IT-Report
2020 Spring

特集

「企業IT利活用動向調査2020」にみるIT化の現状

IT-REPORT

2020
Spring

Contents

特集「企業IT利活用動向調査2020」にみるIT化の現状 01
1．調査概要 01
2．経営における情報セキュリティの位置づけ 02
3．認定／認証制度に対する意識 10
4．国内外の個人情報保護施策への取組み 12
5．セキュリティ製品／技術の利用動向 15
6．働き方改革とクラウドサービスの動向 21
7．電子署名／電子契約など 25
8．総評 29
回答者プロフィール 30

〈資料〉情報化に関する動向（2019年10月～2020年３月） 32

JIPDEC
一般財団法人日本情報経済社会推進協会

本誌「JIPDEC IT-Report 2020 Spring」では、JIPDECが2011年から継続して行っているIT利活用にかかわる「企業IT利活用動向調査2020」の結果をとりまとめ、紹介しています。

経年調査を行っている経営課題については、2019年４月に施行された働き方改革法により、「働き方改革」や「情報セキュリティ強化」を重視する動きが高まってきています。働き方改革への取組みについては、2019年調査に比べ、経営目標に挙げている企業の割合が上昇し、また法人向けコミュニケーションツールの利用や、在宅勤務、テレワーク用のセキュリティ規程の整備・教育など、具体的な対策が進んでいることがわかりました。一方で、働き方改革の実現に重要な役割を示すクラウドサービスの利用に関しては、何らかの形でクラウドサービスを利用している割合は約９割となりましたが、その半数は一部のみの利用にとどまっています。

2020年は個人情報保護法 いわゆる３年後の見直しの時期に該当し、現在法改正にむけ審議が進められていますが、企業の経営課題として「法規制（個人情報保護法）への対応」に意識が高まってきているなか、特に改正内容のうち、「個人識別符号の定義と範囲、取扱い」への関心が高いことがわかりました。

企業がセキュリティ対策を重視する中、十分なセキュリティ対策が講じられているかを第三者の立場で客観的に判断する手段として、認定／認証制度やセキュリティ監査がありますが、今回の調査で、回答企業の約８割が定期的または不定期に情報セキュリティ監査を実施していることがわかりました。

このほか、過去１年間に受けたセキュリティインシデントの状況、セキュリティ支出の動向、情報セキュリティ対策の実施状況、情報セキュリティ製品の導入状況など、広範囲にわたる企業IT化の現状について、経年分析を含めて報告しています。

あわせて、2019年10月から2020年３月の情報化動向をとりまとめ、紹介していますので、今後のIT環境整備の参考にしていただければ幸いです。

2020年５月

一般財団法人日本情報経済社会推進協会

JIPDEC IT-Report 2020 Spring

Contents

特集「企業IT利活用動向調査2020」にみるIT化の現状 …… 01

1. 調査概要 …… 01
2. 経営における情報セキュリティの位置づけ …… 02
3. 認定／認証制度に対する意識 …… 10
4. 国内外の個人情報保護施策への取組み …… 12
5. セキュリティ製品／技術の利用動向 …… 15
6. 働き方改革とクラウドサービスの動向 …… 21
7. 電子署名／電子契約など …… 25
8. 総評 …… 29

回答者プロフィール …… 30

〈資料〉情報化に関する動向（2019年10月～2020年３月） …… 32

特 集

「企業IT利活用動向調査2020」にみるIT化の現状

JIPDECは、調査会社の株式会社アイ・ティ・アール（ITR）の協力を得て、国内企業の情報システム系および経営企画系部門等に所属し、IT投資と製品選定、もしくは情報セキュリティ管理に携わる役職者を対象に、情報セキュリティ対策に重点を置いた「企業IT利活用動向調査」を実施した。ここでは調査結果のなかから特徴的な傾向をピックアップし、日本国内におけるIT利活用の実態を紹介する。設問により、2019年調査（以下、「前回調査」という。）と比較・分析して紹介する。

1 調査概要

1-1. 調査概要

・実査期間：2020年１月14日～１月20日
・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：従業員数50人以上の国内企業に勤務し、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、IT戦略策定または情報セキュリティ従事者で、係長相当職以上の役職者約5,000人（経年比較で紹介する2019年調査に限り、課長相当職以上を対象）。
・有効回答数：878件（１社１人）

1-2. 回答者のプロフィール

回答者の業種で最も多かったのは製造業（30.1％）、次いでサービス業（23.6％）、情報通信（18.3％）、建設・不動産（8.3％）、卸売・小売（7.7％）、金融・保険（6.7％）となった。所属部門では情報システム部門が最も多く（34.2％）、役職は課長（33.8％）、本部長・部長（33.1％）が回答の約７割を占めている。

IT戦略や情報セキュリティへの関与度合いをみると、回答者に情報システム部門所属が多いことも関係しているからか、「セキュリティ製品の導入・製品選定に関与している」（53.9％）、「全社的なリスク管理／コンプライアンス／セキュリティ管理に責任を持っている」（43.2％）とする回答が多く、前回調査と傾向はあまり変わっていない。

2 経営における情報セキュリティの位置づけ

本調査では、企業における重要テーマとして定着しつつある「情報セキュリティ」を一貫してメインテーマとしている。まずは、経営課題の中での情報セキュリティの位置づけと、リスクの重視度合いを中心に調査結果をみる。

2-1. 重視する経営課題

重視する経営課題については、全22項目の経営課題を取り上げ、今後１～３年で何を重視しようとしているかを回答してもらった（図１）。「業務プロセスの効率化」（55.6%）がトップとなり、次いで「従業員の働き方改革」（48.6%）、「情報セキュリティの強化」（41.1%）の順となったが、その差は縮まっている。前回調査と比べ、特に変化が著しかったのは法規制への対応で、なかでも、「個人情報保護法への対応」については、６ポイント以上（15.2%→21.6%）の上昇がみられた。

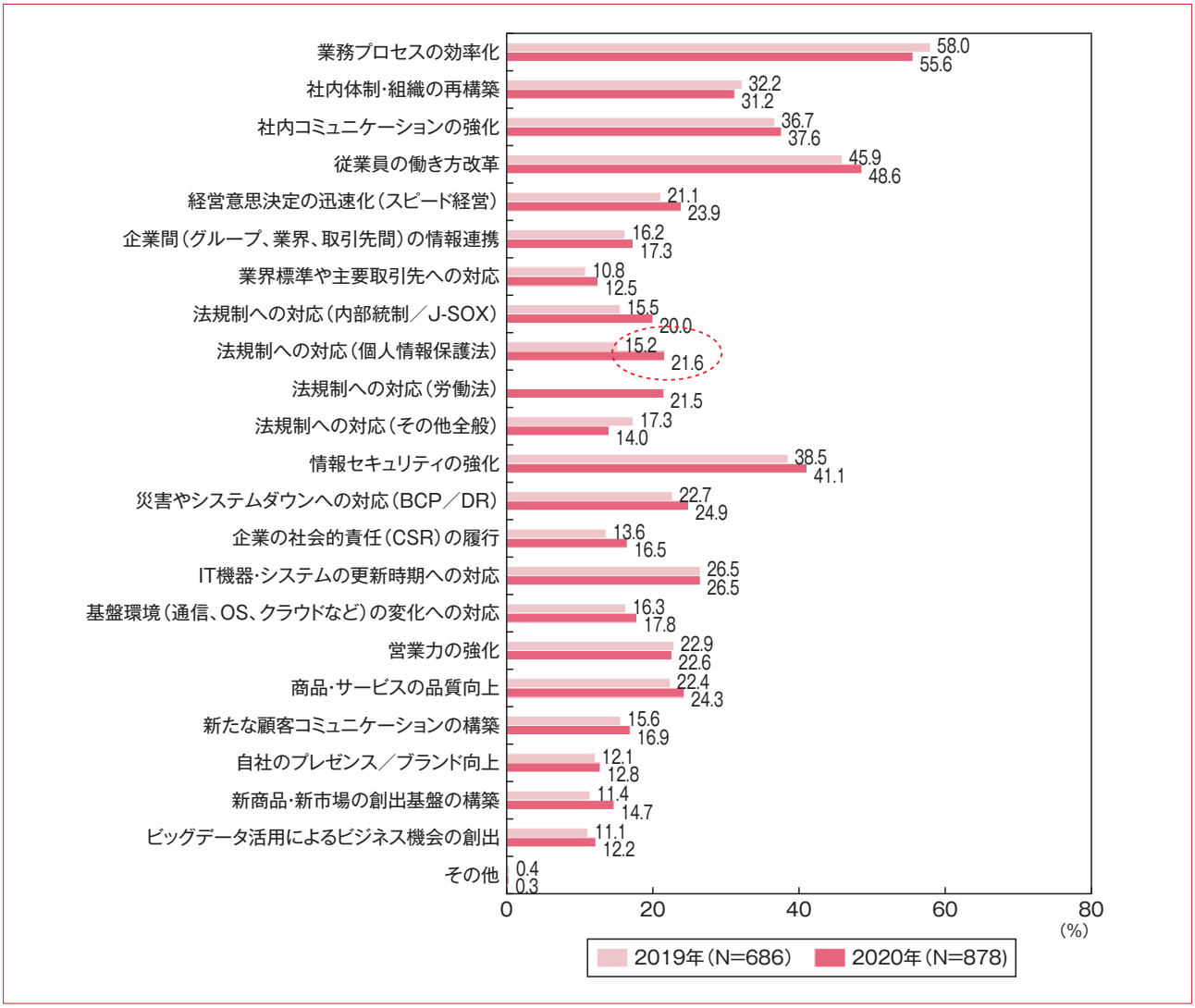

図１．今後重視したい経営課題（2019～2020年比較）

2-2. セキュリティインシデントの認知状況

過去１年間に回答者の勤務先が経験したセキュリティインシデントについて、最も高かったのは前回調査で２位だった「従業員によるデータ・情報の紛失・盗難」（24.8%）であった。次いで前回３位の「社内サーバ／PC／スマートフォン等のマルウェア感染」（24.0%）が２位、前回１位だった「モバイル端末（PC／タブレット／スマートフォン）の紛失・盗難」（20.4%）が３位になるなど、上位の順位が入れ替わった（図２）。

また、個人情報の漏えい・逸失および個人情報をめぐるトラブル発生についても３～４ポイント増加しており、特に従業員数規模が大きくなるほど発生率が高くなっている（図３）。

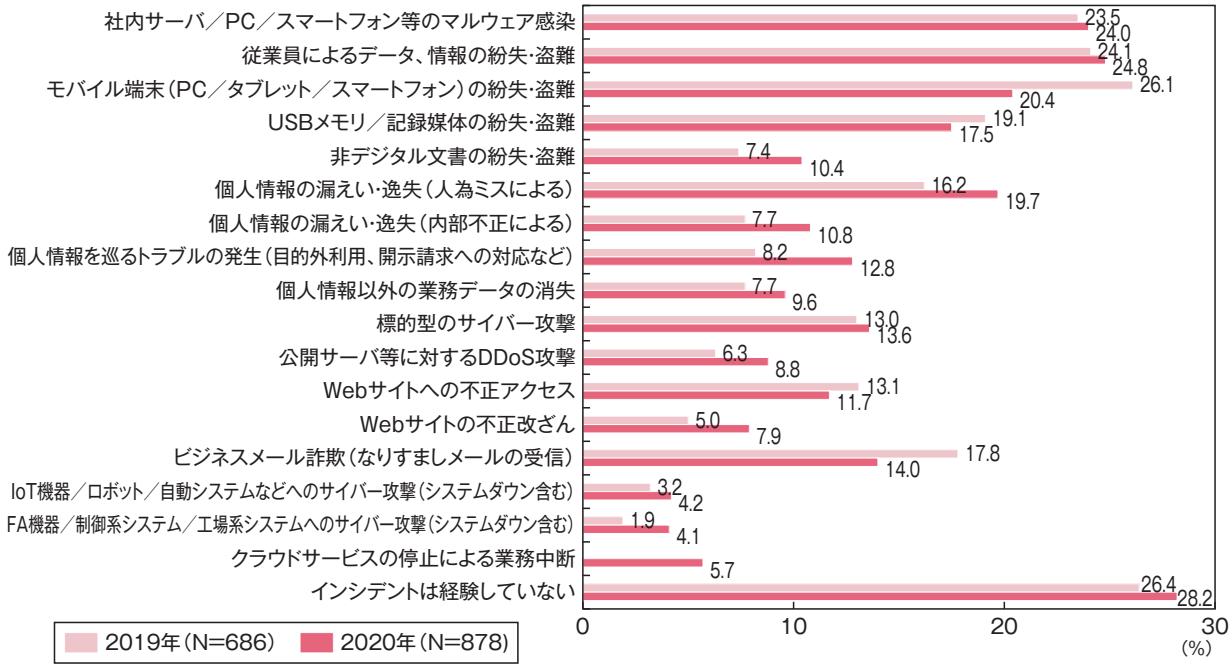

図２．過去１年間に認知したセキュリティインシデント（2019～2020年比較）

	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%

図３．過去１年間に認知したセキュリティインシデント（従業員数規模別）

2-3. セキュリティリスクの重視度合い

本調査では、「標的型のサイバー攻撃」および「内部犯行による重要情報の漏えい・消失」に対するリスクの重視度合いをそれぞれ定点観測しているが、それぞれ「経営陣から最優先で対応するよう求められている」とした回答が約３割となっており、前回調査と同様の結果となった（図４）。

「重視しており、優先度が高い」までを含めれば約７割が回答しており、対応優先度が高いリスクとして認識されていることがわかる。

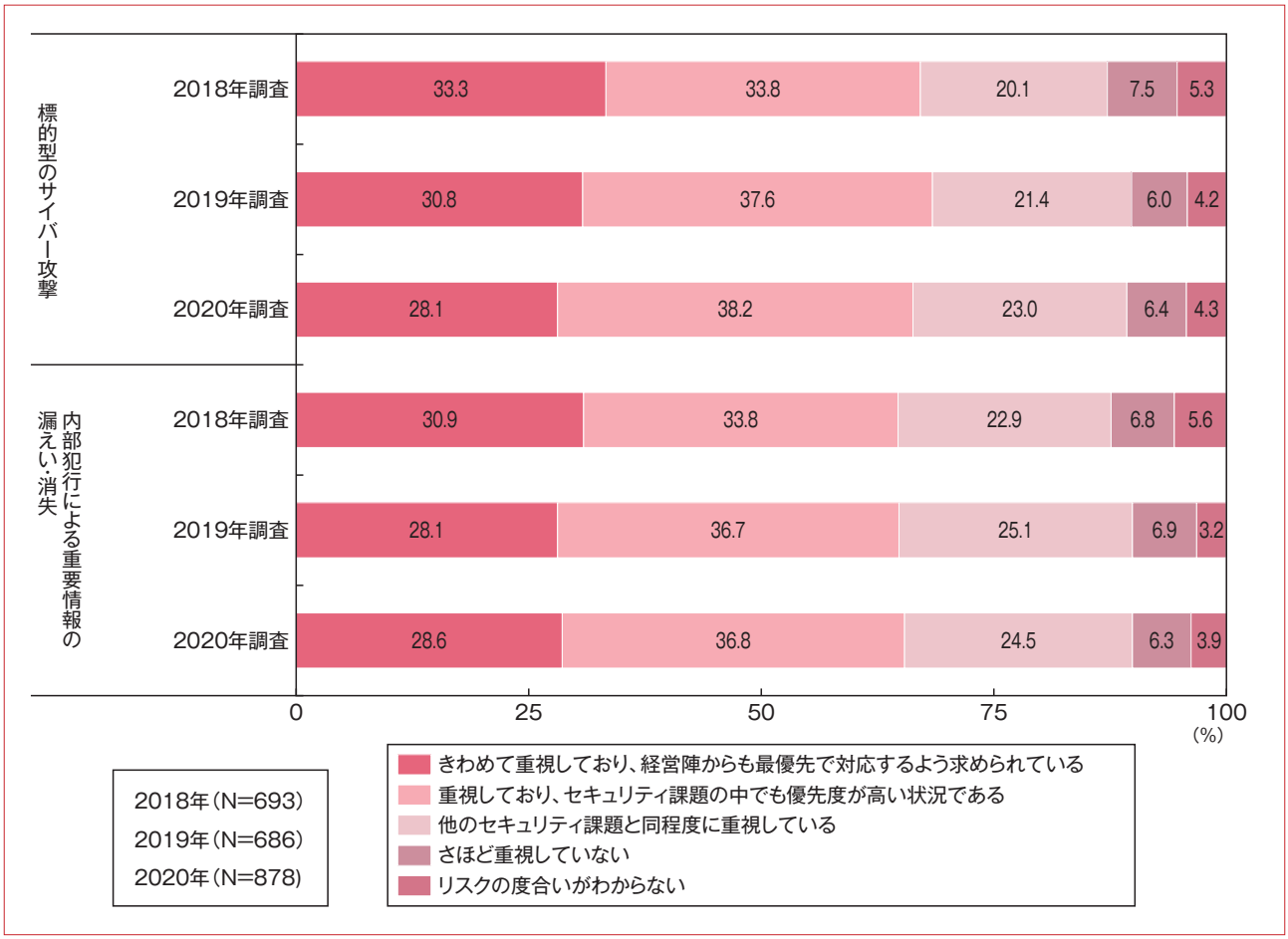

図４．セキュリティリスクの重視度合い（2018～2020年比較）

標的型サイバー攻撃に対する重視度合いについて業種別にみると、「きわめて重視し最優先する」、または「重視し優先度が高い」のは「金融・保険」、「情報通信」、「公共・その他」でいずれも７割を超え、対応優先度の高いリスクとして捉えていることがわかる。一方、「卸売・小売」、「サービス」の割合は５割強と若干低い結果となった（図５）。従業員数規模別にみると、規模が大きくなるほど、重視する割合が高くなっている。

内部犯行リスクについても、標的型サイバー攻撃と同様の傾向が業種別、従業員数規模別ともにみられた。

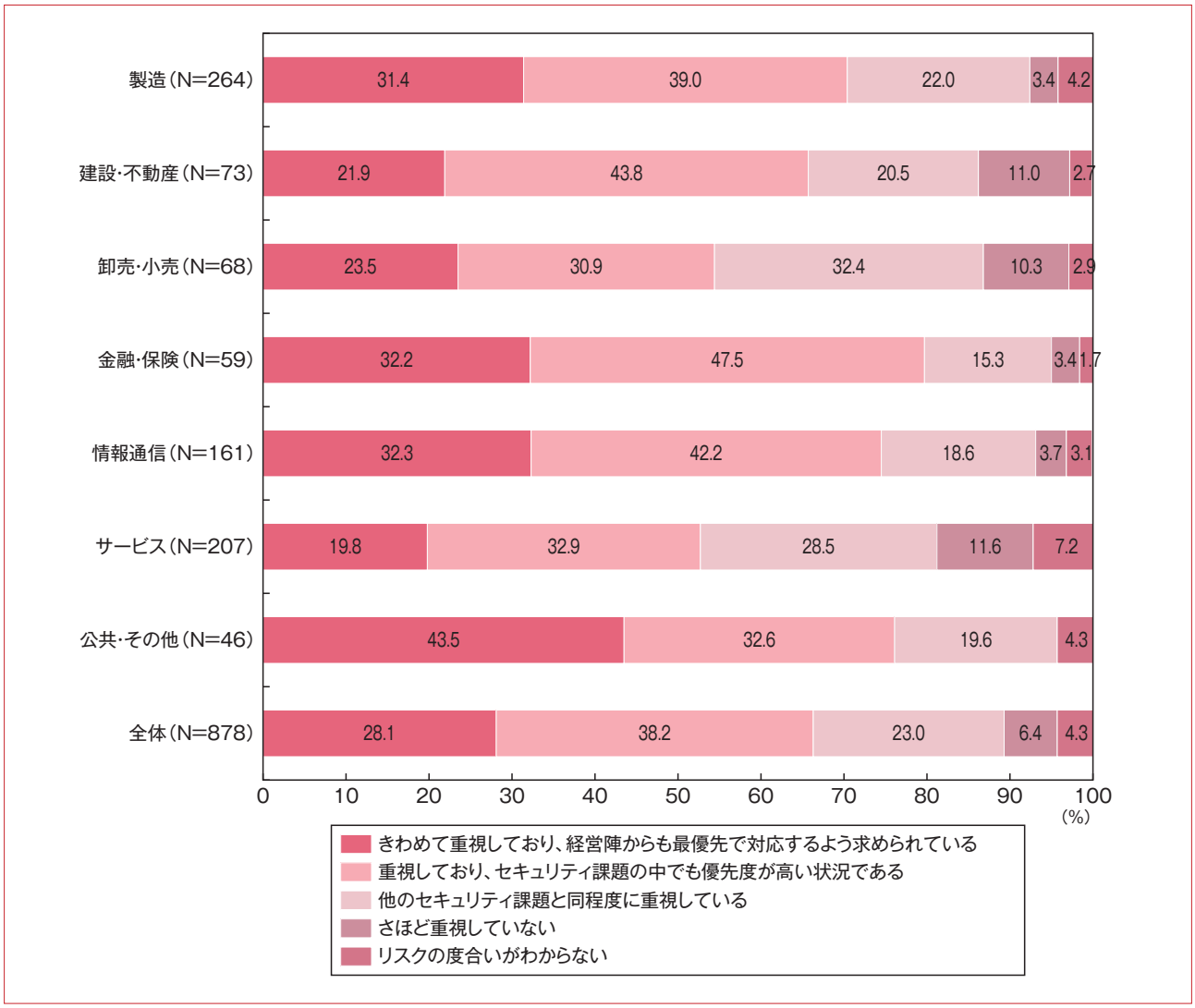

図５．標的型サイバー攻撃に対するリスクの重視度合い（業種別）

2-4. セキュリティ対策の実施状況

具体的なセキュリティ対策の実施状況はどのようになっているのか。この調査では、「標的型のサイバー攻撃対策」、「内部犯行による重要情報の漏えい・消失対策」の代表的な取組みをピックアップし、その実施率についても観測している。

「標的型サイバー攻撃対策」として最も実施率が高かったのは、「重要なシステムのインターネットからの隔離」（56.3%）、「メール添付のフィルタリング」（53.3%）、「PC管理者権限の制御」（53.2%）の順となった。また、現状未実施だが３年以内の実施を予定している対策としては、「IoT/FA/制御システムへのセキュリティ対策」（28.8%）、「CSIRTの立上げ」（27.1%）が多く挙げられた（図６）。

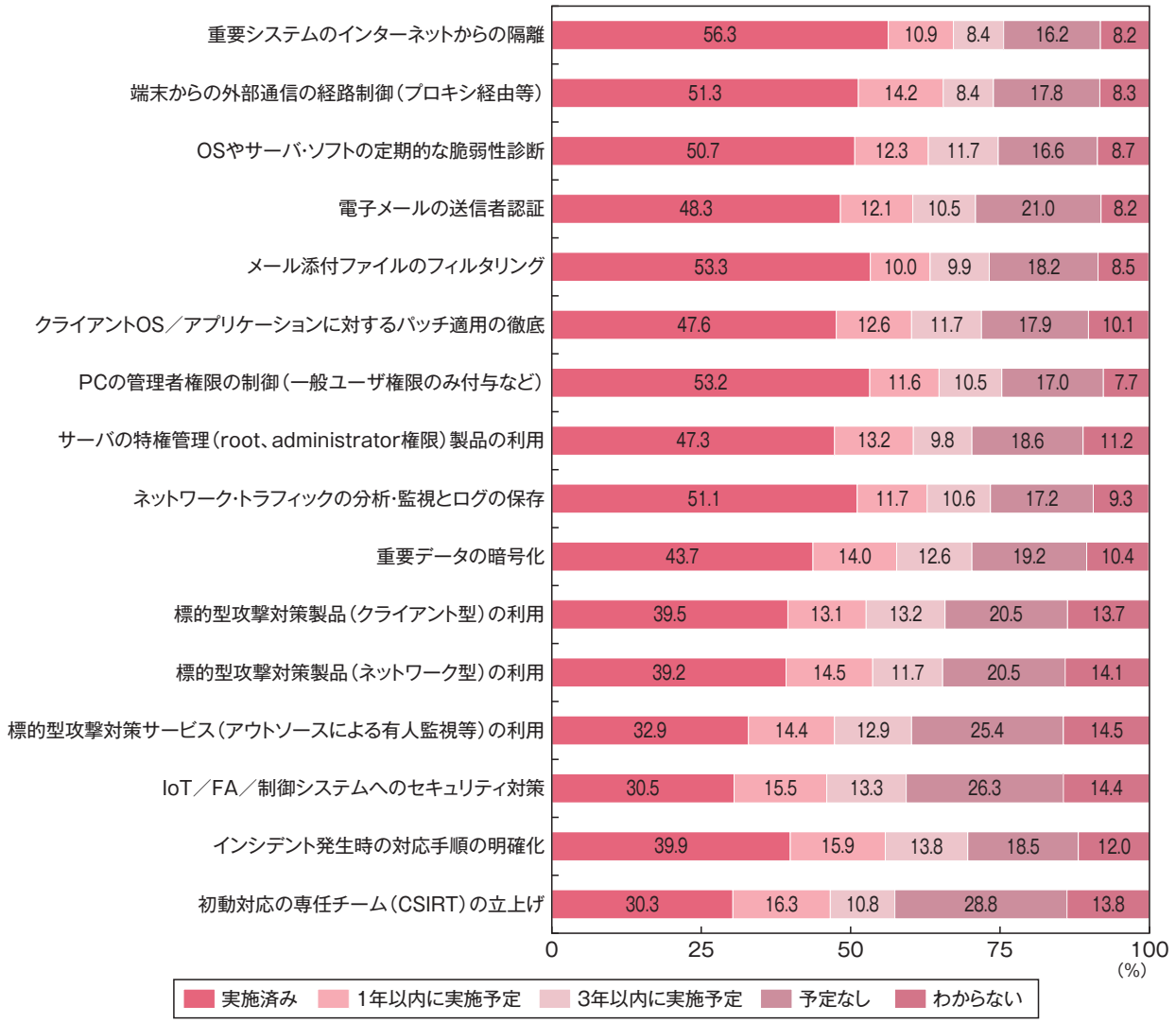

図６．主要な「標的型サイバー攻撃対策」の実施状況

一方、「内部犯行による情報漏えい・消失対策」としては、「重要情報にアクセスできる人員（部署）の制限」（57.2%）の実施率が最も高く、次いで「PCの社外持出しの禁止」（55.9%）、「一般社員向けの教育研修の実施」（54.9％）、「外部デバイスへのデータ移動の制限」（54.4％）の順となった（図７）。

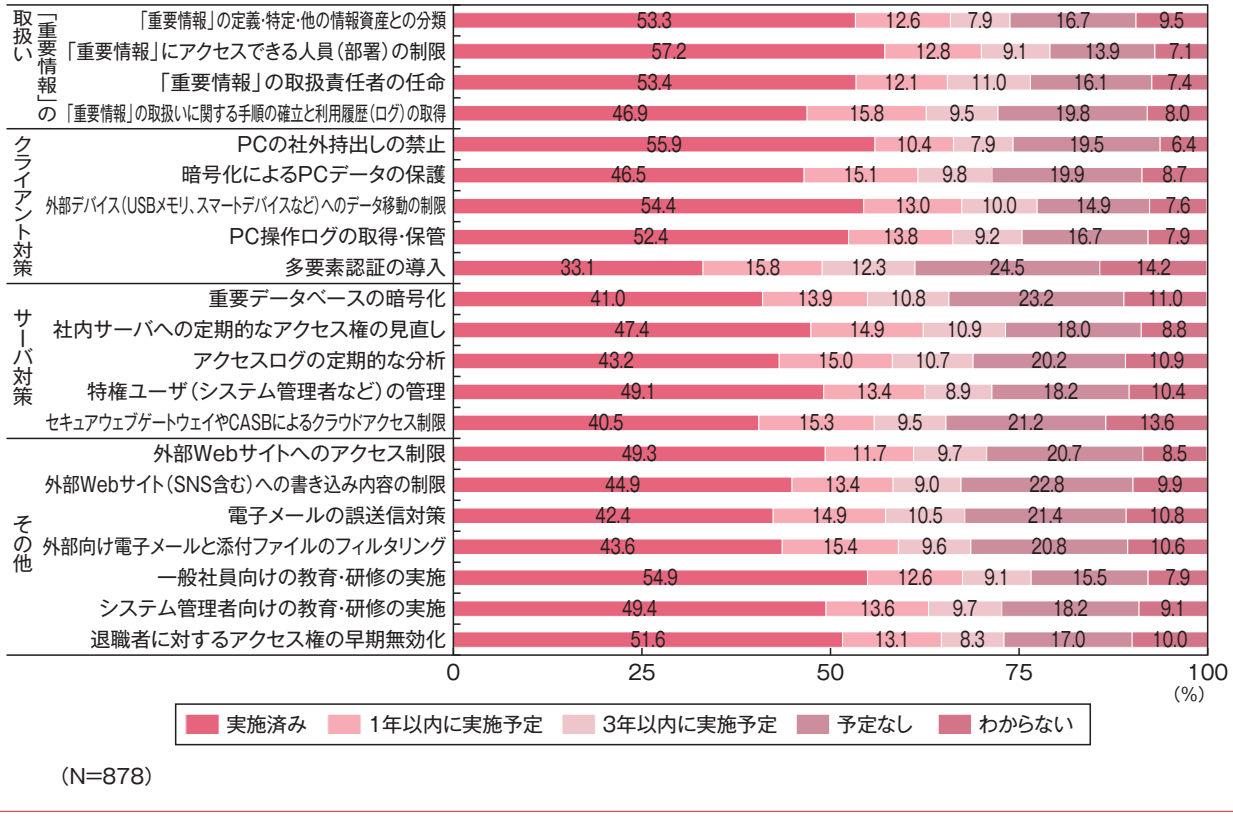

図７．主要な「内部犯行による情報漏えい・消失対策」の実施状況

2-5. システムリスク軽減策への取組み状況

システムリスク軽減策への取組み状況については、「事業継続計画（BCP）の策定」（54.7％）、「セキュリティポリシーに沿った対策の実施」（54.6％）、「全社的なリスクマネジメントシステムの構築」（53.8％）、「ITガバナンスの確立」（50.1％）が半数以上の割合で実施済みとなっており、上位３項目については、「現在実施中・変更中」を合わせれば７割近くで取り組まれている。

一方、「ITサービスマネジメントの実施」は実施済みが約４割となったが、一方で「予定なし・わからない」も３割と、他の対策に比べると取組み状況が低いことがわかる（図８）。

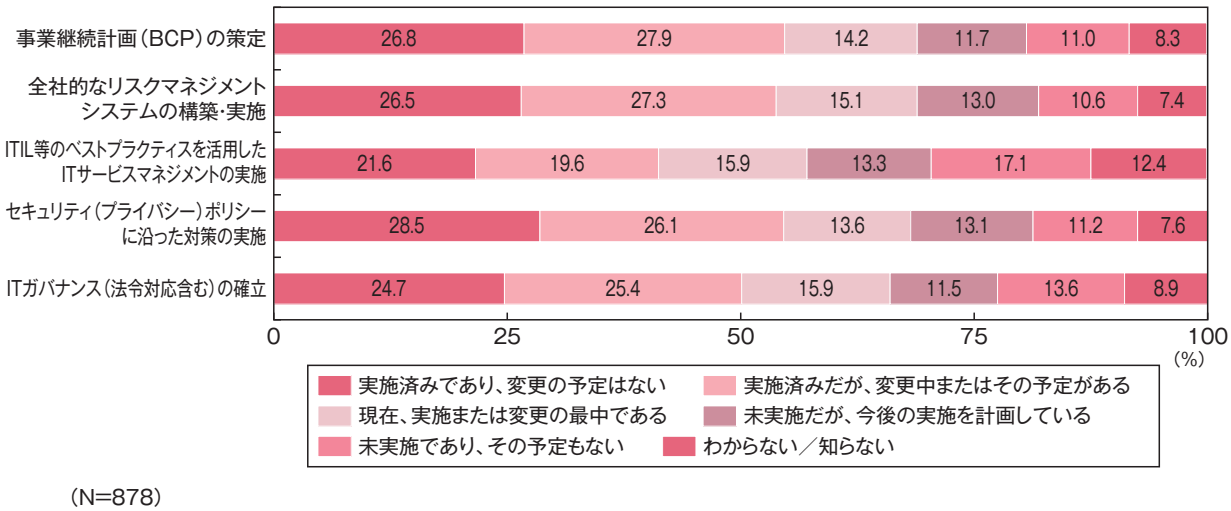

図８．システムリスクの軽減策の取組み状況

2-6. セキュリティ支出の動向

情報セキュリティ強化への意識が年々高まっている中、セキュリティ支出状況はどうなっているのか。主要な支出内訳として15項目を取り上げ、それぞれについて2020年度の支出の増減見込み（対前年度比）を調査した（図９）。

その結果、全項目とも「増加する見込み」と回答した企業の割合が２割前後となり、その中で最も数値が大きかったのは「セキュリティ関連の認証取得に関する費用」（25.3%）、次いで「災害対策（ディザスタリカバリ対策）」（23.3%）となっている。

また、全項目ともに横ばいが５割台、減少が１割未満となった。

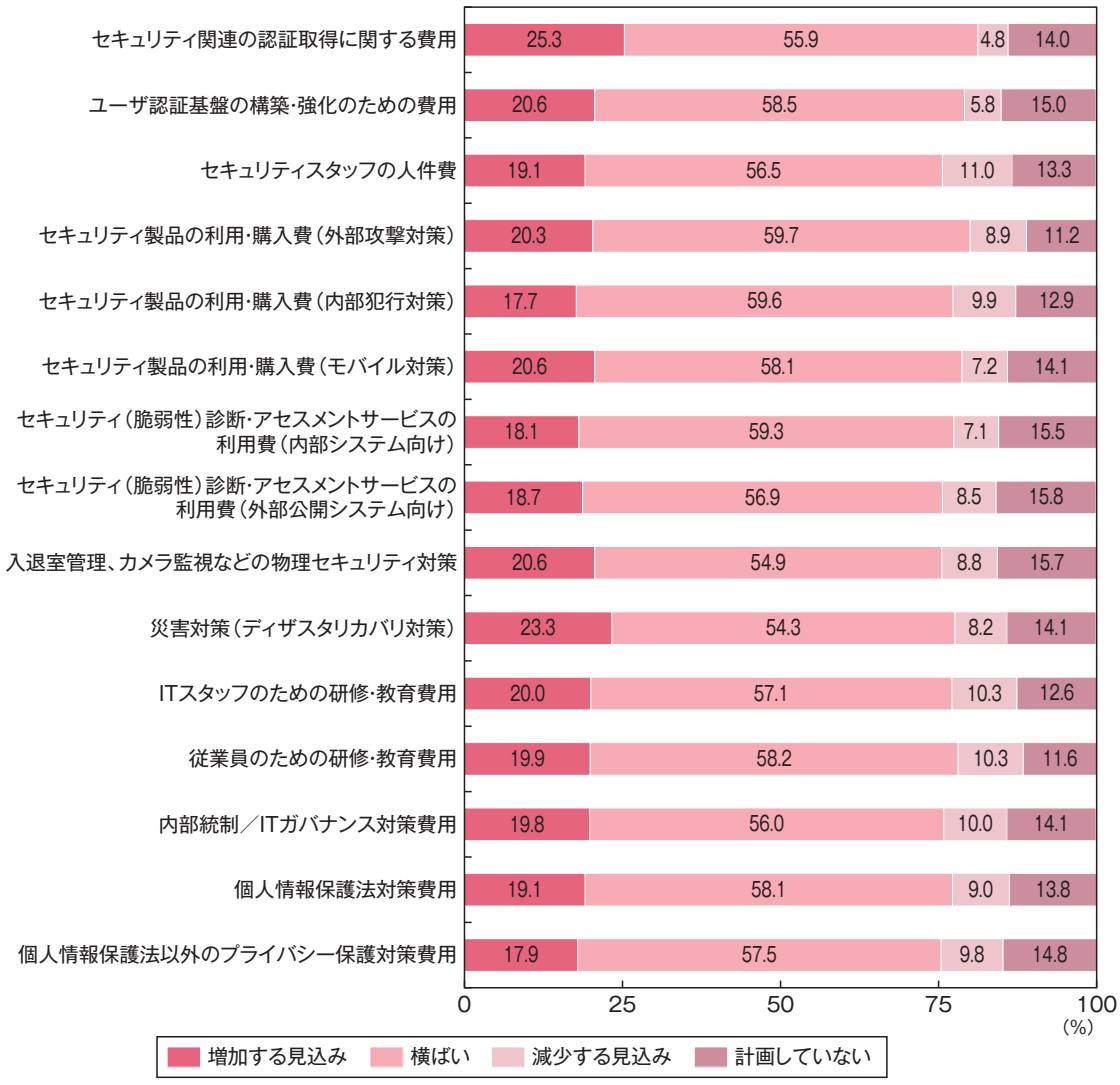

図９．2020年度に想定されるセキュリティ支出の増減傾向

増加するとの回答が最も高かった「セキュリティ関連認証取得費用」について、業種別および従業員数規模別に調査したところ、業種別では、前回調査では「公共・サービス」（42.5％）、「卸売・小売」（39.1％）、「建設・不動産」（33.8％）が３割を超えていたが、今回調査では「建設・不動産」（30.1％）、「金融・保険」（28.8％）、「情報通信」（28.6％）が高くなった。

また、従業員数規模別については、前回調査同様、規模が大きくなるほど、高くなる傾向がでている（図10）。

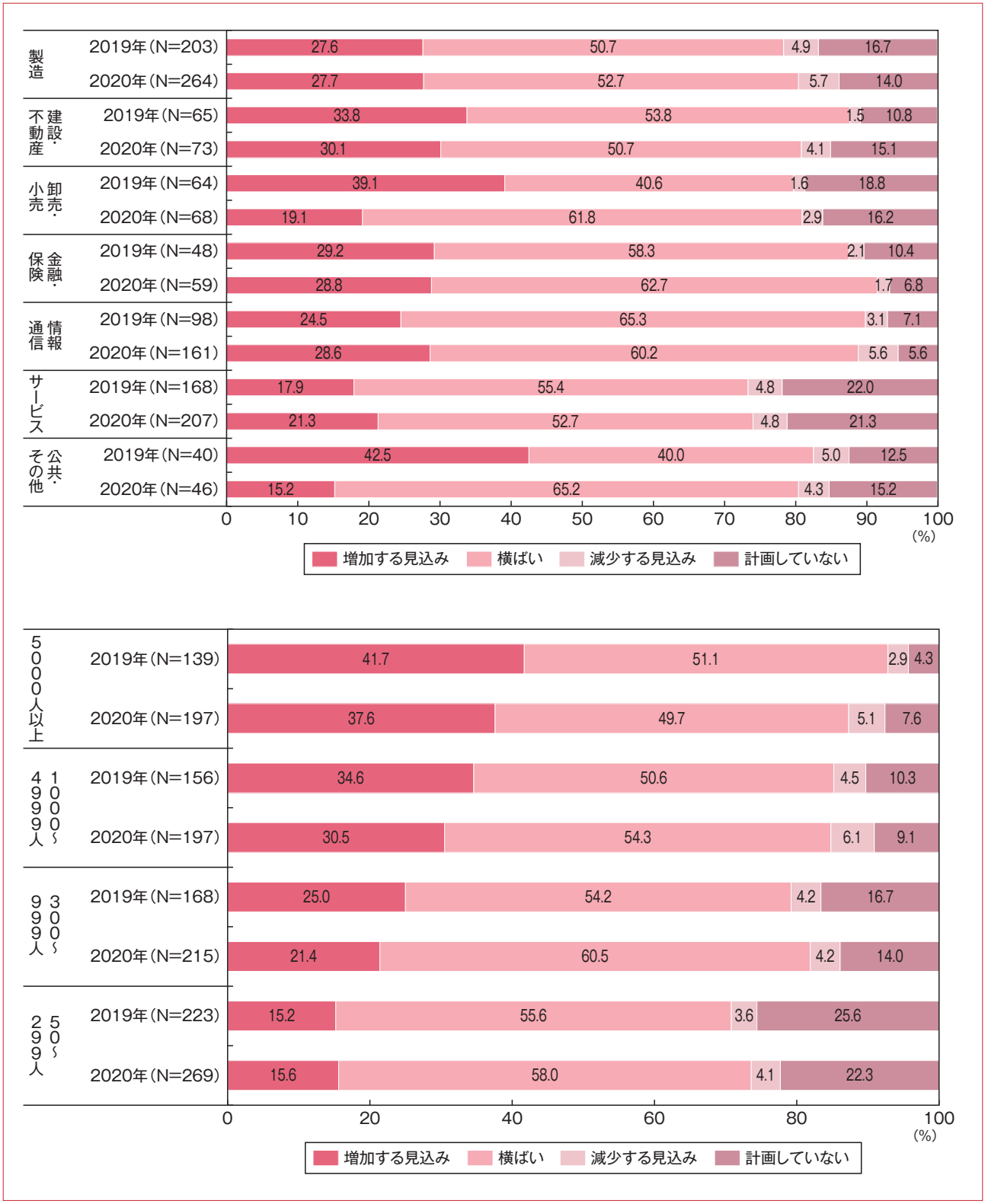

図10. セキュリティ関連認証取得費用の増減傾向（業種別・従業員数規模別）

3　認定／認証制度に対する意識

認定／認証制度は、自社の取組みを第三者に客観的に確認してもらうことで、精度や実効性を高めるのに有効である。また、第三者により評価を得ることで、顧客や取引先からの信頼が高まることも期待できる。

ここでは、認定／認証制度に対する意識について分析する。

3-1. 情報セキュリティに関する認定／認証制度の取組み状況

国内において取得可能である代表的な認定／認証制度について、それぞれの取得状況と今後の取得意欲について調査した。

「プライバシーマーク」の取得済みがやや増加して４割強、「ISMS」は取得済みが４割弱で、予定を含めると６割に近くなっている。他の制度は取得済みが約３割で、予定を含めても５割未満と、やや低い傾向にある（図11）。

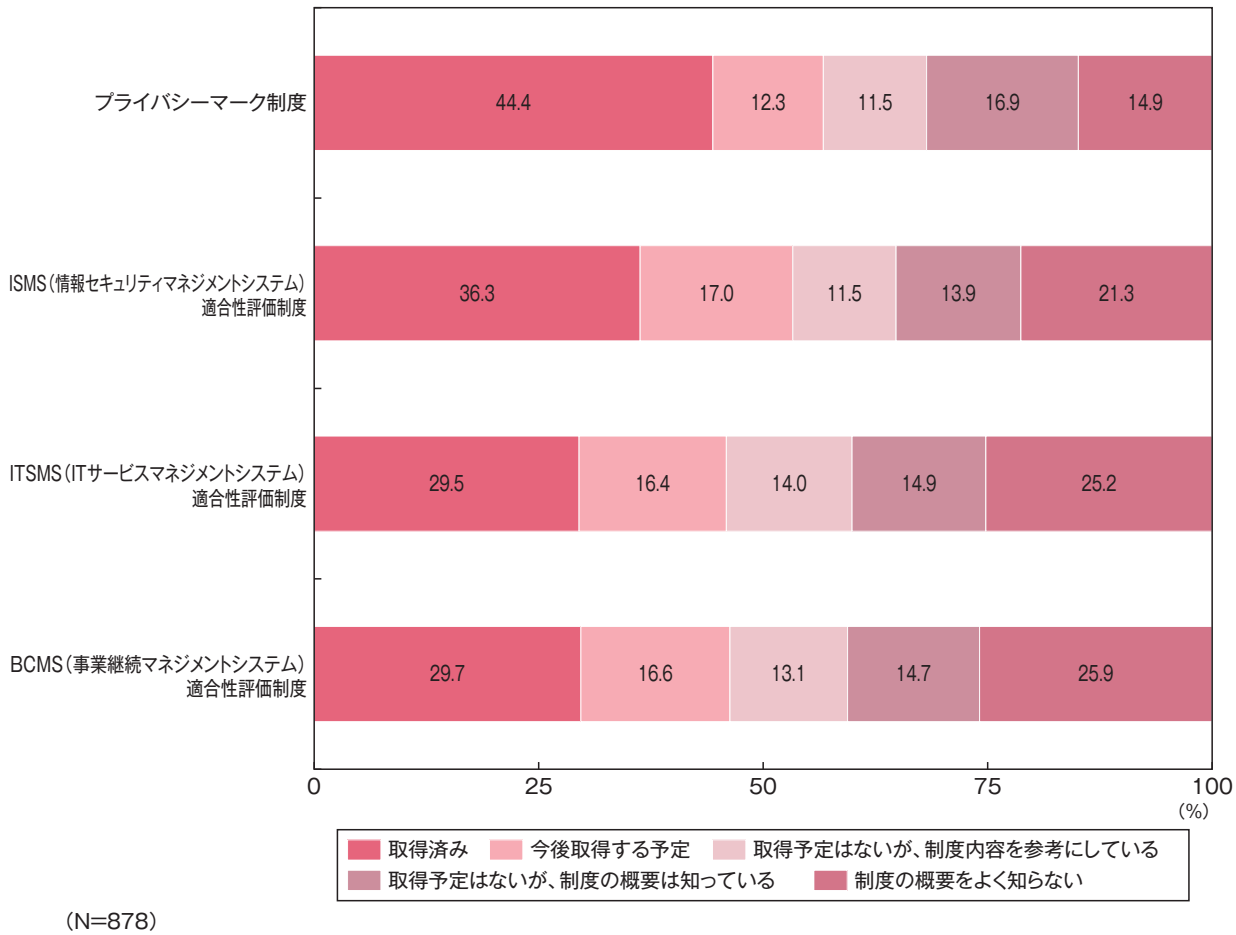

図11．情報セキュリティの認定／認証制度への取組み

2-6で示したように、セキュリティ関連の認定／認証取得費用の支出増加見込みが最も高い数値（25.3%）となった。企業が取引先や消費者からの信頼を得るために第三者による認定／認証を得る必要性が高まっていることと考えられるが、調査結果からも、認証取得の価値（効果）の理由として、「取引先から信頼を得るため」（55.0%）が最も多かった。次いで「社内の情報セキュリティ体制を高度化させるため」（43.5%）、「コンプライアンスのため」（40.1%）が続いている（図12）。

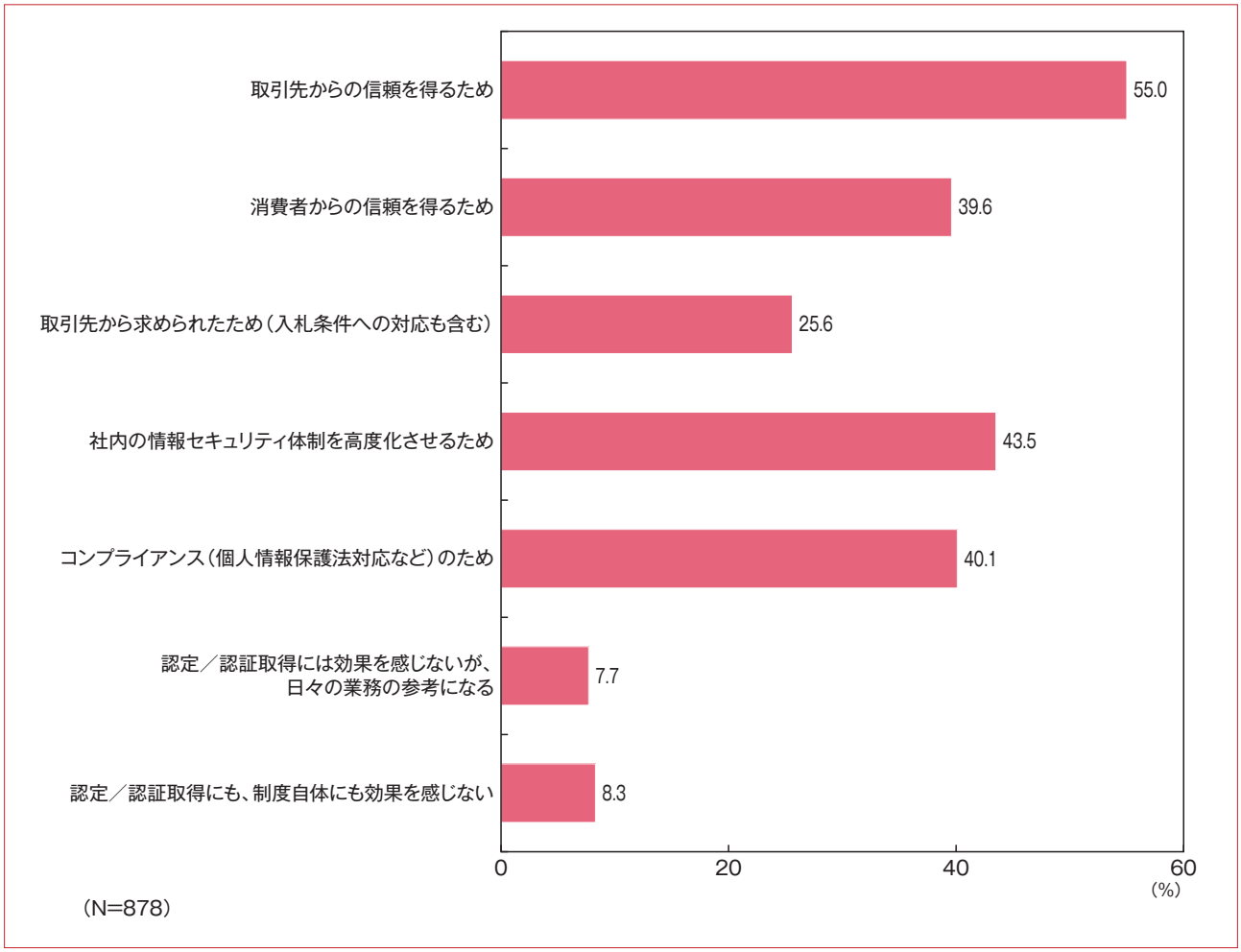

図12. 第三者から認定／認証を取得することの価値（効果）

4　国内外の個人情報保護施策への取組み

個人情報保護施策に関しては、国内では個人情報保護法改正後、2017年にJIS Q 15001規格が改正され、また、個人情報保護法のいわゆる３年ごとの見直しにより、改正案が2020年３月に閣議決定されている。

海外でも2018年５月から一般データ保護規則（GDPR）が運用開始され、米カリフォルニア州消費者プライバシー法（CCPA）も2020年１月１日より施行されるなど、ここ数年の間にグローバルにプライバシー法規制が整備されつつある中、日本企業の取組み状況については、まだ十分ではない状況が見えてきている。

4-1. JIS Q 15001規格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事項

JIS Q 15001:2017規格改正および個人情報保護法再改正検討中の項目についての関心事項については、「個人識別符号の定義と範囲、取扱い」（35.0%）が最も高く、「要配慮個人情報の定義と範囲、取扱い」（30.5%）が続き、「個人データの第三者提供」（29.3%）は３位となった。

保護法再改正検討中項目である「利用停止請求権の拡大」は15.9%、「漏えい時の罰金引上げ」は9.5%とあまり関心は高くなかった（図13）。

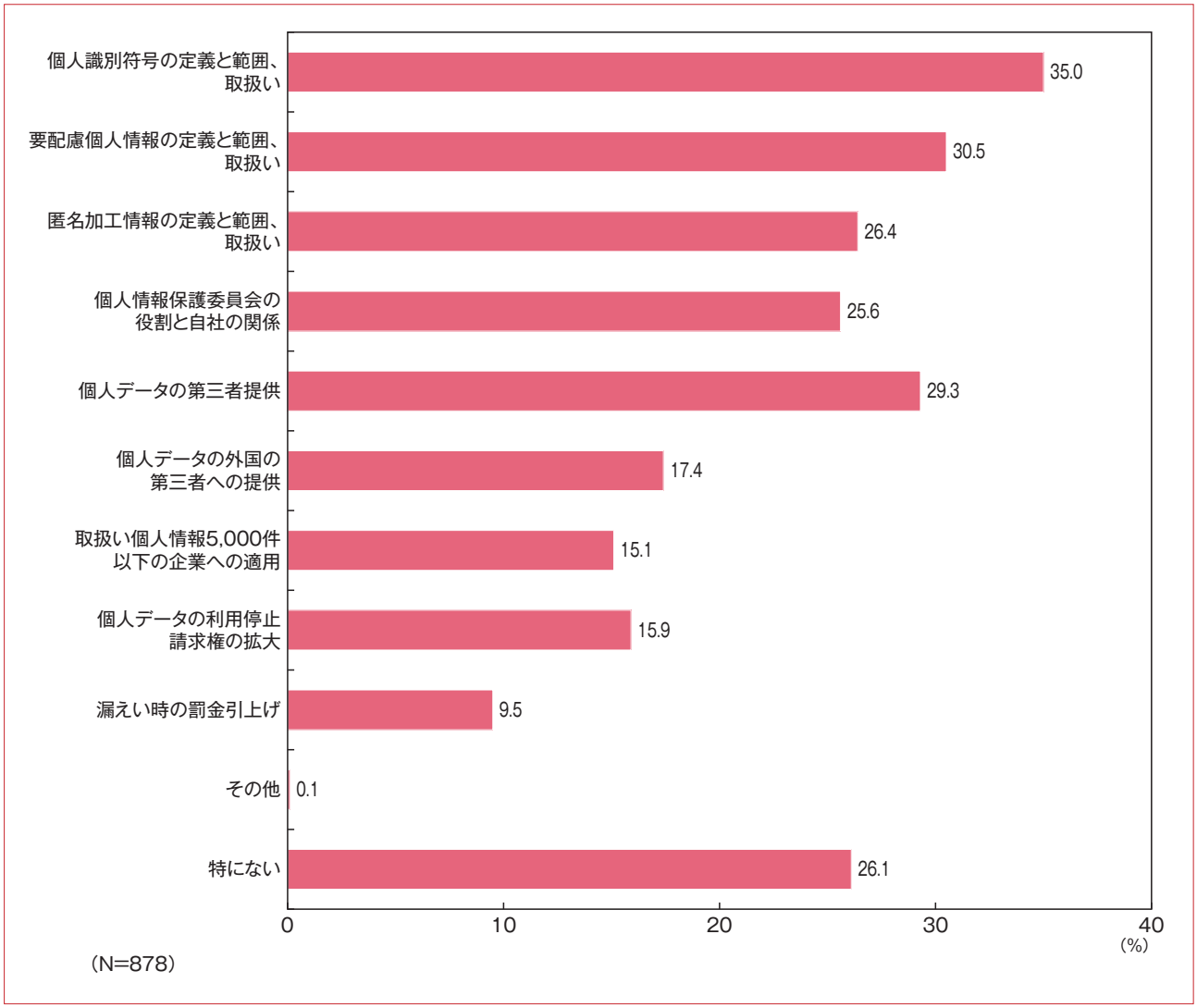

図13.　JIS Q 15001改正および個人情報保護法改正検討中の内容についての関心事項

4-2. 海外のプライバシー規制等の認知度

GDPR施行についてはマスコミ等でも大きく報じられたこともあり、認知度は約５割と最も高く、その他、CBPR（APEC）、米国カリフォルニア州消費者プライバシー法（CCPA）、中国サイバーセキュリティ法の順となった。いずれも本調査（2020年１月）時点で施行されている法規制・枠組みであるが、認知度は約２～３割と、前回調査と比べてもほとんど変化は見られない（図14）。

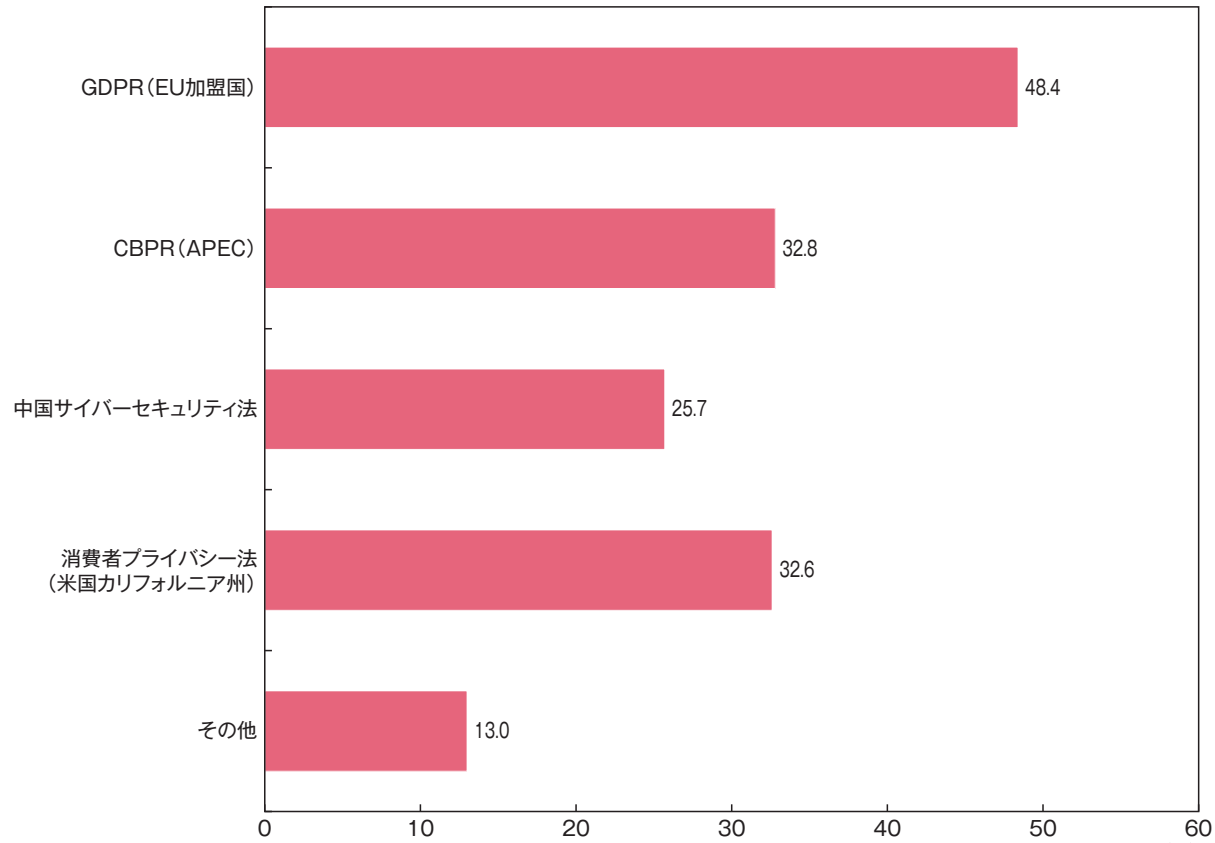

図14. 海外のプライバシー規制・枠組みの認知度

4-3. GDPRへの対応状況

GDPRについては、2019年１月に日本とEUとの間で十分性認定が合意されたことにより、個人情報保護法とGDPR補完ルールを遵守することで対応することとなった。

EUにビジネス拠点または顧客を持つ企業に対し、GDPRへの対応状況を調査した。「GDPRまたはGDPR補完ルールに則った形で個人情報を移転する」は37.9％で最も多く、次いで「GDPRを気にすることなく個人情報を移転する」が18.1％、「現地法人が対応しているので直接GDPRに関与していない」が16.1％という結果となった。この傾向については、前回調査とほとんど変化はない。（図15）。

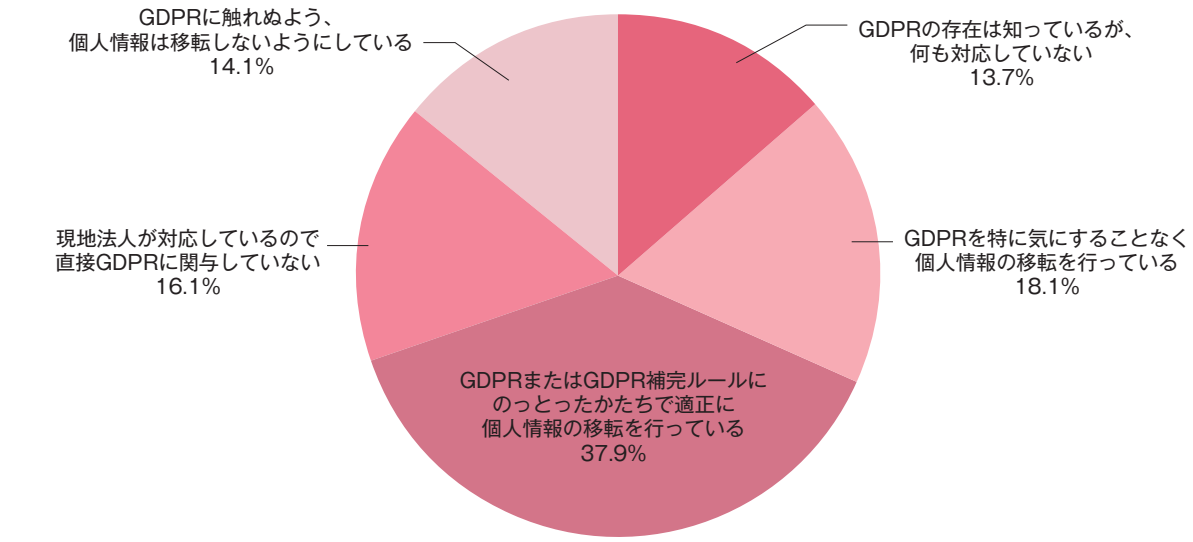

図15. GDPRの対応状況

4-4. GDPRの適正移転の方法

「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（図16）。

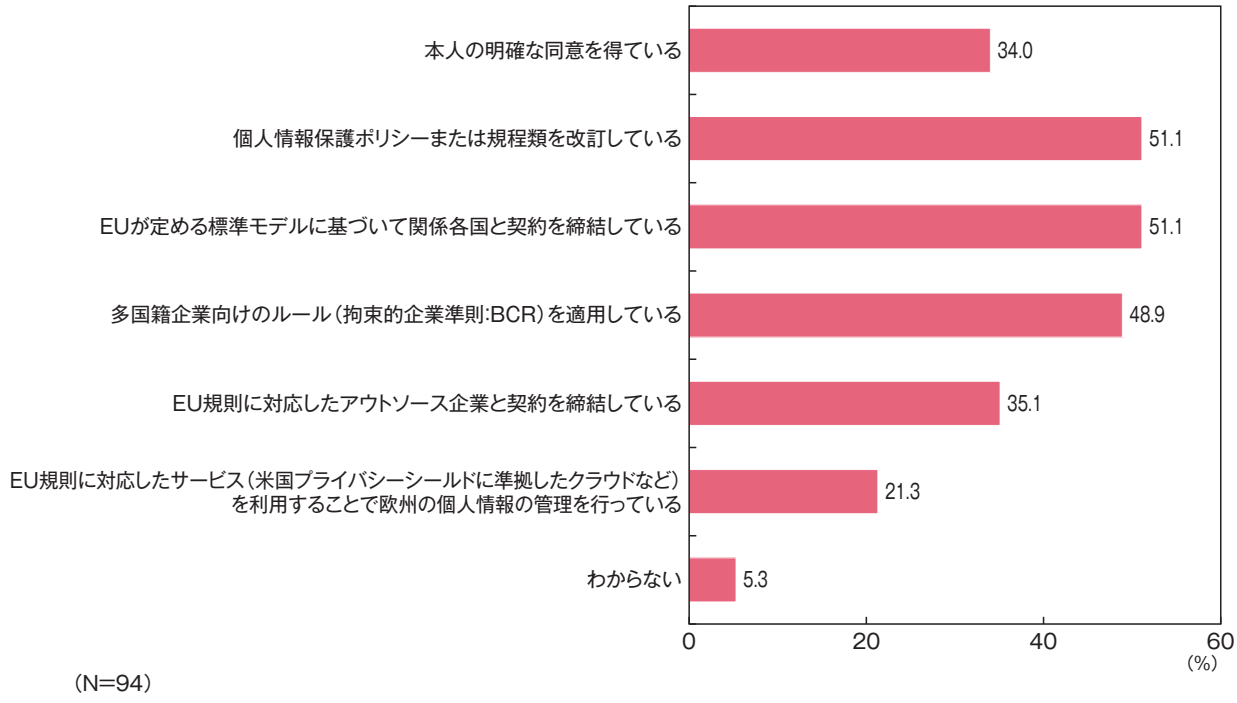

図16. GDPRの適正移転の方法

5　セキュリティ製品／技術の利用動向

サイバー攻撃の巧妙化／複雑化とクラウド化の進行によって、対応するセキュリティ製品／技術も進化してきているが、実際の利用状況はどうなのか。ここでは、主要なセキュリティ製品の導入状況を分野別に調査した。調査結果から、新しい製品／技術の採用は進んでいないことがわかった。

5-1. ネットワーク／ゲートウェイセキュリティ製品の利用状況

ネットワーク／ゲートウェイ系のセキュリティ製品では、これまで社内ネットワークとインターネットを隔てるファイアウォールや、インターネットから社内ネットワークに入るためのVPNが主な製品であったが、社内システムのクラウド環境への移行によってゼロトラストネットワーク化が進み、クラウドサービスへのアクセスを制御するCASB（Cloud Access Security Broker）のような新しいセキュリティ製品が登場してきた。今回の調査結果では、現行のファイアウォール（78.9%）やVPN（50.5%）の利用は若干減少してきたがまだ多く、CASB（22.9%）の利用は増えていない（図17）。

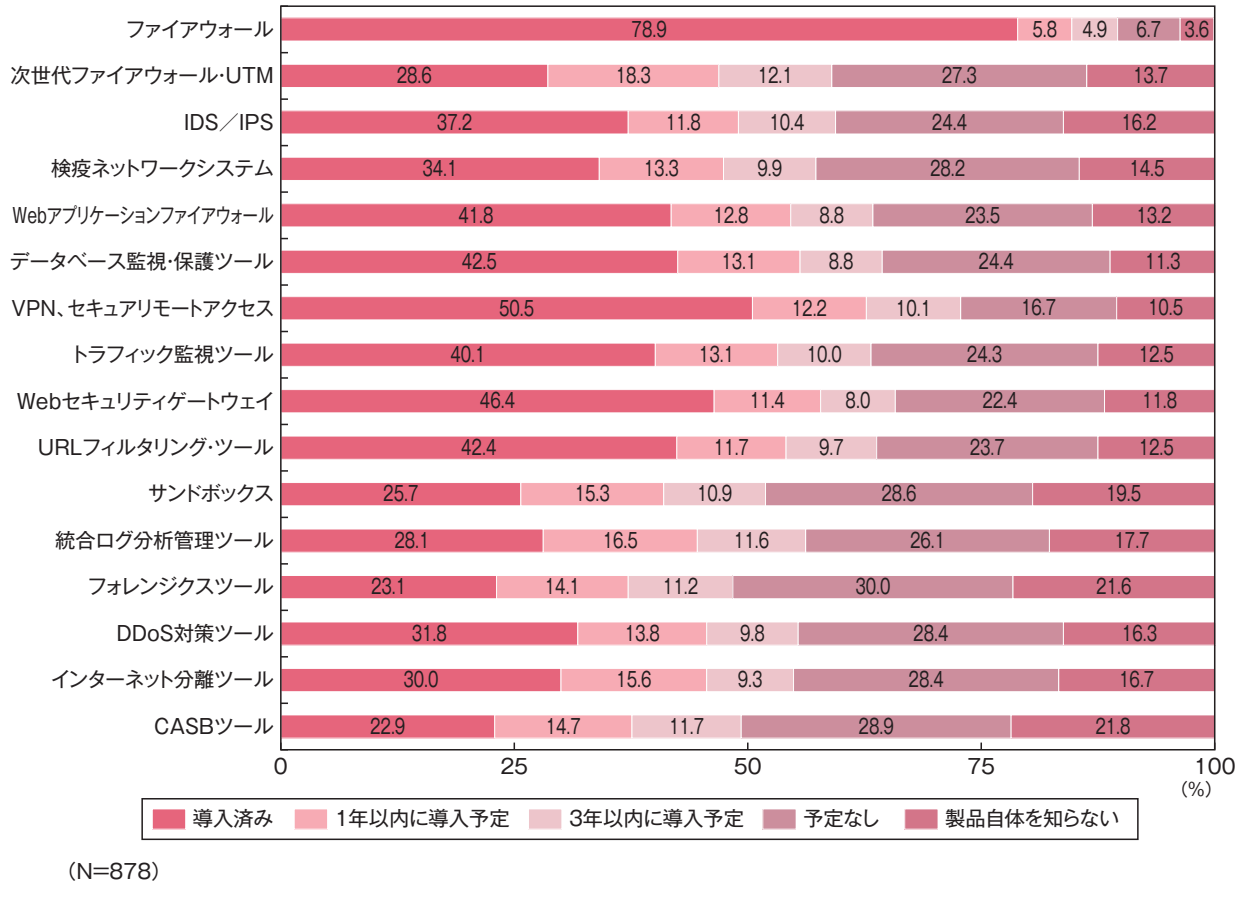

図17. ネットワーク／ゲートウェイセキュリティ製品の利用状況

従業員数規模別にみると、既存ネットワーク／ゲートウェイ系セキュリティ製品の代表であるファイアウォールが中小規模から大規模までまんべんなく導入されているのに対し、次世代セキュリティ製品の代表であるCASBは導入に大きな差が出ており、前回調査同様、大企業ほど新しいセキュリティ製品の導入に積極的であることがわかる（図18）。

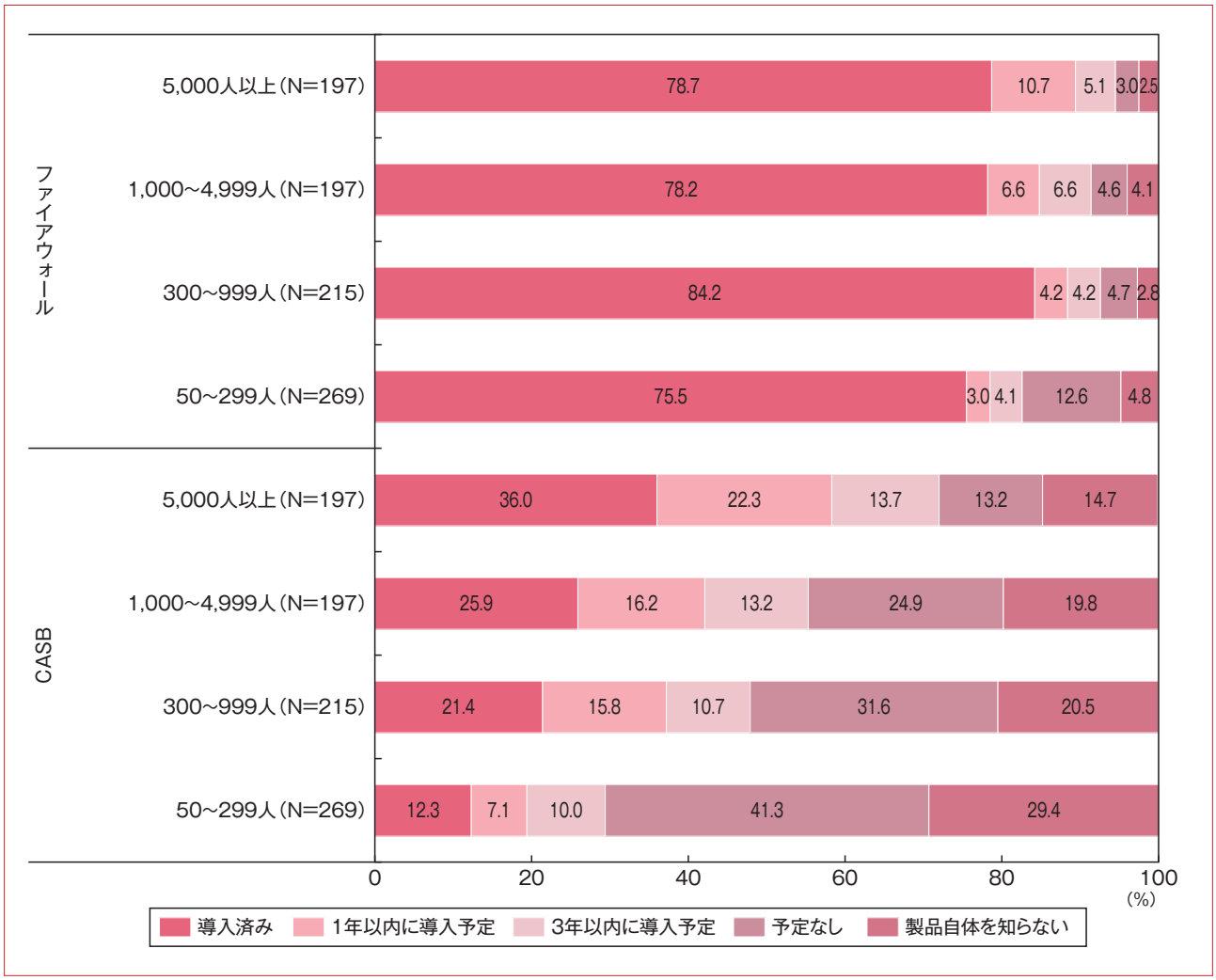

図18. ネットワーク／ゲートウェイセキュリティ製品の利用状況（従業員数規模別）

5-2. エンドポイントセキュリティ製品の利用状況

エンドポイント（クライアント）系のセキュリティ製品についても、従来はウイルス対策ソフトが中心だったが、標的型攻撃やランサムウェアのような巧妙かつ複雑な攻撃に対応するため、振舞いや兆候の段階から検知して対応するEDR（Endpoint Detection and Response）等の次世代型のエンドポイントセキュリティ製品が登場してきている。しかし実際の導入状況の傾向は、前回調査とほとんど変わらず、現行のウイルス対策ソフト（78.8%）が中心であり、次世代型のEDR（26.8%）の導入状況は多くない（図19）。

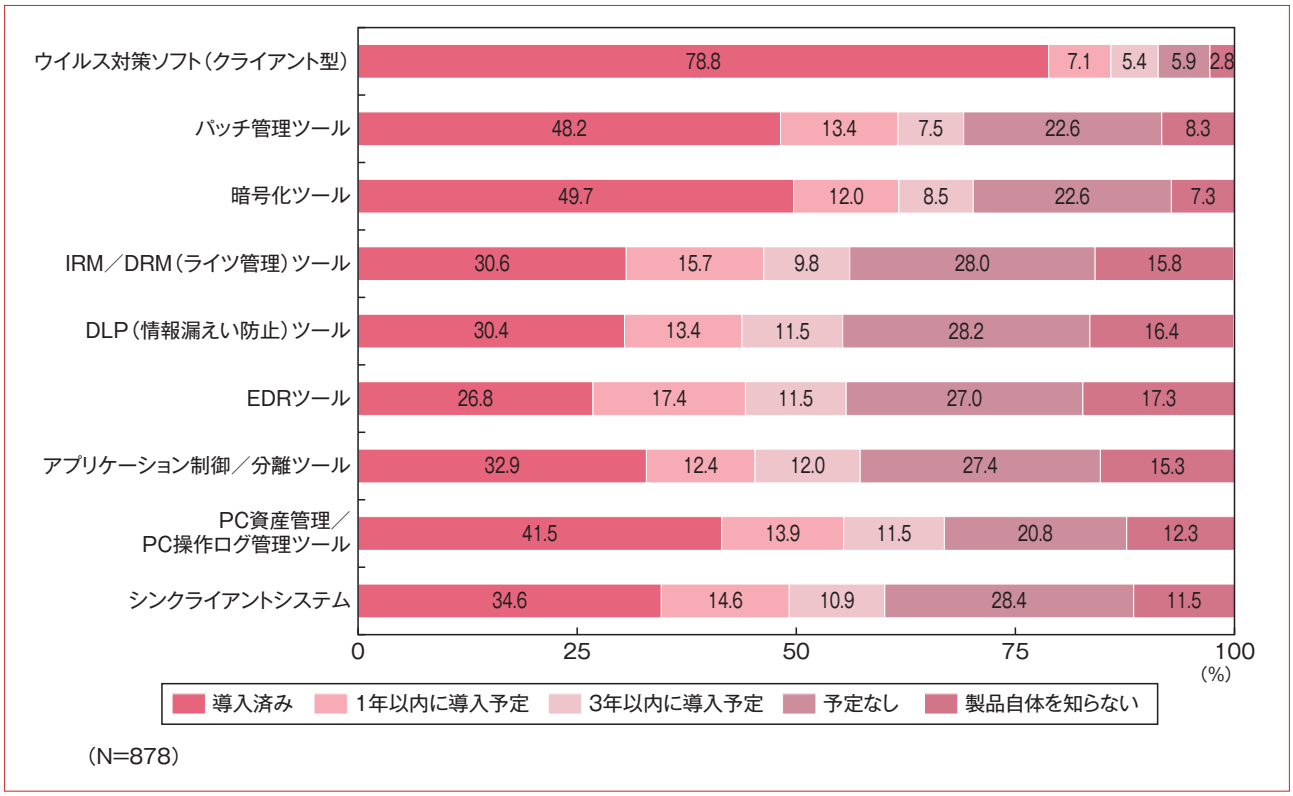

図19. エンドポイントセキュリティ製品の利用状況

従業員数規模別にみると、既存のエンドポイントセキュリティ製品の代表であるマルウェア対策ソフトが中小規模から大企業までまんべんなく導入されているのに対し、次世代型エンドポイントセキュリティ製品の代表であるEDRは導入状況に大きな差があり、大企業では約５割で導入されているが、中小企業では約１割となっている（図20）。

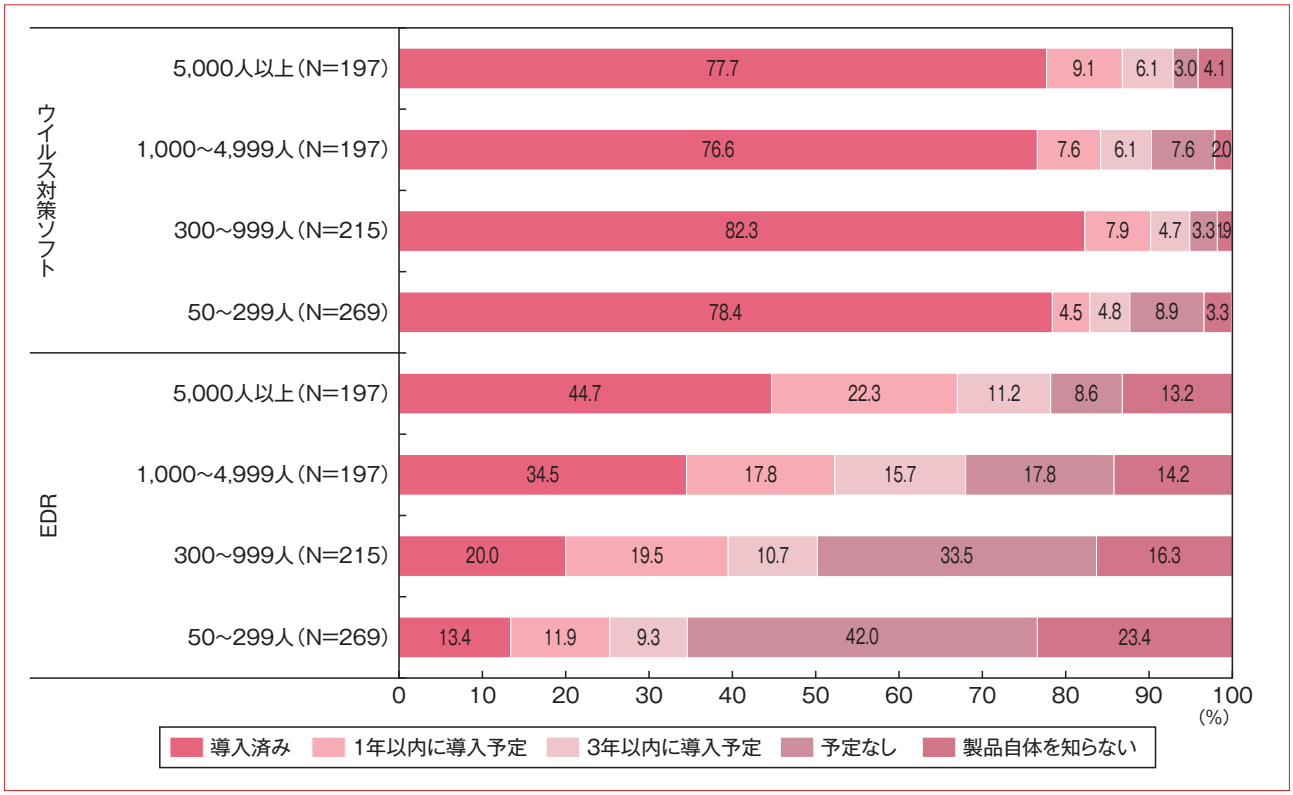

図20. エンドポイントセキュリティ製品の利用状況（従業員数規模別）

5-3. セキュリティサービスの利用状況

セキュリティサービスについて、利用済みが最も多かったのは、各種の脆弱性診断サービス、証明書サービスであり、次いでWebサイトへのサイバー攻撃対策が多い。セキュリティ運用の外部アウトソーシングであるSOC利用やサイバー攻撃の損害を補填するサイバー保険については約３割だが、前回調査より若干増加した。

前回調査と比較すると、「Webサーバ向けSSLサーバ証明書」の導入が今後増えることが予想される（図21）。

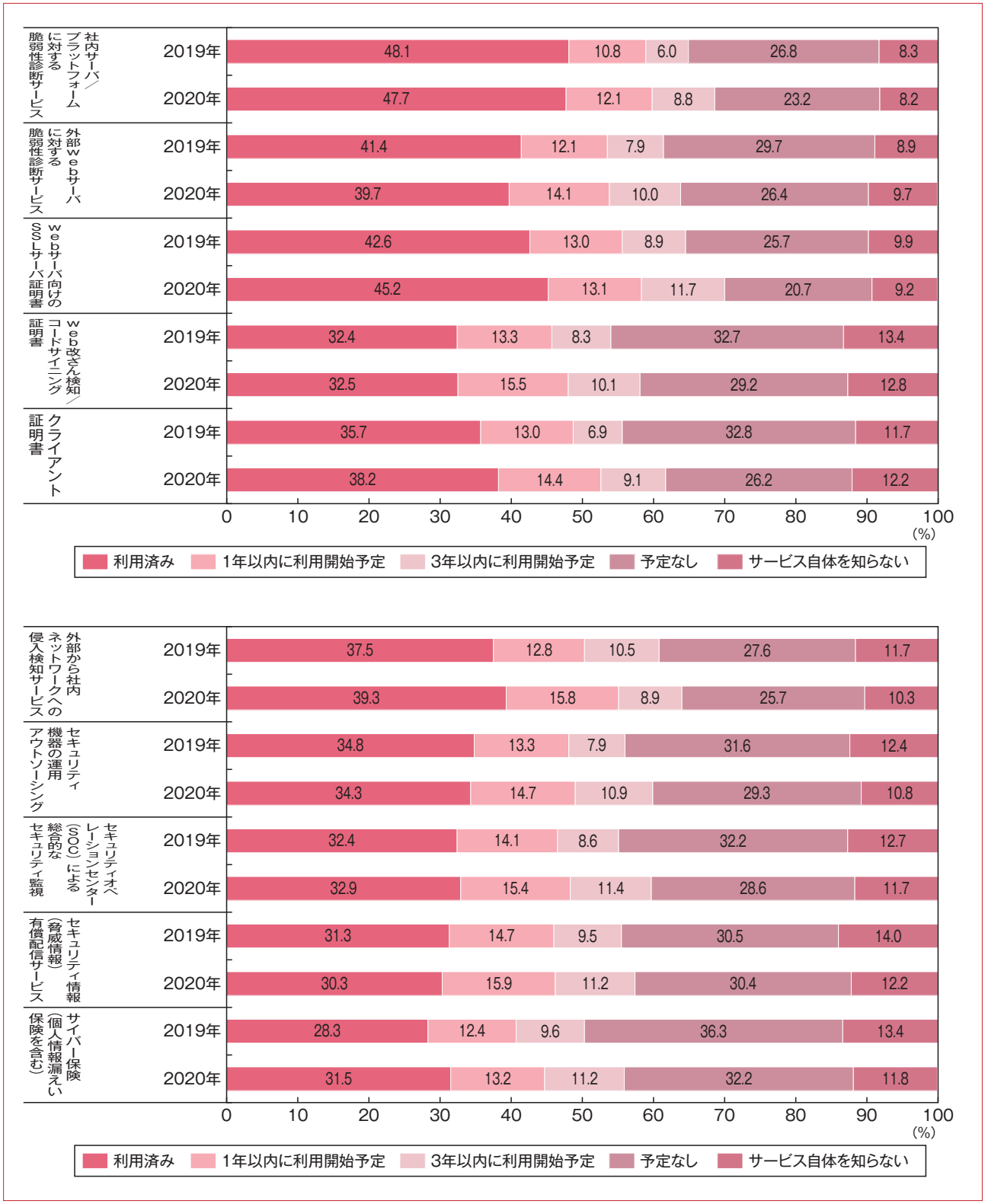

図21. セキュリティサービスの利用状況（2019～2020年比較）

5-4. 電子メールのセキュリティ対策の実施状況

電子メールのセキュリティ対策については、前回調査同様、送信者としての対策は「Zipパスワードによる添付ファイルの暗号化」（45.8%）と「誤送信防止ツール」（44.1%）が多く、受信者としては「シグネチャーベースのマルウェア対策」（53.0%）、「スパムフィルター」（50.6%）が多い（図20）。

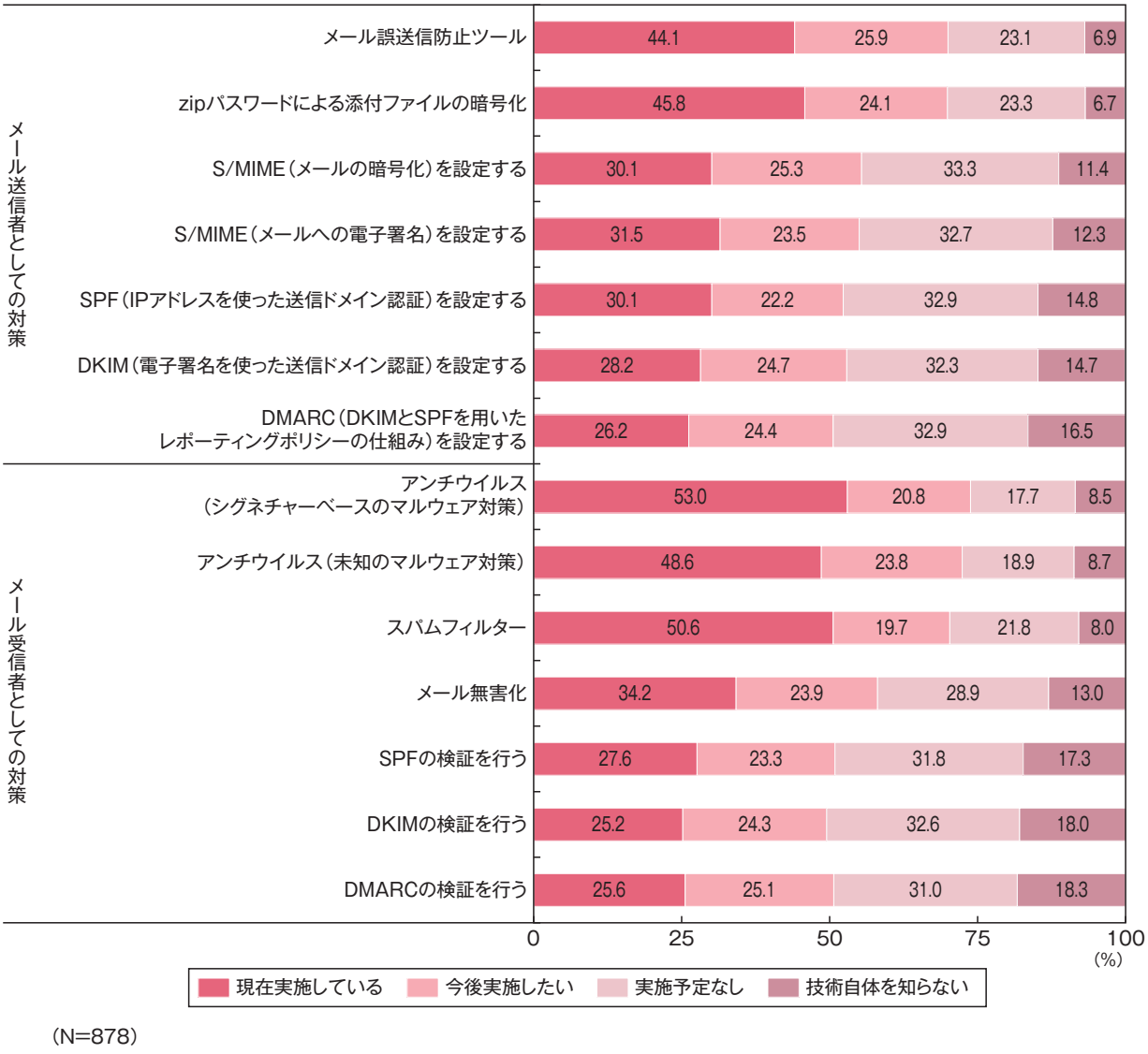

図22. 電子メールのセキュリティ対策の実施状況

5-5. 高機密システムへのアクセス認証手段

セブンペイ事件でアクセス認証の脆弱性が問題となったが、高機密システムに対するアクセス認証手段としてなにが使用されているのかを調査した。

従来どおりの「パスワード方式」が８割を超え、かなりの差はあるが、「電子証明書」（56.0%）、「ハードウェアトークン」（38.0%）、「LDAP／ActiveDirectry」（37.8%）と続く。

一方、今後利用したいとされる手段としては、「生体認証」（36.0%）、次いで「多要素認証」（28.2%）、次世代のアクセス認証の中心技術と言われる「IDaaS」（24.6%）の順となった（図23）。

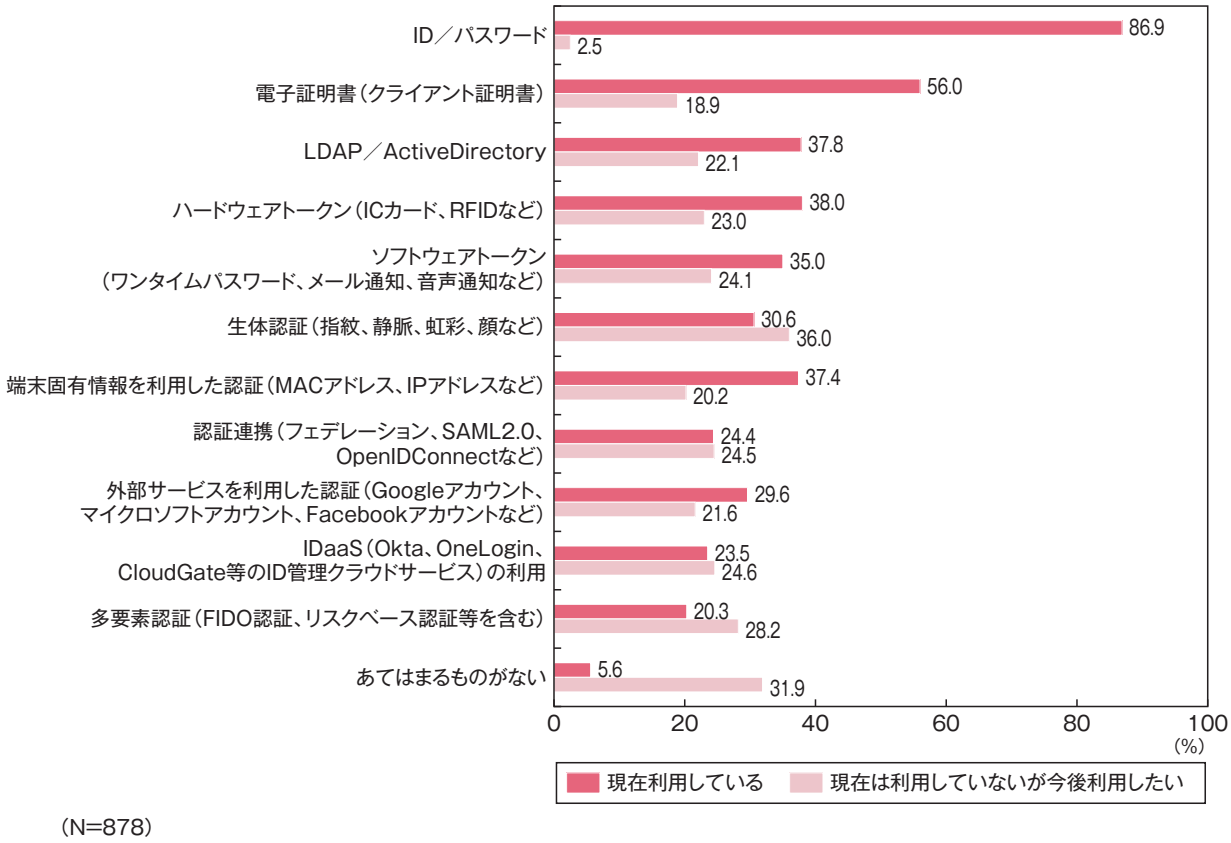

図23. 高機密性システムへのアクセス認証手段

業種別にみると、「金融・保険」、「情報通信」が他の業種と比べ、ID／パスワード以外の認証手段の採用率が高いことがわかる（図24）。

	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%

図24. 高機密性システムへのアクセス認証手段（業種別）

6 働き方改革とクラウドサービスの動向

2019年４月に施行された働き方改革法に対する企業の取組み状況を調査した。法律が施行され、取組みが加速してきている中、社内制度の整備や運用のためのシステムセキュリティ面の対策への取組みが始まっている。

6-1. 働き方改革の取組み状況

働き方改革は、前回調査と比べすべての項目で「実施中」と「検討中」が増加し、あわせて５割を超えており、取組みは本格化している（図25）。

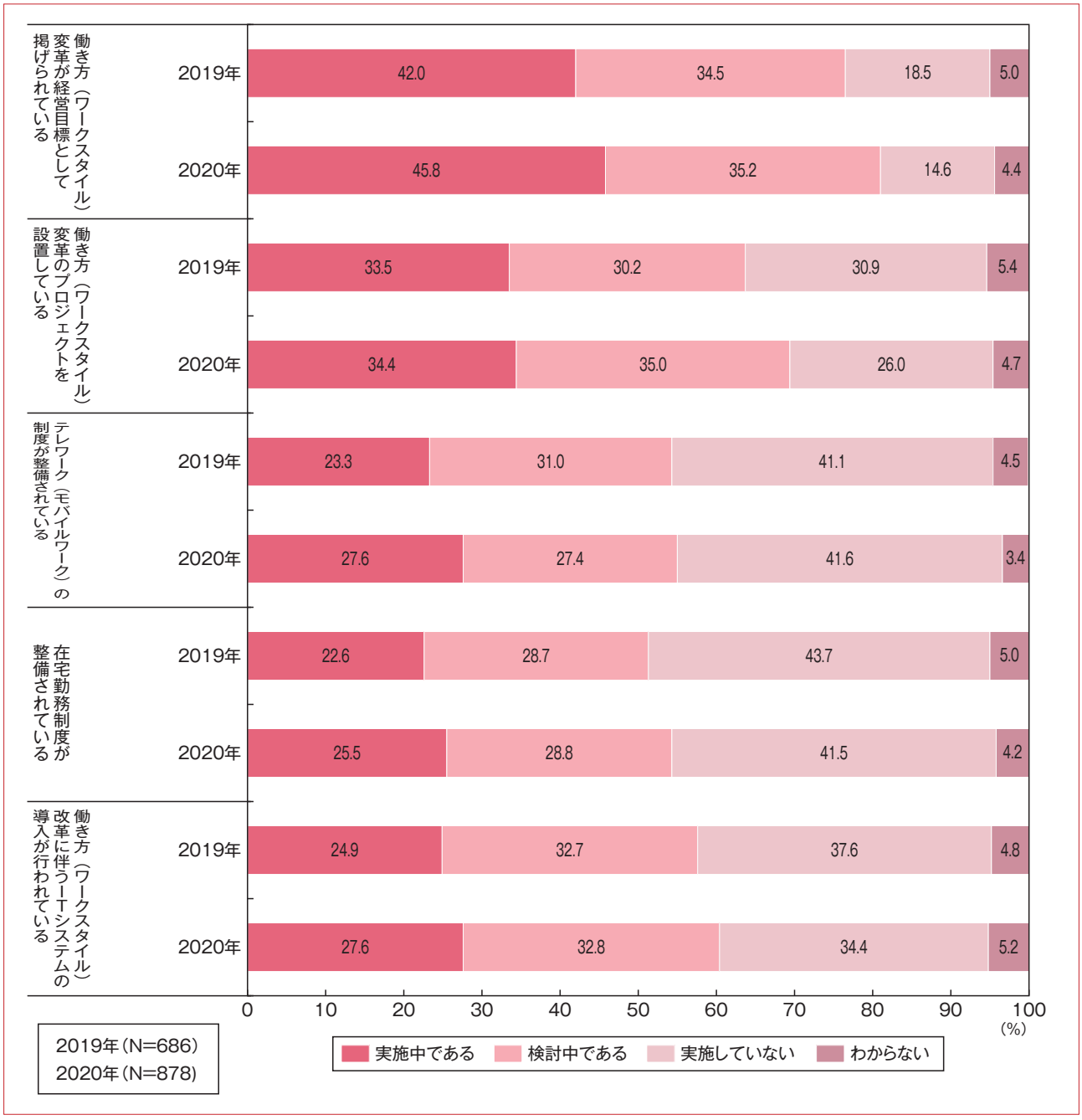

図25.「働き方改革」に関する取組み状況（2019～2020年比較）

6-2. ワークスタイルに関連するセキュリティ対策の実施状況

働き方改革を支えるシステムのセキュリティ対策の実施状況について、実施済みの対策は前回調査とあまり数値的に変わりはなかったが、「コミュニケーションツールの利用」（37.0%）や「在宅勤務・テレワーク用の規程整備」（27.3%）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（図26）。

ただし、本結果は1月中旬時点の調査に基づくものであり、その後の新型コロナ感染症の影響により、この部分については企業に大きな変化が起きた。今後、その変化がどのように企業に定着していくかが注目される。

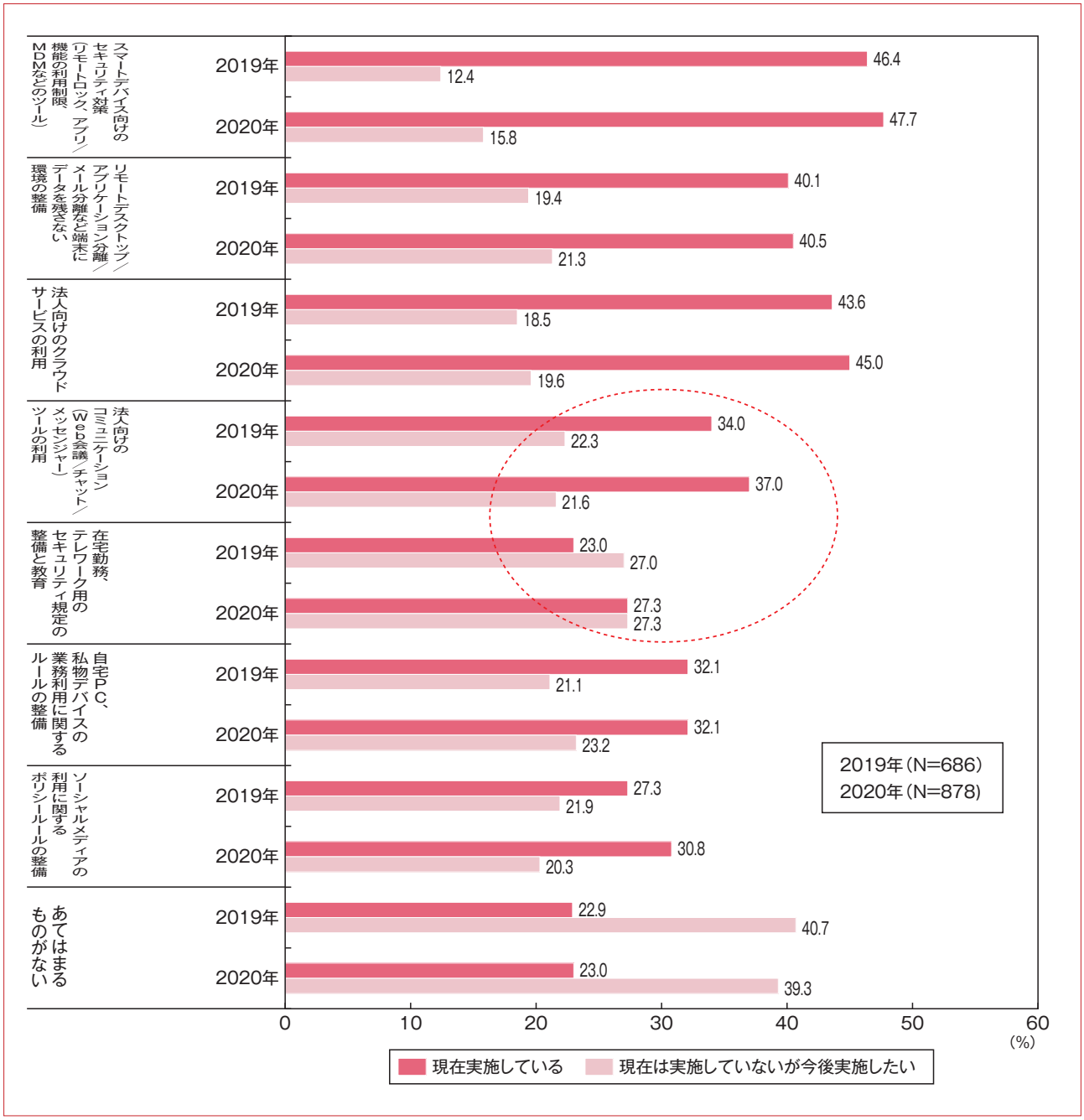

図26. ワークスタイルに関連するセキュリティ対策の取組み状況（2019～2020年比較）

6-3. クラウドサービスの利用状況

働き方改革を進めるうえで、クラウドサービスの利用は重要であることから、クラウドサービスの利用状況について調査を行った（図27）。

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である。

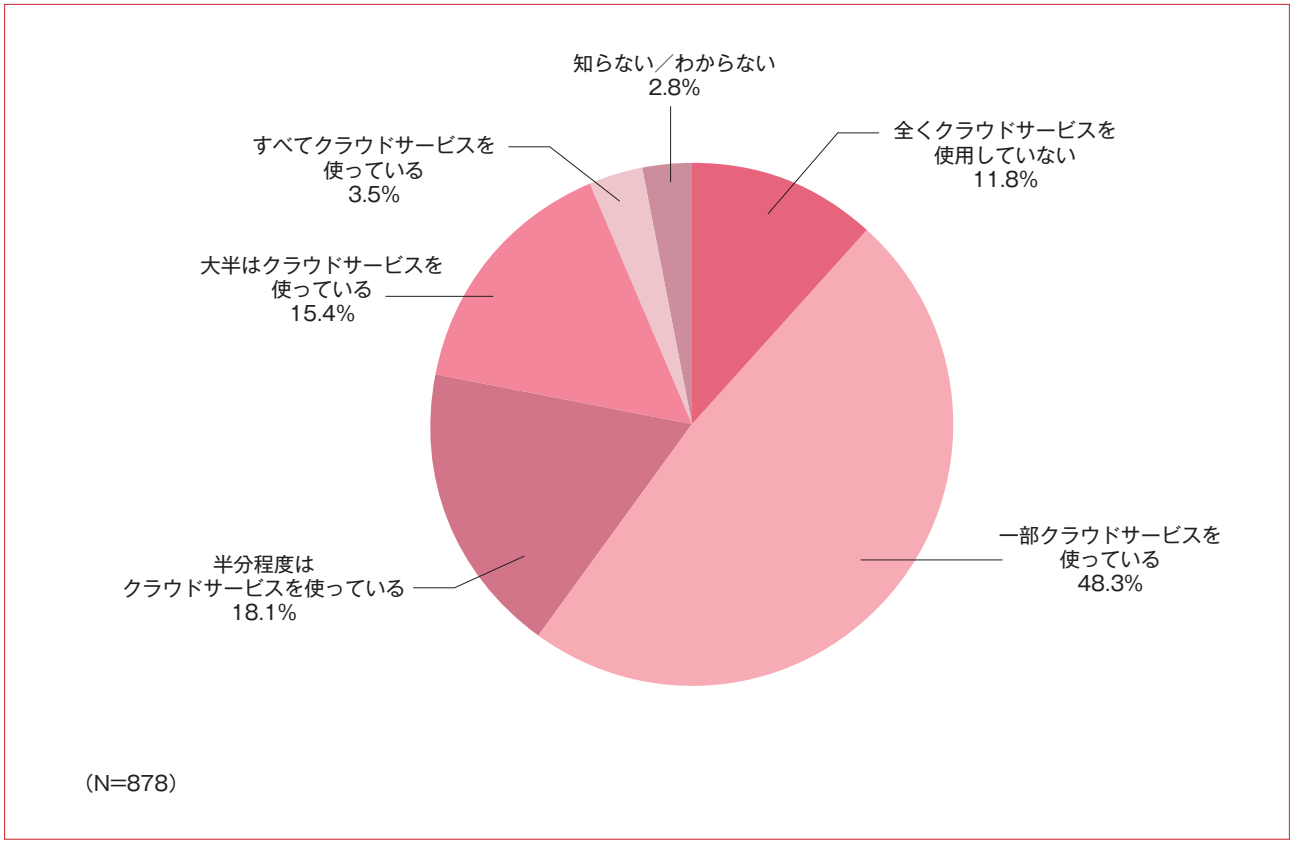

図27. クラウドサービスの利用状況

6-4. クラウドサービスの選定ポイント

クラウドサービス選定のポイントとしては、前回調査に引き続き「コスト」（55.2%）がトップで、「セキュリティ対策」（42.8%）と「セキュリティ認証取得による信頼性の確保」（42.5%）が続いている（図28）。

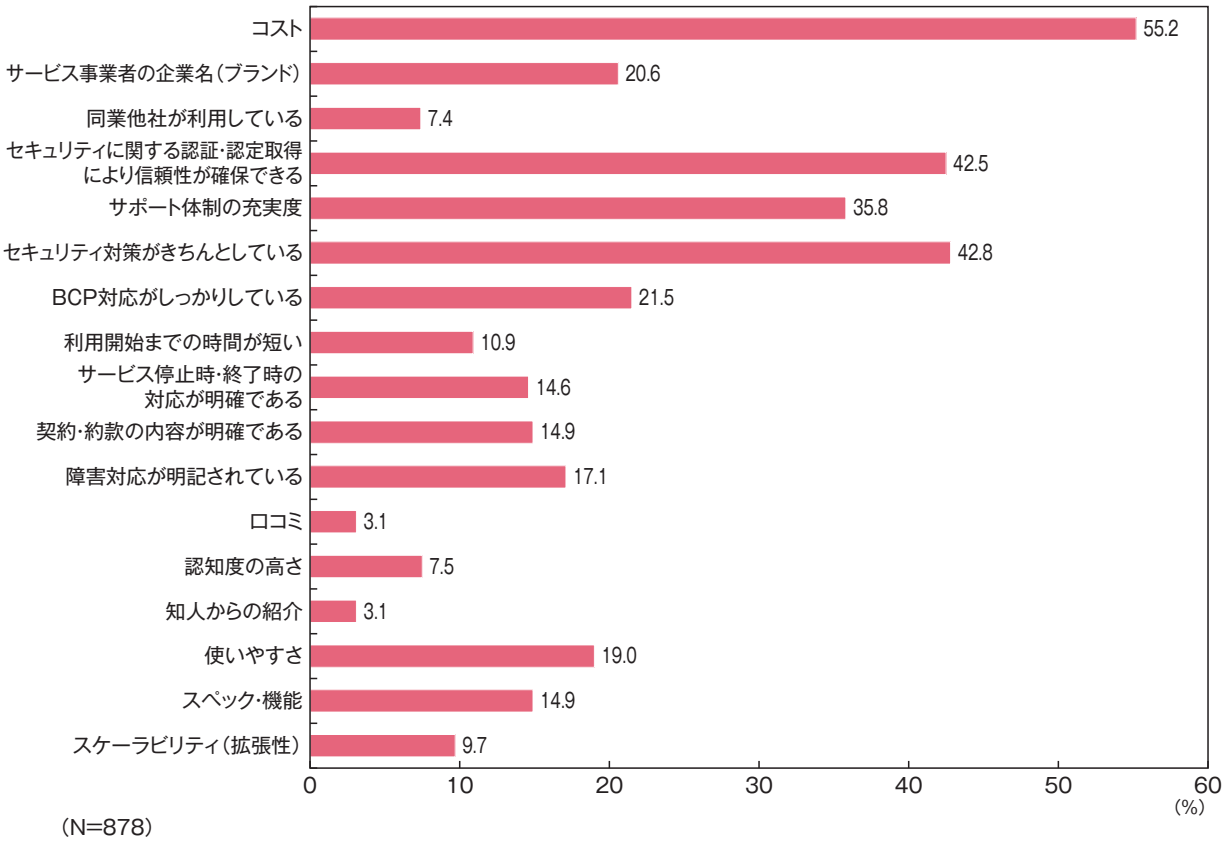

図28.　クラウドサービスを選定する際のポイント

また、信頼性を重視して選ぶクラウドサービスとしてどのようなものがあるかを調査したところ、「グループウェアサービス」（57.9%）が他を引き離してトップとなり、以下、「顧客管理サービス」（38.7%）、「財務会計サービス」（35.1%）と続く（図29）。

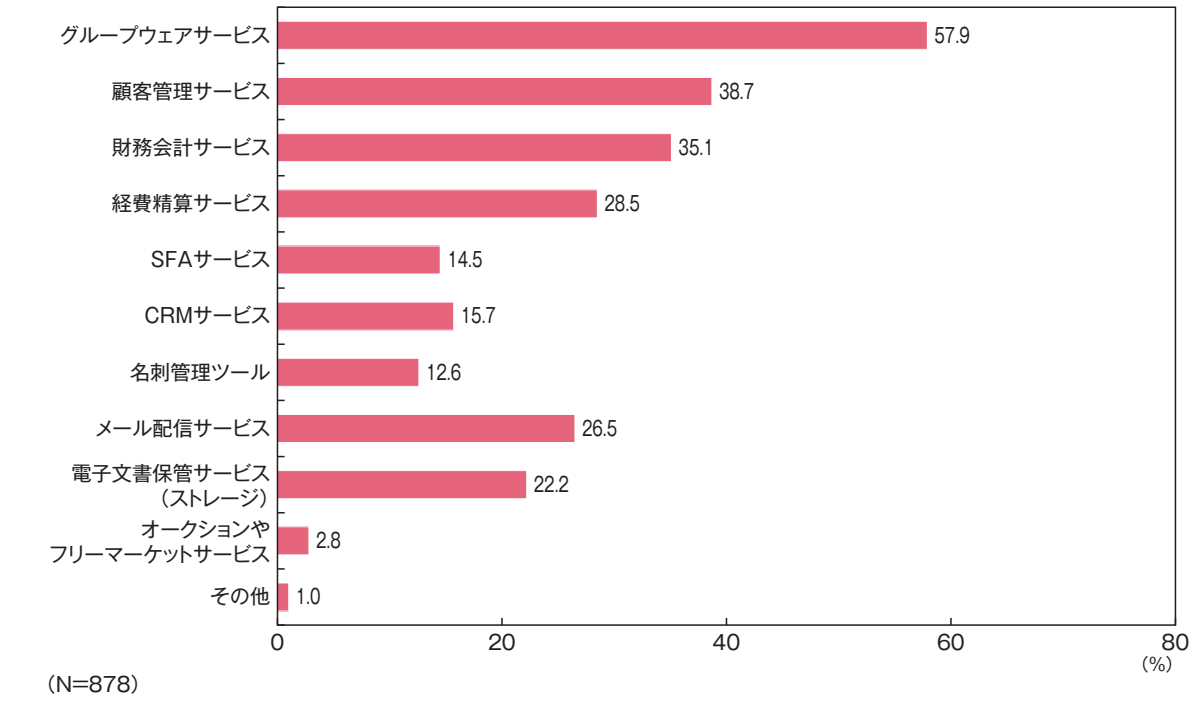

図29.　信頼性を重視して選ぶクラウドサービス

7　電子署名／電子契約など

セキュリティを担保したシステムサービス構築にあたっては、電子署名／電子契約、自社サイトのSSL化、情報セキュリティ監査などが有効となることから、これらの利用／導入状況について調査を行った。

7-1. 電子署名／電子証明書の利用状況

電子署名／電子証明書の利用が最も多いのは「電子メール（S/MIME）」（54.1%）で、被害が多発している「なりすましメール受信」（ビジネスメール詐欺）対策としての利用が考えられる。次いで「電子申請・申告・承認」（52.1%）となっている。また、今後利用が増加することが見込まれるのは「電子文書の保存」（36.1%）と「e-文書法、電子帳簿保存法」（35.9%）である（図30）。

前回調査と比較すると、すでに利用済みの回答は低いものの、未実施ながらも今後に向けて検討中として、「電子入札」は約５ポイント、「電子契約」は３ポイント増加した（図31）。

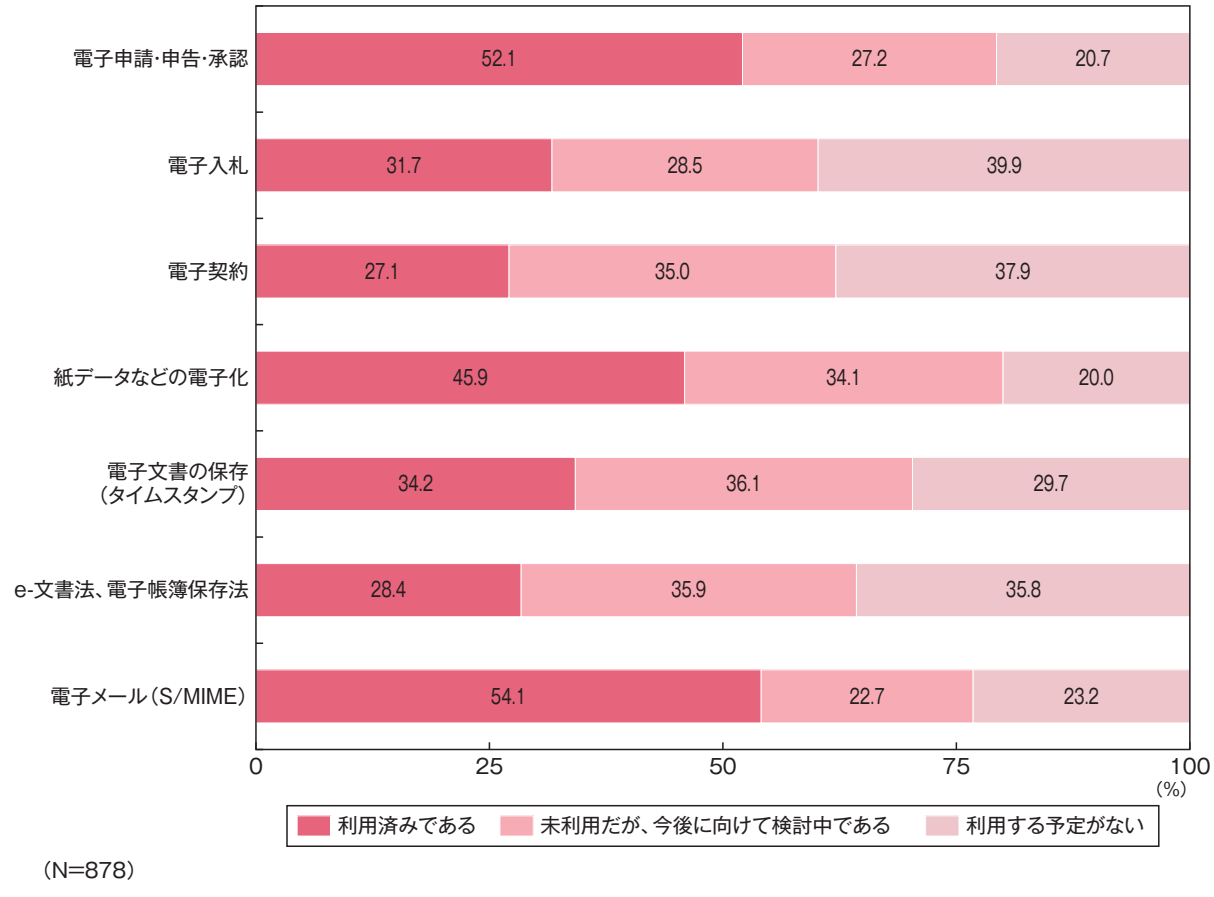

図30.　電子署名／電子証明書の利用状況

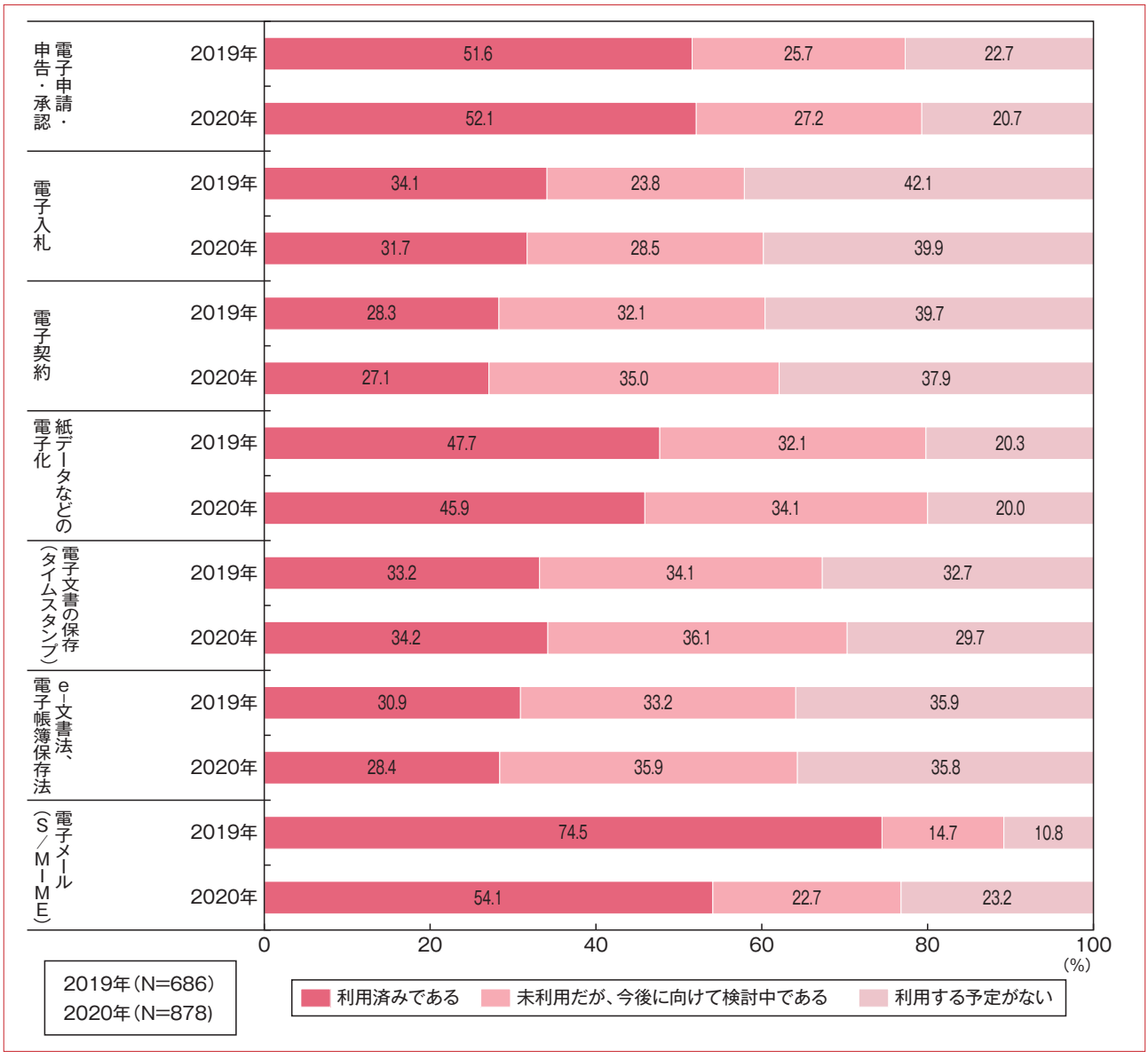

図31. 電子署名／電子証明書の利用状況（2019～2020年比較）

7-2. 電子契約の利用状況

電子契約の利用については、すでに「複数部門での採用（N対N型）」（18.2%）と「一部の取引先で採用（１対N型）」（25.1%）を合わせると約４割が利用していることとなる。また、「今後自社開発／外部の電子契約サービスを利用する予定」は約３割となり、過去調査から若干ではあるが増加傾向となった。（図32）。

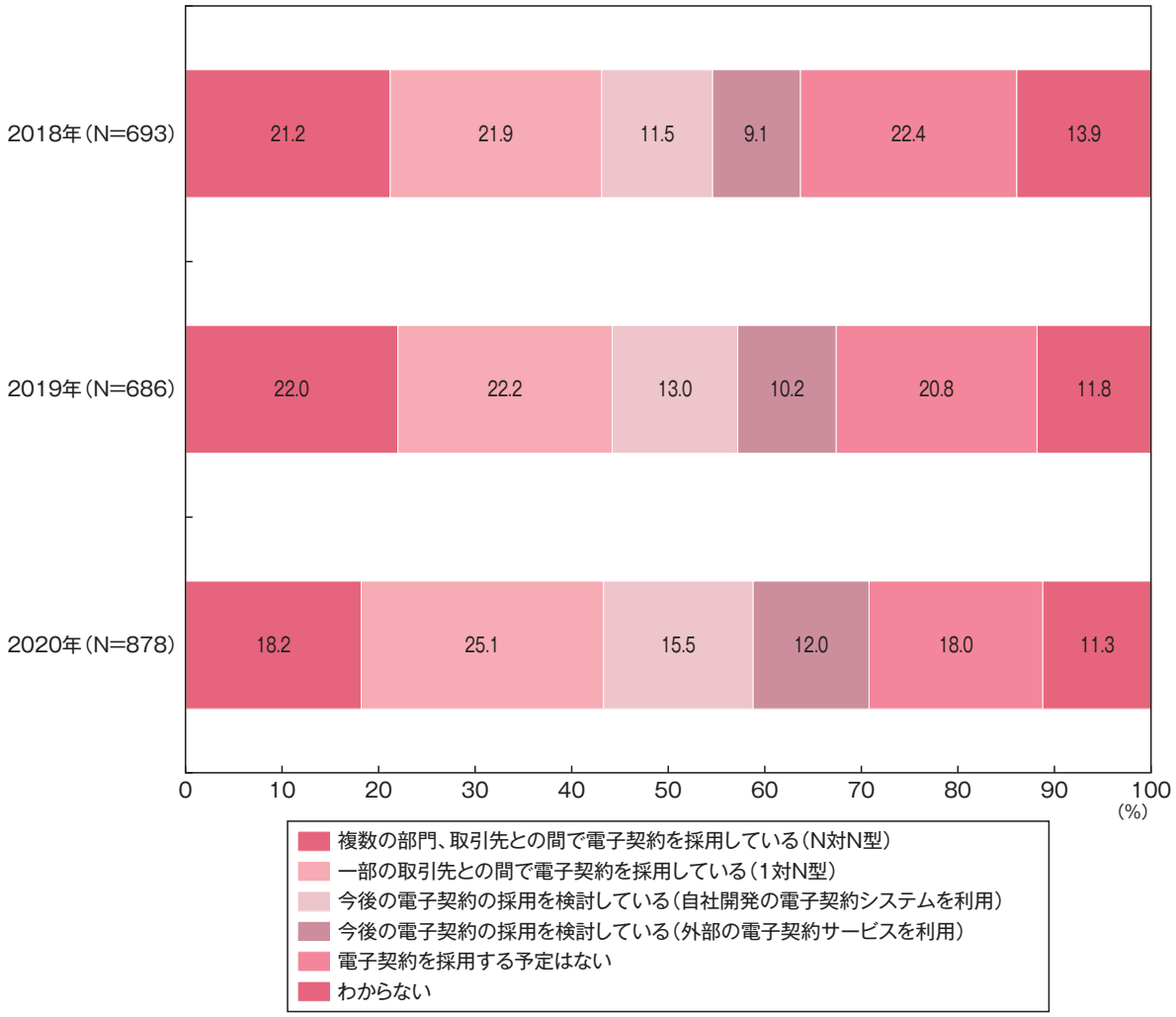

図32. 電子契約の利用状況（2018～2020年比較）

7-3. 自社Webサイトの常時SSL化

自社Webサイトの常時SSL化について、８割以上が何らかのSSL化を行っており、そのうち、すべて常時SSL化している企業も約４割を占めており、全体的にSSL化対応は進んでいる（図33）。

なお、自社の常時SSL化で最も高い効果があると考える理由は、「暗号化による中間者攻撃対策」（48.2％）、「なりすまし対策」（32.1％）であった（図34）。

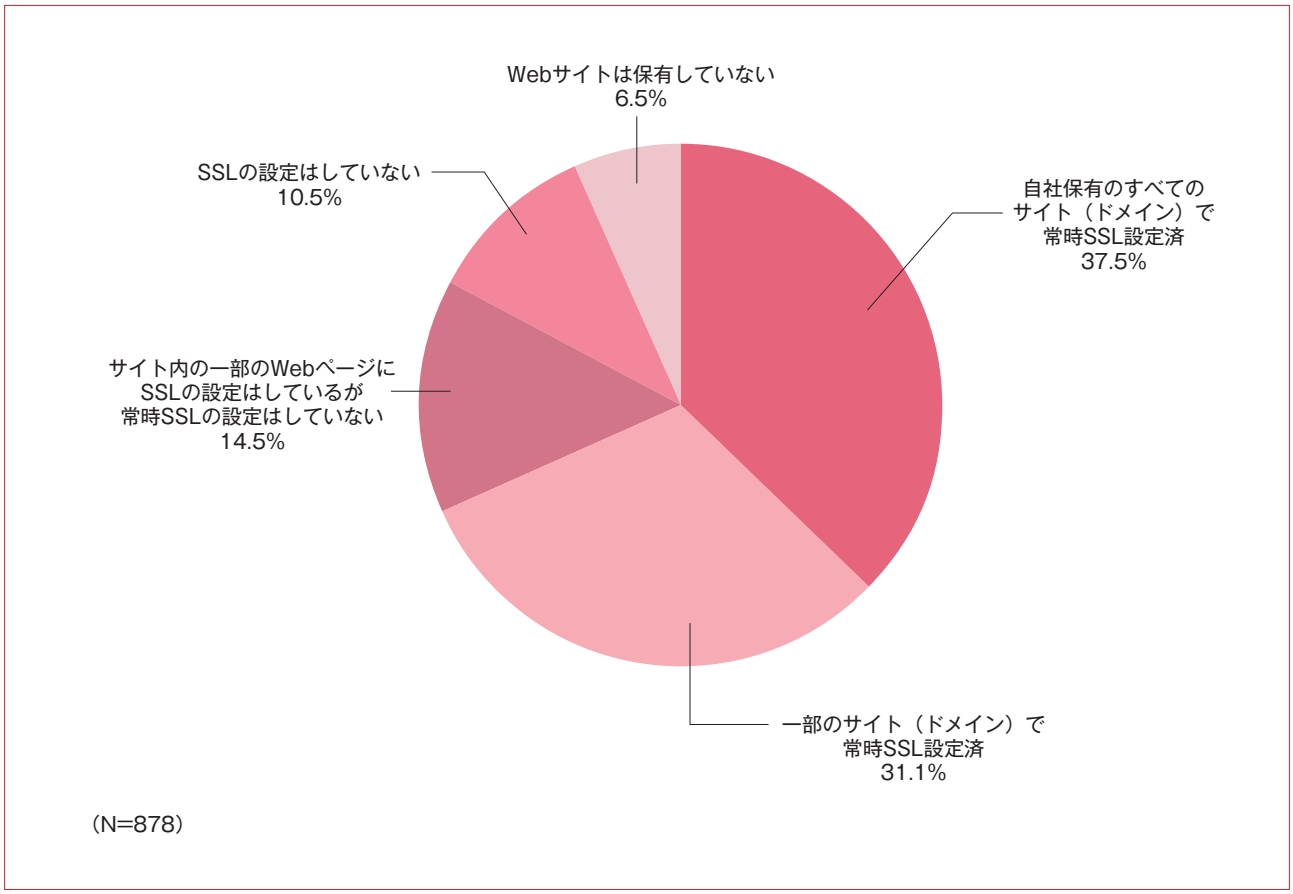

図33.　自社Webサイトの SSL化対応状況

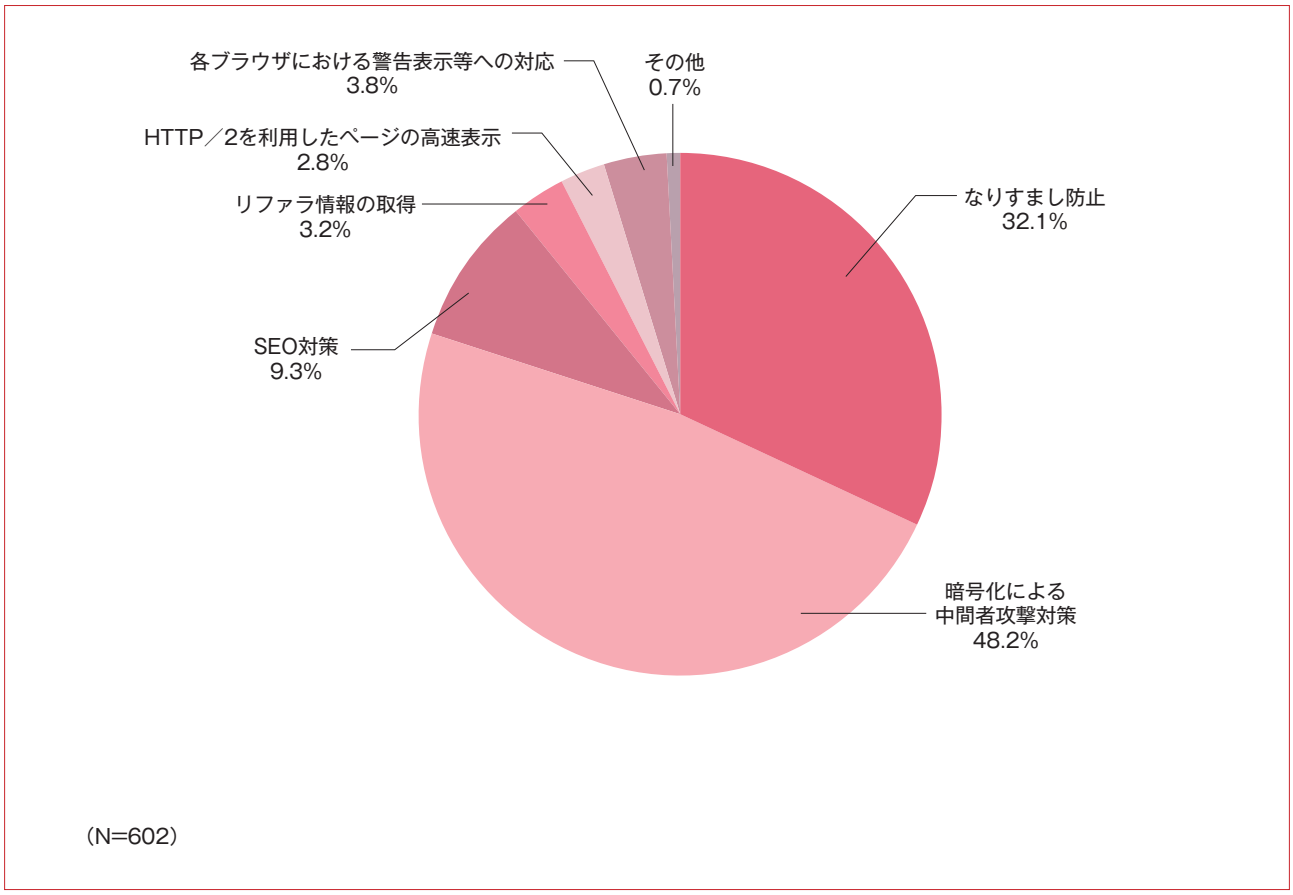

図34.　自社Webサイトの SSL化により最も高い効果

7-4. 情報セキュリティ監査の実施状況

自社保有のシステムや利用しているクラウドサービスについて、必要な対策が実施され、十分なセキュリティが担保されているか否かを検証する手段として、情報セキュリティ監査が考えられることから、情報セキュリティ監査の実施状況について調査を行った。前回調査と比較して、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、大きく増加した（図35）。

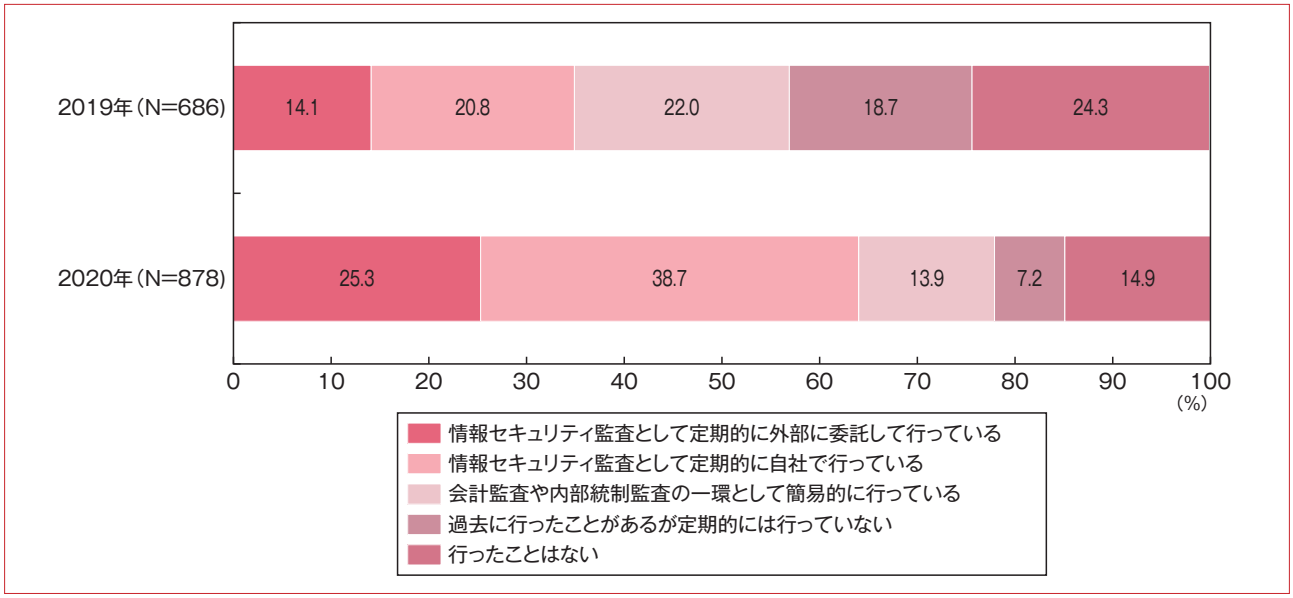

図35. 情報セキュリティ監査の実施状況

8 総評

「企業IT利活用動向調査2020」では、情報セキュリティを中心として企業のIT利活用の状況について約5,000社を対象に調査を行った（回答数：878社）。

情報セキュリティインシデントについては、例年どおり「マルウェア感染」や「従業員によるデータ・情報の紛失・盗難」が多かったが、「PCやスマートフォン等のモバイル端末の紛失・盗難」は減少した。また、「個人情報の漏えい・逸失」や「個人情報に関するトラブル」のような個人情報関連のインシデントが増加している。

一方のセキュリティ対策に関しては、従来型のファイアウォールやマルウェア対策ソフトの導入に留まっており、新しい攻撃に対応できるCASBやEDRのような次世代型のセキュリティシステムの導入の比率は低い。サイバー攻撃は日々巧妙化・複雑化してきており、新しい攻撃に対応できるセキュリティシステムの導入等対策を進めることが必要である。

個人情報保護関連では、JIS Q 15001規格の改定に続き、個人情報保護法の３年ごとの見直しにより、再改正が検討されているが、再改正の検討内容についてはさほど関心は高くなかった。関心が高いのは前回調査同様「個人識別符号」で、マイナンバー等個人識別符号となる番号は業務に多く存在するためだと思われる。

一方、GDPRについてはEUとの間で十分性認定に合意したこともあり、あまり大きな動きにはならなかった。しかし、グローバルではGDPRをきっかけに全世界のあらゆる地域で個人情報保護やセキュリティマネジメントの法律が整備されつつある。今後は自社の取引先や情報の取扱い状況について、関係する諸外国の法制度の動向等も考慮して、将来のビジネス進展も見据えたガバナンスが求められる。

働き方改革については2019年４月の施行以降、各社とも各種取組みの実施が前回調査よりも増加し、取組みが本格化してきており、在宅勤務やテレワーク等の勤務形態に合わせて信頼できるクラウドサービスの活用や、文書の電子化が進みだしている。

在宅勤務やテレワークに対するセキュリティ対策も含め、セキュリティインシデントへの対策が十分機能しているのかを確認するために、客観的な判断を得るための情報セキュリティ監査のニーズは大きく、実施比率が大幅に増加しており、今後もこの傾向は続くと思われる。

本調査結果は2020年１月時点のものであるが、現在猛威を振るっている新型コロナウイルス感染症の影響を受け、クラウドサービスの利用やテレワーク導入など、これまでの経営意識、業務形態の見直しは必須となっている。今後、経営課題、セキュリティ支出対象、セキュリティ対策、サービスの利用形態や、電子契約の導入状況にも大きな変化がみられることが予想される。これらの動向について次回調査で確認していきたい。

回答者プロフィール

業種	回答数	%
製造	264	30.1
建設・不動産	73	8.3
卸売・小売	68	7.7
金融・保険	59	6.7
情報通信	161	18.3
サービス	207	23.6
公共・その他	46	5.2
全体	878	100.0

資本金規模	回答数	%
5,000億円以上	144	16.4
3,000億～5,000億円未満	42	4.8
1,000億～3,000億円未満	81	9.2
500億～1,000億円未満	87	9.9
100億～500億円未満	169	19.2
10億～100億円未満	275	31.3
1億～10億円未満	75	8.5
1,000万円～1億円未満	5	0.6
全体	878	100.0

従業員規模	回答数	%
5,000人以上	197	22.4
1,000～4,999人	197	22.4
300～999人	215	24.5
50～299人	269	30.6
全体	878	100.0

業種別内訳

業種		回答数	%
製造	食品・飲料	16	1.8
	日用品・生活雑貨	4	0.5
	繊維	1	0.1
	パルプ・紙・印刷	10	1.1
	化学工業	22	2.5
	石油製品	9	1.0
	鉄鋼・金属	25	2.8
	プラスチック・ゴム	7	0.8
	機械	24	2.7
	電気機器	48	5.5
	情報通信機器	7	0.8
	電子部品・電子回路	23	2.6
	精密機器	15	1.7
	自動車・輸送機器	22	2.5
	医薬品	10	1.1
	その他の製造業	21	2.4
建設・不動産	建設	51	5.8
	不動産	21	2.4
	住宅	1	0.1
卸売・商社	卸売	25	2.8
	小売	24	2.7
	商社	19	2.2
金融・保険	銀行	29	3.3
	証券	3	0.3
	生命保険	8	0.9
	損害保険	10	1.1
	その他金融	9	1.0

業種		回答数	%
情報通信	通信	28	3.2
	ITベンダ/システムインテグレータ	108	12.3
	インターネットサービス	10	1.1
	情報システム子会社	15	1.7
サービス	電力・ガス・水道	8	0.9
	運輸	28	3.2
	倉庫	5	0.6
	宿泊	8	0.9
	飲食	10	1.1
	娯楽・レジャー	5	0.6
	メディア・出版・放送・広告	9	1.0
	生活関連サービス(旅行業など)	10	1.1
	医療	29	3.3
	福祉・介護	31	3.5
	教育（学校以外）	11	1.3
	人材派遣・業務委託	13	1.5
	その他サービス	40	4.6
公共・その他	学校	12	1.4
	官公庁	10	1.1
	地方自治体	21	2.4
	その他公共機関	3	0.3
全体		878	100.0

IT戦略・情報セキュリティへの関与度合い	回答数	%
全社的なIT戦略に決定権をもっている	276	31.4
全社的なリスク管理／コンプライアンス／セキュリティ管理に責任をもっている	379	43.2
セキュリティ製品の導入、製品選定に関与している	473	53.9
セキュリティ対策の実務に関与している	328	37.4
全体	878	100.0

〈資料〉情報化に関する動向（2019年10月～2020年３月）

国　内	海　外
2019年10月	
・政府、情報信託機能を提供する「情報銀行」について、民間の団体等による任意の認定の仕組みを有効に機能させるための「情報信託機能の認定に係る指針ver2.0」公表。 ・PPC、Amazon通販サイトでの利用者情報の誤表示に対し、行政指導。約11万アカウントが対象の可能性。 ・東京地裁、Twitterに対し、過去の逮捕歴の投稿削除を命令。 ・JIMOS、運営する通販サイトへの不正アクセスで、約11万件のクレジット情報流出の可能性。 ・JPCERT/CC調査、2019年第３四半期のインシデントが全四半期の1.4倍の5,733件。フィッシング被害が増加。 ・IPA、「DX推進指標」に対する企業の自己診断結果を収集・分析する「DX推進指標自己診断結果入力サイト」公開。入力企業には分析結果を提供。 ・総務省、フェイクニュースの実態把握、ファクトチェック対策に向けた検討の場立上げへ。 ・情報通信研究機構（NICT）、量子暗号を用いた生体認証データ伝送を実現。 ・NTTドコモ、3G通信サービス「FOMA」、「iモード」2026年３月末終了を発表。	・米・英・豪政府、共同でFacebookのSNSエンドツーエンド暗号化強化計画を進めないよう求める公開書簡を提示。 ・Twitter、２段階認証用に登録したユーザの電話番号とメールアドレスがターゲティング広告に利用されていたことが判明し、謝罪。 ・経済協力開発機構（OECD）、グローバル企業に対する税収を各国の売上げに応じて配分する新たな国際課税の枠組みを公表。 ・カリフォルニア州消費者プライバシー法（CCPA）改正法制定。企業に対し、同州住民からのデータ開示、削除、売却停止請求対応を義務付け。2020年１月施行 ・日・米政府、インターネットエコノミーに関する日米政策協力対話で、データ流通に関する国際的パートナーとしての連携を継続。グローバルな越境データ流通システム創出に向けた協力体制の構築へ。 ・米セキュリティ企業Emisisoft調査、2019年１月から９月において、621の自治体、医療機関、学術研究機関がランサムウェア感染。FBIが対策強化の徹底化を呼びかけ。 ・Facebookザッカーバーグ CEO、デジタル通過「Libra」は米規制当局の承認なしには立上げないと発言。 ・Facebook、動画上の顔による個人特定を回避する技術に関する論文公開。オリジナル動画をAI加工し、顔認識回避。 ・中国政府、世界インターネット大会開催。中国流ネット空間の中国ー欧州を結ぶ広域経済圏構想「一帯一路」域内の国々への拡大化を強調。

国　内	海　外
2019年11月	
・NICT他、量子暗号を用いた顔認証の安全性を高めるシステム開発。秘密分散手法でデータを分散化。 ・トレンドマイクロ、元従業員が最大12万人分の顧客データを不正持出し、第三者に提供。 ・NEC、歩行者の虹彩を高精度に撮影し、高速度で画像解析できる技術を開発。迅速な虹彩認証を実現。 ・政府、テレワーク・デイズ2019報告会で、７月下旬から９月上旬の実施期間内に約68万人、2,887団体の参加を報告。 ・講談社、著作権侵害で提訴していた海賊版リーチサイト「はるか夢の址」に勝訴。運営者に約1.6億円の支払い命令。 ・大阪高裁、ベネッセ情報流出事件のプライバシー侵害の差戻し訴訟で1,000円の支払い命令。 ・PPC、、個人情報保護法改正に向け、クッキー利用に関する法規制検討へ。個人情報保護法改正に。 ・パナソニック、ディープラーニング活用の顔認証技術をクラウドサービス化。マスク等で顔の一部が見えなくても判別可能。 ・国立情報学研究所と富士通、高速大容量のネットワーク環境で不審な通信の検知成功。	・ロシア政府、主権インターネット法施行。国外からのサイバー攻撃等脅威時に、国外からのインターネット遮断可能に。 ・ICT-ISACと米IT-ISAC、サイバーセキュリティ情報の共有、国際連携強化のための覚書に署名。 ・Microsoft、欧州データ保護監督官によるGDPR違反の可能性に対する調査を受け、商用クラウド契約条項を見直し。 ・GAFA、下院司法委員会による事業慣行への質問状に対し正当性を訴えるも、一部回答なし。 ・Twitter、全世界での政治的広告の全面禁止発効。 ・Google、政治広告運用見直しを発表。広告配信対象を性別、年齢、郵便番号による地域で絞込み。 ・欧州連合（EU）、5G機器共有業者選定に厳しい基準を採用、１社依存を禁止。 ・T-Mobile、不正アクセスで100万件以上の個人情報流出。

国　内	海　外
2019年12月	
・象印マホービン、ECサイトの不正アクセスで、最大28万件の顧客情報流出。 ・ソフトバンク、2024年１月下旬で3Gサービス終了を発表。KDDIは2018年時点で2022年３月末での終了を発表済み。 ・神奈川県、行政文書保存のHDDを破棄後、処分担当会社の従業員に転売され、個人情報を含むデータ最大54TB分が流出。レンタル業者は防衛省とも取引あり。 ・日本電子計算、自治体向けIaaSの障害で、50自治体に影響。 ・政府、全省庁クラウド化に向け、調達の評価基準策定に着手。 ・札幌地裁、グーグル検査結果の削除を求めた裁判で、一部削除を命令。検索結果削除命令は初。 ・NICT、南海トラフ地震等の災害想定実験で、秘密分散と秘匿通信技術で災害に強いセキュアな電子カルテ保管・交換システムを開発。 ・PPC、「個人情報保護法 いわゆる３年ごと見直し制度改正大綱」を公表。企業に対し、データ利用停止を要請できる「利用停止権」導入へ。 ・公正取引委員会、デジタル市場での企業買収審査のため、独占禁止法運用方針見直し。 ・政府、プラットフォーマーへの規制強化へ。契約条件の透明化、個人情報保護法改正に伴う新ルール導入、データ寡占防止へ。 ・政府、デジタルガバメント実行計画を閣議決定。	・中国政府、通信事業者に電話契約時に利用者の顔認証データ収集を義務付け。 ・米政府、全旅行者に顔認証義務化する規則導入提案へ。 ・華為、自社製品調達の一部を停止させる規制の採択は米憲法違反として、米連邦通信委員会（FCC）を提訴。 ・中国政府、画像撮影用衛星Gaofen-7で撮影した高解像度3D衛星画像を公開。上空500kmからの撮影でも１個人の識別可能。 ・米政府発行の出生証明書75万件が流出。 ・Facebook、ユーザ約2.7億人の個人情報がインターネット上で誰でもアクセス可能の状態に。 ・仏政府、ネット広告の利用規約が曖昧で優位的地位の乱用を指摘し、Googleに1.5億ユーロの制裁金。 ・米海軍、サイバーセキュリティ驚異の懸念から、軍属者支給のモバイルデバイスでの中国製アプリ「TikTok」使用禁止を通達。 ・カリフォルニア州、軽量自動運転車の公道テスト実施を許可。食料配達車両なども対象に。 ・米政府、国家安全保障にかかわる技術の海外流出対策として、地理空間画像を分析するAIプログラムの海外輸出を規制。

国　内	海　外
2020年１月	
・Microsoft、Windows7のサポート終了。国内では１月時点で推測約1,400万台が稼働中。 ・東芝、世界初、量子暗号通信を利用したゲノムデータ約500GBの伝送に成功。 ・NICT、38コア・３モードの光ファイバを用いた大容量伝送システムが、容量、周波数利用効率の世界記録達成。 ・東芝、2020年度に量子暗号通信の米国での事業化開始を発表。 ・警視庁、仮想通貨ビットコイン約7,800万円相当を詐取した容疑者２名を電子計算機使用詐欺の疑いで逮捕。 ・IPA、2020年版「情報セキュリティ10大脅威」発表。個人では「スマホ決済の不正利用」が初登場１位に。 ・PPC、２月１日の英国のEU離脱予定（英国時間１月31日）を受け、日英間の個人データ移転について、移行期間中の2020年末まで、EUが日本に対し行った十分性認定が維持されると発表。 ・三菱電機とNEC、相次いで過去の不正アクセス被害を公表。いずれも防衛関連情報取扱い。 ・政府、クラウドサービスを安全に導入するための評価方法の検討成果を公表。今後数年をかけて全省庁のシステムをクラウド化へ。	・中国政府、暗号法施行。ブロックチェーンを利用したデジタル人民元発行に向けた法整備の一環。 ・Facebook、政治広告に関する方針発表。ファクトチェックは行わず。 ・国際法律事務所DLA Piper調査、GDPR施行後18カ月で約16万件の情報漏えい。制裁金の合計額は、1.14億ユーロに。 ・シンガポール、ニュージーランド、チリ政府、「デジタル経済パートナーシップ協定」妥結。国境を越えたビッグデータ移管、AI等先端分野のルール確立を目指す。 ・米・仏政府、仏のデジタル課税に対する米の報復関税の応酬回避で合意。 ・英個人情報保護監督機関、子供のオンラインデータを守る規制を提案。ターゲティング広告や現在地情報の追跡など子供に害を及ぼすネット行為を制限。 ・ロンドン警視庁、重罪犯逮捕に向け、特定の場所でのライブの顔認証運用を開始。 ・イタリア競争当局、2018年にデータの不適切な取扱いで500万ユーロの罰金を課したFacebookに対し、是正措置違反で追加の制裁金。 ・Facebook、プライバシー対策ツール「off-Facebook activity」を世界各国で提供開始。Facebook以外のオンラインサービス上のアクティビティについて、Facebookに提供された個人情報を可視化、自身で管理可能に。 ・日本銀行他６カ国・地域の中央銀行、デジタル通貨発行のための共同研究に着手。

国　内	海　外
2020年２月	
・東京高裁、仮想通貨「Coinhive」設置で刑法不正指令電磁的記録保管罪を問われ、１審無罪のサイト運営者への控訴審で有罪、10万円の罰金。 ・防衛省、防衛関連産業の神戸製鋼所とパスコが過去に不正アクセスを受けていたことを発表。防衛情報の流出はなし。 ・政府、デジタルプラットフォーマーに対し、取引条件の開示、契約変更時の事前通知、運営状況報告を求める規制策を閣議決定。 ・前橋市、2018年に発生した不正アクセス被害に関し、ネットワーク保守担当のNTT東日本を提訴。 ・東京都、「スマート東京（東京版Society 5.0）の実現に向けたデータプラットフォーム構築の基本方針」策定。センサー等で取得したビッグデータをもとに、経済活動、人の流れ、インフラなどの要素をサイバー空間上に再現する「都市のデジタルツイン」実現を目指す。 ・総務省、電気通信事業法とNTT法改正案を閣議決定。外国事業者の提供サービスでの利用者情報の大量漏えい、大規模通信障害時の報告義務づけ。 ・政府、人事、給与、文書システムの政府共通プラットフォームの基幹クラウドとして、アマゾンクラウドサービス（AWS）採用方針を決定。今春正式決定へ。	・英国、EU離脱。 ・Facebook、顔の生体認証データの同意なき収集に対する集団訴訟で、和解金600億円支払いで合意。 ・米司法省、大手信用調査会社へのサイバー攻撃で、米国民約1.5億人の個人情報を摂取した中国軍人４名を起訴。AI開発への利用を指摘し、中国政府を非難。 ・ロンドン警視庁、路上での顔認証技術運用開始。2016年以降の試験運用での実績に基づき。 ・米連邦委員会、GAFA、Microsoftに対し、買収実態調査のため、企業買収・合併に関する取引情報提出を要求。 ・米国防総省傘下のCISAと連邦捜査局、北朝鮮政府使用のマルウェア７種を特定。 ・欧州委員会、データ市場の構築、AI規制などのデジタル戦略を発表。 ・独政府、SNSでのヘイトスピーチを含む違法コンテンツの投稿について、SNS企業に警察への通報を義務付ける法案を承認。 ・米ニューメキシコ州、子供の位置情報やネット閲覧履歴などの個人データを不正収集したとして、サービス提供元のGoogleを提訴。

国　内	海　外
2020年３月	
・政府、「個人情報の保護に関する法律等の一部を改正する法律案」閣議決定。個人情報漏えい時のPPCへの報告および本人への通知義務、匿名加工情報の取扱い等を規定。 ・政府、新型コロナウイルス感染症対策対応策として、テレワーク関連施策情報や支援情報を発信。 ・データサイン、日本IT団体連盟の「情報銀行」認定制度で、提供を開始しているサービスに対する初の「通常認定」。 ・IPA、新型コロナウイルス感染症拡大防止のため、４月実施の春期情報処理技術者試験・情報処理安全確保支援士試験中止を発表。 ・政府、新型コロナウイルス感染症のクラスター早期発見に向け、プラットフォーマー、通信事業者に位置情報や検索履歴の統計データ提供を要請。法的強制力はなし。	・FCC、通信大手加入者の位置情報の販売を法律違反と判断し、T-Mobile等４社に計２億ドルの罰金。 ・ハーバード大の科学者、極限環境での耐性を持ち、永続的に保存状態を維持できる可能な細菌ハロバクテリウム・サリナルムのDNAにデジタルデータ埋込み成功。 ・Facebook、アプリ開発会社に対価を支払い、利用者約950万人のデータを同意なしに収集したとして、データ分析会社を提訴。 ・豪個人情報保護当局、ケンブリッジ・アナリティカに豪ユーザ約31.1万人のユーザ情報を同意なく開示したとして、Facebookを提訴。 ・英政府、４月１日からデジタルサービス税（DST）導入。英国ユーザから得た売上高の２％を徴収。 ・Web会議サービスZoomの運営会社、ユーザデータを無断でFacebookに転送。「同意なしはカリフォルニア州データ保護法違反」として集団代表訴訟へ。 ・Google、独・仏の裁判所命令を受け、製品・サービス内容を利用者に理解してもらえるよう、８年ぶりに利用規約改訂。

JIPDEC IT-Report 2020 Spring

2020年5月29日発行（通巻第15号）

発行所　一般財団法人日本情報経済社会推進協会
〒106-0032 東京都港区六本木1-9-9 六本木ファーストビル12階
TEL：03-5860-7555　　FAX：03-5573-0561

制　作　株式会社ウィザップ

禁・無断転載