

「企業IT利活用動向調査2020」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2020年1月に実施した「企業IT利活用動向調査2020」の集計結果をまとめたものです。

2020年6月



一般財団法人日本情報経済社会推進協会

禁無断転載

引用・転載にあたっては、以下のフォームから申請をお願いします。

[引用・転載お申込み受付けフォーム](#)

「企業IT利活用動向調査2020」調査概要

実査期間 : 2020年1月14日～1月20日

実施主体 : 一般財団法人日本情報経済社会推進協会
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

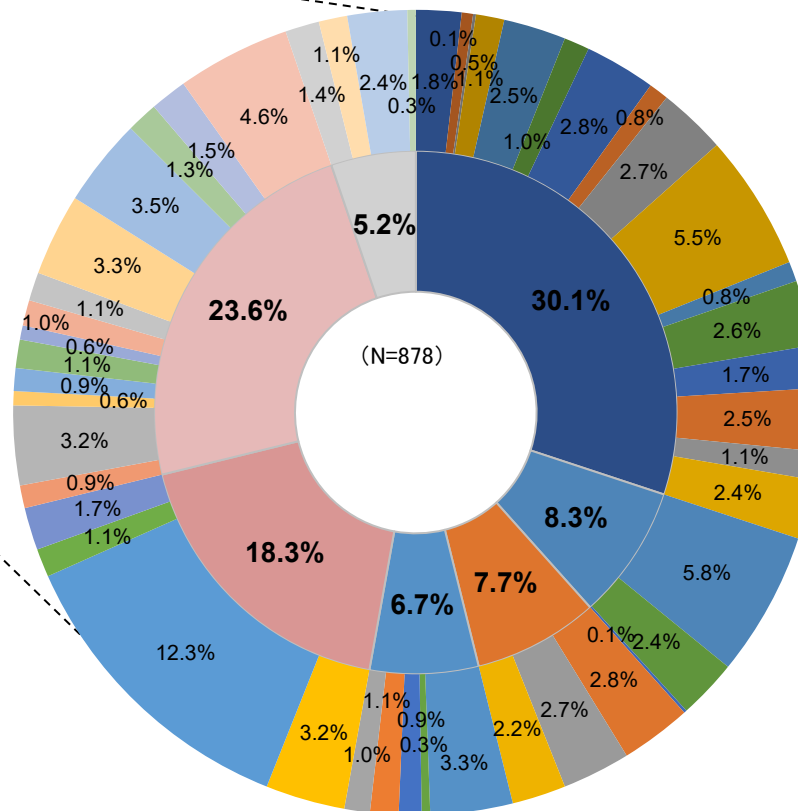
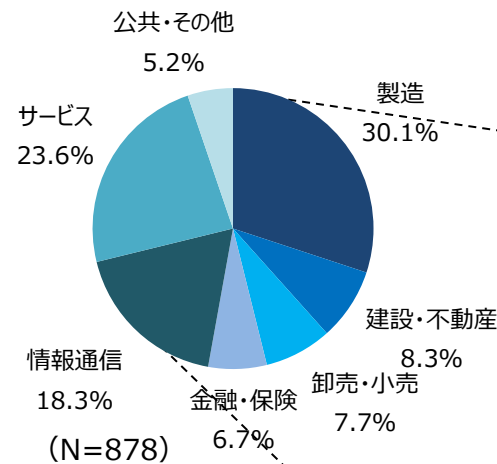
調査対象 : 以下の条件を満たす個人 : **約5,000人**

- 従業員数50人以上の国内企業の勤務者であること
- 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
- 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
- **係長相当職以上**の役職者であること

有効回答数 : 878件（1社1人）

2020年調査：回答者プロフィール①

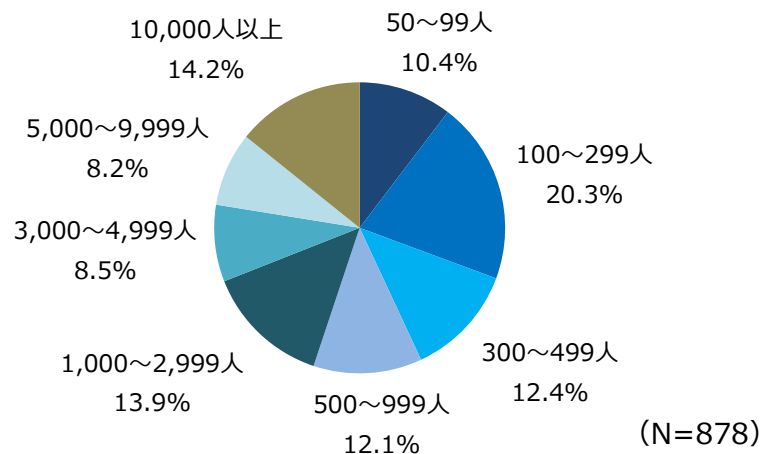
勤務先の業種



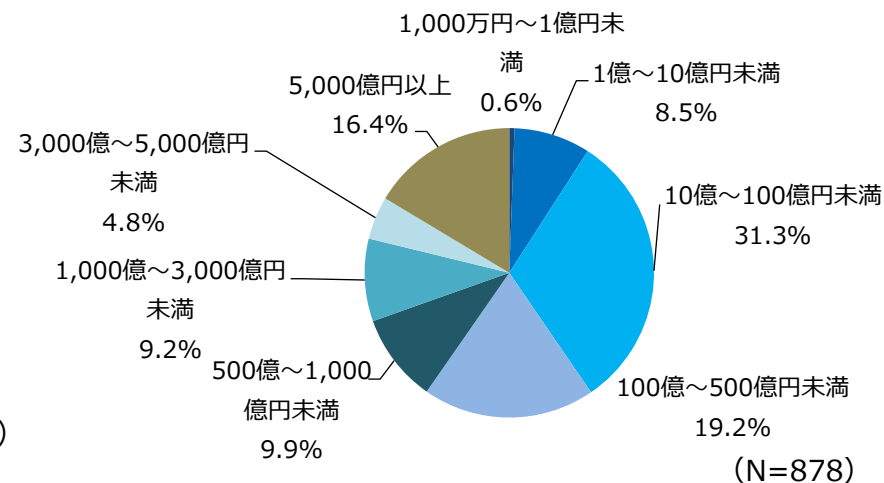
- 食品・飲料
- 日用品・生活雑貨
- 繊維
- パルプ・紙・印刷
- 化学工業
- 石油製品
- 鉄鋼・金属
- プラスチック・ゴム
- 機械
- 電気機器
- 情報通信機器
- 電子部品・電子回路
- 精密機器
- 自動車・輸送機器
- 医薬品
- その他の製造業
- 建設
- 不動産
- 住宅
- 卸売
- 小売
- 商社
- 銀行
- 証券
- 生命保険
- 損害保険
- その他金融
- 通信
- ITベンダー／システムインテグレーター
- インターネット・サービス
- 情報システム子会社
- 電力・ガス・水道
- 運輸
- 倉庫
- 宿泊
- 飲食
- 娯楽・レジャー
- メディア・出版・放送・広告
- 生活関連サービス(旅行業など)

2020年調査：回答者プロフィール②

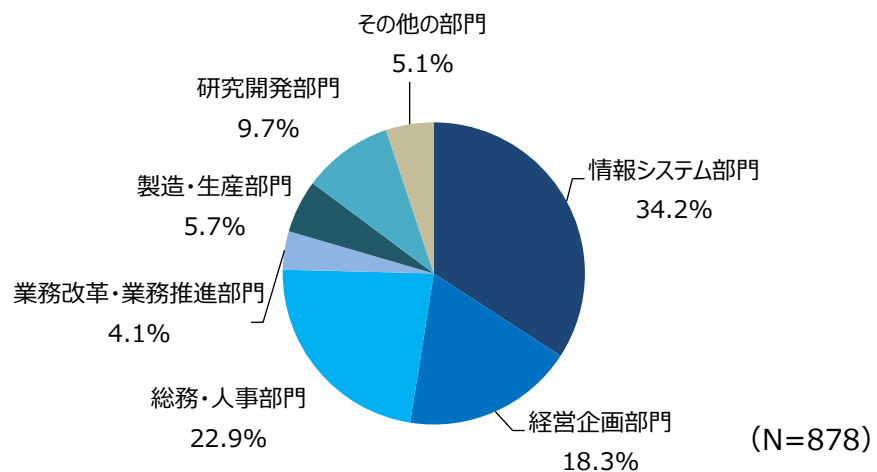
勤務先の従業員規模



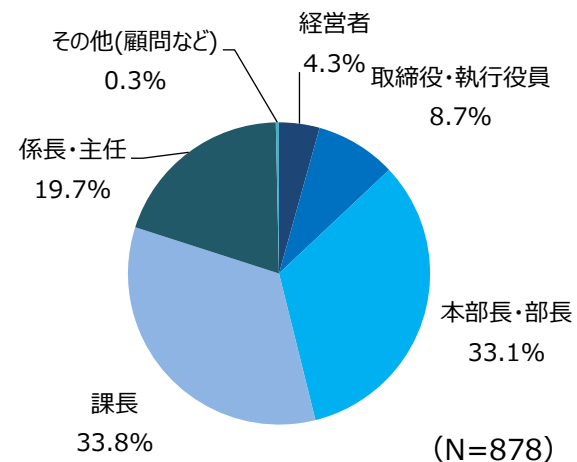
勤務先の売上規模



所属部門

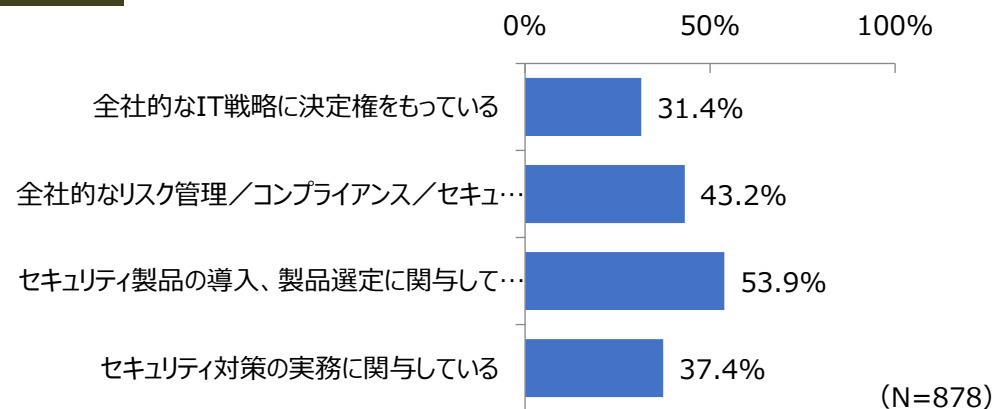


役職

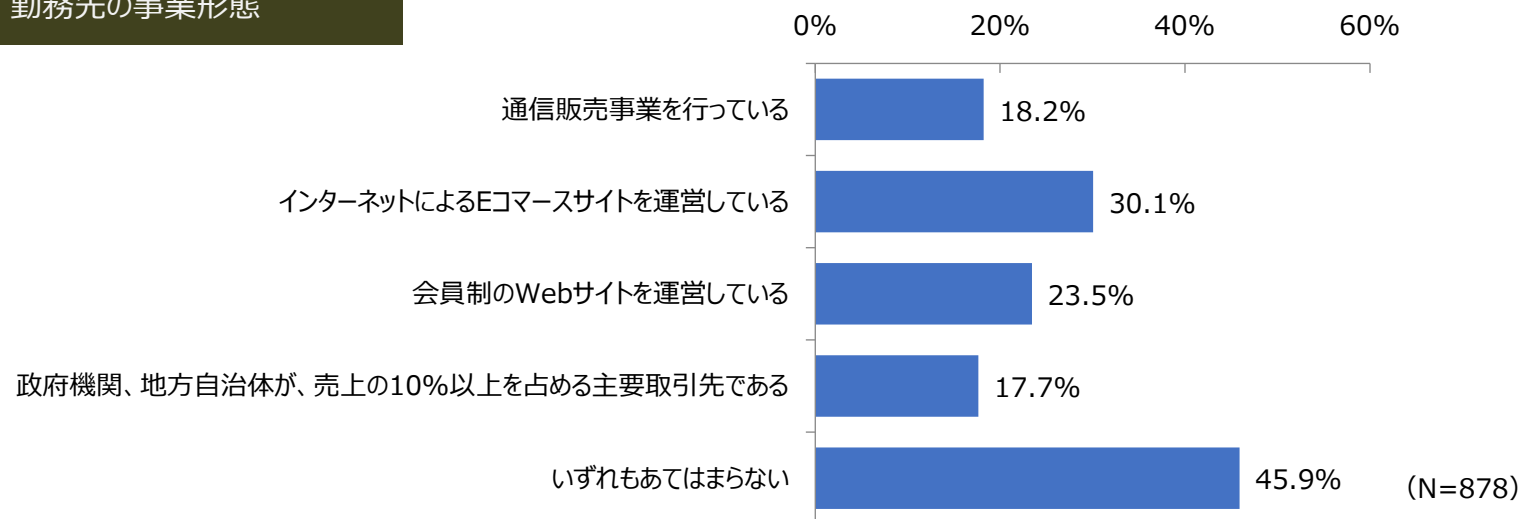


2020年調査：回答者プロフィール③

IT戦略/セキュリティへの関与度

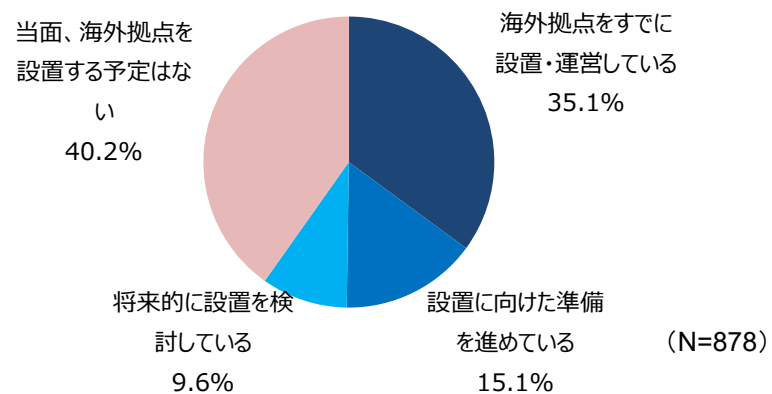


勤務先の事業形態

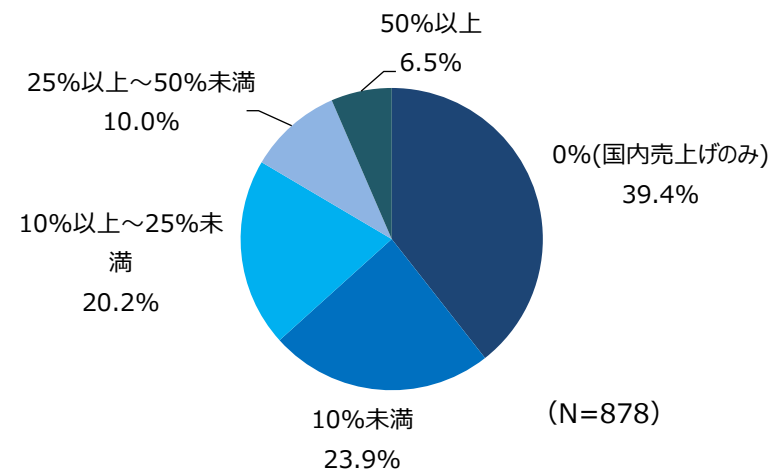


2020年調査：回答者プロフィール④

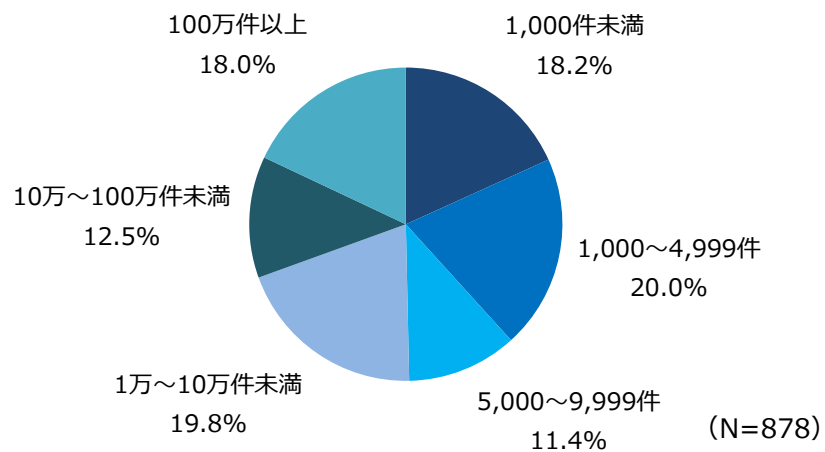
海外拠点の設置状況



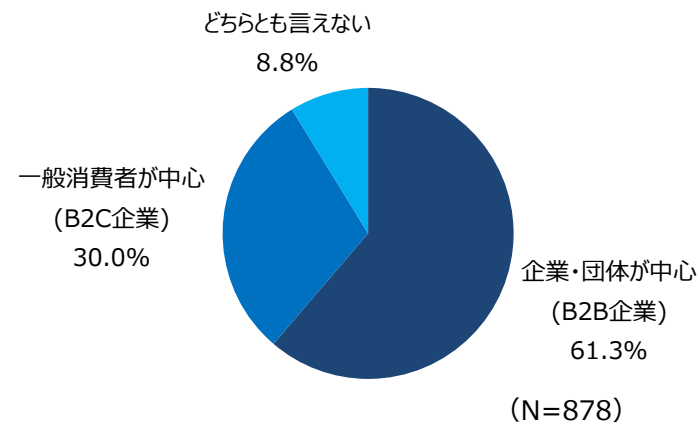
海外売上比率



個人情報保有件数



顧客・取引先のタイプ

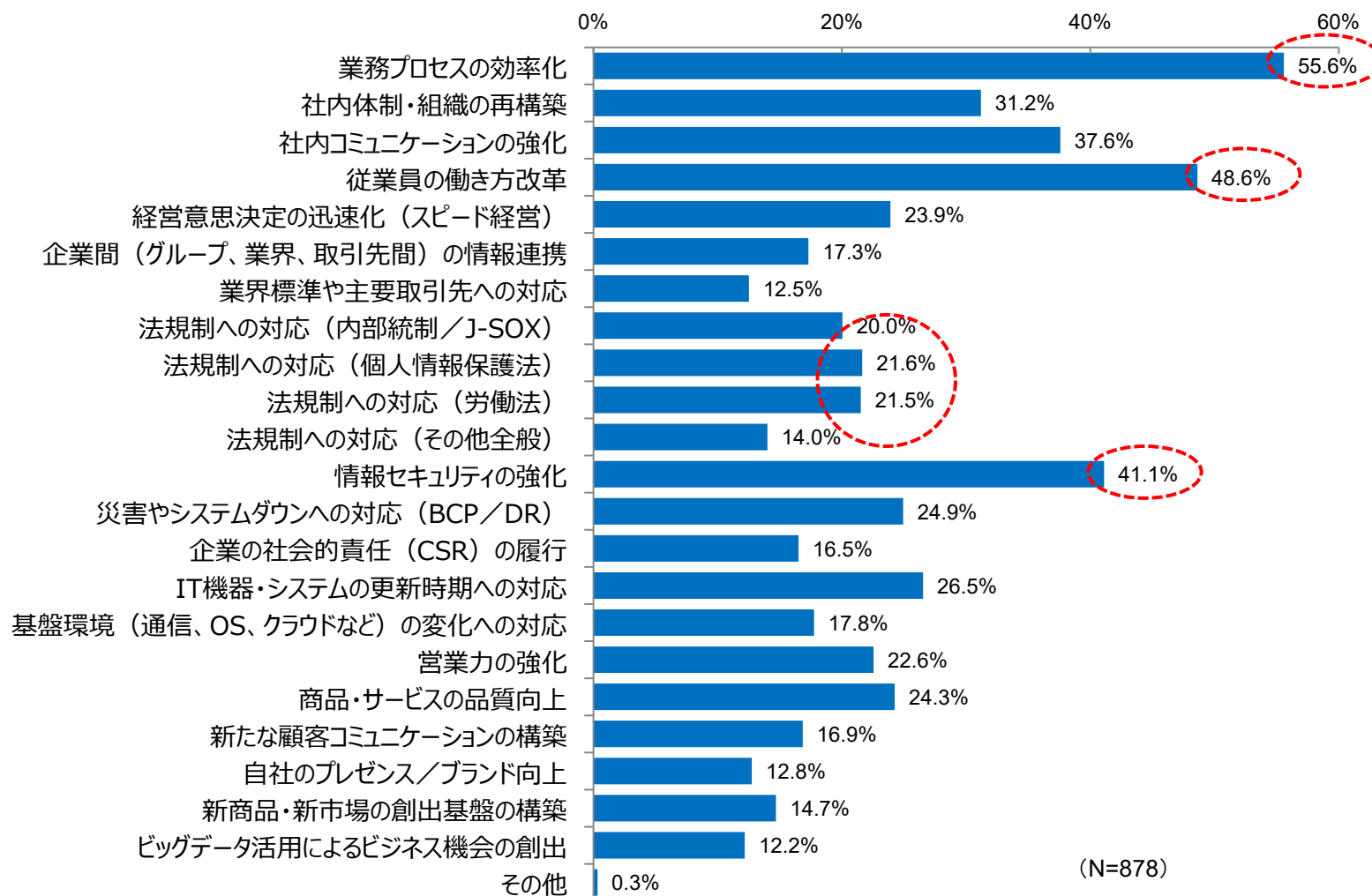


1) 経営課題におけるセキュリティの位置づけ

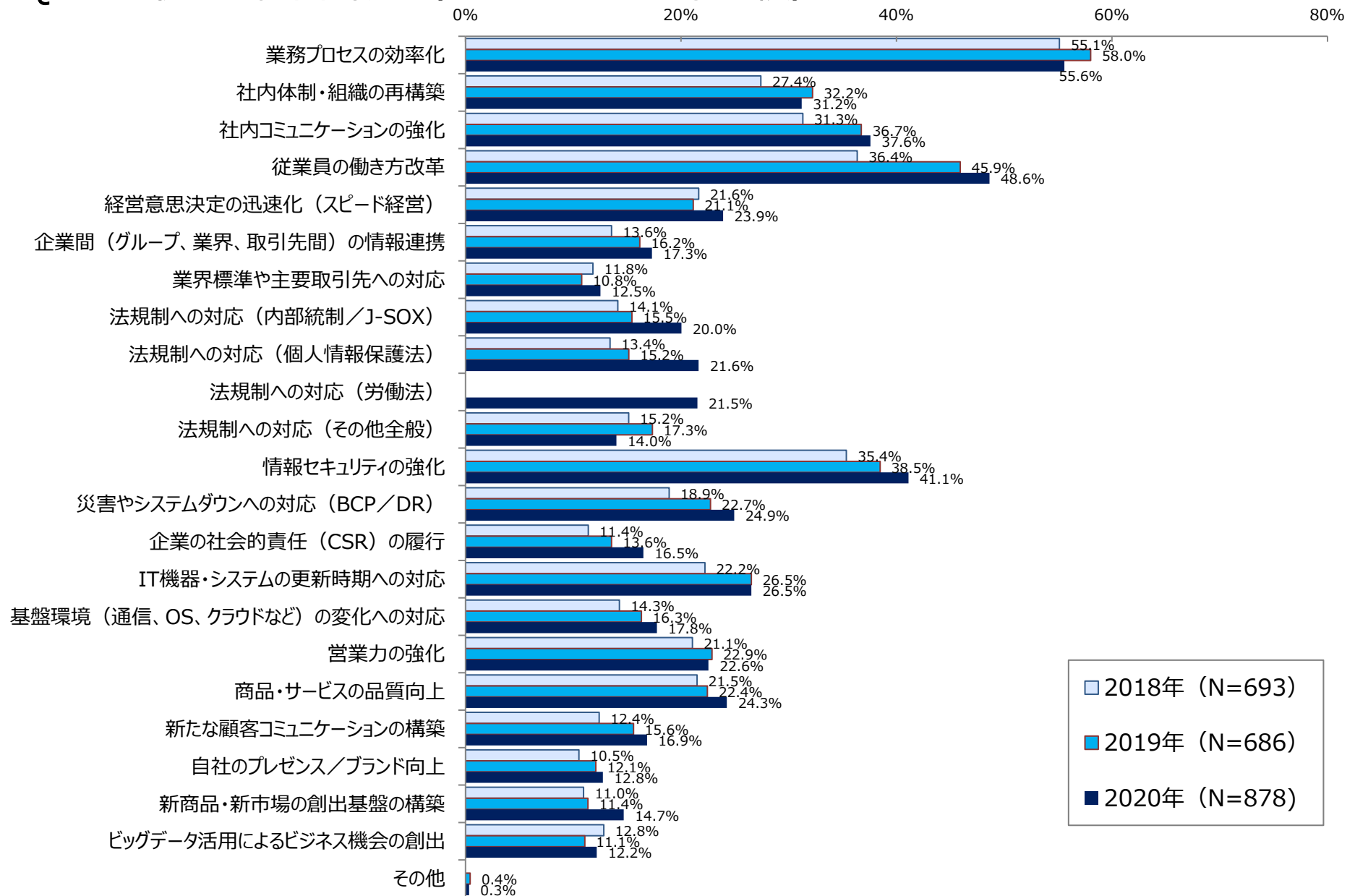
- Q1 : 重視する経営課題
- Q2 : セキュリティインシデントの認知状況
- Q3 : セキュリティリスクの重視度合い

Q1：重視する経営課題

- 「業務プロセスの効率化」が最も高いが昨年よりも比率は低下しており、代わりに「従業員の働き方改革」、「情報セキュリティの強化」が昨年よりも伸びており、差が縮まっている。
- また法規制への対応（3項目）が軒並み伸びている。



Q1：重視する経営課題（2018～2020年比較）



Q1：重視する経営課題（業種別）

- 「業務プロセスの効率化」は全業種で高い数値となっているが卸売・小売は昨年から大幅に減少（75.0%→47.1%）
- 「従業員の働き方改革」は建設不動産、サービス、公共・その他で伸びる一方、卸売・小売で減少し、業種間の格差が縮まっている。
- 「情報セキュリティ強化」は、金融・保険で伸びている。

	製造 (N=264)	建設・不動産 (N=73)	卸売・小売 (N=68)	金融・保険 (N=59)	情報通信 (N=161)	サービス (N=207)	公共・その他 (N=46)	全体 (N=878)
業務プロセスの効率化	59.1%	61.6%	47.1%	74.6%	53.4%	49.3%	50.0%	55.6%
社内体制・組織の再構築	29.9%	35.6%	29.4%	35.6%	27.3%	34.8%	26.1%	31.2%
社内コミュニケーションの強化	39.8%	42.5%	41.2%	33.9%	39.1%	34.3%	26.1%	37.6%
従業員の働き方改革	48.1%	50.7%	48.5%	49.2%	42.9%	54.1%	43.5%	48.6%
経営意思決定の迅速化（スピード経営）	26.5%	30.1%	25.0%	37.3%	21.1%	18.4%	15.2%	23.9%
企業間（グループ、業界、取引先間）の情報連携	20.1%	17.8%	17.6%	20.3%	16.1%	14.5%	13.0%	17.3%
業界標準や主要取引先への対応	15.5%	15.1%	7.4%	16.9%	11.8%	10.6%	4.3%	12.5%
法規制への対応（内部統制／J-SOX）	23.1%	23.3%	19.1%	20.3%	16.8%	16.9%	23.9%	20.0%
法規制への対応（個人情報保護法）	20.8%	21.9%	19.1%	37.3%	18.0%	20.8%	26.1%	21.6%
法規制への対応（労働法）	20.5%	23.3%	27.9%	18.6%	15.5%	26.6%	17.4%	21.5%
法規制への対応（その他全般）	9.8%	23.3%	11.8%	25.4%	9.3%	16.4%	17.4%	14.0%
情報セキュリティの強化	38.6%	50.7%	30.9%	57.6%	41.0%	38.2%	47.8%	41.1%
災害やシステムダウンへの対応（BCP／DR）	25.8%	21.9%	26.5%	35.6%	17.4%	27.1%	26.1%	24.9%
企業の社会的責任（CSR）の履行	16.3%	24.7%	11.8%	25.4%	9.9%	16.9%	21.7%	16.5%
IT機器・システムの更新時期への対応	25.4%	23.3%	22.1%	33.9%	31.7%	24.6%	26.1%	26.5%
基盤環境（通信、OS、クラウドなど）の変化への対応	17.4%	13.7%	17.6%	27.1%	23.0%	13.0%	17.4%	17.8%
営業力の強化	21.6%	34.2%	33.8%	32.2%	14.9%	23.2%	4.3%	22.6%
商品・サービスの品質向上	25.0%	23.3%	22.1%	30.5%	20.5%	29.0%	8.7%	24.3%
新たな顧客コミュニケーションの構築	12.1%	24.7%	26.5%	23.7%	14.9%	18.8%	6.5%	16.9%
自社のプレゼンス／ブランド向上	12.5%	19.2%	13.2%	15.3%	11.8%	12.1%	6.5%	12.8%
新商品・新市場の創出基盤の構築	17.4%	19.2%	23.5%	20.3%	11.2%	11.1%	0.0%	14.7%
ビッグデータ活用によるビジネス機会の創出	12.5%	13.7%	14.7%	20.3%	12.4%	10.1%	2.2%	12.2%
その他	0.4%	0.0%	0.0%	0.0%	0.0%	1.0%	0.0%	0.3%

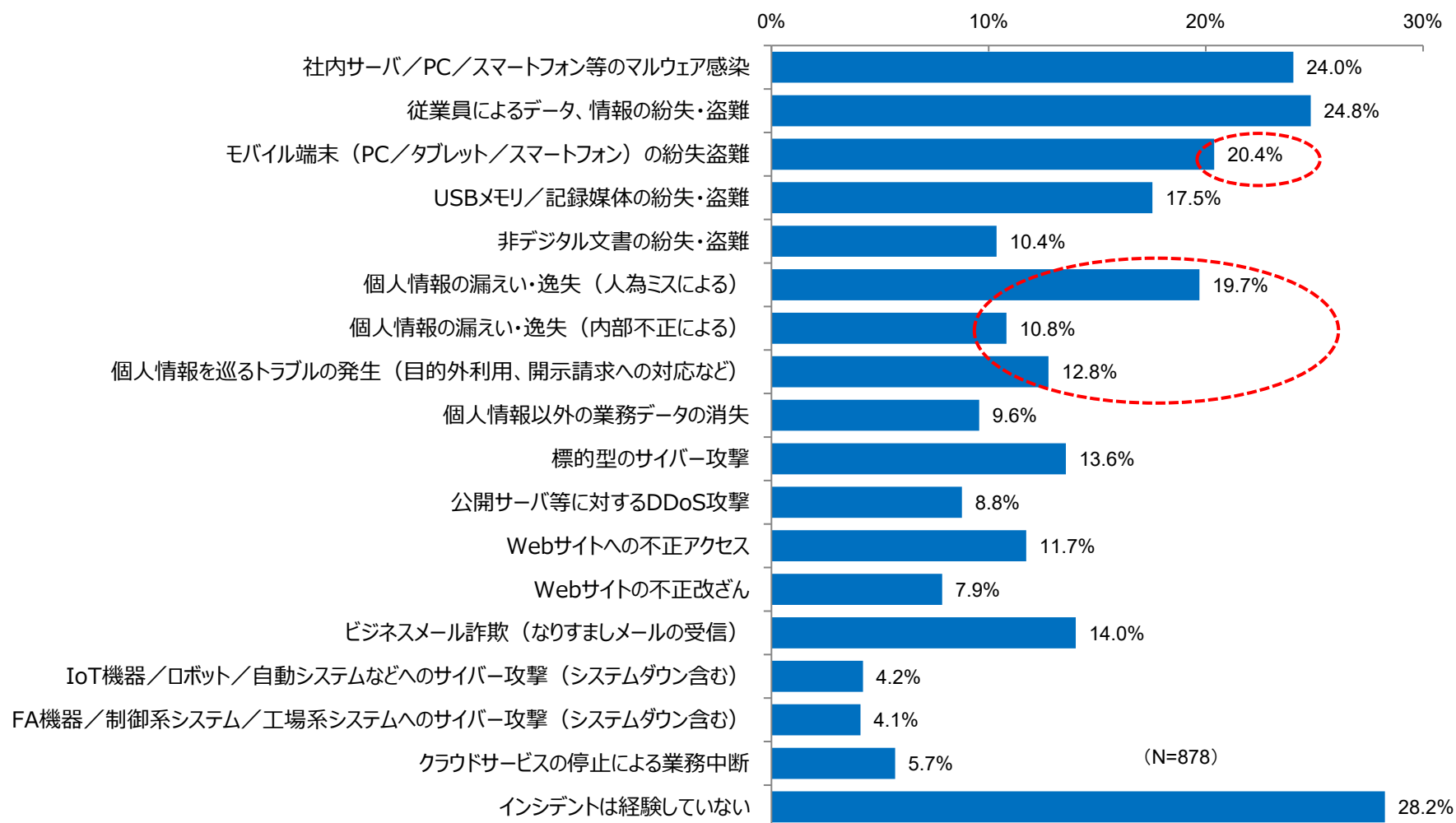
©2020, JIPDEC and ITR, All rights reserved.

Q1：重視する経営課題（従業員数規模別）

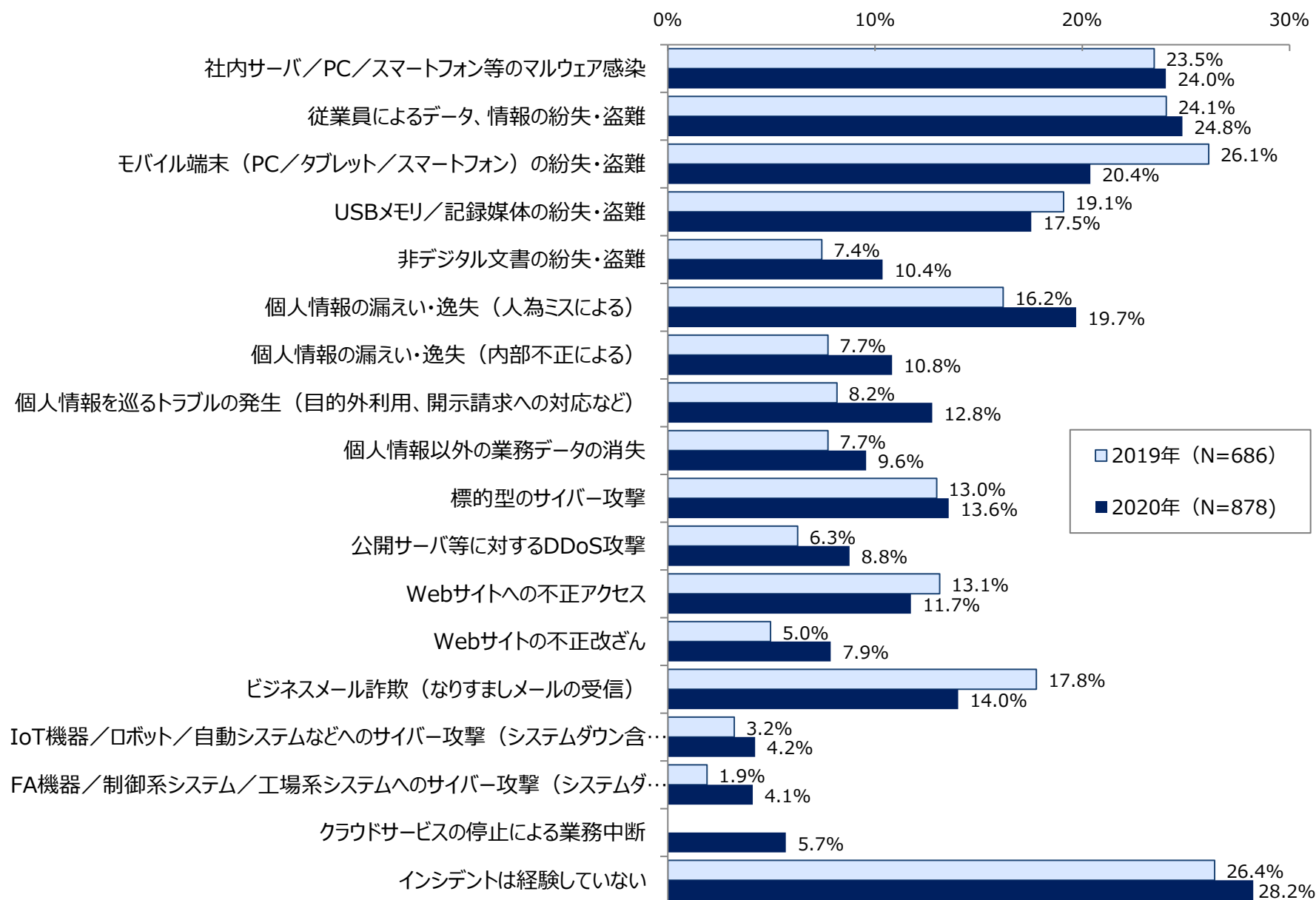
	5,000人以上 (N=197)	1,000～ 4,999人 (N=197)	300～999人 (N=215)	50～299人 (N=269)	全体 (N=878)
業務プロセスの効率化	52.8%	59.9%	59.1%	51.7%	55.6%
社内体制・組織の再構築	27.4%	34.5%	27.4%	34.6%	31.2%
社内コミュニケーションの強化	33.0%	36.0%	38.6%	41.3%	37.6%
従業員の働き方改革	48.7%	44.2%	47.4%	52.8%	48.6%
経営意思決定の迅速化（スピード経営）	22.8%	29.9%	19.5%	23.8%	23.9%
企業間（グループ、業界、取引先間）の情報連携	14.7%	27.4%	16.7%	12.3%	17.3%
業界標準や主要取引先への対応	14.2%	16.8%	9.3%	10.8%	12.5%
法規制への対応（内部統制／J-SOX）	22.8%	24.4%	18.6%	16.0%	20.0%
法規制への対応（個人情報保護法）	22.8%	24.4%	23.3%	17.5%	21.6%
法規制への対応（労働法）	18.8%	24.9%	21.9%	20.8%	21.5%
法規制への対応（その他全般）	13.2%	14.2%	14.9%	13.8%	14.0%
情報セキュリティの強化	44.7%	43.7%	42.8%	35.3%	41.1%
災害やシステムダウンへの対応（BCP／DR）	21.8%	24.4%	27.9%	25.3%	24.9%
企業の社会的責任（CSR）の履行	20.3%	23.4%	13.0%	11.5%	16.5%
IT機器・システムの更新時期への対応	24.4%	28.9%	31.6%	22.3%	26.5%
基盤環境（通信、OS、クラウドなど）の変化への対応	17.8%	24.9%	16.3%	13.8%	17.8%
営業力の強化	16.8%	18.3%	26.0%	27.1%	22.6%
商品・サービスの品質向上	22.3%	25.4%	24.7%	24.5%	24.3%
新たな顧客コミュニケーションの構築	11.7%	22.3%	15.3%	17.8%	16.9%
自社のプレゼンス／ブランド向上	11.7%	16.2%	14.0%	10.0%	12.8%
新商品・新市場の創出基盤の構築	17.3%	17.3%	14.0%	11.5%	14.7%
ビッグデータ活用によるビジネス機会の創出	19.8%	15.2%	11.2%	5.2%	12.2%
その他	0.0%	0.0%	0.0%	1.1%	0.3%

Q2：過去1年間に経験したセキュリティインシデント

- 例年同様、マルウェア感染と従業員によるデータ・情報の紛失盗難が上位になっているが、モバイル端末の紛失が減少し、個人情報の漏えい逸失および個人情報に関するトラブル発生が増加している。



Q2：過去1年間に経験したセキュリティインシデント（2019～2020年比較）



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）

- 「従業員によるデータ・情報紛失盗難」が情報通信で増加（16.3%→32.9%）
- 「人為ミスによる個人情報漏洩逸失」が公共・その他で増加（22.5%→30.4%）
- 「内部不正による個人情報漏洩逸失」が金融・保険で増加（0.0%→15.3%）
- 「標的型のサイバー攻撃」が製造で増加（11.3%→16.3%）

	製造 (N=264)	建設・不動産 (N=73)	卸売・小売 (N=68)	金融・保険 (N=59)	情報通信 (N=161)	サービス (N=207)	公共・その他 (N=46)	全体 (N=878)
社内サーバー／PC／スマートフォン等のマルウェア感染	29.2%	28.8%	17.6%	20.3%	29.2%	15.5%	21.7%	24.0%
従業員によるデータ、情報の紛失・盗難	28.4%	28.8%	16.2%	16.9%	32.9%	18.8%	19.6%	24.8%
モバイル端末（PC／タブレット／スマートフォン）の紛失盗難	25.4%	16.4%	14.7%	15.3%	27.3%	16.4%	6.5%	20.4%
USBメモリ／記録媒体の紛失・盗難	21.6%	21.9%	16.2%	13.6%	15.5%	14.5%	15.2%	17.5%
非デジタル文書の紛失・盗難	10.2%	11.0%	11.8%	16.9%	9.9%	9.7%	4.3%	10.4%
個人情報の漏えい・逸失（人為ミスによる）	18.6%	27.4%	11.8%	28.8%	21.1%	15.0%	30.4%	19.7%
個人情報の漏えい・逸失（内部不正による）	12.9%	12.3%	11.8%	15.3%	9.9%	6.3%	13.0%	10.8%
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）	12.5%	16.4%	5.9%	22.0%	11.8%	11.6%	15.2%	12.8%
個人情報以外の業務データの消失	9.1%	19.2%	8.8%	10.2%	9.3%	6.3%	13.0%	9.6%
標的型のサイバー攻撃	16.3%	17.8%	10.3%	11.9%	14.9%	10.1%	8.7%	13.6%
公開サーバ等に対するDDoS攻撃	7.6%	6.8%	8.8%	13.6%	11.2%	7.2%	10.9%	8.8%
Webサイトへの不正アクセス	11.0%	23.3%	11.8%	16.9%	11.8%	7.7%	8.7%	11.7%
Webサイトの不正改ざん	7.2%	5.5%	4.4%	15.3%	11.2%	6.8%	4.3%	7.9%
ビジネスメール詐欺（なりすましメールの受信）	13.3%	23.3%	16.2%	16.9%	15.5%	9.2%	13.0%	14.0%
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）	4.2%	8.2%	4.4%	6.8%	5.0%	1.9%	2.2%	4.2%
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）	5.7%	5.5%	2.9%	6.8%	5.0%	1.4%	0.0%	4.1%
クラウドサービスの停止による業務中断	4.2%	9.6%	1.5%	13.6%	6.2%	5.8%	2.2%	5.7%
インシデントは経験していない	20.8%	21.9%	39.7%	32.2%	19.9%	42.5%	23.9%	28.2%

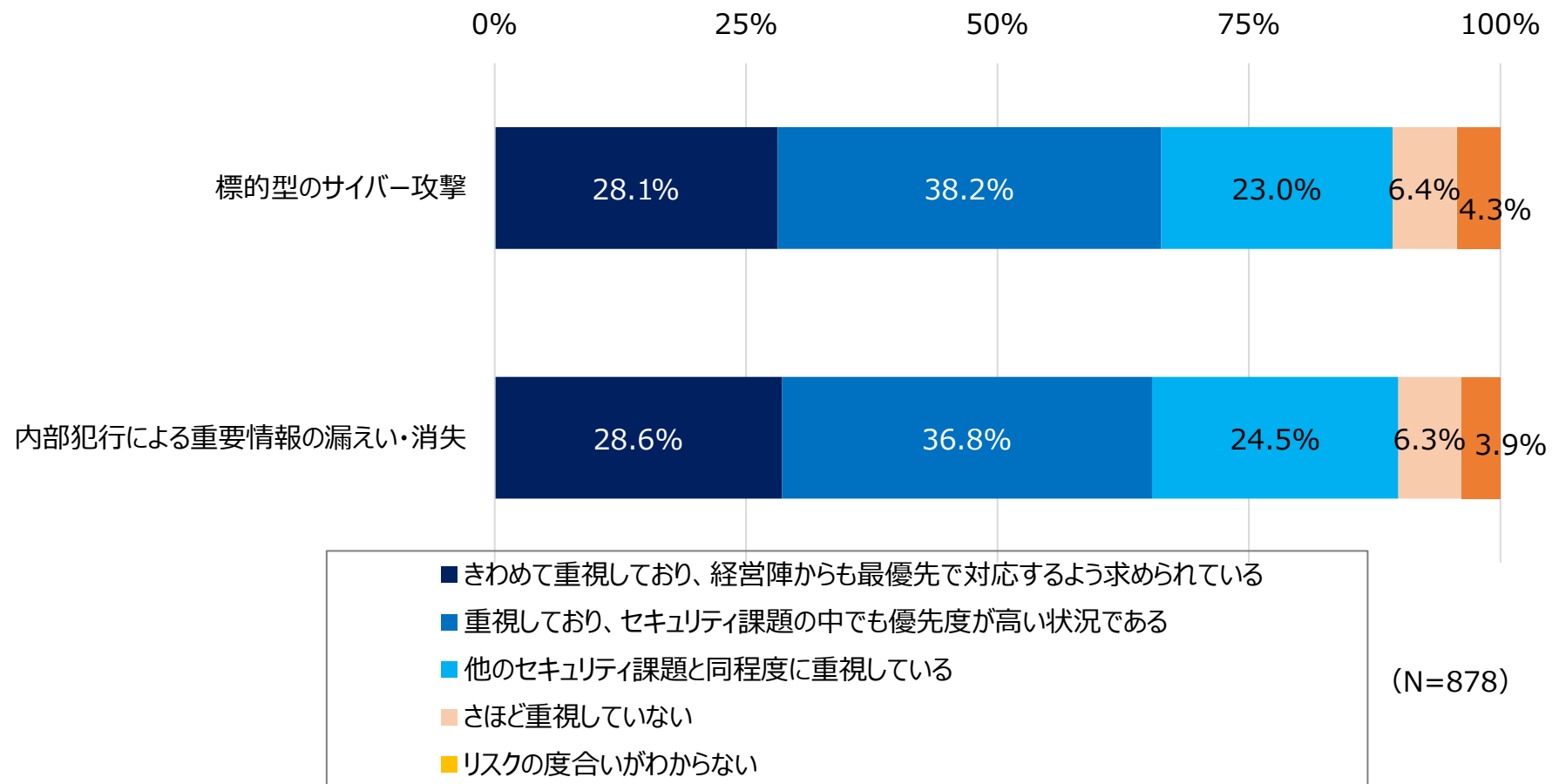
Q2：過去1年間に経験したセキュリティインシデント（2020年/従業員数規模別）

- 従業員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、対前年比では、特に「個人情報の漏えい・逸失と」「個人情報をめぐるトラブルの発生」の増加が目立っている。

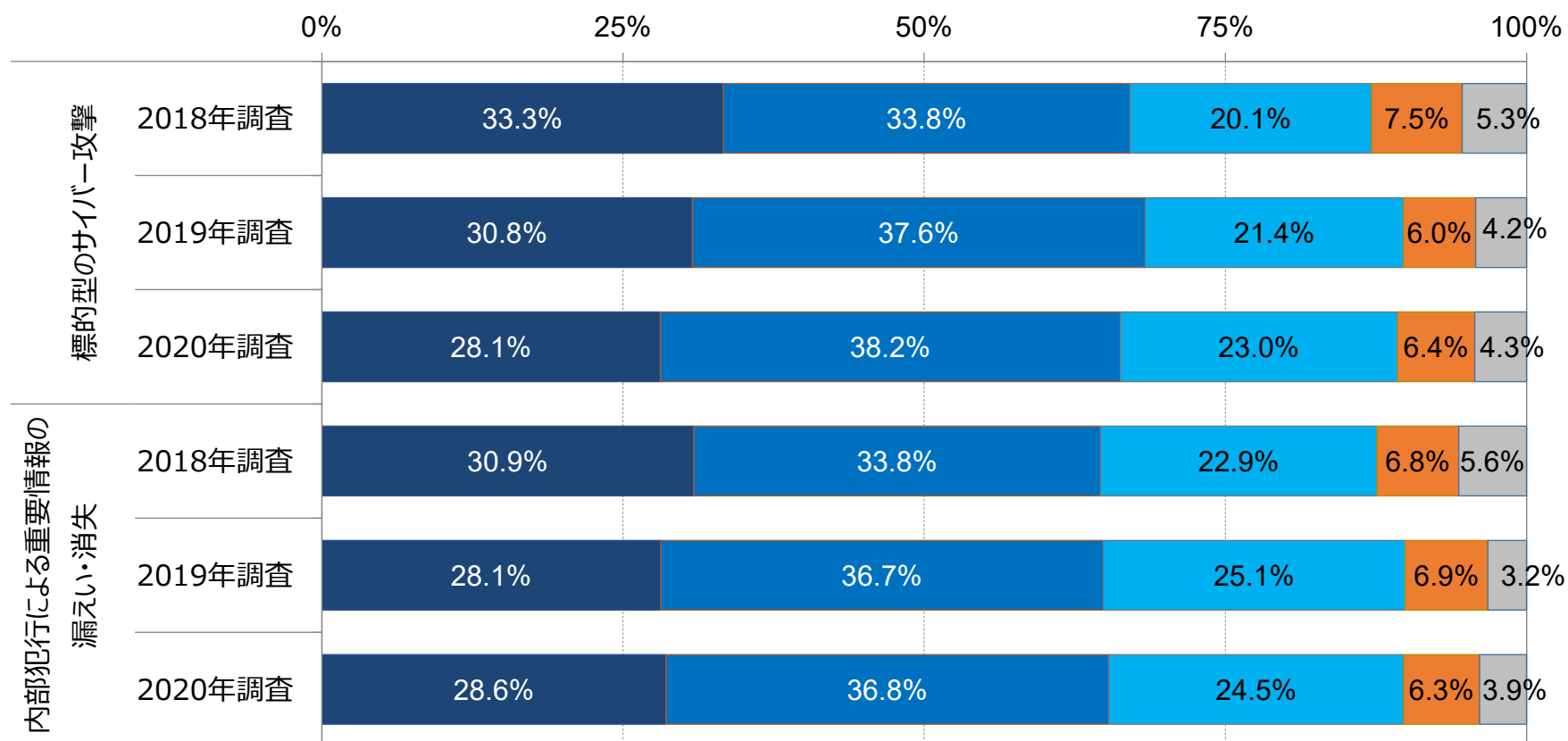
	5,000人以上 (N=197)	1,000～ 4,999人 (N=197)	300～999人 (N=215)	50～299人 (N=269)	全体 (N=878)
社内サーバ／PC／スマートフォン等のマルウェア感染	36.5%	21.3%	21.9%	18.6%	24.0%
従業員によるデータ、情報の紛失・盗難	32.5%	31.0%	20.5%	18.2%	24.8%
モバイル端末（PC／タブレット／スマートフォン）の紛失盗難	27.4%	28.4%	19.5%	10.0%	20.4%
USBメモリ／記録媒体の紛失・盗難	21.3%	19.8%	18.1%	12.6%	17.5%
非デジタル文書の紛失・盗難	13.2%	14.7%	8.8%	6.3%	10.4%
個人情報の漏えい・逸失（人為ミスによる）	27.9%	23.9%	18.6%	11.5%	19.7%
個人情報の漏えい・逸失（内部不正による）	12.7%	14.2%	11.6%	6.3%	10.8%
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）	17.3%	18.8%	11.2%	6.3%	12.8%
個人情報以外の業務データの消失	9.1%	13.7%	9.8%	6.7%	9.6%
標的型のサイバー攻撃	19.8%	18.3%	13.0%	5.9%	13.6%
公開サーバ等に対するDDoS攻撃	10.2%	13.2%	9.8%	3.7%	8.8%
Webサイトへの不正アクセス	15.2%	13.7%	10.2%	8.9%	11.7%
Webサイトの不正改ざん	7.6%	11.7%	7.9%	5.2%	7.9%
ビジネスメール詐欺（なりすましメールの受信）	14.2%	16.2%	16.7%	10.0%	14.0%
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）	3.0%	9.6%	3.3%	1.9%	4.2%
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）	4.1%	6.1%	4.7%	2.2%	4.1%
クラウドサービスの停止による業務中断	6.6%	8.6%	4.7%	3.7%	5.7%
インシデントは経験していない	11.2%	22.3%	31.2%	42.8%	28.2%

Q3_1：セキュリティリスクの重視度合い

- 「標的型のサイバー攻撃」「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」とした割合が約 3 割で例年と同様である。
- 「重視」まで含めれば、6 ～ 7 割となっており、対応優先度の高いリスクとして認識されている。



Q3_1：セキュリティリスクの重視度合い（2018～2020年比較）

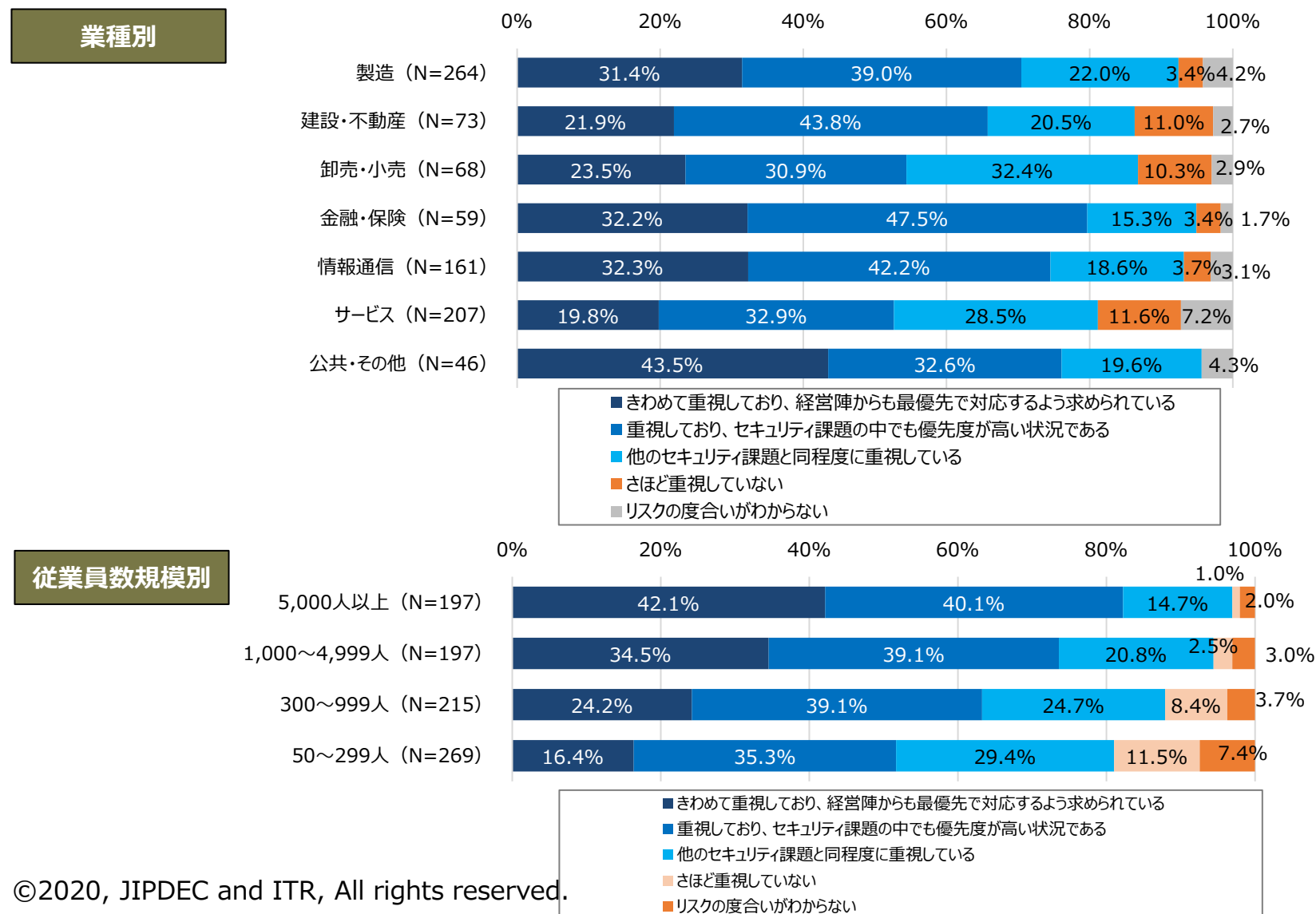


2018年調査 (N=693)
2019年調査 (N=686)
2020年調査 (N=878)

- きわめて重視しており、経営陣からも最優先で対応するよう求められている
- 重視しており、セキュリティ課題の中でも優先度が高い状況である
- 他のセキュリティ課題と同程度に重視している
- さほど重視していない
- リスクの度合いがわからない

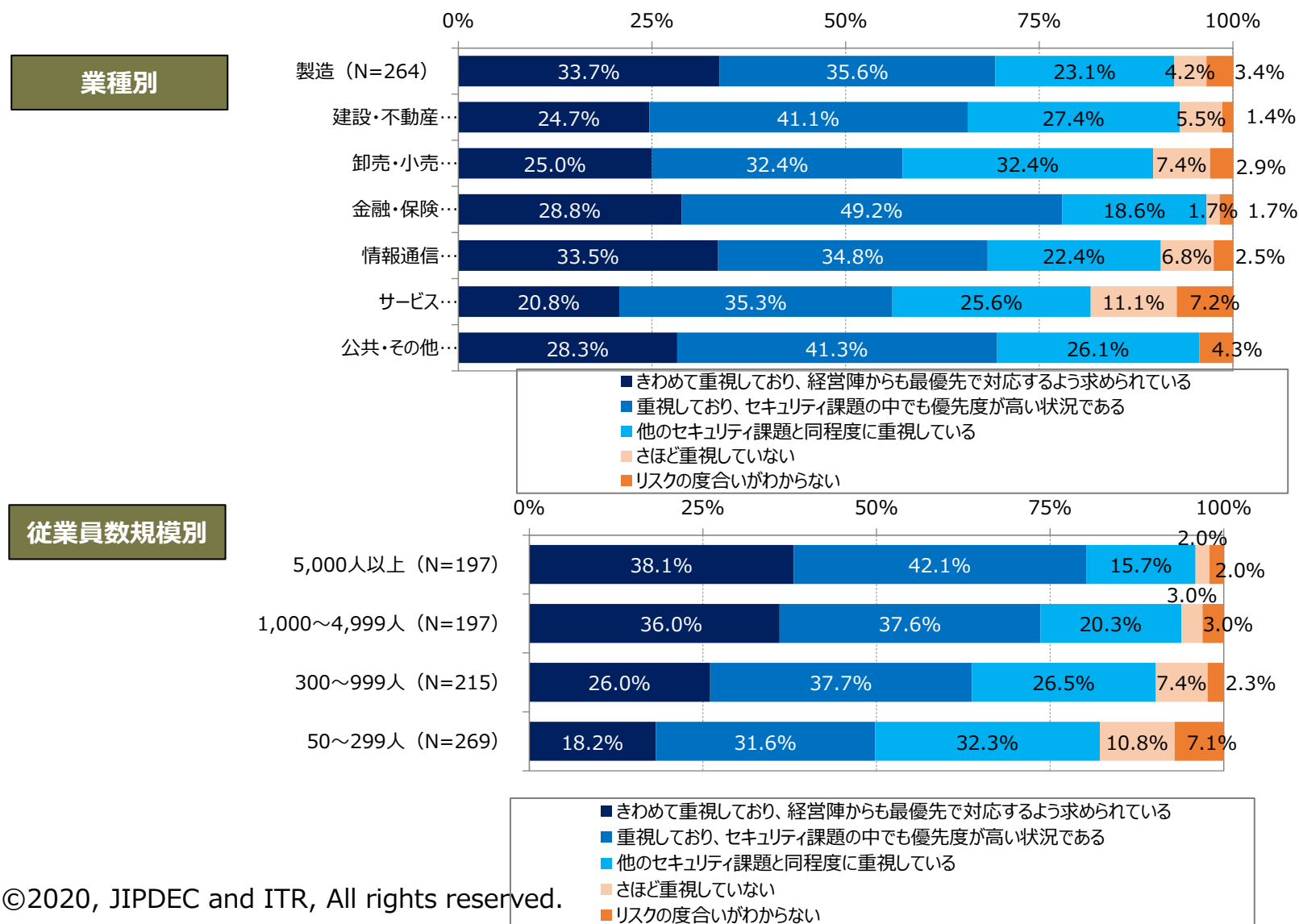
Q3_1:「標的型サイバー攻撃」の重視度合い

- 「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。



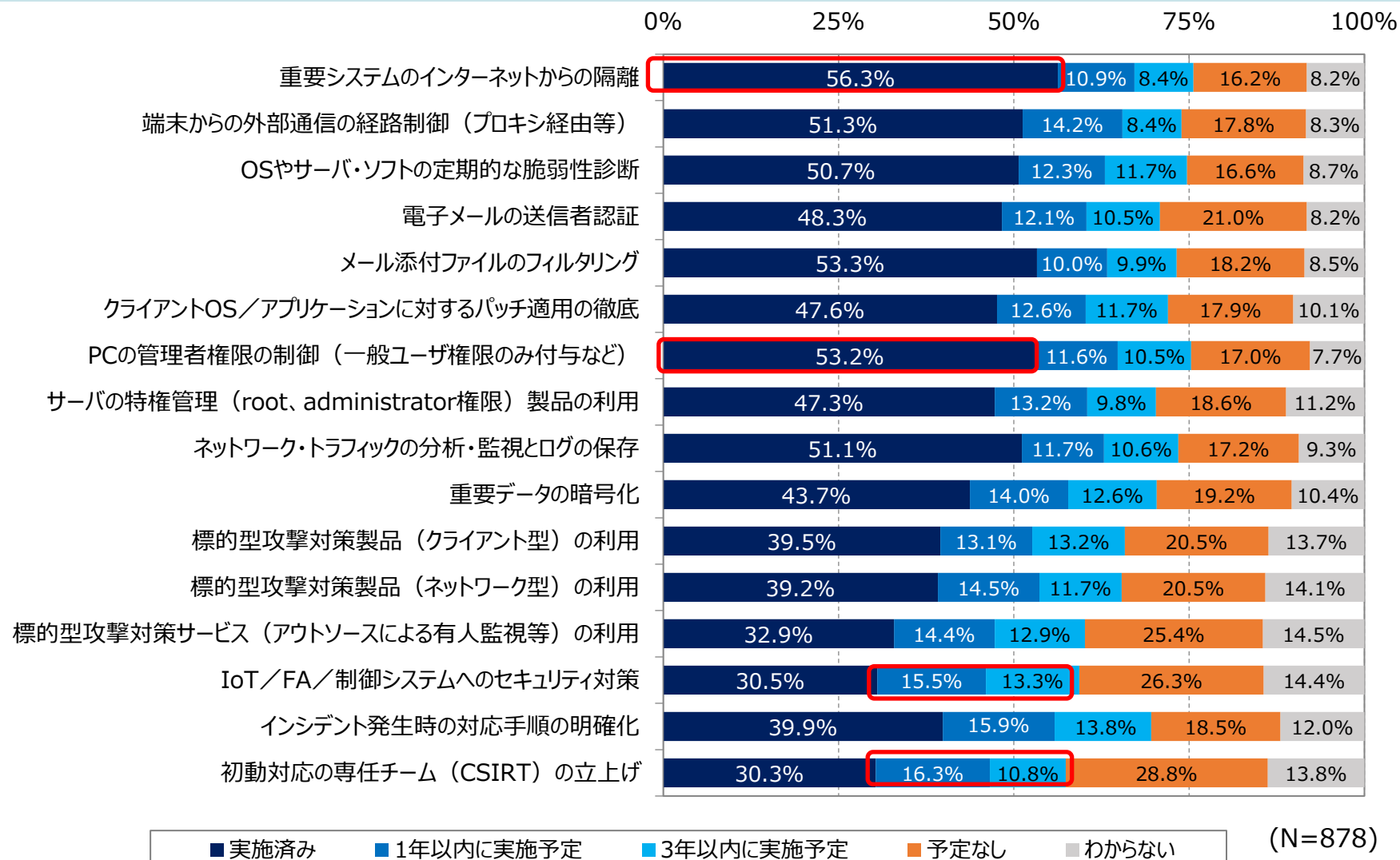
Q3_1: 「内部犯行による重要情報の漏えい・消失」の重視度合い

- 「きわめて重視」と「重視」を合わせると、製造、金融・保険、公共・その他の比率が高くなっている
- 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。



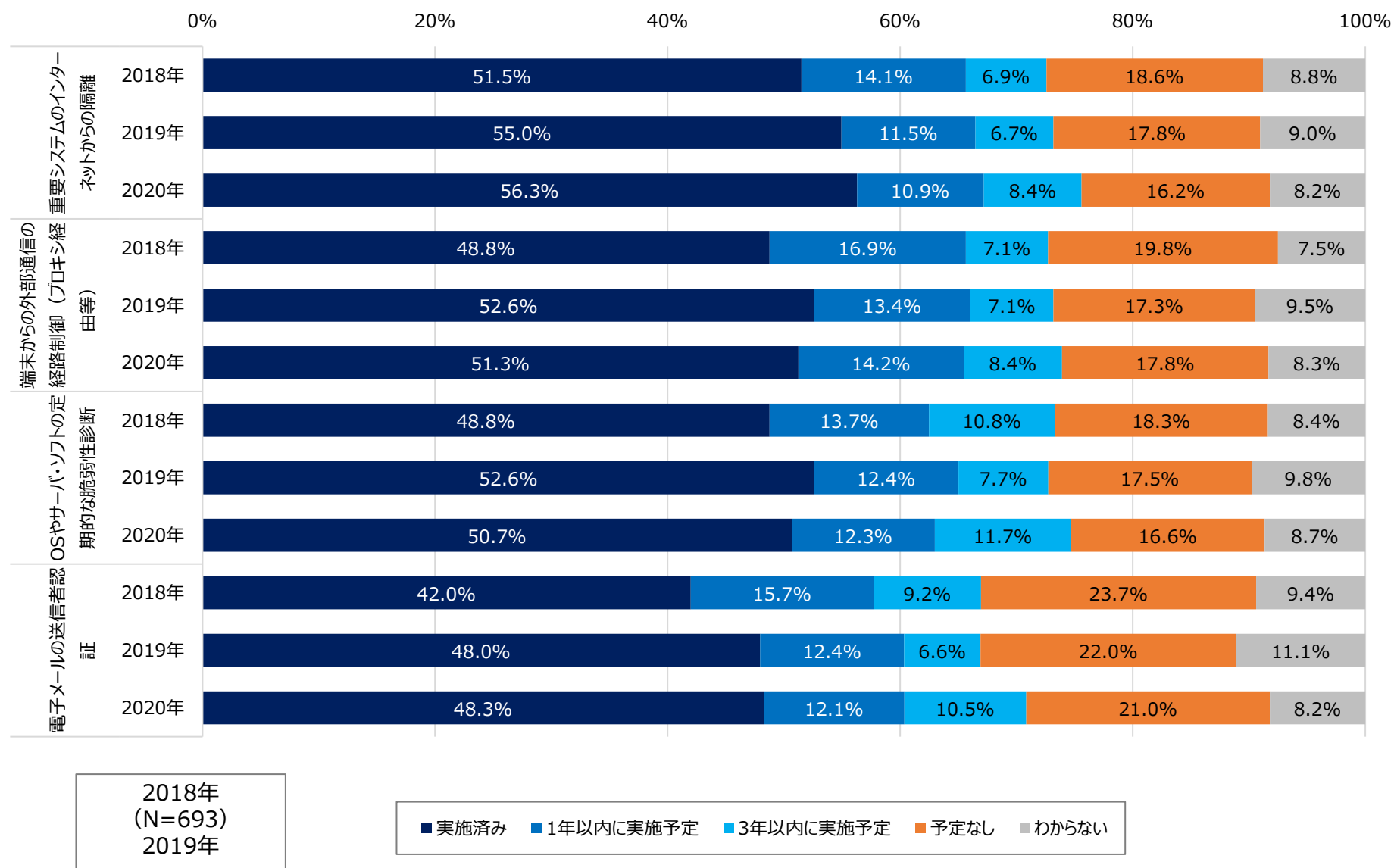
Q3_2 : 「標的型攻撃対策」の実施状況

- 実施済が最も高いのは、2019年同様「インターネットからの隔離」と「PC管理者権限の制御」である。
- 実施済が低く、今後実施予定が高いのは「IoT／FA／制御システムへのセキュリティ対策」と「CSIRTの立上げ」である。

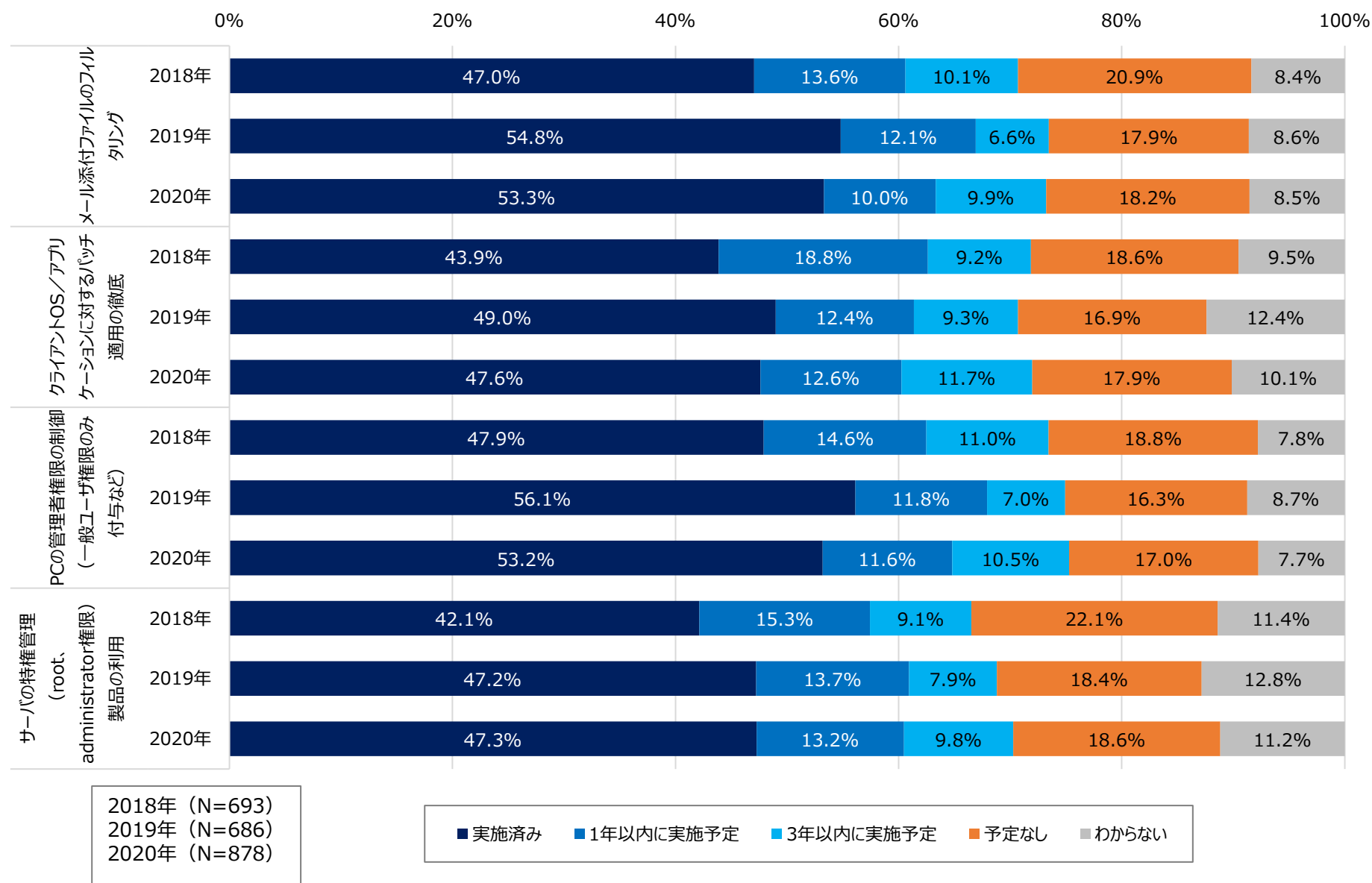


(N=878)

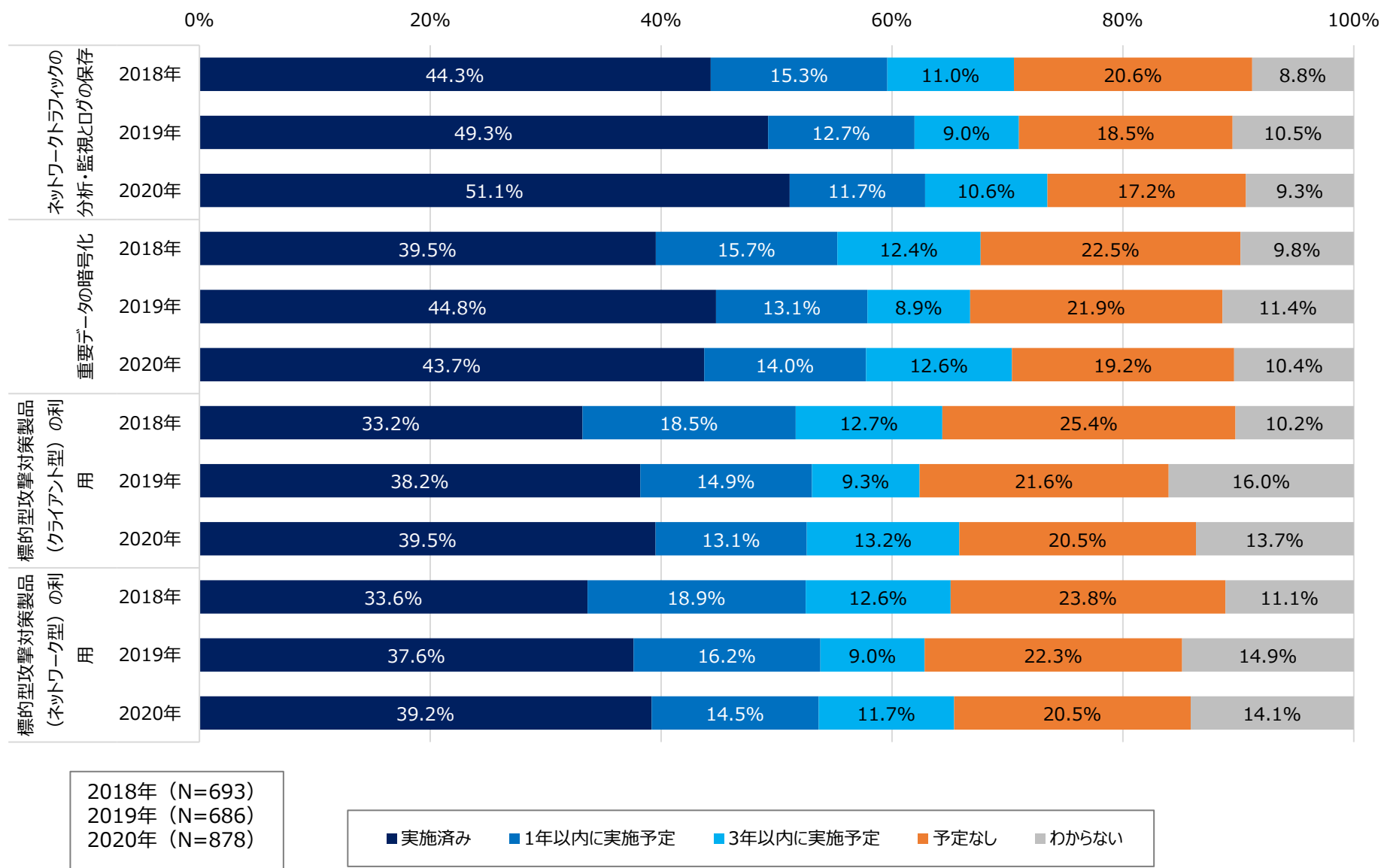
Q3_2：「標的型攻撃対策」の実施状況（2018～2020年比較）



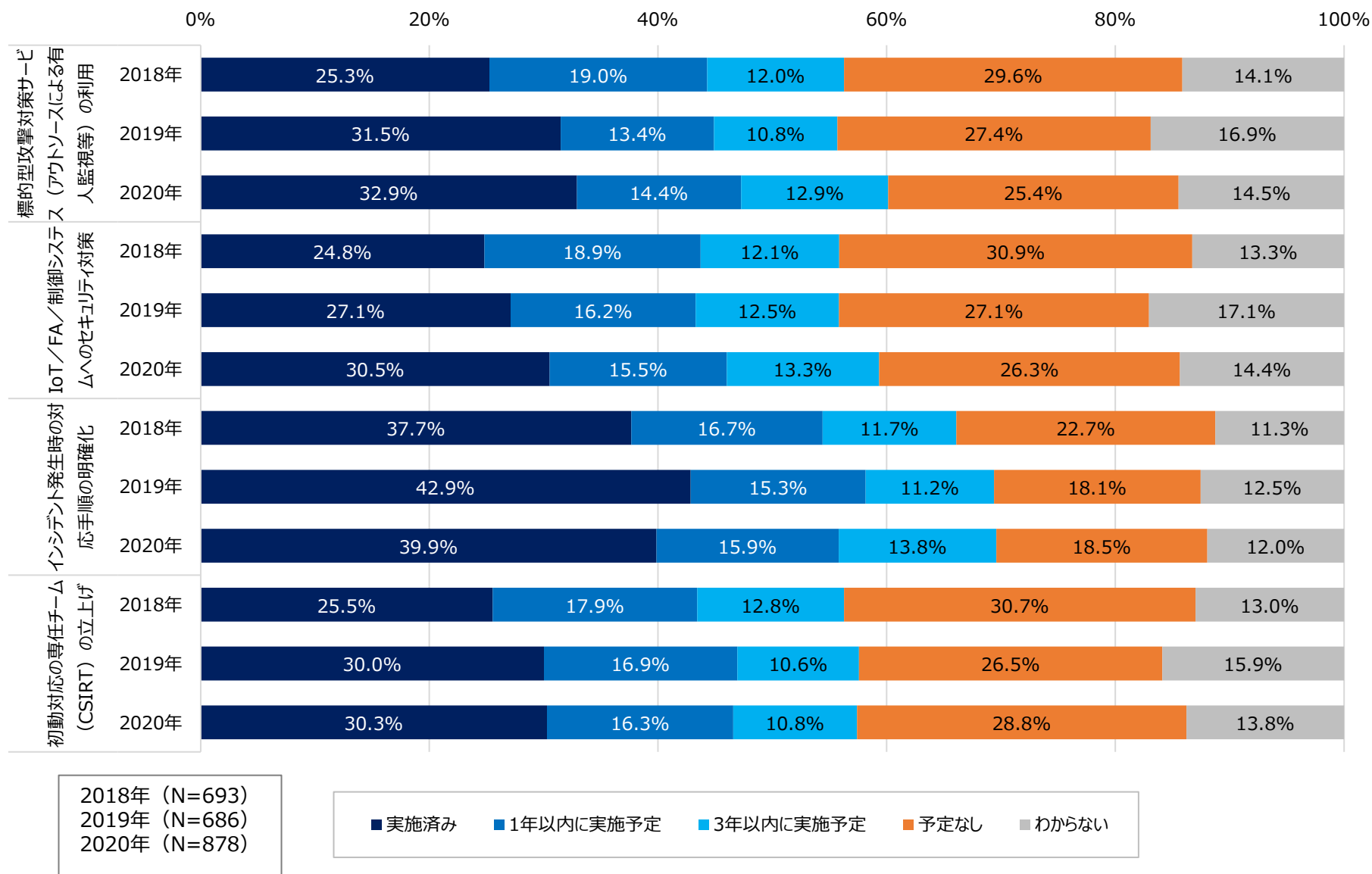
Q3_2 : 「標的型攻撃対策」の実施状況（2018~2020年比較）



Q3_2 : 「標的型攻撃対策」の実施状況（2018~2020年比較）

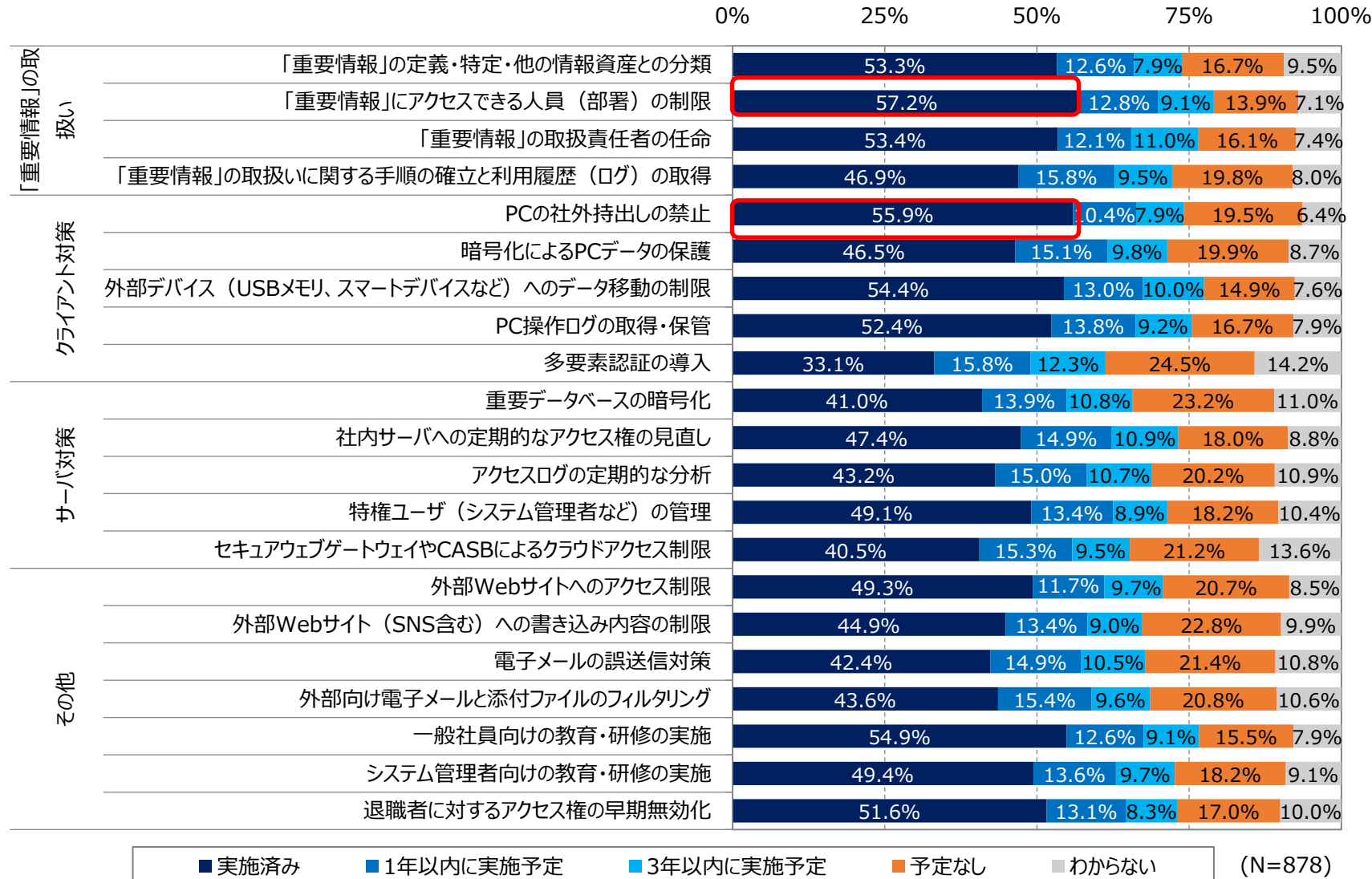


Q3_2 : 「標的型攻撃対策」の実施状況（2018~2020年比較）



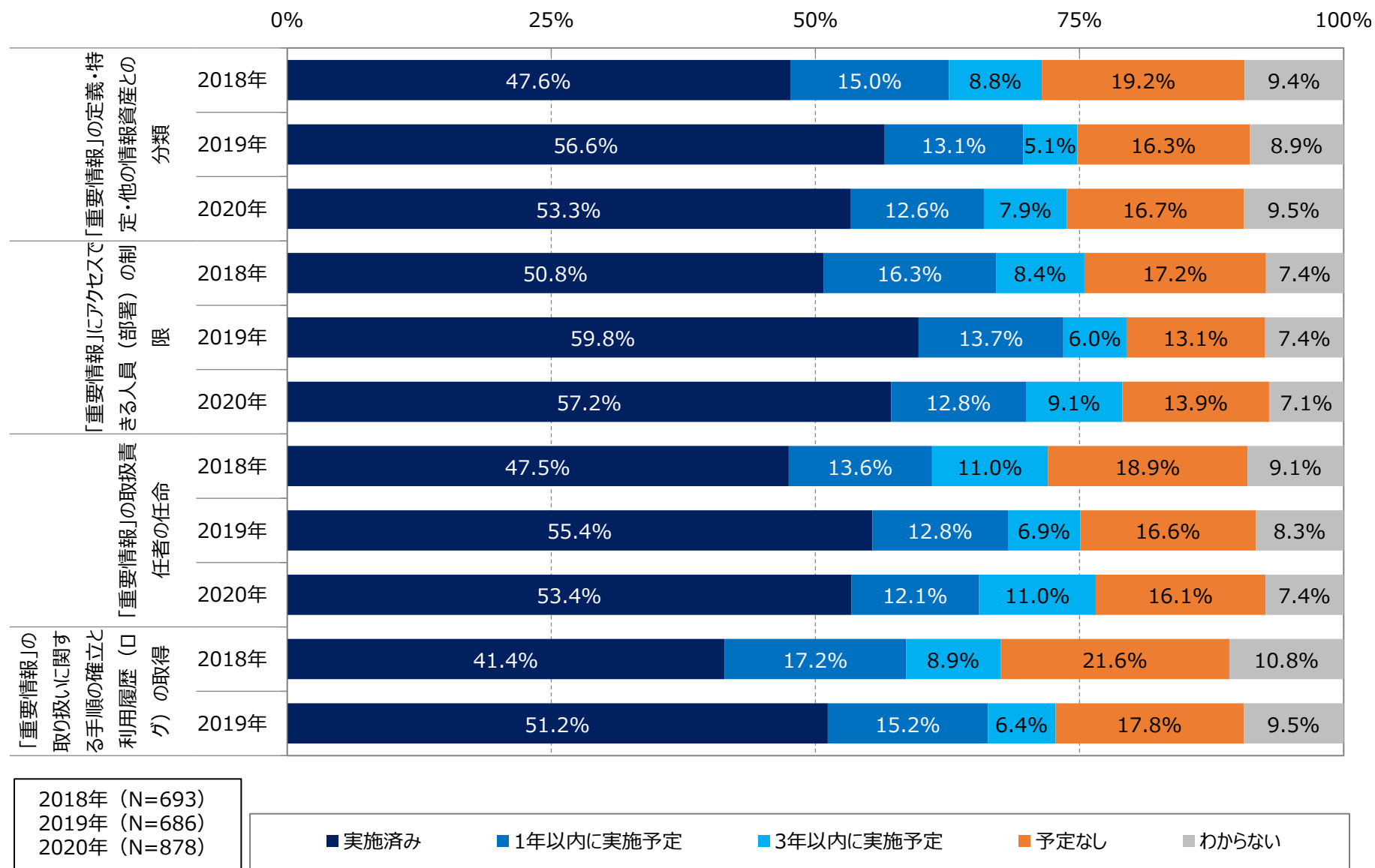
Q3_3 : 「情報漏えい対策」の実施状況（2020年）

■ 実施済は、2019年と同じく「重要情報にアクセスできる人員（部署）の制限」が一番高く、次には2019年3位の「PCの社外持出し禁止」が2位になっている。



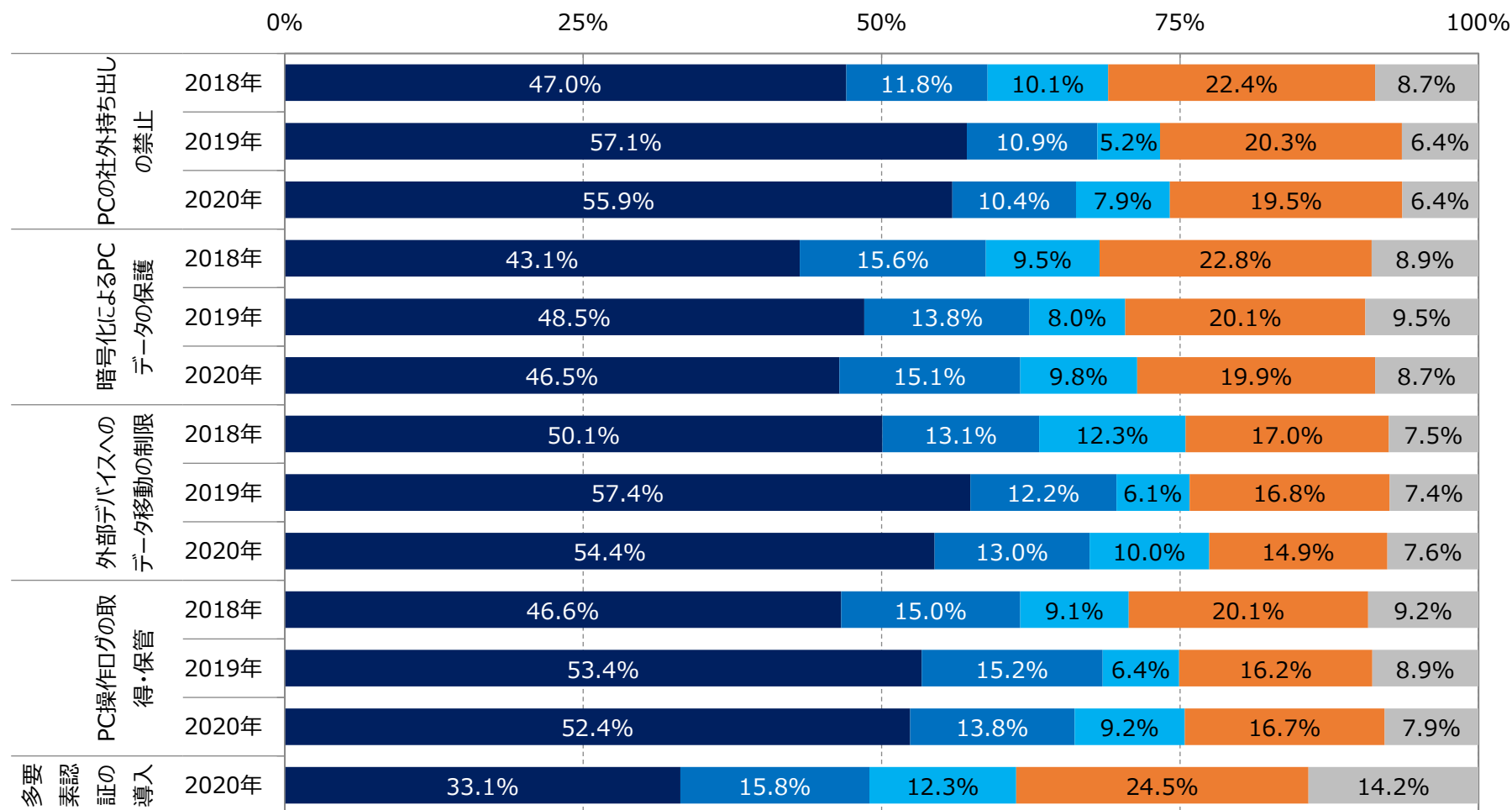
Q3_3：「情報漏えい対策」の実施状況（2018～2020年比較）

①「重要情報」の取扱い



Q3_3 : 「情報漏えい対策」の実施状況（2018～2020年比較）

②クライアント対策

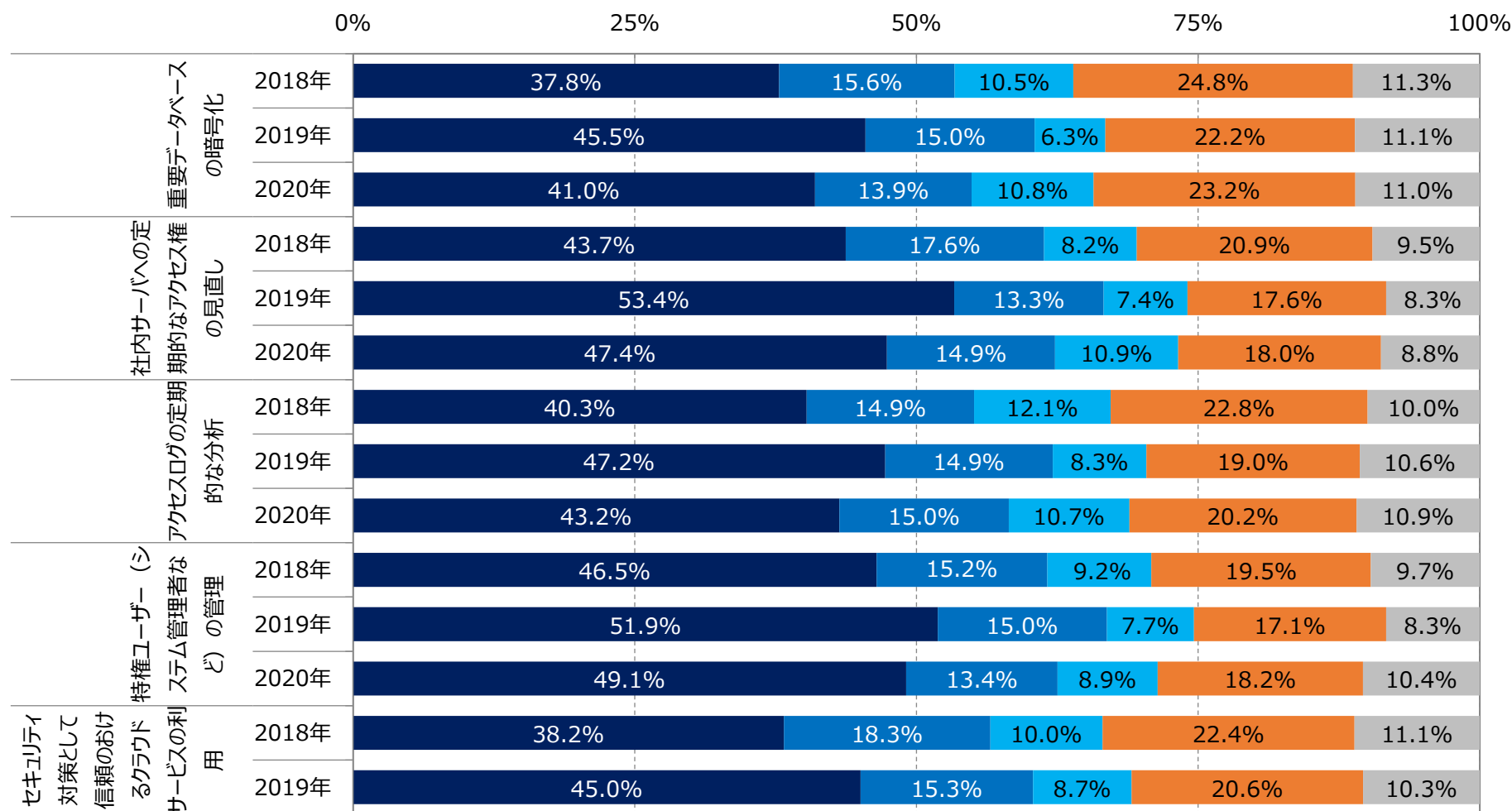


2018年 (N=693)
2019年 (N=686)
2020年 (N=878)

■ 実施済み ■ 1年以内に実施予定 ■ 3年以内に実施予定 ■ 予定なし ■ わからない

Q3_3：「情報漏えい対策」の実施状況（2018～2020年比較）

③サーバ対策

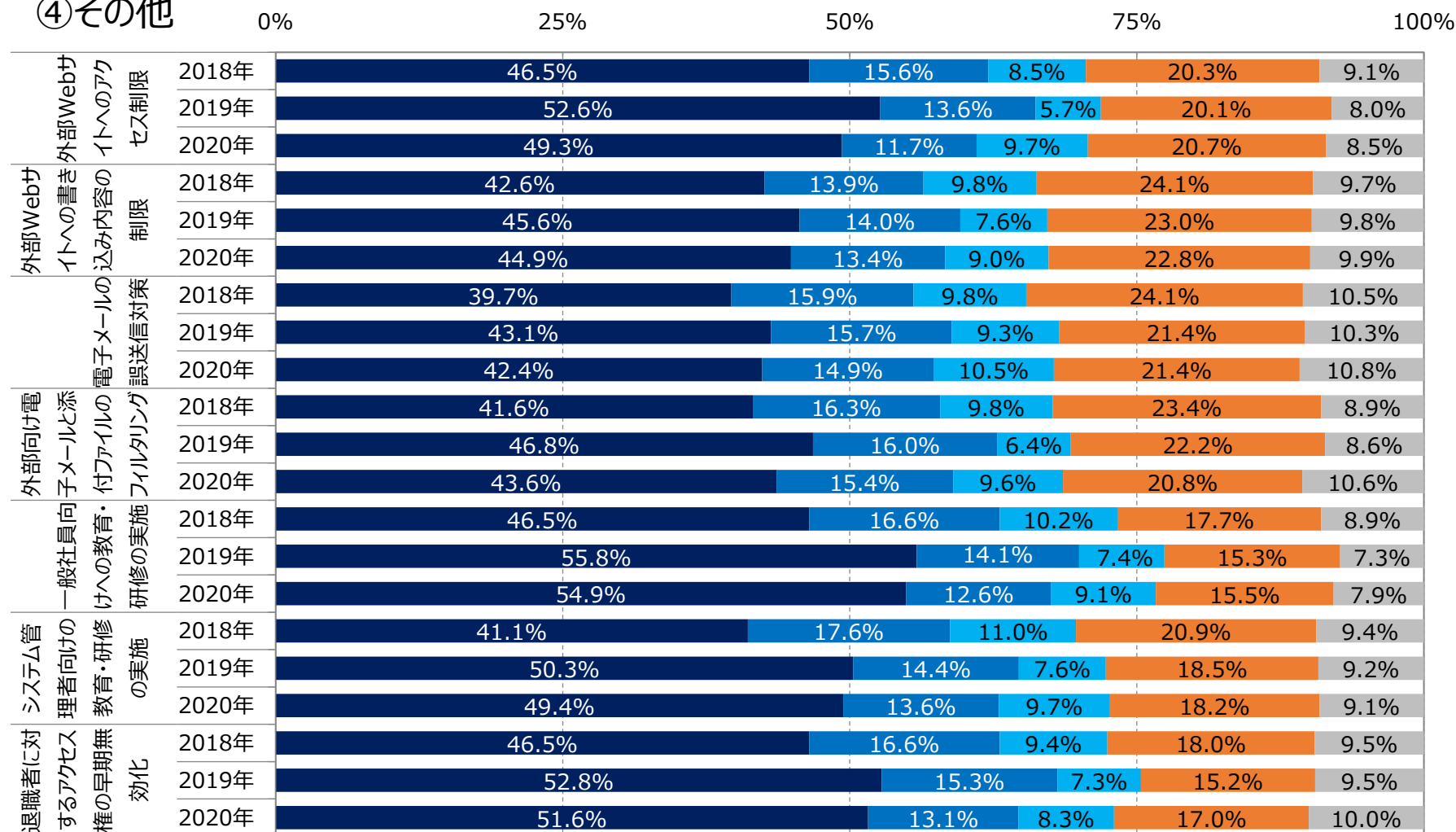


2018年 (N=693)
2019年 (N=686)
2020年 (N=878)

■ 実施済み ■ 1年以内に実施予定 ■ 3年以内に実施予定 ■ 予定なし ■ わからない

Q3_3：「情報漏えい対策」の実施状況（2018～2020年比較）

④その他



2018年 (N=693)
2019年 (N=686)
2020年 (N=878)

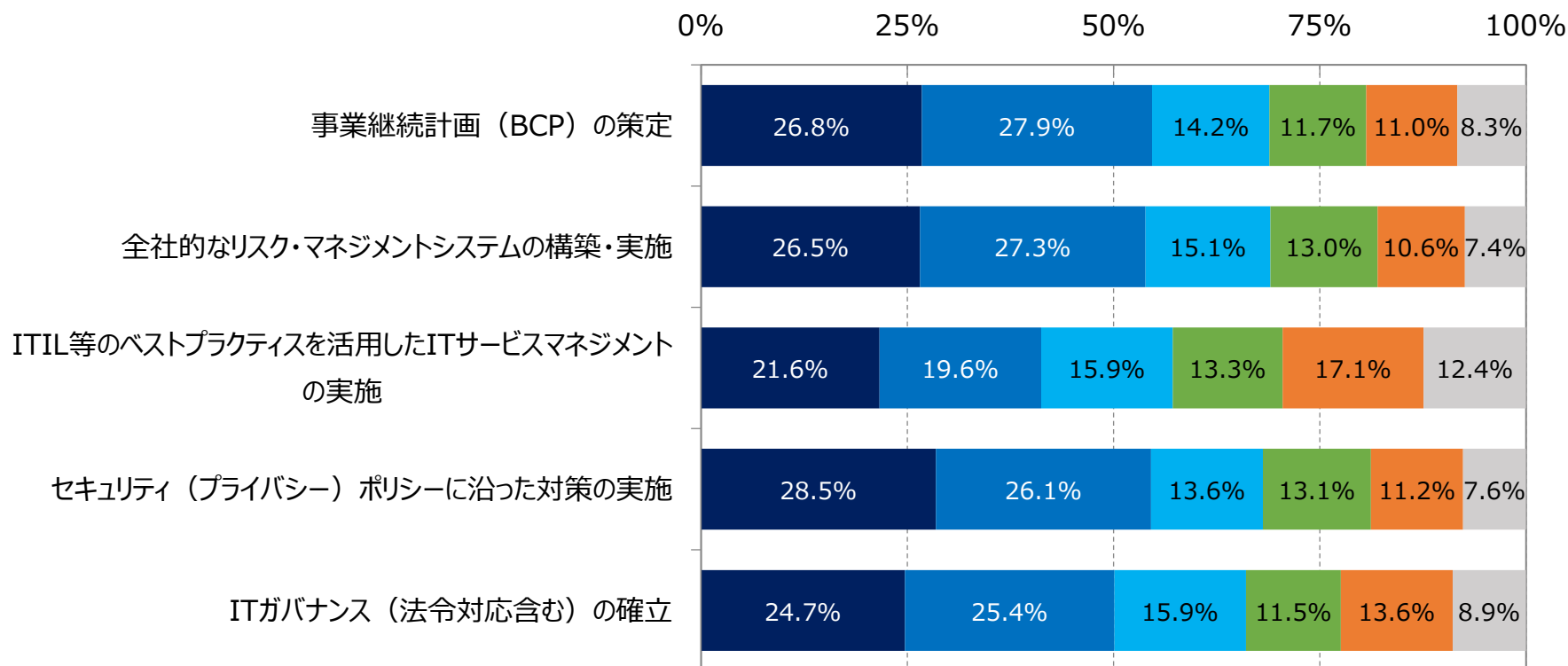
■ 実施済み ■ 1年以内に実施予定 ■ 3年以内に実施予定 ■ 予定なし ■ わからない

2) 認定／認証制度に対する意識

- Q4_1 : システムリスク緩和策の取組み状況
- Q4_2 : 主要認定／認証制度に対する取組み状況
- Q4_3 : 認定／認証を取得することの価値
- Q4_4 : 重視する認定／認証制度

Q4_1：システムリスクの軽減策の取組み状況

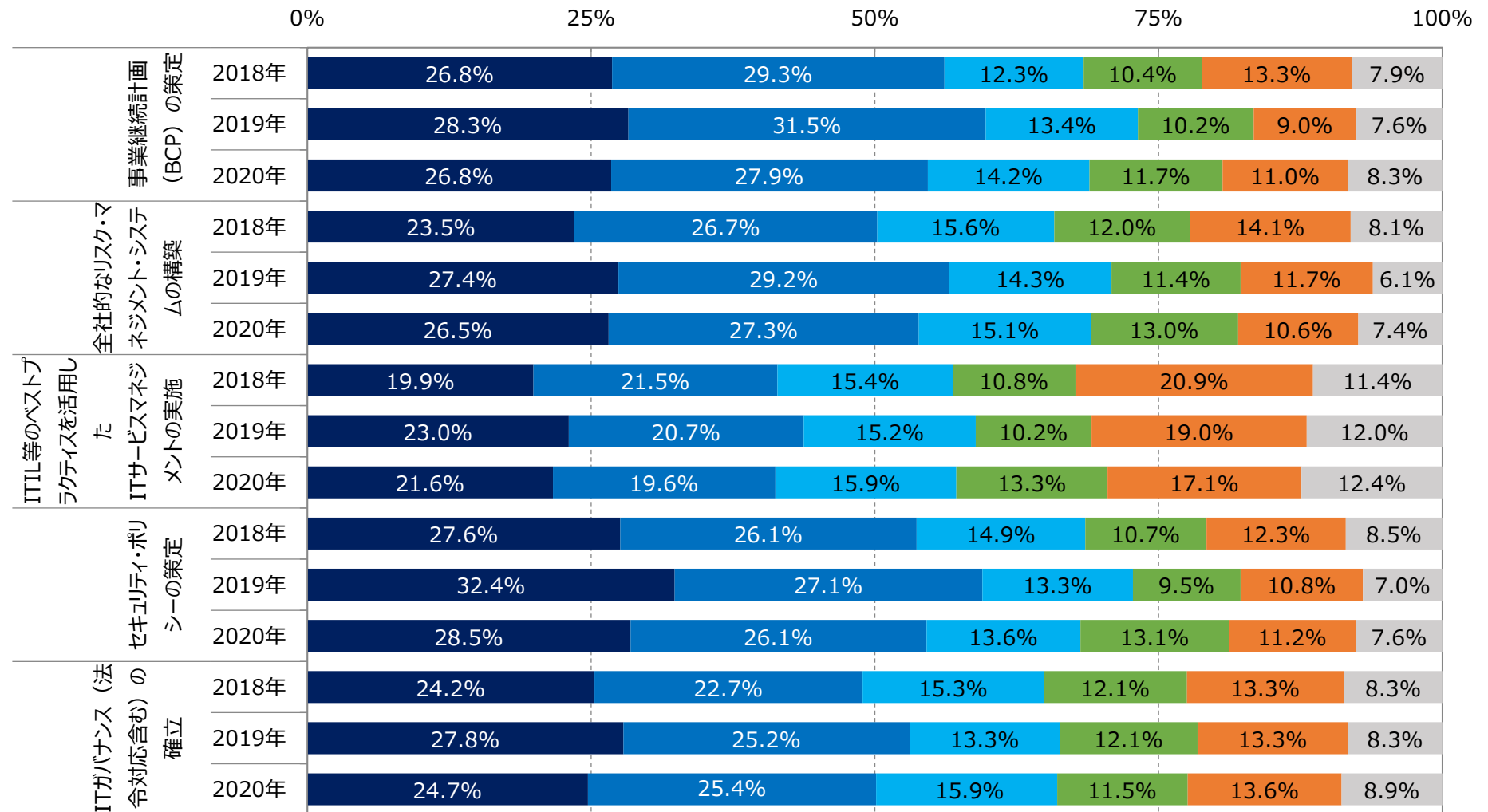
- 「BCPの策定」、「リスクマネジメントの構築」および「セキュリティポリシーの策定」について、実施済の比率がやや低下し、約 5 割弱となった。
- 「ITサービスマネジメントの実施」は昨年同様、実施済が約 4 割で、予定なし・わからないが合わせて約 3 割となっている。



(N=878)

- | | |
|--------------------|------------------------|
| ■ 実施済みであり、変更の予定はない | ■ 実施済みだが、変更中またはその予定がある |
| ■ 現在、実施または変更の最中である | ■ 未実施だが、今後の実施を計画している |
| ■ 未実施であり、その予定もない | ■ わからない／知らない |

Q4_1：システムリスクの軽減策の取組み状況（2018～2020年比較）

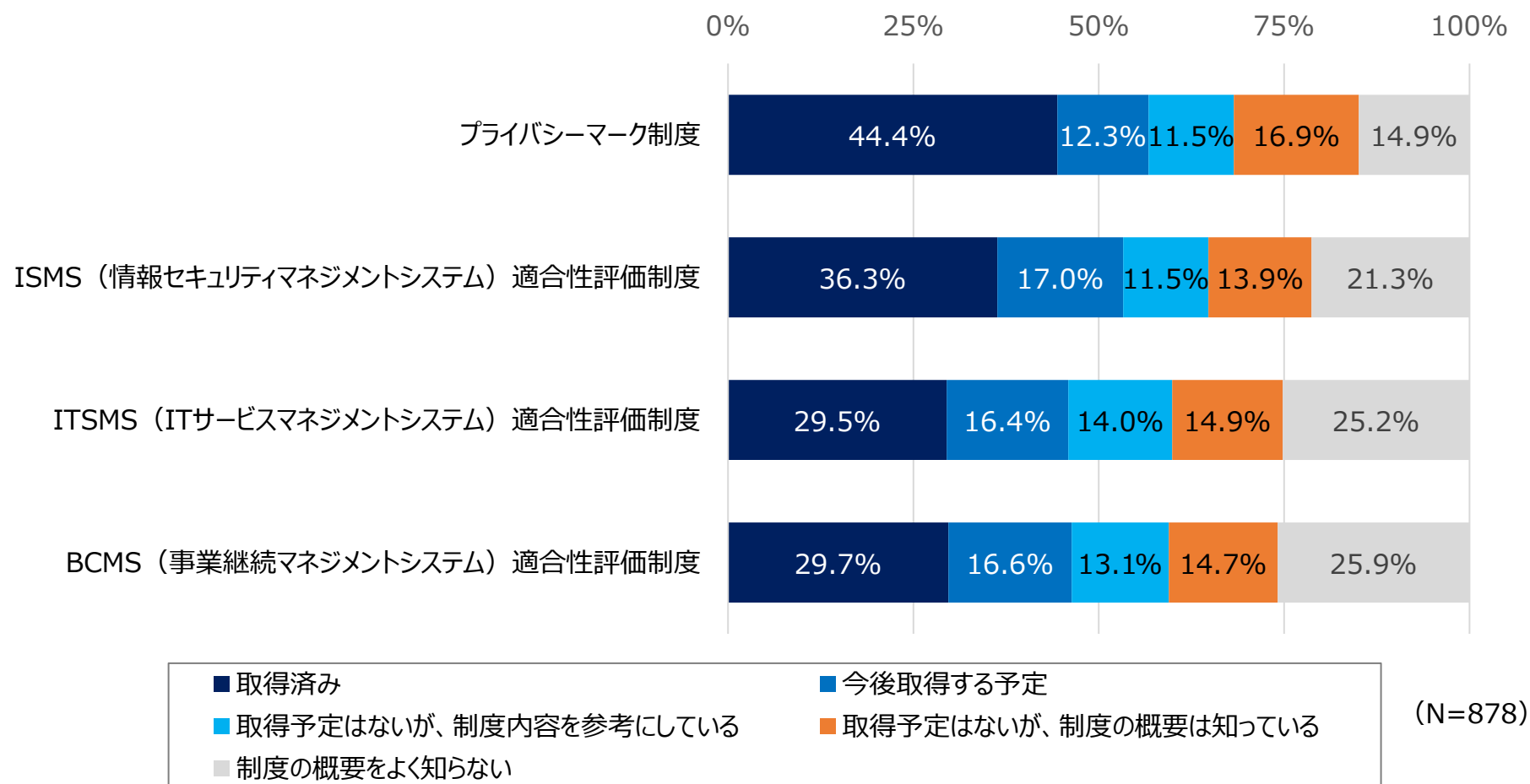


2018年
(N=693)
2019年

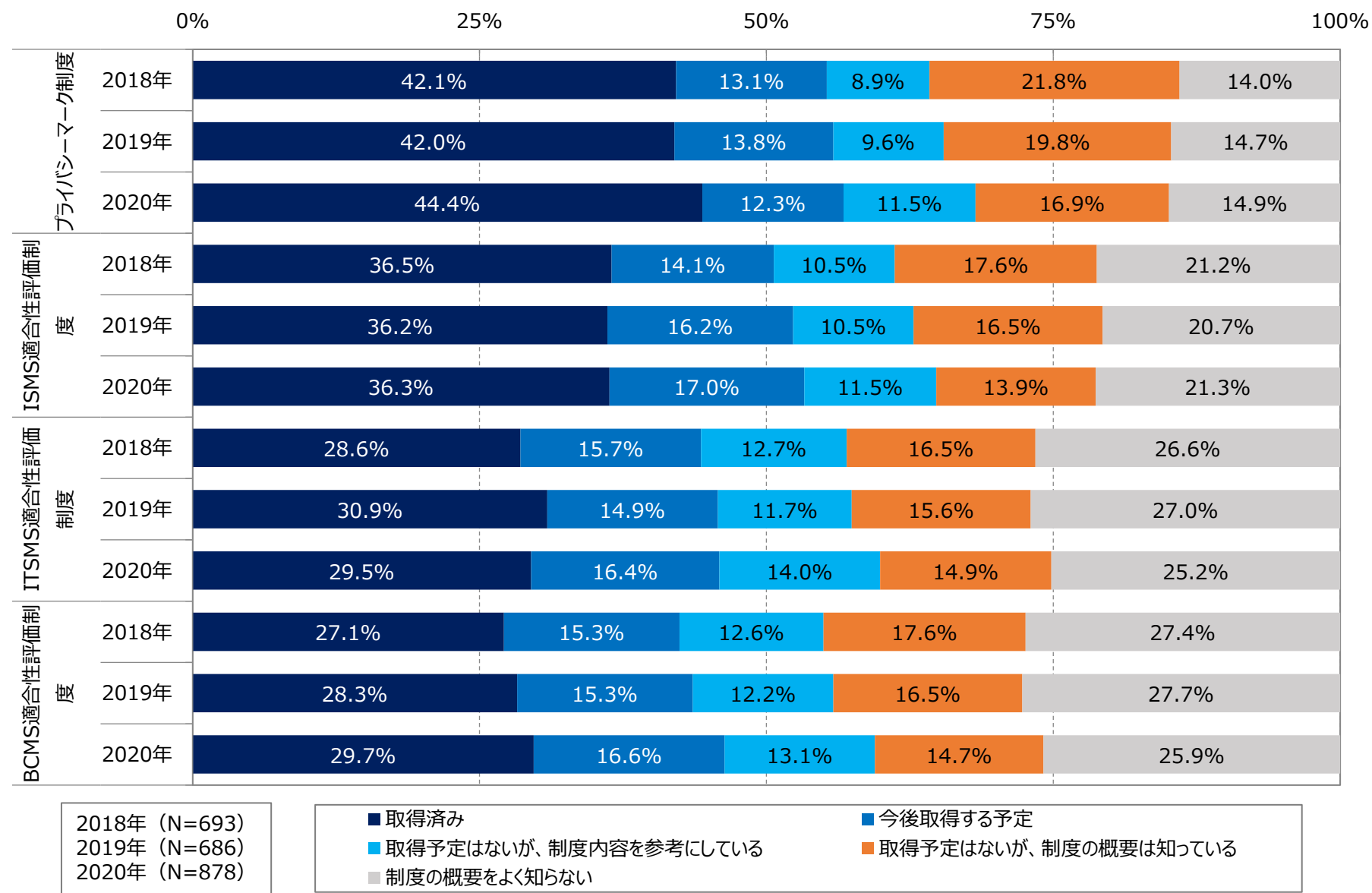
- 実施済みであり、変更の予定はない
- 実施済みだが、変更中またはその予定がある
- 現在、実施または変更の最中である
- 未実施だが、今後の実施を計画している
- 未実施であり、その予定もない
- わからない／知らない

Q4_2：情報セキュリティに関する認定/認証制度の取組み状況

- 「ISMS」の取得済みは2019年同様、「プライバシーマーク」の取得済が2019年よりも若干増加している。
- 「ITSMS」と「BCMS」は取得済みと予定を含め、2019年よりも若干増加している。

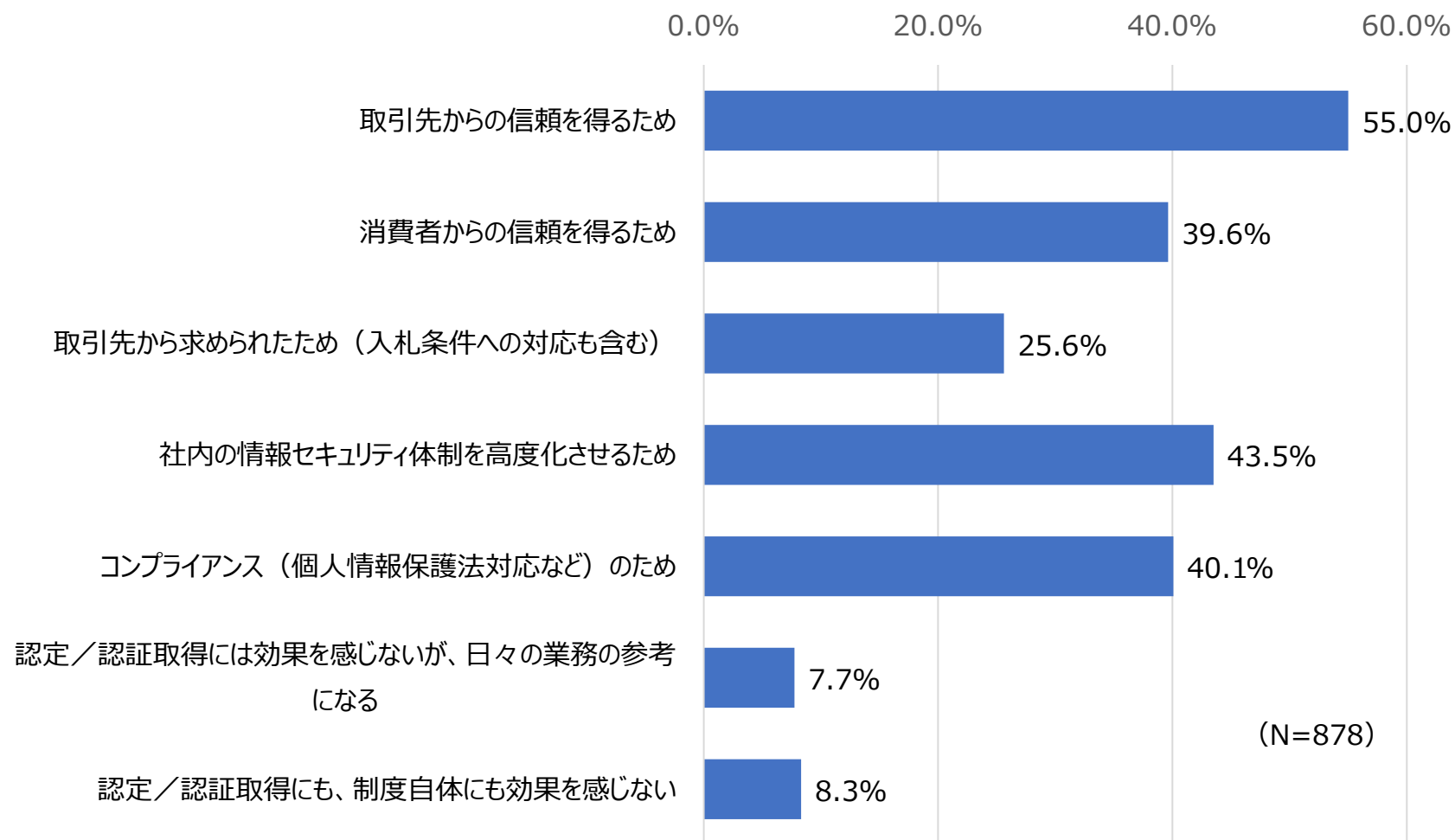


Q4_2：情報セキュリティに関する認定/認証制度の取組み状況

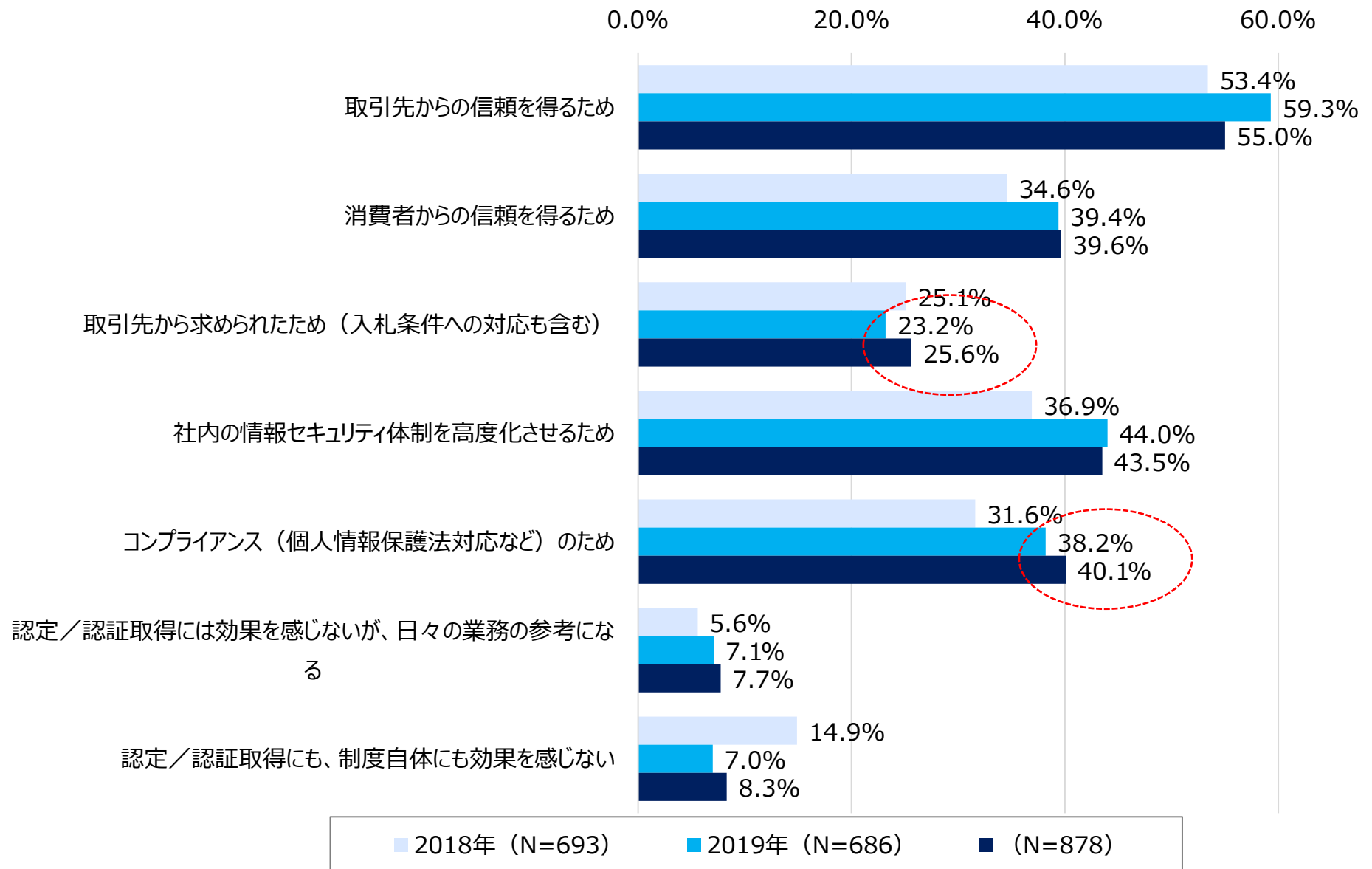


Q4_3：第三者から認定/認証を取得することの価値（効果）

- 昨年同様「取引先から信頼を得るため」が最も多いが、比率はやや低下し、「取引先から求められたため」と「コンプライアンスのため」が2019年よりも若干増加している。



Q4_3：第三者から認定/認証を取得することの価値（効果）（2018～2020年比較）



Q4_3：第三者から認定/認証を取得することの価値

業種別

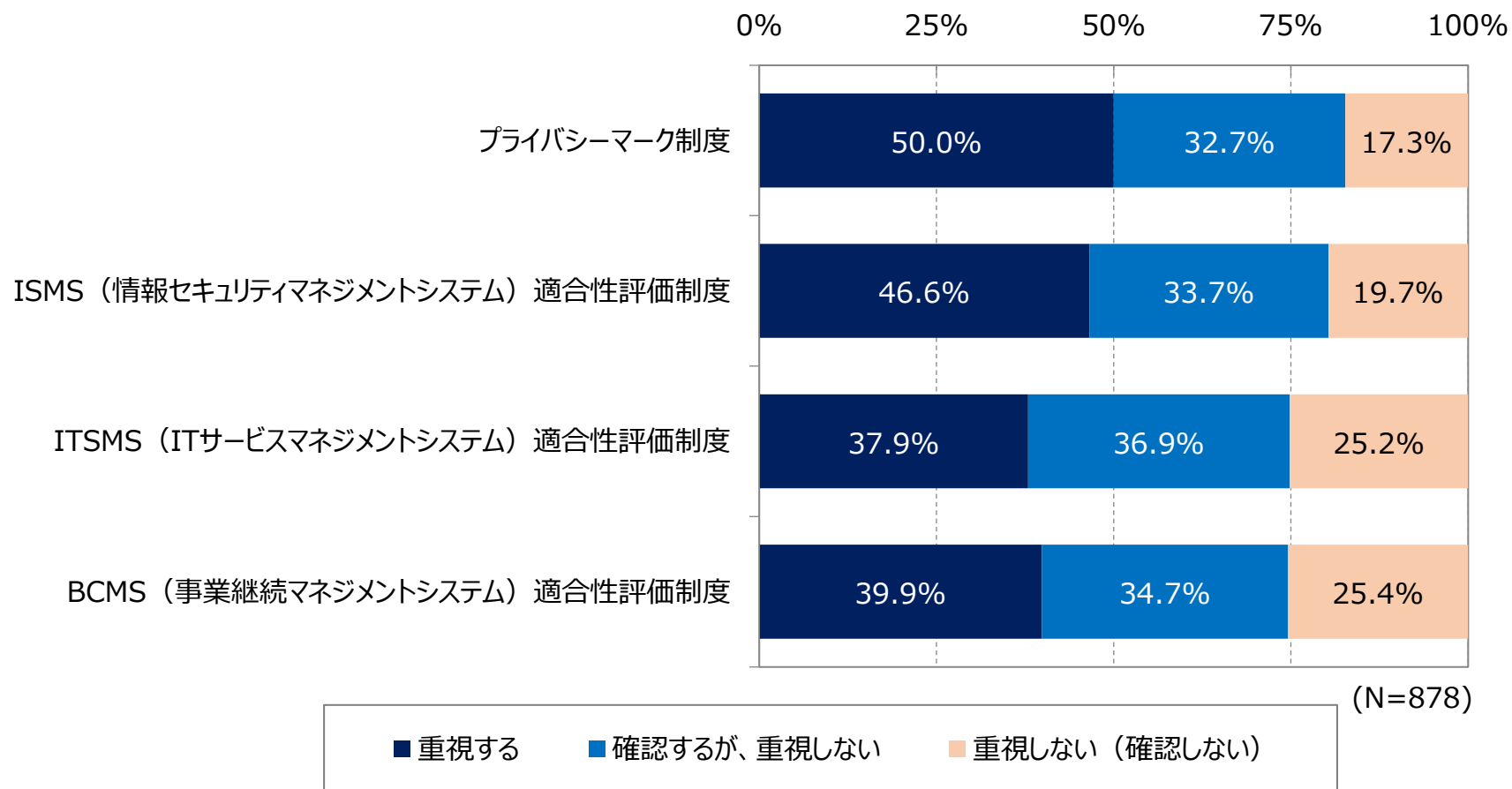
	製造 (N=264)	建設・不動産 (N=73)	卸売・小売 (N=68)	金融・保険 (N=59)	情報通信 (N=161)	サービス (N=207)	公共・その他 (N=46)	全体 (N=878)
取引先からの信頼を得るため	59.5%	65.8%	44.1%	57.6%	71.4%	38.6%	41.3%	55.0%
消費者からの信頼を得るため	33.7%	37.0%	45.6%	64.4%	37.9%	38.6%	47.8%	39.6%
取引先から求められたため（入札条件への対応も含む）	29.2%	31.5%	16.2%	20.3%	34.8%	19.3%	13.0%	25.6%
社内の情報セキュリティ体制を高度化させるため	40.9%	46.6%	39.7%	55.9%	47.8%	38.6%	50.0%	43.5%
コンプライアンス（個人情報保護法対応など）のため	37.9%	34.2%	39.7%	55.9%	41.6%	39.1%	41.3%	40.1%
認定／認証取得には効果を感じないが、日々の業務の参考になる	6.8%	12.3%	4.4%	8.5%	7.5%	8.7%	6.5%	7.7%
認定／認証取得にも、制度自体にも効果を感じない	7.6%	9.6%	7.4%	3.4%	2.5%	14.5%	10.9%	8.3%

従業員数規模別

	5,000人以上 (N=197)	1,000～4,999人 (N=197)	300～999人 (N=215)	50～299人 (N=269)	全体 (N=878)
取引先からの信頼を得るため	58.9%	58.9%	55.3%	49.1%	55.0%
消費者からの信頼を得るため	48.2%	43.7%	38.6%	31.2%	39.6%
取引先から求められたため（入札条件への対応も含む）	35.0%	26.9%	24.2%	19.0%	25.6%
社内の情報セキュリティ体制を高度化させるため	49.2%	50.8%	42.8%	34.6%	43.5%
コンプライアンス（個人情報保護法対応など）のため	39.6%	43.7%	42.8%	35.7%	40.1%
認定／認証取得には効果を感じないが、日々の業務の参考になる	8.6%	6.1%	5.6%	10.0%	7.7%
認定／認証取得にも、制度自体にも効果を感じない	6.1%	5.1%	6.0%	14.1%	8.3%

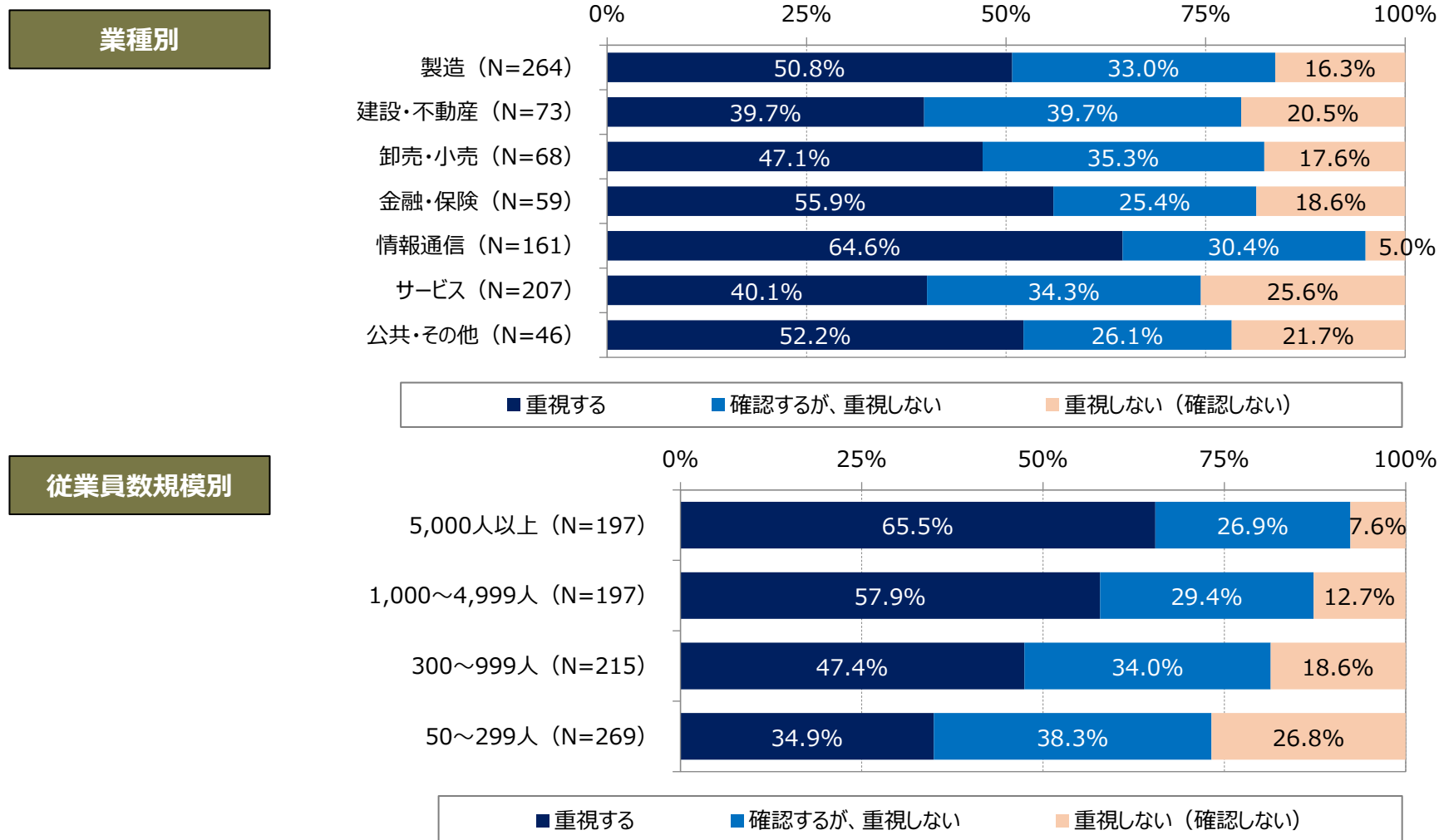
Q4_4：取引相手先を選定する際の認定／認証の有無の重視度

- 取引相手先を選定する際の認定有無の重視度は「プライバシーマーク制度」が5割に増加し、「ISMS制度」が4割強で昨年同様、ITSMSとBCMSも2019年よりも増加し、約4割となった。



Q4_4-1：取引相手先を選定する際の認証有無（プライバシーマーク制度）の重視度

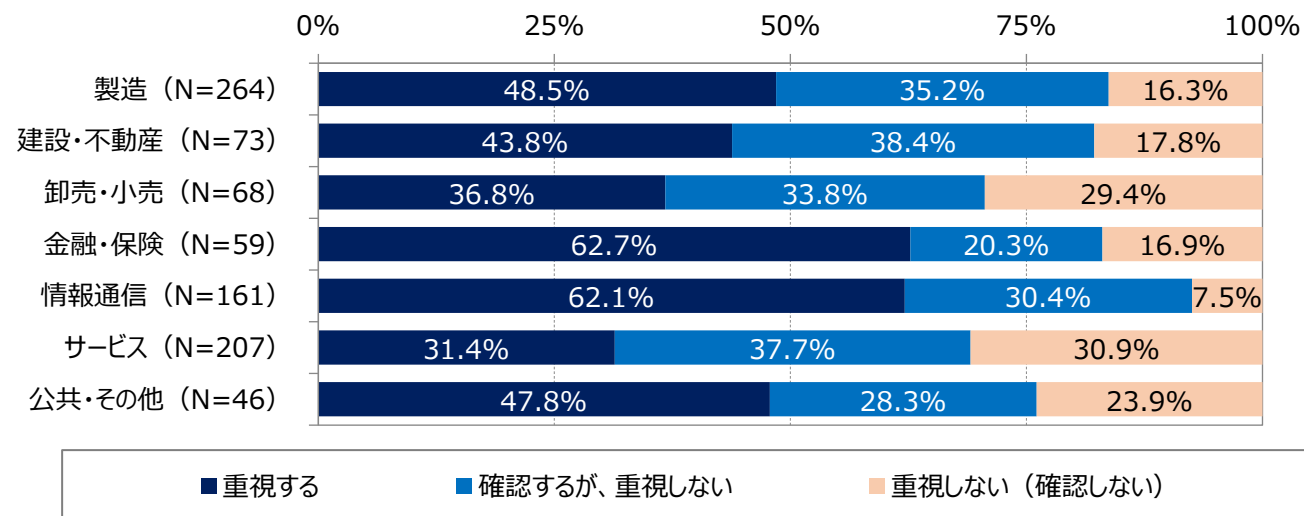
- 業種では、「情報通信」が高く、次は「金融・保険」となっている。
- 規模別では、企業規模が大きいほど重視する傾向がある。



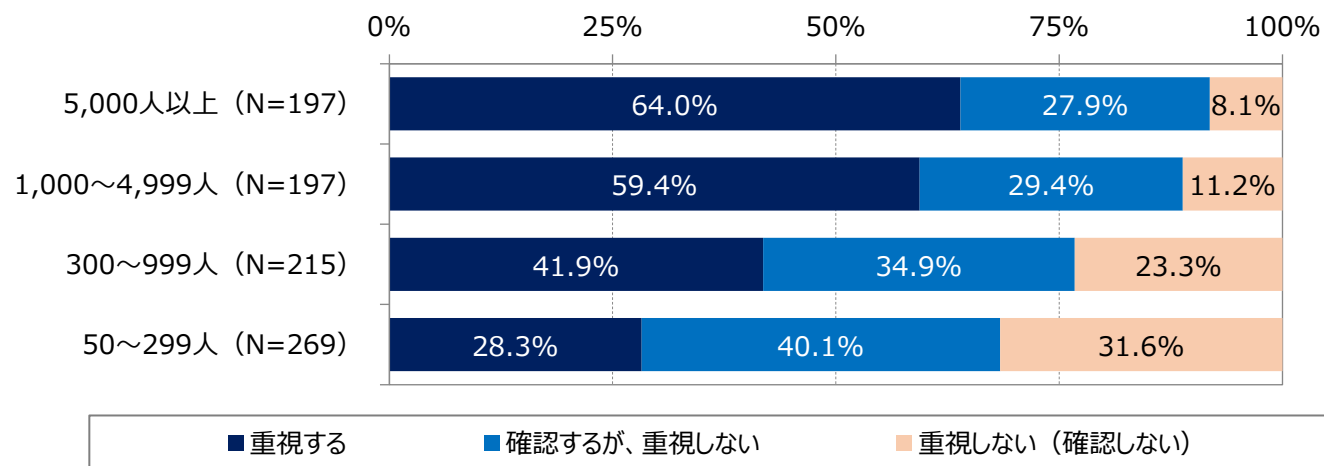
Q4_4-2：取引相手先を選定する際の認証有無（ISMS制度）の重視度

- 業種別では、重視するが「情報通信」と「金融・保険」で6割超となった。
- 規模別では規模が大きいほど重視する比率が高い傾向となった。

業種別



従業員数規模別

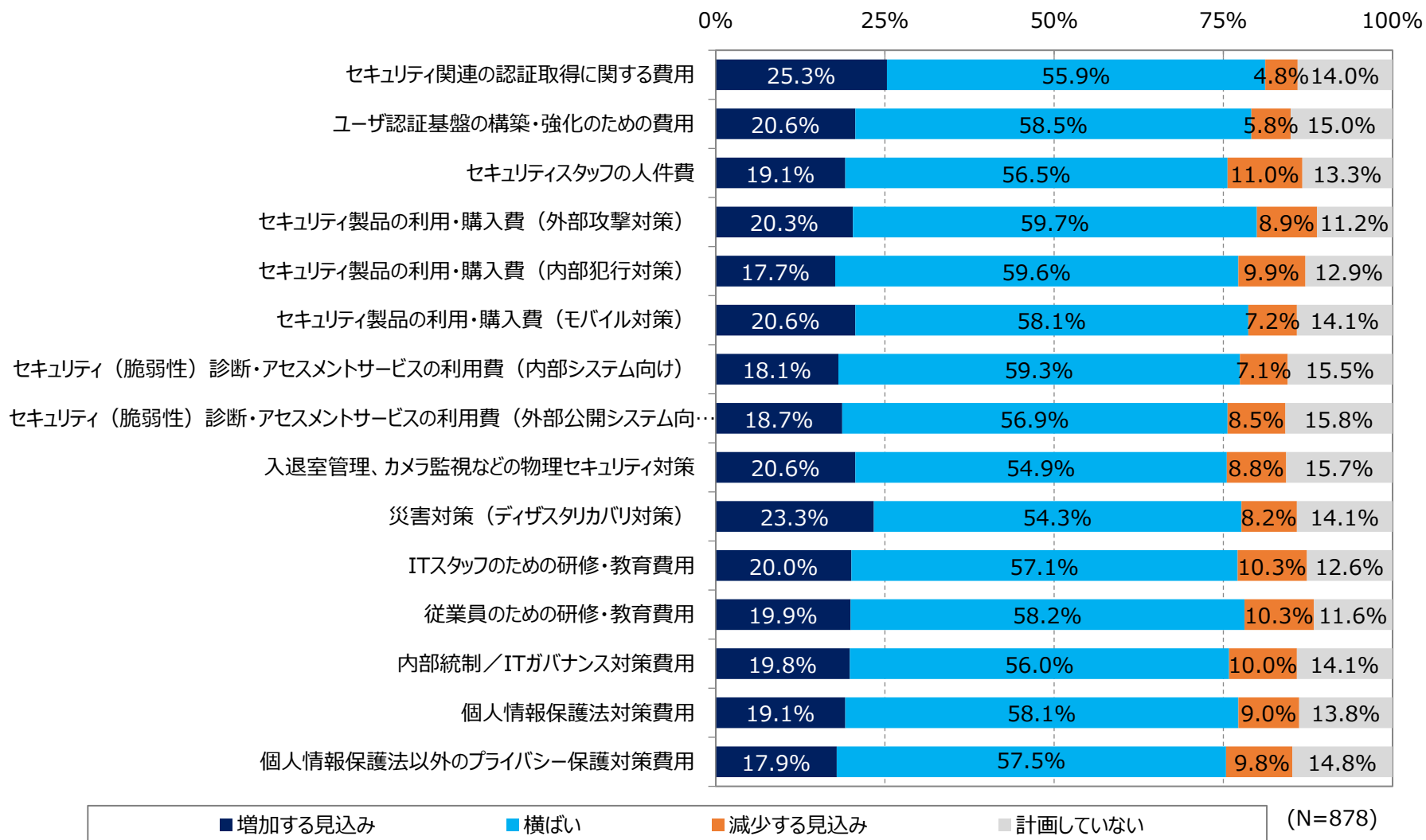


3) セキュリティ支出の動向

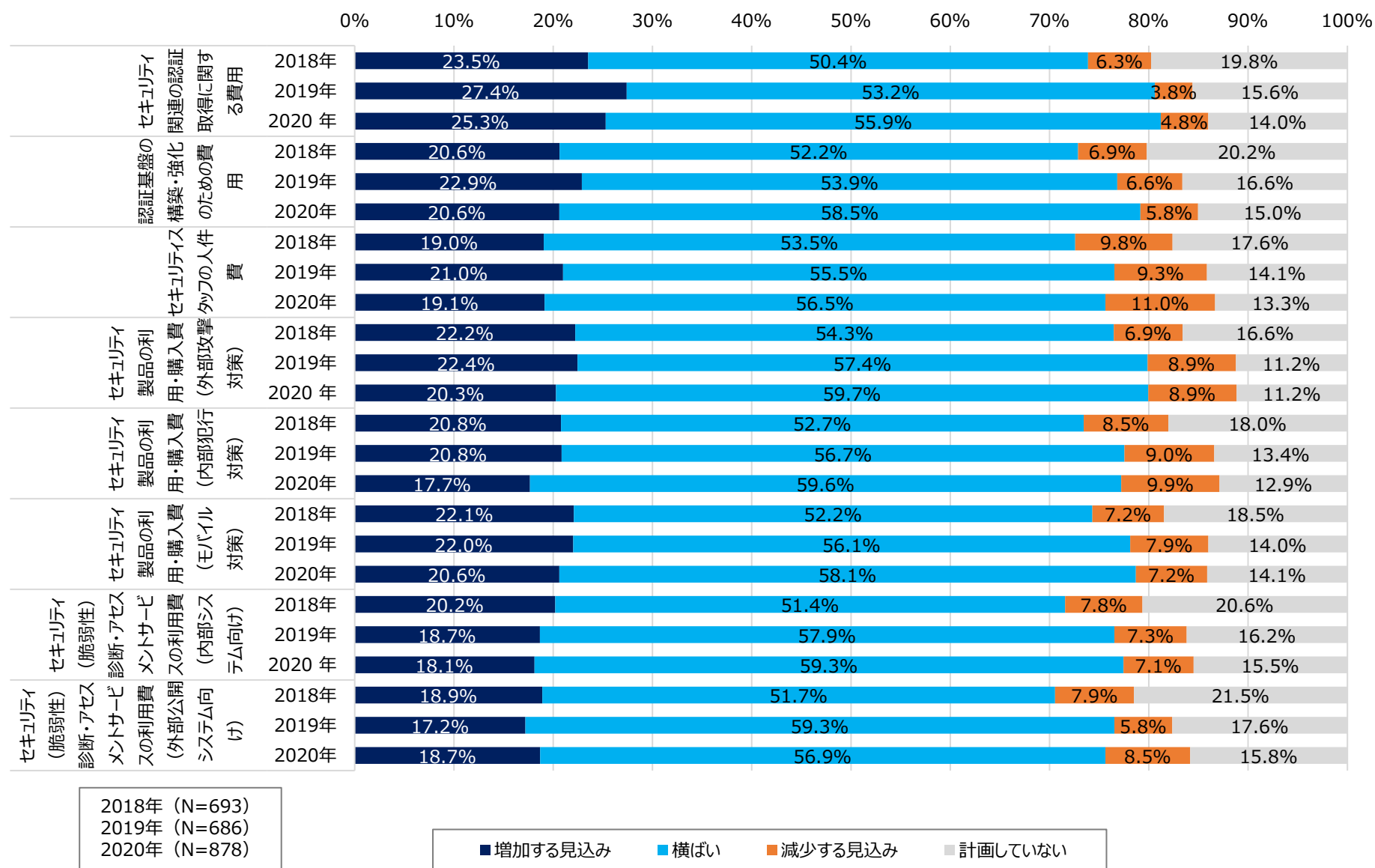
- Q5 : セキュリティ関連支出の動向

Q5：セキュリティ支出の増減傾向（2020年度見込み）

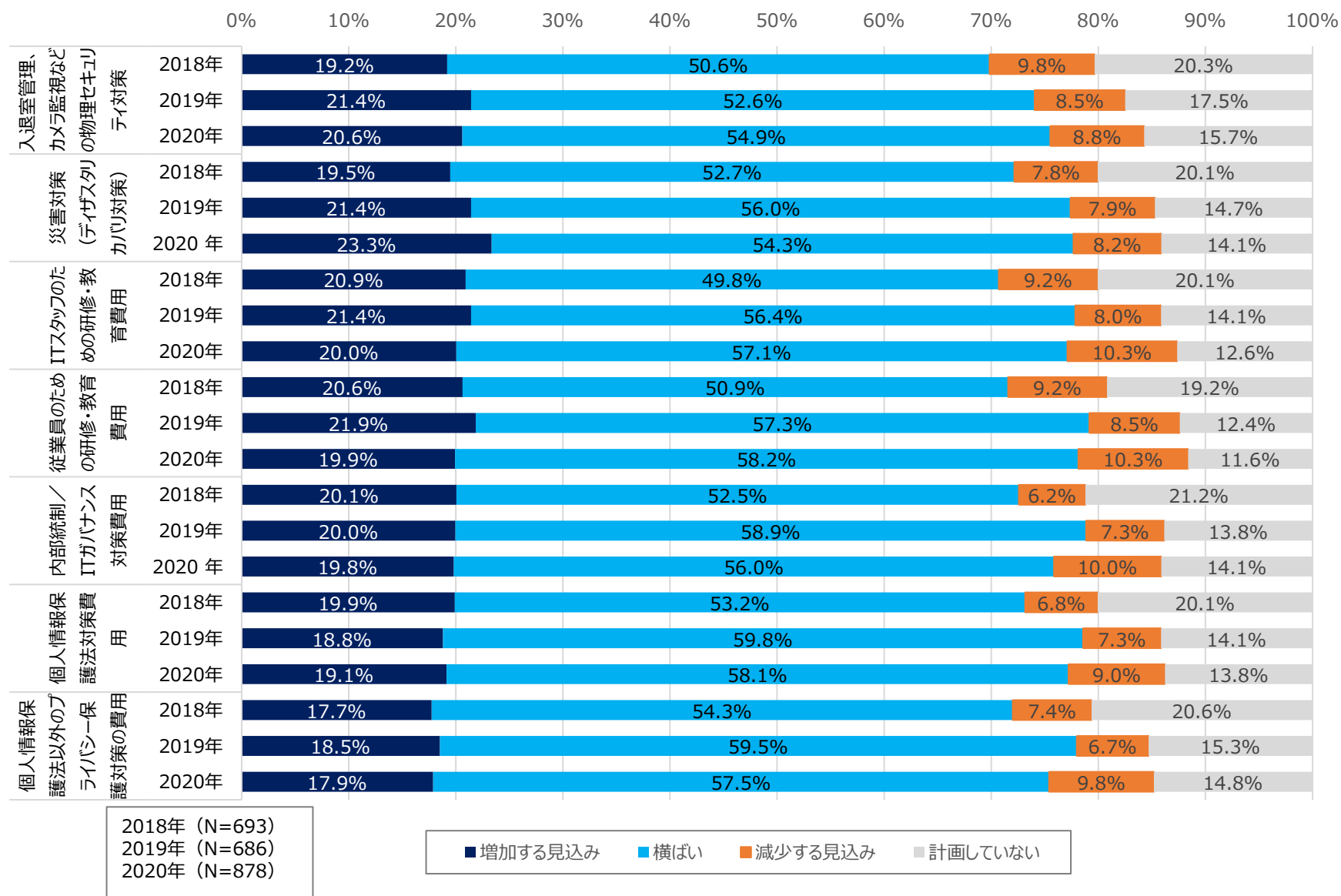
- 支出については、セキュリティ関連の認証取得に関する費用が「増加する」との回答が他の項目と比較して高いが、他の項目については「横ばい」がやや増加して5割超となっている。



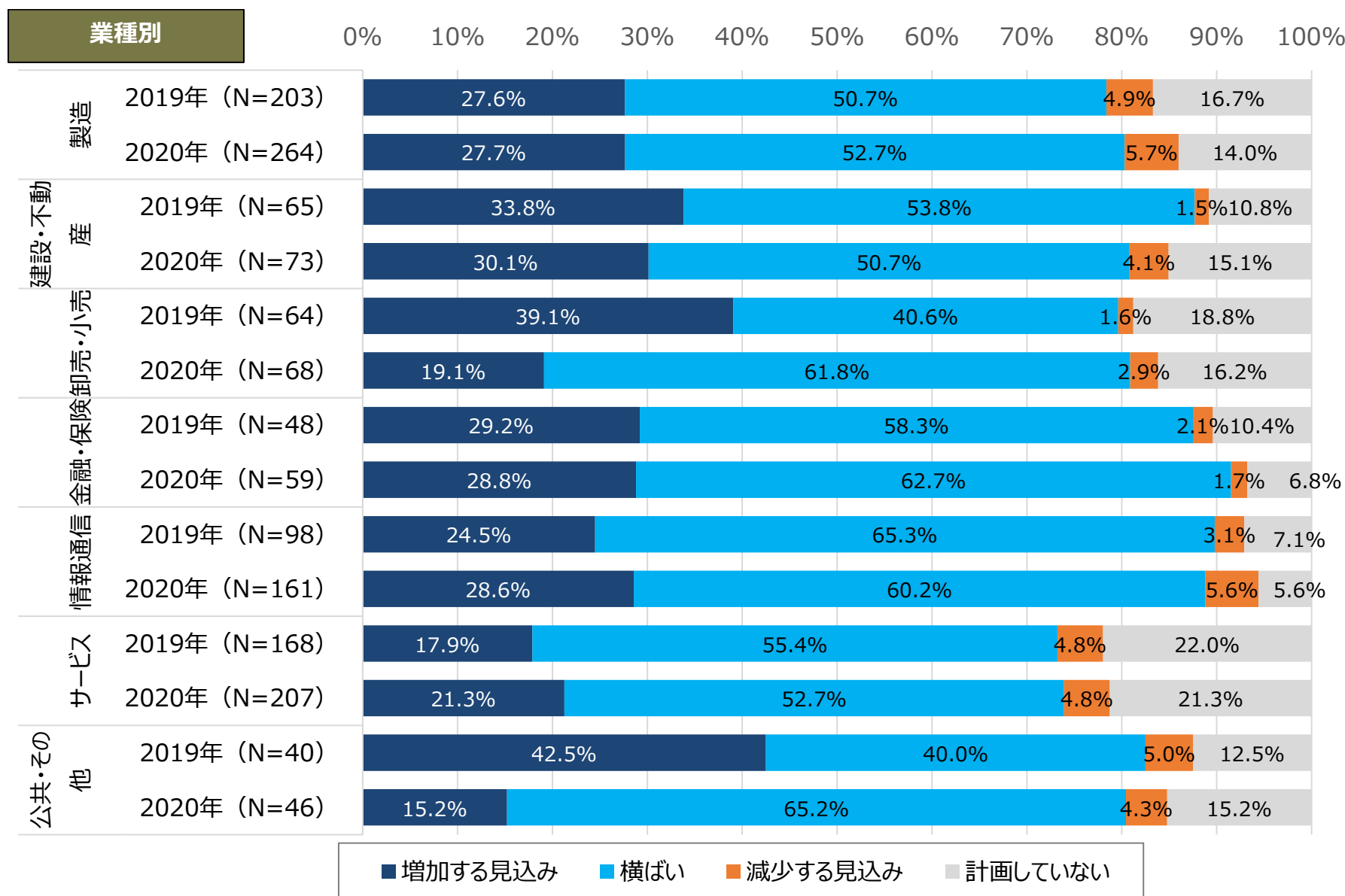
Q5：セキュリティ支出の増減傾向（翌年度見込み）（2018～2020年比較）



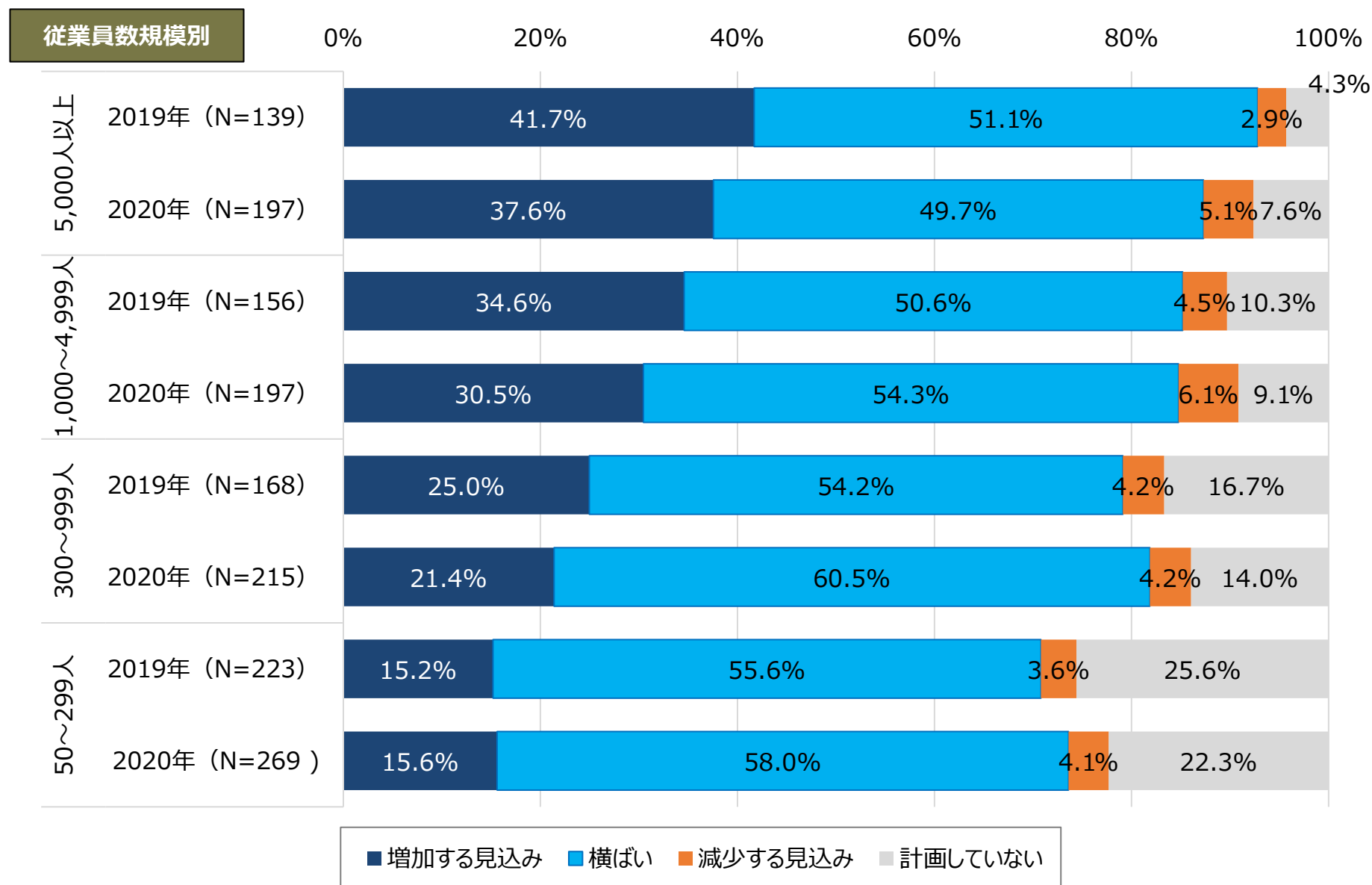
Q5：セキュリティ支出の増減傾向（翌年度見込み）（2018～2020年比較）



Q5_1 : セキュリティ関連認証取得費用（2019～2020年比較）



Q5_1：セキュリティ関連認証取得費用（2019～2020年比較）

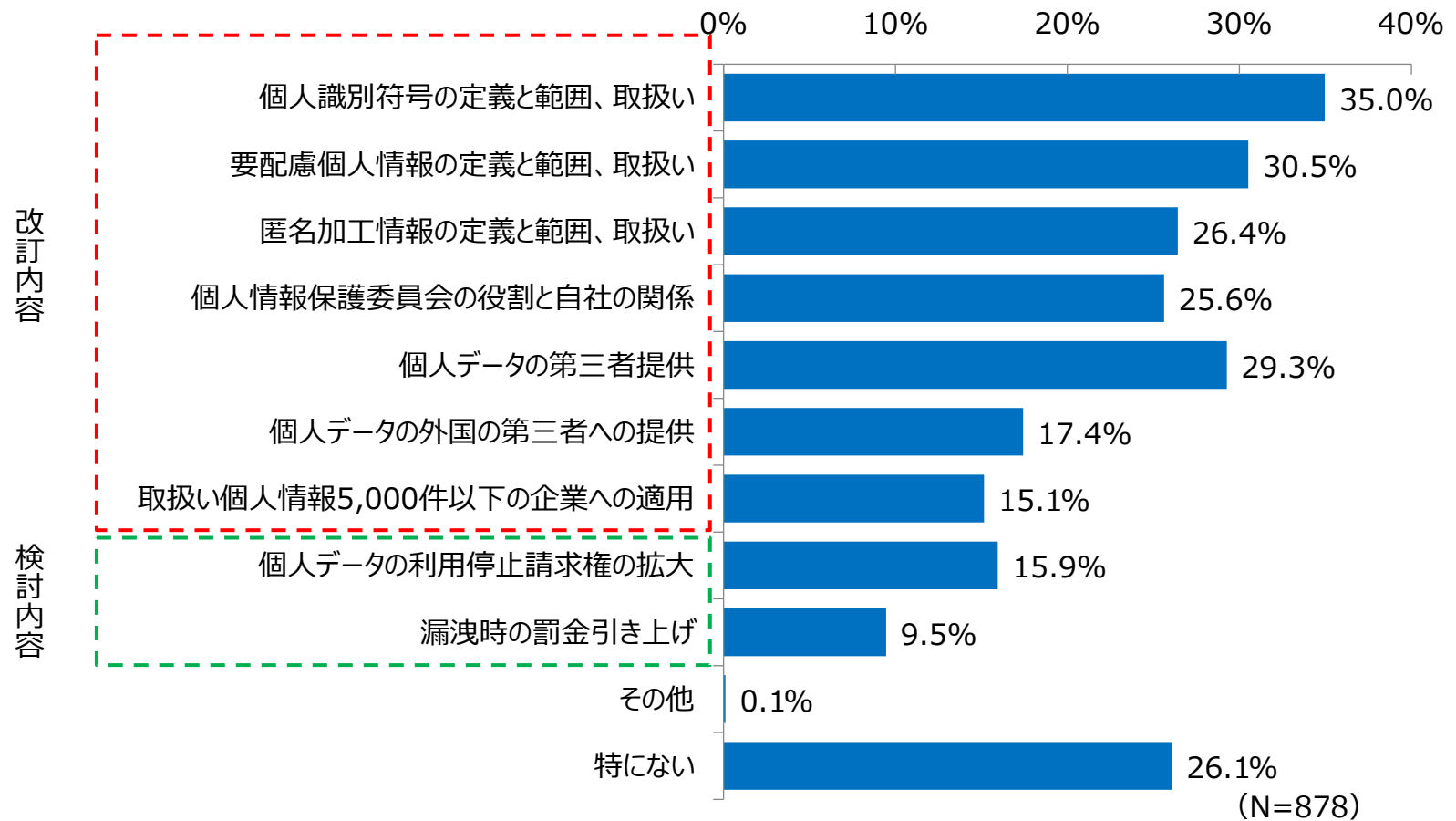


4) グローバルのセキュリティ（プライバシー）ガバナンス

- Q6 : JIS Q15001改訂および個人情報保護法改正検討内容への関心度
- Q7 : 海外のプライバシー規制について

Q6：JIS Q 15001の改訂および個人情報保護法改正検討内容についての関心

- 改訂内容では5,000件以下の適用の関心度が上がっている。
- 今回検討中の内容については利用停止請求権の拡大が約16%、漏えい時の罰金引上げが約10%という結果となった。



Q6 : JIS Q 15001の改正および個人情報保護法改正検討中の内容についての関心

■ 検討中の利用停止請求権拡大については業種別では金融・保険で高く、企業規模では1,000～4,999人で高い結果となった。

業種別

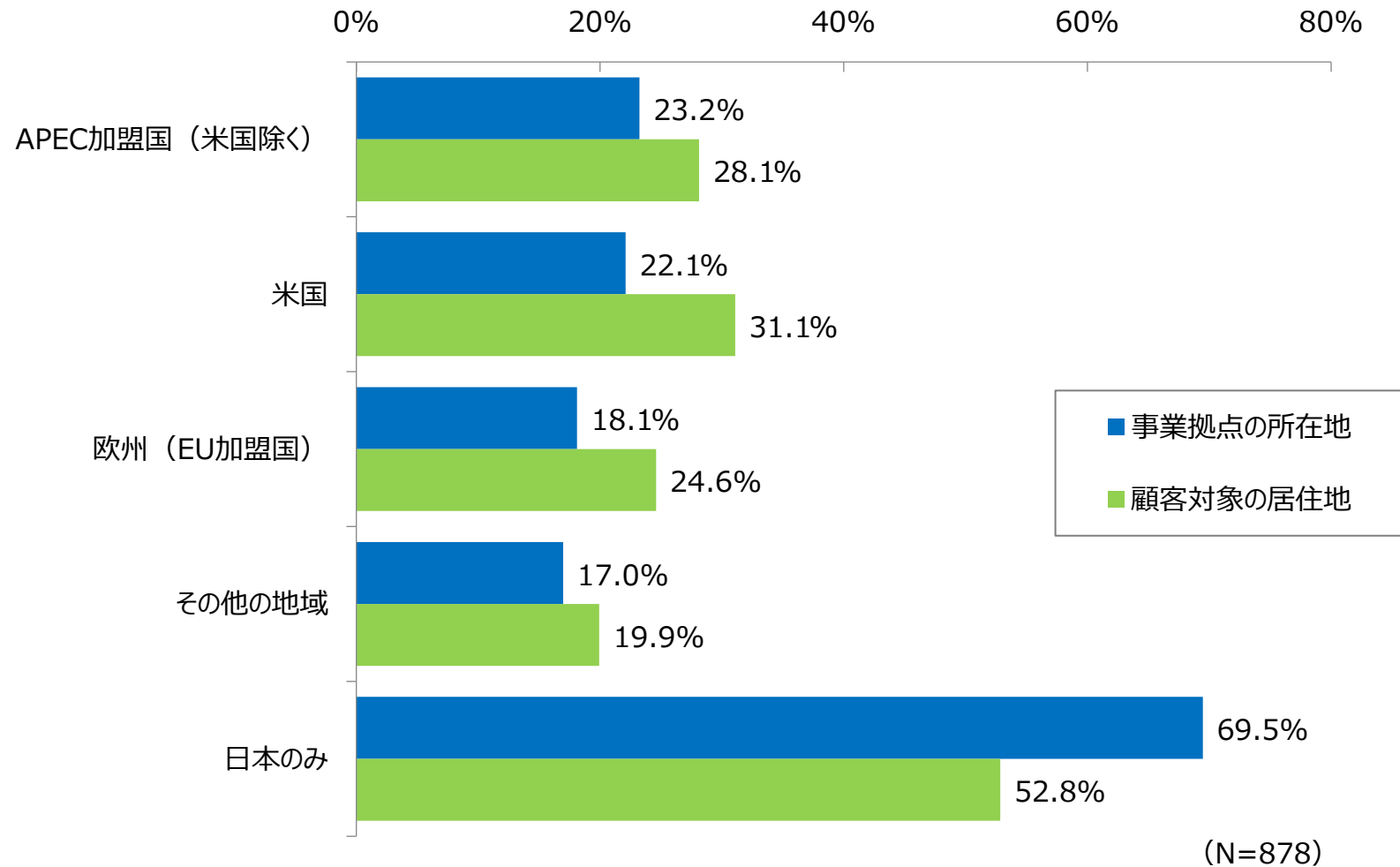
	製造 (N=264)	建設・不動産 (N=73)	卸売・小売 (N=68)	金融・保険 (N=59)	情報通信 (N=161)	サービス (N=207)	公共・その他 (N=46)	全体 (N=878)
個人識別符号の定義と範囲、取扱い	43.2%	32.9%	33.8%	35.6%	36.6%	26.1%	26.1%	35.0%
要配慮個人情報の定義と範囲、取扱い	27.7%	32.9%	26.5%	39.0%	34.2%	30.4%	26.1%	30.5%
匿名加工情報の定義と範囲、取扱い	24.2%	38.4%	23.5%	37.3%	28.0%	20.8%	30.4%	26.4%
個人情報保護委員会の役割と自社の関係	28.4%	23.3%	27.9%	39.0%	23.6%	20.3%	23.9%	25.6%
個人データの第三者提供	25.0%	32.9%	29.4%	37.3%	34.2%	25.6%	37.0%	29.3%
個人データの外国の第三者への提供	17.0%	24.7%	16.2%	23.7%	16.1%	14.0%	21.7%	17.4%
取扱い個人情報5,000件以下の企業への適用	14.0%	17.8%	20.6%	20.3%	14.9%	14.5%	6.5%	15.1%
個人データの利用停止請求権の拡大	14.0%	20.5%	17.6%	25.4%	14.9%	13.5%	19.6%	15.9%
漏えい時の罰金引き上げ	8.0%	12.3%	14.7%	13.6%	11.2%	6.3%	8.7%	9.5%
その他	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	2.2%	0.1%
特になし	20.5%	24.7%	30.9%	27.1%	19.3%	37.7%	23.9%	26.1%

従業員数規模別

	5,000人以上 (N=197)	1,000～ 4,999人 (N=197)	300～999人 (N=215)	50～299人 (N=269)	全体 (N=878)
個人識別符号の定義と範囲、取扱い	43.1%	38.1%	37.2%	24.9%	35.0%
要配慮個人情報の定義と範囲、取扱い	43.1%	32.0%	27.0%	23.0%	30.5%
匿名加工情報の定義と範囲、取扱い	31.5%	29.4%	25.1%	21.6%	26.4%
個人情報保護委員会の役割と自社の関係	33.5%	31.5%	23.7%	17.1%	25.6%
個人データの第三者提供	32.0%	32.5%	32.6%	22.3%	29.3%
個人データの外国の第三者への提供	20.8%	21.8%	17.2%	11.9%	17.4%
取扱い個人情報5,000件以下の企業への適用	14.7%	19.3%	16.3%	11.5%	15.1%
個人データの利用停止請求権の拡大	16.2%	21.8%	13.0%	13.8%	15.9%
漏えい時の罰金引き上げ	7.1%	11.7%	11.6%	7.8%	9.5%
その他	0.5%	0.0%	0.0%	0.0%	0.1%
特になし	12.7%	21.8%	23.7%	40.9%	26.1%

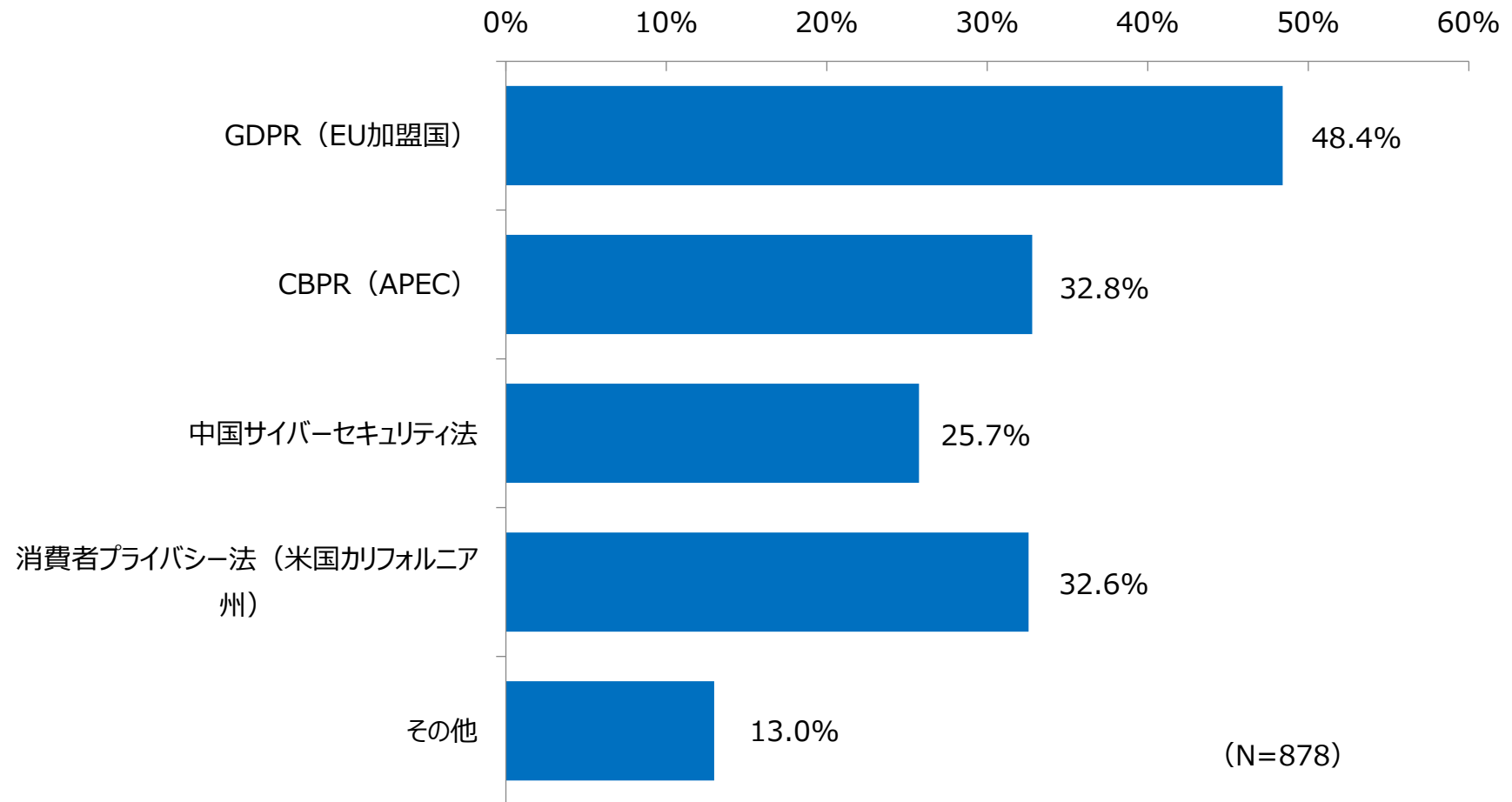
Q7_1：ビジネスを展開する地域

■ 顧客の居住地について昨年とほぼ同じだが、事業拠点についてはAPECを除く地域で若干増加する傾向がある。



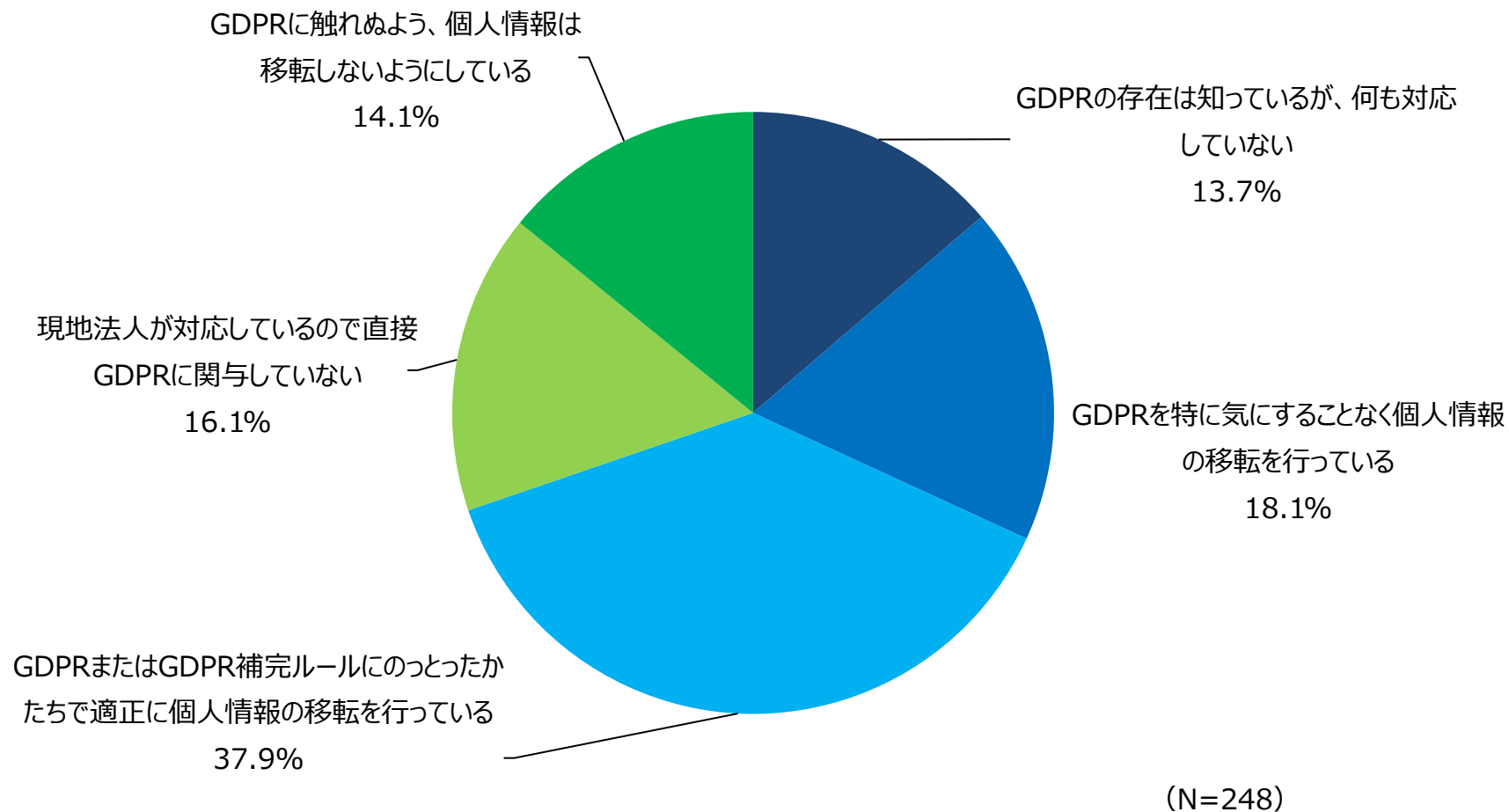
Q7_2：海外のプライバシー規制の認知度

- 海外のプライバシー規制では、2019年同様、GDPRの認知度が約5割で最も高く、その他の規制については約3割にとどまっている。



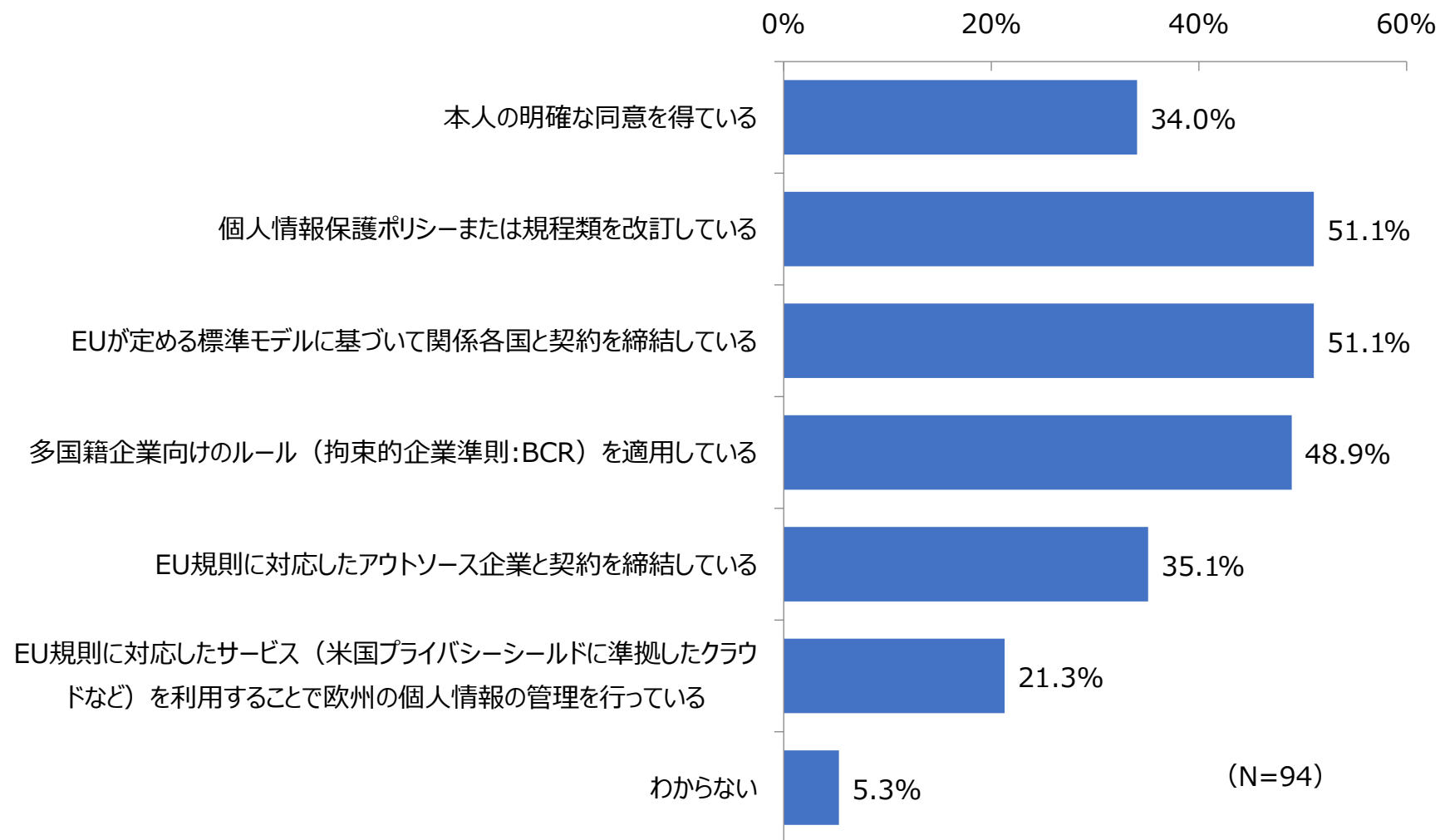
Q7_3 : GDPRの対応状況

- GDPRについては、気にせずに移転しているが若干減少し、代わってルールに則った形で移転しているが若干増加しているが、大きく変化はしていない。



Q7_4 : GDPRに則った適正移転の方法

- 「GDPRに則った適正な移転」の方法については、本人の明確な同意を得ているが減少し、EU標準モデルでの契約締結と多国籍企業向けルールの適用が増加している。

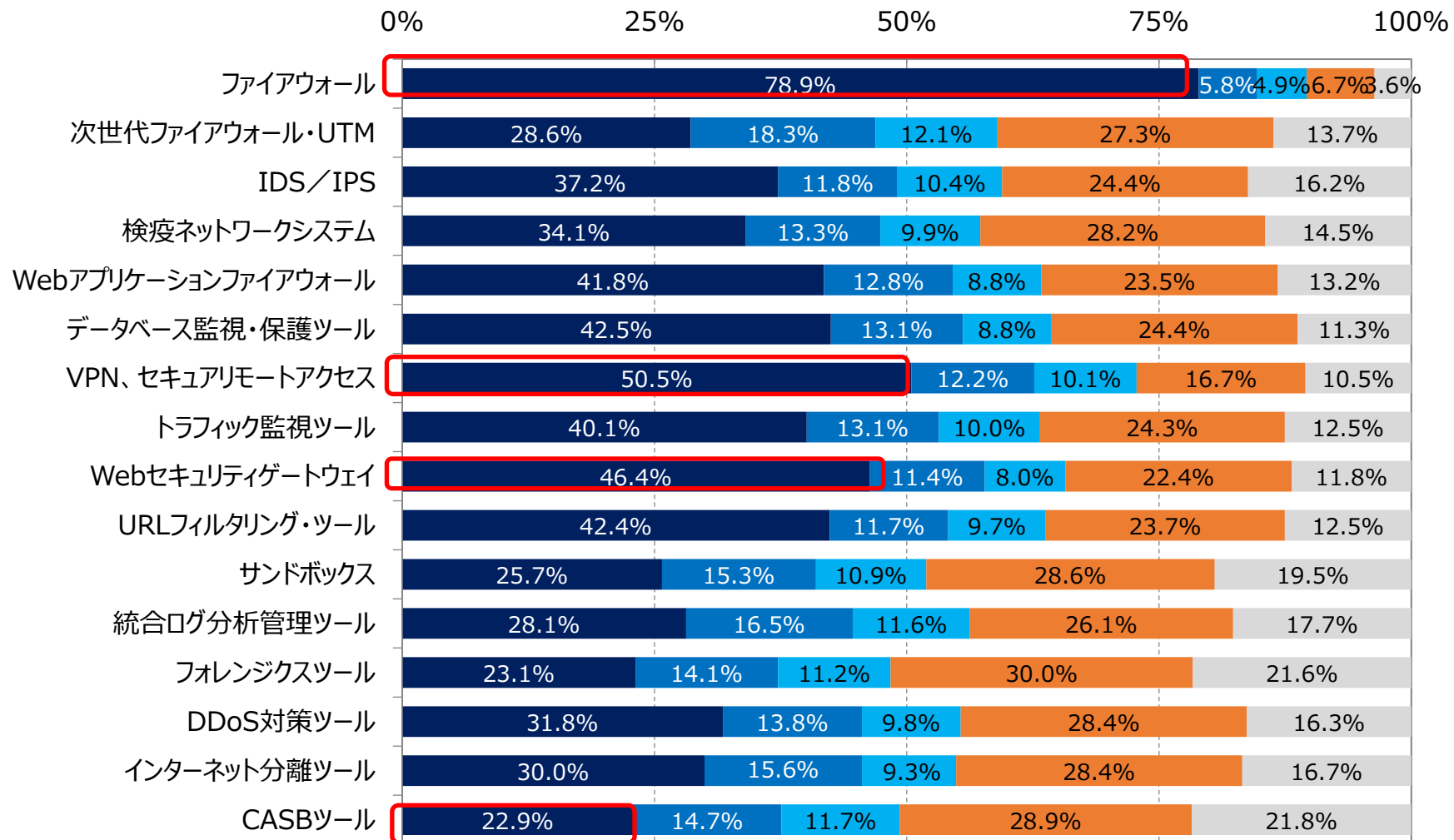


5) セキュリティ製品／技術の利用動向

- Q8 : セキュリティ製品・サービスの導入状況
- Q9 : 電子メールのセキュリティ対策状況
- Q10 : 機密性の高いシステムのアクセス認証手段

Q8_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）

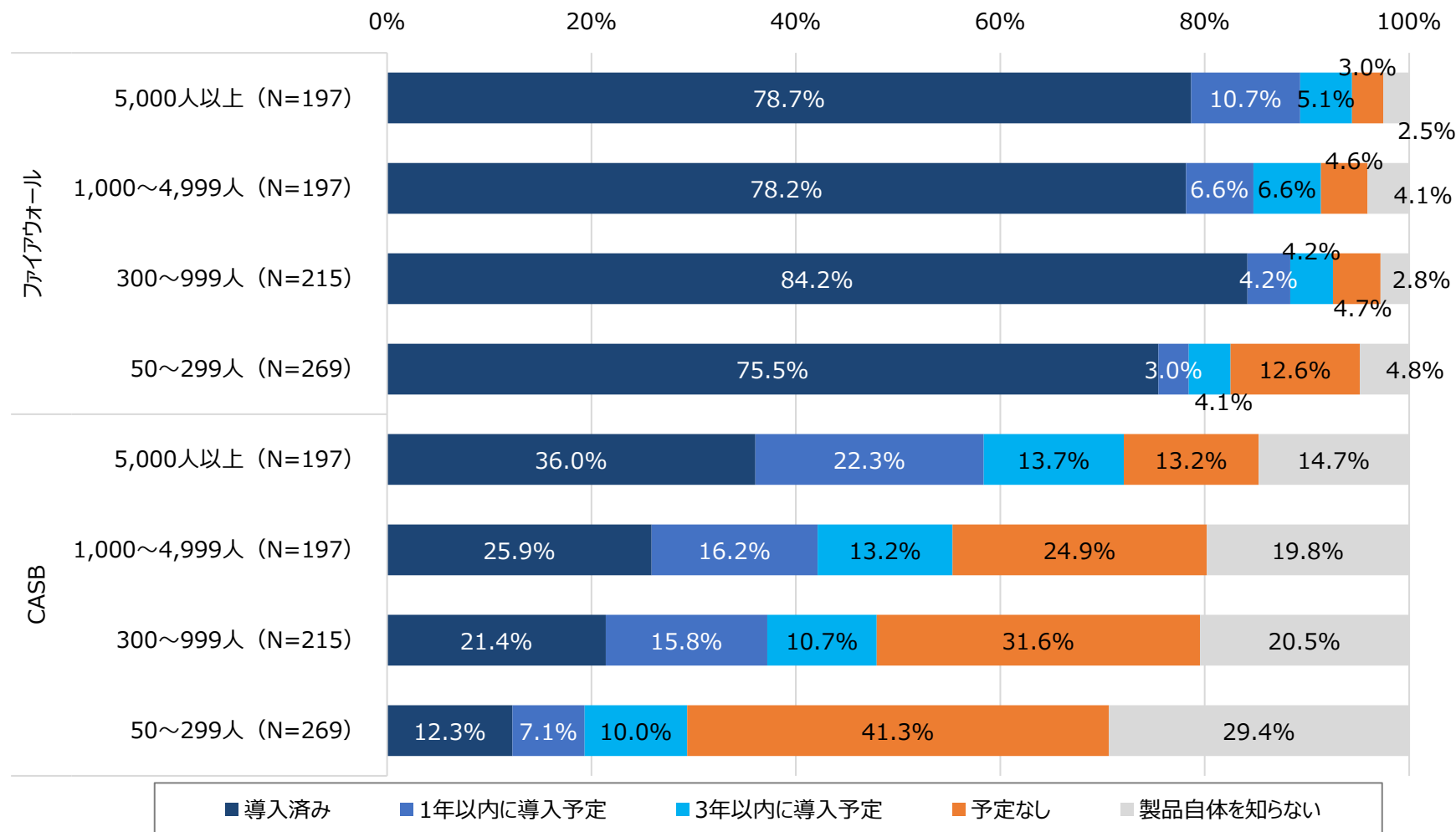
- 2019年同様、導入済が最も多いのは従来型のファイアウォールとVPNで、クラウド環境で本命視されているWebセキュアゲートウェイは高くなってきているが、CASBは低い。



■ 導入済み ■ 1年以内に導入予定 ■ 3年以内に導入予定 ■ 予定なし ■ 製品自体を知らない (N=878)

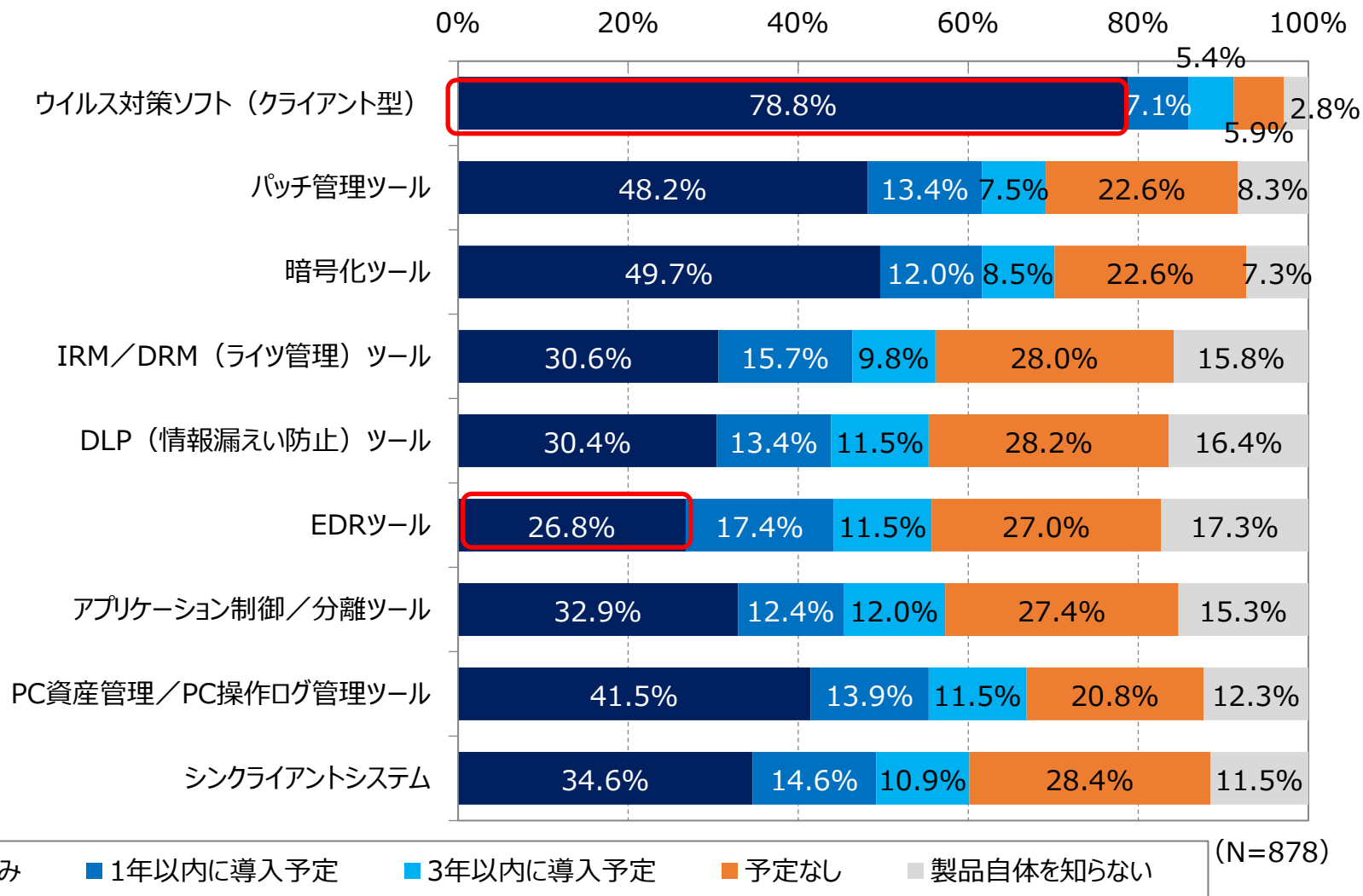
Q8_1_1：セキュリティ製品の利用状況（ネットワーク/ゲートウェイ系） ファイアウォールとCASBでの比較（従業員数規模別）

- 2019年同様、従来型のファイアウォールでは企業規模での差は大きくないが、次世代型のCASBでは企業規模が大きいほど導入が進んでいる。



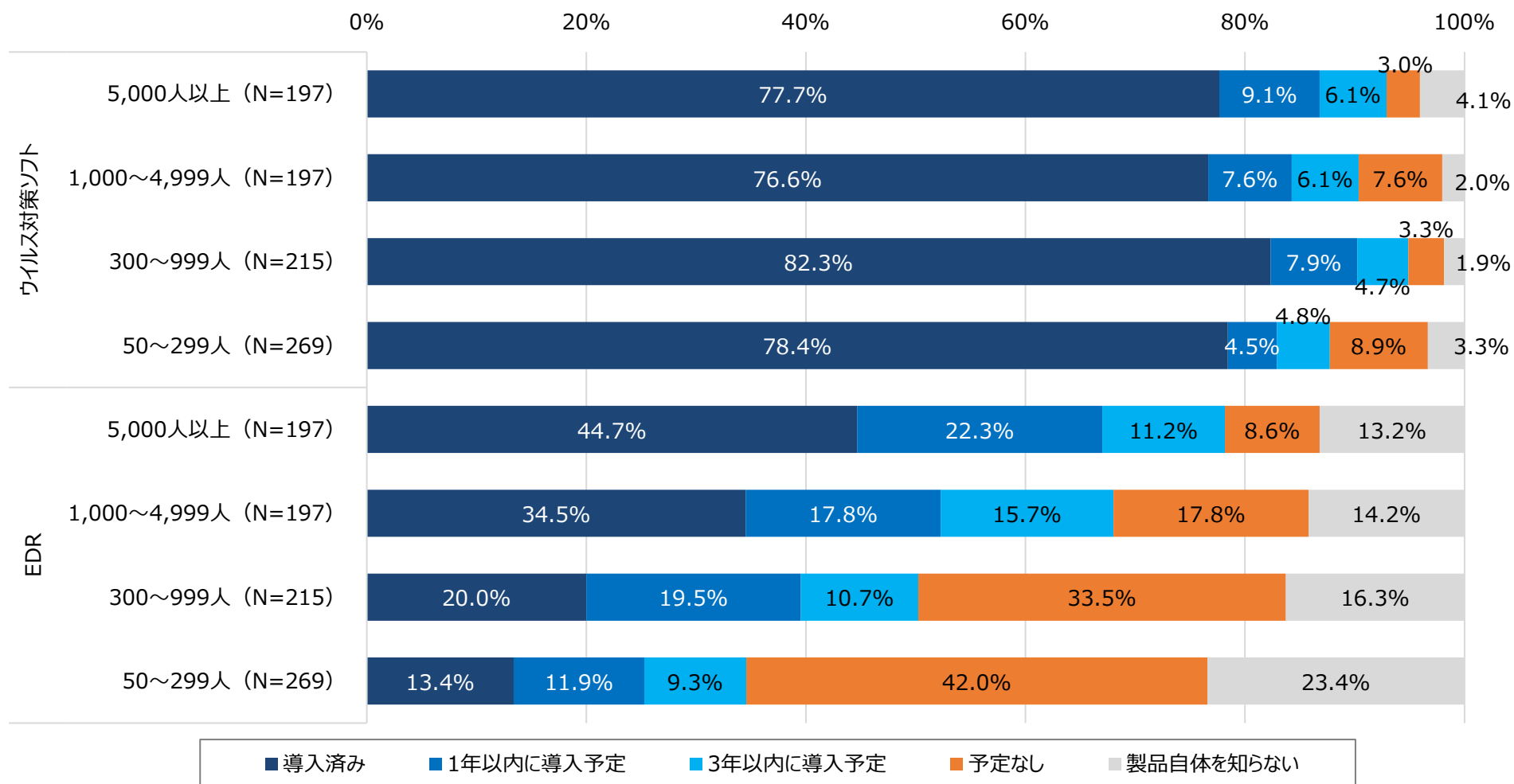
Q8_2：セキュリティ製品の利用状況（エンドポイント対策）

■ 導入済が最も多いのは従来型のウイルス対策ソフトで、次世代型のEDRの比率はまだ低いが、2019年よりも若干増加している。



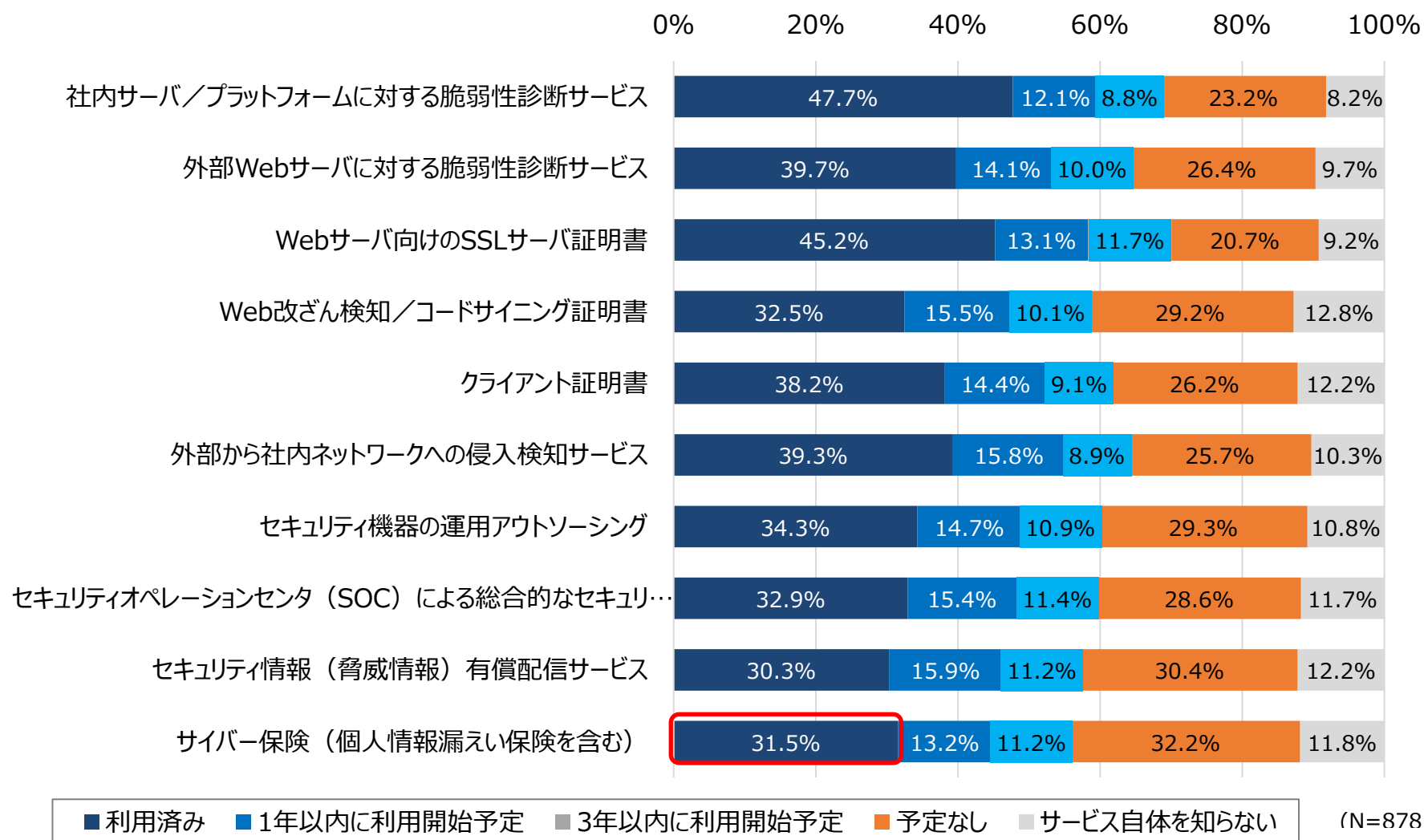
Q8_2_1：セキュリティ製品の利用状況（エンドポイント対策） ウイルス対策ソフトとEDRでの比較（従業員数規模別）

■ 従来型のウイルス対策ソフトでは規模での差は大きくないが、次世代型のEDRでは大企業ほど導入が進んでいる。

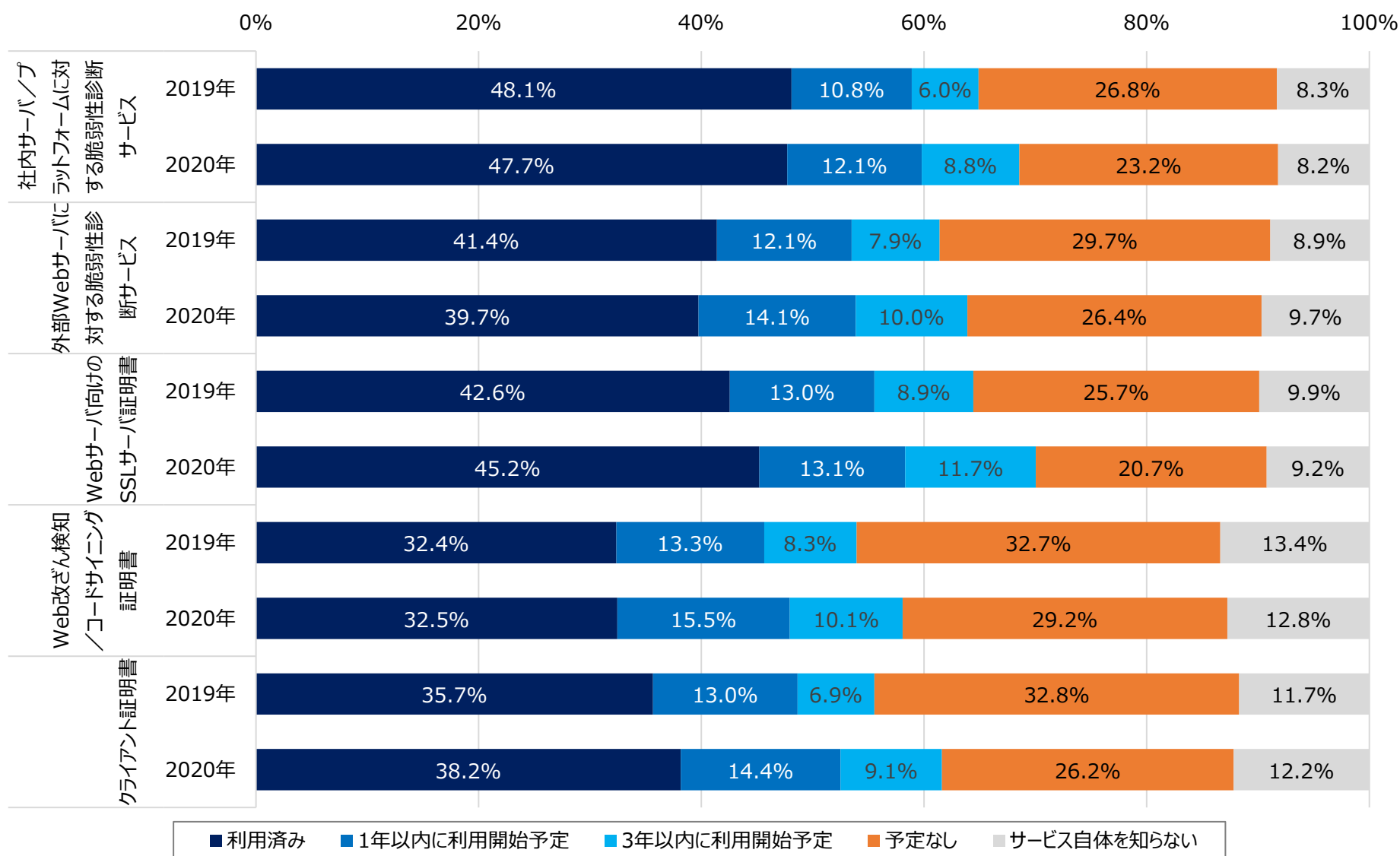


Q8_3：セキュリティ製品の利用状況（セキュリティサービス）

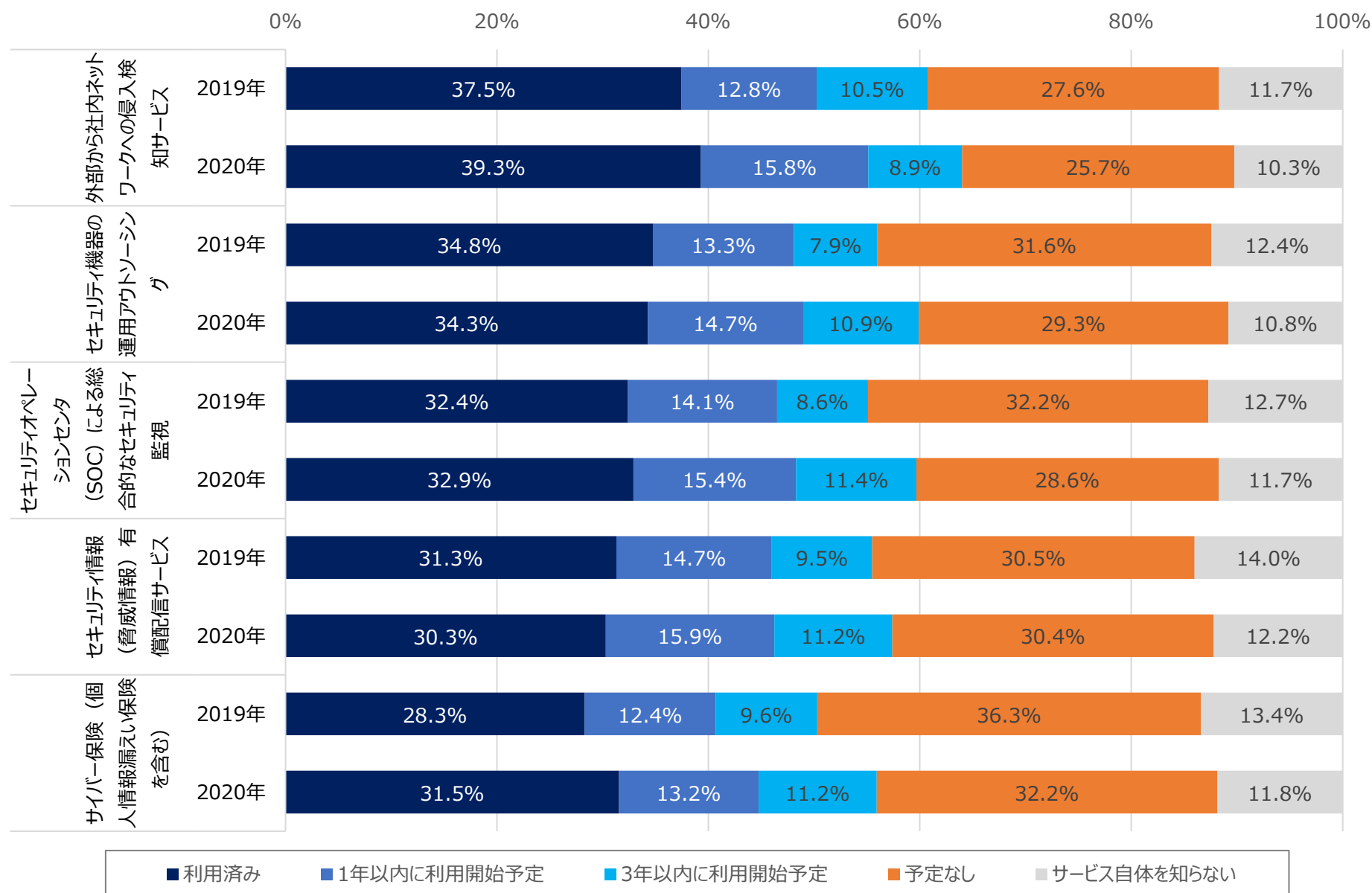
- 2019年同様、導入済が最も多いのは「脆弱性診断サービス」と「証明書サービス」で、「サイバー保険」の比率は約3割だが、2019年より若干増加している。



Q8_3：セキュリティ製品の利用状況（セキュリティサービス）

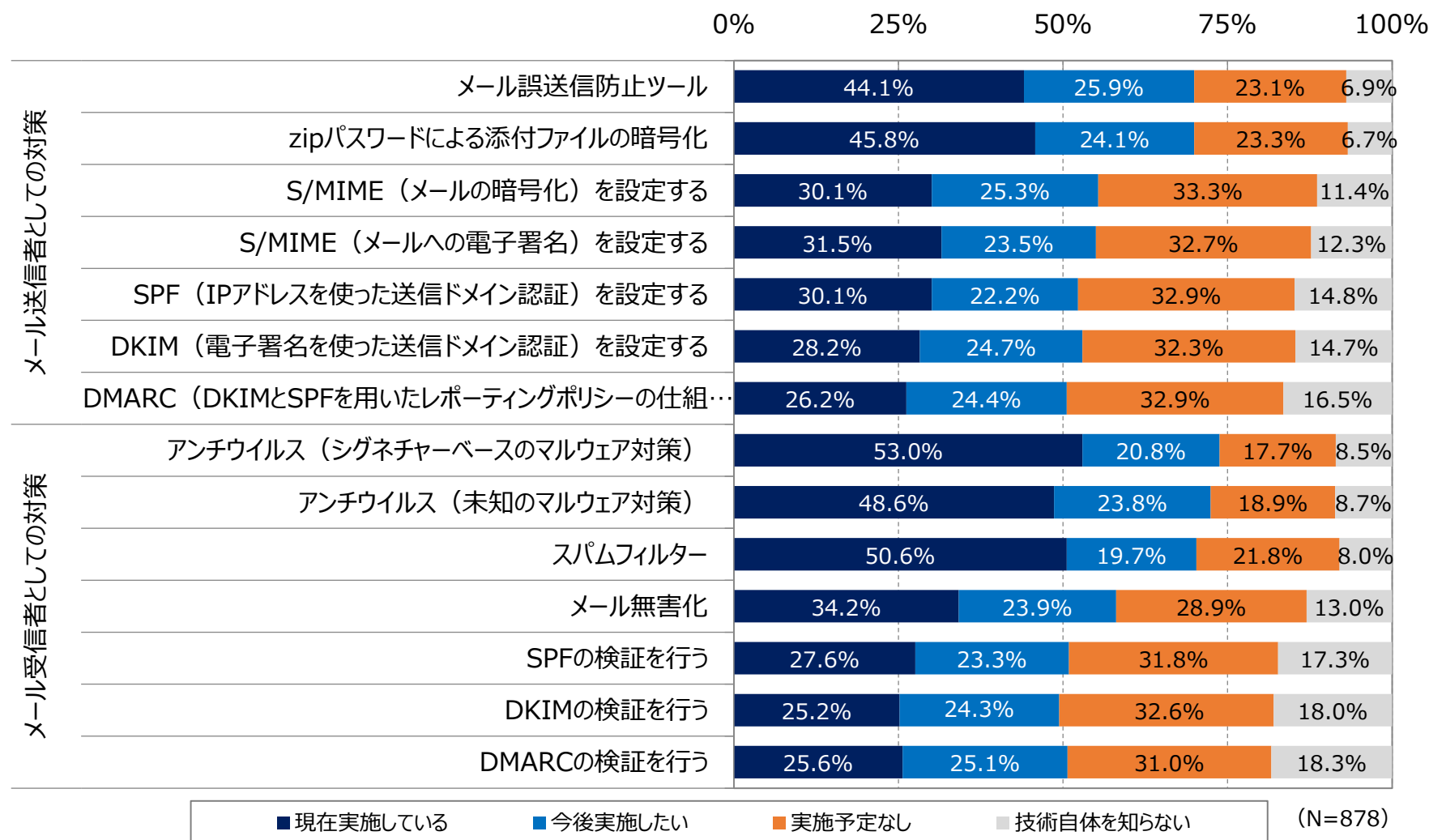


Q8_3：セキュリティ製品の利用状況（セキュリティサービス）



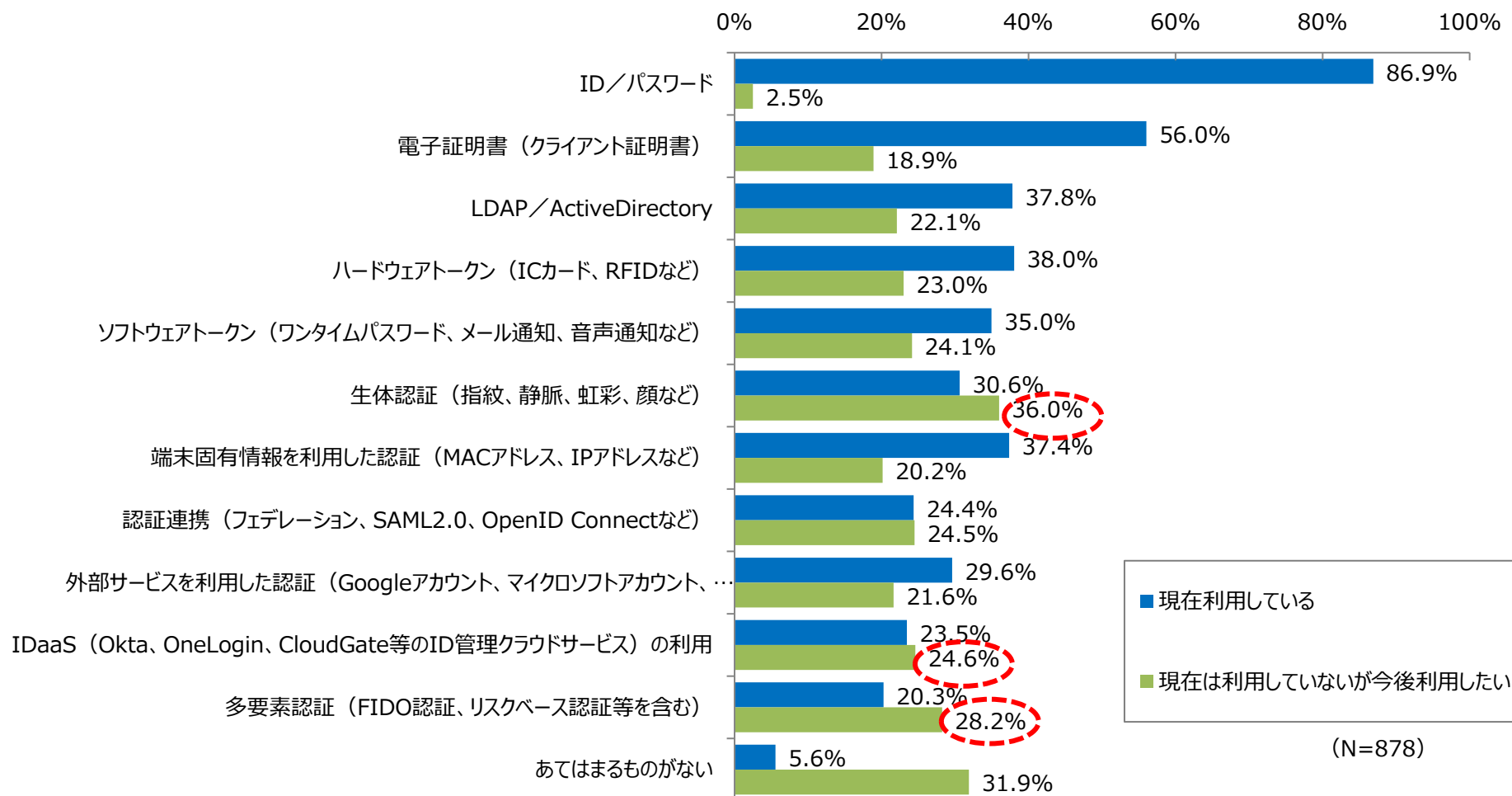
Q9：電子メールのセキュリティ対策状況

- 2019年調査同様、送信者としての対策は「誤送信防止ツール」と「添付ファイル暗号化」が多く、受信者としては「アンチウイルス」と「スパムフィルター」が多い。



Q10：高機密システムへのアクセス認証手段

- 現行の認証手段はID/パスワードが圧倒的に多いが、今後「生体認証」や「多要素認証（FIDO認証）」、「IDaaS」などの新しい認証手段を利用したいとの回答が増えている。



Q10_1：高機密システムへのアクセス認証手段の利用状況（業種別）

■ 業種別では、「金融・保険」や「情報通信」でID/パスワード以外のアクセス認証手段の普及比率が高いことがわかる。

	製造 (N=264)	建設・不動産 (N=73)	卸売・小売 (N=68)	金融・保険 (N=59)	情報通信 (N=161)	サービス (N=207)	公共・その他 (N=46)	全体 (N=878)
ID/パスワード	83.3%	84.9%	83.8%	93.2%	91.3%	86.0%	95.7%	86.9%
電子証明書（クライアント証明書）	57.6%	56.2%	58.8%	71.2%	60.2%	45.9%	54.3%	56.0%
LDAP/ActiveDirectory	38.3%	38.4%	33.8%	50.8%	53.4%	23.2%	34.8%	37.8%
ハードウェアトークン（ICカード、RFIDなど）	36.7%	39.7%	29.4%	57.6%	44.1%	31.9%	37.0%	38.0%
ソフトウェアトークン（ワンタイムパスワード、メール通知、音声通知など）	35.2%	30.1%	25.0%	52.5%	42.2%	30.4%	28.3%	35.0%
生体認証（指紋、静脈、虹彩、顔など）	29.2%	26.0%	23.5%	39.0%	42.2%	23.7%	37.0%	30.6%
端末固有情報を利用した認証（MACアドレス、IPアドレスなど）	37.9%	34.2%	33.8%	49.2%	46.0%	27.5%	43.5%	37.4%
認証連携（フェデレーション、SAML2.0、OpenID Connectなど）	22.3%	20.5%	22.1%	37.3%	32.9%	20.3%	17.4%	24.4%
外部サービスを利用した認証（Googleアカウント、マイクロソフトアカウント、Facebookアカウントなど）	28.4%	27.4%	33.8%	44.1%	37.3%	21.3%	26.1%	29.6%
IDaaS（Okta、OneLogin、CloudGate等のID管理クラウドサービス）の利用	21.6%	23.3%	22.1%	45.8%	27.3%	15.0%	32.6%	23.5%
多要素認証（FIDO認証、リスクベース認証等を含む）	17.8%	17.8%	14.7%	33.9%	30.4%	14.0%	21.7%	20.3%
あてはまるものがない	7.2%	8.2%	7.4%	1.7%	2.5%	6.3%	2.2%	5.6%

Q10_1：高機密システムへのアクセス認証手段の利用状況（従業員数規模別）

■ 規模別には、規模が大きいほどID/パスワード以外のアクセス認証手段が利用されていることがわかる。

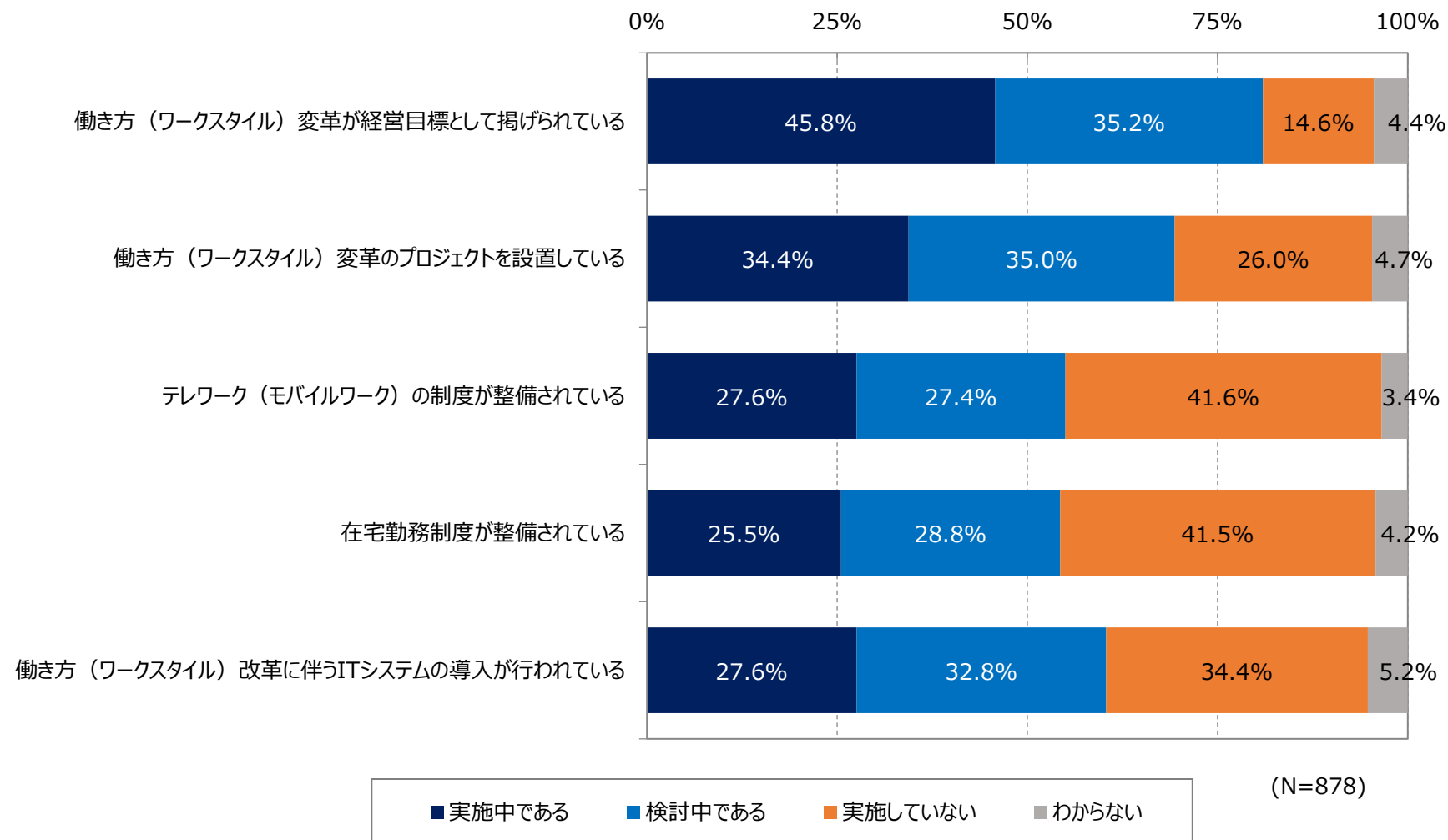
	5,000人以上 (N=197)	1,000～ 4,999人 (N=197)	300～999人 (N=215)	50～299人 (N=269)	全体 (N=878)
ID/パスワード	88.3%	87.8%	90.2%	82.5%	86.9%
電子証明書（クライアント証明書）	70.1%	69.5%	50.2%	40.5%	56.0%
LDAP/ActiveDirectory	54.8%	48.7%	31.2%	22.7%	37.8%
ハードウェア・トークン（ICカード、RFIDなど）	56.9%	49.7%	30.2%	21.9%	38.0%
ソフトウェア・トークン（ワンタイムパスワード、メール通知、音声通知など）	54.8%	44.7%	27.9%	19.0%	35.0%
生体認証（指紋、静脈、虹彩、顔など）	49.2%	30.5%	28.4%	19.0%	30.6%
端末固有情報を利用した認証（MACアドレス、IPアドレスなど）	53.3%	44.2%	32.6%	24.5%	37.4%
認証連携（フェデレーション、SAML2.0、OpenID Connectなど）	42.1%	26.9%	19.5%	13.4%	24.4%
外部サービスを利用した認証（Googleアカウント、マイクロソフトアカウント、Facebookアカウントなど）	47.7%	34.5%	24.2%	17.1%	29.6%
IDaaS（Okta、OneLogin、CloudGate等のID管理クラウドサービス）の利用	40.1%	30.5%	16.3%	11.9%	23.5%
多要素認証（FIDO認証、リスクベース認証等を含む）	36.0%	21.8%	14.9%	11.9%	20.3%
あてはまるものがない	3.0%	3.0%	4.2%	10.4%	5.6%

6) 働き方改革、クラウドの動向

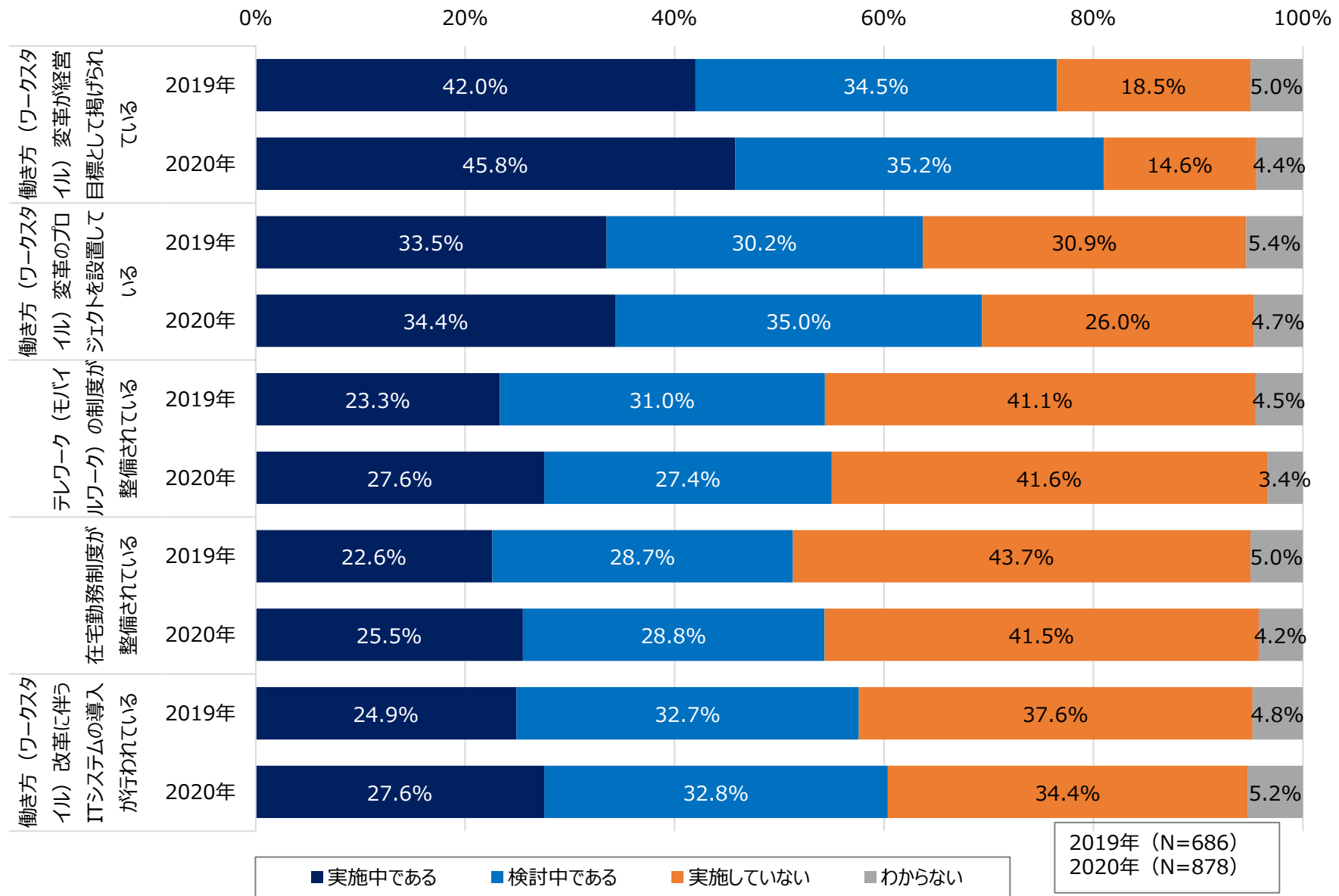
- Q11 : 働き方改革への取組み状況
ワークスタイルに関連するセキュリティ対策
- Q12 : クラウドサービスの動向

Q11_1 : 「働き方改革」に関する取組み状況（2020年）

■ 実施中の割合がすべての項目で2019年調査より増加しており、取組みが進んでいる。

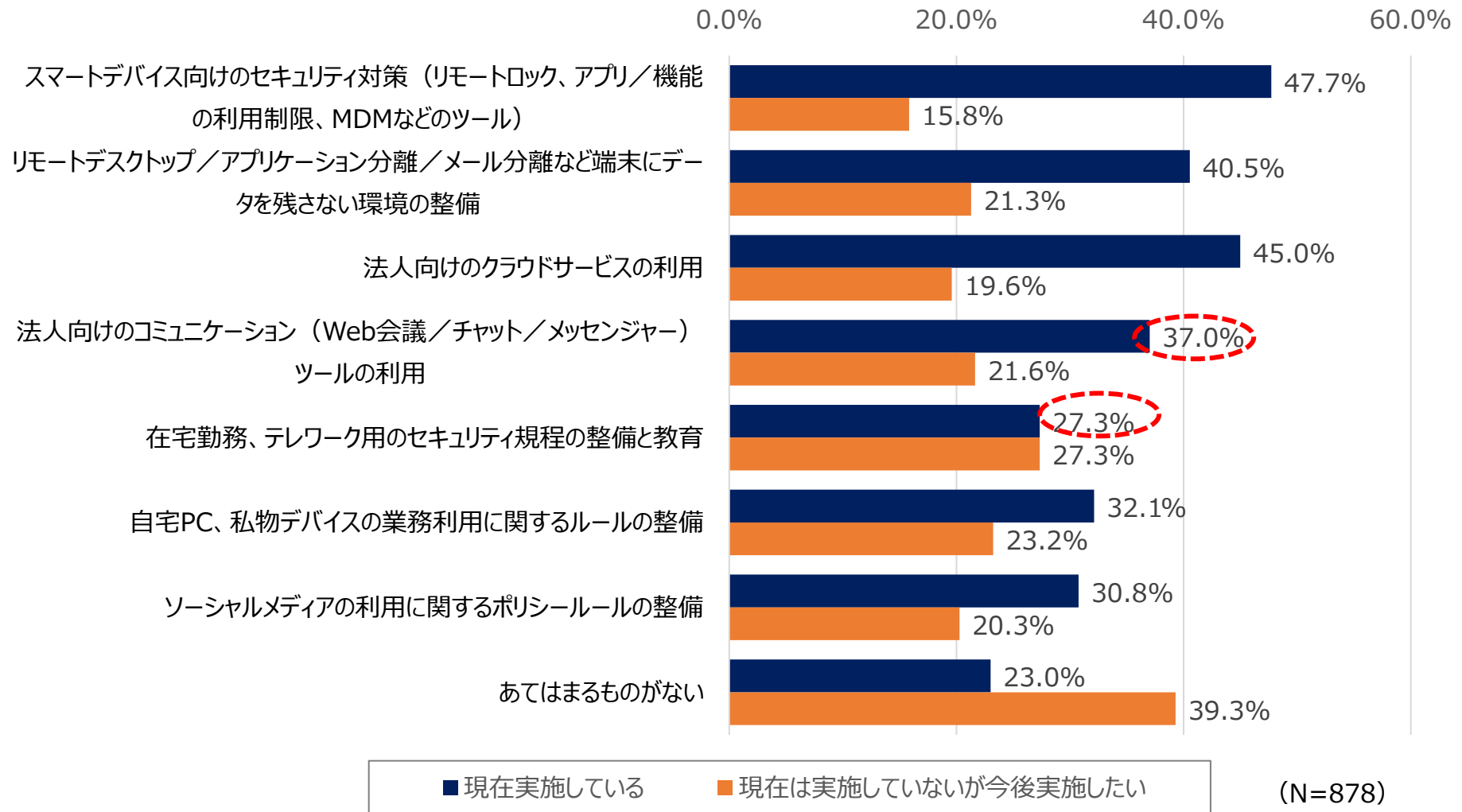


Q11_1 : 「働き方改革」に関する取組み状況（2019～2020年比較）

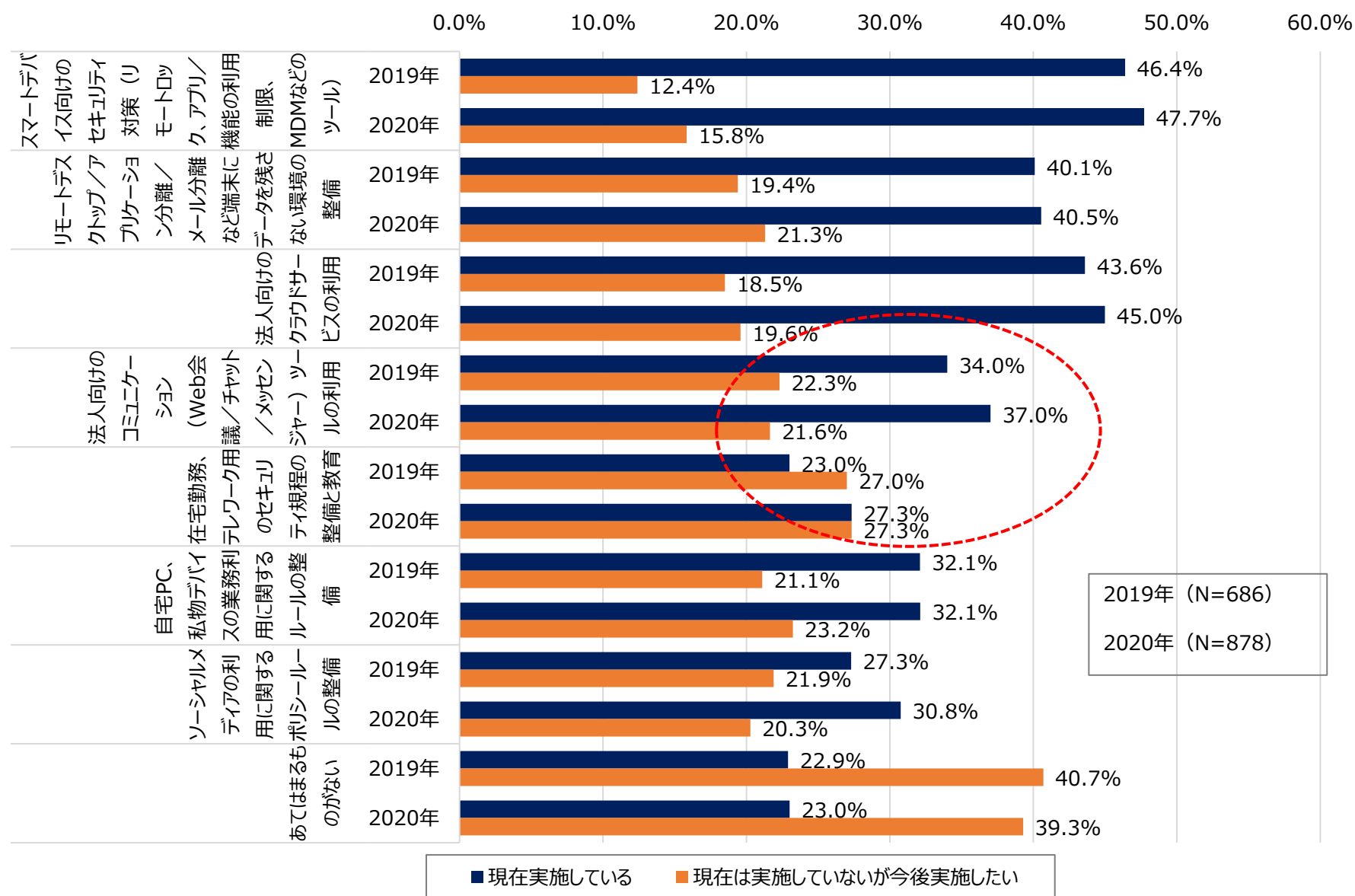


Q11_2：ワークスタイルに関連するセキュリティ対策の状況

■ 実施済の対策については2019年調査同様の傾向となったが、コミュニケーションツールの利用や在宅勤務・テレワーク用の規程整備の比率が若干増加しており、具体的な対策の実施が進みつつある。

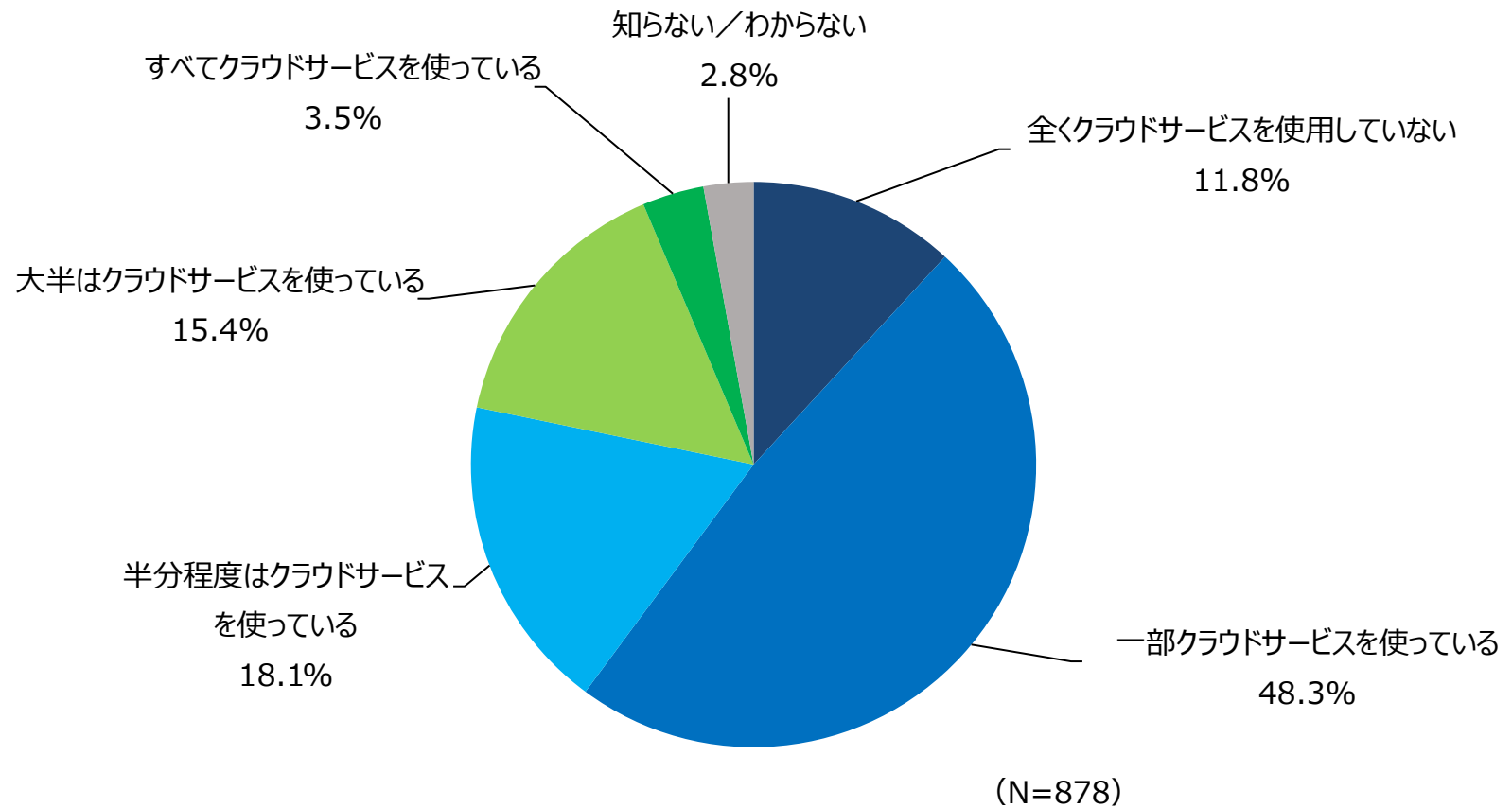


Q11_2：ワークスタイルに関連するセキュリティ対策の状況（2019～2020年比較）



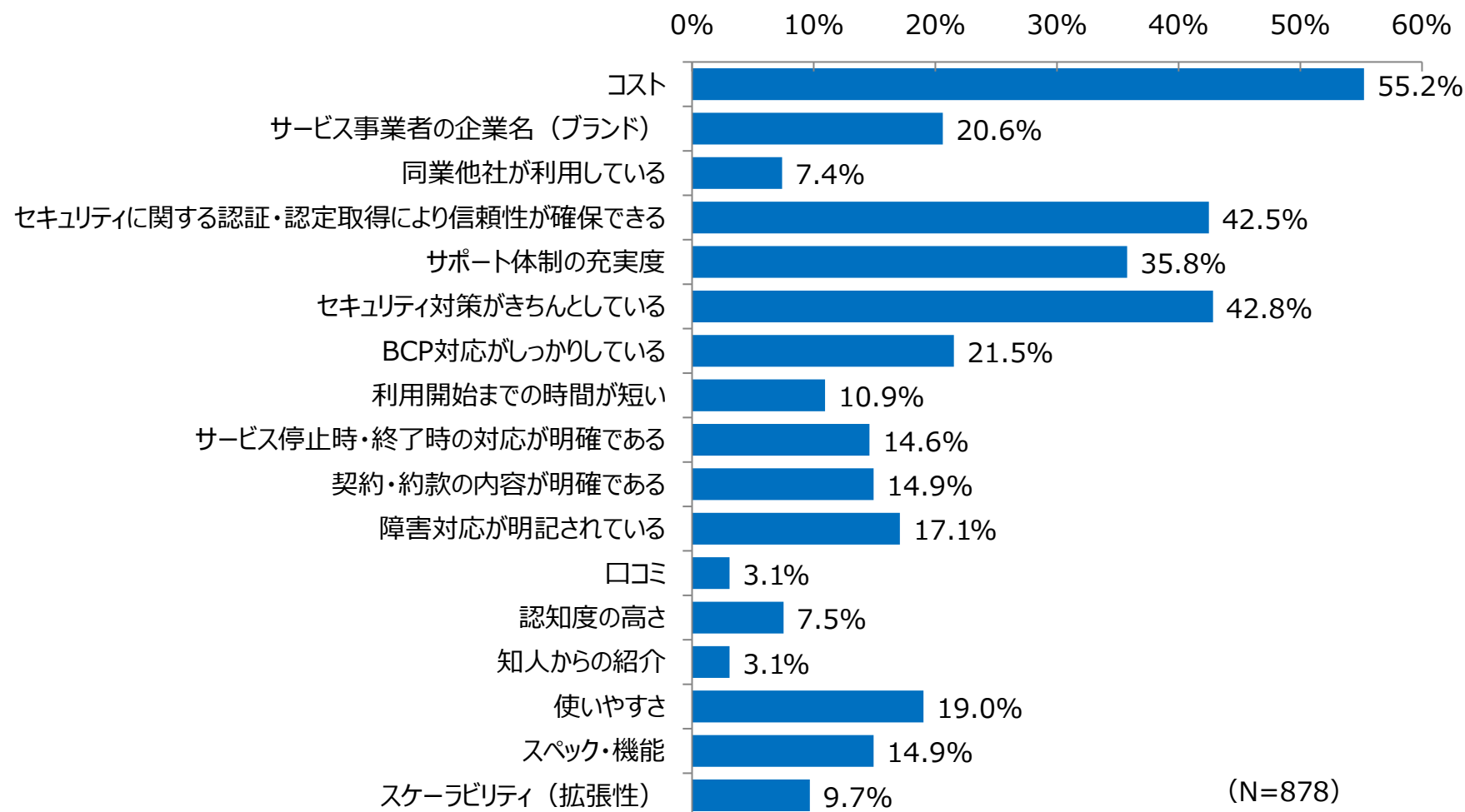
Q12_1：クラウドサービス利用の進捗状況

- 約9割がクラウドサービスを利用していると回答しているが、その半分以上は一部利用にとどまっており、クラウド環境への移行はまだこれから、と考えられる。



Q12_2：クラウドサービス選定する際のポイント

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



Q12_2_1：クラウドサービスを選定する際のポイント（業種別）

■ コスト、認証取得による信頼性確保、セキュリティ対策が全業種で選定のポイントとなっている。

	製造 (N=264)	建設・不動産 (N=73)	卸売・小売 (N=68)	金融・保険 (N=59)	情報通信 (N=161)	サービス (N=207)	公共・その他 (N=46)	全体 (N=878)
コスト	51.5%	56.2%	55.9%	66.1%	53.4%	58.5%	52.2%	55.2%
サービス事業者の企業名（ブランド）	20.8%	23.3%	19.1%	20.3%	19.9%	21.3%	17.4%	20.6%
同業他社が利用している	8.0%	11.0%	5.9%	6.8%	6.2%	7.2%	6.5%	7.4%
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できる	39.8%	39.7%	52.9%	50.8%	45.3%	39.6%	39.1%	42.5%
サポート体制の充実度	33.0%	41.1%	27.9%	42.4%	37.3%	36.7%	37.0%	35.8%
セキュリティ対策がきちんとしている	38.6%	38.4%	47.1%	52.5%	45.3%	42.5%	47.8%	42.8%
BCP対応がしっかりしている	21.2%	19.2%	17.6%	33.9%	23.0%	21.7%	10.9%	21.5%
利用開始までの時間が短い	9.8%	11.0%	5.9%	15.3%	14.9%	11.6%	2.2%	10.9%
サービス停止時・終了時の対応が明確である	17.0%	13.7%	16.2%	13.6%	14.3%	14.0%	4.3%	14.6%
契約・約款の内容が明確である	12.5%	17.8%	17.6%	18.6%	16.1%	14.5%	13.0%	14.9%
障害対応が明記されている	15.5%	23.3%	16.2%	22.0%	14.9%	17.4%	17.4%	17.1%
口コミ	3.4%	4.1%	2.9%	3.4%	1.9%	2.9%	4.3%	3.1%
認知度の高さ	8.7%	13.7%	7.4%	5.1%	5.6%	6.8%	4.3%	7.5%
知人からの紹介	3.0%	2.7%	4.4%	6.8%	0.6%	4.3%	0.0%	3.1%
使いやすさ	19.3%	23.3%	13.2%	16.9%	14.9%	24.6%	10.9%	19.0%
スペック・機能	14.4%	12.3%	14.7%	22.0%	13.7%	16.9%	8.7%	14.9%
スケーラビリティ（拡張性）	9.5%	8.2%	11.8%	22.0%	9.3%	8.7%	0.0%	9.7%

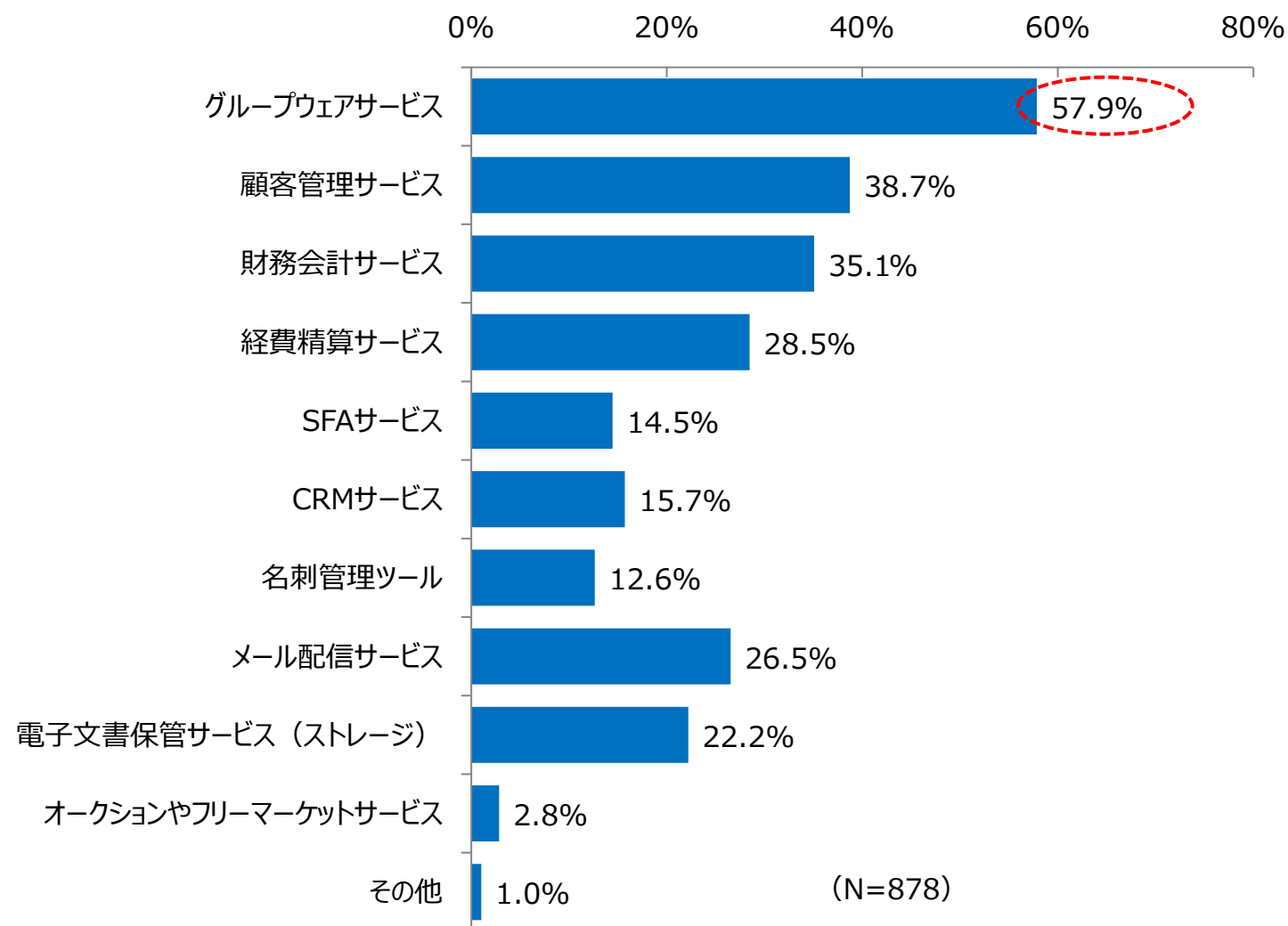
Q12_1：クラウドサービスを選定する際のポイント（従業員数規模別）

- 規模に関係なくコスト、認証取得による信頼性の確保、セキュリティ対応が重視されている。
また、規模が小さいほど使いやすさを重視し、規模が大きくなるとBCP対応を重視している。

	5,000人以上 (N=197)	1,000～ 4,999人 (N=197)	300～999人 (N=215)	50～299人 (N=269)	全体 (N=878)
コスト	45.7%	49.2%	60.0%	62.8%	55.2%
サービス事業者の企業名（ブランド）	25.9%	20.8%	17.2%	19.3%	20.6%
同業他社が利用している	10.2%	6.6%	7.0%	6.3%	7.4%
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できる	45.7%	46.7%	40.5%	38.7%	42.5%
サポート体制の充実度	34.0%	34.0%	39.1%	35.7%	35.8%
セキュリティ対策がきちんとしている	42.1%	44.2%	48.4%	37.9%	42.8%
BCP対応がしっかりしている	29.4%	23.4%	21.9%	14.1%	21.5%
利用開始までの時間が短い	13.7%	12.2%	9.3%	9.3%	10.9%
サービス停止時・終了時の対応が明確である	14.7%	13.7%	14.0%	15.6%	14.6%
契約・約款の内容が明確である	15.7%	18.3%	12.1%	14.1%	14.9%
障害対応が明記されている	16.2%	19.8%	16.3%	16.4%	17.1%
口コミ	3.6%	2.0%	2.3%	4.1%	3.1%
認知度の高さ	7.6%	5.6%	8.4%	8.2%	7.5%
知人からの紹介	4.1%	1.5%	3.3%	3.3%	3.1%
使いやすさ	15.2%	16.8%	20.9%	21.9%	19.0%
スペック・機能	17.3%	17.8%	13.5%	12.3%	14.9%
スケーラビリティ（拡張性）	13.2%	12.2%	7.4%	7.1%	9.7%

Q12_3：信頼性を重視して選ぶクラウドサービスはどれですか？

■ 信頼性重視で選ばれるクラウドサービスとして、グループウェアが最も高く、顧客管理サービス、財務管理サービスが続く。

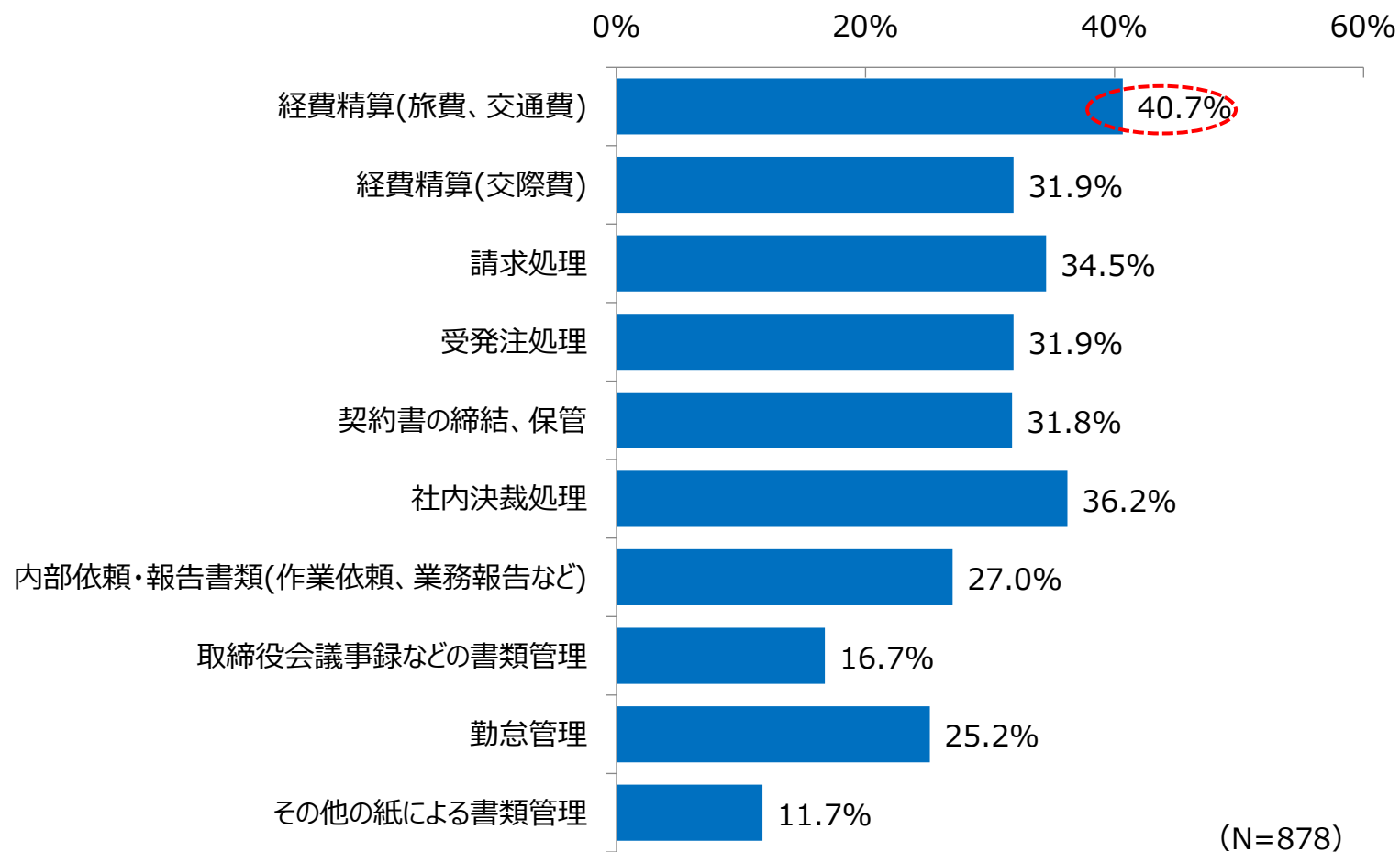


7) 電子契約の利用状況について

- Q13 : 電子署名／電子契約
- Q14 : 自社サイトSSL化
- Q15 : 情報セキュリティ監査

Q13_1：特に電子化したい業務プロセス

- 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、「社内決裁処理」、「請求処理」の順である。



Q13_1：特に電子化したい業務プロセス（2020年調査・業種別／従業員規模別）

- 業種別では、金融・保険は経費精算や内部依頼のような社内事務処理で高く、卸売・小売では契約や受発注のような取引処理が高い
- 規模別では、勤怠処理は規模が小さい方が要望が大きく、経費精算は規模に関係なく要望が高い。

業種別

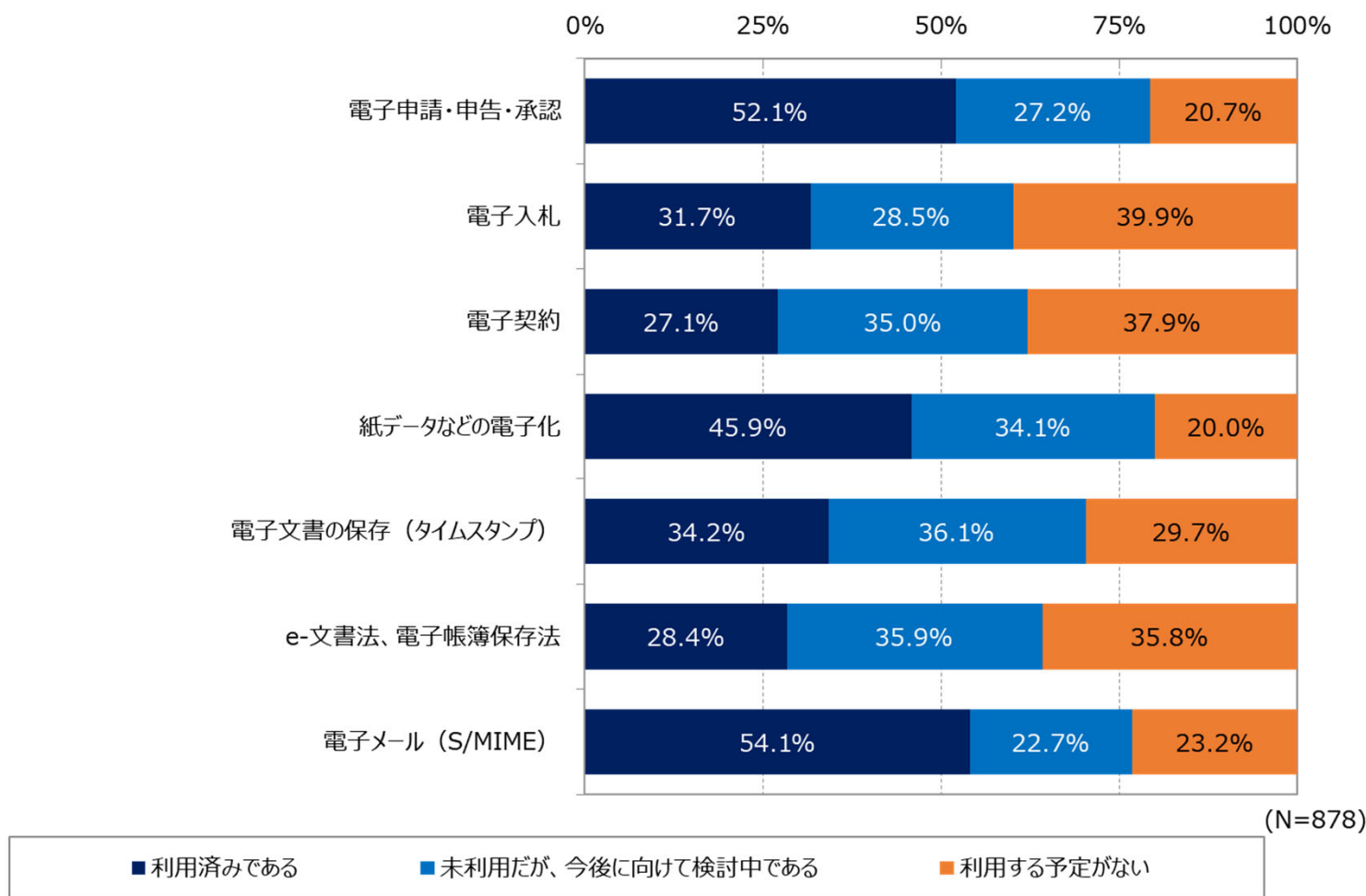
	製造 (N=264)	建設・不動産 (N=73)	卸売・小売 (N=68)	金融・保険 (N=59)	情報通信 (N=161)	サービス (N=207)	公共・その他 (N=46)	全体 (N=878)
経費精算(旅費、交通費)	40.9%	47.9%	30.9%	50.8%	44.1%	35.3%	41.3%	40.7%
経費精算(交際費)	36.0%	32.9%	33.8%	40.7%	29.8%	26.1%	26.1%	31.9%
請求処理	37.5%	42.5%	33.8%	27.1%	33.5%	32.9%	26.1%	34.5%
受発注処理	35.2%	39.7%	41.2%	18.6%	31.7%	25.6%	32.6%	31.9%
契約書の締結、保管	30.3%	32.9%	42.6%	32.2%	33.5%	30.0%	23.9%	31.8%
社内決裁処理	36.7%	45.2%	33.8%	44.1%	31.7%	35.7%	30.4%	36.2%
内部依頼・報告書類(作業依頼、業務報告など)	27.3%	30.1%	32.4%	37.3%	25.5%	22.2%	26.1%	27.0%
取締役会議事録などの書類管理	15.9%	17.8%	20.6%	23.7%	13.0%	16.4%	19.6%	16.7%
勤怠管理	20.1%	23.3%	27.9%	28.8%	24.2%	30.0%	30.4%	25.2%
その他の紙による書類管理	9.5%	12.3%	10.3%	13.6%	11.2%	14.5%	13.0%	11.7%

従業員規模別

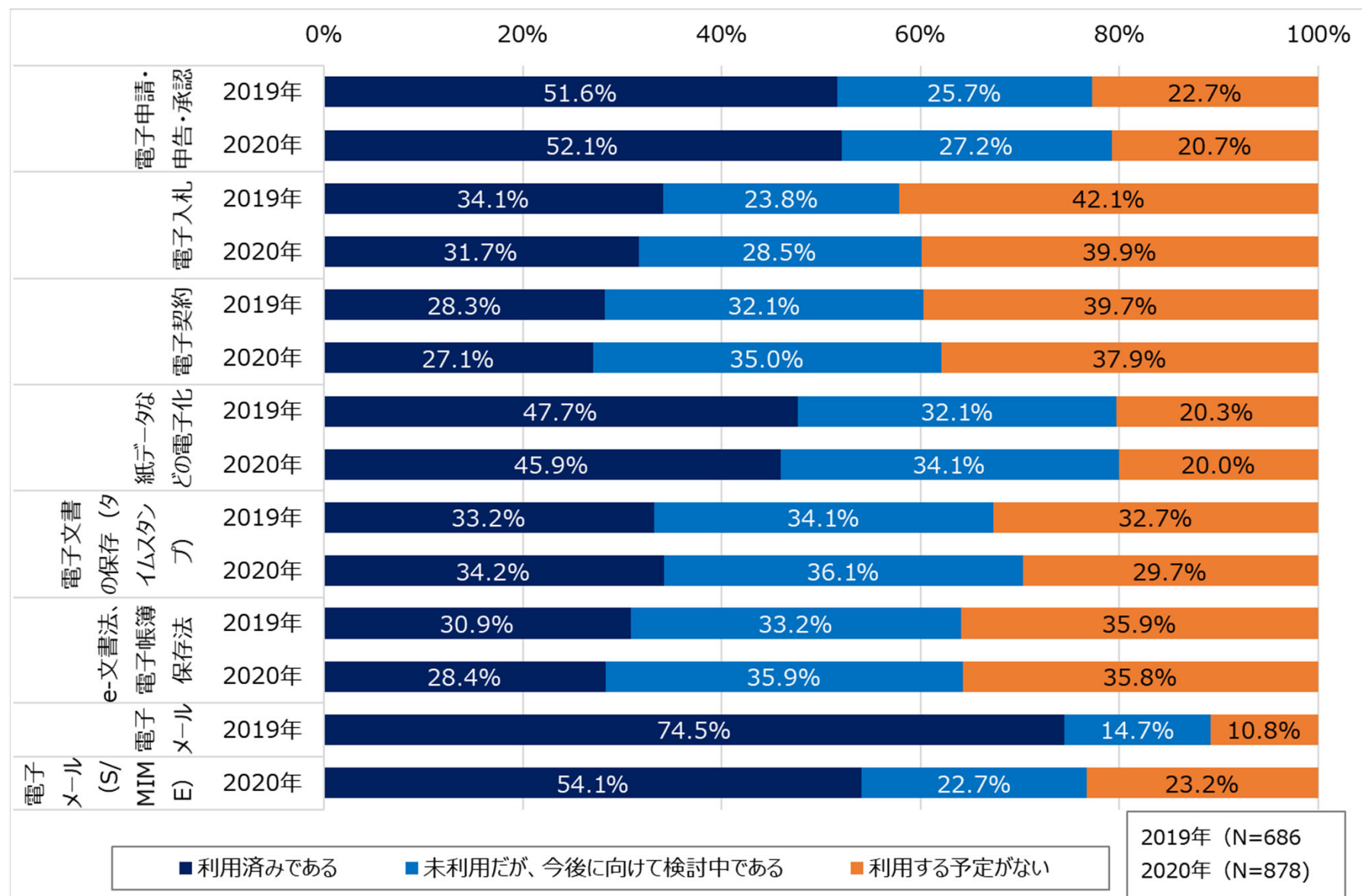
	5,000人以上 (N=197)	1,000～4,999人 (N=197)	300～999人 (N=215)	50～299人 (N=269)	全体 (N=878)
経費精算(旅費、交通費)	40.1%	40.6%	40.9%	40.9%	40.7%
経費精算(交際費)	32.5%	34.5%	32.1%	29.4%	31.9%
請求処理	32.5%	37.6%	34.9%	33.5%	34.5%
受発注処理	29.9%	36.0%	34.9%	27.9%	31.9%
契約書の締結、保管	37.6%	34.5%	32.6%	24.9%	31.8%
社内決裁処理	30.5%	36.5%	41.4%	36.1%	36.2%
内部依頼・報告書類(作業依頼、業務報告など)	32.5%	32.5%	22.3%	22.7%	27.0%
取締役会議事録などの書類管理	17.3%	19.8%	15.8%	14.9%	16.7%
勤怠管理	16.8%	26.4%	26.0%	29.7%	25.2%
その他の紙による書類管理	12.7%	12.2%	9.3%	12.6%	11.7%

Q13_2：電子署名／電子証明書の利用状況

- 利用が多いは電子メールと電子申請・申告・承認で、今後利用される予定なのは電子文書保存とe-文書法・電子帳簿保存法対応である。

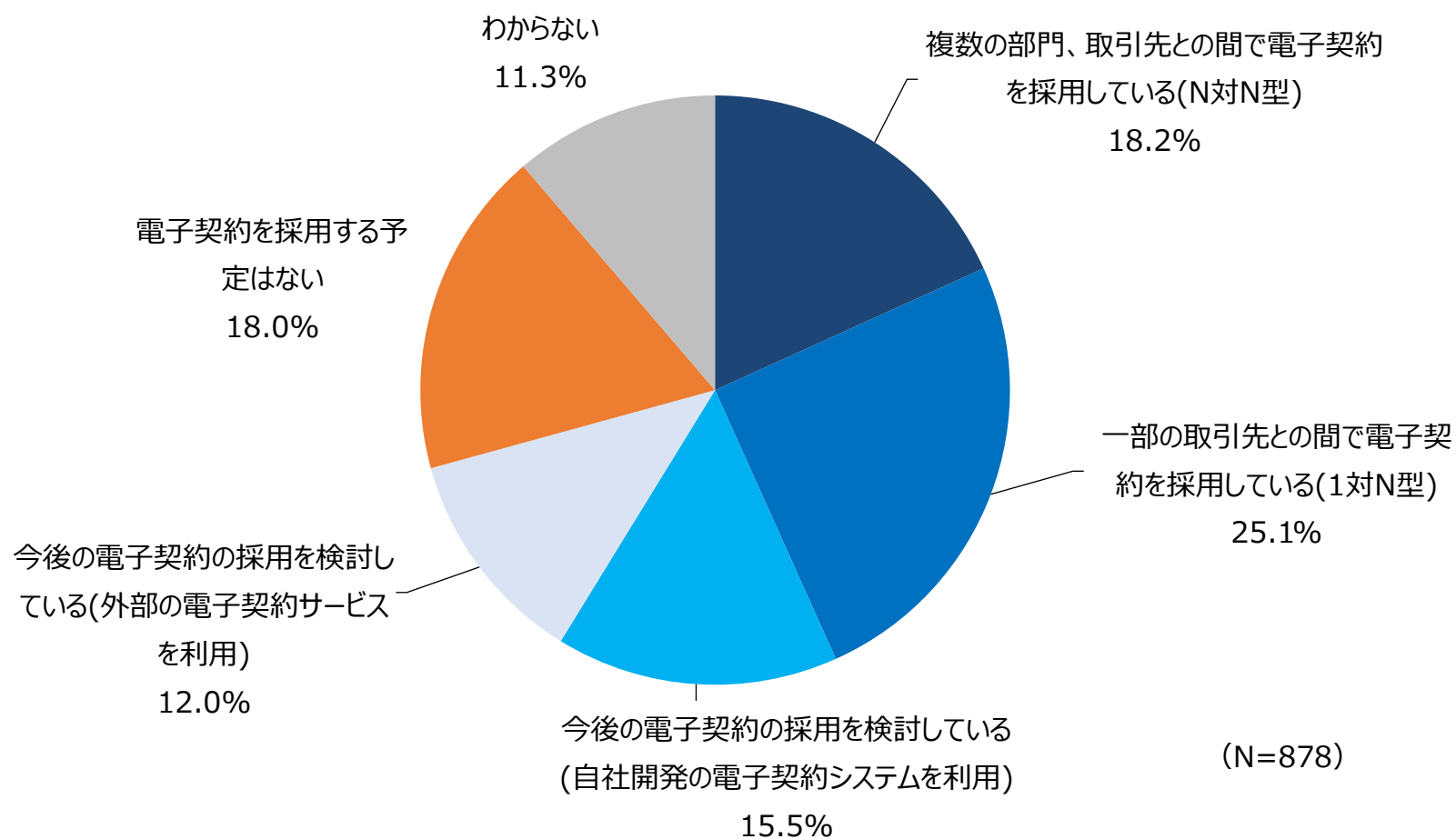


Q13_2：電子署名／電子証明書の利用状況（2019～2020年比較）



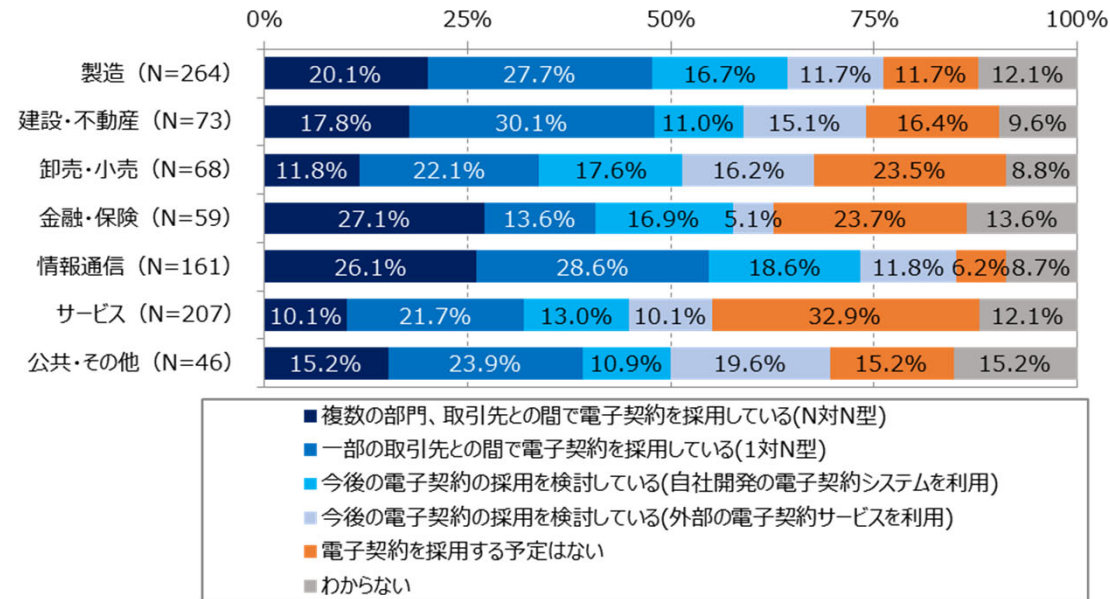
Q13_3：電子契約の利用状況

■ 4割以上で利用しており、今後の利用予定は約3割となった。

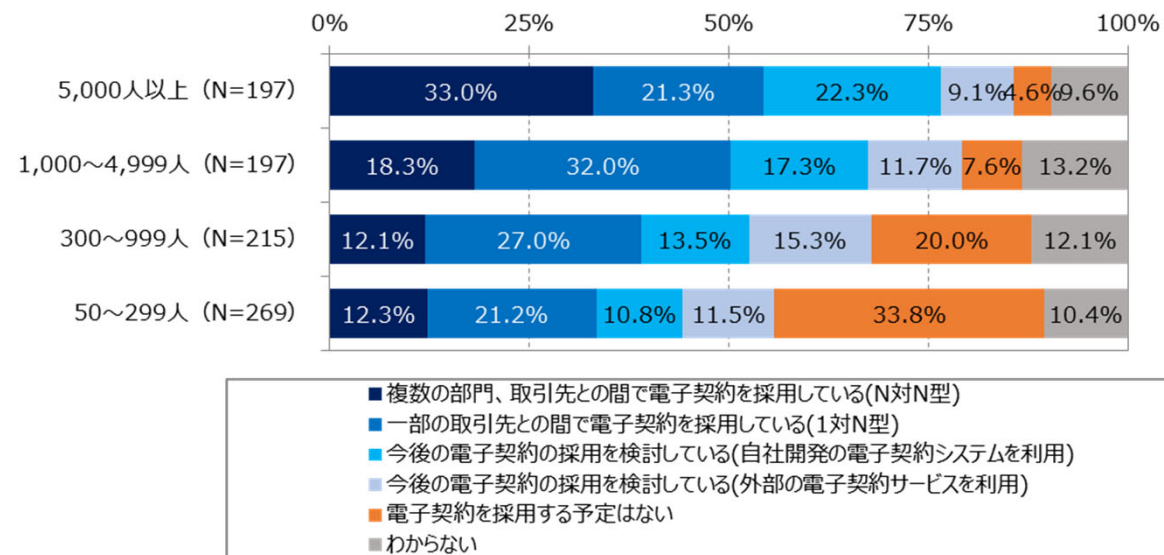


Q13_3：電子契約の利用状況（2020年調査／業種別・従業員規模別）

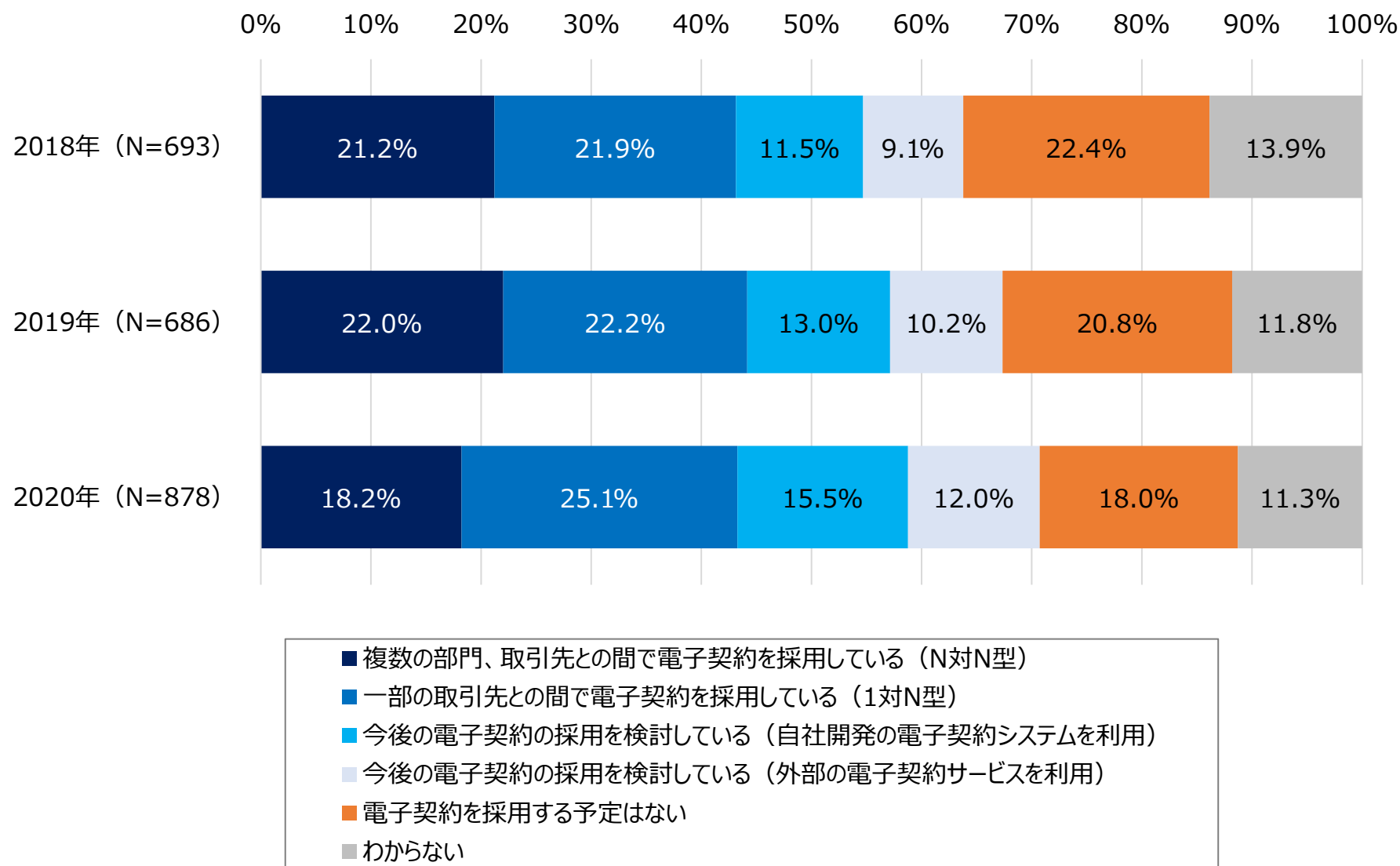
業種別



従業員規模別

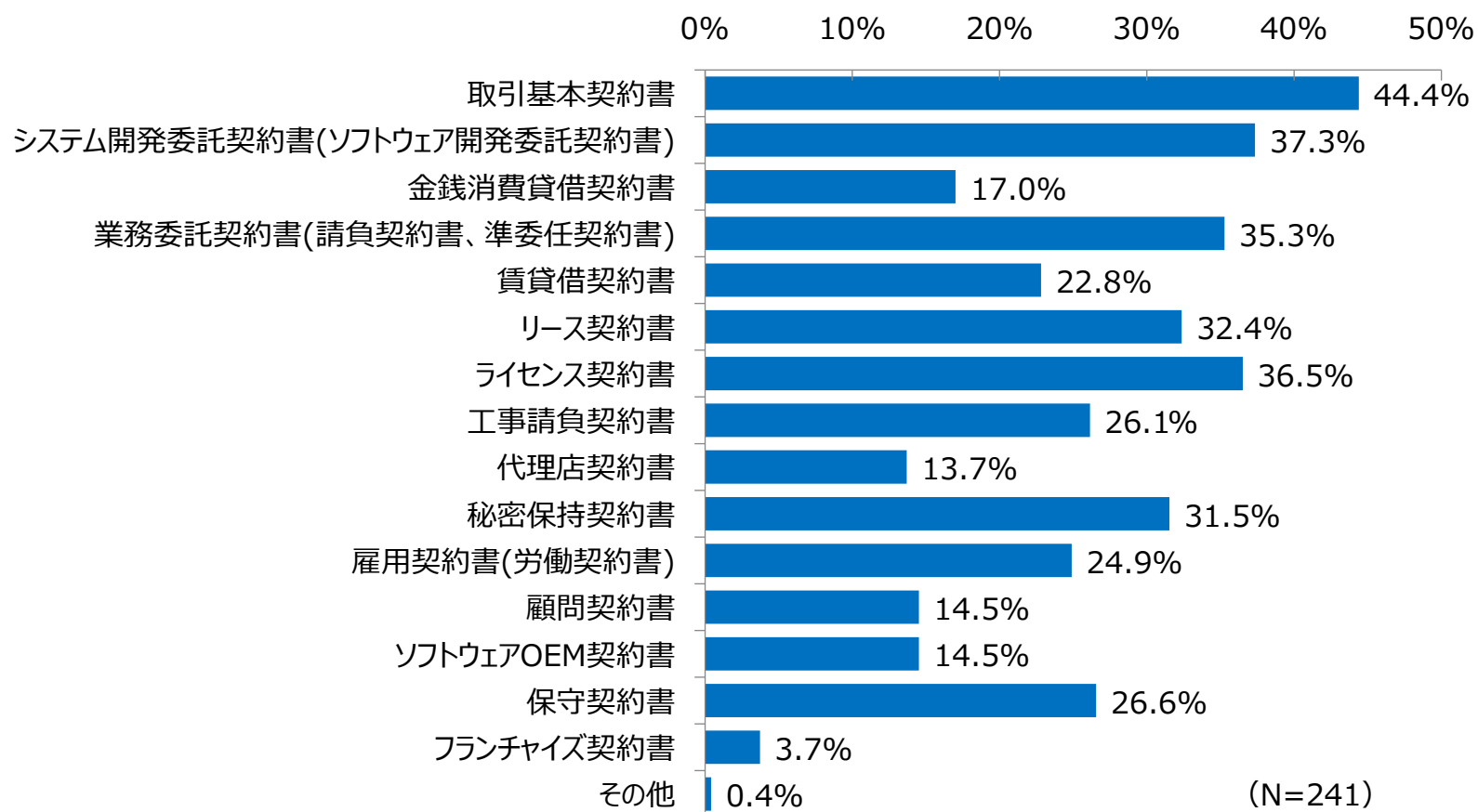


Q13_3：電子契約の利用状況（2018～2020年比較）



Q13_4：今後電子化したい契約書

- 最もニーズが高いのは、取引基本契約書とシステム開発委託契約書となり、3位はライセンス契約書であった。



Q13_4：今後電子化したい契約書（2020年調査／業種別・従業員規模別）

業種別

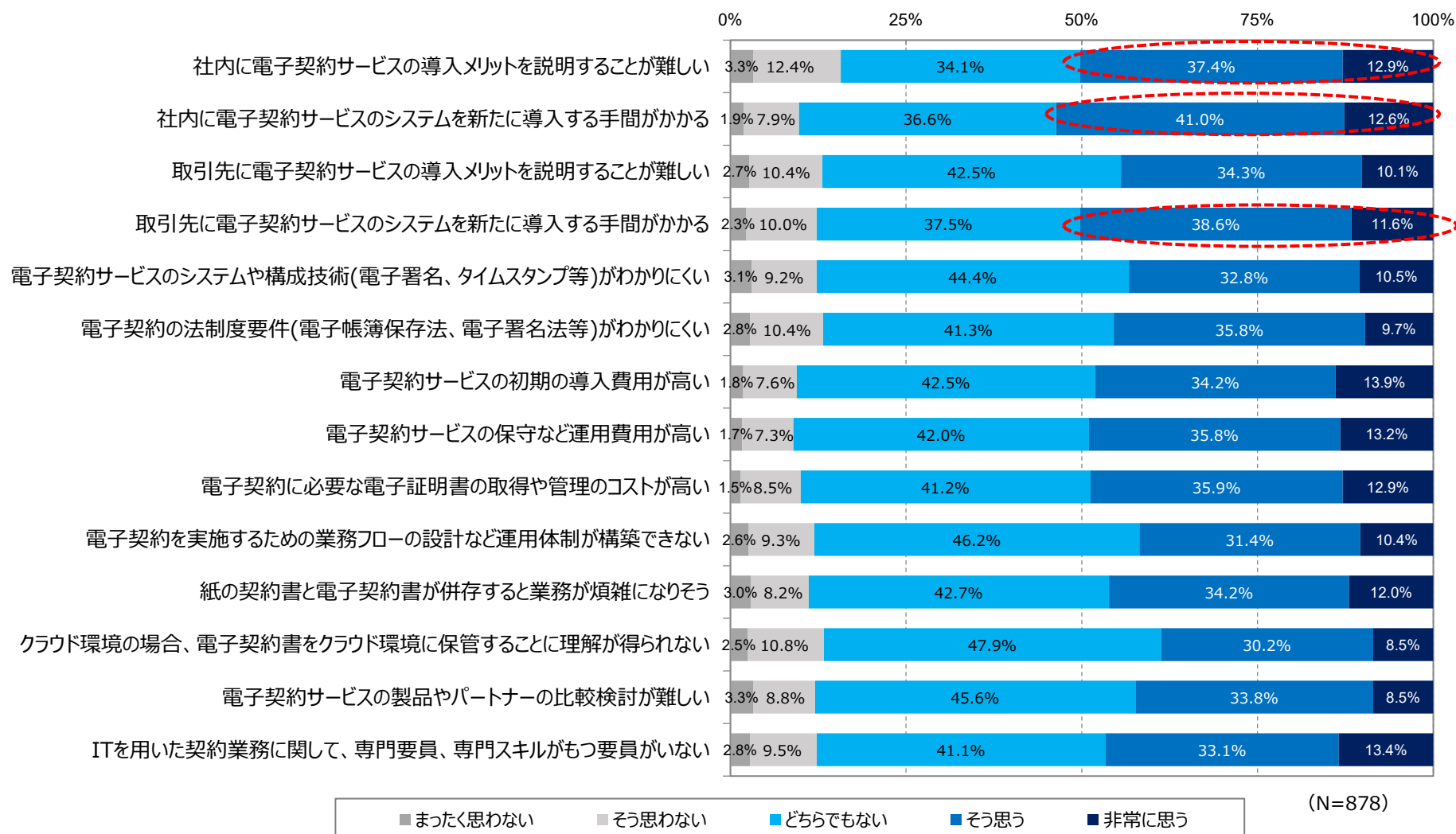
	製造 (N=75)	建設・不動産 (N=19)	卸売・小売 (N=23)	金融・保険 (N=13)	情報通信 (N=49)	サービス (N=48)	公共・その他 (N=14)	全体 (N=241)
取引基本契約書	52.0%	47.4%	43.5%	46.2%	34.7%	50.0%	14.3%	44.4%
システム開発委託契約書（ソフトウェア開発委託契約書）	34.7%	42.1%	17.4%	76.9%	42.9%	33.3%	35.7%	37.3%
金銭消費貸借契約書	21.3%	10.5%	13.0%	38.5%	12.2%	14.6%	14.3%	17.0%
業務委託契約書（請負契約書、準委任契約書）	40.0%	36.8%	39.1%	30.8%	26.5%	39.6%	21.4%	35.3%
賃貸借契約書	21.3%	26.3%	30.4%	23.1%	18.4%	20.8%	35.7%	22.8%
リース契約書	30.7%	21.1%	47.8%	15.4%	34.7%	33.3%	35.7%	32.4%
ライセンス契約書	41.3%	36.8%	52.2%	30.8%	34.7%	25.0%	35.7%	36.5%
工事請負契約書	34.7%	47.4%	34.8%	7.7%	8.2%	22.9%	28.6%	26.1%
代理店契約書	13.3%	21.1%	21.7%	0.0%	8.2%	16.7%	14.3%	13.7%
秘密保持契約書	37.3%	36.8%	39.1%	23.1%	24.5%	29.2%	21.4%	31.5%
雇用契約書（労働契約書）	28.0%	21.1%	34.8%	23.1%	14.3%	29.2%	21.4%	24.9%
顧問契約書	20.0%	31.6%	17.4%	15.4%	2.0%	10.4%	14.3%	14.5%
ソフトウェアOEM契約書	14.7%	10.5%	17.4%	38.5%	14.3%	8.3%	14.3%	14.5%
保守契約書	28.0%	15.8%	39.1%	23.1%	28.6%	14.6%	50.0%	26.6%
フランチャイズ契約書	5.3%	5.3%	4.3%	0.0%	2.0%	2.1%	7.1%	3.7%
その他	0.0%	0.0%	0.0%	0.0%	0.0%	2.1%	0.0%	0.4%

従業員規模別

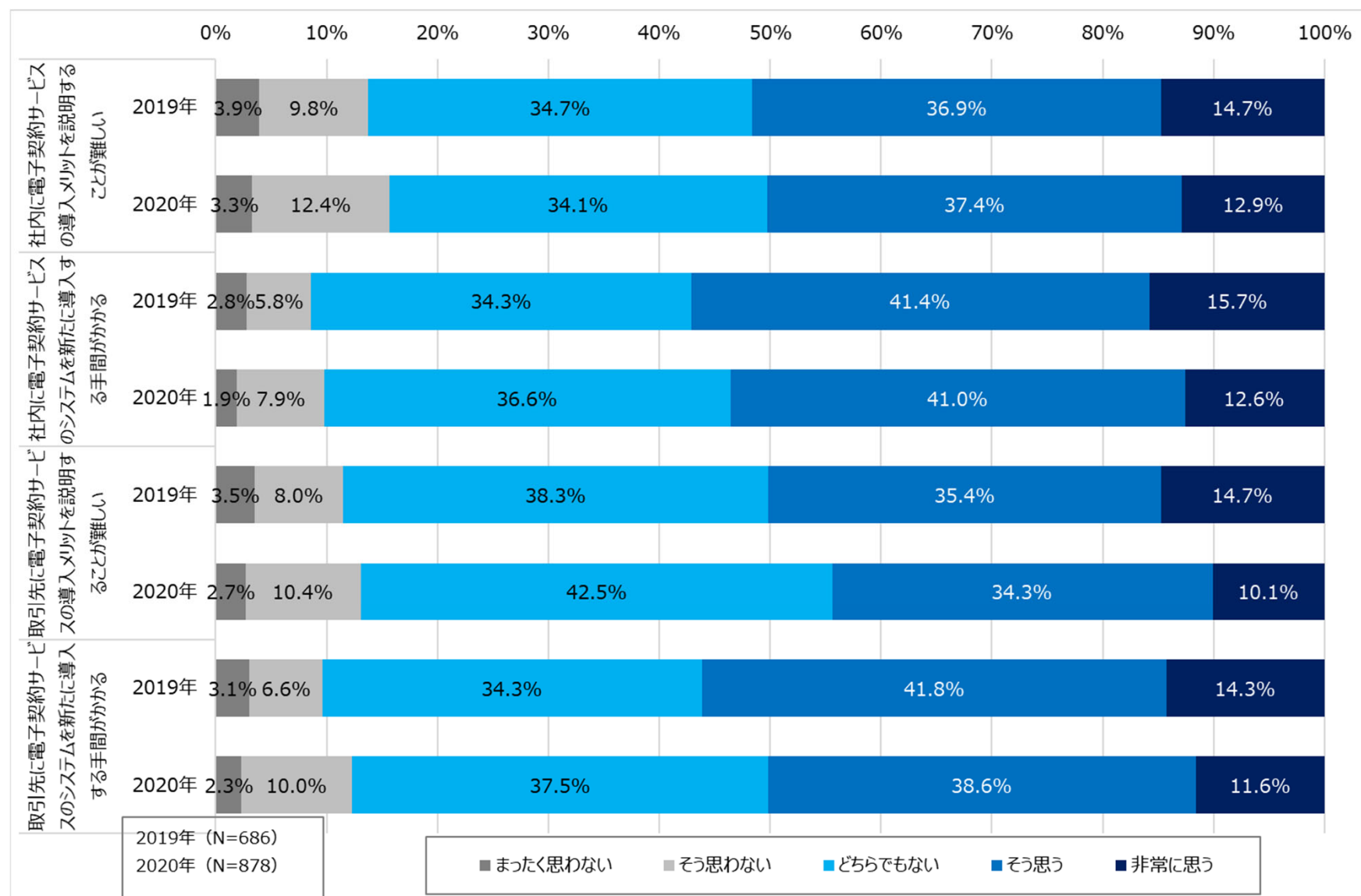
	5,000人以上 (N=62)	1,000～4,999人 (N=57)	300～999人 (N=62)	50～299人 (N=60)	全体 (N=241)
取引基本契約書	30.6%	45.6%	48.4%	53.3%	44.4%
システム開発委託契約書（ソフトウェア開発委託契約書）	37.1%	36.8%	41.9%	33.3%	37.3%
金銭消費貸借契約書	14.5%	26.3%	11.3%	16.7%	17.0%
業務委託契約書（請負契約書、準委任契約書）	35.5%	42.1%	38.7%	25.0%	35.3%
賃貸借契約書	25.8%	22.8%	19.4%	23.3%	22.8%
リース契約書	33.9%	29.8%	35.5%	30.0%	32.4%
ライセンス契約書	40.3%	42.1%	37.1%	26.7%	36.5%
工事請負契約書	22.6%	31.6%	25.8%	25.0%	26.1%
代理店契約書	11.3%	17.5%	9.7%	16.7%	13.7%
秘密保持契約書	30.6%	40.4%	25.8%	30.0%	31.5%
雇用契約書（労働契約書）	32.3%	24.6%	17.7%	25.0%	24.9%
顧問契約書	8.1%	17.5%	16.1%	16.7%	14.5%
ソフトウェアOEM契約書	14.5%	15.8%	11.3%	16.7%	14.5%
保守契約書	24.2%	31.6%	21.0%	30.0%	26.6%
フランチャイズ契約書	1.6%	7.0%	1.6%	5.0%	3.7%
その他	0.0%	0.0%	0.0%	1.7%	0.4%

Q13_5：電子契約／電子契約サービスの課題

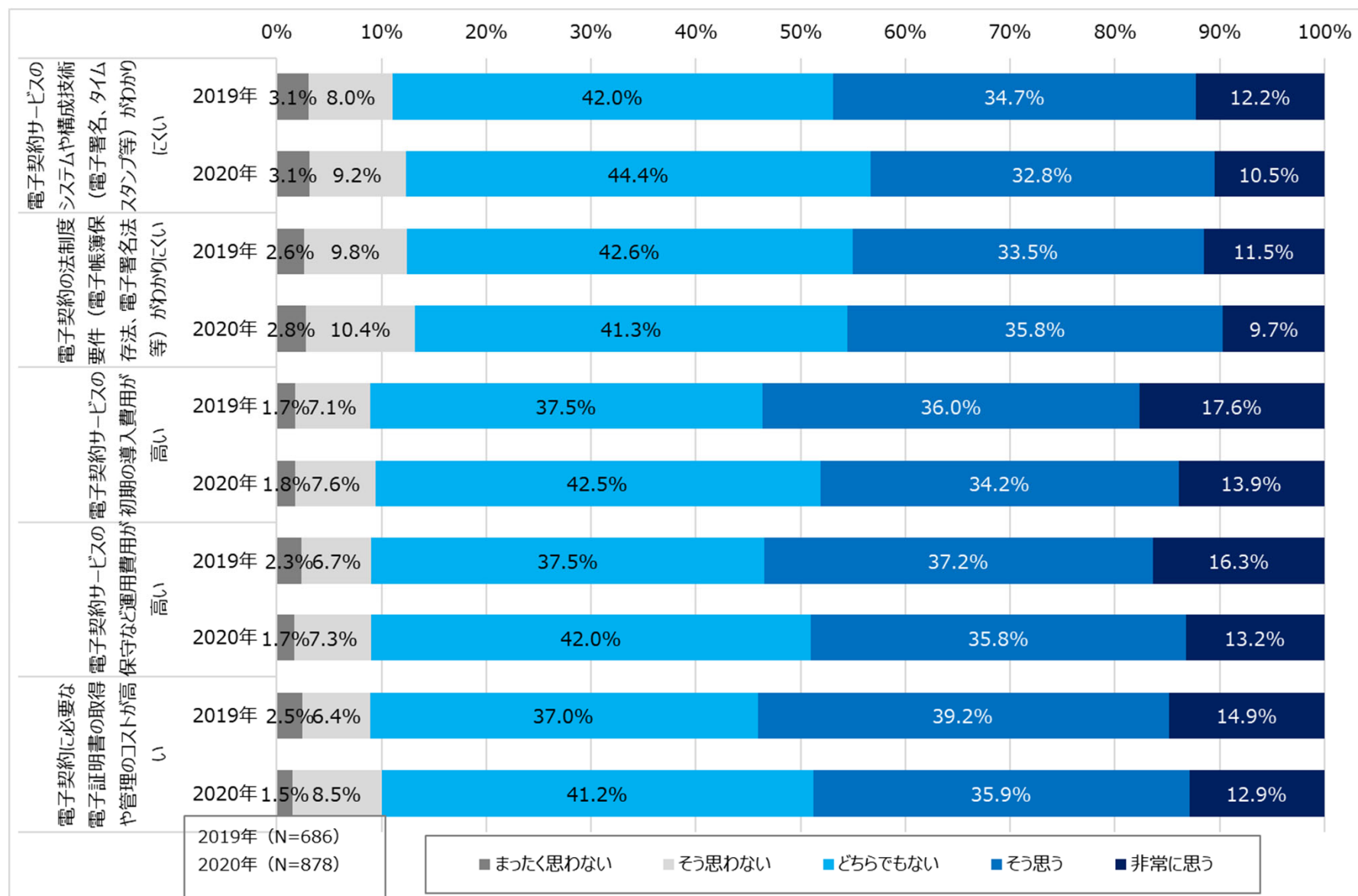
- 課題としては、社内または取引先において導入の手間がかかると導入メリットを説明することが難しいという回答（非常に思う、そう思う）が多い。



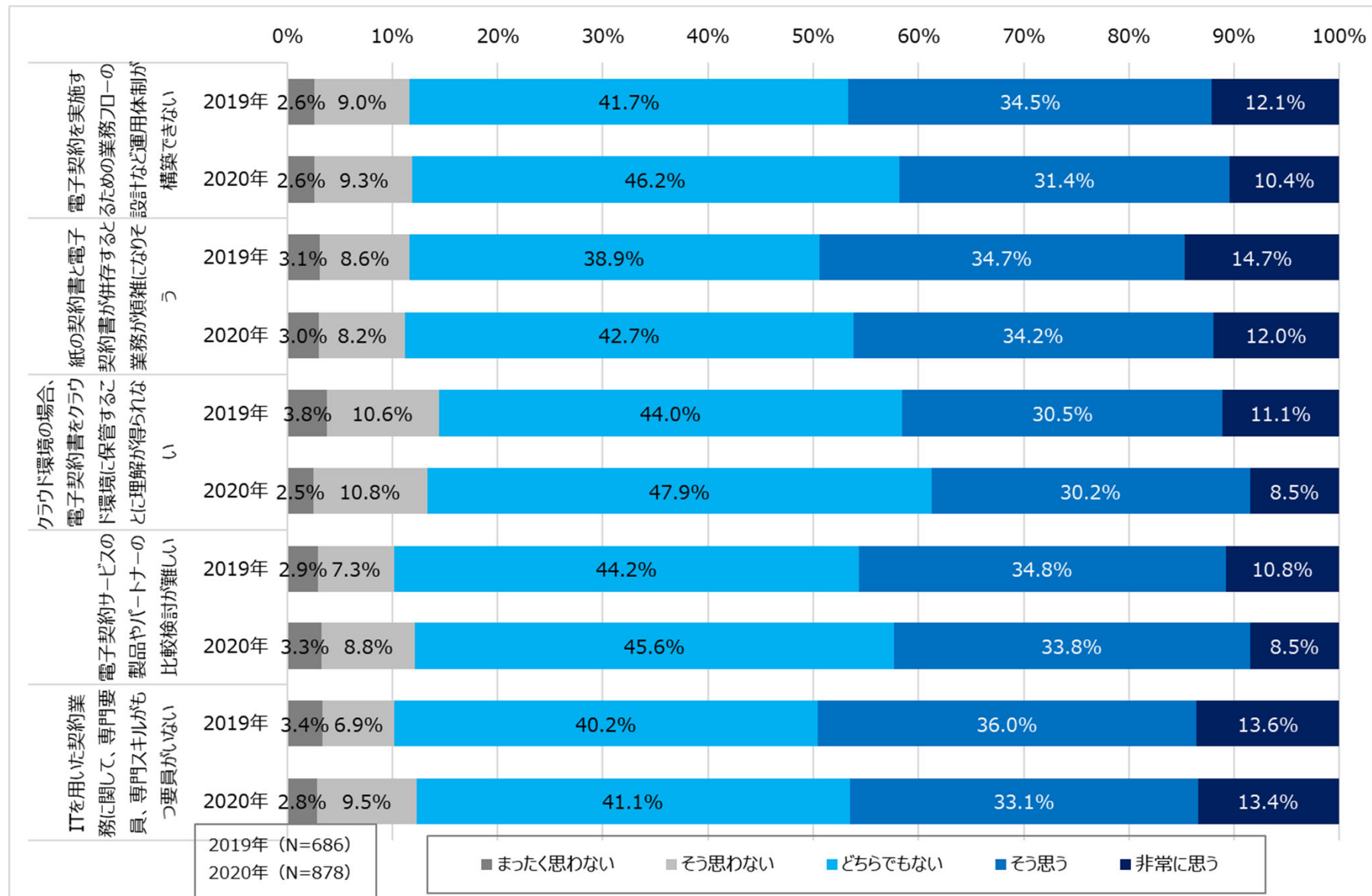
Q13_5：電子契約／電子契約サービスの課題（2019～2020年比較）



Q13_5：電子契約／電子契約サービスの課題（2019～2020年比較）

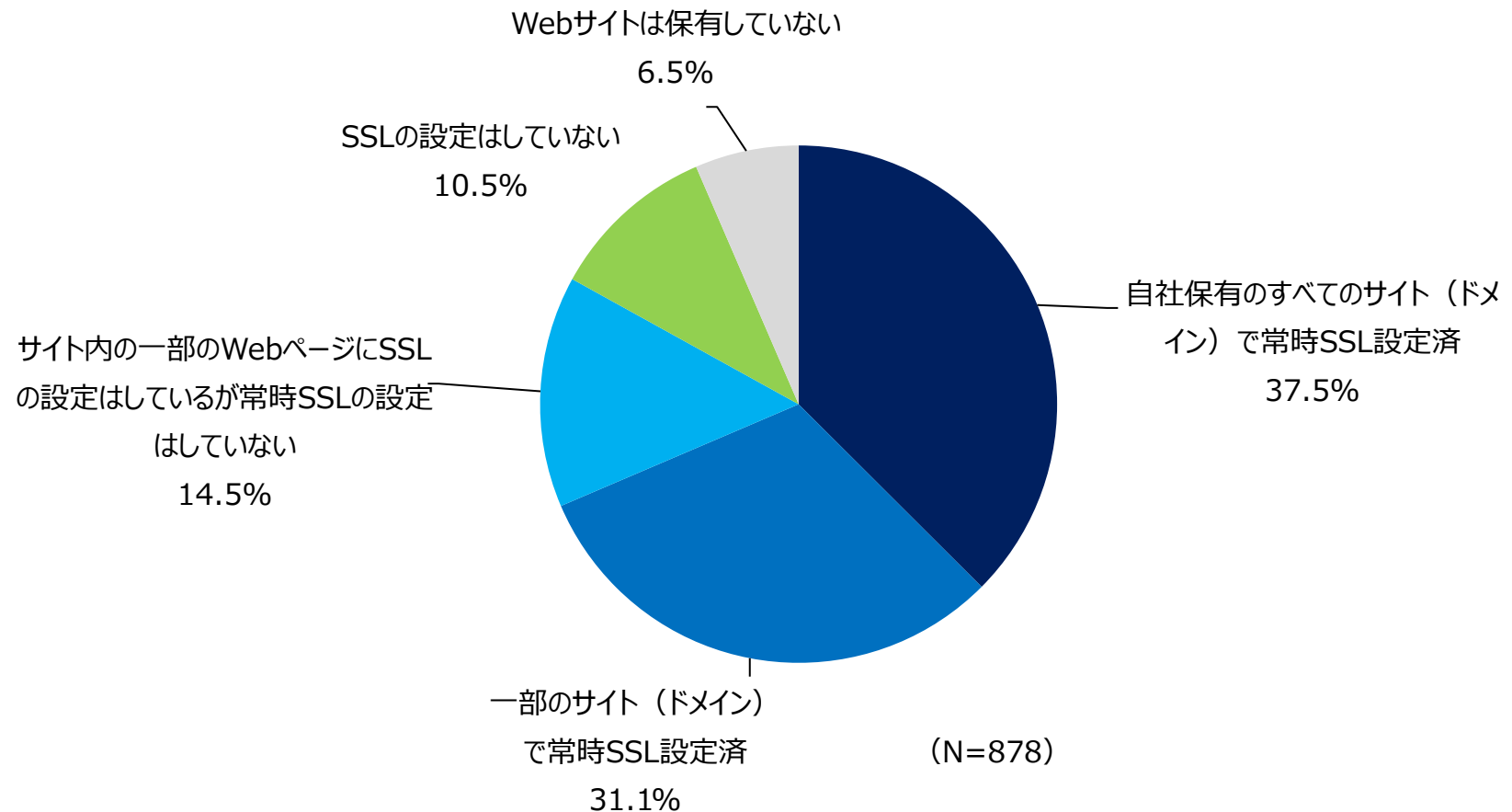


Q13_5：電子契約／電子契約サービスの課題（2019～2020年比較）



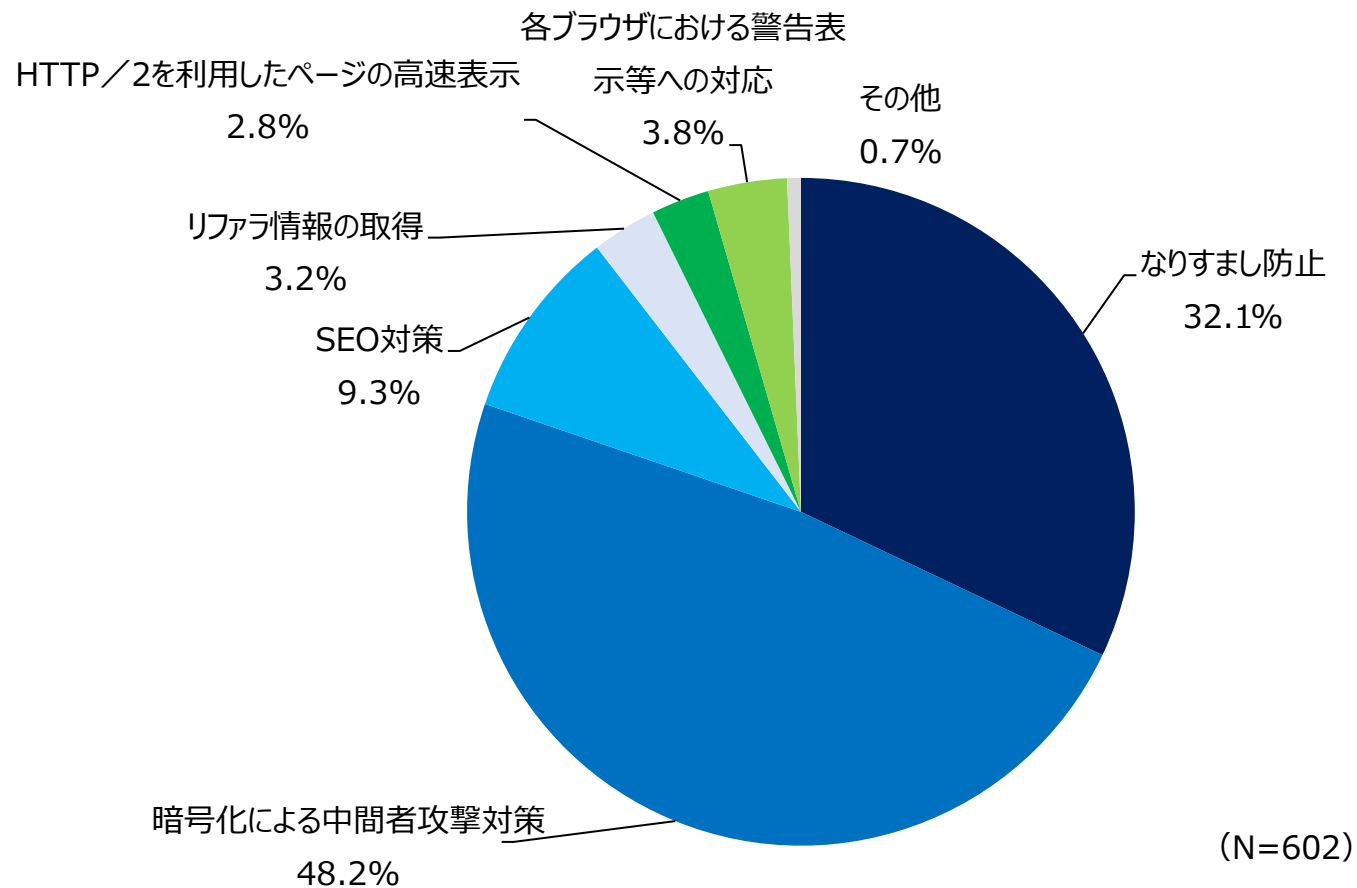
Q14_1：自社WebサイトのSSL化対応状況

- 8割以上で何らかのSSL化を行っており、すべて常時SSL化している企業も約4割にのぼっており、SSL化対応が進んでいる。



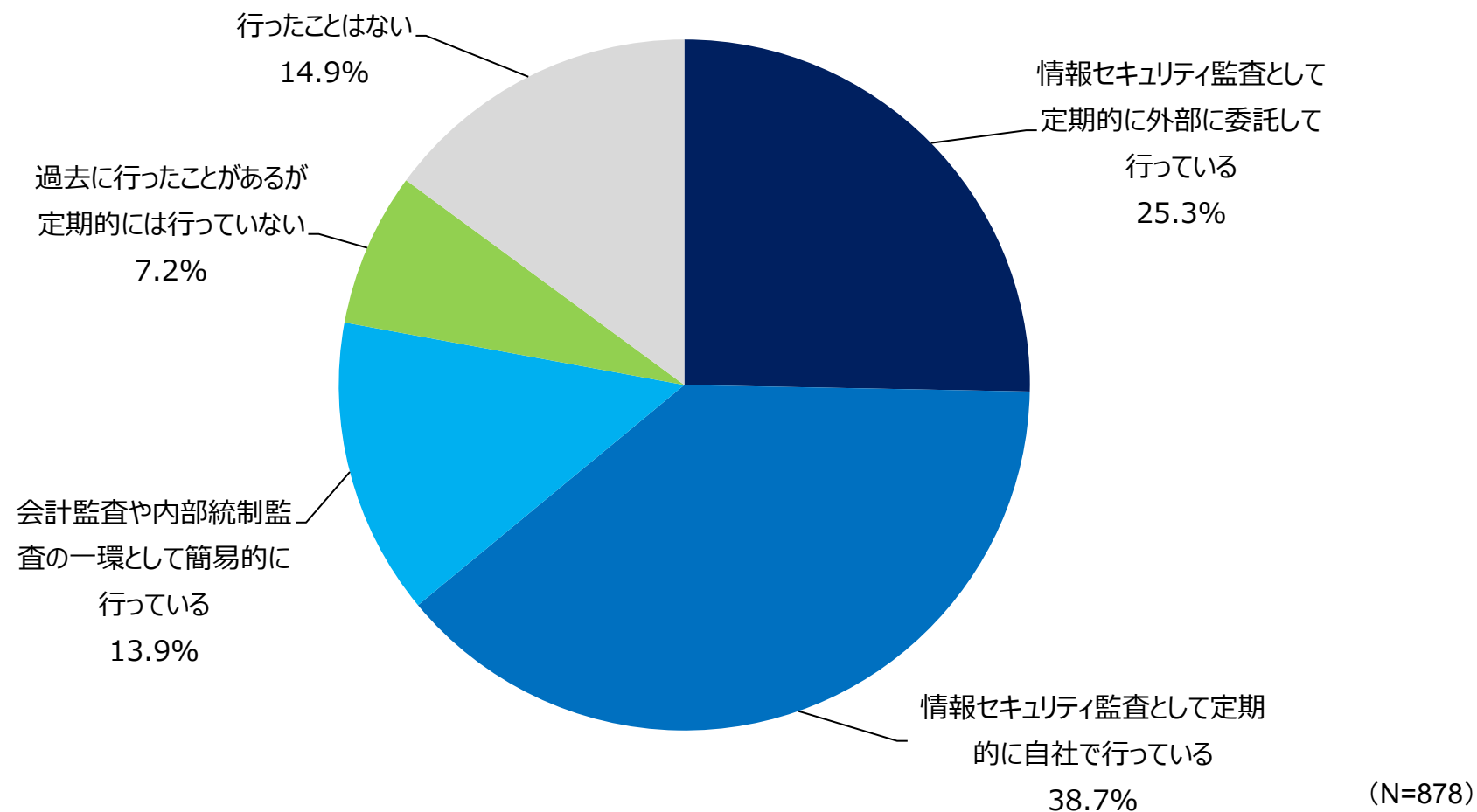
Q14_2：自社Webサイトの常時SSL化の理由

- 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く。

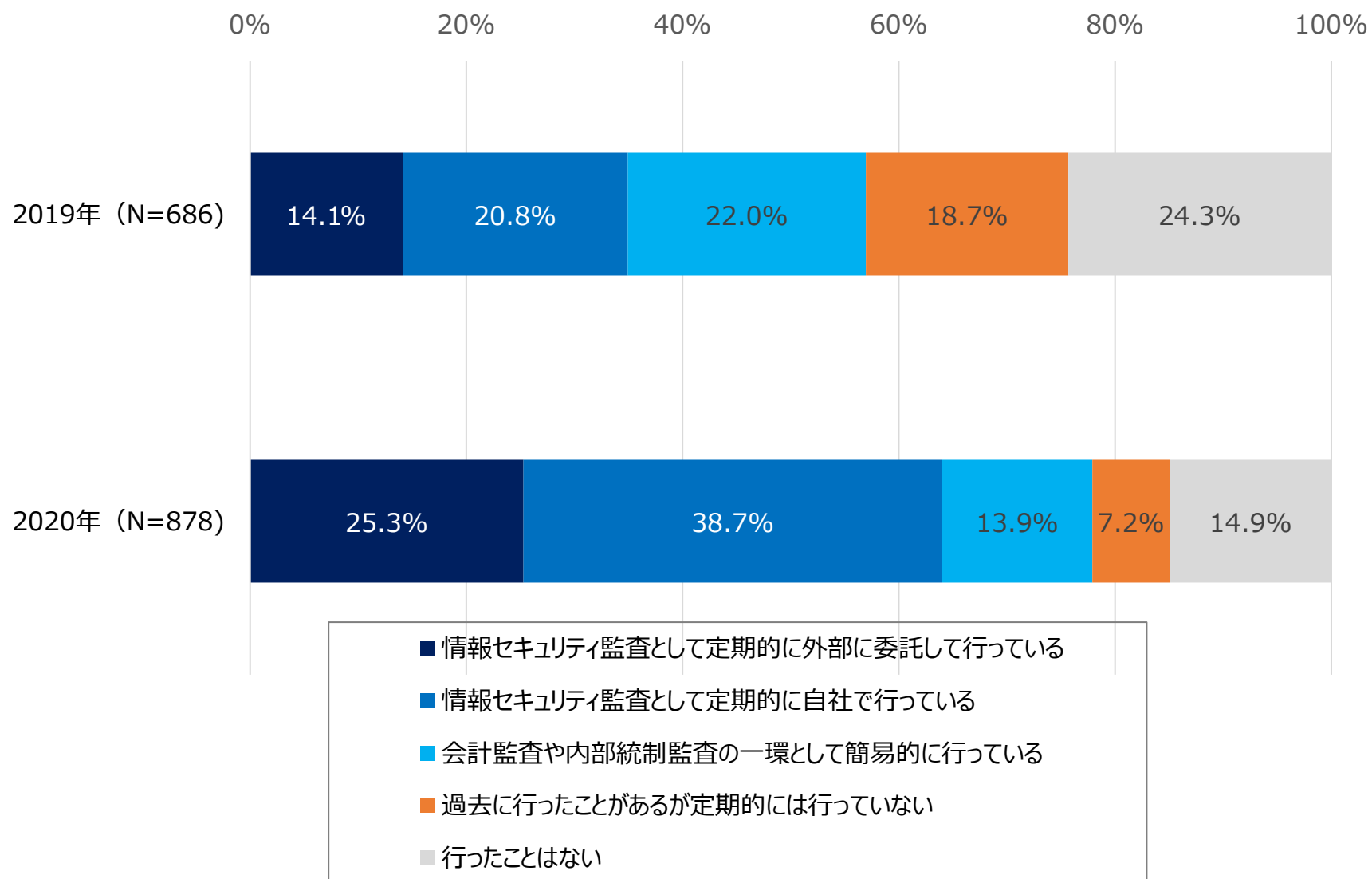


Q15：情報セキュリティ監査の実施状況

- 2019年と比較して、不定期の実施を含め実施したことがあるが8割を超え、定期的に実施している会社も約7割に上り、大きく増加している。



Q15_2：情報セキュリティ監査の実施状況（2019～2020年比較）



総括

情報セキュリティインシデントについては、依然としてマルウェア感染やPC・スマホ等情報機器の紛失・盗難が多く、個人情報の漏洩・逸失や個人情報に係るトラブルが増加しており、セキュリティ強化が重要な経営課題として認識されている。

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、従来型のファイアウォールやマルウェア対策ソフトの比率が未だに高いが、大企業を中心に次世代型のSWG・CASBやEDRの導入が進みつつある。

働き方改革については、経営目標化や組織体制整備の段階を過ぎて、具体的なルールの策定やテレワークのためのシステム整備が開始されており、着実に進行している。

増加する情報セキュリティインシデントに対応して、認定／認証制度の取得や次世代型のセキュリティ製品・サービスの導入と並行して、情報セキュリティ監査の実施が増加しており、実効性のある情報セキュリティシステムの構築が進みつつある