 機器全般を対象に IoT 機器の安心・安全な普及に向け、セキュリティ意識の実態、啓蒙による意識の変化、対策に対するコスト負担の許容範囲等を前回とどのように変化しているか調査しました。

(1) 調査期間 2021 年 11 月 10 日～11 月 11 日

(2) 調査方法 インターネットリサーチ

(3) 有効回答数 420 名

1 調査概要

(1) 調査の目的

あらゆるものが繋がる IoT 時代となり、脆弱な IoT 機器を狙ったサイバー攻撃も増加しています。多数の IoT 機器を踏み台とした大規模 DDoS 攻撃などがインターネットにおける重大な脅威となっています。国立研究開発法人 情報通信研究機構 (NICT) の観測によると 2020 年のサイバー攻撃は 2017 年と比べると 3.3 倍に達し、Web カメラやルーター等の IoT 機器への攻撃が 40% 程度に及んでいます。これらは、認証機能の不備等の製品単体のセキュリティ上の問題だけでなく、IoT システムの構成上の問題や、初期パスワードを変更せずに利用するなどの利用者側の運用上の問題など様々な要因が絡んで発生しています。このため、IoT システムのセキュリティ対策においては、IoT 機器の設計・製造者、IoT システムの供給者・運用者、サービスの利用者らが、セキュリティ対策における認識を共有、各々の役割・立場に応じて適切なセキュリティ対策を検討することが必要です。

このような状況の中で設立された IoT 推進コンソーシアムは、IoT 機器の設計・製造等に係る製造事業者や IoT の運用等に関わる企業利用者及び一般利用者向けのセキュリティガイドラインが策定されました。更に「IoT セキュリティ総合ガイドライン」が策定されるとともに、IoT セキュリティ総合対策のもと進捗状況を「IoT セキュリティ総合対策プログレスレポート」として公表しています。

MCPC では、2016 年と 2018 年に「IoT セキュリティ」に関する一般利用者の意識調査を行いました：

2016 年：一般消費者の意識がどのような実体なのか、「IoT セキュリティガイドライン」に記載されている「一般利用者のためのルール」をもとに身近な Web カメラを事例として調査を行いました。

2018 年：2016 年の調査に加え、Wi-Fi ルーターを事例とし、IoT 機器の安心・安全な普及に向け、セキュリティ意識の実態、啓蒙による意識の変化、対策に対するコスト負担の許容範囲等を調査しました。

今回、IoT 機器の浸透に伴い、特定機器を事例とせず、IoT 機器全般を対象に IoT 機器の安心・安全な普及に向け、セキュリティ意識の実態、啓蒙による意識の変化、対策に対するコスト負担の許容範囲等を前回とどのように変化しているか調査しました。本調査が、IoT 機器の設計・製造等に関わる製造事業者や IoT の運用等に関わる企業等が、一般利用者の認識を共有し、IoT システムのセキュリティ対策を検討する上での参考になれば幸いです。

（２）調査内容

本調査では、一般利用者を対象に IoT セキュリティ全般に関わる意識の実態、IoT セキュリティガイドラインが示す「一般利用者のためのルール」と一般利用者の振る舞いの乖離の有無や程度、製造者責任やコスト負担許容度等の IoT 機器のセキュリティに関する考えについての調査を実施しました。

ここでの調査の対象とした IoT 機器は、①パソコン ②スマートフォン・タブレット端末 ③ Web カメラ ④ Wi-Fi ルーター ⑤スマートスピーカー の 5 種類です。

2 IOT セキュリティガイドラインに対する 一般利用者の意識の実態調査

調査対象：マクロミルモニタ 15 ～ 69 歳の男女

インターネットに接続する電子機器を使用している方

調査地域：全国

調査方法：インターネットリサーチ

調査時期：【事前調査】2021 年 11 月 8 日（月）～ 11 月 10 日（水）

【本調査】2021 年 11 月 10 日（水）～ 11 月 11 日（木）

有効回答数：【事前調査】10,000 サンプル

【本調査】420 サンプル

調査実施機関：株式会社マクロミル

（アンケート調査結果は「別冊 アンケート調査結果」に示す）

3 考察

(1) セキュリティ対策全般に対する意識

セキュリティの観点から見た IoT 機器の普及プロセスは、まず、セキュリティリスクが広く認知されることで、セキュリティ対策製品の購入等による対策が進み、適切なセキュリティ対策に支えられ、より積極的な活用の段階に至るものと考えられます。

セキュリティ対策全般に対する意識調査の結果からは、パソコンやスマートフォン・タブレット端末に関してはリスクが認知され対策も導入された上での活用が進んでいるように見えます。これに対し、Web カメラ、Wi-Fi ルーター、スマートスピーカーに関しては、購入時にパソコンやスマートフォン・タブレット端末と同様にセキュリティ対策を重視していますが、購入した後のセキュリティ対策は実施することなく、利用に関しては不安、懸念は感じていない状況です。

また、パソコン、スマートフォン・タブレット端末、Web カメラ、Wi-Fi ルーターのすべてにわたり、前回調査とほぼ同様の調査結果になりました（スマートスピーカーについては、前回調査では対象外です）。すなわち、「セキュリティ対策全般に対する意識」という観点では、変化していない状況と言えます。

（「セキュリティ対策全般に対する意識」参照アンケート番号：Q1、Q2、Q3、Q4）

(2) 一般利用者のためのルールと利用者意識の現状

IoT セキュリティガイドラインの一般利用者のためのルールでは、IoT 機器を利用する際に注意すべき事項として次の 4 つを挙げています：

- ① 問い合わせ窓口やサポートがない機器やサービスの購入・利用を控える
- ② 初期設定に気を付ける
- ③ 使用しなくなった機器については電源を切る
- ④ 機器を手放すときにはデータを消す

今回の調査結果より、それぞれの利用者意識は、次のようになっています：

- ① 問い合わせ窓口やサポートがない機器やサービスの購入・利用を控える

電子機器購入時の重視点として、問い合わせ窓口やサポートの有無は挙がるものの、30% 程度（スマートスピーカーについては 50%）はサポート期限到来後も使用を続けると回答しています。使用をやめると回答した利用者は、10% 程度です。この傾向は、前回の調査結果と同様です。

（「問い合わせ窓口・サポートサービス期限への考え方」参照アンケート番号：Q5、Q6、Q7）

- ② 初期設定に気を付ける

利用者の 30% が初期パスワードを「特に変更しない」、45% が「(どちらかといえば) 同じパスワードを使い回す」と回答しています。この傾向は、前回の調査結果と同様です。

初期設定の重要性に関する適切な啓発活動に加えて、利用開始時のパスワード変更を必須とするなどの IoT 機器側の対策も望まれる状況です。前回の調査結果と傾向が同じことを踏まえ、継続的啓発活動と令和 2 年 4 月 1 日以降に技術基準適合認定を取得した製品を利用することを期待します。

（「初期設定に対する意識」参照アンケート番号：Q8、Q9、Q10）

③ 使用しなくなった機器については電源を切る

いずれの機器も半数以上が「常にインターネットに接続」して機器を使用するとの回答です。この傾向は、前回の調査と同様です。また、使用しなくなった機器についても、30%強は「常にインターネットに接続」していると回答しており増加傾向にあります。これは、サポートできなくなったIoT機器が放置される懸念があることを示しています。

(「電子機器の電源、インターネット接続状況」参照アンケート番号 :Q15、Q16)

④ 機器を手放すときにはデータを消す

保存データの把握に関して、「Wi-Fi ルーター」使用者では、保存データを「把握」している利用者が 20% 台に留まり、「保存されていない」意識の利用者が 35% 程度存在します。「スマートスピーカー」使用者も同様に「保存されていない」意識の利用者が 30% 強となっており、「パソコン」「スマートフォン・タブレット端末」に比べて意識が低いとなっています。従い、機器を手放すときのデータ削除については、パソコンやスマートフォン・タブレット端末に比べ、IoT 機器においては、データを削除せずに手放す割合が高くなるという結果です。但し、「スマートスピーカー」使用者の 80% 強がデータ削除について「データ削除を行ってから手放す」と回答しています。これは、仮説として、利用者と直接会話するインタフェースでサービスを提供しているため、ユーザーにとって「データを削除せずに手放すのは気持ちが悪い。」「クラウドサービスのアカウントと紐づいた機器であり、悪用の可能性がある。」等の感情・意識があるためと考えられます。

(「保存データに対する意識」参照アンケート番号 :Q17、Q18)

(3) セキュリティ対策意識の向上に向けて

「クラウドサービスのアカウントと紐づけて利用していた電子機器を紐づけの情報を削除せずに廃棄してしまい悪用された事例」の認知度は、50% 強です。事例認知後のデータ削除意向は、「パソコン」「スマートフォン・タブレット端末」で 90% 強、「スマートスピーカー」で 80% 強、「ウェブカメラ」「Wi-Fi ルーター」で 75% 程度です。これにより、適切な事例を用いた啓蒙活動、特に、「機器を手放すときにはデータを消す」に対しては効果があることが示していると考えます。

また、「インターネットに接続されたウェブカメラが、外部から自由にのぞき見された事例」「インターネットに接続された電子機器がマルウェアに感染し、サイバー攻撃の踏み台として悪用された事例」いずれも 70% 強が認知していました。事例認知後のセキュリティ対策費用感は、「セキュリティ重視」が 60% 強と「価格重視」の 10% 程度を大きく上回っています。従い、適切な事例によるセキュリティ喚起は、コストに関する寛容性が増すことが分かりました。

(「呈示事例」 参照アンケート番号 :Q19、Q20、Q22、Q23)

MCPC セキュリティ委員会では、今後も、総務省などの中央省庁、個人情報保護委員会、情報処理推進機構 (IPA)、IoT 推進コンソーシアム、産業技術総合研究所や情報セキュリティ大学院大学等のアウトプットを活用した普及啓蒙活動、及び IoT 普及に向け優先すべきセキュリティ施策の検討に資する調査を行っていきたいと考えています。

4 アンケート調査結果

アンケートの調査結果を次ページ以降に示す。

IoTに関する調査結果

2021年12月

目次

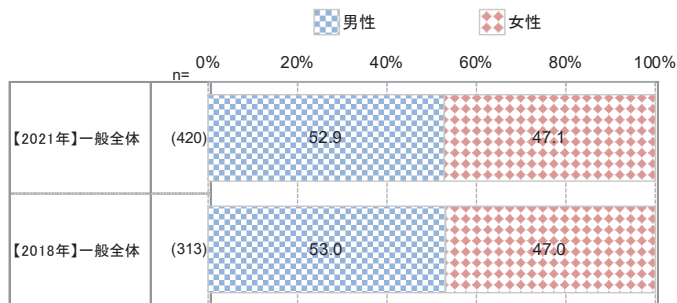
■ 調査概要	3
■ 回答者プロフィール	4
■ セキュリティ対策全般に対する意識	5
■ 問い合わせ窓口・サポートサービス期限への考え方	10
■ 初期設定に対する意識	13
■ 電子機器の電源、インターネット接続状況	17
■ 保存データに対する意識	19
■ WiFiルーター事例を通じたセキュリティ対策意識の変化	21

調査概要

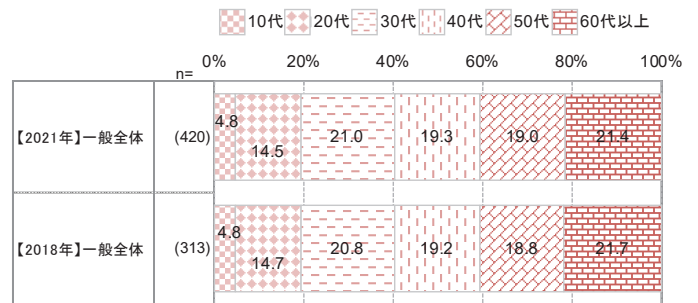
■ 調査目的	IoTセキュリティガイドライン「一般消費者のためのルール」と実際の一般消費者の意識とのギャップをあぶりだし、サービス提供者側が実施すべき対応の啓蒙を行う基礎資料の一助とする。
■ 調査対象	マクロミルモニタ 15～69歳の男女 インターネットに接続する電子機器を使用している方
■ 調査地域	全国
■ 調査方法	インターネットリサーチ
■ 調査時期	【事前調査】 2021年11月8日（月）～11月10日（水） 【本調査】 2021年11月10日（水）～11月11日（木）
■ 有効回答数	【事前調査】 10,000サンプル 【本調査】 420サンプル
■ 調査実施機関	株式会社マクロミル

回答者プロフィール n=420

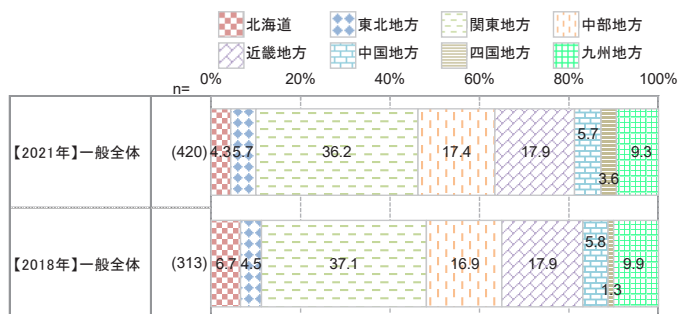
性別



年齢



居住地



© Macromill, Inc.

4

MACROMILL

セキュリティ対策全般に対する意識

© Macromill, Inc.

©ALL rights reserved by MCPC 2022

5

モバイルコンピューティング推進コンソーシアム

電子機器購入重視点

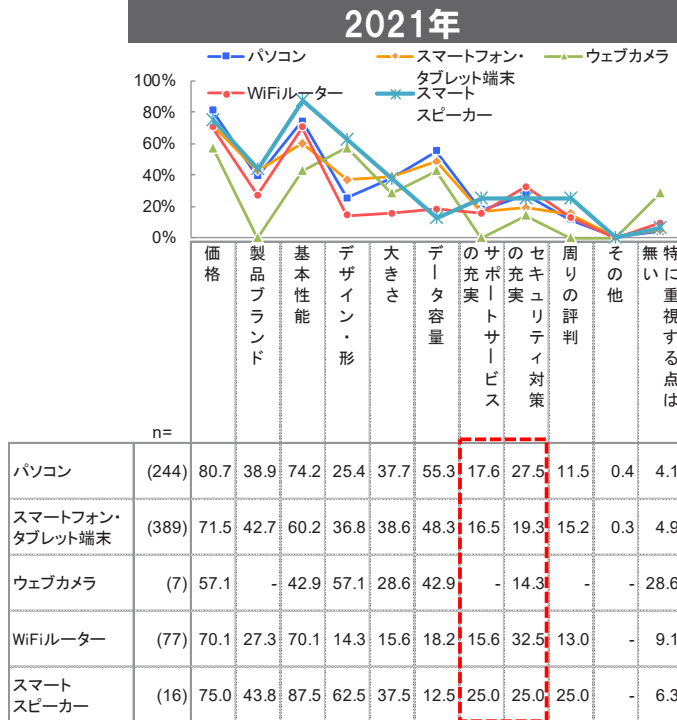
「パソコン」「スマホ」は、各購入者における「セキュリティ対策」を重視する方の割合は2018年と比べても大きくは変わらず、「Wi-Fiルーター」はやや増加。

- 総じて、「セキュリティ対策の充実」は上位項目には挙げられず、2018年調査と概ね同じ傾向。「サポートサービスの充実」については、「スマホ」が微減。
- 新規聴取の「スマートスピーカー」は「セキュリティ対策の充実」「サポートの充実」をいずれも4人に1人が挙げている。

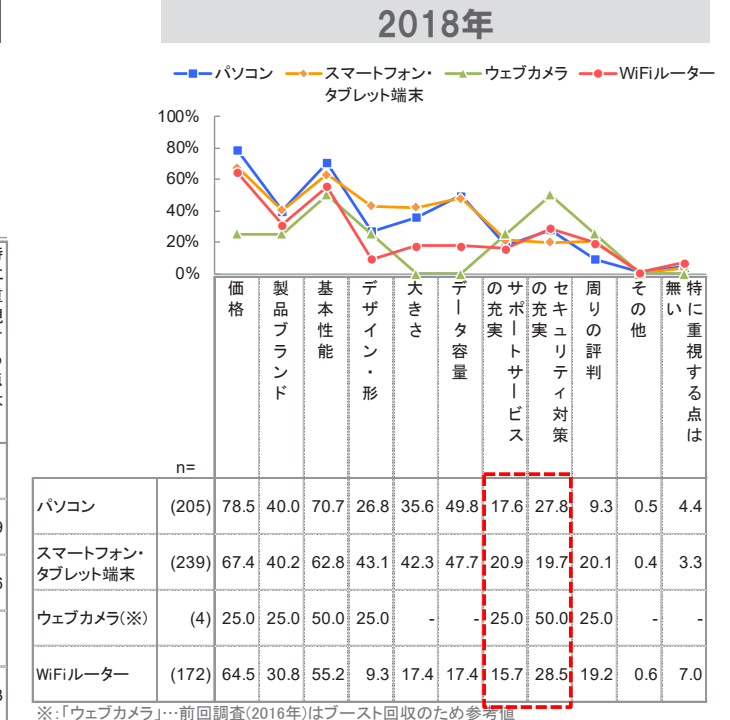
Q1 あなたが以下のインターネットに接続して使用している電子機器を購入される際、重視する点としてあてはまるものをすべてお答えください。

MA

※各機器購入者ベース



© Macromill, Inc.



MACROMILL

電子機器のセキュリティ対策

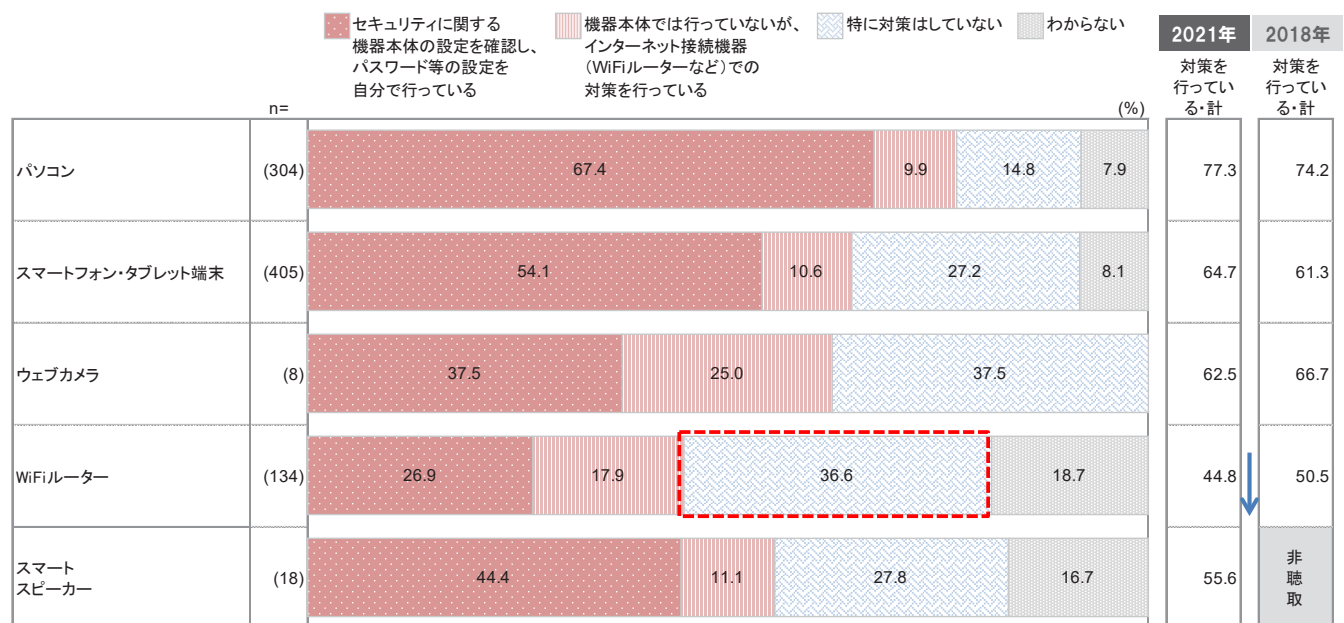
「Wi-Fiルーター」使用者の3割半ばが、セキュリティ対策について「特に対策はしていない」と回答。

- セキュリティ対策について2018年調査と比べると、「パソコン」の7割台、「スマホ」では6割台がスコア維持しているのに対し、「Wi-Fiルーター」については4割半ばと減少傾向。「スマートスピーカー」は5割半ばが対策を行っている」と回答。

Q2 あなたがインターネットに接続して使用している以下の電子機器について、セキュリティ対策を行っていますか。それぞれ最もあてはまるものを1つお答えください。

SA

※各機器使用者ベース



※対策を行っている・計(「セキュリティに関する機器本体の設定を確認し、パスワード等の設定を自分でやっている」+「機器本体では行っていないが、インターネット接続機器(Wi-Fiルーターなど)での対策を行っている」)

7

© Macromill, Inc.

MACROMILL

©ALL rights reserved by MCPC 2022

モバイルコンピューティング推進コンソーシアム

電子機器に対するセキュリティ不安

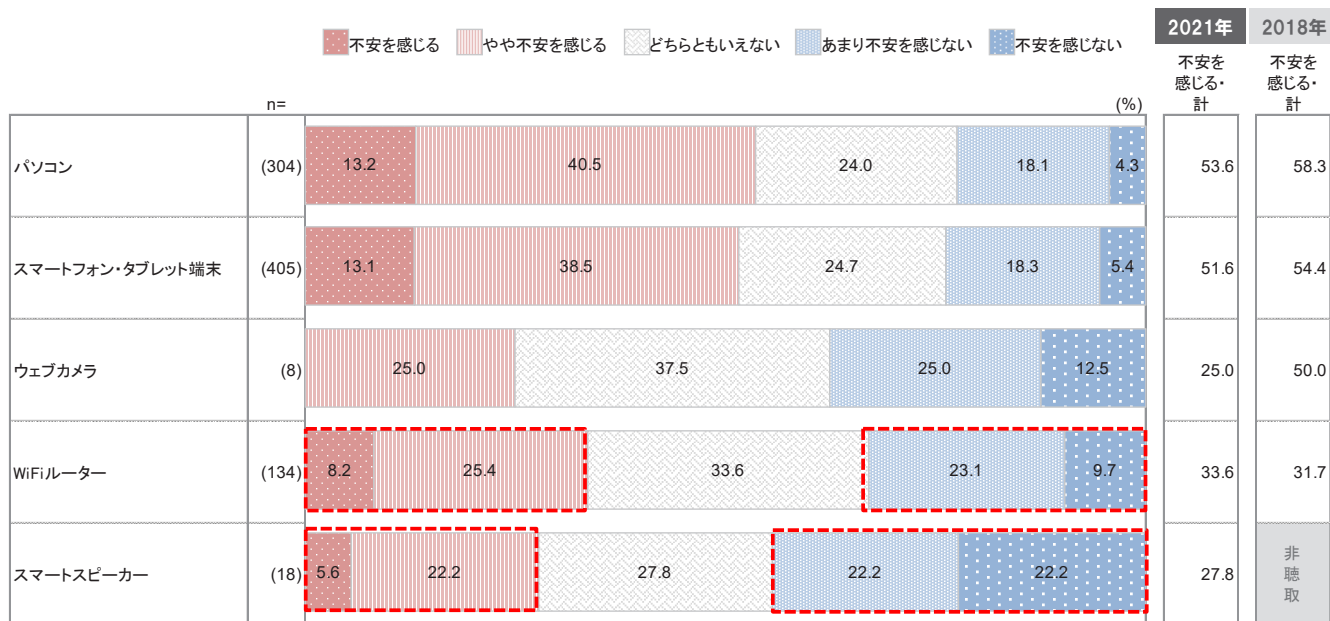
「Wi-Fiルーター」「スマートスピーカー」では、「パソコン」「スマホ」に比べ、セキュリティ不安を感じていない。

- 「Wi-Fiルーター」のセキュリティ対策について、使用者の3割強が「（あまり）不安を感じていない」と回答しており、「パソコン」「スマホ」に比べ多い。逆に「（やや）不安を感じる」については、使用者の3割強に留まり、「パソコン」「スマホ」に比べ少ない。「スマートスピーカー」も同様の傾向。
- 2018年調査と比べても「パソコン」「スマホ」「Wi-Fiルーター」は「不安を感じる・計」のスコアに大きな変化は見られない。

Q3 あなたがインターネットに接続して使用している以下の電子機器について、どの程度セキュリティに対する不安を感じますか。それぞれ最もあてはまるものを1つお答えください。

SA

※各機器使用者ベース



※不安を感じる・計（「不安を感じる」+「やや不安を感じる」）

MACROMILL

© Macromill, Inc.

8

セキュリティ上の懸念

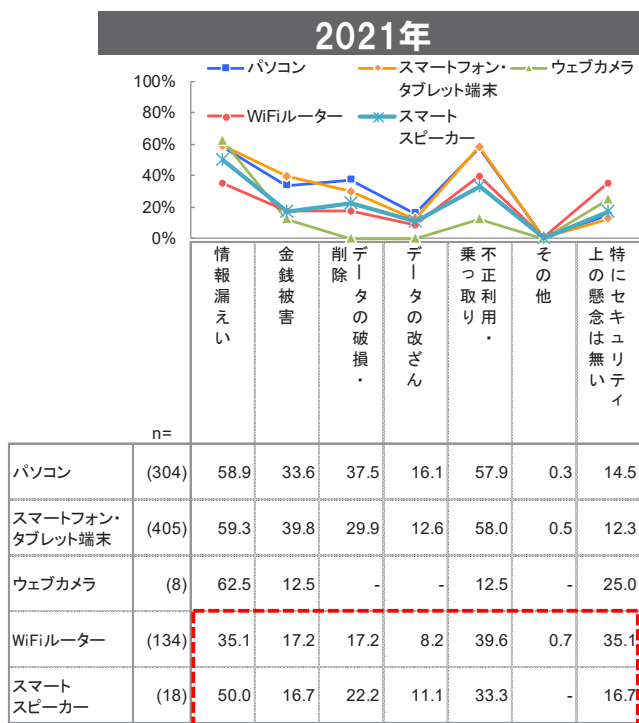
総じて「Wi-Fiルーター」「スマートスピーカー」では、「パソコン」「スマホ」に比べ、セキュリティ上の懸念を感じていない。

- セキュリティ上の懸念は、「Wi-Fiルーター」「スマートスピーカー」はいずれの事項も「パソコン」「スマホ」より低い。「Wi-Fiルーター」に関しては、3割半ばが「セキュリティ上の懸念は無い」と回答。2018年調査と比べても大きな変化は見られない。

Q4 あなたがインターネットに接続して使用している以下の電子機器について、どのようなセキュリティ上の懸念を感じますか。あてはまるものをすべてお答えください。

MA

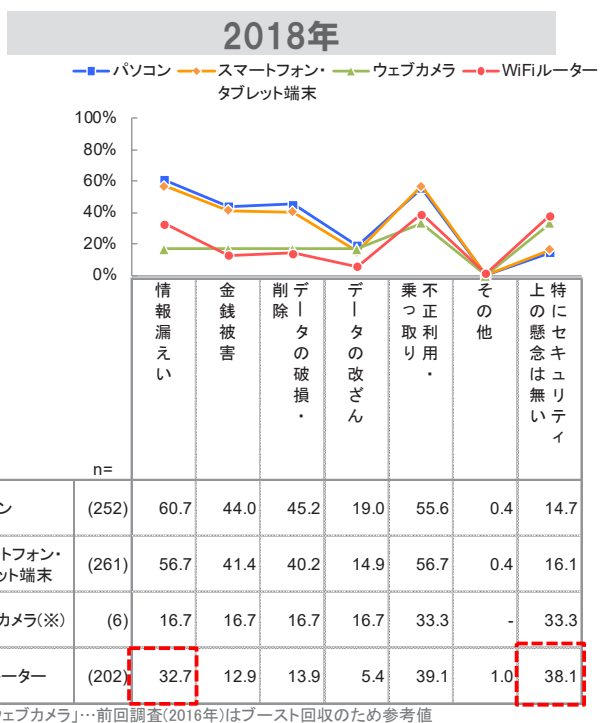
※各機器使用者ベース



© Macromill, Inc.

©ALL rights reserved by MCPC 2022

15



※:「ウェブカメラ」…前回調査(2016年)はブースト回収のため参考値

MACROMILL

モバイルコンピューティング推進コンソーシアム

問い合わせ窓口・サポートサービス期限への考え方

問い合わせ窓口・サポートサービス期限への考え方【重視度・許容度】

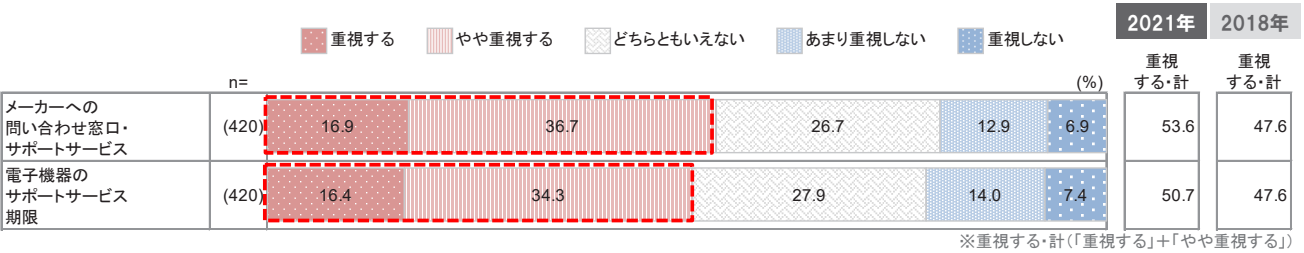
2018年調査と同様に、「問い合わせ窓口・サポートサービス」「サポートサービス期限」ともに、半数が「重視する」と回答。

「問い合わせ窓口・サポートサービス」は、「基本的に提供されている」、「サポートサービス期限」は「ある程度しょうがない」意識が強いことも、2018年度調査と同様で、変化は見られない。

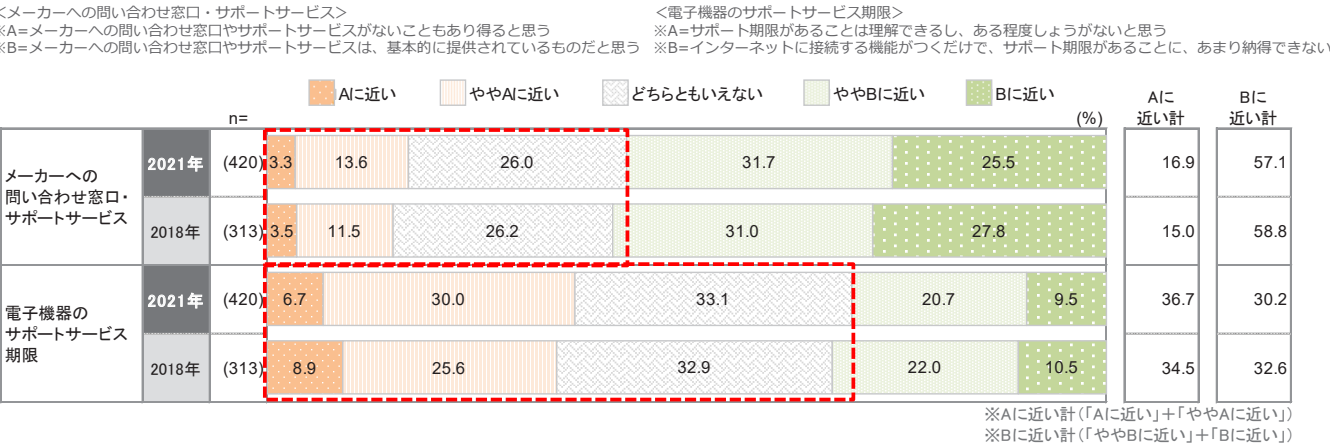
Q5 あなたは、インターネットに接続する電子機器を購入する際、メーカーへの問い合わせ窓口やサポートをどの程度重視しますか。
Q6 インターネットに接続する電子機器のメーカーのサポートサービスに対する考え方として、あなたのお考えにより近いものをそれぞれ1つお答えください。

SA

重視度



許容度

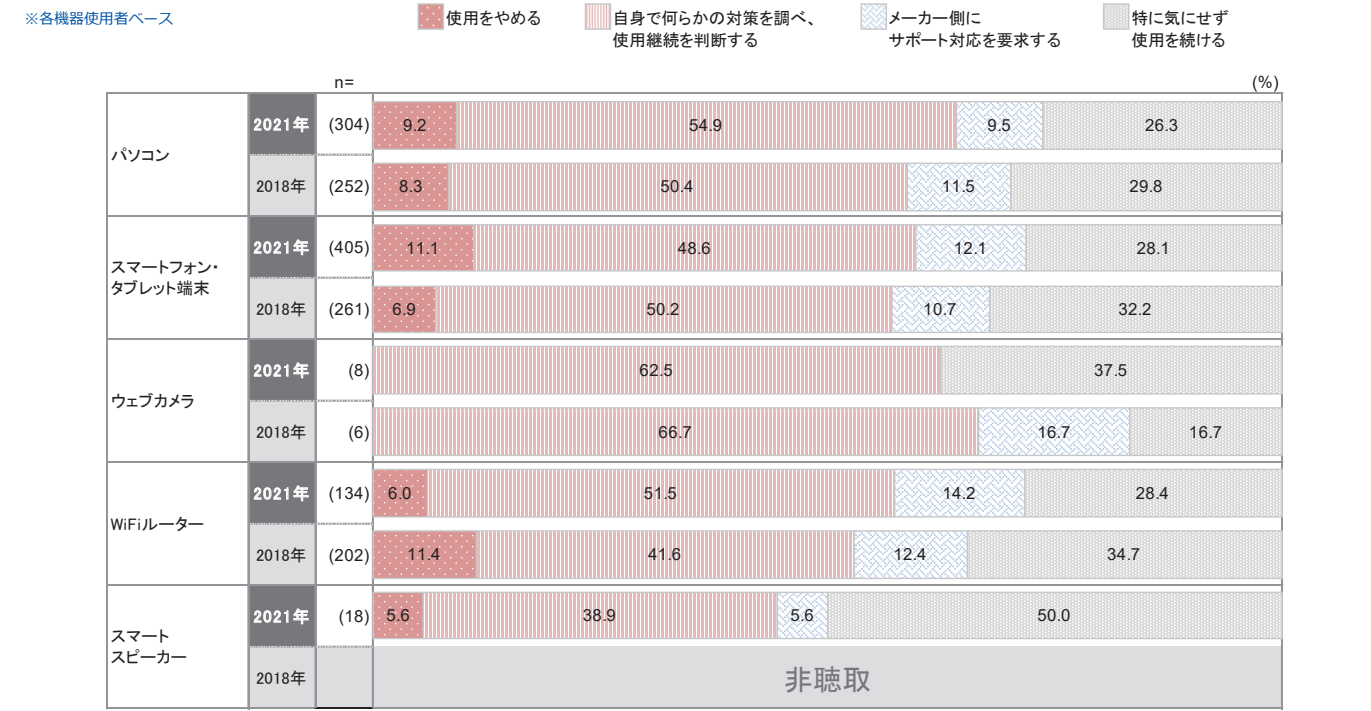


サポート期限到来時の行動

サポート期限が来た場合、「パソコン」「スマホ」「Wi-Fiルーター」は3割弱程度が、「スマートスピーカー」は半数が、「特に気にせず使用を続ける」と回答。

■ 2018年調査と同様に、「パソコン」「スマホ」「ウェブカメラ」「Wi-Fiルーター」とも使用者の約5割以上が「自身で何らかの対策を調べ、使用継続を判断する」と回答。「使用をやめる」方は「スマホ」で1割強、2018年調査からやや増加傾向。

Q7 インターネットに接続する電子機器のサポート期限が来た場合の考え方として、あなたのお考えに最も近いものを1つお答えください。 SA



初期設定に対する意識

パスワード設定の実態

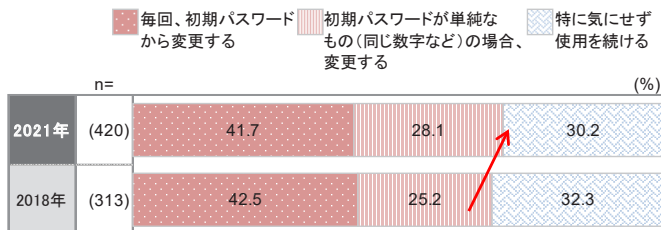
2018年調査と同様に、3割が初期パスワードを「特に変更しない」、4割半ばが「（どちらかといえば）同じパスワードを使い回す」。

- 2018年調査に比べて、初期パスワードを「特に変更せず」、「同じパスワードを使い回す」方が増加傾向にある。
- セキュリティに対する考え方も、基本的に「自身の対策に問題がある」「普段から自分で気を付けるべき」の回答が多数で、2018年調査と変化は見られない。

Q8 あなたは、インターネットに接続する電子機器の使用開始時に、パスワード設定を初期値から変更しますか。最も多いケースを1つお答えください。
Q9 あなたは、インターネットに接続する電子機器のパスワードをどのように設定しますか。ご自身により近いものを1つお答えください。
Q10 仮にあなたがお使いのインターネットに接続する電子機器が第三者による攻撃を受け、個人情報が流出したとします。その際のあなた自身のお考えとして、あてはまるものをすべてお答えください。

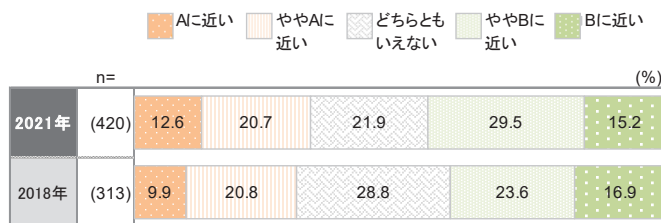
SA
SA
MA

初期パスワードの変更

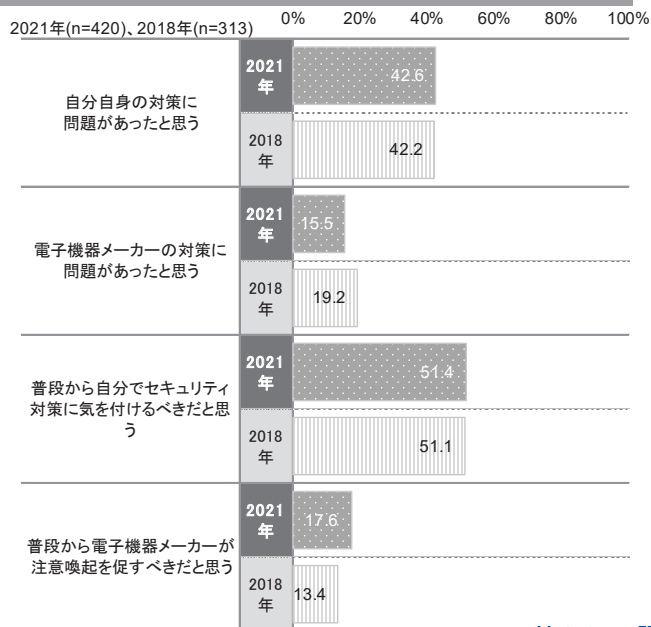


パスワードの設定

※A=それぞれ毎に、異なるパスワードを使用する
※B=同じパスワードを使い回す



セキュリティに対する考え方



© Macromill, Inc.

14

アップデートの実施と考え方

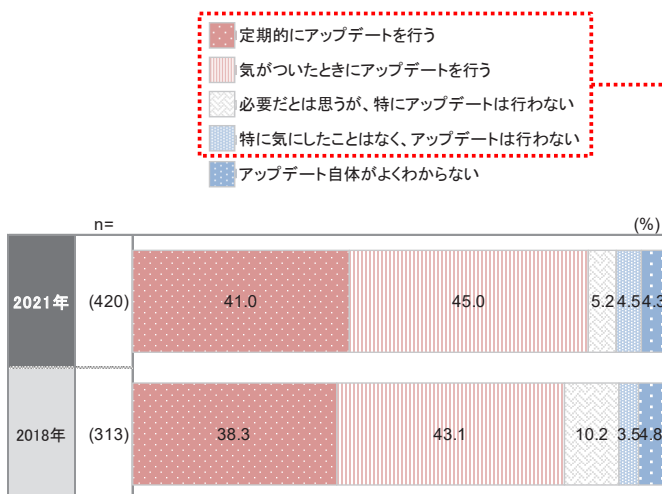
8割半ばがアップデート実施、「定期的な」アップデートは4割、2018年度調査からやや増加。特に行わない方は1割程度。

アップデート方法は、「メーカーからの通知」で「自分で」行うことを希望する方が多数だが、「メーカーが自動で」を希望する方も増加傾向にある。

Q11 あなたは、インターネットに接続する電子機器を使用する中で、取扱説明書等にあるアップデートを行いますか。
Q14 あなたは、インターネットに接続する電子機器のアップデートについて、誰がどのように行うのが良いと思いますか。あなたのお考えに最も近いものを1つお答えください。

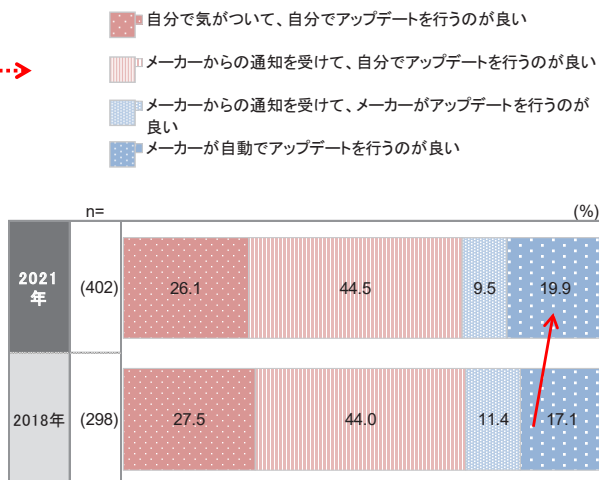
SA

アップデートの頻度



アップデートへの考え方

※アップデート理解者ベース



© Macromill, Inc.

15

MACROMILL

©ALL rights reserved by MCPC 2022

モバイルコンピューティング推進コンソーシアム

アップデートをしないことによる個人情報流出に対する危機感

7割半ばが、アップデートを行わない場合、「自分の機器でも個人情報流出し得る」と感じており、2018年調査より増加傾向。

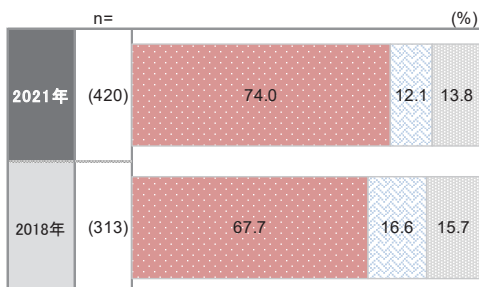
自身が使用している「Wi-Fiルーター」「スマートスピーカー」について、アップデートを行わないことによる個人情報の流出について、「パソコン」「スマホ」に比べ、流出の懸念を感じる方が少ない。

- Q12 インターネットに接続する電子機器のアップデートを行わないと、第三者による不正利用を受け、個人情報流出したり、機器が故障したりすることがあります。上記に対する、あなたの考えに最も近いものを1つお答えください。
- Q13 あなたがインターネットに接続して使用している以下の電子機器について、仮にアップデートを行わなかった場合、どの程度個人情報の流出や機器の故障が起きると思いますか。あなたのお考えに最も近いものをそれぞれ1つお答えください。

SA

個人情報流出への考え方

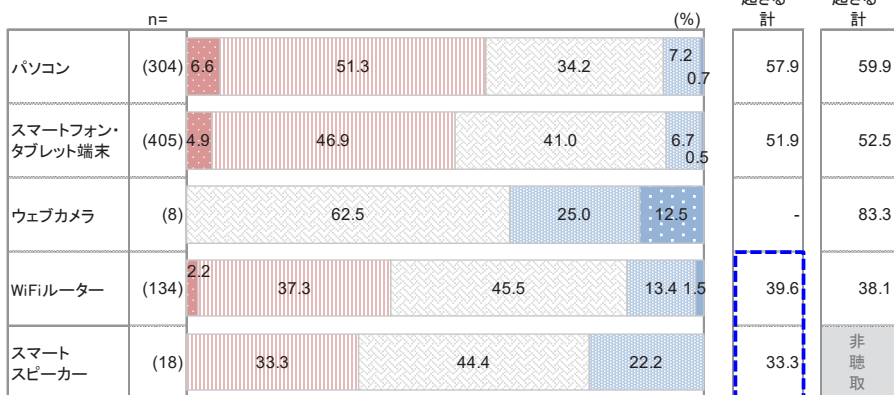
- 自身の使用する機器にも起こり得ることだと思う
- 知識として知っているが、自分の使用する機器で起こることではないように思う
- 知らなかった、考えたことがなかった



使用電子機器の個人情報流出

※各機器使用者ベース

- 必ず起きると思う
- 起きる可能性は高いと思う
- どちらともいえない
- 起きる可能性は低いと思う
- 絶対起きないと思う



※起きる・計（「必ず起きると思う」＋「起きる可能性は高いと思う」）

電子機器の電源、インターネット接続状況

電子機器の電源接続状況

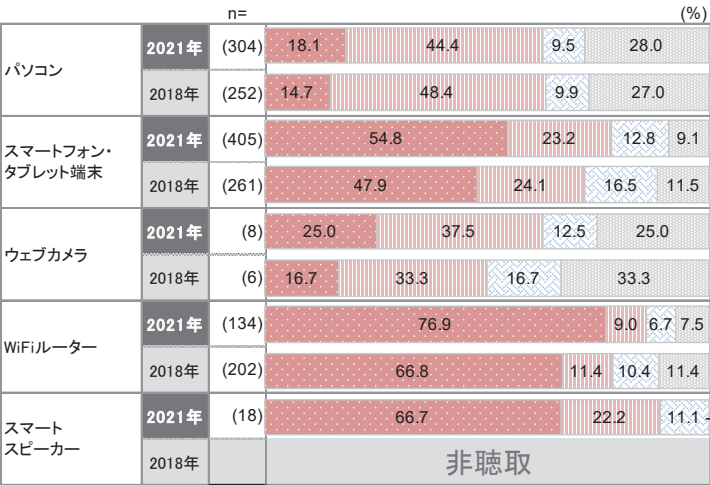
2018年度調査と同様に、いずれの機器も半数以上が「常にインターネットに接続」して機器を使用。
使用しなくなった機器についても、3割強は「常にインターネットに接続」していると回答しており増加傾向。

Q15 あなたがインターネットに接続して使用している以下の電子機器について、普段のインターネット接続および電源接続の状況として、最も近いものをそれぞれ1つお答えください。
Q16 あなたが、インターネットに接続して使用する機器のうち、【使用しなくなったもの】のインターネット接続および電源接続の状況として、最も近いものをそれぞれ1つお答えください。 SA

※各機器使用者ベース

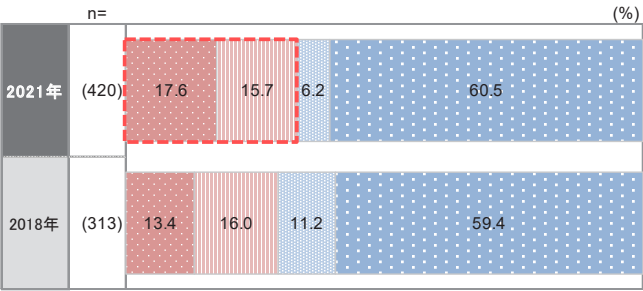
使用電子機器

- 常にインターネットに接続し、電源も入れている
- 常にインターネットに接続しているが、使用する時のみ電源を入れている
- 使用する時のみインターネットに接続し、電源は常に入れている
- 使用する時のみインターネットに接続し、使用する時のみ電源を入れている



使用しなくなった電子機器

- 常にインターネットに接続し、電源も入れている
- 常にインターネットに接続しているが、電源は入れていない
- インターネットには接続していないが、電源は常に入れている
- インターネットに接続しておらず、電源も入れていない



保存データに対する意識

電子機器の保存データに対する意識

「Wi-Fiルーター」使用者では、保存データを「把握」している方が2割台に留まり、「保存されていない」意識の方が3割半ば存在。

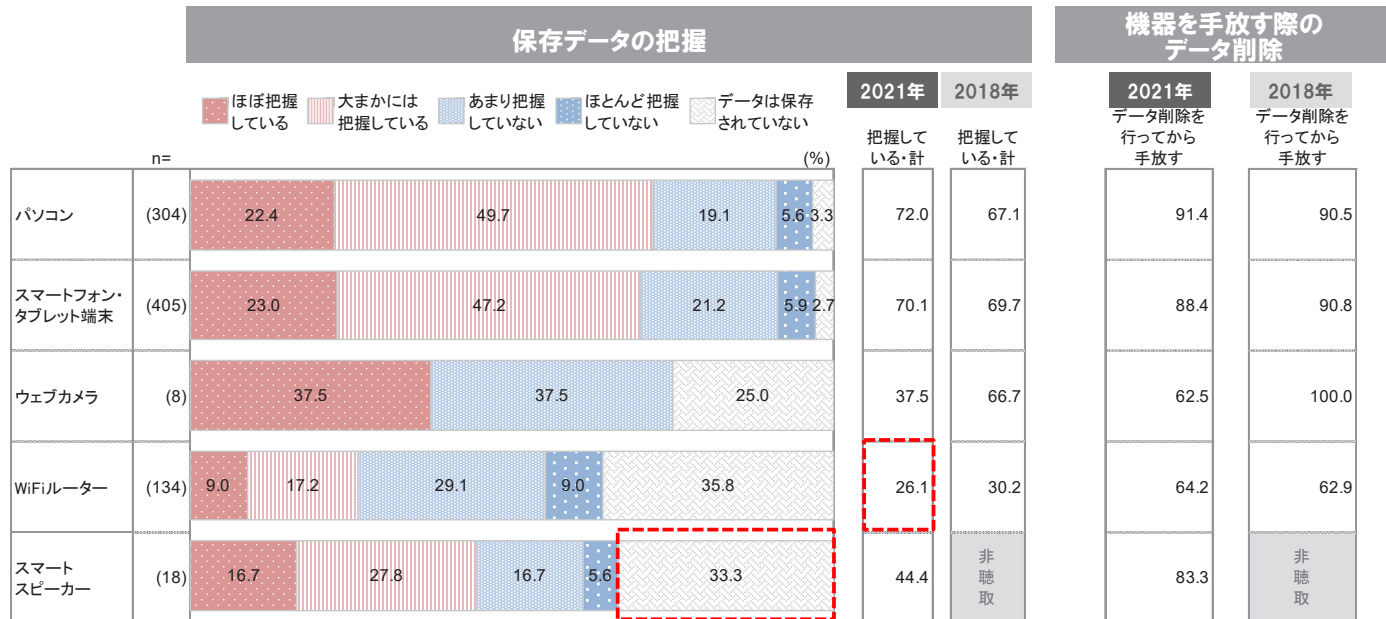
「スマートスピーカー」使用者も同様に「保存されていない」意識の方が3割強となっており、「パソコン」「スマホ」に比べて意識が低い。

機器を手放す際は、「スマートスピーカー」使用者の8割強がデータ削除について「データ削除を行ってから手放す」と回答。

- Q17 あなたがインターネットに接続して使用している以下の電子機器について、それぞれの機器にデータは保存されていますか。
また、保存されているデータ内容についてどの程度把握していますか。
Q18 あなたがインターネットに接続して使用している以下の電子機器について、仮に手放す（破棄・売却・譲渡など）ことになった場合、
何らかの方法でデータの削除を行うと思いますか。

SA

※各機器使用者ベース



※スコアは把握している・計（「ほぼ把握している」＋「大まかには把握している」）
20

© Macromill, Inc.

MACROMILL

WiFiルーター事例を通じたセキュリティ対策意識の変化

© Macromill, Inc.

©ALL rights reserved by MCPC 2022

21

モバイルコンピューティング推進コンソーシアム

21

呈示事例

Q19 呈示事例

機器自体には画像等の個人的なデータは保存されないが、クラウドサービス（ショッピング、動画配信、健康管理等）のアカウントと紐づけて利用していた電子機器を、紐づけの情報を削除せずに廃棄してしまい悪用された事例

© Macromill, Inc.

22

MACROMILL

アカウント悪用事例認知度

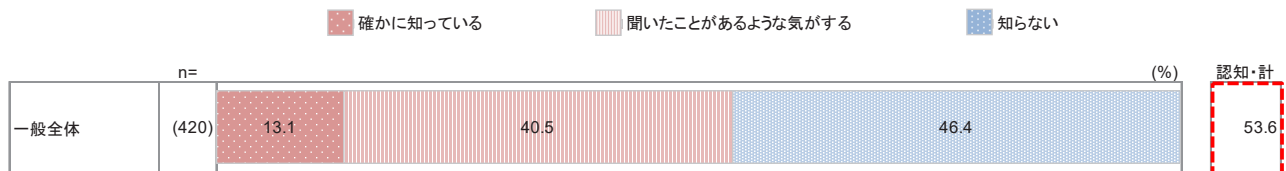
事例認知は、全体で5割強。事例認知後のデータ削除意向は、「パソコン」「スマホ」で9割強、「スマートスピーカー」で8割強、「Wi-Fiルーター」で7割半ば。「ウェブカメラ」は事例認知前後でデータ削除以降に大きな違いが見られる。

Q19 あなたは、インターネットに接続された電子機器に関する上記の事例をご存知ですか。
Q20 改めて上記のような事例をご覧になり、あなたがインターネットに接続して使用している以下の電子機器について、仮に手放す（破棄・売却・譲渡など）ことになった場合、何らかの方法でデータの削除を行うと思いますか。

SA

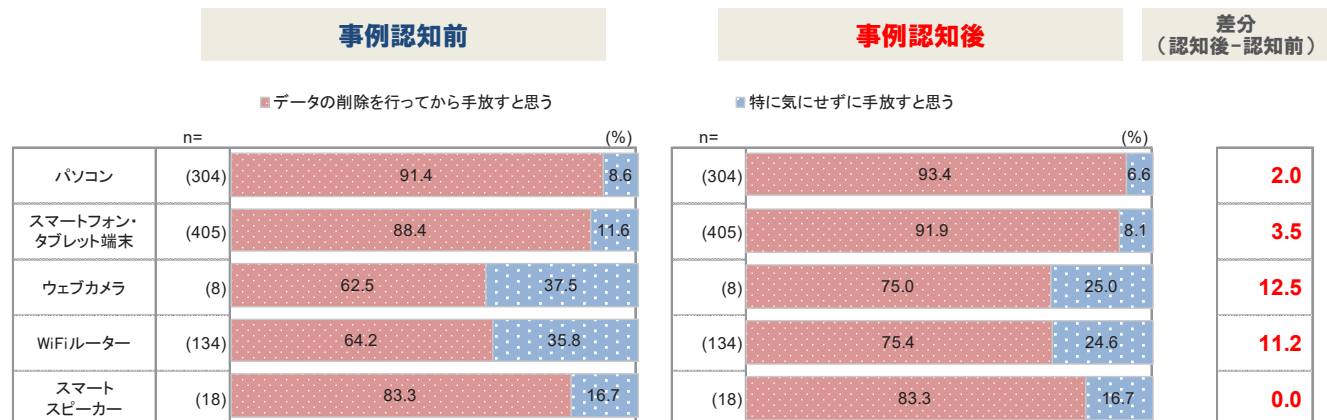
MTS

認知度



※スコアは認知・計（「確かに知っている」+「聞いたことがあるような気がする」）

データの削除



© Macromill, Inc.

23

MACROMILL

©ALL rights reserved by MCPC 2022

モバイルコンピューティング推進コンソーシアム

事例認知度/セキュリティ対策費用感

「インターネットに接続されたウェブカメラが、外部から自由にのぞき見された事例」「インターネットに接続された電子機器がマルウェアに感染し、サイバー攻撃の踏み台として悪用された事例」いずれも7割強が認知。

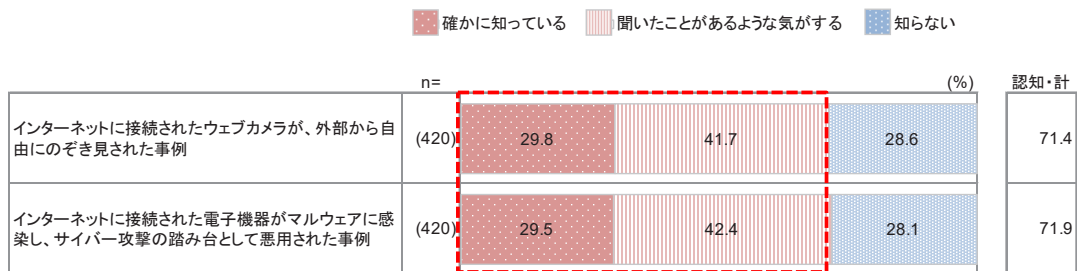
事例認知後のセキュリティ対策費用感は、「セキュリティ重視・計」が6割強と「価格重視・計」の1割を大きく上回る。

Q22 あなたは、インターネットに接続された電子機器に関する以下の事例をご存知ですか。

Q23 改めて上記のような事例をご覧になり、あなたが、インターネットに接続する電子機器を購入するにあたり、セキュリティ対策やサポートの有無による価格差があった場合の考え方として、あなたのお考えにより近いものを1つお答えください。

SA

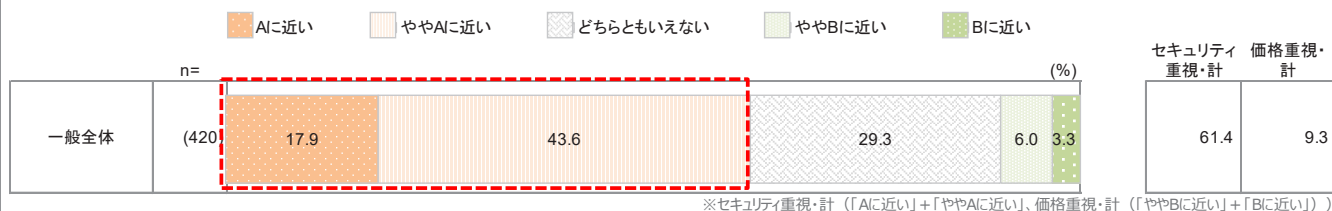
認知度



※スコアは認知・計（「確かに知っている」＋「聞いたことがあるような気がする」）

※A=価格が高くてもセキュリティ対策やサポートが充実しているものを買う
※B=セキュリティ対策やサポートはやや弱い、価格が安いものを買う

セキュリティ対策



© Macromill, Inc.

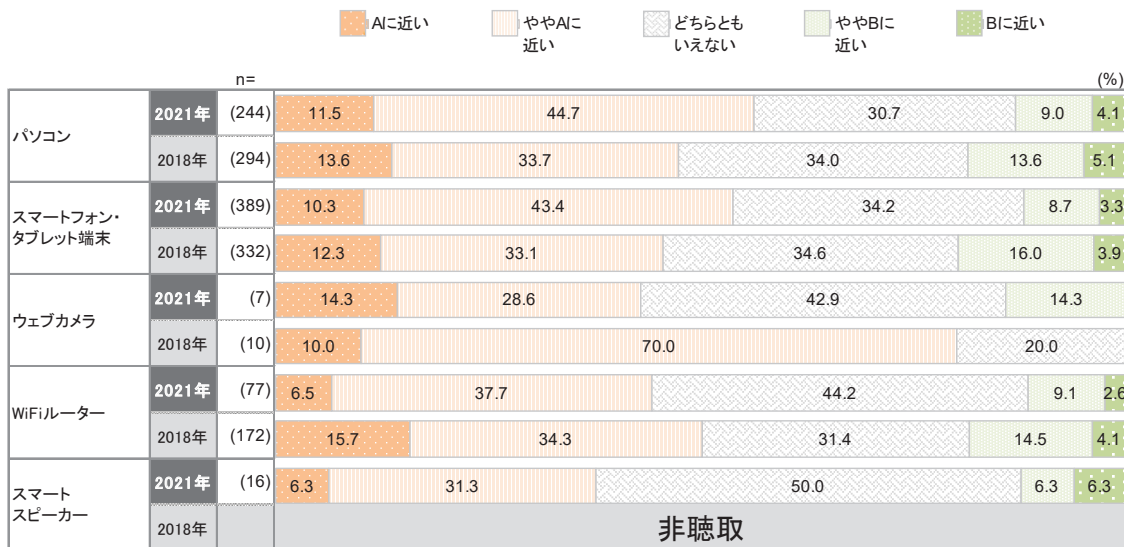
24

MACROMILL

【参考】機器別 セキュリティ対策費用感

Q21 あなたが、インターネットに接続する電子機器を購入するにあたり、セキュリティ対策やサポートの有無による価格差があった場合の考え方として、あなたのお考えにより近いものを1つお答えください。※プライベートで使用するものについてお答えください。

※A=価格が高くてもセキュリティ対策やサポートが充実しているものを買う
※B=セキュリティ対策やサポートはやや弱い、価格が安いものを買う



© Macromill, Inc.

25

MACROMILL

©ALL rights reserved by MCPC 2022

モバイルコンピューティング推進コンソーシアム

MCPC セキュリティ委員会

「IoT セキュリティガイドラインに対する 一般利用者の意識の実態調査（その３）」

<企画・編集メンバー>

セキュリティ委員会委員長	井上 栄	FCNT 株式会社
副委員長	窪田 歩	KDDI 株式会社
副委員長	鷲尾 諭	株式会社 NTT ドコモ
アドバイザー	華井 克育	
メンバー	安達 智雄	日本電気株式会社
	岩木 邦彦	ソフトバンク株式会社
	大塚 拓也	株式会社エヌアイデイ
	原 聖樹	トレンドマイクロ株式会社
	濱田 圭	富士通クライアントコンピューティング株式会社
	小島 純一	一社 情報通信ネットワーク産業協会
	島本 幸夫	株式会社日立製作所
事務局	前島 幸仁	MCPC

企画・編集メンバーは 2022 年 3 月現在のメンバーです。

【MCPC について】

ワイヤレスデータ通信とコンピューティングシステム（モバイルシステム）の普及を促進するために、1997 年我が国を代表する移動体通信会社、コンピュータハードウェア / ソフトウェア会社、携帯電話、システムインテグレータなどにより組織化されました。現在、世界をリードするワイヤレステクノロジーで最先端の IoT・AI ソリューション追求し飛躍的発展を目指しており、そのための技術課題への対応、運用課題の調査・研究、開発の推進、標準化、相互接続性検証、普及啓発活動、人材育成などの活動を行っています。さらには、米国姉妹組織の USB-IF、Bluetooth SIG などと連携を図りながら、モバイル利活用 of IoT・AI ソリューションの市場拡大と利用環境の高度化に務めています。

（2022 年 3 月現在 会員会社数 178 社）

D X を 推 進 す る MCPC

調査報告書

「IoT セキュリティガイドラインに対する 一般利用者の意識の実態調査（その3）」

発 行 元 モバイルコンピューティング推進コンソーシアム（MCPC）
発 行 日 2022 年 3 月 31 日
製作／編集 MCPC セキュリティ委員会

問合わせ先：MCPC 事務局

〒105-0011 東京都港区芝公園 3-5-12 長谷川グリーンビル 2 階

TEL：03-5401-1935

FAX：03-5401-1937

E-mail：office@mcpc-jp.org

URL：<https://www.mcpc-jp.org/>



本冊子の一部あるいは全部について、モバイルコンピューティング推進コンソーシアム（MCPC）から文書による承諾を得ることなしに、いかなる方法においても無断で複写・複製・転載することを禁じます。