2023 SPRING

IT-REPORT

特　集

デジタルワークスタイル定着に向けた企業の対応
―「企業IT利活用動向調査2023」結果から

Contents

JIPDEC
一般財団法人日本情報経済社会推進協会

本誌「JIPDEC IT-Report 2023 Spring」では、JIPDECが2011年から継続して行っている「企業IT利活用動向調査2023」の結果をとりまとめ、紹介しています。

コロナ禍を契機に企業はクラウドサービスやテレワーク、電子契約を導入するなど、ワークスタイルが変わってきています。

クラウドサービスの利用動向については、９割以上の企業が全部または一部でクラウドサービスを利用していることがわかりました。電子契約の導入状況については、立会人型や当事者型など、何らかの形で電子契約を導入している割合が７割を超えました。また、電子契約サービス事業者を選定するにあたり、クラウドのセキュリティ認証の取得状況を参考にするケースが５割程度となっています。

コロナ禍での行動規制によりテレワークの導入率が増加していた前回調査と比べ、政府の行動規制緩和等を受け、従来の出社／テレワークの併用や導入を中止する企業も出てきています。

今年は毎年実施している過去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、情報セキュリティ製品の導入状況、プライバシーテックの利用状況等の他、昨年１月より施行された電子帳簿保存法への対応や、今年10月に施行される「インボイス制度」の登録申請状況についても聞くなど、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。

なお、今号では、調査分析結果を踏まえ、「プライバシーマーク制度」「電子メールのセキュリティ対策」「ISMSクラウドセキュリティ認証」「電子契約」「デジタルトランスフォーメーション」の最新動向をテーマに、当協会職員によるコラムも掲載しています。

あわせて、2022年10月から2023年３月の国内外の情報化動向をとりまとめていますので、今後のIT環境整備の参考にしていただければ幸いです。

2023年５月

一般財団法人日本情報経済社会推進協会

JIPDEC IT-Report 2023 Spring

Contents

特 集

デジタルワークスタイル定着に向けた企業の対応 ―「企業IT利活用動向調査2023」結果から

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、経営企画、総務・人事、業務改革部門等に所属し、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、2010年から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」を実施している。

2020年からは社会のさまざまな場面に大きく影響を与えているコロナ禍において、デジタルワークスタイルに対する企業の考え方や、どのように対応しているのかについても調査を行っている。

本誌では、2023年１月の調査結果をもとに、これまでの調査結果との経年比較を含め、企業の取組みについて、特徴的な傾向をピックアップして紹介する。

1 2023年調査の概要

1-1. 調査概要

・実査期間：2023年１月19日～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２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17,000人
・有効回答数：1,022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（31.2%）、次いでサービス業（20.9%）、情報通信（15.9%）、卸売・小売（10.1%）、建設・不動産（9.9%）、公共・その他（6.4%）、金融・保険（5.7%）となった。

所属部門では情報システム部門（23.7%）が最も多く、役職は、本部長・部長（32.5%）、課長（31.2%）が回答の約６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から、「セキュリティ製品の導入・製品選定に関与している」（50.7%）、「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」（50.3%）とする回答が多く、2022年調査と傾向はあまり変わっていない（巻末に詳細データ掲載）。

以下、テーマ別に分析結果を紹介する。

2 経営課題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見る。

2-1. 重視する経営課題

重視する経営課題については、全23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複数回答で調査した。（図１）

前回調査同様、「業務プロセスの効率化」（62.6％）がトップとなったが、比率自体は前回調査より減少した。２位の「従業員の働き方改革」（45.9％）は前回同様、コロナ禍を機に重視されている。

各課題について前回と比べ微増傾向が多いのに対し、「情報セキュリティの強化・ゼロトラストセキュリティの実現」については、前回の35.4％から29.3％に６ポイント大幅に減少した。セキュリティを強化すること自体、今後の課題と捉えるのではなく、喫緊で取り組んでいることが想定できる。

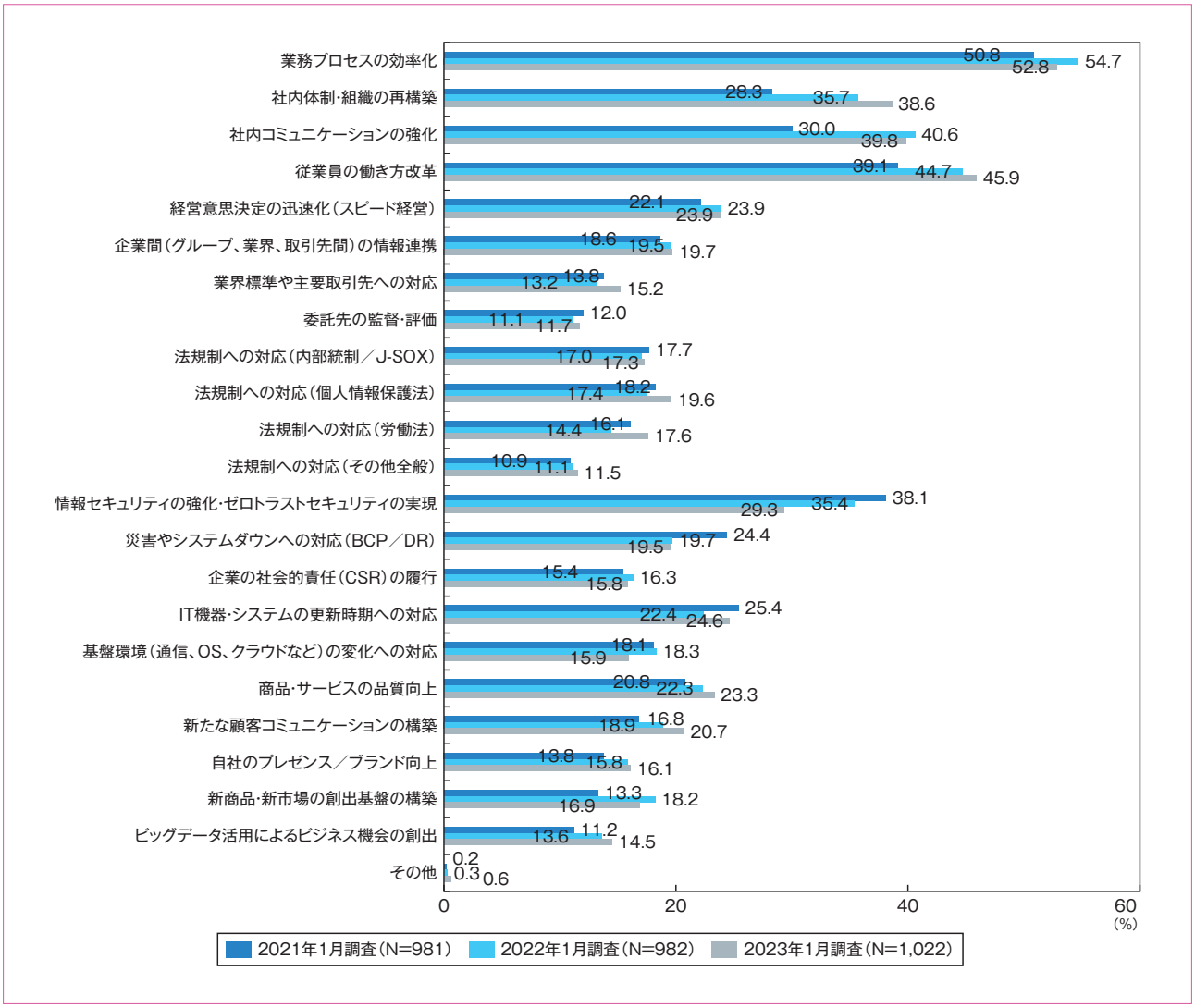


図１．今後重視したい経営課題

2-2. セキュリティインシデントの認知状況

回答者の勤務先が過去１年間に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「従業員によるデータ・情報の紛失・盗難」（34.1％）で、２位は「社内サーバー／PC／スマートフォン等のマルウェア感染」（27.7％）となり、前回調査と同様となった。（図２）

なお、前回調査と比べ大きく差がでたのは、「Webサイトへの不正アクセス」で14.8％から10.9％と、４ポイント減少した。

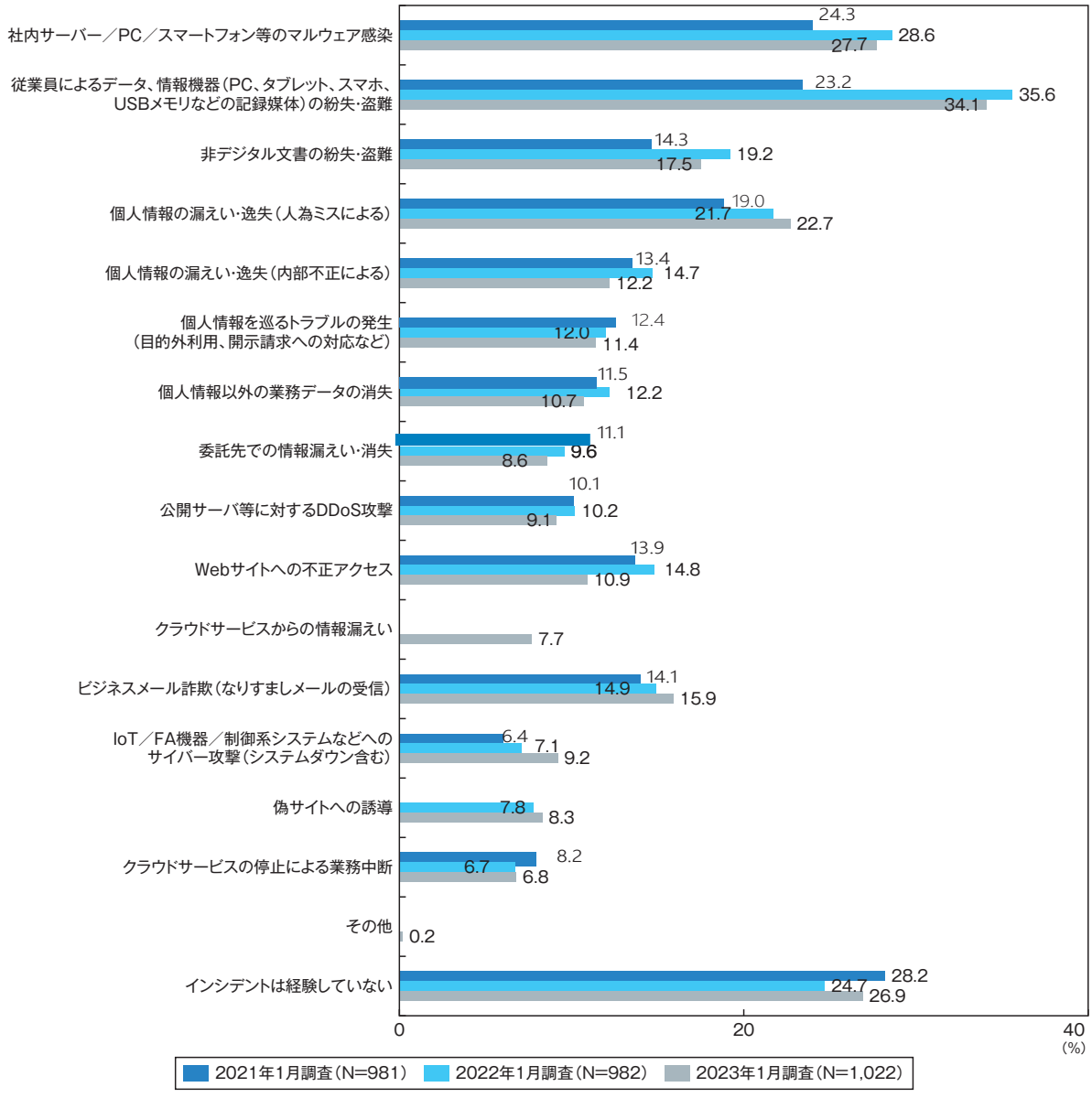


図２．過去１年間に認知したセキュリティインシデント

2-3. セキュリティリスクの重視度合い

外部から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について、それぞれ定点観測しているが、外部からのサイバー攻撃についてはほとんど変化は見られなかったのに対し、内部犯行・過失については、「きわめて重視され、経営陣からも最優先で対応するよう求められている」が前回調査から2.7ポイント増加した。（図３）

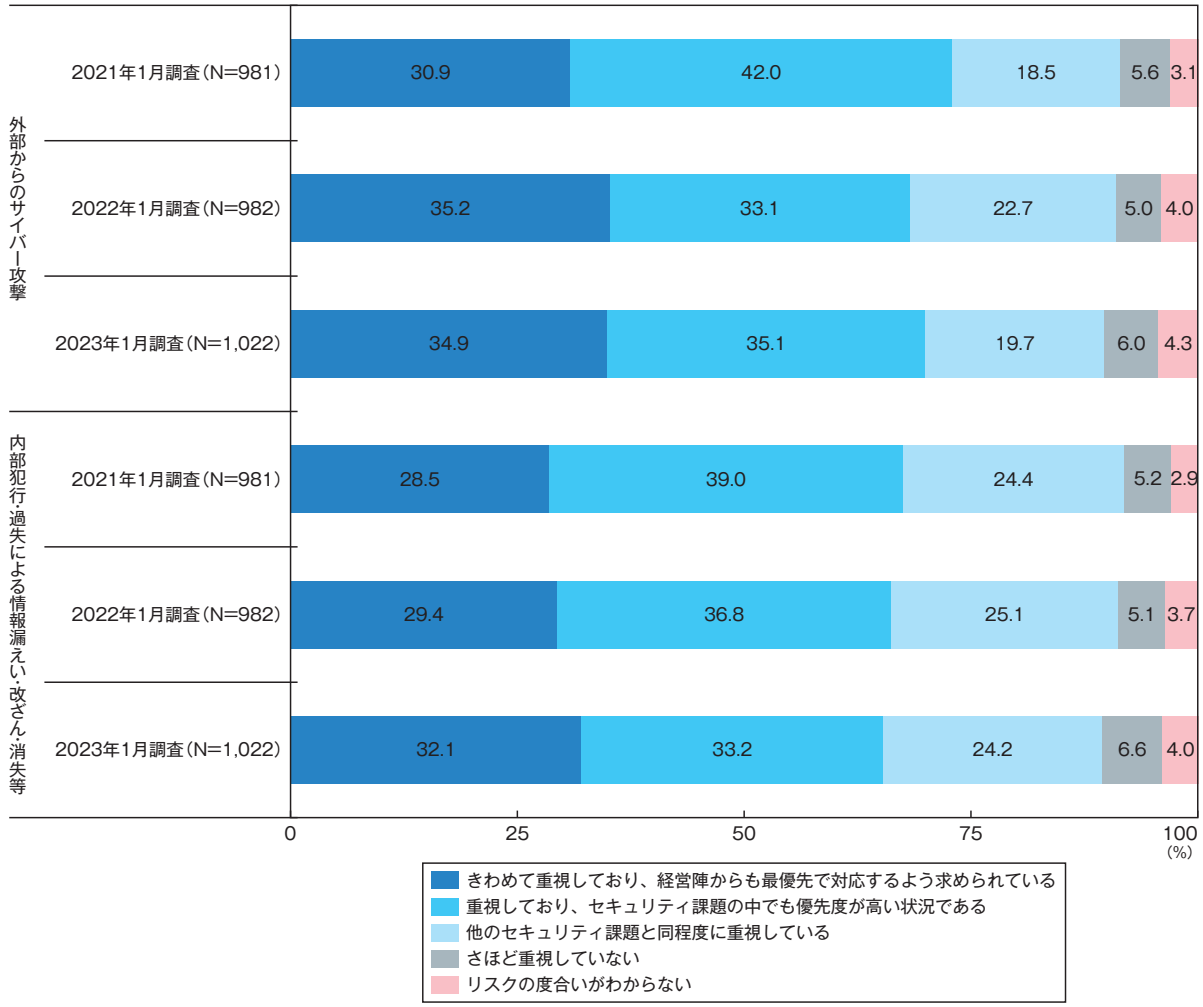
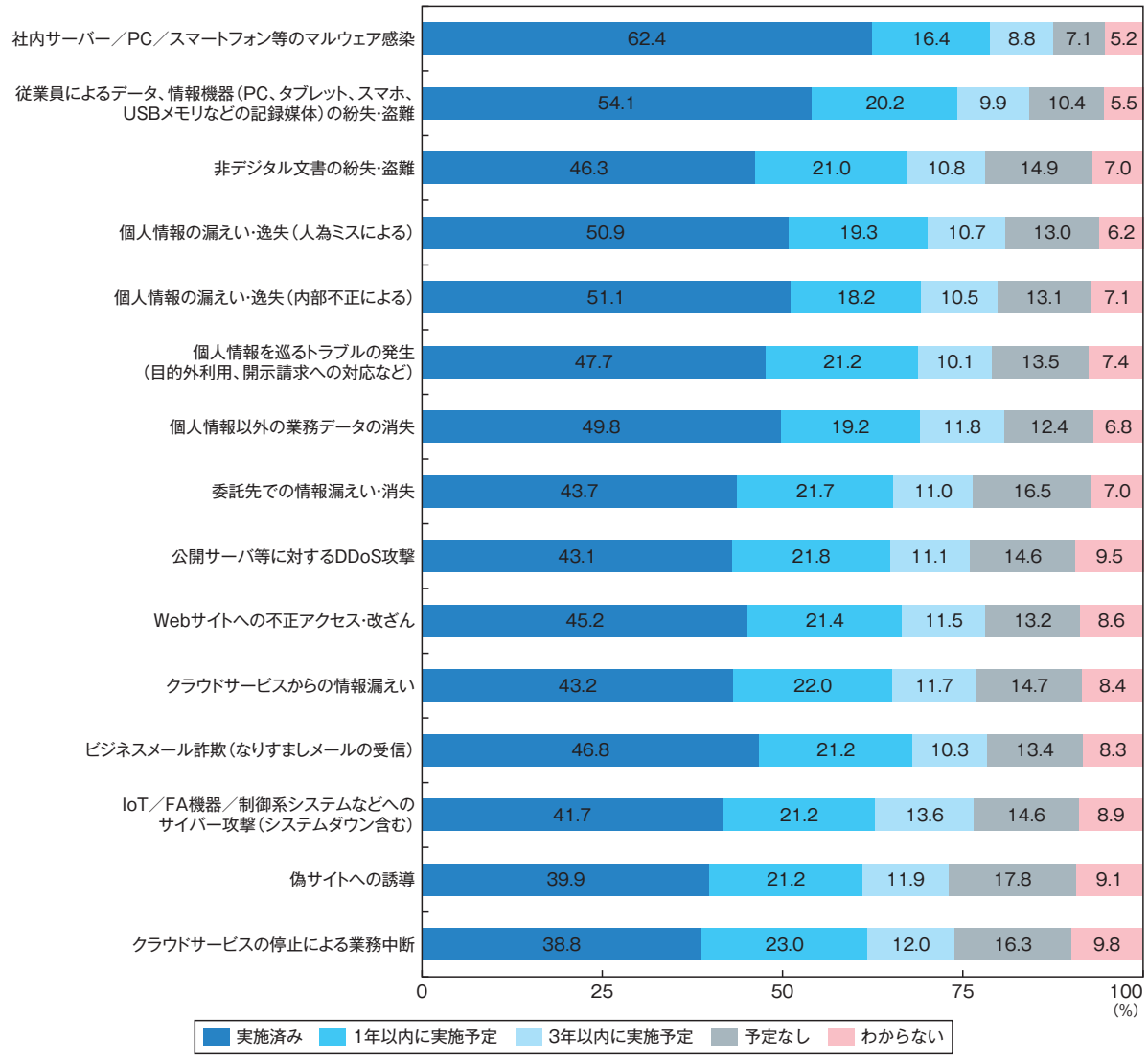


図３．セキュリティリスクの重視度合い

2-4. セキュリティ対策の実施状況

セキュリティ対策の実施状況について、ここでは「外部からのサイバー攻撃対策」と「内部犯行の情報漏えい対策」について代表的な取組みをピックアップし、その実施率について観測している。

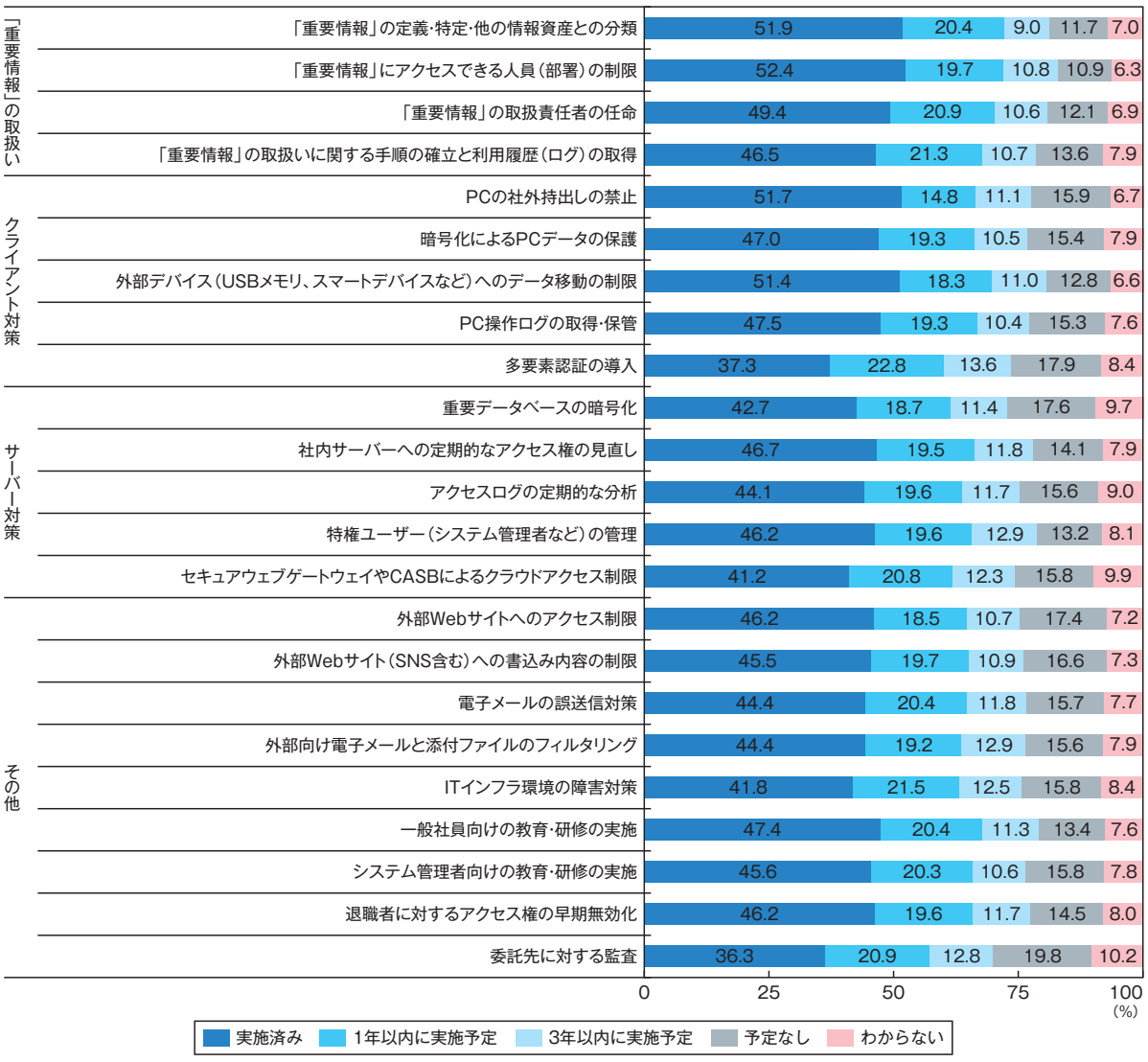
「外部からのサイバー攻撃対策」として最も実施率が高かったのが「マルウェア感染対策」（62.4％）で、次いで「従業員による紛失・盗難対策」（54.1％）となり、いずれも５割を超えた。（図４）



（N=1,022）

図４．主要な「外部からサイバーの攻撃対策」の実施状況

一方、「情報漏えい対策」としては、「重要情報にアクセスできる人員（部署）の制限」（52.4%）がトップになり、次いで「重要情報の定義・特定・他の情報資産との分類」（51.9%）、「PCの社外持出しの禁止」（51.7%）、「外部デバイス（USBメモリ、スマートデバイスなど）へのデータ移動の制限」（51.4%）が５割を超えた。（図５）



（N=1,022）

図５．主要な「情報漏えい対策」の実施状況

3 第三者認証に対する意識

システムリスクの緩和策としては「リスクマネジメントシステムの構築」や「セキュリティポリシーの策定」があり、その一環として主要なセキュリティ関連の第三者認証の取得がある。認証を取得する目的には、顧客が取引先から信頼を得ることも大きい。

3-1. システムリスクの緩和策の取組み状況

システムリスク緩和策への取組み状況については、「実施済み」の５項目すべてが５割を超え、「実施予定」を含めると約８割に達した。（図６）

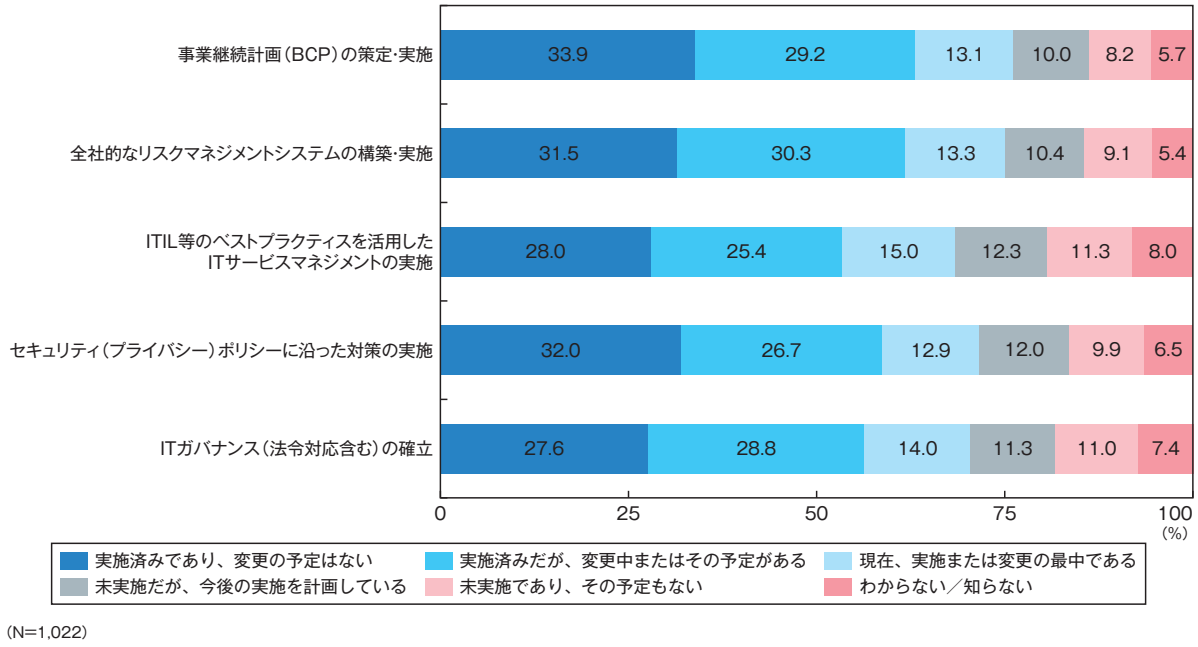


図６．システムリスクの緩和策の取組み状況

3-2. 情報セキュリティに関する第三者認証への取組み

情報セキュリティに関連した第三者認証への取組みについては、プライバシーマークの「取得済み」が52.0％、ISMSの「取得済み」が49.3％となっており、前回調査より若干増加した。（図７）

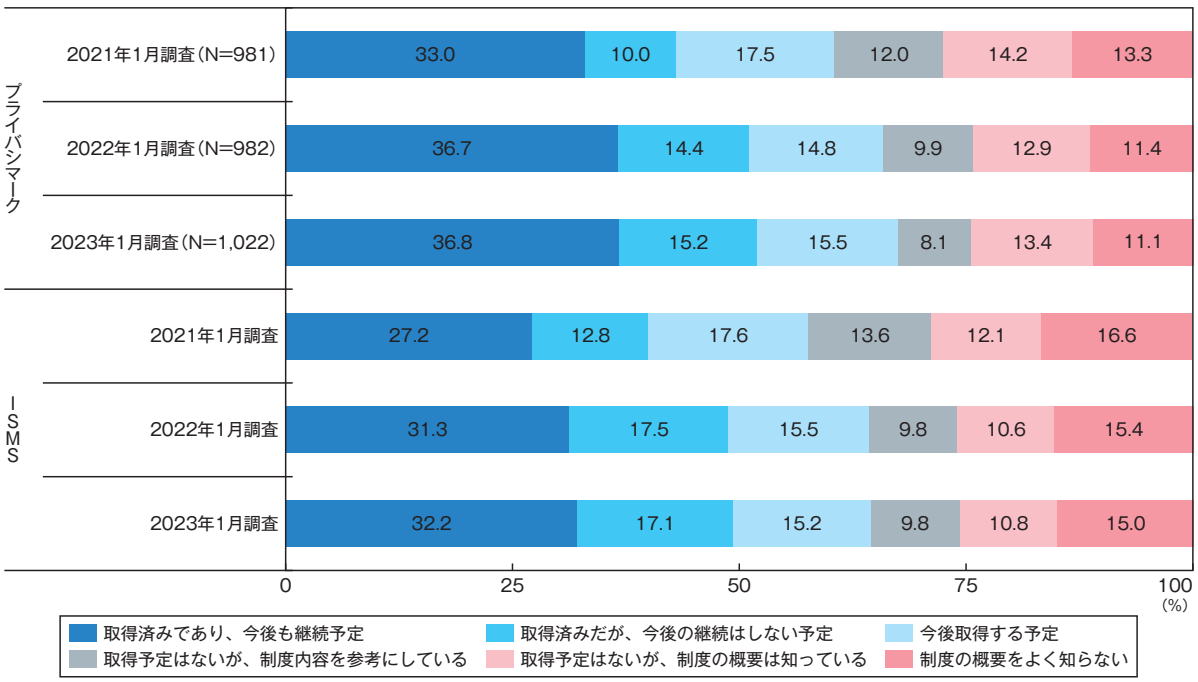


図７．情報セキュリティ認証への取組み状況

3-3．第三者認証取得の効果

第三者認証を取得することの効果としては、「取引先からの信頼性が向上」が最も多く、プライバシーマークで47.1％、ISMSで39.1％となった。（図８）

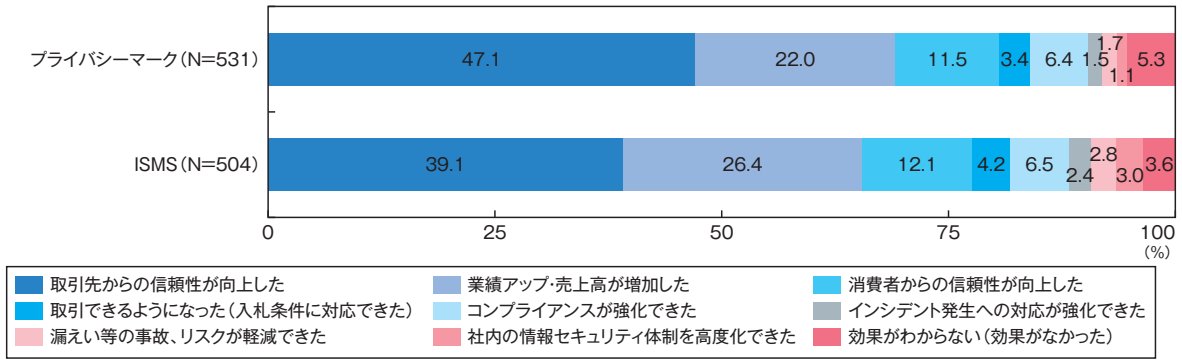


図８．第三者認証取得の効果

【コラム】プライバシーマーク制度創設25周年

JIPDEC　プライバシーマーク推進センター　福岡　峻

DX の推進やテレワークが増加する中で、個人情報を取り扱うケースが今まで以上に多くなっています。それに伴い、個人情報に関する事故も増加しています。個人情報の取扱いに関する事故は、企業のイメージ・信頼を毀損し、また、賠償等を支払うケースに発展することもあり、再発防止策への投資など企業は大きなダメージを被ることとなります。

事故を防ぐために企業が行っていることとして、当協会による調査では、「社内教育」が最多、次いで「体制の構築」となっています※1。組織として個人情報を適切に取り扱っていくためには、一人ひとりが個人情報保護の意識を持ちつつ情報を取り扱うこと、全員が同じ（適切な）ルールのもとで動くこと、そのための体制を整備することが大切です。

一方、消費者は個人情報保護についてどう考えているのでしょう。こちらも当協会による調査では「プライバシー保護に関して関心がある」「金銭的利益やポイントの有無に関わらず、個人に関する情報の提供に関し、慎重」と答えた人が共に 70％を超えています※2。消費者も、サービスを受ける際、日常的に個人情報を入力する機会がある昨今だからこそ、企業の個人情報保護に関する取組みに注目をしている、と言えるでしょう。

さて、企業においては個人情報を適切に取り扱う社内体制の整備が重要であることは当然ですが、一方で、消費者も個人情報保護に注目していると考えると、自社の取組みが適切であることを対外部に伝える必要もあるのではないでしょうか。プライバシーマークは企業の個人情報の取扱いが適切であることを消費者にわかりやすく示すマークです。このマークを通じ、個人情報に関して安心できる社会になってほしい。これが、当協会が 1998 年から運営しているプライバシーマーク制度の根幹にある考え方です。

プライバシーマーク制度は 2023 年４月で 25 周年を迎えました。25 周年を機に、個人情報保護に関するさまざまなコンテンツを公開していく予定です。たとえば、多くの企業が社内教育に力を入れていることから、社内教育用参考資料としての動画を、YouTube に今年４月に公開しました。

この 25 年間がそうであったように、個人情報保護は、事業活動上はもちろん消費者行動上でも、ますます重要なものになっていくでしょう。プライバシーマーク制度は、一人ひとりが個人情報に関する安心を当たり前に享受できる未来を目指し、邁進してまいります。個人情報保護に適切に取り組むためにも、ぜひ、25 周年を迎えたプライバシーマーク制度にご注目ください。

プライバシーマーク制度25周年ロゴ

プライバシーマーク制度 25 周年特設サイト：https://privacymark.jp/lp/25th/

YouTube「【JIPDEC 公式】プライバシーマークチャンネル」：https://www.youtube.com/@jipdec_pmarkchannel

※1　JIPDEC/ITR「企業 IT 利活用動向調査 2023」（2023 年 3 月）
https://www.jipdec.or.jp/archives/publications/tjvsos000000175t-att/J0005187.pdf

※2　JIPDEC「プライバシーガバナンスに関する調査結果 ～アンケート調査 詳細報～」（2022 年 3 月）
https://www.jipdec.or.jp/news/news/htpisq0000002w03-att/20220318_summary_privacygovernance_research.pdf

4　個人情報保護への取組み

2022年４月に改正個人情報保護法が施行され、グローバルではEUの一般データ保護規則（GDPR）をベースに各国でプライバシー法規制の整備が進んでいる。改正個人情報保護法に対してどのように取り組み、ソリューションやテクノロジーが検討・導入されつつあるのかを前回調査に続き調査した。

4-1. 個人情報保護についての取組み

個人情報保護についての取組みとして「社員教育」（57.6％）が最も多く、次いで「管理体制の構築」（48.6％）、「規程類の整備」（39.7％）と続き、傾向は前回調査と同様となった。（図９）

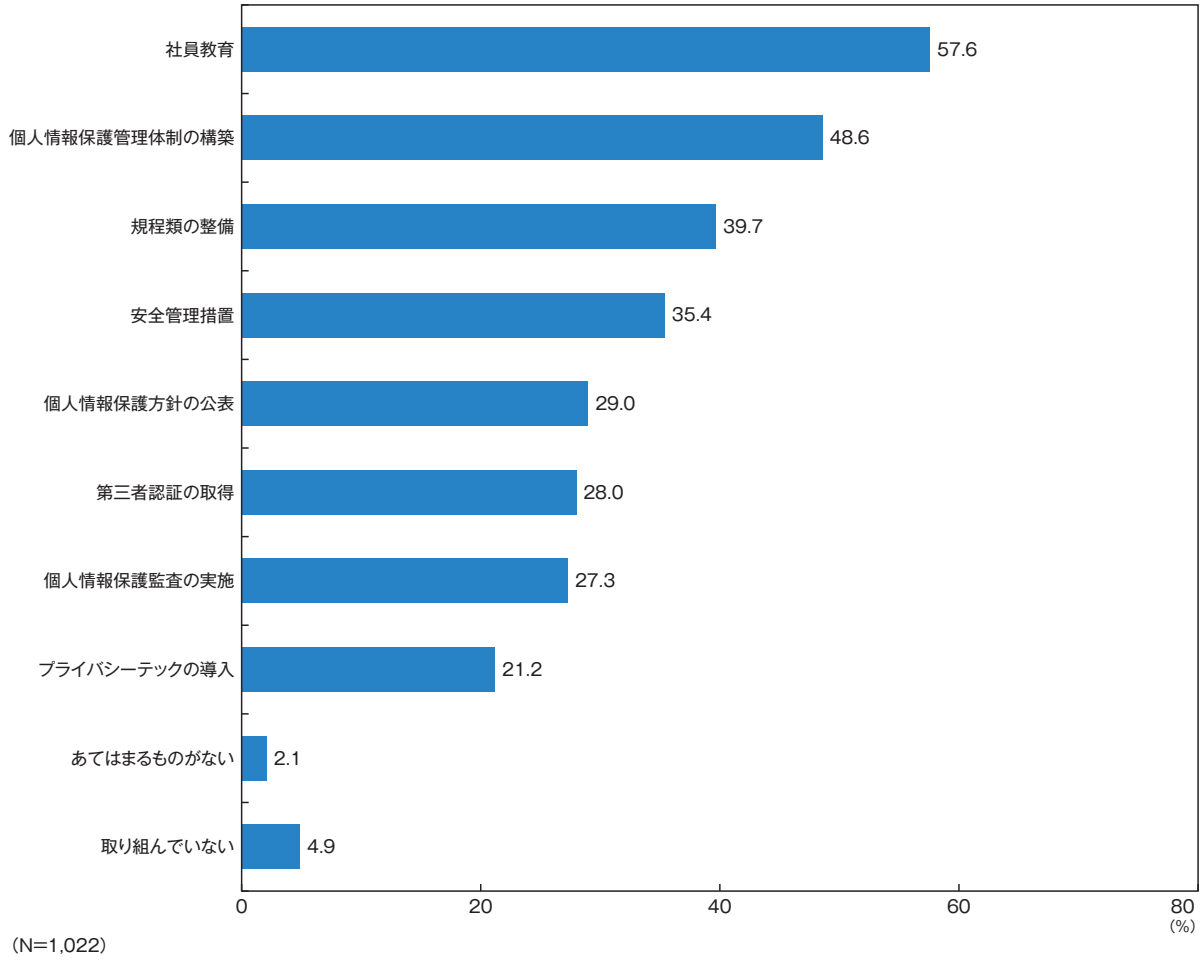


図９．個人情報保護についての取組み

4-2. 改正個人情報保護法遵守の課題

2022年４月に施行された改正個人情報保護法を遵守する際の課題についても、現行の取組み同様、「社員教育」（39.2％）と「体制整備」（38.7％）の比率が高い。（図10）

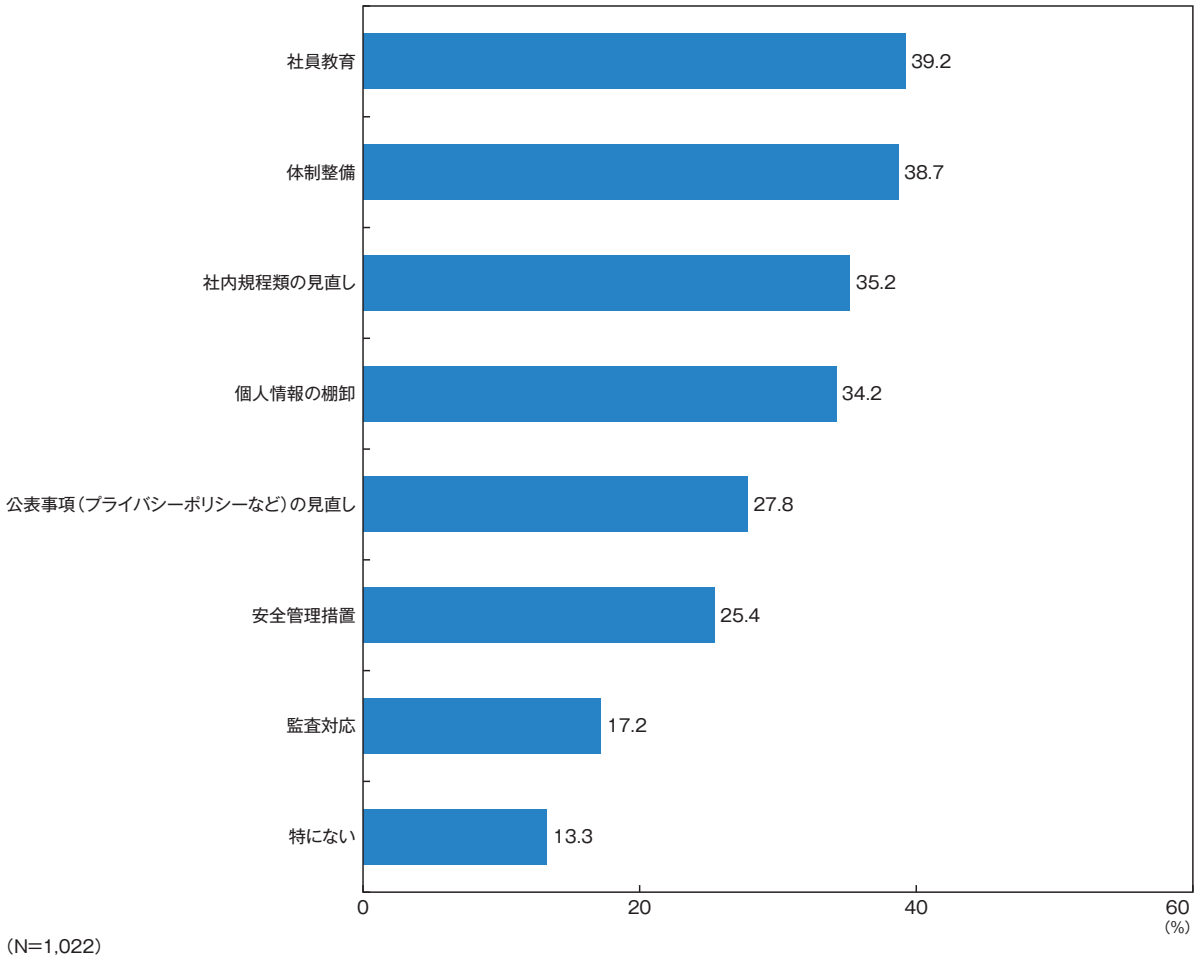
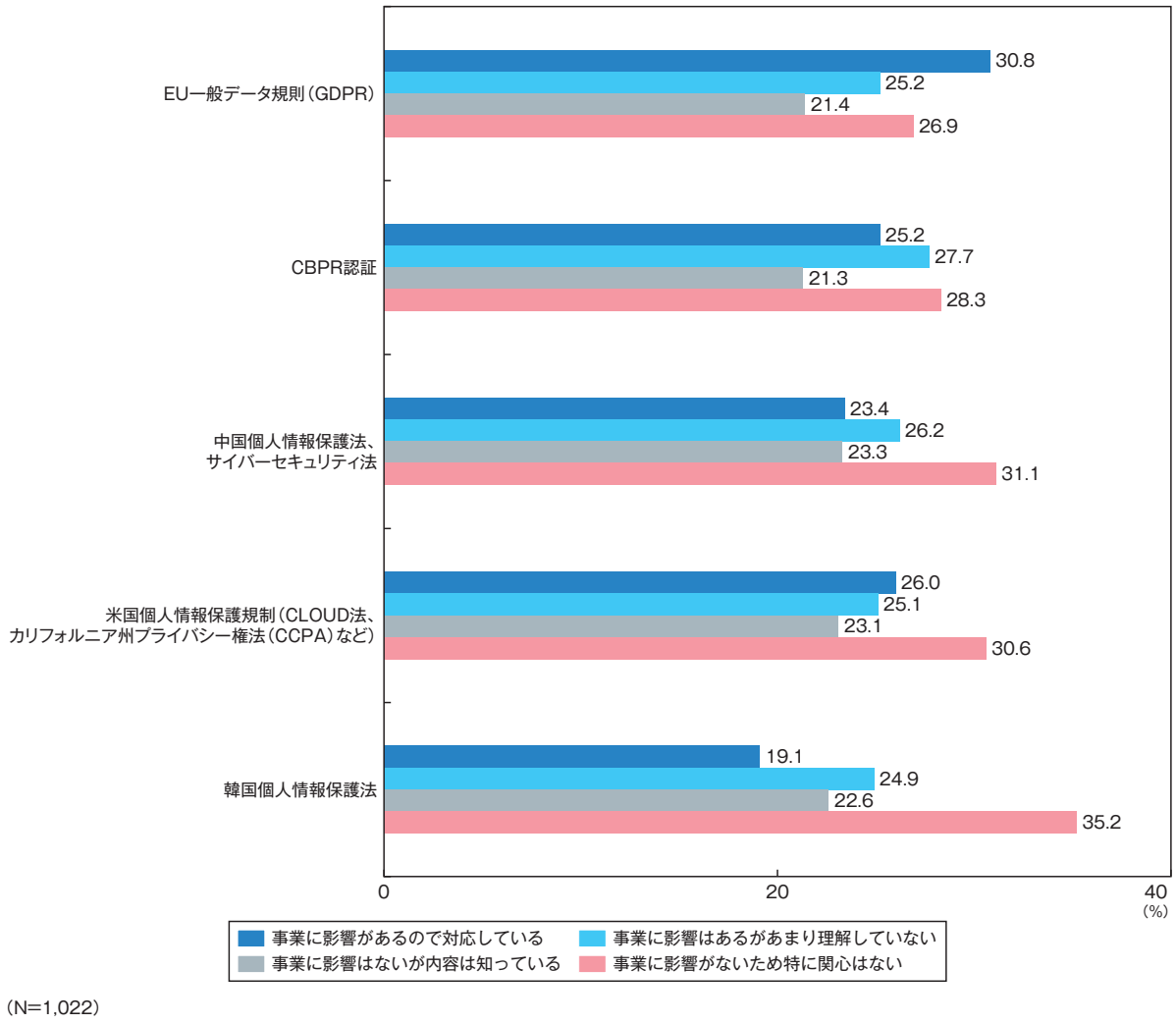


図10. 改正個人情報保護法遵守の課題

4-3. 各国のプライバシー法規制の影響

各国で強化されつつあるプライバシー法規制について、最も影響を受けて対応しているのは「EU一般データ保護規則（GDPR)」（30.8％）で、逆にあまり影響がないと思われるのは「韓国個人情報保護法」で、「事業に影響がないため特に関心がない」が35.2％となった。（図11）



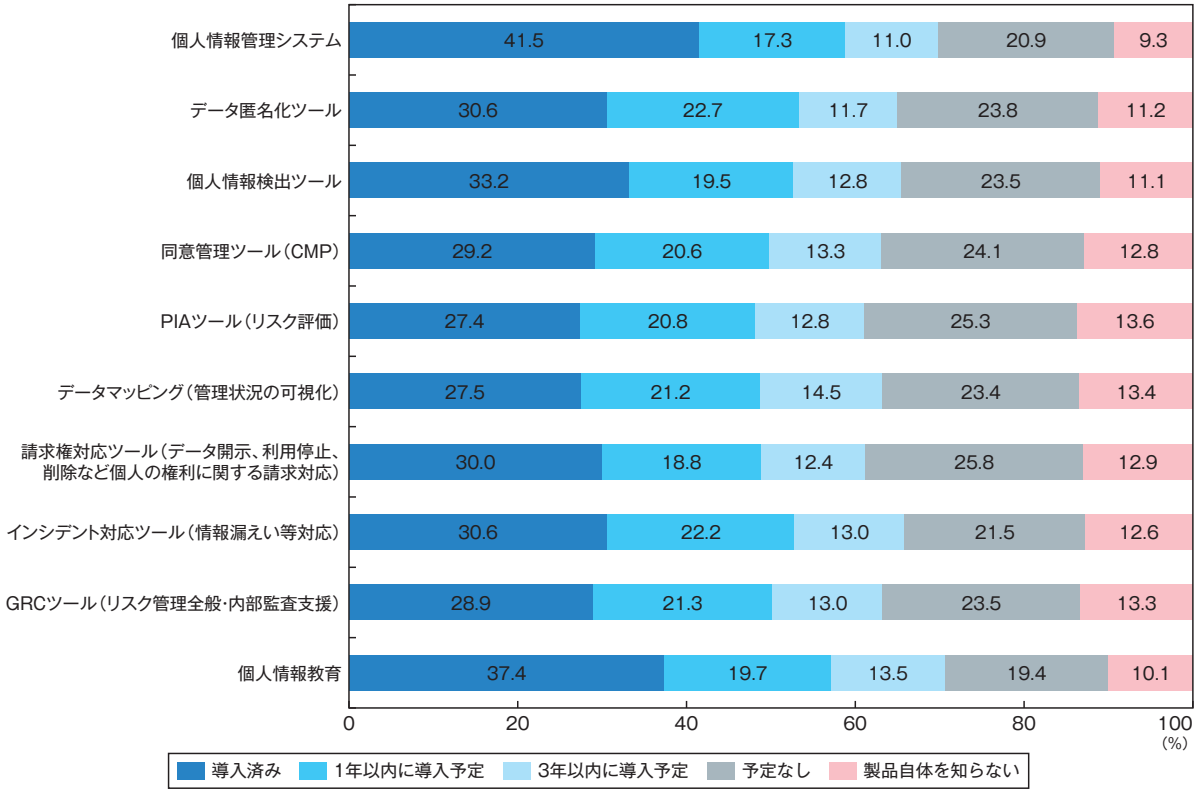
（N=1,022）

図11. 各国のプライバシー法規制の影響

4-4. プライバシーソリューション／テックの導入状況

プライバシーソリューション／テックの導入状況としては、すでに導入済みなのは「個人情報管理システム」（41.5%）が最も多く、次いで「個人情報教育」（37.4%）、「個人情報検出ツール」（33.2%）と続いた。

今回取り上げたソリューション／テックについては、３年以内に６割以上で導入されているであろうことが予想される。（図12）



（N=1,022）

図12. プライバシーソリューション／テックの導入状況

5　セキュリティ支出／セキュリティ製品／技術の利用動向

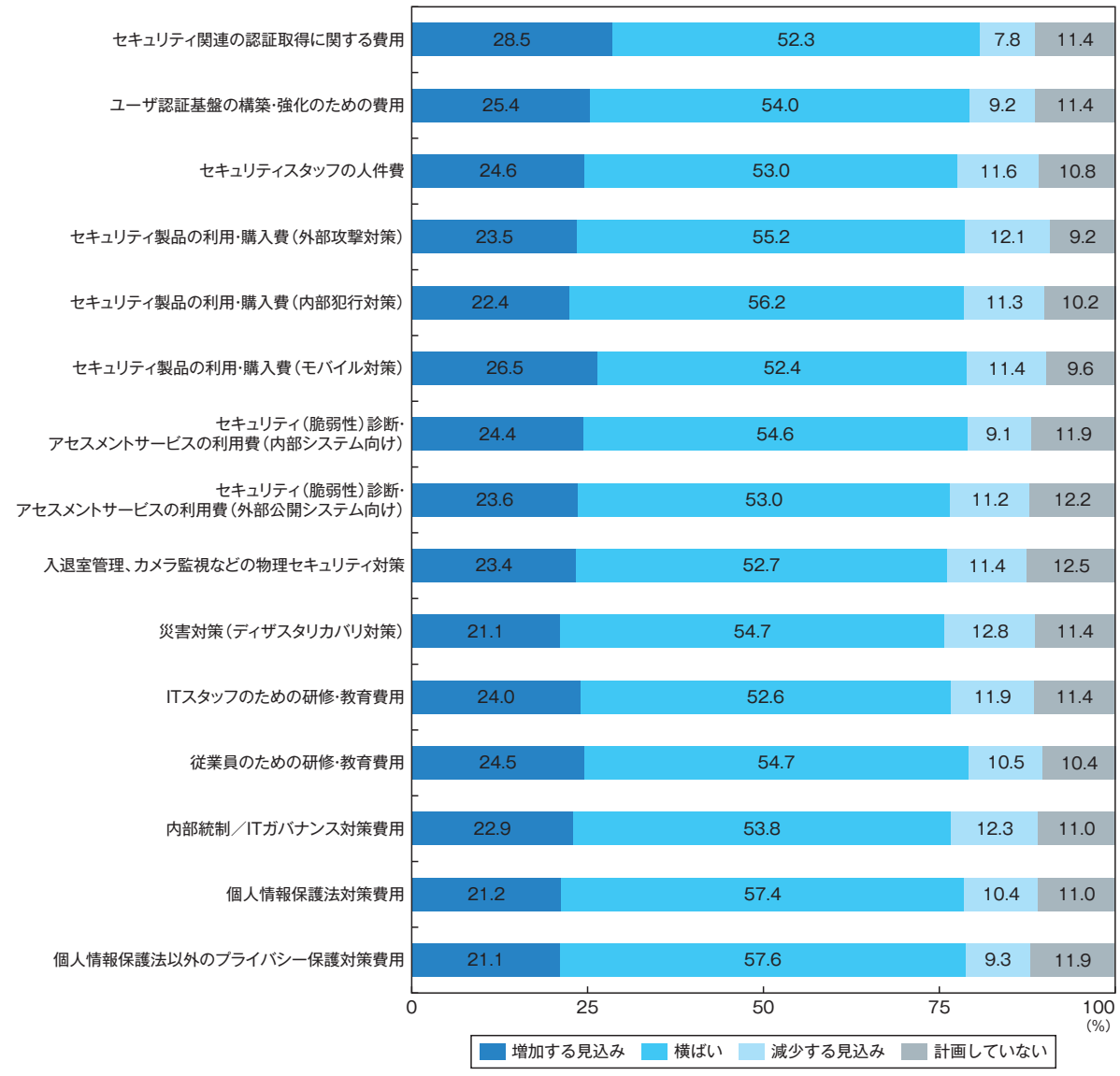
コロナ禍を経て、リモートワークやクラウドサービスの利用が常態化していくなか、2022年度のセキュリティ支出動向と、次年度の支出予算と、セキュリティ製品や技術の利用動向について調査を行った。

セキュリティ支出については、実績・予算ともに増加が約２割、横ばいが約５割で前回調査と同様となった。

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おり、利用シーンにおいても従来の境界防御型セキュリティ製品からゼロトラスト型セキュリティサービスへ移行が進んでいる。

5-1. セキュリティ支出（実績）の増減傾向

セキュリティ支出の増減動向については、すべての支出項目において「横ばい」が５割を超えているが、「増加」と回答している比率もすべての費用で２割を超えている。（図13）

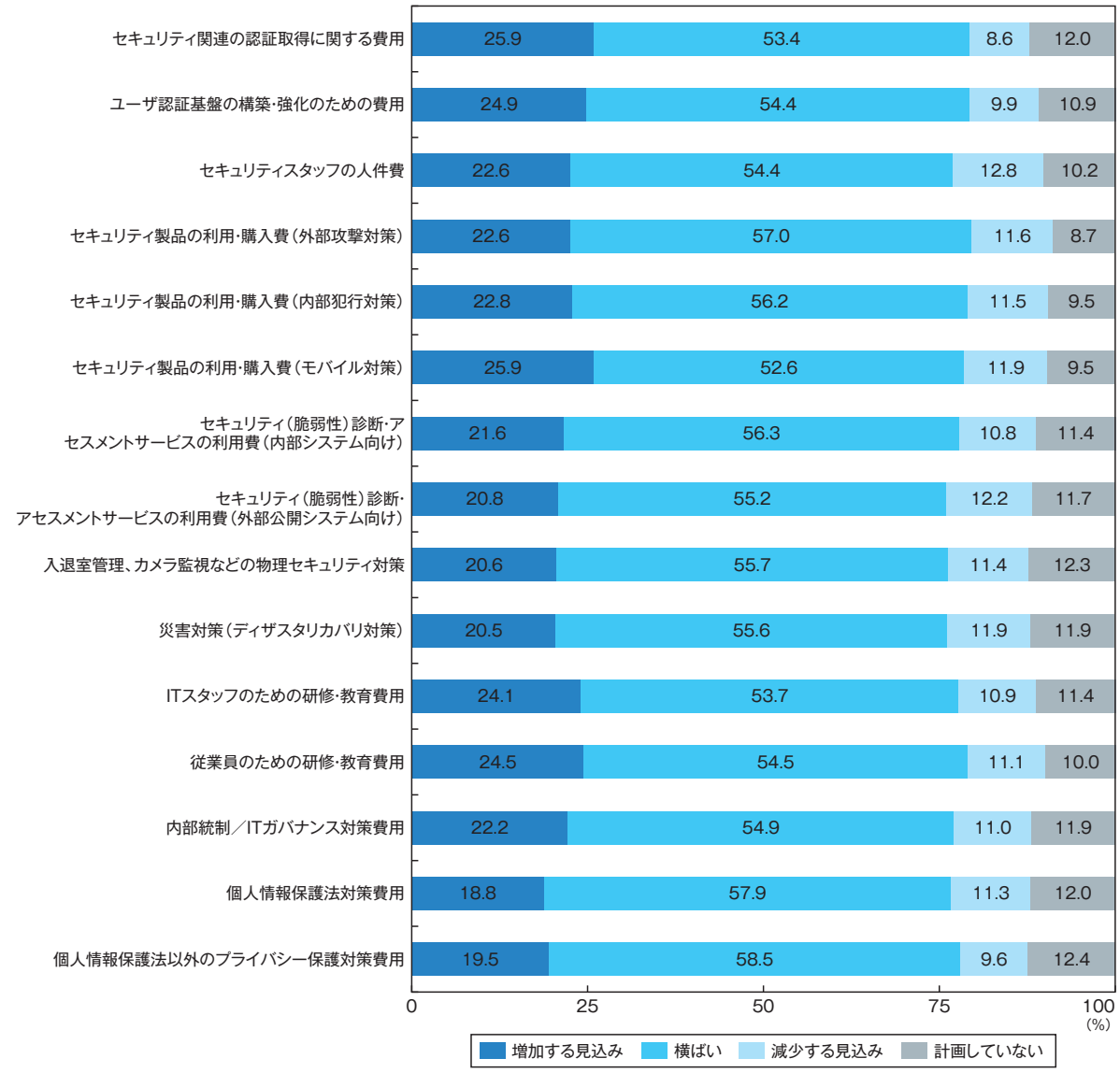


(N=1,022)

図13.　セキュリティ支出実績の増減傾向

5-2. セキュリティ支出（計画）の増減傾向

今年度のセキュリティ支出計画については、全項目で「増加」が約２割、「横ばい」が約５割となっている。（図14）



(N=1,022)

図14. セキュリティ支出計画の増減傾向

5-3. ネットワーク／ゲートウェイ製品の利用状況

すでに導入済の製品としては、「ファイアウォール・NGFW・URM」が53.7％、次いで「VPN、セキュアリモートアクセス、プライベートアクセス」（45.1％）が続いた。（図15）

最近注目されている「統合振舞い検知サービス（XDR）」や「CSPM（Cloud Security Posture Management）ツール」の導入状況は、「導入済み」「１年以内の導入予定」をあわせても、他の製品と比べ比率はまだ低い。

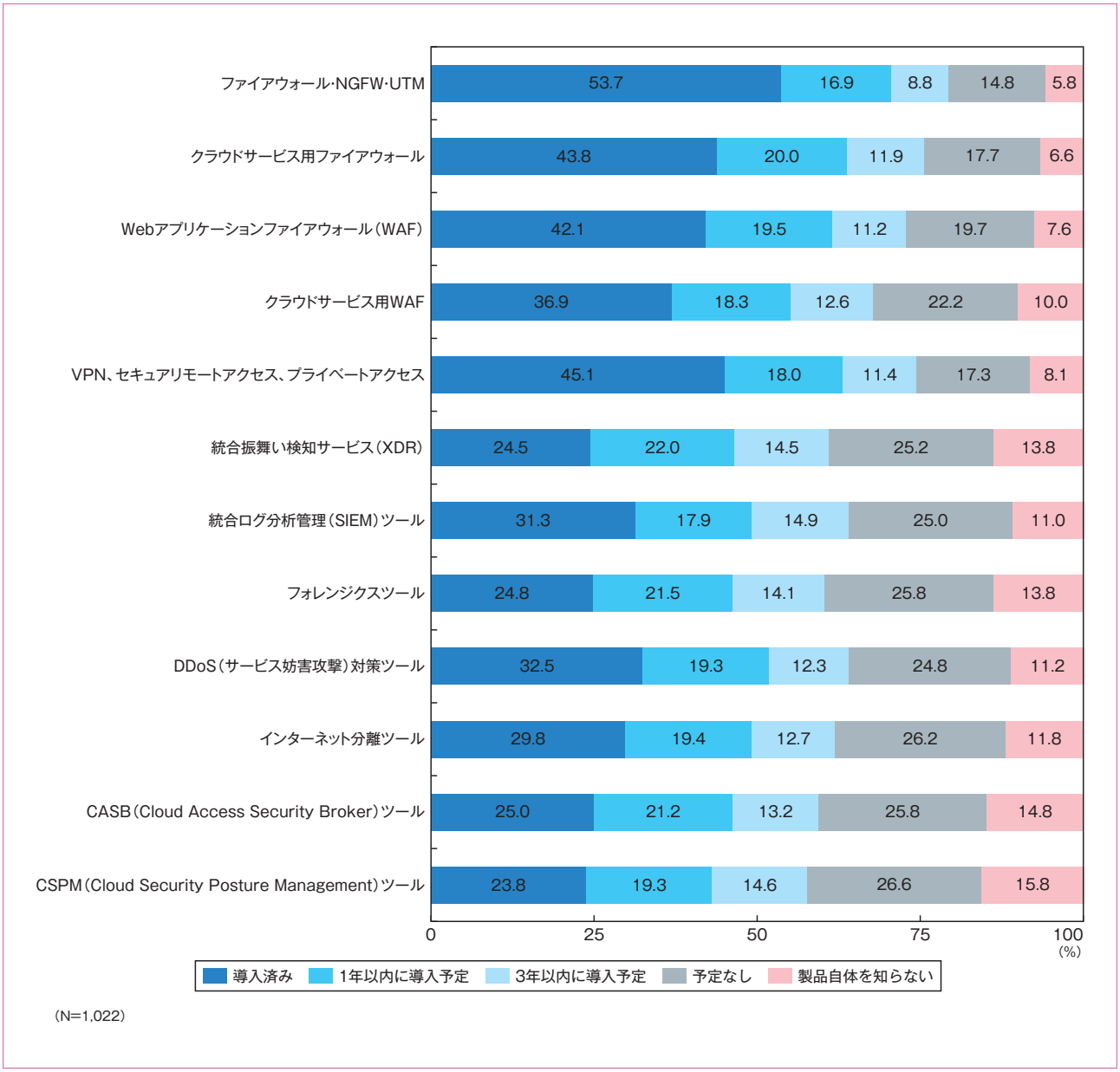
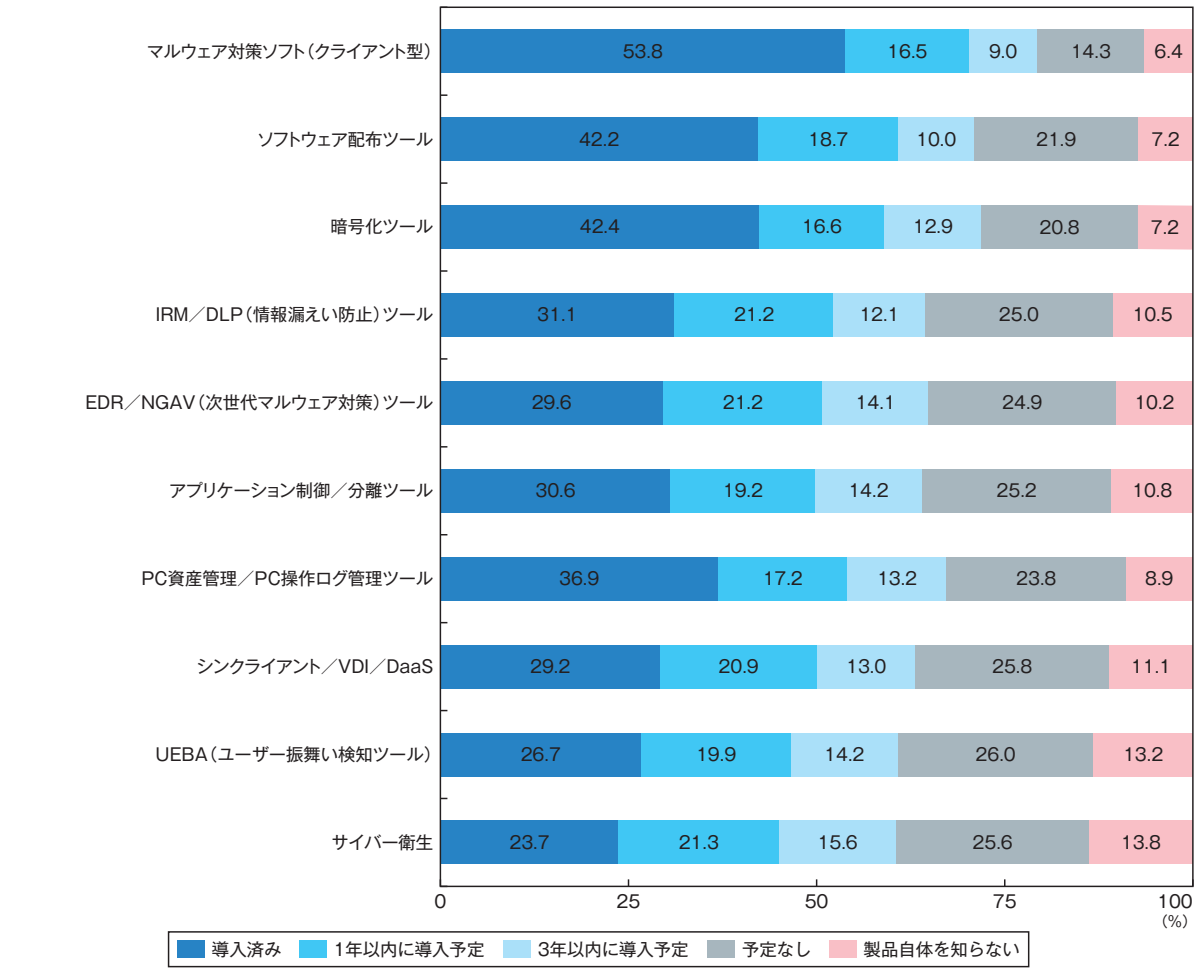


図15. ネットワーク／ゲートウェイセキュリティ製品の利用状況

5-4. 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は、従来型のマルウェア対策ソフトの利用率が依然高く53.8％だが、次世代型ウイルス対策ソフトである「EDR」を今後「１～３年以内に導入予定」は35.3％となっており、今後導入率の差は縮まっていくことが予想される。次いで導入率が高いのは「暗号化ツール」（42.4％）、「ソフトウェア配布ツール」（42.2％）となっており、これらについても７割が今後導入予定としている。（図16）



(N=1,022)

図16. エンドポイントセキュリティ製品の利用状況

5-5. セキュリティサービスの利用状況

サイバー攻撃被害の増加が確認される中、セキュリティサービスは、前回調査と同様、攻撃を検知する「脆弱性診断サービス」や「侵入検知サービス」の導入率が約４割となっており、「導入予定」を含めると約７割に達した。（図17）

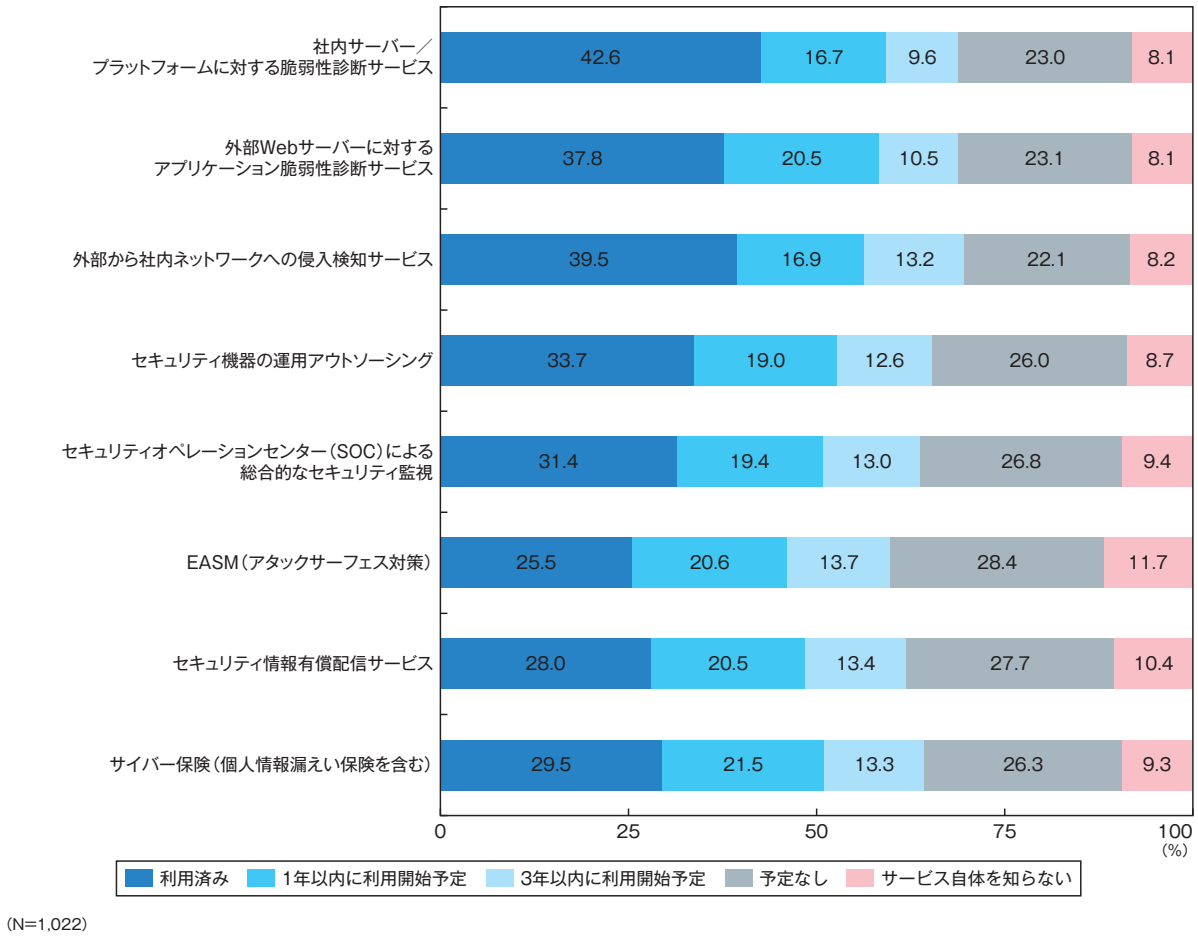
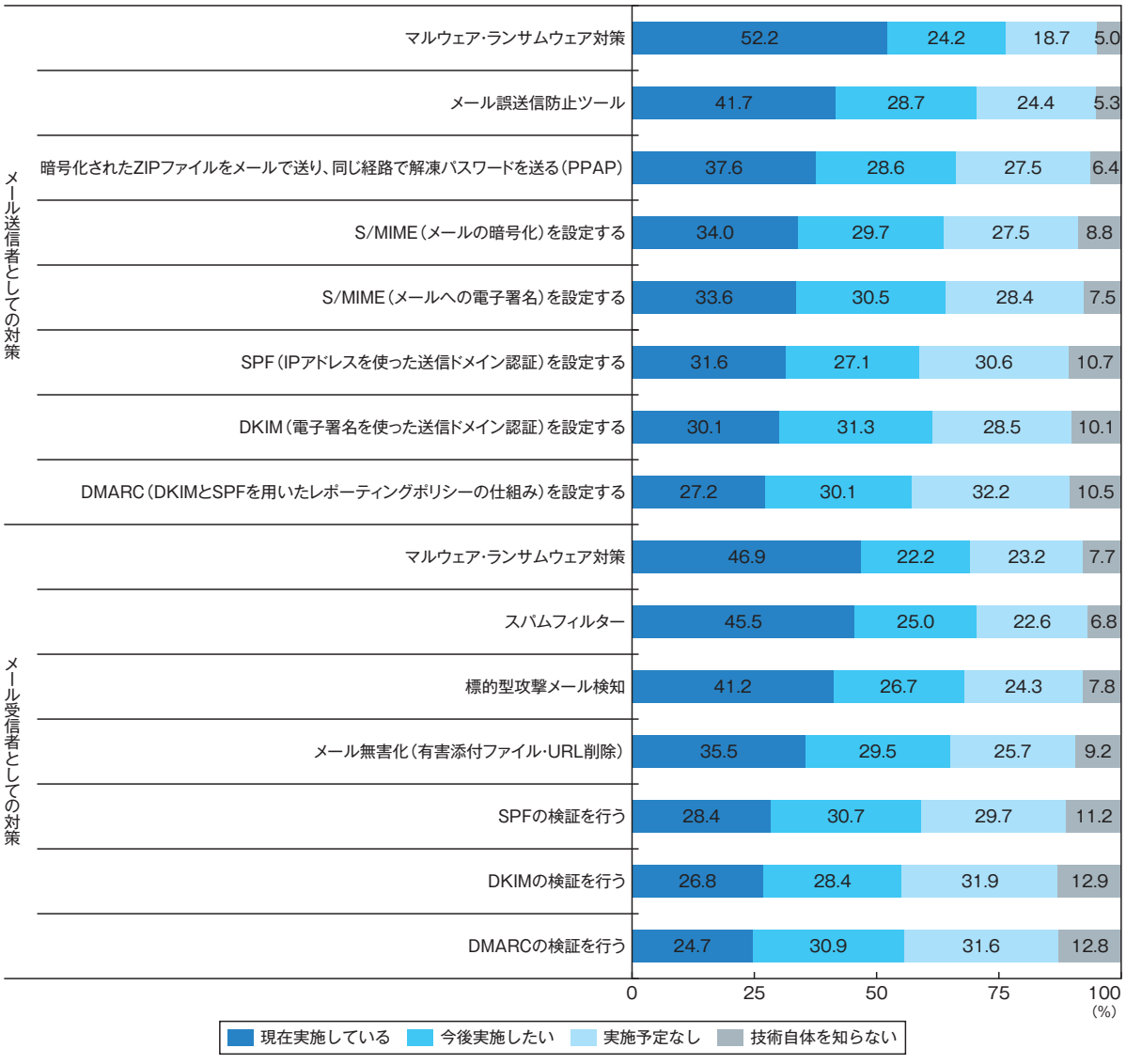


図17. セキュリティサービスの利用状況

5-6. 電子メールのセキュリティ対策状況

「実施済み」の電子メールのセキュリティ対策は、送信側・受信側共に「マルウェア・ランサムウェア対策」がトップで、メール経由の感染対策が重視されている。（図18）



（N=1,022）

図18. 電子メールのセキュリティ対策状況

【コラム】受信者がひとめでわかるなりすましメールの確認方法

JIPDEC　セキュリティマネジメント推進室　主幹　高倉 万記子

メールのセキュリティ対策のうち、送信者が誰かになりすましてメールを送っているかどうかを受信者が見分けるためのものとして、S/MIME（エスマイム）と BIMI（ビミ）が代表的です。

S/MIME は電子証明書を利用したなりすまし対策の仕組みですが、この電子証明書については、認証局とブラウザの集まりである CA/Browser フォーラムで、国際的なルールを決めていこうとしています。今年 9 月より、S/MIME Baseline Requirements（S/MIME BR）が施行される予定です。S/MIME BR では S/MIME 用の電子証明書を発行する認証局のセキュリティ基準や運用基準が定められています。各認証局ベンダーは S/MIME BR に対応した認証局への改修対応を進めています。世界的な動向に左右される仕組みですが、その分、国際的に使われるメーラーが利用を意識しており、2023 年 4 月に Thunderbird がバージョンアップで S/MIME を正常に取り扱いできるよう、改善したとリリースしているようです。

BIMI は、ブランドアイコンをメーラーに表示させることができるので、広告宣伝として利用できると関心が高いですが、まずは DMARC に対応させることが求められるため、挫折するという話を聞きます。また、各メーラーで表示する枠は正方形に近く、通常の企業名ロゴだと細長い長方形が多く、正方形の枠にあわせて表示させると小さく視認性に欠けるという欠点があります。そのため、新たにサービス用にロゴを商標登録しようとすると、日本では登録まで何カ月もかかるというのが欠点のようです。それでも、BIMI 対応メーラーを使っていると、企業ロゴをセットした企業が増えているのがわかります。

本調査では、企業のセキュリティ対策状況について調査したものですが、別途 JIPDEC が調査している「デジタル社会における消費者意識調査 2023」の結果[※1]によると、企業からの受信メールについて、送信元として表示されている企業が本当にその企業なのかを、どのように確認しているか尋ねたところ、S/MIME や BIMI も 1 割程度となりました。企業側が送信メールにこの対策を行うことで、企業や個人の受信者は確認するようになるのではないでしょうか。

※1　JIPDEC「デジタル社会における消費者意識調査 2023」（2023 年 3 月）
https://www.jipdec.or.jp/news/news/20230413.html

5-7. PPAPへの対応状況（送信系）

政府が非推奨としたPPAP（Zip暗号化添付メール＆パスワード同一経路送付）の送信系について、利用の有無に限らず、PPAPを知っている事業者のうち、「もともと利用していない」が10.4%、「利用を禁止している」が8.8%で、「今後利用を禁止予定」の27.2%を含めると、約５割弱が禁止する方向となっており、前回調査に比べ、PPAPの利用は減少傾向にある。（図19）

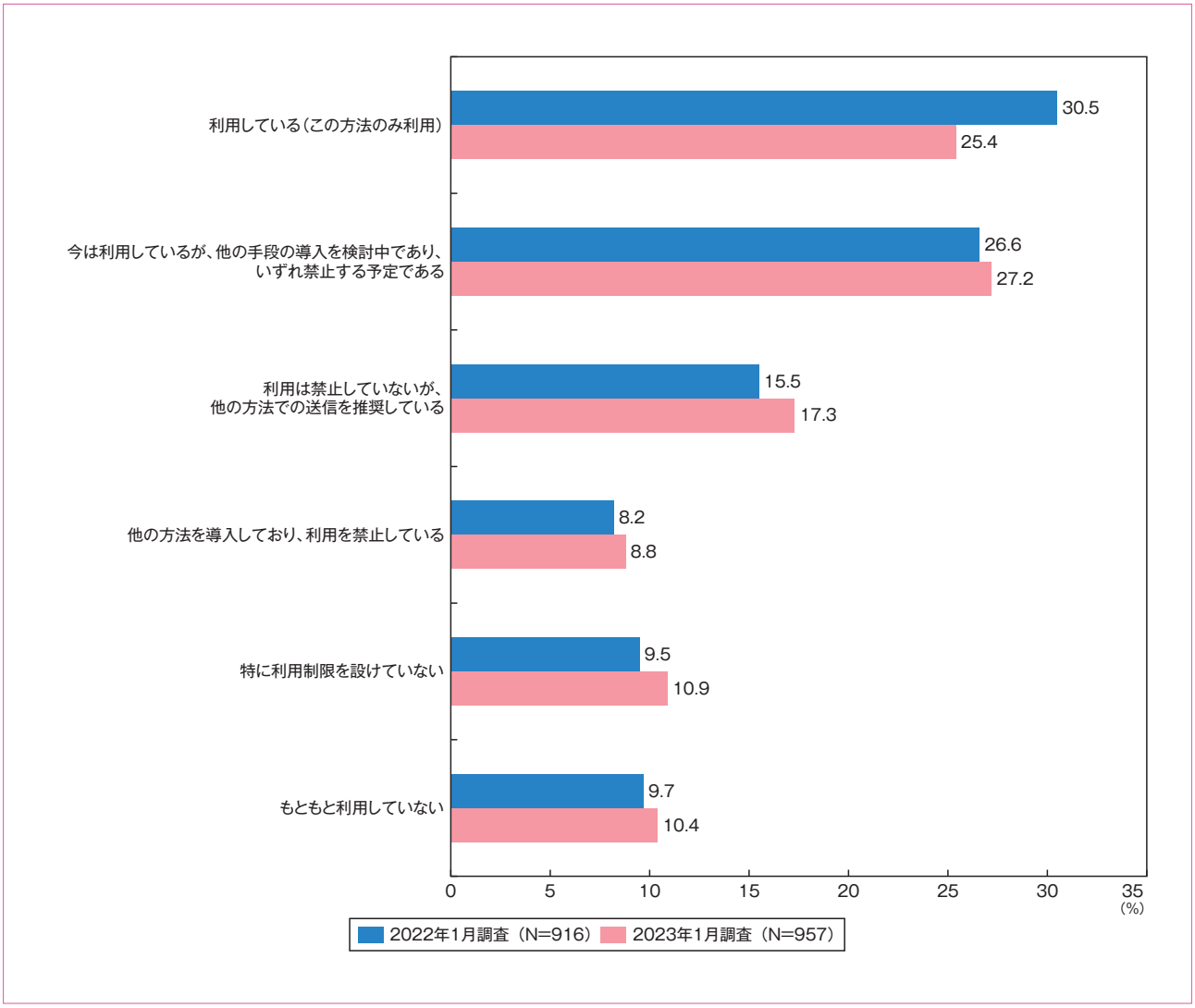
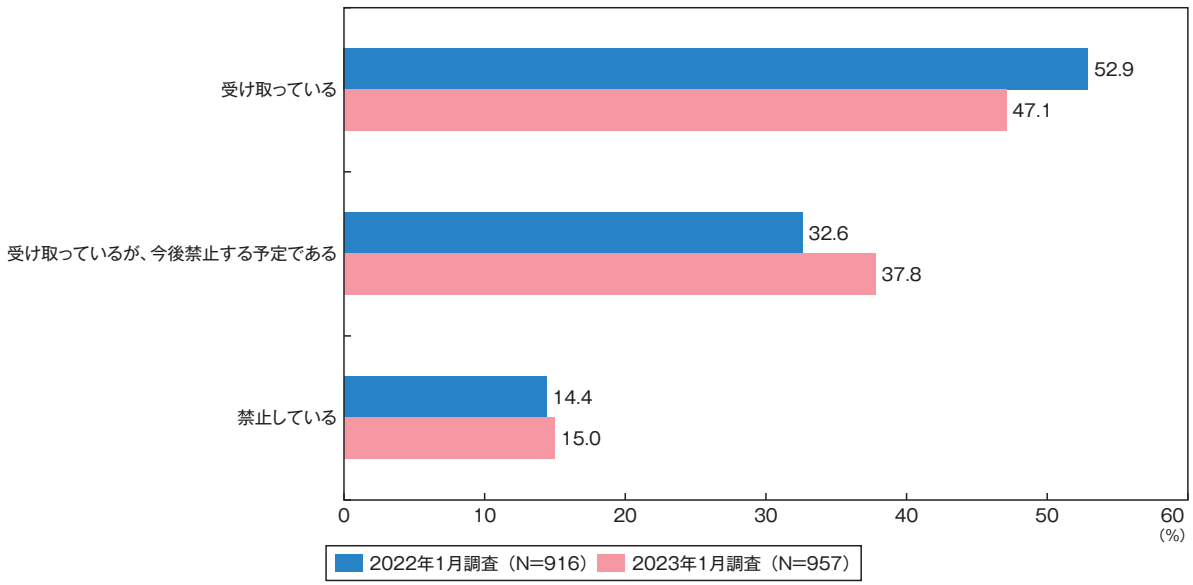


図19. PPAP（送信系）への対応状況

5-8. PPAPへの対応状況（受信系）

一方、PPAPの受信系は「禁止している」が15.0%、「今後禁止予定」が37.8%となり、約５割が禁止する方向となった。前回調査に比べ、PPAPを使ったメールのやりとりの制限が進んできている。（図20）



※「電子メールのセキュリティ対策状況でPPAPの「技術自体を知らない」と回答した2022:66件、2023:65件を除く

図20. PPAP（受信系）の対応状況

5-9. 高機密システムへのアクセス認証手段の利用状況

現在利用している認証手段として最も多い「ID・パスワード」（79.7％）は、前回調査の82.6％から３ポイント減少した。一方、前回調査と比べ増加が見られたのは「生体認証」で、前回30.8％から35.9％へと５ポイント増加した。

また、今後利用したいとする手段で多かったのは「多要素認証」（31.5％）、「生体認証」（30.8％）となった。（図21）

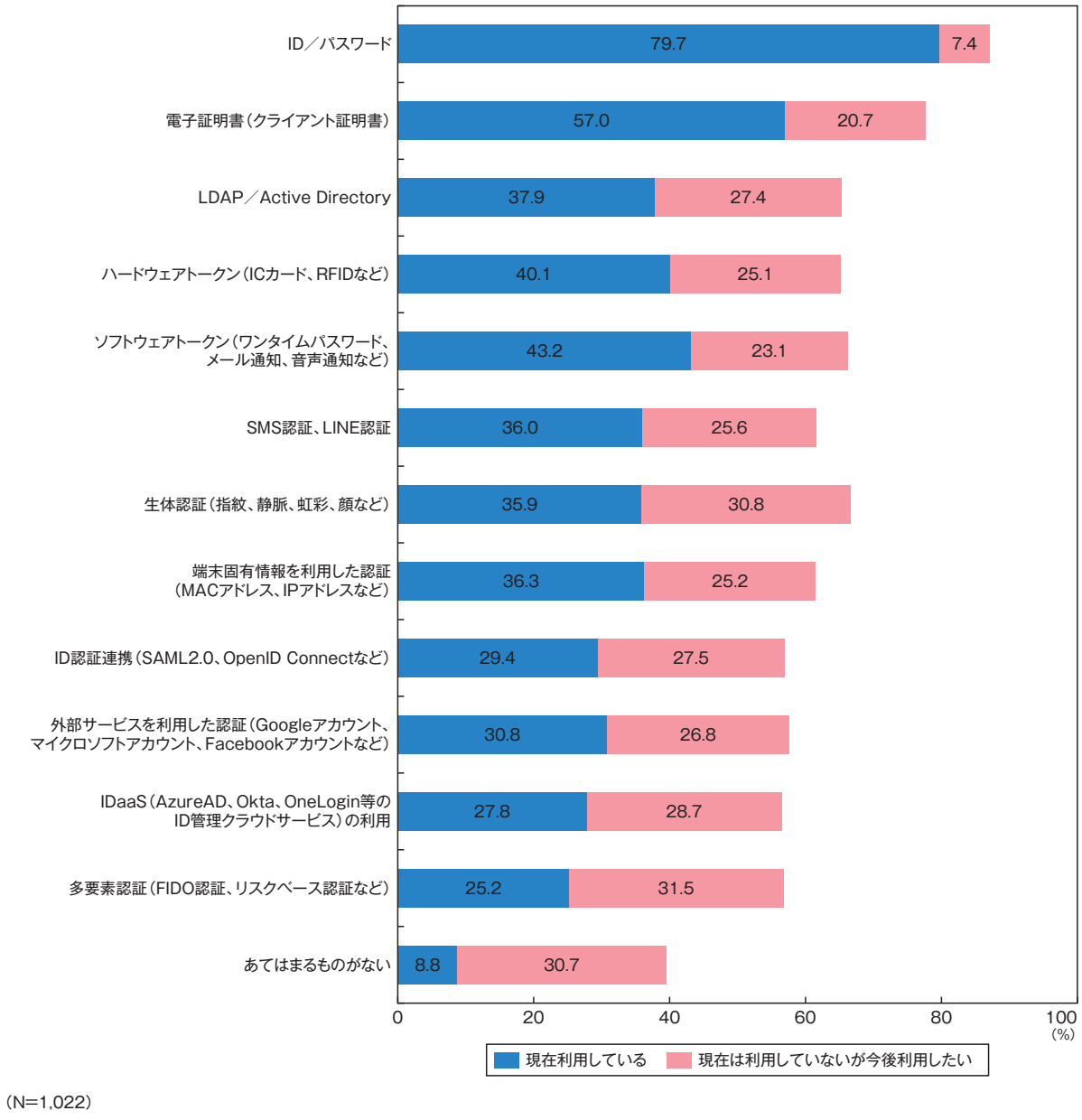


図21. 高機密性システムへのアクセス認証手段の利用状況

6　柔軟なワークスタイルとクラウドの動向

コロナ禍も４年目を迎え、テレワークは勤務形態の一つとして定着しつつある。また、クラウドサービス利用も増加していることから、ここでは、クラウドサービスの導入にあたってのポイント等について調査を実施した。

6-1. 柔軟なワークスタイルを実現するためのセキュリティ対策

柔軟なワークスタイルを実現するためのセキュリティ対策としては「スマートデバイス向け対策」（52.1％）が最も多く、「法人向けクラウドサービス利用」（48.6％）、「端末にデータを残さない環境整備」（47.1％）が続いた。（図22）

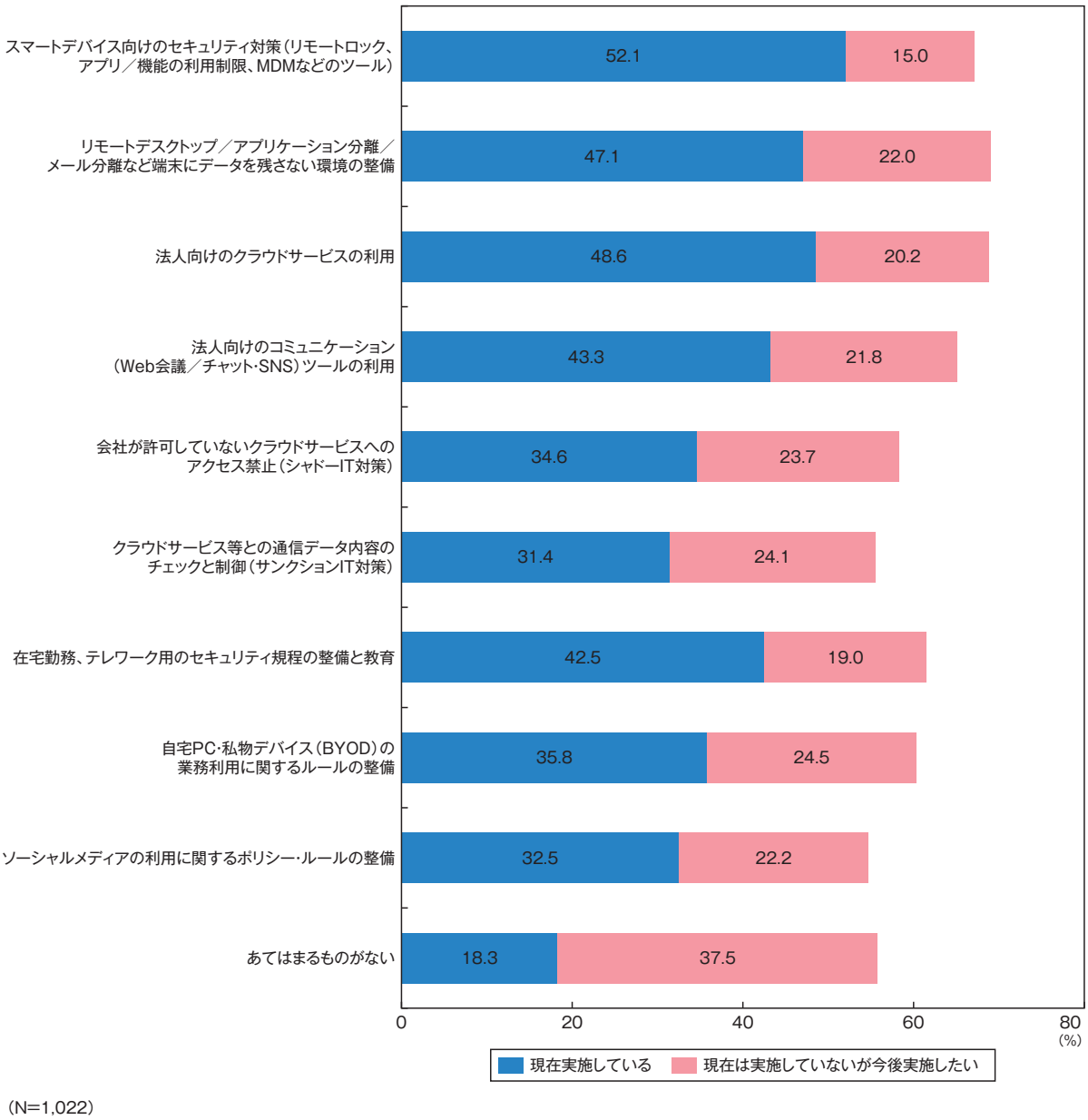


図22.　柔軟なワークスタイルのためのセキュリティ対策

6-2. クラウドサービスの利用状況

クラウドサービスの利用状況では、「すべてクラウドを利用」している割合自体は前回と変わりはないが、「半分以上クラウドサービスを利用している」比率が約５割に近づいた。また、多少なりともクラウドサービスを利用しているのは全体の約９割にのぼり、前回に比べ利用比率が５ポイント増加した。（図23）

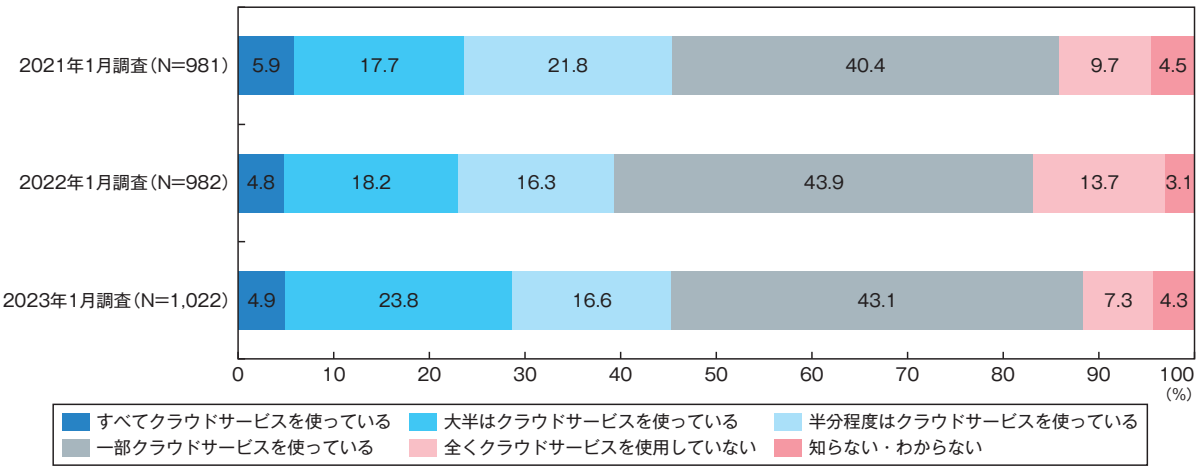


図23. クラウドサービスの利用状況

6-3. クラウドサービスの利用形態

クラウドサービスの利用形態では「コンテナサービス上での開発」（38.2%）がトップで、「SaaSを使用」（34.3%）、「IaaS/PaaS上での開発」（28.2%）が続く。（図24）

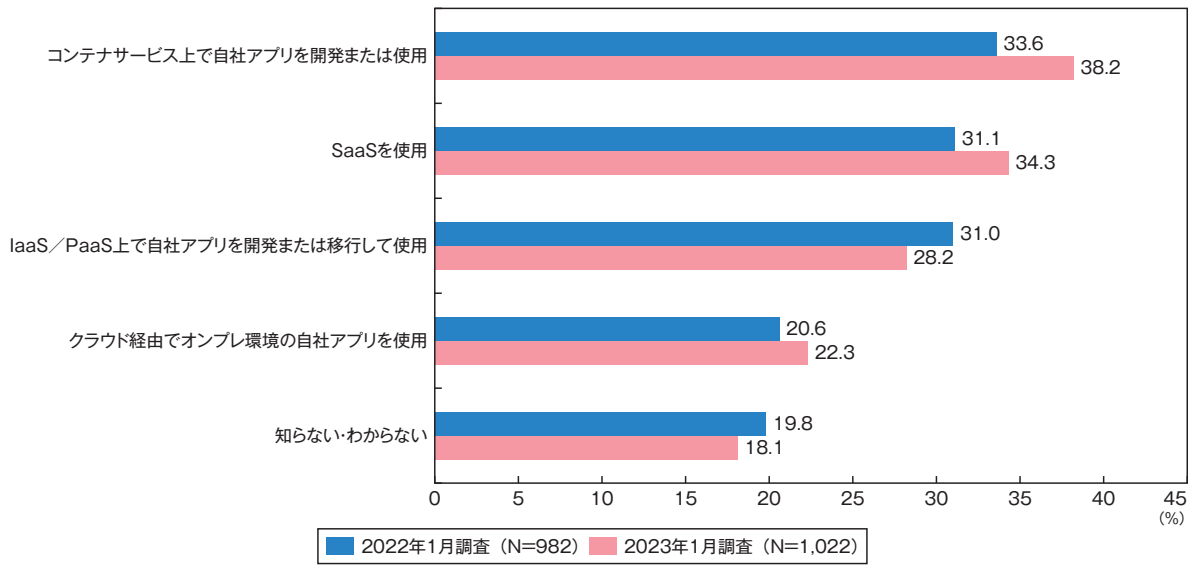


図24. クラウドサービスの利用形態

6-4. クラウドサービスを選定する際のポイント

クラウドサービスを選定する際のポイントとしては、「コスト」（54.7%）が最も高く、「第三者認証・認定制度取得により信頼性が確保できる」（41.6%）、「サポート体制の充実」（33.4%）、「セキュリティ対策」（33.3%）が続いた。（図25）

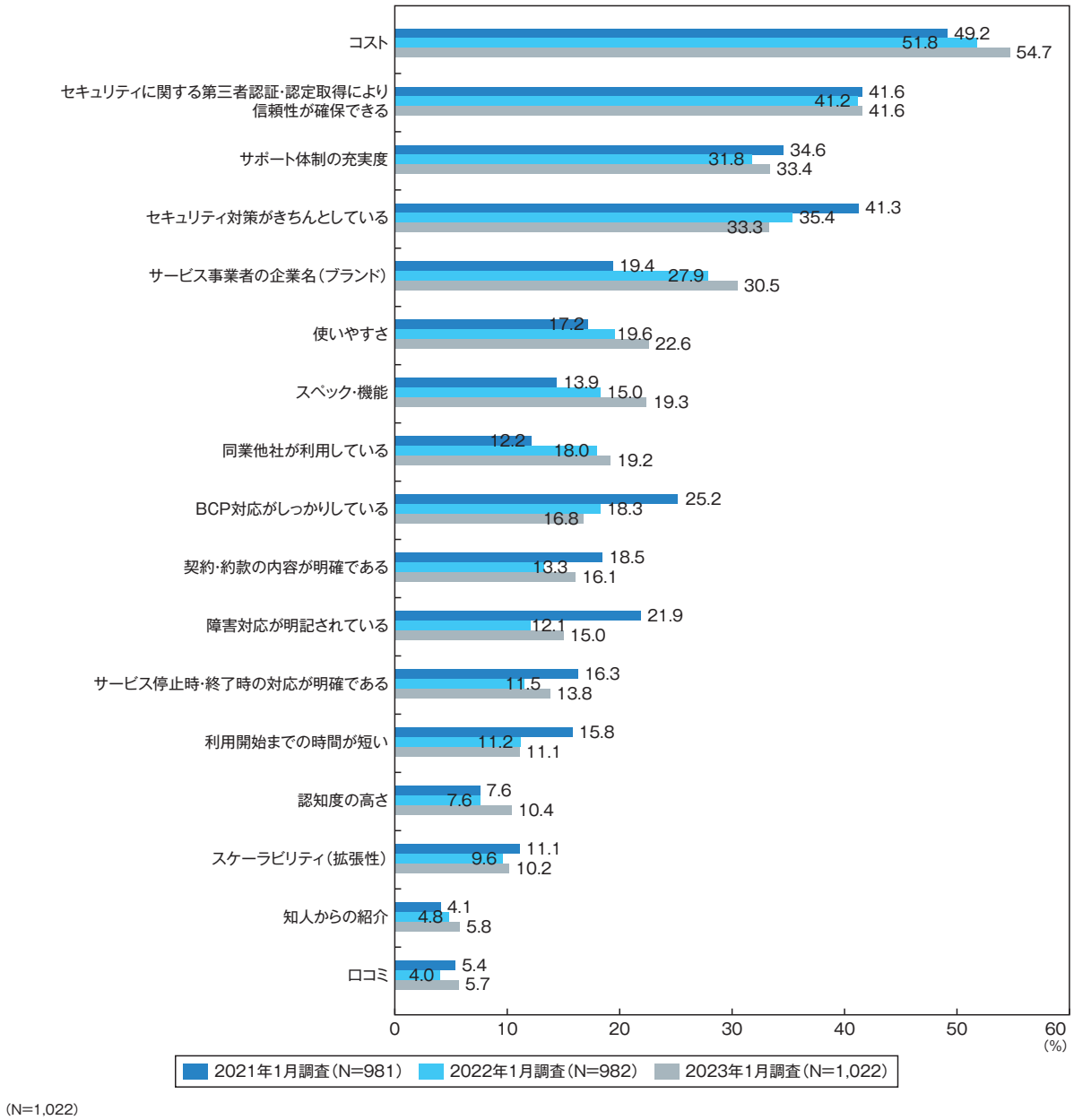


図25. クラウドサービスを選定する際のポイント

6-5. 信頼性を重視して選ぶクラウドサービス

「セキュリティに関する認証・認定制度取得により信頼性を確保できる」と回答した事業者が選定時に信頼性を重視するクラウドサービスは、「顧客管理」（58.1％）がトップで、「グループウェア」（52.0％）、「財務会計」（49.6％）が続く。（図26）

前回調査と比較すると、「経費精算」（41.7％から47.1％）、「財務会計」（44.4％から49.6％）、「SFA」（24.0％から29.2％）が５ポイント増加したのに対し、「グループウェア」が57.5％から52.0％と、５ポイント減少した。

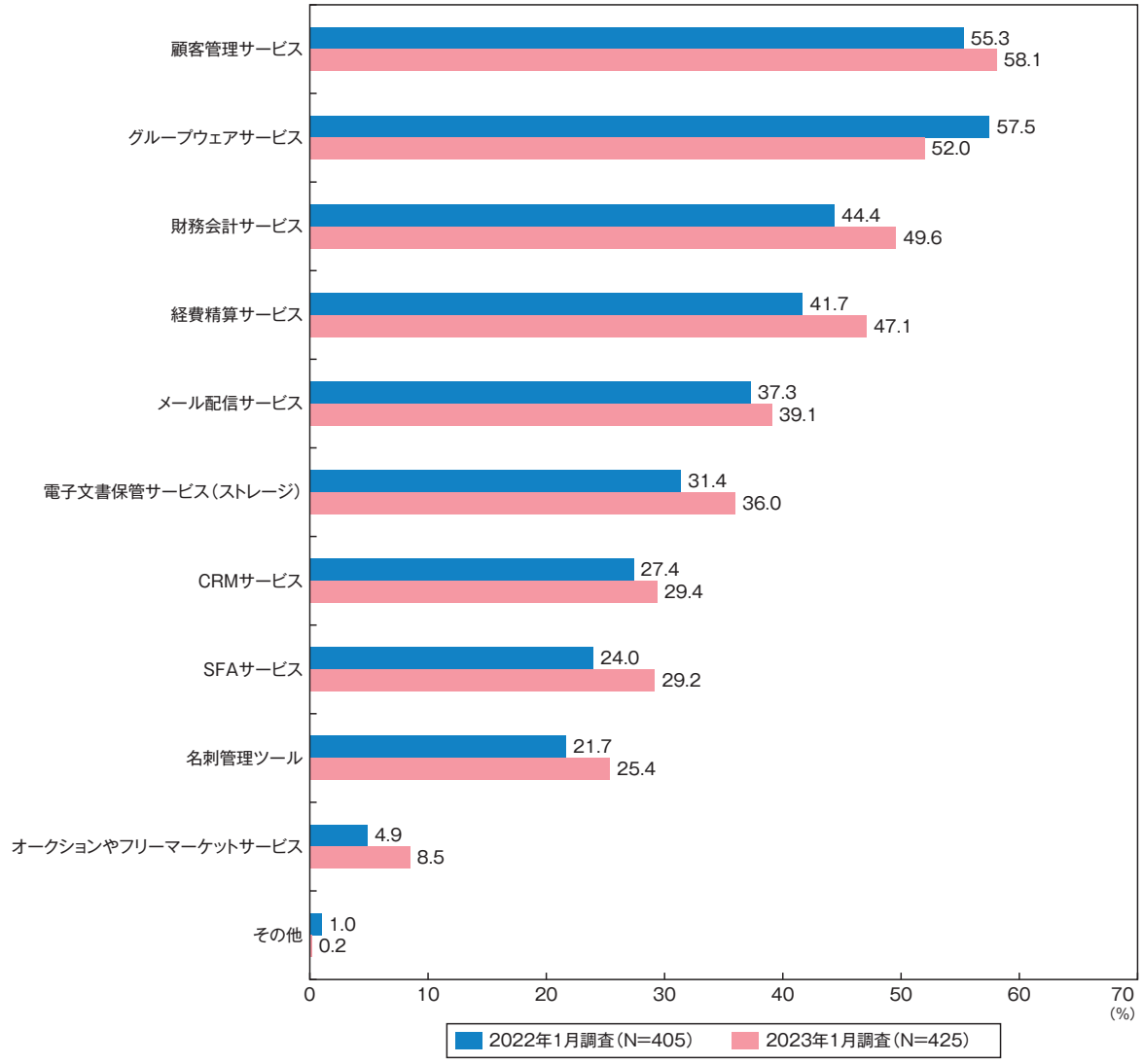


図26. 信頼性を重視して選ぶクラウドサービス

【コラム】ISMSクラウドセキュリティ認証

JIPDEC　セキュリティマネジメント推進室　室長　成田 康正

コロナ禍を契機に在宅勤務やデータ共有の必要性からクラウドサービスの利用は急拡大しています。その一方で、クラウドサービスの活用によって新しいリスク（クラウドサービスの障害、データ保存先の法域の違い等）に対応していく必要があります。この状況において、ISO ではクラウドサービスに関するリスク対策のガイドライン規格として、ISO/IEC 27017:2015「ISO/IEC 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範」を発行しました（日本語訳をした JIS Q 27017 は、2016 年に発行）。この規格では、クラウドサービスを提供する組織および利用する組織の両方に適用できる情報セキュリティ管理策を示しています。

ISO/IEC 27017 発行を受け、国内ではクラウドサービス関連のリスクへ対応していることを表明するための認証ニーズの声が寄せられたため、「ISMS クラウドセキュリティ認証」の制度を 2016 年 8 月に開始しました。

ISMS クラウドセキュリティ認証は、ISO/IEC 27001 を前提として、ISO/IEC 27017 に沿ったクラウドサービス固有のセキュリティ対策を実施していることを認証する仕組みです。ISO/IEC 27001 を前提としていることから、ISMS クラウドセキュリティ認証を希望する組織は ISMS 認証の取得が必要となります。認証を行うためには要求事項が必要になりますが、ISO/IEC 27017 はガイドライン規格であるため、認証基準には適用できません。そこで、JIPDEC では ISO/IEC 27017 の管理策を ISO/IEC 27001 に取り込むための認証基準として JIP-ISMS517-1.0 を策定しました。

ISMS クラウドセキュリティ認証の認証基準

JIP-ISMS517-1.0「ISO/IEC 27017:2015 に基づく ISMS クラウドセキュリティ認証に関する要求事項」※1

「ISMS クラウドセキュリティ認証」の対象者は、クラウドサービスの提供者（クラウドサービスプロバイダ）またはクラウドサービスの利用者（クラウドサービスカスタマ）のいずれか、あるいはその両方の立場である組織になります。ISMS クラウドセキュリティ認証の被認証組織は、一般社団法人情報マネジメントシステム認定センター（ISMS-AC）の Web サイトで公開されており、2023 年 4 月現在 417 の組織が認証を取得しています※2。

ISO/IEC 27017 については、現在改訂作業が行われており、ISO/IEC 27002:2022 への対応等が予定されています。ISO/IEC 27000 ファミリー規格の改訂状況については、セキュリティマネジメント推進室が「国際動向」※3 のページで定期的に公開しています。

最後に、ISMS クラウドセキュリティ認証は、ここ 1 年で被認証組織が 100 件以上増加しており、クラウドサービス利用が増加している状況を考えると、今後、さらに被認証組織が増加し、取引要件等で活用されることを期待します。

※1　ISO/IEC 27017:2015 に基づく ISMS クラウドセキュリティ認証に関する要求事項
https://www.jipdec.or.jp/archives/publications/JIP-ISMS517-10.pdf
※2　ISMS クラウドセキュリティ認証　被認証組織　https://isms.jp/isms-cls/lst/ind/index.html
※3　国際動向　https://www.jipdec.or.jp/project/smpo/kokusai.html

7 電子契約関連、DX 推進

コロナ禍により電子契約の普及が進み、さらに2022年に電子帳簿保存法が改訂され、2023年にはインボイス制度が導入されることとなった。このような環境変化について対応状況を調査した。またDXの推進状況についても調査を実施した。

7-1. 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、今回調査で初めて「請求処理」（44.0％）がトップとなった。次いで、「経費精算（交際費）」（43.8％）、「経費精算（旅費・交通費）」（42.9％）と続いた。（図27）

過去２年の調査と比べ大きく変化が見られたのは、「経費精算（交際費）」で、2021年調査の30.3％から今回は43.8％と、２年で約14ポイントの増加がみられた。

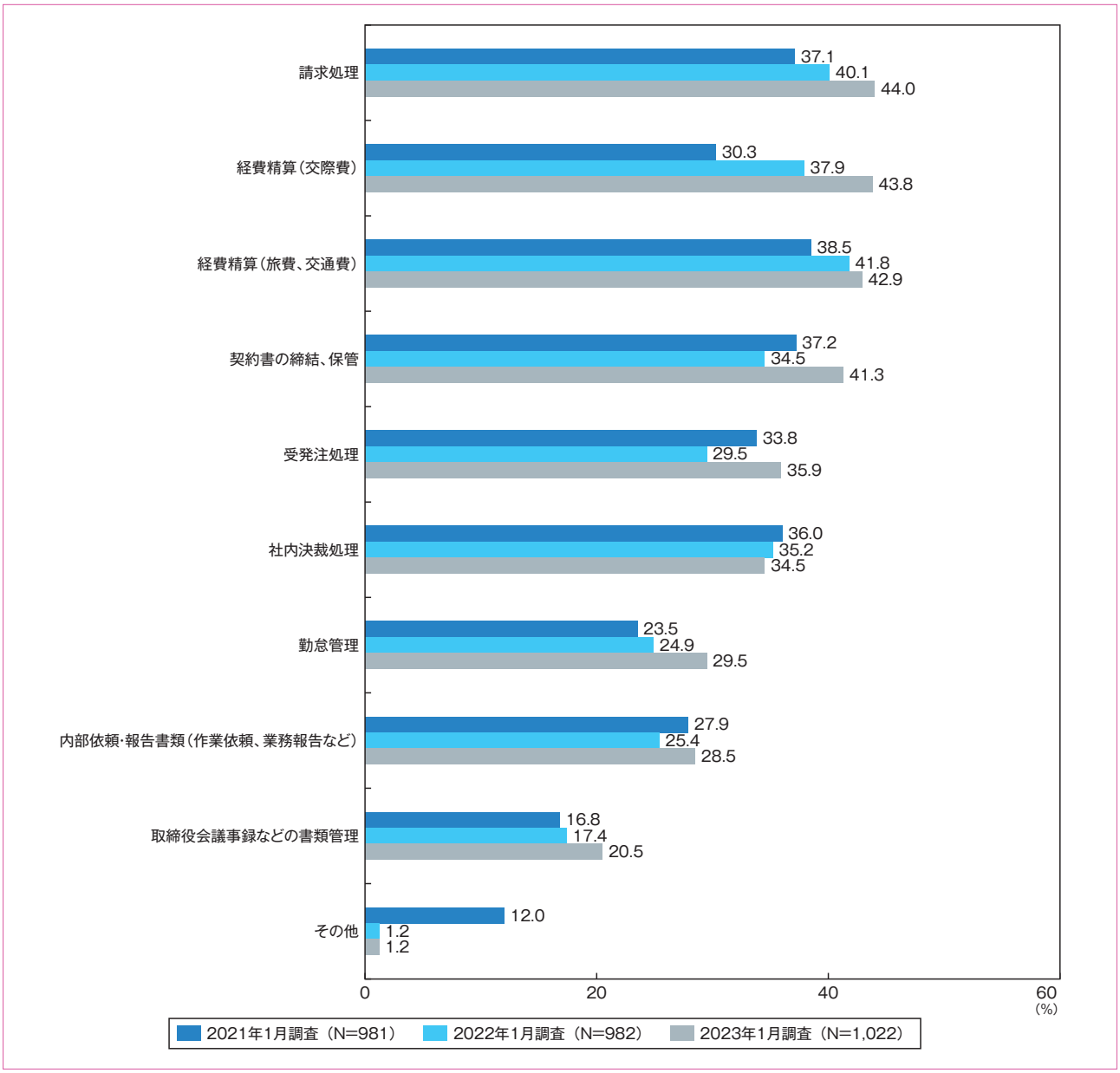


図27. 電子化したい業務プロセス

7-2. 電子帳簿保存法の保存要件への対応

2022年１月に改正された電子帳簿保存法の保存要件への対応方法として、「授受後のタイムスタンプ」（35.7%）がトップで、「訂正削除不可システムでの保存」（16.5%）、「社内規程での運用」（16.4%）が続いた。（図28）

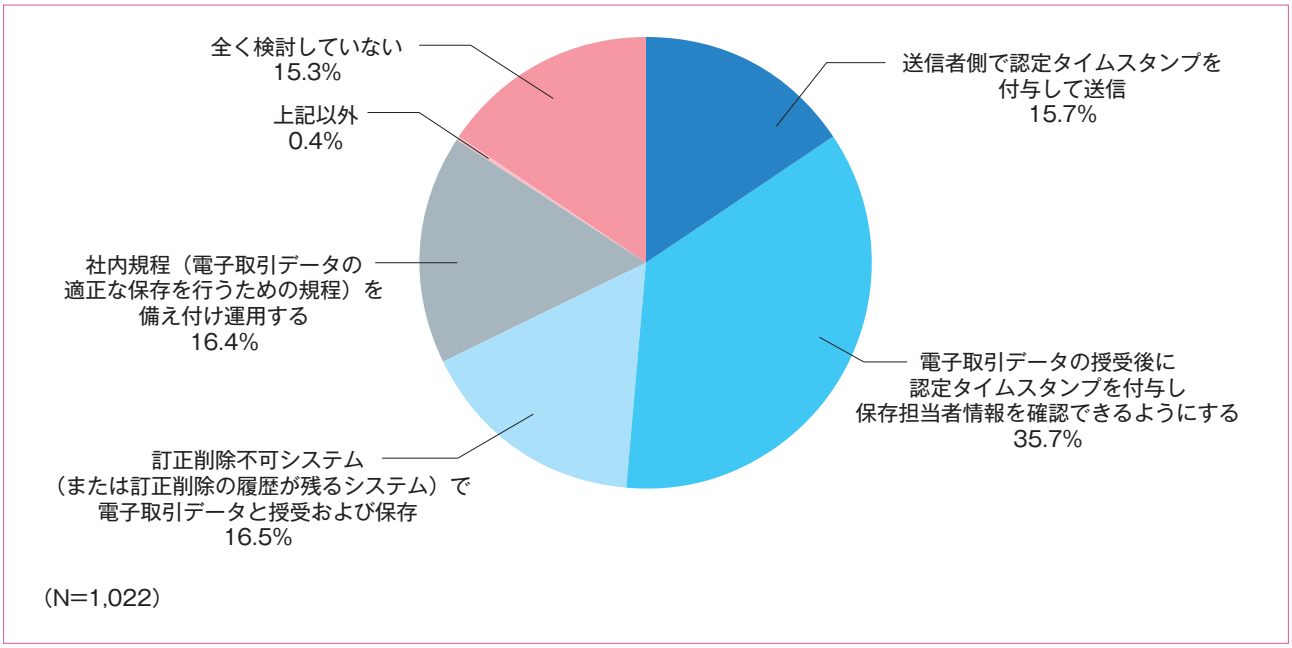


図28. 電子帳簿保存法の保存要件への対応

7-3. インボイス制度の登録申請書の提出状況

2023年10月から導入されるインボイス制度に対応するため、適格請求書発行事業者として「登録申請書を提出し、すでに登録番号の通知を受けている」のは34.3％となった。さらに「提出済みで登録処理中」（31.3%）、「今後提出予定」（23.0%）まで含めると、約９割が「対応中」または「対応予定」となった。（図29）

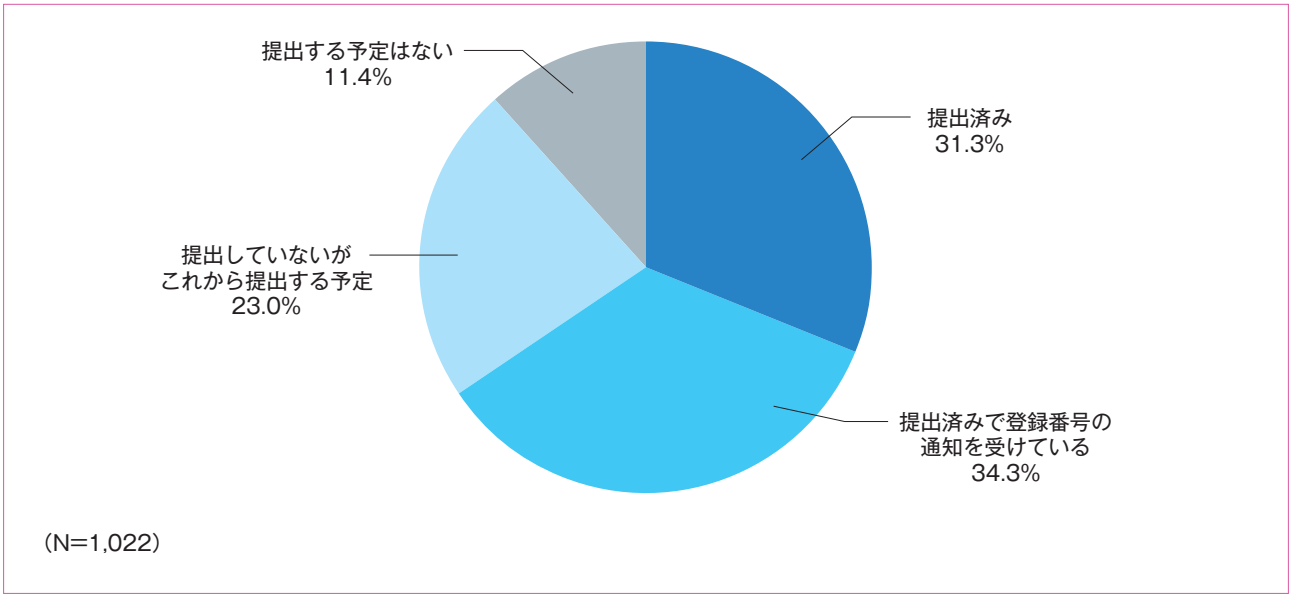


図29. インボイス制度の登録申請書の提出状況

7-4. インボイス制度の登録申請書を提出しない理由

一方、インボイス制度の登録申請書を提出していない理由としては、「義務ではない」が84.5％で圧倒的に多く、「免税事業者」が13.8％となった。（図30）

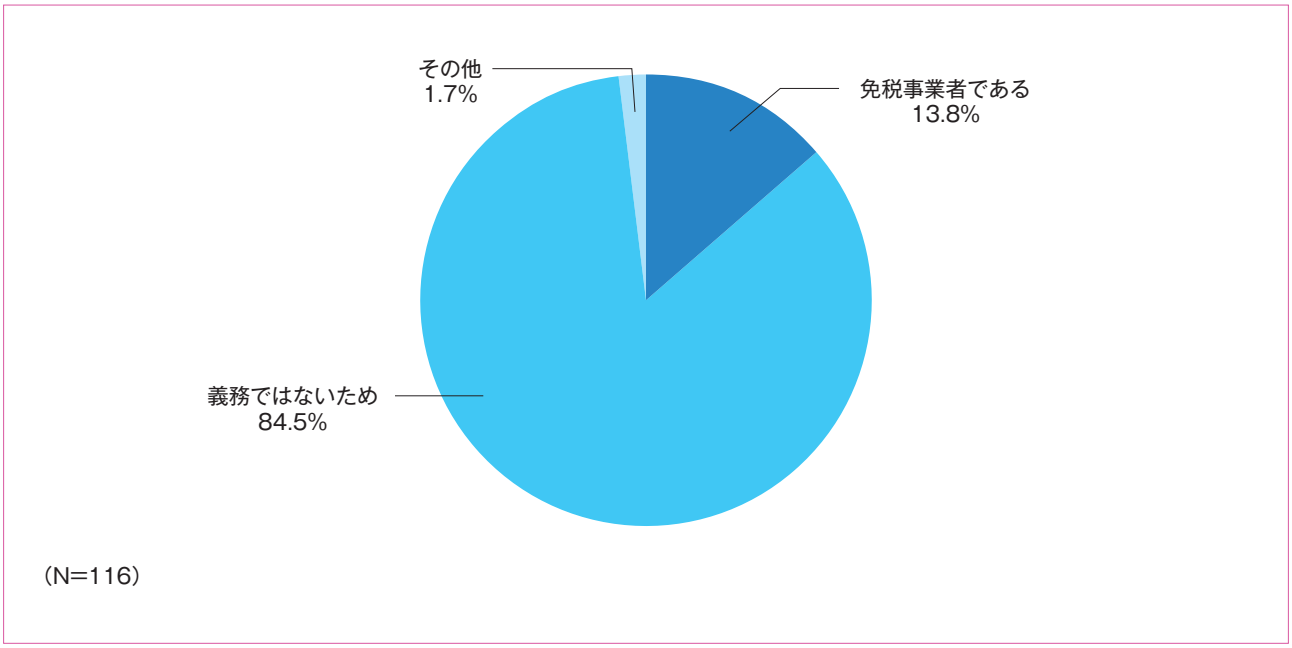


図30. インボイス制度の登録申請書を提出しない理由

7-5. インボイスの作成・発行の検討状況

インボイスの検討状況では、「電子インボイスで検討中」（41.3％）がトップで、「書面インボイスで検討中」（28.5％）、「検討する予定」（20.5％）を含めると約９割が「検討」または「検討予定」となった。（図31）

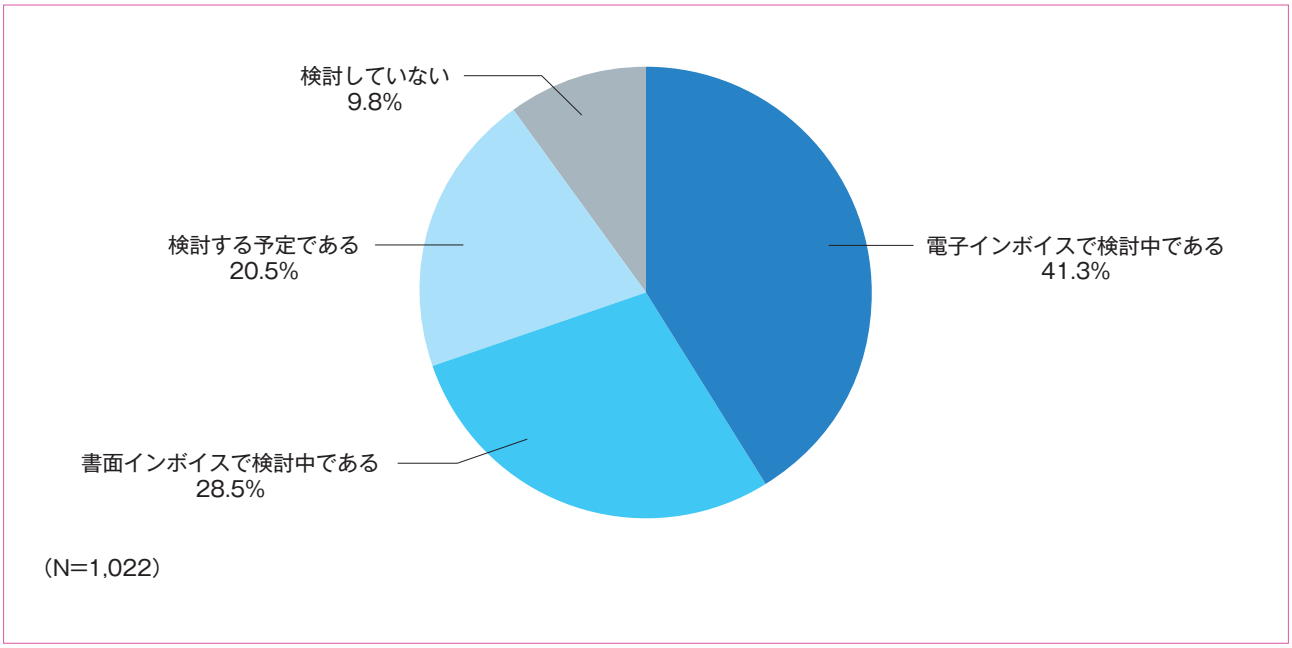


図31. インボイスの作成・発行の検討状況

7-6. 電子インボイスの発行方法

「電子インボイスを検討中」と回答した事業者による電子インボイスの発行方法としては、「メールに添付して送信」（41.5%）がトップで、「クラウドで請求書等のデータを発行」（40.5%）が続いた。（図32）

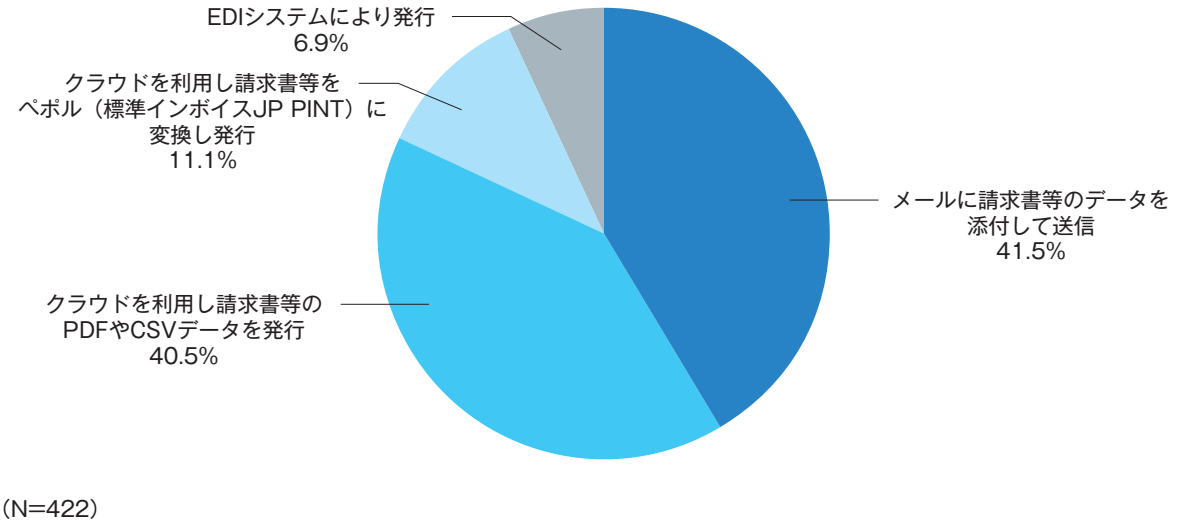


図32. 電子インボイスの発行方法

7-7. 電子契約の利用状況

電子契約の利用状況では、「採用している」比率が毎回増加しており、今年は73.9％に達した。内訳では「当事者型」が25.8％と最も多い。（図33）

従業員規模別にみると、50人未満の小規模事業者では、電子署名付きかは不明ながらも何らかの電子契約を「利用している」割合は約５割だったのに対し、50人以上の事業者は、８割近くが利用しており、さらに、「利用に向けて準備・検討中」を合わせれば９割が近い将来、電子契約を活用することとなる。（図34）

業種別にみると、「情報通信」「金融・保険業」「製造業」の利用割合が高いのに対し、「サービス業」「卸売・小売業」での利用率は低い。なお、形態としては、契約当事者の電子署名を用いた「当事者型」の方がいずれの業種でも利用率が高い。（図35）

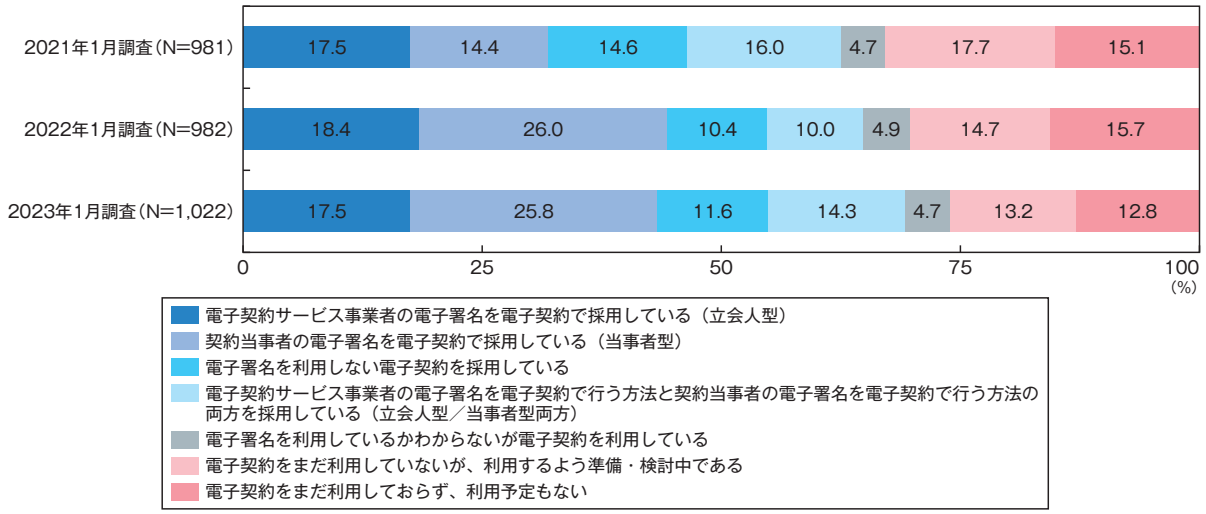


図33. 電子契約の利用状況

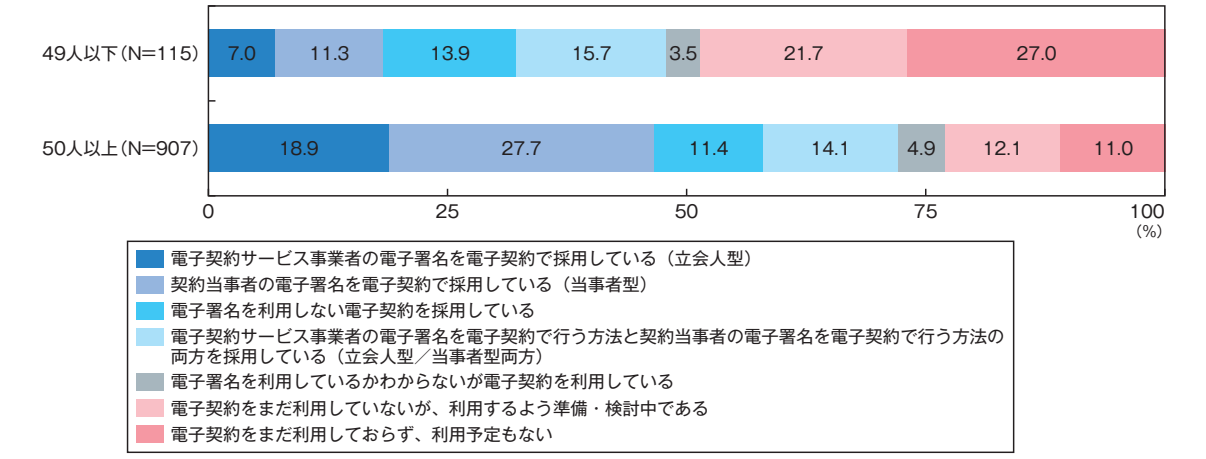


図34. 電子契約の利用状況（従業員規模別）

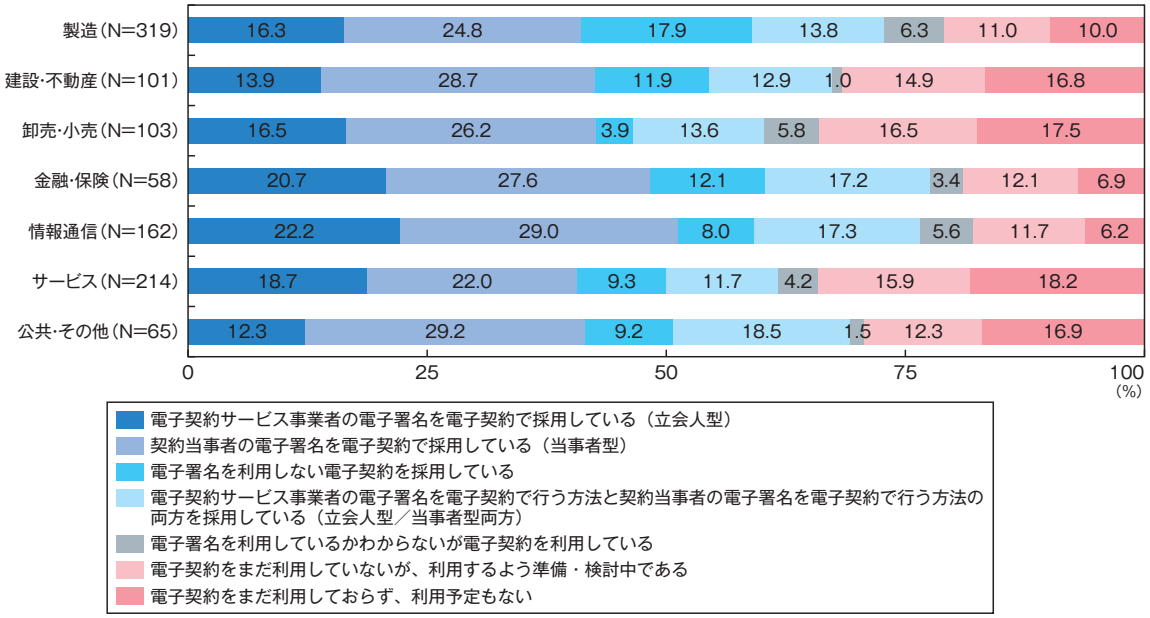


図35.　電子契約の利用状況（業種別）

7-8.　電子契約導入の目的

何らかの形で電子契約を利用している事業者の回答では、導入目的として、「業務の効率化」が最も高く46.2%。次いで、「文書の電子化」（19.6%）、「コスト削減」（17.6%）と続いた。（図36）

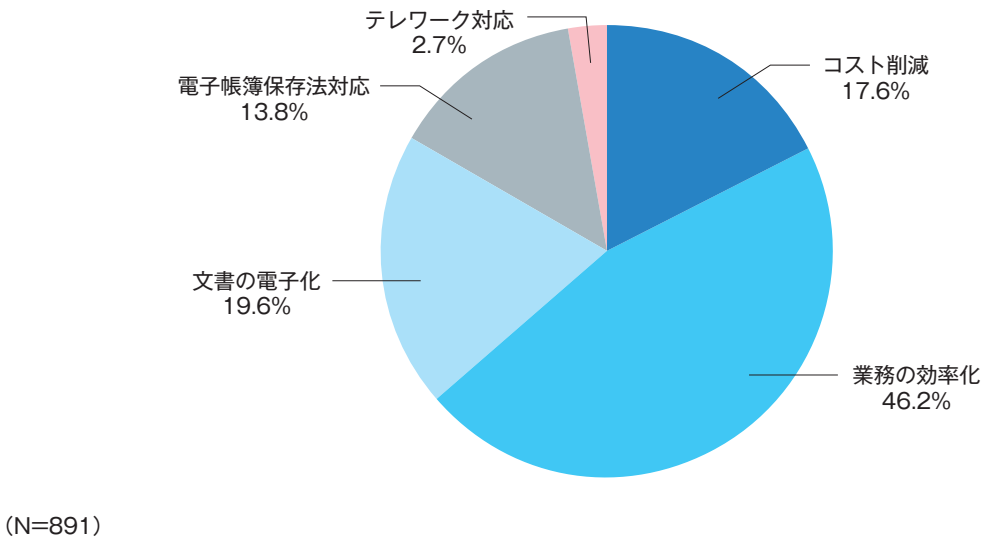


図36.　電子契約導入の目的

7-9. 電子契約を選定する際に重視するポイント

電子契約を選定する際に重視するポイントは、前回調査同様、「サービスのコスト」（48.6%）がトップとなった。次いで、「セキュリティに関する第三者認証・認定を受けていること」（41.5%）、「セキュリティ対策」（29.0%）、「サポート体制」（28.7%）が続いた。（図37）

前回調査と比べて特に差が見られたのは、「第三者認証・認定を受けていること」が35.0%から41.5%へと6.5ポイント、「電子証明書による電子署名機能があること」が6.3ポイント増加した点である。

今後、電子契約サービス利用にあたり、文書の真正性を確保する電子署名やサービス事業者の運用体制等について、第三者認証制度等のお墨付きがあることが、さらにサービス選定の重要ポイントとなることが予想される。

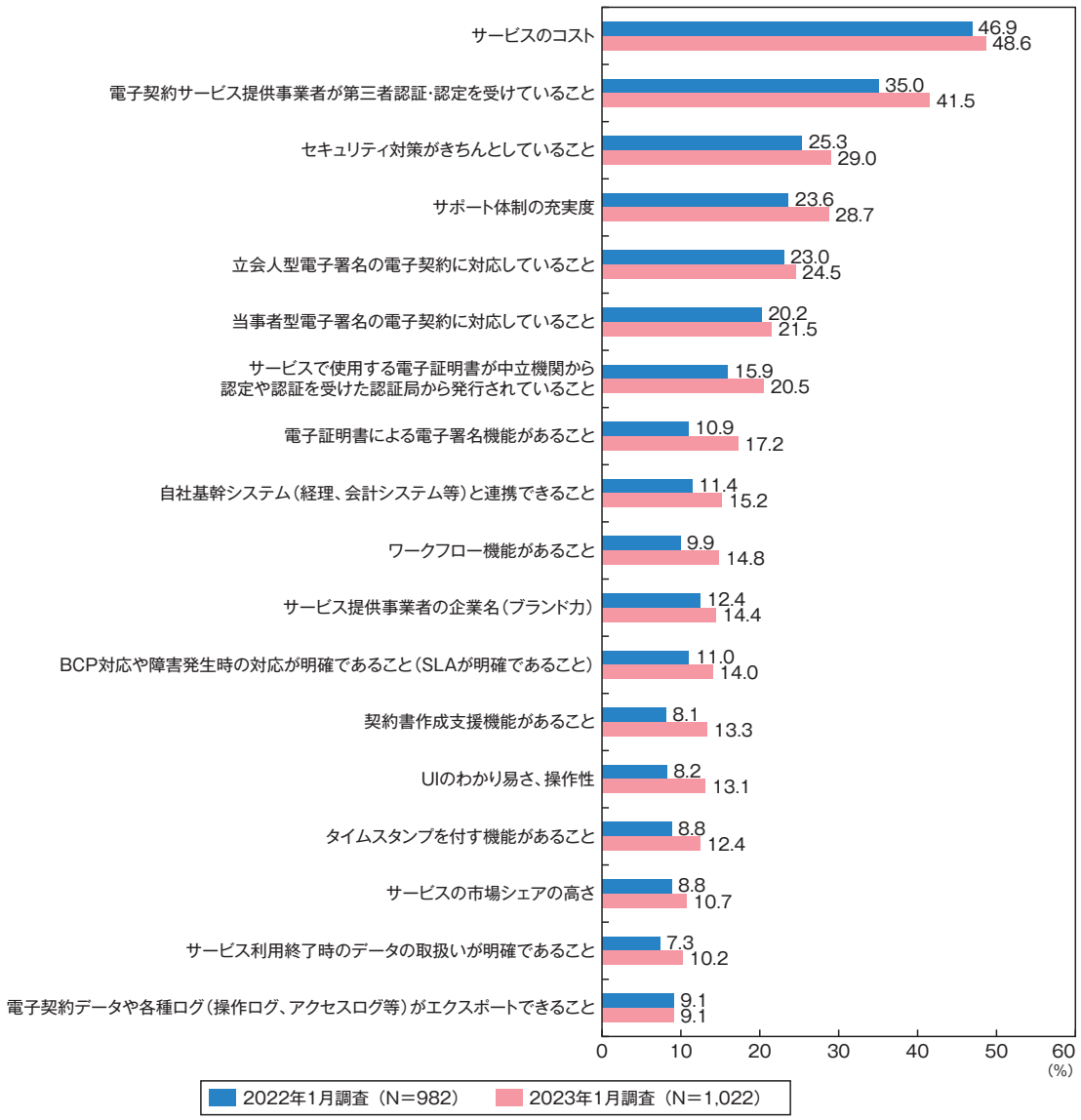


図37. 電子契約を選定する際に重視するポイント

7-10. 電子契約サービス事業者を選定する場合の第三者認証

電子契約サービス事業者を選定する際、どのような第三者認証を参考にするかを聞いたところ、「クラウドに関するセキュリティ認証」取得の有無を参考にするとの回答が半数近くの44.6％を占めた。（図38）

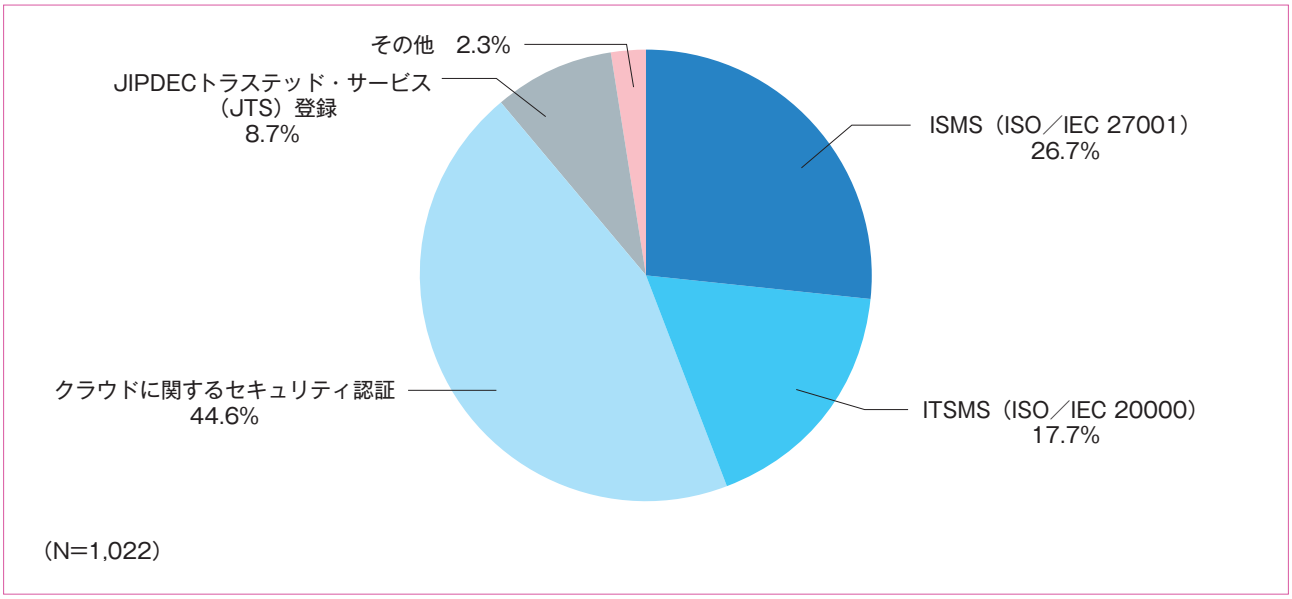


図38. 電子契約サービス事業者を選定する場合の第三者認証

【コラム】電子契約サービスにおける第三者認証の重要性

JIPDEC　デジタルトラスト評価センター　小林 拓矢

電子契約の利用状況は、取引文書に関する電子契約の導入企業が７割以上となり、年々と増えています。

本調査結果として、電子契約サービスが導入されているタイプは、電子契約サービス事業者の電子証明書で、契約書に電子署名を行う“立会人型”と、契約当事者が所有する電子証明書を用いて契約書に電子署名を行う“当事者型”が約６割を占めていることから、電子署名の技術が用いられた電子契約サービスを選択している傾向があります。

また、信頼性のある電子契約サービスを選択する場合の基準として、第三者認証の有無を重視する企業が増加していることが本調査結果より読み取れます。「クラウドに関するセキュリティ認証」が 44.6％で１番であり、その次に、「ISMS（ISO/IEC27001）」が 26.7％と「ITSMS（ISO/IEC20000）が 17.7％であり、４番目に当協会が運営する「JIPDEC トラステッド・サービス登録（JTS 登録）」が 8.7％となっています。

第三者認証の有無が重視される背景として、昨今、電子契約サービスが続々と提供されている中、電子証明書による電子署名の技術が用いられたセキュリティ対策やサポート体制が充実していても、ユーザーにとっては安心・安全なサービスなのかを判断することが非常に難しくなっている点が挙げられます。

第三者認証の一例として、「電子契約サービス」等を対象とした、JTS 登録があります。

JTS 登録とは、電子契約サービス等に用いられる電子証明書の発行、失効を行う「認証局」や、その認証局の代わりに利用者の意思確認や本人確認による電子証明書の発行処理および失効処理を行う「電子証明書取扱業務」「電子契約サービス」や「リモート署名」の機能について、JIPDEC が適合性評価機関として厳格な審査を行う第三者評価制度です。

JTS 登録の審査は、JIPDEC が定める審査基準のもと、登録対象サービスの運用状況やセキュリティ対策、設備等について、書類審査と現地審査を実施しています。

特に、金融機関が提供している電子契約サービスで用いられる電子証明書の信頼性について、JTS 登録（電子証明書取扱業務）として厳格な審査を行っています。2023 年４月現在、金融機関の登録状況を本店所在地の場所に置き換えて集計した結果、47 都道府県のうち 19 都道府県（シェア４割）の登録が確認できました。

電子契約サービス事業者は、サービスの機能について、JTS 登録における必要な審査を受けることで、対外的にトラストサービスであることを公表することができます。一方で、電子契約サービスの導入を検討する企業においては、トラストサービスを選択する指標になるのではないでしょうか。

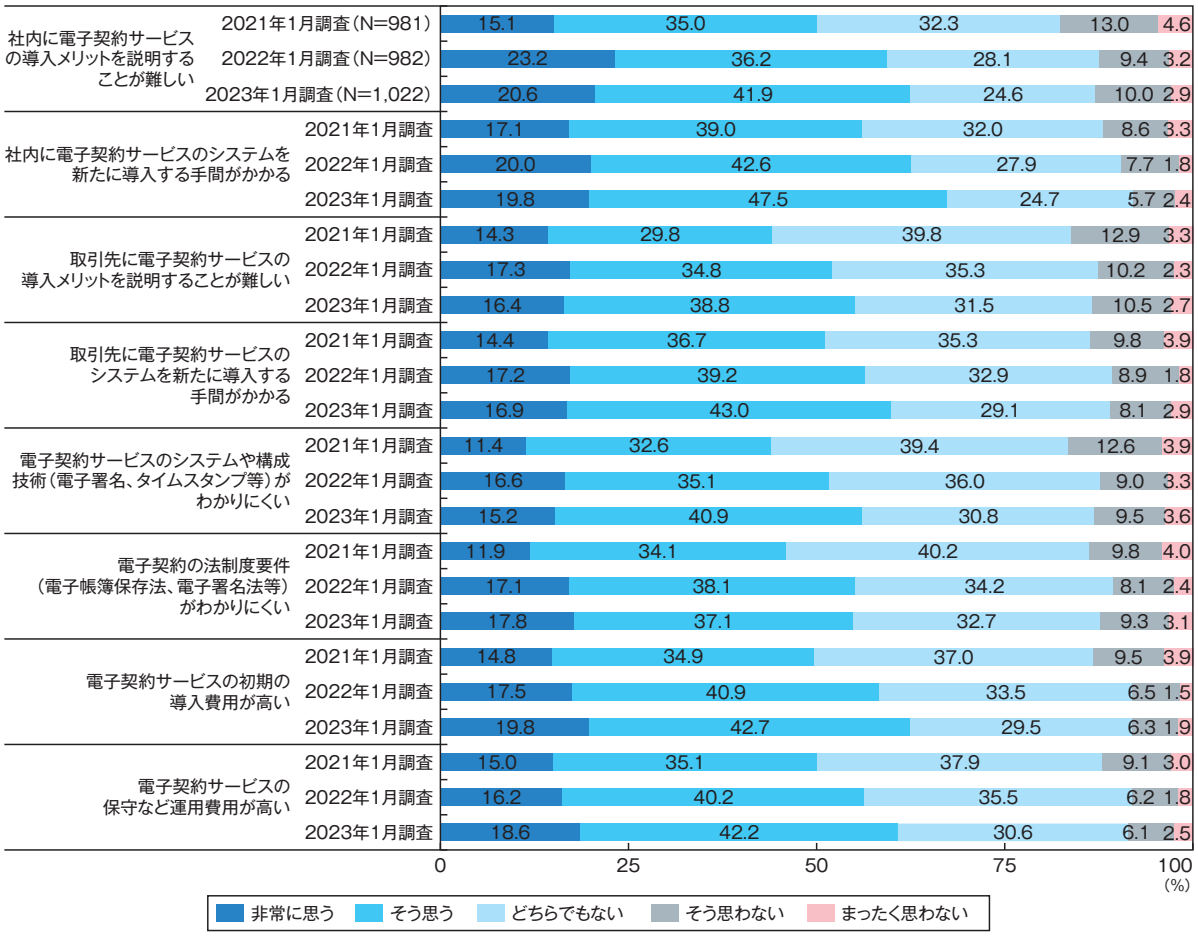
JIPDEC としては、デジタル社会において、第三者認証は重要であると考えており、トラストサービスであることを証明するための大きな役割を持っていると考えています。多くの皆さんが、安心・安全なサービスを利用できるよう、デジタルトラストの縁の下の力持ちとして引き続き活動してまいります。

JIPDEC Trusted Service Registration

7-11. 電子契約の利用拡大を図る上での課題

電子契約の利用拡大を図る上で、特に課題として捉えている割合が高いのが「社内の導入の手間がかかる」（67.3%）で、次いで、「導入のメリットの説明が難しい」（62.5%）、「初期導入コストが高い」（62.5%）が続いた。（図39）

過去２回の調査と比較しても、電子契約の利用機会が増えていくのに合わせ、今回取り上げた内容を課題として意識する割合が徐々に高くなっているのがわかる。



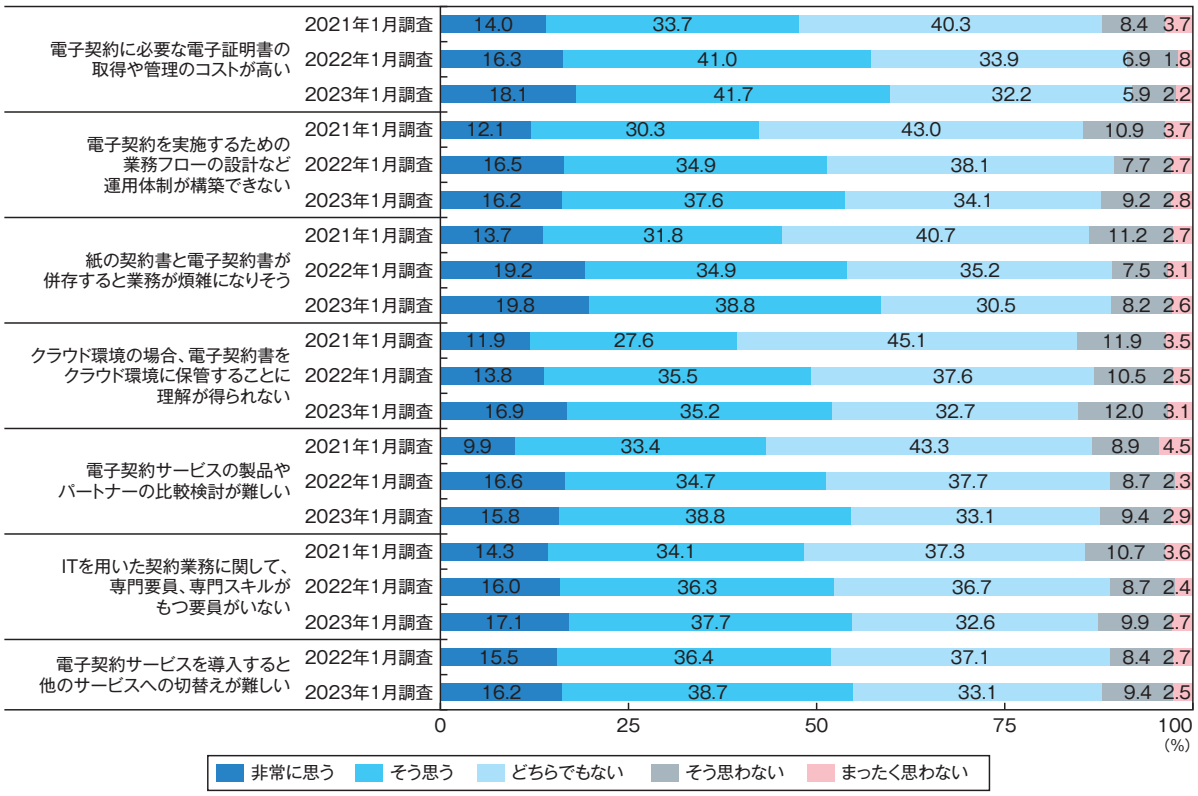


図39. 電子契約の利用拡大を図る上での課題

7-12. デジタルトランスフォーメーション（DX）の目的

DXの目的としては、「コスト削減」（60.7%）が最も多く、「労働時間の短縮」（46.6%）、「人員削減」（38.4%）が続き、事業拡大というよりも事業の効率化の方が多い。（図40）

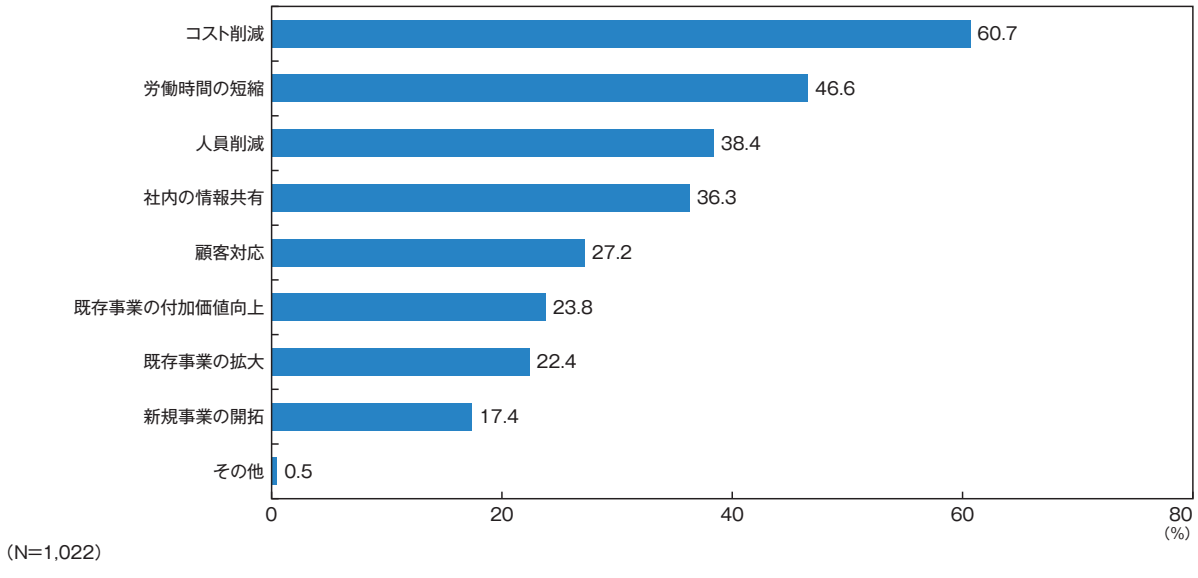


図40. デジタルトランスフォーメーション（DX）の目的

【コラム】「デジタルトランスフォーメーション（DX）の目的」に対する結果から見るDXへの取組みの動向

JIPDEC　電子情報利活用研究部　調査研究グループ　グループリーダ　松下 尚史

経済産業省が 2022 年９月に改訂版を発行したデジタルガバナンス・コード 2.0 では、「企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること。」となっています。また、DX レポート２（中間とりまとめ）※1 では、経営者・IT 部門・業務部門が協調して共通認識を形成した上で、「顧客や社会の問題の発見と解決による新たな価値の創出」と、「組織内の業務生産性向上や働き方の変革」という２つのアプローチを同時並行に進めることが重要であると示し、DX をデジタイゼーション（アナログ・物理データの単純なデジタルデータ化）、デジタライゼーション（個別業務・プロセスのデジタル化）、デジタルトランスフォーメーション（全社的な業務・プロセスのデジタル化、および顧客起点の価値創造のために事業やビジネスモデルを変革すること）という３つの異なる段階に分解し、整理しています。

今回実施した調査の結果（図 40）を見ると、デジタルガバナンス・コード 2.0 や DX レポートに記載されている“競争上の優位性を確立すること”、“新たな価値の創出”、“顧客起点の価値創造”に該当しそうな回答は「既存事業の付加価値向上（23.8％）」「既存事業の拡大（22.4％）」「新規事業の開拓（17.4％）」という回答結果になっており、取組みの目的としては少数派という結果となりました。回答結果の上位３つは「コスト削減（60.7％）」「労働時間の短縮（46.6％）」「人員削減（38.4％）」となっていますが、この３つの項目を商品の販売価格を下げることによる顧客への価値提供と考えるのであれば、“新たな価値創造”と言うことは難しくても、“競争上の優位性を確立すること”や“顧客起点の価値創造”と捉えることは難しくはありません。ただ、このような既存の製品・サービス等の販売価格を下げるための人員削減・労働時間の短縮・コスト削減は、無駄がない業務最適化を実現することであり、既存事業の枠組み内でデジタル技術を用いて業務最適化を図る取組みは、IPA の DX 実践手引書 IT システム構築編（完成第 1.0 版）において、DX ではなくデジタルオプティマイゼーション※2 であるとされており、デジタルオプティマイゼーションは DX に至る前段階として設定されていることから、DX を実現するための過渡期と考えることもできます。

また、DX であってもデジタルオプティマイゼーションであっても人や予算を投じて取組みを進めることから、成果をステークホルダーに報告するために、KGI や KPI を設けて、効果検証を行う必要があります。DX 白書 2023※3 によると、米国企業の場合は、「売上が増加した」「コストが下がった」と回答した企業はすべての職種で６割以上になっているのに対し、日本企業の約半数は、そもそも「成果を測定していない」と回答しています。

DX は単なるデジタル化ではなく、“競争上の優位性を確立すること”、“新たな価値の創出”、“顧客起点の価値創造”を伴うものであることを意識しつつ、DX を推進していくことが日本経済を失われた 30 年から脱却させることにつながるのではないでしょうか。

※１　経済産業省「デジタルガバナンス・コード 2.0」（2022 年９月）
https://www.meti.go.jp/policy/it_policy/investment/dgc/dgc2.pdf

※２　独立行政法人情報処理推進機構（IPA）が 2023 年３月に公表した「DX 実践手引書 IT システム構築編（完成第 1.0 版）」では、デジタルオプティマイゼーションを既存事業の枠組み内での変革、デジタルトランスフォーメーションを既存事業の枠組みを超えた変革として整理している。
https://www.ipa.go.jp/files/000094497.pdf

※３　IPA「DX 白書 2023」（2023 年３月）
https://www.ipa.go.jp/files/000108041.pdf

7-13. DXを推進するにあたっての課題

DX推進にあたっての企業の課題としては、「体制構築が難しい（人材不足）」（41.7%）が最も多く、次いで「規程整備が難しい」（35.4%）、「業務の洗出しが難しい」（35.4%）が続いた。（図41）

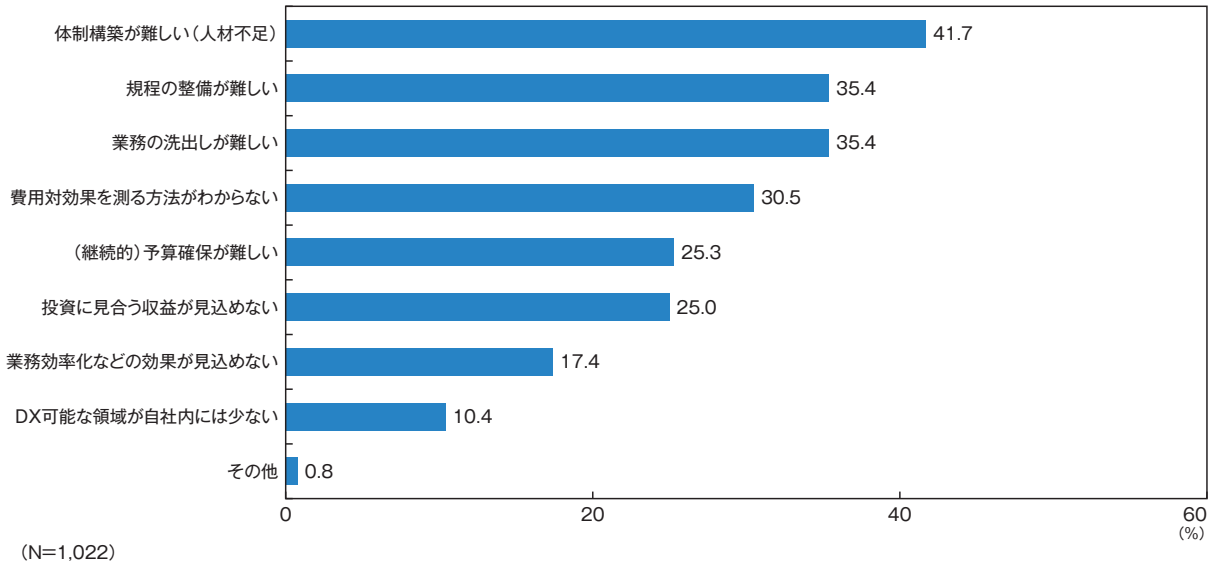


図41. DX推進上の課題

7-14. DX取組みについての課題

DX取組みにあたっての企業課題としては「体制構築が難しい」（50.8%）、「効果が得られるかわからない」（38.9%）、「予算確保が難しい」（38.1%）が主な課題と言える。（図42）

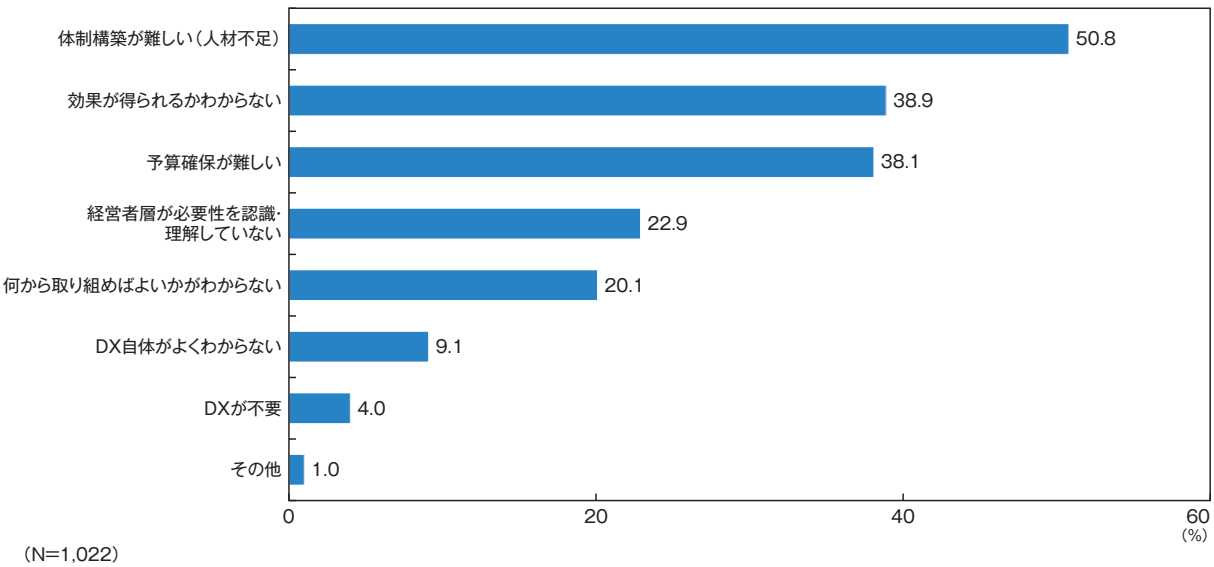


図42. DXへの取組みについての課題

7-15. テレワークの導入状況

テレワークの導入状況について、「全面的に導入中」（14.3%）、「出社とテレワークを併用」（38.4%）、「導入しているが、今後継続するか検討中」（19.4%）を合わせると、調査時点でテレワークを導入している割合は７割を超えている。

ただし、新型コロナの収束状況や政府の行動制限緩和に伴い、すでに導入を中止した企業も出てきており、今後テレワークの導入状況も変わっていく可能性がある。（図43）

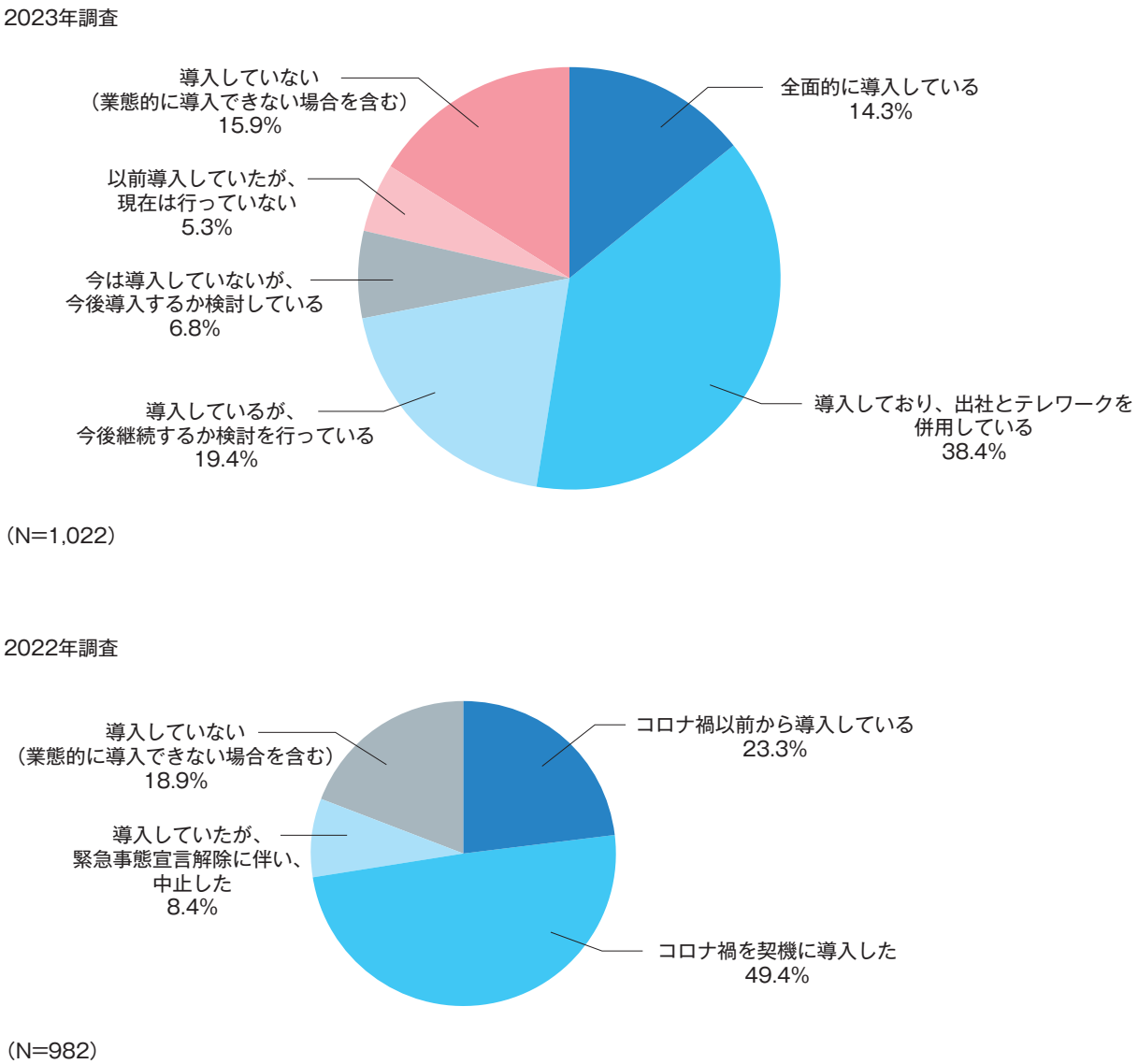


図43. テレワークの導入状況

8 総評

「企業IT利活用調査2023」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17,000社を対象に調査を行った（回答数：1,022社）。

コロナ禍も４年目を迎え、企業はハイブリッドワークとクラウド利用を中心とした柔軟なワークスタイルを確立しつつある。一方、DX（デジタルトランスフォーメーション）への取組みや、電子帳簿保存法の改正、電子契約の普及、今年秋のインボイス制度の導入など、業務の進め方も変わってきている。

情報セキュリティインシデントは「マルウェア感染」と「従業員によるデータ・情報の紛失・盗難」が依然多く、外部からの攻撃と内部からの情報漏えいと両方のリスクを抱えている。企業のセキュリティ対策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ような境界防御型のツールから、ゼロトラスト型に対応したSWG・CASBやEDRのような次世代型のセキュリティサービスへ移りつつある。サイバー攻撃は日々巧妙化・複雑化してきており、脆弱性診断やCSPMのようなクラウドサービスの診断サービスも増加してきており、今後クラウド環境を前提とした次世代型セキュリティアーキテクチャへの移行が加速していくことが予測される。

個人情報保護関連では、2022年４月に改正個人情報保護法が施行され、海外ではEUのGDPRや中国サイバーセキュリティ法を参考に各国でプライバシー法規制が施行されてきている。それを受けて企業ではプライバシーソリューション／テックの導入が進みつつある。

柔軟なデジタルワークスタイルでは、電子契約が普及し、電子インボイスへの準備も進んでいる。DXについてはコスト削減や効率化を中心に成果を生みつつあるが、今後、既存事業拡大や新規事業拡大に向けて取り組むことが期待される。

回答者プロフィール

業種	回答数	%
製造	319	31.2
建設・不動産	101	9.9
卸売・小売	103	10.1
金融・保険	58	5.7
情報通信	162	15.9
サービス	214	20.9
公共・その他	65	6.4
全体	1,022	100.0

従業員規模	回答数	%
5,000人以上	199	19.5
1,000～4,999人	196	19.2
300～999人	222	21.7
50～299人	290	28.4
50人未満	115	11.3
全体	1,022	100.0

資本金規模	回答数	%
5,000億円以上	156	15.3
3,000億～5,000億円未満	52	5.1
1,000億～3,000億円未満	70	6.8
500億～1,000億円未満	77	7.5
100億～500億円未満	180	17.6
10億～100億円未満	265	25.9
1億～10億円未満	187	18.3
1,000万円～1億円未満	29	2.8
1,000万円未満	6	0.6
全体	1,022	100.0

業種別内訳		回答数	%
製造	食品・飲料	35	3.4
	日用品・生活雑貨	13	1.3
	繊維	12	1.2
	パルプ・紙・印刷	16	1.6
	化学工業	22	2.2
	石油製品	2	0.2
	鉄鋼・金属	21	2.1
	プラスチック・ゴム	11	1.1
	機械	30	2.9
	電気機器	38	3.7
	情報通信機器	18	1.8
	電子部品・電子回路	21	2.1
	精密機器	26	2.5
	自動車・輸送機器	27	2.6
	医薬品	11	1.1
	その他の製造業	16	1.6
建設・不動産	建設	53	5.2
	不動産	42	4.1
	住宅	6	0.6
卸売・商社	卸売	28	2.7
	小売	52	5.1
	商社	23	2.3
金融・保険	銀行	36	3.5
	証券	6	0.6
	生命保険	6	0.6
	損害保険	3	0.3
	その他金融	7	0.7

業種別内訳		回答数	%
情報通信	通信	24	2.3
	ITベンダー／システムインテグレータ	101	9.9
	インターネットサービス	26	2.5
	情報システム子会社	11	1.1
サービス	電力・ガス・水道	17	1.7
	運輸	31	3.0
	倉庫	4	0.4
	宿泊	6	0.6
	飲食	10	1.0
	娯楽・レジャー	11	1.1
	メディア・出版・放送・広告	6	0.6
	生活関連サービス（旅行業など）	11	1.1
	医療	26	2.5
	福祉・介護	30	2.9
	教育（学校以外）	18	1.8
	人材派遣・業務委託	13	1.3
	その他サービス	31	3.0
公共・その他	学校	14	1.4
	官公庁	12	1.2
	地方自治体	19	1.9
	農業・水産・鉱業	3	0.3
	その他の業種	10	1.0
	その他公共機関	7	0.7
	全体	1,022	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	359	35.1
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	514	50.3
セキュリティ製品の導入、製品選定に関与している	518	50.7
セキュリティ対策の実務に関与している	326	31.9
全体	1,022	100.0

〈資料〉情報化に関する動向（2022年10月～2023年３月）

国　内	海外／国際連携
2022年10月	
・政府、「特定デジタルプラットフォームの透明性及び公正性の向上に関する法律」に基づき、世界初のデジタル広告規制。Google、Meta、Yahoo Japanを規制対象に。取引条件変更時の事前通知、政府への報告書提出等義務付け。 ・個人情報保護委員会（PPC）、事業者が保有データの管理を可視化できるデータマッピング・ツールキット公表。 ・凸版印刷と情報通信研究機構（NICT）、耐量子計算機暗号搭載のICカード開発。2025年の実用化に向け、医療従事者のICカード認証と電子カルテのアクセス制御に適用し、有効性確認。	・欧州連合（EU）理事会、オンライン上のユーザーの安全性向上に向け、仲介サービス事業者を規制する「デジタルサービス法（DSA）」を最終承認。2024年２月に全面施行へ。 ・米科学技術政策局、米国民をAIから派生する害や差別から守るための「AI権利章典」発表。 ・Google、アリゾナ州が2020年に起こした位置情報の追跡訴訟で和解。8,500万ドルの和解金支払い。 ・バイデン大統領、米EU間のデータ移転ルールで大統領令署名。2022年３月の基本合意を受け、米側の具体的な取組み明示。 ・欧州データ保護委員会（EDPB）、GDPR準拠を認証する「Europrivacy」を欧州データ保護シールとして承認。EU以外の個人情報保護法にも適用可能。 ・米テキサス州、Googleが同意なしに州民の生体認証データを収集したとして提訴。 ・英消費者団体、Amazonの販売方法が独占禁止法に抵触するとして、９億ポンドの提訴。 ・Microsoft、クラウド用ストレージサービスの設定ミスで顧客の機密データ公開。111カ国65,000企業に影響。 ・Eron Musk氏、総額440億ドルでTwitter社買収完了。

国　内	海外／国際連携
2022年11月	
・PPC、破産者の個人情報をサイト公開するのは個人情報保護法違反として、事業者にデータの削除命令。 ・政府、新型コロナウイルス接触確認アプリCOCOAの機能停止。	・NTTデータスペイン、顧客情報漏えいでGDPR違反・6.4万ユーロの制裁金。日本の海外子会社で初の処分。 ・Google、全米40州から位置情報を不適切に収集していたとする訴訟で、計3.9億ドルの制裁金支払いで和解。 ・イタリアデータ保護局（GPDP）、レッチェ市による顔認識技術の利用提供システムの実験導入の発言を受け、司法捜査、犯罪抑止目的外での顔認識システム設置・利用は不許可と表明。 ・米連邦取引委員会（FTC）、不公正な競争方法を禁止するFTC法の執行強化方針を発表。 ・FTCと米７州、Googleスマホの虚偽広告問題で、Google、ラジオ局運営会社と和解。940万ドルの制裁金。 ・アイルランドデータ保護委員会（DPC）、Facebook他で5.3億人の個人情報の流出について、GDPR違反でMetaに2.65万ユーロの制裁金。 ・韓国とEU、デジタルパートナーシップ署名。インフラ、セキュリティなど11項目について優先的に協力・推進。

国　内	海外／国際連携
2022年12月	
・NTTドコモ、西日本地域で２回の通信障害。電気通信事業法上で「重大な事故」にあたる約310万人に影響。	・米シークレットサービス社、米の新型コロナウイルス救済資金数千万ドルが中国ハッカー集団に窃取されたと発表。 ・EDPB、Metaのパーソナライズド広告表示の同意強要をEUの個人情報保護法が許容していないと判断。 ・米サウスダコタ州、州機関でのTikTok使用を一部禁止。これを契機に米政府も禁止の動き。 ・中国政府、ネット大手を規制する不正競争防止法改正案公表。 ・欧州司法裁判所、誤情報の検索結果削除をGoogleに求めた訴訟で、誤情報が明らかな場合、削除が必要と判断。 ・欧州委員会（EC）、EU米データプライバシー枠組みの十分性認定の決定案発表。正式採択に向け手続き開始。 ・Epic Games、保護者の同意なく児童のデータを収集し、意図しない課金を行ったとして、児童プライバシー法違反で5.2億ドルの罰金と、ユーザーをだましたとして2.4億ドルの払戻しが確定。 ・EC、Amazonが反トラスト法違反調査で指摘された非マーケットプレイス販売者データの使用と、ショッピングカートボックス等の利用を許可する取組みを許容し、和解。制裁金支払い回避。 ・Meta、2018年のCambridge Analytica事件後の集団訴訟で和解。和解金は7.25億ドル。 ・米連邦控訴裁、Googleに対する保護者非同意での13歳未満のYouTube閲覧履歴収集の裁判で、児童オンラインプライバシー法（COPPA）が州法より優先すると訴えを棄却した連邦地裁の判断を覆し、訴訟を容認。裁判再開へ。

国　内	海外／国際連携
2023年１月	
・アフラック生命保険とチューリッヒ保険、外部委託先のサーバー不正アクセスで、それぞれ130万人、75万人の個人情報流出。 ・PPC、破産者の個人情報をサイト上で違法に公開している事業者を個人情報保護法違反で捜査機関に告発。 ・ならコープ、2022年10月に受けたサイバー攻撃で約49万人の個人情報漏えいの可能性。 ・経済産業省、関西・中国電力の顧客情報の不正閲覧を問題視し、報告書提出を命令。２月には中部電力、九州電力の不正も発覚。	・アイルランドDPC、Metaのターゲティング広告表示がGDPR違反として3.9億ユーロの制裁金と、３カ月以内のデータ業務処理の改善命令。 ・米T-Mobile、ハッカーによる3,700万人の顧客データ盗難被害を報告。 ・米司法省と８つの州、Googleのデジタル広告市場における独占的立場を巡り、事業分離を求め提訴。 ・米司法省他各国捜査当局、80カ国、1,500人以上に被害をもたらしたランサムウェア「Hive」を解体。1.3億ドルの身代金支払いを阻止。

国　内	海外／国際連携
2023年２月	
	・EC、サイバーセキュリティ上の懸念から職員のTikTok利用停止。 ・カナダ個人情報保護委員会、TikTokの個人情報管理の適切性の調査に着手。 ・ロシア連邦独占禁止局、Appleのモバイルアプリ市場の独占的地位乱用に対し、９億ルーブルの制裁金。

国　内	海外／国際連携
2023年３月	
・理化学研究所他、超伝導方式による国産量子コンピュータ初号機を公開、クラウドでのサービス利用開始。 ・人材サービスのエン・ジャパン、不正アクセスで25万人超の履歴書情報漏えいの可能性。 ・NTTドコモ、外部委託先で顧客情報、最大約529万件流出の可能性。	・FTC、Epic Gamesのユーザーが意図しない課金手法に対し、制裁金2.4億ドルの支払い命令。 ・オランダ裁判所、Facebookのプライバシー侵害裁判で、ユーザーデータの処理を違法と判断。 ・GPDP、ChatGPTをプライバシー規制遵守まで一時的に禁止。ユーザー情報の違法収集、年齢確認システムの未導入を指摘。

プライバシーマーク創設25周年特設サイトのご紹介

本誌コラムでもご紹介しましたが、JIPDECは1998年にプライバシーマーク制度を創設し、今年４月に25周年を迎えました。

周年を記念し、周年ロゴ・周年のブランドメッセージを制作し、特設サイトを公開しています。ブランドメッセージは「あなたの未来を守る、創る。」と設定。個人情報を守ることは、漏えいなどによって起きうる不当な不利益を被る可能性のある未来から守ること、つまりそれは、一人ひとりの未来を創ることであると考えています。

特設サイトでは、JIPDEC　プライバシーマーク推進センター　担当常務理事　竹内 英二の挨拶とともに、1986年１月に協会内に設置した「民間部門におけるプライバシー保護に関する調査研究委員会」の委員長就任以降、長年にわたりJIPDECの個人情報保護に関する調査研究、プライバシーマーク制度創設にご尽力をいただいた、一橋大学　名誉教授　堀部 政男先生に、「個人情報の過去と未来と」をテーマに、25年のさまざまな出来事を振り返っていただきました。

さらにプライバシーマークを取得いただいている事業者様や、制度運営に携わっていただいた審査員の方々、また、その他にも有識者の皆様へのインタビューなど、１年をかけてさまざまなコンテンツをご紹介していく予定です。ぜひ、25周年を迎えたプライバシーマークへご注目ください。

特設サイト　https://privacymark.jp/lp/25th/

JIPDEC

JIPDEC IT-Report 2023 Spring
2023年5月31日発行（通巻第21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
制　作　株式会社ウィザップ