

本調査結果は、総務省の「令和5年度無線LANセキュリティに係る実態調査の請負業務」事業（受託者：株式会社ITグローバルブレイン）により作成したものを、総務省で一部加工の上、公表するものです。

本資料に関する問合せ先等は次のページを確認願います。

https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/

令和5年度
無線LANのセキュリティに係る
実態調査報告書

令和6年3月
株式会社ITグローバルブレイン

目 次

第 1 章 調査目的.....	4
第 1 節 調査概要.....	4
1-1 調査目的.....	4
1-2 調査内容.....	4
第 2 節 体制・スケジュール.....	4
2-1 業務実施体制.....	4
2-2 スケジュール.....	5
第 2 章 無線 LAN のセキュリティ実態調査.....	6
第 1 節 無線 LAN 利用者調査.....	6
1-1 調査概要.....	6
1-2 調査票.....	7
1-3 無線 LAN 利用の状況.....	8
第 2 節 無線 LAN 提供者に対するアンケート調査.....	89
2-1 調査概要.....	89
2-2 調査結果概要.....	91

第1章 調査目的

第1節 調査概要

1-1 調査目的

自宅等において無線 LAN の利用はもはや日常になり、観光や防災の観点等からも公衆無線 LAN の普及が進んできているが、その中にはセキュリティ対策が十分でないものも多く、無線 LAN を踏み台にした攻撃や情報漏洩等のインシデントの発生が懸念されている。

無線 LAN について、その利用者が快適で安全に利用するためには、利用者が、その利用に際しての情報セキュリティ上の脅威を正しく認識して適切な情報セキュリティ対策を行うことに加え、提供者が、アクセスポイントに適切な設定を行った上で設置・運用を行うなど、無線 LAN の利用者・提供者の双方の取組が重要である。

こうした状況を踏まえ、無線 LAN を誰もが安心して快適に利用できるようにするため、無線 LAN のセキュリティ実態調査を行い、関連ガイドラインの改定や新規策定について検討の材料とすることを目的とし、これにより無線 LAN の不適切な利用による周波数の逼迫を防ぎ、無線 LAN の利用を含む IoT の安心・安全かつ適正な利用環境を構築することを目的とする広報活動で使用予定としており、当該取組を通じて電波の能率的な利用を確保するためのリテラシー向上をはかるものである。

1-2 調査内容

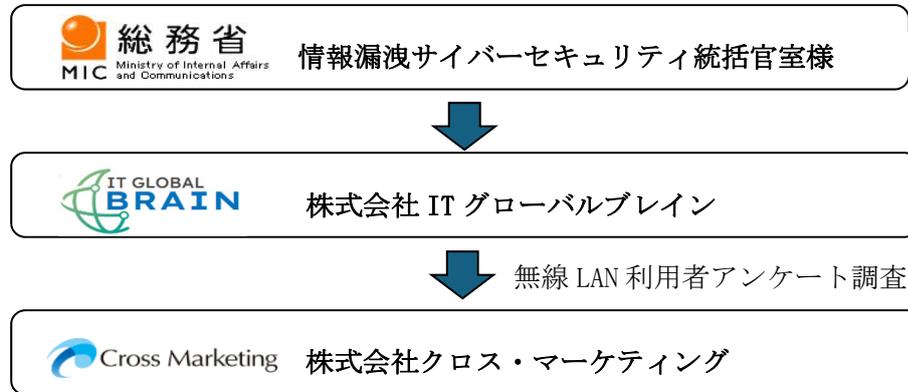
上記の目的を達するため、主として、「無線 LAN のセキュリティ実態調査（無線 LAN 利用者に対する調査）（以下、無線 LAN 利用者調査）」及び「無線 LAN のセキュリティ実態調査（無線 LAN 提供者に対する調査）（以下、無線 LAN 提供者調査）」を行う。

第2節 体制・スケジュール

2-1 業務実施体制

業務の実施にあたっては、総務省サイバーセキュリティ統括官室様との連携により実施した。

図表 1 業務実施体制



2-2 スケジュール

令和 6 年 1 月 22 日から令和 6 年 3 月 31 日に業務を実施した。

第2章 無線 LAN のセキュリティ実態調査

第1節 無線 LAN 利用者調査

1-1 調査概要

第1章の目的を達成するため、無線 LAN のセキュリティ実態調査を実施した。

無線 LAN の利用状況及びセキュリティ対策状況に関して、Web アンケートによる調査を実施した。

調査対象は、日常的にスマートフォン、タブレット端末、パソコン等で無線 LAN（公衆無線 LAN に限らない。）を利用している者とし、特定の年代や居住地域に偏らないように実施した。

具体的には、インターネット調査会社のモニタを対象として、インターネット上での WEB 調査を実施した。調査は、プレ調査（スクリーニング調査）を経て、無線 LAN 利用者を対象とした本調査を実施する二段階の調査とした。

■対象地域：全国

■有効回答数

【プレ調査（スクリーニング調査）】：1,422 標本

【本調査】：1,000 標本

■サンプリング

【プレ調査（スクリーニング調査）】

株式会社クロス・マーケティングが保有するリサーチパネルを用いて、15 歳以上 79 歳以下のモニタを自然抽出した。

【本調査】

プレ調査（スクリーニング調査）において、現在、自宅での無線 LAN または公衆無線 LAN を利用していると回答した利用者を抽出。

ただし抽出は、性・年代ごと及び居住地ごとに回答者を次の通り割り付けて実施した。

性年代：均等（男女／20 代以下・30 代・40 代・50 代・60 代以上）

居住地：エリア別人口比

北海道・東北：北海道、青森県、岩手県、宮城県、秋田県、山形県、福島県
関東：茨城県、栃木県、群馬県、埼玉県、千葉県、東京都、神奈川県
中部：新潟県、山梨県、長野県、富山県、石川県、福井県、岐阜県、静岡県、愛知県
近畿：三重県、滋賀県、和歌山県、京都府、大阪府、兵庫県、奈良県
中国：鳥取県、島根県、岡山県、広島県、山口県
四国：徳島県、香川県、愛媛県、高知県
九州・沖縄：福岡県、佐賀県、長崎県、熊本県、大分県、宮崎県、鹿児島県、沖縄県

■調査期間

【プレ調査（スクリーニング調査）および本調査】

令和6年3月4日(月)～3月8日(金)

1-2 調査票

調査票を参考資料に示す。

プレ調査（スクリーニング調査）においては、無線 LAN 利用の概況について把握し、本調査においては、自宅での無線 LAN 利用について、公衆無線 LAN サービス利用について、その他、を把握した。

1-3 無線 LAN 利用の状況

アンケート調査によって得られた無線 LAN 利用の状況を以下に示す。
今年度は、過去の調査とは調査対象の母集団が違っている。そのため、これまでの傾向と異なる結果が出ている可能性がある。

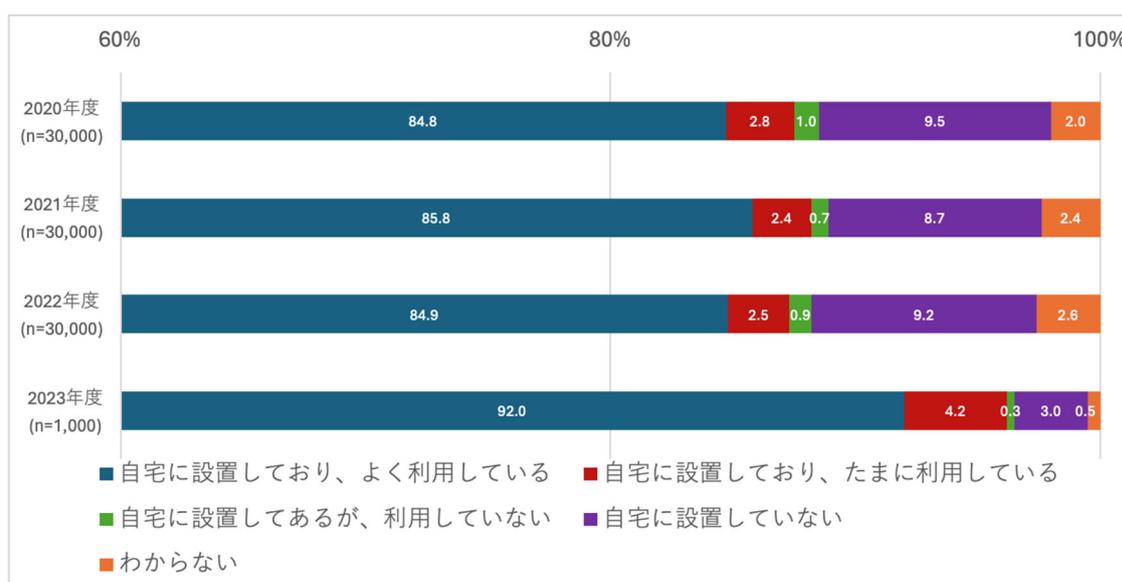
(1) 自宅に設置する無線 LAN (その 1)

① 自宅無線 LAN の利用有無 (SC5)

自宅で無線 LAN を利用しているユーザは、全体の約 96%とほとんどの家庭で利用されている。

利用率は、毎年、87~88%程度の利用率であったものが、今年度は 92%となっており、十分に普及しきったサービスになっていると言える。

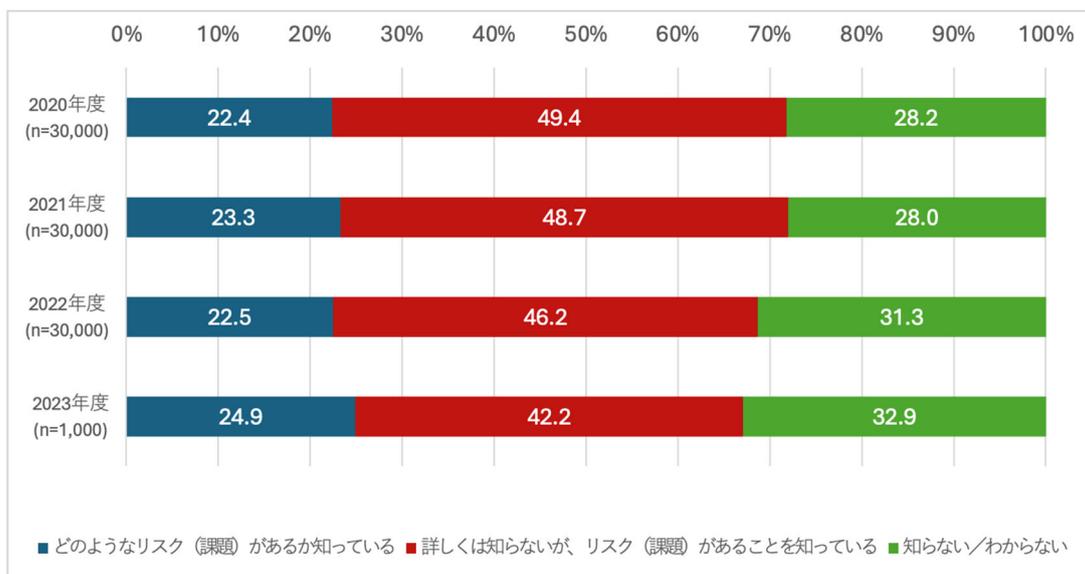
図表 2-1- 1 自宅無線 LAN の利用有無 (SC5)



② 無線 LAN 利用時におけるセキュリティ上のリスク認知 (SC10)

無線 LAN を利用する際に、設定や利用方法に注意しておかないと、セキュリティ上のリスクがあることを知っている人が全体の約 67%で、年々低下傾向にある。一方で、リスクの内容まで知っている人は約 25%になっており、リスク認知度は少し高まってきたと言える。

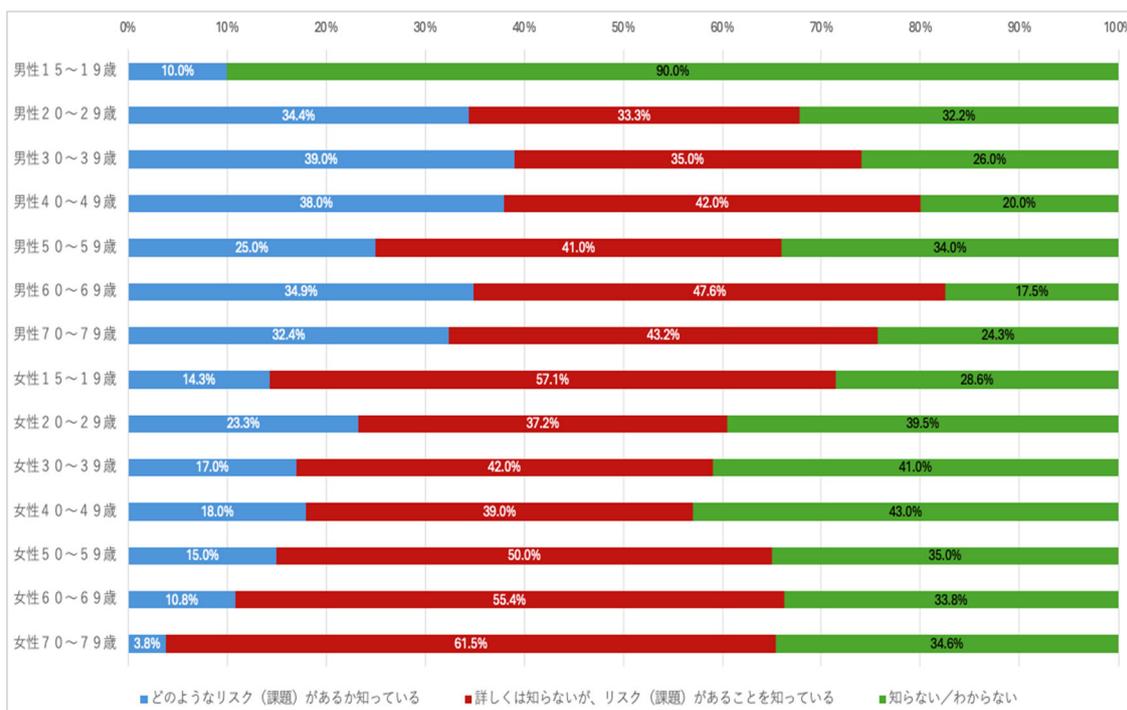
図表 2-1- 2 無線 LAN 利用時におけるセキュリティ上のリスク認知 (SC10)



全体的に男性にはリスク認知層のユーザが多く、女性には少ない傾向がある。

また、若年層にはリスク認知層が多く、高年層には少ない。特に、女性では、20歳から39歳の層が、顕著にリスク不認知層が多い傾向にあると言える。

図表 2-1- 3 無線 LAN 利用時におけるセキュリティ上のリスク認知 (SC10) × 性年代

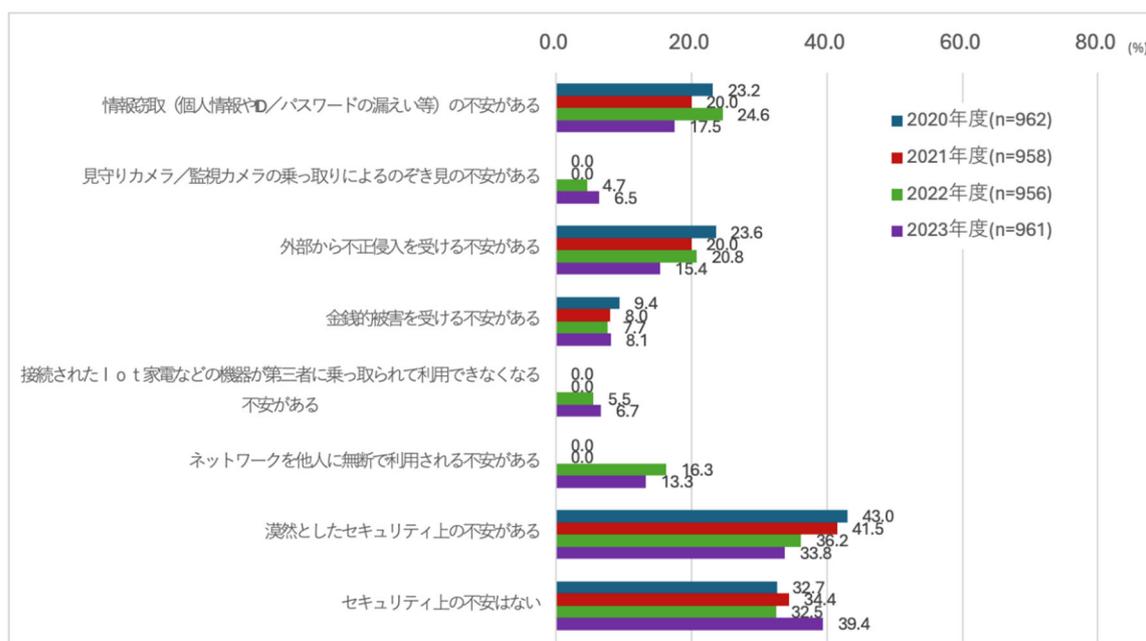


③ 自宅無線 LAN でのセキュリティ上の不安 (Q15)

自宅無線 LAN 利用者のうち、約 60%が何らかのセキュリティ上の不安を抱いているが、その過半の約 34%は漠然とした不安を抱いている状態である。ただ、年々減少している。

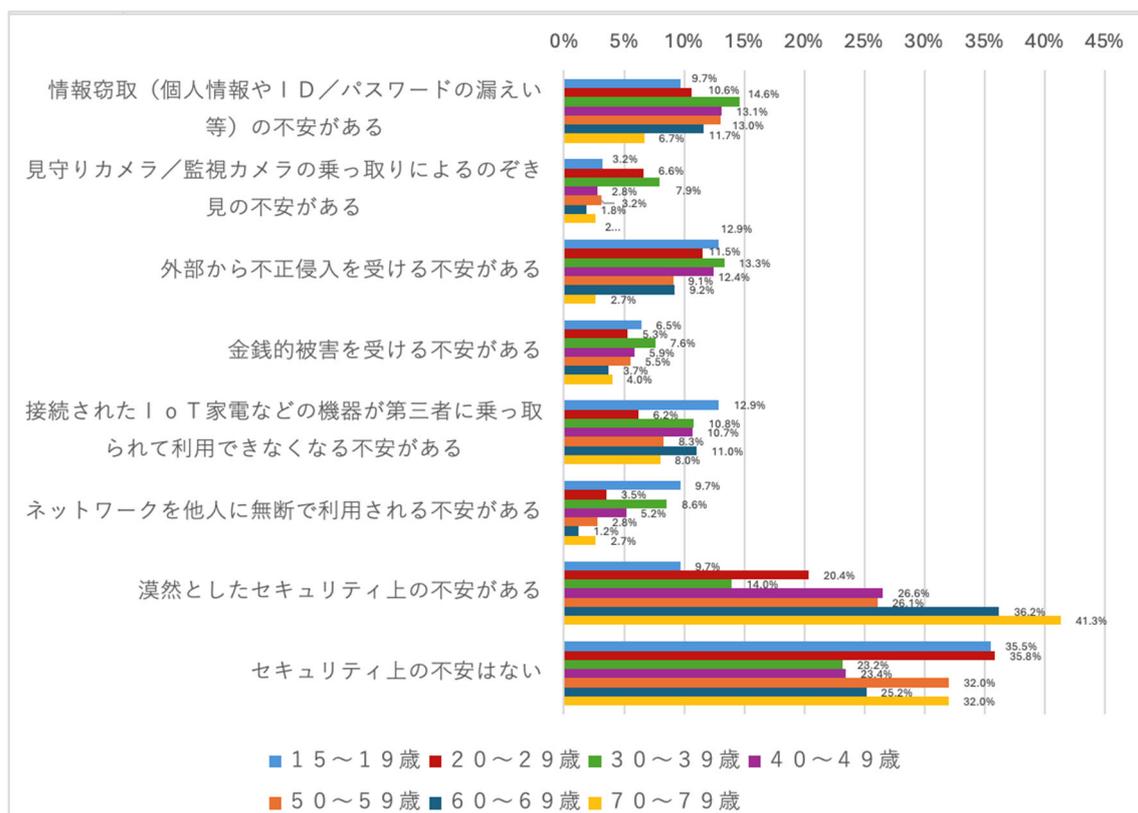
具体的な不安としては、情報窃取(約 18%)や外部からの不正侵入(約 16%)などの比率が高いが、この4年で、不安を感じることは減少しつつある。

図表 2-1- 4 自宅無線 LAN でのセキュリティ上の不安 (Q15)



30歳代の自宅無線LAN利用者を中心に、情報窃取や不正侵入に対する不安感が強い。高年層（60歳以上）の自宅無線LAN利用者は漠然とした不安を抱く一方、若年層（15歳から29歳）の自宅無線LAN利用者にはセキュリティ上の不安を感じない人が多い。また、70歳以上で、セキュリティ上の不安はないという人が目立っている。

図表 2-1- 5 自宅無線LANでのセキュリティ上の不安 (Q15) ×年代

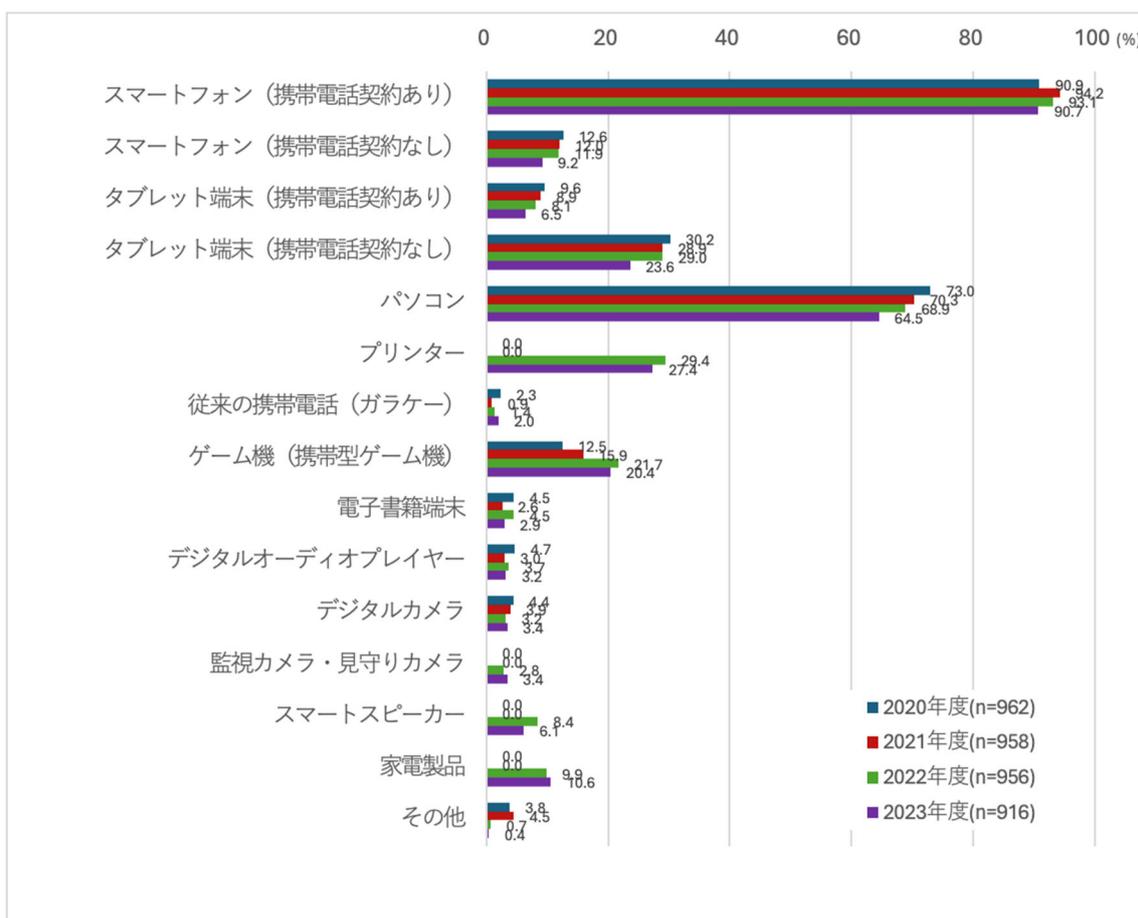


④ 自宅無線 LAN 利用端末 (Q1)

自宅無線 LAN ユーザが接続して利用するデバイスで最も多いものはスマートフォン (SIM あり) で約 91%。次いで、パソコン (約 65%)、プリンター (約 27%)、タブレット端末 (SIM なし) (約 24%)、ゲーム機 (約 20%) などである。

近年は、家電製品 (約 11%)、スマートスピーカー (約 6%) を接続するユーザも多くなっている。

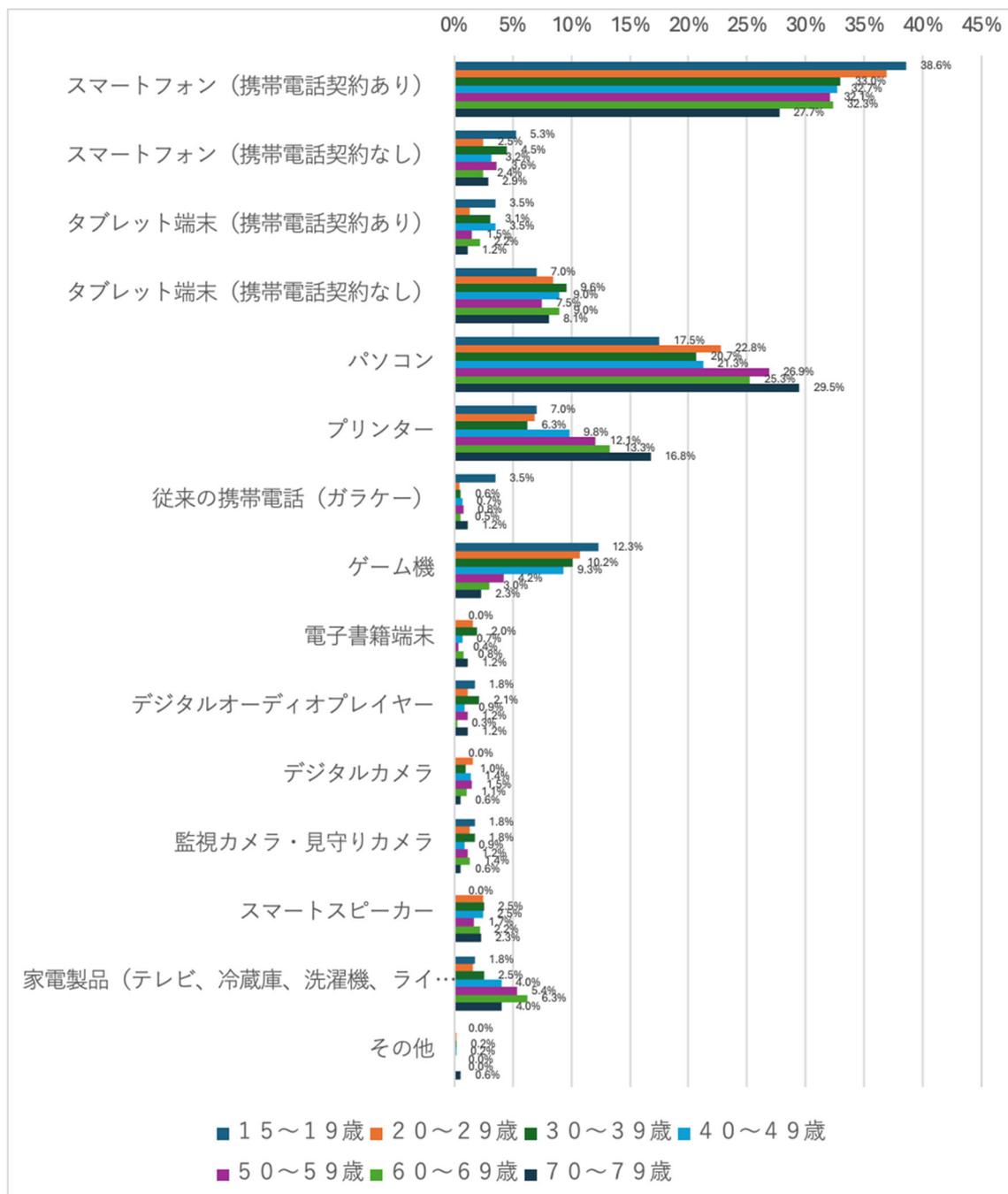
図表 2-1- 6 自宅無線 LAN 利用端末 (Q1)



自宅無線 LAN ユーザが接続して利用するデバイスで最も多いものは年齢に関わらずスマートフォン(SIMあり)。続いて、パソコン、プリンターである。

高年層の自宅無線 LAN ユーザは、パソコンを接続している比率が高い一方、ゲーム機を接続している比率がかなり低い。若者層は、ゲーム機の接続が目立つ。

図表 2-1- 7 自宅無線 LAN 利用端末 (Q1) ×年代

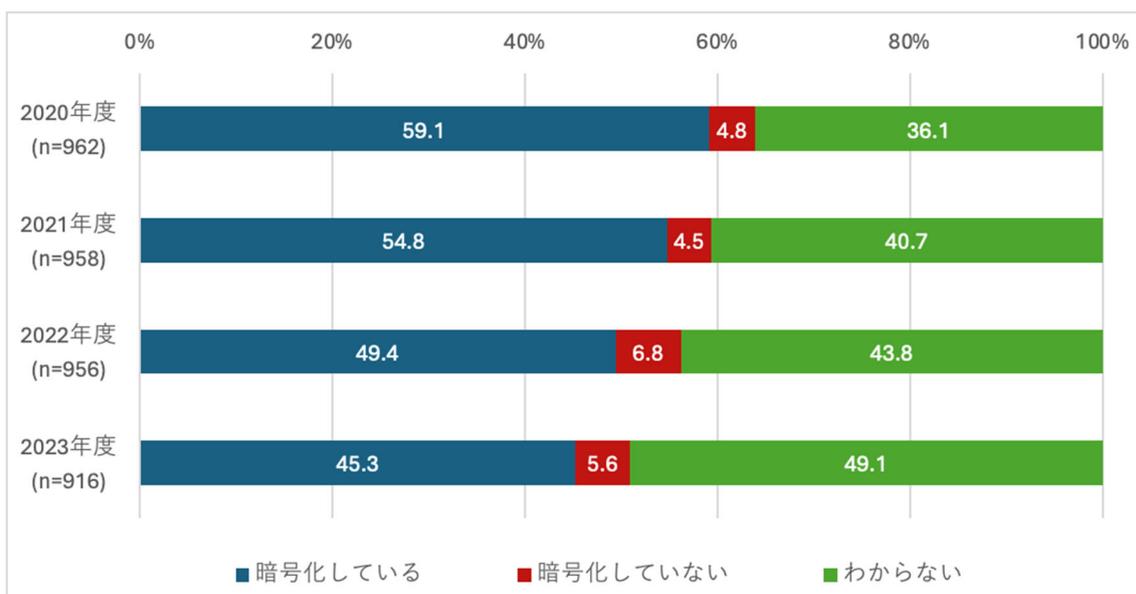


⑤ 自宅無線 LAN の暗号化 (Q6)

自宅の無線 LAN の無線を暗号化しているユーザの比率は約 45%に留まり、年々、暗号化率が低下している。

ただし、暗号化の有無が分からないユーザの比率が年々、高くなっており、「暗号化していないユーザが増えている」と言うよりは、「暗号化が分からないユーザが増えている」と言えそうである。

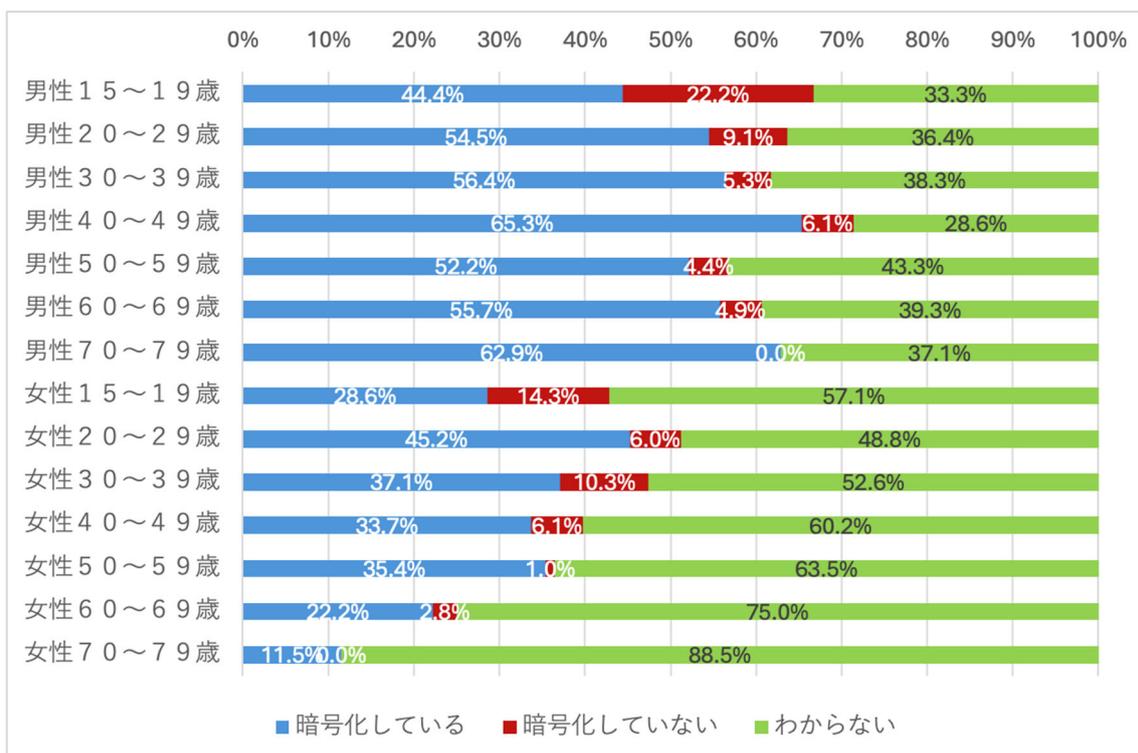
図表 2-1- 8 自宅無線 LAN の暗号化 (Q6)



男性の自宅無線 LAN ユーザは、無線を暗号化している比率が高いが、女性は認識していないユーザが多い。

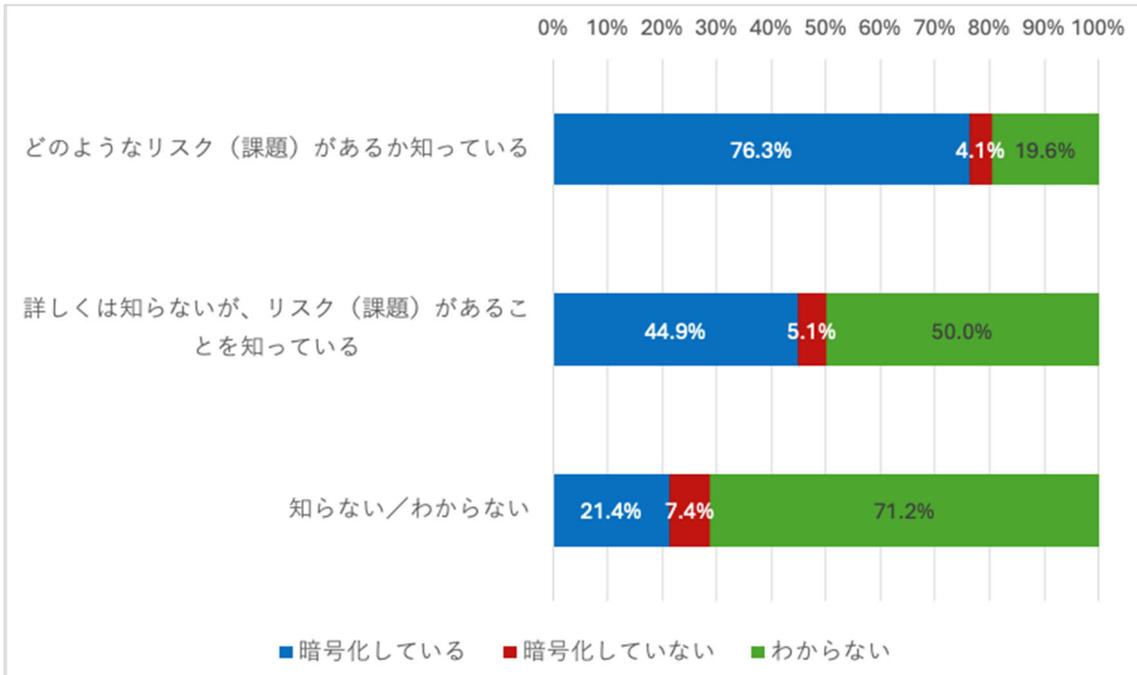
特に、若年層（15 歳から 19 歳）と高年層の女性ユーザは暗号化を認識していない傾向が強い。

図表 2-1- 9 自宅無線 LAN の暗号化 (Q6) ×性年代



無線 LAN のリスクを認知している自宅無線 LAN ユーザは、約 76%が無線を暗号化しているのに対して、リスクを認知していない自宅無線 LAN ユーザの約 71%は暗号化を認識していない。

図表 2-1- 10 自宅無線 LAN の暗号化 (Q6) × リスク認知

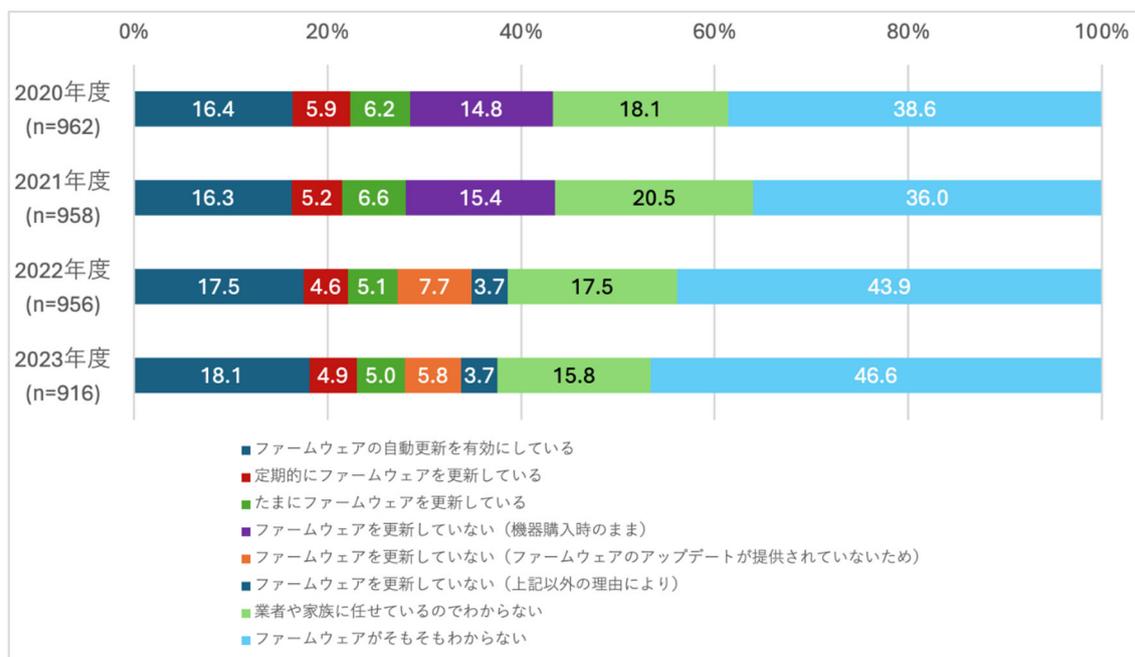


⑥ 自宅無線 LAN のファームウェア更新 (Q13)

自宅無線 LAN ユーザのうち、AP(親機)のファームウェアを着実に更新している(自動更新+定期的更新)ユーザは約 23%に留まるが、増える傾向がある。

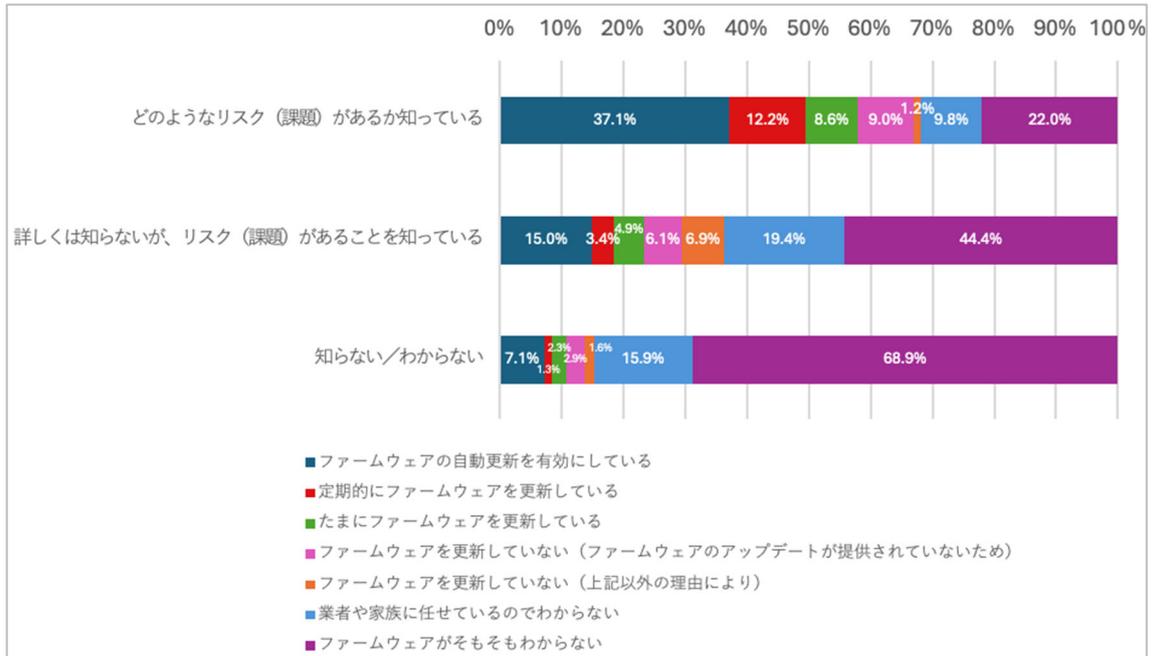
また、毎年ファームウェアが分からないユーザの比率が大きく増加している。

図表 2-1- 11 自宅無線 LAN のファームウェア更新 (Q13)



自宅無線 LAN ユーザのうち、無線 LAN のリスクを認知している層は、AP(親機)のファームウェアを着実に更新している(自動更新+定期的更新)ユーザが多く、5割を超えている。リスクを認識していない層は1割に満たず、7割以上がファームウェアが分からない。

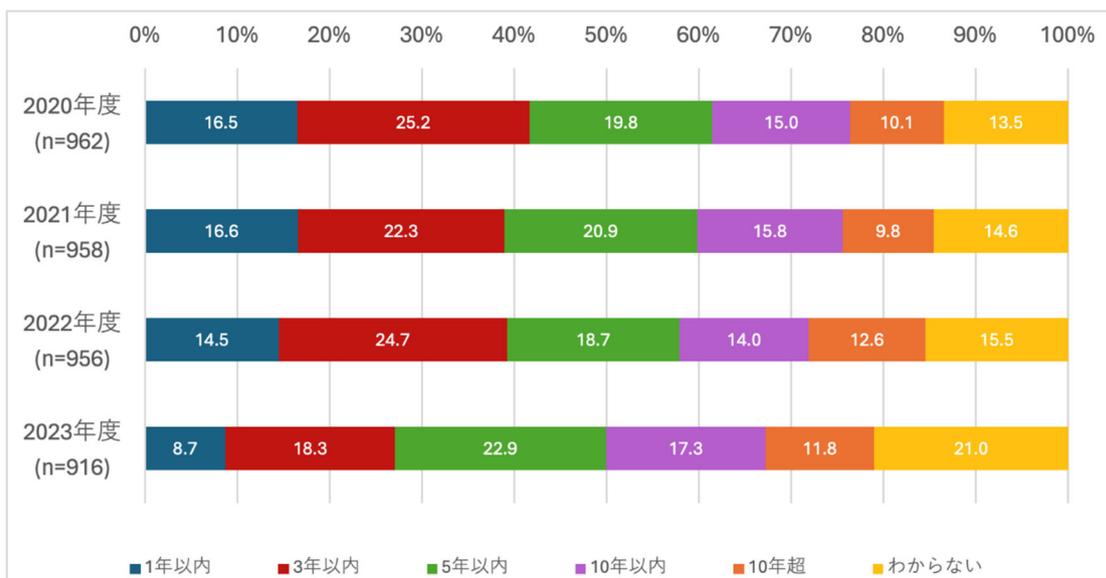
図表 2-1- 12 自宅無線 LAN のファームウェア更新 (Q13) × リスク認知



⑦ 自宅無線 LAN の購入時期 (Q2)

自宅の無線 LAN が十分に普及しきったサービスになっている傾向を反映して、購入後 5 年超の AP(親機)を使用しているユーザが約 29%いるのに加え、購入時期が分からないユーザが約 21%など、古い AP(親機)を利用しているユーザが、年々、増加している。

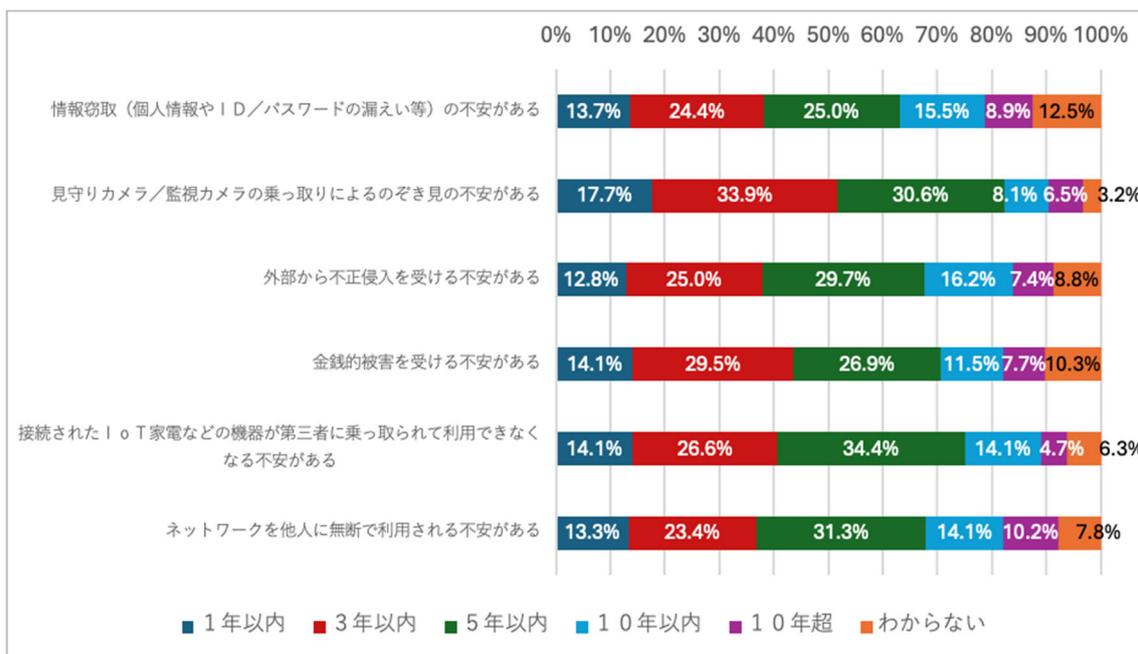
図表 2-1- 13 自宅無線 LAN の購入時期 (Q2)



自宅の無線 LAN について、接続機器（カメラや IoT 家電など）の乗っ取りを不安に思うユーザでは、新しい AP(親機)を使用している比率が高く、より安全な機器利用の動機になっている可能性が高い。

他方、漠然としたセキュリティ上の不安があるユーザやセキュリティについて不安を持たないユーザは、比較的古い AP(親機)を使い続けている傾向が認められる。

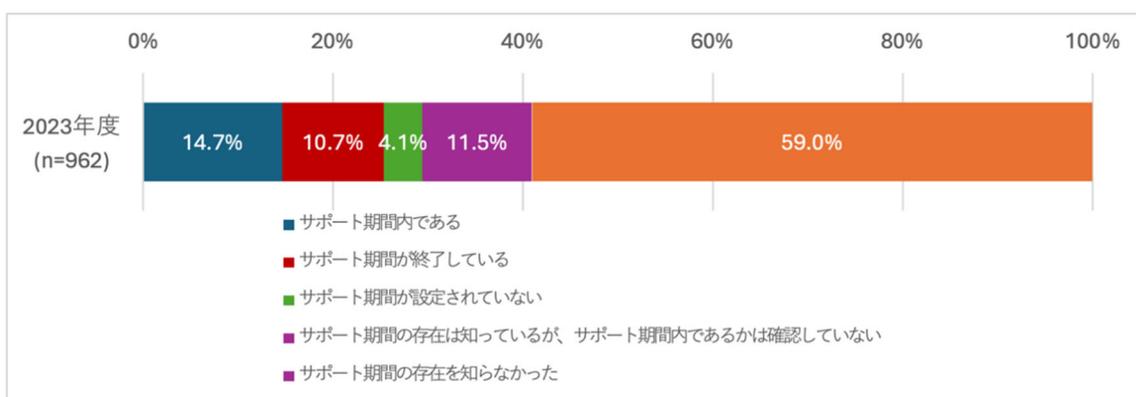
図表 2-1- 14 自宅無線 LAN の購入時期 (Q2) ×自宅無線 LAN のセキュリティ上の不安



⑧ 自宅無線 LAN のサポート期間 (Q14)

自宅の無線 LAN の AP(親機)について、明確にサポート期間内であると認識しているユーザは約 15%に過ぎず、約 71%のユーザは、サポート期間を認識していない。

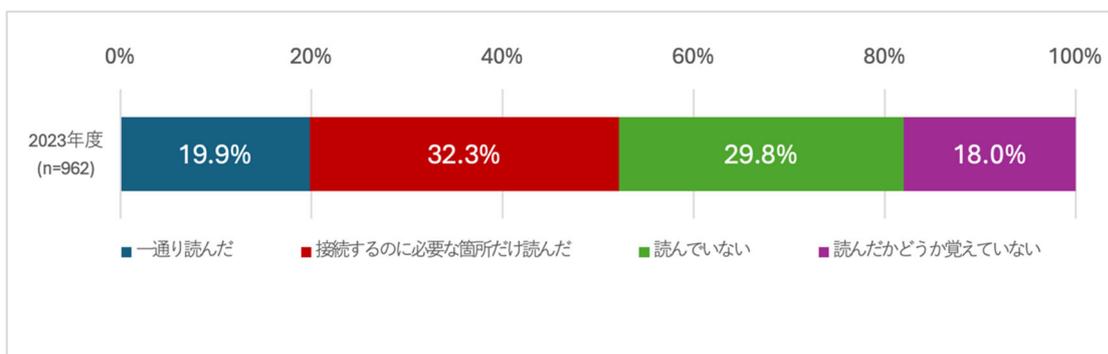
図表 2-1- 15 自宅無線 LAN のサポート期間 (Q14)



⑨ 自宅無線 LAN の AP 取説の把握 (Q3)

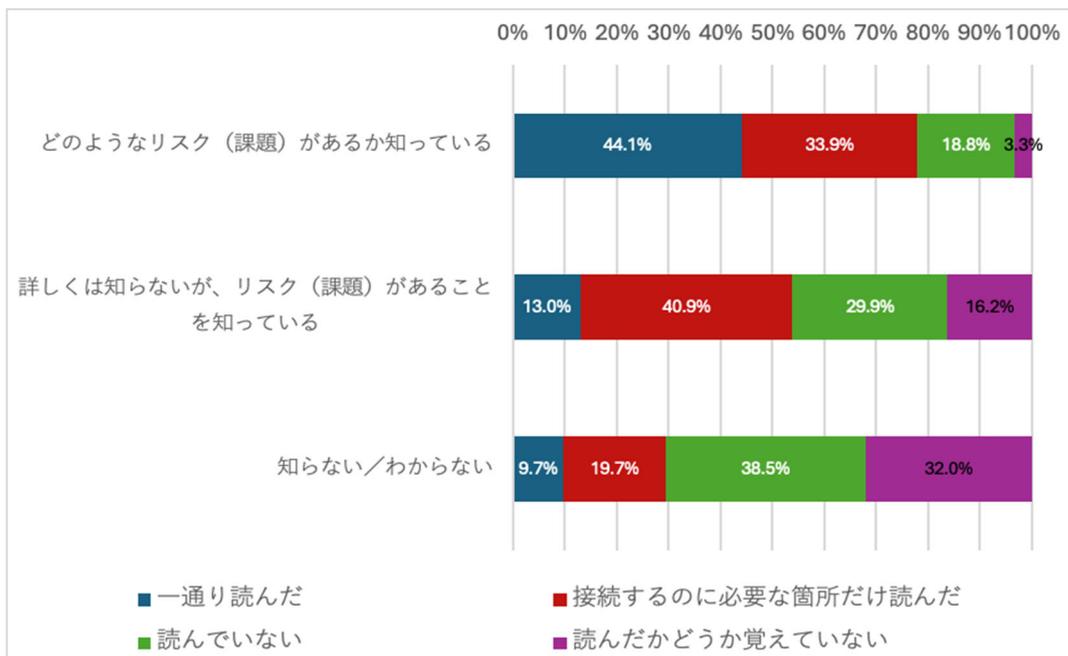
自宅の無線 LAN ユーザの約 52%は、AP(親機)の取扱説明書を読んでいる。

図表 2-1- 16 自宅無線 LAN の AP 取説の把握 (Q3)



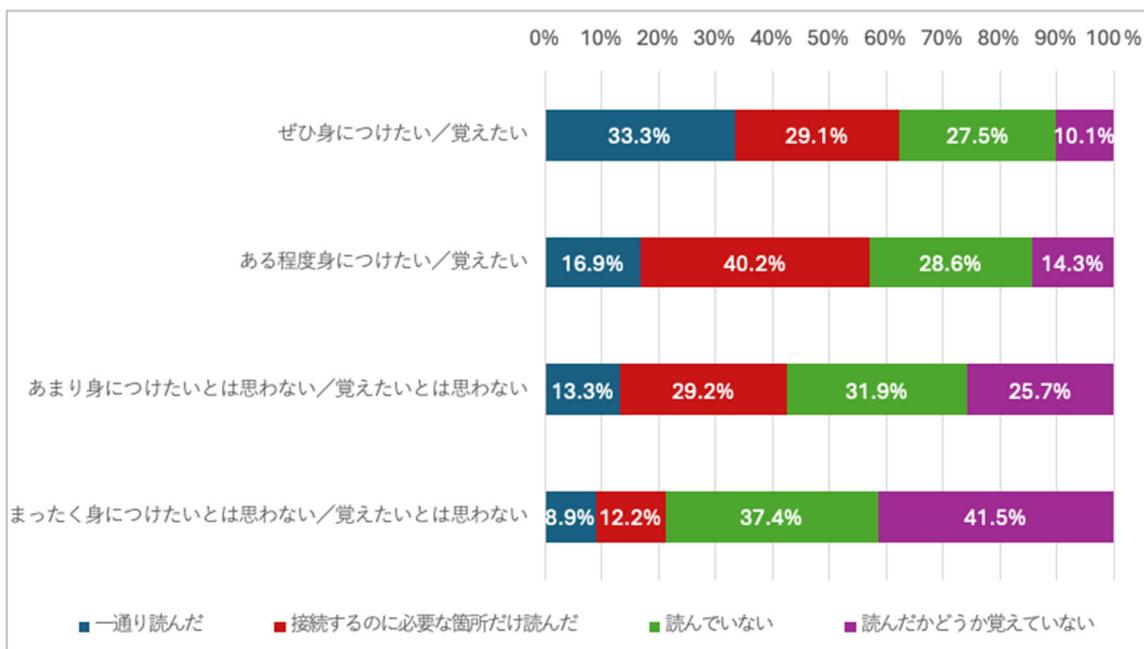
無線 LAN のリスクを認知している自宅無線 LAN ユーザの約 78%は、AP(親機)の取扱説明書を読んでいる一方で、リスクを認知していないユーザが取扱説明書を読む比率は約 30%に留まっている。

図表 2-1- 17 自宅無線 LAN の AP 取説の把握 (Q3) × リスク認知



無線 LAN セキュリティに関する知識をぜひ身につけたいという意欲を持つ自宅無線 LAN ユーザの約 69%は、AP(親機)の取扱説明書を読んでいる一方で、セキュリティに関する知識をまったく身につけたいとは思わないユーザが取扱説明書を読む比率は約 11%に留まっている。

図表 2-1- 18 自宅無線 LAN の AP 取説の把握 (Q3) × セキュリティ知識意欲

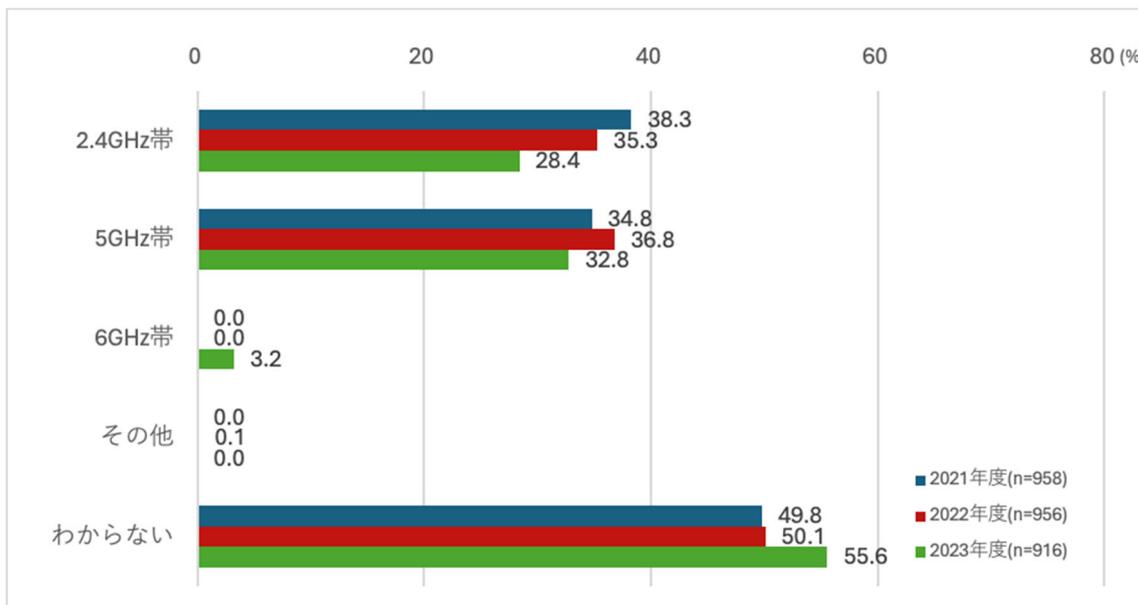


⑩ 自宅無線 LAN の周波数帯 (Q4)

自宅の無線 LAN で使用している周波数帯は、2.4GHz 帯(約 28%)よりも 5GHz 帯(約 33%)の方が多く、明らかに、5GHz が逆転した。

ただし、半数以上のユーザは使用している周波数帯が分かっていない。また、6GHz 帯が増えてくると予想される。

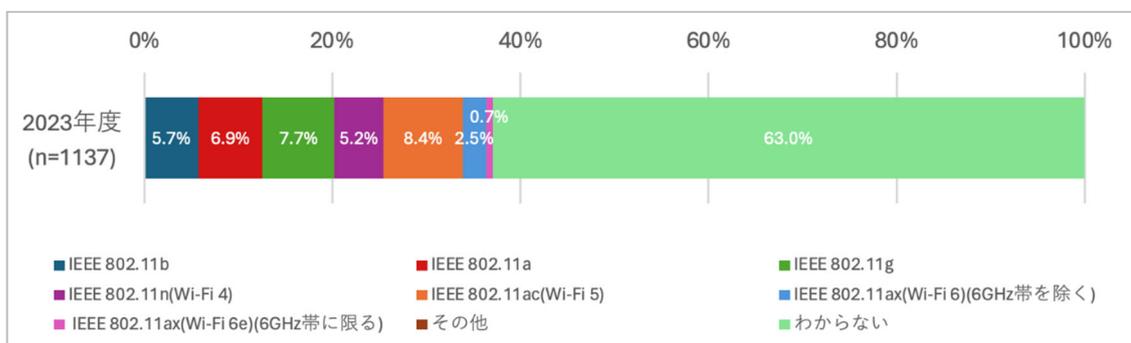
図表 2-1- 20 自宅無線 LAN の周波数帯 (Q4)



⑪ 自宅無線 LAN の使用している通信規格 (Q5)

分からないユーザが約 63%と多い。

図表 2-1- 21 自宅無線 LAN の使用している通信規格 (Q5)



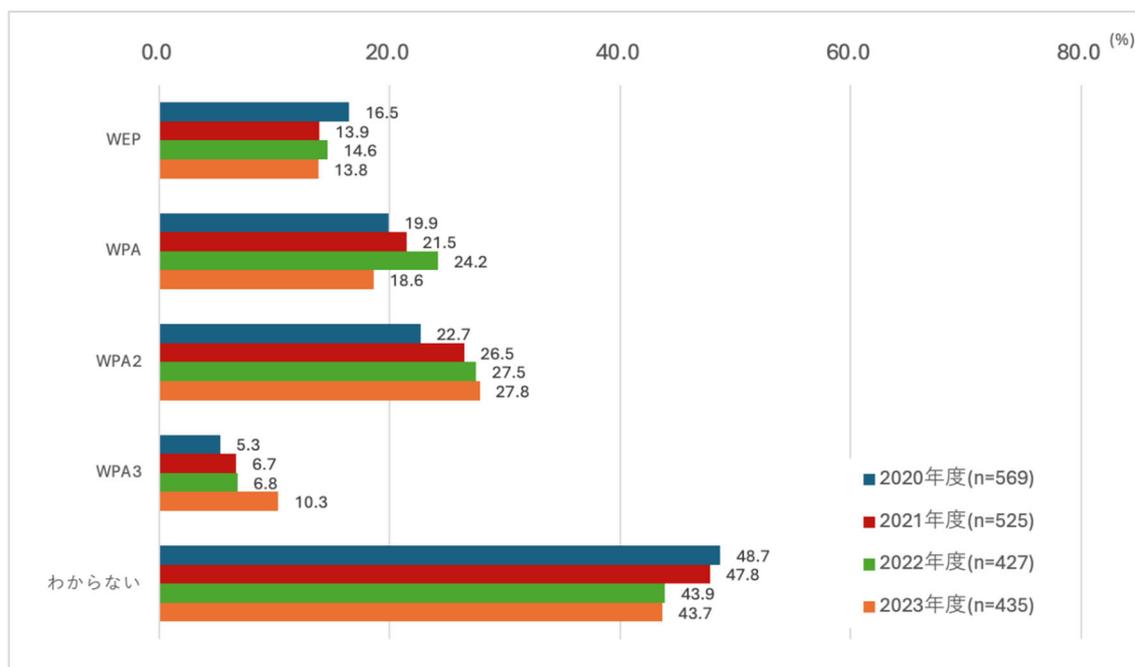
(2) 自宅に設置する無線 LAN (その2)

① 自宅無線 LAN のセキュリティ方式 (Q7)

自宅の無線 LAN のセキュリティ方式として、安全性の高い方式のユーザは約 38%(WPA3(約 10%)・WPA2(約 28%))に対し、安全性に懸念がある方式のユーザは約 33%(WEP(約 14%)・WPA(約 19%))である。全体的には、安全性の高い方式を選ぶユーザが増えつつある。ただし、セキュリティ方式が分からないユーザが 44%を占めている。

WPA はこれまで増加傾向にあったが、今年度は減少している。母集団が変わった影響も排除できないが、WPA は脆弱性が指摘され、無線 LAN のセキュリティに関するガイドラインでも使わないことを推奨されているため、セキュリティ意識の高まりとも考えられる。今後の推移を追っていくことが必要である。

図表 2-1- 22 自宅無線 LAN のセキュリティ方式 (Q7)



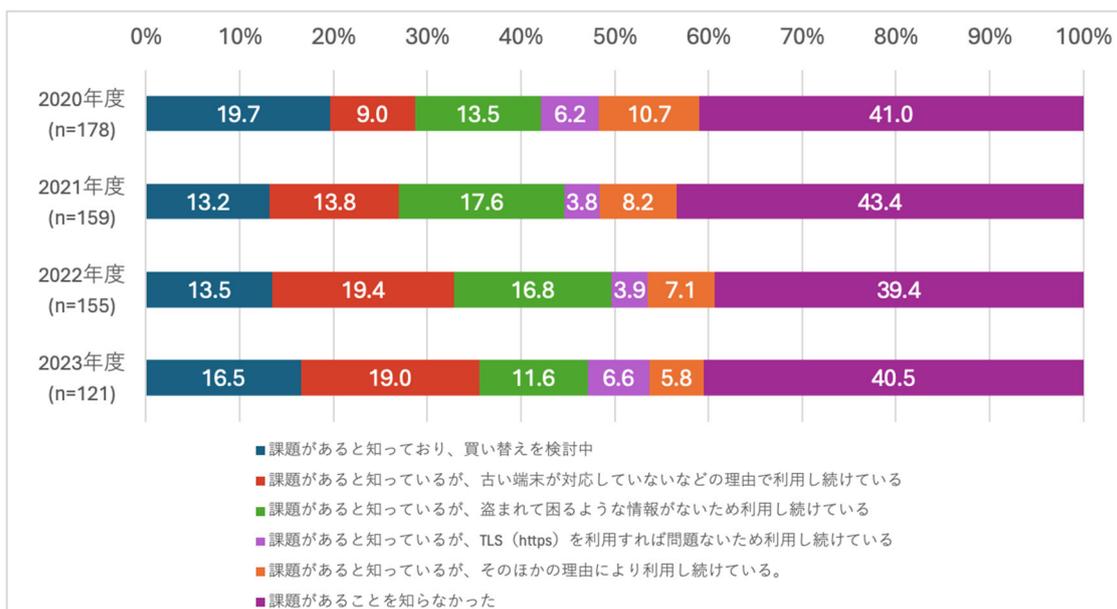
② WEP・WPA を利用する理由 (Q8)

自宅無線 LAN のセキュリティ方式として、WEP や WPA を使用しているユーザのうち、課題を認識し買い換えを検討しているユーザは約 17%に過ぎないが、増加している傾向がある。

約 43%のユーザは課題を認識しつつも利用し続けているが、その比率は、年々、減少している。

一方、約 41%のユーザは、課題を認識していない。

図表 2-1- 23 WEP・WPA を利用する理由 (Q8)

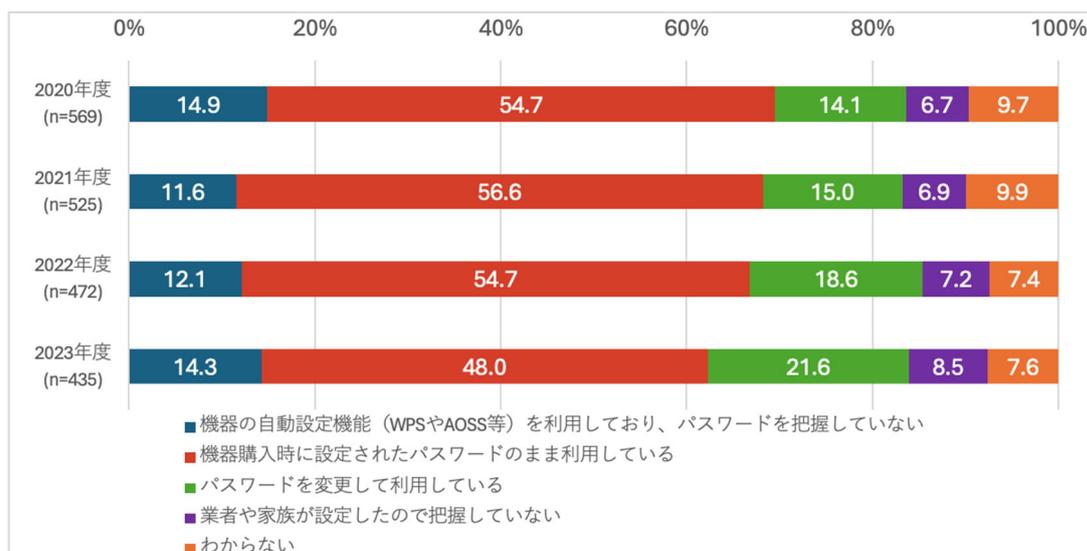


③ 自宅無線 LAN の暗号化パスワード (Q9)

自宅の無線 LAN の暗号化に用いているパスワードを変更しているユーザは、年々、増加しているが、2023 年度で約 22%である。

初期パスワードのまま利用しているユーザが約 48%にのぼるほか、把握していないユーザも多い(約 16%)。

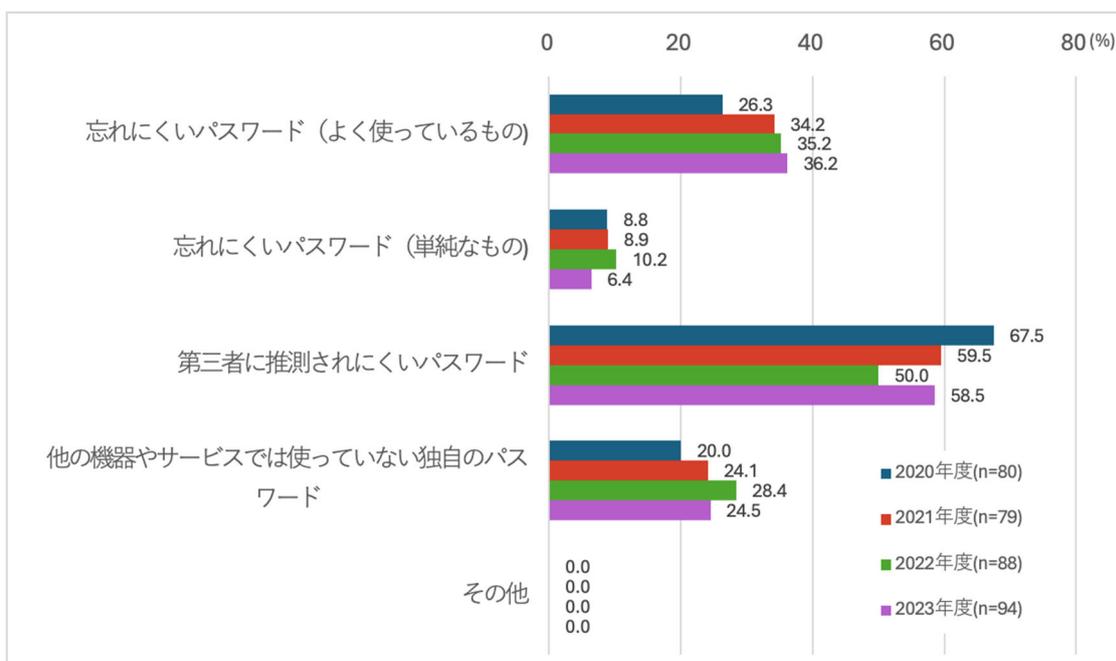
図表 2-1- 24 自宅無線 LAN の暗号化パスワード (Q9)



④ 暗号化パスワード設定の留意点 (Q10)

自宅の無線LANの暗号化に用いているパスワードを変更しているユーザのうち、約59%が第三者に推測されにくいパスワードを用いているものの、よく使っている忘れにくいパスワードを使いまわすユーザも約36%を占める。

図表 2-1- 25 暗号化パスワード設定の留意点 (Q10)

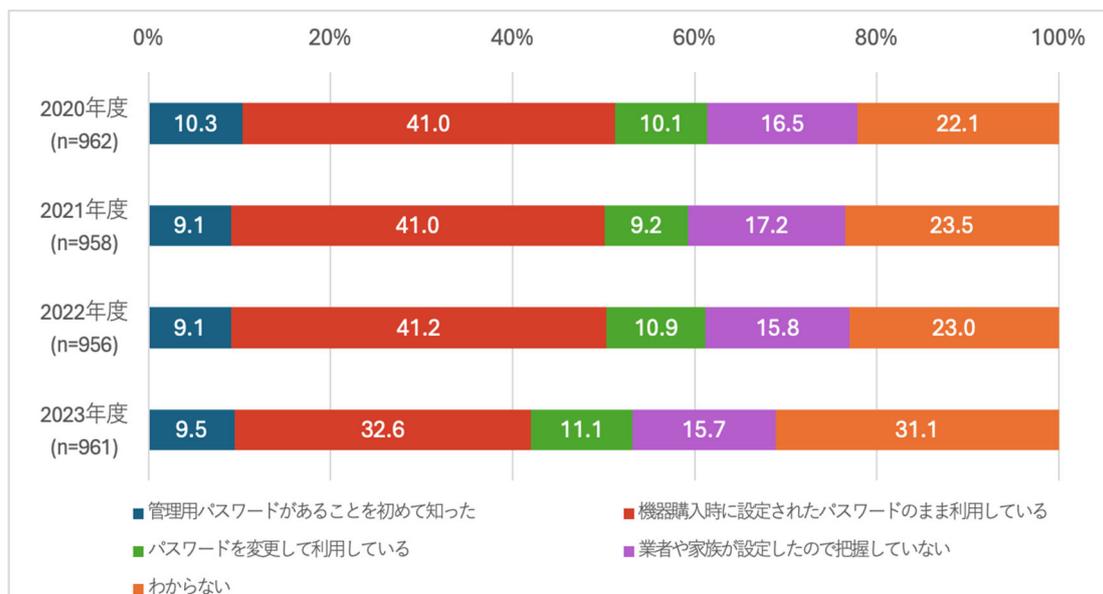


⑤ 自宅無線 LAN の管理用パスワード (Q11)

自宅の無線 LAN の AP(親機)の管理用パスワードを変更しているユーザは、約 11%に過ぎない。

初期パスワードのまま利用しているユーザが約 33%にのぼるほか、今年度は特に、把握していないユーザも多い(約 46%)。

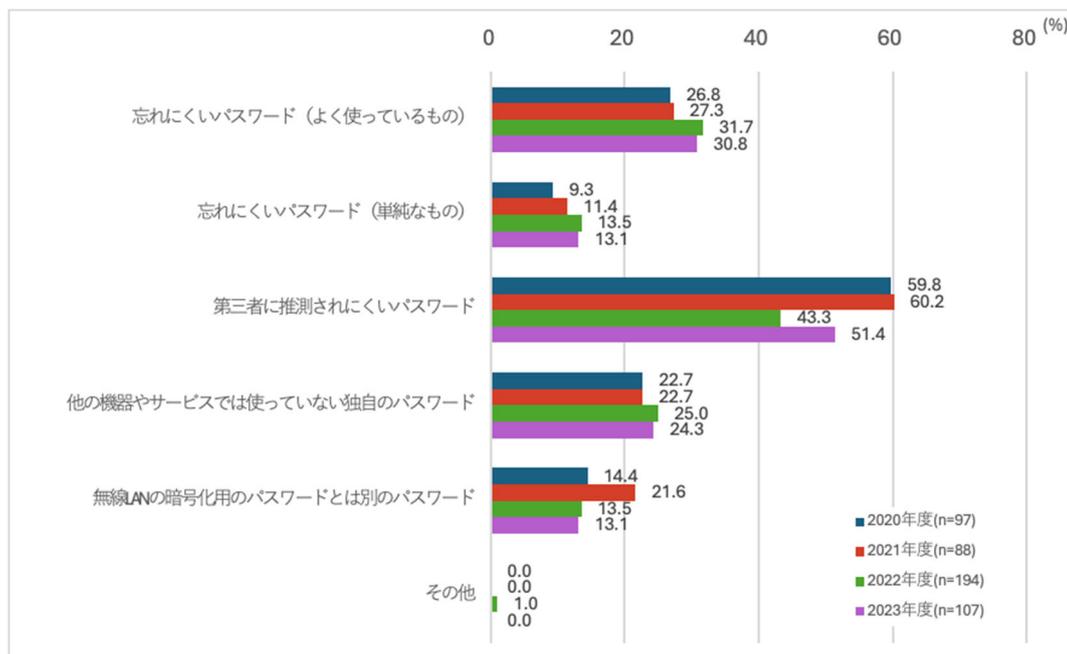
図表 2-1- 26 自宅無線 LAN の管理用パスワード (Q11)



⑥ 管理用パスワード設定の留意点 (Q12)

自宅の無線 LAN の AP(親機)の管理用パスワードを変更しているユーザのうち、約 51%が第三者に推測されにくいパスワードを用いているものの、よく使っている忘れにくいパスワードを使いまわすユーザも約 31%を占める。

図表 2-1- 27 管理用パスワード設定の留意点 (Q12)

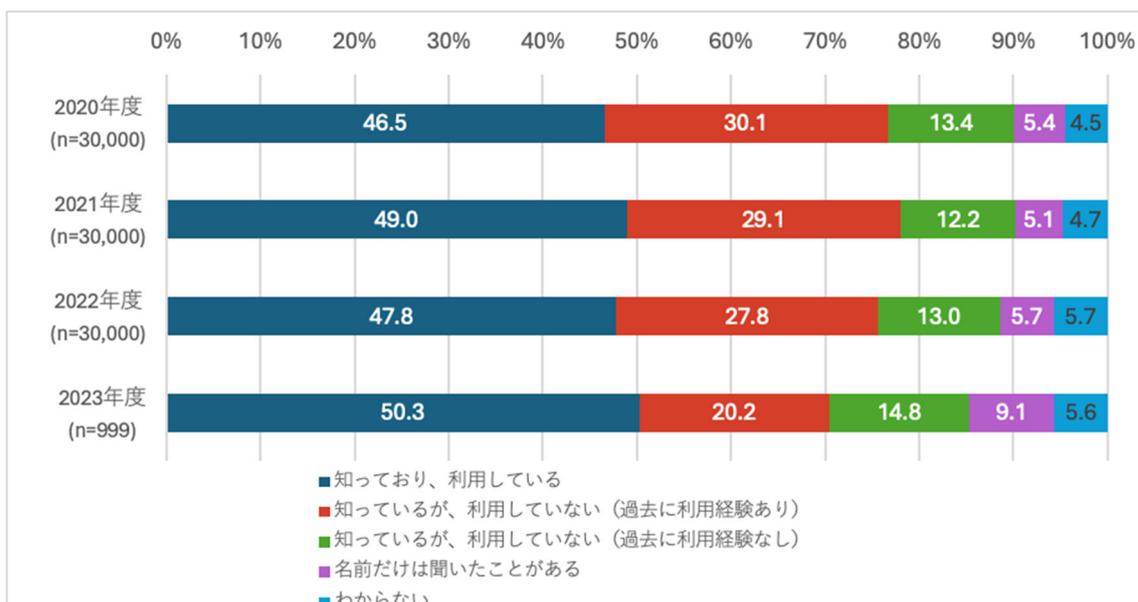


(3) 公衆無線 LAN 利用 (その1)

①公衆無線 LAN の利用有無 (SC6)

公衆無線 LAN の認知度は高い(約 94%)が、利用経験率は約 71%である。
現在、利用している人は約 50%であり、増加傾向にある。

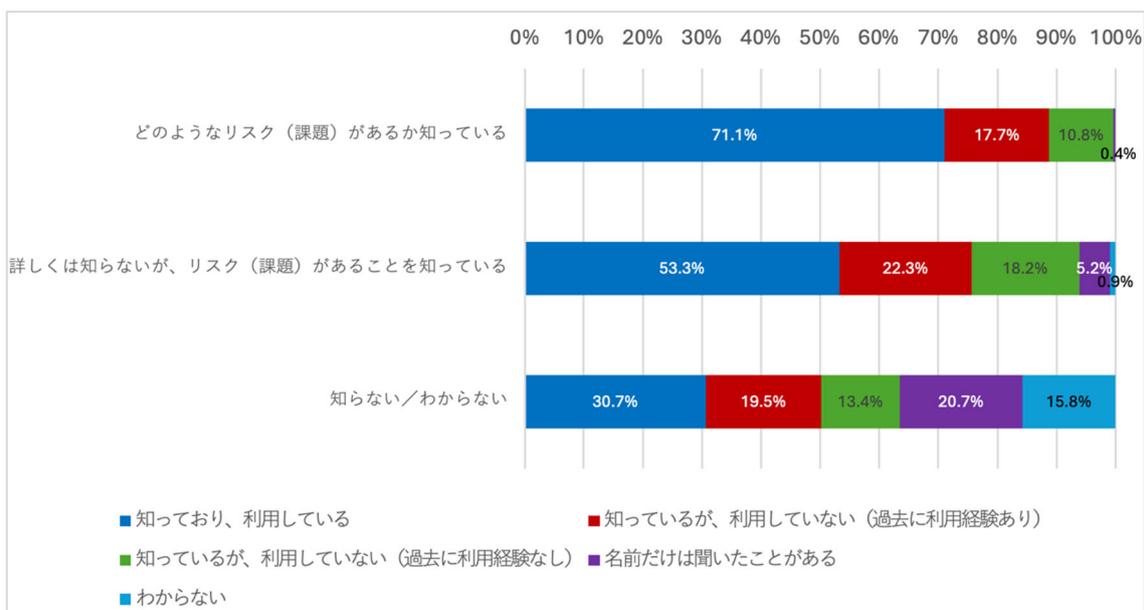
図表 2-1- 28 公衆無線 LAN の利用有無 (SC6)



無線 LAN のリスクを認知している層では、公衆無線 LAN の認知度は高く（約 99%）、利用経験率も約 9 割に達している。

一方、リスクを認知していない層は、そもそも公衆無線 LAN の認知度が低く（約 78%）、利用経験率は約 50%である。

図表 2-1-29 公衆無線 LAN の利用有無（SC6）×リスク認知

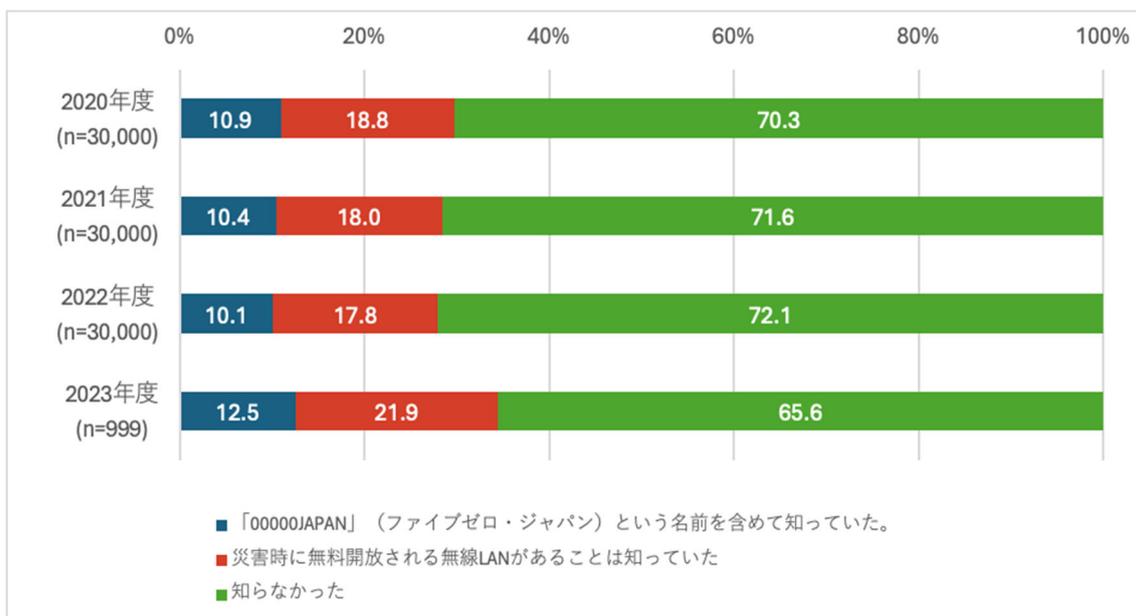


② 「00000JAPAN」 の認知 (SC8)

災害時に被災地域の人々のために無料開放される公衆無線 LAN の認知度は約 35%であり、年々、増加傾向にある。

そのうち、「00000JAPAN」 という名称まで含めて知っている人は約 13%である。

図表 2-1-30 「00000JAPAN」 の認知 (SC8)

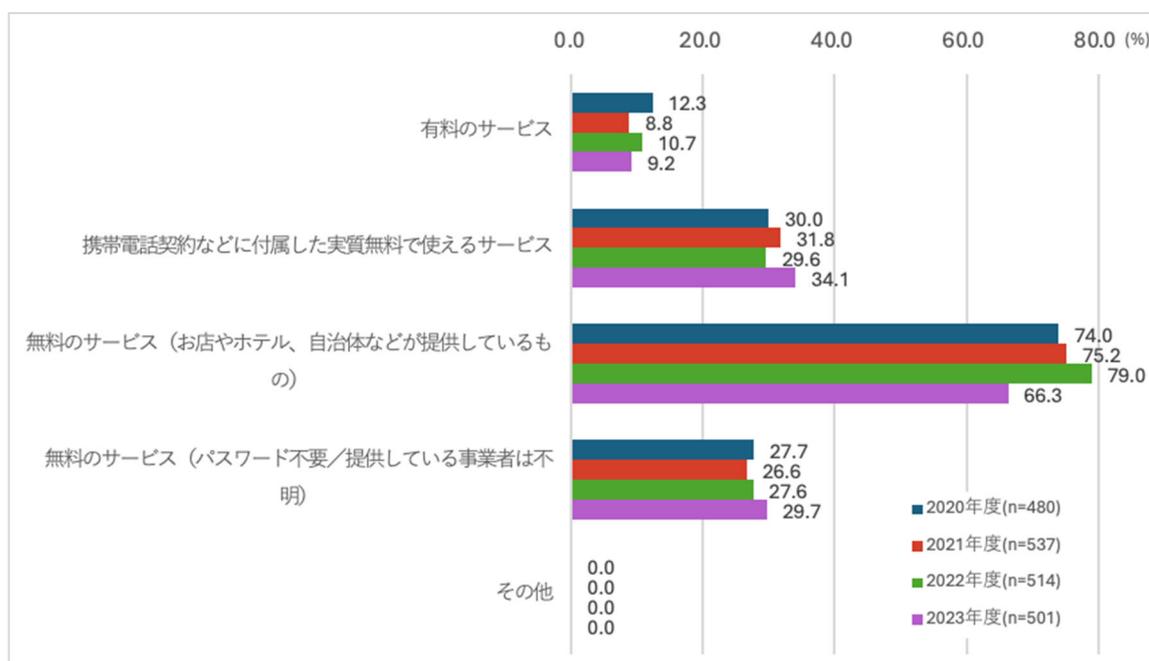


③公衆無線 LAN の利用種別 (Q16)

公衆無線 LAN ユーザが利用しているサービスの大半(約 66%)は、お店やホテル・自治体などが提供している無料のサービスである。

「無料のサービス (お店やホテル、自治体などが提供しているもの)」が昨年まで増加傾向であったものが減少している。「携帯電話契約などに付属した実質無料で使えるサービス」を利用している割合が増えていることが連動している可能性もある。母集団が変わったことによる影響も考えられるので今後の推移を見ていく必要がある。

図表 2-1- 31 公衆無線 LAN の利用種別 (Q16)

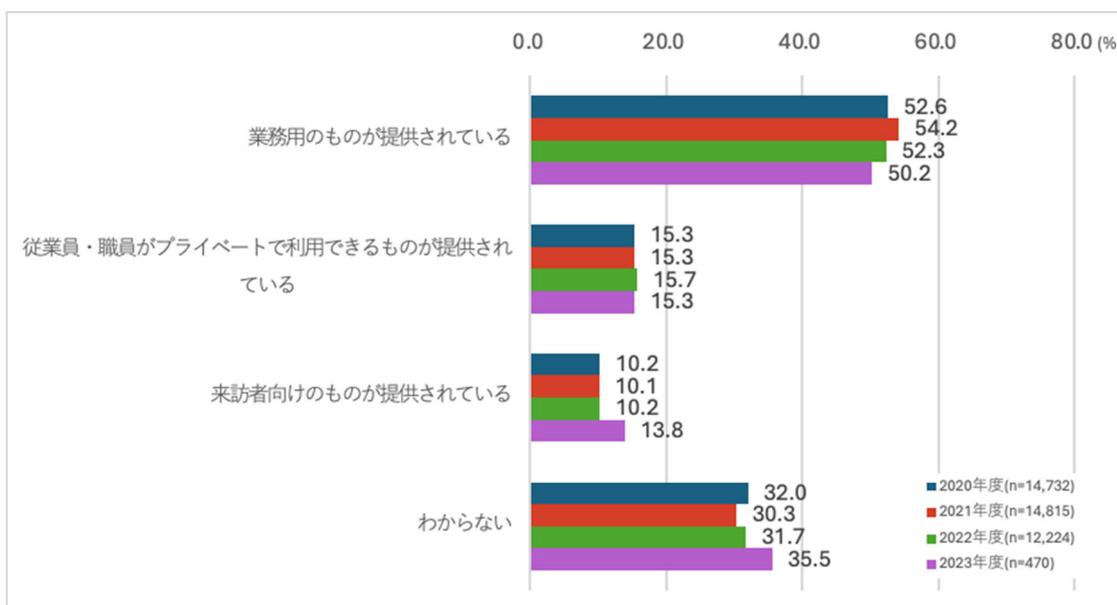


④勤務先での無線 LAN 提供 (SC9)

勤め人の勤務先では、業務用の無線 LAN が提供されているケースが多い(約 50%)。従業員等がプライベートに利用できる無線 LAN が提供されているケース(約 15%)、来訪者向けの無線 LAN が提供されているケース(約 14%)、なども含め、その比率はほぼ変動していない。

複数の無線 LAN が提供されている職場も少なくない点には、情報セキュリティの観点からの注意が必要と言える。

図表 2-1- 32 勤務先での無線 LAN 提供 (SC9)

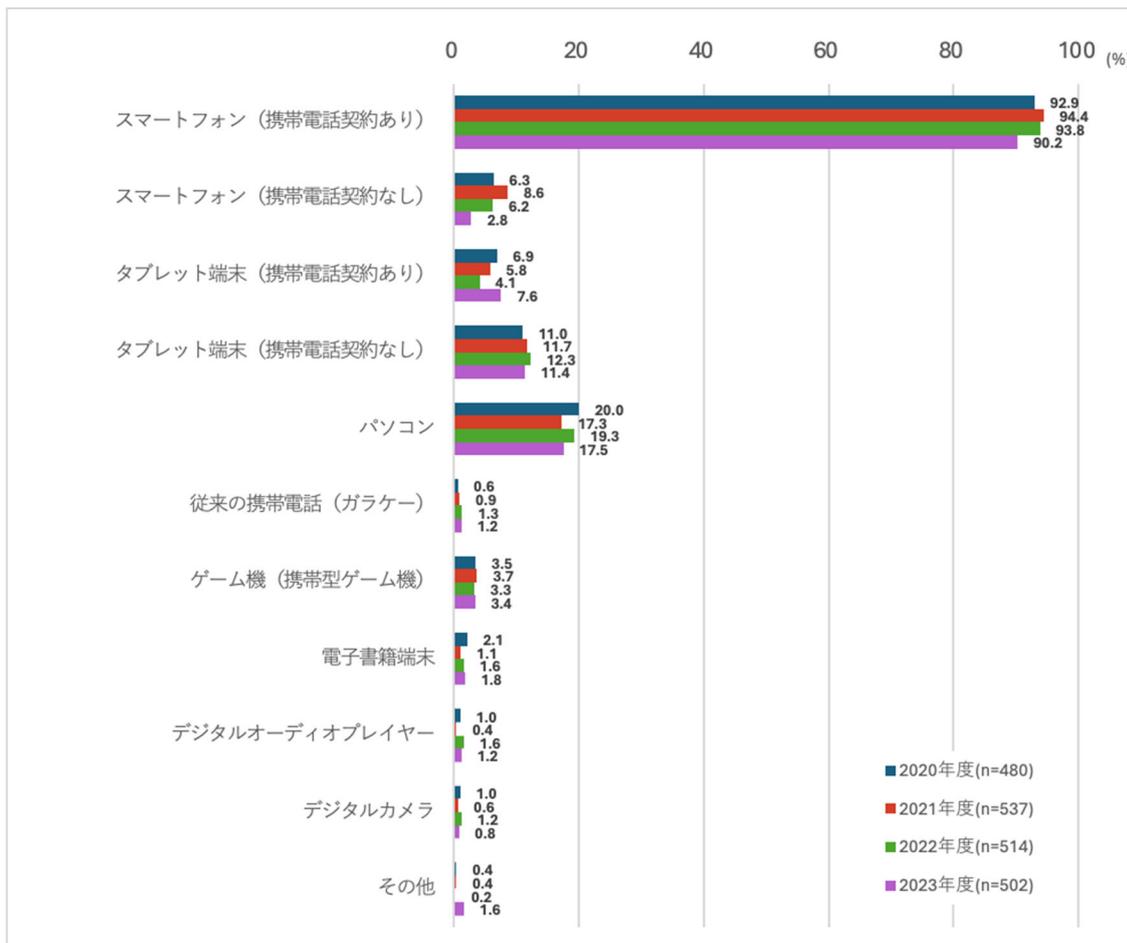


⑤公衆無線 LAN 利用端末 (Q17)

公衆無線 LAN ユーザが接続して利用するデバイスで最も多いものはスマートフォン(SIMあり)で約90%。次いで、パソコン(約18%)、タブレット端末(SIMなし)(約11%)である。

これらの比率には余り変動がないが、タブレット端末 (SIMあり) の利用は伸びている。

図表 2-1-33 公衆無線 LAN 利用端末 (Q17)

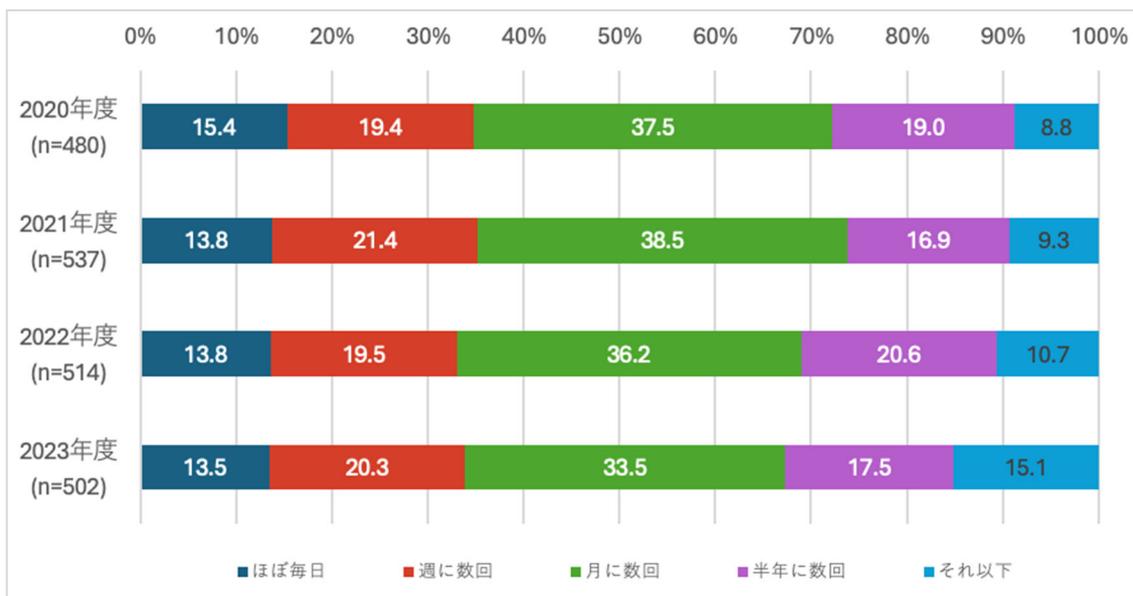


⑥ 公衆無線 LAN の利用頻度 (Q18)

公衆無線 LAN をほぼ毎日利用しているヘビーユーザは約 14%であり、年々、微減傾向にある。

対して、半年に数回やそれ以下の頻度でのユーザは約 33%おり、年々、利用頻度が下がっている。

図表 2-1-34 公衆無線 LAN の利用頻度 (Q18)

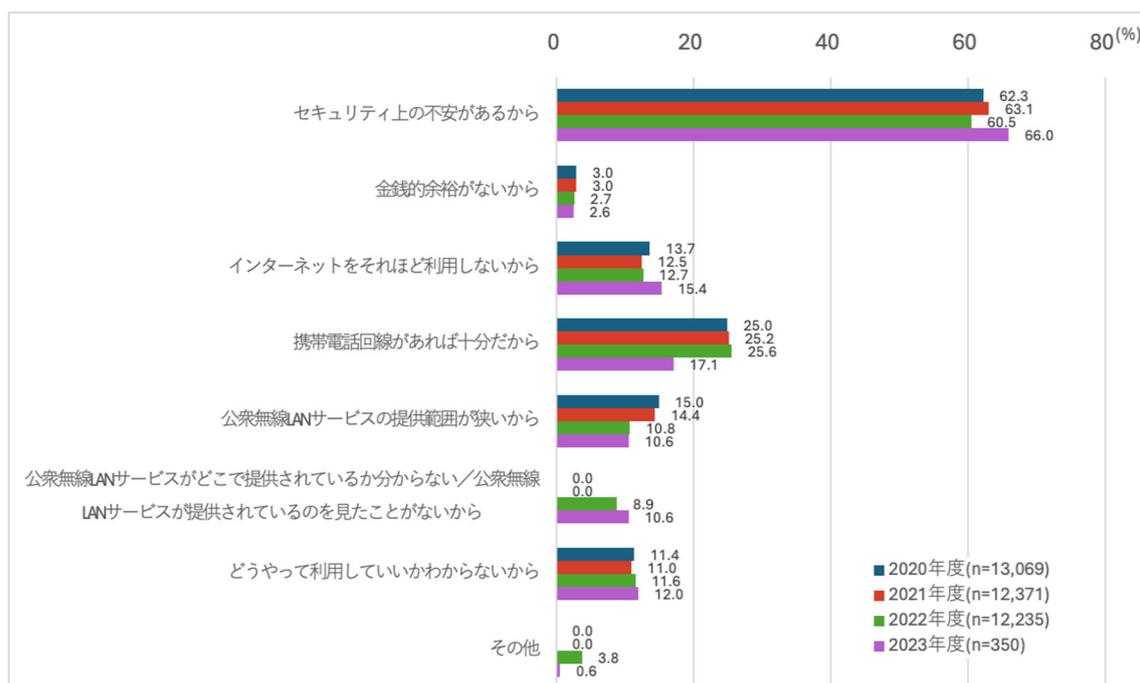


⑦ 公衆無線 LAN を利用していない理由 (SC7)

公衆無線 LAN を利用しない人は、セキュリティ上の不安を最大の理由にあげている(約66%)。

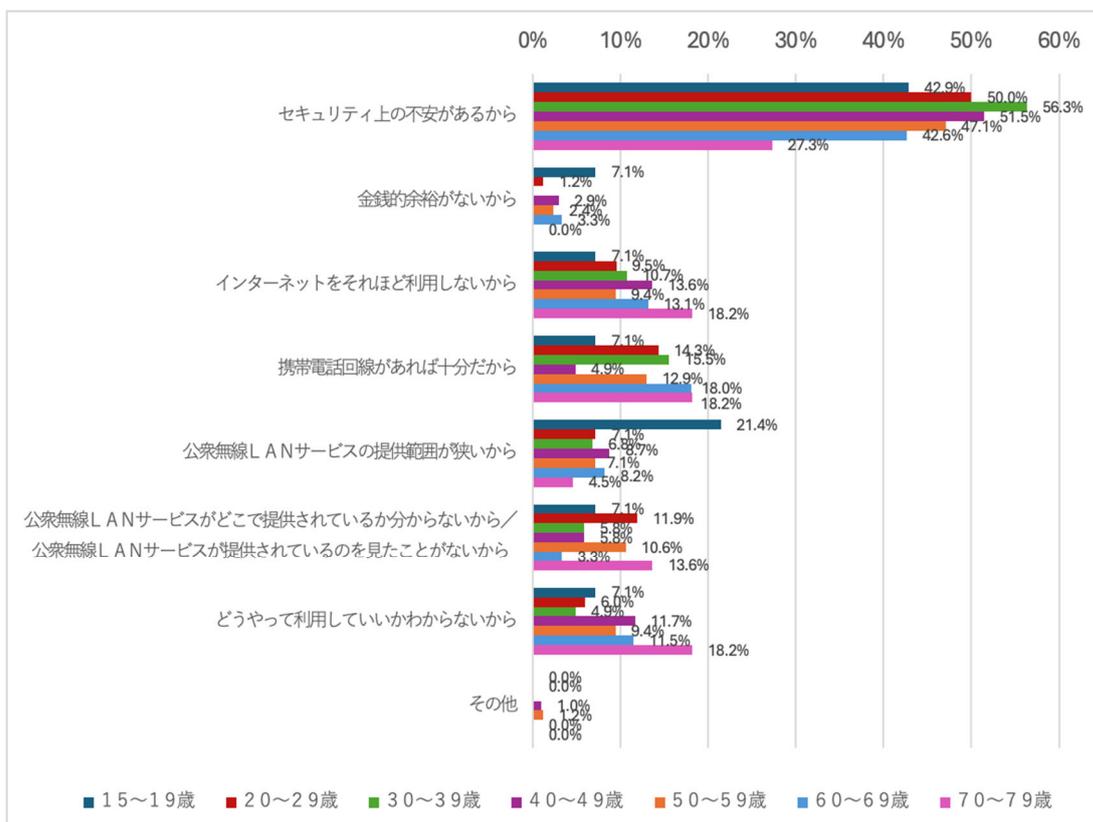
次いで、携帯電話回線があれば十分とする人が約17%おり、これらの比率は今年度は減った。

図表 2-1-35 公衆無線 LAN を利用していない理由 (SC7)



中年層では、公衆無線 LAN を利用しない理由として、セキュリティ上の不安をあげる人が若年層や高年層と比べて多い。逆に、携帯電話回線があれば十分とする人は若年層や高年層と比べて少ない傾向にある。また、15 歳から 19 歳の層で、公衆無線 LAN サービスの提供範囲が狭いからを理由に挙げる人が突出している。

図表 2-1-36 公衆無線 LAN を利用していない理由 (SC7) ×年代

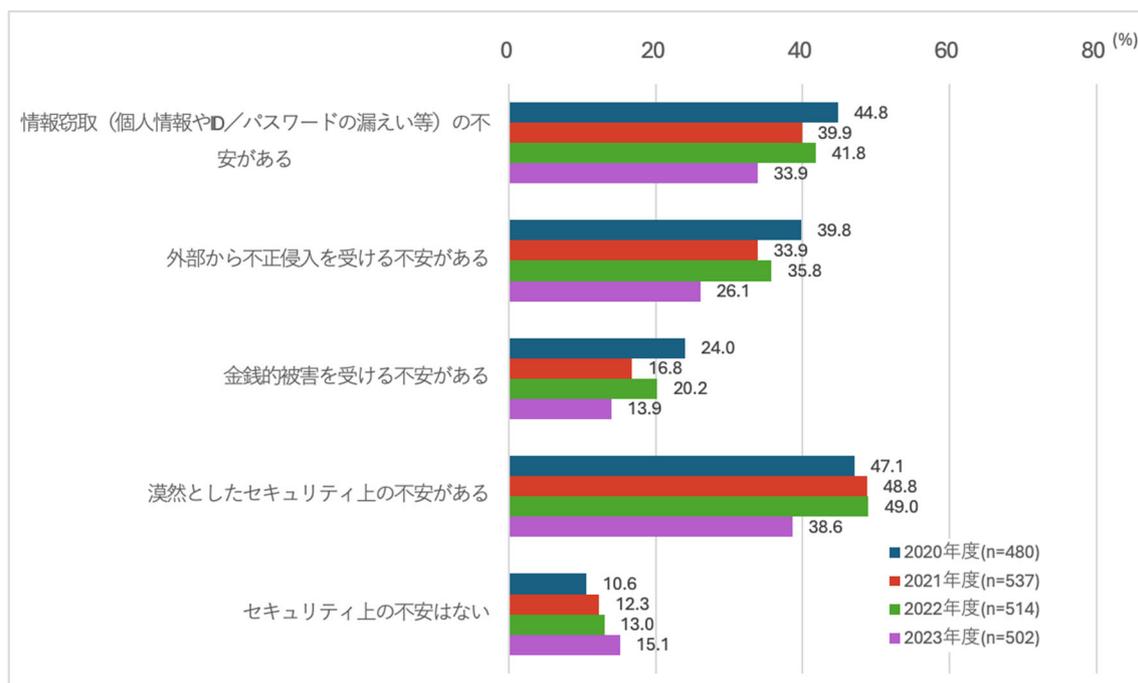


⑧ 公衆無線 LAN でのセキュリティ上の不安 (Q38)

公衆無線 LAN 利用者のうち、約 85%がセキュリティ上の不安を抱いているが、約 39%は漠然とした不安を抱いている状態である。

具体的な不安としては、情報窃取(約 34%)や不正侵入(約 26.1%)などの比率が高く、全体的に、自宅での無線 LAN 利用よりも公衆無線 LAN 利用の方が、セキュリティ上の不安を感じさせている。

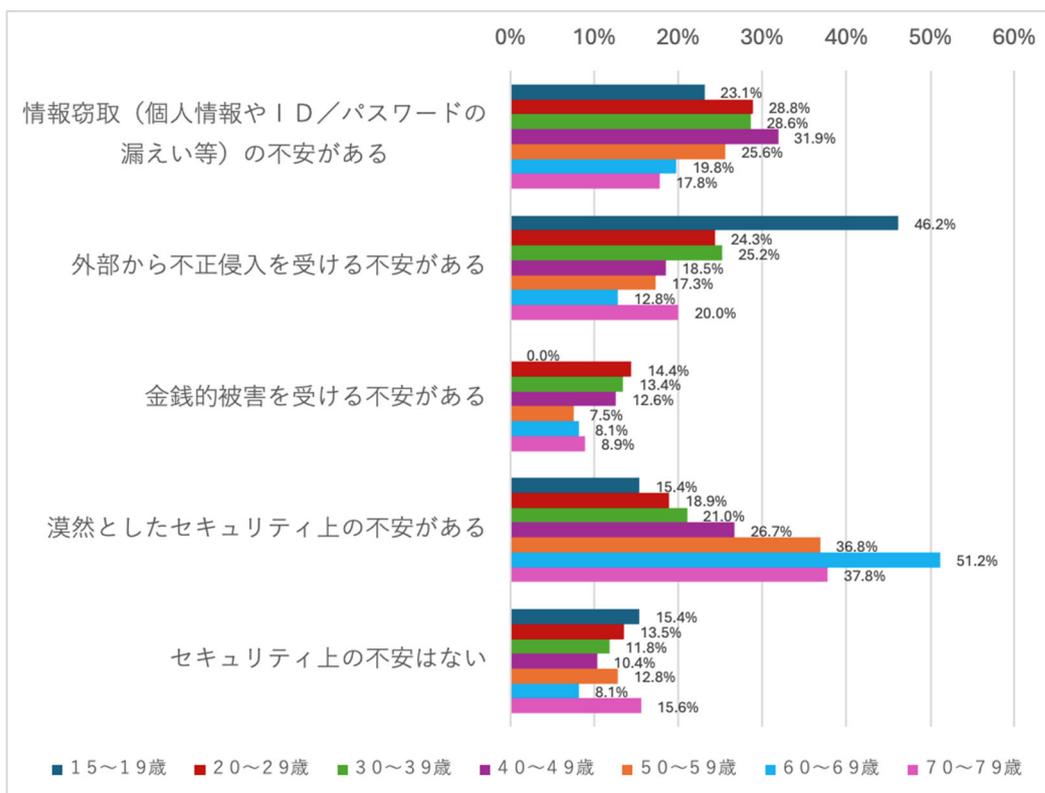
図表 2-1-37 公衆無線 LAN でのセキュリティ上の不安 (Q38)



公衆無線 LAN ユーザは、年代があがるにつれて、具体的な不安ではなく、漠然とした不安を抱いている傾向にある。

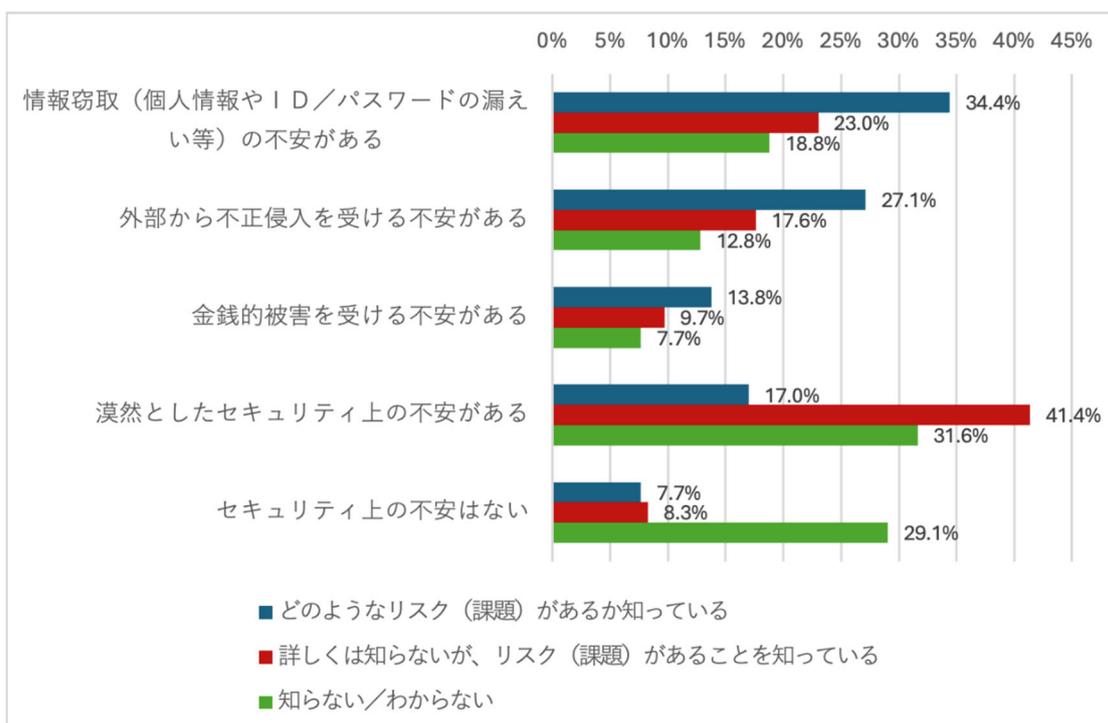
若年層のユーザは、中高年層と比べると、不安感が薄いですが、情報窃取には敏感な傾向がある。また、15歳から19歳の層は、外部からの不正侵入に特に不安がある。

図表 2-1-38 公衆無線 LAN でのセキュリティ上の不安 (Q38) ×年代



無線 LAN のリスクを認知している公衆無線 LAN 利用者は、情報窃取や不正侵入といったセキュリティ上の不安を抱いているが、リスクを認知していない公衆無線 LAN 利用者は、そもそもセキュリティ上の不安を感じていない比率が高い。

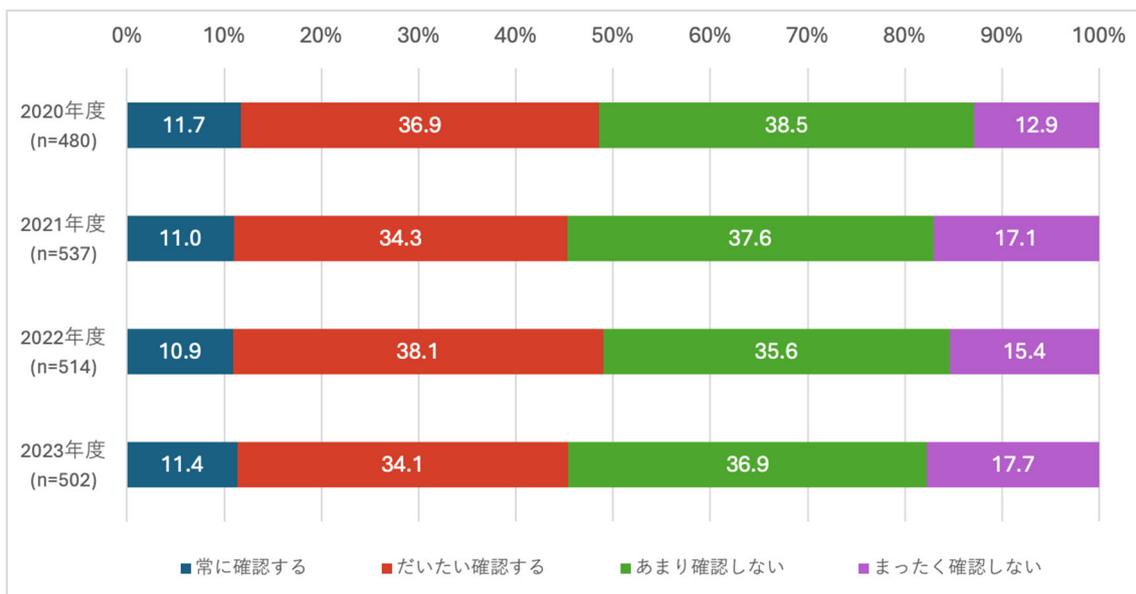
図表 2-1-39 公衆無線 LAN でのセキュリティ上の不安 (Q38) × リスク認知



⑨ 公衆無線 LAN 初回利用時の利用規約・注意事項の確認 (Q21)

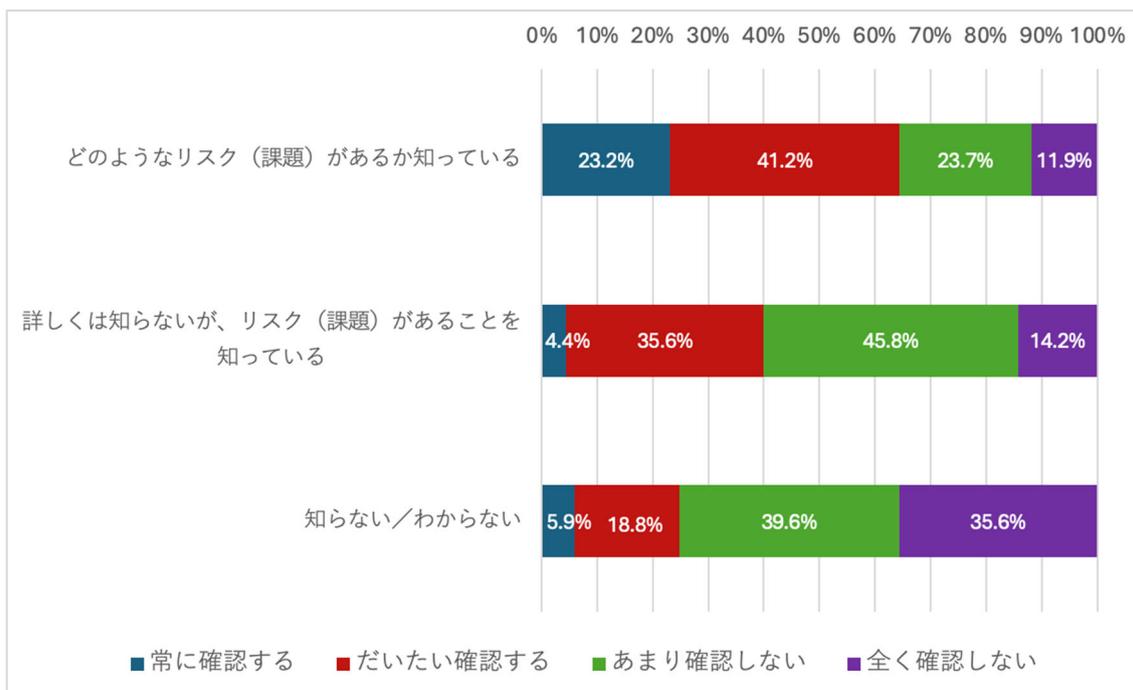
公衆無線 LAN ユーザのうち、サービスを初めて利用する際に、利用規約や注意事項を確認するユーザ(約 46%)と確認しないユーザ(約 54%)は、概ね半々に分かれている。

図表 2-1- 40 公衆無線 LAN 初回利用時の利用規約・注意事項の確認 (Q21)



無線 LAN のリスクを認知している公衆無線 LAN ユーザは、サービスを初めて利用する際に、利用規約や注意事項を確認する比率が 5 割を超えているが、リスクを認知していない公衆無線 LAN ユーザは確認しない比率が 7 割を超えている。

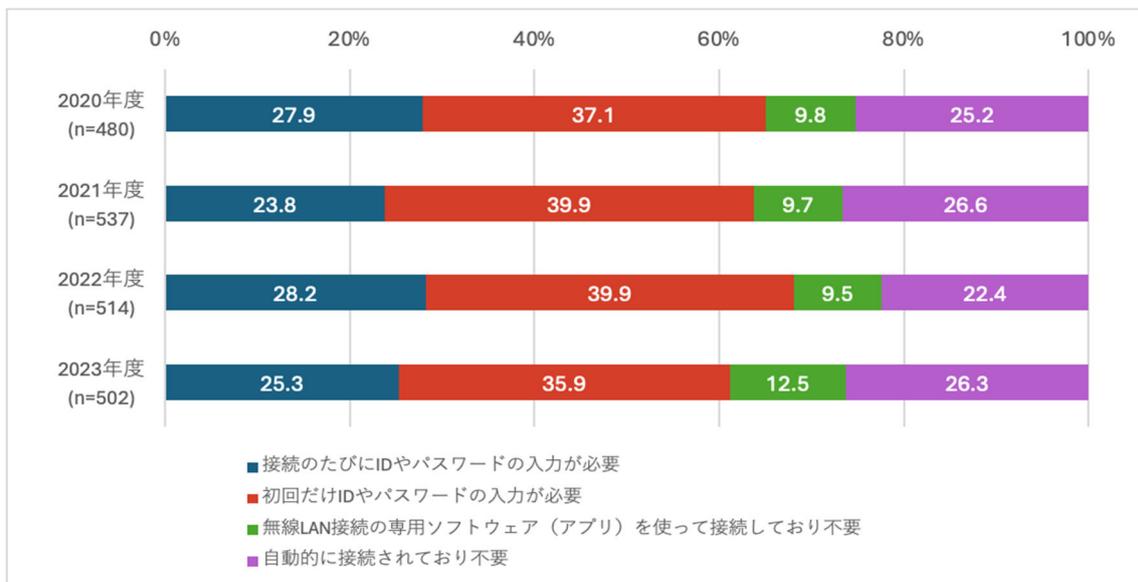
図表 2-1-41 公衆無線 LAN 初回利用時の利用規約・注意事項の確認 (Q21) × リスク認知



⑩ 公衆無線 LAN 接続都度の認証 (Q26)

公衆無線 LAN ユーザが、普段、使用するサービスは、接続のたびに ID やパスワードの入力が必要なものが約 25%であり、初回だけ ID やパスワードの入力が必要なものが約 36%となっている。全体的に、ID やパスワードの入力が不要なケースが増えつつある。

図表 2-1-42 公衆無線 LAN 接続都度の認証 (Q26)

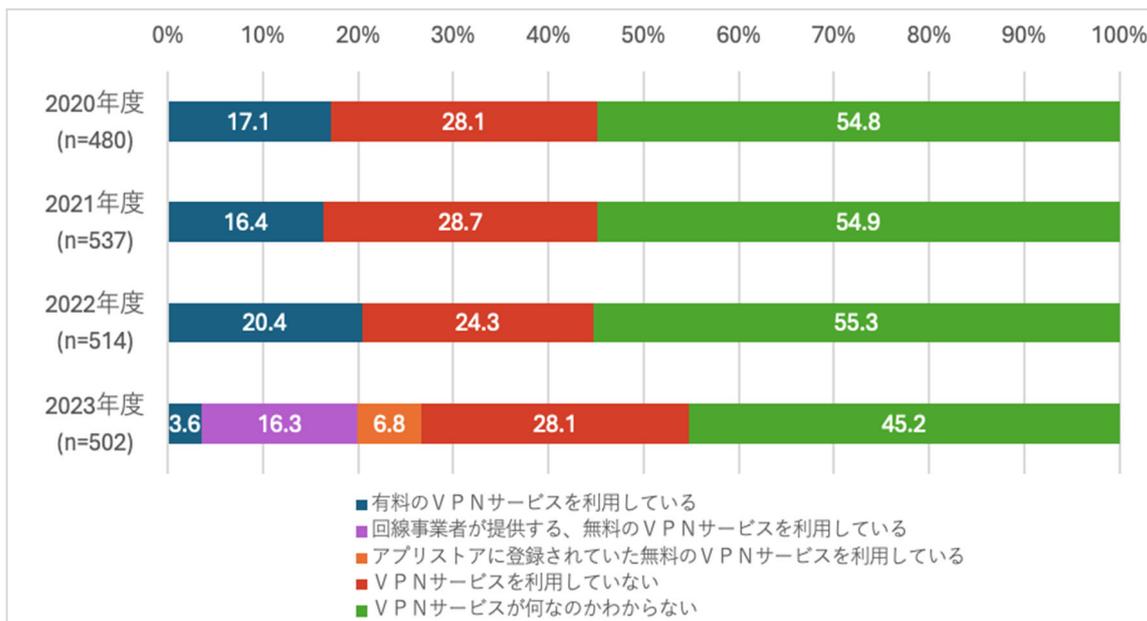


⑪ 公衆無線 LAN 接続時の VPN の利用 (Q36)

公衆無線 LAN 利用時に VPN サービスを利用しているユーザは約 28%であるのに対し、約 27%は VPN サービスを利用しておらず、拮抗している。

ただし、約 45%のユーザは VPN サービスが何なのか分かっていない。今年度から、無料の VPN の利用に対する問いができたが、全体的に無料のユーザが増えているのがわかる。

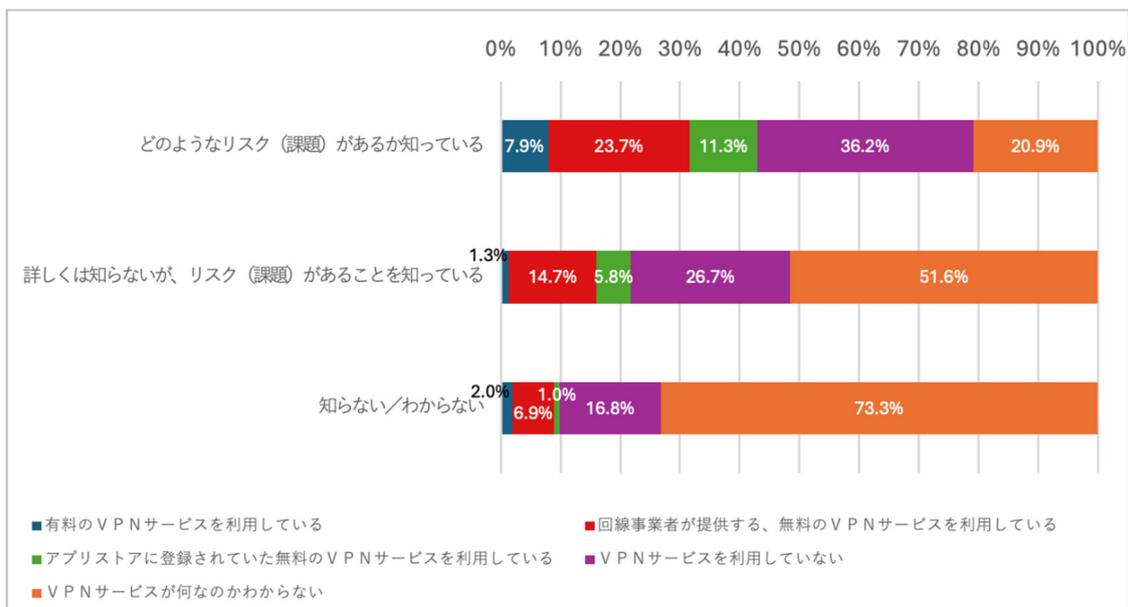
図表 2-1-43 公衆無線 LAN 接続時の VPN の利用 (Q36)



無線 LAN のリスクを認知している公衆無線 LAN ユーザは、約 79.1%が VPN サービスを認知しており、うち半数以上が VPN サービスを利用している。

対して、リスクを認知していない公衆無線 LAN ユーザは、そもそも VPN サービスを認知していないユーザが約 73%を占め、認知していても利用しているユーザは少ない。

図表 2-1-44 公衆無線 LAN 接続時の VPN の利用 (Q36) × リスク認知

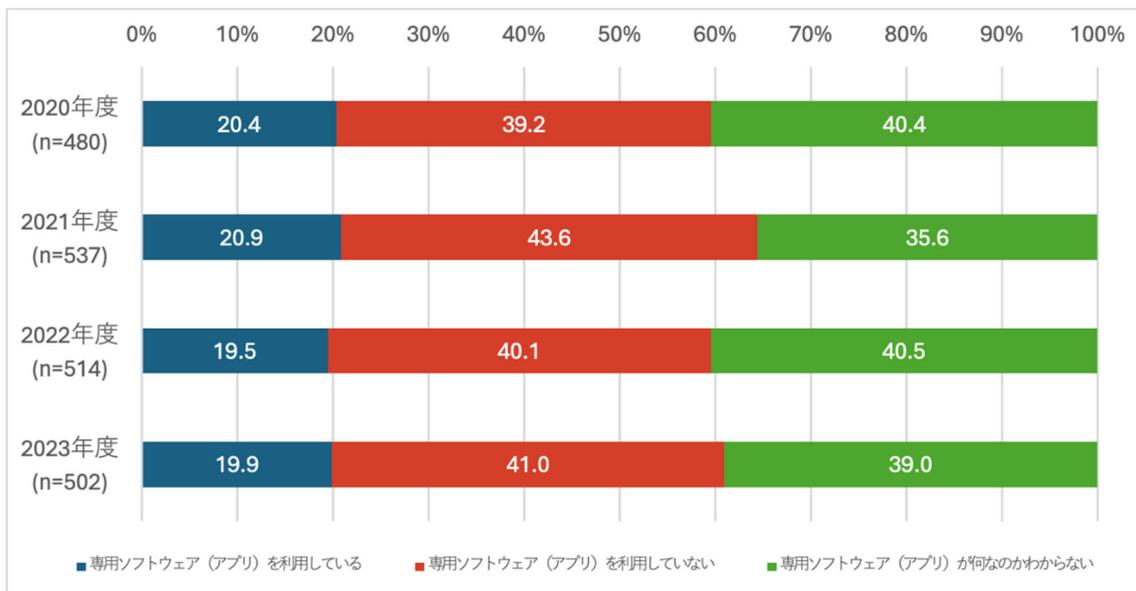


⑫ 公衆無線 LAN 接続時の専用アプリの利用 (Q37)

公衆無線 LAN 利用時に専用アプリを利用しているユーザは約 20%であるのに対し、約 41%は専用アプリを利用していない。

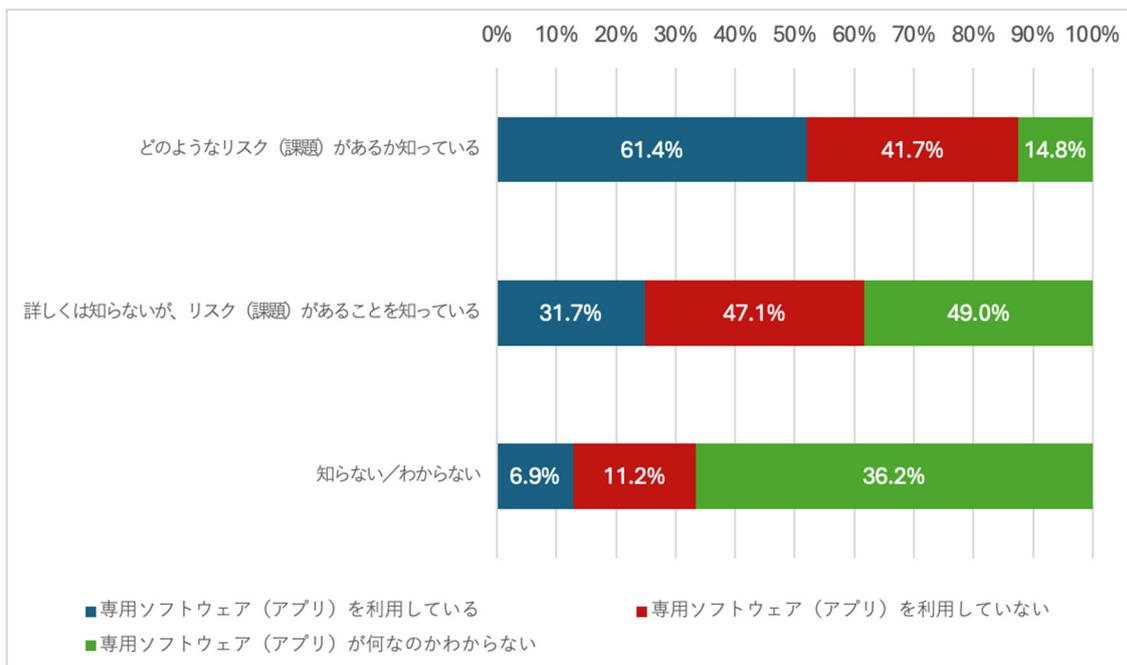
ただし、約 39%のユーザは専用アプリが何なのか分かっていない。

図表 2-1-45 公衆無線 LAN 接続時の専用アプリの利用 (Q37)



無線 LAN のリスクを認知している公衆無線 LAN ユーザの約 85%は専用アプリを認知しており、うち約 4 割が専用アプリを利用しているのに対して、リスクを認知していない公衆無線 LAN ユーザの 6 割はそもそも専用アプリを認知しておらず、認知していても利用しているユーザは非常に少ない。

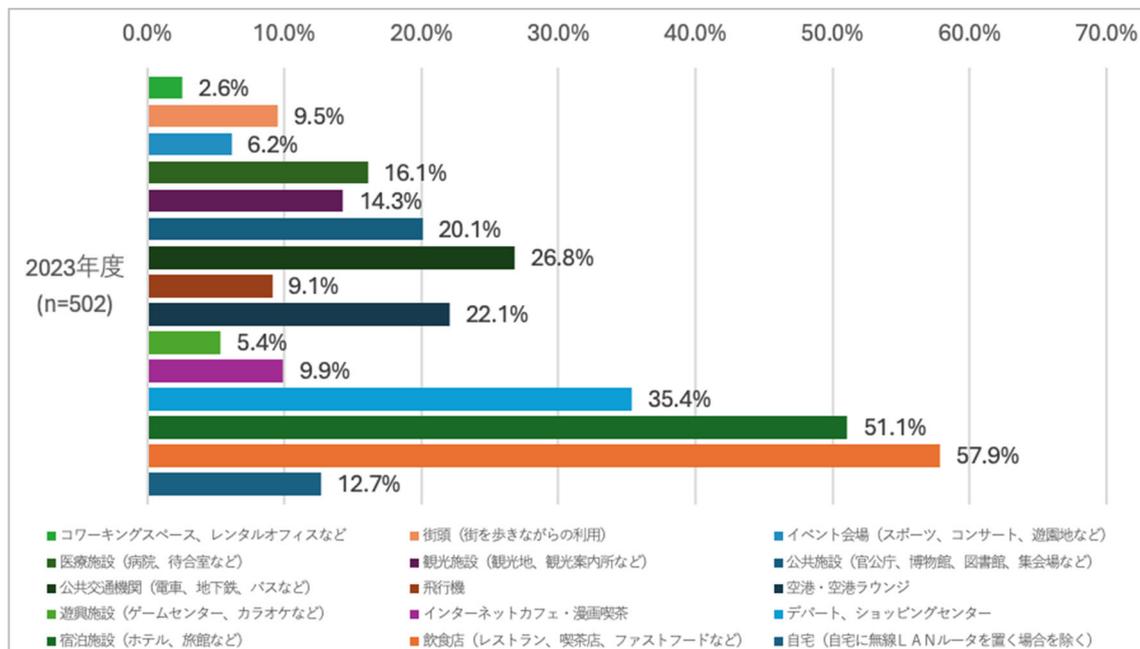
図表 2-1-46 公衆無線 LAN 接続時の専用アプリの利用 (Q37) × リスク認知



⑬ 公衆無線 LAN 利用が不安な場所 (Q39)

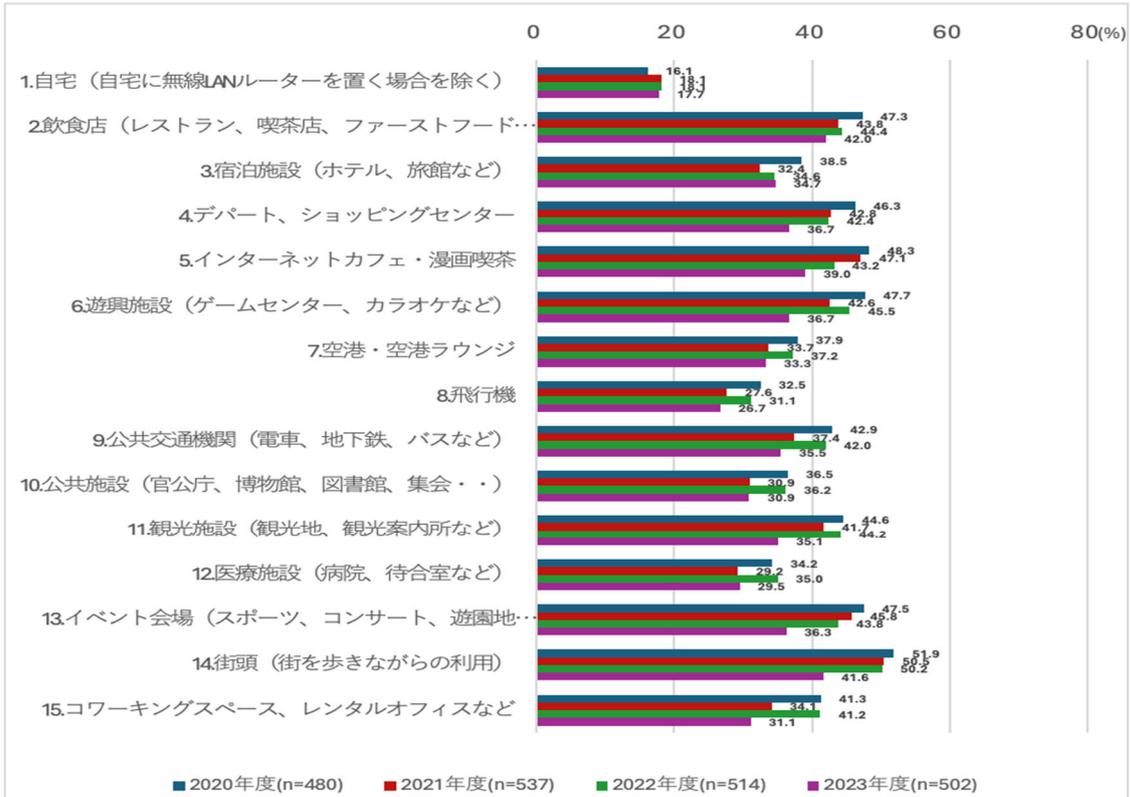
公衆無線 LAN ユーザがサービスを利用する場所は、飲食店、宿泊施設、デパート・ショッピングセンターが中心である。

図表 2-1-47 公衆無線 LAN 接続時の利用場所 (Q39)



公衆無線 LAN ユーザがサービスを利用する際に最も不安を感じる場所は飲食店 (約 42%)。次いで、街頭 (約 42%)、イベント会場 (約 37%)、遊興施設 (約 37%)、観光施設 (約 35%)、などが不安視されており、周囲に不特定多数の人がいる環境での利用が不安に結びついていそうである。なので、自宅での不安は全体的に少ない。

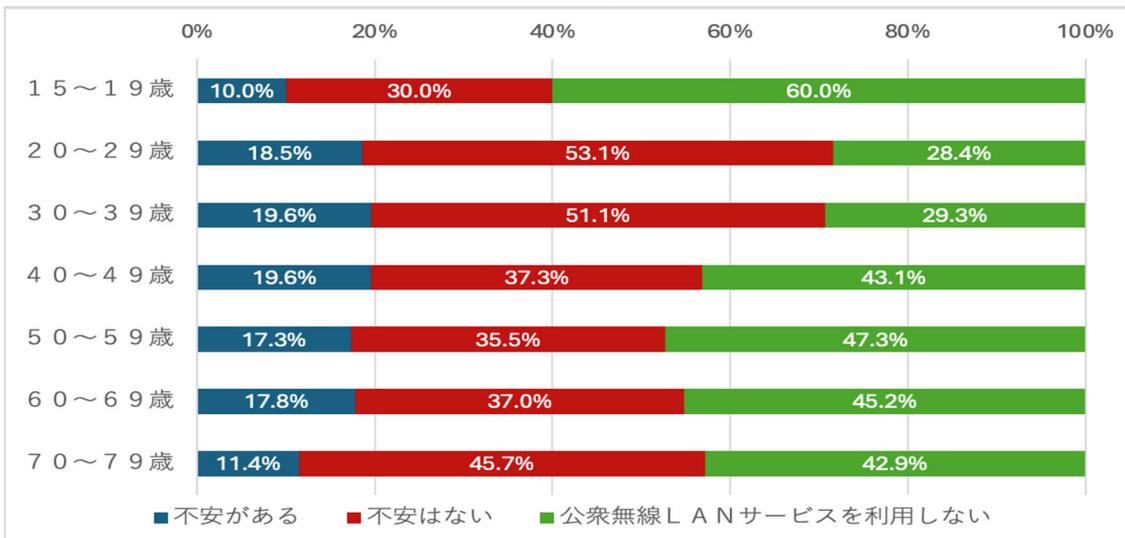
図表 2-1- 48 公衆無線 LAN 利用が不安な場所 (Q39)



公衆無線 LAN ユーザのなかで、自宅での利用は概ね不安視されていない傾向にあるが、20 歳代、30 歳代の利用者は、特に不安感がない。

図表 2-1-49 公衆無線 LAN 利用が不安な場所 (Q39) ×年代

1. 自宅

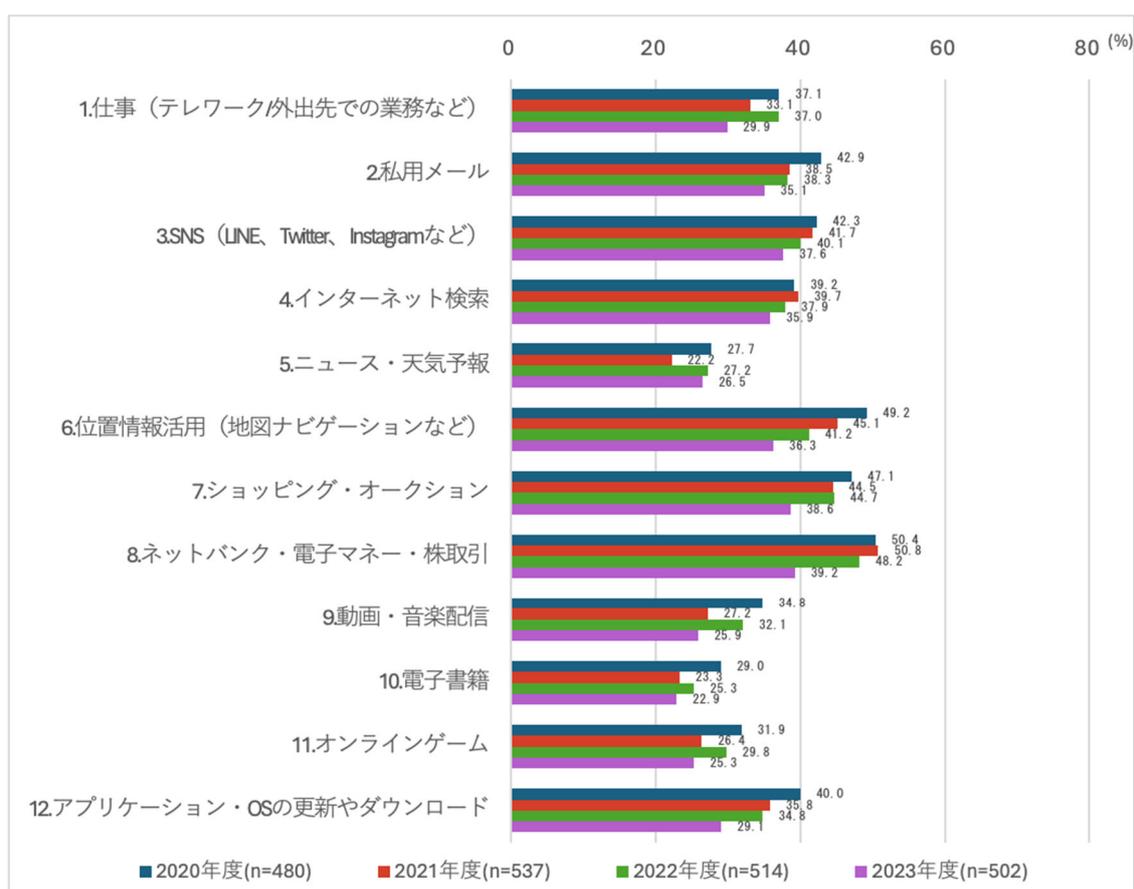


⑭ 公衆無線 LAN 利用が不安なサービス (Q40)

公衆無線 LAN ユーザが利用時に最も不安を感じるサービスはネットバンキング・電子マネー・株取引(約 39%)である。

次いで、ショッピング・オークション(約 39%)、SNS(約 38%)、位置情報活用(約 36%)、などが不安視されており、個人情報の発信を伴うサービスの利用が不安に結びついていそうである。ただし、全体的に今年度の母集団の特徴として、不安が前年以前よりも少ない傾向がある。セキュリティに対して免疫が高まってきている傾向とも理解できるが、翌年度から検証が必要と思われる。

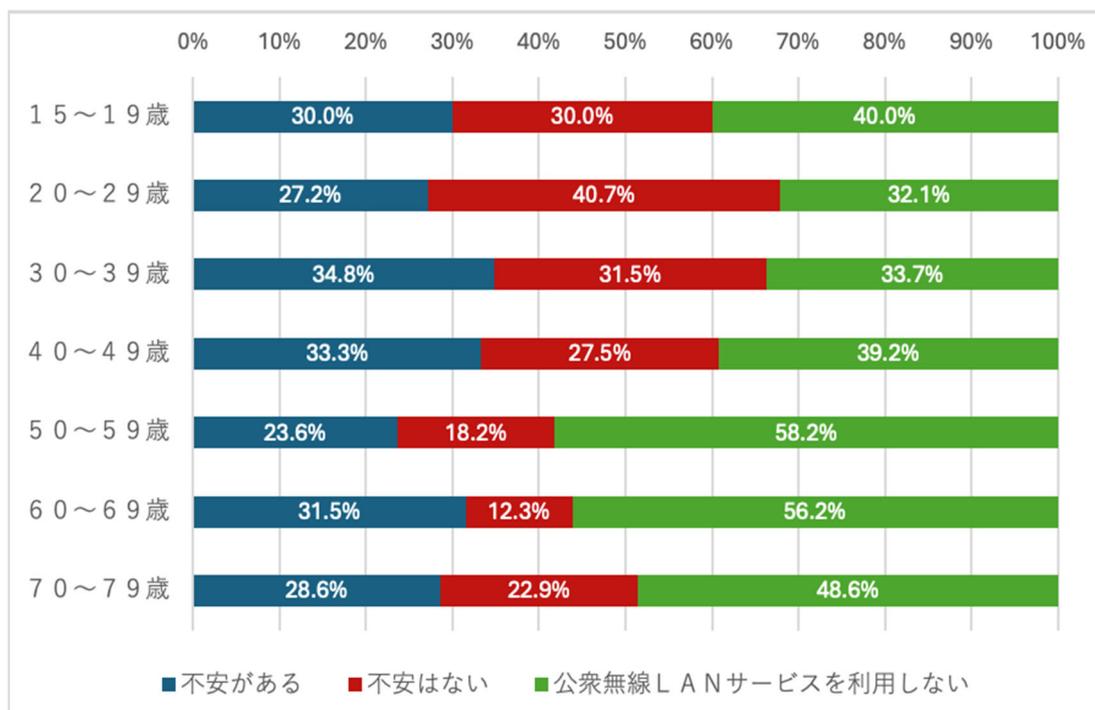
図表 2-1-50 公衆無線 LAN 利用が不安なサービス (Q40)



全体的に、公衆無線 LAN ユーザの 3 分の 1 強が仕事（テレワーク／外出先での業務など）での利用に不安を感じている。その傾向は高齢層（60 歳以上）と中年層（30 歳から 49 歳）強く、熟年層（50 歳代）は不安がない傾向である。

図表 2-1-51 公衆無線 LAN 利用が不安なサービス（Q40）×年代

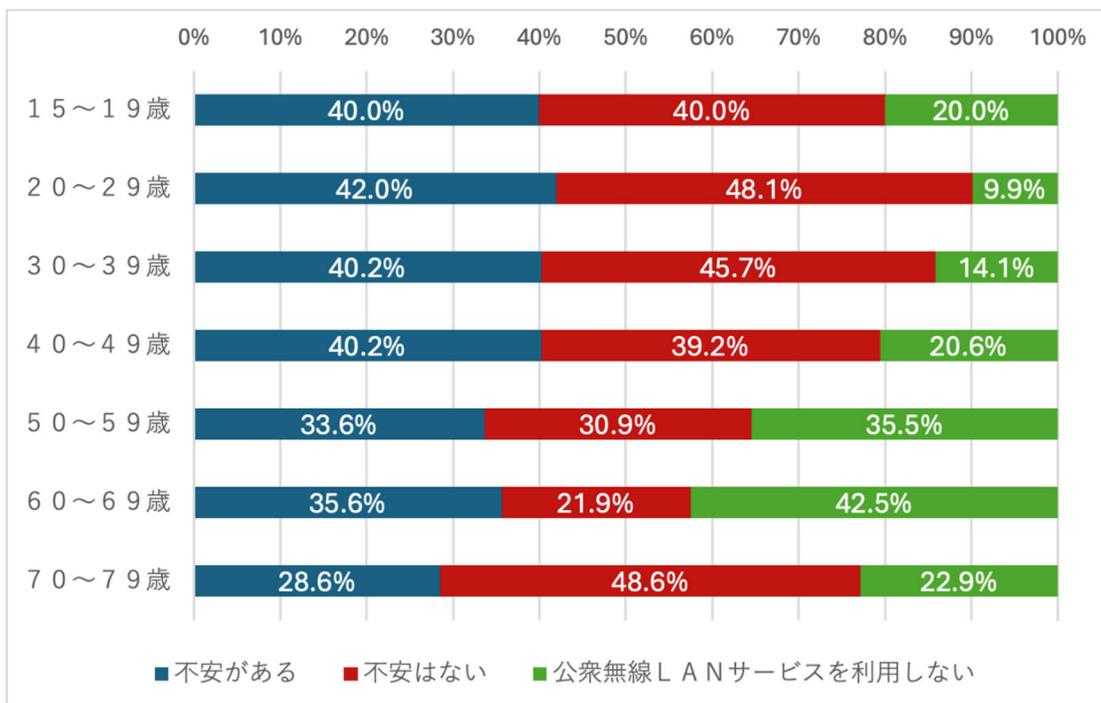
2. 仕事(テレワーク/外出先での業務など)



公衆無線 LAN ユーザの 4 割程度が SNS での利用に不安を感じているが、その傾向は 15 歳から 49 歳までの層のユーザに強く、年代があがるにつれ、不安層の比率は減少する傾向にある。

図表 2-1-52 公衆無線 LAN 利用が不安なサービス (Q40) ×年代

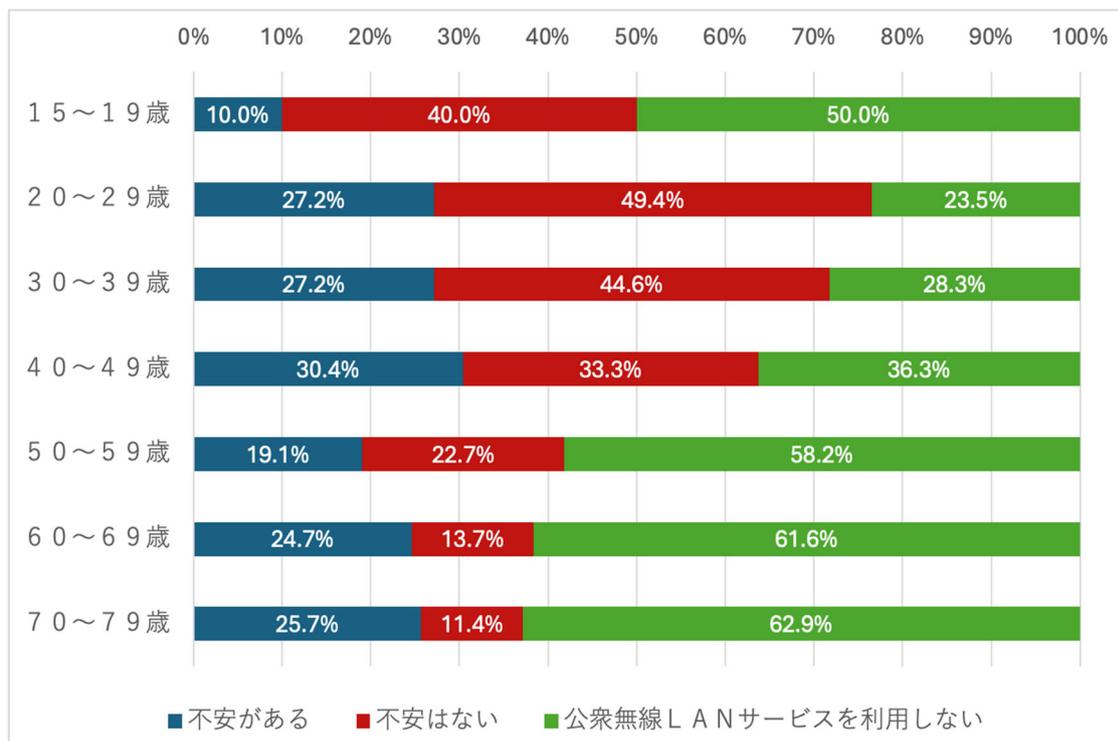
3. SNS



オンラインゲームでの利用には公衆無線 LAN ユーザの 3 割弱が不安を感じているが、その傾向は 20 歳から 49 歳代のユーザに強く、特に若い (15 歳から 20 歳) ユーザや高齢 (50 歳から 79 歳) のユーザでは、不安層の比率は減少する傾向にある。

図表 2-1- 53 公衆無線 LAN 利用が不安なサービス (Q40) ×年代

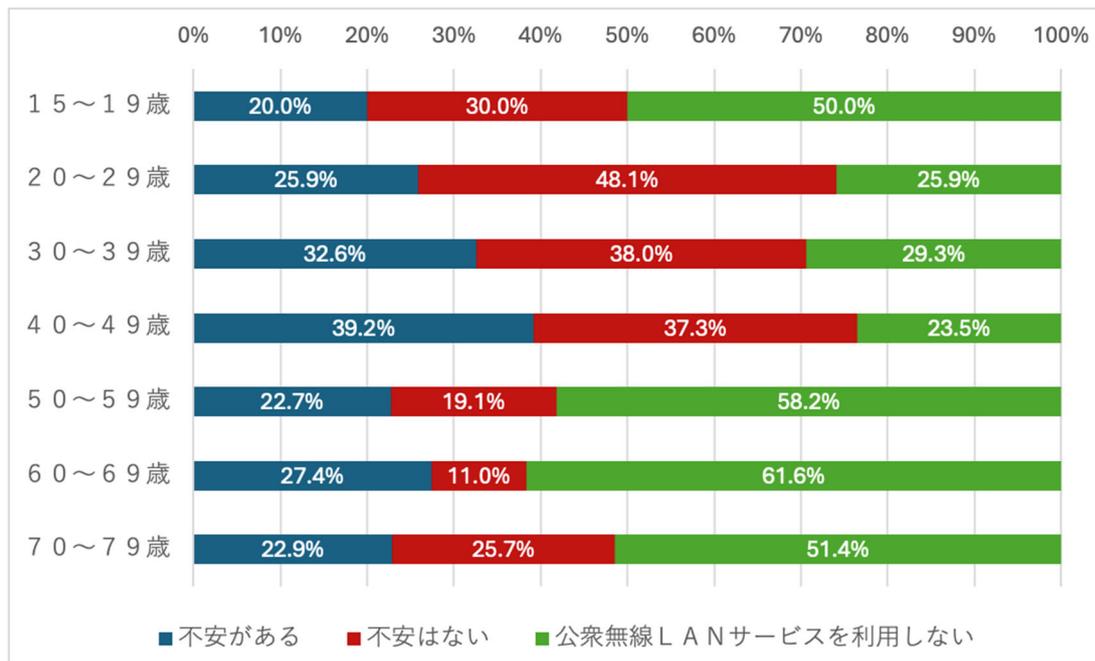
11. オンラインゲーム



全体的に、公衆無線 LAN ユーザの 3 分の 1 弱がアプリケーション・OS の更新やダウンロードでの利用に不安を感じているが、特に、20 歳から 49 歳の層が不安を感じていることが目立つ。また、不安を感じないユーザは若年層に多く、高年層に少ない。50 歳以上では、サービスを利用しないユーザが多い。

図表 2-1-54 公衆無線 LAN 利用が不安なサービス (Q40) ×年代

12. アプリケーション・OS の更新やダウンロード

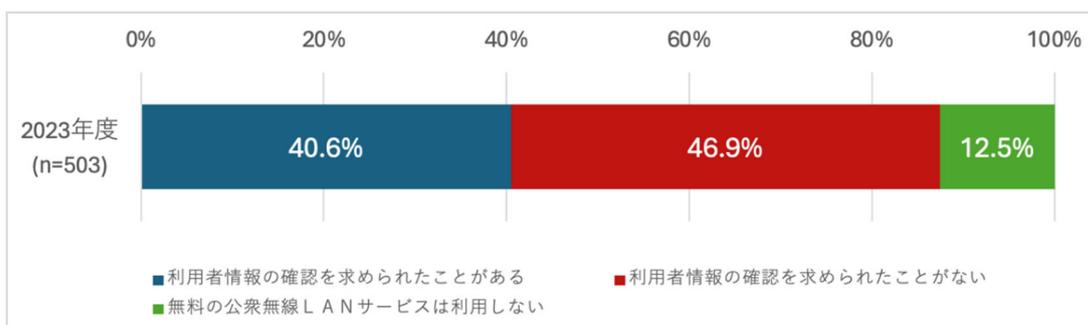


⑮ 公衆無線 LAN 利用時の利用者情報の確認 (Q41)

全体的に、公衆無線 LAN 利用時に、SNS アカウント・メールアドレス・携帯電話番号などの利用者情報の確認を求められたことがあるユーザは約 41%である。

他方、利用者情報の確認を求められたことのないユーザは約 47%、と拮抗している。

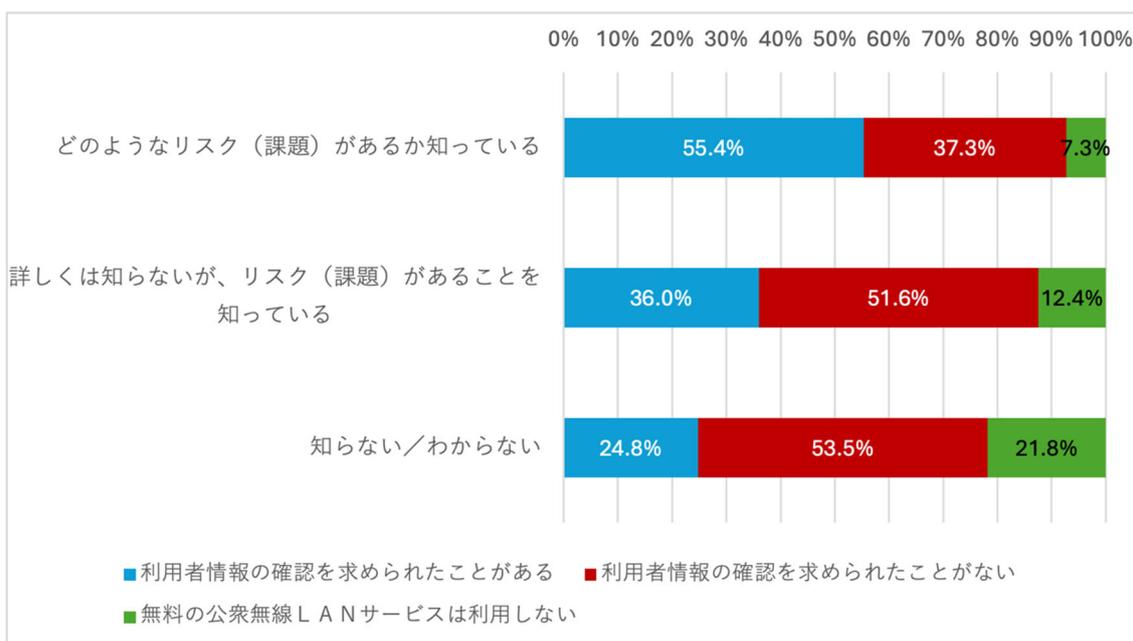
図表 2-1-55 公衆無線 LAN 利用時の利用者情報の確認 (Q41)



無線 LAN のリスクを認知している公衆無線 LAN ユーザの約 55%は公衆無線 LAN 利用時に、SNS アカウント・メールアドレス・携帯電話番号などの利用者情報の確認を求められたことがある。一方、リスクを認知していない公衆無線 LAN ユーザは約 25%程度しか利用者情報の確認を求められていない。

実際には、「利用者情報の確認」というプロセスに対する認識に差異が大きいものと想定される。

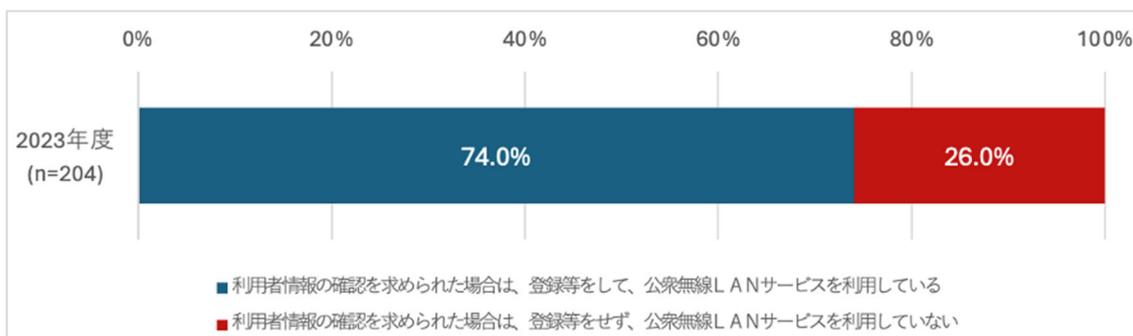
図表 2-1-56 公衆無線 LAN 利用時の利用者情報の確認 (Q41) × リスク認知



⑩ 公衆無線 LAN 利用時の利用者情報確認への対応 (Q42)

サービス利用時に利用者情報の確認を求められた場合、登録等をして、公衆無線 LAN サービスを利用しているユーザが約 74%なのに対して、利用者情報の確認を求められた場合には登録等をせず、公衆無線 LAN サービスを利用しないユーザは約 26%である。

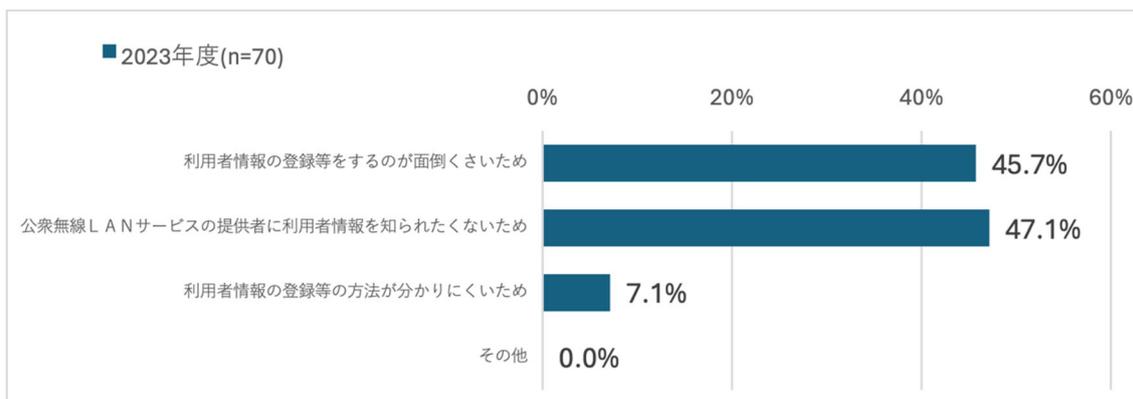
図表 2-1-57 公衆無線 LAN 利用時の利用者情報確認への対応 (Q42)



⑪ 公衆無線 LAN 利用時の利用者情報確認の拒否理由 (Q43)

ユーザが、利用者情報の確認を求められた場合には登録等をせず、公衆無線 LAN サービスを利用しない理由として最も多いのは、公衆無線 LAN サービス提供者に利用者情報を知られたくないためで、約 47%にのぼる。

図表 2-1-58 公衆無線 LAN 利用時の利用者情報確認の拒否理由 (Q43)

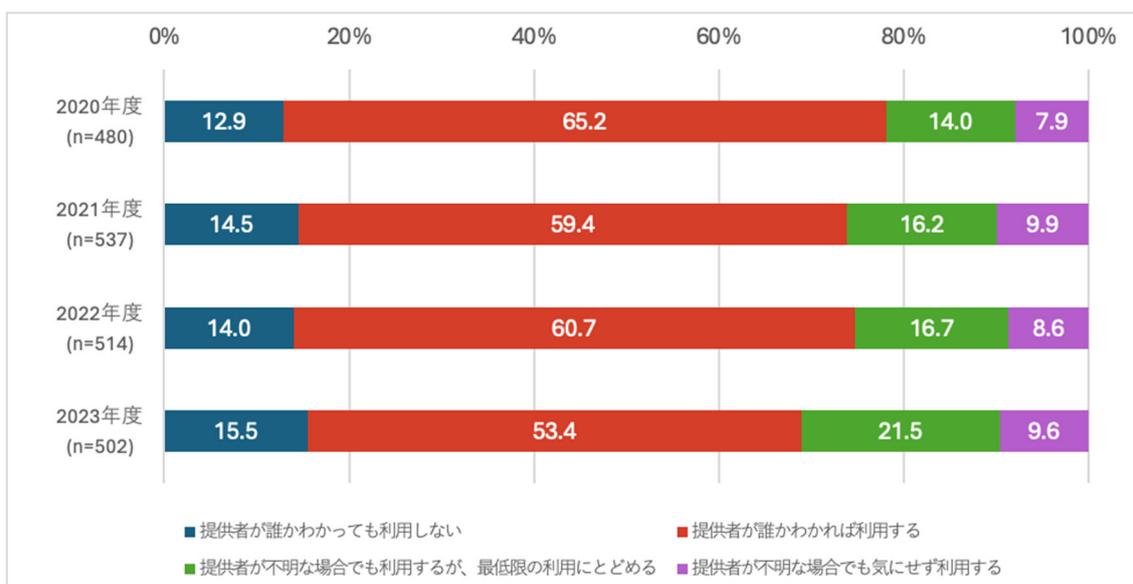


(4) 公衆無線 LAN 利用 (その2: SSID 確認)

① パスワード不要の無線 LAN を見つけた際の利用有無 (Q20)

外出先でパスワードなしで接続可能な無線 LAN を見つけた場合、提供者が分かっても利用しないユーザが約 16%であり、増加傾向にある。一方で、提供者が不明でも利用するユーザが約 32%なのに対して、提供者が分かれば利用するユーザは約 53%であり、提供者の顕名性が重視されていることが分かる。

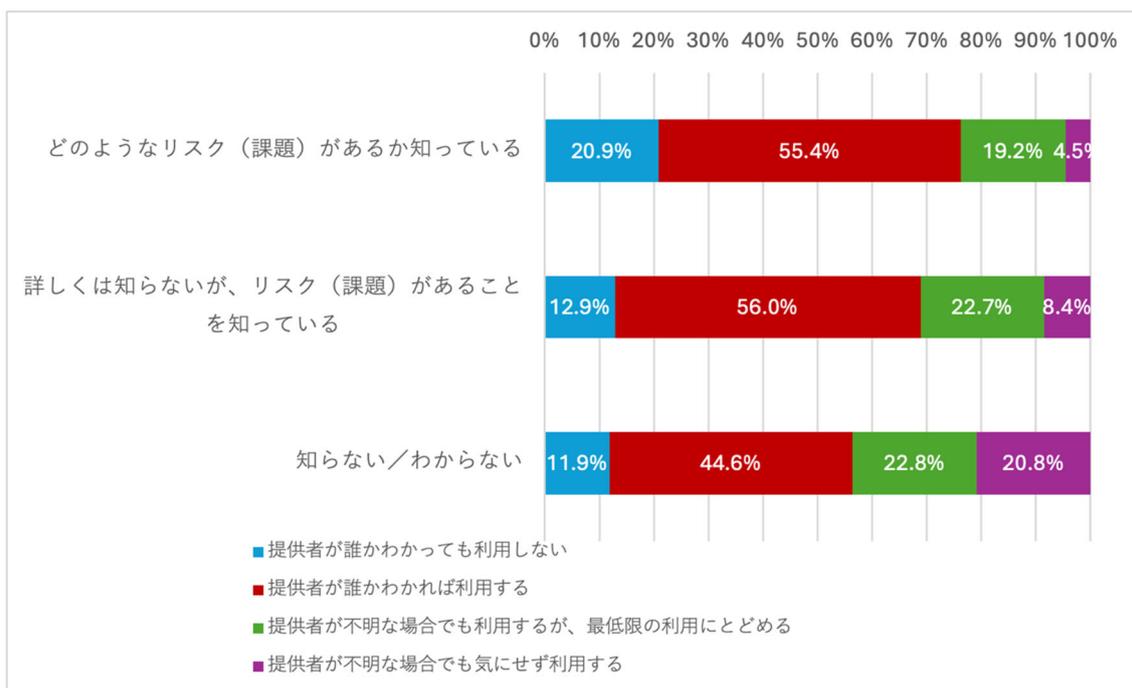
図表 2-1-59 パスワード不要の無線 LAN を見つけた際の利用有無 (Q20)



無線 LAN のリスクを認知している公衆無線 LAN ユーザの約 21%は、外出先でパスワードなしで接続可能な無線 LAN を見つけた場合、提供者が分かっても利用しないのに対し、リスクを認知していない公衆無線 LAN ユーザでは約 12%程度に留まる。

むしろ、リスクを認知していないユーザは、提供者が不明な場合でも気にせず利用するユーザが約 5 分の 1 と高い比率を示している。

図表 2-1-60 パスワード不要の無線 LAN を見つけた際の利用有無 (Q20) × リスク認知

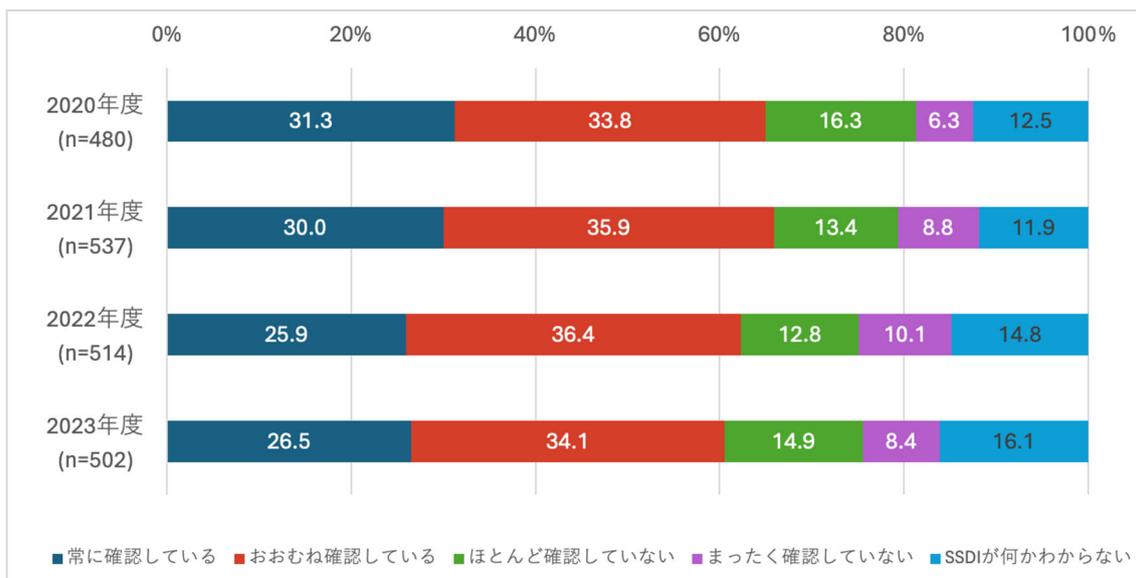


② 公衆無線 LAN 利用時の SSID 確認 (Q22)

公衆無線 LAN サービスを外出先で利用する場合に、常に SSID を確認しているユーザは約 27%に過ぎず、年々、その比率が減少している。

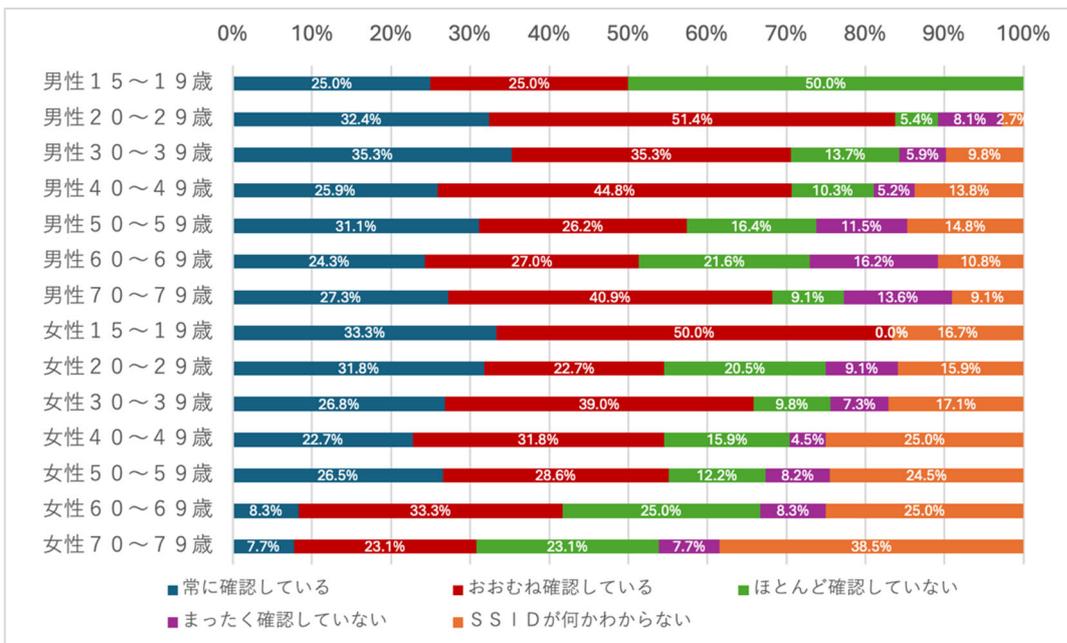
SSID が何か分からない公衆無線 LAN ユーザも約 16%おり、増加している。

図表 2-1-61 公衆無線 LAN 利用時の SSID 確認 (Q22)



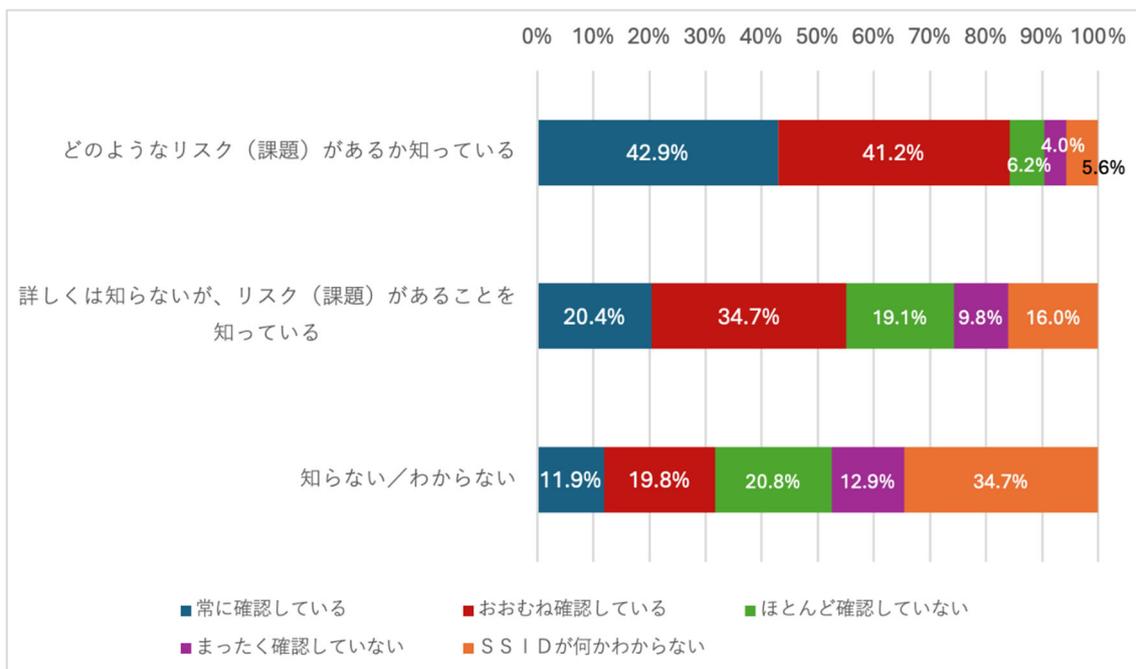
若年層の公衆無線 LAN ユーザは、公衆無線サービスを外出先で利用する場合に、常に SSID を確認している比率が 3～4 割前後と比較的高いが、高年層のユーザは 1～3 割程度に過ぎない。特に、高年層の女性で（60 歳から 79 歳）の確認率が低い。

図表 2-1-62 公衆無線 LAN 利用時の SSID 確認 (Q22) × 性年代



無線 LAN のリスクを認知している公衆無線 LAN ユーザの 4 割以上が、公衆無線 LAN サービスを外出先で利用する場合に、常に SSID を確認しているが、リスクを認知していないユーザは約 1 割に留まっている。

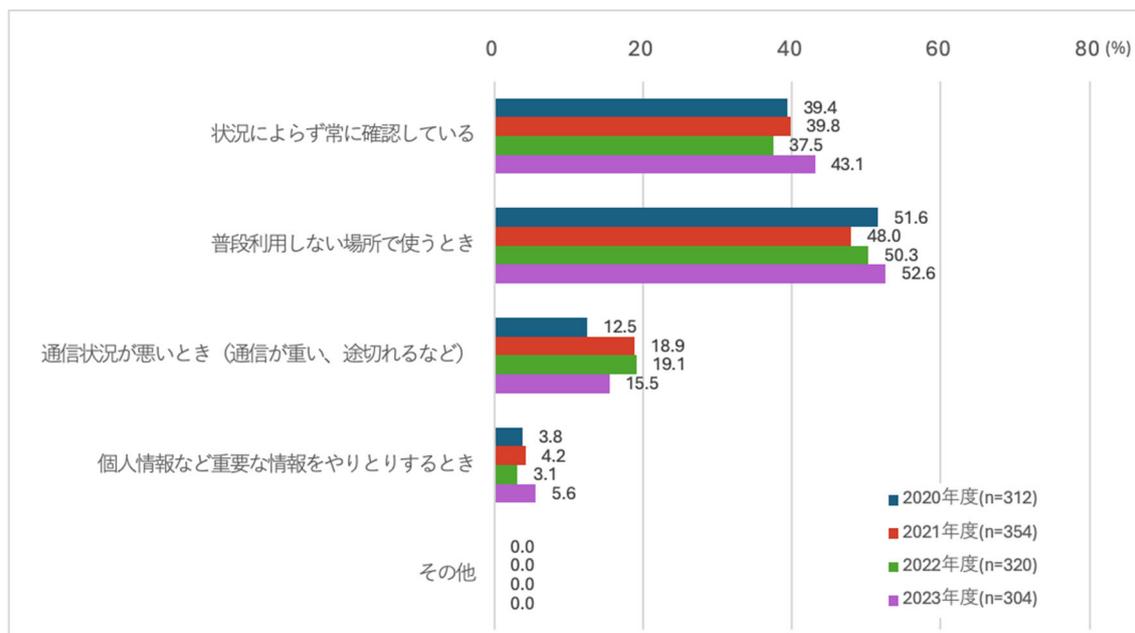
図表 2-1-63 公衆無線 LAN 利用時の SSID 確認 (Q22) × リスク認知



③ 公衆無線 LAN の SSID の確認場面 (Q23)

公衆無線 LAN サービスを外出先で利用する場合、SSID を確認するユーザのうち、状況によらず確認するユーザは約 43%であり、増加している。普段利用しない場所(約 53%)や通信状況が悪いとき(約 16%)に確認するユーザが多い。

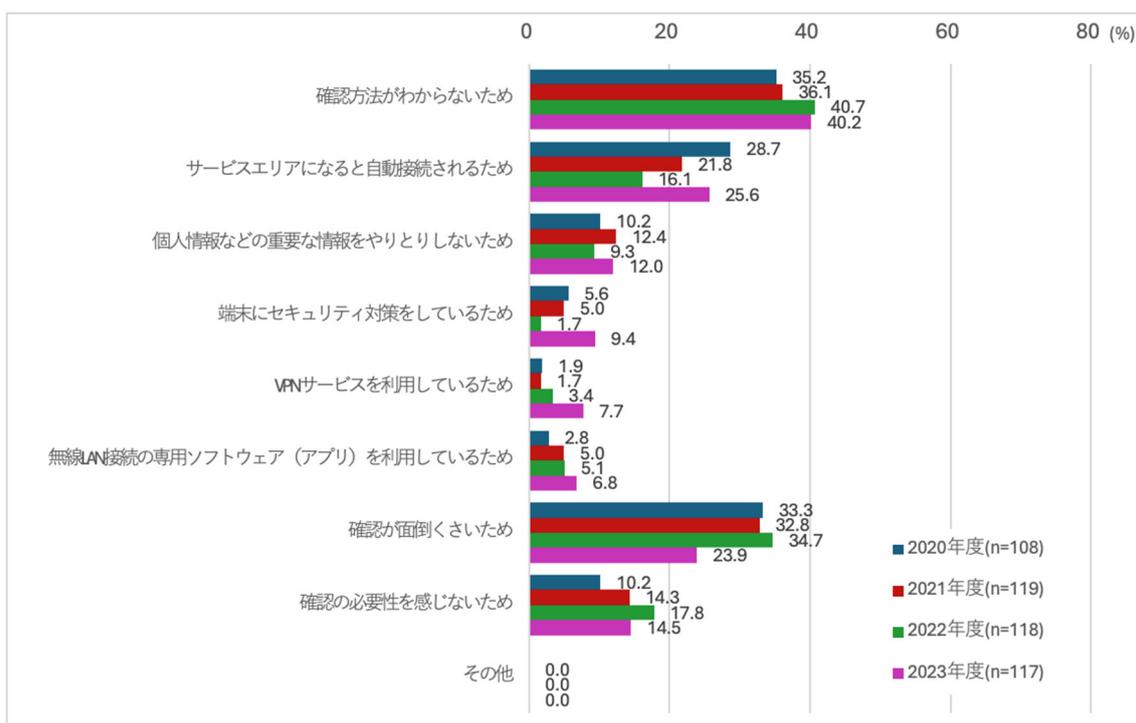
図表 2-1-64 公衆無線 LAN の SSID の確認場面 (Q23)



④ 公衆無線 LAN の SSID を確認しない理由 (Q24)

公衆無線 LAN サービスを外出先で利用する場合、SSID を確認しないユーザは、確認方法がわからない(約 40%)や確認が面倒くさい(約 24%)とするユーザが大半を占め、確認の必要性を感じない(約 15%)、を含め、セキュリティ意識が低いと言わざるを得ない理由を挙げるユーザもある。

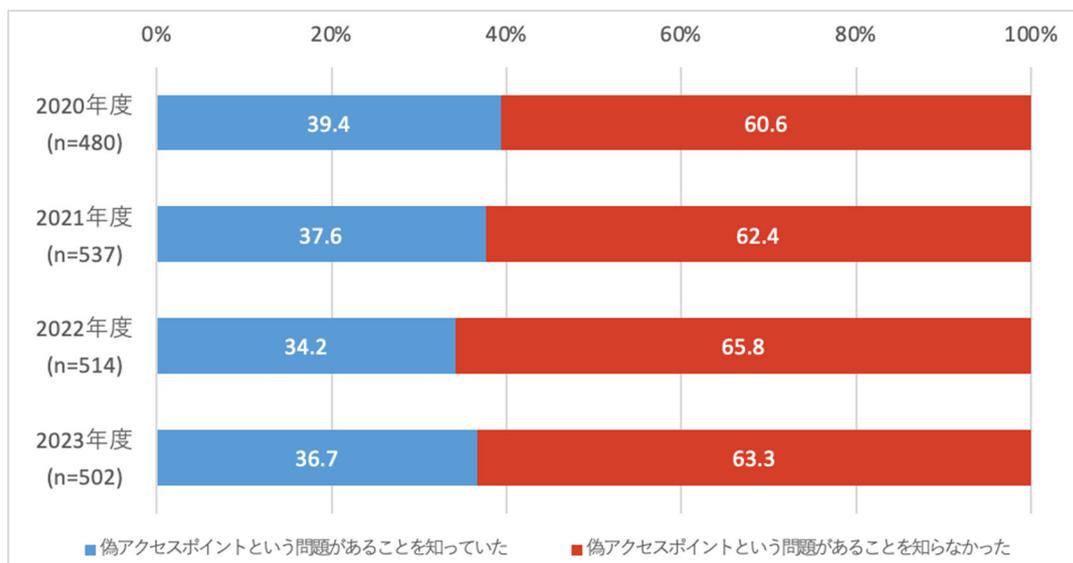
図表 2-1-65 公衆無線 LAN の SSID を確認しない理由 (Q24)



⑤ 偽アクセスポイント問題の認知状況 (Q25)

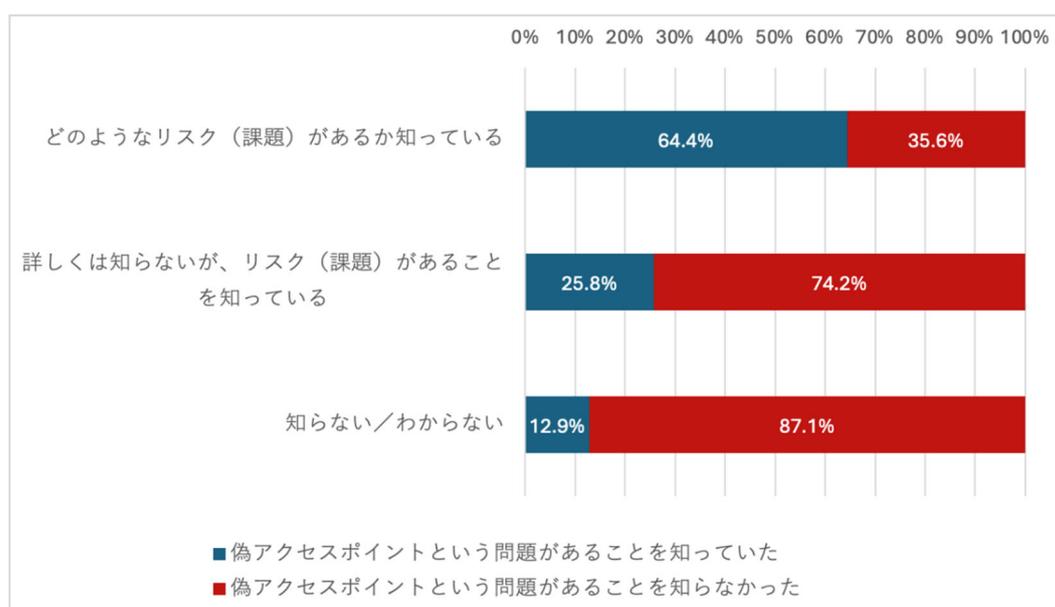
公衆無線 LAN ユーザのうち、偽アクセスポイント問題を認識しているユーザは約 37%に過ぎず、認識率は横ばいである。

図表 2-1-66 偽アクセスポイント問題の認知状況 (Q25)



無線 LAN のリスクを認知している公衆無線 LAN ユーザのうち、約 6 割以上のユーザが偽アクセスポイント問題を認識しているのに対し、無線 LAN のリスクを認知していないユーザでは 1 割程度しか偽アクセスポイント問題を認識していない。

図表 2-1-67 偽アクセスポイント問題の認知状況 (Q25) × リスク認知



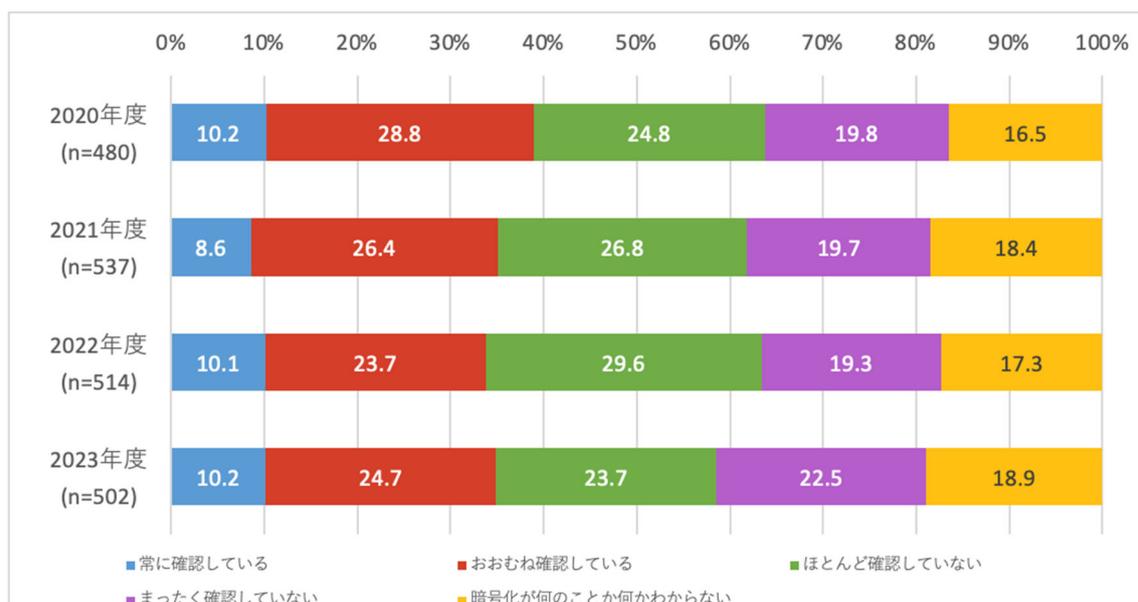
(5) 公衆無線 LAN 利用 (その3: 暗号化確認)

① 公衆無線 LAN 利用時の暗号化確認 (Q27)

公衆無線 LAN サービスを外出先で利用する場合に、無線区間の暗号化を常に確認しているユーザは約 10%に過ぎず、概ね確認しているユーザを含めても約 35%で、年々、その比率が減少している。

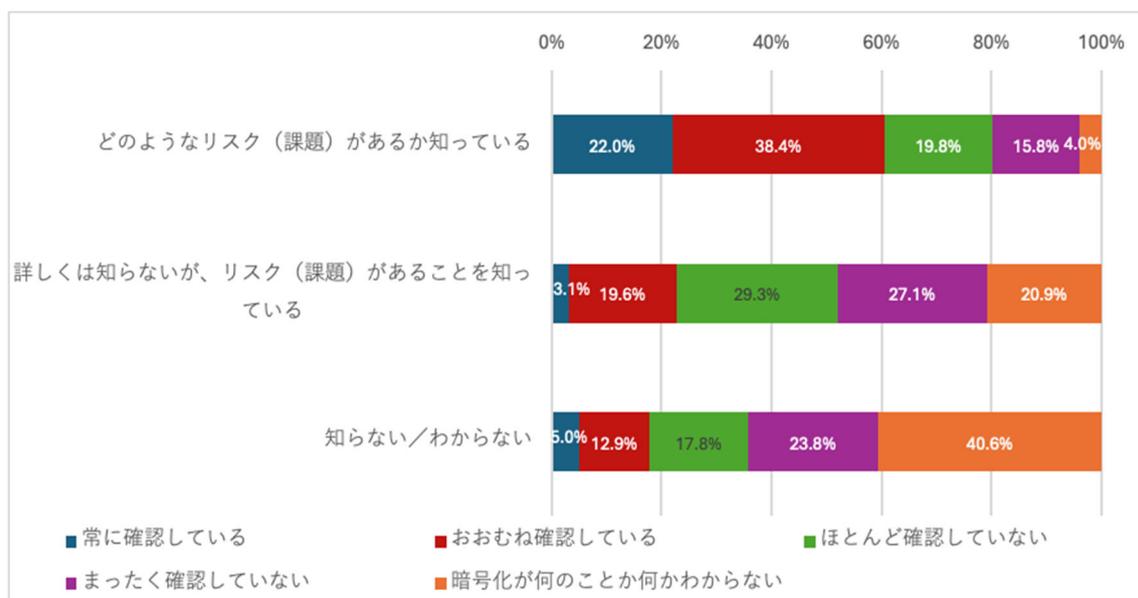
無線区間の暗号化が何か分からない公衆無線 LAN ユーザも約 19%いる。

図表 2-1-68 公衆無線 LAN 利用時の暗号化確認 (Q27)



無線 LAN のリスクを認知している公衆無線 LAN ユーザの 2 割以上が、サービスを外出先で利用する場合に、無線区間の暗号化を常に確認しているのに対し、無線 LAN のリスクを認知していないユーザは 5%程度に過ぎず、概ね確認しているユーザを含めても 2 割に満たない。また、暗号化のことを知らないユーザが多い。

図表 2-1-69 公衆無線 LAN 利用時の暗号化確認 (Q27) × リスク認知

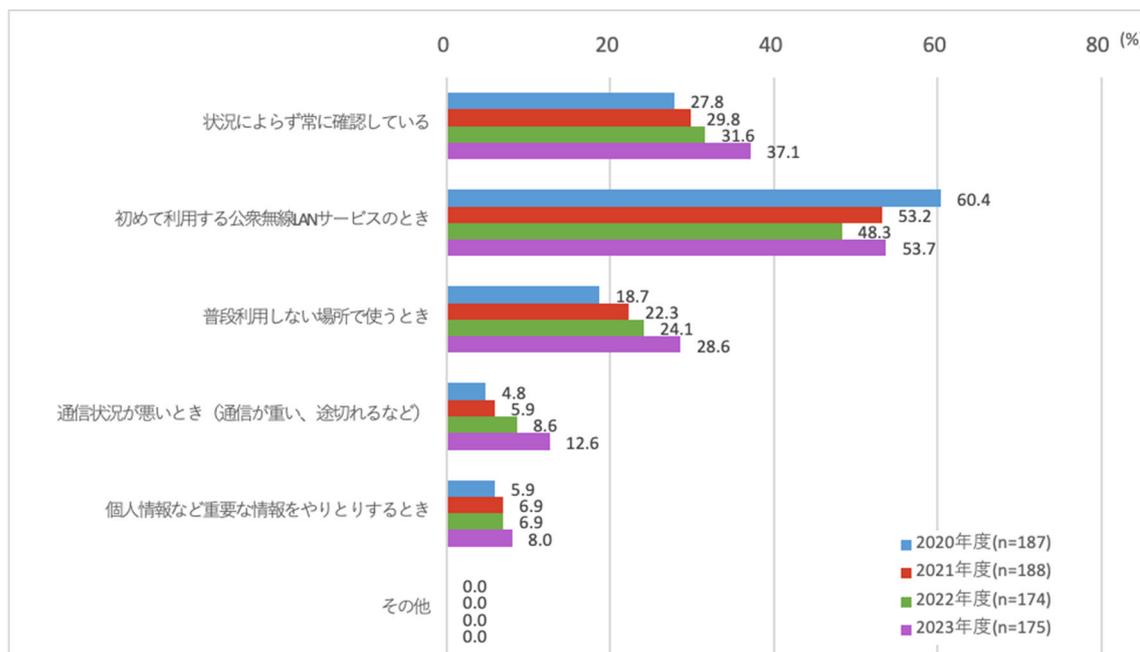


② 公衆無線 LAN の暗号化の確認場面 (Q28)

公衆無線 LAN サービスを外出先で利用する場合、無線区間の暗号化を確認するユーザーのうち、状況によらず確認するユーザーは約 37%。初めて利用する公衆無線 LAN サービスのとき(約 54%)や普段利用しない場所(約 29%)に確認するユーザーが多い。

また、全般的に、暗号化を確認するユーザーの比率は、年々、増えてきている。

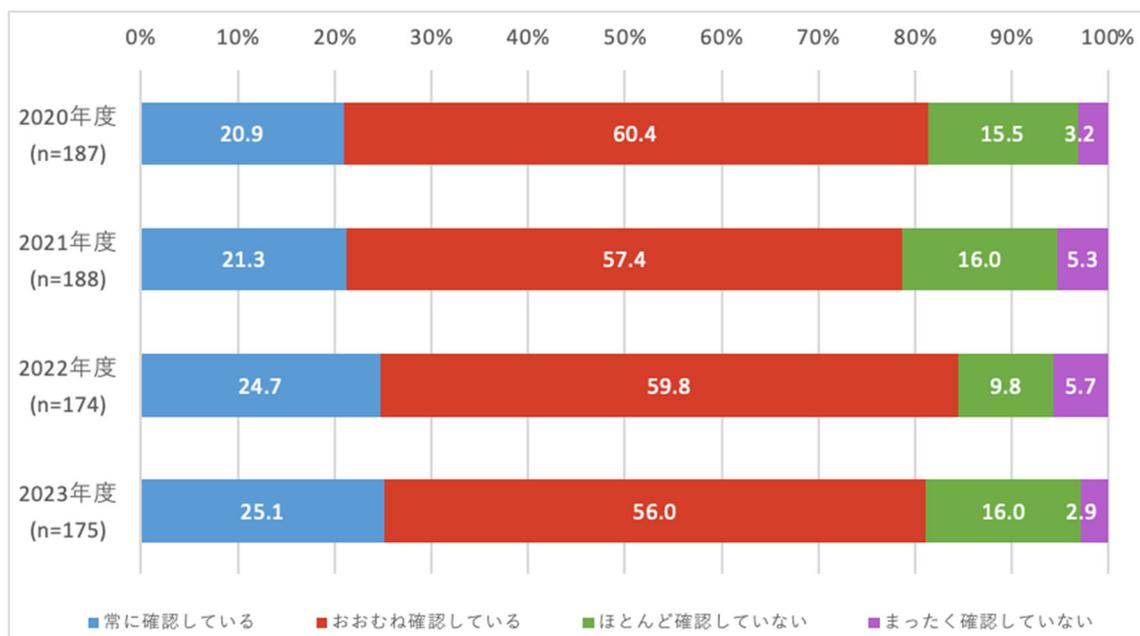
図表 2-1- 70 公衆無線 LAN の暗号化の確認場面 (Q28)



③ 暗号化有無に加えて方式(WPA等)確認 (Q29)

公衆無線 LAN サービスを外出先で利用する場合に、無線区間の暗号化を確認しているユーザのうち、暗号化の有無に加えて暗号化の種類も確認しているユーザが(常に+概ねを合わせて)81%となっている。

図表 2-1-71 暗号化有無に加えて方式(WPA等)確認 (Q29)

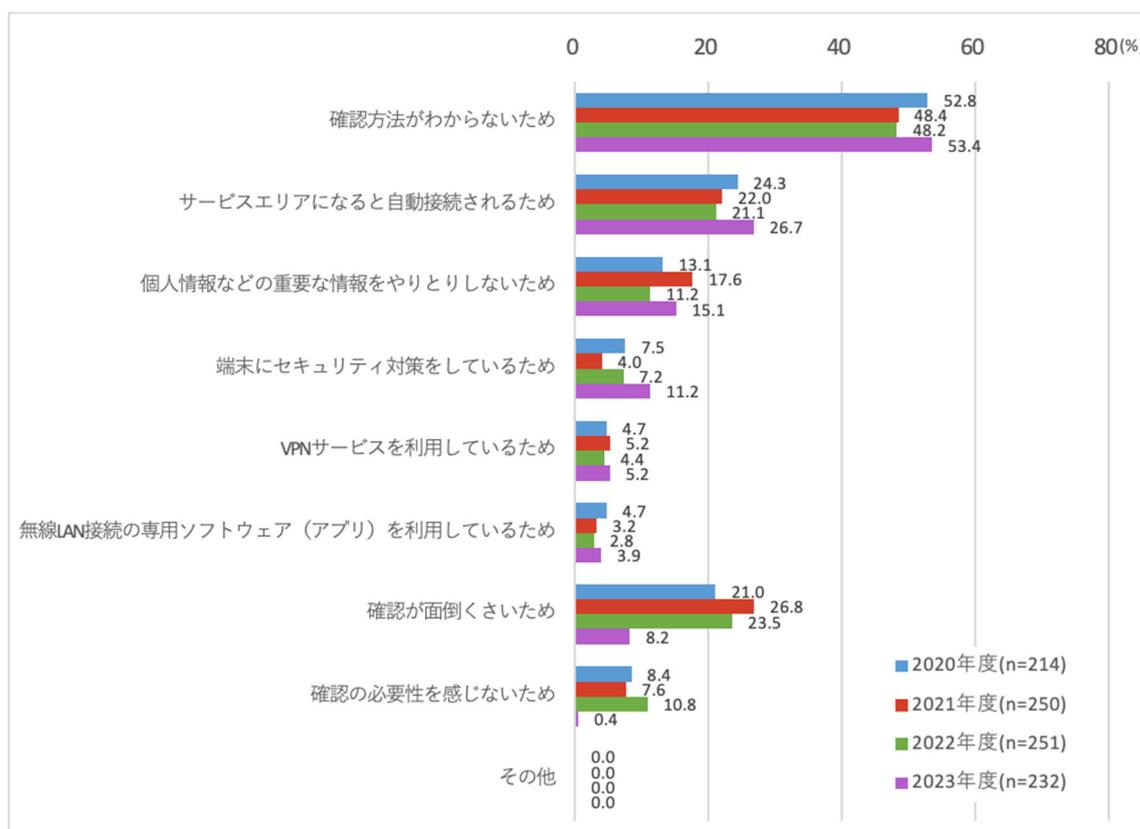


④ 公衆無線 LAN の暗号化を確認しない理由 (Q30)

公衆無線 LAN サービスを外出先で利用する場合、暗号化を確認しないユーザは、確認方法がわからない(約 53%)やサービスエリアでは自動接続されるため (約 27%)とするユーザが多い。

ほかには、確認が面倒くさいことを理由とするユーザも一定数いる(約 8%)。

図表 2-1-72 公衆無線 LAN の暗号化を確認しない理由 (Q30)



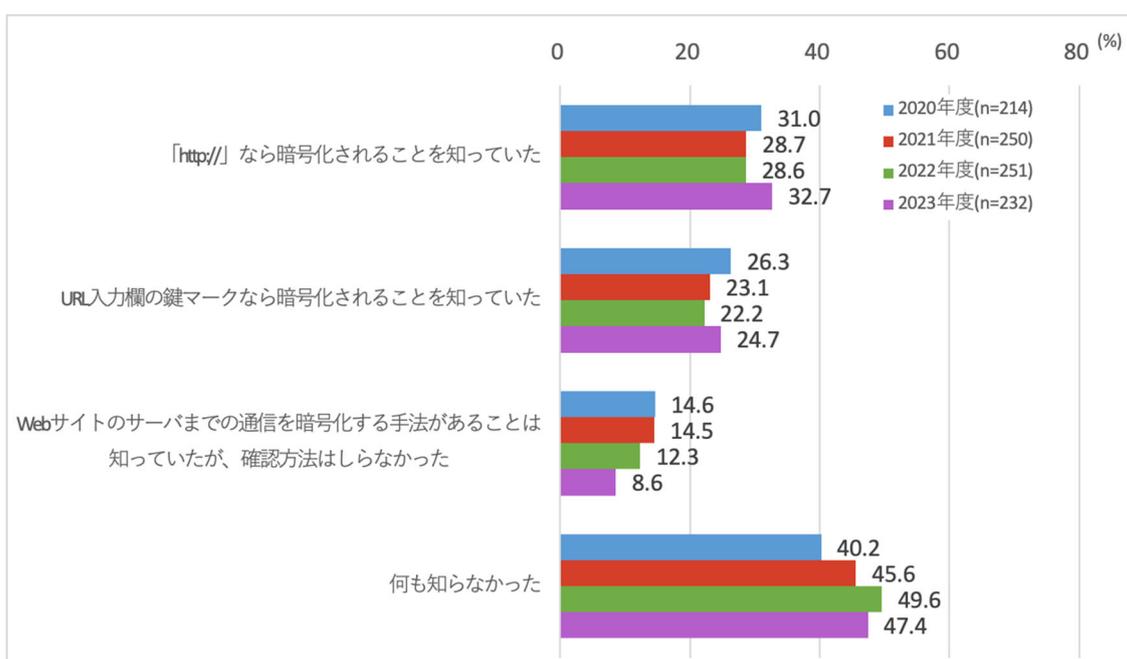
(6) 公衆無線 LAN 利用 (その 4 : HTTPS 通信確認)

① HTTPS 通信の認知状況 (Q31)

公衆無線 LAN ユーザのうち、Web サイトの閲覧等の際に、手元の端末から、Web サイトのサーバまでの間の通信を暗号化する手法としての HTTPS 通信について、知らないユーザが約 47%おり、年々、増加傾向にある。

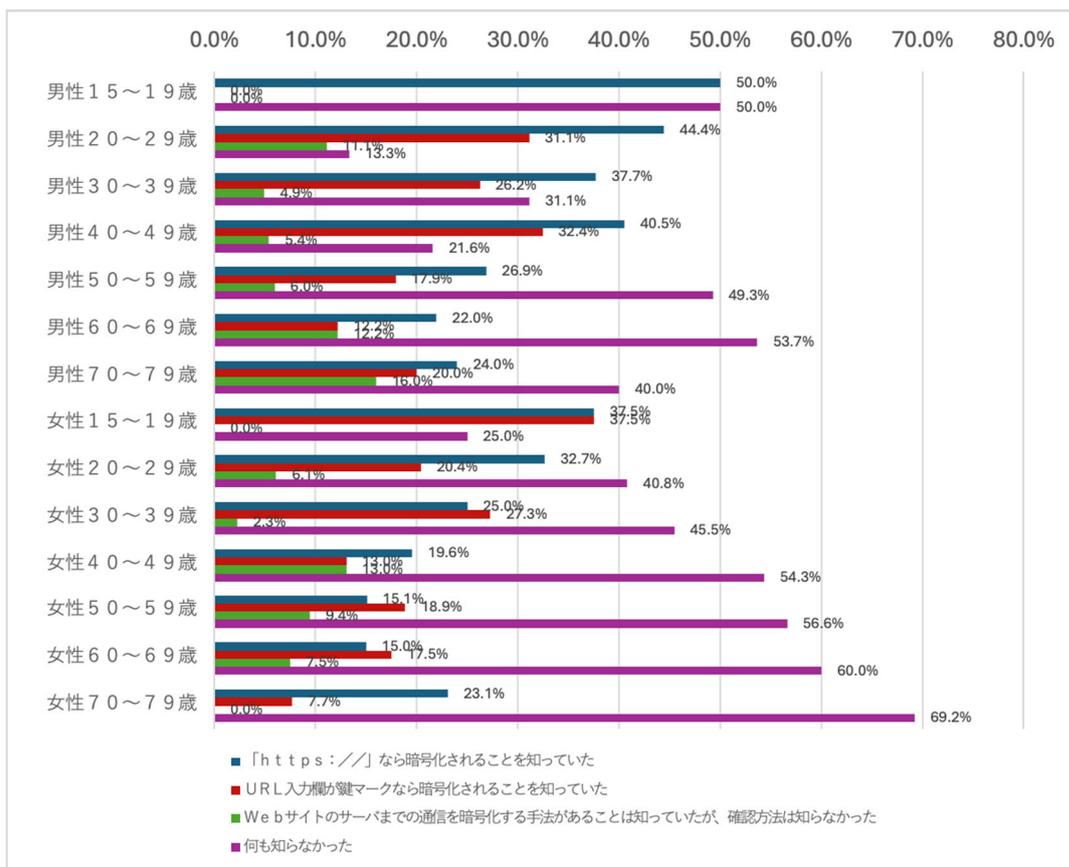
HTTPS 通信の具体的な理解のうち、確認方法は知らなかったというユーザは、減少している。

図表 2-1-73 HTTPS 通信の認知状況 (Q31)



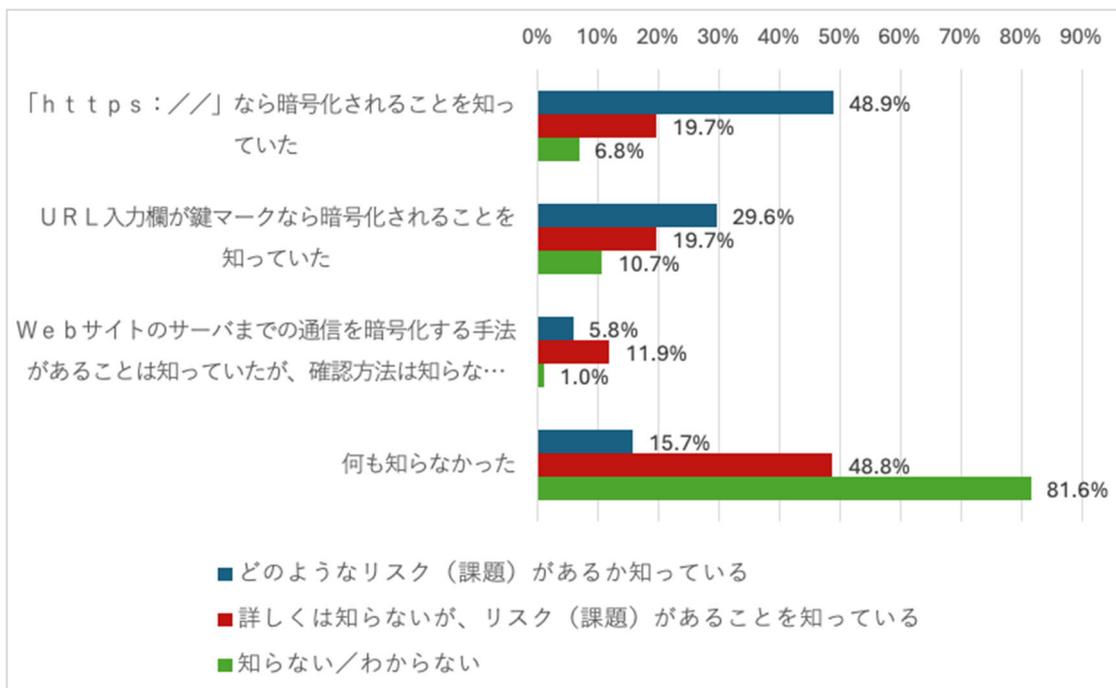
HTTPS 通信の認知について、公衆無線 LAN ユーザの性・年代による差異が大きく、若年層・中年層の男性ユーザは、https://なら暗号化されることを認識しているユーザが4~5割程度いるのに対して、女性ユーザや高年層の男性ユーザは、HTTPS 通信を知らないユーザが最も多い。

図表 2-1-74 HTTPS 通信の認知状況 (Q31) × 性年代



HTTPS 通信について認知している公衆無線 LAN ユーザは、無線 LAN のリスクを認知しているユーザが多く、HTTPS 通信について認知していない公衆無線 LAN ユーザは、無線 LAN のリスクを認知していないユーザが多い。

図表 2-1-75 HTTPS 通信の認知状況 (Q31) × リスク認知

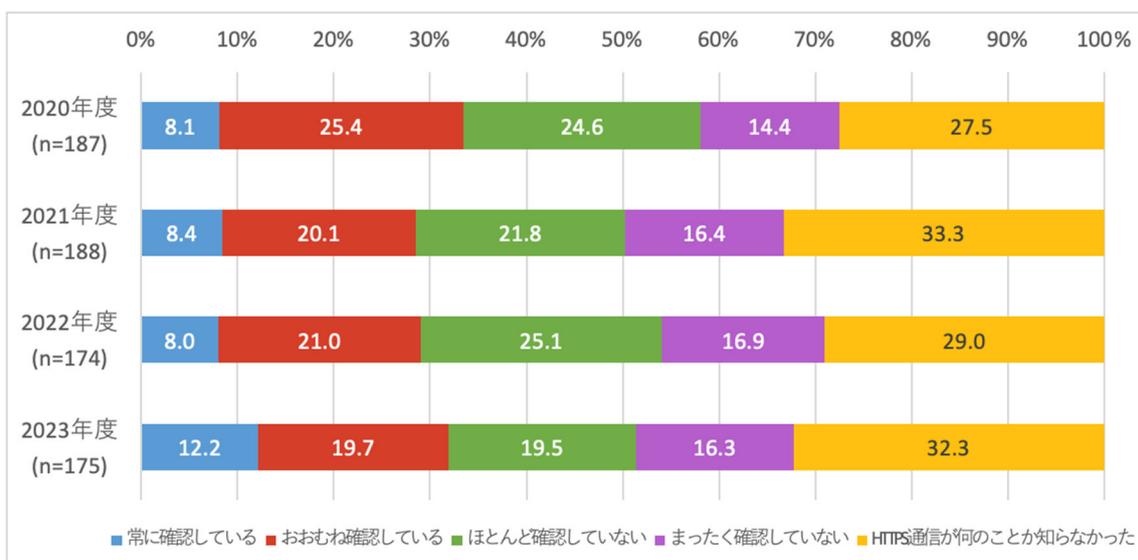


② 公衆無線 LAN 利用時の HTTPS 通信確認 (Q32)

公衆無線 LAN サービスを外出先で利用する場合に、HTTPS 通信の有無を常に確認しているユーザは約 12%に過ぎず、概ね確認しているユーザを含めても約 32%で、その比率は増加傾向にある。

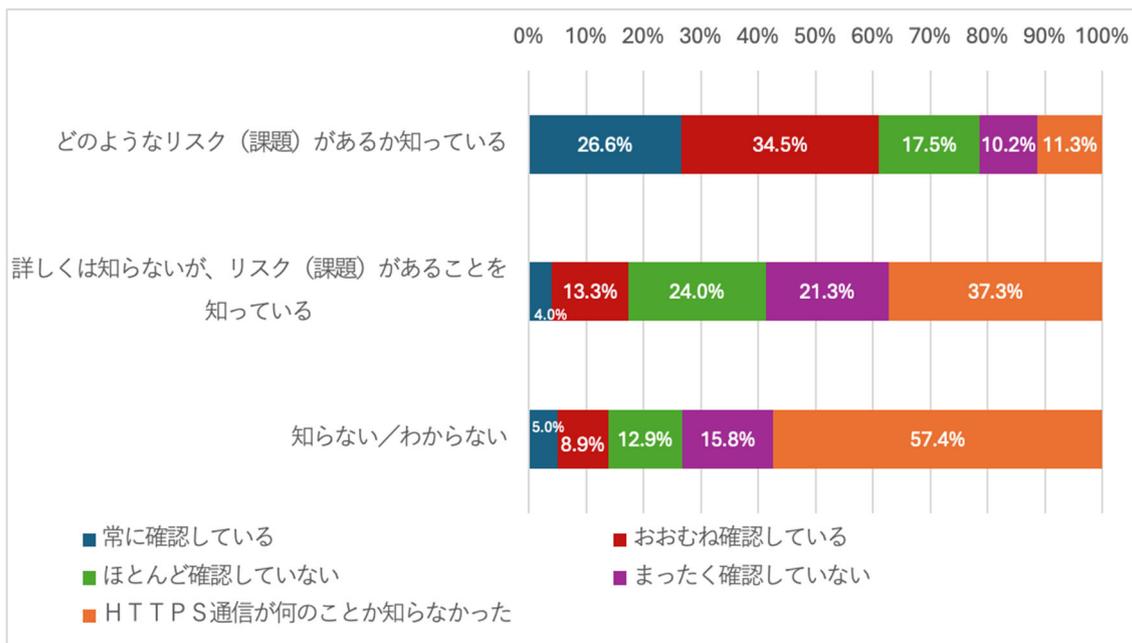
HTTPS 通信が何か分からない公衆無線 LAN ユーザも約 32%いる。

図表 2-1-76 公衆無線 LAN 利用時の HTTPS 通信確認 (Q32)



無線 LAN のリスクを認知している公衆無線 LAN ユーザは、約 6 割程度が公衆無線 LAN 利用時に HTTPS 通信を確認しているが、無線 LAN のリスクを認知していないユーザは 14%程度しか HTTPS 通信を確認しておらず、そもそも HTTPS 通信が何か分からないユーザが約 6 割いる。

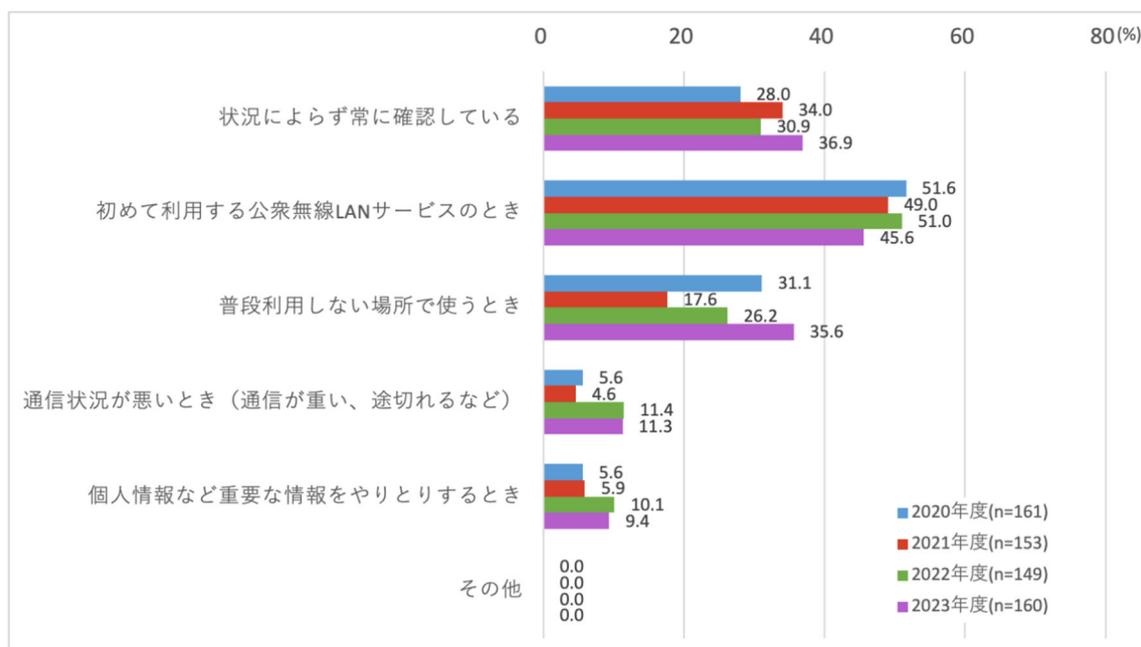
図表 2-1-77 公衆無線 LAN 利用時の HTTPS 通信確認 (Q32) × リスク認知



③ 公衆無線 LAN の HTTPS 通信の確認場面 (Q33)

公衆無線 LAN サービスを外出先で利用する場合、HTTPS 通信の有無を確認するユーザのうち、状況によらず確認するユーザは約 37%であり、初めて利用する公衆無線 LAN サービス(約 46%)や普段利用しない場所(約 36%)などの際に確認するユーザが多い。

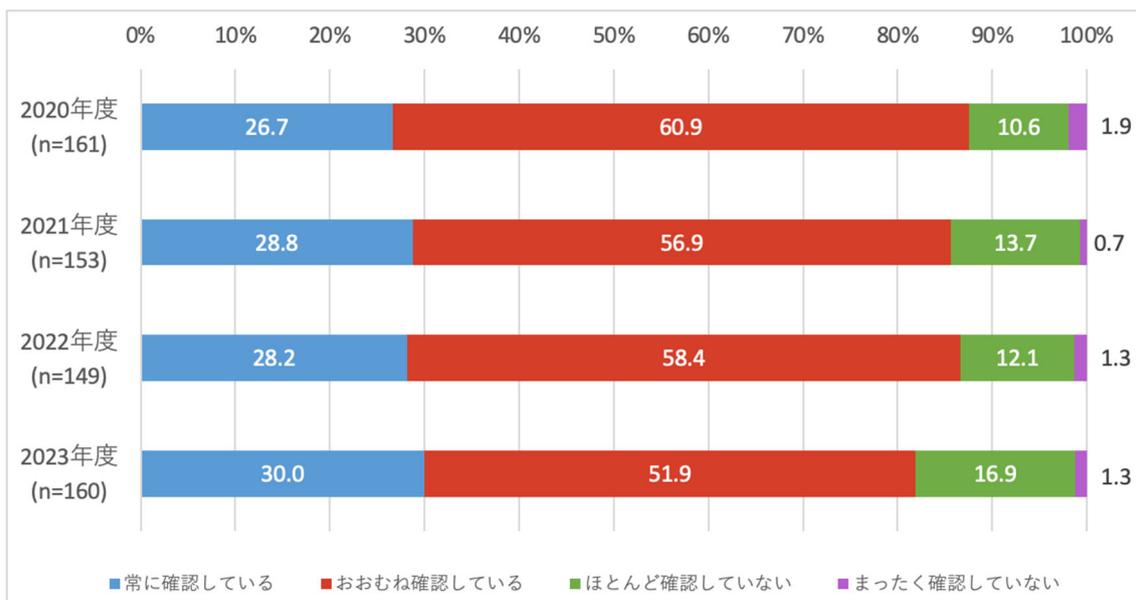
図表 2-1-78 公衆無線 LAN の HTTPS 通信の確認場面 (Q33)



④ HTTPS 通信に加えてドメイン確認 (Q34)

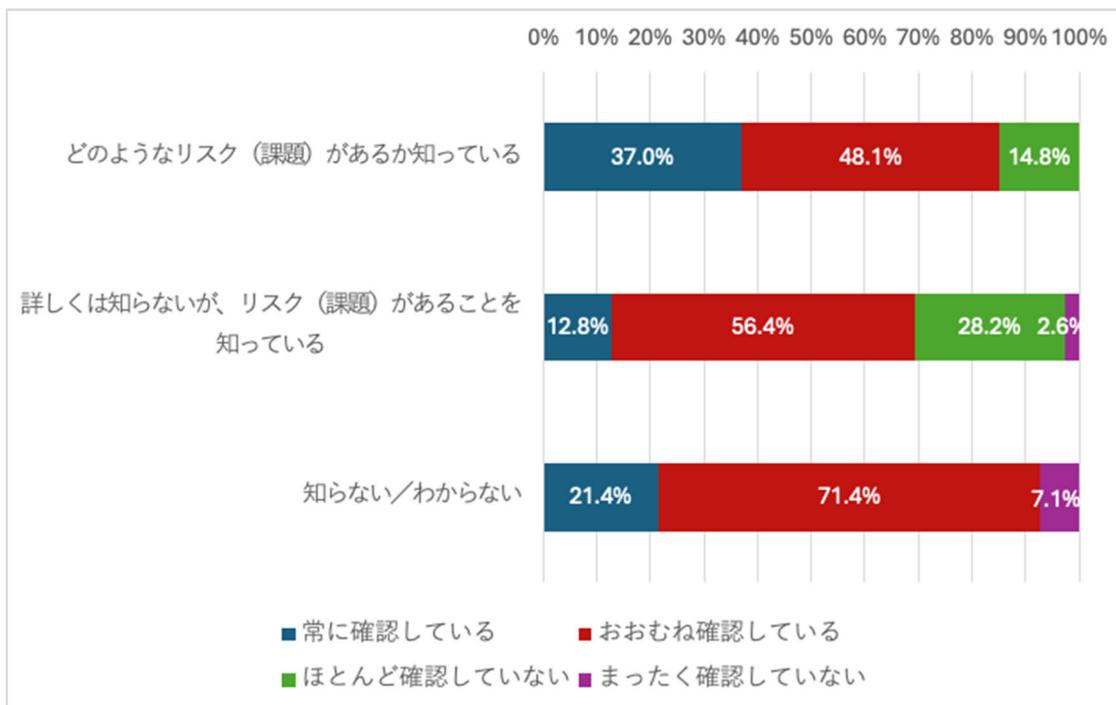
公衆無線 LAN サービスを外出先で利用する場合に、HTTPS 通信の有無を確認しているユーザのうち、HTTPS 通信の有無に加えてドメインも確認しているユーザが(常に+概ねを合わせて)82%となっている。また、まったく確認していないユーザが増えている。

図表 2-1-79 HTTPS 通信に加えてドメイン確認 (Q34)



無線 LAN のリスクを認知している公衆無線 LAN ユーザがサービスを外出先で利用する場合に、HTTPS 通信の有無を確認しているユーザのうち、HTTPS 通信の有無に加えてドメインも確認しているユーザが(常に+概ねを合わせて)約 85%を超えているが。無線 LAN のリスクを認知していない公衆無線 LAN ユーザでまったく確認していないユーザが約 7%である。

図表 2-1-80 HTTPS 通信に加えてドメイン確認 (Q34) ×リスク認知

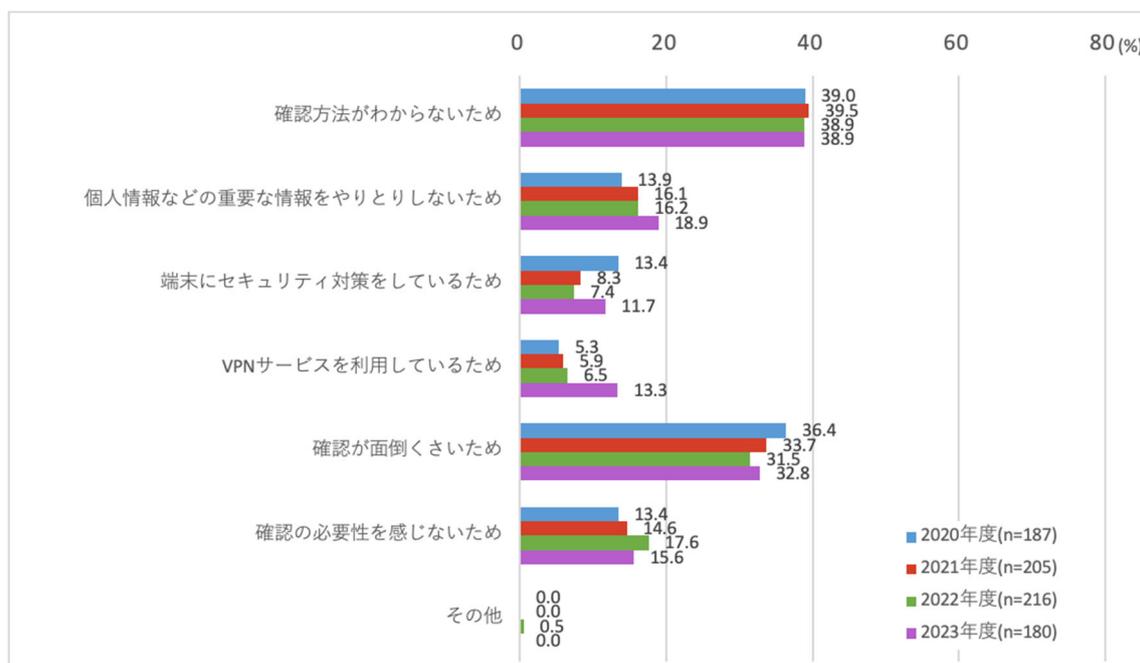


⑤ 公衆無線 LAN の HTTPS 通信を確認しない理由 (Q35)

公衆無線 LAN サービスを外出先で利用する場合、HTTPS 通信を確認しないユーザは、確認方法がわからない(約 39%)や確認が面倒くさい(約 33%)とするユーザが多い。

個人情報などの重要な情報をやりとりしないユーザも約 19%おり、年々、増加傾向にある。

図表 2-1-81 公衆無線 LAN の HTTPS 通信を確認しない理由 (Q35)



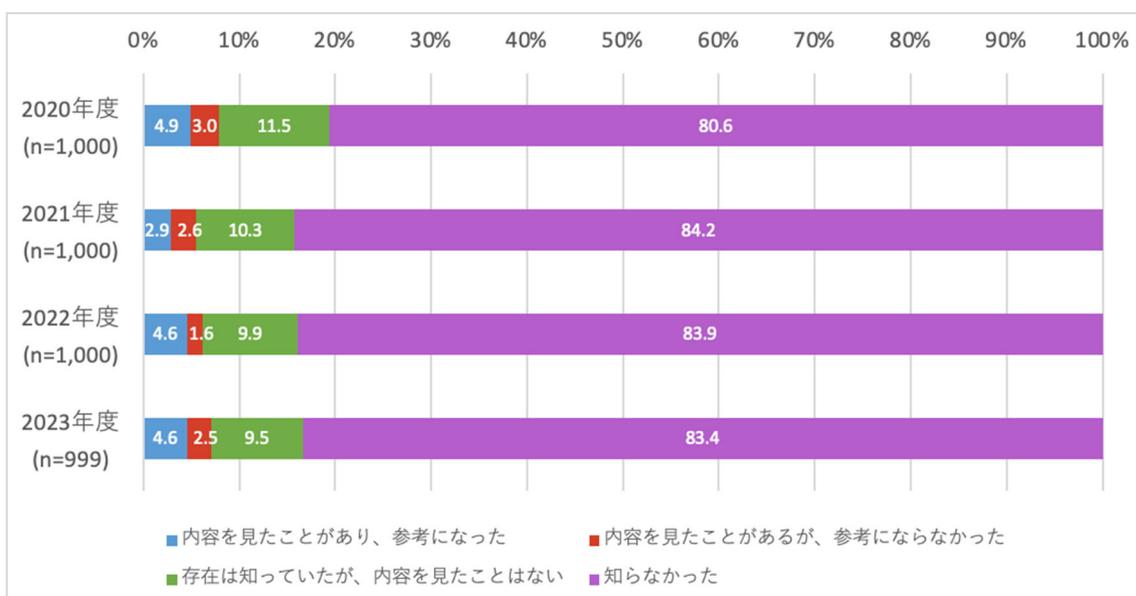
(7) 無線 LAN セキュリティ周知啓発

① 無線 LAN セキュリティガイドラインの認知状況 (Q44)

総務省「Wi-Fi 利用者向け 簡易マニュアル」(セキュリティガイドライン)を見たことがある無線 LAN ユーザは約 7%で閲覧経験比率は高まっていない。

認知率も約 16%に留まっている。

図表 2-1-82 無線 LAN セキュリティガイドラインの認知状況 (Q44)

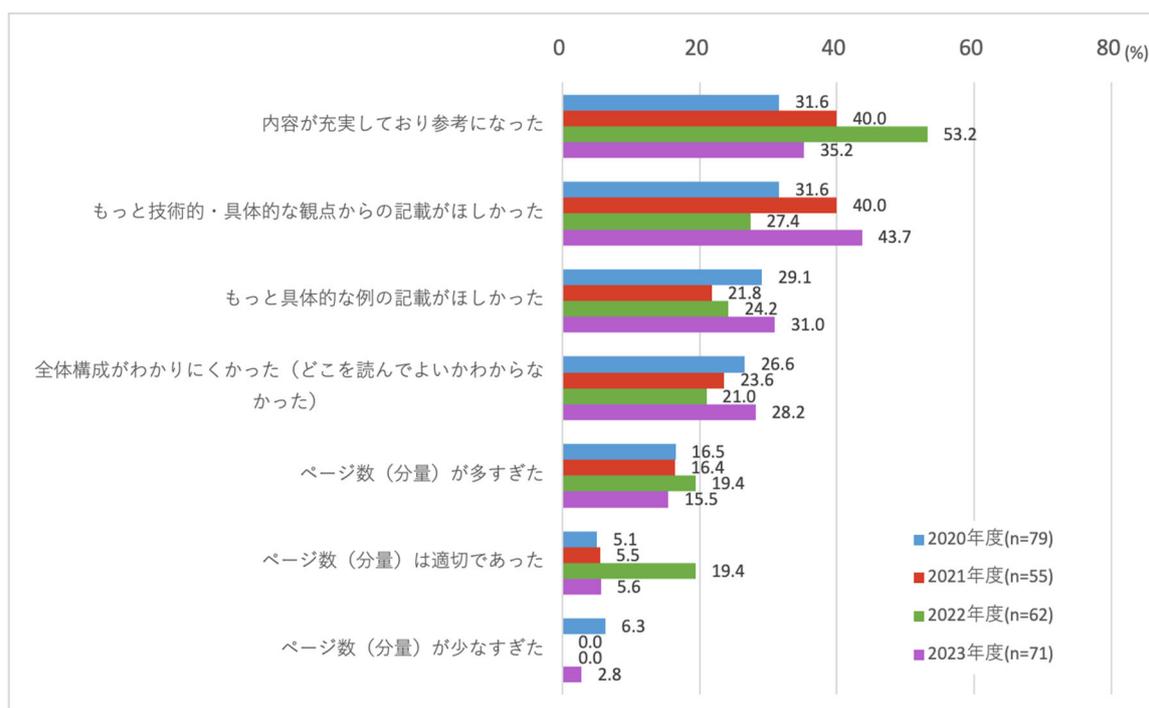


② 無線 LAN セキュリティガイドラインの評価 (Q45)

ガイドラインの閲覧経験者の約 35%は、内容が充実しており参考になったと評価している。

より技術的・具体的観点からの記載を望むユーザ(約 44%)や、より具体的な例示を望むユーザ(約 31%)、全体構成が分かりにくいとするユーザ(約 28%)、ページ数が多すぎとするユーザ(約 16%)などの意見も多い。

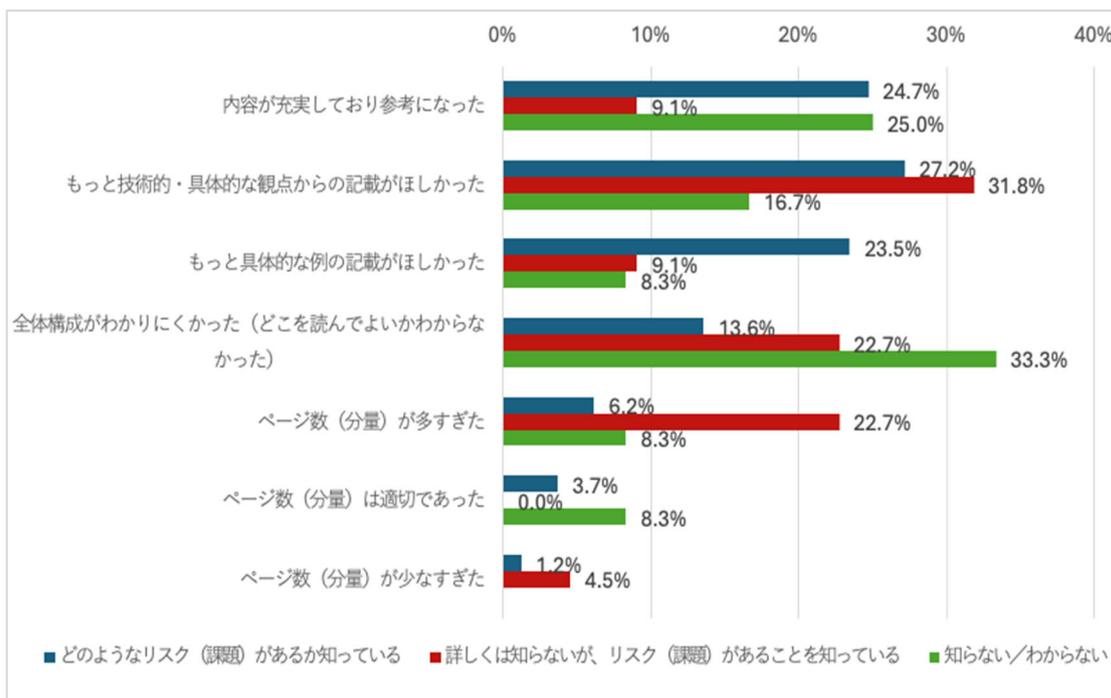
図表 2-1-83 無線 LAN セキュリティガイドラインの評価 (Q45)



無線 LAN のリスクを認知しているユーザは、より技術的・具体的観点からの記載を望むユーザや、より具体的な例示を望むユーザの比率が突出している。

また、無線 LAN のリスクを認知していないユーザは、全体構成がわかりにくかったという比率が突出している。

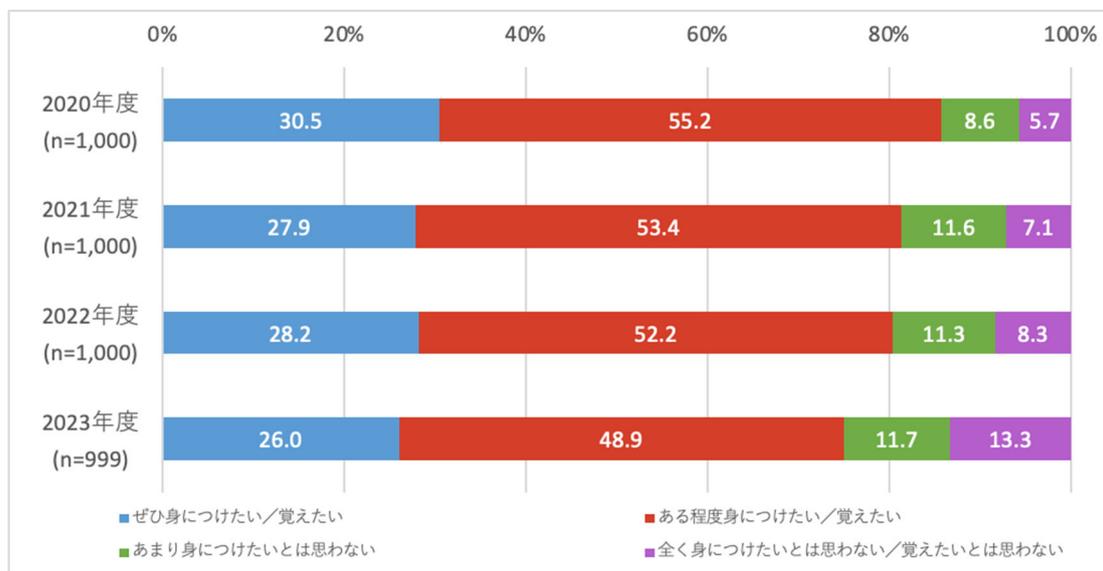
図表 2-1-84 無線 LAN セキュリティガイドラインの評価 (Q45) × リスク認知



③ 無線 LAN セキュリティの知識 (Q47)

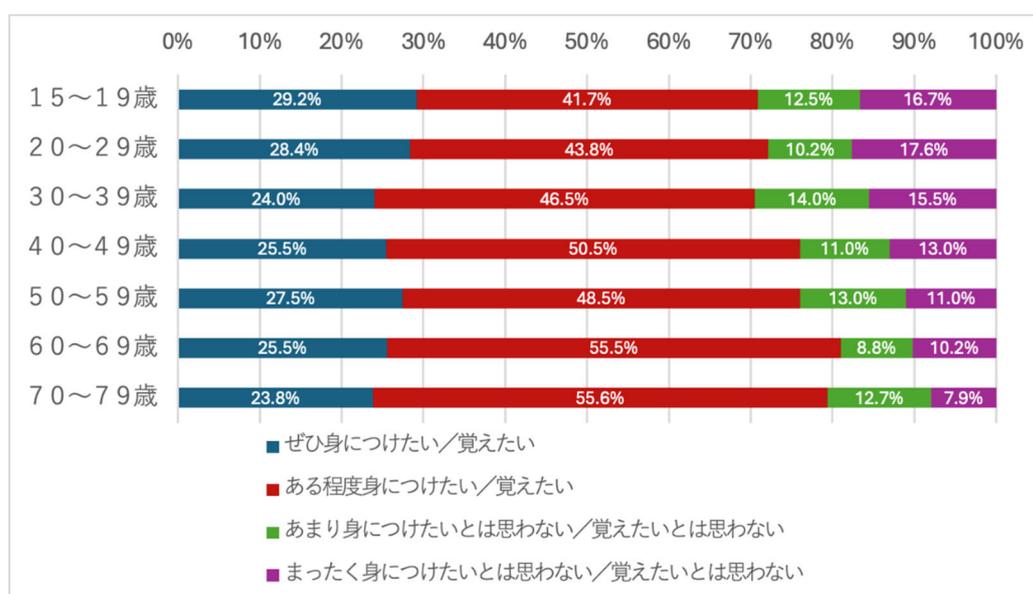
無線 LAN の利用に際して、セキュリティの正しい知識を身につけたい・覚えたいと考える無線 LAN ユーザは約 75%いるが、減少傾向にある。

図表 2-1-85 無線 LAN セキュリティの知識 (Q47)



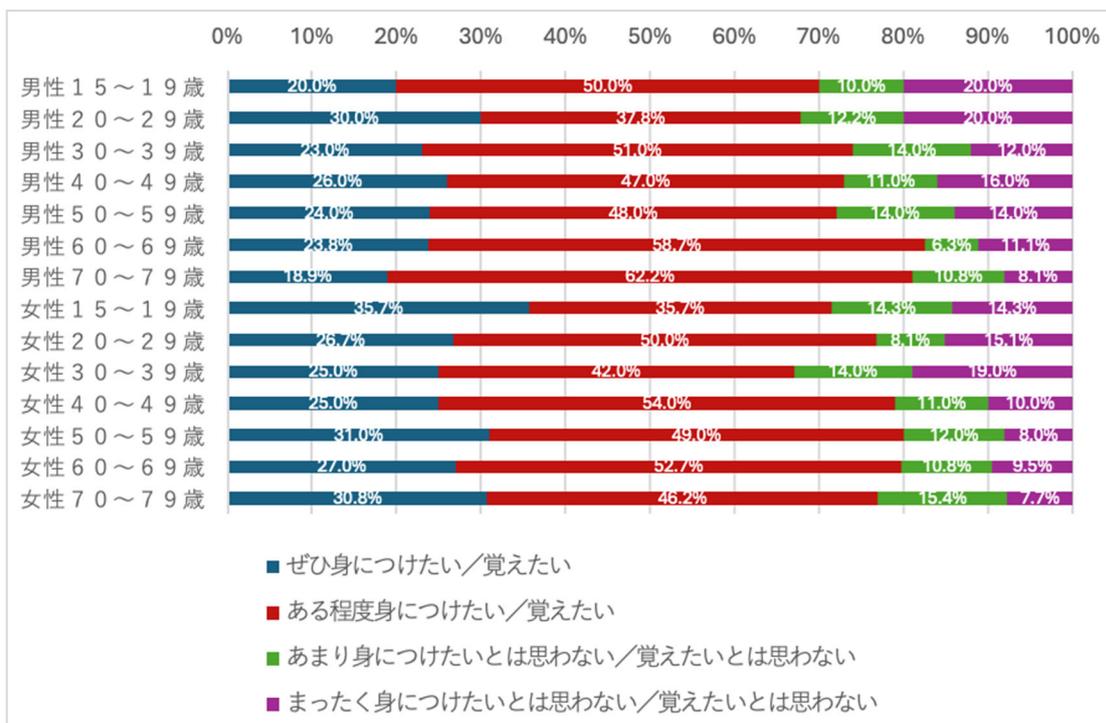
中高年層 (40 歳以上) のユーザは無線 LAN の利用に際して、セキュリティの正しい知識を身につけたい・覚えたい (ある程度も含む) と考えるユーザの比率が高い (約 75%から約 80%近く)。

図表 2-1-86 無線 LAN セキュリティの知識 (Q47) ×年代



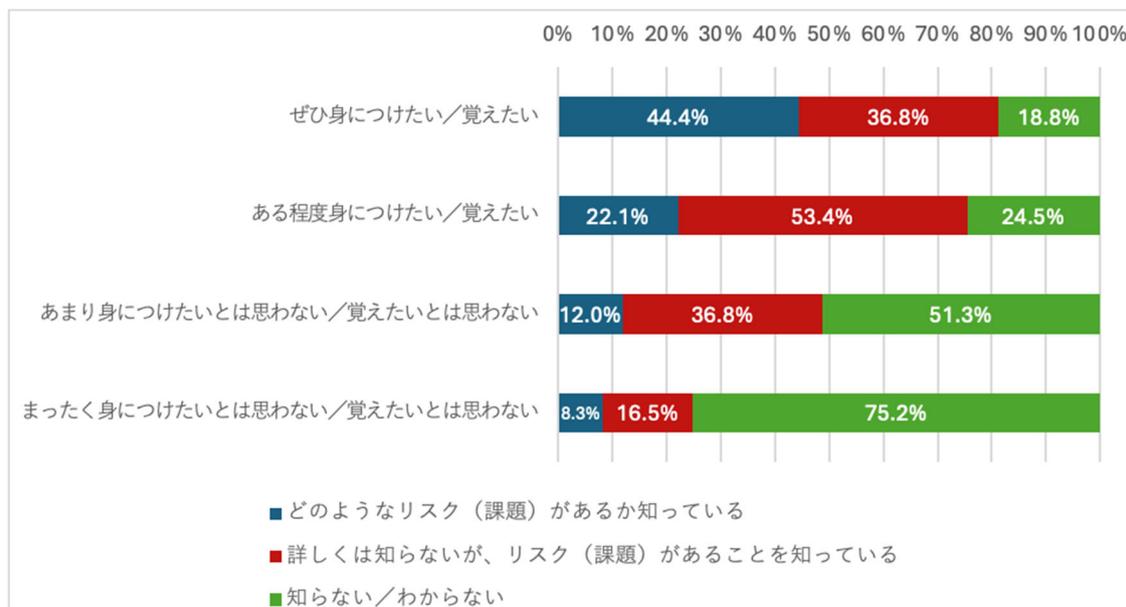
この傾向は、特に高年層（50歳以上）の女性ユーザに顕著であり、積極的にセキュリティの正しい知識を身につけたい・覚えたいと考えるユーザは多い。

図表 2-1-87 無線 LAN セキュリティの知識 (Q47) × 性年代



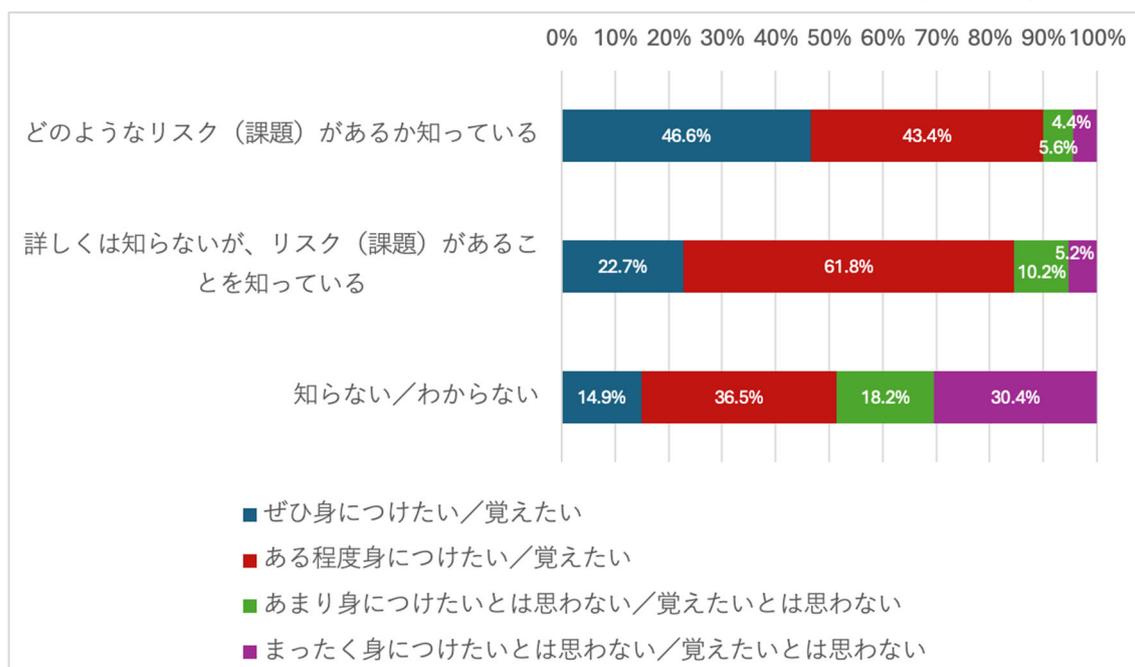
積極的にセキュリティの正しい知識を身につけたい・覚えたいと考えるユーザには、元々、無線 LAN のリスクを認知している層が多い一方、セキュリティの正しい知識を身につけたい・覚えたいと思わないユーザの約 75%は、元々、無線 LAN のリスクを認知していない。

図表 2-1-88 無線 LAN セキュリティの知識 (Q47) × リスク認知



表頭・表側を反転させてみた場合、無線 LAN のリスクを認知しているユーザは、セキュリティの正しい知識を身につけたい・覚えたいと考える層が多い反面、無線 LAN のリスクを認知していないユーザには、セキュリティの正しい知識を身につけたい・覚えたいと思わない層が多い。

図表 2-1-89 無線 LAN セキュリティの知識 (Q47) × リスク認知【表頭・表側反転】

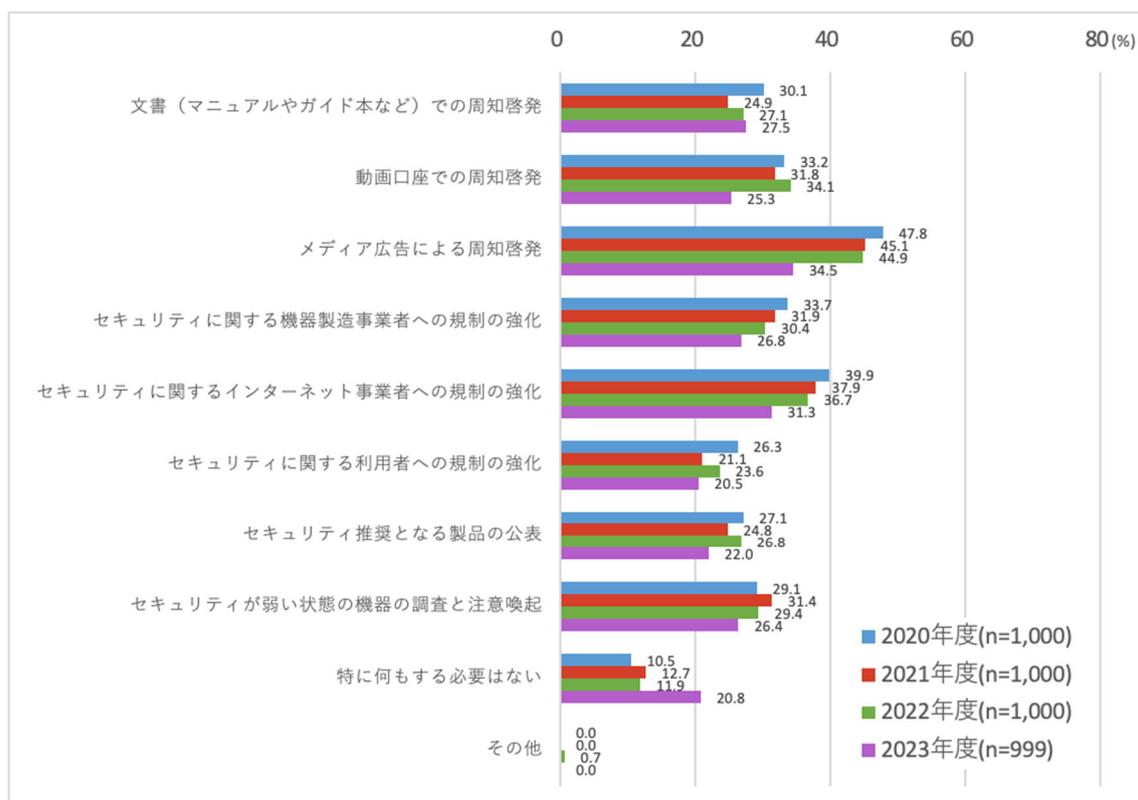


④ 無線 LAN セキュリティ確保のため国が進めるべき取組 (Q48)

無線 LAN のセキュリティ確保のために、国が進めるべき取組としては、メディア広告による周知啓発を望むユーザが約 35%で最も多い。

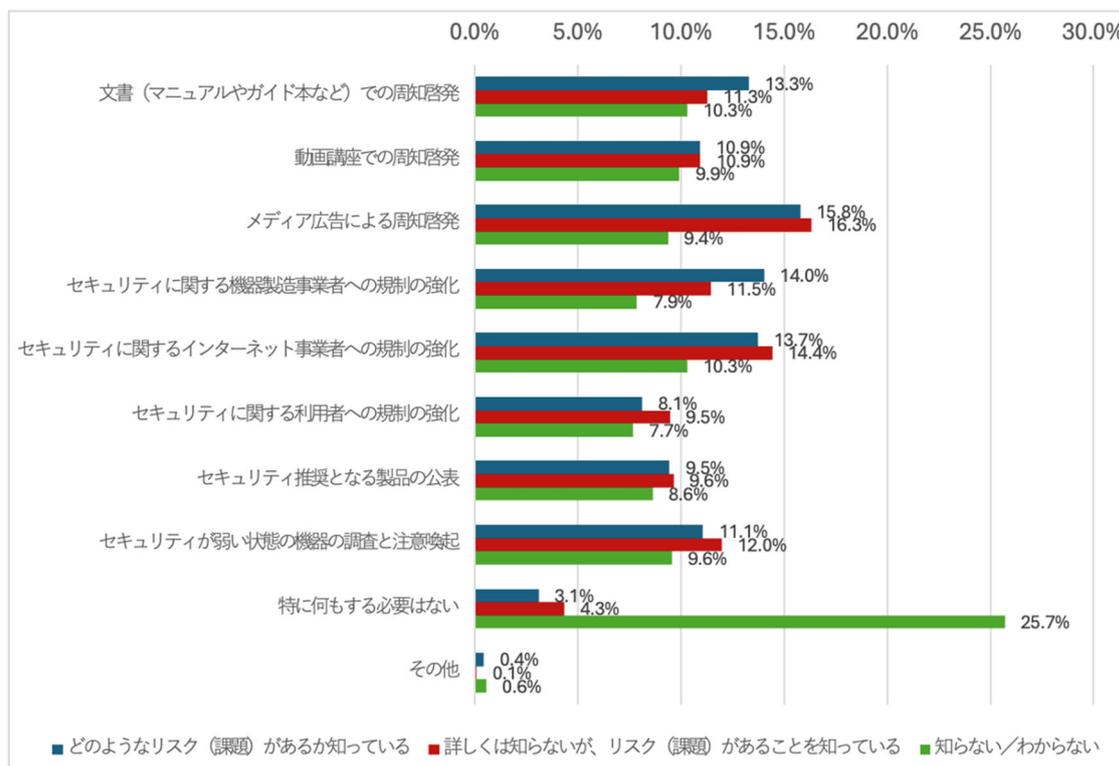
次いで、インターネット事業者への規制の強化(約 31%)、文章 (マニュアルやガイド本など) での周知啓発 (約 28%) などの取組を求めるユーザが多い。

図表 2-1-90 無線 LAN セキュリティ確保のため国が進めるべき取組 (Q48)



無線 LAN のリスクを認知しているユーザは、他のユーザに比べ、セキュリティ確保のために国が進めるべき取り組みとして、動画講座や文書(マニュアルやガイド本など)による周知啓発を望む傾向が強い。無線 LAN のリスクを認知していないユーザは、特に何もする必要はないが一番多い。

図表 2-1-91 無線 LAN セキュリティ確保のため国が進めるべき取組 (Q48) × リスク認知



第2節 無線LAN提供者に対するアンケート調査

2-1 調査概要

(1) 調査目的

地方自治体や民間企業が提供する公衆無線LANサービスに関する実態把握・情報収集を目的として、アンケート調査を実施した。

(2) 調査対象

我が国の全国の都道府県市区町村（1,726団体）及び、無線LANを提供していることが多い業態の民間企業等（交通機関、宿泊施設、小売業、医療施設関連、娯楽遊戯施設関連）から主要な企業を714社抽出し、計2,440団体を対象にアンケート調査を実施した。

尚、令和6年能登半島地震の影響を考慮して、石川県・富山県・潟県の内、新潟市、糸魚川市、上越市は対象から除いた。

(3) 調査方法

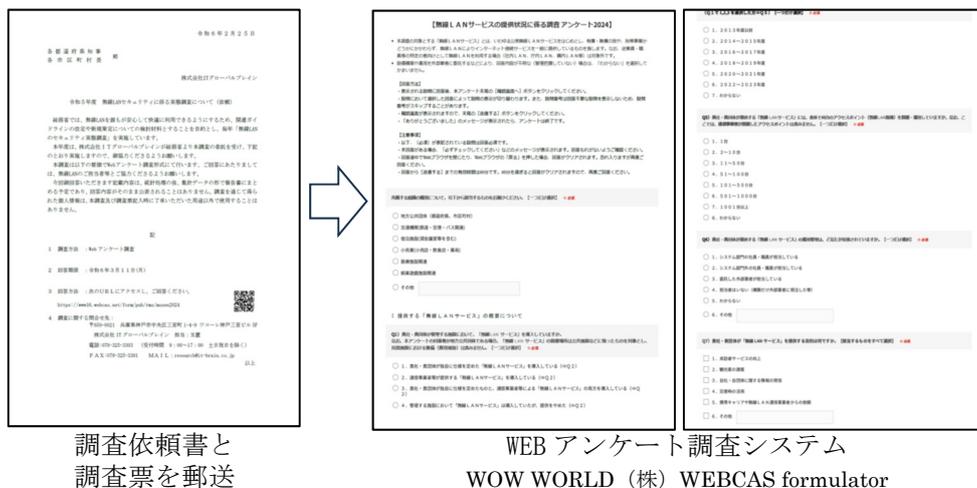
調査対象の地方自治体及び民間企業等に対して、アンケート調査票を郵送し、回答者には指定のWebサイトにアクセスしてWebアンケート調査システムにて回答を求めた。

なお、1つの自治体で複数の無線LANサービスを提供している場合は、自治体によっては複数の回答をいただいている。調査イメージを以下に示す。

図表 2-2-1 調査方法

■WEBアンケート調査

- ・対象自治体・企業等に対して調査依頼書及び調査票を郵送
- ・特定のWEBサイトにアクセスしてアンケート調査システムにて回答



(4) 調査時期

調査は以下のスケジュールにて実施した。

調査開始：2024年2月26日(月)

回答締め切り：2024年3月11日(月) (実際は3月14日(木)まで受け付け延長)

(5) 回答の状況

以下の地方自治体・企業団体から回答を得た。

地方自治体においては、1,726 団体に依頼し 850 (前年は 849) の回答があり (複数回答あり)、回答率は 49.2% (前年は 41.4%) であった。企業等においては、714 社中 147 社 (前年は 129 団体) から回答があり、回答率は 20.6% (前年は 18.3%) であった。前年と比較すると、自治体は約 19%、企業は約 13%程度、回答率数が増加した。原因としては、新型コロナウイルスの影響の低下や、例年のアンケート調査の定着などが考えられる。

図表 2-2-2 アンケート調査回答状況

調査種別		調査依頼数	回答数	回答率(%)
自治体		1,726	850	49.2%
企業	交通機関	77	29	37.7%
	宿泊施設	436	74	17.0%
	小売業	81	7	8.6%
	医療施設	100	33	33.0%
	娯楽遊戯施設	20	4	20.0%
企業合計		714	147	20.6%
総合計		2,440	997	40.9%

(6) 調査内容

以下のテーマについて、概況を把握した。

- I. 提供する「無線 LAN サービス」の概要について
- II. 利用者を守るための対策について
- III. 無線 LAN を安全に提供するための対策について
- IV. 利用者に安心を提供するための対策について
- V. 無線 LAN のセキュリティ等全般について

なお、調査票 (提供者アンケート内容) を参考資料として巻末に付す。

2-2 調査結果概要

調査結果の概要を以下に示す。まず設問ごとに自治体及び企業に対する集計結果をまとめるとともに、自治体のデータに関しては、サービス導入時期やサービスの規模で分類した結果について知見が得られるものを合わせて示した。

また、企業については業種別の特徴を、地方自治体についてはセキュリティ責任者の設置の有無による特徴を別項目でまとめた。

さらに、調査結果については、前年の結果と比較するとともに、優位な知見が得られるもののみを報告書には記載するものとする。

各項目のカッコ内 (Q) は調査票の設問番号を示す。

(1) 提供する「無線 LAN サービス」の概要について

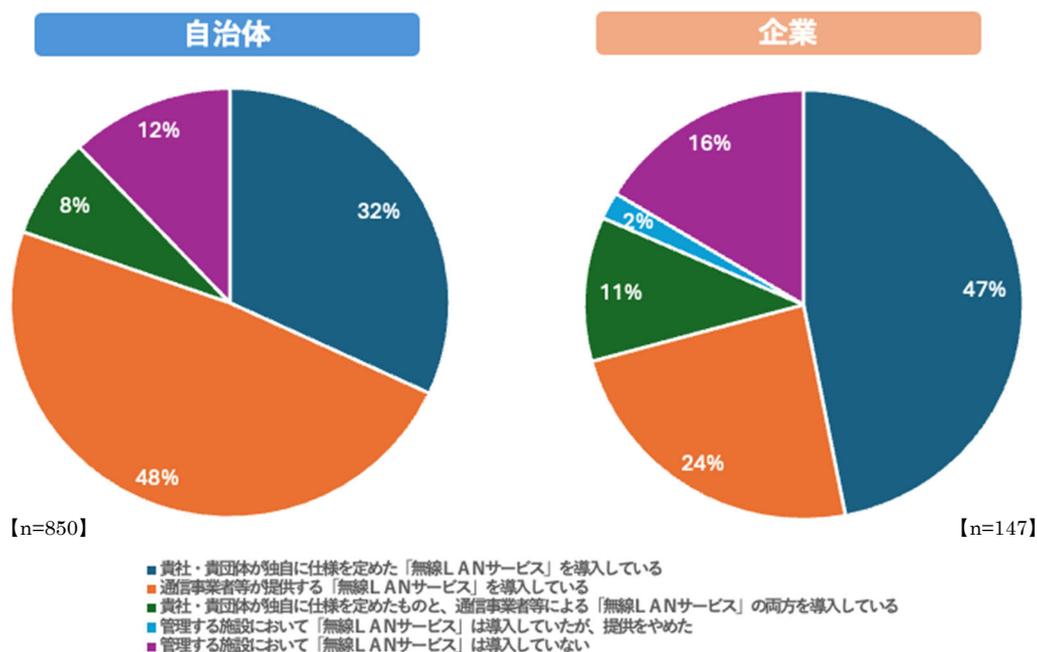
前年と同様の内容であったが、回答には以下のような特徴がみられた。

- ・アンケート回答に対して、自治体、企業ともに、おおむね 8 割が無線 LAN サービスを導入していると回答。
- ・無線 LAN サービス自体は年々増加している。
- ・運用管理については、内製率が自治体では約 6 割、企業では約 5 割であったが、自治体の 1 割、企業の 0.6 割が、担当者が不在またはわからないとの回答があった。
- ・目的としては、前年に比較して、相対的に「災害時の活用」が減少しているが新型コロナウイルス感染症が落ち着いたのが、影響していると思われる。
- ・最新の方式 (Wi-Fi 6E / 自動車用 5.2GHz) については、まだまだ導入率、導入検討率は低い。

① 無線 LAN サービスの導入について (Q1)

地方自治体の無線 LAN サービスの提供率は、84%→86%→91%→88%と増加傾向から今年より減少に転じている。企業は 88%→90%→89%→82%と推移しており、減少幅が増加している。地方自治体、企業ともに無線 LAN サービスの提供の見直しが行われていることが考えられる。

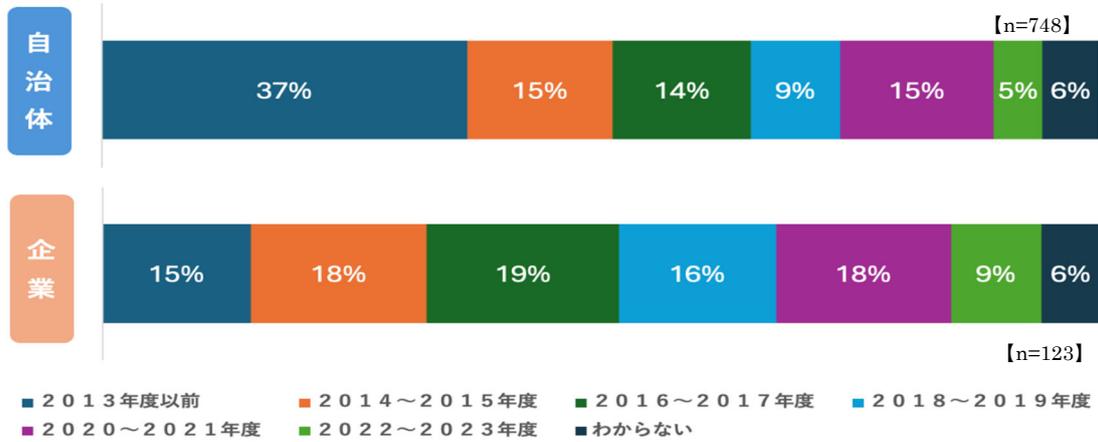
図表 2-2-3 無線 LAN サービスの導入 (Q1)



② 無線 LAN サービスの導入時期 (Q2)

公衆無線 LAN サービスを開始した時期について調査したところ、自治体は 2013 年度以降、2020～2021 年度を除いて減少傾向にある。企業は 2013 年度以降、明確な増減傾向は見られないが、2022～2023 年度の新規導入数は他の年度に比較すると少ないことが確認できる。

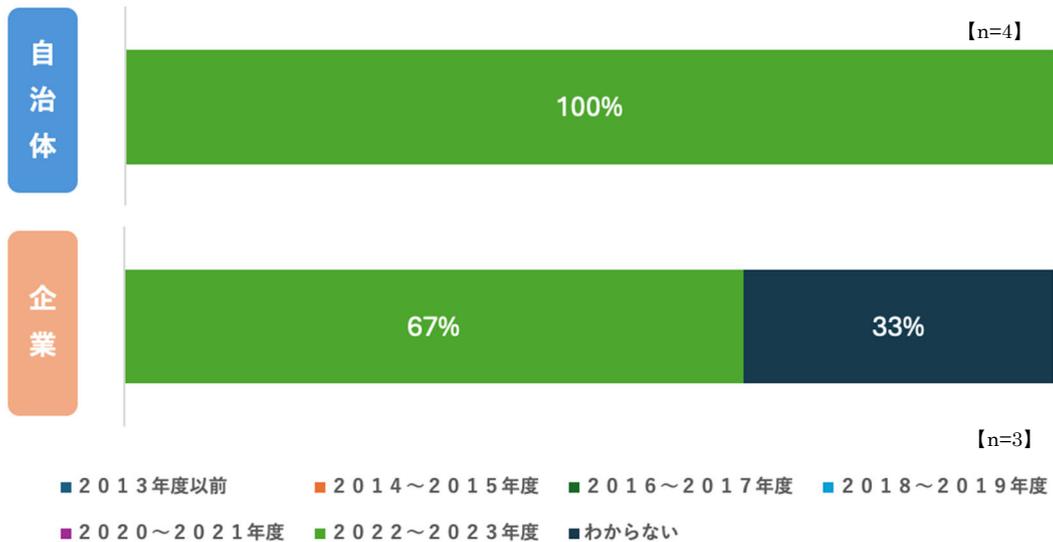
図表 2-2-4 無線 LAN サービスの導入時期 (Q2)



③ 無線 LAN サービスの終了時期 (Q3)

今回、サービスの終了に関する設問を行ったところ、2022年度以降に自治体、企業ともに無線 LAN サービスを終了した場所があった。

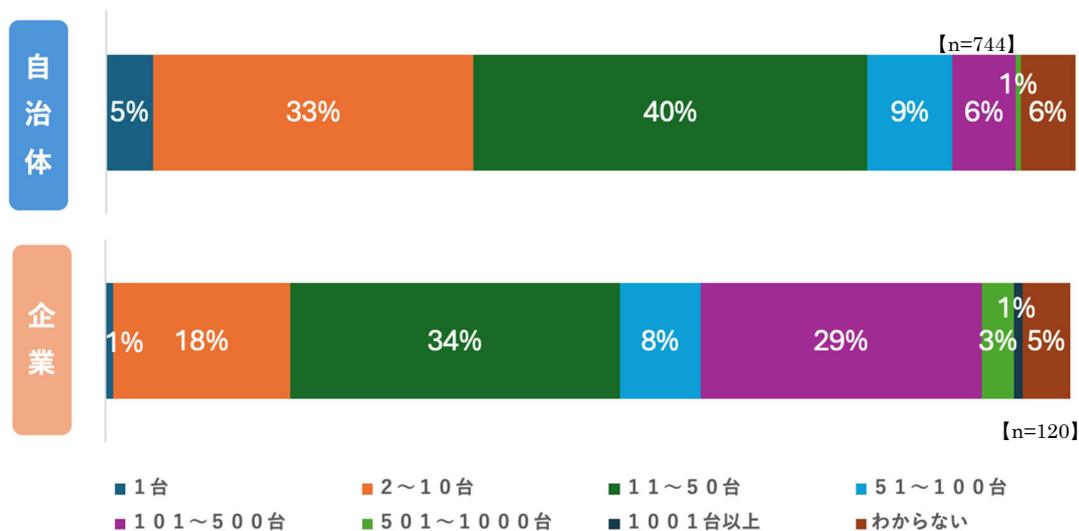
図表 2-2-5 無線 LAN サービスの終了時期 (Q3)



④ 無線 LAN サービスの規模 (Q5)

無線 LAN サービスの規模としてアクセスポイント台数について調査したところ、地方自治体が提供する無線 LAN サービスは、これまでの調査と同様に、企業に比べて小規模なものが多いことが分かった。

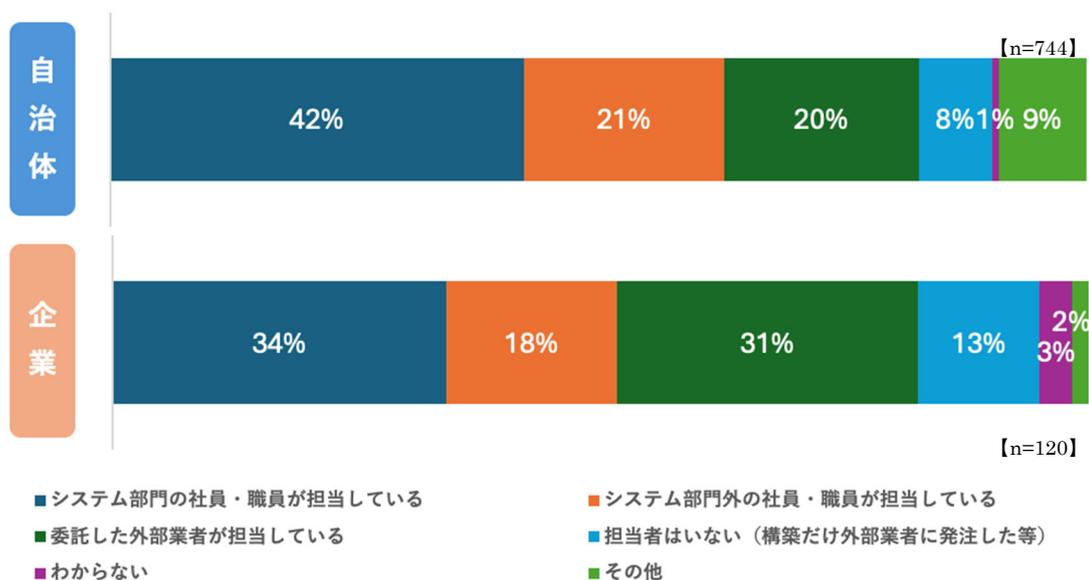
図表 2-2-6 無線 LAN サービスの規模 (Q5)



⑤ 無線 LAN サービスの運用管理 (Q6)

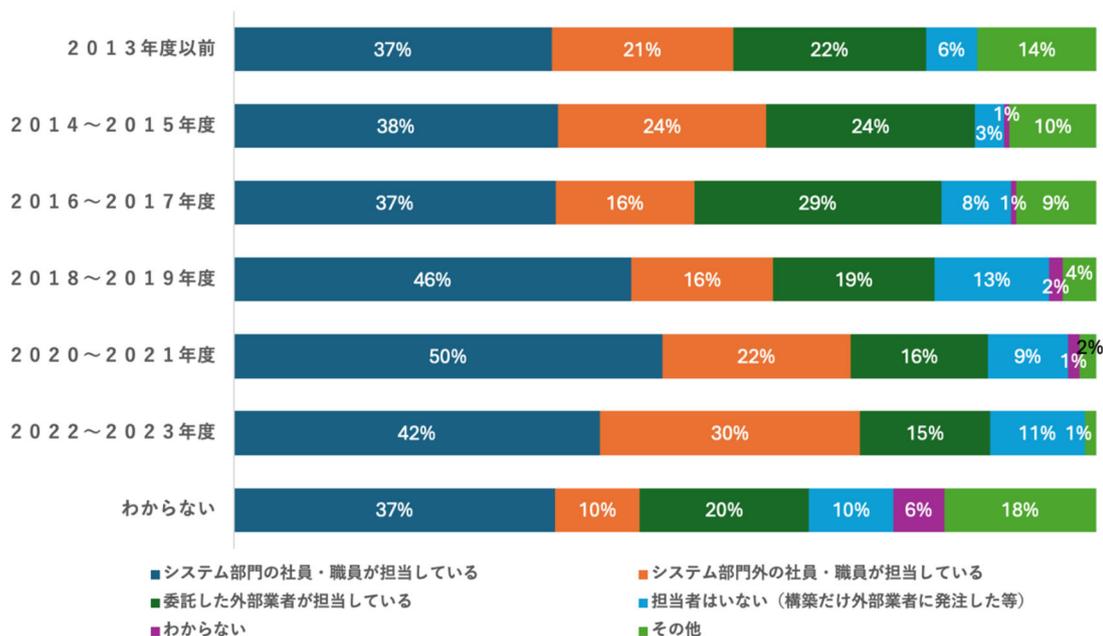
運用管理については、自治体は企業よりも外部に委託している率が低いことが分かった。

図表 2-2-7 無線 LAN サービスの運用管理 (Q6)

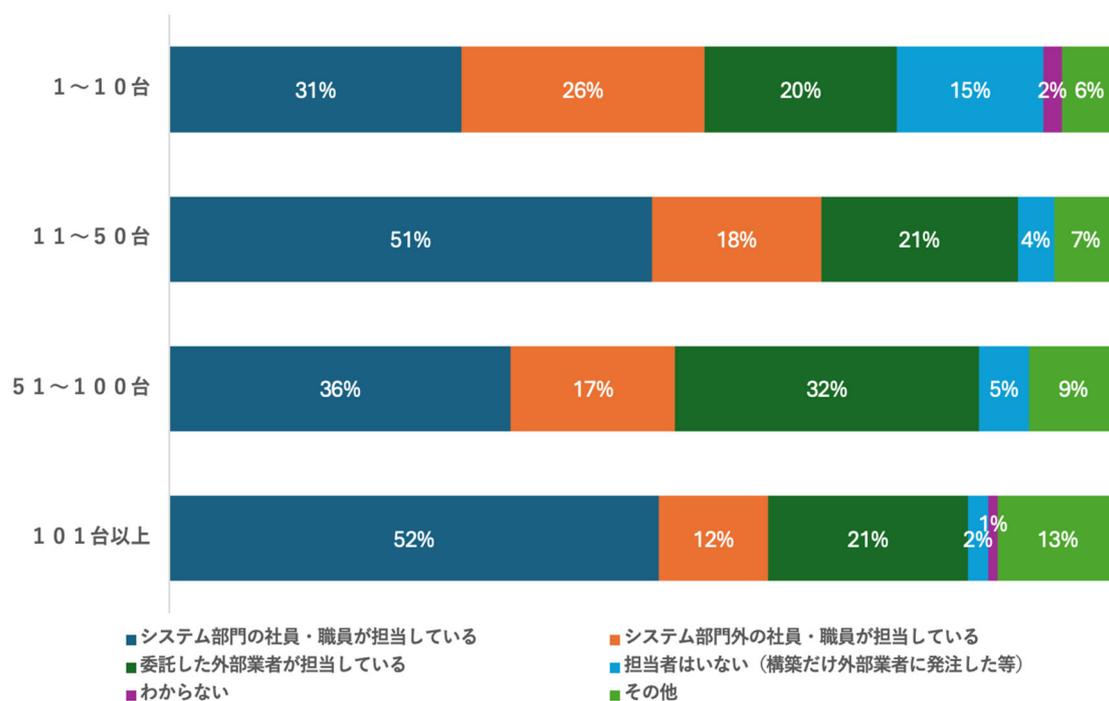


また、サービスを導入した時期をベースとして分類したところ、2016年度以降2021年度までは、自治体は内製率が徐々に増加していたが、2022~2023年度に減少に転じていることが分かった。さらに導入規模をベースとして分類すると、導入台数の多寡にかかわらず、外部への委託は一定の割合で行われており、小規模の団体では担当者がいない状態が多いことが分かった。

図表 2-2-7a 無線 LAN サービスの運用管理 (Q6) (導入時期ベース)



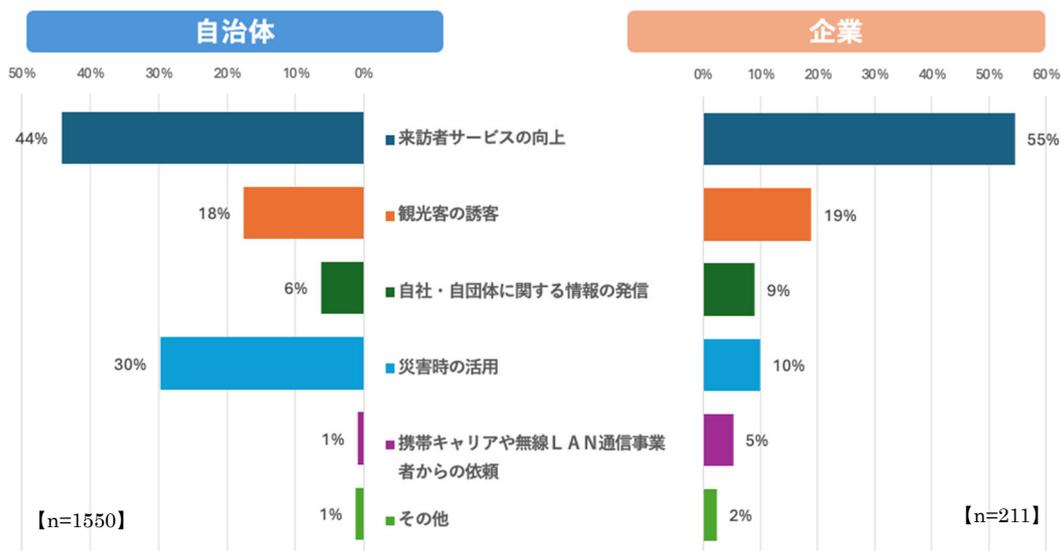
図表 2-2-7b 無線 LAN サービスの運用管理 (Q6) (導入規模ベース)



⑥ 無線 LAN サービスの目的 (Q7)

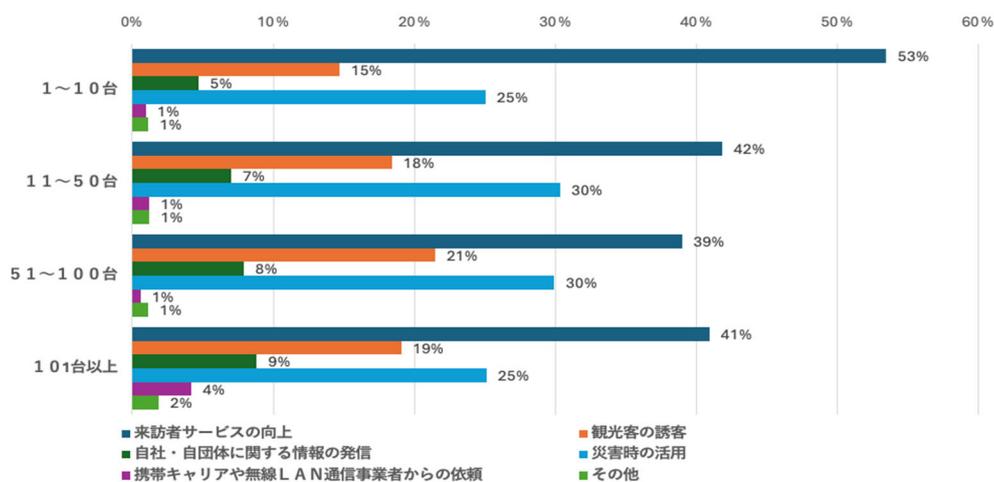
自治体及び企業ともに「来訪者サービスの向上」、「観光客の誘客」が多いが、自治体は「災害時の活用」も比率が高い。

図表 2-2-8 無線 LAN サービスの目的 (Q7)

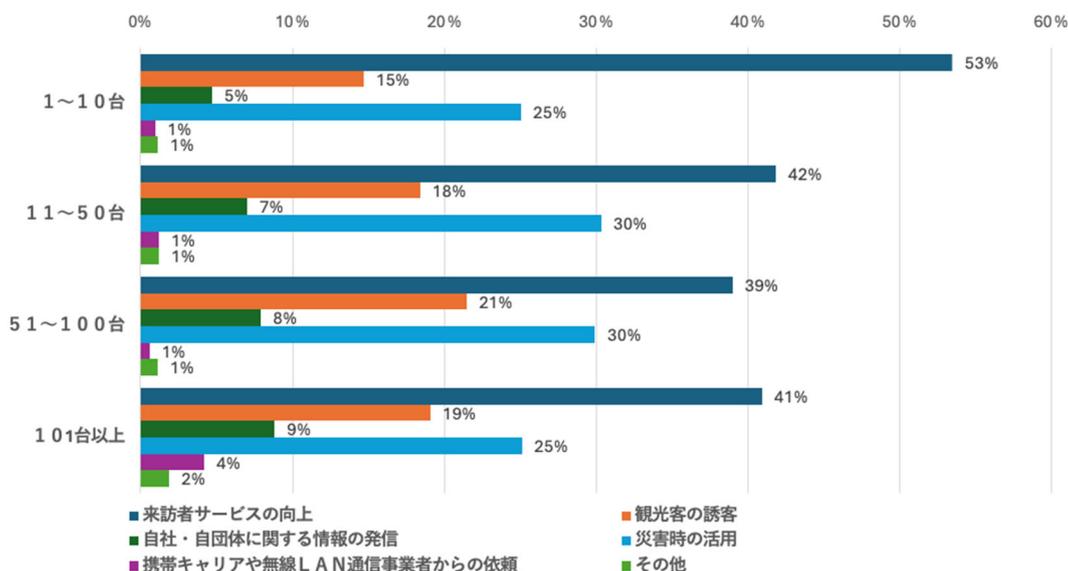


また、サービスを導入した時期をベースとして目的を分類したところ、2019 年度から「観光客の誘客」を目的とした導入が大きく低下していることが分かった（新型コロナウイルスの影響と考えられる）。さらに導入規模をベースとして分類すると、規模が大きいほど「観光客の誘客」と「災害時の活用」目的が増加することが分かった。

図表 2-2-8a 無線 LAN サービスの目的 (Q7) (導入時期ベース)



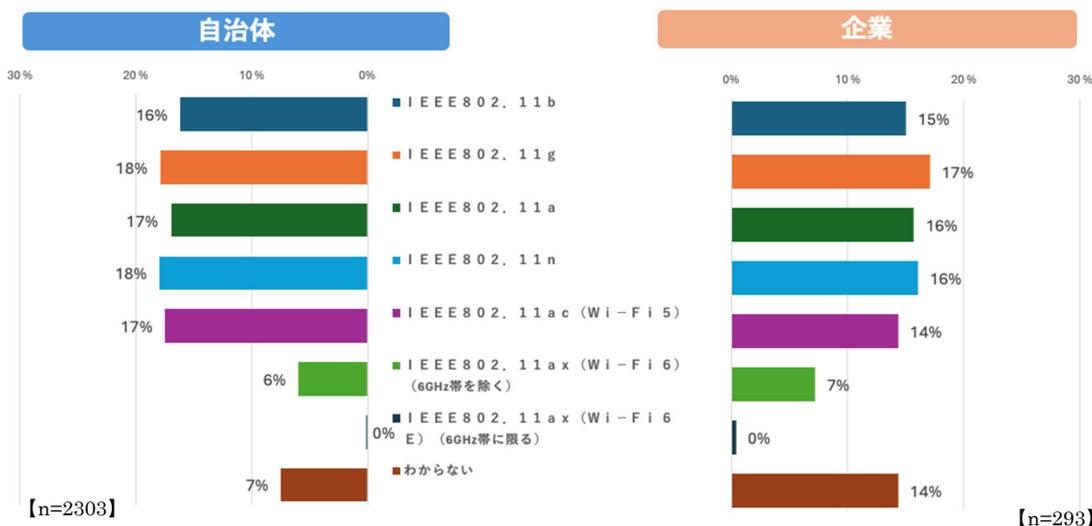
図表 2-2-8b 無線 LAN サービスの目的 (Q7) (導入規模ベース)



⑦ 無線 LAN サービスの伝送規格 (Q8)

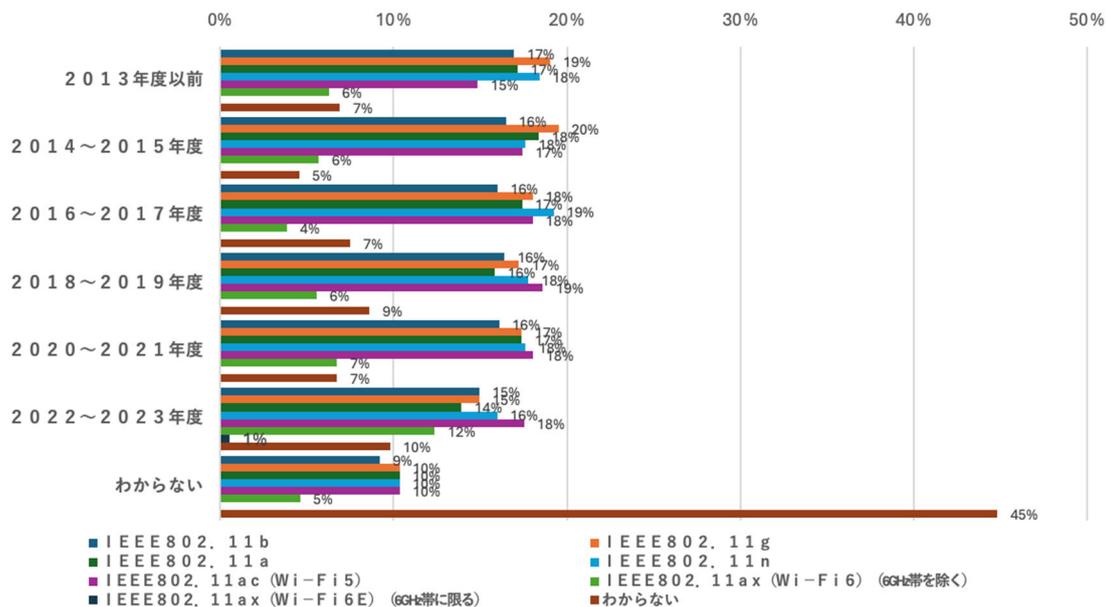
最新の規格 (802.11ax) の採用の割合は、昨年度と比較して地方自治体は減少、企業はほぼ横ばいとなっている。(自治体: 12%→6%、企業 6%→7%)。

図表 2-2-9 無線 LAN サービスの伝送規格 (Q8)

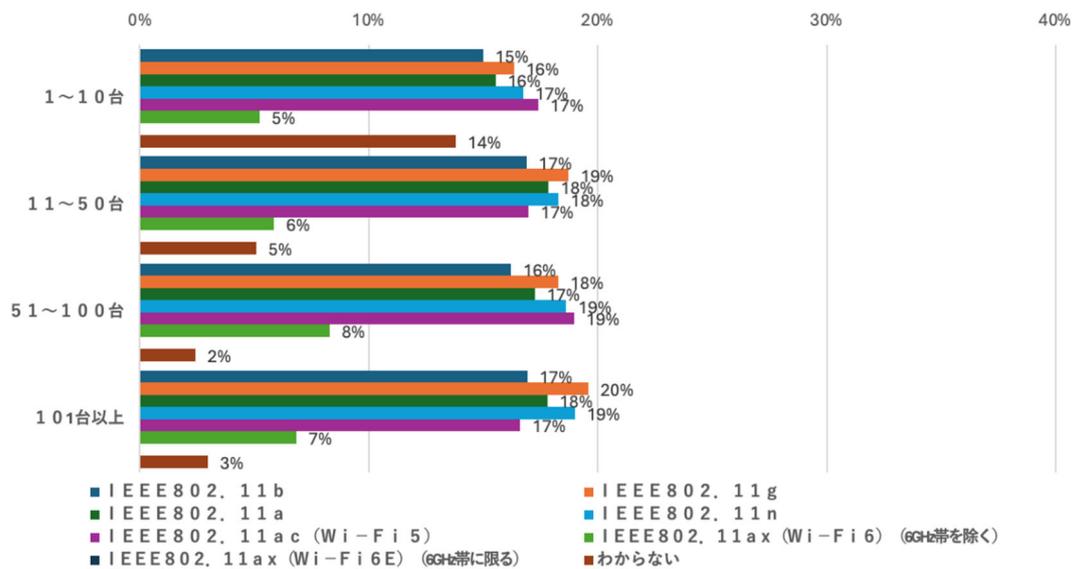


また、サービスを導入した時期をベースとして分類したところ、最近にサービスを開始した団体は、最新の規格 (802.11ax) に対応したものの割合が、高いことが分かった (7%→13%)。さらに、サービスを導入した規模をベースとして分類したところ、規模による導入規格の違いに大きな傾向は見られなかった。

図表 2-2-9a 無線 LAN サービスの伝送規格 (Q8) (導入時期ベース)



図表 2-2-9b 無線 LAN サービスの伝送規格 (Q8) (導入規模ベース)



(2) 利用者を守るための対策について

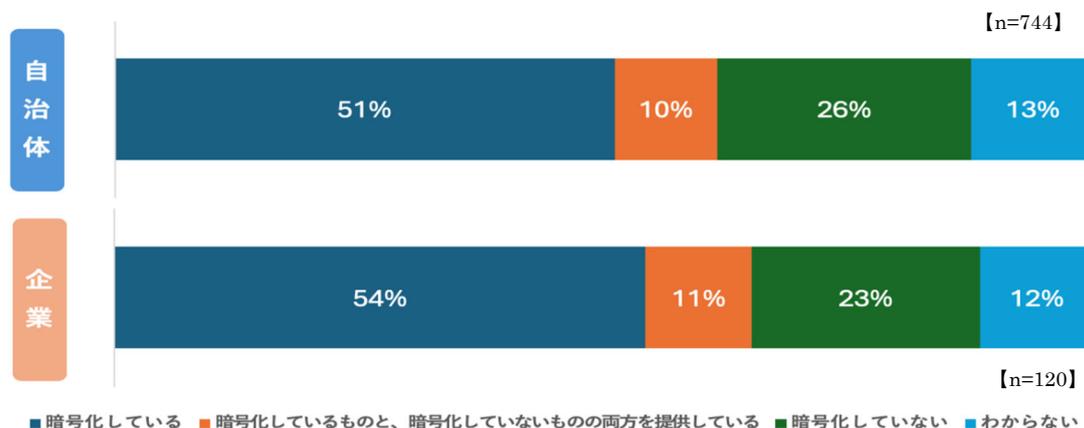
回答には以下のような特徴がみられた。

- 最近の傾向として無線 LAN を暗号化している率は着実に伸びている。特に 2016 年以降に導入されたものは暗号化率が高い。
- 暗号化方式も WPA3 の採用は着実に増加しているが、WEP/WPA を活用している事例も一定数みられる（特に規模の小さなもの）。これらは、知識のある人が不在であったり、設備を更改するコストを捻出できない、などの理由が考えられる。
- セキュリティのリスクについては、規模の大きなものほど認知率が高くなるが、認知率そのものは、大きな改善は見られない。
- 端末の折り返し通信のリスクについては認知率が向上しているが偽アクセスポイントに対する対策がされていない割合は多い。

① 無線 LAN サービスの暗号化 (Q9)

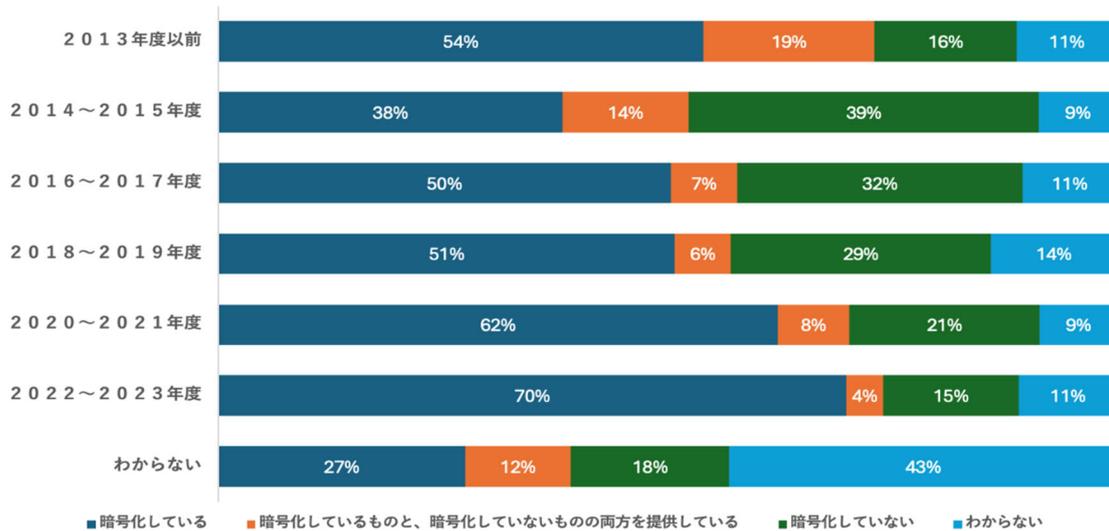
地方自治体、企業ともに、無線 LAN サービスを暗号化している率は昨年から横ばいとなっている（地方自治体：54%→63%→64%→61%、企業：63%→66%→64%→65%）。

図表 2-2-10 無線 LAN サービスの暗号化 (Q9)



また、サービスを導入した時期をベースとして分類したところ、2016 年度以降、「暗号化している」サービスの導入が年々増加していることが分かった。

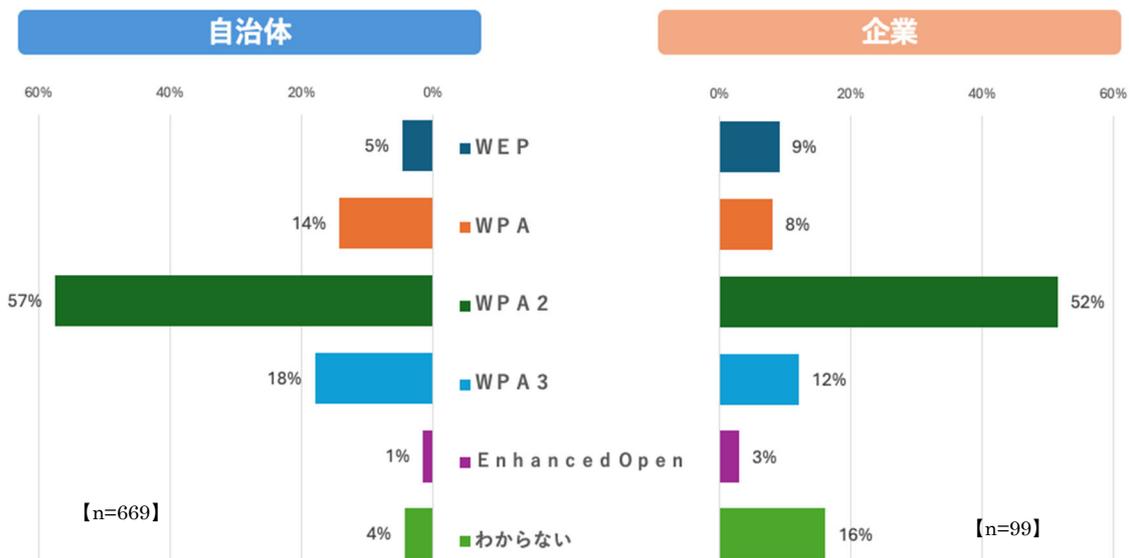
図表 2-2-10a 無線 LAN サービスの暗号化 (Q9) (導入時期ベース)



② 無線 LAN サービスの暗号化方式 (Q10)

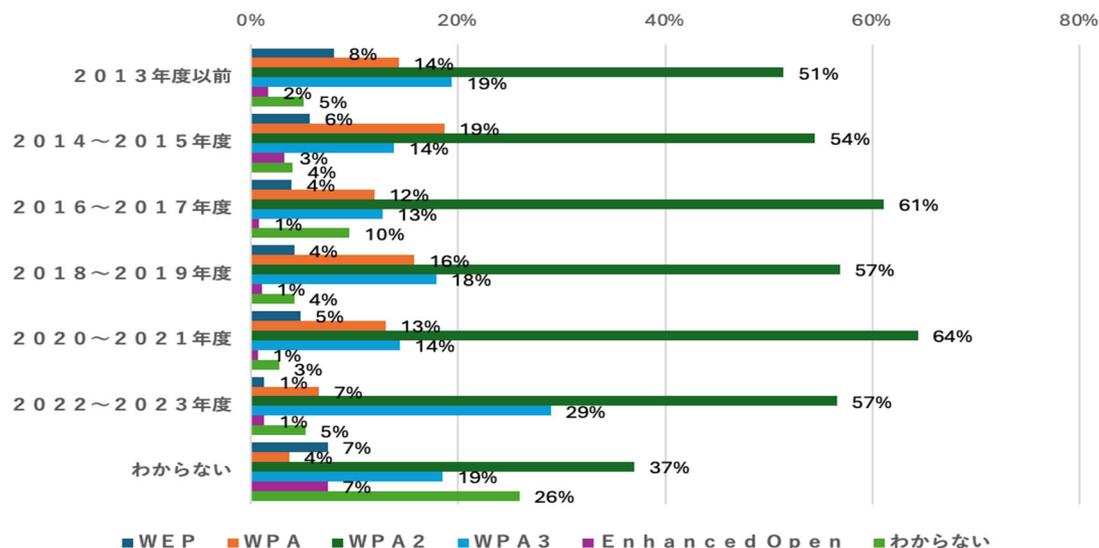
すでに解読・盗聴のリスクがある「WEP/WPA」の利用率は低い値ではあるが、依然として無くならない。

図表 2-2-11 無線 LAN サービスの暗号化方式 (Q10)



また、サービスを導入した時期をベースとして分類したところ、長年サービスを提供しているところに「WEP/WPA」を使っているものが多いことが分かった。

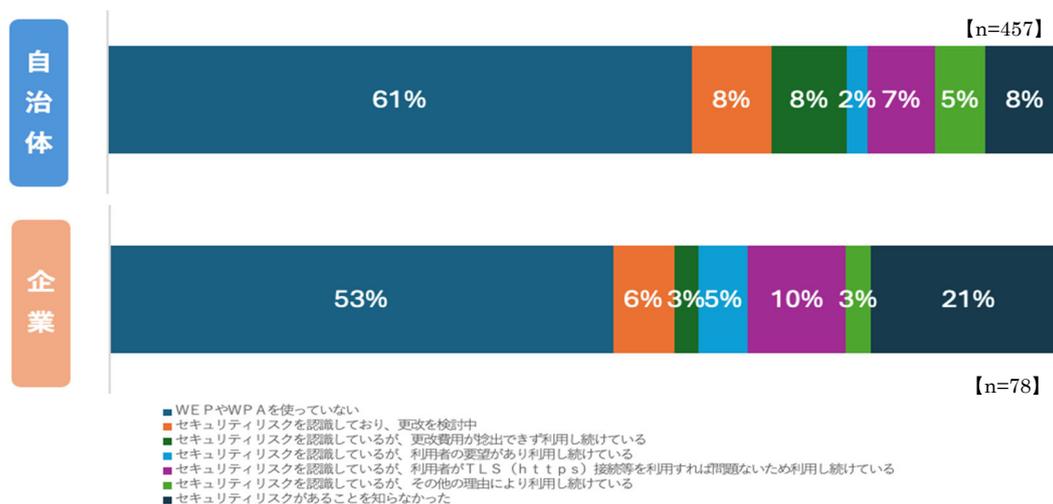
図表 2-2-11a 無線 LAN サービスの暗号化方式 (Q10) (導入時期ベース)



③ 暗号化方式のセキュリティリスク (Q11)

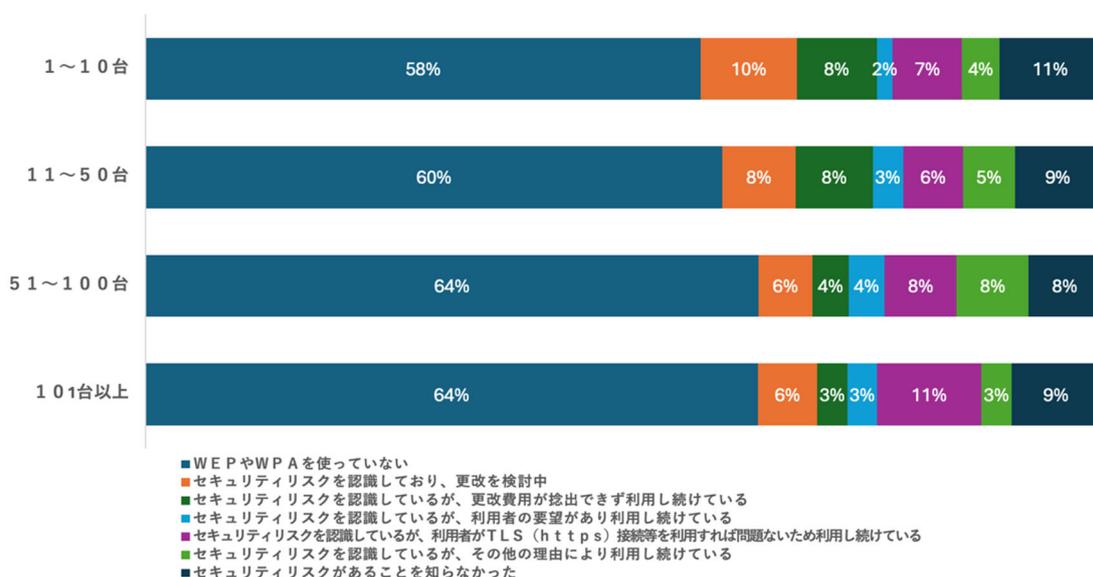
ほとんどの団体は WEP や WPA のセキュリティリスクについて認識をしているが、費用が捻出できない、等の理由でそのままになっている事例が見られる。また、企業については、セキュリティ対策を利用者自身が行うから問題ないとの認識も多い。

図表 2-2-12 暗号化方式のセキュリティリスク (Q11)



また、また導入規模をベースとして分類したところ、規模が大きいほどセキュリティリスクへの認識度は高くなっていることが分かった。

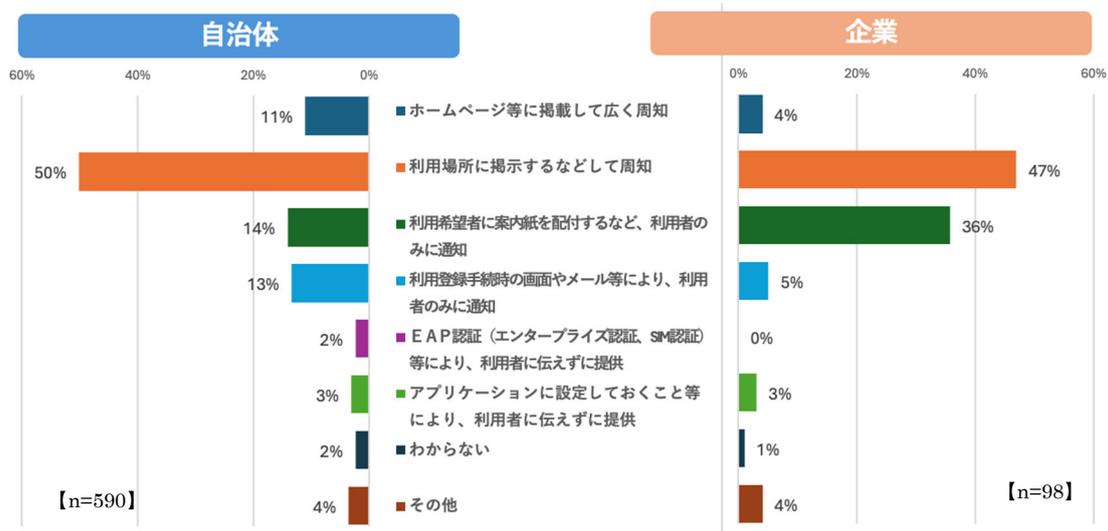
図表 2-2-12b 暗号化方式のセキュリティリスク (Q11) (導入規模ベース)



④ 暗号鍵の利用者への伝達方法 (Q12)

前年と同様に、自治体、企業ともに利用場所へ直接掲示する事例が多いが、企業では案内紙を直接配布する事例も多い。

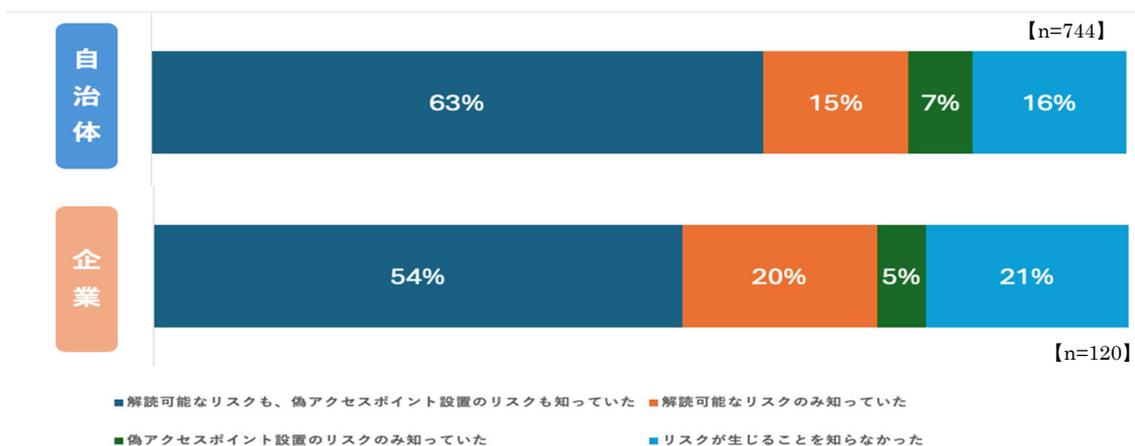
図表 2-2-13 暗号鍵の利用者への伝達方法 (Q12)



⑤ セキュリティリスクに対する認識 (Q13)

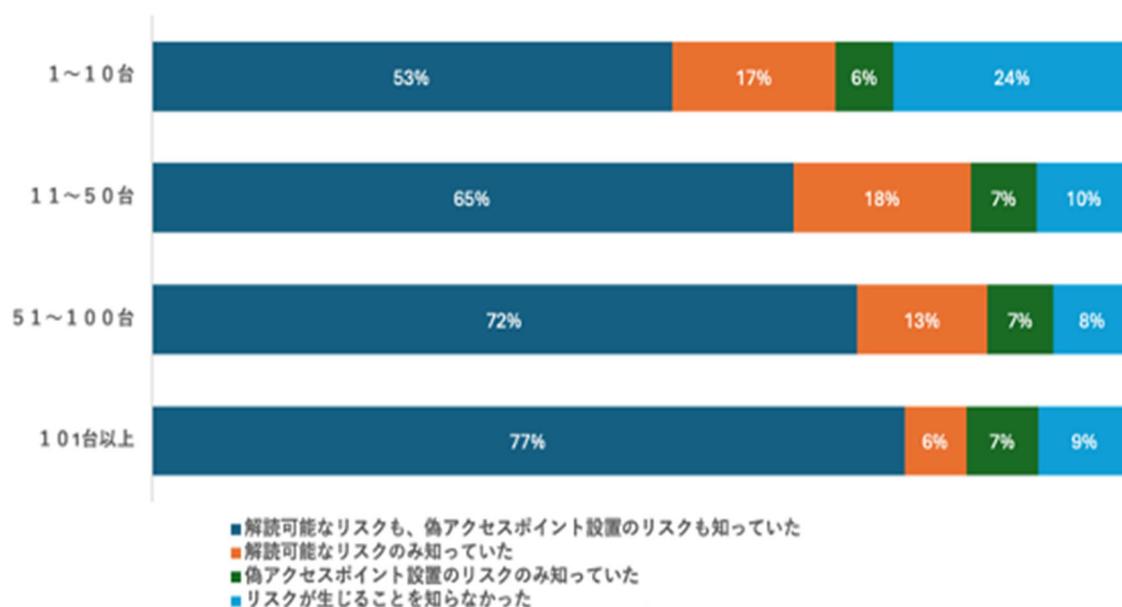
前年と同様の傾向であるが、自治体の両方のリスクを認識している率は向上していることが分かった (52%→60%→63%)。

図表 2-2-14 セキュリティリスクに対する認識 (Q13)



また、導入規模をベースとして分類したところ、規模が大きいほどセキュリティリスクへの認識度は高くなっていることが分かった。

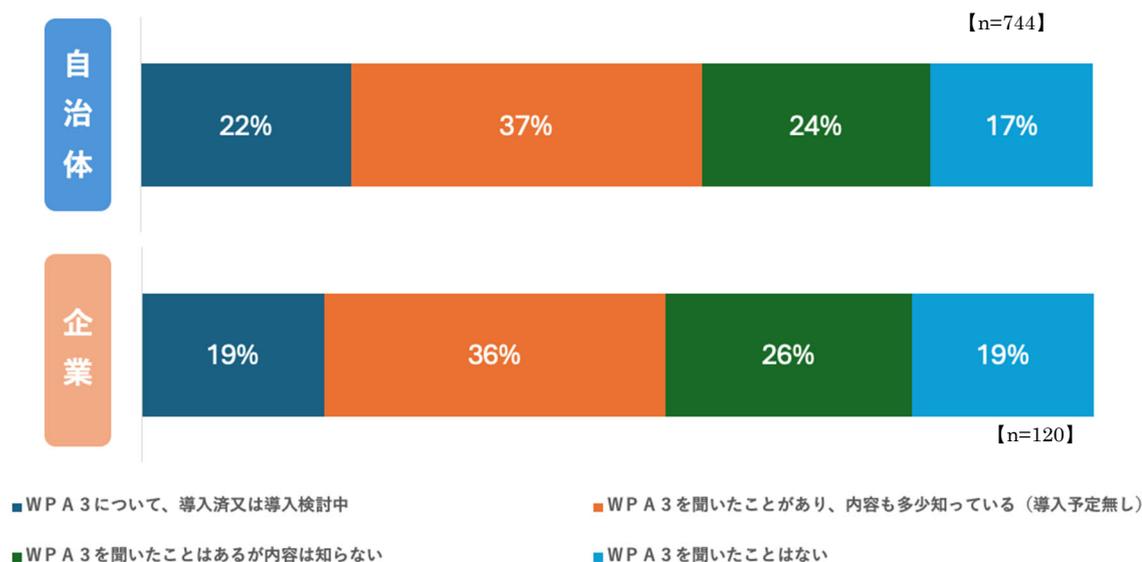
図表 2-2-14b セキュリティリスクに対する認識 (Q13) (導入規模ベース)



⑥ 新しい暗号化方式（WPA3）（Q14）

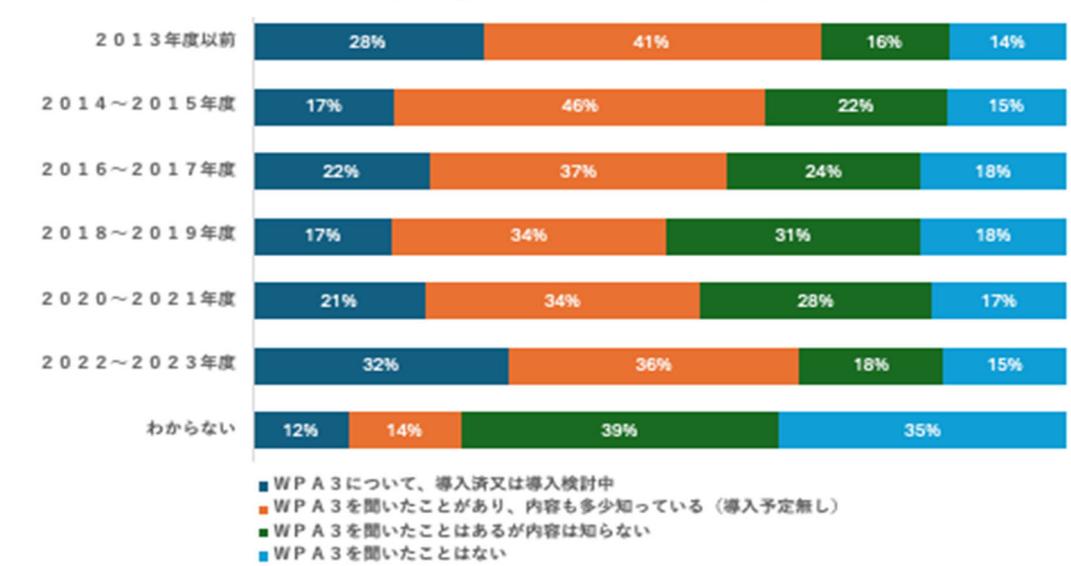
自治体、企業ともに認知度は若干の増加傾向である（自治体：74%→76%→83%、企業79%→80%→81%）。導入または導入検討については、自治体は増加（11%→15%→22%）し、企業も今年度に増加に転じた（14%→11%→19%）。

図表 2-2-15 新しい暗号化方式（WPA3）（Q14）



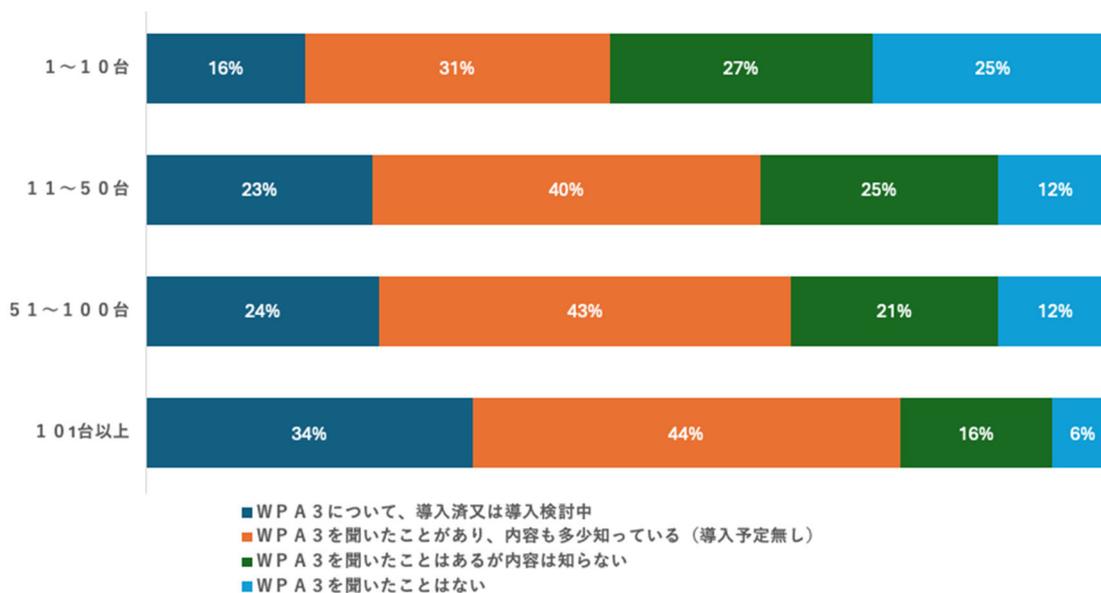
また、導入時期をベースとして分類したところ、最近サービスを開始した団体からWPA3に前向きな率が増加している。

図表 2-2-15a 新しい暗号化方式（WPA3）（Q14）（導入時期ベース）



さらに、導入規模をベースとして分類したところ、設備規模の大きなものほど、WPA3の導入検討が進んでいる率が高いことが分かった。

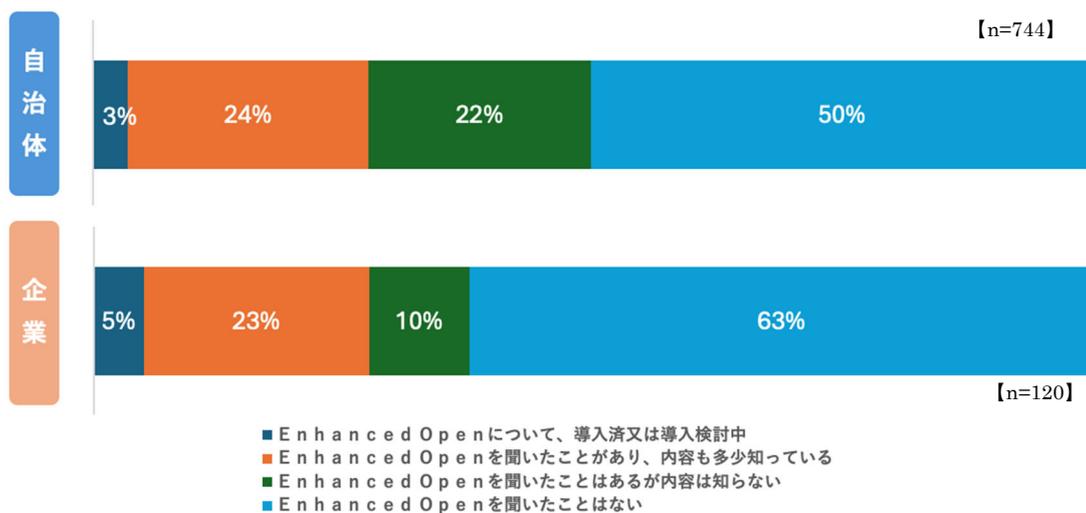
図表 2-2-15b 新しい暗号化方式 (WPA3) (Q14) (導入規模ベース)



⑦ 新しい暗号化方式 (Enhanced Open) (Q15)

新しいセキュリティ規格である Enhanced Open については、認知度はある程度あるものの、自治体、企業ともに導入はまだ進んでいないことが分かった。

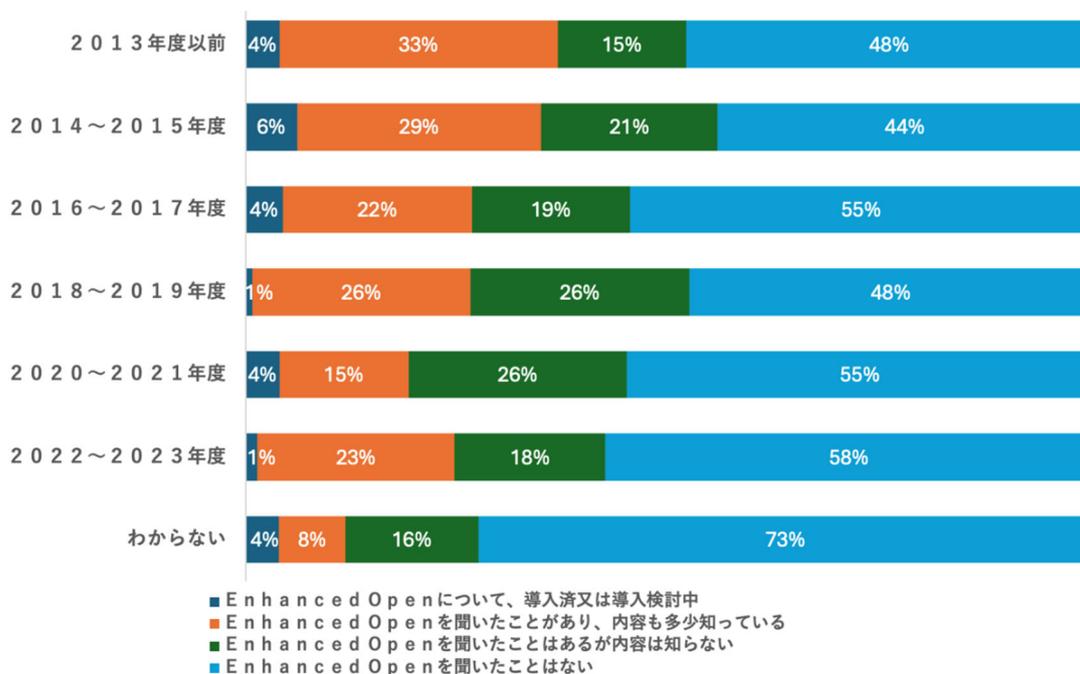
図表 2-2-16 新しい暗号化方式 (Enhanced Open) (Q15)



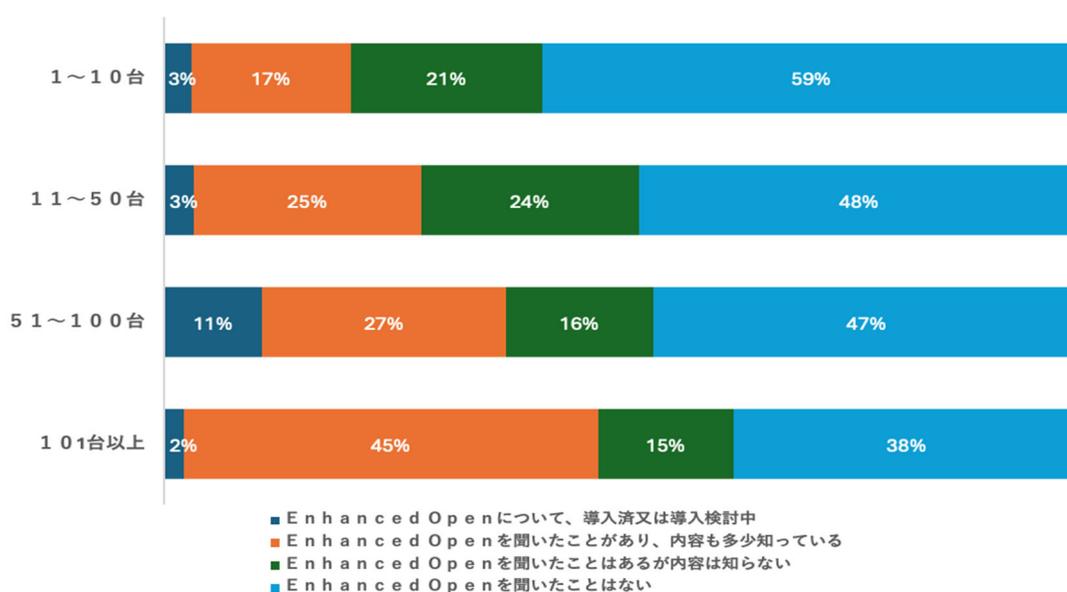
また、導入時期をベースとして分類したところ、最近サービスを開始した団体ほど

「聞いたことがない」率が高い一方、導入規模をベースとして分類したところ、規模の大きな団体ほど、Enhanced Open の認知度が高いことが分かった。

図表 2-2-16a 新しい暗号化方式 (Enhanced Open) (Q15) (導入時期ベース)



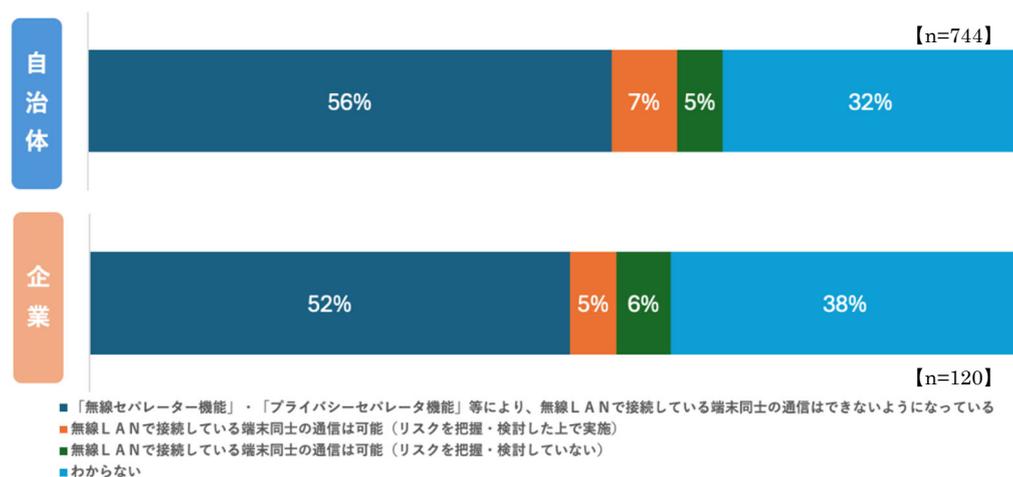
図表 2-2-16b 新しい暗号化方式 (Enhanced Open) (Q15) (導入規模ベース)



⑧ 端末同士の折り返し通信 (Q16)

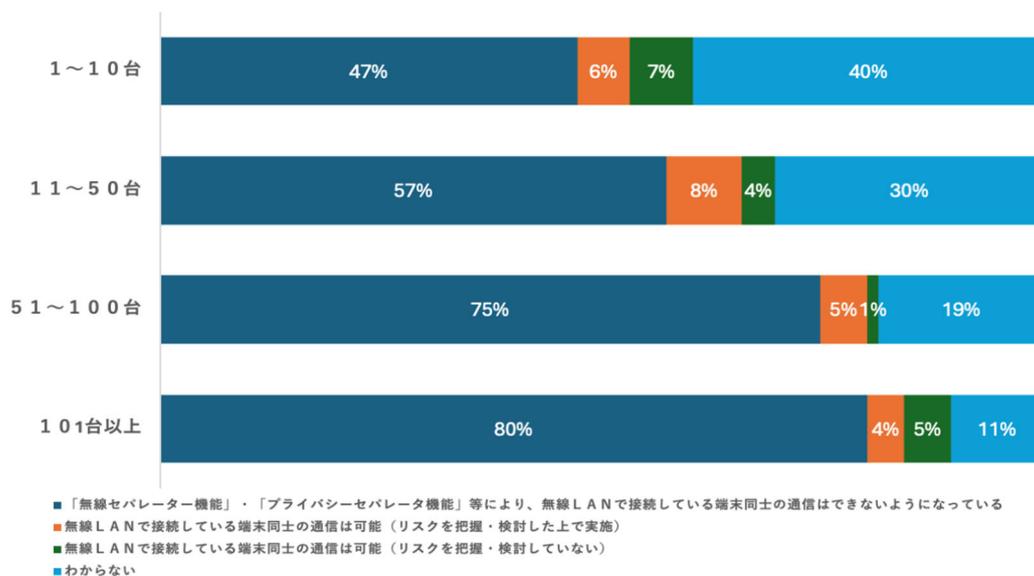
端末同士の折り返し通信については無線 LAN 特有の問題であり、公衆サービスの場合、知らずに情報が漏れてしまう危険性があるが、前年と同様に自治体、企業ともに「わからない」という回答が3割程度ある（改善は見られない）。

図表 2-2-17 端末同士の折り返し通信 (Q16)



また、導入規模をベースとして分類したところ、規模が大きいほど折り返し通信のリスクに対する認識度は高いことが分かった。

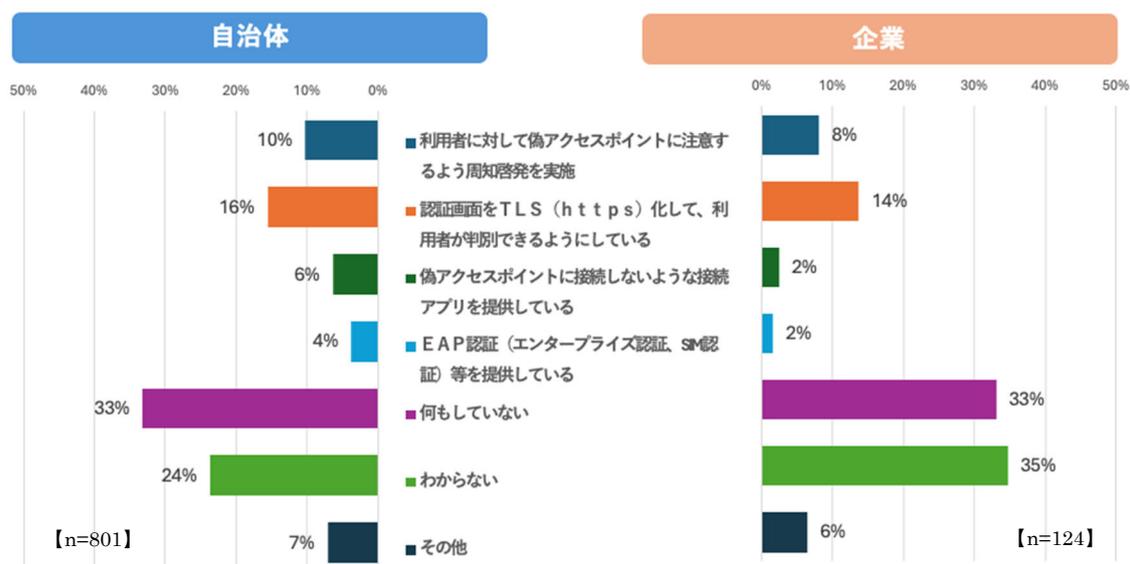
図表 2-2-17b 端末同士の折り返し通信 (Q16) (導入規模ベース)



⑨ 偽アクセスポイントへの対策 (Q17)

偽アクセスポイントについては「何もしていない」と「わからない」という回答が半数近くあり、多い傾向にある。

図表 2-2-18 偽アクセスポイントへの対策 (Q17)



(3) 無線 LAN を安全に提供するための対策について

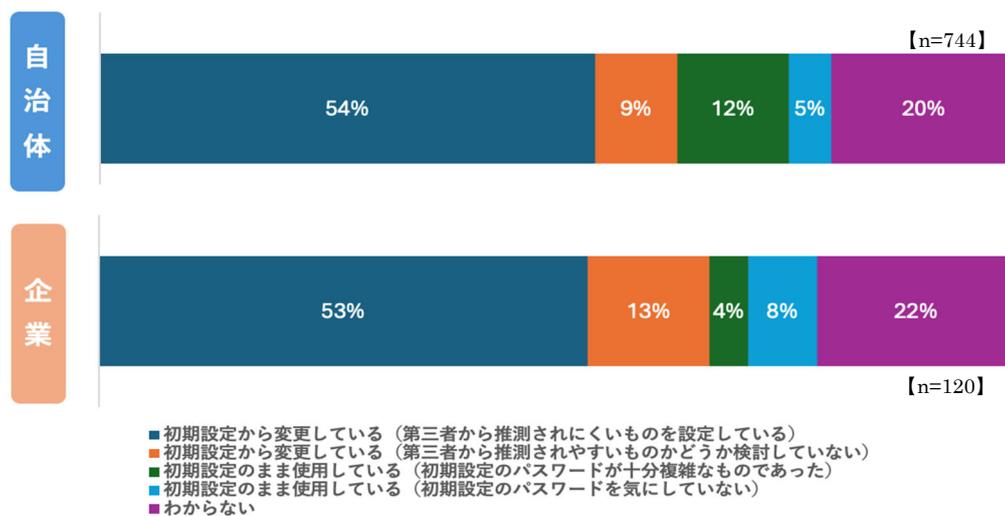
回答には以下のような特徴がみられた。

- 全般的に、各対策の実施率は横ばいであり、大きな改善は見られない。
- 一般的に、規模の大きな事業者ほど、いろいろな策を実施している率は高くなっている。
- 端末認証は「メール認証方式」と「SNS 認証方式」が定着してきている。企業では利便性のため、無認証の事例も多い。
- セキュリティ責任者を設定している組織の率は、年々増加傾向にある。

① 管理者パスワードの管理 (Q18)

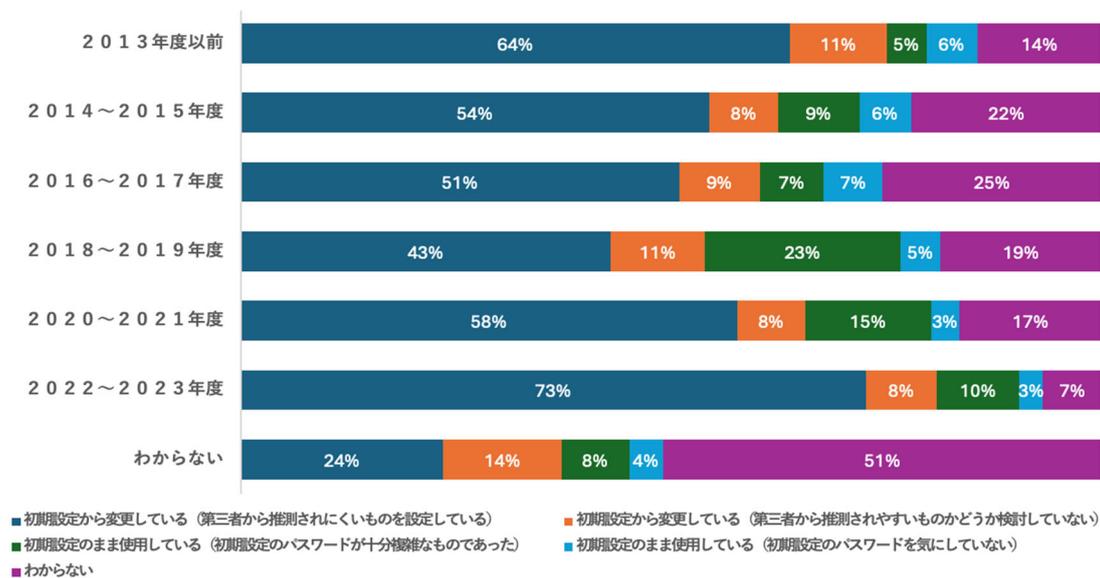
セキュリティ上安全と考えられるもの (回答 1 ~ 3) の割合が 7 割以上であり、前年と同様の傾向 (自治体 : 73% → 74% → 75%、企業 78% → 75% → 70%)。

図表 2-2-19 管理者パスワードの管理 (Q18)

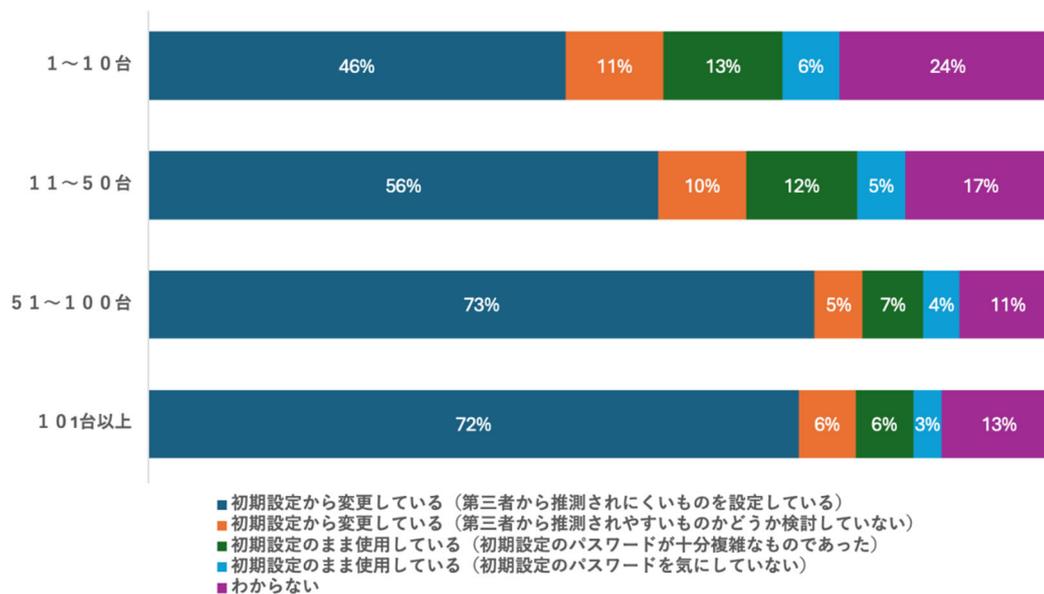


さらに、導入時期をベースとして分類したところ、2020年度以降、「初期設定から変更している」という回答が増加している。また、導入規模をベースとして分類したところ、設備規模が大きいくほど、管理を厳格にしている率が高いことが分かった。

図表 2-2-19a 管理者パスワードの管理 (Q18) (導入時期ベース)



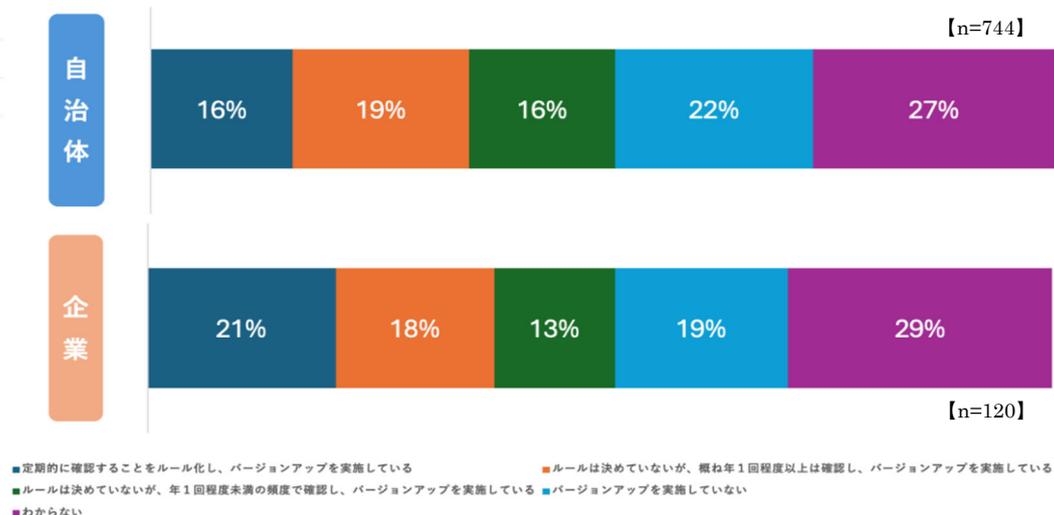
図表 2-2-19b 管理者パスワードの管理 (Q18) (導入規模ベース)



② ネットワーク機器のファームアップ (Q19)

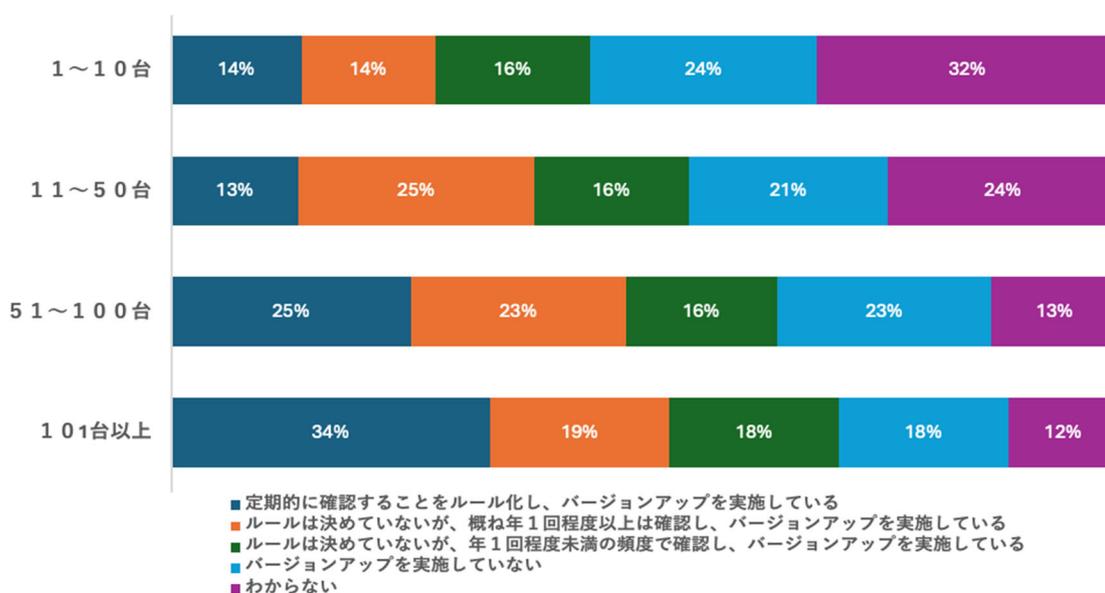
ネットワーク機器のバージョンアップの実施率は、自治体、企業ともほぼ同じ割合で半数程度（自治体：46%→48%→51%、企業54%→50%→52%）。

図表 2-2-20 ネットワーク機器のファームアップ (Q19)



また、導入規模をベースとして分類すると、規模が大きいほどバージョンアップに対応している率が高い。

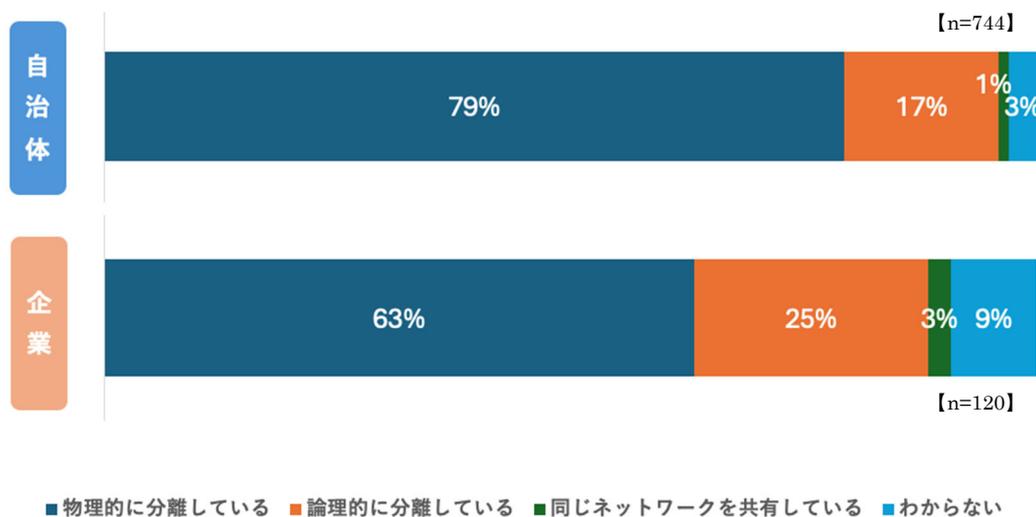
図表 2-2-20b ネットワーク機器のファームアップ (Q19) (導入規模ベース)



③ 業務用ネットワークとの分離 (Q20)

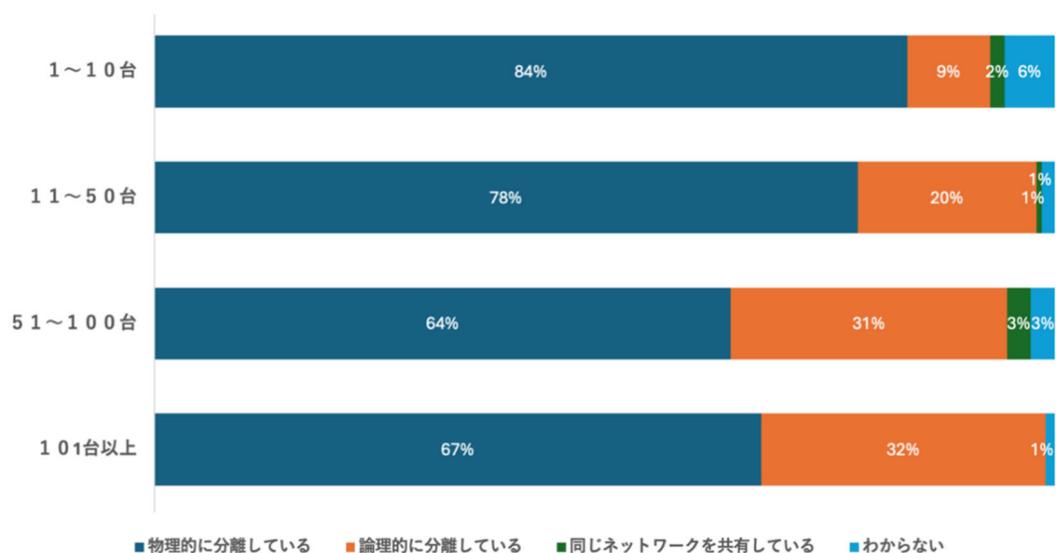
前年と同様に90%以上の団体が、サービス用ネットワークと業務用ネットワークを物理的あるいは論理的にネットワークを分離している。

図表 2-2-21 業務用ネットワークとの分離 (Q20)



導入規模をベースとして分類すると、規模が大きいほど、論理的に分離する率が増加していることが分かった。

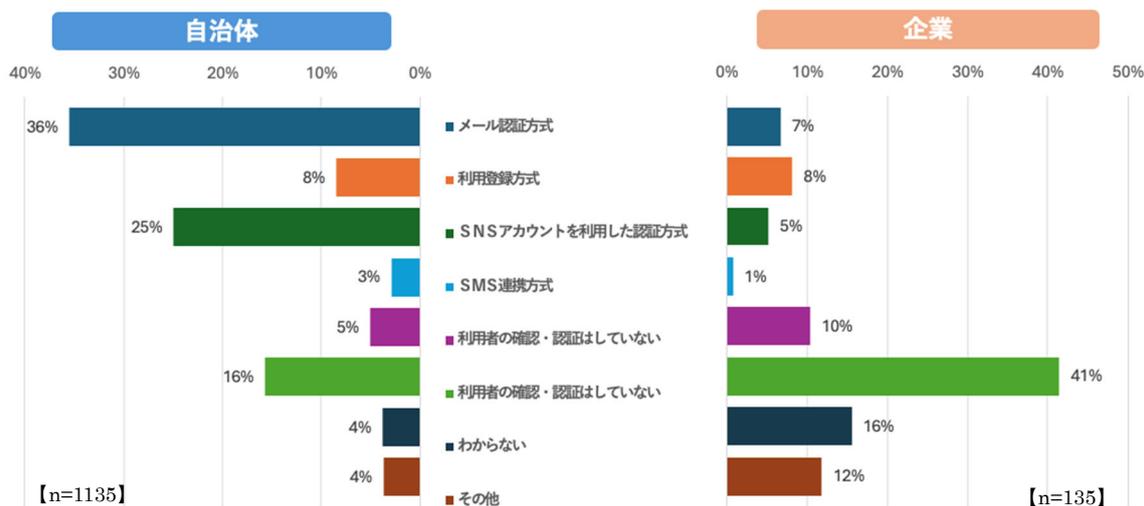
図表 2-2-21b 業務用ネットワークとの分離 (Q20) (導入規模ベース)



④ サービス利用者の認証方式 (Q21)

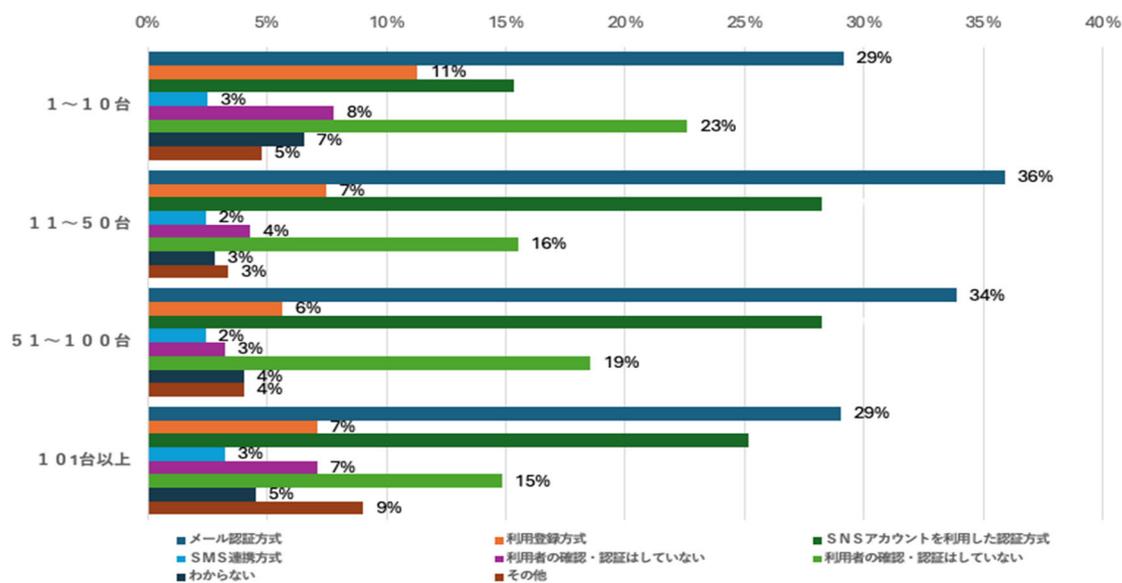
無線 LAN サービスの利用者を確認していない割合は、自治体よりも企業の方が、比率が高い。自治体は「メール認証方式」や「SNS 認証方式」を利用している率が多い。

図表 2-2-22 サービス利用者の認証方式 (Q21)



また、サービスの導入規模をベースとして分類したところ、導入規模が大きいほど「メール認証方式」の利用率は下がる傾向にある。

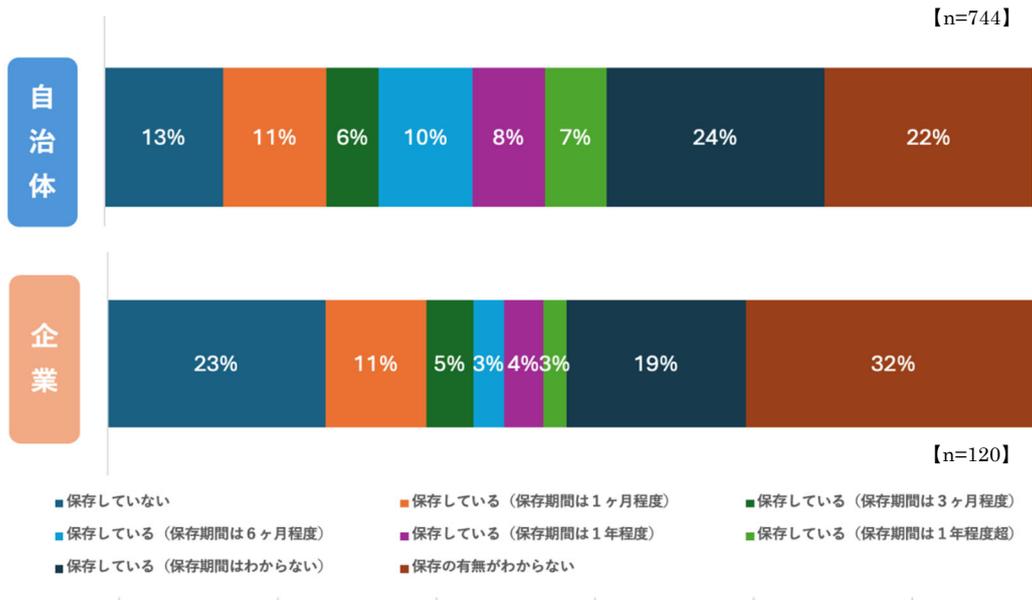
図表 2-2-22b サービス利用者の認証方式 (Q21) (導入規模ベース)



⑤ アクセスログ（通信記録等）の保存（Q23）

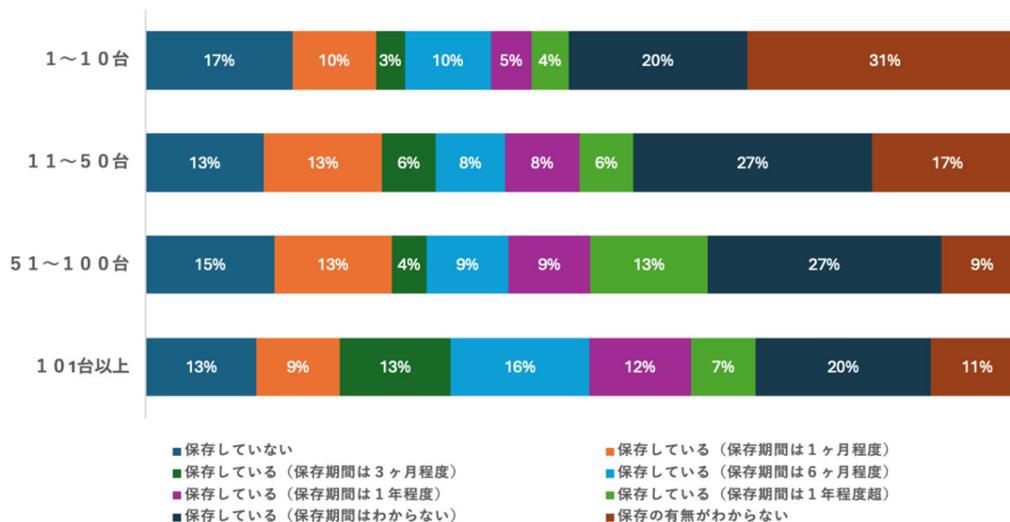
アクセスログを保管している事例は、自治体は 65%であり、前年の 63%より微増したが、企業は 45%で前年の 51%より減少している。

図表 2-2-23 アクセスログ（通信記録等）の保存（Q23）



また、導入規模をベースとして分類すると、規模が大きいほどアクセスログを保存している率が高い。

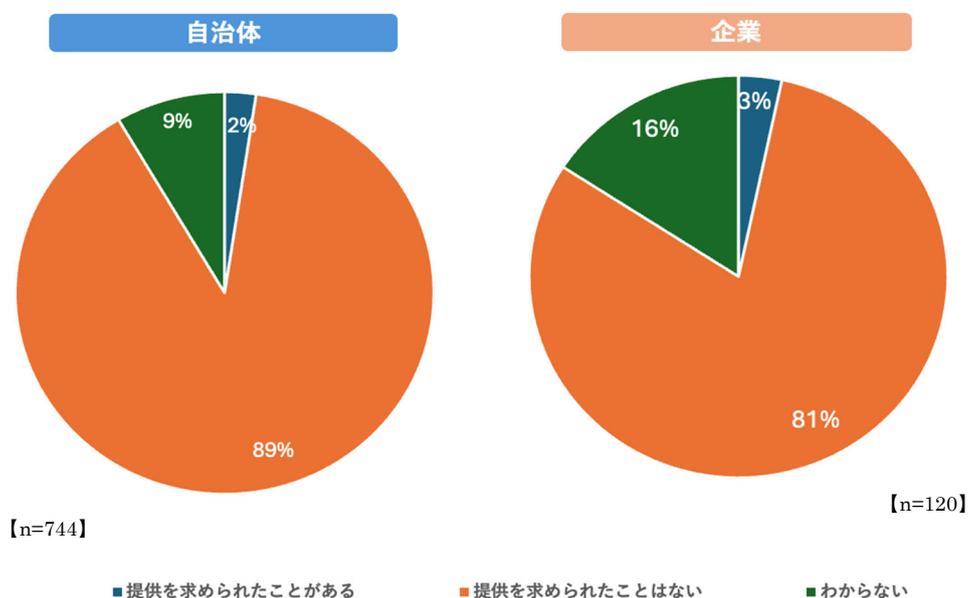
図表 2-2-23b アクセスログ（通信記録等）の保存（Q23）（導入規模ベース）



⑥ アクセスログ（通信記録等）の提供（Q24）

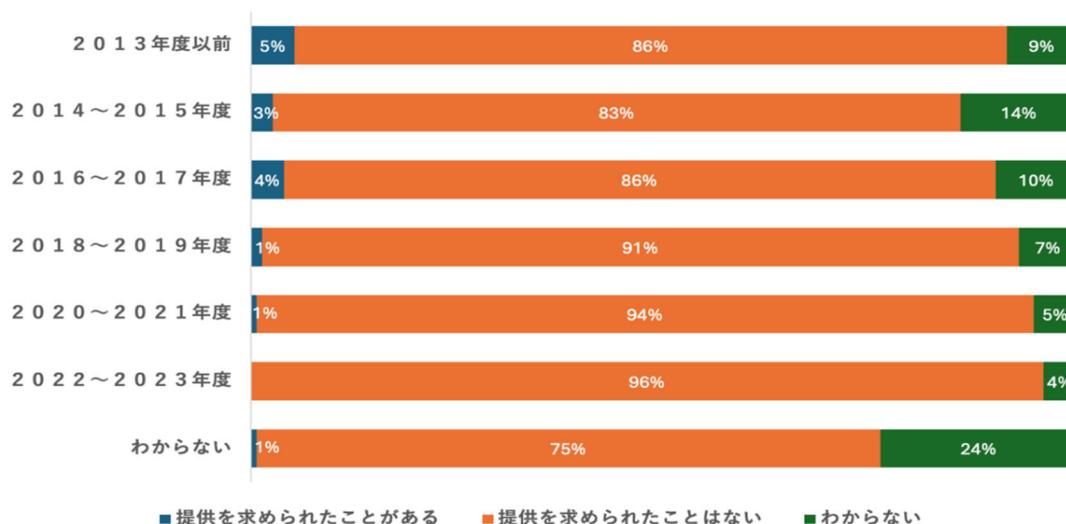
警察からログの提供を求められている事例は前年と同様、自治体・企業ともに少ない。

図表 2-2-24 アクセスログ（通信記録等）の提供（Q24）

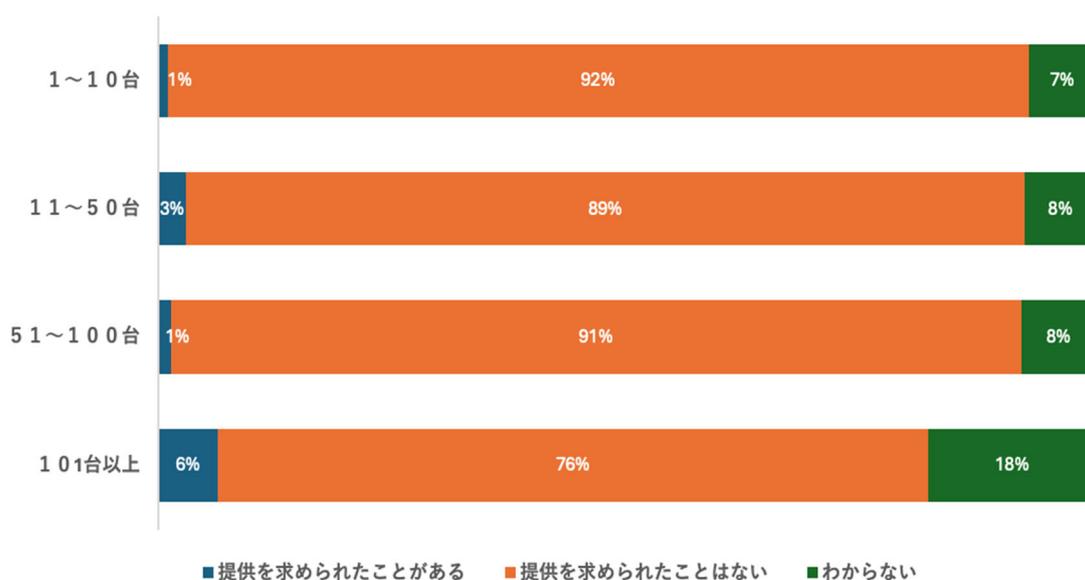


また、導入時期をベースとして分類したところ、2018年度以降、サービスを開始した団体でログの提供を求められているのは極めてまれである。さらに、導入規模をベースとして分類したところ、設備規模が大きいほど、ログの提供を求められている比率が高いことが分かった。

図表 2-2-24a アクセスログ（通信記録等）の提供（Q24）（導入時期ベース）



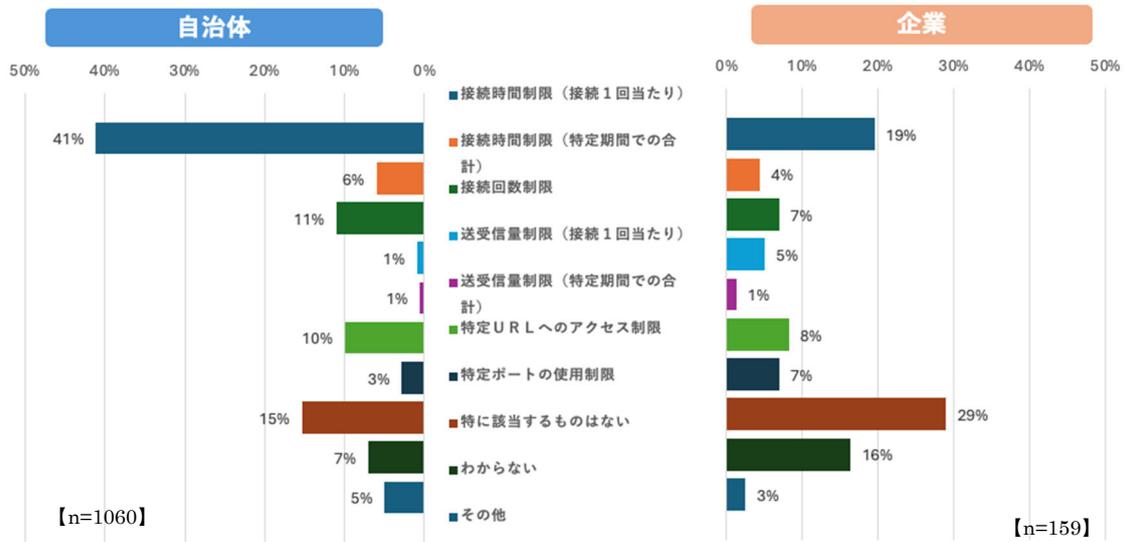
図表 2-2-24b アクセスログ（通信記録等）の提供（Q24）（導入規模ベース）



⑦ その他のセキュリティ対策（Q25）

その他のセキュリティ対策としては、前年と同様に自治体は接続時間を制限する対策がトップ、企業は何も対策をしていない事例がトップになっている。

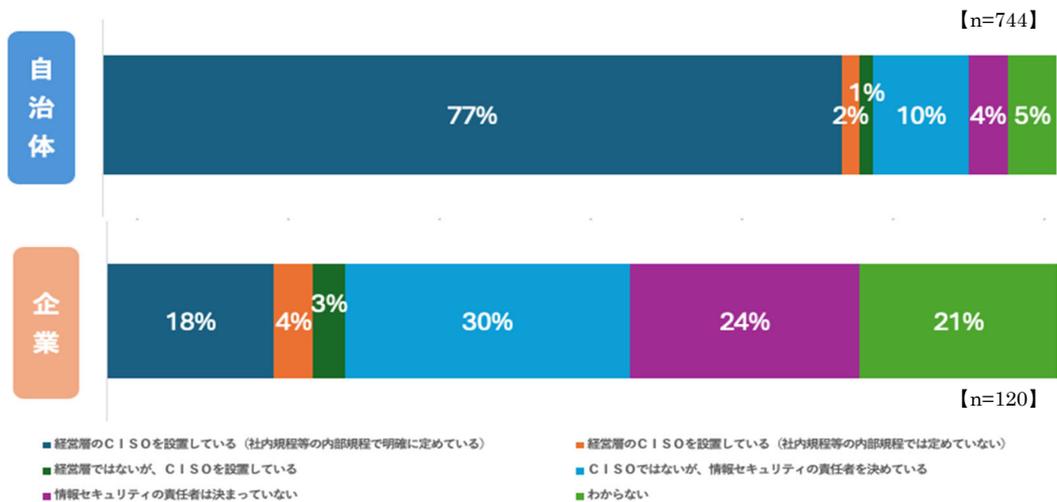
図表 2-2-25 その他のセキュリティ対策 (Q25)



⑧ 情報セキュリティ責任者の設置 (Q26)

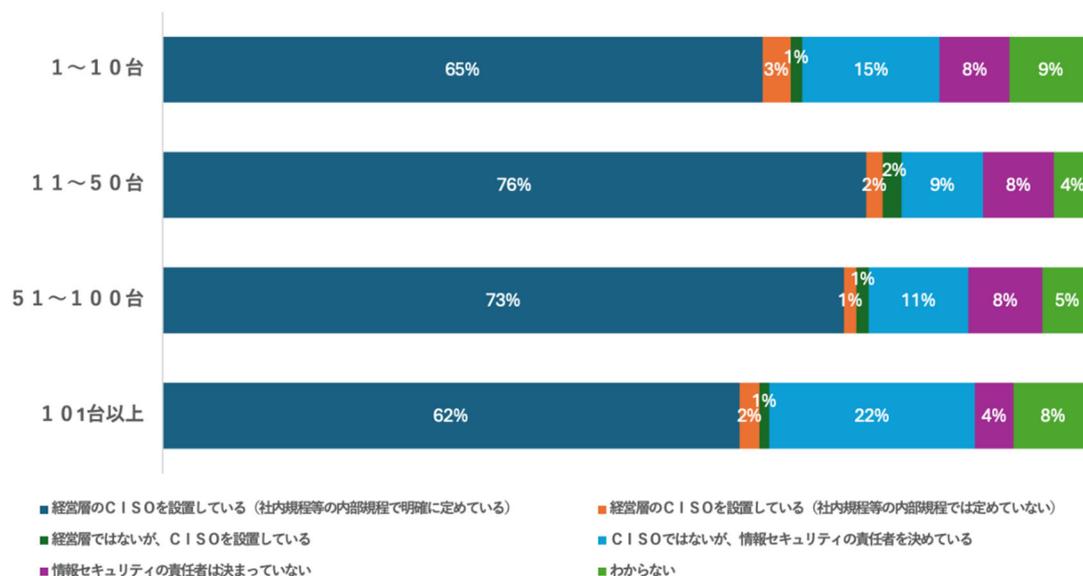
情報セキュリティ責任者を設置している率は自治体、企業ともに前年より増加している（自治体：88%→91%、企業 54%→55%）。自治体は設置している率は企業よりも著しく高い上に、内部規定で明確に定めている率も圧倒的に高い。

図表 2-2-26 セキュリティ責任者の設置 (Q26)



また、導入規模をベースとして分類すると、規模が大きいほど責任者を設置している率が高いことがわかる。

図表 2-2-26b セキュリティ責任者の設置 (Q26) (導入規模ベース)



(4) 利用者に安心を提供するための対策について

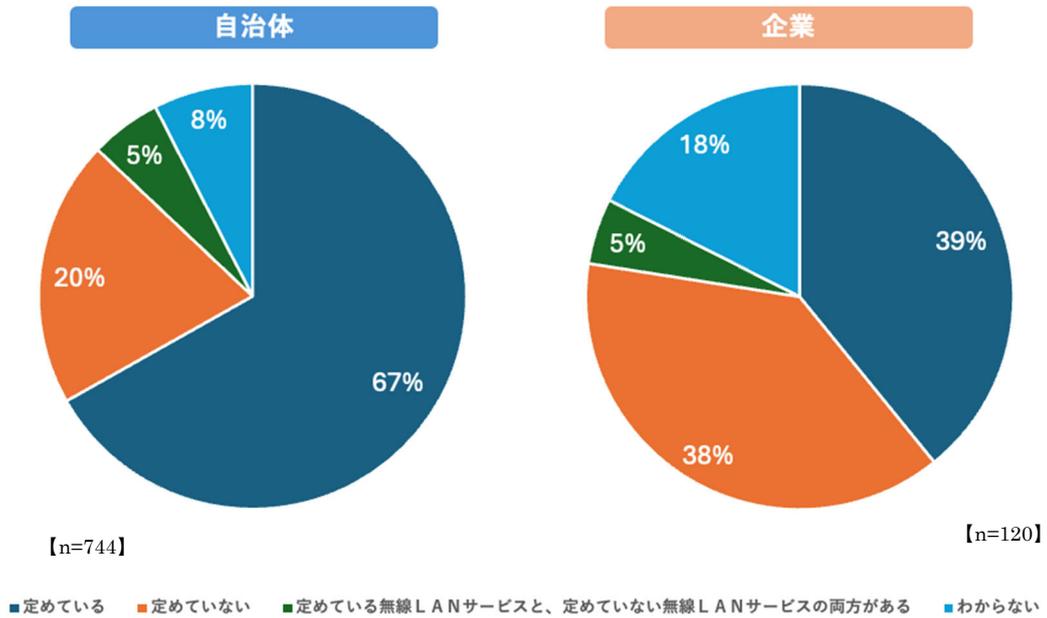
回答には以下のような特徴がみられた。

- 全般的に、昨年改善が見られた対策の実施率は、本年は横ばい状態で改善は見られなかった。

① 無線 LAN サービスの利用規約 (Q27)

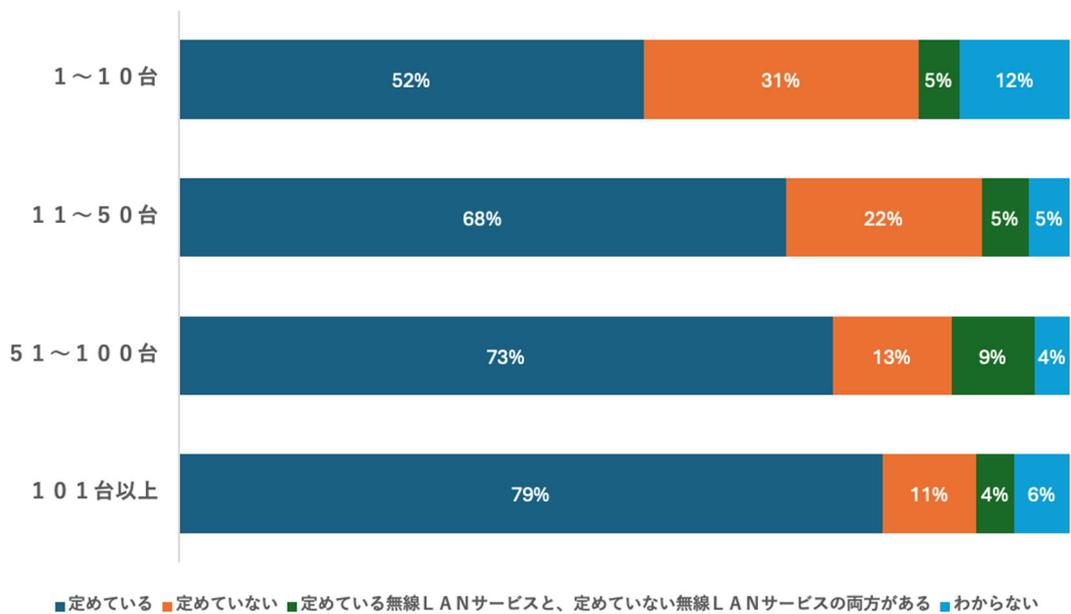
自治体は「利用規約を定めている」率が前年と横ばい、企業は大幅に減少している (自治体：67%→67%、企業 50%→39%)。

図表 2-2-27 無線 LAN サービスの利用規約 (Q27)



さらに、導入規模をベースとして分類すると、規模が大きいほど「利用規約を定めている」率が高いことがわかる。

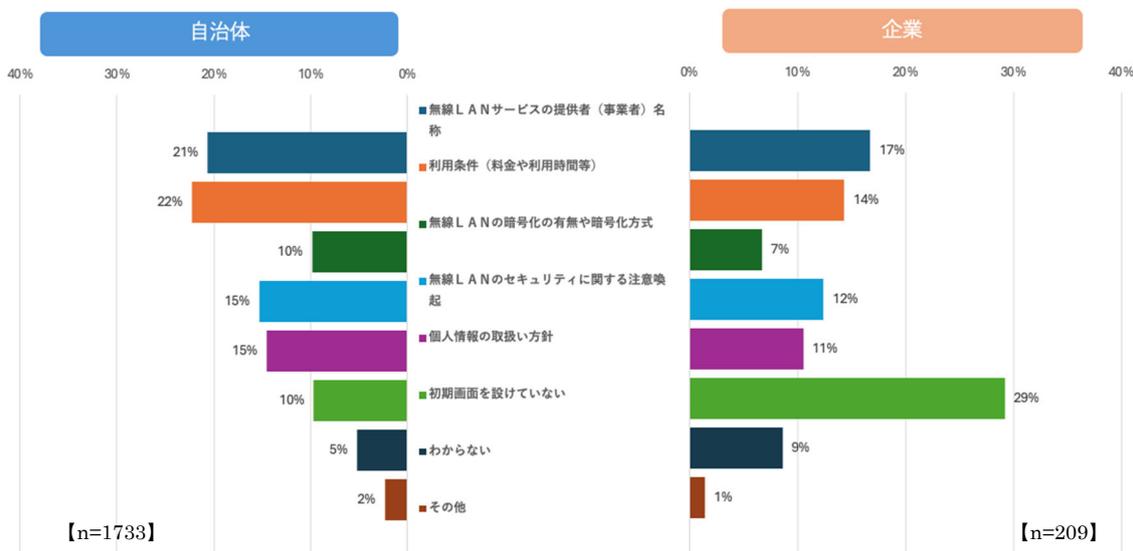
図表 2-2-27b 無線 LAN サービスの利用規約 (Q27) (導入規模ベース)



② 無線 LAN サービスの初期画面 (Q28)

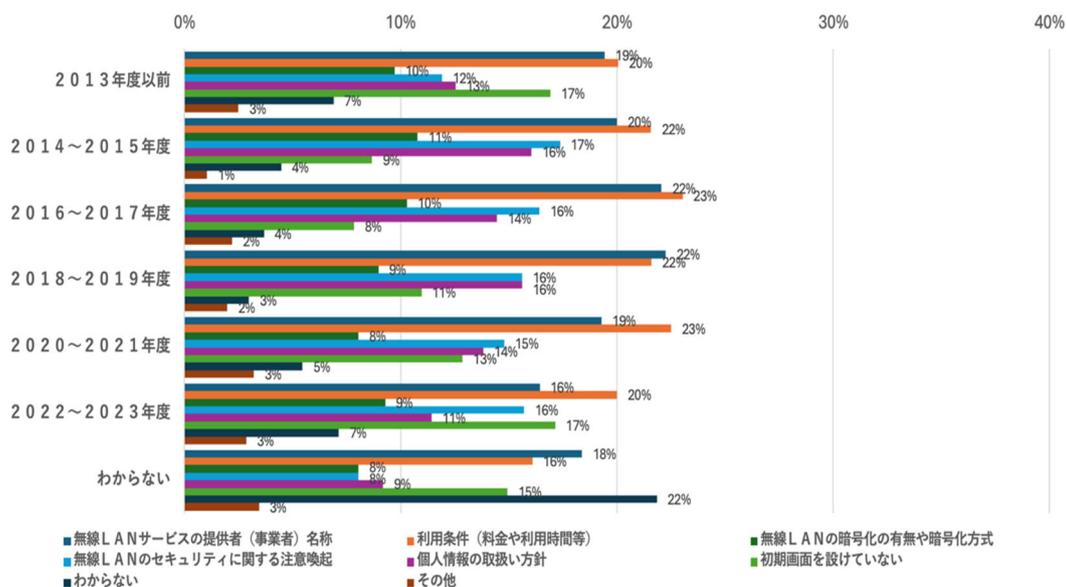
前年と同様に、自治体は約半数が名称及び利用条件を掲載しており、企業は約半数近くが初期画面を設けていない。

図表 2-2-28 無線 LAN サービスの初期画面 (Q28)

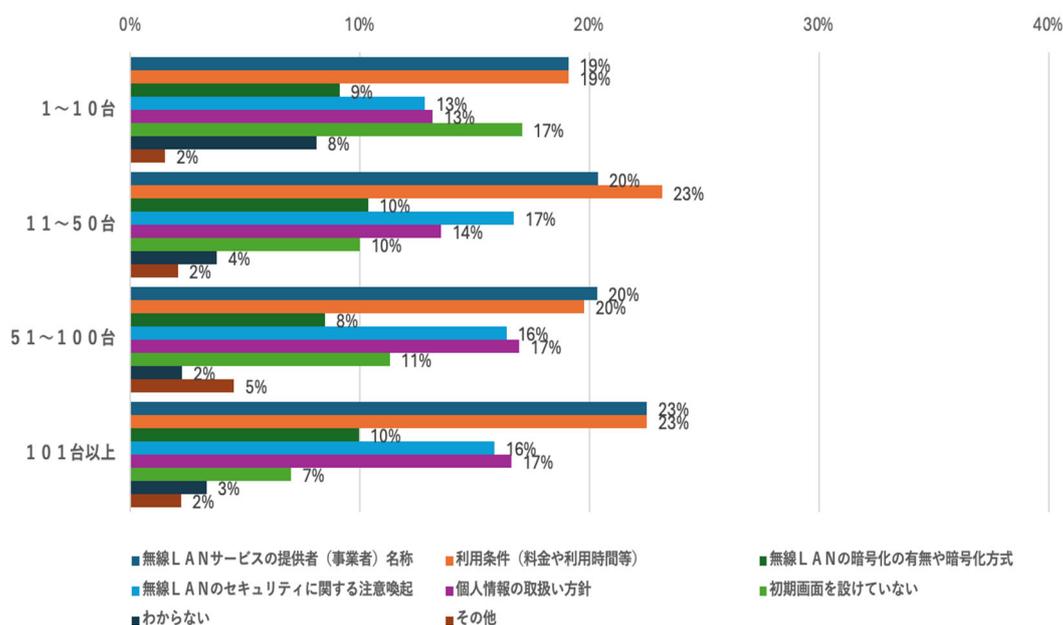


また、導入時期をベースとして分類すると、最近では初期画面を設けていない事例が増加していることが分かった。

図表 2-2-28a 無線 LAN サービスの初期画面 (Q28) (導入時期ベース)



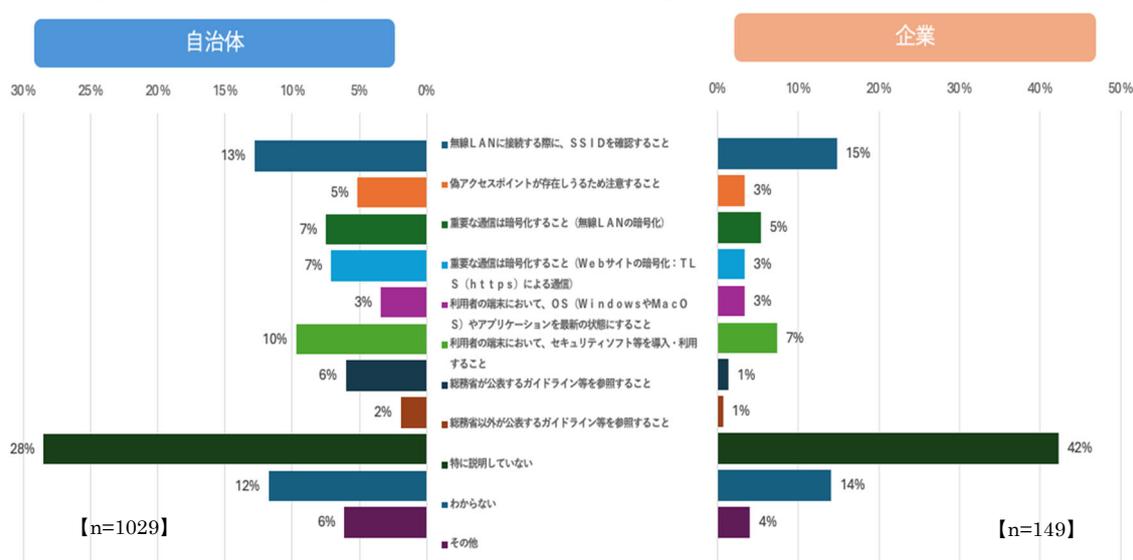
図表 2-2-28b 無線 LAN サービスの初期画面 (Q28) (導入規模ベース)



③ セキュリティに関する注意喚起 (Q29)

自治体、企業ともに、昨年増加した「特に説明していない」が減少した (自治体 : 42% → 46% → 28%、企業 47% → 63% → 42%)。

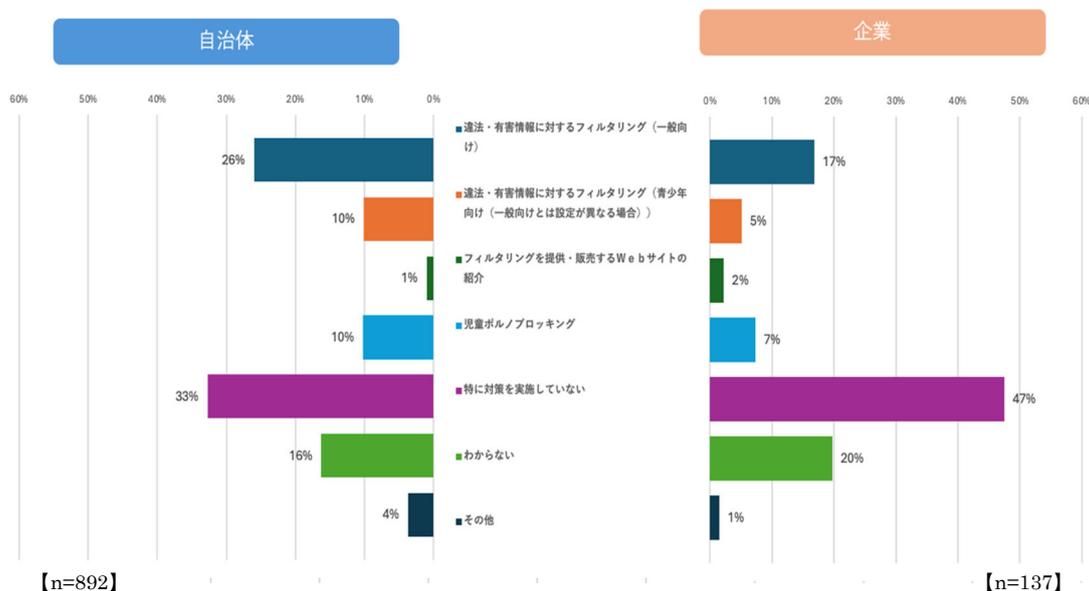
図表 2-2-29 セキュリティに関する注意喚起 (Q29)



④ 違法・有害情報への対策 (Q30)

前年と同様の傾向で自治体、企業ともに「特に対策を実施していない」が最も多い。

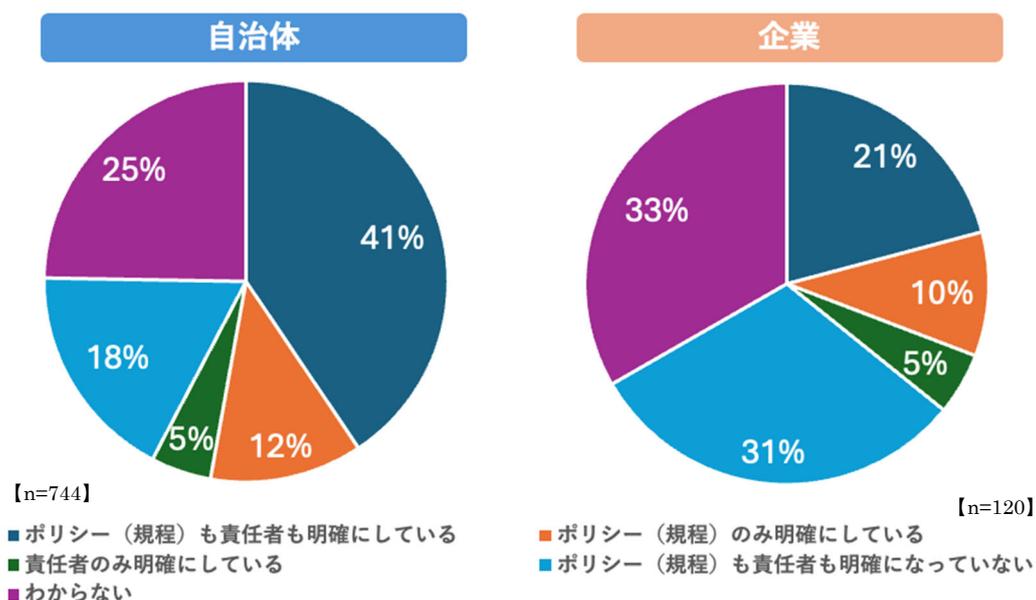
図表 2-2-30 違法・有害情報への対策 (Q30)



⑤ 利用者情報のデータ保護 (Q31)

前年と同様の傾向であり、利用者情報のデータ保護に対して何らかの対応をしている率は、地方自治体が58%で、企業の36%に比べ高い。

図表 2-2-31 利用者情報のデータ保護 (Q31)



(5) 無線 LAN のセキュリティ等全般について

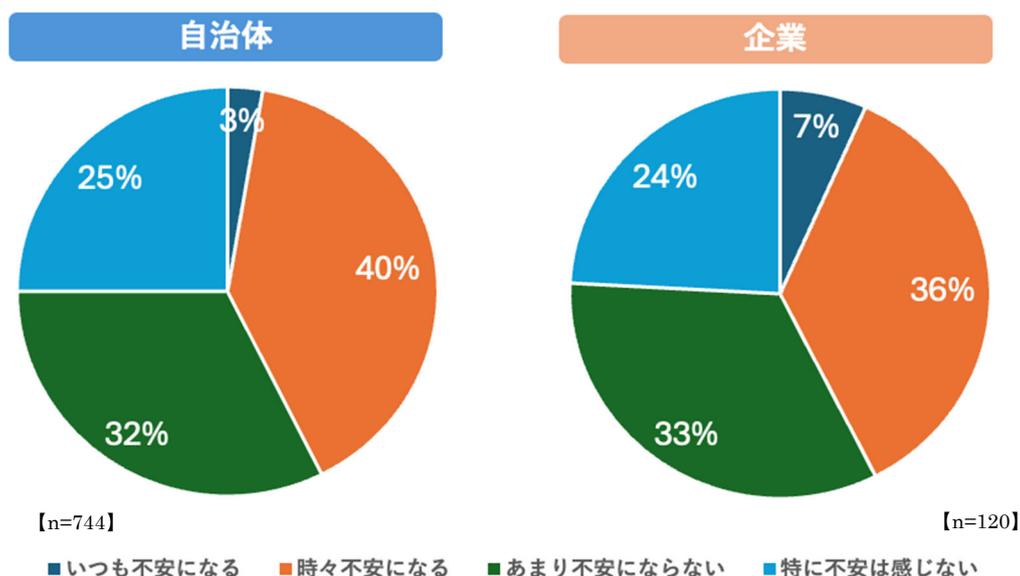
回答には以下のような特徴がみられた。

- セキュリティに対する不安がある団体は自治体が増加しており、企業については減少している。
- サービスの整備更改や、セキュリティに関する整備更改を実施または検討している自治体は微増、企業は横ばいの状況であった。円安と原材料コストの上昇による企業業績の悪化が投資計画に影響を及ぼしていると考えられる。
- 新規技術として、Wi-Fi 6 の導入あるいは導入検討をしている率は微増している。ローカル 5 G の導入については導入を検討する自治体、企業ともに増加しており、普及の兆しがうかがえる。
- 前年向上したセキュリティの手引きの認知率は、自治体は横ばいであったが、企業は減少している。
- 手引きには、技術的な観点や具体的な事例などの記載が要望されていることがわかった。

① サービスのセキュリティへの不安 (Q32)

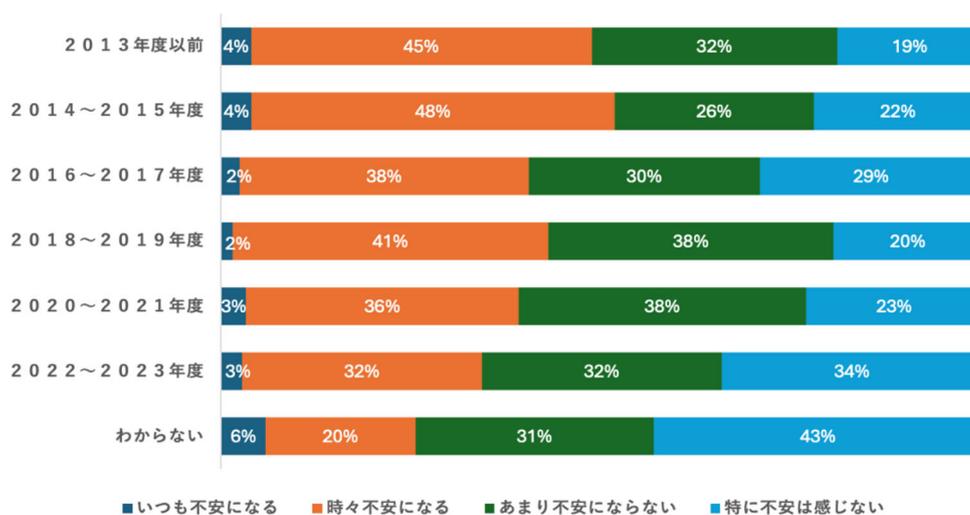
セキュリティに対する不安がある団体は、地方自治体が微増、企業は減少 (自治体 38% →43%、企業 66%→43%)。

図表 2-2-32 サービスのセキュリティへの不安 (Q32)



また、導入時期をベースとして分類すると、2013 年以降、サービス導入時期が最近になるほどセキュリティを不安感じる団体が減少している。

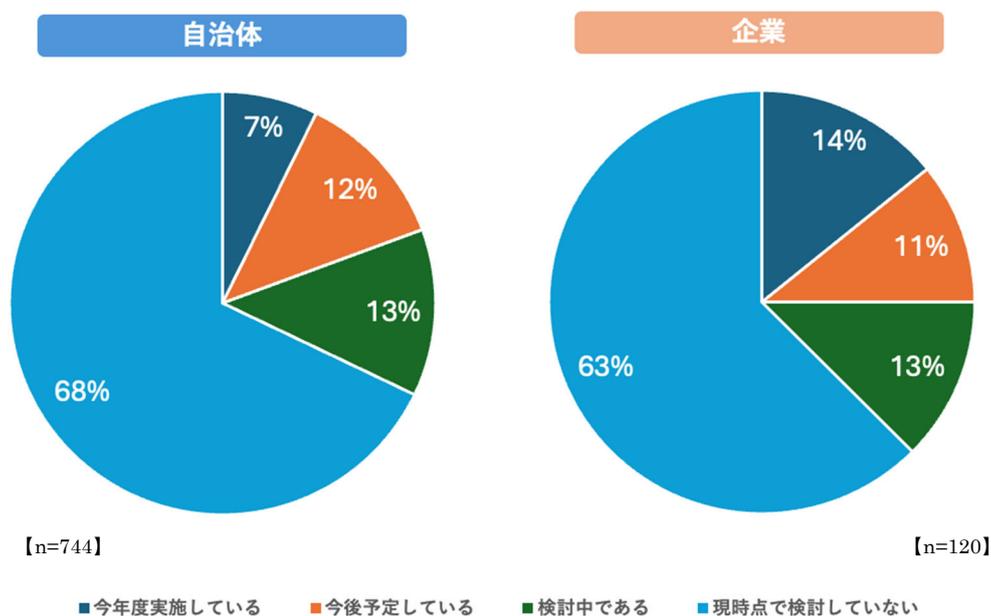
図表 2-2-32a サービスのセキュリティへの不安 (Q32) (導入時期ベース)



② サービスの設備拡充や更改計画 (Q33)

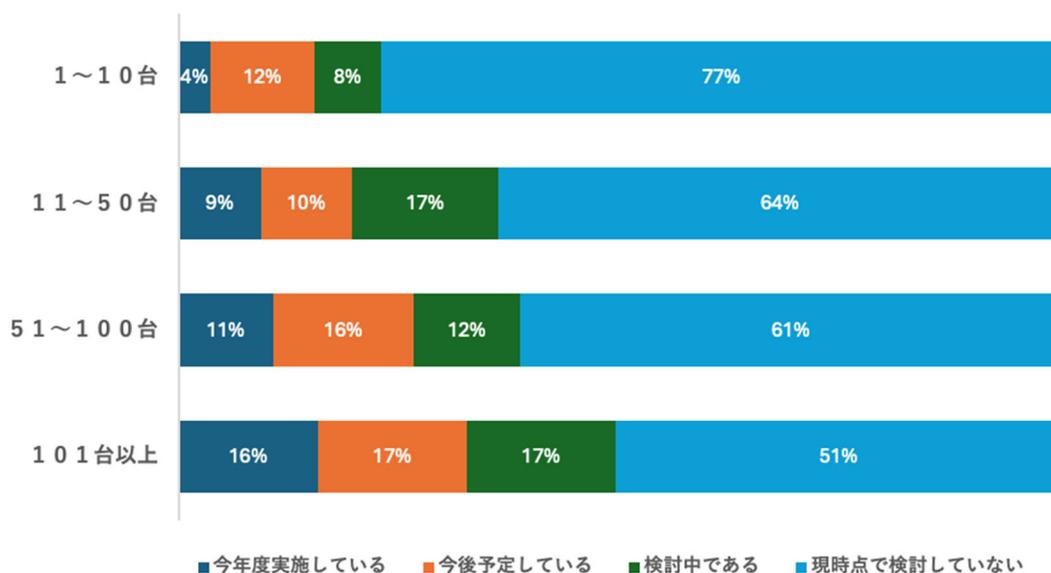
前年に比べ、整備更改等を実施・検討している率は自治体が微増しており、企業は横ばいであった (自治体 29%→32%、企業 38%→38%)。

図表 2-2-33 サービスの設備拡充や更改計画 (Q33)



また、導入規模をベースとして分類すると、規模が大きいほど整備更改等を実施あるいは計画している率が高いことがわかる。

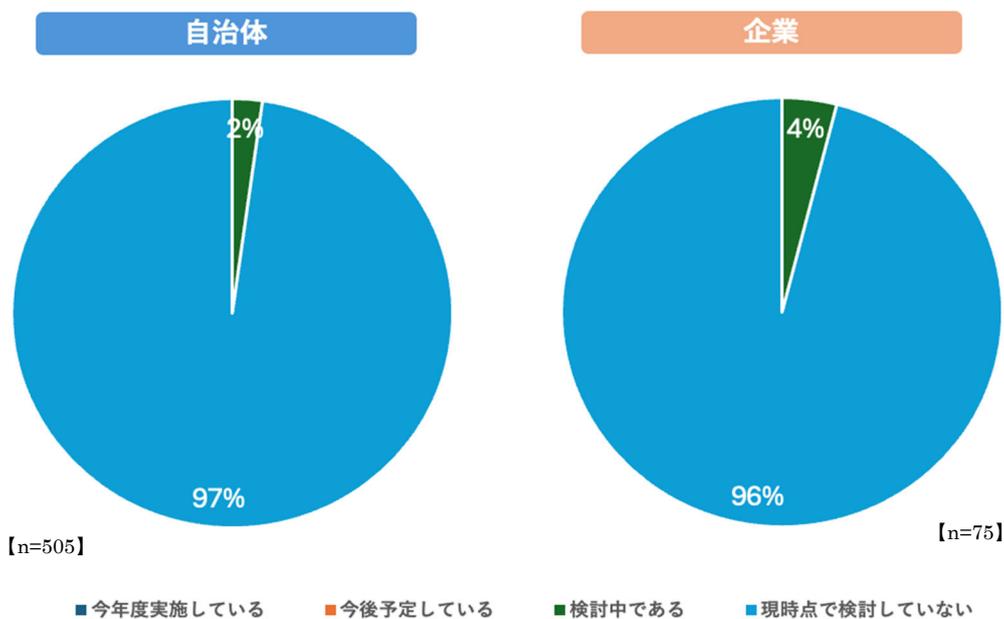
図表 2-2-33b サービスの設備拡充や更改計画 (Q33) (導入規模ベース)



③ サービスのセキュリティ強化計画 (Q35)

前年に比べ、セキュリティ強化を実施・検討している割合が大きく減少している（自治体 13%→2%、企業 19%→4%）。

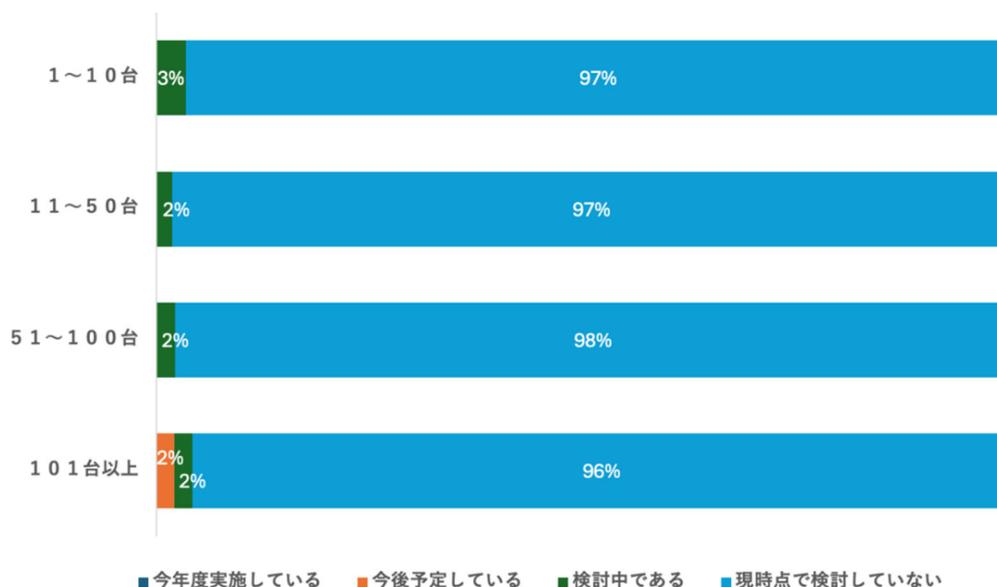
図表 2-2-34 サービスのセキュリティ強化計画 (Q35)



また、導入規模をベースとして分類すると、セキュリティ強化を実施あるいは計画し

ている率は規模の大小に関わらず低い割合であることがわかる。

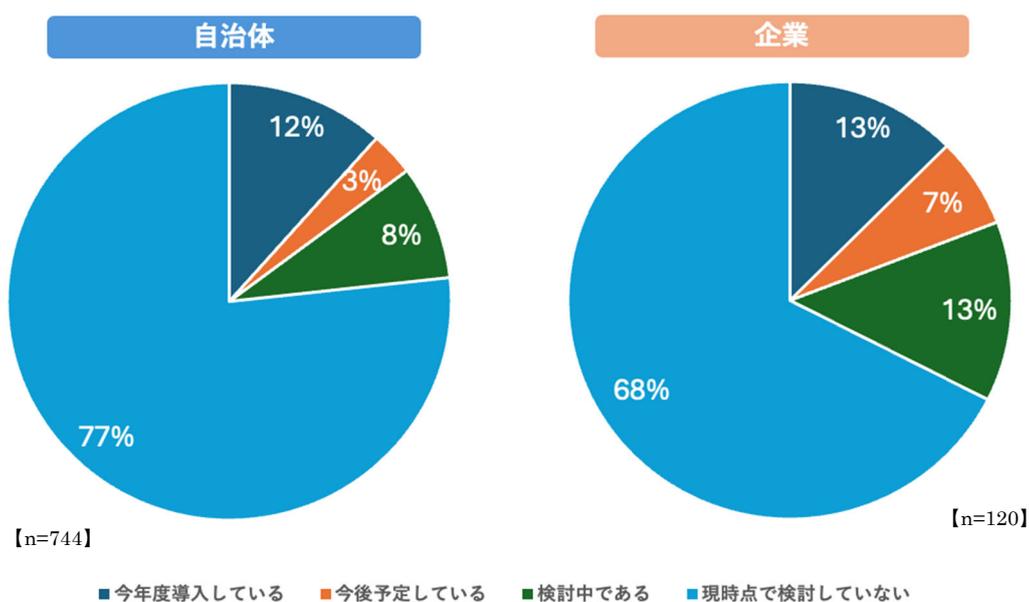
図表 2-2-34b サービスのセキュリティ強化計画 (Q35) (導入規模ベース)



④ Wi-Fi 6 の導入予定 (Q37)

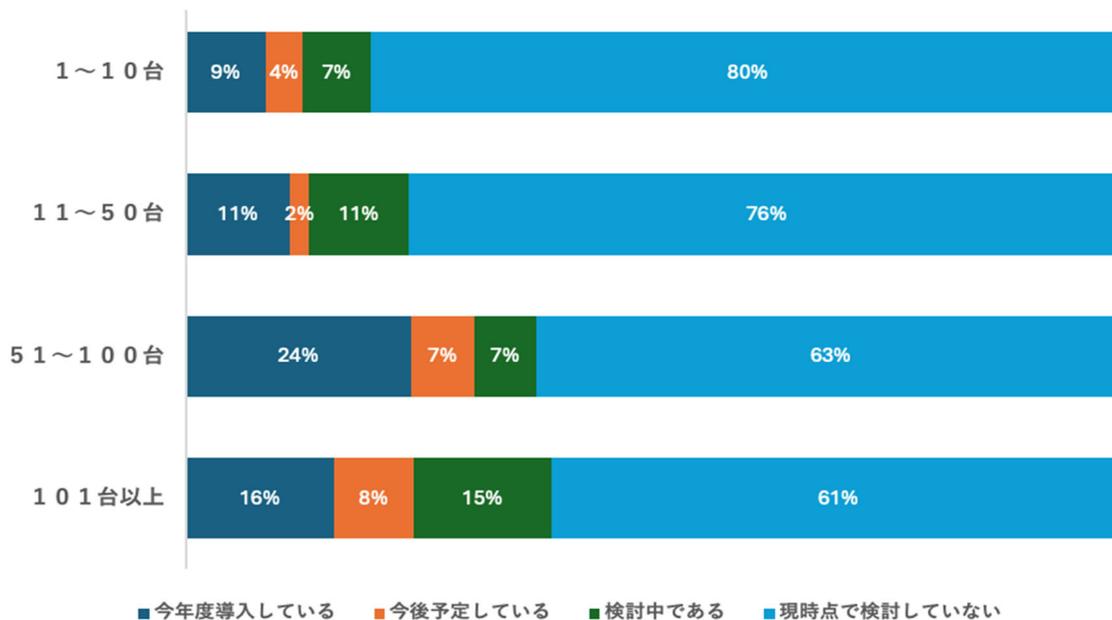
Wi-Fi 6 の導入更改を実施検討している割合は増加しており (自治体 18%→23%、企業 27%→33%)、自治体、企業ともに 2~3 割程度。

図表 2-2-35 Wi-Fi 6 の導入予定 (Q37)



また、導入規模をベースとして分類すると、規模が大きいほどWi-Fi 6の導入更改を実施あるいは計画している率が高いことがわかる。

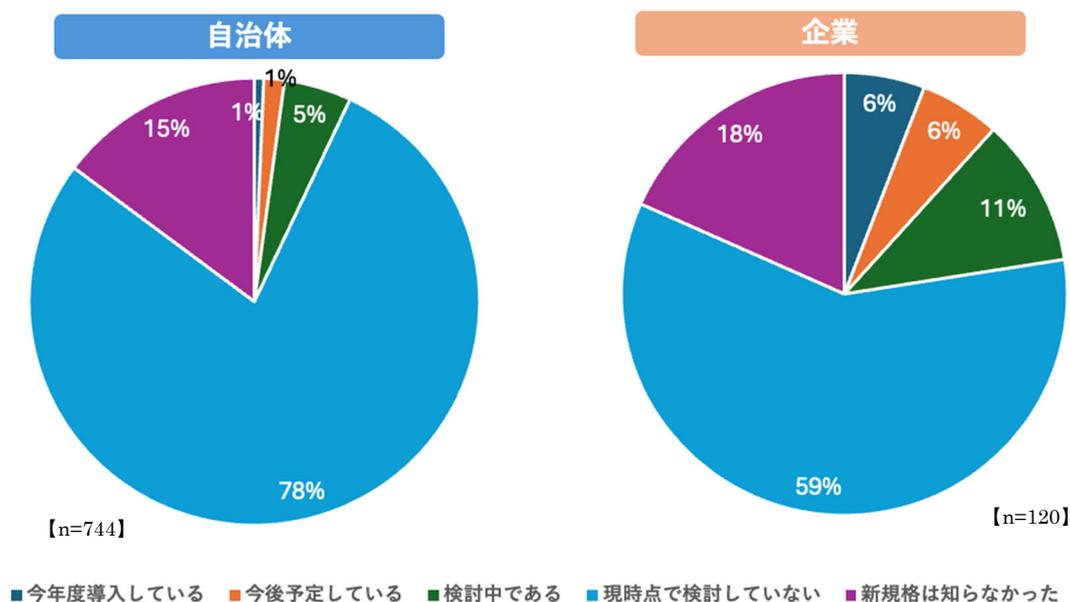
図表 2-2-35b Wi-Fi 6 の導入予定 (Q37) (導入規模ベース)



⑤ Wi-Fi 6E 導入予定 (Q38)

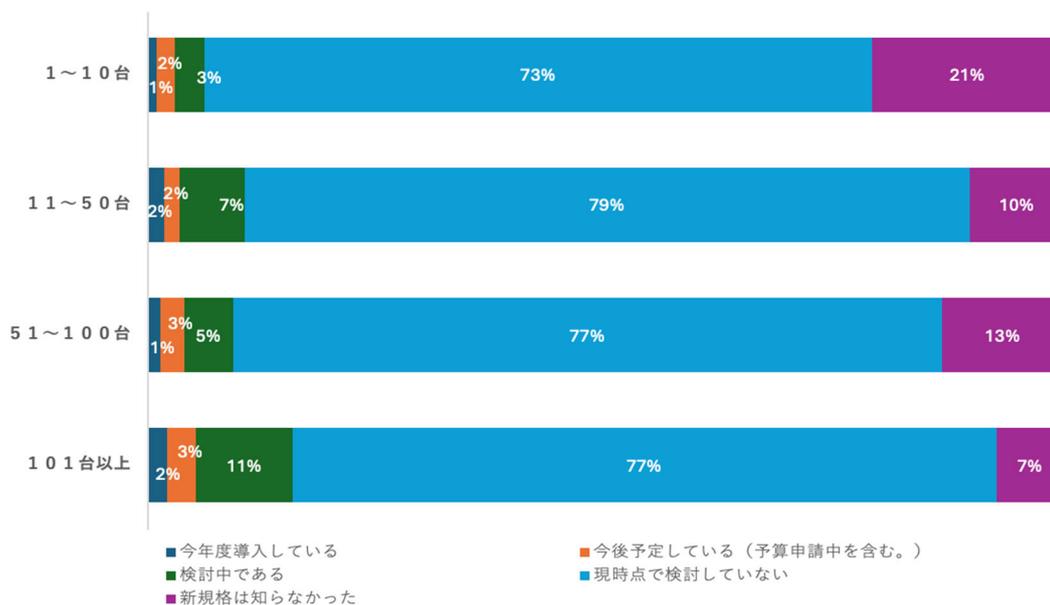
Wi-Fi 6Eの導入・更改を実施・検討している割合は自治体は1割以下、企業は2割程度である。

図表 2-2-36 Wi-Fi 6E の導入予定 (Q38)



また、導入規模をベースとして分類すると、規模が大きいほど Wi-Fi 6 の導入更改を実施あるいは計画している率が高いことがわかる。

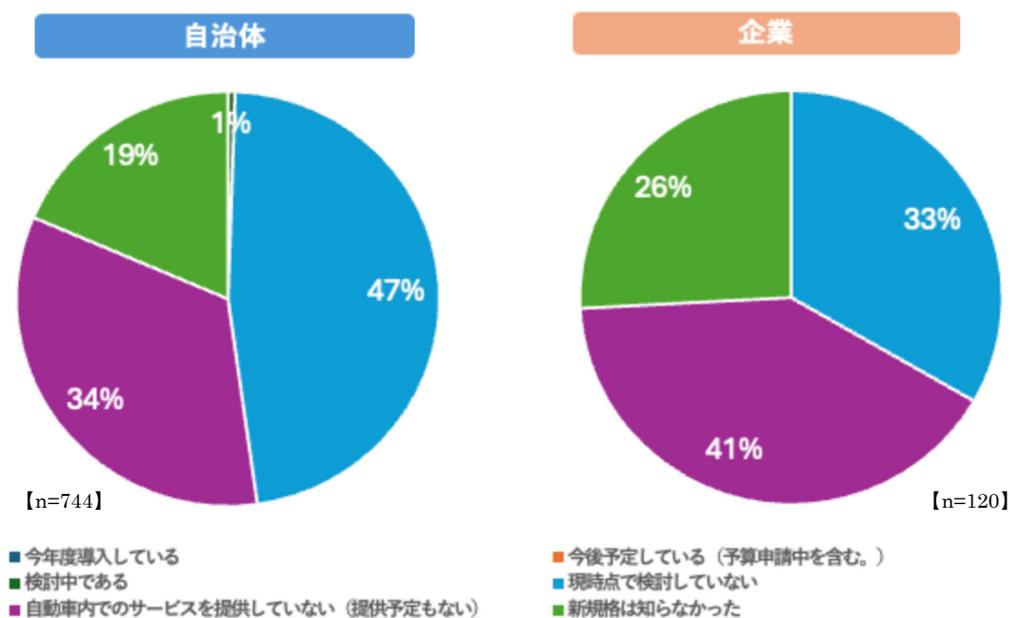
図表 2-2-36b Wi-Fi 6E の導入予定 (Q38) (導入規模ベース)



⑥ 5.2GHz 自動車内利用の導入予定 (Q39)

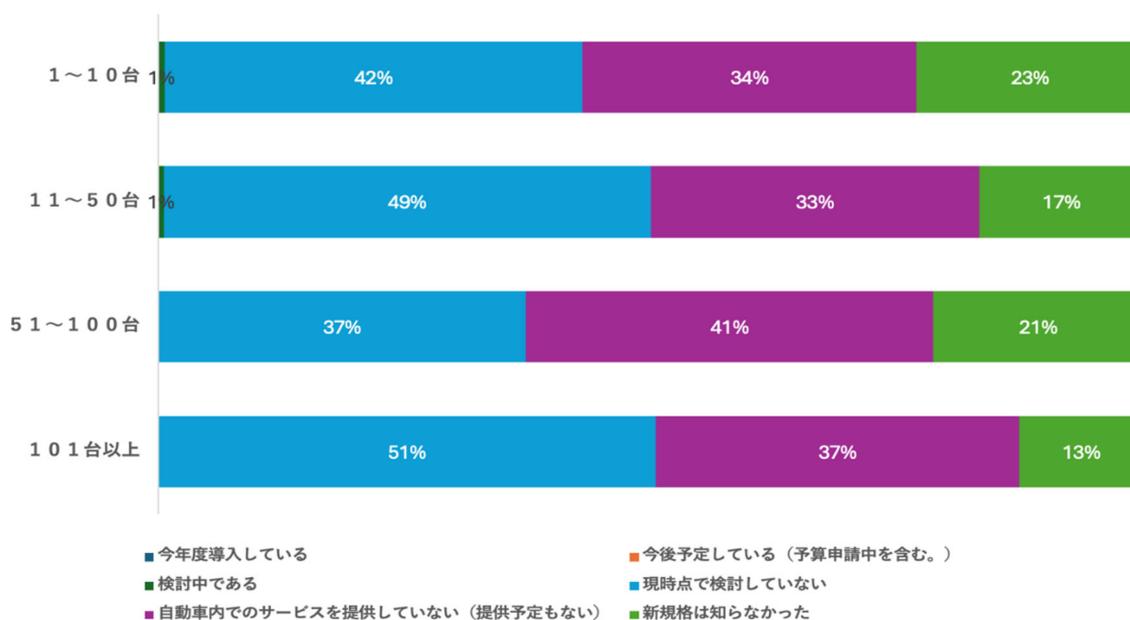
5.2GHz 自動車内利用の導入更改を実施あるいは計画している自治体および企業はほとんどないことがわかった。

図表 2-2-37 5.2GHz 自動車内利用の導入予定 (Q39)



また、導入規模をベースとして分類すると、規模の大小を問わず、5.2GHz 自動車内利用の導入更改を実施あるいは計画している自治体、企業はほとんどないことがわかる。

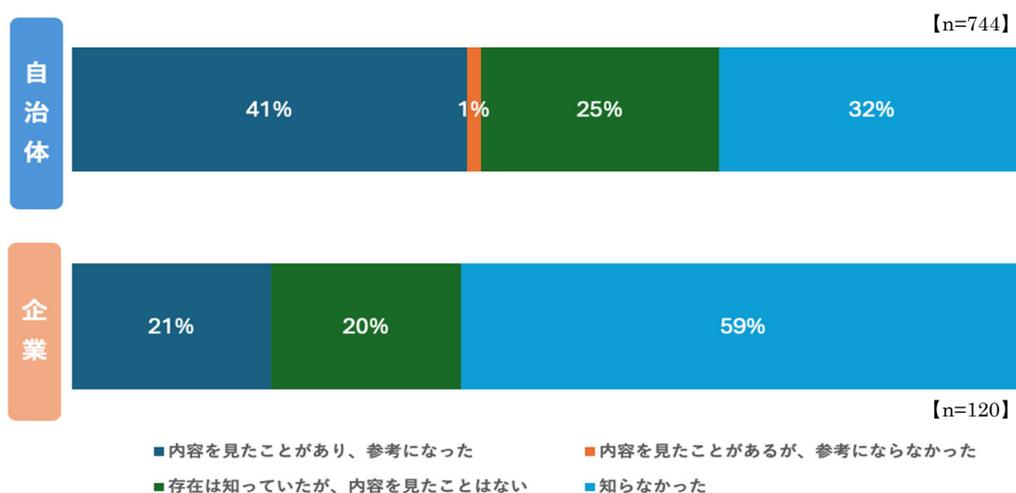
図表 2-2-37b 5.2GHz 自動車内利用の導入予定 (Q39) (導入規模ベース)



⑦ セキュリティ対策の手引き (Q40)

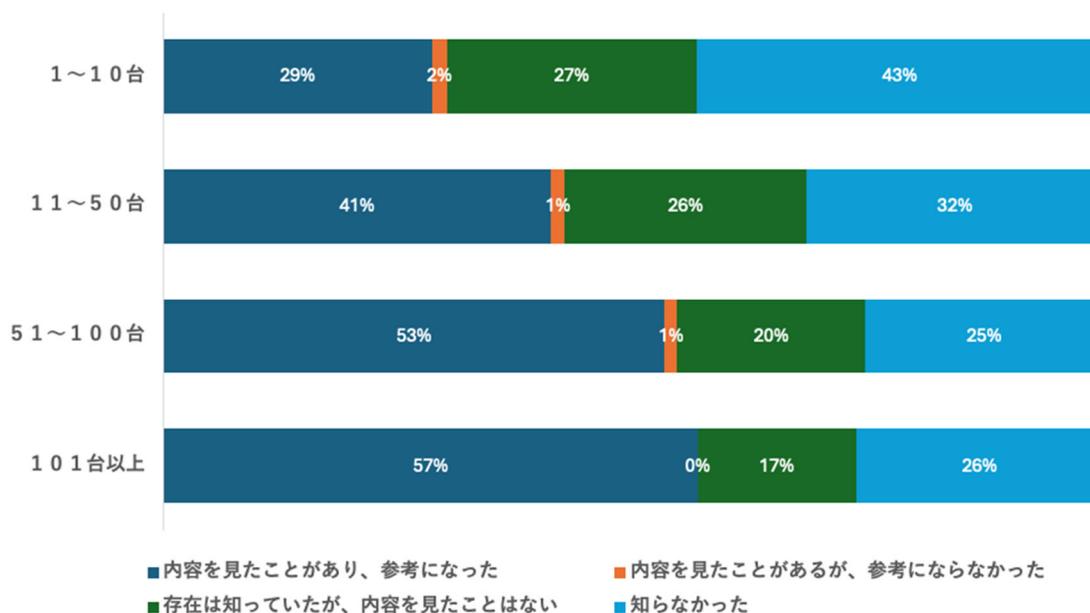
「手引き」の内容を見た団体の率は自治体は横ばいであり、企業は減少している（自治体 39%→42%、企業 26%→21%）。

図表 2-2-39 セキュリティ対策の手引き (Q40)



また、サービスの導入規模をベースとして分類したところ、規模が大きいものほど「手引き」を認識している率が高いことが分かった。

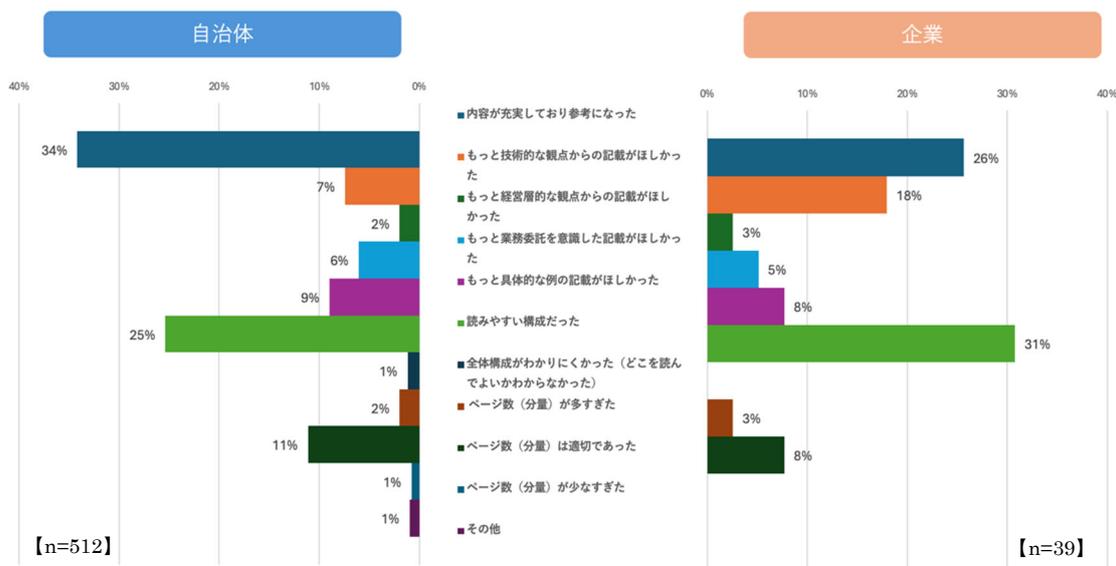
図表 2-2-39b セキュリティ対策の手引き (Q40) (導入規模ベース)



⑧ セキュリティ対策の手引きの内容 (Q41)

手引きの内容については、自治体、企業ともに良い評価は減少 (51%→43% 41%→17%) した。また、技術的な観点及び具体的な例の記載への要望が自治体、企業ともに多くなっている。

図表 2-2-40 セキュリティ対策の手引きの内容 (Q41)



(6) 企業における業種による特徴について

企業のデータについて、業種別の特徴についてまとめて示す。なお、集計はサンプル数の少ないものについては一つにまとめた。小売店、飲食店、薬局は小売業としてまとめ、貸会議室、コワーキングスペース関連は宿泊施設とまとめた。

娯楽遊戯施設については分計してまとめたが、サンプル数が少なく、考察の対象外となる事例も生まれた。

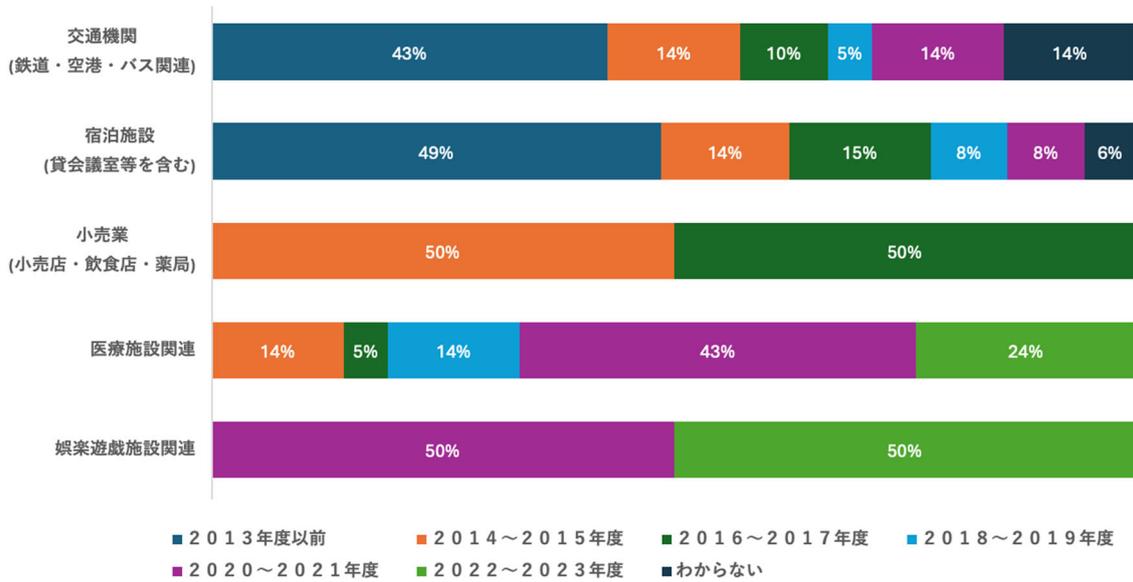
回答には以下のような特徴がみられた。

- ・無線 LAN サービスの導入時期は交通機関、宿泊施設は 2013 年以前からの比率が高いが、医療施設関連、娯楽遊戯施設関連については 2020 年以降の導入が多く占める。無線 LAN の目的は「来訪者サービスの向上」はあらゆる業種で多く、「災害時の活用」は交通機関、医療関連施設に多い。なお「通信事業者からの依頼」については交通機関と小売業に集中している。
- ・無線 LAN の暗号化については、利用の簡便性（ユーザの利便性）から交通機関は暗号化なしが多いが、宿泊施設や医療施設関連は暗号化率が高い。
- ・宿泊施設は、全回答がセキュリティの責任者が決まっていない、セキュリティに関する認識も低い事例が多い。特に、利用規約や初期画面など利用者に対する対応についても不十分な例が多く、新技術に対する認識度も低い。
- ・医療施設関連は、他と明確に異なる数字を示しており、特に電子カルテなどを扱うことから、セキュリティへの不安や、セキュリティ対策についての関心も高い。

① 無線 LAN サービスの導入時期 (Q2)

医療施設関連は 2020 年度以降の導入が 6 割、娯楽遊戯施設関連はすべての施設が 2020 年以降の導入となっている。

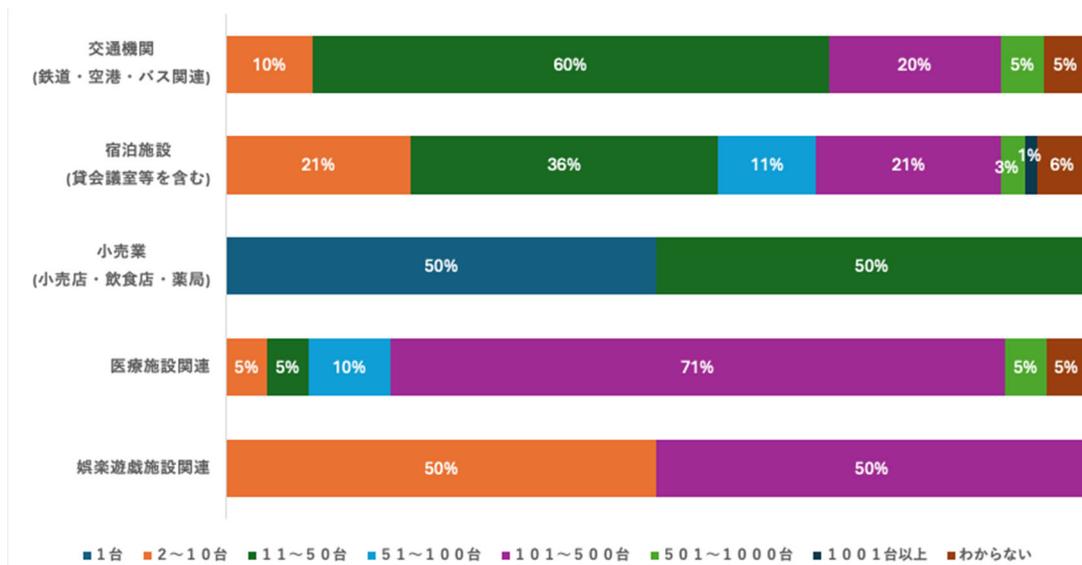
図表 2-2-41 無線 LAN サービスの導入時期 (Q2) (業種ベース)



② 無線 LAN サービスの規模 (Q5)

医療施設関連、娯楽遊戯施設関連は交通機関や宿泊施設に比べ、大規模な設備の率が高いことが分かった。

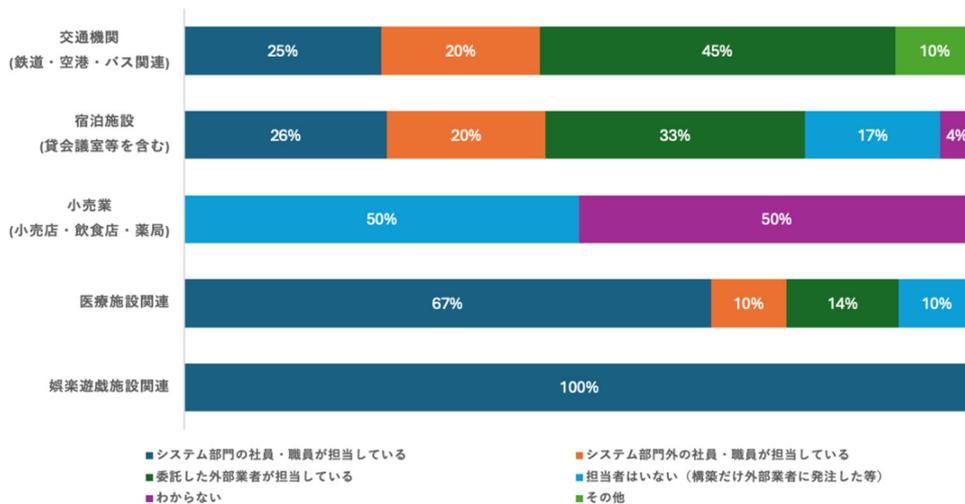
図表 2-2-42 無線 LAN サービスの規模 (Q5) (業種ベース)



③ 無線 LAN サービスの運用管理 (Q6)

医療施設関連、娯楽遊戯施設関連は、無線サービスの運用管理を内部のシステム部門が担当している率が極めて高いことが分かった。

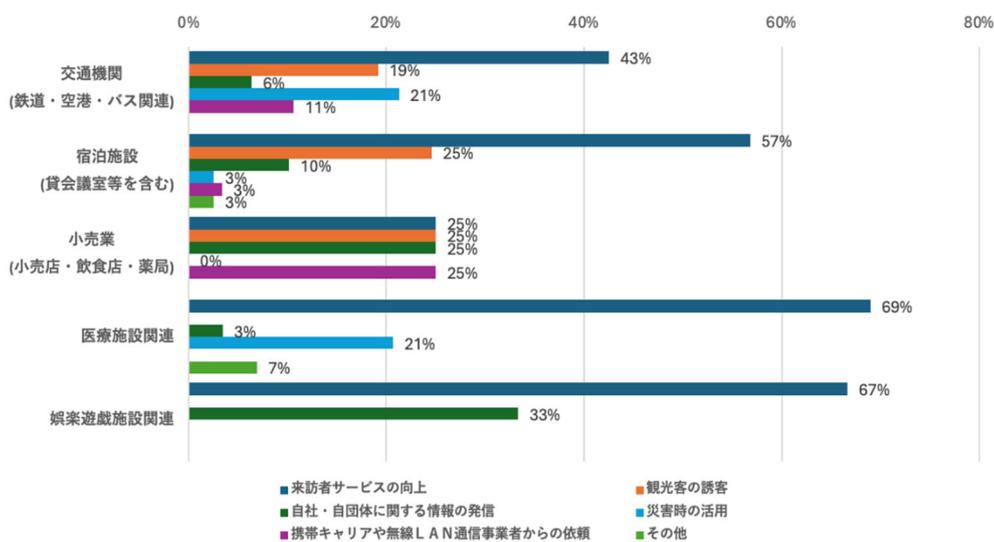
図表 2-2-43 無線 LAN サービスの運用管理 (Q6) (業種ベース)



④ 無線 LAN サービスの目的 (Q7)

「来訪者サービスの向上」はあらゆる業種で多く、「災害時の活用」は交通機関、医療施設関連で多い。なお「通信事業者からの依頼」については交通機関と小売業に集中している。

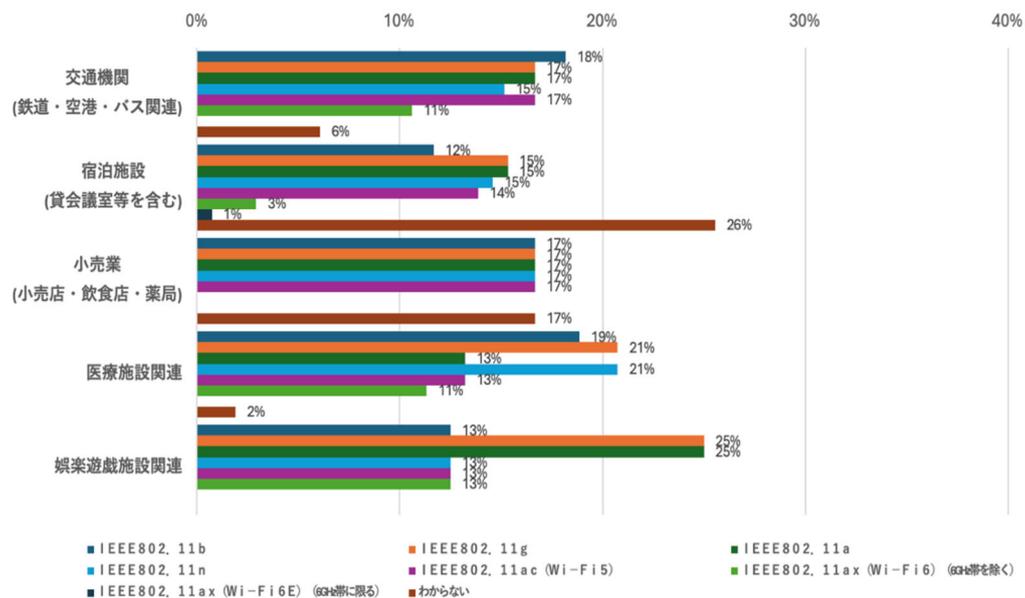
図表 2-2-44 無線 LAN サービスの目的 (Q7) (業種ベース)



⑤ 無線 LAN サービスの伝送規格 (Q8)

宿泊施設、小売業は無線 LAN サービスの伝送規格について「わからない」の率が多い。

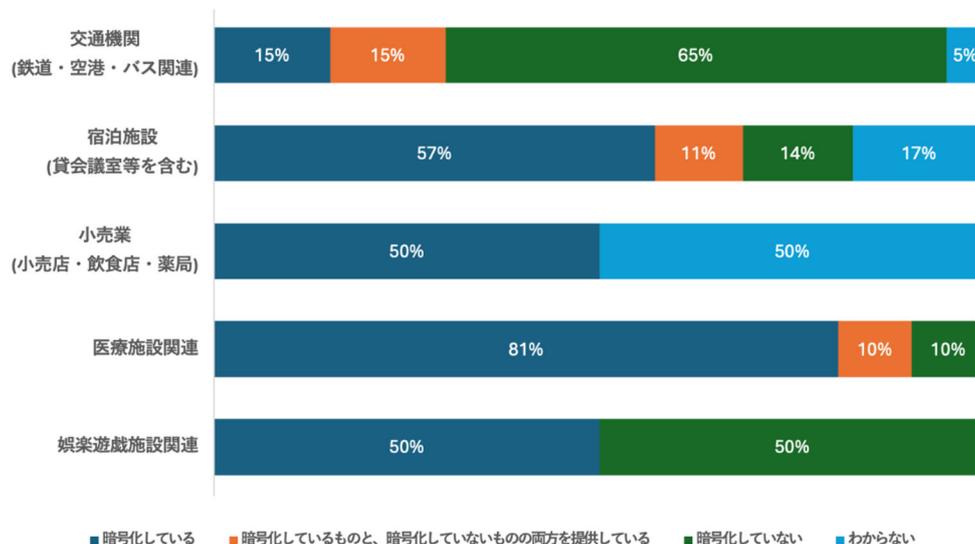
図表 2-2-45 無線 LAN サービスの伝送規格 (Q8) (業種ベース)



⑥ 無線 LAN サービスの暗号化 (Q9)

前年と同様に交通機関は暗号化していない率が高い(規模が大きいものが多く利便性のためと思われる)。逆に宿泊施設や小売業、医療施設関連、娯楽遊戯施設関連の半数以上は、暗号鍵を配布することが容易であるため暗号化している率が高い。

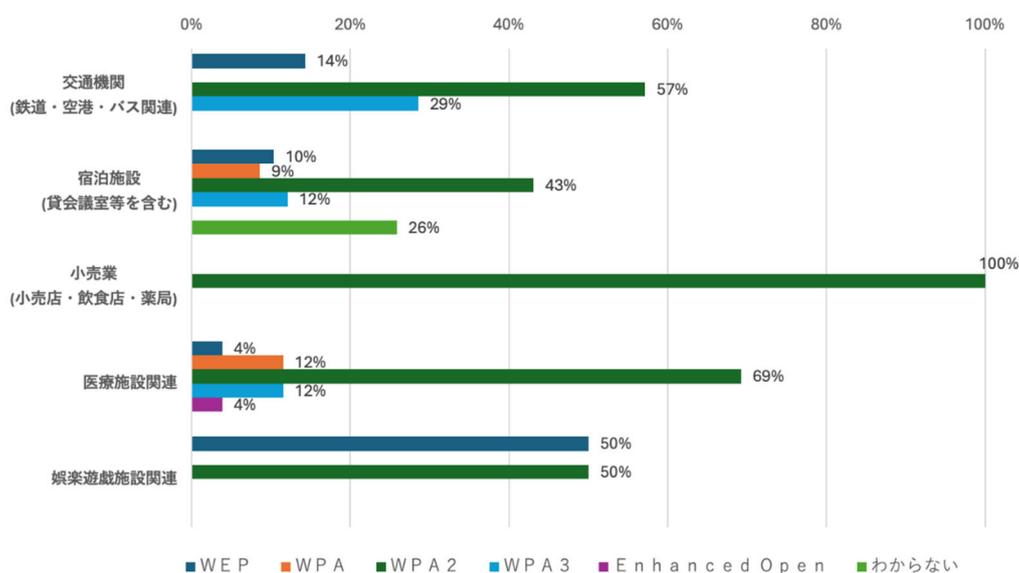
図表 2-2-46 無線 LAN サービスの暗号化 (Q9) (業種ベース)



⑦ 無線 LAN サービスの暗号化方式 (Q10)

暗号方式の危殆化により利用が禁止されている WEP は、交通機関、宿泊施設、娯楽遊戯施設関連で多く使われている。

図表 2-2-47 無線 LAN サービスの暗号化方式 (Q10) (業種ベース)

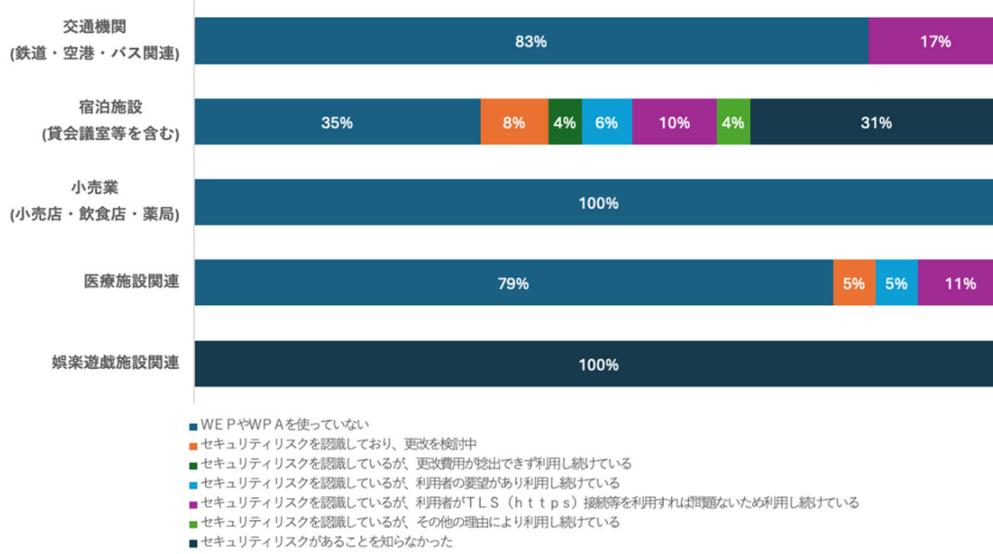


⑧ 暗号化方式のセキュリティリスク (Q11)

交通機関、小売業、医療施設は暗号化方式のセキュリティリスクに対する認識率が高く、宿泊施設はリスクに対する認識率が低いことが分かった。特に、娯楽遊戯施設

関連にいたっては認識率がきわめて低い。

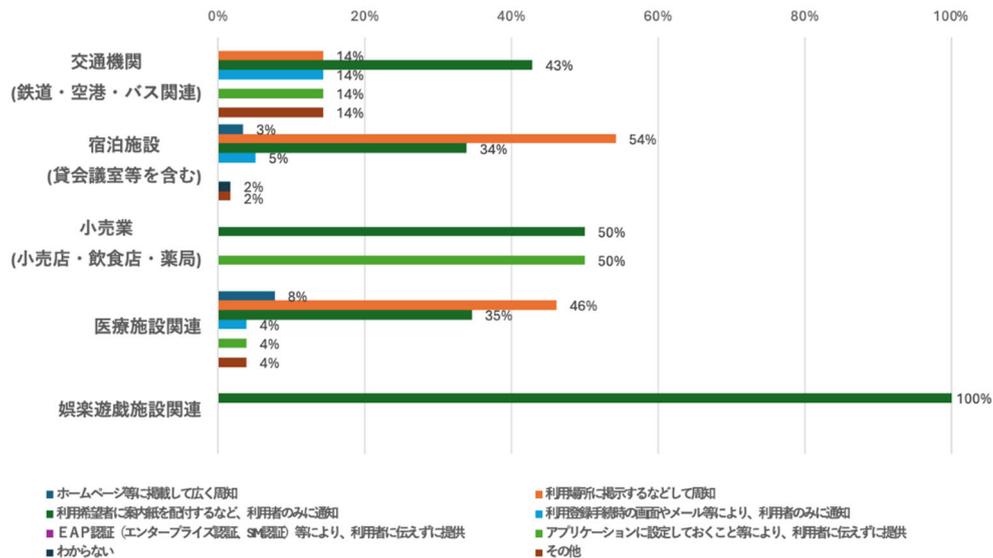
図表 2-2-48 暗号化方式のセキュリティリスク (Q11) (業種ベース)



⑨ 暗号鍵の利用者への伝達方法 (Q12)

宿泊施設や医療施設は「利用場所に掲示」または「案内紙を配布」する率が高い。
娯楽遊戯施設については「案内紙を配布」が全回答を占める。

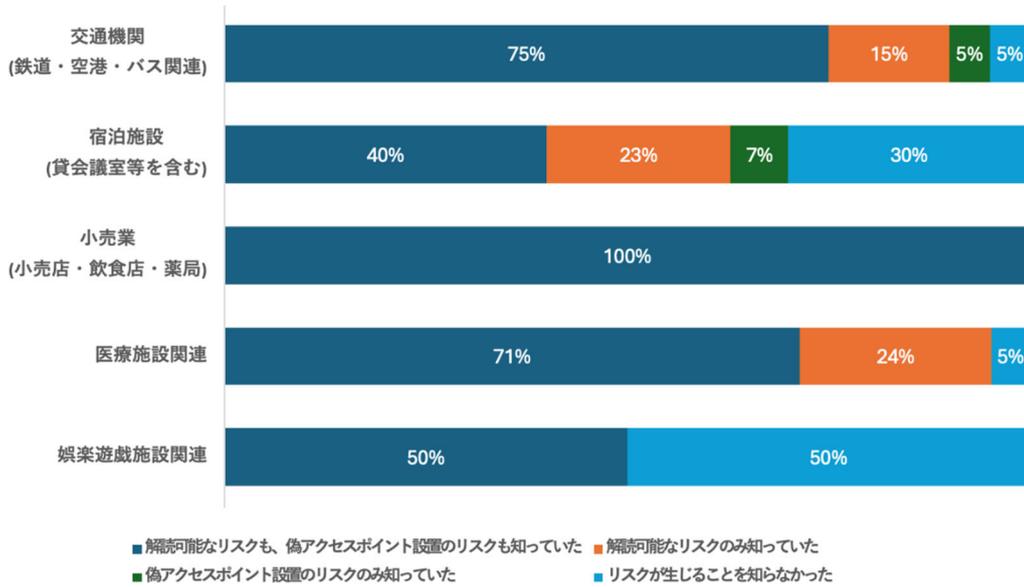
図表 2-2-49 暗号鍵の利用者への伝達方法 (Q12) (業種ベース)



⑩ セキュリティリスクに対する認識 (Q13)

宿泊施設は、他に比べその他のセキュリティリスクに対する認識率は低い。

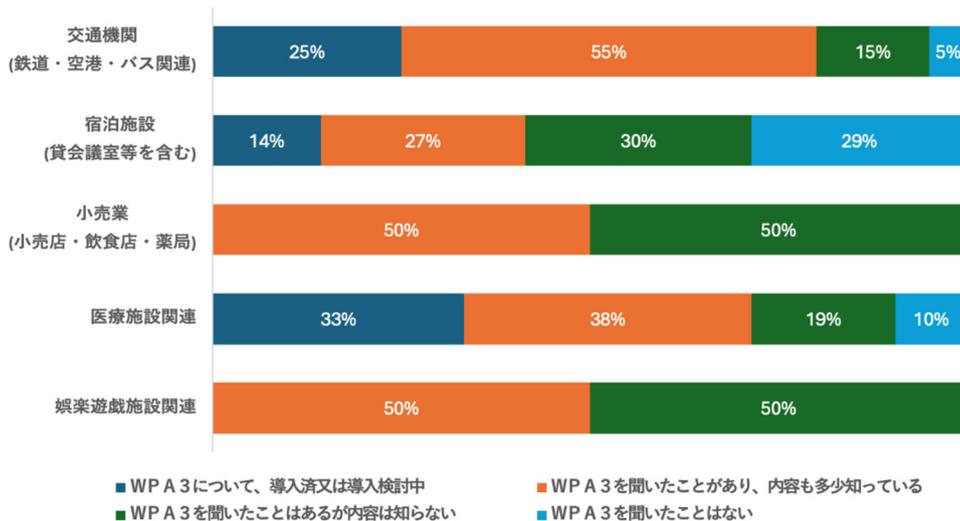
図表 2-2-50 セキュリティリスクに対する認識 (Q13) (業種ベース)



⑪ 新しい暗号化方式 (WPA3) (Q14)

宿泊施設、娯楽遊戯施設関連は他に比べ「WPA3」の認知度が低い。

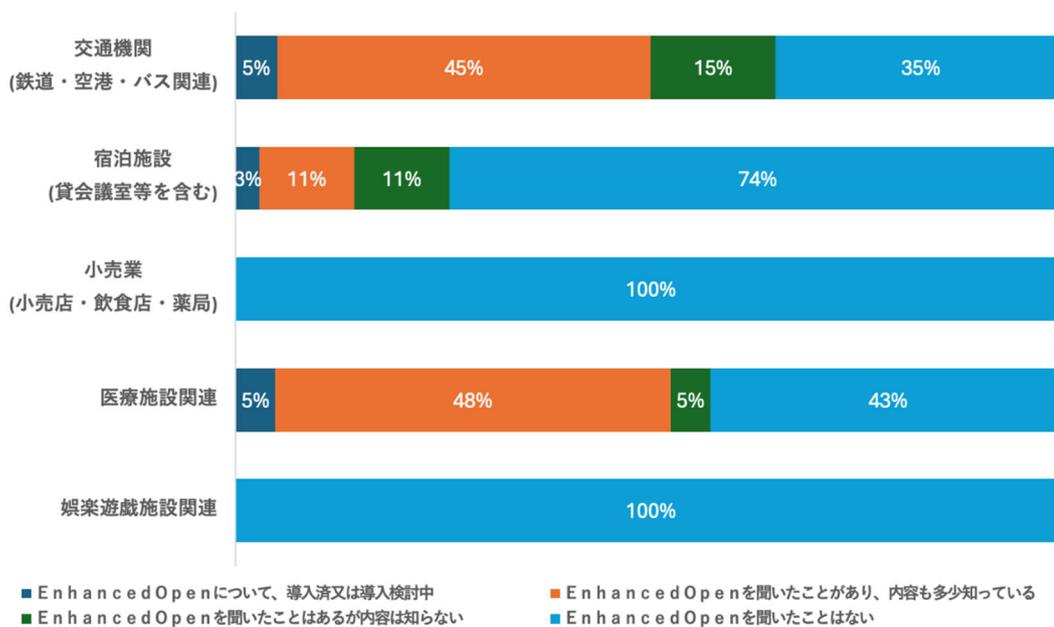
図表 2-2-51 新しい暗号化方式 (WPA3) (Q14) (業種ベース)



⑫ 新しい暗号化方式（Enhanced Open）（Q15）

宿泊施設、小売業、娯楽遊戯関連施設については「Enhanced Open」の認識率が低い。

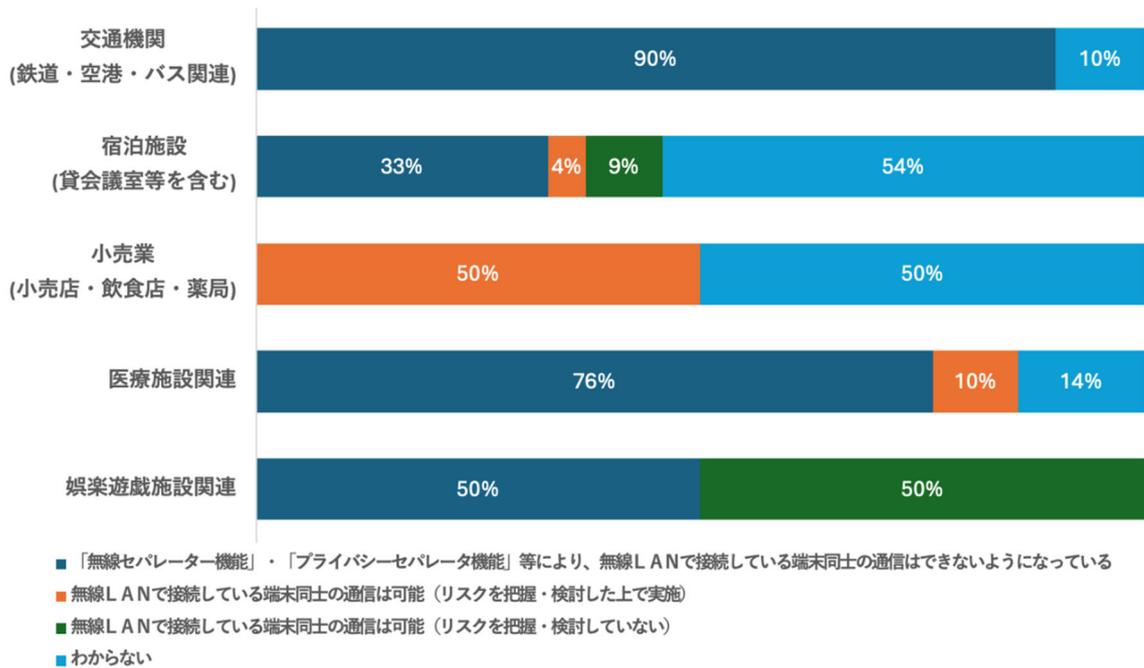
図表 2-2-52 新しい暗号化方式（Enhanced Open）（Q15）（業種ベース）



⑬ 端末同士の折り返し通信（Q16）

交通機関、医療施設関連の折り返し通信のリスクに対する認識率は極めて高い。

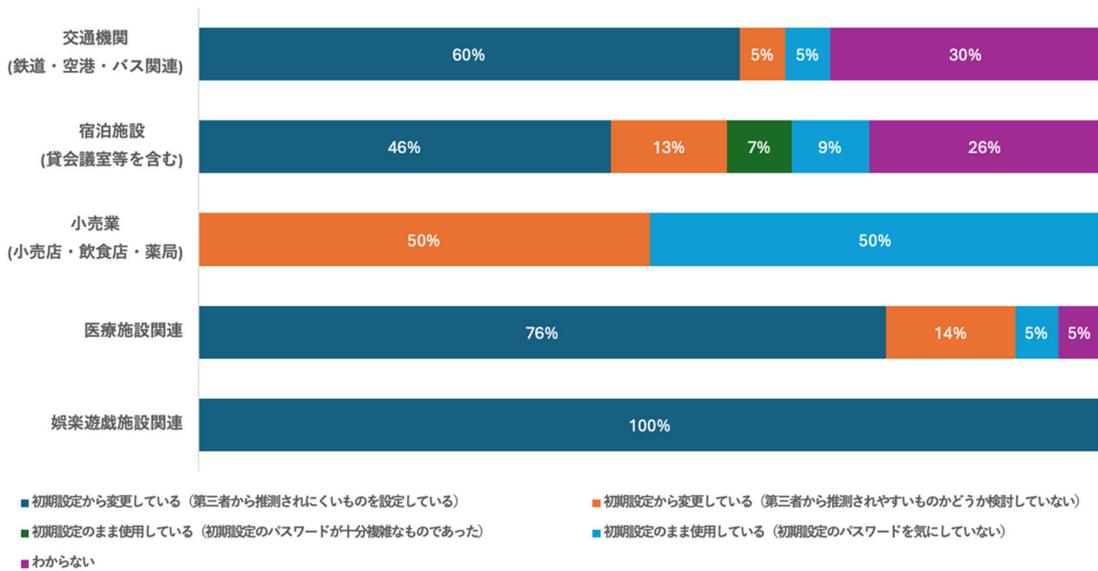
図表 2-2-53 端末同士の折り返し通信（Q16）（業種ベース）



⑭ 管理者パスワードの管理 (Q18)

パスワード管理について小売業の認知度が低い。

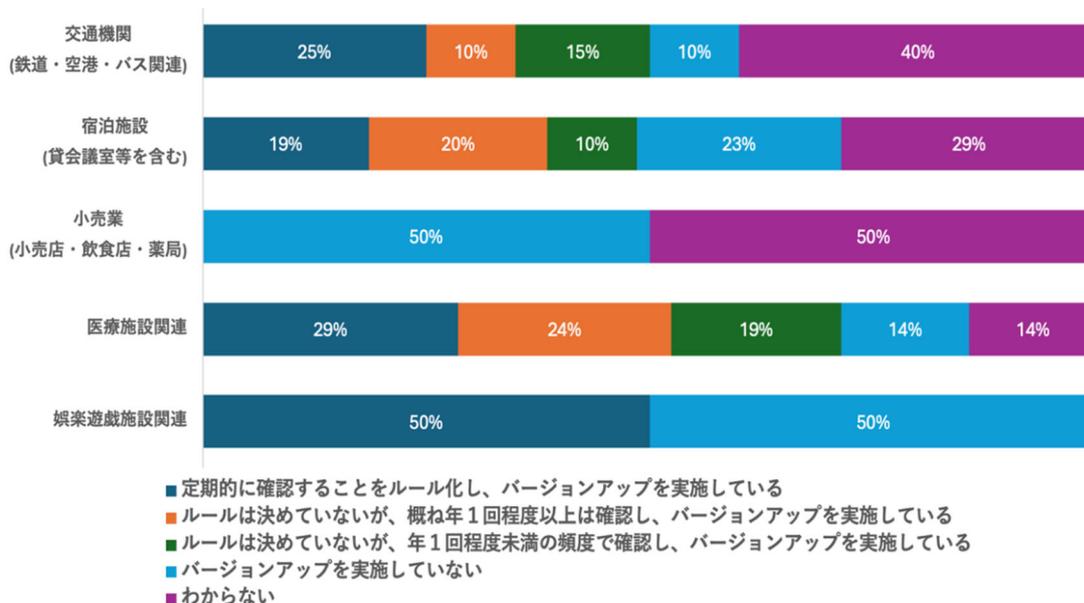
図表 2-2-54 管理者パスワードの管理 (Q18) (業種ベース)



⑮ ネットワーク機器のファームアップ (Q19)

小売業と娯楽遊戯施設関連は、ネットワーク機器のファームウェアのバージョンアップしていない率が高い。

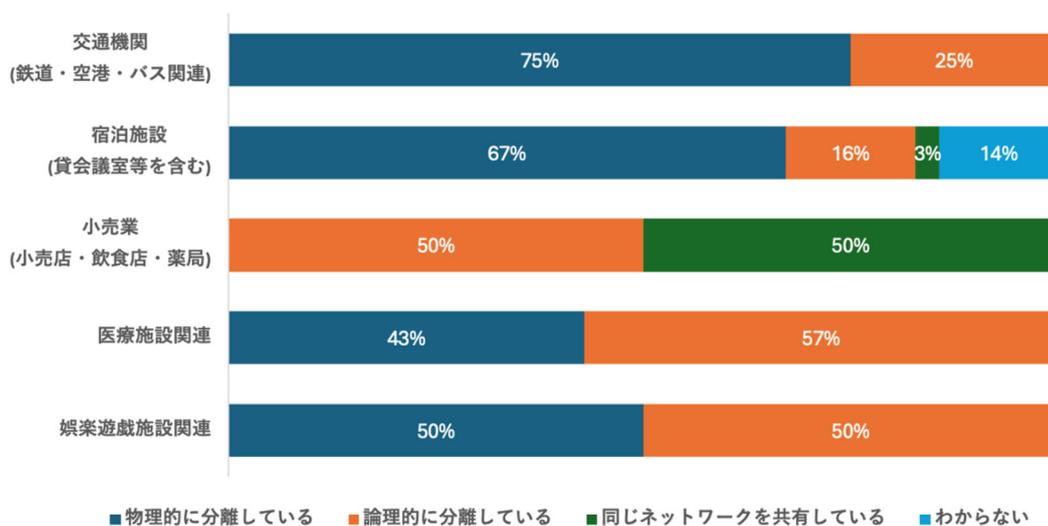
図表 2-2-55 ネットワーク機器のファームアップ (Q19) (業種ベース)



⑯ 業務用ネットワークとの分離 (Q20)

交通機関と宿泊施設は物理的に分離している率が高い。小売業、医療施設関連、娯楽遊戯施設関連は論理的に分離している率が高い。

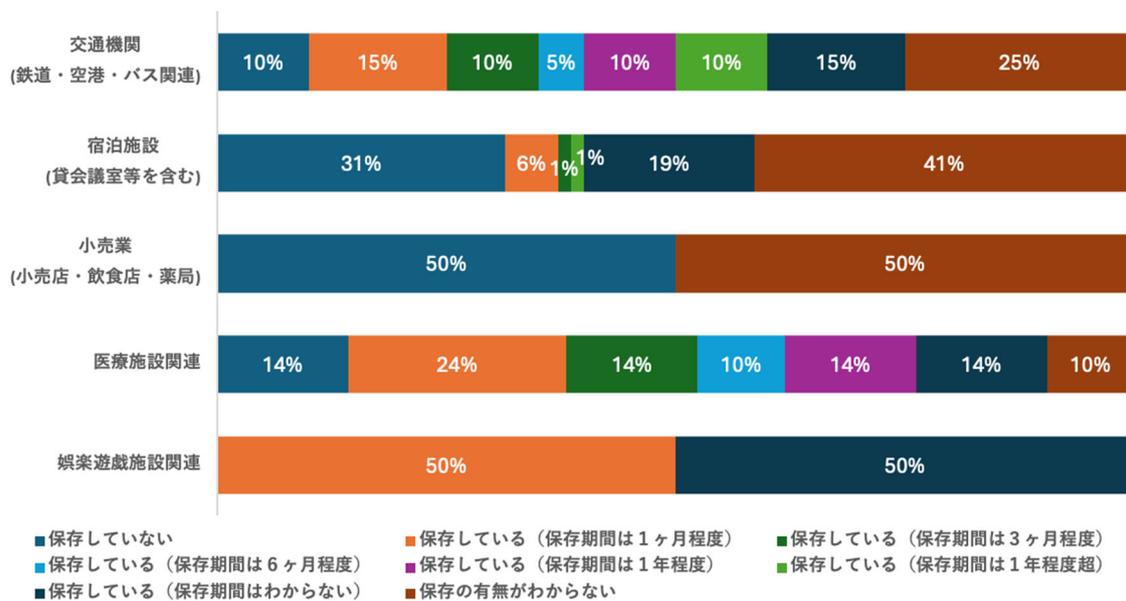
図表 2-2-56 業務用ネットワークとの分離 (Q20) (業種ベース)



⑰ アクセスログ（通信記録等）の保存（Q23）

宿泊施設や小売業では保存の有無を認識していない率が高い。

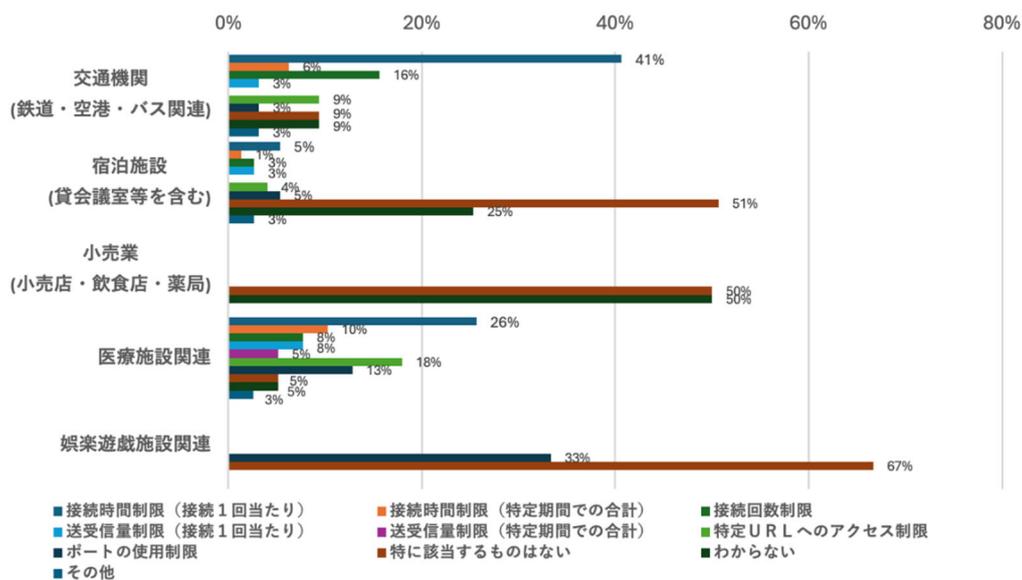
図表 2-2-57 アクセスログ（通信記録等）の保存（Q23）（業種ベース）



⑱ その他のセキュリティ対策 (Q25)

宿泊施設、小売業、娯楽遊戯施設関連は制限事項がない事例が多い。宿泊施設、娯楽遊戯施設関連についてはプライベート空間がほとんどであるためと思われる。

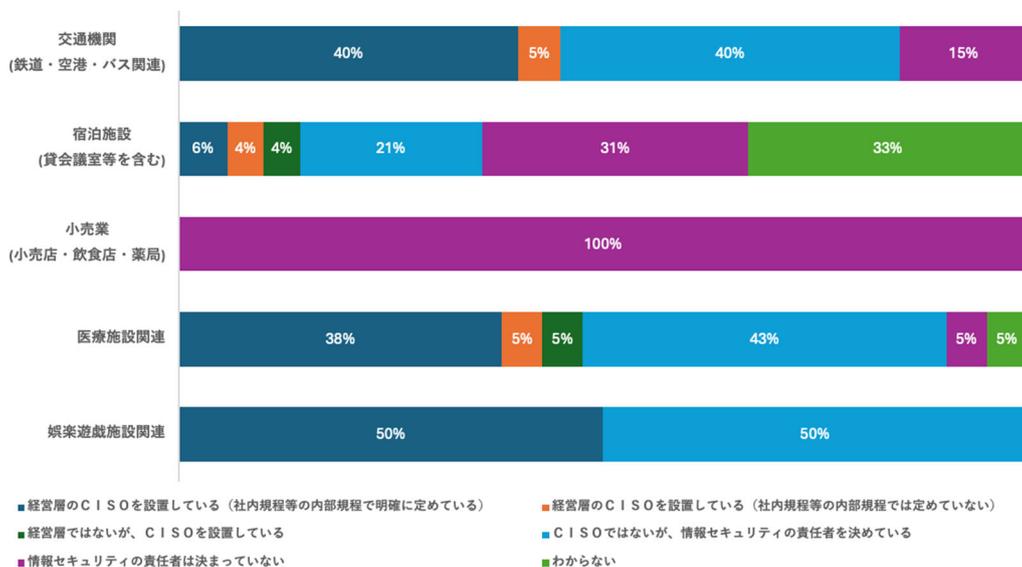
図表 2-2-58 その他のセキュリティ対策 (Q25) (業種ベース)



⑲ 情報セキュリティ責任者の設置 (Q26)

宿泊施設は「情報セキュリティの責任者が決まっていない」率が多い。小売業については「情報セキュリティの責任者が決まっていない」が全回答を占めた。

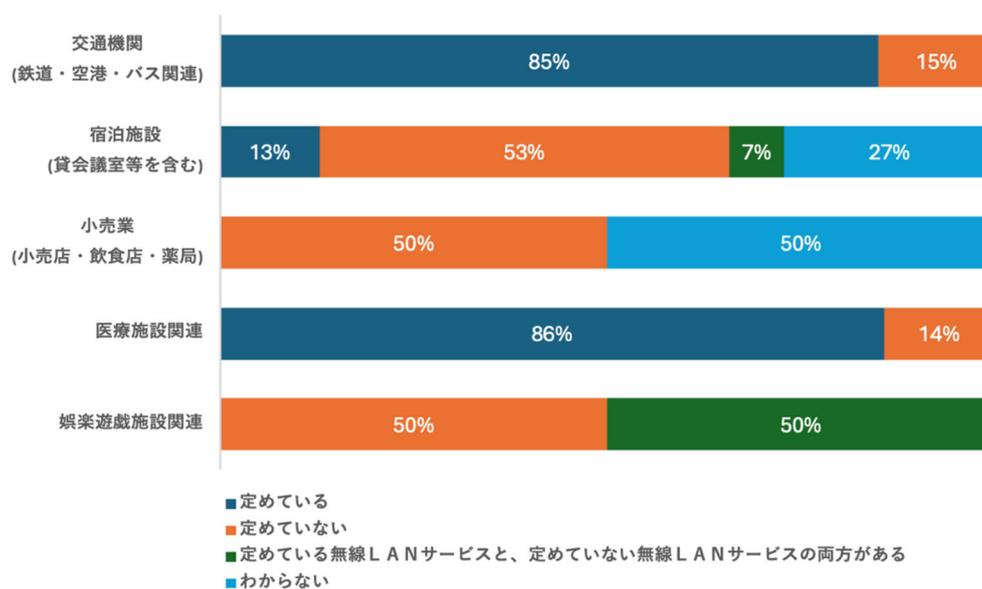
図表 2-2-59 セキュリティ責任者の設置 (Q26) (業種ベース)



⑳ 無線 LAN サービスの利用規約 (Q27)

宿泊施設、小売業、娯楽遊戯施設関連は、他の業種に比べ利用規約を定めていない率が高い。

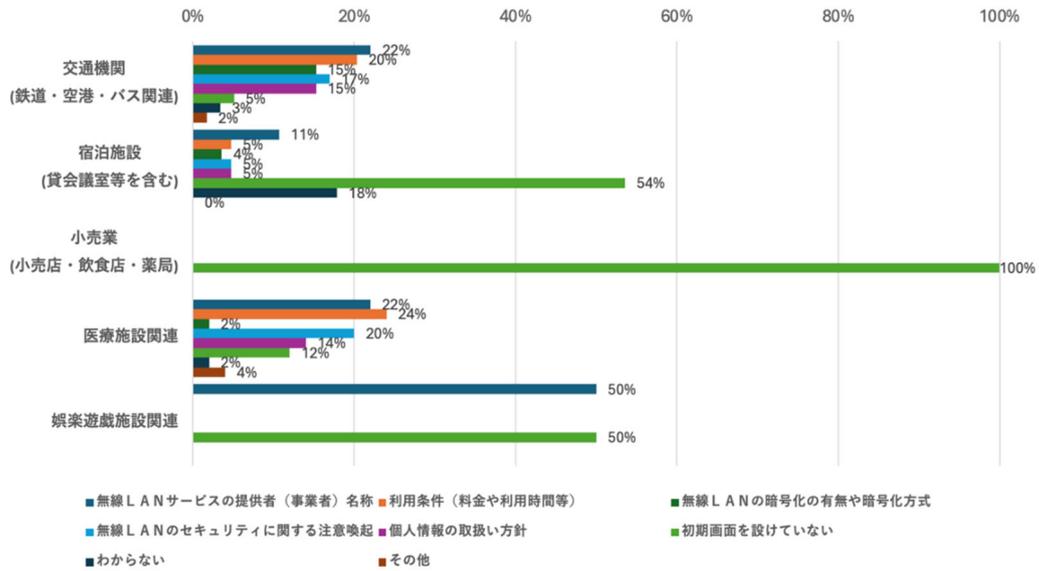
図表 2-2-60 無線 LAN サービスの利用規約 (Q27) (業種ベース)



㉑ 無線 LAN サービスの初期画面 (Q28)

宿泊施設、小売業、娯楽遊戯施設関連は、他の業種に比べ、初期画面を設けていない率が高い。小売業は全回答を占めた。

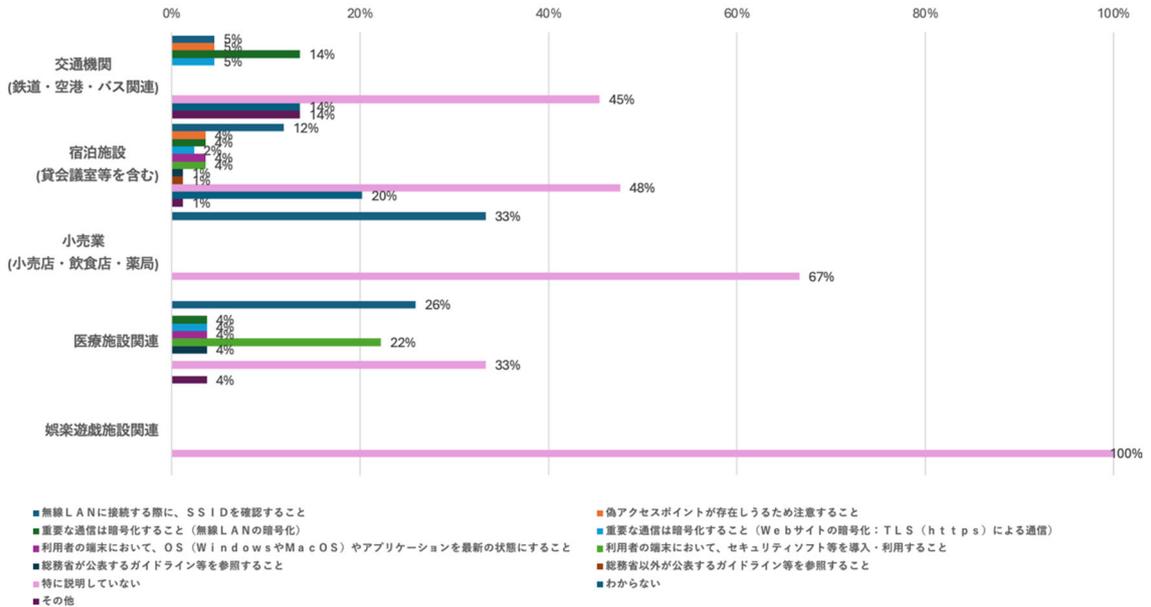
図表 2-2-61 無線 LAN サービスの初期画面 (Q28) (業種ベース)



② セキュリティに関する注意喚起 (Q29)

医療施設関連は、セキュリティに関する注意喚起をしている率が高い。一方で小売業、娯楽遊戯施設関連は注意喚起をしていない率が高い。

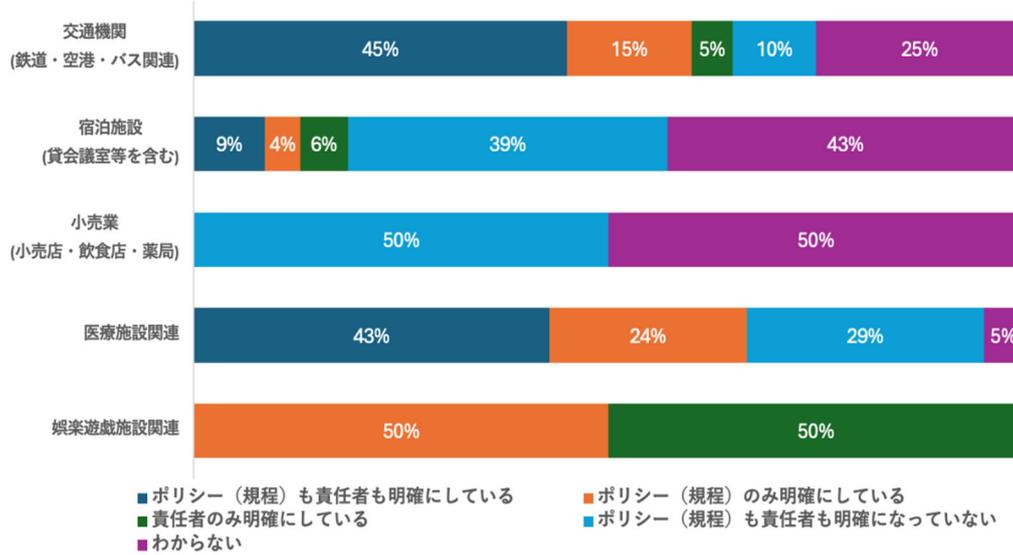
図表 2-2-62 セキュリティに関する注意喚起 (Q29) (業種ベース)



②③ 利用者情報のデータ保護 (Q31)

宿泊施設、小売業は、他の業種に比べ、利用者情報の保護規定やデータ保護責任者が不明確な事例が多い。「わからない」の回答もそれぞれ半数近くを占めている。

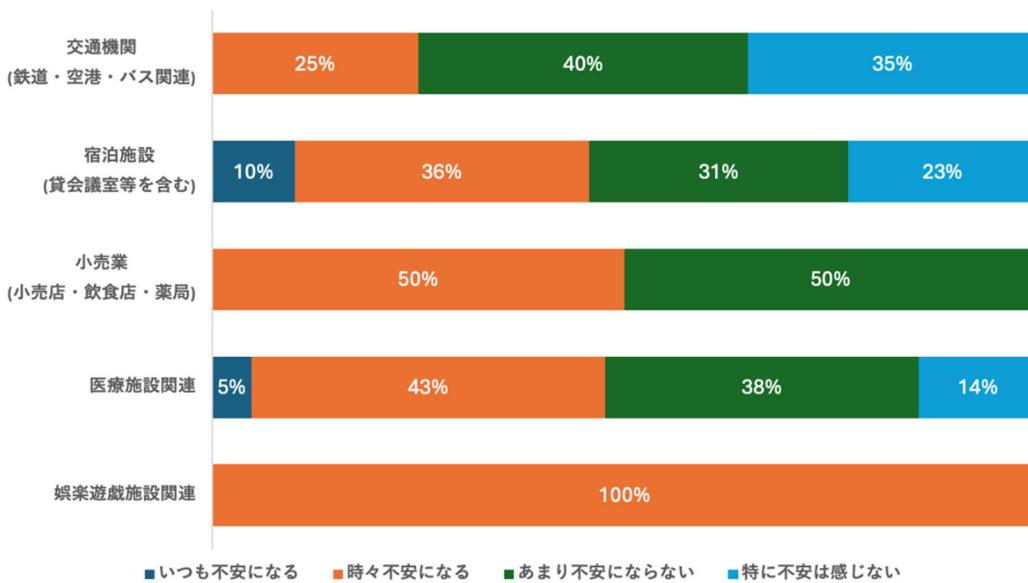
図表 2-2-63 利用者情報のデータ保護 (Q31) (業種ベース)



②④ サービスのセキュリティへの不安 (Q32)

交通機関以外はセキュリティに対する不安を持っている率が高いことがわかる。

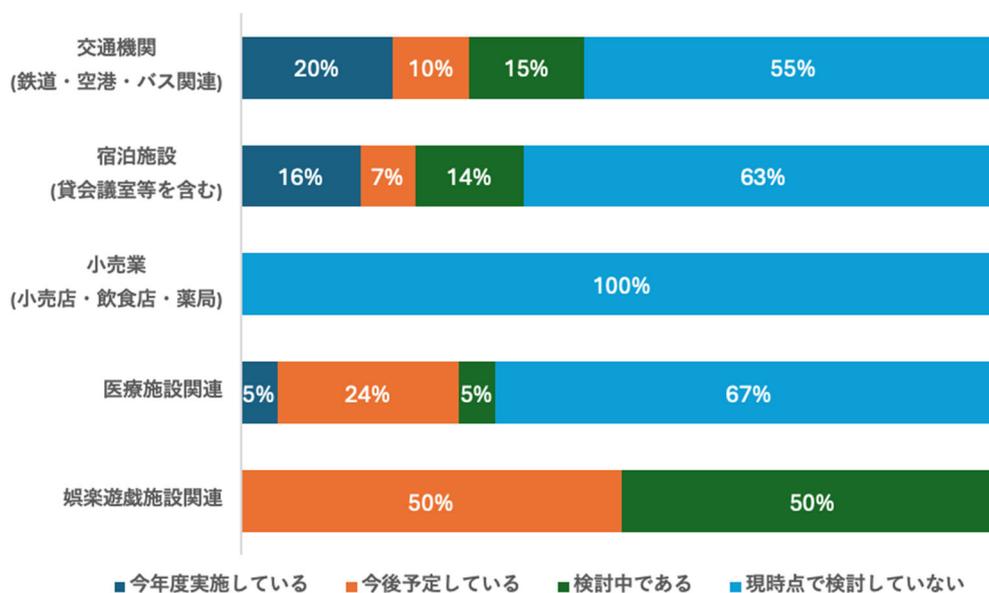
図表 2-2-64 サービスのセキュリティへの不安 (Q32) (業種ベース)



②⑤ サービスの設備拡充や更改計画（Q33）

交通機関、宿泊施設、娯楽遊戯施設関連は整備更改等を実施あるいは計画している事例が多い（おそらく古くからサービスを開始している事例が多いため）。医療施設関連についても3割以上が整備更改等を実施あるいは計画している。

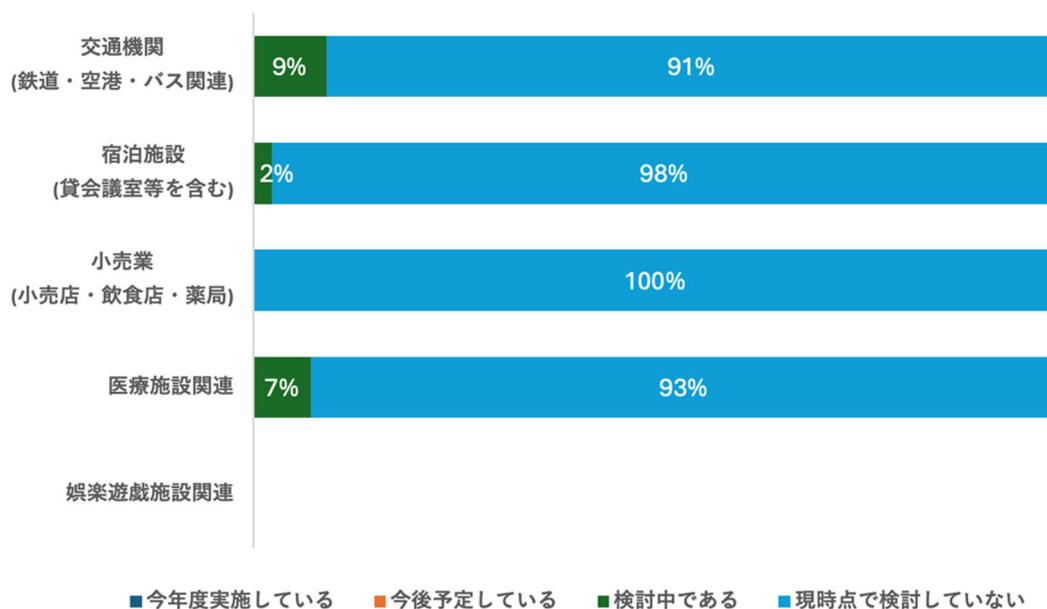
図表 2-2-65 サービスの設備拡充や更改計画（Q33）（業種ベース）



②⑥ サービスのセキュリティ強化計画（Q35）

どの業界もほとんどがセキュリティ強化計画を現時点で検討していない。

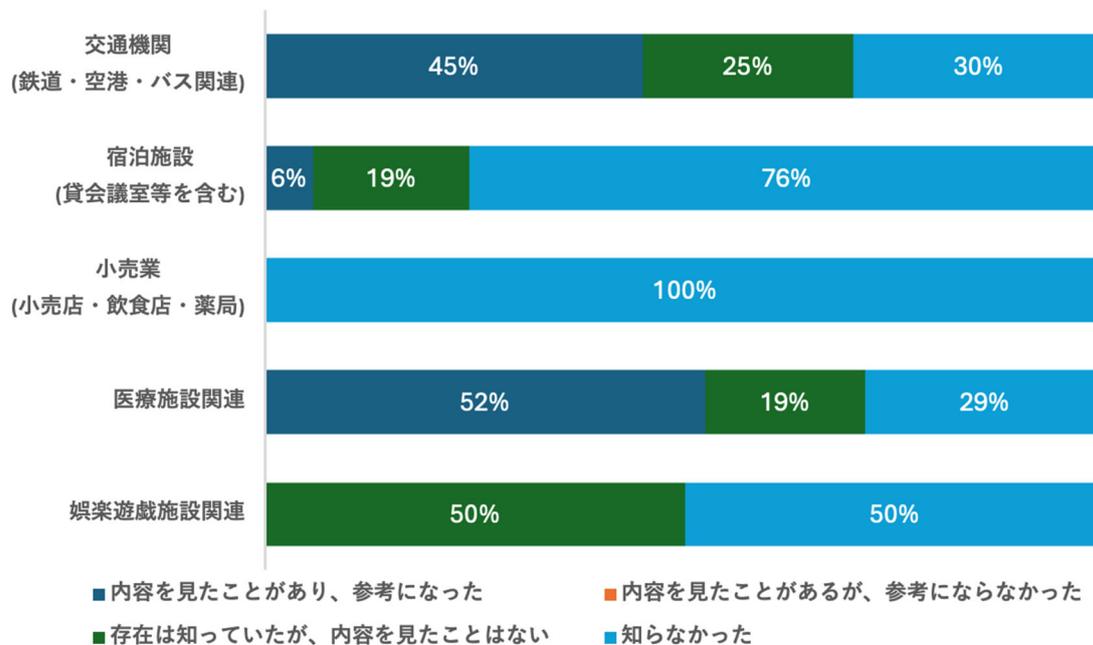
図表 2-2-66 サービスのセキュリティ強化計画 (Q35) (業種ベース)



⑳ セキュリティ対策の手引き (Q40)

交通機関や医療施設は「手引き」を参考にしている率が多い。

図表 2-2-67 セキュリティ対策の手引き (Q40) (業種ベース)



(7) 情報セキュリティ責任者の設定の有無による結果の差異について

Q22 の設問（セキュリティ責任者を設定）をベースに、自治体データを対象として解析を本年も行った。

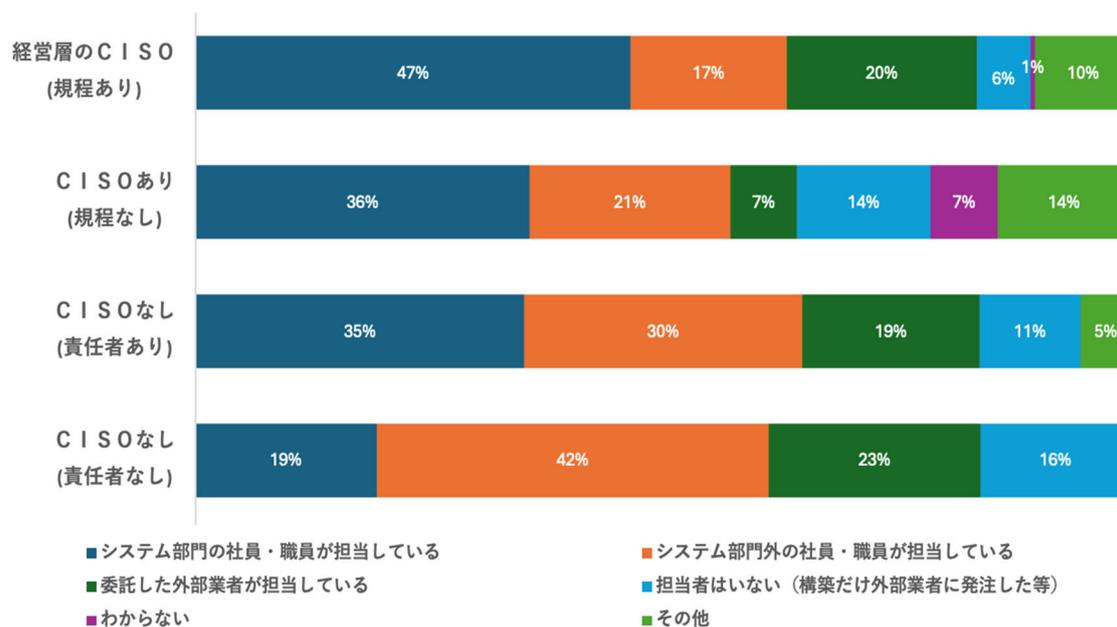
回答には以下のような特徴がみられた。

- セキュリティ責任者の設置は、全般的に、セキュリティの向上をもたらしていることがわかる。セキュリティリスクに対する認知率も高い傾向がみられる。
- また、新技術の認知率も高く、導入に対して前向きであることが分かった。

① 無線 LAN サービスの運用管理 (Q6)

セキュリティ責任者が設置されている方がサービスの運用管理をしている率が高く、また、経営層の責任者が設置されている方が、内部のシステム部門で運用管理をしている率が高い。

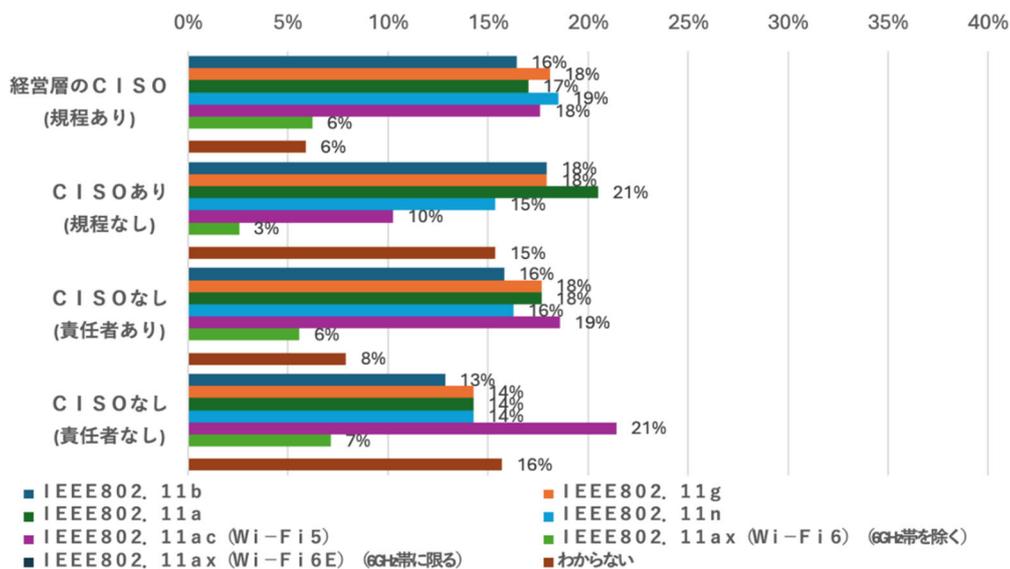
図表 2-2-68 無線 LAN サービスの運用管理 (Q6) (管理者有無ベース)



② 無線 LAN サービスの伝送規格 (Q8)

セキュリティ責任者が設置されている方が、「わからない」との回答が少ない。

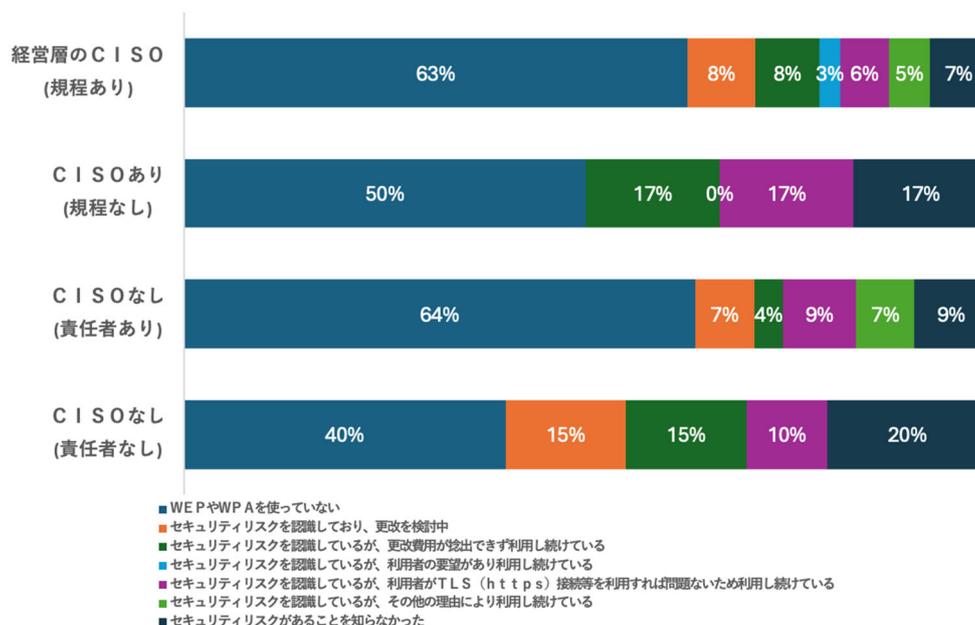
図表 2-2-69 無線 LAN サービスの伝送規格 (Q8) (管理者有無ベース)



③ 暗号化方式のセキュリティリスク (Q11)

セキュリティ責任者が設置されている方が非推奨暗号化方式である (WEP/WPA) を利用していない率が高い。

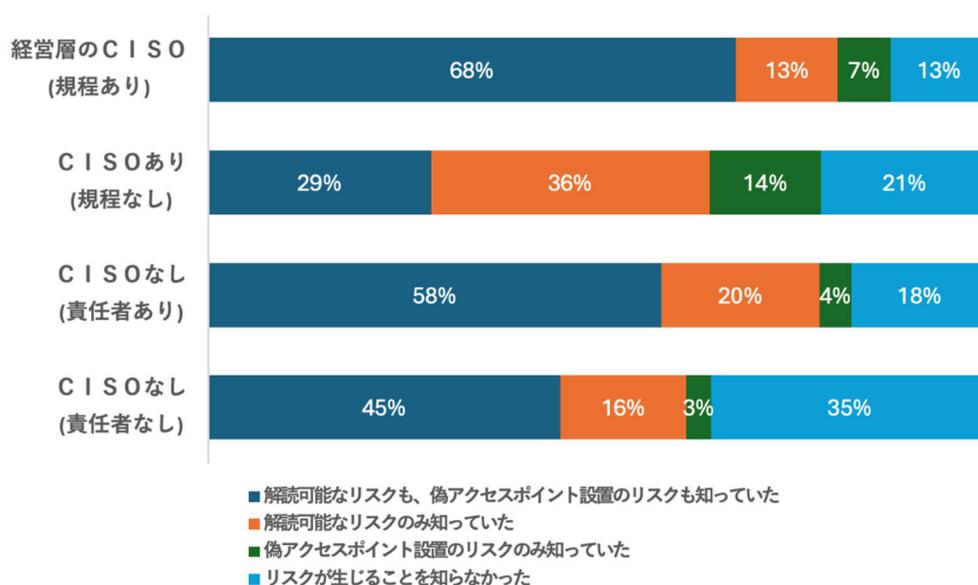
図表 2-2-70 暗号化方式のセキュリティリスク (Q11) (管理者有無ベース)



④ セキュリティリスクに対する認識 (Q13)

セキュリティ責任者を設置している方が、セキュリティリスクの認識率は高い。さらに経営層の責任者を設置しているところは、それ以上に高い数値が出ている。

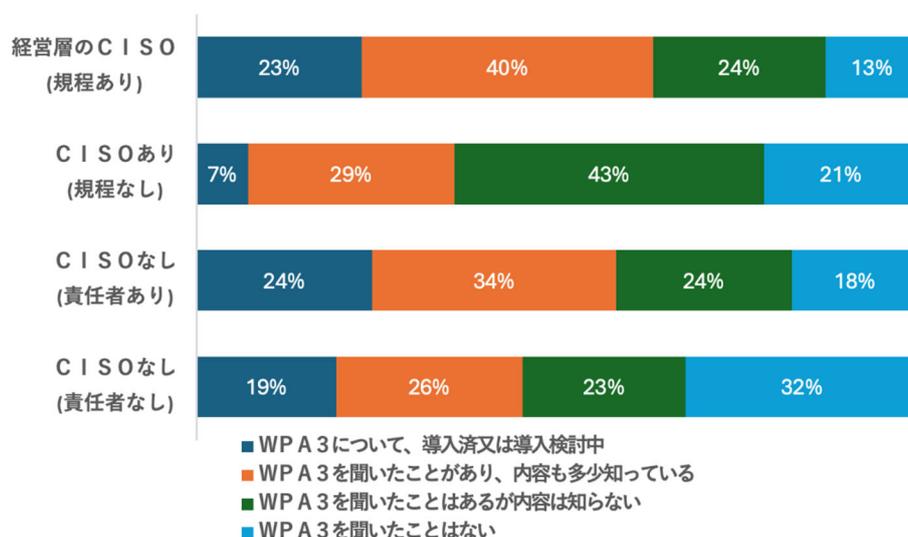
図表 2-2-71 セキュリティリスクに対する認識 (Q13) (管理者有無ベース)



⑤ 新しい暗号化方式 (WPA3) (Q14)

セキュリティ責任者を設置している場合は、設置していないものと比べて、新技術 (WPA3) の認識率は高い。さらに経営層の責任者を設置しているところは、それ以上に比率が高い。

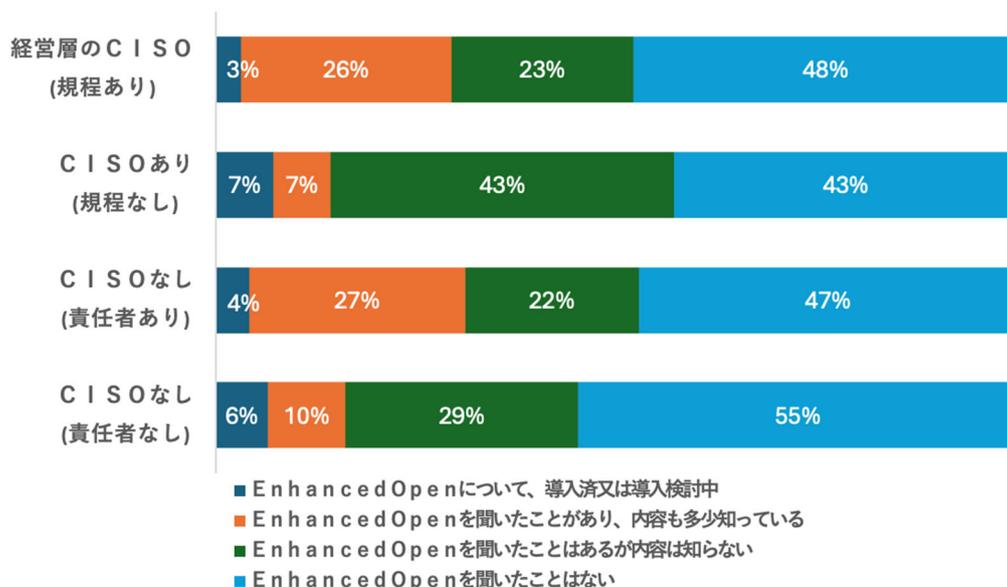
図表 2-2-72 新しい暗号化方式 (WPA3) (Q14) (管理者有無ベース)



⑥ 新しい暗号化方式 (Enhanced Open) (Q15)

セキュリティ責任者を設置している場合は、設置していないものと比べて、新技術 (Enhanced Open) の認識率は高い。さらに経営層の責任者を設置しているところは、それ以上に比率が高い。

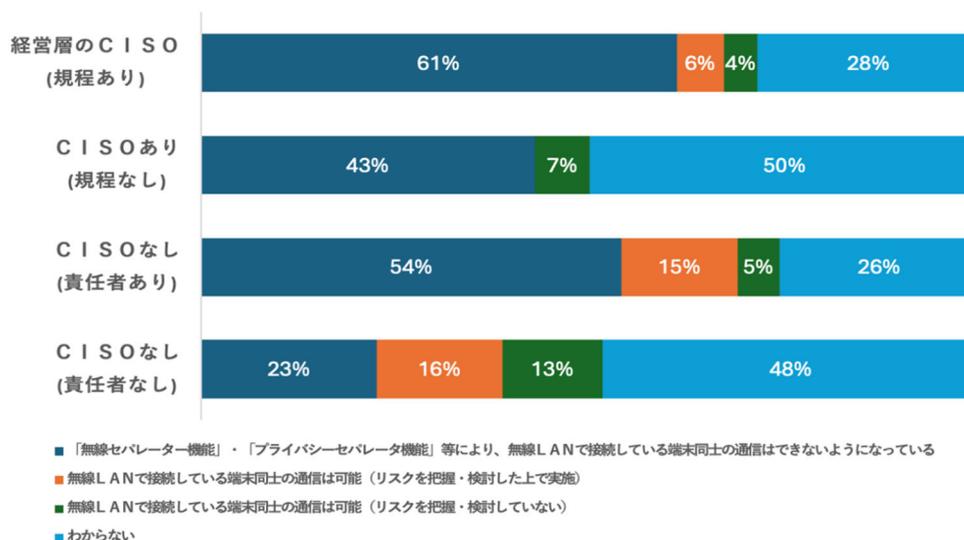
図表 2-2-73 新しい暗号化方式 (Enhanced Open) (Q15) (管理者有無ベース)



⑦ 端末同士の折り返し通信 (Q16)

セキュリティ責任者を設置しているものは、「折り返し通信」のリスクに対する認識率が高い。

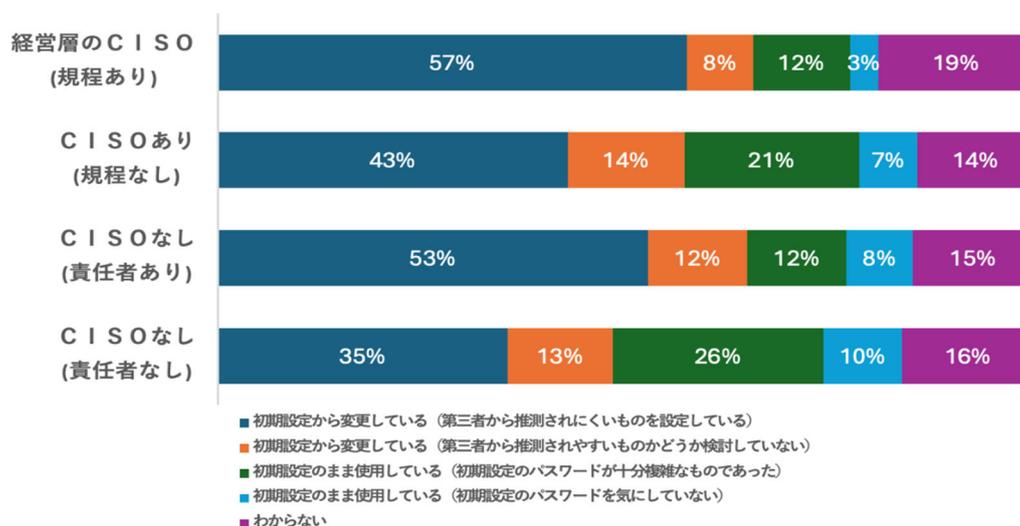
図表 2-2-74 端末同士の折り返し通信 (Q16) (管理者有無ベース)



⑧ 管理者パスワードの管理 (Q18)

セキュリティ責任者を設置しているものは、パスワードの管理が適切に行われている率が高い。特に、責任者を設置していないところは、パスワードを「初期設定のまま使用している」率が高い。

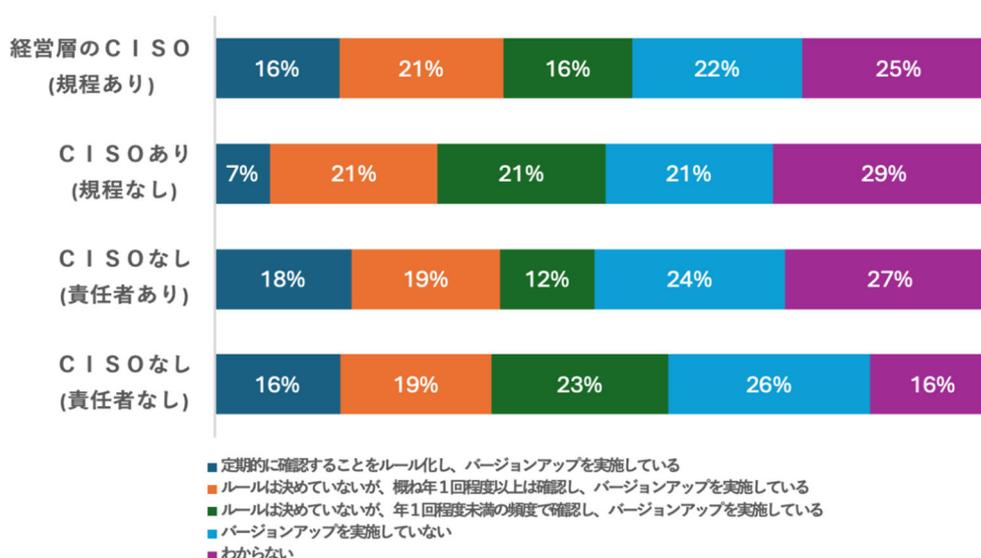
図表 2-2-75 管理者パスワードの管理 (Q18) (管理者有無ベース)



⑨ ネットワーク機器のファームアップ (Q19)

「バージョンアップを実施している」比率はセキュリティ責任者の設置有無で大きな差はなかった。

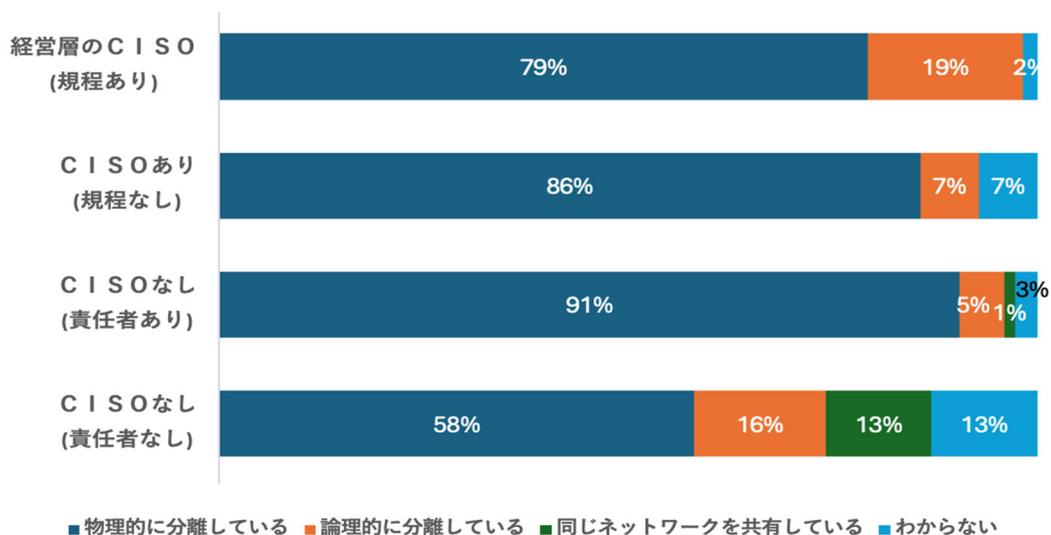
図表 2-2-76 ネットワーク機器のファームアップ (Q19) (管理者有無ベース)



⑩ 業務用ネットワークとの分離 (Q20)

セキュリティ責任者を設置しているものはネットワークを物理的に分離している率が高かった。また、同一ネットワークを共用で使っている率はネットワーク責任者を設置していないものが高い率を示している。

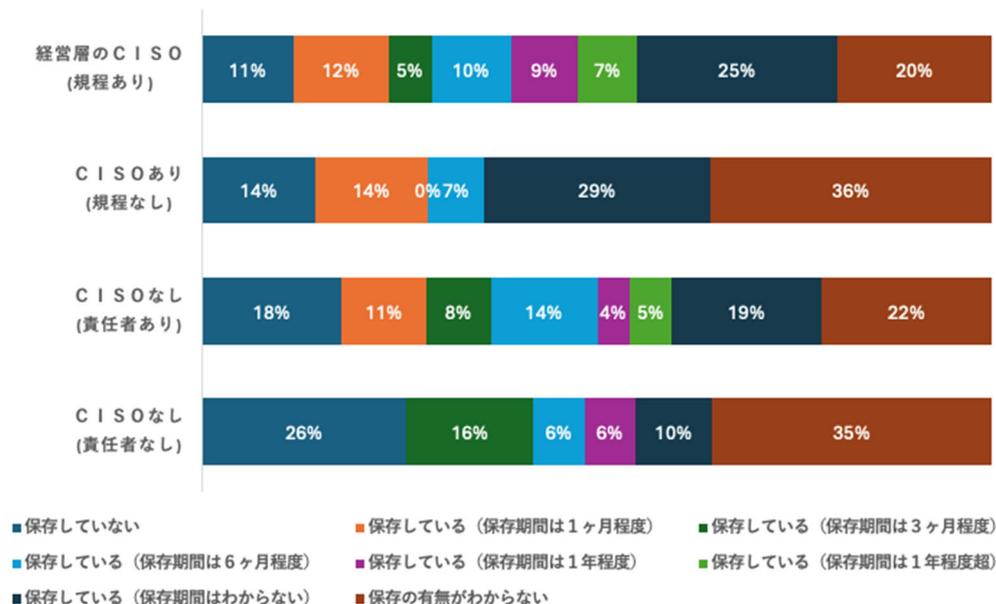
図表 2-2-77 業務用ネットワークとの分離 (Q20) (管理者有無ベース)



⑪ アクセスログ (通信記録等) の保存 (Q23)

セキュリティ責任者を設置していないものは、アクセスログ (通信記録等) を「保存していない」比率が極めて高い。

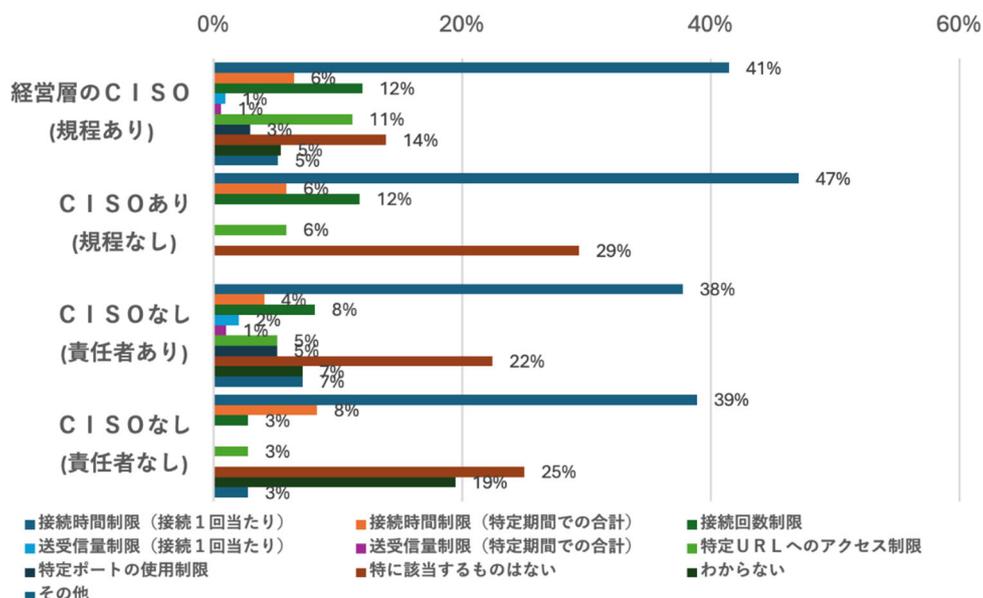
図表 2-2-78 アクセスログ（通信記録等）の保存（Q23）（管理者有無ベース）



⑫ その他のセキュリティ対策（Q25）

セキュリティ責任者を設置していないものは、制限事項などのセキュリティ対策について「わからない」と回答する率が高い。

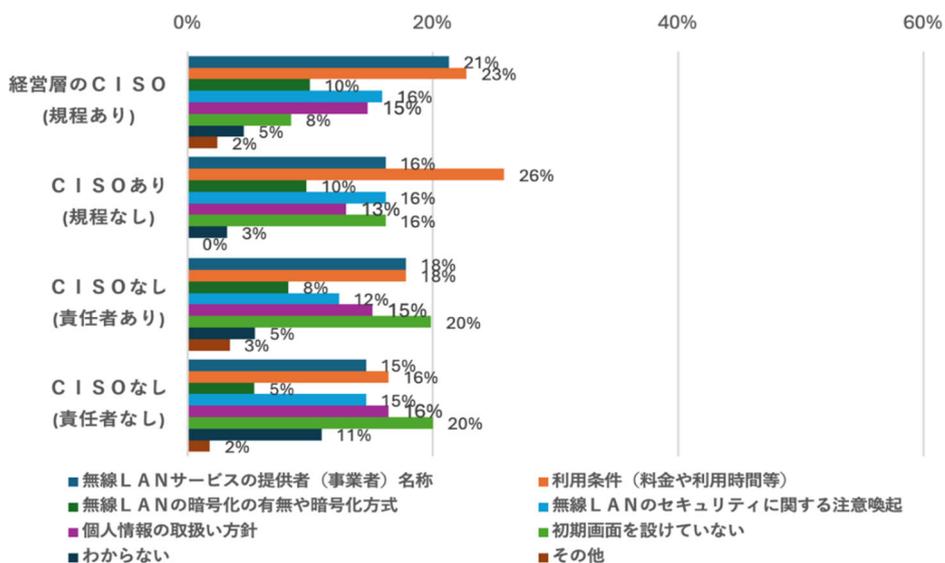
図表 2-2-79 その他のセキュリティ対策（Q25）（管理者有無ベース）



⑬ 無線 LAN サービスの初期画面 (Q28)

セキュリティ責任者を設置しているものは、初期画面を設けている率が高い。

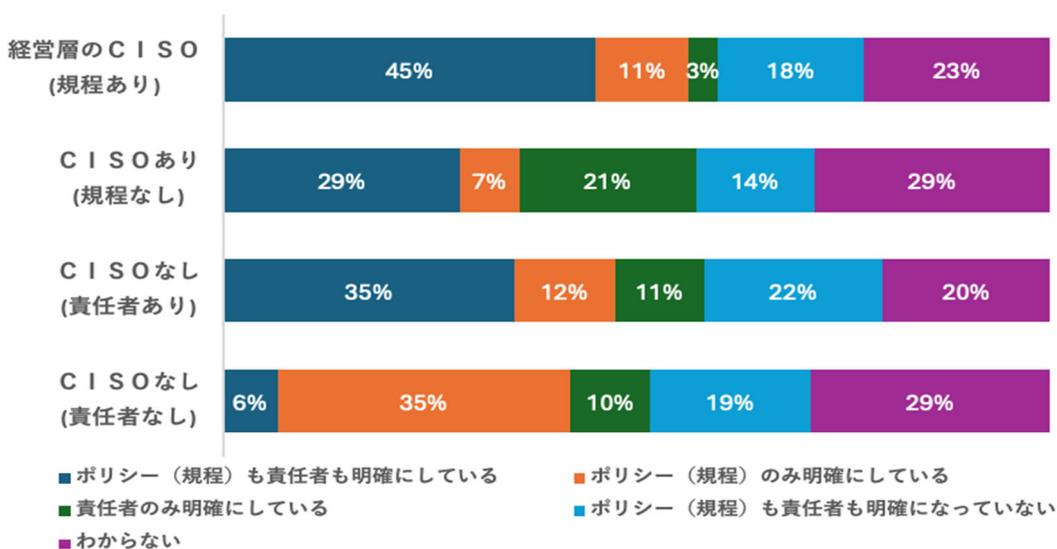
図表 2-2-80 無線 LAN サービスの初期画面 (Q28) (管理者有無ベース)



⑭ 利用者情報のデータ保護 (Q31)

セキュリティ責任者を設置しているものは、利用者情報のデータ (個人情報等) に対しても適切に対応している率が高い。

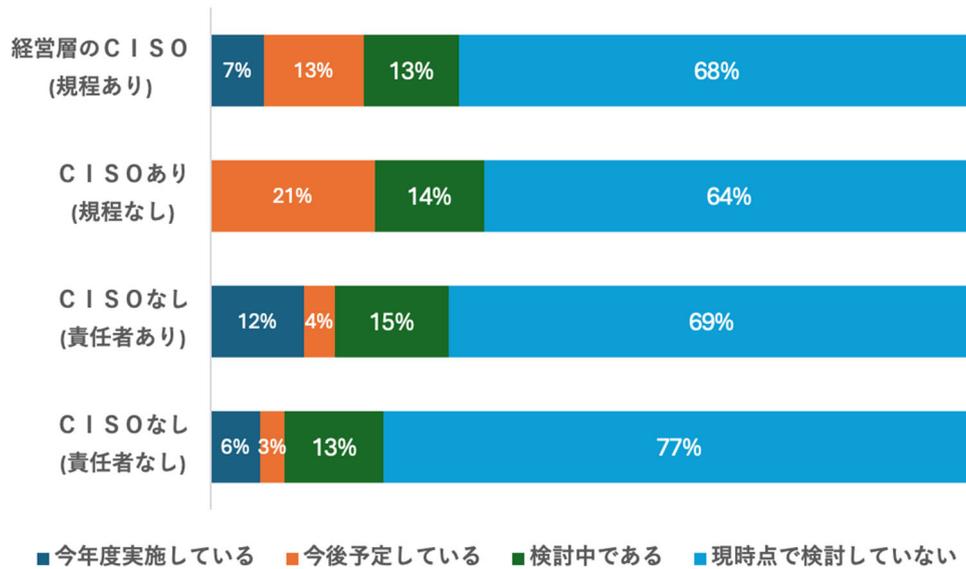
図表 2-2-81 利用者情報のデータ保護 (Q31) (管理者有無ベース)



⑮ サービスの設備拡充や更改計画 (Q33)

セキュリティ責任者を設置しているものは、整備更改等を実施あるいは計画している率が高い。

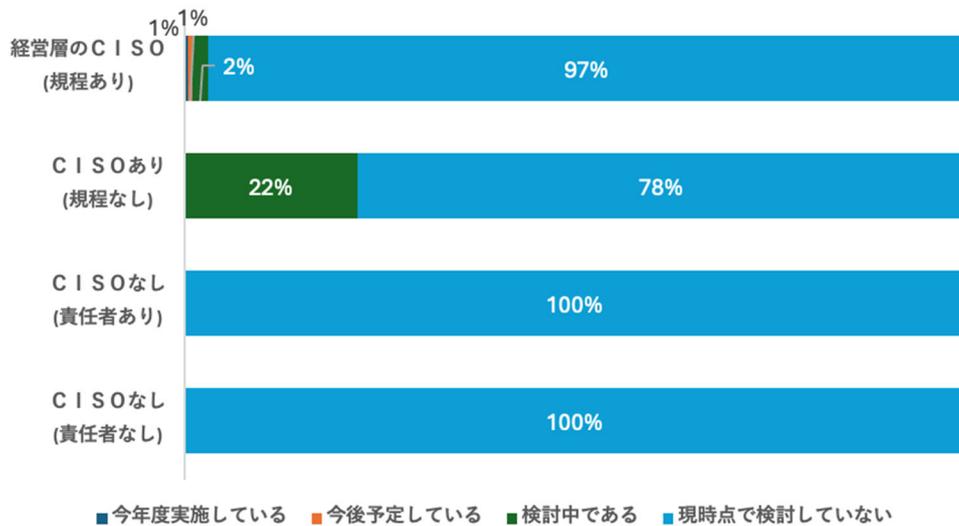
図表 2-2-82 サービスの設備拡充や更改計画 (Q33) (管理者有無ベース)



⑯ サービスのセキュリティ強化計画 (Q35)

セキュリティ責任者を設置しているところは、セキュリティの強化等の実施あるいは計画している率が高い。

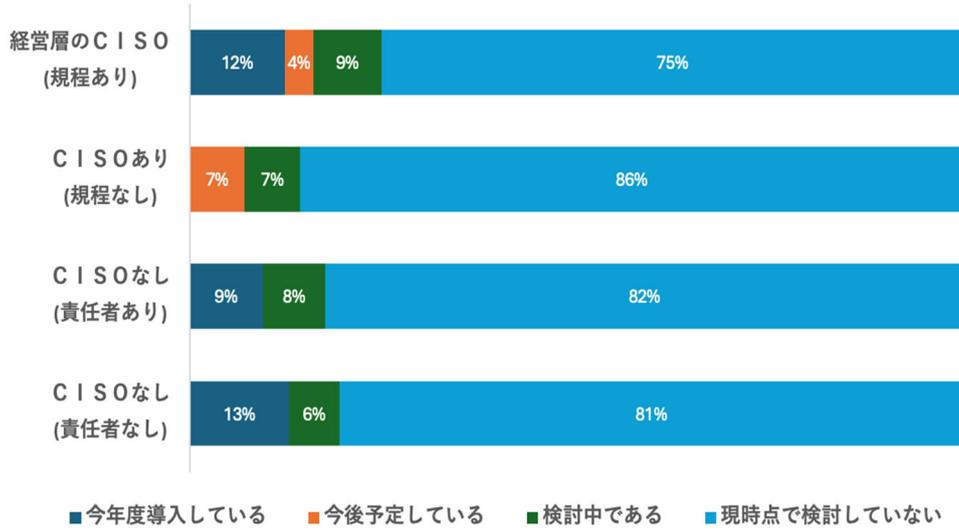
図表 2-2-83 サービスのセキュリティ強化計画 (Q35) (管理者有無ベース)



⑰ Wi-Fi 6 の導入予定 (Q37)

経営層のセキュリティ責任者がいる場合、Wi-Fi 6 の導入を検討している率が高い。

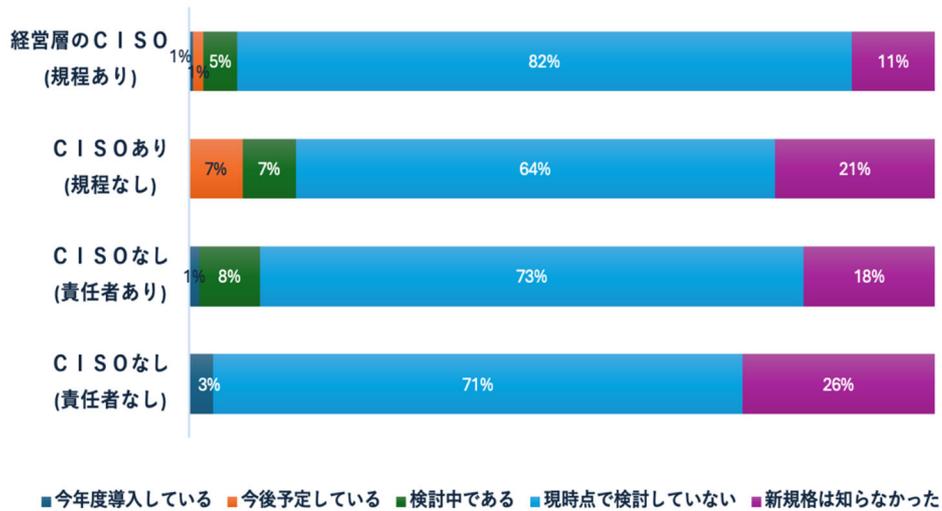
図表 2-2-84 Wi-Fi 6 の導入予定 (Q37) (管理者有無ベース)



⑱ Wi-Fi 6E の導入予定 (Q38)

セキュリティ責任者がいるものはWi-Fi 6E の導入を検討している率が高い。

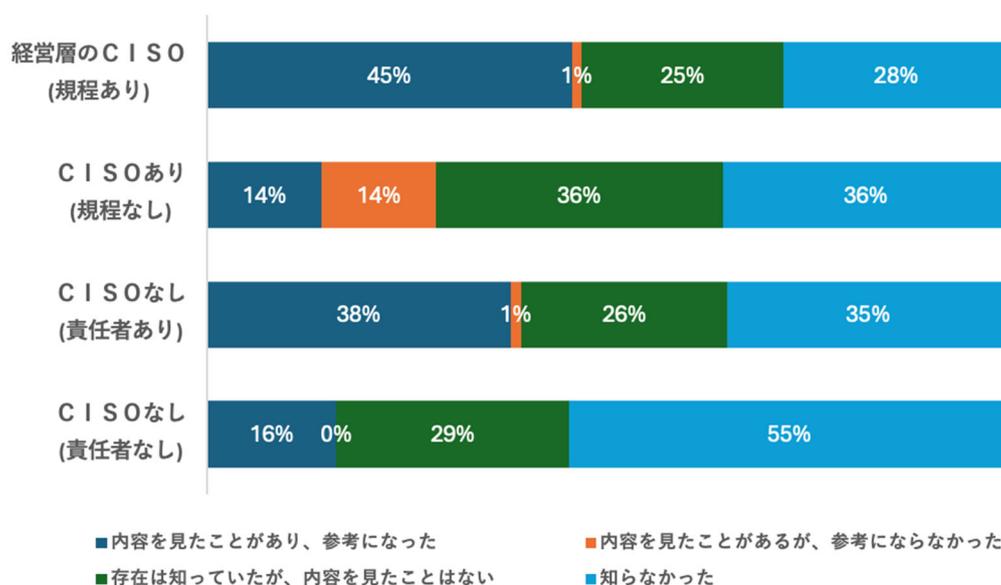
図表 2-2-85 Wi-Fi 6E の導入予定 (Q38) (管理者有無ベース)



⑩ セキュリティ対策の手引き (Q40)

情報セキュリティ責任者を設置しているものは、「手引き」の内容を知っている、あるいは参考になっている比率が高い。

図表 2-2-86 セキュリティ対策の手引き (Q40) (管理者有無ベース)



(8) その他

回答した地方自治体・企業等に対して、自由意見を求めたところ、次のご意見をいただきました。

- ・補助金制度があればすぐにでも導入したい (医療関連施設)
- ・最新規格のWi-Fi 導入事例などあれば情報をいただければと思います。(医療施設関連)
- ・もっと具体的なセキュリティ対策を公表してほしい。(宿泊施設)
- ・今後、ご利用者さまご自身のキャリア契約スマートフォンやご契約プロバイダのWi-Fi ルータ持ち歩きが当たり前になるなら基本的に、公衆や施設提供の無線 LAN サービスは行うべきでない。そこに事業者の努力を強いるのは間違いである。仕様もどんどん進化し、セキュリティが不安で犯罪の温床となるネット空間に変わりやすい。合わせていくためには設備改更やポリシー改更のエネルギーが継続してかかり過ぎで現実的でない。(宿泊施設)
- ・無線 LAN は、情報を盗まれても目で見えない。同じ周波数の電波で抑圧すると不通にでき、テロが簡単。無線 LAN サービスを介して、家でネットを禁止されている子供がいないだり、悪意を持った人がウイルスを撒いたりリスクが高いため導入していない。(自治体)

- ・無線 LAN サービス設備更新に係る補助制度を創設してほしい。(自治体)
- ・利便性とセキュリティは二律背反の関係だと思っていたが、Enhanced Open を使えばどちらも高レベルで両立できそうなので今後導入を検討したい。セキュリティ強化に有効なサービスがあることは知っているものの、やはり導入経費がネックとなる。また、経営の観点からは、インシデントが発生しない常況においてセキュリティ対策は単なるコストとなってしまうのでなかなか導入の理解が得られない。セキュリティ対策強化の補助金があると助かります。(自治体)
- ・法律で対策を義務化(罰則付き)しない限り、国全体としてのセキュリティは向上しない。Enhanced Open の利用も良いが、設置者に OpenRoaming の義務化が最善と思われる。(自治体)
- ・Q31(利用者情報のデータ保護)についてそもそも登録不要としているため、ポリシーも定めていない(自治体)
- ・広く利用いただくためにサービス提供にあたり、古い規格にしか対応していない機器でも利用可能なよう、新しい規格が出ても一定期間は古い規格でも接続できるよう設定しているため、セキュリティリスクが存在する。(自治体)
- ・次年度以降、こういった調査があれば、回答フォームや回答方法、回答期間の延長などをご検討いただけますと幸いです。(自治体)
- ・無線 LAN については、道の駅に設置しているが、都道府県が用意した無線 LAN を設置しているため規格等は不明。(自治体)
- ・市内ネットワーク環境は L G W A N 環境で閉鎖域(有線 LAN 使用)となっておりますが、L G W A N 環境を無線 LAN 化となった場合どんなことが必要となってくるか。インターネット環境の無線 LAN 双方について教えていただきたいところ。(自治体)
- ・病院等通信が制限される環境下で、提供されるフリー Wi-Fi での最低限のセキュリティ対策例など、現実に即した構成例を示してほしい。
利用者は一般的なスマホ利用を想定しているため、セキュリティよりも利便性を求めている。施設としては、ストレスを感じさせないことを優先したいので、セキュリティを堅牢にするより、ある程度は自己責任で提供した方がよいと考えている。(自治体)
- ・自団体での無線 LAN サービスを検討しているため、機器の更新や、設定・運用に関する情報を集められればと思います。(自治体)
- ・市が主導して無線 Wi-Fi 環境を整える事が望ましい。(自治体)
- ・セキュリティまで気にしたらボランティアではやってられない。(自治体)
- ・NTT の光ステーションと、Japan Connected-free Wi-Fi を利用している。(自治体)
- ・Wi-Fi 更新の補助金があれば教えてほしい。(自治体)
- ・設備の更新で利用できる補助金があれば教えてほしい。(自治体)
- ・無線 LAN に変更可能ですが、現在事務所内のみ有線で接続して使用しています。(自治体)

- ・本年度導入予定（自治体）
- ・情報化社会の中で、今後公設の無線 LAN サービスの需要が高まってくると想定はできるが、自治体が負担するコスト面や、無線 LAN を利用する方の情報を守るセキュリティ面の対策が非常に困難である。（自治体）
- ・要望として、公衆無線 LAN に対して、ペネトレーションテストのような監査を実施していただけると、その監査結果が今後の対応の検討材料になると考える。（自治体）

以上