# 「企業IT利活用動向調査2021」
# 集計結果（詳細版）

本資料は、JIPDECと株式会社アイ・ティ・アールが2021年1月に実施した「企業IT利活用動向調査2021」の集計結果をまとめたものです。

2021年5月31日

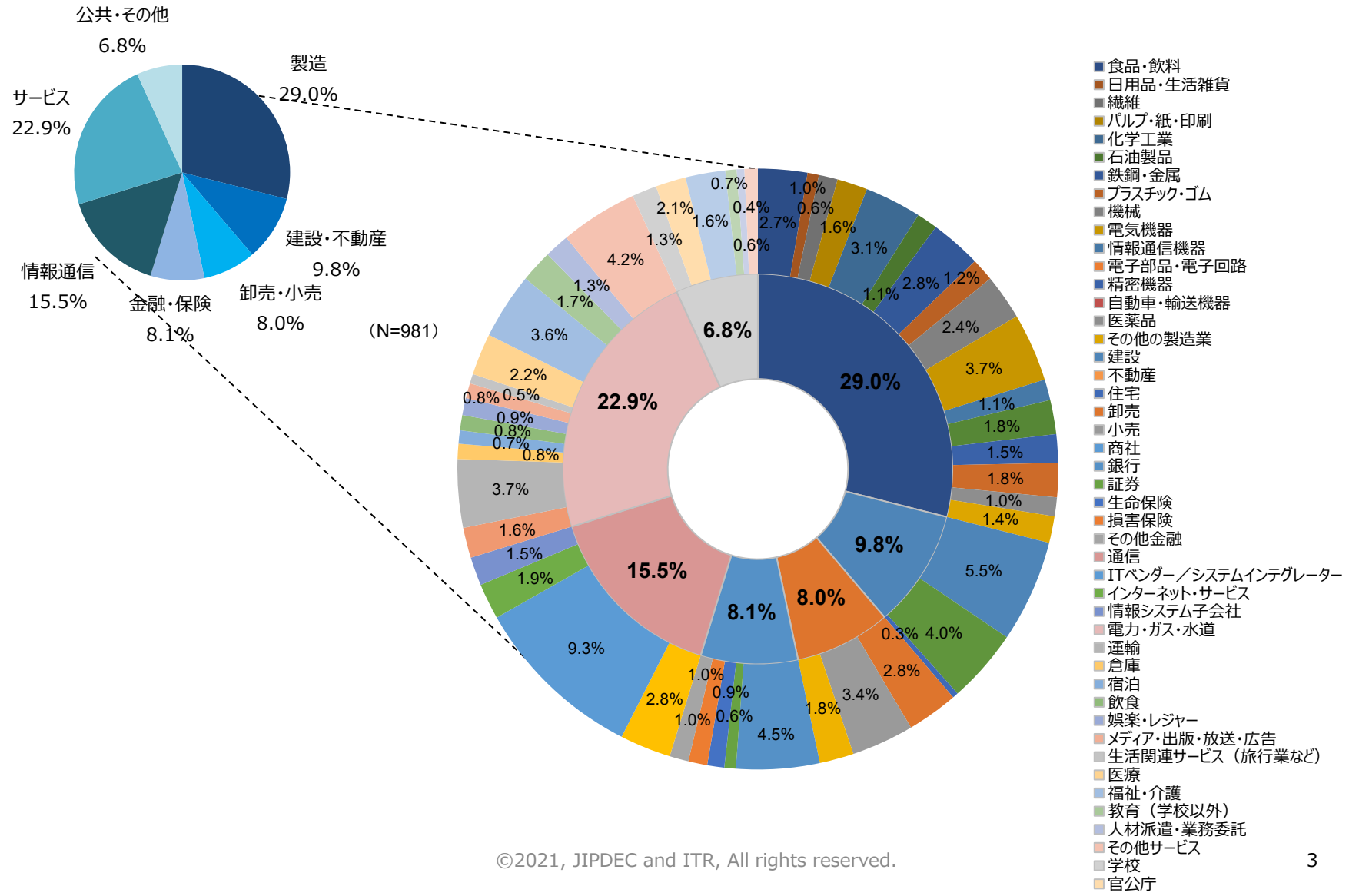
一般財団法人日本情報経済社会推進協会

# 調査概要

| | | |
|---|---|---|
| 実査期間 | ： | 2021年1月13日～1月15日 |
| 実施主体 | ： | 一般財団法人日本情報経済社会推進協会<br>株式会社アイ・ティ・アール |
| 調査方式 | ： | ITR独自パネルを利用したWebアンケート |
| 調査対象 | ： | 以下の条件を満たす個人：**約9,000人**<br>• 従業員数50人以上の国内企業の勤務者であること<br>• 情報システム、経営企画、総務・人事、業務改革系部門のいずれかに所属していること<br>• IT戦略策定または情報セキュリティの従事者であること<br>• **係長相当職以上**の役職者であること |
| 有効回答数 | ： | 981件（1社1人） |

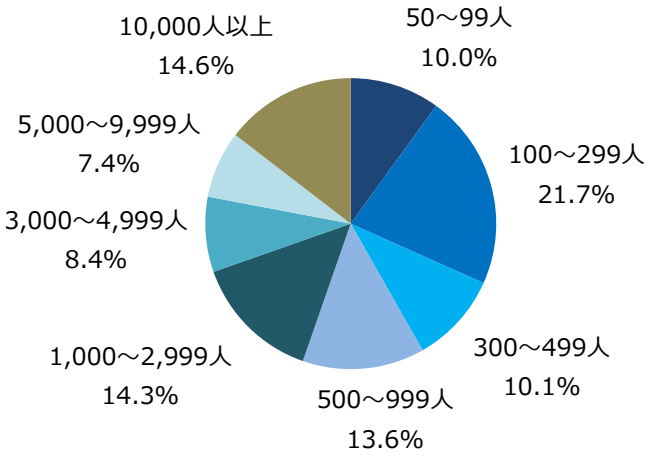
# 2021年調査：回答者プロフィール①

## 勤務先の業種



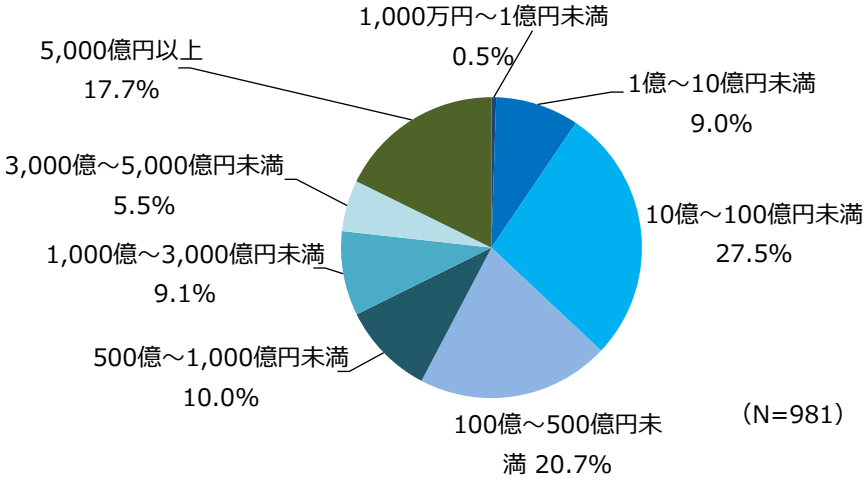
# 2021年調査：回答者プロフィール②

## 勤務先の従業員規模



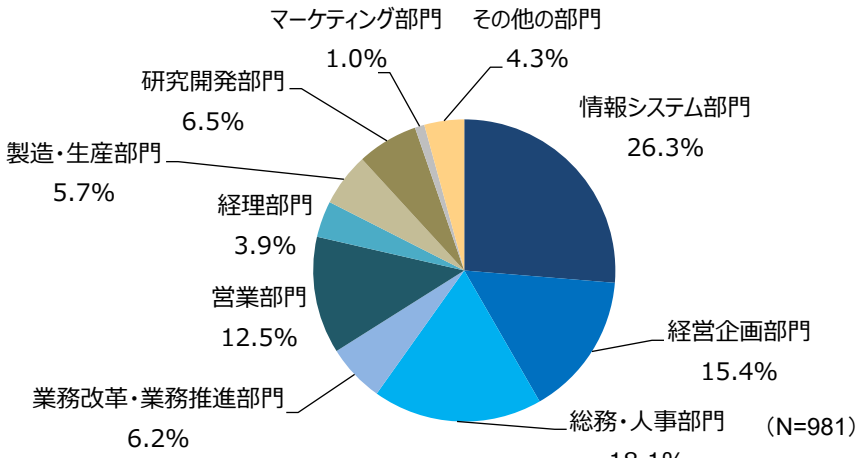

（N=981）

## 勤務先の売上規模



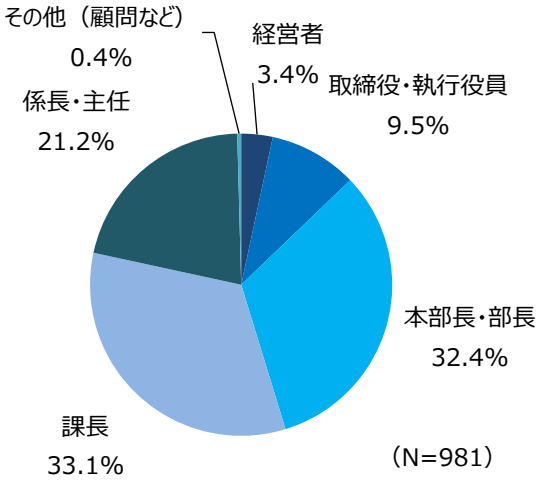

（N=981）

## 所属部門




（N=981）

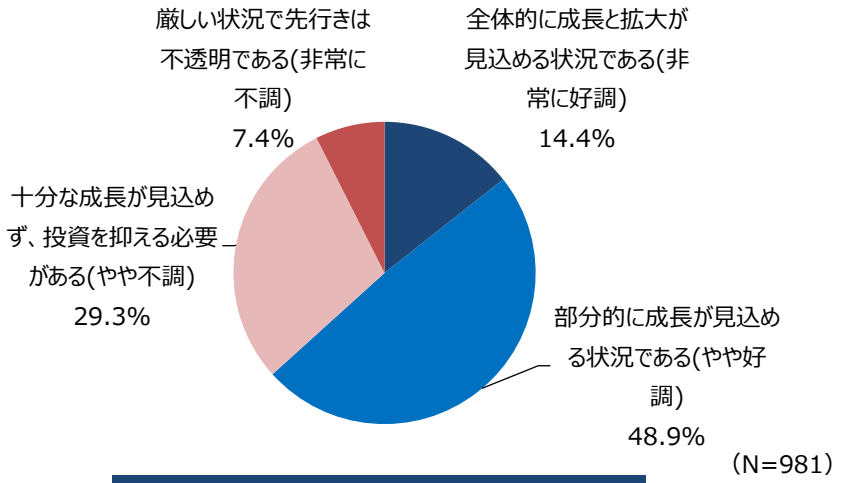
## 役職




（N=981）

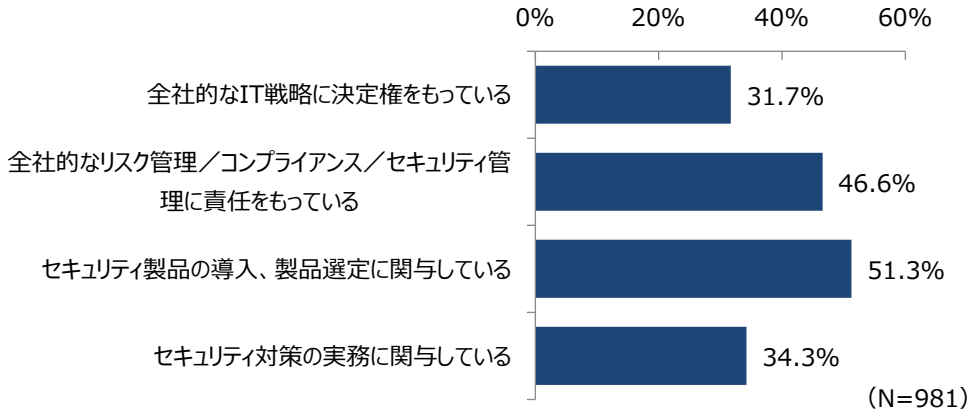
# 2021年調査：回答者プロフィール③

## 勤務先を取り巻くビジネス環境



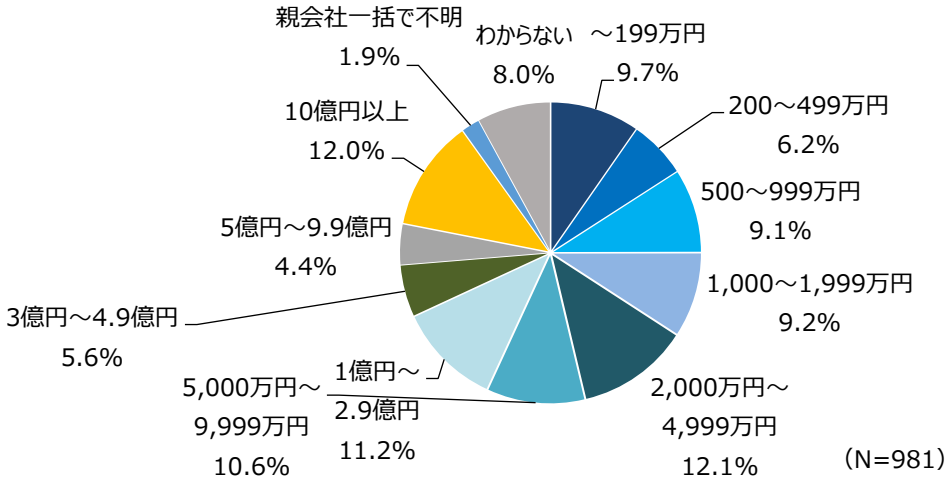

(N=981)

## IT戦略/セキュリティへの関与度




(N=981)

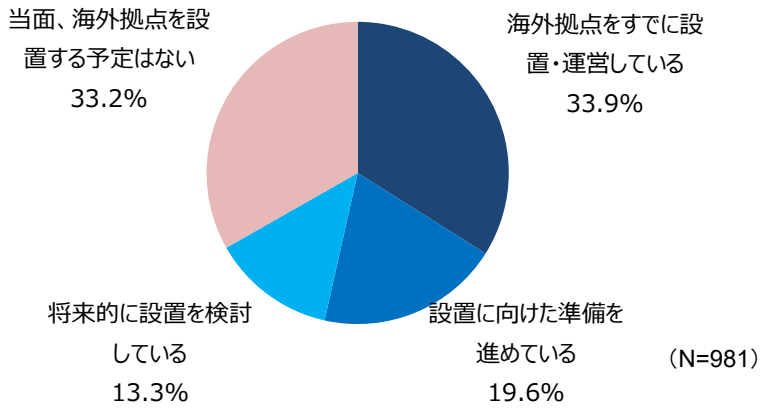
## 年間セキュリティ投資額



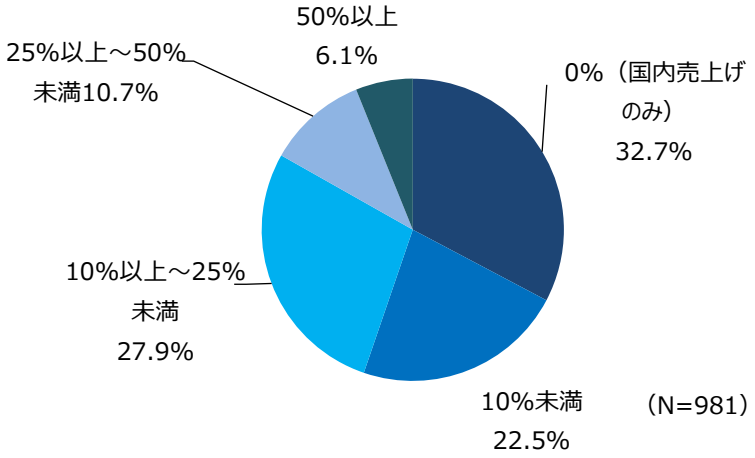

(N=981)

# 2021年調査：回答者プロフィール④

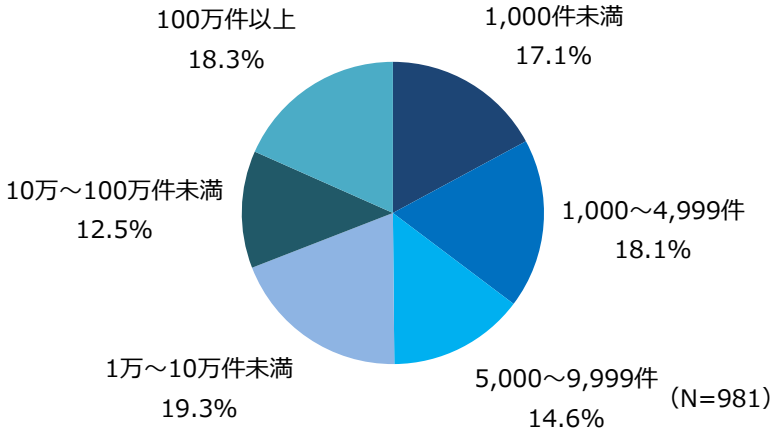
## 海外拠点の設置状況



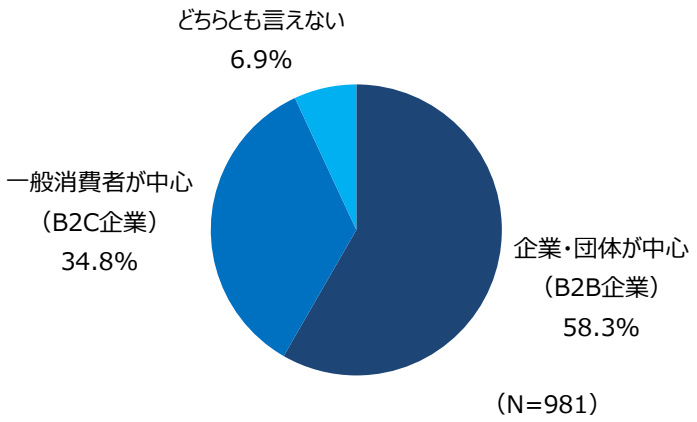

## 海外売上比率




## 個人情報保有件数




## 顧客・取引先のタイプ



# 全体の所見

## 経営課題におけるセキュリティ

■コロナ禍による勤務環境のテレワーク化と事業環境の変化に適合するシステムセキュリティ面の整備が経営課題となっている

## プライバシーガバナンスガイドブックの認知

■プライバシーガバナンスガイドブックの認知が進む

## 働き方改革の施策・システム化

■コロナ禍を受けてテレワークを前提として働き方改革の施策実施とシステム化が具体的に進む

## クラウド利用比率上昇

■コロナ禍を受けてクラウドを利用している比率が上昇

## 情報セキュリティ監査は前回同様

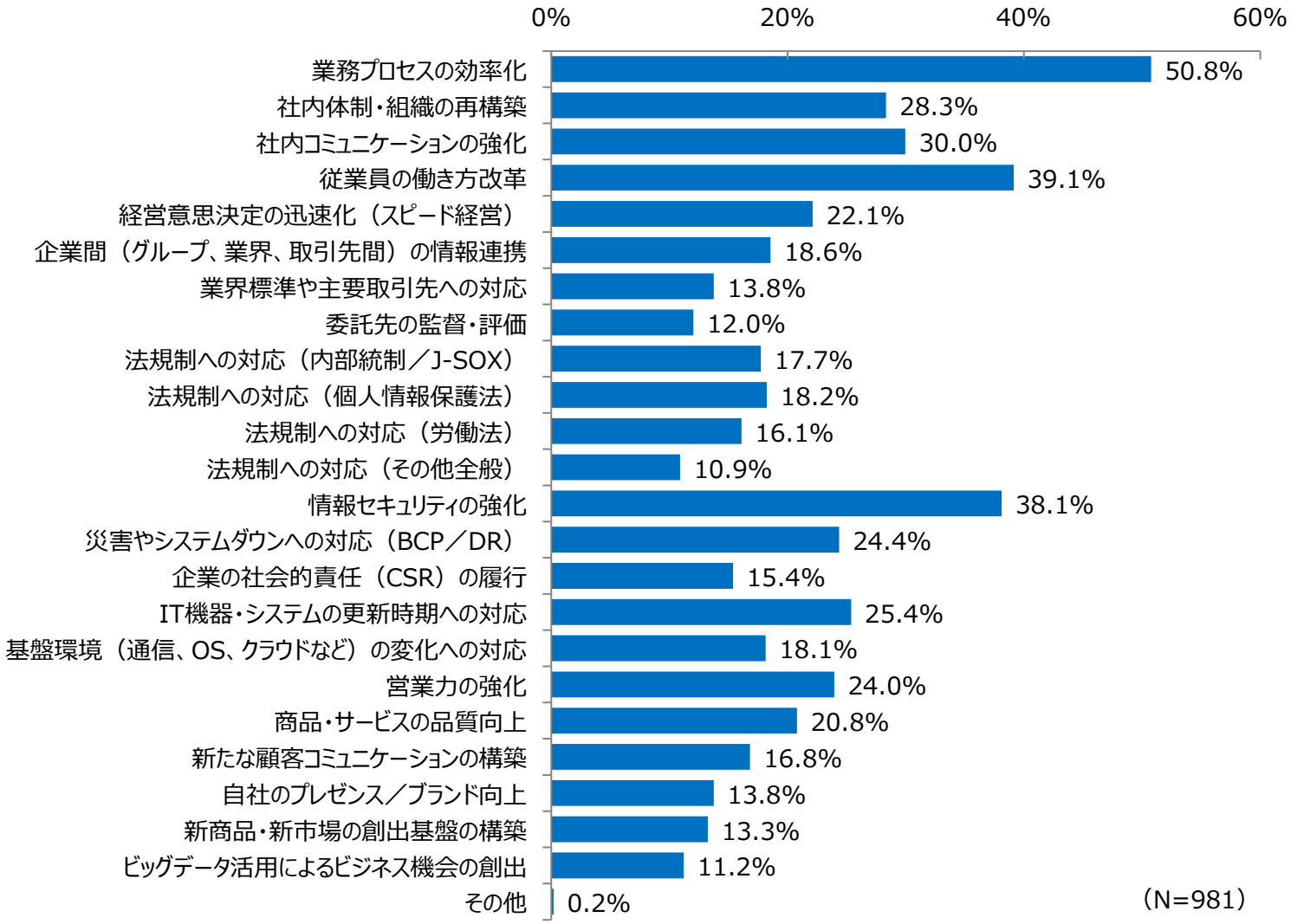
■情報セキュリティ監査の実施企業比率は前回と同様

# 1）経営課題におけるセキュリティの位置づけ

- Q1：　重視する経営課題
- Q2：　過去1年間に経験したセキュリティインシデント
- Q3：　セキュリティリスクの重視度合い

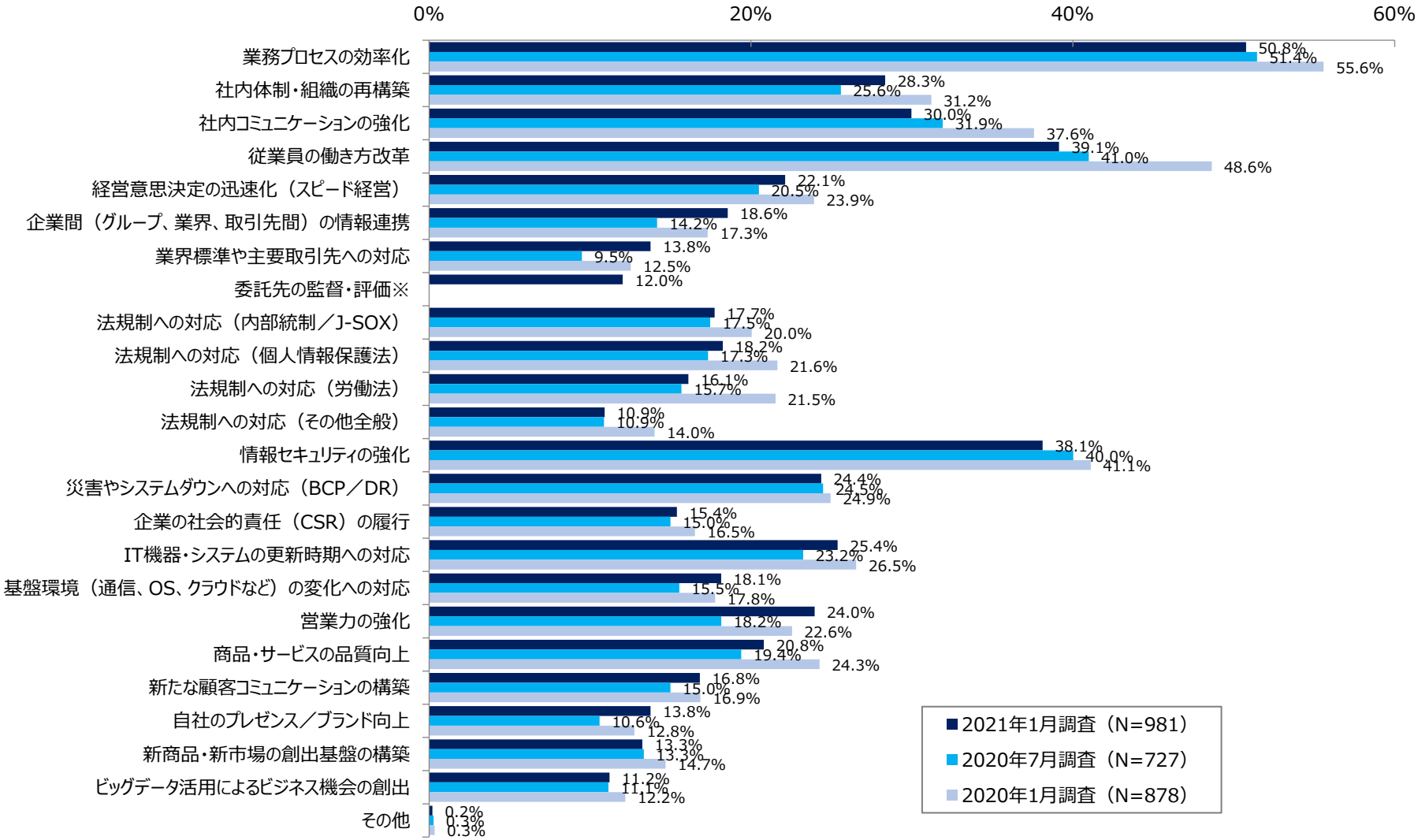
# Q1：重視する経営課題（2021年調査）

■「業務プロセスの効率化」、「従業員の働き方改革」、「情報セキュリティの強化」の順で、大きな傾向の変化は見られないが、過去２回との比較ではコロナ禍への対応が経営課題となっていることがわかる。



# Q1：重視する経営課題（2020～2021年比較）

■ 「基盤環境の変化への対応」、「営業力の強化」、「自社のプレゼンス／ブランドの向上」が過去最高となっており、コロナ禍による事業環境の変化への対応が経営課題となっていることがわかる。




※2021年1月のみ調査

# Q1：重視する経営課題［業種別］（2021年調査）

■ 公共・その他で「社内体制・組織の再構築」、建設・不動産で「従業員の働き方改革」、卸売・小売で「営業力の強化」と「新たな顧客コミュニケーションの構築」が高くなっている。

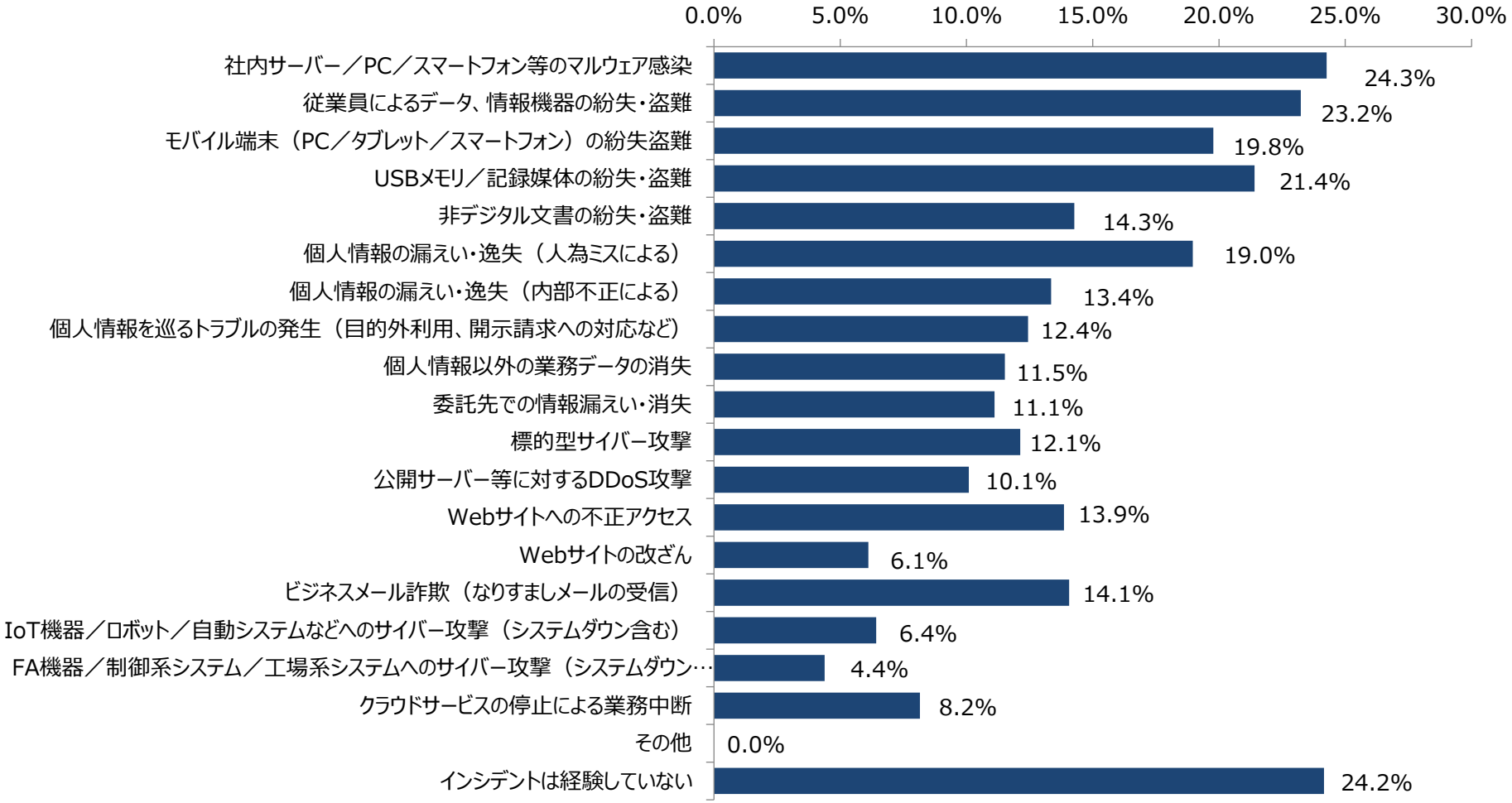
| | 製造（N=284） | 建設・不動産（N=96） | 卸売・小売（N=78） | 金融・保険（N=79） | 情報通信（N=152） | サービス（N=225） | 公共・その他（N=67） | 全体（N=981） |
|---|---|---|---|---|---|---|---|---|
| 業務プロセスの効率化 | 47.2% | 58.3% | 56.4% | 53.2% | 55.3% | 44.4% | 56.7% | 50.8% |
| 社内体制・組織の再構築 | 23.9% | 30.2% | 26.9% | 21.5% | 30.9% | 30.7% | 40.3% | 28.3% |
| 社内コミュニケーションの強化 | 29.6% | 26.0% | 35.9% | 21.5% | 36.8% | 31.1% | 20.9% | 30.0% |
| 従業員の働き方改革 | 34.9% | 55.2% | 43.6% | 40.5% | 41.4% | 34.2% | 38.8% | 39.1% |
| 経営意思決定の迅速化（スピード経営） | 21.5% | 16.7% | 29.5% | 16.5% | 28.3% | 19.6% | 25.4% | 22.1% |
| 企業間（グループ、業界、取引先間）の情報連携 | 16.5% | 17.7% | 20.5% | 15.2% | 24.3% | 20.4% | 10.4% | 18.6% |
| 業界標準や主要取引先への対応 | 18.3% | 14.6% | 14.1% | 7.6% | 15.1% | 10.2% | 9.0% | 13.8% |
| 委託先の監督・評価 | 12.3% | 9.4% | 11.5% | 11.4% | 13.8% | 12.4% | 10.4% | 12.0% |
| 法規制への対応（内部統制／J-SOX） | 20.4% | 16.7% | 19.2% | 16.5% | 18.4% | 13.8% | 19.4% | 17.7% |
| 法規制への対応（個人情報保護法） | 15.8% | 20.8% | 19.2% | 24.1% | 18.4% | 15.6% | 25.4% | 18.2% |
| 法規制への対応（労働法） | 15.5% | 17.7% | 24.4% | 8.9% | 13.2% | 17.3% | 17.9% | 16.1% |
| 法規制への対応（その他全般） | 8.8% | 10.4% | 16.7% | 10.1% | 13.8% | 11.1% | 7.5% | 10.9% |
| 情報セキュリティの強化 | 34.2% | 31.3% | 47.4% | 32.9% | 46.1% | 36.9% | 46.3% | 38.1% |
| 災害やシステムダウンへの対応（BCP／DR） | 22.2% | 24.0% | 25.6% | 15.2% | 28.9% | 25.3% | 29.9% | 24.4% |
| 企業の社会的責任（CSR）の履行 | 15.8% | 14.6% | 16.7% | 15.2% | 17.1% | 14.2% | 13.4% | 15.4% |
| IT機器・システムの更新時期への対応 | 23.9% | 21.9% | 32.1% | 22.8% | 31.6% | 23.1% | 25.4% | 25.4% |
| 基盤環境（通信、OS、クラウドなど）の変化への対応 | 15.8% | 20.8% | 25.6% | 8.9% | 28.3% | 12.9% | 20.9% | 18.1% |
| 営業力の強化 | 22.2% | 34.4% | 39.7% | 13.9% | 25.7% | 23.6% | 7.5% | 24.0% |
| 商品・サービスの品質向上 | 21.1% | 16.7% | 24.4% | 16.5% | 25.0% | 23.1% | 9.0% | 20.8% |
| 新たな顧客コミュニケーションの構築 | 13.0% | 11.5% | 30.8% | 16.5% | 25.0% | 16.0% | 9.0% | 16.8% |
| 自社のプレゼンス／ブランド向上 | 10.9% | 15.6% | 16.7% | 12.7% | 17.8% | 14.2% | 10.4% | 13.8% |
| 新商品・新市場の創出基盤の構築 | 14.1% | 12.5% | 23.1% | 8.9% | 15.8% | 11.6% | 4.5% | 13.3% |
| ビッグデータ活用によるビジネス機会の創出 | 8.5% | 10.4% | 17.9% | 5.1% | 19.1% | 8.9% | 13.4% | 11.2% |
| その他 | 0.0% | 0.0% | 0.0% | 0.0% | 0.7% | 0.4% | 0.0% | 0.2% |

# Q1：重視する経営課題［従業員規模別］（2021年調査）

| | 5,000人以上（N=216） | 1,000～4,999人（N=222） | 300～999人（N=232） | 50～299人（N=311） | 全体（N=981） |
|---|---|---|---|---|---|
| 業務プロセスの効率化 | 59.3% | 50.5% | 50.9% | 45.0% | 50.8% |
| 社内体制・組織の再構築 | 33.3% | 26.1% | 26.7% | 27.7% | 28.3% |
| 社内コミュニケーションの強化 | 31.9% | 28.8% | 31.0% | 28.6% | 30.0% |
| 従業員の働き方改革 | 42.1% | 36.0% | 43.1% | 36.3% | 39.1% |
| 経営意思決定の迅速化（スピード経営） | 28.2% | 23.0% | 22.0% | 17.4% | 22.1% |
| 企業間（グループ、業界、取引先間）の情報連携 | 26.9% | 18.9% | 16.8% | 13.8% | 18.6% |
| 業界標準や主要取引先への対応 | 20.4% | 14.4% | 15.1% | 7.7% | 13.8% |
| 委託先の監督・評価 | 15.7% | 13.1% | 11.2% | 9.3% | 12.0% |
| 法規制への対応（内部統制／J-SOX） | 24.1% | 18.5% | 16.8% | 13.5% | 17.7% |
| 法規制への対応（個人情報保護法） | 22.2% | 18.9% | 19.0% | 14.5% | 18.2% |
| 法規制への対応（労働法） | 19.0% | 16.2% | 16.4% | 13.8% | 16.1% |
| 法規制への対応（その他全般） | 14.8% | 13.5% | 9.1% | 7.7% | 10.9% |
| 情報セキュリティの強化 | 44.9% | 39.6% | 41.4% | 29.9% | 38.1% |
| 災害やシステムダウンへの対応（BCP／DR） | 30.6% | 23.4% | 22.4% | 22.2% | 24.4% |
| 企業の社会的責任（CSR）の履行 | 22.7% | 17.1% | 15.5% | 9.0% | 15.4% |
| IT機器・システムの更新時期への対応 | 28.7% | 19.4% | 29.7% | 24.1% | 25.4% |
| 基盤環境（通信、OS、クラウドなど）の変化への対応 | 25.5% | 16.7% | 19.0% | 13.5% | 18.1% |
| 営業力の強化 | 24.1% | 17.6% | 26.3% | 26.7% | 24.0% |
| 商品・サービスの品質向上 | 24.1% | 18.5% | 22.8% | 18.6% | 20.8% |
| 新たな顧客コミュニケーションの構築 | 19.9% | 17.6% | 19.0% | 12.5% | 16.8% |
| 自社のプレゼンス／ブランド向上 | 18.1% | 12.2% | 15.9% | 10.3% | 13.8% |
| 新商品・新市場の創出基盤の構築 | 18.5% | 10.8% | 12.9% | 11.6% | 13.3% |
| ビッグデータ活用によるビジネス機会の創出 | 20.8% | 11.7% | 10.3% | 4.8% | 11.2% |
| その他 | 0.5% | 0.0% | 0.0% | 0.3% | 0.2% |

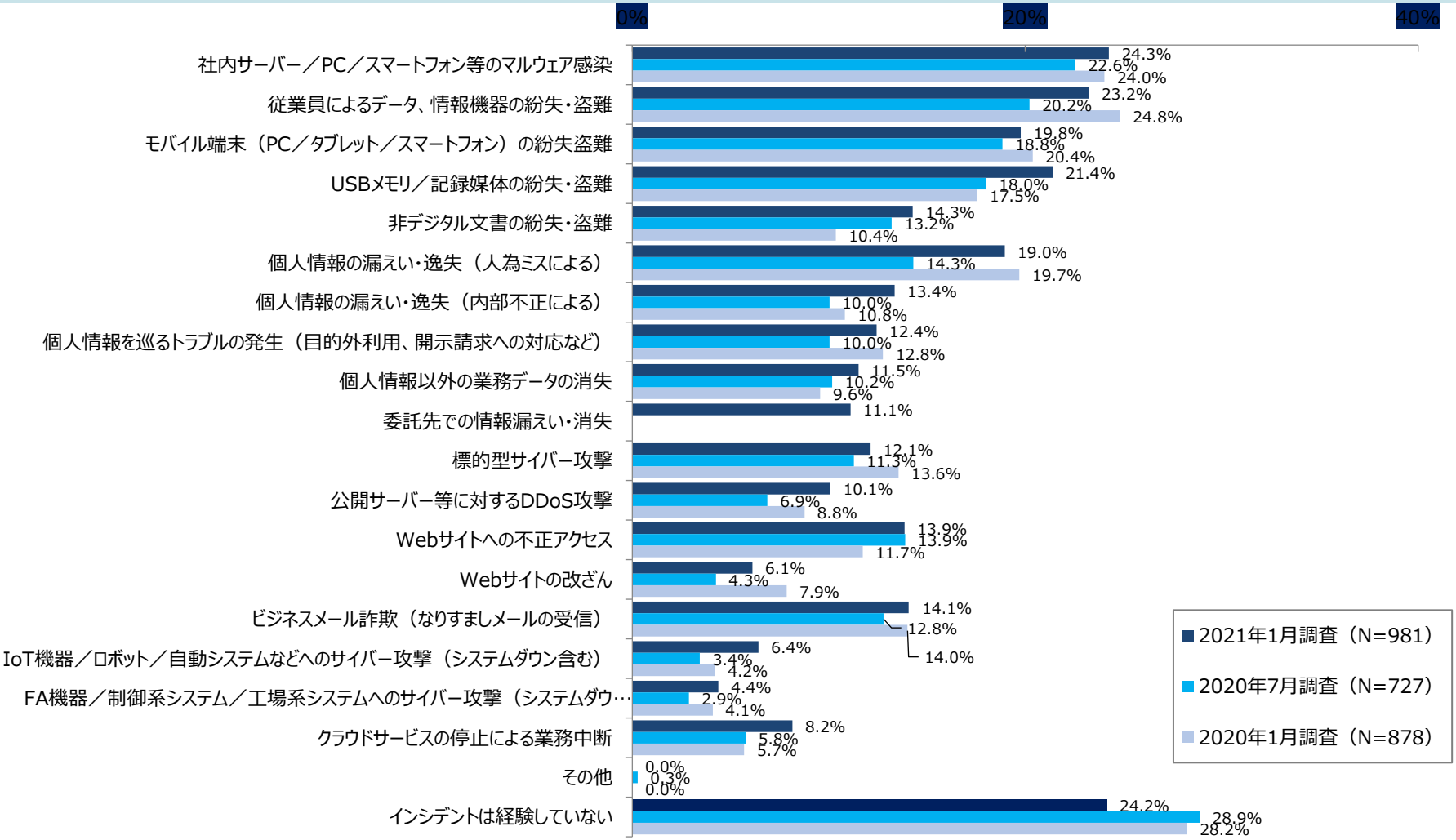
# Q2 ：過去1年間に経験したセキュリティインシデント（2021年調査）

■依然として、マルウェア感染や機器や情報の紛失・盗難、Webサイトへの攻撃、ビジネスメール詐欺が高い割合で発生している。



# Q2 ：過去1年間に経験したセキュリティインシデント（2020~2021年比較）

■過去２回の調査と比較して、全体的にセキュリティインシデントが増加傾向にあり、マルウェア感染、個人情報の紛失・盗難も多く、Webサイト攻撃、クラウドサービスの停止が増えている。



# Q2：過去1年間に経験したセキュリティインシデント［業種別］（2021年調査）

■ビジネスメール詐欺が金融・保険と卸売・小売で多くなっている。

| | 製造 (N=284) | 建設・不動産 (N=96) | 卸売・小売 (N=78) | 金融・保険 (N=79) | 情報通信 (N=152) | サービス (N=225) | 公共・その他 (N=67) | 全体 (N=981) |
|---|---|---|---|---|---|---|---|---|
| 社内サーバー／PC／スマートフォン等のマルウェア感染 | 27.5% | 26.0% | 26.9% | 20.3% | 27.6% | 20.4% | 14.9% | 24.3% |
| 従業員によるデータ、情報機器の紛失・盗難 | 23.9% | 27.1% | 21.8% | 24.1% | 26.3% | 18.2% | 25.4% | 23.2% |
| モバイル端末（PC／タブレット／スマートフォン）の紛失盗難 | 21.8% | 22.9% | 20.5% | 12.7% | 26.3% | 16.0% | 11.9% | 19.8% |
| USBメモリ／記録媒体の紛失・盗難 | 22.9% | 26.0% | 19.2% | 21.5% | 23.0% | 16.4% | 23.9% | 21.4% |
| 非デジタル文書の紛失・盗難 | 12.7% | 10.4% | 12.8% | 16.5% | 17.8% | 15.6% | 13.4% | 14.3% |
| 個人情報の漏えい・逸失（人為ミスによる） | 16.5% | 25.0% | 12.8% | 24.1% | 19.7% | 19.1% | 19.4% | 19.0% |
| 個人情報の漏えい・逸失（内部不正による） | 12.7% | 10.4% | 14.1% | 15.2% | 11.8% | 13.8% | 19.4% | 13.4% |
| 個人情報を巡るトラブルの発生（目的外利用、開示請求への対応など） | 12.3% | 5.2% | 10.3% | 12.7% | 15.8% | 12.4% | 17.9% | 12.4% |
| 個人情報以外の業務データの消失 | 8.8% | 12.5% | 9.0% | 13.9% | 9.9% | 15.1% | 13.4% | 11.5% |
| 委託先での情報漏えい・消失 | 9.5% | 14.6% | 12.8% | 8.9% | 11.8% | 11.6% | 10.4% | 11.1% |
| 標的型サイバー攻撃 | 14.1% | 11.5% | 9.0% | 11.4% | 13.8% | 10.2% | 11.9% | 12.1% |
| 公開サーバー等に対するDDoS攻撃 | 8.8% | 9.4% | 14.1% | 3.8% | 11.8% | 10.7% | 13.4% | 10.1% |
| Webサイトへの不正アクセス | 13.4% | 13.5% | 11.5% | 13.9% | 13.8% | 13.3% | 20.9% | 13.9% |
| Webサイトの改ざん | 5.3% | 6.3% | 9.0% | 2.5% | 7.2% | 5.8% | 9.0% | 6.1% |
| ビジネスメール詐欺（なりすましメールの受信） | 12.7% | 10.4% | 20.5% | 20.3% | 13.8% | 12.9% | 14.9% | 14.1% |
| IoT機器／ロボット／自動システムなどへのサイバー攻撃（システムダウン含む） | 6.0% | 4.2% | 10.3% | 3.8% | 9.2% | 5.3% | 7.5% | 6.4% |
| FA機器／制御系システム／工場系システムへのサイバー攻撃（システムダウン含む） | 5.3% | 1.0% | 5.1% | 2.5% | 5.9% | 3.1% | 7.5% | 4.4% |
| クラウドサービスの停止による業務中断 | 3.5% | 11.5% | 11.5% | 5.1% | 14.5% | 8.4% | 7.5% | 8.2% |
| その他 | 0.0% | 0.0% | 0.0% | 0.0% | 0.0% | 0.0% | 0.0% | 0.0% |
| インシデントは経験していない | 17.3% | 21.9% | 34.6% | 24.1% | 18.4% | 31.6% | 32.8% | 24.2% |

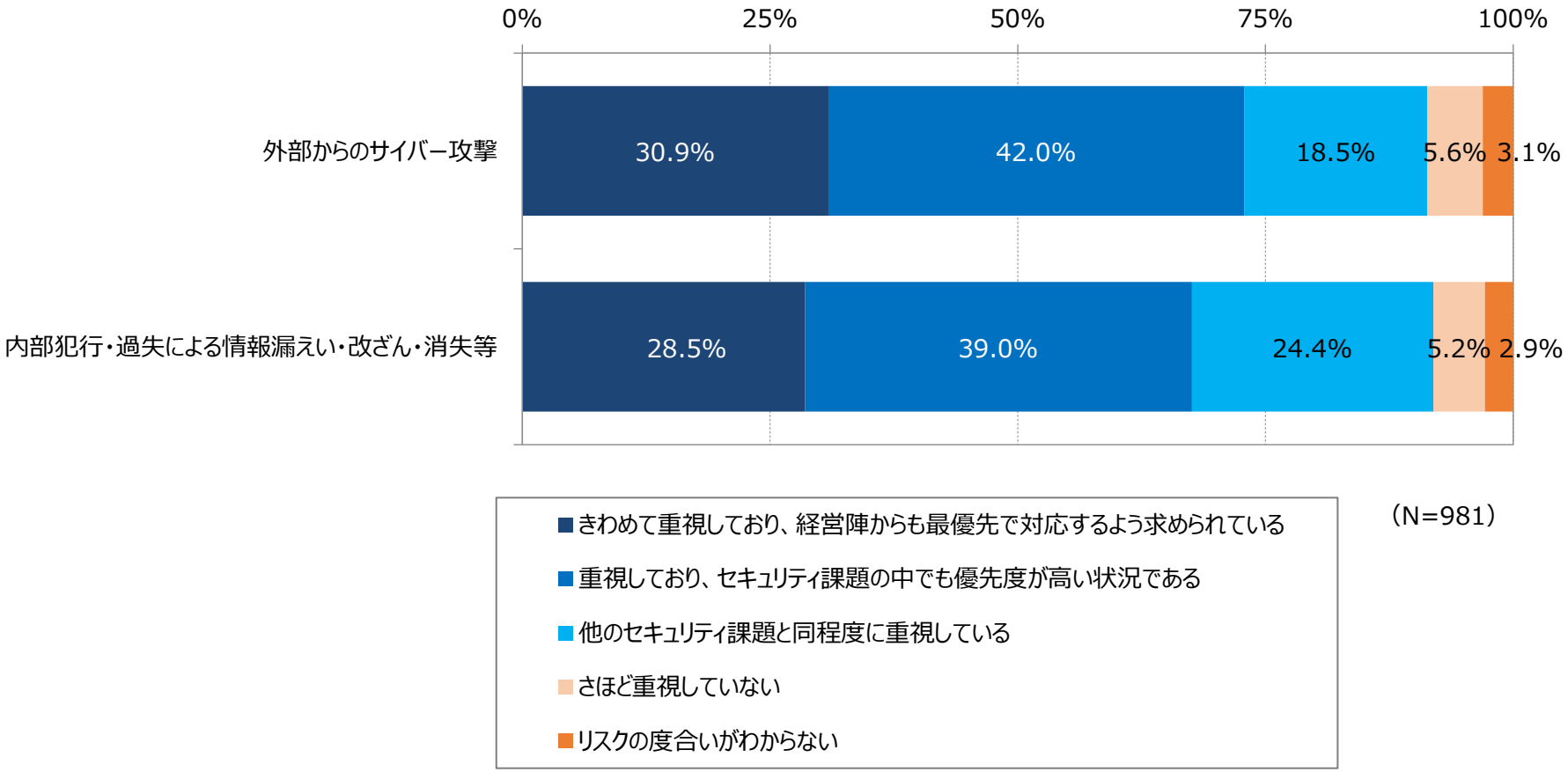
# Q2：過去1年間に経験したセキュリティインシデント［従業員規模別］（2021年調査）

■企業規模が大きくなればインシデント件数が増加する傾向にあるが、特に「マルウェア感染」「データ、情報機器の紛失・盗難」「標的型サイバー攻撃」が増加している。

| | 5,000人以上（N=216） | 1,000～4,999人（N=222） | 300～999人（N=232） | 50～299人（N=311） | 全体（N=981） |
|---|---|---|---|---|---|
| 社内サーバー／PC／スマートフォン等のマルウェア感染 | 37.5% | 24.8% | 19.4% | 18.3% | 24.3% |
| 従業員によるデータ、情報機器の紛失・盗難 | 37.0% | 24.3% | 19.4% | 15.8% | 23.2% |
| モバイル端末（PC／タブレット／スマートフォン）の紛失盗難 | 27.3% | 26.1% | 18.5% | 10.9% | 19.8% |
| USBメモリ／記録媒体の紛失・盗難 | 26.9% | 24.3% | 22.4% | 14.8% | 21.4% |
| 非デジタル文書の紛失・盗難 | 18.1% | 18.5% | 15.5% | 7.7% | 14.3% |
| 個人情報の漏えい・逸失（人為ミスによる） | 26.4% | 19.8% | 17.2% | 14.5% | 19.0% |
| 個人情報の漏えい・逸失（内部不正による） | 17.1% | 17.1% | 11.2% | 9.6% | 13.4% |
| 個人情報を巡るトラブルの発生（目的外利用、開示請求への対応など） | 19.4% | 14.9% | 9.1% | 8.4% | 12.4% |
| 個人情報以外の業務データの消失 | 14.8% | 9.0% | 11.6% | 10.9% | 11.5% |
| 委託先での情報漏えい・消失 | 13.9% | 15.3% | 12.1% | 5.5% | 11.1% |
| 標的型サイバー攻撃 | 21.8% | 14.0% | 7.3% | 7.7% | 12.1% |
| 公開サーバー等に対するDDoS攻撃 | 15.3% | 9.9% | 9.9% | 6.8% | 10.1% |
| Webサイトへの不正アクセス | 18.1% | 16.2% | 11.2% | 11.3% | 13.9% |
| Webサイトの改ざん | 7.4% | 7.7% | 6.5% | 3.9% | 6.1% |
| ビジネスメール詐欺（なりすましメールの受信） | 19.0% | 14.9% | 15.1% | 9.3% | 14.1% |
| IoT機器／ロボット／自動システムなどへのサイバー攻撃（システムダウン含む） | 13.0% | 6.3% | 6.0% | 2.3% | 6.4% |
| FA機器／制御系システム／工場系システムへのサイバー攻撃（システムダウン含む） | 8.3% | 4.5% | 3.9% | 1.9% | 4.4% |
| クラウドサービスの停止による業務中断 | 11.6% | 7.7% | 10.8% | 4.2% | 8.2% |
| その他 | 0.0% | 0.0% | 0.0% | 0.0% | 0.0% |
| インシデントは経験していない | 11.6% | 17.6% | 23.3% | 38.3% | 24.2% |

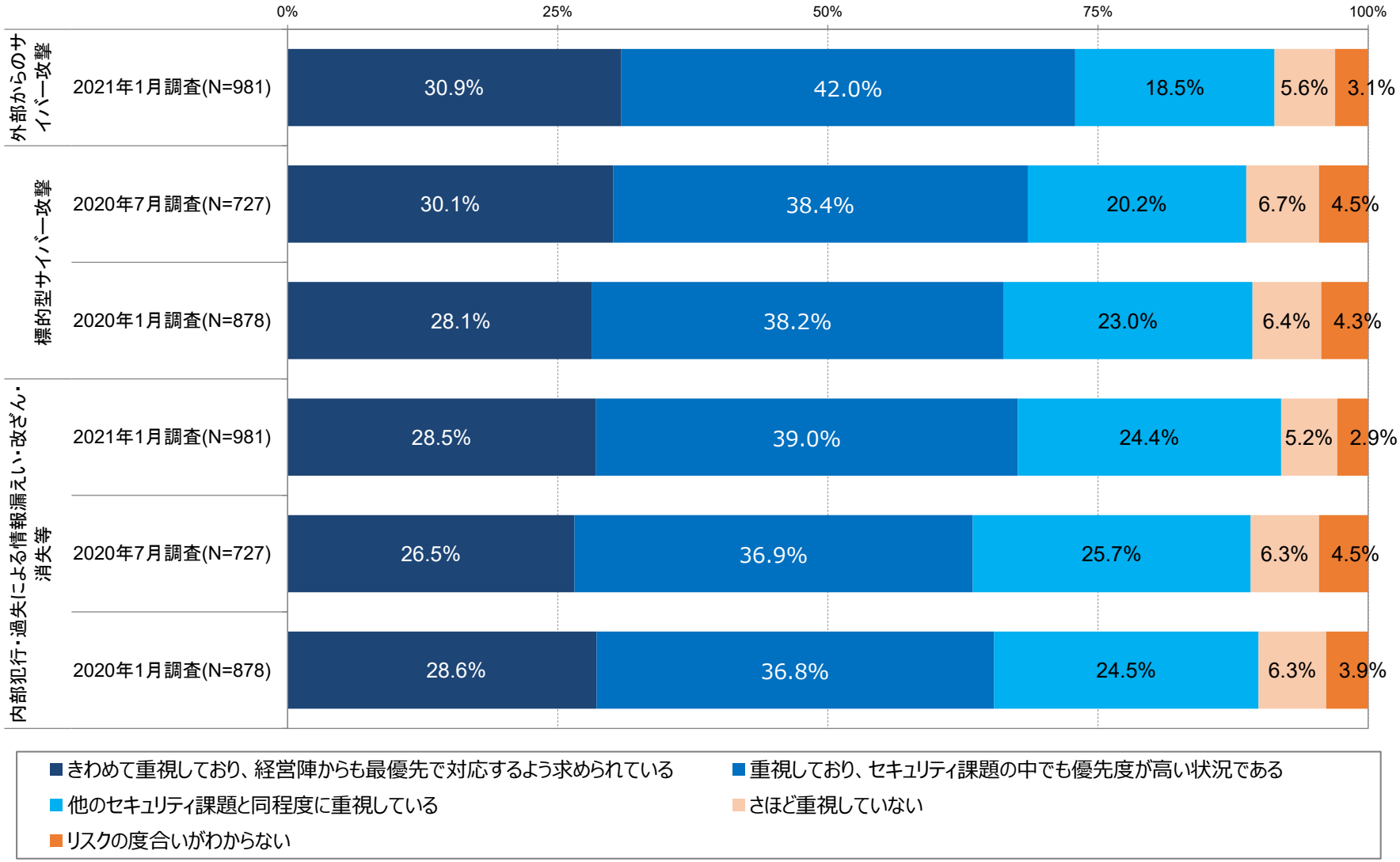
# Q3_1：セキュリティリスクの重視度合い（2021年調査）

■「外部からのサイバー攻撃」「内部犯行による重要情報の漏えい・消失」ともに、きわめて重視しているとした割合は約３割で例年と同様であるが、「外部からのサイバー攻撃」は重視しているまでを含めれば、初めて７割を超え、重視度合いがアップしている。




（N=981）

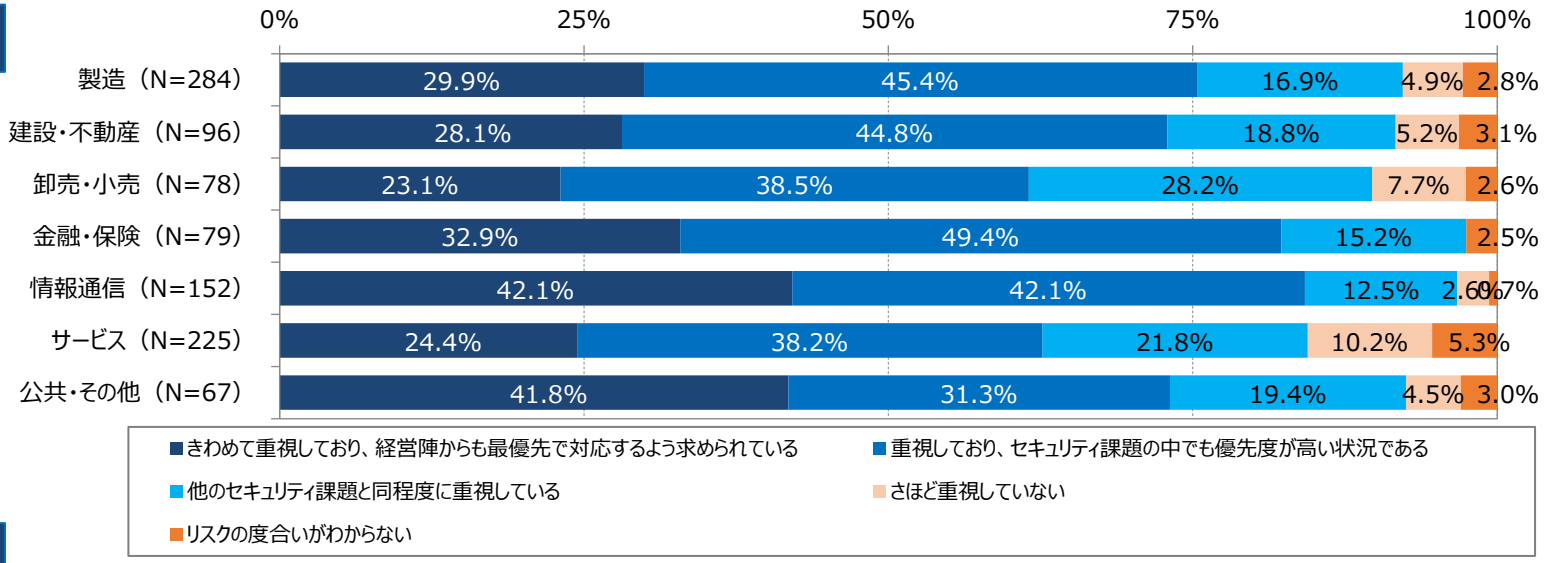
# Q3_1：セキュリティリスクの重視度合い（2020～2021年比較）



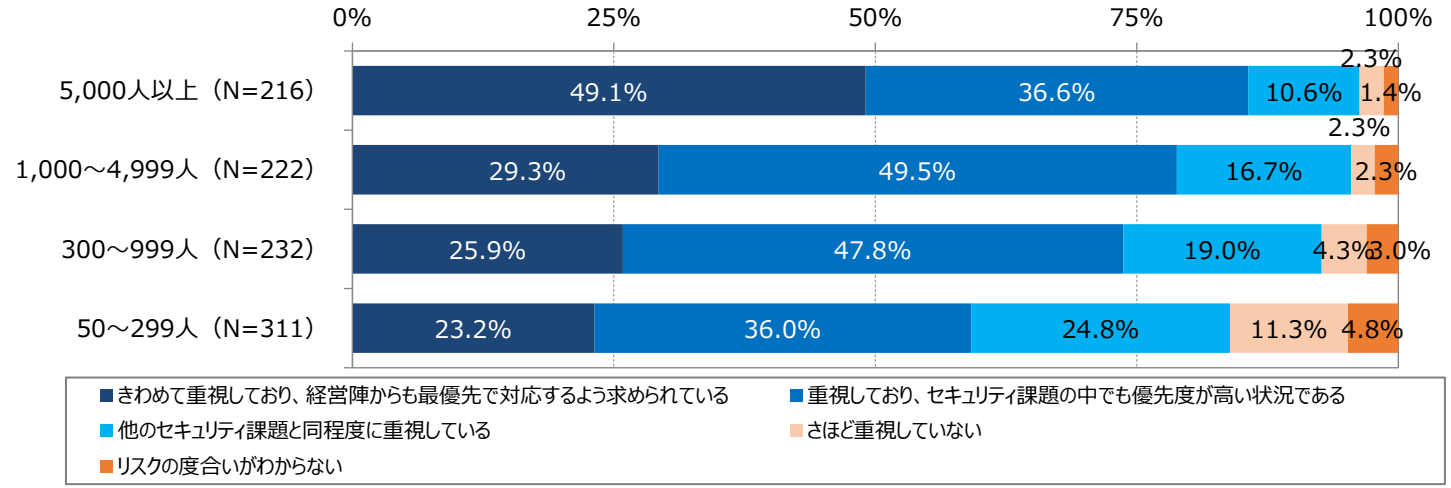
# Q3_1:「外部からのサイバー攻撃」の重視度合い［業種別／従業員規模別］（2020年調査）

- きわめて重視と重視を合わせると他業種と比較して卸売・小売とサービスの比率が低くなっている。
- 規模が大きくなればなるほどきわめて重視と重視の合計の比率が高くなる傾向がある。

**業種別**



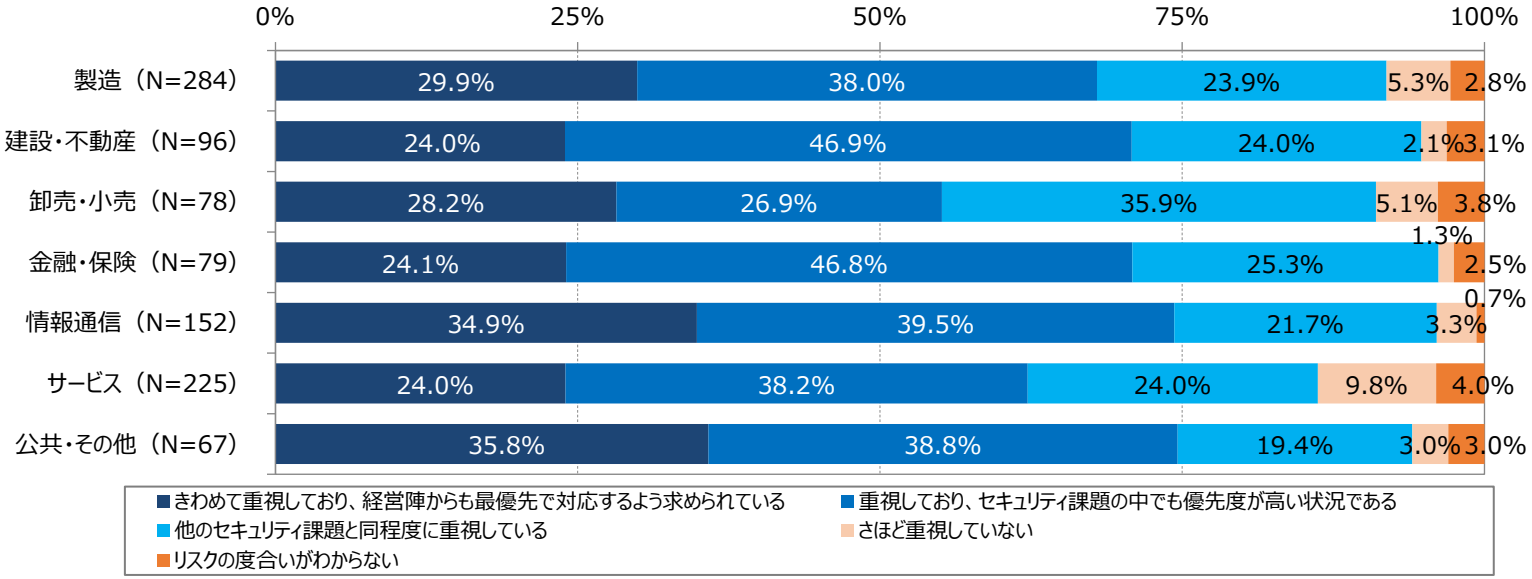

**従業員規模別**



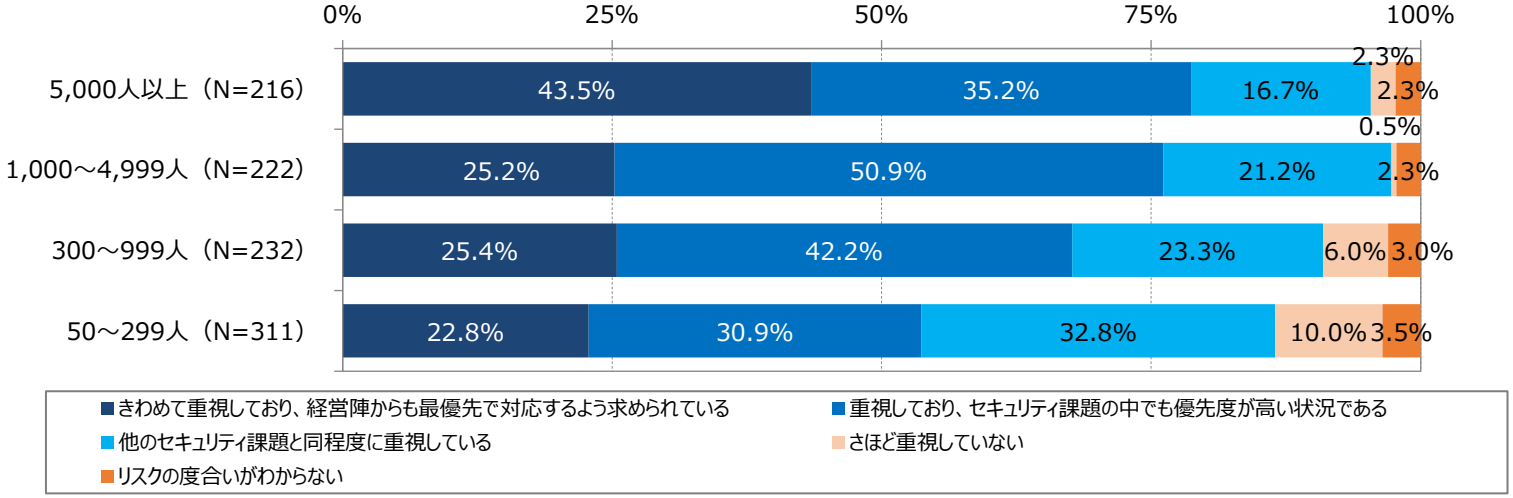
# Q3_1:「内部犯行リスク」の重視度合い［業種別／従業員規模別］（2021年調査）

- きわめて重視と重視を合わせると、他業種と比較して卸売・小売とサービスの比率が低くなっている。
- 規模が大きくなればなるほど、きわめて重視と重視の合計の比率が高くなる傾向がある。

**業種別**

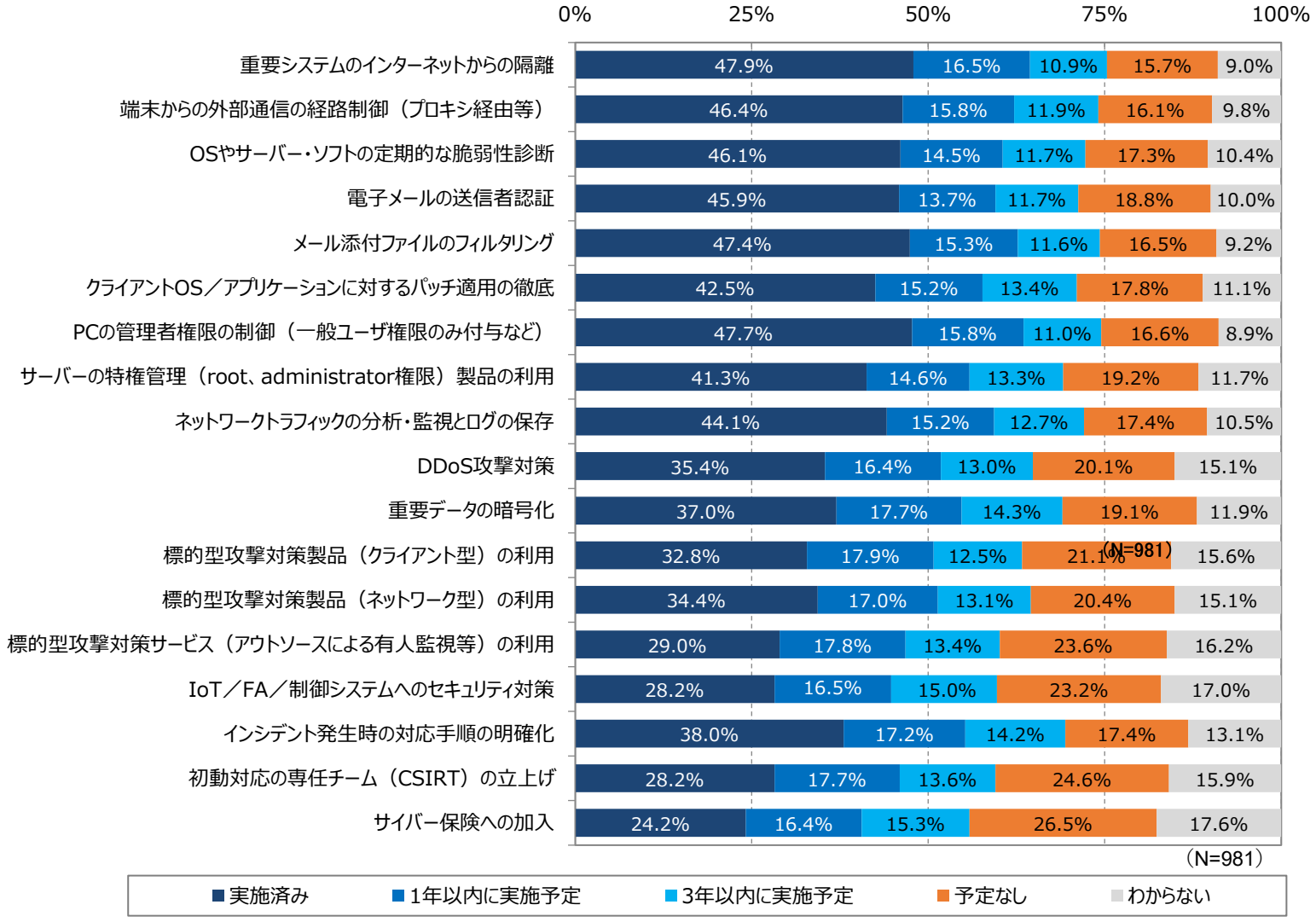



**従業員規模別**



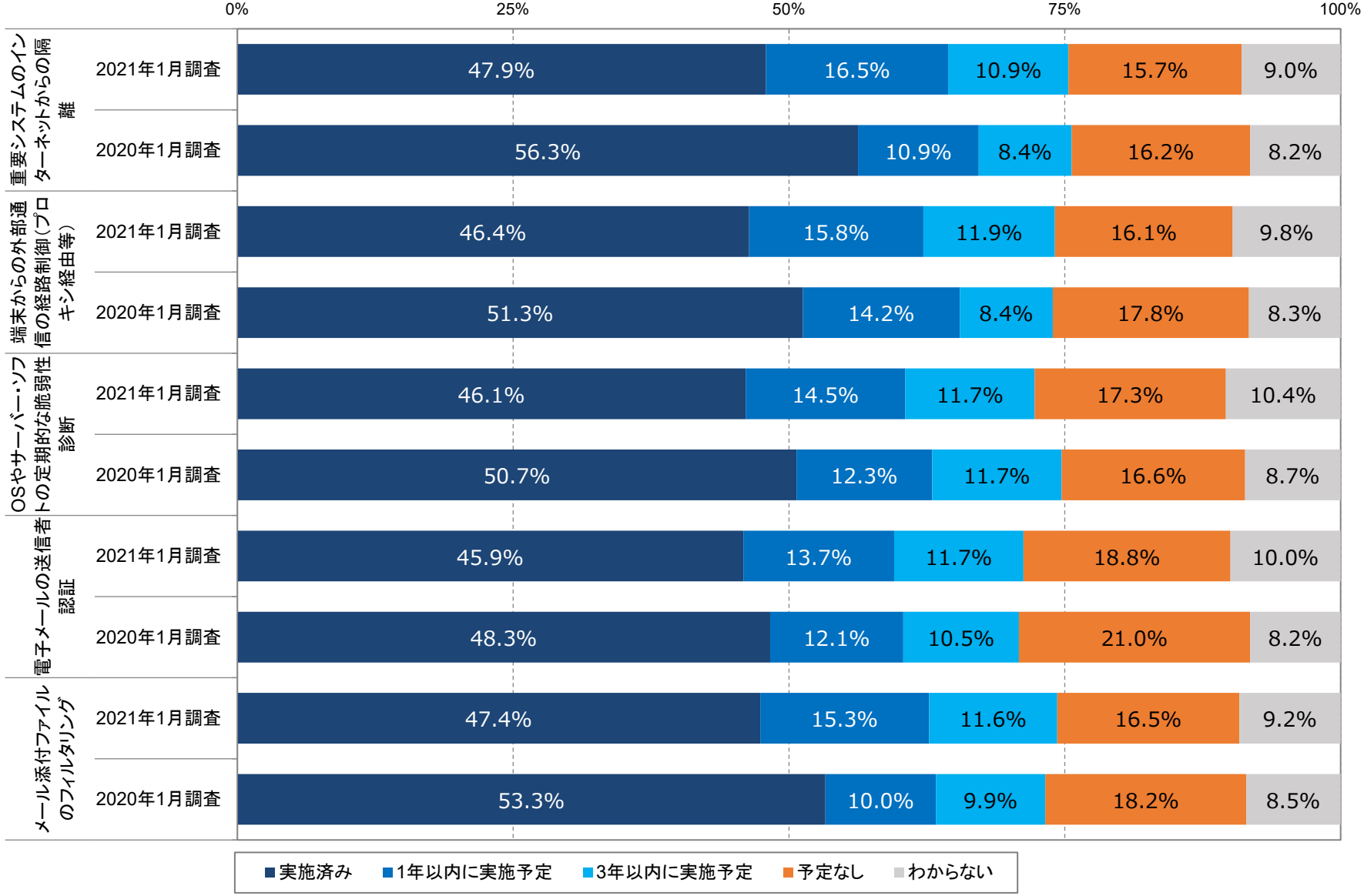
# Q3_2：「外部からの攻撃対策」の実施状況（2021年調査）

■実施済が高いのは、「インターネットからの隔離」「PC管理者権限の制御」「メール添付のフィルタリング」の順で、前回の調査と同様の結果となっている。



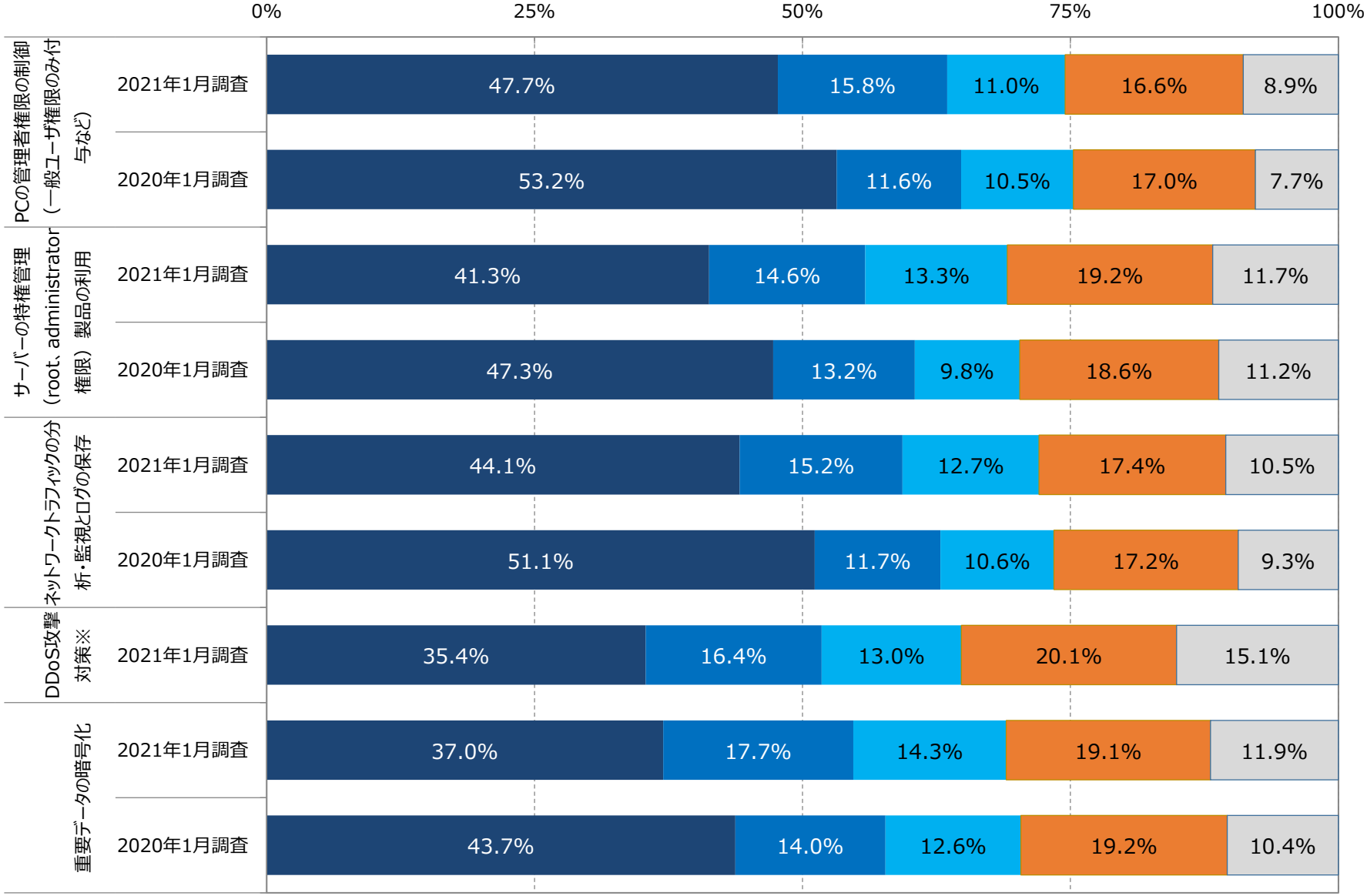
# Q3_2：「外部からの攻撃対策」の実施状況-1（2020～2021年比較）

※2020年調査は「標的型攻撃」で実施




2021年1月調査（N=981）
2020年1月調査（N=878）

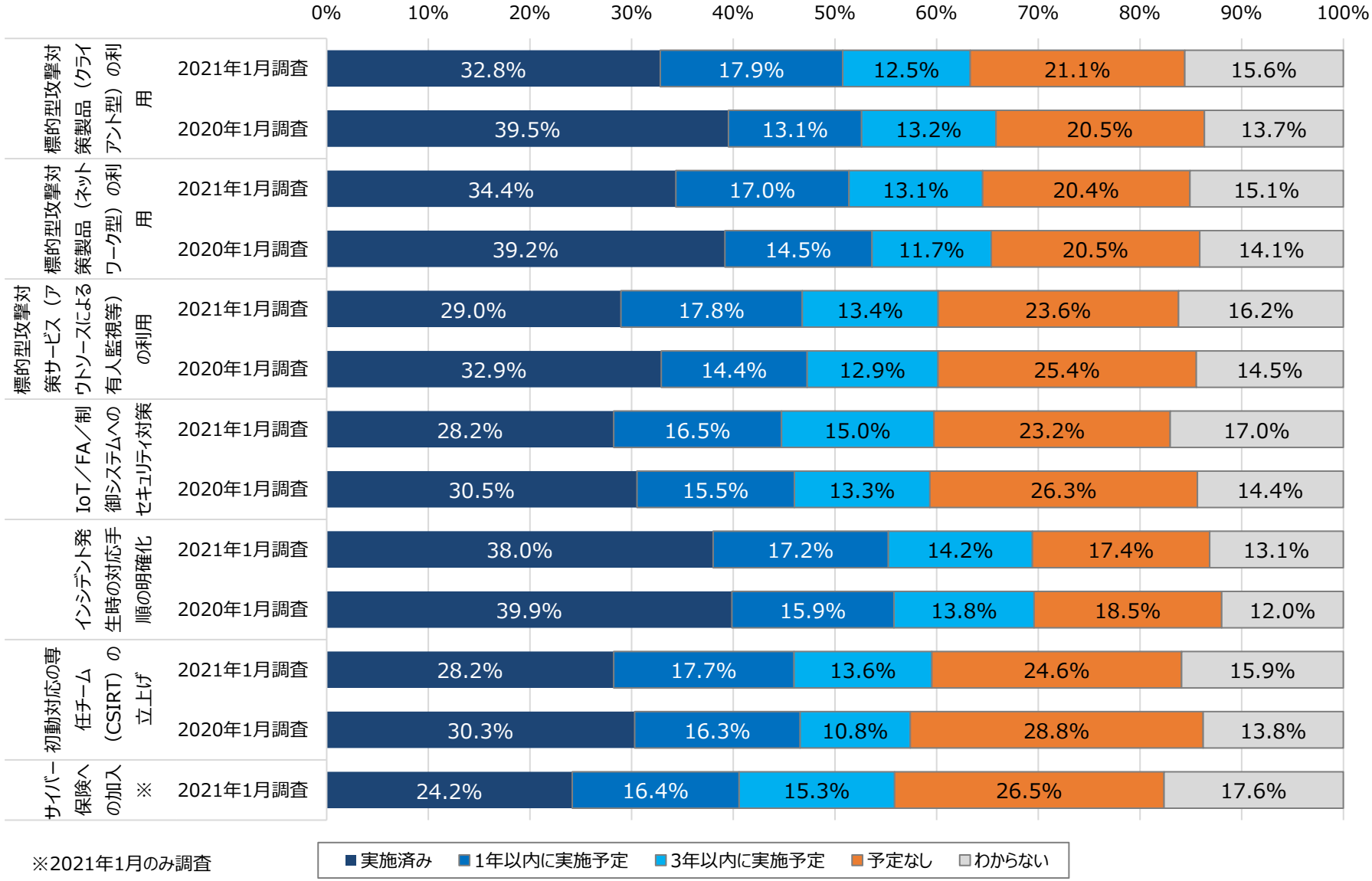
# Q3_2：「外部からの攻撃対策」の実施状況-2（2020～2021年比較）




※2021年1月のみ調査

2021年1月調査（N=981）
2020年1月調査（N=878）

# Q3_2：「外部からの攻撃対策」の実施状況-3（2020～2021年比較）

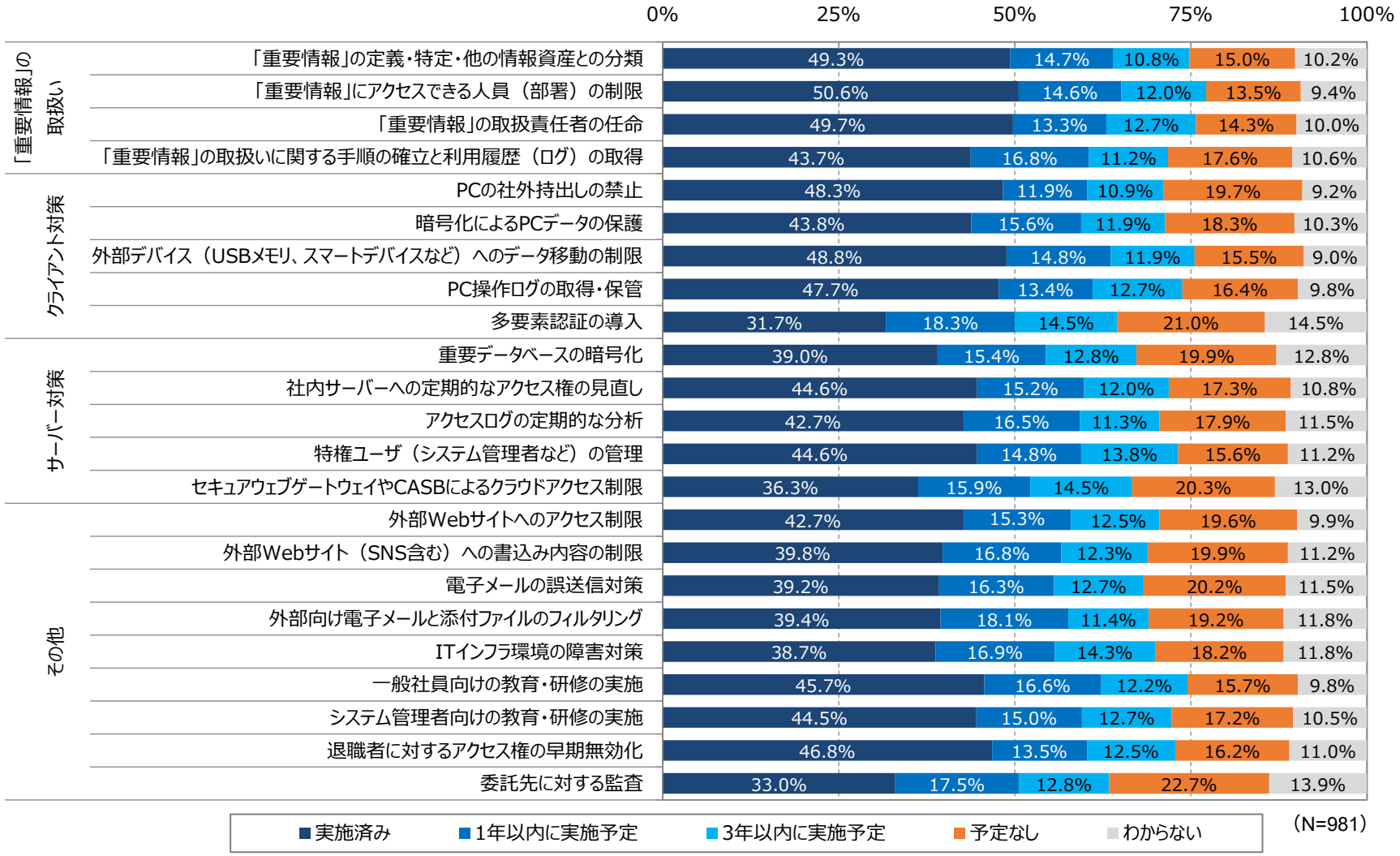



※2021年1月のみ調査

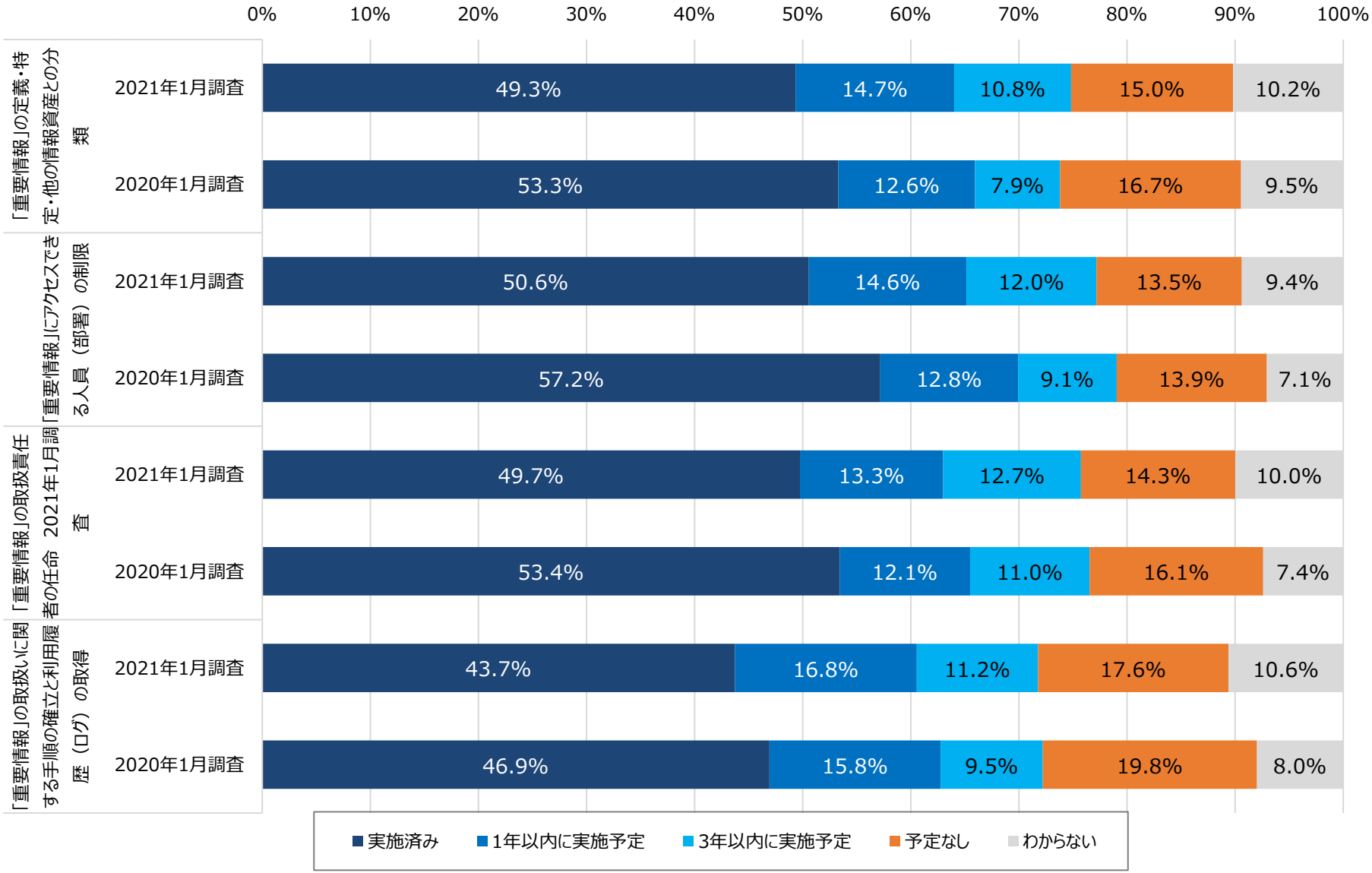
2021年1月調査（N=981）
2020年1月調査（N=878）

# Q3_3：「情報漏えい対策」の実施状況（2021年調査）

■実施済が高いのは「重要情報の取扱い」についての項目で、前年と同様の傾向となっている。

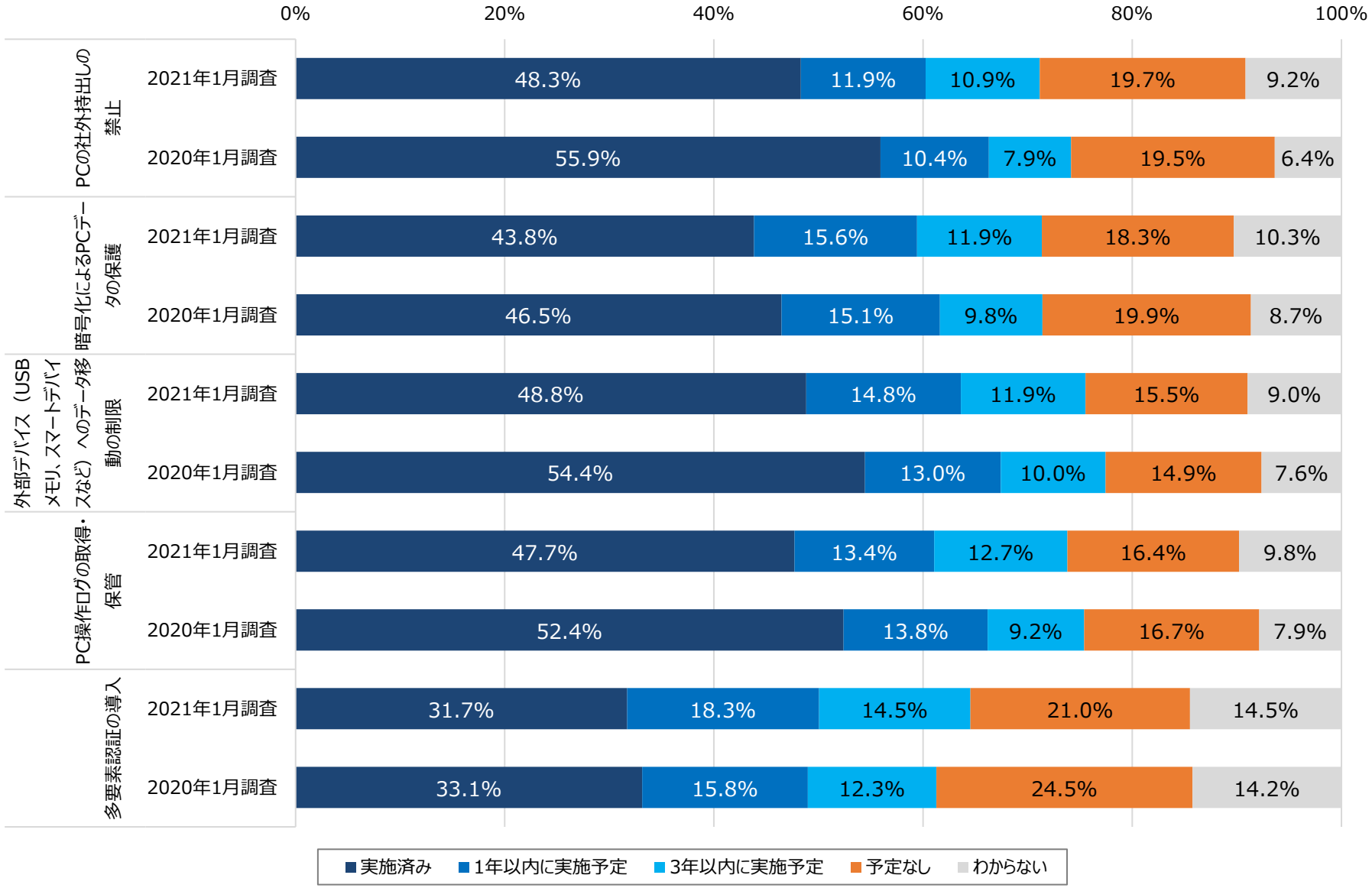


# Q3_3：「情報漏えい対策」の実施状況［重要情報の取扱い］（2020～2021年比較査）



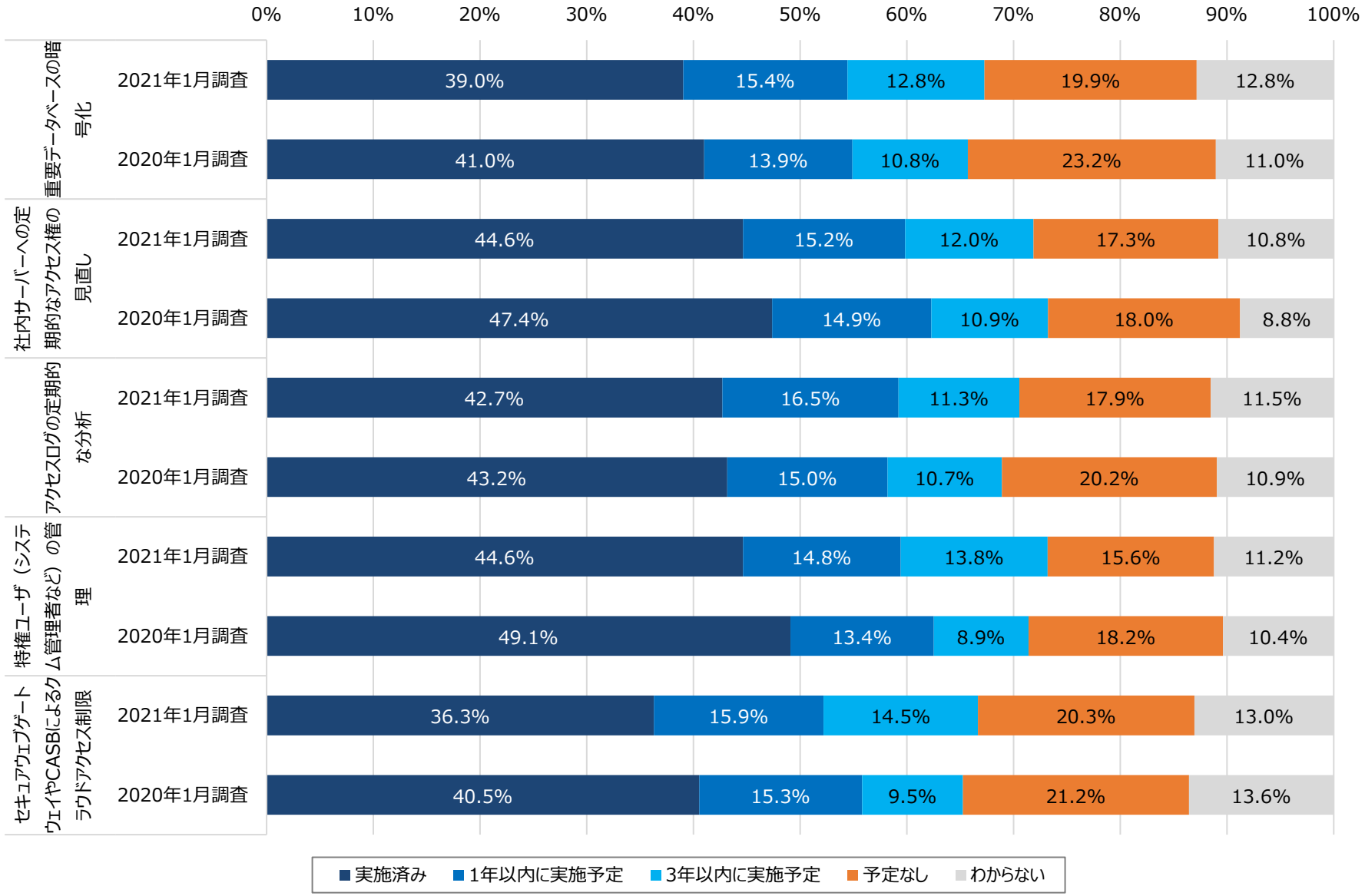

2021年1月調査（N=981）
2020年1月調査（N=878）

# Q3_3：「情報漏えい対策」の実施状況［クライアント対策］（2020～2021年比較）



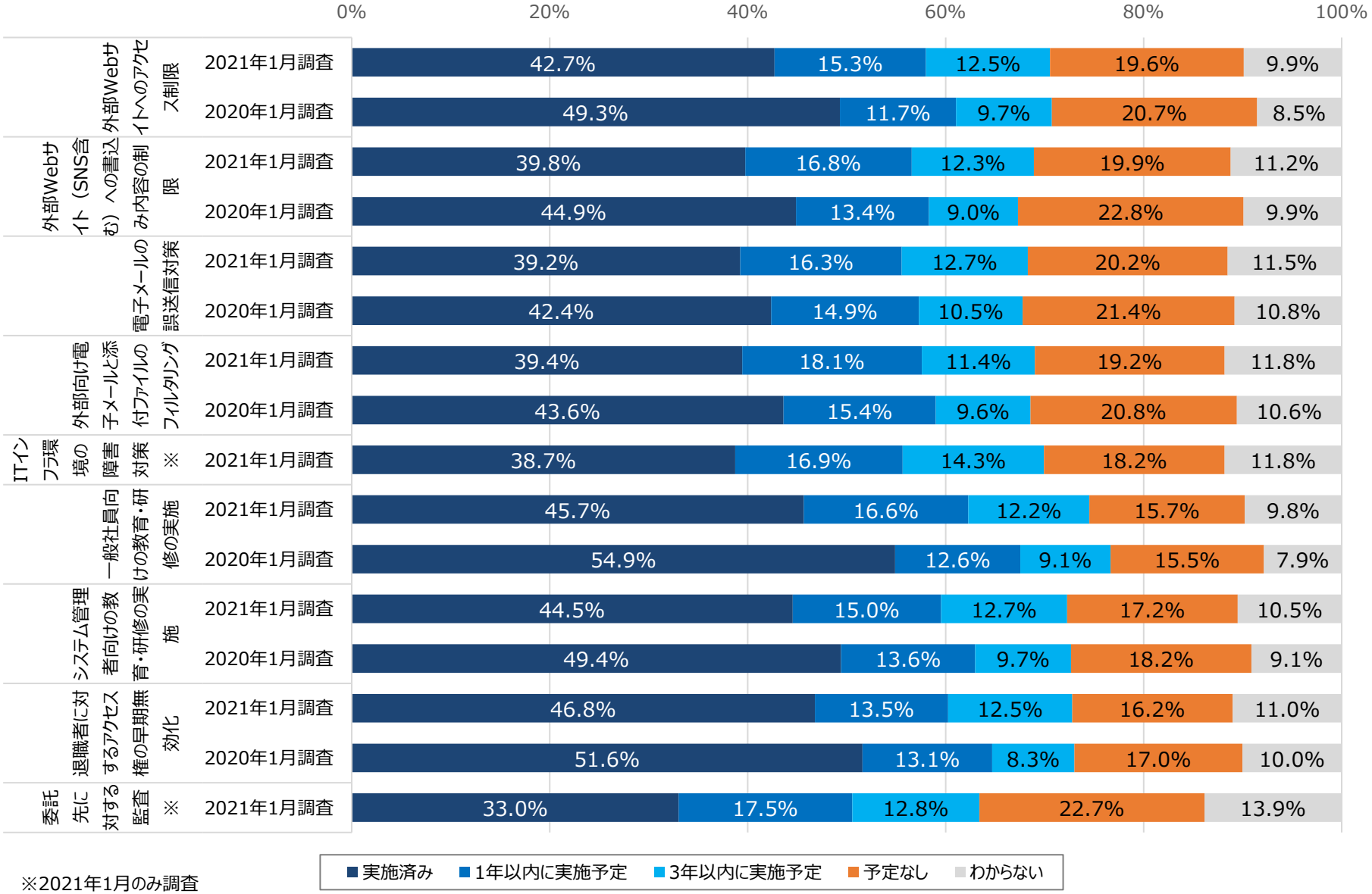

2021年1月調査（N=981）
2020年1月調査（N=878）

# Q3_3：「情報漏えい対策」の実施状況［サーバー対策］（2020～2021年比較）




2021年1月調査（N=981）
2020年1月調査（N=878）

# Q3_3：「情報漏えい対策」の実施状況［その他］（2020～2021年比較）




※2021年1月のみ調査

2021年1月調査（N=981）
2020年1月調査（N=878）

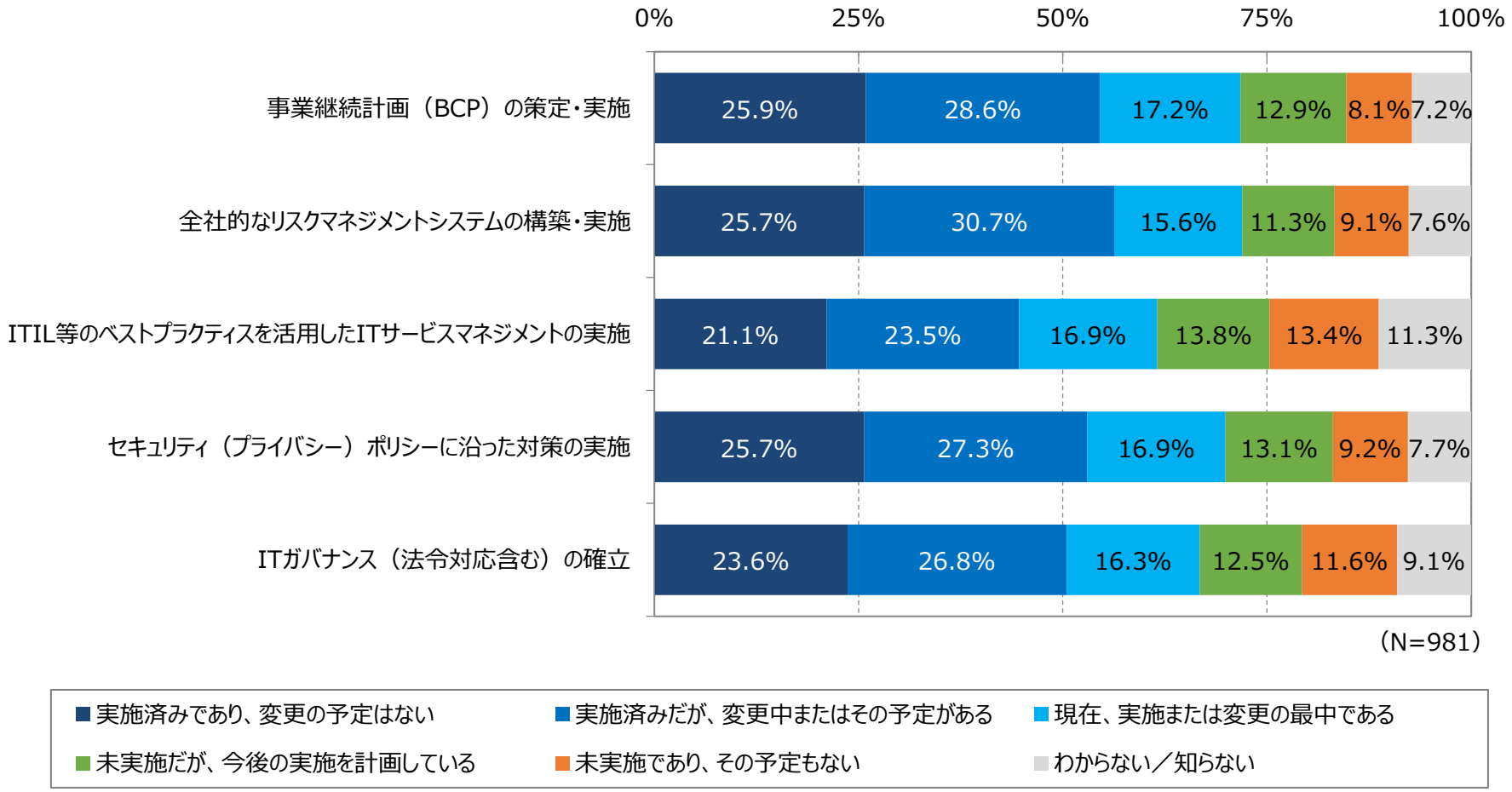
# 2）認定／認証制度に対する意識

- Q4_1：　システムリスク軽減策の取組み状況
- Q4_2：　第三者から認定／認証を取得することの価値・効果
- Q4_3：　取引先選定時に重視する認定／認証制度の重視度
- Q5_1：　コロナ禍におけるプライバシーマーク制度の取組みの変化
- Q5_2：　コロナ禍におけるプライバシーマーク制度の取引先評価重視度の変化
- Q5_3：　コロナ禍におけるISMS評価制度の取組みの変化
- Q5_4：　コロナ禍におけるISMS評価制度の取引先評価重視度の変化

# Q4_1：システムリスクの軽減策の取組み状況（2021年調査）

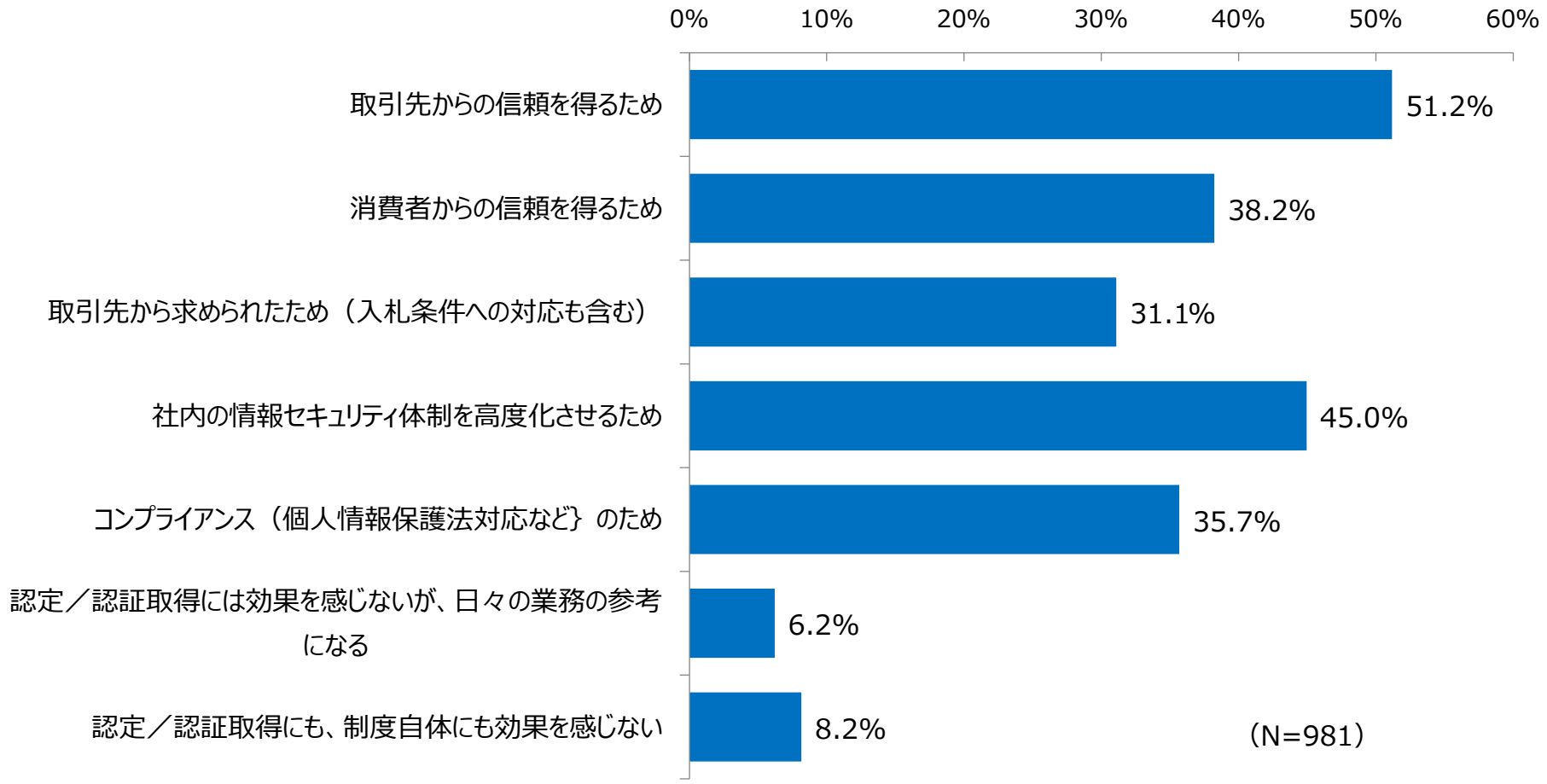
■「BCPの策定・実施」「リスクマネジメントの構築・実施」「セキュリティポリシーの策定」は実施済が約５割で前年と同様である。

■「ITサービスマネジメントの実施」も前年同様、実施済が約４割となっている。



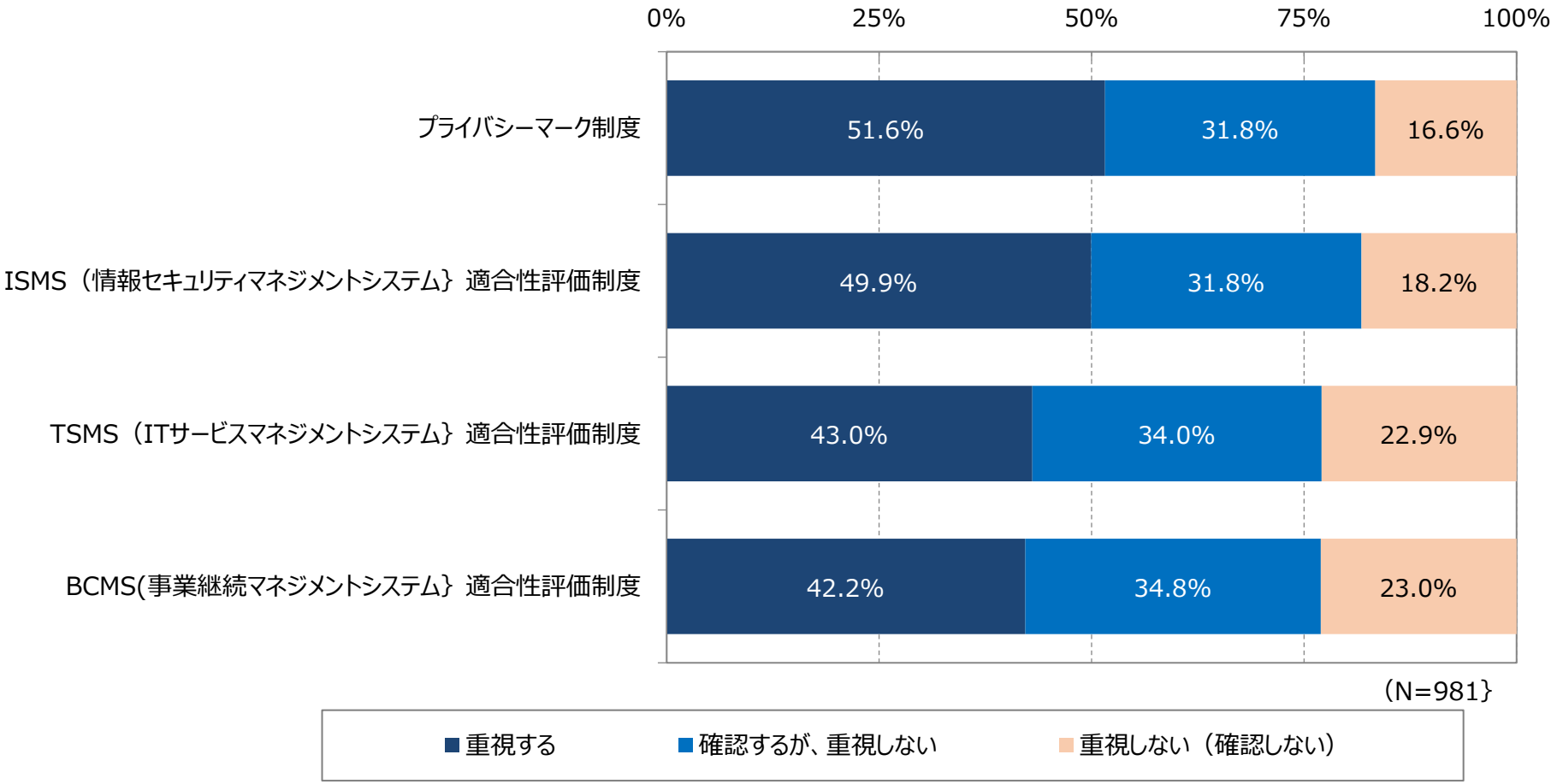
# Q4_2：第三者から認定／認証を取得することの価値・効果（2021年調査）

■大きくは前年と同様の傾向であるが、「取引先からの信頼を得るため」と「情報セキュリティ体制を高度化するため」が高い。



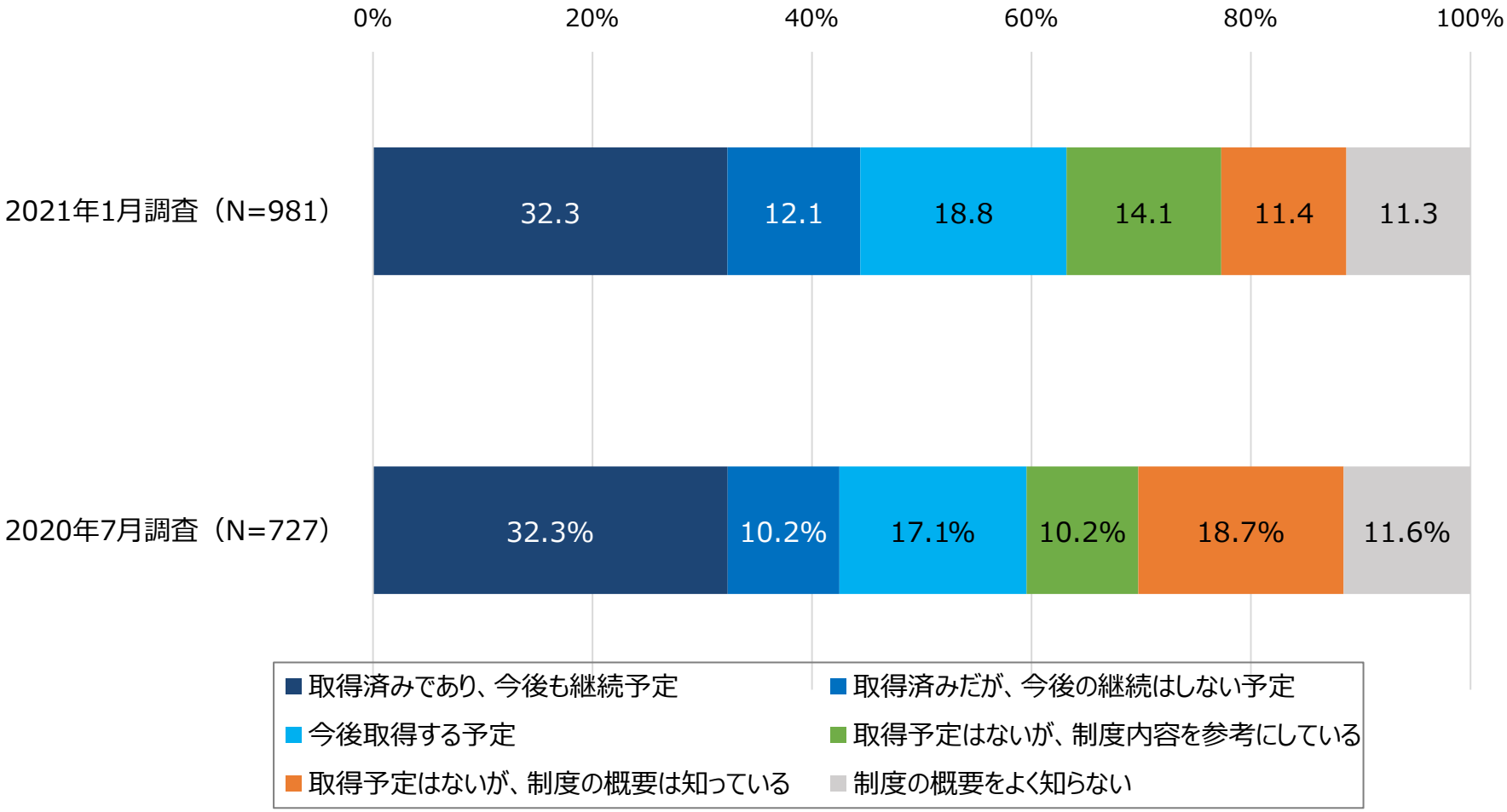
# Q4_3：取引相手先を選定する際の認定／認証の有無の重視度（2021年調査）

■ 大きくは前年と同様の傾向だったが、ITSMS評価制度とBCMS評価制度を重視する比率が若干上昇している。



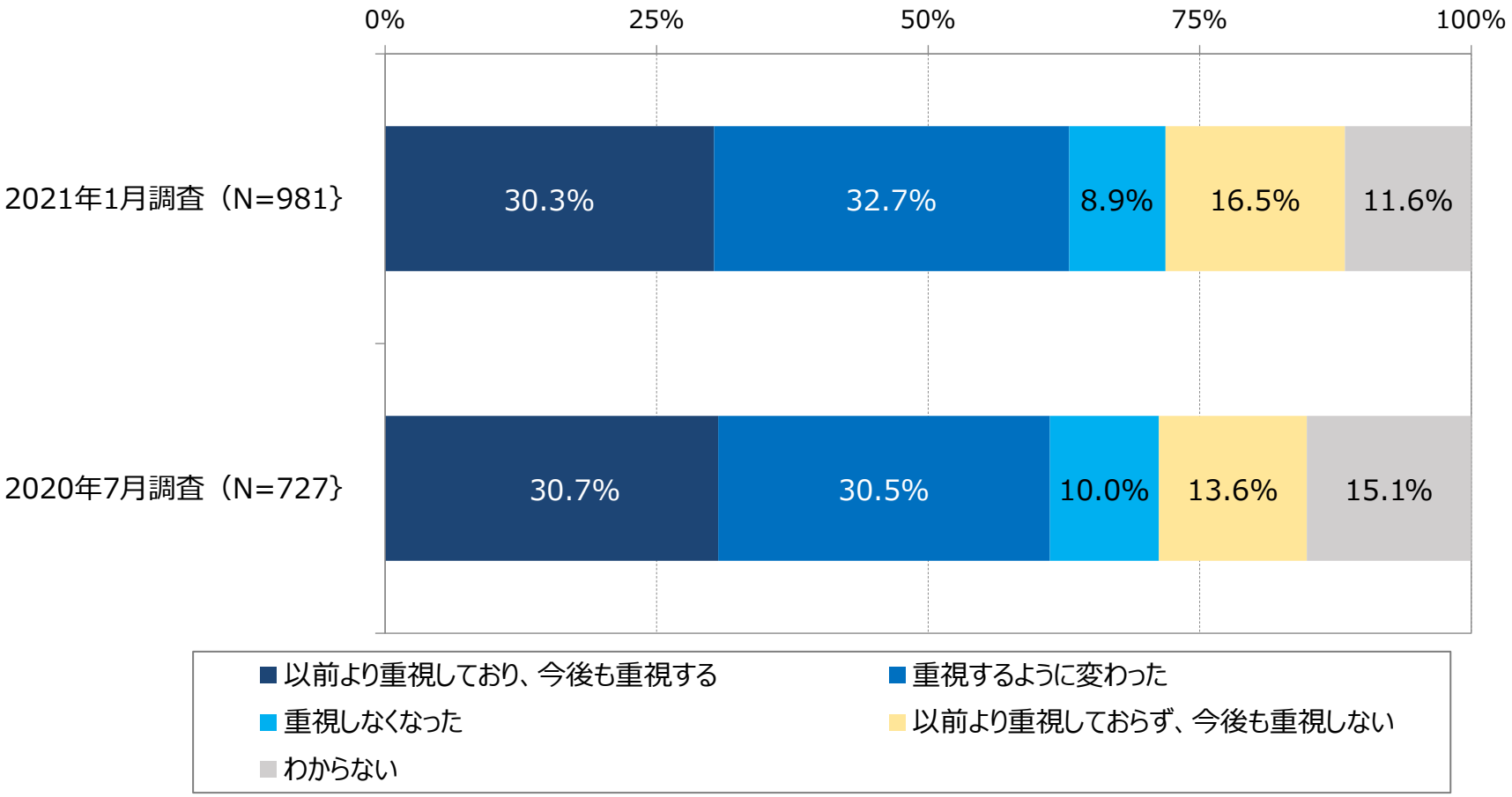
# Q5_1：コロナ禍対策に伴うプライバシーマーク制度への取組みの変化（2021~2021年比較）

■ 前回と比較して、取得する予定と制度内容を参考にするが若干増加している。



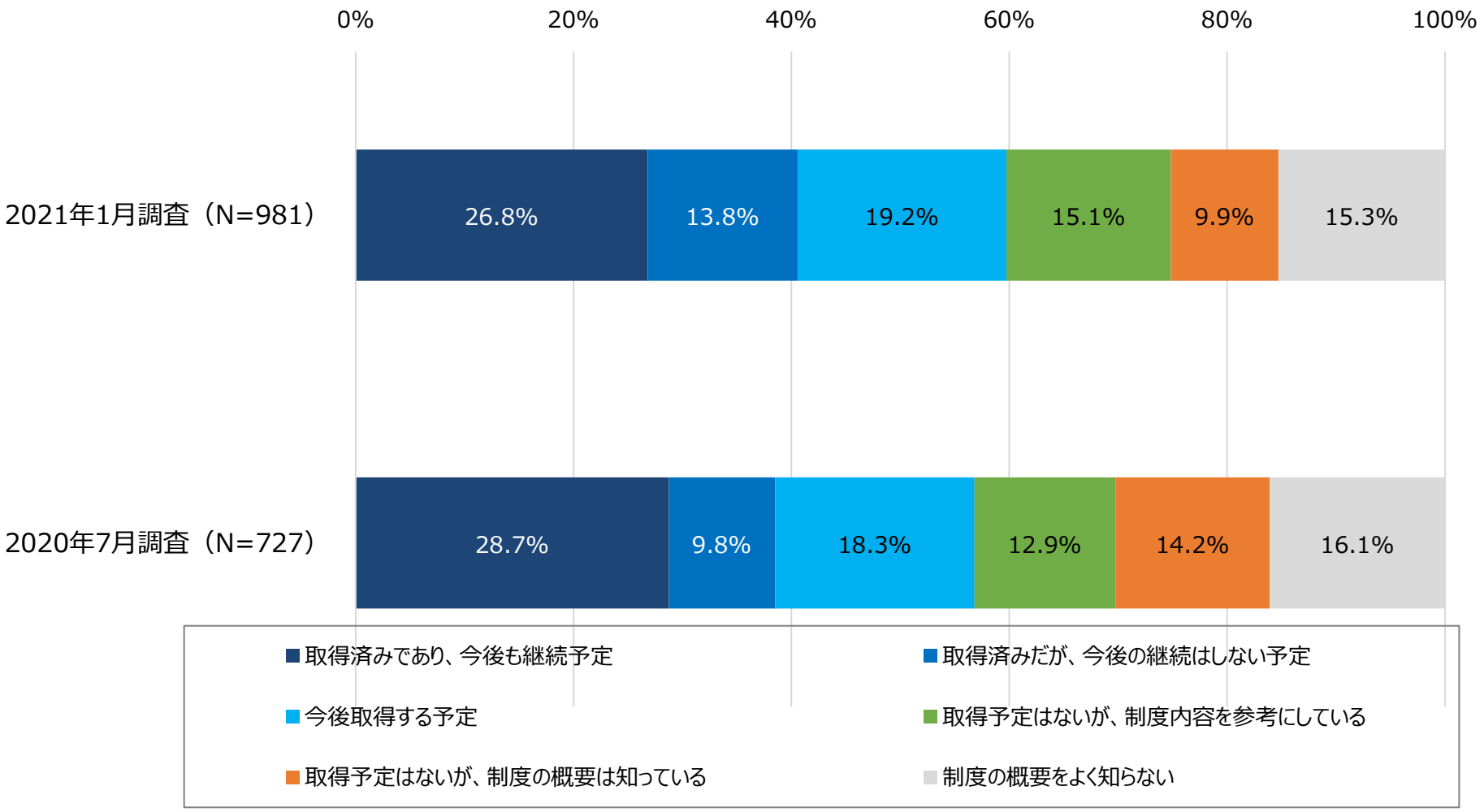
# Q５_２：コロナ禍対策に伴うプライバシーマーク制度の取引先評価時の重視度（2020~2021年比較）

■ 前回と比較してあまり変化はないが、「重視するようになった」と「以前どおり重視しない」が若干増加している。



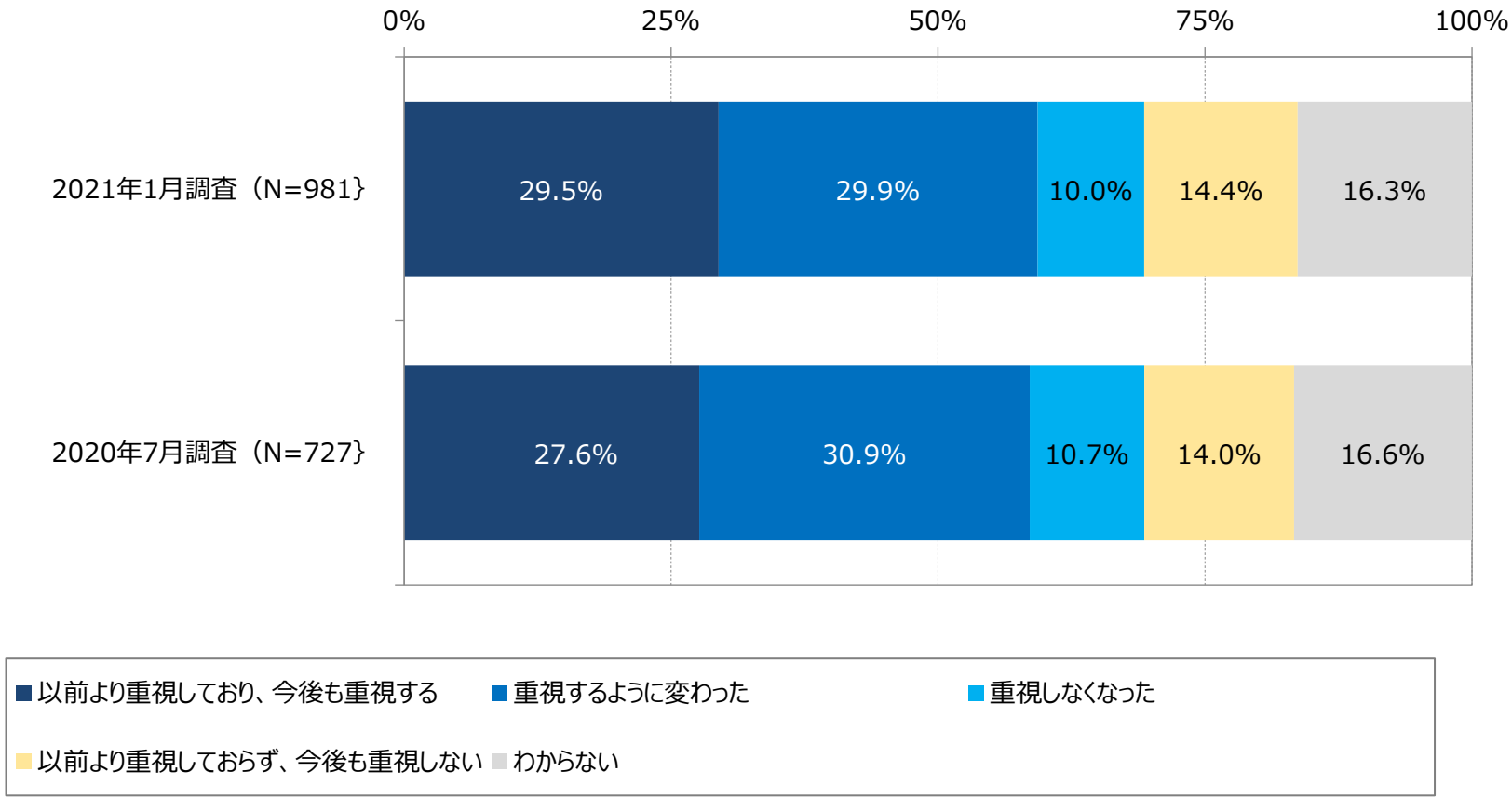
# Q5_3：コロナ禍対策に伴うISMS評価制度への取組みの変化（2020~2021年比較）

■ 前回と比較して、取得済、取得する予定、制度内容を参考にするが若干増加している。



# Q5_4：コロナ禍対策に伴うISMS評価制度の取引先評価時の重視度（2020~2021年比較）

■ 前回と比較してあまり変化はない。

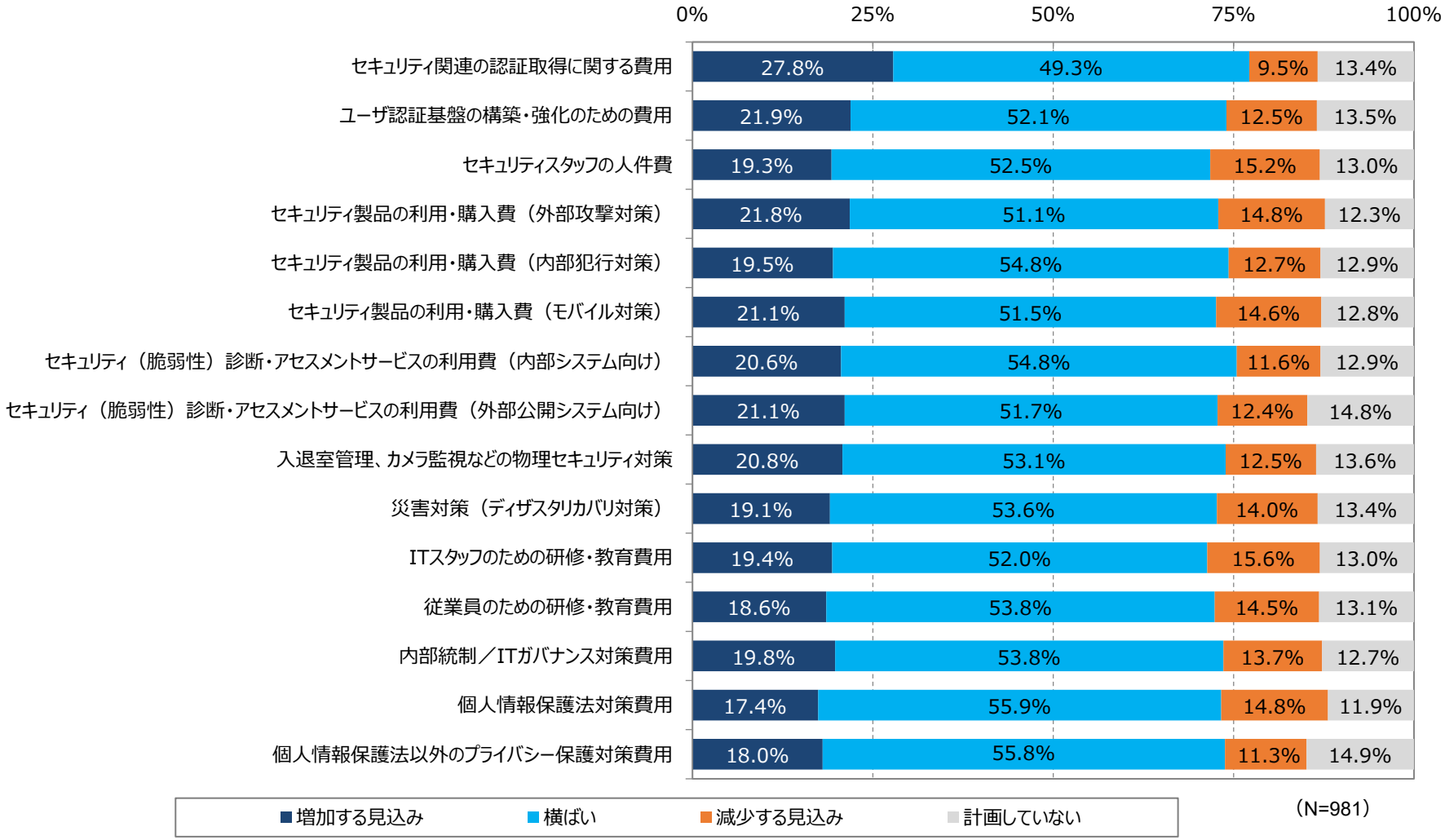


# 3）セキュリティ支出の動向

- Ｑ６_１：　コロナ禍を受けたセキュリティ関連支出（実績）の動向
- Ｑ６_２：　セキュリティ関連支出計画

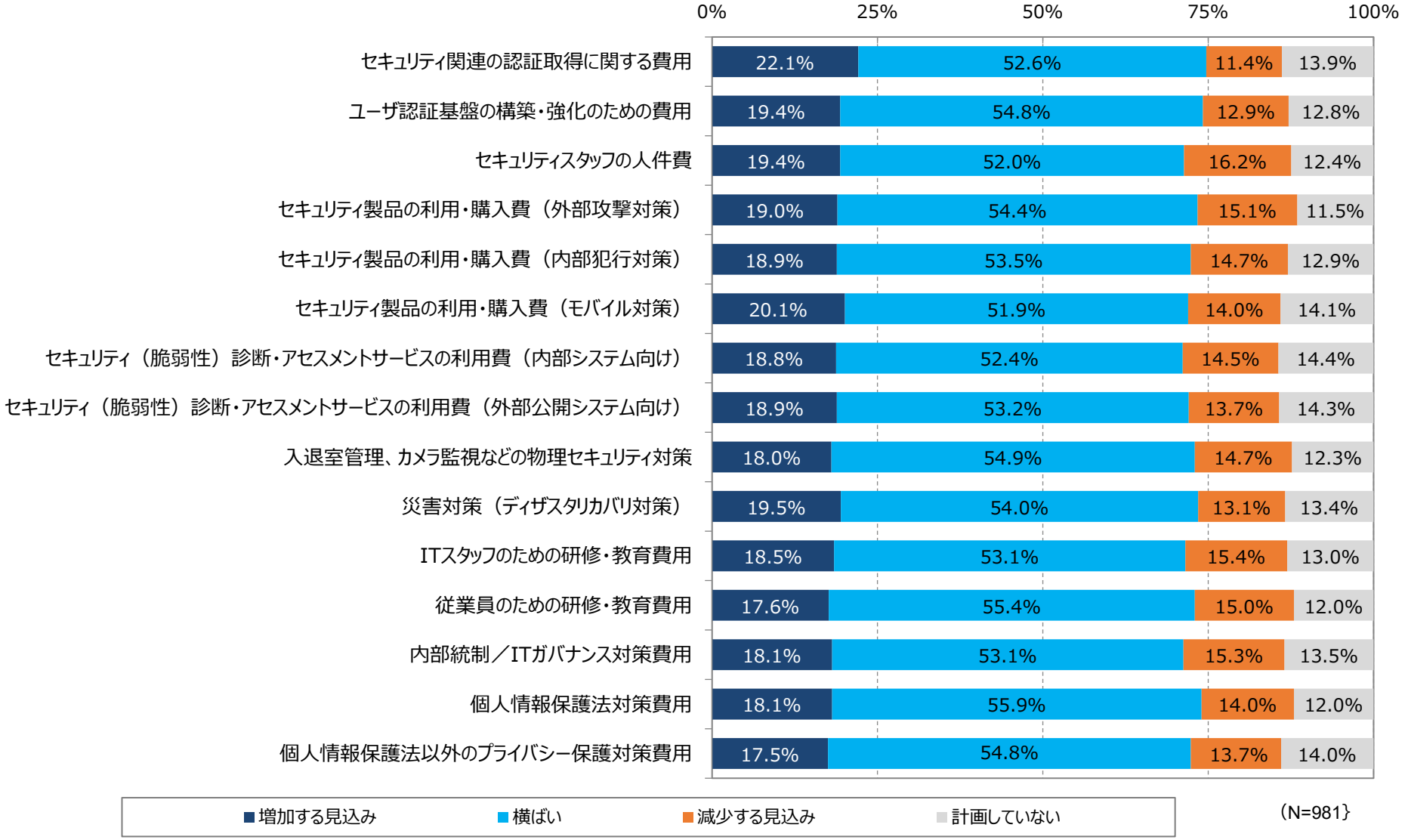
# Q6_1：コロナ禍を受けたセキュリティ関連支出の増減傾向（2021年調査）

■ コロナ禍においてもほとんどの支出実績は「横ばい」と見込んでいる。



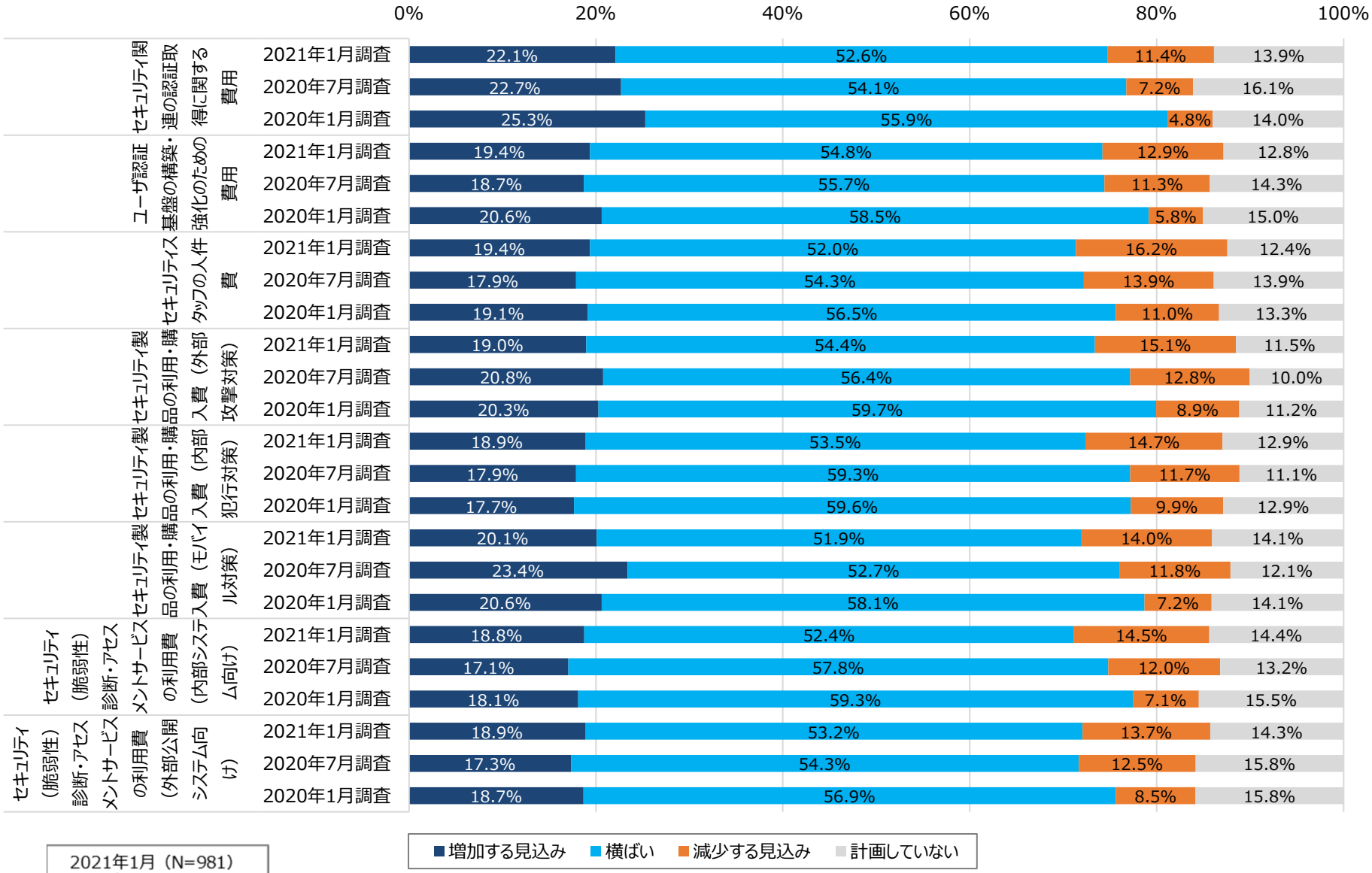
# Q6_2：セキュリティ関連支出計画（2021年調査）

■ 2020年度実績と比較した2021年度セキュリティ関連支出計画については、横這いが５割超、増加が約２割前後となっている。



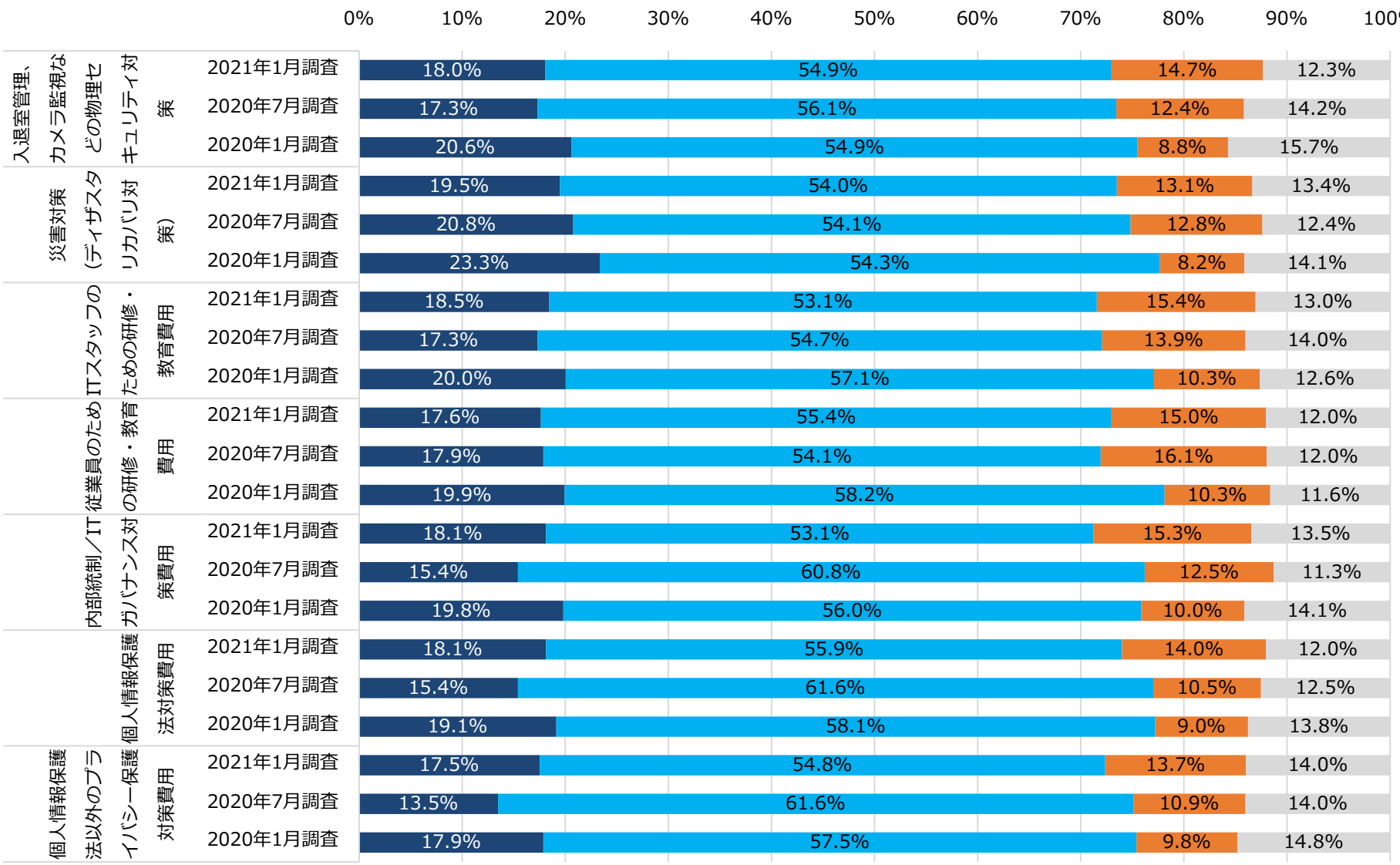

〔N=981〕

# Q6_2：セキュリティ関連支出の計画-1 （2020~2021年比較）




2021年1月（N=981）
2020年7月（N=727）
2020年1月（N=878）

# Q6_2：セキュリティ関連支出の計画-2（2020~2021年比較）

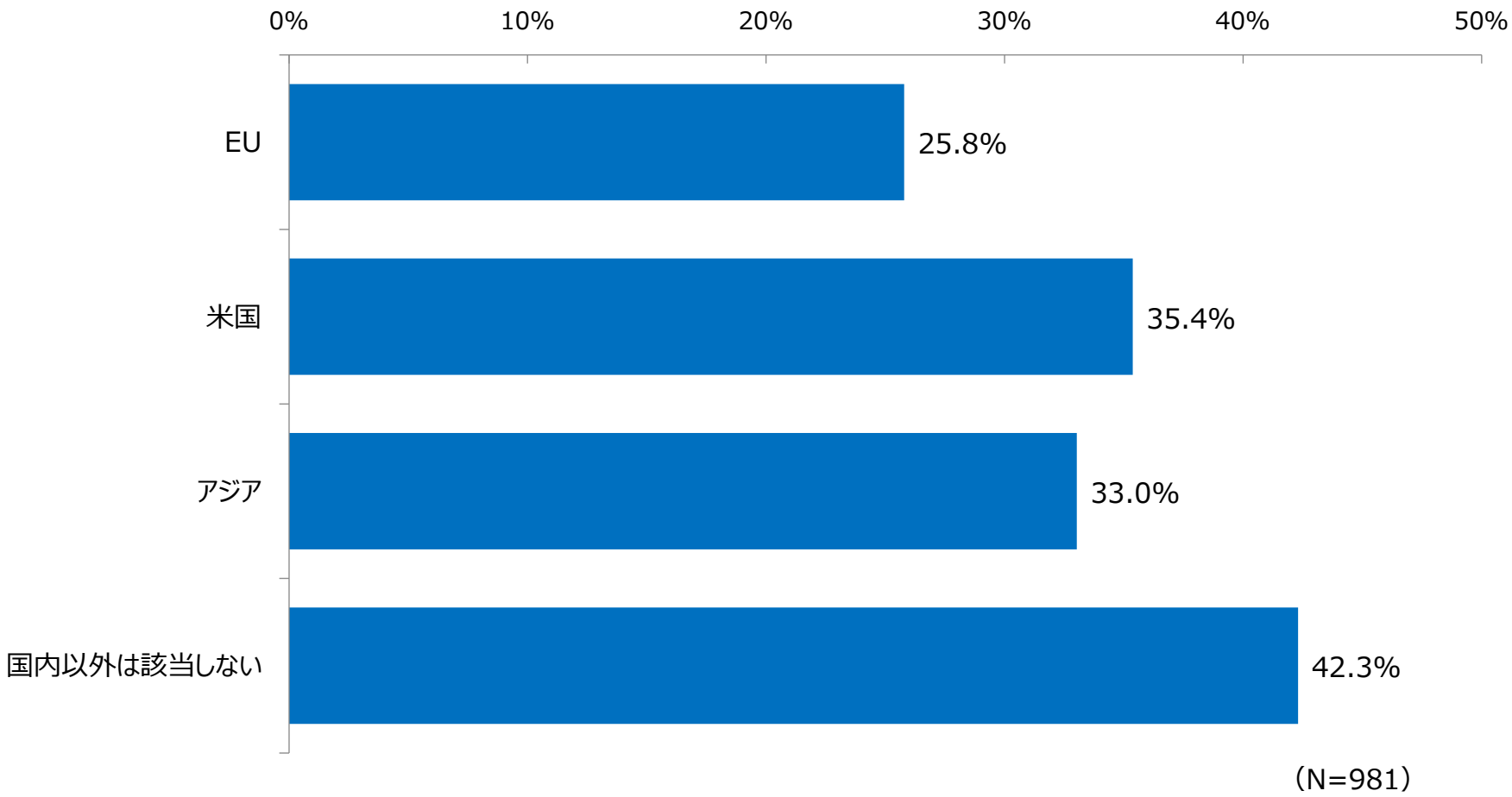


# 4）プライバシーガバナンス

- Q７_１：　グローバル個人情報保護規制
- Q７_２：　国内におけるGDPR対応状況
- Q７_３：　EUとの個人データのやり取り状況
- Q７_４：　国内におけるCBPR認知度
- Q８_１：　プライバシ―ガバナンスの課題認識
- Q８_２：　プライバシーガバナンスガイドブックの認知度
- Q８_３：　プライバシーガバナンスガイドブックの活用ポイント

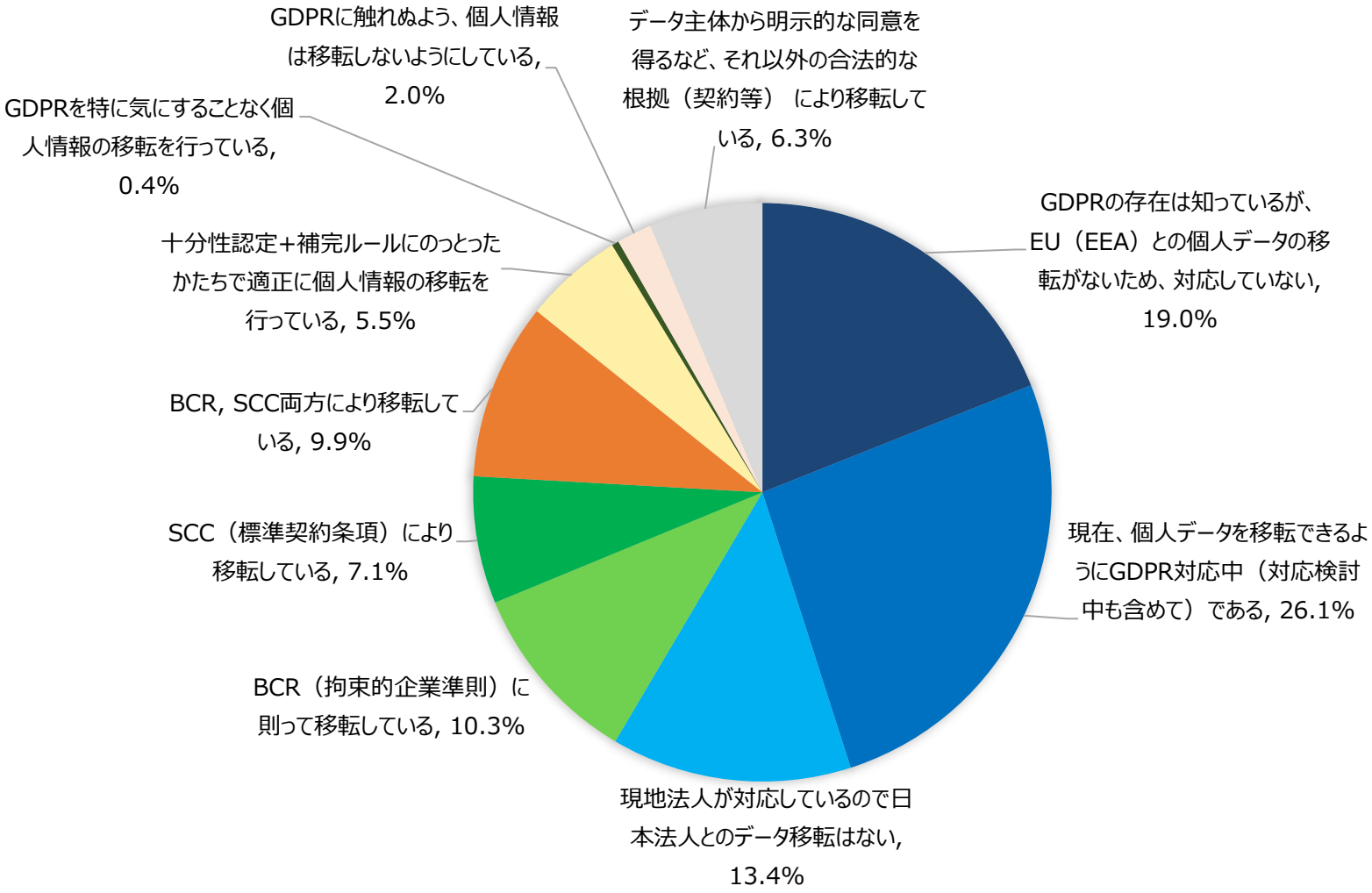
# Q7_1：グローバル個人情報保護規制（2021年調査）

■グローバルの個人情報保護規制で対応しなければならないと地域では日本国内が最も多く、海外では米国、アジア圏、EU圏の順となった。



# Q7_2：国内におけるGDPR対応状況（2021年調査）

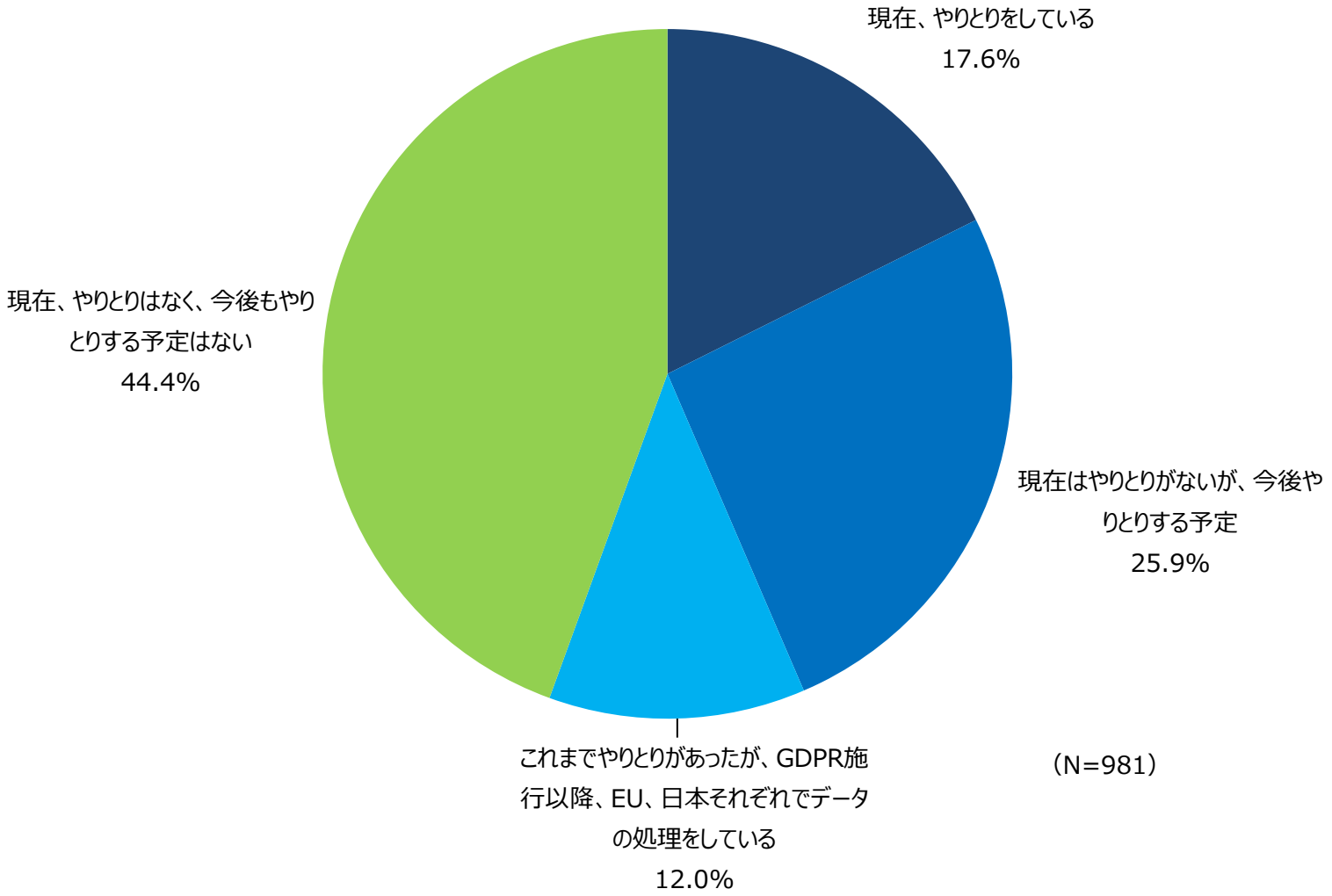
■国内とEU圏でビジネスを行っている企業のGDPR対応状況は、個人データの移転がないので対応していないが最も多く、次はデータ主体からの明示的な合意を得るとなっており、BCRやSCCの締結のケースは少ない。




(N=253)

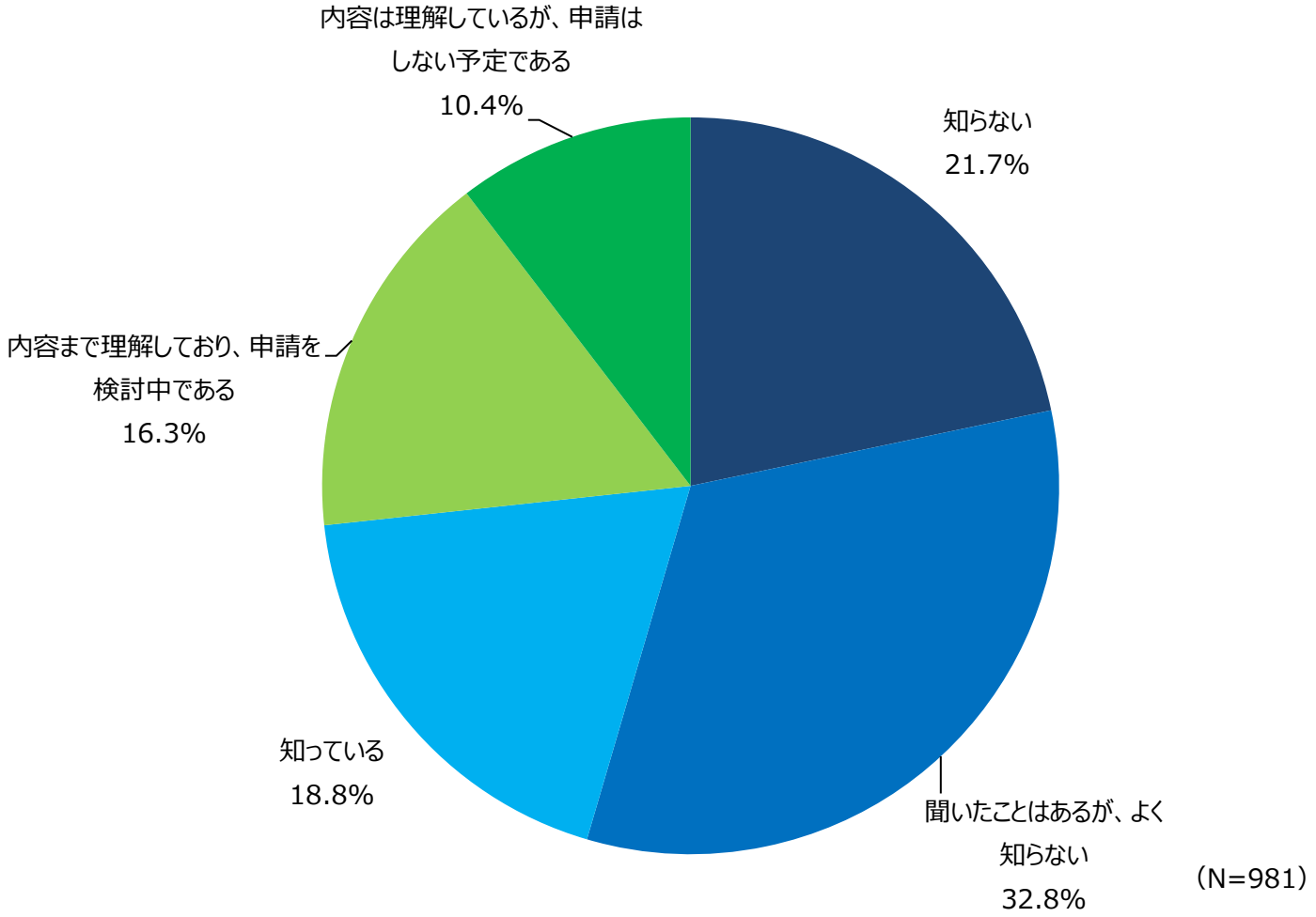
# Q7_3：EUとの個人データのやり取り状況（2021年調査）

■EUとの個人データのやり取りについては行っていないが44.4%で最も多く、GDPR施行以降やりとりを止めて、それぞれで処理をしているが12%となっており、現時点でやりとりをしているは17.6%となっている。



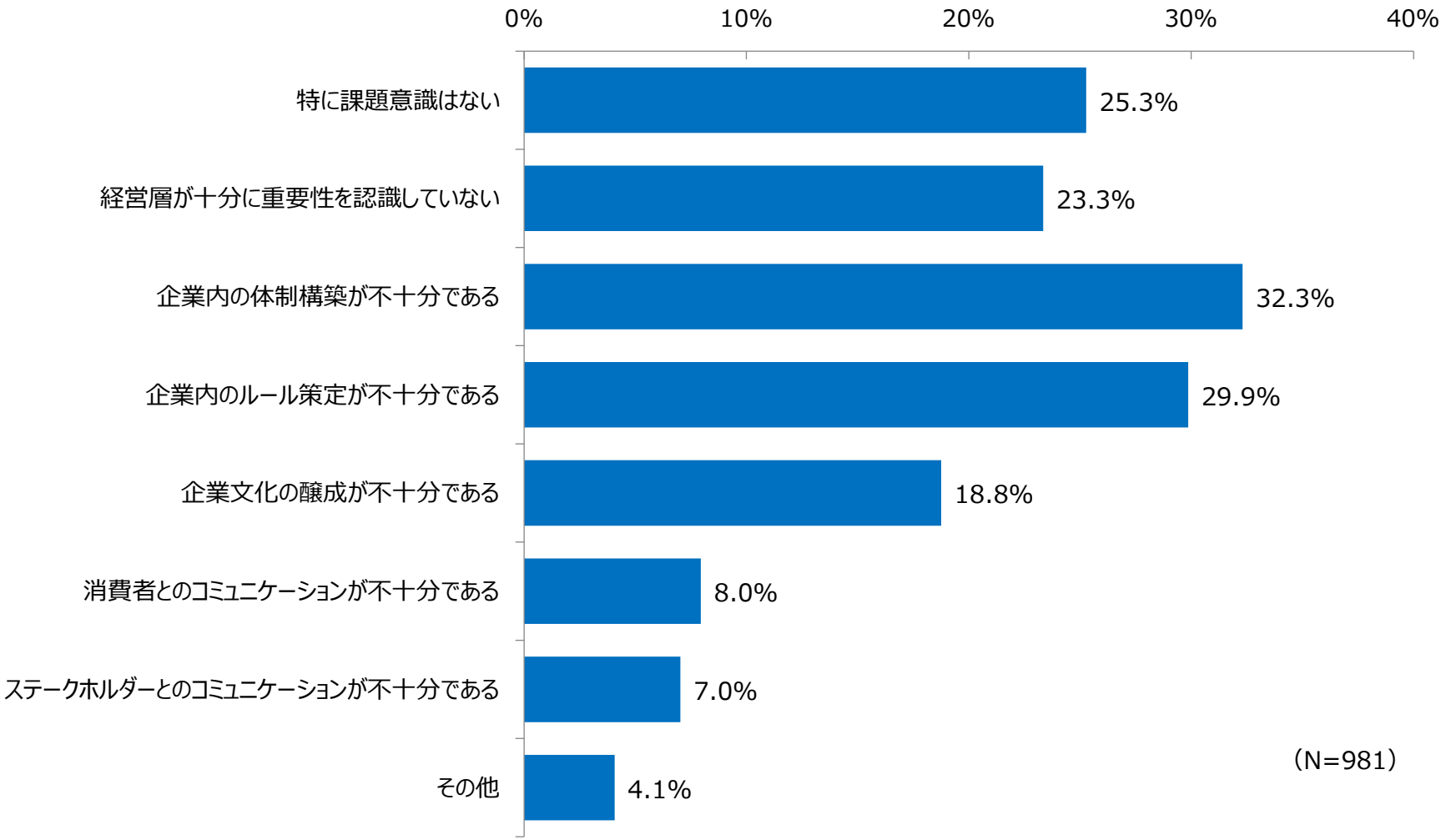
# Q7_4：国内におけるCBPR認知度（2021年調査）

■CBPR（APEC越境プライバシールール）の国内での認知状況は、「聞いたことがあるがよく知らない」と「知らない」で５割を超えており、認知は進んでいない。一方、「申請を検討中」も16.3%ある。



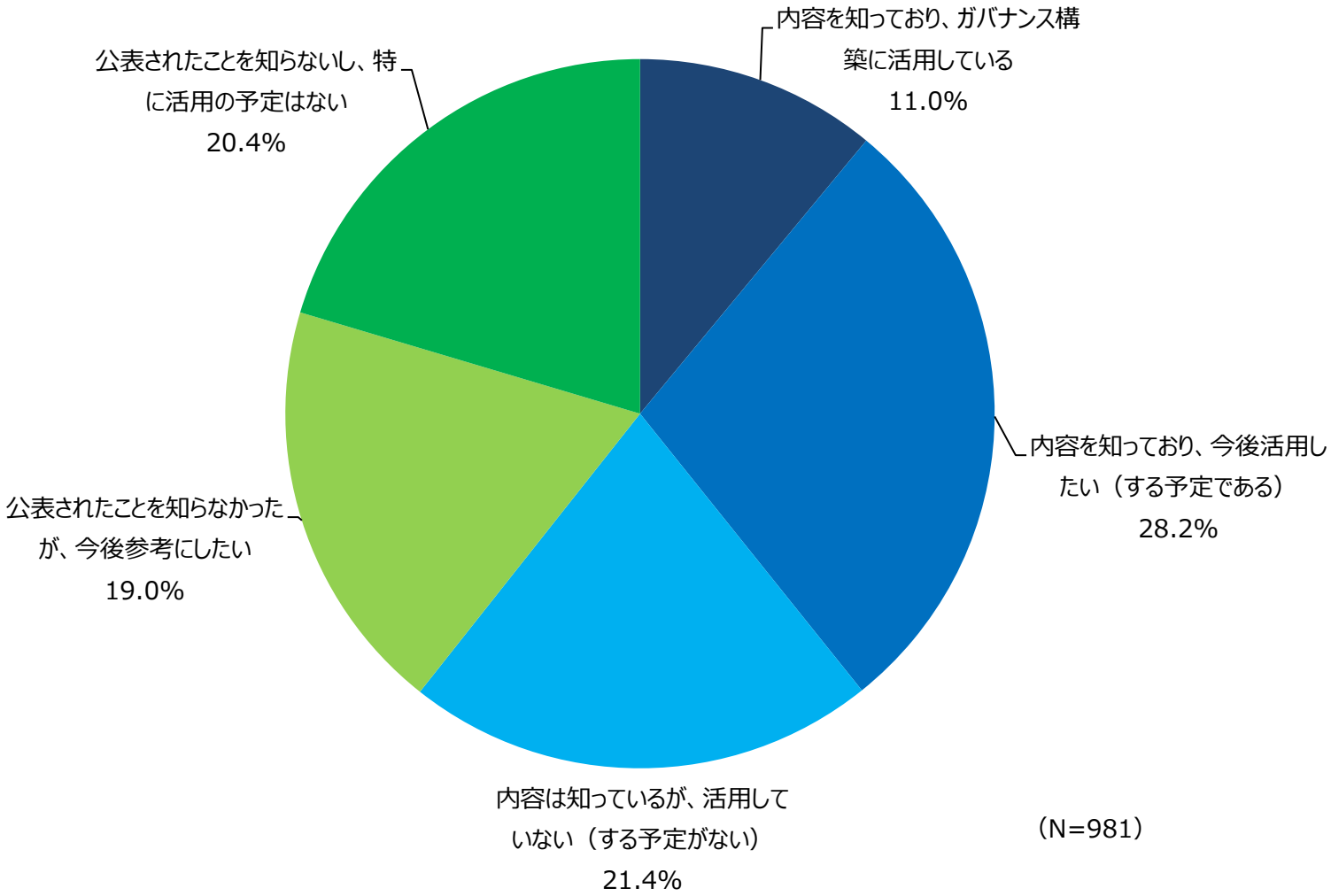
# Q8_1：プライバシーガバナンスについての課題認識（2021年調査）

■プライバシーガバナンスの課題として認識されているのは、企業内の体制構築が不十分が32.3%でトップ。企業内のルール策定が不十分が29.9%で２位となっている。



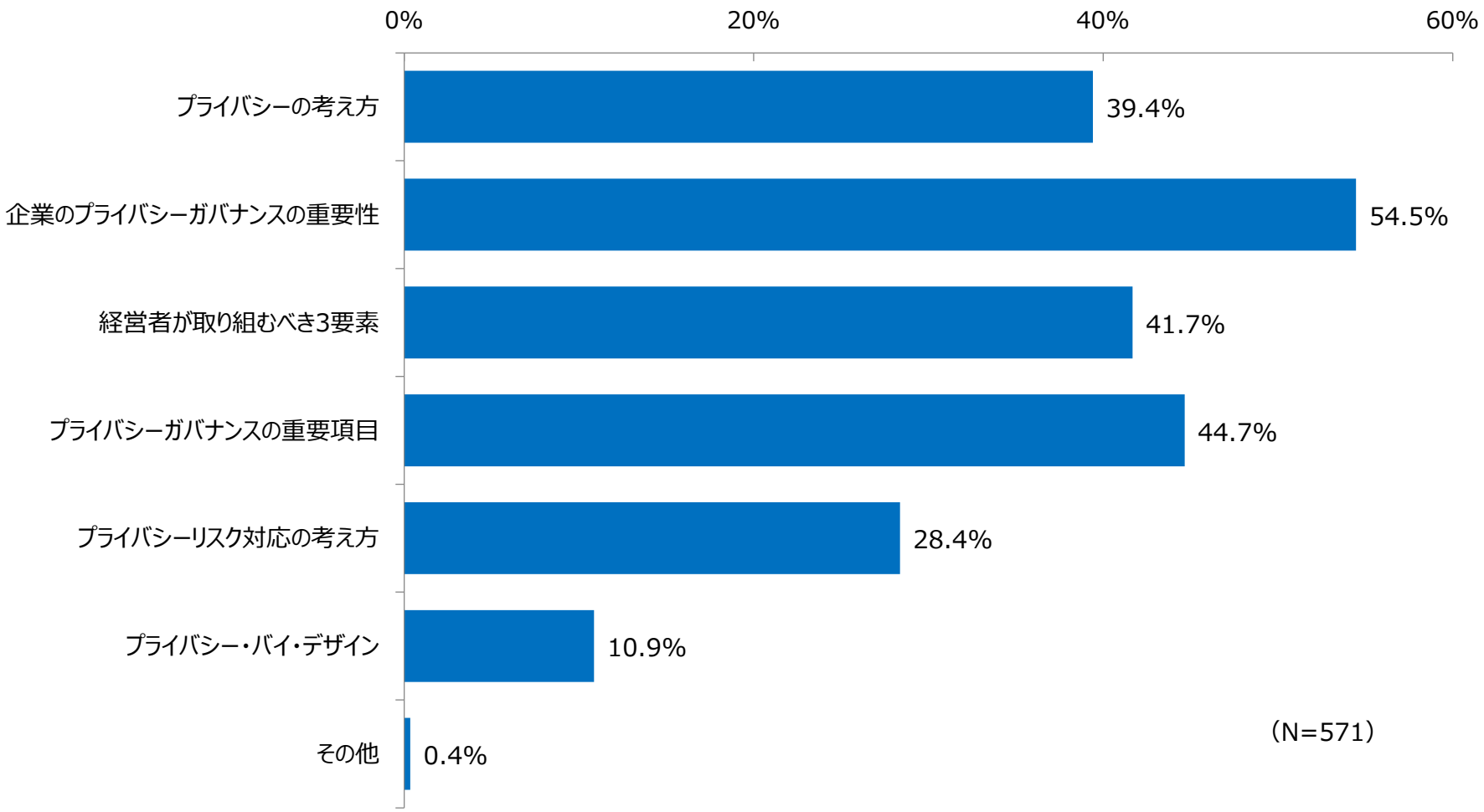
# Q8_2：プライバシーガバナンスガイドブックの認知度（2021年調査）

■プライバシーガバナンスガイドブックを知っているが６割を超えており、４割が活用している、または活用予定と回答している。



# Q8_3：プライバシーガバナンスガイドブックの活用ポイント（2021年調査）

■プライバシーガバナンスガイドブックの活用ポイントしては、プライバシーガバナンスの重要性の訴求がトップで
プライバシーガバナンスの重要項目が２番目となっている。

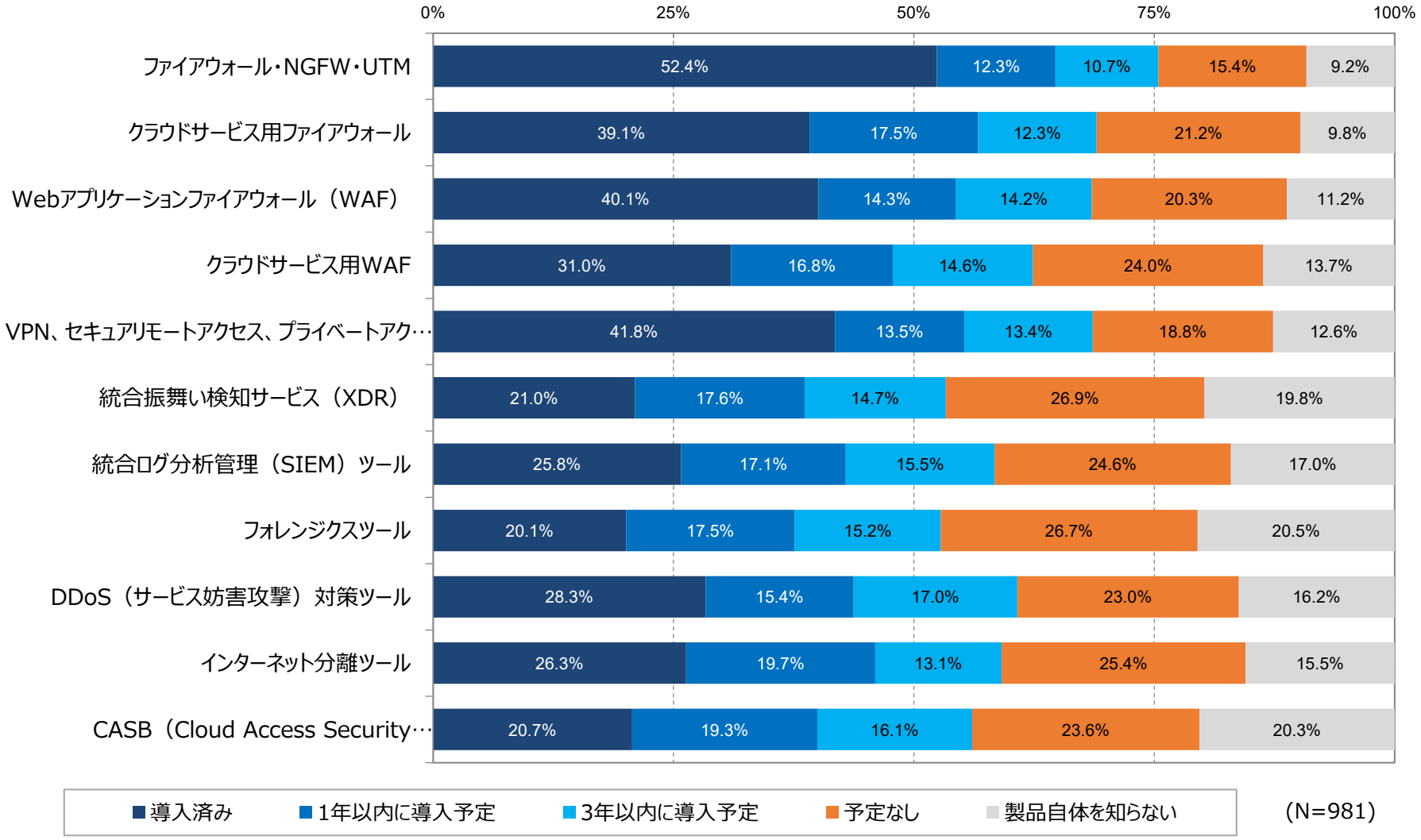


# 5）セキュリティ製品／技術の利用動向

- Q9　：　セキュリティ製品・サービスの導入状況
- Q10：　電子メールのセキュリティ対策状況
- Q11：　高機密システムのアクセス認証手段

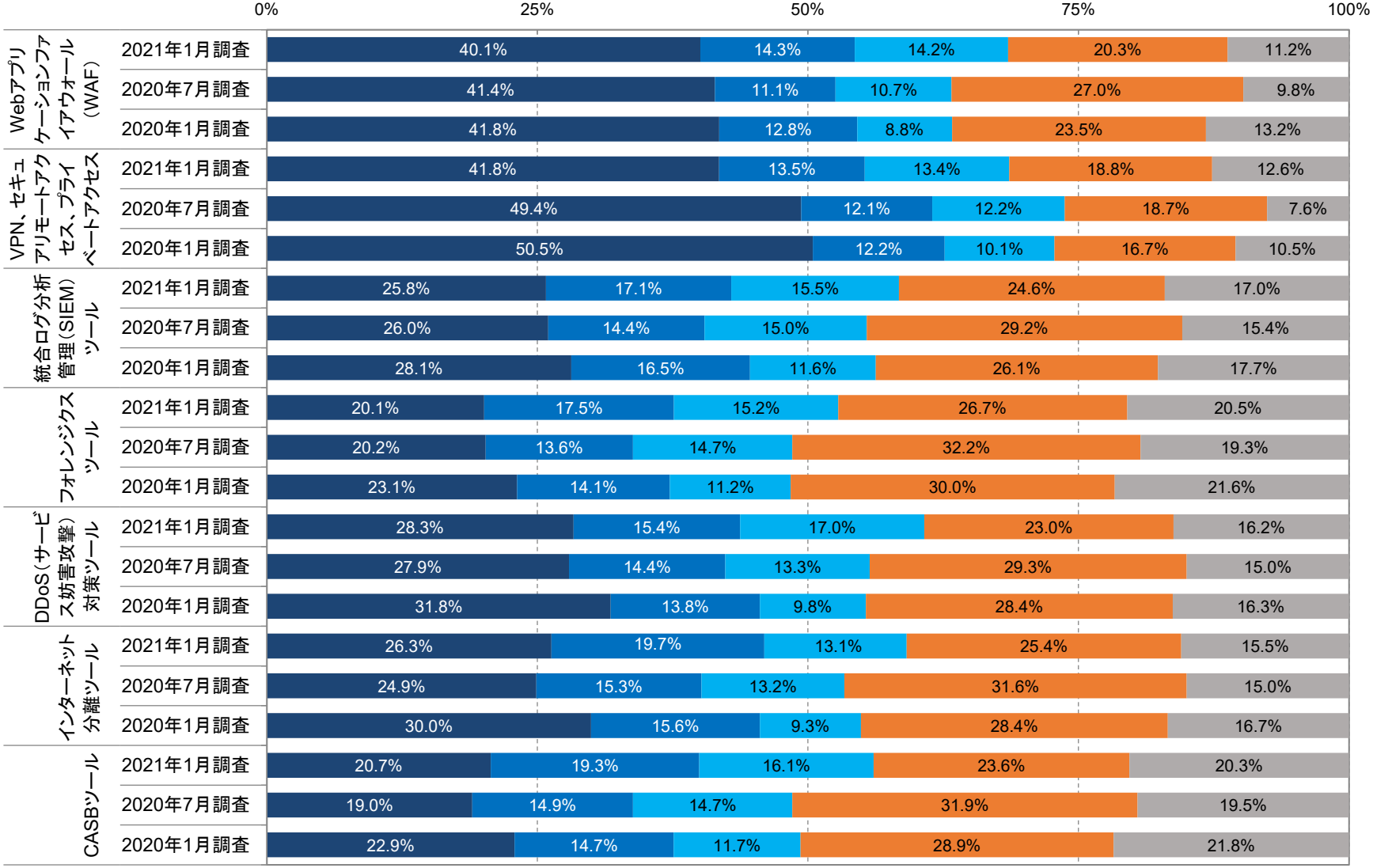
# Q9_1：セキュリティ製品の利用状況［ネットワーク/ゲートウェイ系］（2021年調査）

■ オンプレミス用のセキュリティ製品からクラウド用のセキュリティ製品への移行が進みつつあるが、まだ導入済の比率は高くない。




(N=981)

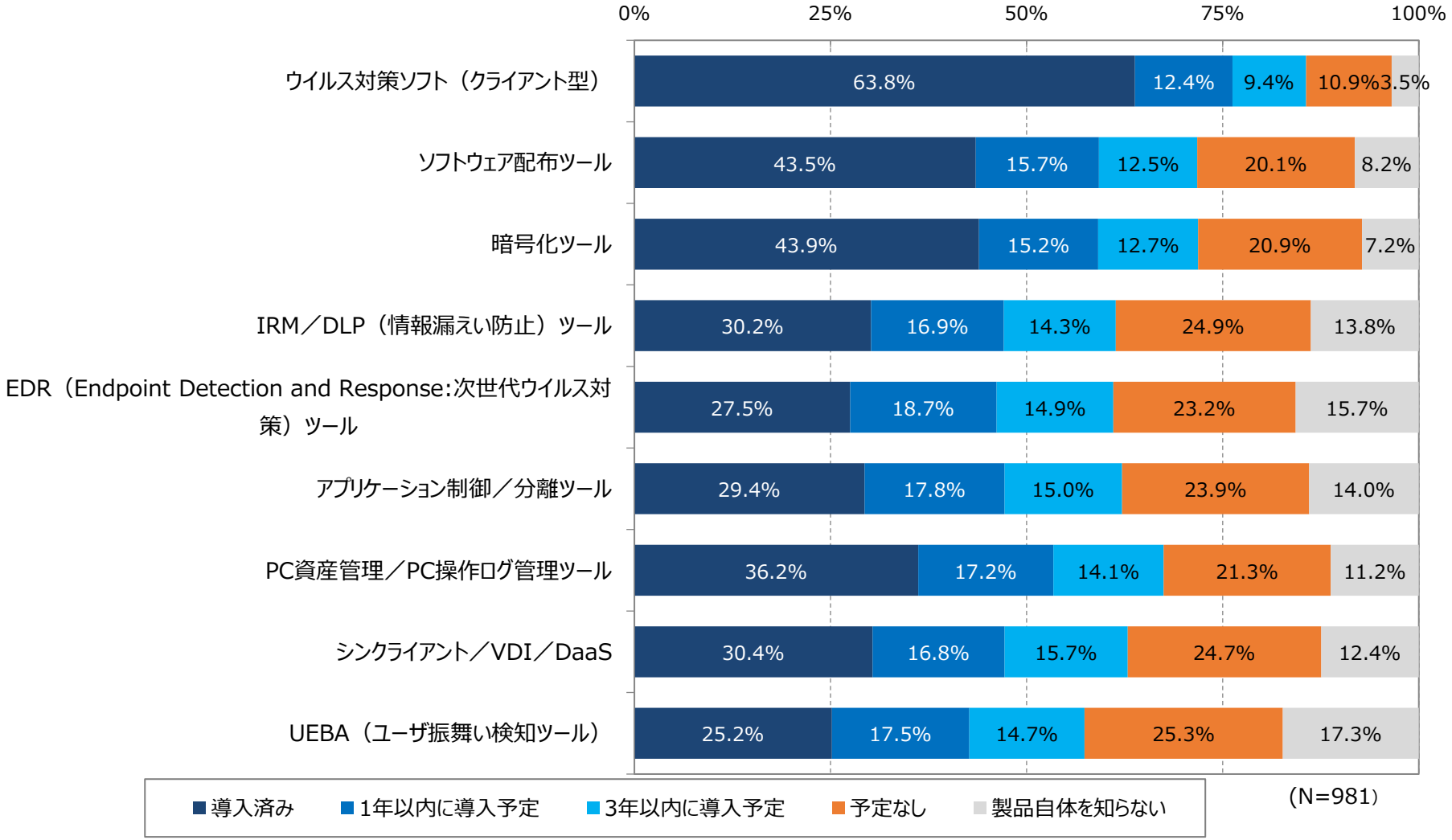
# Q9_1：セキュリティ製品の利用状況［ネットワーク/ゲートウェイ系］（2020~2021年比較）



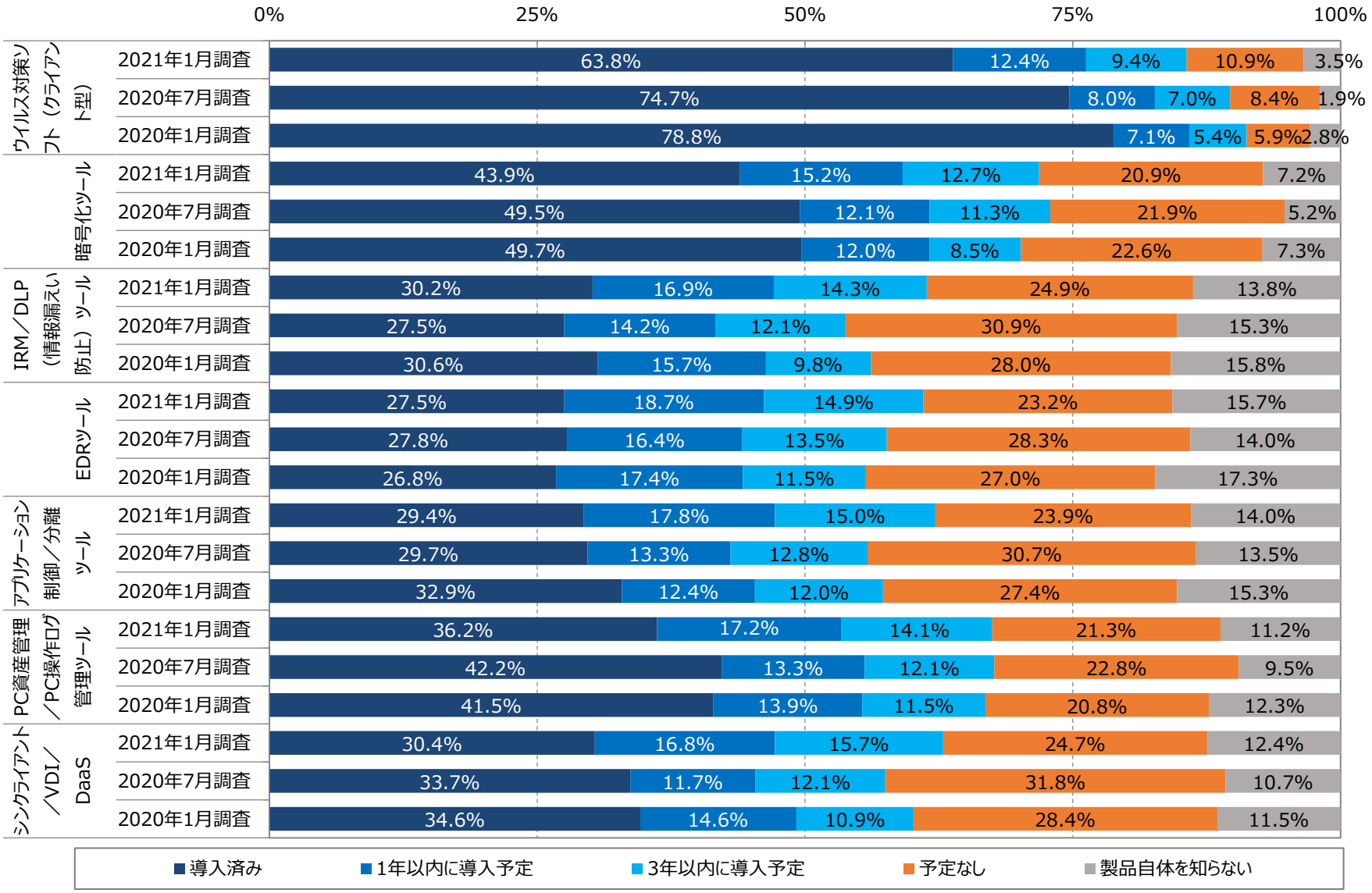

2021年1月（N=981）
2020年7月（N=727）
2020年1月（N=878）

# Q9_2：セキュリティ製品の利用状況［エンドポイント対策］（2021年調査）

■ 従来型のウイルス対策ソフトの導入済比率が低下する一方、次世代型のウイルス対策ソフトであるEDRが少しづつ伸びてきておりエンドポイント領域における世代交代が進みつつある。



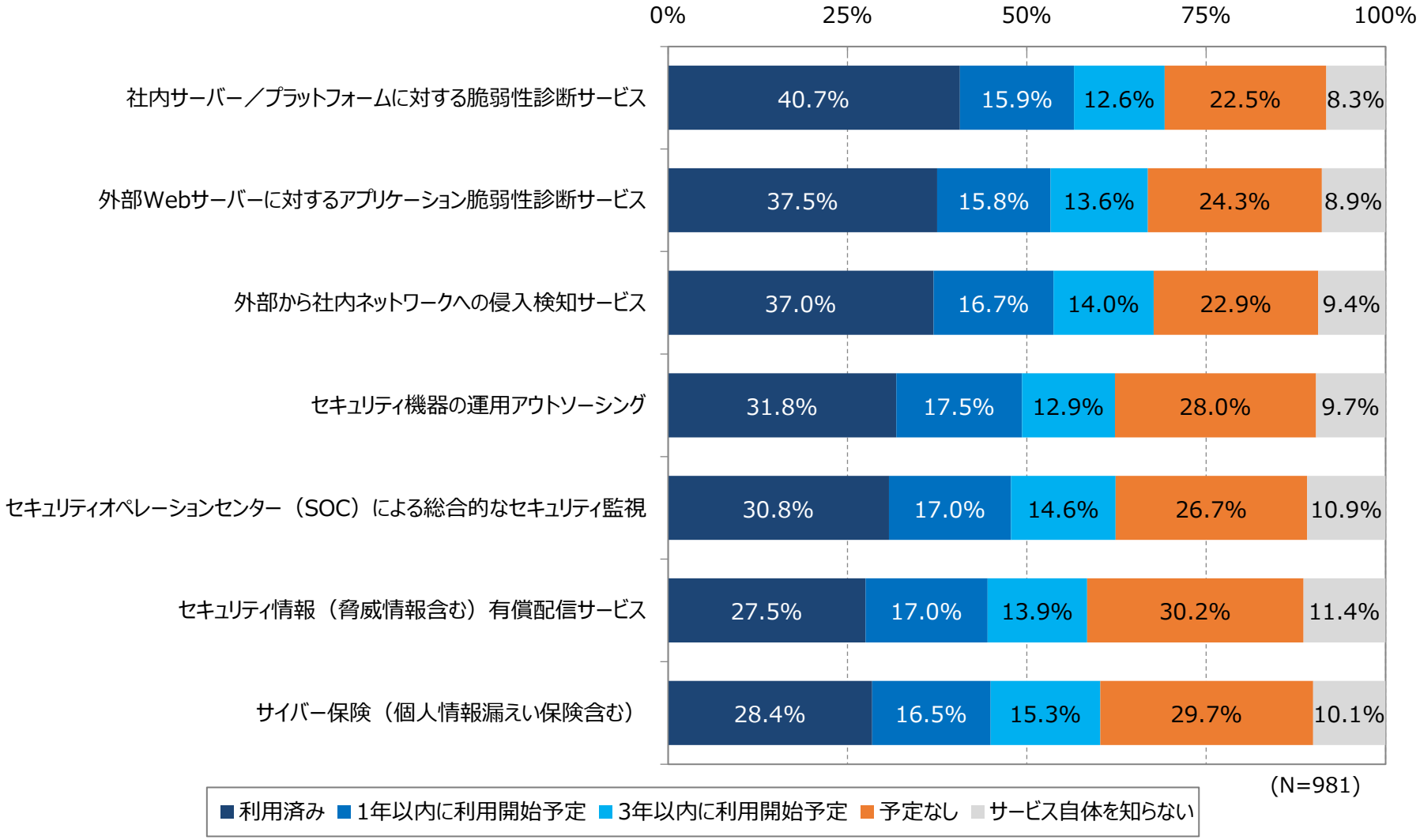
# Q9_2：セキュリティ製品の利用状況［エンドポイント対策］（2020~2021年比較）



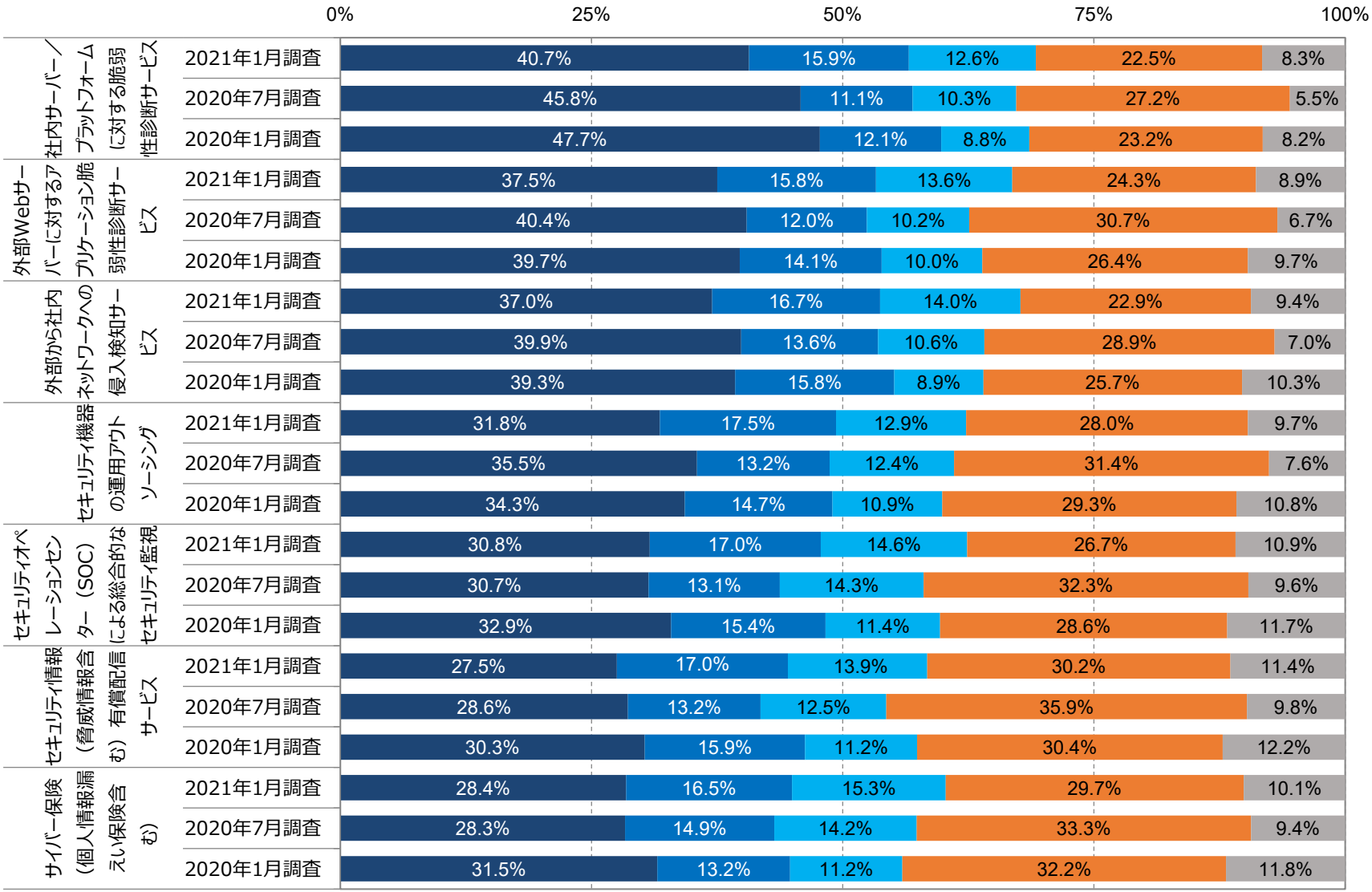

2021年1月（N=981）
2020年7月（N=727）
2020年1月（N=878）

# Q9_3：セキュリティ製品の利用状況［セキュリティサービス］（2021年調査）

■ 前回と傾向は同じで自社システムの脆弱性診断サービスや侵入検知サービスの比率が高い。



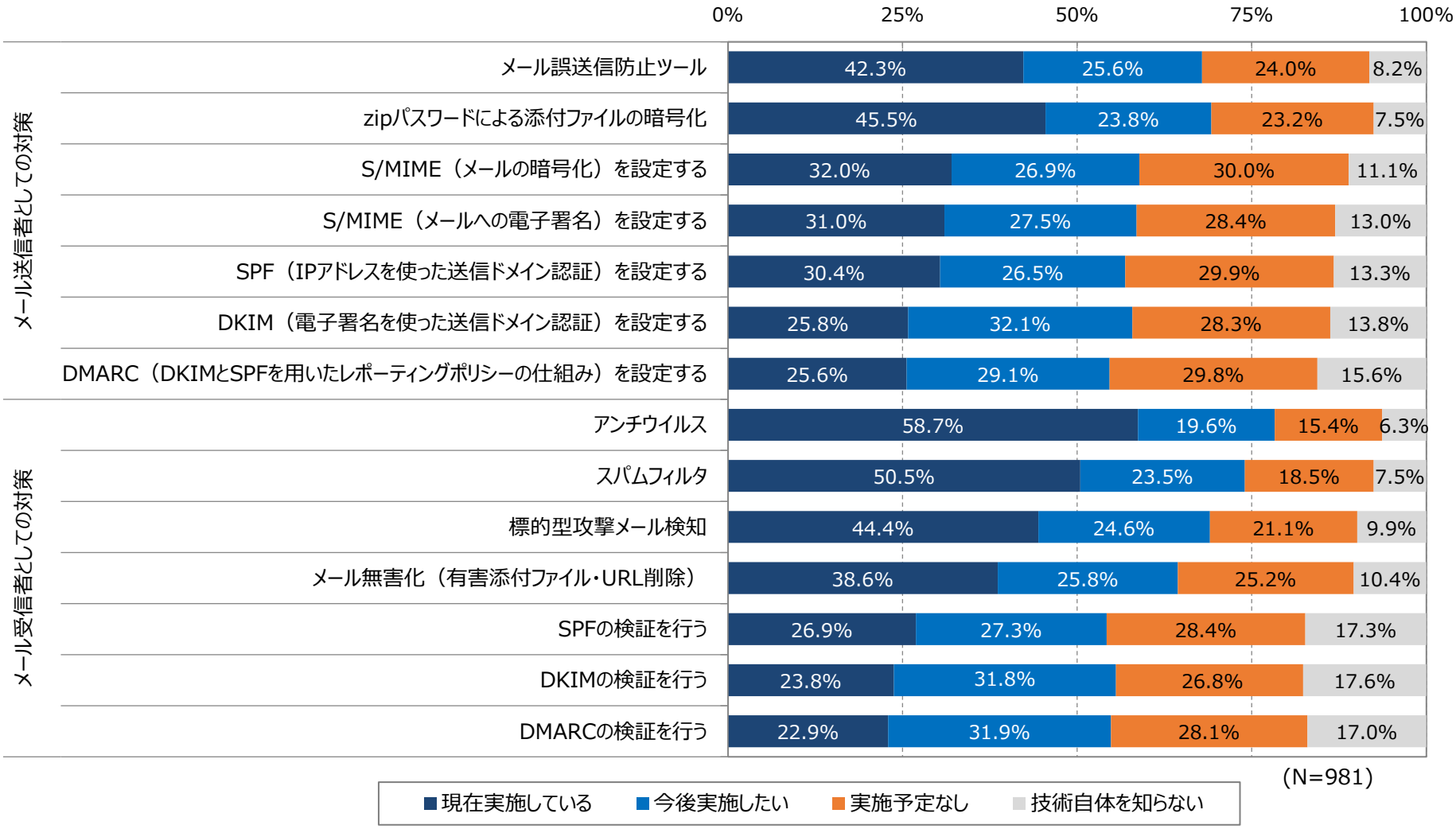
# Q9_3：セキュリティ製品の利用状況［セキュリティサービス］（2020~2021年調査比較）




2021年1月（N=981）
2020年7月（N=727）
2020年1月（N=878）

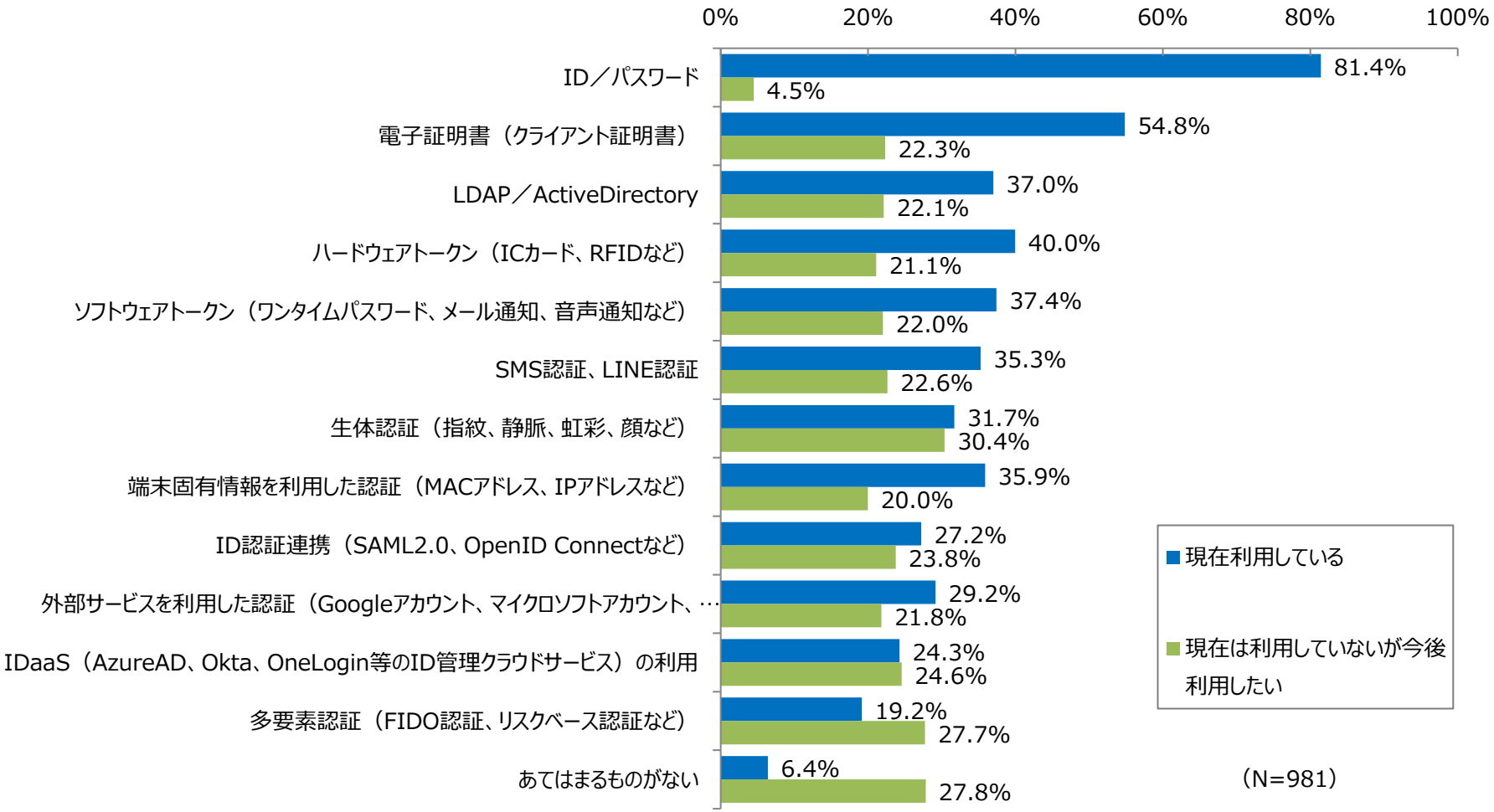
# Q10：電子メールのセキュリティ対策状況（2021年調査）

■ 送信側は政府非推奨となったZipパスワード暗号化添付ファイル（PPAP）が最も多く、次がメール誤送信防止ツールで、受信側はアンチウイルスとスパムフィルタとなり、前回同様の結果となっている。

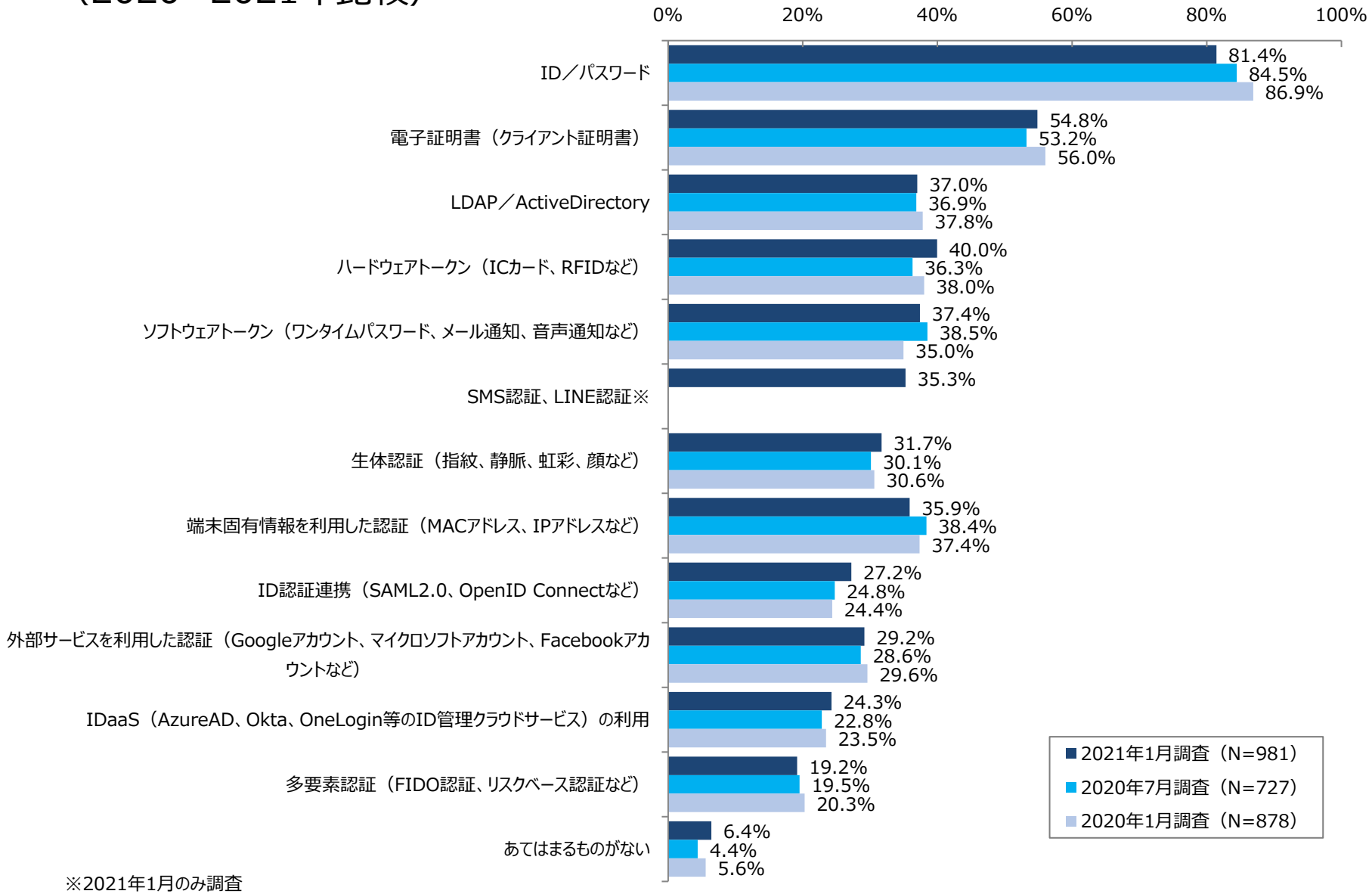


# Q11：高機密システムへのアクセス認証手段（2021年調査）

■ 現在利用している認証手段としてはID・パスワードが最も多いが、減少に転じつつある。かわりに生体認証や多要素認証、IDaaS（クラウドID認証サービス）が増えつつある。

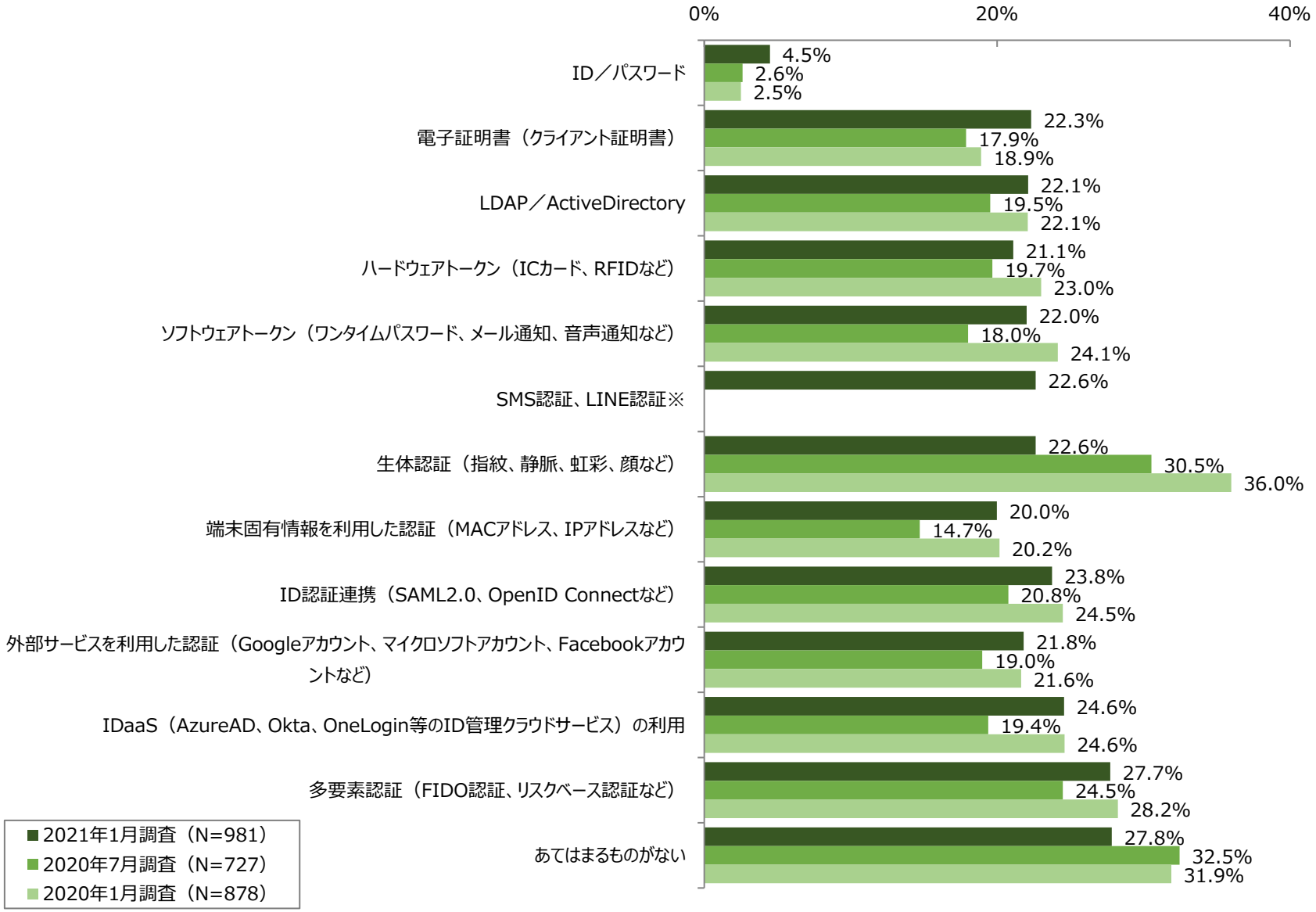


# Q11：高機密システムへのアクセス認証手段［現在利用中のシステム］（2020~2021年比較）




※2021年1月のみ調査

# Q11：高機密システムへのアクセス認証手段［今後利用したいシステム］（2020~2021年比較）



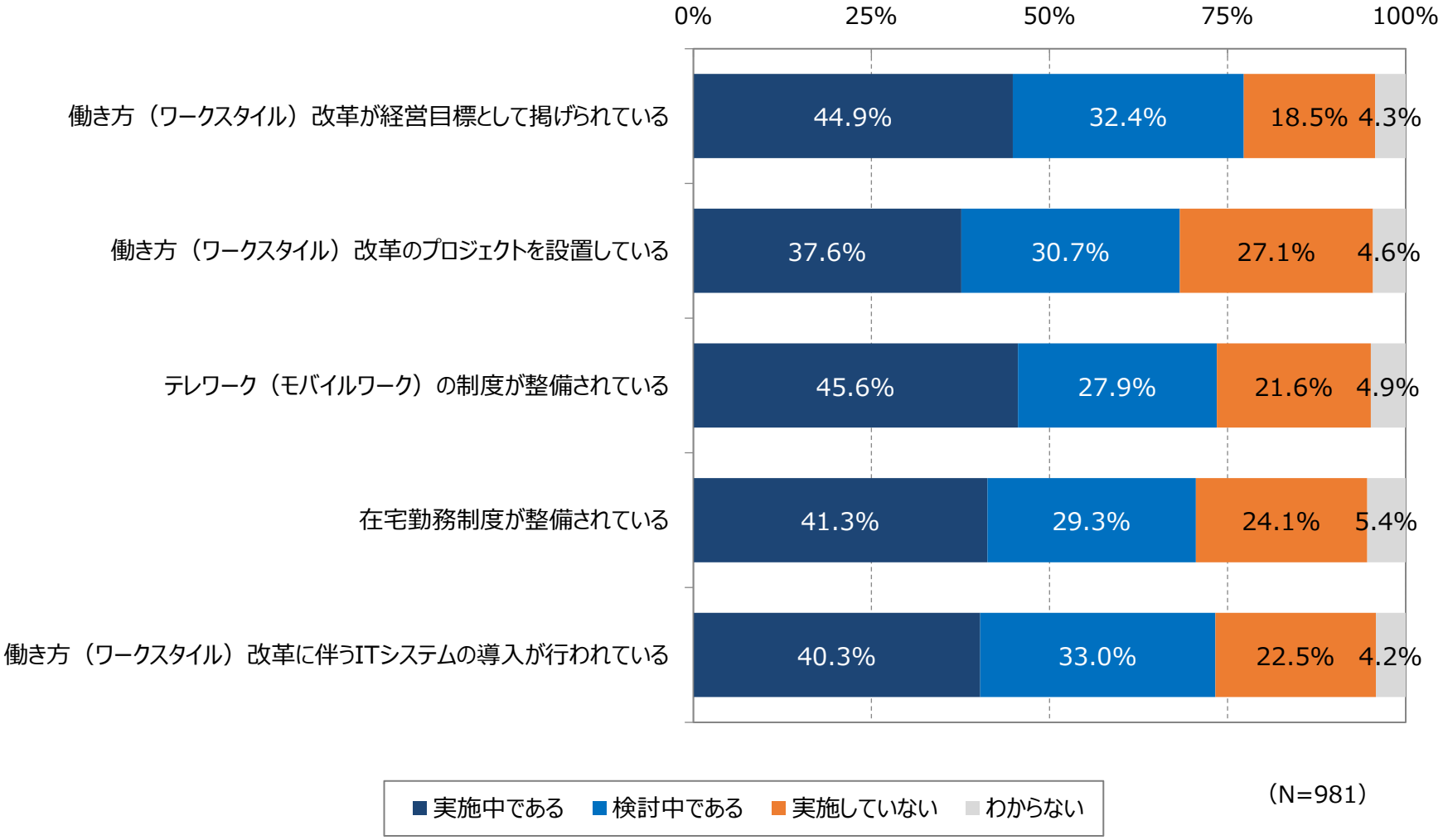

※2021年1月のみ調査

# ６）働き方改革、クラウドの動向

- Q12_1：　働き方改革への取組み状況
- Q12_2：　ワークスタイルに関連するセキュリティ対策
- Q13_1：　クラウドサービスの利用状況
- Q13_2：　クラウドサービスの利用方法
- Q13_3：　クラウドサービスの選定ポイント
- Q13_4：　信頼性を重視するクラウドサービス

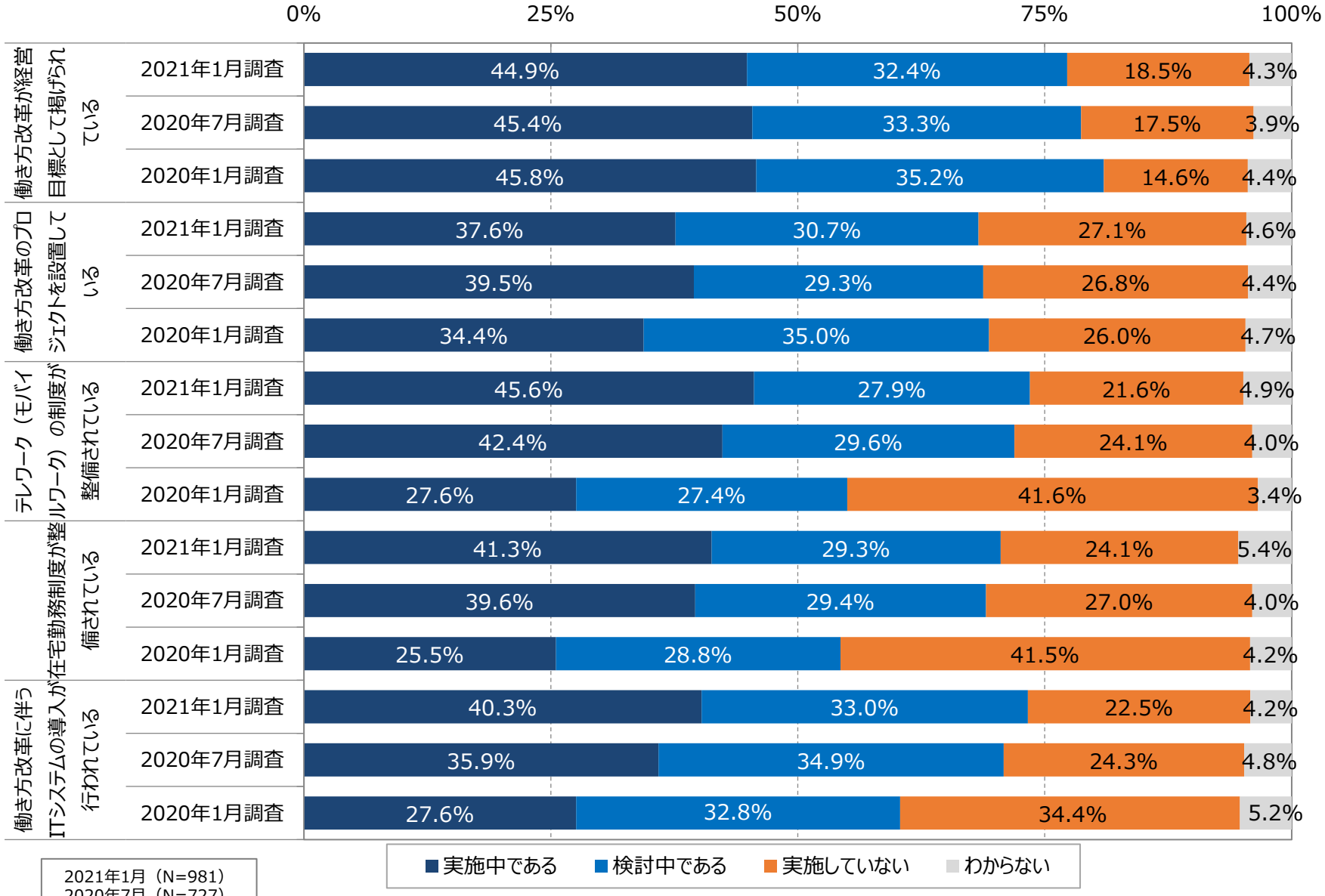
# Q12_1：「働き方改革」への取組み状況（2021年調査）

■テレワーク制度の整備、在宅勤務制度の整備、働き改革に伴うシステム導入の比率が明確に上がっておりコロナ禍における勤務形態の変更と働き方改革が一気に進んだことがわかる。




（N=981）

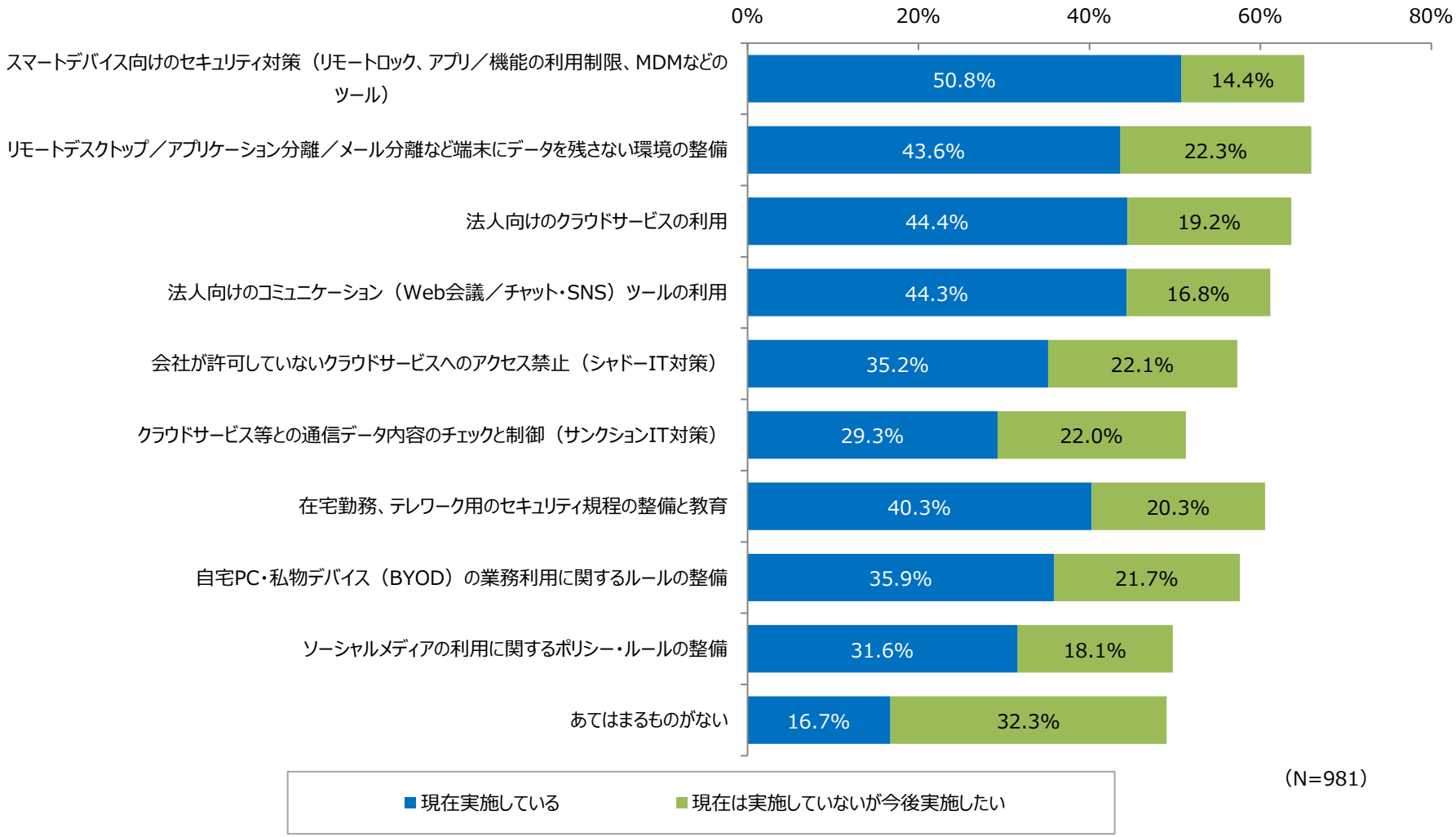
# Q12_1：「働き方改革」への取組み状況（2020~2021年比較）




2021年1月（N=981）
2020年7月（N=727）
2020年1月（N=878）

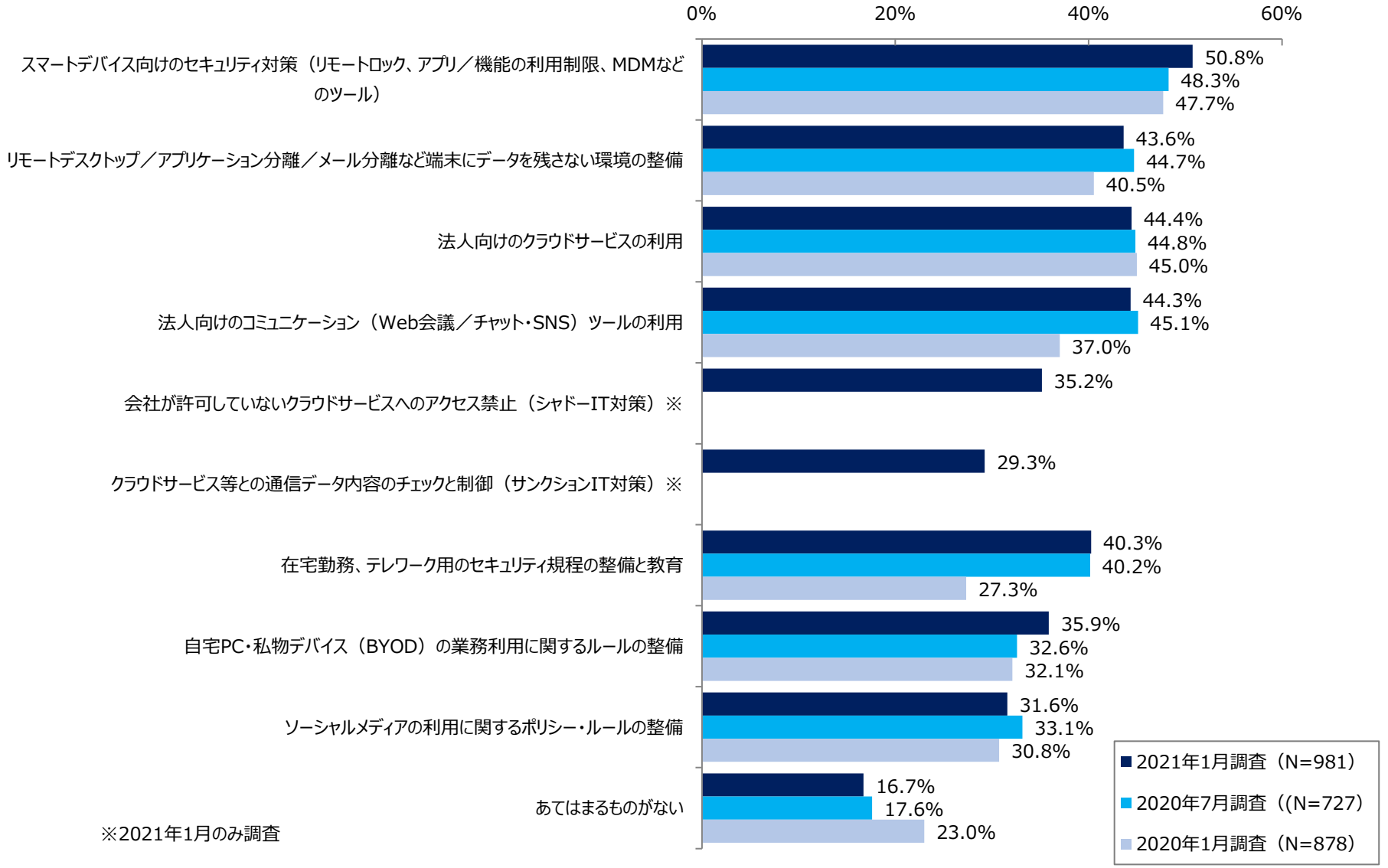
# Q12_2：ワークスタイルに関連するセキュリティ対策の状況（2021年調査）

■ 実施済の対策についてはスマートデバイスのセキュリティ対策が５割を超え、法人向けクラウドサービスの利用や法人向けコミュニケーションツールの利用が続いている。



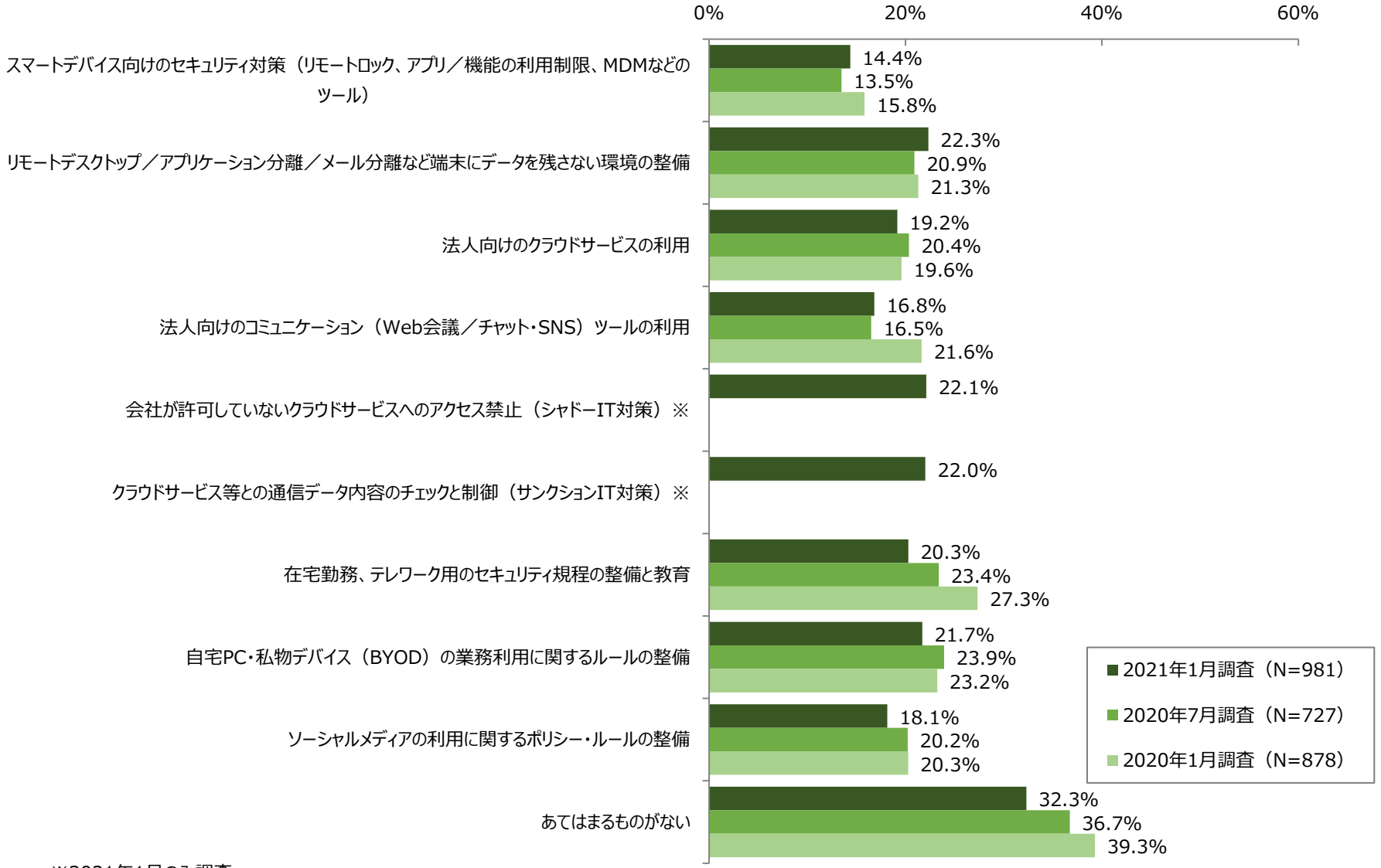

（N=981）

# Q12_2：ワークスタイルに関連するセキュリティ対策の状況［現在利用中の対策］（2020~2021年比較）




※2021年1月のみ調査

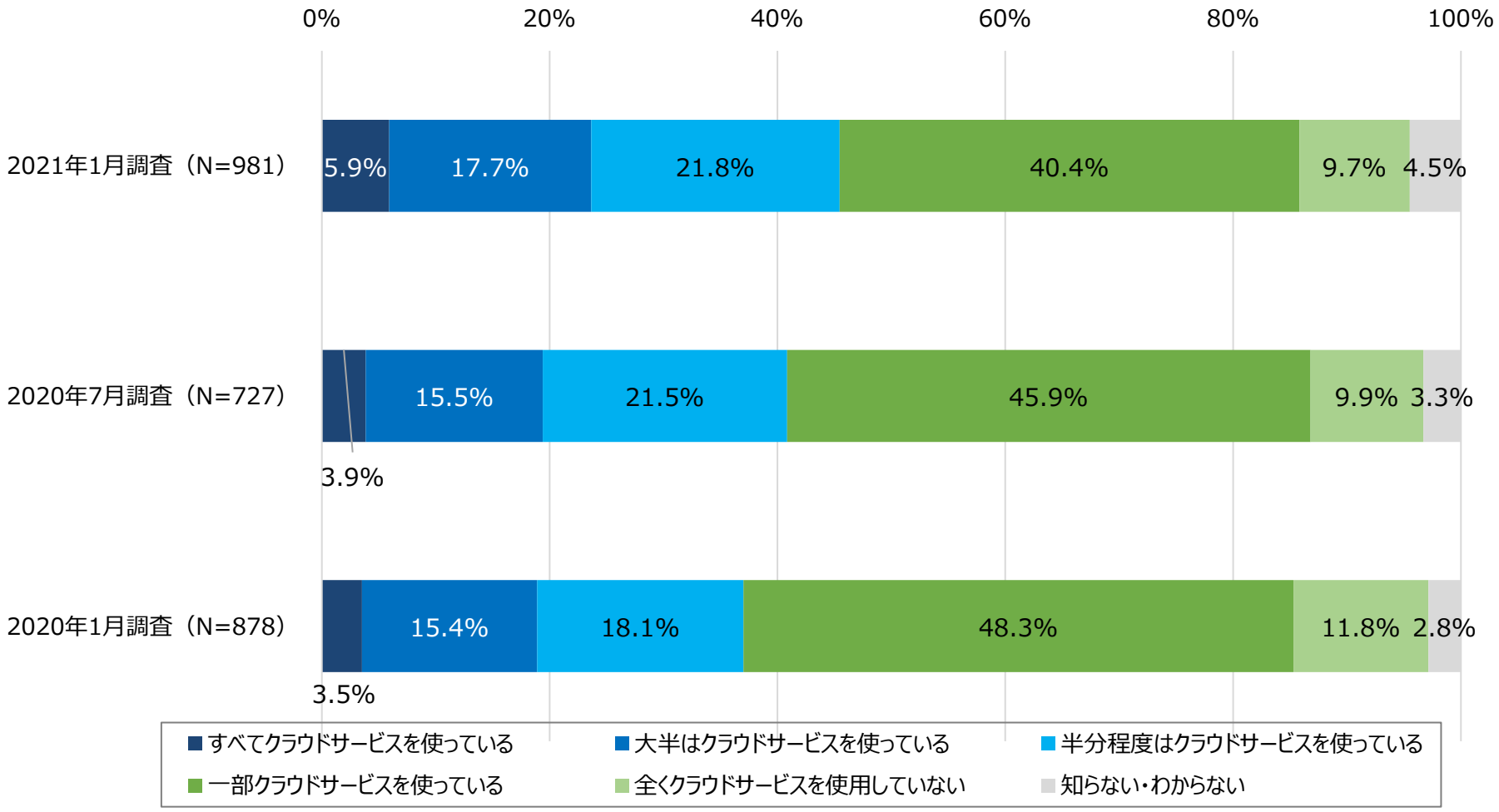
# Q12_2：ワークスタイルに関連するセキュリティ対策の状況［今後利用したい対策］（2020~2021年比較）




※2021年1月のみ調査

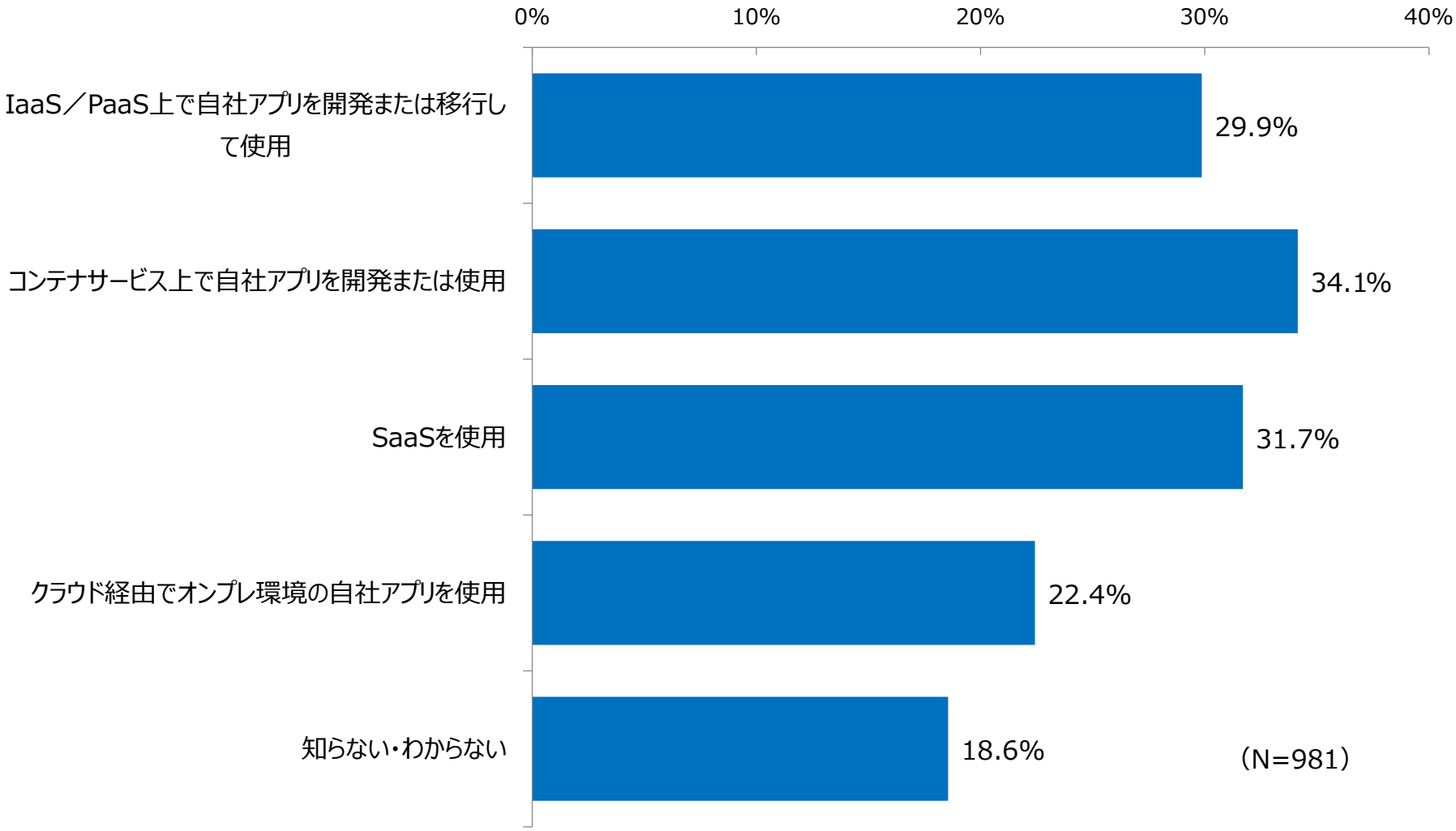
# Q13_1：クラウドサービスの利用状況（2020～2021年比較）

■半分以上クラウドサービスを利用している比率が 5 割に近づきつつあり、クラウドサービスの利用率は高くなっている。



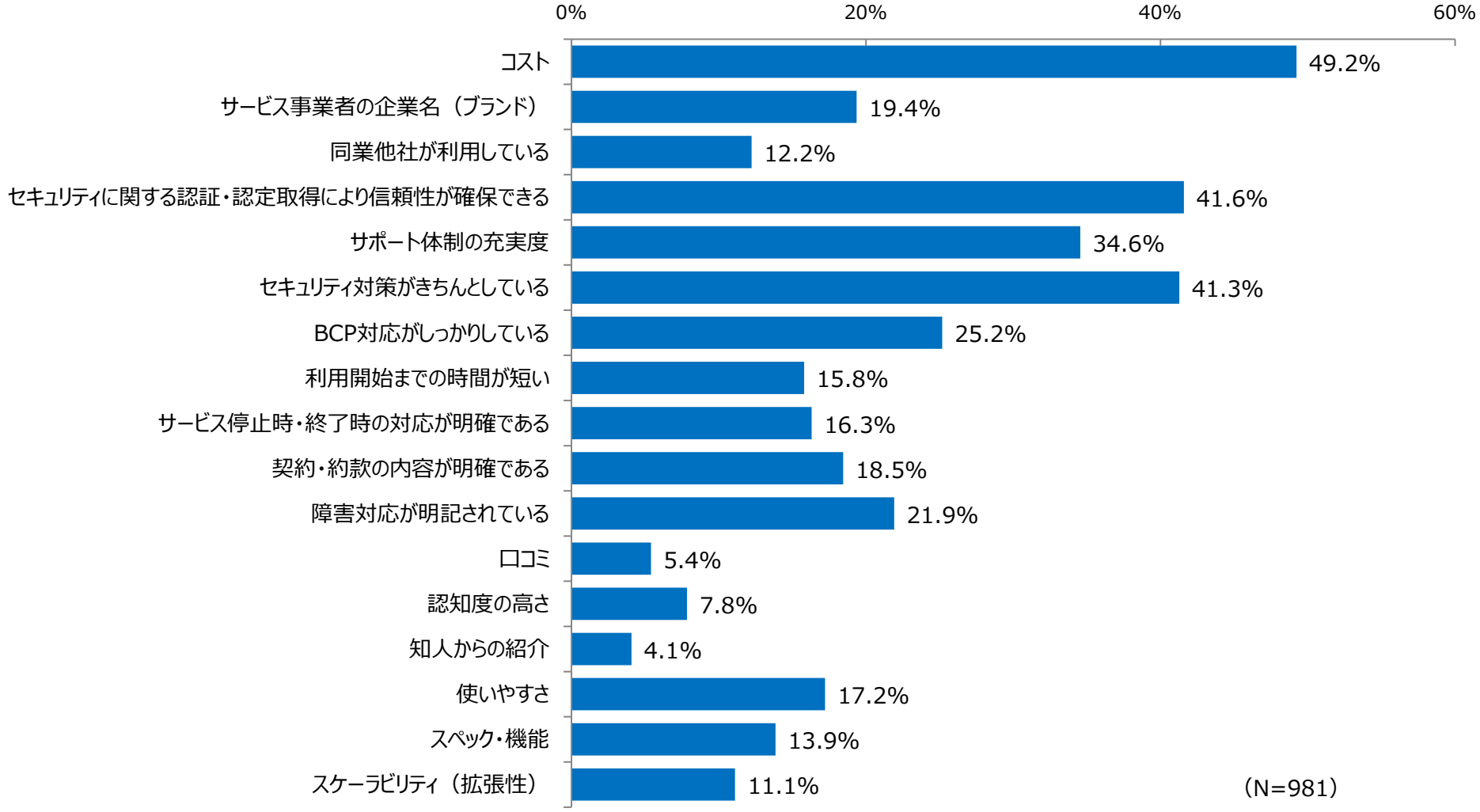
# Q13_2：クラウドサービスの利用方法（2021年調査）

- コンテナサービス上での開発がトップとなっており、SaaSの利用、IaaS/PaaS上での開発が続いており、コンテナサービスが普及してきている。

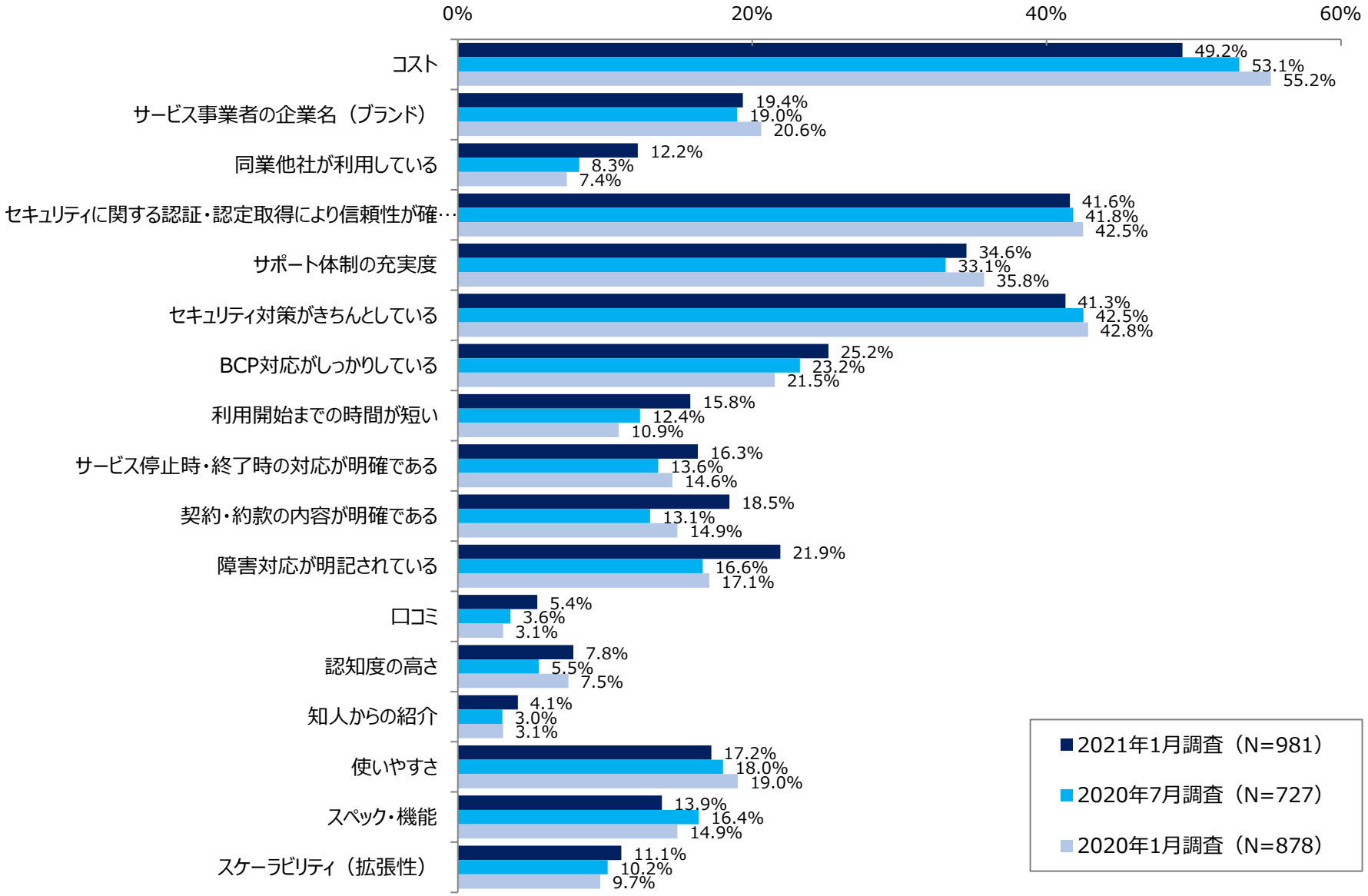


# Q13_3：クラウドサービスを選定する際のポイント（2021年調査）

■ クラウドサービス選定時のポイントの1位はコストで、信頼性の確保とセキュリティ対策が続いている。



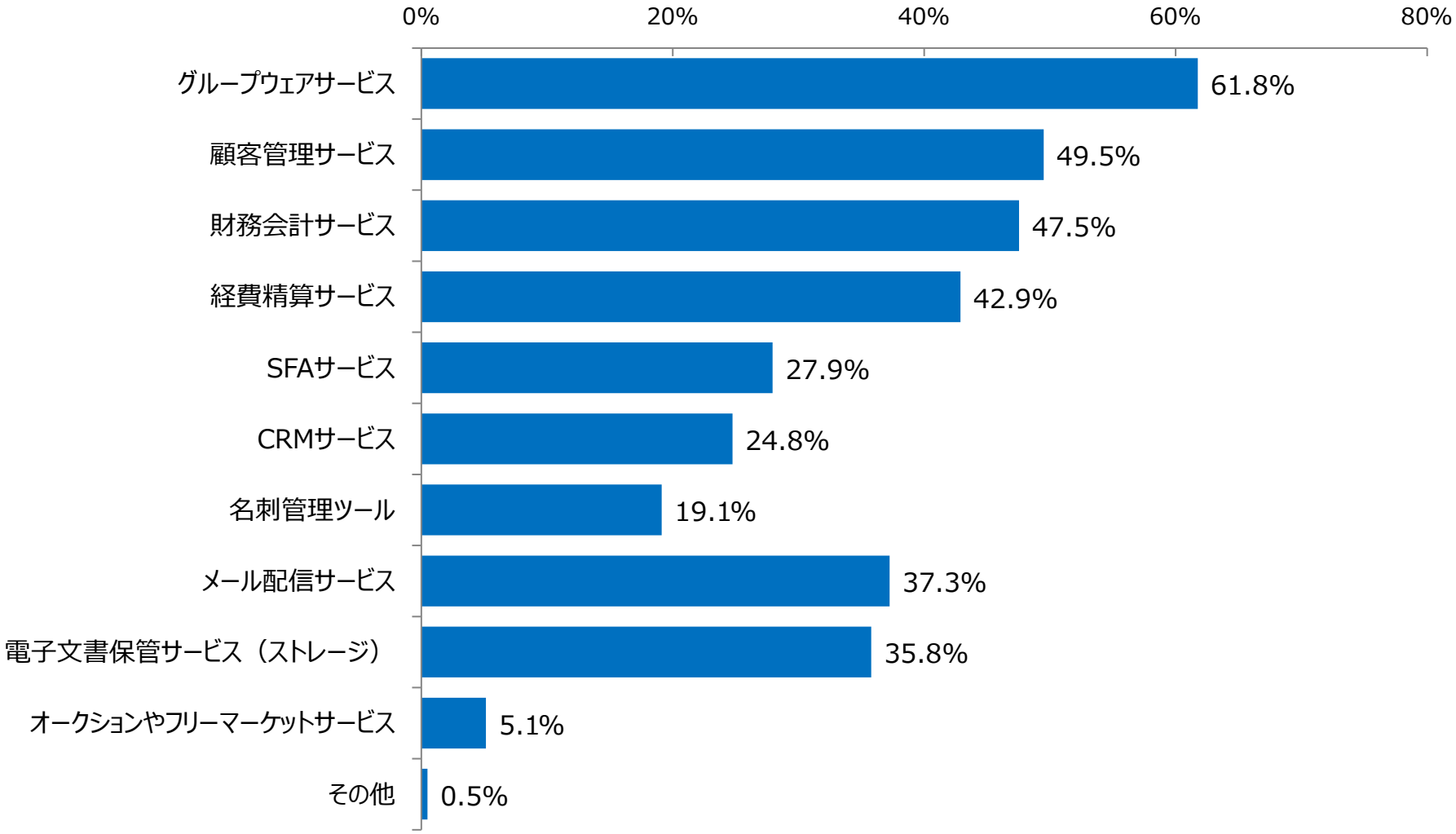
# Q13_3：クラウドサービスを選定する際のポイント（2020~2021年比較）



# Q13_4：信頼性を重視して選ぶクラウドサービス（2021年調査）

（対象：Q13_3で「セキュリティに関する認証・認定取得により信頼性が確保されている」を回答）

■ 信頼性重視で選ばれるクラウドサービスとして、グループウェアがNo.1で、顧客管理サービス、財務管理サービスが続いている。



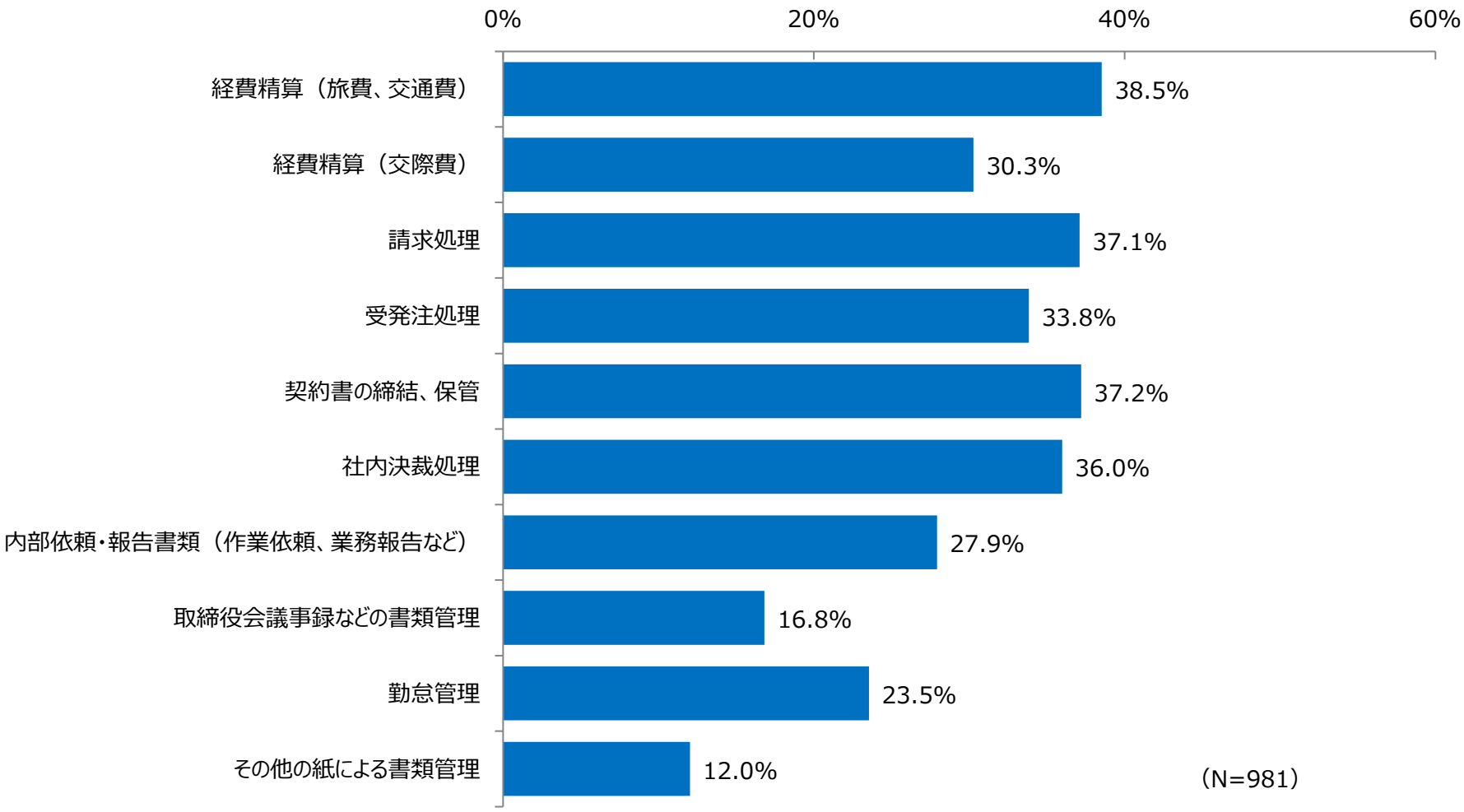

（N=408）

# 7）電子署名／電子契約など

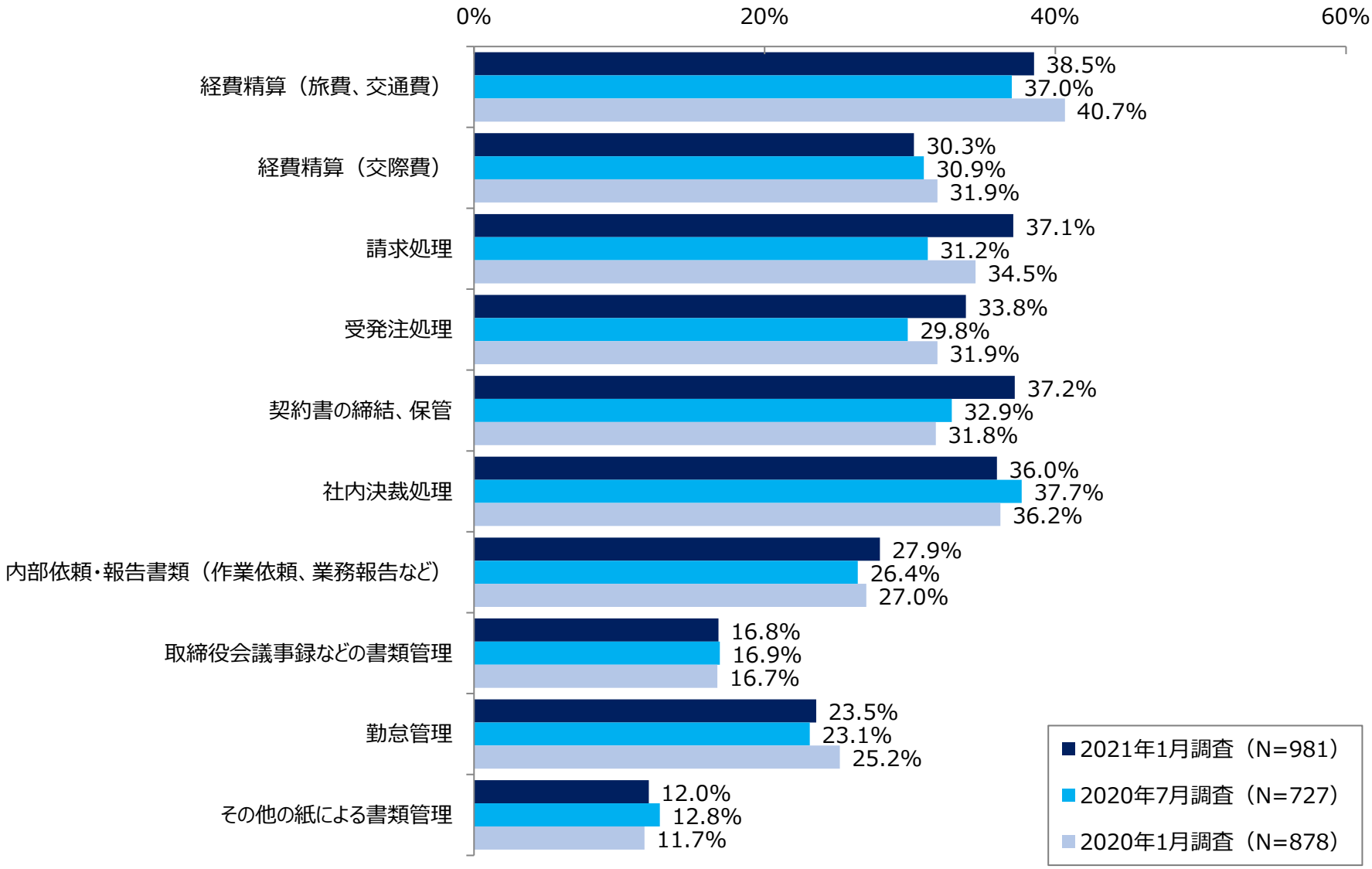
- Q14：電子署名／電子契約
- Q15：自社WebサイトSSL化
- Q16：情報セキュリティ監査

# Q14_1：特に電子化したい業務プロセス（2021年調査）

■ 電子化したいと回答が最も多かったのは、「経費精算（旅費・交通費）」で、前回は低かった「契約書の締結・保管」が伸びて２位になった。

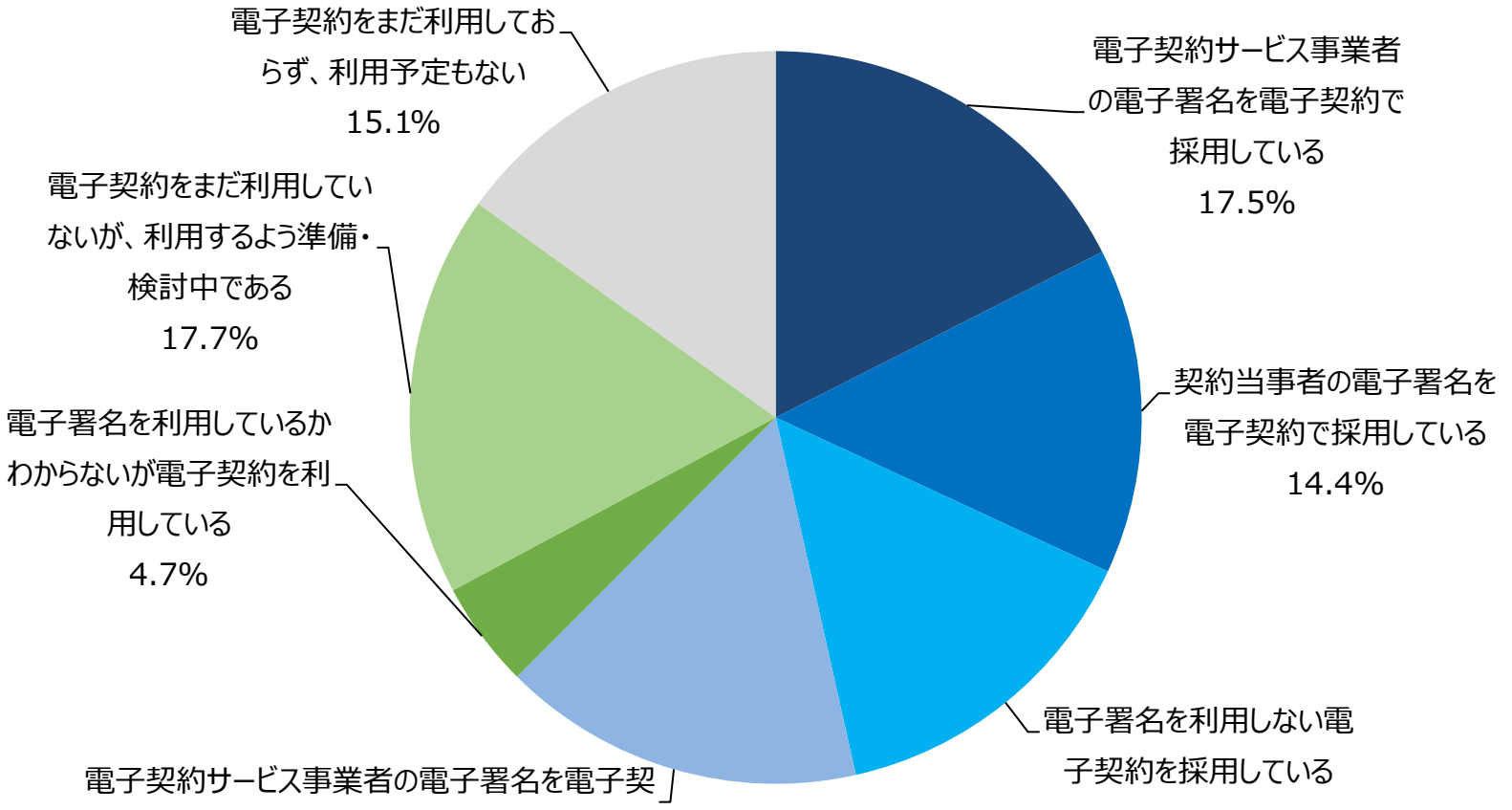


# Q14_1：特に電子化したい業務プロセス（2020~2021年比較）



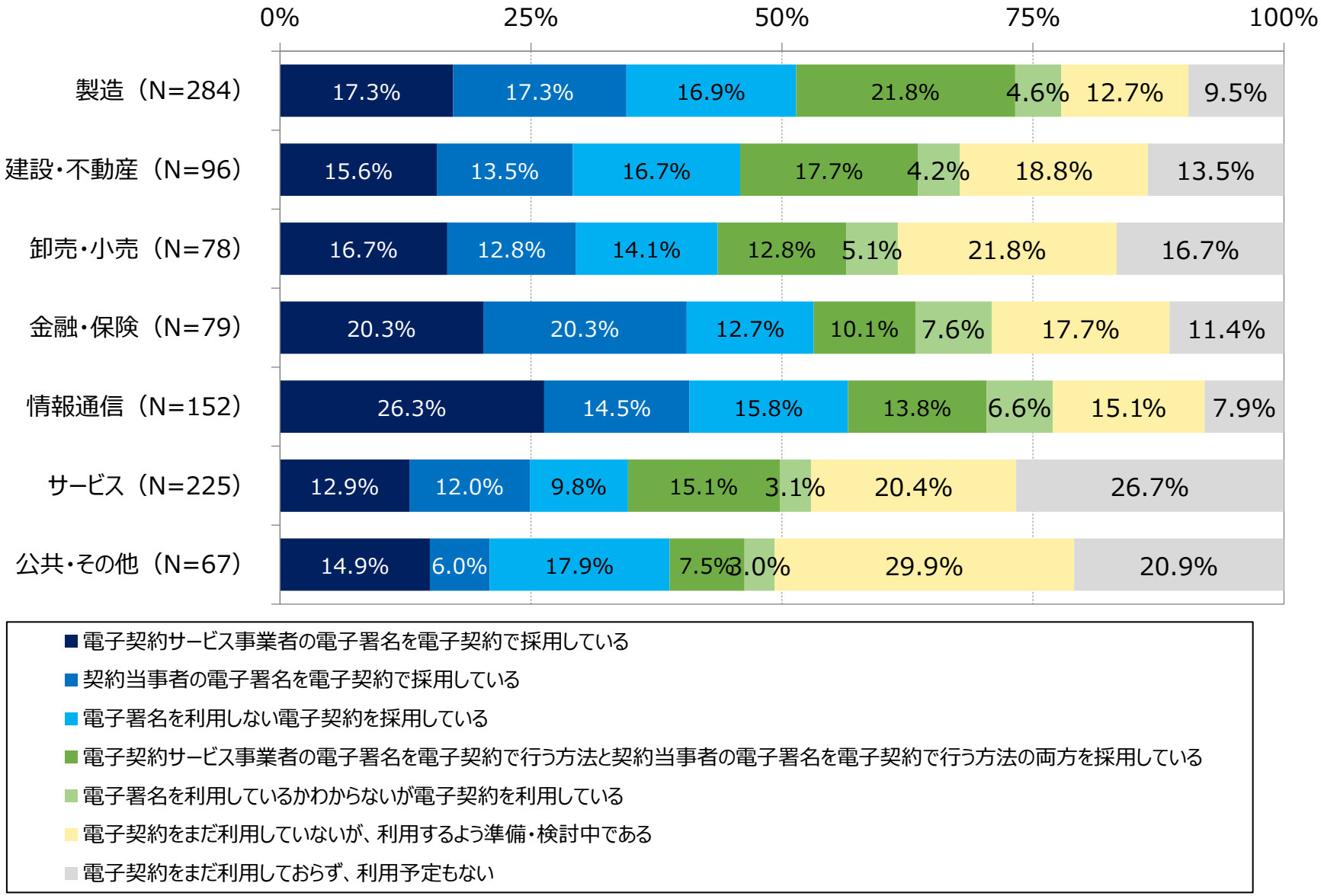
# Q14_2：電子契約の利用状況（2021年調査）

■ コロナ禍の勤務上形態の変化に対応し、電子契約を利用している比率は合計で約７割となっており、前回の約４割から大幅に増加している。

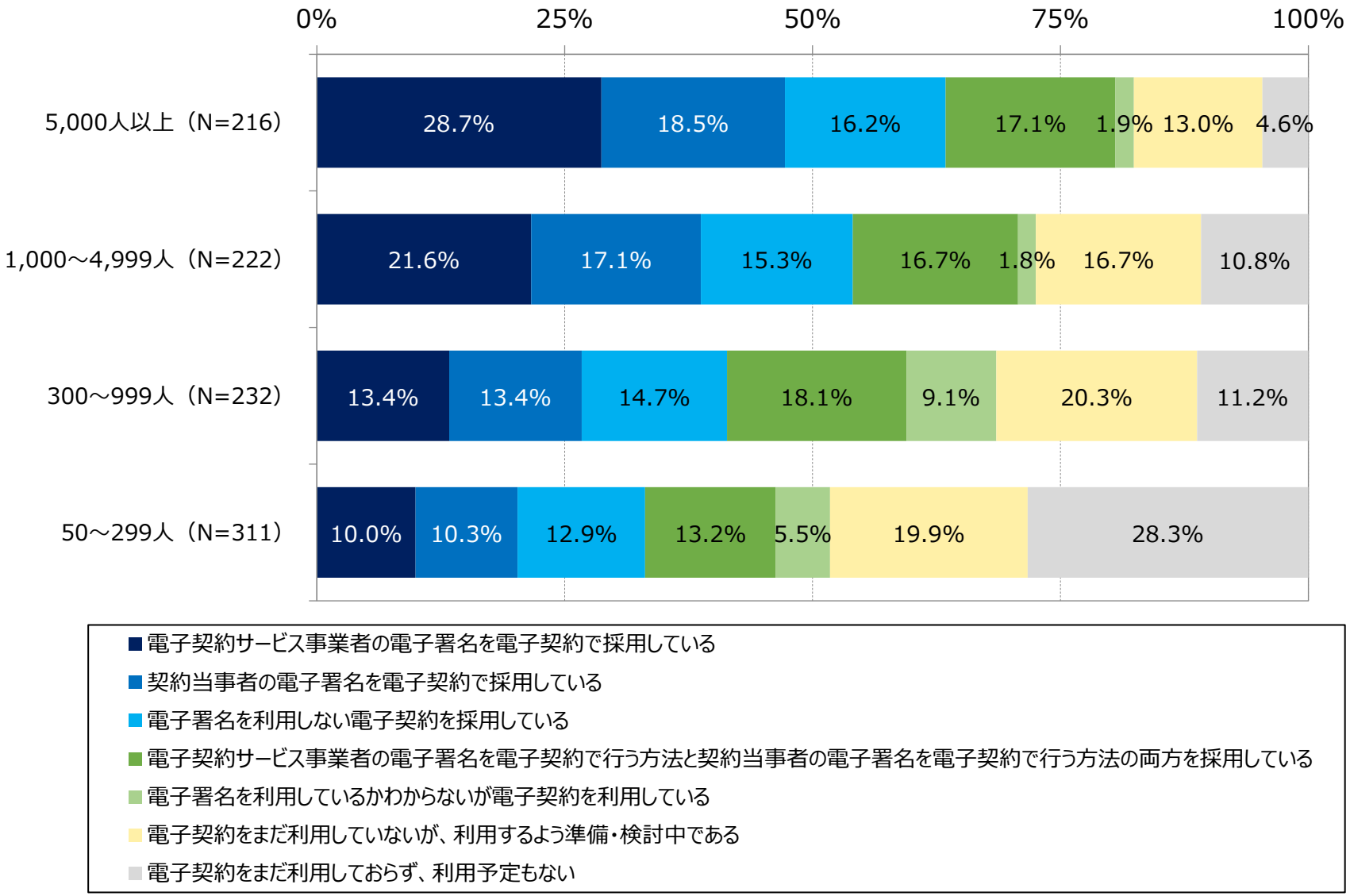



（N=981）

# Q14_2：電子契約の利用状況［業種別］（2021年調査）

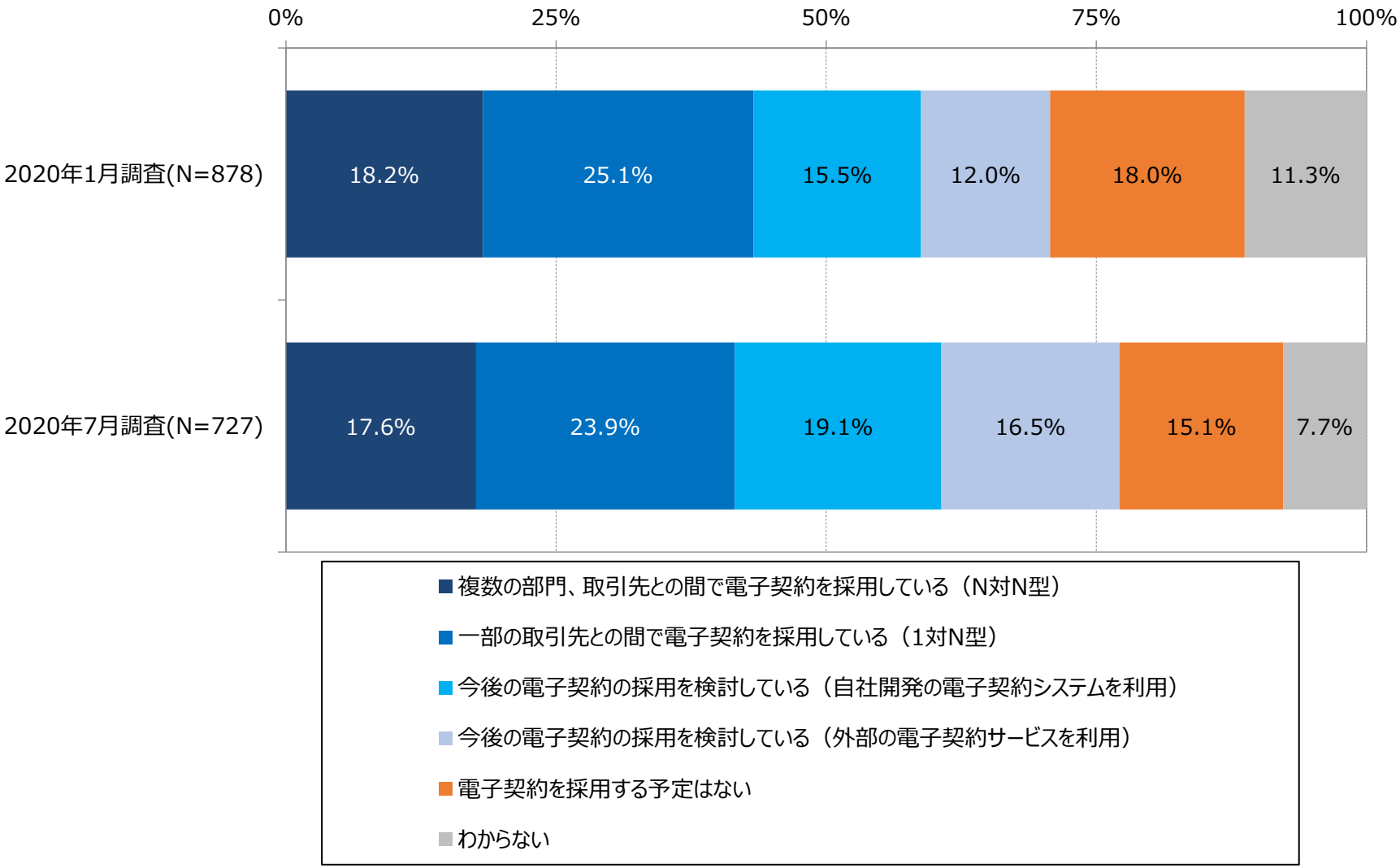


# Q14_2：電子契約の利用状況［従業員規模別］（2021年調査）



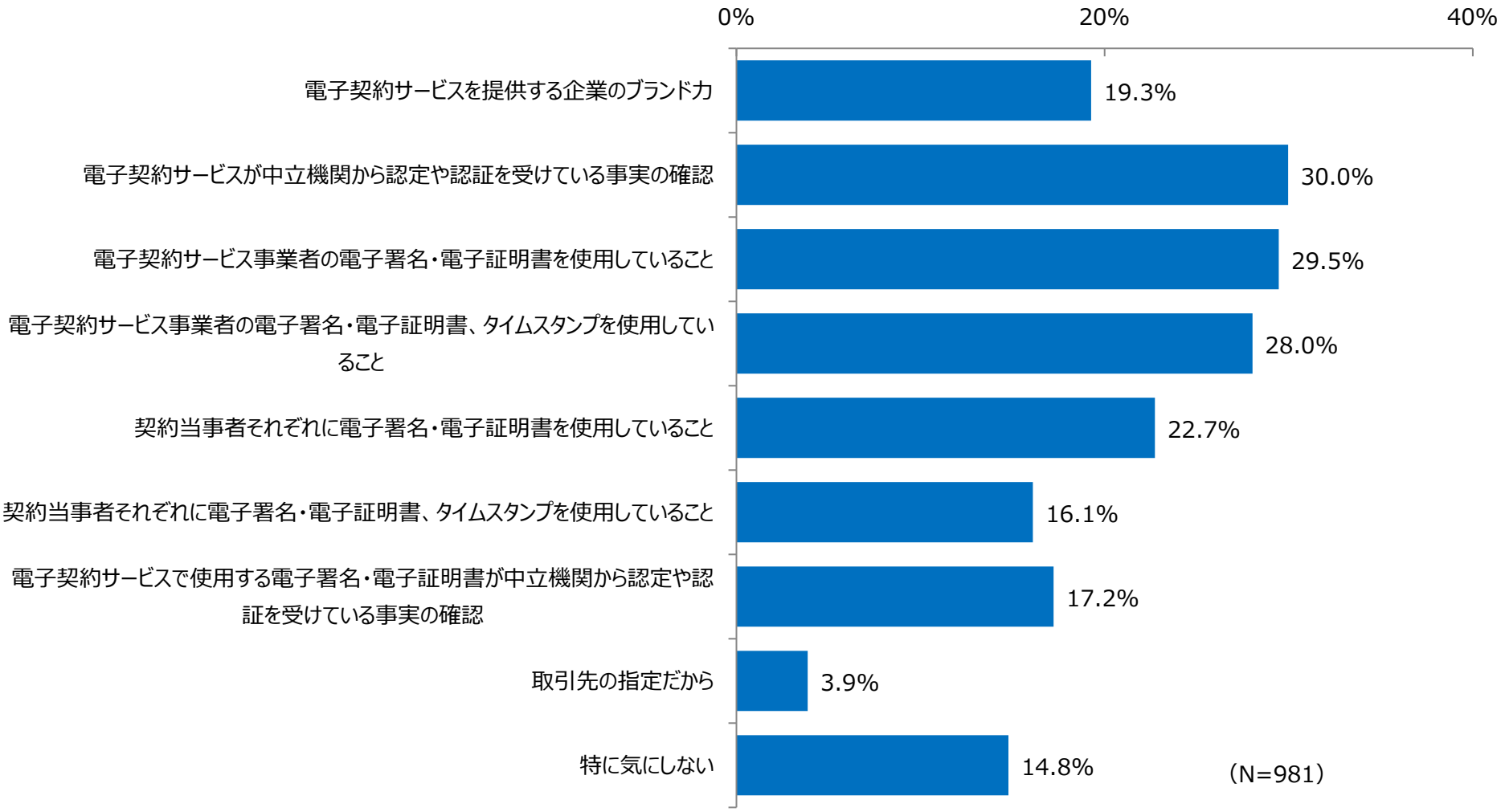
# 参考）電子契約の利用状況（2020年１月と７月の比較）

※本質問では、電子署名利用の有無は区別していない。



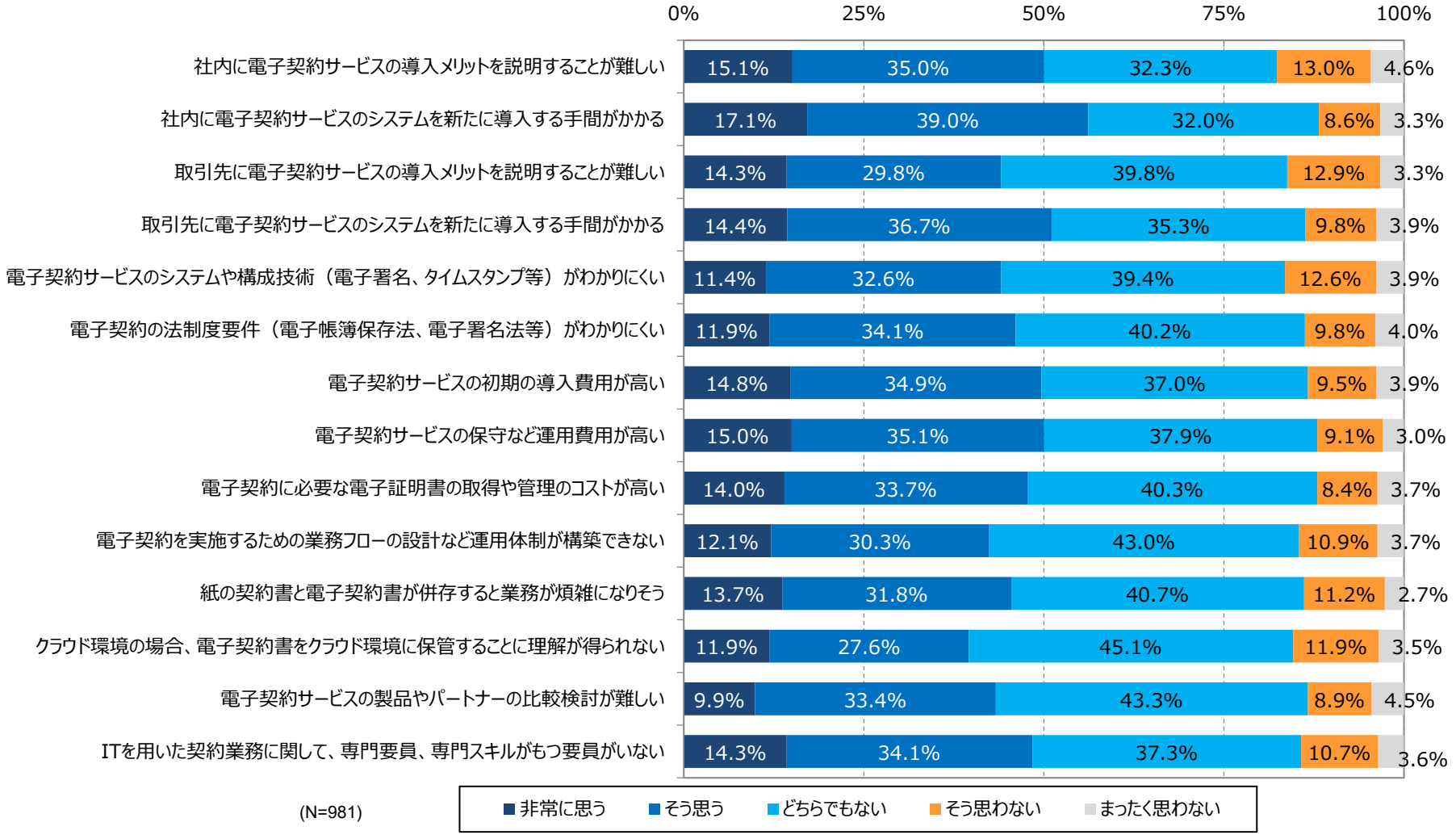
# Q14_3：電子契約が安全だと判断する基準（2021年調査）

■ 電子契約が安全だと判断する基準としては認定・認証を受けていること、または電子署名・電子証明書を使用していることが挙げられ、第三者による認証・証明が根拠となっている。

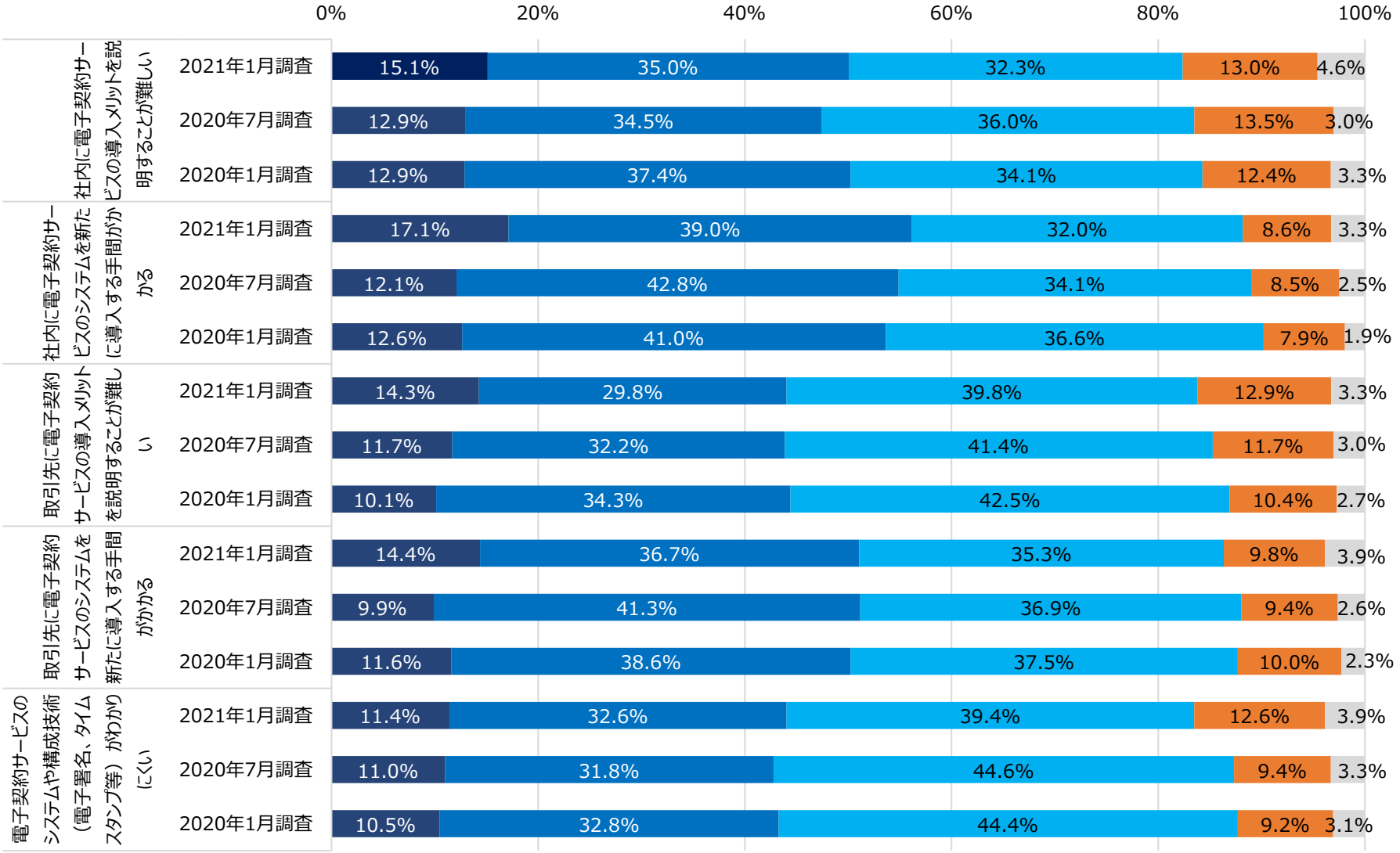


# Q14_4：電子契約を採用または利用拡大するための課題（2021年調査）

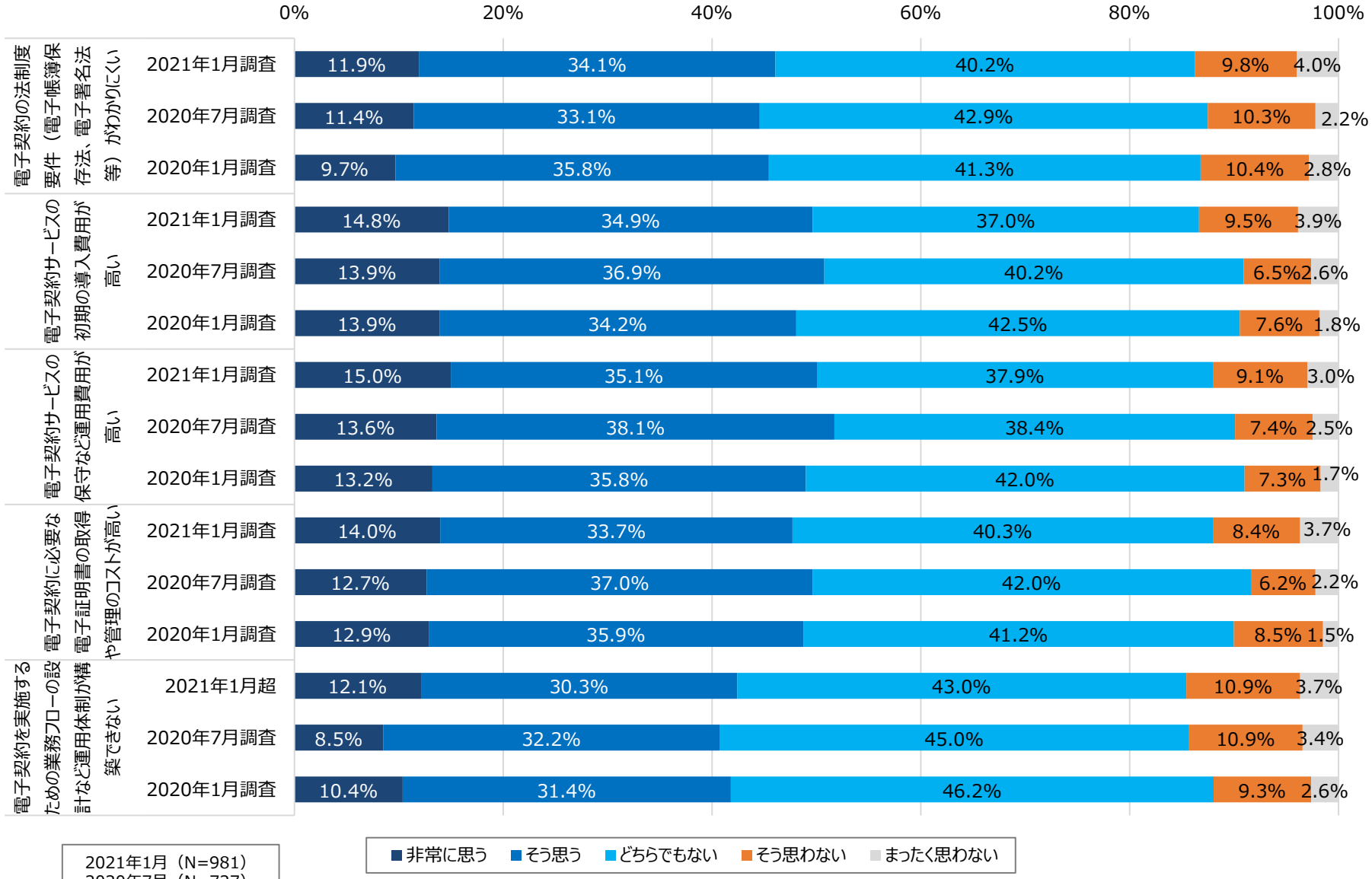
■ 課題として、“非常に思う”と“そう思う”の合計が多いのは「社内または取引先に新たに導入する手間がかかる」で、その次は「導入費用または運用費用が高い」が挙げられている。



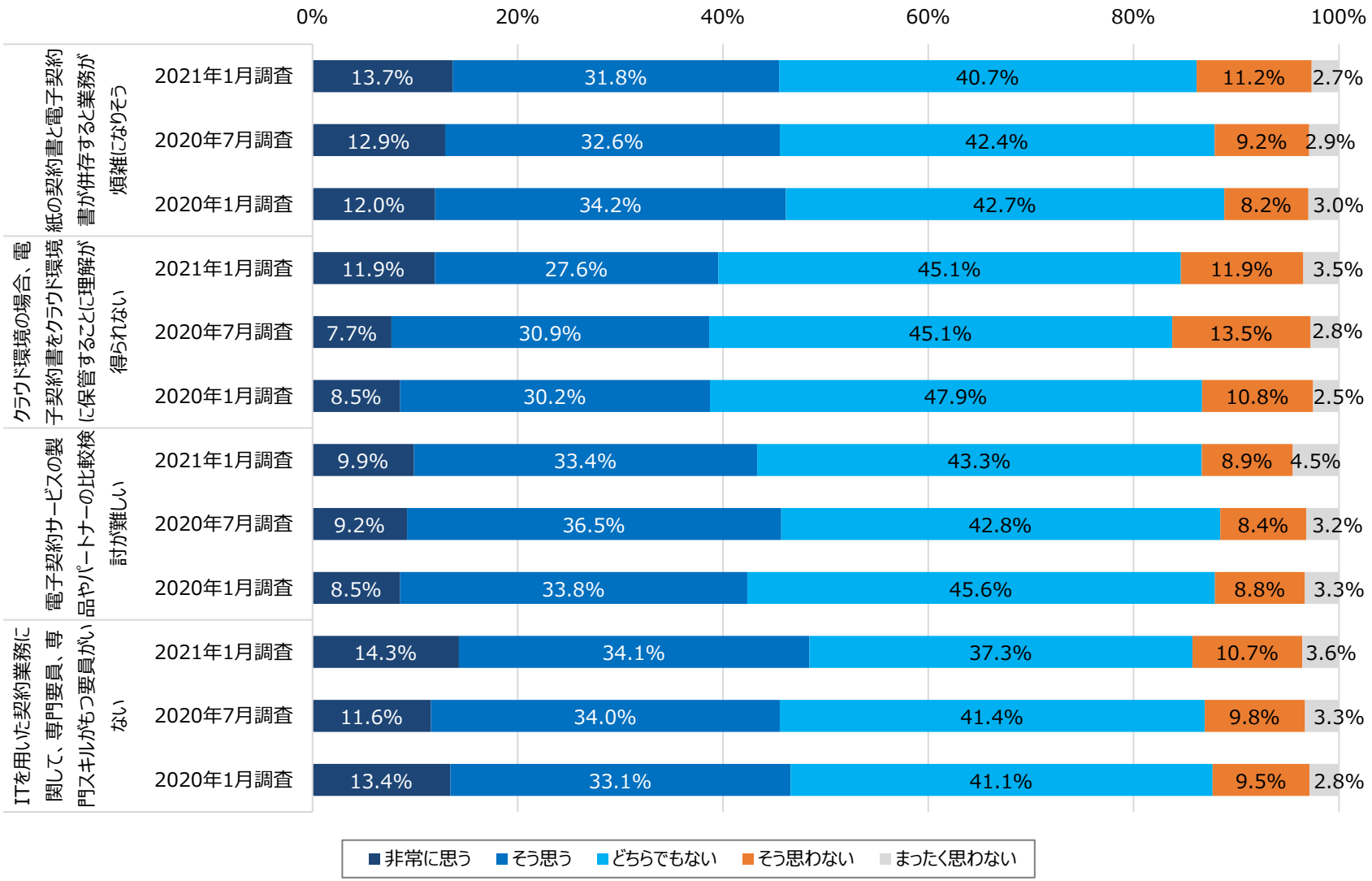
# Q14_4：電子契約を採用または利用拡大するための課題-1（2020~2021年比較）



# Q14_4：電子契約を採用または利用拡大するための課題-2（2020~2021年比較）



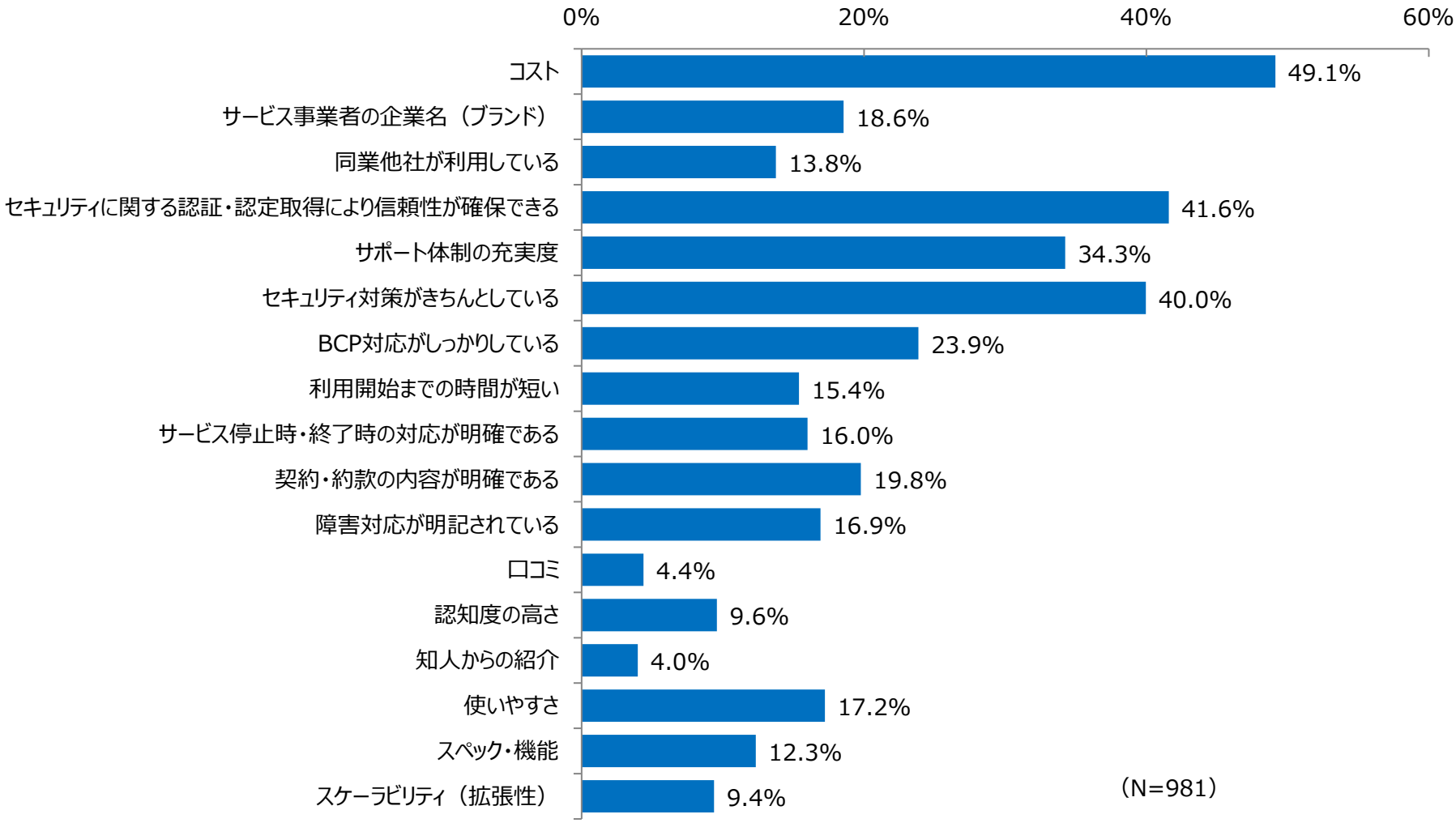
# Q14_4：電子契約を採用または利用拡大するための課題-3（2020~2021年比較）




2021年1月（N=981）
2020年7月（N=727）
2020年1月（N=878）

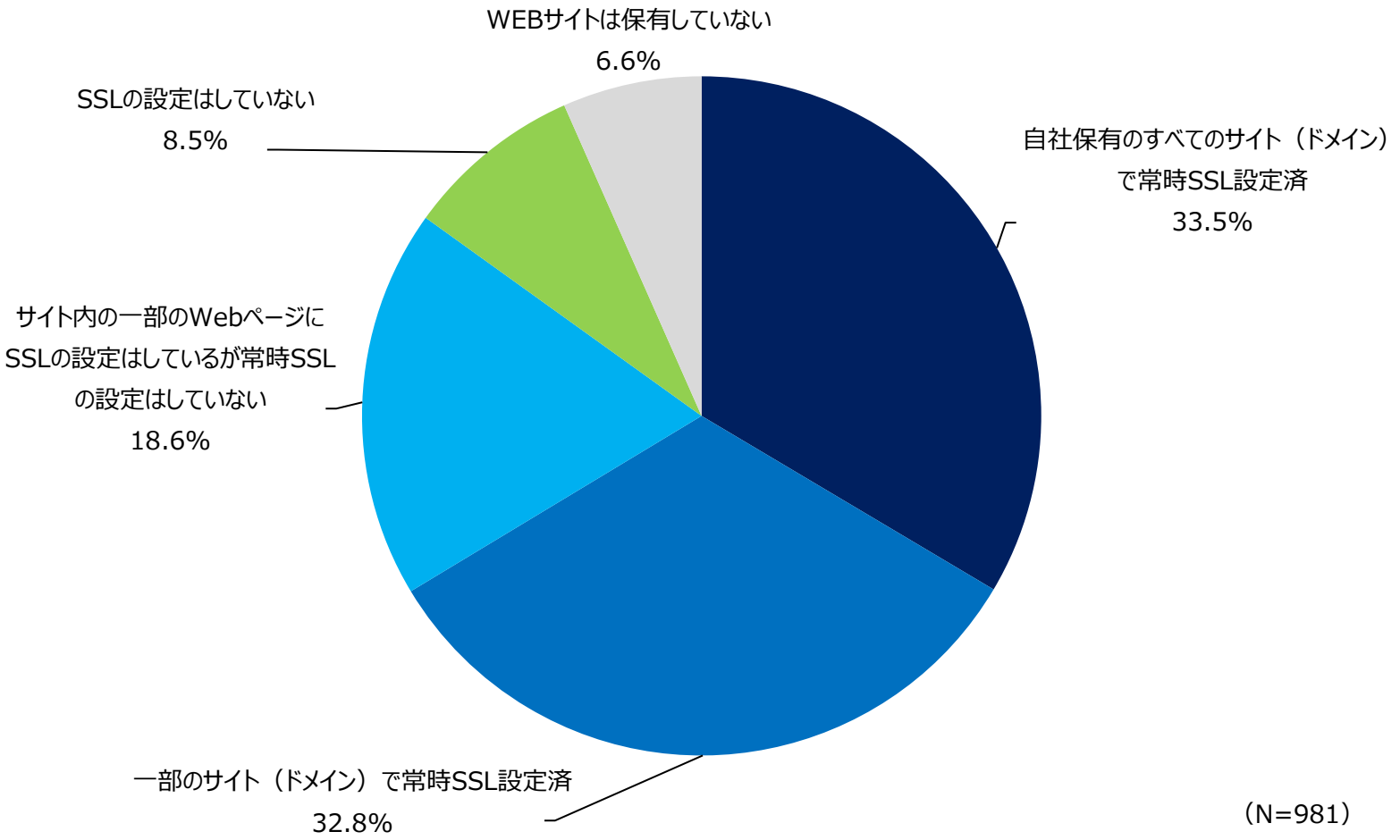
# Q14_5：電子契約の選定のポイント（2021年調査）

■ 選定のポイントで高いのは、コストがトップで、次は認証・認定による信頼性、セキュリティ対策の順となっている。



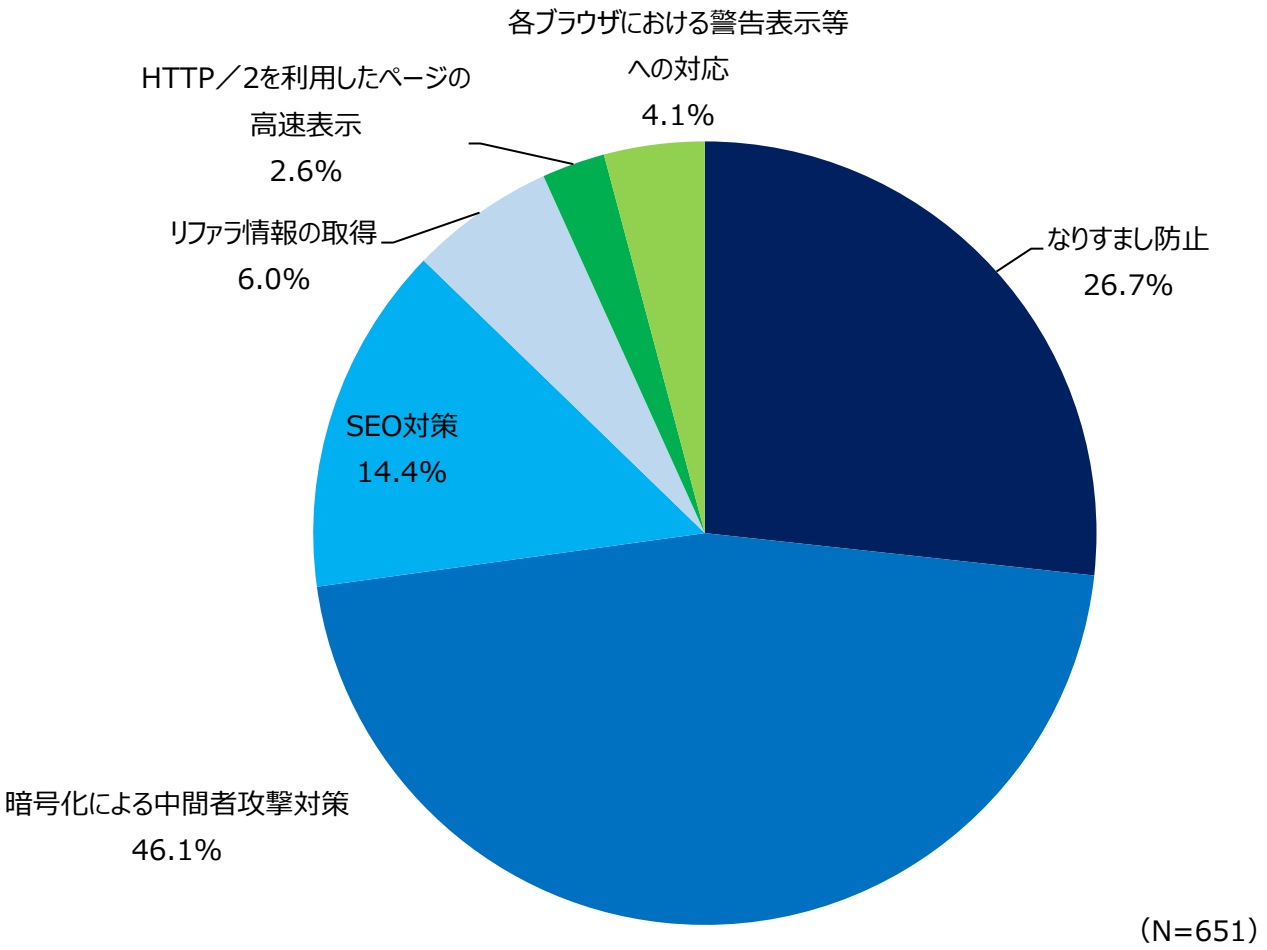
# Q15_1：自社WebサイトのSSL化対応状況（2021年調査）

■ 8割以上で何らかのSSL化を行っており、前回とほぼ同じ結果となっている。



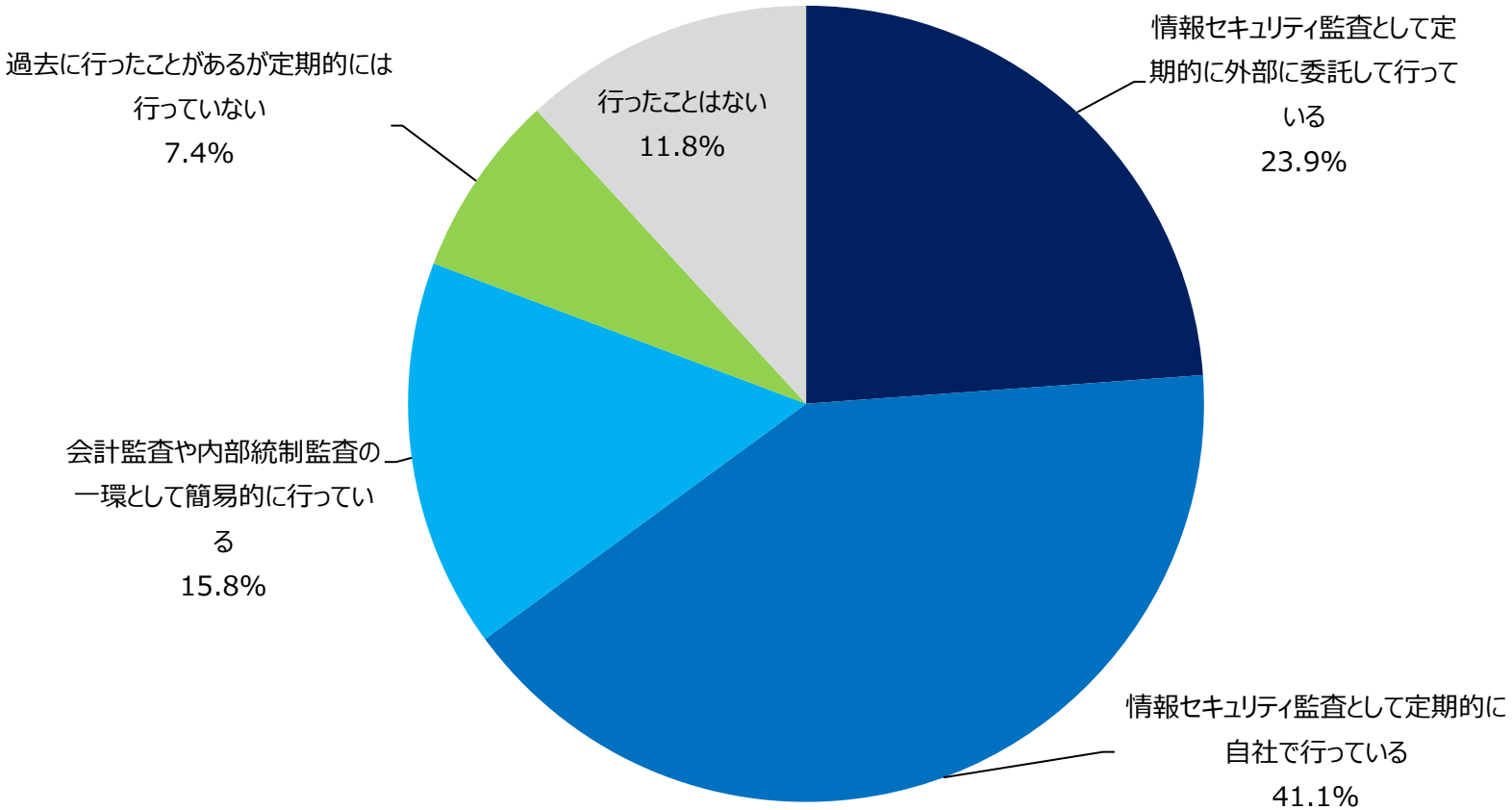
# Q15_2：自社Webサイトの常時SSL化の理由（2021年調査）

■ 常時SSL化の理由としては、中間者攻撃対策が1位となり、なりすまし防止が続き、前回と同様の結果となっている。



# Q16：情報セキュリティ監査の実施状況（2021年調査）

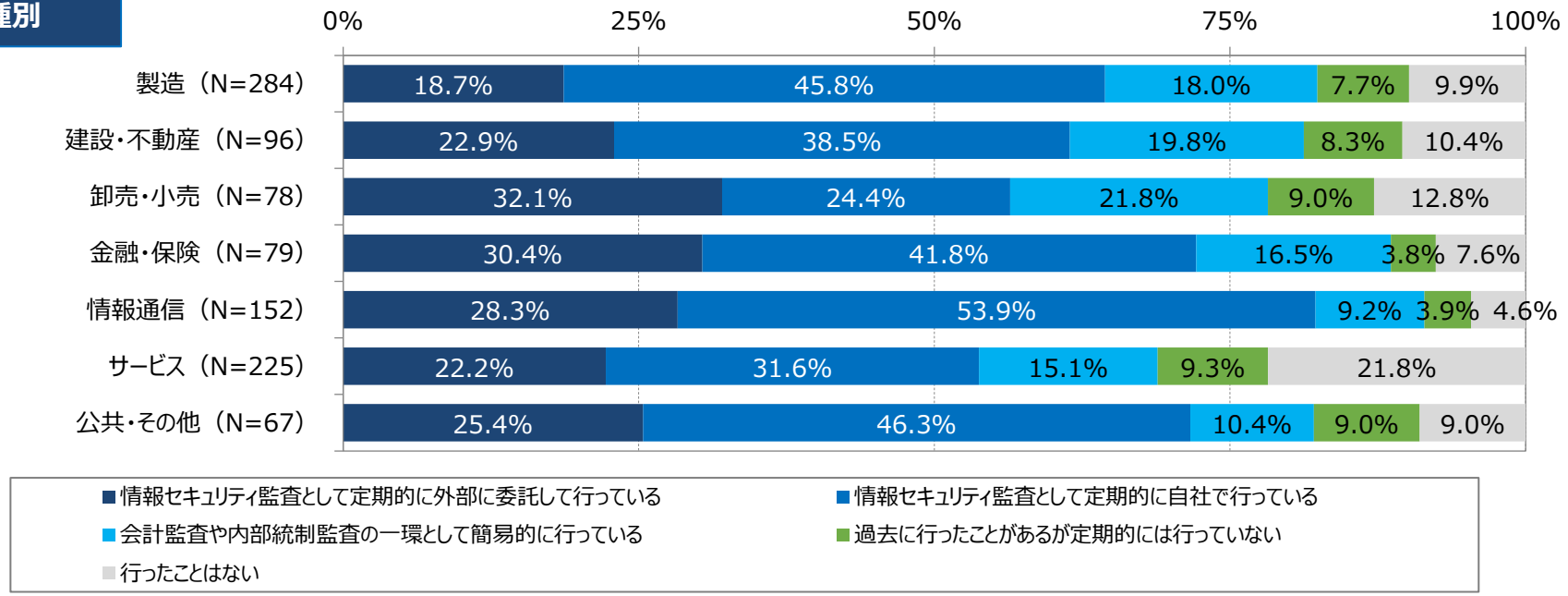
■ 不定期の実施を含め実施したことがあるが約９割となっており、前回と同様の結果となっている。



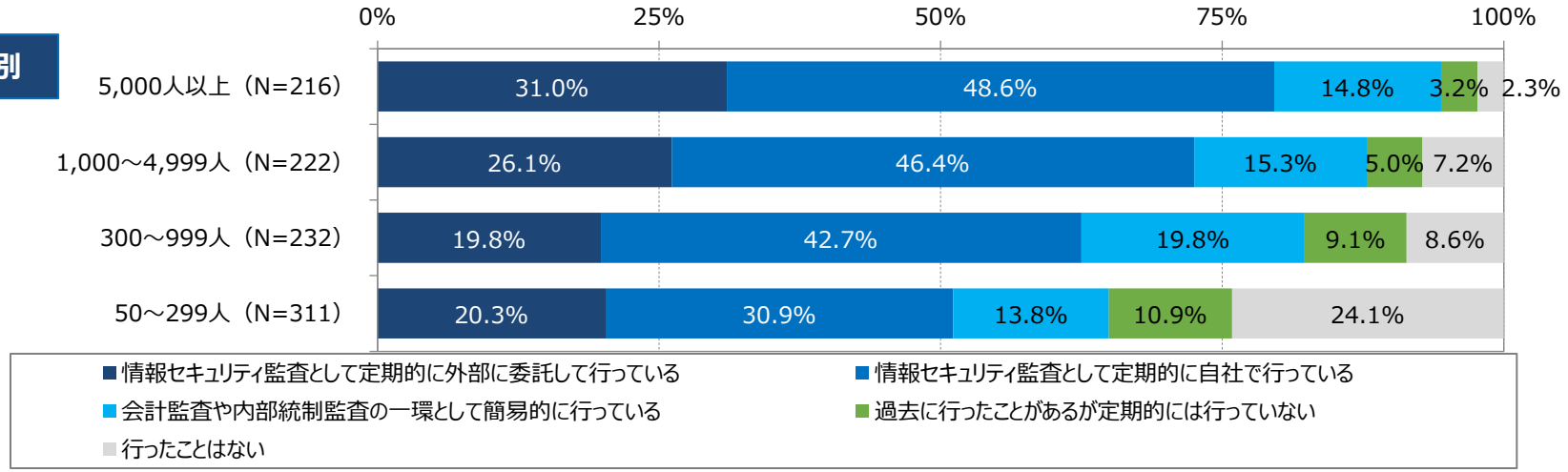

（N=981）

# Q16：情報セキュリティ監査の実施状況［業種別／従業員規模別］（2021年調査）

**業種別**




**従業員規模別**



# 総括

コロナ禍に対応して企業がテレワークによる勤務形態へ移行したことにより、テレワークを前提とした事業環境への対応とシステム面・セキュリティ面での対応が経営課題となっている。

情報セキュリティ関連の製品・サービスの適用状況については、コロナ禍に対応したクラウド化の進行により、従来のオンプレ環境用の製品・サービスからクラウド環境用のサービスへの移行が見られる。

働き方改革についても、コロナ禍に対応してテレワークへ勤務形態が大きく変わり、テレワークに適合した制度の整備やシステム・セキュリティ面の整備が一気に進んだ。

コロナ禍に対応したテレワーク化でクラウド利用が進み、電子契約が大きく伸びており、今後もテレワーク環境を前提としたサービスに置き換わっていくと思われる。情報セキュリティ監査についてはかなり普及しており、今後もこの傾向が続くと思われる。