不正アクセス行為対策等の実態調査

アクセス制御機能に関する技術の研究開発の状況等に関する調査

調査報告書

令和４年１２月

警察庁サイバー警察局 サイバー企画課

不正アクセス行為対策等の実態調査
アクセス制御機能に関する技術の研究開発の状況等に関する調査
目次

第１部

不正アクセス行為対策等の実態調査

1. 調査概要

1.1 調査の目的

不正アクセス行為の禁止等に関する法律において、国家公安委員会は、アクセス制御機能を有する特定電子計算機の不正アクセス行為からの防御に資するため、アクセス制御機能に関する技術の研究開発の状況等を公表するものとされており、また、国はアクセス制御機能を有する特定電子計算機の不正アクセス行為からの防御に関する啓発及び知識の普及に努めなければならないとされている。

本調査は、アクセス制御機能を有する特定電子計算機の不正アクセス行為からの防御に関する啓発や知識の普及に資することを目的とし、民間企業、行政機関等における不正アクセス行為対策等について調査を実施したものである。

1.2 調査の対象と調査方法

調査対象は、市販のデータベース（四季報）に掲載された企業、教育機関（国公立、私立の大学等）、医療機関、地方公共団体（県・市区町村等）、独立行政法人（教育機関及び医療機関に掲げるものを除く。）、特殊法人から特定の業種、地域に偏りのないよう2,950件を無作為に抽出した。

調査は、調査票を郵送で配付し、次の2つの方法で回収することで実施した。

① 電子メールでの回答

調査票のファイルに回答内容を入力してもらい、電子メールにて回答

② 郵送等での回答

配付した調査票を、郵送で送付してもらい回答

（調査期間：令和4年9月9日(金)（発送日)～12月7日(水)（締切日））

1.3 調査内容

付録資料にある調査票「不正アクセス行為対策等の実態に関するアンケート調査」のとおりである。

1.4 送付、回収状況

調査票の送付総数は2,951件、回収総数は600件であった。回収率は20.3%である。

業種	発送数	回収数	回収率
農林・水産・鉱業	10	1	10.0%
製造業	901	151	16.8%
不動産・建築	187	25	13.4%
金融	108	28	25.9%
エネルギー	15	4	26.7%
運輸業	75	22	29.3%
情報通信	291	14	4.8%
サービス	837	126	15.1%
教育	290	105	36.2%
行政サービス	237	104	43.9%
無回答		20	-
合計	2,951	600	20.3%

1.5 報告書を見る際の留意点

- 回答のあった調査票のうち、不備があったものを集計対象外としたため、集計総数は590件となっている。
- 集計結果の比率は、小数第二位を四捨五入し、小数第一位までを百分率（%）で表示しているため、その数値の合計が100%を前後する場合がある。
- 本文やグラフ中の選択肢は、調査票の言葉を短縮しているものがある。
- 回答数が５未満のもの（例：業種別にみた場合の「農林・水産・鉱業」〔回収数1〕など）については、コメントの対象としていない。

2. 調査結果の概要等

2.1 概要

令和4年度の調査結果については、次のような特徴がみられる。

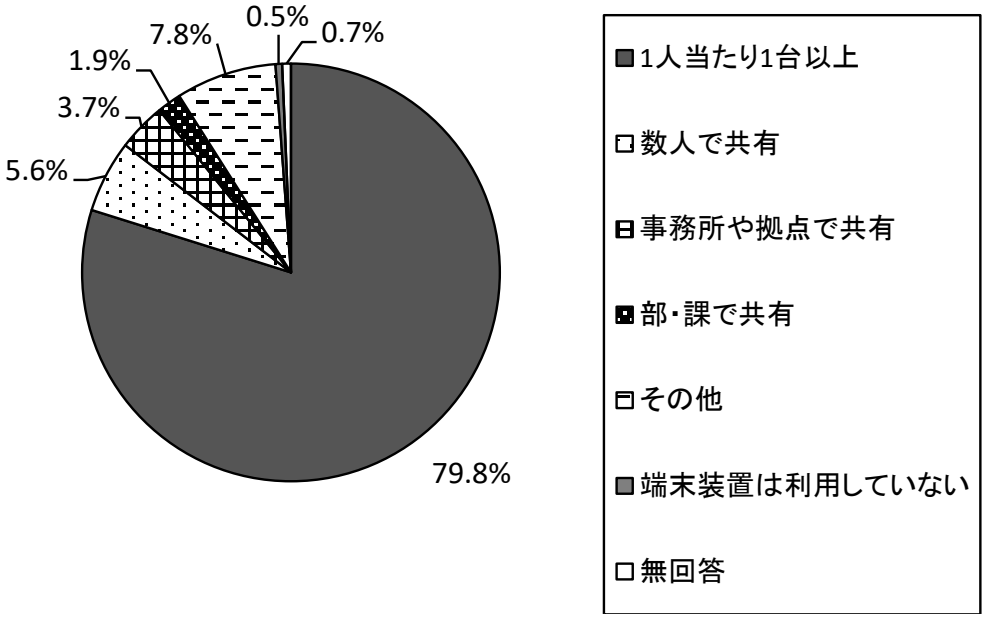
1　組織的対策状況

【情報システム等の環境】

パソコン・スマートフォン等の整備環境については、79.8%で「1人当たり1台以上」で整備されており、「数人で共有」が5.6%、「事業所や拠点で共有」が3.7%となっている。テレワークの実施状況については、「行っている」が71.9%となっている。

事業体内のネットワーク利用状況については、「有線ネットワークと無線ネットワークを併用」が88.5%で最も高く、次いで「全て有線ネットワークで構築」が8.8%となっている。「全て無線ネットワークで構築」を含めるとほぼ全ての事業所でネットワークが導入されている。外部からの接続に対する許可についても、「許可している」が64.4%で、半数以上が外部からの接続を許可している。

【全体】端末装置（タブレット・スマートフォン等）の整備環境(SA,n=590)



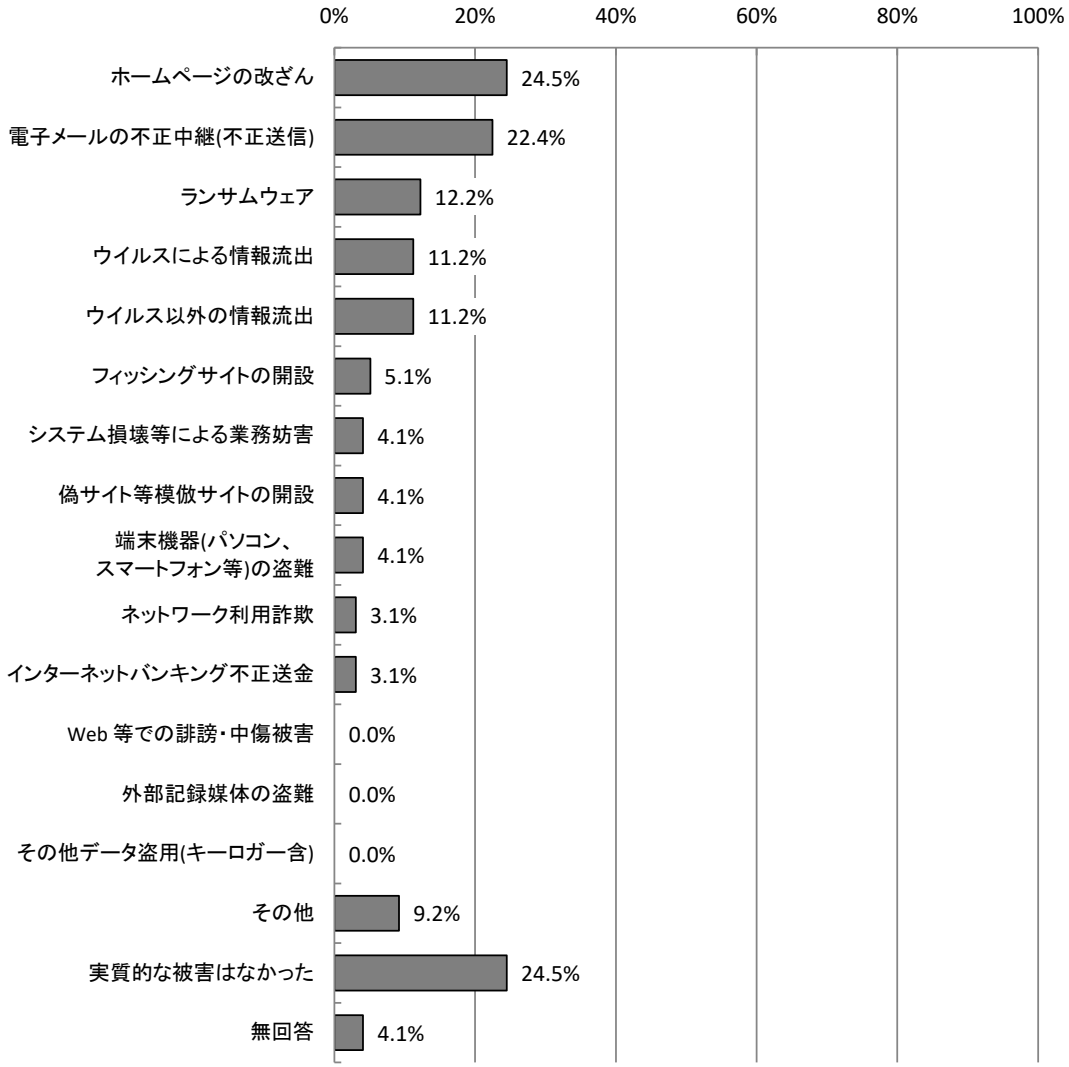
【不正アクセス等の被害状況】

過去１年間に不正アクセス等の攻撃・被害にあったと回答した社・団体等（98団体）について、被害内容をみると「ホームページの改ざん」が24.5%、「電子メールの不正中継」が22.4%で高い。

届出先機関等については、「警察」が28.6%、「監督官庁」が21.4%、「IPA （情報処理推進機構）」が19.4%となっている。「届け出なかった」は43.9%と4割を超えている。

届出を躊躇させる要因は、「実質的な被害が無かったので」が74.4%で高く、次いで「社・団体内で対応できたので」が32.6%、「自社内だけの被害だったので」が16.3%で、被害が無かったと感じた場合や、自社以外に被害が及ばなかった場合、届出を躊躇する傾向が見られる。

【全体】過去に受けたことのある被害状況（MA,n=98）



【情報セキュリティの運用・管理体制】

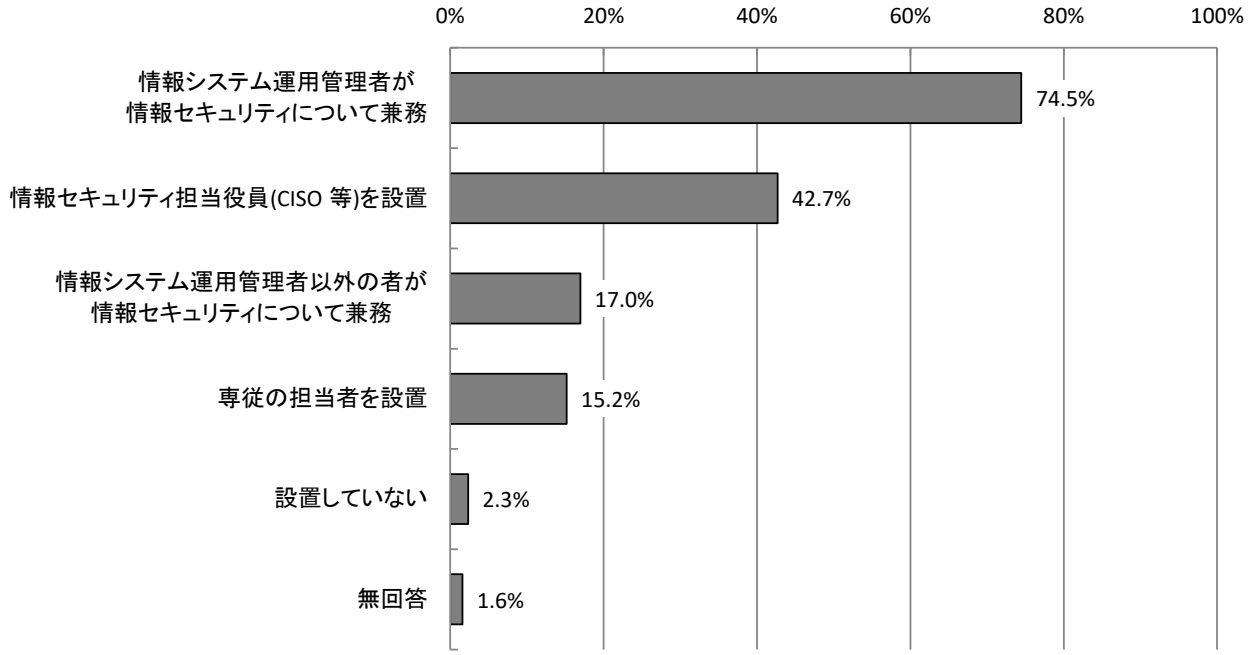
情報セキュリティ対策を行っている社・団体等（560団体）のうち、情報セキュリティ運用・管理専門部署の有無については、「ある」が69.5%であり、管理体制は「情報システム運用管理者が情報セキュリティについて兼務」が74.5%で最も多くなっており、「情報セキュリティ担当役員（ＣＩＳＯ等）を設置」は42.7%となっている。

セキュリティポリシーの策定状況は、「策定している」が85.2%で高く、「今のところ、策定する予定はない」は3.6%となっている。策定済みに今後予定と策定作業中を入れると90.7%であり、情報セキュリティポリシーの策定が浸透している状況となっている。

情報セキュリティ侵害事案発生時の対応マニュアル等の策定状況については、「策定している」が52.9%と過半数で、「策定することを検討」が28.6%となっている。

第三者認証機関制度の利用は、「特に利用していない」が79.1%となっている。

【全体】情報セキュリティ管理体制（MA, n=560）

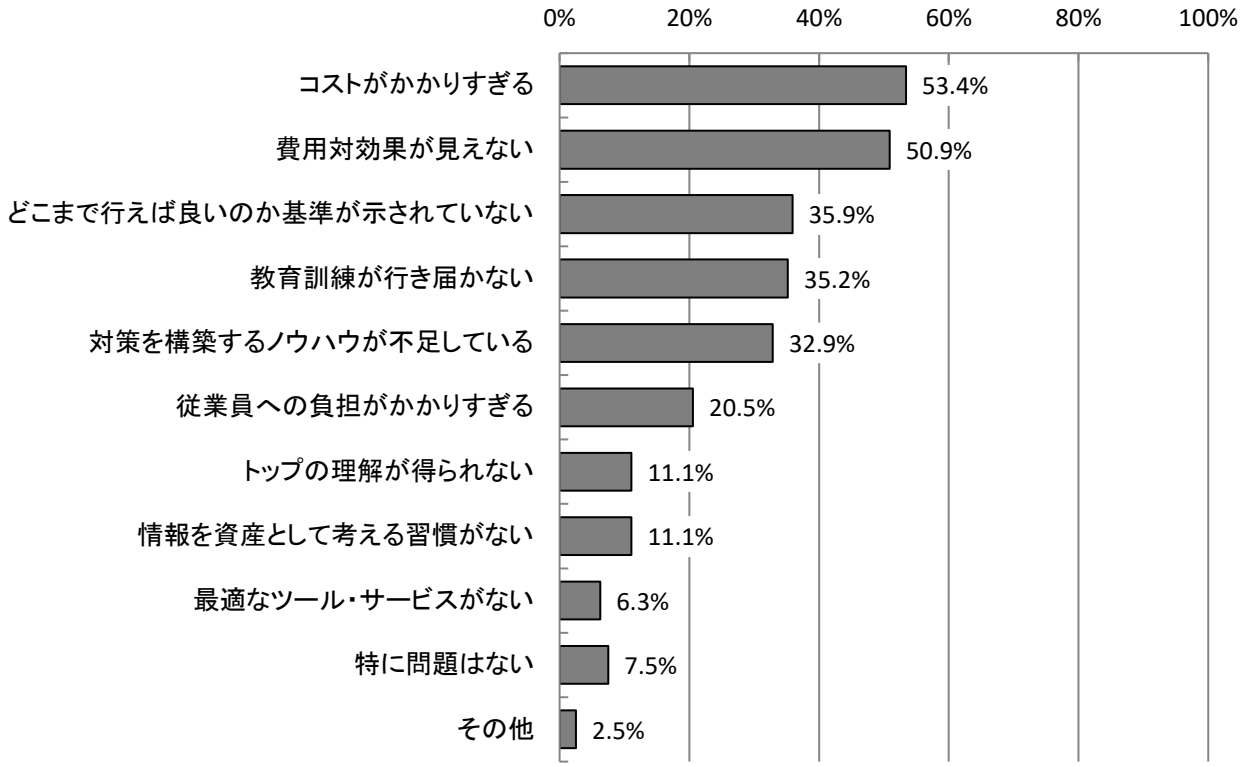


【情報セキュリティ対策への投資】

令和５年度次の情報セキュリティ対策の投資計画については、令和４年度と比較して「現状どおりの予定」が57.9%で最も高く、「増額する予定」が34.8%、「減額する予定」は0.7%となっている。

情報セキュリティ対策への投資に関する問題点は、「コストがかかりすぎる」が53.4%、「費用対効果が見えない」が50.9%で高なっている。次いで「どこまで行えば良いのか基準が示されていない」が35.9%、「教育訓練が行き届かない」が35.2%となっている。

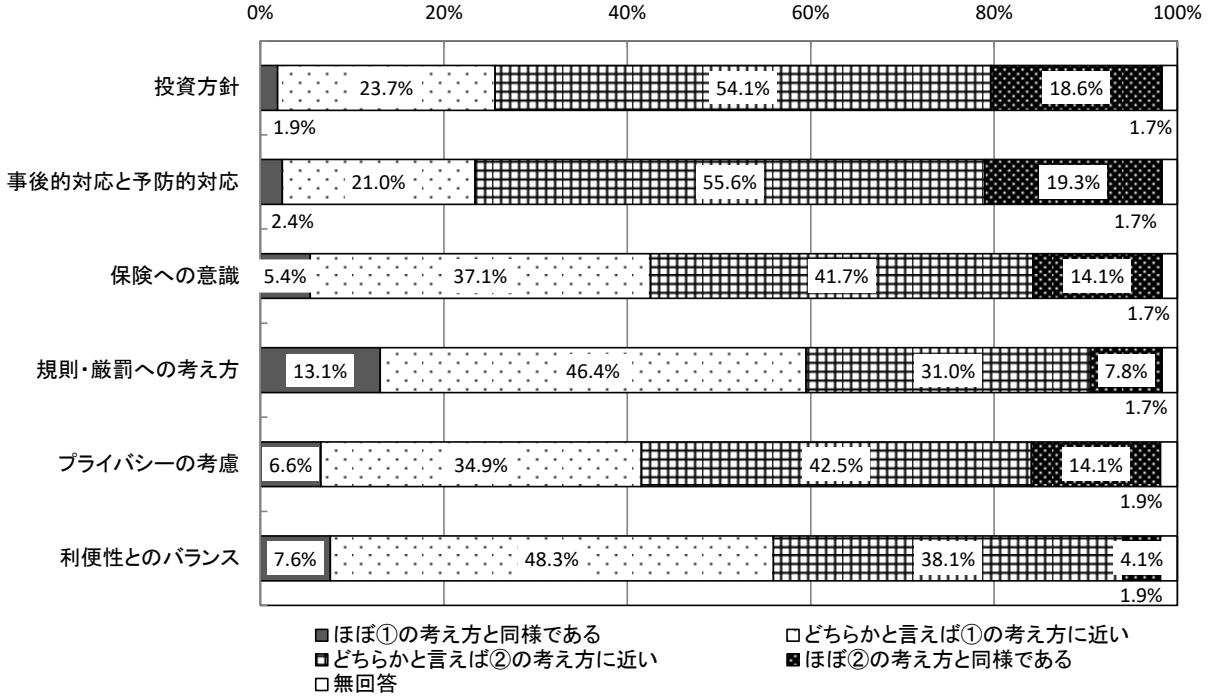
【全体】情報セキュリティ対策への投資に関する問題点(MA,n=560)



【情報セキュリティ対策に関する考え方】

情報セキュリティ対策を実施する上での「投資方針」については「②積極的」が「①必要最低限」を上回り、「事後的対応と予防的対応」については「②予防的対応」が「①問題発生への適切な対応」を大幅に上回っている。「保険への意識」については「②保険的対応が必要」が「①人的・技術的な対策で十分」を、「規制・罰則への考え方」については「①教育と情報提供を中心とした対応」が「②規則・罰則も含む強制力のある対応」を、「プライバシーの考慮」については「②ある程度のプライバシーの侵害はやむをえない」が「①プライバシーはある程度考慮されるべきだ」を、「利便性とのバランス」については「①利便性とのバランスを考慮」が「②負担を強いてでもセキュリティを守る」を、それぞれ上回っている。

【全体】情報セキュリティ対策実施上の方針（SA, n=590）



項目	考え方①	ほぼ①の考え方と同様である	どちらかと言えば①の考え方に近い	どちらかと言えば②の考え方に近い	ほぼ②の考え方と同様である	考え方②
投資方針	セキュリティ投資は必要最低限に抑えるべきである。	1	2	3	4	来るべき問題事案に備えて、積極的に投資を行うべきである。
事後的対応と予防的対応	情報セキュリティ対策としては、問題発生に対しての応急対応や、再発防止・被害拡大防止に注力するべきである。	1	2	3	4	情報セキュリティ対策としては、リスクの検知など、予防上の対策に注力するべきである。
保険への意識	情報セキュリティ対策としては、人的・技術的な対策によりカバーできるところを対策すれば十分である。	1	2	3	4	情報セキュリティ対策としては、人的・技術的対策によりカバーすることに加え、保険によりまかなうべきである。
規制・罰則への考え方	技術以外の面での対策としては、従業員等への教育と、適切な情報提供により対策を促すことが重要である。	1	2	3	4	技術以外の面での対策としては、教育はもちろんのこと、規制・罰則などの強制力のある制度的対応を行うことが重要である。
プライバシーの考慮	職場とはいえ、従業員等のプライバシーは保護された上で、情報セキュリティ対策は行われるべきである。	1	2	3	4	職場のセキュリティ保護のためにはシステム利用状況のモニタリングなどによるプライバシー保護の制約はやむをえない。
利便性とのバランス	業務実施に負担をかけるほどのセキュリティ対策は不適当であり、利便性とのバランスを考慮すべきである。	1	2	3	4	ユーザにシステム利用上・業務上の負担を強いてでもセキュリティを守るべきである。

2　技術的対策

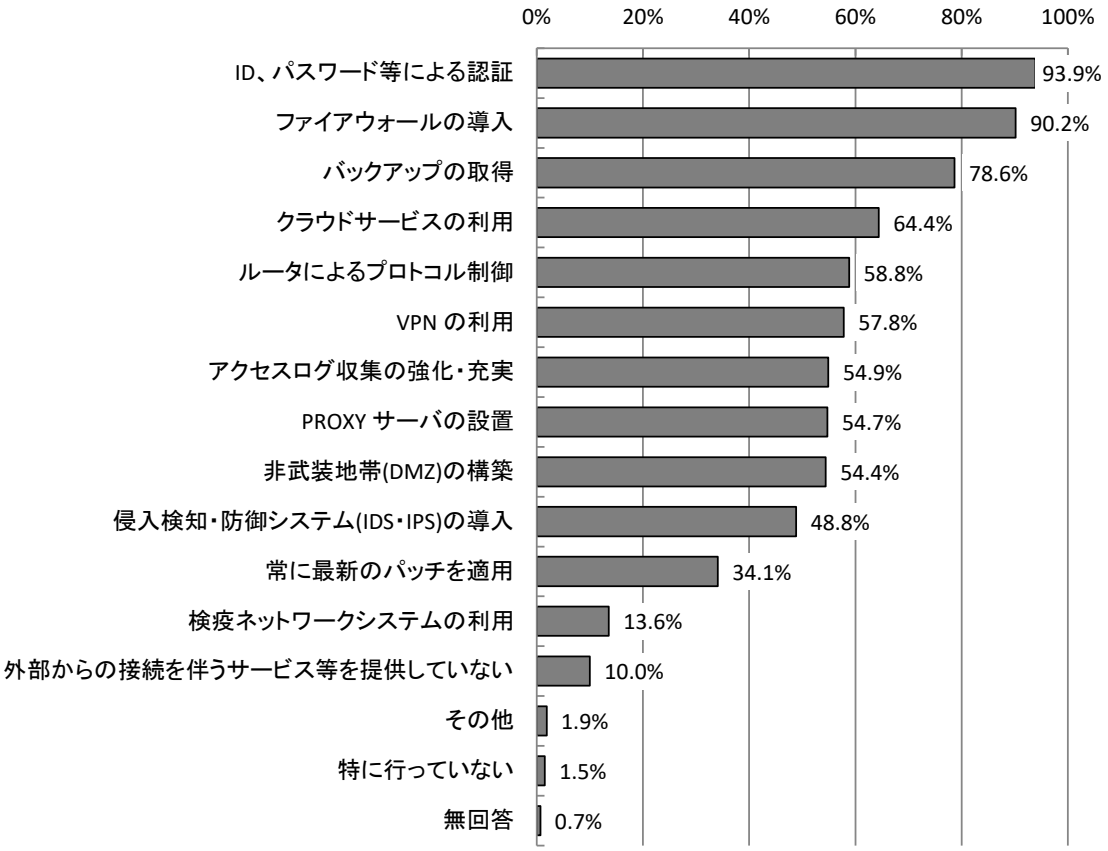
【ネットワークに対する情報セキュリティ対策】

外部からの接続に対するセキュリティ対策（通信路に対する対策）については、「ID・パスワード等による認証」が91.1%で最も高く、次いで「通信の暗号化」が73.2%、「MACアドレス、クライアント証明書等使用する端末機器の固有情報を用いた認証」が48.7%となっている。

端末に対する対策については、「ウイルス対策ソフト等の導入」が89.2%で最も高く、次いで「OS、アプリケーション等をアップデートする仕組みの導入」が51.3%、となっている。

インターネット接続に対するセキュリティ対策については、「ID、パスワード等による認証」が93.9%で最も高く、次いで「ファイアウォールの導入」が90.2%となっている。

【全体】インターネット接続に対するセキュリティ対策（MA,n=590）

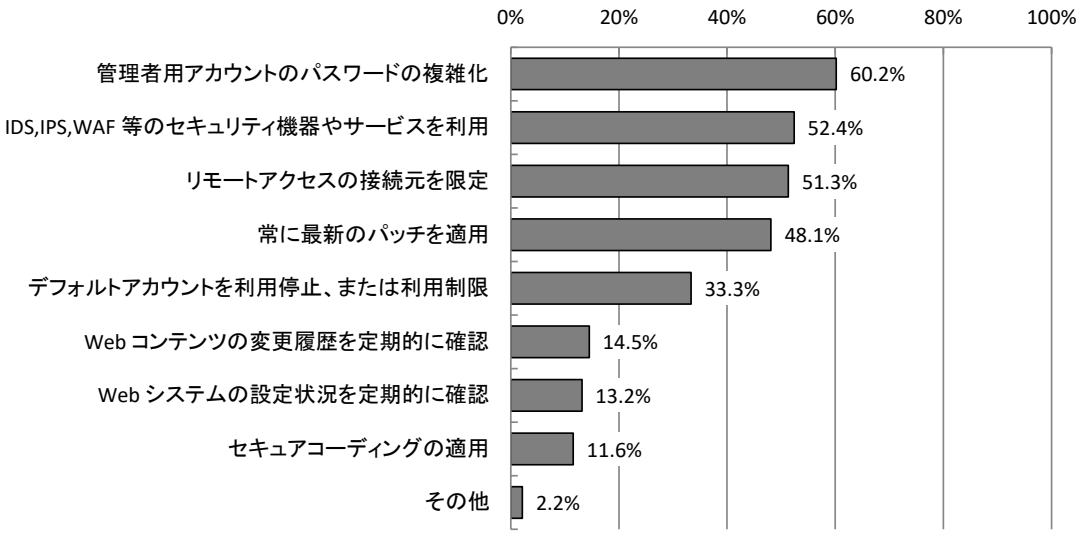


【各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）のセキュリティ対策】

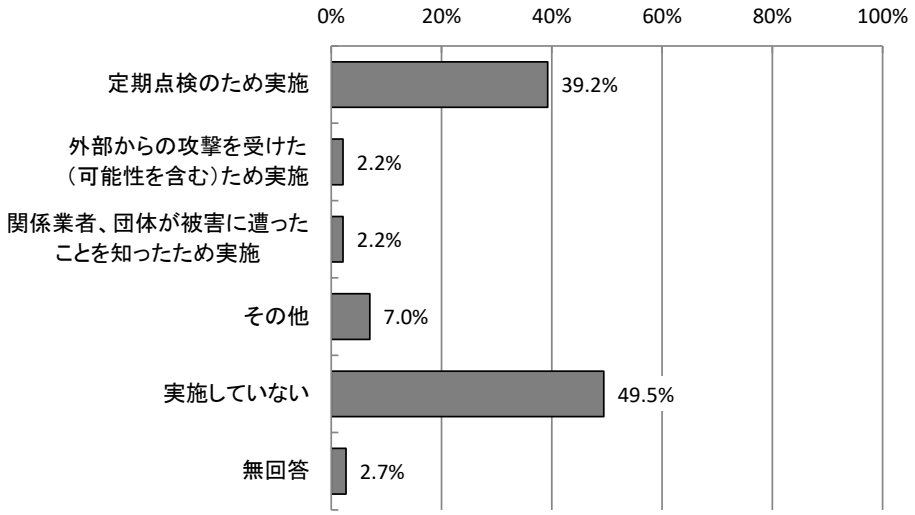
各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）のセキュリティ対策については、「管理者用アカウントのパスワードの複雑化」が60.2%で最も多く、次いで「ＩＤＳ、ＩＰＳ、ＷＡＦ等のセキュリティ機器やサービスを利用」が52.4%、「リモートアクセスの接続元を限定」が51.3%となっている。

ぜい弱性調査（ペネトレーションテスト）実施の有無については、「実施していない」が49.5%と最も多く、次いで「定期点検のため実施」が39.2%となっている。

【全体】各種サービスのセキュリティ対策（MA, n=372）



【全体】ぜい弱性調査（ペネトレーションテスト）実施の有無（MA, n=372）

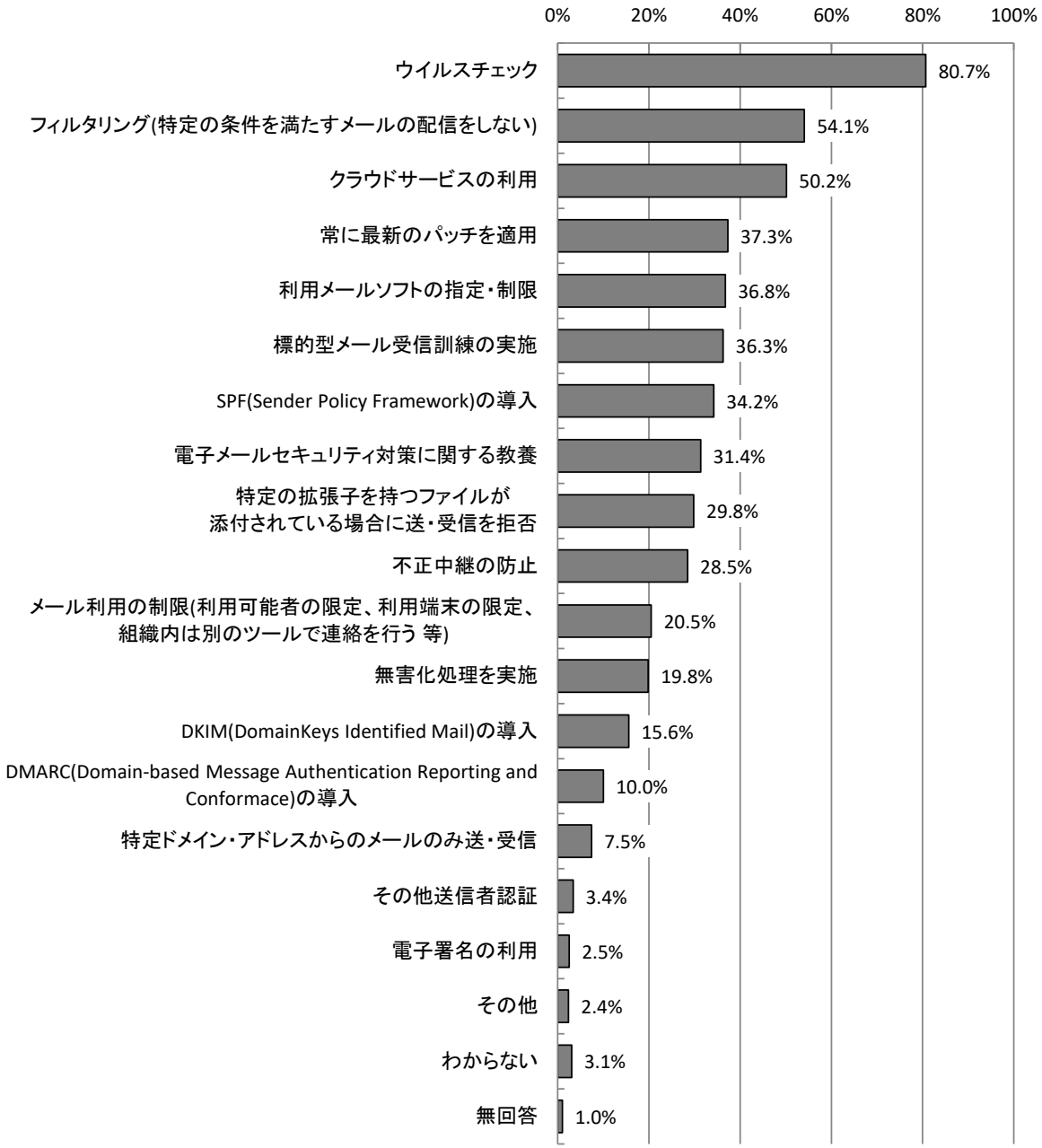


【電子メールに関するセキュリティ対策】

電子メールに関するセキュリティ対策については、「ウイルスチェック」が80.7%で最も高く、次いで「フィルタリング（特定の条件を満たすメールの配信をしない）」が54.2%、「クラウドサービスの利用」が50.2%となっている。

添付ファイルの取り扱いについては、「ウイルスチェックをしてから受信」が76.8%で最も高い。一方、「特にチェック等はしていない」は8.6%であった。

【全体】電子メールに関するセキュリティ対策（MA, n=590）

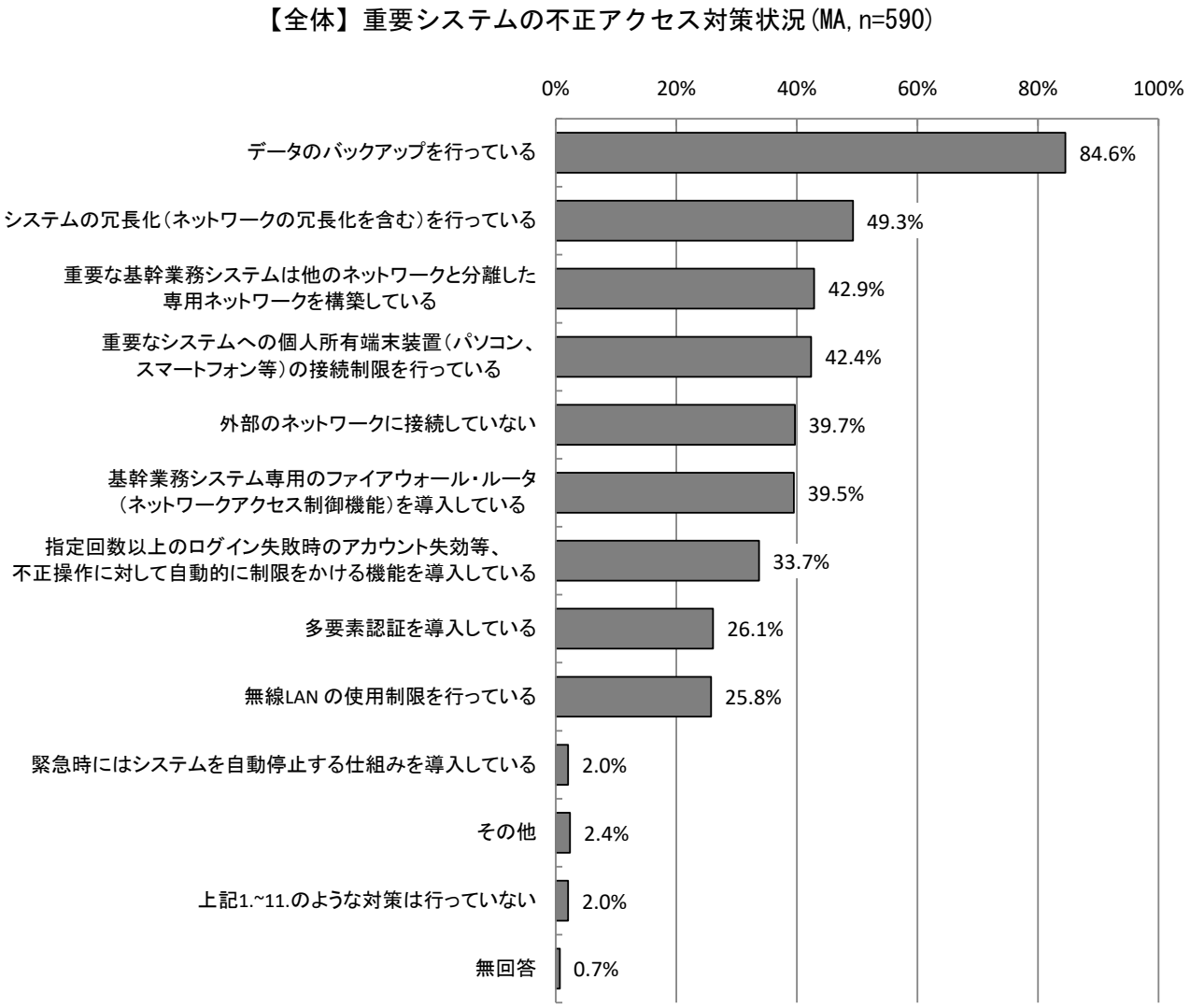


【不正アクセス、情報漏えい等に対する情報セキュリティ対策】

重要システムの不正アクセス対策状況については、「データのバックアップを行っている」が84.6%で最も高く、「システムの冗長化（ネットワークの冗長化を含む）を行っている」が49.3%、「重要な基幹業務システムは他のネットワークと分離した専用ネットワークを構築している」が42.9%、「重要なシステムへの個人所有端末装置（パソコン、スマートフォン等）の接続制限を行っている」が42.4%となっている。

不正アクセス等への対策状況については、「定期的なバックアップ」が78.1%で最も高く、次いで「情報資産へのアクセス権の設定」が72.7%「端末装置（パソコン、スマートフォン等）廃棄時の適正なデータ消去」が67.3%、となっている。

不正プログラムへの対策状況については、「ウイルス対策ソフト（クライアント）の使用」が92.2%で最も高く、次いで「ウイルス対策ソフト（サーバ）の使用」が76.9%、「パターンファイルを定期的に更新する（自動更新システムを利用）」が75.4%となっている。



３　人的対策

【情報セキュリティ教育】

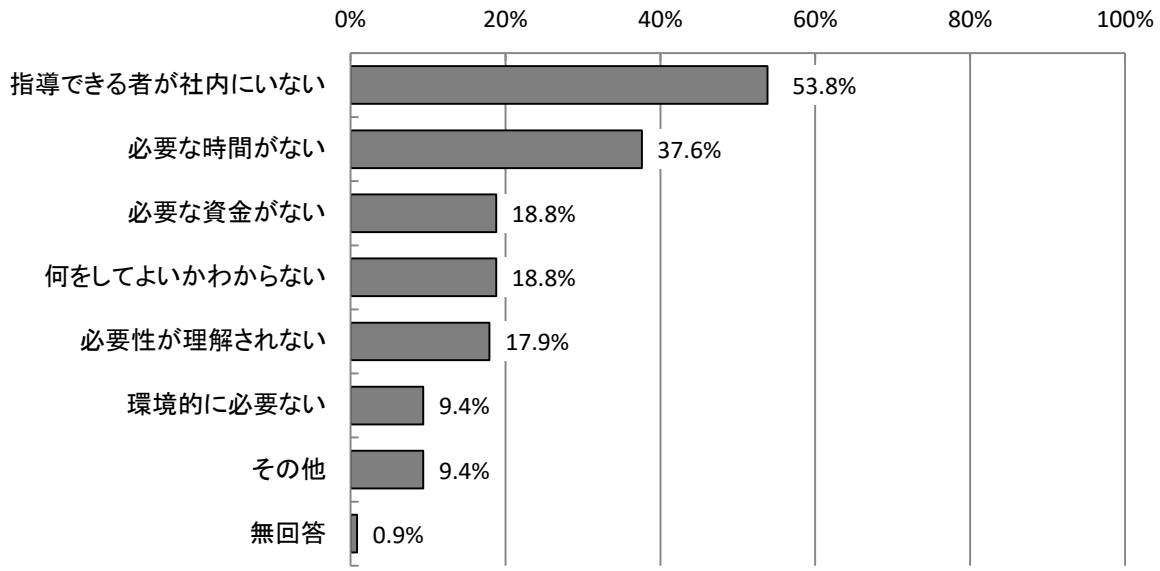
情報セキュリティ教育の実施状況は「実施している」が73.6%、「実施していない」が19.8%、「実施を予定している」が4.4%となっている。実施状況は従業員規模で違いがみられ、従業員数100人未満の社・団体では32.2%であり小規模ほど実施率が低い状況にある。

なお。情報セキュリティ教育を実施しない理由については、「指導できる者が社内にいない」が53.8%で最も多く、次いで「必要な時間がない」が37.6%となっている。

情報セキュリティ教育の内容については、「個人情報の保護・管理」が73.7%、「ウイルス等のマルウェア対策」が72.4%、「情報セキュリティポリシー」が72.0%で高くなっている。

教育の頻度については、「年に１回」が45.0%で最も高く、次いで「年に数回」が35.0%、「採用、異動時等に実施」が27.0%となっている。

【全体】情報セキュリティ教育を実施しない理由(MA,n=117)

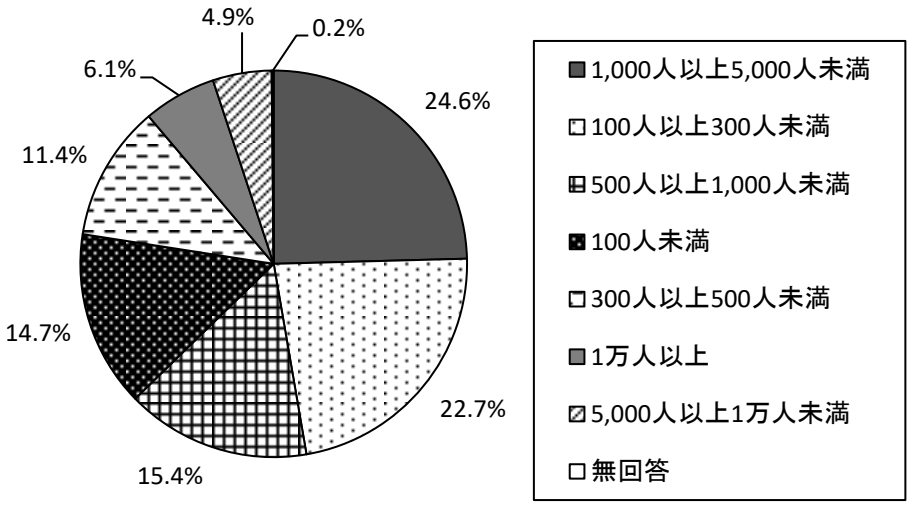


今回の調査結果では、情報セキュリティポリシーが、全体の８割以上で制定されており、情報セキュリティに関する教育においても、全体の７割で実施されている等、情報セキュリティに関する意識について一定の浸透が図られていることがうかがえるが、その一方で、小規模組織におけるセキュリティ教育の実施率が低いことや、情報セキュリティ対策について費用対効果が見えづらい・基準が示されていない等の問題意見が出されるなど、問題点も明らかになった。

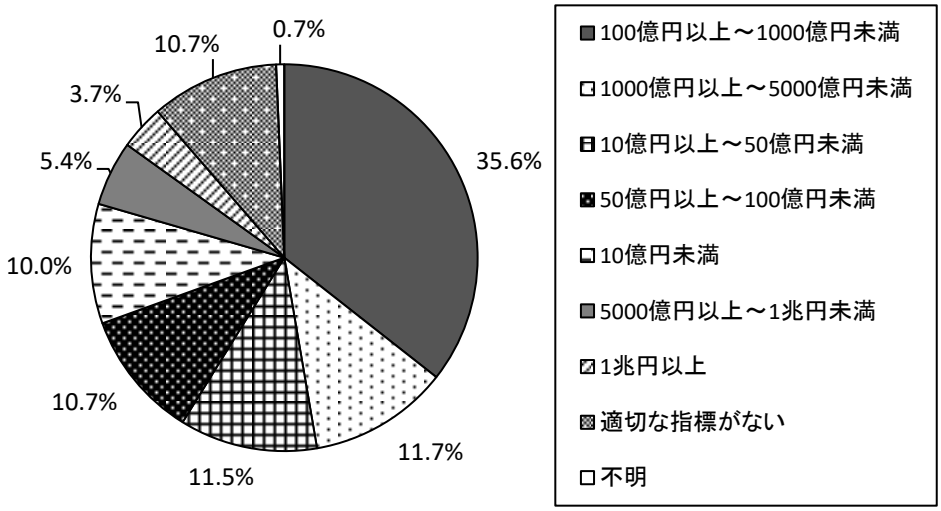
また、過去１年間に攻撃・被害を受けた社・団体等が全体の16.6%と依然として少なくない。そのうちホームページの改ざんが最も高い割合であり、セキュリティ対策が重要と認められる。セキュリティ侵害事案発生時における対応マニュアルの策定が、半数程度にとどまっている状況であり、事案発生の際の被害拡大防止のため、これら対策意識の浸透が今後の課題といえよう。

2.2 回答事業体の属性等

【全体】従業員規模（SA, n=590）【問2】



【全体】予算規模（SA, n=590）【問3】



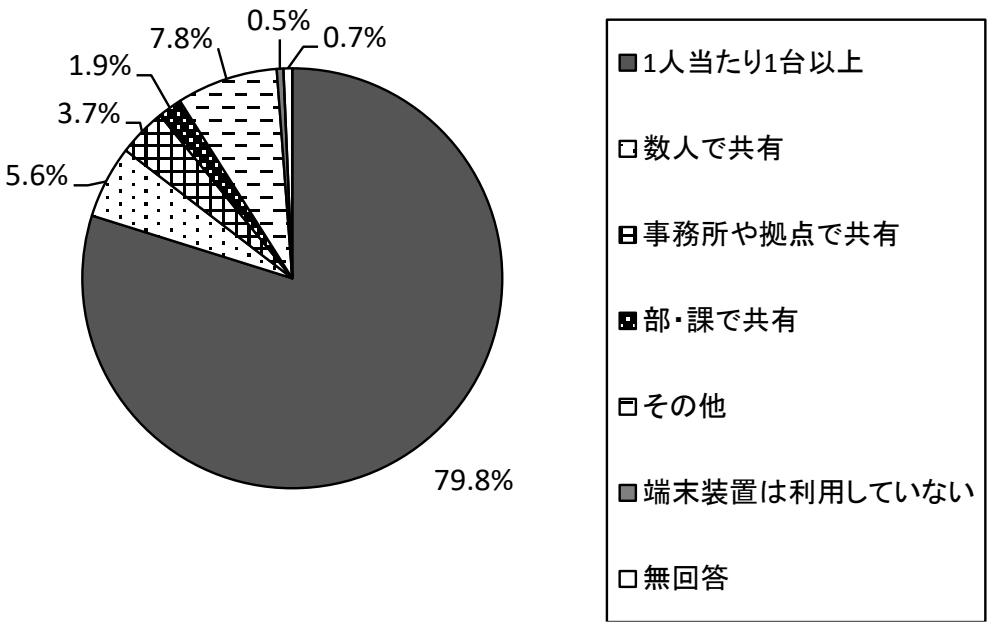
3. 調査結果

3.1　組織的対策

3.1.1　端末装置（パソコン、スマートフォン等）の整備環境　【問4】

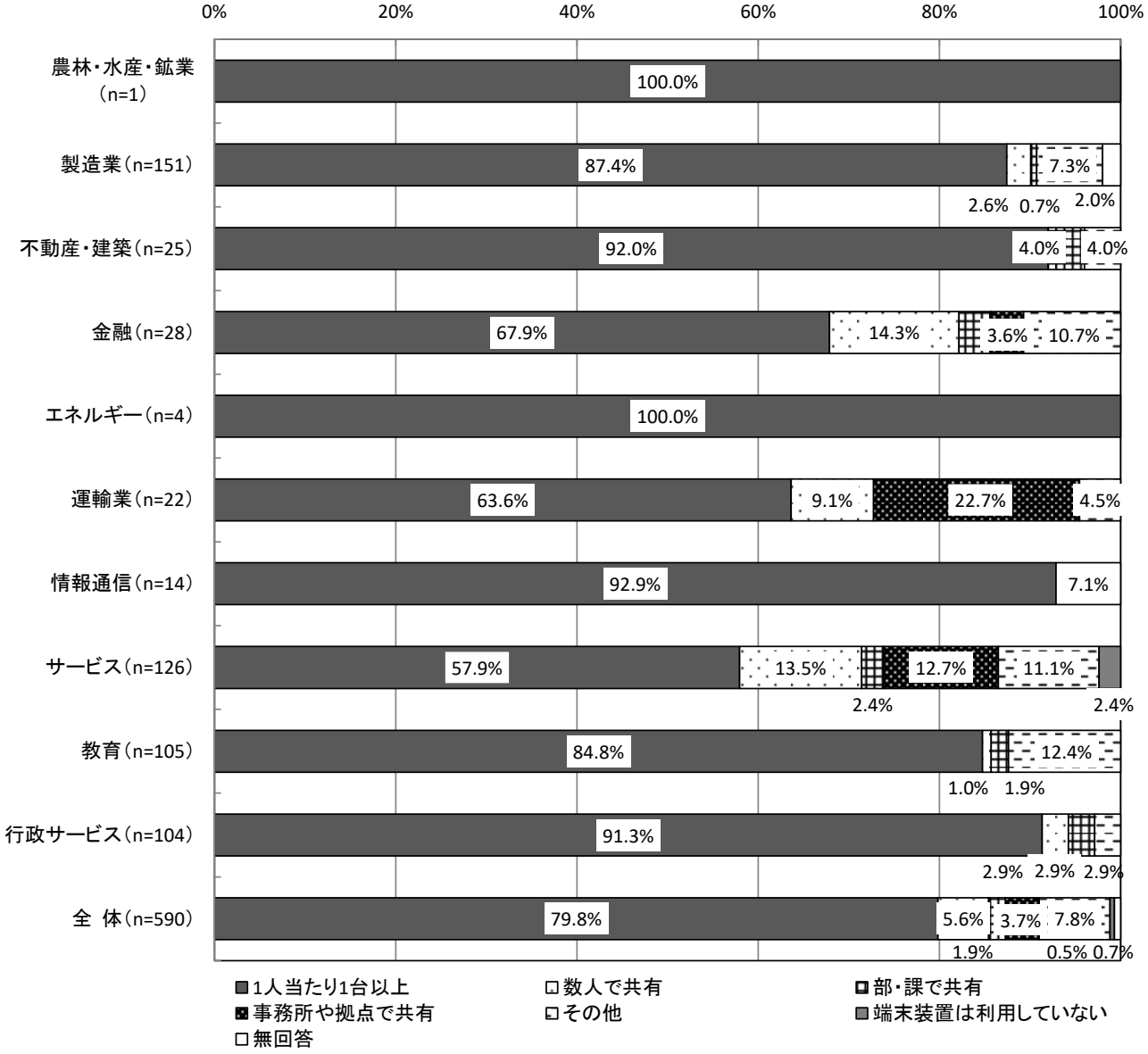
端末装置（パソコン）の整備環境については、「1人当たり1台以上」が79.8%で最も多く、「数人で共有」が5.6%、「事務所や拠点で共有」が3.7%となっている。

【全体】端末装置（パソコン、スマートフォン等）の整備環境（SA,n=590）



【業種別分析】業種別にみると、「1人当たり1台以上」では、「情報通信」で92.9%、「不動産・建築」で92.0%、「行政サービス」で91.3%で9割を超えて高い割合となっている。一方、「サービス」で57.9%と最も低く、「運輸業」で63.6%、「金融」で67.9%と低くなっている。

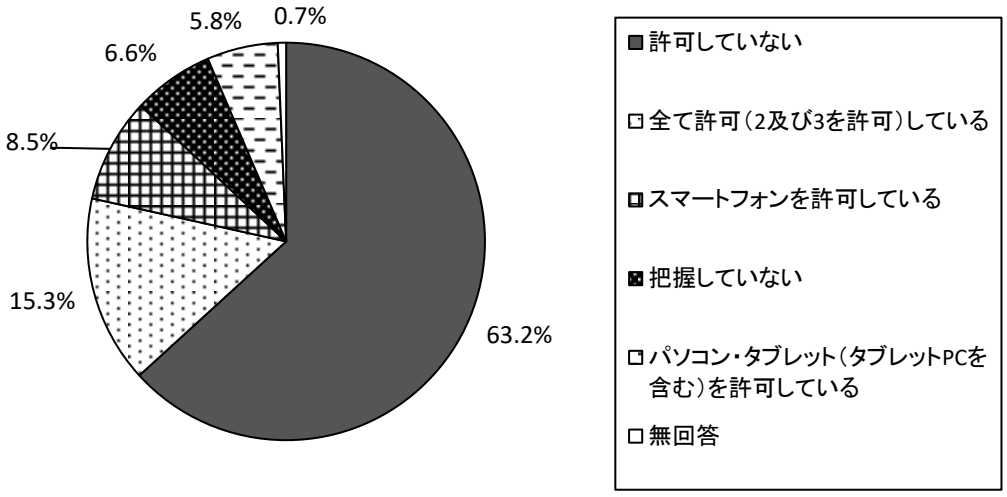
【業種別分析】端末装置（パソコン、スマートフォン等）の整備環境



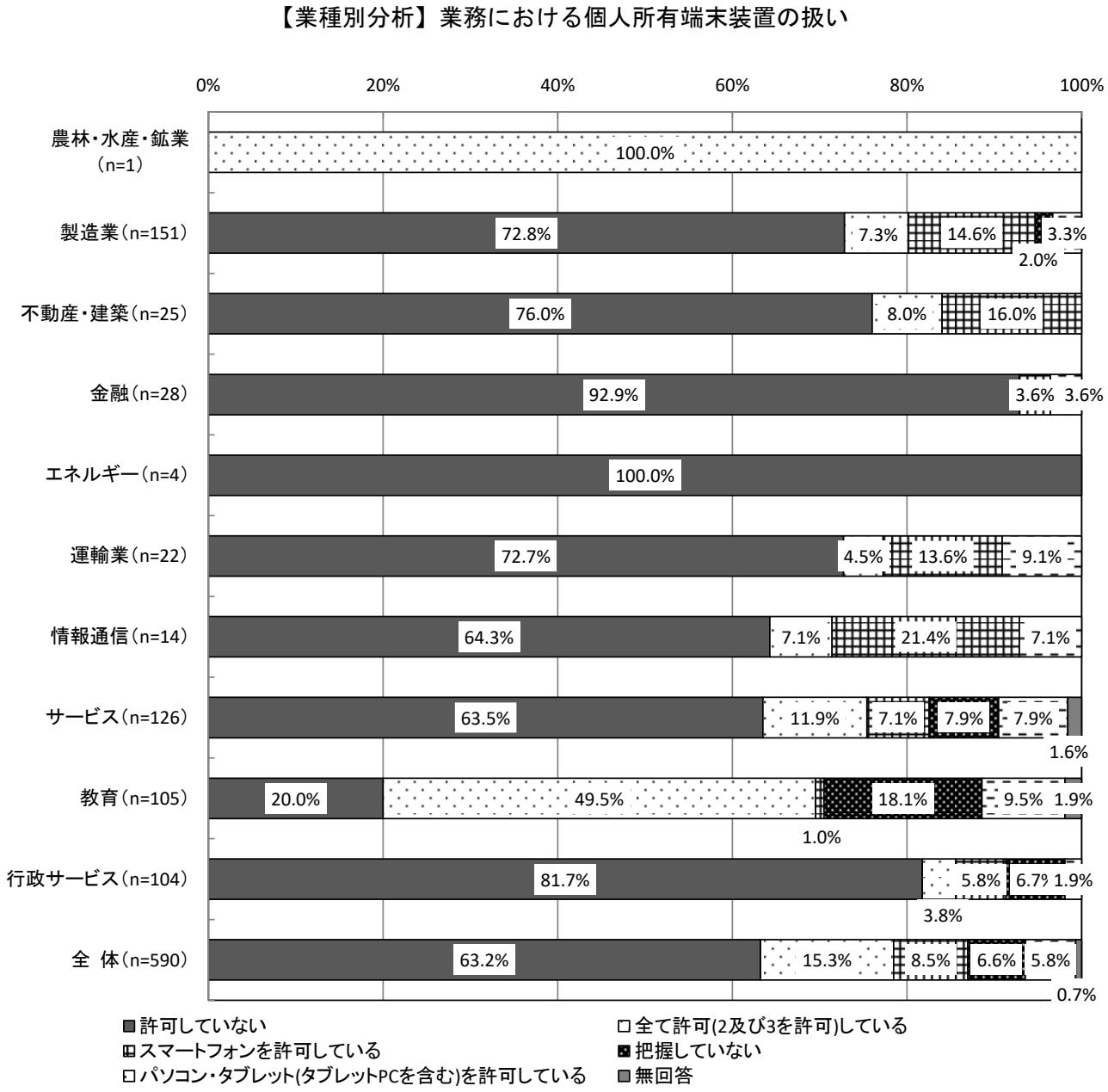
3.1.2　業務における個人所有端末装置の扱い　【問5】

業務における個人所有端末装置の扱いについては、「許可していない」が63.2%で最も高く、「全て許可している」が15.3%、「スマートフォンを許可している」が8.5%となっている。

【全体】業務における個人所有端末装置の扱い（SA,n=590）

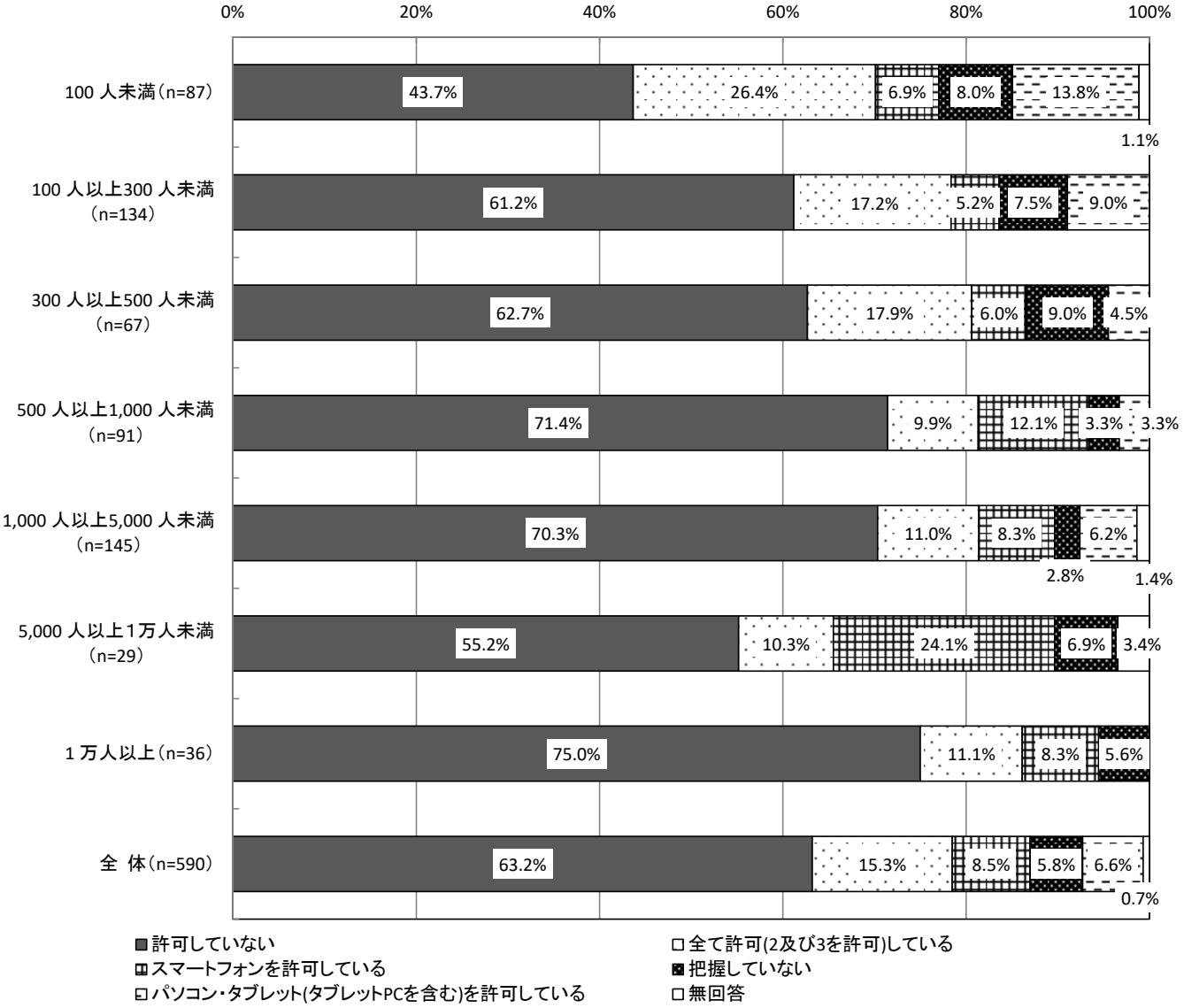


【業種別分析】業種別にみると、「許可していない」では、「金融」が92.9%で最も高く、次いで「行政サービス」が81.7%、「不動産・建築」が76.0%となっている。一方、最も低いのは「教育」で20.0%となっている。



【従業員規模別分析】従業員規模別にみると、「許可していない」では、「１万人以上」が75.0％で最も高く、次いで「500人以上1,000人未満」が71.4％、「1,000人以上5,000人未満」が70.3％で7割近くとなっている。一方、最も低いのは「100人未満」が43.7%で、ついで「5,000人以上1万人未満」で55.2％となっている。

【従業員規模別分析】業務における個人所有端末装置の扱い

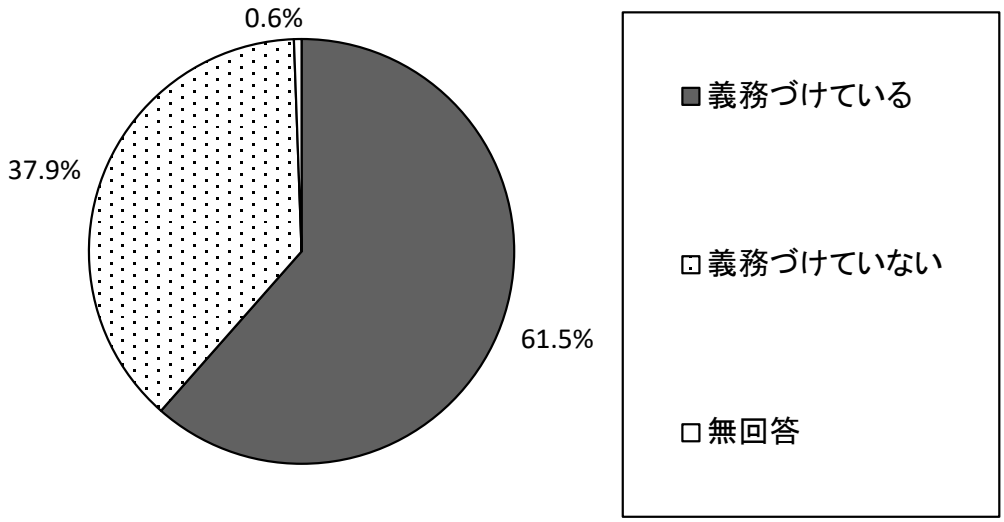


3.1.3　個人所有端末装置のセキュリティ対策【問5-1】

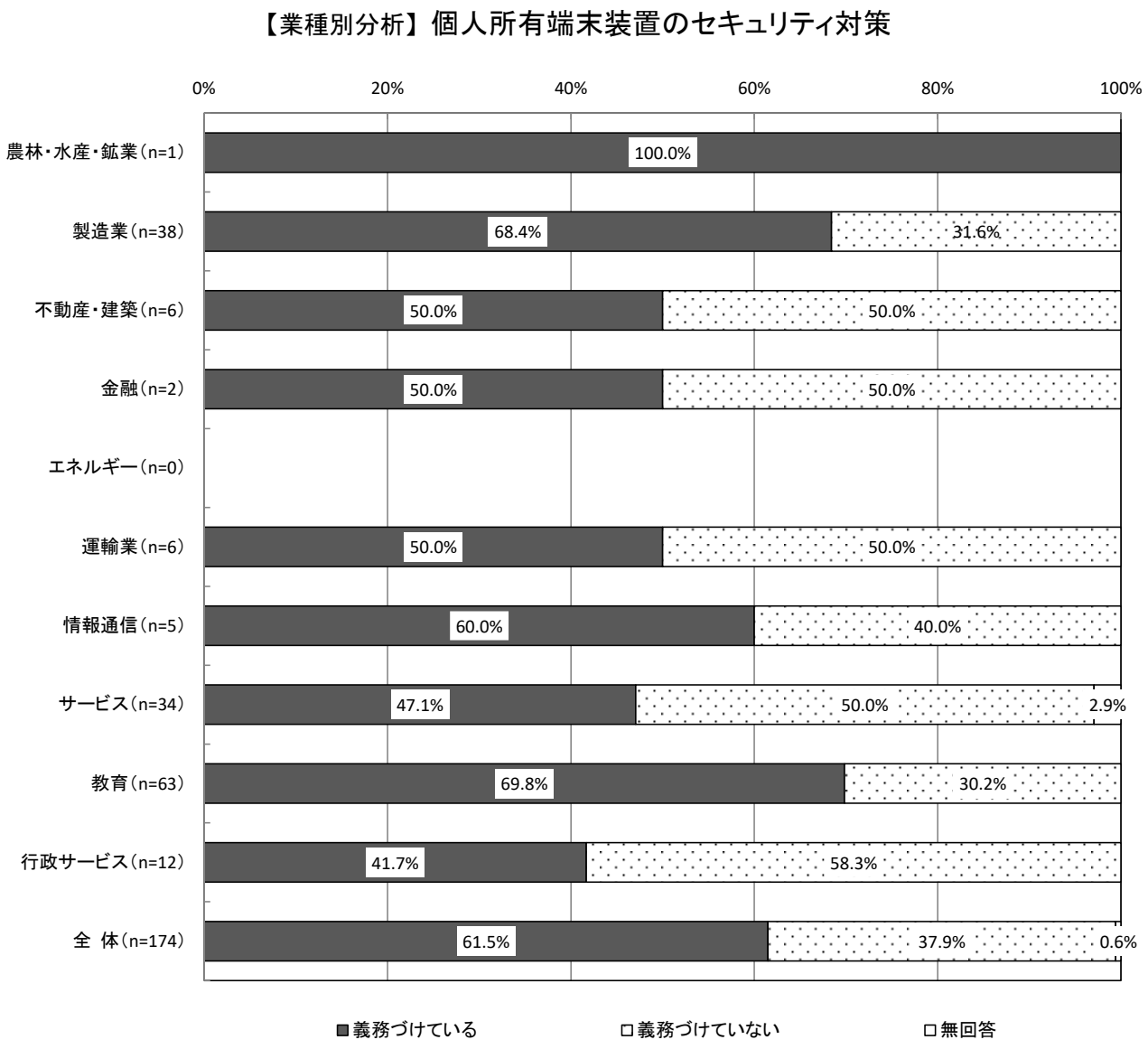
個人所有端末装置のセキュリティ対策については「義務付けている」が61.5%で高くなっている。これに対して「義務付けていない」は37.9%となっている。

※本項目は、個人所有端末装置を許可している社・団体等を対象としている。

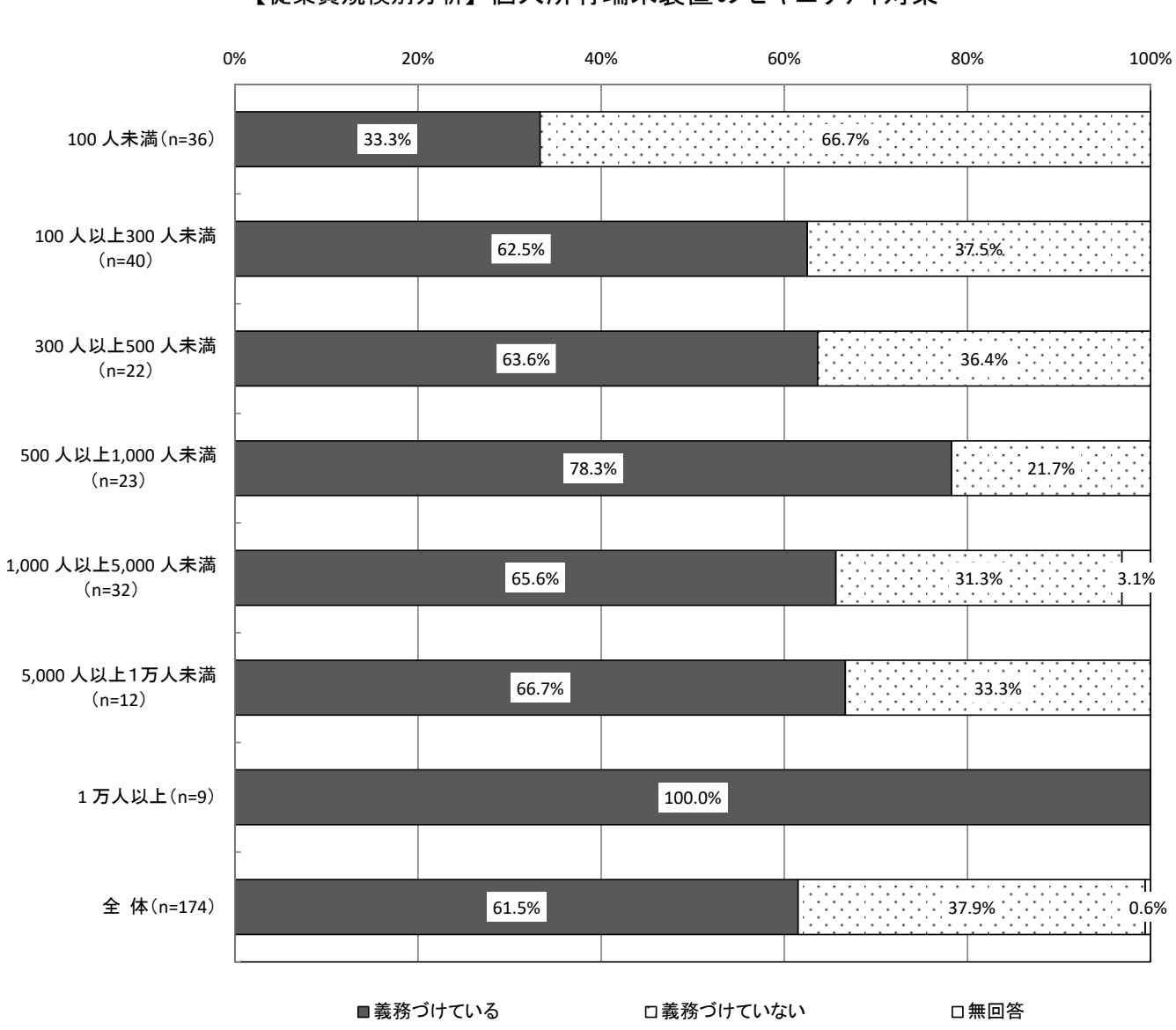
【全体】個人所有端末装置のセキュリティ対策（SA,n=174）



【業種別分析】業種別にみると、「教育」が69.8%、「製造業」が68.4%でいずれも7割近くで高い。一方「行政サービス」が41.7%、「サービス」が47.1%で低くなっている。



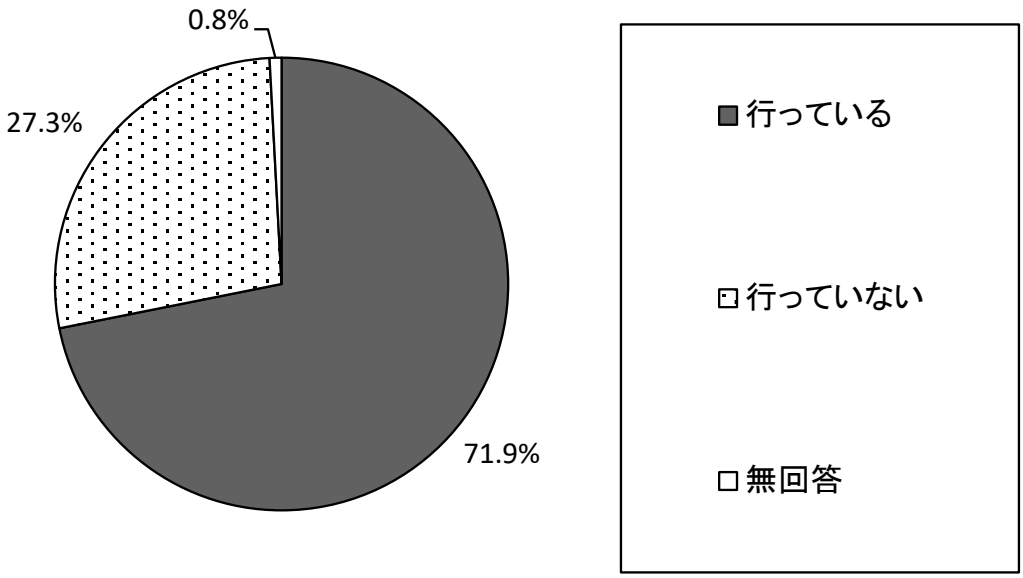
【従業員規模別分析】従業員規模別にみると、「1万人以上」が100.0%となっている。これに対して「100人未満」は33.3%と低くなっている。



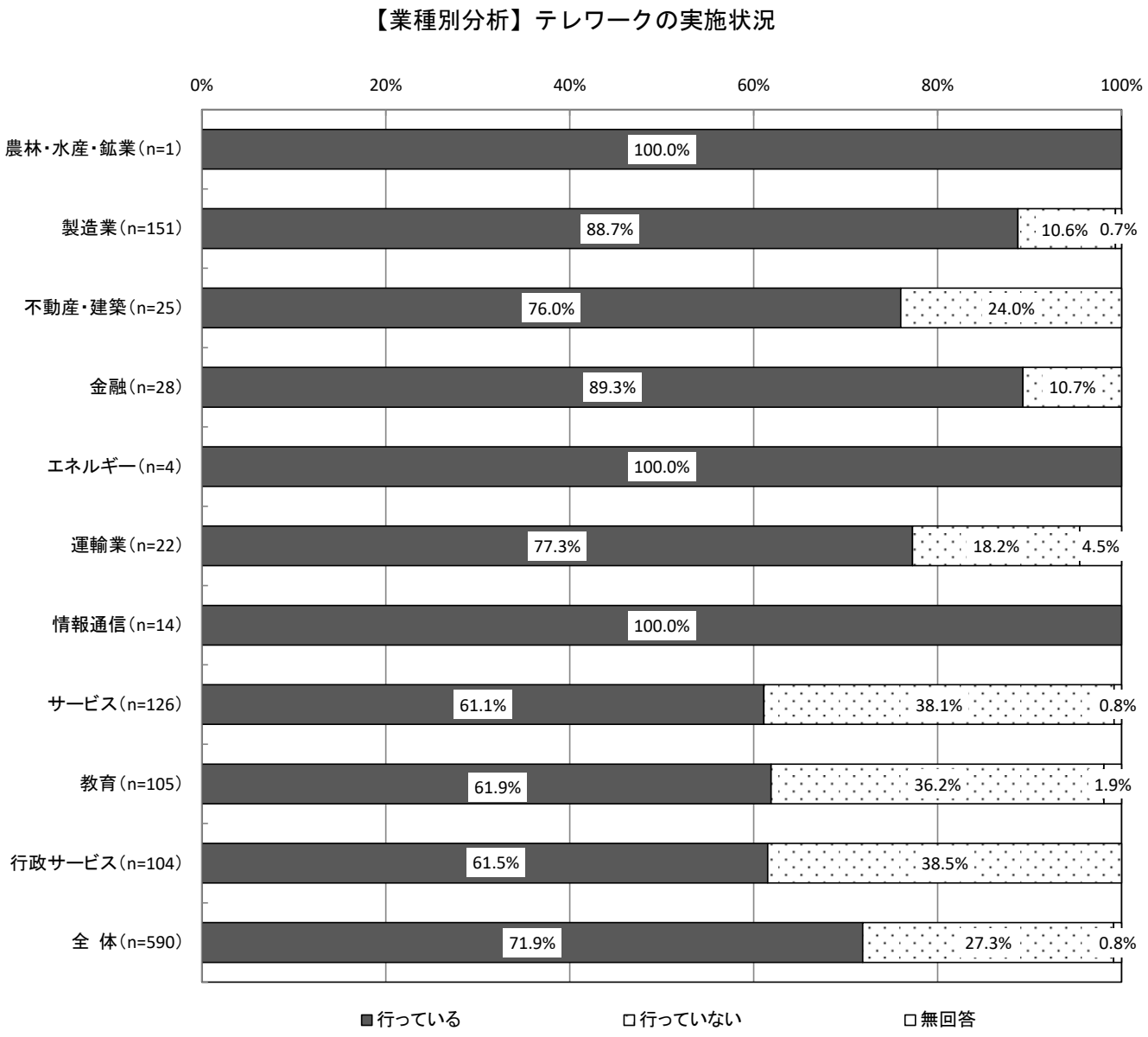
3.1.4　テレワークの実施状況　【問6】

テレワークの実施状況については、「行っている」が71.9%と高くなっている。これに対して、「行っていない」は、27.3%となっている。

【全体】テレワークの実施状況（SA,n=590）

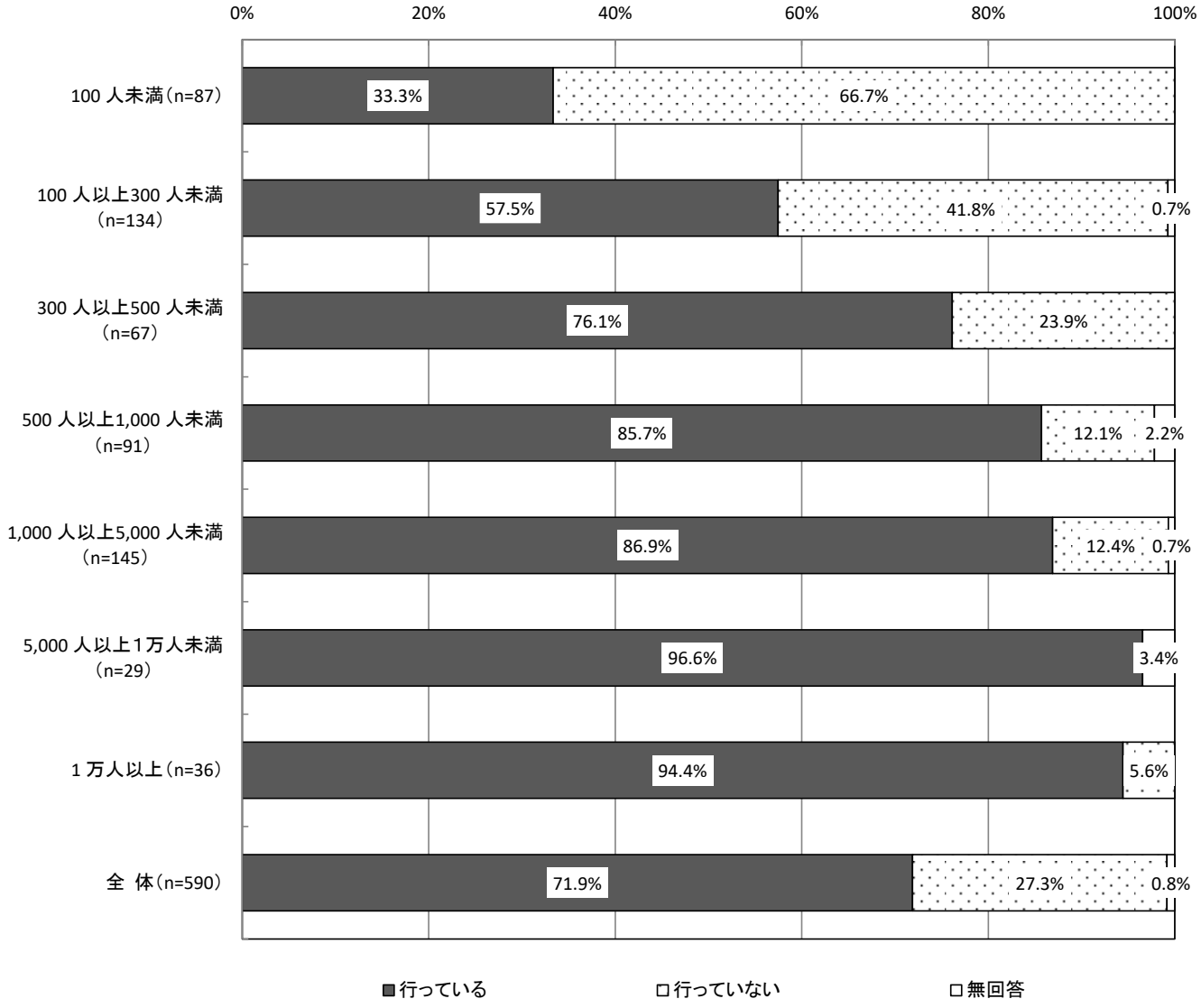


【業種別分析】業種別にみると、「行っている」は、「情報通信」が100.0%で高く、次いで「金融」が89.3%、「製造業」が88.7%となっている。一方、最も低いのは「行政サービス」で38.5%で、「サービス」も38.1%とほぼ同じ割合となっている。



【従業員規模別分析】従業員規模別にみると、「行っている」では、「5,000人以上１万人未満」が96.6%、「１万人以上」が94.4%で9割を超えて高くなっている。「行っている」割合はおおむね従業員数規模が大きいほど高くなっている。従業員規模が「100人未満」で33.3%と最も低くなっている。

【従業員規模別分析】テレワークの実施状況

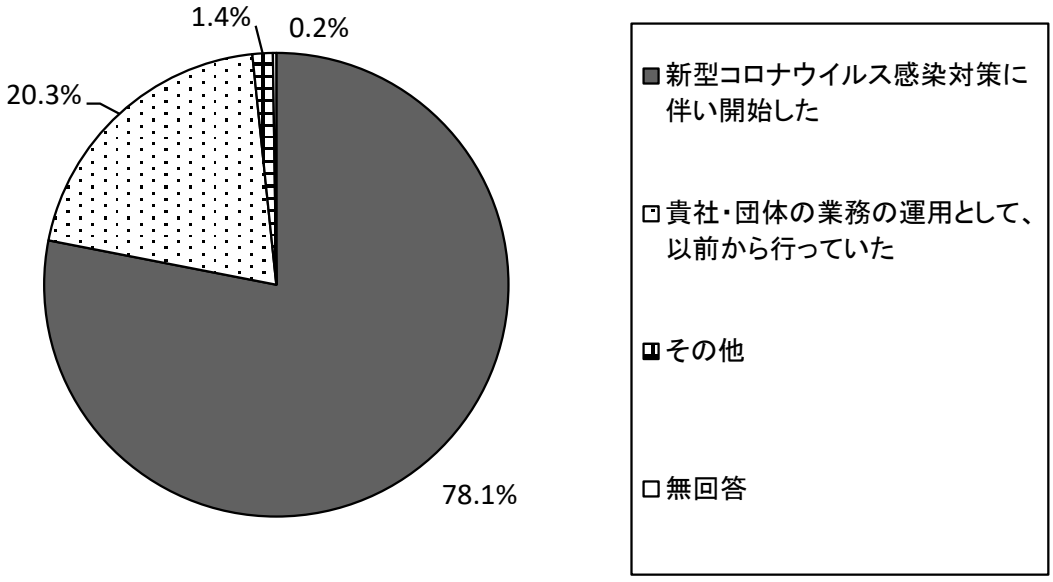


3.1.5　テレワークの開始時期　【問6-1】

テレワークの開始時期については、「新型コロナウイルス感染拡大に伴い開始した」が78.1%、「貴社・団体の業務の運用として、以前から行っていた」が20.3%となっている。

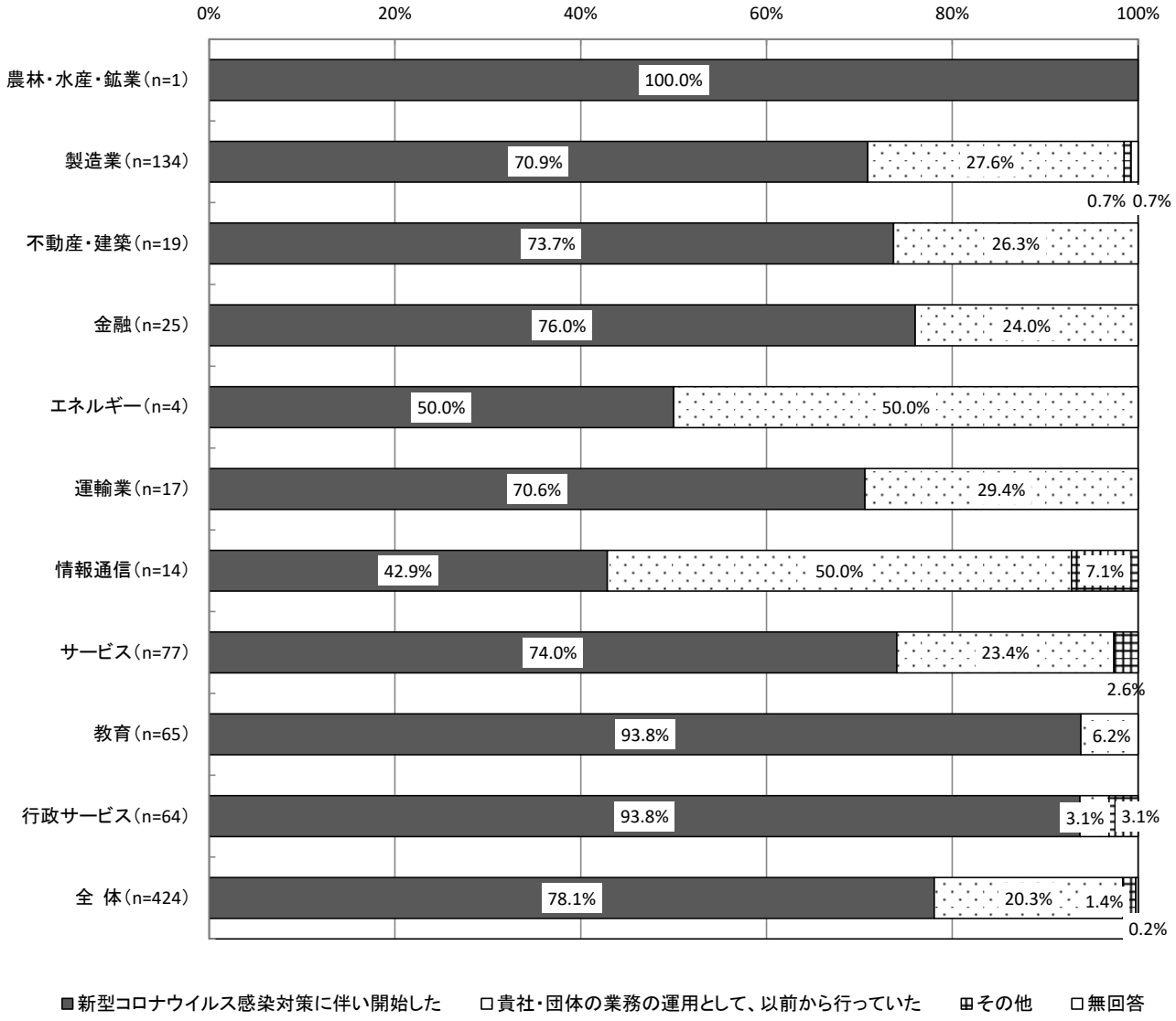
※本項目は、テレワークを実施している社・団体等を対象としている。

【全体】テレワークの開始時期（SA,n=424）



【業種別分析】業種別にみると、新型コロナウイルス感染拡大に伴い開始した」では、「教育」と「行政サービス」がいずれも93.8%で高くなっている。一方、最も低いのは「情報通信」で、42.9%となっている。

【業種別分析】テレワークの開始時期

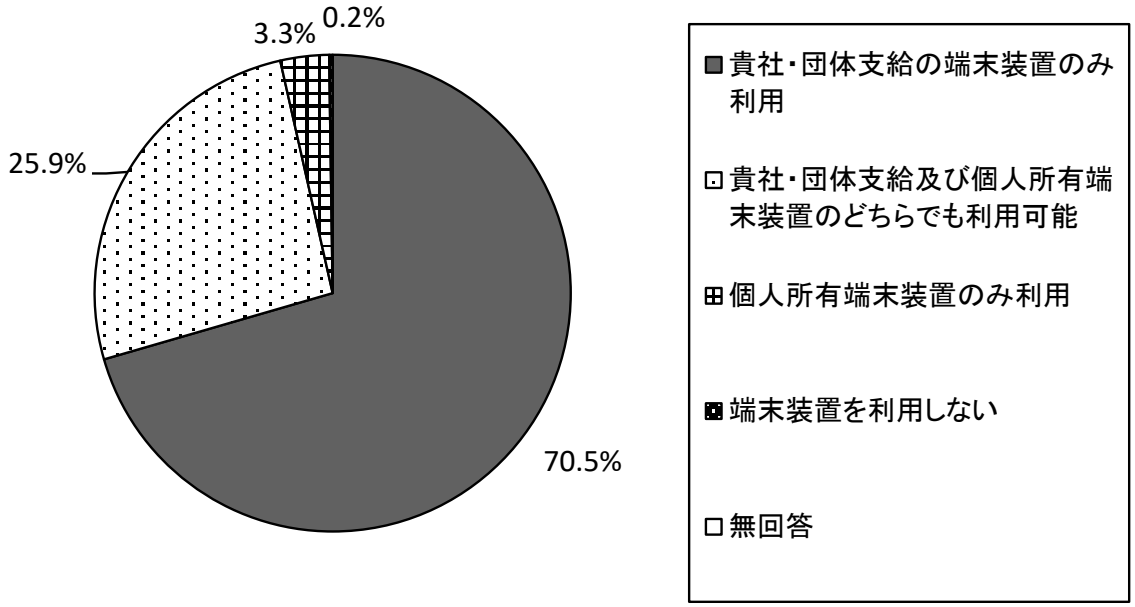


3.1.6　テレワーク業務の端末装置（パソコン、スマートフォン等）の利用環境　【問6-2】

テレワーク業務の端末装置（パソコン、スマートフォン等）の利用環境については、「貴社・団体支給の端末装置のみ利用」が70.5%で最も高く、「貴社・団体支給及び個人所有端末装置のどちらでも利用可能」が25.9%、「個人所有端末装置のみ利用」が3.3%となっている。

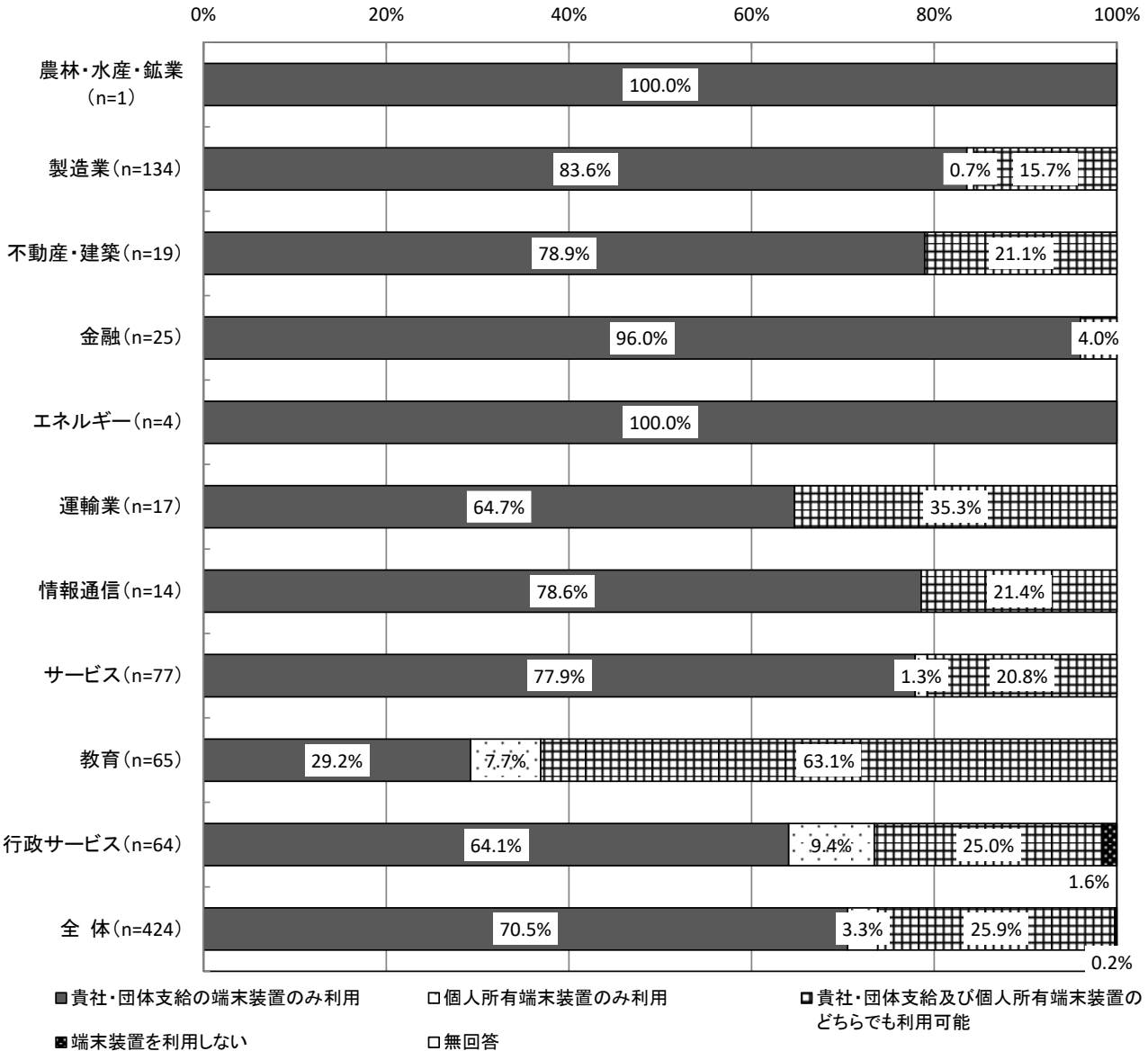
※本項目は、テレワークを実施している社・団体等を対象としている。

【全体】テレワーク業務の端末装置（パソコン、スマートフォン等）の利用環境（SA,n=424）



【業種別分析】業種別にみると、「貴社・団体支給の端末装置のみ利用」では、「金融」が96.0%、「製造業」が83.6%で高い。一方で、「教育」は29.2%で最も低くなっている。

【業種別分析】テレワーク業務の端末装置（パソコン、スマートフォン等）の利用環境

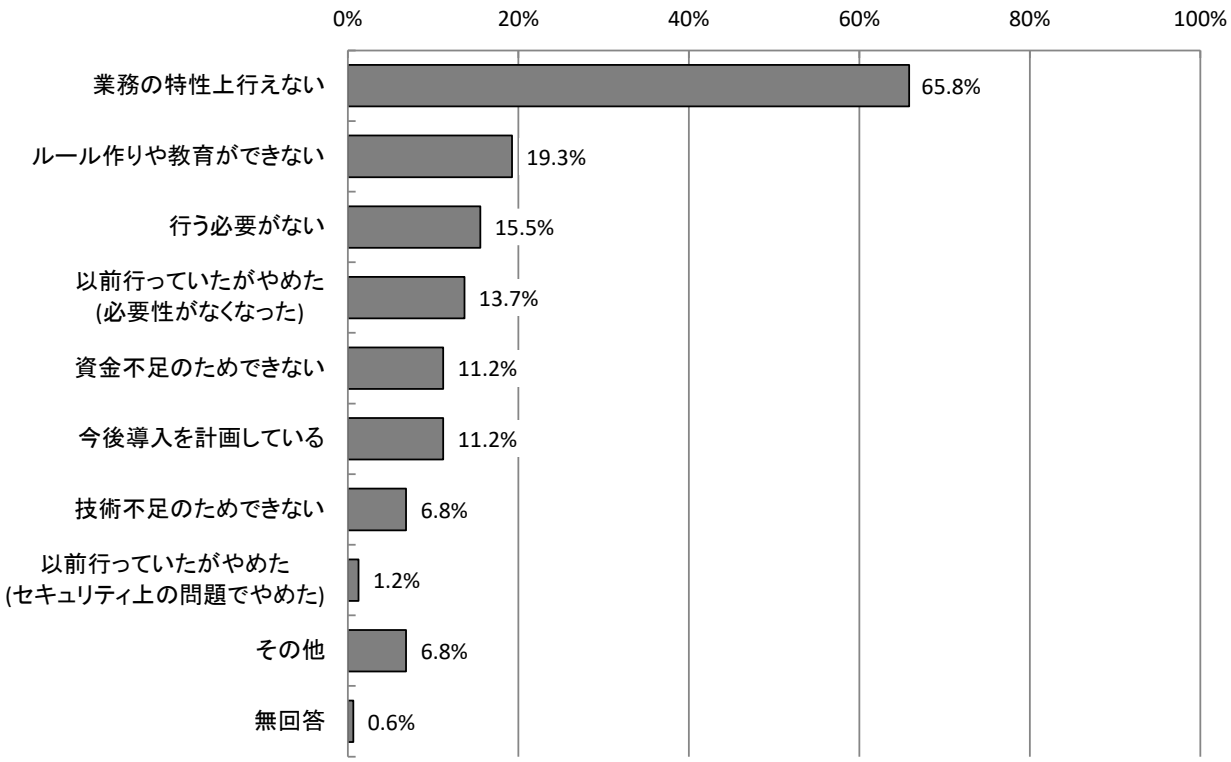


3.1.7　テレワークを行っていない理由　【問6-3】

テレワークを行っていない理由については、「業務の特性上行えない」が65.8%で最も高くなっている。次いで「ルール作りや教育ができない」が19.3%、「行う必要がない」が15.5%となっているが、「業務の特性上行えない」との差は大きくなっている。

※本項目は、テレワークを実施していない社・団体等を対象としている。

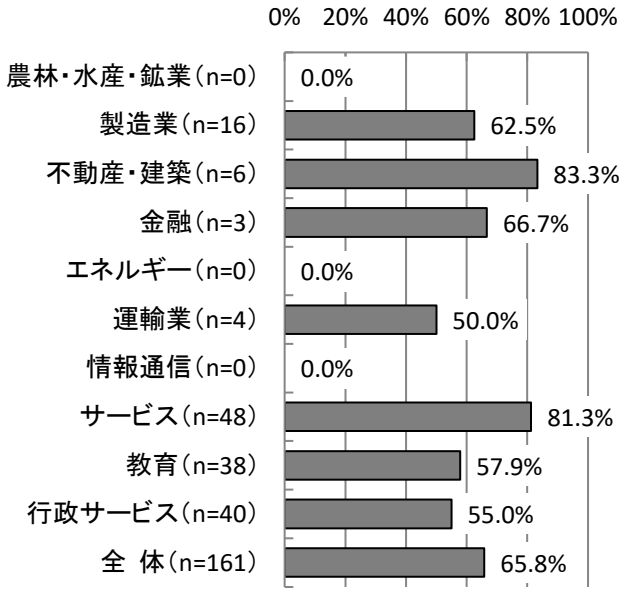
【全体】テレワークを行っていない理由（MA, n=161）



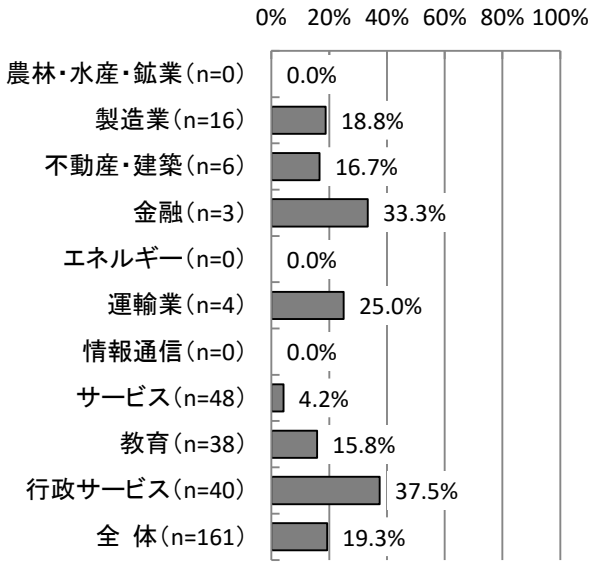
【業種別分析】業種別にみると、「業務の特性上行えない」では、「不動産・建築」が83.3%で最も高く、次いで「サービス」も81.3%と8割を超えている。一方、「運輸業」では50.0%と最も低く、「行政サービス」の55.0%、「教育」の57.9%も6割未満と低くなっている。

【業種別分析】テレワークを行っていない理由

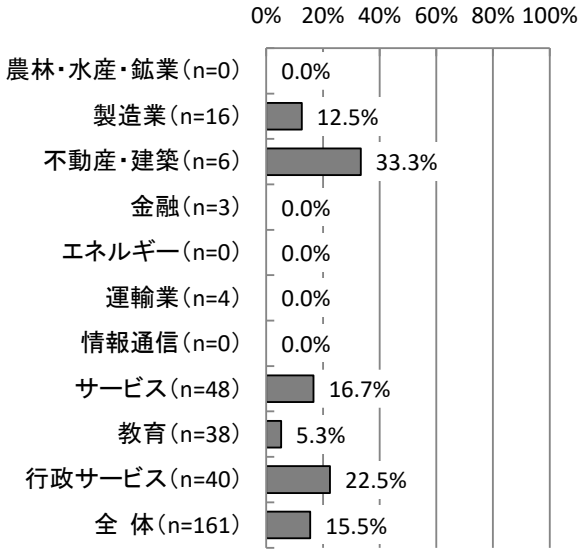
業務の特性上行えない



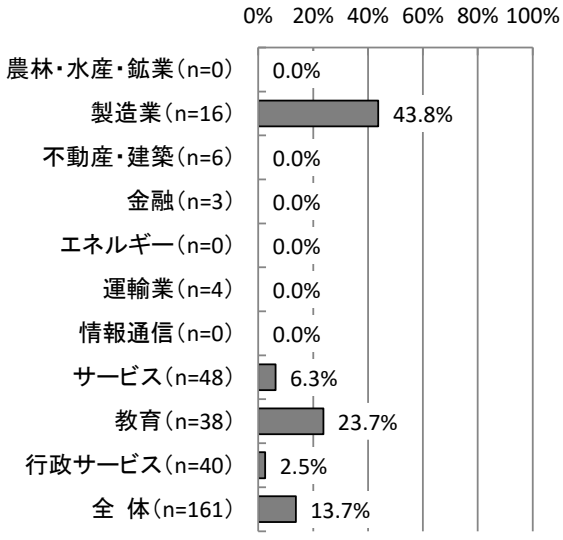
ルール作りや教育ができない



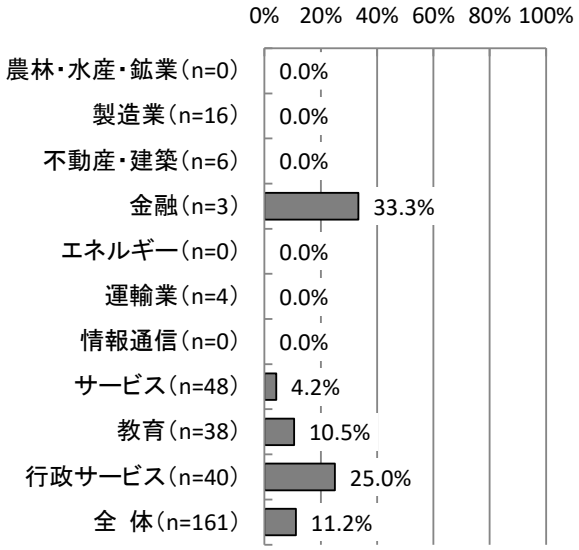
行う必要がない



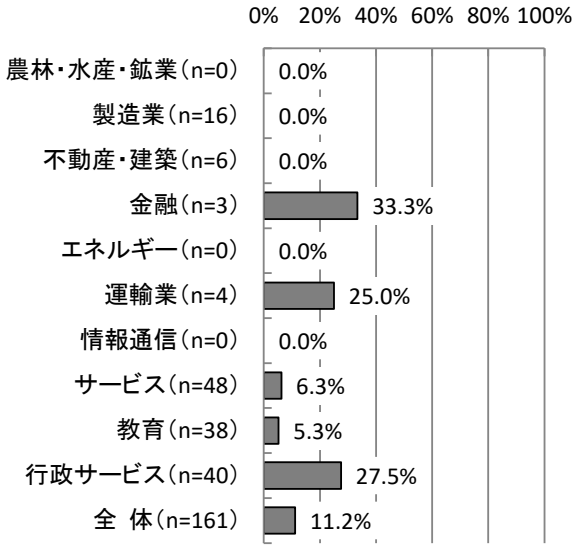
以前行っていたがやめた（必要性がなくなった）



資金不足のためできない



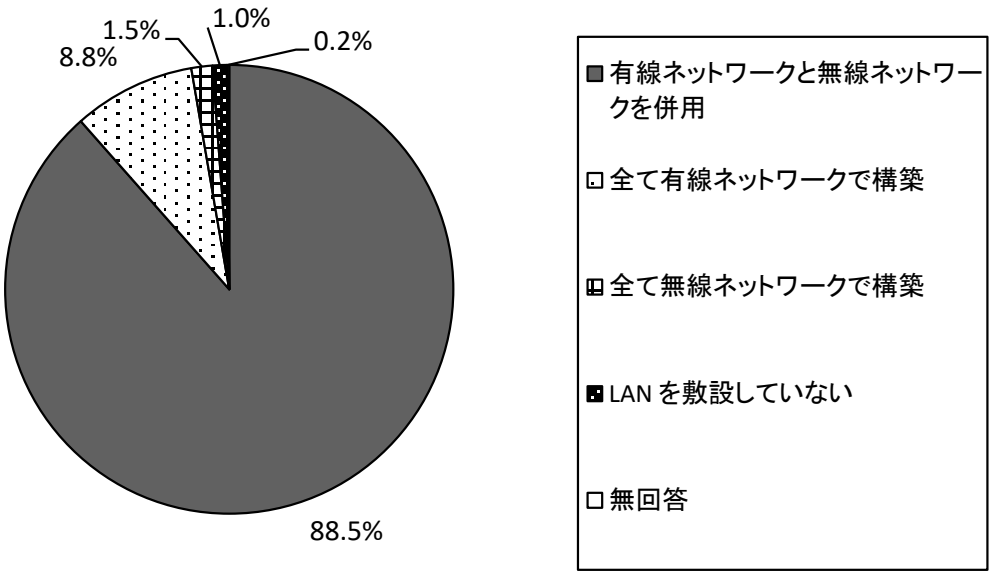
今後導入を計画している



3.1.8　事業体内のネットワーク利用状況　【問7】

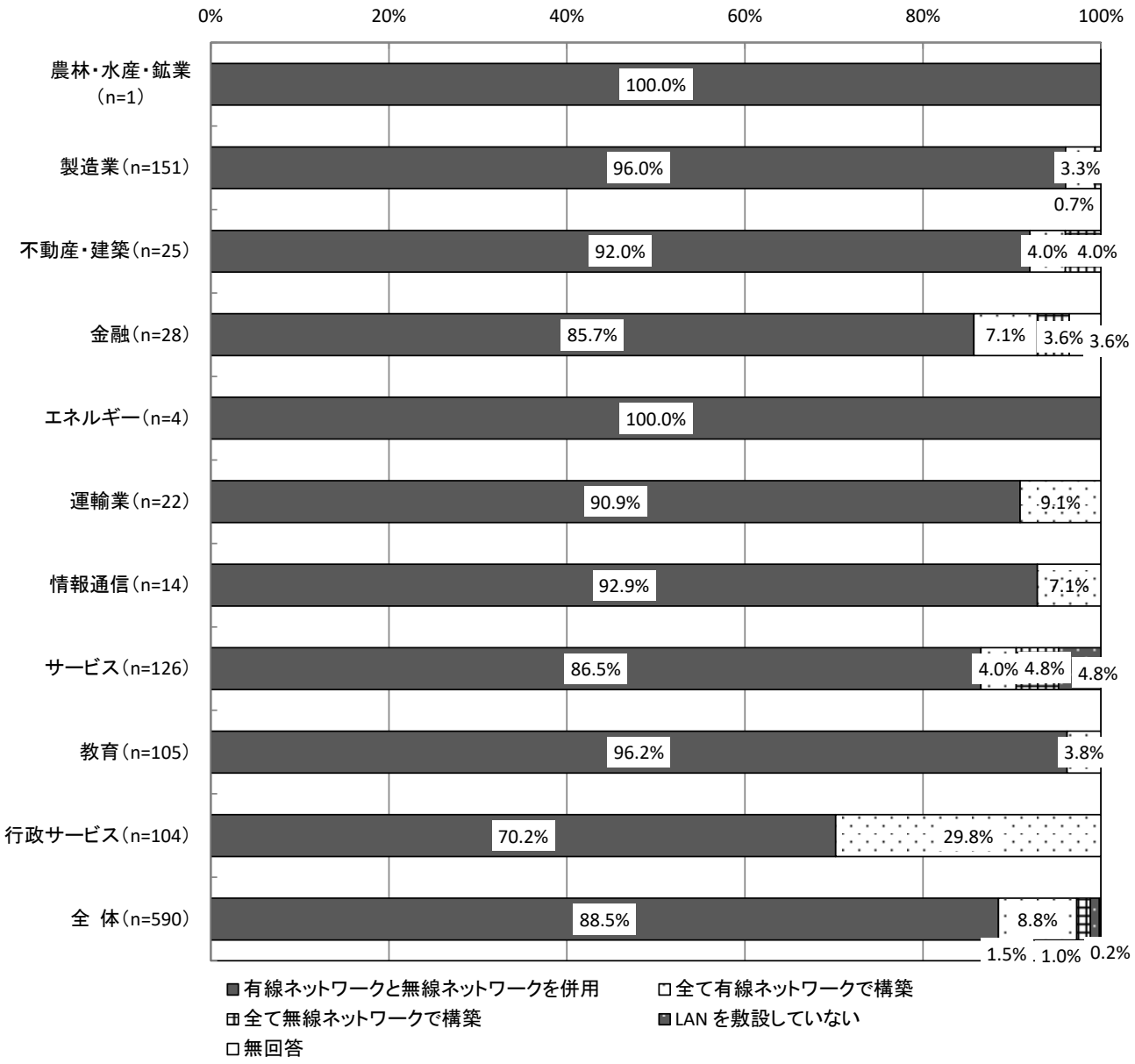
事業体内のネットワーク利用状況については、「有線ネットワークと無線ネットワークを併用」が88.5%で最も高く、次いで「全て有線ネットワークで構築」が8.8%となっている。

【全体】事業体内のネットワーク利用状況（SA,n=590）



【業種別分析】業種別にみると、「有線ネットワークと無線ネットワークを併用」については、「教育」で96.2%、「製造業」で96.0%と高くなっている。「全て有線ネットワークで構築」は「行政サービス」が29.8%で高くなっている。

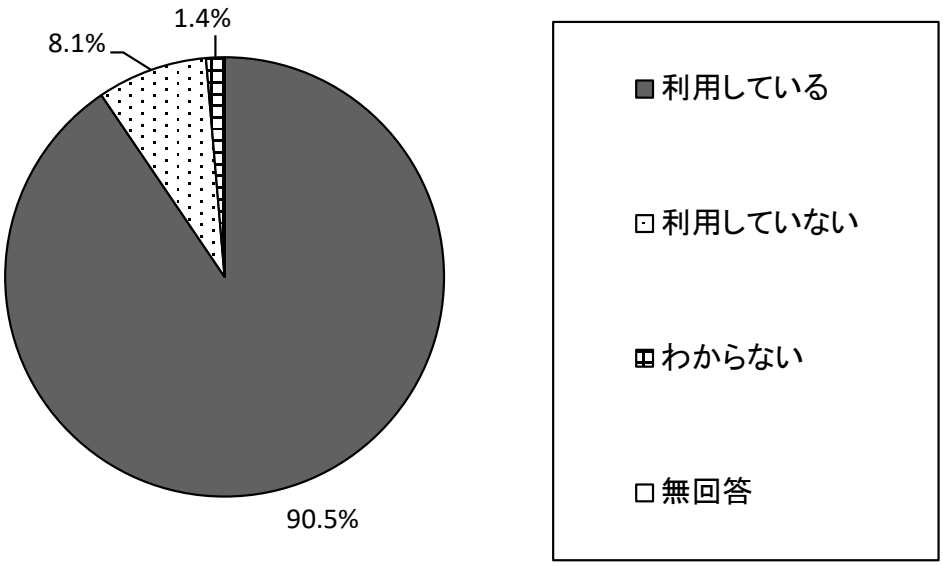
【業種別分析】事業体内のネットワーク利用状況



3.1.9　クラウドサービスの利用状況　【問8】

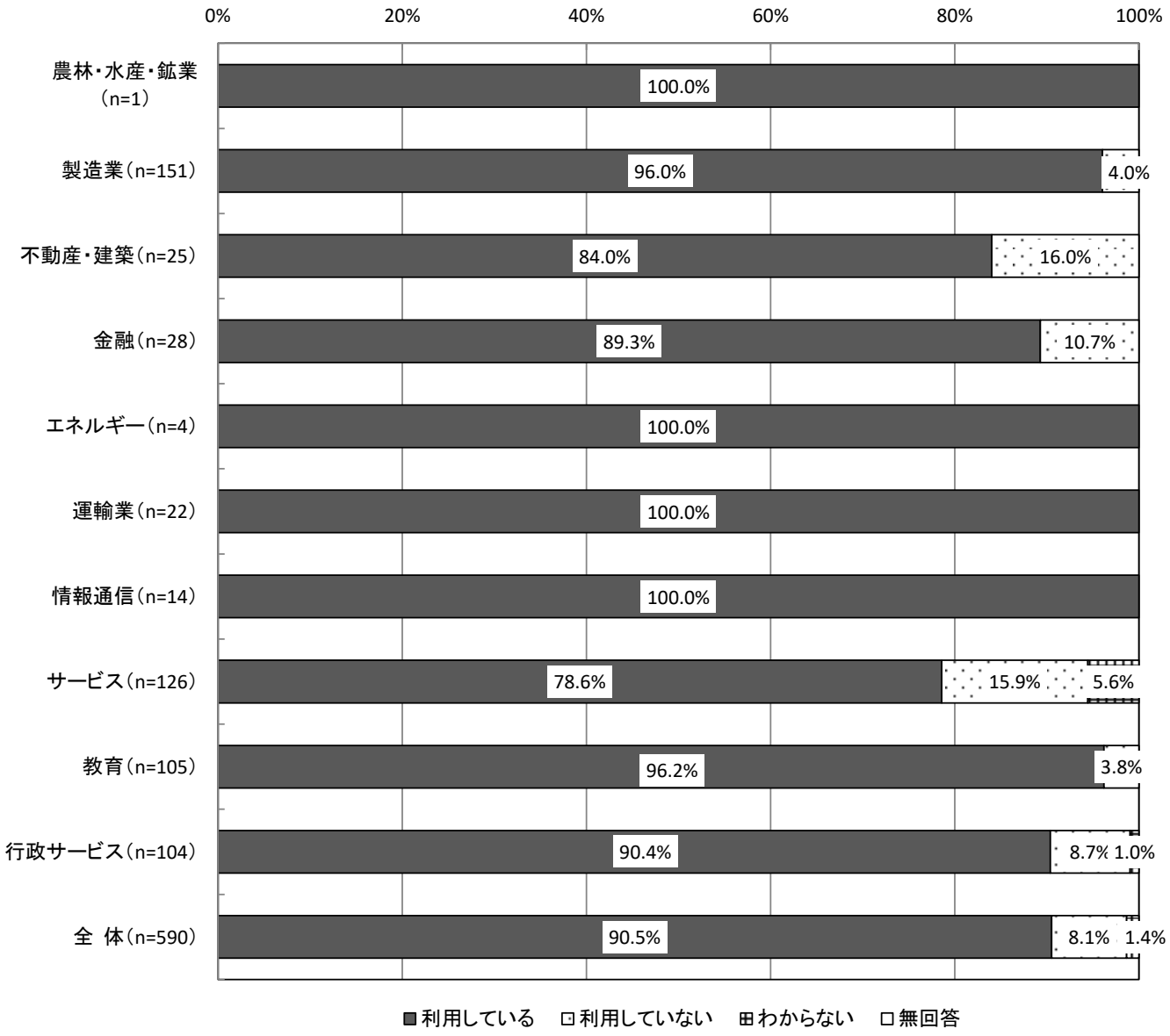
クラウドサービスの利用状況については、「利用している」が90.5%で最も高く、「利用していない」が8.1%、「わからない」が1.4%となっている。

【全体】クラウドサービスの利用状況（SA,n=590）



【業種別分析】業種別にみると、「使用している」については、「運輸業」「情報通信」などで100.0%と高く、次いで「教育」で96.2%、「製造」で96.0%と高くなっている。一方で「サービス」では78.6%と低くなっている。

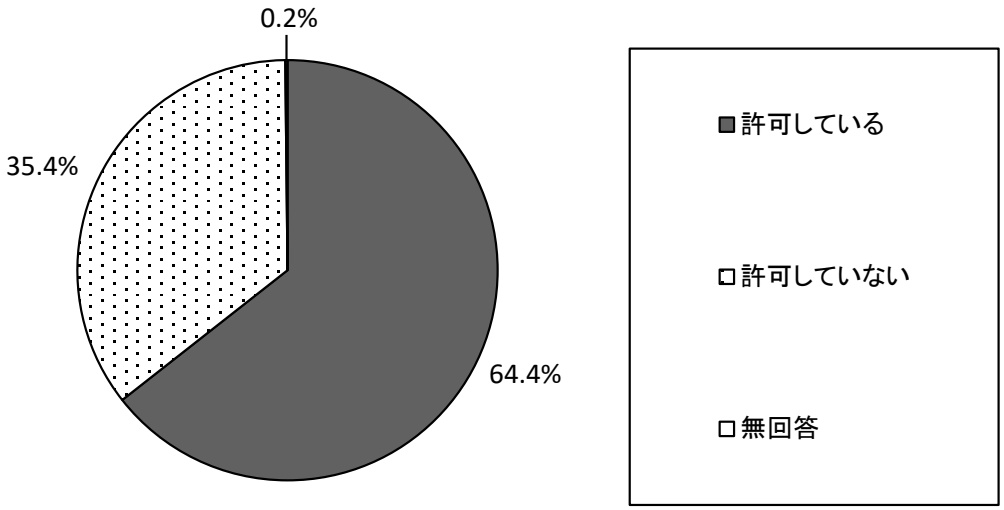
【業種別分析】クラウドサービスの利用状況



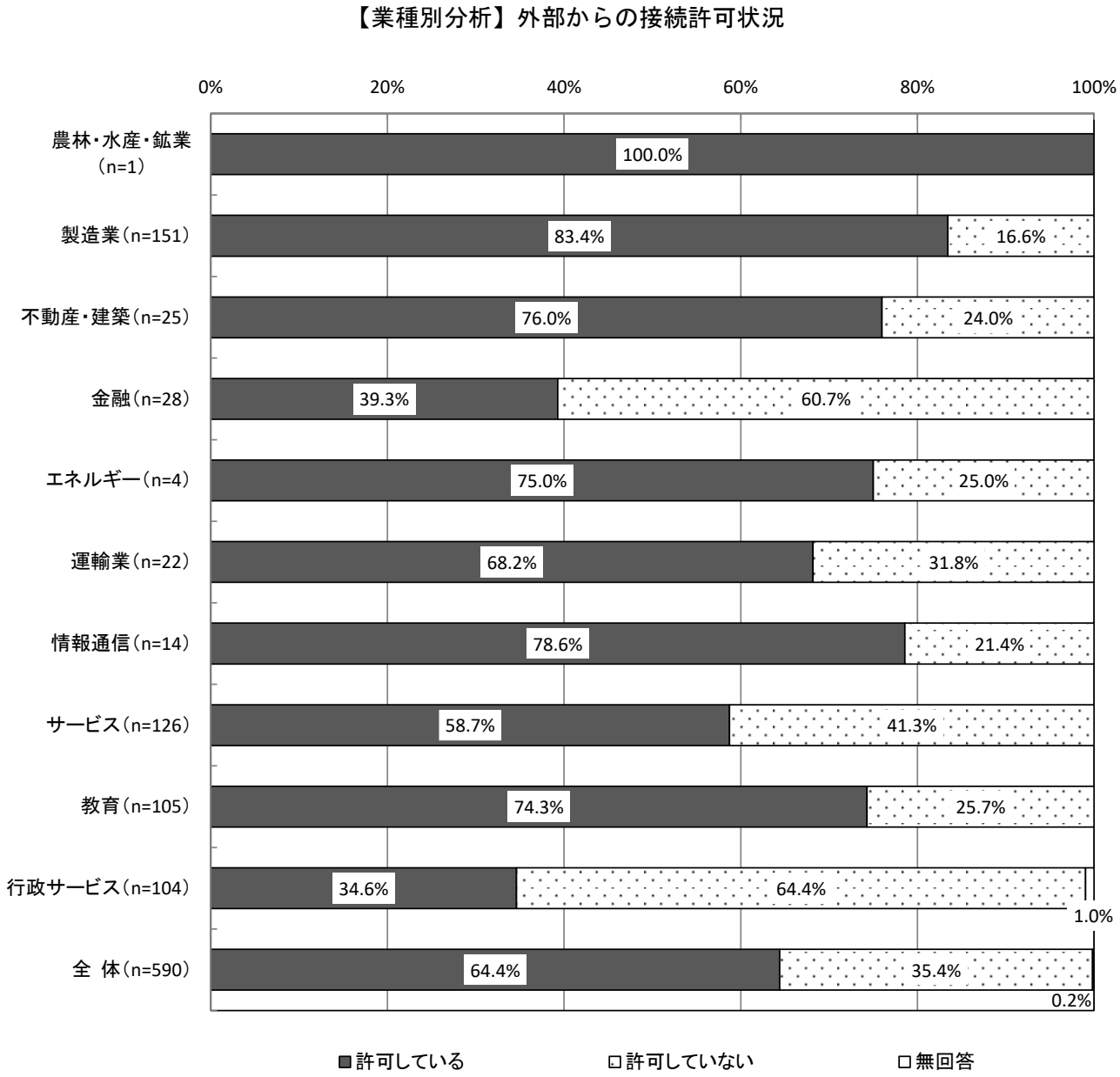
3.1.10　外部からの接続許可状況　【問9】

外部から事業体内ネットワークへの接続許可状況については、「許可している」が64.4%で高く、「許可していない」は35.4%となっている。

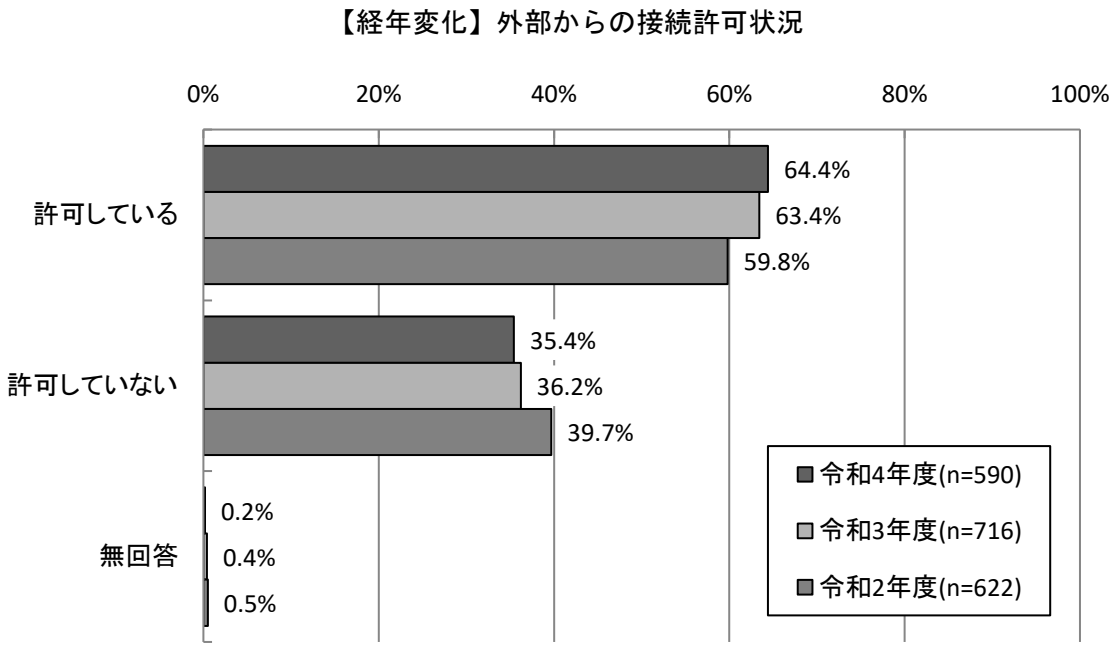
【全体】外部からの接続許可状況（SA,n=590）



【業種別分析】業種別にみると、「許可している」では、「製造業」の83.4%、「情報通信」の78.6%で高くなっている。一方「許可していない」は「行政サービス」が64.4%で最も高く、次いで「金融」が60.7%となっている。



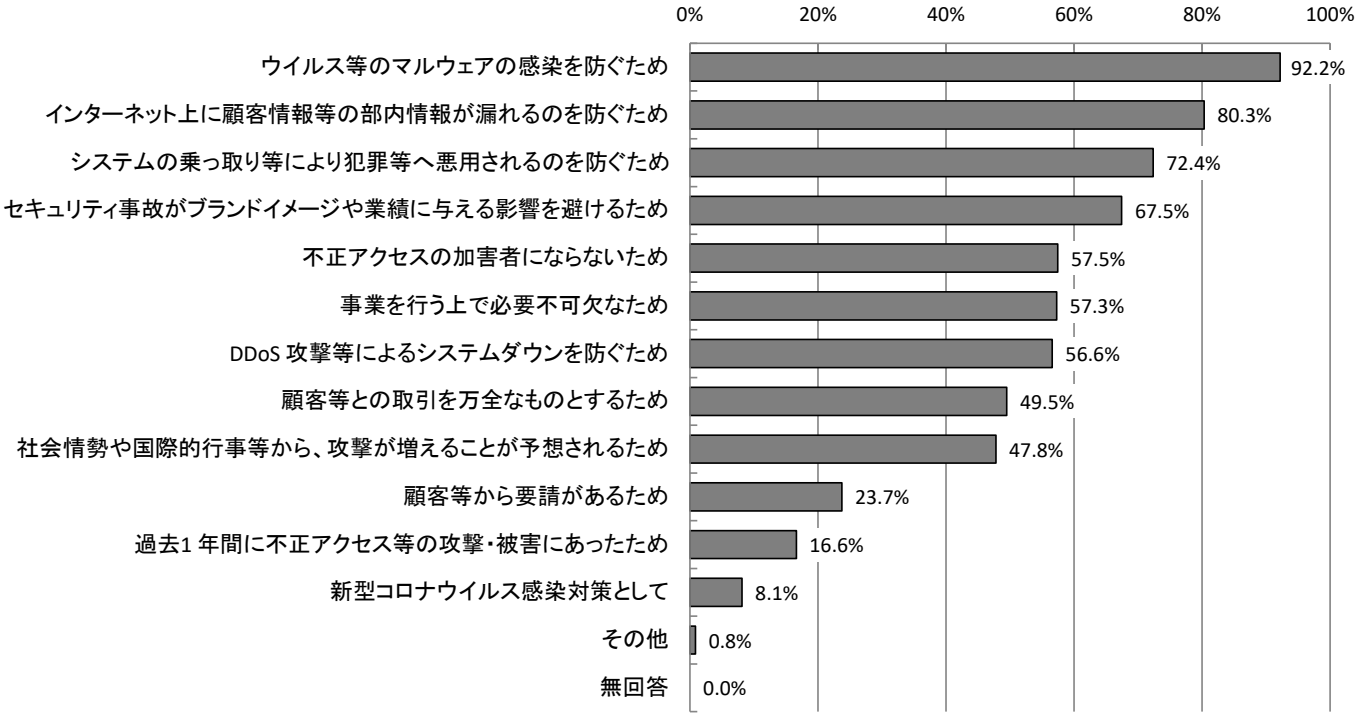
【経年変化】昨年度と比較すると、「許可している」が1.0ポイントの増加、「許可していない」が0.8ポイントの減少となっており、大きな変化はみられない。



3.1.11　情報セキュリティ対策の必要性の理由【問10】

情報セキュリティ対策の必要性の理由については、「ウイルス等のマルウェアの感染を防ぐため」が92.2%で最も高く、次いで「インターネット上に顧客情報等の部内情報が漏れるのを防ぐため」が80.3%、「システムの乗っ取り等により犯罪等へ悪用されるのを防ぐため」が72.4%、「セキュリティ事故がブランドイメージや業績に与える影響を避けるため」が67.5%となっている。

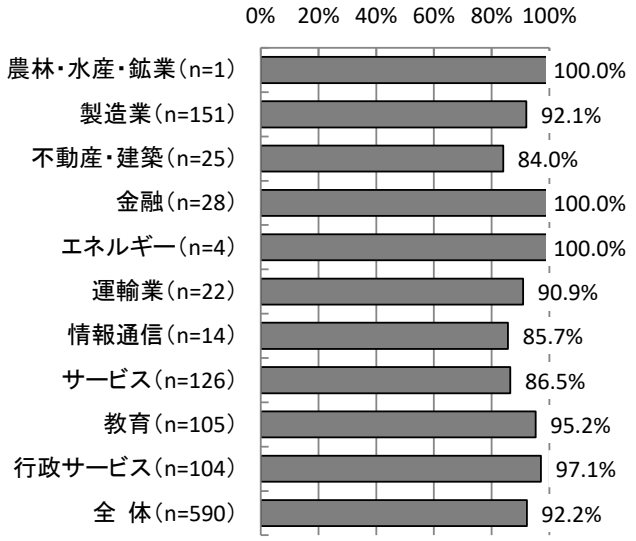
【全体】情報セキュリティ対策の必要性の理由（MA,n=590）



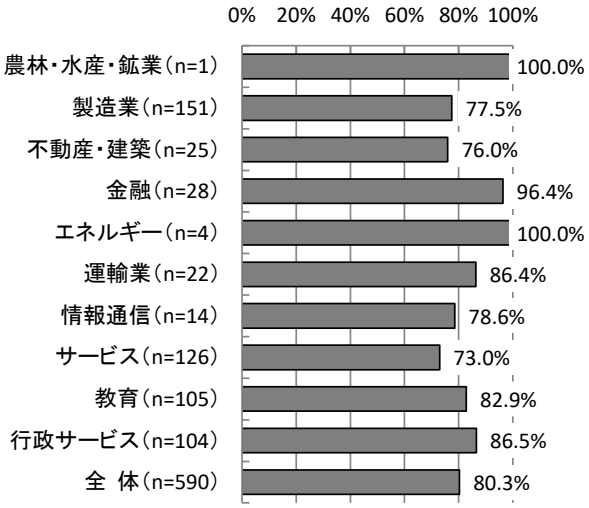
【業種別分析】業種別にみると、「金融」で「ウイルス等のマルウェアの感染を防ぐため」が、100.0%、「インターネット上に顧客情報等の部内情報が漏れるのを防ぐため」が96.4%、「システムの乗っ取り等により犯罪等へ悪用されるのを防ぐため」が89.3%、「セキュリティ事故がブランドイメージや業績に与える影響を避けるため」が92.9%、「事業を行う上で必要不可欠なため」が85.7%、「DDoS攻撃等によるシステムダウンを防ぐため」が96.4%、「顧客等との取引を万全なものとするため」が89.3%と高くなっている。「不正アクセスの加害者にならないため」については、「運輸業」の68.2%と「金融」の67.9%が高くなっている。

【業種別分析】情報セキュリティ対策の必要性の理由

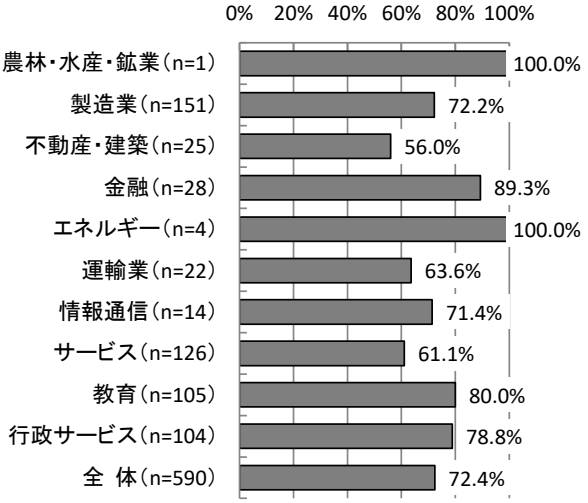
ウイルス等のマルウェアの感染を防ぐため



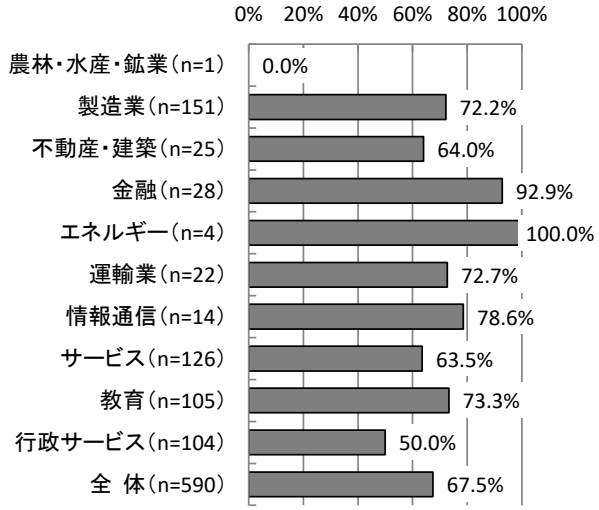
インターネット上に顧客情報等の部内情報が漏れるのを防ぐため



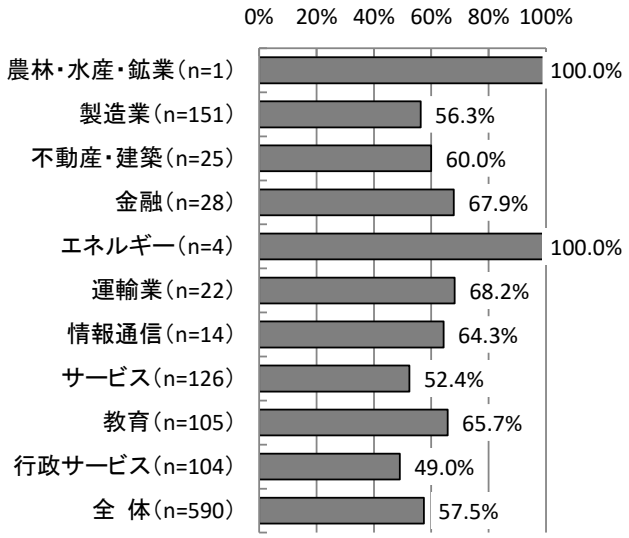
システムの乗っ取り等により犯罪等へ悪用されるのを防ぐため



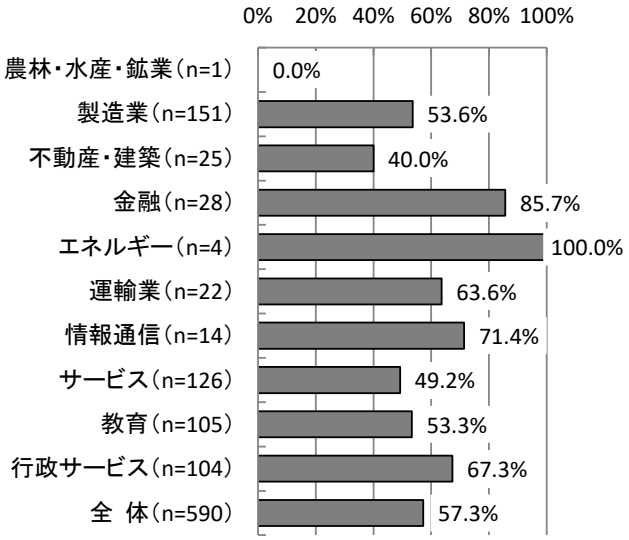
セキュリティ事故がブランドイメージや業績に与える影響を避けるため



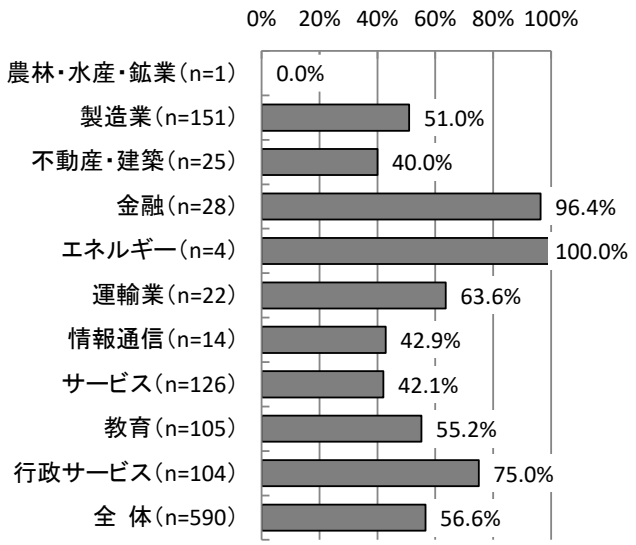
不正アクセスの加害者にならないため



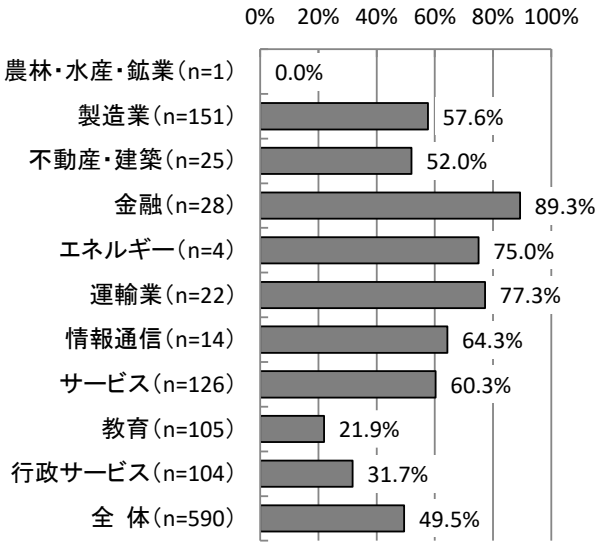
事業を行う上で必要不可欠なため



DDoS 攻撃等によるシステムダウンを防ぐため

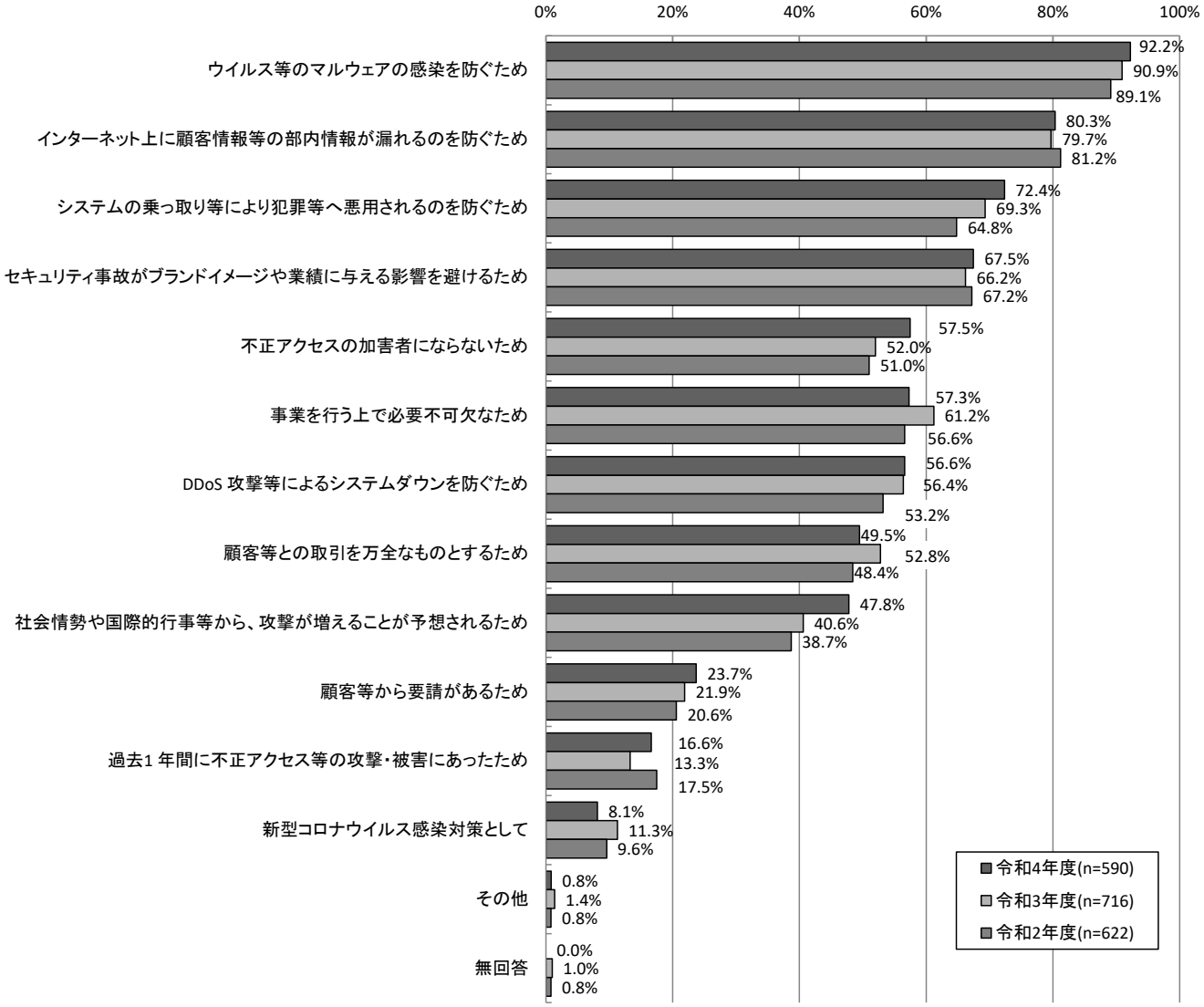


顧客等との取引を万全なものとするため



【経年変化】昨年度と比較すると、「社会情勢や国際的行事等から、攻撃が増えることが予想されるため」が7.2ポイント、「不正アクセスの加害者にならないため」が5.5ポイント増加し、「事業を行う上で必要不可欠なため」が3.9ポイント減少している。

【経年変化】情報セキュリティ対策の必要性の理由

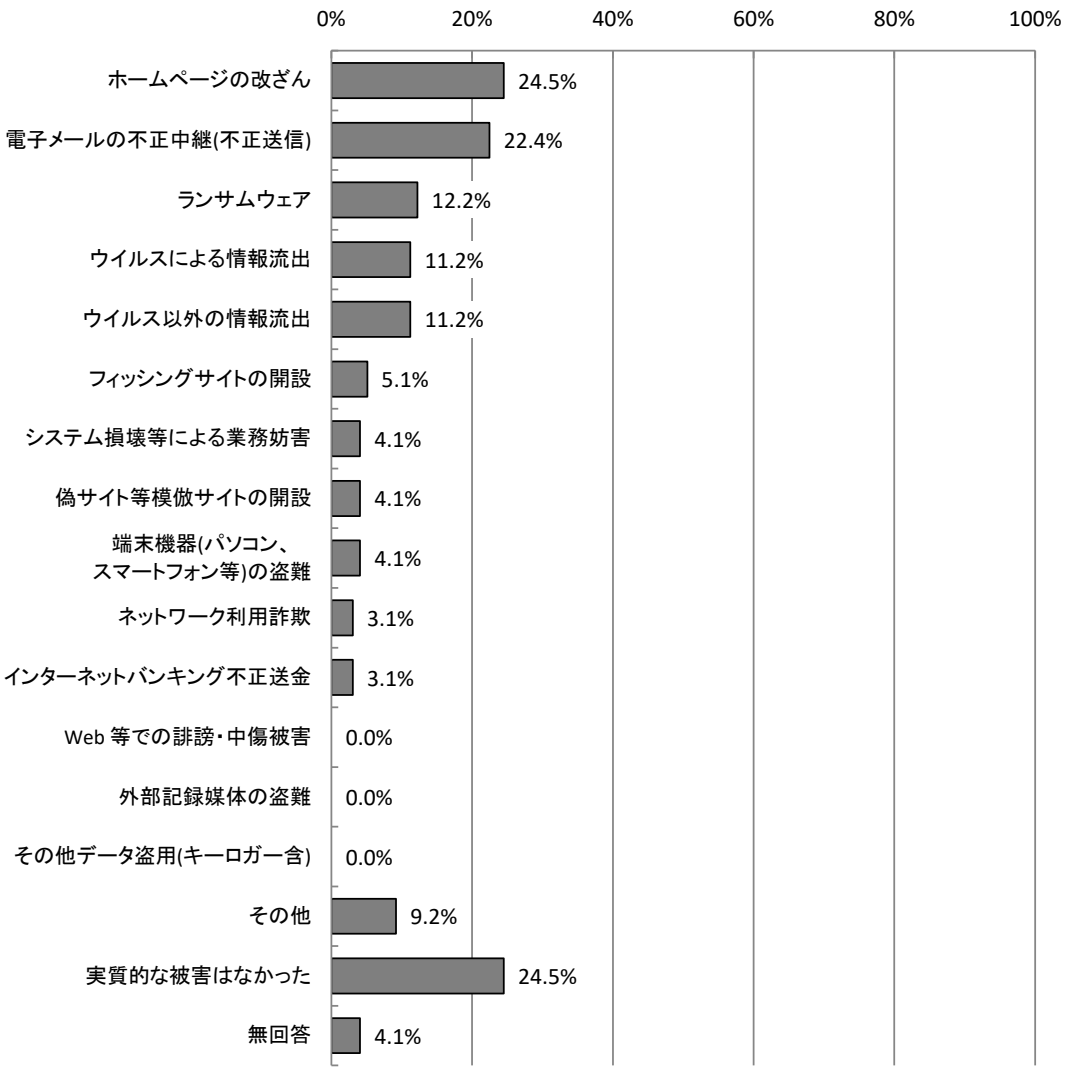


3.1.12　過去に受けたことのある被害状況　【問10-1-1】

過去に受けたことのある被害状況については、「ホームページの改ざん」が24.5%で最も高く、次いで「電子メールの不正中継」が22.4%、「ランサムウェア」が12.2%となっている。また、「実質的な被害はなかった」が24.5%となっている。

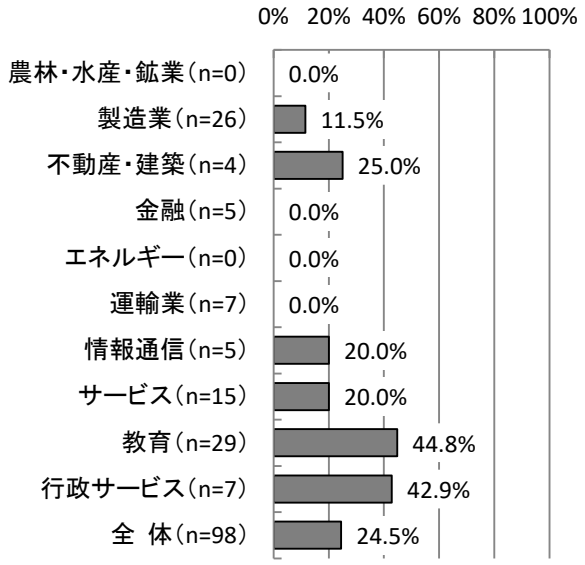
※本項目は、過去に不正アクセス等の被害にあった社・団体等を対象としている。

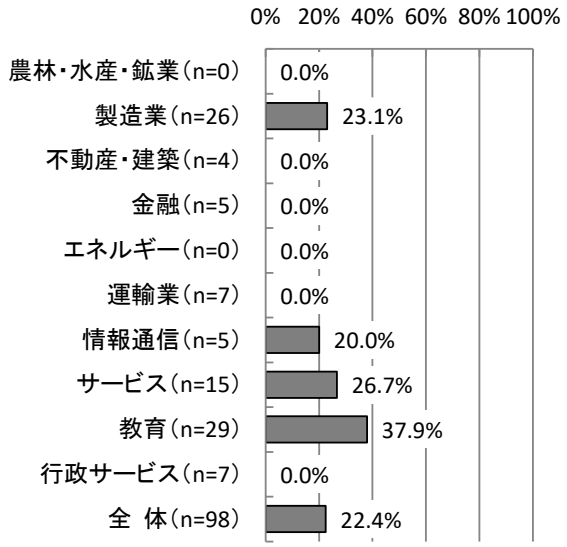
【全体】過去に受けたことのある被害状況（MA,n=98）

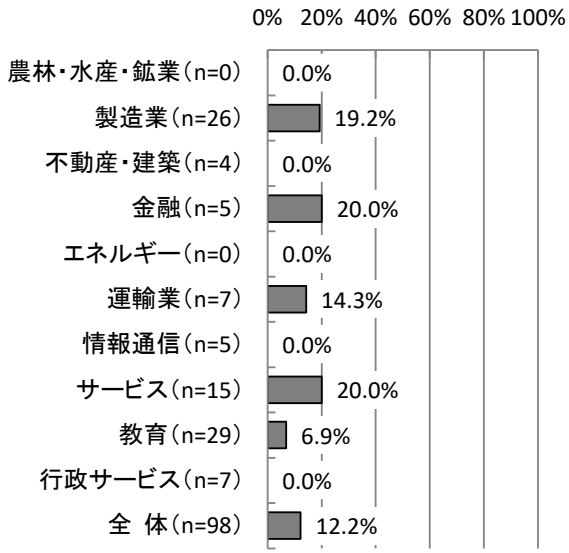


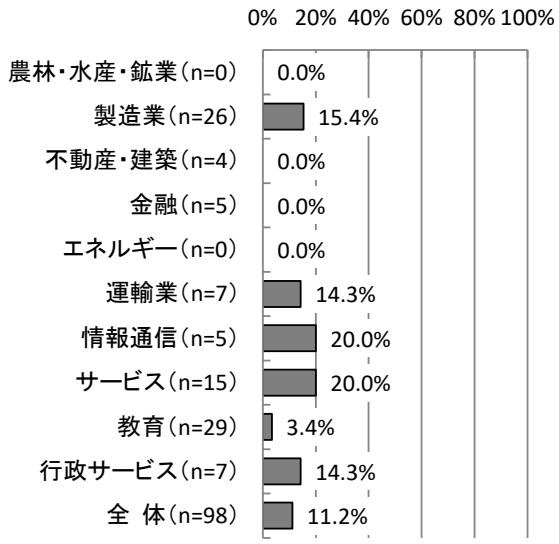
【業種別分析】業種別にみると、「ホームページの改ざん」については、「教育」の44.8%と「行政サービス」の42.9%が高い。「電子メールの不正中継」については、「教育」が37.9%となっている。また、「ランサムウェア」については、「金融」と「サービス」で20.0%と高くなっている。

【業種別分析】過去に受けたことのある被害状況



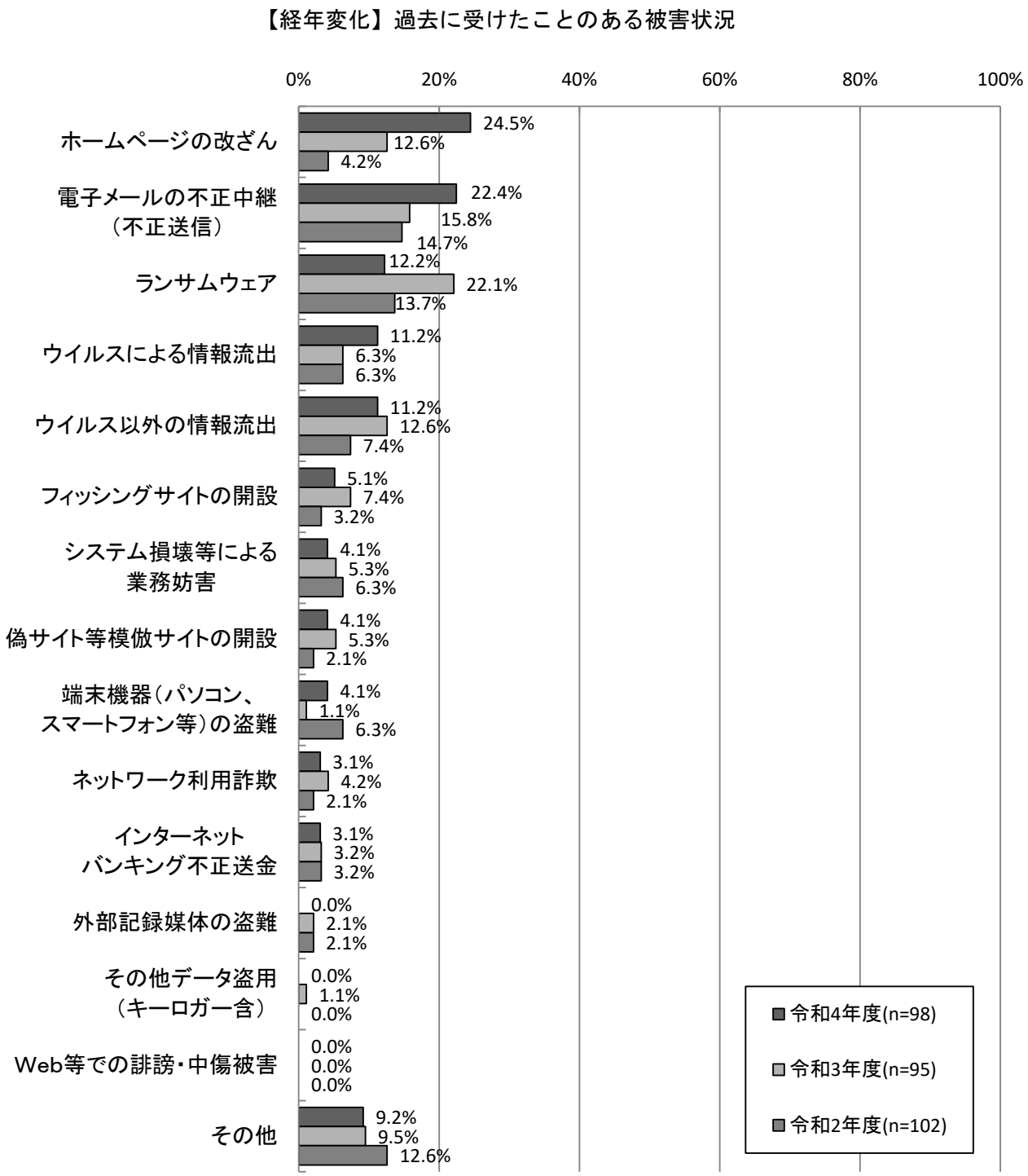






【経年変化】昨年度と比較すると、「ホームページの改ざん」が11.9%、「電子メールの不正中継（不正送信）」が6.6%増加している。一方、「ランサムウェア」は9.9ポイントの減少となっている。

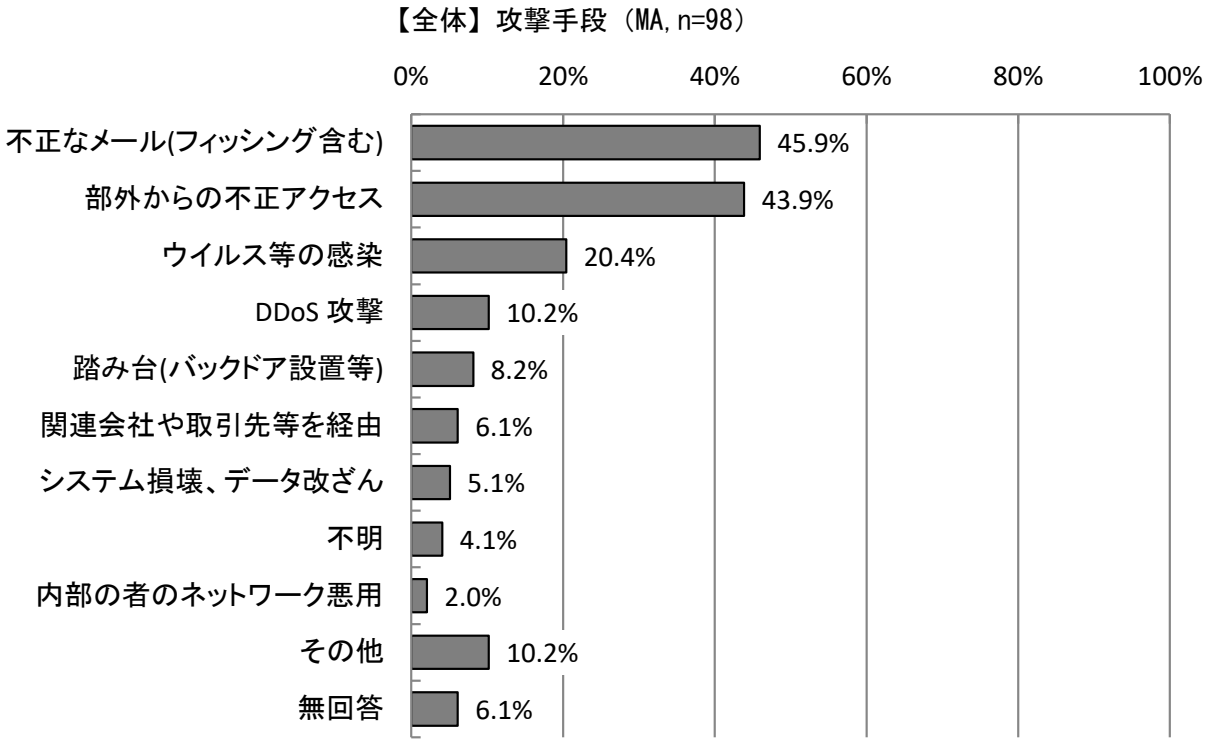
※「無回答」を除いた総数で比較している。



3.1.13　攻撃手段　【問10-1-2】

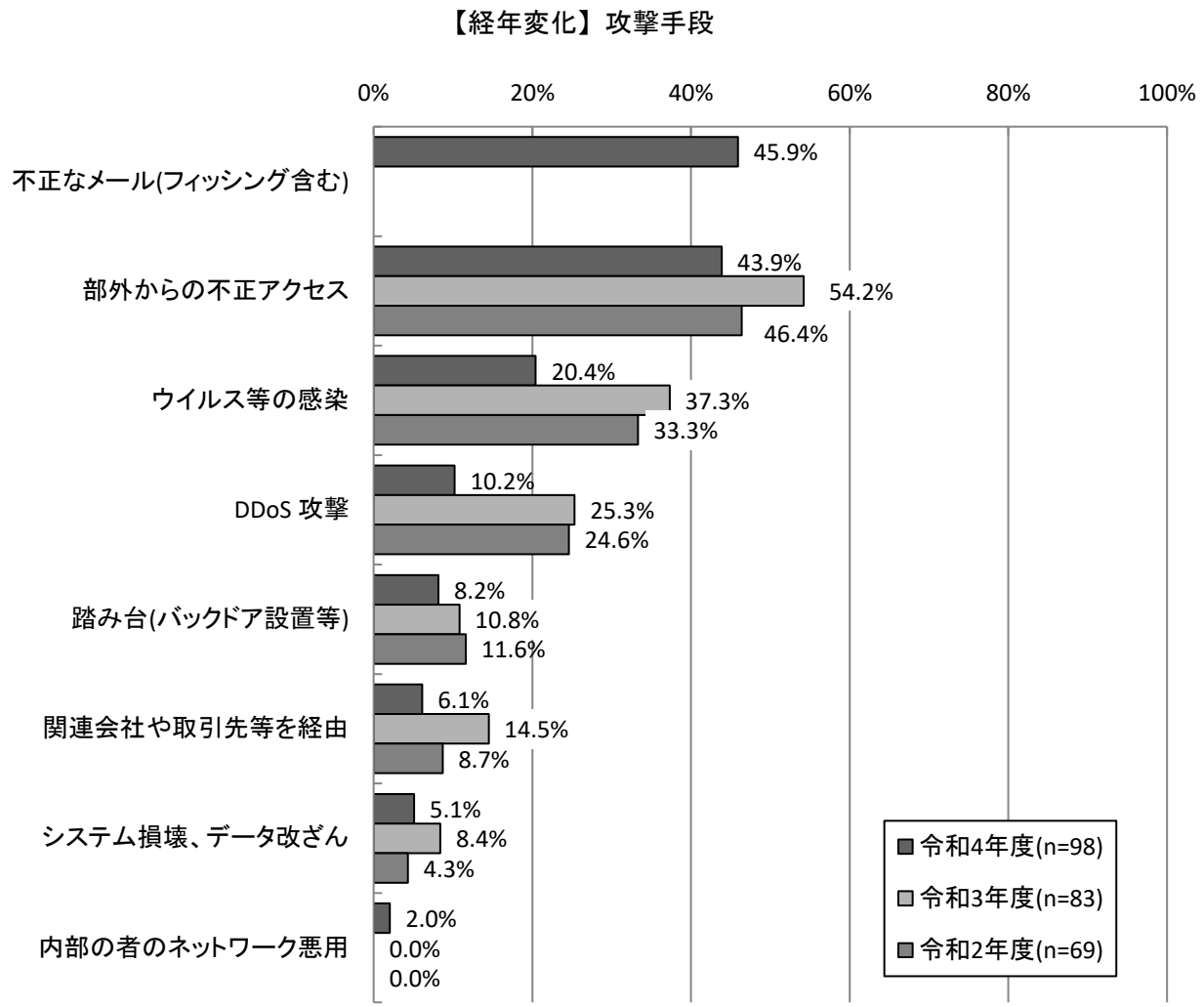
攻撃手段については、「不正なメール（フィッシング含む）」が45.9%で最も高く、次いで「部外からの不正アクセス」が43.9%、「ウイルス等の感染」が20.4%となっている。

※本項目は、過去に不正アクセス等の被害にあった社・団体等を対象としている。



【経年変化】昨年度と比較すると、「ウイルス等の感染」が16.9ポイント、「DDoS 攻撃」が15.1ポイント、「部外からの不正アクセス」が10.3ポイント減少するなど、「内部の者のネットワーク悪用」を除き、いずれの項目も減少している。

※「不明」「無回答」を除いた総数で比較している。



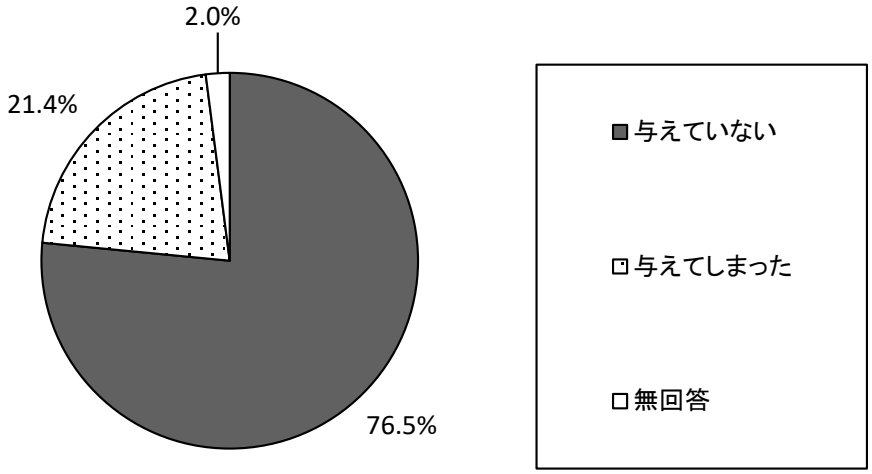
※「不正なメール（フィッシング含む）」は令和4年度から追加されている

3.1.14　関連会社や取引先等に被害を与えてしまったことがあるか　【問10-2】

不正アクセス等の被害によって被害を与えてしまったことがあるかについて、「与えていない」が76.5%で高くなっている。一方で「与えてしまった」は21.4%と2割を超えて一定の割合となっている。

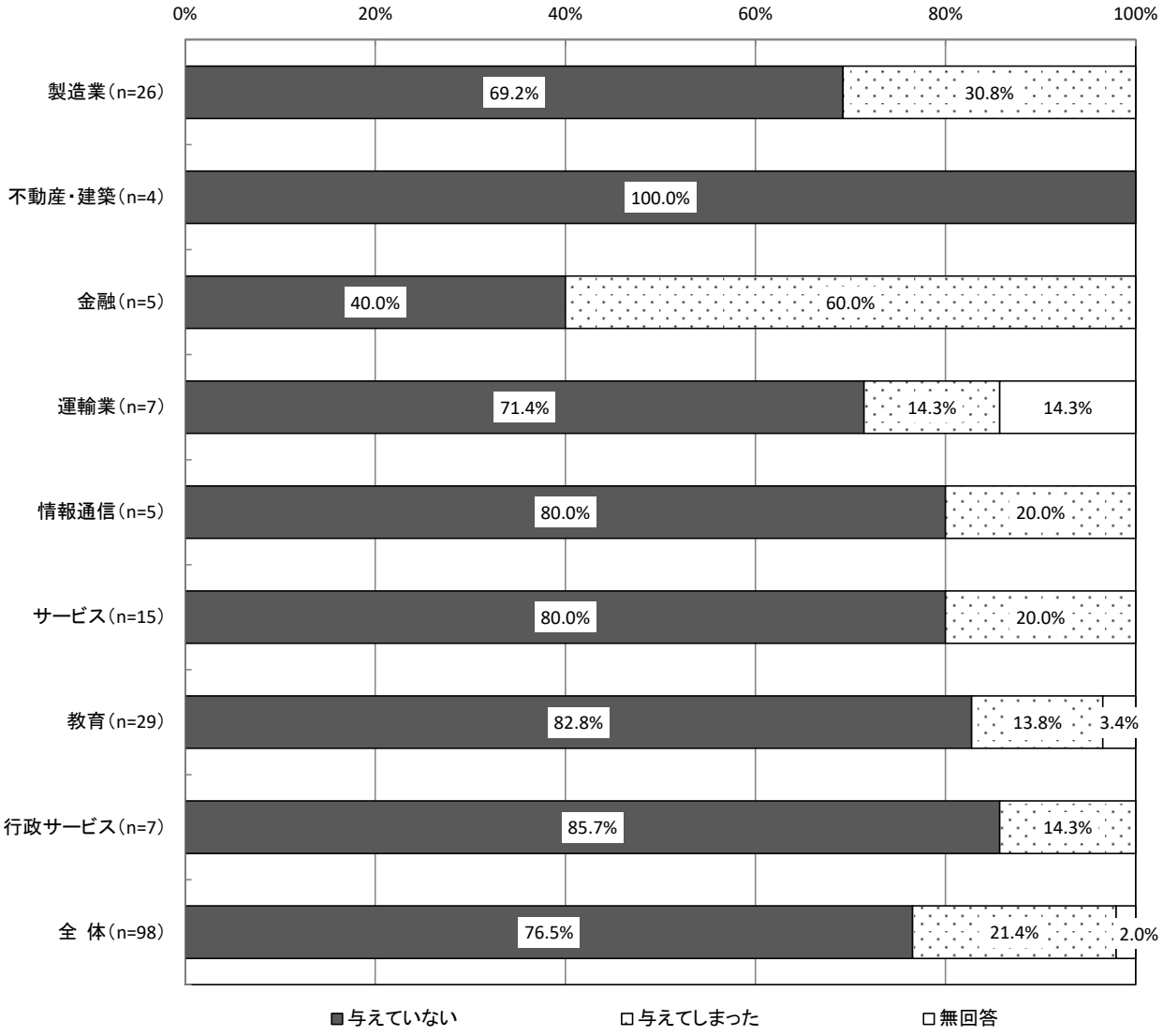
※本項目は、過去に不正アクセス等の被害にあった社・団体等を対象としている。

【全体】関連会社や取引先等に被害を与えてしまったことがあるか（MA,n=98）



【業種別分析】業種別にみると、「与えてしまった」が「金融」で5件中3件（60.0%）、「製造業」で30.8%と高くなっている。

【業種別分析】関連会社や取引先等に被害を与えてしまったことがあるか



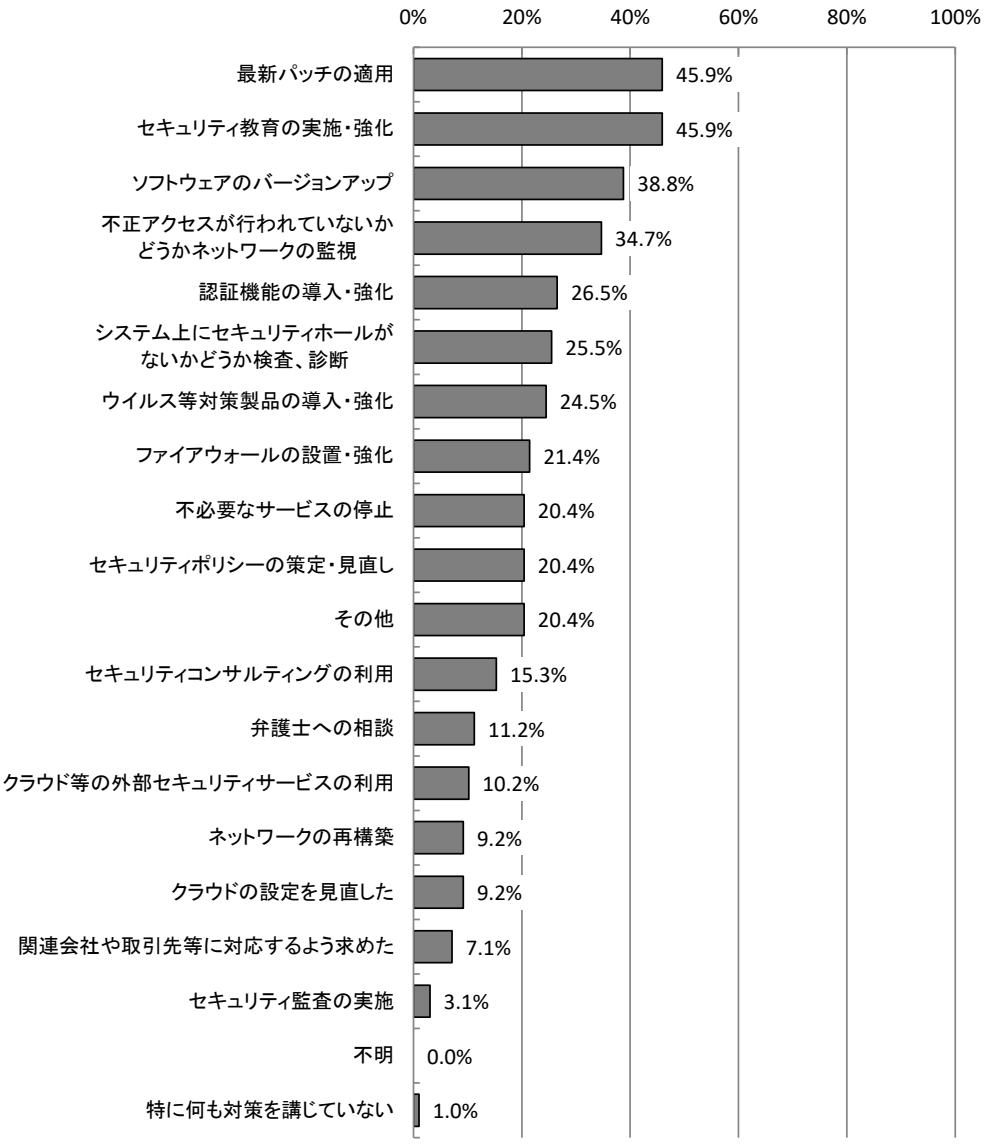
※「農林・水産・鉱業」、及び「エネルギー」は回答がない為除く

3.1.15　被害を受けたことによる対策　【問10-3】

被害を受けたことによる対策については、「最新パッチの適用」と「セキュリティ教育の実施・強化」が45.9%で最も高く、次いで「ソフトウェアのバージョンアップ」が38.8%、「不正アクセスが行われていないかどうかネットワークの監視」が34.7%となっている。

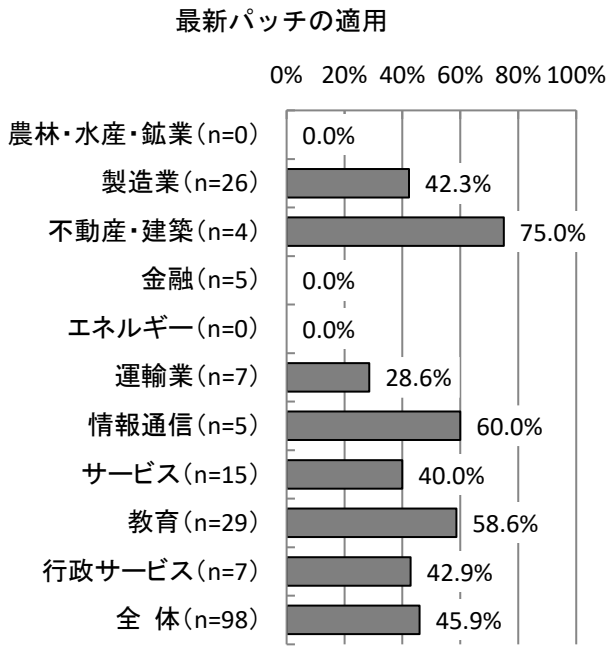
※本項目は、過去に不正アクセス等の被害にあった社・団体等を対象としている。

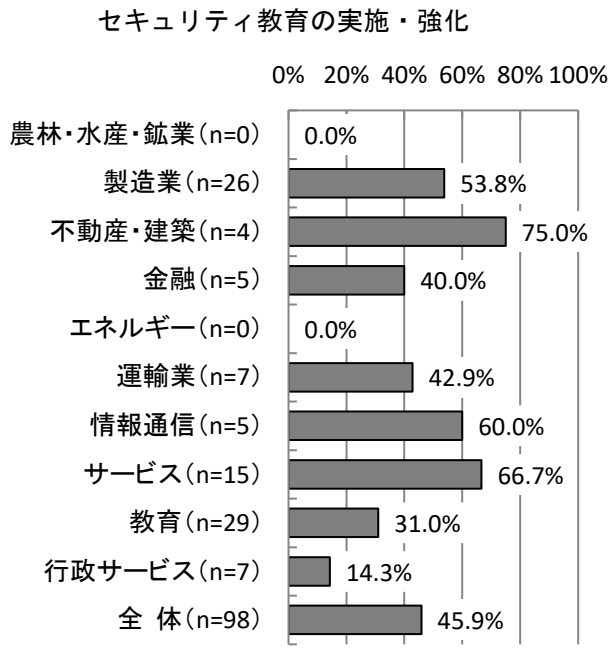
【全体】被害を受けたことによる対策（MA,n=98）

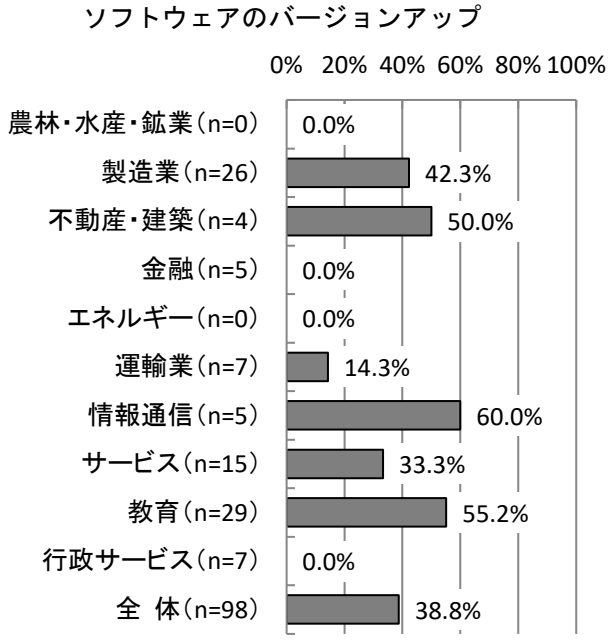


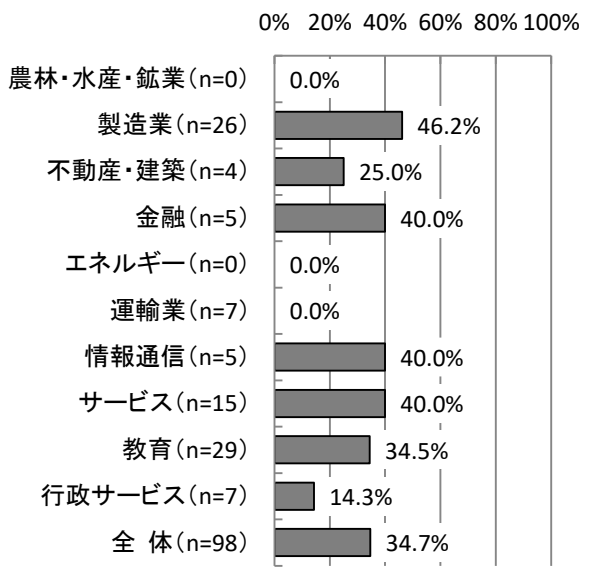
【業種別分析】業種別にみると、「最近パッチの適用」では「情報通信」の60.0%と「教育」の58.6%が高く、「セキュリティ教育の実施・強化」については、「サービス」の66.7%が高くなっている。また、「ソフトウェアのバージョンアップ」では、「情報通信」が60.0%で高くなっている。

【業種別分析】被害を受けたことによる対策

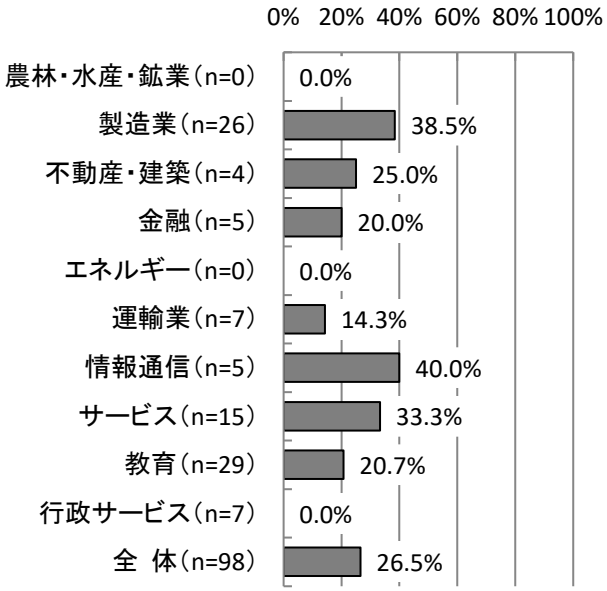




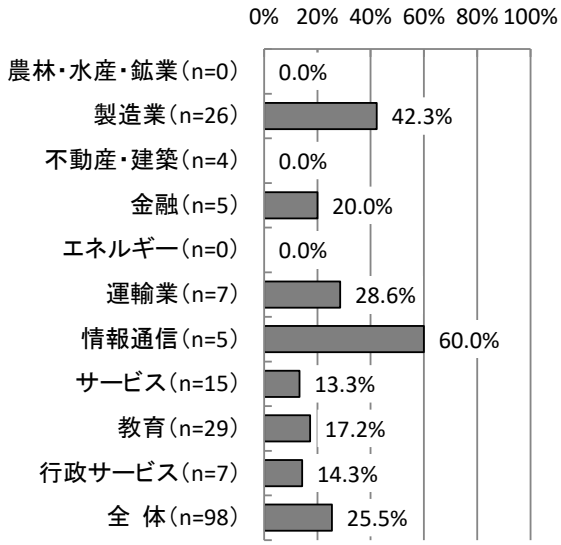




認証機能の導入・強化



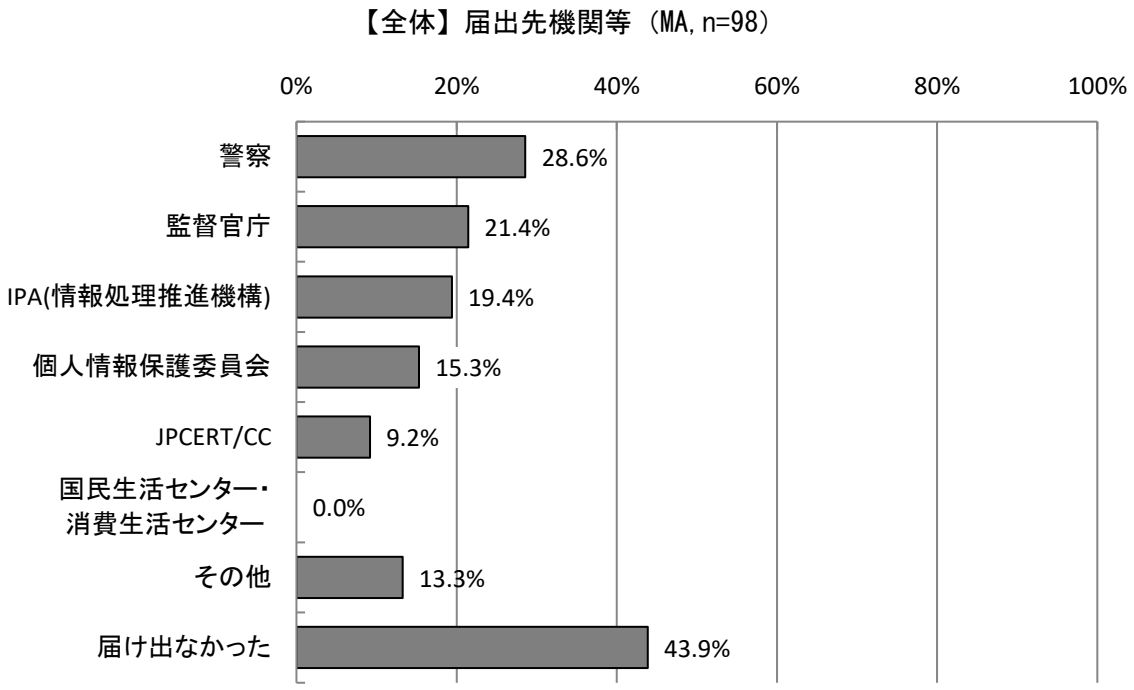
システム上にセキュリティホールが
ないかどうか検査、診断



3.1.16　届出先機関等　【問10-4-1】

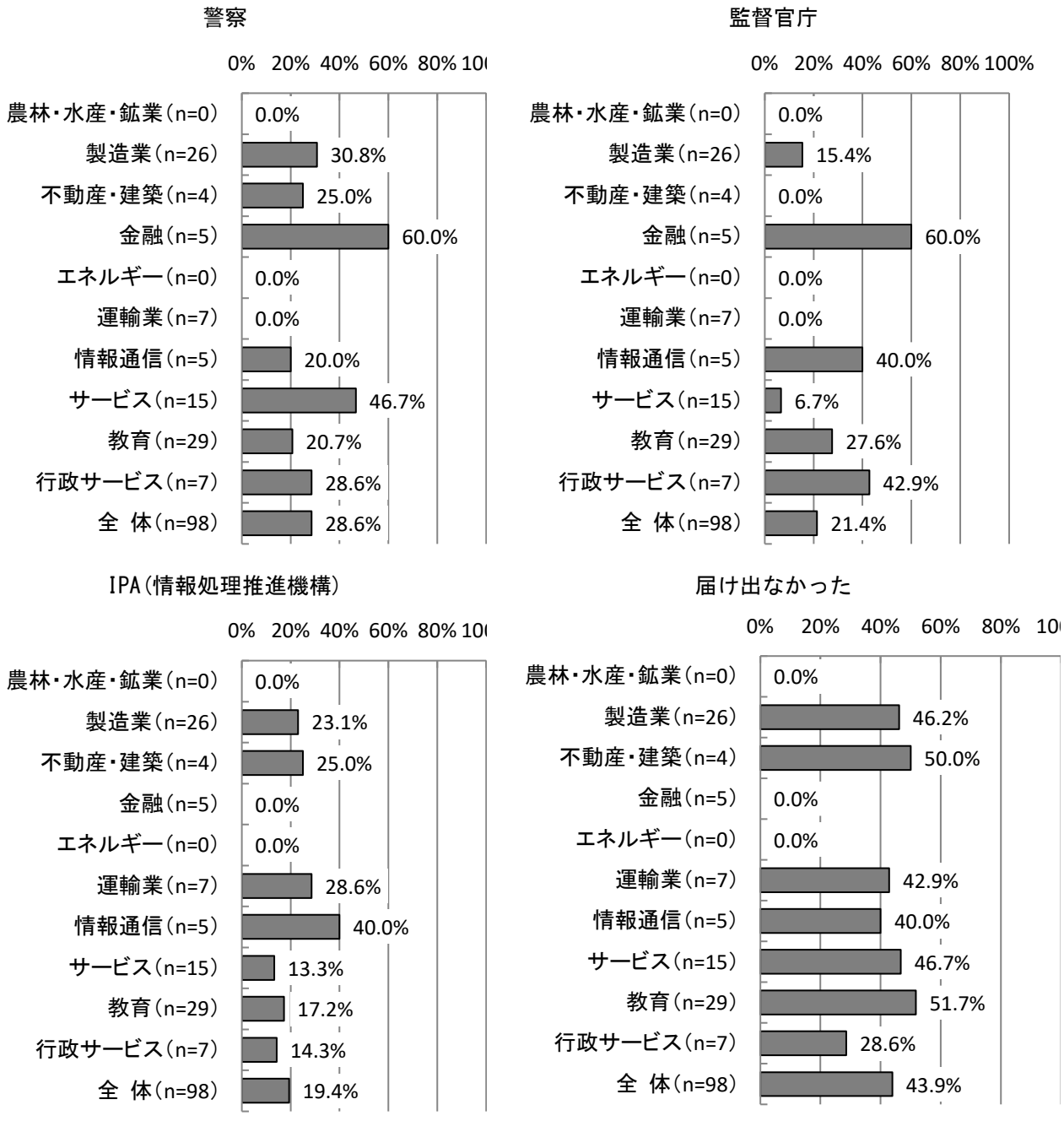
届出先機関等については、「警察」が28.6%で最も高く、次いで「監督官庁」が21.4%、「IPA （情報処理推進機構）」が19.4%となっている。一方、「届け出なかった」は43.9%となっている。

※本項目は、過去に不正アクセス等の被害にあった社・団体等を対象としている。



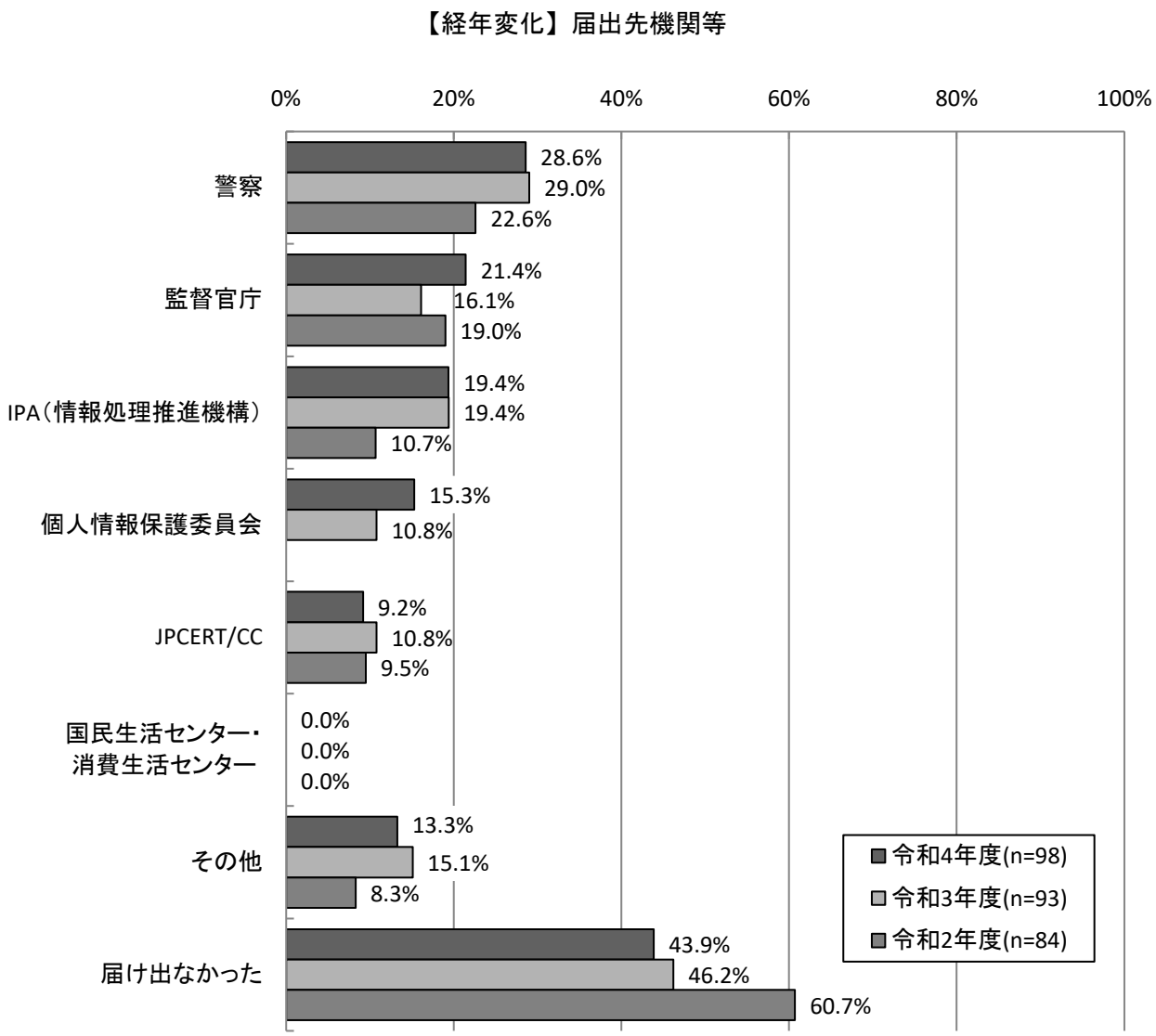
【業種別分析】業種別にみると、「警察」と「監督官庁」については「金融」がいずれも60.0%で高くなっている。一方、「届け出なかった」については、「教育」が51.7と多くなっている。

【業種別分析】届出先機関等



【経年変化】昨年度と比較すると、「警察」と「IPA （情報処理推進機構）」が、昨年度とほぼ同率で横ばいとなっている。「監督官庁」が5.3ポイント、「個人情報保護委員会」が4.5ポイントそれぞれ増加している。一方で、「届け出なかった」は2.3ポイント減少している。

※「無回答」を除いた総数で比較している。



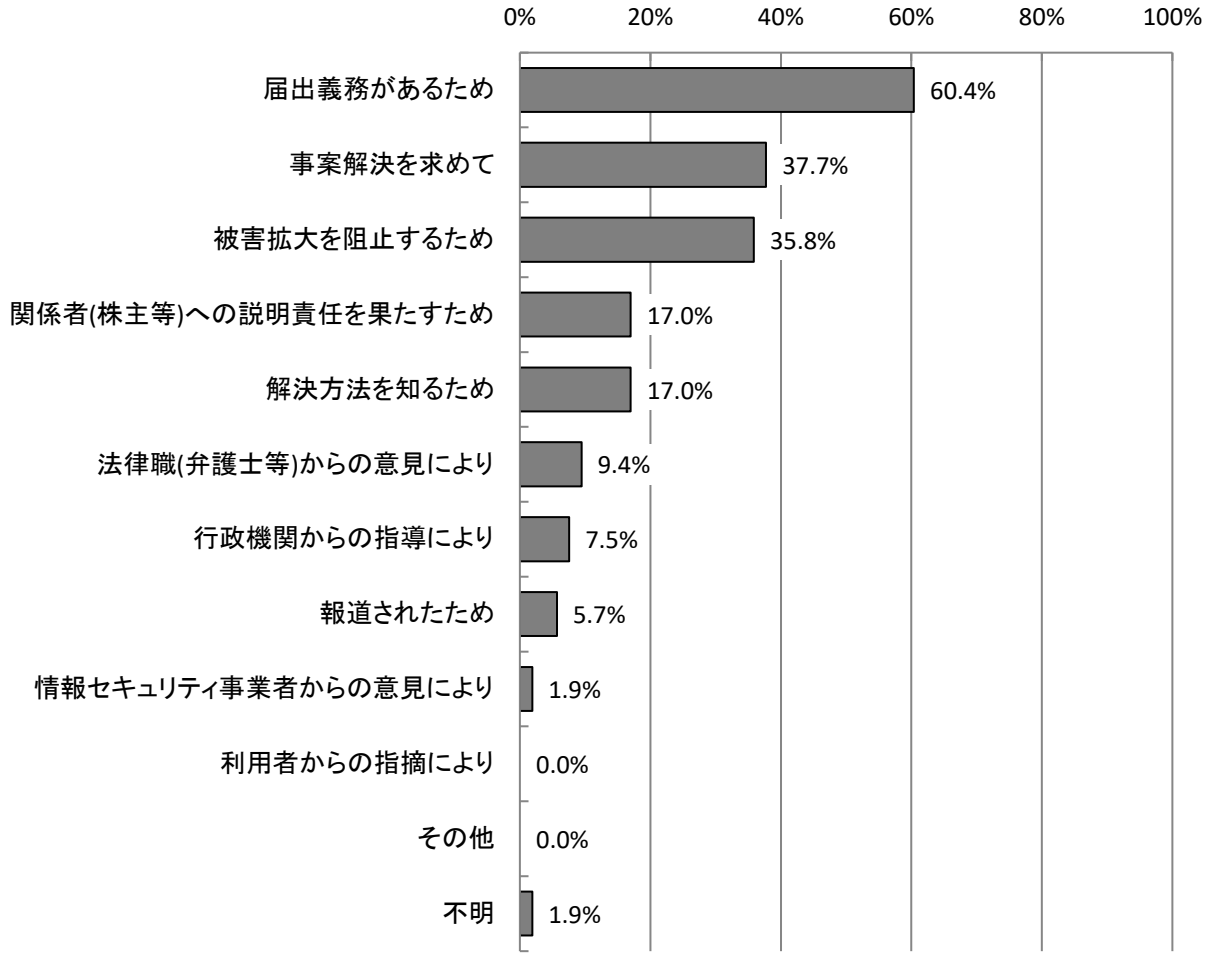
※令和３年度調査で、「個人情報保護委員会」を新設。

3.1.17　届出した理由　【問10-4-2】

届出した理由については、「届出義務があるため」が60.4%で最も多く、次いで「事案解決を求めて」が37.7%「被害拡大を阻止するため」が35.8%となっている。

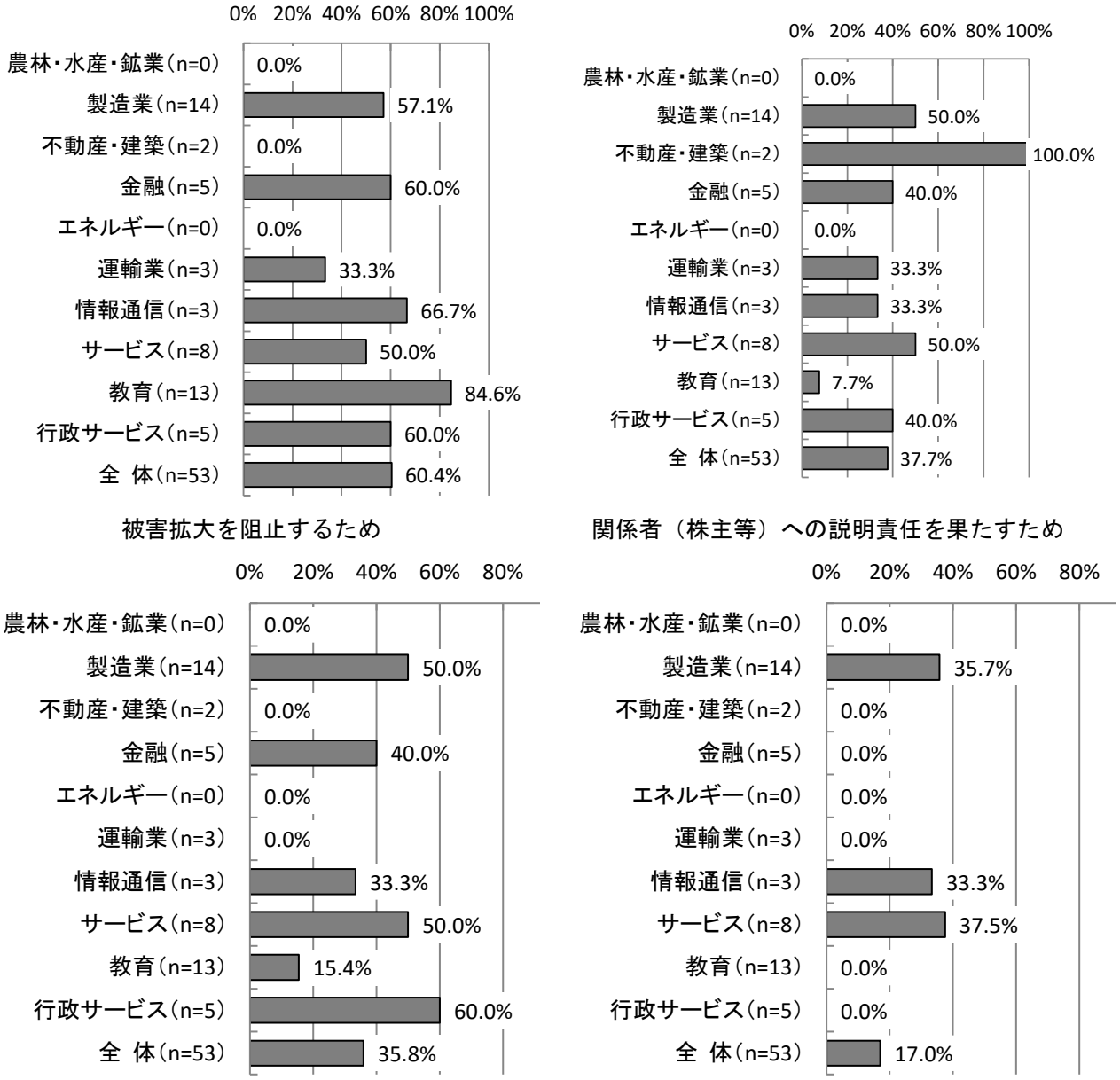
※本項目は、被害の届出を行った社・団体等を対象としている。

【全体】届出した理由（MA,n=53）



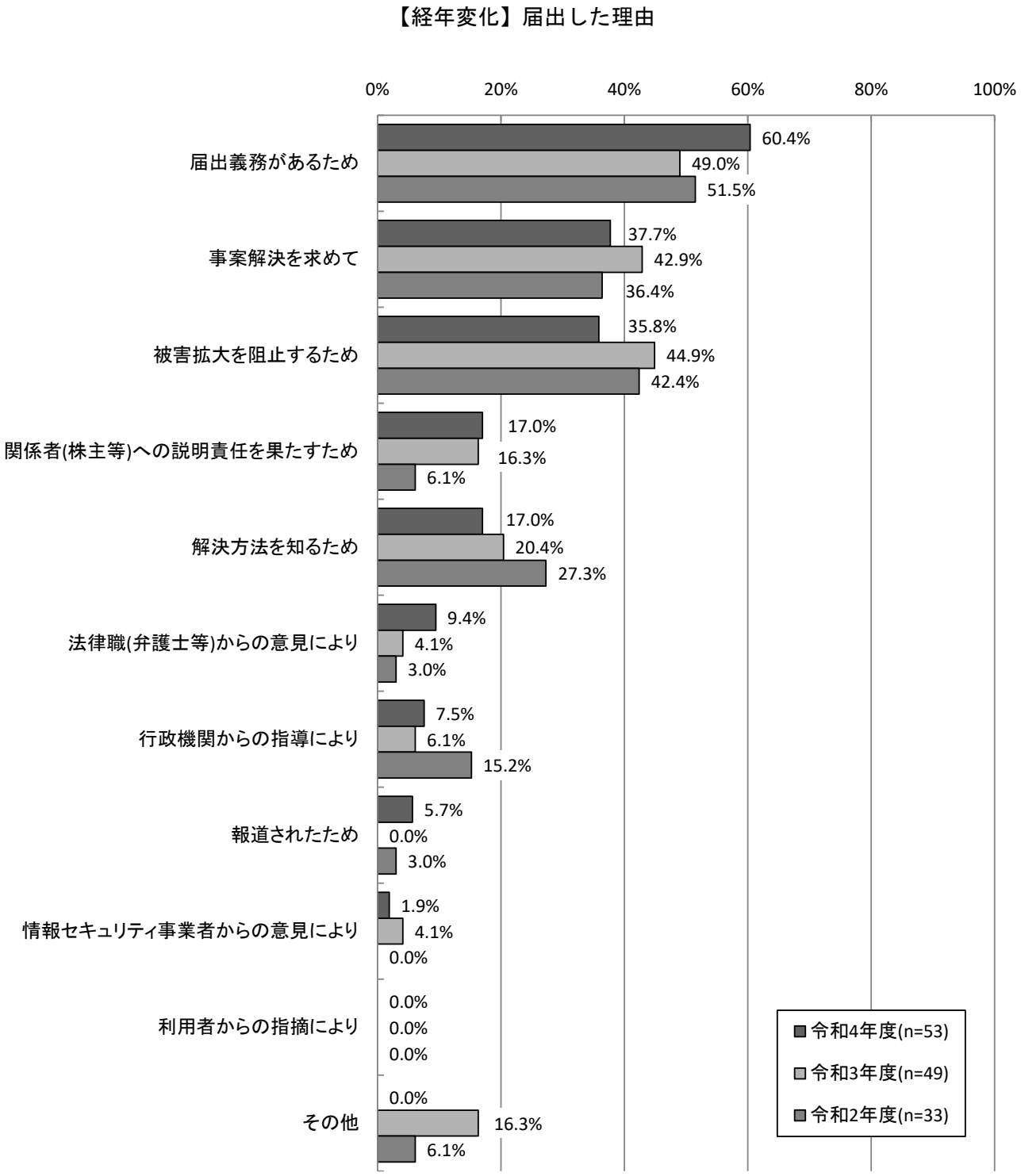
【業種別分析】業種別にみると、「届出義務があるため」は「教育」が84.6%で高く、「事案解決を求めて」では「製造業」と「サービス」が50.0%で高い。「被害拡大を阻止するため」については「行政サービス」が60.0%と最も多くなっている。

【業種別分析】届出した理由



【経年変化】昨年度と比較すると、「届出義務があるため」が11.4ポイント増加し、「被害拡大を阻止するため」が9.1ポイント、「事案解決を求めて」が5.2ポイント減少となっている

※「無回答」を除いた総数で比較している。

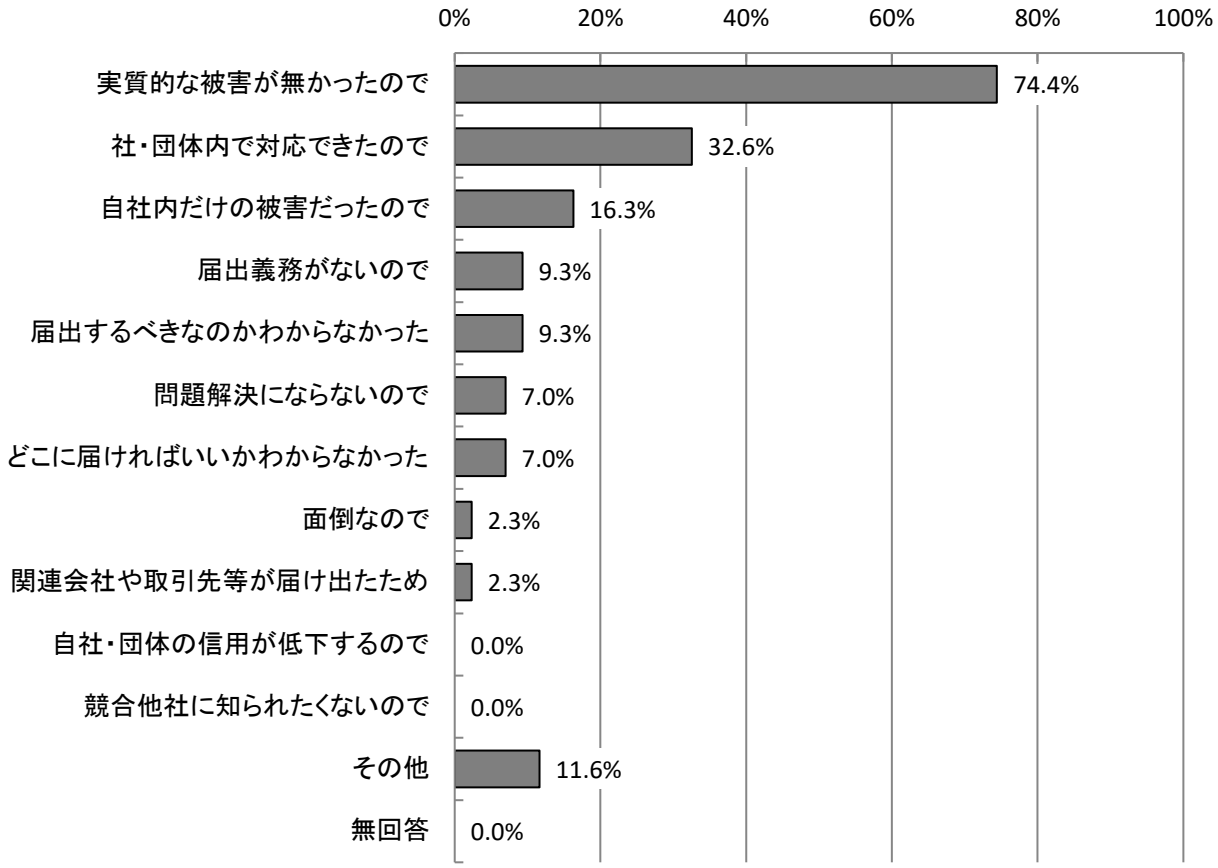


3.1.18　届出を躊躇させる要因　【問10-5】

届出を躊躇させる要因については、「実質的な被害が無かったので」が74.4%で最も高く、次いで「社・団体内で対応できたので」が32.6%、「自社内だけの被害だったので」が16.3%となっている。

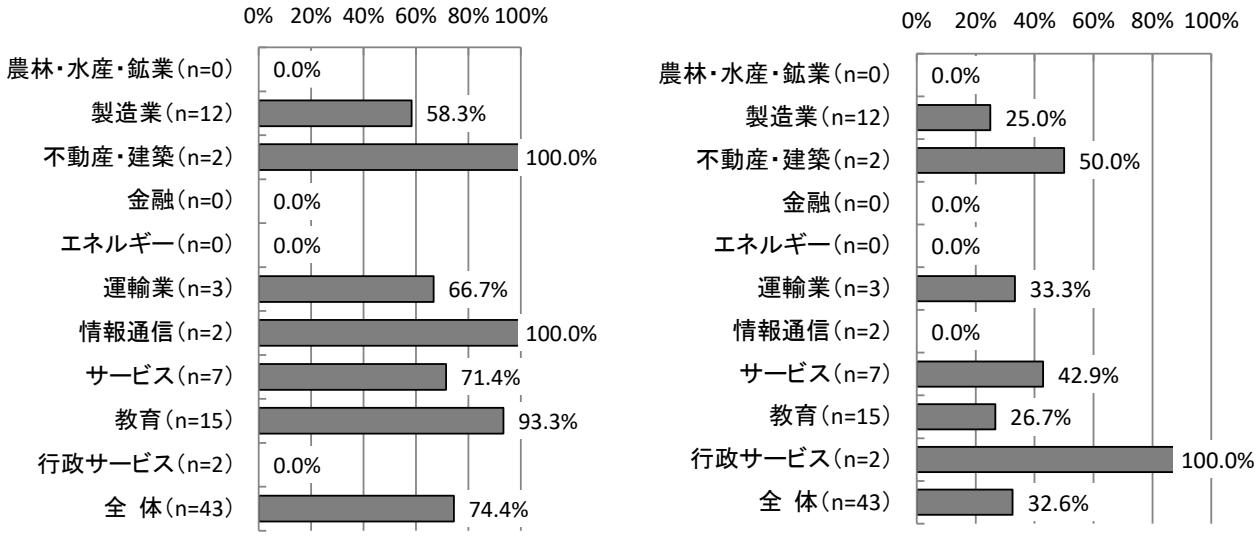
※本項目は、被害の届出を行わなかった社・団体等を対象としている。

【全体】届出を躊躇させる要因（MA, n=43）

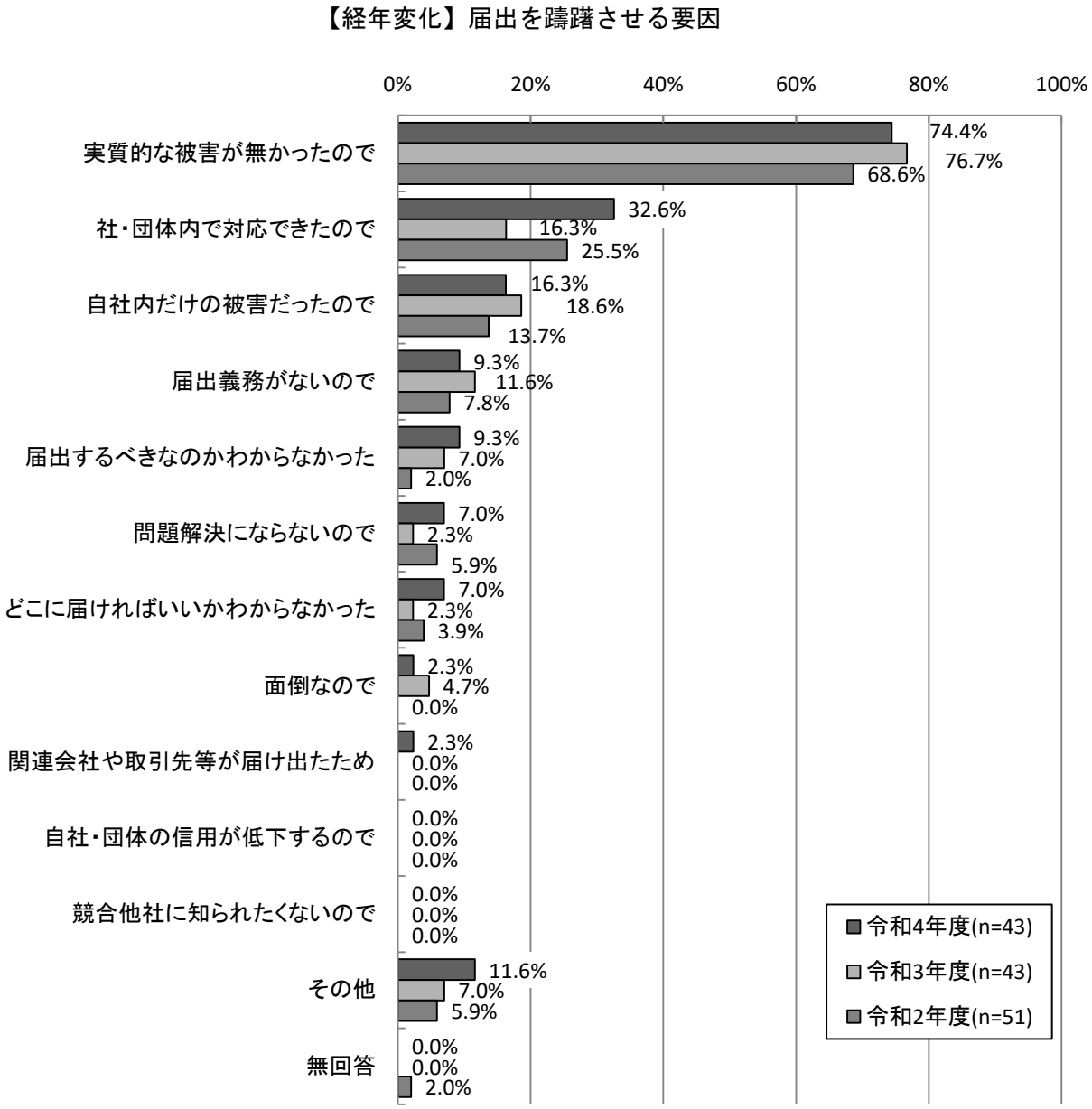


【業種別分析】業種別にみると、「実質的な被害が無かったので」については、「教育」が93.3%、「サービス」が71.4%となっている。「社・団体内で対応できたので」については、「サービス」が42.9%となっている。

【業種別分析】届出を躊躇させる要因



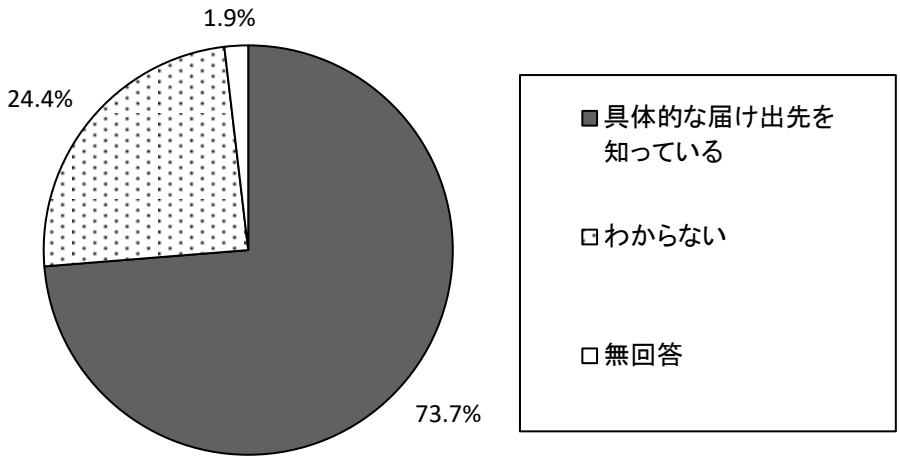
【経年変化】昨年度と比較すると、「社・団体内で対応できたので」が16.3ポイントの増加であった。一方、「面倒なので」は2.4ポイント減少している。



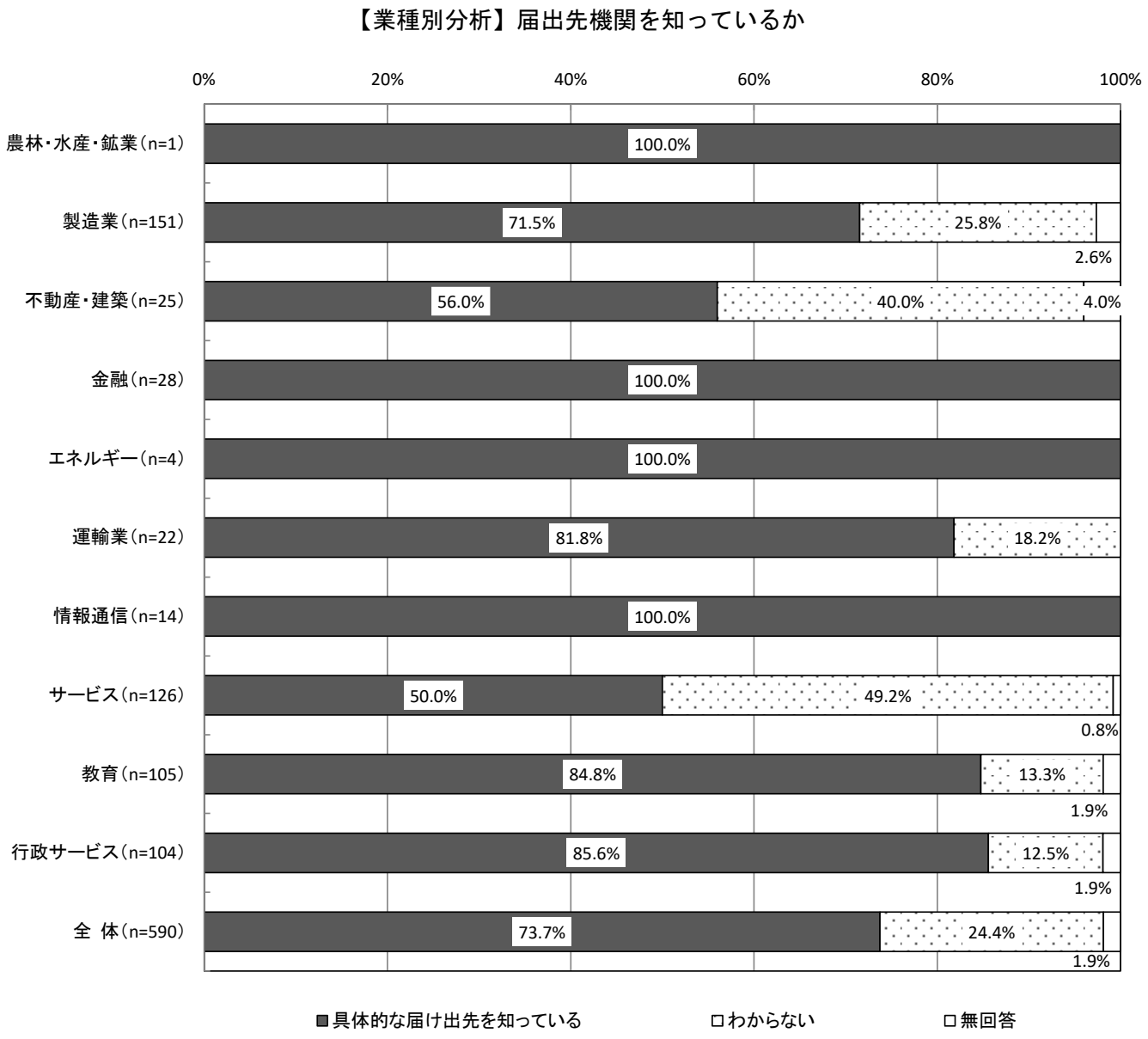
3.1.19　届出先機関を知っているか　【問11】

届出先機関を知っているかについては、「具体的な届け出先を知っている」が73.7%と高く、「わからない」は24.4%となっている。

【全体】届出先機関を知っているか（SA,n=590）

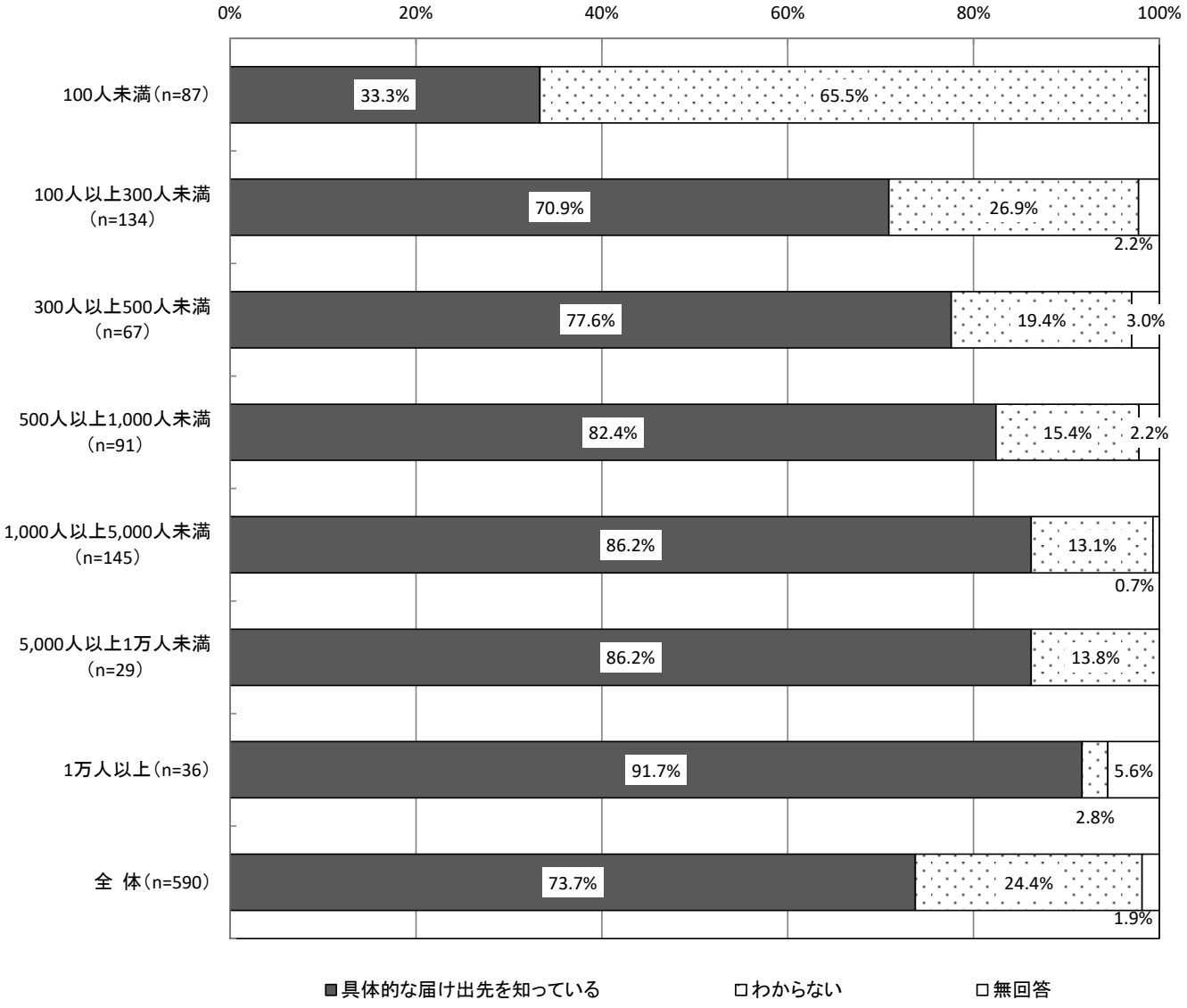


【業種別分析】業種別にみると、届出先機関を「知っている」については、「金融」「情報通信」が100.0%で高い。一方、「わからない」については、「サービス」が49.2%、「不動産・建築」が40.0%となっている。



【従業員規模別分析】従業員規模別にみると、従業員数が多くなるほど「知っている」の割合が高くなる傾向であり、「100人未満」では65.5%が「わからない」となっている。

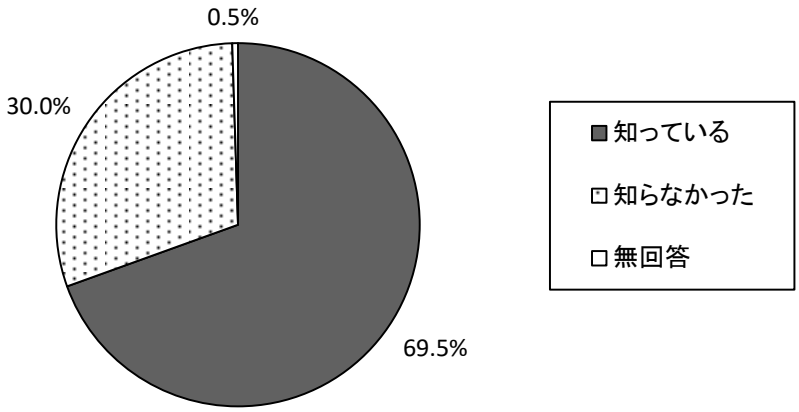
【従業員規模別分析】届出先機関を知っているか



3.1.20　不正アクセス禁止法でアクセス管理者による防御措置についての努力義務【問12】

アクセス管理者による防御措置についての努力義務については、「知っている」が69.5%、「知らなかった」は30.0%となっている。

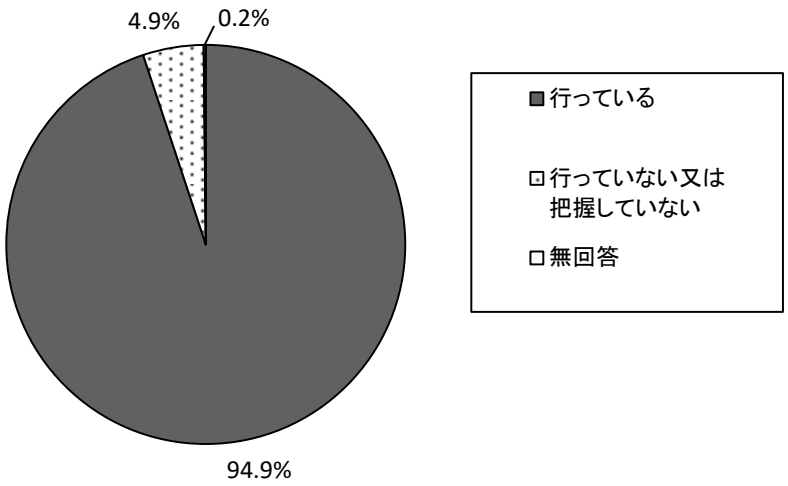
【全体】不正アクセス禁止法でアクセス管理者による防御措置についての努力義務（SA,n=590）



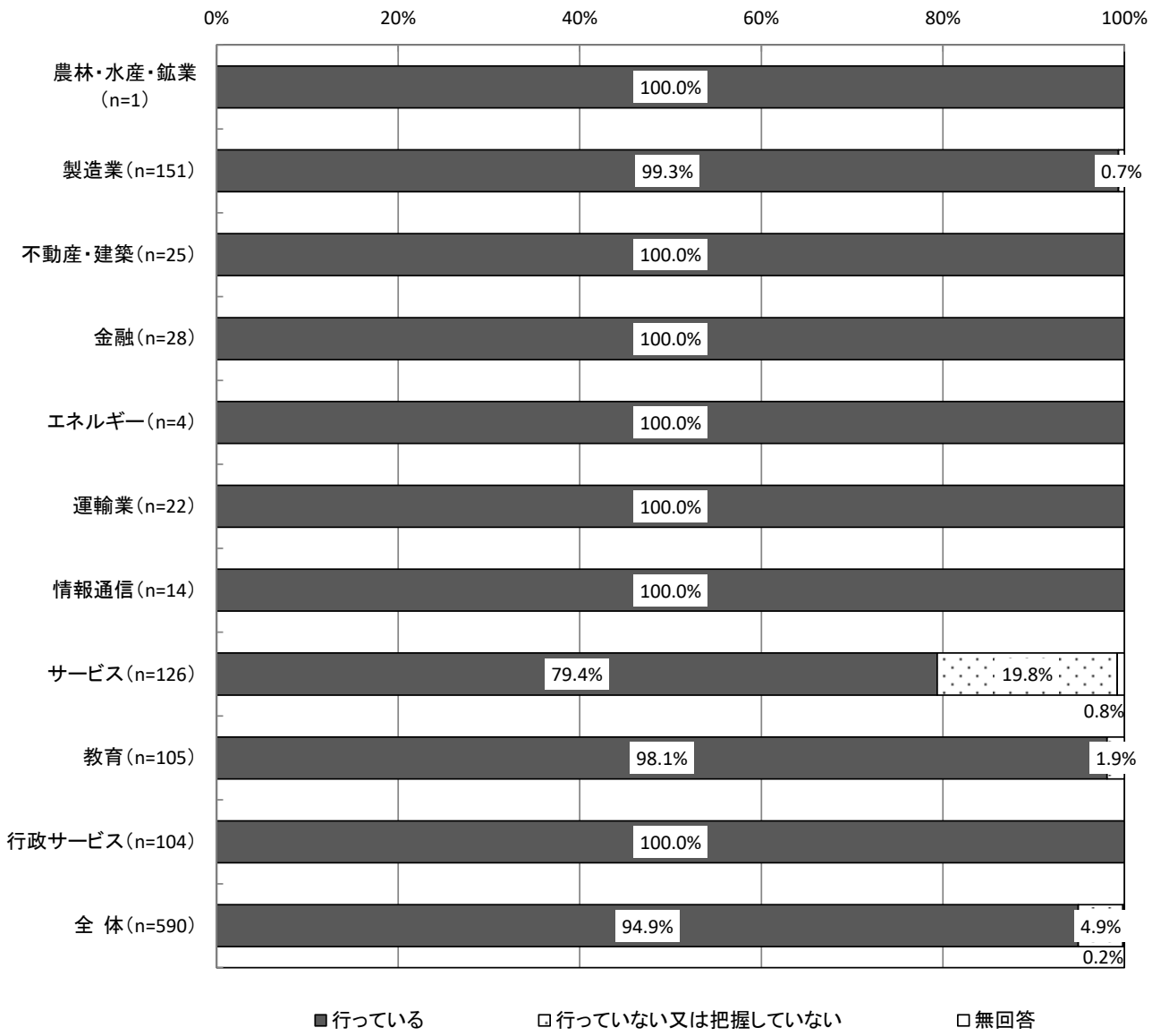
3.1.21　情報セキュリティ対策の実施状況　【問13】

情報セキュリティ対策の実施状況については、「行っている」が94.9%、「行っていない又は把握していない」が4.9%となっている。

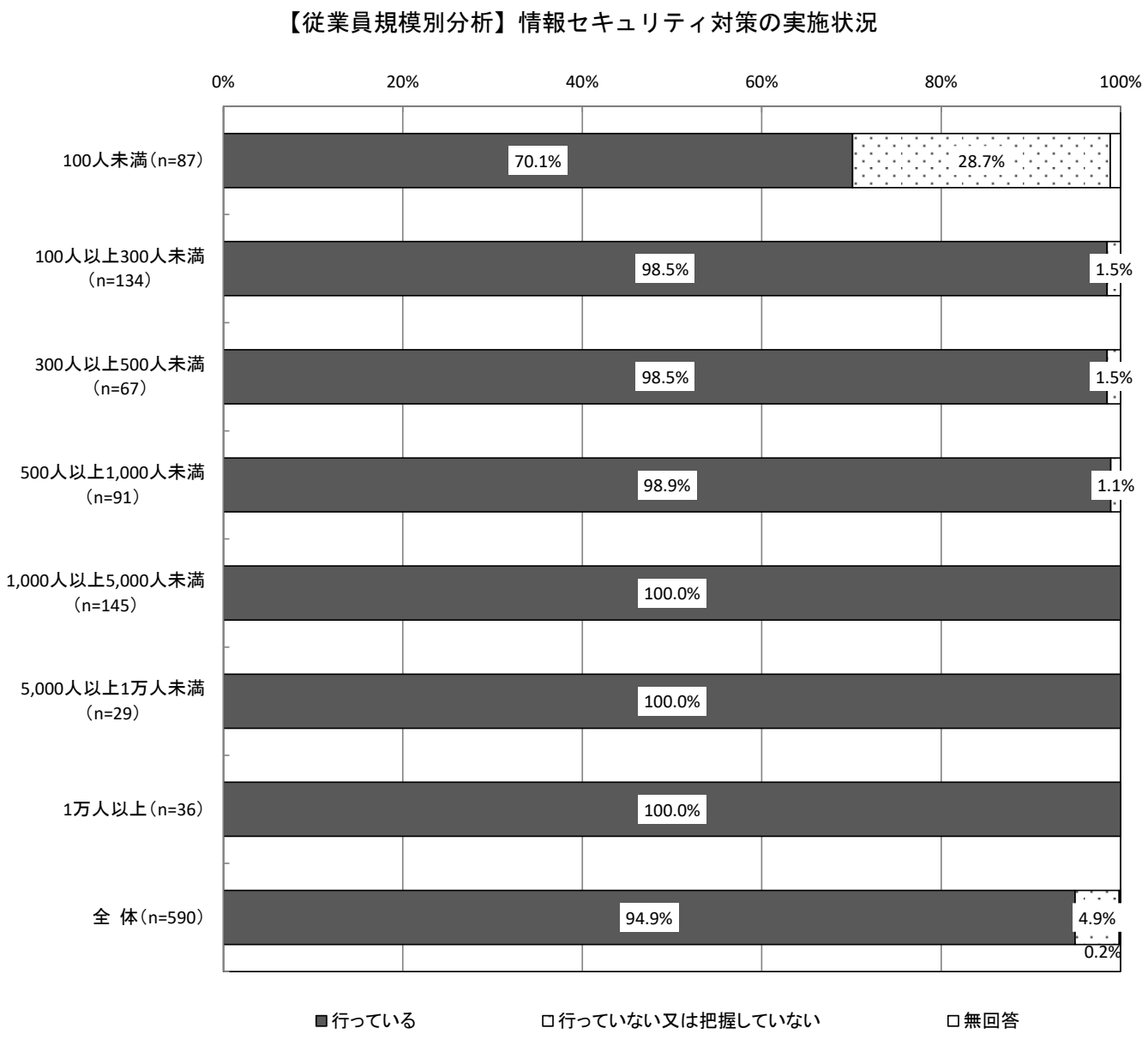
【全体】情報セキュリティ対策の実施状況（SA,n=590）



【業種別分析】業種別で情報セキュリティ対策を「行っている」が 100.0%でないのは 3 業種のみである。このうち「製造業」は 99.3%、「教育」は 98.1%と高い割合であるが、最も低いのは「サービス」の 79.4%で、約 8 割にとどまっている。



【従業員規模別分析】従業員規模別にみると、従業員数100人以上は「行っている」が98%以上であるのに対して、「100人未満」では「行っていない又は把握していない」が28.7%となっている。

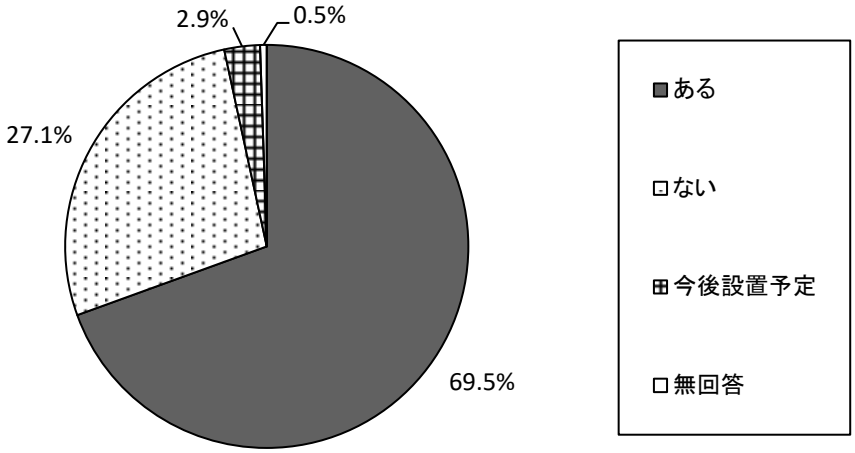


3.1.22　情報セキュリティ運用・管理専門部署の有無　【問13-1】

情報セキュリティ運用・管理専門部署の有無については、「ある」が69.5%と高く、「ない」は27.1%となっている。

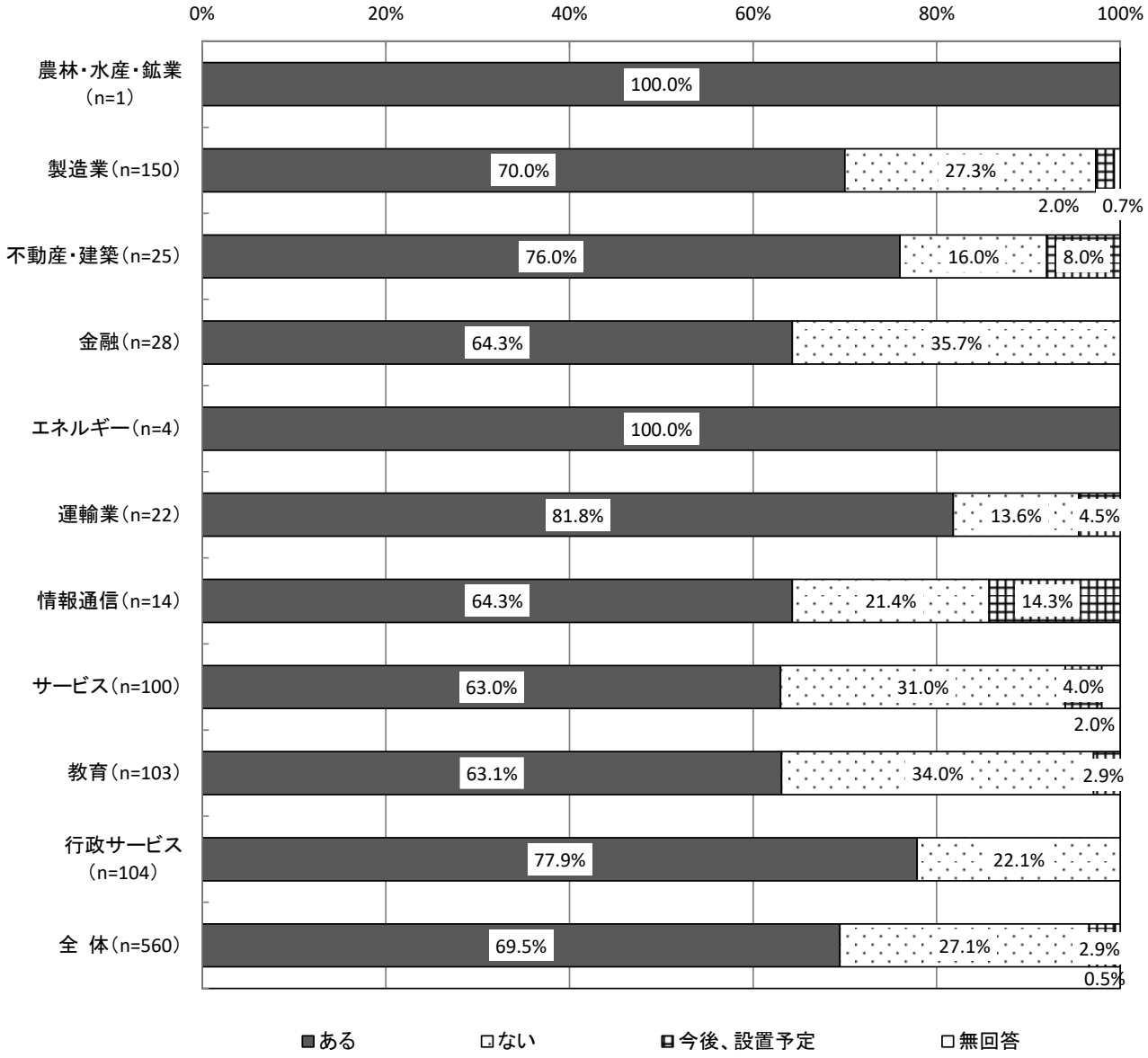
※本項目は、情報セキュリティ対策を行っている社・団体等を対象としている。

【全体】情報セキュリティ運用・管理専門部署の有無（SA,n=560）

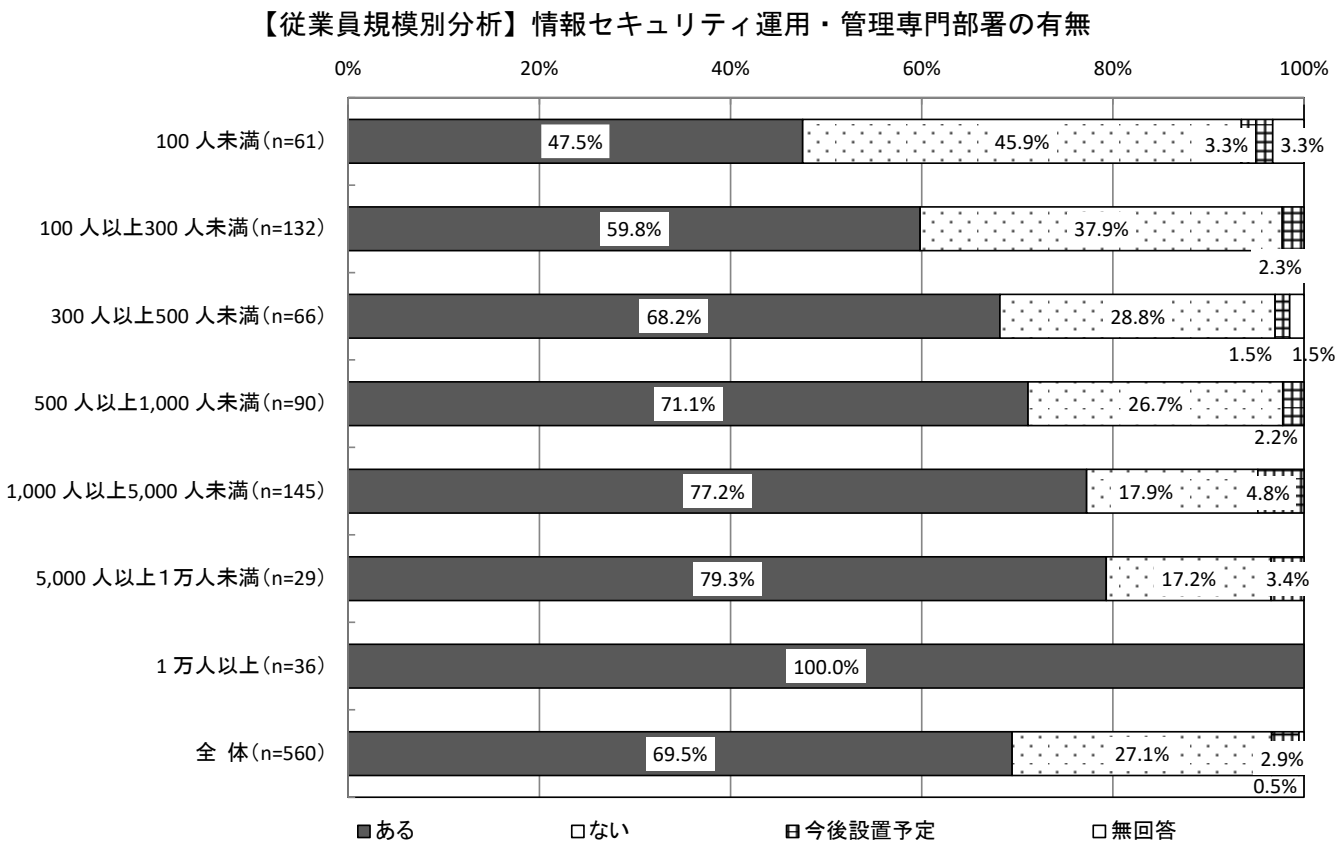


【業種別分析】業種別にみると、情報セキュリティ運用・管理専門部署が「ある」については、「運輸業」が 81.8%、「行政サービス」が 77.9%などで高くなっている。一方、情報セキュリティ運用・管理専門部署が「ない」については、「金融」が 35.7%、「教育」が 34.0%、「サービス」が 31.0%と高くなっている。

【業種別分析】情報セキュリティ運用・管理専門部署の有無

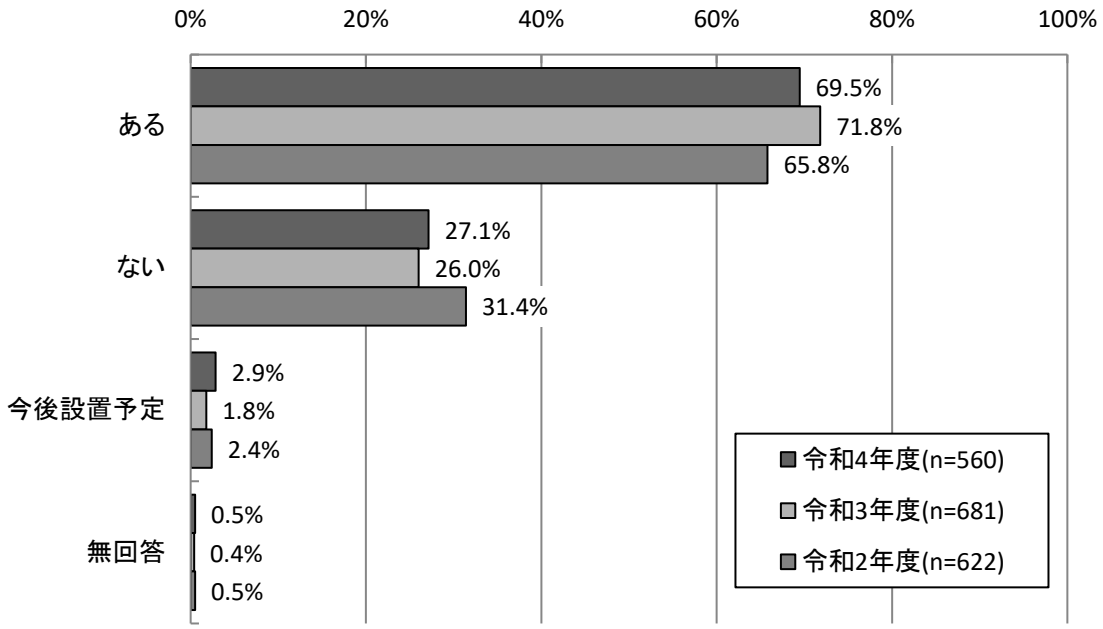


【従業員規模別分析】従業員規模別にみると、「ある」は「１万人以上」では100.0%となっている。一方、「ない」は「100人未満」で47.5%と最も多くなっている。



【経年変化】昨年度と比較すると、情報セキュリティ運用・管理専門部署が「ある」が2.3ポイント減少し、「ない」が1.1ポイント増加している。

【経年変化】情報セキュリティ運用・管理専門部署の有無

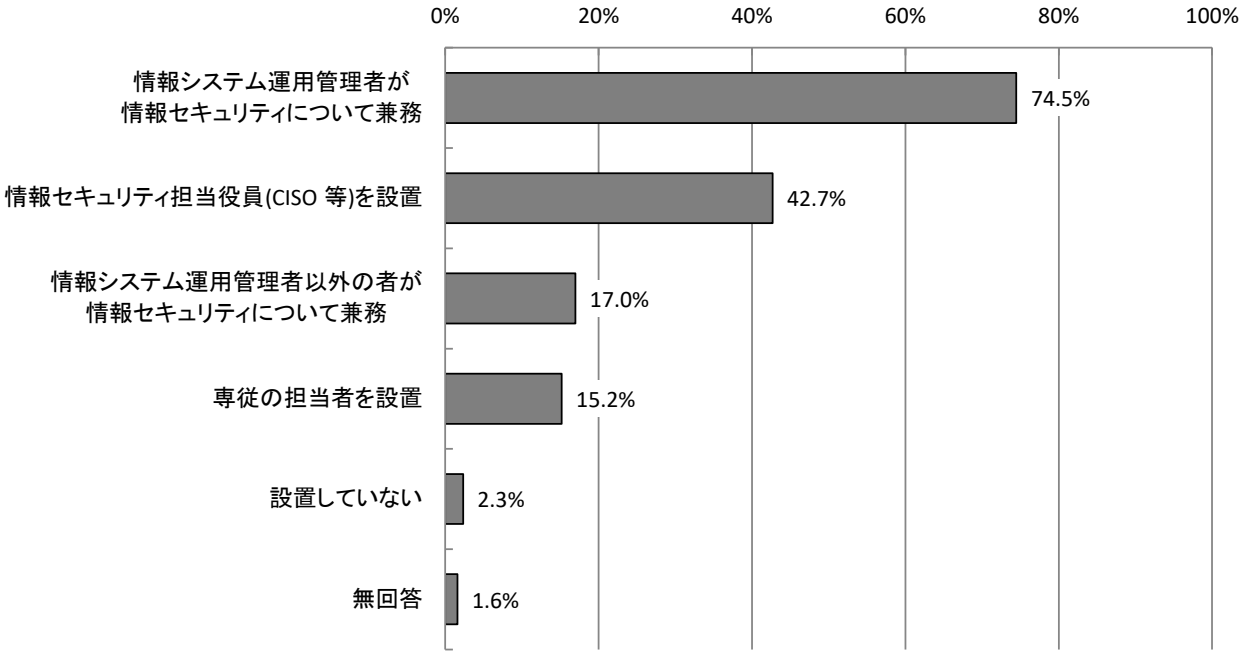


3.1.23　情報セキュリティ管理体制　【問13-2】

情報セキュリティ管理体制については、「情報システム運用管理者が情報セキュリティについて兼務」が74.5%で最も高く、次いで「情報セキュリティ担当役員（ＣＩＳＯ等）を設置」が42.7%、「情報システム運用管理者以外の者が情報セキュリティについて兼務」が17.0%となっている。

※本項目は、情報セキュリティ対策を行っている社・団体等を対象としている。

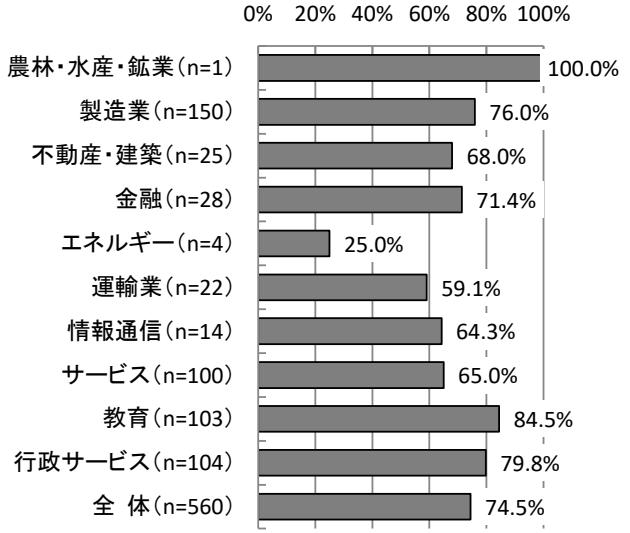
【全体】情報セキュリティ管理体制（MA, n=560）



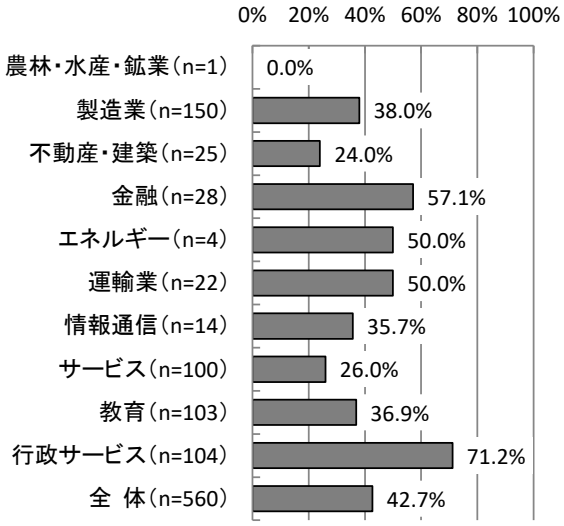
【業種別分析】業種別にみると、「情報システム運用管理者が情報セキュリティについて兼務」については、「教育」が84.5%、「行政サービス」が79.8%と高くなっている。「情報セキュリティ担当役員（ＣＩＳＯ等）を設置」については、「行政サービス」が71.2%で最も高く、次いで「金融」が57.1%となっている。「情報システム運用管理者以外の者が情報セキュリティについて兼務」では、「情報通信」が42.9%で最も高い。

【業種別分析】情報セキュリティ管理体制

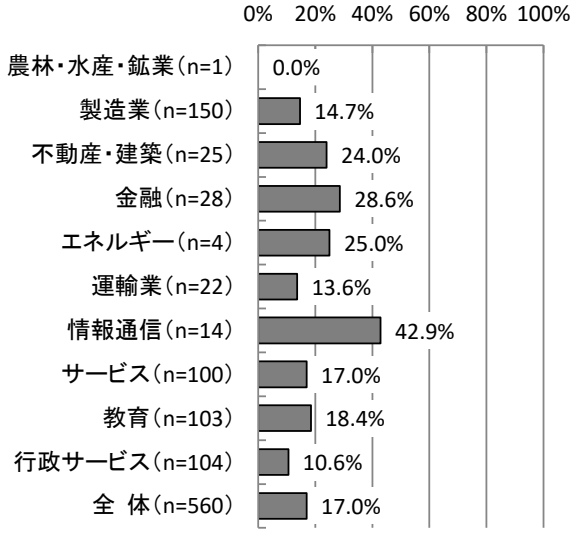
情報システム運用管理者が情報セキュリティについて兼務



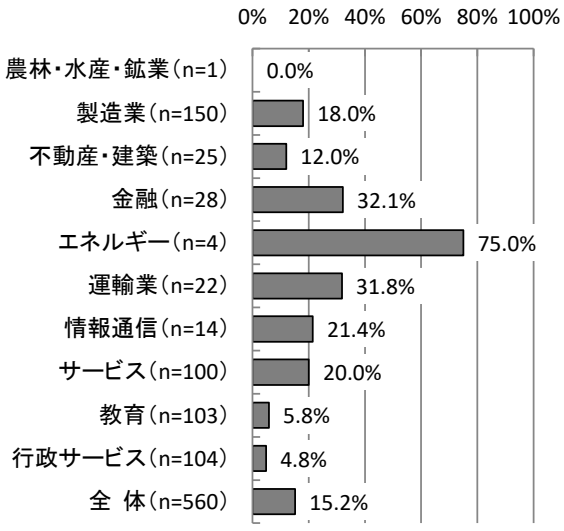
情報セキュリティ担当役員（ＣＩＳＯ等）を設置



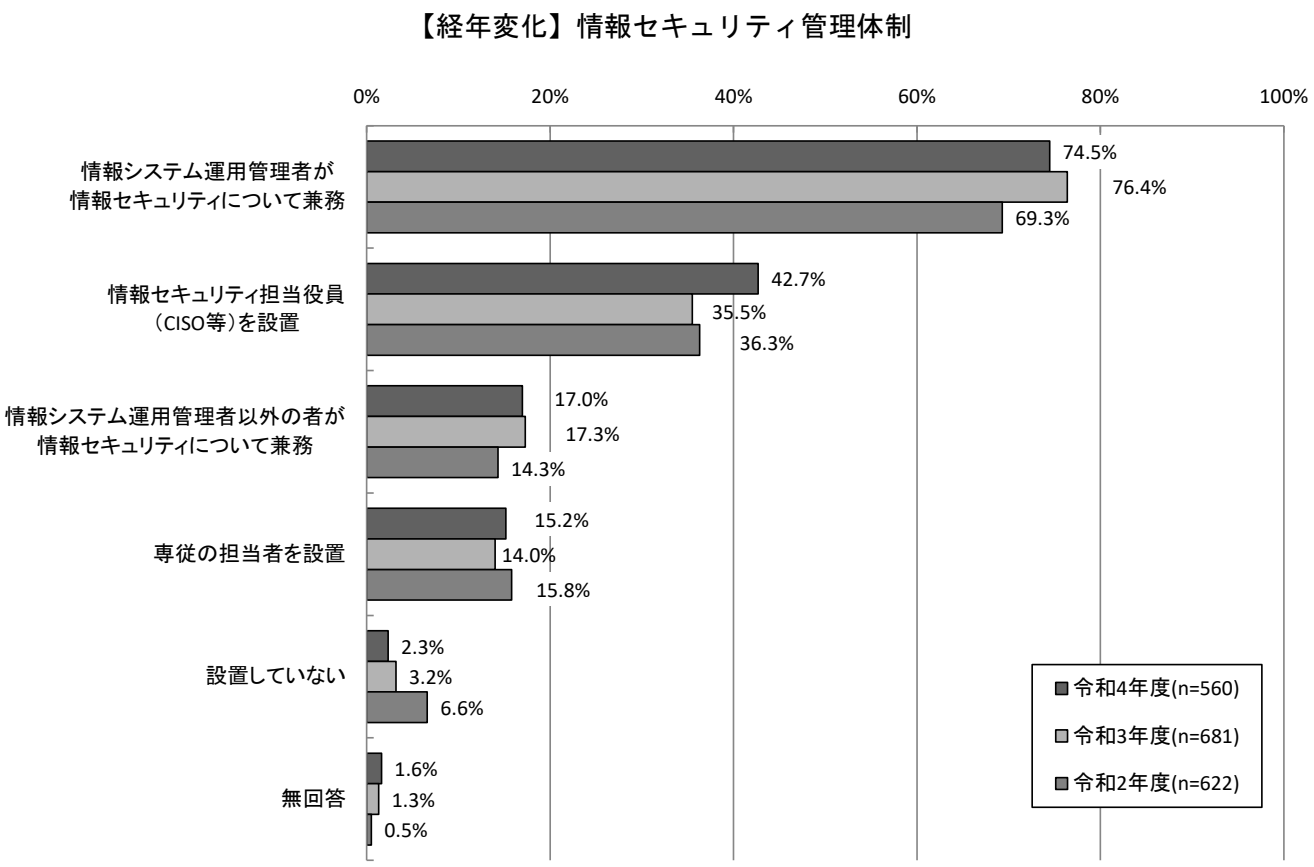
情報システム運用管理者以外の者が情報セキュリティについて兼務



専従の担当者を設置



【経年変化】昨年度と比較すると、「情報セキュリティ担当役員（ＣＩＳＯ）等を設置」が7.2ポイントポイント増加している。また「設置していない」は昨年度に続き減少している。

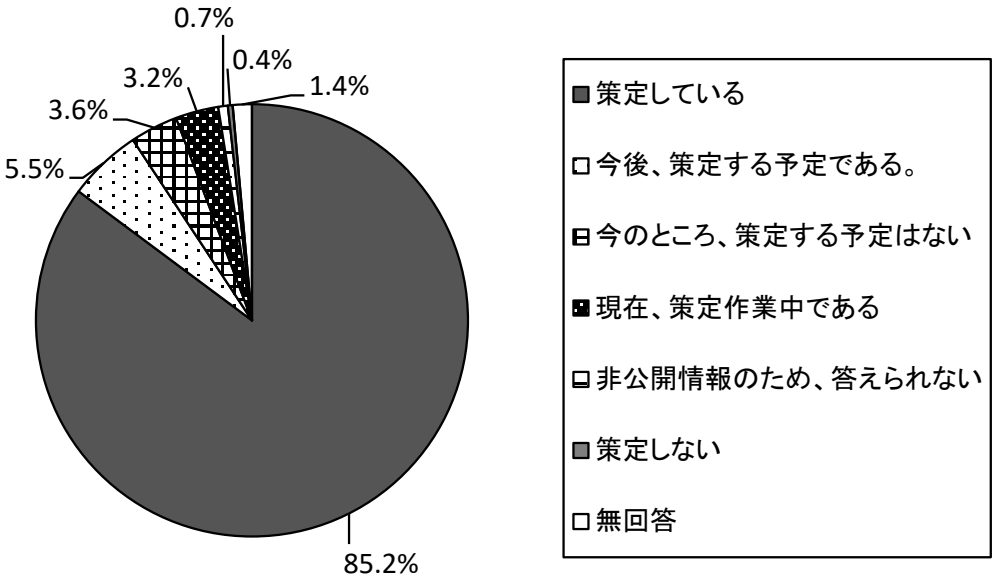


3.1.24　セキュリティポリシーの策定状況　【問13-3】

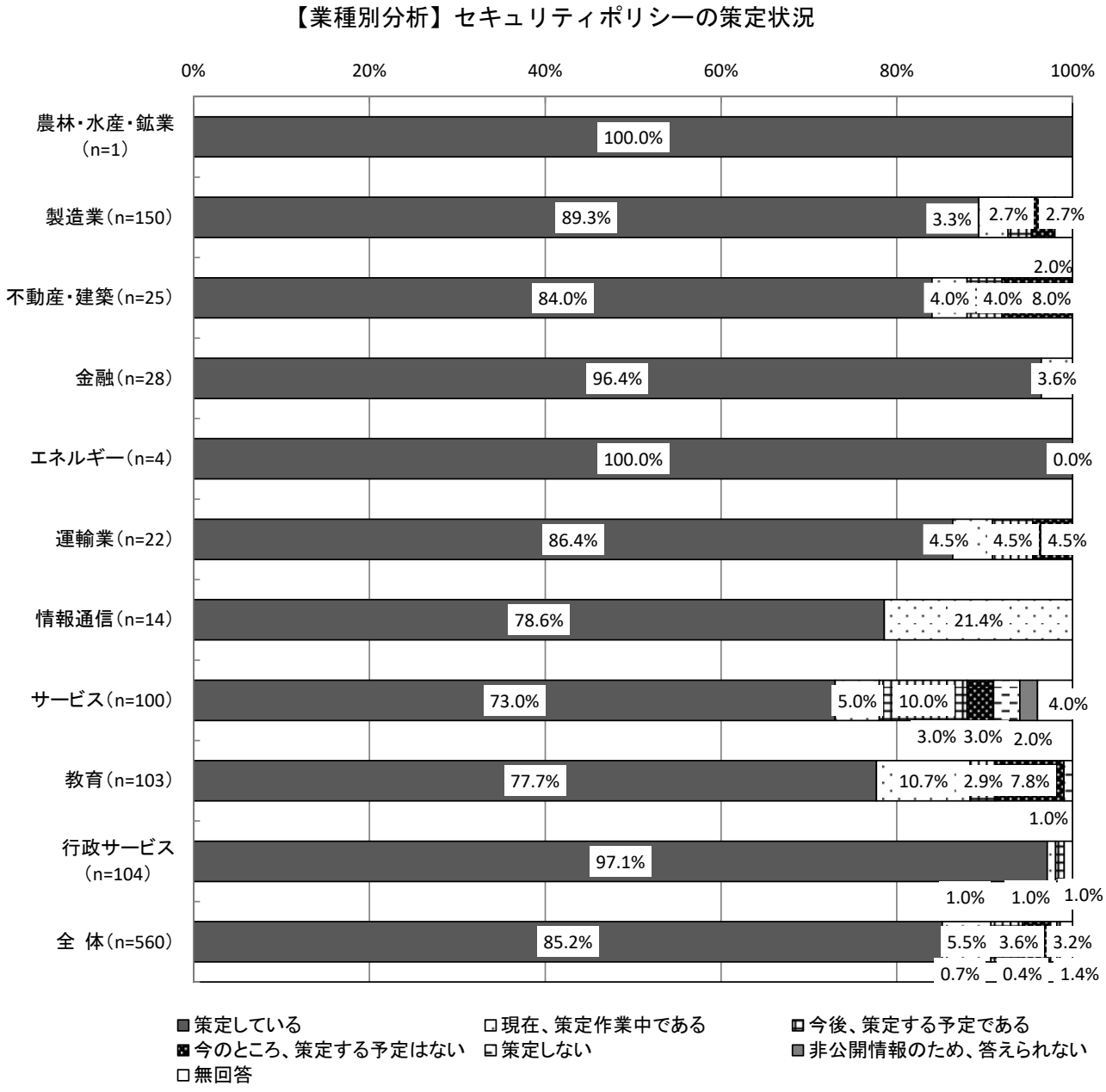
セキュリティポリシーの策定状況については、「策定している」が85.2%で最も高く、次いで「今後、策定する予定である」が5.5%、「今のところ、策定する予定はない」が3.6%となっている。「策定している」「今後、策定する予定である」「現在、策定作業中である」を加えた「策定（予定）」は、全体の93.9%となっている。

※本項目は、情報セキュリティ対策を行っている社・団体等を対象としている。

【全体】セキュリティポリシーの策定状況（SA,n=560）



【業種別分析】業種別にみると、セキュリティポリシーを「策定している」については「行政サービス」が97.1%、「金融」が96.4%と9割を超えている。一方「策定している」が低いのは、「サービス」の73.0%、「教育」の77.7%、「情報通信」が78.6%となっている。

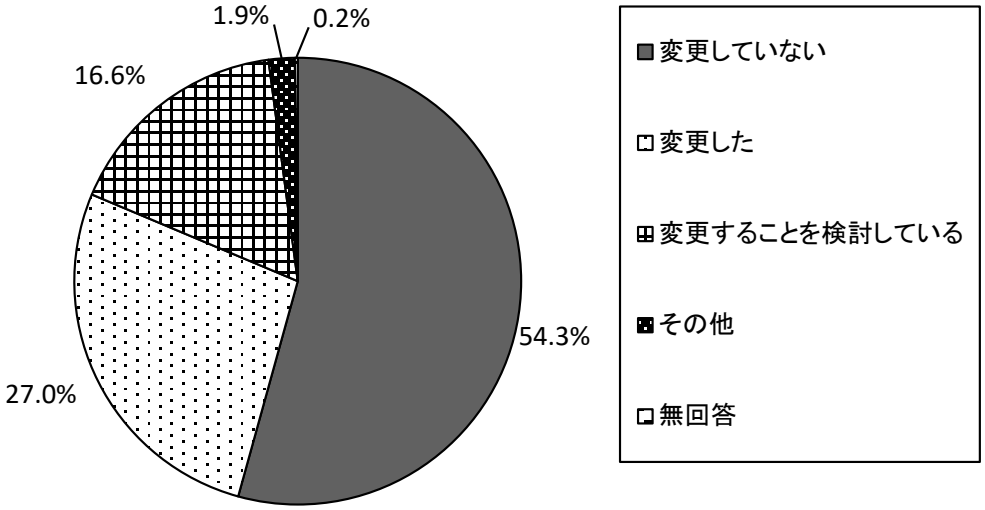


3.1.25　新型コロナウイルスの影響によるセキュリティポリシーの変更状況【問13-3-1】

新型コロナウイルスの影響によるセキュリティポリシーの変更状況については、「変更していない」が54.3%で過半数となっている。次いで「変更した」が27.0%、「変更することを検討している」が16.6%となっている。

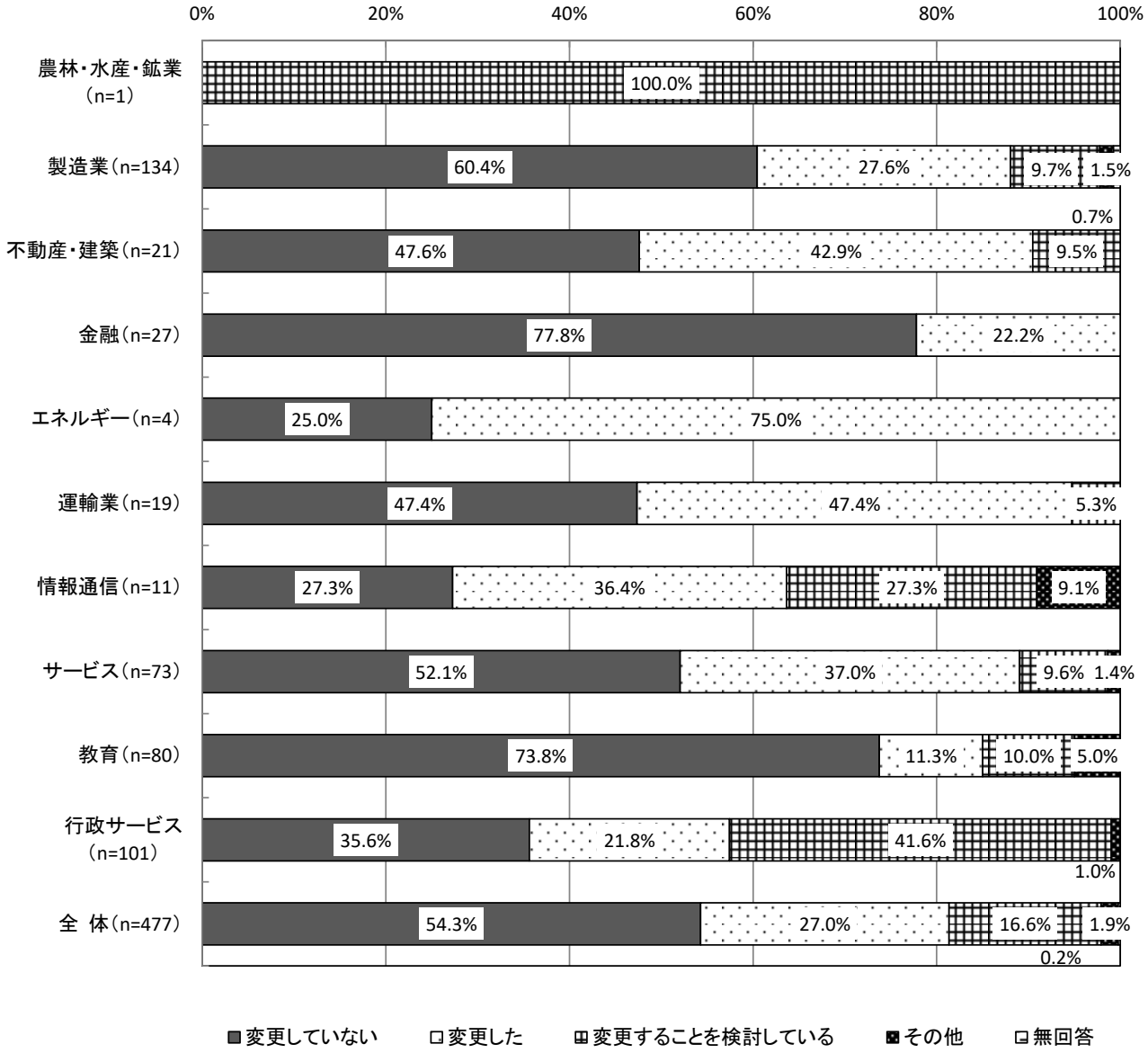
※本項目は、セキュリティポリシーを策定している社・団体等を対象としている。

【全体】新型コロナウイルスの影響によるセキュリティポリシーの変更状況（SA,n=560）



【業種別分析】業種別にみると、新型コロナウイルスの影響によるセキュリティポリシーの変更状況については、「変更していない」については「金融」の77.8%が最も高く、次いで「教育」が73.8%となっている。

【業種別分析】新型コロナウイルスの影響によるセキュリティポリシーの変更状況

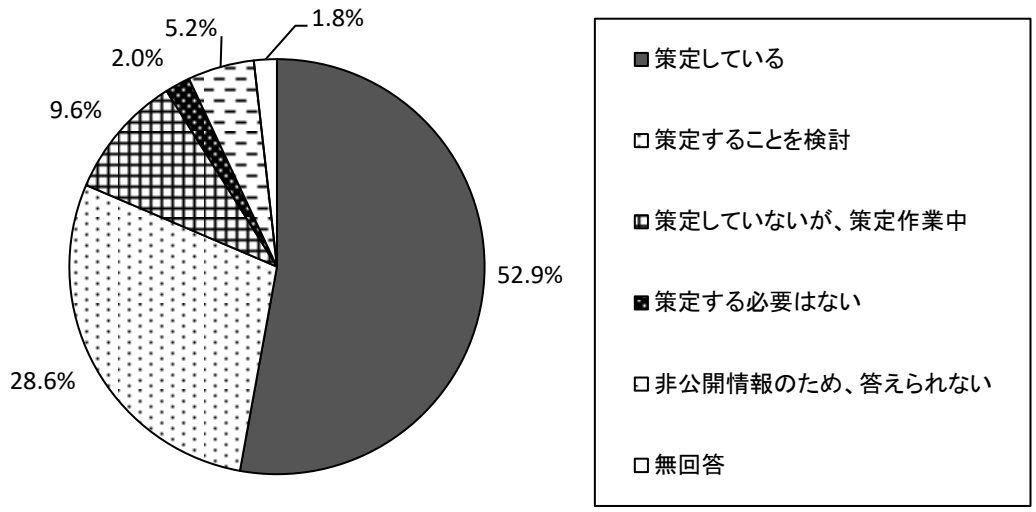


3.1.26　情報セキュリティ侵害事案発生時の対応マニュアル等の策定状況　【問13-4】

情報セキュリティ侵害事案発生時の対応マニュアル等の策定状況については、「策定している」が52.9%で過半数となっている。次いで「策定することを検討」が28.6%、「策定していないが、策定作業中」が9.6%となっている。

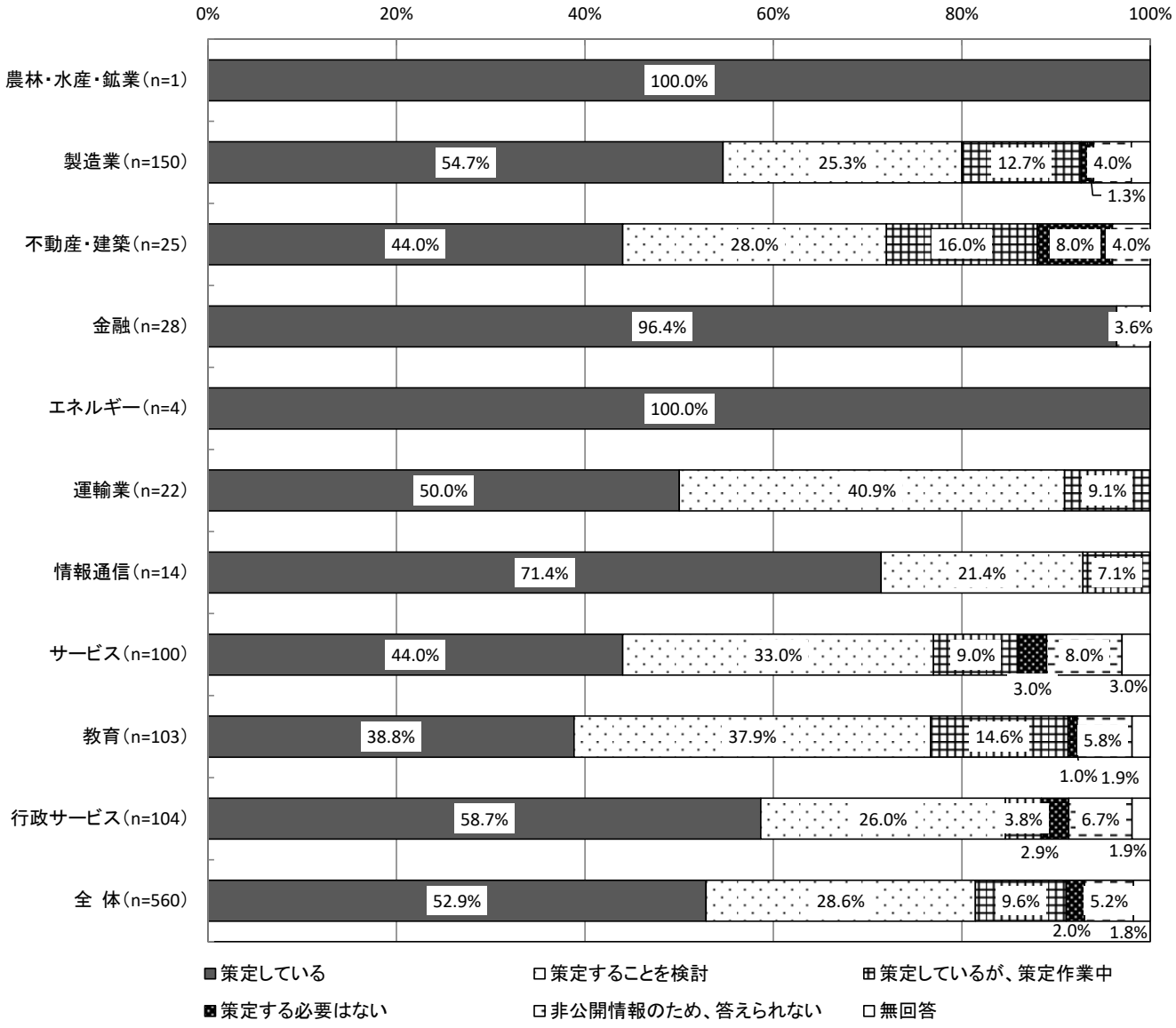
※本項目は、情報セキュリティ対策を行っている社・団体等を対象としている。

【全体】情報セキュリティ侵害事案発生時の対応マニュアル等の策定状況（SA,n=560）



【業種別分析】業種別にみると、「策定している」については、「金融」の96.4%、「情報通信」の71.4%などで高い。これに対して「教育」が38.8%と低くなっている。

【業種別分析】情報セキュリティ侵害事案発生時の対応マニュアル等の策定状況

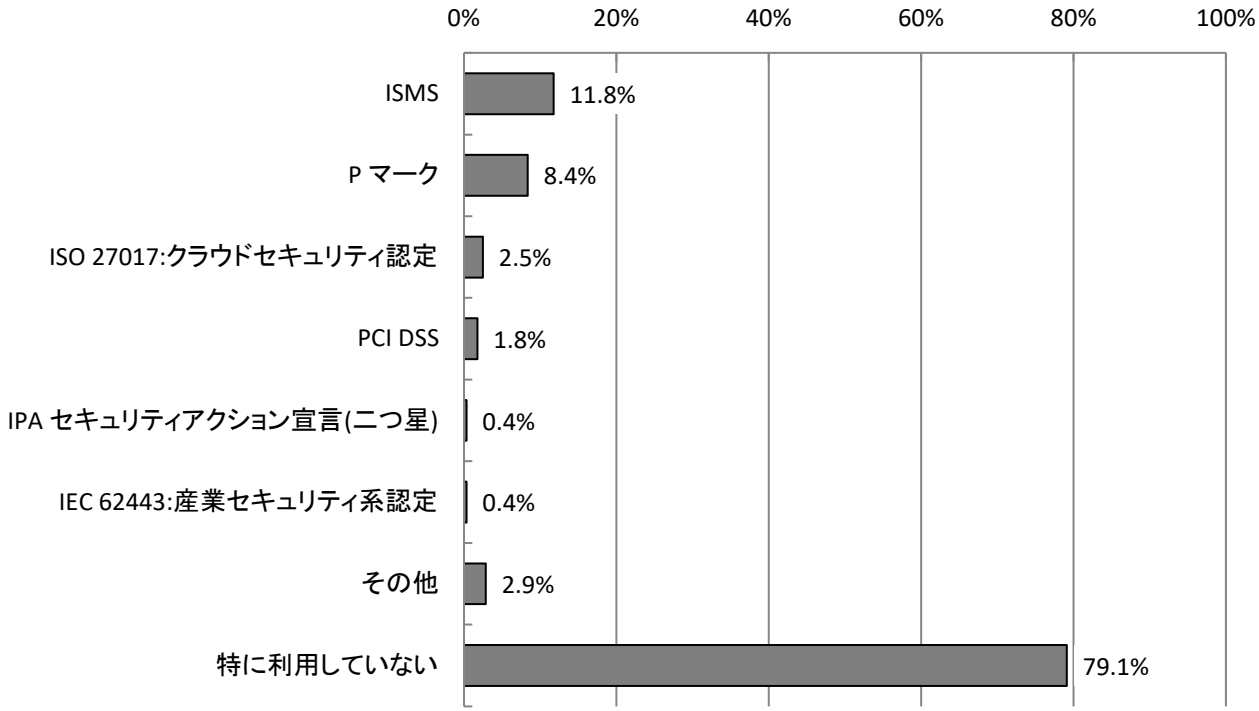


3.1.27　第三者機関の認証制度等の利用状況　【問13-5】

第三者機関の認証制度等の利用状況については、「特に利用していない」が79.1％で最も高い。次いで「ＩＳＭＳ」が11.8％、「Ｐマーク」が8.4％となっている。

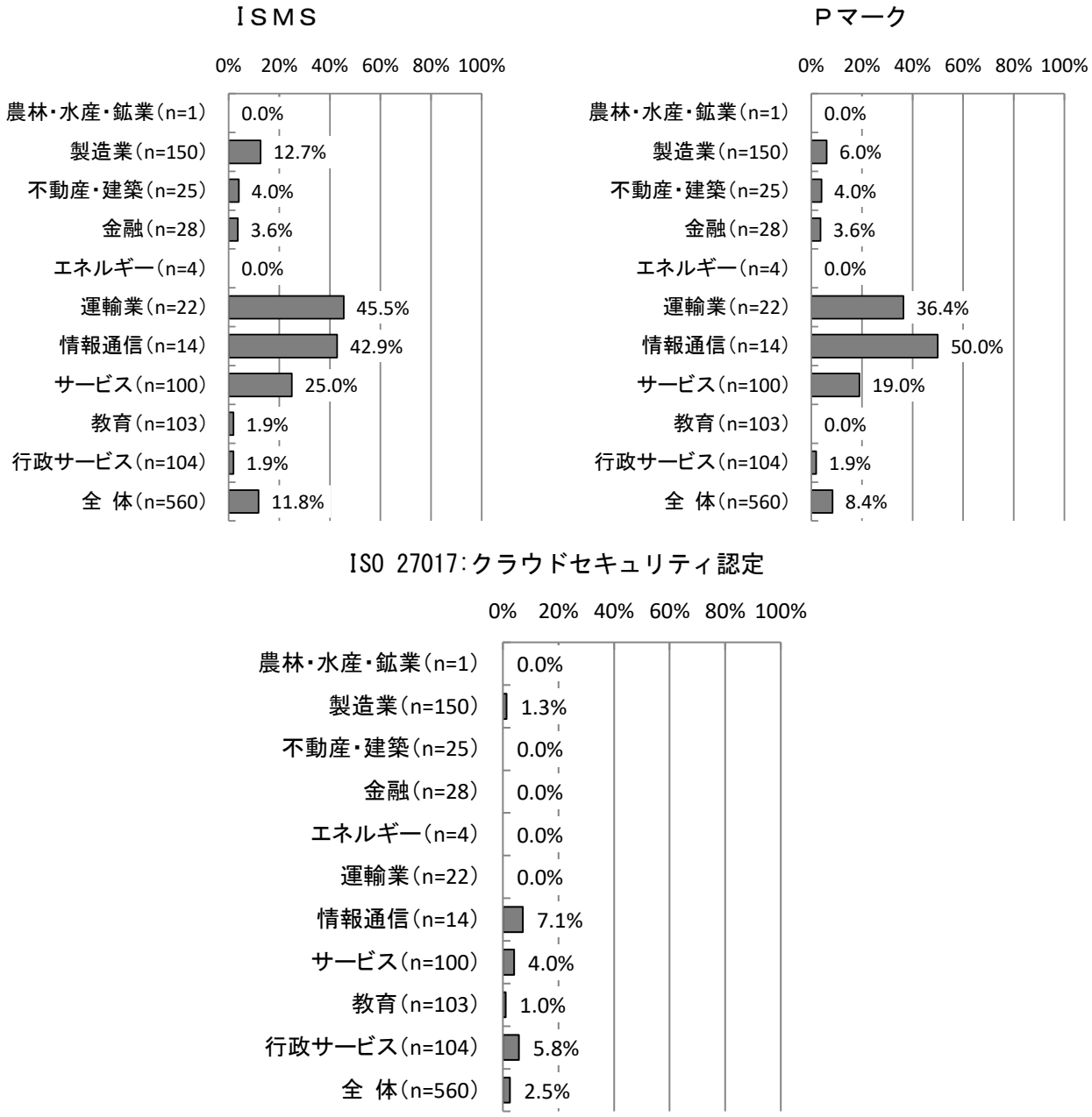
※本項目は、情報セキュリティ対策を行っている社・団体等を対象としている。

【全体】第三者機関の認証制度等の利用状況（MA, n=560）



【業種別分析】業種別にみると、「ＩＳＭＳ」については、「運輸業」の45.5%、「情報通信」の42.9%で高くなっている。「Pマーク」については、「情報通信」で50.0%で高くなっている。

【業種別分析】第三者機関の認証制度等の利用状況

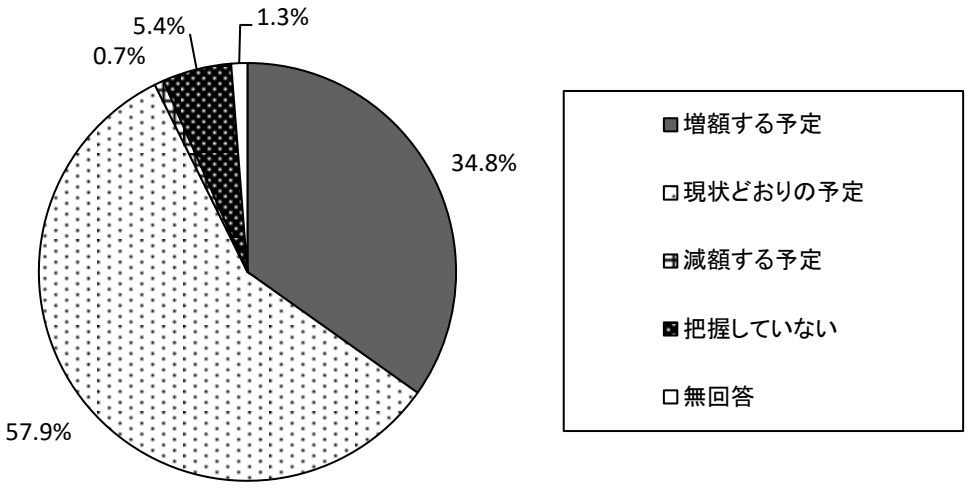


3.1.28　次年期の情報セキュリティ対策の投資計画　【問13-6】

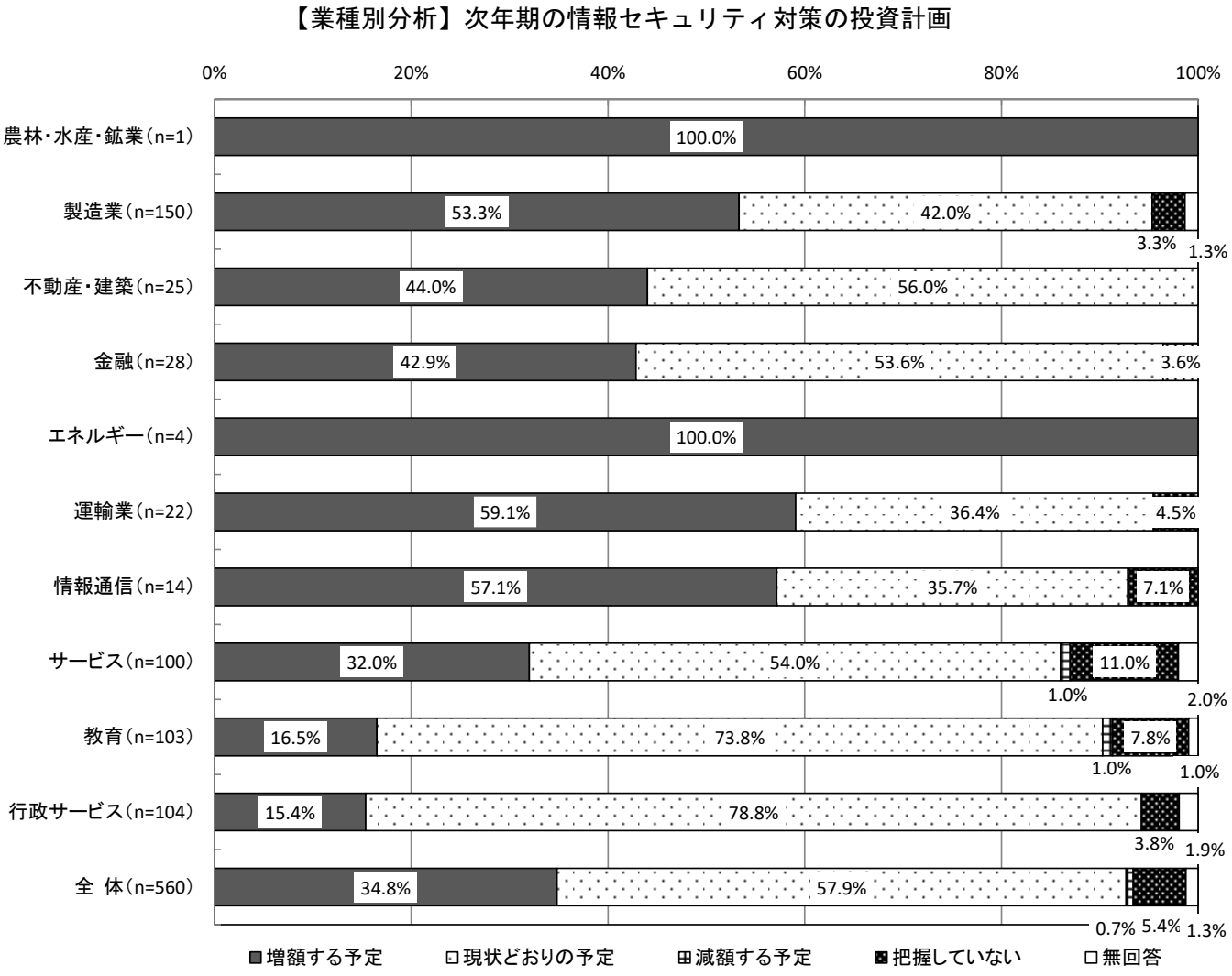
次年期（年単位）の情報セキュリティ対策の投資計画については、「現状どおりの予定」が57.9%で最も高く、次いで「増額する予定」が34.8%となっている。これに対して「減額する予定」は0.7%とわずかな割合にとどまっている。

※本項目は、情報セキュリティ対策を行っている社・団体等を対象としている。

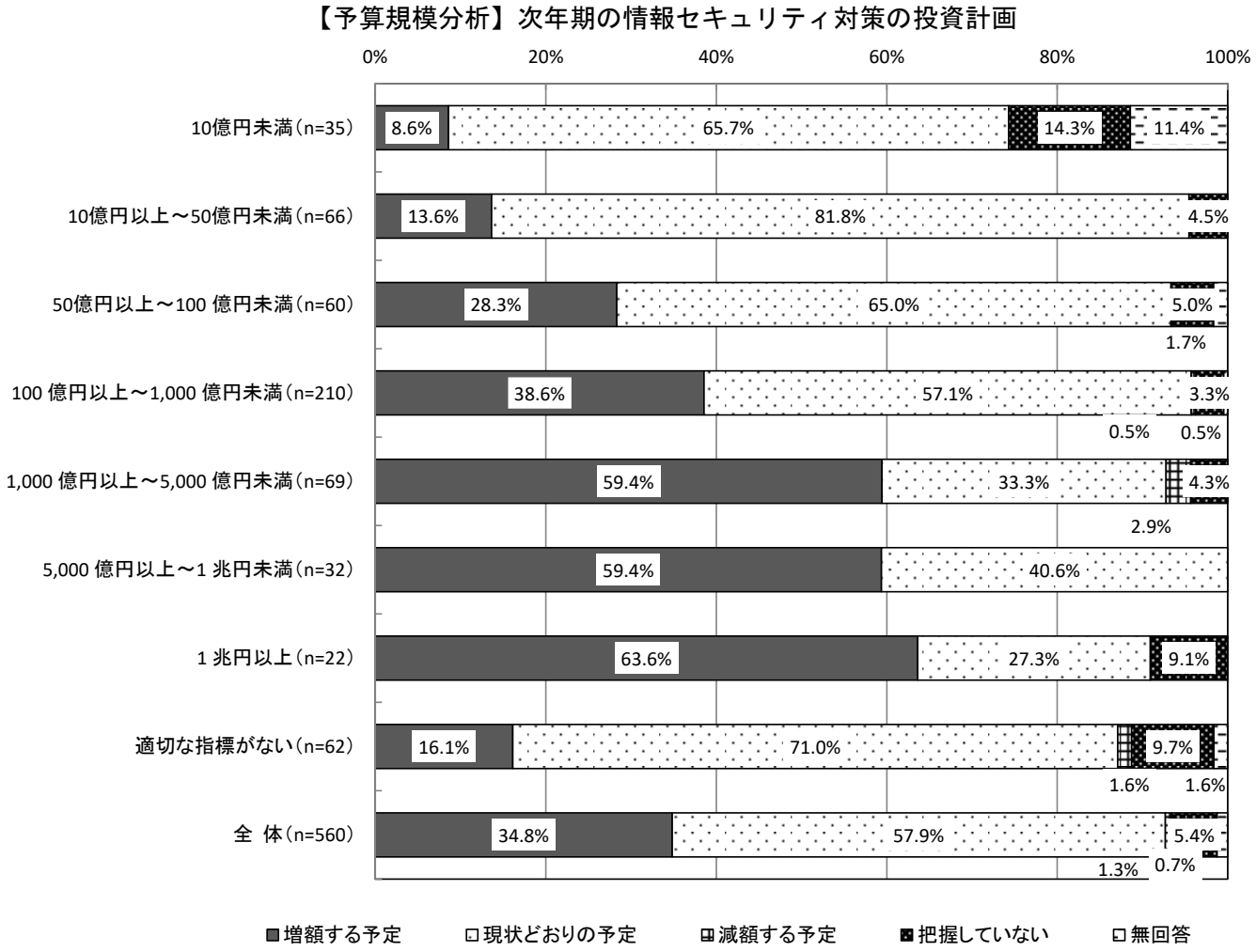
【全体】次年期の情報セキュリティ対策の投資計画（SA,n=560）



【業種別分析】業種別にみると、今期と比較して投資額を「増額する予定」については、「運輸業」が59.1%、「情報通信業」が57.1%で「現状どおりの予定」については、「行政サービス」が78.8%で最も高く、次いで「教育」が73.8%となっている。



【予算規模別分析】予算規模別にみると、今期と比較して投資額を「増額する予定」は、については、「1兆円以上」が63.6%で最も高く、次いで「5,000億円以上～１兆円未満」と「1,000億円以上～5,000億円未満」が59.4%となっている。これに対して「10億円未満」では8.6%と低く、規模が大きくなるほど増額する予定も高くなっている。

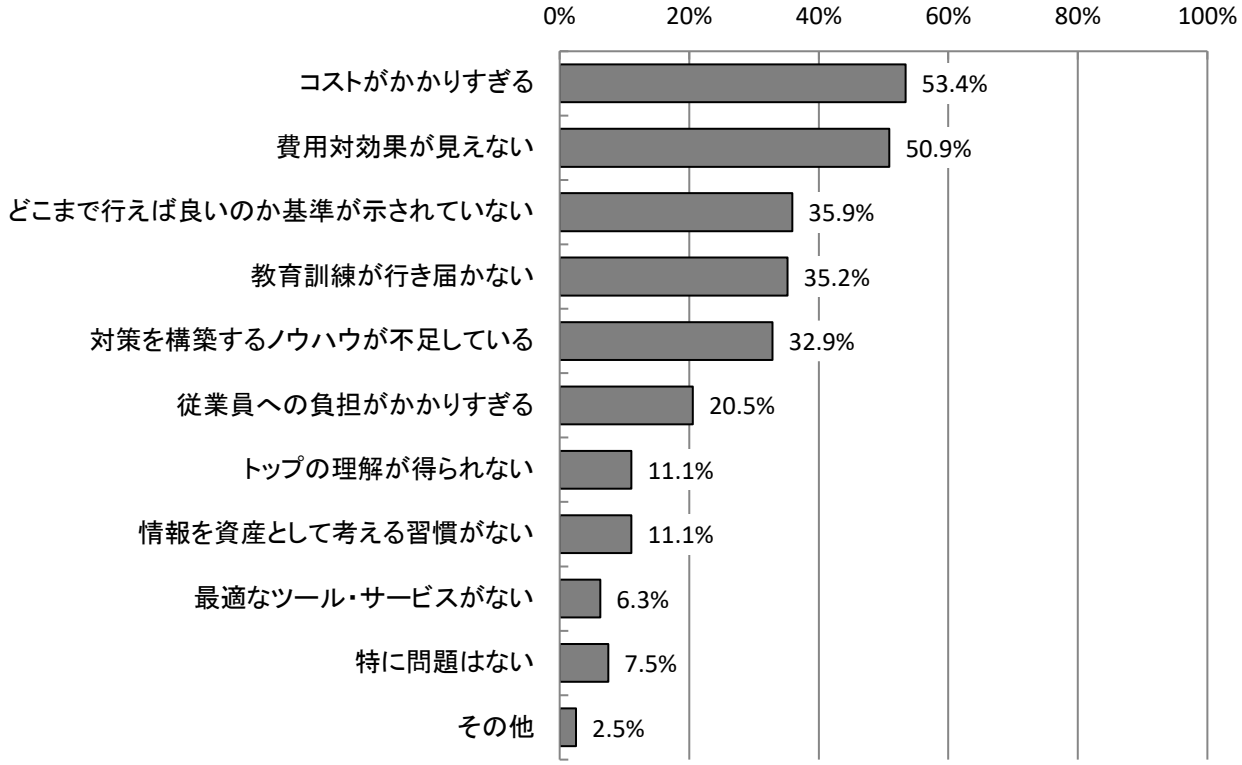


3.1.29　情報セキュリティ対策への投資に関する問題点　【問13-7】

情報セキュリティ対策への投資に関する問題点については、「コストがかかりすぎる」が53.4%、「費用対効果が見えない」が50.9%で高く、過半数となっている。次いで「どこまで行えば良いのか基準が示されていない」が35.9%、「教育訓練が行き届かない」が35.2%となっている。

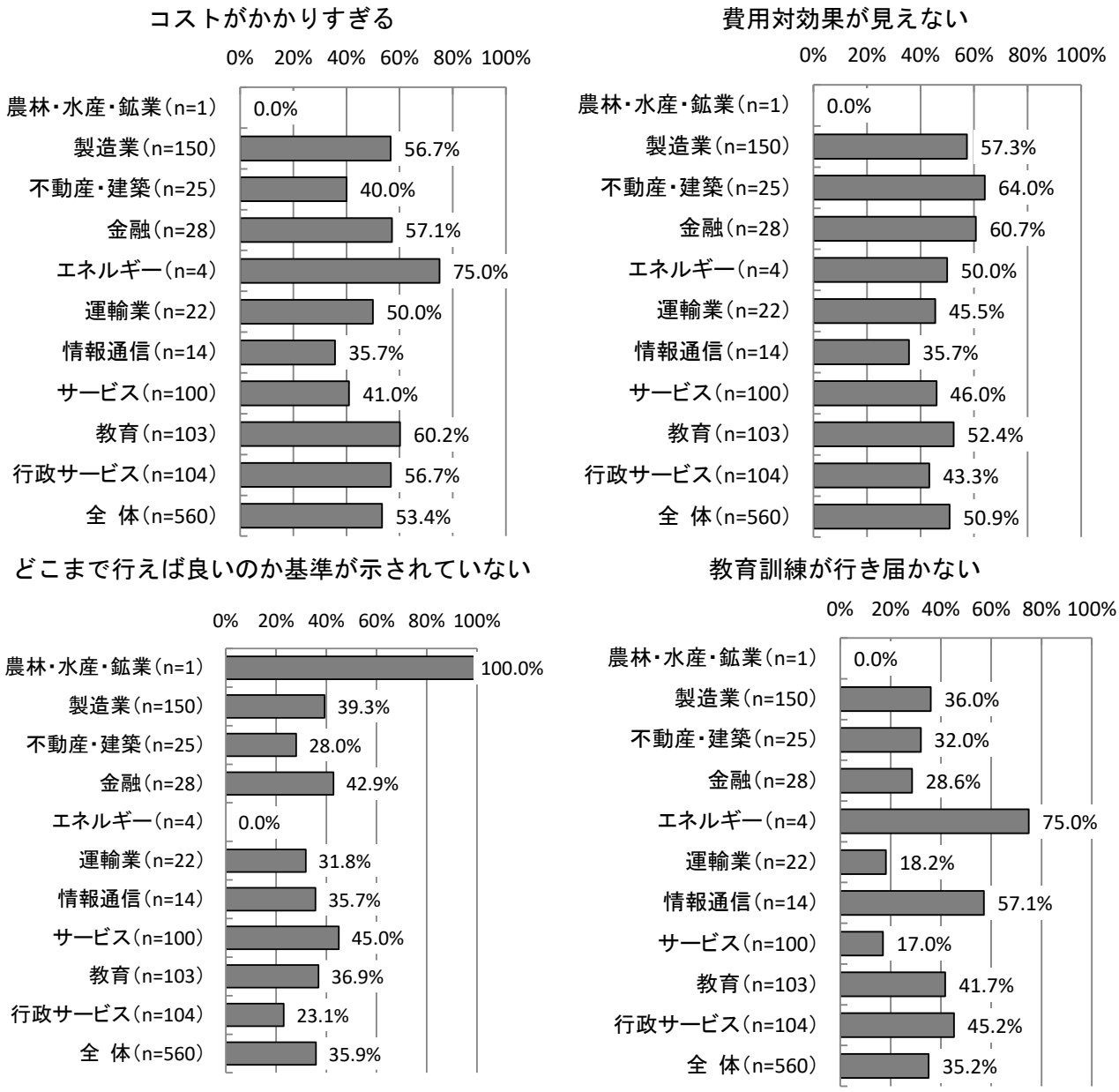
※本項目は、情報セキュリティ対策を行っている社・団体等を対象としている。

【全体】情報セキュリティ対策への投資に関する問題点（MA,n=560）



【業種別分析】業種別にみると、「コストがかかりすぎる」については、「教育」が60.2%で高くなっている。「費用対効果が見えない」については、「不動産・建築」が64.0%、「金融」が60.7%で高い。「どこまで行えば良いのか基準が示されていない」については、「サービス」が45.0%、「金融」が42,9%」で高く、「教育訓練が行き届かない」では、「情報通信」が57.1%で高くなっている。

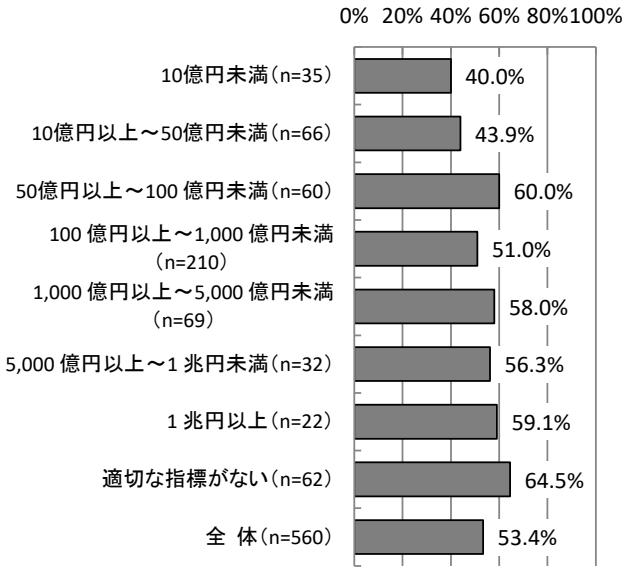
【業種別分析】情報セキュリティ対策への投資に関する問題点



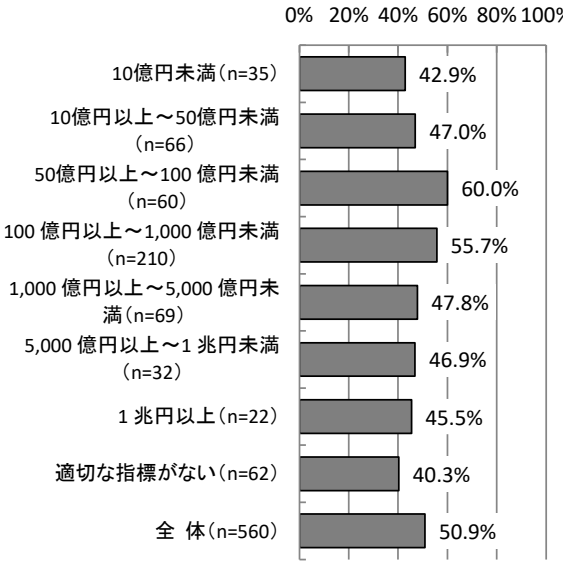
【売上・予算規模別分析】売上・予算規模別にみると、「コストがかかりすぎる」については、「50億円以上～100億円未満」が60.0%で最も高く、ついで「１兆円以上」が59.1%となっている。「どこまで行えば良いのか基準が示されていない」については、1,000億円以上～5,000億円未満」が43.5%高い。「費用対効果が見えない」については、「50億円以上～100億円未満」が60.0%で最も高くなっている。「教育訓練が行き届かない」では「適切な指標がない」の48.4%と、「50億円以上～１00億未満」の48.3%がほぼ同じ割合で高くなっている。

【売上・予算規模別分析】情報セキュリティ対策への投資に関する問題点

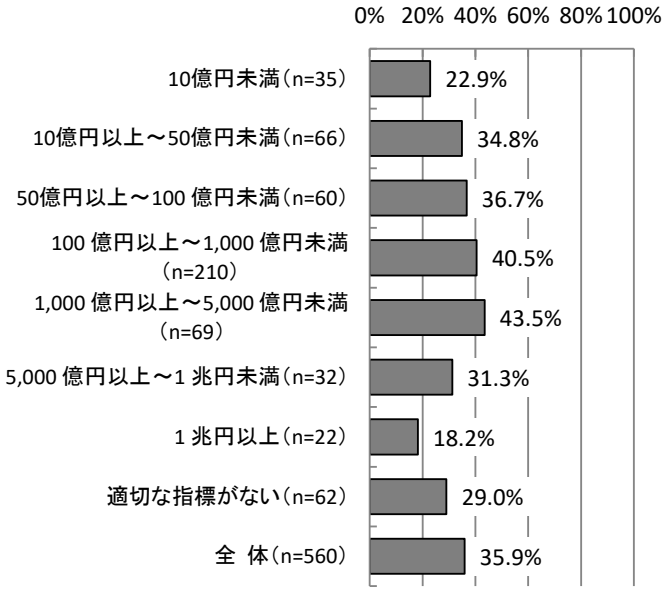
コストがかかりすぎる



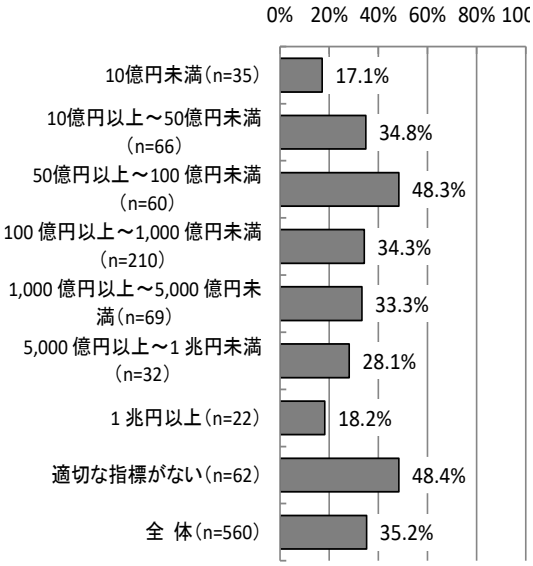
費用対効果が見えない



どこまで行えば良いのか基準が示されていない

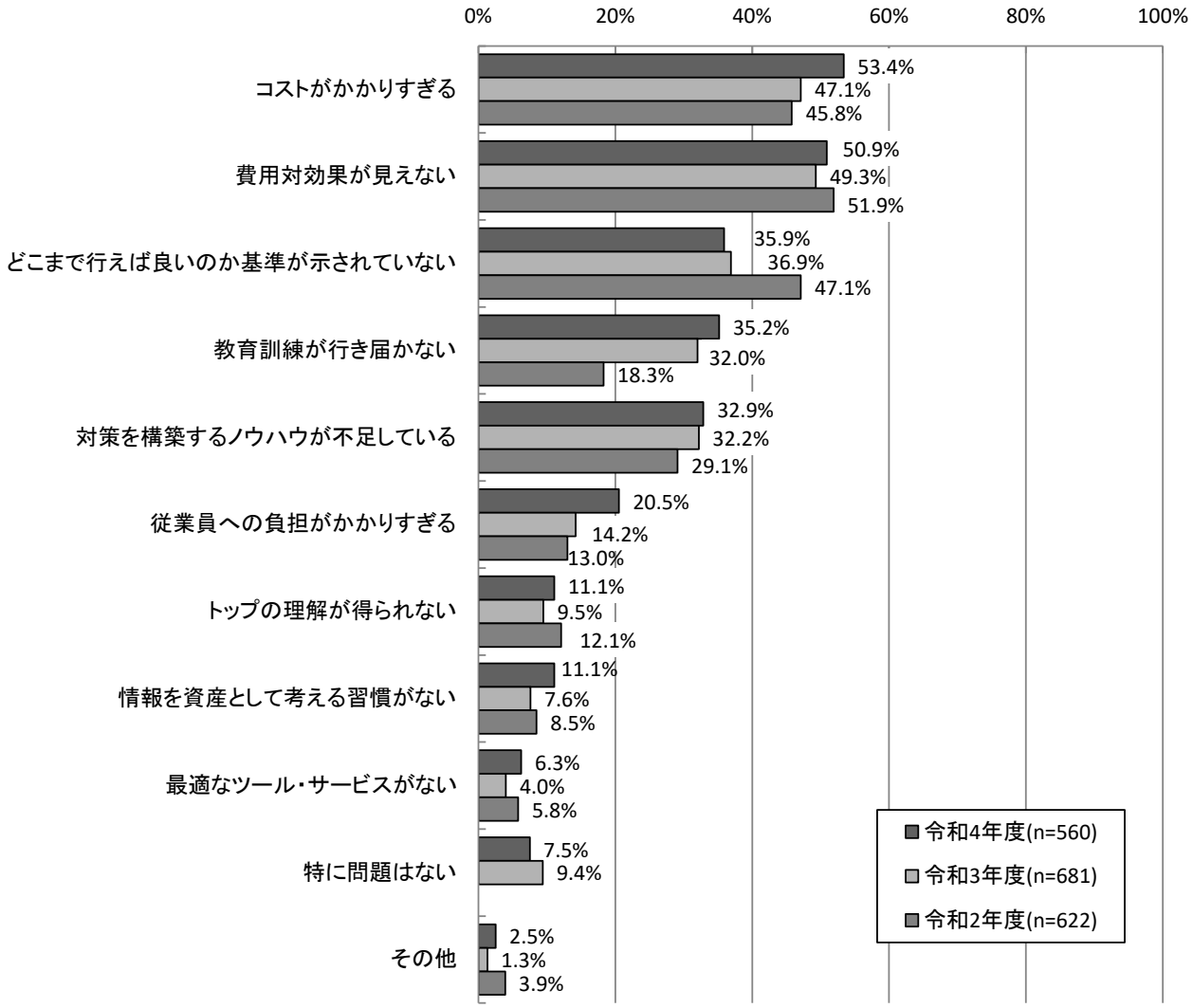


教育訓練が行き届かない



【経年変化】昨年度と比較すると、「コストがかかりすぎる」と「従業員への負担がかかりすぎる」が6.3ポイント増加している。一方、「どこまで行えば良いのか基準が示されていない」は減少幅は縮小したものの連続して減少している。

【経年変化】情報セキュリティ対策への投資に関する問題点



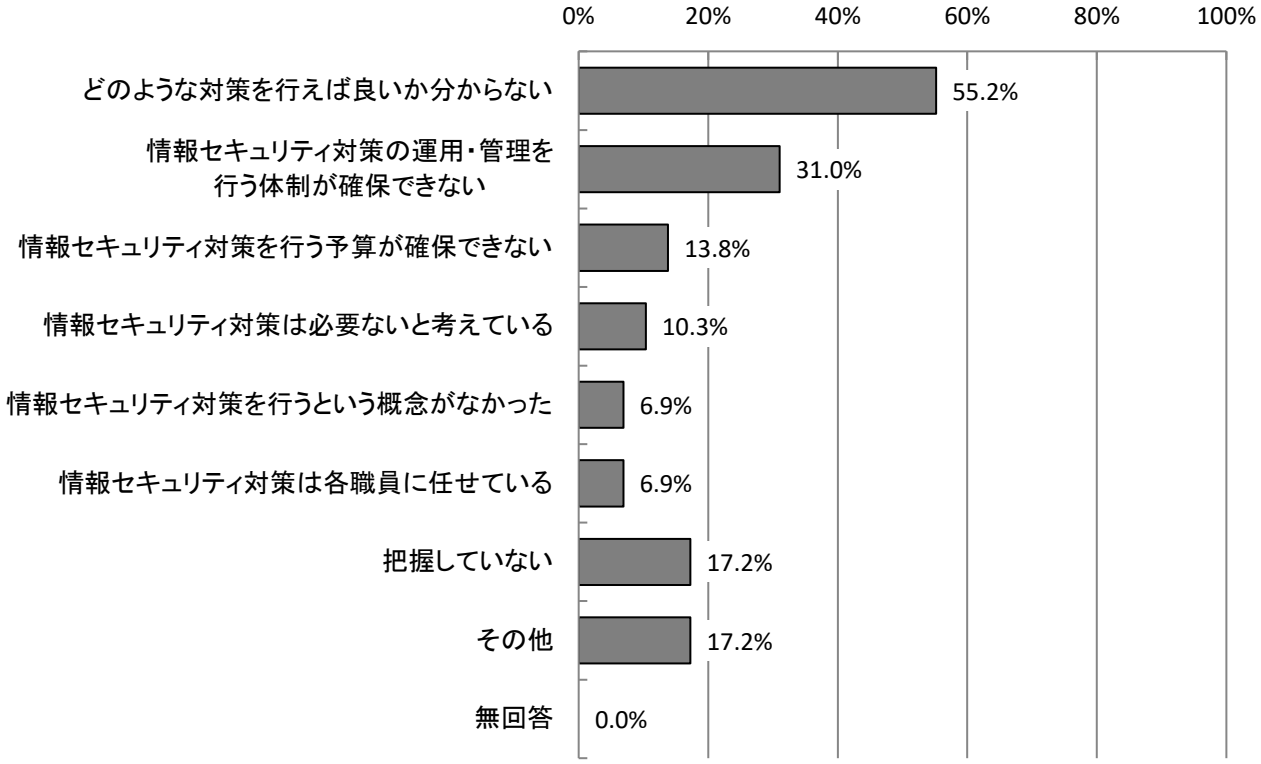
※令和３年度調査で、「特に問題はない」を新設。

3.1.30　情報セキュリティ対策を行っていない理由　【問13-8】

情報セキュリティ対策を行っていない理由については、「どのような対策を行えば良いか分からない」が55.2%で最も高く、次いで「情報セキュリティ対策の運用・管理を行う体制が確保できない」が31.0%となっている。

※本項目は、情報セキュリティ対策を行っていないと回答した社・団体等を対象としている。

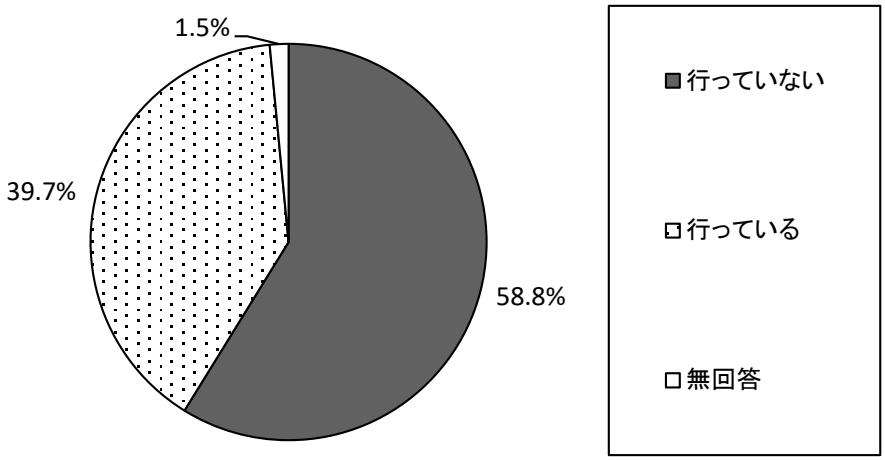
【全体】情報セキュリティ対策を行っていない理由（MA,n=29）



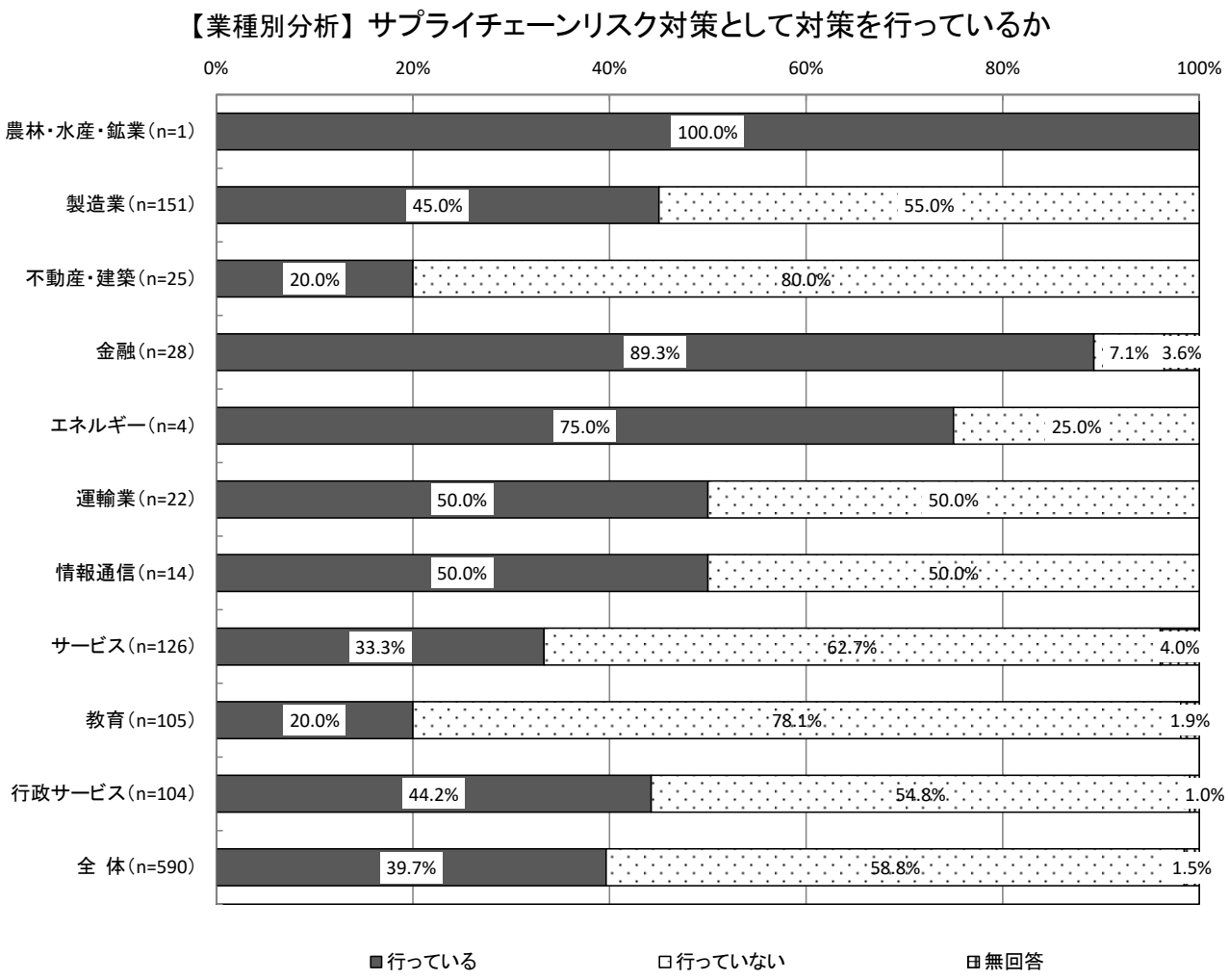
3.1.31　サプライチェーンリスク対策として対策を行っているか 【問14】

サプライチェーンリスク対策については「行っていない」が58.8%と高く、「行っている」が39.7%となっている。

【全体】サプライチェーンリスク対策として対策を行っているか（MA,n=590）



【業種別分析】業種別では、サプライチェーンリスク対策を「行っている」は「金融」の89.3%で高くなっている。一方、「教育」と「不動産」はいずれも20.0%で最も低くなっている。



3.1.32 情報セキュリティ対策に関する考え方 【問15】

本調査では、情報セキュリティ対策実施上の方針について、「投資方針」等6つの項目に関して尋ねた。具体的には、各項目について相対する2つの考え（①②）を提示し、社・団体等における考え方が①②のどちらの考え方に近いかを尋ねている。各項目について、「①とほぼ同様」「どちらかといえば①に近い」「どちらかといえば②に近い」「②とほぼ同様」のいずれか1つを回答する形式となっている。

本調査で尋ねた6つの項目と、それぞれにおいて示した、相対する2つの考え方は下記の通りとなっている。

調査対象とした基本的な考え方と相対する2つの考え

①として提示した考え方	②として提示した考え方
1. 投資方針	
セキュリティ投資は必要最低限に抑えるべきである。	来るべき問題事案に備えて、積極的に投資を行うべきである。
2. 事後的対応と予防的対応	
情報セキュリティ対策としては、問題発生に対しての応急対応や、再発防止・被害拡大防止に注力するべきである。	情報セキュリティ対策としては、リスクの検知など、予防上の対策に注力するべきである。
3. 保険への意識	
情報セキュリティ対策としては、人的・技術的な対策によりカバーできるところを対策すれば十分である。	情報セキュリティ対策としては、人的・技術的対策によりカバーできないリスクは保険によりまかなうべきである。
4. 規制・罰則への考え方	
技術以外の面での対策としては、従業員等への教育と、適切な情報提供により対策を促すことが重要である。	技術以外の面での対策としては、教育はもちろんのこと、規制・罰則などの強制力のある制度的対応を行うことが重要である。
5. プライバシーの考慮	
職場とはいえ、従業員等のプライバシーはある程度考慮したうえで、情報セキュリティ対策は行われるべきである。	職場のセキュリティ保護のためにはシステム利用状況のモニタリングなどによるプライバシー保護の制約はやむをえない。
6. 利便性とのバランス	
業務実施に負担をかけるほどのセキュリティ対策は不適当であり、利便性とのバランスを考慮すべきである。	ユーザーにシステム利用上・業務上の負担を強いてでもセキュリティを守るべきである。

【全体】「投資方針」については、「①セキュリティ投資は必要最低限度に抑えるべきである」に近いとする割合が25.6%、「②来るべき問題事案に備えて、積極的に投資を行うべきである」に近いとする割合が72.7%となっており、「積極的」とする割合が「必要最低限」とする割合を47.1ポイント上回っている。

「事後的対応と予防的対応」については、「①情報セキュリティ対策としては、問題発生に対しての応急対応や、再発防止・被害拡大防止に注力するべきである」に近いとする割合が23.4%、「②情報セキュリティ対策としては、リスクの検知など、予防上の対策に注力するべきである」に近いとする割合が74.9%となっており、「予防的対応」とする割合が「問題発生への適切な対応」とする割合を51.5ポイントと大幅に上回っている。

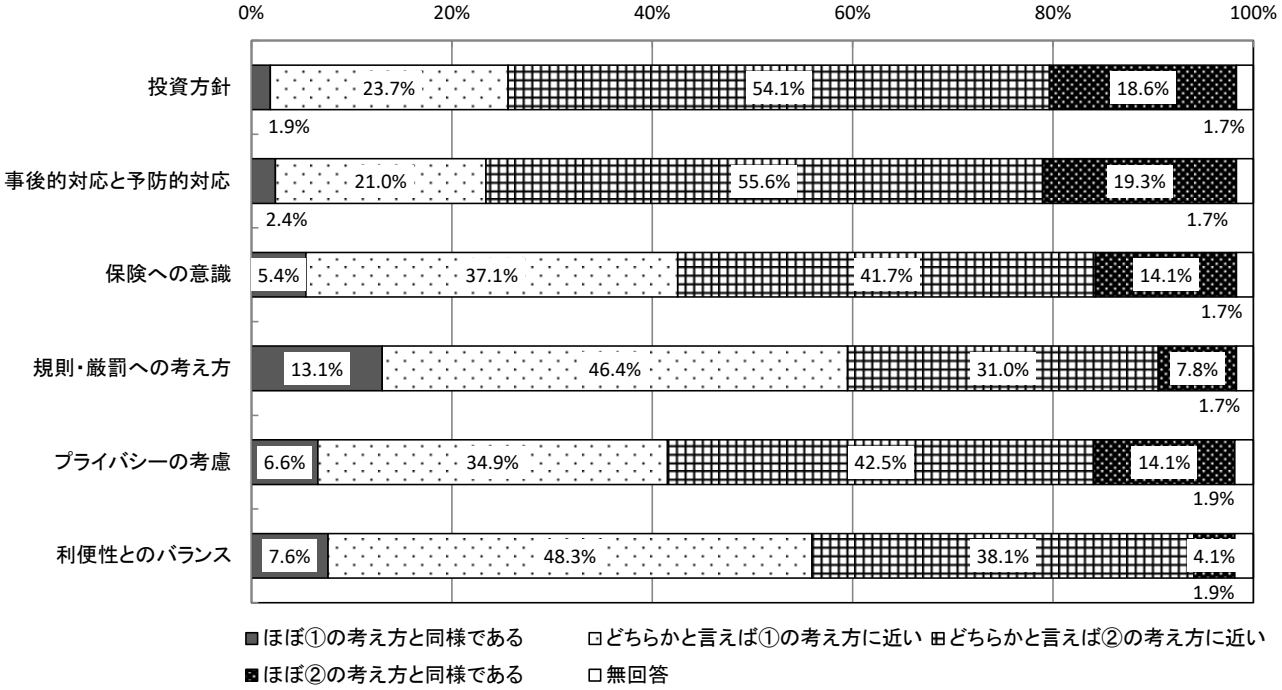
「保険への意識」については、「①情報セキュリティ対策としては、人的・技術的な対策によりカバーできるところを対策すれば十分である」に近いとする割合が42.5%、「②情報セキュリティ対策としては、人的・技術的対策によりカバーできないリスクは保険によりまかなうべきである」に近いとする割合が55.8%で、「保険的な対応が必要」とする割合が「人的・技術的な対策で十分」を13.3ポイント上回っている。

「規制・罰則への考え方」については、「①技術以外の面での対策としては、従業員等への教育と、適切な情報提供により対策を促すことが重要である」に近いとする割合が59.5%、「②技術以外の面での対策としては、教育はもちろんのこと、規制・罰則などの強制力のある制度的対応を行うことが重要である」に近いとする割合が38.8%となっており、「教育と情報提供を中心とした対応」とする割合が「規則・罰則も含む強制力のある対応」を20.7ポイント上回っている。

「プライバシーの考慮」については、「①職場とはいえ、従業員等のプライバシーはある程度考慮したうえで、情報セキュリティ対策は行われるべきである」に近いとする割合が41.5%、「②職場のセキュリティ保護のためにはシステム利用状況のモニタリングなどによるプライバシーの侵害はやむをえない」に近いとする割合が56.6%となっており、「ある程度のプライバシー保護の制約はやむをえない」とする割合が「プライバシーはある程度考慮されるべきだ」とする割合を15.1ポイント上回っている。

「利便性とのバランス」については、「①業務実施に負担をかけるほどのセキュリティ対策は不適当であり、利便性とのバランスを考慮すべきである」に近いとする割合が55.9%、「②ユーザーにシステム利用上・業務上の負担を強いてでもセキュリティを守るべきである」とする42.2%となっており、「利便性とのバランスを考慮」とする割合が「負担を強いてでもセキュリティを守る」とする割合を13.7ポイント上回っている。

【全体】情報セキュリティ対策に関する考え方（SA,n=590）

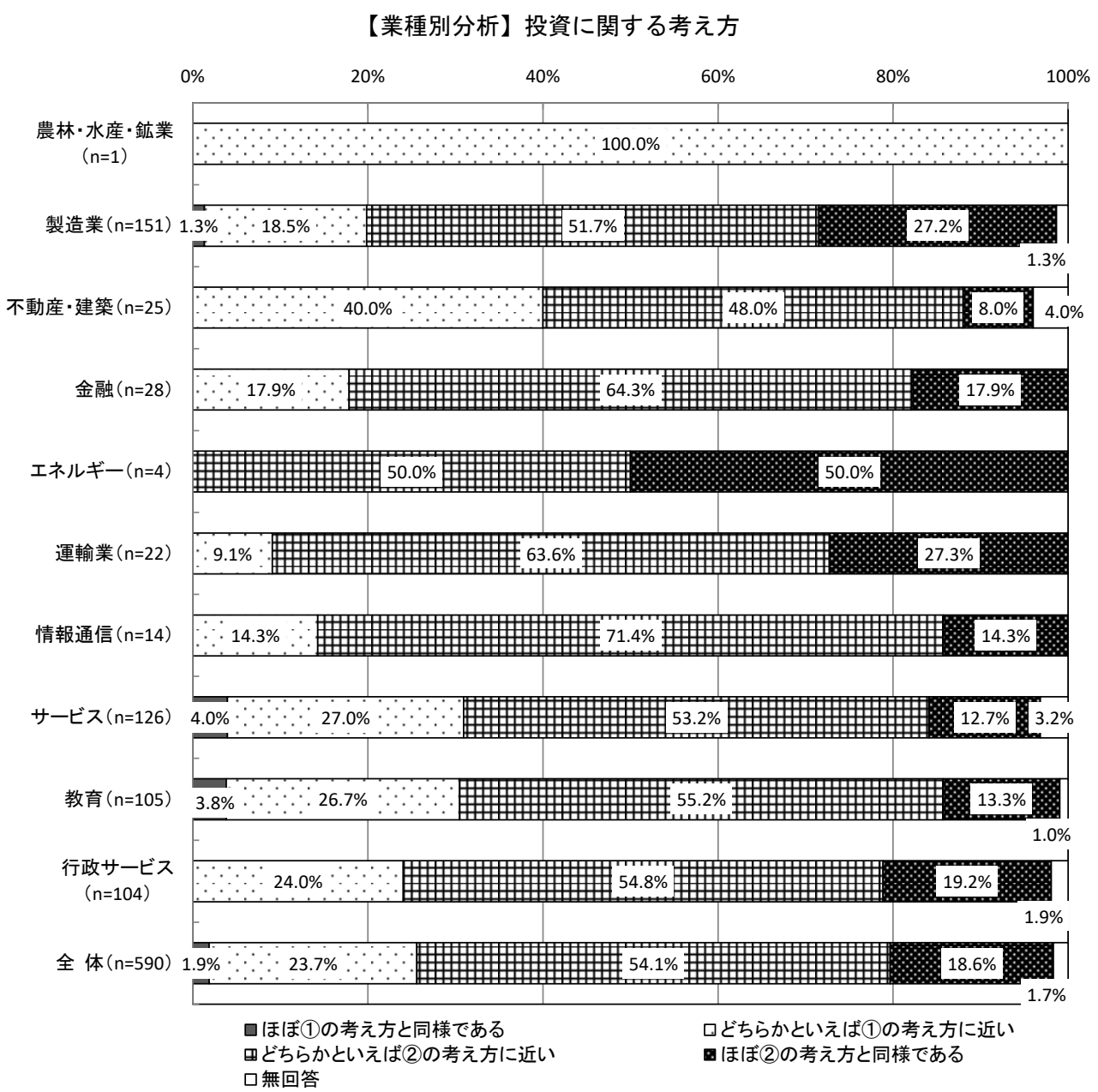


3.1.33　投資に関する考え方　【問15-1】

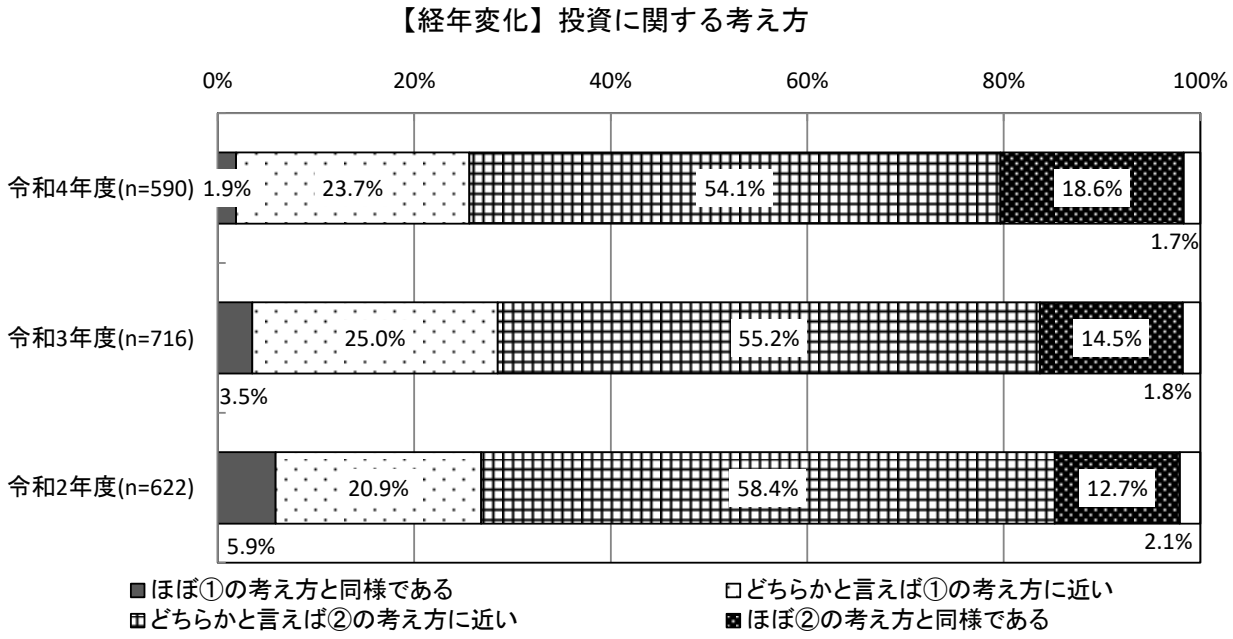
情報セキュリティに対する投資方針については、下記に挙げる2つの考え方のいずれに近いかを尋ねている。

①として提示した考え方	②として提示した考え方
セキュリティ投資は必要最低限に抑えるべきである。	来るべき問題事案に備えて、積極的に投資を行うべきである。

【業種別分析】業種別にみると、投資方針に関して全ての業種で、「②積極的投資」の割合が多く、特に「運輸業」が90.9%、「金融」が82.2%と高くなっている。



【経年変化】昨年度と比較すると、「①必要最低限」は2.9ポイントの減少、「②積極的投資」は3.0ポイントの増加となっている。



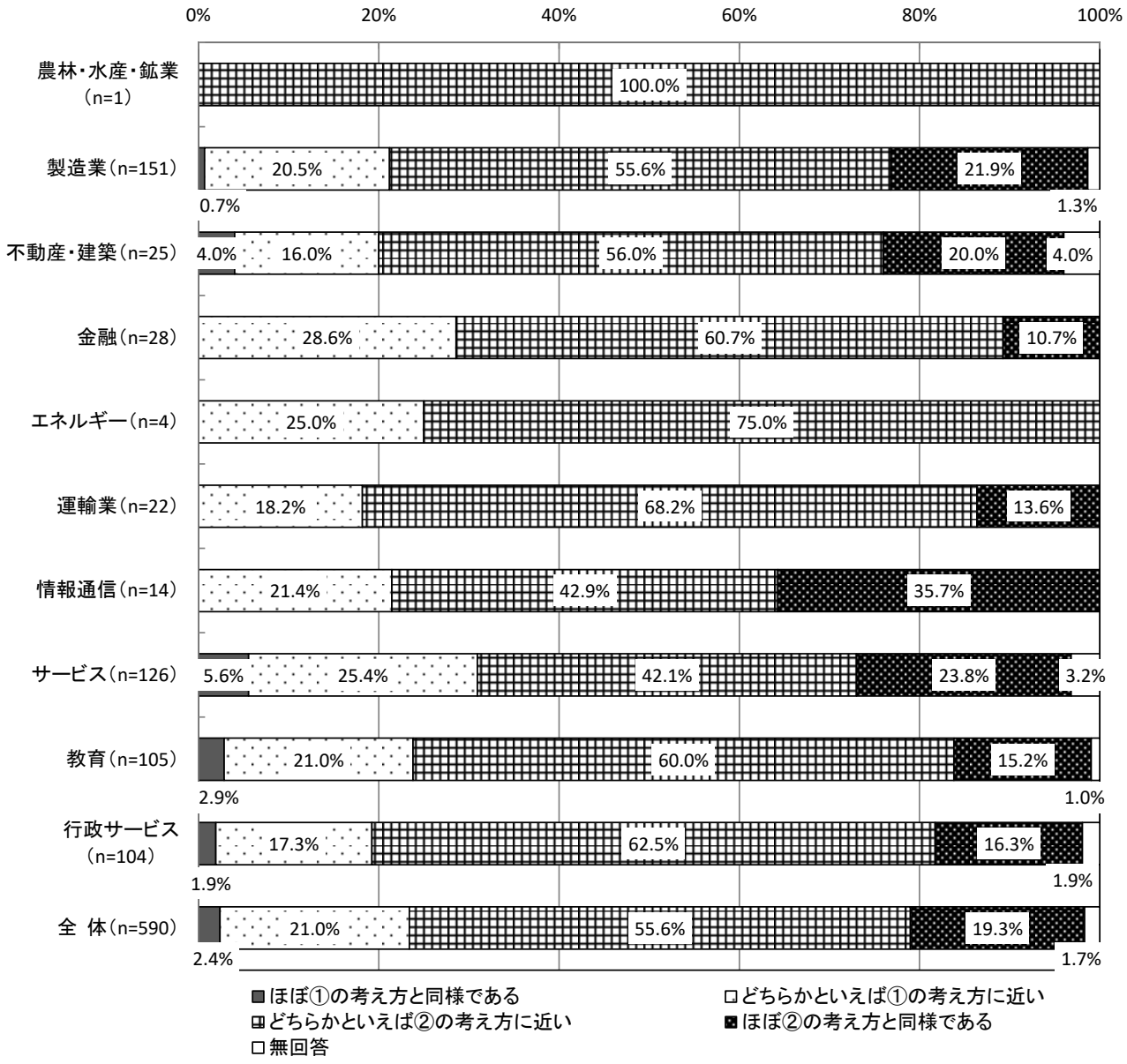
3.1.34　事後的対応と予防的対応に関する考え方　【問15-2】

情報セキュリティ対策については、下記に挙げる2つの考え方のいずれに近いかを尋ねている。

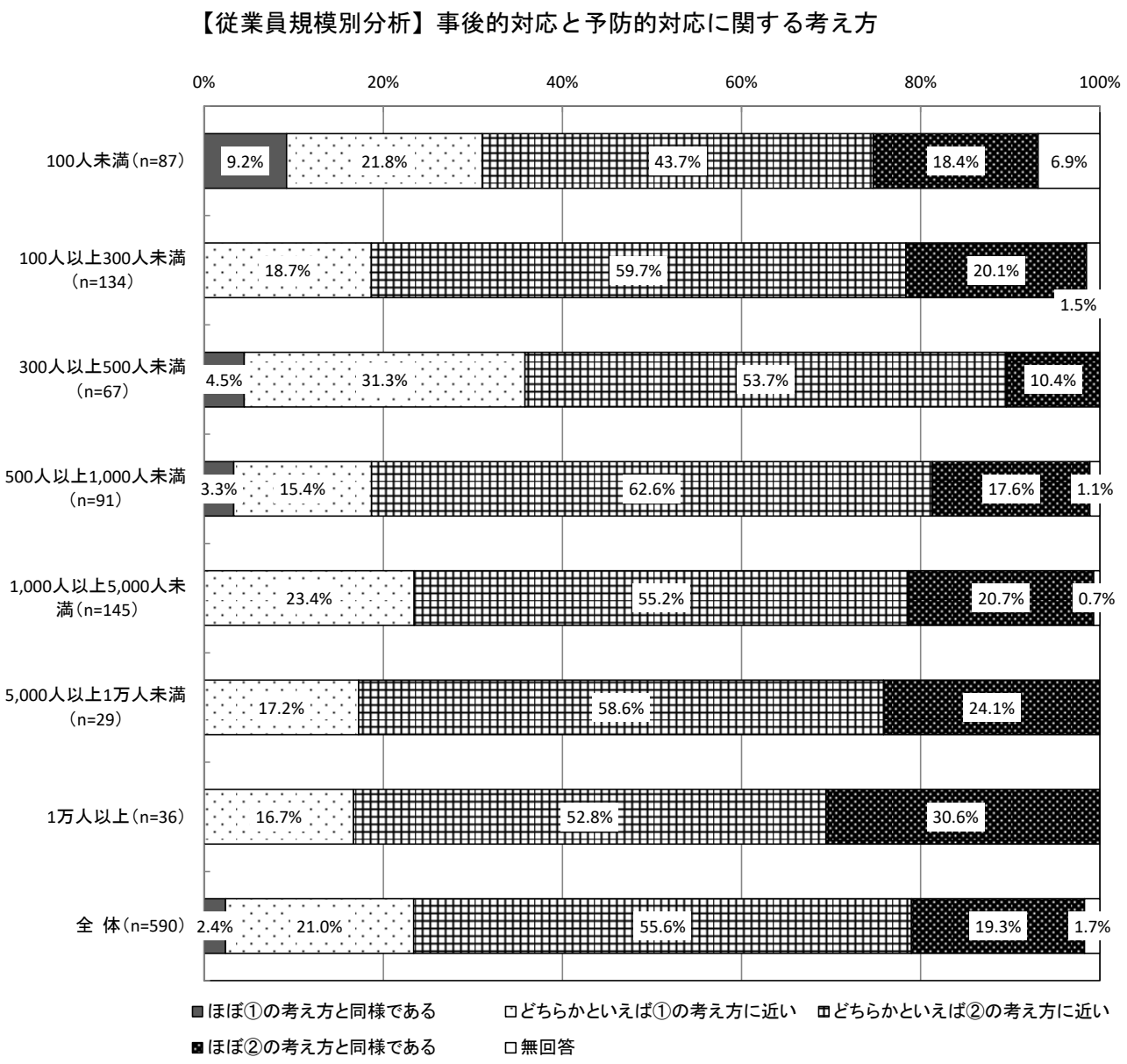
①として提示した考え方	②として提示した考え方
情報セキュリティ対策としては、問題発生に対しての応急対応鞠や、再発防止・被害拡大防止に注力すべきである。	情報セキュリティ対策としては、リスク検知など、予防上の対策に注力すべきである。

【業種別分析】業種別にみると、全ての業種で「②予防的対応」の割合が多く、特に「運輸業」が81.8%、「行政サービス」が78.8%と高くなっている。

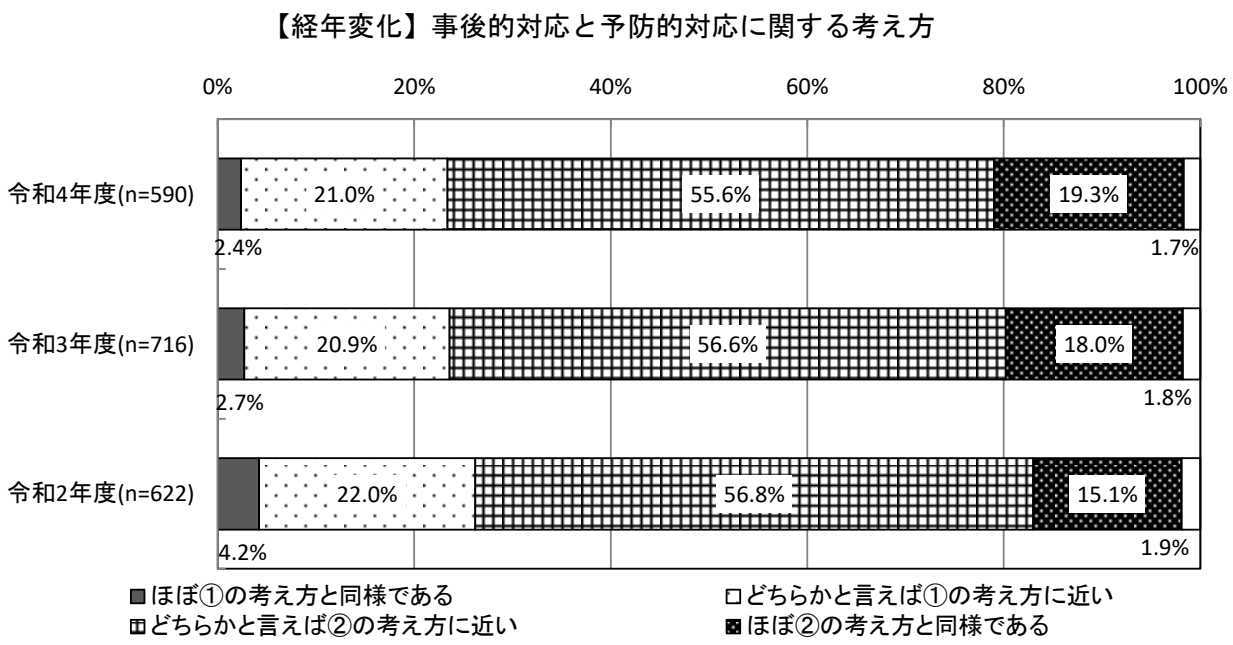
【業種別分析】事後的対応と予防的対応に関する考え方



【従業員規模別分析】従業員規模別にみると、全ての従業員規模で「②予防的対応」が「①問題発生への適切な対応」を上回っている。



【経年変化】昨年度と比較すると、「①事後的対応」は0.2ポイントの減少、「②予防的対応」は0.3ポイントの増加と、ほぼ同じ結果となっている。



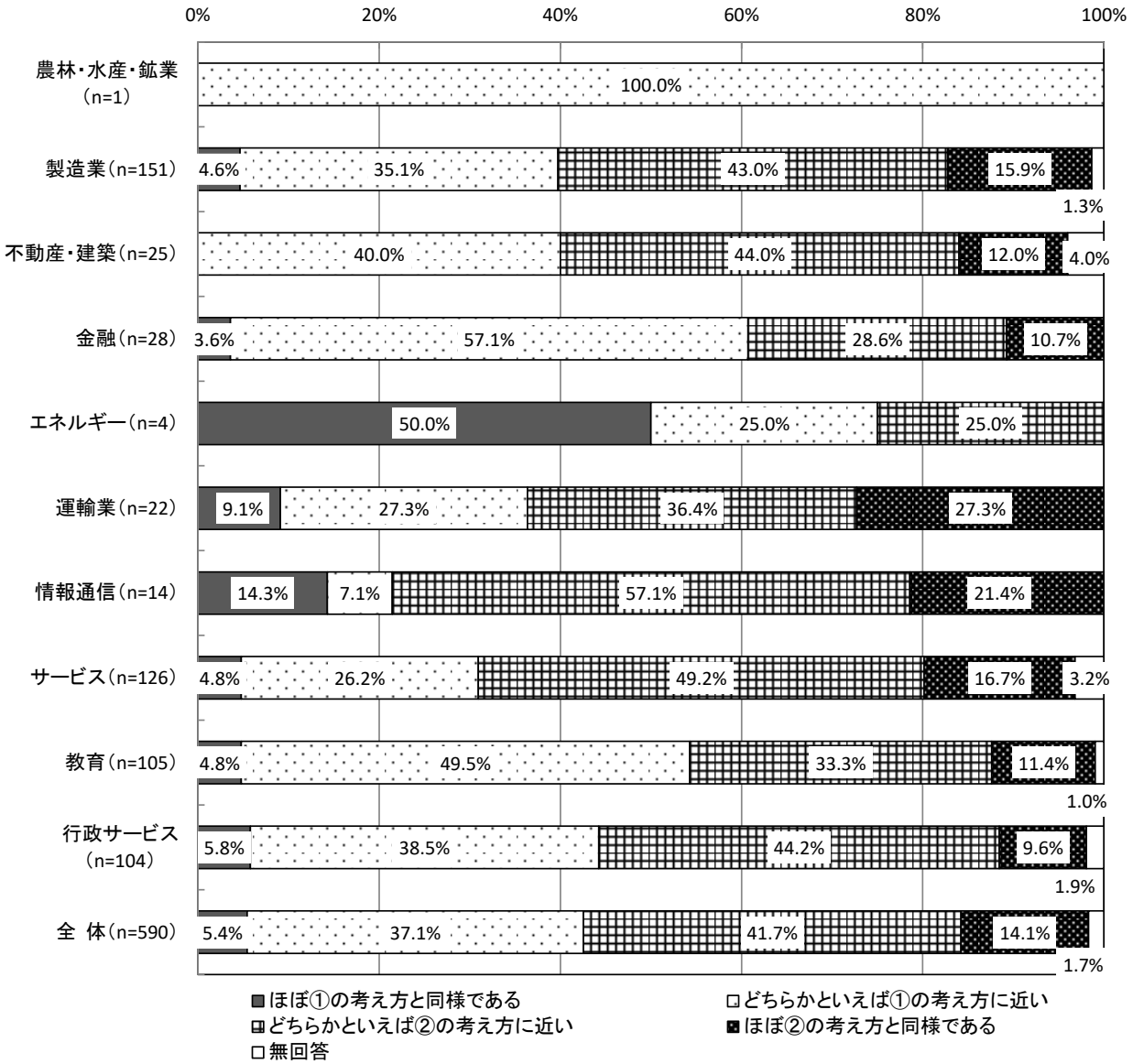
3.1.35　保険への意識　【問15-3】

情報セキュリティ対策において保険への意識については、下記に挙げる2つの考え方のいずれに近いかを尋ねている。

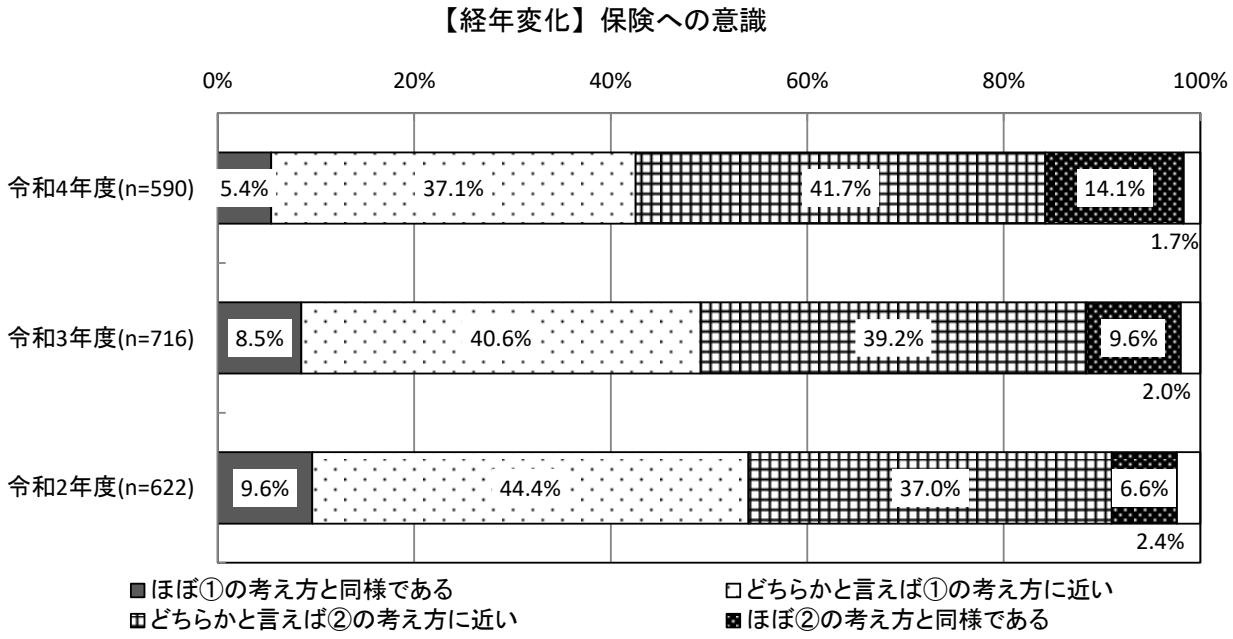
①として提示した考え方	②として提示した考え方
情報セキュリティ対策としては、人的・技術的な対策によりカバーできるところを対策すれば十分である。	情報セキュリティ対策としては、人的・技術的対策によりカバーできないリスクは保険によりまかなうべきである。

【業種別分析】業種別にみると、「金融」「教育」で「①人的・技術的な対策で十分」が「②保険的な対応が必要」を上回っており、特に「金融で」で60.7%と高い。一方、「製造業」「不動産・建築」「運輸業」「情報通信」「サービス」「行政サービス」では「②保険的な対応が必要」が「①人的・技術的な対策で十分」を上回っており、特に「情報通信」で78.5%と高くなっている。

【業種別分析】保険への意識



【経年変化】昨年度と比較すると、「①人的・技術的な対策で十分」は6.6ポイントの減少となり、「②保険的な対応が必要」は7.0ポイントの増加となっている。

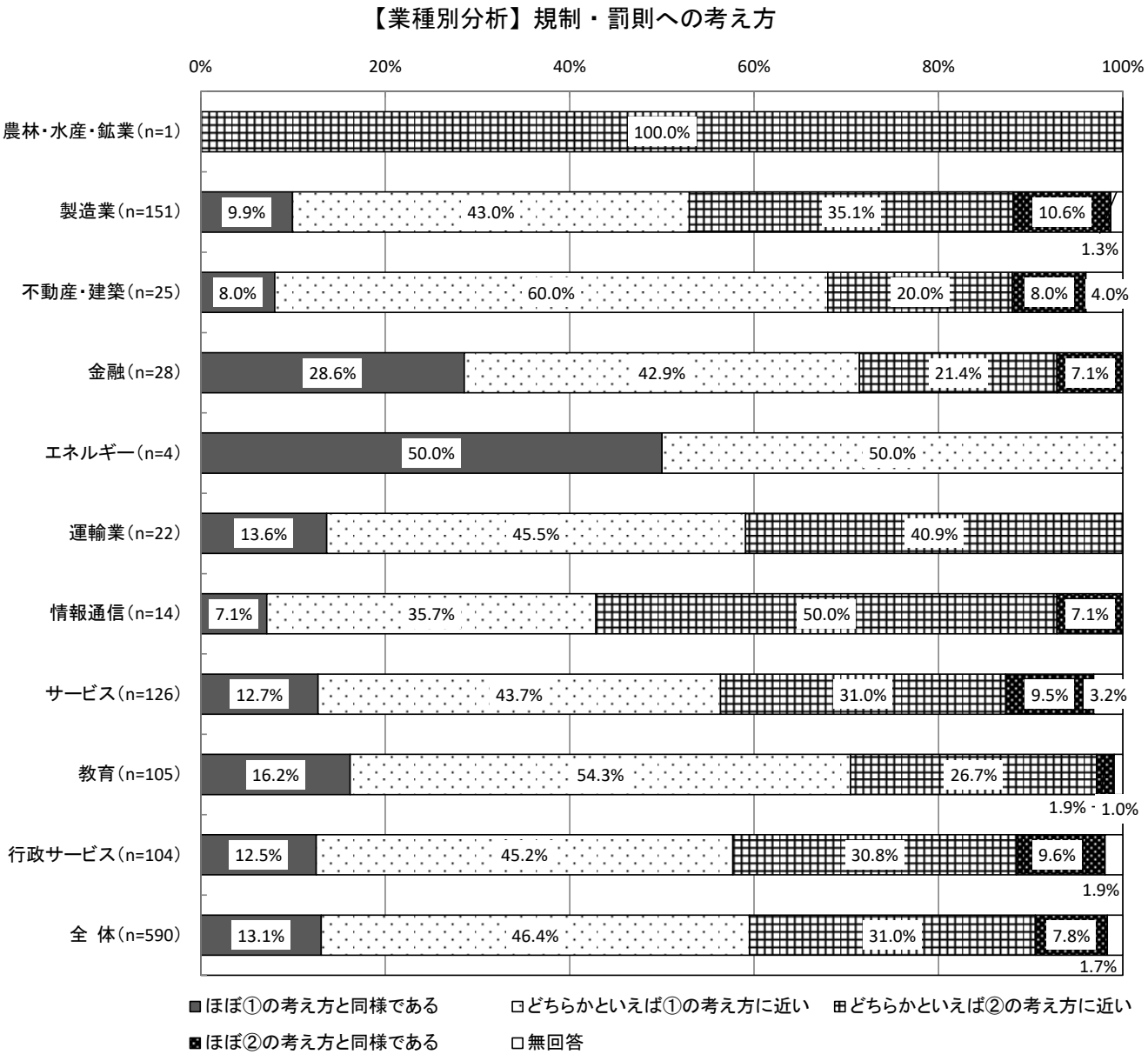


3.1.36　規制・罰則への考え方　【問15-4】

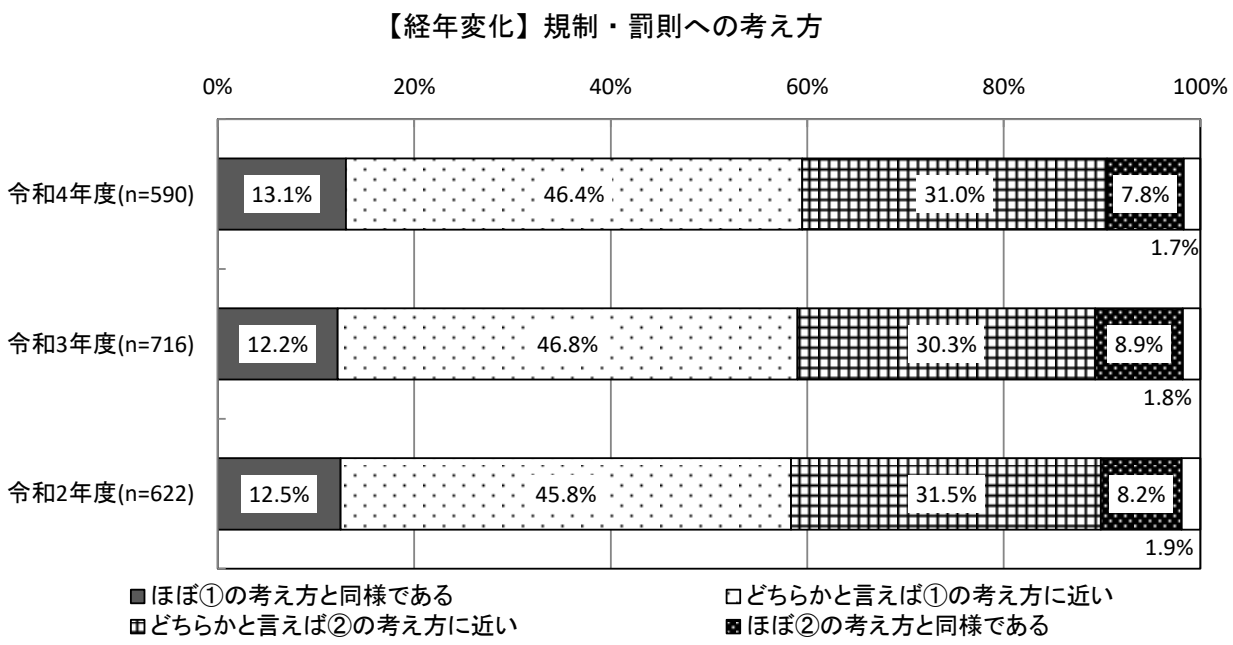
規制・罰則への考え方については、下記に挙げる2つの考え方のいずれに近いかを尋ねている。

①として提示した考え方	②として提示した考え方
技術以外の面での対策としては、従業員等への教育と適切な情報提供により対策を促すことが重要である。	技術以外の面での対策としては、教育はもちろんのこと、規則・罰則などの強制力のある制度的対応を行うことが重要である。

【業種別分析】業種別にみると、「情報通信」を除くほぼすべての業種で「①教育と情報提供を中心とした対応」が「②規則・罰則も含む強制力のある対応」を上回っている。特に「金融」と「教育」では「①人的・技術的な対策で十分」が40.0ポイント上回っている。



【経年変化】昨年度と比較すると、「①教育と情報提供を中心とした対応」は0.5ポイントの増加、「②規則・罰則も含む強制力のある対応」は0.4ポイントの減少となっている。



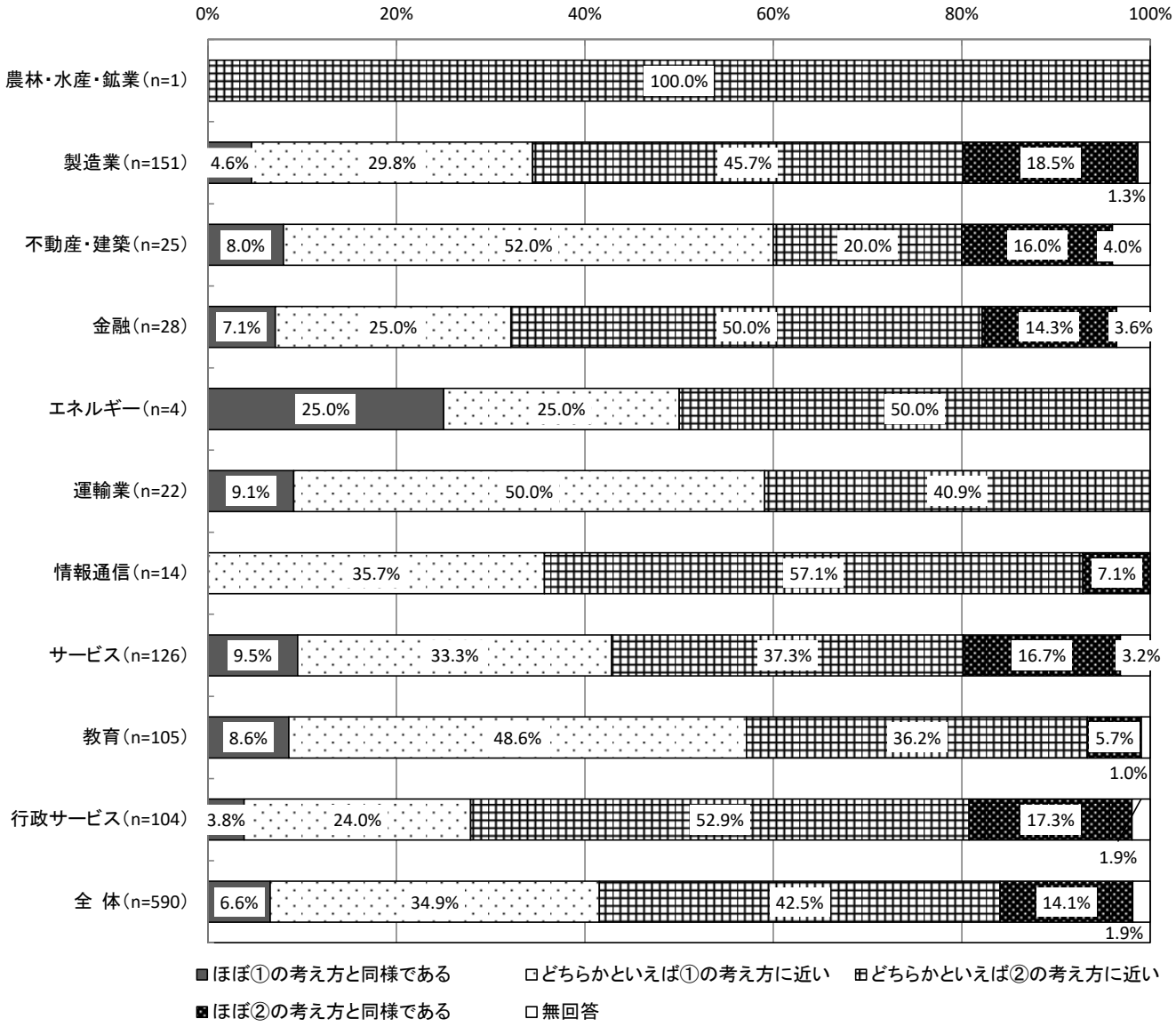
3.1.37　プライバシーの考慮に関する考え方　【問15-5】

従業員等のプライバシーの取扱いについて、下記に挙げる2つの考え方のいずれに近いかを尋ねている。

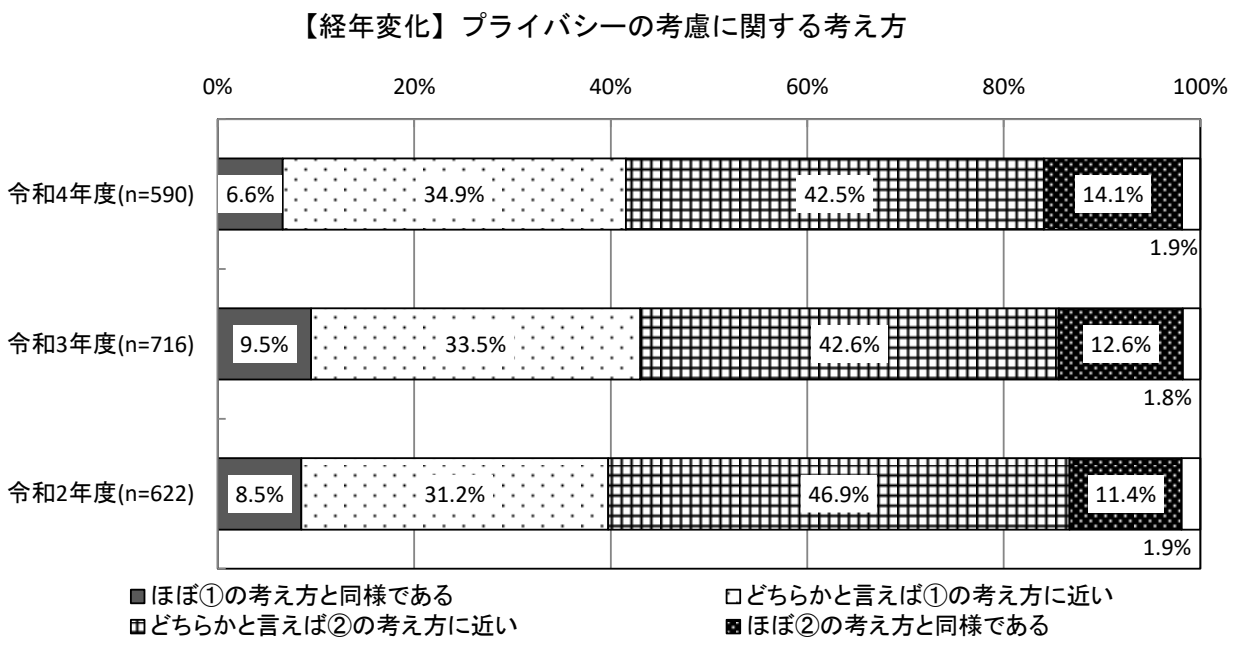
①として提示した考え方	②として提示した考え方
職場とはいえ、従業員等のプライバシーはある程度考慮したうえで、情報セキュリティ対策は行われるべきである。	職場のセキュリティ保護のためにはシステム利用状況のモニタリングなどによるプライバシー保護の制約はやむをえない。

【業種別分析】業種別を見ると、「不動産・建築」「教育」を除くすべての業種で「②プライバシーの侵害はやむをえない」が「①プライバシーはある程度考慮すべき」を上回っている。特に「行政サービス」で42.4ポイント「②プライバシー保護の制約はやむをえない」が多くなっている。

【業種別分析】プライバシーの考慮に関する考え方



【経年変化】昨年度と比較すると、「①プライバシーはある程度考慮すべき」は1.5ポイントの減少、「②プライバシーの保護の制約はやむをえない」は1.4ポイントの増加となっている。



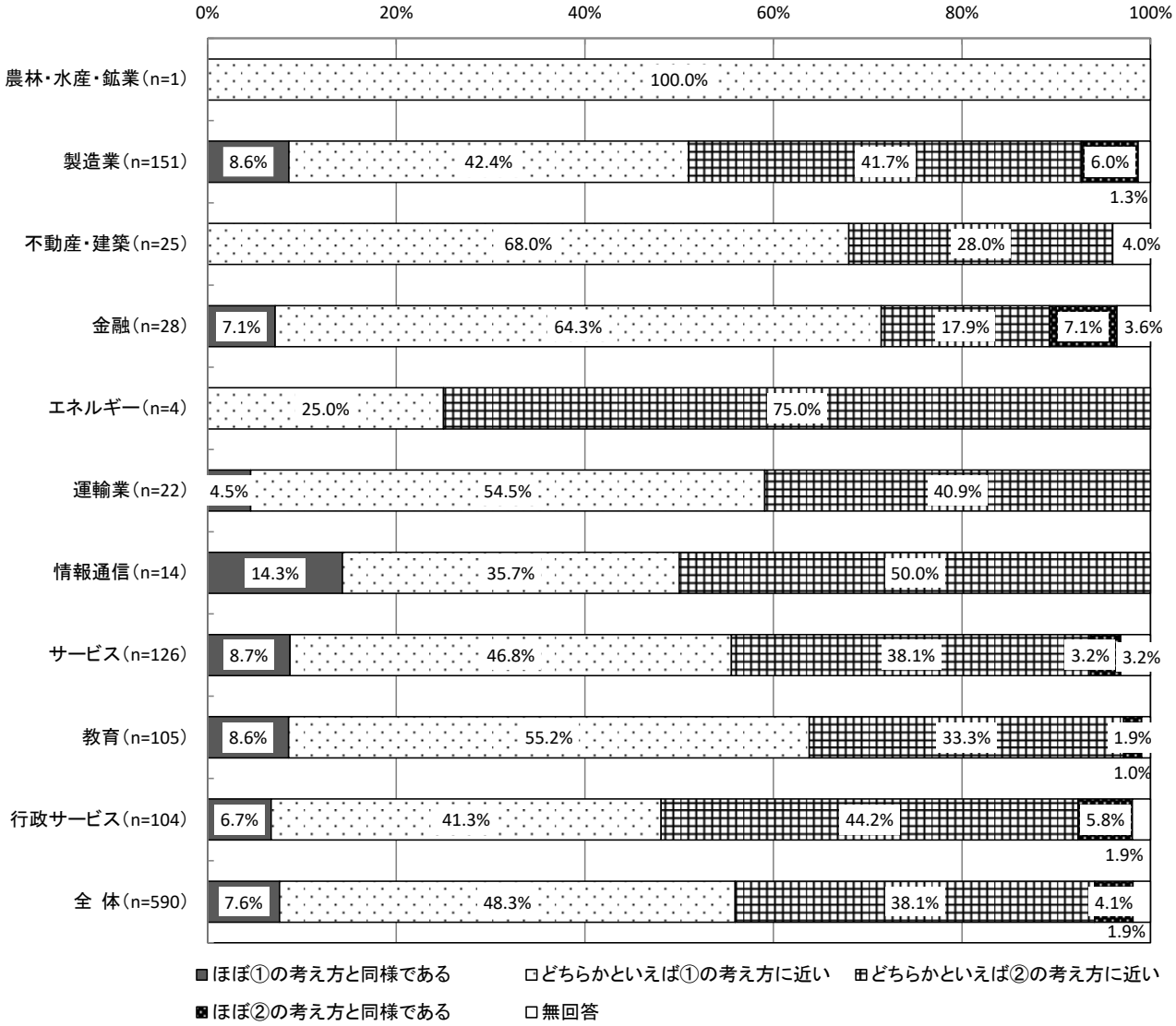
3.1.38　利便性とのバランスに関する考え方　【問15-6】

情報セキュリティ対策と利便性との兼ね合いについては、下記に挙げる2つの考え方のいずれに近いかを尋ねている。

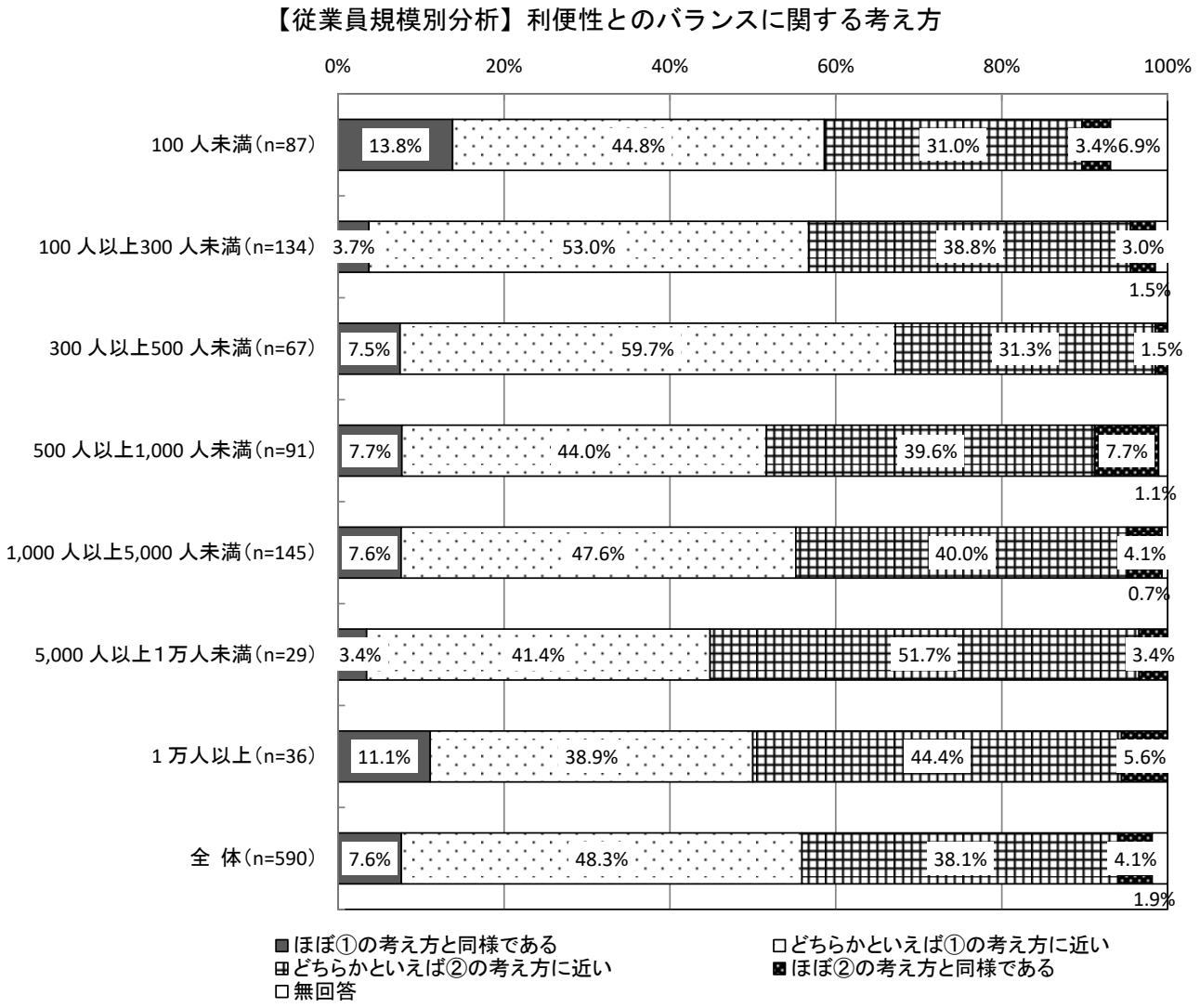
①として提示した考え方	②として提示した考え方
業務実務に負担をかけるほどのセキュリティ対策は不適当であり、利便性とのバランスを考慮すべきである。	ユーザーにシステム利用上・業務上の負担を強いてでもセキュリティを守るべきである。

【業種別分析】業種別にみると、「行政サービス」と「情報通信」を除く、ほぼすべての業種で「①利便性とのバランスを考慮」が「②負担を強いてでもセキュリティを守る」を上回っている。特に「金融」で46.4ポイント、「不動産・建築」で40.0ポイント「①利便性とのバランスを考慮」が多くなっている。

【業種別分析】利便性とのバランスに関する考え方

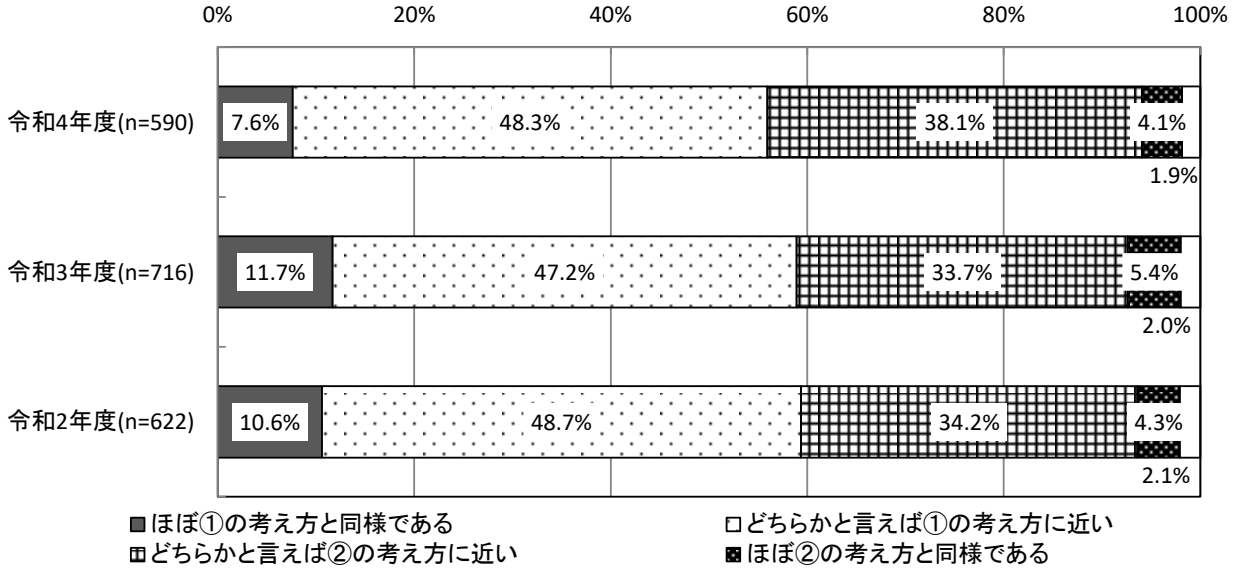


【従業員規模別分析】従業員規模別にみると、5,000人未満の従業員規模で「①利便性とのバランスを考慮」が「②負担を強いてでもセキュリティを守る」を上回っている。「5,000人以上1万人未満」では「②負担を強いてでもセキュリティを守る」がやや高く、「1万人以上」では「①利便性とのバランスを考慮」と「②負担を強いてでもセキュリティを守る」が同じ割当となっている。



【経年変化】昨年度と比較すると、「①利便性とのバランスを考慮」は3.0ポイントの減少、「②負担を強いてでもセキュリティを守る」は3.1ポイントの増加となっている。

【経年変化】利便性とのバランスに関する考え方

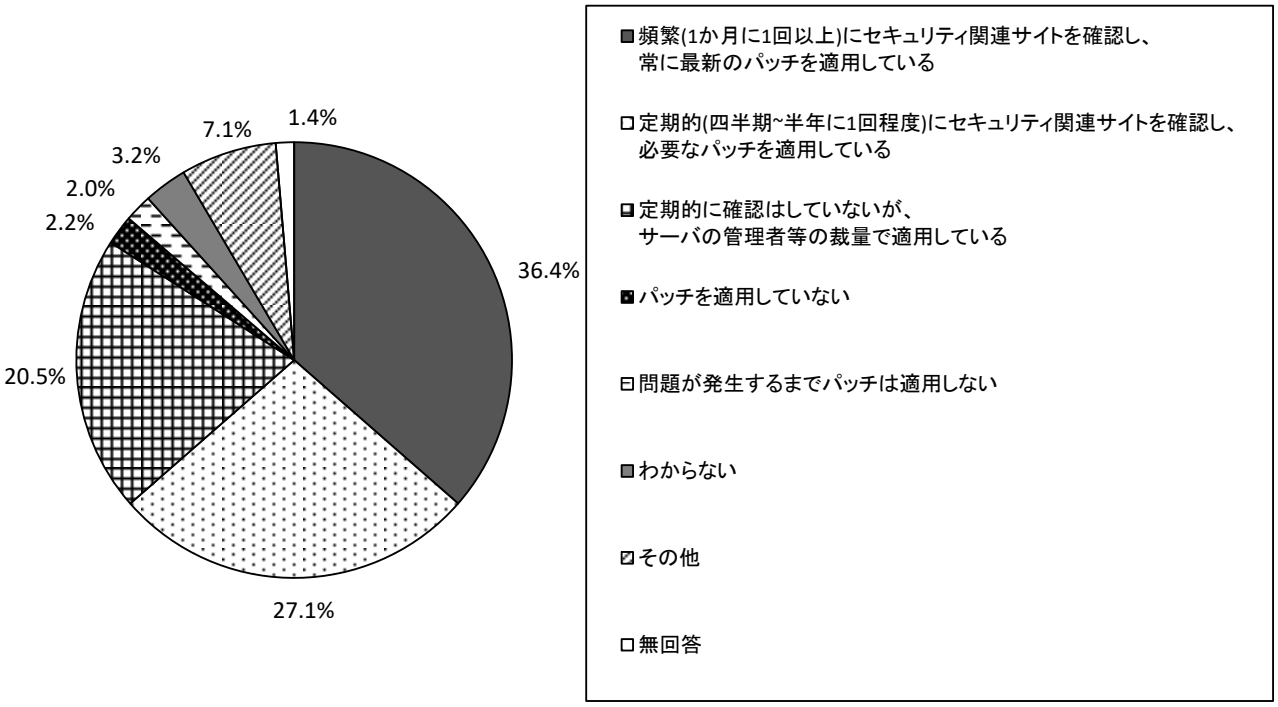


3.2 技術的対策

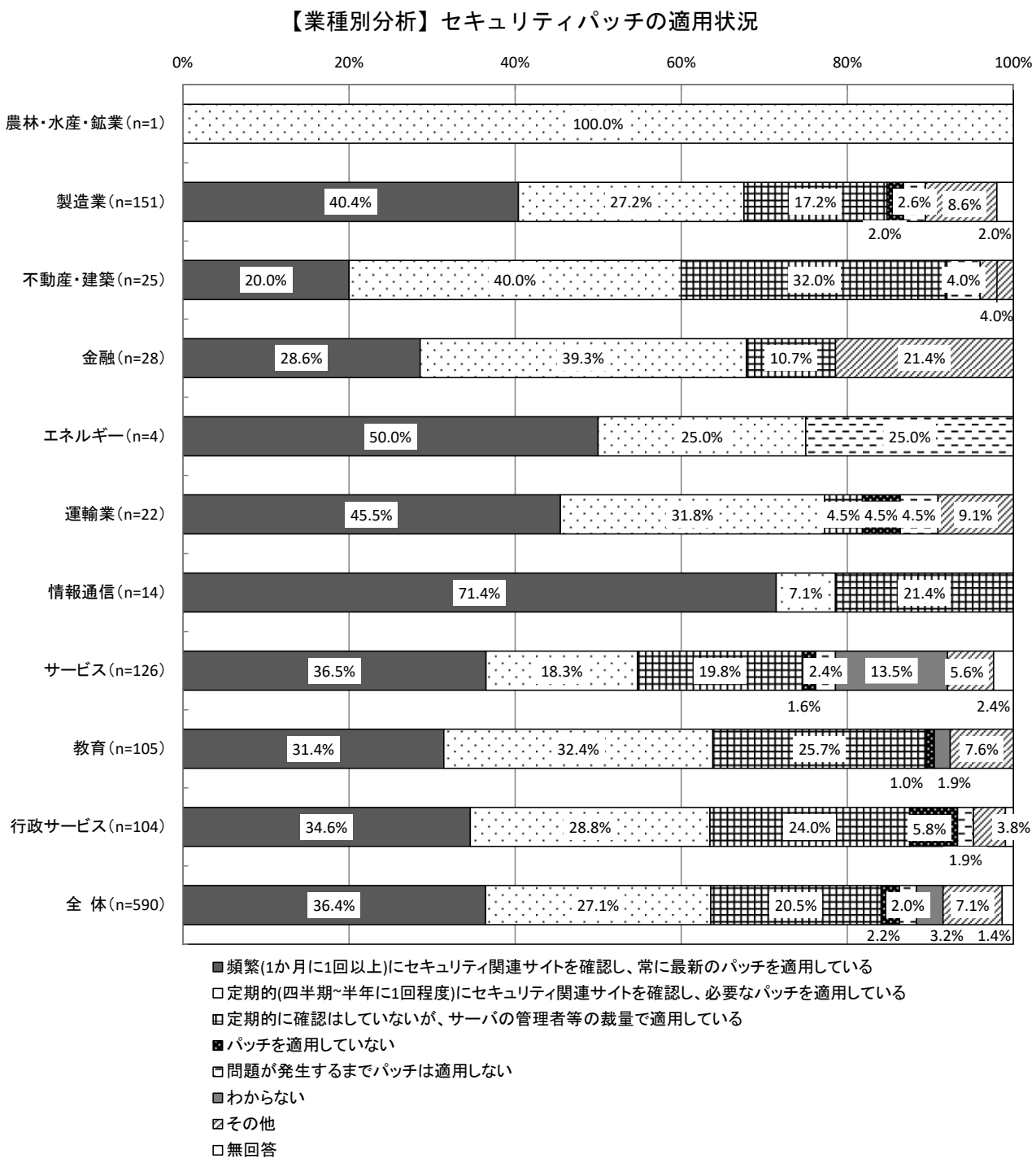
3.2.1 セキュリティパッチの適用状況 【問16】

セキュリティパッチの適用状況については、「頻繁（１か月に１回以上）にセキュリティ関連サイトを確認し、常に最新のパッチを適用している」が36.4%で最も多く、次いで「定期的（四半期～半年に１回程度）にセキュリティ関連サイトを確認し、必要なパッチを適用している」が27.1%、「定期的に確認はしていないが、サーバの管理者等の裁量で適用している」が20.5%となっている。

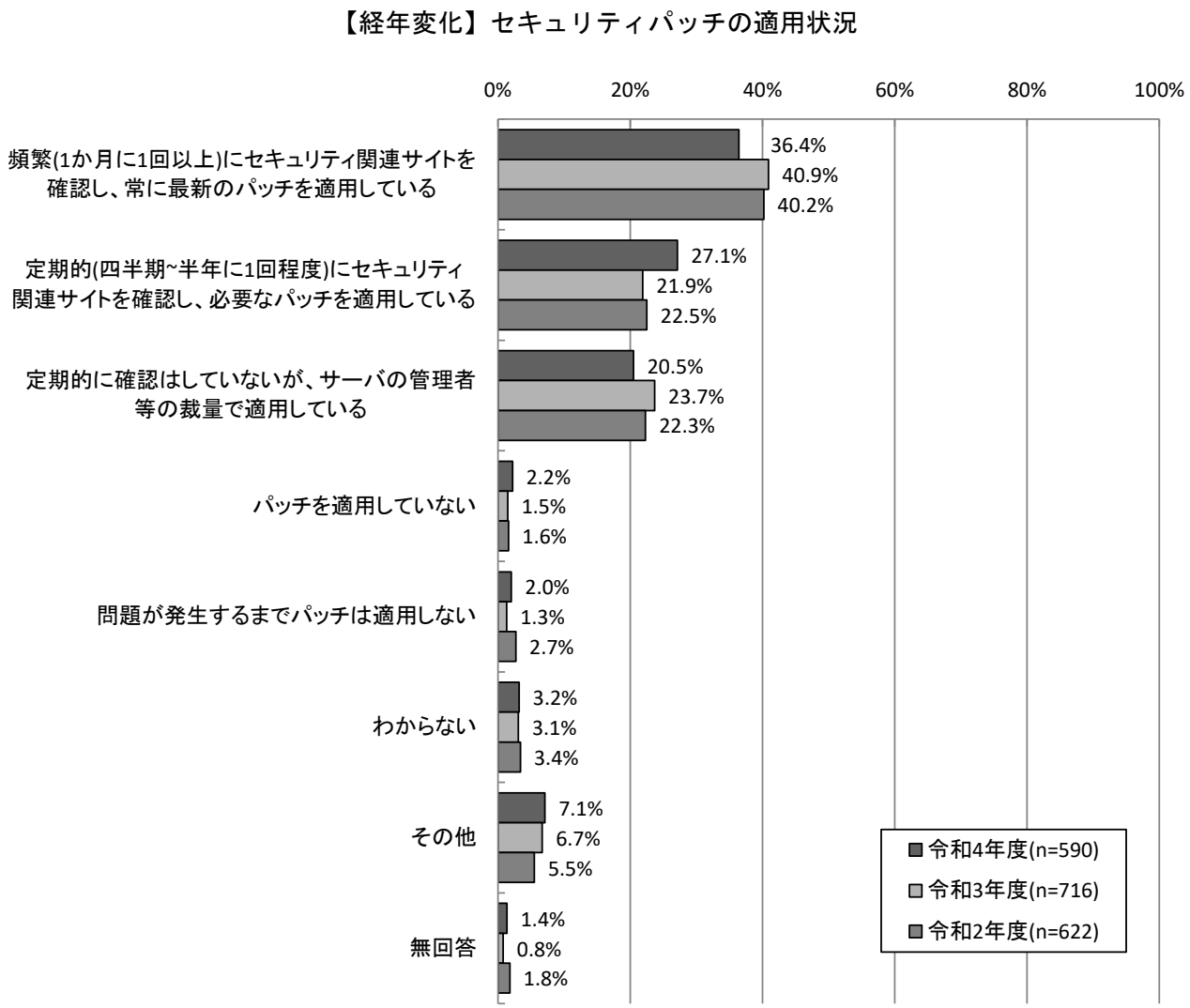
【全体】セキュリティパッチの適用状況（SA,n=590）



【業種別分析】業種別にみると、「頻繁（１か月に１回以上）にセキュリティ関連サイトを確認し、常に最新のパッチを適用している」については、「情報通信」が71.4%と最も高くなっている。

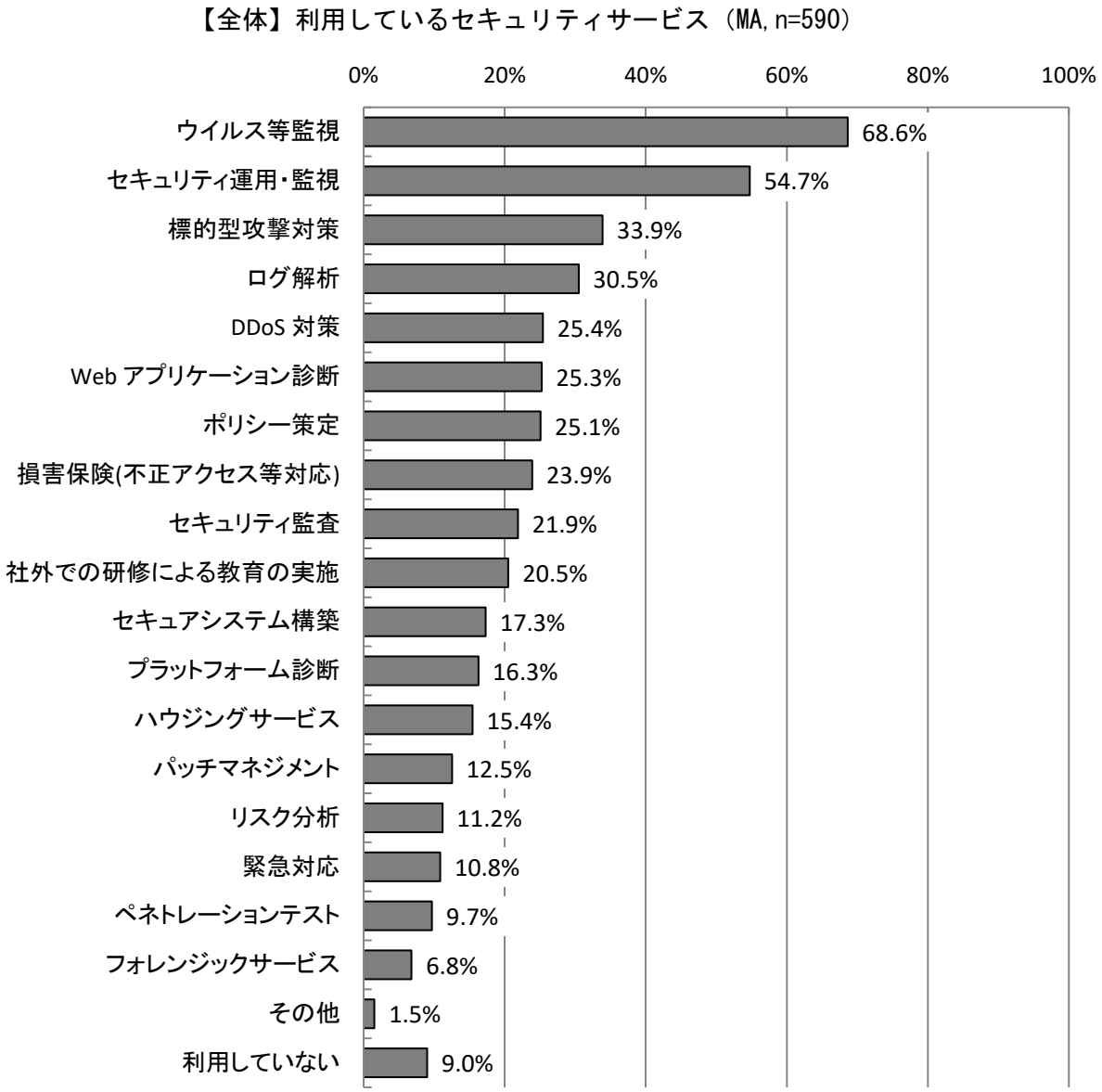


【経年変化】昨年度と比較すると、「定期的にセキュリティ関連サイトを確認し、必要なパッチを適用している」が5.2ポイント増加している。



3.2.1　利用しているセキュリティサービス　【問17】

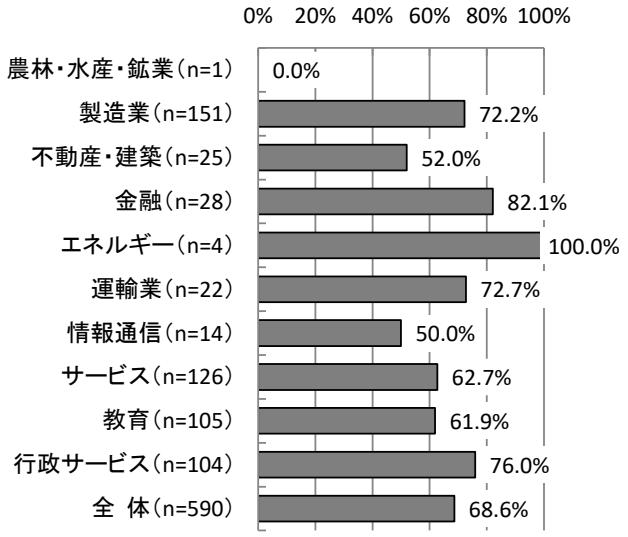
利用しているセキュリティサービスについては、「ウイルス等監視」が68.6%で最も多く、次いで「セキュリティ運用・監視」が54.7%となっている。一方「利用していない」は9.0%となっている。



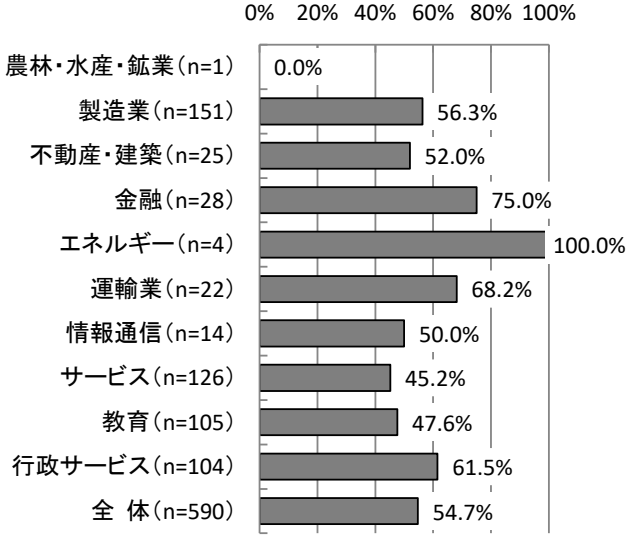
【業種別分析】業種別にみると、「ウイルス等監視」については、「金融」が82.1%、「行政サービス」が76.0%で高い。「セキュリティ運用・監視」については、「金融」が75.0%、「運輸業」が68.2%で高くなっている。

【業種別分析】利用しているセキュリティサービス

ウイルス等監視



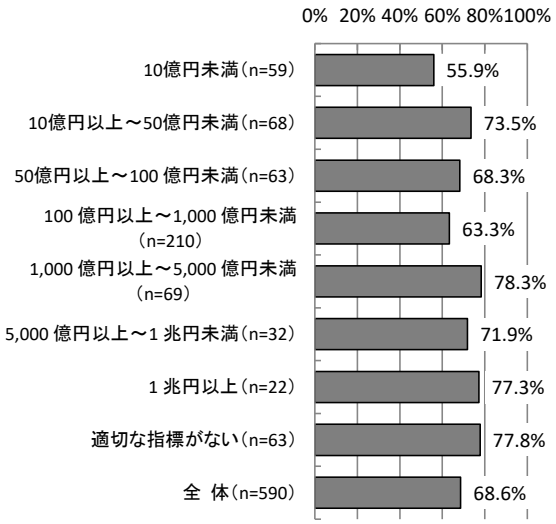
セキュリティ運用・監視



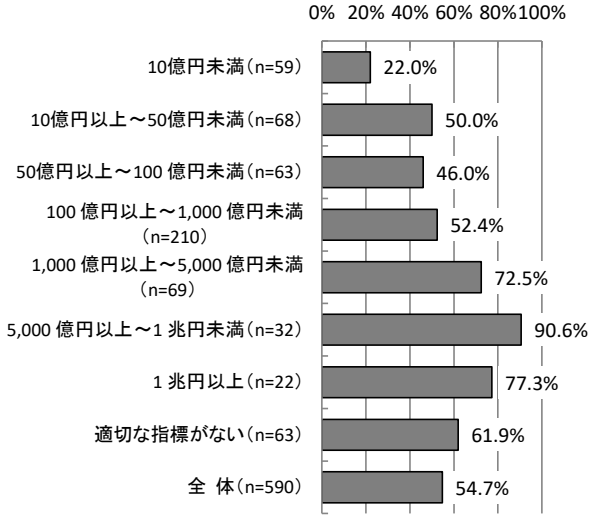
【予算規模別分析】予算規模別にみると、「ウイルス等監視」については、「1,000億円以上～5,000億円未満」が78.3%で最も高くなっている。「セキュリティ運用・監視」については、「5,000億円以上～１兆円未満」が90.6%で最も高くなっている。

【予算規模別分析】利用しているセキュリティサービス

ウイルス等監視



セキュリティ運用・監視

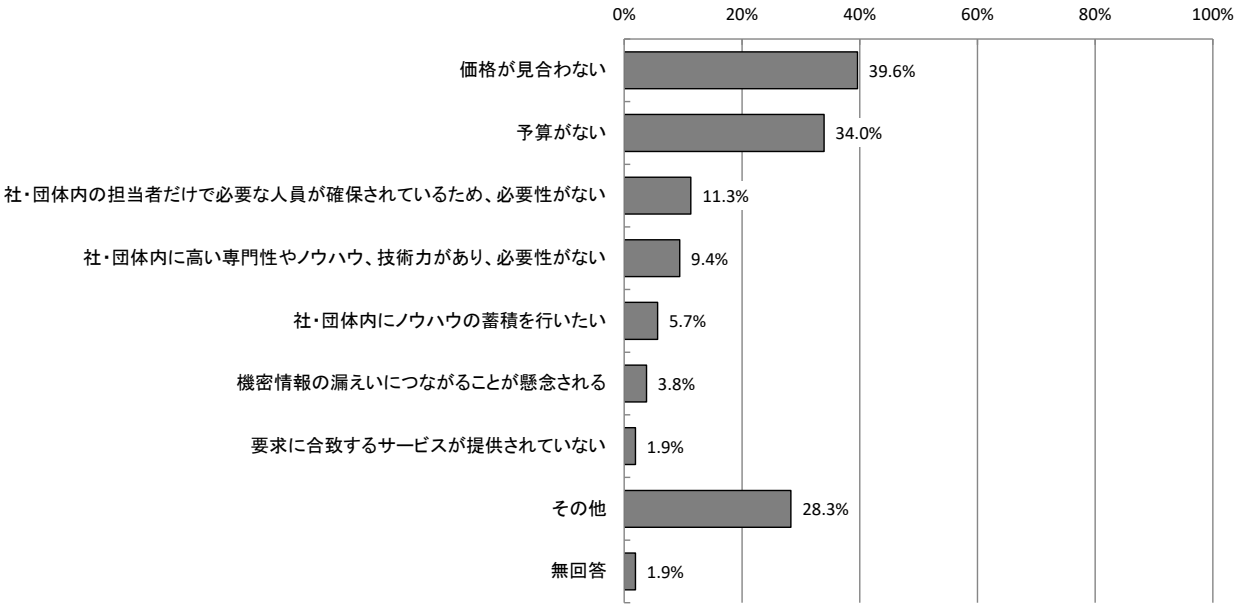


3.2.2　セキュリティサービスを利用していない理由　【問17-1】

セキュリティサービスを利用していない理由については、「価格が見合わない」が39.6%で最も多く、次いで「予算がない」が34.0%と、金銭面の理由が上位に挙げられている。

※本項目は、現在、セキュリティサービスを利用していない社・団体等を対象としている。

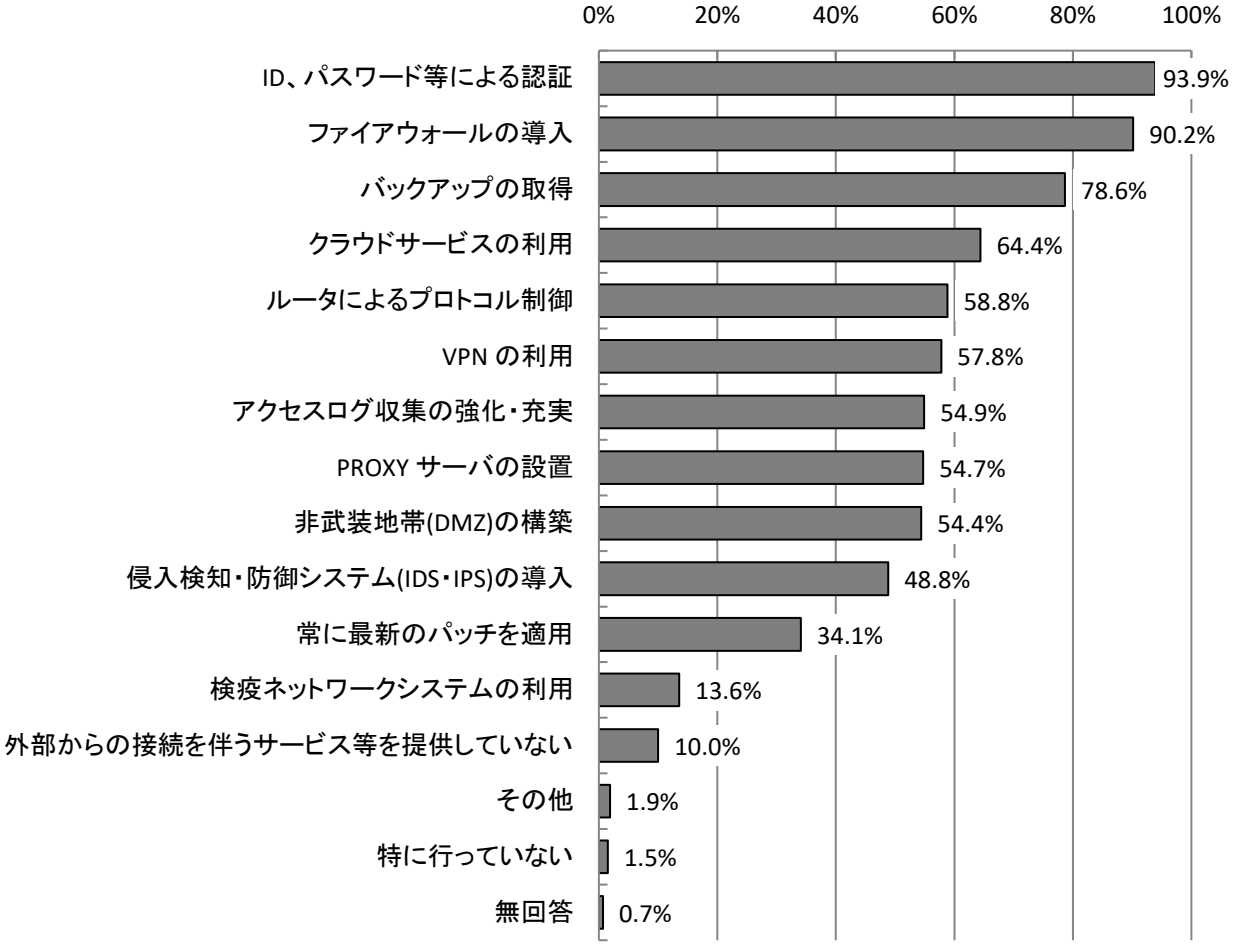
【全体】セキュリティサービスを利用していない理由（MA,n=53）



3.2.3　インターネット接続に対するセキュリティ対策　【問18】

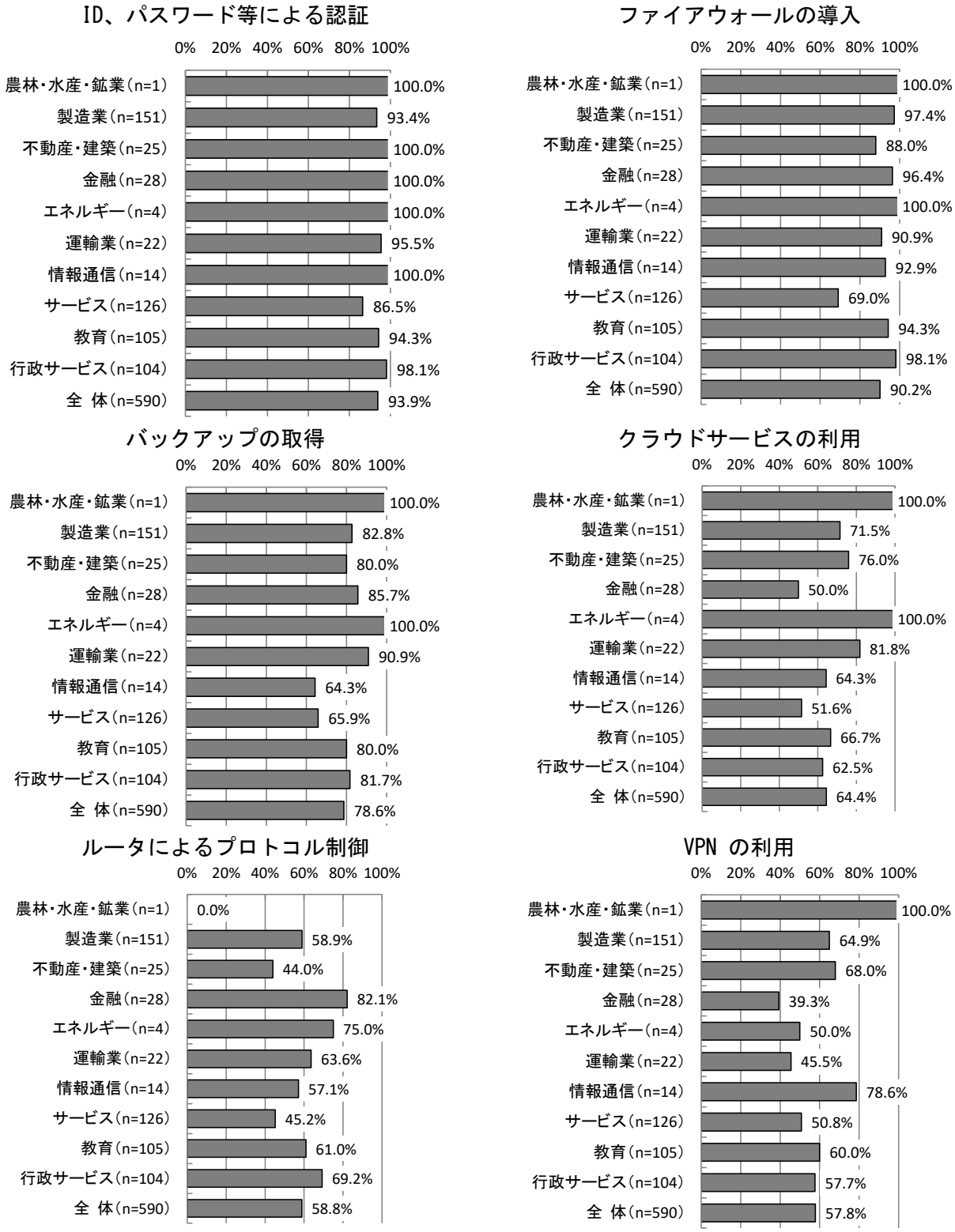
インターネット接続に対するセキュリティ対策については、「ID、パスワード等による認証」が93.9%で最も高く、次いで「ファイアウォールの導入」が90.2%となっている。

【全体】インターネット接続に対するセキュリティ対策（MA,n=590）



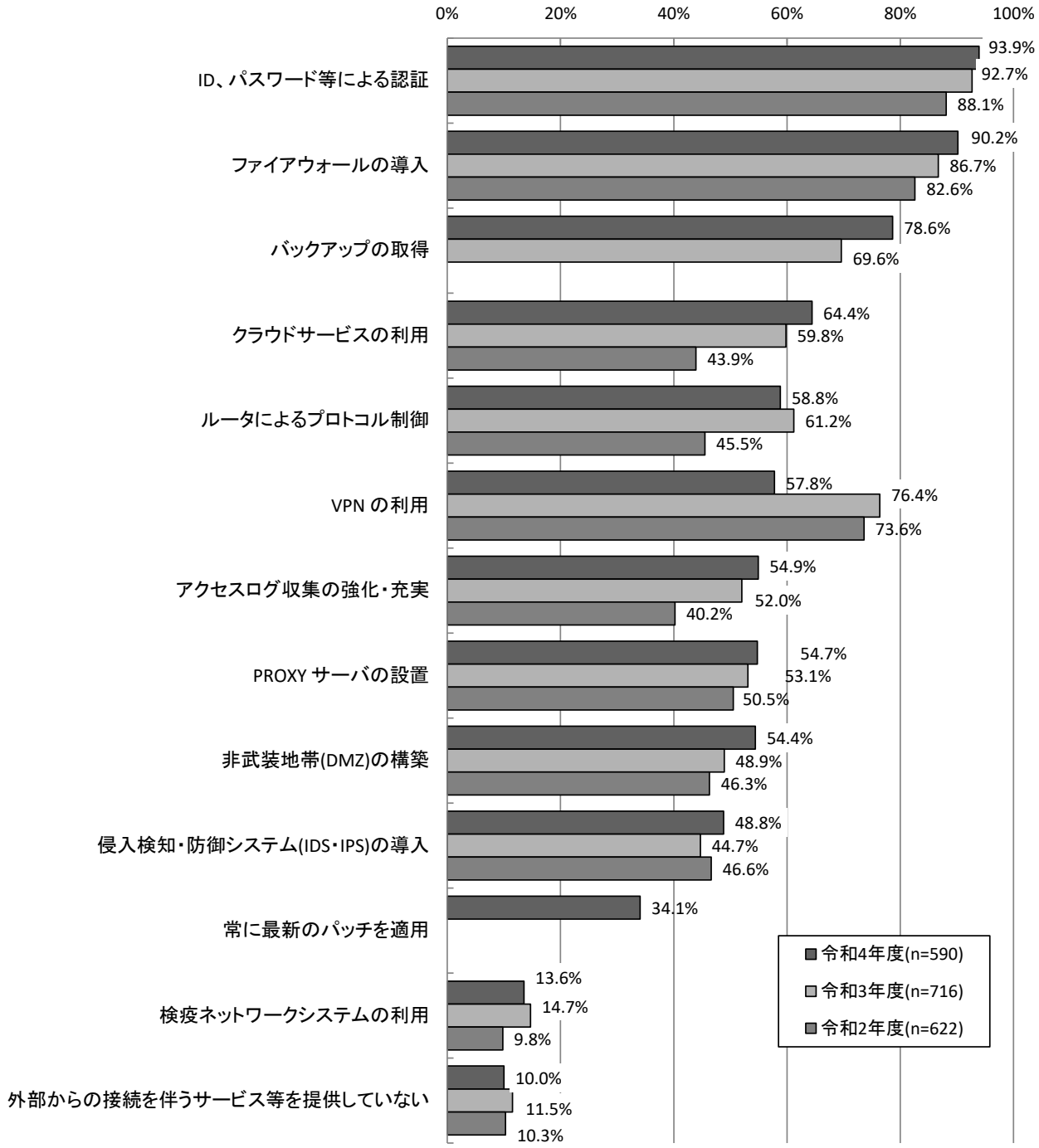
【業種別分析】業種別にみると、「ID、パスワード等による認証」については、「サービス」の86.5%を除き、いずれも90%以上と高くなっている。「ファイアウォールの導入」についても「サービス」が69.0%で低く、「不動産・建築」で88.0%となっているほかはいずれも90%以上と高くなっている。

【業種別分析】インターネット接続に対するセキュリティ対策



【経年変化】昨年度と比較すると、「バックアップの取得」が9.0ポイント、「非武装地帯（DMZ）の構築」が5.5ポイント、「クラウドサービスの利用」が4.6ポイントなど、増加している項目が多い。減少しているのは「ルータによるプロトコル制御」「VPNの利用」「検疫ネットワークの利用」の3項目となっている。

【経年変化】インターネット接続に対するセキュリティ対策



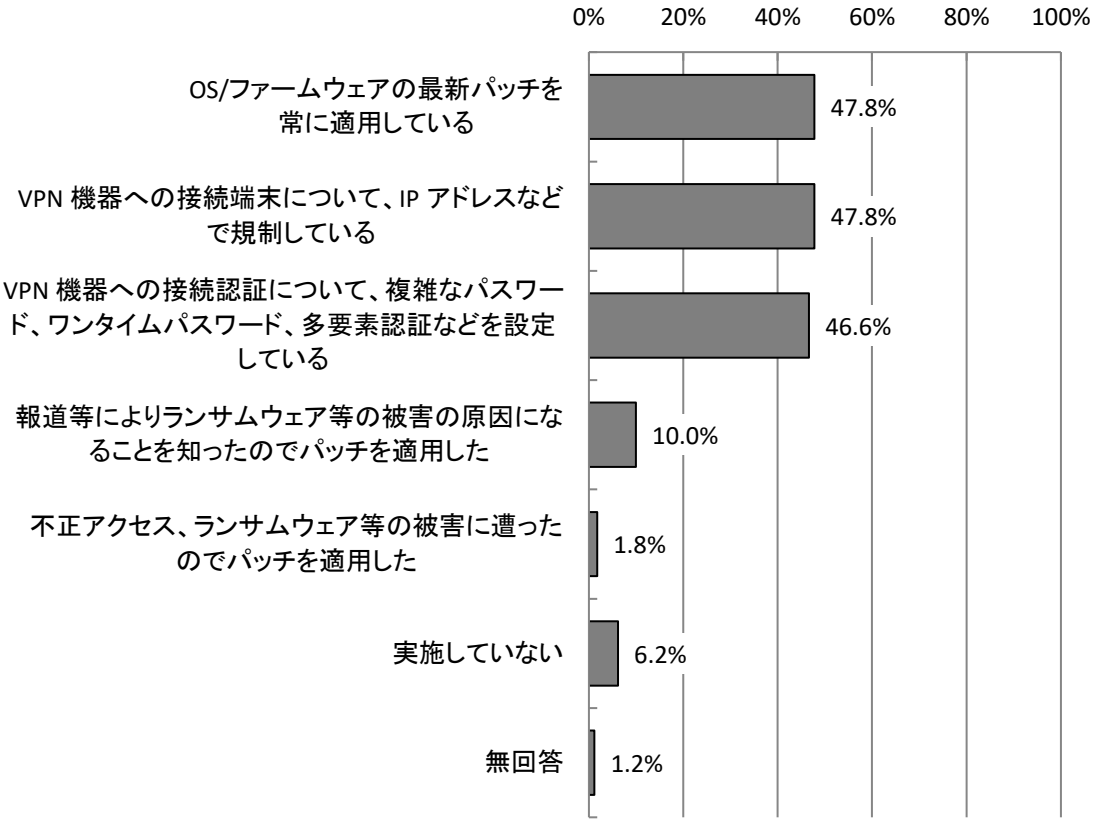
※令和３年度調査で「バックアップの取得」を新設
※令和４年度調査で「常に最新のパッチを適用」を新設

3.2.4　VPN機器のセキュリティ対策　【問18-1】

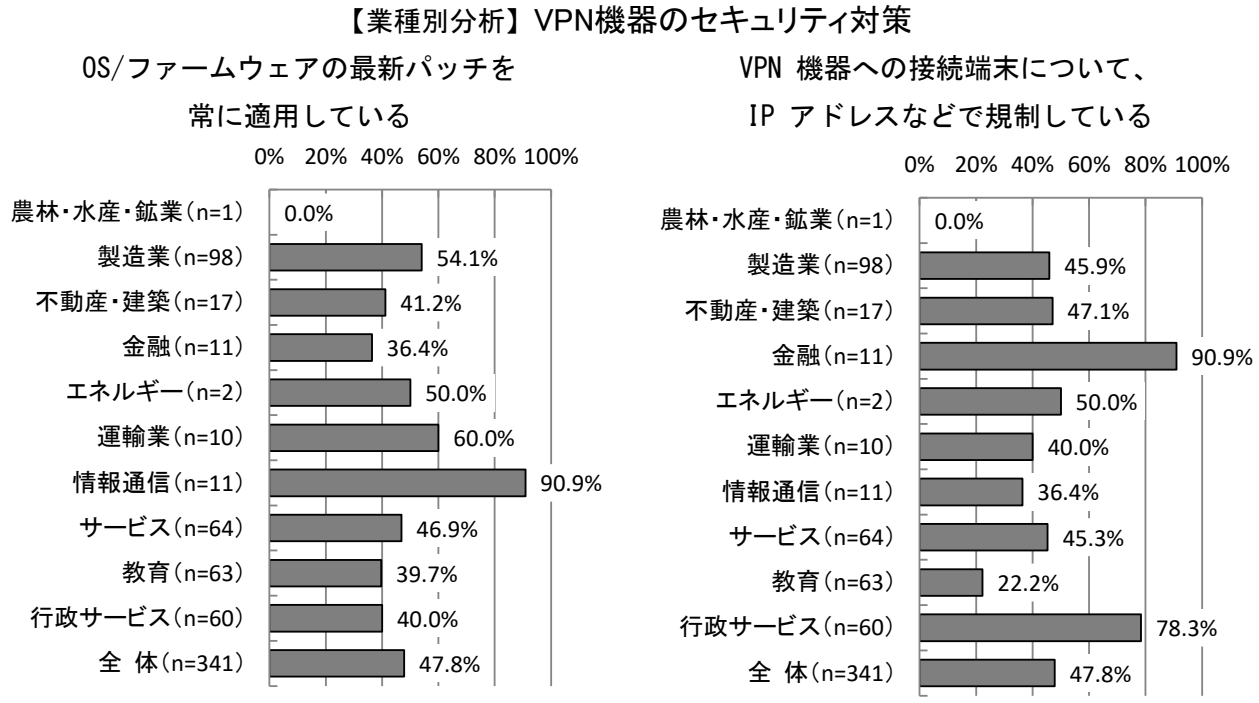
VPN機器のセキュリティ対策は、「OS/ファームウェアの最新パッチを常に適用している」と「VPN機器への接続端末についてIPアドレスなどで規制している」がいずれも47.8%で最も高い。「VPN機器への接続認証について、複雑なパスワード、ワンタイムパスワード、多要素認証などを設定している」も46.6%と高くなっている。「実施していない」は6.2%と1割未満となっている。

※本項目は、ＶＰＮを利用している社・団体等を対象としている。

【全体】VPN機器のセキュリティ対策　（MA,n=341）



【業種別分析】業種別にみると、「OS/ファームウェアの最新パッチを常に適用している」は「情報通信」が90.9%で最も高く、「VPN機器への接続端末についてIPアドレスなどで規制している」は「金融」が90.9%で最も高い。

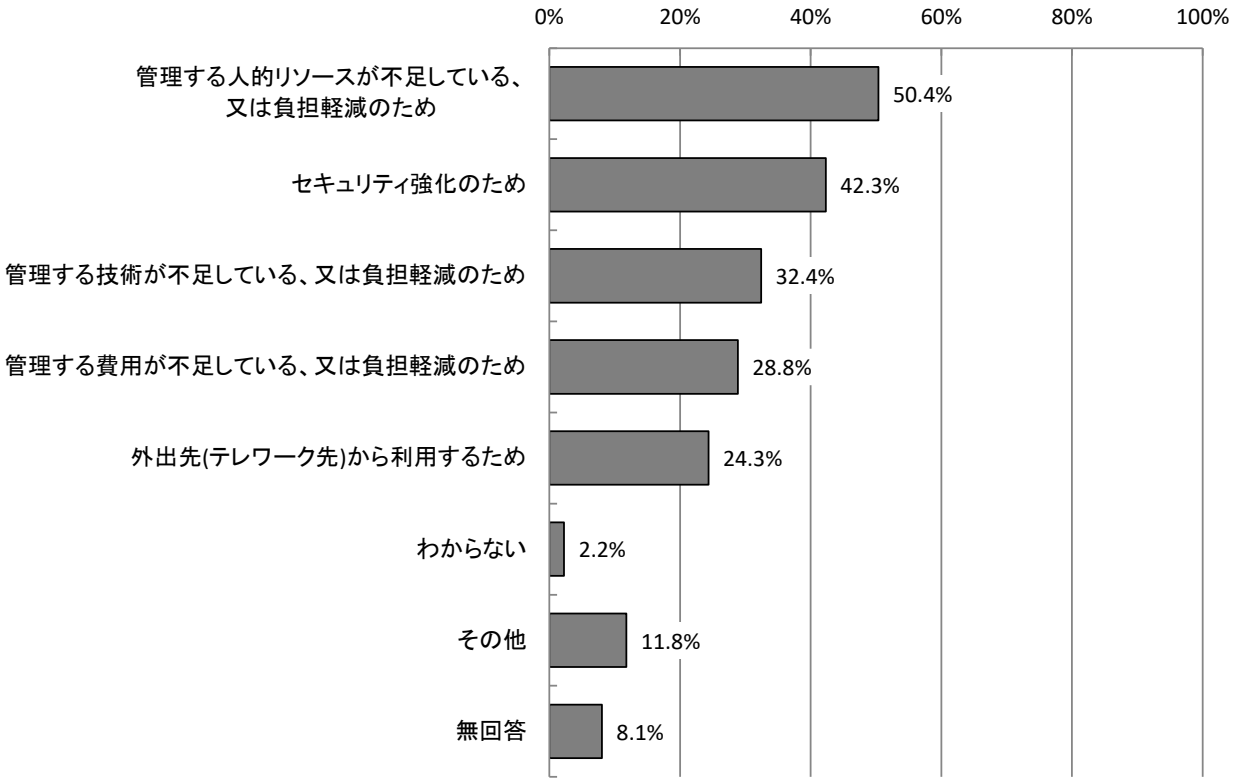


3.2.5　クラウドサービスを使用することになった理由　【問19】

クラウドサービスを使用することになった理由については、「管理する人的リソースが不足している、又は負担軽減のため」が50.4%で最も高く、次いで「セキュリティ強化のため」が42.3%となっている。

※本項目は、クラウドサービスを使用している社・団体等を対象としている。

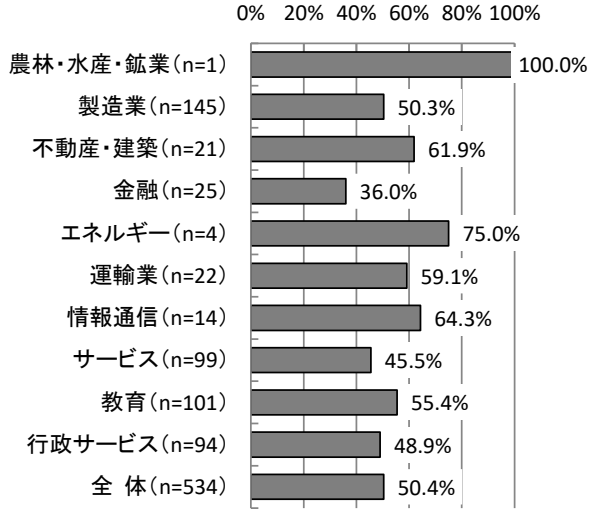
【全体】クラウドサービスを使用することになった理由（MA,n=534）



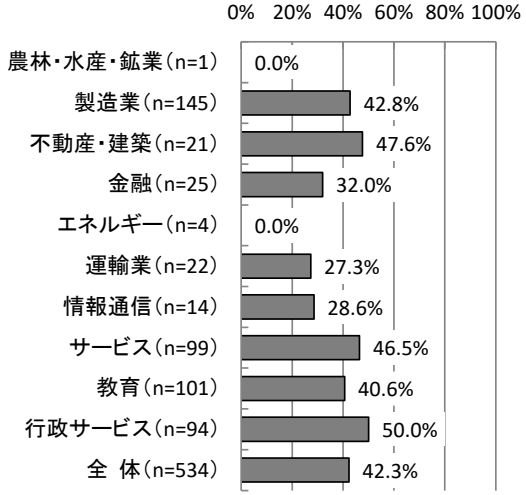
【業種別分析】業種別にみると、「管理する人的リソースが不足している、又は負担軽減のため」については、「情報通信」が64.3%、「不動産・建築」が61.9%で高い。「セキュリティ強化のため」については、「行政サービス」が50.0%で高くなっている。

【業種別分析】クラウドサービスを使用することになった理由

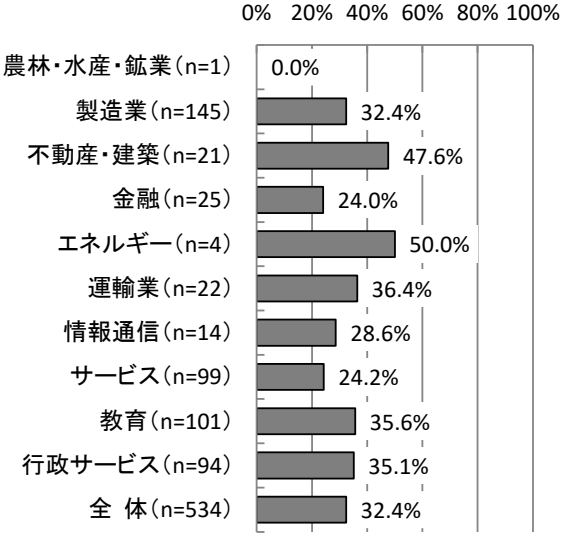
管理する人的リソースが不足している、又は負担軽減のため



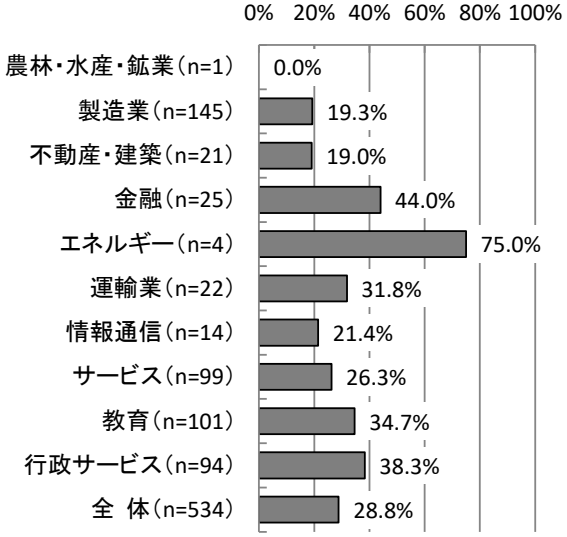
セキュリティ強化のため



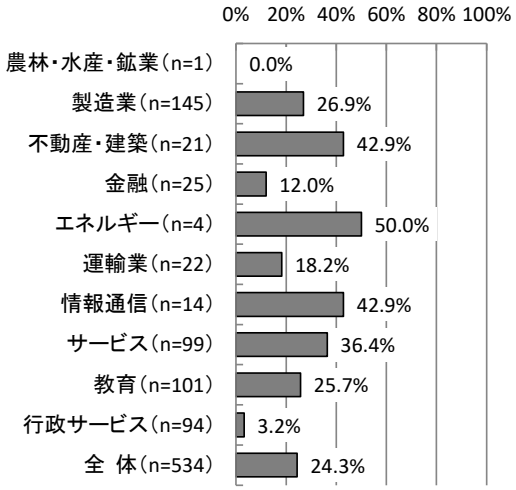
管理する技術が不足している、又は負担軽減のため



管理する費用が不足している、又は負担軽減のため



外出先(テレワーク先)から利用するため

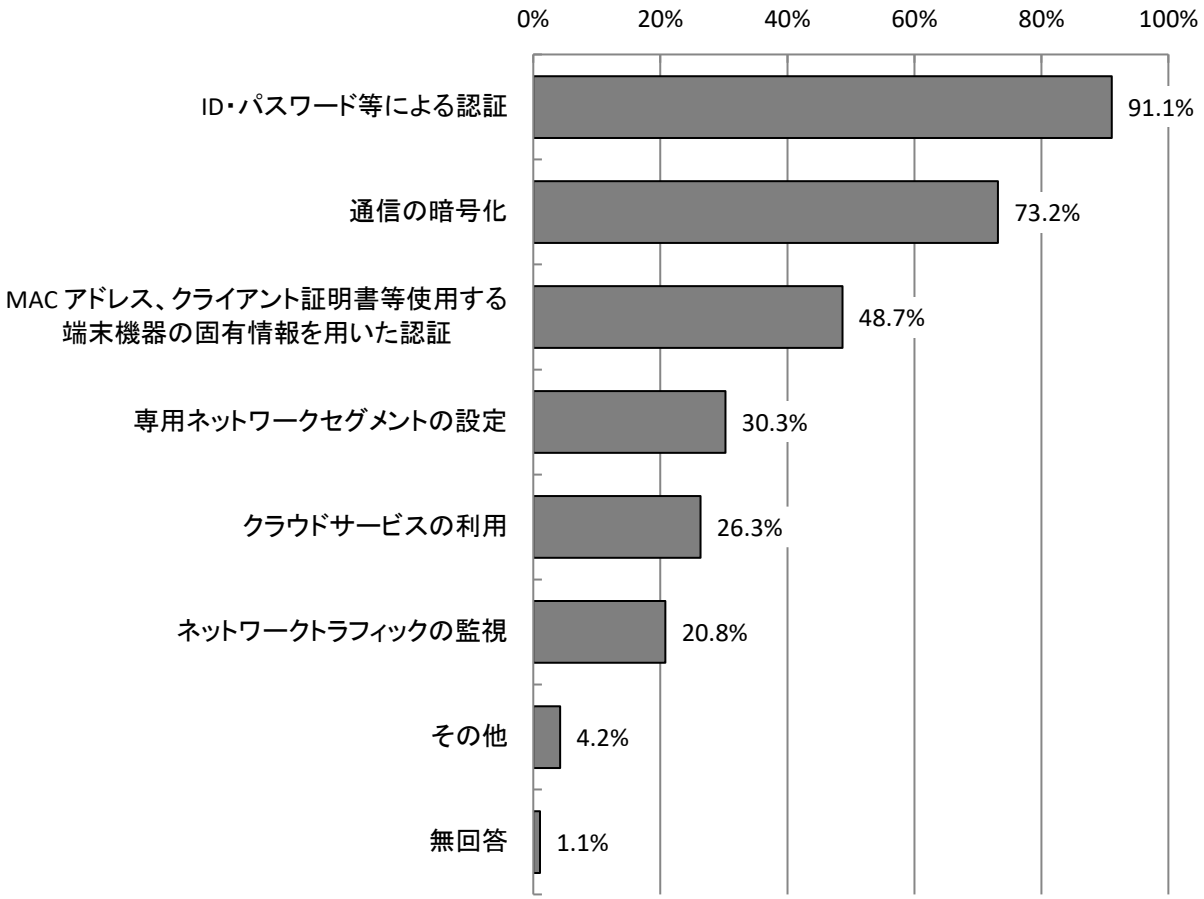


3.2.6　外部からの接続に対するセキュリティ対策　（通信路に対する対策）　【問20-A】

外部からの接続に対するセキュリティ対策（通信路に対する対策）については、「ID・パスワード等による認証」が91.1%で最も高く、次いで「通信の暗号化」が73.2%、「MACアドレス、クライアント証明書等使用する端末機器の固有情報を用いた認証」が48.7%となっている。

※本項目は、外部から内部ネットワークへの接続を許可している社・団体等を対象としている。

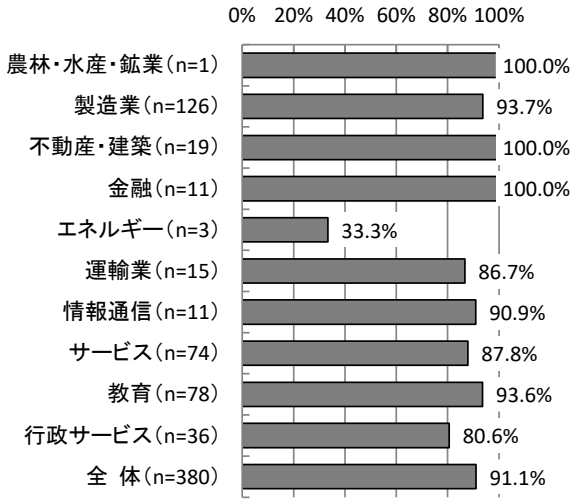
【全体】外部からの接続に対するセキュリティ対策（通信路に対する対策）（MA, n=380）



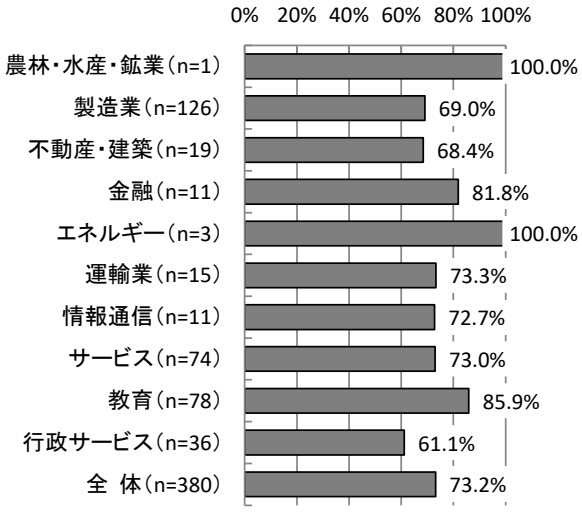
【業種別分析】業種別にみると、「ID・パスワード等による認証」では「金融」「不動産・建築」がそれぞれ100.0%と最も高く、「通信の暗号化」では「教育」が85.9%、「金融」が81.8%で高くなっている。

【業種別分析】外部からの接続に対するセキュリティ対策（通信路に対する対策）

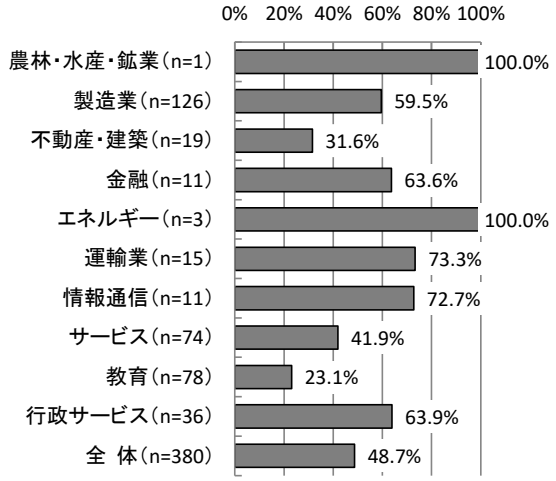
ID・パスワード等による認証



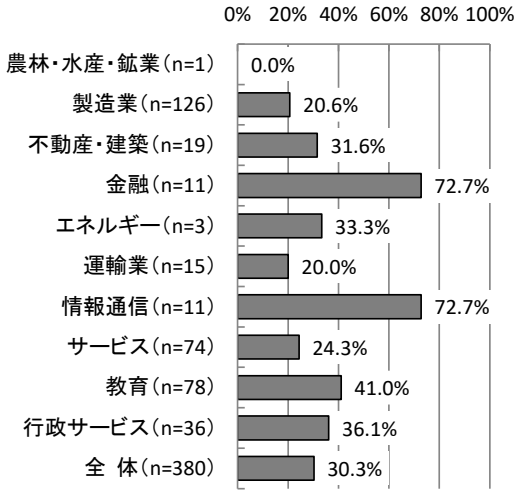
通信の暗号化



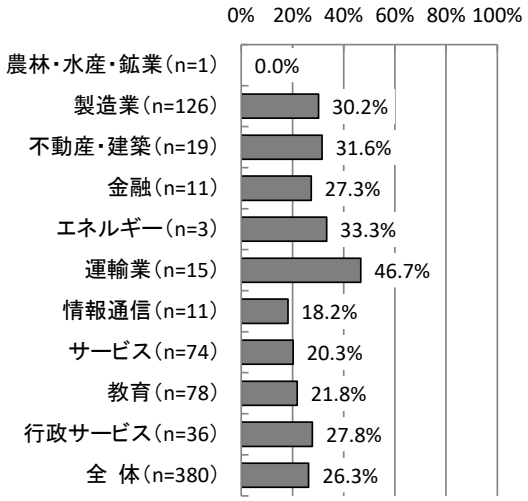
MAC アドレス、クライアント証明書等使用する端末機器の固有情報を用いた認証



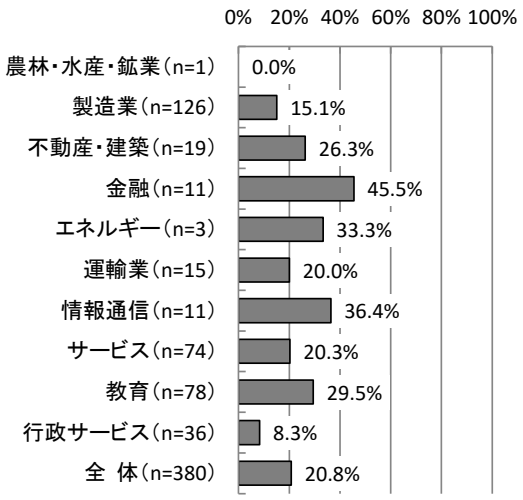
専用ネットワークセグメントの設定



クラウドサービスの利用



ネットワークトラフィックの監視

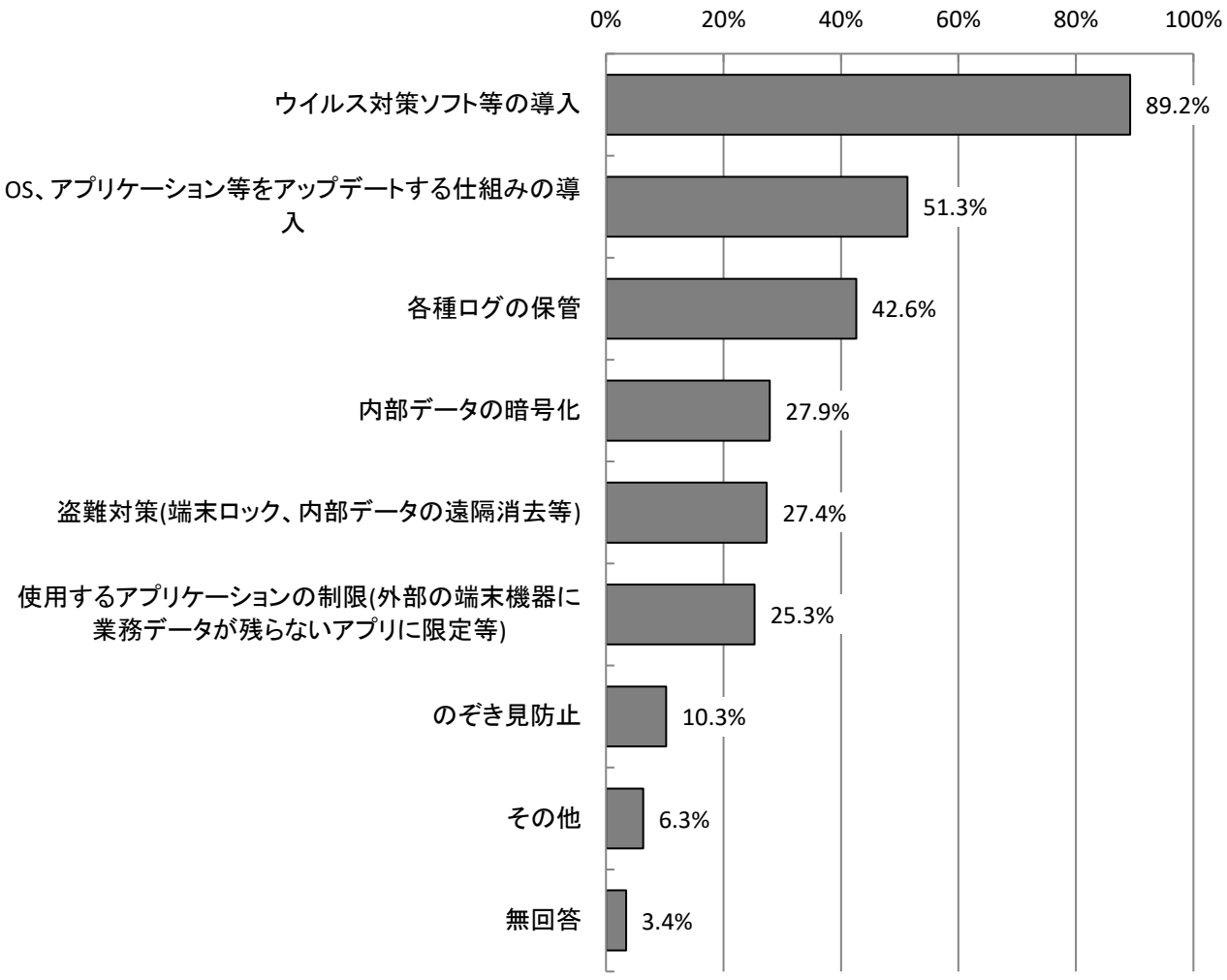


3.2.7　外部からの接続に対するセキュリティ対策　（端末に対する対策）　【問20-B】

外部からの接続に対するセキュリティ対策（端末に対する対策）については、「ウイルス対策ソフト等の導入」が89.2%で最も高く、次いで「OS、アプリケーション等をアップデートする仕組みの導入」が51.3%、となっている。

※本項目は、外部から内部ネットワークへの接続を許可している社・団体等を対象としている。

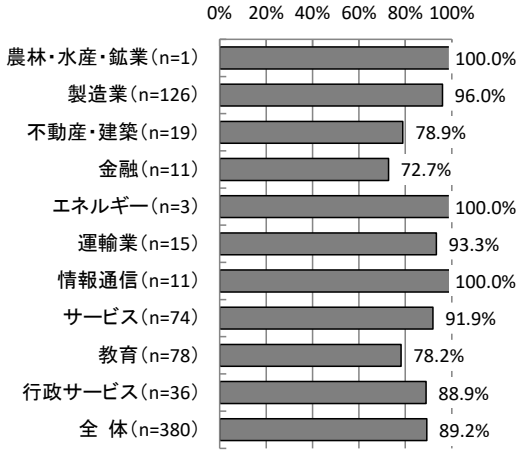
【全体】外部からの接続に対するセキュリティ対策（端末に対する対策）（MA, n=380）



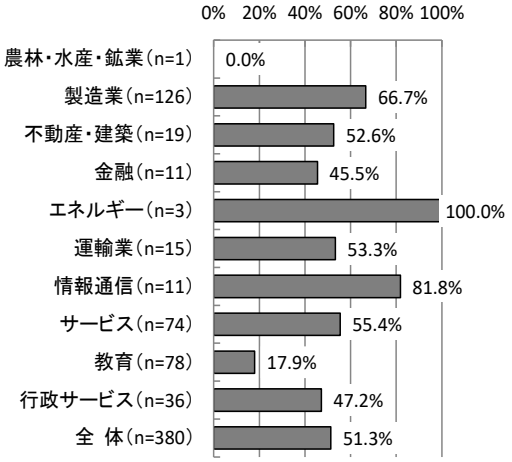
【業種別分析】業種別にみると、「ウイルス対策ソフト等の導入」「OS、アプリケーション等をアップデートする仕組みの導入」「各種ログの保管」では「情報通信」がそれぞれ100.0%、81.8%、72.7%で高くなっている。

【業種別分析】外部からの接続に対するセキュリティ対策（端末に対する対策）

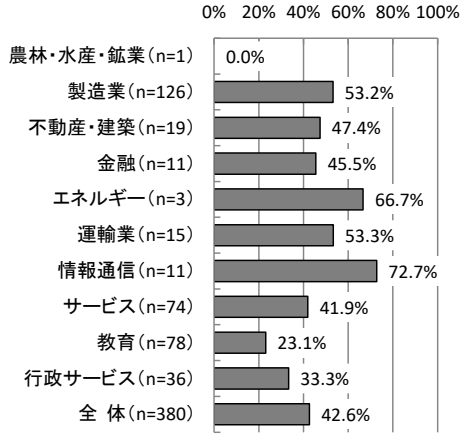
ウイルス対策ソフト等の導入



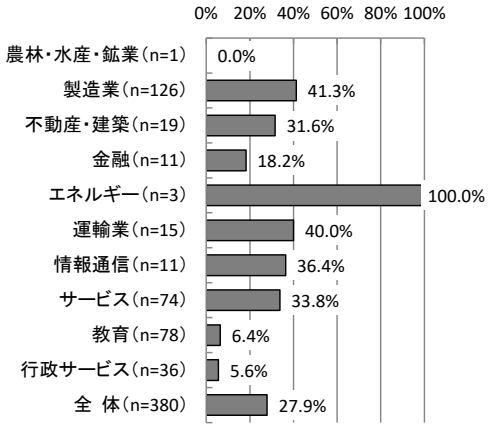
OS、アプリケーション等をアップデートする仕組みの導入



各種ログの保管



内部データの暗号化

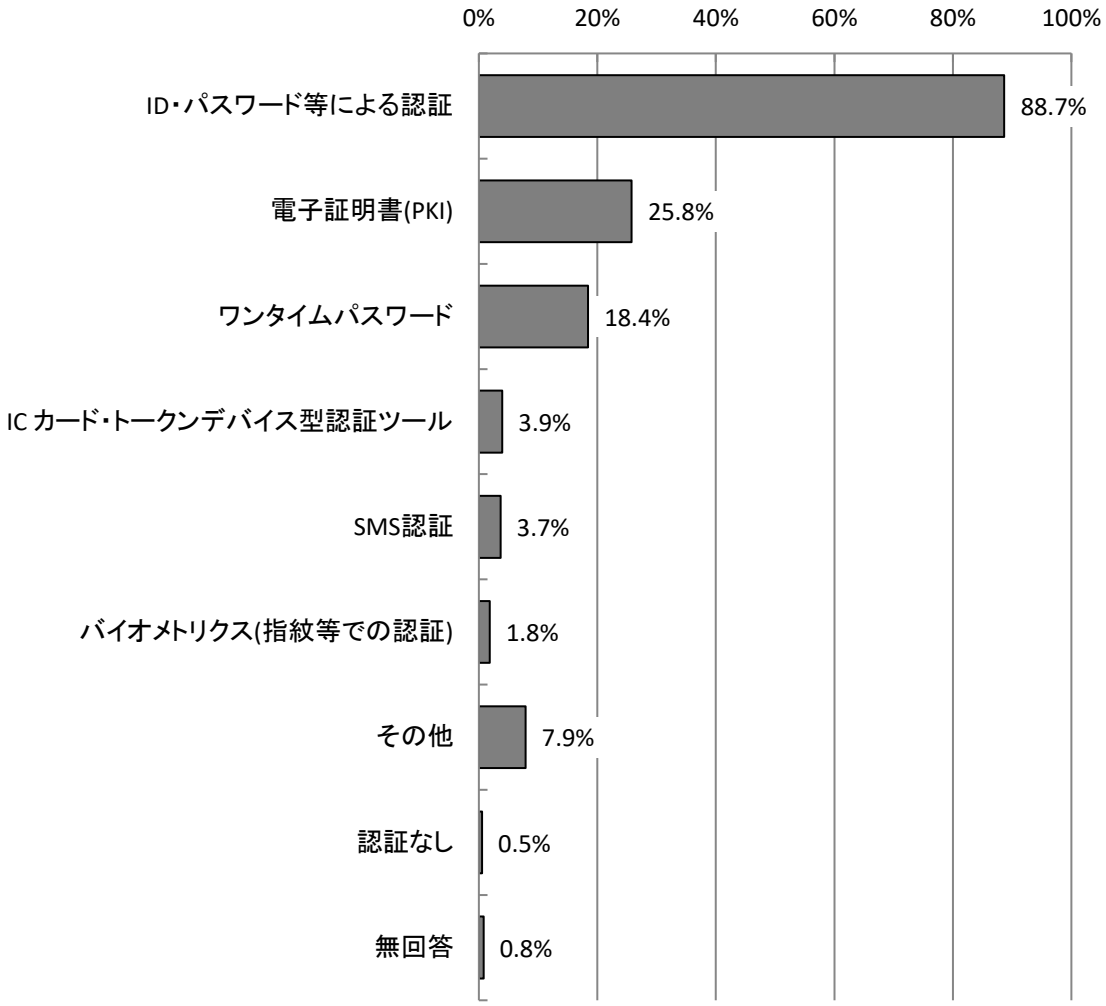


3.2.8　社外等からのインターネット接続経由の認証方法　【問21】

社外等からのインターネット接続経由の認証方法については、「ID・パスワード等による認証」が88.7%で最も高い。次いで「電子証明書（PKI）」が25.8%であるが、「ID・パスワード等による認証」とは50ポイント以上の大きな差がある。一方、「認証なし」は0.5%となっている。

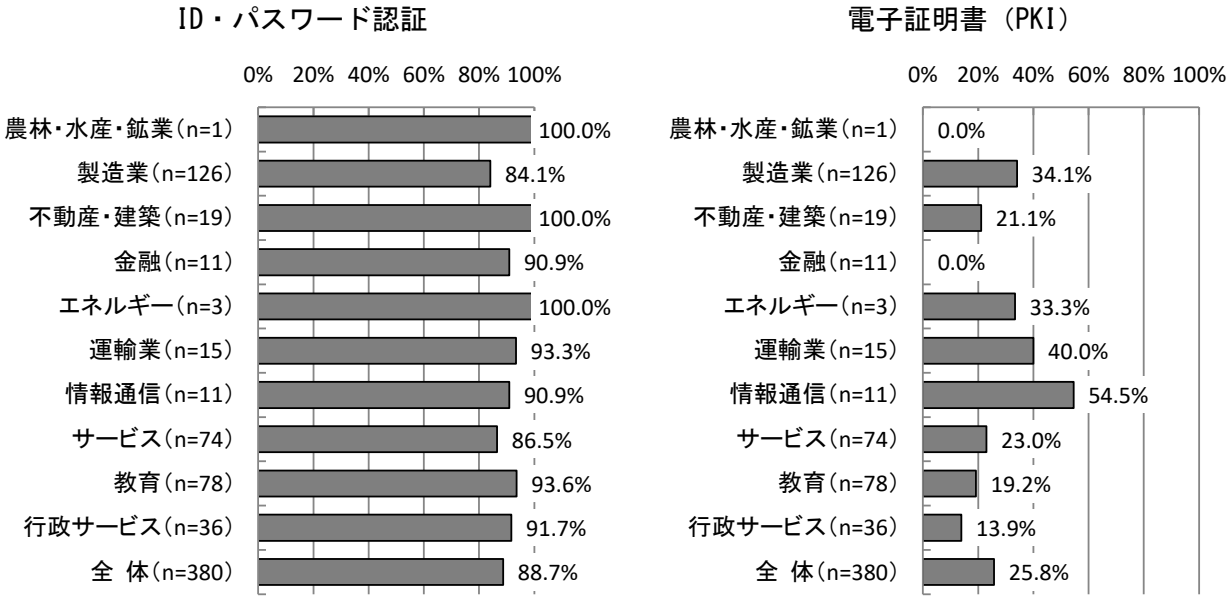
※本項目は、外部から内部ネットワークへの接続を許可している社・団体等を対象としている。

【全体】社外等からのインターネット接続経由の認証方法（MA, n=３８０）



【業種別分析】業種別にみると、「ID・パスワード認証」については、「製造業」が84.1%、「サービス」が86.5%と低くなっている他はいずれも90%以上と高くなっている。

【業種別分析】社外等からのインターネット接続経由の認証方法

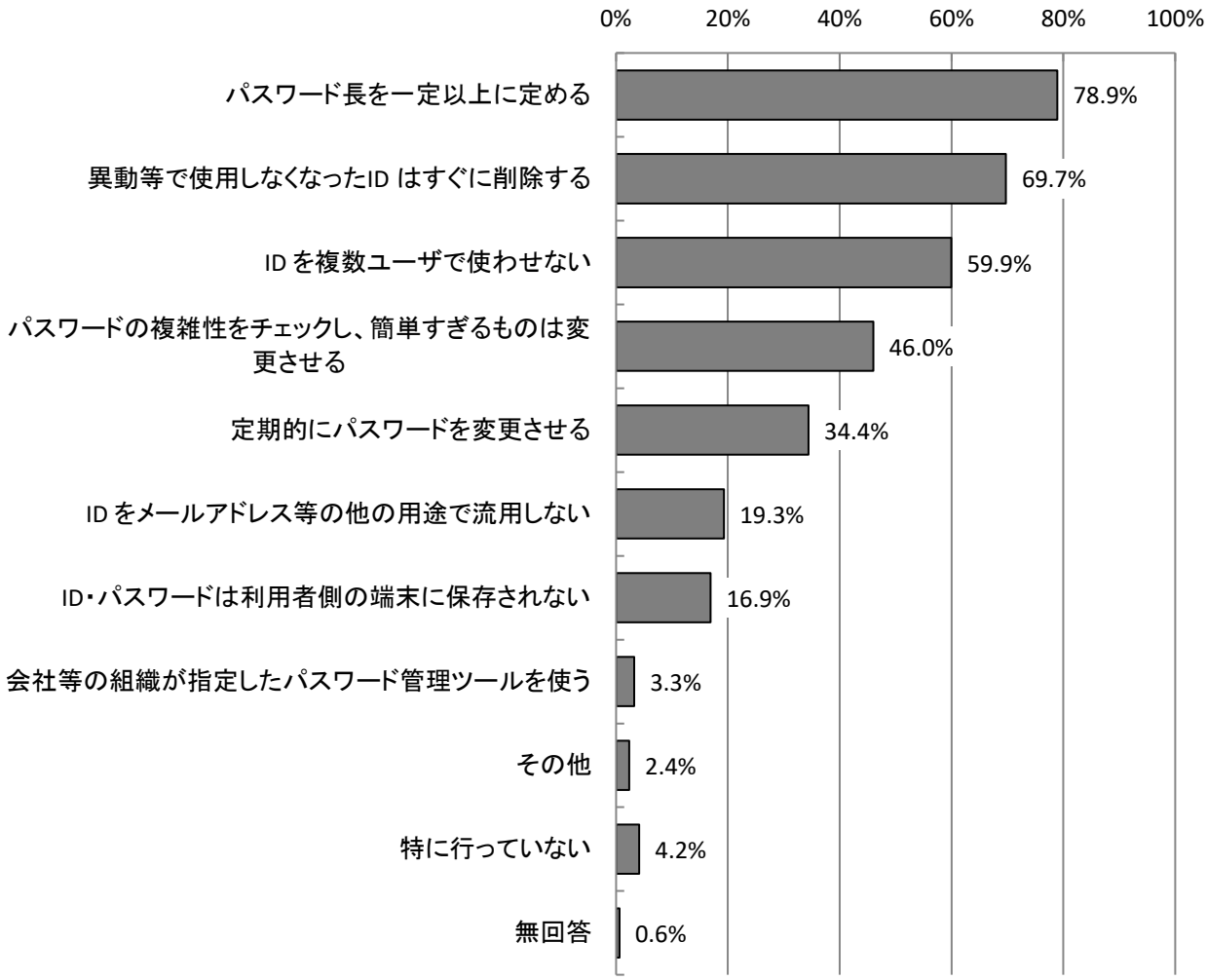


3.2.9　ID・パスワードの管理方法　【問21-1】

ID・パスワードの管理方法については、「パスワード長を一定以上に定める」が78.9%で最も高く、次いで「異動等で使用しなくなったIDはすぐに削除する」が69.7%となっている。

※本項目は、社外等からのインターネット接続を行う際ID・パスワード認証を利用している社・団体等を対象としている。

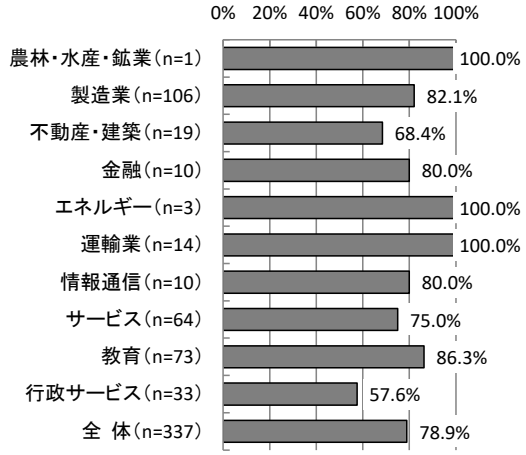
【全体】ID・パスワードの管理方法（MA,n=337）



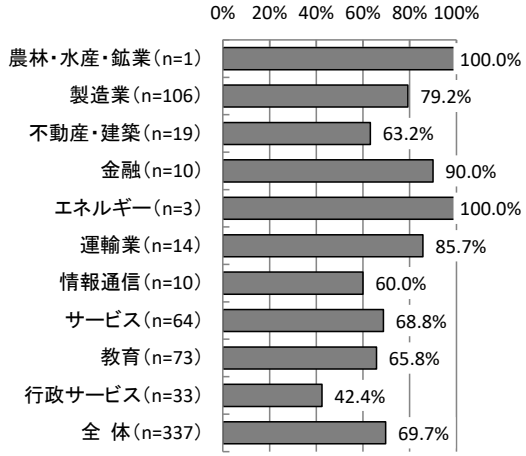
【業種別分析】業種別にみると、「パスワード長を一定以上に定める」については、「運輸業」が100.0%、「教育」が86.3%などで高くなっている。「異動等で使用しなくなったIDはすぐに削除する」については、「金融」が90.0%、「運輸業」が85.7%で高くなっている。

【業種別分析】ID・パスワードの管理方法

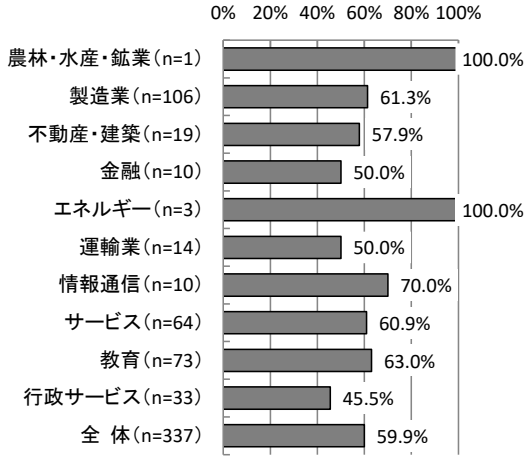
パスワード長を一定以上に定める



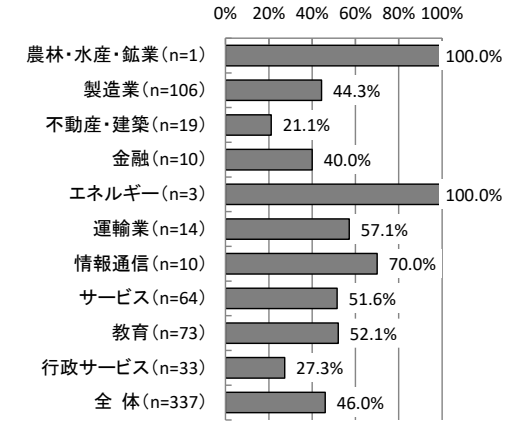
異動等で使用しなくなったIDはすぐに削除する



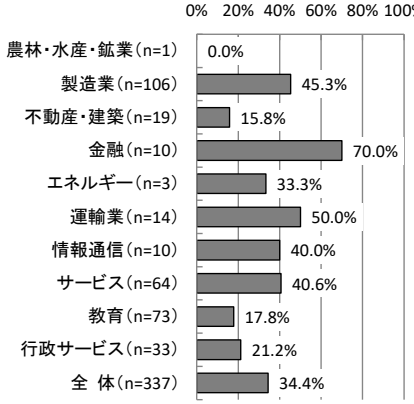
IDを複数ユーザーで使わせない



パスワードの複雑性をチェックし、簡単すぎるものは変更させる



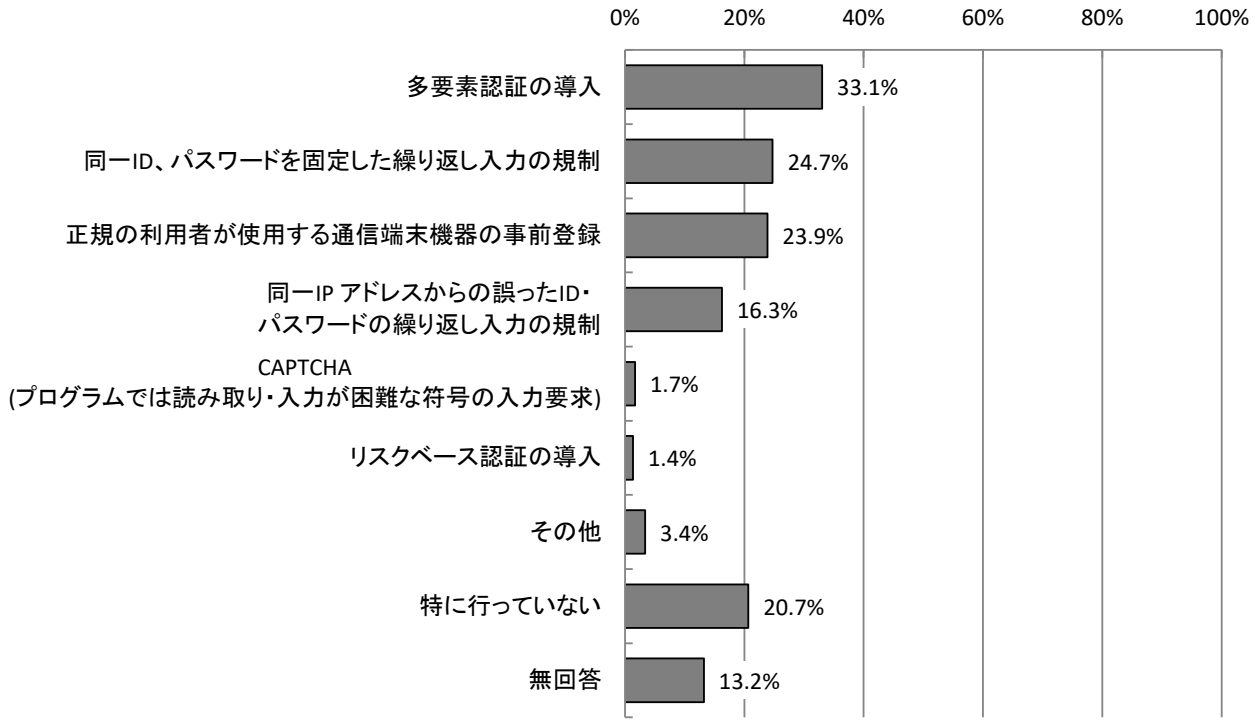
定期的にパスワードを変更させる



3.2.10　不正ログイン対策　【問21-2】

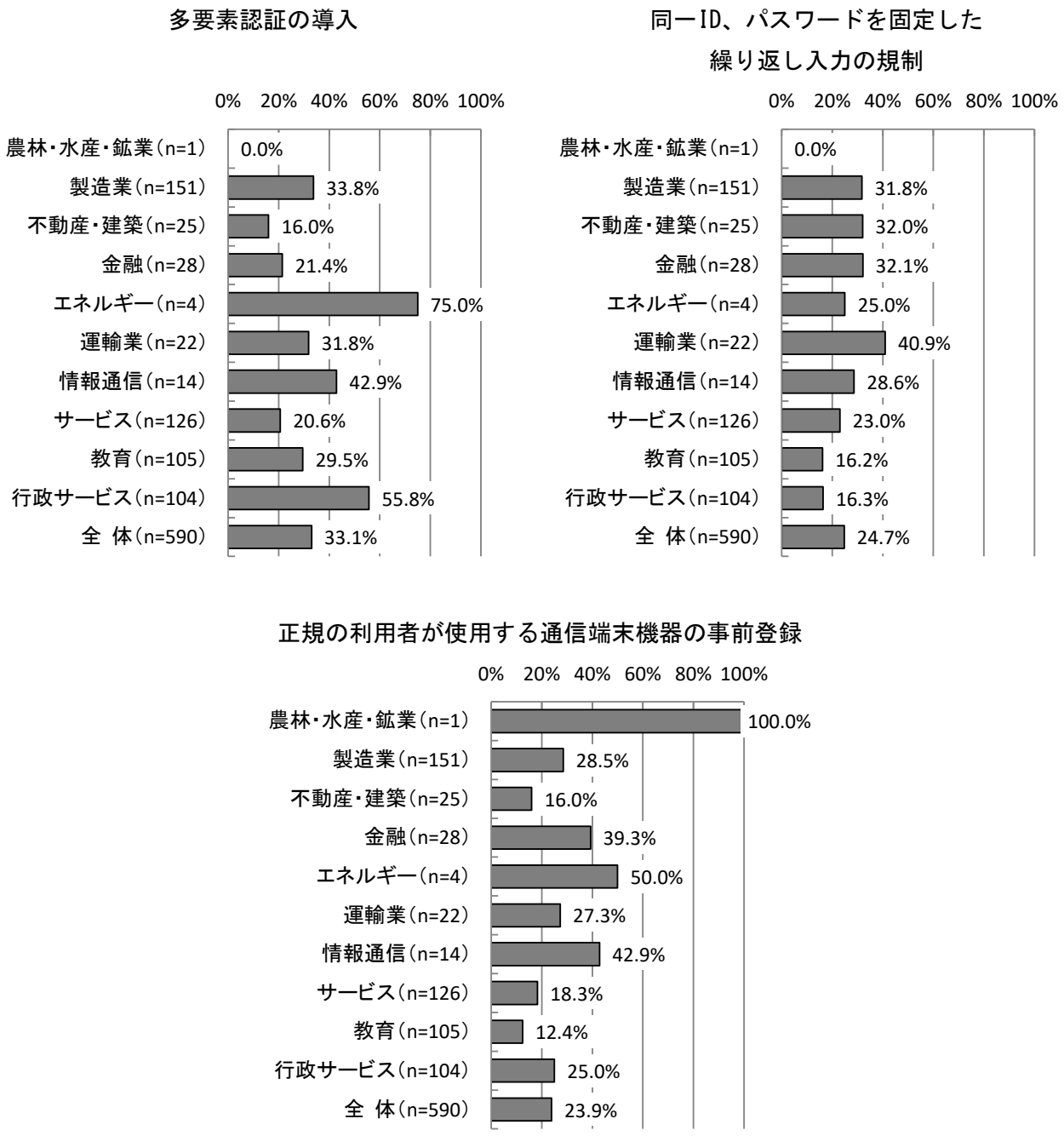
不正ログイン対策については、「多要素認証の導入」が33.1%で最も高くなっている。次いで「同一ID、パスワードを固定した繰り返し入力の規制」が24.7%、「正規の利用者が使用する通信端末機器の事前登録」が23.9%となっている。一方、「特に行っていない」は20.7%となっている。

【全体】不正ログイン対策（MA, n=590）



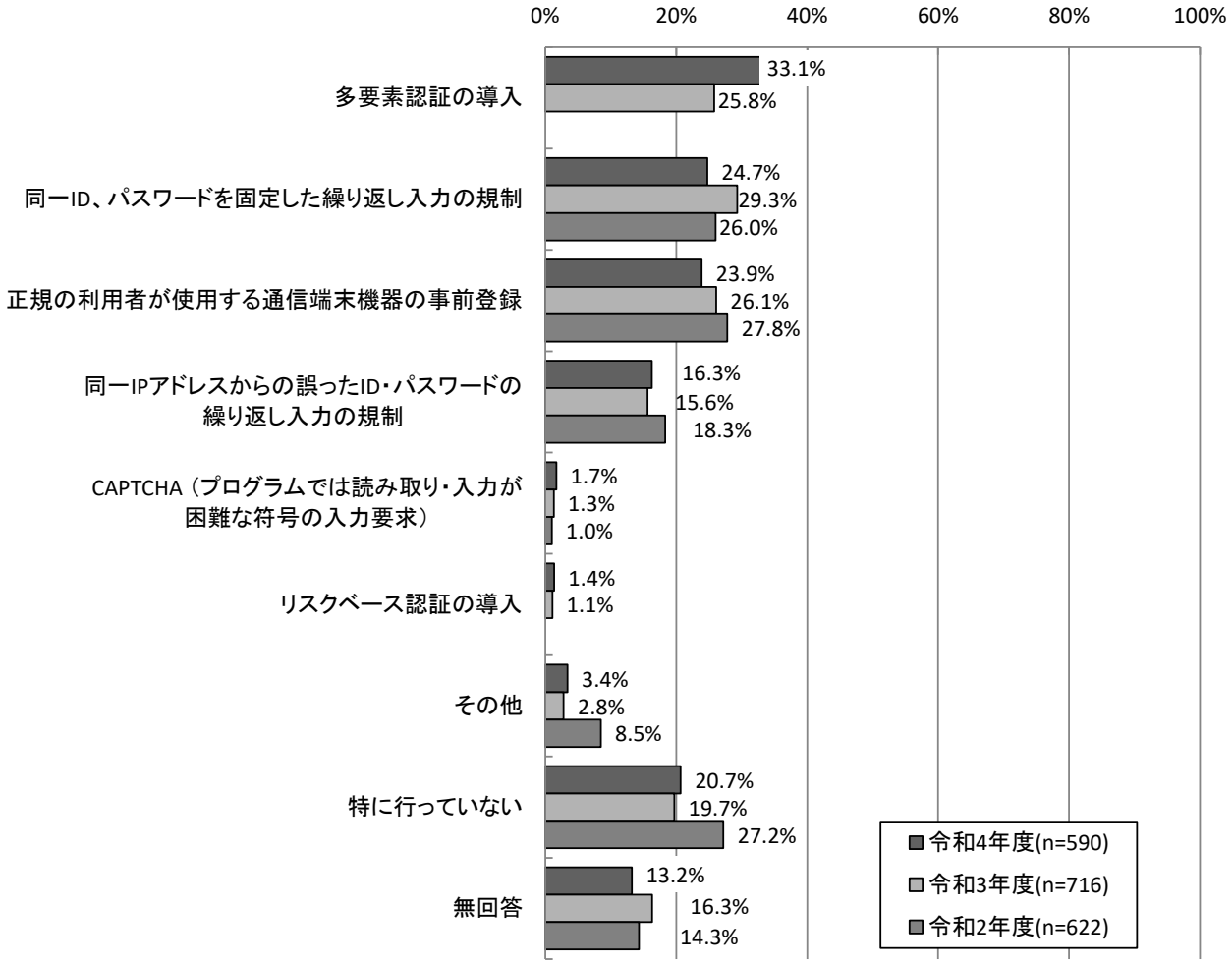
【業種別分析】業種別にみると、「多要素認証の導入」については、「行政サービス」が55.8%、「情報通信」が42.9%で高くなっている。「同一ID、パスワードを固定した繰り返し入力の規制」については、「運輸業」が40.9%で最も高くなっている。「正規の利用者が使用する通信端末機器の事前登録」については、「情報通信」が42.9%、「金融」が39.3%で高くなっている。

【業種別分析】不正ログイン対策



【経年変化】３年間を比較したところ、「多要素認証の導入」で7.3ポイント増加し、「同一ID、パスワードを固定した繰り返し入力の規制」で4.6ポイント減少している。

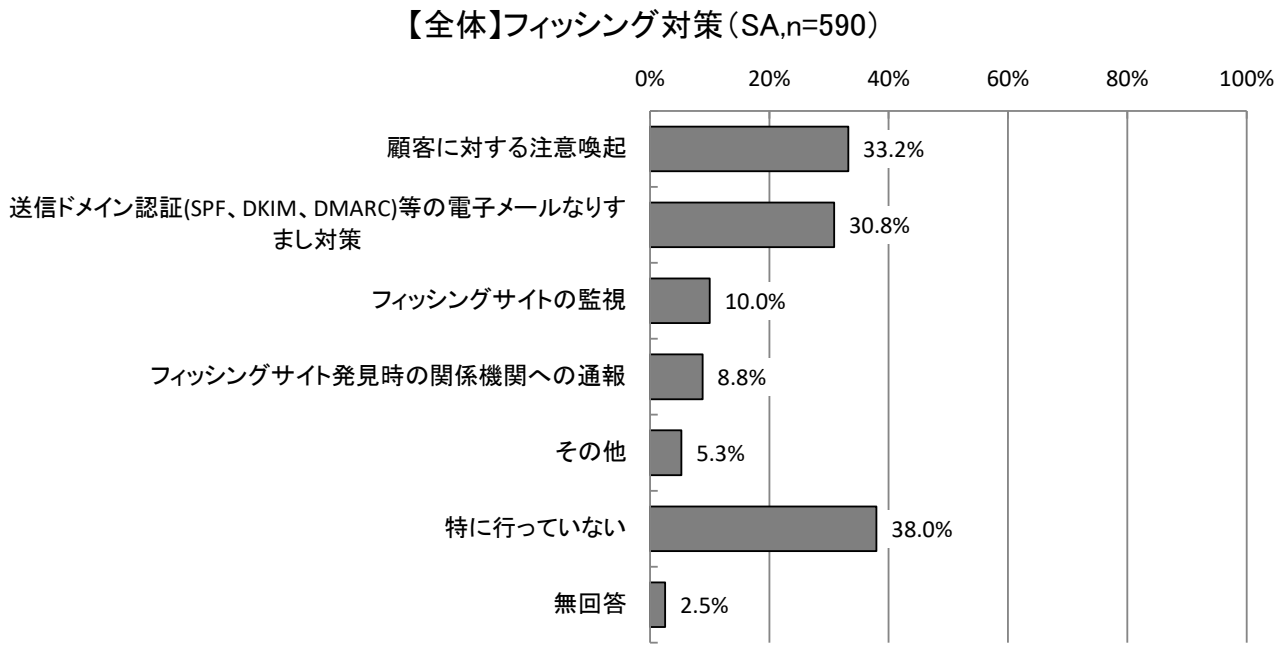
【経年変化】不正ログイン対策



※令和３年度調査で「多要素認証の導入」「リスクベース認証の導入」を新設

3.2.11　フィッシング対策【問22】

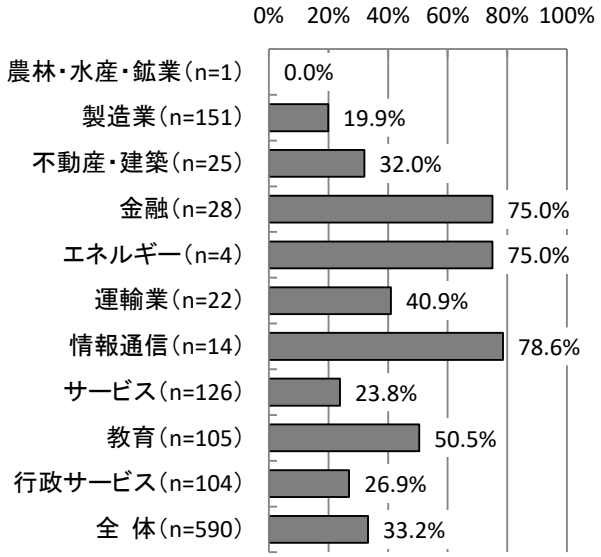
フィッシング対策については、「顧客に関する注意喚起」が33.2%で最も高く、次いで「送信ドメイン認証等の電子メールなりすまし対策」が30.8%となっている。一方で「特に行っていない」が38.0%となっている。



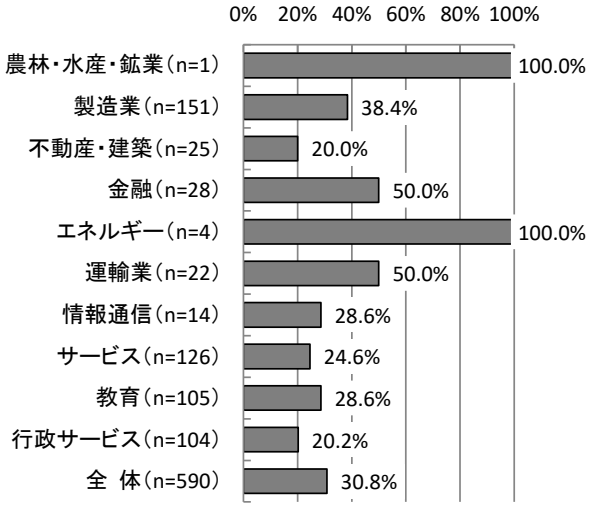
【業種別分析】業種別にみると、「顧客に関する注意喚起」では「情報通信」が78.6%、「金融」が75.0%で高くなっている。「送信ドメイン認証等の電子メールなりすまし対策」では「金融」と「運輸」がいずれも50%で高くなっている。

【業種別分析】フィッシング対策

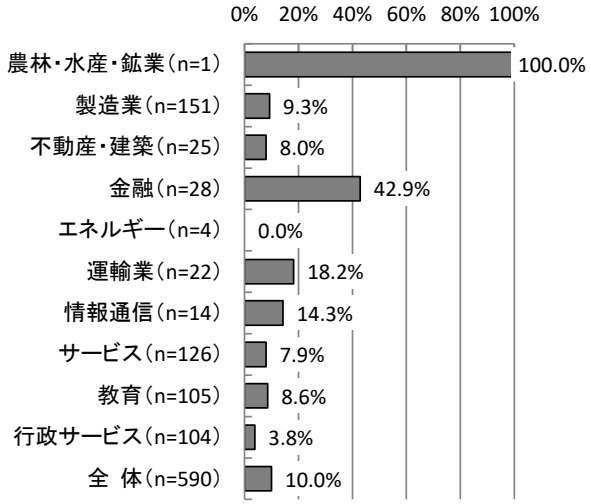
顧客に対する注意喚起



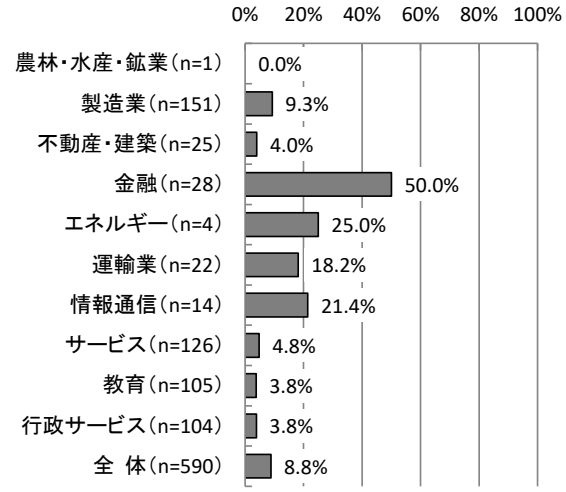
送信ドメイン認証(SPF、DKIM、DMARC)等の電子メールなりすまし対策



フィッシングサイトの監視



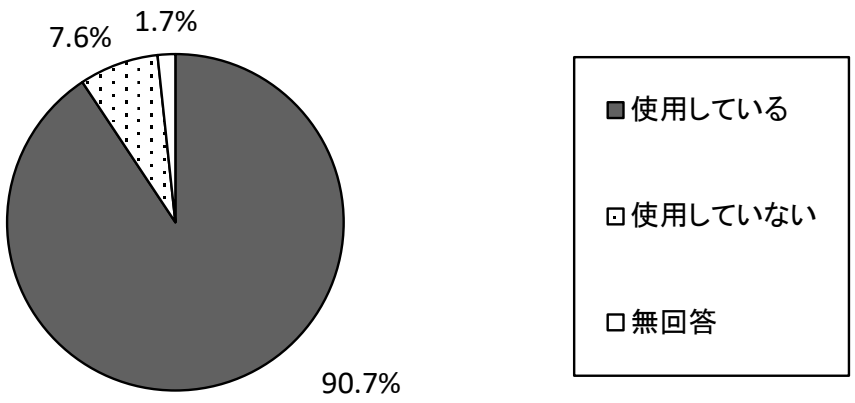
フィッシングサイト発見時の関係機関への通報



3.2.11　各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）の利用状況【問23】

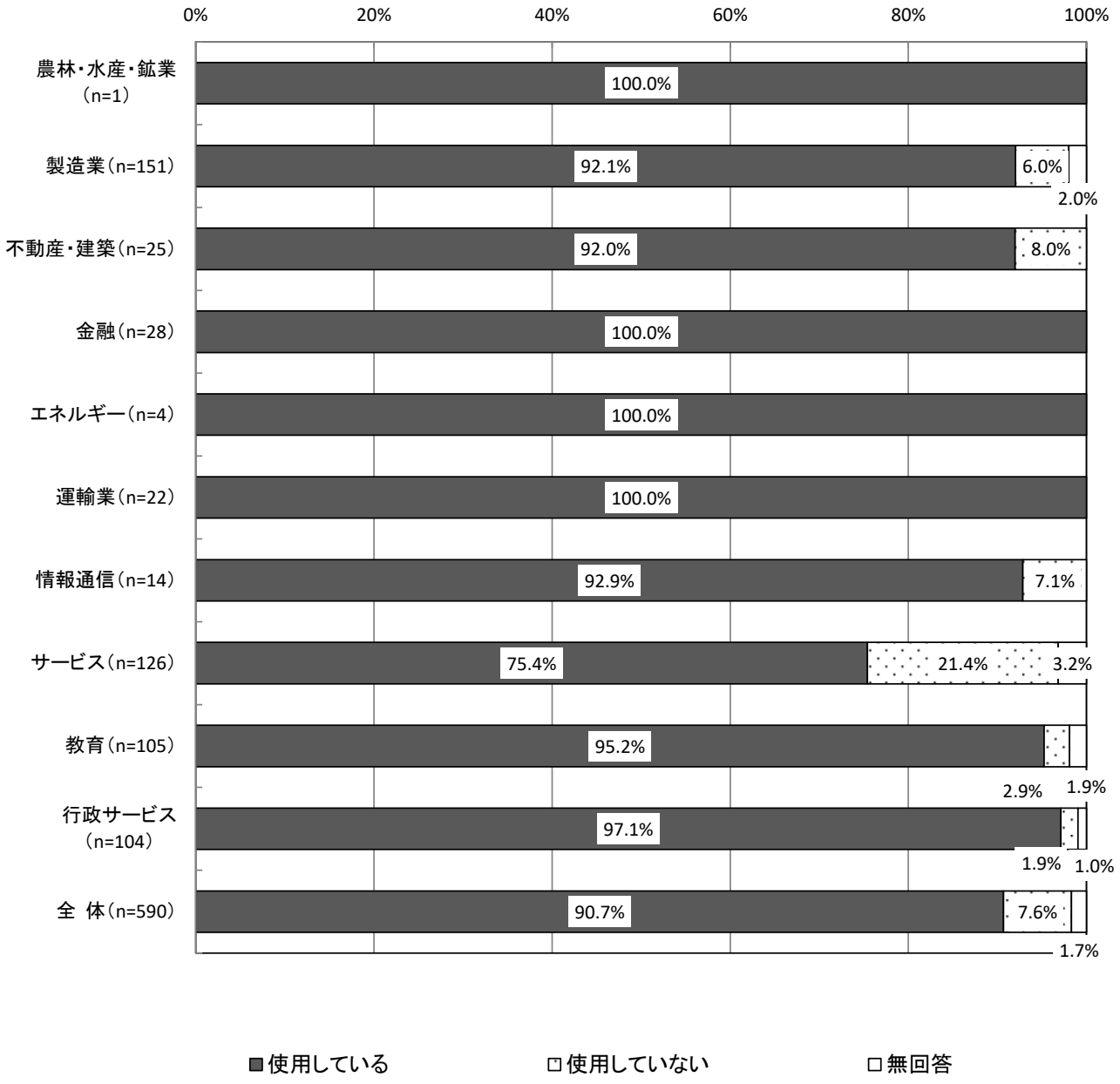
各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）の利用状況については、「使用している」が90.7%、「使用していない」が7.6%となっている。

【全体】各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）の利用状況（SA,n=590）



【業種別分析】業種別にみると、各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）を「使用している」については、「金融」「運輸業」などで100.0%と高くなっている。90%を下回っているのは「サービス」の75.4%で「使用していない」が21.4%となっている。

【業種別分析】各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）の利用状況

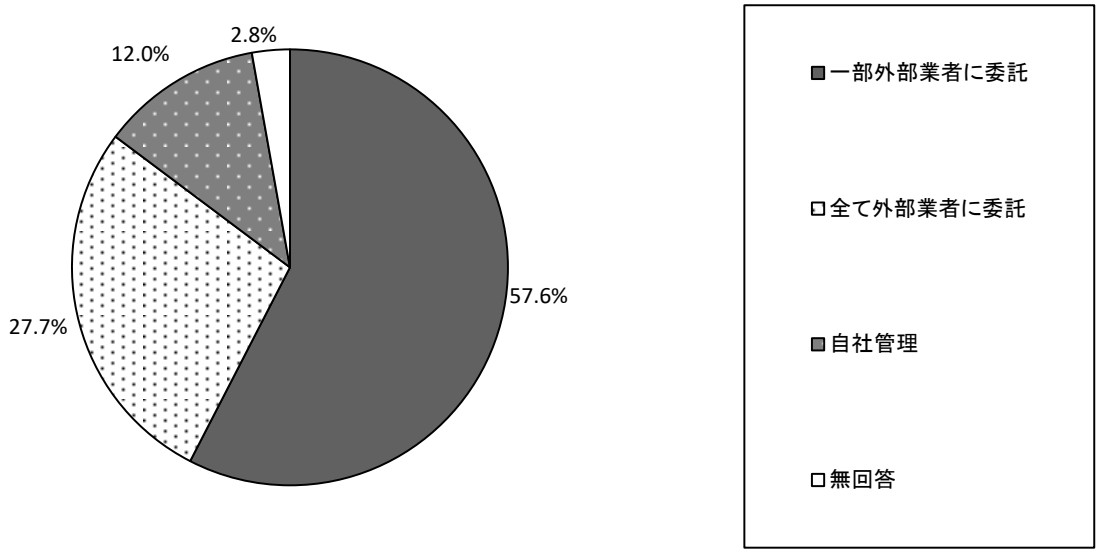


3.2.12　各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）の管理環境【問23-1】

各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）の管理環境については、「一部外部業者に委託」が57.6%で最も高く、次いで「全て外部業者に委託」が27.7%、「自社管理」が12.0%となっている。

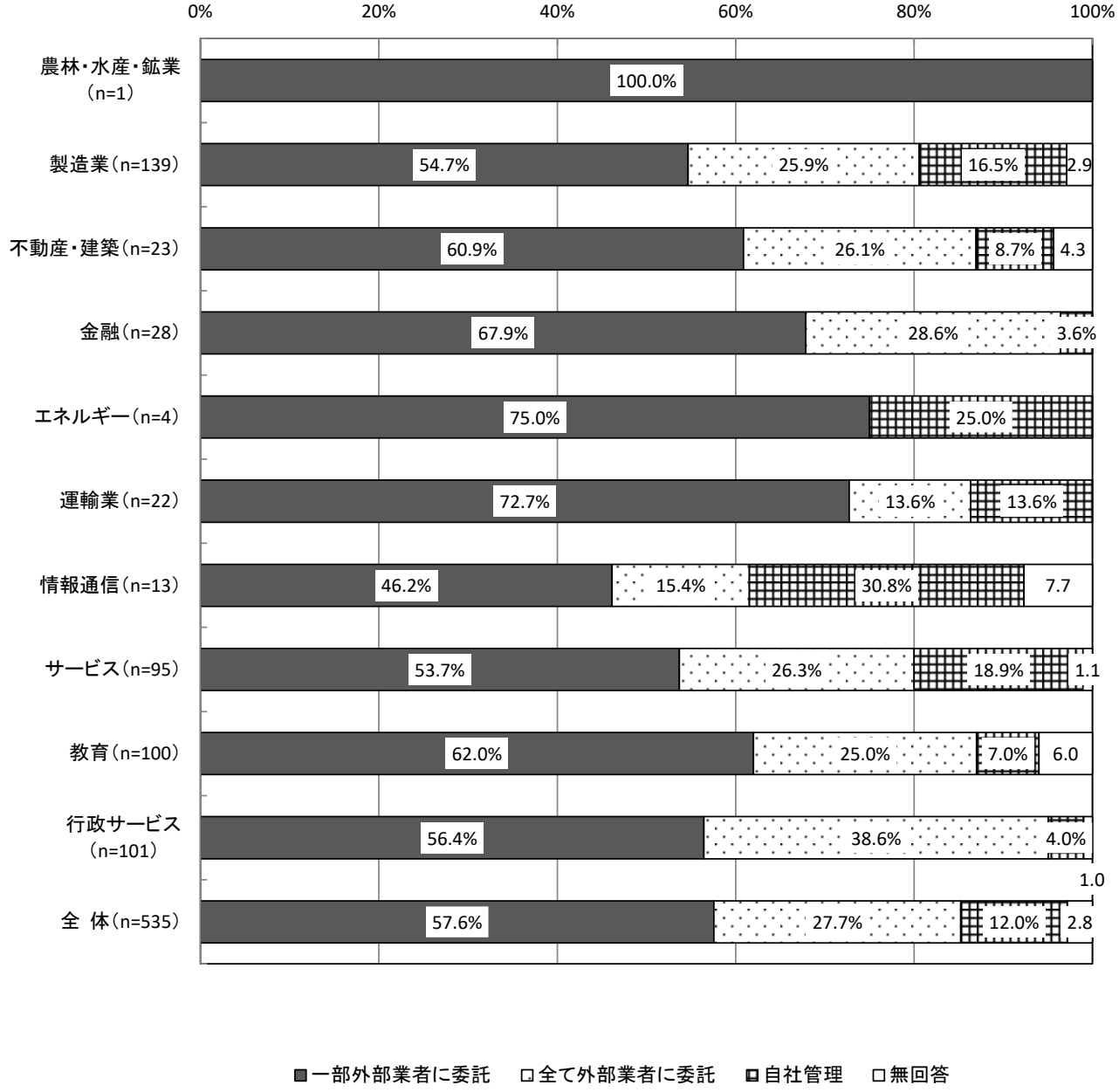
※本項目は、各種サービス（Webサイト、メール管理、ファイル管理等）を使用している社・団体等を対象としている。

【全体】各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）の管理環境（SA,n=535）



【業種別分析】業種別にみると、「自社管理」については、「情報通信」、「サービス」、「製造業」で多く、「行政サービス」で少なくなっている。

【業種別分析】各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）の管理環境

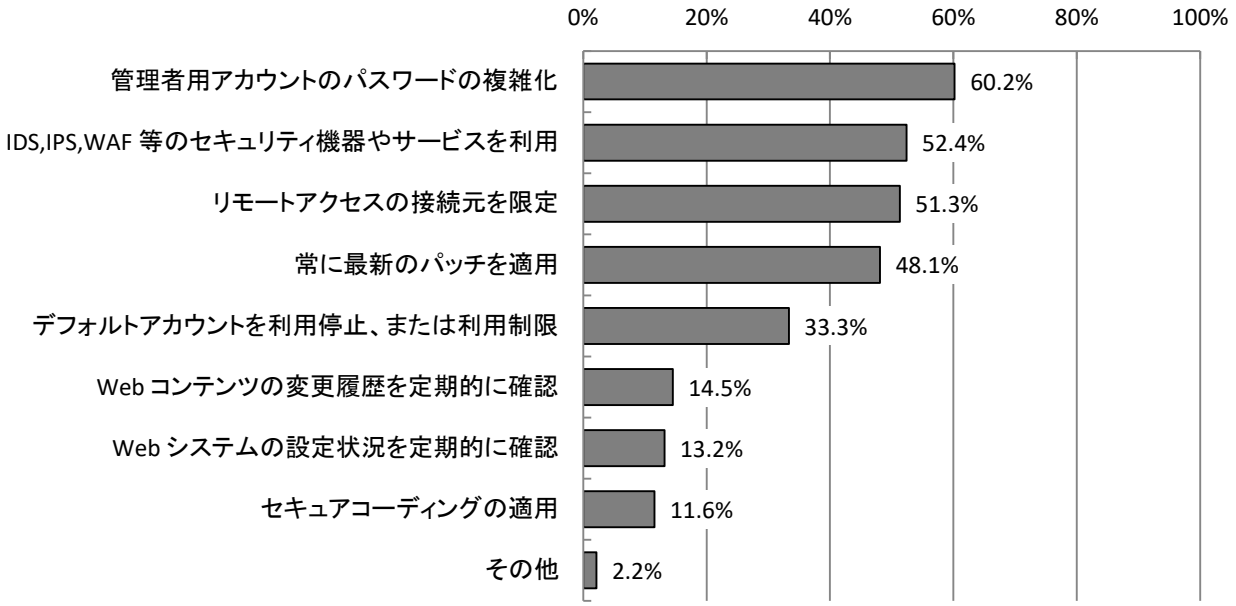


3.2.13 各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）のセキュリティ対策【問23-2】

各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）のセキュリティ対策については、「管理者用アカウントのパスワードの複雑化」が60.2%で最も高く、次いで「IDS、IPS、WAF等のセキュリティ機器やサービスを利用」が52.4%、「リモートアクセスの接続元を限定」が51.3%となっている。

※本項目は、各種サービスの全部又は一部を自社で管理している社・団体等を対象としている。

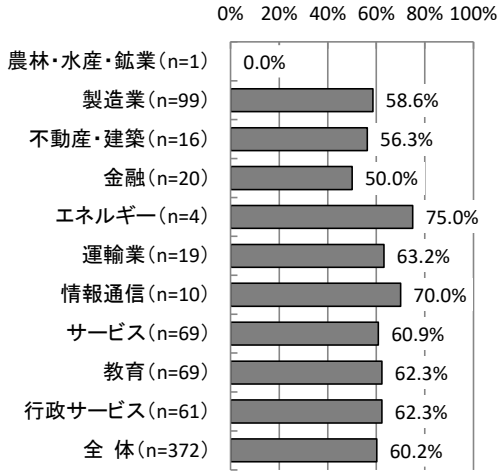
【全体】各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）のセキュリティ対策（MA,n=372）



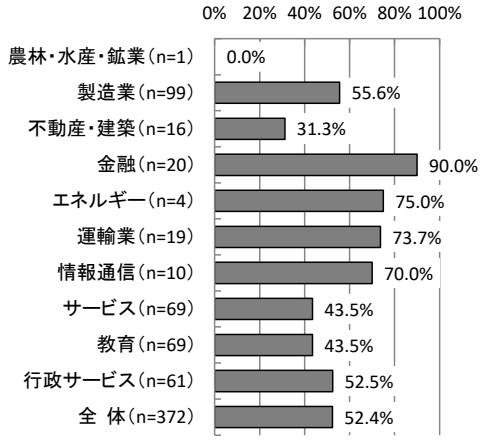
【業種別分析】業種別に見ると、「管理者用アカウントのパスワードの複雑化」については、「情報通信」が70.0%、「運輸業」が63.2%で高くなっている。「IDS, IPS,WAF等のセキュリティ機器やサービスを利用」については、「金融」が90.0%、「運輸業」が73.7%で高くなっている。

【業種別分析】各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）のセキュリティ対策

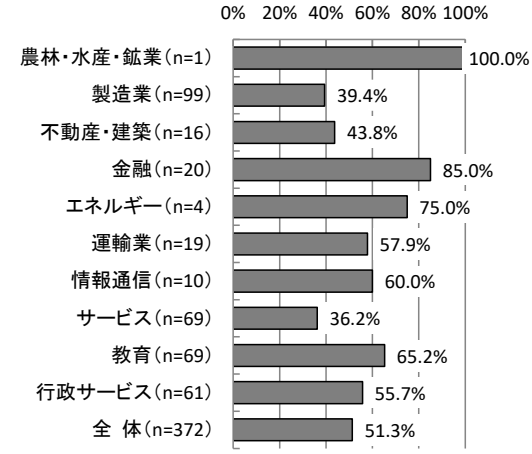
管理者用アカウントのパスワードの複雑化



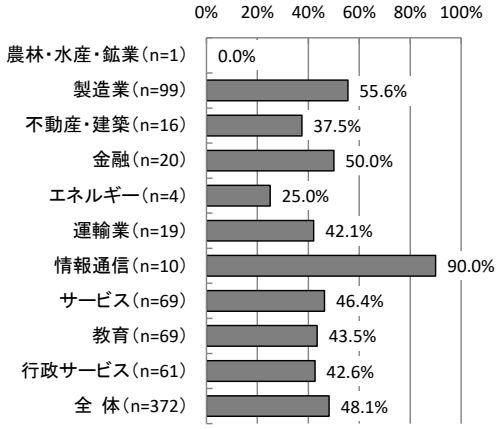
IDS, IPS, WAF 等のセキュリティ機器やサービスを利用



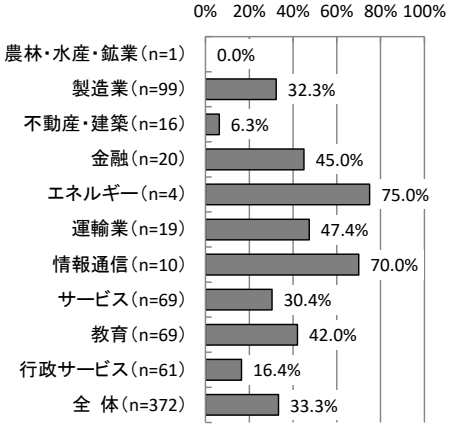
リモートアクセスの接続元を限定



常に最新のパッチを適用



デフォルトアカウントを利用停止、または利用制限

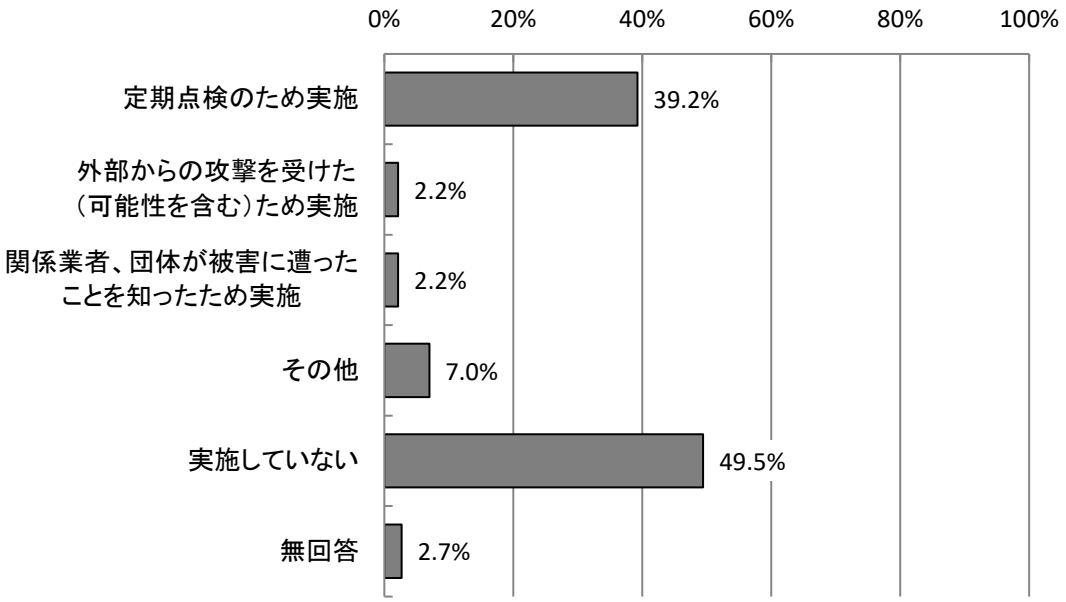


3.2.14　ぜい弱性調査（ペネトレーションテスト）実施の有無　【問23-3】

ぜい弱性調査（ペネトレーションテスト）実施の有無については、「実施していない」が49.5%と半数近くで最も高い。実施しているとの回答では、「定期点検のため実施」が39.2%と多くなっている。

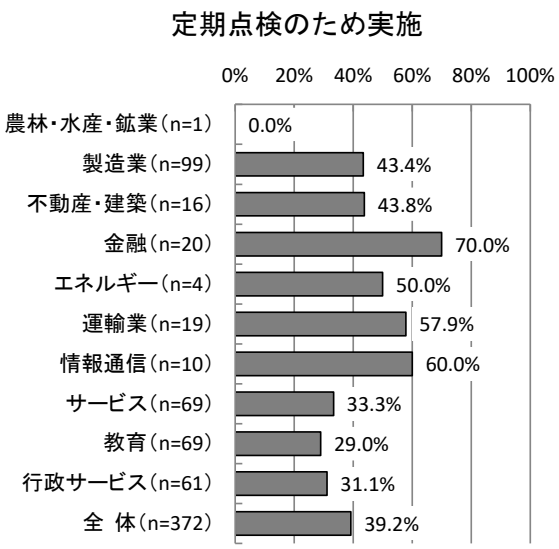
※本項目は、各種サービスの全部又は一部を自社で管理している社・団体等を対象としている。

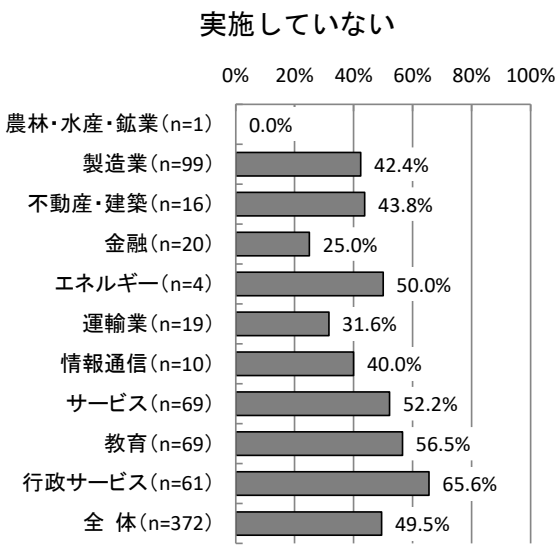
【全体】ぜい弱性調査（ペネトレーションテスト）実施の有無（MA,n=372）



【業種別分析】業種別にみると、「定期点検のため実施」については、「金融」が70.0%で最も高く、次いで「情報通信」が60.0%となっている。一方、「実施していない」については、「行政サービス」が65.6%、「教育」が56.5%で高くなっている。

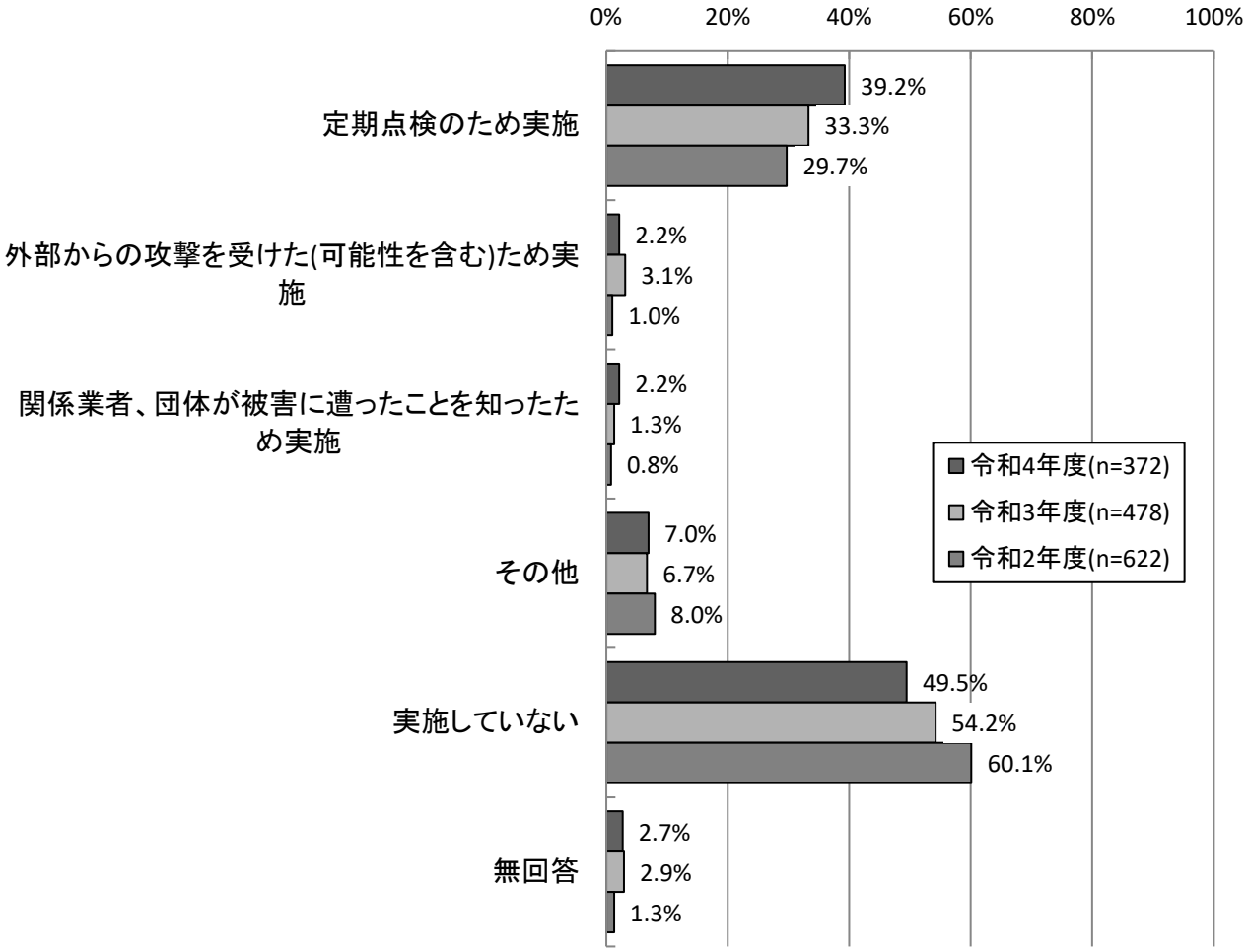
【業種別分析】ぜい弱性調査（ペネトレーションテスト）実施の有無





【経年変化】昨年度と比較すると、「定期点検のための実施」が 5.9 ポイント増加し、「実施していない」は 4.7 ポイント減少している。

【経年変化】ぜい弱性調査（ペネトレーションテスト）実施の有無

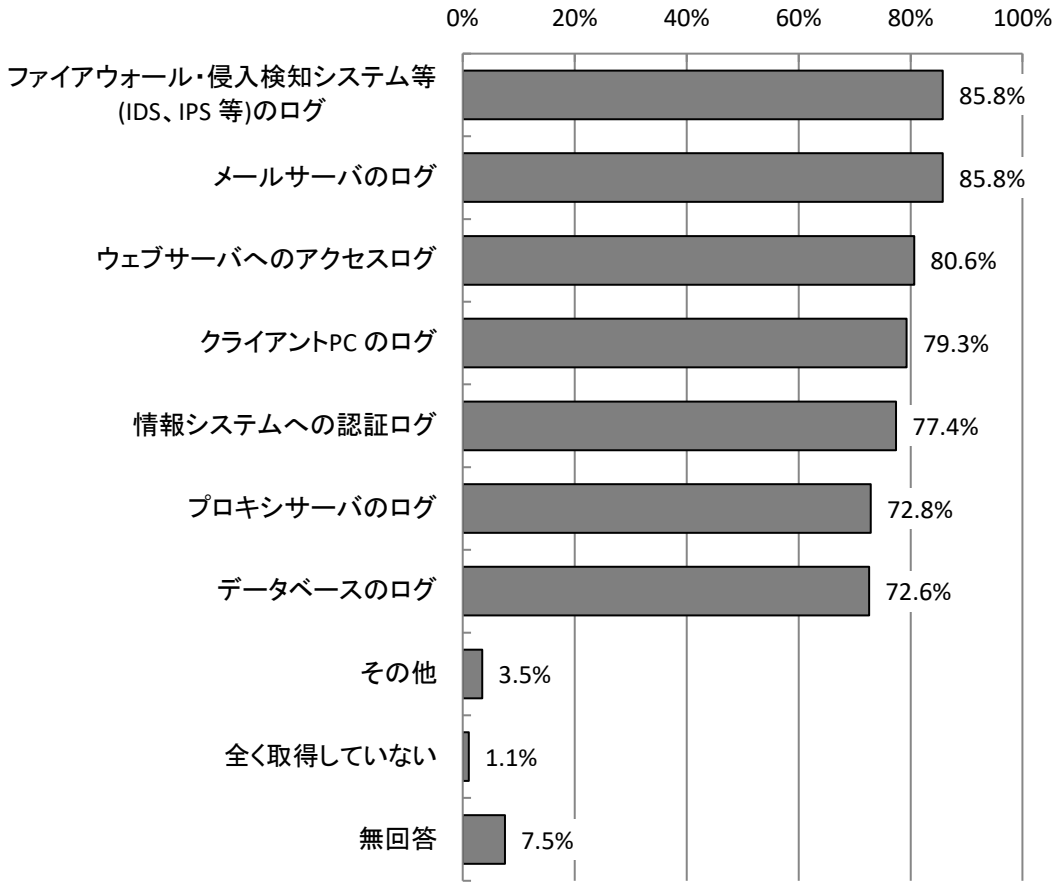


3.2.15　ログの取得状況　【問23-4】

ログの取得状況については、「ファイアウォール・侵入検知システム等（IDS、IPS等）のログ」と「メールサーバのログ」が85.8%で最も高く、「ウェブサーバへのアクセスログ」が80.6%、「情報システムへの認証ログ」が79.3%となっている。

※本項目は、各種サービスの全部又は一部を自社で管理している社・団体等を対象としている。

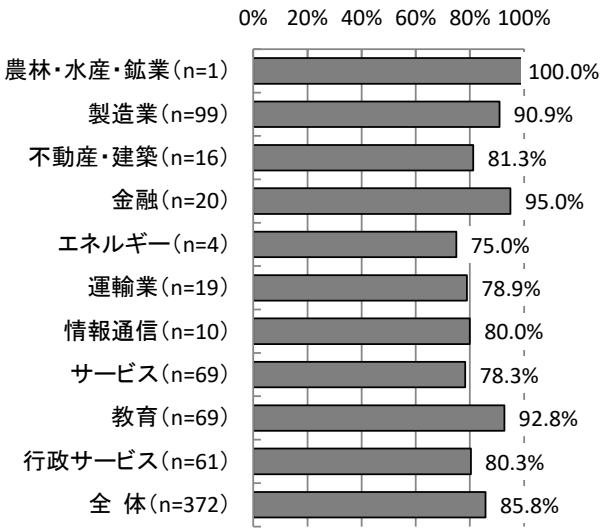
【全体】ログの取得状況（MA, n=372）



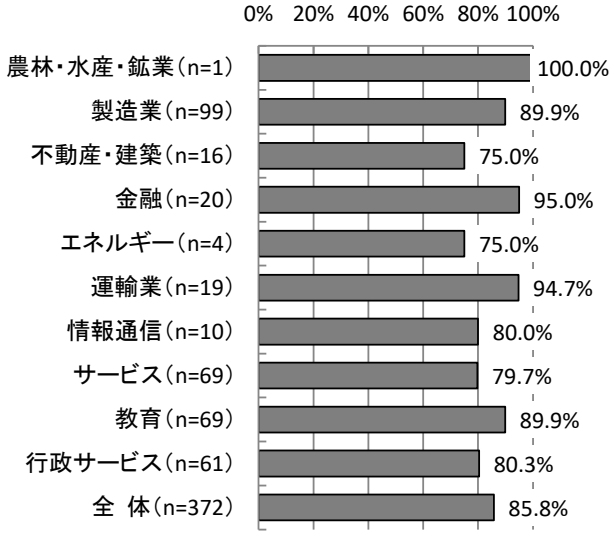
【業種別分析】業種別にみると、「ファイアウォール・侵入検知システム等（IDS、IPS等）のログ」では、「金融」が95.0%、「教育」が92.8%で高い。「メールサーバのログ」では「金融」が95.0%、「運輸業」が94.7%で高くなっている。また「ウェブサーバへのアクセスログ」では「金融」が95.0%、「教育」が88.4%で高くなっている。

【業種別分析】ログの取得状況

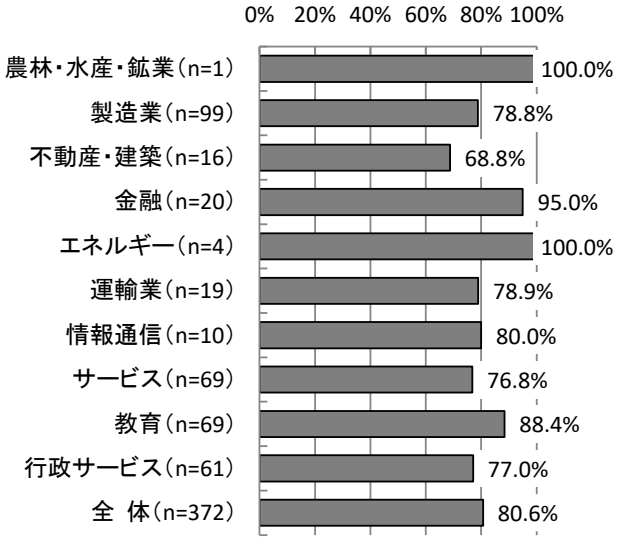
ファイアウォール・侵入検知システム等（IDS 、IPS 等）のログ



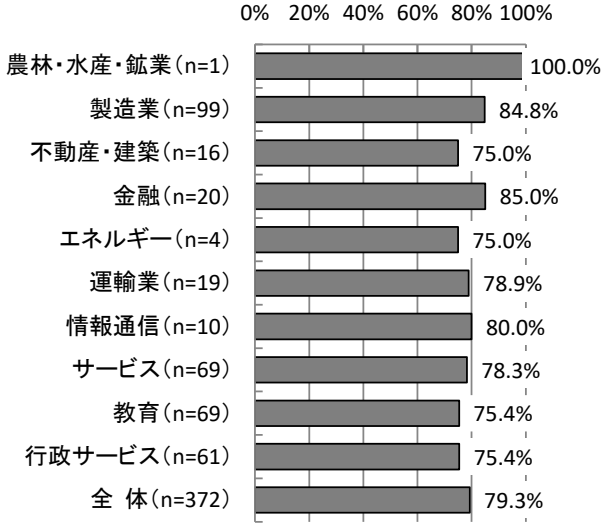
メールサーバのログ



ウェブサーバへのアクセスログ



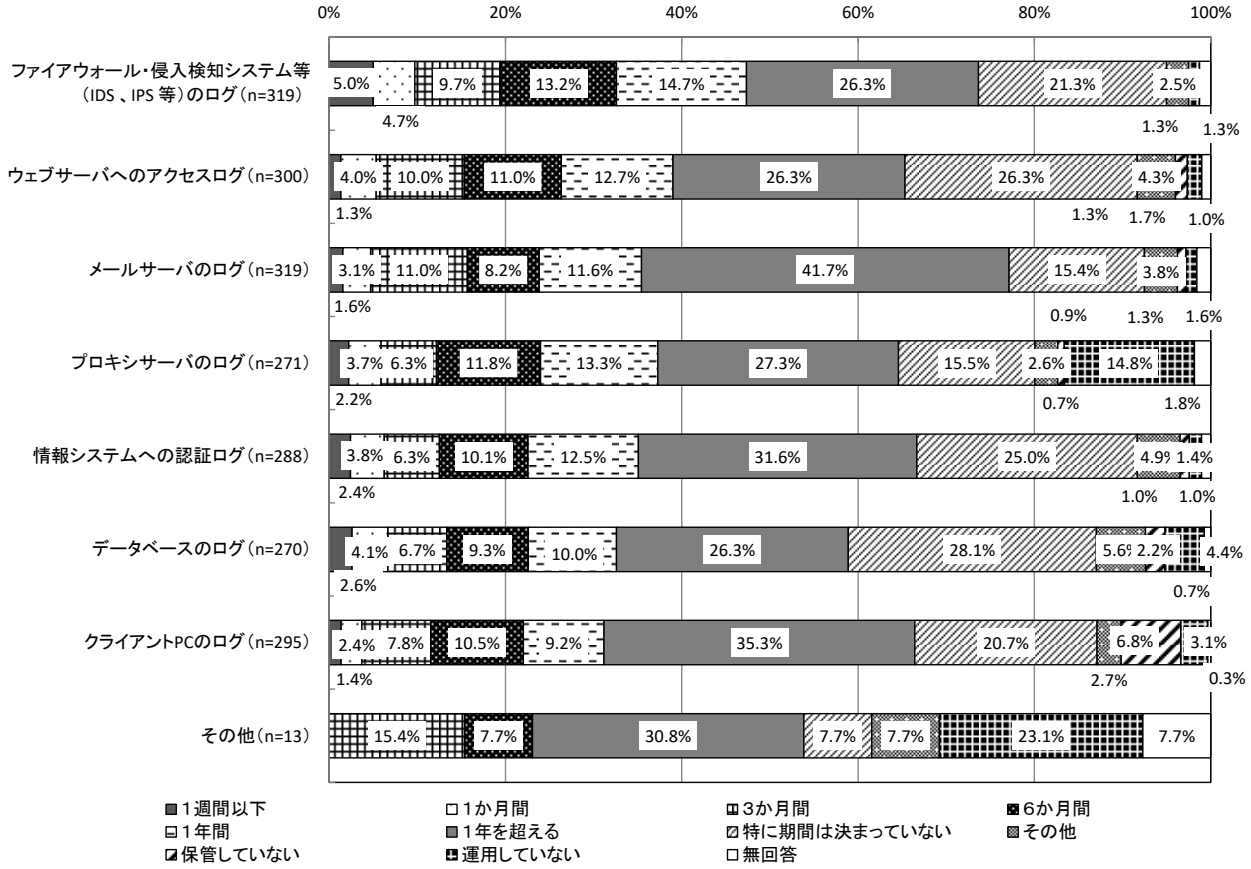
クライアントPCのログ



3.2.16　ログの保管期間　【問23-4A】

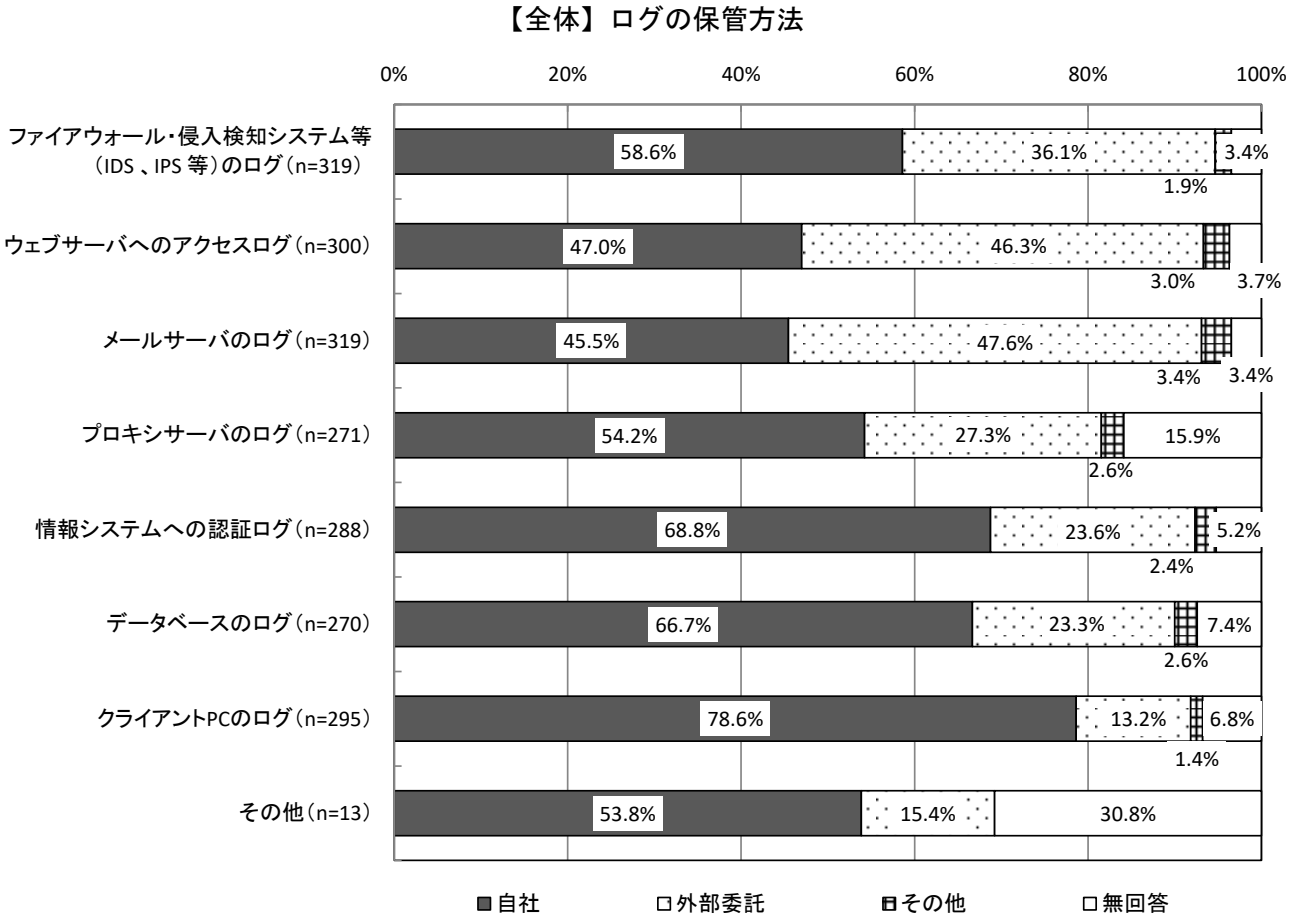
ログの保管期間については、「ウェブサーバへのアクセスログ」で「1年を超える」と「特に期間は決まっていない」が同じ割合、「データベースのログ」で「特に期間は決まっていない」が最も高い割合の他は、「１年を超える」が最も高い割合となっている。

【全体】ログの保管期間



3.2.17　ログの保管方法　【問23-4B】

ログの保管方法については、「メールサーバのログ」で「外部委託」が最も高い。その他のログの種類では「自社」が最も高い割合を占めている。

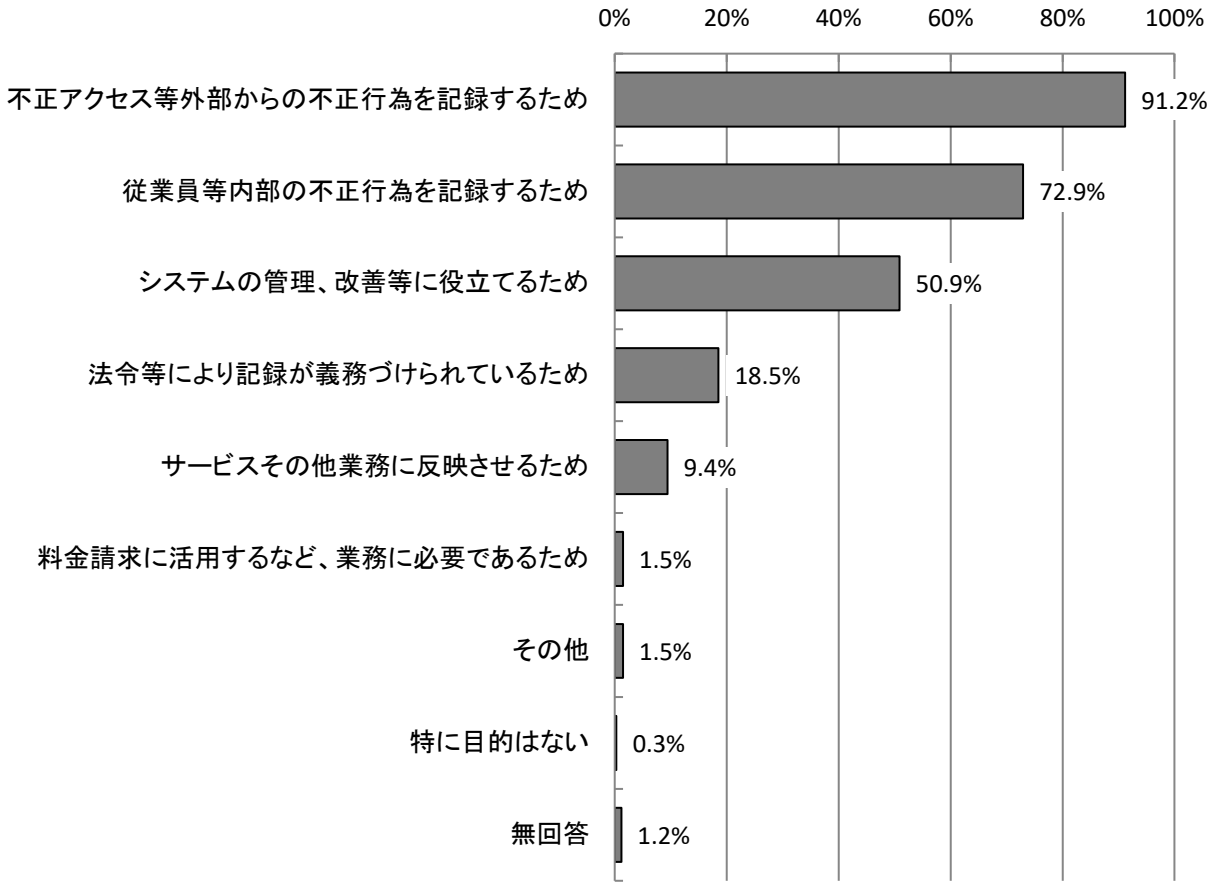


3.2.18　ログを取得・保管している理由　【問23-4-1】

ログを取得・保管している理由については、「不正アクセス等外部からの不正行為を記録するため」が91.2最も高く、次いで「従業員等内部の不正行為を記録するため」が72.9%、「システムの管理、改善等に役立てるため」が50.9%となっている。

※本項目は、ログを取得している社・団体等を対象としている。

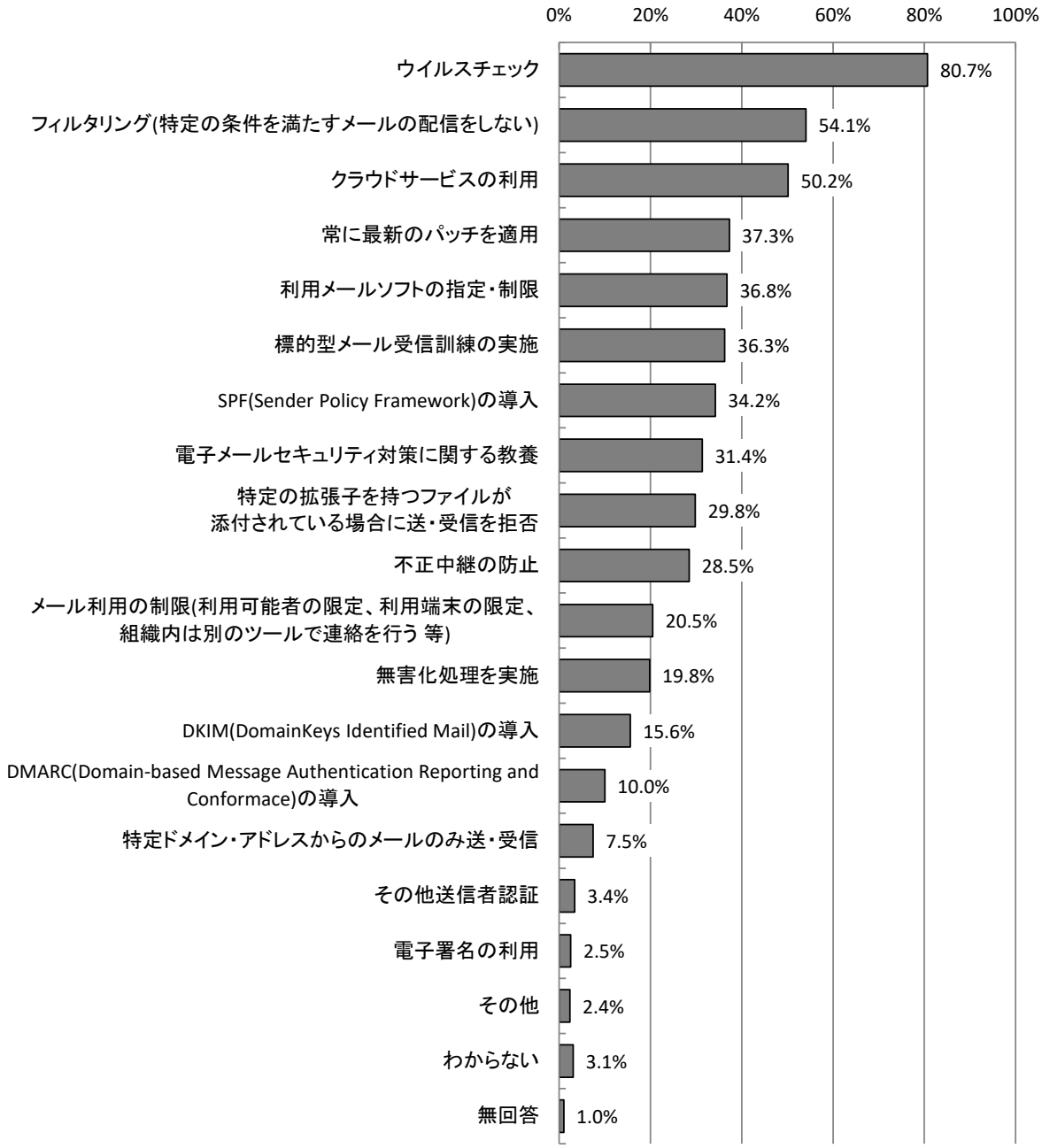
【全体】ログを取得・保管している理由（MA,n=340）



3.2.19　電子メールに関するセキュリティ対策　【問24】

電子メールに関するセキュリティ対策については、「ウイルスチェック」が80.7%で最も高く、次いで「フィルタリング（特定の条件を満たすメールの配信をしない）」が54.1%、「クラウドサービスの利用」が50.2%となっている。

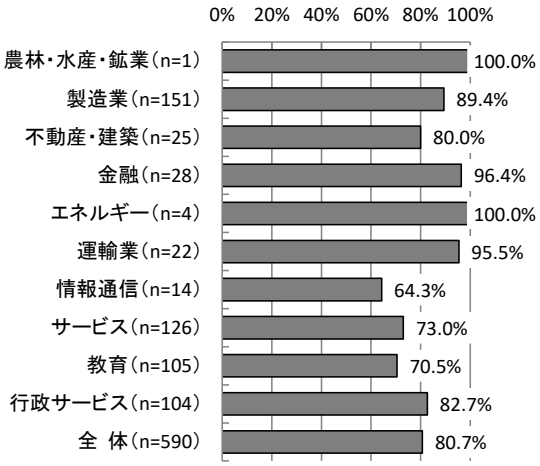
【全体】電子メールに関するセキュリティ対策（MA, n=590）



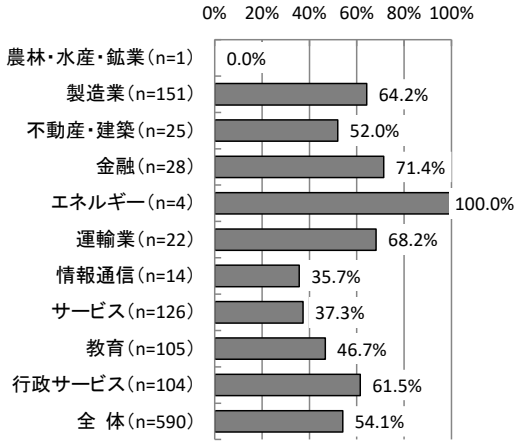
【業種別分析】業種別にみると、「ウイルスチェック」については、「金融」が96.4と高く、「運輸業」も95.5%と高くなっている。「フィルタリング」については「金融」が71.4%、「クラウドサービスの利用」については「情報通信」が71.3%と高くなっている。

【業種別分析】電子メールに関するセキュリティ対策

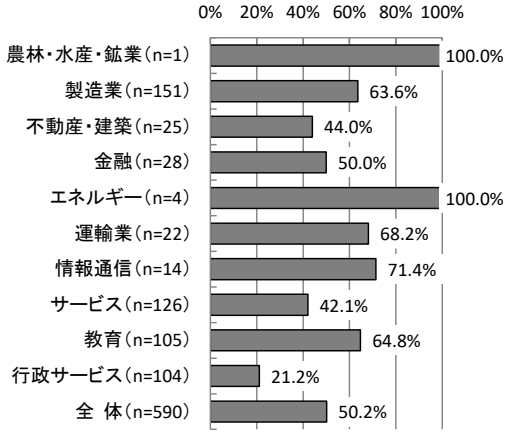
ウイルスチェック



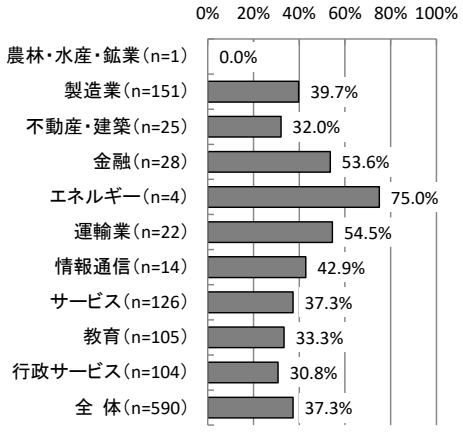
フィルタリング（特定の条件を満たすメールの配信をしない）



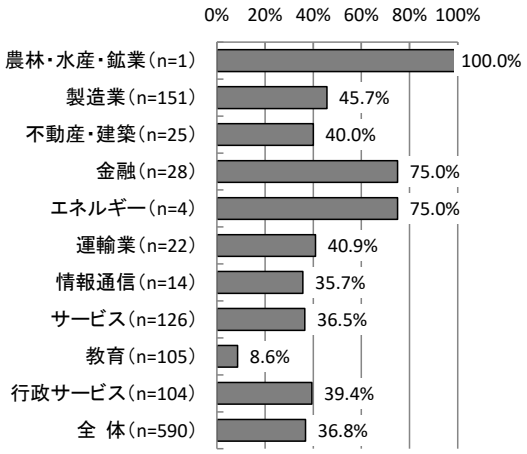
クラウドサービスの利用



常に最新のパッチを適用



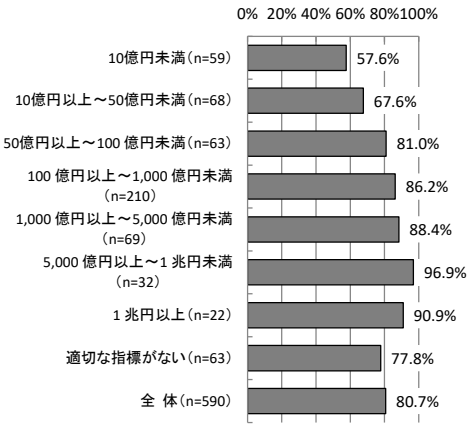
利用メールソフトの指定・制限



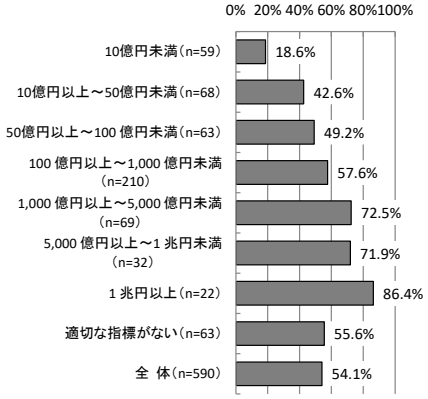
【予算規模別分析】予算規模別にみると、「ウイルスチェック」については、「5,000億円以上～１兆円未満」が96.9%で最も高く、次いで「１兆円以上」が90.9%となっている。「フィルタリング」については「１兆円以上」が86.4%で最も高く、次いで「1,000億円以上～5,000億円未満」が72.5%、「5,000億円以上～１兆円未満」が71.9%となっている。

【予算規模別分析】電子メールに関するセキュリティ対策

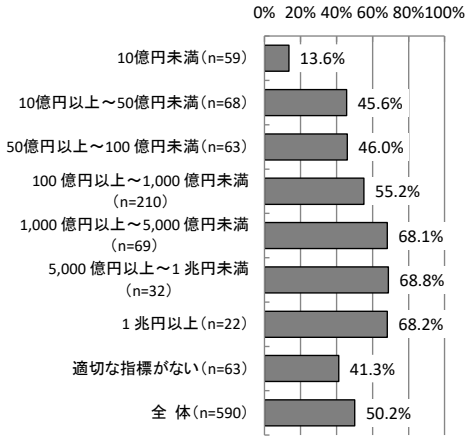
ウイルスチェック



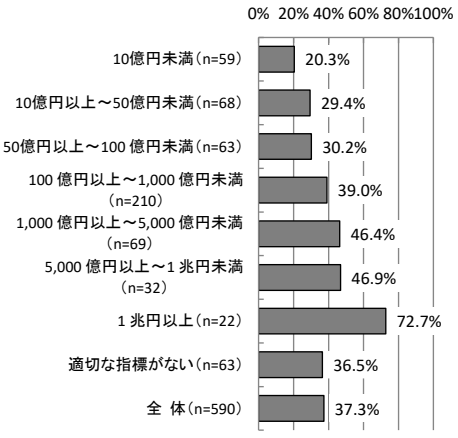
フィルタリング（特定の条件を満たすメールの配信をしない）



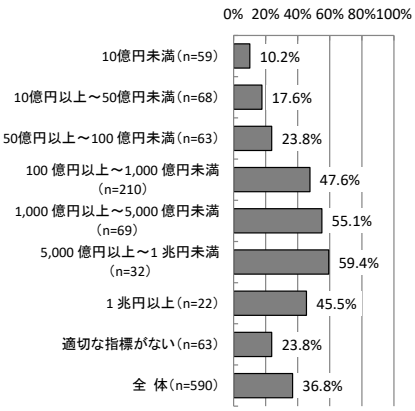
クラウドサービスの利用



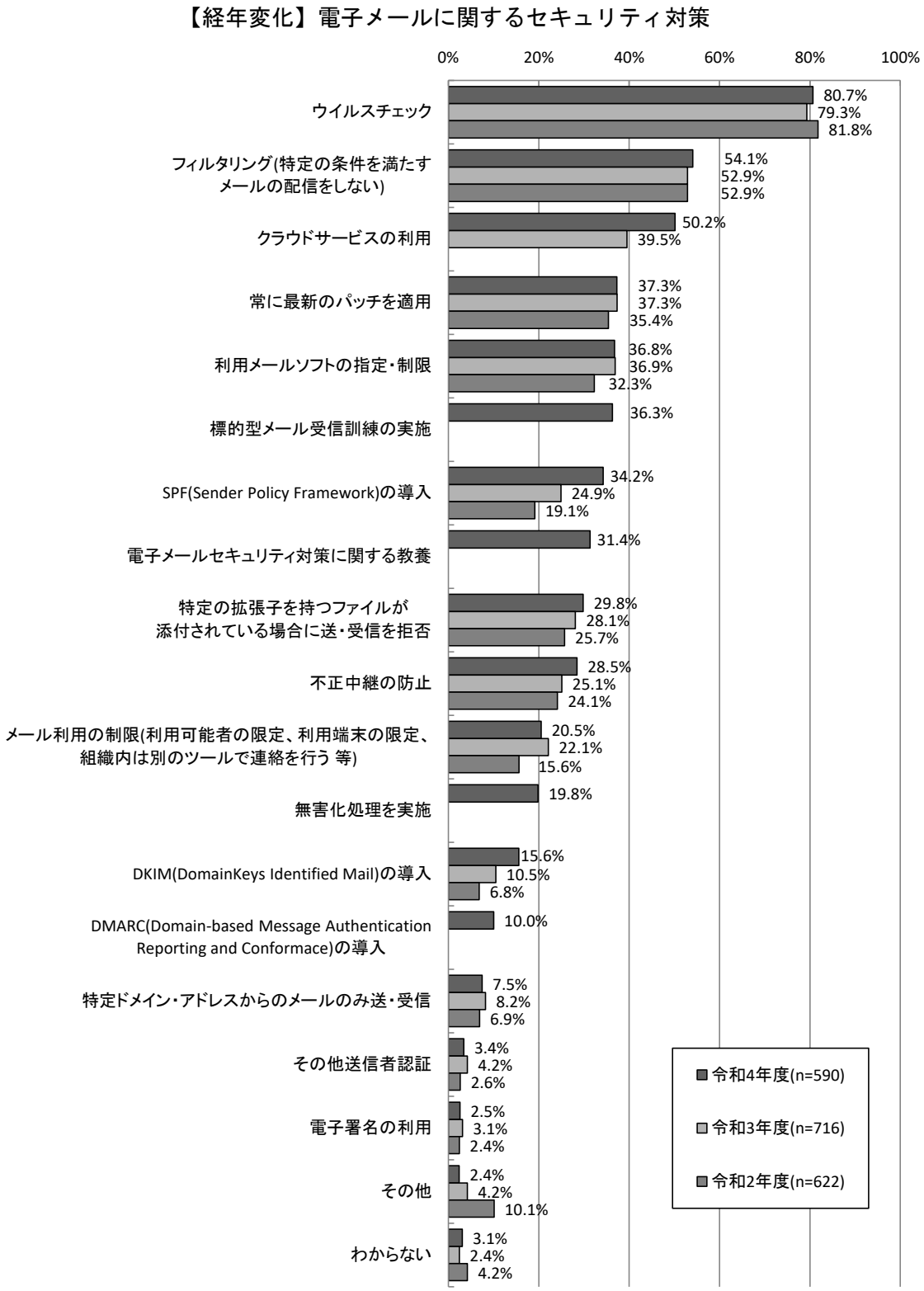
常に最新のパッチを適用



利用メールソフトの指定・制限



【経年変化】昨年度と比較すると、「クラウドサービスの利用」が10.7ポイント、「SPF（Sender Policy　Framework ）の導入」が9.3ポイント増加している。



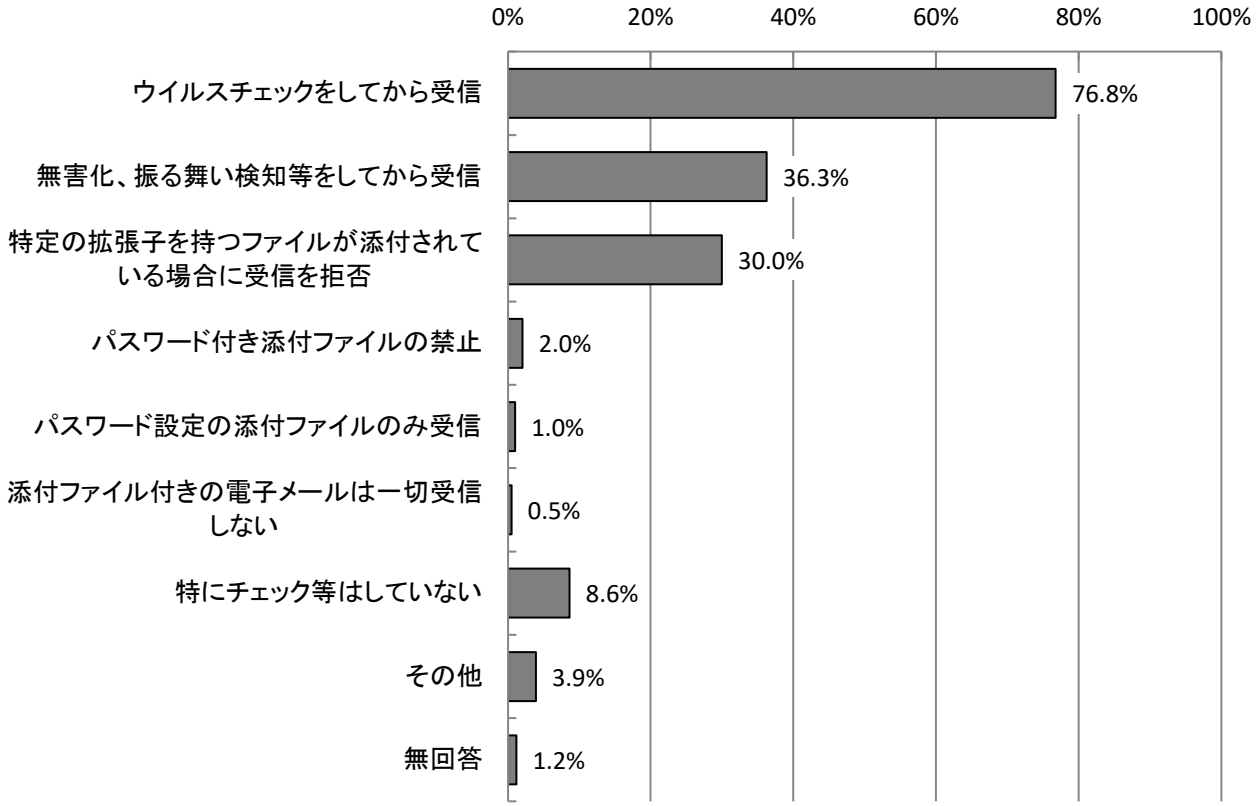
※令和３年度調査で、「クラウドサービスの利用」を新設。

※令和４年度調査で、「DMARC（Domain-based Message Authentication Reporting and Conformace）の導入」「無害化処理を実施」「標的型メール受信訓練の実施」「電子メールセキュリティ対策に関する教養」を新設。

3.2.20　添付ファイルの取り扱い　【問25】

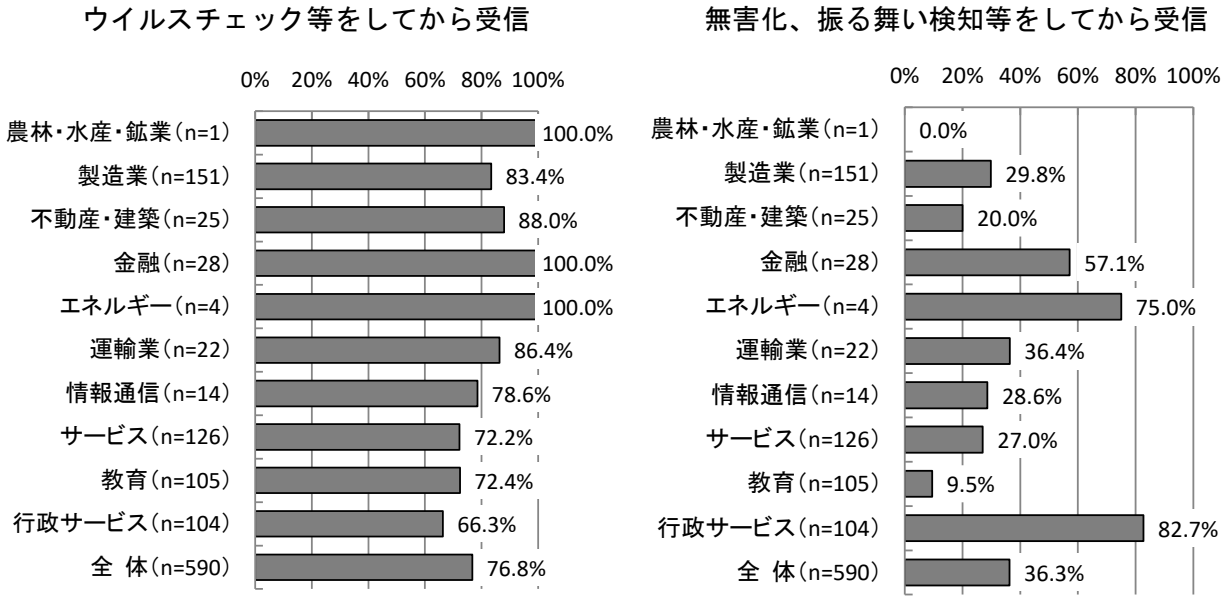
添付ファイルの取り扱いについては、「ウイルスチェックをしてから受信」が76.8%で最も高い。一方、「特にチェック等はしていない」は8.6%であった。

【全体】添付ファイルの取り扱い（MA,n=590）

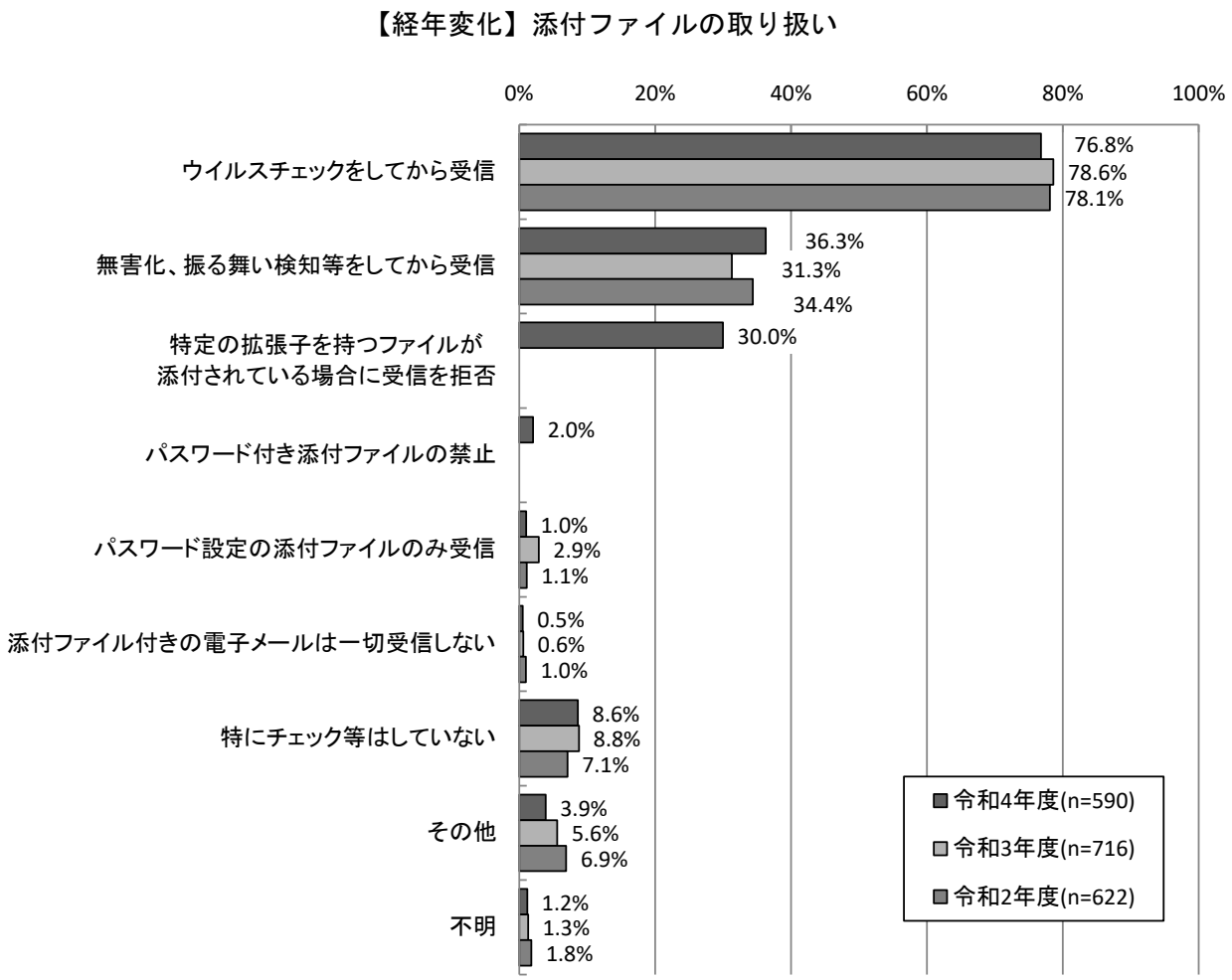


【業種別分析】業種別にみると、「ウイルスチェック等をしてから受信」は「金融」で 100.0%、「不動産・建築」で 88.0%、「運輸業」で 86.4%となっている。

【業種別分析】添付ファイルの取り扱い



【経年変化】経年変化をみると、「無害化、振る舞い検知等をしてから受信」が5.0ポイント増加し、「パスワード設定の添付ファイルのみ受信」が1.9ポイント減少している。

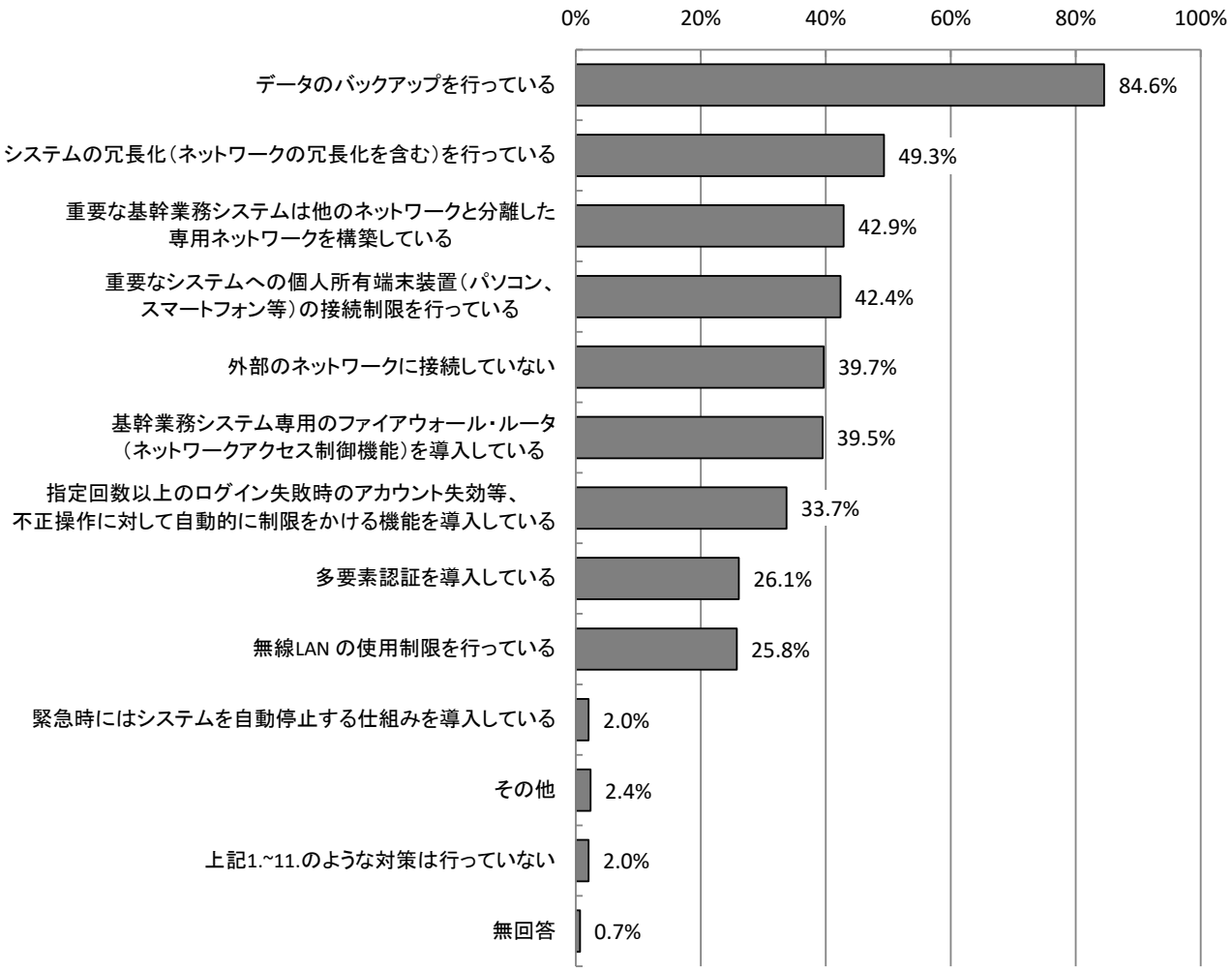


※令和４年度調査で、「特定の拡張子を持つファイルが添付されている場合に受信を拒否」「パスワード付き添付ファイルの禁止」を新設。

3.2.21　重要システムの不正アクセス対策状況　【問26】

重要システムの不正アクセス対策状況については、「データのバックアップを行っている」が84.6%で最も高く、「システムの冗長化（ネットワークの冗長化を含む）を行っている」が49.3%、「重要な基幹業務システムは他のネットワークと分離した専用ネットワークを構築している」が42.9%、「重要なシステムへの個人所有端末装置（パソコン、スマートフォン等）の接続制限を行っている」が42.4%となっている。

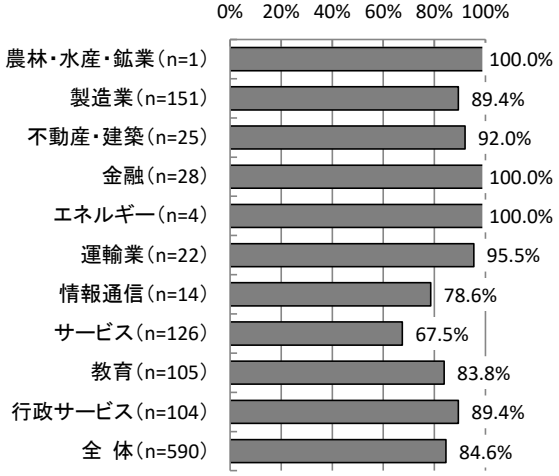
【全体】重要システムの不正アクセス対策状況（MA,n=590）



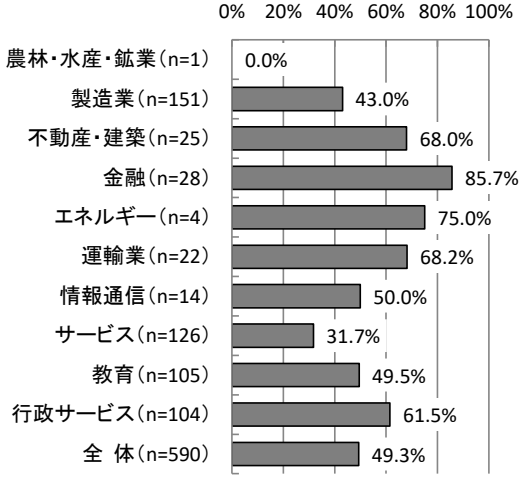
【業種別分析】業種別にみると、「データのバックアップを行っている」については、「金融」が100.0%、「運輸業」が95.5%で高くなっている。「システムの冗長化を行っている」については、「金融」が85.7%で最も高くなっている。

【業種別分析】重要システムの不正アクセス対策状況

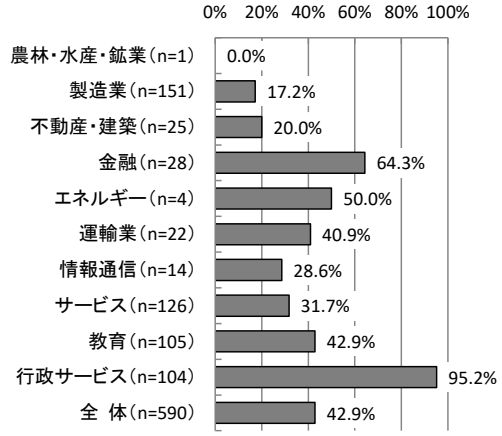
データのバックアップを行っている



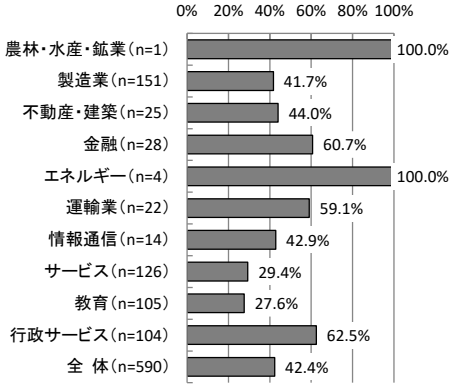
システムの冗長化
（ネットワークの冗長化を含む）を行っている



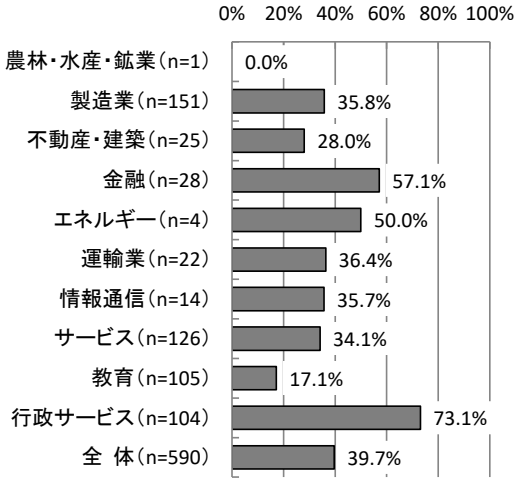
重要な基幹業務システムは他のネットワークと
分離した専用ネットワークを構築している



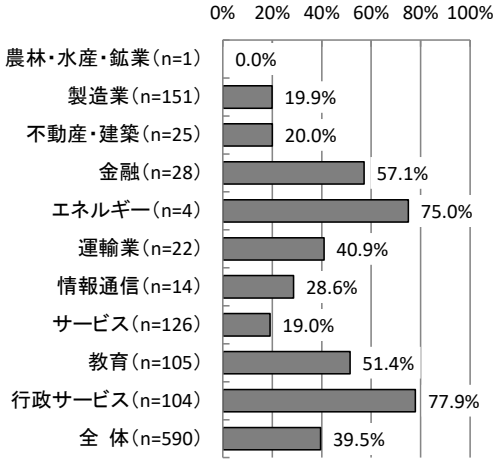
重要なシステムへの個人所有端末装置（パソコン、スマートフォン等）の接続制限を行っている



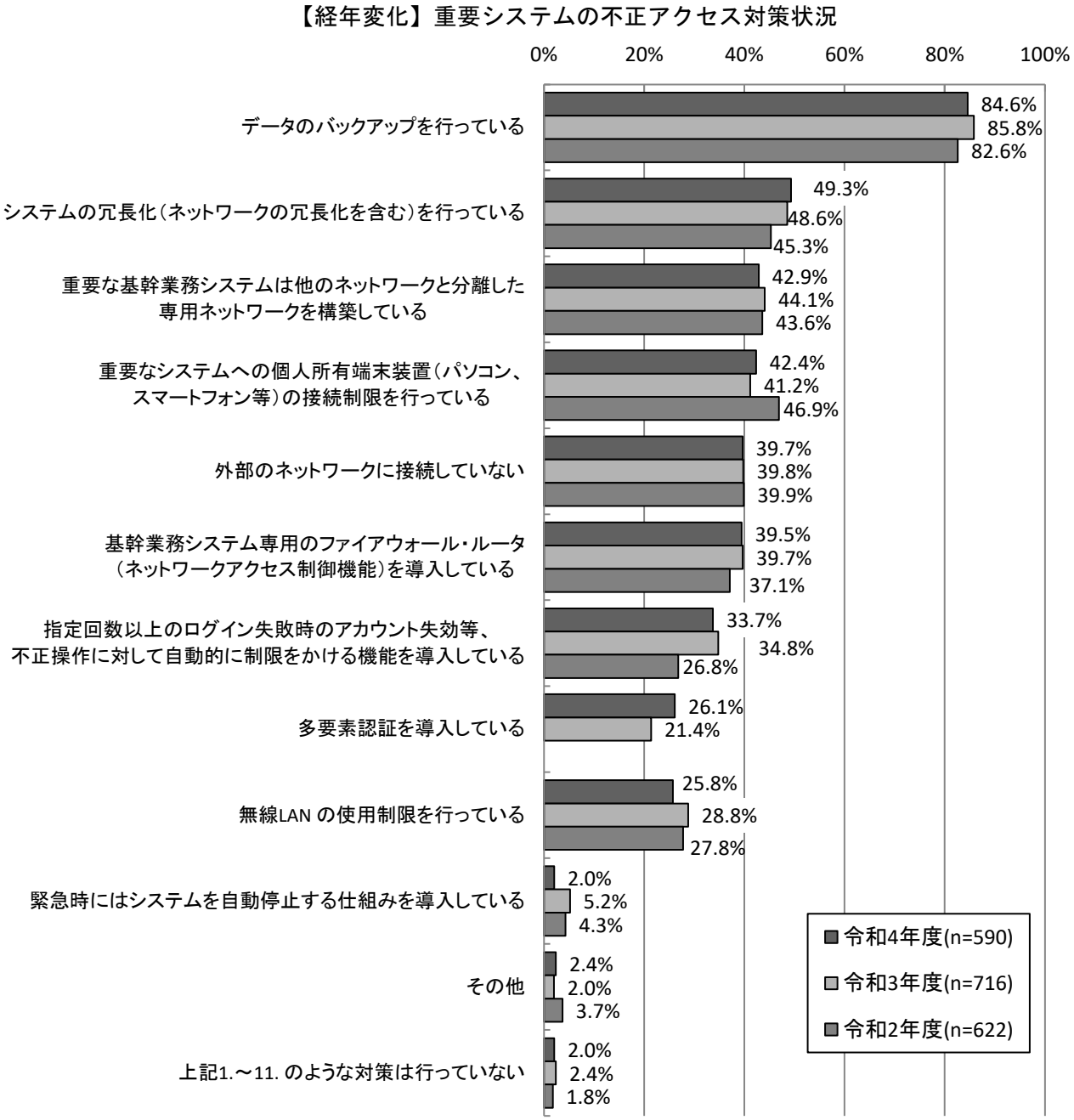
外部のネットワークに接続していない



基幹業務システム専用のファイアウォール・ルーター（ネットワークアクセス制御機能）を導入している



【経年変化】昨年度と比較すると、「多要素認証を導入している」が 4.7 ポイント増加している。一方、「緊急時にはシステムを自動停止する仕組みを導入している」が 3.2 ポイント、「無線 LAN の使用制限を行っている」が 3.0 ポイントの減少となっている。

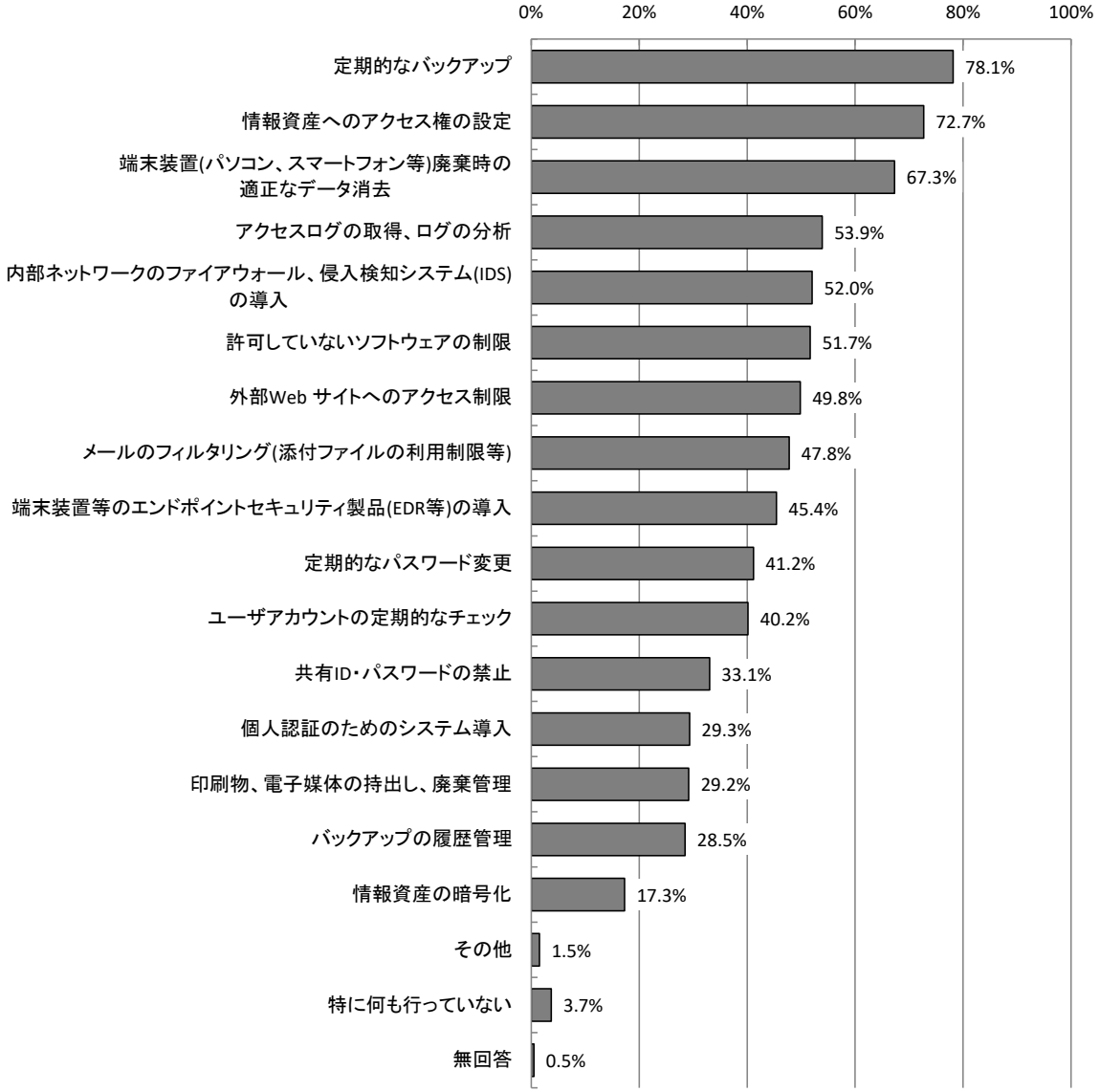


※令和３年度調査で、「多要素認証を導入している」を新設。

3.2.22　不正アクセス等への対策状況　【問27】

不正アクセス等への対策状況については、「定期的なバックアップ」が78.1%で最も高く、次いで「情報資産へのアクセス権の設定」が72.7%、「端末装置（パソコン、スマートフォン等）廃棄時の適正なデータ消去」が67.3%となっている。

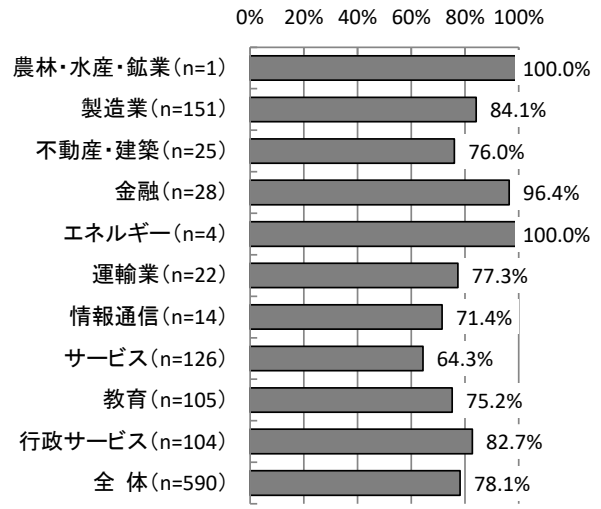
【全体】不正アクセス等への対策状況（MA, n=590）



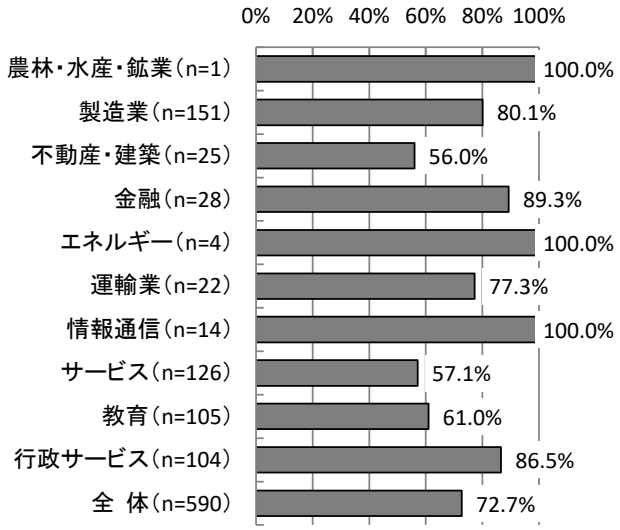
【業種別分析】業種別にみると、「情報資産へのアクセス権の設定」は「情報通信」が100.0%で高く、「定期的なバックアップ」と「情報資産へのアクセス権の設定」、「端末装置廃棄時の適正なデータの消去」については、「金融」がいずれも96.4%で高くなっている。

【業種別分析】不正アクセス等への対策状況

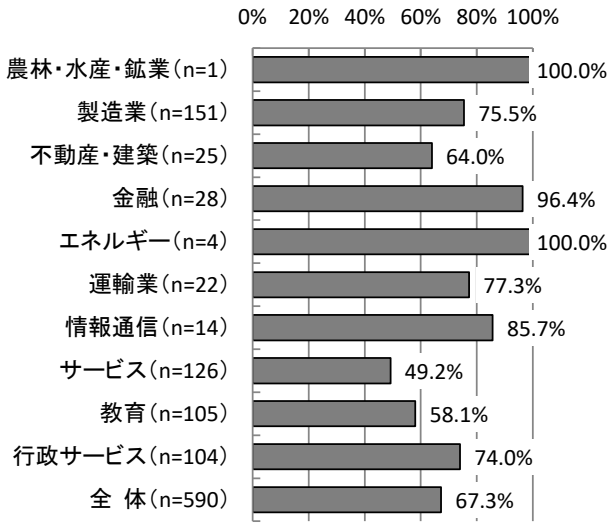
定期的なバックアップ



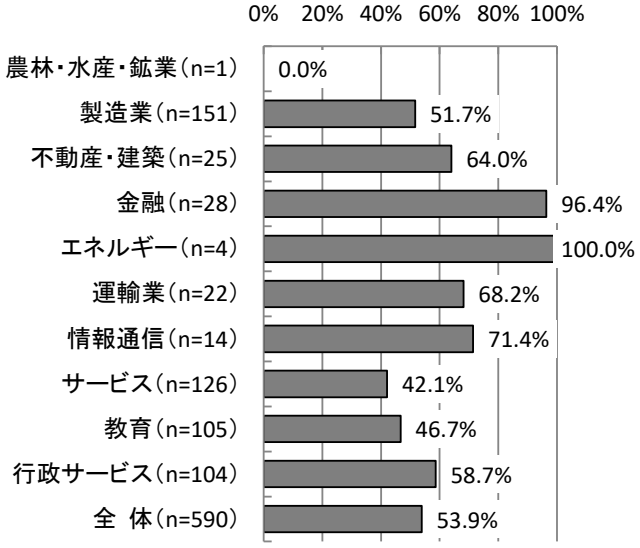
情報資産へのアクセス権の設定



端末装置（パソコン、スマートフォン等）廃棄時の適正なデータ消去

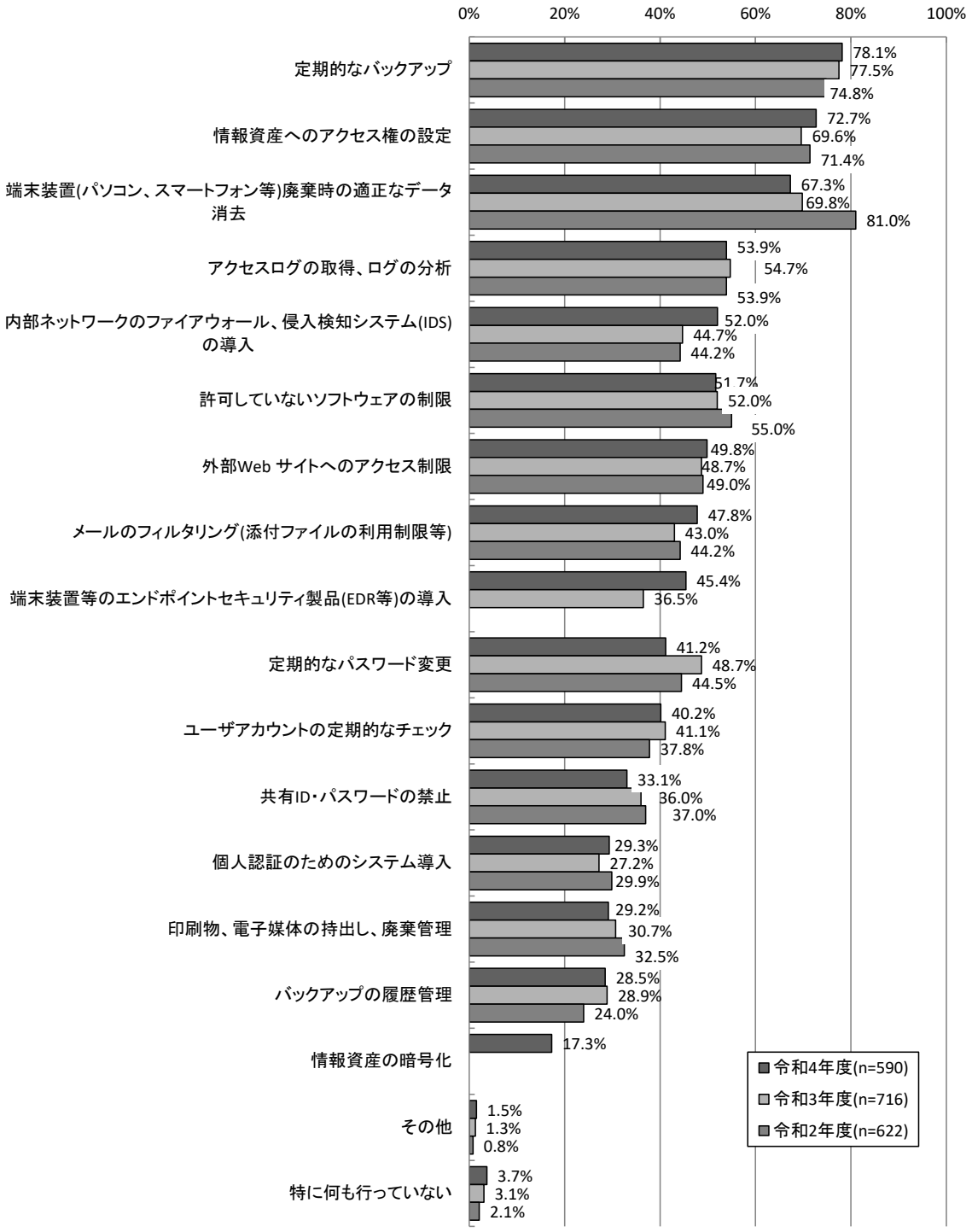


アクセスログの取得、ログの分析



【経年変化】昨年度と比較すると、「端末装置等のエンドポイントセキュリティ製品(EDR 等)の導入」が 8.9 ポイント、「内部ネットワークのファイアウォール、侵入検知システム(IDS)の導入」が 7.3 ポイント、「メールのフィルタリング(添付ファイルの利用制限等)」が 4.8 ポイント減少している。一方、「定期的なパスワード変更」が 7.5 ポイント減少している。

【経年変化】不正アクセス等への対策状況

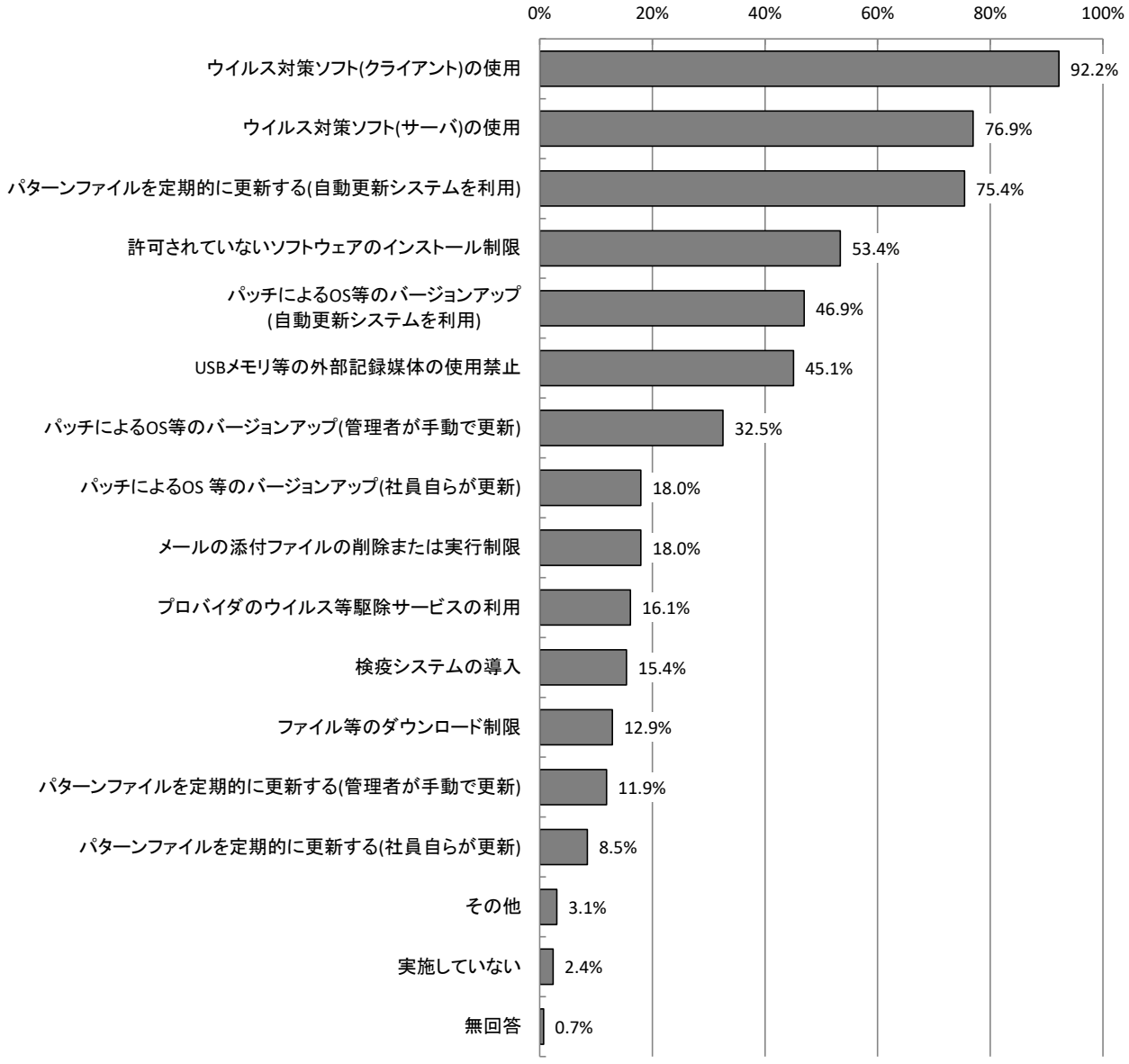


※令和３年度調査で、「端末装置等のエンドポイントセキュリティ製品（EDR等）の導入」を新設。
※令和４年度調査で、「情報資産の暗号化」を新設。

3.2.23　不正プログラムへの対策状況　【問28】

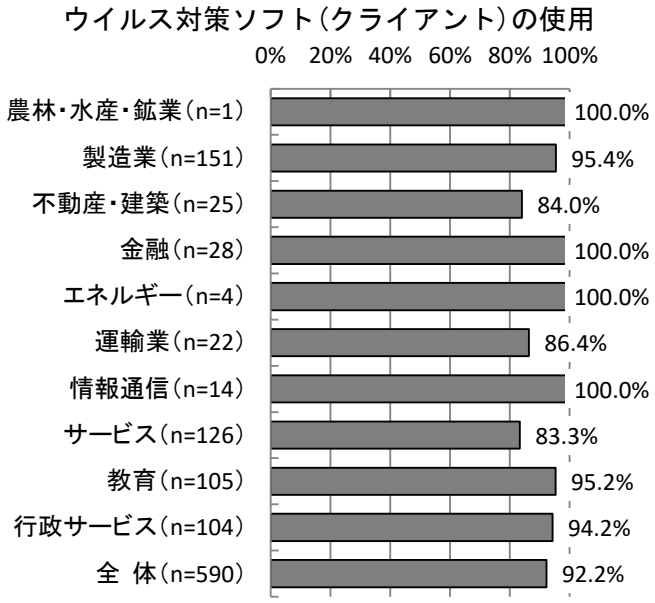
不正プログラムへの対策状況については、「ウイルス対策ソフト（クライアント）の使用」が92.2%で最も高く、次いで「ウイルス対策ソフト（サーバ）の使用」が76.9%、「パターンファイルを定期的に更新する（自動更新システムを利用）」が75.4%となっている。

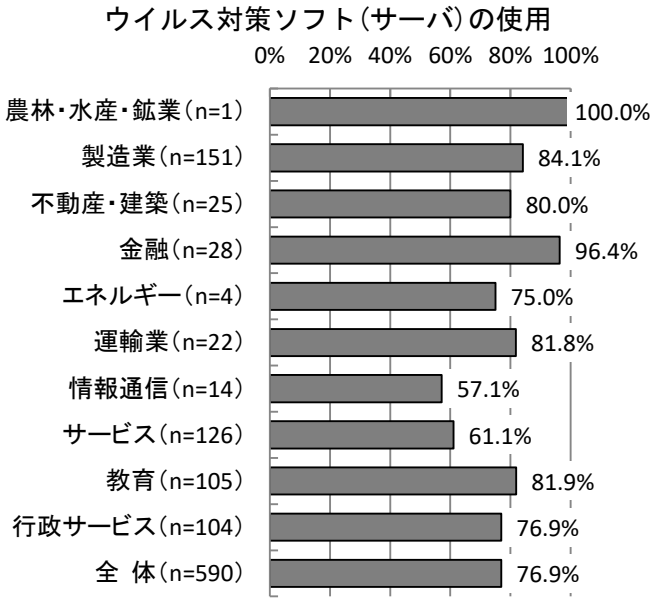
【全体】不正プログラムへの対策状況（MA, n=590

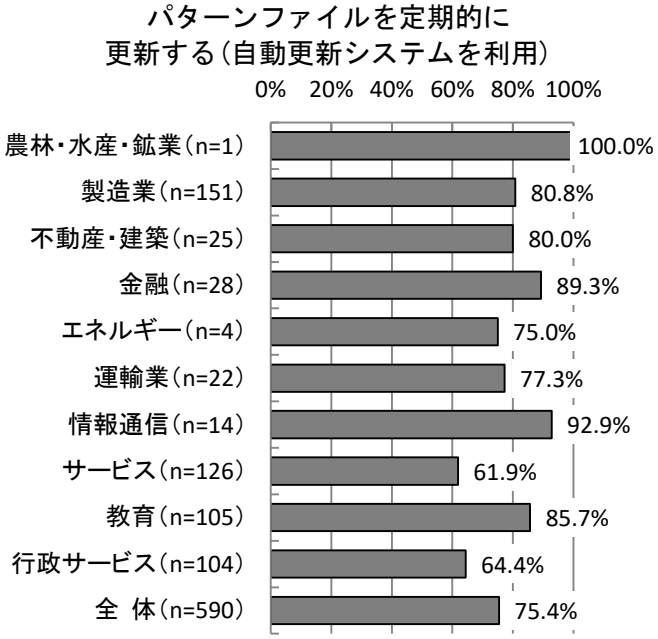


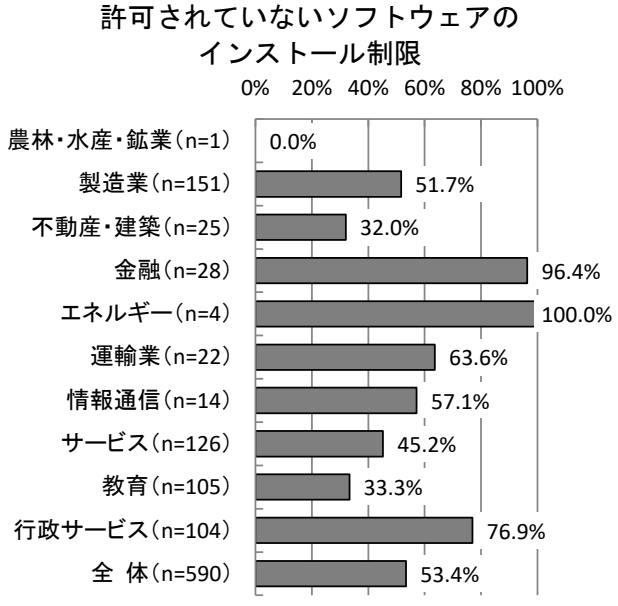
【業種別分析】業種別にみると、「ウイルス対策ソフト（クライアント）の使用」については、いずれも8割以上と高くなっている。「ウィルス対策ソフト（サーバ）の使用」については、「情報通信」「サービス」以外の業種でそれぞれの項目が7割を超えている。また、「パターンファイルの定期的な更新」については、「情報通信」が92.9%、「金融」が89.3%、で高くなっている。

【業種別分析】不正プログラムへの対策状況







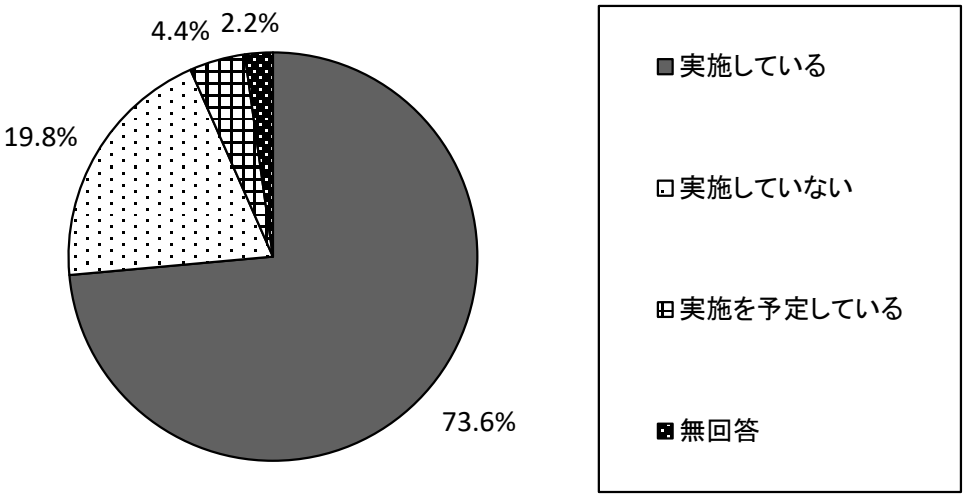


3.3 人的対策

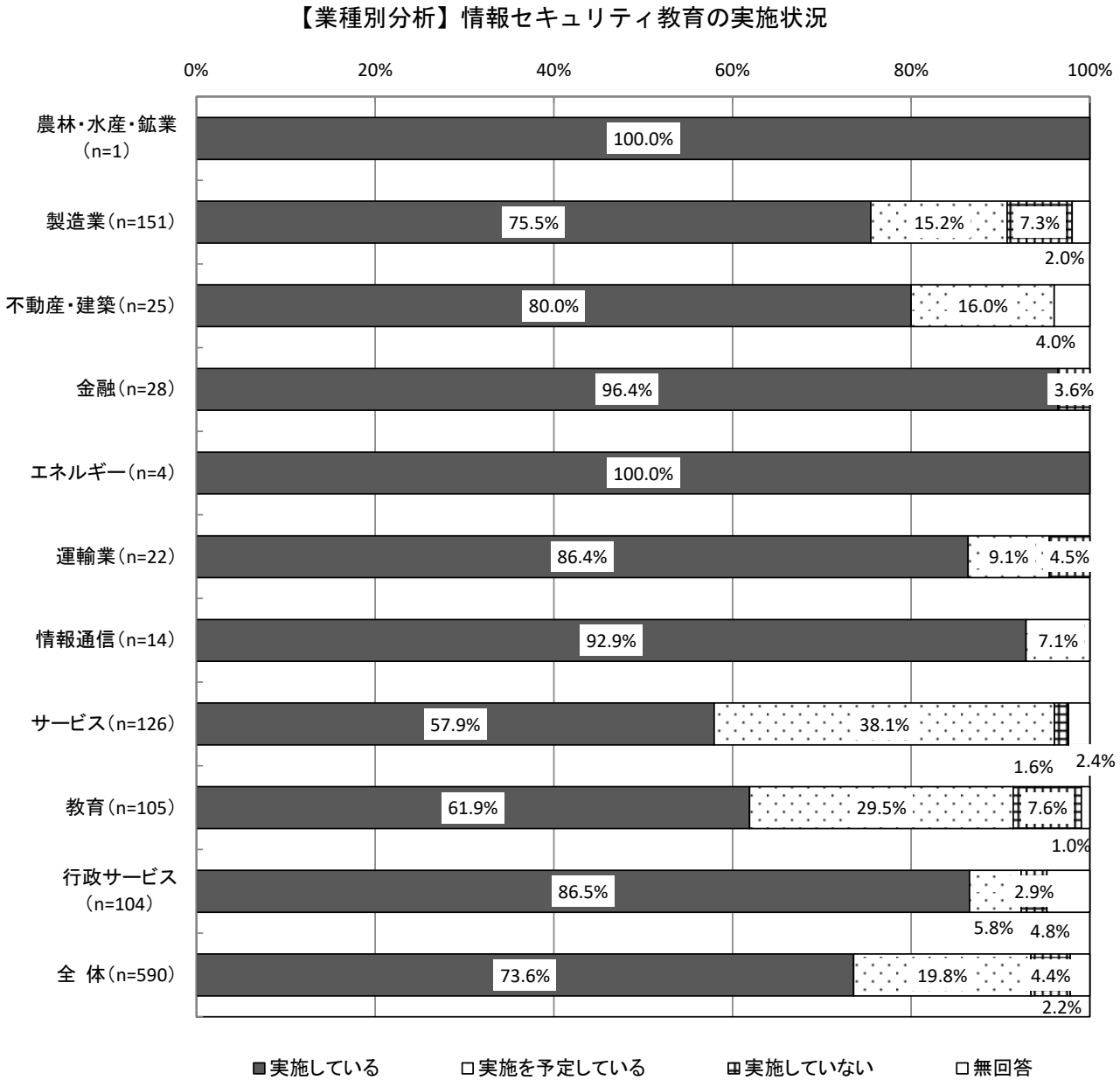
3.3.1 情報セキュリティ教育の実施状況 【問29】

情報セキュリティ教育の実施状況は「実施している」が73.6%、「実施していない」が19.8%、「実施を予定している」が4.4%となっている。

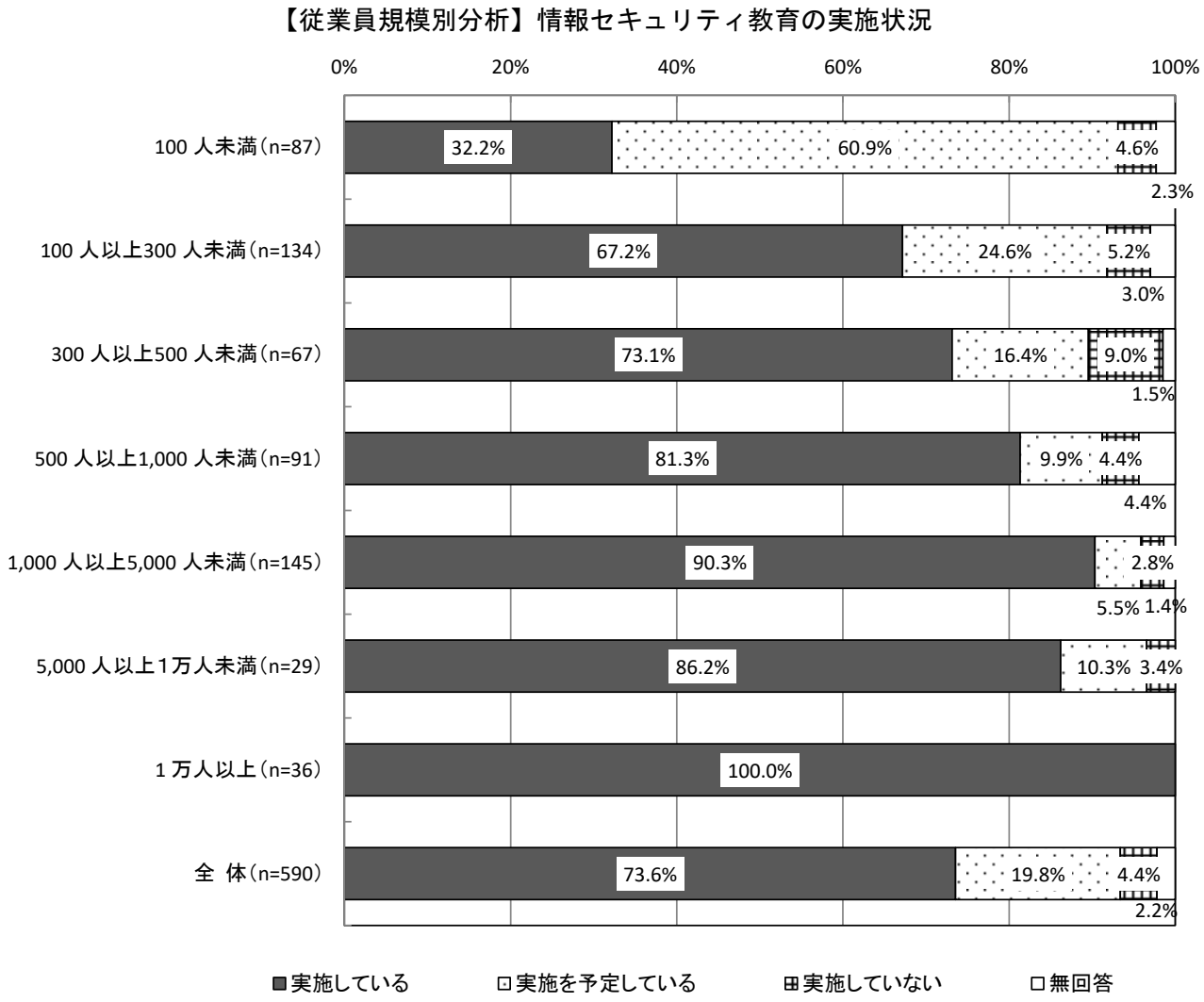
【全体】情報セキュリティ教育の実施状況（SA,n=590）



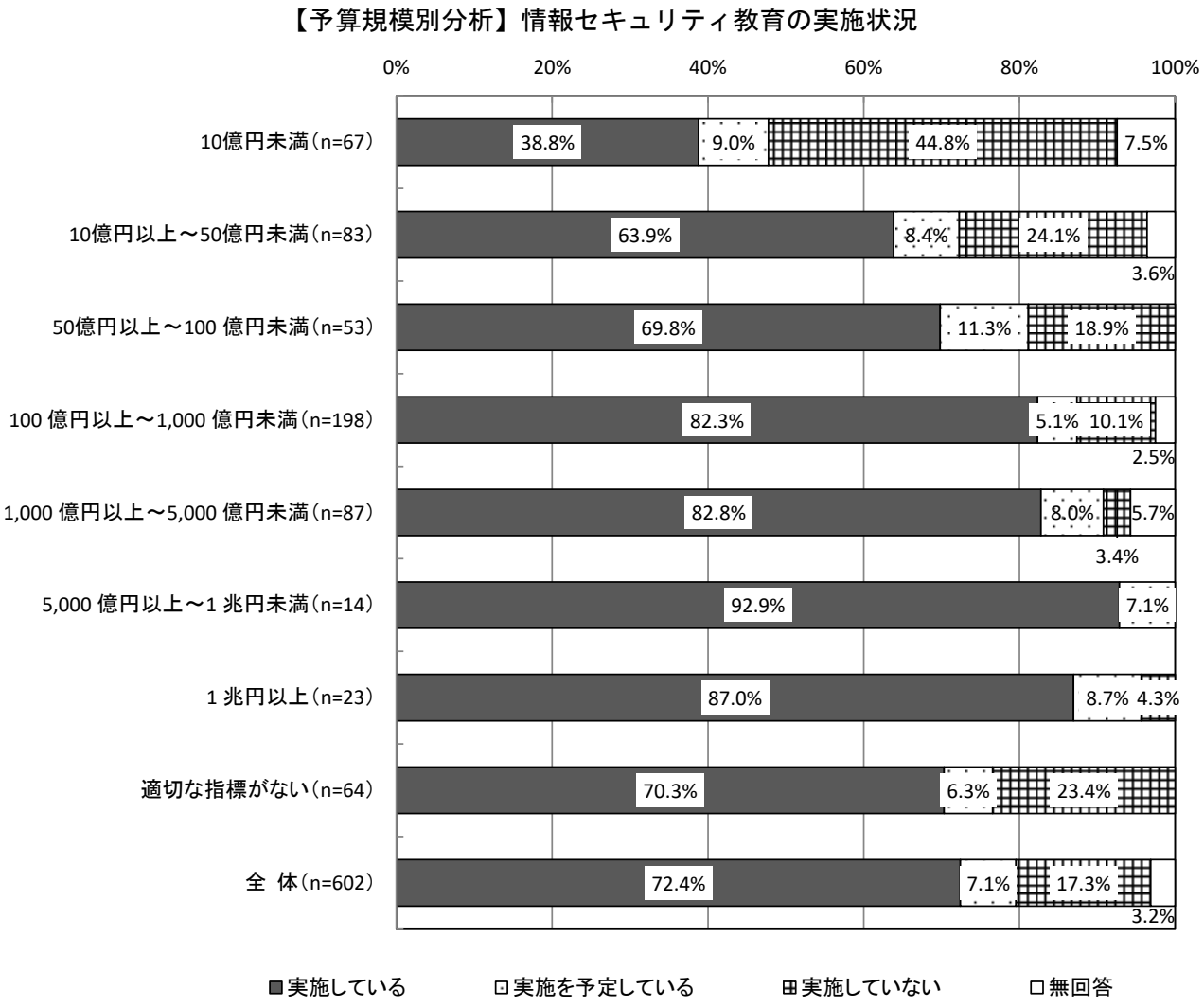
【業種別分析】業種別にみると、「実施している」については、「金融」が96.4%、「情報通信」が92.9%となっている。一方、「実施していない」は「サービス」で38.1%、「教育」が29.5%となっている。



【従業員規模別分析】従業員規模別にみると、「実施している」については、概ね従業員規模が大きくなるにつれて多くなる傾向にあり、「１万人以上」で100.0%となっている。



【予算規模別分析】予算規模別にみると、「実施している」については「10億円未満」では38.8%だが、概ね予算規模が大きくなるにつれて多くなる傾向にある。

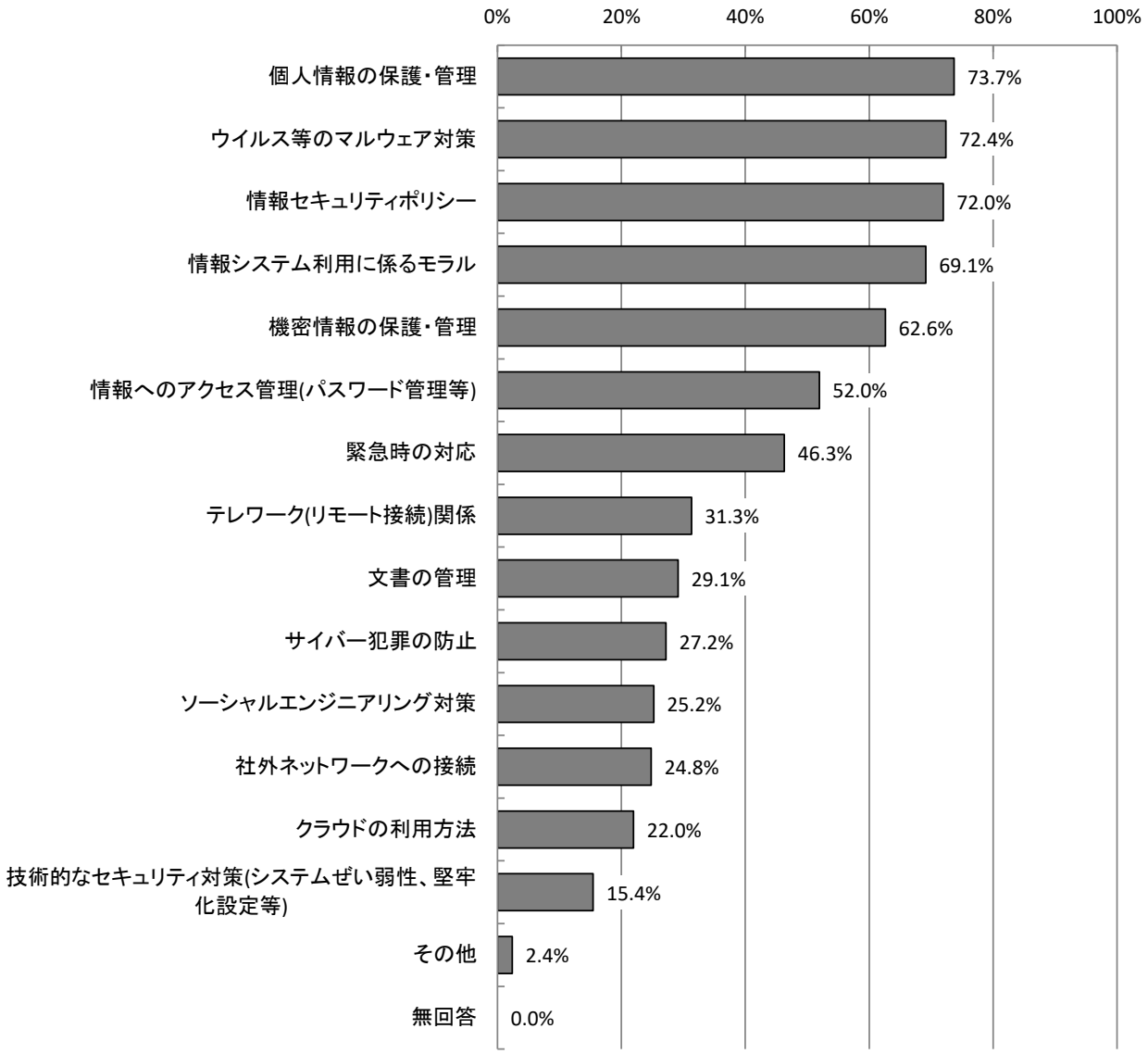


3.3.2　情報セキュリティ教育の内容　【問29-1】

情報セキュリティ教育の内容については、「個人情報の保護・管理」が73.7%、「ウイルス等のマルウェア対策」が72.4%、「情報セキュリティポリシー」が72.0%で高くなっている。

※本項目は、情報セキュリティ教育を行っている社・団体等を対象としている。

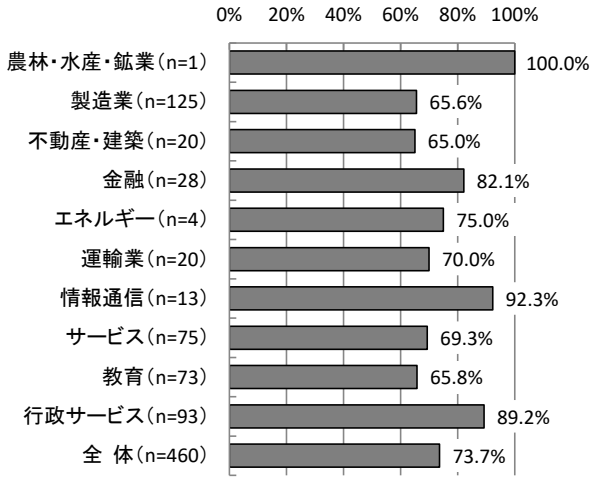
【全体】情報セキュリティ教育の内容（MA, n=460）



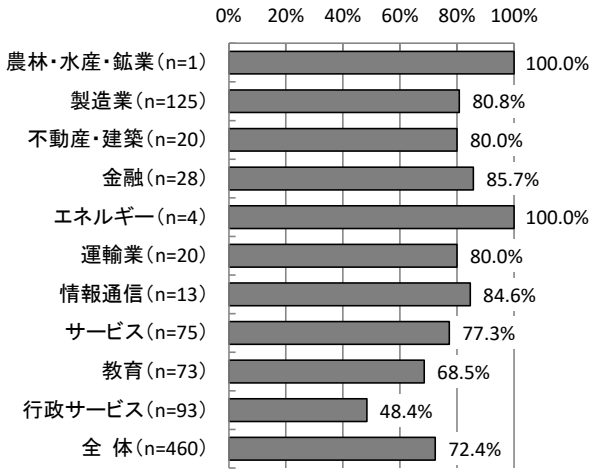
【業種別分析】業種別にみると、「個人情報の保護・管理」は、「情報通信」が92.3%、「行政サービス」が89.2%と高くなっている。「ウイルス等のマルウェア対策」は「金融」が85.7%、「情報通信」が84.6%で高い。「情報セキュリティポリシー」については、「サービス」が82.7%で高くなっている。

【業種別分析】情報セキュリティ教育の内容

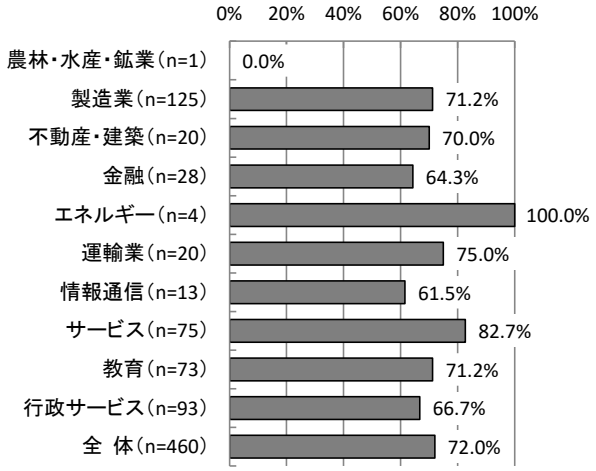
個人情報の保護・管理



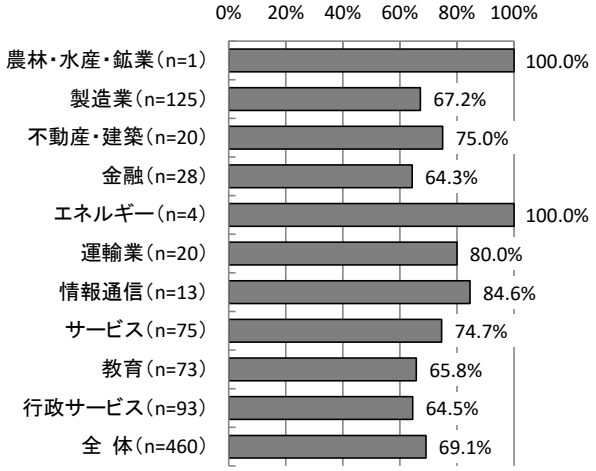
ウイルス等のマルウェア対策

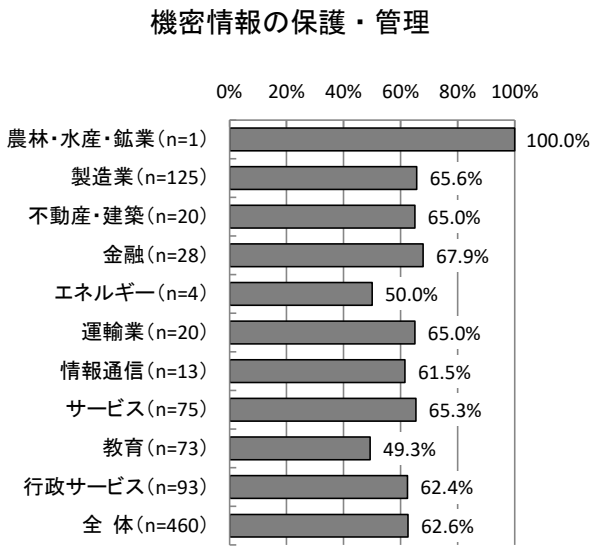


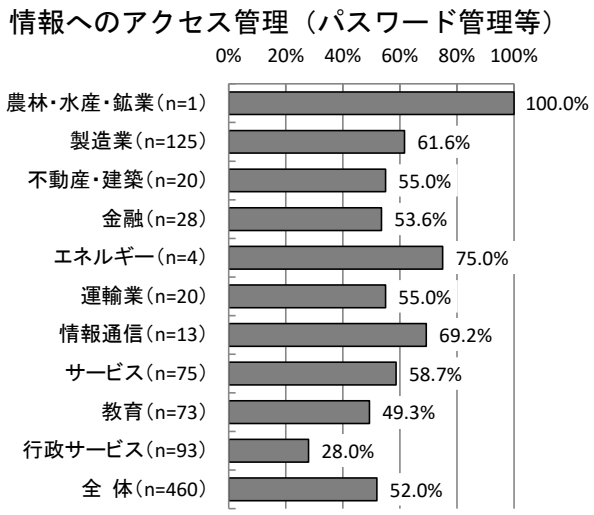
情報セキュリティポリシー



情報システム利用に係るモラル



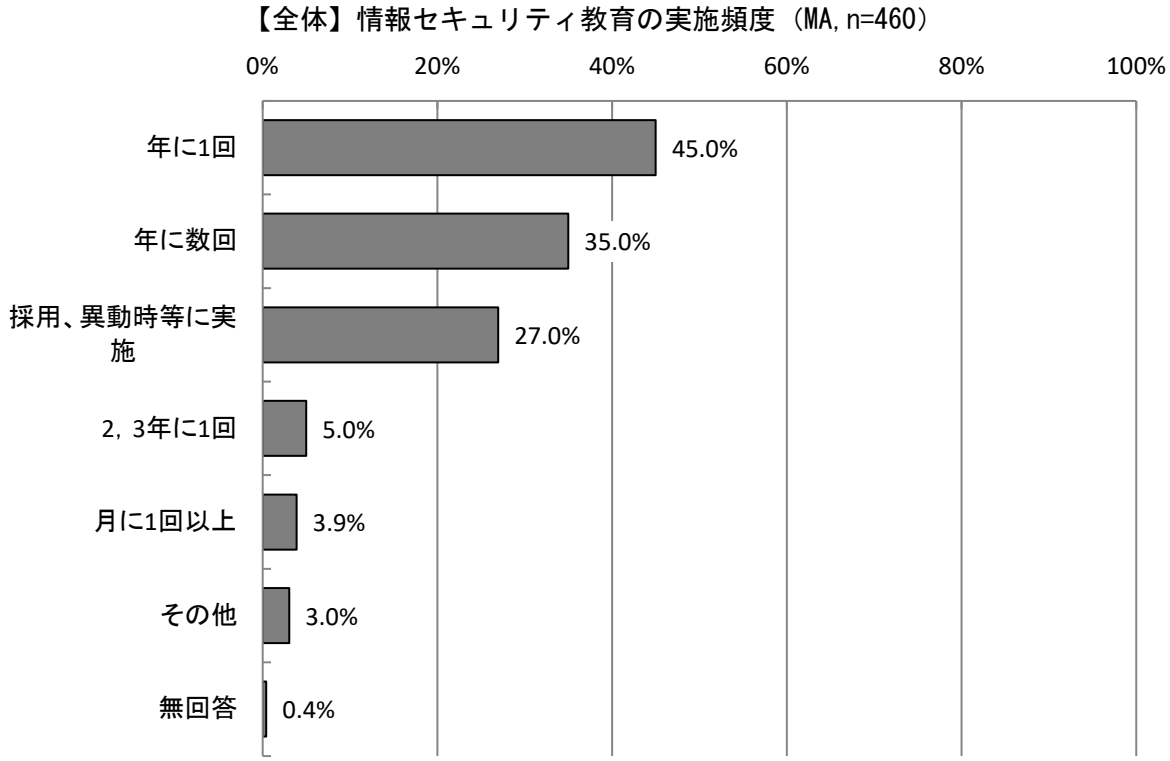




3.3.3 情報セキュリティ教育の頻度 【問29-2】

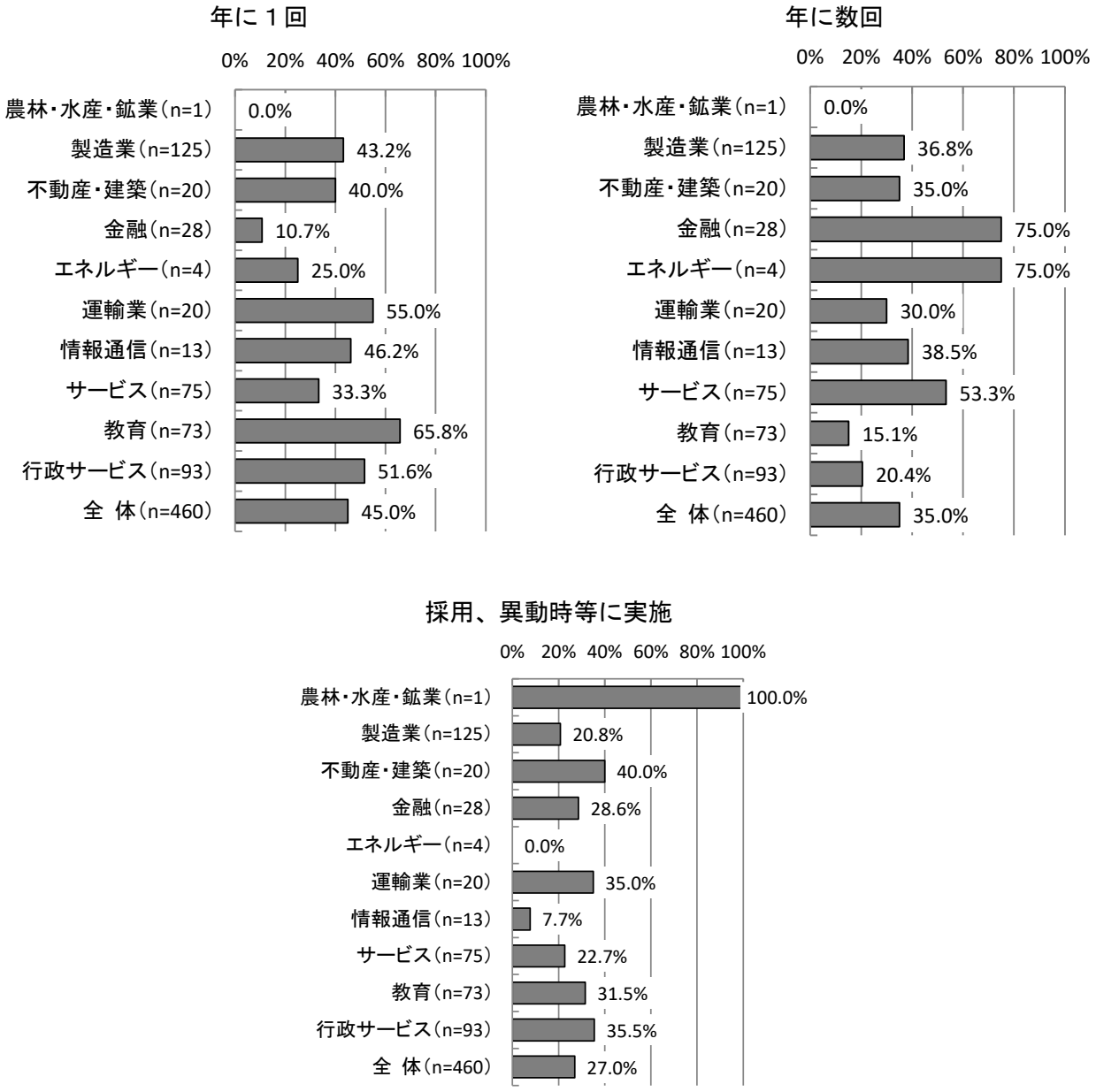
情報セキュリティ教育の頻度については、「年に１回」が45.0％で最も高く、次いで「年に数回」が35.0％、「採用、異動時等に実施」が27.0％となっている。

※本項目は、情報セキュリティ教育を行っている社・団体等を対象としている。



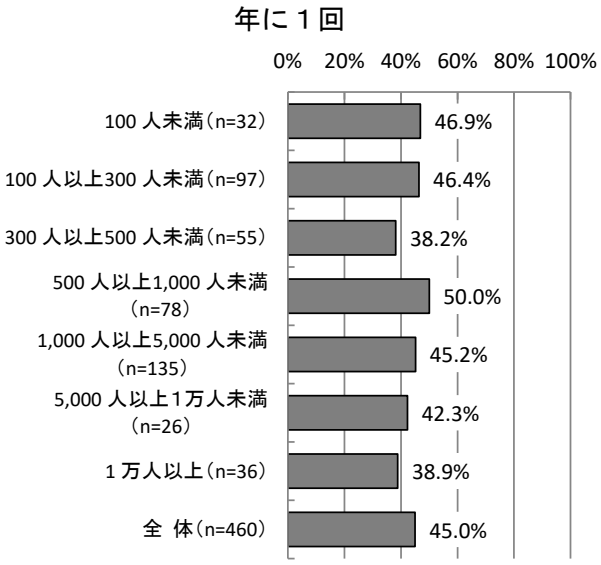
【業種別分析】業種別にみると、「年に１回」については、「教育」が65.8%で最も多く、「年に数回」については、「金融」が75.0%となっている。「採用、異動時等に実施」については、「不動産・建築」で40.0%となっている。

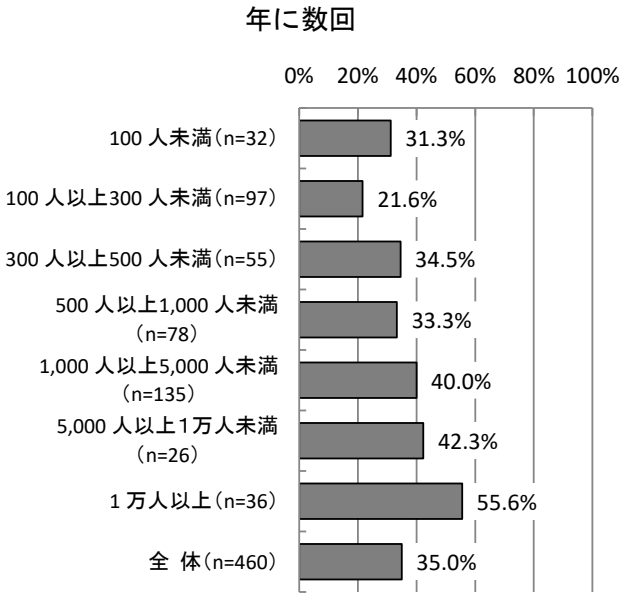
【業種別分析】情報セキュリティ教育の実施頻度

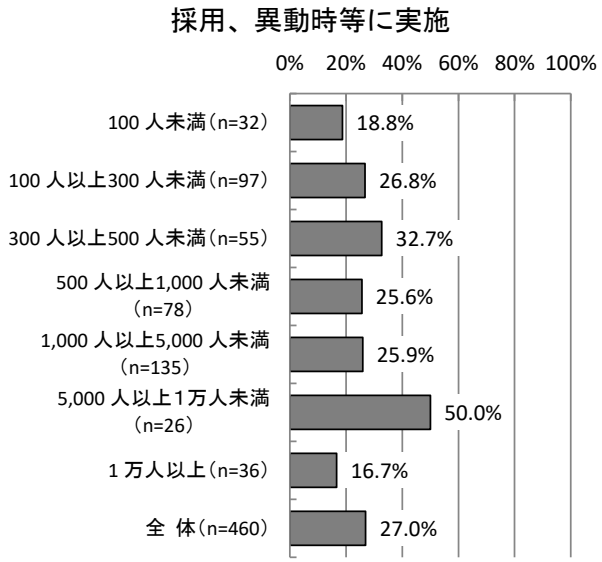


【従業員規模別分析】従業員規模別にみると、「年に１回」については「500人以上1,000人未満」が50.0%、「年に数回」については、「１万人以上」が55.6%と最も多くなっている。

【従業員規模別分析】情報セキュリティ教育の実施頻度





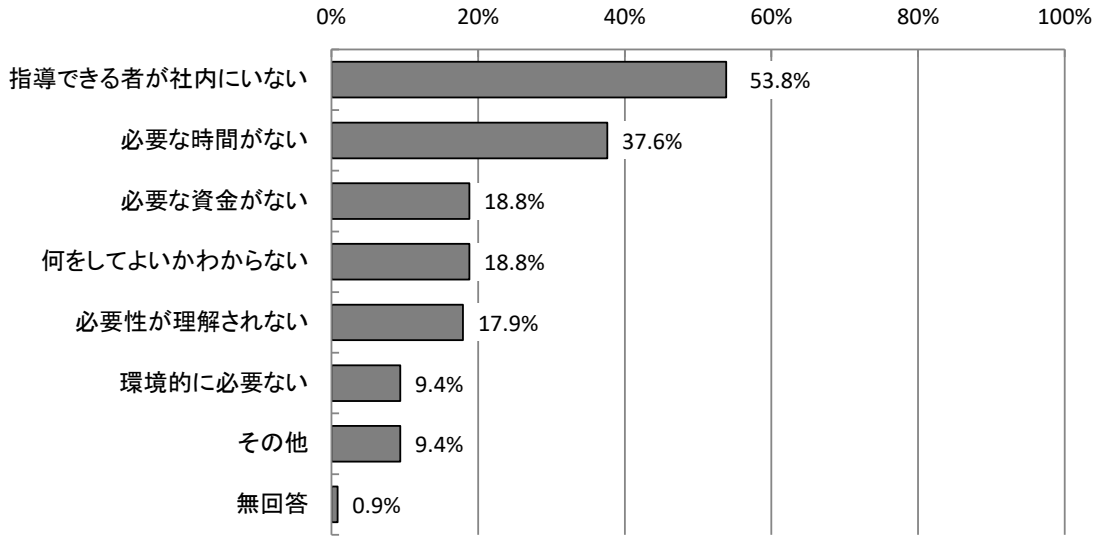


3.3.4　情報セキュリティ教育を実施しない理由　【問29-3】

情報セキュリティ教育を実施しない理由については、「指導できる者が社内にいない」が53.8%で最も多く、次いで「必要な時間がない」が37.6%となっている。

※本項目は、情報セキュリティ教育を実施していない社・団体等を対象としている。

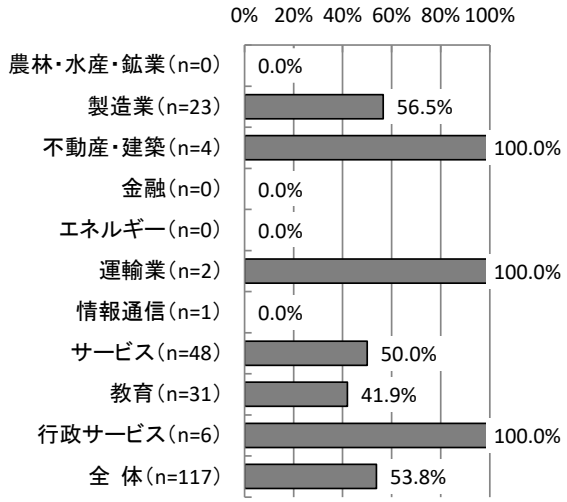
【全体】情報セキュリティ教育を実施しない理由（MA, n=117）



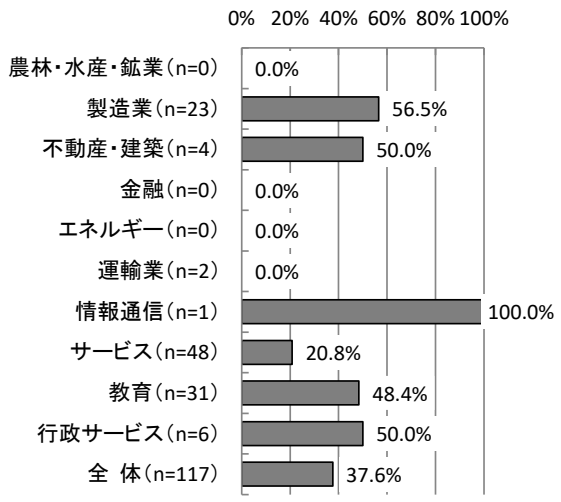
【業種別分析】業種別にみると、「指導できる者が社内にいない」は、「行政サービス」で100.0%、「必要な時間がない」は、「製造業」で56.5%と高くなっている。

【業種別分析】情報セキュリティ教育を実施しない理由

指導できる者が社内にいない



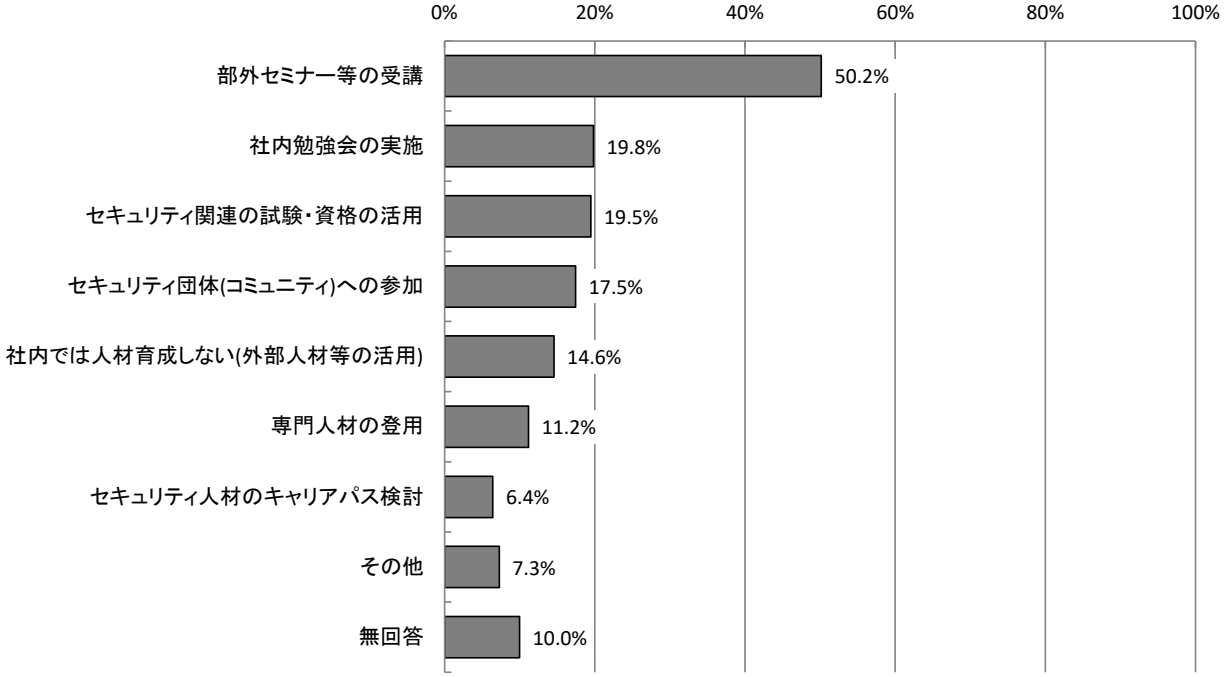
必要な時間がない



3.3.5　セキュリティ人材を確保するための施策　【問30】

セキュリティ人材を確保するための施策は「部外セミナー等の受講」が50.2%で最も高く、次いで「社内勉強会の実施」が19.8%、セキュリティ関連の試験・資格の活用」が19.5%となっている。

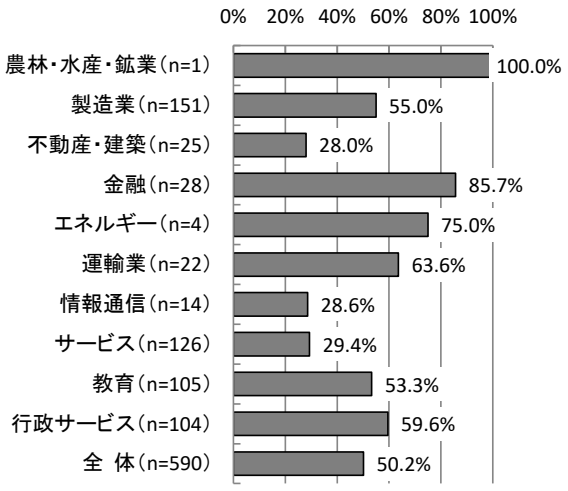
【全体】セキュリティ人材を確保するための施策（MA, n=590）



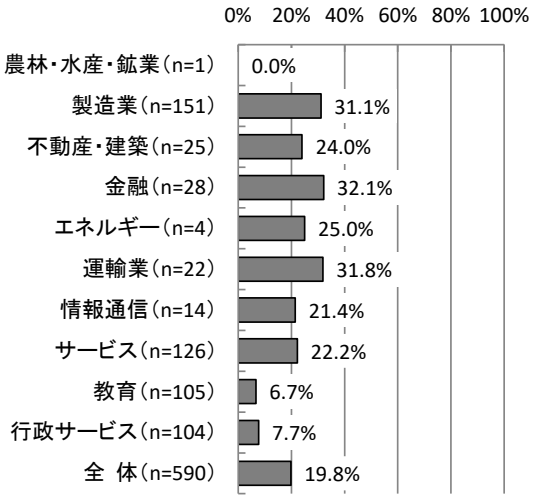
【業種別分析】業種別にみると、「部外セミナー等の受講」は、「金融」が85.7%で高い。「社内勉強会」の実施は、「金融」で32.1%、「運輸業」で31.8%、「製造業」で31.1%と高くなっている。

【業種別分析】セキュリティ人材を確保するための施策

部外セミナー等の受講



社内勉強会の実施



3.3.6 セキュリティ対策の問題点や不安等

１．組織的対策

- セキュリティ上限の妥協ポイント。費用と対策の限界値の見極め
- 情報セキュリティについて今後数年かけて対策、体制、方針、教育を目指す計画ですが、CISOもCIOも不在の組織においてガバナンスを効かせられるのか、個人的に危惧している所です。
- インシデント発生時に、すぐ相談、対応出来る窓口が欲しい
- 大学開設後約10年、外部委託してきて、セキュリティ対策はうまく回っており、不正アクセス等はありません。
- あまりにも企業に対する負担が大きい。まったく同じような対策を全企業が行なうのは効率が悪すぎると感じます。
- セキュリティやITリテラシーに関して、知識と意識にレベル差があり、社員教育に苦労している。個人（自身のスマホやPC）は自分事だが、会社は他人事としているのも問題。役員（経営陣）の意識も低い。セキュリティソフト（2重）ネットワーク防御など費用や人材を割く増加しており、以前より会社の経費も上っている。
- どこに対して優先的に投資していくべきかは専門のITベンダーによる診断で明確にすることができた。そうした取組みがないと社内を説得することが難しいと感じる。
- 会社の規模に合った、対策が不明で、どこまで実施したらよいかわからない。
- セキュリティをちゃんとしたいけど費用面技術面でむずかしい
- ITベースで業務をしている一方、あってあたり前、使えて当たり前で、保守、運用にコストを投資しようという経営判断をしない経営層が多い。法令で規制、厳格に適用、罰則を与えるようにしないと、IT統制の普遍化と浸透は不可能。デジタル社会は、社会全体に共通化･普遍化されたIT統制を実現した上で展開しないと、犯罪の横行、産業に限らずスパイの跳梁跋扈を招くだけだ。
- コメント①リアルな世界では国境という概念があり、自衛隊、海上保安庁、入国管理局、警察など持ち場持ち場で対応していただいていることから、企業は一個人も安全･安心にビジネスや社会生活ができています。しかしサイバーセキュリティの世界では国境がなく、愉快犯、犯罪組織、国家が関与するサイバー軍などとも一企業が対峙しなければならない環境となっており、圧倒的に不利な状況になります。そのため、企業と警察がもっと密に連絡とりながら、上記攻撃者を検挙、TakeDownさせることが必要だと感じています。政府の「遺憾表明」だけではなんら変わらないと思います。法改正含めて簡単ではない事は承知していますが、今から動かなければ、手遅れになります。また、民間では業界ISACを越えての産業横断的な活動やサプライチェーン連携も始まっています。官民で連携して、実効性のあるサイバーディフェンス、集団防衛能力の向上を一緒に目指せればと思います。ご検討お願いします。●コメント②もし可能でしたら、今後は紙ベースでなくWEBベースのアンケートにして頂けますと幸いです。(リモートワークの為、書面だと対応に遅れる可能性があるため)またその際は警察庁様からの依頼と明確に分かるようにして頂ければと思います。(アンケート自体の信ぴょう性の確認が必要なため)
- 日本のセキュリティ管理は企業まかせとなっている。国家が率先して対策をしないため野ばなしである。法的整備をすすめ、ウィルス･フィッシング等のメールは除却してほしい。
- 予算の確保が困難。･どこまで対策すれば良いかのゴールが不明確。
- セキュリティは出来るだけ強化したと考えていますが、費用対効果を会社へ説明しにくく、政府推奨または法整備による、明確な基準が指し示されれば導入しやすくなると思います。
- 海外拠点を含むグループ全体の情報セキュリティ対策水準を揃えて上げることが課題

２．技術的対策

- どこまでセキュリティ対策を実施すればよいかゴールが見えない
- 各種団体などから啓発文書、ガイドが多数公表されているが、情報の洪水が起きている。方行性としては良いが、整理できないものか、煽られても、状況は進展しにくいものである。
- ランサムウェアの脅威が不安。
- CSIRTのようなきっちりとした体制までは組めていない。EDR+SOCを導入し、少し安信感は増したが、仮にインシデントが発生したら迅速に対応できる体制を早く構築しなければならないと考えている。
- 困難に感じる点は、情報セキュリティ対策と年々高度化するサイバー攻撃は一進一退を繰り返し、そこに世界情勢も絡み自社の対応が遅れているのか、それとも十分なのか指標がない事。
- ローカルのパソコンにウイルス対策ソフトを入れファイアウォールを導入しているが機能しているかまた、被害にあっているのかが分からない(見えない)
- 国外を含めたグループ会社のサイバーセキュリティガバナンス、サイバーセキュリティ対策、教育研修の一元的なコントロールが遅れている。サイバーセキュリティに係る予算･人材が十分でないグループ会社がある。
- セキュリティ対策のサービスやツールの調達コストが年々上昇していると感じる。
- 日進月歩で終わりがないこと。アンケートの調査方法としてフォーム形式を希望します。

- 当医院で扱うデータは2種類。一つはエックス線画像データ、もう一つはレセプト請求用データ。画像データはインターネットに接続しない院内無線LANで共有している。レセプトコンピュータ用ソフトはインターネットを介して定期的にバージョンアップし、日々のレセプトデータは診療終了時にクラウド上に保存している。メールおよびインターネットのセキュリティは市販のウイルスソフトを使用している。

３．人的対策

- ユーザーリテラシーの低さ、担当部署の人員不足
- セキュリティと利便性は相反するもので、セキュリティを高めると利便性が落ちるわけですが、ユーザは利便性重視ですので、その間に立って情報セキュリティ対策を進める事に困難を感じています。
- 最新のセキュリティリスクへの対策･セキュリティ人材の確保
- 情報セキュリティの人材が不足している(外部も含めて)。情報セキュリティの対策費用が不足している
- セキュリティインシデントが発生した際のコストとそれを起こさないために必要なコストのバランスがとれていない　情報部門以外では未だセキュリティリスクに対する根本的な危機感が低いと常に感じている※本庁のみではなく他業種、等念め。
- 経営側で情報セキュリティの知識が少なく、ポリシー等の制定、改訂に時間がかかる。必要な対策が承認されづらい
- 技術者不足
- 人材の確保、業務過多　不正アクセスに対してはUEBAを導入。
- 高度化への対応、予算や人員の限界
- セキュリティ人材の確保。
- 市町村の職員自ら情報セキュリティ対策を実施するにはスキル、マンパワー共に不足しているため、国で調査、提供するなど支援をしていただきたい
- セキュリティに対する認識が薄い

４．その他

- なぜ電子化されないのでしょうか？アンケートの集計に多大の時間を要すと思います
- 情報セキュリティにくわしくないため質問に正しく回答できているか不明であります。申し分けありません
- なにをしたらいいかわからない。（対策）
- 大学であるため、主として教員、職員に対しての対策として回答しています。
- メールで解答ならForm等(Web)入力などになりませんか?
- メール以外のオンラインで実施させてほしい
- 警察庁として一企業にどのような対策を行ってほしいか、昨今はどのようなサイバー攻撃に気を付けるべきかなど、ご担当者の方にお話をおうかがいしてみたいです。事例の紹介もしくは機会があれば、面談などを希望いたします。
- WEB回答用フォームを用意して欲しい。
- なんでもかんでも"webで""デジタルで""ペーパーレスで"といいますが歯科医のようにアナログな世界でしか本業をできない業種もあります。ネットを使うのは業者さんとのメールのやりとりぐらいでしょうか。ご理解下さい。
- 「調査ご協力のお願い」に「ご回答をいただけていない方に個別に連絡をさせていただく」とあるが、企業、団体名の記入もなく、どのように追跡するのか、興味をもった。
- 調査項目が多く、毎年の調査となると回答作成に負担感を感じてしまいます。定期的に調査されるご予定であれば、回答をWEB入力でできるようにするなど、ご配慮いただけると助かります。
- Webで回答できるようにご検討いただけますと幸いです。
- Webのアンケートフォームで頂けると助かります。
- 調査に関して、ウェブ上に回答フォームがあれば、より回答しやすかった。
- 紙やメールでの提出ではなく、専用回答入力サイトがあるとよい。
- 回答が遅くなり、大変申し訳ございません。
- 調査項目が多い。また、電子データによる回答が可能とあったが、エクセル等で「○」を選ぶような形式ではなく、ワードで作成されているため、回答しづらいと感じた。

不正アクセス行為対策等の実態調査　付録資料

付録１：調査票
付録２：集計表

付録１

１． 組織的対策

【貴社・団体について伺います】

問１． 貴社・団体は、どの業種に該当しますか。（○は一つ）

業種分類	業種			
農林・水産・鉱業	1.農林・水産	2.鉱業	3. その他（ ）	
製造業	4.食品	5.繊維	6. 紙・パルプ	7.化学
	8.薬品	9.ゴム・窯業	10.非鉄金属	11.機械
	12.電気機器	13.造船	14.輸送機器	15.精密機器
	16.その他（ ）			
不動産・建築	17.不動産	18.建築	19.その他（ ）	
金融	20.銀行	21.証券	22.保険	23.クレジット
	24.消費者金融	25.信用金庫・組合	26.その他（ ）	
エネルギー	27.電力	28.ガス	29.水道	30.石油製造(精製)
	31.その他（ ）			
運輸業	32.鉄道・地下鉄	33.航空	34.陸運	35.海運
	36.倉庫	37.その他（ ）		
情報通信	38.新聞	39.放送	40.通信	41.ISP
	42.その他（ ）			
サービス	43.流通・卸売	44.小売	45.娯楽・アミューズメント	
	46.飲食	47.ホテル・旅行	48.情報処理・ソフトウェア	
	49.警備	50.医療・福祉	51.その他（ ）	
教育	52.大学	53.短大	54.専門学校	
	55.その他（ ）			
行政サービス	56.都道府県	57.政令指定都市	58.市町村	

（太枠線内にご回答ください）

問２． 貴社・団体の従業員は、どのくらい在籍されていますか。（○は一つ）

１．100人未満
２．100人以上300人未満
３．300人以上500人未満
４．500人以上1,000人未満
５．1,000人以上5,000人未満
６．5,000人以上１万人未満
７．1万人以上

問３． 貴社・団体の売上げ、予算の総額は、どれくらいの規模ですか。（○は一つ）

１．10億円未満
２．10億円以上～50億円未満
３．50億円以上～100億円未満
４．100億円以上～1,000億円未満
５．1,000億円以上～5,000億円未満
６．5,000億円以上～1兆円未満
７．1兆円以上
８．適切な指標がない

【情報システム等の環境について伺います】

問４．　貴社・団体支給の端末装置（パソコン、スマートフォン等）の整備環境は、どのようになっていますか。（○は一つ）

１．１人当たり１台以上
２．数人で共有
３．部・課で共有
４．事業所や拠点で共有
５．その他（　　）
６．端末装置は利用していない

問５．　貴社・団体では業務における個人所有端末装置（パソコン、スマートフォン等）の扱いをどうしていますか。（○は一つ）

１．全て許可（２及び３を許可）している
２．パソコン・タブレット（タブレットＰＣを含む）を許可している
３．スマートフォンを許可している
→ 問5-1へお進みください

４．許可していない
５．把握していない
→ 問６へお進みください

問5-1.　問５で個人所有端末装置の使用を許可している（１～３）と回答された方に伺います。個人所有端末装置のセキュリティ対策（ウイルス対策ソフトの導入など）を義務づけていますか。（○は一つ）

１．義務づけている
２．義務づけていない

問６．　昨今の新型コロナウイルス感染拡大防止策等により、テレワーク業務が急激に普及していますが、貴社・団体においてテレワークを行っていますか。（○は一つ）

１．行っている → 問6-1～6-2へお進みください
２．行っていない → 問6-3へお進みください

問6-1.　問６で「１．行っている」と回答された方に伺います。いつ頃からテレワークを行っていますか。（○は一つ）

１．新型コロナウイルス感染対策に伴い開始した
２．貴社・団体の業務の運用として、以前から行っていた
３　その他（　　）

問6-2.　問６で「１．行っている」と回答された方に伺います。テレワーク業務を行う際の端末装置（パソコン、スマートフォン等）の利用環境はどのようになっていますか。（○は一つ）

１．貴社・団体支給の端末装置のみ利用
２．個人所有端末装置のみ利用
３．貴社・団体支給及び個人所有端末装置のどちらでも利用可能
４．端末装置を利用しない

問6-3.　問６で「２.行っていない」と回答された方に伺います。テレワークを行っていない理由はなぜですか。（○はいくつでも）

１．行う必要がない
２．業務の特性上行えない
３．以前行っていたがやめた（必要性がなくなった）
４．以前行っていたがやめた（セキュリティ上の問題でやめた）
５．技術不足のためできない
６．資金不足のためできない
７．ルール作りや教育ができない
８．今後導入を計画している
９．その他（　　）

問７．　貴社・団体内LANには、有線、無線のいずれかのネットワークを利用していますか。（○は一つ）

１．有線ネットワークと無線ネットワークを併用
２．全て無線ネットワークで構築
３．全て有線ネットワークで構築
４．LANを敷設していない

問８．　クラウドサービスを利用していますか。（○は一つ）

１．利用している　　２．利用していない　　３．わからない

問９．　外部から内部ネットワークへの接続を許可していますか。（○は一つ）

１．許可している　　２．許可していない

【情報セキュリティの運用・管理体制について伺います】

問10.　情報セキュリティ対策の必要性を感じるのは、どのような理由からですか。（○はいくつでも）

１．過去1年間に不正アクセス等の攻撃・被害にあったため　→ 問10-1～10-5へお進みください

２．ウイルス等のマルウェアの感染を防ぐため

３．DDoS 攻撃等によるシステムダウンを防ぐため

４．システムの乗っ取り等により犯罪等へ悪用されるのを防ぐため

５．顧客等との取引を万全なものとするため

６．インターネット上に顧客情報等の部内情報が漏れるのを防ぐため　問11へお進みください

７．セキュリティ事故がブランドイメージや業績に与える影響を避けるため

８．事業を行う上で必要不可欠なため

９．顧客等から要請があるため

10. 社会情勢や国際的行事等から、攻撃が増えることが予想されるため

11. 新型コロナウイルス感染対策として

12. 不正アクセスの加害者にならないため

13. その他（　　）

問10-1.　過去1年間に攻撃・被害を受けられた方にお伺いします。それは、どのような被害であり、また、攻撃手段
でしたか。（○はいくつでも）

【→被害は？】

１．ホームページの改ざん

２．システム損壊等による業務妨害

３．ウイルスによる情報流出

４．ウイルス以外の情報流出

５．ネットワーク利用詐欺

６．偽サイト等模倣サイトの開設

７．フィッシングサイトの開設

８．電子メールの不正中継（不正送信）

９．Web 等での誹謗・中傷被害

10. 端末機器（パソコン、スマートフォン等）の盗難

11. 外部記録媒体の盗難

12. インターネットバンキング不正送金

13. ランサムウェア

14. その他データ盗用（キーロガー含）

15. その他（　　）

16. 実質的な被害はなかった

【→攻撃手段は？】

１．DDoS 攻撃

２．踏み台（バックドア設置等）

３．部外からの不正アクセス

４．ウイルス等の感染

５．システム損壊、データ改ざん

６．内部の者のネットワーク悪用

７．関連会社や取引先等を経由

８．不明

９．不正なメール（フィッシング含む）

10. その他（　　）

問10-2.　過去1年間に攻撃・被害を受けられた方にお伺いします。攻撃・被害を受けた結果、関連会社や取引先等に
被害を与えてしまったことはありますか。与えてしまった場合はどのような被害を与えてしまいましたか。（○は一つ）

１．与えてしまった（　　）

２．与えていない

問10-3.　過去１年間に攻撃・被害を受けられた方にお伺いします。攻撃・被害を受けた結果、実際に講じられた
対応策はどういったものですか。（○はいくつでも）

1．ファイアウォールの設置・強化
2．ウイルス等対策製品の導入・強化
3．最新パッチの適用
4．ソフトウェアのバージョンアップ
5．認証機能の導入・強化
6．ネットワークの再構築
7．不必要なサービスの停止
8．セキュリティポリシーの策定・見直し
9．セキュリティ教育の実施・強化
10．不正アクセスが行われていないかどうかネットワークの監視
11．クラウド等の外部セキュリティサービスの利用
12．システム上にセキュリティホールがないかどうか検査、診断
13．セキュリティコンサルティングの利用
14．セキュリティ監査の実施
15．弁護士への相談
16．関連会社や取引先等に対応するよう求めた
17．クラウドの設定を見直した
18．不明
19．その他（　　）
20．特に何も対策を講じていない

問10-4.　過去1年間に攻撃・被害を受けられた方にお伺いします。どこに届出・相談をなされましたか。また、その理由は何ですか。（○はいくつでも）

〈届出・相談先機関等〉

1．警察
2．IPA（情報処理推進機構）
3．JPCERT/CC
4．国民生活センター・消費生活センター
5．監督官庁
6．個人情報保護委員会
7．その他（　　）
8．届け出なかった　→ 問10-5へお進みください

〈届出・相談した理由〉へお進みください

〈届出・相談した理由〉

1．届出義務があるため
2．事案解決を求めて
3．被害拡大を阻止するため
4．関係者（株主等）への説明責任を果たすため
5．報道されたため
6．情報セキュリティ事業者からの意見により
7．法律職（弁護士等）からの意見により
8．解決方法を知るため
9．行政機関からの指導により
10．利用者からの指摘により
11．その他（　　）

問10-5.　過去1年間に攻撃・被害を受けられたが、届け出なかった方にお伺いします。届出・相談を躊躇させる要因としては、どういったことがあげられますか。（○はいくつでも）

1．自社・団体の信用が低下するので
2．社・団体内で対応できたので
3．届出義務がないので
4．自社内だけの被害だったので
5．実質的な被害が無かったので
6．問題解決にならないので
7．面倒なので
8．競合他社に知られたくないので
9．届出するべきなのかわからなかった
10．どこに届ければいいかわからなかった
11．関連会社や取引先等が届け出たため
12．その他（　　）

問11.　不正アクセス等の攻撃・被害に遭われた場合の届出先を知っていますか。それはどこですか。（○は一つ）

1．具体的な届出先（　　）
2．わからない

問12.　不正アクセス禁止法では第８条において、アクセス管理者による防御措置について《努力義務》が規定されていますが、そのことを知っておられましたか。（○は一つ）

１．知っている　　２．知らなかった

問13.　情報セキュリティ対策を行っていますか。（○は一つ）

１．行っている　→ 問13-1～13-7へお進みください

２．行っていない又は把握していない　→ 問13-8へお進みください

問13-1.　問13で「１．行っている」と回答された方に伺います。情報セキュリティに関して、その運用、管理を専門に行う部署はありますか。（○は一つ）

１．ある　　２．ない　　３．今後設置予定

問13-2.　問13で「１．行っている」と回答された方に伺います。情報セキュリティに関する管理体制は、どのようになっていますか。（○はいくつでも）

１．情報セキュリティ担当役員（CISO 等）を設置
２．専従の担当者を設置
３．情報システム運用管理者が情報セキュリティについて兼務
４．情報システム運用管理者以外の者が情報セキュリティについて兼務
５．設置していない

問13-3.　問13で「１．行っている」と回答された方に伺います。情報セキュリティポリシー等は、策定されていますか。（○は一つ）

１．策定している　→ 問13-3-1へお進みください
２．現在、策定作業中である
３．今後、策定する予定である。
４．今のところ、策定する予定はない
５．策定しない
６．非公開情報のため、答えられない

→ 問13-4へお進みください

問13-3-1.　問13-3で「１．策定している」と回答された方に伺います。新型コロナウイルス感染対策又はテレワーク業務の開始により、情報セキュリティポリシー等を変更しましたか。（○は一つ）

１．変更した
２．変更していない
３．変更することを検討している
４．その他（　　）

問13-4.　問13で「１．行っている」と回答された方に伺います。不正アクセス等の侵害事案が発生した場合のために、現在、対応マニュアルや要領等を策定しておられますか。（○は一つ）

１．策定している
２．策定していないが、策定作業中
３．策定することを検討
４．策定する必要はない
５．非公開情報のため、答えられない

問13-5.　問13で「１．行っている」と回答された方に伺います。情報システムのセキュリティ対策について、認証制度等を利用していますか。（○はいくつでも）

１．ISMS
２．P マーク
３．PCI DSS
４．IPA セキュリティアクション宣言（二つ星）
５．ISO 27017：クラウドセキュリティ認定
６．IEC 62443：産業セキュリティ系認定
７．その他（　　）
８．特に利用していない

問13-6.　問13で「１．行っている」と回答された方に伺います。次年期（年単位）の情報セキュリティ対策の投資総額については、今年期（年単位）と比較してどのようになりますか（未定の場合は見込みでご回答ください）。（○は一つ）

１．　増額する予定
２．　現状どおりの予定
３．　減額する予定
４．　把握していない

問13-7.　問13で「１．行っている」と回答された方に伺います。これらの経費に関しては、どういった問題点が考えられますか。（○はいくつでも）

１．コストがかかりすぎる
２．費用対効果が見えない
３．教育訓練が行き届かない
４．従業員への負担がかかりすぎる
５．対策を構築するノウハウが不足している
６．どこまで行えば良いのか基準が示されていない
７．トップの理解が得られない
８．情報を資産として考える習慣がない
９．最適なツール・サービスがない
10．特に問題はない
11．その他（　　）

問13-8.　問13で「２．行っていない又は把握していない」と回答された方に伺います。なぜ、情報セキュリティ対策を行っていませんか。（○はいくつでも）

１．どのような対策を行えば良いか分からない
２．情報セキュリティ対策の運用・管理を行う体制が確保できない
３．情報セキュリティ対策を行う予算が確保できない
４．情報セキュリティ対策を行うという概念がなかった
５．情報セキュリティ対策は各職員に任せている
６．情報セキュリティ対策は必要ないと考えている
７．把握していない
８．その他（　　）

問14.　サプライチェーンリスク対策として、関連会社や取引先に情報セキュリティ対策を求めるなど何らかの対策を行っていますか。行っている場合はどのようなことを行っていますか。（○は一つ）

１．行っている（　　）
２．行っていない

問15.　今後、どのようなことに重点をおいて、情報セキュリティ対策を行うべきだと考えておられますか。下表の各行に考え方①、②の内容を比較し、より考え方が近いものをお選びください。（○は各項目一つ）

項目	考え方①	ほぼ①の考え方と同様である	①どちらかと言えばの考え方に近い	②どちらかと言えばの考え方に近い	ほぼ②の考え方と同様である	考え方②
投資方針	セキュリティ投資は必要最低限に抑えるべきである。	1	2	3	4	来るべき問題事案に備えて、積極的に投資を行うべきである。
事後的対応と予防的対応	情報セキュリティ対策としては、問題発生に対しての応急対応や、再発防止・被害拡大防止に注力するべきである。	1	2	3	4	情報セキュリティ対策としては、リスクの検知など、予防上の対策に注力するべきである。
保険への意識	情報セキュリティ対策としては、人的・技術的な対策によりカバーできるところを対策すれば十分である。	1	2	3	4	情報セキュリティ対策としては、人的・技術的対策によりカバーすることに加え、保険によりまかなうべきである。
規制・罰則への考え方	技術以外の面での対策としては、従業員等への教育と、適切な情報提供により対策を促すことが重要である。	1	2	3	4	技術以外の面での対策としては、教育はもちろんのこと、規制・罰則などの強制力のある制度的対応を行うことが重要である。
プライバシーの考慮	職場とはいえ、従業員等のプライバシーは保護された上で、情報セキュリティ対策は行われるべきである。	1	2	3	4	職場のセキュリティ保護のためにはシステム利用状況のモニタリングなどによるプライバシー保護の制約はやむをえない。
利便性とのバランス	業務実施に負担をかけるほどのセキュリティ対策は不適当であり、利便性とのバランスを考慮すべきである。	1	2	3	4	ユーザにシステム利用上・業務上の負担を強いてでもセキュリティを守るべきである。

２． 技術的対策

【端末装置（パソコン、スマートフォン等）やサーバ機器に対するセキュリティ対策について伺います】

問16.　OS やアプリケーションのセキュリティ・パッチの適用や更新状況をお答えください。（○は一つ）

１．頻繁（１か月に１回以上）にセキュリティ関連サイトを確認し、常に最新のパッチを適用している
２．定期的（四半期～半年に１回程度）にセキュリティ関連サイトを確認し、必要なパッチを適用している
３．定期的に確認はしていないが、サーバの管理者等の裁量で適用している
４．パッチを適用していない
５．問題が発生するまでパッチは適用しない
６．わからない
７．その他（　　）

【情報セキュリティサービスの利用状況について伺います】

問17.　現在、どのようなサービスを利用されていますか。（○はいくつでも）

１．Web アプリケーション診断	11. 社外での研修による教育の実施
２．プラットフォーム診断	12. セキュリティ運用・監視
３．リスク分析	13. ウイルス等監視
４．ポリシー策定	14. セキュアシステム構築
５．セキュリティ監査	15. フォレンジックサービス
６．ログ解析	16. ペネトレーションテスト
７．パッチマネジメント	17. 緊急対応
８．ハウジングサービス	18. 損害保険（不正アクセス等対応）
９．DDoS 対策	19. その他（　　）
10. 標的型攻撃対策	20. 利用していない

→ 問18へお進みください　　→ 問17-1へお進みください

問17-1.　問17で「20. 利用していない」と回答された方に伺います。その理由は何故ですか。（○はいくつでも）

１．社・団体内に高い専門性やノウハウ、技術力があり、必要性がない
２．社・団体内の担当者だけで必要な人員が確保されているため、必要性がない
３．社・団体内にノウハウの蓄積を行いたい
４．予算がない
５．価格が見合わない
６．要求に合致するサービスが提供されていない
（求める具体的なサービス例：　　）
７．機密情報の漏えいにつながることが懸念される
８．その他（　　）

【ネットワークに対する情報セキュリティ対策について伺います】

問18.　安全なアクセス環境を維持するために、どのような対策をされていますか。（○はいくつでも）

1．ID、パスワード等による認証	9．アクセスログ収集の強化・充実
2．ファイアウォールの導入	10．クラウドサービスの利用
3．ルータによるプロトコル制御	11．外部からの接続を伴うサービス等を提供していない
4．PROXY サーバの設置	
5．侵入検知・防御システム（IDS・IPS）の導入	12．バックアップの取得
	13．常に最新のパッチを適用
6．検疫ネットワークシステムの利用	14．その他（　　）
7．非武装地帯（DMZ）の構築	15．特に行っていない

8．VPN の利用

→ 問18-1へお進みください

↓ 問19へお進みください

問18-1.　問18で「8．VPN の利用」と回答された方に伺います。VPN 機器のセキュリティ対策として、どのような対策を行っていますか。（○はいくつでも）

1．OS/ファームウェアの最新パッチを常に適用している
2．不正アクセス、ランサムウェア等の被害に遭ったのでパッチを適用した
3．報道等によりランサムウェア等の被害の原因になることを知ったのでパッチを適用した
4．VPN 機器への接続認証について、複雑なパスワード、ワンタイムパスワード、多要素認証などを設定している
5．VPN 機器への接続端末について、IP アドレスなどで規制している
6．実施していない

問19.　問8でクラウドサービスを「1．使用している」と回答された方に伺います。
クラウドサービスを使用することになった理由は何ですか。（○はいくつでも）

1．セキュリティ強化のため
2．管理する技術が不足している、又は負担軽減のため
3．管理する人的リソースが不足している、又は負担軽減のため
4．管理する費用が不足している、又は負担軽減のため
5．外出先（テレワーク先）から利用するため
6．わからない
7．その他（　　）

問20.　問９で外部から内部ネットワークへの接続を「１．許可している」と回答された方に伺います。どのような報セキュリティ対策を講じておられますか。通信路に対する対策は、回答群Ａから、端末に対する対策は、回答群Ｂからそれぞれ選択してください。（○はいくつでも）

【回答群Ａ（通信路に対する対策）】

１．ID・パスワード等による認証
２．MAC アドレス、クライアント証明書等使用する端末機器の固有情報を用いた認証
３．通信の暗号化
４．専用ネットワークセグメントの設定
５．ネットワークトラフィックの監視
６．クラウドサービスの利用
７．その他（　　）

【回答群Ｂ（端末に対する対策）】

１．ウイルス対策ソフト等の導入
２．OS、アプリケーション等をアップデートする仕組みの導入
３．使用するアプリケーションの制限（外部の端末機器に業務データが残らないアプリに限定等）
４．内部データの暗号化
５．各種ログの保管
６．盗難対策（端末ロック、内部データの遠隔消去等）
７．のぞき見防止
８．その他（　　）

問21.　問９で外部から内部ネットワークへの接続を「１．許可している」と回答された方に伺います。従業員等が社外等からインターネット接続経由で業務アクセスを行う場合に利用しているのはどういった認証方法ですか。（○はいくつでも）

→ 問21-1～21-2へお進みください

１．ID・パスワード等による認証
２．ワンタイムパスワード
３．IC カード・トークンデバイス型認証ツール
４．電子証明書（PKI）
５．バイオメトリクス（指紋等での認証）
６．ＳＭＳ認証
７．その他（　　）
８．認証なし

→ 問21-2へお進みください

問21-1.　問21で「１．ＩＤ・パスワード等による認証」と回答された方に伺います。ＩＤ・パスワード等の管理を徹底するために、どのような対策をされていますか。（○はいくつでも）

１．パスワード長を一定以上に定める
２．定期的にパスワードを変更させる
３．パスワードの複雑性をチェックし、簡単すぎるものは変更させる
４．異動等で使用しなくなった ID はすぐに削除する
５．ID をメールアドレス等の他の用途で流用しない
６．ID を複数ユーザで使わせない
７．ID・パスワードは利用者側の端末に保存されない
８．会社等の組織が指定したパスワード管理ツールを使う
９．その他（　　）
10．特に行っていない

問21-2.　不正ログイン（他人のＩＤ・パスワードを無断で入力する不正アクセス行為）を防止するために、どのような対策をされていますか。（○はいくつでも）

1．同一 ID、パスワードを固定した繰り返し入力の規制
2．同一 IP アドレスからの誤った ID・パスワードの繰り返し入力の規制
3．正規の利用者が使用する通信端末機器の事前登録
4．CAPTCHA（プログラムでは読み取り・入力が困難な符号の入力要求）
5．多要素認証の導入
6．リスクベース認証の導入
7．その他（　　）
8．特に行っていない

問22.　お客様などがフィッシング被害に遭わないための対策として、どのような対策をされていますか。（○はいくつでも）

1．顧客に対する注意喚起
2．フィッシングサイトの監視
3．フィッシングサイト発見時の関係機関への通報
4．送信ドメイン認証（SPF、DKIM、DMARC）等の電子メールなりすまし対策
5．その他（　　）
6．特に行っていない

【各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）に対するセキュリティ対策について伺います】

問23.　各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）を利用していますか。（○は一つ）

1．使用している　→　**問23-1へお進みください。**
2．使用していない　→　**問24へお進みください。**

問23-1.　当該サービスは、どのように管理されていますか。（○は一つ）

1．自社管理
2．一部外部業者に委託　→　**問23-2～23-4へお進みください。**
3．全て外部業者に委託　→　**問24へお進みください。**

問23-2.　問23-1で「１．自社管理」「２．一部外部業者に委託」と回答された方に伺います。セキュリティ対策は、どのような取組みをされていますか。（○はいくつでも）

1．常に最新のパッチを適用
2．管理者用アカウントのパスワードの複雑化
3．デフォルトアカウントを利用停止、または利用制限
4．セキュアコーディングの適用
5．リモートアクセスの接続元を限定
6．Web コンテンツの変更履歴を定期的に確認
7．Web システムの設定状況を定期的に確認
8．IDS,IPS,WAF 等のセキュリティ機器やサービスを利用
9．その他（　　）

問23-3.　問23-1で「１．自社管理」「２．一部外部業者に委託」と回答された方に伺います。過去1年間にシステム
のぜい弱性検査（ペネトレーションテスト等）を実施しましたか。（○はいくつでも）

１．定期点検のため実施
２．外部からの攻撃を受けた（可能性を含む）ため実施
３．関係業者、団体が被害に遭ったことを知ったため実施
４．その他（　　）
５．実施していない（理由：　　）

問23-4.　問23-1で「１．自社管理」「２．一部外部業者に委託」と回答された方に伺います。ログは取得後、どれく
らいの期間保管されていますか。また、どの様な方法で行っておられますか。（下表の各欄に、取得しているログの種類は該当する番号に○を、ログの保管期間及び方法は回答群Ａ（保管期間）・Ｂ（方法）からそれぞれ回答を選び、番号をご記入ください。）
※　回答が複数あるときは、最も長い期間を選んでご記入ください。

該当する選択肢の番号に○

ログの種類	回答群A	回答群B
回答例		
４．プロキシサーバのログ	5	1
１．ファイアウォール・侵入検知システム等（IDS、IPS 等）のログ		
２．ウェブサーバへのアクセスログ		
３．メールサーバのログ		
４．プロキシサーバのログ		
５．情報システムへの認証ログ		
６．データベースのログ		
７．クライアント PC のログ		
８．その他（　　）		
９．全く取得していない　→　問24にお進みください。		

各解答欄に該当する回答群から当てはまる番号を記入

回答群　A	
１．１週間以下	７．決めていない
２．１か月間	８．その他
３．３か月間	（　　）
４．６か月間	９．保管していない
５．１年間	10．運用していない
６．１年を超える	

回答群　B
１．自社
２．外部委託
３．その他
（　　）

問23-4-1へお進みください

問23-4-1. 問23-4で１～８の選択肢を回答された方に伺います。ログを取得・保管されているのは、どのような理由からですか。（○はいくつでも）

１．不正アクセス等外部からの不正行為を記録するため
２．従業員等内部の不正行為を記録するため
３．システムの管理、改善等に役立てるため
４．サービスその他業務に反映させるため
５．料金請求に活用するなど、業務に必要であるため
６．法令等により記録が義務づけられているため
７．その他（　　）
８．特に目的はない

【電子メールに対する情報セキュリティ対策について伺います】

問24.　電子メールに関するセキュリティ対策では、どのような取組みをされていますか。（○はいくつでも）

１．常に最新のパッチを適用
２．不正中継の防止
３．フィルタリング（特定の条件を満たすメールの配信をしない）
４．ウイルスチェック
５．特定ドメイン・アドレスからのメールのみ送・受信
６．特定の拡張子を持つファイルが添付されている場合に送・受信を拒否
７．利用メールソフトの指定・制限
８．メール利用の制限
（利用可能者の限定、利用端末の限定、組織内は別のツールで連絡を行う　等）
９．SPF（Sender　Policy　Framework）の導入
10. DKIM（DomainKeys Identified Mail）の導入
11. DMARC（Domain-based Message Authentication Reporting and Conformace）の導入
12. その他送信者認証
13. 電子署名の利用
14. クラウドサービスの利用
15. 無害化処理を実施
16. 標的型メール受信訓練の実施
17. 電子メールセキュリティ対策に関する教養
18. その他（　　）
19. わからない

問25.　電子メールに添付されたファイルは、どのように取り扱っておられますか。（○はいくつでも）

１．ウイルスチェックをしてから受信
２．無害化、振る舞い検知等をしてから受信
３．パスワード設定の添付ファイルのみ受信
４．特定の拡張子を持つファイルが添付されている場合に受信を拒否
５．添付ファイル付きの電子メールは一切受信しない
６．パスワード付き添付ファイルの禁止
７．特にチェック等はしていない
８．その他（　　）

【不正アクセス、情報漏えい等に対する情報セキュリティ対策について伺います】

問26.　重要なシステム（基幹業務、製造　等に関わるシステム）への侵入阻止や侵入時における被害軽減に向けて、
どのような対策を導入されていますか。（〇はいくつでも）

1．外部のネットワークに接続していない
2．重要な基幹業務システムは他のネットワークと分離した専用ネットワークを構築している
3．基幹業務システム専用のファイアウォール・ルータ（ネットワークアクセス制御機能）を導入している
4．システムの冗長化（ネットワークの冗長化を含む）を行っている
5．データのバックアップを行っている
6．緊急時にはシステムを自動停止する仕組みを導入している
7．指定回数以上のログイン失敗時のアカウント失効等、不正操作に対して自動的に制限をかける機能を導入している
8．重要なシステムへの個人所有端末装置（パソコン、スマートフォン等）の接続制限を行っている
9．無線 LAN の使用制限を行っている
10. 多要素認証を導入している
11. その他（　　）
12. 上記1.～11.のような対策は行っていない

問27.　不正アクセス、データ改ざん、情報漏えい等の行為に対して、どのような対策を実施されていますか。
（〇はいくつでも）

1．情報資産へのアクセス権の設定
2．定期的なパスワード変更
3．許可していないソフトウェアの制限
4．ユーザアカウントの定期的なチェック
5．アクセスログの取得、ログの分析
6．個人認証のためのシステム導入
7．定期的なバックアップ
8．バックアップの履歴管理
9．印刷物、電子媒体の持出し、廃棄管理
10. 端末装置（パソコン、スマートフォン等）廃棄時の適正なデータ消去
11. 共有 ID・パスワードの禁止
12. 情報資産の暗号化
13. 内部ネットワークのファイアウォール、侵入検知システム（IDS）の導入
14. メールのフィルタリング（添付ファイルの利用制限等）
15. 外部 Web サイトへのアクセス制限
16. 端末装置等のエンドポイントセキュリティ製品（EDR 等）の導入
17. その他（　　）
18. 特に何も行っていない

問28.　ウイルスやマルウェア等の不正プログラムに対して、どのような対策を実施されていますか。
（○はいくつでも）

1．ウイルス対策ソフト（クライアント）の使用
2．ウイルス対策ソフト（サーバ）の使用
3．パターンファイルを定期的に更新する
(社員自らが更新)
4．パターンファイルを定期的に更新する
(自動更新システムを利用)
5．パターンファイルを定期的に更新する
(管理者が手動で更新)
6．パッチによるOS等のバージョンアップ
(社員自らが更新)
7．パッチによるOS等のバージョンアップ
(自動更新システムを利用)
8．パッチによるOS等のバージョンアップ
(管理者が手動で更新)
9．許可されていないソフトウェアのインストール制限
10. ファイル等のダウンロード制限
11. プロバイダのウイルス等駆除サービスの利用
12. メールの添付ファイルの削除または実行制限
13. USBメモリ等の外部記録媒体の使用禁止
14. 検疫システムの導入
15. その他（　　）
16. 実施していない

３．人的対策

【情報セキュリティ教育に関する取り組みについて伺います】

問29.　現在、情報セキュリティ教育を行っておられますか。（○は一つ）

１．実施している
２．実施を予定している（具体的に実施計画を立てている）　→ 問29-1～29-2へお進みください

３．実施していない　→ 問29-3へお進みください

問29-1.　問29で「１．実施している」「２．実施を予定している」と回答された方に伺います。情報セキュリティに関する教育では、どのような内容を行っておられますか。（○はいくつでも）

１．情報セキュリティポリシー
２．情報システム利用に係るモラル
３．個人情報の保護・管理
４．機密情報の保護・管理
５．ウイルス等のマルウェア対策
６．情報へのアクセス管理（パスワード管理等）
７．社外ネットワークへの接続
８．文書の管理
９．緊急時の対応
10．ソーシャルエンジニアリング対策
11．技術的なセキュリティ対策（システムぜい弱性、堅牢化設定等）
12．サイバー犯罪の防止
13．クラウドの利用方法
14．テレワーク（リモート接続）関係
15．その他（　　）

問29-2.　問29で「１．実施している」「２．実施を予定している」と回答された方に伺います。情報セキュリティに関する教育は、どのくらいの頻度で行われていますか。（○はいくつでも）

１．月に１回以上
２．年に数回
３．年に１回
４．２、３年に１回
５．採用、異動時等に実施
６．その他（　　）

→ 問29-2を回答後、問30へお進みください。

問29-3.　問29で「３．実施していない」と回答された方に伺います。なぜ実施しないのですか。（○はいくつでも）

１．指導できる者が社内にいない
２．必要な資金がない
３．環境的に必要ない
４．必要な時間がない
５．必要性が理解されない
６．何をしてよいかわからない
７．その他（　　）

問30.　セキュリティ人材（専門家）を確保するための施策を行っておられますか。（○はいくつでも）

１．社内勉強会の実施
２．セキュリティ関連の試験・資格の活用
３．部外セミナー等の受講
４．セキュリティ団体(コミュニティ)への参加
５．セキュリティ人材のキャリアパス検討
６．専門人材の登用
７．社内では人材育成しない（外部人材等の活用）
８．その他（　　）

問31.　情報セキュリティ対策を実施するに当たって、困難に感じていることや、不正アクセス行為対策に対する不安
等、または、本アンケート調査に対するご意見等がございましたら、次の空欄に記載してください。

アンケートはこれで終わりです。ご協力ありがとうございました。
お手数ですが、令和 4年 9月 30日(金) までに、ご返送ください。

◆郵送での回答：同封の返信用封筒をご利用ください（切手は不要です）
◆電子メールでの回答：「cyber@researchworks.co.jp」　までお送りください

付録２

集計表

問1. 業種別回収数

農林・水産・鉱業	
農林・水産	0
鉱業	1
農林・水産・鉱業　その他	0
小計	1
製造業	
食品	13
繊維	4
紙・パルプ	1
化学	21
薬品	6
ゴム・窯業	7
非鉄金属	7
機械	24
電気機器	18
造船	0
輸送機器	13
精密機器	11
製造業　その他	26
小計	151
不動産・建築	
不動産	8
建築	13
不動産・建築　その他	4
小計	25
金融	
銀行	20
証券	3
保険	0
クレジット	0
消費者金融	1
信用金庫・組合	0
金融　その他	4
小計	28
エネルギー	
電力	2
ガス	2
水道	0
石油製造(精製)	0
エネルギー　その他	0
小計	4

運輸業	
鉄道・地下鉄	4
航空	1
陸運	8
海運	3
倉庫	5
運輸業　その他	1
小計	22
情報通信	
新聞	0
放送	3
通信	4
ISP	0
情報通信　その他	7
小計	14
サービス	
流通・卸売	34
小売	15
娯楽・アミューズメント	1
飲食	4
ホテル・旅行	4
情報処理・ソフトウェア	12
警備	0
医療・福祉	39
サービス　その他	17
小計	126
教育	
大学	104
短大	0
専門学校	0
教育　その他	1
小計	105
行政サービス	
都道府県	2
政令指定都市	0
市町村	102
小計	104
無回答	20
合計	600

第２部

アクセス制御機能に関する技術の研究開発の状況等に関する調査

4.調査概要

4.1 調査の目的

不正アクセス行為の禁止等に関する法律において、国家公安委員会は、アクセス制御機能を有する特定電子計算機の不正アクセス行為からの防御に資するため、毎年少なくとも1回、アクセス制御機能に関する技術の研究開発の状況を公表するものとされている。

本調査は、大学、民間企業等において、研究開発や製品化（実用化）が進められているアクセス制御機能に関する技術の研究開発状況等について調査を実施したものである。

4.2 調査の対象と調査方法

調査対象：以下に該当する調査対象から無作為に1,884件抽出した。

・企業（1,599社）

市販のデータベース（会社四季報）に掲載された企業であって、業種分類が「情報・通信」「サービス」「電気機器」「金融」であるもの

・大学（285校）

国公立・私立大学のうち、理工系学部又はこれに準ずるものを設置するもの

調査方法は、次の方法で実施した。

① 電子メールでの回答

調査票のファイルに直接回答内容を入力してもらい、電子メールにて回答

② 郵送等での回答

配付した調査票を、郵送で送付してもらい回答

（調査期間：令和4年9月9日(金)（発送日)～10月17日(月)（締切日)）

4.3 調査内容

本調査では次の2つを調査した。

① 研究開発の傾向

アクセス制御機能に関する技術サービスの研究開発の傾向を分析するために、アクセス制御機能を８つの分野に分類し、企業や大学において力をいれている分野等を調査した。

質問項目は次の通りである。

・研究開発体制

・アクセス制御機能に関する技術研究開発に係る現状と今後の展望

・アクセス制御機能に関する実用化（製品化）に係る現状と今後の展望

調査票：付録資料にある『回答用紙A』を参照

【分類の票】

分類	例
暗号技術	暗号技術（アルゴリズム開発など）、暗号化ソフト（ファイルの暗号化、ディスクの暗号化など）
認証技術	ワンタイムパスワード、IC カード、USB 等デバイスによる認証、バイオメトリクス認証、PKI、アクセスコントロール（シングルサインオン含む）
ネットワークセキュリティ	VPN（IPsec、SSL、Secure Shellなど）、無線 LAN セキュリティ、ファイアウォール、パケットフィルタリング、コンテンツセキュリティ（コンテンツフィルタ､メールフィルタ）、ネットワーク管理
不正侵入対策	侵入検知（IDS）、ハニーポット、アクセスログ収集管理
セキュリティマネジメント	ログ解析、資産管理、情報保護、セキュリティ情報管理
ウイルス（不正プログラム）対策	ウイルス対策ソフト、スパイウェア対策ソフト
セキュリティサービス	セキュリティ診断、不正アクセスウイルス監視、コンサルティング、レスキューサービス
クラウドコンピューティング	ネットワークを経由してアクセスするサーバ、ストレージ等の資産管理、運用管理クラウドサービス提供、利用に係るセキュリティ全般

② 実用化された製品及び研究開発中の技術・サービス

既に実用化された個々の製品（ハードウェア、ソフトウェア、サービス）及び現在開発中の個々の技術・サービスの内容について調査した。

質問項目は以下の通りである。

・何を守るか

・何から保護するのか

・どのようなセキュリティ上の効果があるか

・どのような機能を持っているか

・どのようなレイヤーのセキュリティを守るか

・不正アクセスからの防御対象

・どのようなサービスか

調査票：付録資料の『回答用紙B』、『回答用紙C』を参照

4.4 送付・回収状況、集計対象件数

全体では、1,884件を送付して、227件を回収し、回収率は12.0％であった。

全体での回収数227件のうち、回答用紙A「アクセス制御機能に関する技術の研究開発の現状と方向性に係る調査」の問１「アクセス制御機能に関する技術の研究開発を行っていますか」に「はい」と回答した有効回答数は34件であった。また、回答用紙B「実用化（製品化）されているアクセス制御機能に関する技術」に対する回答は10件、回答用紙C「研究開発中のアクセス制御機能に関する技術」に対する回答は22件であった。

4.5 報告書を見る際の留意点

・集計結果の比率は、小数点第二位を四捨五入し、小数点第一位までを百分率（％）で表示しているため、その数値の合計が100％を前後する場合がある。

・本文やグラフ中の選択肢は、調査票の言葉を短縮しているものがある。

5.調査結果(概要と考察)

5.1 アクセス制御機能に関する技術研究開発に係る現状と今後の展望

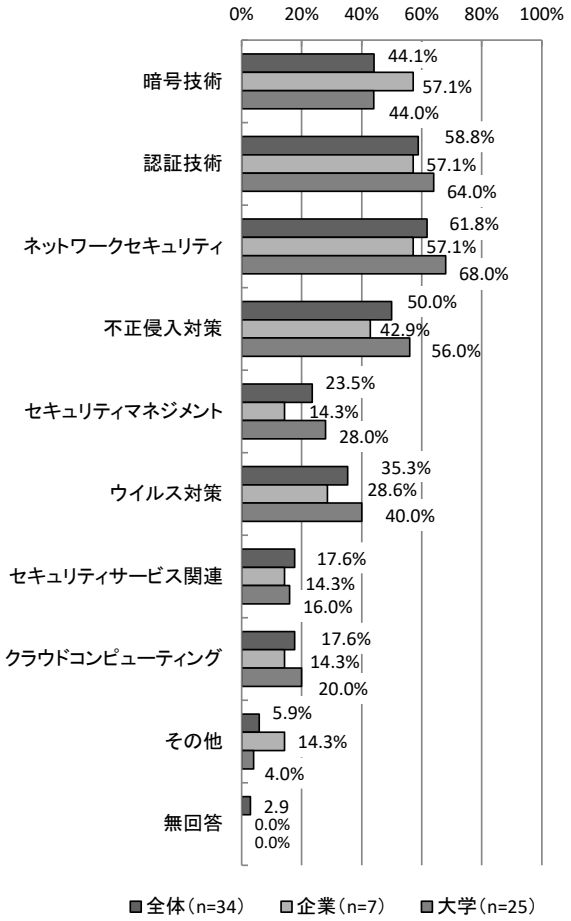
現在、取り組んでいる分野について、全体では「ネットワークセキュリティ」が最も高い。企業では「暗号技術」「認証技術」及び「ネットワークセキュリティ」が同率で高く、大学では「ネットワークセキュリティ」が高くなっている。

今後、取り組んでいく分野について、全体では「暗号技術」、「ネットワークセキュリティ」が最も高い。企業では「認証技術」「不正侵入対策」「セキュリティサービス関連」が高く、大学では「暗号技術」「ネットワークセキュリティ」が高い。

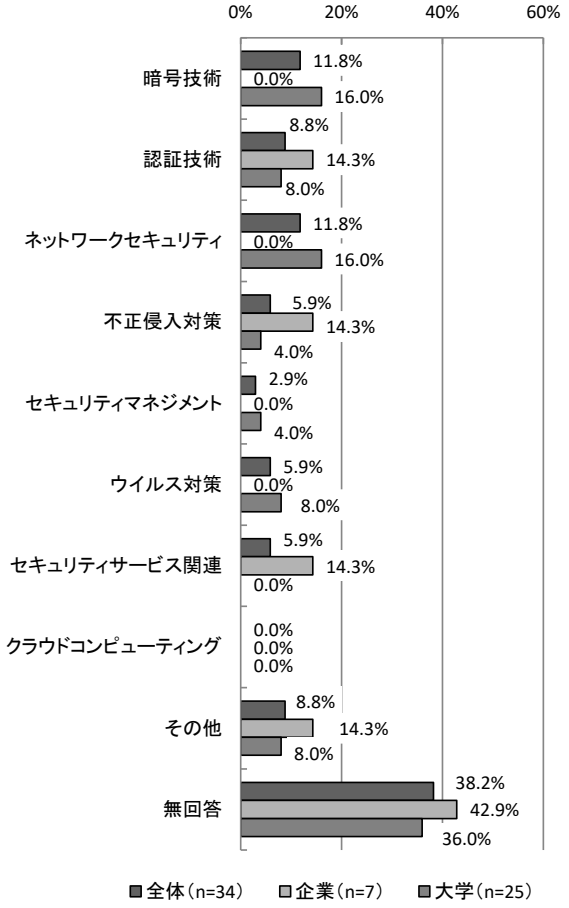
現在、取り組んでいる分野については、「ネットワークセキュリティ」が61.8%（21件）で最も多く、次いで「認証技術」が58.8%（20件）となっている。企業では「暗号技術」「認証技術」「ネットワークセキュリティ」が同率の57.1%（4件）で最も多く、大学では「ネットワークセキュリティ」が68.0%（17件）で最も多い。

今後、もっとも力を入れたい分野については、「暗号技術」「ネットワークセキュリティ」が11.8%（4件）で最も多くなっている。企業では「認証技術」「不正侵入対策」「セキュリティサービス関連」がそれぞれ14.3%（1件）、大学では「暗号技術」「ネットワークセキュリティ」が16.0%（4件）と最も多くなっている。

【本調査】現在、取り組んでいる分野（MA）【A-問2】



【本調査】今後、もっとも力を入れたい分野（SA）【A-問3】



5.1.1 現在、取り組んでいる分野 【A-問2】

【経年変化】

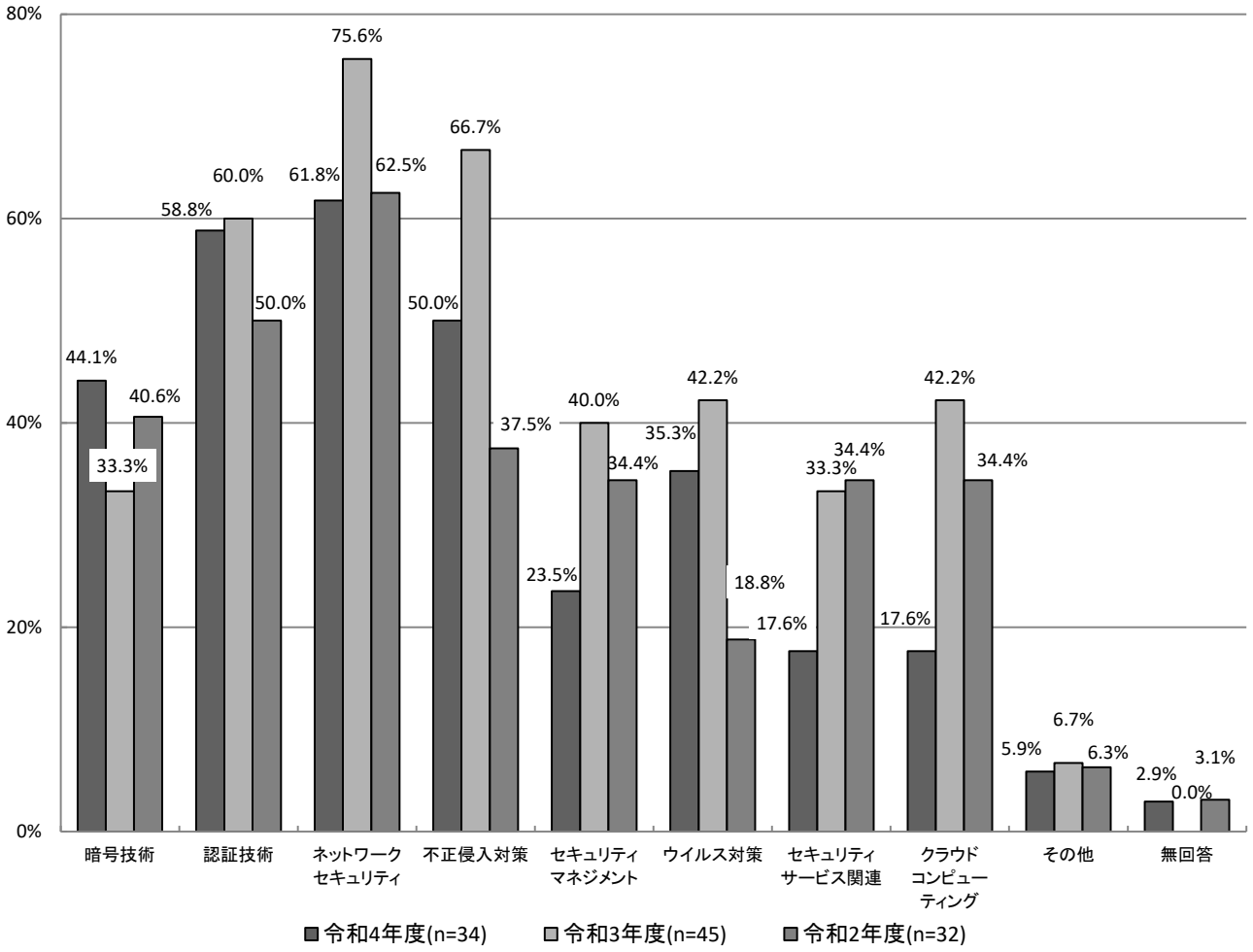
全体では、昨年度より減少となった分野が多く、特に「クラウドコンピューティング」、「不正侵入対策」が大きく減少している一方で、「暗号技術」のみ増加している。

企業では、「暗号技術」が増加し「クラウドコンピューティング」が最も減少している。大学では、「暗号技術」が最も増加し「セキュリティサービス関連」が減少している。

【経年変化(全体)】

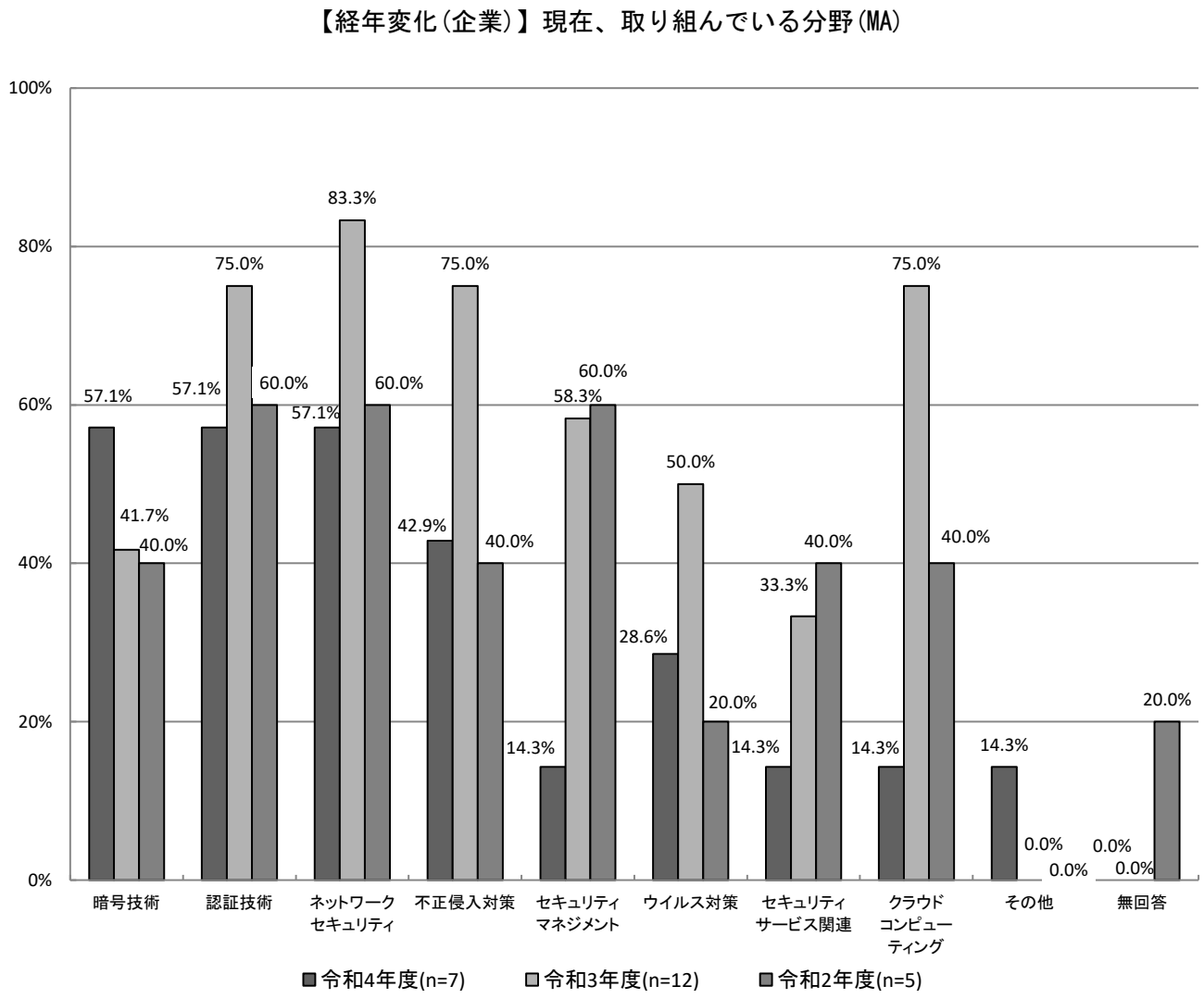
昨年度と比較すると全体では、「クラウドコンピューティング」が24.6ポイント、「不正侵入対策」が16.7ポイント減少しており、「暗号技術」が10.8ポイント増加している。

【経年変化(全体)】現在、取り組んでいる分野(MA)



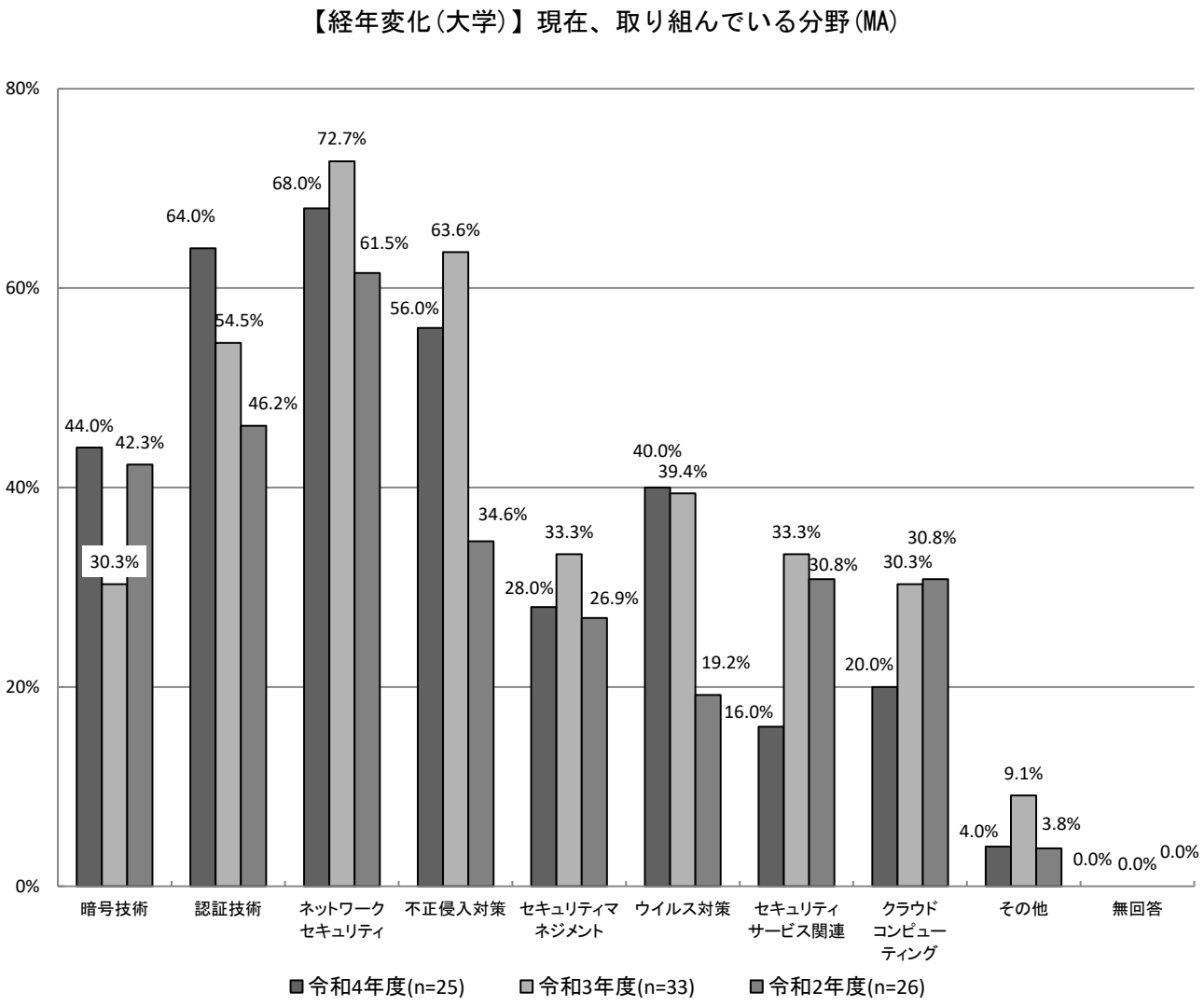
【経年変化(企業)】

昨年度と比較すると企業では、「クラウドコンピューティング」が60.7ポイント、「セキュリティマネジメント」が44.0ポイント減少しており、「暗号技術」が15.4ポイント増加している。



【経年変化(大学)】

昨年度と比較すると大学では、「セキュリティサービス関連」が17.3ポイント減少しており、「暗号技術」が13.7ポイント増加している。

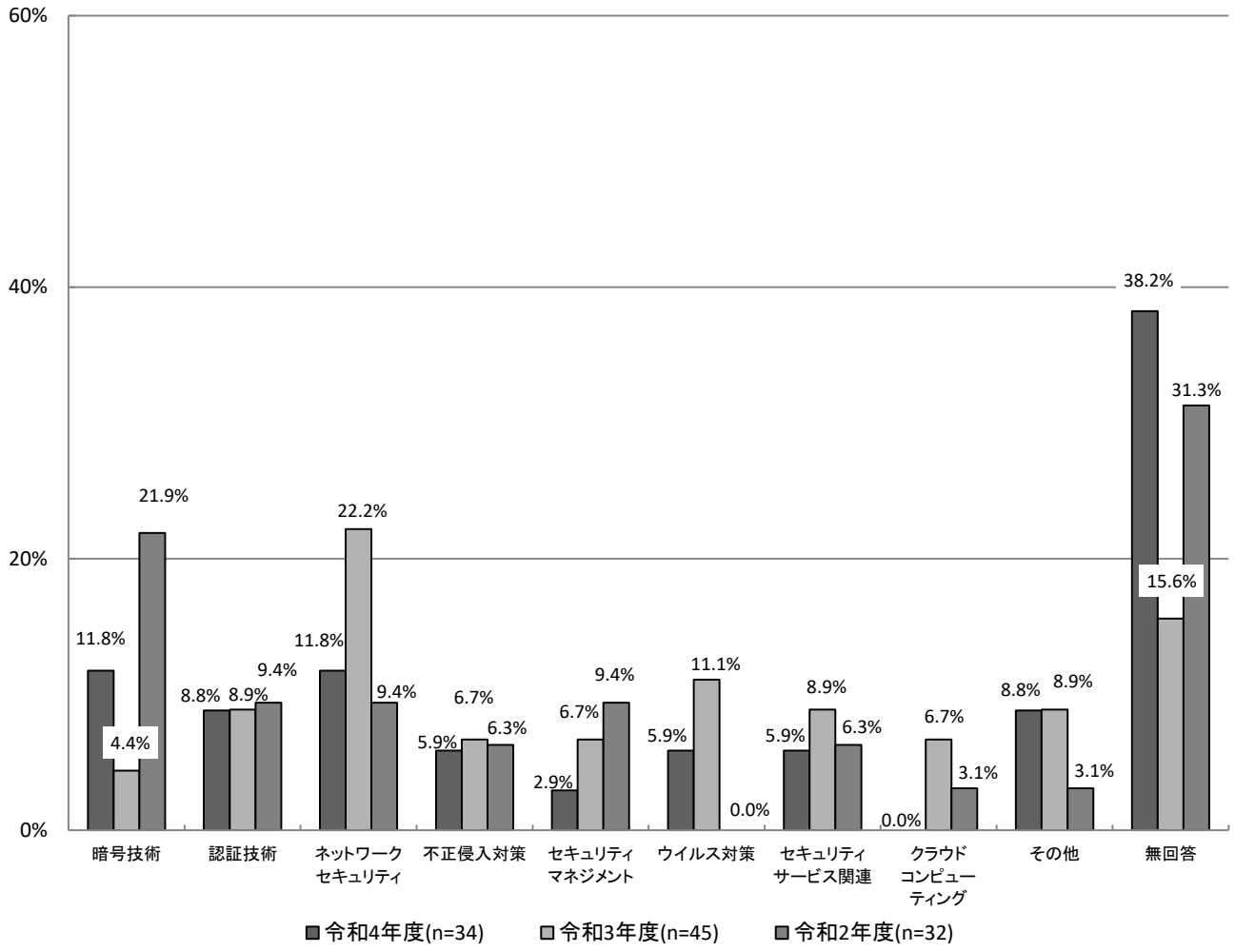


5.1.2 今後、もっとも力を入れたい分野 【A-問3】

【経年変化】
全体では、「暗号技術」が増加しているが、一方で、それ以外はすべて減少している。企業では、「ネットワークセキュリティ」、「クラウドコンピューティング」が減少しており、大学では、「暗号技術」が昨年度よりも増加している、一方で「セキュリティサービス関連」が最も減少している。

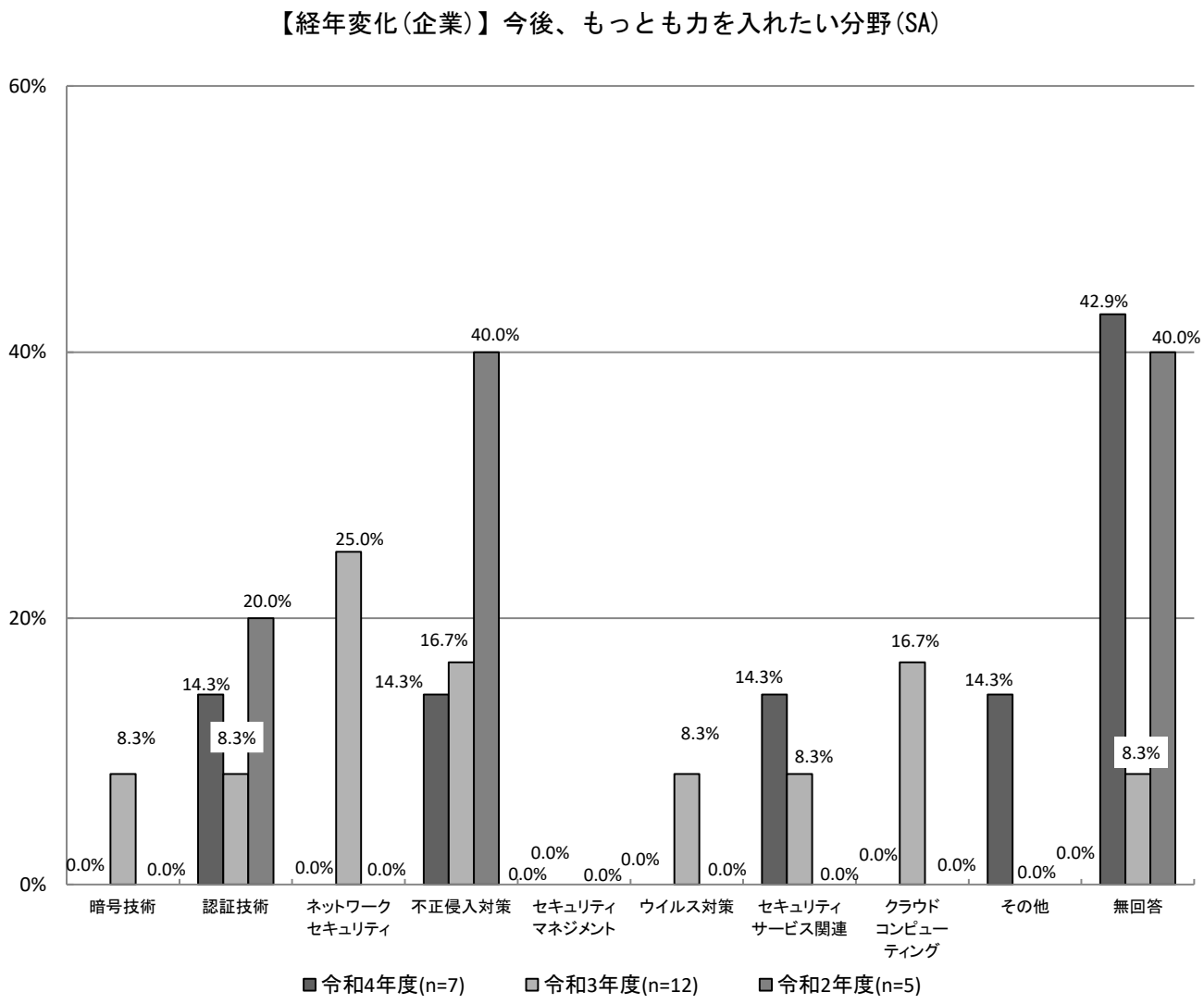
【経年変化(全体)】
昨年度と比較すると全体では、「暗号技術」が7.4ポイント増加している。一方、「ネットワークセキュリティ」が10.4ポイント、「クラウドコンピューティング」が6.7ポイント減少している。

【経年変化(全体)】今後、もっとも力を入れたい分野(SA)



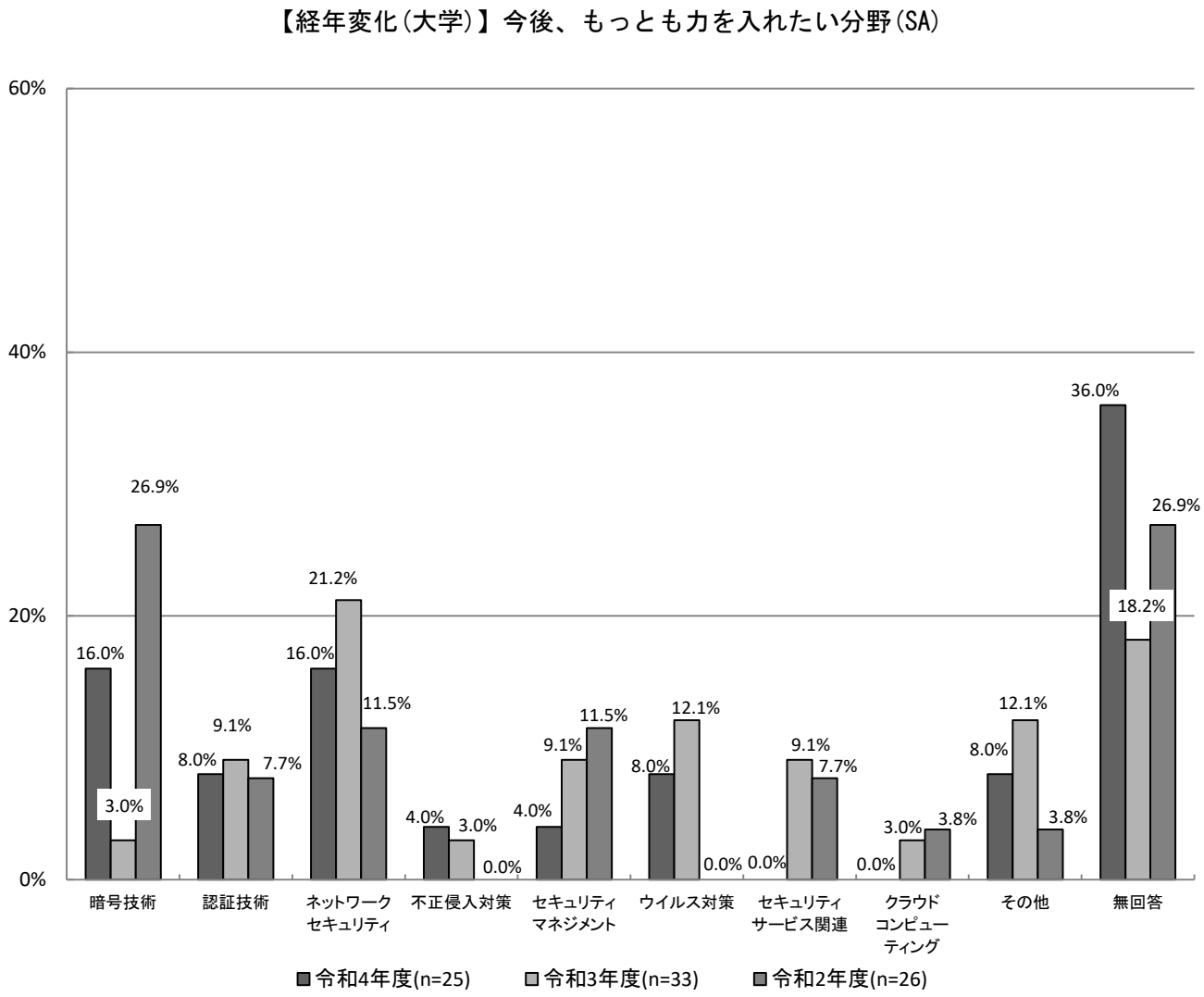
【経年変化(企業)】

昨年度と比較すると企業では、「ネットワークセキュリティ」が25.0ポイント、「クラウドコンピューティング」が16.7ポイント減少している。



【経年変化(大学)】

昨年度と比較すると大学では、「暗号技術」が13.0ポイント増加している。一方、「セキュリティサービス関連」は9.1ポイント減少している。



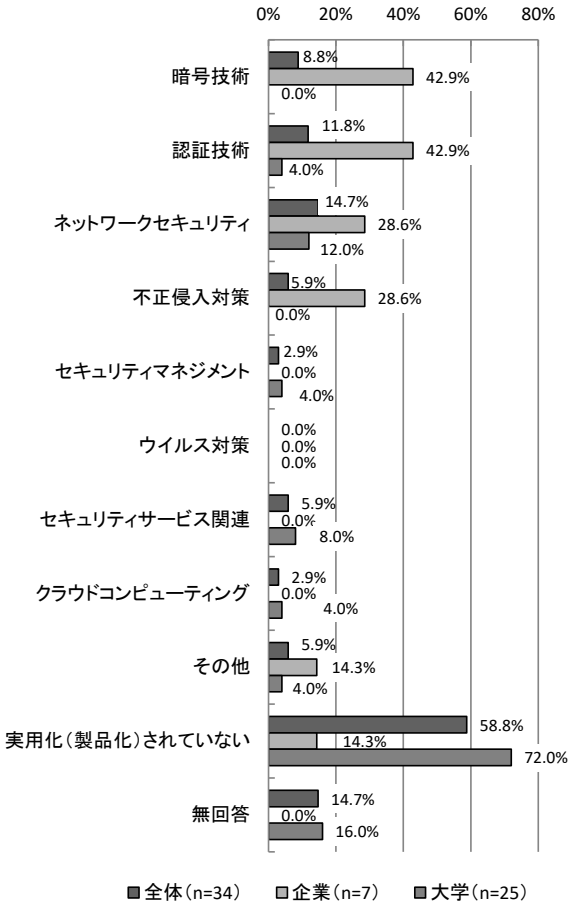
5.2 アクセス制御機能に関する実用化(製品化)に係る現状と今後の展望

実用化（製品化）の現状については、「ネットワークセキュリティ」が最も多くなっている。
今後、実用化（製品化）を見込んでいるアクセス制御機能については、「認証技術」が最も多くなっている。

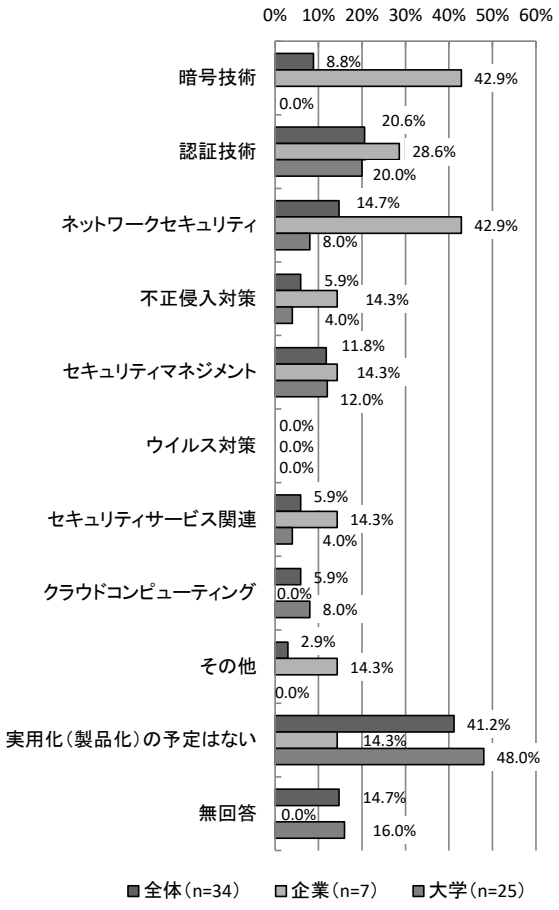
現在、実用化（製品化）されている分野については、全体では「ネットワークセキュリティ」が14.7%（5件）で最も多く、次いで「認証技術」が11.8%（4件）、「暗号技術」が8.8%（3件）となっている。企業では「暗号技術」「認証技術」がそれぞれ42.9%（3件）で最も多く、大学では「ネットワークセキュリティ」が12.0%（3件）で最も多くなっている。

今後、実用化（製品化）を見込んでいる分野については、全体では「認証技術」が20.6%（7件）で最も多く、次いで「ネットワークセキュリティ」が14.7%（5件）となっている。企業では「暗号技術」「ネットワークセキュリティ」がそれぞれ42.9%（3件）で最も多く、大学では「認証技術」が20.0%（5件）で最も多くなっている。

【本調査】現在、実用化(製品化)されている
アクセス制御機能(MA)【A-問4】



【本調査】今後、実用化(製品化)を見込んでいる
アクセス制御機能(MA)【A-問5】

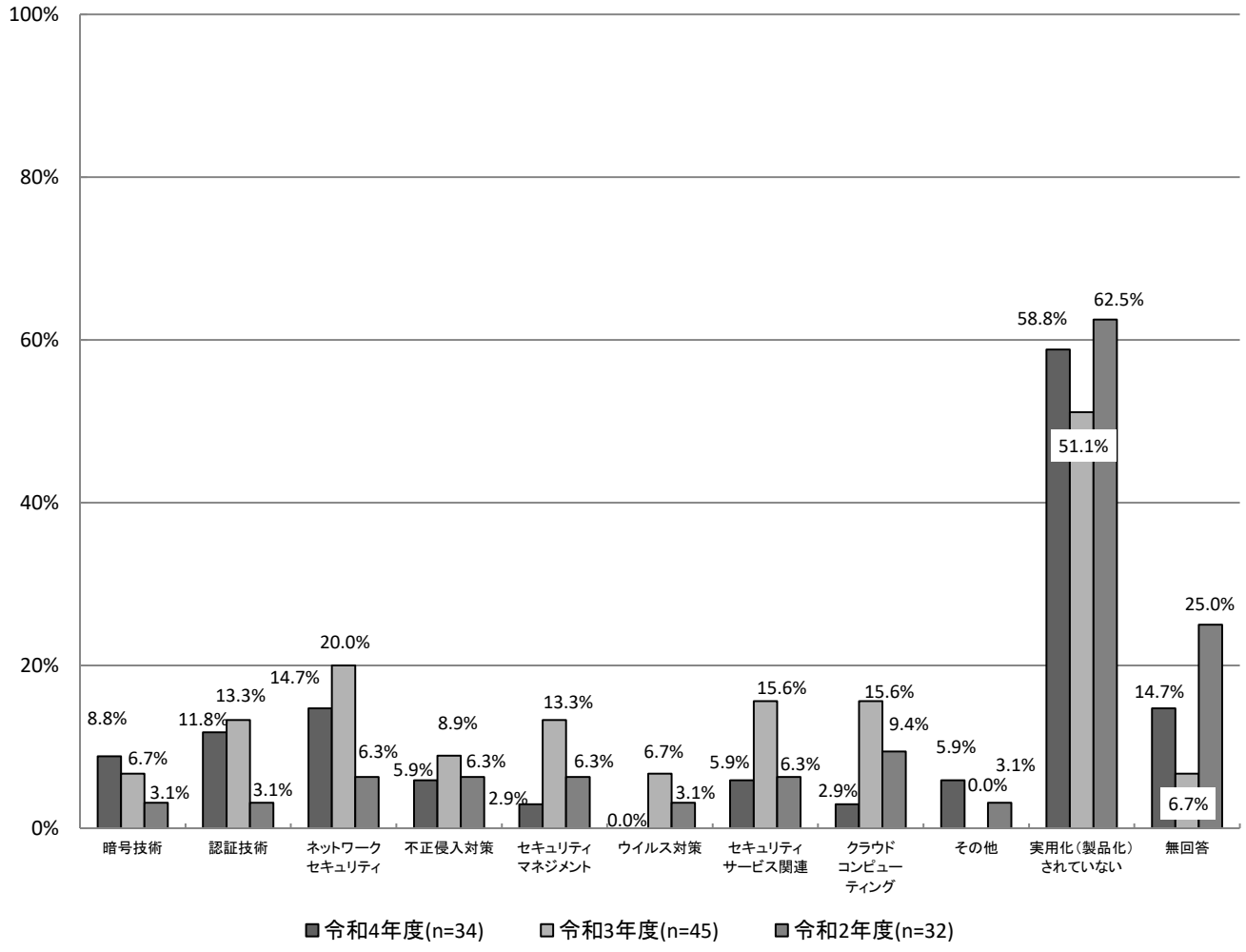


5.2.1　現在、実用化(製品化)されている分野　【A-問4】

【経年変化】
全体では、「暗号技術」の分野以外で減少している。
企業では、「暗号技術」が26.2ポイント増加し、大学では、すべての分野で減少または横ばいとなっている。

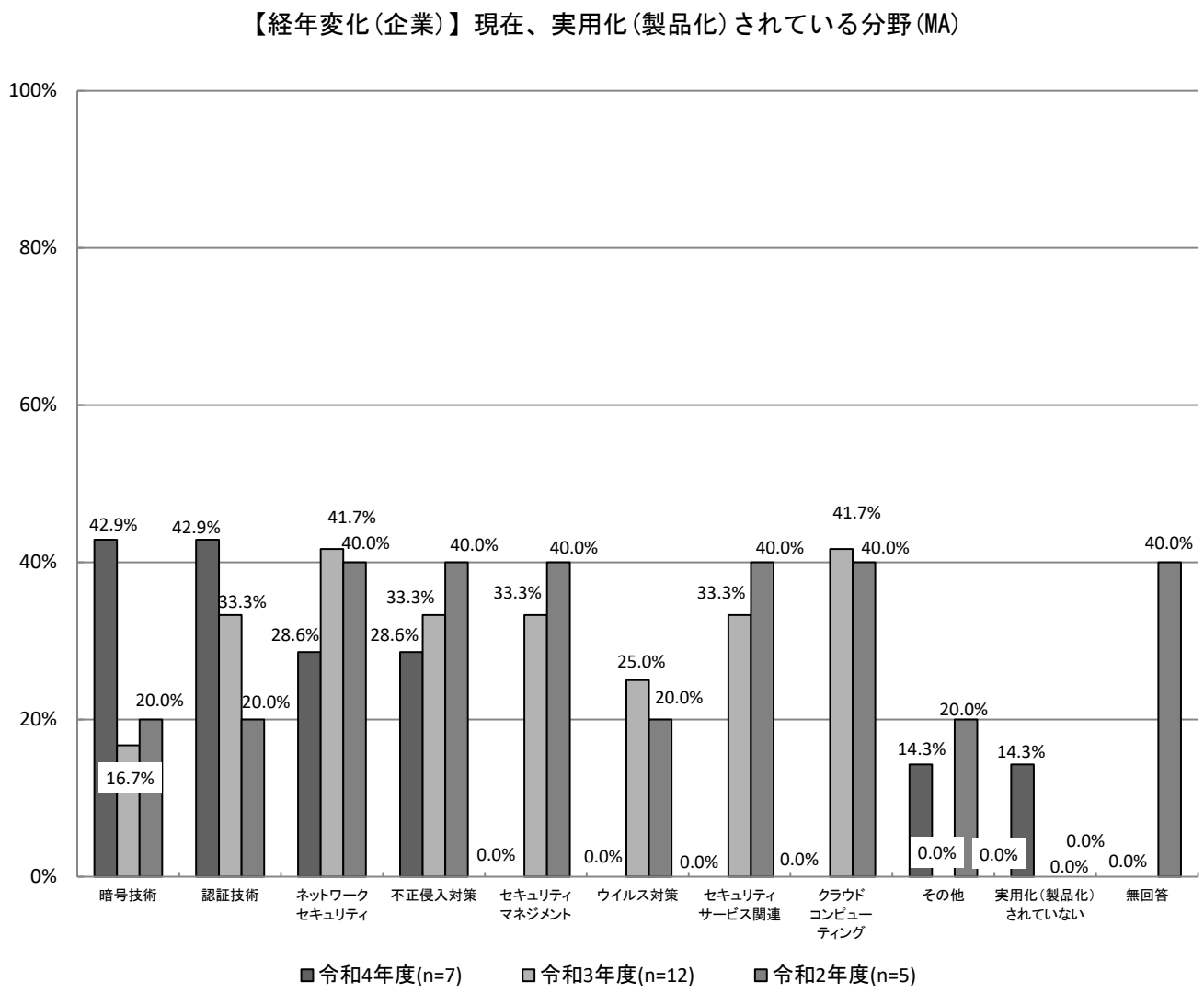
【経年変化(全体)】
昨年度と比較すると「暗号技術」が2.1ポイント増加しており、それ以外の分野ではすべて減少している。

【経年変化(全体)】現在、実用化(製品化)されている分野(MA)



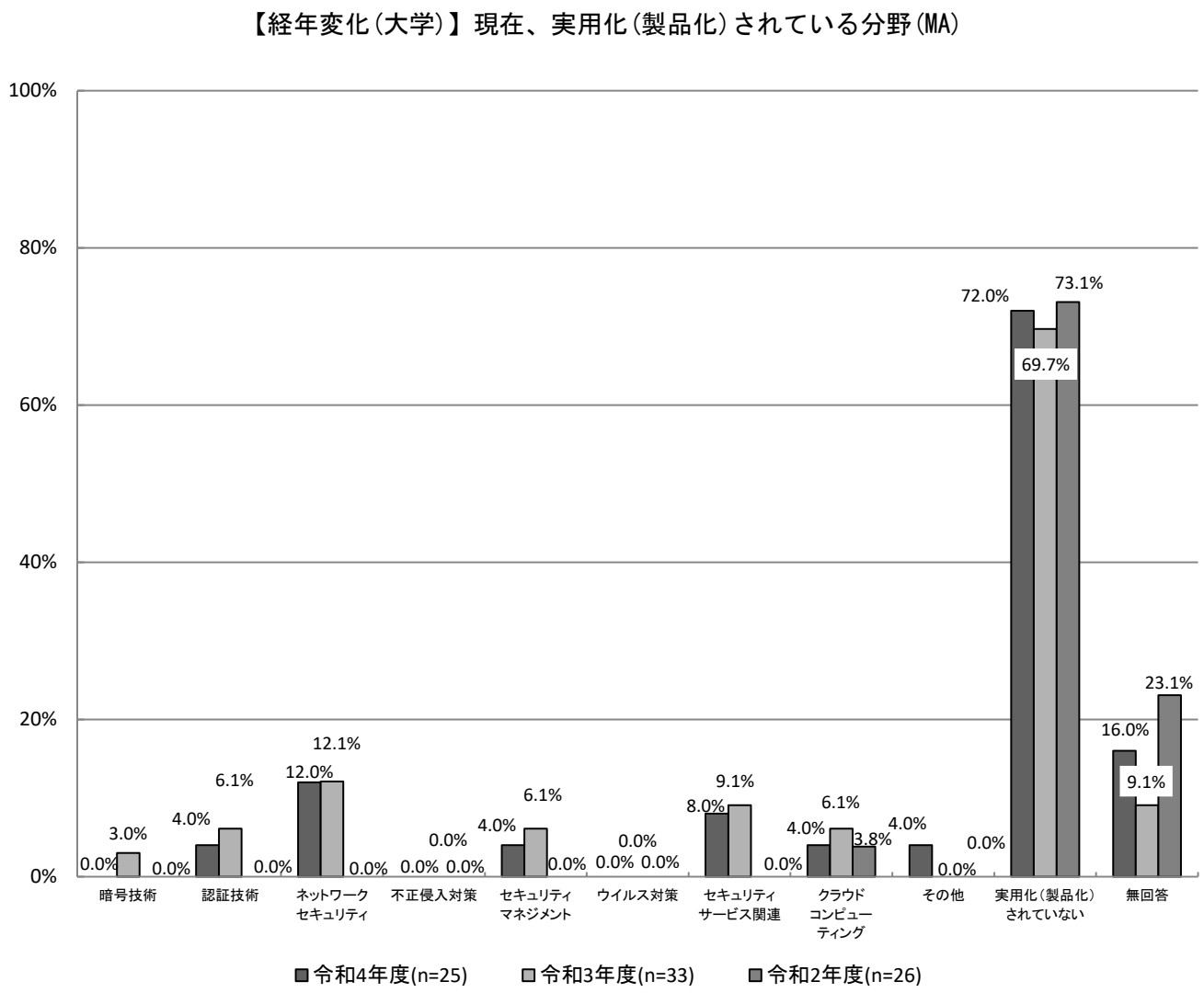
【経年変化(企業)】

昨年度と比較すると企業では、「暗号技術」が26.2ポイント増加している。



【経年変化(大学)】

昨年度と比較すると大学では、すべての分野で減少または横ばいとなっている。

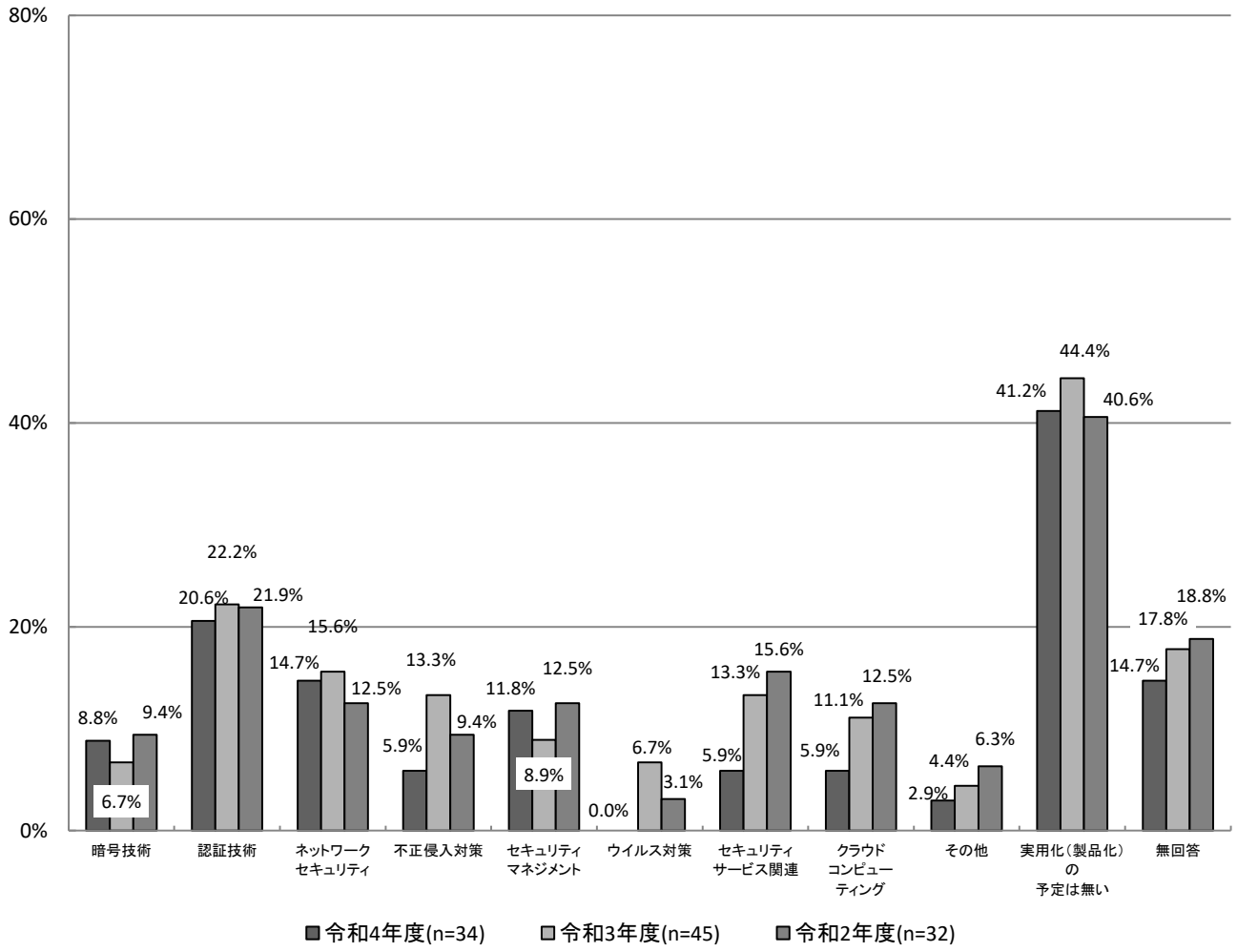


5.2.2　今後、実用化(製品化)を見込んでいる分野　【A-問5】

【経年変化】
　全体では、「セキュリティサービス関連」、「不正侵入対策」、「ウイルス対策」などが減少している。
　企業では「暗号技術」「ネットワークセキュリティ」などが増加しており、大学では「セキュリティサービス関連」が最も減少している。

【経年変化(全体)】
　昨年度と比較すると全体では、「セキュリティサービス関連」、「不正侵入対策」がそれぞれ7.4ポイント減少している。次いで、「ウイルス対策」が6.7ポイント減少している。

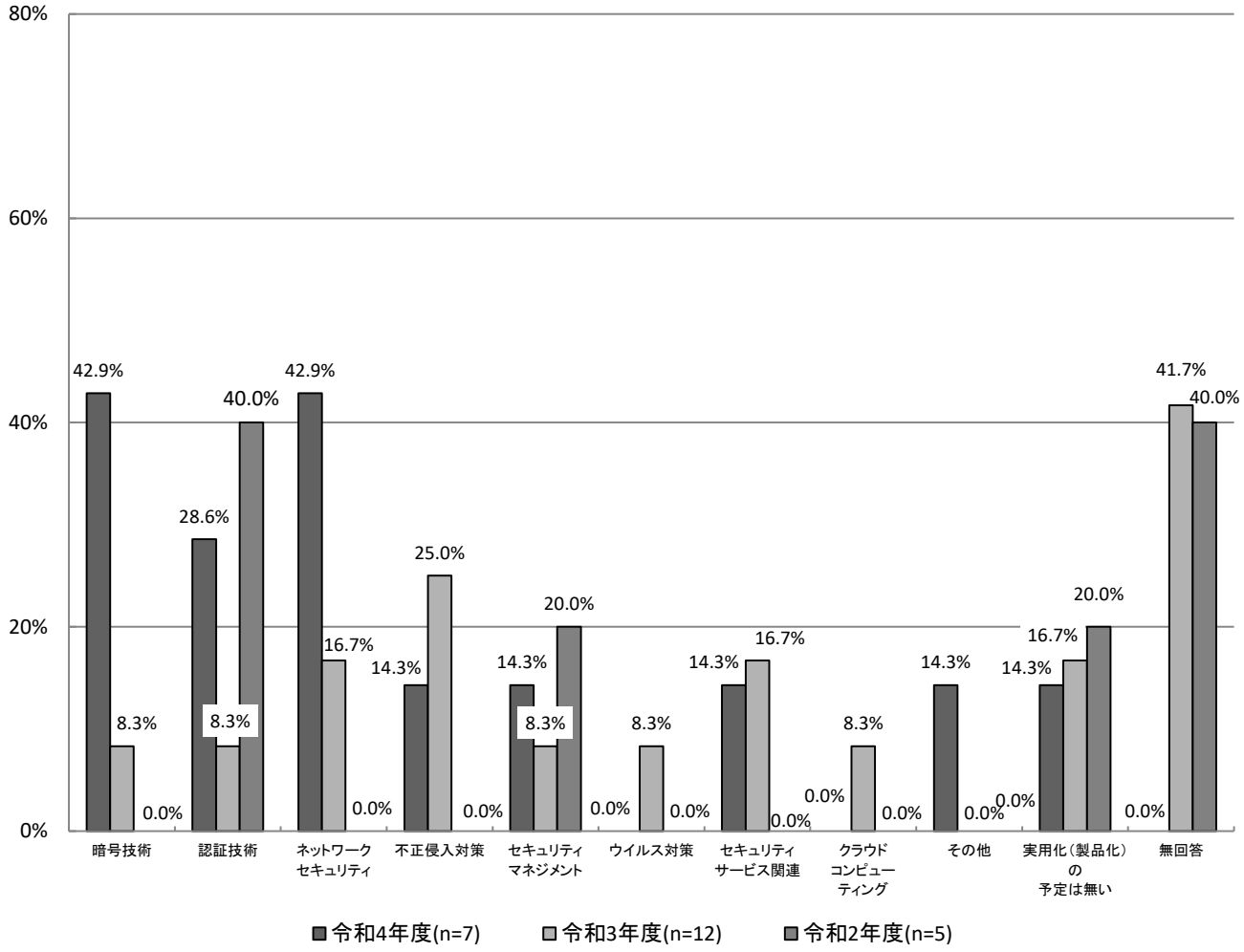
【経年変化(全体)】今後、実用化(製品化)を見込んでいる分野(MA)



【経年変化(企業)】

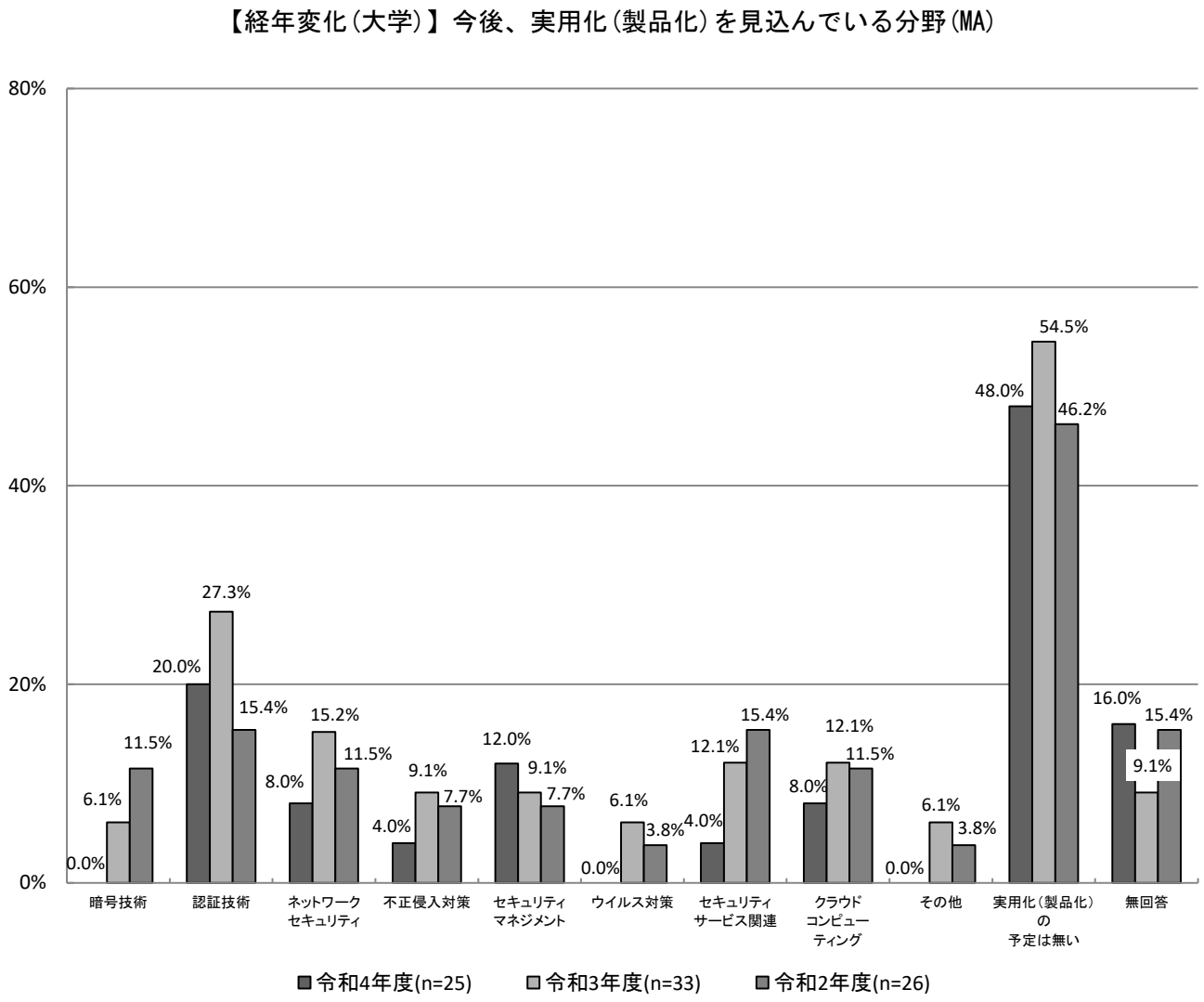
昨年度と比較すると企業では、「暗号技術」が34.6ポイントと最も増加しており、次いで「ネットワークセキュリティ」が26.2ポイント、「認証技術」が20.3ポイント増加している。

【経年変化(企業)】今後、実用化(製品化)を見込んでいる分野(MA)



【経年変化(大学)】

昨年度と比較すると大学では、「セキュリティサービス関連」が8.1ポイントと最も減少しており、「セキュリティマネジメント」以外の全ての分野が減少している。



5.3 研究開発体制

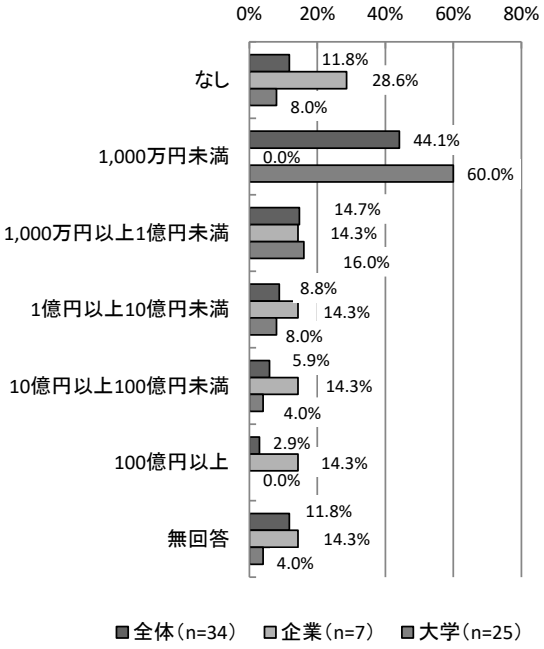
研究開発費について、企業は「なし」が最も多く、大学は「1,000万円未満」が最も多くなっている。

研究開発人数について、企業は「10人以上50人未満」、大学は「1人以上10人未満」が最も多くなっている。

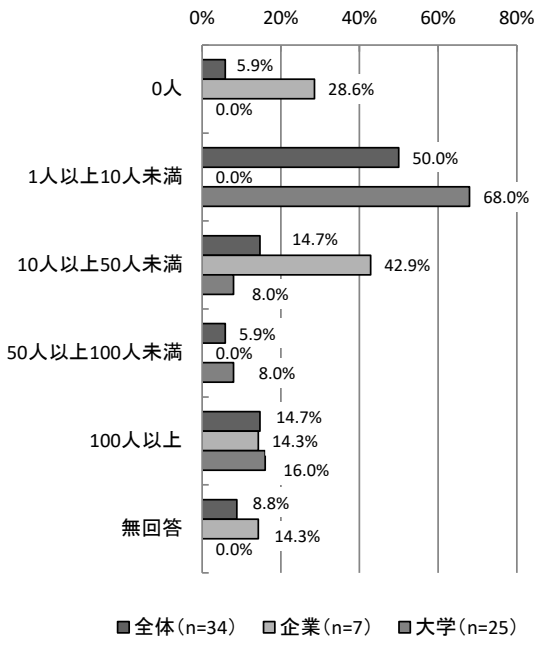
年間の研究開発費については、全体では「1,000万円未満」が44.1%（15件）で最も多くなっている。企業では「なし」が28.6%（2件）で最も多く大学では「1,000万円未満」が60.0%（15件）と最も多くなっている。

研究開発人員については、全体では「1人以上10人未満」が50.0%（17件）と最も多くなっている。企業では「10人以上50人未満」が42.9%（3件）で最も多く、大学では「1人以上10人未満」が68.0%（17件）で最も多くなっている。

【本調査】年間の研究開発費（SA）【A-問6】



【本調査】研究開発に携わっている人数（SA）【A-問7】



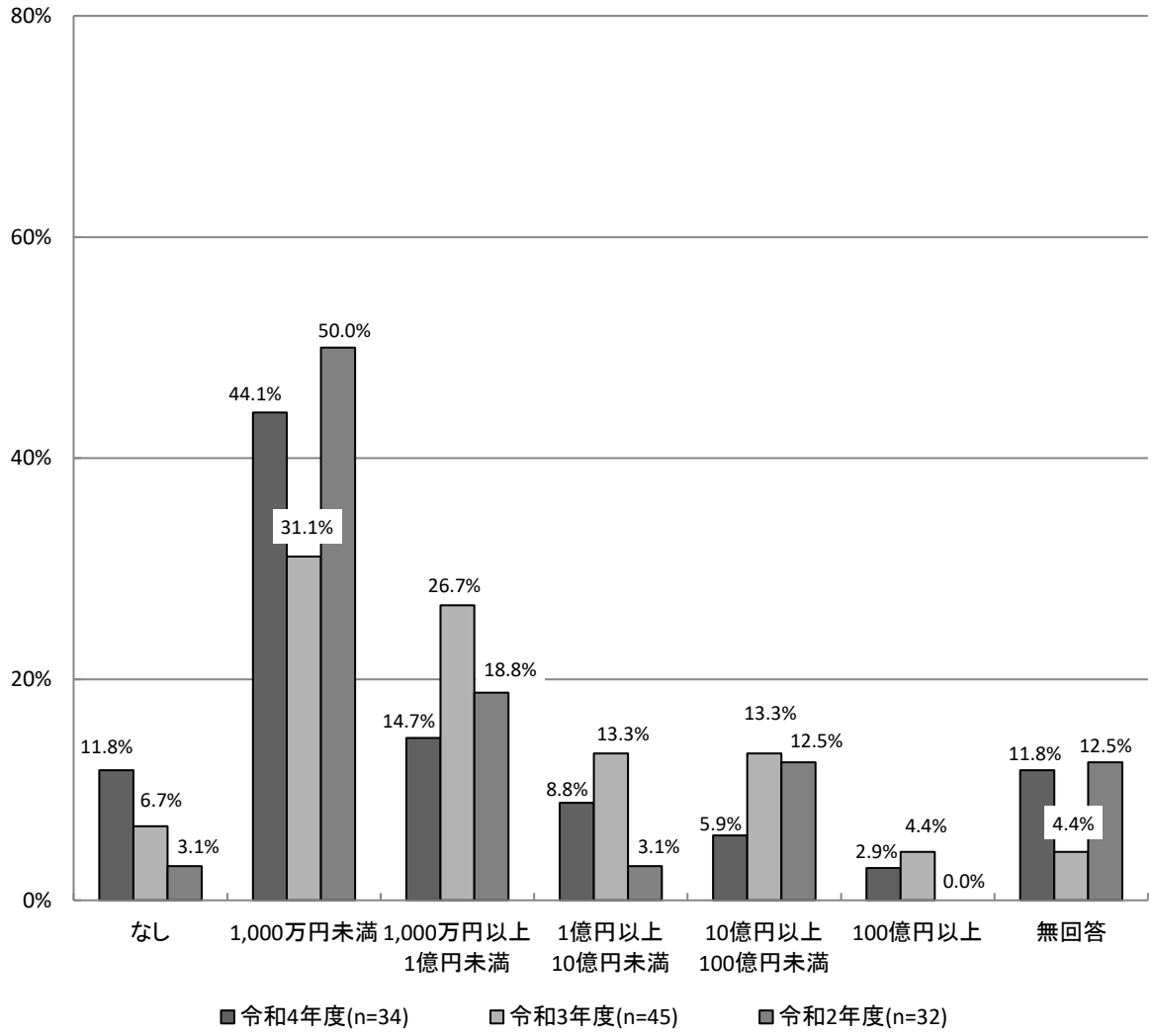
5.3.1　年間の研究開発費　【A-問6】

【経年変化】
全体では「1,000万円未満」が最も増加している。
企業では「なし」、大学では「1,000万円未満」が最も増加している。

【経年変化(全体)】

昨年度と比較すると全体では、「1,000万円未満」が13.0ポイント増加している。一方、「1,000万円以上1億円未満」が12.0ポイント、「10億円以上100億円未満」が7.4ポイント減少している。

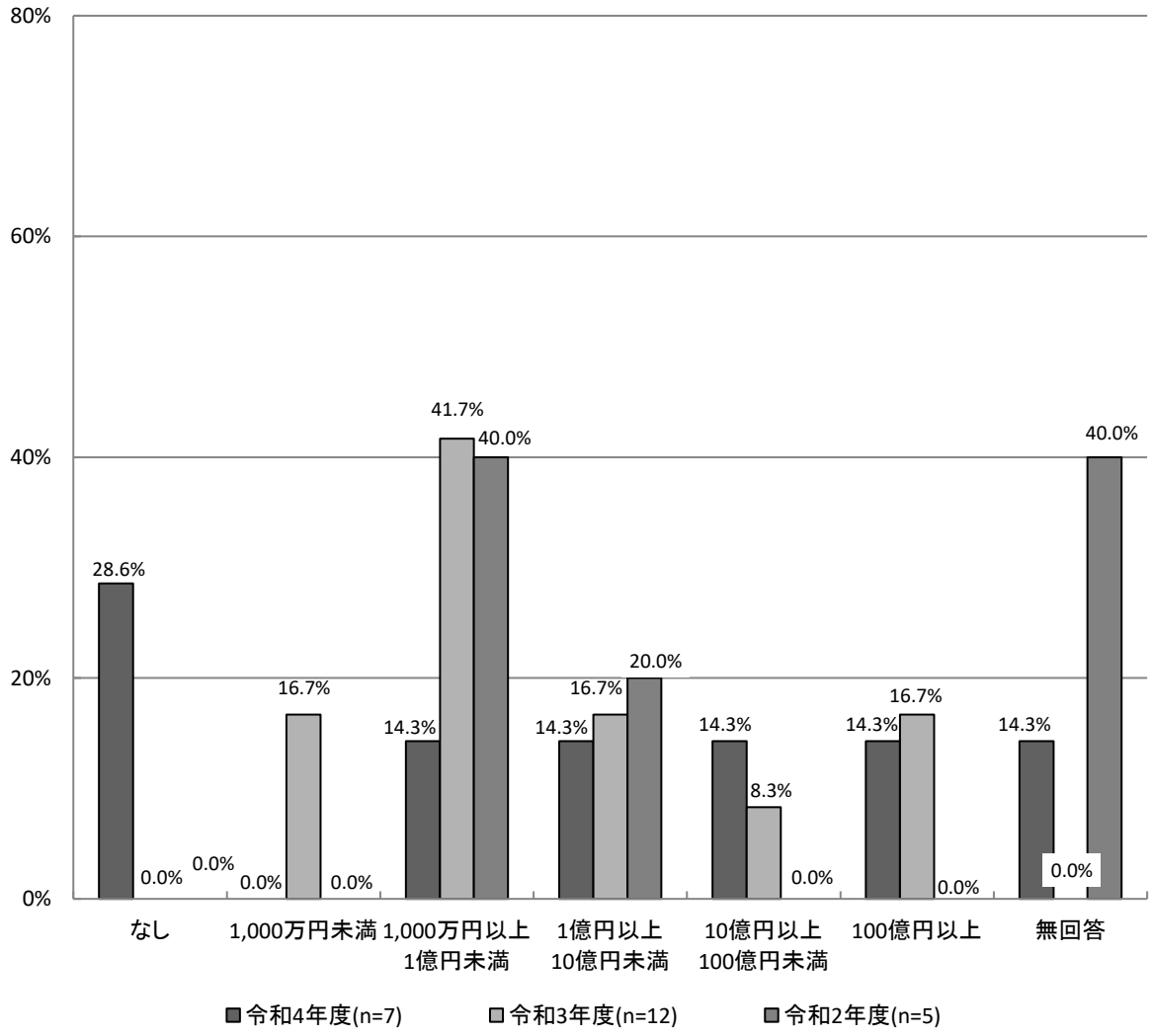
【経年変化(全体)】年間の研究開発費(SA)



【経年変化(企業)】

昨年度と比較すると企業では、「なし」が28.6ポイント増加している。一方、「1,000万円以上1億円未満」が27.4ポイントと最も減少しており、次いで「1,000万円未満」が16.7ポイント減少している。

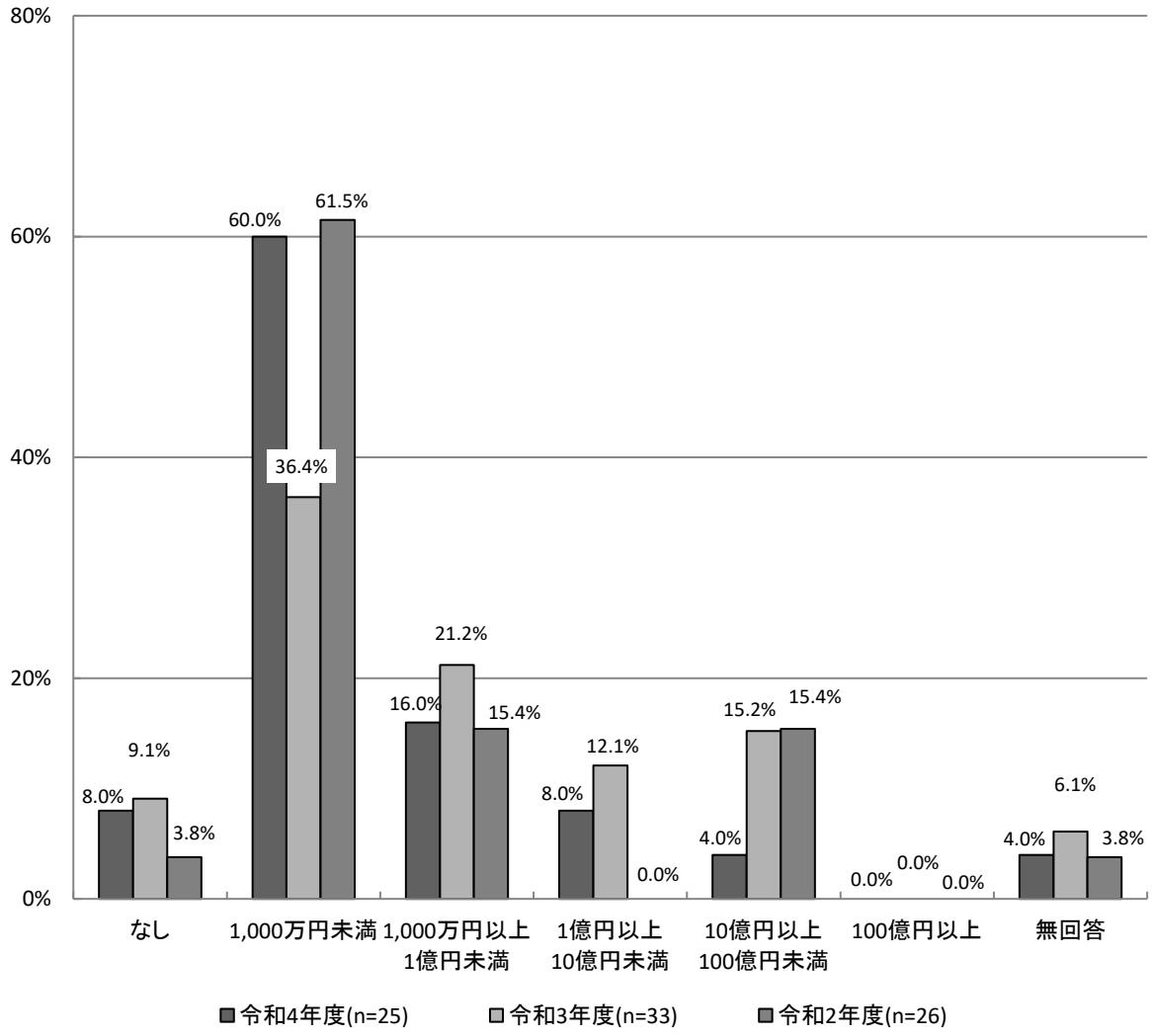
【経年変化(企業)】年間の研究開発費(SA)



【経年変化(大学)】

昨年度と比較すると大学では、「1,000万円未満」が23.6ポイントと増加している。一方、「10億円以上100億円未満」が11.2ポイントと最も減少している。

【経年変化(大学)】年間の研究開発費(SA)

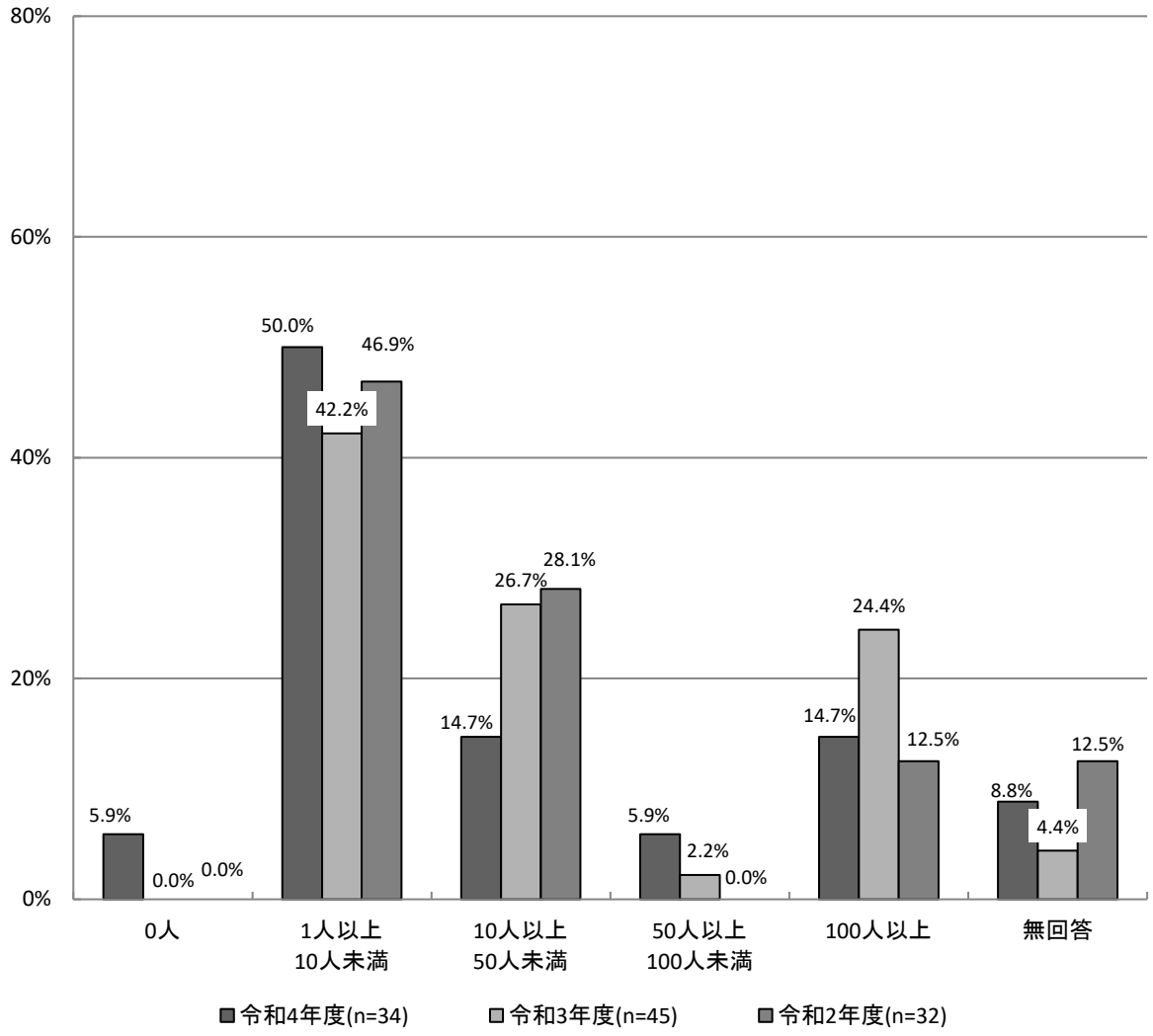


5.3.2　研究開発に携わっている人数　【A-問7】

【経年変化】
　全体では「10人以上50人未満」「100人以上」で減少している。企業では「0人」などが増加している一方で「1人以上10人未満」などが減少している。大学では、「1人以上10人未満」が最も増加している。

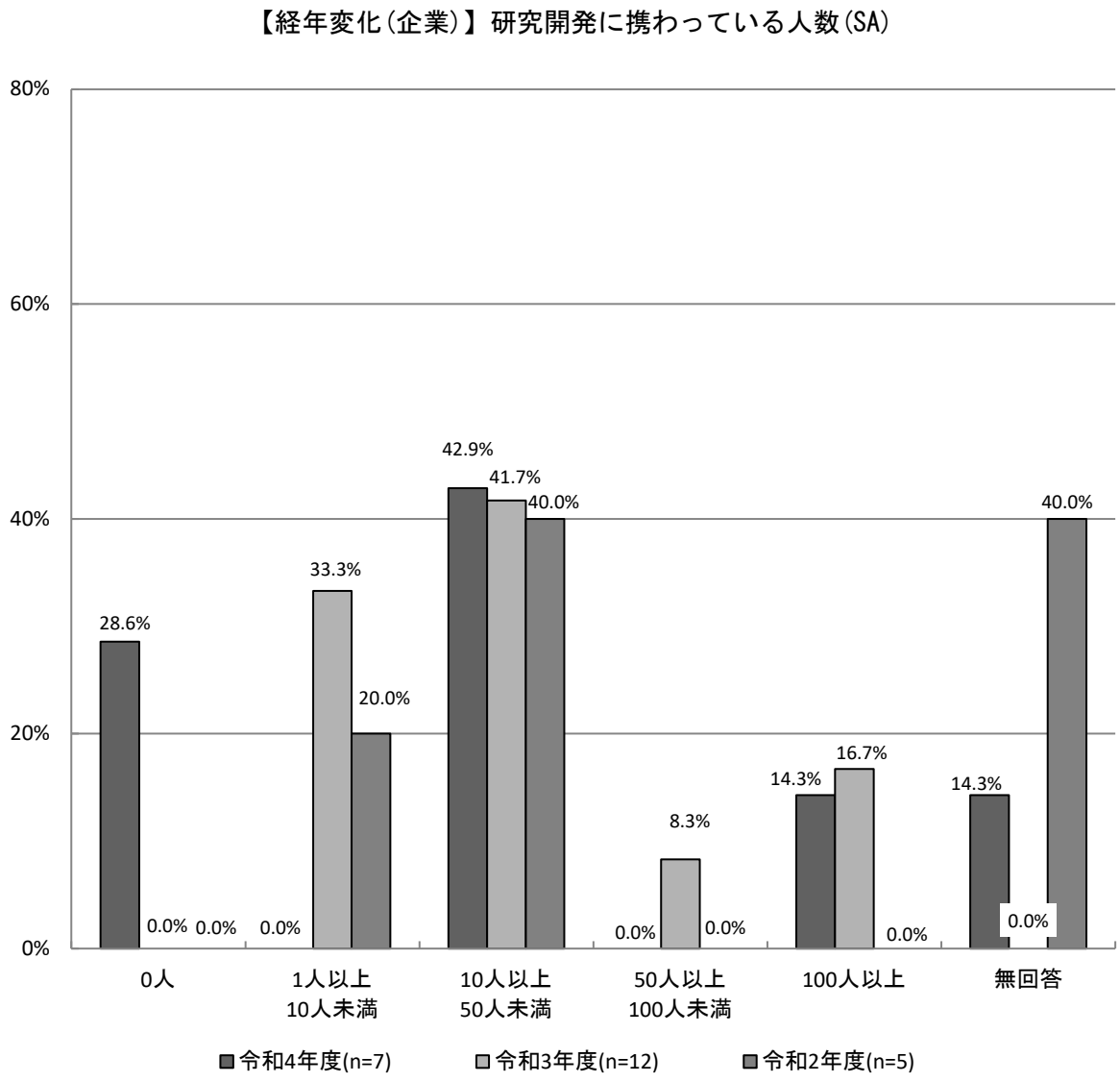
【経年変化(全体)】
　昨年度と比較すると全体では、「10人以上50人未満」が12.0ポイントと最も減少しており、次いで「100人以上」が9.7ポイント減少している。

【経年変化(全体)】研究開発に携わっている人数(SA)



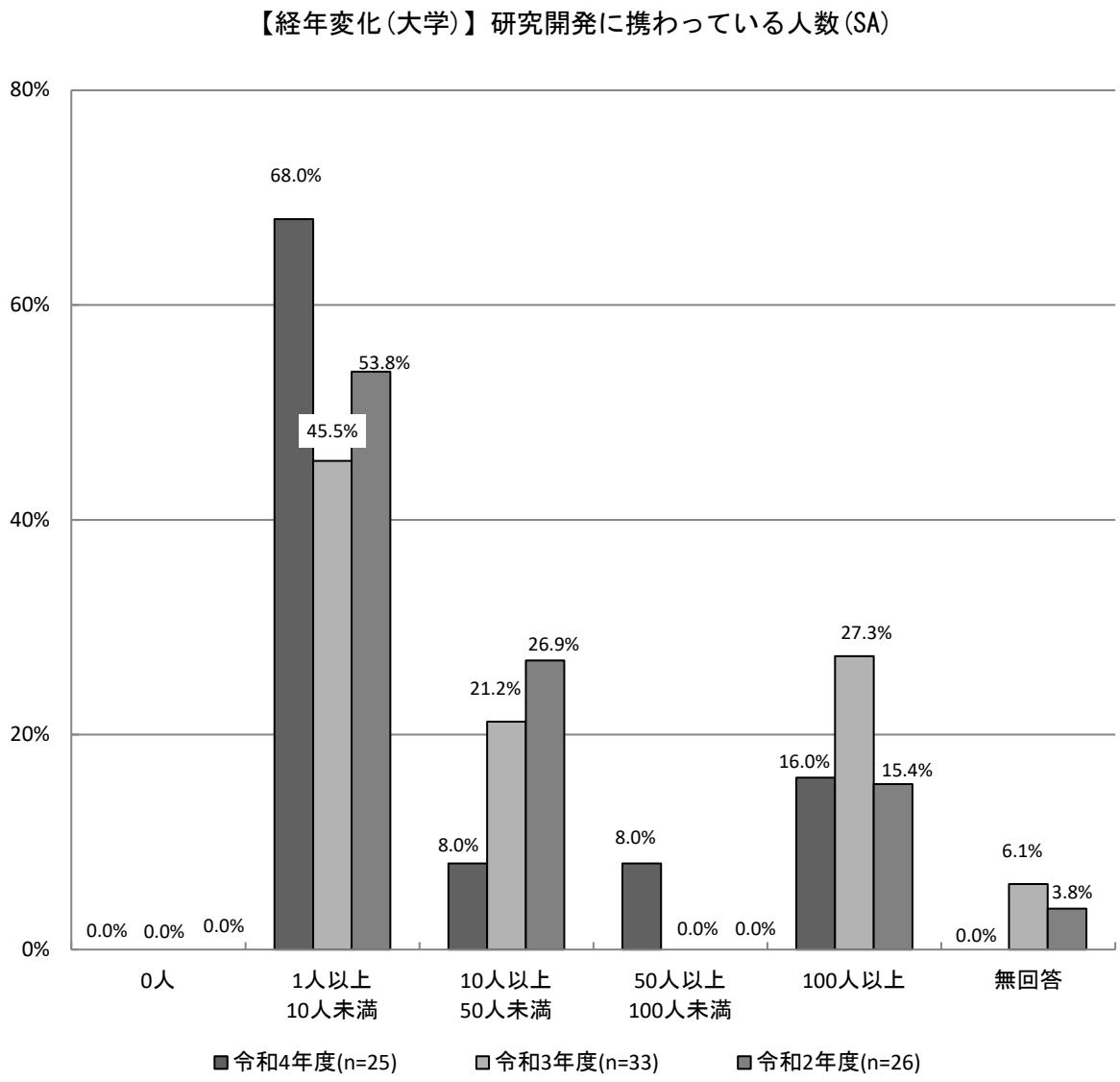
【経年変化(企業)】

昨年度と比較すると企業では、「0人」が28.6ポイント増加している。一方「1人以上10人未満」が33.3ポイント減少している。



【経年変化(大学)】

昨年度と比較すると大学では、「1人以上10人未満」が22.5ポイントと最も増加しており、次いで「50人以上100人未満」が8.0ポイント増加している。一方「10人以上50人未満」は13.2ポイント減少している。



5.4 実用化された製品及び研究開発中の技術・サービス

『回答用紙B』『回答用紙C』により調査した、研究開発中及び実用化された技術・サービスの動向について考察した。調査項目は、下記の内容について複数選択で聞いている。

(1)何を守るか？

・どのコンポーネントを守るのか、という観点から見た分類。

・ネットワーク、サーバ、クライアント等の大きなくくりの視点で見る。

(2)何から保護するか？

・どのような脅威から守るのか、という観点から見た分類。

・買う側の立場から見て、どのような対策をしたいかという視点でもある。

(3)どのようなセキュリティ上の効果があるか？

・どのような効果を狙ったものか、という観点から見た分類。

・事前対応、事中・事後対応という視点でもある。

(4)どのような機能を持っているか？

・どのような技術要素を使って守るのか、という観点から見た分類。

・売る側や開発する側の立場から見た、機能要素という視点でもある。

(5)どのようなレイヤーのセキュリティを守るか？

・どのようなレイヤーでセキュリティを守るのか、という観点から見た分類。

(6)どのようなサービスか？

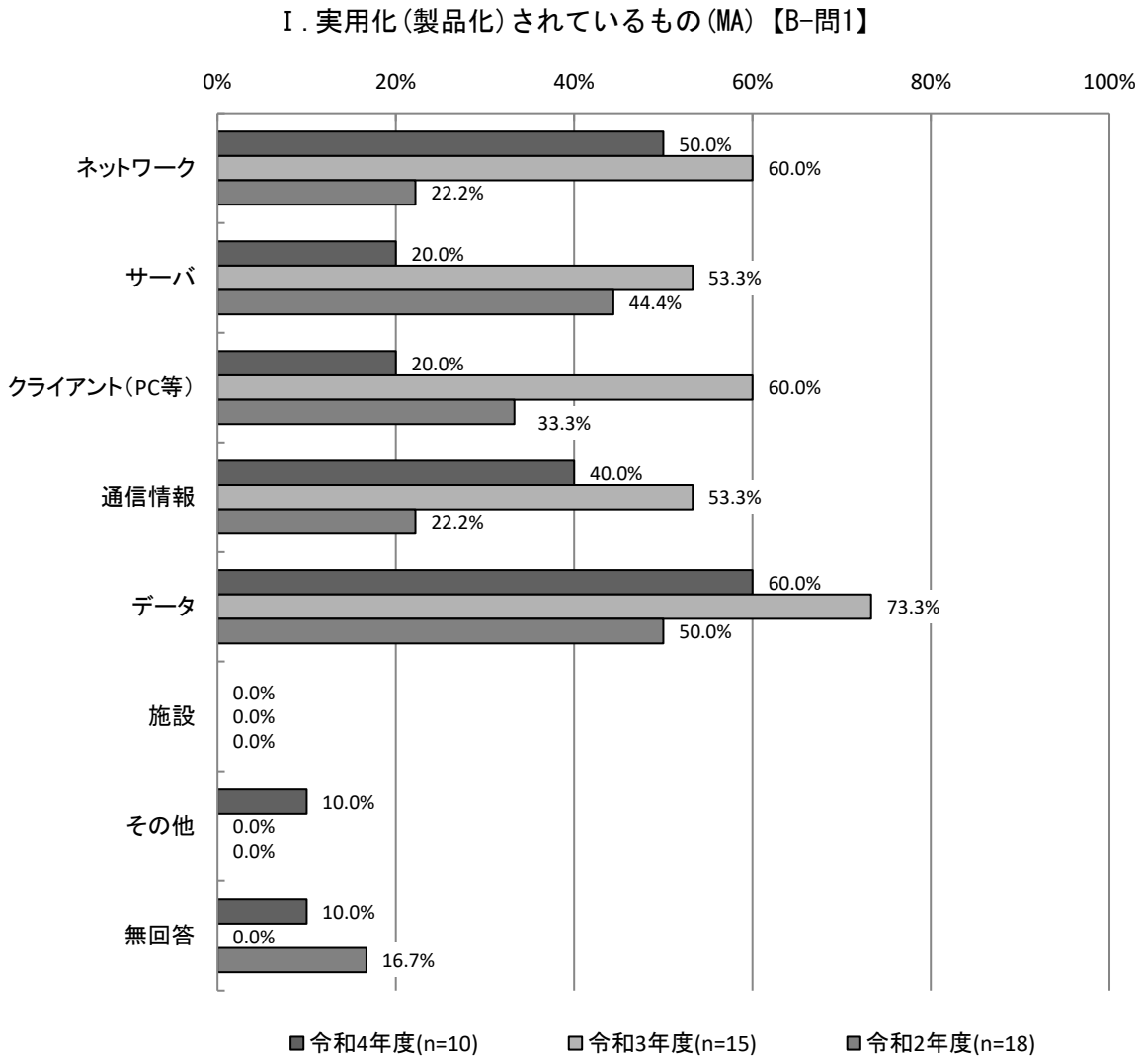
・サービスの場合、どのような内容か、という観点から見た分類。

5.4.1　何を守るか？

Ⅰ.実用化(製品化)されているもの

実用化（製品化）されているものについては、「データ」が60.0%（6件）で最も多く、次いで「ネットワーク」が50.0%（5件）となっている。

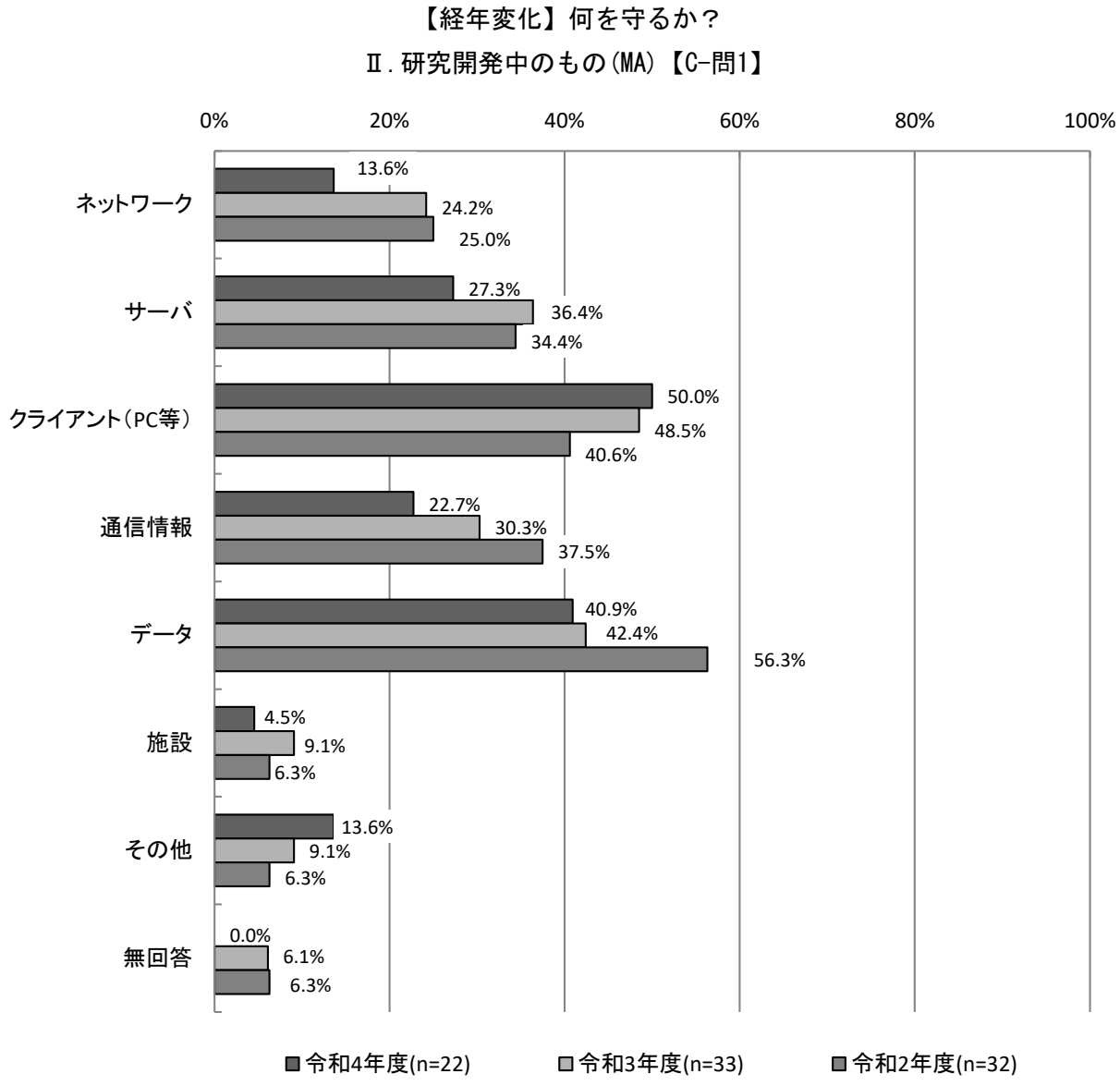
昨年度と比較すると、「クライアント（PC等）」が40.0ポイント、「サーバ」が33.3ポイント減少している。



Ⅱ.研究開発中のもの

研究開発中のものについては、「クライアント（PC等）」が50.0％（11件）で最も多く、次いで「データ」が40.9％（9件）、「サーバ」が27.3％（6件）となっている。

昨年度と比較すると、「ネットワーク」が10.6ポイントと最も減少しており、次いで「サーバ」が9.1ポイント減少している。

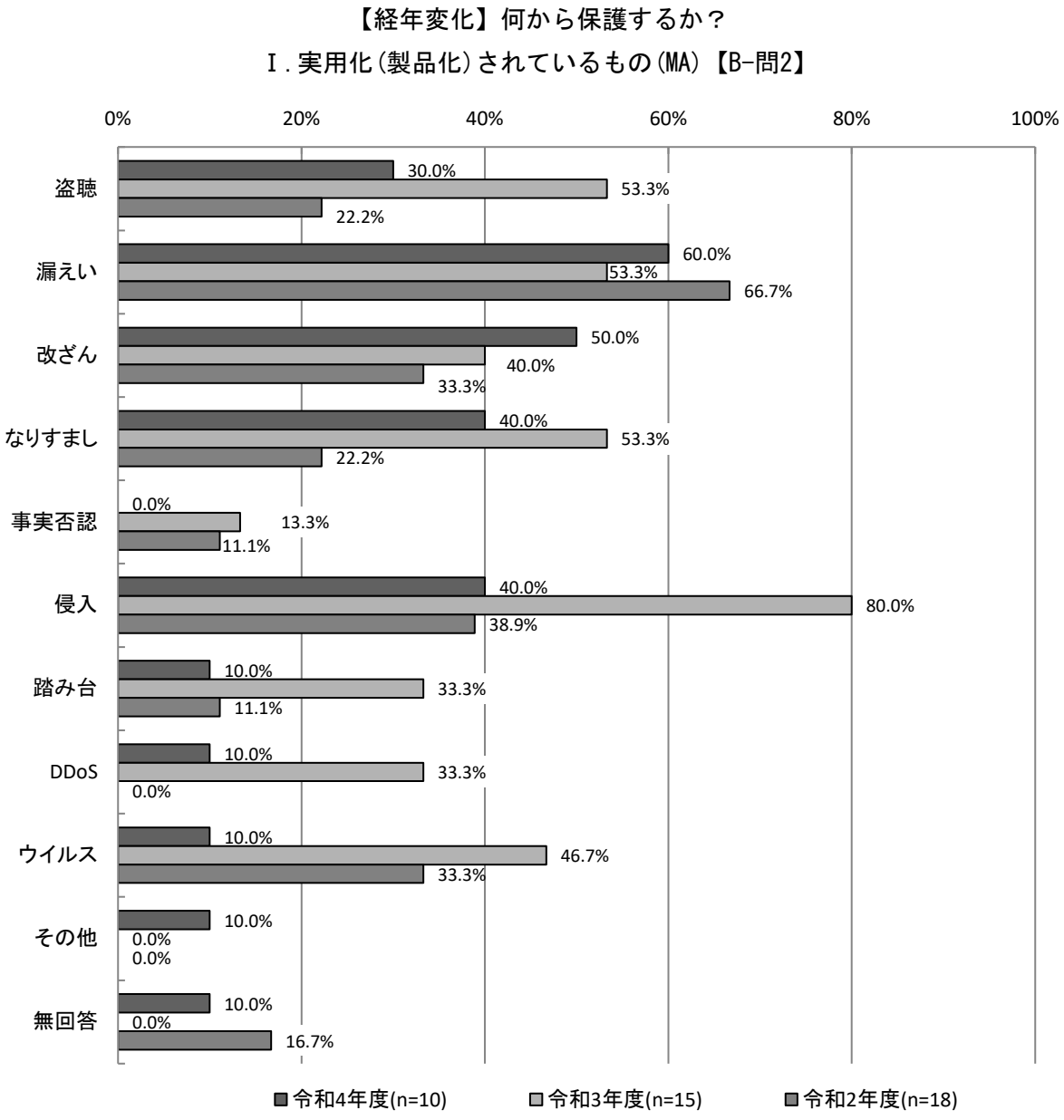


5.4.2　何から保護するか？

Ⅰ.実用化(製品化)されているもの

実用化（製品化）されているものについては、「漏えい」が60.0%（6件）で最も多く、次いで「改ざん」が50.0%（5件）となっている。

昨年度と比較すると、「改ざん」が10.0ポイント増加している。一方「侵入」が40.0ポイントで最も減少しており、次いで「ウイルス」が36.7ポイント減少している。



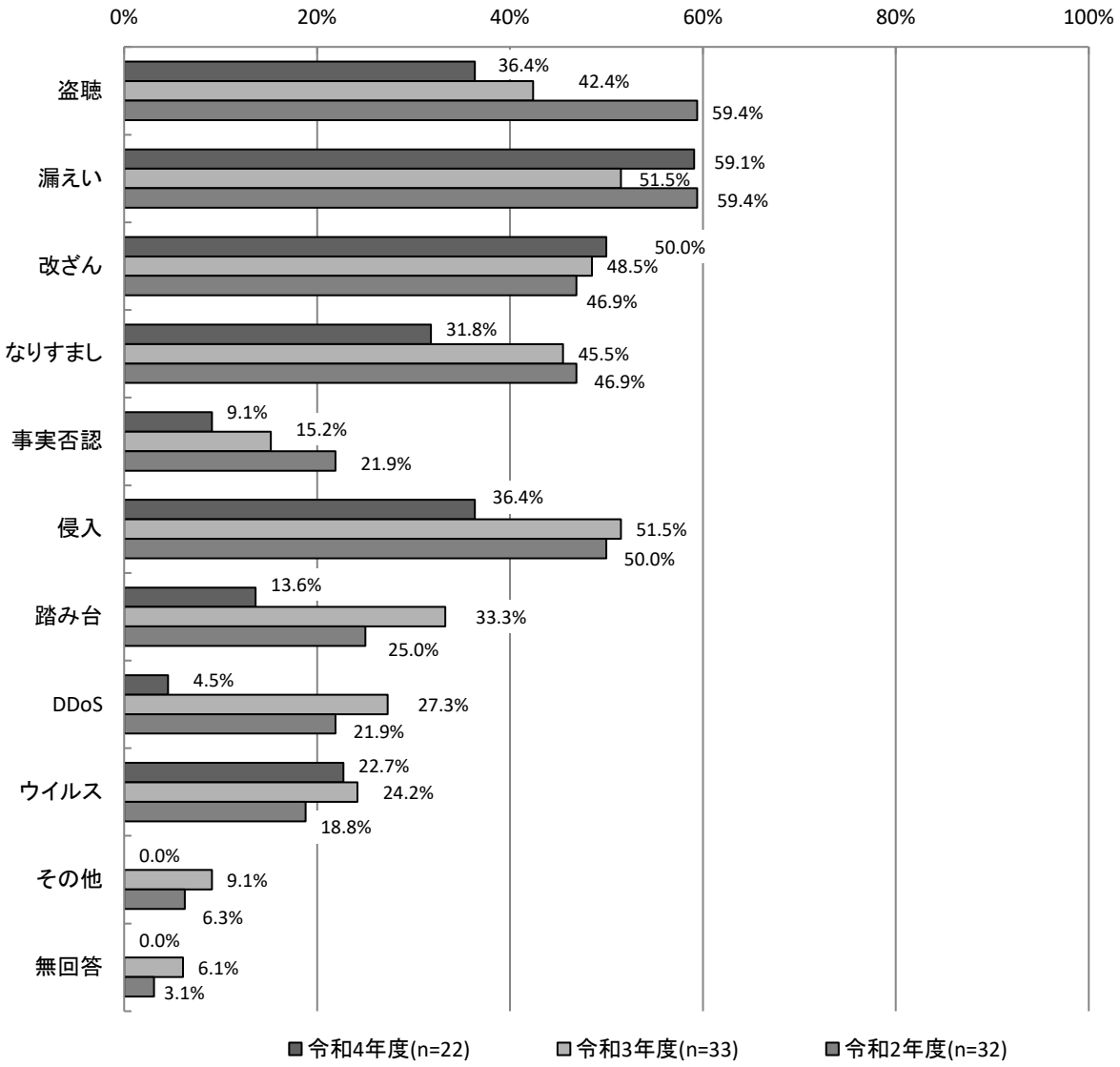
Ⅱ.研究開発中のもの

研究開発中のものについては、「漏えい」が59.1%（13件）で最も多く、次いで「改ざん」が50.0%（11件）となっている。

昨年度と比較すると、「漏えい」が7.6ポイントで増加している。一方「DDoS」が22.8ポイントと最も減少しており、次いで「踏み台」が19.7ポイント減少している。

【経年変化】何から保護するか？

Ⅱ.研究開発中のもの(MA)【C-問2】



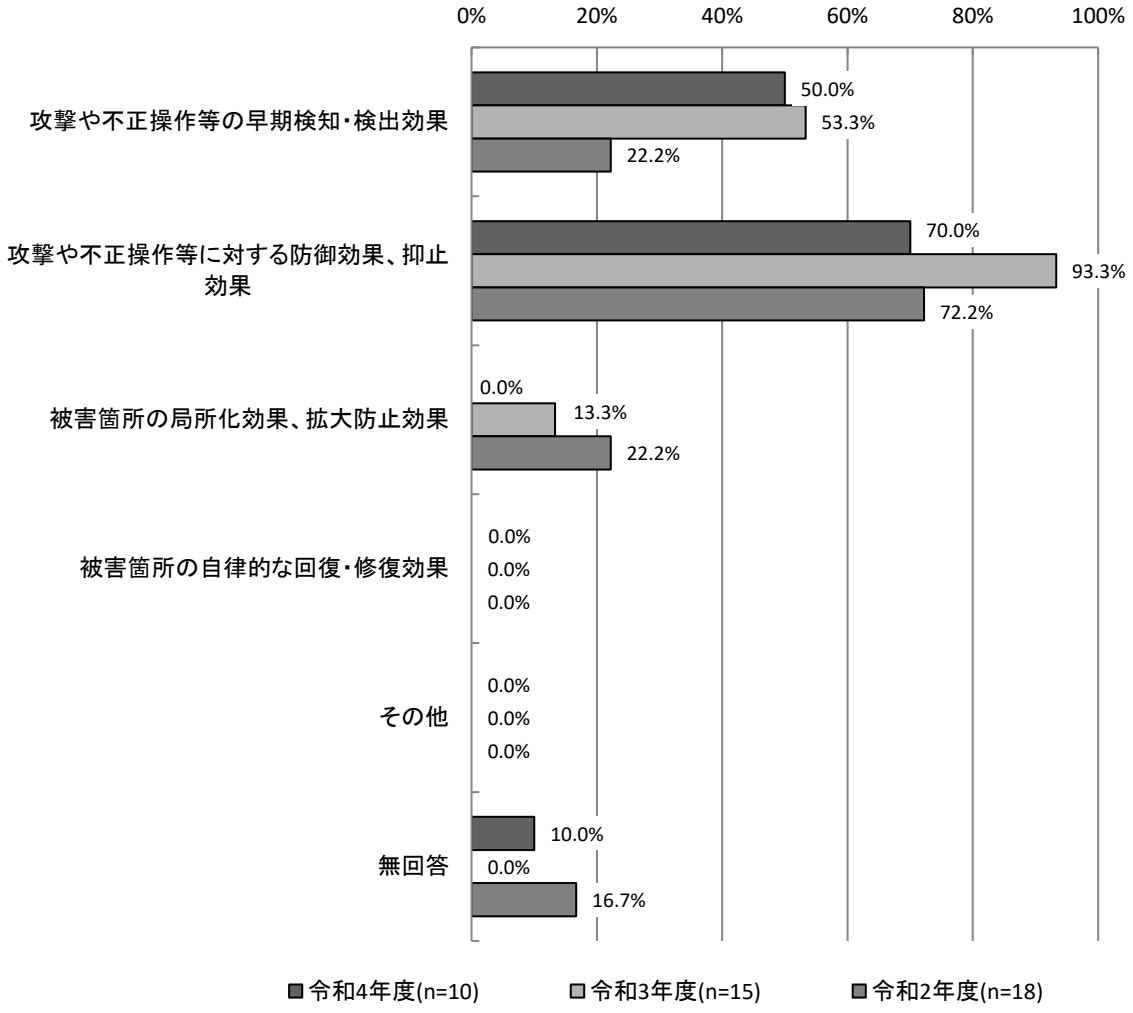
5.4.3　どのようなセキュリティ上の効果があるか？

Ⅰ.実用化(製品化)されているもの

実用化（製品化）されているものについては、「攻撃や不正操作等に対する防御効果、抑止効果」が70.0%（7件）で最も多くなっている。

昨年度と比較すると、「攻撃や不正操作等に対する防御効果、抑止効果」が23.3ポイントで最も減少している。

【経年変化】どのようなセキュリティ上の効果があるか？
Ⅰ.実用化(製品化)されているもの(MA)【B-問3】

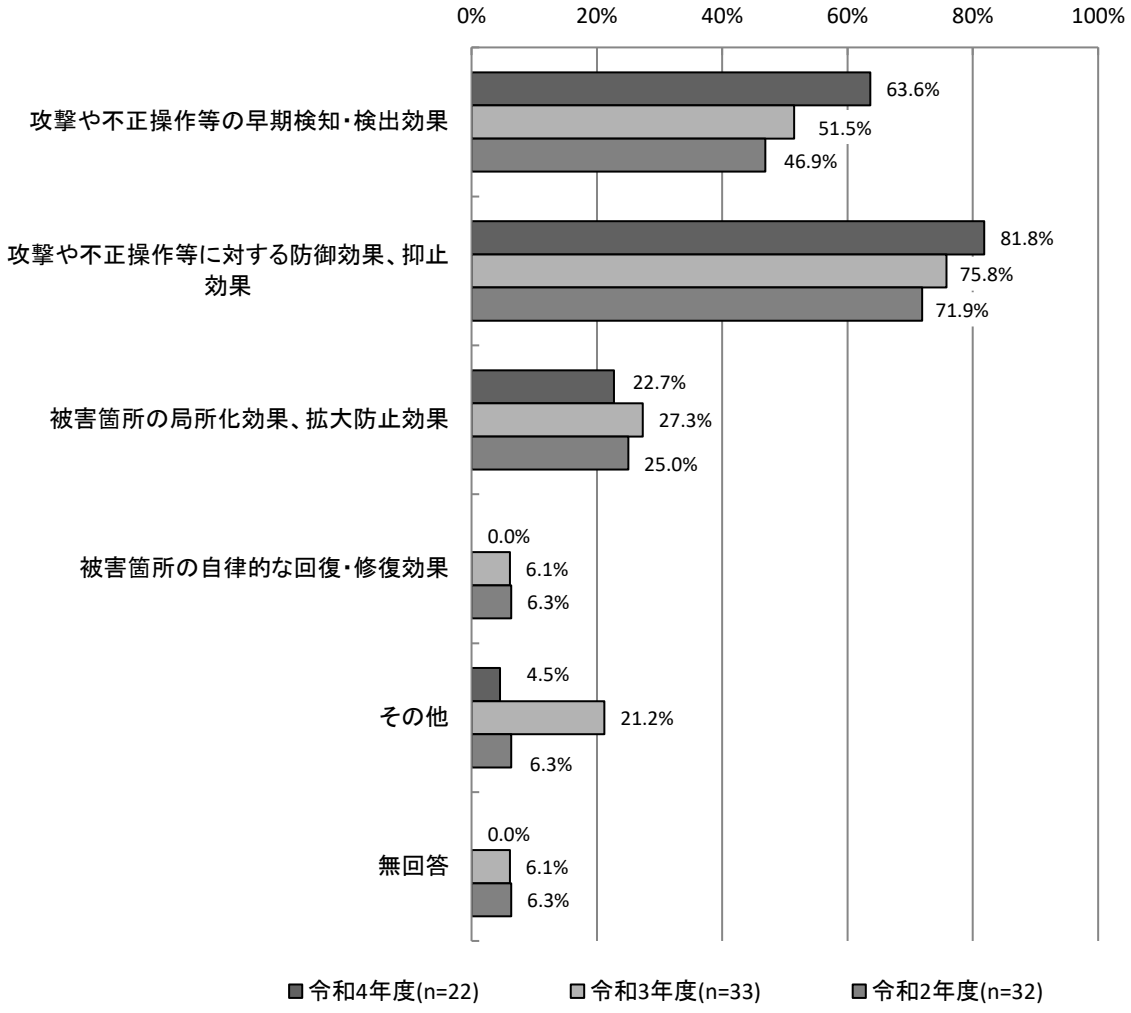


Ⅱ.研究開発中のもの

研究開発中のものについては、「攻撃や不正操作等に対する防御効果、抑止効果」が81.8%（18件）と最も多く、次いで「攻撃や不正操作等の早期検知・検出効果」が63.6%（14件）となっている。

昨年度と比較すると、「攻撃や不正操作等の早期検知・検出効果」が12.1ポイント、「攻撃や不正操作等に対する防御効果、抑止効果」が6.0ポイント増加している。

【経年変化】どのようなセキュリティ上の効果があるか？
Ⅱ.研究開発中のもの(MA)【C-問3】



5.4.4　どのような機能を持つか？

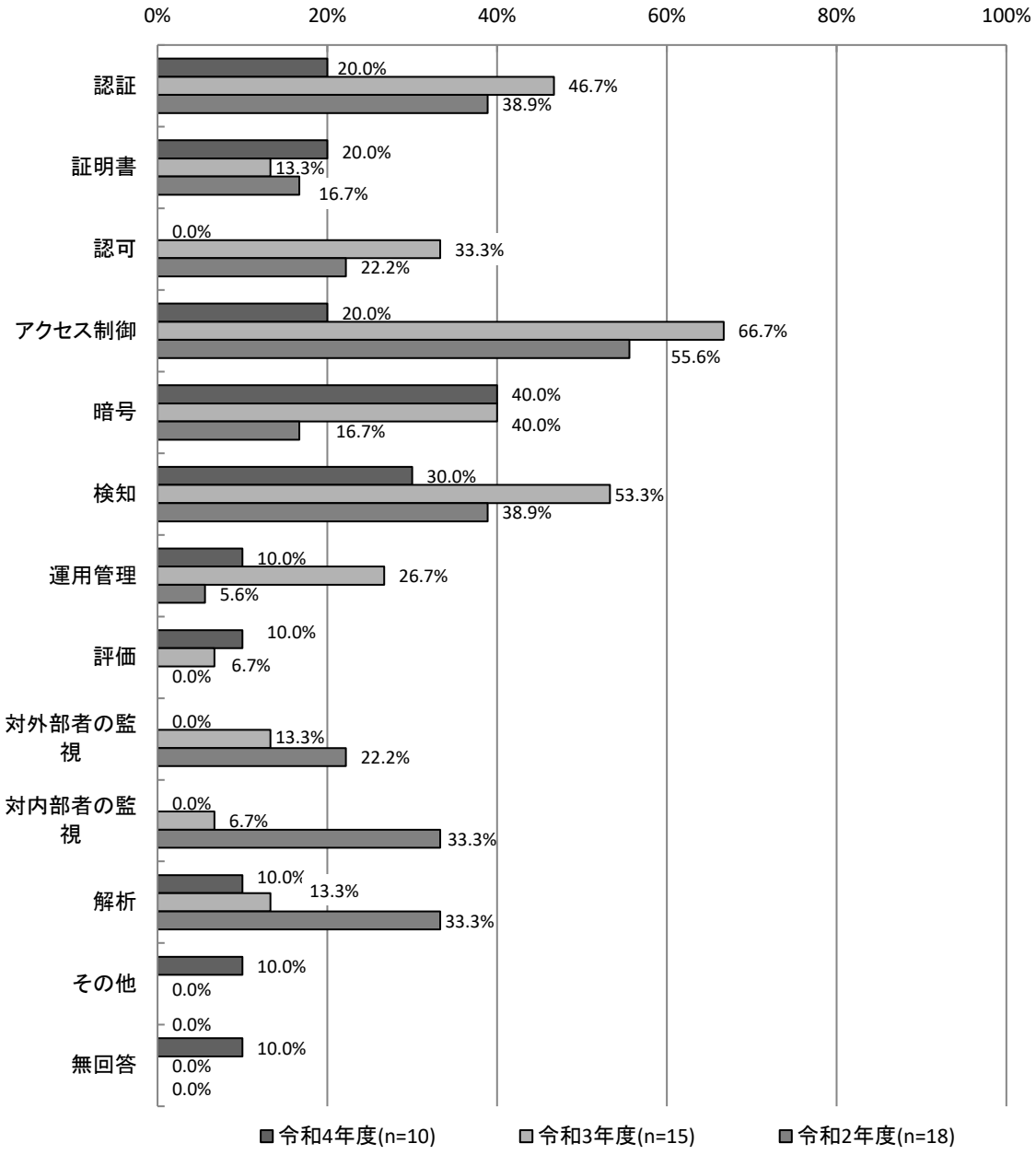
Ⅰ.実用化(製品化)されているもの

実用化（製品化）されているものについては、「暗号」が40.0%（4件）で最も多く、次いで「検知」が30.0%（3件）となっている。

昨年度と比較すると、「証明書」が6.7ポイントと最も増加している。一方で「アクセス制御」が46.7ポイントと最も減少しており、次いで「認可」が33.3ポイント減少している。

【経年変化】どのような機能を持つか？

Ⅰ.実用化(製品化)されているもの(MA)【B-問4】



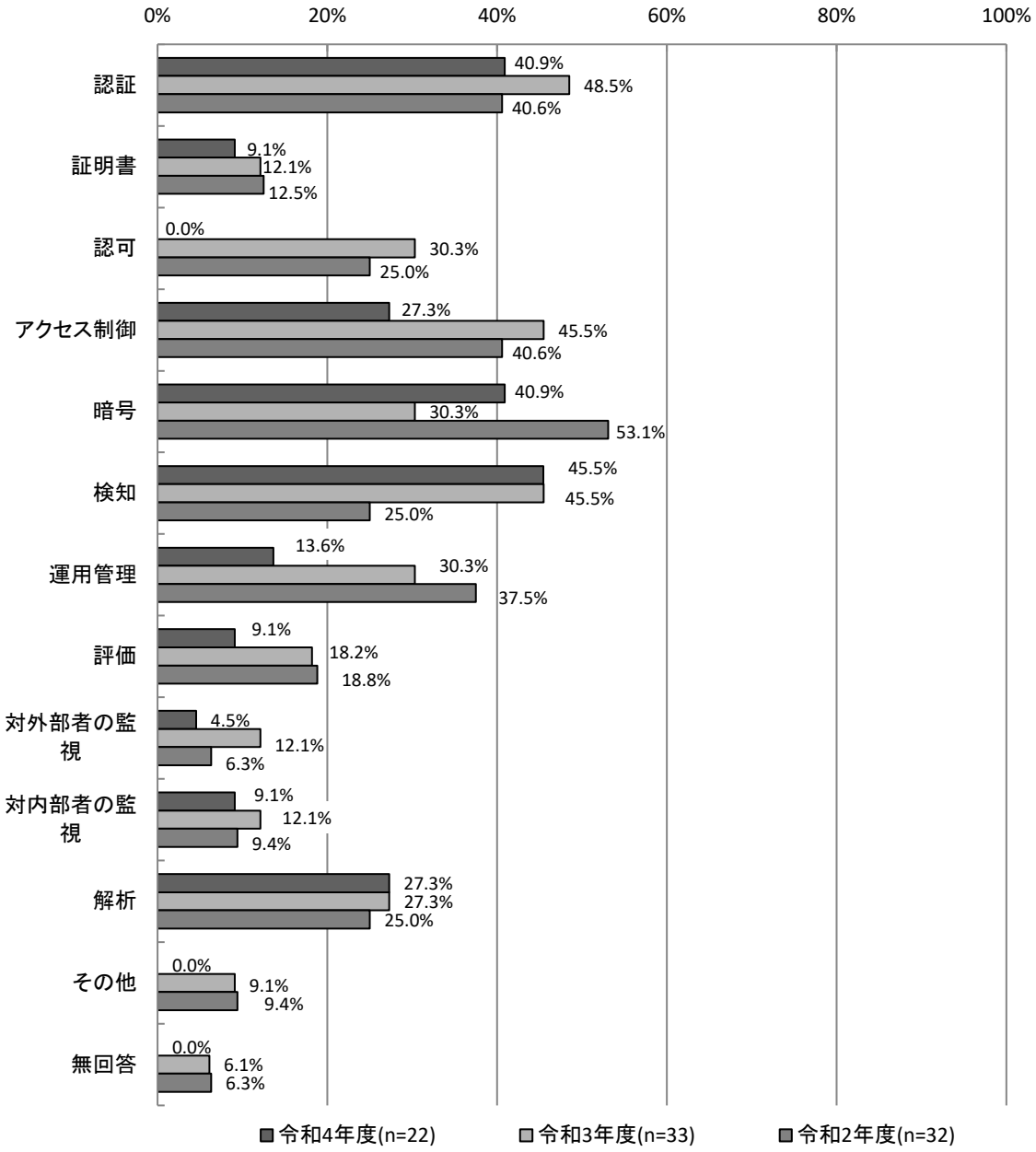
Ⅱ.研究開発中のもの

研究開発中のものについては、「検知」が45.5%（10件）で最も多く、次いで「暗号」「認証」がそれぞれ40.9%（9件）となっている。

昨年度と比較すると、「暗号」が10.6ポイント増加している。一方、「認可」は30.3ポイントと最も減少している。

【経年変化】どのような機能を持つか？

Ⅱ.研究開発中のもの(MA)【C-問4】



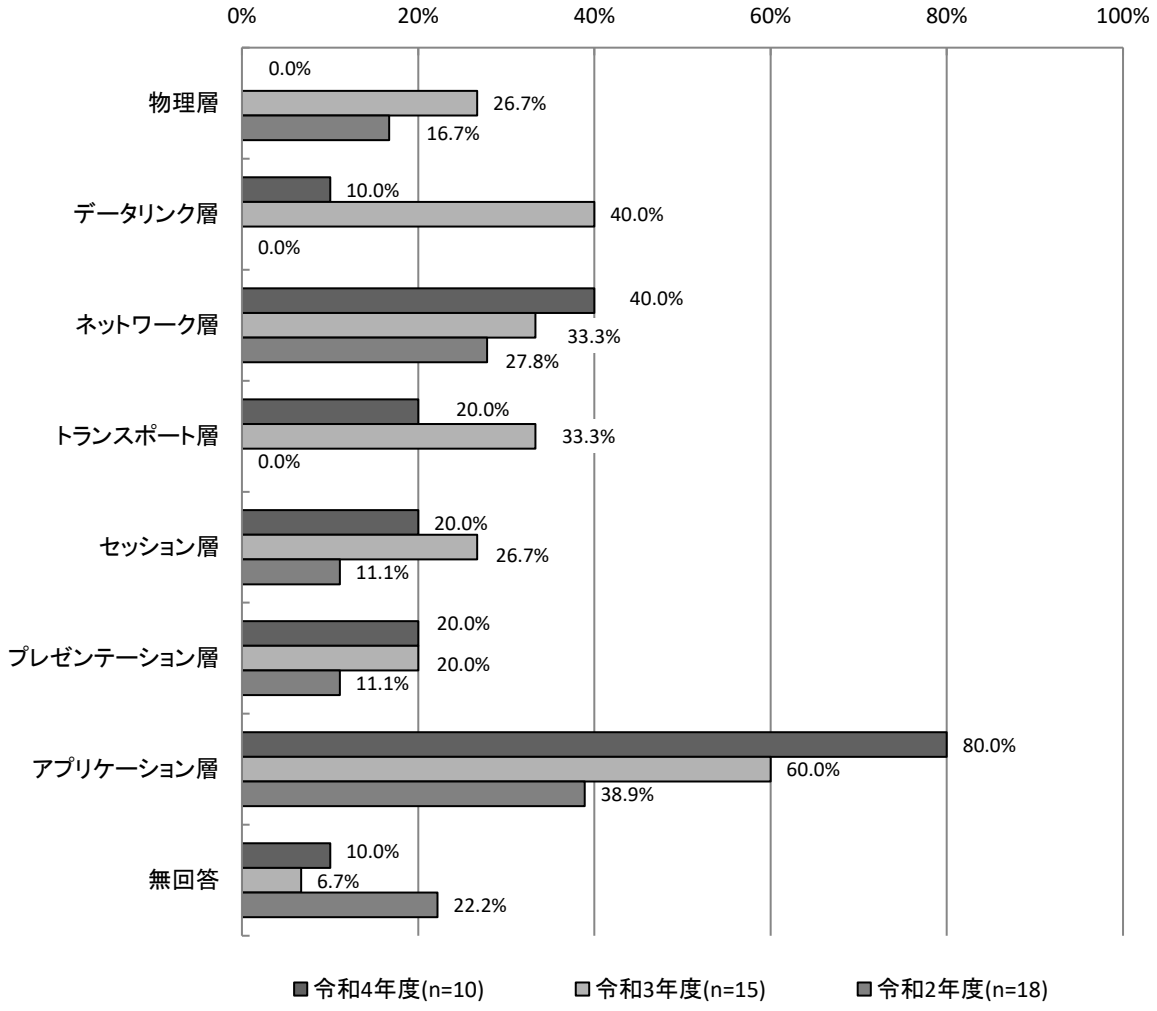
5.4.5　どのようなレイヤーのセキュリティを守るか？

Ⅰ.実用化(製品化)されているもの

実用化（製品化）されているものについては、「アプリケーション層」が80.0%（8件）で最も多く、次いで「ネットワーク層」が40.0%（4件）となっている。

昨年度と比較すると、「アプリケーション層」が20.0ポイント増加している。一方「データリンク層」が30.0ポイントと最も減少しており、次いで「物理層」が26.7ポイント減少している。

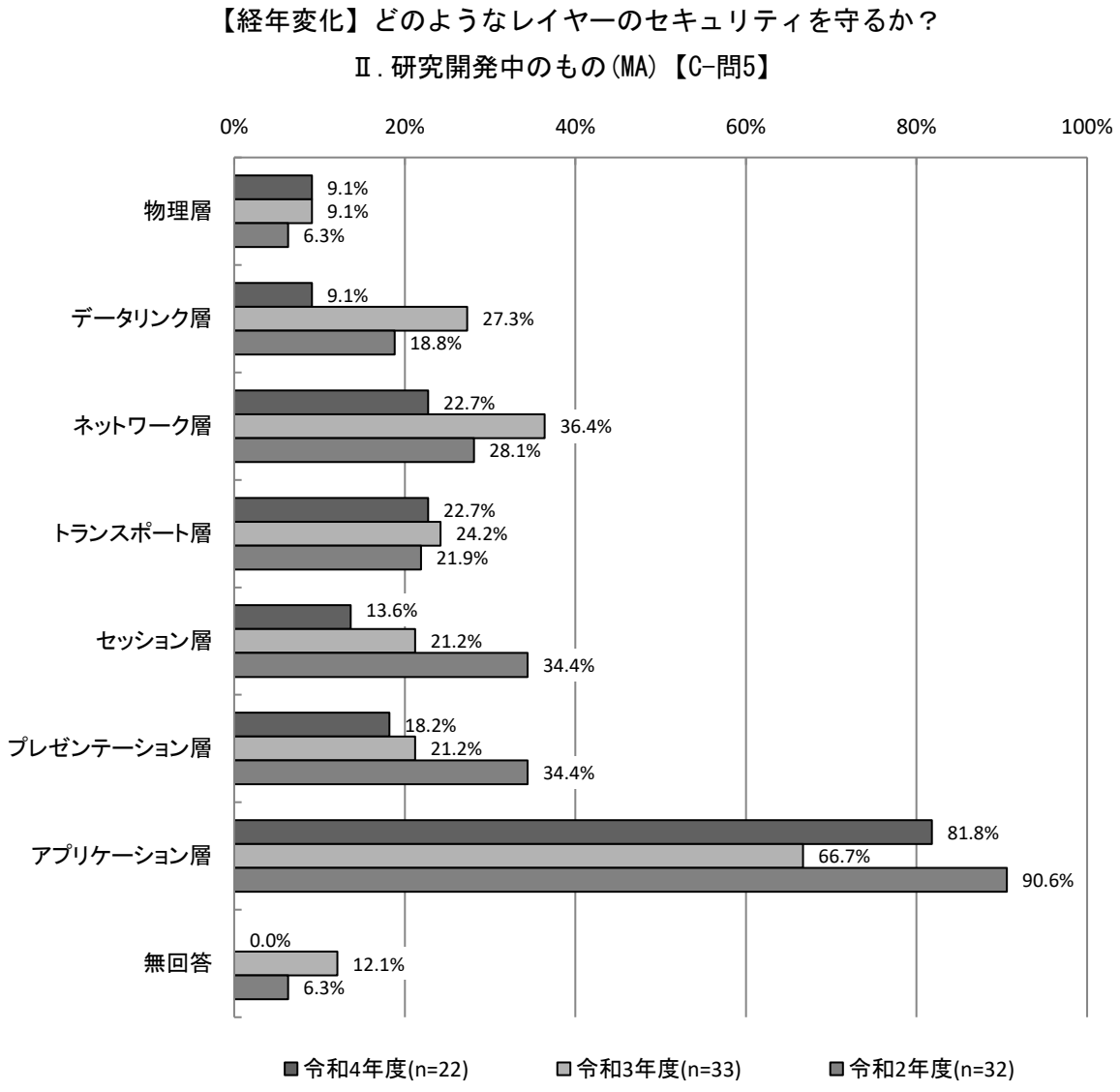
【経年変化】どのようなレイヤーのセキュリティを守るか？
Ⅰ.実用化(製品化)されているもの(MA)【B-問5】



Ⅱ.研究開発中のもの

研究開発中のものについては、「アプリケーション層」が81.8%（18件）で最も多く、次いで「ネットワーク層」「トランスポート層」がそれぞれ22.7%（5件）となっている。

昨年度と比較すると、「アプリケーション層」が15.1ポイント増加している。一方、「データリンク層」が18.2ポイントと最も減少しており、次いで「ネットワーク層」がそれぞれ13.7ポイント減少している。



5.4.6　不正アクセスからの防御対象

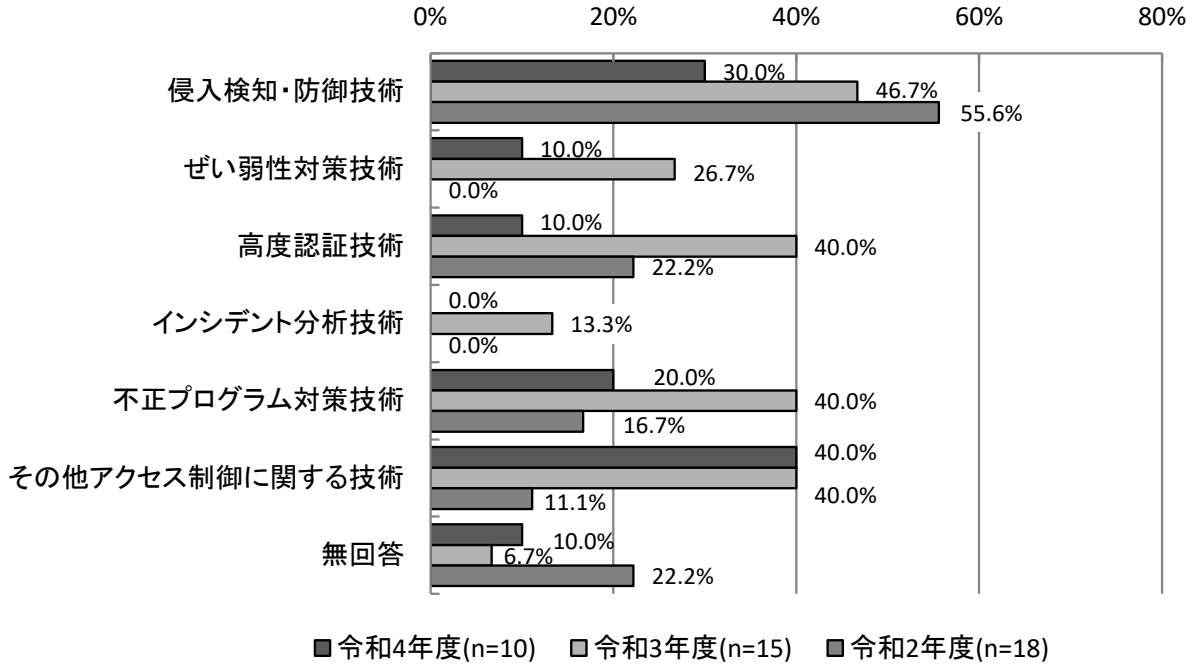
Ⅰ.実用化(製品化)されているもの

実用化（製品化）されているものについては、「侵入検知・防御技術」が30.0%（3件）で最も多くなっている。

昨年度と比較すると、「高度認証技術」が30.0ポイントと最も減少している。次いで「不正プログラム対策技術」が20.0ポイント減少している。

【全体】不正アクセスからの防御対象

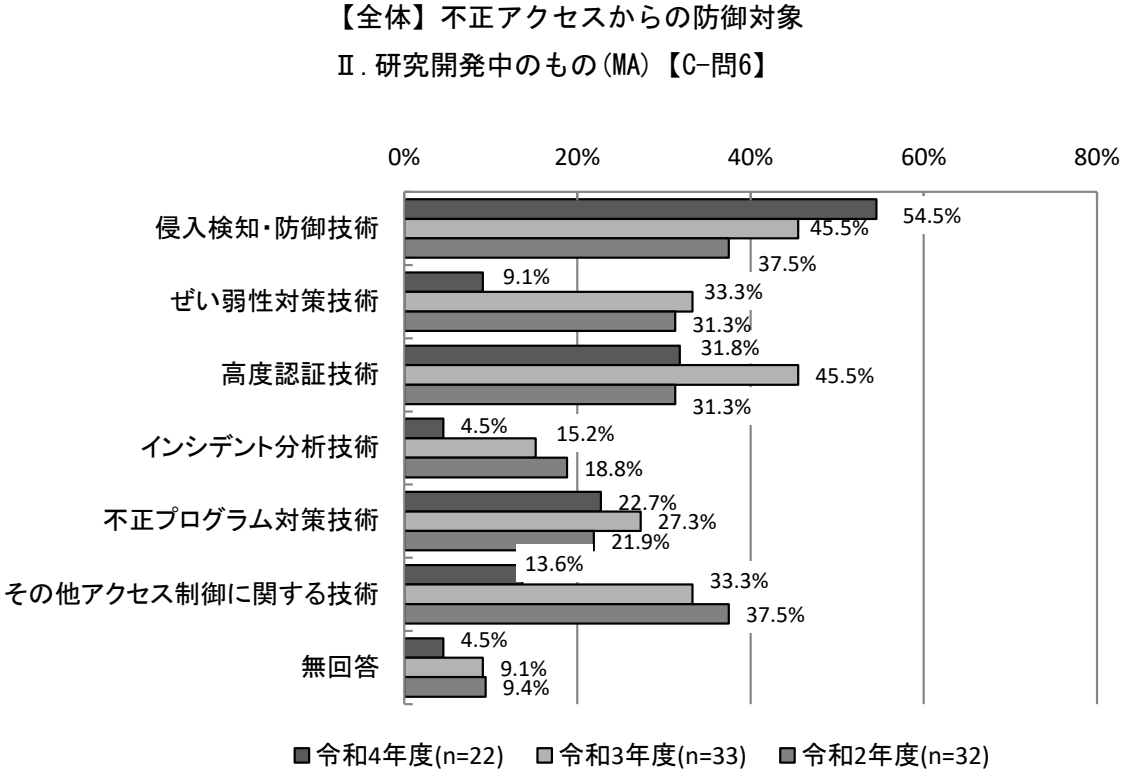
Ⅰ.実用化(製品化)されているもの(MA)【B-問6】



Ⅱ.研究開発中のもの

研究開発中のものについては、「侵入検知・防御技術」が54.5%（12件）で最も多くなっている。次いで、「高度認証技術」が31.8%（7件）で増加している。

昨年度と比較すると、「侵入検知・防御技術」が9.0ポイント増加している。一方、「ぜい弱性対策技術」が24.2ポイントと最も減少している。



5.4.7　どのようなサービスか？

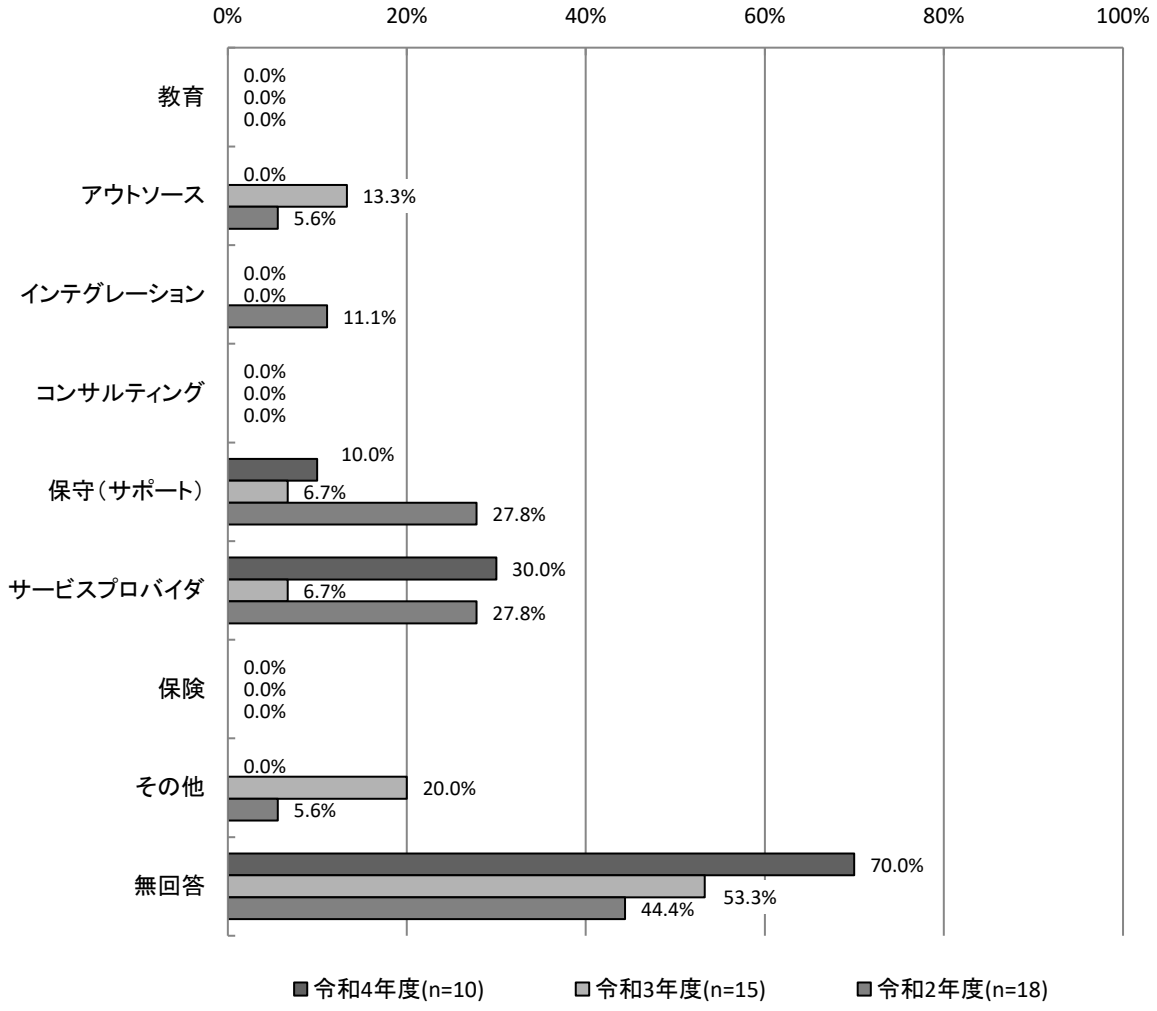
Ⅰ.実用化(製品化)されているもの

実用化（製品化）されているものについては、「サービスプロバイダ」が30.0%（3件）、「保守（サポート）」が10.0%（1件）となっている。

昨年度と比較すると、「サービスプロバイダ」が23.3ポイントと増加している。一方「アウトソース」が13.3ポイント減少している。

【経年変化】どのようなサービスか？

Ⅰ.実用化(製品化)されているもの(MA)【B-問7】



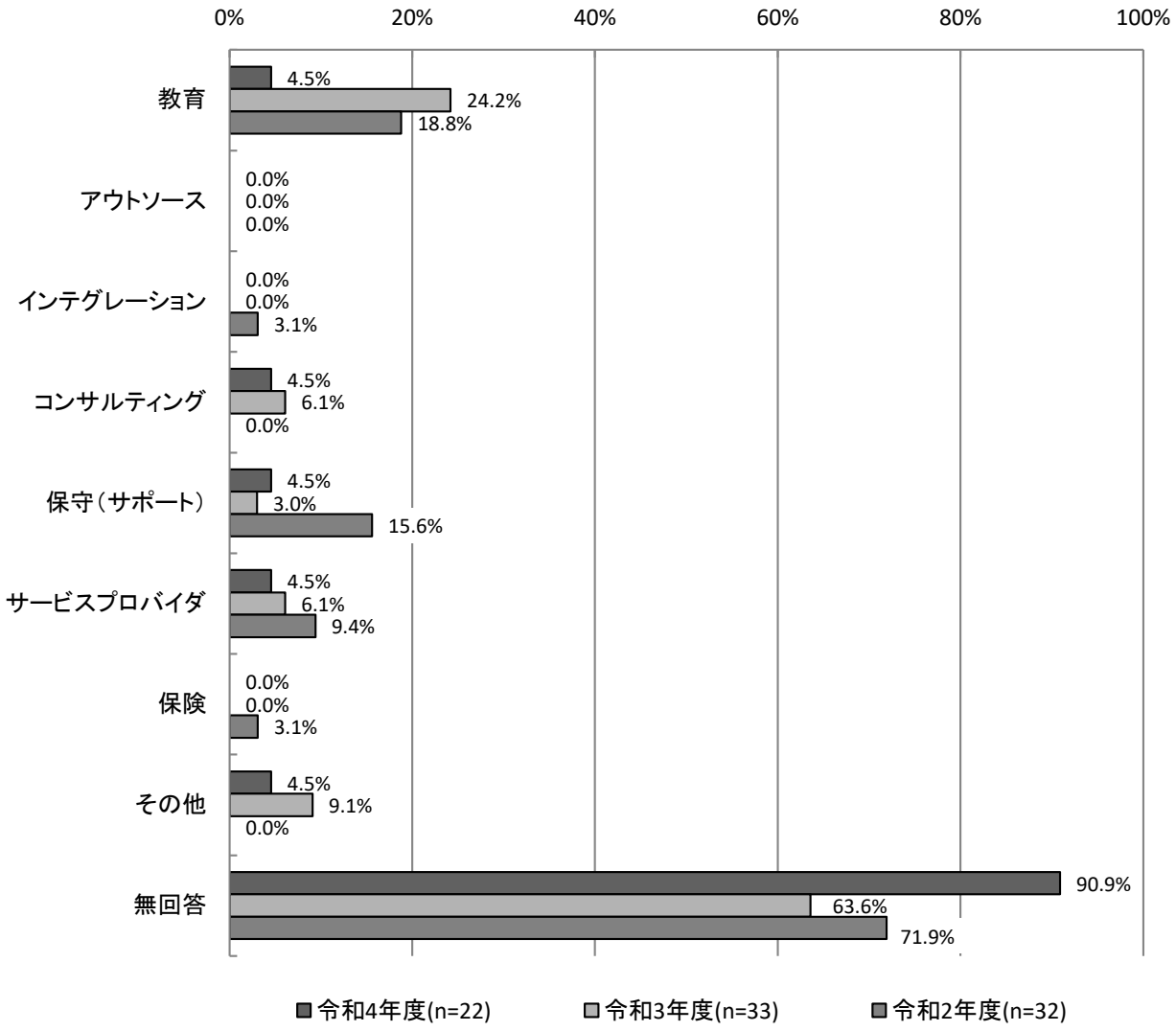
Ⅱ.研究開発中のもの

研究開発中のものについては、「教育」「コンサルティング」「保守(サポート)」「サービスプロバイダ」が4.5%（1件）となっている。

昨年度と比較すると、「保守」が1.5ポイント増加している。一方、「教育」は19.7ポイントと最も減少している。

【経年変化】どのようなサービスか？

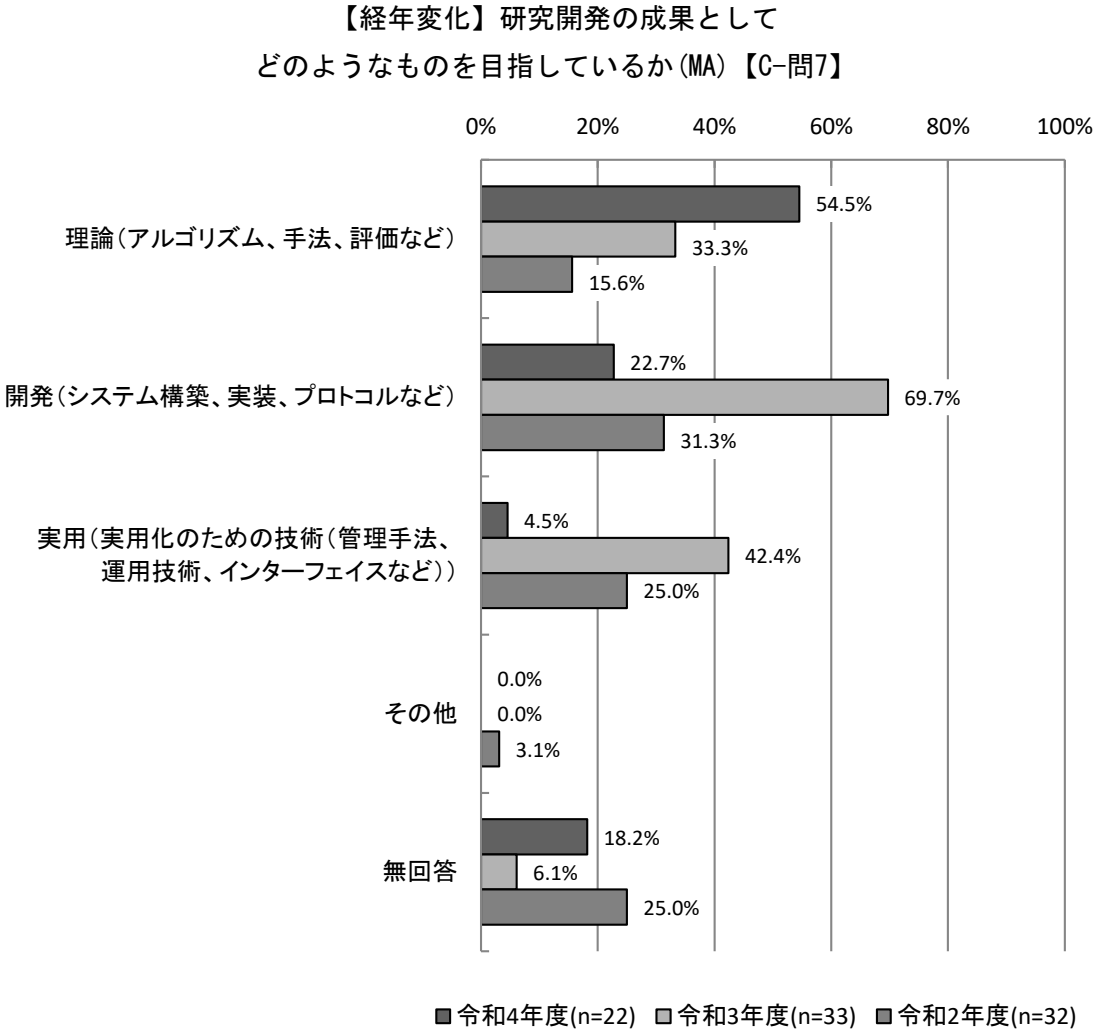
Ⅱ.研究開発中のもの(MA)【C-問8】



5.5 研究開発の成果としてどのようなものを目指しているか？

研究開発の目指す成果については、「理論（アルゴリズム、手法、評価など)」が54.5%（12件）で最も多く、次いで「開発（システム構築、実装、プロトコルなど)」が22.7%（5件)、「実用（実用化のための技術（管理手法、運用技術、インターフェイスなど))」が4.5%（1件）となっている。

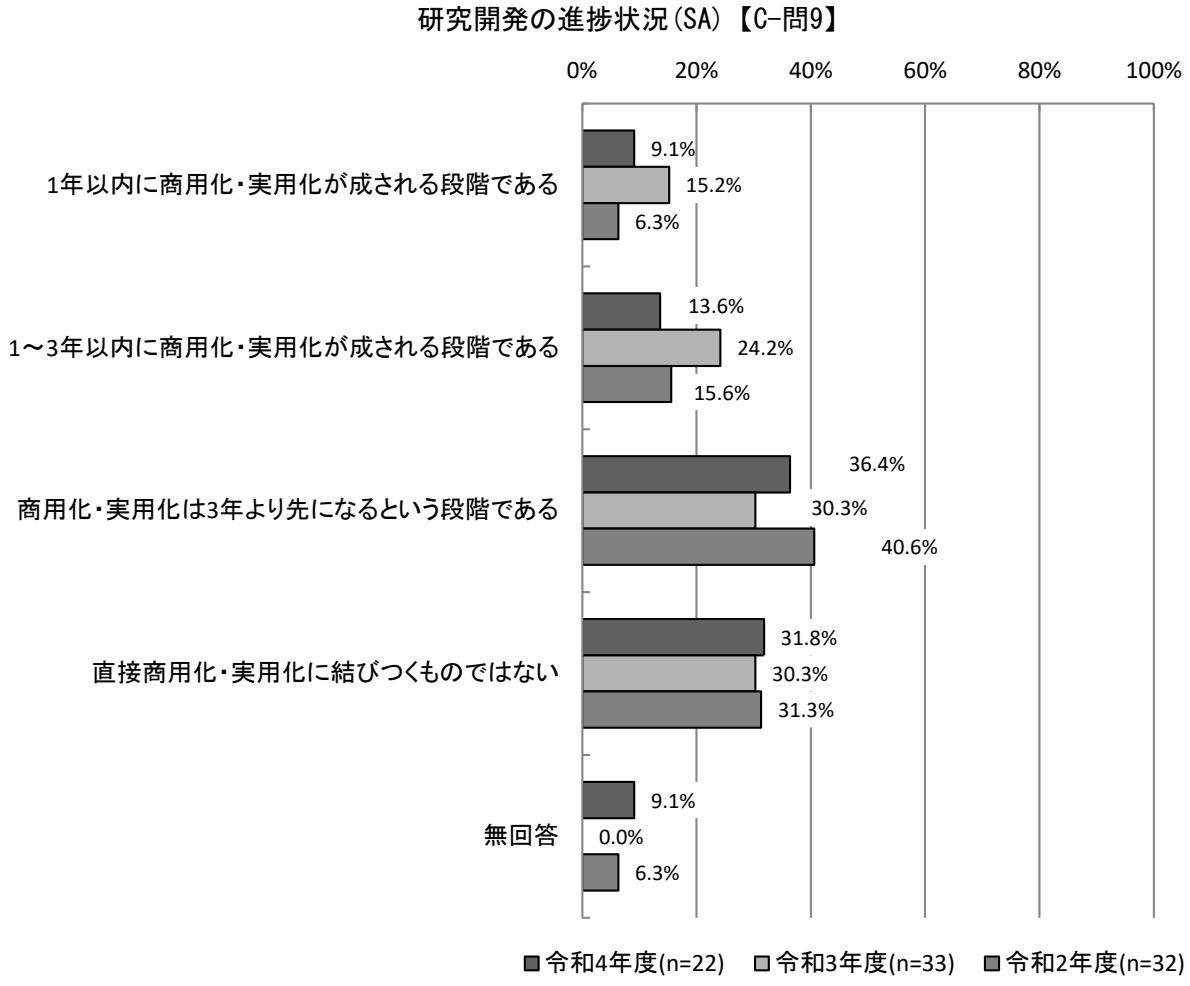
昨年度と比較すると、「理論（アルゴリズム、手法、評価など)」が21.2ポイント増加している。一方「開発（システム構築、実装、プロトコルなど)」が47.0ポイントと最も減少しており、次いで「実用（実用化のための技術（管理手法、運用技術、インターフェイスなど))」が37.9ポイント減少している。



5.6 研究開発の進捗状況

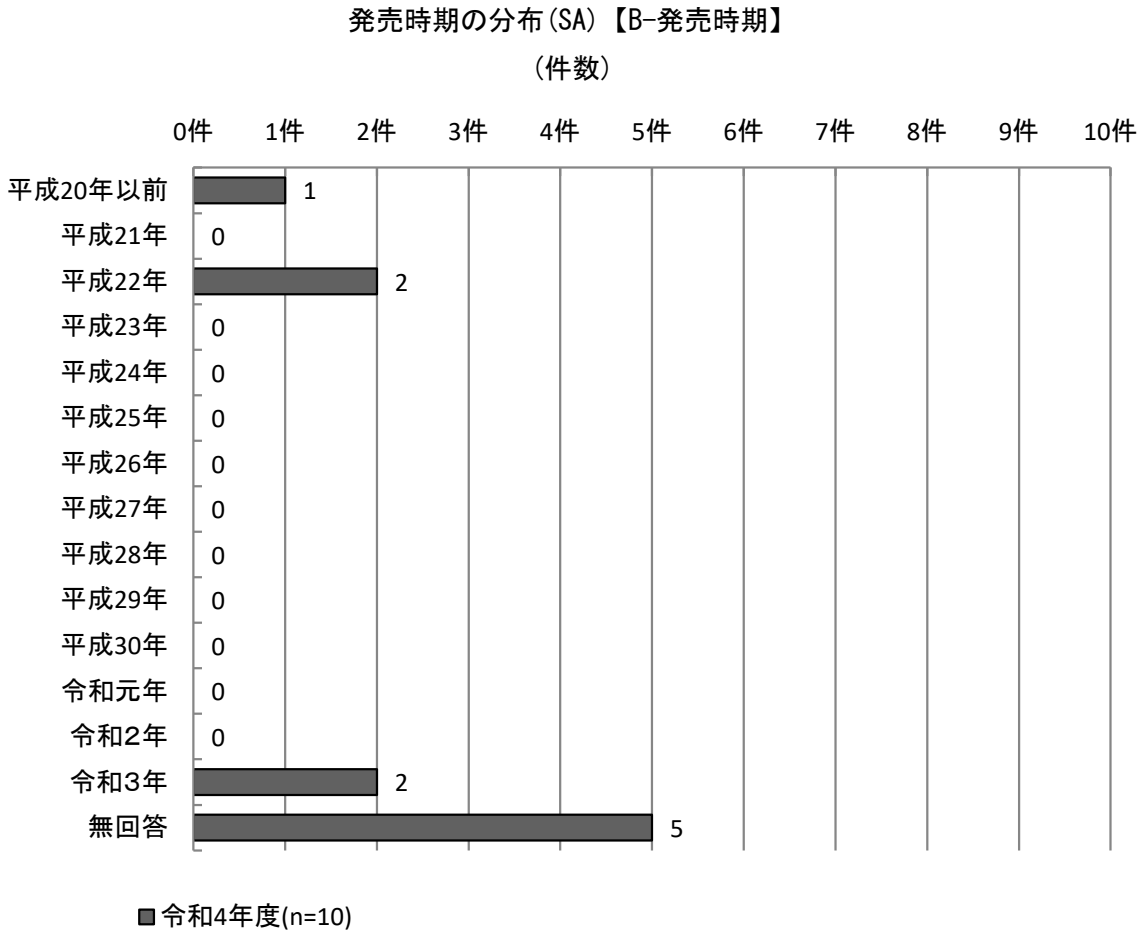
研究開発の進捗状況については、「商用化・実用化は3年より先になるという段階である」が36.4%（8件）と最も多い。次いで「直接商用化・実用化に結びつくものではない」が31.8%（7件）となっている。

昨年度と比較すると、「商用化・実用化は3年より先になるという段階である」が6.1ポイント増加している。一方、「1～3年以内に商用化・実用化が成される段階である」が10.6ポイントと最も減少している。次いで、「1年以内に商用化・実用化が成される段階である」は6.1ポイント減少している。



5.7 発売時期の分布

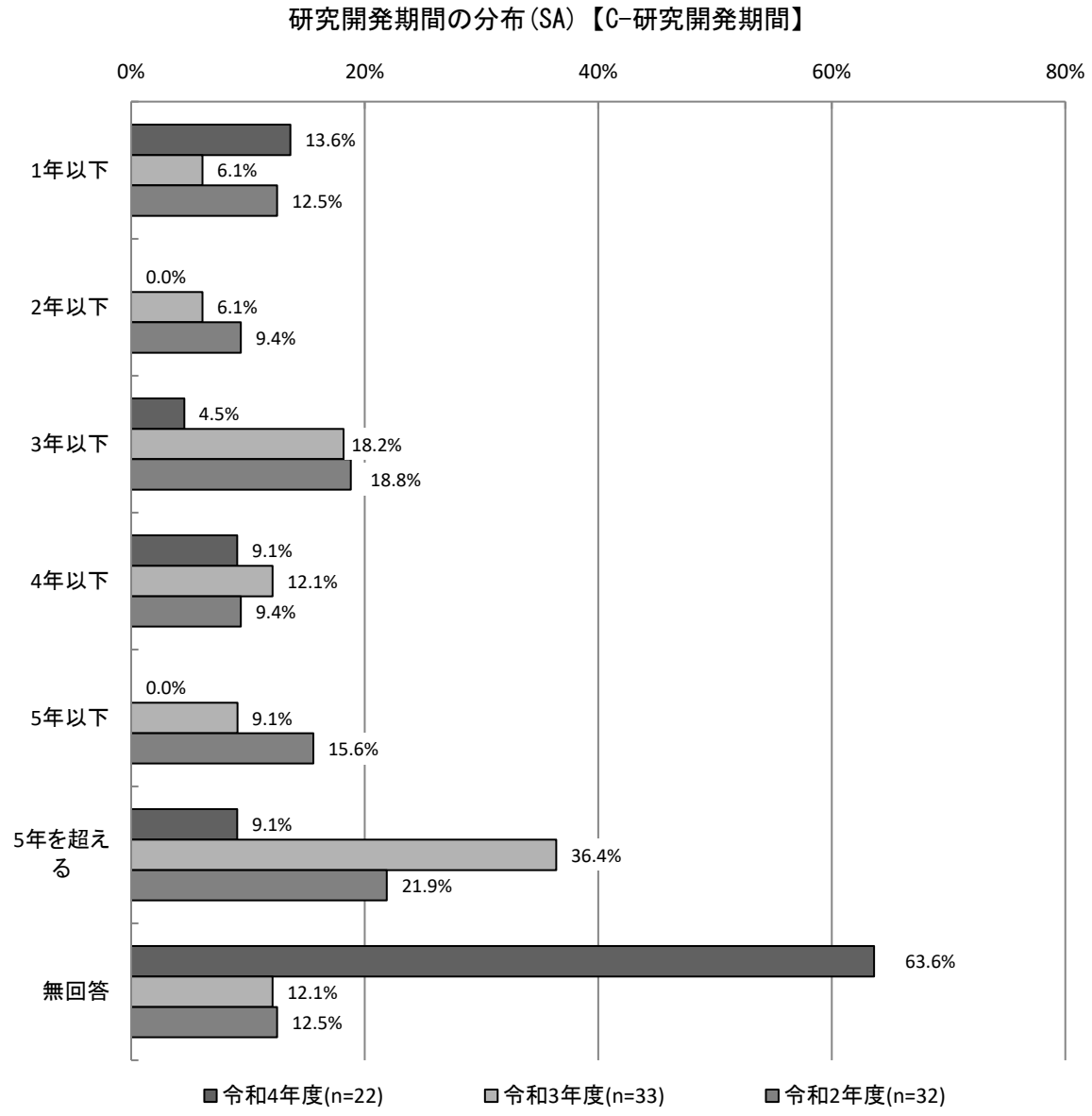
発売時期については、「平成22年」及び「令和3年」が2件となっている。



5.8 研究開発期間の分布

研究開発期間については、「1年以下」が13.6%（3件）で最も多く、次いで「4年以下」「5年を超える」がそれぞれ9.1%（2件）となっている。

昨年度と比較すると、「1年以下」が7.5ポイント増加している。一方「5年を超える」が27.3ポイントと最も減少しており、次いで「3年以下」が13.7ポイント減少となっている。



5.9 実用化された製品及び研究開発中の技術・サービス

本節では、回答用紙B（実用化（製品化））及び回答用紙C（研究開発）の各々の状況について、一覧表にまとめたものを示す。この一覧表は、バイヤーズガイドのような製品一覧表として使うことを想定しておらず、あくまで今回の調査対象とした大学・企業の母集団で抽出してきたものを参考までに掲載したものである。この資料で一般的な傾向を知るなど、具体的な製品を選択する際の参考として使われたい。

また、表中の「技術開発状況」及び「概要・特徴など」については、回答をそのまま、または簡略化して掲載しており、調査者の意見を示すものではない。

■ 技術の実用化（製品化）状況

製品名	企業・大学名	開発元(メーカー名等)	侵入検知・防御技術	ぜい弱性対策技術	高度認証技術	インシデント分析技術	不正プログラム対策技術	その他アクセス制御に関する技術
THX	（株）テリロジーワークス	（株）テリロジーワークス	○					
セキュリティ対応マイコン	ルネサスエレクトロニクス株式会社	ルネサスエレクトロニクス株式会社					○	
IoTハニーポット	三菱電機株式会社	三菱電機					○	
MistyGuard<CERTMANAGER>	三菱電機株式会社	三菱電機インフォメーションシステムズ						○
Camellia	三菱電機株式会社	NTTと三菱電機による共同開発						○
パスワード共有サービスPASSPATH	学校法人福岡大学	福岡大学情報基盤センター 中國研究室						○

※ 回答用紙Bにおいて、公開用情報が得られなかったもの及び「製品名」、「企業・大学名」、「開発元」のいずれか記載がないものは省略している

■　技術の研究開発状況

研究開発名称	企業・大学名	関連部門名	侵入検知・防御技術	ぜい弱性対策技術	高度認証技術	インシデント分析技術	不正プログラム対策技術	その他アクセス制御に関する技術
IoTデバイスにおけるセキュリティソフト導入の検討	明星大学　情報学部	情報学部　情報学科　末田研究室					○	
ブロックチェーン上での安全な鍵管理方式の研究	関東学院大学理工学部	理工学部ネットワークセキュリティ研究室			○			
組込みシステム向けのセキュリティ技術	国立大学法人東海国立大学機構名古屋大学	大学院情報学研究科　高田・松原研究室/組込みシステム研究センター	○	○			○	
キーボード入力のタイミングを用いた生体認証	学校法人福岡大学	福岡大学情報基盤センター中國研究室			○			
イントラネットにおけるデバイスの柔軟なアクセス制御に関する研究	学校法人東北工業大学	工学部情報通信工学科　角田研究室	○					
光通信量子暗号（Y00）	学校法人玉川学園	量子情報科学研究所	○					
SecureIP開発	ルネサスエレクトロニクス株式会社	ルネサスエレクトロニクス株式会社 セキュリティコンピテンスセンター					○	
マルウェアの検出・分類に関する研究	国立大学法人岩手大学	理工学部システム創成工学科知能・メディア情報コース					○	
生体情報の継続認証による時間追従型本人認証システム	日本文理大学	工学部・情報メディア学科	○		○			
認証暗号アルゴリズム	三菱電機株式会社	情報記述総合研究所	○					
耐量子計算機暗号	三菱電機株式会社	情報技術総合研究所	○					
秘匿検索（検索可能暗号）	三菱電機株式会社	情報技術総合研究所	○					
センサーセキュリティ	三菱電機株式会社	情報技術総合研究所	○					○

※　回答用紙Cにおいて、公開用情報が得られなかったもの及び「研究開発名称」、「企業・大学名」、「関連部門名」のいずれか記載がないものは省略している

5.9.1 「技術の実用化（製品化）状況」について

※一覧表の下には対象となる防御対象について○を付与している。

企業・大学名	（株）テリロジーワークス
代表者名	
所在地	〒102-0073 千代田区九段北1-10-1
窓口部署名	ビズネス開発部
電話番号	03-5213-5533
ホームページのURL	www.twx-threetintel.com
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： THX 開発元(メーカー名等)： （株）テリロジーワークス 開発国： 日本 価格：300万～ 発売時期： 2021年10月 出荷数：	ネットワークトラフィックから得られるメタデータ情報を集収し解析プラットフォームに提供します。

不正アクセスからの防御対象	
侵入検知・防御技術	○
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	

企業・大学名	ルネサスエレクトロニクス株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
ホームページのURL	https://www.renesas.com
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： 　セキュリティ対応マイコン 開発元(メーカー名等)： 　ルネサスエレクトロニクス株式会社 開発国： 　日本 価格： 発売時期： 出荷数： 	セキュリティ対応マイコンは、外部からのアクセス不可能なSecureIPを搭載します。SecureIP内にて鍵データと暗号エンジンを強固に保護し、領域保護機能や製品固有の機能と組み合わせることで、認証プログラムを改ざんの脅威から保護します。これにより、Root of Trustによる自立したセキュリティを実現し、様々な脅威から簡単かつ強固に保護するシステムを構築することが可能となります。

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	○
その他アクセス制御に関する技術	

企業・大学名	三菱電機株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
ホームページのURL	
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： IoTハニーポット 開発元(メーカー名等)： 三菱電機 開発国： 日本 価格： 発売時期： 出荷数： 	IoT機器への攻撃動向を観察するためのハニーポット 販売目的での研究開発しているわけではないため、価格・発売時期等は記載しません。

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	○
その他アクセス制御に関する技術	

企業・大学名	三菱電機株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
ホームページのURL	
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： MistyGuard<CERTMANAGER> 開発元(メーカー名等)： 三菱電機インフォメーション システムズ 開発国： 日本 価格： オープン 発売時期： 2010年4月1日 出荷数： 不明	特定認証業務に対応する高度なセキュリティ運用機能、IoT機器利用に適した証明書発行、失効API機能を提供し、大規模の公的認証基盤やIoT運用基盤から中規模の企業内プライベートPKI利用システムまで様々な用途に応じた利用が可能です。弊社MistyGuardシリーズの電子署名製品と組み合わせることで、電子証明書を利用した電子契約、電子認証等のセキュリティシステムを構築できます。出展 https://www.mdis.co.jp/service/certmanager/

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	○

企業・大学名	三菱電機株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
ホームページのURL	
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： Camellia 開発元(メーカー名等)： NTTと三菱電機による共同開発 開発国： 日本 価格： オープン 発売時期： 2000年3月10日 出荷数： 不明	Camellia(カメリア)は、世界トップクラスの暗号研究者を抱えるNTTと三菱電機が共同で2000年に開発した共通鍵ブロック暗号です。技術的に高い安全性を有するのは当然のこと、効率性と実用性にも優れており、さまざまなプラットフォーム上でのソフトウェアにより高速に実装することができます。ハードウェア実装においても、高速実装はもとよりコンパクトかつ低消費電力型の実装が可能です。これらの技術的優位性は、例えば欧州連合推奨暗号選定プロジェクトNESSIEにおいて「米国政府標準暗号AESと多くの点で同等の安全性と性能を有している」と評価されるなど、国際的にも認められています。現在では、AESと同等の安全性・処理機能を有しているほぼ唯一の暗号として国際的にも認知されつつあり、多くの国際的な標準暗号・推奨暗号に選定されています。とりわけ、日本国産暗号としては、初めてインターネット標準暗号(IETF Standard Track RFC)として承認されました。また、オープンソースの提供も積極的に実施しており、現在では国産暗号としては初めてOpenSSL,Linux,FreeBSDをはじめとする国際的にも主要なオープンソースソフトウェアに搭載されています。さらには欧米企業等との連携を促進するため、NTTはMITケルベロスコンソーシアムへ加盟しました。出展 https://info.isl.ntt.co.jp/crypt/camellia/intro.html

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	○

企業・大学名	学校法人福岡大学
代表者名	
所在地	
窓口部署名	
電話番号	
ホームページのURL	
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： パスワード共有サービス PASSPATH 開発元(メーカー名等)： 福岡大学情報基盤センター中 國研究室 開発国： 日本 価格： 発売時期： 出荷数：	現在話題になっているPPAP（パスワードの後送問題）を解決するソリューションである。サービスを提供しているサイトのURLは以下のとおり。https://passpath.net/

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	○

5.9.2 「技術の研究開発状況」について

※一覧表の下には対象となる防御対象について〇を付与している

企業・大学名	明星大学　情報学部
代表者名	
所在地	〒191-8506 東京都日野市程久保2-1-1
窓口部署名	情報学部支援センター
電話番号	
関連部門名	情報学部　情報学科　末田研究室
ホームページのURL	https://www.meisei-u.ac.jp
研究説明のURL	
対象技術	技術の概要・特徴など
研究開発名称： IoTデバイスにおけるセキュリティソフト導入の検討 研究開発国： 日本 研究開発時期： 2022年4月～2023年3月	IoT機器は数や種類、使用用途が豊富であることや、スペック等の問題からアンチウイルスソフトの導入が困難とされており、ユーザ側で有効な対策が実施できないとされている。こうしたことを背景に、近年のCPU、メモリ等の軽量化が進んでいることに着目しIoT機器のスペックを考慮したアンチウィルスソフトの調査および導入を検討し、問題点についても明らかにする。現在、アンチウィルスソフトの調査を実施中である。

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	〇
その他アクセス制御に関する技術	

企業・大学名	関東学院大学理工学部
代表者名	理工学部長　辻森淳
所在地	〒236-8501 神奈川県横浜市金沢区六浦東1-50-1
窓口部署名	学部庶務課（理工学部、建築・環境学部）
電話番号	045-786-7096
関連部門名	理工学部ネットワークセキュリティ研究室
ホームページのURL	https://univ.kanto-gakuin.ac.jp/
研究説明のURL	
対象技術	技術の概要・特徴など
研究開発名称： ブロックチェーン上での安全な鍵管理方式の研究 研究開発国： 日本 研究開発時期： 2018年～2022年	ブロックチェーンの性質を損なうことなく秘匿化した情報を利活用するために、秘密分散などの手法を応用することで、ブロックチェーン上で安全に秘密鍵を運用する方式を提案した[1]。[1]吉田祥悟、塚田恭章：ブロックチェーン上での安全な鍵管理方式と単一障害点のない秘密計算方式の提案.情報処理学会論文誌（採録決定）

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	○
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	

企業・大学名	国立大学法人東海国立大学機構名古屋大学
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	大学院情報学研究科　高田・松原研究室/組込みシステム研究センター
ホームページのURL	
研究説明のURL	https://www.ertl.jp https://www.nces.i.nagoya-u.ac.jp
対象技術	技術の概要・特徴など
研究開発名称： 組込みシステム向けのセキュリティ技術 研究開発国： 日本 研究開発時期： 2014年4月1日	大学の研究組織にて、組込みシステムや自動車制御システムを対象に、次のようなセキュリティ技術について研究・開発を進めている。なお、これらの活動は、研究室独自、または企業との共同研究として実施している。開発した成果の一部は、学術論文として発表している。 ・脅威、脆弱性分析技術・ソフトウェアの実行フロー保証技術・ソフトウェア更新の支援技術・ソフトウェアに対するファジングによるテスト技術・制御ネットワークへの不正アクセス防止技術・制御ネットワークにおけるメッセージ認証技術　上記に関連して、組込み・自動車セキュリティに関する社会人向け教育活動を、名古屋大学NCES人材育成プログラムとして提供している。 https://www.nces.i.nagoya-u.ac.jp/NEP/index.html

不正アクセスからの防御対象	
侵入検知・防御技術	○
ぜい弱性対策技術	○
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	○
その他アクセス制御に関する技術	

企業・大学名	学校法人福岡大学
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	福岡大学情報基盤センター中國研究室
ホームページのURL	
研究説明のURL	なし
対象技術	技術の概要・特徴など
研究開発名称： キーボード入力のタイミングを用いた生体認証 研究開発国： 日本 研究開発時期： 2016年9月1日～2023年3月31日	現段階では少数の被験者の協力による認証精度を確認している。極めて高い認証精度を確認しており、近日中に多くの被験者を用いて、認証精度を検証する計画である。現在は、国内のセキュリティ製品を開発するメーカーと共同研究開発を推進することを協議しており、同メーカーから日本国内に向けて販売することを目指す。

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	○
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	

企業・大学名	学校法人東北工業大学
代表者名	
所在地	〒982-8577 宮城県仙台市太白区八木山香澄町35番1号
窓口部署名	情報サービスセンター
電話番号	022-305-3896
関連部門名	工学部情報通信工学科　角田研究室
ホームページのURL	https://www.tohtech.ac.jp/
研究説明のURL	

対象技術	技術の概要・特徴など
研究開発名称： イントラネットにおけるデバイスの柔軟なアクセス制御に関する研究 研究開発国： 日本 研究開発時期： 2022年4月～	要素技術の検討とアイディアの実現性の検証を進めている状況にある。

不正アクセスからの防御対象	
侵入検知・防御技術	○
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	

企業・大学名	学校法人玉川学園
代表者名	小原芳明
所在地	〒194-8610 東京都町田市玉川学園6-1-1
窓口部署名	玉川大学　学術研究所　研究推進室
電話番号	042-739-8666
関連部門名	量子情報科学研究所
ホームページのURL	https://www.tamagawa.jp
研究説明のURL	https://www.tamagawa.jp/research/quantum/qec.
対象技術	技術の概要・特徴など
研究開発名称： 光通信量子暗号（Y00） 研究開発国： 日本 研究開発時期： 2011年4月1日～	光通信量子暗号Y-00は光が本質的に持つ量子力学的な雑音の効果を活用してデータを秘匿する機能を実現する、光通信回線を守る技術です。この機能を実証するためのプロトタイプをすでに公開しており、引き続き大学の研究機関としてその基礎的解明・発展に向けて実験研究と理論研究の両面から研究を推進しています。最新の研究成果は論文として発表しているのでそちらを参照されたい。

不正アクセスからの防御対象	
侵入検知・防御技術	○
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	

企業・大学名	ルネサスエレクトロニクス株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	ルネサスエレクトロニクス株式会社　セキュリティコンピテンスセンター
ホームページのURL	https://www.renesas.com
研究説明のURL	https://www.renesas.com/rx-security-solution
対象技術	技術の概要・特徴など
研究開発名称： SecureIP開発 研究開発国： 日本 研究開発時期：	

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	○
その他アクセス制御に関する技術	

企業・大学名	国立大学法人岩手大学
代表者名	学長　小川智
所在地	〒020-8550 岩手県盛岡市上田3-18-8
窓口部署名	理工学部事務部
電話番号	019-621-6305
関連部門名	理工学部システム創成工学科知能・メディア情報コース
ホームページのURL	https://www/iwate-u.ac.jp/
研究説明のURL	
対象技術	技術の概要・特徴など
研究開発名称： マルウェアの検出・分類に関する研究 研究開発国： 日本 研究開発時期： 2016年4月～	マルウェアの表層あるいは動的解析結果を利用した機械学習による検出・分類手法の研究を行っている。

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	○
その他アクセス制御に関する技術	

企業・大学名	日本文理大学
代表者名	学長　橋本堅次郎
所在地	〒870-0397 大分市一木1727
窓口部署名	大学総務・経理担当
電話番号	097-524-2700
関連部門名	工学部・情報メディア学科
ホームページのURL	www.nbu.ac.jp
研究説明のURL	https://www.nbu.ac.jp/～fukushima https://sites.google.com/view/fukulab
対象技術	技術の概要・特徴など
研究開発名称： 生体情報の継続認証による時間追従型本人認証システム 研究開発国： 日本 研究開発時期： 2000年9月～	通信回線が低遅延化が進むとともに、新型コロナに伴うニーズの多様化等の社会的変化があることから、ニーズの変化に伴う設計と、確定した設計から実装による社会実装の可能性検証、の2つを並走しての開発を進めている。　【ニーズ分析と設計（基礎理論/アルゴリズム）】・時間追従アルゴリズム　短時間推定および推定精度評価アルゴリズム　・特徴量記述　音声の特徴量化（頭部構造に着目したうめき声も対象とした取組）環境音の特徴量化（使用端末検知の次を見越した取組）【社会実装に向けた可能性検証】確定アルゴリズムの適用先としていくつかの企業と協力して試作・評価に向けた取り組みを進めている。

不正アクセスからの防御対象	
侵入検知・防御技術	○
ぜい弱性対策技術	
高度認証技術	○
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	

企業・大学名	三菱電機株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	情報記述総合研究所
ホームページのURL	
研究説明のURL	https://www.mitsubishielectric.co.jp/corporate/randd/list/info_tel/a41/index.html
対象技術	技術の概要・特徴など
研究開発名称： 認証暗号アルゴリズム 研究開発国： 日本 研究開発時期： 2018年頃	「MACアルゴリズム」では共通鍵を使って送信者は改ざん検知用のタグを生成し、データとともに送信します。受信者も受け取ったデータと共通鍵を使ってタグを生成します。両方のタグを照合し、もしその内容が異なっていれば、送信の途中で第三者によってデータに手が加えられたことになり、改ざんを検知できます。「認証暗号アルゴリズム」はタグによる改ざん検知に加え、秘匿機能を備えています。利用モードでは長いデータを扱うために、1つのデータを複数のブロックに分けて処理します。その際に暗号化毎に異なる値(ナンス)を加えて暗号化します。通常、仮にブロック1とブロック2が同じ平分であった場合、暗号文も同じになるため、第三者から見て同じ平文が続いていると推察でき、データの内容を知るヒントになりかねません。ナンスを加えて暗号化することで、同じ平文が続いても違った暗号文が出力されるため、同じ平文を繰り返し使った場合に起こりうる危険を回避でき、安全性が担保できます。

不正アクセスからの防御対象	
侵入検知・防御技術	○
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	

企業・大学名	三菱電機株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	情報技術総合研究所
ホームページのURL	
研究説明のURL	https://www.mitsubishielectric.co.jp/coeporate/special/convention/ceatec2021/cryptography/
対象技術	技術の概要・特徴など
研究開発名称： 耐量子計算機暗号 研究開発国： 日本 研究開発時期： 2018頃	格子暗号と同種写像暗号について安全性を向上したアルゴリズムを開発中

不正アクセスからの防御対象	
侵入検知・防御技術	○
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	

企業・大学名	三菱電機株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	情報技術総合研究所
ホームページのURL	
研究説明のURL	https://www.mitsubishielectric.co.jp/corporate/randd/list/info_tel/a29/index.html
対象技術	技術の概要・特徴など
研究開発名称： 秘匿検索（検索可能暗号） 研究開発国： 日本 研究開発時期： 2016頃	基本方式の開発は完了し、システム化のためのライブリや鍵管理方式、高速化・効率化の検討を継続

不正アクセスからの防御対象	
侵入検知・防御技術	○
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	

企業・大学名	三菱電機株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	情報技術総合研究所
ホームページのURL	
研究説明のURL	https://www.mitsubishielectric.co.jp/corporate/randd/list/info_tel/b242/index.html
対象技術	技術の概要・特徴など
研究開発名称： センサーセキュリティ 研究開発国： 日本 研究開発時期： 2019	センサーへの攻撃手法の解析と、その解析結果を元にした攻撃対策を研究。攻撃手法と対策を評価するためのシュミレータを開発。

不正アクセスからの防御対象	
侵入検知・防御技術	○
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	○

アクセス制御機能に関する技術の研究開発の状況等に関する調査　付録資料

付録３：調査票

付録３

回答用紙Ａ

■ 研究開発分野については別紙「表１アクセス制御機能の分類表」を参考にしてください。
■ 研究開発が海外ベンダーで行われている場合は、回答できる範囲でお答えください。

■ お手数ですが、令和４年９月３０日(金)までに、ご返送ください。
◆郵送での回答：同封の返信用封筒をご利用ください（切手は不要です）
◆電子メールでの回答：「cyber@researchworks.co.jp」までお送りください

問１．アクセス制御機能に関する技術の研究開発を行っていますか。（○は一つ）

１．はい
２．いいえ

※以下の設問には「1．はい」と答えた方のみお進みください。

問２．現在、取り組んでいるのは、どのような分野ですか。（○はいくつでも）

１．暗号技術
２．認証技術
３．ネットワークセキュリティ
４．不正侵入対策
５．セキュリティマネジメント
６．ウイルス対策
７．セキュリティサービス関連
８．クラウドコンピューティング
９．その他（　　）

問３．今後、もっとも力を入れたいのは、どのような分野ですか。（○は一つ）

１．暗号技術
２．認証技術
３．ネットワークセキュリティ
４．不正侵入対策
５．セキュリティマネジメント
６．ウイルス対策
７．セキュリティサービス関連
８．クラウドコンピューティング
９．その他（　　）

問４．現在、実用化（製品化）されている分野をお答えください。（○はいくつでも）

１．暗号技術
２．認証技術
３．ネットワークセキュリティ
４．不正侵入対策
５．セキュリティマネジメント
６．ウイルス対策
７．セキュリティサービス関連
８．クラウドコンピューティング
９．その他（　　）
10．実用化（製品化）されていない

問５．今後、実用化（製品化）を見込んでいる分野をお答えください。（○はいくつでも）

１．暗号技術
２．認証技術
３．ネットワークセキュリティ
４．不正侵入対策
５．セキュリティマネジメント
６．ウイルス対策
７．セキュリティサービス関連
８．クラウドコンピューティング
９．その他（　　）
10．実用化（製品化）の予定はない

問６．貴事業体（研究所）での年間の研究開発費について、ご回答ください。（○は一つ）

１．なし
２．1,000万円未満
３．1,000万円以上1億円未満
４．1億円以上10億円未満
５．10億円以上100億円未満
６．100億円以上

問７．貴事業体（研究所）での研究開発に携わっている人員について、ご回答ください。（○は一つ）

１．0人
２．1人以上10人未満
３．10人以上50人未満
４．50人以上100人未満
５．100人以上

問８.貴事業所（研究所）は、どの業種にあてはまりますか。（○は一つ）

業種分類	業種			
農林・水産・鉱業	1.農林・水産	2.鉱業	3. その他（　　）	
製造業	4.食品	5.繊維	6. 紙・パルプ	7.化学
	8.薬品	9.ゴム・窯業	10.非鉄金属	11.機械
	12.電気機器	13.造船	14.輸送機器	15.精密機器
	16.その他（　　）			
不動産・建築	17.不動産	18.建築	19.その他（　　）	
金融	20.銀行	21.証券	22.保険	23.クレジット
	24.消費者金融	25.信用金庫・組合	26.その他（　　）	
エネルギー	27.電力	28.ガス	29.水道	30.石油製造(精製)
	31.その他（　　）			
運輸業	32.鉄道・地下鉄	33.航空	34.陸運	35.海運
	36.倉庫	37.その他（　　）		
情報通信	38.新聞	39.放送	40.通信	41.ISP
	42.その他（　　）			
サービス	43.流通・卸売	44.小売	45.娯楽・アミューズメント	
	46.飲食	47.ホテル・旅行	48.情報処理・ソフトウェア	
	49.警備	50.医療・福祉	51.その他（　　）	
教育	52.大学	53.短大	54.専門学校	
	55.その他（　　）			
行政サービス	56.都道府県	57.政令指定都市	58.市町村	

（太枠線内にご回答ください）

回答用紙B

実用化（製品化）されているアクセス制御機能に関する技術の個別調査

■ １製品（ハードウェア、ソフトウェア、サービス）につき1枚の回答用紙をご使用ください。
■ 対象がハードウェアやソフトウェアの場合は、問７はご回答いただかなくて結構です。
■ 対象がサービスの場合は、問１～問６はご回答いただかなくて結構です。
■ 製品が複数ある場合は、この用紙をコピーしてご記入ください。
■ （※）の付いた用語については別紙「表２ 用語説明」を参考にしてください。

★ご回答内容の報告書への掲載及び警察庁ホームページでの公開につきまして、「公開情報及びご連絡先記入用紙」にもご回答ください。

※ 本調査票（回答用紙B）に回答する製品がない場合は回答用紙Cへお進みください。

製品名	
開発元（メーカー名等）	
開発国	
問1 何を守りますか **（○はいくつでも）**	１．ネットワーク ２．サーバ ３．クライアント（ＰＣ等） ４．通信情報（※） ５．データ ６．施設（※） ７．その他 （　　）
問2 何から保護しますか **（○はいくつでも）**	１．盗聴 ２．漏えい ３．改ざん（※） ４．なりすまし（※） ５．事実否認（※） ６．侵入 ７．踏み台（※） ８．DDoS（※） ９．ウイルス 10．その他 （　　）
問3 どのようなセキュリティ上の効果がありますか **（○はいくつでも）**	１．攻撃や不正操作等の早期検知・検出効果 ２．攻撃や不正操作等に対する防御効果、抑止効果 ３．被害箇所の局所化効果、拡大防止効果 ４．被害箇所の自律的な回復・修復効果 ５．その他（　　）
問4 どのような機能を持っていますか **（○はいくつでも）**	１．認証（※） ２．証明書 ３．認可（※） ４．アクセス制御 ５．暗号 ６．検知 ７．運用管理 ８．評価（※） ９．対外部者の監視 10．対内部者の監視 11．解析 12．その他 （　　）

問5　どのようなレイヤーのセキュリティを守りますか **（○はいくつでも）**	1．物理層 2．データリンク層 3．ネットワーク層 4．トランスポート層 5．セッション層 6．プレゼンテーション層 7．アプリケーション層
問6　この製品はどのような不正アクセスからの防御を対象としていますか。 **（○はいくつでも）**	1．侵入検知・防御技術 2．ぜい弱性対策技術 3．高度認証技術 4．インシデント分析技術 5．不正プログラム対策技術 6．その他アクセス制御に関する技術
問7　どのようなサービスですか（対象がサービスの場合） **（○はいくつでも）**	1．教育 2．アウトソース 3．インテグレーション 4．コンサルティング 5．保守（サポート） 6．サービスプロバイダ 7．保険 8．その他 （　　）
概要・特徴など	
価格	
発売時期	西暦　　年　　月　　日頃～
出荷数	累計

回答用紙C

研究開発中のアクセス制御機能に関する技術の個別調査

- 1研究開発分野（技術、サービス）につき１枚の回答用紙を使用ください。
- 研究開発対象が技術の場合は、問８はご回答いただかなくて結構です。
- 研究開発対象がサービスの場合は、問１～問７はご回答いただかなくて結構です。
- 研究開発中の技術・サービスが複数ある場合は、この用紙をコピーしてご記入ください。
- （※）の付いた用語については別紙「表２ 用語説明」を参考にしてください。

★ご回答内容の報告書への掲載及び警察庁ホームページでの公開につきまして、「公開情報及びご連絡先記入用紙」にもご回答ください。

関連部門名	
研究開発名称	
研究開発国	
問1　何を守りますか **（○はいくつでも）**	１．ネットワーク ２．サーバ ３．クライアント（ＰＣ等） ４．通信情報（※） ５．データ ６．施設（※） ７．その他 （　　）
問2　何から保護しますか **（○はいくつでも）**	１．盗聴 ２．漏えい ３．改ざん（※） ４．なりすまし（※） ５．事実否認（※） ６．侵入 ７．踏み台（※） ８．DDoS（※） ９．ウイルス 10．その他 （　　）
問3　どのようなセキュリティ上の効果がありますか **（○はいくつでも）**	１．攻撃や不正操作等の早期検知・検出効果 ２．攻撃や不正操作等に対する防御効果、抑止効果 ３．被害箇所の局所化効果、拡大防止効果 ４．被害箇所の自律的な回復・修復効果 ５．その他（　　）
問4　どのような機能を持っていますか **（○はいくつでも）**	１．認証（※） ２．証明書 ３．認可（※） ４．アクセス制御 ５．暗号 ６．検知 ７．運用管理 ８．評価（※） ９．対外部者の監視 10．対内部者の監視 11．解析 12．その他 （　　）
問5　どのようなレイヤーのセキュリティを守りますか **（○はいくつでも）**	１．物理層 ２．データリンク層 ３．ネットワーク層 ４．トランスポート層 ５．セッション層 ６．プレゼンテーション層 ７．アプリケーション層

問6　この研究開発中の技術はどのような不正アクセスからの防御を対象としていますか。 **（○はいくつでも）**	１．侵入検知・防御技術 ２．ぜい弱性対策技術 ３．高度認証技術 ４．インシデント分析技術 ５．不正プログラム対策技術 ６．その他アクセス制御に関する技術
問7　研究開発の成果として、どのようなものを目指していますか	１．理論（アルゴリズム、手法、評価など） ２．開発（システム構築、実装、プロトコルなど） ３．実用（実用化のための技術（管理手法、運用技術、インターフェイスなど）） ４．その他（　　）
問8　どのようなサービスですか（対象がサービスの場合） **（○はいくつでも）**	１．教育 ２．アウトソース ３．インテグレーション ４．コンサルティング ５．保守（サポート） ６．サービスプロバイダ ７．保険 ８．その他 （　　）
問9　進捗状況はどの段階にありますか **（○は一つ）**	１．1年以内に商用化・実用化が成される段階である ２．1～3年以内に商用化・実用化が成される段階である ３．商用化・実用化は3年より先になるという段階である ４．直接商用化・実用化に結びつくものではない
研究開発状況	
研究開発期間	西暦　　年　　月　　日 ～ 西暦　　年　　月　　日
研究内容の説明がされているURL	

＜別紙＞　アクセス制御機能について

インターネット、ＬＡＮなどのネットワークに接続されている電子計算機を、ネットワークを介して、正規のユーザ以外の者が利用できないように制限するために、アクセス管理者が対象となる電子計算機などに持たせている機能で、「不正アクセス行為の禁止等に関する法律」の第２条第３項に定められたものをいいます。

本アンケートでは、このアクセス制御機能に関連する技術の開発状況について調査を行っています。

＜参考＞

「不正アクセス行為の禁止等に関する法律」第２条第３項

この法律において「アクセス制御機能」とは、特定電子計算機の特定利用を自動的に制御するために当該特定利用に係るアクセス管理者によって当該特定電子計算機又は当該特定電子計算機に電気通信回線を介して接続された他の特定電子計算機に付加されている機能であって、当該特定利用をしようとする者により当該機能を有する特定電子計算機に入力された符号が当該特定利用に係る識別符号（識別符号を用いて当該アクセス管理者の定める方法により作成される符号と当該識別符号の一部を組み合わせた符号を含む。次項第１号及び第２号において同じ。）であることを確認して、当該特定利用の制限の全部又は一部を解除するものをいう。

＜回答用紙Aの補足＞表１　アクセス制御機能の分類表

分類	例
暗号技術	暗号技術（アルゴリズム開発など）、暗号化ソフト（ファイルの暗号化、ディスクの暗号化など）
認証技術	ワンタイムパスワード、IC カード、USB 等デバイスによる認証、バイオメトリクス認証、PKI、アクセスコントロール（シングルサインオン含む）
ネットワークセキュリティ	VPN（IPsec、SSL/TLS、Secure Shellなど）、無線 LAN セキュリティ、ファイアウォール、パケットフィルタリング、コンテンツセキュリティ（コンテンツフィルタ、メールフィルタ）、ネットワーク管理
不正侵入対策	侵入検知（IDS）、ハニーポット、アクセスログ収集管理
セキュリティマネジメント	ログ解析、資産管理、情報保護、セキュリティ情報管理
ウイルス（不正プログラム）対策	ウイルス対策ソフト、スパイウェア対策ソフト
セキュリティサービス	情報セキュリティ監査、デジタルフォレンジック、脆弱性診断、セキュリティ監視運用
クラウドコンピューティング	ネットワークを経由してアクセスするサーバ、ストレージ等の資産管理、運用管理 クラウドサービス提供、利用に係るセキュリティ全般

＜回答用紙B・Cの補足＞表２　用語説明

用語	説明
通信情報	ネットワークなど通信経路上を流れている情報です。
施設	建屋や部屋を指しますが、広義に電源設備などを含めても結構です。
改ざん	保存されている情報やネットワークなどを流れている情報が、第三者により書き換えられることを意味します。
なりすまし	他人のふりをしてメールを交換したり、情報や金銭を引き出したりする行為です。IPアドレスのなりすまし等も含みます。
事実否認	事実を認めないことを意味します。例えば、発注をしていながら、後にそのようなことが無かったかのように振舞うことです。
踏み台	攻撃者が他人のコンピュータなどを経由することで身元を隠匿するような場合、経由されたコンピュータを踏み台と呼びます。
DDoS	インターネット上で、特定のサーバやサイトに向けて一斉に大量の通信を試みることで、当該サーバやサイトのサービスを妨害する攻撃手法です。
認証	パスワードや電子署名、バイオメトリクス認証により、人物（又はシステム）の正当性を確認する行為を意味します。
認可	認証後の、細かなサービス・ファイル等の利用許可・制限等やサーバへのアクセス許可・制限等を含みます。
評価	一定の基準に沿って機能や性能を検証することです。例えば、脆弱性調査ツールなどを指します。

公開情報及びご連絡先記入用紙

１．ご回答頂いた技術開発状況を「個別事例一覧表」として本調査の報告書に記載する際に下記の情報を公開いたします。公開して差し支えのない範囲で下記項目にご記入ください。

【公開用情報】

貴事業体(研究所)名 【必須】	
法人番号 【必須】	
代表者名	
所在地	〒　　－
窓口部署名	
電話番号	
ホームページのURL	

２．次にご記入いただいたお名前とご連絡先は、下記の「個人情報の取り扱いについて」により取り扱います。
なお、ご回答内容の確認のため、ご記入いただいたご連絡先に別途、株式会社リサーチワークスからご連絡させていただくことがあります。

【ご担当者様のご連絡先】

貴社名	
貴部署名	
ご担当者様　氏名	
ご住所	〒　　－
電話番号	
e-mail	

【個人情報のお取り扱いについて】

■　ご担当者様の個人情報は、株式会社リサーチワークスが適切な保護措置を講じ、厳重に管理いたします。
■　ご担当者様の個人情報は、不正アクセス行為対策等の実態の把握・今後の方向性の検討等の実施、及び回答内容のご確認のため以外には利用いたしません。また、ご担当者の個人情報が特定される形で調査結果が公開されることはありません。