

本調査結果は、総務省の「令和 6 年度 無線LANのセキュリティ確保のためのガイドライン等周知啓発コンテンツ策定検討に関する調査研究の請負」事業（受託者：NRIセキュアテクノロジーズ株式会社）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。

本資料に関する問い合わ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/](https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/)

## 第1章 無線 LAN 提供者に対するアンケート調査

### 1-1 調査の概要

#### (1) 調査の目的

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) 調査の対象

我が国の全ての市区町村（1,741 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 698 社抽出し、計 2,439 団体を対象にアンケート調査を実施した。

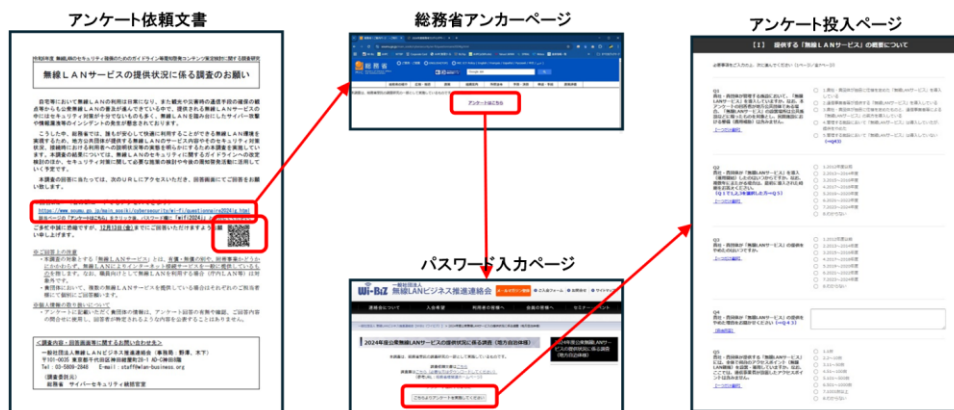
#### (3) 調査の方法

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、それぞれ別々に回答をしていただく旨の但し書きを行った。調査イメージを以下に示す。

図表 1-1 アンケート実施方法

- ・ 調査対象の地方自治体及び民間企業等に対して、アンケート依頼文書を郵送
- ・ 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
- ・ 本年より、いったん総務省のアンカーページにアクセスしてから、Wi-Biz のサーバを経由してアンケート投入ページに移動する形とした。



### 1-2 調査の時期

調査は以下のスケジュールにて実施した。

調査依頼発送：2024 年 11 月 11 日（月）

回答締め切り：2024 年 12 月 13 日（金）（回収率向上のため 12 月 20 日まで延長）

### 1-3 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、1,741 団体中 544 団体（前年は 850 団体）から回答があり、回答率は 31.2%（前年は 49.2%）であった。

企業等においては、698 社中 95 社（前年は 147 団体）から回答があり、回答率は 13.6%（前年は 20.6%）であった。前年と比較すると、大きく回答率が低下したが、原因の一つとして、本年より、依頼文書のみを送付し、調査票を同封しなかったことによるものと考えられる。

図表 1-2 提供者アンケート調査回答数

#### ・調査スケジュール

✓ 調査依頼発送:2024年11月11日(月)

✓ 回答締め切り:2024年12月13日(金)(回収率向上のため12月20日まで延長)

| 送付先団体 | 送付先分類  | 2024年度 |      | 2023年度 |      |
|-------|--------|--------|------|--------|------|
|       |        | 回答数    | 送付数  | 回答数    | 送付数  |
| 自治体   | 全自治体   | 544    | 1741 | 850    | 1726 |
| 企業    | 交通機関   | 20     | 75   | 29     | 77   |
|       | 宿泊施設等  | 40     | 426  | 74     | 436  |
|       | 小売業    | 8      | 78   | 7      | 81   |
|       | 医療     | 25     | 100  | 33     | 100  |
|       | 娯楽遊戯施設 | 2      | 20   | 4      | 20   |
|       | 合計     | 95     | 698  | 147    | 714  |
| 合計    |        | 639    | 2439 | 997    | 2440 |

### 1-4 調査の内容

本資料では、調査の概要（結果の傾向に対する考察）を、以下の 7 つの分類ごとにまとめ、図表化して説明する。

なお、(1)～(5)については、導入時期や導入規模による結果の分析も併せて行った。

- (1) 提供する「無線 LAN サービス」の概要について
- (2) 利用者を守るための対策について
- (3) 無線 LAN を安全に提供するための対策について
- (4) 利用者に安心を提供するための対策について
- (5) 無線 LAN のセキュリティ等全般について
- (6) 企業における業種による特徴について
- (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

(8) Q42 自由意見について

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。

## 1-5 調査結果の概要

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し、個々の回答に対する図表はすべて付属資料にまとめた。

なお、企業については、もともとの回答数が少ない関係で、データ数そのものが小数（おおむね5程度以下）のものについては、傾向を把握するには数量が不十分という考え方をもとに考察対象から外した（特に業種別の特徴の解析時）。

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。

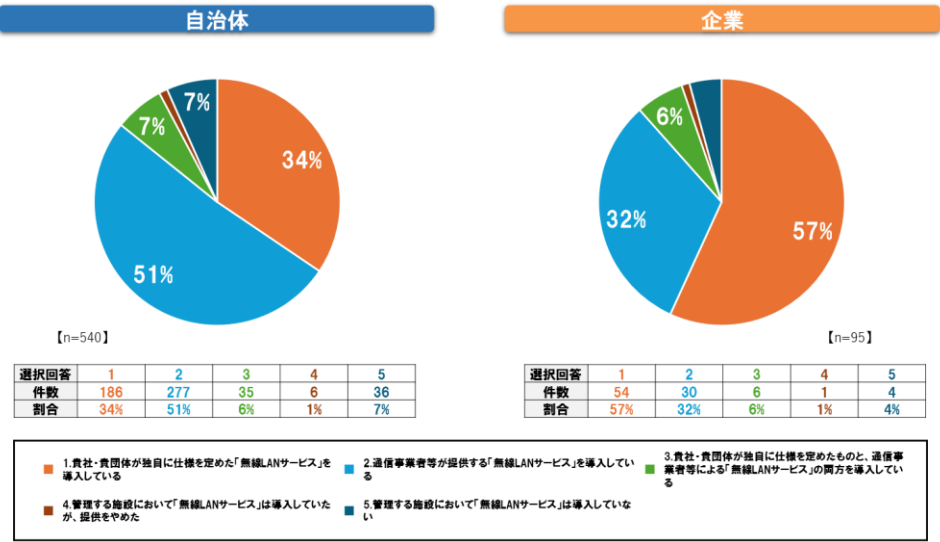
- ✓ アンケート回答に対して、自治体、企業ともに、おおむね9割が無線LANサービスを導入していると回答（前年よりやや増加）。
- ✓ 無線LANサービス自体は増加しているが、新規導入数は2017年頃を境に少しずつ減少している（前年から継続）。
- ✓ 運用管理については、内製率が自治体では約60%、企業で47%であったが、企業、自治体ともに約2割が「担当者が不在」または「わからない」との回答があった（前年と同様の傾向）。
- ✓ 目的として「観光客の誘客」が減少し、相対的に「災害時の活用」が増加しているがこれらは、新型コロナウイルス感染症が影響していると思われる（直近は「観光客の誘客」が増加している）。
- ✓ 利用している無線方式は現在のメジャー規格（802.11ac/11ax）が着実に増加している。また、前年は利用のなかった6GHz帯の利用が始まっている。
- ✓ 最新の方式（Wi-Fi 7）については、まだ利用はない。

#### ● 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、91%→88%→92%と毎年増加してきている。企業は89%→82%→95%と推移しており、ほぼ横ばい状態となっているが、いずれも

90%程度であり、地方自治体、企業ともに無線 LAN サービスの提供が定着していることを示している。

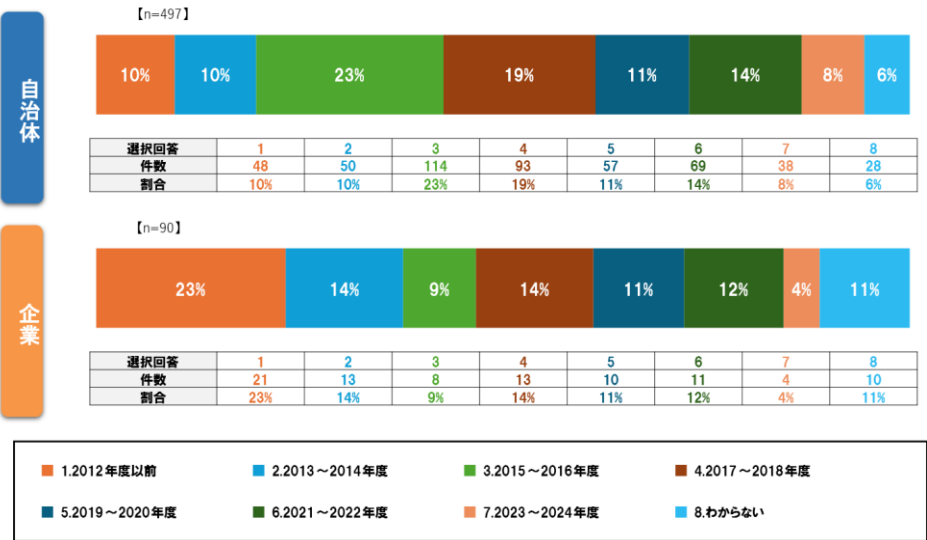
図表 1-3 無線 LAN サービスの導入（Q1）



● 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、企業は 2013 年頃から自治体は 2015 年頃から 2018 年をピークに、新規導入数が減少傾向にある。

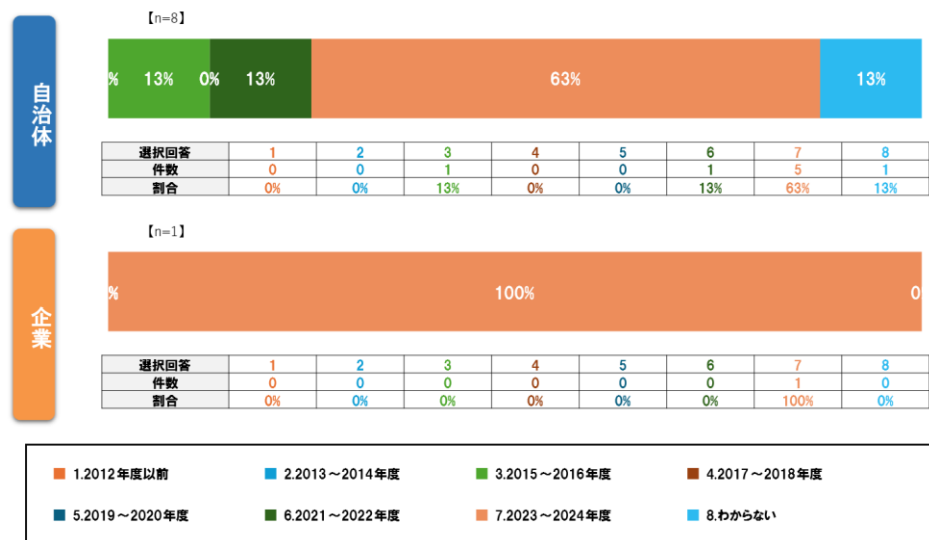
図表 1-4 無線 LAN サービスの導入時期（Q2）



● 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、2023 年以降、自治体で 6 か所、企業で 1 か所、無線 LAN サービスを終了した場所があった。

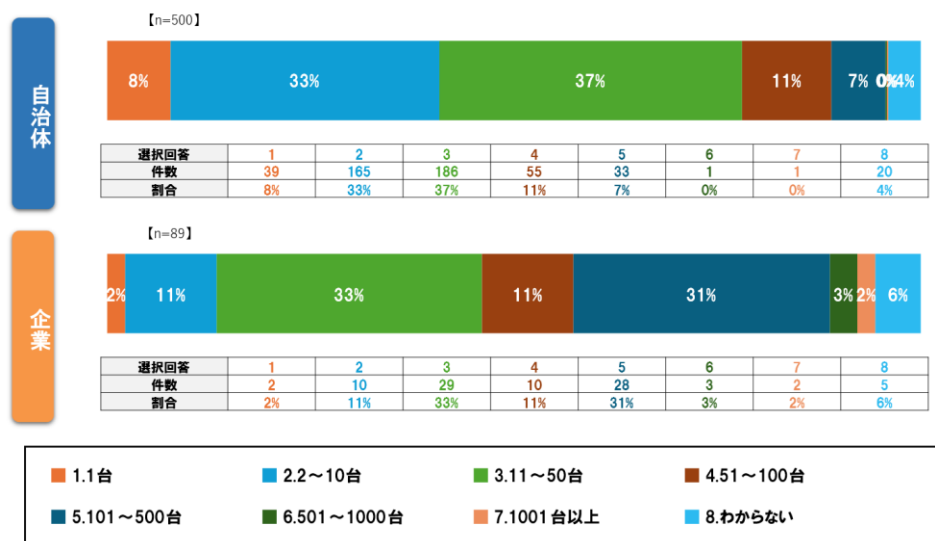
図表 1-5 無線 LAN サービスの終了時期（Q3）



● 無線 LAN サービスの規模（Q5）

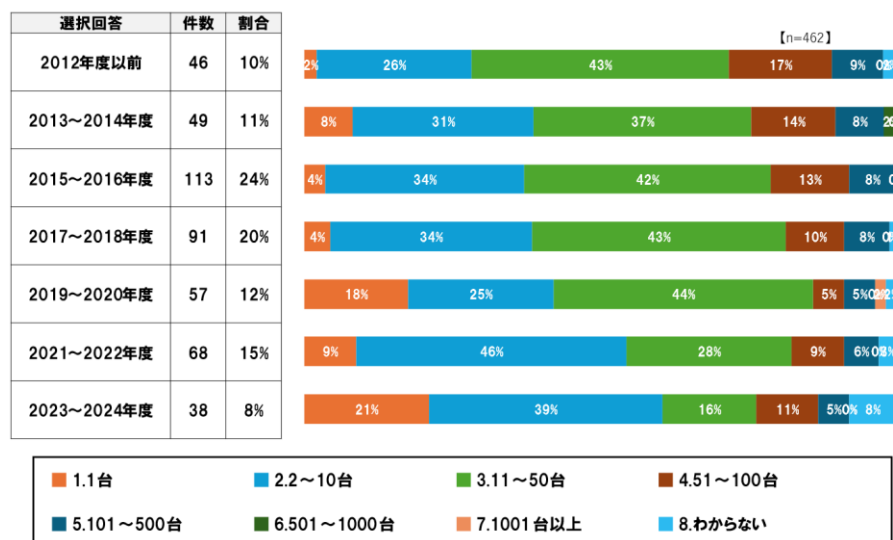
無線 LAN サービスの規模としてアクセスポイント台数について調査したところ、地方自治体が提供する無線 LAN サービスは、これまでの調査と同様に、企業に比べて小規模なことが多いことが分かった。

図表 1-6 無線 LAN サービスの規模（Q5）



また、サービスの導入時期をベースとして分類したところ、コロナ（2020年）以降、規模の小さな案件が増加していることが分かった。

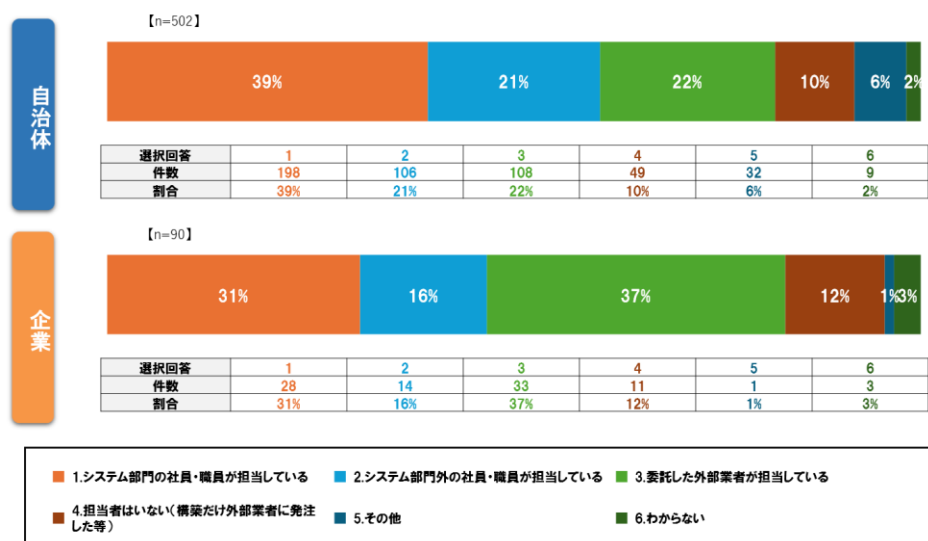
図表 1-6a 無線 LAN サービスの規模（Q5）（導入時期ベース）



#### ● 無線 LAN サービスの運用管理（Q6）

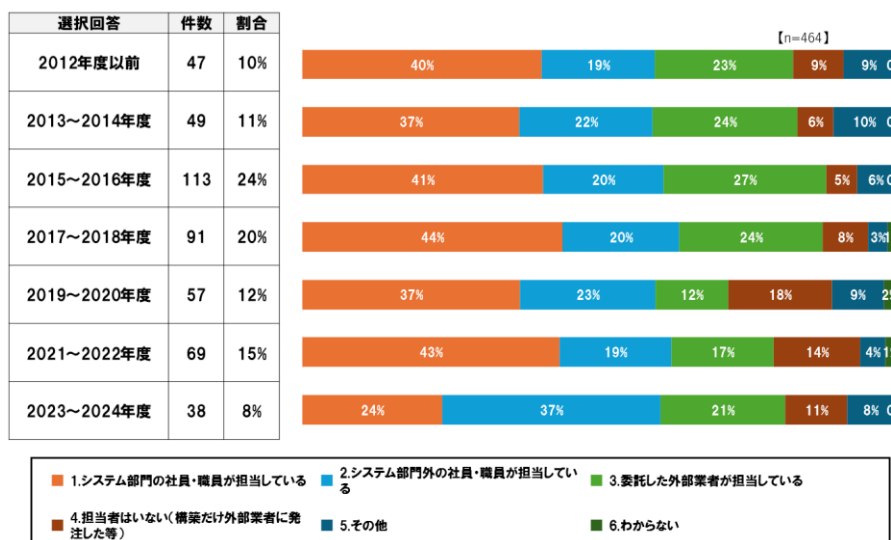
昨年と同様の傾向であり、地方自治体の内製率は60%で、企業・団体（47%）よりも多く、10%以上の自治体で運用担当者が不明状態となっている。

図表 1-7 無線 LAN サービスの運用管理（Q6）

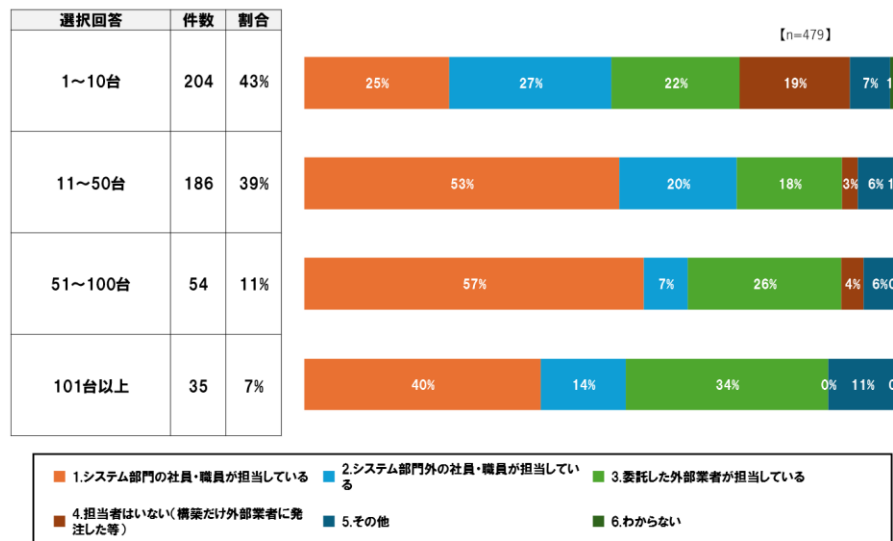


また、サービスを導入した時期をベースとして分類したところ、地方自治体で、直近はシステム部門外の社員が担当している事例が増加している。さらに導入規模をベースとして分類すると、規模が大きな団体は外部への委託が多いことが分かった。

図表 1-7a 無線 LAN サービスの運用管理（Q6）（導入時期ベース）



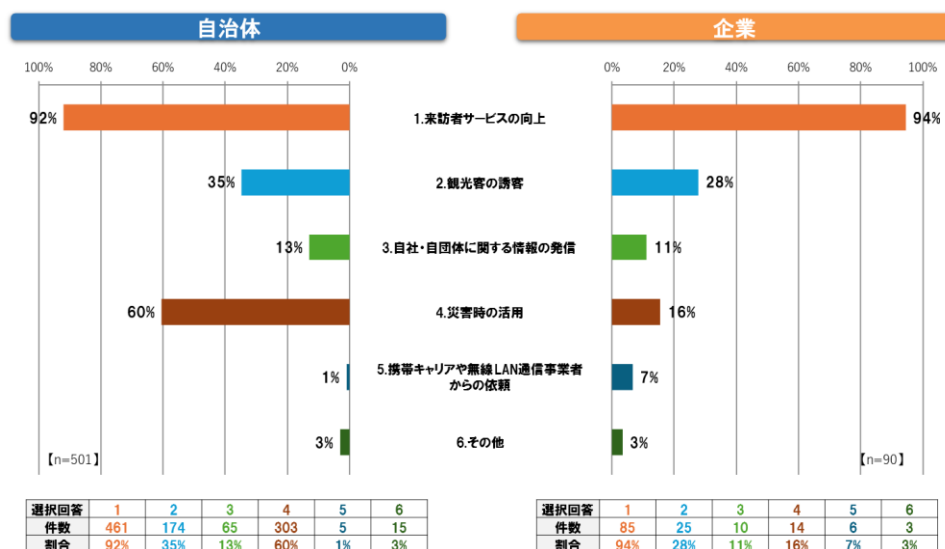
図表 1-7b 無線 LAN サービスの運用管理（Q6）（導入規模ベース）



● 無線 LAN サービスの目的（Q7）

昨年と同様の傾向で、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」が2番目に比率が高い。

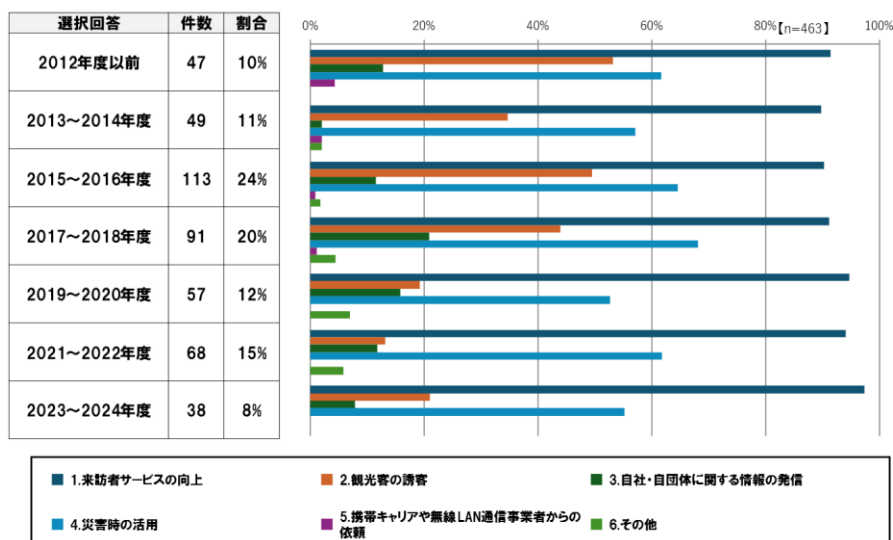
図表 1-8 無線 LAN サービスの目的（Q7）



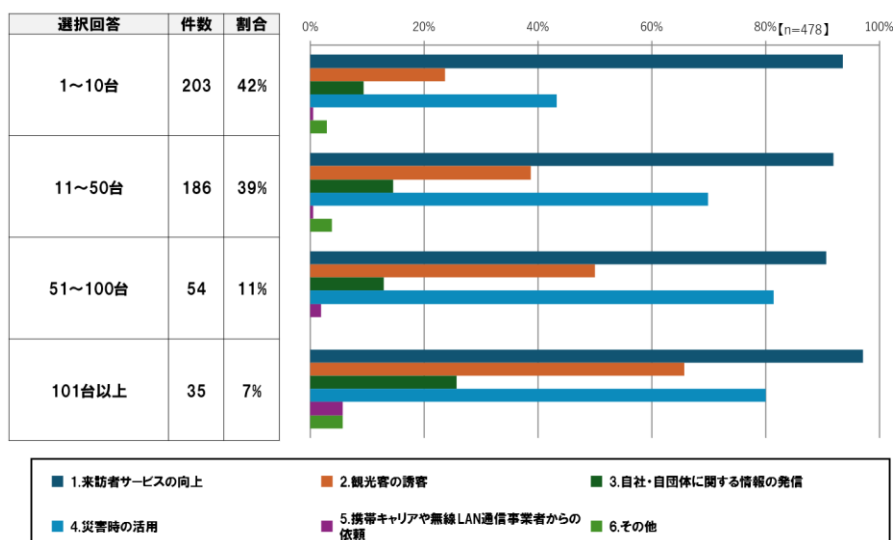
また、サービスを導入した時期をベースとして目的を分類したところ、2020年度から「観光客の誘客」を目的とした導入が大きく低下しているが（新型コロナの影響と考えられる）直近のデータでは回復の兆しがある（インバウンドの増加によるものと考えられる）。さら

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」目的が増加することが分かった。

図表 1-8a 無線 LAN サービスの目的（Q7）（導入時期ベース）



図表 1-8b 無線 LAN サービスの目的（Q7）（導入規模ベース）

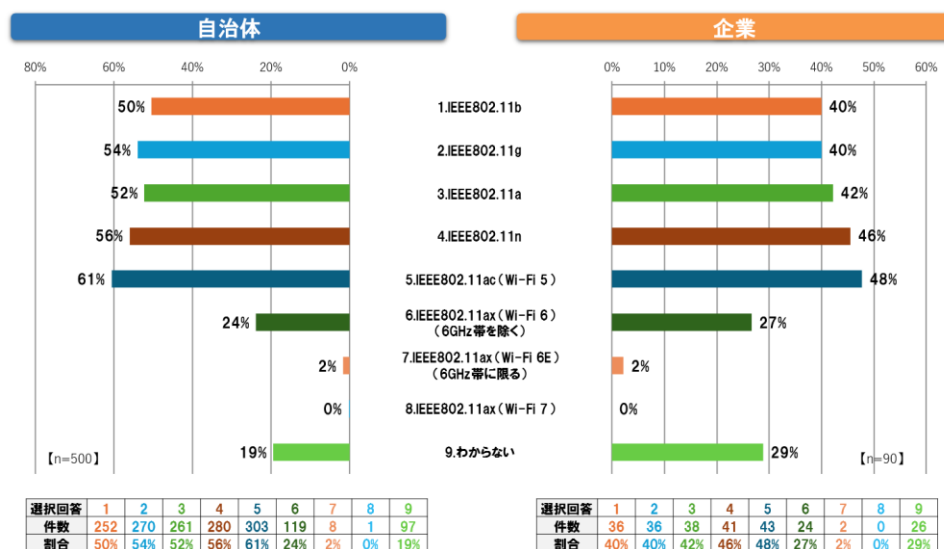


### ● 無線 LAN サービスの伝送規格（Q8）

最新の規格（802.11ax）の採用の割合が、地方自治体、企業ともに年々増加している（自治体：12%→19%→24%、企業：6%→17%→27%）。また昨年利用がなかった 6GHz 帯を

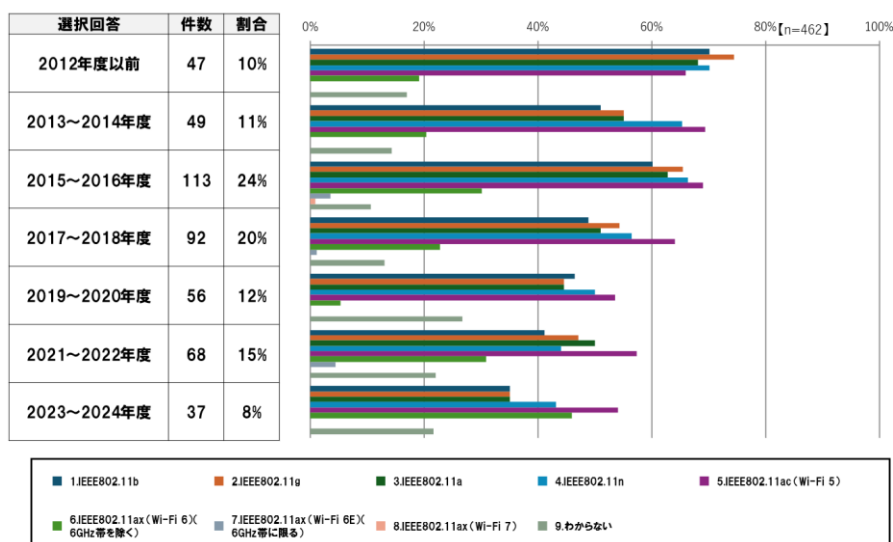
採用した団体も出てきた。

図表 1-9 無線 LAN サービスの伝送規格 (Q8)

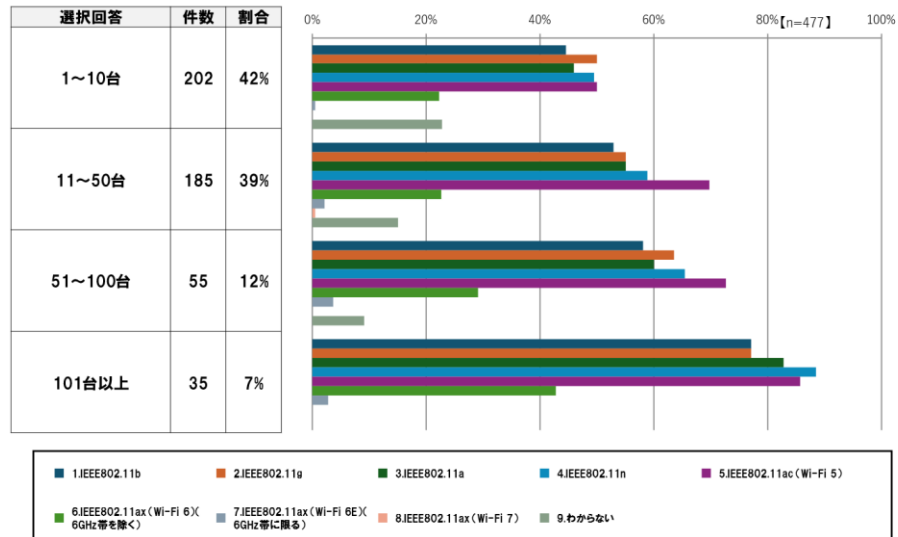


また、サービスを導入した時期をベースとして分類したところ、最近にサービスを開始した団体は、最新の規格 (802.11ax) に対応したものの割合が、さらに高いことが分かった。さらに、サービスを導入した規模をベースとして分類したところ、規模が大きいほど 11ax の採用が多く、規模が小さいほど「わからない」の率が多くなることが分かった。

図表 1-9a 無線 LAN サービスの伝送規格 (Q8) (導入時期ベース)



図表 1-9b 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

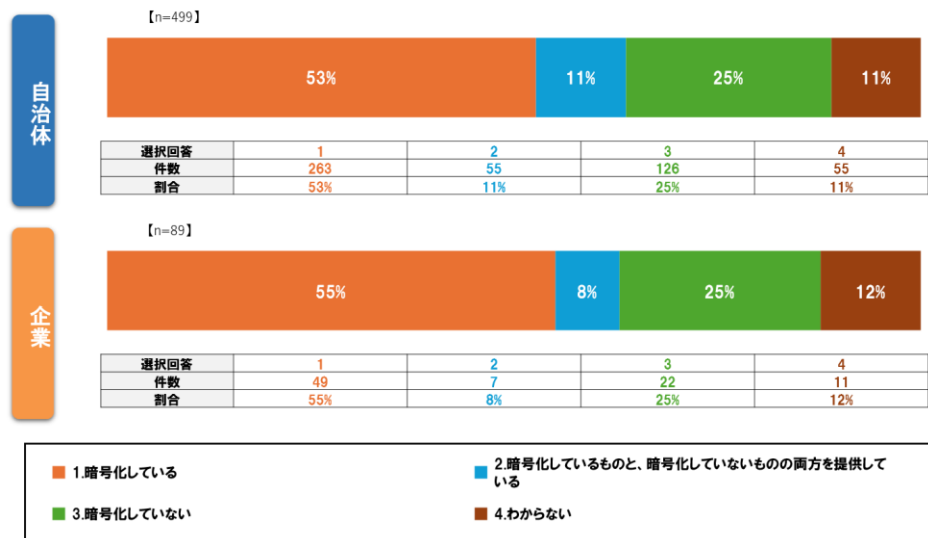
回答には以下のような特徴がみられた。

- ✓ 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 2017 年以降に導入されたものは暗号化率が高い（前年と同様の傾向）。
- ✓ 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（前年と同様の傾向）。
- ✓ 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（前年と同様の傾向）。
- ✓ 端末の折り返し通信のリスクの認識率については横ばい。
- ✓ 偽アクセスポイントに対する対策は企業で「何もしていない」率が改善。また対策として EAP 認証対応が増加。

### ● 無線 LAN サービスの暗号化（Q9）

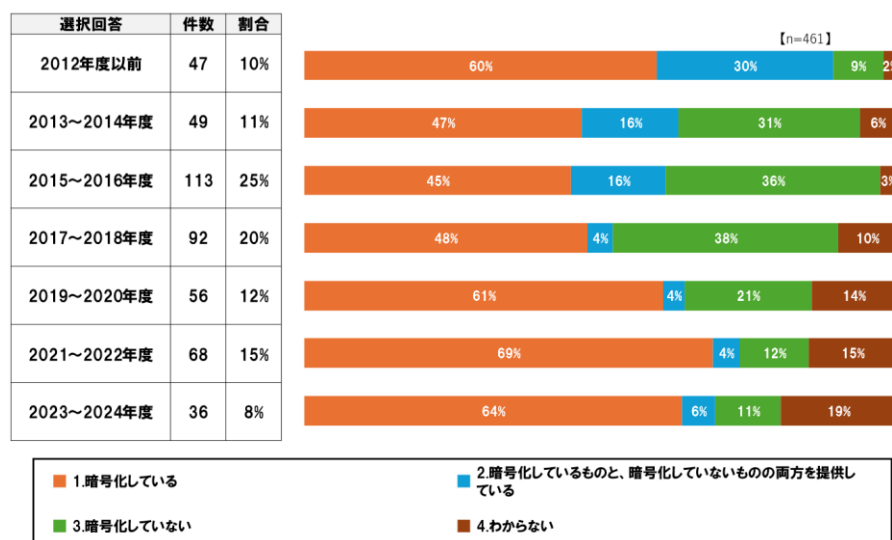
地方自治体、企業ともに、無線 LAN サービスを暗号化している率は昨年から横ばいとなっている（地方自治体：64%→61%→64%、企業：63%→65%→63%）。

図表 1-10 無線 LAN サービスの暗号化（Q9）

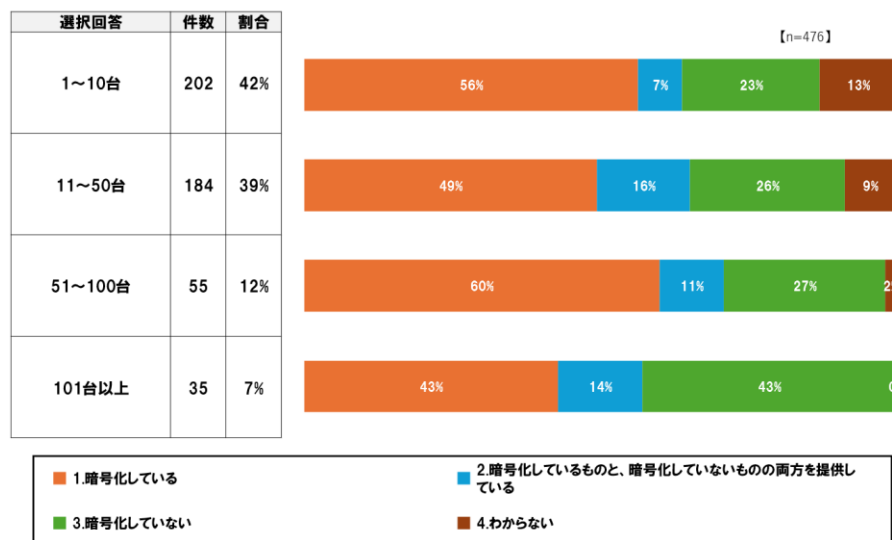


また、サービスを導入した時期をベースとして分類したところ、2019 年以降導入されたものは暗号化率が高いことがわかる。さらに、サービスを導入した規模をベースとして分類したところ、規模が特に大きなものは「暗号化していない」の率が高いことがわかった。

図表 1-10a 無線 LAN サービスの暗号化（Q9）（導入時期ベース）



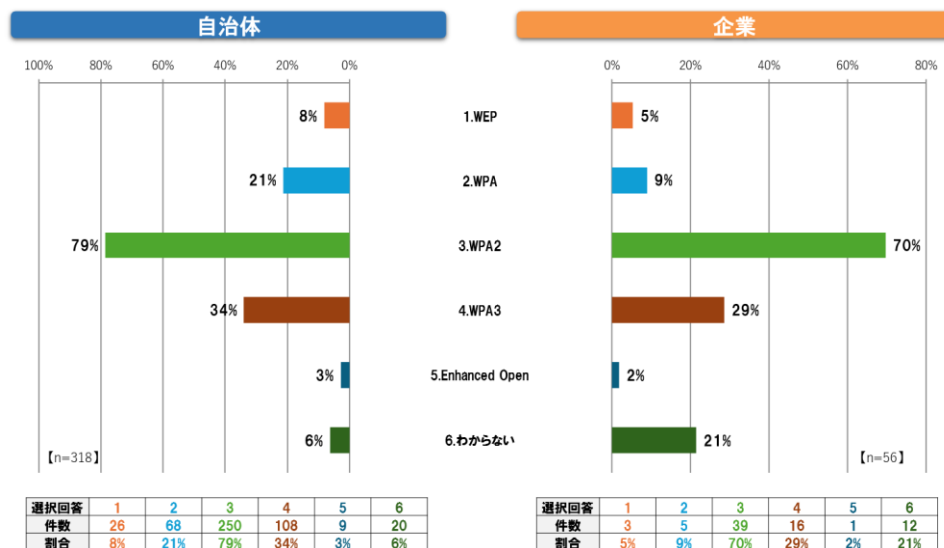
図表 1-10b 無線 LAN サービスの暗号化（Q9）（導入規模ベース）



● 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。最新規格の WPA3 の採用が増加している（自治体：19%→16%→34%、企業：6%→10%→29%）。

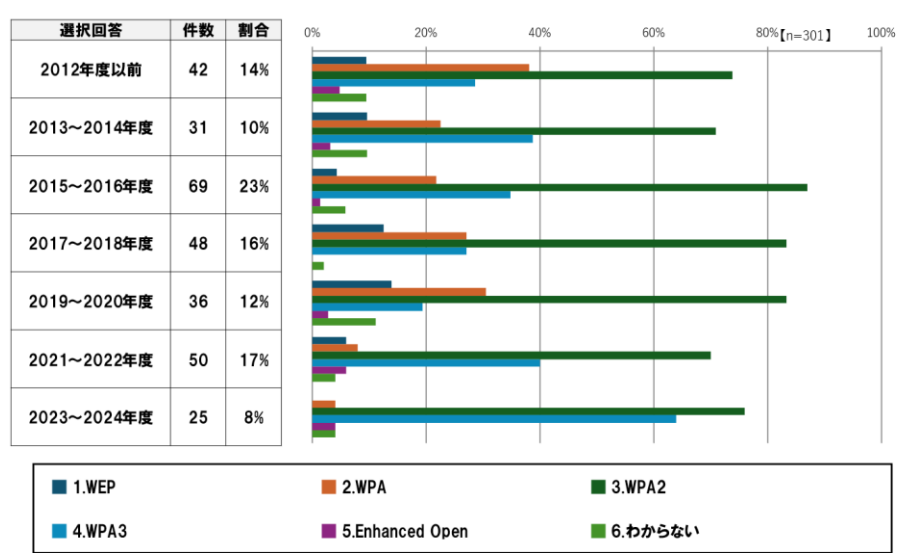
図表 1-11 無線 LAN サービスの暗号化方式 (Q10)



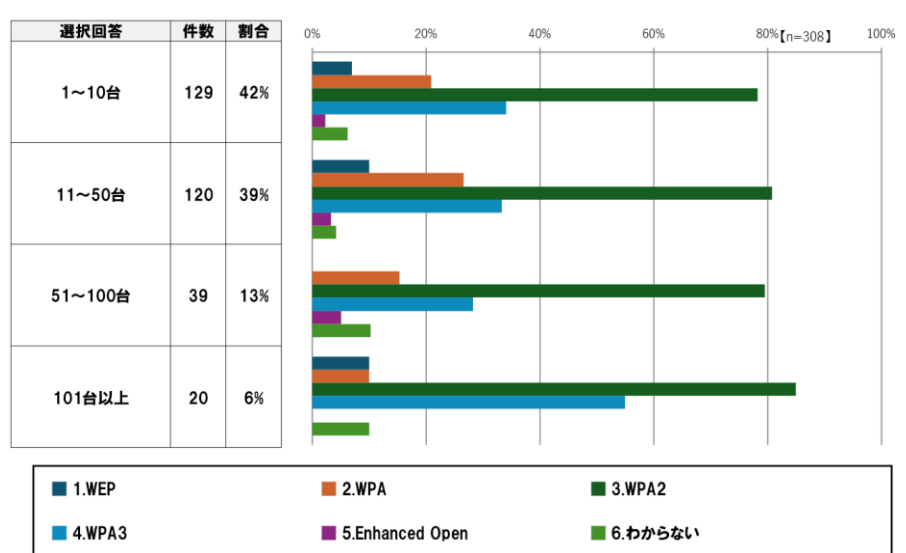
また、サービスを導入した時期をベースとして分類したところ、長年サービスを提供しているところに「WEP/WPA」を使っているものが多く、最近始めたところはほとんど採用し

ていないことが分かった。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、規模が特に大きなものは「WPA3」の採用率が高いことがわかった。

図表 1-11a 無線 LAN サービスの暗号化方式（Q10）（導入時期ベース）



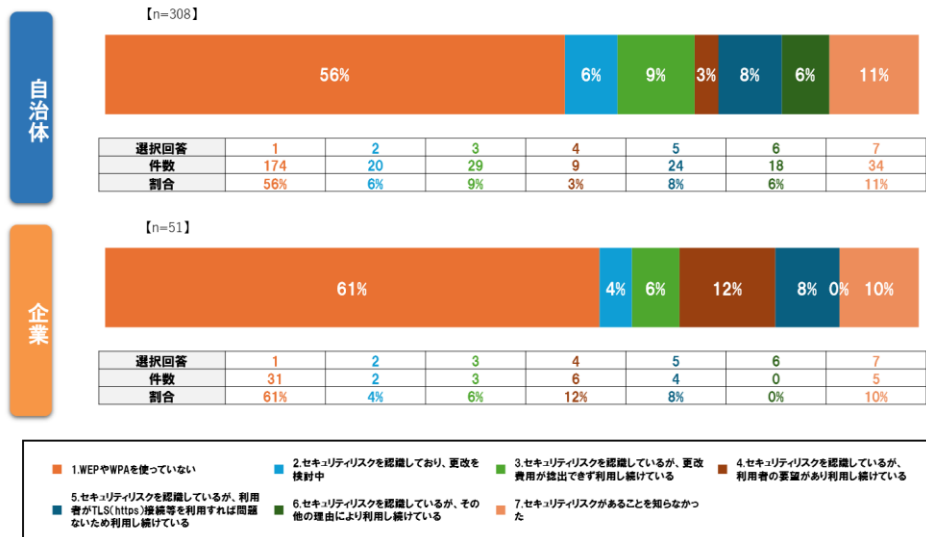
図表 1-11b 無線 LAN サービスの暗号化方式（Q10）（導入規模ベース）



● 暗号化方式のセキュリティリスク（Q11）

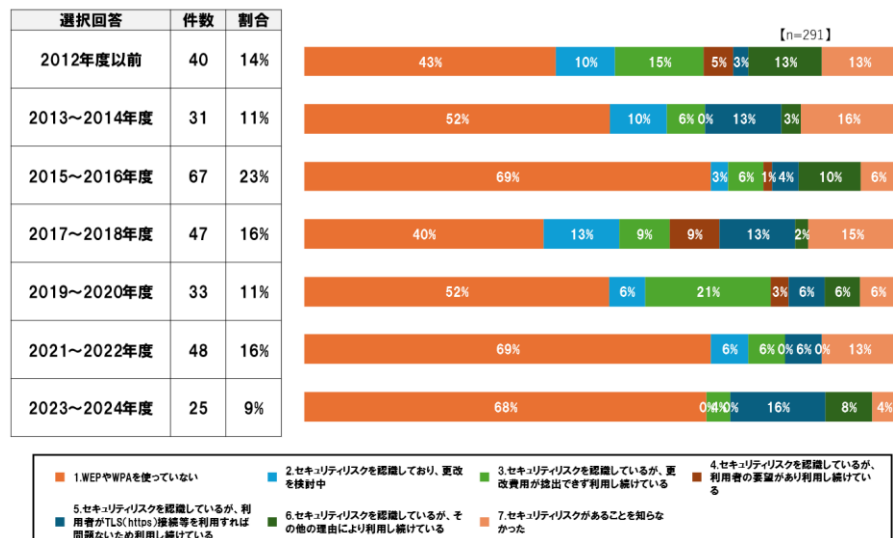
昨年と同じ傾向で、ほとんどの団体は WEP や WPA のセキュリティリスクについて認識をしているが、費用が捻出できない、等の理由でそのままになっている事例が見られる。

図表 1-12 暗号化方式のセキュリティリスク (Q11)

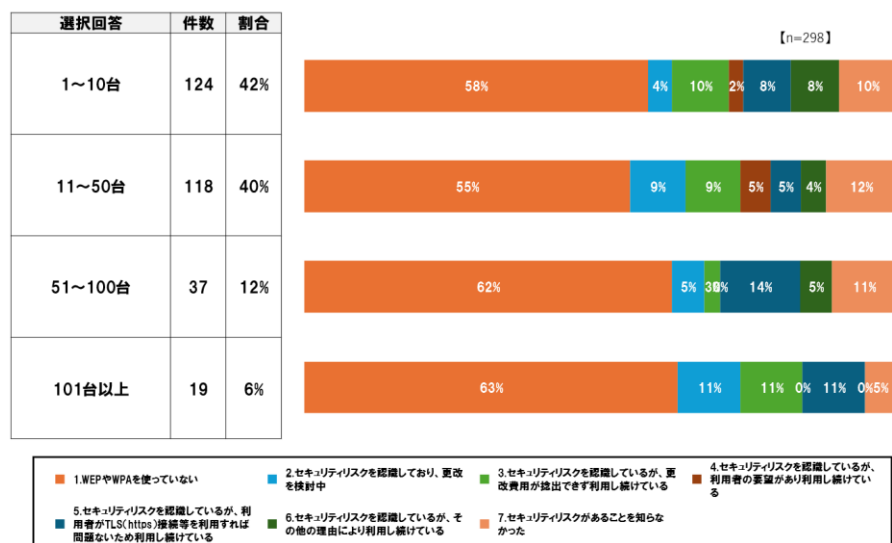


また、サービスを導入した時期をベースとして分類したところ、2021 年以降の導入で WEP/WPA を使っていない率がさらに高いことが分かった。さらに、また導入規模をベースとして分類したところ、規模が大きいほどセキュリティリスクへの認識度は高くなっていることが分かった。

図表 1-12a 暗号化方式のセキュリティリスク (Q11) (導入時期ベース)



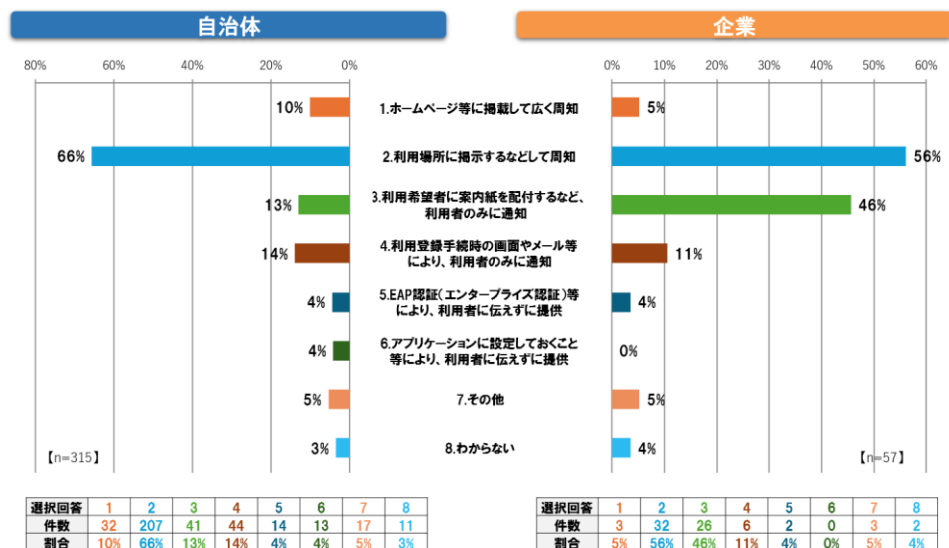
図表 1-12b 暗号化方式のセキュリティリスク（Q11）（導入規模ベース）



● 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 1-13 暗号鍵の利用者への伝達方法（Q12）

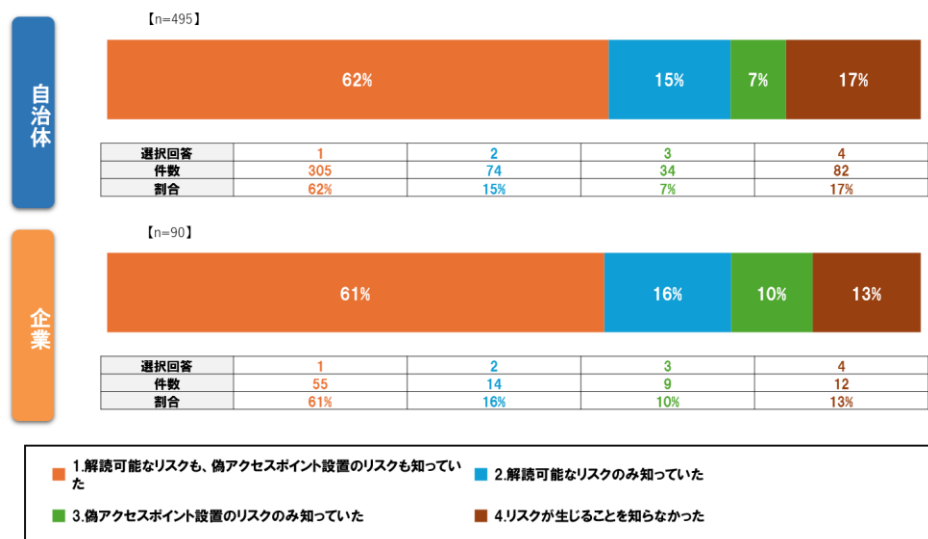


● セキュリティリスクに対する認識（Q13）

前年と同様の傾向。両方のリスクを認識している率は地方自治体は横ばい（60%→63%

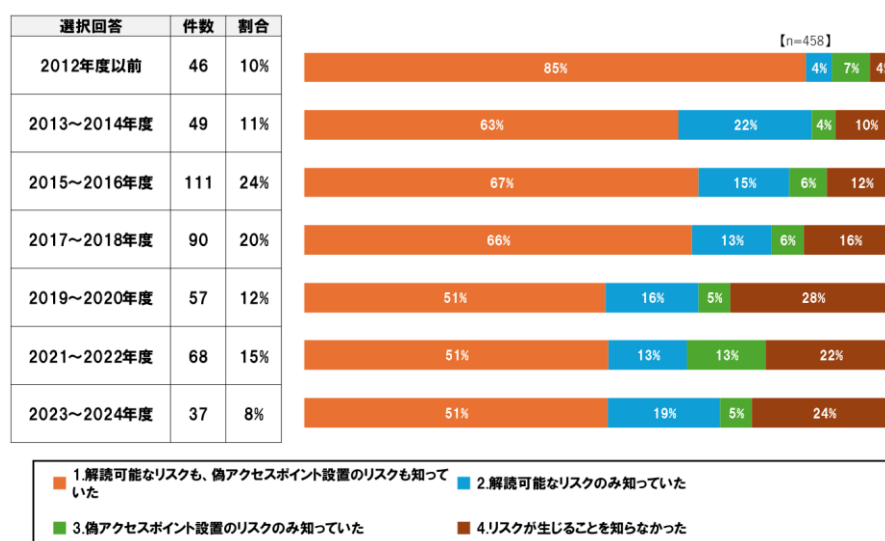
→63%)、企業は、昨年の低下傾向から回復（58%→54%→61%）した。

図表 1-14 セキュリティリスクに対する認識（Q13）

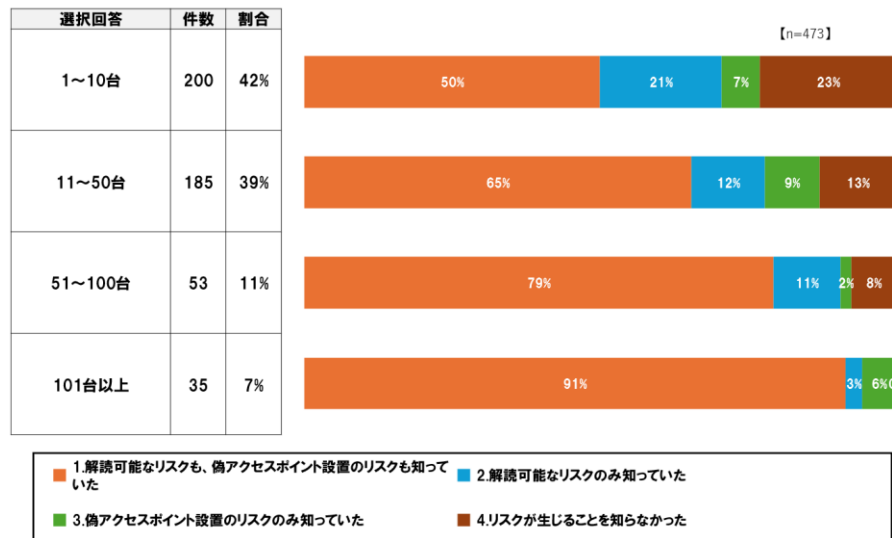


また、サービスを導入した時期をベースとして分類したところ、2019 年以降の導入案件についてセキュリティリスクへの認識度が低くなっていることが分かった。さらに、導入規模をベースとして分類したところ、規模が大きいほどセキュリティリスクへの認識度は高くなっていることが分かった。

図表 1-14a セキュリティリスクに対する認識（Q13）（導入時期ベース）



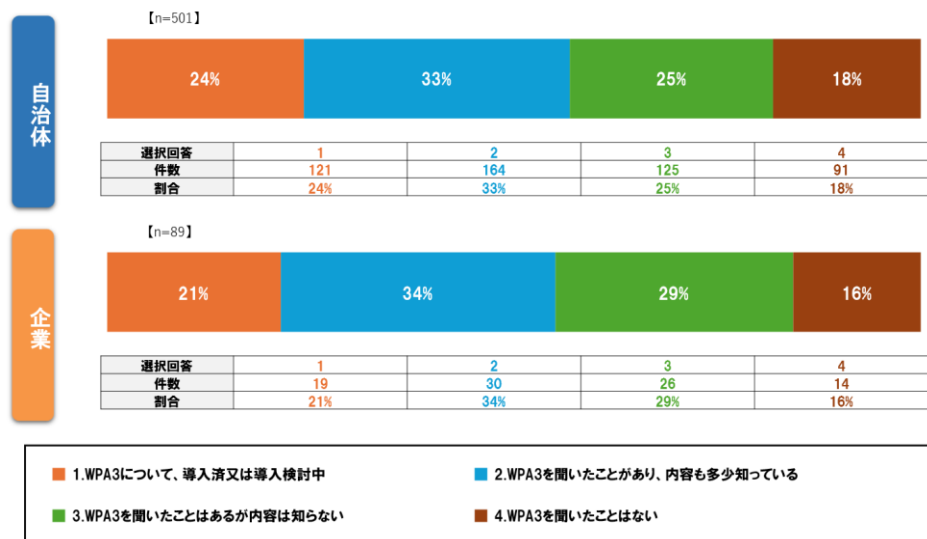
図表 1-14b セキュリティリスクに対する認識（Q13）（導入規模ベース）



● 新しい暗号化方式（WPA3）（Q14）

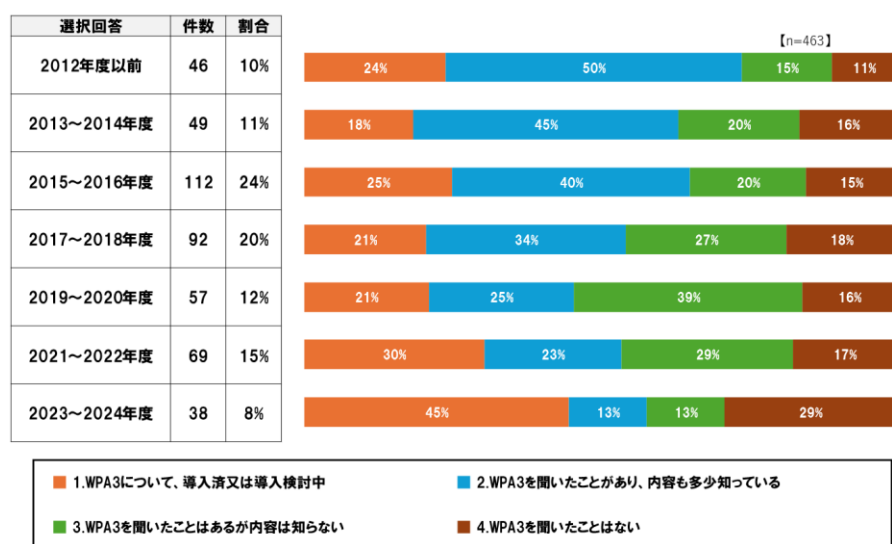
自治体、企業ともに認知度は横ばい（自治体：76%→81%→82%、企業 80%→83%→84%）。だが、導入または導入検討については増加している（自治体：15%→22%→24%、企業：11%→19%→21%）。

図表 1-15 新しい暗号化方式（WPA3）（Q14）

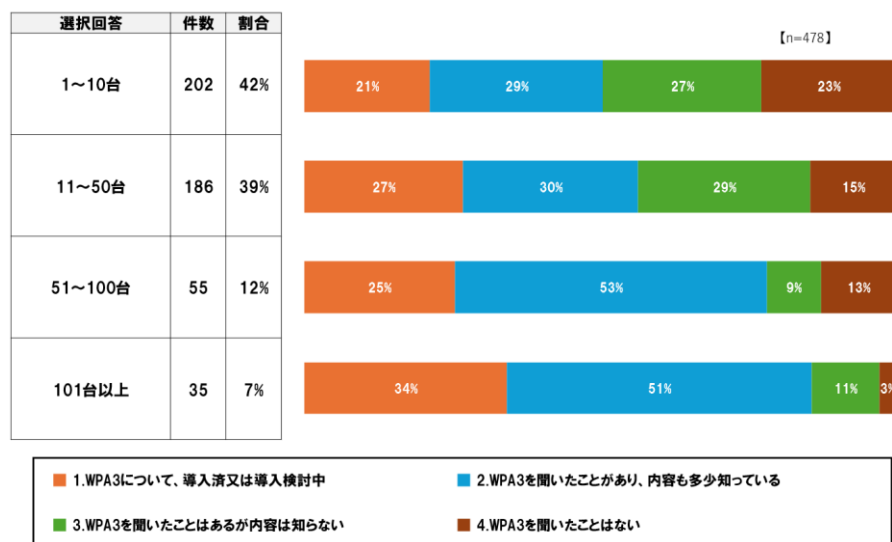


また、導入時期をベースとして分類したところ、2021年以降導入で、WPA3（2018年に方式リリース）の導入が増加している。さらに、導入規模をベースとして分類したところ、規模が大きいほどセキュリティリスクへの認識度は高くなっていることが分かった。

図表 1-15a 新しい暗号化方式（WPA3）（Q14）（導入時期ベース）



図表 1-15b 新しい暗号化方式（WPA3）（Q14）（導入規模ベース）

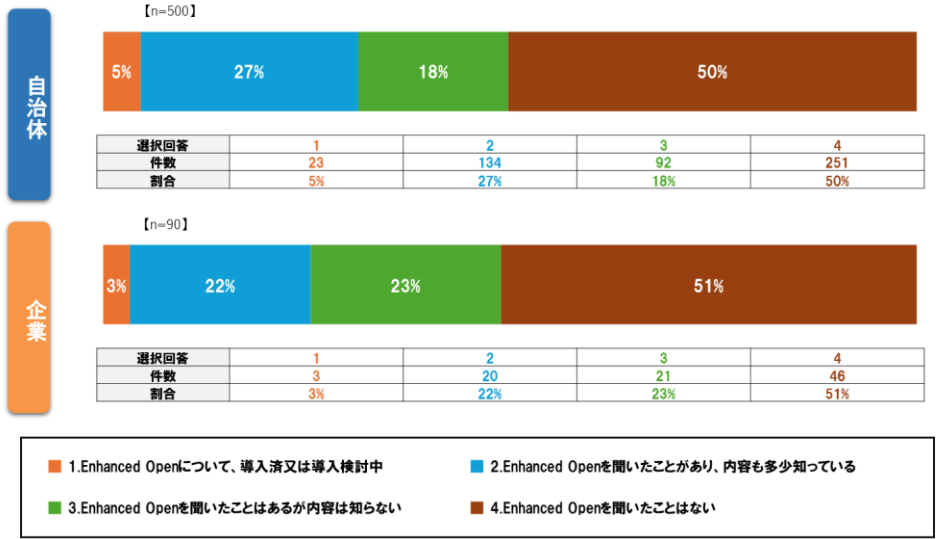


# ● 新しい暗号化方式（Enhanced Open）（Q15）

新しいセキュリティ規格である Enhanced Open についての認識度については、自治体

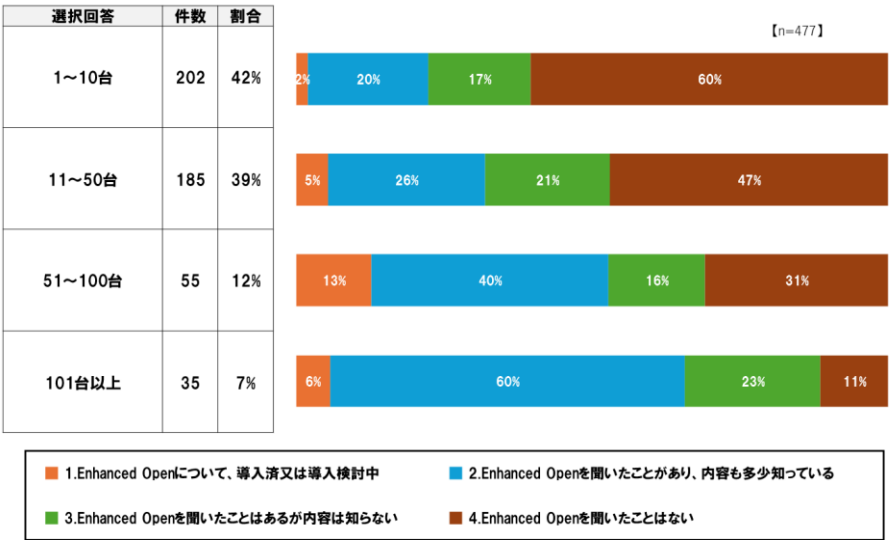
は向上（22%→27%→32%）、企業は横ばい（27%→28%→25%）。自治体、企業ともに導入はまだ進んでいない。

図表 1-16 新しい暗号化方式（Enhanced Open）（Q15）



また、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。

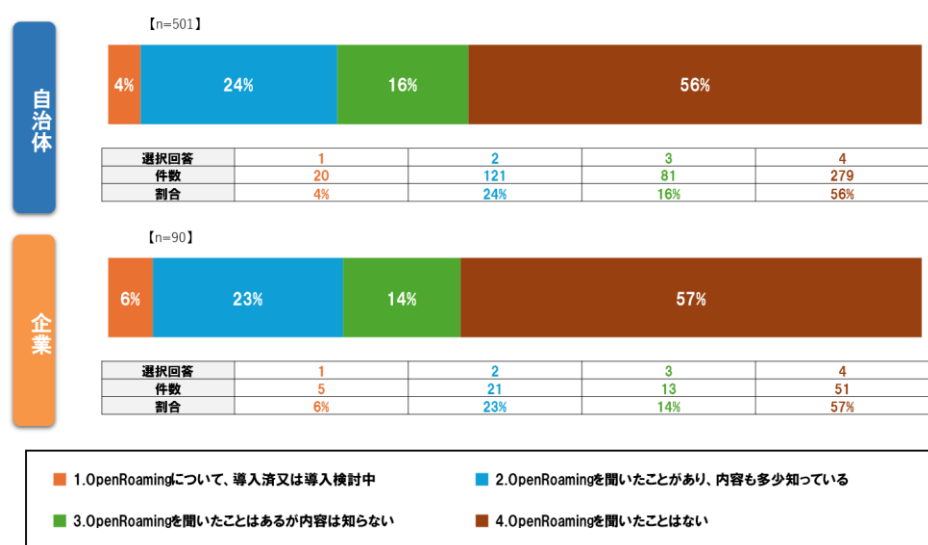
図表 1-16b 新しい暗号化方式（Enhanced Open）（Q15）（導入規模ベース）



● 新しい認証暗号化方式（OpenRoaming）（Q16）

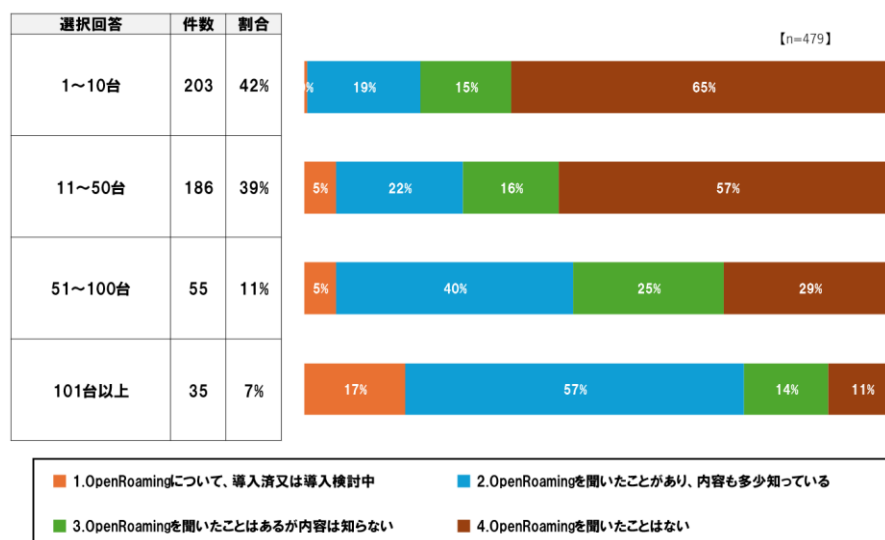
新しい認証暗号化方式として、自治体を中心に導入が始まっている OpenRoaming の認識度は、概ね 50%程度であることが分かった。

図表 1-17 新しい認証暗号化方式（OpenRoaming）（Q16）



また、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、OpenRoaming の認知度が高いことが分かった。

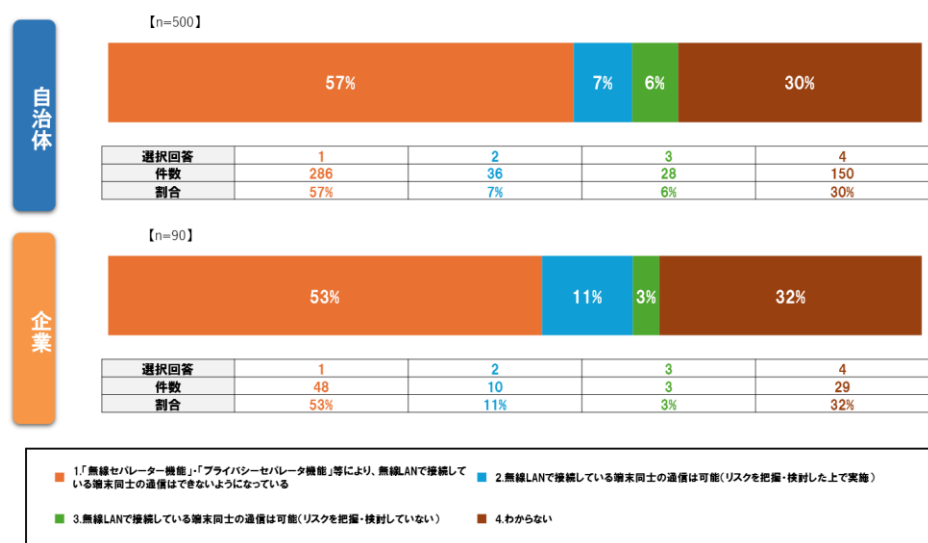
図表 1-17b 新しい認証暗号化方式（OpenRoaming）（Q16）（導入規模ベース）



● 端末同士の折り返し通信（Q17）

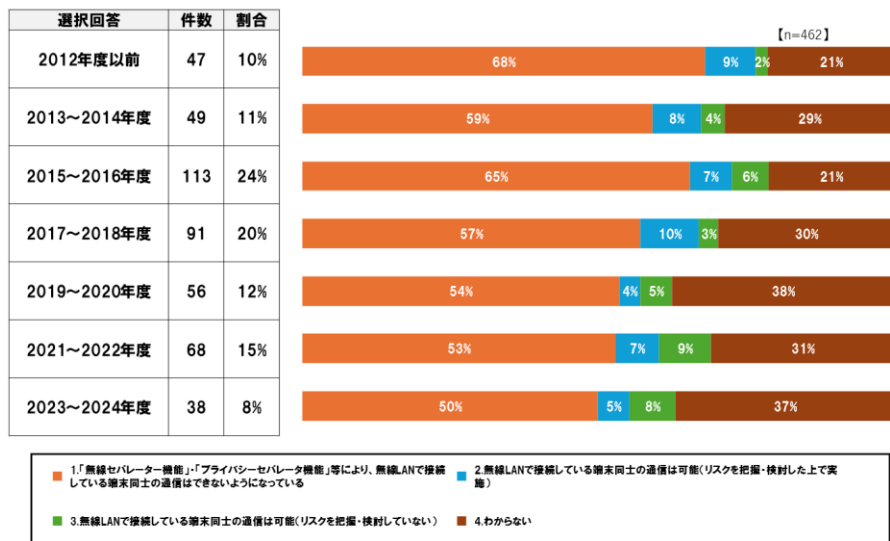
端末同士の折り返し通信については無線 LAN 特有の問題であり、公衆サービスの場合、知らずに情報が漏れてしまう危険性があるが、前年と同様に自治体、企業ともに「わからない」という回答が 3 割程度ある（改善は見られない）。

図表 1-18 端末同士の折り返し通信（Q17）

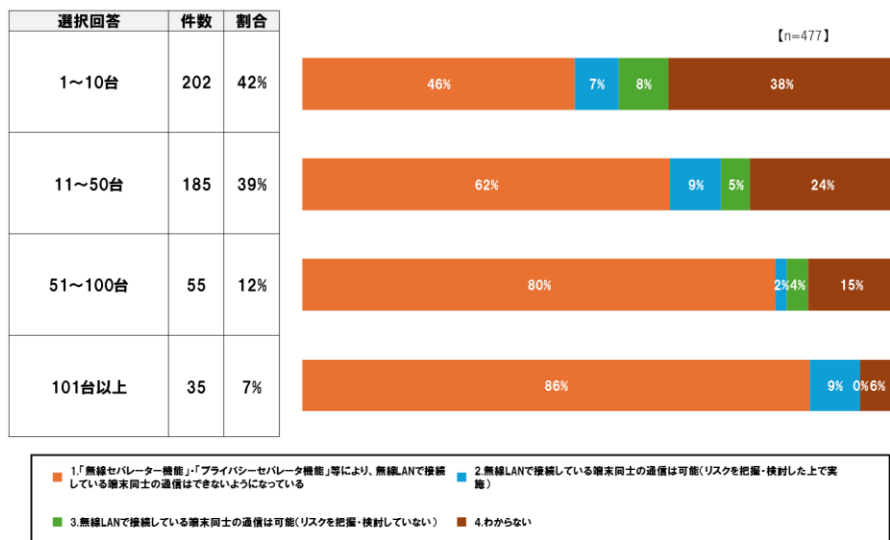


また、導入時期をベースとして分類したところ、年々認知度が下がってきていることが分かった。さらに、導入規模をベースとして分類したところ、規模が大きいほど折り返し通信のリスクに対する認識度は高いことが分かった。

図表 1-18a 端末同士の折り返し通信（Q17）（導入時期ベース）



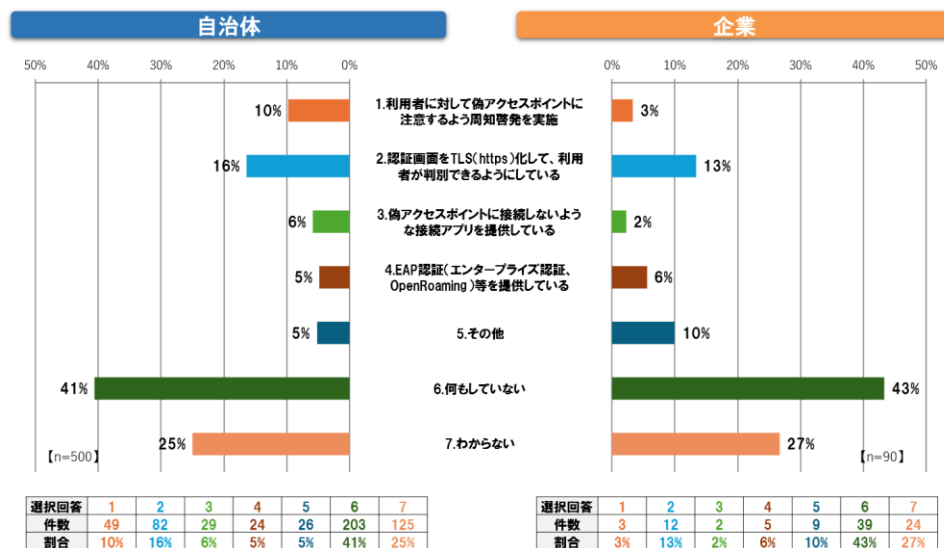
図表 1-18b 端末同士の折り返し通信（Q17）（導入規模ベース）



### ● 偽アクセスポイントへの対策（Q18）

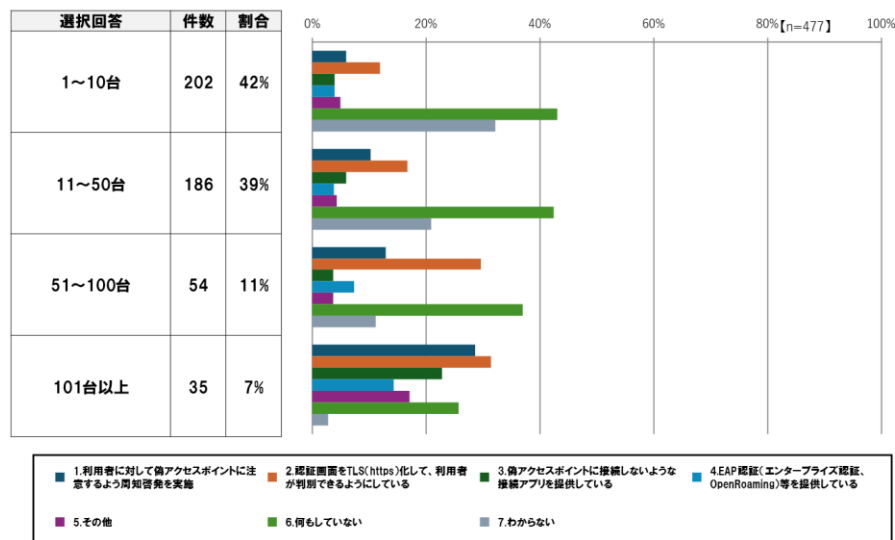
偽アクセスポイントについては何も対策をしていないという回答が 40%強、前年と同様の傾向である。なお、OpenRoaming 導入開始によるものと思われるが EAP 認証は増加傾向。

図表 1-19 偽アクセスポイントへの対策（Q18）



また、導入規模をベースとして分類したところ、規模が大きいほど何らかの対策をしている率が高いことが分かった。

図表 1-19b 偽アクセスポイントへの対策（Q18）（導入規模ベース）



### (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。

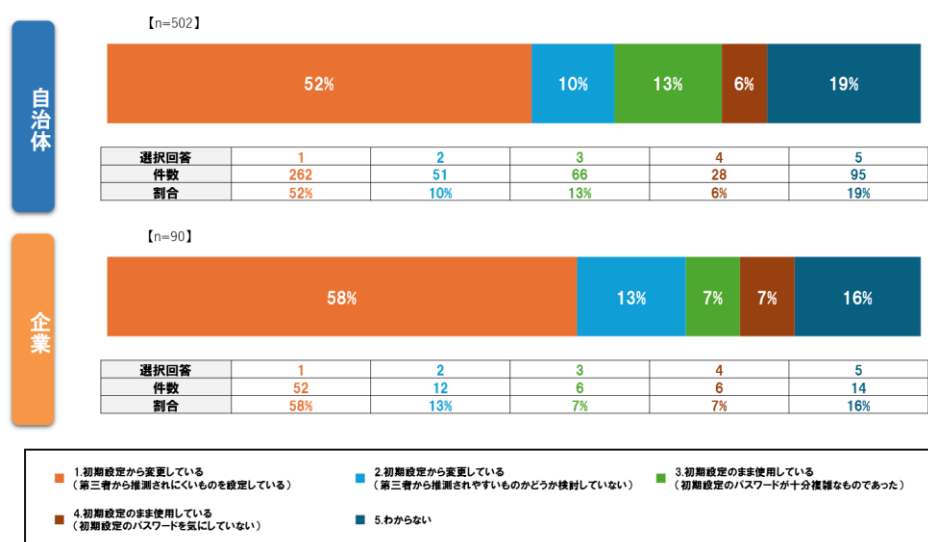
- ✓ 全般的に、各対策の実施率は横ばいであり、大きな改善は見られない（前年と同様の傾向）。

- ✓ 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（前年と同様の傾向）。
- ✓ 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（前年と同様の傾向）。
- ✓ セキュリティ責任者を設定している組織の率は、自治体は高止まり、企業団体は前年に比べ増加。

#### ● 管理者パスワードの管理（Q19）

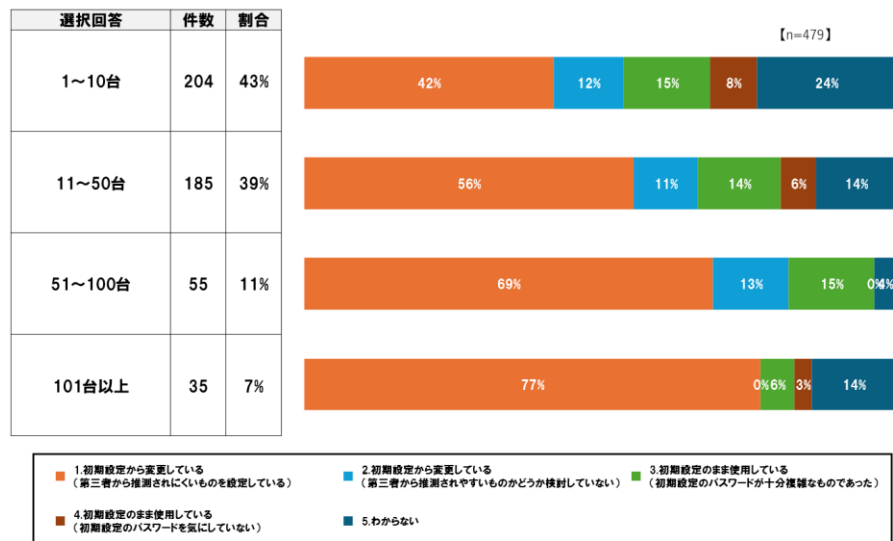
セキュリティ上安全と考えられるもの（回答 1～3）の割合が 7 割以上であり、ここ数年横ばい状態（地方自治体：74%→75%→75%、企業：75%→70%→77%）。

図表 1-20 管理者パスワードの管理（Q19）



また、導入規模をベースとして分類したところ、設備規模が大きいほど、パスワードを適切に管理している率が高いことが分かった。

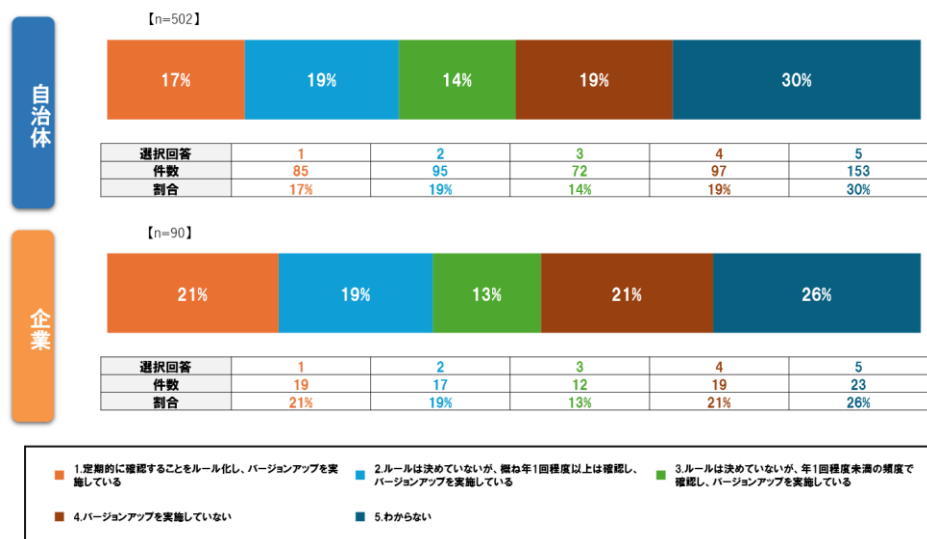
図表 1-20b 管理者パスワードの管理（Q19）（導入規模ベース）



● ネットワーク機器のファームアップ (Q20)

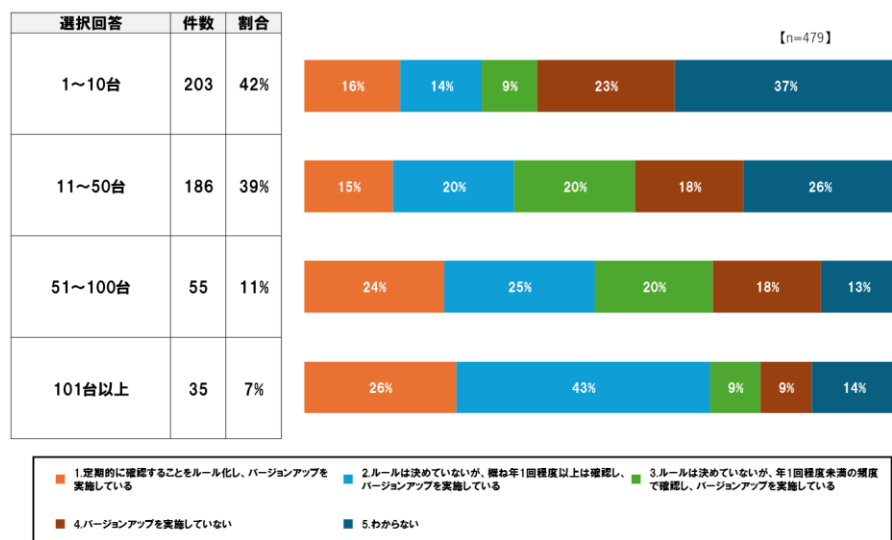
昨年と同様の傾向で、地方自治体、企業ともほぼ半数程度で横ばい状態（自治体：48%→51%→51%、企業 50%→52%→53%）。

図表 1-21 ネットワーク機器のファームアップ (Q20)



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。

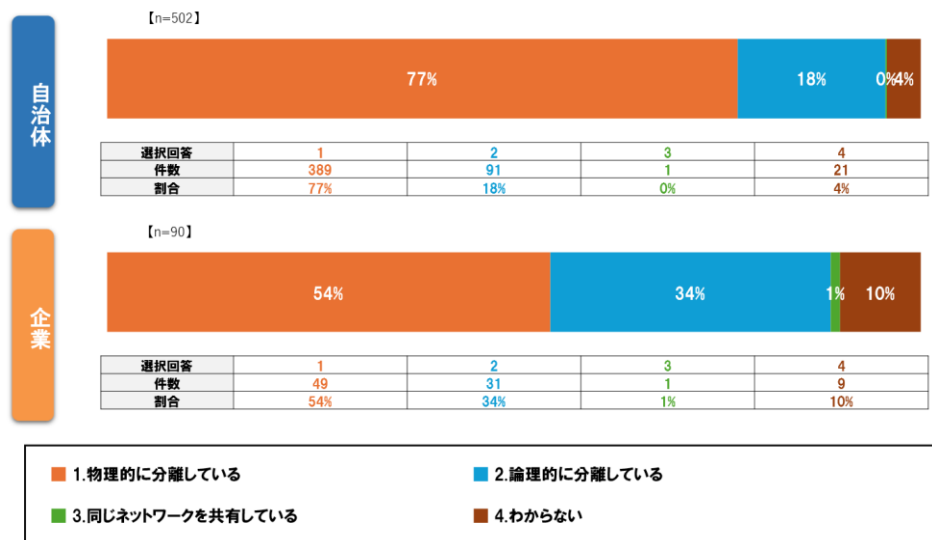
図表 1-21b ネットワーク機器のファームアップ（Q20）（導入規模ベース）



● 業務用ネットワークとの分離（Q21）

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 1-22 業務用ネットワークとの分離（Q21）

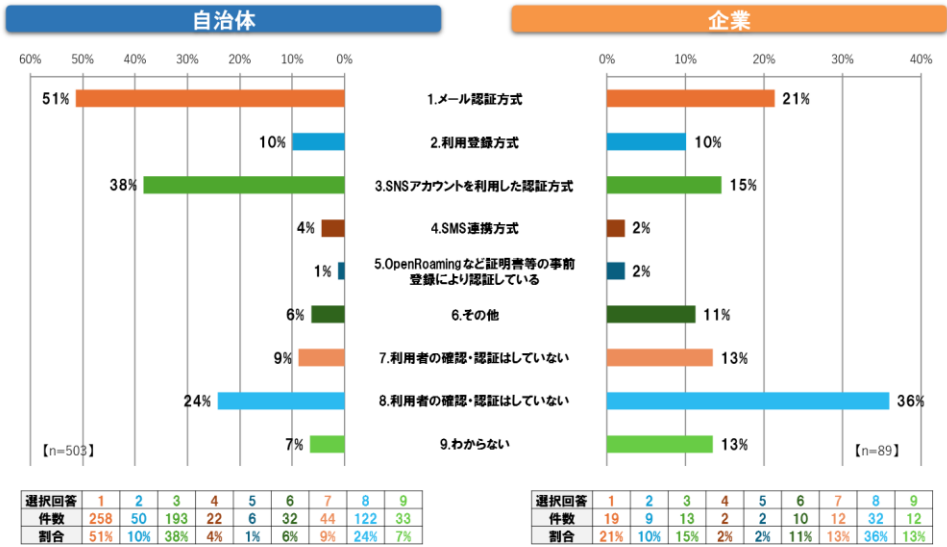


● サービス利用者の認証方式（Q22）

地方自治体は昨年と同様の傾向。企業については、「メール認証方式」や「SNS 認証方式」

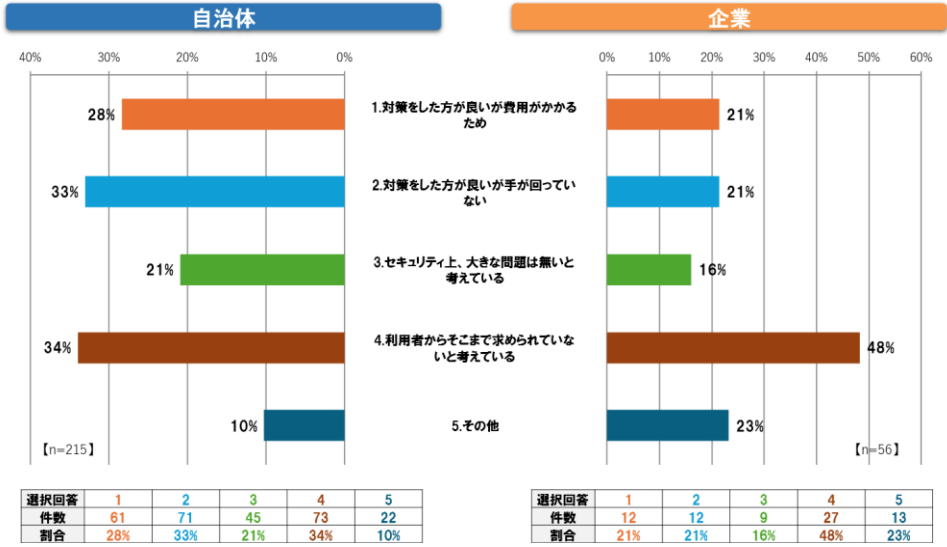
を利用している率が増加している（メール認証方式：9%→7%→21%、SNS 認証方式：7 %  
→5%→15%）

図表 1-23 サービス利用者の認証方式（Q22）



- セキュリティ対策をしていない理由（Q23）  
地方自治体、企業ともに「利用者から求められていない」が最も多いが、自治体はリソースの不足を理由にしている率が企業よりも多い。

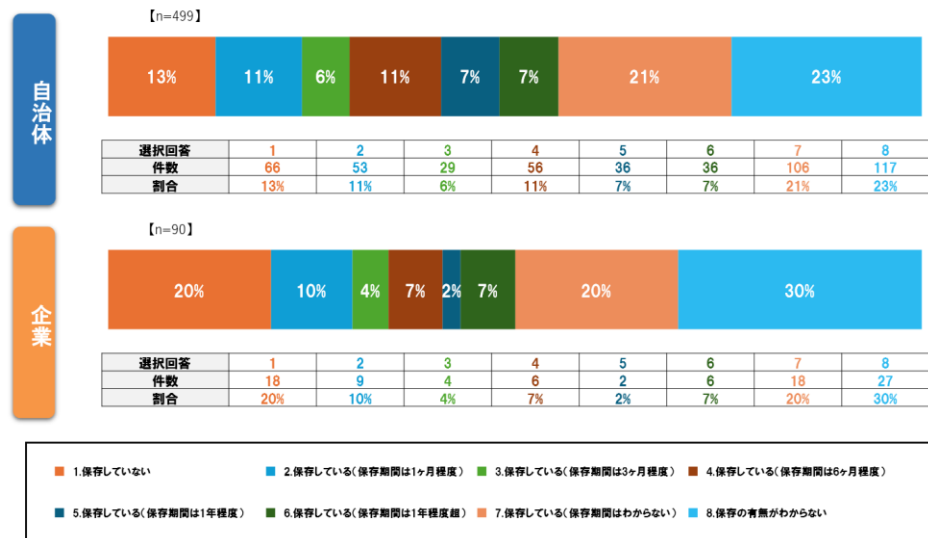
図表 1-24 セキュリティ対策をしていない理由（Q23）



● アクセスログ（通信記録等）の保存（Q24）

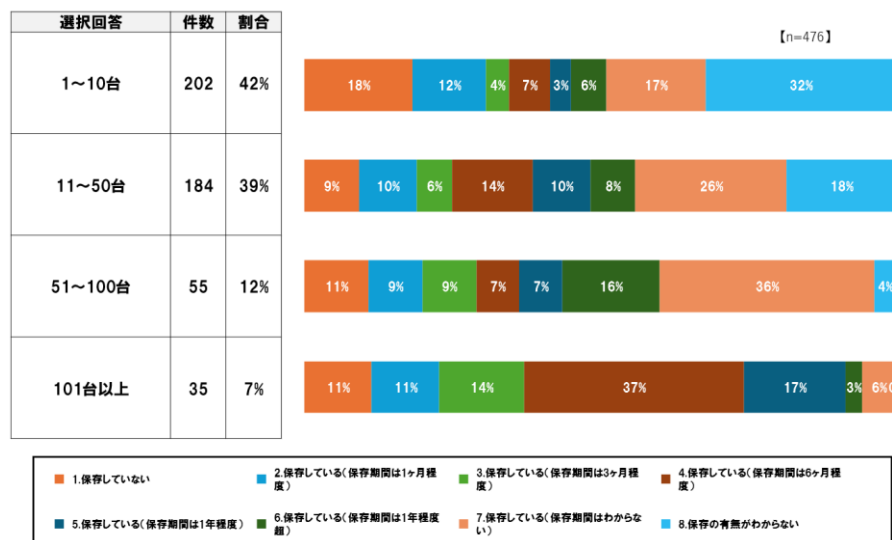
昨年と同様で、アクセスログを保管している率は横ばい（自治体：63%→65%→64%、企業：51%→45%→50%）。

図表 1-25 アクセスログ（通信記録等）の保存（Q24）



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。

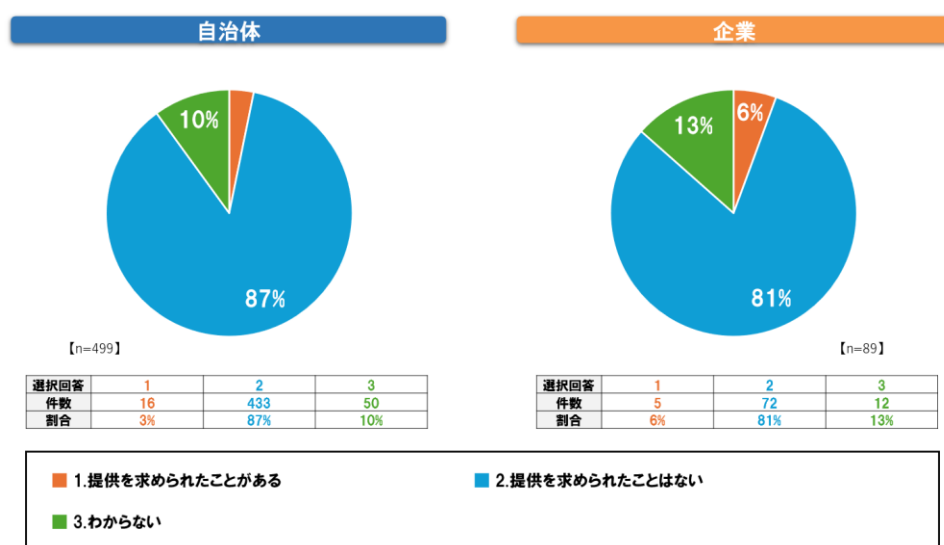
図表 1-25b アクセスログ（通信記録等）の保存（Q24）（導入規模ベース）



● アクセスログ（通信記録等）の提供（Q25）

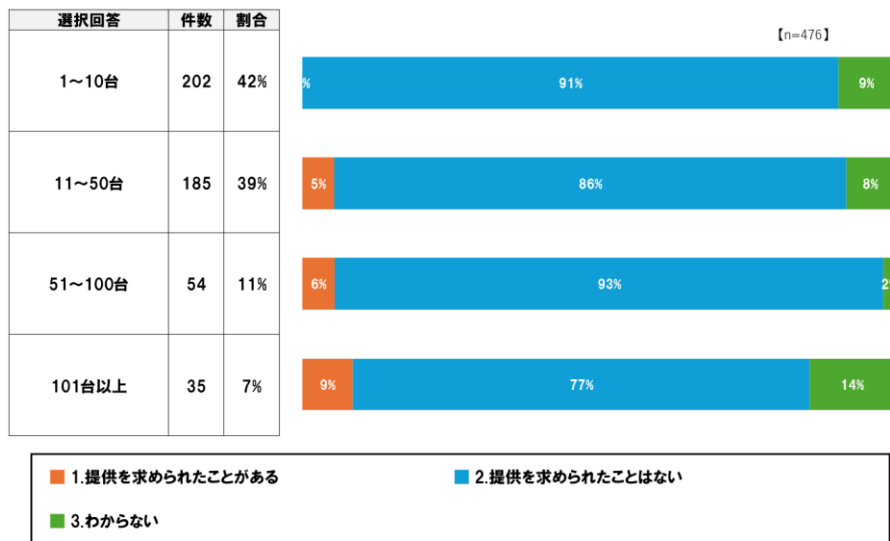
警察からログの提供を求められている事例は前年と同様。自治体は 10%、企業は 15%程度と、ともに少ない。

図表 1-26 アクセスログ（通信記録等）の提供（Q25）



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。

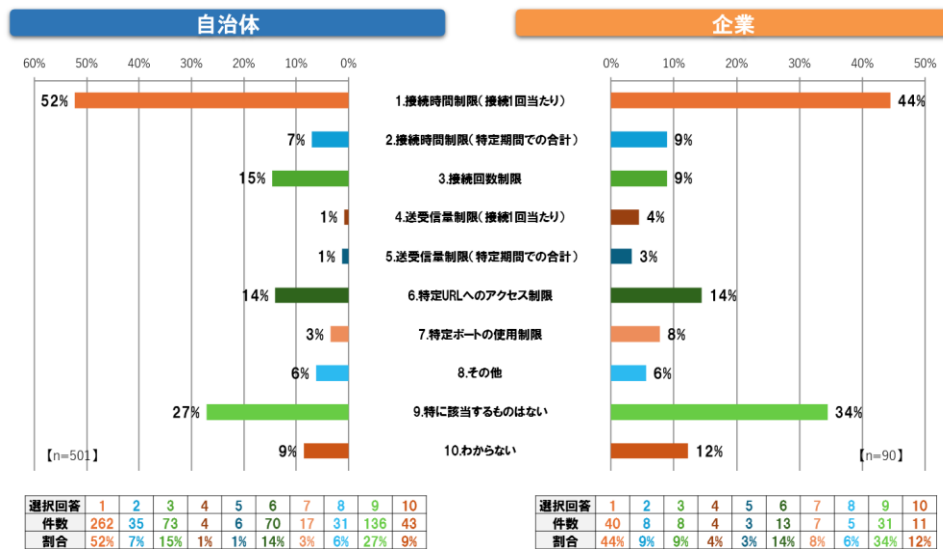
図表 1-26b アクセスログ（通信記録等）の提供（Q25）（導入規模ベース）



● その他のセキュリティ対策（Q26）

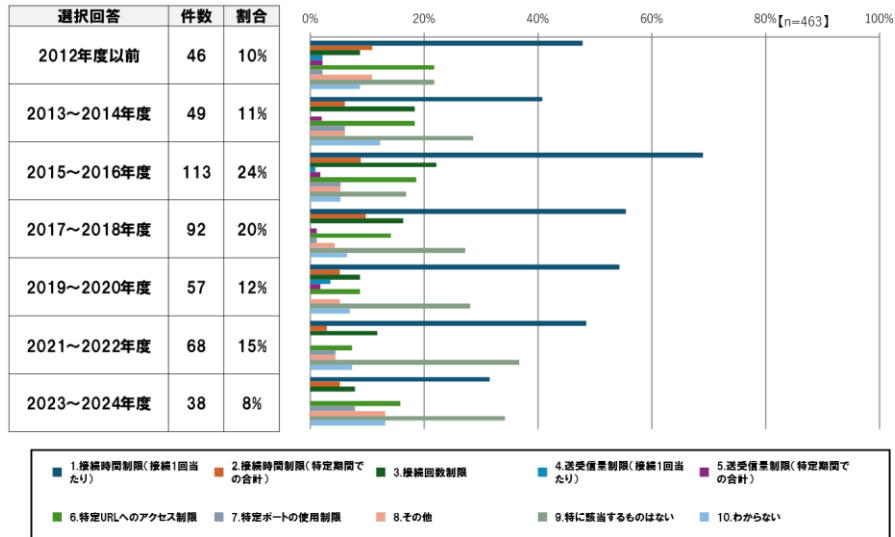
自治体は昨年と同様の傾向だが、企業については、「接続時間制限」及び「URL アクセス制限」が増加している（接続時間制限：26%→26%→44%、URL アクセス制限：8%→10%→14%）。

図表 1-27 その他のセキュリティ対策（Q26）



また、導入時期をベースとして分類したところ、最近導入したものは「接続時間制限」が減少し、「該当なし」が増加していることが分かった。

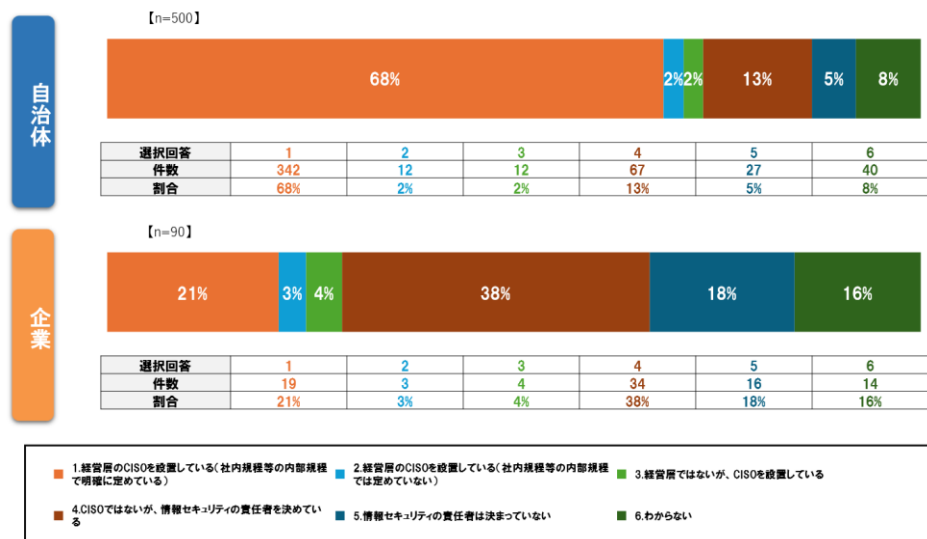
図表 1-27a その他のセキュリティ対策（Q26）（導入時期ベース）



### ● 情報セキュリティ責任者の設置（Q27）

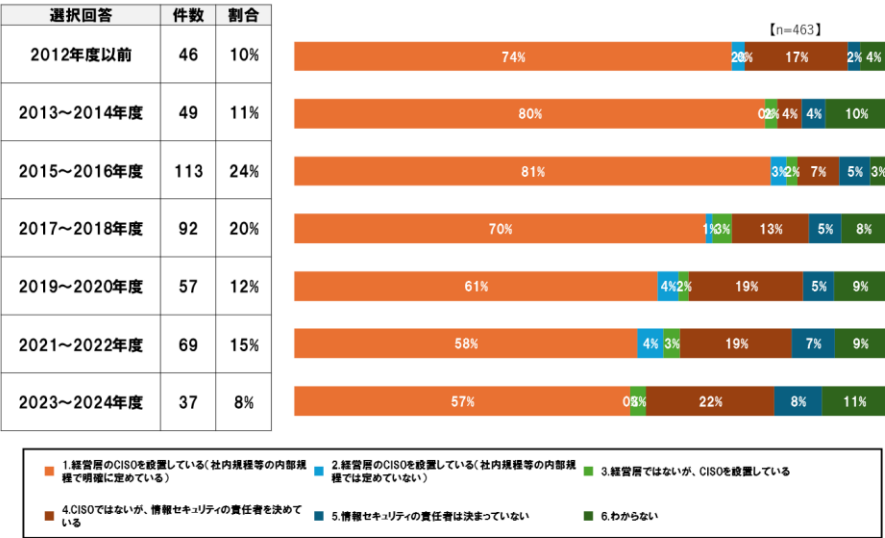
情報セキュリティ責任者を設置している率は自治体が企業よりも多いが、企業は前年より増加している（自治体：88%→91%→87%、企業 54%→55%→66%）。自治体は設置している率は企業よりも著しく高い上に、内部規定で明確に定めている率も高い。

図表 1-28 セキュリティ責任者の設置（Q27）

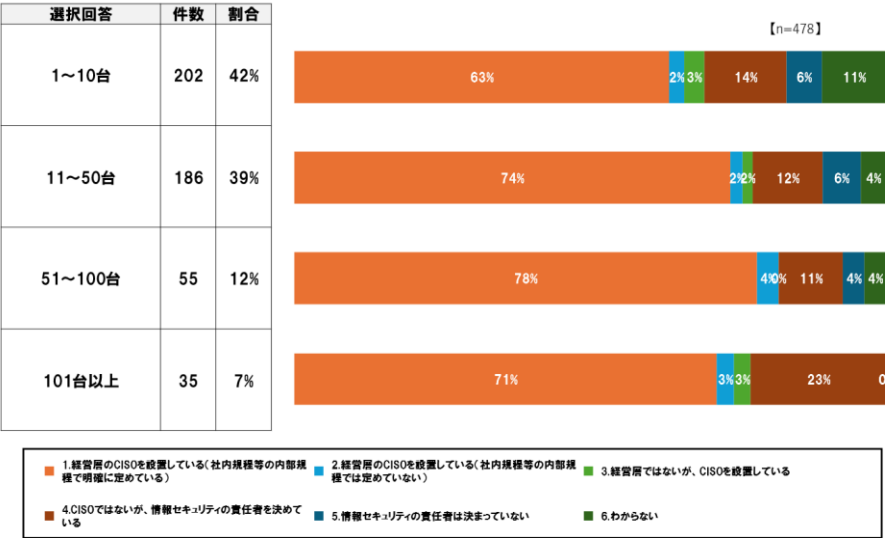


また、導入時期をベースとして分類したところ、自治体では年々「CISO」が減少し「情報セキュリティ責任者」設置が増加していることが分かった。さらに、導入規模をベースとして分類すると、規模が大きいほど責任者を設置している率が高いことがわかる。

図表 1-28a セキュリティ責任者の設置（Q27）（導入時期ベース）



図表 1-28b セキュリティ責任者の設置（Q27）（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。

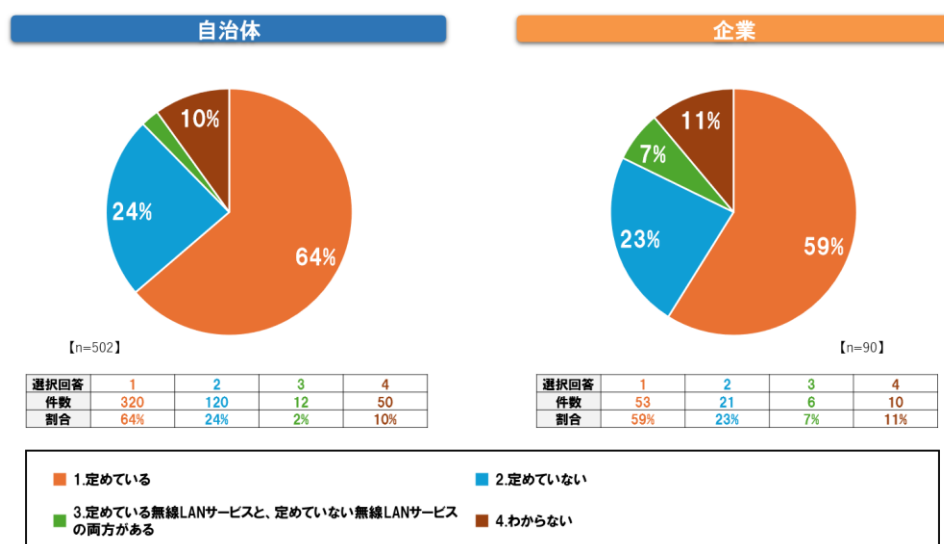
- ✓ 利用規約を定めている率について、自治体は横ばいであったが、企業団体は大幅に増加した。
- ✓ またサービス導入が最近になるほど利用規約を定めている率が低下していることが分かった。
- ✓ 初期画面については、企業団体の「初期画面を設けていない」率が減少した。
- ✓ データ保護の認識について、企業団体は昨年に比べ増加した。
- ✓ それ以外のデータは、例年通り、基本的に規模の大きな団体ほどいろいろな対策していることが分かった。

● 無線 LAN サービスの利用規約 (Q28)

利用規約を定めている率は、自治体は横ばい、企業は前年より増加した。

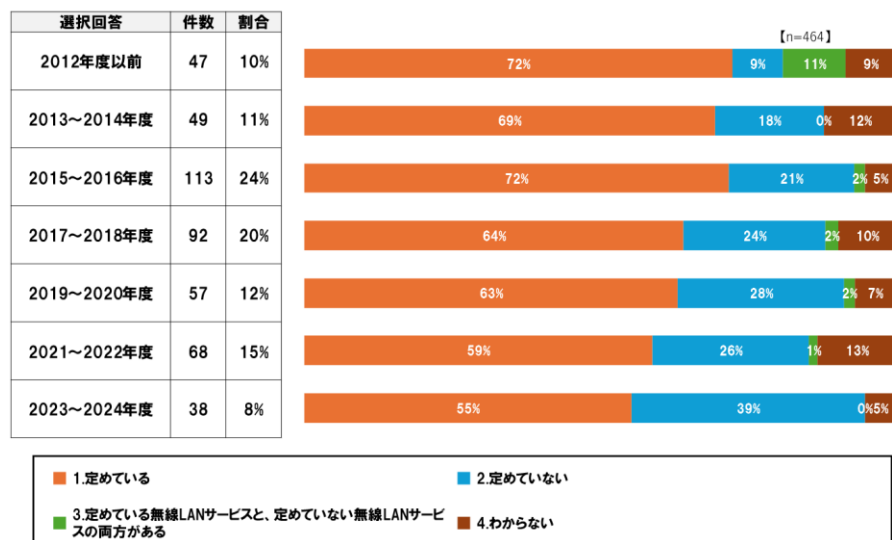
(自治体：67%→70%→67%、企：58%→39%→59%)。

図表 1-29 無線 LAN サービスの利用規約 (Q28)

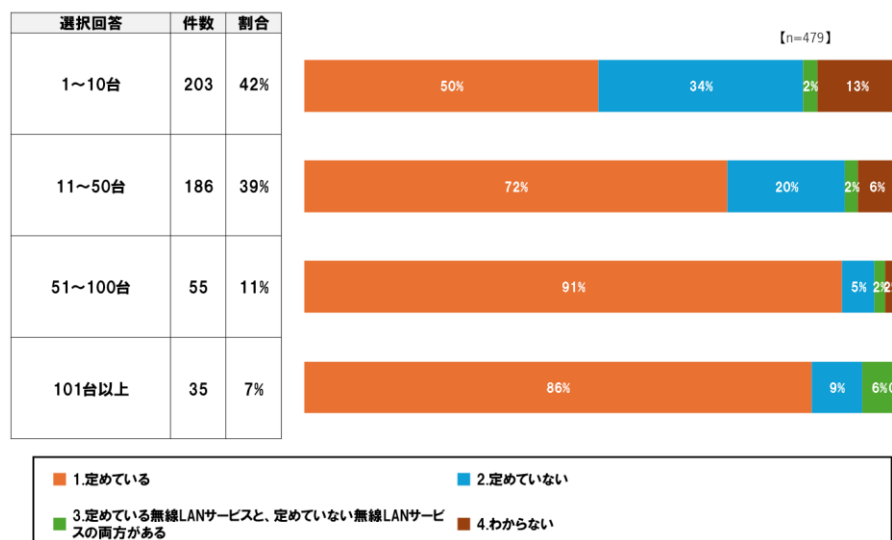


また、導入時期をベースとして分類すると、年々「利用規約を定めている」率が減少していることが分かった。さらに、導入規模をベースとして分類すると、規模が大きいほど「利用規約を定めている」率が高いことがわかる。

図表 1-29a 無線 LAN サービスの利用規約 (Q28) (導入時期ベース)



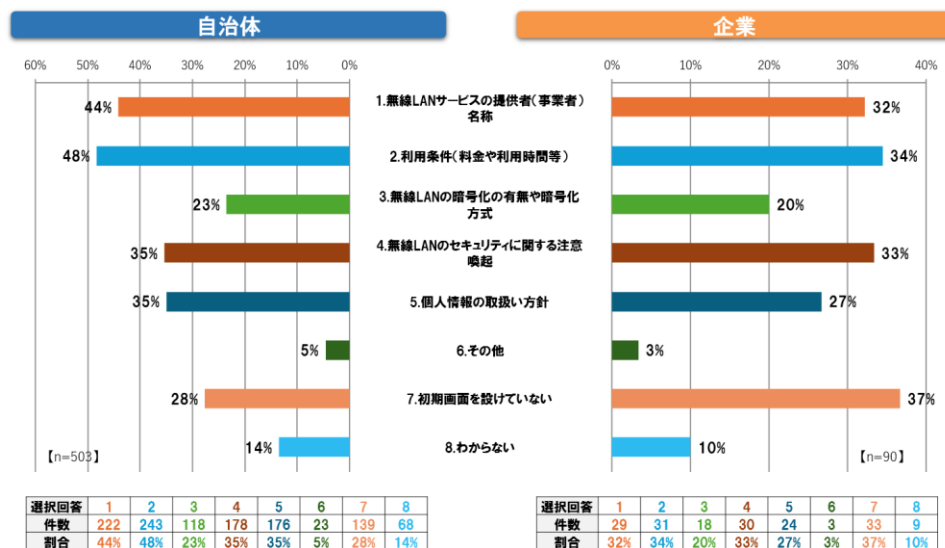
図表 1-29b 無線 LAN サービスの利用規約（Q28）（導入規模ベース）



● 無線 LAN サービスの初期画面（Q29）

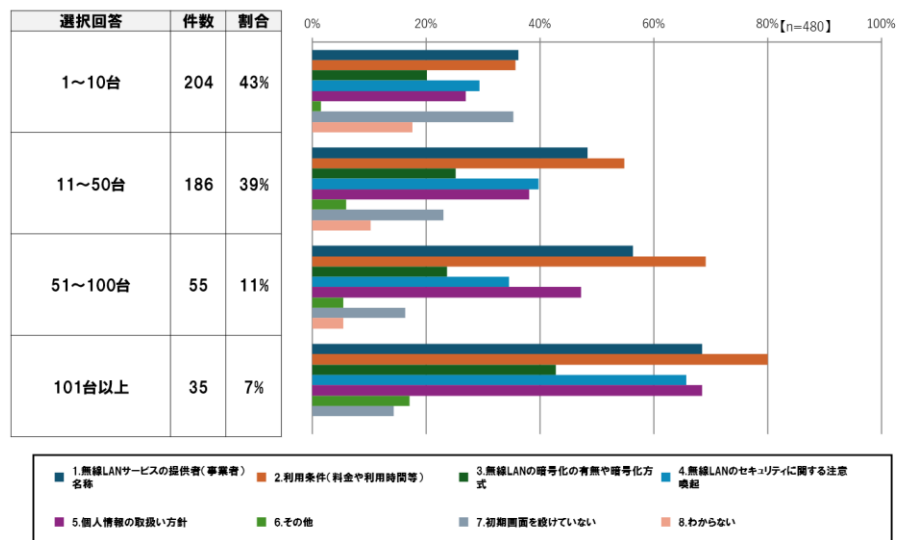
自治体は前年と同様の傾向だが、企業は「初期画面を設けていない」率が減少している（57%→51%→37%）。

図表 1-30 無線 LAN サービスの初期画面（Q29）



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「利用規約を定めている」率が高いことがわかる。

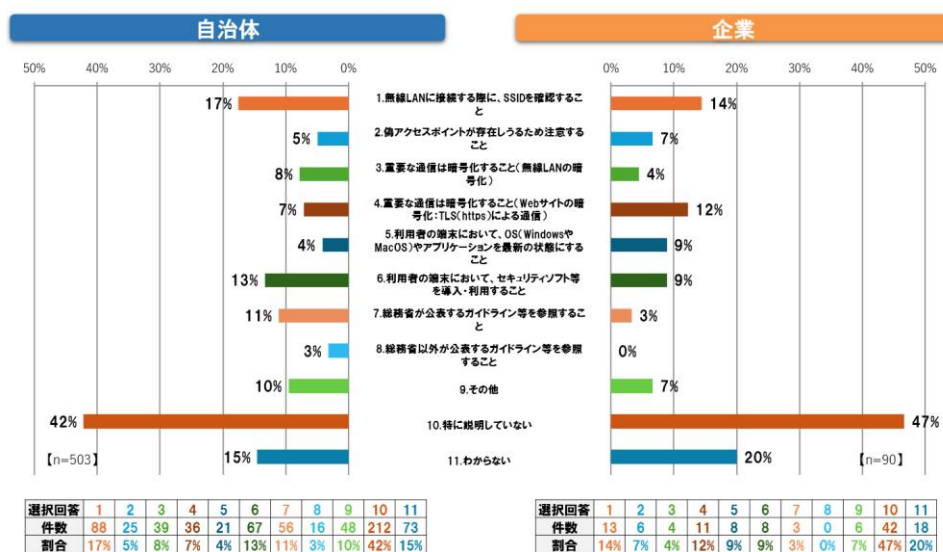
図表 1-30b 無線 LAN サービスの初期画面（Q29）（導入規模ベース）



### ● セキュリティに関する注意喚起（Q30）

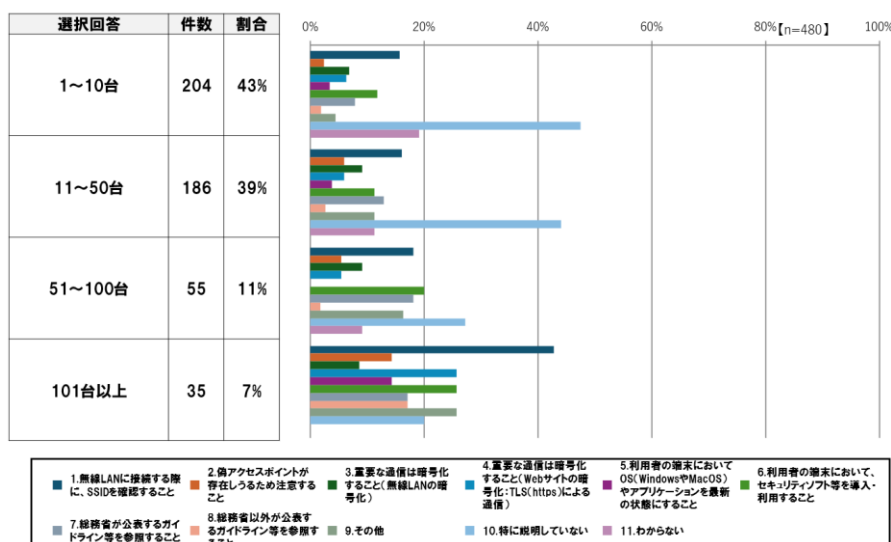
自治体は前年と同様の傾向だが、企業は「特に説明していない」率が減少している（63%→52%→47%）。

図表 1-31 セキュリティに関する注意喚起（Q30）



また、導入規模をベースとして分類すると、規模が小さいほど「特に説明していない」という事例が多いことがわかる。

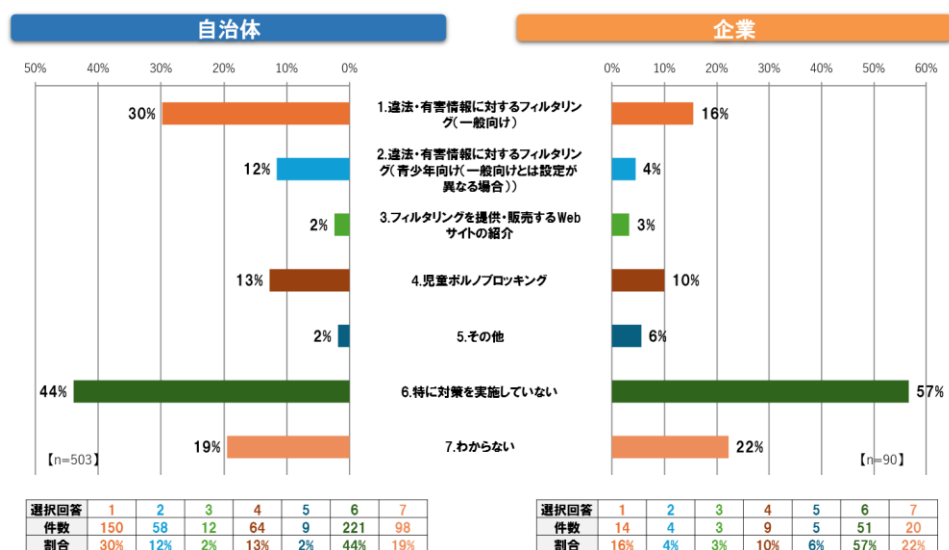
図表 1-31b セキュリティに関する注意喚起（Q30）（導入規模ベース）



### ● 違法・有害情報への対策（Q31）

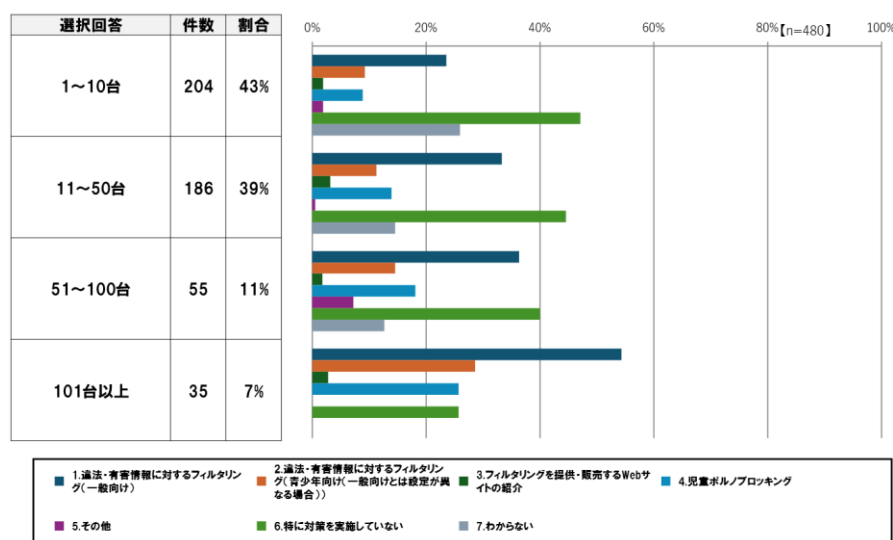
前年と同様の傾向で「特に対策を実施していない」が多い。

図表 1-32 違法・有害情報への対策（Q31）



また、導入規模をベースとして分類すると、規模が大きいくほど何らかの対策をしている率が高いことがわかる。

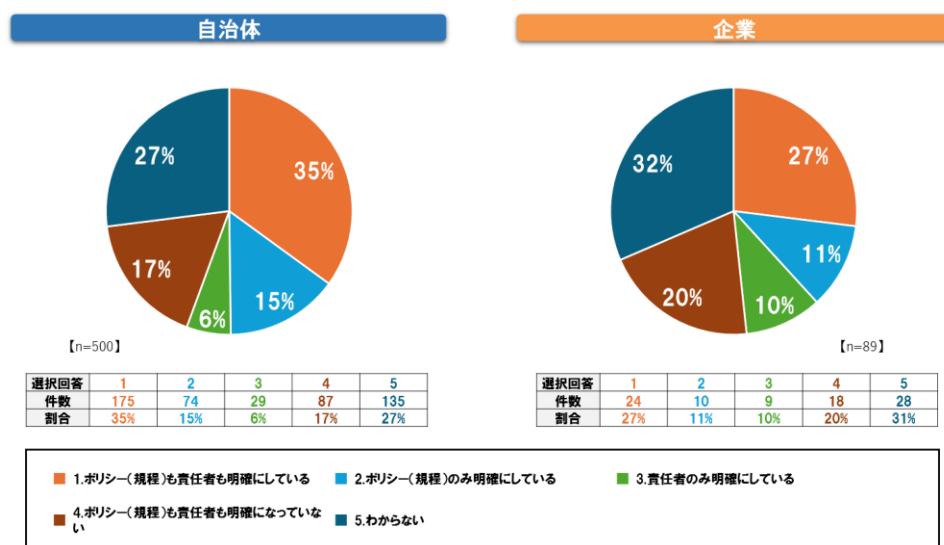
図表 1-32b 違法・有害情報への対策（Q31）（導入規模ベース）



### ● 利用者情報のデータ保護（Q32）

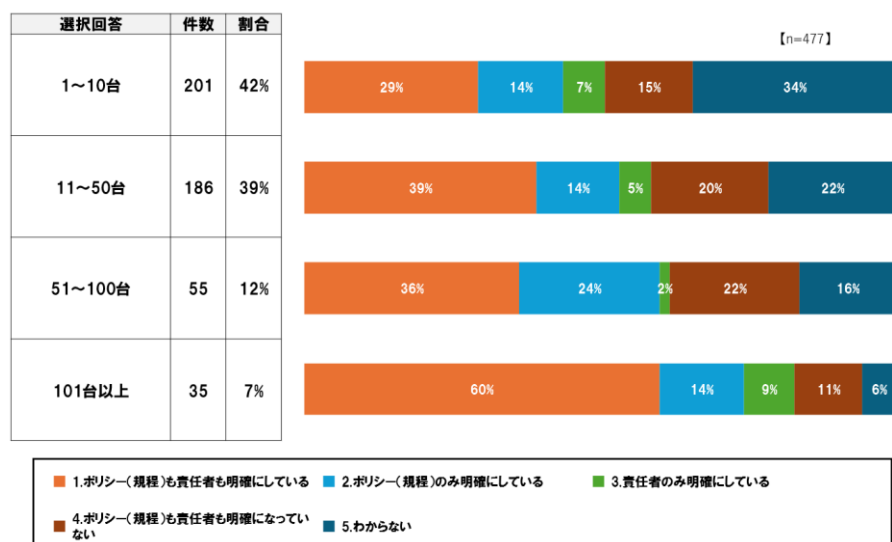
前年と同様の傾向であり、利用者情報のデータ保護に対して何らかの対応をしている率は、地方自治体が企業の37%に比べ高い。データ保護の認識は企業は増加（自治体54%→57%→56%、企業43%→36%→48%）

図表 1-33 利用者情報のデータ保護（Q32）



また、導入規模をベースとして分類すると、規模が大きいほど何らかの対策をしている率が高いことがわかる。

図表 1-33b 利用者情報のデータ保護（Q32）（導入規模ベース）



#### （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。

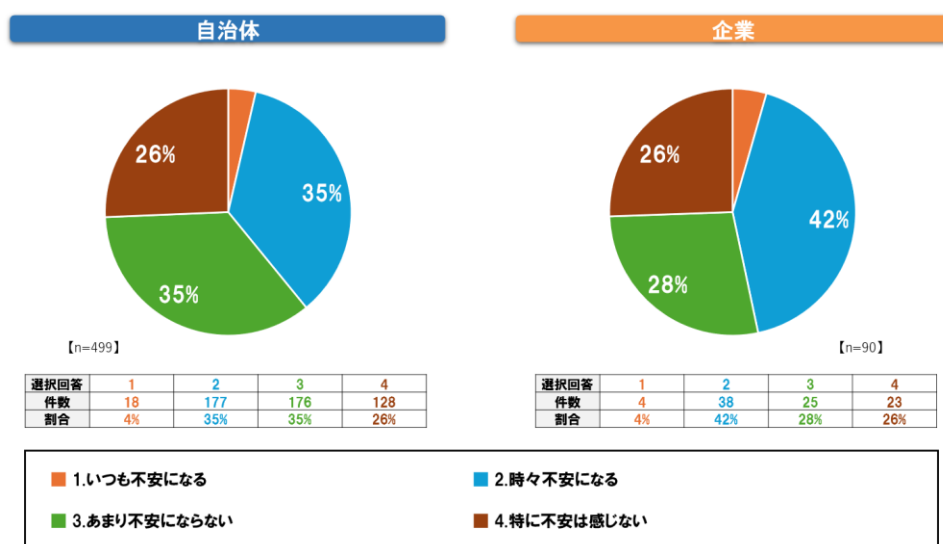
- ✓ セキュリティに対する不安がある団体は自治体、企業ともに横ばい状態。

- ✓ 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企業は、昨年に比べ大きく増加した。これらは、新型コロナウイルス感染症の5類移行に伴い、再び投資計画の拡大につながっていると考えられる。
- ✓ 新規技術として、Wi-Fi 6 及び Wi-Fi 6E/7 の導入あるいは導入検討をしている率は増加傾向であることが分かった。
- ✓ セキュリティの手引きの認知率は、自治体は横ばい、企業団体は増加した。
- ✓ セキュリティの手引きについて「参考になった」率は自治体、企業団体ともに増加傾向。

● サービスのセキュリティへの不安（Q33）

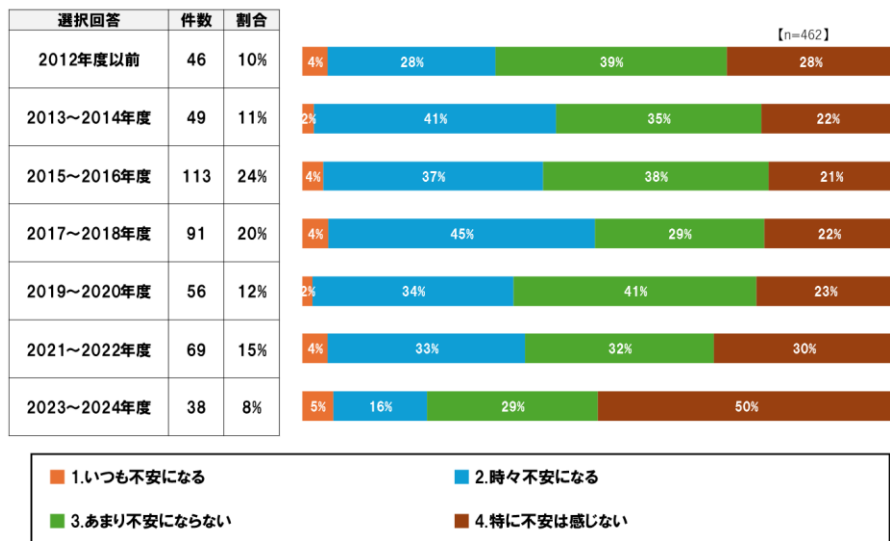
自治体は横ばいだが、企業は不安の比率が徐々に増加している（自治体：38%→43%→39%、企業：36%→43%→46%）。

図表 1-34 サービスのセキュリティへの不安（Q33）



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

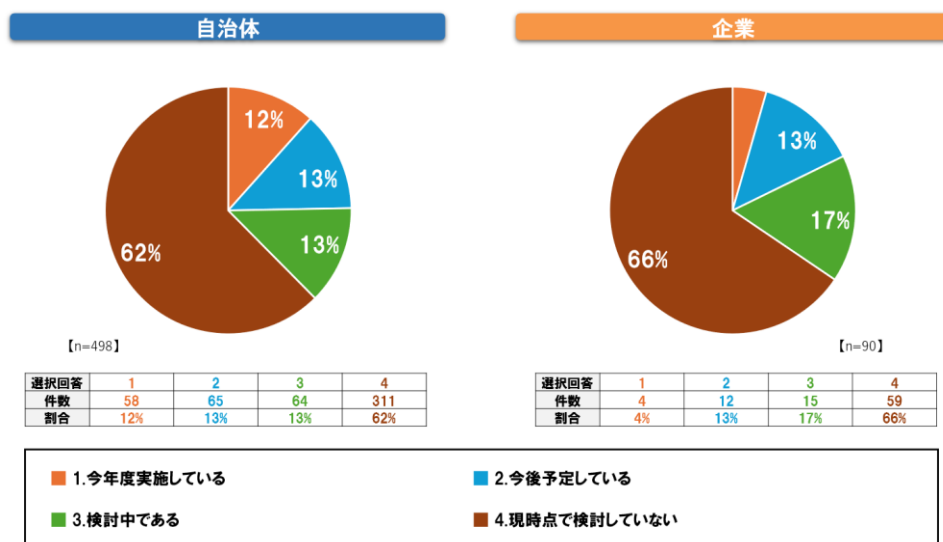
図表 1-34a サービスのセキュリティへの不安（Q33）（導入時期ベース）



● サービスの設備拡充や更改計画（Q34）

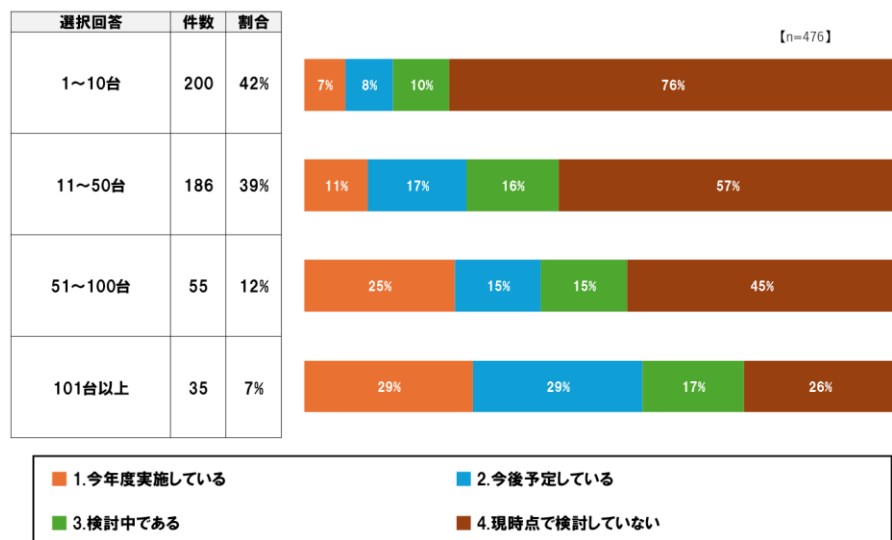
前年に比べ、自治体で設備拡充や更改計画を実施・検討している率が増加（自治体 29%→32%→38%、企業 38%→37%→34%）

図表 1-35 サービスの設備拡充や更改計画（Q34）



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。

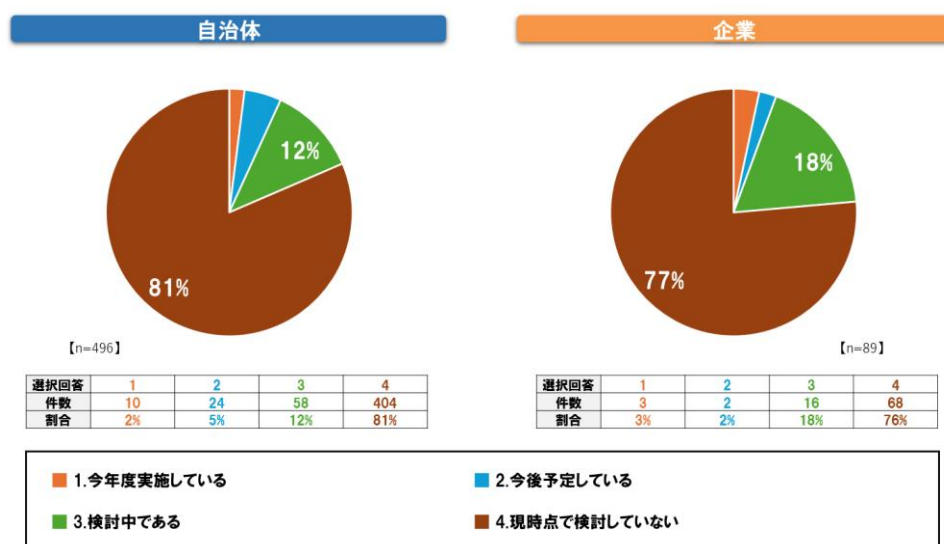
図表 1-35b サービスの設備拡充や更改計画（Q34）（導入規模ベース）



● サービスのセキュリティ強化計画（Q36）

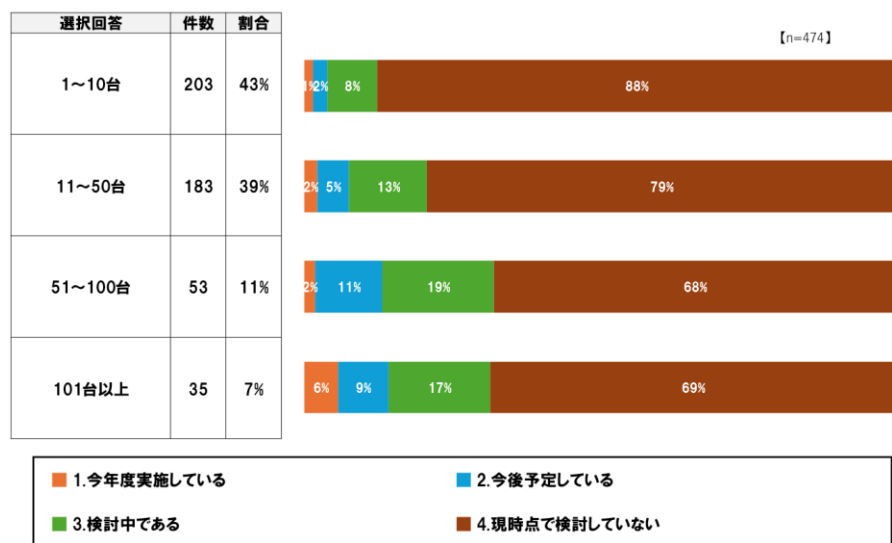
セキュリティ強化について、実施・検討している割合が再び増加（自治体 13%→3%→19%、企業 19%→4%→23%）

図表 1-36 サービスのセキュリティ強化計画（Q36）



また、導入規模をベースとして分類すると、規模が大きいほどセキュリティ強化を実施あるいは計画している率が高いことがわかる。

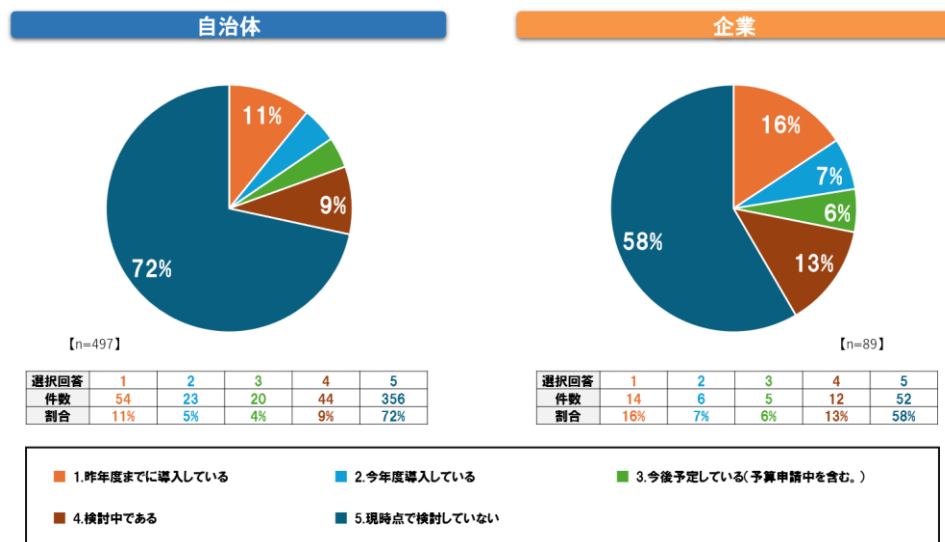
図表 1-36b サービスのセキュリティ強化計画（Q36）（導入規模ベース）



● Wi-Fi 6 の導入予定（Q38）

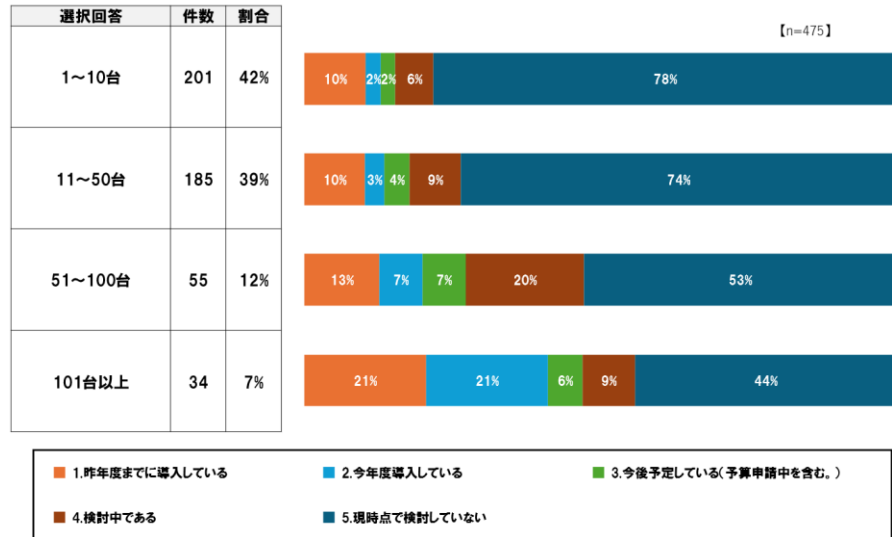
Wi-Fi 6 の導入更改を実施検討している割合は着実に増加（自治体 18%→23%→28%、企業 27%→32%→42%）

図表 1-37 Wi-Fi 6 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。

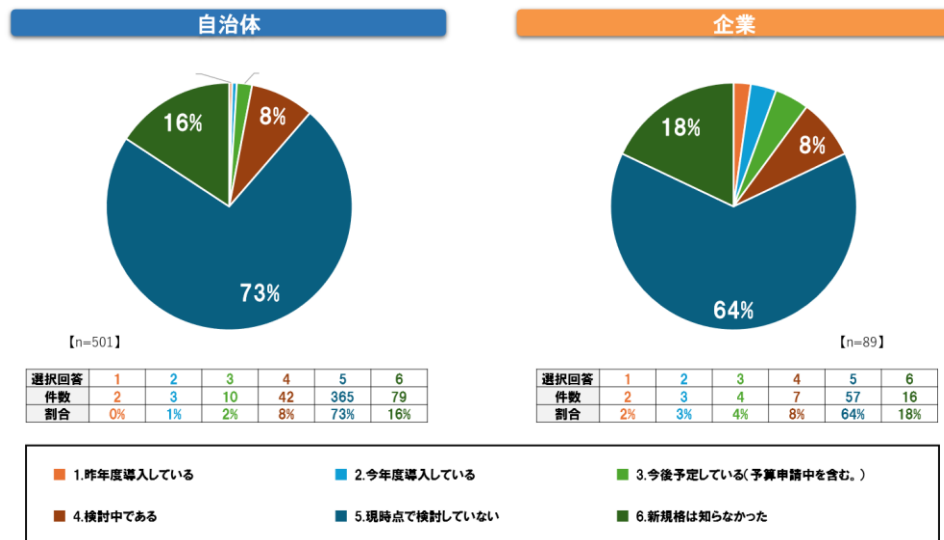
図表 1-37b Wi-Fi 6 の導入予定 (Q38) (導入規模ベース)



● Wi-Fi 6E/7 の導入予定 (Q39)

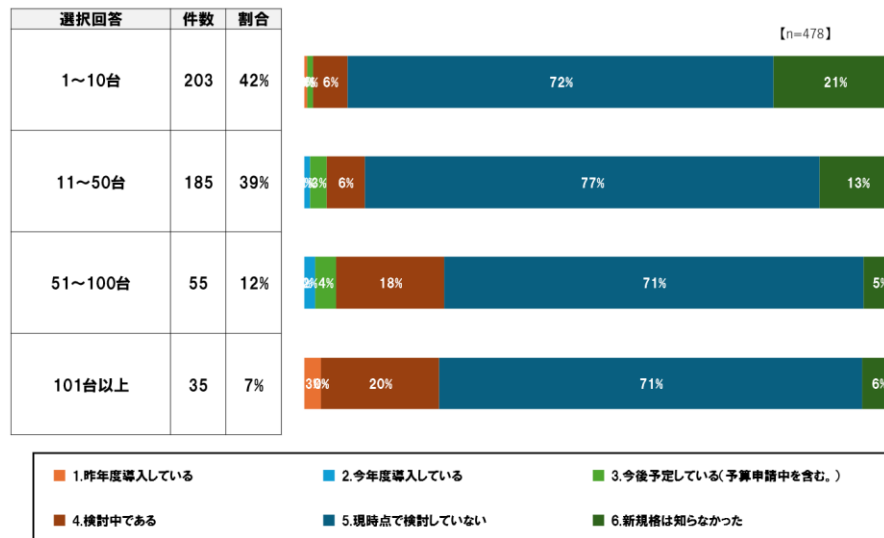
実施検討している割合は増加傾向 (自治体 6%→7%→11%、企業 10%→23%→18%)。

図表 1-38 Wi-Fi 6E/7 の導入予定 (Q39)



また、導入規模をベースとして分類すると、規模が大きいほど Wi-Fi 6E/7 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。

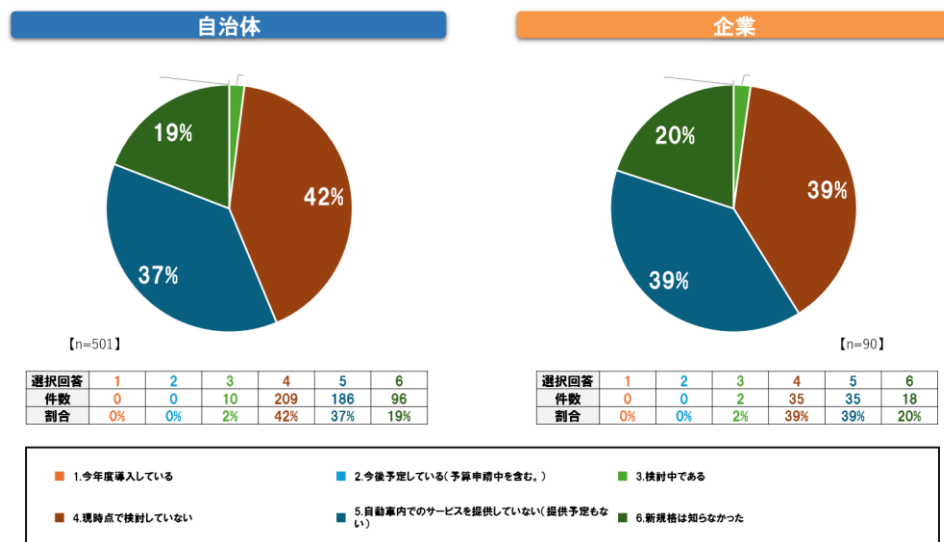
図表 1-38b Wi-Fi 6E/7 の導入予定（Q39）（導入規模ベース）



● 5.2GHz 自動車内利用の導入予定（Q40）

導入を検討している割合は自治体、企業ともに 2%程度。

図表 1-39 5.2GHz 自動車内利用の導入予定（Q40）

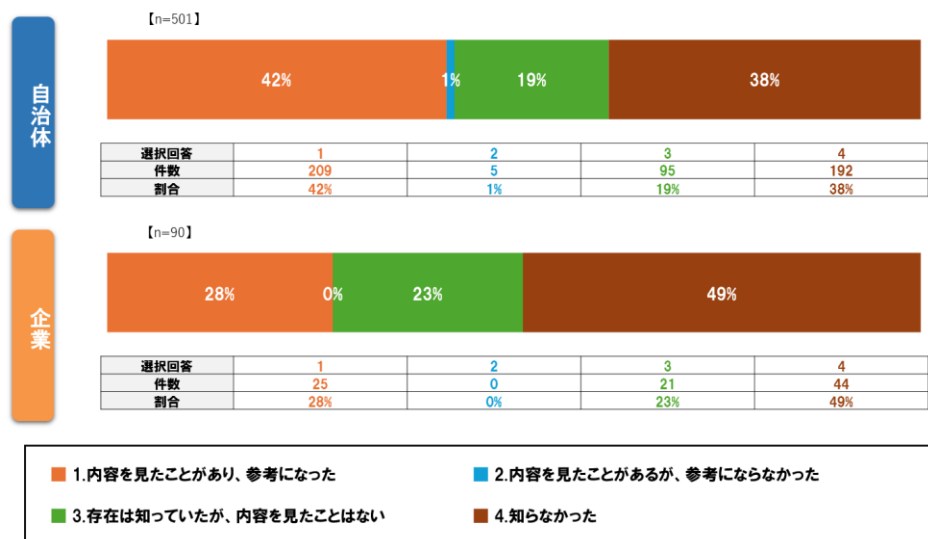


● セキュリティ対策の手引き（Q41）

「手引き」の内容を見た団体の率は横ばい。自治体（39%→42%→43%）、企業（26%→21%

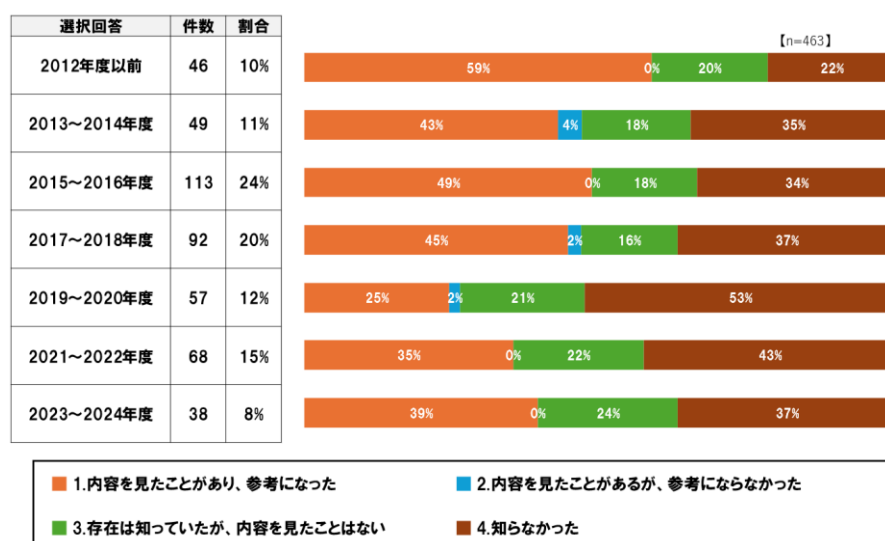
→28%)。

図表 1-40 セキュリティ対策の手引き (Q41)

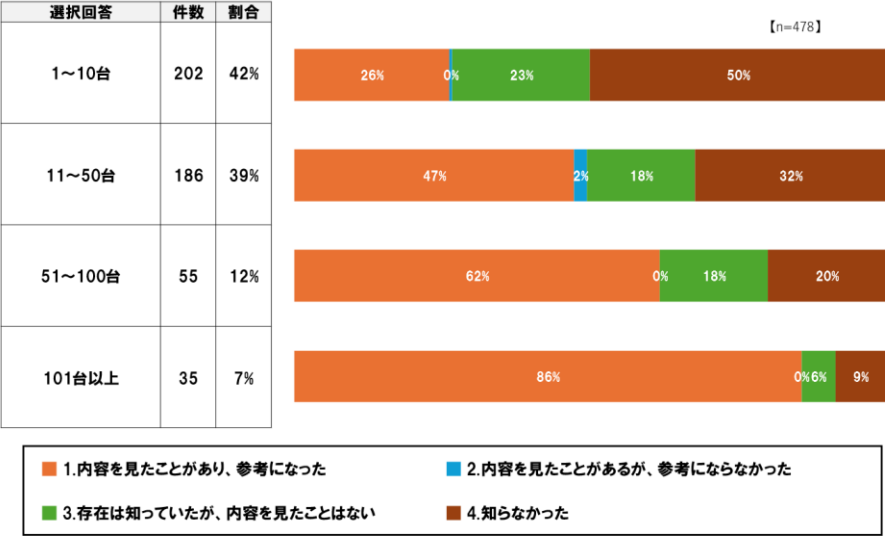


また、サービスの導入時期をベースとして分類したところ、コロナ時期（2020 年頃）に見ている率が減少したが最近は回復していることが分かった。さらに、サービスの導入規模をベースとして分類したところ、規模が大きいものほど「手引き」を認識している率が高いことが分かった。

図表 1-40a セキュリティ対策の手引き (Q41) (導入時期ベース)



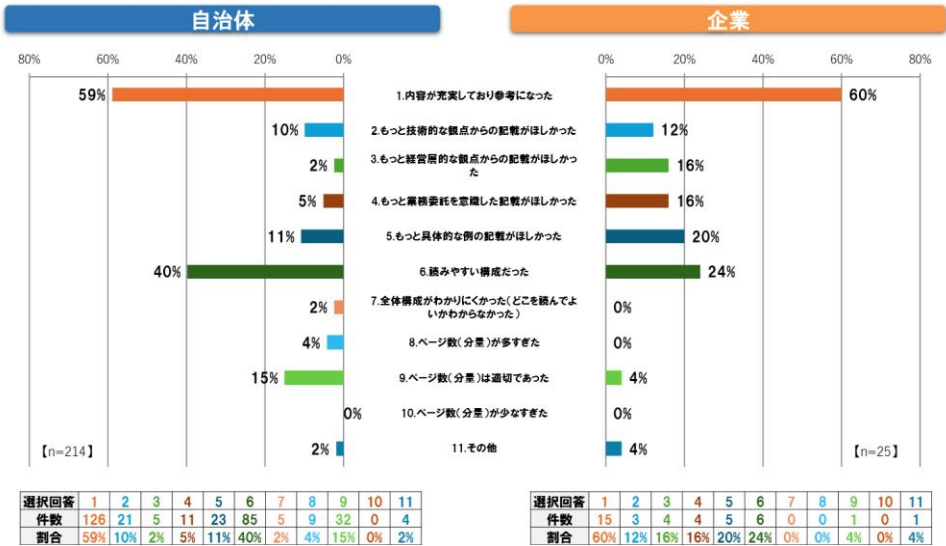
図表 1-40b セキュリティ対策の手引き（Q41）（導入規模ベース）



● セキュリティ対策の手引きの内容（Q42）

手引きの内容については、自治体は良い評価が増加した（自治体：52%→54%→59%、企業：41%→46%→60%）。

図表 1-41 セキュリティ対策の手引きの内容（Q42）



#### (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。娯楽遊戯施設については分計してまとめたが、サンプル数が少ないため考察の対象外とした。

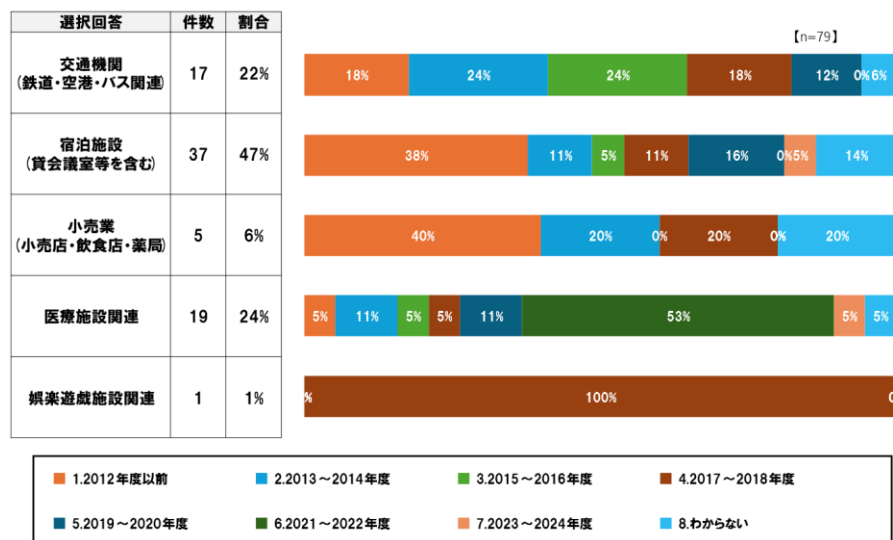
回答には以下のような特徴がみられた。

- ✓ 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、小売業、医療関連施設が多く、「観光客の誘客」は交通機関、宿泊施設、小売業に多い。なお「通信事業者からの依頼」については交通機関と宿泊施設にあるが、小売業はなくなった。
- ✓ 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、宿泊施設や医療機関は暗号化率が高い（昨年と同様の傾向）。
- ✓ 宿泊施設は、セキュリティの責任者が決まっていない事例が多く、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い。なお、セキュリティ強化を検討している率が高い（インバウンドの復活が理由である可能性あり）。
- ✓ 医療関係は、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認識、関心も高い（年々高くなっている傾向がある）。また、医療施設はコロナ中にサービスの整備に前向きな回答が多かったが、現在は落ち着いている。

#### ● 無線 LAN サービスの導入時期（Q2）

医療施設関連は 2021～2022 年度の導入が 5 割以上を占めており、極めて高い比率を示している。

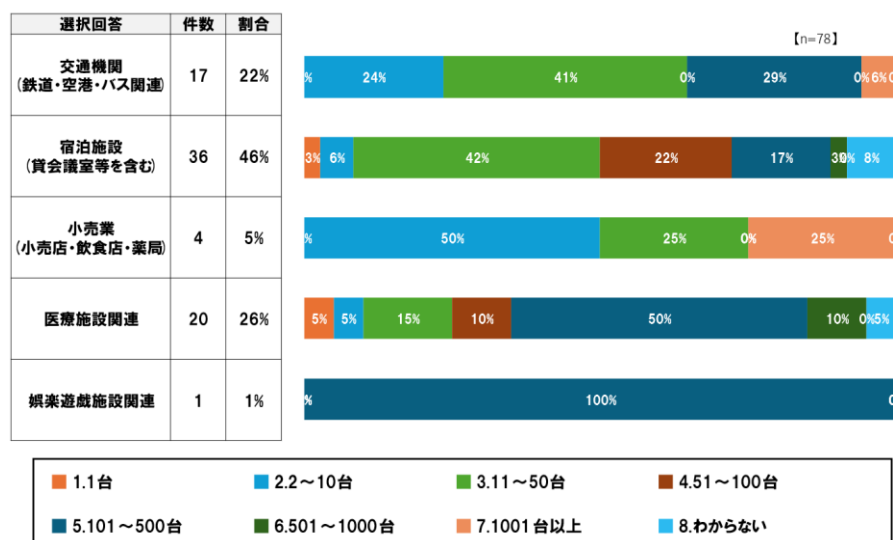
図表 1-42 無線 LAN サービスの導入時期（Q2）（業種ベース）



● 無線 LAN サービスの規模（Q5）

医療施設関連は大規模（AP100 台以上）のサービスが多く、宿泊関連は中規模（AP100 台以下）のサービスが多い。

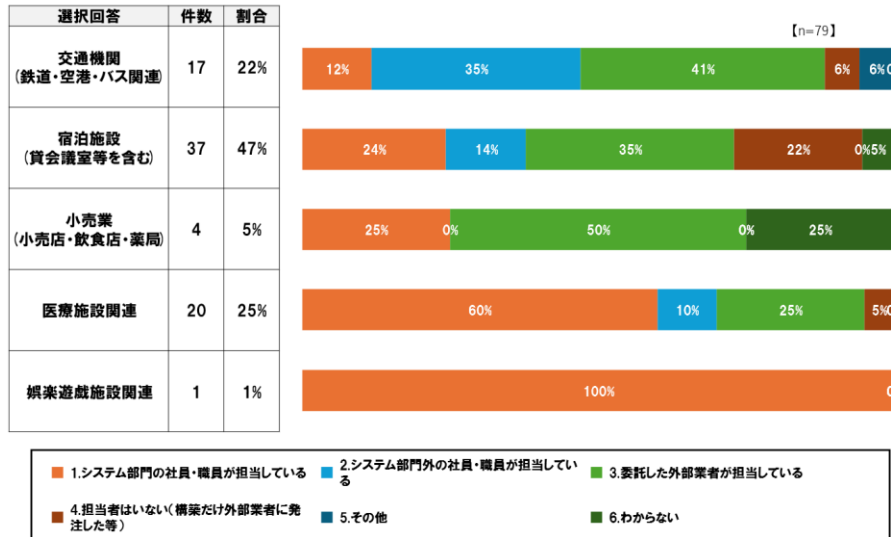
図表 1-43 無線 LAN サービスの規模（Q5）（業種ベース）



● 無線 LAN サービスの運用管理（Q6）

医療施設関連は、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他の部門と比べて極めて高いことが分かった。

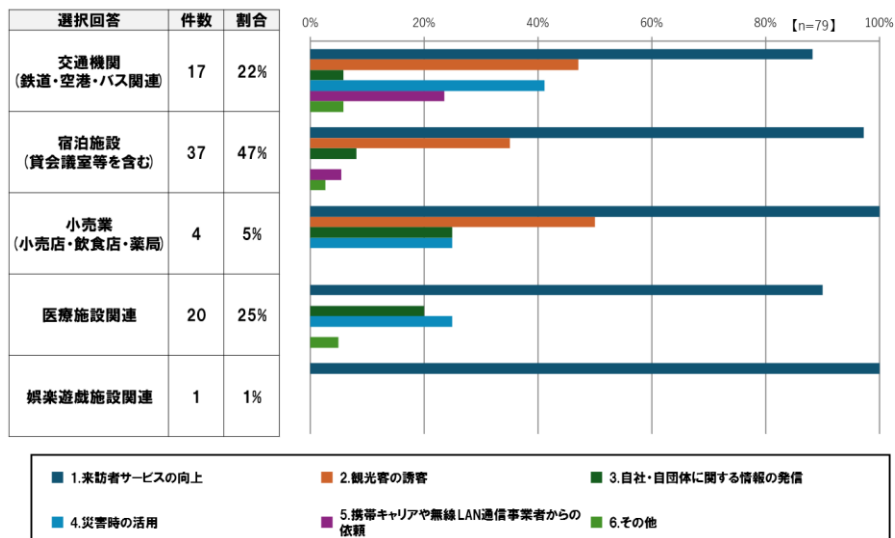
図表 1-44 無線 LAN サービスの運用管理（Q6）（業種ベース）



● 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、また医療機関関連以外は「観光客の誘客」が次に多い。また「災害時の活用」は交通機関、小売業、医療関連施設に多い。なお、昨年は何社かあった小売業の「通信事業者からの依頼」については本年はなくなった。

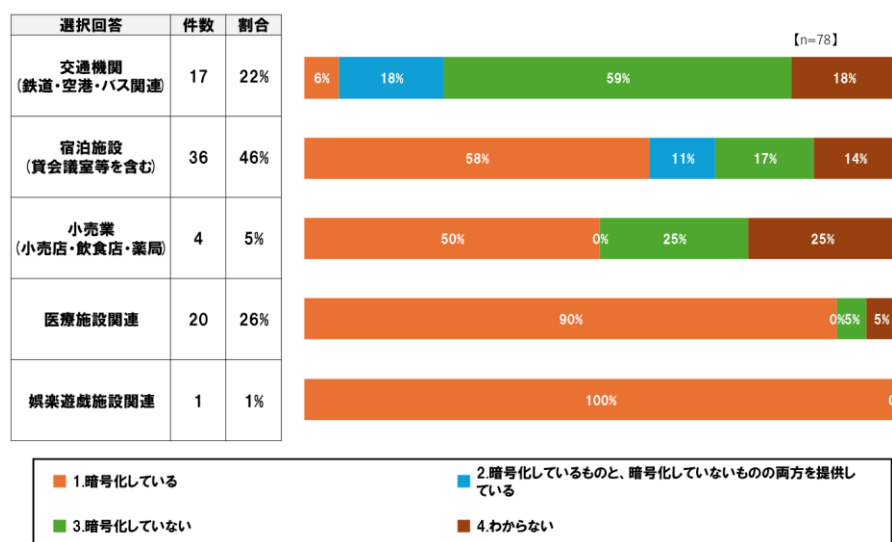
図表 1-45 無線 LAN サービスの目的（Q7）（業種ベース）



● 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）。逆に宿泊施設や医療関連は、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。

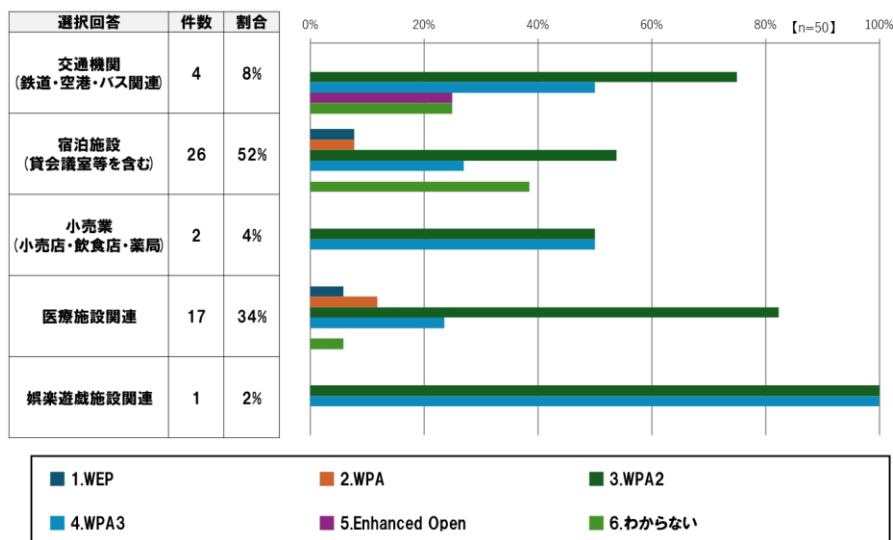
図表 1-46 無線 LAN サービスの暗号化（Q9）（業種ベース）



● 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/WPA が使われているのは、今回のデータについては宿泊施設、医療施設関連のみであることが分かった（昨年は交通機関にもみられたが今年のデータはなし）。

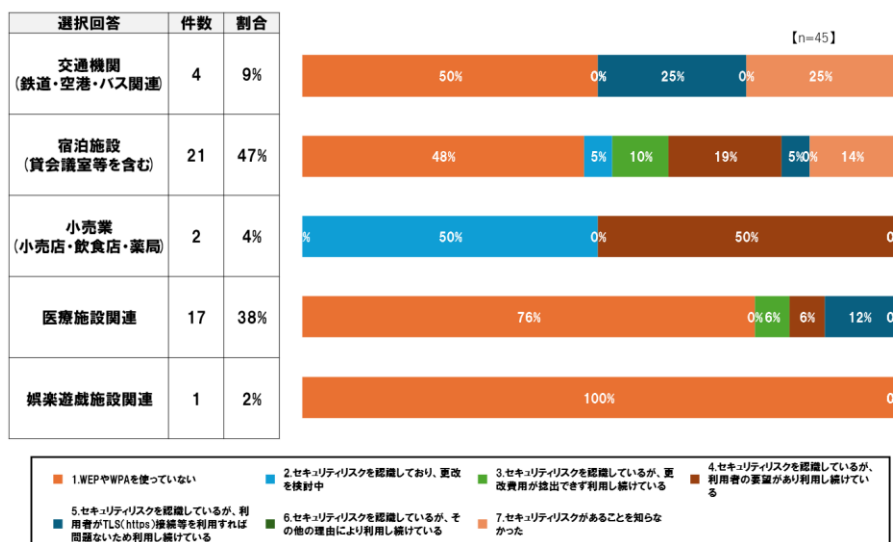
図表 1-47 無線 LAN サービスの暗号化方式（Q10）（業種ベース）



● 暗号化方式のセキュリティリスク (Q11)

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いことが分かった。

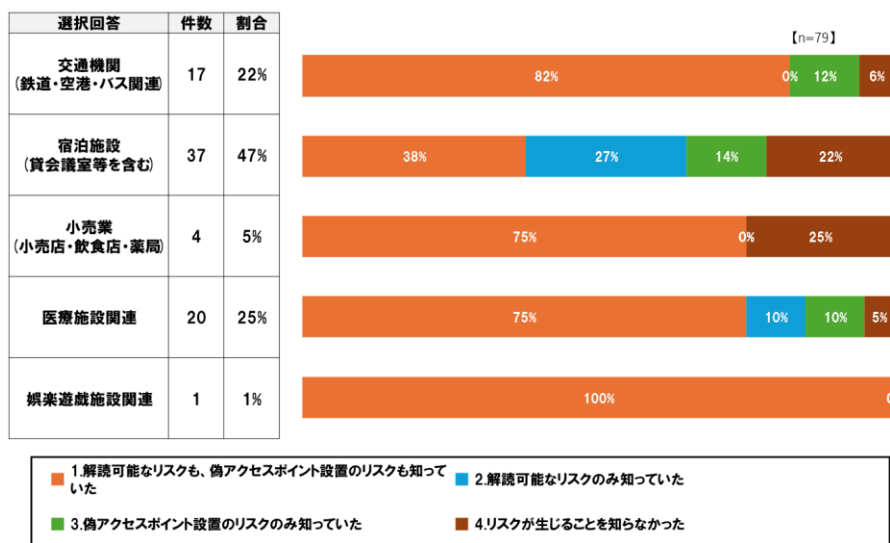
図表 1-48 無線 LAN サービスのセキュリティリスク (Q11) (業種ベース)



● セキュリティリスクに対する認識 (Q13)

宿泊施設や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。一方、医療機関は、年々認識率が向上している (50%→71%→75%)

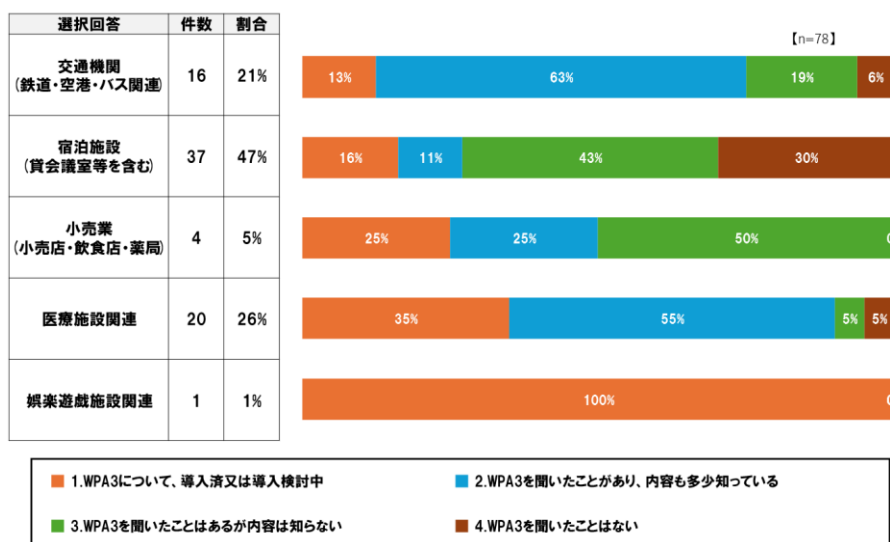
図表 1-49 セキュリティリスクに対する認識（Q13）（業種ベース）



● 新しい暗号化方式（WPA3）（Q14）

宿泊施設は他に比べ「WPA3」の認知度は低い。

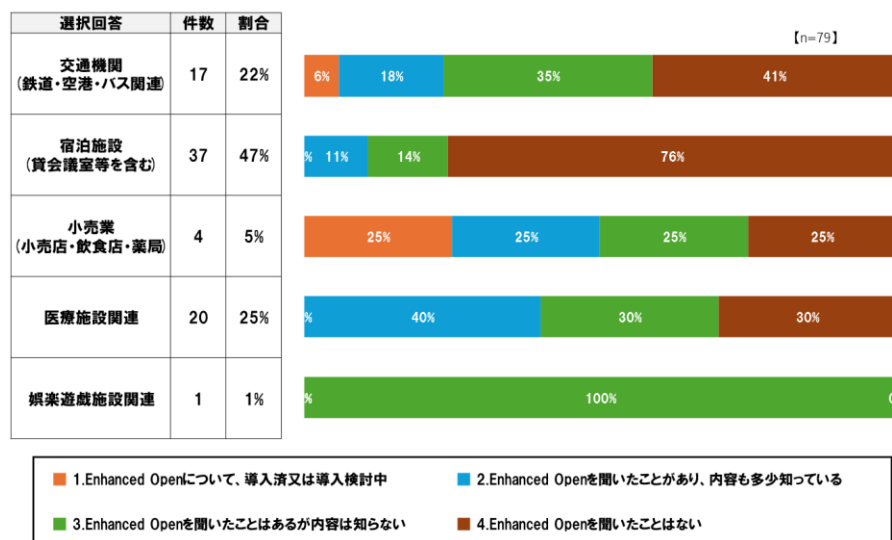
図表 1-50 新しい暗号化方式（WPA3）（Q14）（業種ベース）



● 新しい暗号化方式（Enhanced Open）（Q15）

宿泊施設は他に比べ「Enhanced Open」の認知度は低い。

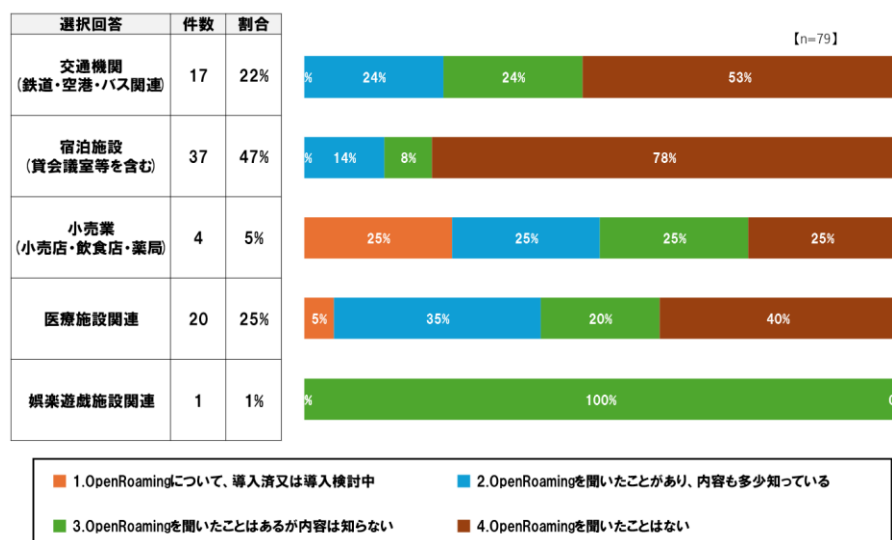
図表 1-51 新しい暗号化方式（Enhanced Open）（Q15）（業種ベース）



● 新しい暗号化方式（OpenRoaming）（Q16）

宿泊施設は他に比べ「OpenRoaming」の認知度は低い。

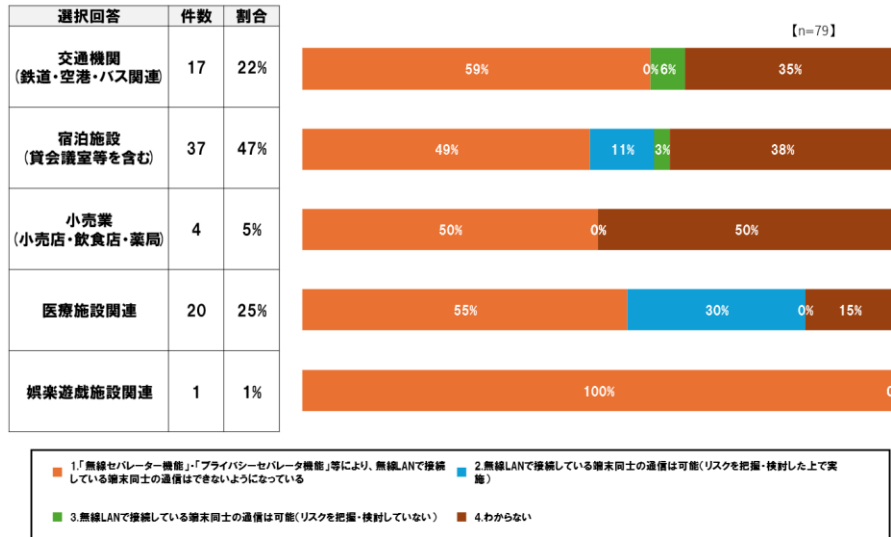
図表 1-52 新しい認証暗号化方式（OpenRoaming）（Q16）（業種ベース）



● 端末同士の折り返し通信（Q17）

交通機関は前年と同様に折り返し通信を認めていない事例が多い。宿泊施設、医療関連は意識して折り返し通信を認めている事例がある。

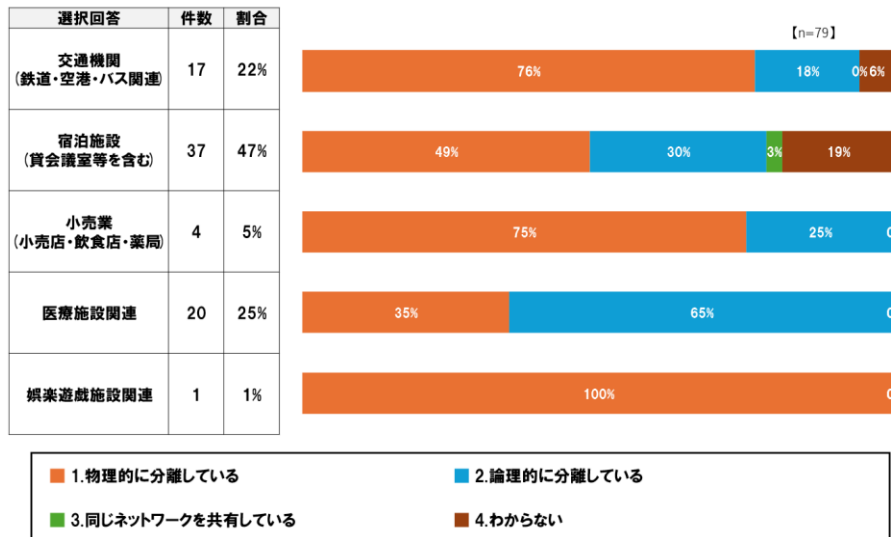
図表 1-53 端末同士の折り返し通信（Q17）（業種ベース）



● 業務用ネットワークとの分離（Q21）

交通機関は物理的に分離、医療機関は論理的に分離の率が高い。

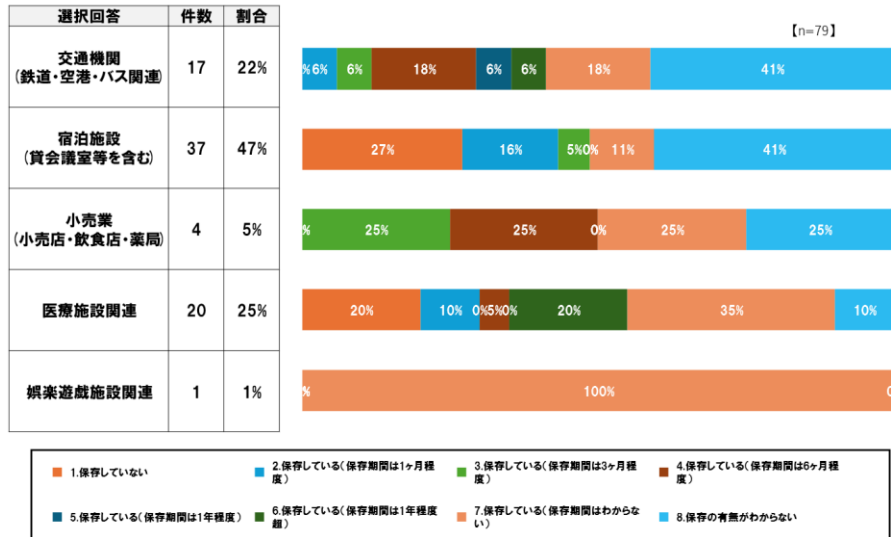
図表 1-54 業務用ネットワークとの分離（Q21）（業種ベース）



● アクセスログ（通信記録等）の保存（Q24）

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。

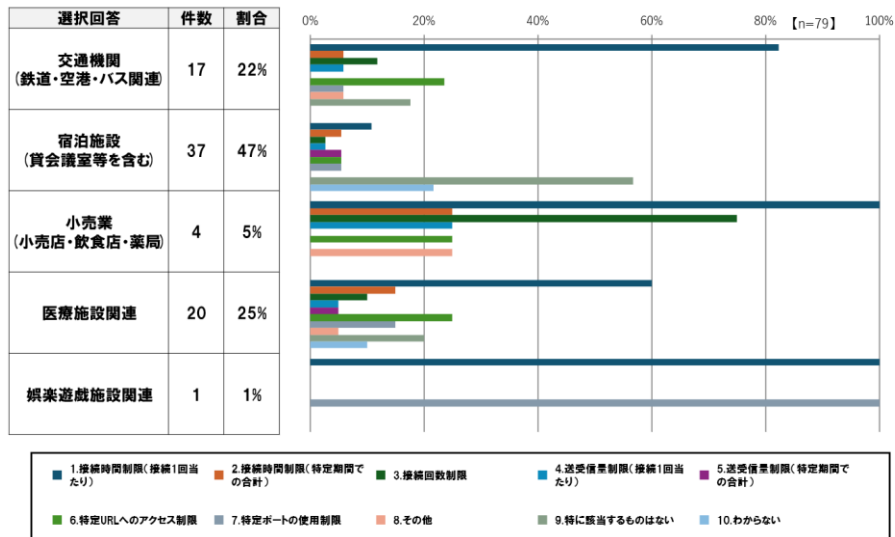
図表 1-55 アクセスログ（通信記録等）の保存（Q24）（業種ベース）



● その他のセキュリティ対策（Q26）

医療施設は年々、制限事項の設定を追加している割合が増加している。

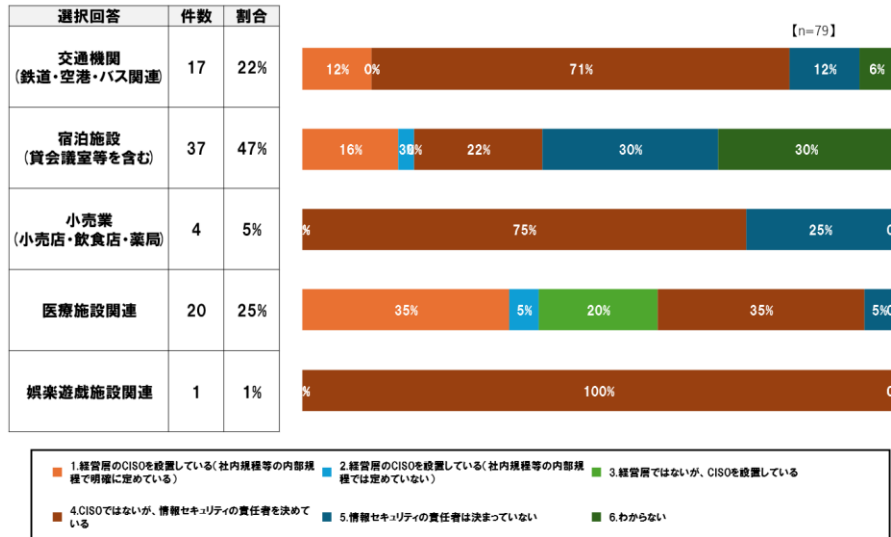
図表 1-56 その他のセキュリティ対策（Q26）（業種ベース）



● 情報セキュリティ責任者の設置（Q27）

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」事例が多く半数を超えている。

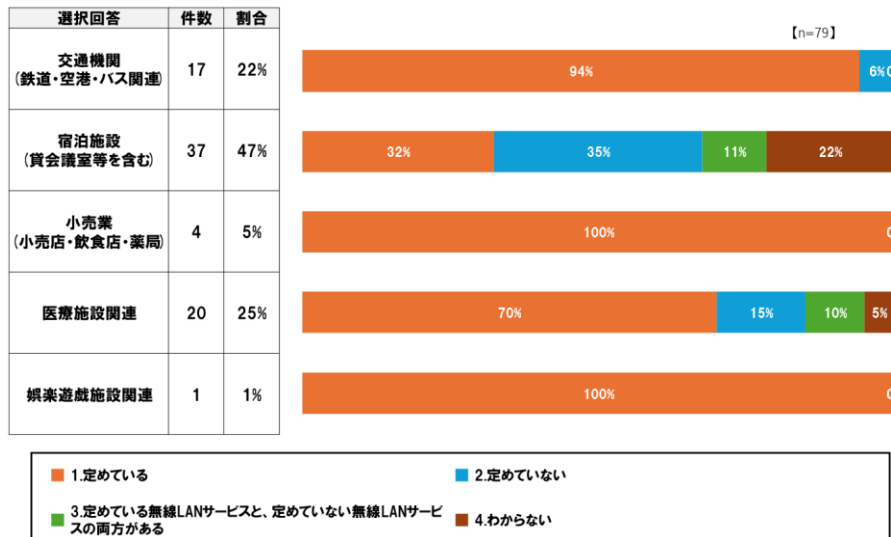
図表 1-57 情報セキュリティ責任者の設置（Q27）（業種ベース）



● 無線 LAN サービスの利用規約（Q28）

宿泊施設は、他の業種に比べ利用規約を定めている率が低い。

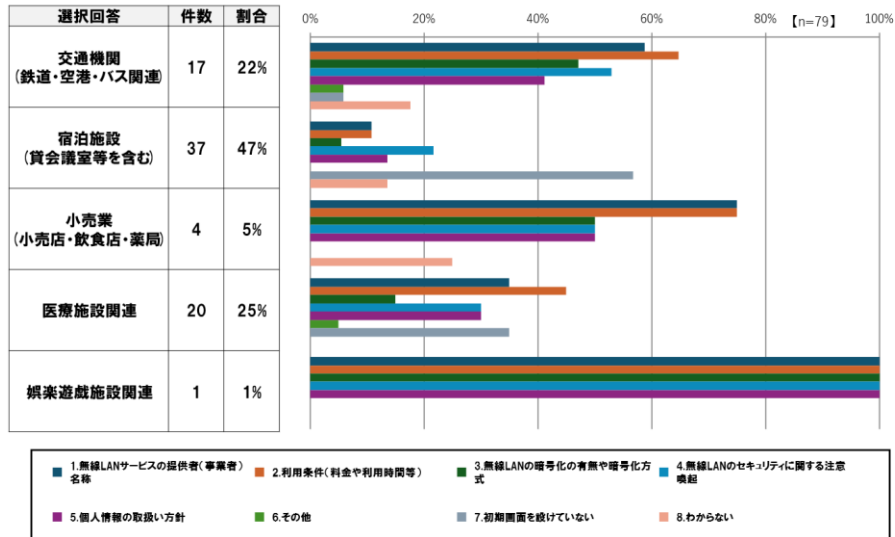
図表 1-58 無線 LAN サービスの利用規約（Q28）（業種ベース）



● 無線 LAN サービスの初期画面（Q29）

宿泊施設は、他の業種に比べ、初期画面を設けていない率が高い。

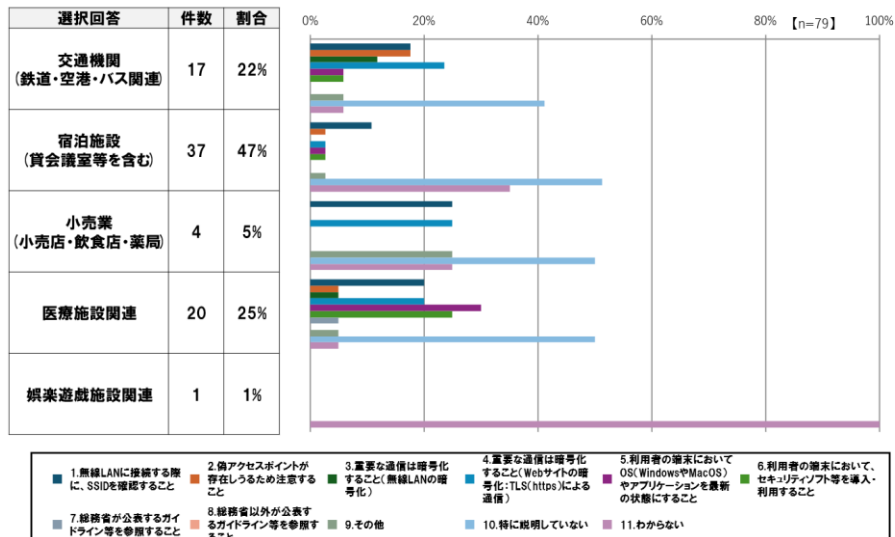
図表 1-59 無線 LAN サービスの初期画面（Q29）（業種ベース）



● セキュリティに関する注意喚起（Q30）

交通機関、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。

図表 1-60 セキュリティに関する注意喚起（Q30）（業種ベース）

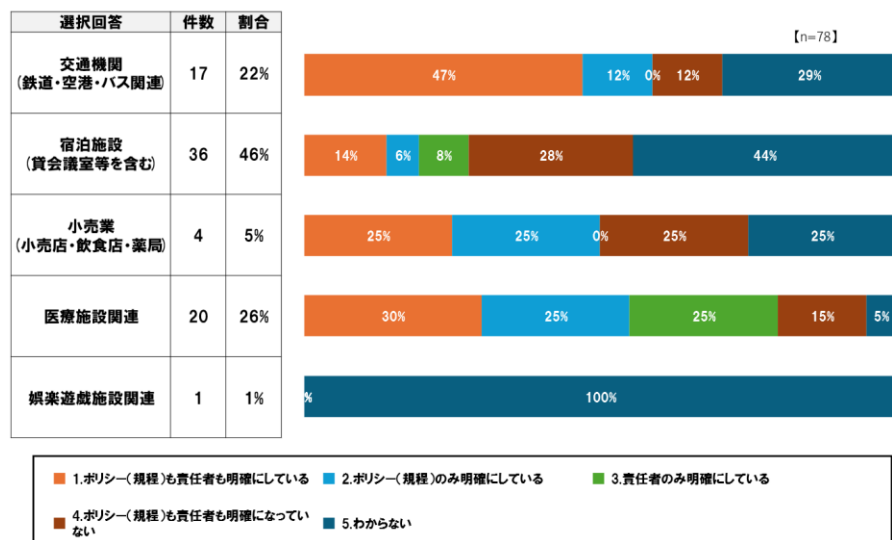


● 利用者情報のデータ保護（Q32）

宿泊施設は、他の業種に比べ、利用者情報保護のポリシーやデータ保護責任者が不明確

な事例が多い。

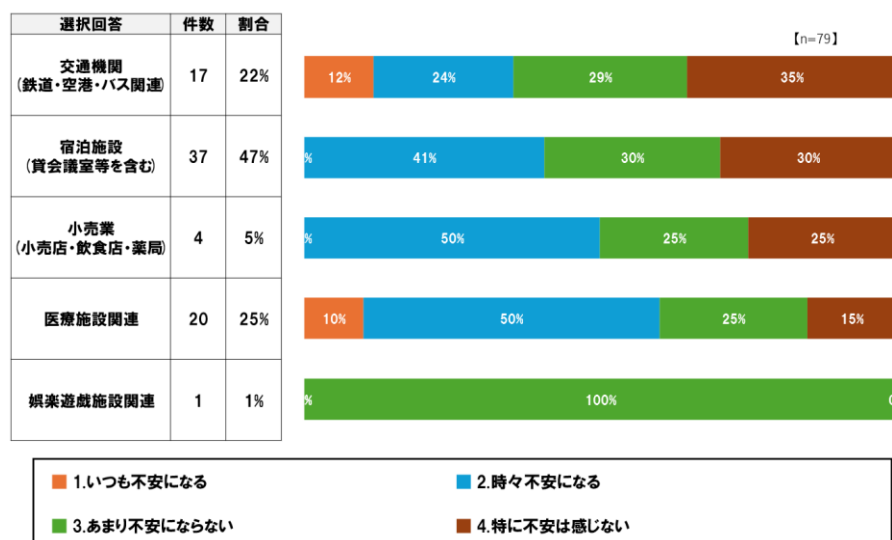
図表 1-61 利用者情報のデータ保護（Q32）（業種ベース）



● サービスのセキュリティへの不安（Q33）

医療関連施設はセキュリティに対する不安を持っている事例が多い。

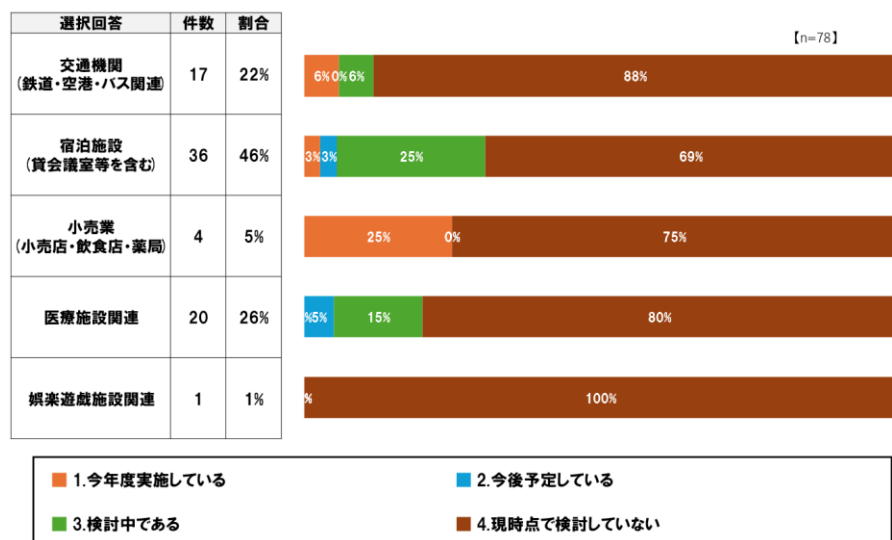
図表 1-62 サービスのセキュリティへの不安（Q33）（業種ベース）



● サービスのセキュリティ強化計画（Q36）

宿泊施設および医療関連施設はセキュリティ強化を検討している事例が多い。

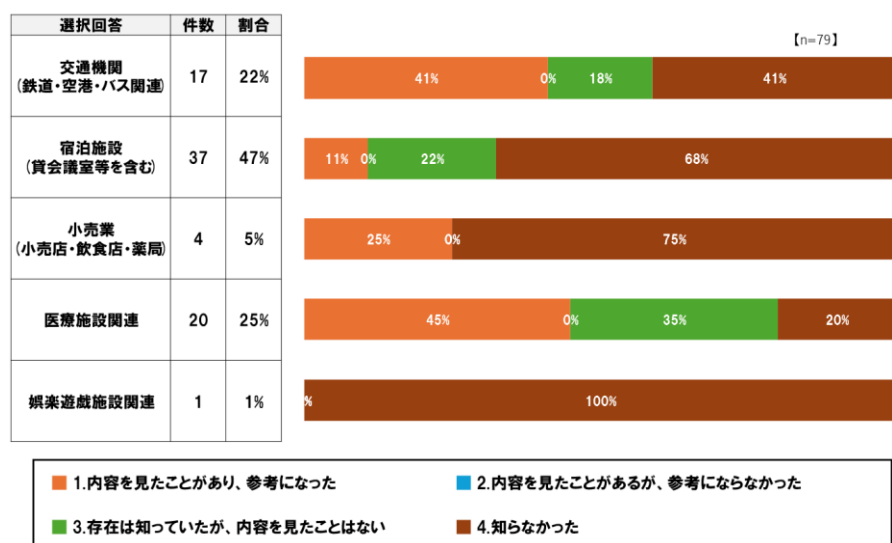
図表 1-63 サービスのセキュリティ強化計画（Q36）（業種ベース）



● セキュリティ対策の手引き（Q41）

交通機関や医療施設は「手引き」を参考にしている率が高く、宿泊施設は低い。

図表 1-64 セキュリティ対策の手引き（Q41）（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。

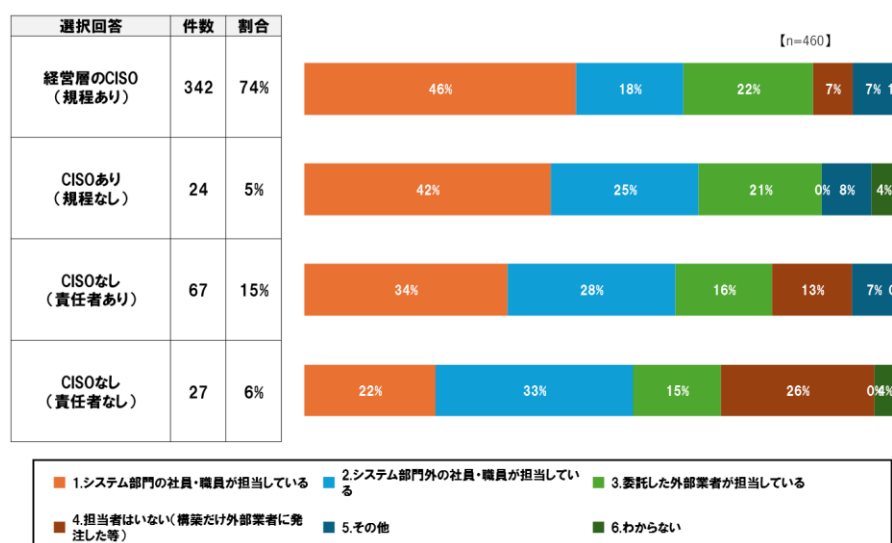
回答には、前年と同様に以下のような特徴がみられた。

- ✓ 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。

### ● 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。

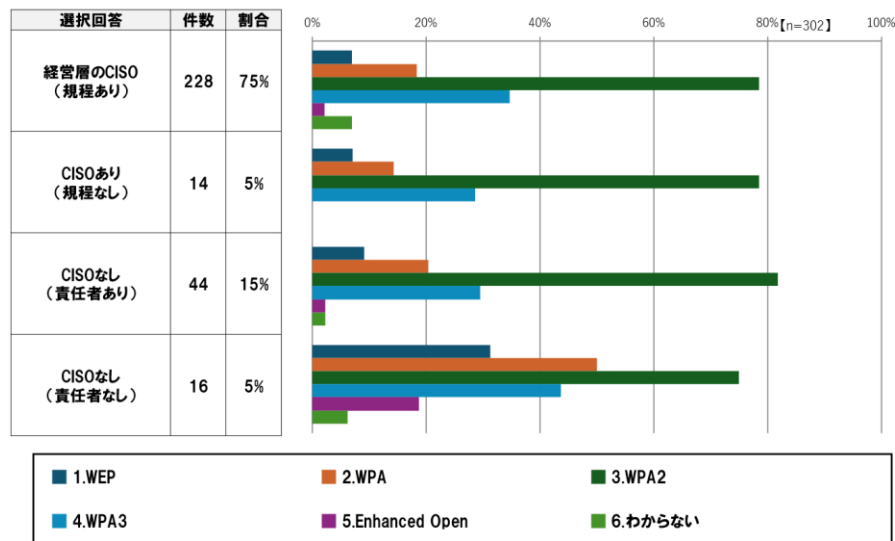
図表 1-65 無線 LAN サービスの運用管理（Q6）（管理者有無ベース）



### ● 無線 LAN サービスのセキュリティリスク（Q10）

セキュリティ責任者を設置していないところが、非推奨暗号化方式である（WEP/WPA）をいまだに利用している率が高い。

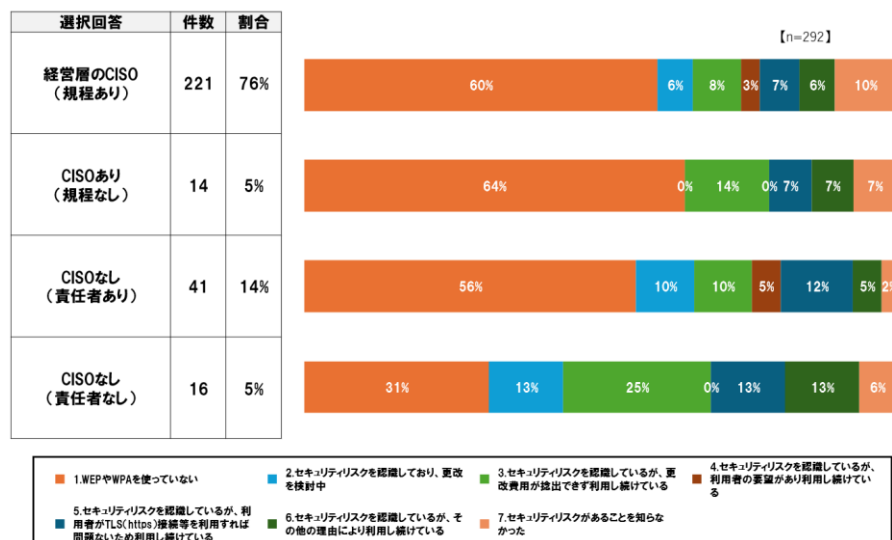
図表 1-66 無線 LAN サービスの暗号化方式（Q10）（管理者有無ベース）



● 無線 LAN サービスの暗号化方式 (Q11)

セキュリティ責任者を設置していないところが、非推奨暗号化方式である (WEP/WPA) をいまだに利用している率が高い。

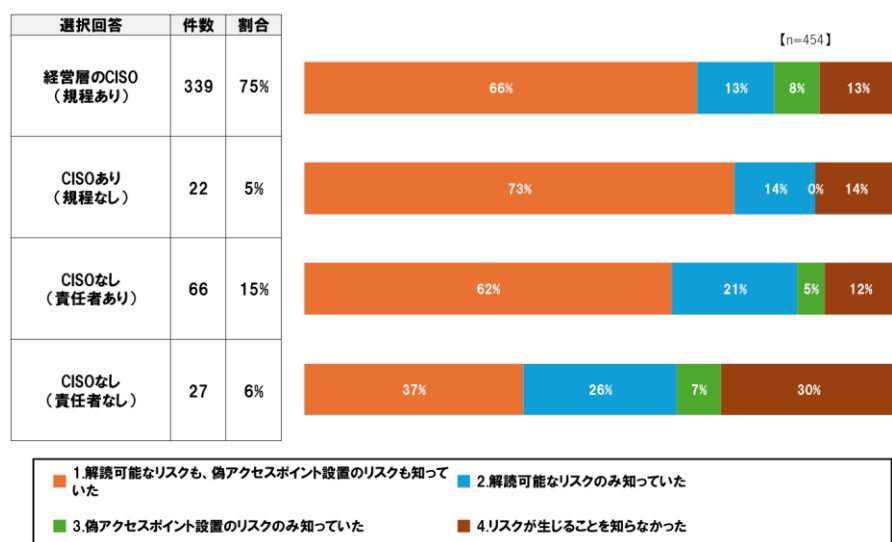
図表 1-67 無線 LAN サービスのセキュリティリスク (Q11) (管理者有無ベース)



● 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ないところは、セキュリティリスクの認識率が低い。

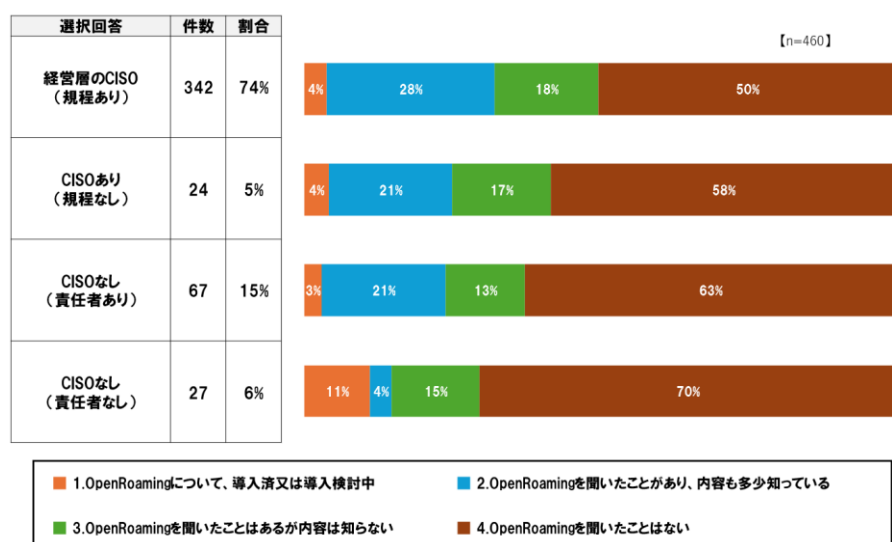
図表 1-68 セキュリティリスクに対する認識（Q13）（管理者有無ベース）



● 新しい暗号化方式（OpenRoaming）（Q16）

セキュリティ責任者を設置しているところは、新技術（OpenRoaming）の認識率が高い。昨年までは WPA3 や Enhanced Open など同様の傾向がみられたが、本年にはその傾向がなかった（既知の技術になったと思われる）。

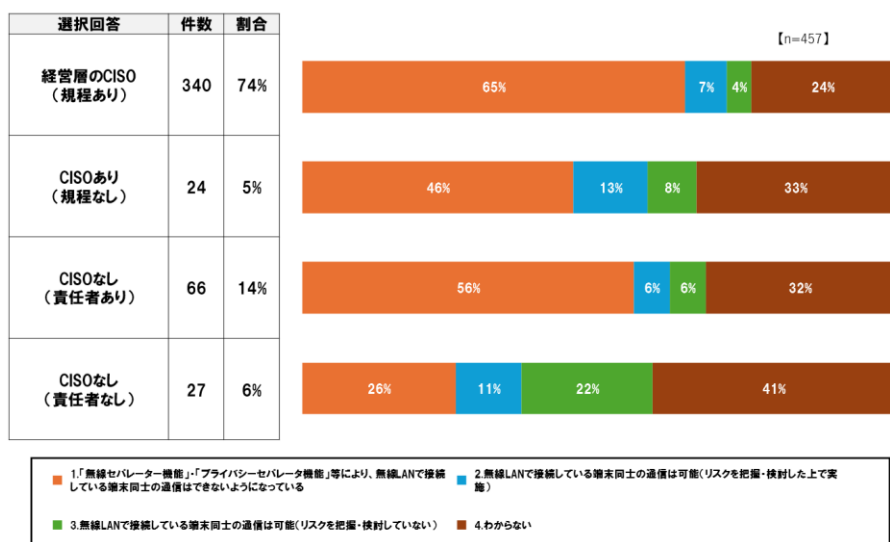
図表 1-69 新しい認証暗号化方式（OpenRoaming）（Q16）（管理者有無ベース）



● 端末同士の折り返し通信（Q17）

セキュリティ責任者のいないところは折り返し通信のリスクを把握していない率が高い。

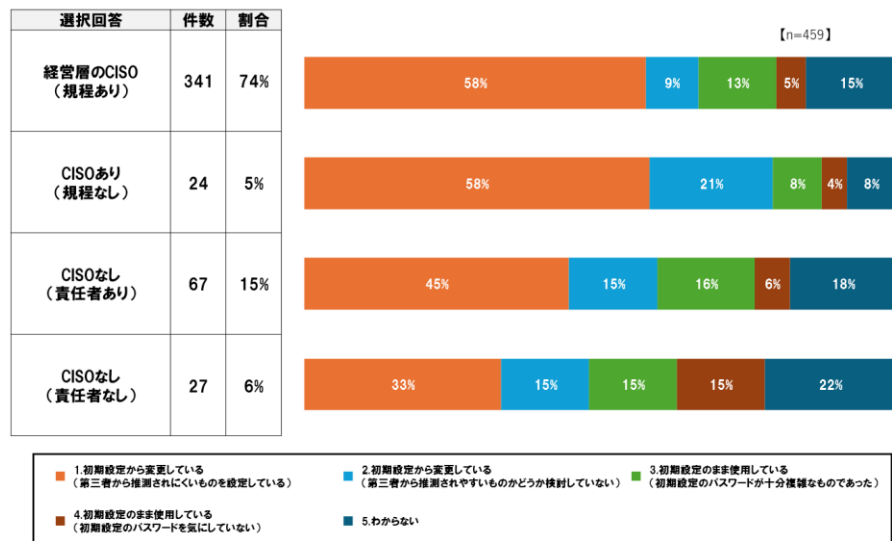
図表 1-70 端末同士の折り返し通信（Q17）（管理者有無ベース）



● 管理者パスワードの管理（Q19）

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。

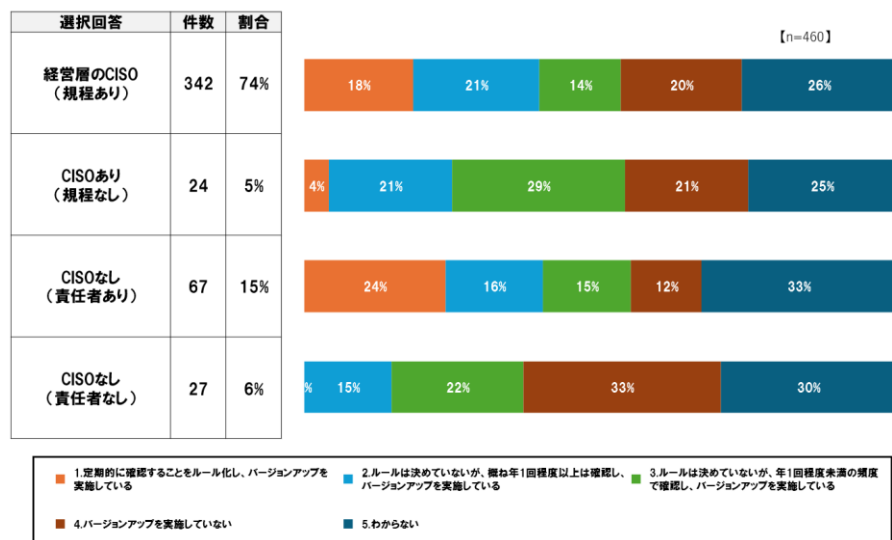
図表 1-71 管理者パスワードの管理（Q19）（管理者有無ベース）



## ● ネットワーク機器のファームアップ (Q20)

セキュリティ責任者を設置していないものは、「バージョンアップを実施していない」率が高い。

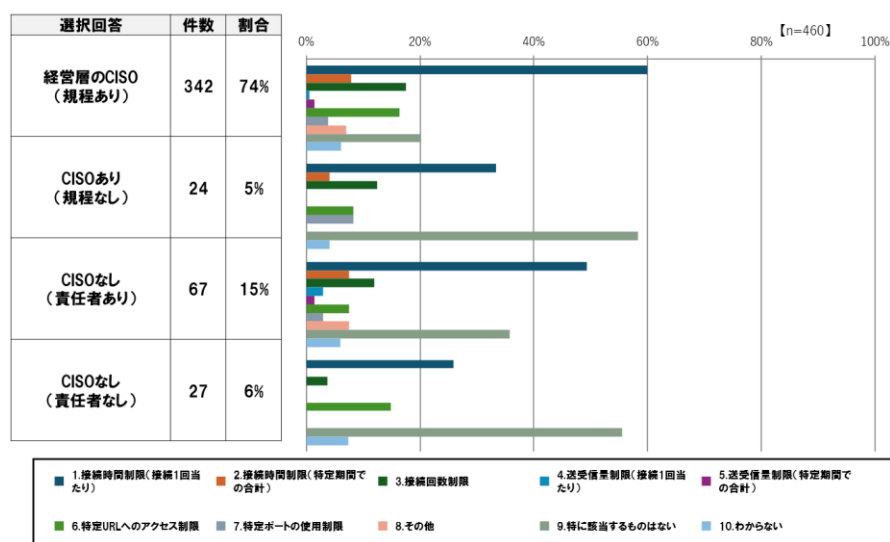
図表 1-72 ネットワーク機器のファームアップ (Q20) (管理者有無ベース)



## ● その他のセキュリティ対策 (Q26)

セキュリティ責任者を設置しているものは、何らかの制限事項を設けている場合が多い。

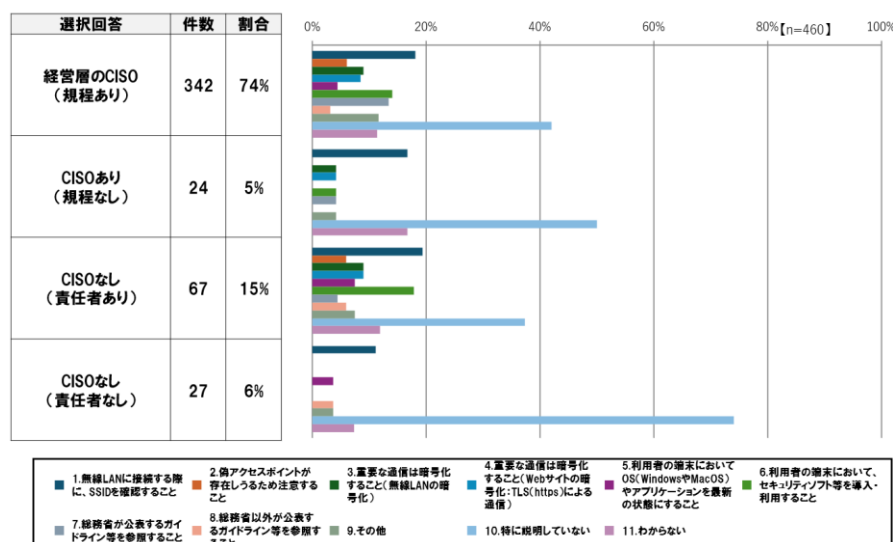
図表 1-73 その他のセキュリティ対策（Q26）（管理者有無ベース）



● 無線 LAN サービスの注意喚起（Q30）

セキュリティ責任者を設置していないところは、注意喚起をしていない率が高い。

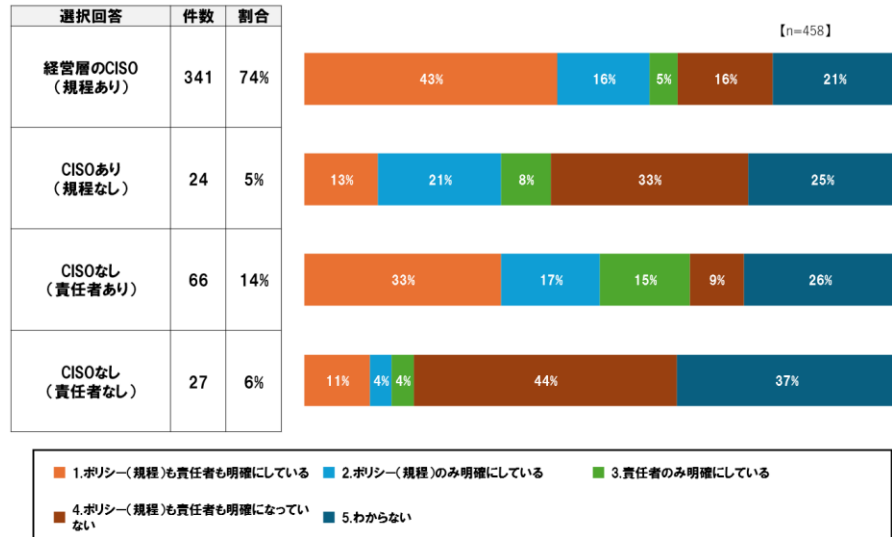
図表 1-74 セキュリティに関する注意喚起（Q30）（管理者有無ベース）



● 利用者情報のデータ保護（Q32）

セキュリティ責任者を設置していないところは、利用者情報のデータ（個人情報等）の保護に対する認識が低い（8割以上）。

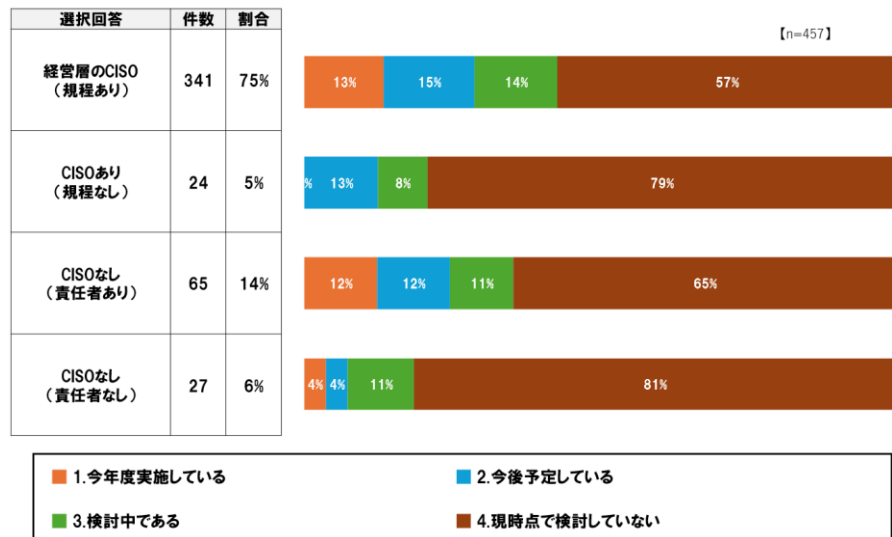
図表 1-75 利用者情報のデータ保護（Q32）（管理者有無ベース）



● サービスの設備拡充や更改計画（Q34）

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

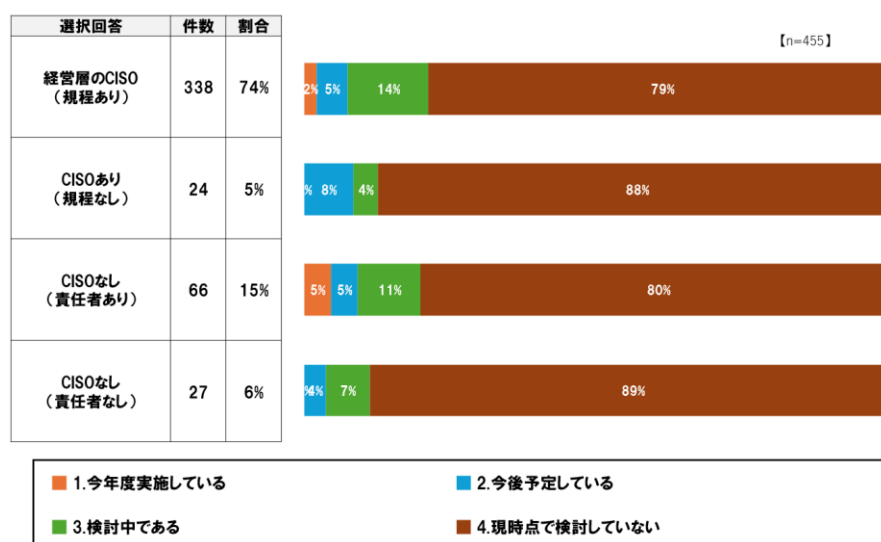
図表 1-76 サービスの設備拡充や更改計画（Q34）（管理者有無ベース）



● サービスのセキュリティ強化計画（Q36）

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。

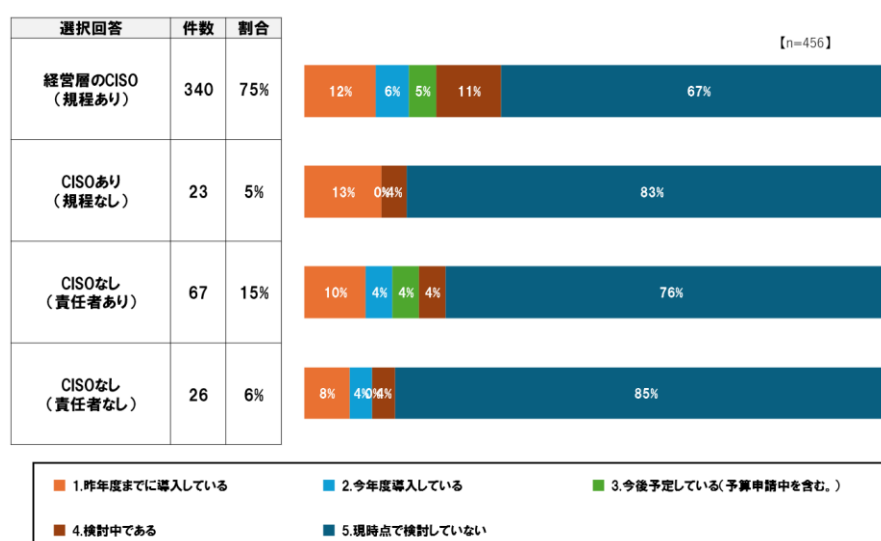
図表 1-77 サービスのセキュリティ強化計画（Q36）（管理者有無ベース）



● Wi-Fi 6 の導入予定（Q38）

セキュリティ責任者を設置しているところは、Wi-Fi 6 の導入を検討している率が高い。

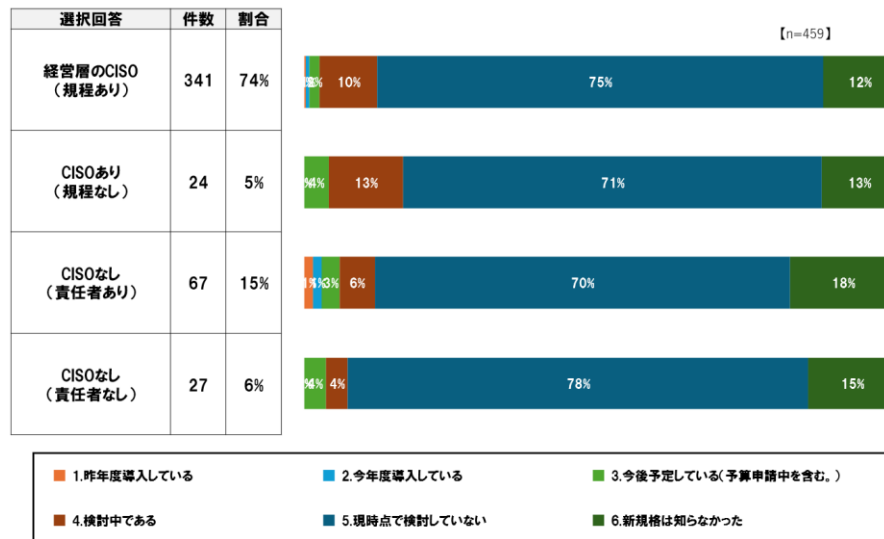
図表 1-78 Wi-Fi 6 の導入予定（Q38）（管理者有無ベース）



● Wi-Fi 6E の導入予定 (Q39)

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

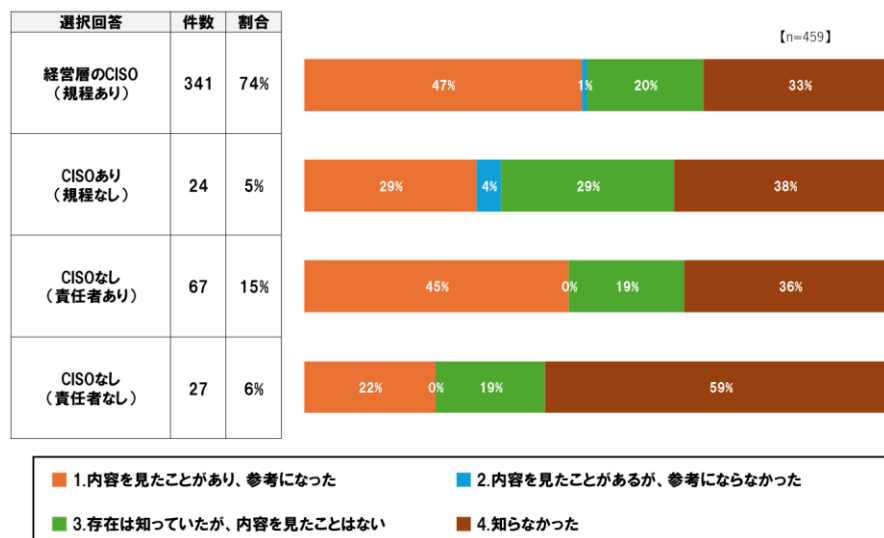
図表 1-79 Wi-Fi 6E/7 の導入予定 (Q39) (管理者有無ベース)



● セキュリティ対策の手引き (Q41)

情報セキュリティ責任者を設置していないところは、「手引き」の内容を知らない率が高い。

図表 1-80 セキュリティ対策の手引き (Q41) (管理者有無ベース)



(8) Q42 自由意見について

回答した地方自治体・企業等に対して、Q42 で自由意見を求めたところ、

- ① 無線 LAN サービス及びサービスのセキュリティの考え方について
- ② 導入や運用にかかわるさまざまな課題について
- ③ 「手引き」および本アンケートへの要望など

などの意見があった。

具体的な意見は参考資料の巻末に付す。