

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提供者実態調査
概要版**

**令和6年3月29日
株式会社ITグローバルブレイン**

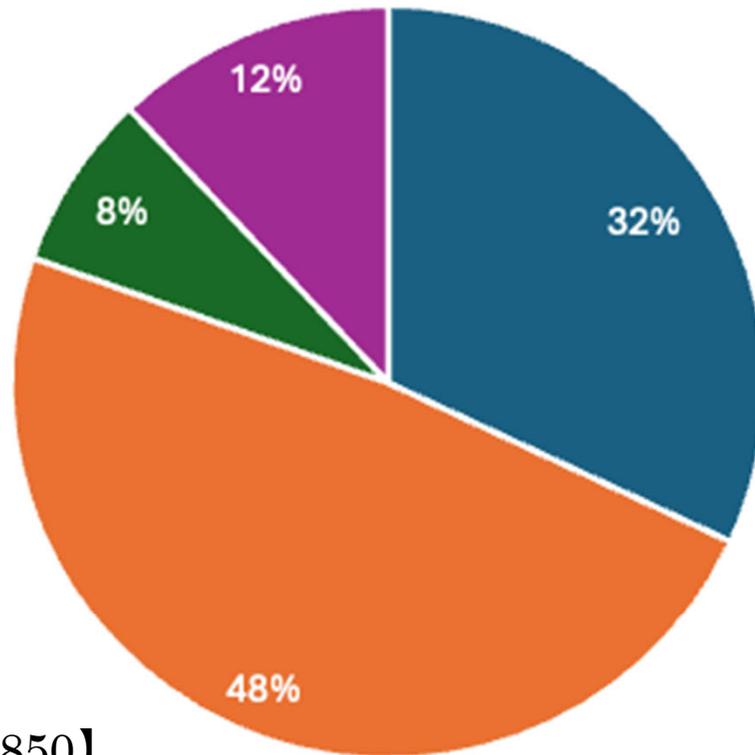
前年と同様の内容であったが、回答には以下のような特徴がみられた。

- 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 / WiGig / Wi-Fi HaLow）については、まだまだ導入率、導入検討率は低い。

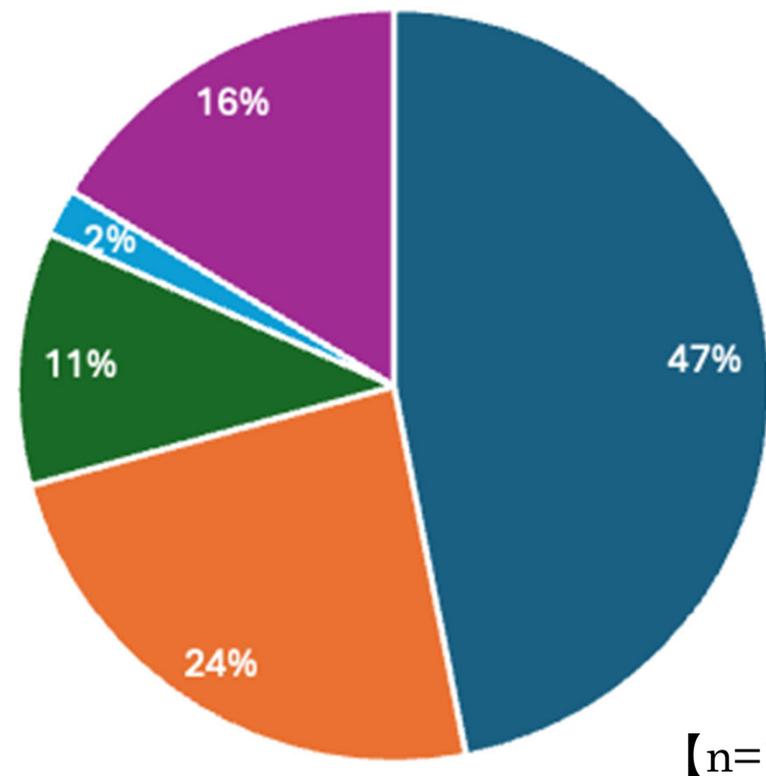
無線LANサービスの導入（Q1）

- 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。

自治体



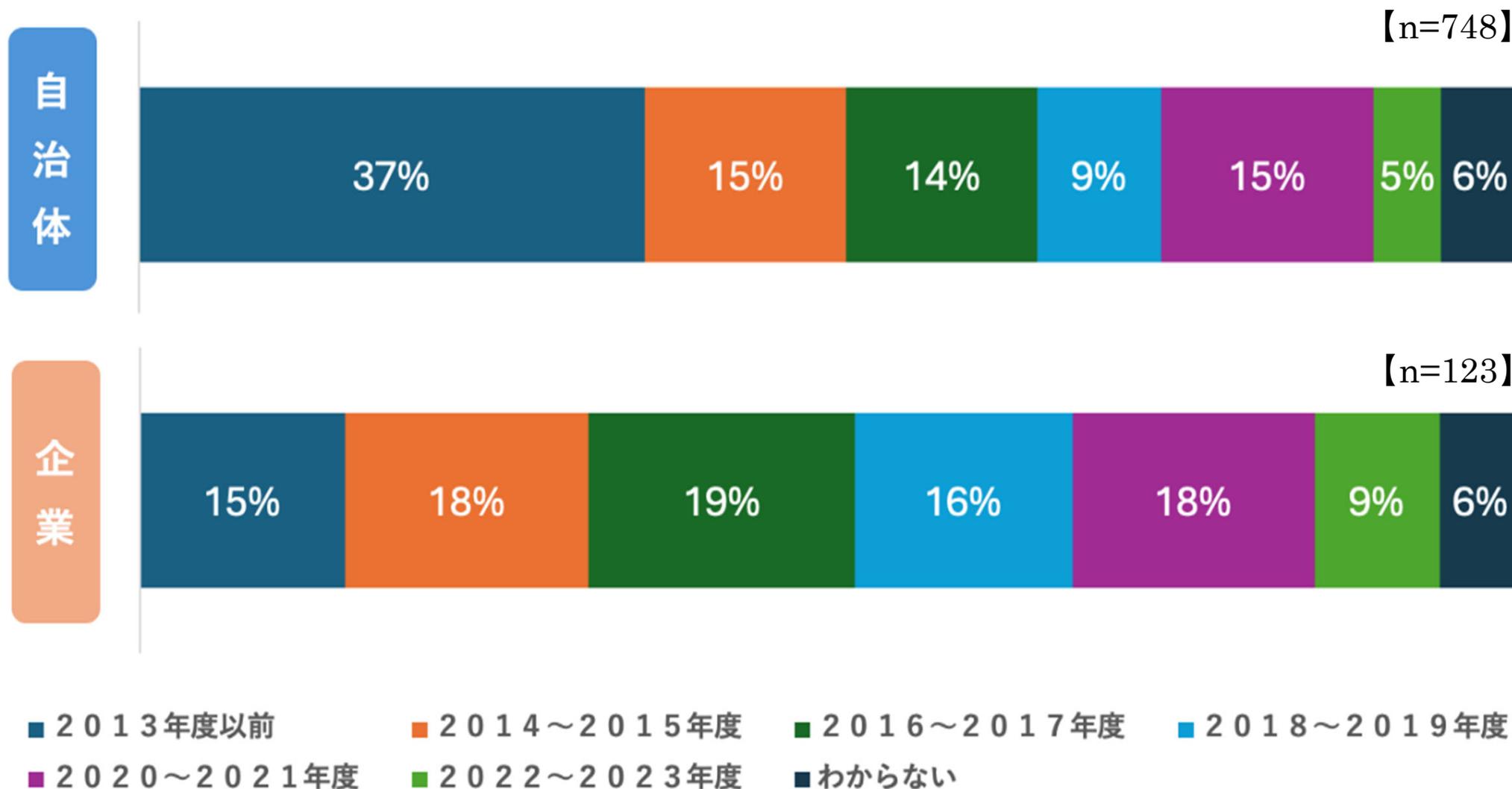
企業



- 貴社・貴団体が独自に仕様を定めた「無線LANサービス」を導入している
- 通信事業者等が提供する「無線LANサービス」を導入している
- 貴社・貴団体が独自に仕様を定めたものと、通信事業者等による「無線LANサービス」の両方を導入している
- 管理する施設において「無線LANサービス」は導入していたが、提供をやめた
- 管理する施設において「無線LANサービス」は導入していない

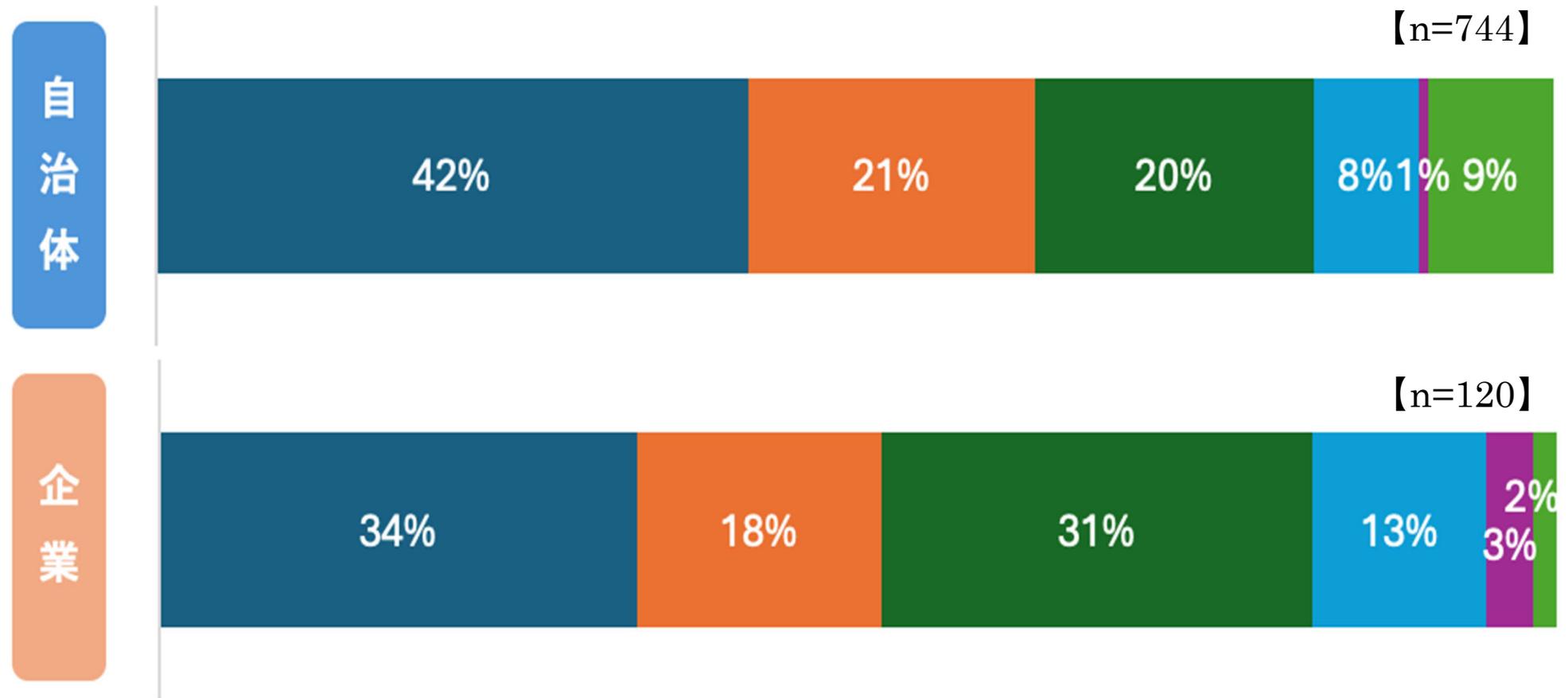
無線LANサービスの導入時期（Q2）

- 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。



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。

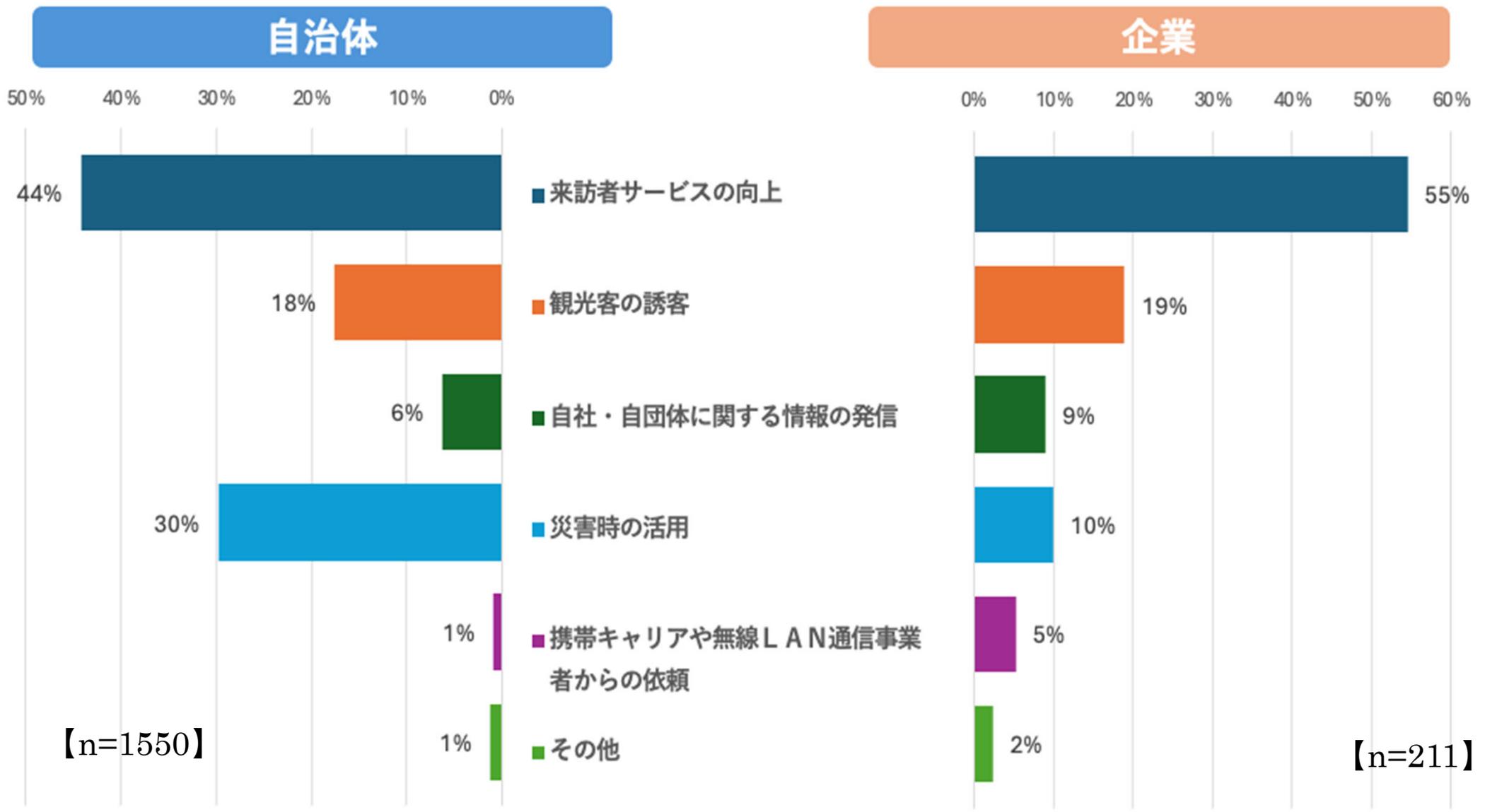


- システム部門の社員・職員が担当している
- 委託した外部業者が担当している
- わからない

- システム部門外の社員・職員が担当している
- 担当者はいない（構築だけ外部業者に発注した等）
- その他

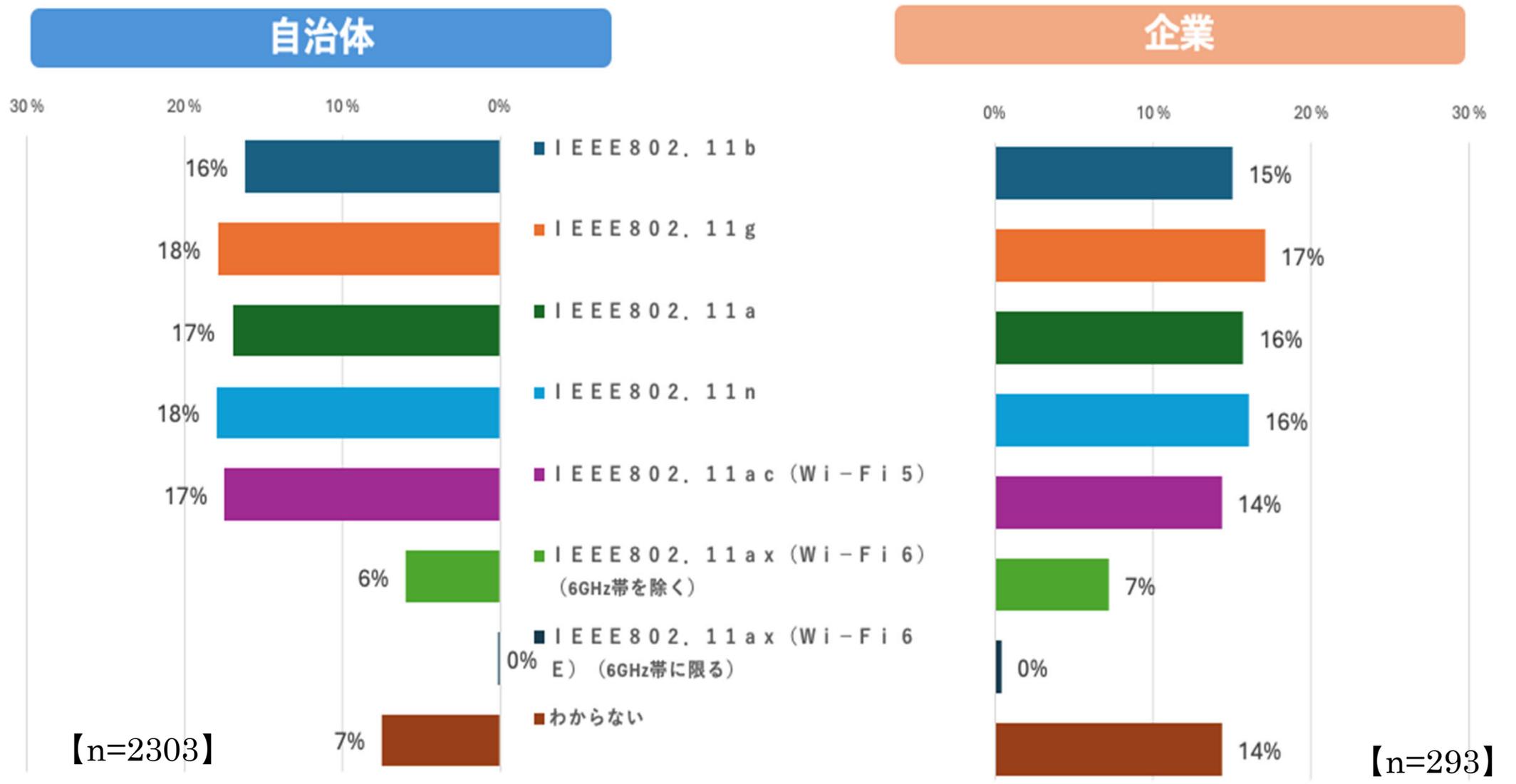
無線LANサービスの目的 (Q7)

➤ 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。



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%）。

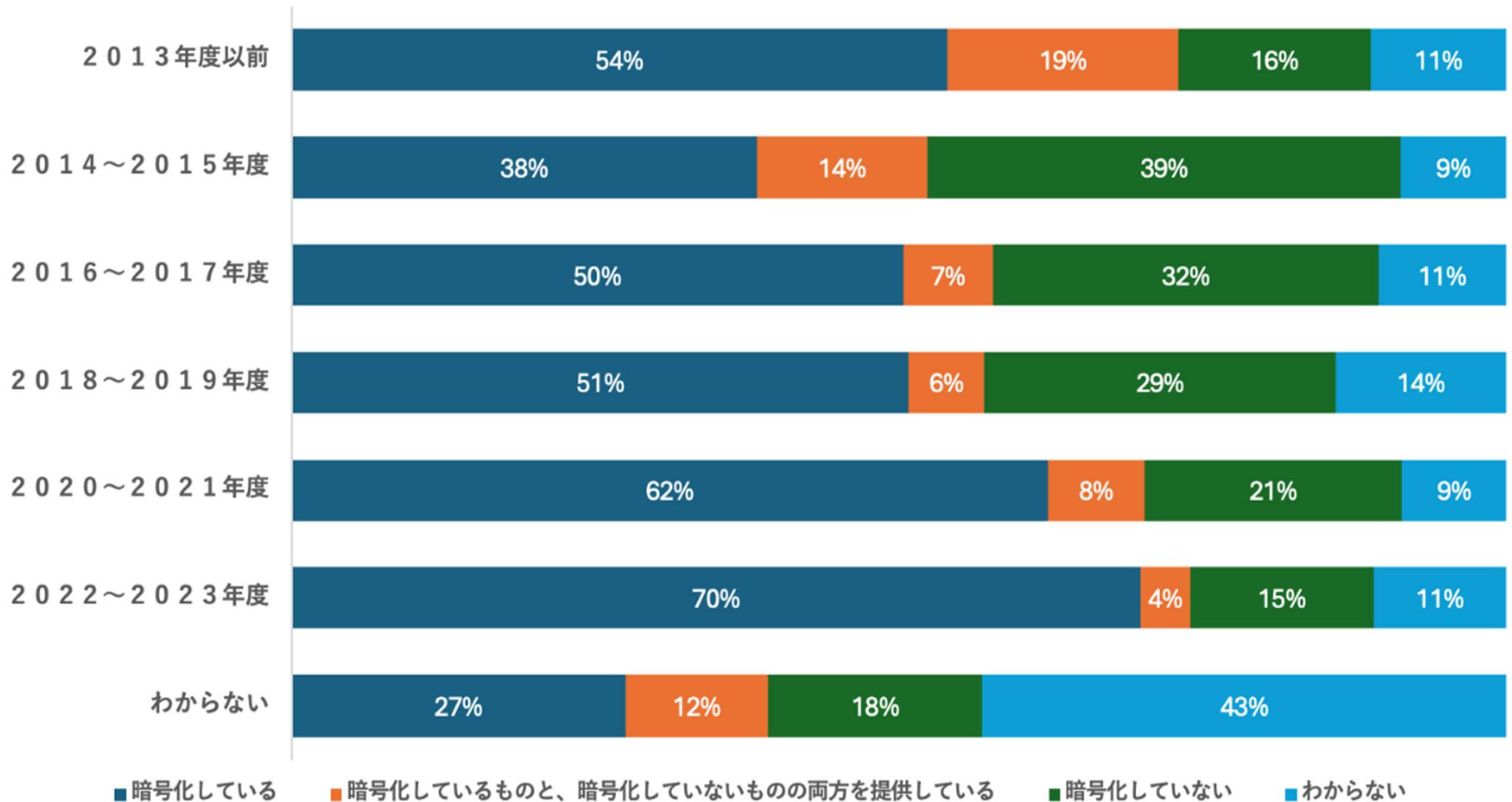


回答には以下のような特徴がみられた。

- 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。

無線LANサービスの暗号化（Q9）（導入時期ベース）

- 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。

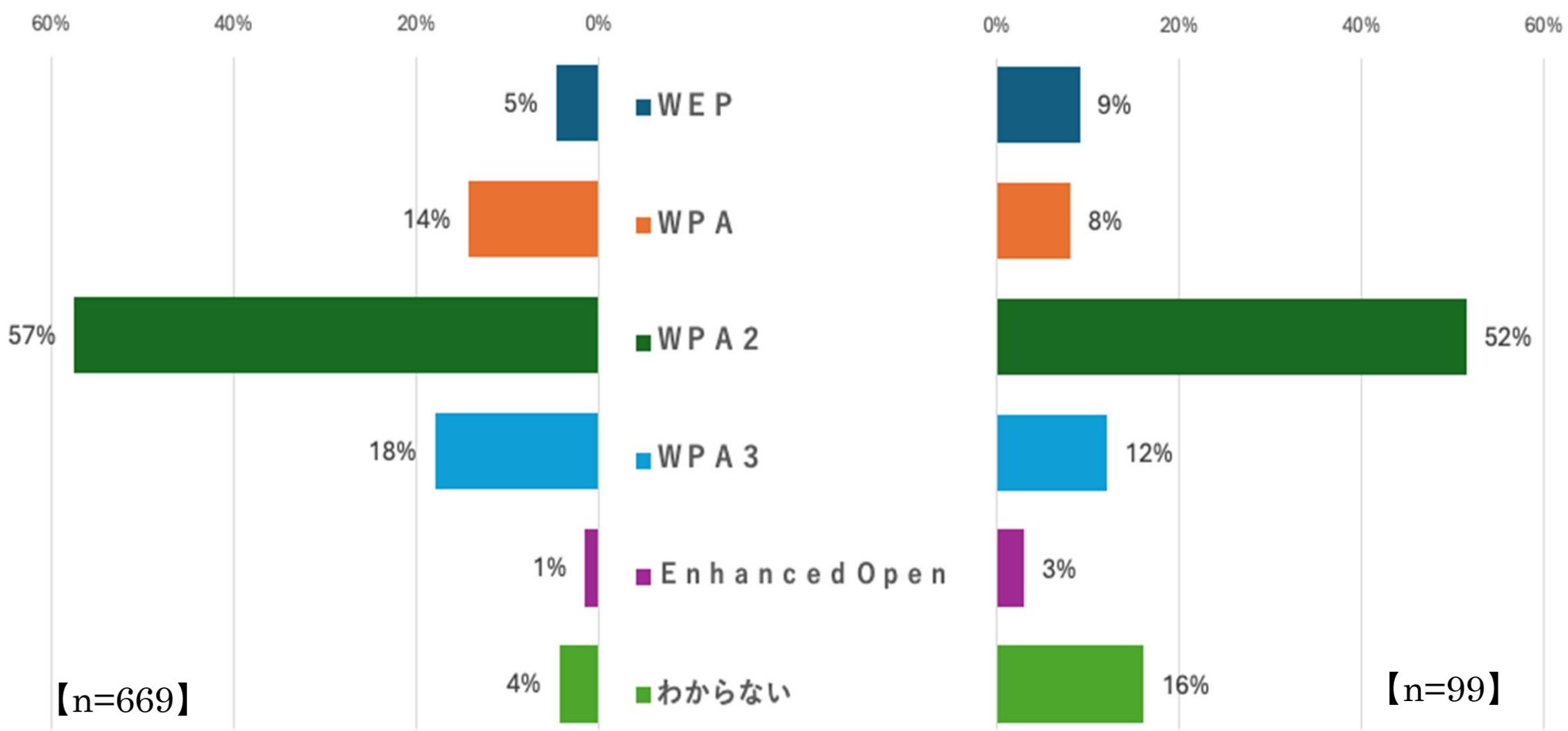


無線LANサービスの暗号化方式（Q10）

➤ 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。

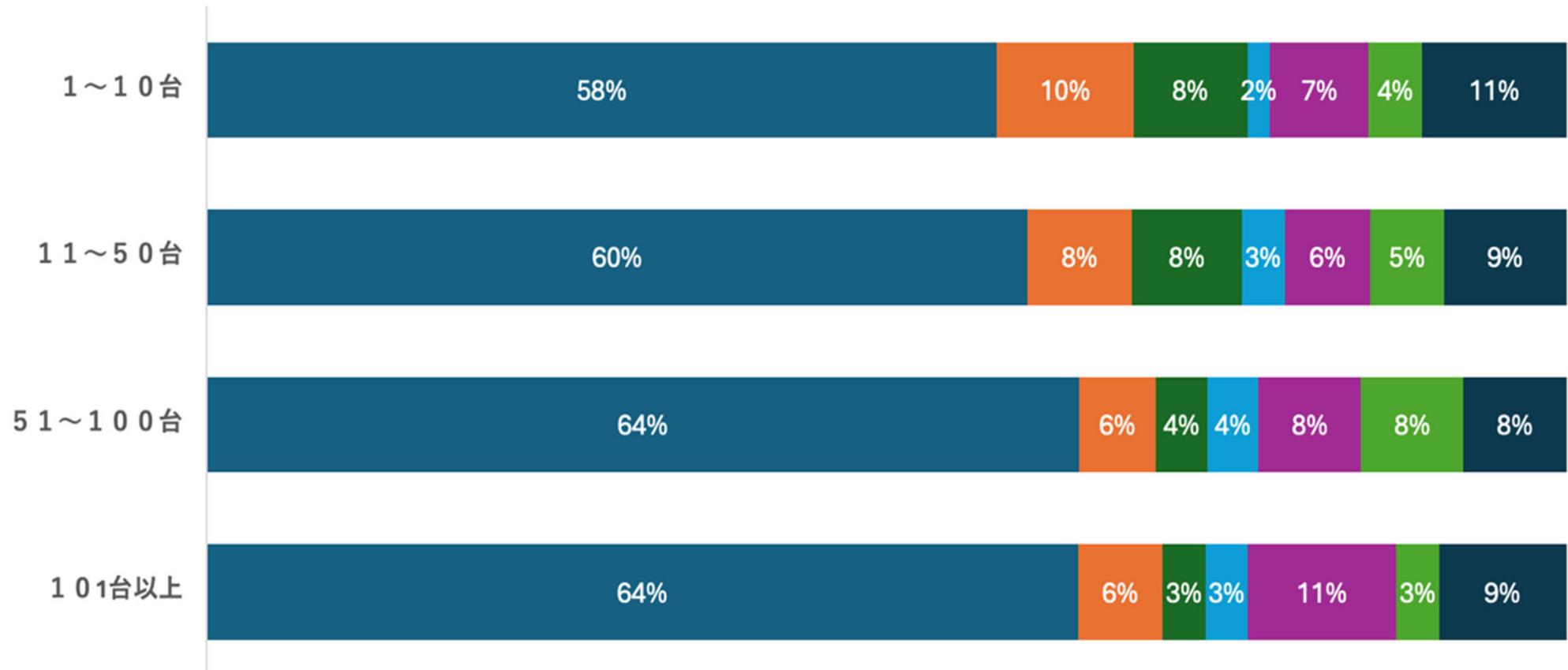
自治体

企業



暗号化方式のセキュリティリスク（Q11）（導入規模ベース）

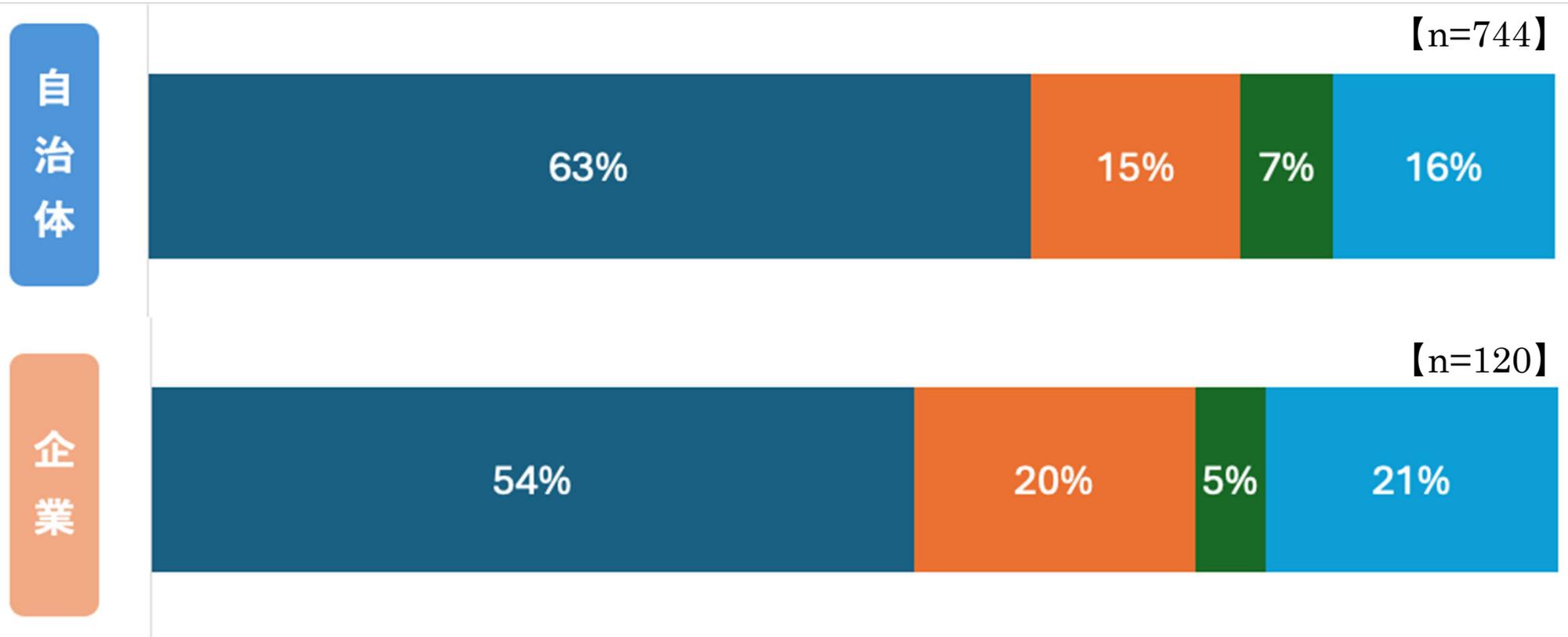
➤ 導入規模をベースとして分類したところ、規模が大きいほどセキュリティリスクへの認識度は高くなっていることが分かった。



- WE PやWPAを使っていない
- セキュリティリスクを認識しており、更改を検討中
- セキュリティリスクを認識しているが、更改費用が捻出できず利用し続けている
- セキュリティリスクを認識しているが、利用者の要望があり利用し続けている
- セキュリティリスクを認識しているが、利用者がTLS (https) 接続等を利用すれば問題ないため利用し続けている
- セキュリティリスクを認識しているが、その他の理由により利用し続けている
- セキュリティリスクがあることを知らなかった

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%)。



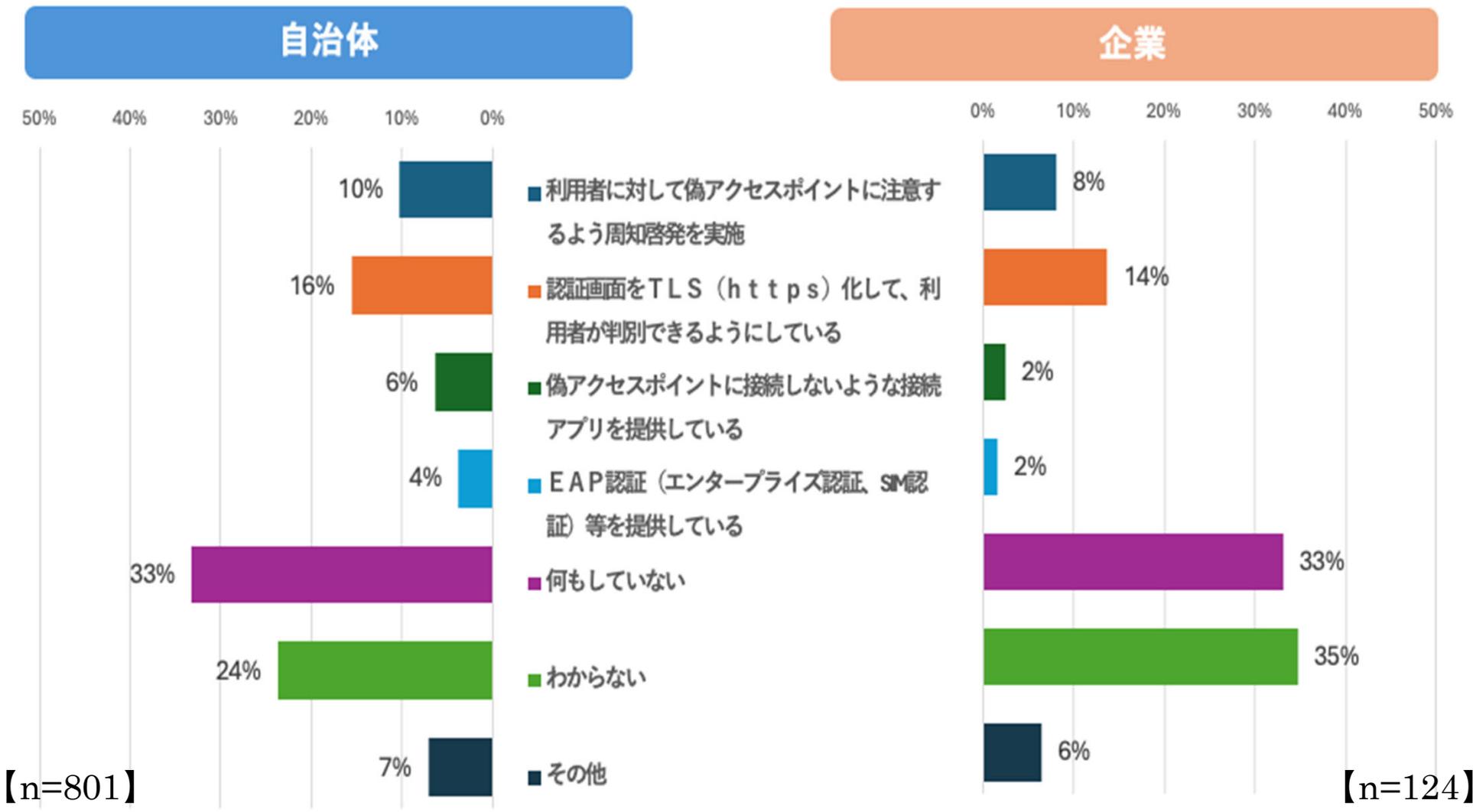
■ 読解可能なリスクも、偽アクセスポイント設置のリスクも知っていた ■ 読解可能なリスクのみ知っていた

■ 偽アクセスポイント設置のリスクのみ知っていた

■ リスクが生じることを知らなかった

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。

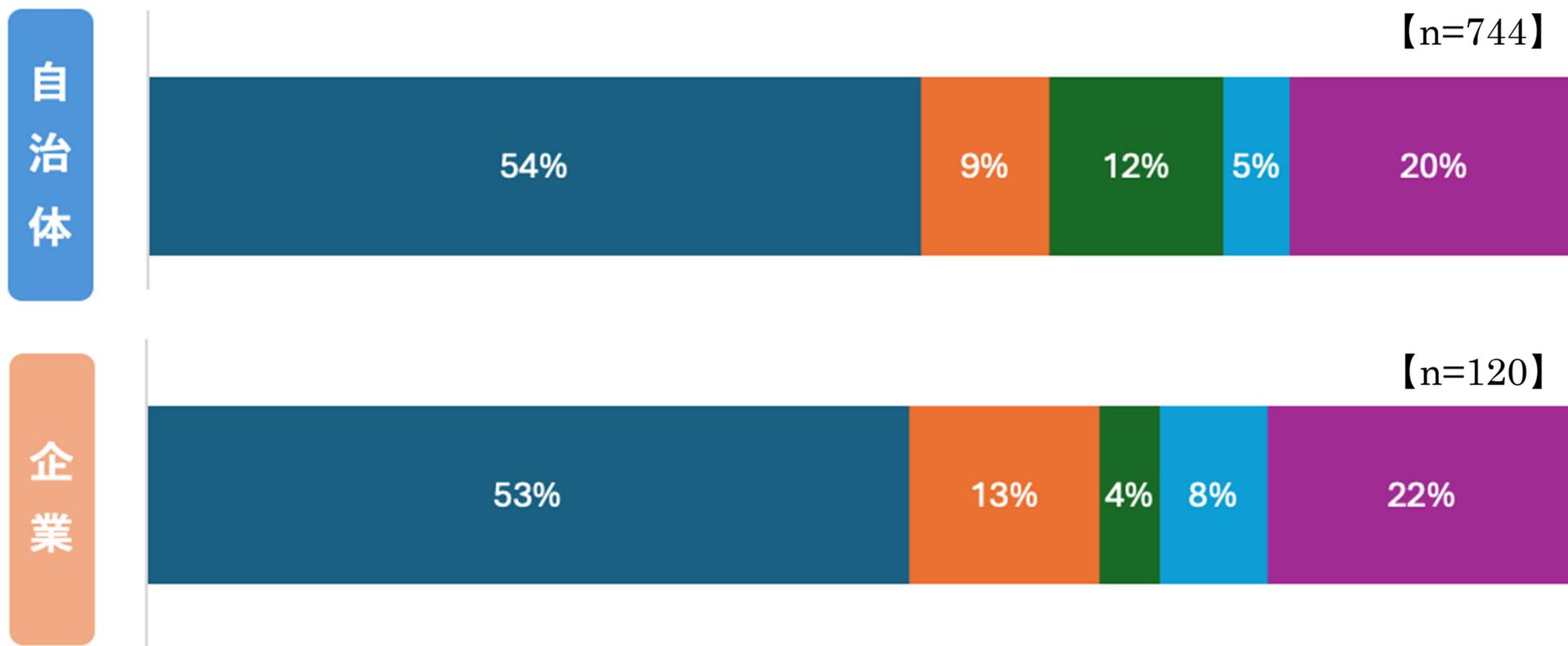


回答には以下のような特徴がみられた。

- ・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。

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%）。



- 初期設定から変更している（第三者から推測されにくいものを設定している）
- 初期設定から変更している（第三者から推測されやすいものかどうか検討していない）
- 初期設定のまま使用している（初期設定のパスワードが十分複雑なものであった）
- 初期設定のまま使用している（初期設定のパスワードを気にしていない）
- わからない

管理者パスワードの管理（Q18）（導入規模ベース）

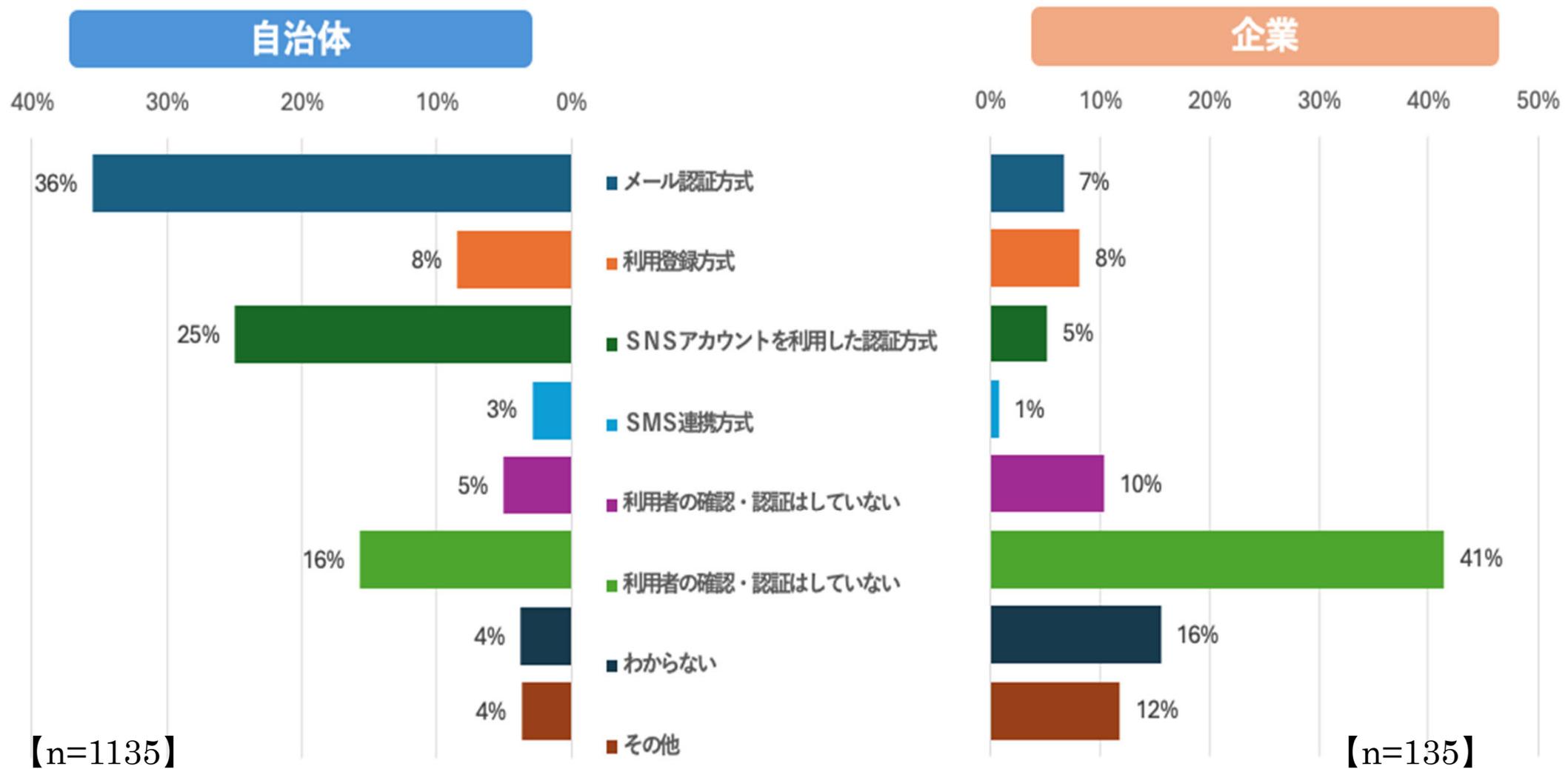
➤ 導入規模をベースとして分類したところ、設備規模が大きいほど、管理を厳格にしている率が高いことが分かった。



- 初期設定から変更している（第三者から推測されにくいものを設定している）
- 初期設定から変更している（第三者から推測されやすいものかどうか検討していない）
- 初期設定のまま使用している（初期設定のパスワードが十分複雑なものであった）
- 初期設定のまま使用している（初期設定のパスワードを気にしていない）
- わからない

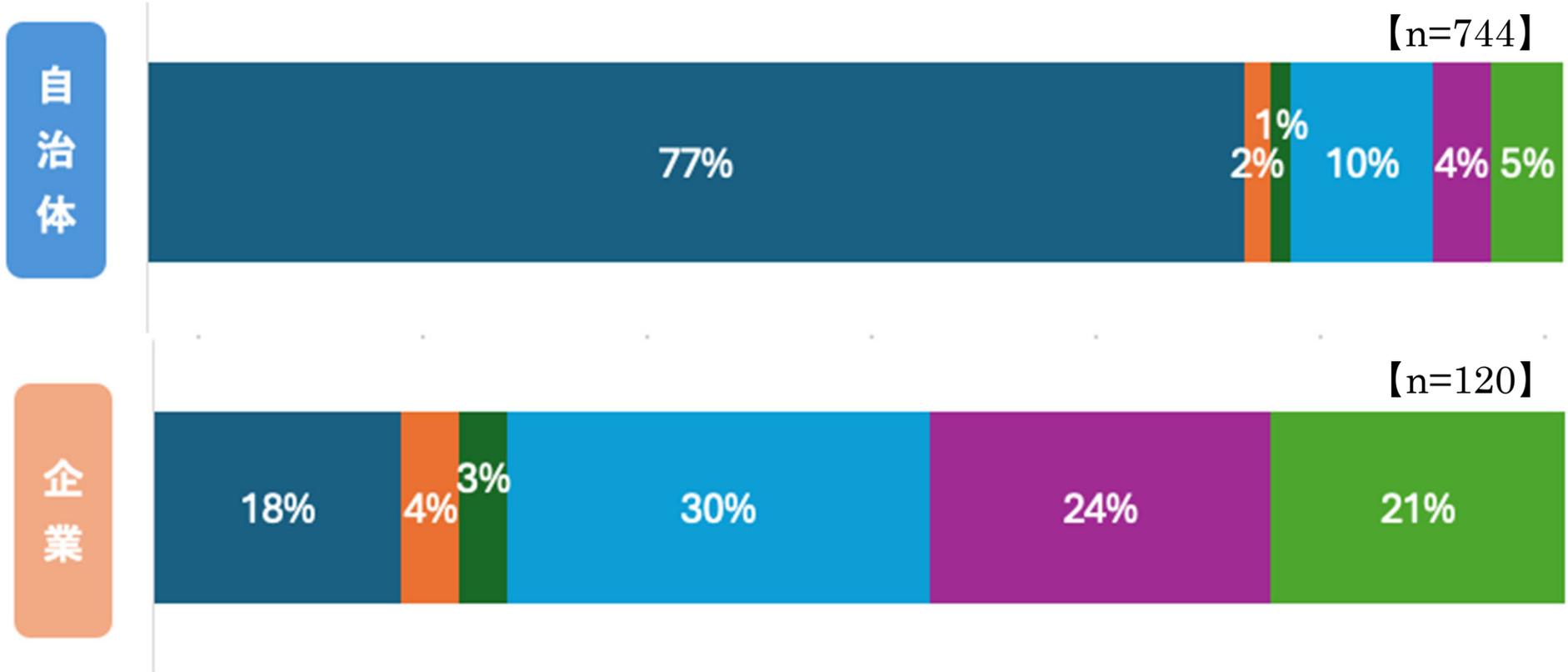
サービス利用者の認証方式 (Q21)

➤ 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。



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。



- 経営層のCISOを設置している（社内規程等の内部規程で明確に定めている）
- 経営層ではないが、CISOを設置している
- 情報セキュリティの責任者は決まっていない
- 経営層のCISOを設置している（社内規程等の内部規程では定めていない）
- CISOではないが、情報セキュリティの責任者を決めている
- わからない

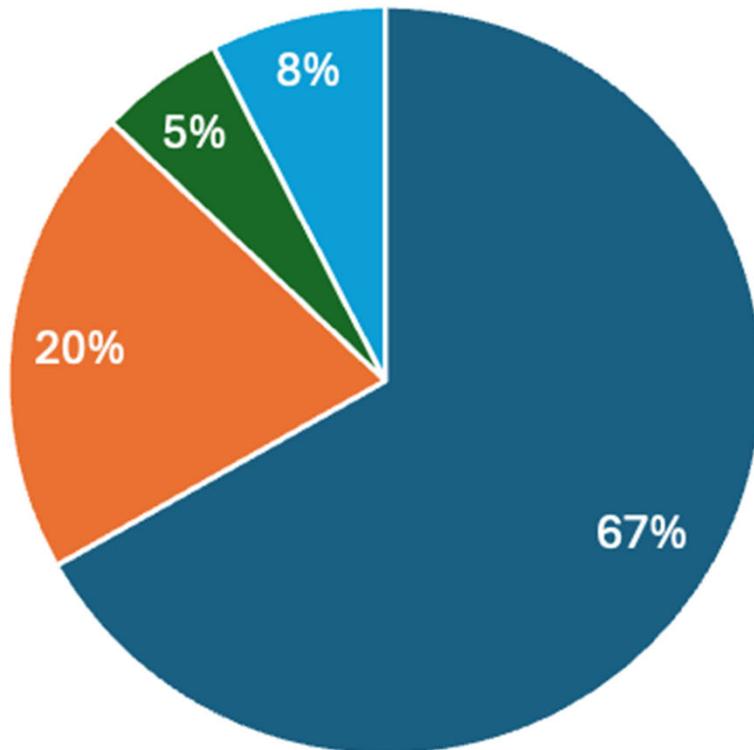
回答には以下のような特徴がみられた。

- ・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。

無線LANサービスの利用規約（Q27）

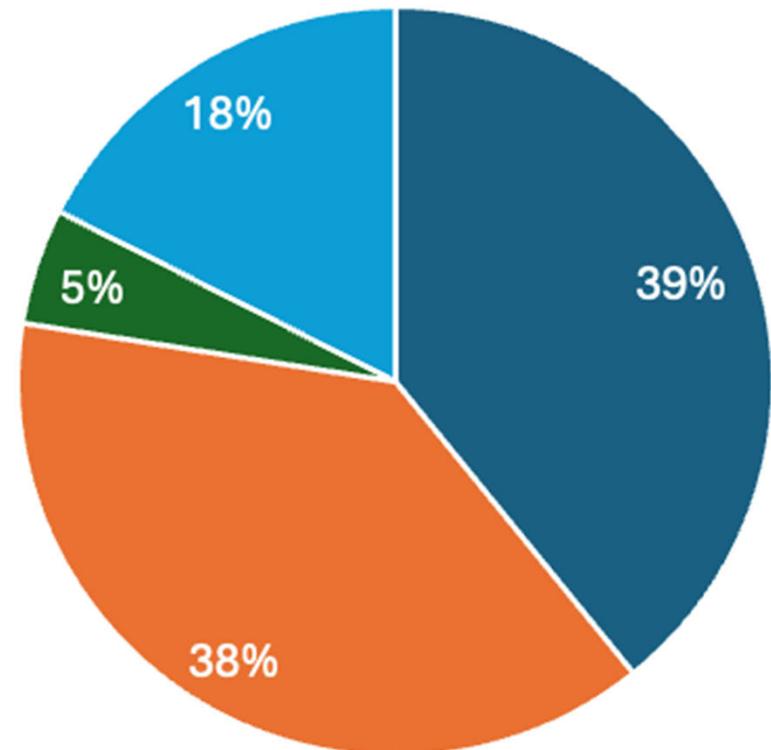
- 自治体は「利用規約を定めている」率が前年と横ばい、企業は大幅に減少している（自治体：67%→67%、企業50%→39%）。

自治体



【n=744】

企業



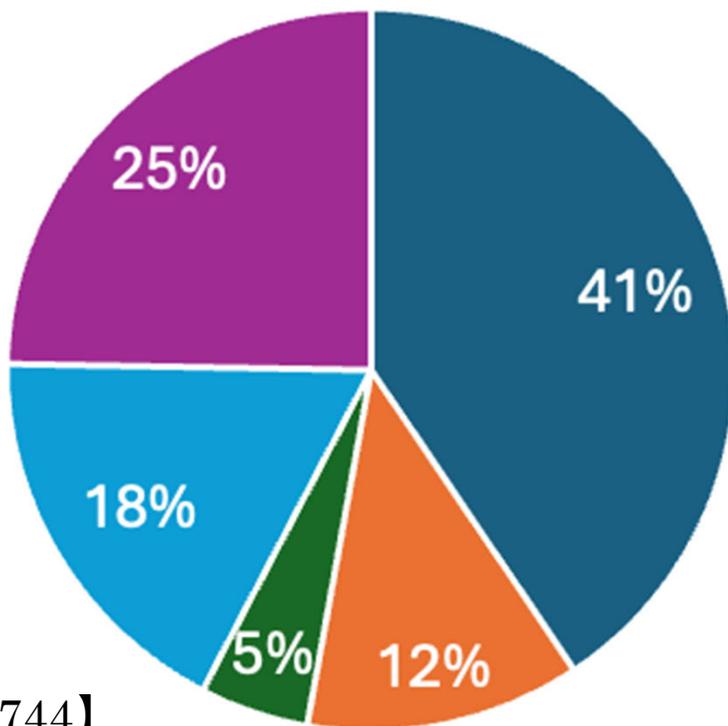
【n=120】

■ 定めている ■ 定めていない ■ 定めている無線LANサービスと、定めていない無線LANサービスの両方がある ■ わからない

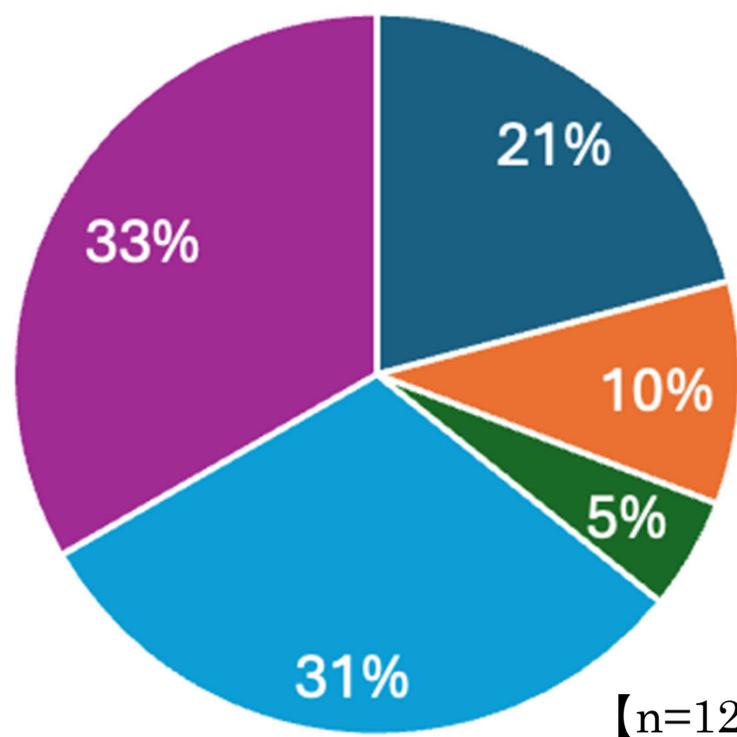
利用者情報のデータ保護 (Q31)

➤ 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。

自治体



企業



- ポリシー（規程）も責任者も明確にしている
- 責任者のみ明確にしている
- わからない

- ポリシー（規程）のみ明確にしている
- ポリシー（規程）も責任者も明確になっていない

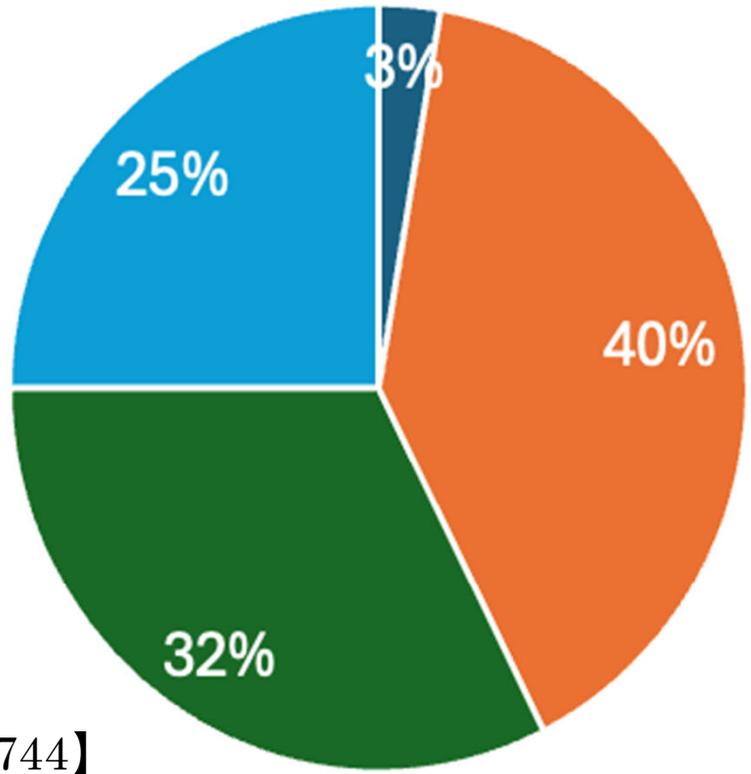
回答には以下のような特徴がみられた。

- 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5G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。

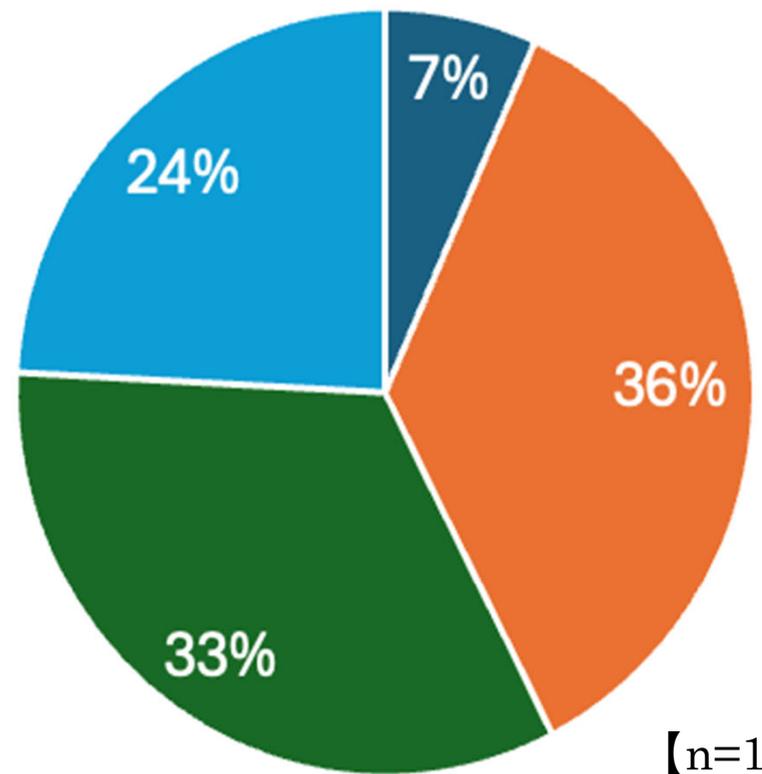
サービスのセキュリティへの不安 (Q32)

➤ 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%）。

自治体



企業

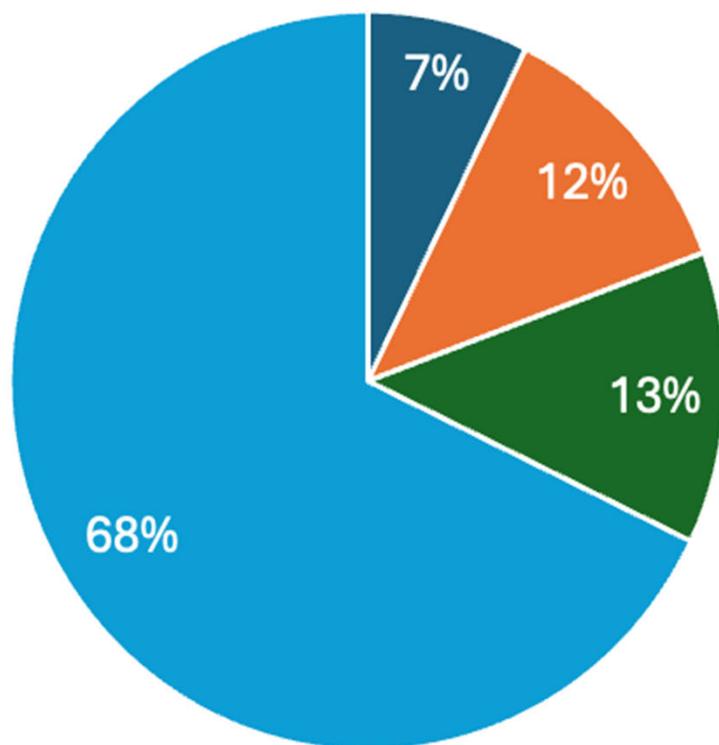


■ いつも不安になる ■ 時々不安になる ■ あまり不安にならない ■ 特に不安は感じない

サービスの設備拡充や更改計画 (Q33)

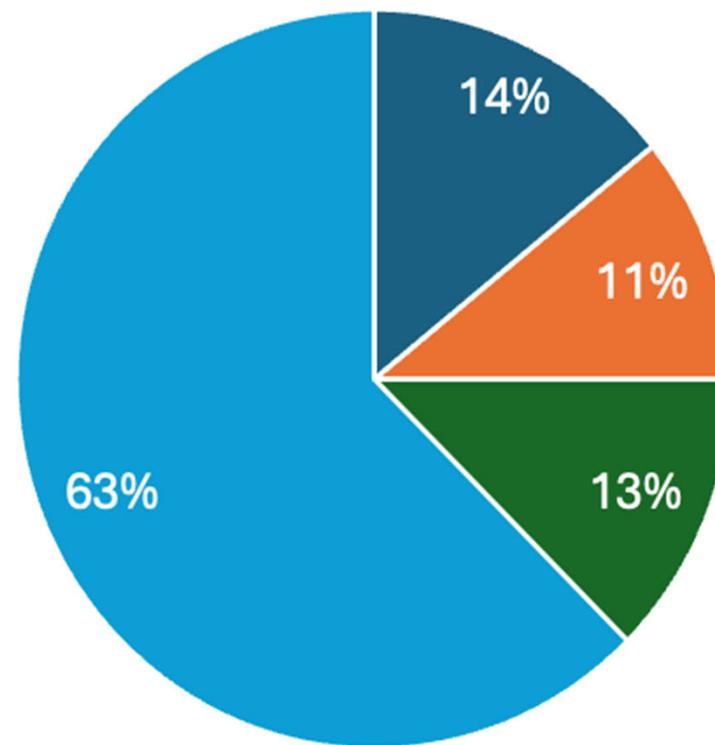
- 前年に比べ、整備更改等を実施・検討している率は自治体が微増しており、企業は横ばいであった（自治体29%→32%、企業38%→38%）。

自治体



【n=744】

企業



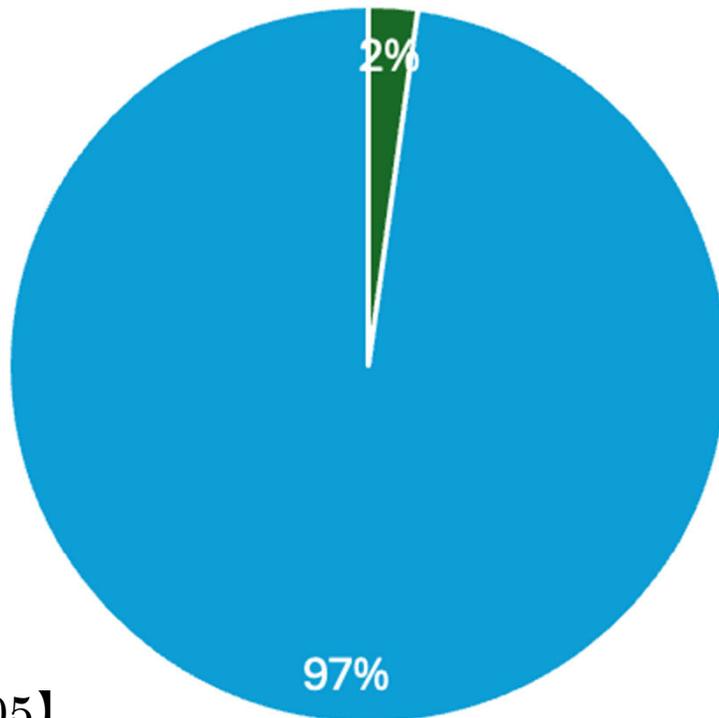
【n=120】

■ 今年度実施している ■ 今後予定している ■ 検討中である ■ 現時点で検討していない

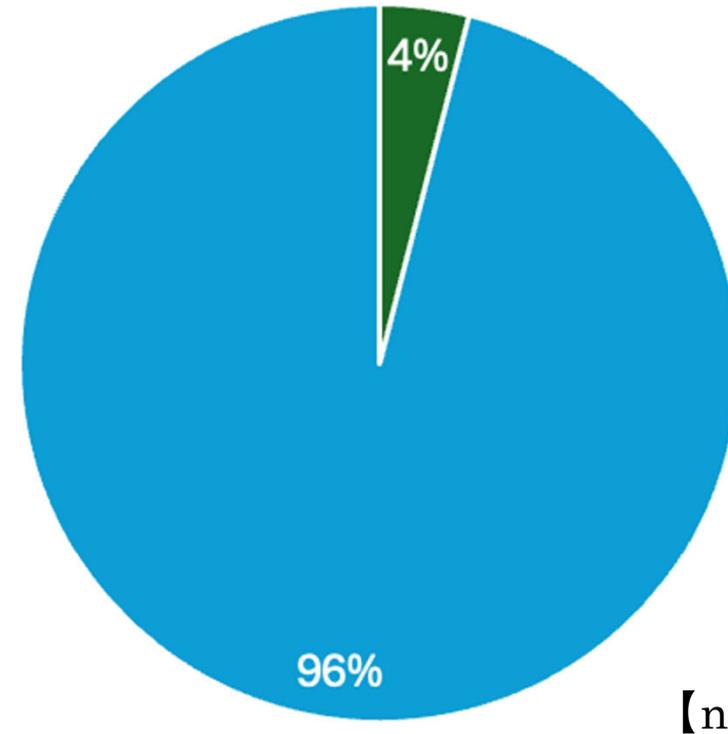
サービスのセキュリティ強化計画（Q35）

- 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%）。

自治体



企業

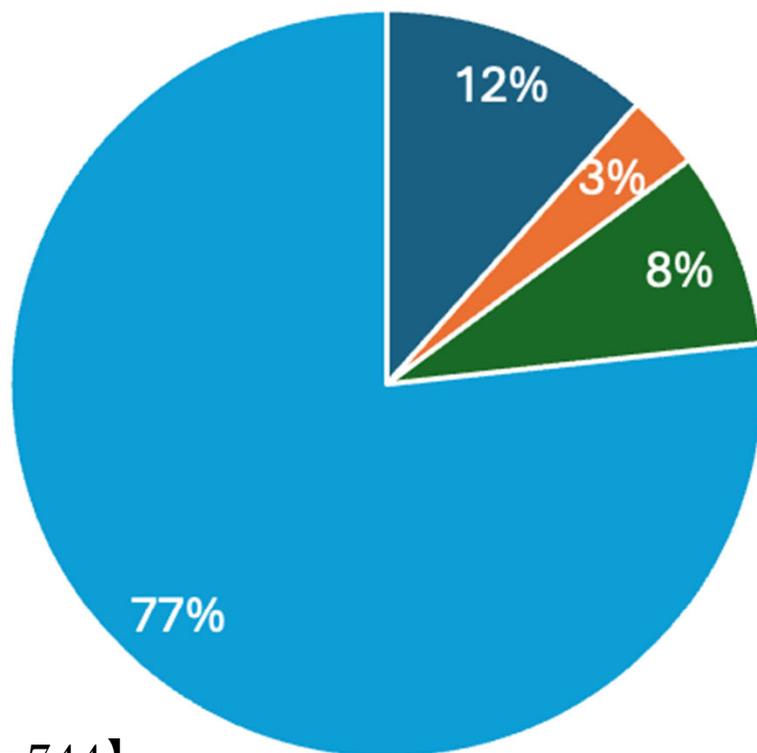


■ 今年度実施している ■ 今後予定している ■ 検討中である ■ 現時点で検討していない

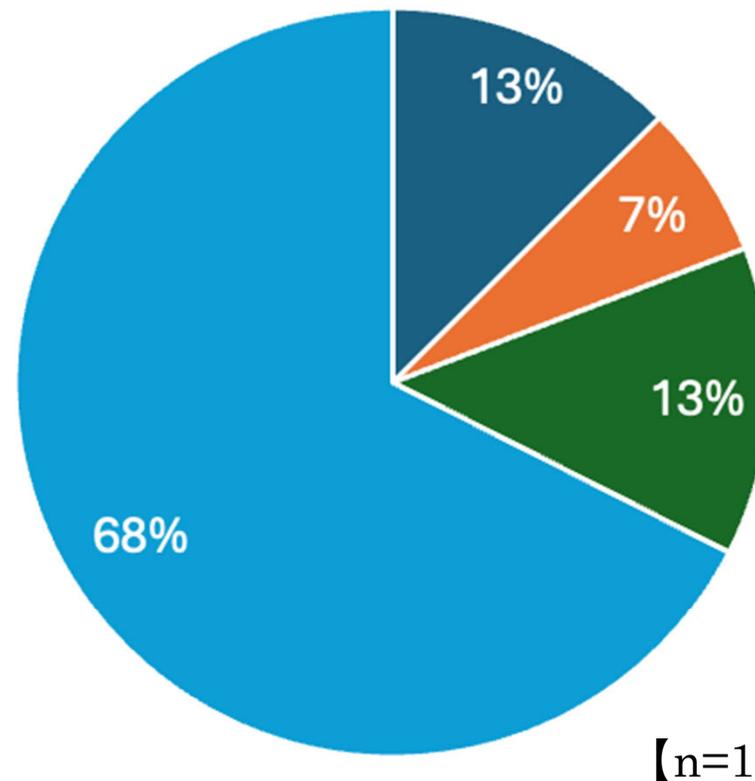
Wi-Fi 6の導入予定 (Q37)

- 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。

自治体



企業

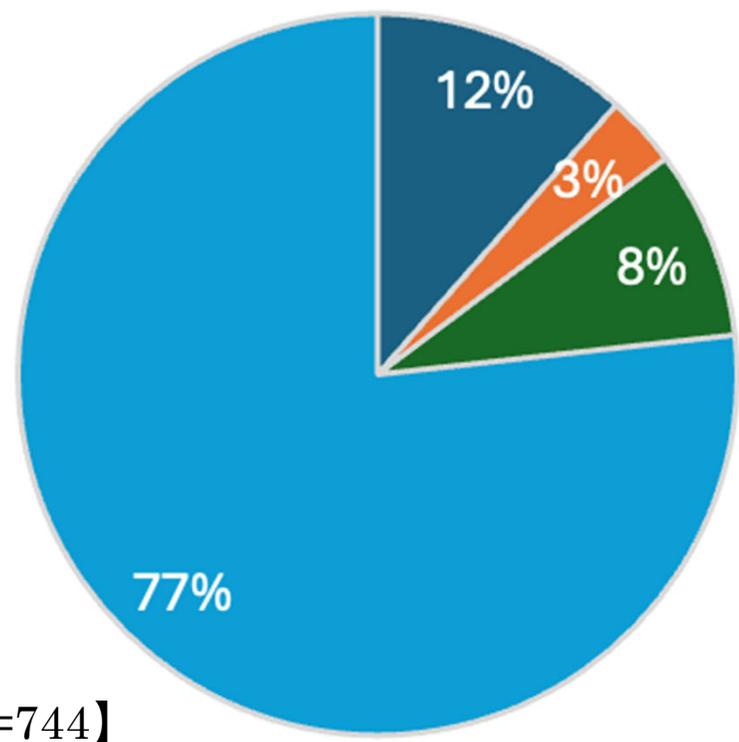


■ 今年度導入している ■ 今後予定している ■ 検討中である ■ 現時点で検討していない

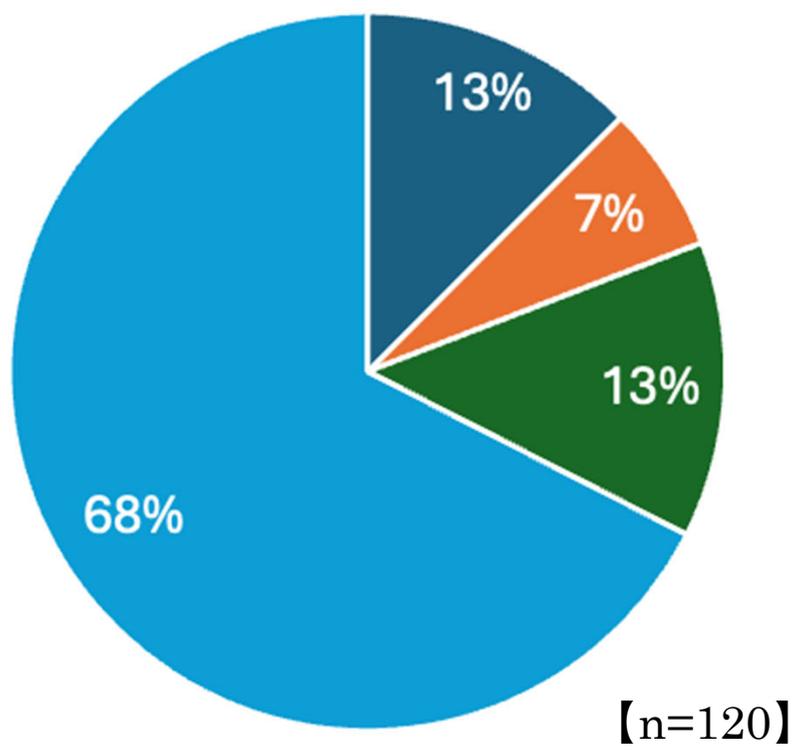
ローカル5Gの導入予定 (Q37)

➤ 「ローカル5G」の導入を検討している割合は前年よりも増加している（自治体7%→11%、企業9%→21%）。

自治体



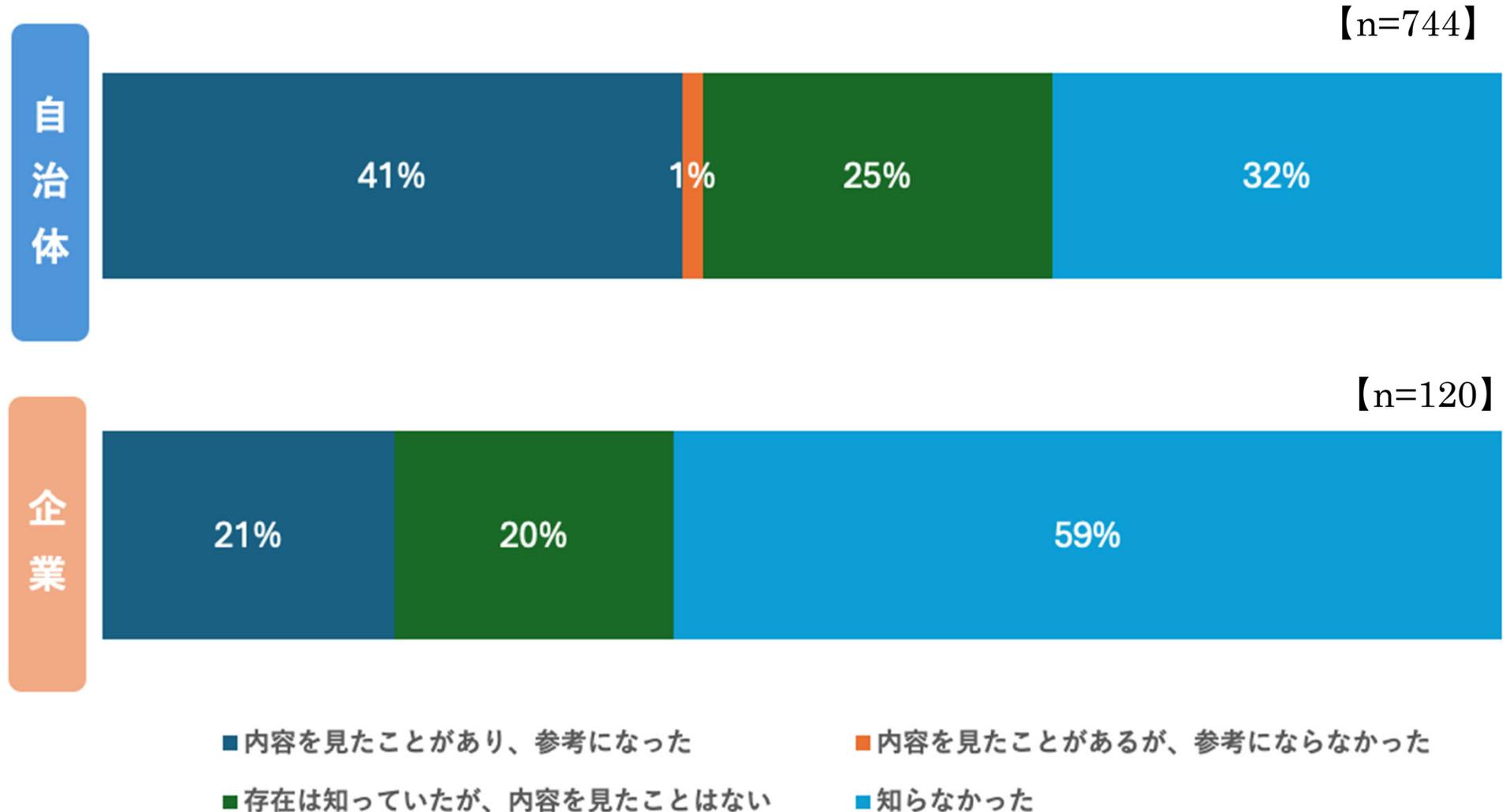
企業



■ 今年度導入している ■ 今後予定している ■ 検討中である ■ 現時点で検討していない

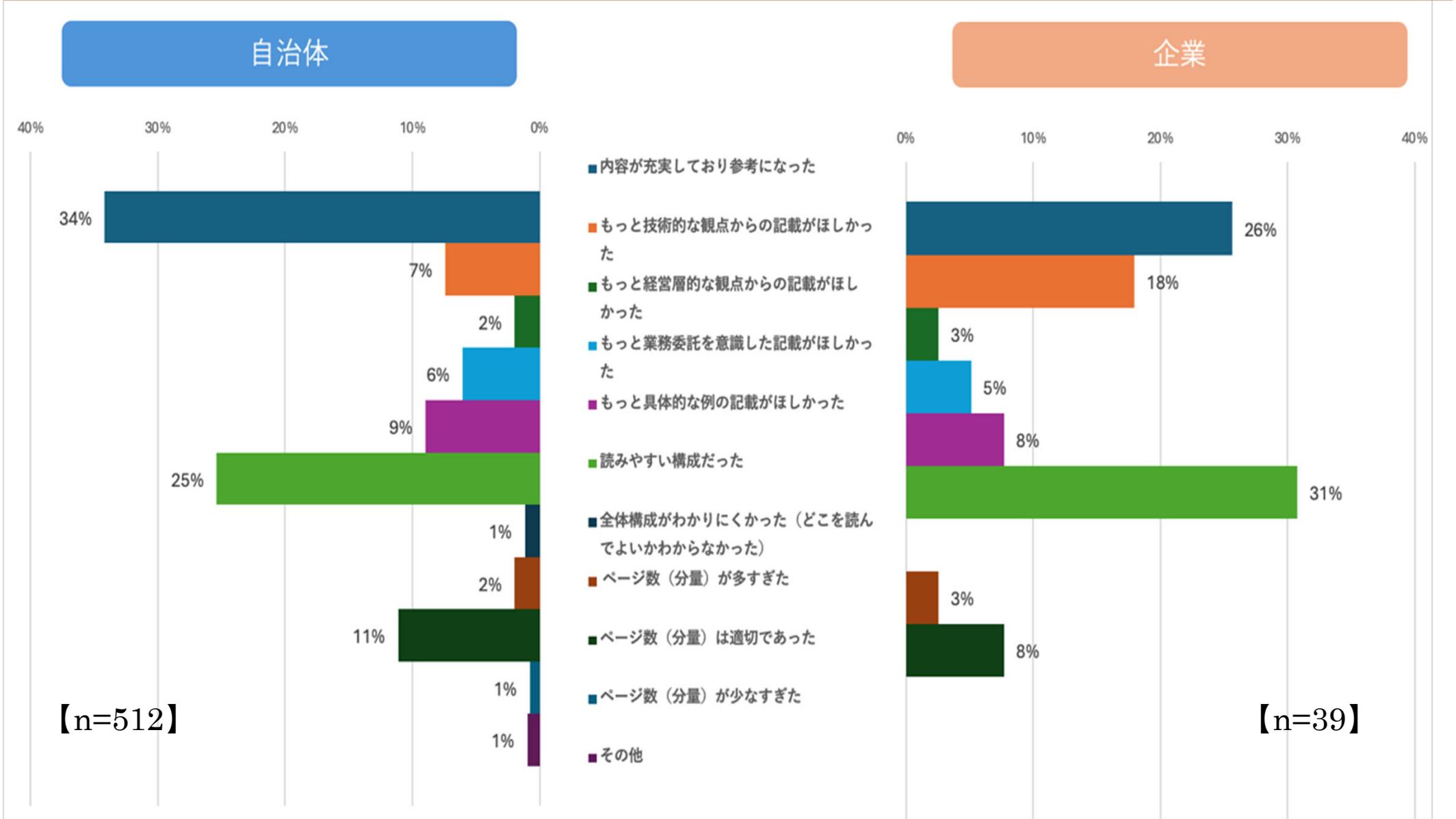
セキュリティ対策の手引き（Q40）

- 「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%）。



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。



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。

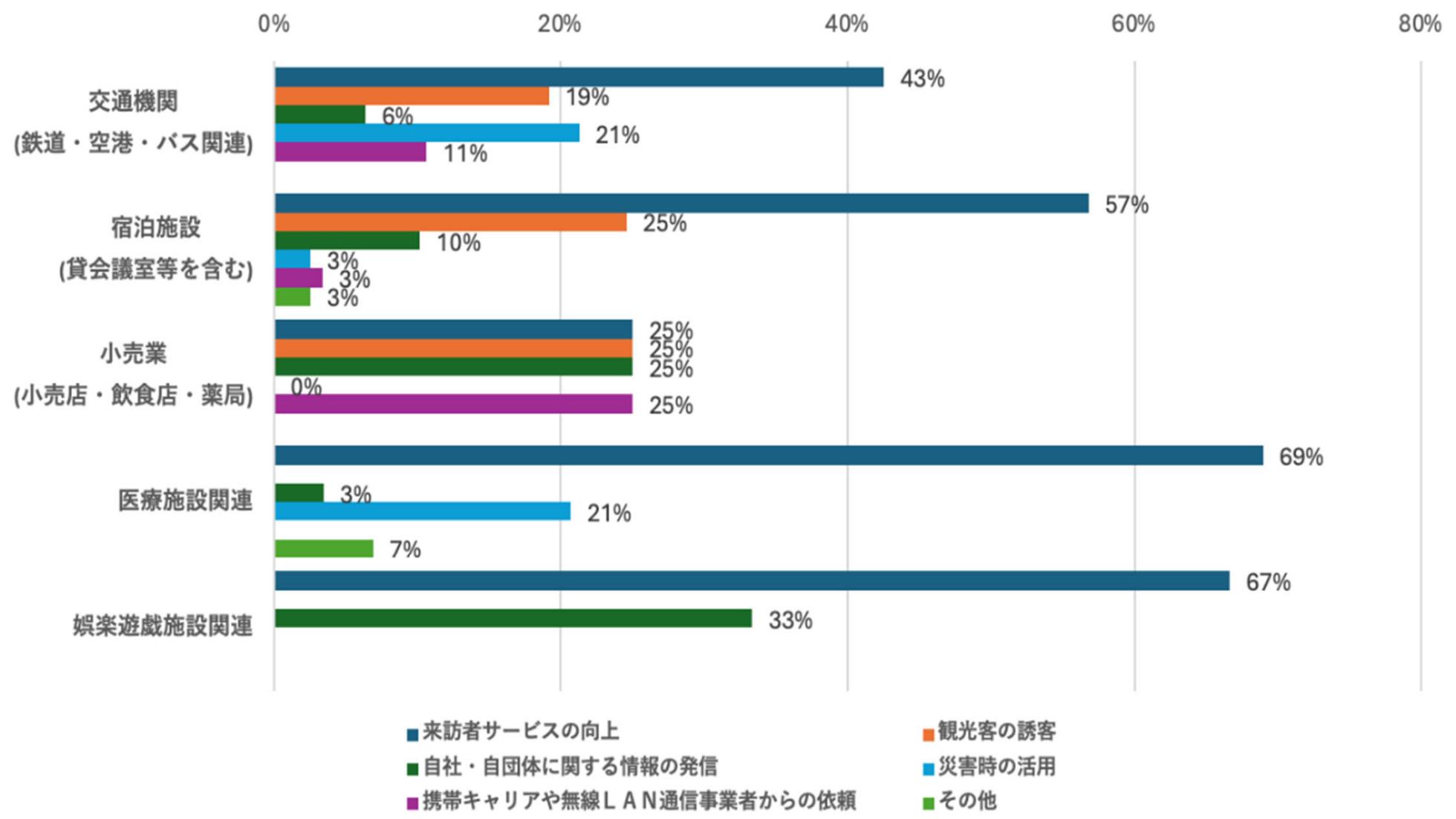
娯楽遊戯施設については分計してまとめたが、サンプル数が少なく、考察の対象外となる事例も生まれた。

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。

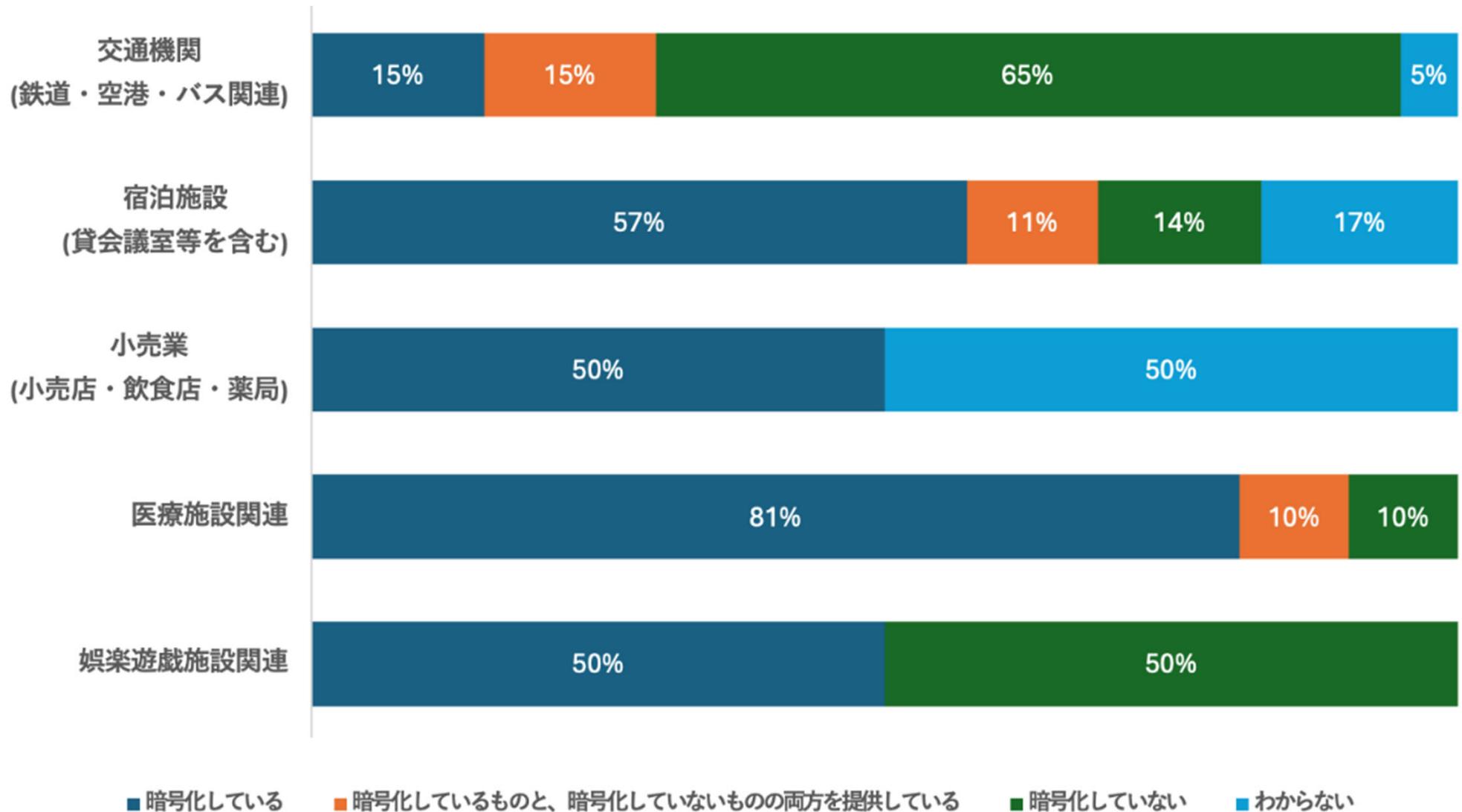
無線LANサービスの目的 (Q7) (業種ベース)

➤ 「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、医療施設関連が多い。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。



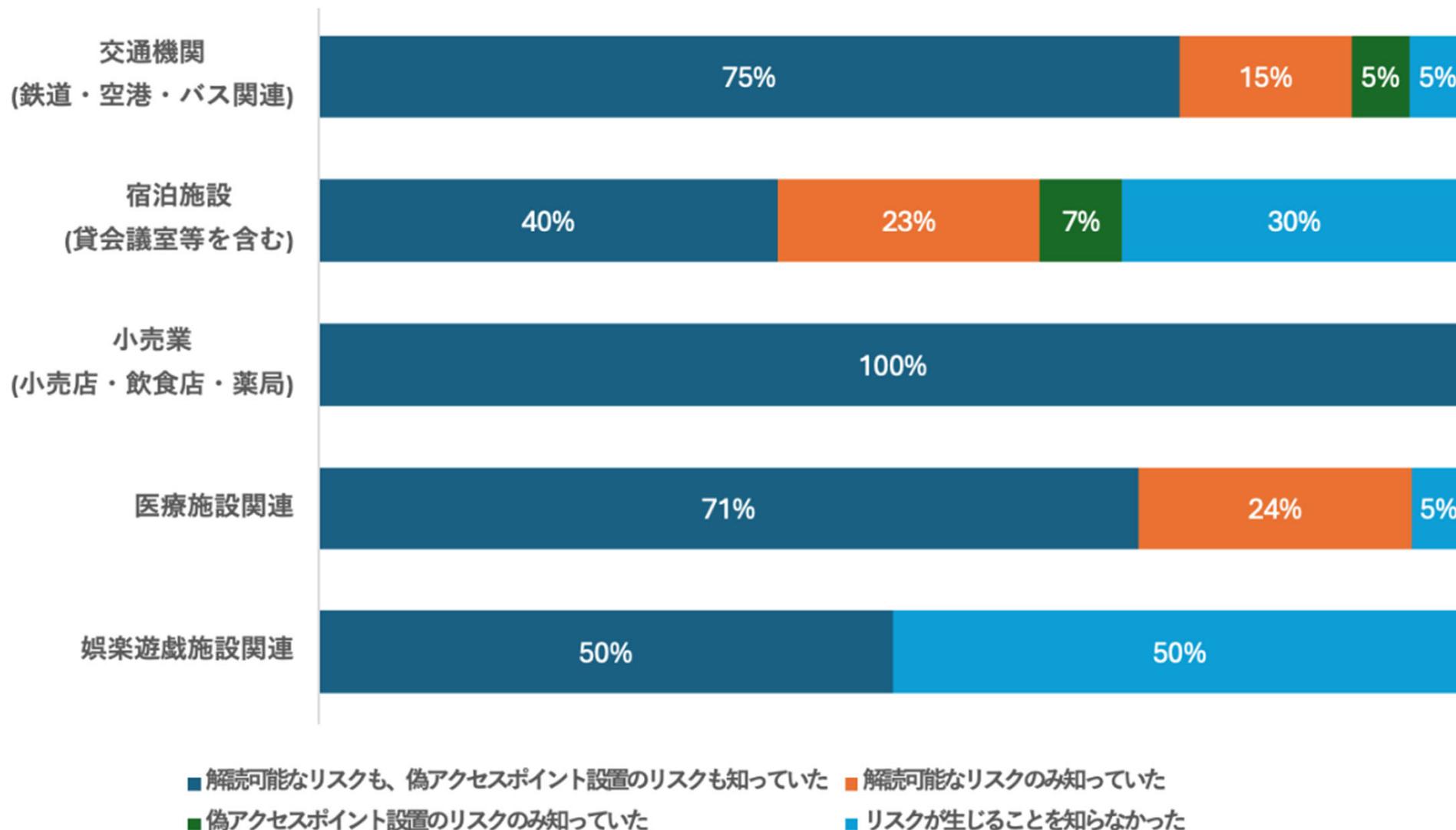
無線LANサービスの暗号化（Q9）（業種ベース）

- 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。



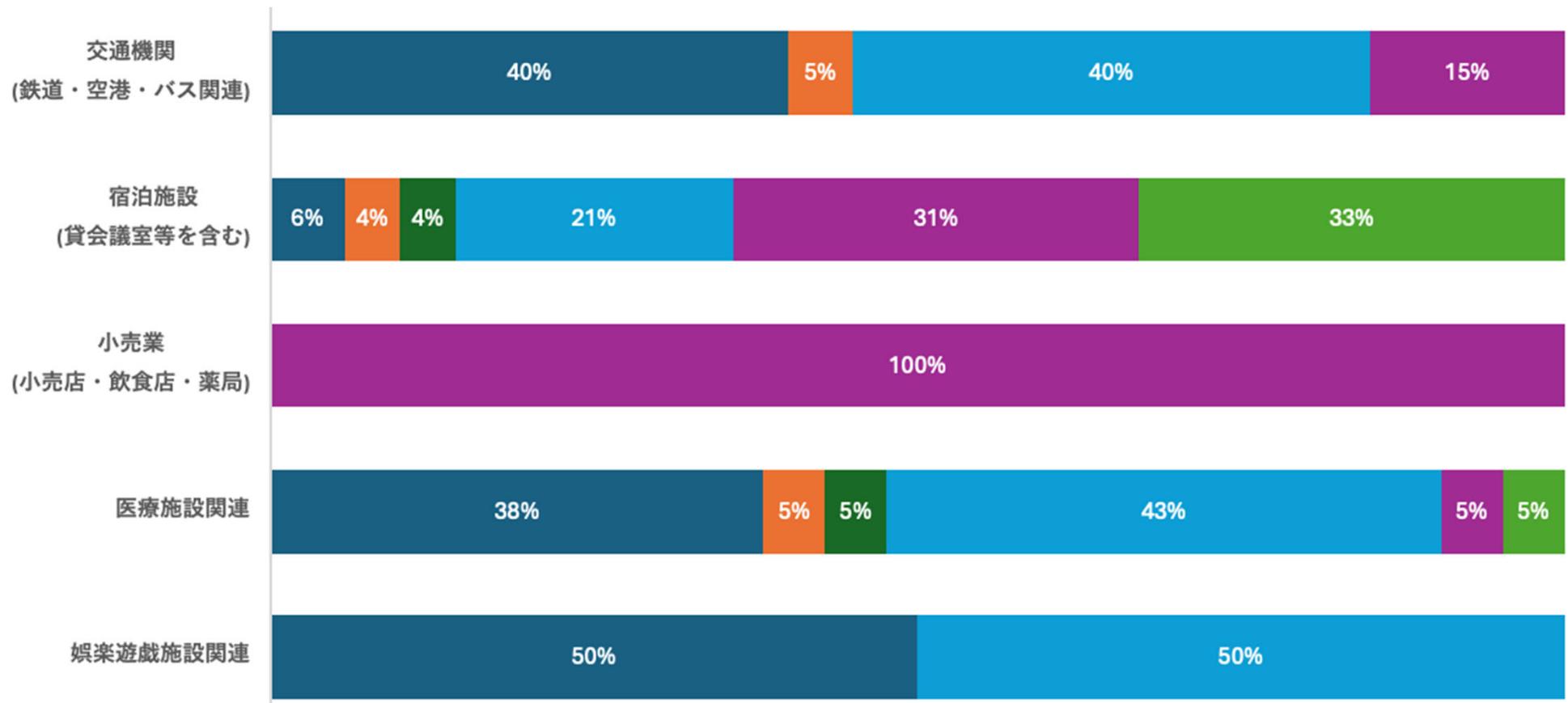
セキュリティリスクに対する認識 (Q13) (業種ベース)

➤ 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。



セキュリティ責任者の設置（Q26）（業種ベース）

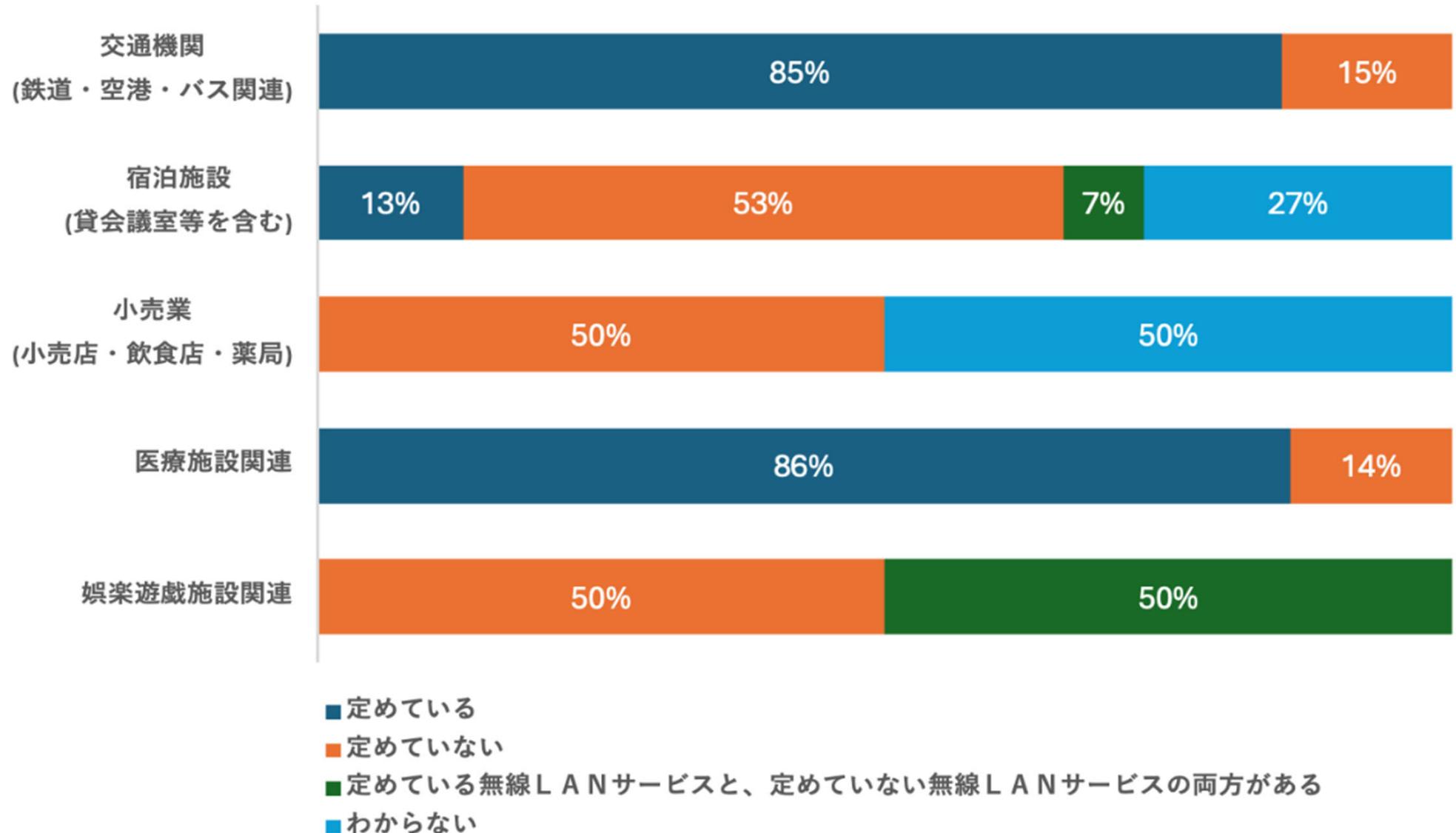
➤ 宿泊施設は「情報セキュリティの責任者が決まっていない」率が多い。小売業については「情報セキュリティの責任者が決まっていない」が全回答を占めた。



- 経営層のCISOを設置している（社内規程等の内部規程で明確に定めている）
- 経営層ではないが、CISOを設置している
- 情報セキュリティの責任者は決まっていない
- 経営層のCISOを設置している（社内規程等の内部規程では定めていない）
- CISOではないが、情報セキュリティの責任者を決めている
- わからない

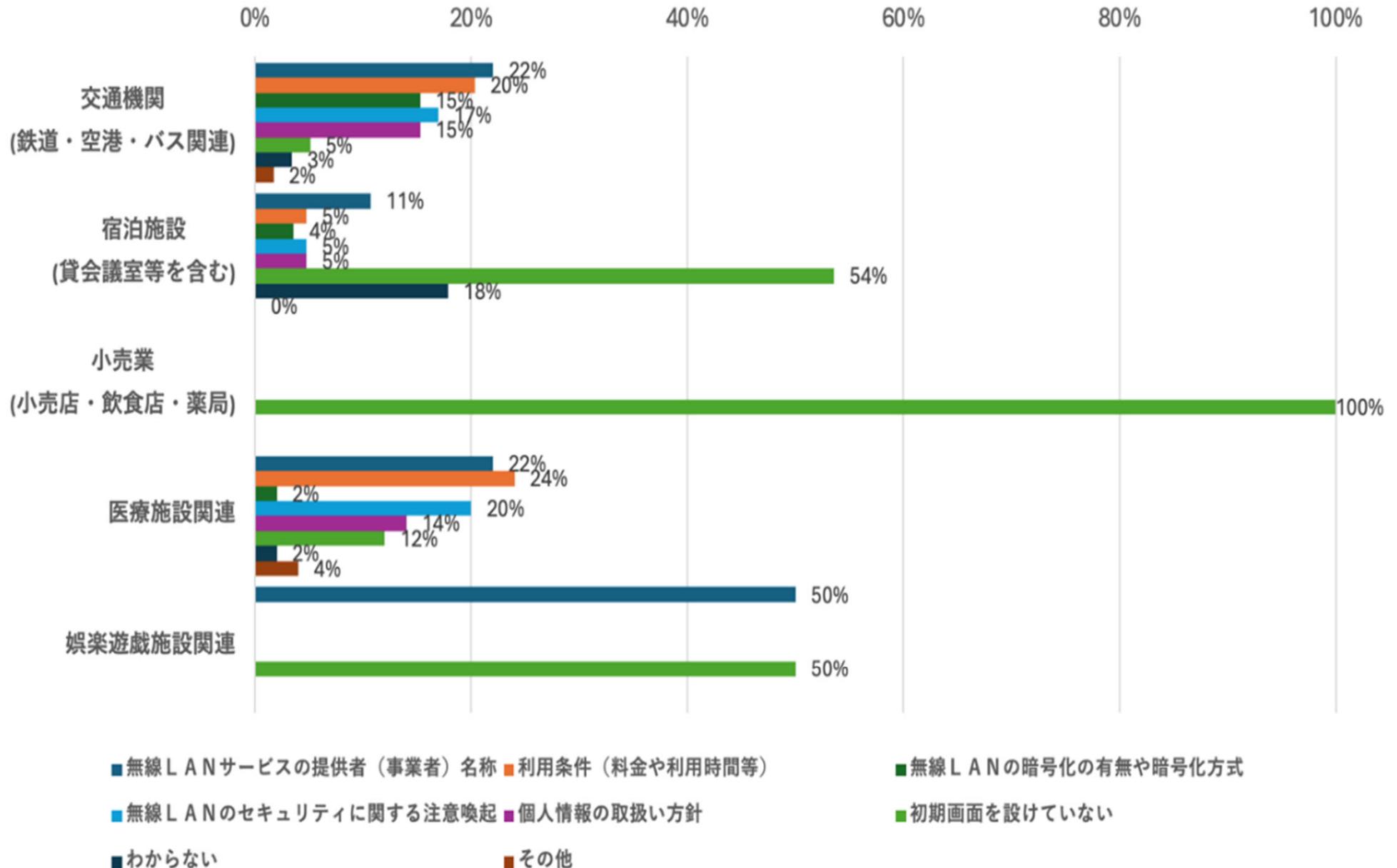
無線LANサービスの利用規約（Q27）（業種ベース）

➤ 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。



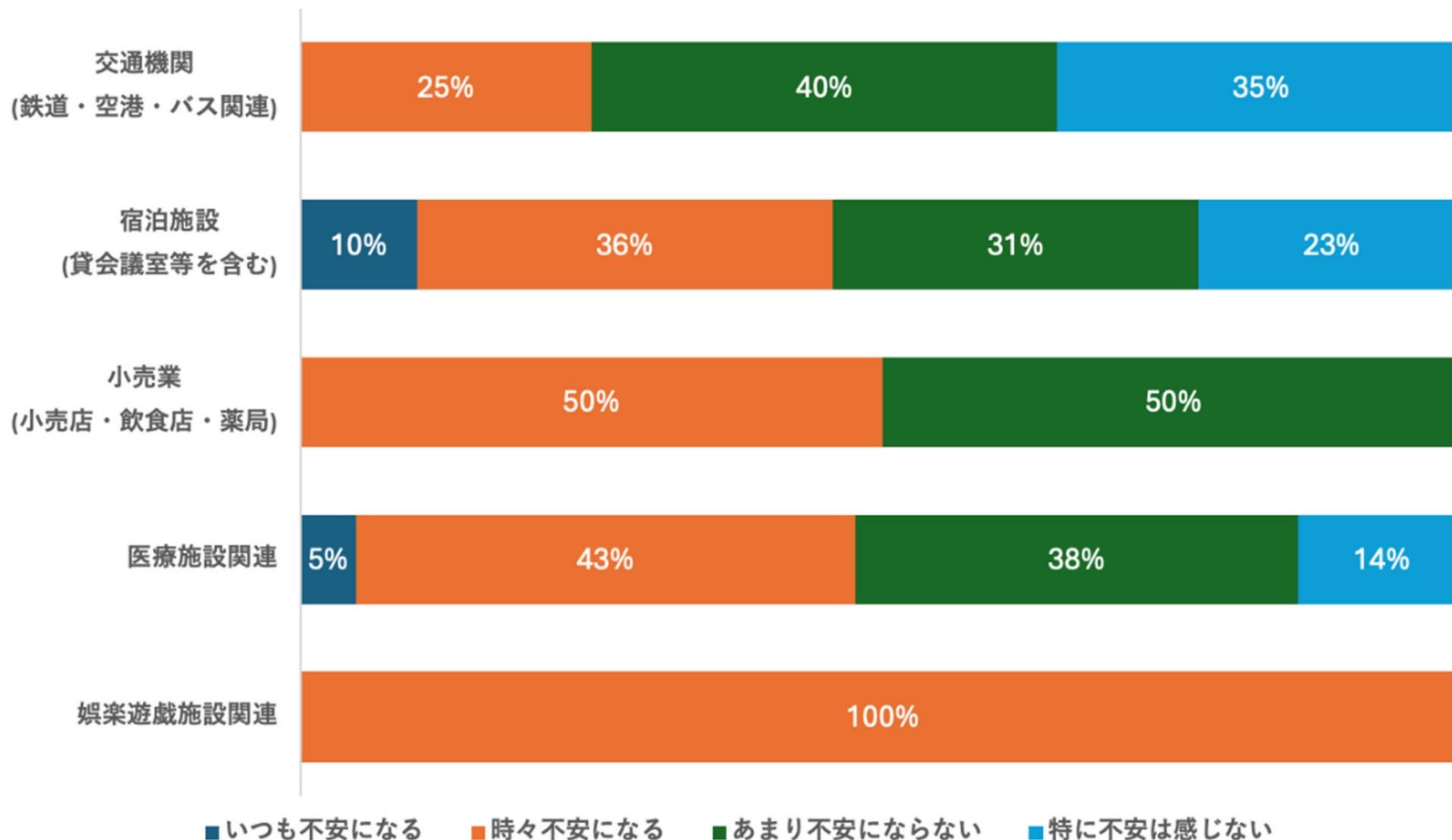
無線LANサービスの初期画面（Q28）（業種ベース）

➤ 宿泊施設、小売業は、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。



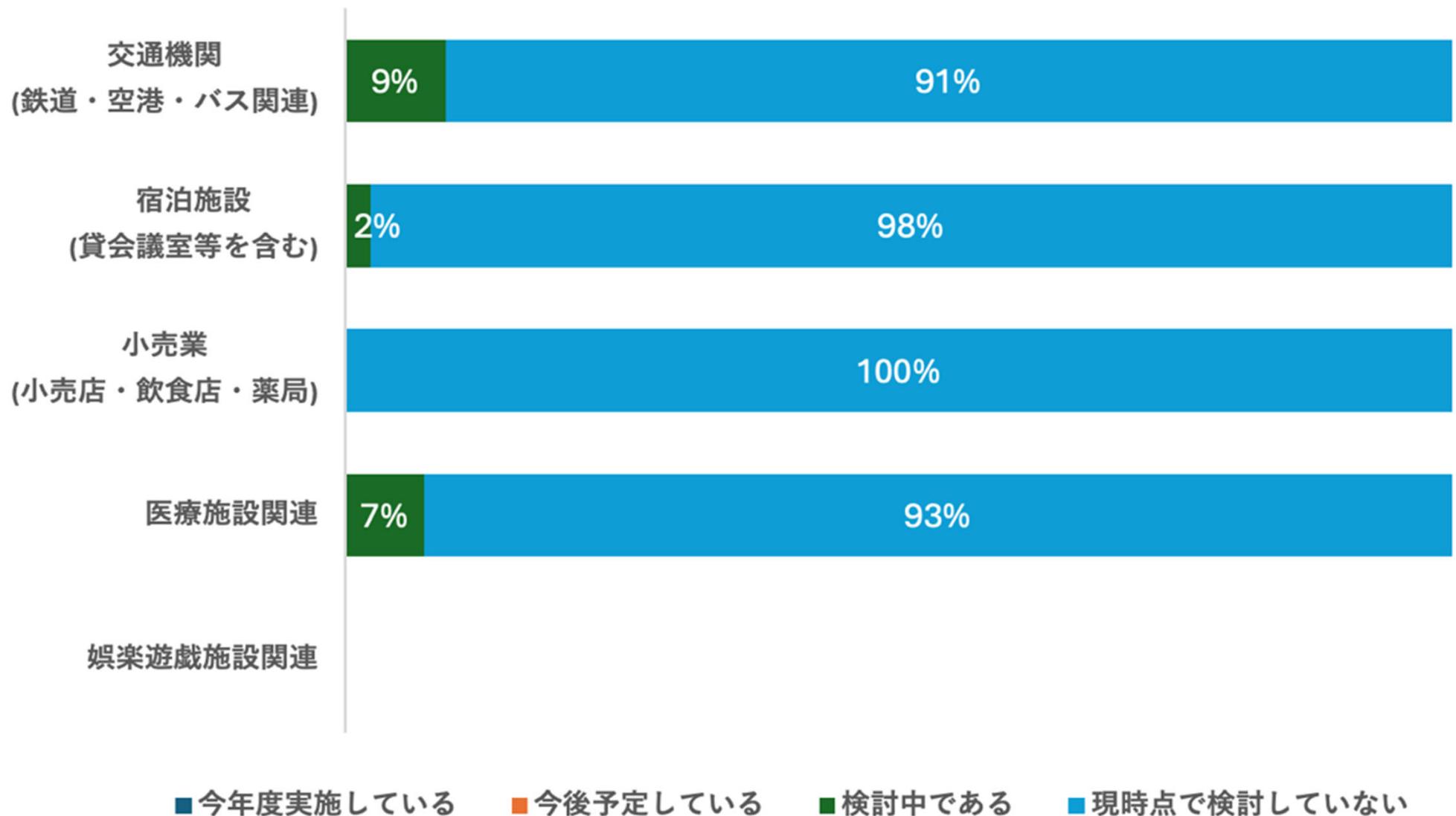
サービスのセキュリティへの不安（Q32）（業種ベース）

➤ 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。



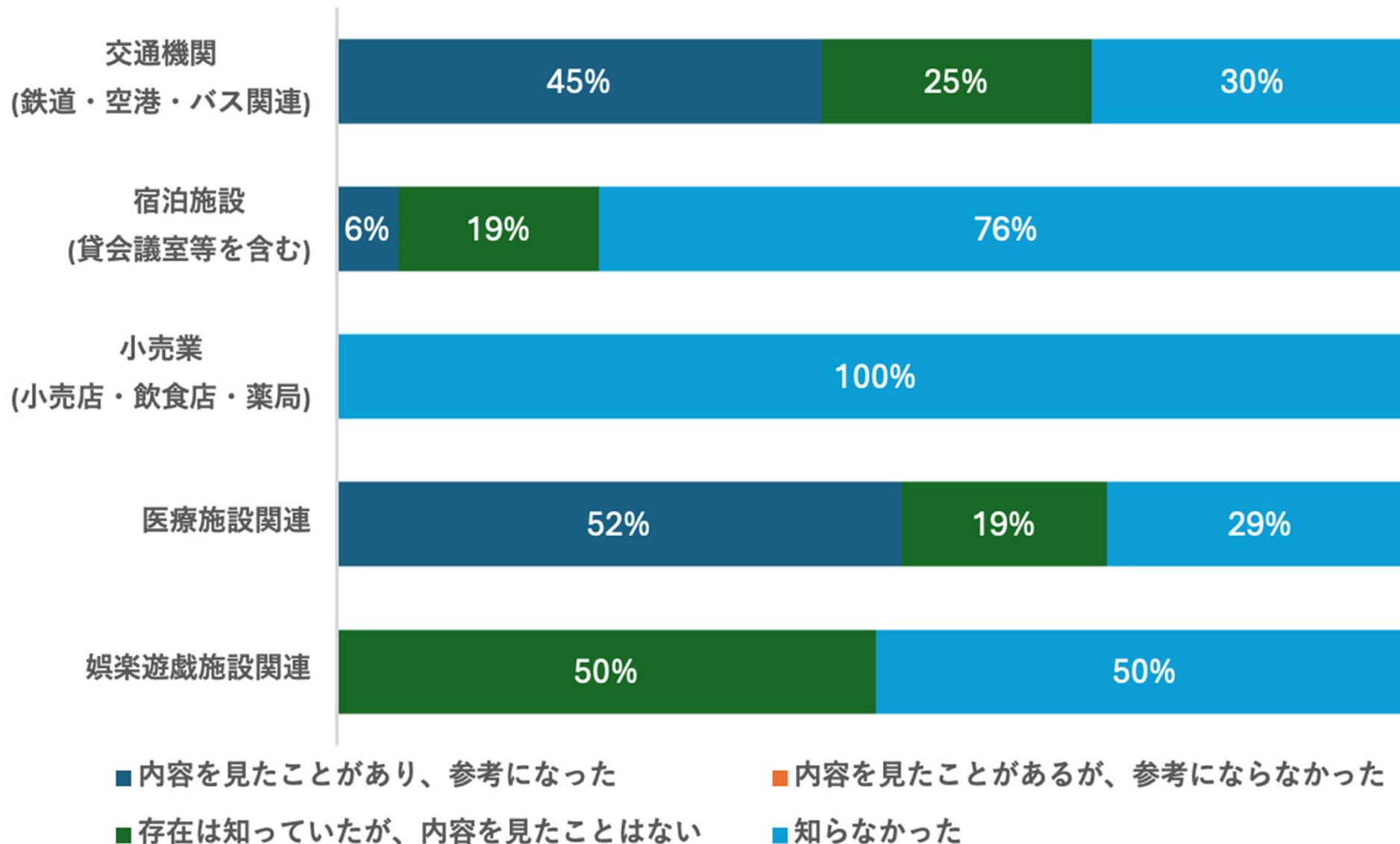
サービスのセキュリティ強化計画（Q35）（業種ベース）

➤ 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。



セキュリティ対策の手引き（Q40）（業種ベース）

➤ 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。



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

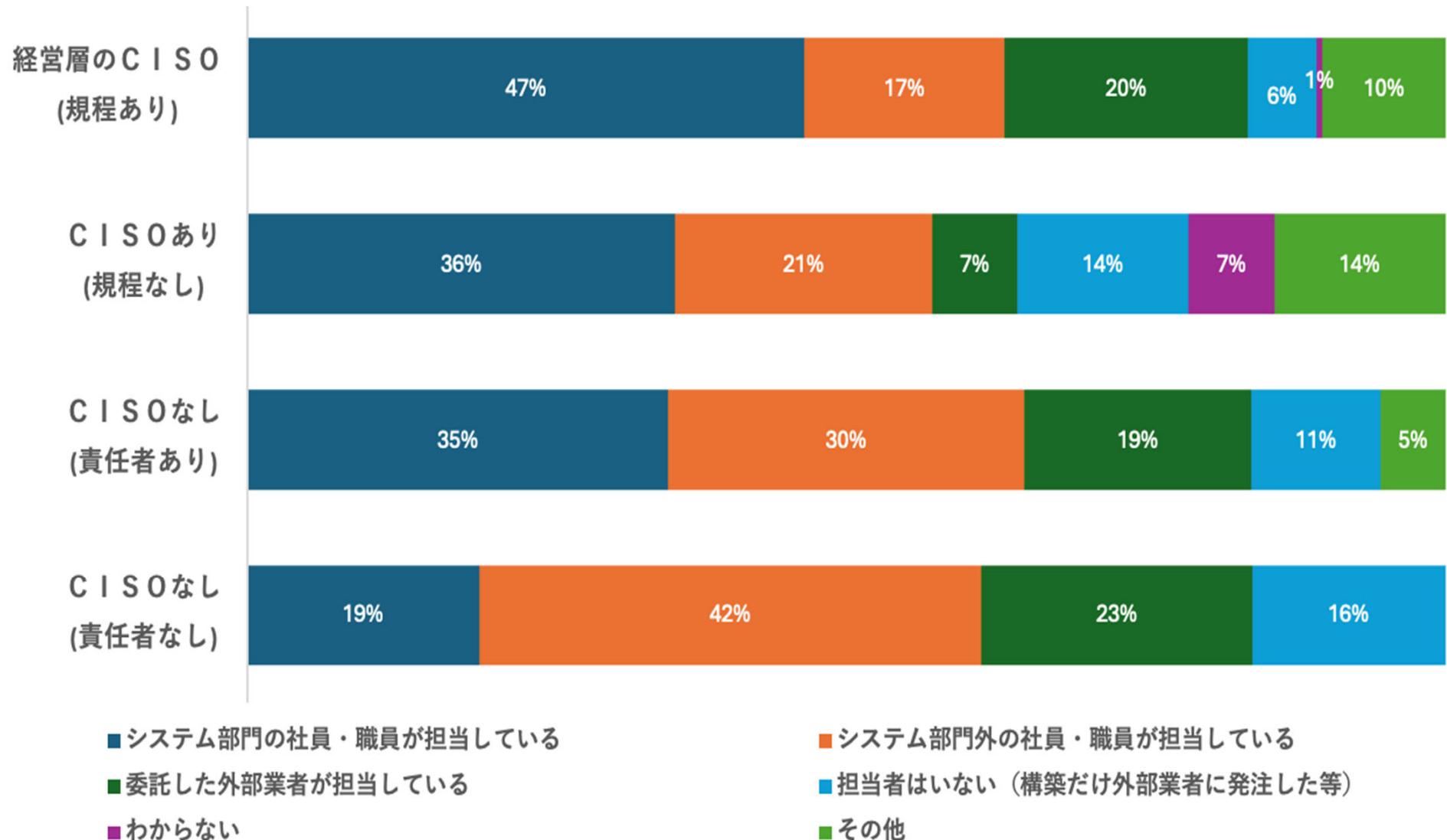
Q22の設問（セキュリティ責任者を設定）をベースに、自治体データを対象として解析を本年も行った。

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。

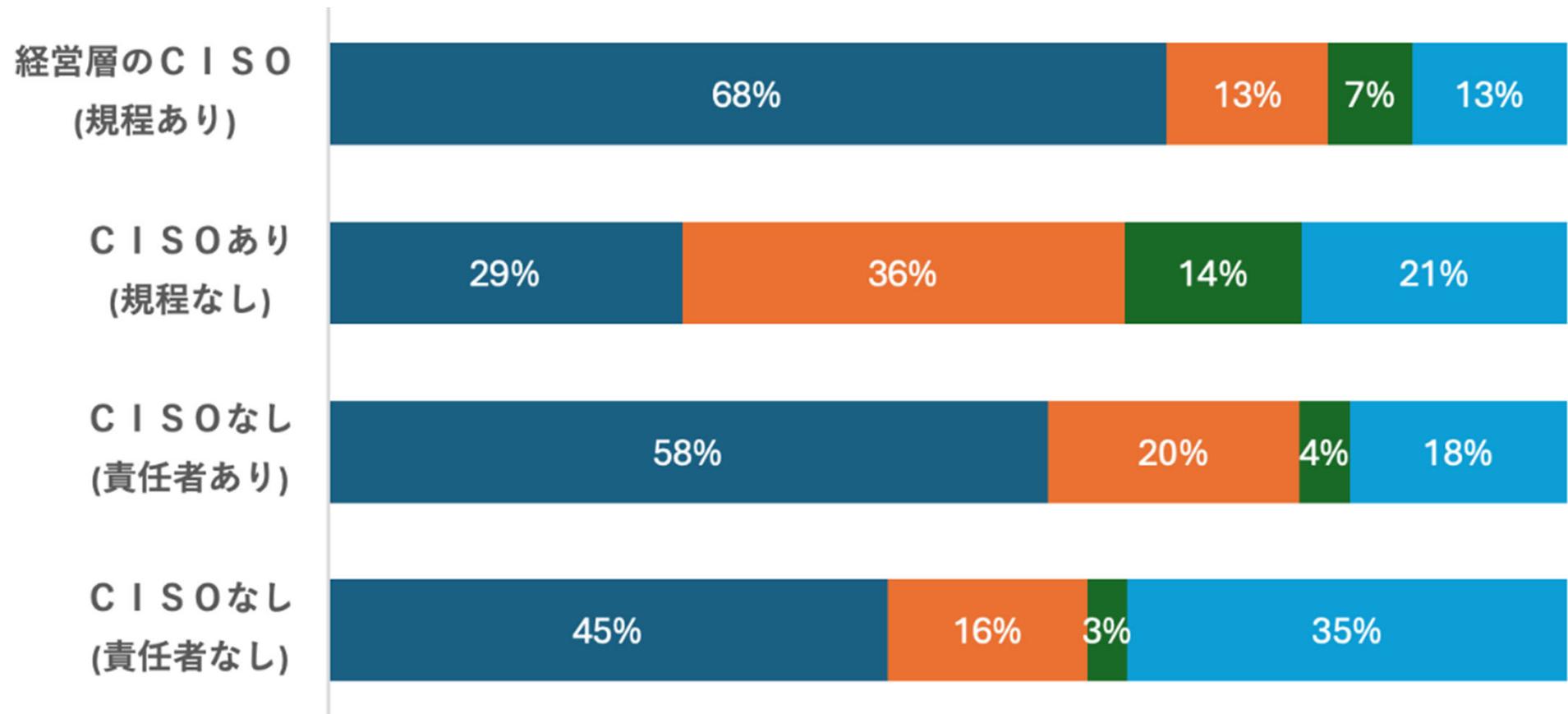
無線LANサービスの運用管理（Q6）（管理者有無ベース）

- 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。



セキュリティリスクに対する認識 (Q13) (管理者有無ベース)

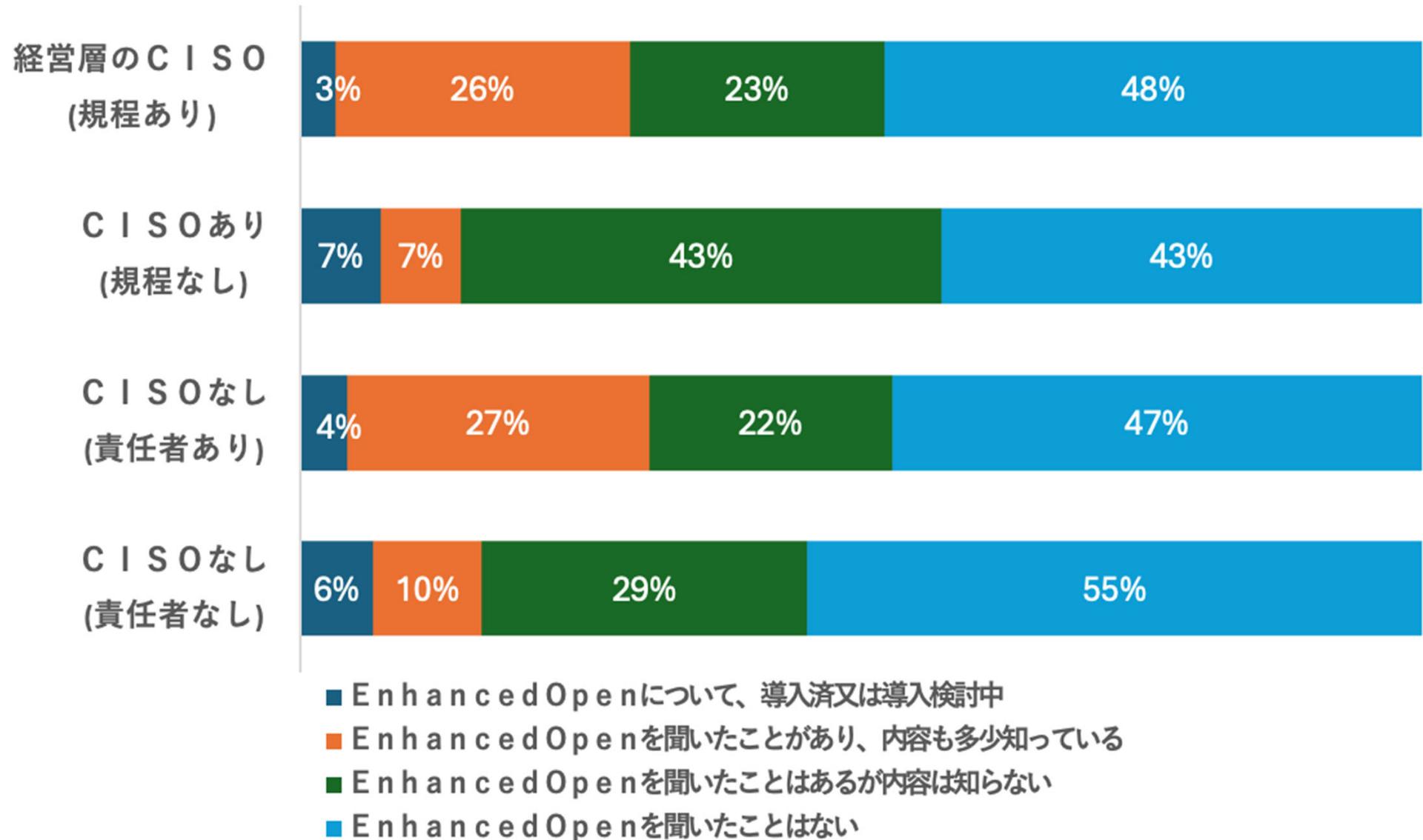
- セキュリティ責任者を設置している方が、セキュリティリスクの認識率が高い。さらに経営層の責任者を設置しているところは、それ以上に高い数値が出ている。



- 解読可能なリスクも、偽アクセスポイント設置のリスクも知っていた
- 解読可能なリスクのみ知っていた
- 偽アクセスポイント設置のリスクのみ知っていた
- リスクが生じることを知らなかった

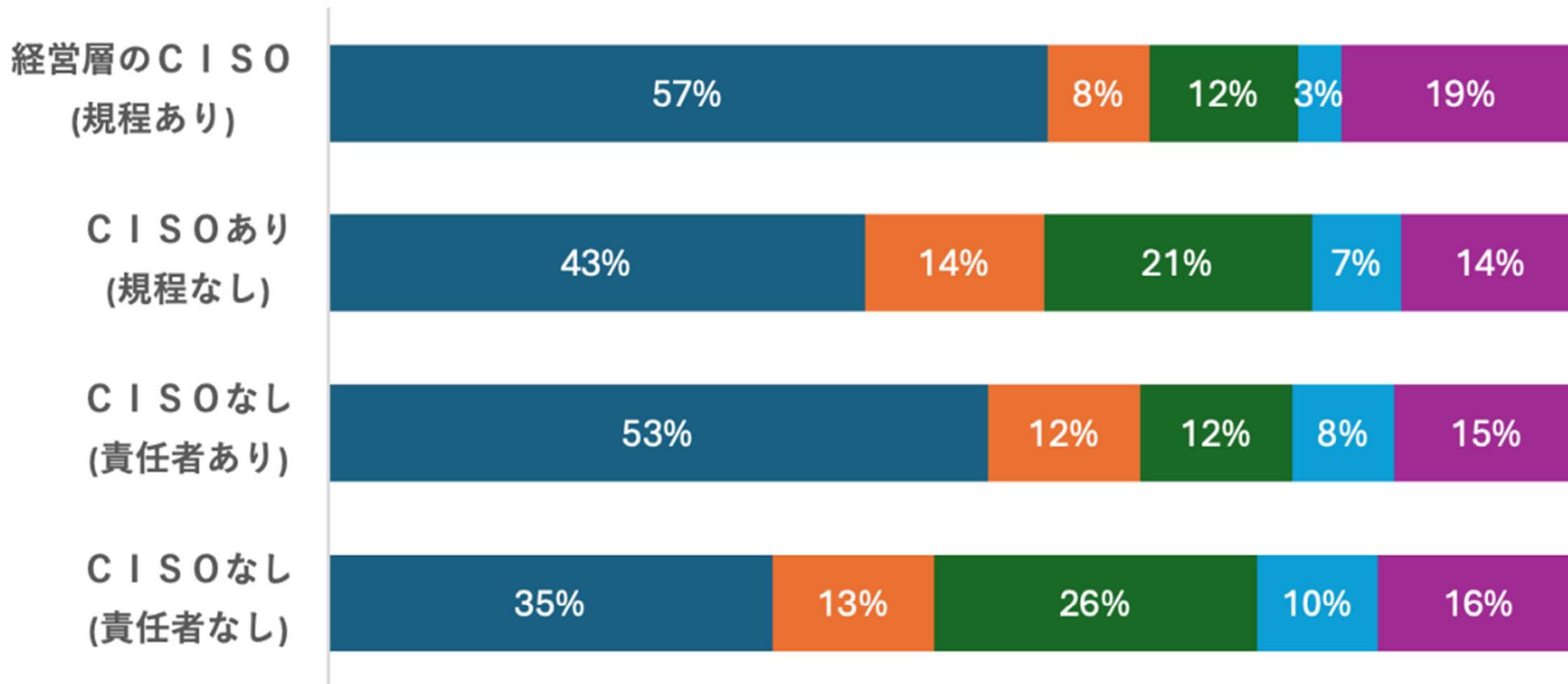
新しい暗号化方式（Enhanced Open）（Q15）（管理者有無ベース）

- 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。



管理者パスワードの管理 (Q18) (管理者有無ベース)

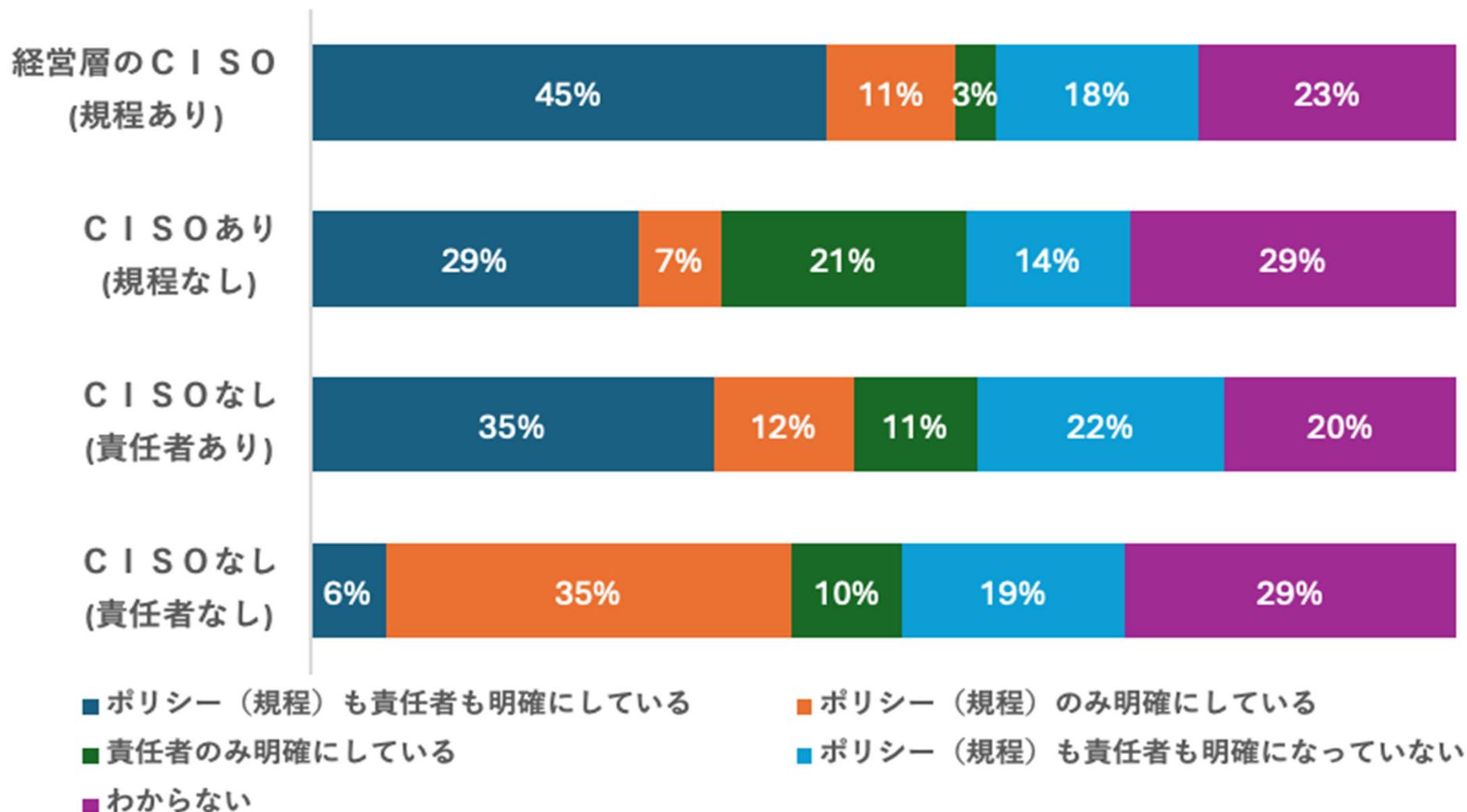
➤ セキュリティ責任者を設置しているものは、パスワードの管理が適切に行われている率が高い。特に、責任者を設置していないところは、パスワードを「初期設定のまま使用している」率が高い。



- 初期設定から変更している (第三者から推測されにくいものを設定している)
- 初期設定から変更している (第三者から推測されやすいものかどうか検討していない)
- 初期設定のまま使用している (初期設定のパスワードが十分複雑なものであった)
- 初期設定のまま使用している (初期設定のパスワードを気にしていない)
- わからない

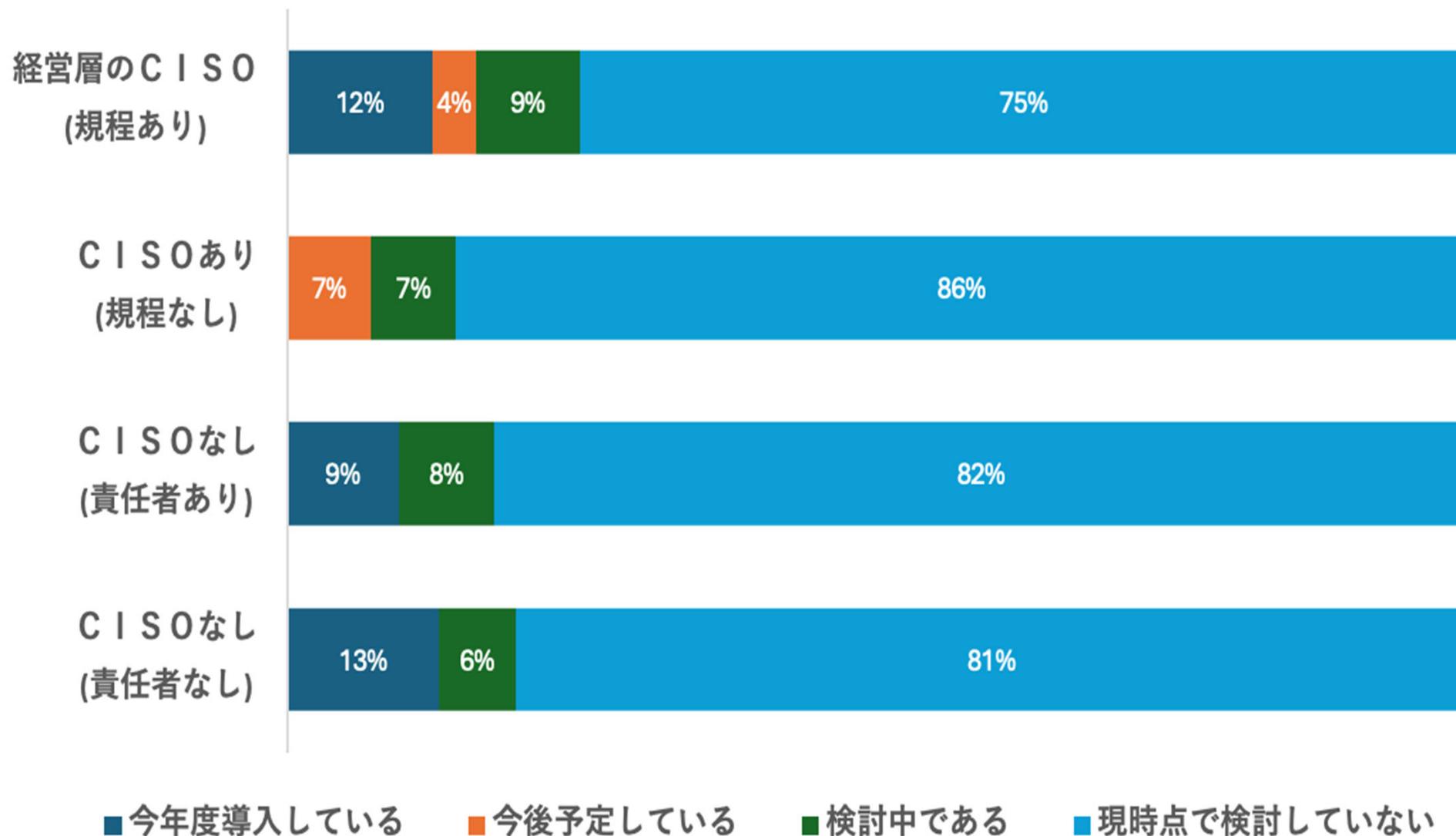
利用者情報のデータ保護（Q31）（管理者有無ベース）

- 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。



Wi-Fi 6の導入予定（Q37）（管理者有無ベース）

➤ 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。



セキュリティ対策の手引き（Q40）（管理者有無ベース）

- 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。

