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６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2,951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

調査票ファイルに回答内容を入力し、電子メールにて回答

② 郵送等での回答

配付した調査票に回答内容を記入し、郵送等にて回答

（調査期間：令和6年8月28日(水)（発送日）～9月20日(金)（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634件であった。回収率は21.5％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	176	19.5%
不動産・建築	187	38	20.3%
金融	108	28	25.9%
エネルギー	15	4	26.7%
運輸業	75	18	24.0%
情報通信	291	15	5.2%
サービス	837	137	16.4%
教育	290	128	44.1%
行政サービス	237	83	35.0%
無回答		6	－
合計	2,951	634	21.5%

1.5 報告書を見る際の留意点

- 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

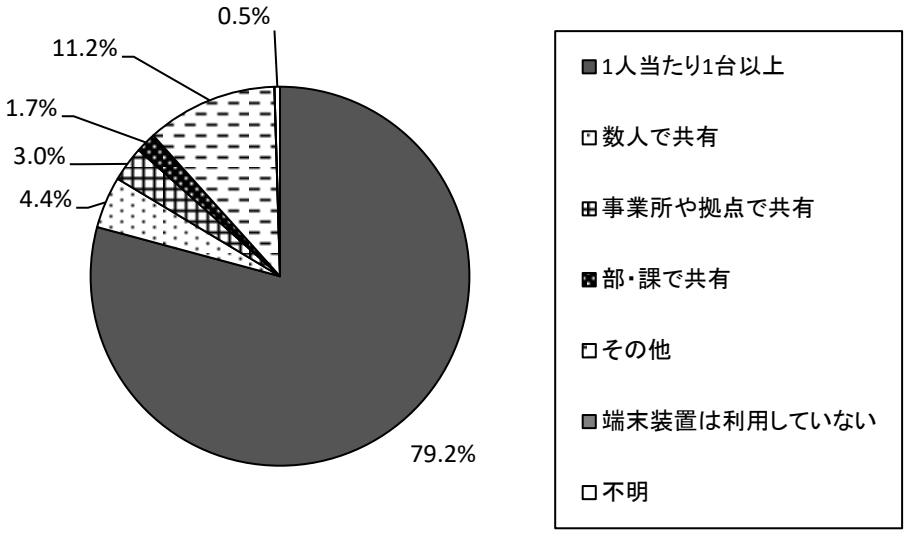
令和6年度の調査結果については、次のような特徴がみられる。

1　組織的対策

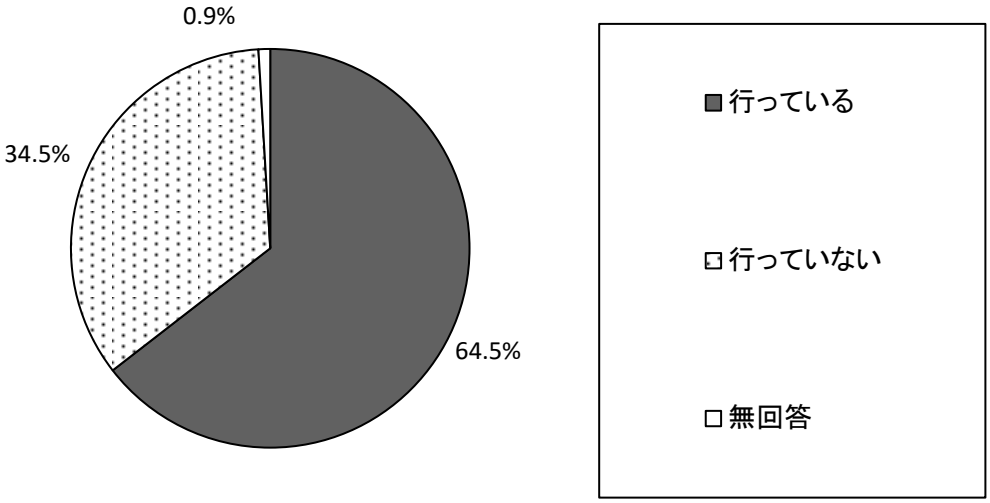
【情報システム等の環境】

パソコン・スマートフォン等の整備環境については、79.2%で「1人当たり1台以上」で整備されており、「数人で共有」が4.4%、「事業所や拠点で共有」が3.0%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64.5%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=634)



【全体】テレワークの実施状況（SA,n=634）



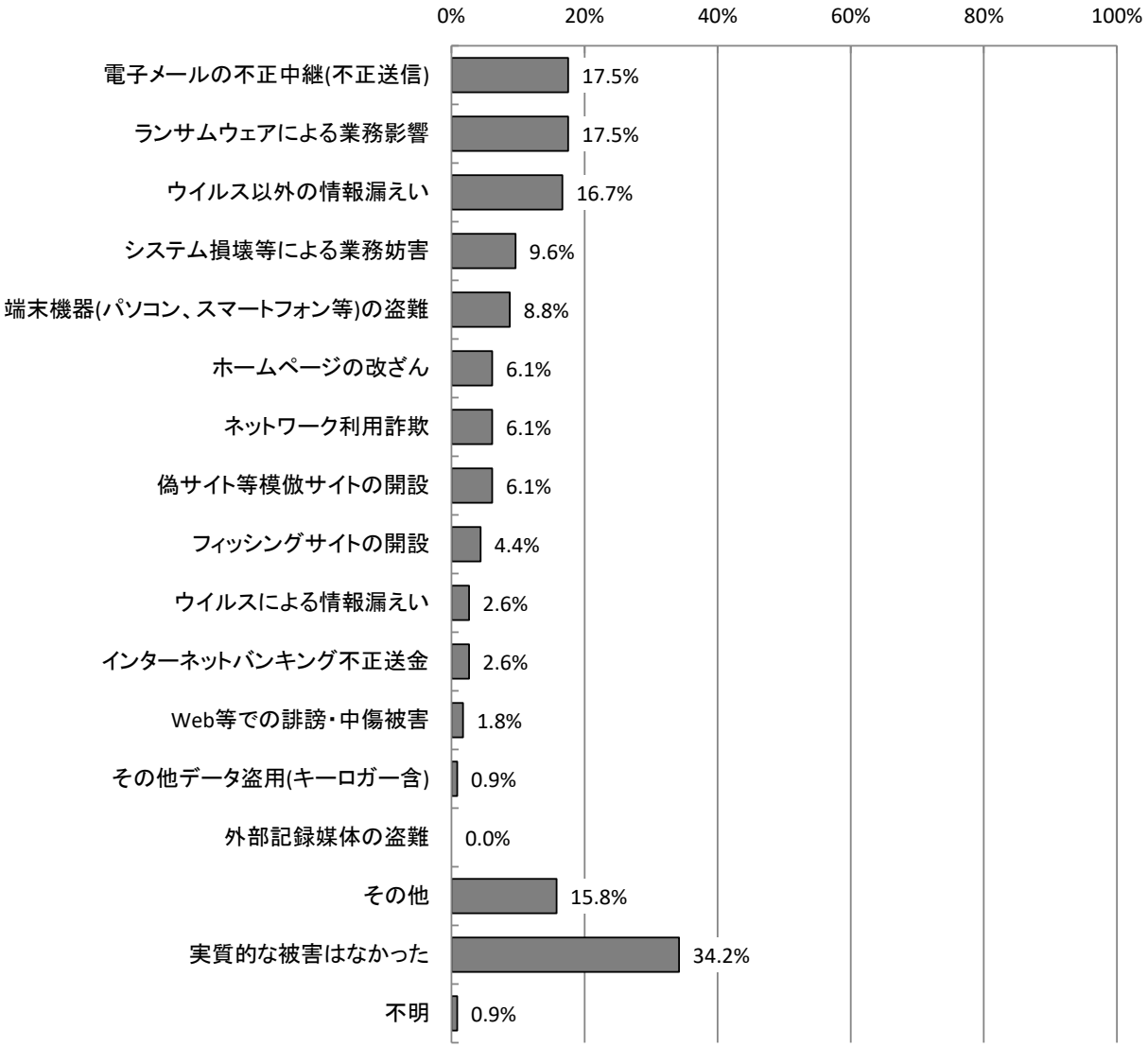
【不正アクセス等の被害状況】

過去1年間に受けたことのある被害状況については、「電子メールの不正中継（不正送信）」「ランサムウェアによる業務影響」が17.5%で最も高く、次いで「ウイルス以外の情報漏えい」が16.7%となっている。また、「実質的な被害はなかった」が34.5%となっている。

届出先機関等については、「警察」が29.8%で最も高く、次いで「個人情報保護委員会」「ベンダー」が27.2%となっている。一方、「届け出なかった」は31.6%と3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86.1%で最も高く、次いで「社・団体内で対応できたので」「自社内だけの被害だったので」がいずれも13.9%となっている。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1年間に受けたことのある被害状況（MA,n=114）



【情報セキュリティの運用・管理体制】

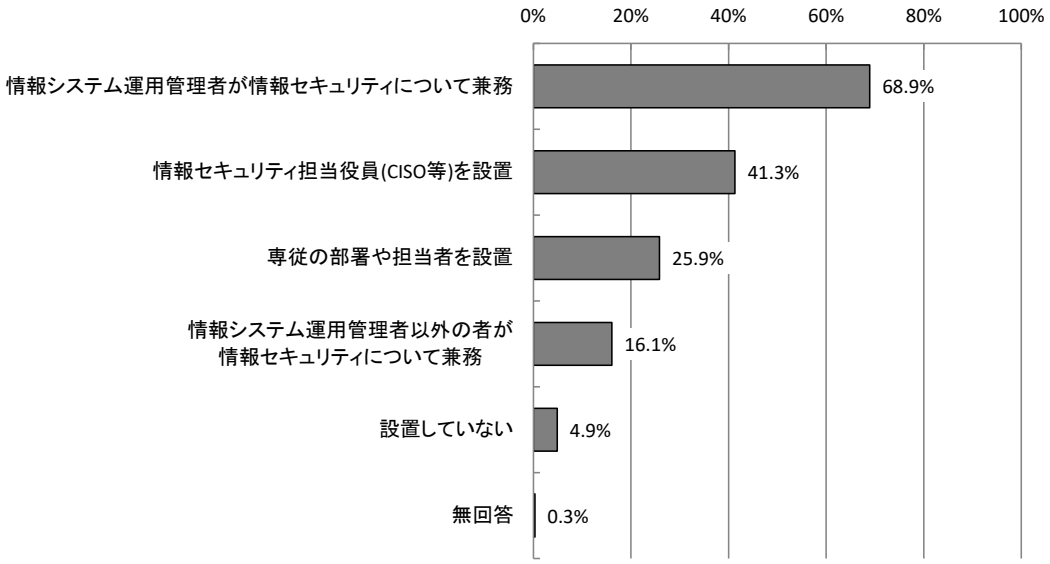
情報セキュリティ管理体制については、「情報システム運用管理者が情報セキュリティについて兼務」が68.9%で最も高く、次いで「情報セキュリティ担当役員(CISO等)を設置」が41.3%、「専従の部署や担当者を設置」が25.9%となっている。

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（定期的な見直しあり）」が61.5%で最も高く、次いで「策定している（定期的な見直しなし）」が21.9%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91.7%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。

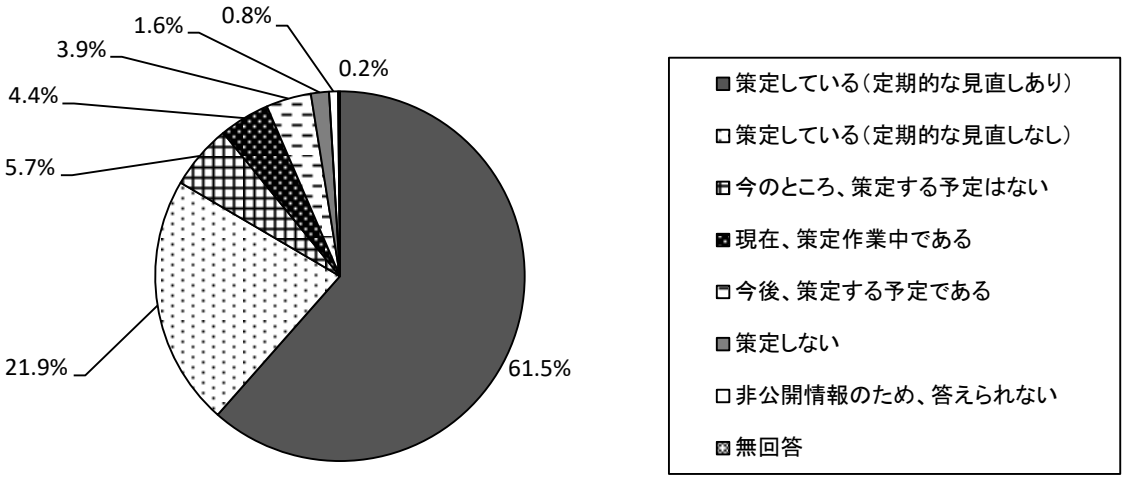
情報セキュリティ侵害事案発生時の対応マニュアル等の策定状況については、「策定している」が51.4%で過半数で、「策定することを検討」が30.3%となっている。

第三者認証機関制度の利用は、「特に利用していない」が77.9%となっている。

【全体】情報セキュリティ管理体制（MA, n=634）



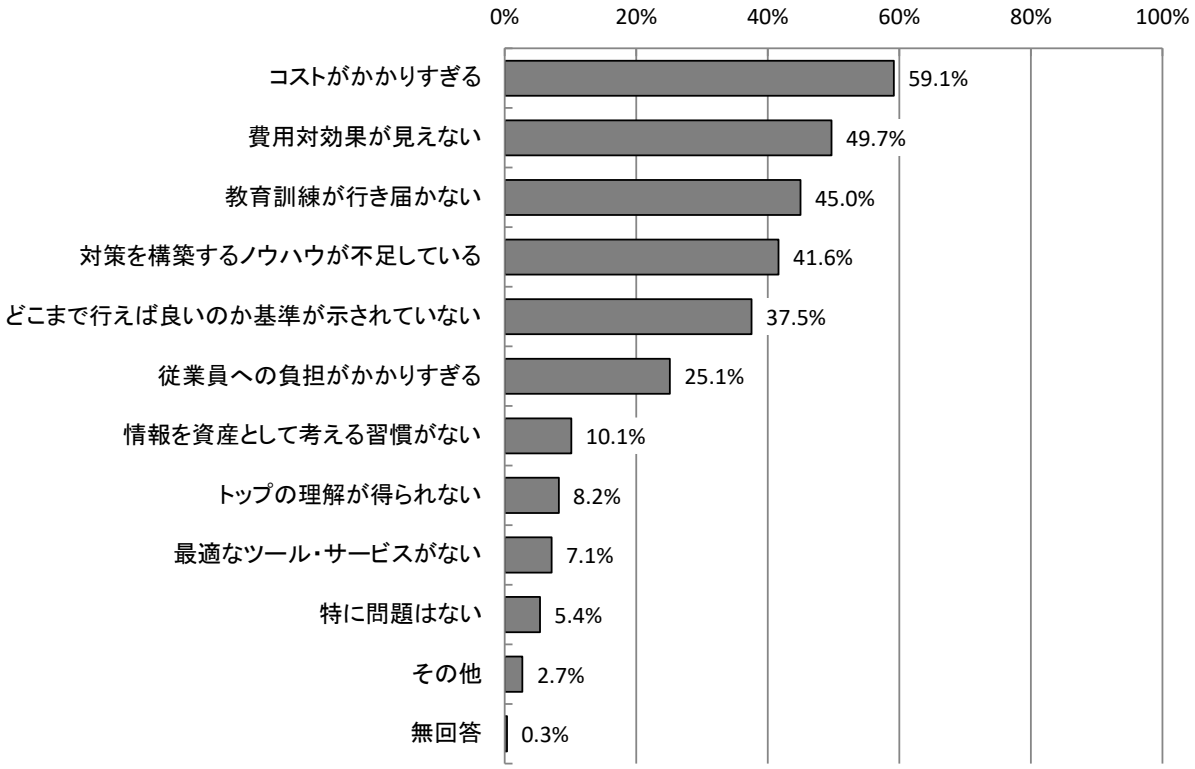
【全体】セキュリティポリシーの策定状況（SA, n=634）



【情報セキュリティ対策への投資】

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59.1%、「費用対効果が見えない」が49.7%で高くなっている。次いで「教育訓練が行き届かない」が45.0%、「対策を構築するノウハウが不足している」が41.6%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=634)

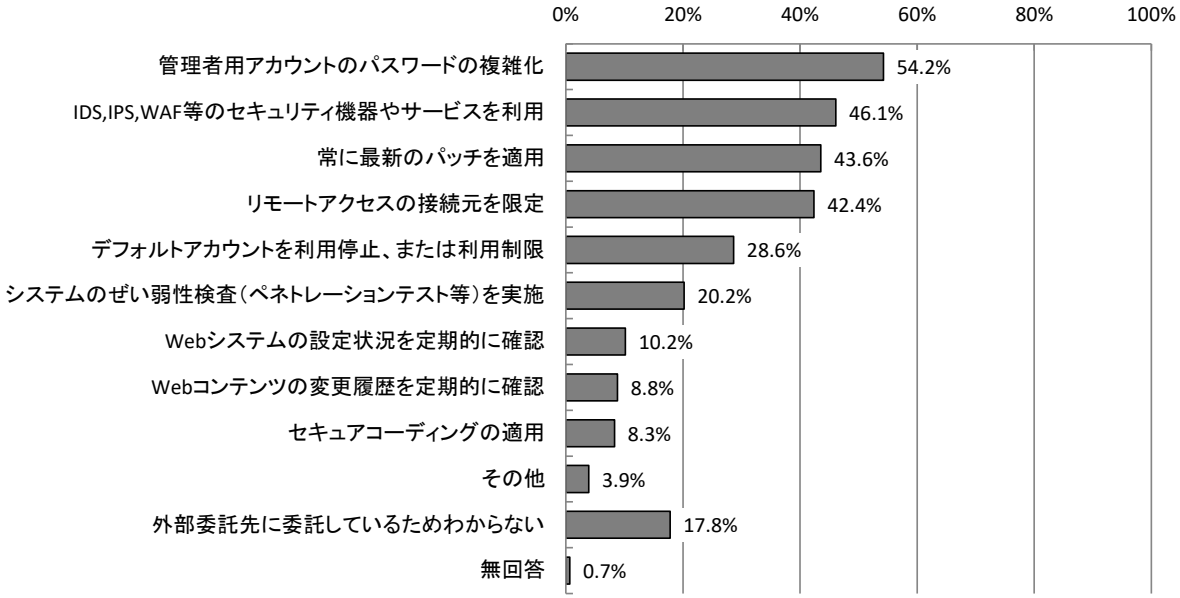


２　技術的対策

【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】

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54.2%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46.1%、「常に最新のパッチを適用」が43.6%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=590）

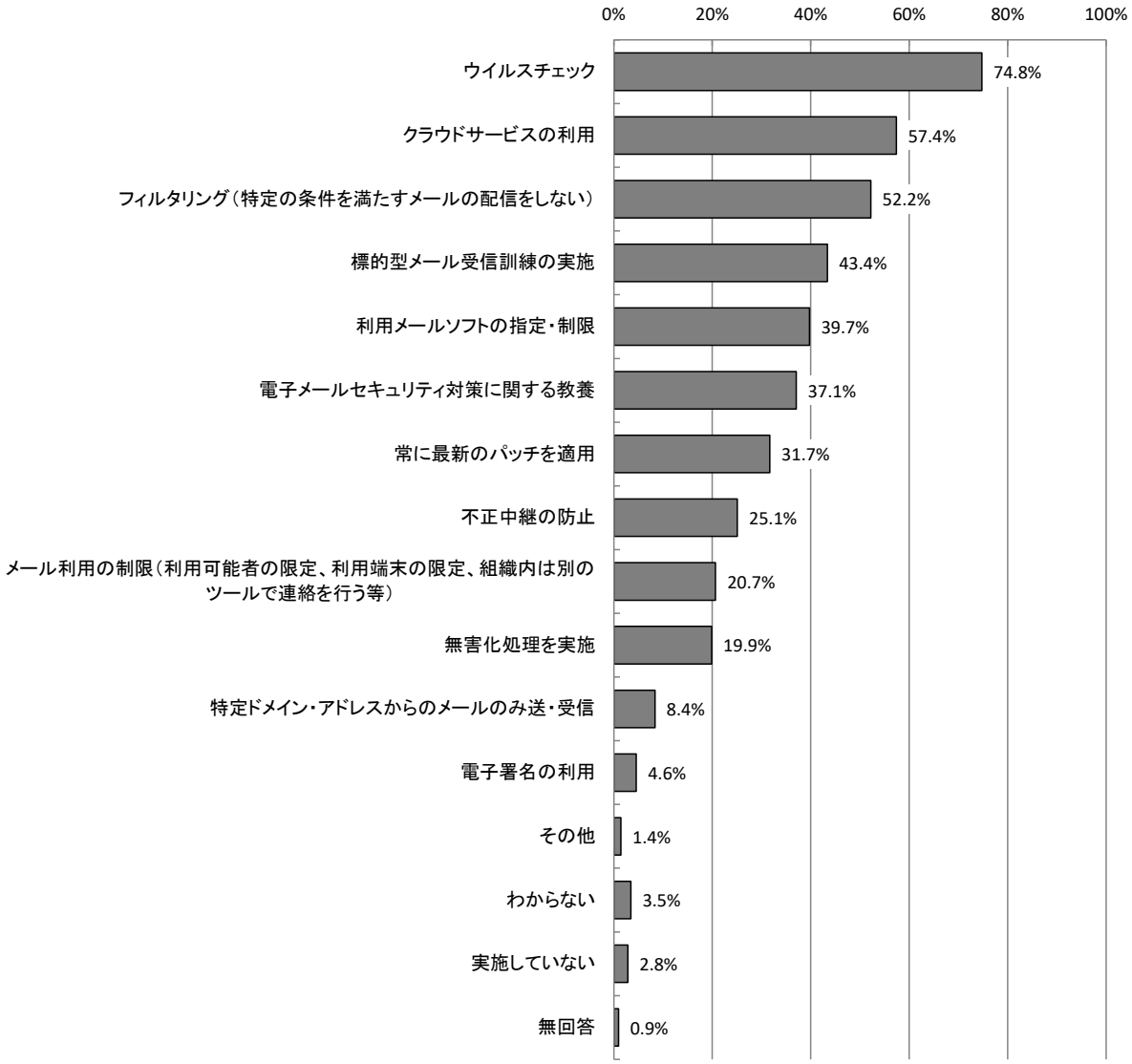


【電子メールに関するセキュリティ対策】

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74.8%で最も高く、次いで「クラウドサービスの利用」が57.4%、「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52.2%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74.0%で最も高い。一方、「特にチェック等はしていない」は13.6%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=634）



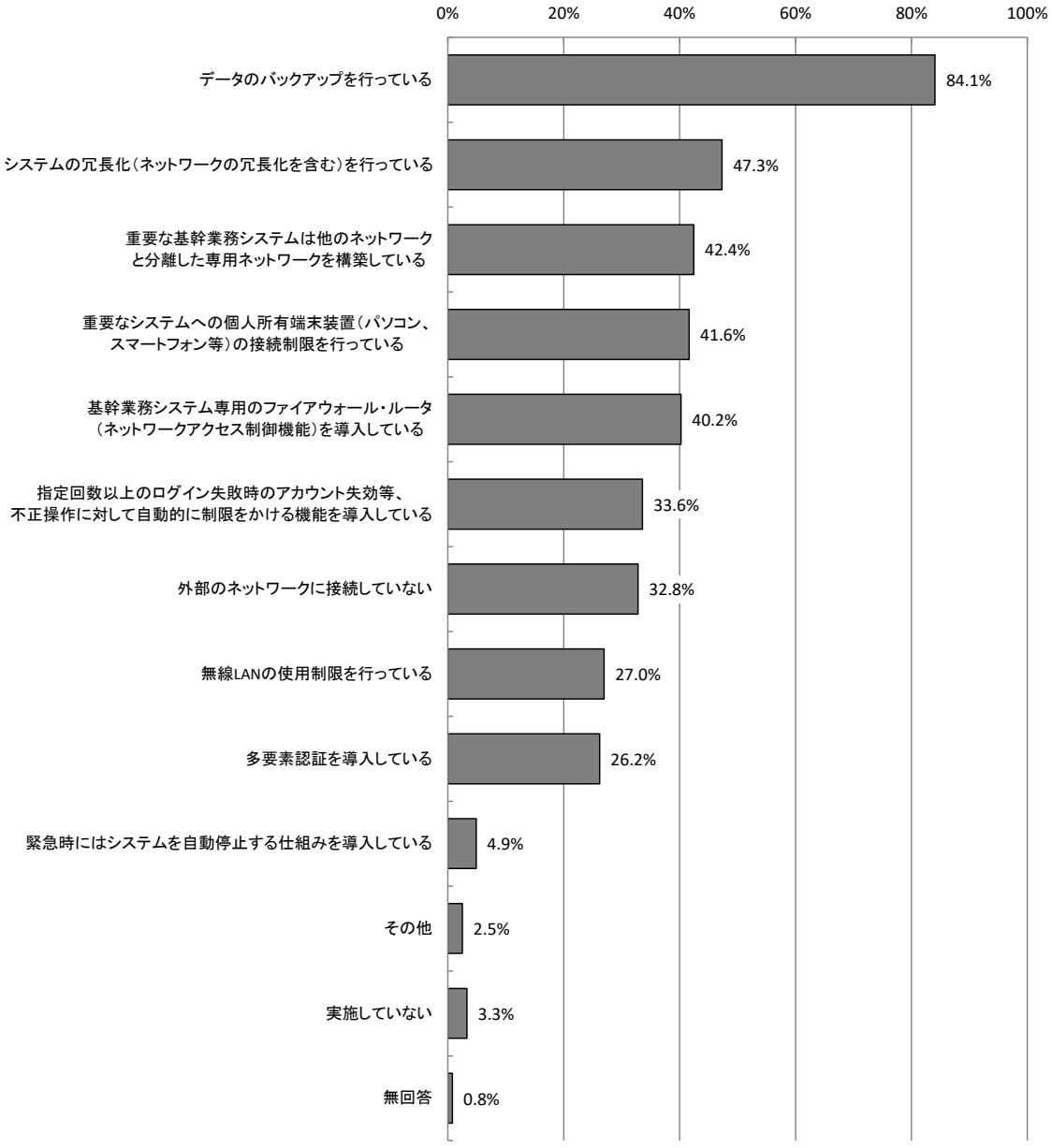
【不正アクセス、情報漏えい等に対する情報セキュリティ対策】

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84.1%で最も高い。

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78.2%で最も高く、次いで「情報資産へのアクセス権の設定」が71.8%、「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69.6%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90.9%で最も高く、次いで「ウイルス対策ソフト（サーバ）の使用」が79.5%、「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71.3%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=634)



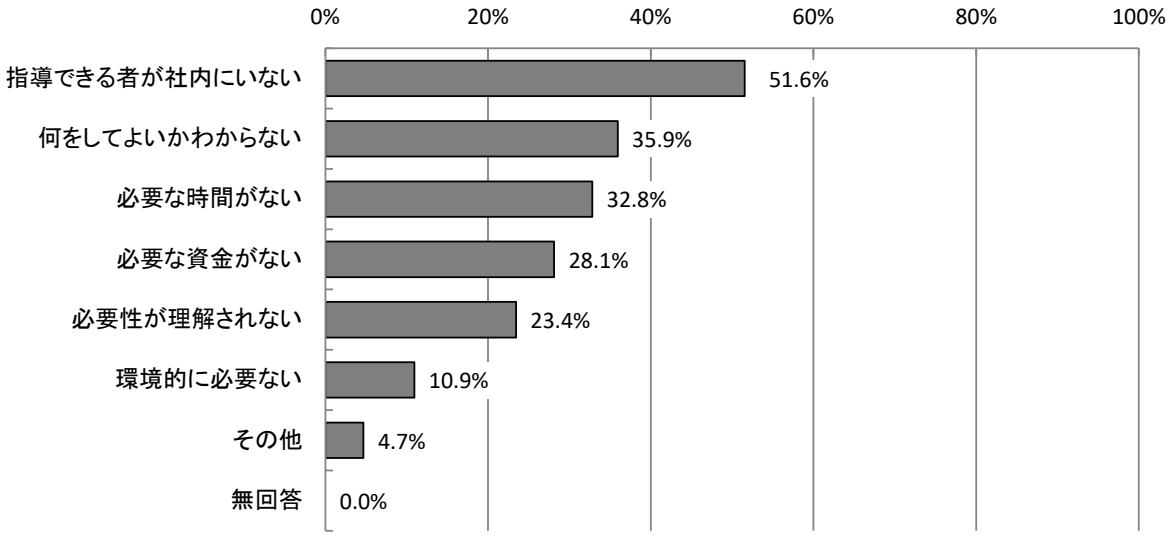
３　人的対策

【情報セキュリティ教育】

情報セキュリティ教育の内容については、「ITリテラシー教育（インターネット・電子メール・SNS等の利用）」が68.3%、「情報セキュリティポリシー」が62.5%で高くなっている。

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51.6%で最も高く、次いで「何をしてよいかわからない」が35.9%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=64)

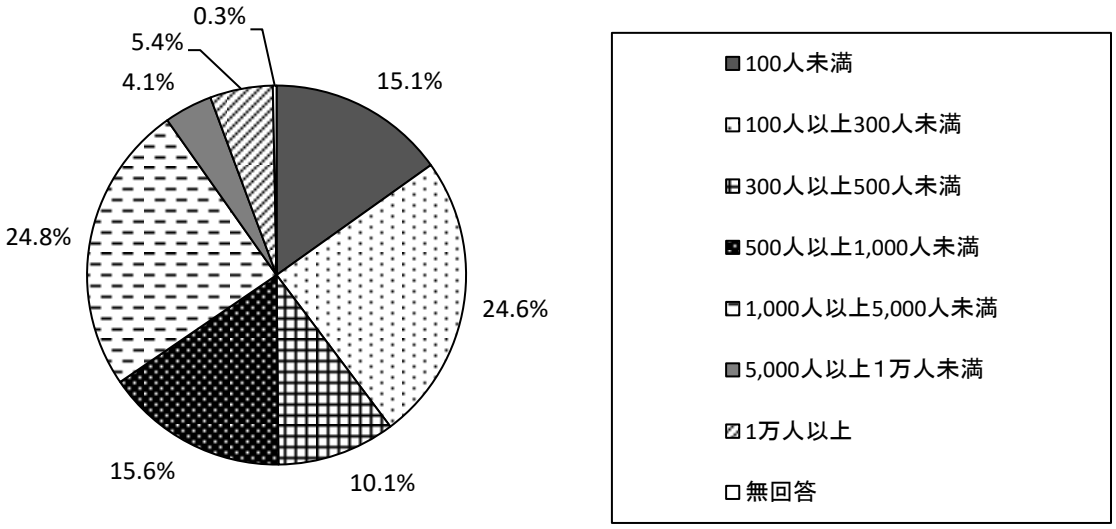


今回の調査結果では、全体の８割以上で情報セキュリティポリシーが制定されており、情報セキュリティに関する教育においても、「実施していない」は10.1%と全体の１割程度で、情報セキュリティに関する意識について一定の浸透が図られていることがうかがえる。その一方で、情報セキュリティ対策についてコストがかかりすぎる・費用対効果が見えない等の問題意見が出されるなど、問題点も明らかになった。

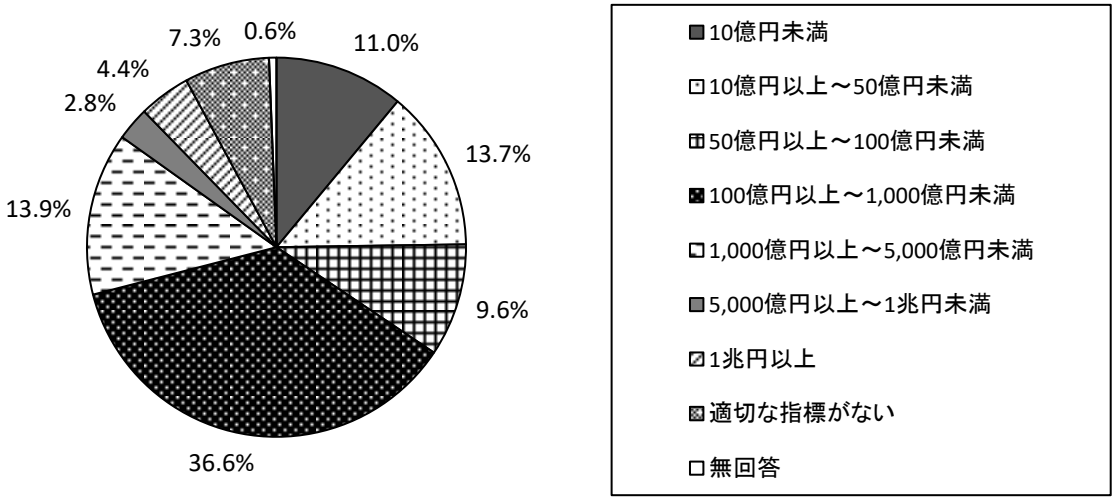
また、過去1年間に攻撃・被害を受けた社・団体等が全体の18.0%と依然として少なくない。セキュリティ侵害事案発生時における対応マニュアルを策定していると回答した社・団体は半数程度にとどまっている状況であり、事案発生の際の被害拡大防止のため、これら対策意識の浸透が今後の課題といえよう。

2.2 回答事業体の属性等

【全体】従業員規模（SA, n=634）【問2】



【全体】予算規模（SA, n=634）【問3】



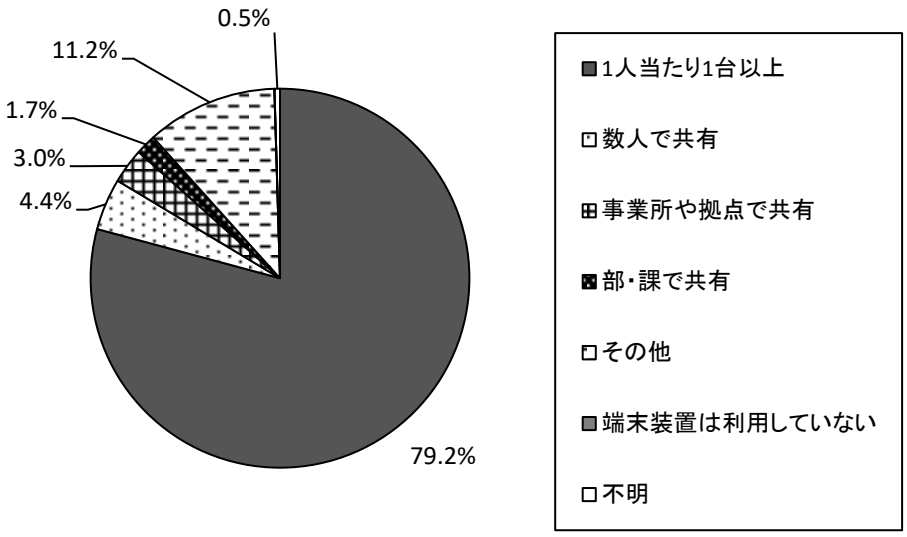
3. 調査結果

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】

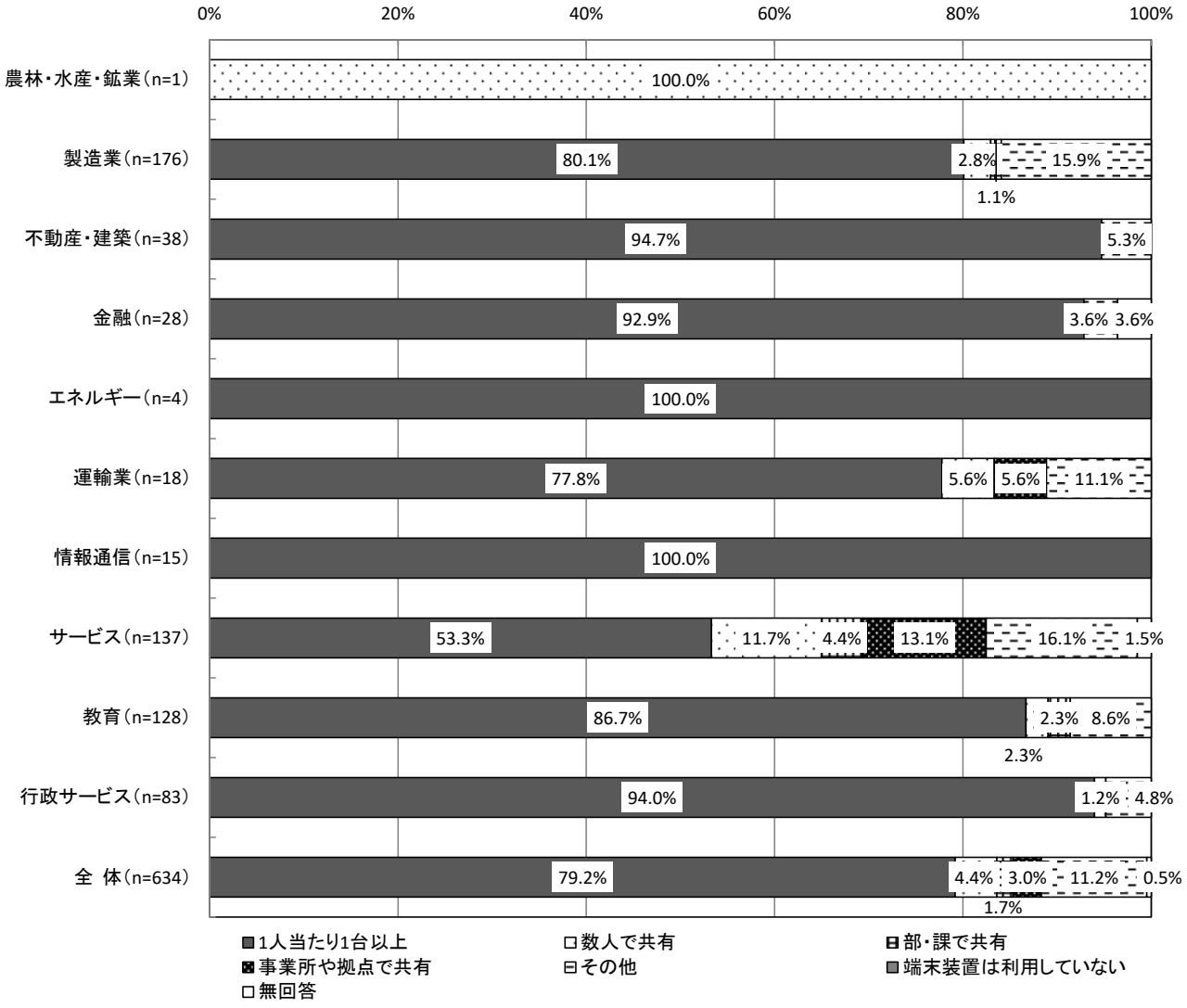
端末装置（パソコン）の整備環境については、「1人当たり1台以上」が79.2%で最も高く、「数人で共有」が4.4%、「事務所や拠点で共有」が3.0%となっている。

【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=634）



【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」が100.0%、「不動産・建築」が94.7%、「行政サービス」が94.0%、「金融」が92.9%で9割を超えて高い割合となっている。一方、「サービス」で53.3%と最も低くなっている。

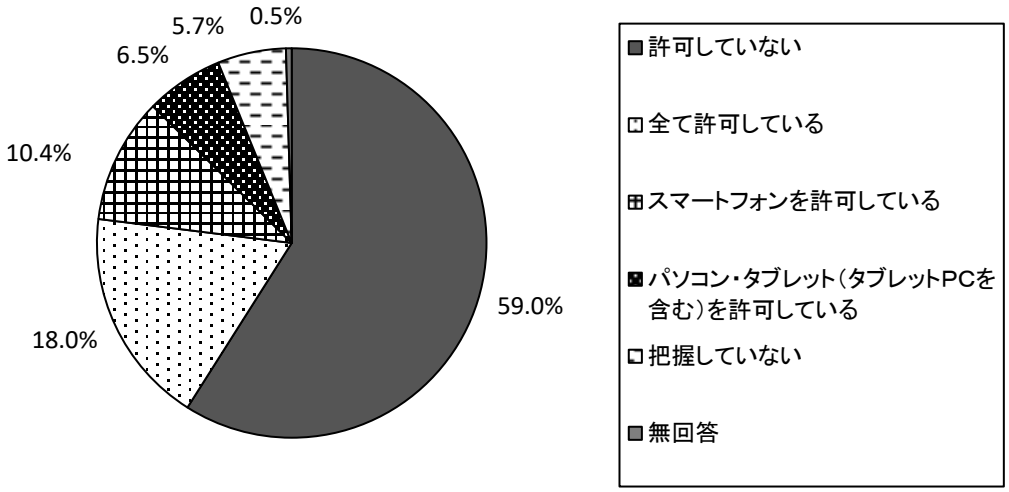
【業種別分析】端末装置（パソコン、スマートフォン等）の整備環境



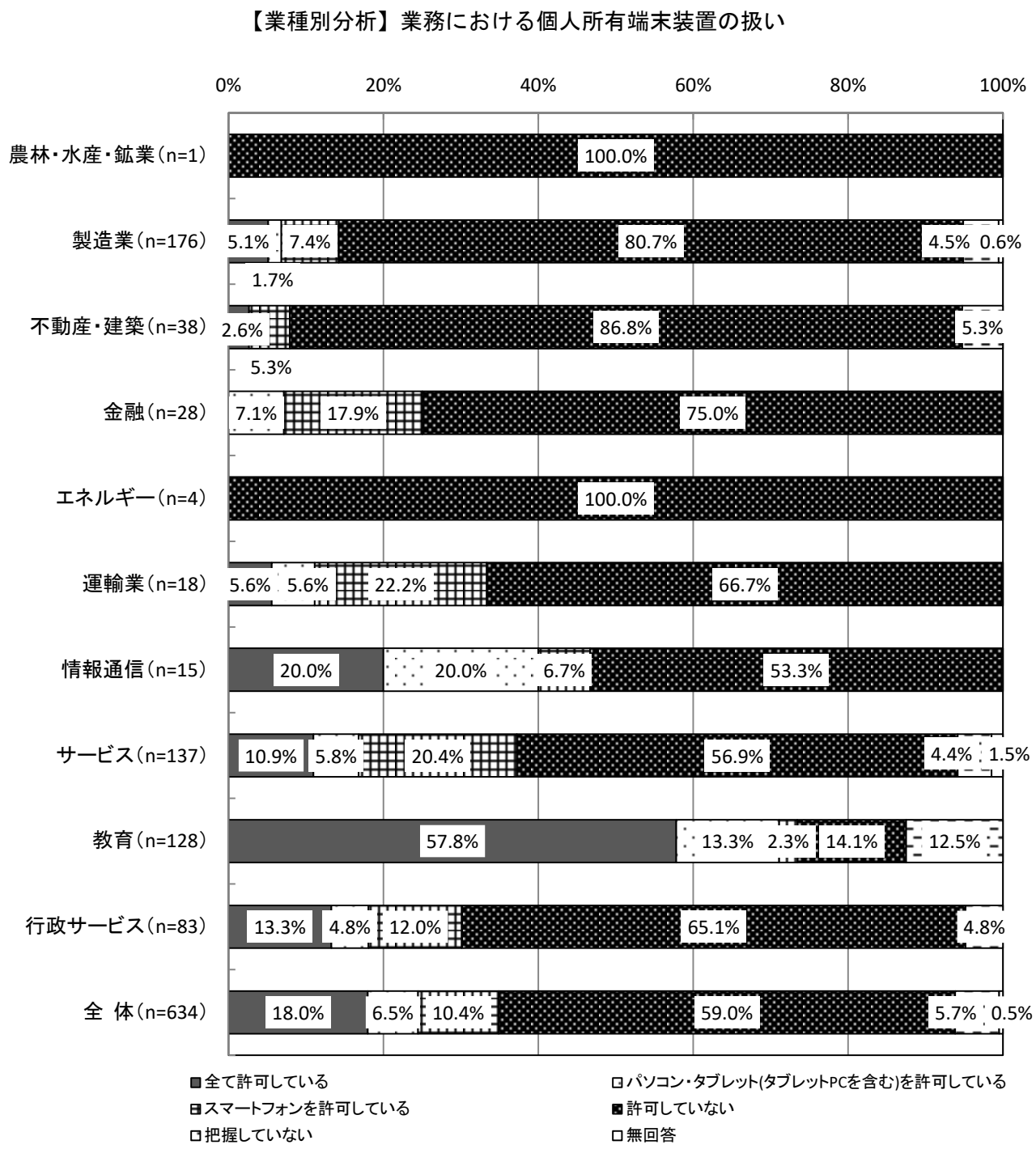
3.1.2　業務における個人所有端末装置の扱い　【問5】

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59.0％で最も高く、「全て許可している」が18.0％、「スマートフォンを許可している」が10.4％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=634）

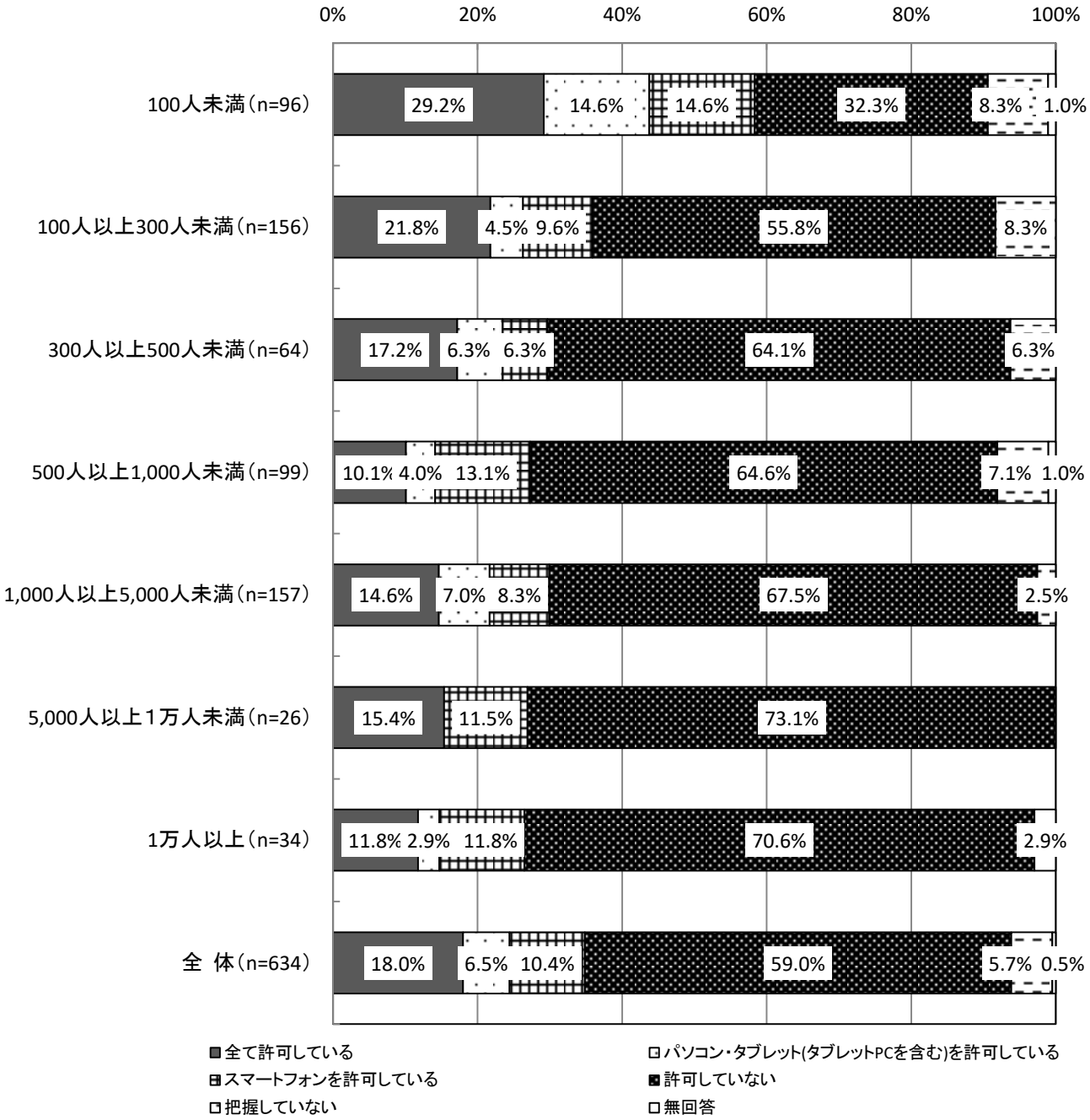


【業種別分析】業種別にみると、「許可していない」では、「不動産・建築」が86.8%で最も高く、次いで「製造業」が80.7%となっている。一方、最も低いのは「教育」で14.1%となっている。



【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、「5,000人以上１万人未満」が73.1%、「1万人以上」が70.6%で7割を超えている。一方、最も低いのは「100人未満」32.3%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

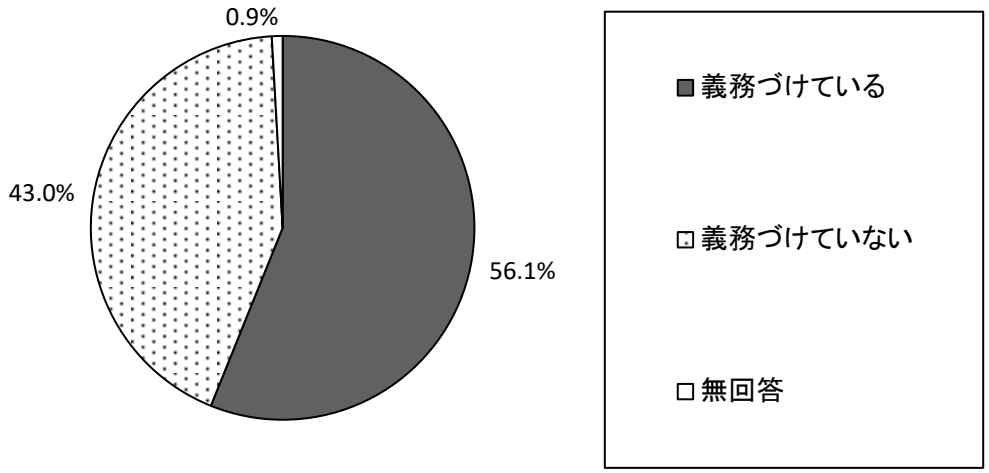


3.1.3　個人所有端末装置のセキュリティ対策【問5-1】

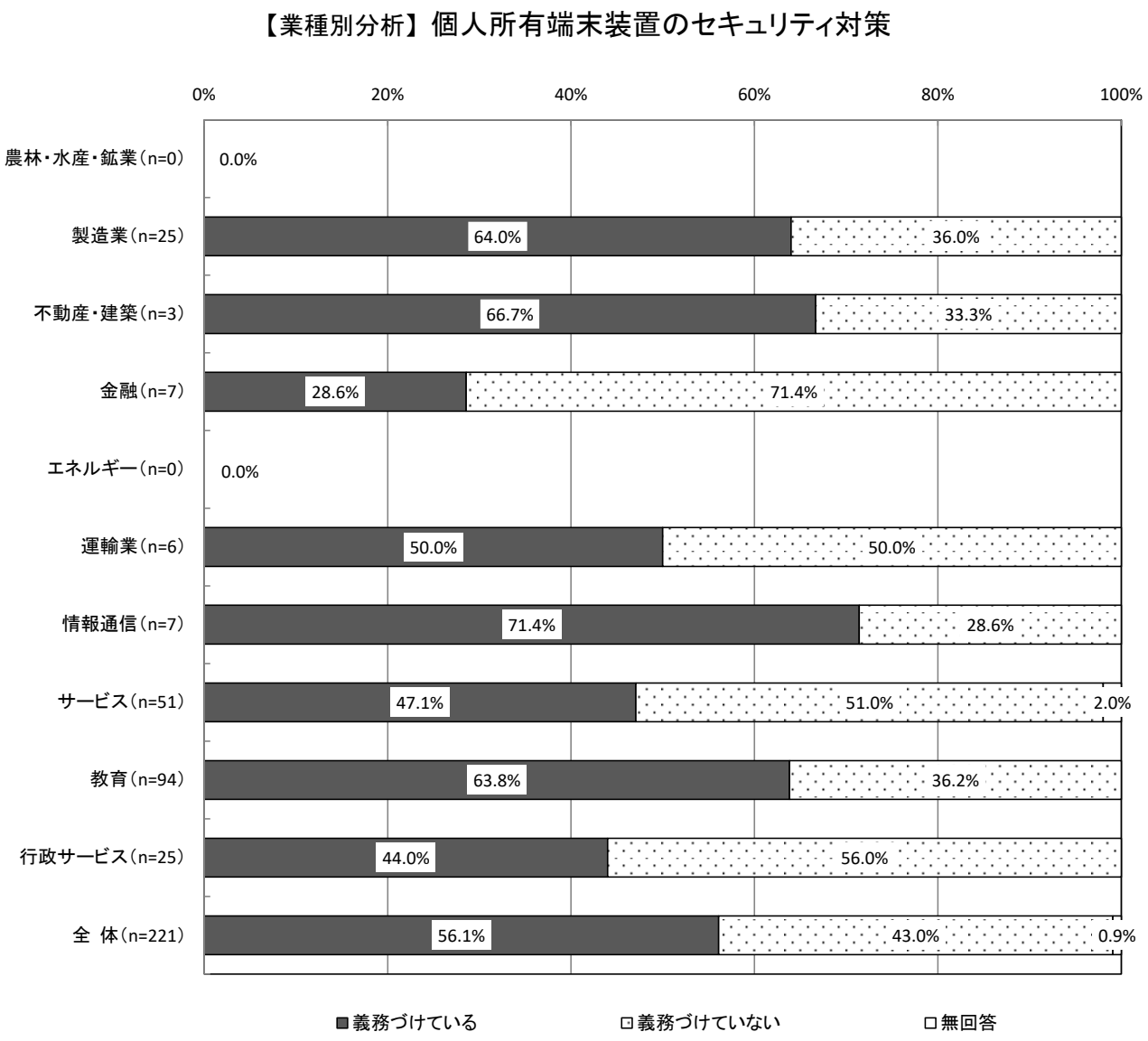
個人所有端末装置のセキュリティ対策については「義務づけている」が56.1%で高くなっている。これに対して「義務づけていない」は43.0%となっている。

※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=221）

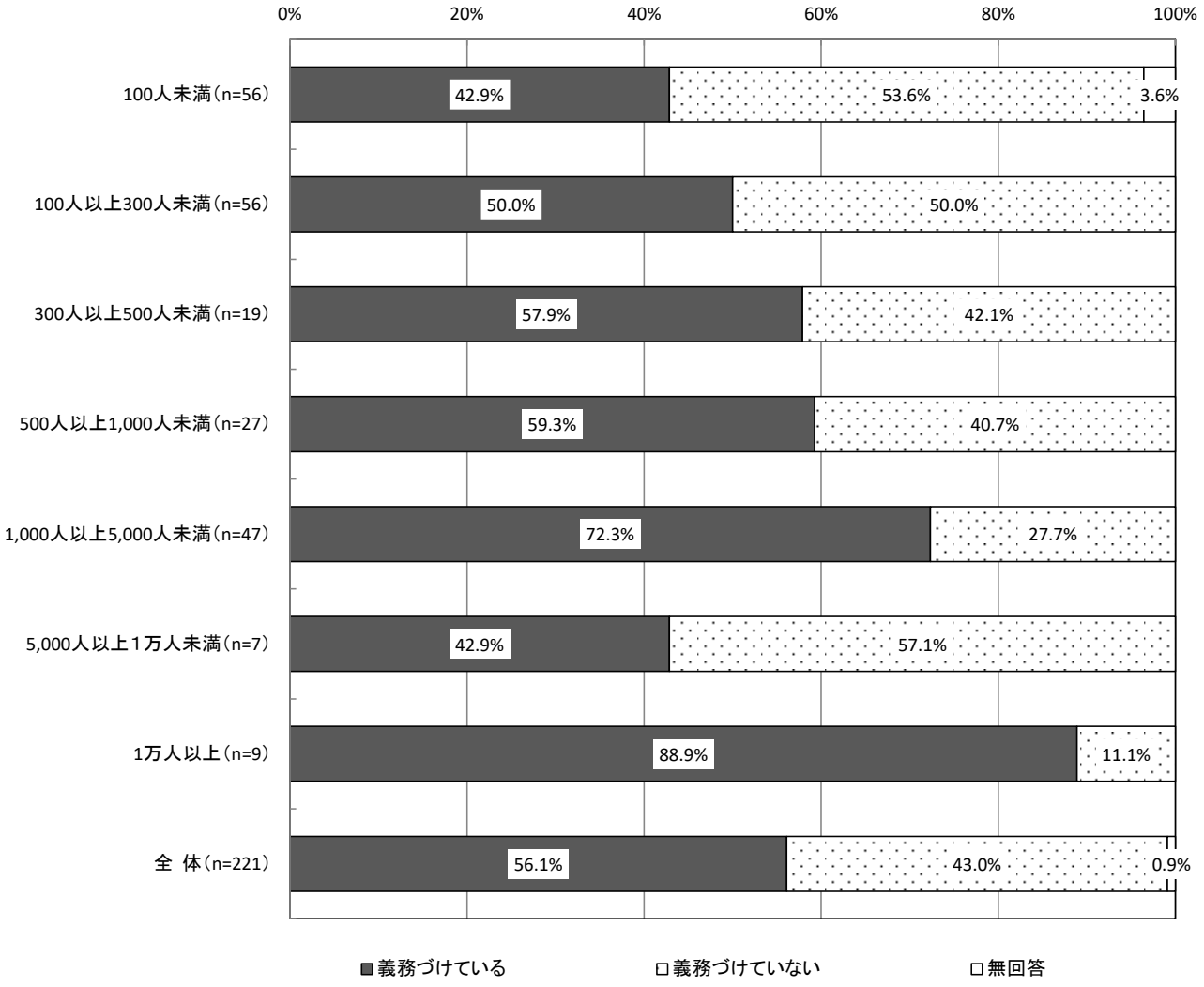


【業種別分析】業種別にみると、「義務づけている」は「情報通信」が71.4%、「製造業」が64.0%、「教育」が63.8%でいずれも高い。一方「金融」が28.6%で低くなっている。



【従業員規模別分析】従業員規模別にみると、「義務づけている」は「1万人以上」が88.9%、「1,000人以上5,000人未満」が72.3%、「500人以上1,000人未満」が59.3%で高くなっている。これに対して「100人未満」「5,000人以上1万人未満」は42.9%と低くなっている。

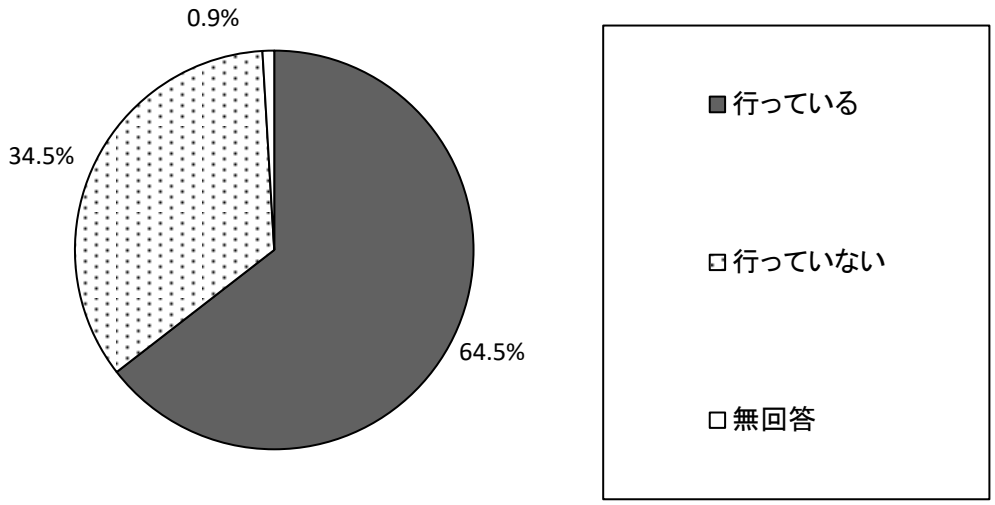
【従業員規模別分析】個人所有端末装置のセキュリティ対策



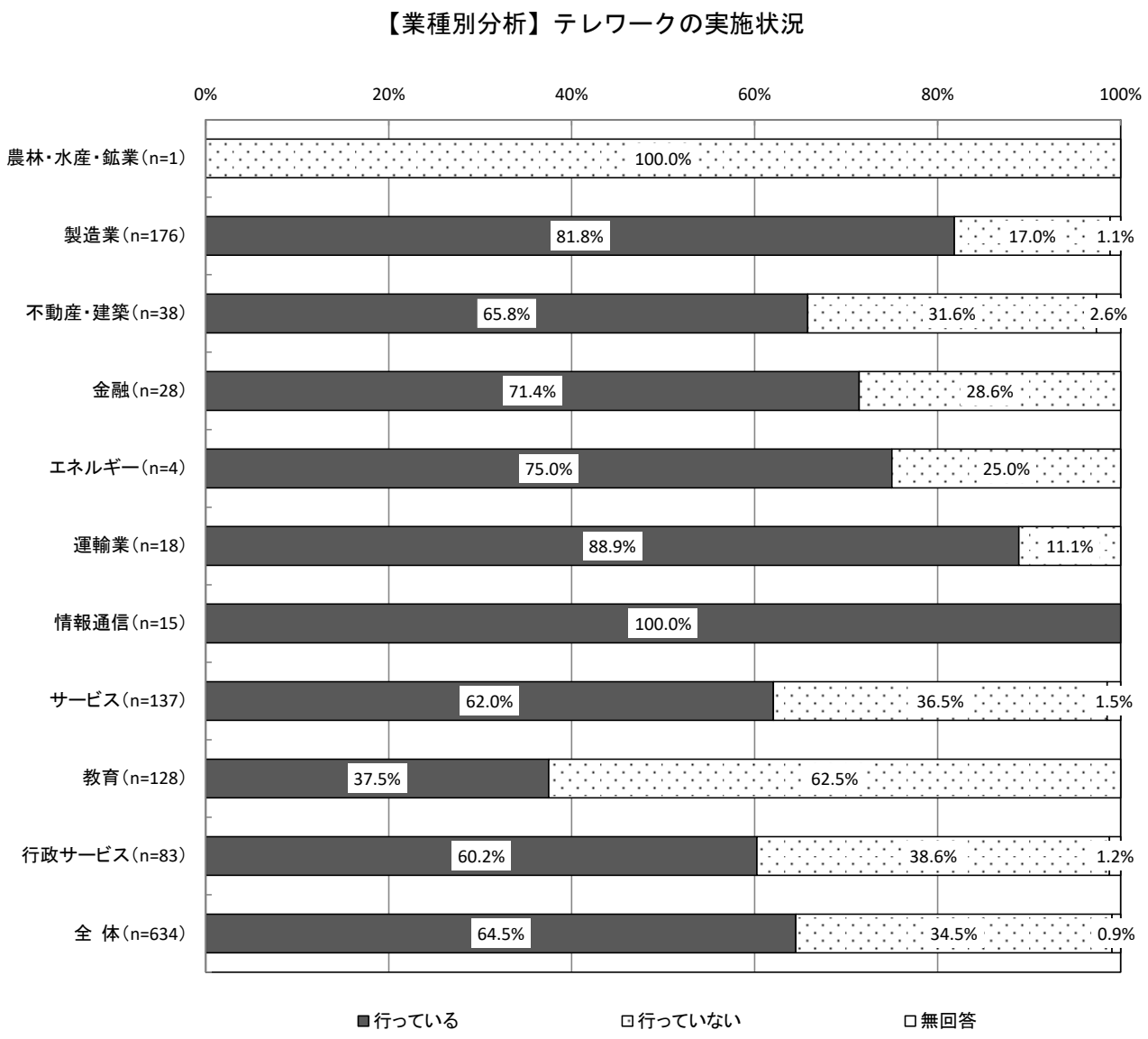
3.1.4　テレワークの実施状況　【問6】

テレワークの実施状況については、「行っている」が64.5%と高くなっている。これに対して、「行っていない」は、34.5%となっている。

【全体】テレワークの実施状況（SA,n=634）

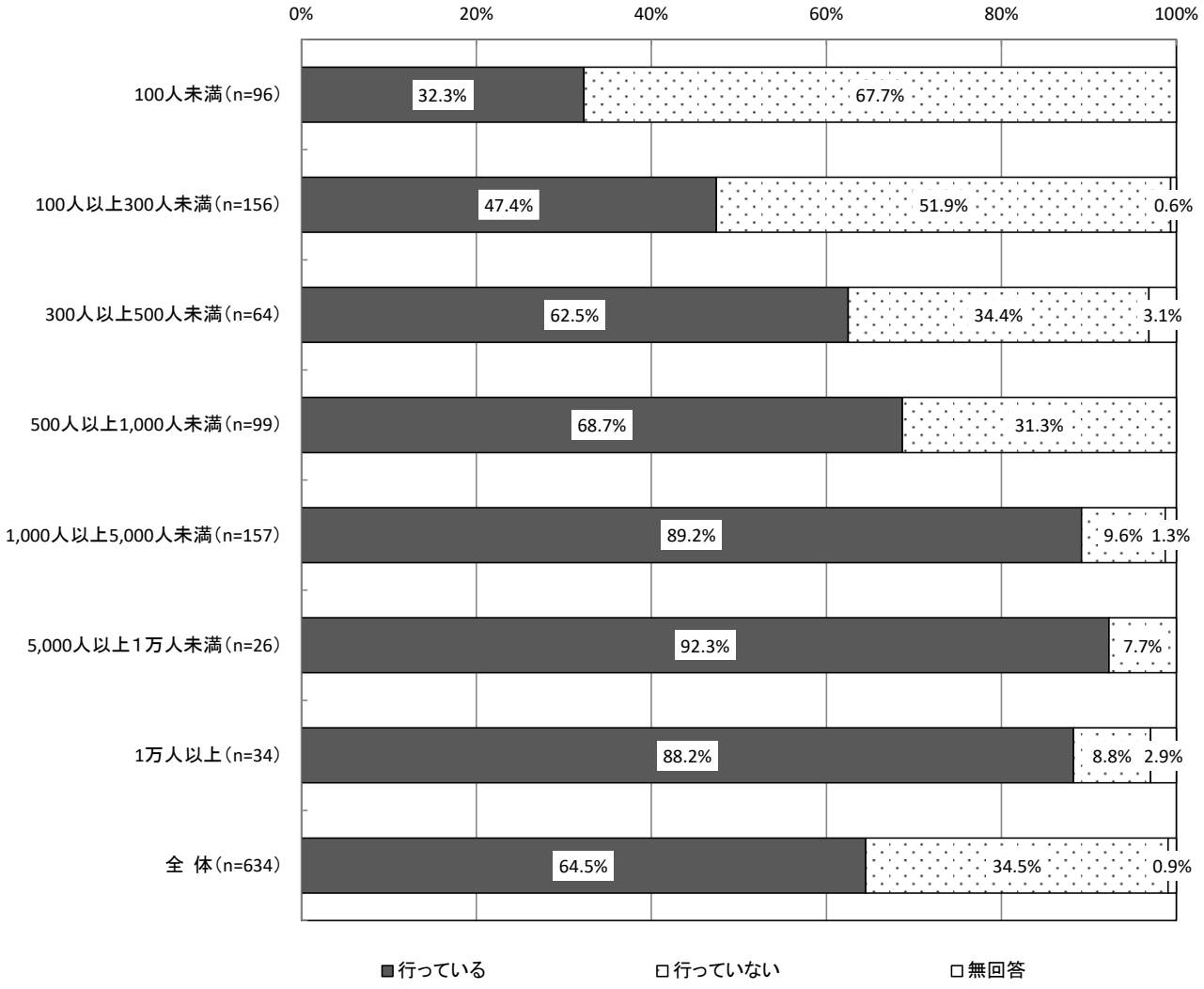


【業種別分析】業種別にみると、「行っている」は、「情報通信」が100.0％で高く、次いで「運輸業」が88.9％、「製造業」が81.8％となっている。一方、最も低いのは「教育」で37.5％となっている。



【従業員規模別分析】従業員規模別にみると、「行っている」では、「5,000人以上１万人未満」が92.3%で9割を超えて高くなっている。「行っている」割合は概ね従業員数規模が大きいほど高くなっており、従業員規模が「100人未満」で32.3%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

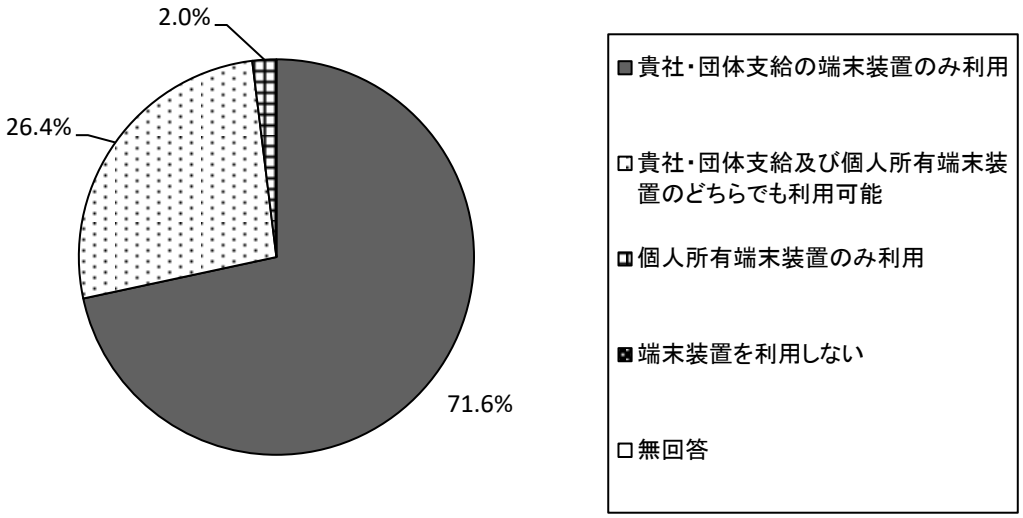


3.1.5　テレワーク業務の端末装置（パソコン、スマートフォン等）の利用環境　【問6-1】

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71.6%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26.4%、「個人所有端末装置のみ利用」が2.0%となっている。

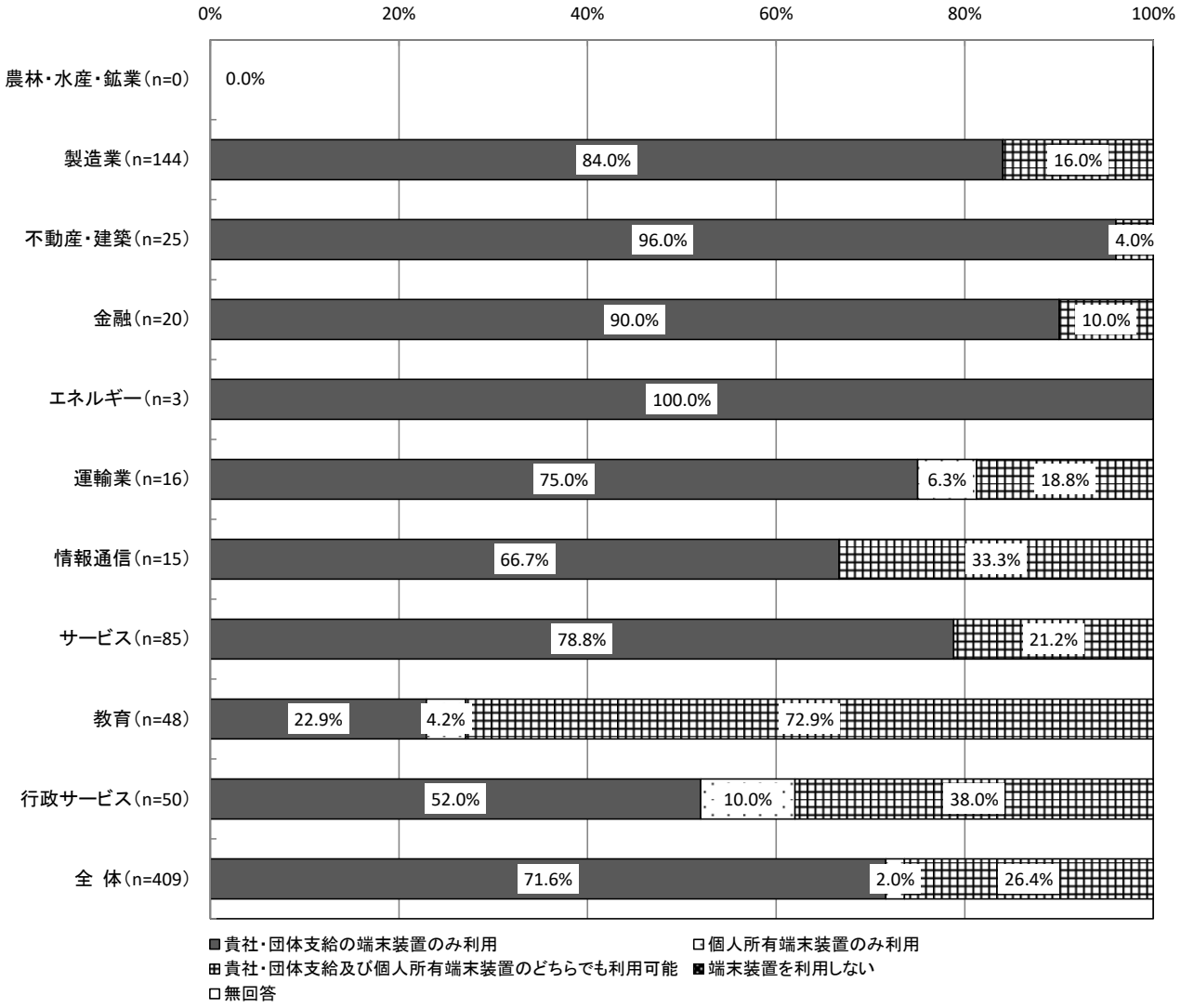
※本項目は、テレワークを実施している社・団体等を対象としている。

【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=409）



【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、「不動産・建築」が96.0%、「金融」が90.0%で高い。一方で、「教育」は22.9%で最も低くなっている。

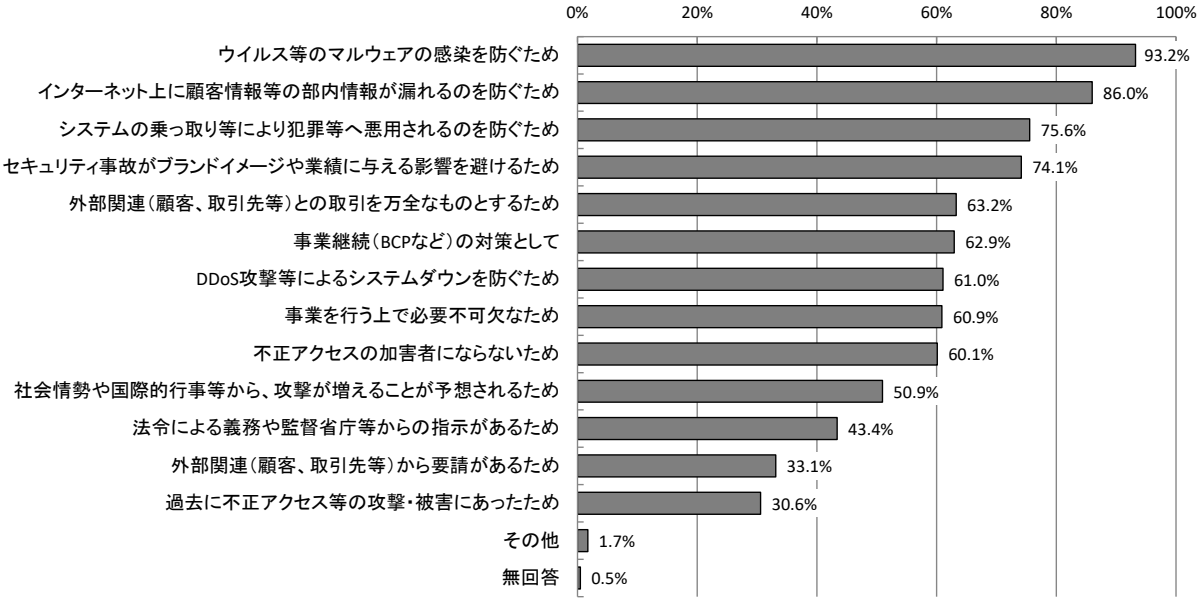
【業種別分析】テレワーク業務の端末装置（パソコン、スマートフォン等）の利用環境



3.1.6　情報セキュリティ対策の必要性の理由【問7】

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93.2%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86.0%、「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75.6%、「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74.1%となっている。

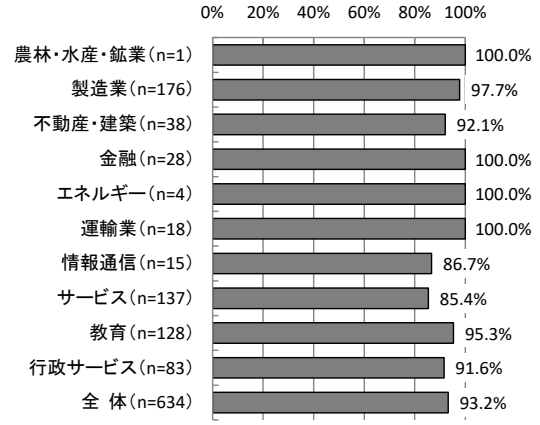
【全体】情報セキュリティ対策の必要性の理由（MA,n=634）



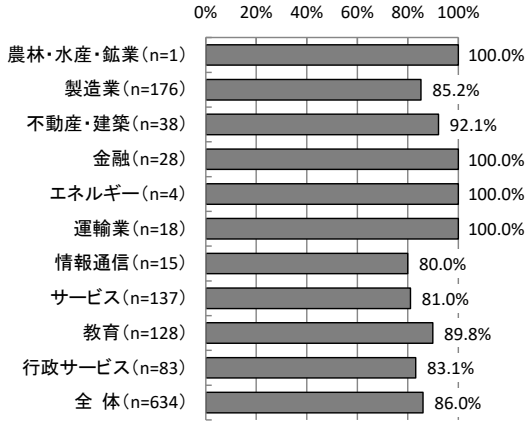
【業種別分析】業種別にみると、「ウイルス等のマルウェアの感染を防ぐため」では「金融」「運輸業」が100.0%、「製造業」が97.7%、「教育」が95.3%と高い。「インターネット上に顧客情報等の部内情報が漏れるのを防ぐため」では「金融」「運輸業」が100.0%で高い。

【業種別分析】情報セキュリティ対策の必要性の理由

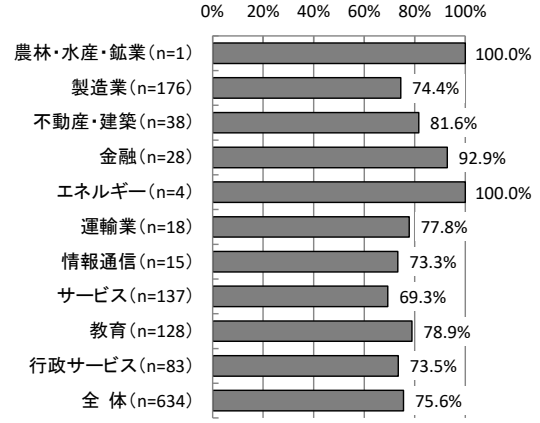
ウイルス等のマルウェアの感染を防ぐため



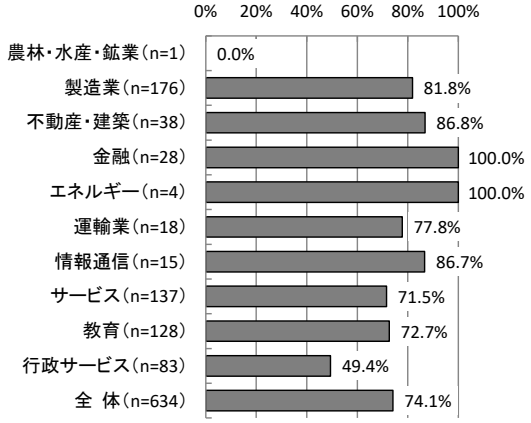
インターネット上に顧客情報等の部内情報が漏れるのを防ぐため



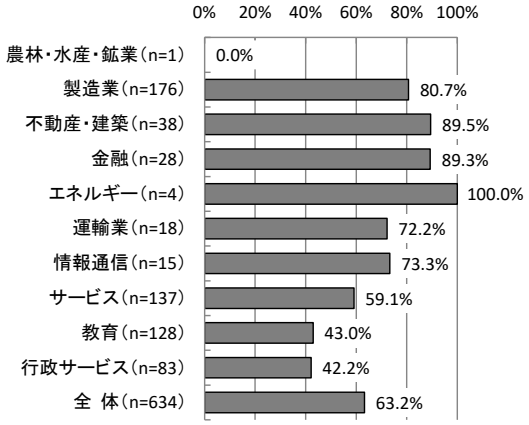
システムの乗っ取り等により犯罪等へ悪用されるのを防ぐため



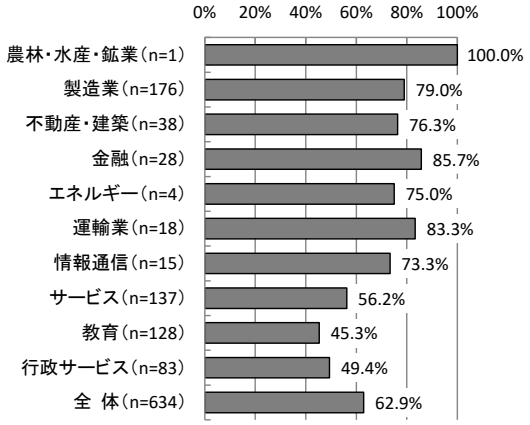
セキュリティ事故がブランドイメージや業績に与える影響を避けるため



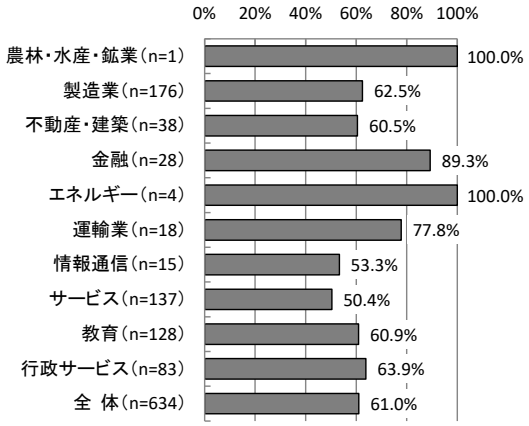
外部関連（顧客、取引先等）との取引を万全なものとするため



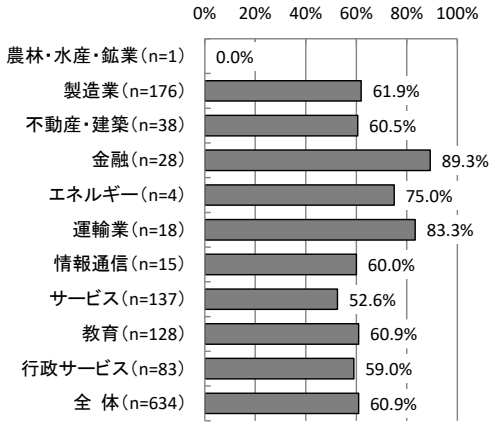
事業継続（BCPなど）の対策として



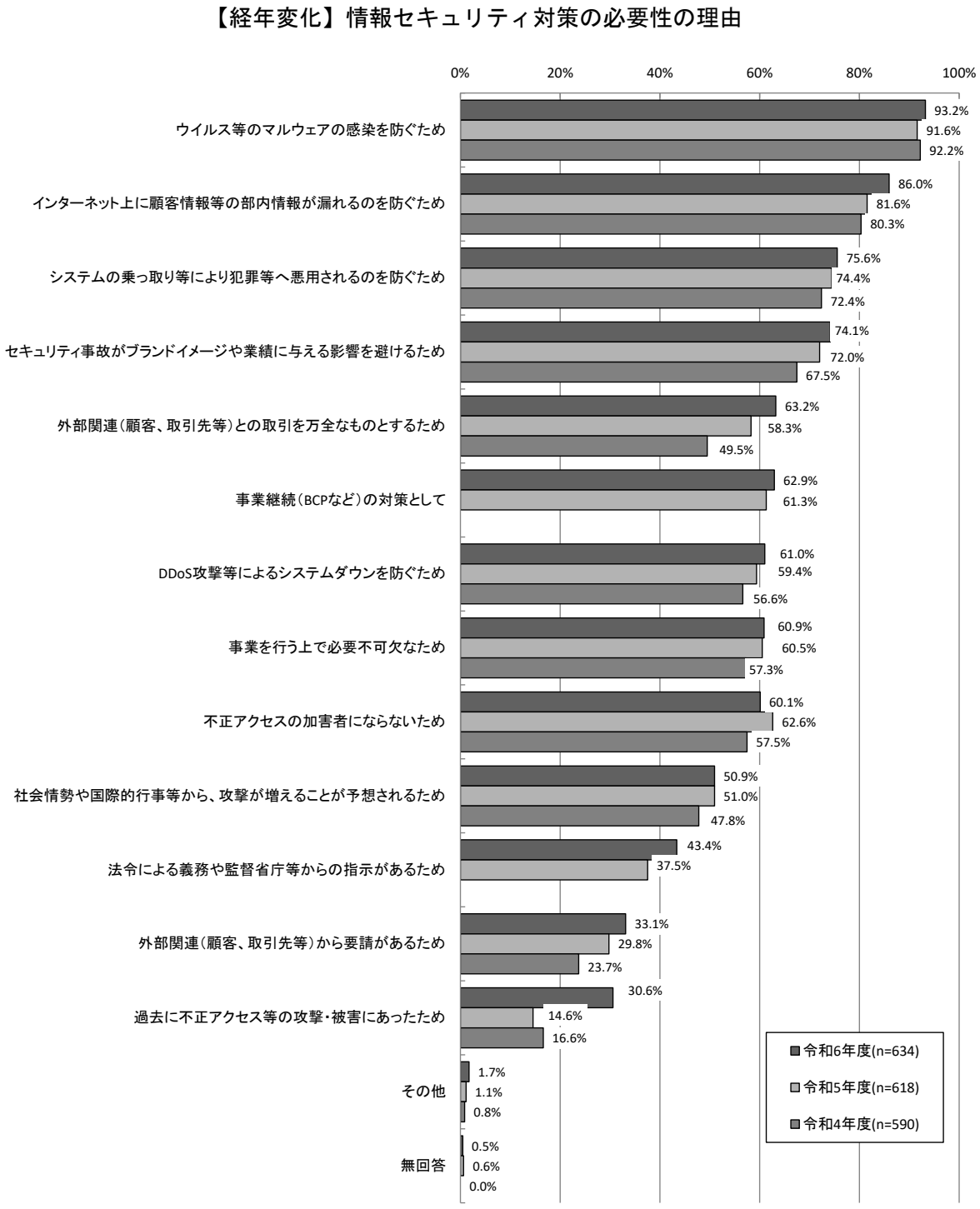
DDoS攻撃等によるシステムダウンを防ぐため



事業を行う上で必要不可欠なため



【経年変化】昨年度と比較すると、「過去に不正アクセス等の攻撃・被害にあったため」が16.0ポイント増加している。

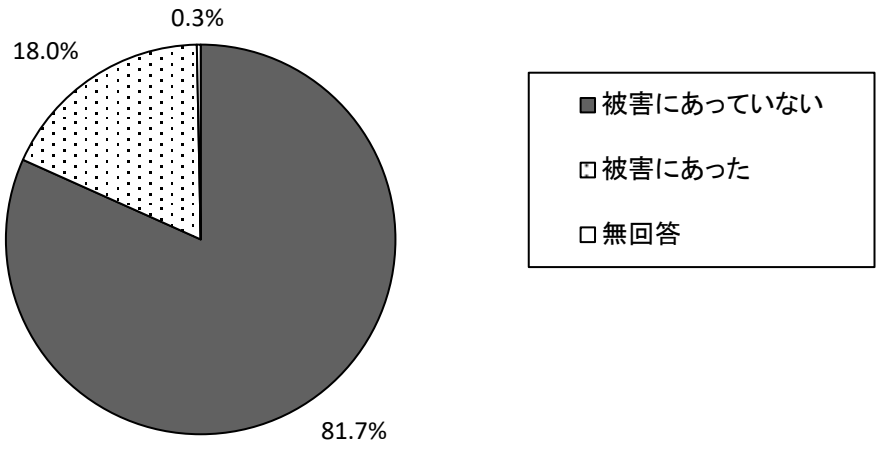


※令和５年度調査で「事業継続(BCPなど)の対策として」「法令による義務や監督省庁等からの指示があるため」を新設

3.1.7　過去1年間の不正アクセス攻撃・被害【問8】

過去1年間の不正アクセス攻撃・被害については、「被害にあっていない」が81.7%、「被害にあった」が18.0%となっている。

【全体】過去1年間の不正アクセス攻撃・被害（SA,n=634）

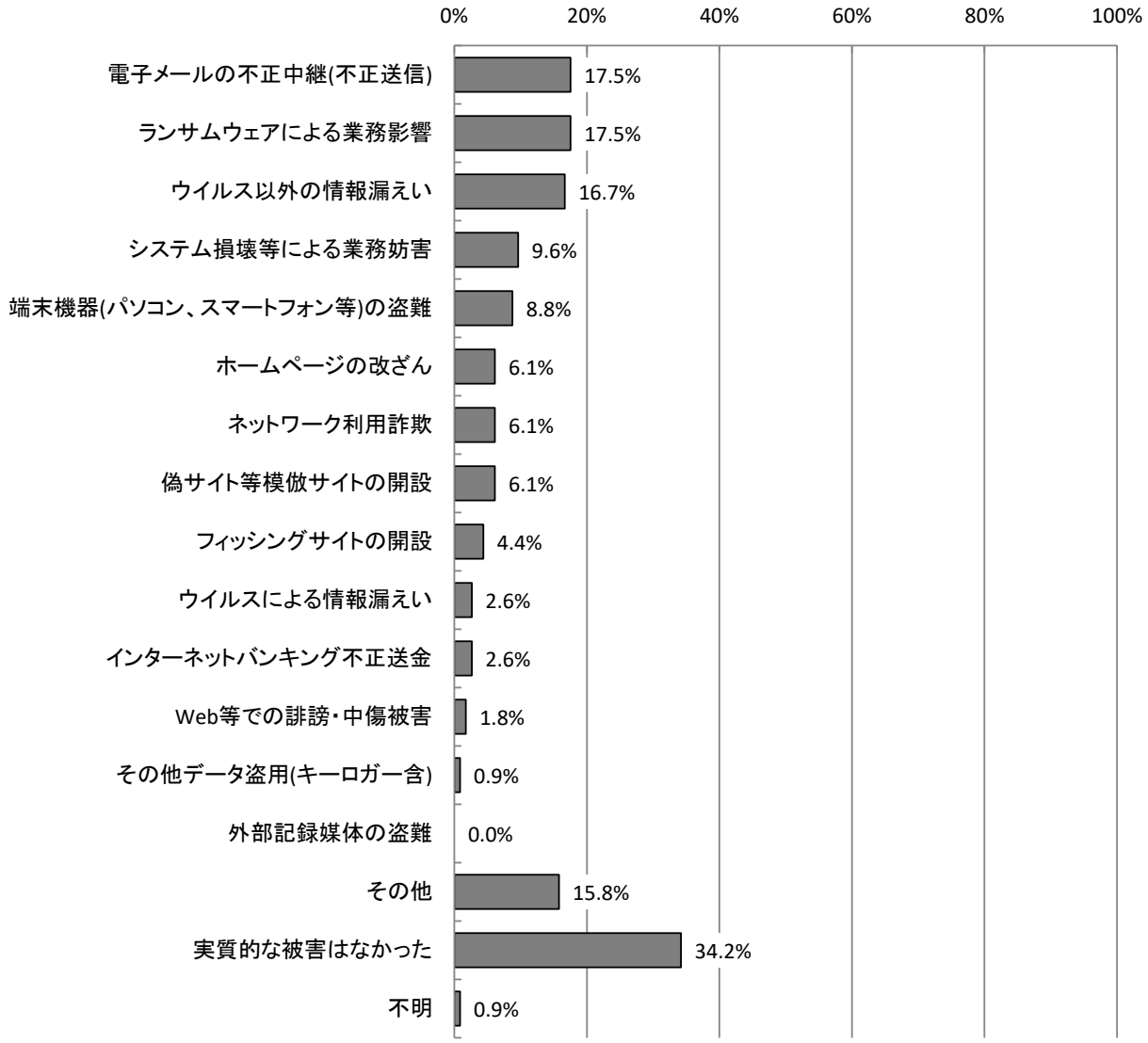


3.1.8　過去1年間に受けたことのある被害状況【問8-1】

過去1年間に受けたことのある被害状況については、「電子メールの不正中継（不正送信）」「ランサムウェアによる業務影響」が17.5%で最も高く、次いで「ウイルス以外の情報漏えい」が16.7%となっている。また、「実質的な被害はなかった」が34.2%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。

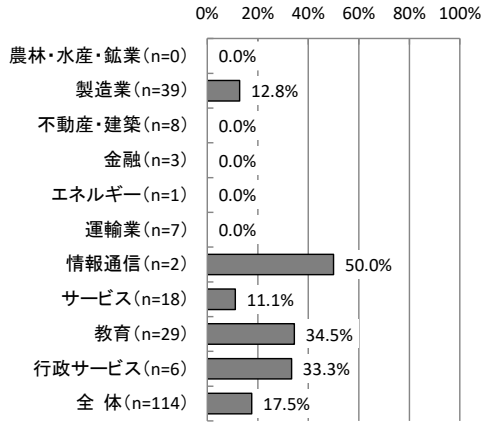
【全体】過去1年間に受けたことのある被害状況（MA, n=114）



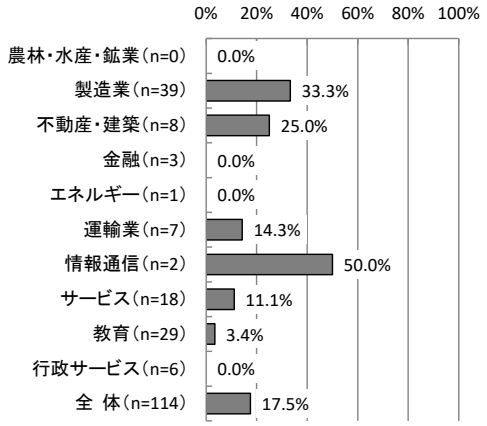
【業種別分析】業種別にみると、「電子メールの不正中継（不正送信）」については、「教育」が34.5%で高い。「ランサムウェアによる業務影響」については、「製造業」が33.3%で高くなっている。また、「ウイルス以外の情報漏えい」については、「不動産・建築」が37.5%で高くなっている。

【業種別分析】過去に受けたことのある被害状況

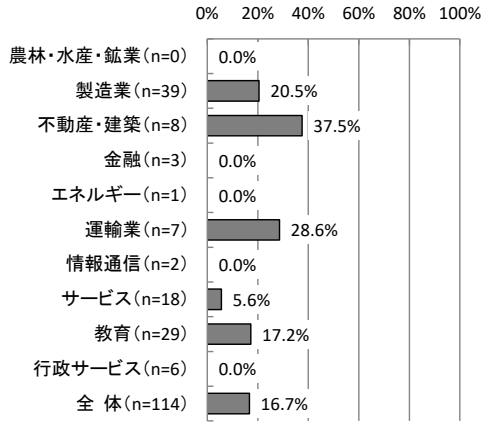
電子メールの不正中継（不正送信）



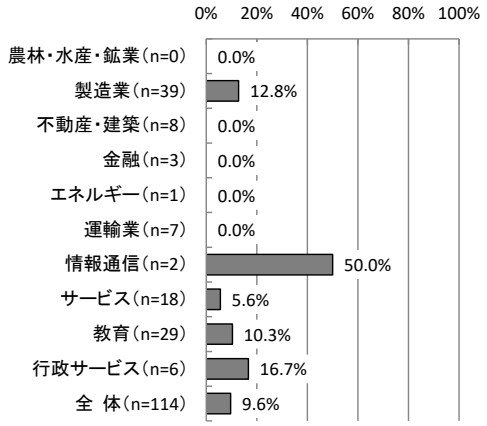
ランサムウェアによる業務影響



ウイルス以外の情報漏えい

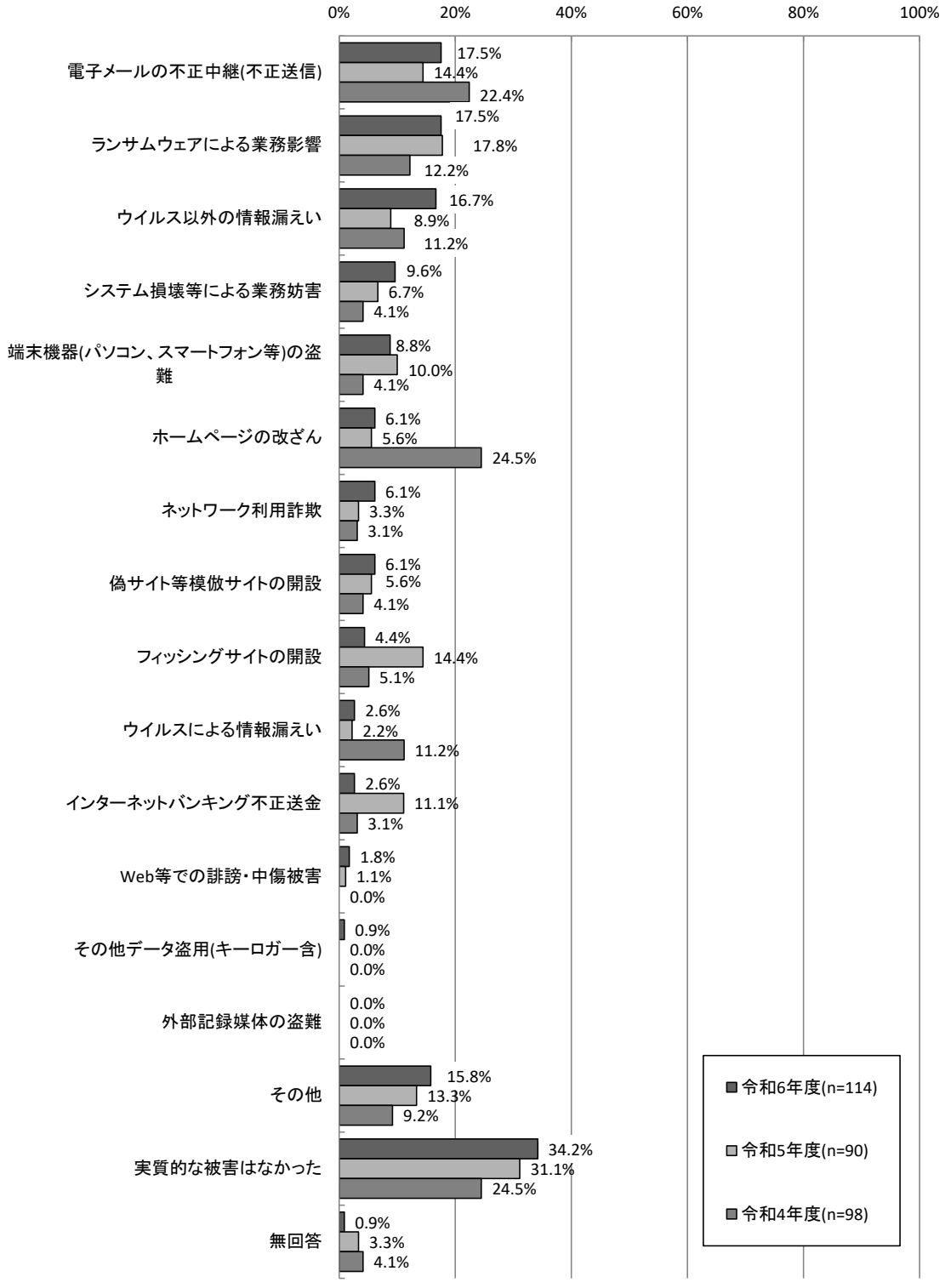


システム損壊等による業務妨害



【経年変化】昨年度と比較すると、「フィッシングサイトの開設」が10.0ポイント、「インターネットバンキング不正送金」が8.5ポイント減少している。一方、「ウイルス以外の情報漏えい」が7.8ポイントの増加となっている。

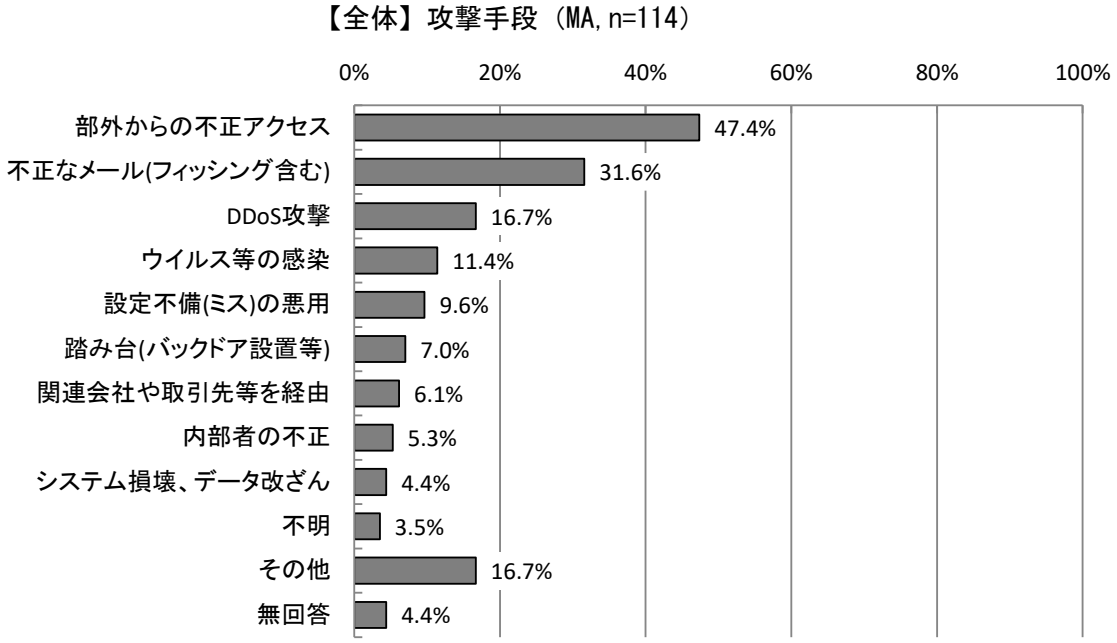
【経年変化】過去に受けたことのある被害状況



3.1.9　攻撃手段　【問8-1】

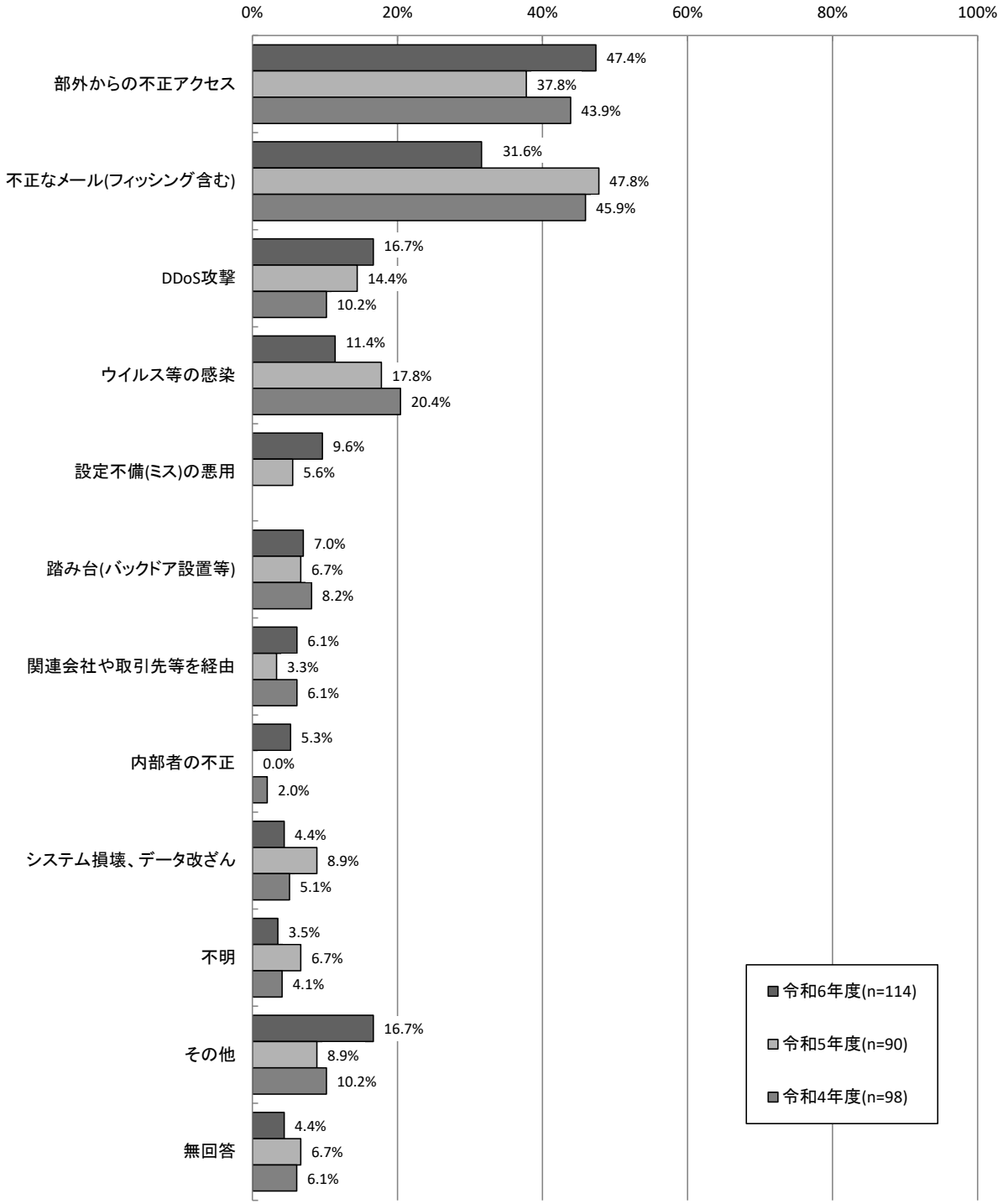
攻撃手段については、「部外からの不正アクセス」が47.4%で最も高く、次いで「不正なメール(フィッシング含む)」が31.6%となっている。

※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、「不正なメール(フィッシング含む)」が16.2ポイント、「ウイルス等の感染」が6.4ポイント減少している。一方で、「部外からの不正アクセス」が9.6ポイント増加している。

【経年変化】攻撃手段



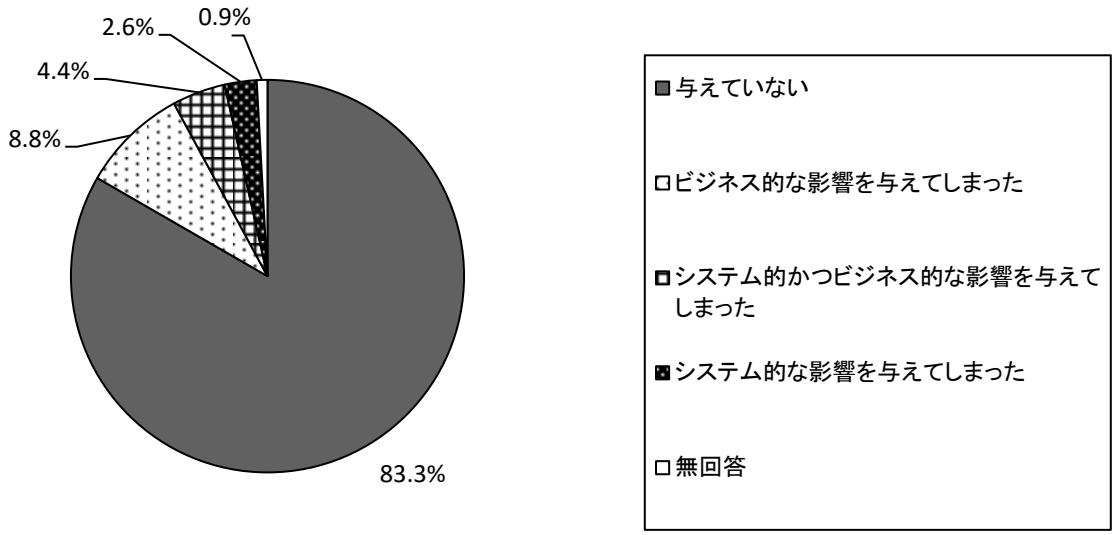
※令和５年度調査で「設定不備(ミス)の悪用」を新設

3.1.10　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8-2】

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83.3%で高くなっている。

※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=114）

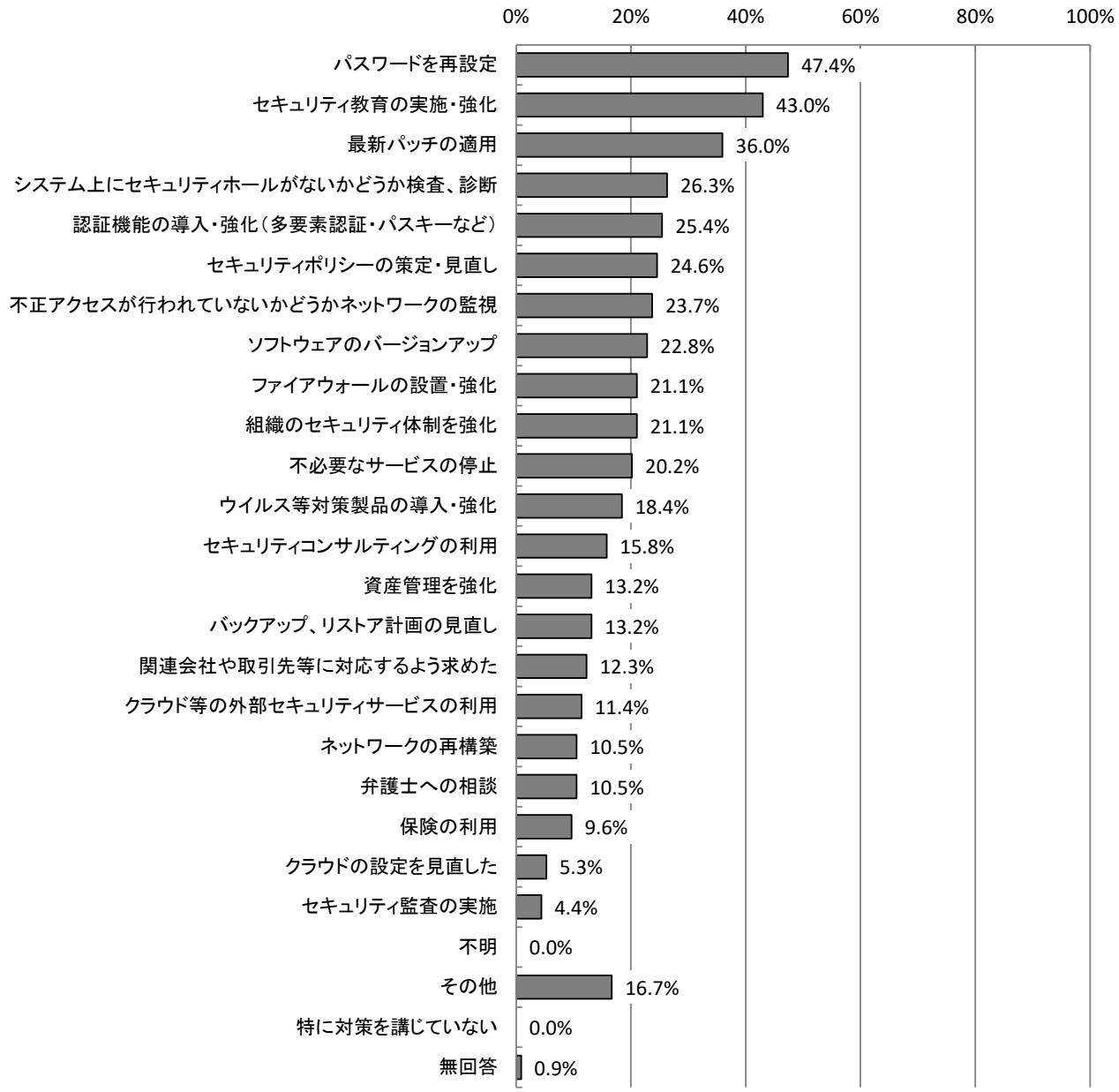


3.1.11　被害を受けたことによる対策　【問8-3】

被害を受けたことによる対策については、「パスワードを再設定」が47.4%、「セキュリティ教育の実施・強化」が43.0%、「最新パッチの適用」が36.0%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。

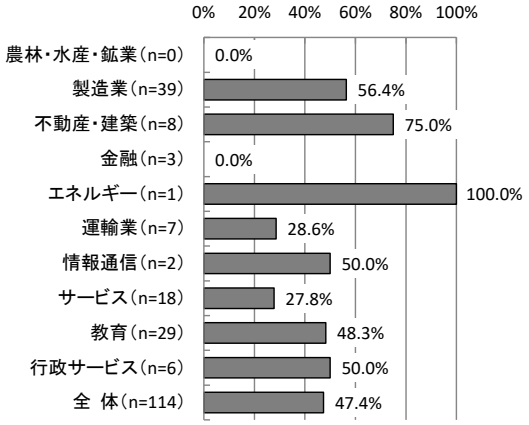
【全体】被害を受けたことによる対策（MA, n=114）



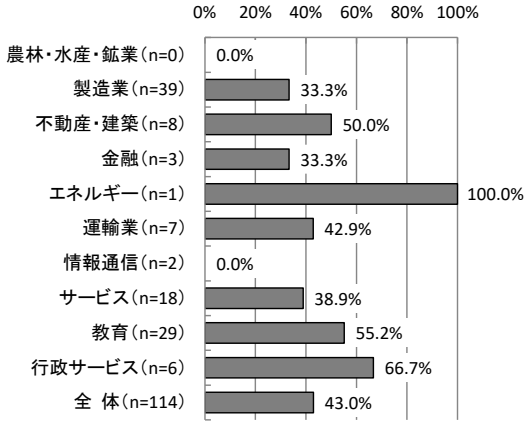
【業種別分析】業種別にみると、「パスワードを再設定」では「不動産・建築」の75.0%が高く、「セキュリティ教育の実施・強化」については、「行政サービス」の66.7%が高くなっている。

【業種別分析】被害を受けたことによる対策

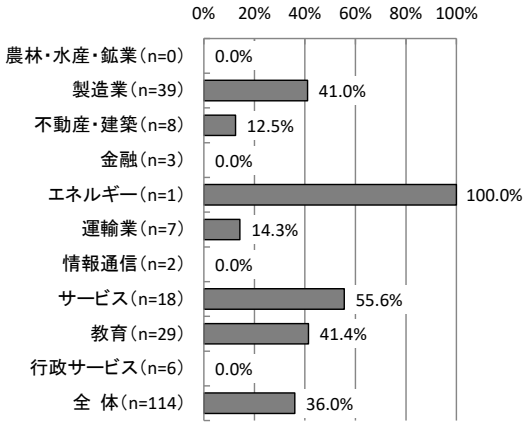
パスワードを再設定



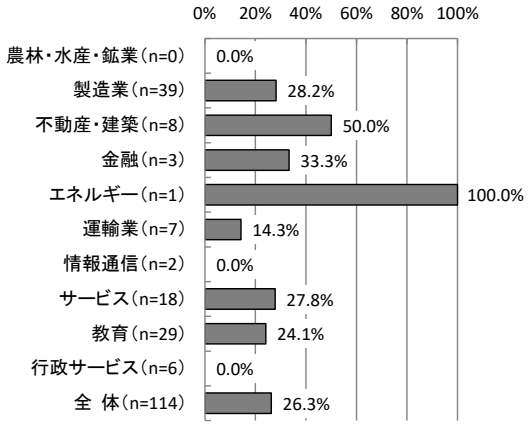
セキュリティ教育の実施・強化



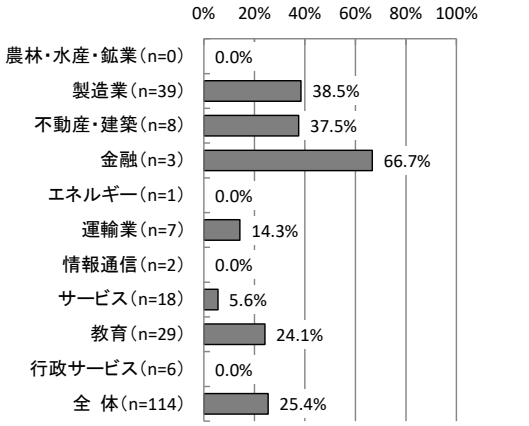
最新パッチの適用



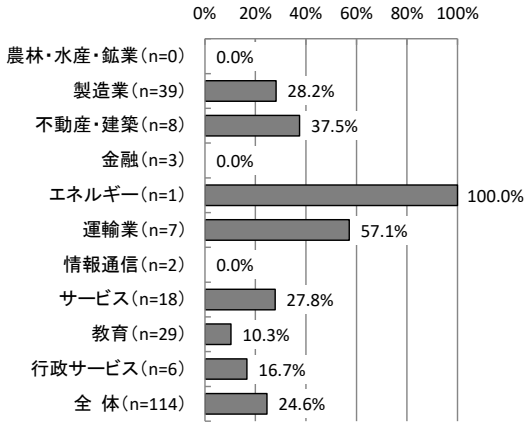
システム上にセキュリティホールがないかどうか検査、診断



認証機能の導入・強化（多要素認証、パスキーなど）



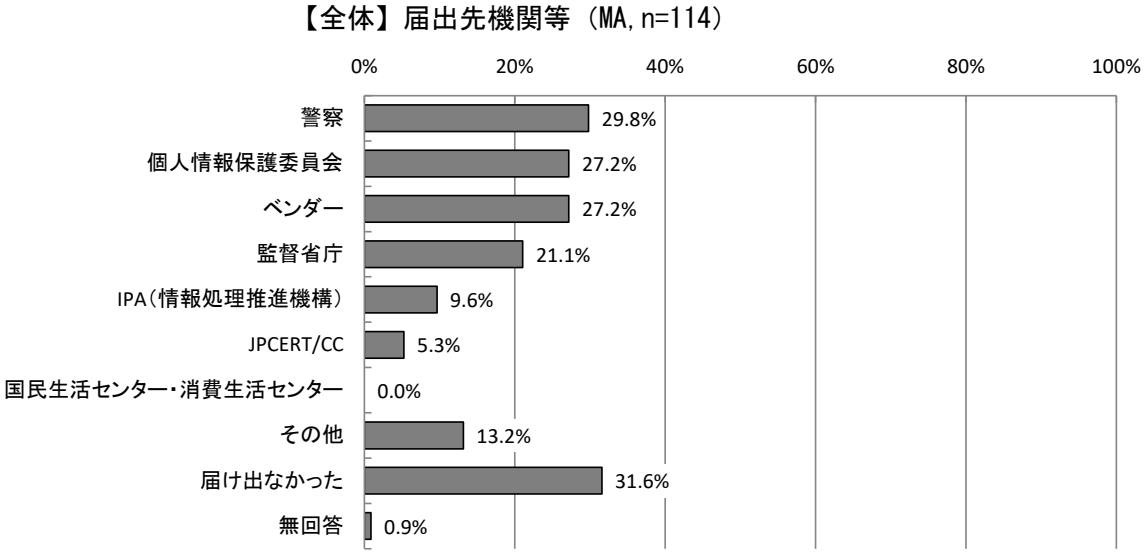
セキュリティポリシーの策定・見直し



3.1.12　届出先機関等　【問8-4】

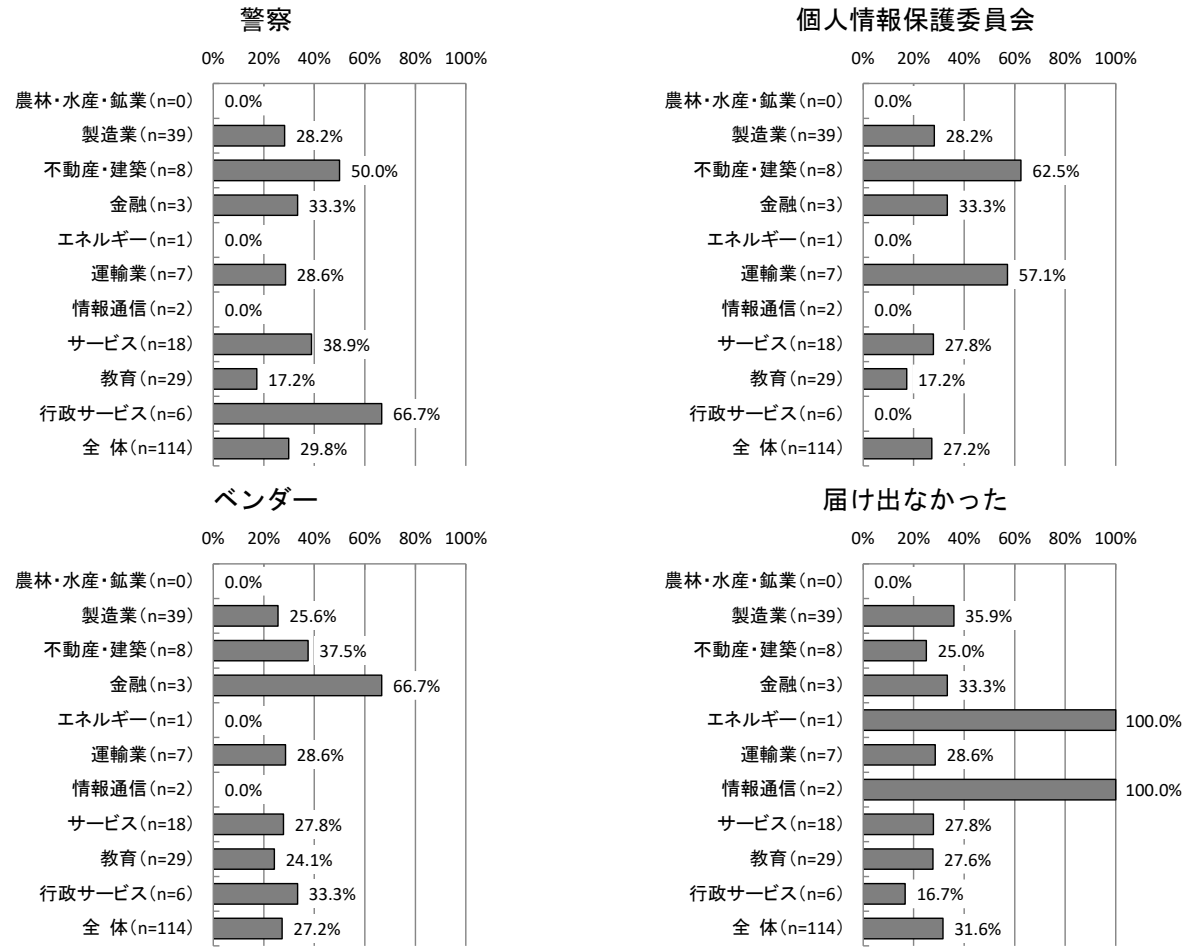
届出先機関等については、「警察」が29.8%で最も高く、次いで「個人情報保護委員会」「ベンダー」が27.2%となっている。一方、「届け出なかった」は31.6%となっている。

※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。



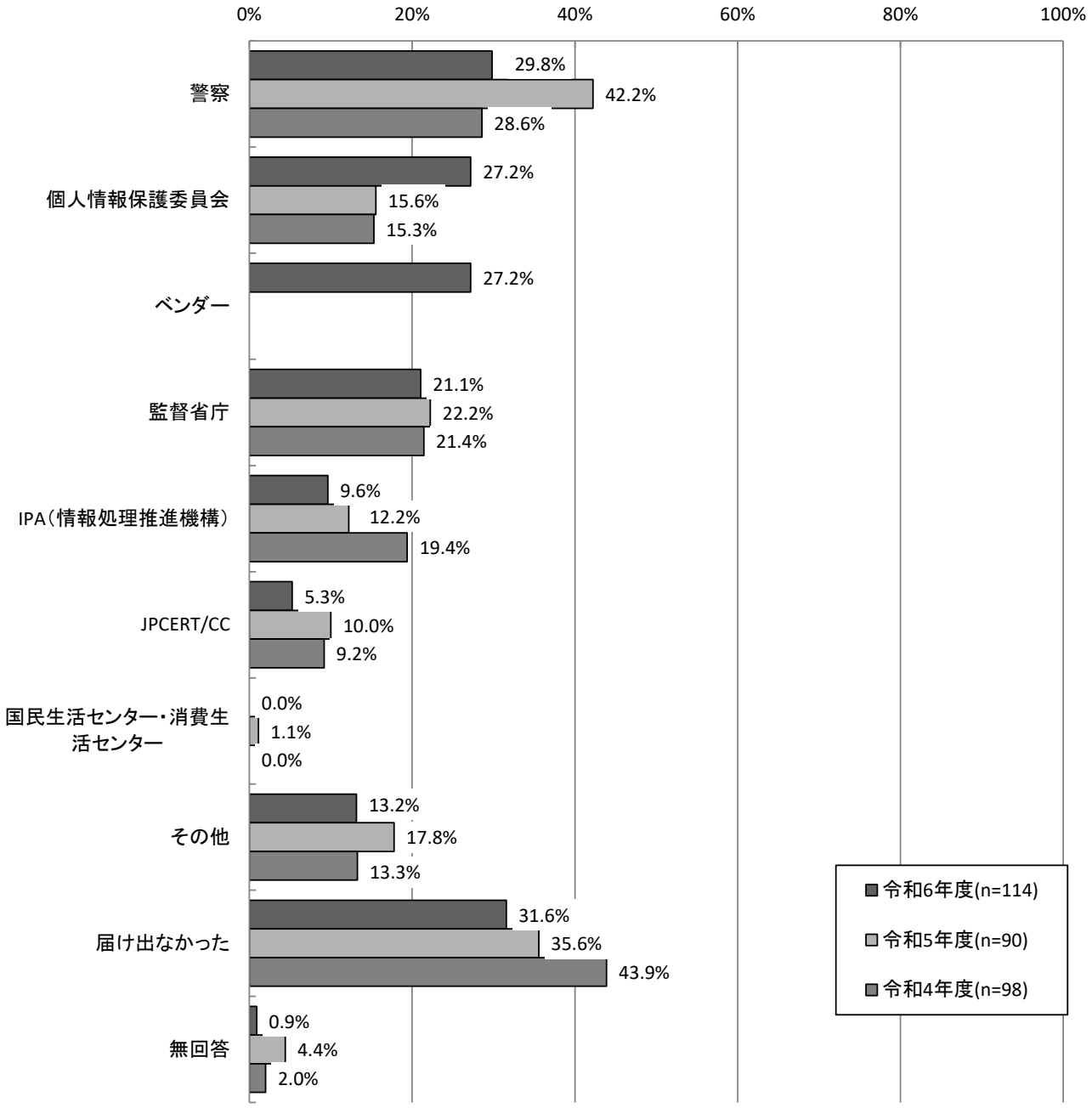
【業種別分析】業種別にみると、「警察」については「行政サービス」で66.7%と高くなっている。一方、「届け出なかった」については、「製造業」が35.9%とやや高くなっている。

【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」が12.4ポイント減少した一方で、「個人情報保護委員会」が11.6ポイント増加している。「届け出なかった」は4.0ポイント減少している。

【経年変化】届出先機関等



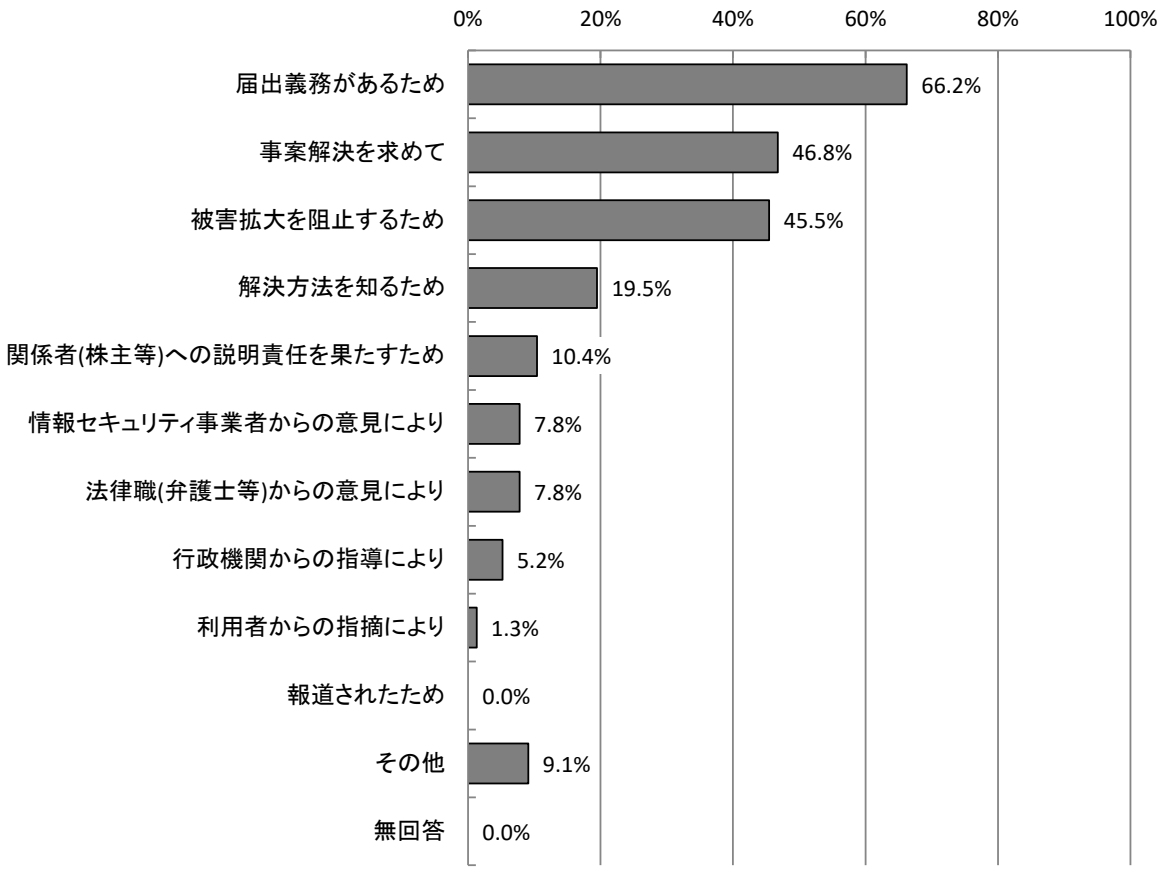
※令和６年度調査で「ベンダー」を新設

3.1.13　届出した理由　【問8-4】

届出した理由については、「届出義務があるため」が66.2%で最も多く、次いで「事案解決を求めて」が46.8%、「被害拡大を阻止するため」が45.5%となっている。

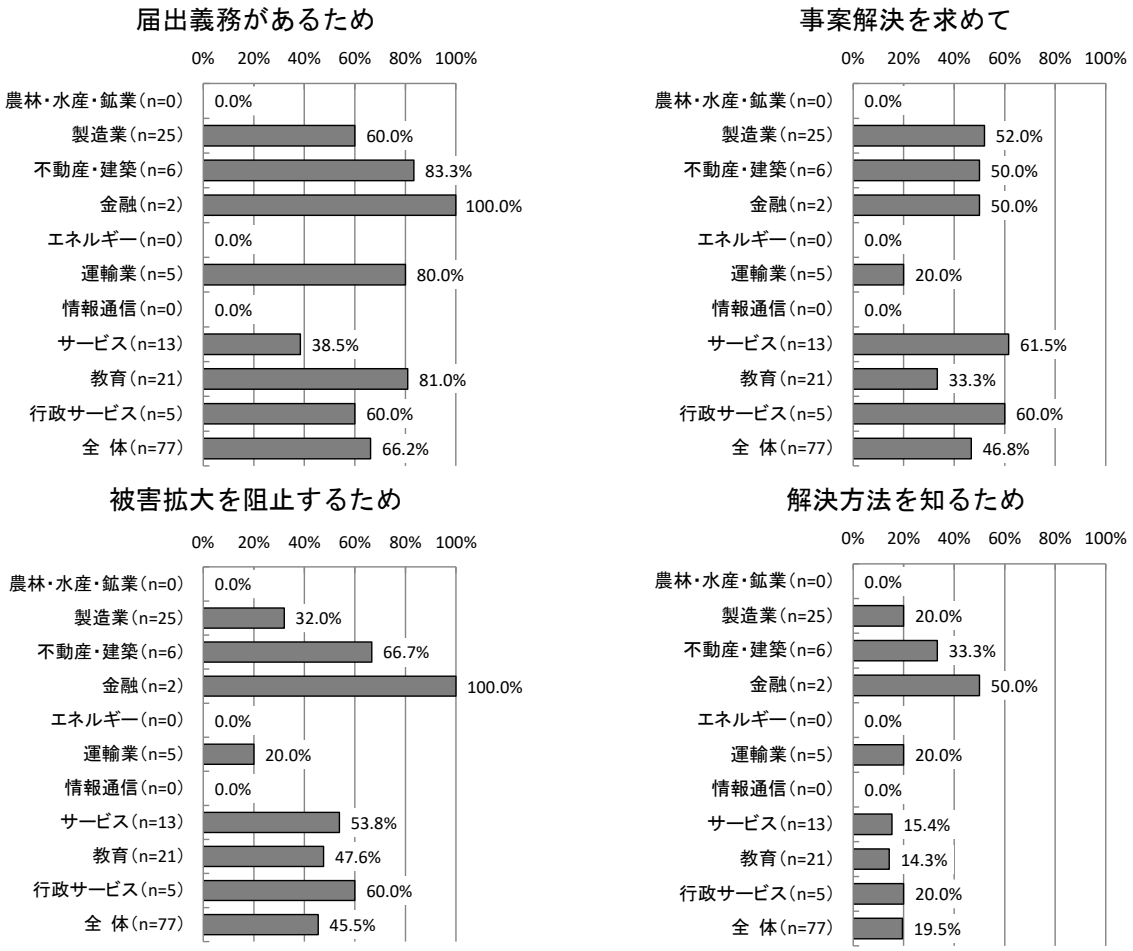
※本項目は、被害の届出を行った社・団体等を対象としている。

【全体】届出した理由（MA, n=77）

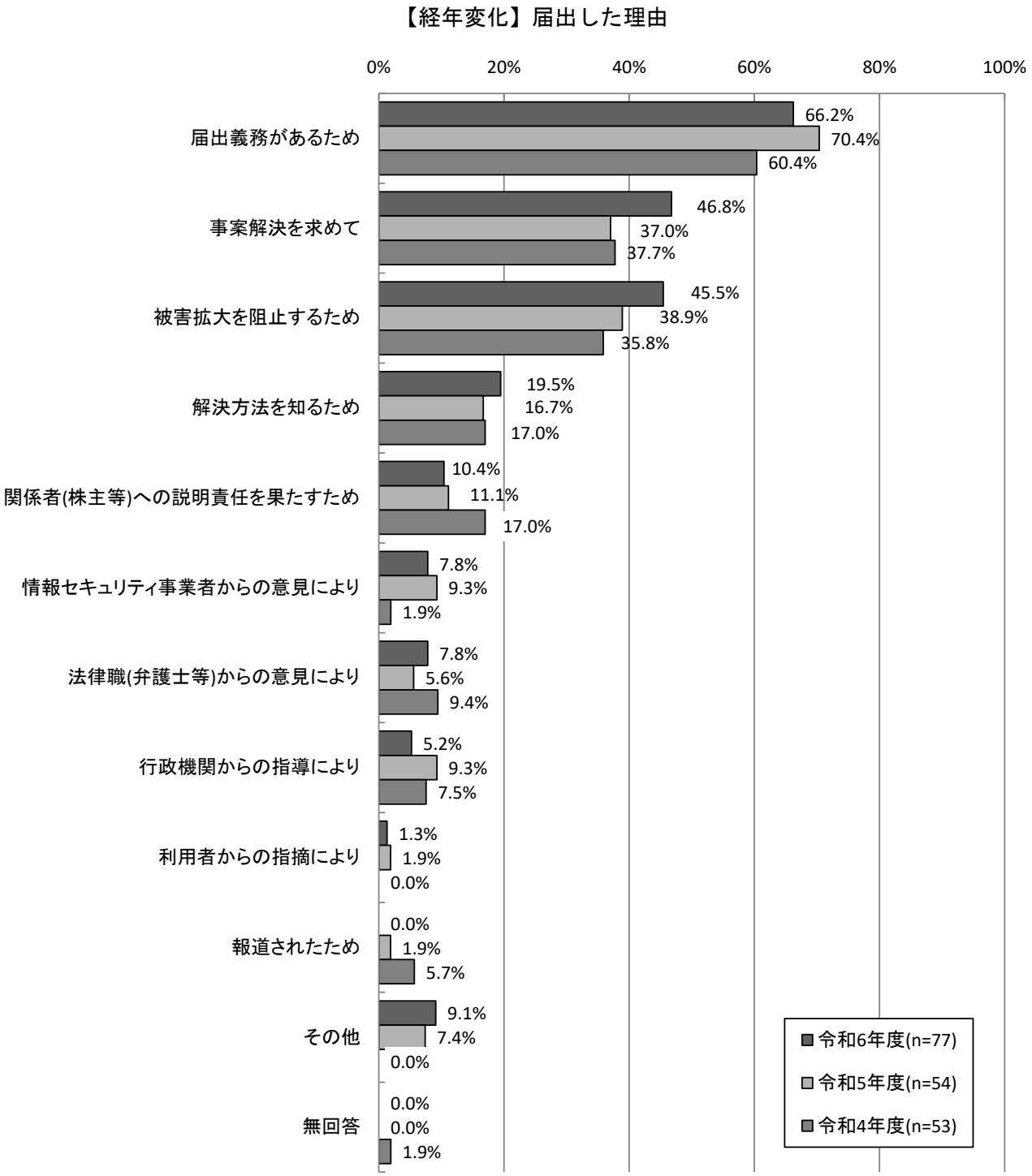


【業種別分析】業種別にみると、「届出義務があるため」は「不動産・建築」が83.3％で高く、「事案解決を求めて」では「サービス」が61.5％、「行政サービス」が60.0％で高い。「被害拡大を阻止するため」については「不動産・建築」が66.7％で高い。

【業種別分析】届出した理由



【経年変化】昨年度と比較すると、「事案解決を求めて」が9.8ポイント、「被害拡大を阻止するため」が6.6ポイント増加し、「届出義務があるため」が4.2ポイント減少している。

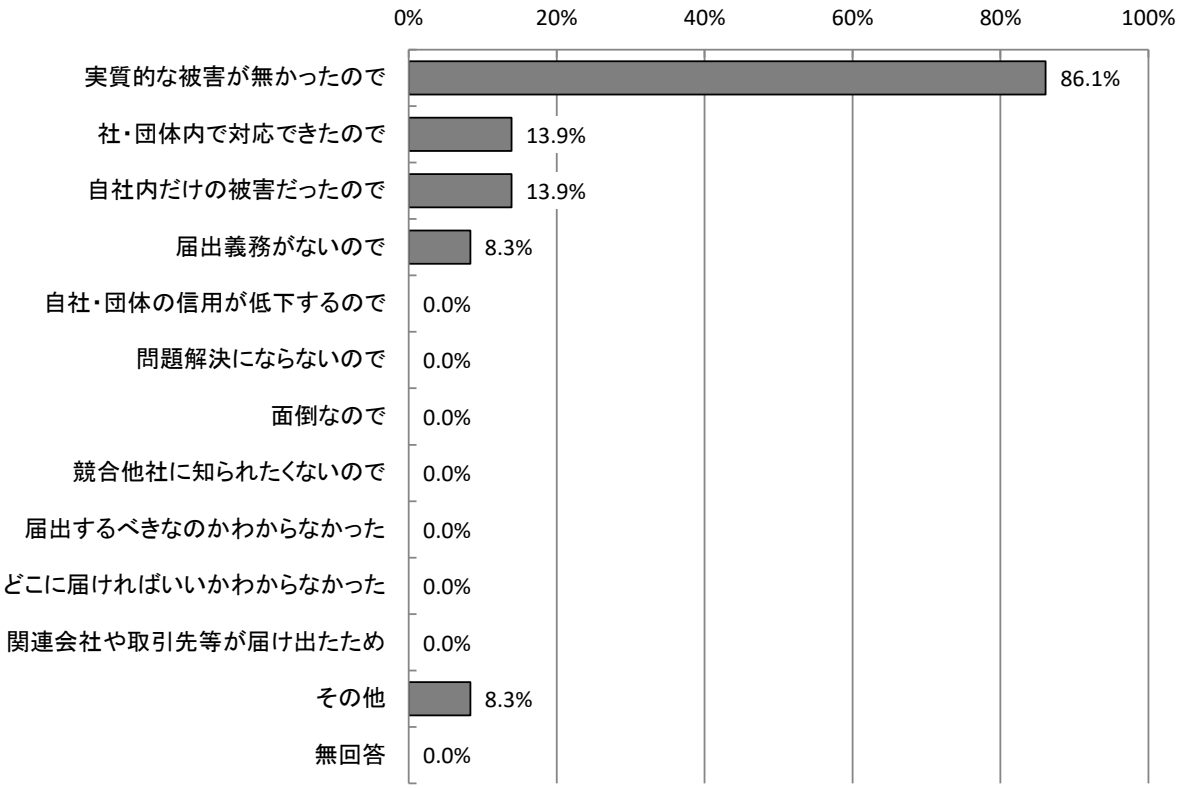


3.1.14　届出を躊躇させる要因　【問8-5】

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86.1%で最も高く、次いで「社・団体内で対応できたので」「自社内だけの被害だったので」がいずれも13.9%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。

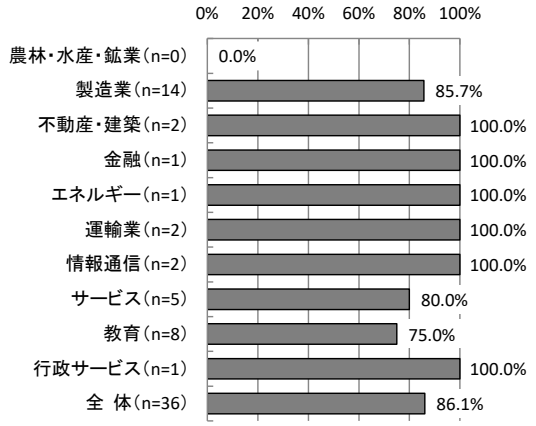
【全体】届出を躊躇させる要因（MA, n=36）



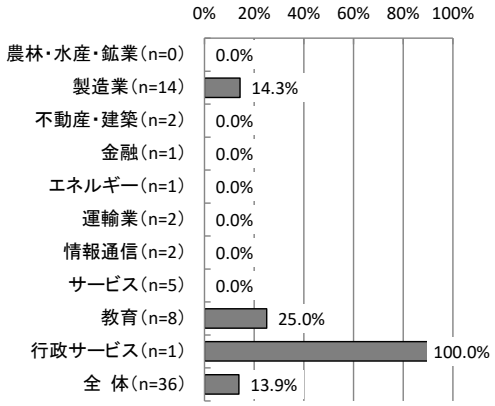
【業種別分析】業種別にみると、「実質的な被害が無かったので」については、「製造業」が85.7%となっている。「社・団体内で対応できたので」については、「教育」が25.0%、「製造業」が14.3%となっている。

【業種別分析】届出を躊躇させる要因

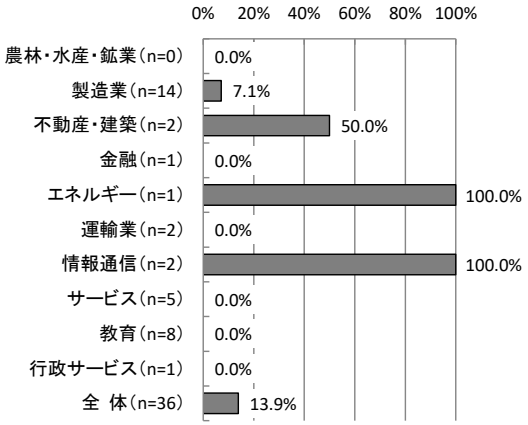
実質的な被害が無かったので



社・団体内で対応できたので

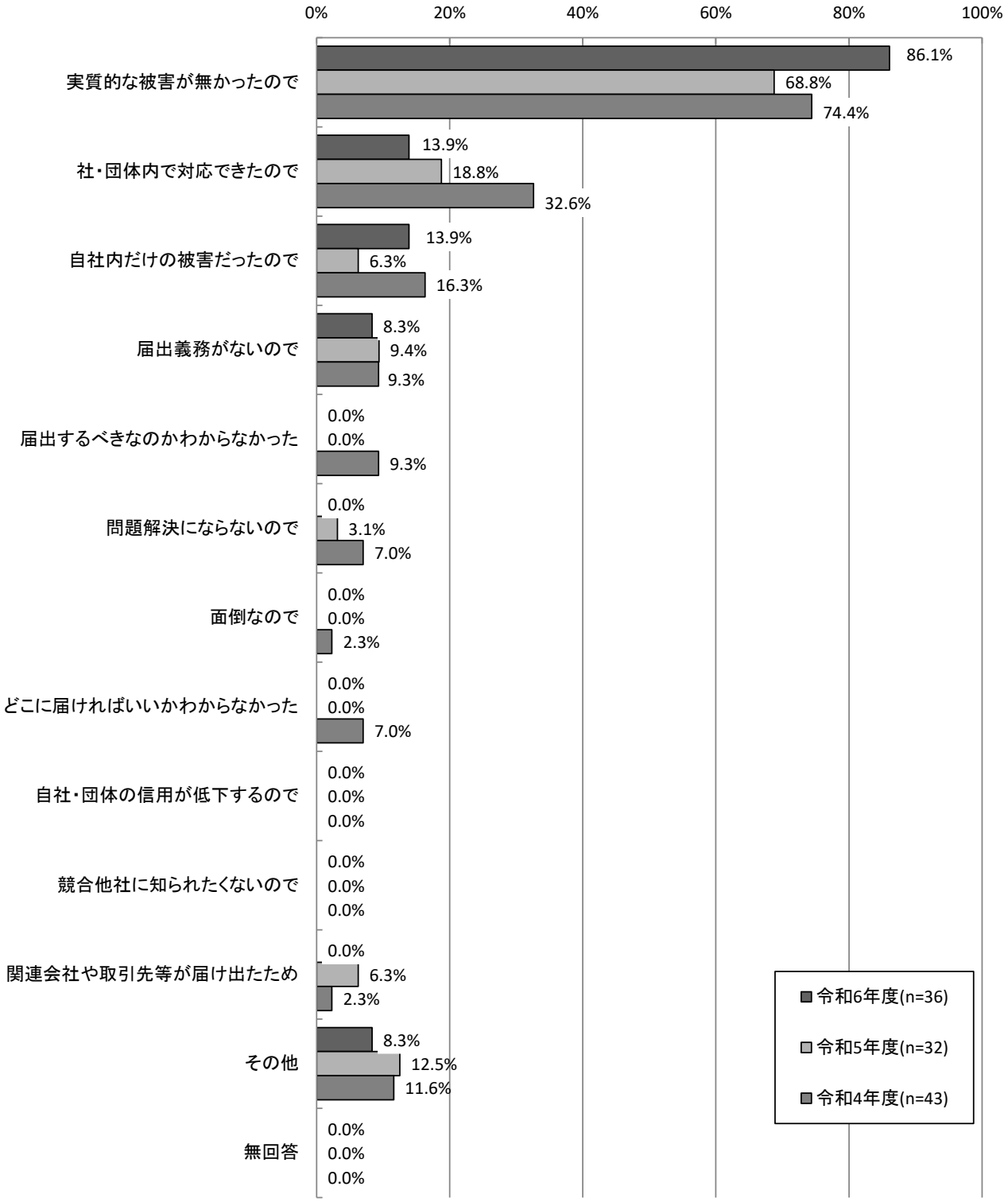


自社内だけの被害だったので



【経年変化】昨年度と比較すると、「実質的な被害が無かったので」が17.3ポイント、「自社内だけの被害だったので」が7.6ポイント増加している。

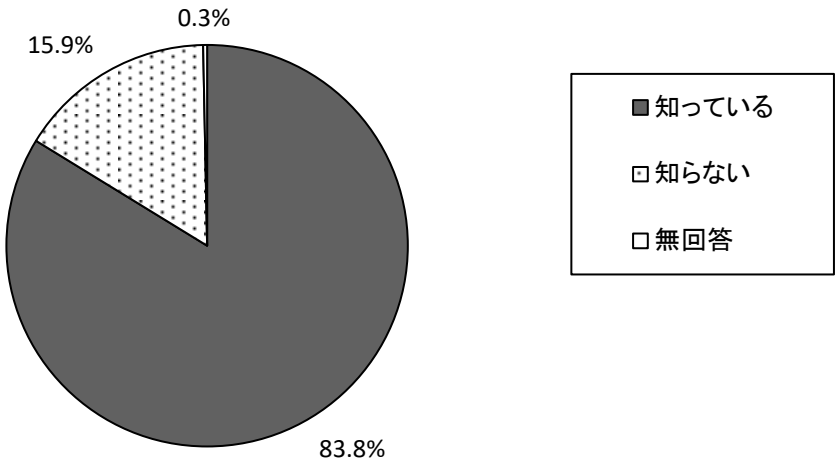
【経年変化】届出を躊躇させる要因



3.1.15　届出先機関を知っているか　【問9】

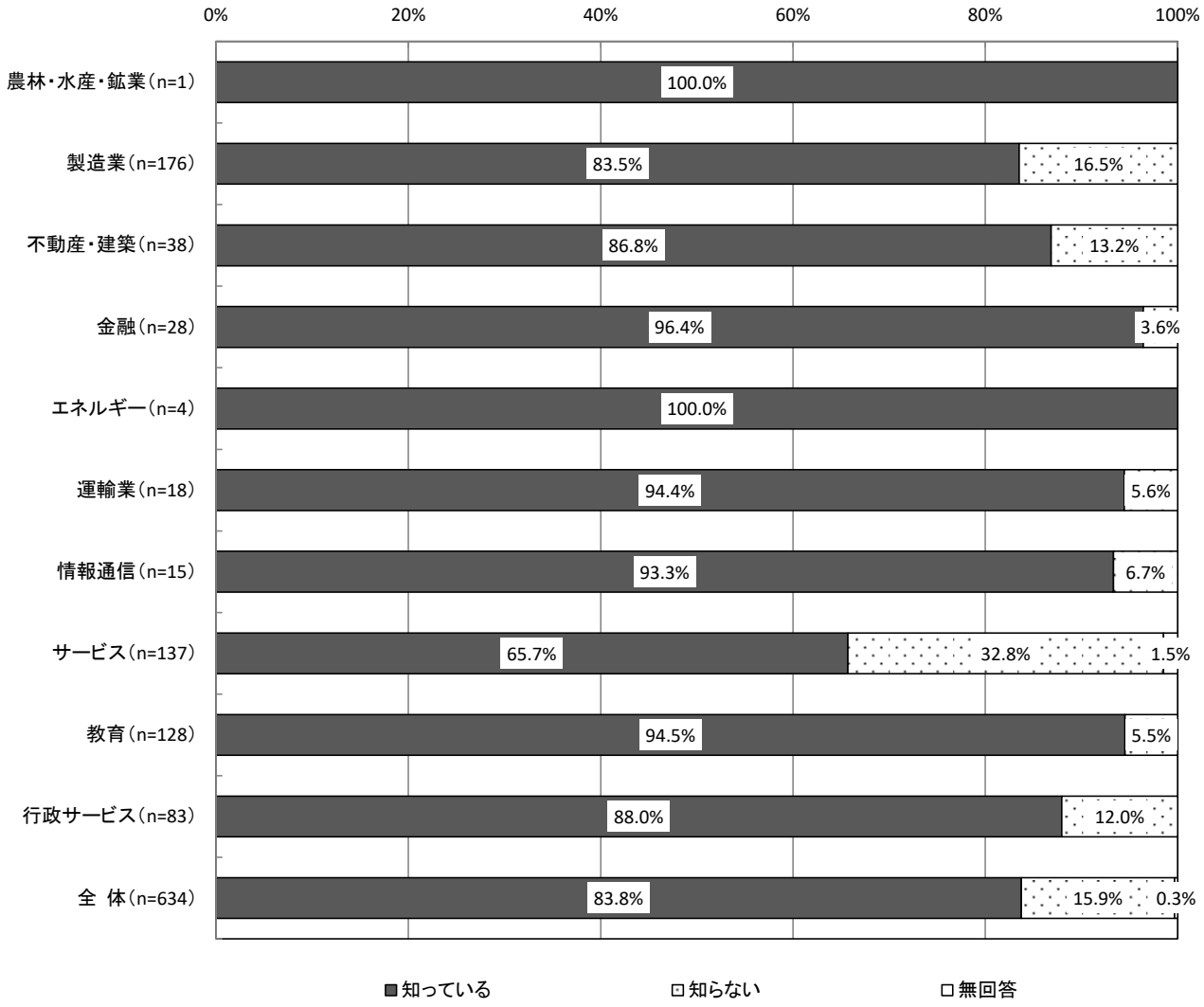
届出先機関を知っているかについては、「知っている」が83.8%と高く、「知らない」は15.9%となっている。

【全体】届出先機関を知っているか（SA,n=634）



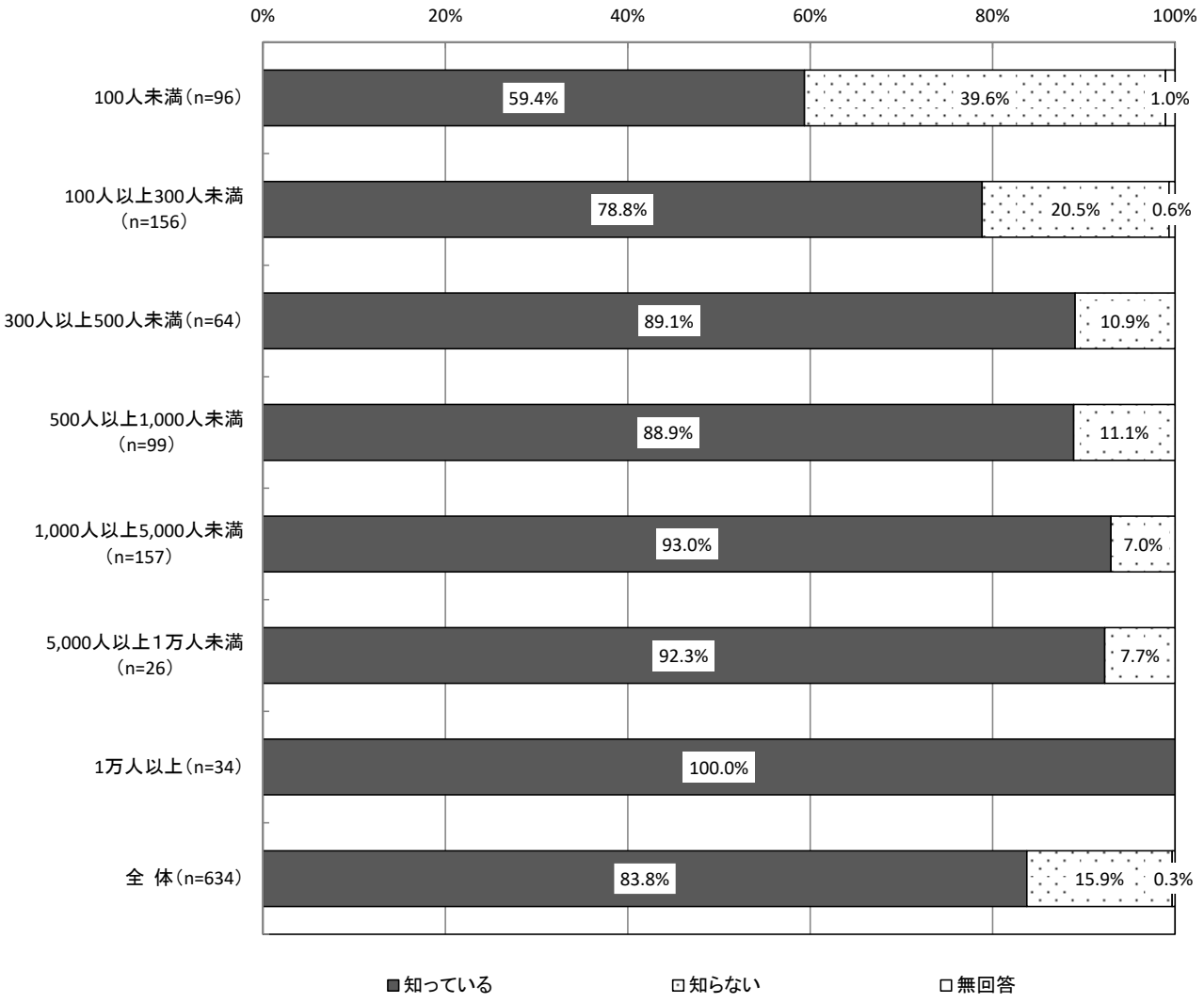
【業種別分析】業種別にみると、届出先機関を「知っている」については、「金融」が 96.4%、「教育」が 94.5%、「運輸業」が 94.4%で高い。一方、「知らない」については、「サービス」が 32.8%となっている。

【業種別分析】届出先機関を知っているか



【従業員規模別分析】従業員規模別にみると、いずれも「知っている」が「知らない」より高くなっている。「100人未満」では39.6%が「知らない」と回答している。

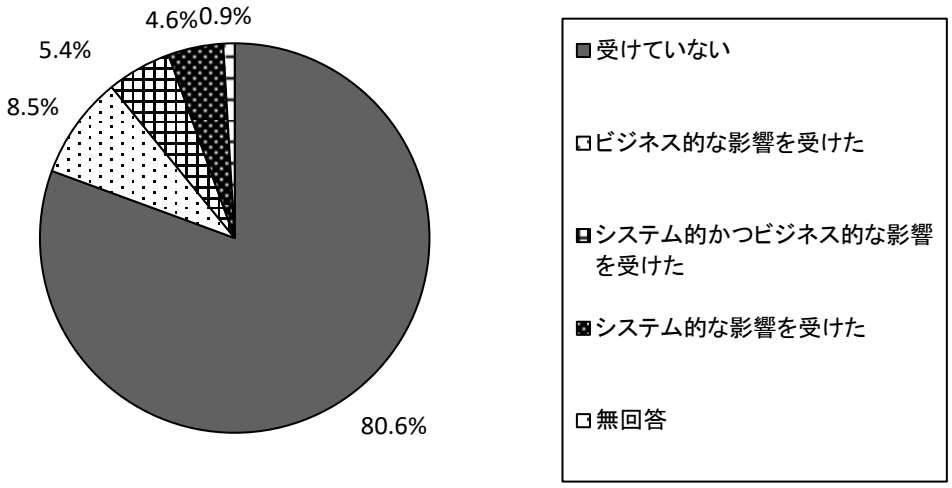
【従業員規模別分析】届出先機関を知っているか



3.1.16　過去に不正アクセス等の攻撃・被害をサプライチェーンが受けたことによる影響【問10】

過去に不正アクセス等の攻撃・被害をサプライチェーンが受けたことによる影響については、「受けていない」が80.6%と高い。「ビジネス的な影響を受けた」「システム的かつビジネス的な影響を受けた」「システム的な影響を受けた」をあわせると18.5%となっている。

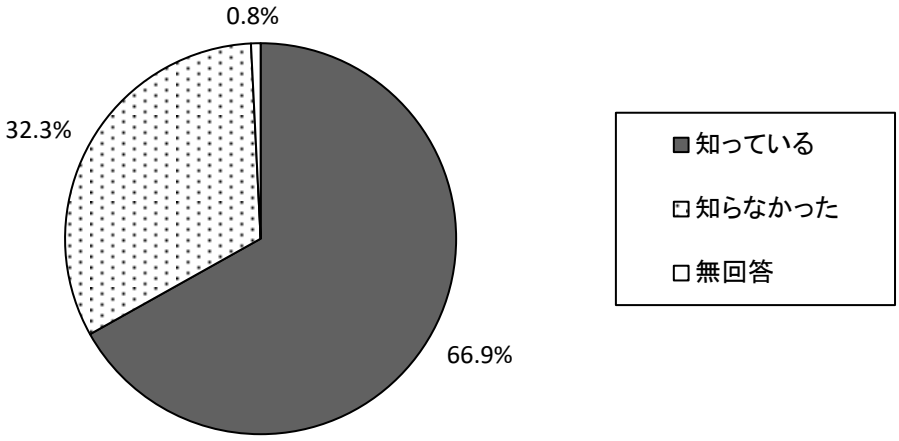
【全体】過去に不正アクセス等の攻撃・被害をサプライチェーンが受けたことによる影響（SA,n=634）



3.1.17　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11】

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66.9%、「知らなかった」は32.3%となっている。

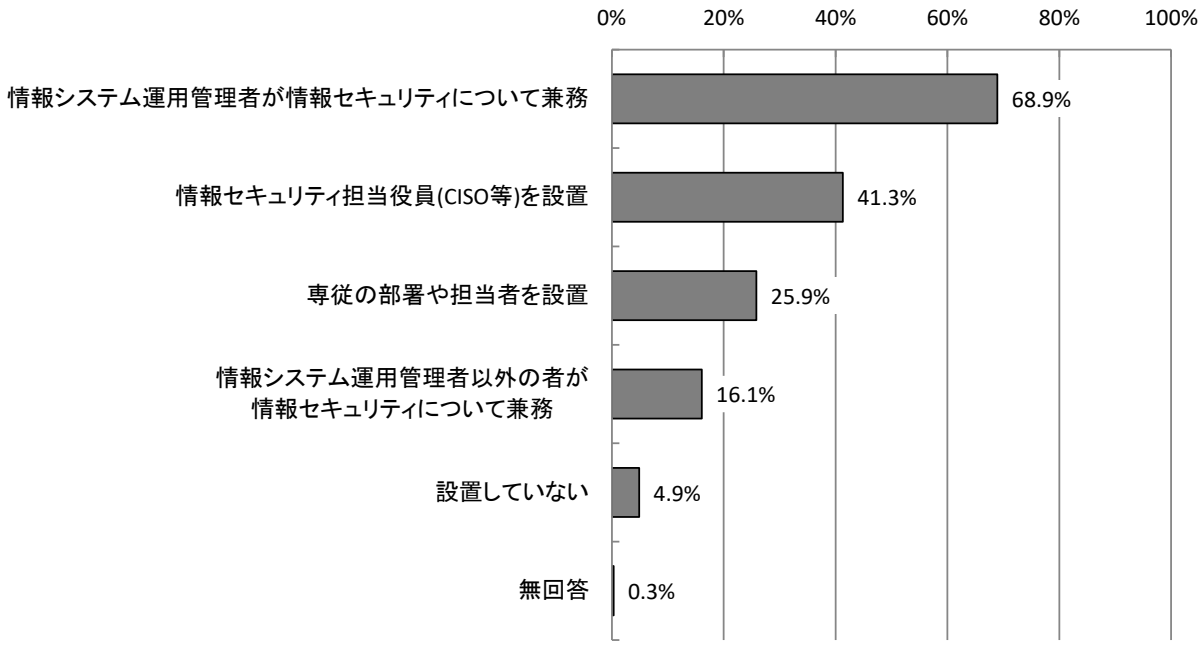
【全体】不正アクセス禁止法でアクセス管理者による防御措置についての努力義務（SA,n=634）



3.1.18　情報セキュリティ管理体制　【問12】

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68.9%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41.3%、「専従の部署や担当者を設置」が25.9%となっている。

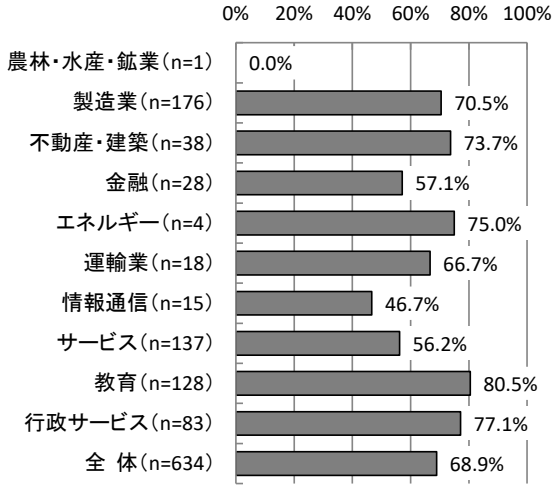
【全体】情報セキュリティ管理体制（MA, n=634）



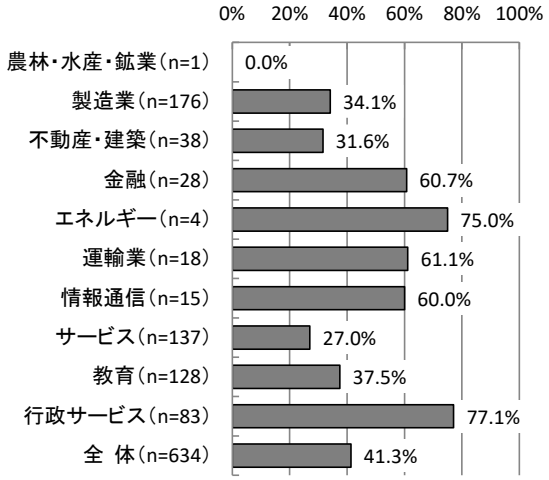
【業種別分析】業種別にみると、「情報システム運用管理者が情報セキュリティについて兼務」については、「教育」が80.5%、「行政サービス」が77.1%、「不動産・建築」で73.7%、「製造業」で70.5%と高くなっている。「情報セキュリティ担当役員(CISO等)を設置」については、「行政サービス」が77.1%で最も高い。「専従の部署や担当者を設置」では、「情報通信」が53.3%で最も高い。

【業種別分析】情報セキュリティ管理体制

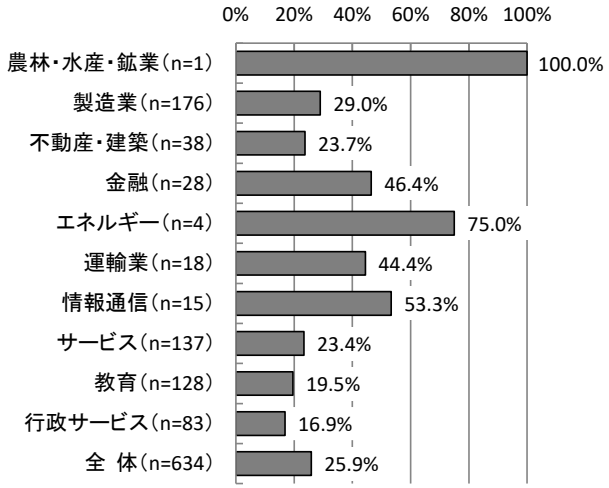
情報システム運用管理者が情報セキュリティについて兼務



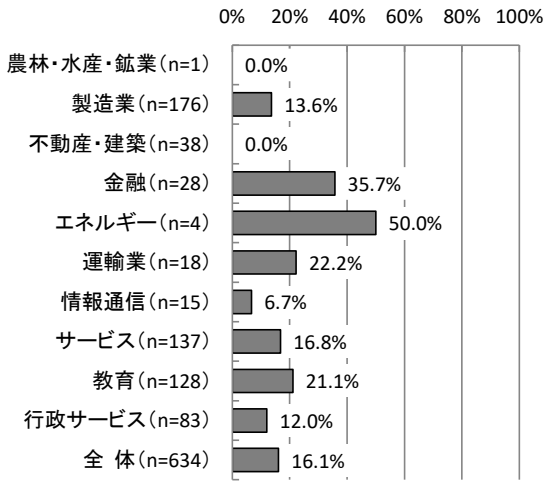
情報セキュリティ担当役員(CISO等)を設置



専従の部署や担当者を設置

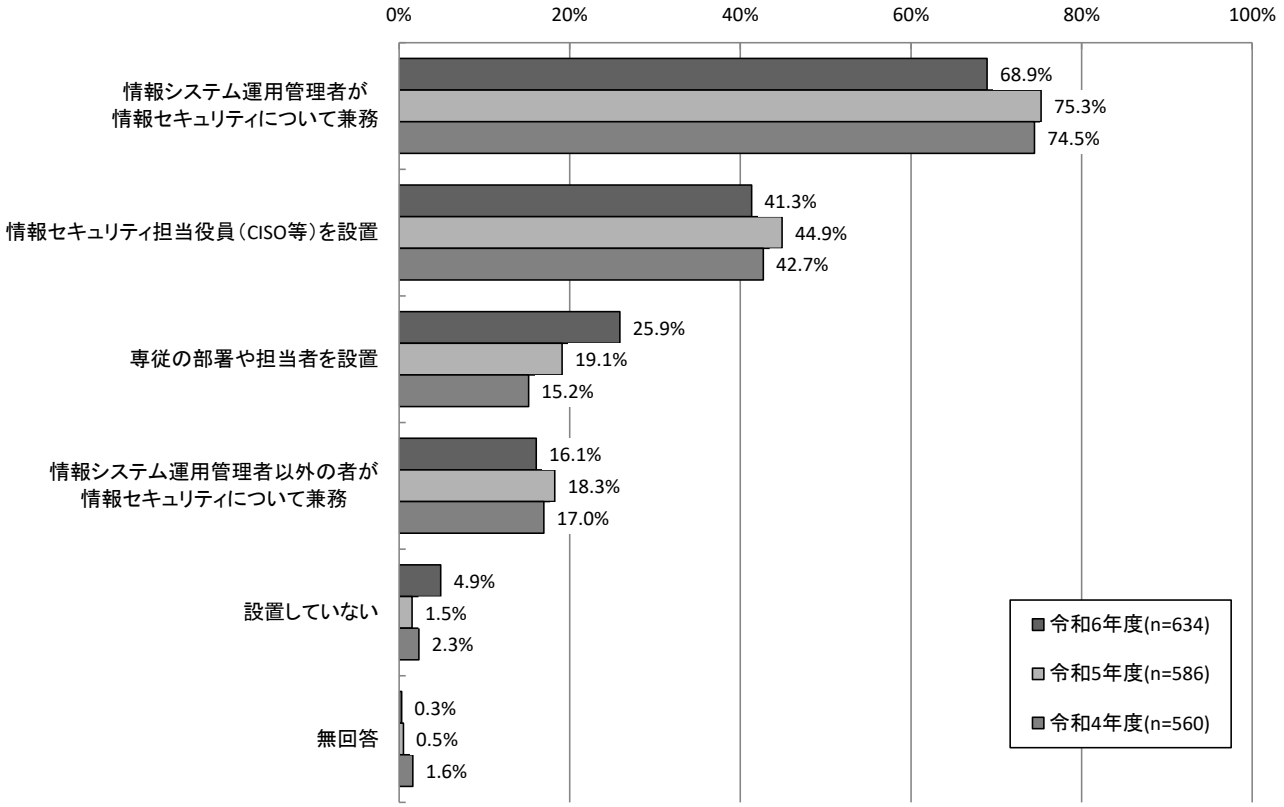


情報システム運用管理者以外の者が情報セキュリティについて兼務



【経年変化】昨年度と比較すると、「専従の部署や担当者を設置」が6.8ポイント増加している。一方、「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6.4ポイント減少している。「設置していない」は3.4ポイント増加している。

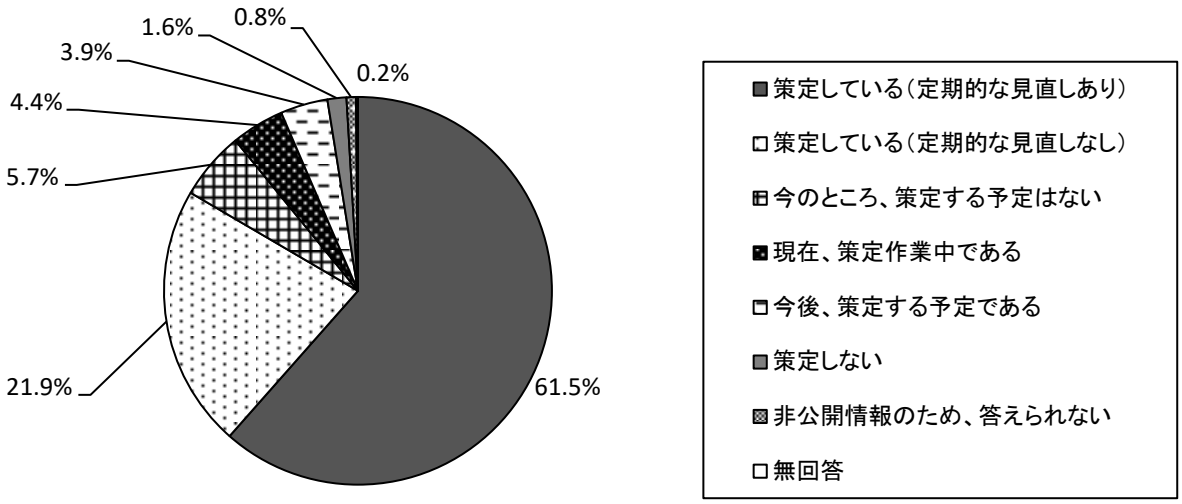
【経年変化】情報セキュリティ管理体制



3.1.19　セキュリティポリシーの策定状況　【問13】

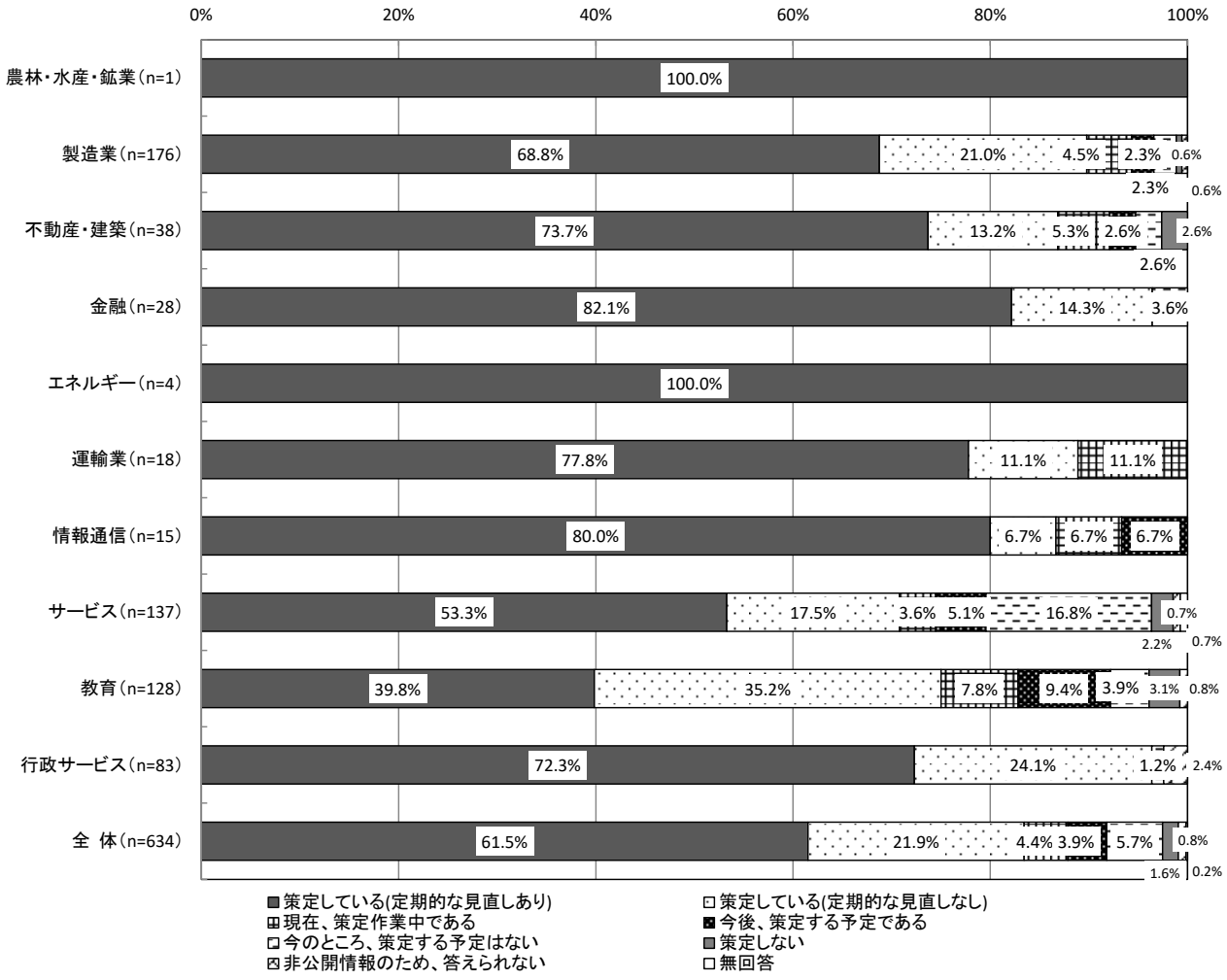
セキュリティポリシーの策定状況については、「策定している（定期的な見直しあり）」が61.5%で最も高く、次いで「策定している（定期的な見直しなし）」が21.9%となっている。「策定している（定期的な見直しあり）」「策定している（定期的な見直しなし）」「現在、策定作業中である」に「今後、策定する予定である」を加えた「策定（予定）」は、全体の91.7%となっている。

【全体】セキュリティポリシーの策定状況（SA,n=634）



【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（定期的な見直しあり）」については「金融」が82.1%、「情報通信」が80.0%と8割を超えている。一方「策定している（定期的な見直しあり）」が低いのは、「教育」の39.8%となっている。

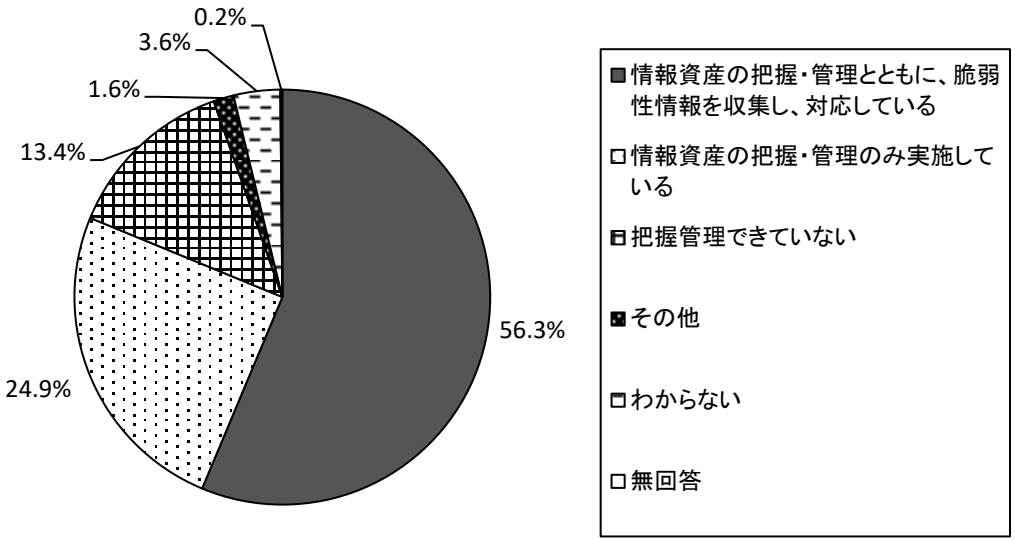
【業種別分析】セキュリティポリシーの策定状況



3.1.20　情報資産の把握・監理と脆弱性情報の定期的な収集を行っているか【問14】

情報資産の把握・監理と脆弱性情報の定期的な収集状況については、「情報資産の把握・管理とともに、脆弱性情報を収集し、対応している」が56.3%で最も高く、次いで「情報資産の把握・管理のみ実施している」が24.9%、「把握管理できていない」が13.4%となっている。

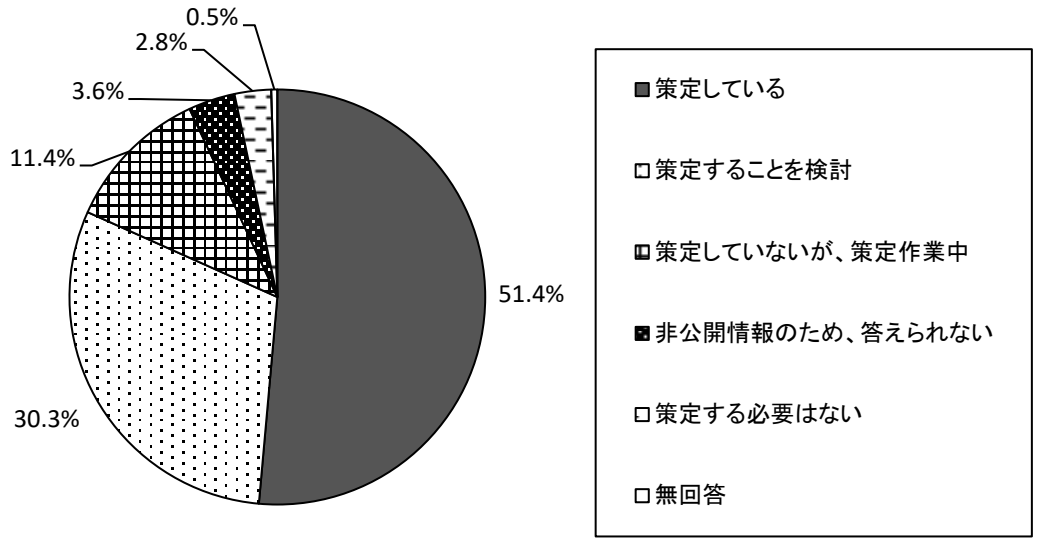
【全体】情報資産の把握・監理と脆弱性情報の定期的な収集状況（SA,n=634）



3.1.21　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15】

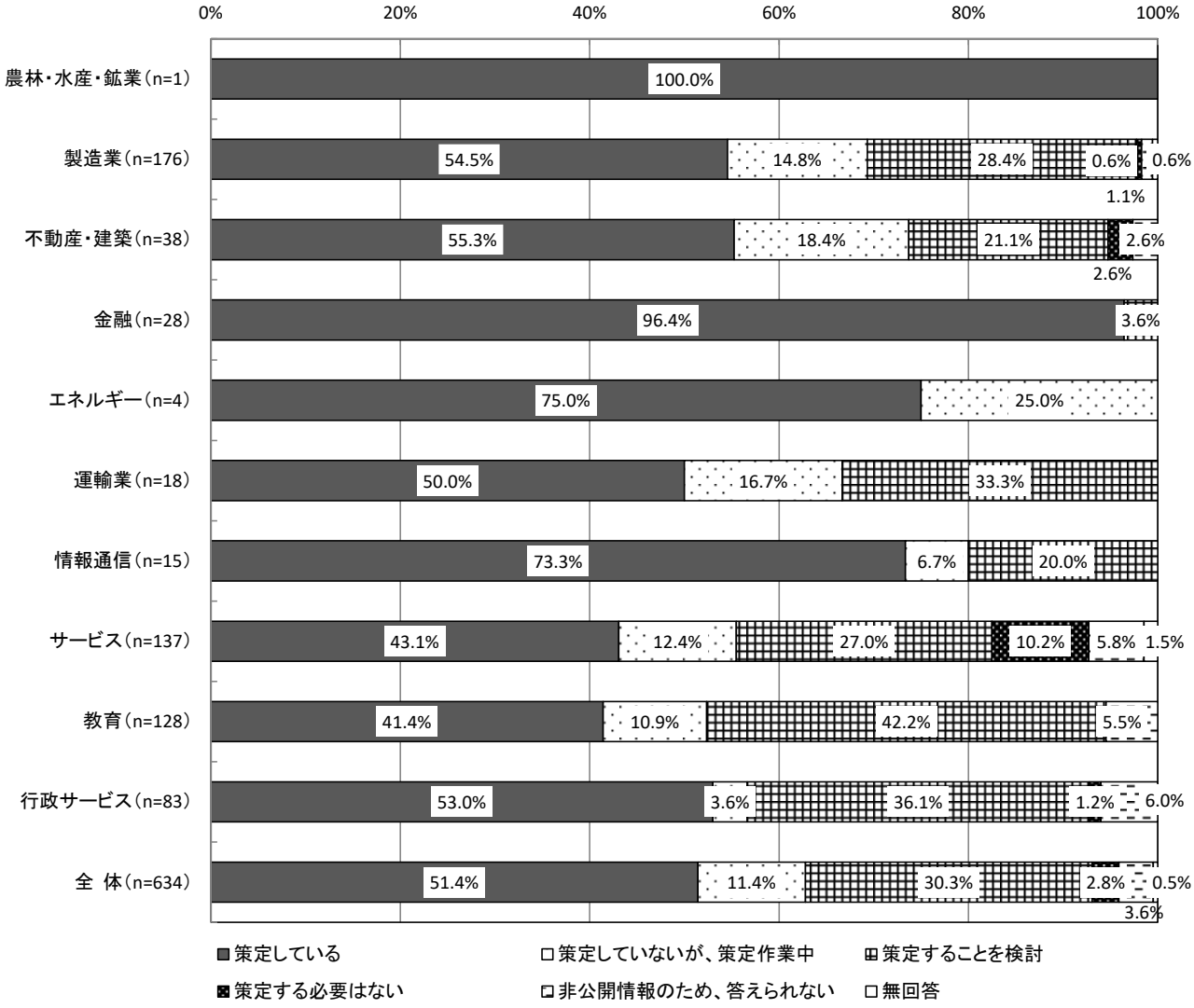
情報セキュリティ侵害事案発生時の対応マニュアル等の策定状況については、「策定している」が51.4%で過半数となっている。次いで「策定することを検討」が30.3%、「策定していないが、策定作業中」が11.4%となっている。

【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=634）



【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73.3%が高い。これに対して「教育」が41.4%、「サービス」が43.1%と低くなっている。

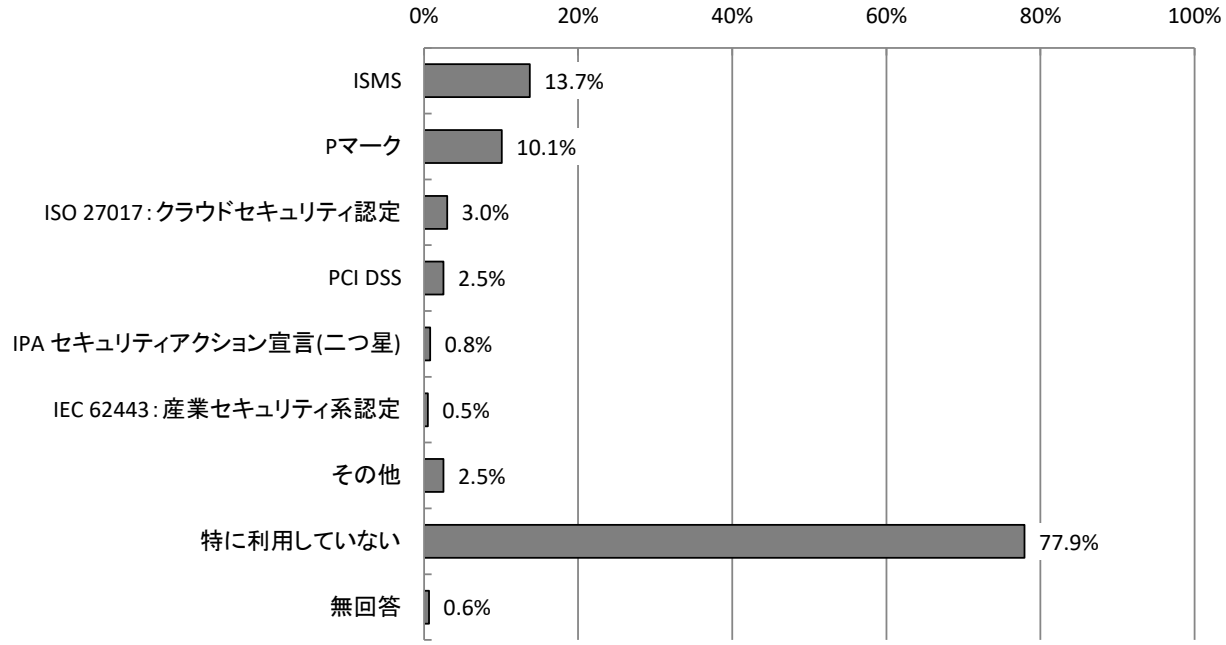
【業種別分析】情報セキュリティ侵害事案発生時の対応マニュアル等の策定状況



3.1.22　第三者機関の認証制度等の利用状況　【問16】

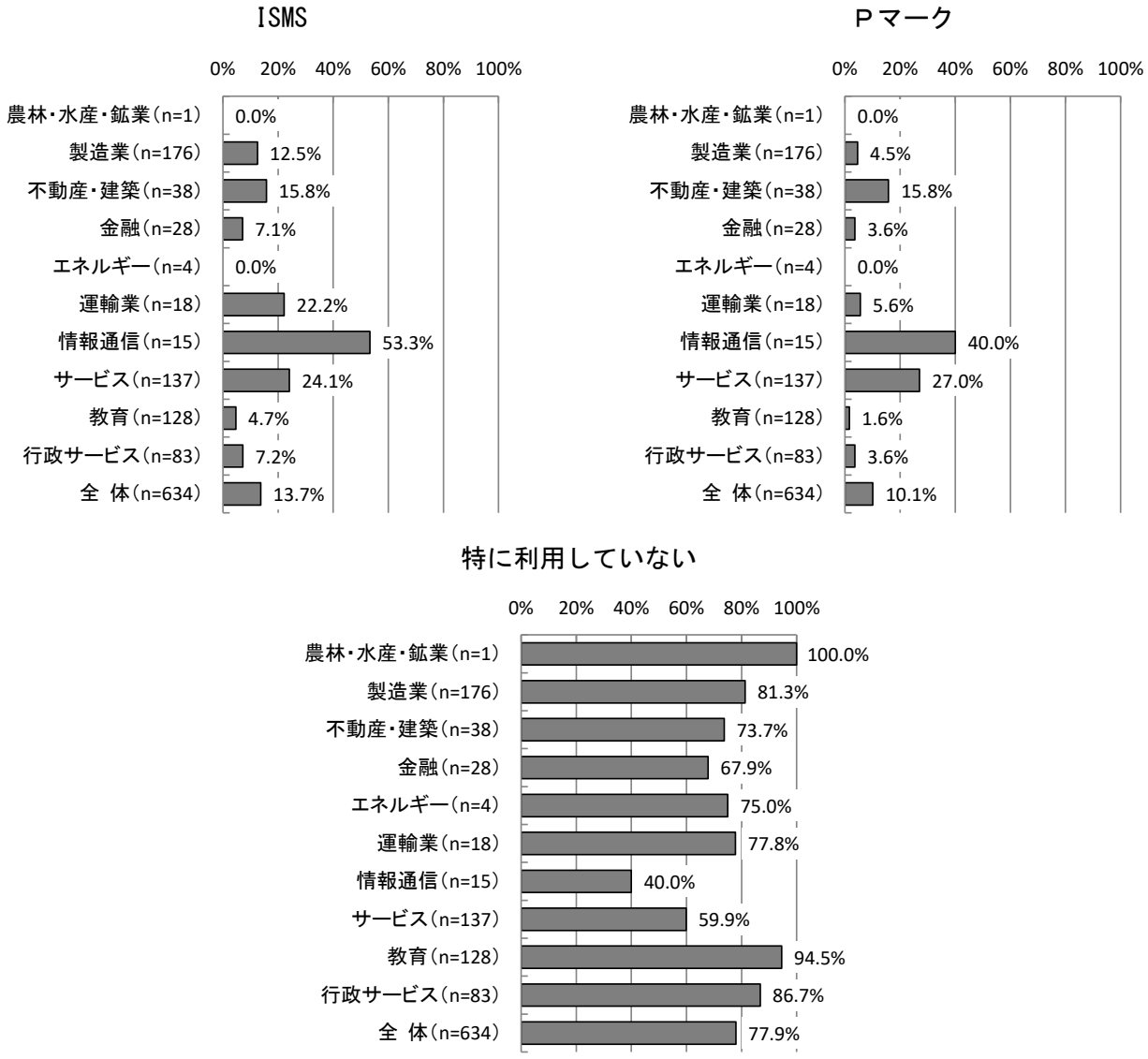
第三者機関の認証制度等の利用状況については、「特に利用していない」が77.9%で最も高い。次いで「ISMS」が13.7%、「Ｐマーク」が10.1%となっている。

【全体】第三者機関の認証制度等の利用状況（MA,n=634）



【業種別分析】業種別にみると、「ISMS」については、「情報通信」が53.3%で高くなっている。「特に利用していない」については、「教育」で94.5%と高くなっている。

【業種別分析】第三者機関の認証制度等の利用状況

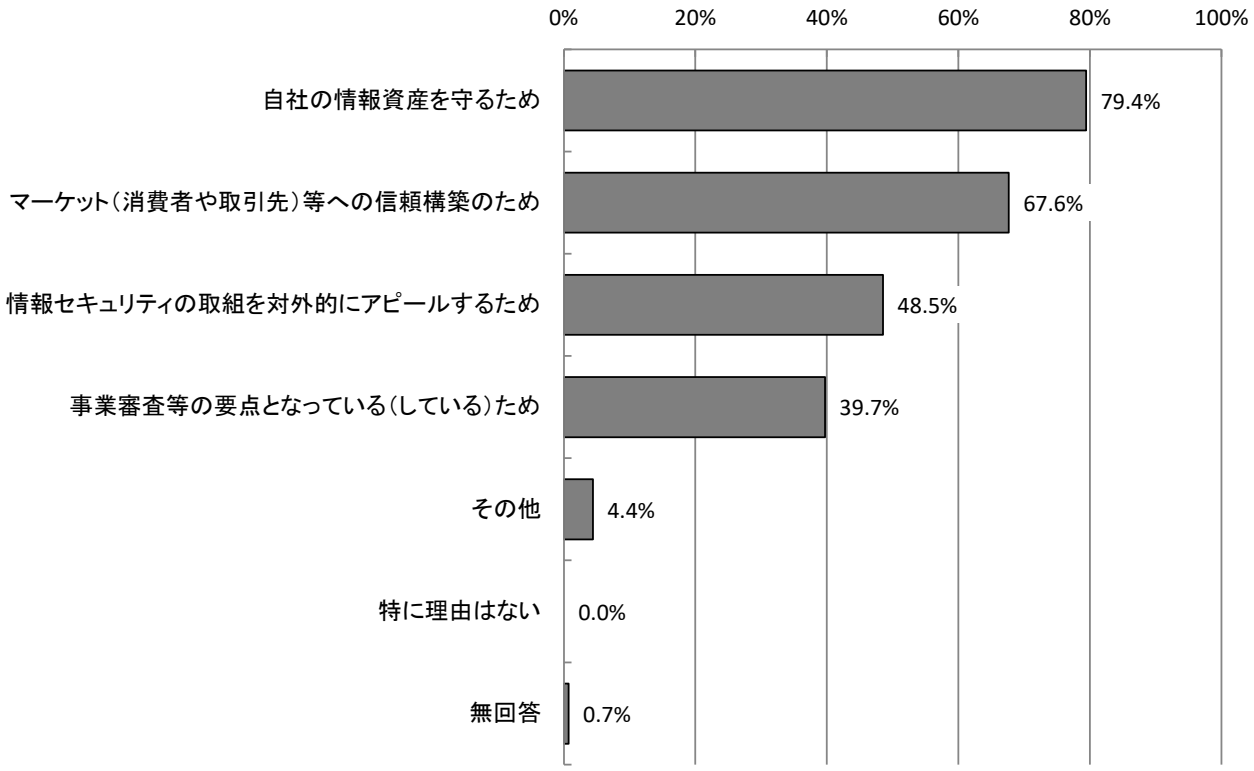


3.1.23　認証制度等を活用する理由　【問16-1】

認証制度等を活用する理由については、「自社の情報資産を守るため」が79.4%で最も高い。次いで「マーケット（消費者や取引先）等への信頼構築のため」が67.6%となっている。

※本項目は、認証制度等を活用している社・団体等を対象としている。

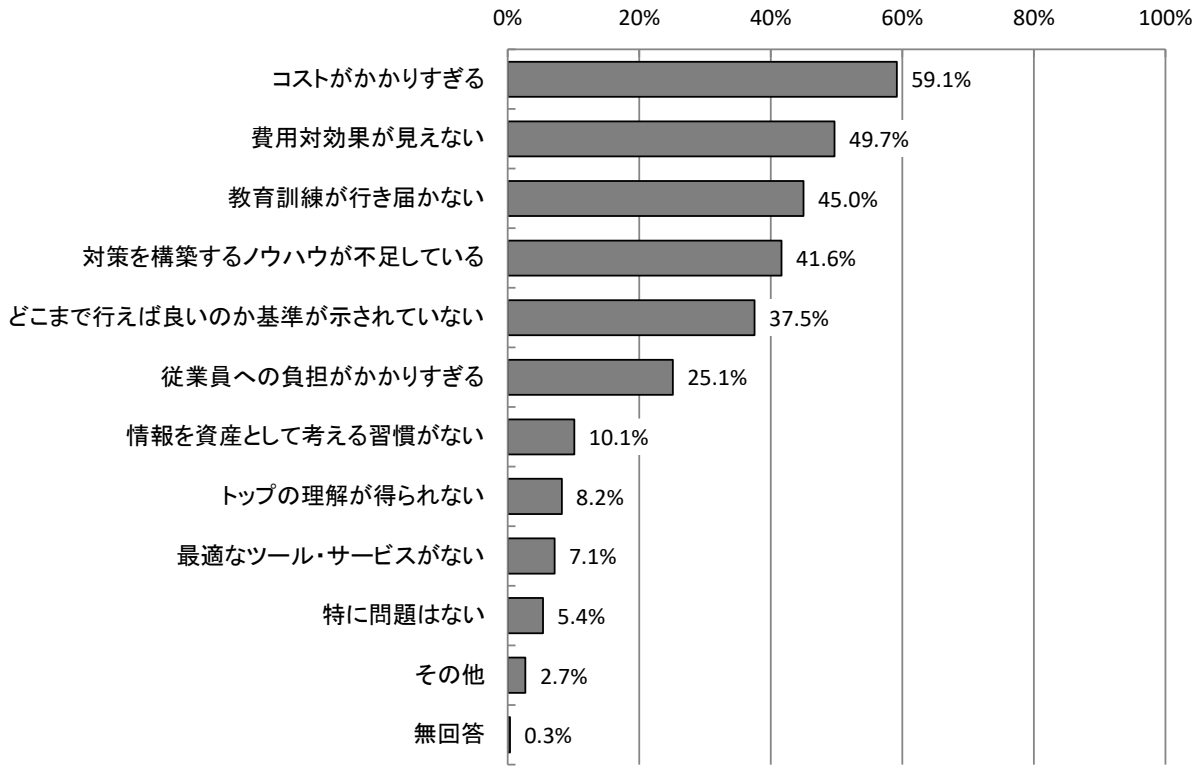
【全体】第三者機関の認証制度等の利用状況（MA, n=136）



3.1.24　情報セキュリティ対策への投資に関する問題点　【問17】

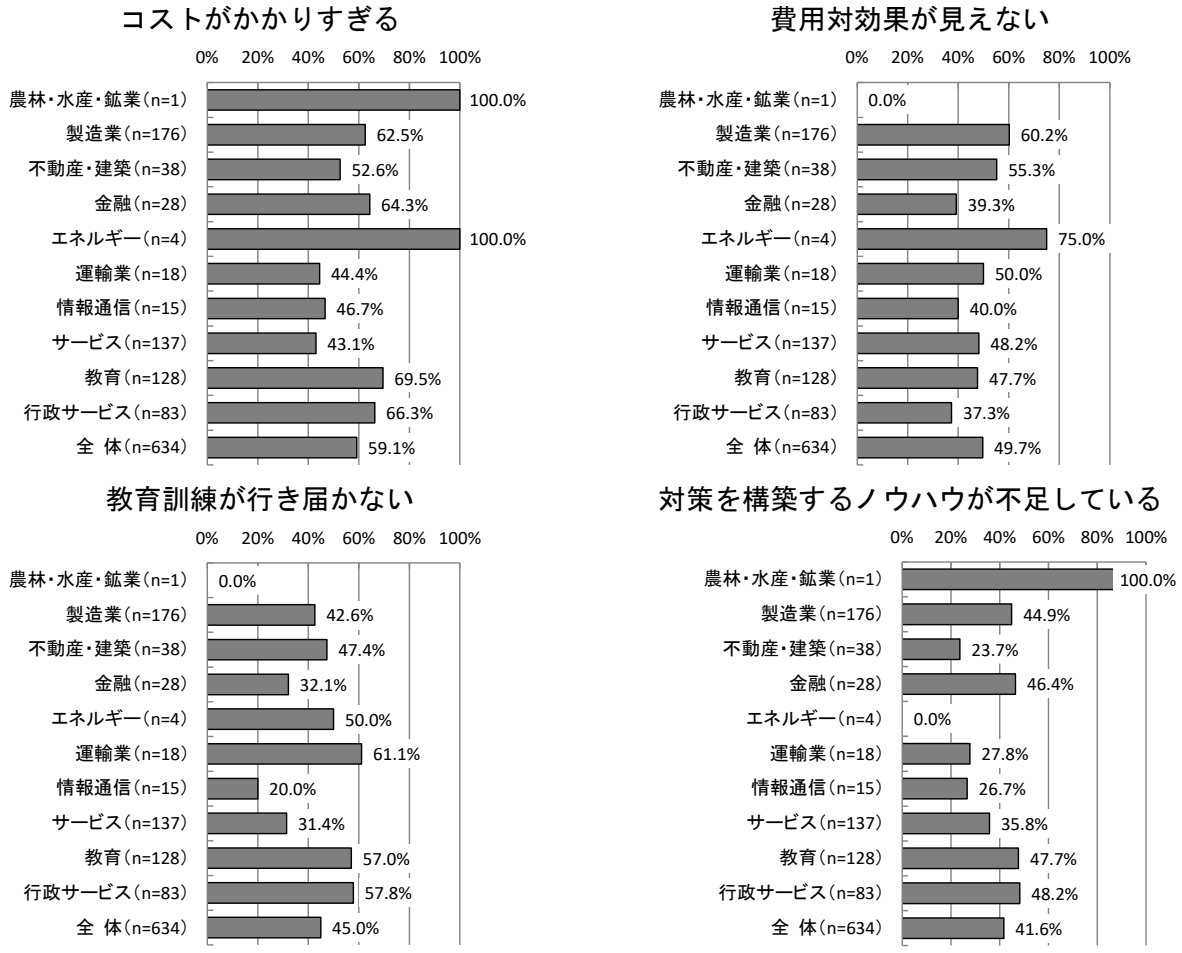
情報セキュリティ対策への投資に関する問題点については、「コストがかかりすぎる」が59.1%、「費用対効果が見えない」が49.7%で高くなっている。次いで「教育訓練が行き届かない」が45.0%、「対策を構築するノウハウが不足している」が41.6%となっている。

【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=634）



【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69.5%で高くなっている。「費用対効果が見えない」については、「製造業」が60.2%で高い。「教育訓練が行き届かない」については、「運輸業」が61.1%で高く、「対策を構築するノウハウが不足している」では、「行政サービス」が48.2%、「教育」が47.7%で高くなっている。

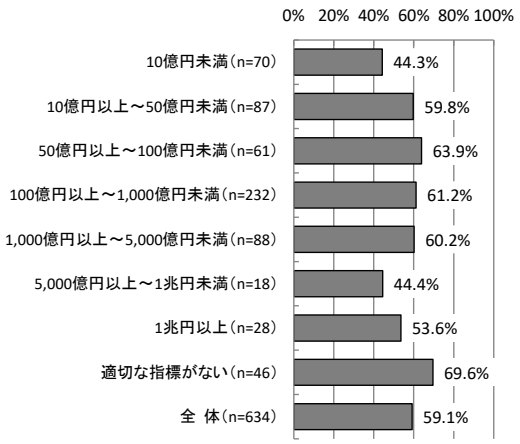
【業種別分析】情報セキュリティ対策への投資に関する問題点



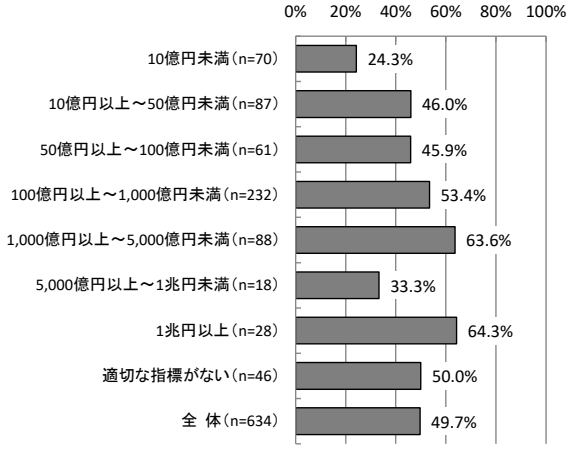
【売上・予算規模別分析】売上・予算規模別にみると、「コストがかかりすぎる」については、「50億円以上～100億円未満」が63.9％で最も高く、次いで「100億円以上～1,000億円未満」が61.2％となっている。「費用対効果が見えない」については、「1兆円以上」が64.3％、「1,000億円以上～5,000億円未満」が63.6％で高い。「教育訓練が行き届かない」については、「10億円以上～50億円未満」が55.2％で最も高くなっている。

【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

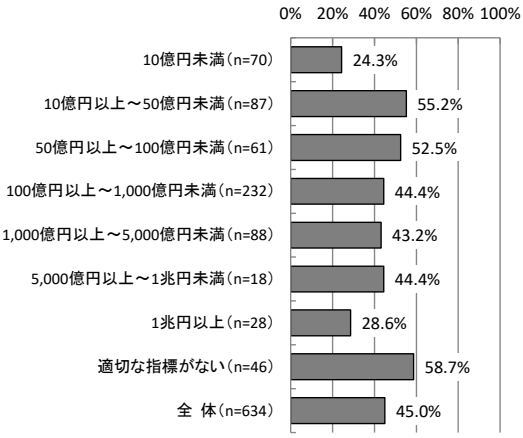
コストがかかりすぎる



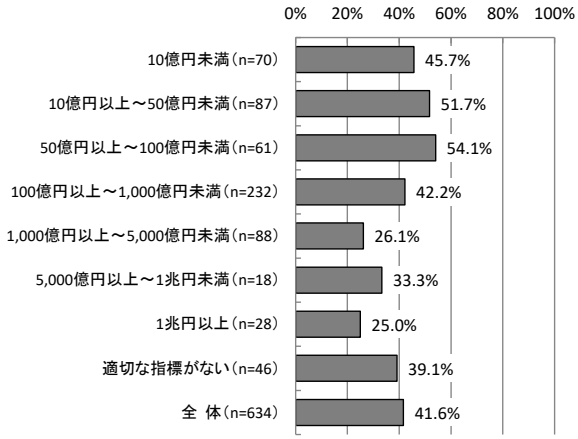
費用対効果が見えない



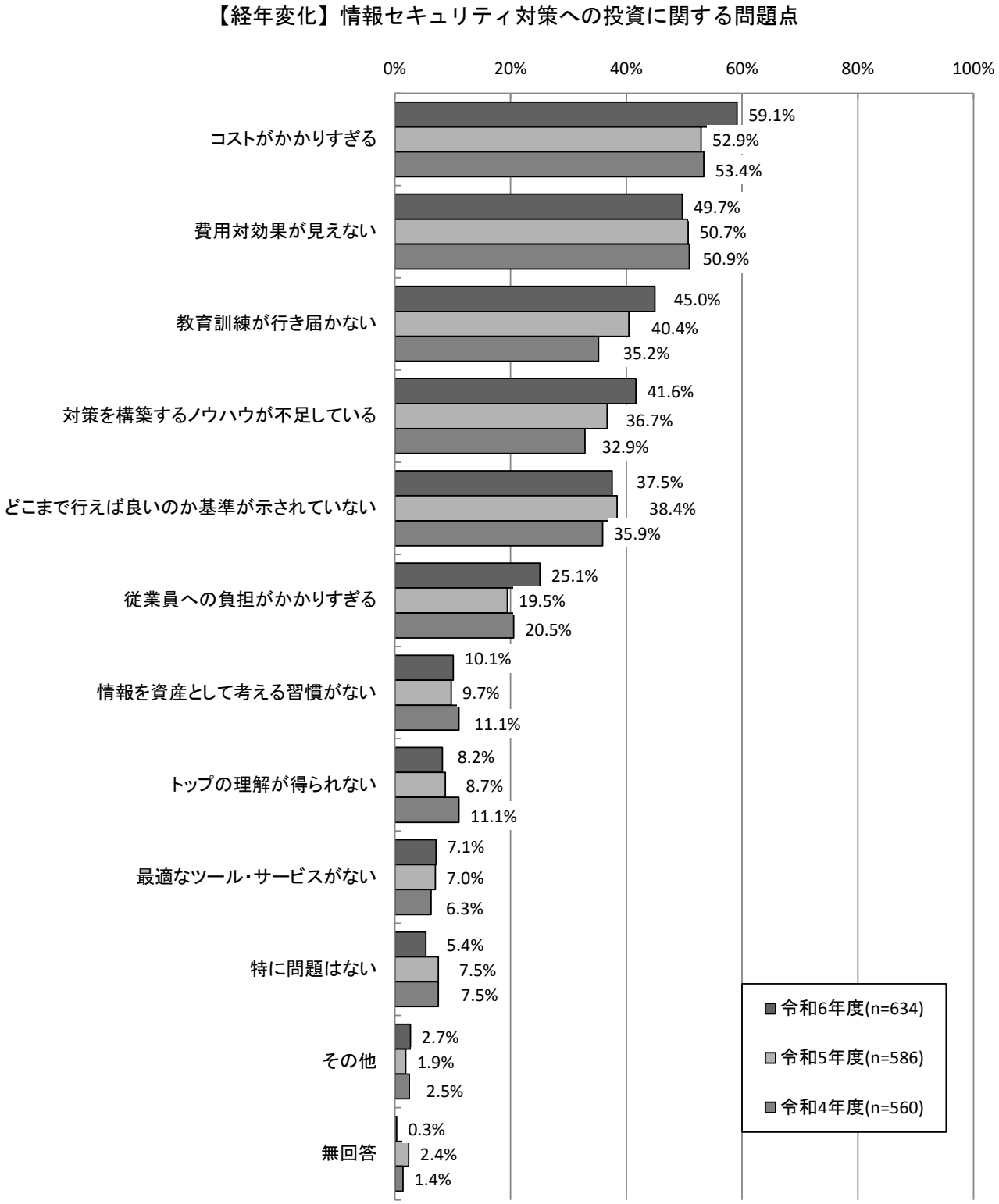
教育訓練が行き届かない



対策を構築するノウハウが不足している



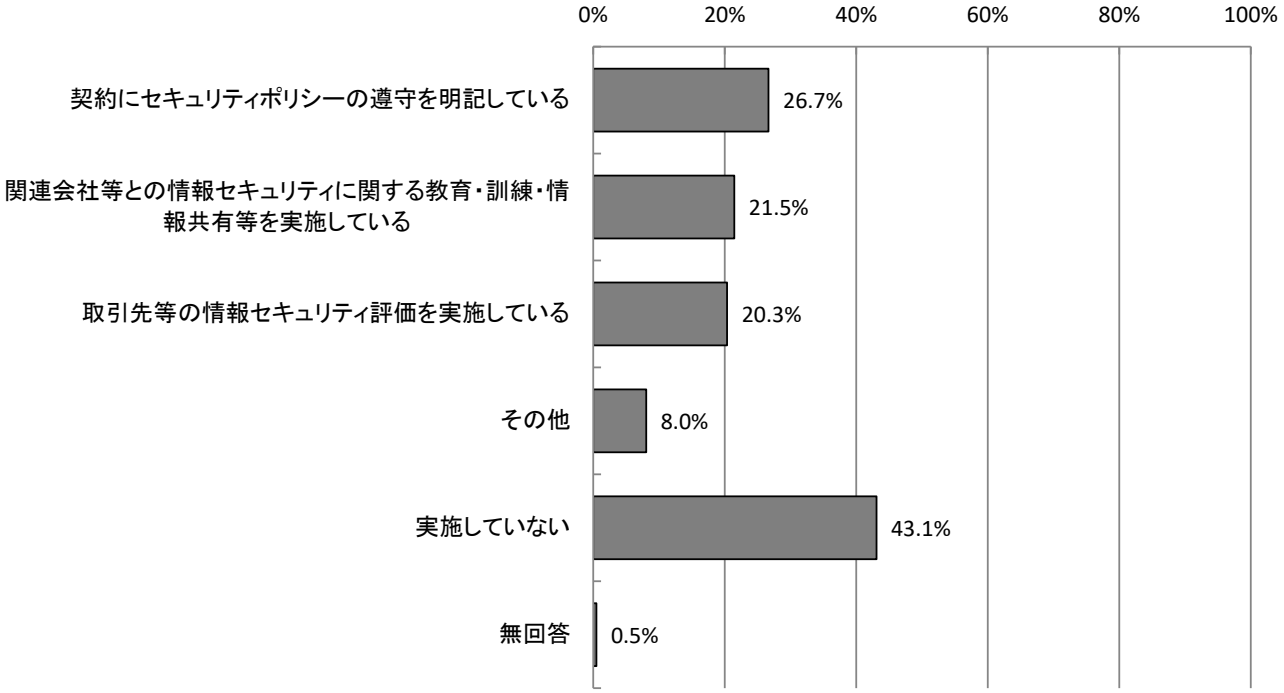
【経年変化】昨年度と比較すると、「コストがかかりすぎる」が6.2ポイント、「従業員への負担がかかりすぎる」が5.6ポイント、「対策を構築するノウハウが不足している」が4.9ポイント増加している。



3.1.25　サプライチェーンリスク対策として情報セキュリティ対策を求めているか　【問18】

サプライチェーンリスク対策については「契約にセキュリティポリシーの遵守を明記している」が26.7%と高く、次いで「関連会社等との情報セキュリティに関する教育・訓練・情報共有等を実施している」が21.5%となっている。

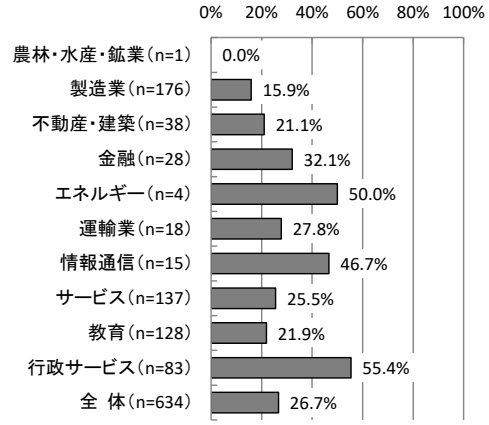
【全体】サプライチェーンリスク対策として対策を行っているか（MA, n=634）



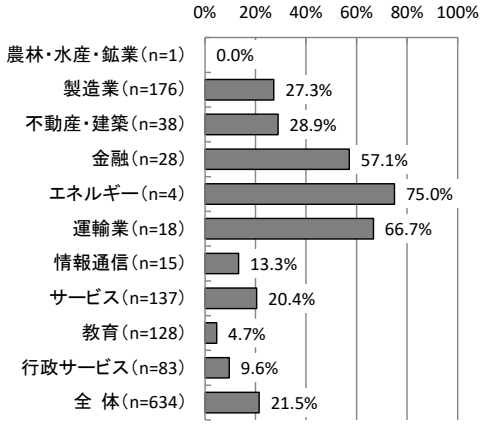
【業種別分析】業種別では、「契約にセキュリティポリシーの遵守を明記している」は「行政サービス」が55.4%、「情報通信」が46.7%で高くなっている。一方、「製造業」は15.9%で最も低くなっている。

【業種別分析】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

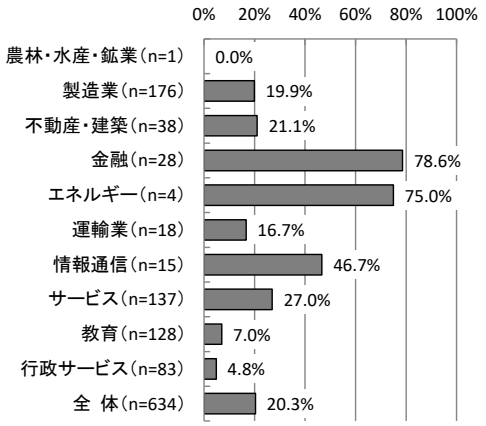
契約にセキュリティポリシーの遵守を明記している



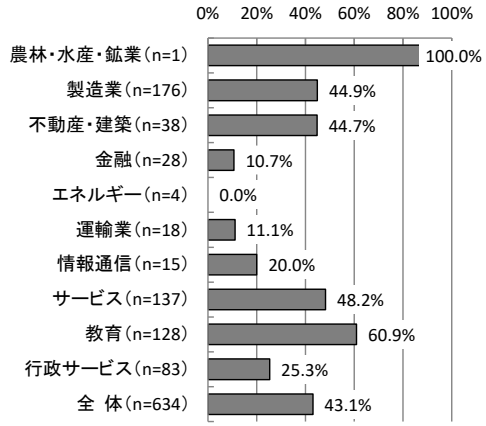
関連会社等との情報セキュリティに関する教育・訓練・情報共有等を実施している



取引先等の情報セキュリティ評価を実施している



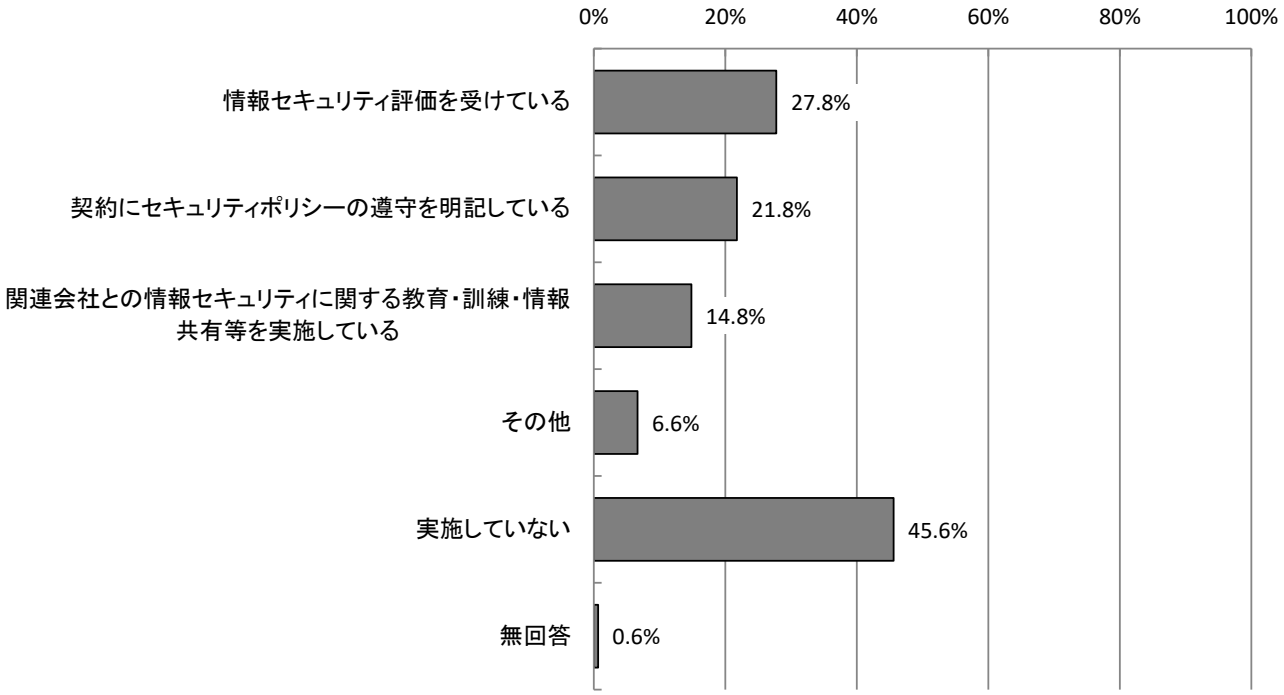
実施していない



3.1.26　サプライチェーンリスク対策として情報セキュリティ対策を求められているか【問19】

サプライチェーンリスク対策については「情報セキュリティ評価を受けている」が27.8%と高く、次いで「契約にセキュリティポリシーの遵守を明記している」が21.8%となっている。

【全体】サプライチェーンリスク対策として情報セキュリティ対策を求められているか（MA, n=634）

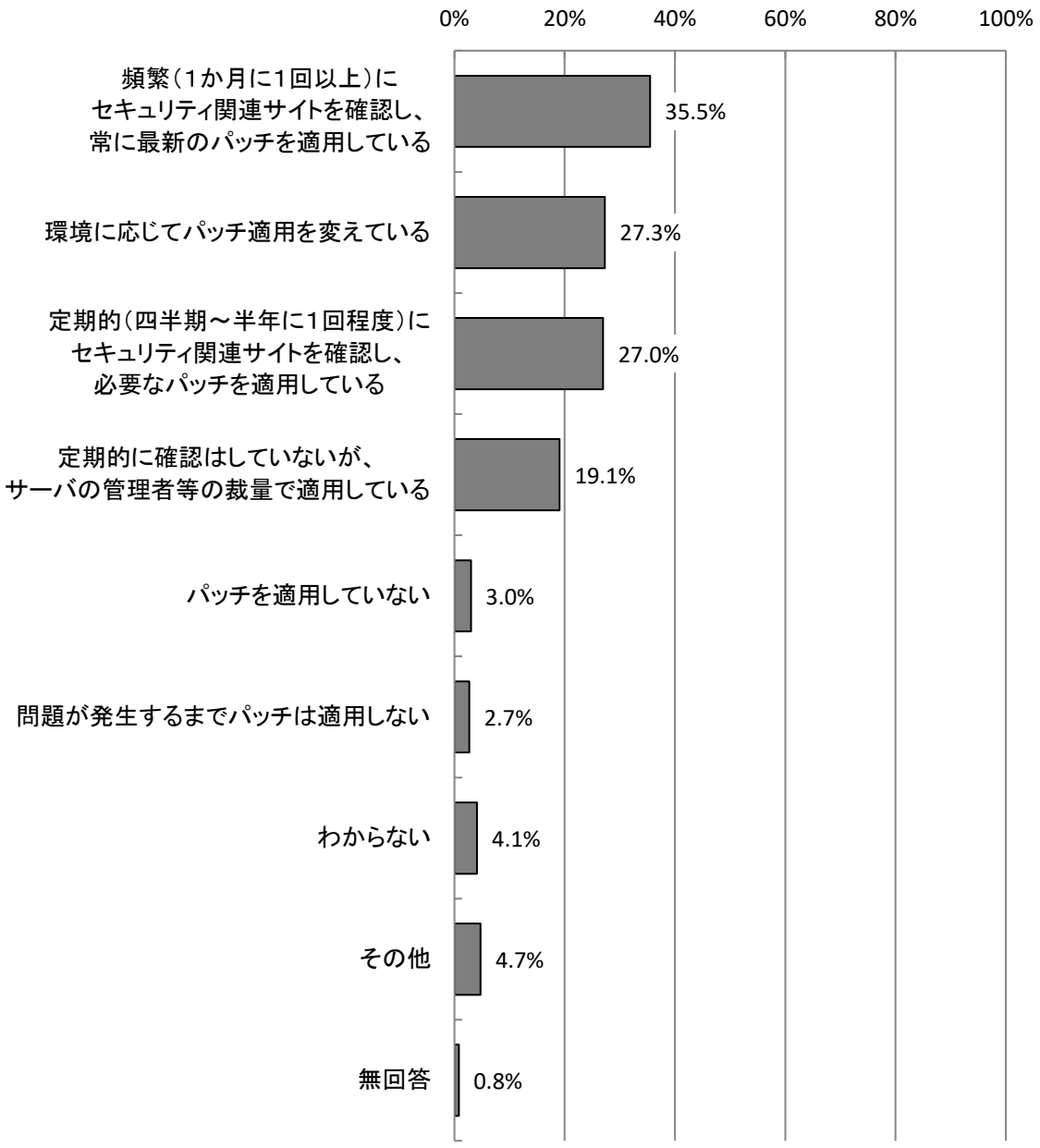


3.2 技術的対策

3.2.1 セキュリティパッチの適用状況 【問20】

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35.5%で最も高く、次いで「環境に応じてパッチ適用を変えている」が27.3%、「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27.0%となっている。

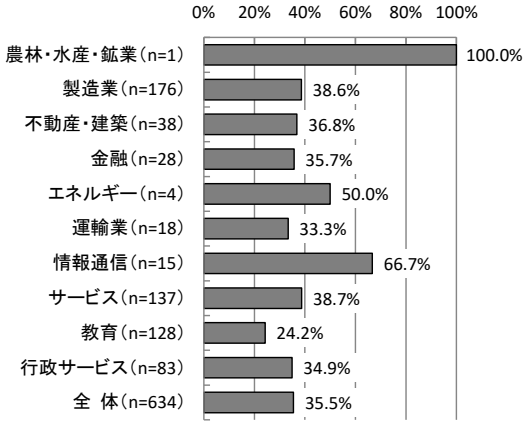
【全体】セキュリティパッチの適用状況（MA,n=634）



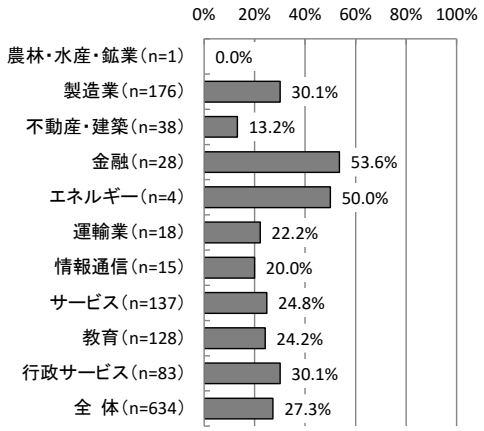
【業種別分析】業種別にみると、「頻繁（１か月に１回以上）にセキュリティ関連サイトを確認し、常に最新のパッチを適用している」については、「情報通信」が66.7%と最も高くなっている。

【業種別分析】セキュリティパッチの適用状況

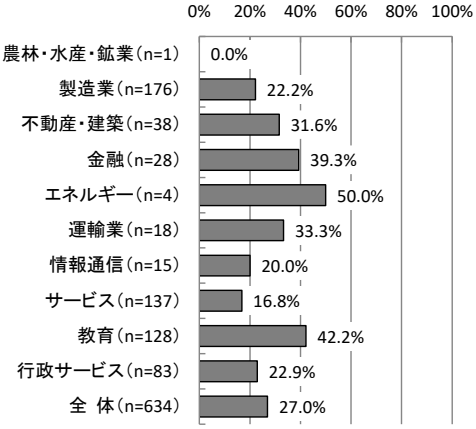
頻繁（１か月に１回以上）に
セキュリティ関連サイトを確認し、
常に最新のパッチを適用している



環境に応じてパッチ適用を変えている



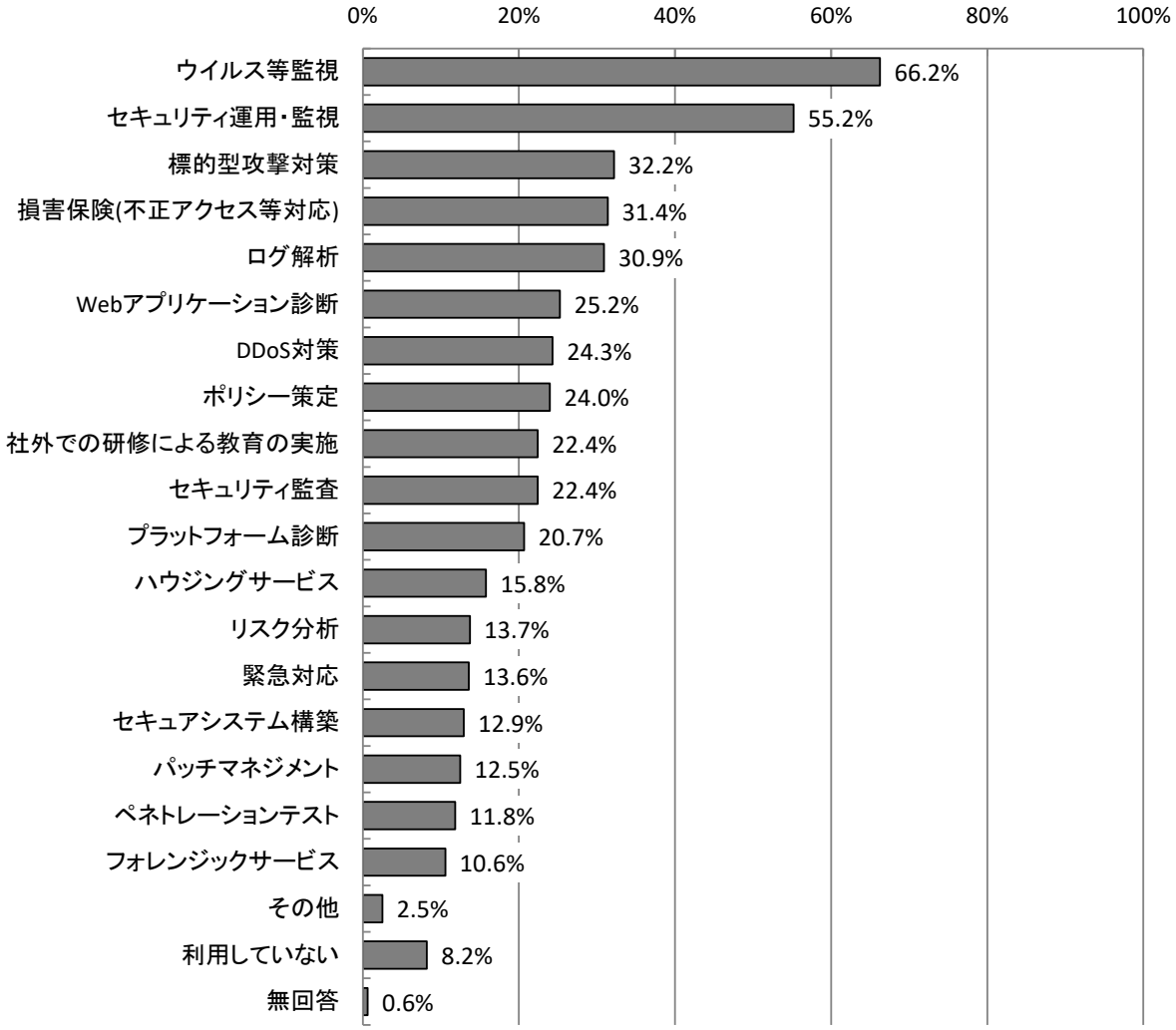
定期的（四半期～半年に１回程度）に
セキュリティ関連サイトを確認し、必要なパッチを適用している



3.2.2　利用しているセキュリティサービス　【問21】

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66.2%で最も高く、次いで「セキュリティ運用・監視」が55.2%となっている。一方「利用していない」は8.2%となっている。

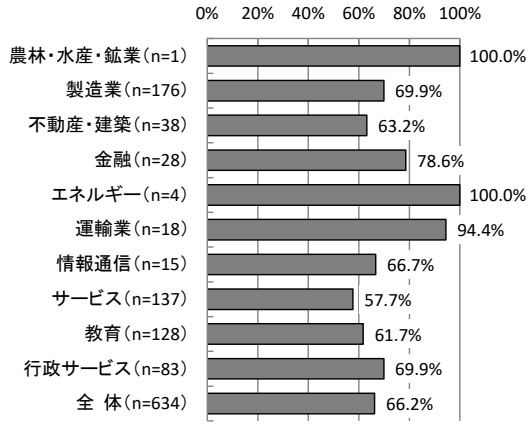
【全体】利用しているセキュリティサービス（MA,n=634）



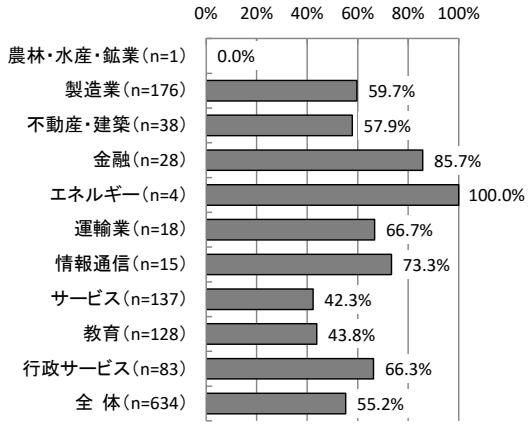
【業種別分析】業種別にみると、「ウイルス等監視」については、「運輸業」が94.4%、「金融」が78.6%で高い。「セキュリティ運用・監視」については、「金融」が85.7%、「情報通信」が73.3%で高くなっている。

【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



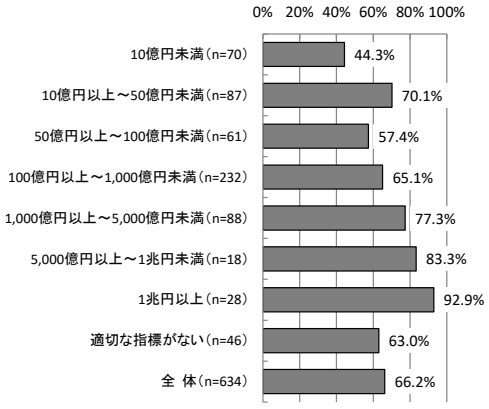
セキュリティ運用・監視



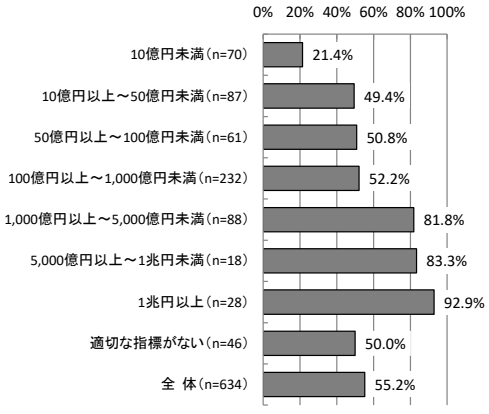
【予算規模別分析】予算規模別にみると、「ウイルス等監視」については、「1兆円以上」が92.9%で最も高くなっている。「セキュリティ運用・監視」についても、「1兆円以上」が92.9%で最も高くなっている。

【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



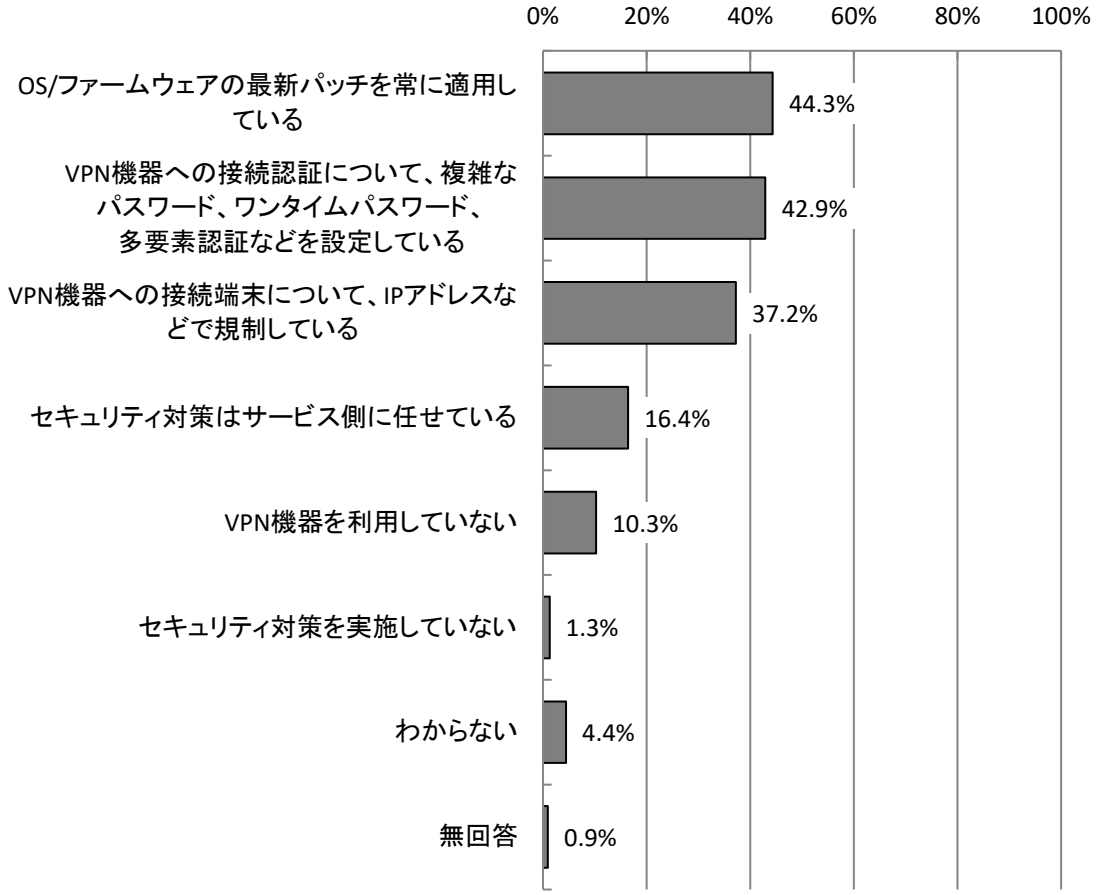
セキュリティ運用・監視



3.2.3 VPN機器のセキュリティ対策 【問22】

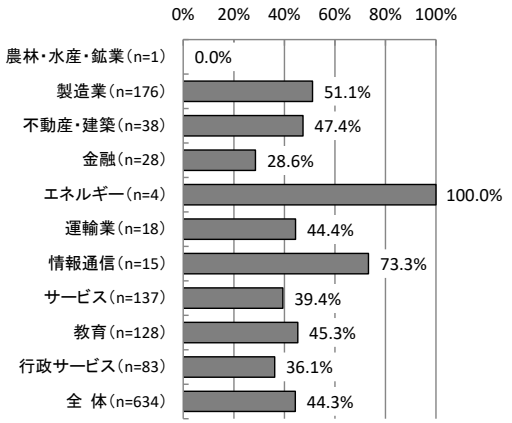
VPN機器のセキュリティ対策は、「OS/ファームウェアの最新パッチを常に適用している」が44.3%で最も高い。「VPN機器への接続認証について、複雑なパスワード、ワンタイムパスワード、多要素認証などを設定している」も42.9%と高くなっている。「セキュリティ対策を実施していない」は1.3%と1割未満となっている。

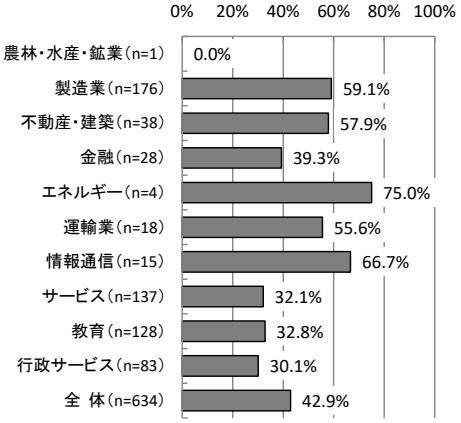
【全体】VPN機器のセキュリティ対策 (MA,n=634)



【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73.3と最も高くなっている。「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」でも「情報通信」が66.7%と最も高くなっている。

【業種別分析】VPN機器のセキュリティ対策

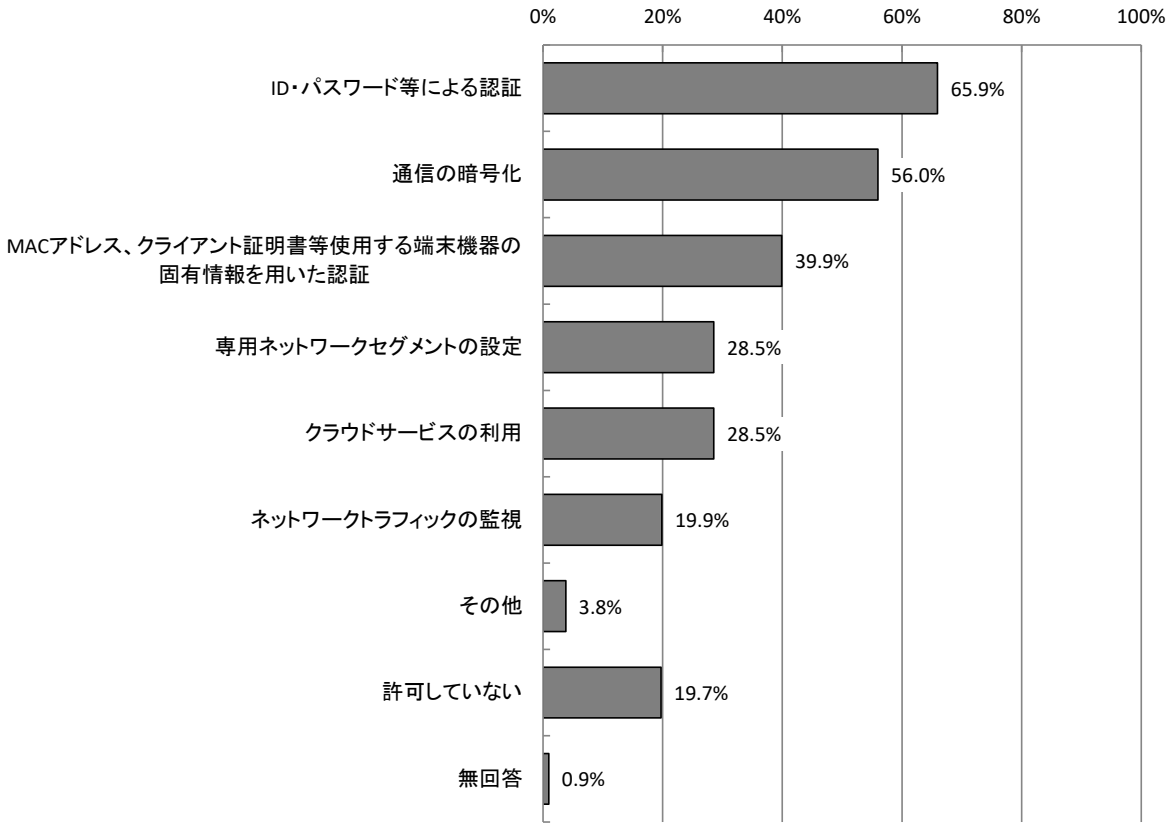




3.2.4　外部からの接続に対するセキュリティ対策　（通信路に対する対策）　【問23-A】

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65.9%で最も高く、次いで「通信の暗号化」が56.0%、「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39.9%となっている。

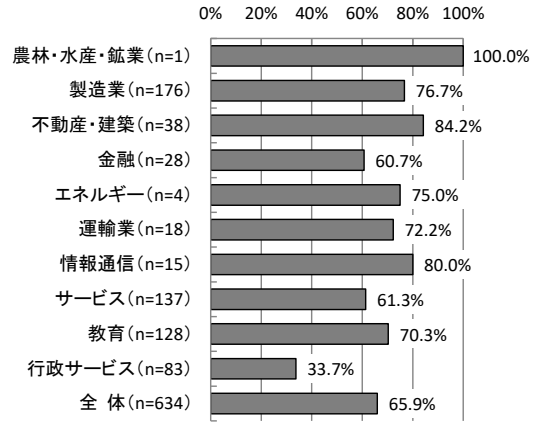
【全体】外部からの接続に対するセキュリティ対策（通信路に対する対策）（MA, n=634）



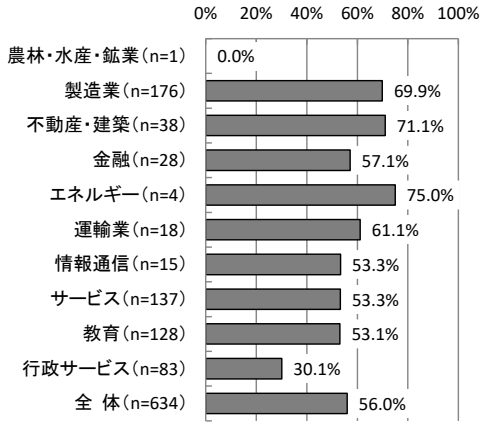
【業種別分析】業種別にみると、「ID・パスワード等による認証」では「不動産・建築」が84.2%と最も高く、「通信の暗号化」では「不動産・建築」が71.1%、「製造業」が69.9%で高い。

【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）

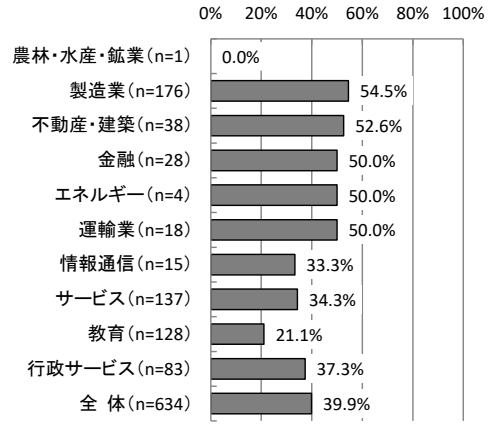
ID・パスワード等による認証



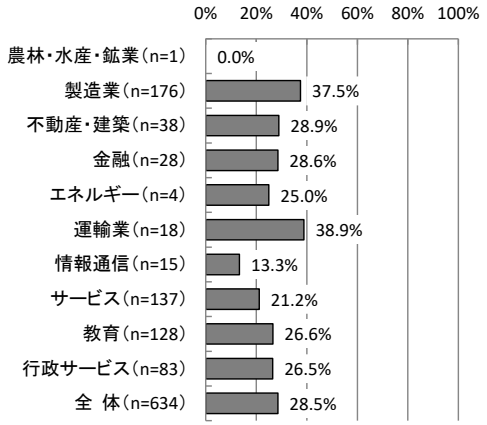
通信の暗号化



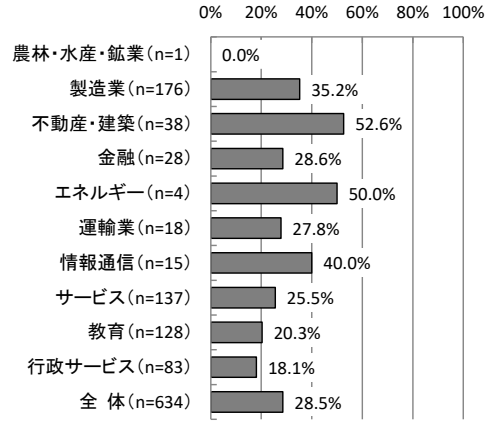
MAC アドレス、クライアント証明書等使用する端末機器の固有情報を用いた認証



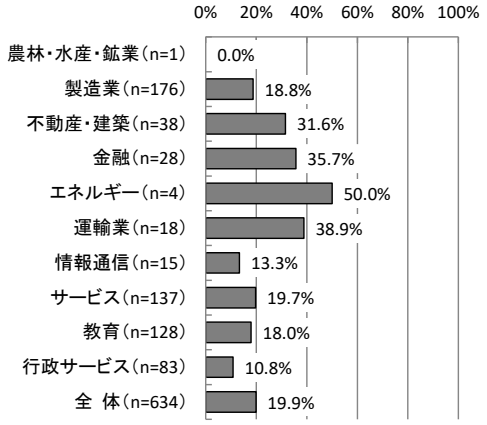
専用ネットワークセグメントの設定



クラウドサービスの利用



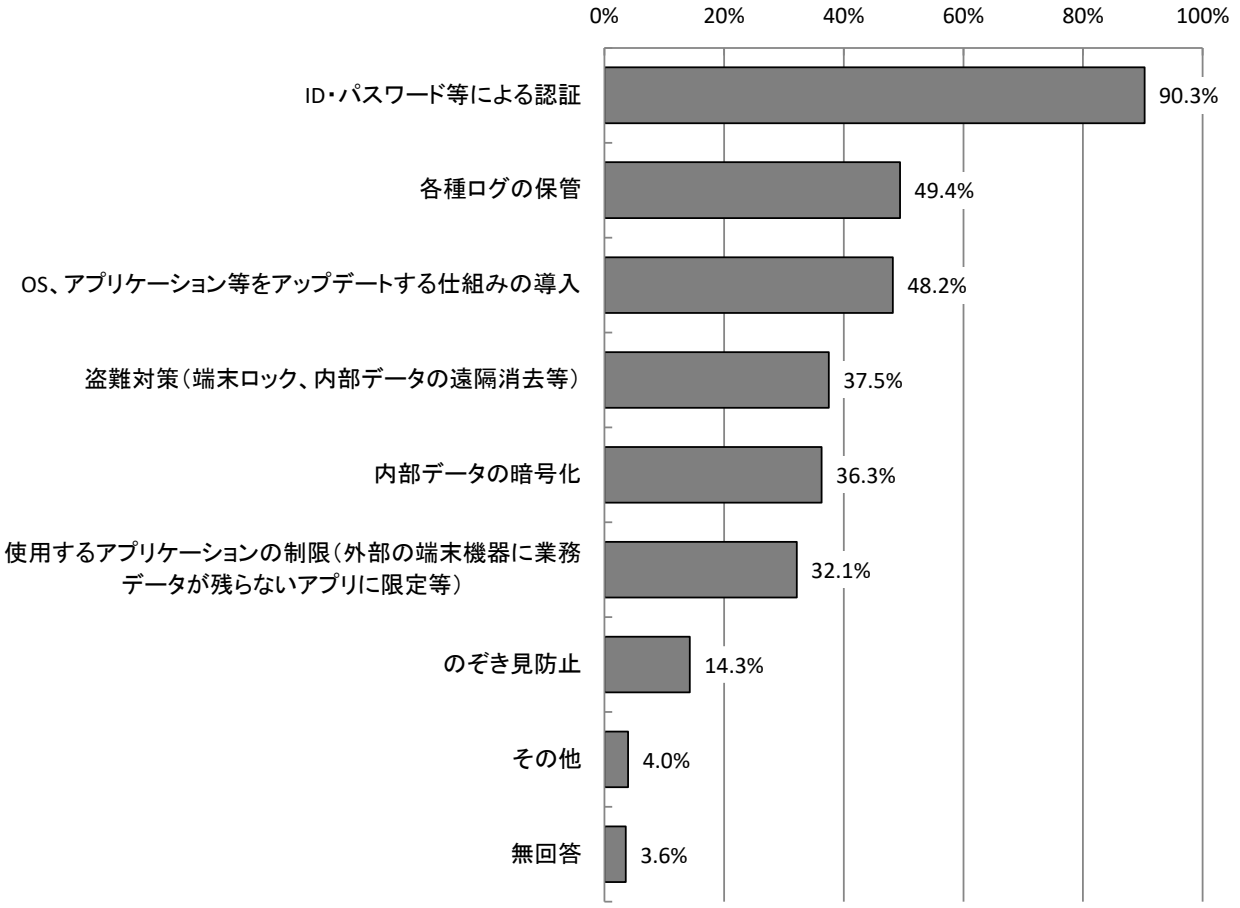
ネットワークトラフィックの監視



3.2.5　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23-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、「ID・パスワード等による認証」が90.3%で最も高く、次いで「各種ログの保管」が49.4%、「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48.2%となっている。

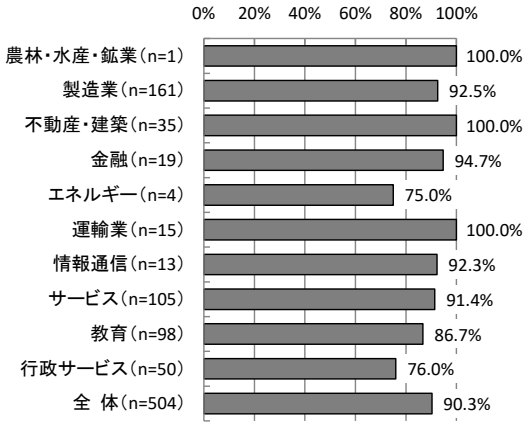
【全体】外部からの接続に対するセキュリティ対策（端末に対する対策）（MA, n=504）



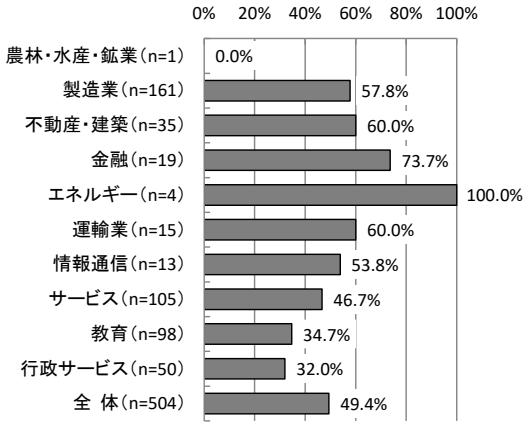
【業種別分析】業種別にみると、「ID・パスワード等による認証」では「不動産・建築」「運輸業」が100.0%と最も高く、「製造業」「金融」「情報通信」「サービス」で90%以上と高くなっている。

【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）

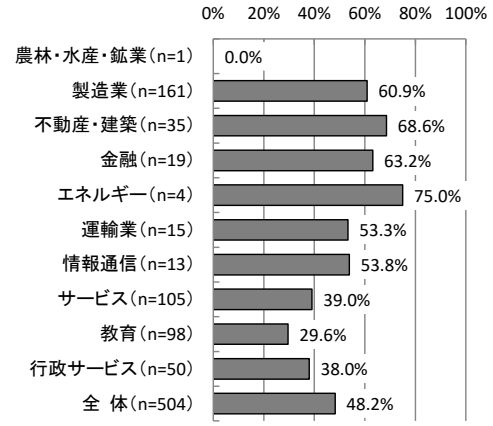
ID・パスワード等による認証



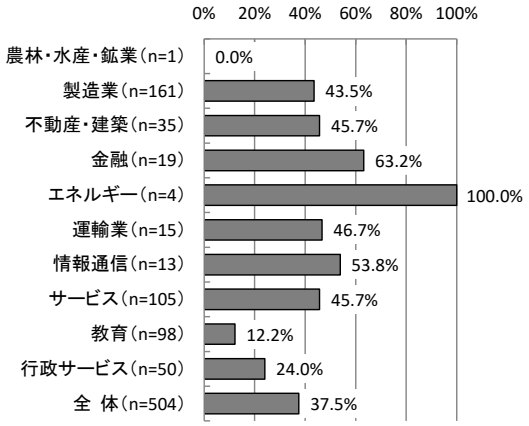
各種ログの保管



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



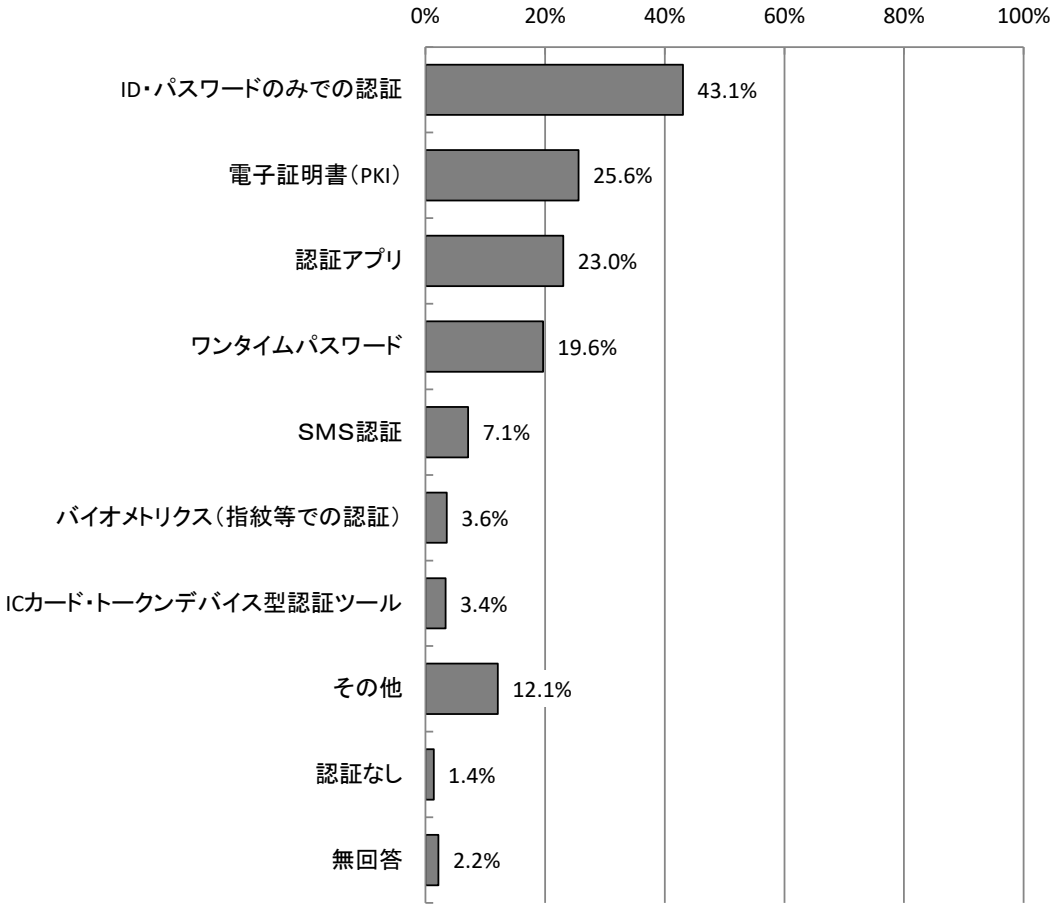
盗難対策
（端末ロック、内部データの遠隔消去等）



3.2.6　社外等からのインターネット接続経由の認証方法　【問24】

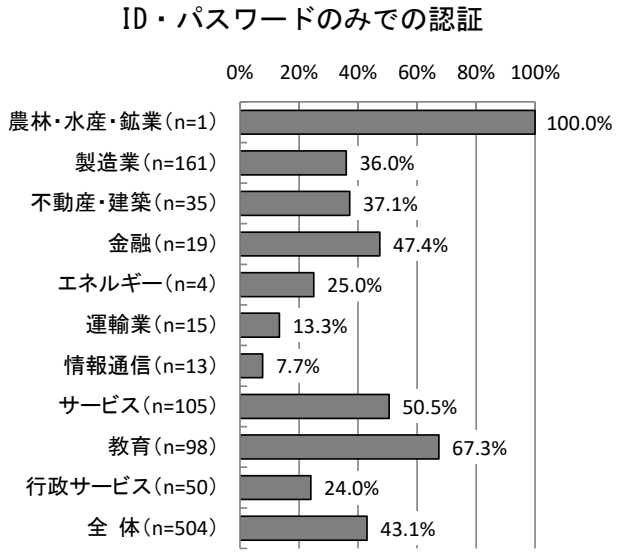
社外等からのインターネット接続経由の認証方法については、「ID・パスワードのみでの認証」が43.1%で最も高い。次いで「電子証明書（PKI）」が25.6%となっている。一方、「認証なし」は1.4%と1割未満となっている。

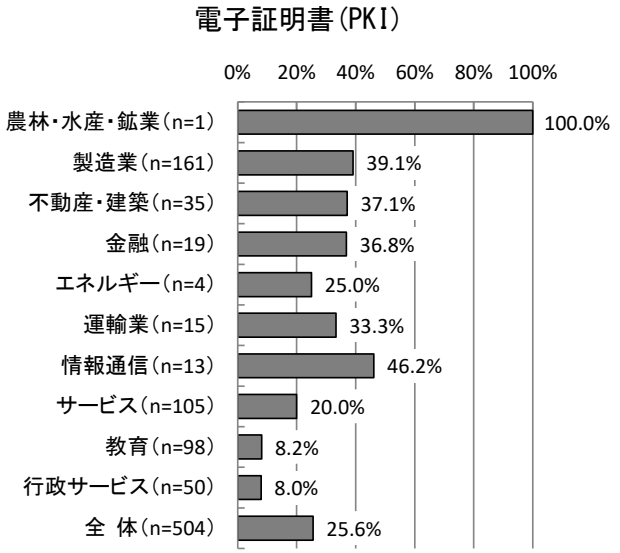
【全体】社外等からのインターネット接続経由の認証方法（MA, n=504）



【業種別分析】業種別にみると、「ID・パスワードのみでの認証」については、「教育」が67.3%、「電子証明書（PKI）」については、「情報通信」が46.2%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



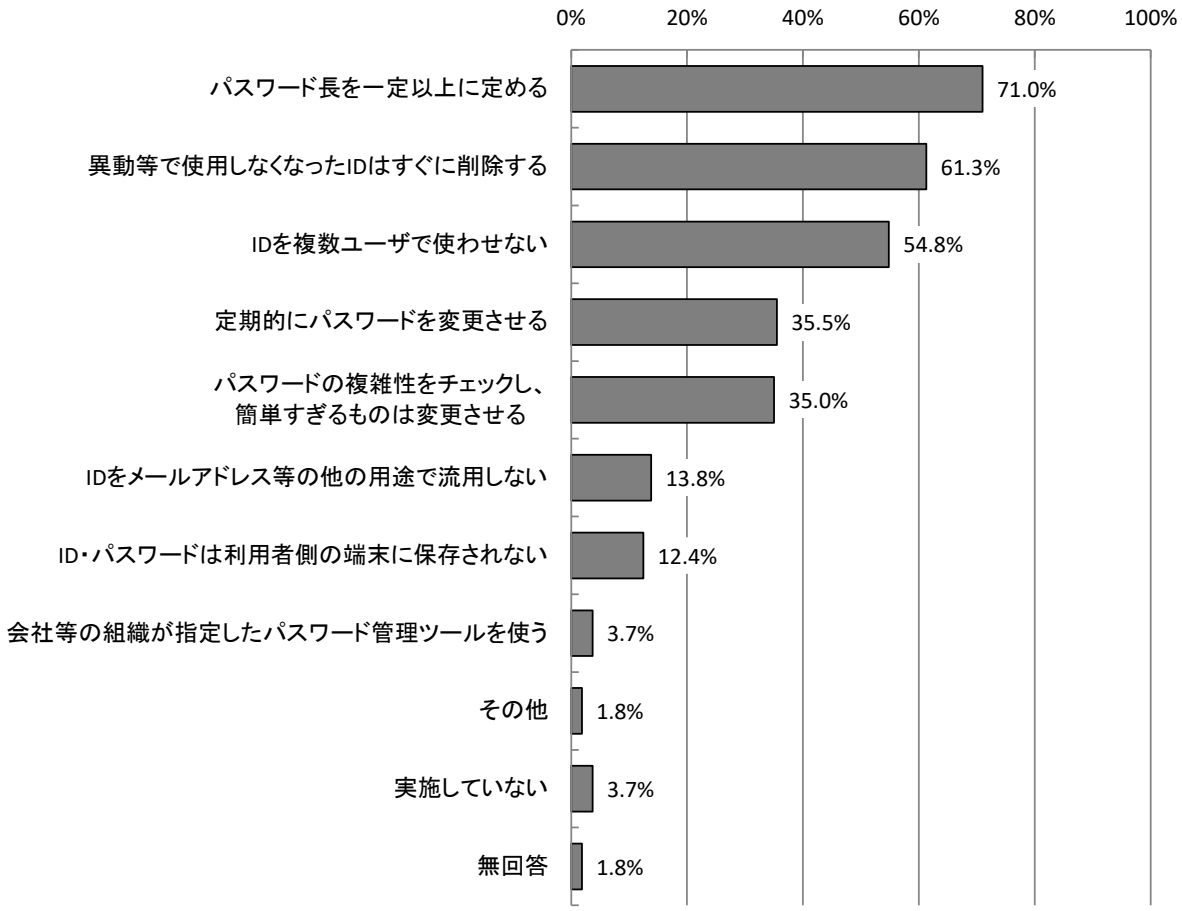


3.2.7　ID・パスワードの管理方法　【問24-1】

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71.0%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61.3%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。

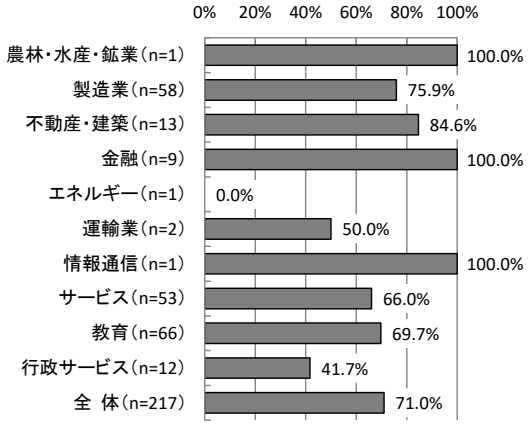
【全体】ID・パスワードの管理方法（MA,n=217）



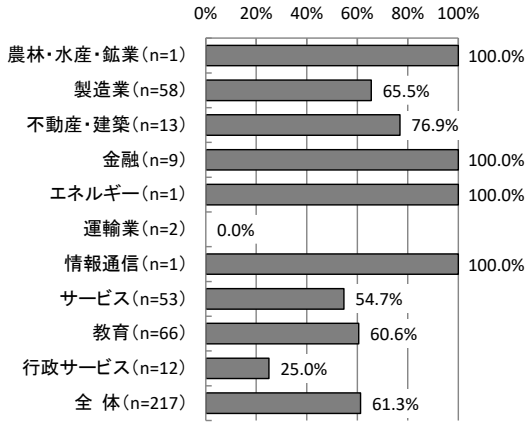
【業種別分析】業種別にみると、「パスワード長を一定以上に定める」については、「金融」が100.0%、「不動産・建築」が84.6%で高くなっている。「異動等で使用しなくなったIDはすぐに削除する」については、「金融」が100.0%、「不動産・建築」が76.9%で高い。

【業種別分析】ID・パスワードの管理方法

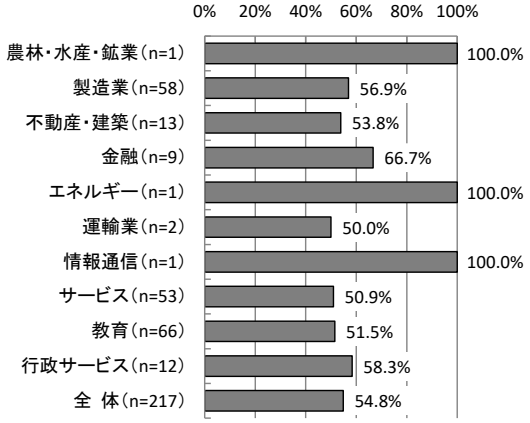
パスワード長を一定以上に定める



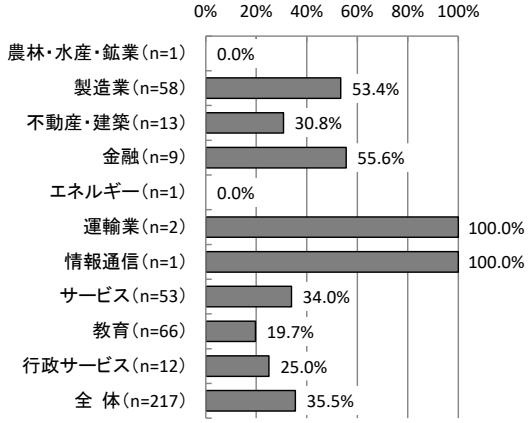
異動等で使用しなくなったIDはすぐに削除する



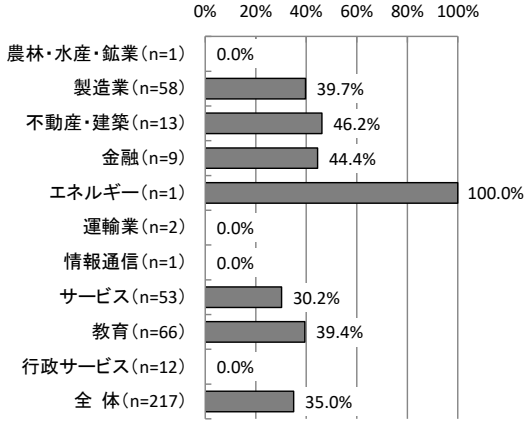
IDを複数ユーザで使わせない



定期的にパスワードを変更させる



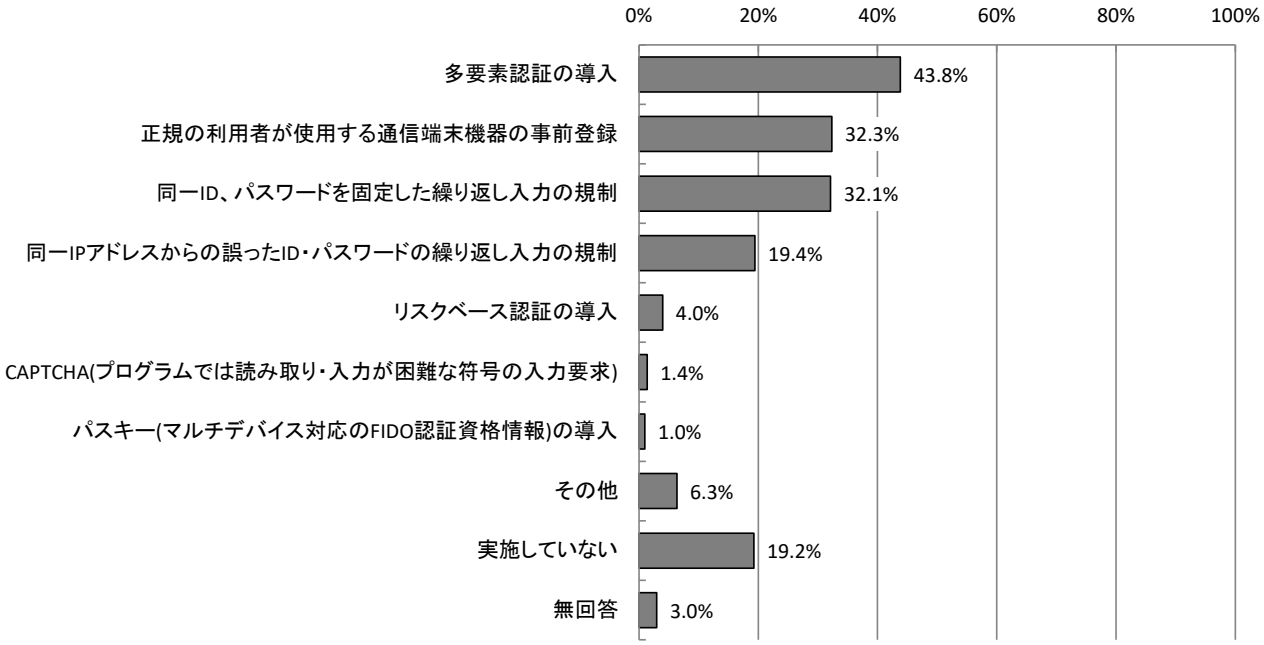
パスワードの複雑性をチェックし、簡単すぎるものは変更させる



3.2.8　不正ログイン対策　【問24-2】

不正ログイン対策については、「多要素認証の導入」が43.8%で最も高くなっている。次いで「正規の利用者が使用する通信端末機器の事前登録」が32.3%、「同一ID、パスワードを固定した繰り返し入力の規制」が32.1%となっている。一方、「実施していない」は19.2%となっている。

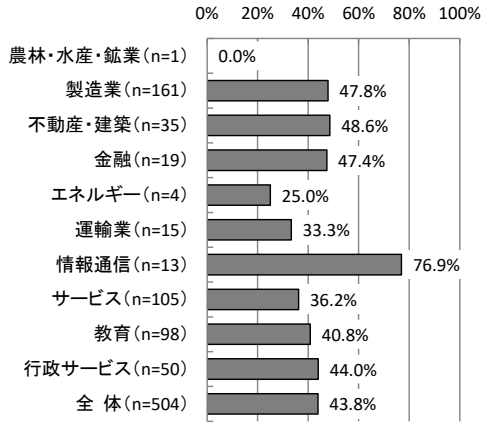
【全体】不正ログイン対策（MA, n=504）



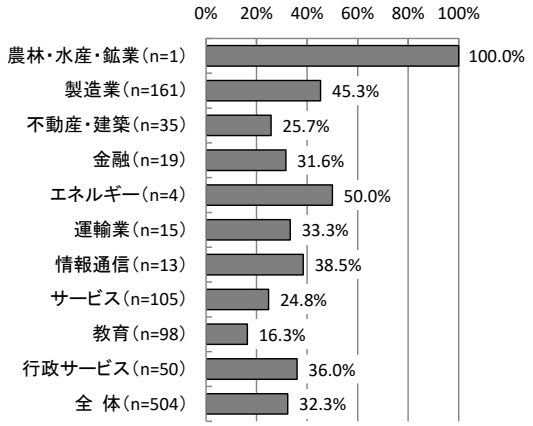
【業種別分析】業種別にみると、「多要素認証の導入」については、「情報通信」が76.9%で高くなっている。「正規の利用者が使用する通信端末機器の事前登録」については、「製造業」が45.3%で高くなっている。「同一ID、パスワードを固定した繰り返し入力の規制」については、「運輸業」が53.3%で高くなっている。

【業種別分析】不正ログイン対策

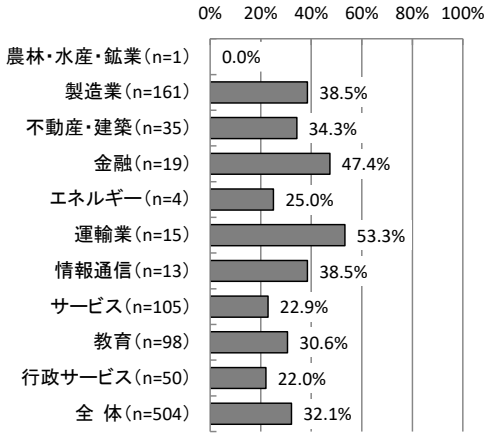
多要素認証の導入



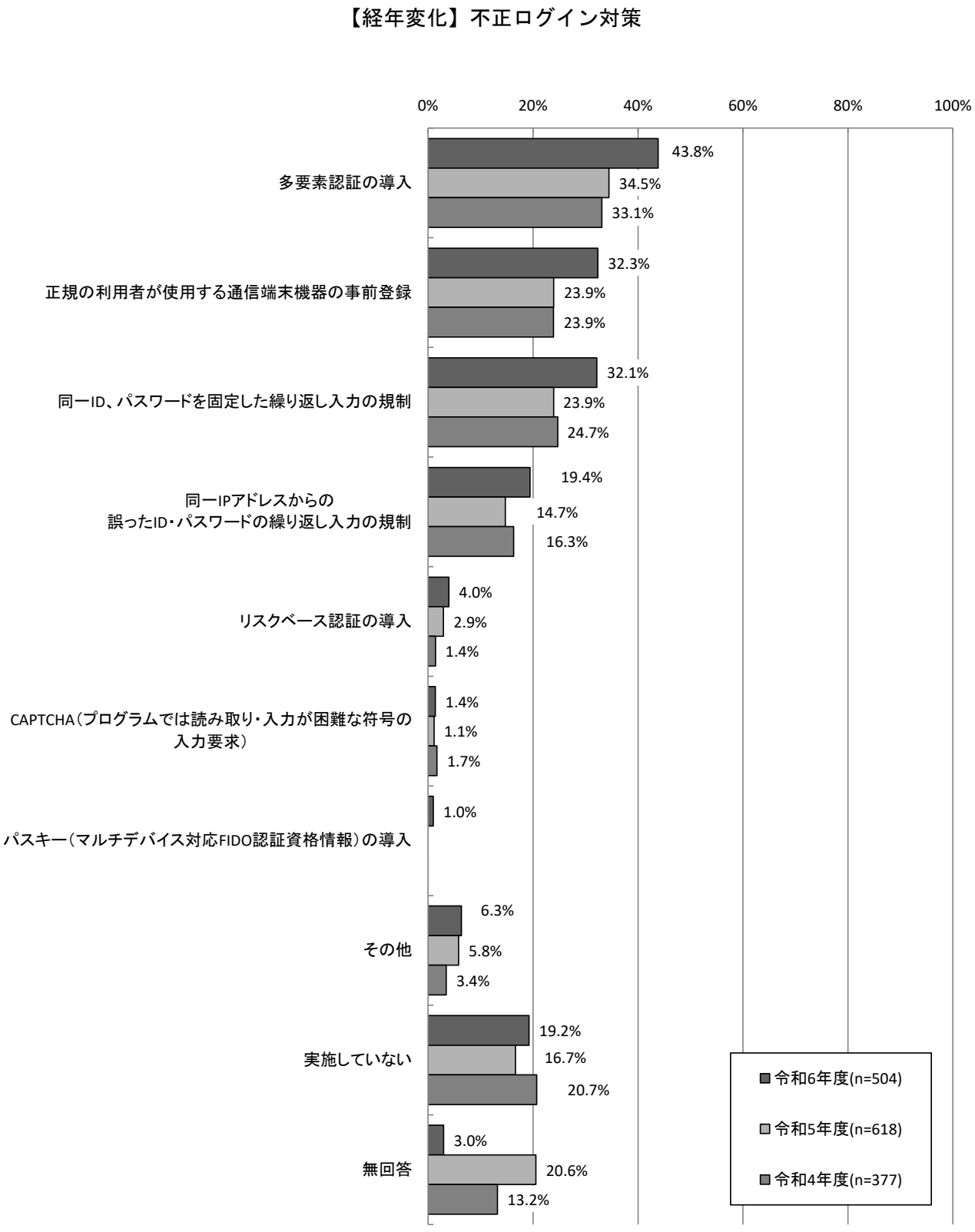
正規の利用者が使用する
通信端末機器の事前登録



同一 ID、パスワードを固定した
繰り返し入力の規制



【経年変化】３年間を比較したところ、「正規の利用者が使用する通信端末機器の事前登録」が8.4ポイント、「同一ID、パスワードを固定した繰り返し入力の規制」が8.2ポイント増加している。

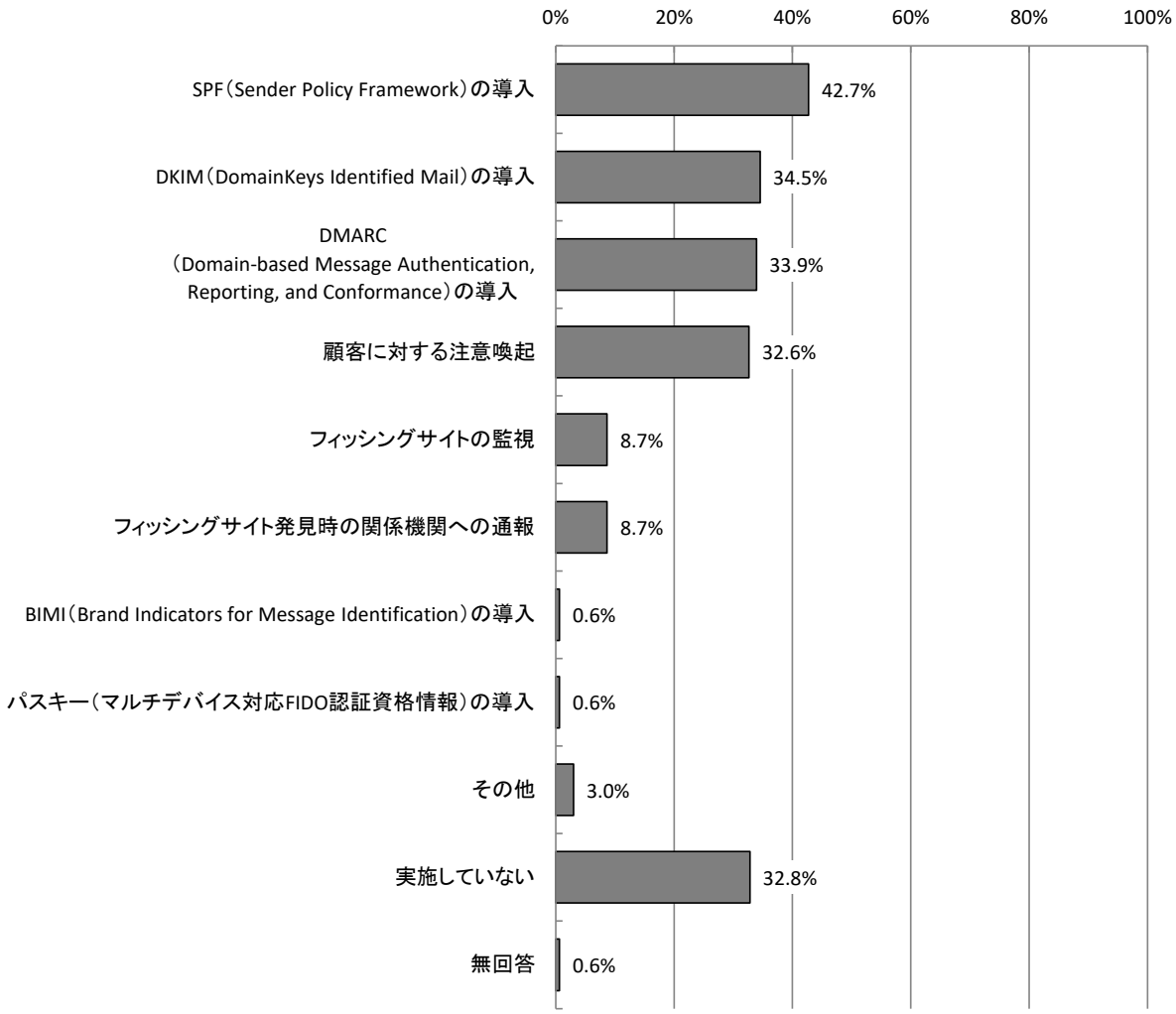


※令和６年度調査で「パスキー（マルチデバイス対応FIDO認証資格情報）の導入」を新設

3.2.9　フィッシング対策【問25】

フィッシング対策については、送信ドメイン認証（SPF、DKIM、DMARC）をみると、「SPF（Sender Policy Framework）の導入」が42.7%、「DKIM（DomainKeys Identified Mail）の導入」が34.5%、「DMARC（「Domain-based Message Authentication, Reporting, and Conformance）の導入」が33.9%、「顧客に対する注意喚起」が32.6%となっている。一方で、「実施していない」は32.8%となっている。

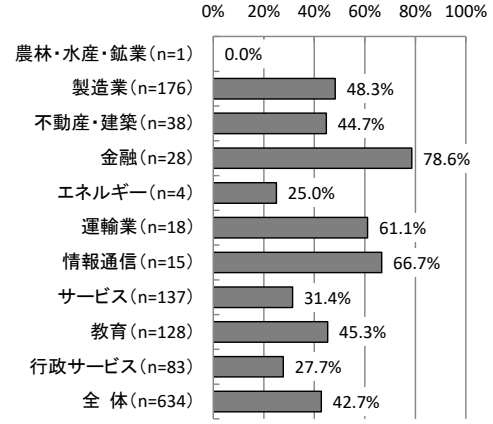
【全体】フィッシング対策（SA, n=634）



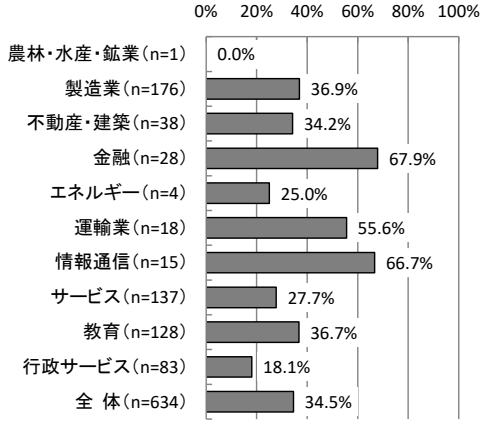
【業種別分析】業種別にみると、送信ドメイン認証（SPF、DKIM、DMARC）については、「SPF（Sender Policy Framework）の導入」では「金融」が78.6%、「DKIM（DomainKeys Identified Mail）の導入」では「金融」が67.9%、「情報通信」が66.7%、「DMARC（Domain-based Message Authentication, Reporting, and Conformance）の導入」では「情報通信」が73.3%で高くなっている。「顧客に対する注意喚起」では「金融」が78.6%で高くなっている。

【業種別分析】フィッシング対策

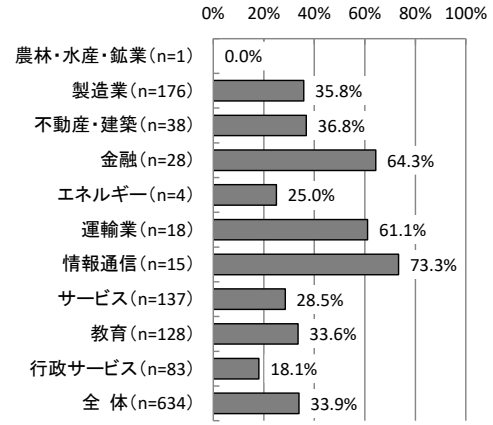
SPF（Sender Policy Framework）の導入



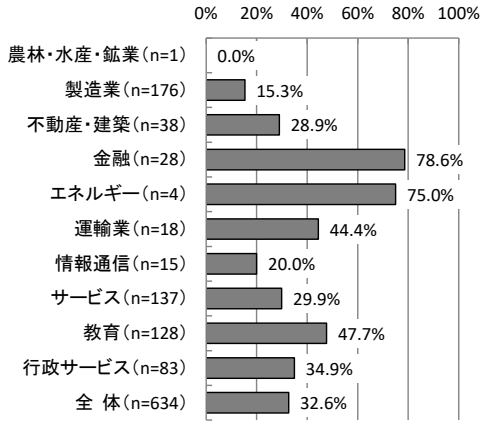
DKIM（DomainKeys Identified Mail）の導入



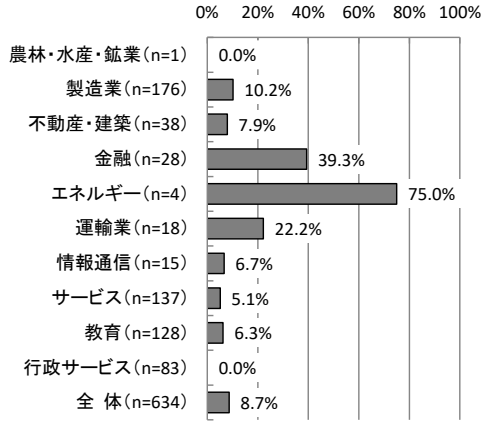
DMARC（Domain-based Message Authentication, Reporting, and Conformance）の導入



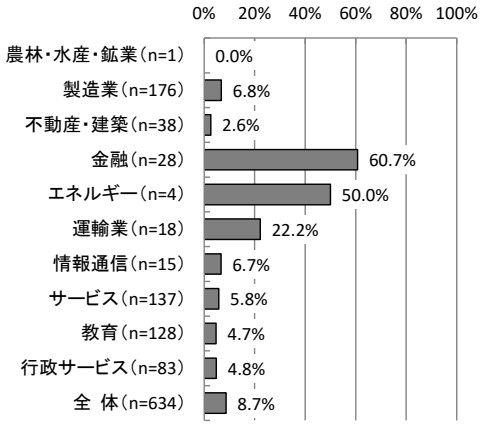
顧客に対する注意喚起



フィッシングサイトの監視



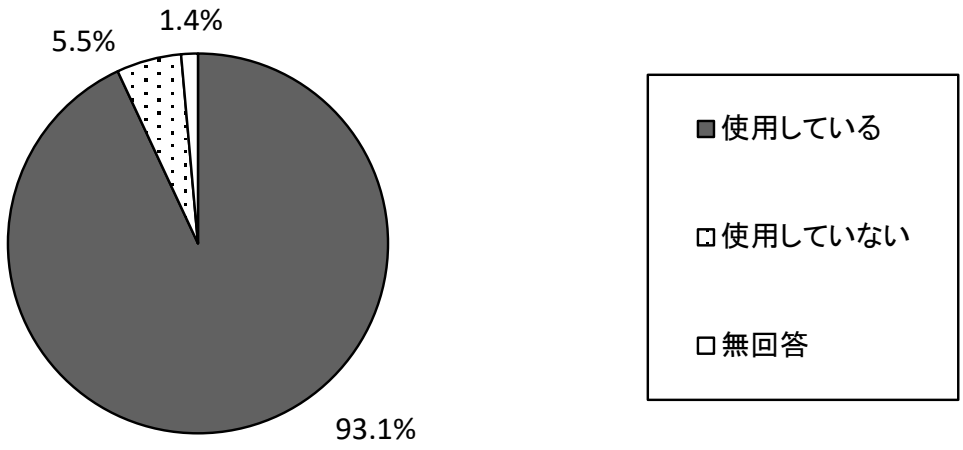
フィッシングサイト発見時の関係機関への通報



3.2.10　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26】

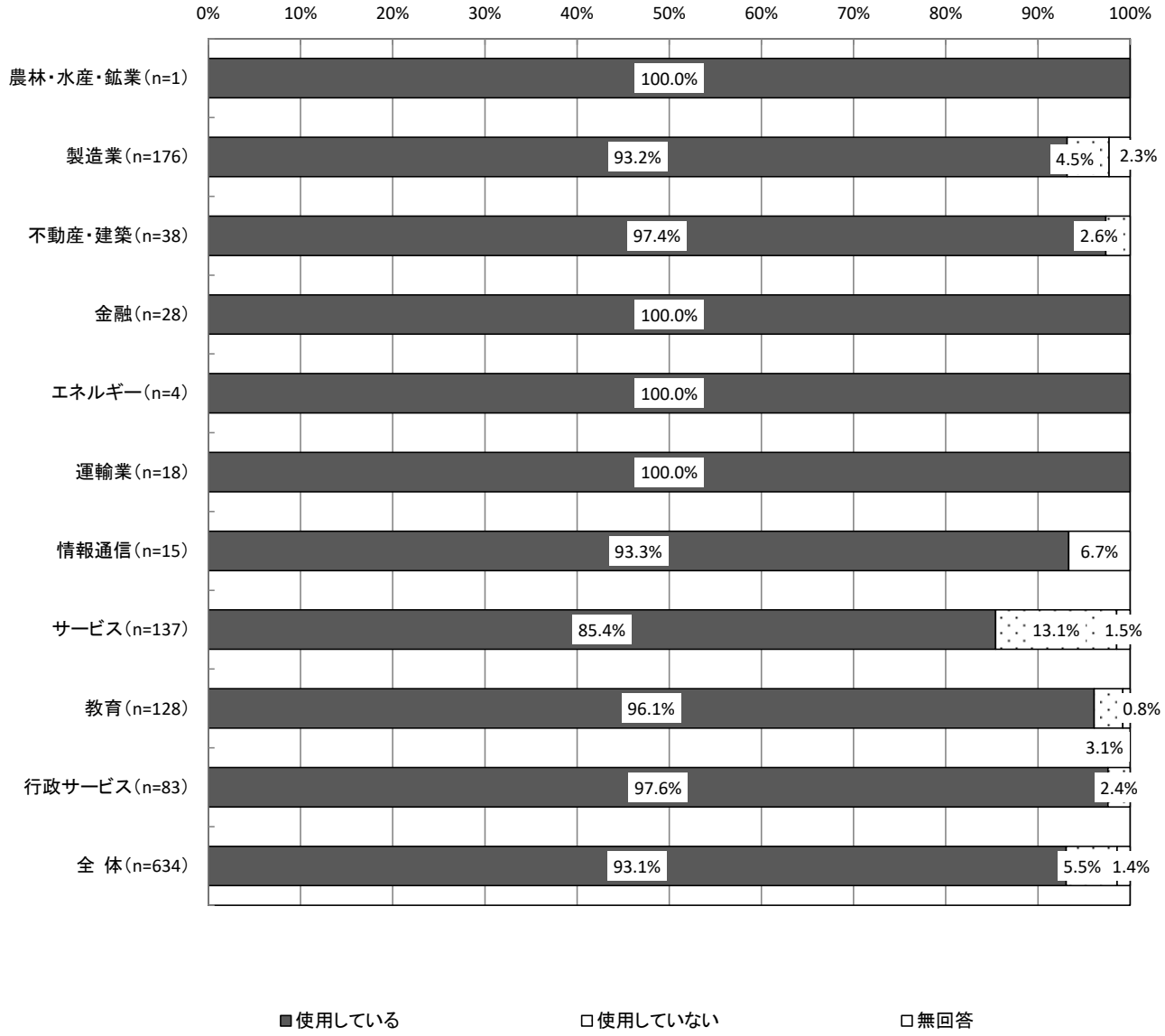
各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）の利用状況については、「使用している」が93.1%、「使用していない」が5.5%となっている。

【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=634）



【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」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85.4％で「使用していない」が13.1％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

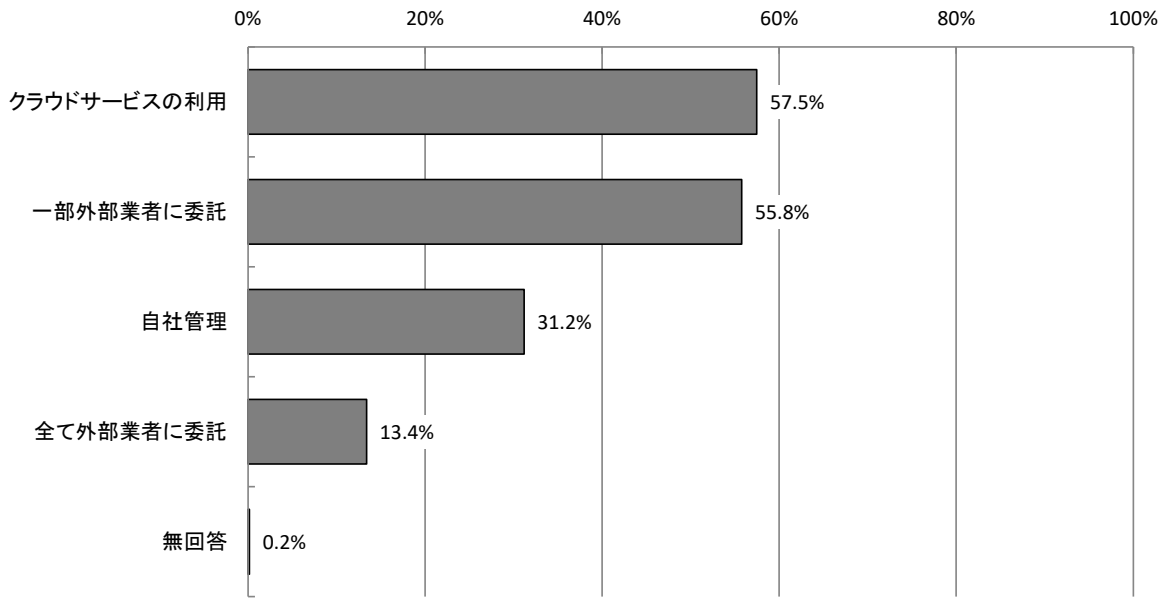


3.2.11　各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）の管理環境【問26-1】

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、「クラウドサービスの利用」が57.5%で最も高く、次いで「一部外部業者に委託」が55.8%、「自社管理」が31.2%となっている。

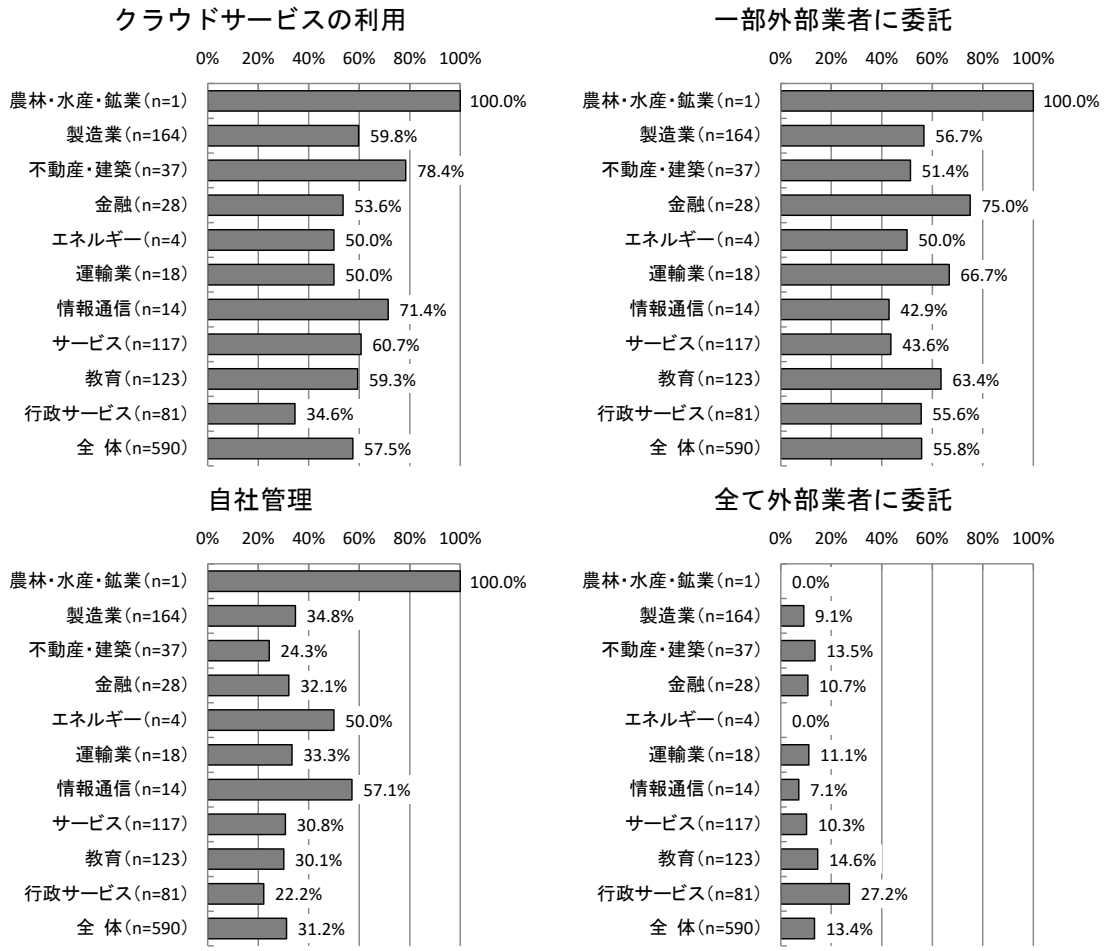
※本項目は、各種サービス（Webサイト、メール管理、ファイル管理等）を使用している社・団体等を対象としている。

【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（MA,n=590）



【業種別分析】業種別にみると、「クラウドサービスの利用」については、「不動産・建築」が78.4%で最も高く、「行政サービス」が34.6%で最も少なくなっている。「一部外部業者に委託」については、「金融」が75.0%で最も高くなっている。

【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）の管理環境

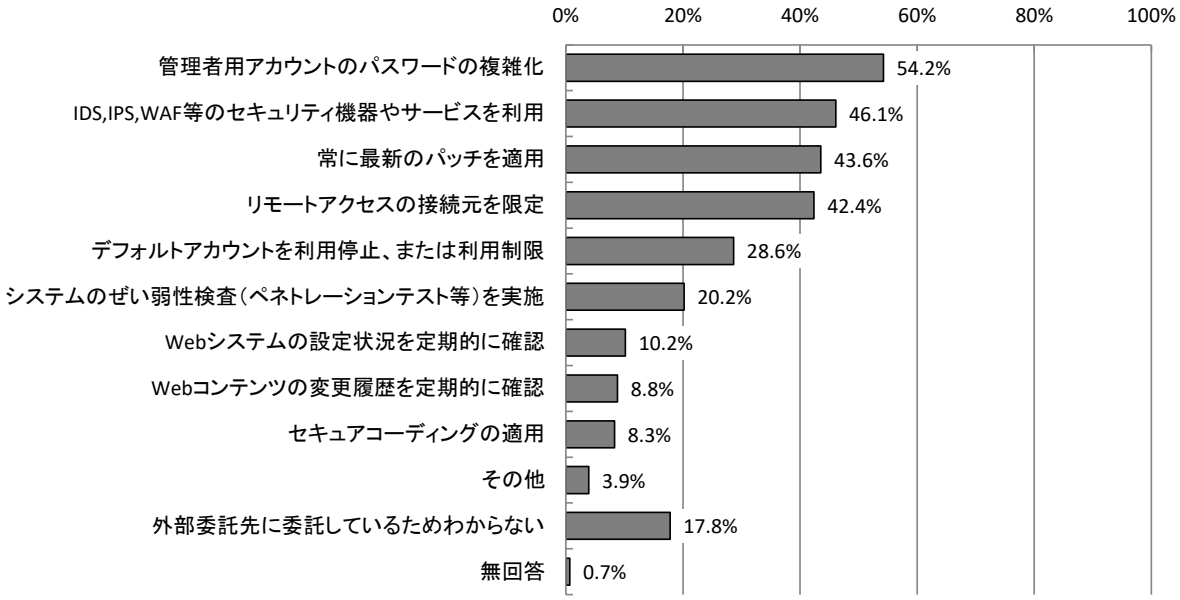


3.2.12 各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）のセキュリティ対策【問26-2】

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54.2%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46.1%、「常に最新のパッチを適用」が43.6%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。

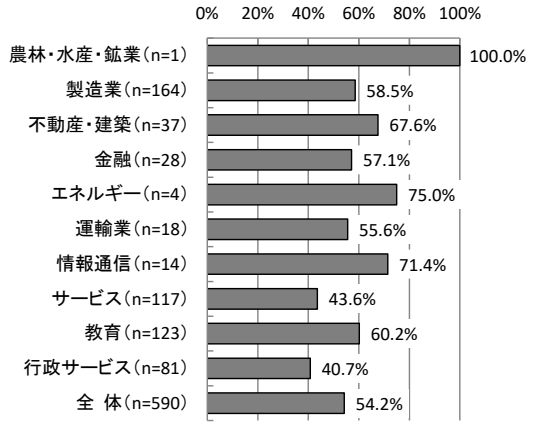
【全体】各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）のセキュリティ対策（MA,n=590）



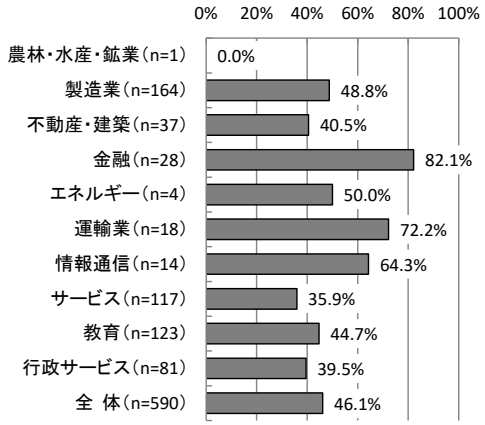
【業種別分析】業種別に見ると、「管理者用アカウントのパスワードの複雑化」については、「情報通信」が71.4%、「不動産・建築」が67.6%、「教育」が60.2%で高くなっている。「IDS,IPS,WAF等のセキュリティ機器やサービスを利用」については、「金融」が82.1%で高くなっている。

【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

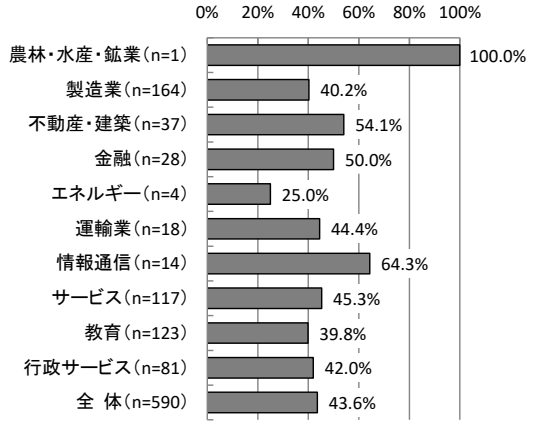
管理者用アカウントのパスワードの複雑化



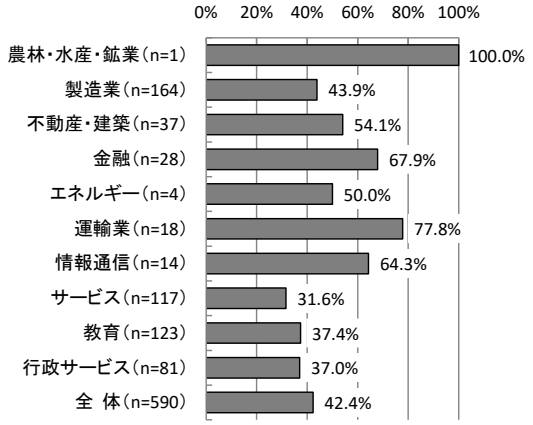
IDS,IPS,WAF等のセキュリティ機器やサービスを利用



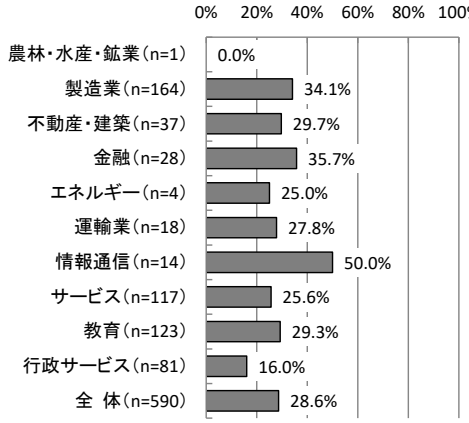
常に最新のパッチを適用



リモートアクセスの接続元を限定



デフォルトアカウントを利用停止、または利用制限

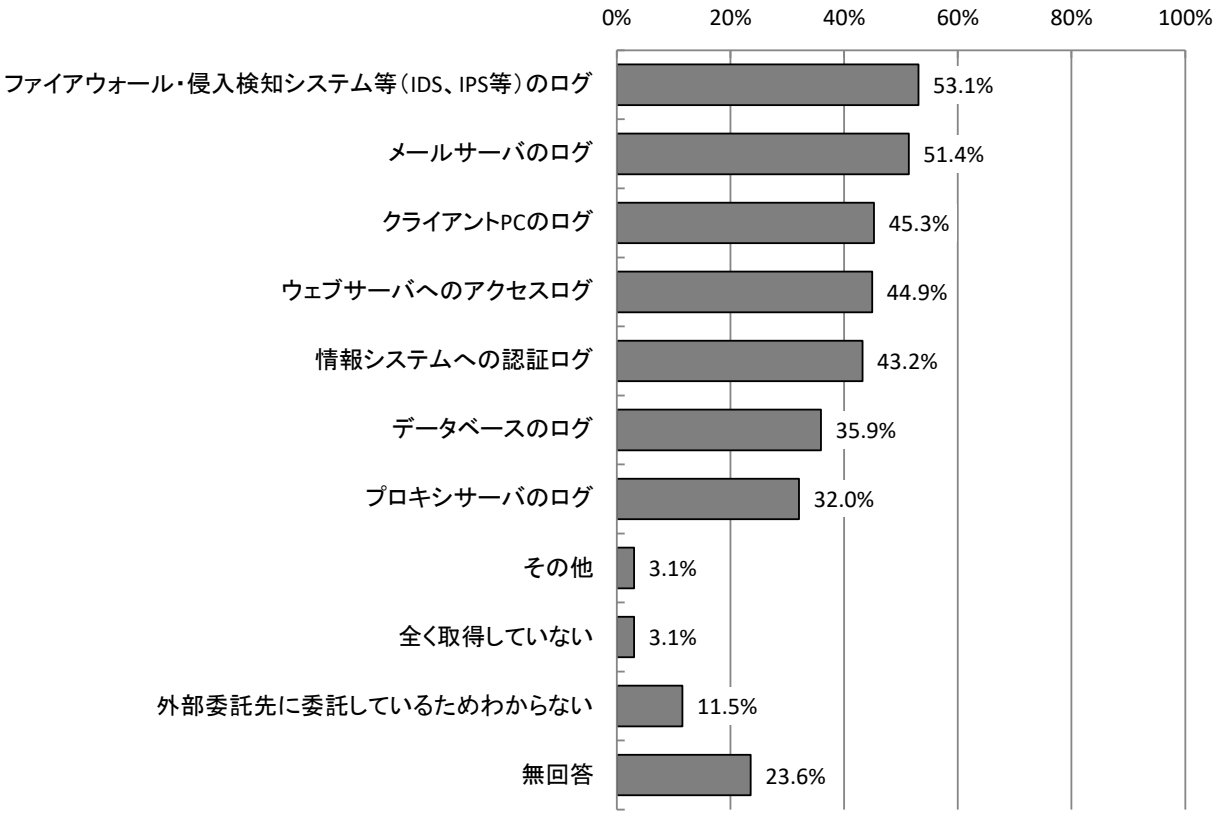


3.2.13　ログの取得状況　【問26-3】

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」が53.1%で最も高く、「メールサーバのログ」が51.4%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。

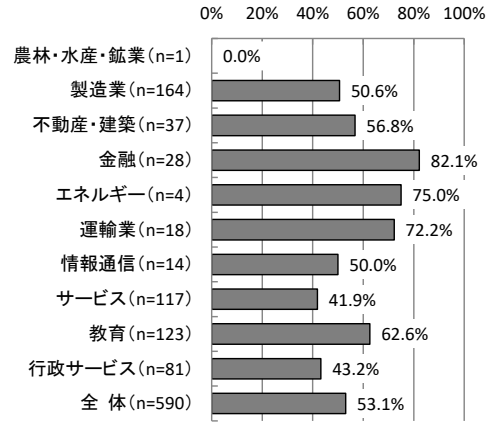
【全体】ログの取得状況（MA, n=590）



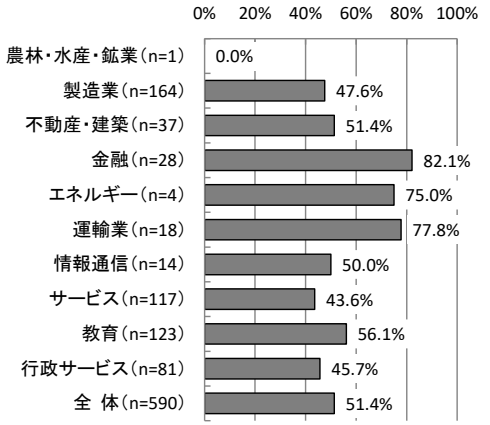
【業種別分析】業種別にみると、「ファイアウォール・侵入検知システム等（IDS、IPS等）のログ」では、「金融」が82.1%、「運輸業」が72.2%で高い。「メールサーバのログ」では「金融」が82.1%、「運輸業」が77.8%で高くなっている。

【業種別分析】ログの取得状況

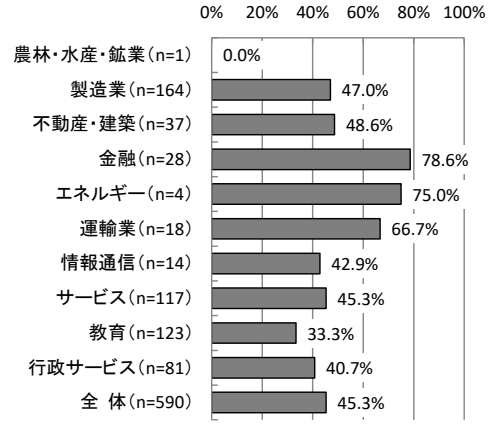
ファイアウォール・侵入検知システム等（IDS、IPS等）のログ



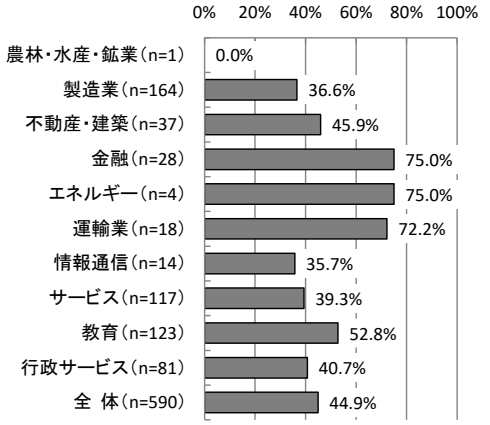
メールサーバのログ



クライアントPCのログ



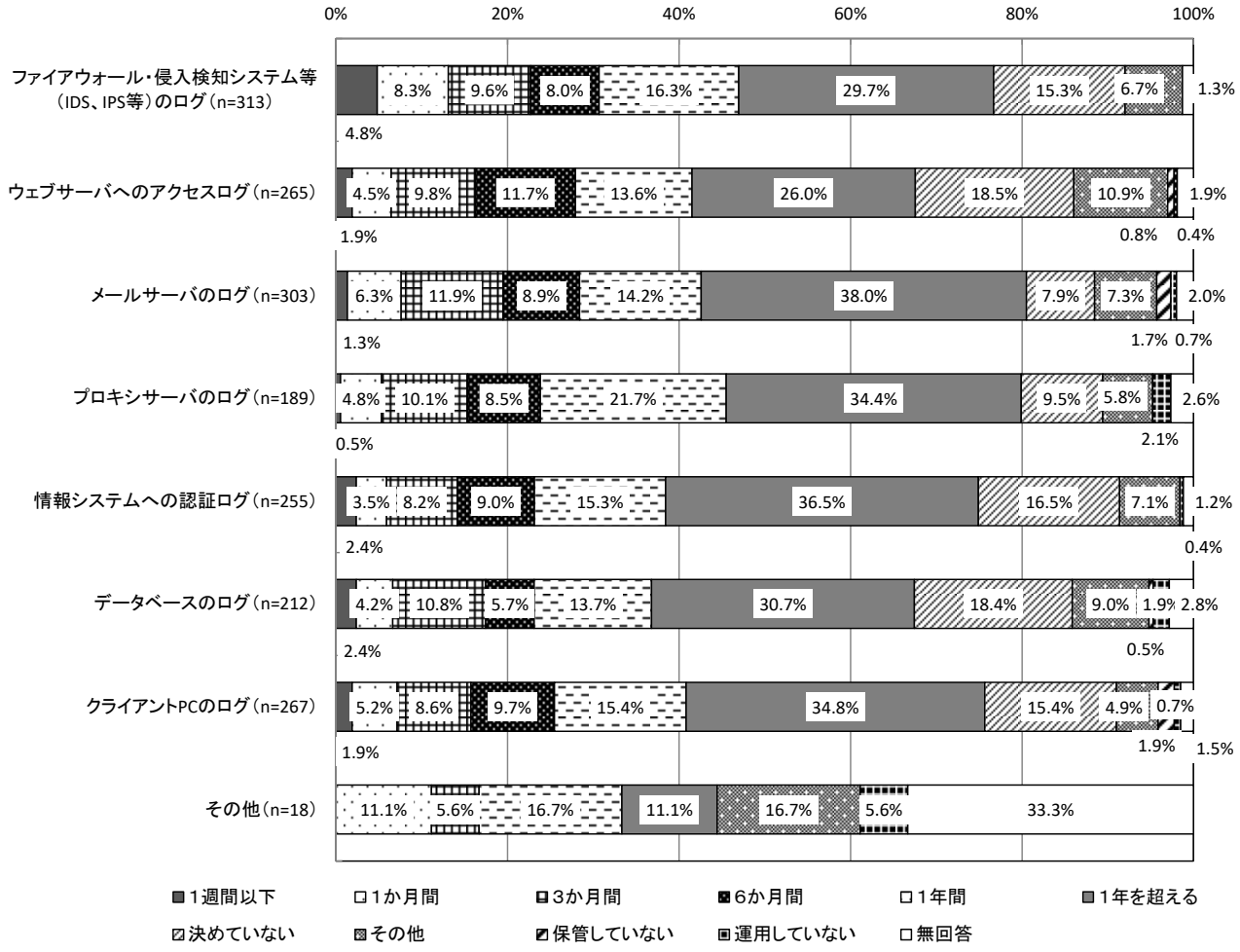
ウェブサーバへのアクセスログ



3.2.14　ログの保管期間　【問26-3A】

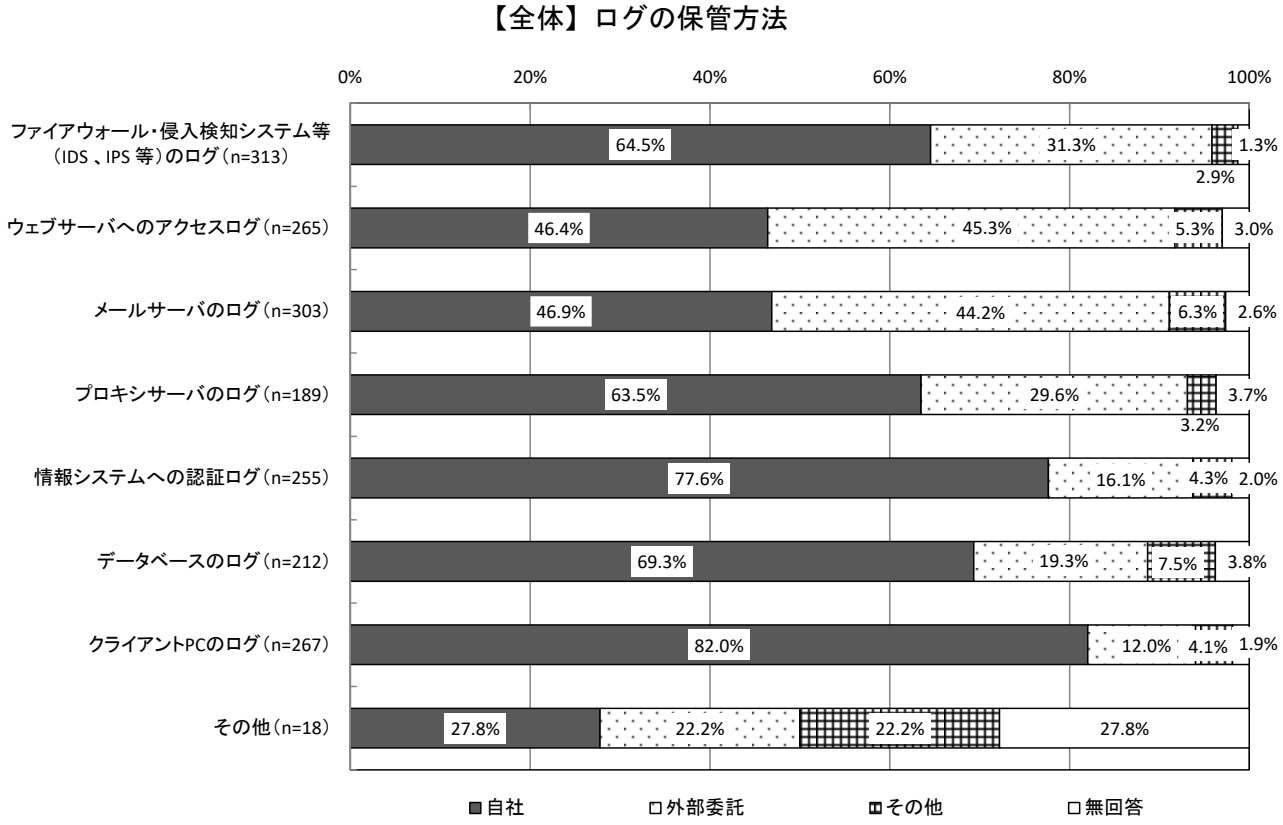
ログの保管期間については、「その他」を除くすべての項目で「１年を超える」が最も高い割合となっている。

【全体】ログの保管期間



3.2.15　ログの保管方法　【問26-3-B】

ログの保管方法については、すべての項目で「自社」が最も高い割合となっている。

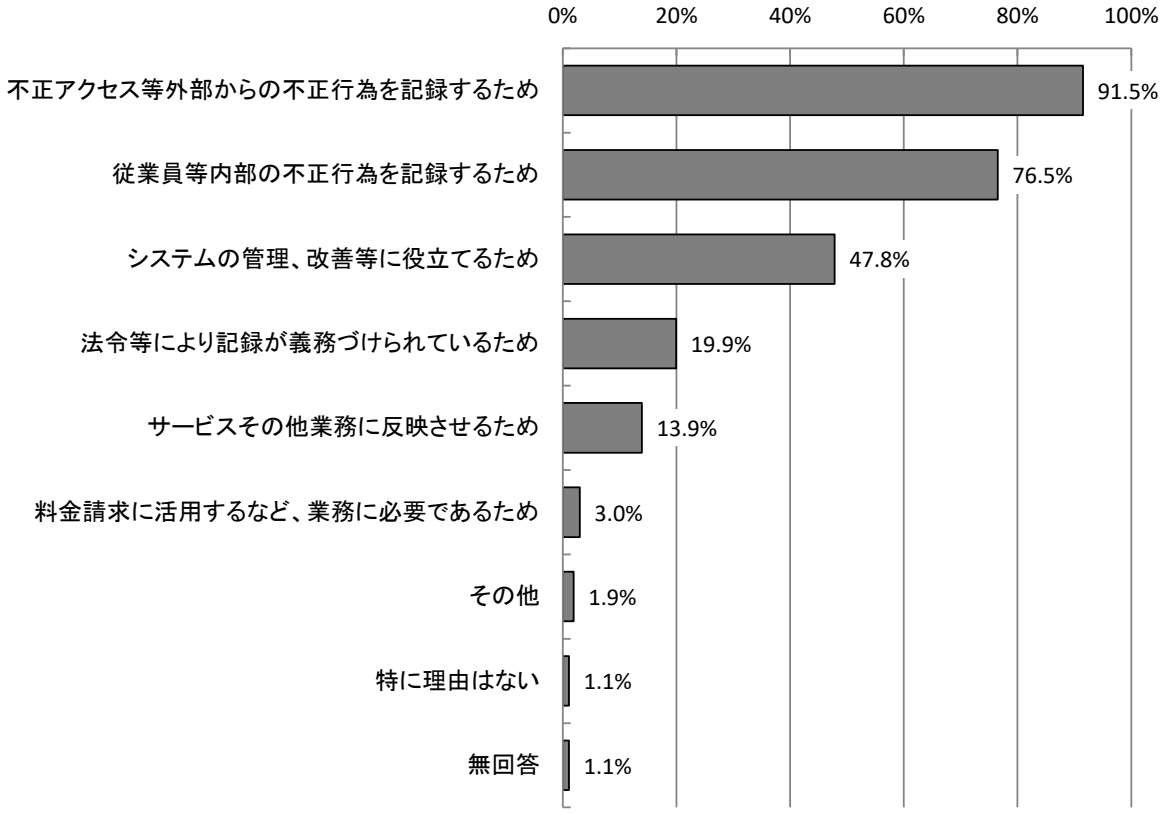


3.2.16　ログを取得・保管している理由　【問26-4】

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91.5%と最も高く、次いで「従業員等内部の不正行為を記録するため」が76.5%、「システムの管理、改善等に役立てるため」が47.8%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。

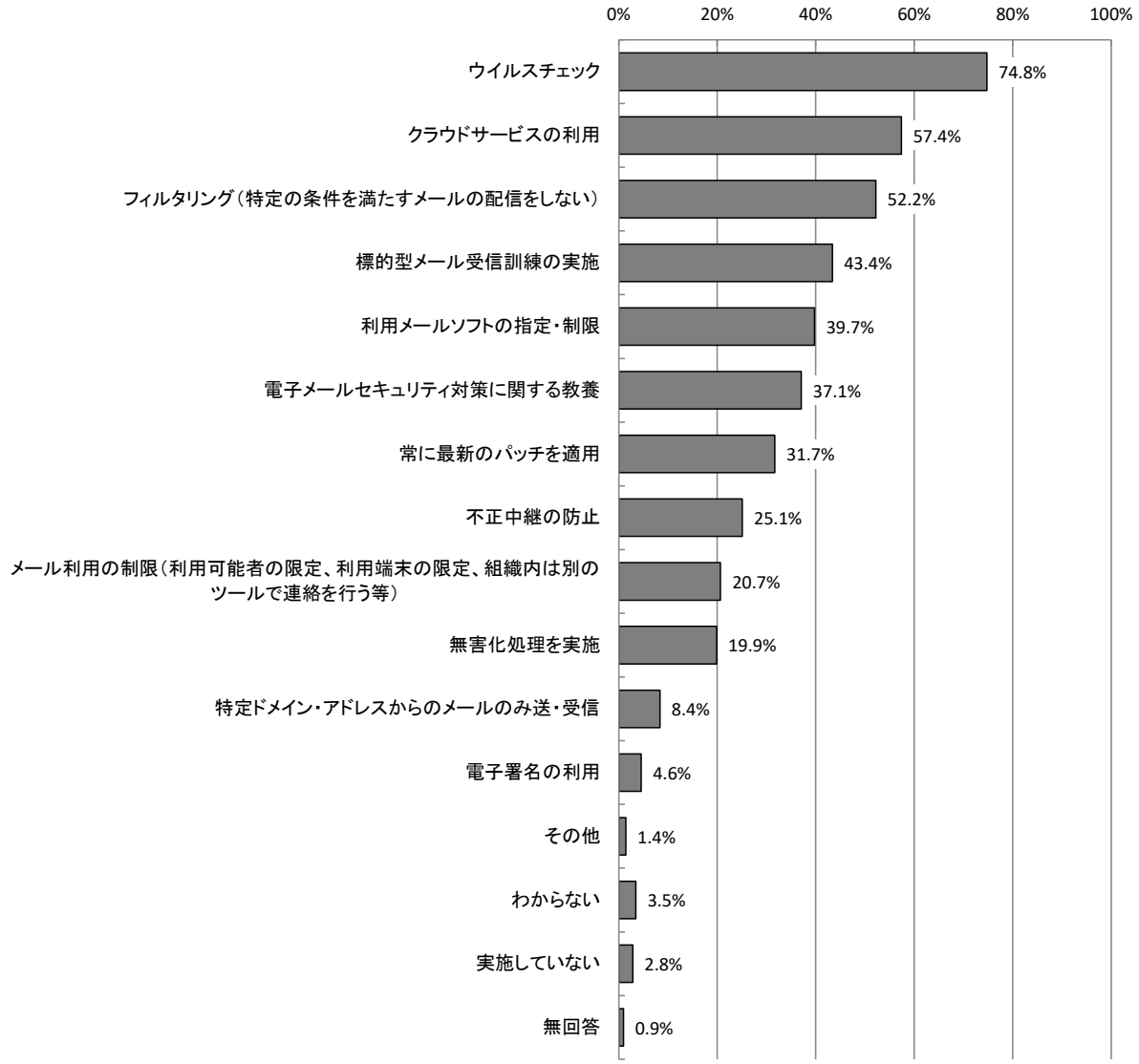
【全体】ログを取得・保管している理由（MA,n=366）



3.2.17　電子メールに関するセキュリティ対策　【問27】

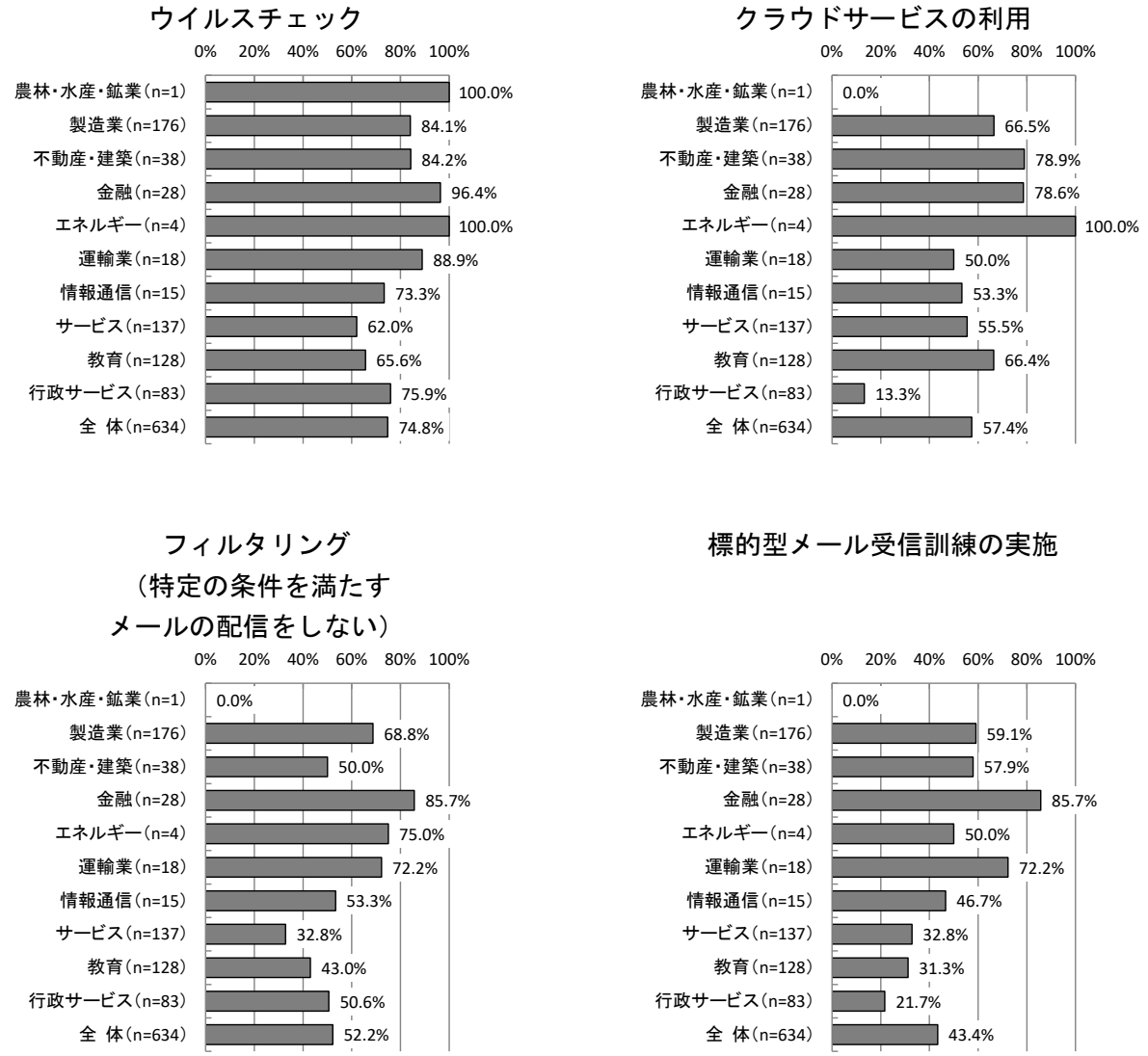
電子メールに関するセキュリティ対策については、「ウイルスチェック」が74.8%で最も高く、次いで「クラウドサービスの利用」が57.4%、「フィルタリング（特定の条件を満たすメールの配信をしない）」が52.2%となっている。

【全体】電子メールに関するセキュリティ対策（MA,n=634）



【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、次いで「運輸業」が88.9%と高くなっている。「クラウドサービスの利用」については「不動産・建築」が78.9%、「金融」が78.6%、「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）」については「金融」が85.7%と高くなっている。

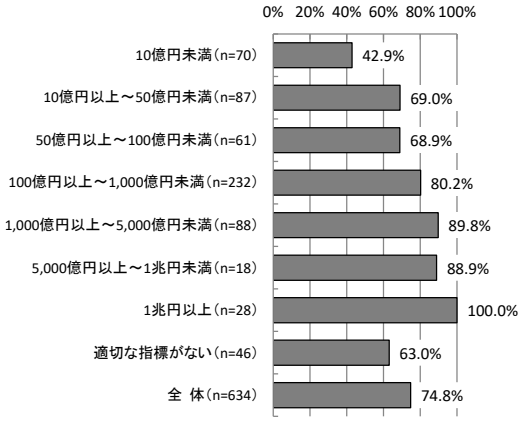
【業種別分析】電子メールに関するセキュリティ対策



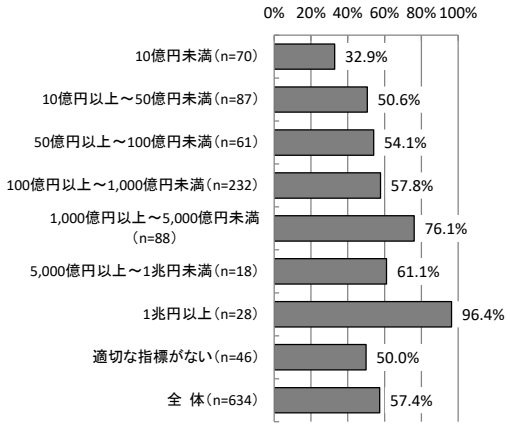
【予算規模別分析】予算規模別にみると、「ウイルスチェック」については、「1兆円以上」が100.0％で最も高く、次いで「1,000億円以上～5,000億円未満」が89.8％、「5,000億円以上～1兆円未満」が88.9％となっている。「クラウドサービスの利用」についても「1兆円以上」が96.4％で最も高い。

【予算規模別分析】電子メールに関するセキュリティ対策

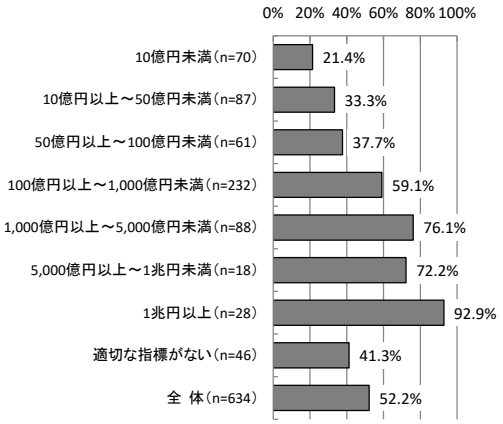
ウイルスチェック



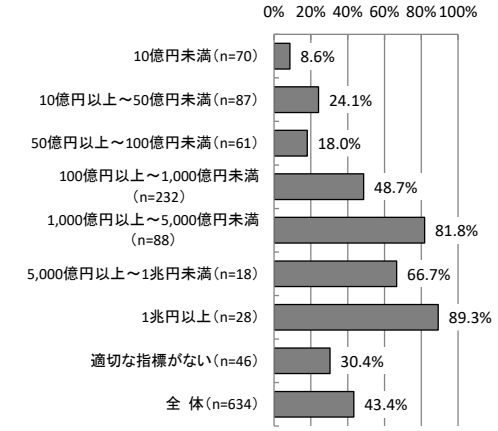
クラウドサービスの利用



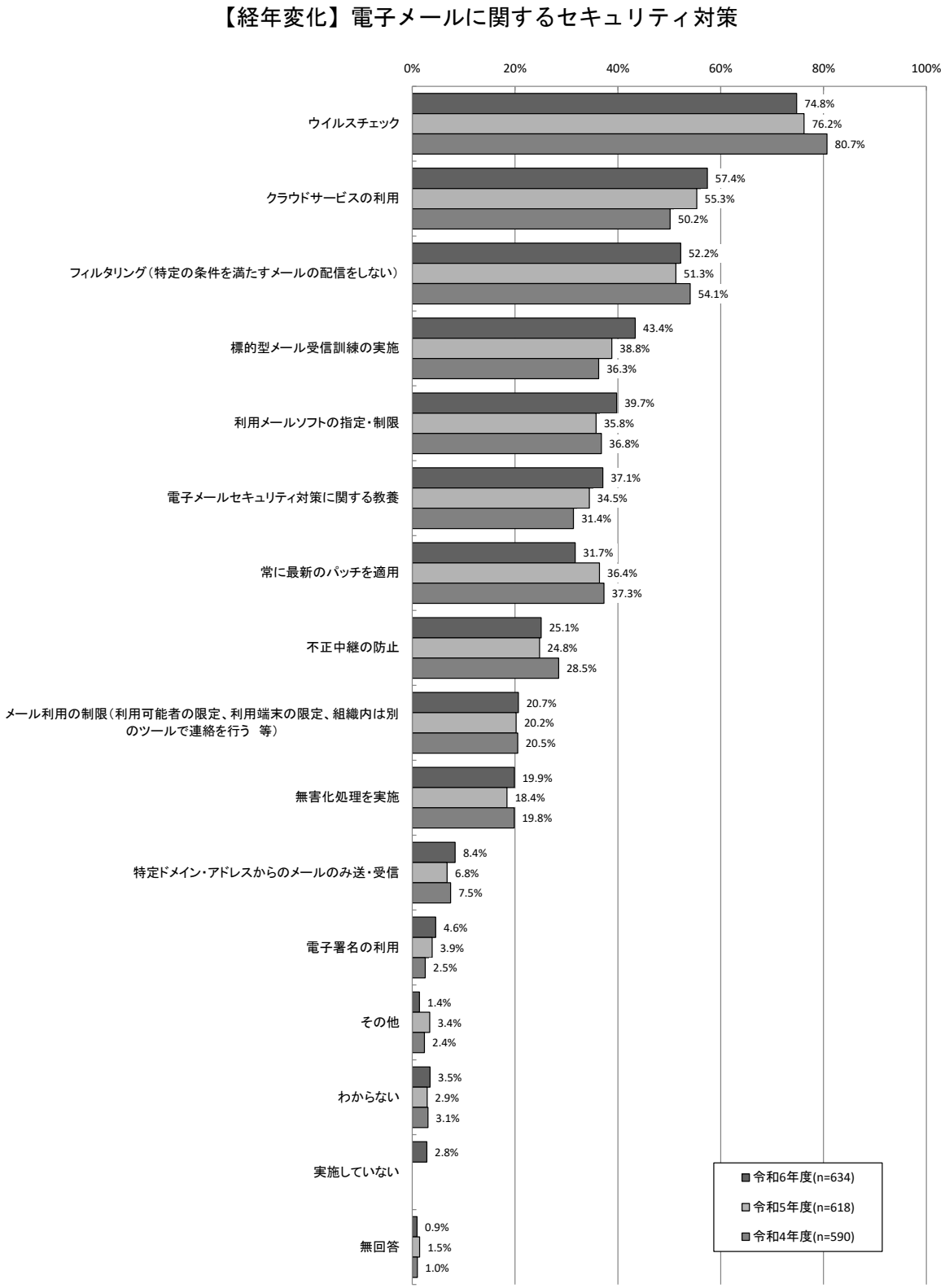
フィルタリング
（特定の条件を満たす
メールの配信をしない）



標的型メール受信訓練の実施



【経年変化】昨年度と比較すると、「常に最新のパッチを適用」が4.7ポイント減少している。一方、「標的型メール受信訓練の実施」が4.6ポイント増加している。

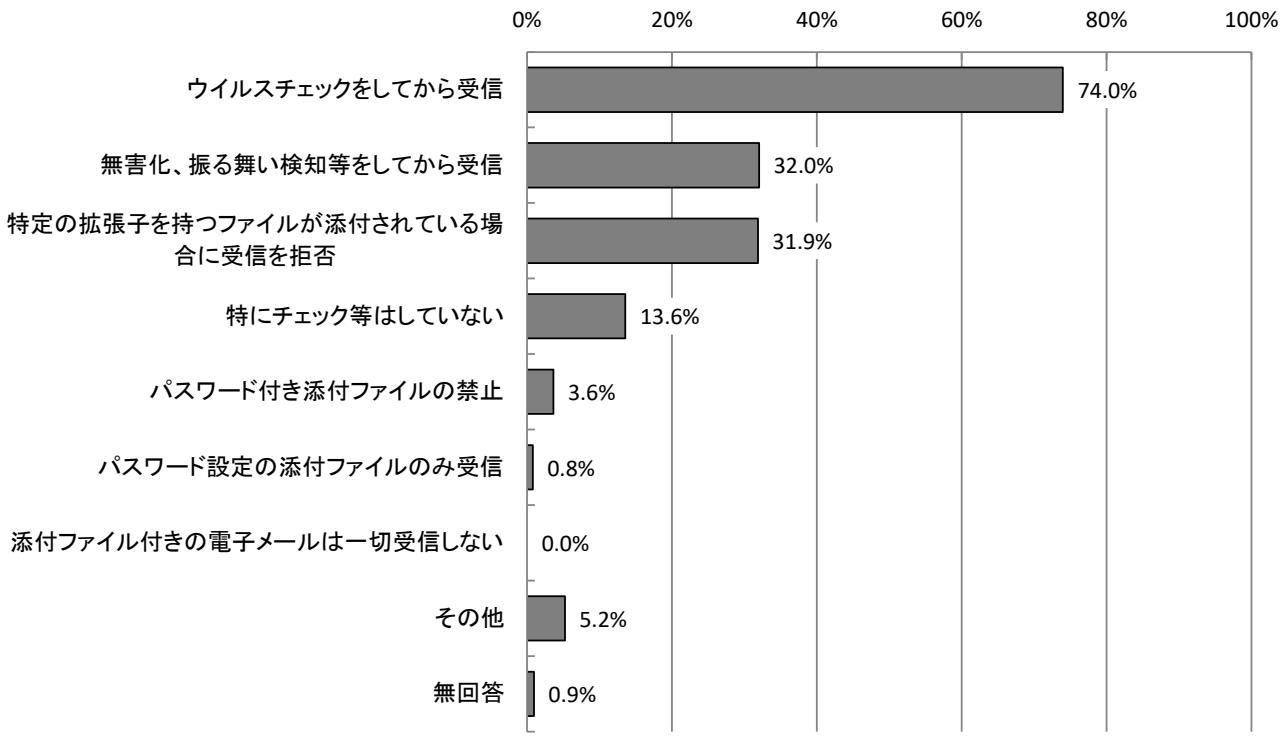


※令和６年度調査で「実施していない」を新設

3.2.18　添付ファイルの取り扱い　【問28】

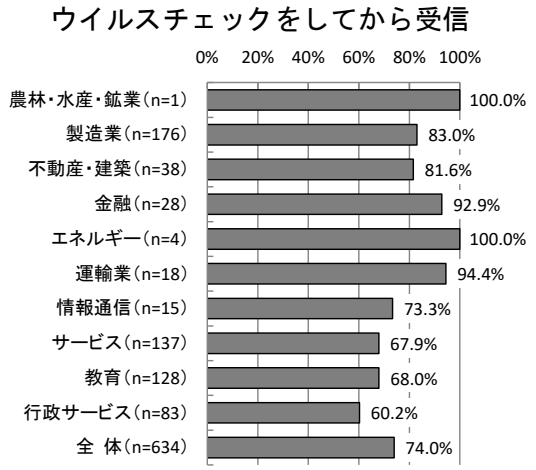
添付ファイルの取り扱いについては、「ウイルスチェックをしてから受信」が74.0%で最も高い。一方、「特にチェック等はしていない」は13.6%であった。

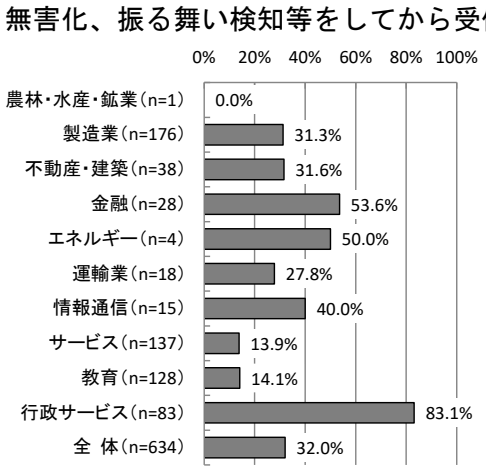
【全体】添付ファイルの取り扱い（MA,n=634）



【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「運輸業」で 94.4%、「金融」で 92.9%となっている。「無害化、振る舞い検知等をしてから受信」は「行政サービス」で 83.1%となっている。

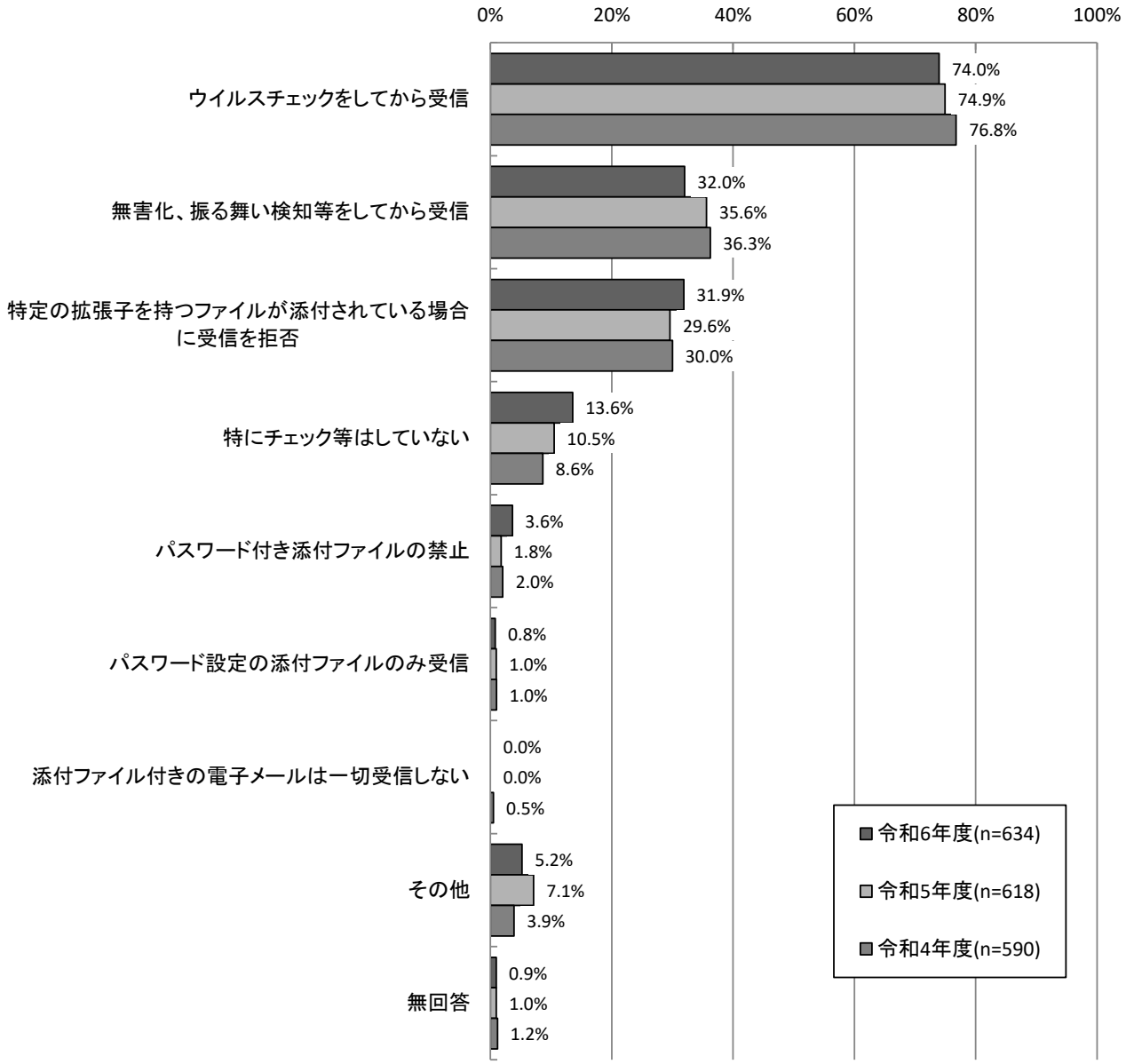
【業種別分析】添付ファイルの取り扱い





【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3.6ポイント減少し、「特にチェック等はしていない」が3.1ポイント増加している。

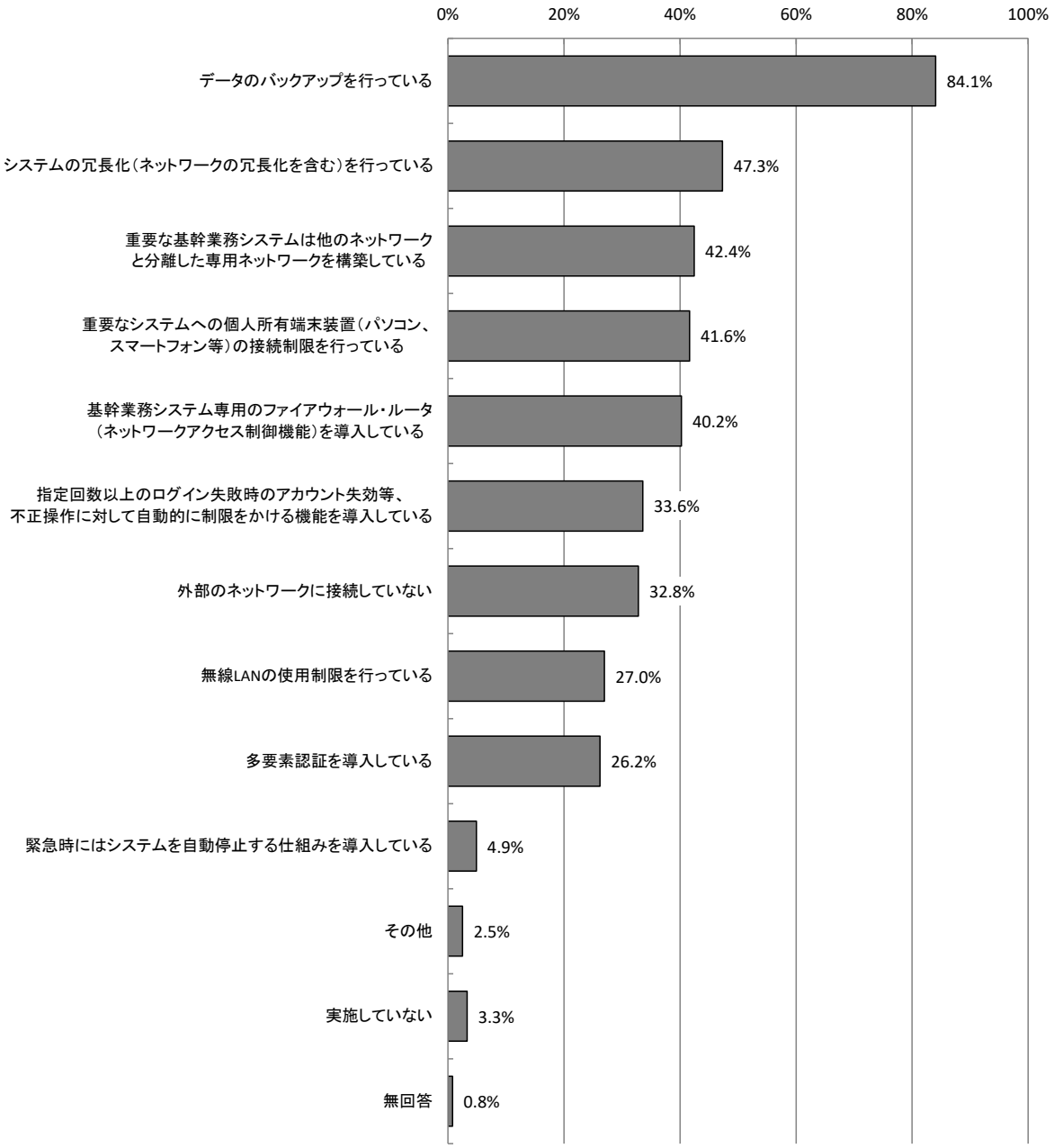
【経年変化】添付ファイルの取り扱い



3.2.19　重要システムの不正アクセス対策状況　【問29】

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84.1%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47.3%、「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42.4%、「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41.6%、「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」が40.2%となっている。

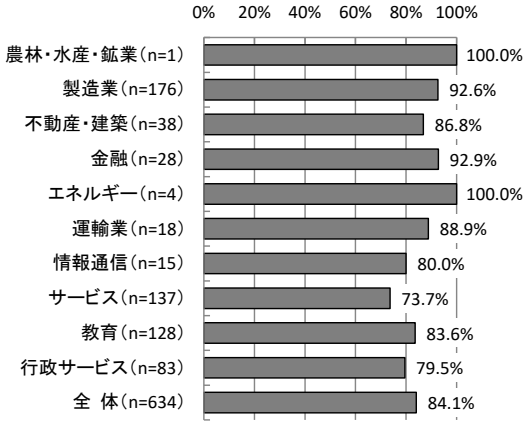
【全体】重要システムの不正アクセス対策状況（MA,n=634）



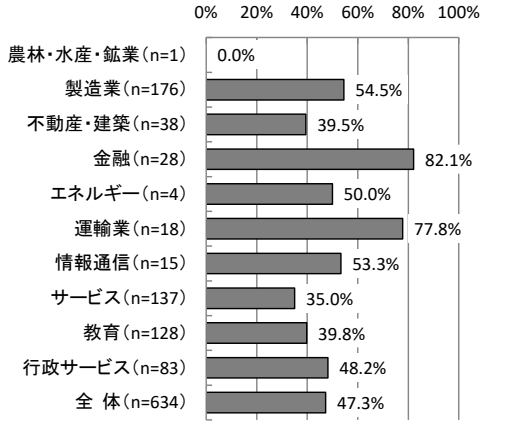
【業種別分析】業種別にみると、「データのバックアップを行っている」については、「金融」が92.9%、「製造業」が92.6%で高くなっている。「システムの冗長化（ネットワークの冗長化を含む）を行っている」については、「金融」が82.1%、「運輸業」が77.8%で高くなっている。

【業種別分析】重要システムの不正アクセス対策状況

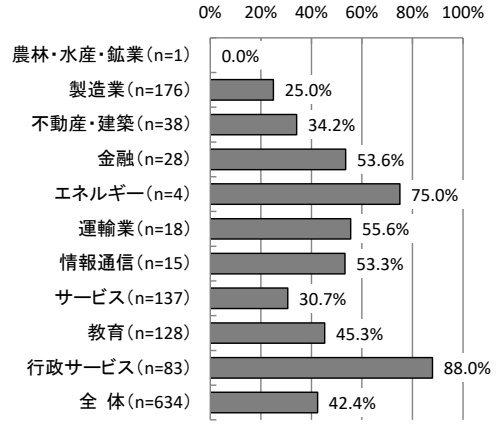
データのバックアップを行っている



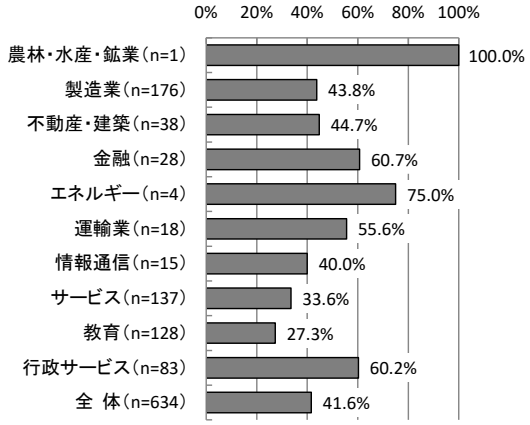
システムの冗長化（ネットワークの冗長化を含む）を行っている



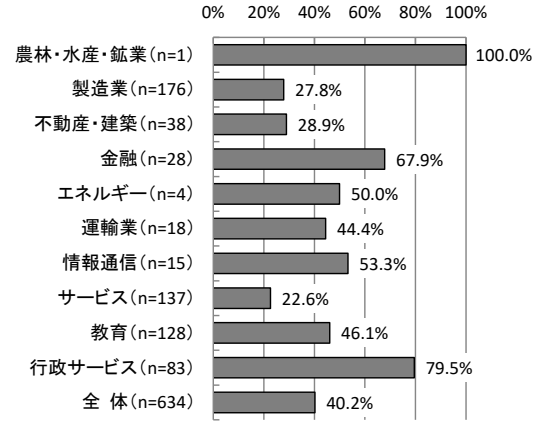
重要な基幹業務システムは他のネットワークと分離した専用ネットワークを構築している



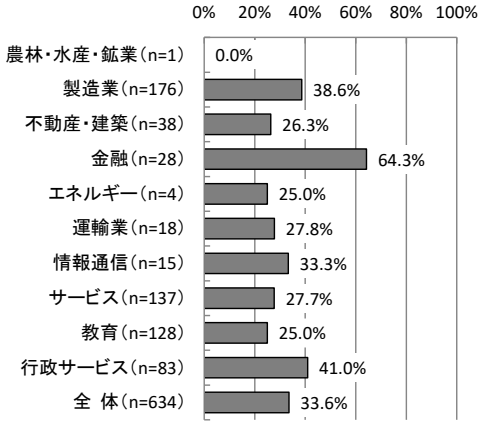
重要なシステムへの個人所有端末装置（パソコン、スマートフォン等）の接続制限を行っている



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

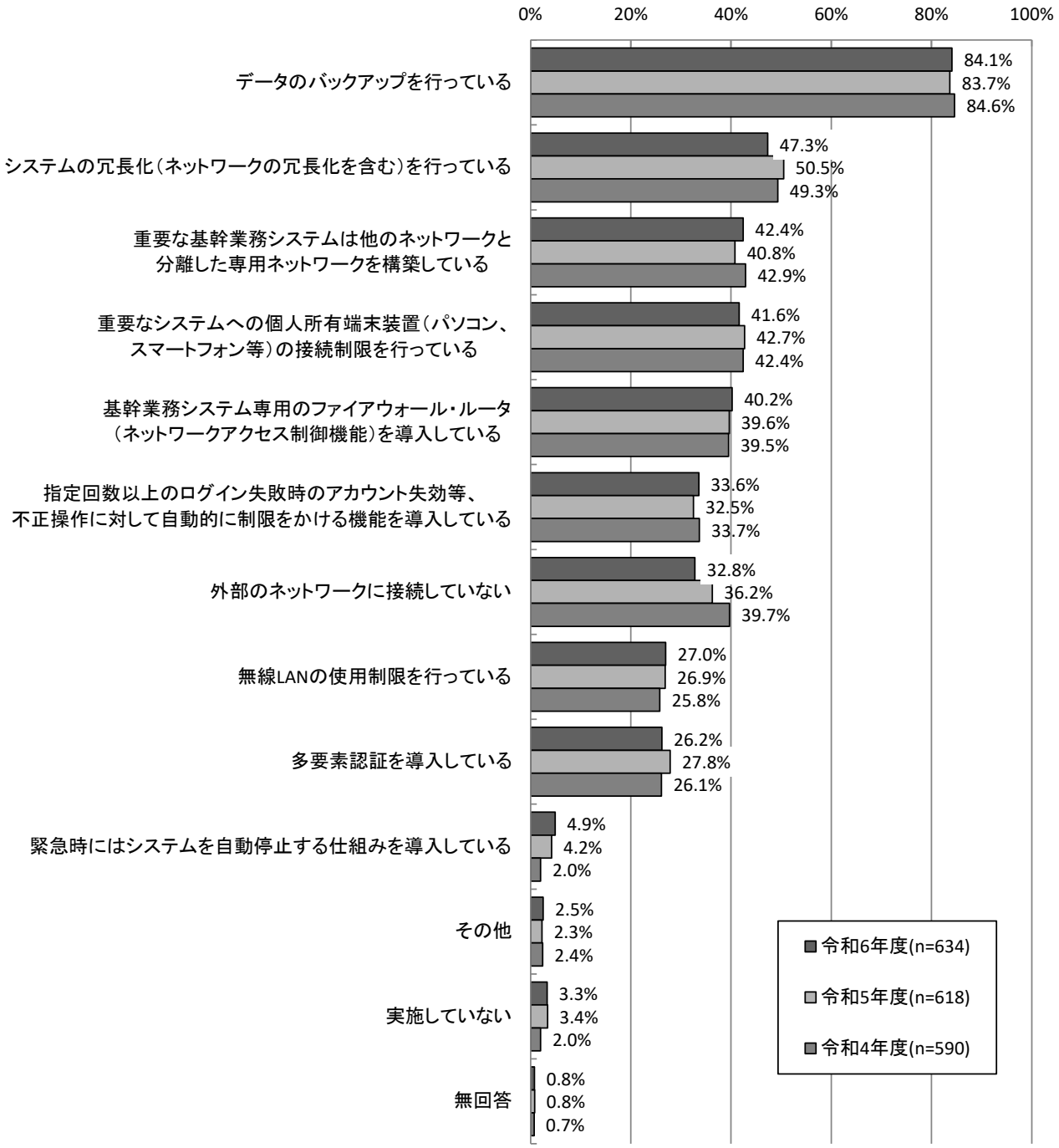


指定回数以上のログイン失敗時のアカウント失効等、不正操作に対して自動的に制限をかける機能を導入している



【経年変化】昨年度と比較すると、「外部のネットワークに接続していない」が 3.4 ポイント、「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 3.2 ポイント減少している。

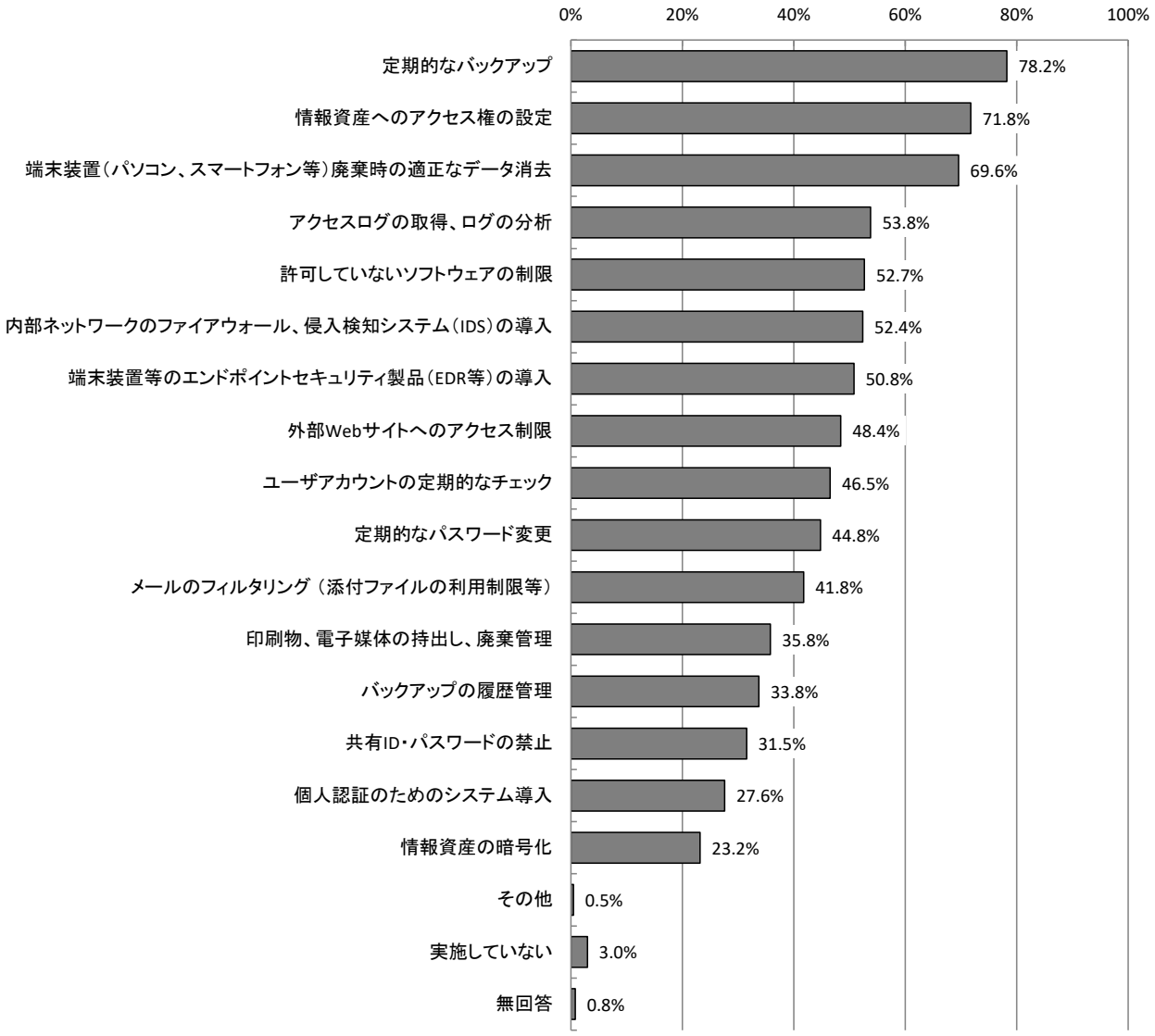
【経年変化】重要システムの不正アクセス対策状況



3.2.20　不正アクセス等への対策状況　【問30】

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78.2%で最も高く、次いで「情報資産へのアクセス権の設定」が71.8%、「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69.6%となっている。

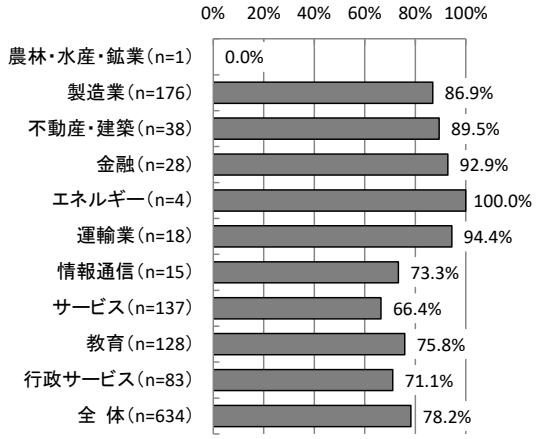
【全体】不正アクセス等への対策状況（MA, n=634）



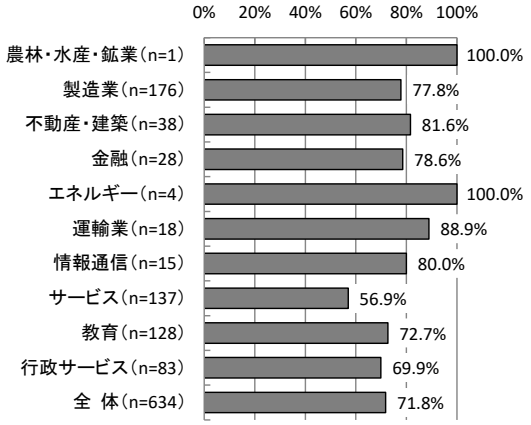
【業種別分析】業種別にみると、「定期的なバックアップ」は「運輸業」が94.4%、「金融」が92.9%で高く、「不動産・建築」「製造業」で80%以上となっている。「情情報資産へのアクセス権の設定」は「運輸業」が88.9%、「不動産・建築」が81.6%、「情報通信」が80.0%で高くなっている。

【業種別分析】不正アクセス等への対策状況

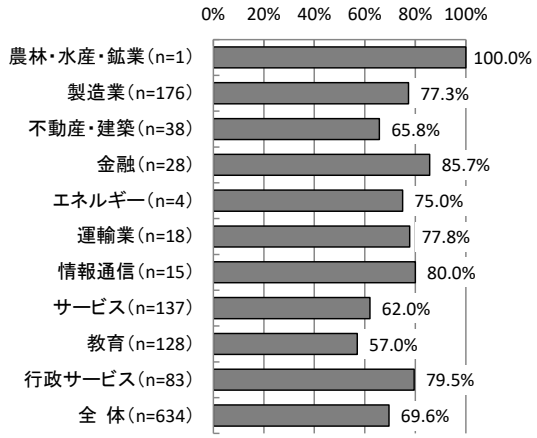
定期的なバックアップ



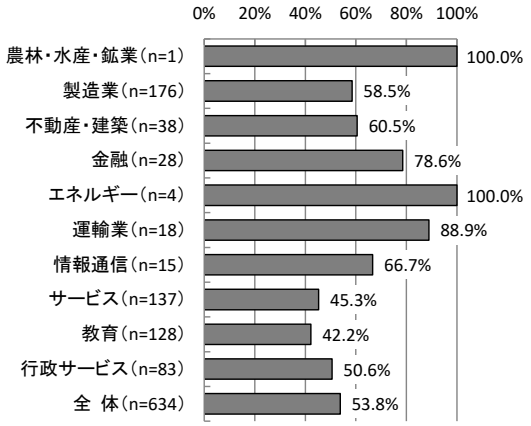
情報資産へのアクセス権の設定



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

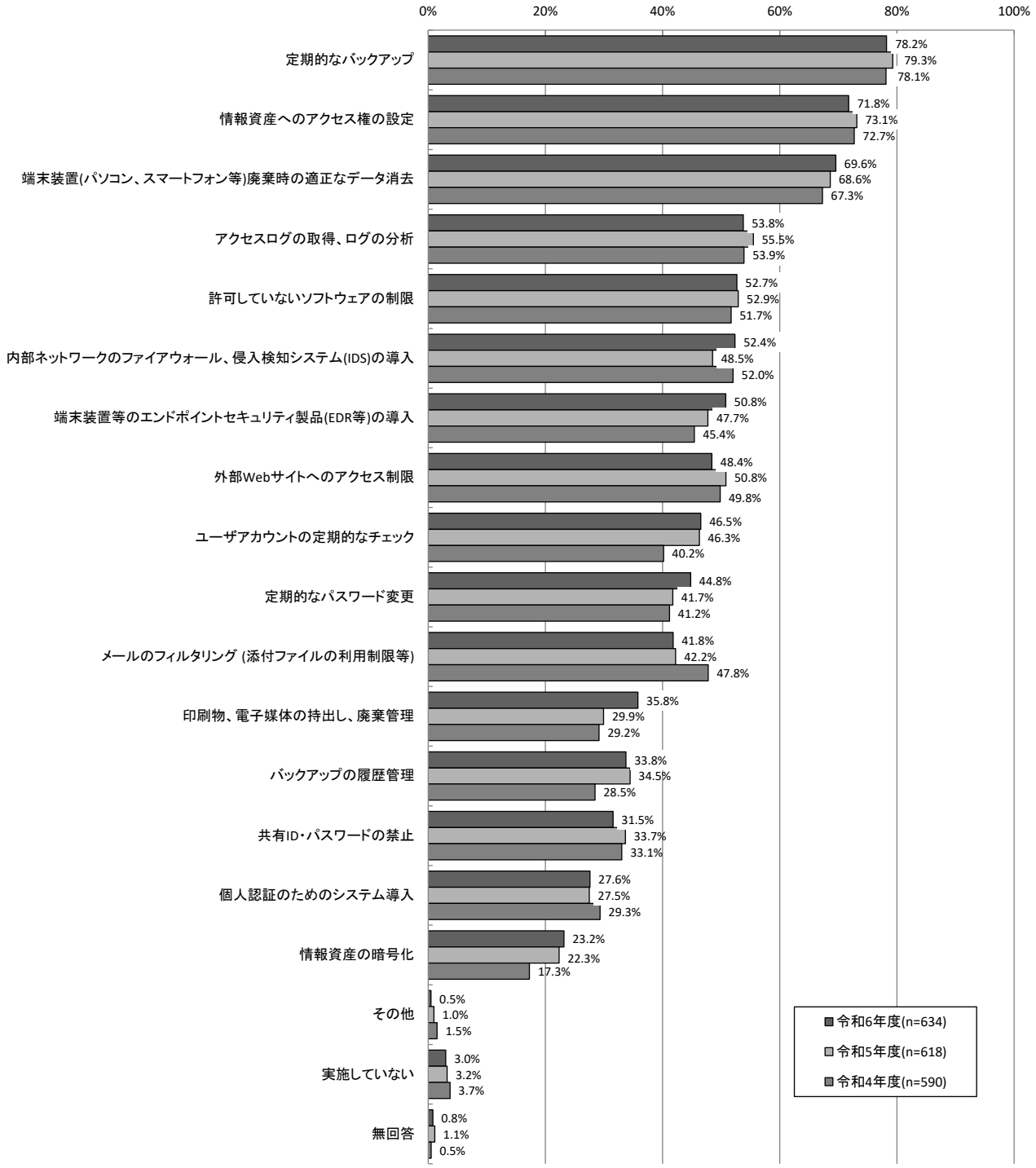


アクセスログの取得、ログの分析



【経年変化】昨年度と比較すると、「印刷物、電子媒体の持出し、廃棄管理」が 5.9 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 3.9 ポイント、「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」「定期的なパスワード変更」が 3.1 ポイント増加している。

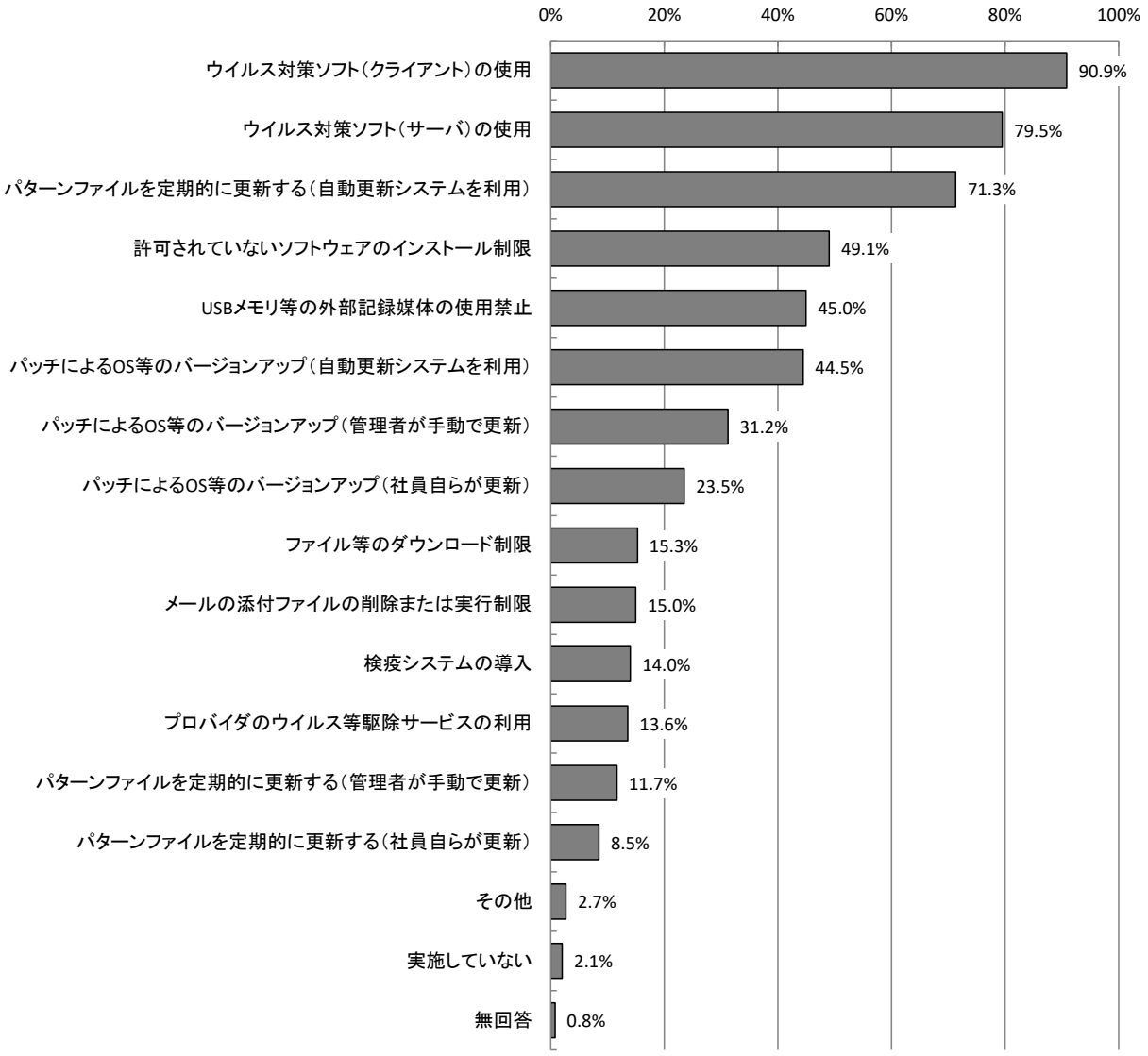
【経年変化】不正アクセス等への対策状況



3.2.21　不正プログラムへの対策状況　【問31】

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90.9%で最も高く、次いで「ウイルス対策ソフト（サーバ）の使用」が79.5%、「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71.3%となっている。

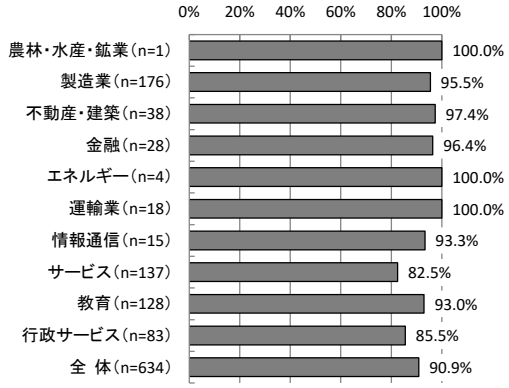
【全体】不正プログラムへの対策状況（MA, n=634）



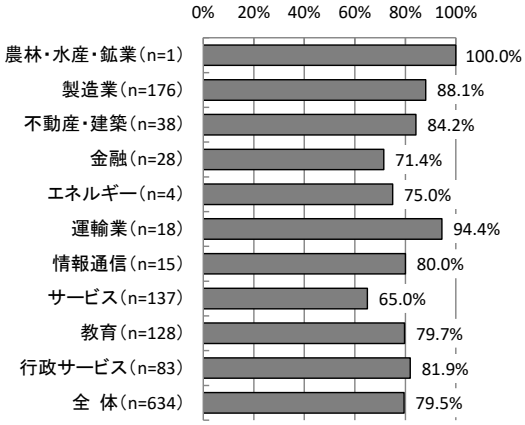
【業種別分析】業種別にみると、「ウイルス対策ソフト（クライアント）の使用」については、すべての業種で80%以上と高くなっている。「ウイルス対策ソフト（サーバ）の使用」については、「運輸業」が94.4%、「製造業」が88.1%で高くなっている。

【業種別分析】不正プログラムへの対策状況

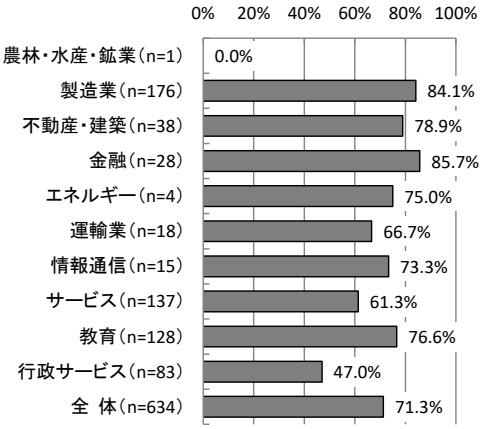
ウイルス対策ソフト（クライアント）の使用



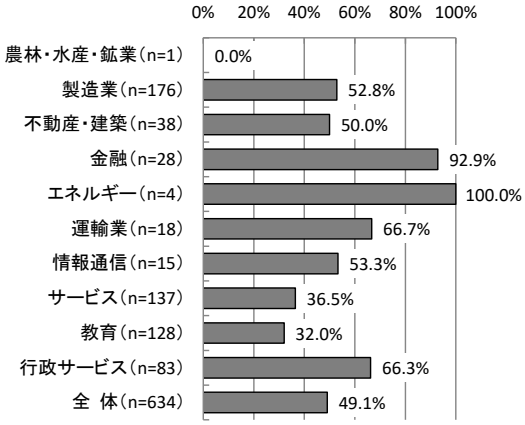
ウイルス対策ソフト（サーバ）の使用



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）



許可されていないソフトウェアのインストール制限

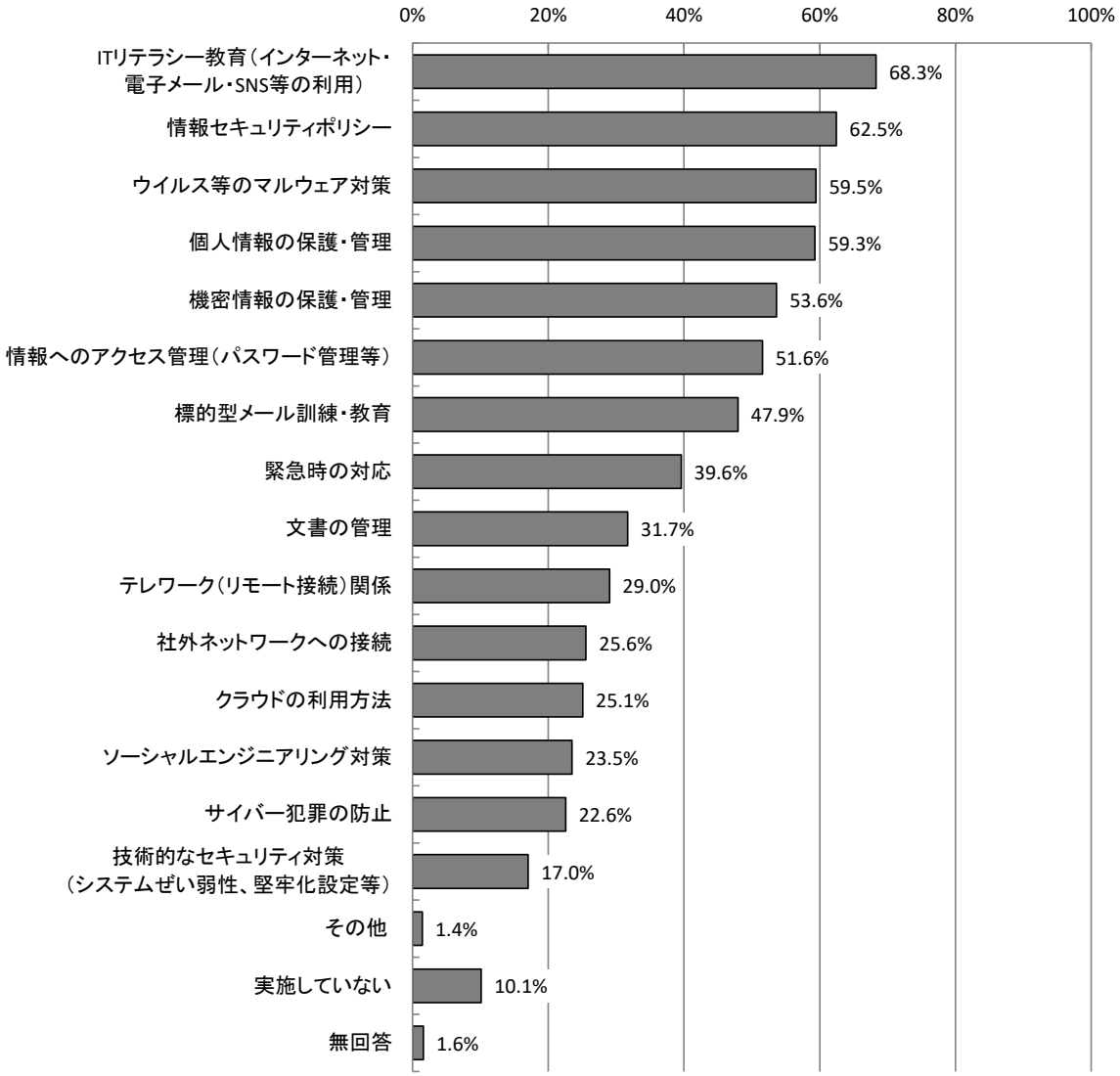


3.3 人的対策

3.3.1 情報セキュリティ教育の内容 【問32】

情報セキュリティ教育の内容については、「ITリテラシー教育（インターネット・電子メール・SNS等の利用）」が68.3%、「情報セキュリティポリシー」が62.5%で高くなっている。

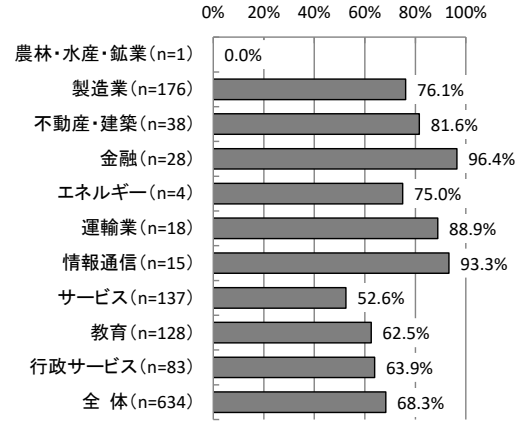
【全体】情報セキュリティ教育の内容（MA, n=634）



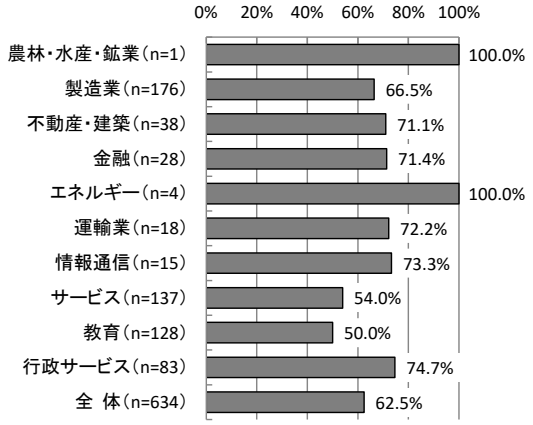
【業種別分析】業種別にみると、「ITリテラシー教育(インターネット・電子メール・SNS等の利用)」は、「金融」が96.4%、「情報通信」が93.3%と高くなっている。「情報セキュリティポリシー」は「行政サービス」が74.7%、「情報通信」が73.3%、「運輸業」が72.2%で高い。「ウイルス等のマルウェア対策」は「金融」が85.7%、「運輸業」が72.2%で高くなっている。

【業種別分析】情報セキュリティ教育の内容

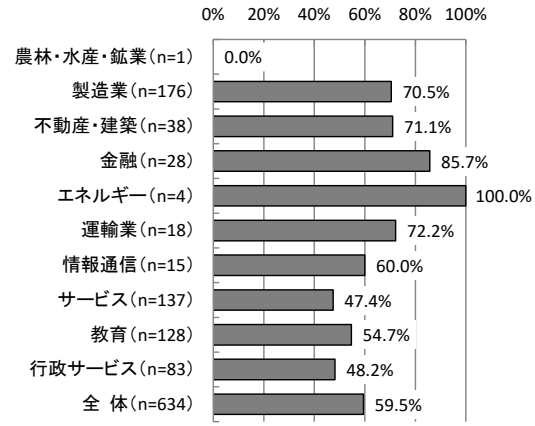
ITリテラシー教育（インターネット・電子メール・SNS等の利用）



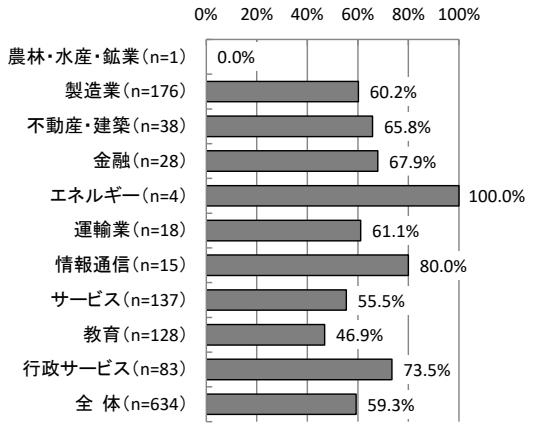
情報セキュリティポリシー



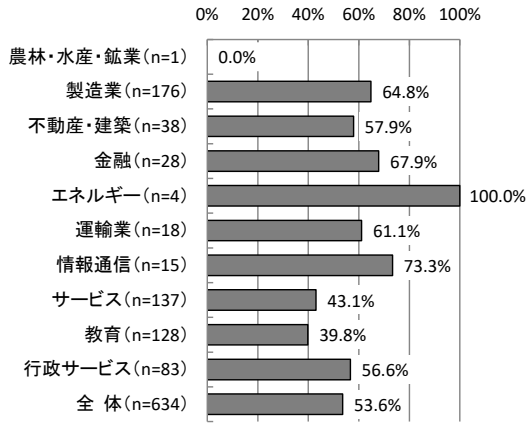
ウイルス等のマルウェア対策



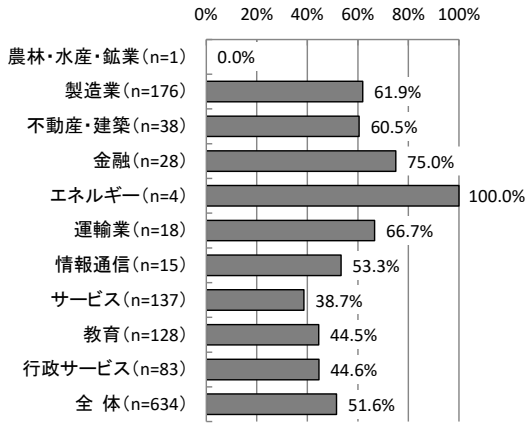
個人情報の保護・管理



機密情報の保護・管理



情報へのアクセス管理
（パスワード管理等）

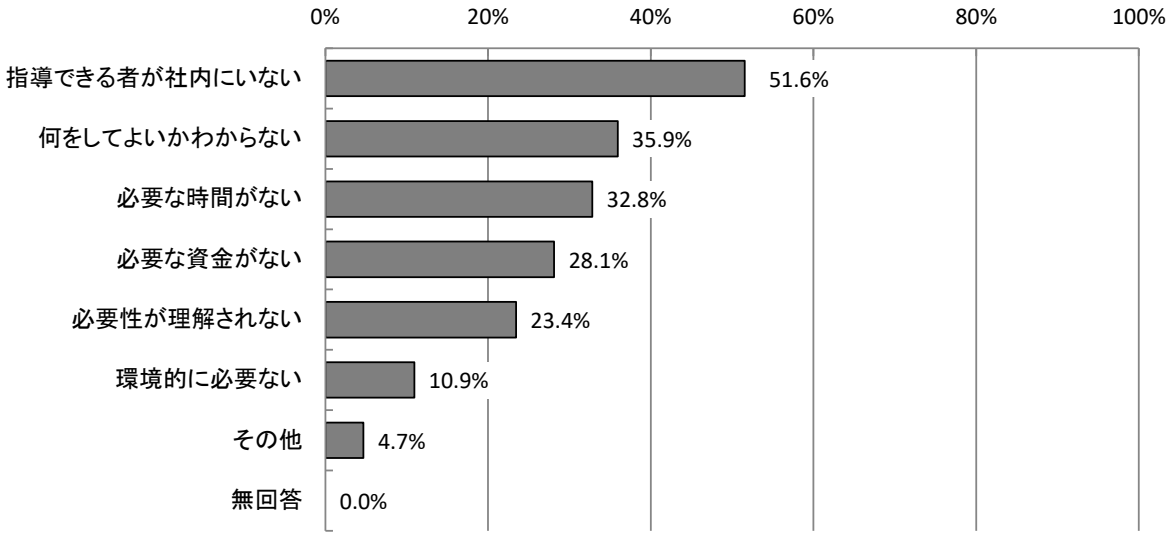


3.3.2　情報セキュリティ教育を実施しない理由　【問32-1】

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51.6%で最も高く、次いで「何をしてよいかわからない」が35.9%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。

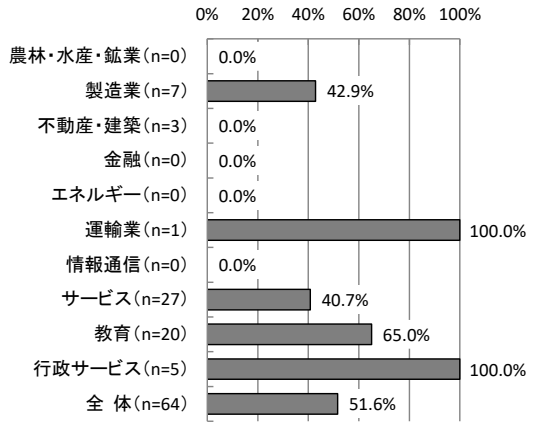
【全体】情報セキュリティ教育を実施しない理由（MA, n=64）



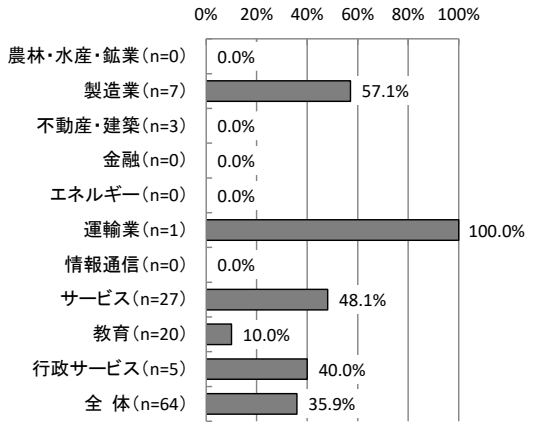
【業種別分析】業種別にみると、「指導できる者が社内にいない」は、「行政サービス」で100.0%、「何をしてよいかわからない」は、「製造業」で57.1%と高くなっている。

【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



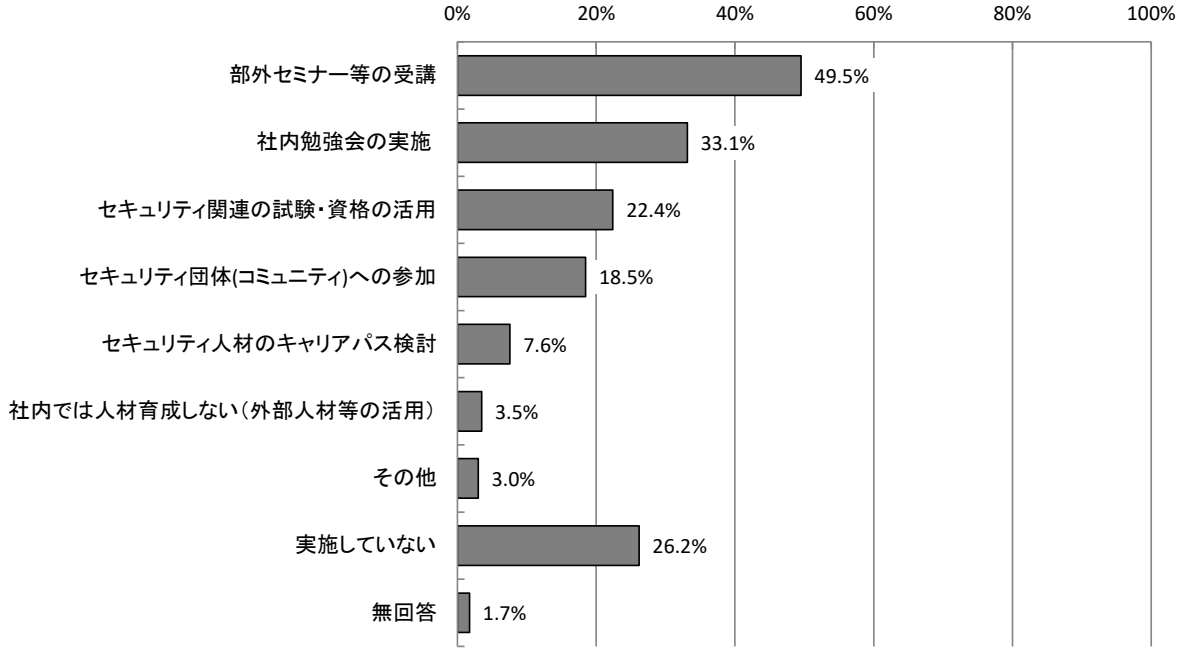
何をしてよいかわからない



3.3.3　セキュリティ人材を確保するための施策　【問33】

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49.5%で最も高く、次いで「社内勉強会の実施」が33.1%、「セキュリティ関連の試験・資格の活用」が22.4%となっている。

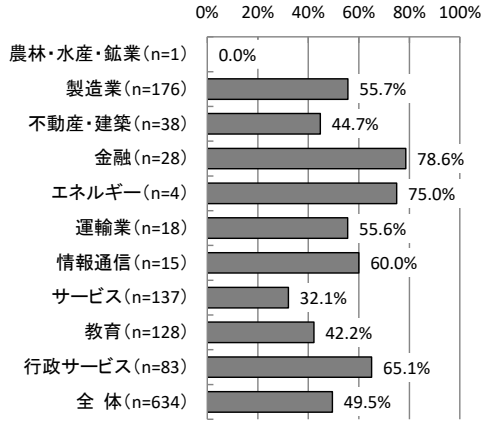
【全体】セキュリティ人材を確保するための施策（MA, n=634）



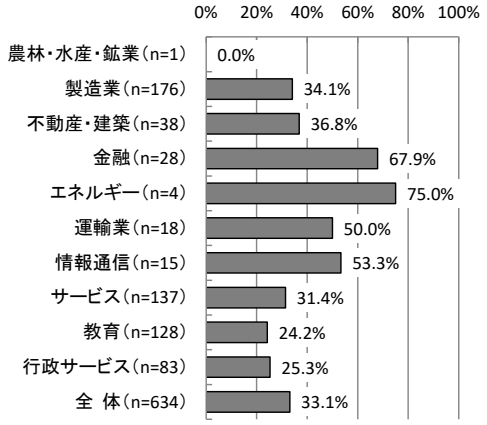
【業種別分析】業種別にみると、「部外セミナー等の受講」は、「金融」が78.6%、「行政サービス」が65.1%で高い。「社内勉強会の実施」の実施は、「金融」が67.9%、「情報通信」で53.3%、「運輸業」で50.0%と高くなっている。

【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



3.3.4　セキュリティ対策の問題点や不安等

- 人財確保・育成とコスト削減。
- 情報セキュリティ対策を実施しようとしても、職場の上層部が自分事として捉えていないため 担当させられたものが空回りする場合が多いと思われます。また、多少コンピュータが使える人間に任せようとするため、兼任になりがちです。そのため、対策を考える・行う時間が取れない事に対して不安はあります。
- 費用対効果の算出が難しいことや、セキュリティ人材が不足していることに対し困難を感じている。
- マンパワーが足りないため、外部委託以外で検討できない。
- 情報システムの人材が不足しており、細やかな対応を行っている時間がない。
- ランサムウェア攻撃などセキュリティ攻撃は後を絶たないが、自社の対策がそれらに対してどこまで有効に機能するのかが見えない。
- セキュリティ対策はどこまで実施したらよいのか、コストとセキュリティのバランスが悩ましい。
  EDR等製品の導入検討、ログ取得の範囲、ユーザー教育の実施、リスク分析や脆弱性診断の範囲・頻度、等。
  マイクロソフト製品を数多く利用しており、それらは毎月の最新パッチ適用が推奨されている。ところがパッチに不具合があると障害が発生し、業務に悪影響が出てしまう。パッチが安全に適用できるかの見極めたうえで適用したいが、ゼロデイ攻撃等のリスクを考えると適用のタイミングが難しい。
- 対策の優先度付けと企業業態や規模に応じた対策深度に試行錯誤している。
- セキュリティ関連投資は効果が見えにくいことから、経営層にとってはコストとして認識されやすく予算取得しずらいことがあります。
- 社内で使用しているソフトウェアの多様化に加え、取引先が要求してくるソフトウェア等、どのように制限をかけるべきかわからないことが多い。
- なかなか採用や育成が難しい領域なので、体系立てた育成プログラムがあると嬉しい。攻撃対策に関しては「完璧が存在しない」ので、どこまで対策すべきか？を迷うことが多い。
- 個人情報である住民情報や関係する業務システムは三層分離によって物理的に分けている。また、県のセキュリティが強化されたインターネット回線を使ったり、市独自にセキュリティ対策ソフトを整備したりとハード面では不足がないよう整備を行っている。一方、情報セキュリティポリシーの改定や周知、庁内職員へのセキュリティ教育、緊急事態発生時の事案処理体制などソフト面での対応が不十分であると感じている。
- 情報セキュリティ対策にさける人的リソースが圧倒的に不足している。
- 経営層の理解は得られているものの、専門組織がなく人的リソースの不足が課題。
- システム部門が情報セキュリティ対応について、経営側にボトムアップで報告している。トップダウンでの方針がなく、セキュリティに関する対応計画の説明では、過剰であるとの指摘があり、苦慮している。
- 費用の確保、使い易さとの両立、職員の意識向上の難しさ。
- システム部門の対応課題が多くリソース不足でセキュリティ対策に十分なリソースを充てて網羅的・体系的な検討ができない。点での対応になりがちである。
- 情報セキュリティに係るリスクが年々高まっていることは認識しており、UTMやEPP、バックアップなどの運用の整備といった最低限の備えはしているものの、専属部署・専任者がいないため当社状況に適した十分な対策がとれているとは言い難く、また、今後さらに高度化するリスクへの対応していくことに困難であり不安を感じている。
- 現時点ではサイバーセキュリティは企業間での競争力の源泉にはなっていないため、自助の取り組みは当然ながら、公助として情報セキュリティ機関との連携強化、共助として企業間でのノウハウや取り組みの共有をおこなうことで、より効率的、効果的な施策、活動が可能となると感じています。特に教育コンテンツなどは、海外の子会社を持つ企業においては、英語化や現地語化には相当の工数を費やしていると感じています。
- 教職員への適切な周知。また、対策が日々更新されており、実施すべき対策をタイムリーに一覧化していただき、教育機関向けには補助金による対策ができるようにしていただけると大変ありがたく存じます。
- 何をどこまで（どのレベル）まで対策すべきか判断に迷う。特にサプライチェーンへのセキュリティ対策について、建設業における協力会社は意識や対策レベルも低い傾向があり、どこまで要求するのか、法的観点も考慮し、注意が必要であり、課題である。
- デジタル人材の不足。
- 調査の実施主体に関する裏取りについて、警察庁ウェブサイト上の掲示にて実施の存在については確認できるものの、実際に当社に届いた封筒が正規のものであるかどうかの確証が得られない点にやや不安が有ります。
  また、アンケート自体は匿名で回答可能な内容となるよう配慮頂いておりますが、回答をEメールで送付する場合は必然的に身元を明かした状態となる点は若干の抵抗を感じます。
  導線はNPAのサイト起点で問題ありませんので、依頼先ごとに別送されたid/pass等でアンケートシステムにログインして回答するような形式だと上述したような確認の手間や回答時の不安について軽減できる面もあると思います。左記は一例ですが、来年度以降の実施形式についてアップデートをご検討頂けますと幸いです。
- コストがかかる。直接的に利益を生み出すためのものではないため、導入の理解を得るのに苦労する。
  業務効率とのトレードオフが発生する場合があり、現業部門からの反発が出ることが多い。

- 年々サイバーセキュリティの重要性が増大するに連れ、対策用のシステムの価格も増大し、予算取りに苦労している。
  優れたシステムを導入できたとしても、内部で働く教員、事務局職員のリテラシーが非常に低く、教育しきれていない。
  インシデント発生時に対応可能な人員が不足しており、実働可能な人間が実質的に情報センター職員一名であることが組織のサイバーセキュリティを考慮した場合の単一障害点となっている状況にあることに不安を感じている。
- ノウハウの不足。
- 近年増加しているランサムウェア対策などの対策はこれまでのウイルス対策などでは対処できず、対応製品・機器の導入には多額の費用がかかるが、予算の上限もあり万全な対策までは困難。
- IoT機器の増加により設備に対する攻撃への対策強化が必要な点や、標的型攻撃にAIが活用されることにより不正を見破ることが困難になってくることが不安である。
- 業務の利便性とセキュリティのバランスが課題。
- 国内グループ会社へのセキュリティポリシー適用になると、個社単位で対応指定行く必要があり時間がかかりそうな気がする。海外グループ会社へのセキュリティポリシー適用になると、国内と違うポリシーが必要になる。その為、１から作りなおす必要があるのと、それが受け入れられるのかが気になる。
- 社内に情報セキュリティ対策を行うための人材や体制、スキルが十分でない。
- 企業の社会的責務として、セキュリティ対策は鋭意推進してまいりますが、警察庁におかれては、国際共同捜査による被疑者の確実な検挙など、犯罪の拡大を防ぎ、その芽を摘む諸施策の尚一層の強化をお願いしたいと思います。
- 多様化するサイバー攻撃に対応するためには、人的方法では検知が遅れてしまうことが懸念されます。そのため、検知システムの導入が望ましいのですが、導入、維持にコストがかかるため、導入が困難な状況です。また、昨今、サイバーセキュリティの重要性が認知されてきてはいるものの、未だ専従でセキュリティ人材を確保することは常識ではありません。その為、現状、専門的に学んだことのない者がセキュリティ対策を講じていることが多く、不安を感じています。
- 所属内各職員へのセキュリティ意識の醸成に苦慮しております。
- 当社企業規模に応じた身の丈でのセキュリティの仕組化・運用の常態化を目指し、セキュリティ業務のPDCAを行っている。確実な正解がないセキュリティについて、フルスペックの対策・体制を取れれば相当の安心感を得られるが、コスト等を鑑みるとそこまで出来るものでもない。「身の丈」で「最善」を検討し運用していく事が最も困難な事と感じている。
- セキュリティ人材の不足。
- 業務の違いから事務部門と教育職員とでセキュリティのポリシーを分ける必要がある場合があることへの対応において、内部統制上さまざまな問題が生じている。
- 人員不足により十分な対策が出来ていないと感じている。
- 情報セキュリティ対策はどこまで実施すればよいか終わりが見えないが、かけられる費用は決まっているのでどこまでを妥協点とするのかが難しい。
- セキュリティを管理できる専門的なスキルを持った人材の確保が困難な状況となっている。
- 人的リソースが不足していること。
  何をどこまで実施する必要があるのかの整理、把握、判断が難しい。
  実際にインシデントが発生した場合に、適切に対応が出来るのか不安がある。
- サイバー攻撃が日々巧妙化、高度化し、リスクが増しているにも関わらず、セキュリティ人員と予算について、経営の理解が得にくく不足している。
- 高度化・巧妙化する攻撃に対応した情報セキュリティ対策を行っているが、運用、監視、インシデント対応等に必要なセキュリティ人材の確保が難しい状況がある。
- ＜困難に感じている事項＞
  ・サプライチェーンのセキュリティ対策強化。
  ・地政学的リスクに伴うサイバー攻撃リスクの増加および軍事行為としてのサイバー攻撃への対処。
  ・セキュリティ人材の確保および育成。
- セキュリティ対策の費用対効果が明瞭に試算できないことから、適切な投資規模感や維持すべきセキュリティ水準を明示化することに関して困難と感じている。
- 現状のネットワーク上、各デバイス上での弱い部分が明確でない。調査して明らかにする⇒セキュリティ強化対応が必要です。

- 人材と予算の確保。
- どこまで対策をすれば充分なのか判断に悩んでいます。
- EDRが入っていない未管理端末の対応 EU圏のNIS2指令といった、国際的な法制への対応。
- ユーザ企業のIT部門におけるセキュリティ人材の獲得・育成は難しいように感じています。
- ルールの策定や役割の明確化、CSIRT構築などの組織的なセキュリティ対策が弱いと感じている。
- 外部委託先や取引先から当社の情報が漏えいするケースが年々増加している。委託先や取引先の選定を厳格にするよう注意喚起をしているが、再委託先で発生するケースもあり、対策は非常に難しいと感じている。
  海外現地法人や海外子会社に対するサイバー攻撃（ランサムウエア、ＢＥＣ等）で実際に被害が発生しており、対策を急いでいるが、人材不足、人件費の高騰、ベンダーへの支払いコストの増加に苦慮している。
- 予算規模が大きくない中で限られた予算をどのような対策に利用するのが効果的・効率的かを考えることが難しい。
- 自社で物理サーバを保有すると、不正アクセスや災害対策などのコストや工数負担が大きいので、クラウドのストレージに移管していっているが、大容量データのクラウドストレージの保管にかかる利用料の増加が悩ましい。
- 費用対効果が見えない為、金銭が発生するものは導入へのハードルがある。
  専門の人材がおらず、十分な調査・研究・対策への時間をかけられない。
  サプライチェーン全体でセキュリティ対策を高めるのは、自社からの発信だけでは難しい。
- 本アンケートを情報セキュリティ意識の啓発や知識の普及に役立てていただければと存じます。
- 防御すればそれを超える攻撃が出てくるので、どこまでやれば大丈夫とは言えず、継続的にコストがかかってしまう。根本的に攻撃から守られる手段が開発されないと、いつまでも不安な状況が継続する。情報セキュリティ対策はコストと捉えられて、継続的な投資を得ることが困難。
- グループ会社を含めたサプライチェーン全体でのガバナンスや見える化をどのように進めるのか、直接的な対策とあるべき姿を目指すハイジーン領域を相互に関連付けしながら進める具体的なガイド等あると助かります。
- 実被害が発生しなければ、問題ないと判断され、十分な予算が付きにくい。ネットワーク機器等の保守費用の値上がり。ネットワークや機器に関する技術者不足。
- 様々な業者が色んな提案をしてくるが、それぞれ内容が異なるため、本学の規模で実際にどのレベルの対策をしたらよいのか、わからない。
- セキュリティ意識が高い職場とそうでない職場の温度差が大きいこと。
- 最低限、どのようなことを行えば「情報セキュリティ対策がとれている」と言えるのか、『簡単に分かる』資料が欲しい。
- セキュリティに関する人材育成の観点から以下の点を主な課題として認識しています。
  １．専門知識の不足：サイバーセキュリティに関する専門知識を持つ人材が不足しているため、サイバーインシデント発生時に適切な対応をとれるかが不安。
  ２．従業員全体のセキュリティ意識の向上：従業員全体のセキュリティ意識を高めることが重要だが、セキュリティ対策が特定部門の技術的な問題と捉えられがちとなっている。
- セキュリティ人材不足。一般従業員への教育は進めているが、システム部門のセキュリティ専門人材の育成や獲得が課題。また、デジタル化の進展で、「情報セキュリティ対策」の範囲が広がっているので、各部門（広報、生産、研究など）との連携が必須となり、そのコミュニケーション能力を如何に育てるかが課題。
- 内容で、公開できるものは積極的に公開し、総務省や経産省、デジタル庁などで類似のアンケートを頻発させないようにしていただきたい。
- 情報セキュリティ対策はどの程度が当社の適切なレベルなのか判断が難しい。対策を強固にすればするほど費用面のみならず利用者のリテラシーも必要になり、当社は自動車向け資材から農家まで幅広い業界が顧客でデジタル利用度がかなり異なっているため、自動車など高いレベルを基準に社内すべてを合わせていくことはビジネス的に見合わなくなってしまうという実状もあるため、そのあたりの考え方をどうすれば良いか困惑している。またそのような実状もあり当社内では「情報」はデジタルでないものも多数あり、アナログとデジタルを含めてビジネスレベルに見合う実効的な考え方で参考情報や指針があると非常にありがたいと考えている。
- 子会社・関連会社によって実施している対策に差があり、CSIRTを中心に平準化・高度化を同時に実施している。
- セキュリティ人材の育成、確保の困難さ。特に関西地方。
- 費用面との折り合いが合わず、優先度をつけながら対策をしていく必要があるため、不十分な対策となっている可能性があり、解決について困難だと感じる。また、同理由によりセキュリティ人事の育成についても取り組めていない状況となる。
- 情報セキュリティに関する技術は最新且つ高度であるため、導入や運用にコストがかかる。本学などの教育機関の場合、NICTなどの公的機関、または、複数の私立学校などによる共同出資によるセキュリティ監視センター（SOC）などを設立し、セキュリティ監視レベルの底上げと持続可能な運用体制の確立が必要と考えています。

- セキュリティ業務に関してのリソース割り当てをいかに増やしていくか(上層部への必要性の説明や、効果の確認)に難しさを感じている。
- 当社は情報セキュリティ対策を重要視しており、定期監査や社内研修を行っております。また、弊社を管轄する麻布警察署様から様々なサポートを受けており、情報セキュリティ担当者に対する講習や「技術流出の防止～あなたに迫るリスク」のデータを社内研修用にお貸し頂いております。引き続き、情報セキュリティ対策を講じて参ります。
- 不正アクセスやセキュリティインシデントは、どのような対策を行ったとしても、いつ発生してもおかしくないという認識です。お金をかければある程度情報を守ることはできますが、利便性は確実に損なわれます。そこまでやれば安心というものが無いのが最大の不安材料と思います。
- 予算と人員が不足している点が困難に感じています。
- 教育機関では、学生・生徒などについても、情報セキュリティから守る必要があるため、どこまでの対策が必要なのか、バランスやはんだが難しい。
- 社内にセキュリティ人材に対する育成、評価制度がない。
  サプライヤーとのセキュリティ製品の金額交渉を当社単体にて行っており、交渉力が弱い。業界団体単位で取り組むなどの指針を公共機関として出していただきたい。
  ※次回アンケート依頼を実施される際には是非、Web上での回答が行える形式にて実施いただけませんでしょうか。
- アンケート調査回答内容についての補足事項です。 以下、設問の解釈に迷った点は、「その他」の記述回答を使用して補足説明を付記しました。
  問8以降の設問で「攻撃・被害」は、「攻撃」又は「被害」と解釈して回答しています。
  「被害」の解釈として、「犯罪被害」に至らず「実質的な被害はなかった」未然防止事案も一部回答に含んでいます。
  設問8-4の届出については、サイバー攻撃以外のインシデント案件としての事案を含んでいます。また「警察」への届出は国内でなく海外事案です。それぞれ不要な場合は除外ください。
- 構成員のPCの監視システムを導入しておらず、セキュリティ対策は個々で行っているが、全ての構成員が必要な対策を取っていることを確認できないこと。
- アンケートの質問項目が曖昧なため、回答に困る部分が非常に多い。システムと一言で言ってもそれぞれのNWで構築や対策が違い、一概に回答することが難しい。
- セキュリティは一番弱いところから破られるため、注意喚起を行っても行っても失敗する人が出る。特に一部の失敗がドメイン全体に波及するメールはもう使いたくない。
- 教員のPC環境はBYODとなっているが、セキュリティ対策が不十分なため改善の検討をしているが、セキュリティ対策を行うと、環境の自由が無くなるが、研究を行うにはある程度の自由な環境が必要になる為、どこでバランスをとるかが難しい。
- セキュリティ専門の人材が学内に雇用されていない状況のため、技術的な知識や判断が求められる際に外部の力を頼らざるを得ない状況である。
- 標的型攻撃などに対応するための訓練には、詐欺メールをすり抜けるような工夫が必要で、実施には費用がかかってしまう。
- セキュリティレベルを上げるとユーザビリティが下がり、バランスが難しい（SSOを廃止しゼロトラストを構築すると、都度ログイン操作が必要となる）。
  セキュリティ対策要員を複数かつ世代別に配置できると継続的なセキュリティレベルの維持が可能だが、現在の組織ではそれが叶わない。
  たまたま、運よくサイバー攻撃の対象になっていないだけで、いつ自分たちの身に降りかかってくるか、を一般ユーザーに分からせることが難しい。
- 教員、職員、学生も含めた全構成員に、情報セキュリティ研修を実施していますが、受講率を上げる事がとても難しいです。
- 本アンケート自体が、何らかの攻撃ではないかと疑い、警察庁のサイトなどで確認に手間取りました。
- 対策は強化しているが、どこまでのレベル強化を実施すればよいか難しい。
- 困難に感じていること：
  ランサムウェア対策が困難に感じる。
  対策製品の導入は、高いコストの割りに費用対効果が見えにくい、さらにEDR等の対策ソフトウェアを導入しても100%被害を防げる保証がないこと。
- 技術的な課題については、外部業者にヘルプデスク業務を委託し、情報セキュリティ関連業務を担わせているものの、定期的な人事異動があることから、担当者の情報セキュリティに関する専門性が高まらない。
- セキュリティ製品を運用する(できる)人材が不足している。子会社で情報セキュリティを推進する組織、人材が不足している。

- 高度化に追いつけていない。
- セキュリティの為に認証の仕組が面倒になってしまったり、多要素認証でアプリが必要になったりで、スマートフォン等が必要なケースが増えてきており、認証の為だけに支給するのはコストが見合わず、個人のスマートフォンを使わせるわけにもいかずに困難を感じている。
- ハッカーとセキュリティ対策の戦いは永遠に「いたちごっこ」が続くと思われる。重要な情報を持つパソコンは一切外部と接続しないに限る。
- セキュリティ人材の育成について、根本的に人員が不足している。
- 介護業界は、1人1台PCやスマートフォンの配置が難しいため、SmartHRを使用して、研修などを行っているが、研修専用ではないので、Yes･Noの簡易的なアンケート形式になっている。共用の端末でも動画研修が可能な仕組みがコストをかけずにあると助かる。
- セキュリティ対策や教育を実施する人員が不足しているが、社内で人材を育成するのも難しいと感じている。
- セキュリティ人材の育成が大きな課題です。
- 自社CSIRTの立場で、サイバーセキュリティ堅牢化基本要件やインシデント発生で惹起される各種リスクなどに関して、自社ならびに関連会社･サプライチェーン企業への研修･訓練活動を継続的に実施して参りました。ただ、各人の理解(実装)度や運営サイドへの協力度合には組織毎に大きな乖離を確認できる現状にあり、相対的低リテラシー層の水準引き上げが目下の課題であると認識しております。
- ランサムウェア対策としてEDRが有効と思われるが、ウィルスソ対策ソフトと比べると、かなり高額である為、導入が難しい。中小企業のレベルでの現実解がほしい。
- 自社での人材育成が困難。
  海外子会社を含めた体制づくりが困難※環境や言語のちがいがあり、教育が難しい。
- なかなか理解されない。金食虫と思われている。
- どこまで対策する必要があるか不明。
  年々セキュリティ関連の費用が増加する。
  社員のセキュリティ意識がなかなか向上しない。
  グループ会社も含めたセキュリティ強化は負荷が大きい。
- 社員の理解が得られにくい(面倒、仕事が止まる)→特に50代以上会社役員のITリテラシーが低い(予算がとれず対策が遅れる。)社会全体として、情報セキュリティに対するリテラシーを上げる取り組み(学校教育、等)が必要。
- 学内でのセキュリティ人材不足、経費の捻出に苦慮している。
- 予算の確保。(どれくらい予算をかけたらよいのか、基準が見えない)内部不正の検出(UEBAでも限界がある)アンケート自体をWebで回答できるようにすれば?時代遅れな気がする。
- 困難に感じている点
  ゼロトラスト対応
  安全なテレワーク方法
- お金、人手、手間がかかる。
- 費用対効果がわからないため投資額が決めづらい。(終わりがなく最適な基準もない。)
- こちらのアンケートに回答していくうちに、いかに無知で対策不足であるのかを痛感致しました。委託してあるので大丈夫、ではなく自分達で対策する意識をもたねばならないと思いました。低レベルな回答でお恥ずかしい限りですが、どうぞよろしくお願い致します。
- 郵送された「調査ご協力のお願い」にあるURLでしかエクセルダウンロードできないのは、信用できない。警察庁のホームページからサイトに飛んで、ダウンロードできるようにして欲しい。(←新着情報にやるよと書いてあったが)もしあったとしてもどこかわからない。
- 情報セキュリティ対策コストを投資と捉える環境になかなか成りえないところでしょうか。
- 技術的対策は終わりが見えず、費用面、運用面で不安がつきまとう。
  IPAサイトを参考に、組織的人的対策に取り組み始めた。
  インシデント発生時に、法的にどこへ通知が必要なのか、分からない。
- セキュリティ対策を強化するための、予算･人材の確保が困難。
  「どこまで対策すれば良いか」のゴールが、明確に設定できない。
- 経営者のリーダーシップ。情報セキュリティ対策に対する社内の理解が得られない。
- コストをどこまでかけるか、が課題と感じる(お金、人)。
  リテラシーの低いユーザへの教育。

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

調査票ファイルに回答内容を入力し、電子メールにて回答

② 郵送等での回答

配付した調査票に回答内容を記入し、郵送等にて回答

（調査期間：令和6年8月28日(水)（発送日）～9月20日(金)（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

【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

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、225件を回収し、回収率は11.9%であった。

全体での回収数225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32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29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

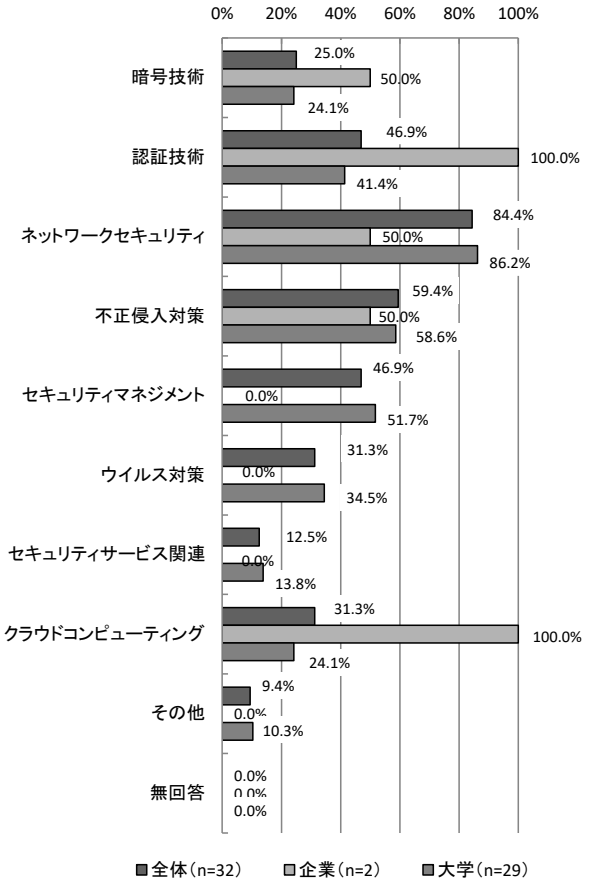
現在、取り組んでいる分野について、全体では「ネットワークセキュリティ」が最も高い。企業では「認証技術」、「クラウドコンピューティング」が高く、大学では「ネットワークセキュリティ」が高くなっている。

今後、取り組んでいく分野について、全体では「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」「ネットワークセキュリティ」が高く、大学では「ネットワークセキュリティ」が高い。

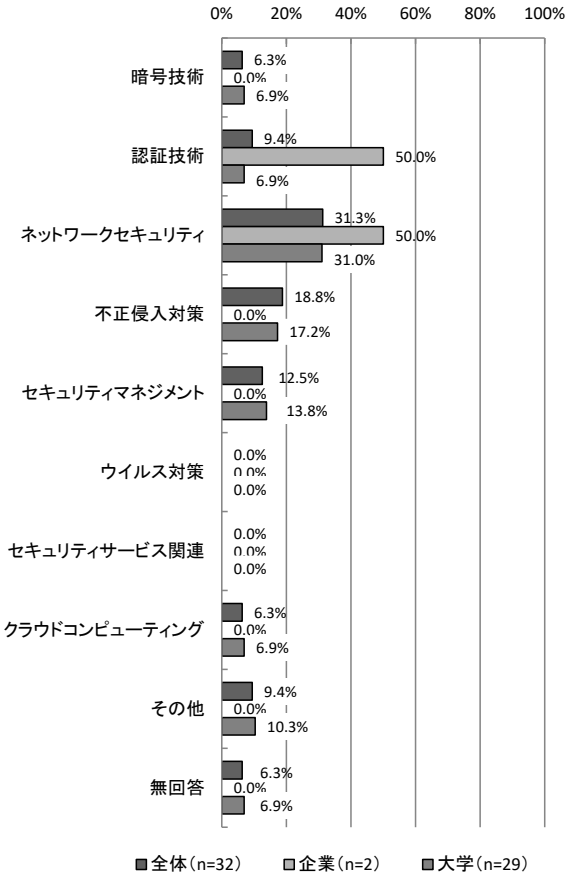
現在、取り組んでいる分野については、全体では「ネットワークセキュリティ」が84.4%（27件）で最も多く、次いで「不正侵入対策」が59.4%（19件）となっている。企業では「認証技術」、「クラウドコンピューティング」がそれぞれ100.0%（2件）で最も多く、大学では「ネットワークセキュリティ」が86.2%（25件）で最も多い。

今後、もっとも力を入れたい分野については、全体では「ネットワークセキュリティ」が31.3%（10件）で最も多くなっている。企業では「認証技術」「ネットワークセキュリティ」がそれぞれ50.0%（1件）、大学では「ネットワークセキュリティ」が31.0%（9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】

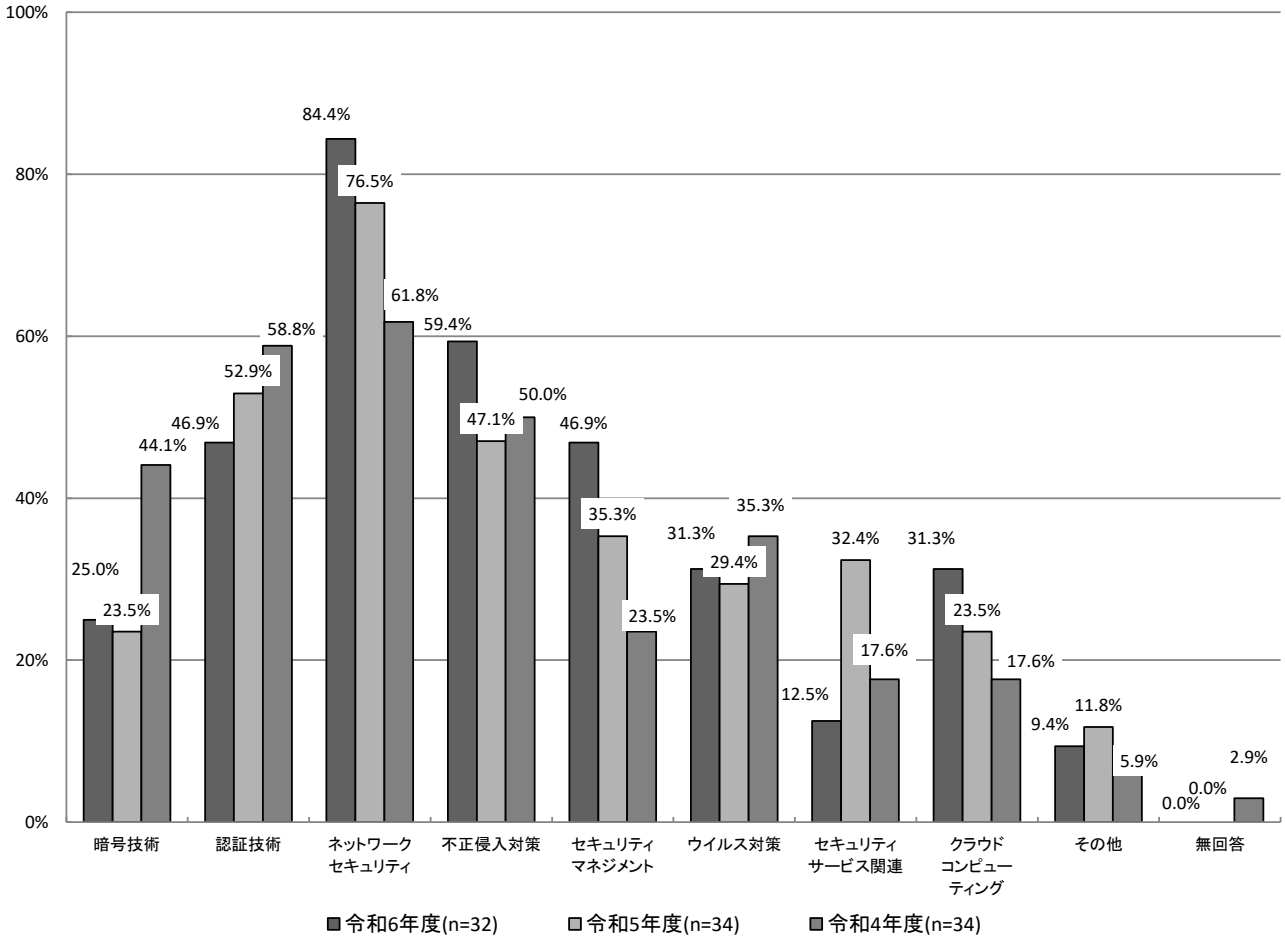


5.1.1 現在、取り組んでいる分野 【A-問2】

【経年変化】
全体では、特に「セキュリティサービス関連」が減少している一方で、「不正侵入対策」「セキュリティマネジメント」が増加している。
企業では、「セキュリティマネジメント」「セキュリティサービス関連」が減少し、「クラウドコンピューティング」が増加している。大学では、「セキュリティサービス関連」が減少し、「セキュリティマネジメント」が増加している。

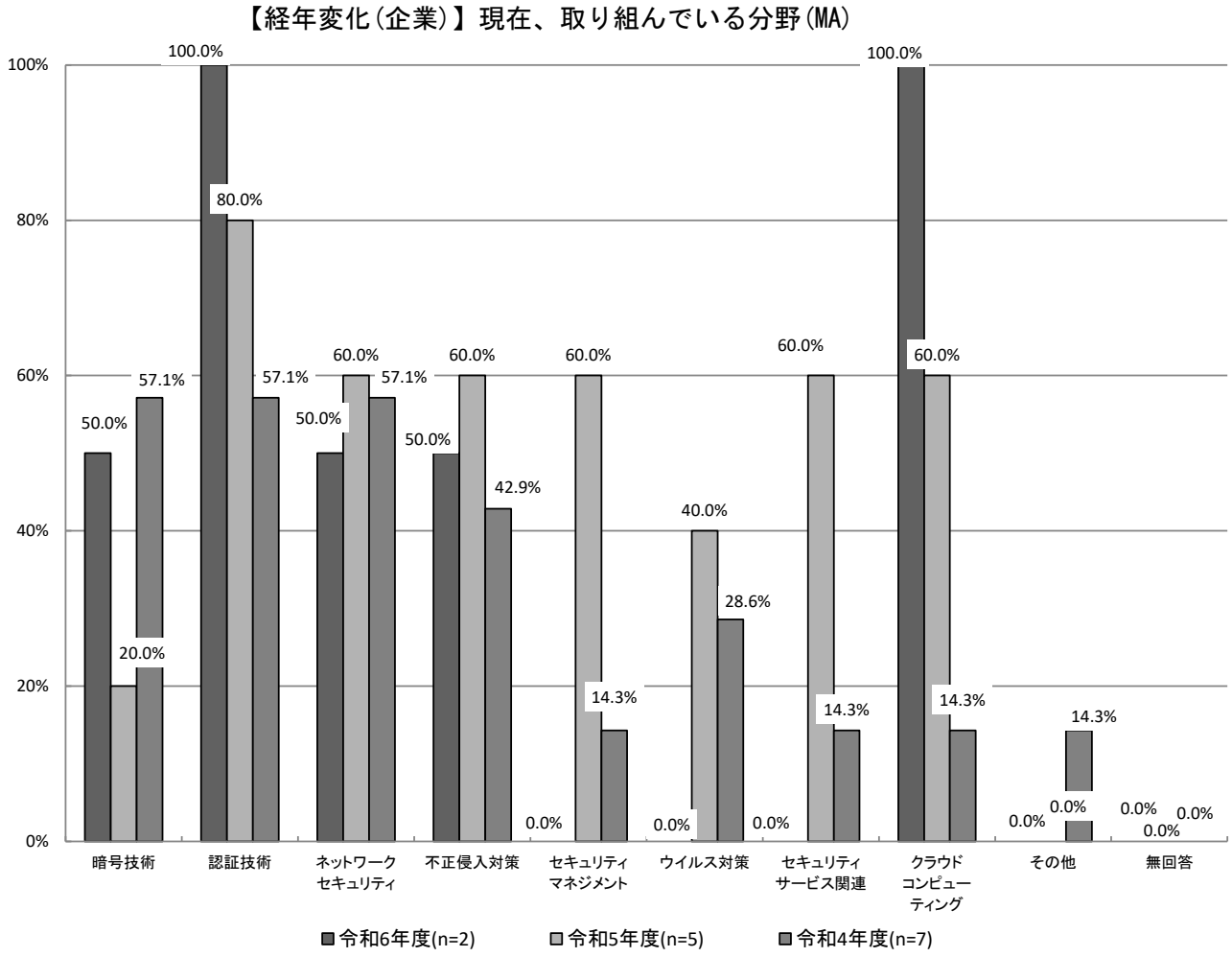
【経年変化(全体)】
昨年度と比較すると全体では、「セキュリティサービス関連」が19.9ポイント減少しており、「不正侵入対策」が12.3ポイント、「セキュリティマネジメント」が11.6ポイント増加している。

【経年変化(全体)】現在、取り組んでいる分野(MA)

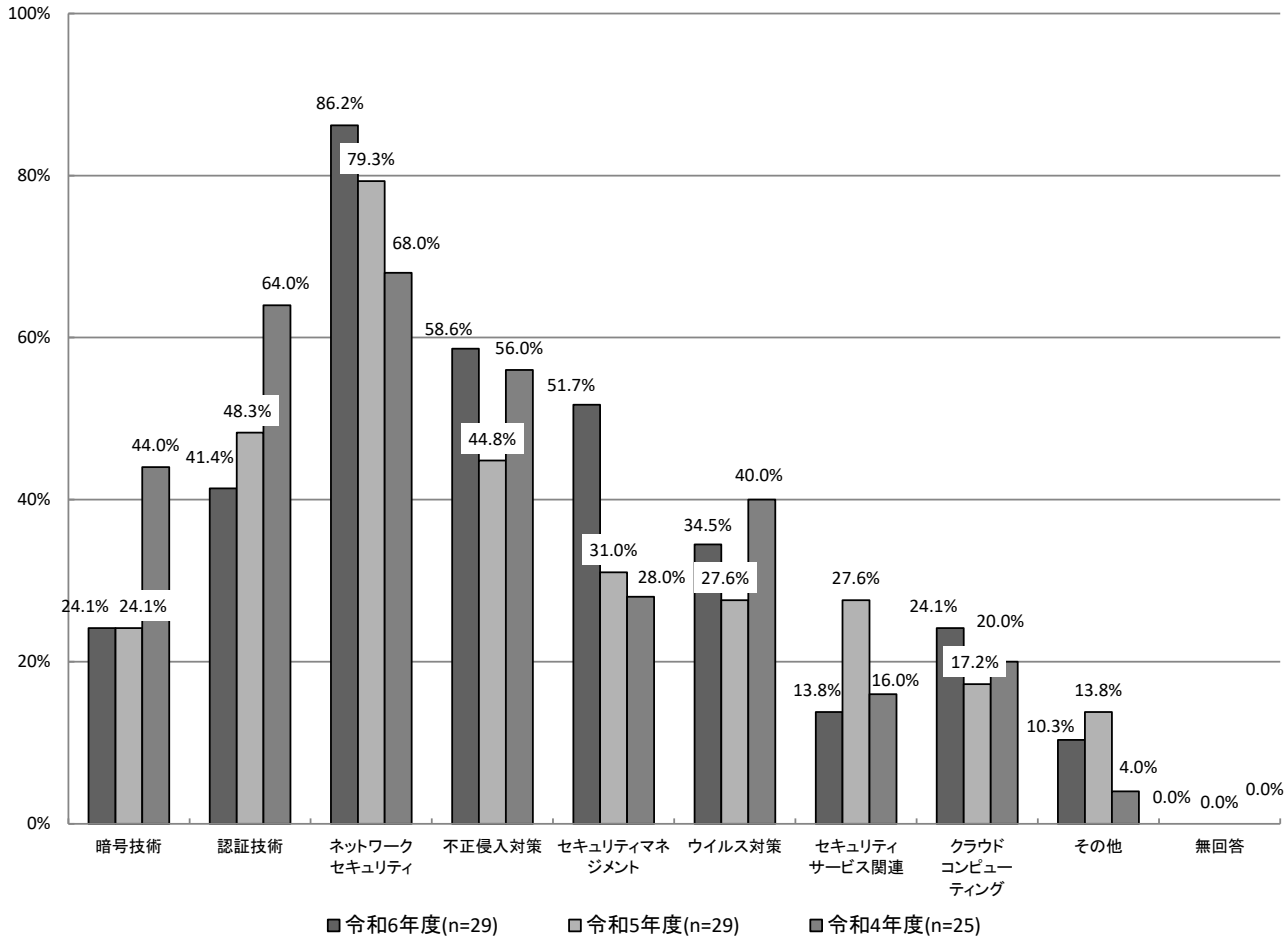


【経年変化(企業)】

昨年度と比較すると企業では、「セキュリティマネジメント」「セキュリティサービス関連」が 60.0 ポイント減少しており、「クラウドコンピューティング」が 40.0 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、「セキュリティマネジメント」が20.7ポイント増加しており、「セキュリティサービス関連」が13.8ポイント減少している。

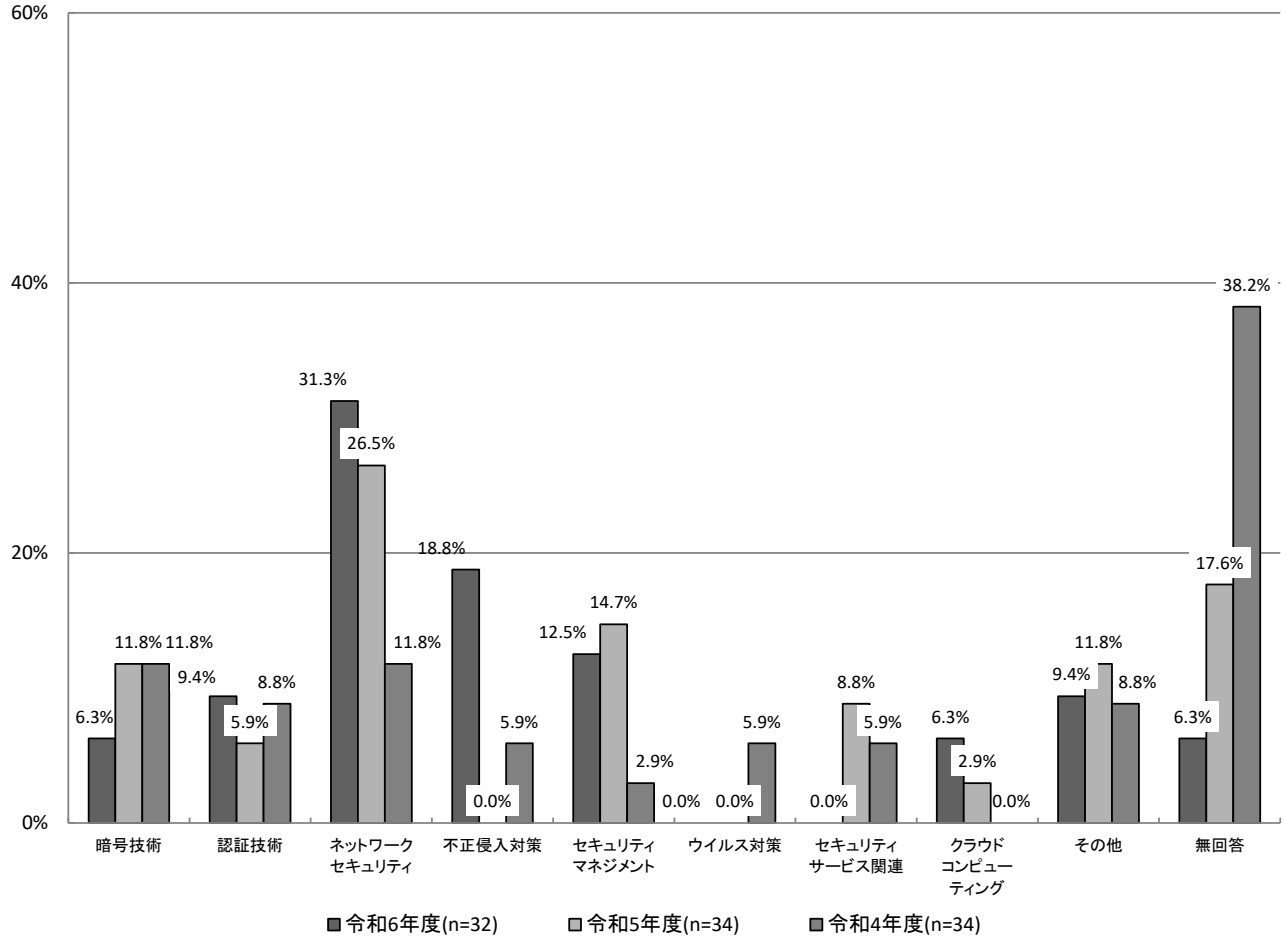


5.1.2 今後、もっとも力を入れたい分野 【A-問3】

【経年変化】
全体では、「不正侵入対策」が増加している一方で、「セキュリティサービス関連」が減少している。
企業では、「ネットワークセキュリティ」が増加しており、大学では「不正侵入対策」が増加している。

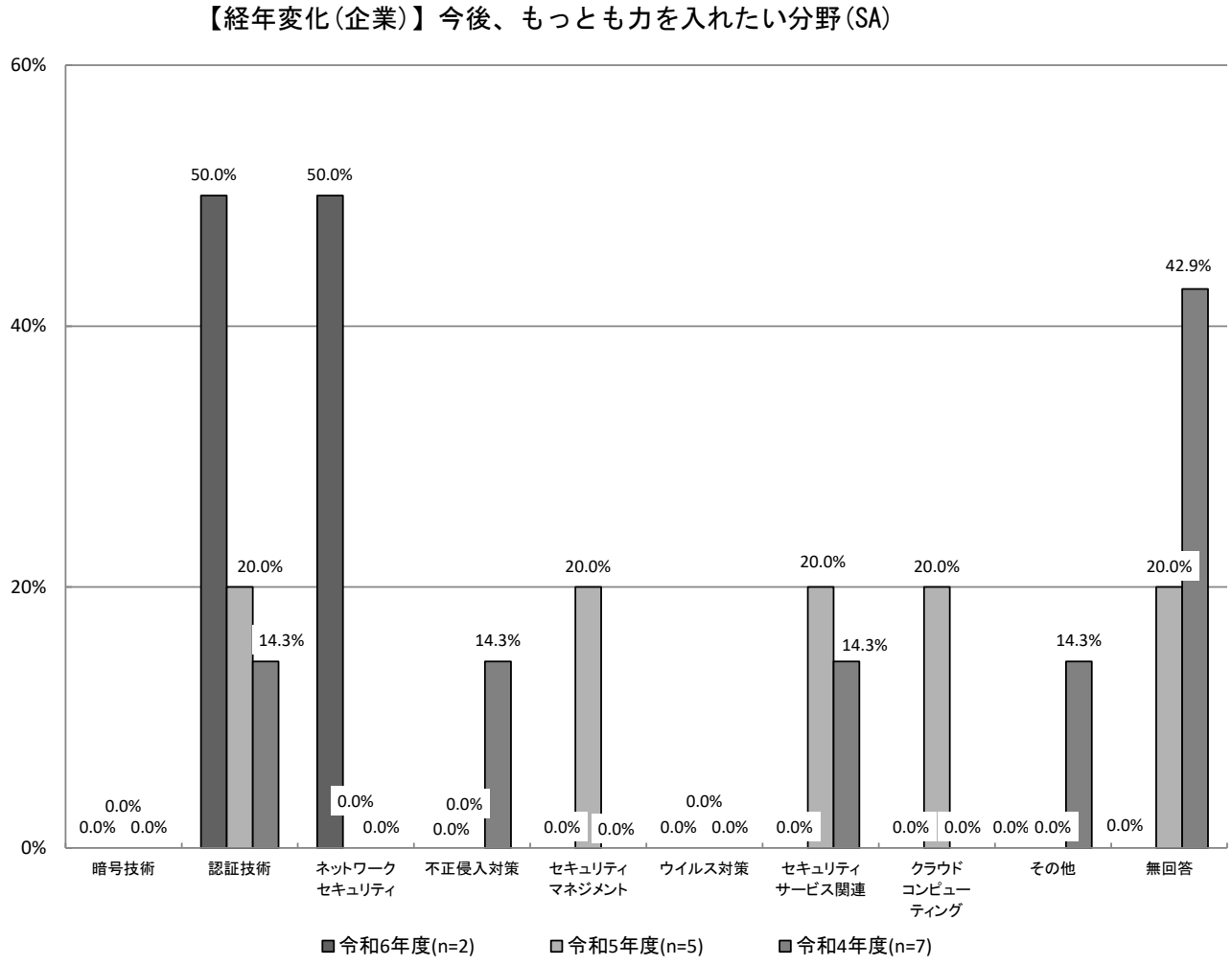
【経年変化(全体)】
昨年度と比較すると全体では、「不正侵入対策」が18.8ポイント増加している。一方、「セキュリティサービス関連」が8.8ポイント減少している。

【経年変化(全体)】今後、もっとも力を入れたい分野(SA)

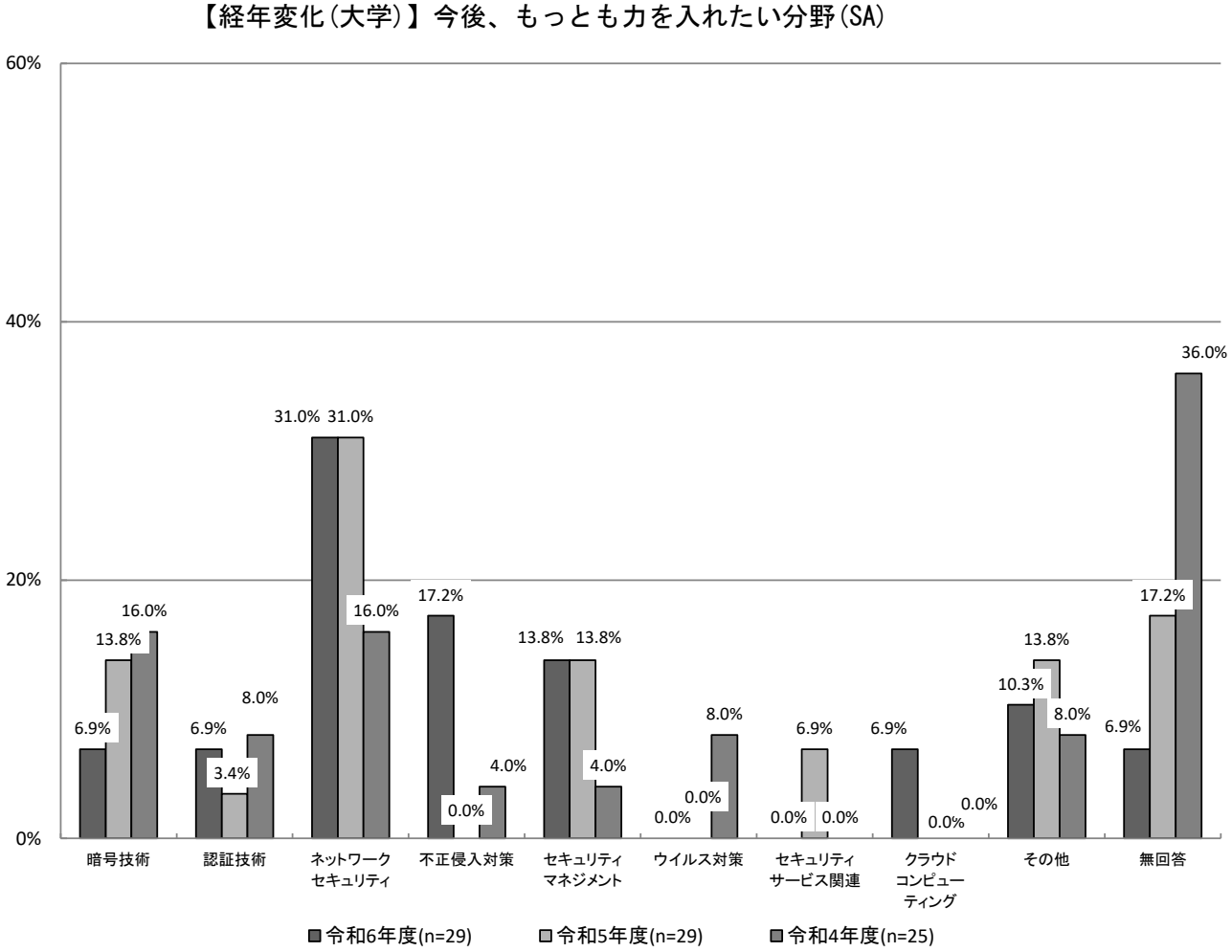


【経年変化(企業)】

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50.0ポイント増加している。一方、「セキュリティマネジメント」「セキュリティサービス関連」「クラウドコンピューティング」が20.0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、「不正侵入対策」が17.2ポイント増加している。一方、「暗号技術」は6.9ポイント減少している。

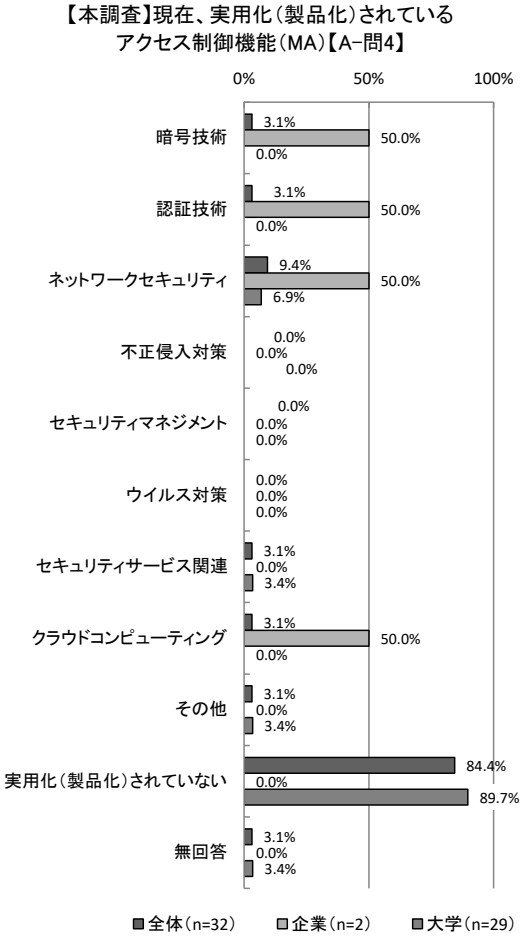


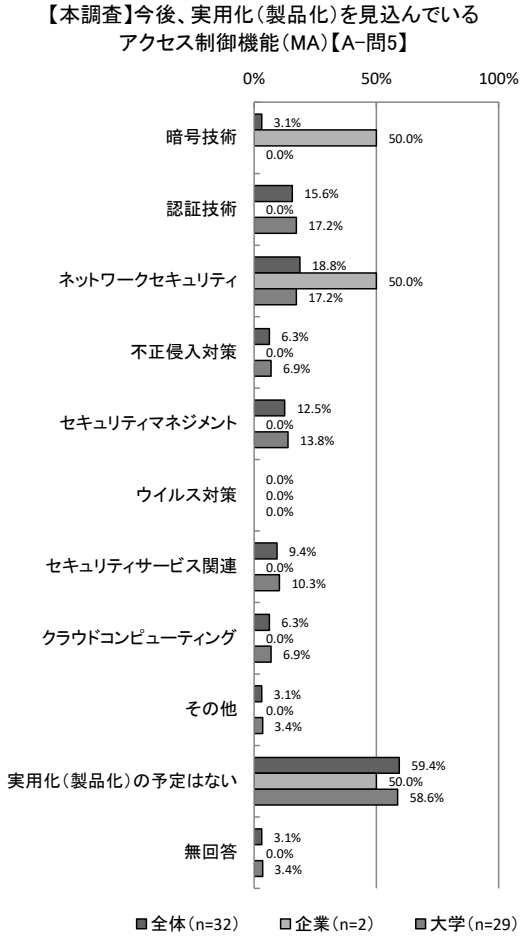
5.2 アクセス制御機能に関する実用化(製品化)に係る現状と今後の展望

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も、「ネットワークセキュリティ」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9.4%（3件）で最も多い。企業では「暗号技術」「認証技術」「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50.0%（1件）、大学では「ネットワークセキュリティ」が6.9%（2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「ネットワークセキュリティ」が18.8%（6件）で最も多く、次いで「認証技術」が15.6%（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50.0%（1件）、大学では「認証技術」「ネットワークセキュリティ」がそれぞれ17.2%（5件）で最も多くなっている。



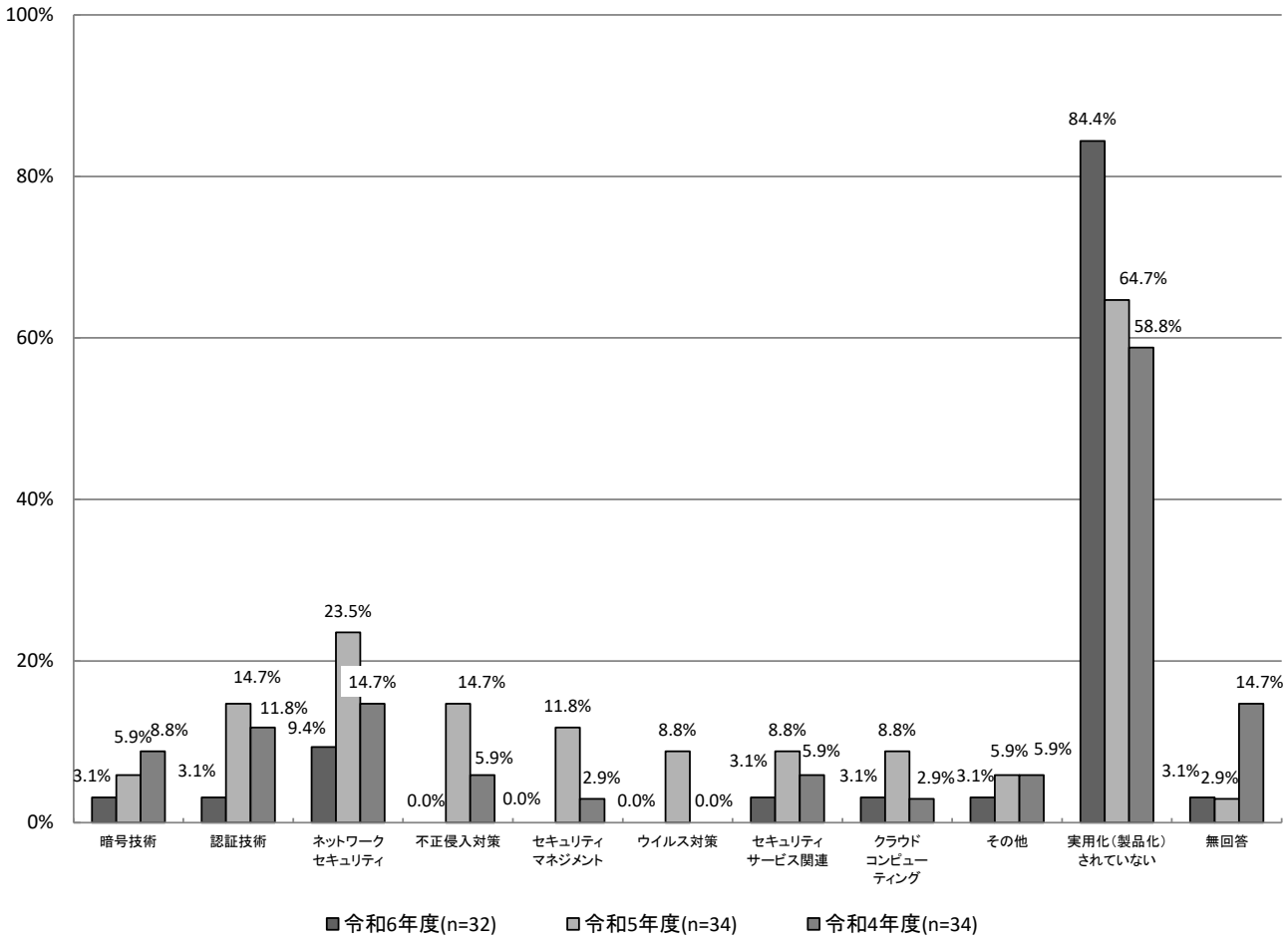


5.2.1　現在、実用化(製品化)されている分野　【A-問4】

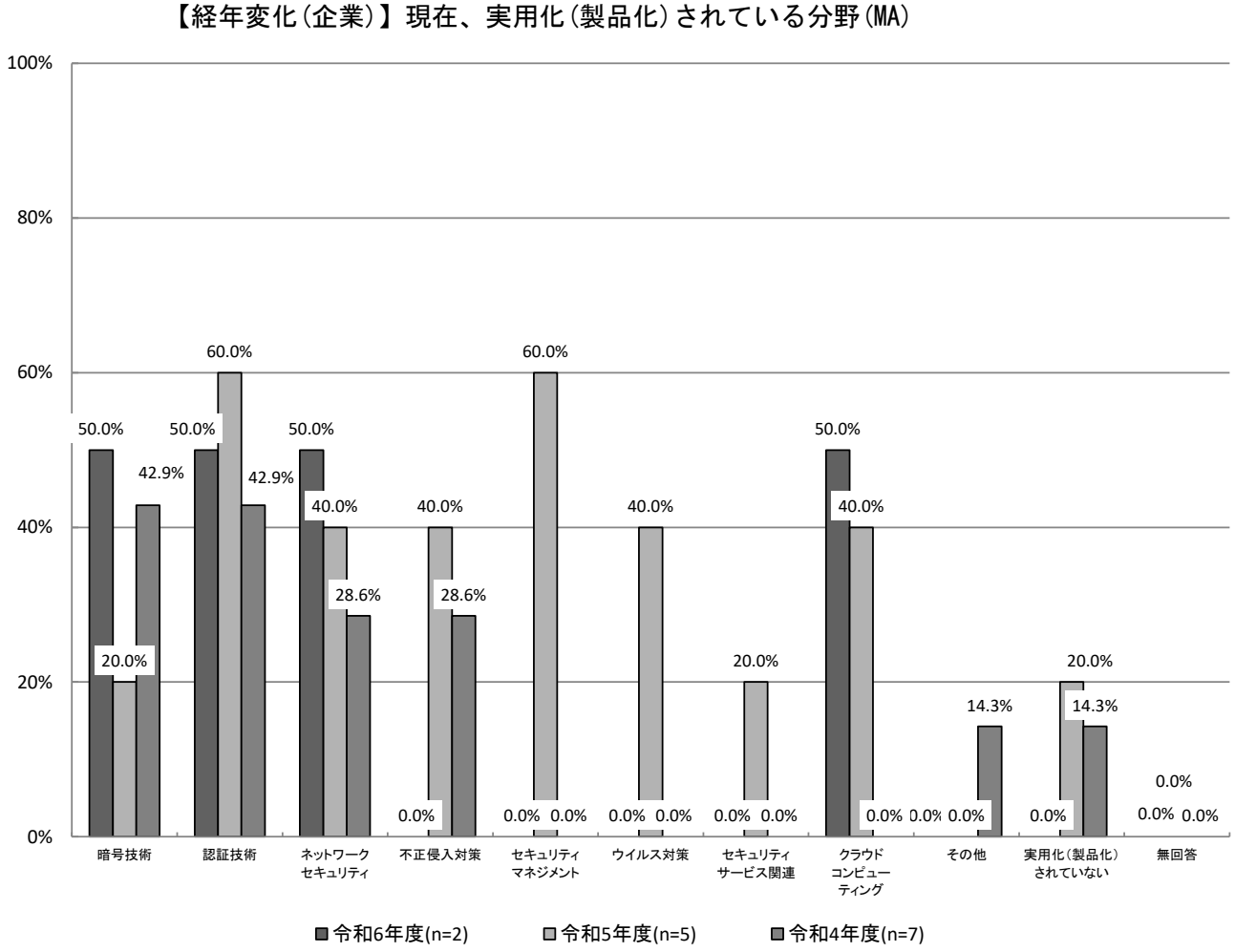
【経年変化】
　全体では、すべての分野で減少している。
　企業では、「セキュリティマネジメント」が60.0ポイント減少、大学では「ネットワークセキュリティ」が13.8ポイント、「不正侵入対策」が10.3ポイント減少している。

【経年変化(全体)】
　昨年度と比較すると「不正侵入対策」が14.7ポイント減少しており、それ以外の分野でも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)

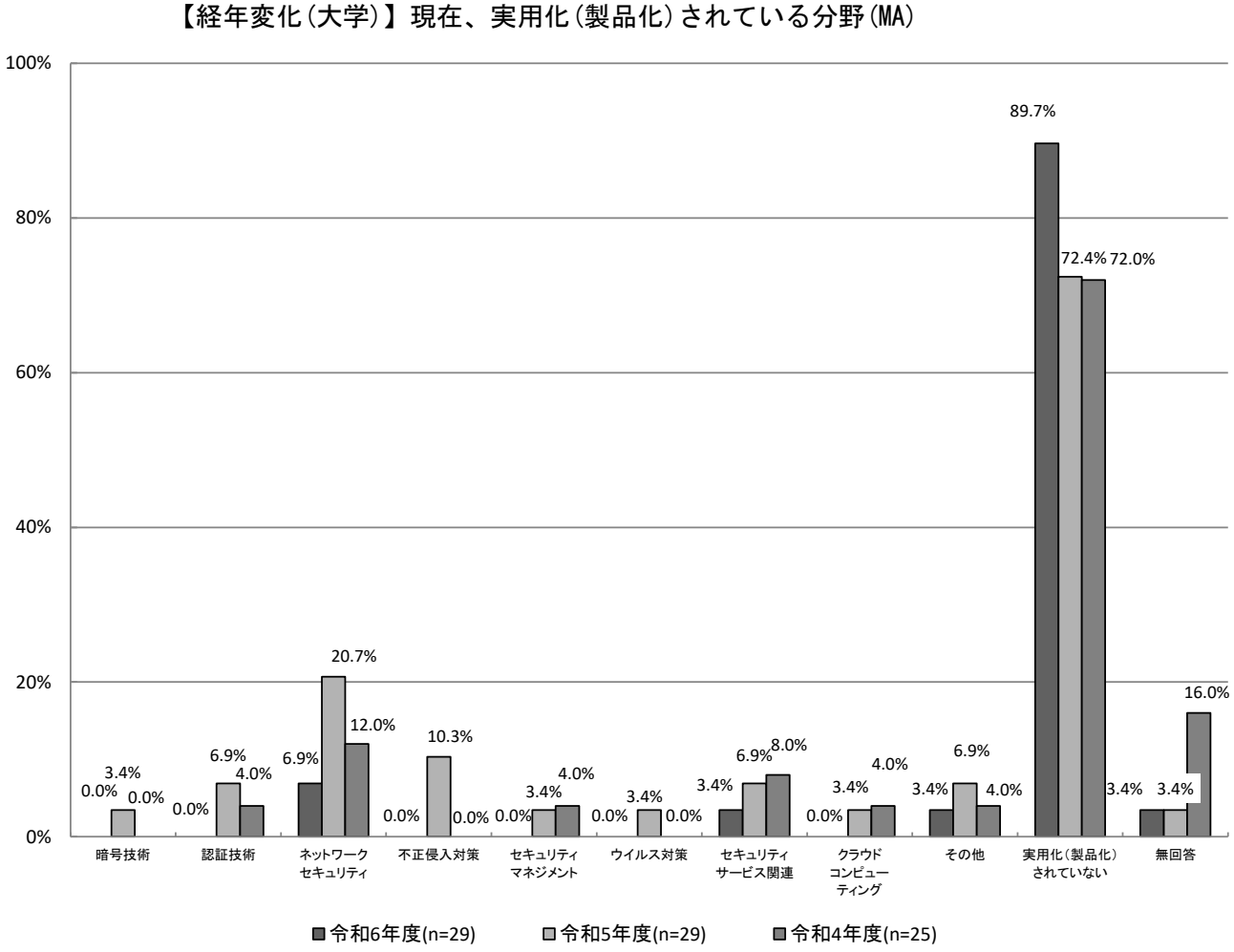


【経年変化(企業)】
昨年度と比較すると企業では、「セキュリティマネジメント」が60.0ポイント減少している。



【経年変化(大学)】

昨年度と比較すると大学では、「ネットワークセキュリティ」が13.8ポイント、「不正侵入対策」が10.3ポイント減少している。

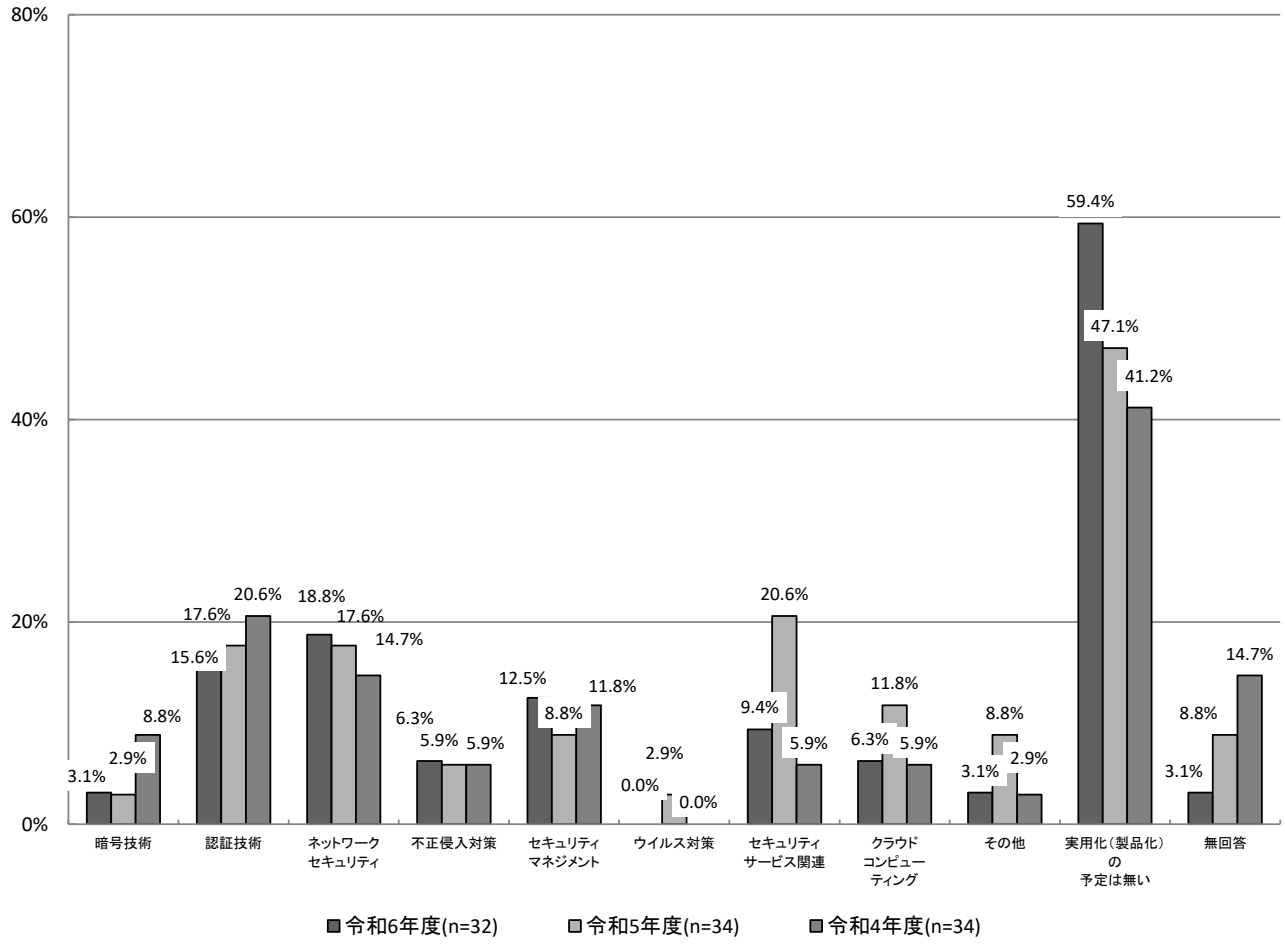


5.2.2　今後、実用化(製品化)を見込んでいる分野　【A-問5】

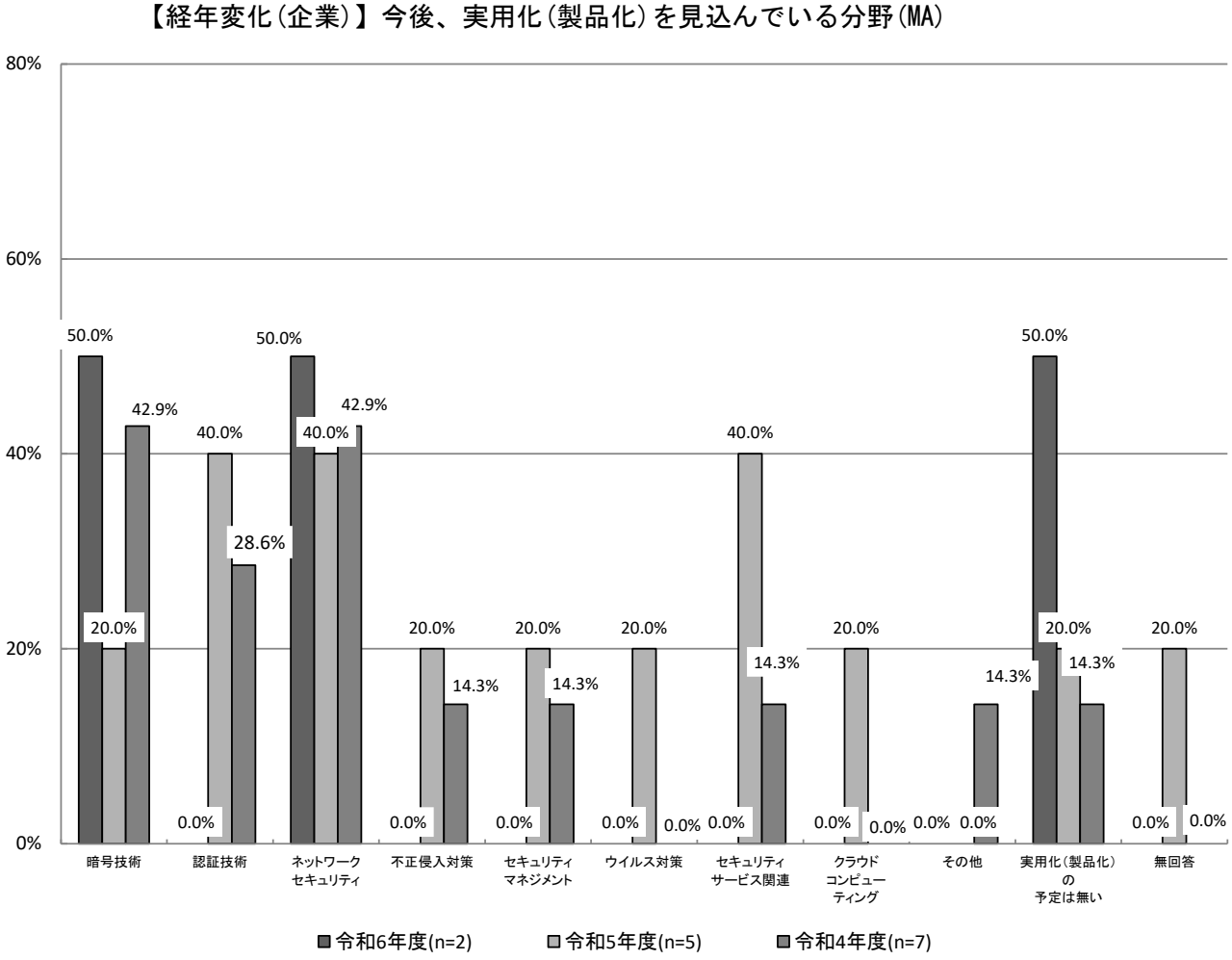
【経年変化】
　全体では、「セキュリティサービス関連」が減少している。
　企業では「認証技術」「セキュリティサービス関連」などが減少しており、大学では「セキュリティサービス関連」が減少、「セキュリティマネジメント」が増加している。

【経年変化(全体)】
　昨年度と比較すると全体では、「セキュリティサービス関連」が11.2ポイント減少している。次いで、「クラウドコンピューティング」が5.5ポイント減少している。

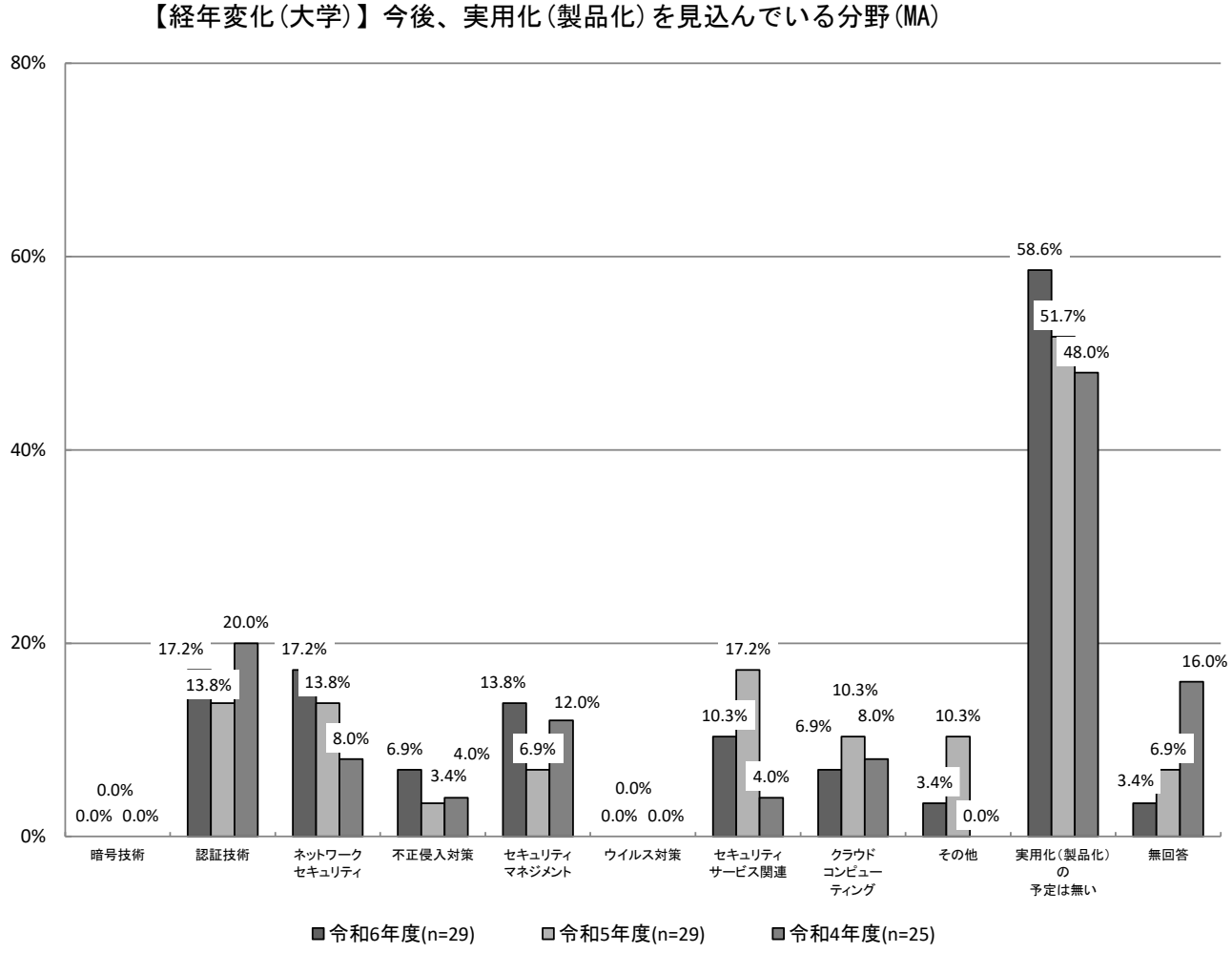
【経年変化(全体)】今後、実用化(製品化)を見込んでいる分野(MA)



【経年変化(企業)】
昨年度と比較すると企業では、「認証技術」「セキュリティサービス関連」が40.0ポイント減少しており、「暗号技術」が30.0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6.9ポイント減少している。一方、「セキュリティマネジメント」が6.9ポイント増加している。



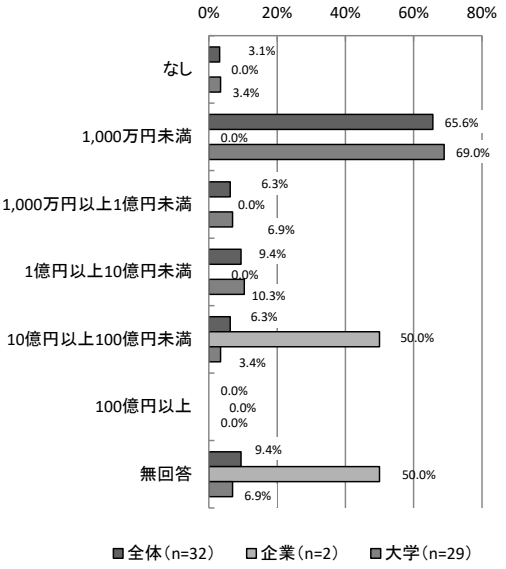
5.3 研究開発体制

研究開発費について、全体では「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、全体では「1人以上10人未満」が最も多くなっている。

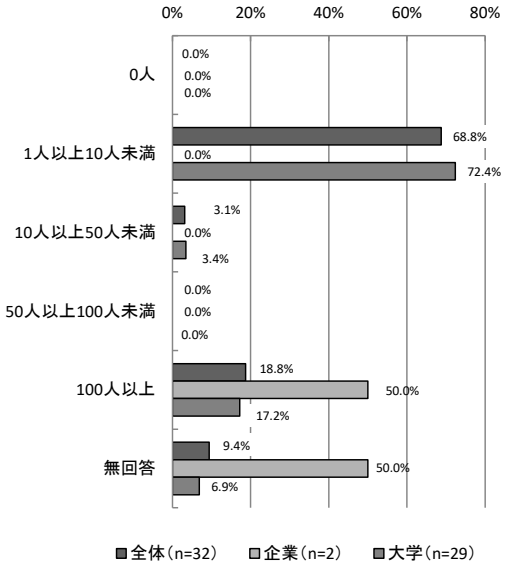
年間の研究開発費については、全体では「1,000万円未満」が65.6%（21件）で最も多くなっている。大学では「1,000万円未満」が69.0%（20件）と最も多くなっている。

研究開発人員については、全体では「1人以上10人未満」が68.8%（22件）と最も多くなっている。大学では「1人以上10人未満」が72.4%（21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】

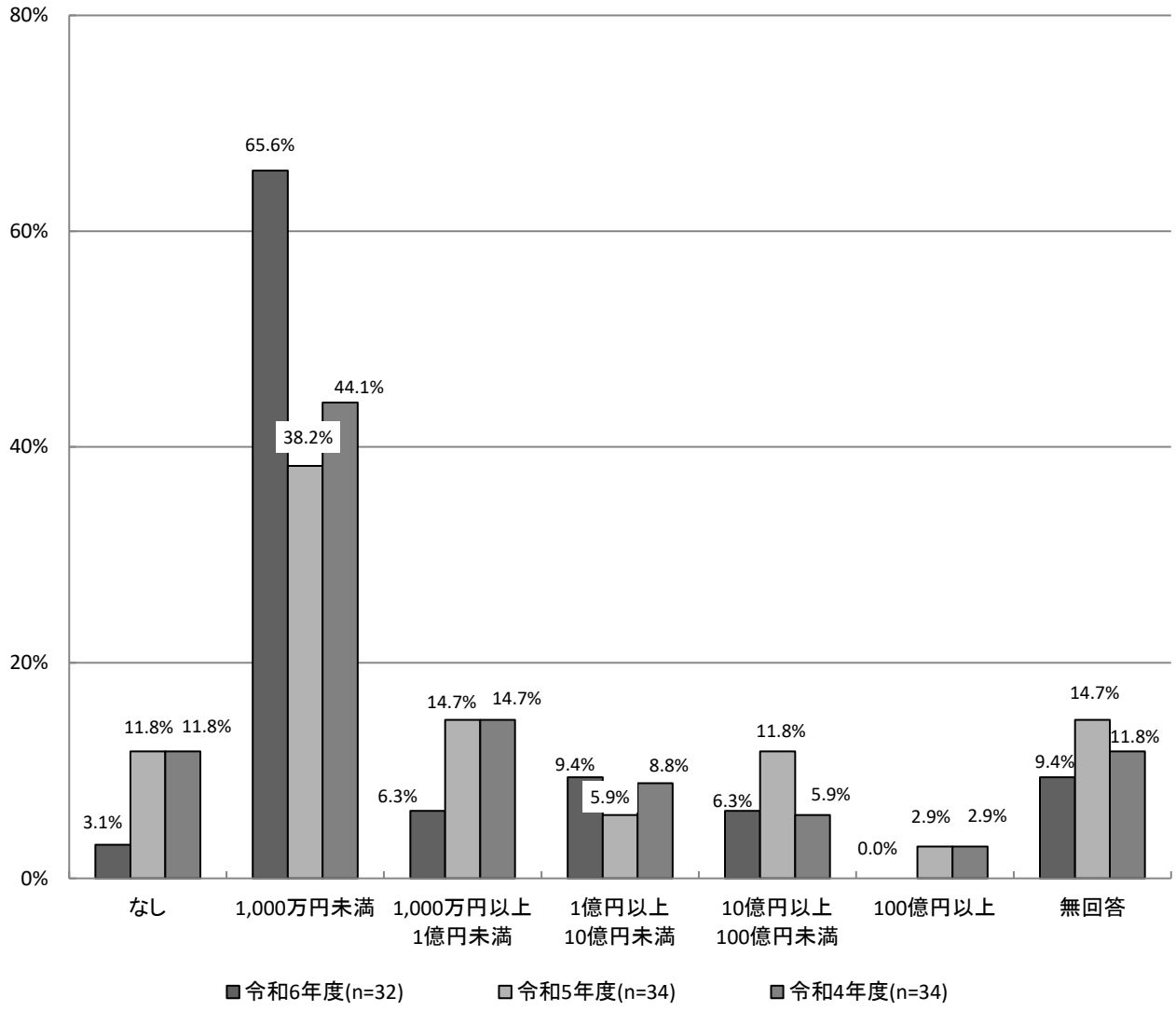


5.3.1　年間の研究開発費　【A-問6】

【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、「1,000万円以上1億円未満」が減少している。
大学では「1,000万円未満」が最も増加している。

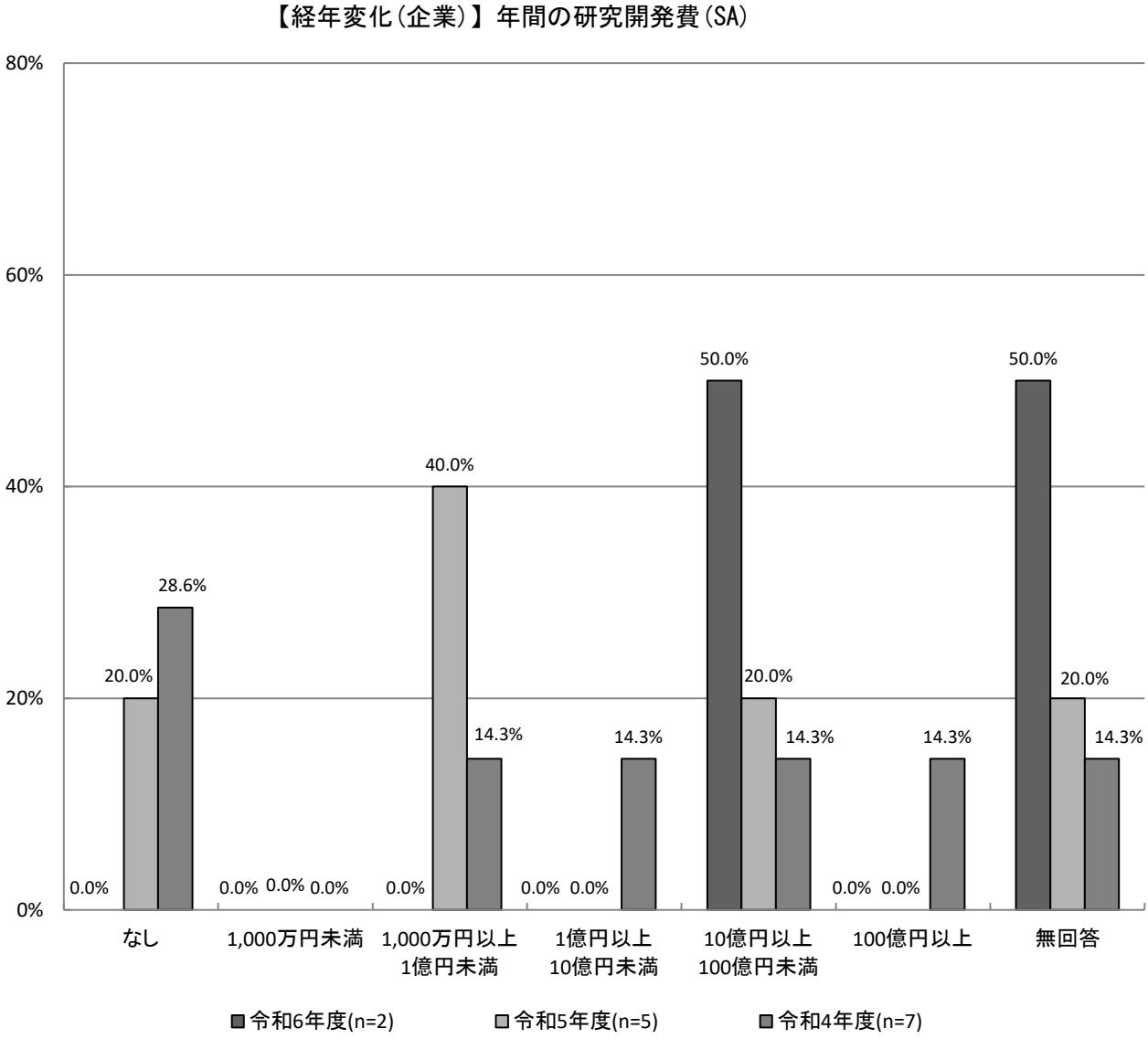
【経年変化(全体)】
昨年度と比較すると全体では、「1,000万円未満」が27.4ポイント増加している。一方、「1,000万円以上1億円未満」が8.4%減少している。

【経年変化(全体)】年間の研究開発費(SA)

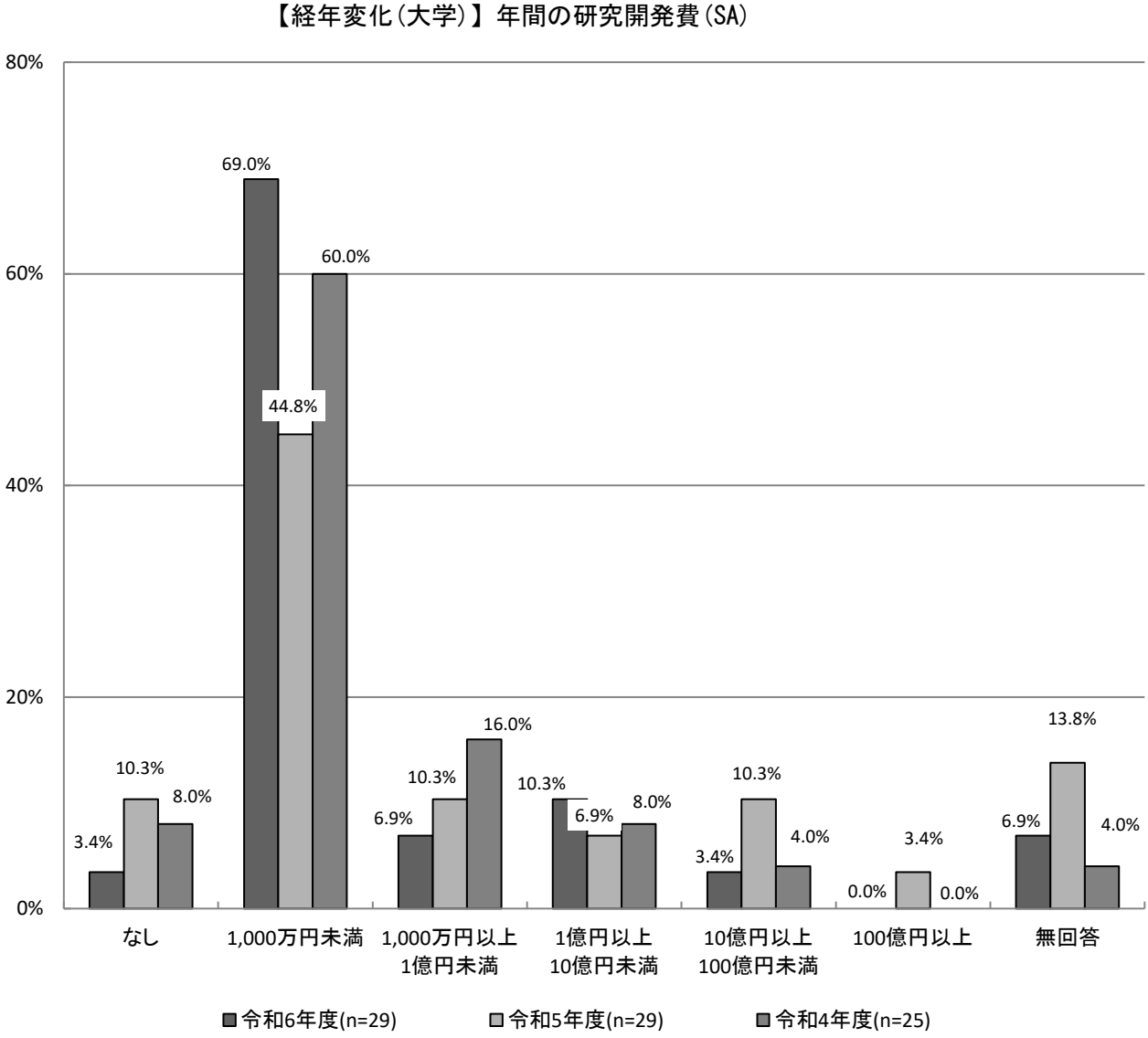


【経年変化(企業)】

昨年度と比較すると企業では、「1億円以上10億円未満」が50ポイント増加している。一方、「1,000万円以上1億円未満」が40.0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、「1,000万円未満」が24.2ポイント増加している。一方、「10億円以上100億円未満」が6.9ポイント減少している。

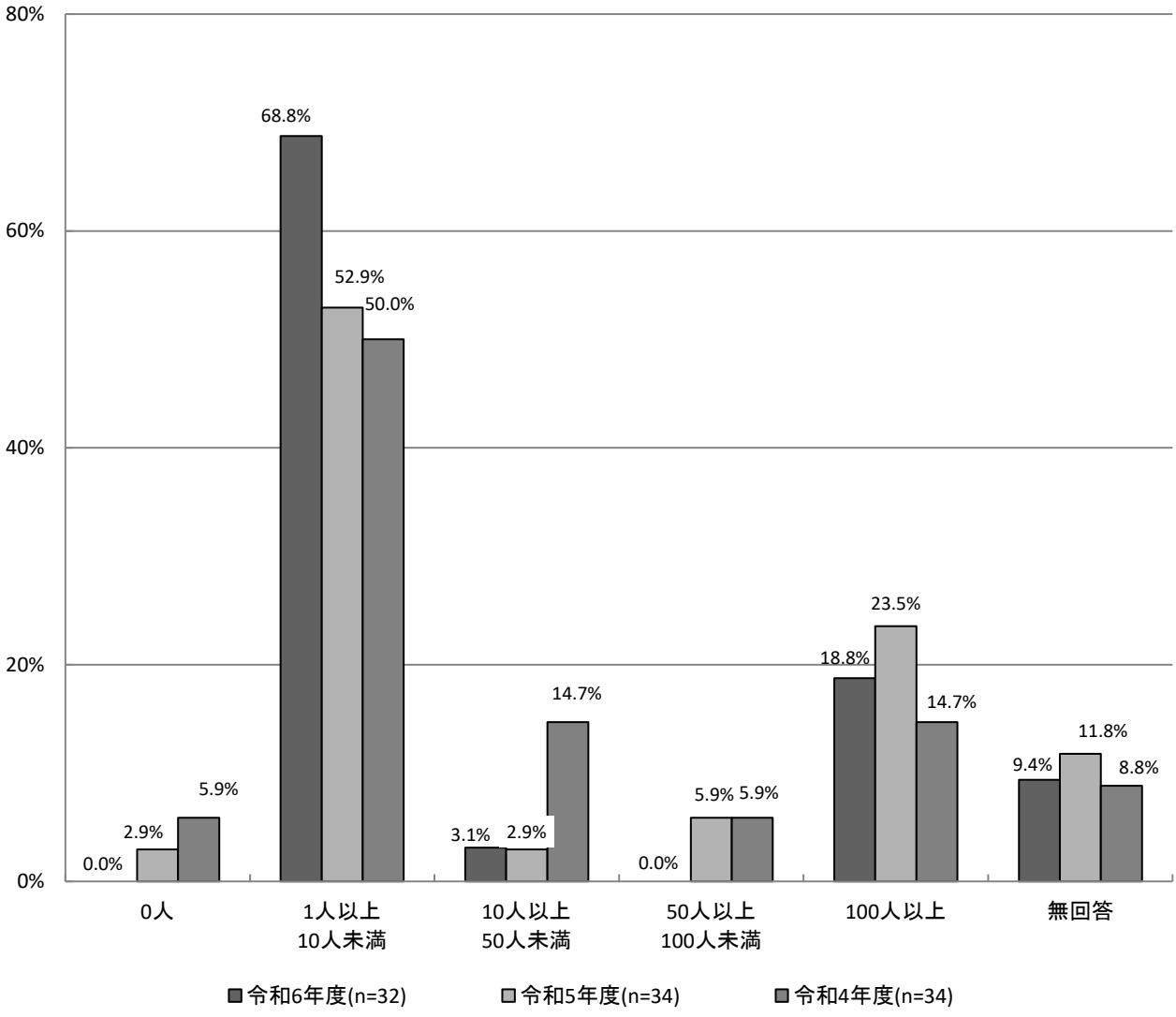


5.3.2　研究開発に携わっている人数　【A-問7】

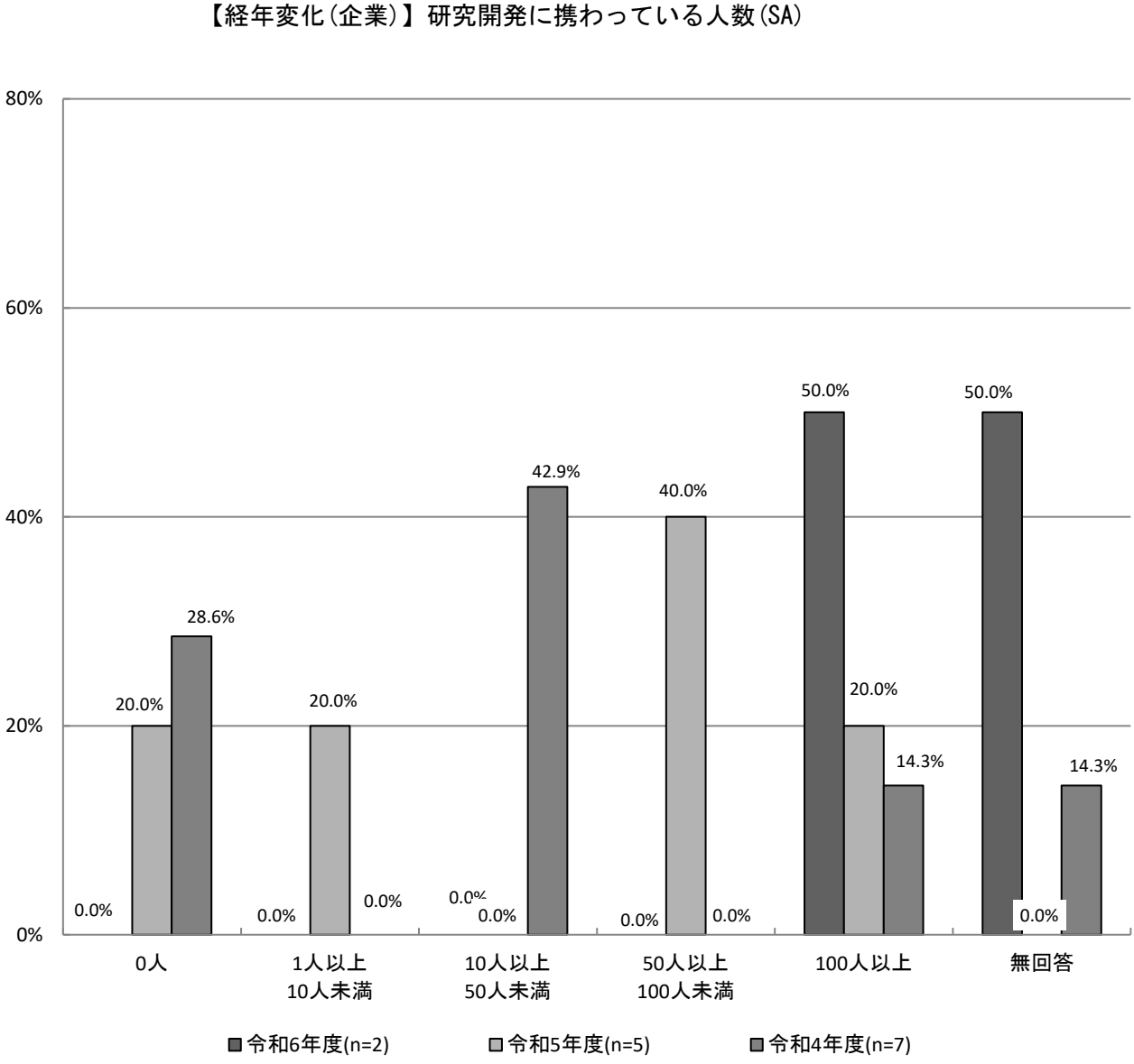
【経年変化】
　全体では、「1人以上10人未満」が最も増加している。企業では、「100人以上」が増加している。大学では、「1人以上10人未満」が増加している。

【経年変化(全体)】
　昨年度と比較すると全体では、「1人以上10人未満」が15.9ポイント増加している。一方、「50人以上100人未満」が5.9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)

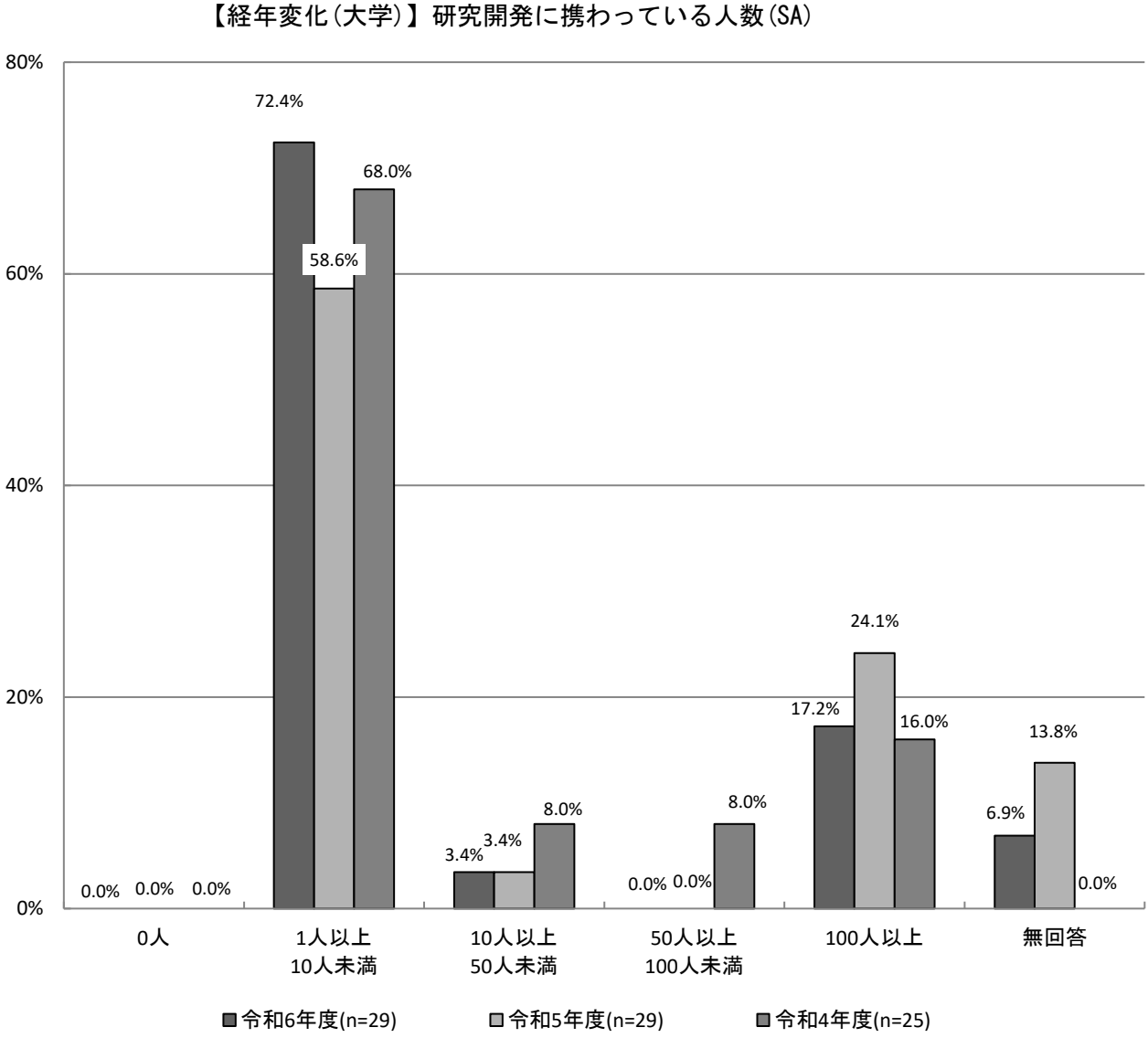


【経年変化(企業)】
　昨年度と比較すると企業では、「50人以上100人未満」が40.0ポイント減少している。一方、「100人以上」が30.0ポイント増加している。



【経年変化(大学)】

昨年度と比較すると大学では、「1人以上10人未満」が13.8ポイント増加している。一方、「100人以上」は6.9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。

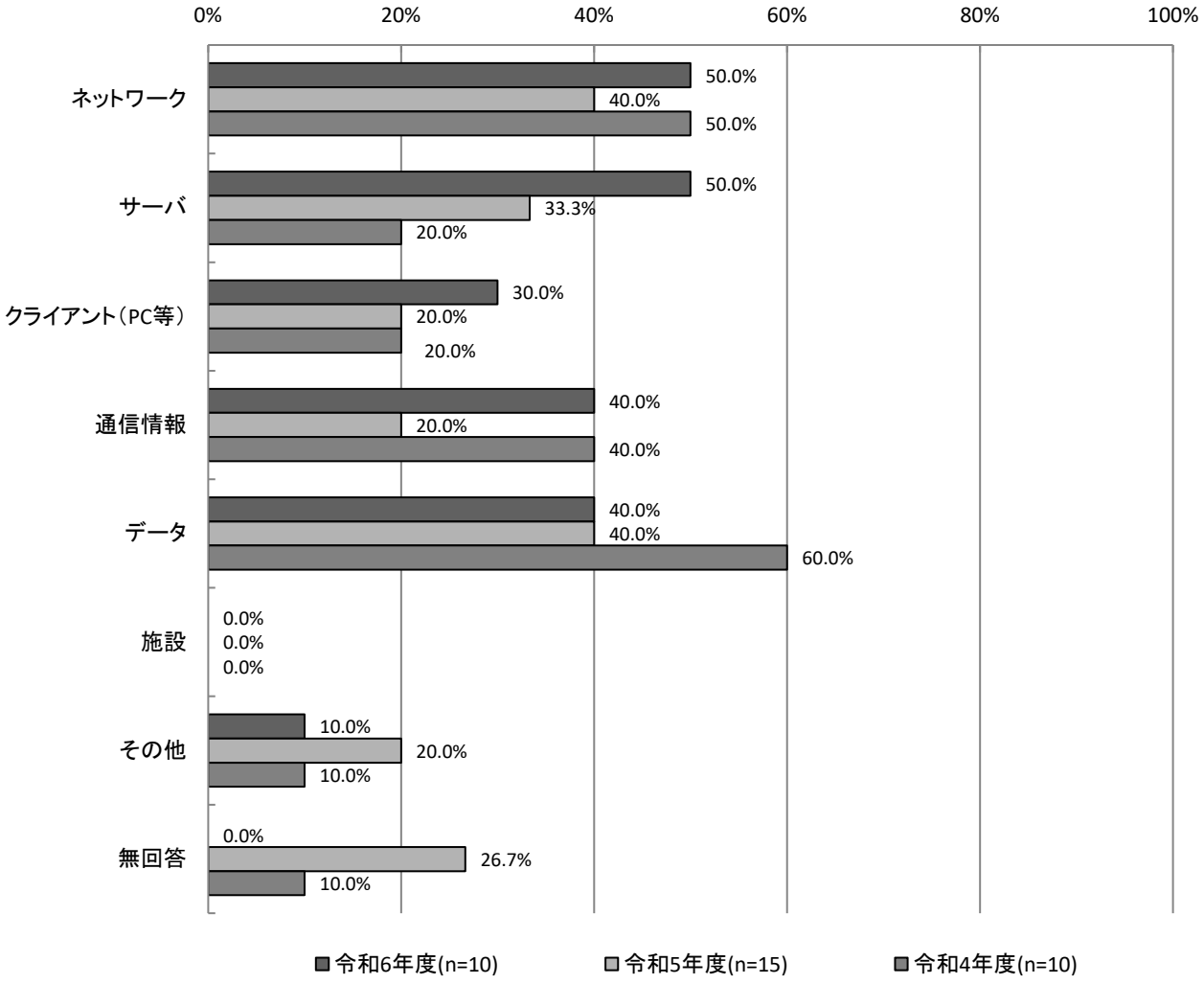
5.4.1　何を守るか？

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、「ネットワーク」「サーバ」がそれぞれ50.0%（5件）で最も多く、次いで「通信情報」「データ」がそれぞれ40.0%（4件）となっている。

昨年度と比較すると、「通信情報」が20.0ポイント増加している。

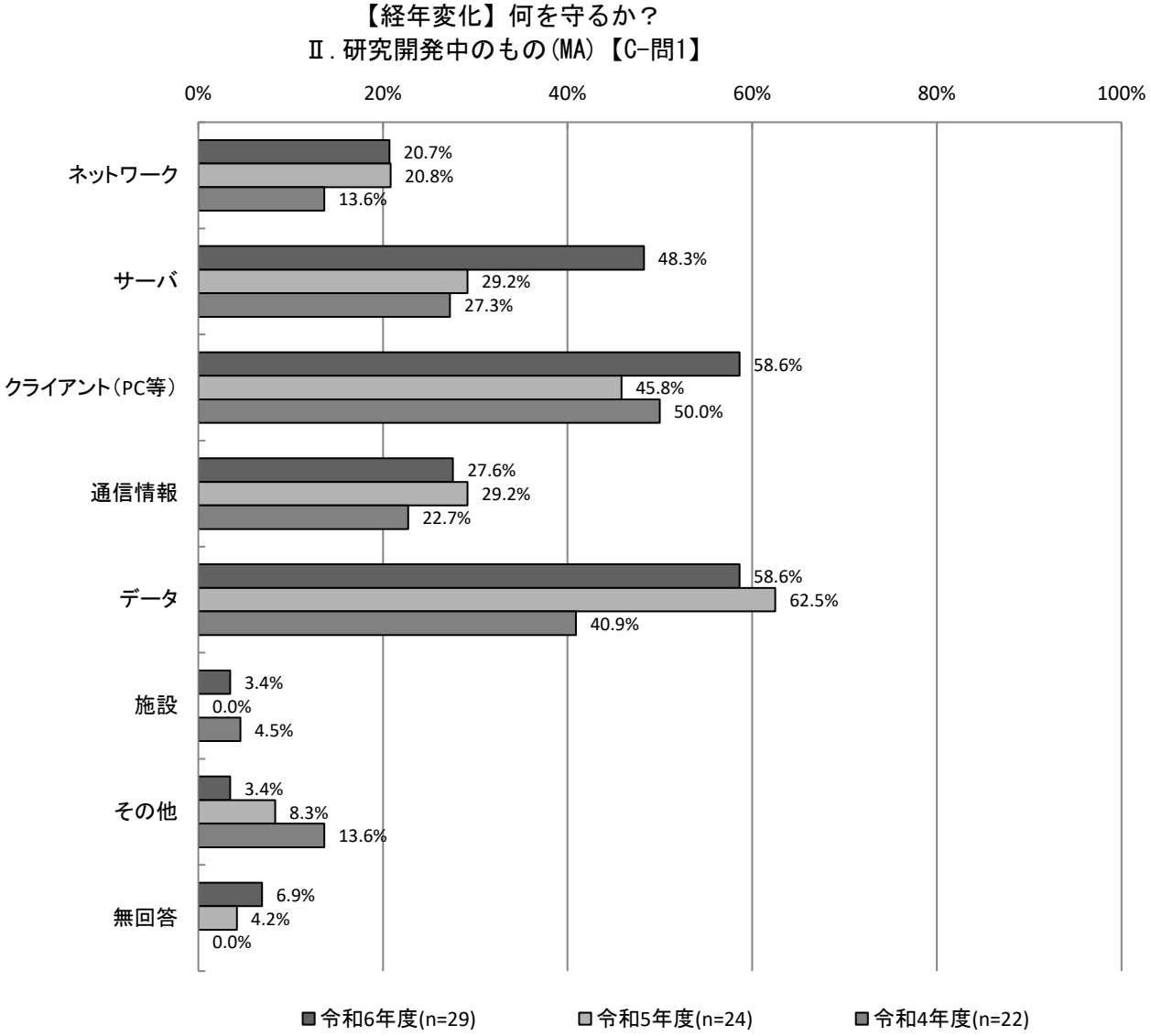
Ⅰ.実用化(製品化)されているもの(MA)【B-問1】



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）」「データ」が58.6%（17件）で最も多く、次いで「サーバ」が48.3%（14件）となっている。

昨年度と比較すると、「サーバ」が19.1ポイント増加している、一方で「データ」が3.9ポイント減少している。



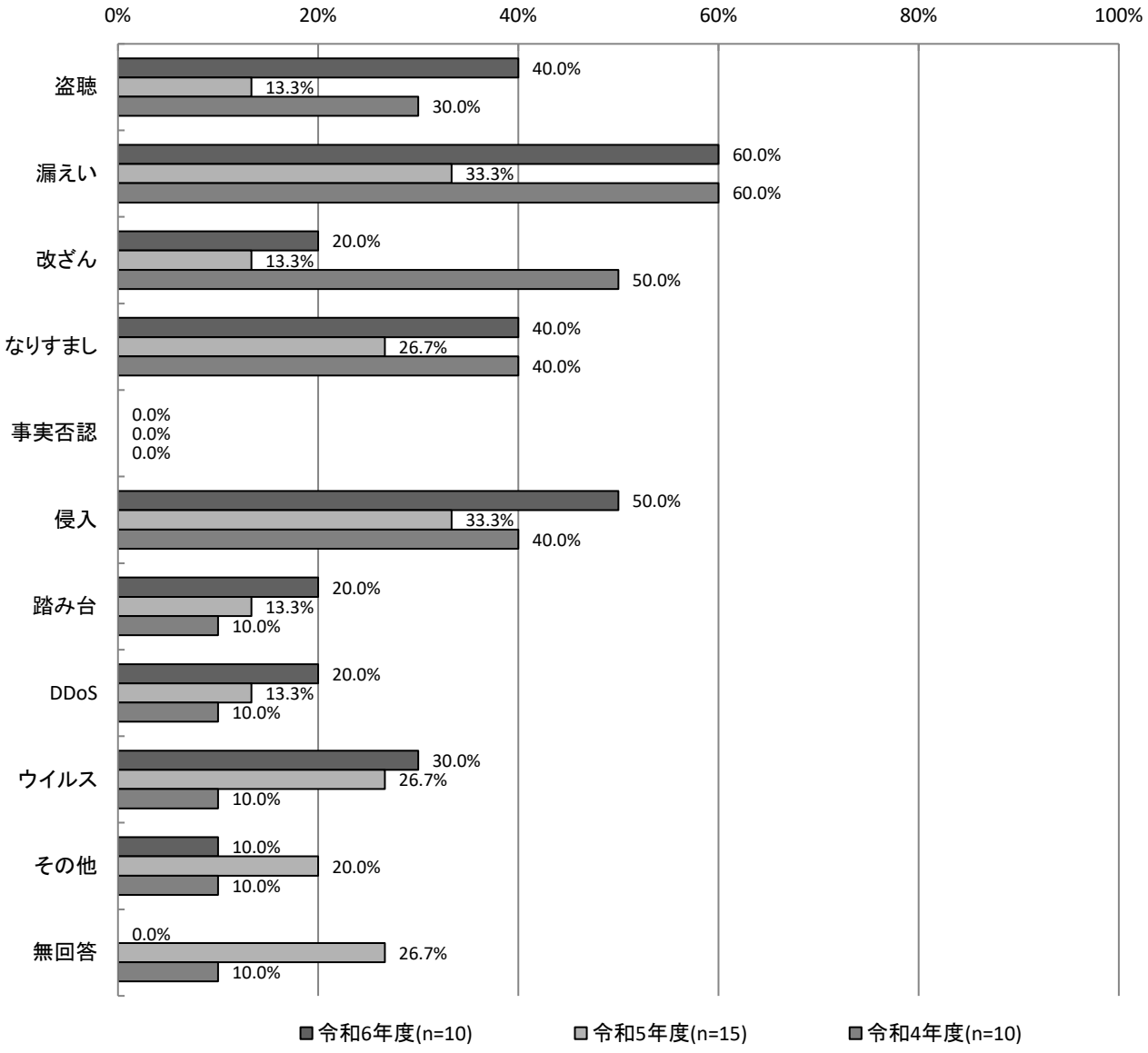
5.4.2　何から保護するか？

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「侵入」が50.0%（5件）となっている。

昨年度と比較すると、「盗聴」「漏えい」が26.7ポイント増加している。

【経年変化】何から保護するか？
Ⅰ.実用化(製品化)されているもの(MA)【B-問2】

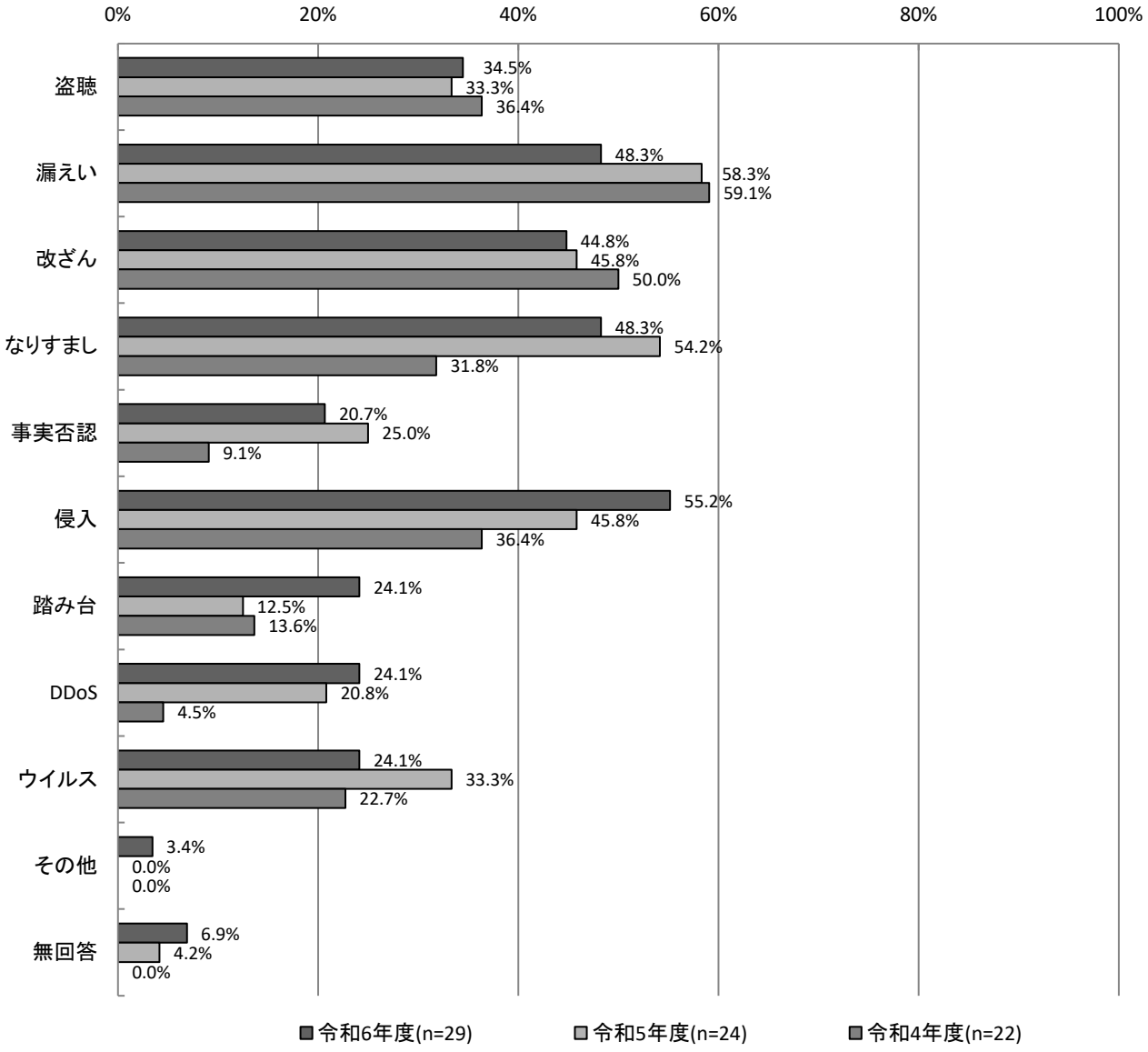


Ⅱ.研究開発中のもの

研究開発中のものについては、「侵入」が55.2%（16件）で最も多く、次いで「漏えい」「なりすまし」が48.3%（14件）となっている。

昨年度と比較すると、「踏み台」が11.6ポイント増加している。

【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】



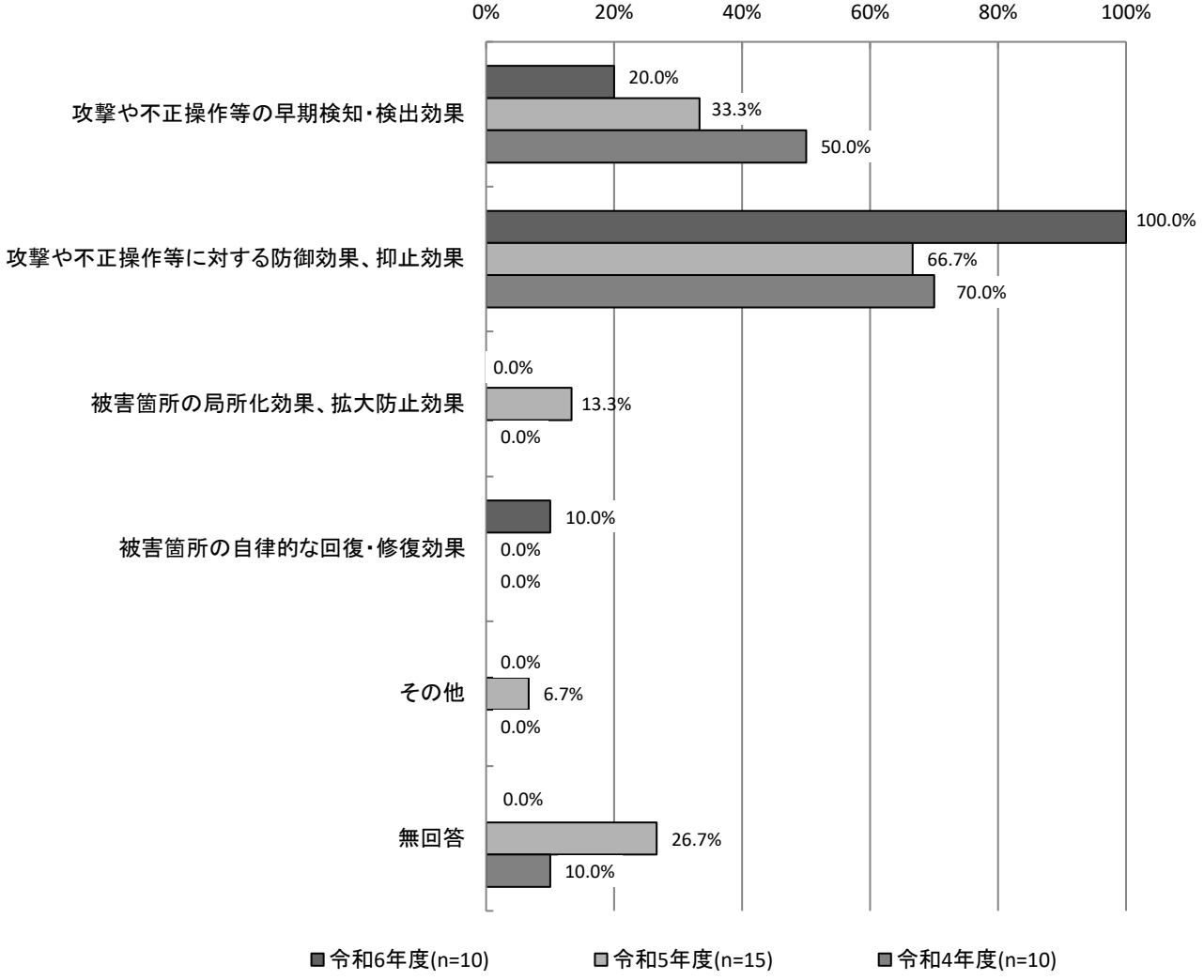
5.4.3　どのようなセキュリティ上の効果があるか？

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100.0%（10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33.3ポイント増加している。一方、「攻撃や不正操作等の早期検知・検出効果」「被害箇所の局所化効果、拡大防止効果」がそれぞれ13.3ポイント減少している。

【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】

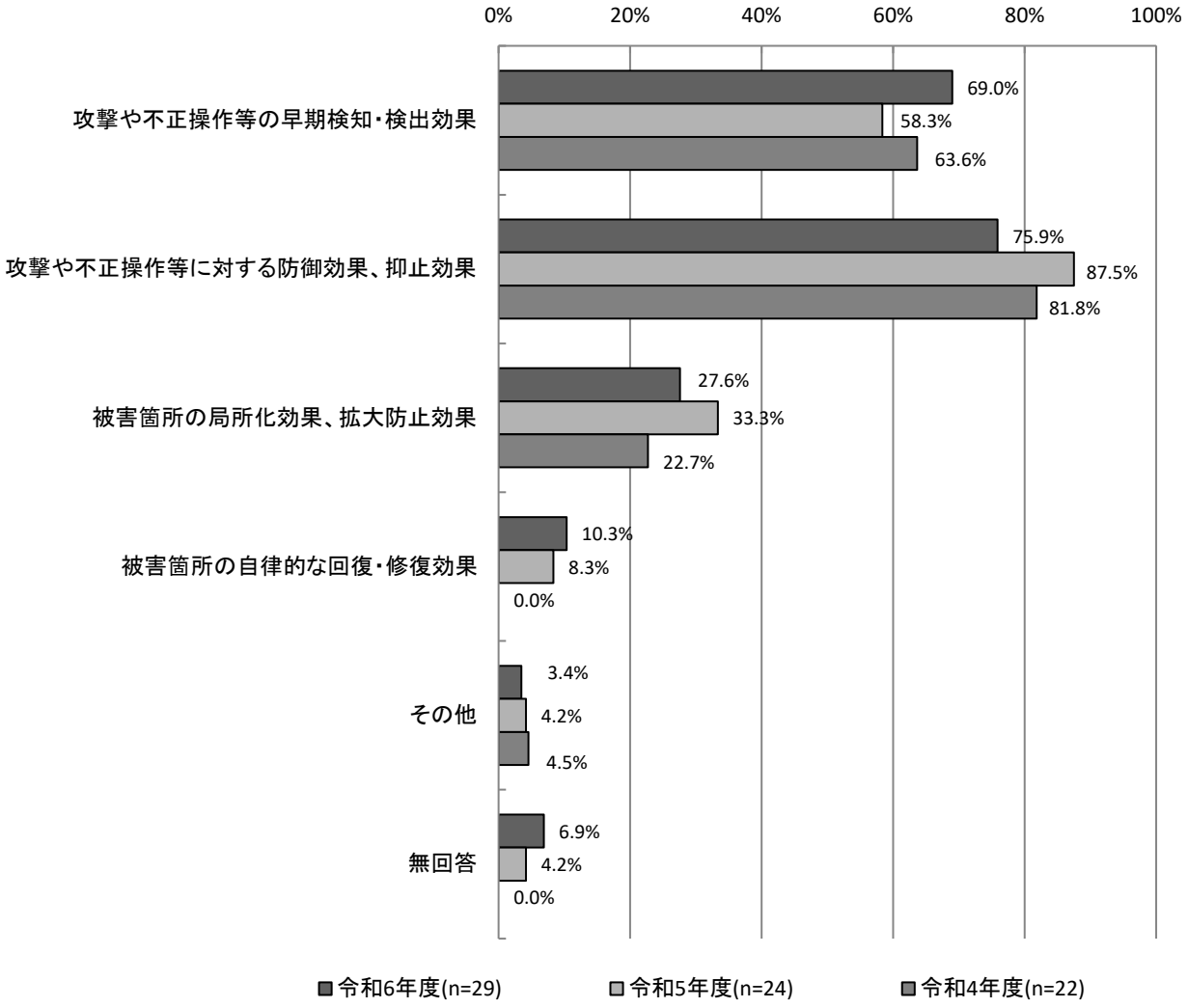


Ⅱ.研究開発中のもの

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75.9%（22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69.0%（20件）となっている。

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11.6ポイント、「被害箇所の局所化効果、拡大防止効果」が5.7ポイント減少している。一方、「攻撃や不正操作等の早期検知・検出効果」が10.7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】



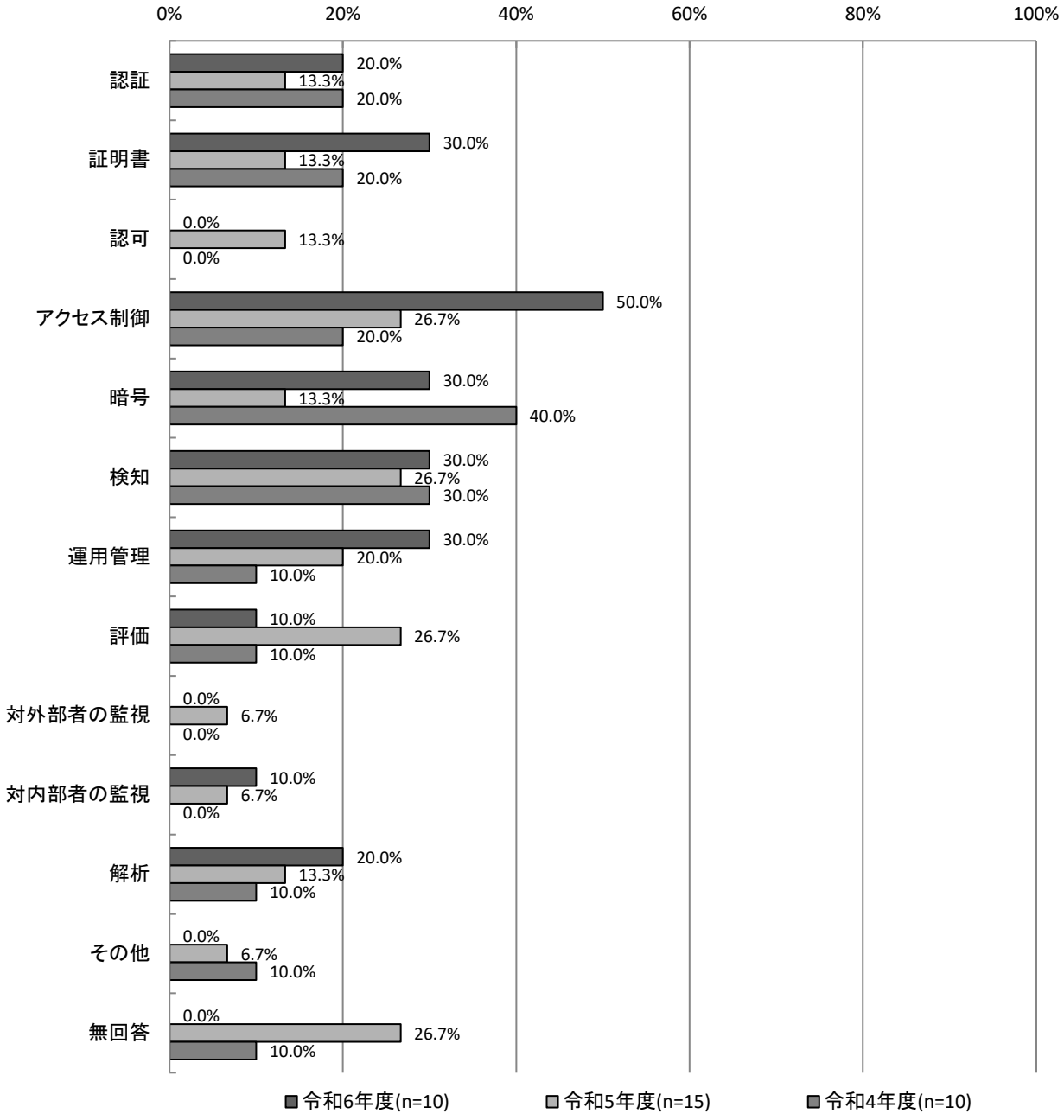
5.4.4　どのような機能を持つか？

Ⅰ.実用化(製品化)されているもの

研究開発中のものについては、「アクセス制御」が50.0%（5件）で最も多く、次いで「証明書」「暗号」「検知」「運用管理」が30.0%（3件）となっている。

昨年度と比較すると、「アクセス制御」が23.3ポイント増加している。

【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】

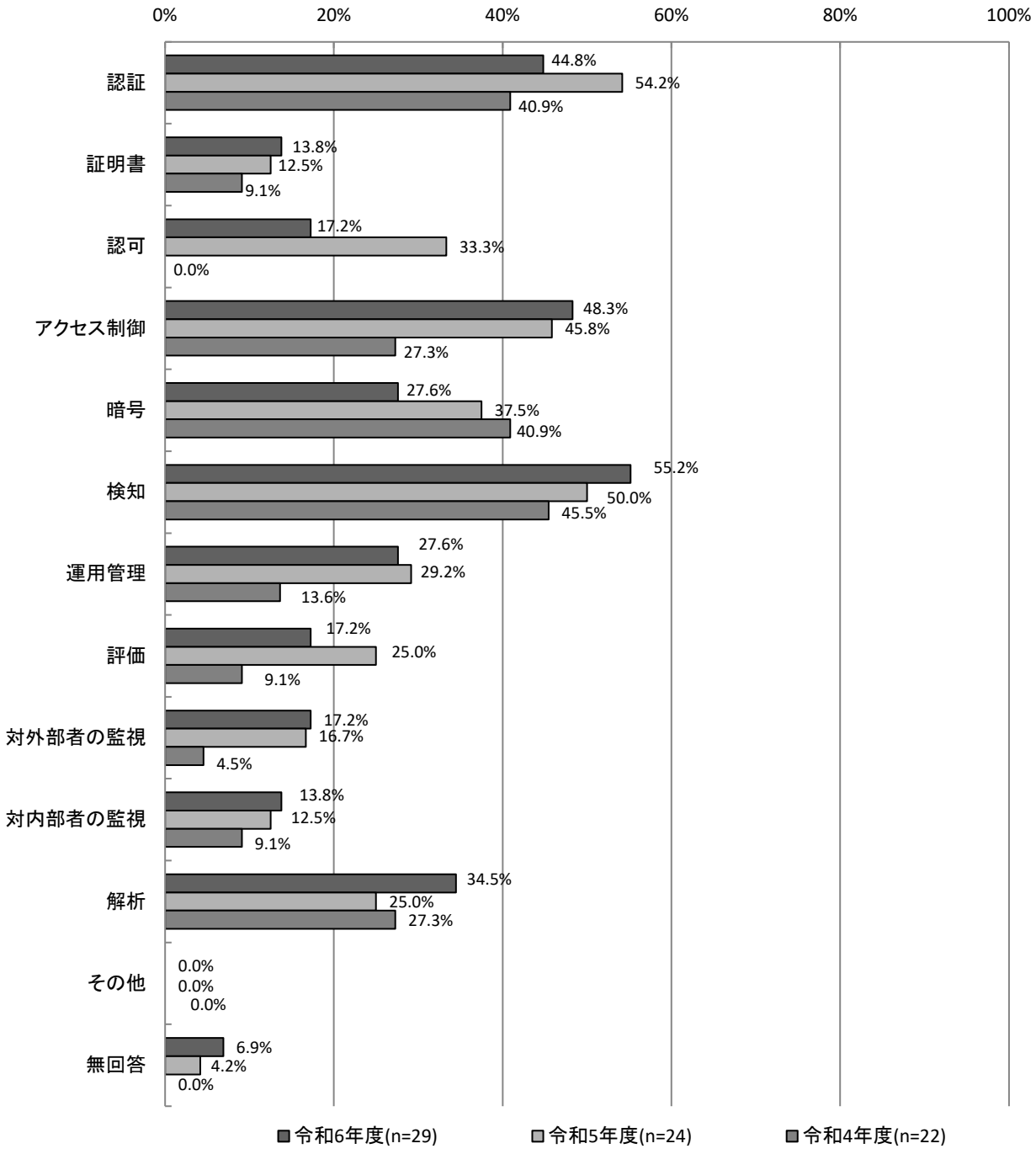


Ⅱ.研究開発中のもの

研究開発中のものについては、「検知」が55.2%（16件）で最も多く、次いで「アクセス制御」が48.3%（14件）となっている。

昨年度と比較すると、「認可」が16.1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？
Ⅱ.研究開発中のもの(MA)【C-問4】



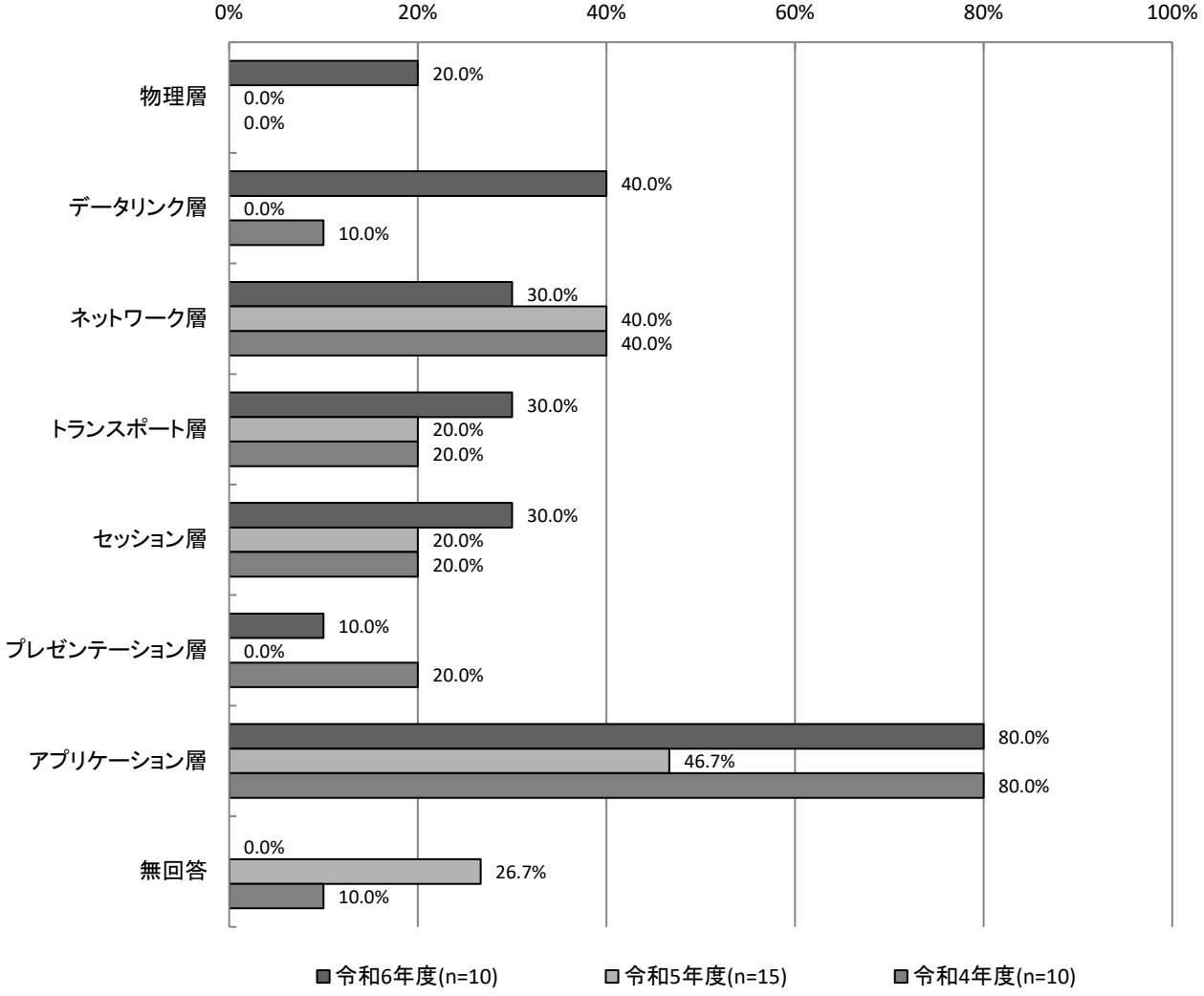
5.4.5　どのようなレイヤーのセキュリティを守るか？

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「データリンク層」が40.0%（4件）となっている。

昨年度と比較すると、「データリンク層」が40.0ポイント増加しており、次いで「アプリケーション層」が33.3ポイント増加している。

【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】

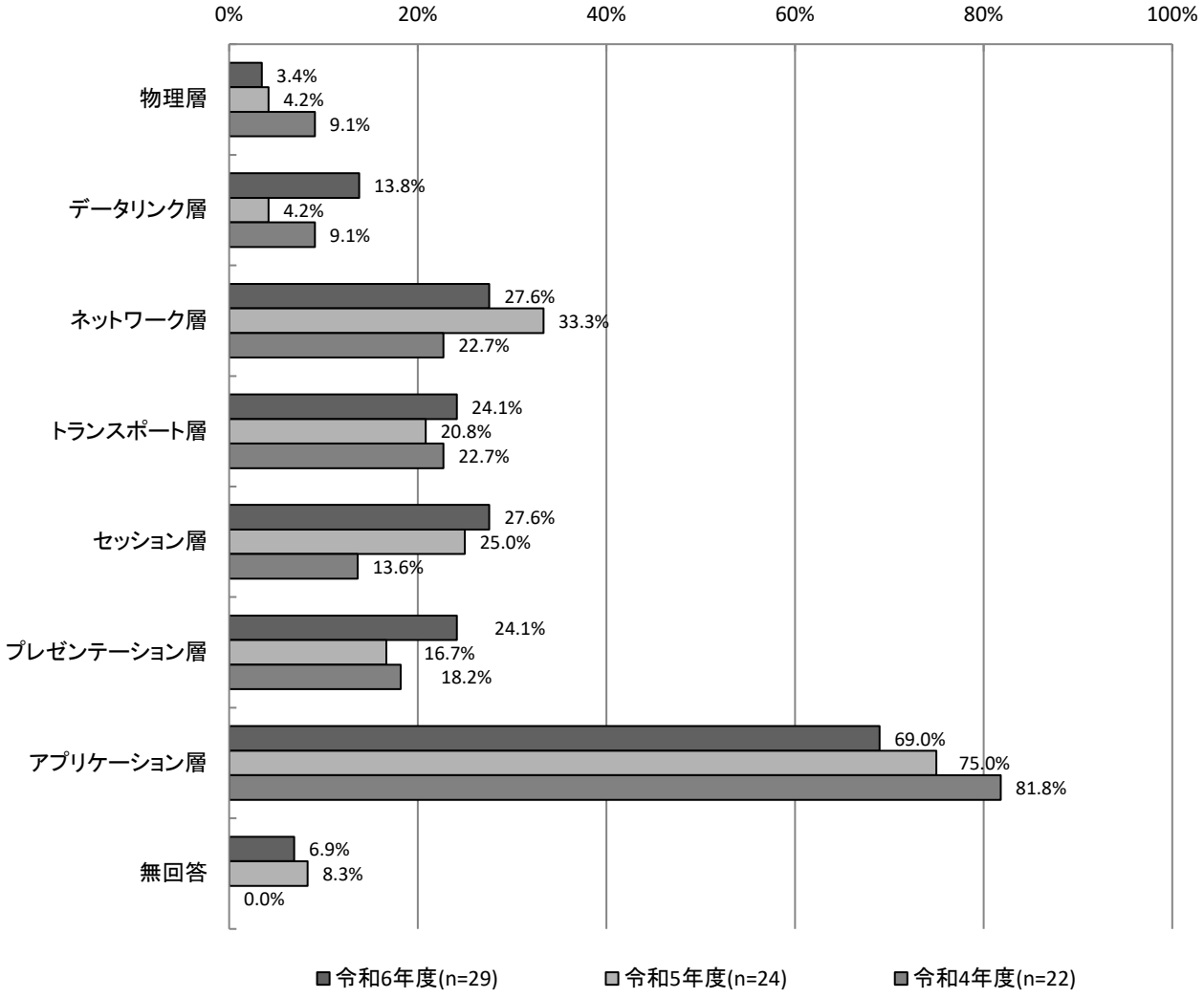


Ⅱ.研究開発中のもの

研究開発中のものについては、「アプリケーション層」が69.0%（20件）で最も多く、次いで「ネットワーク層」が27.6%（8件）となっている。

昨年度と比較すると、「データリンク層」が9.6ポイント、「プレゼンテーション層」が7.4ポイント増加している。一方、「アプリケーション層」が6.0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？
Ⅱ.研究開発中のもの(MA)【C-問5】



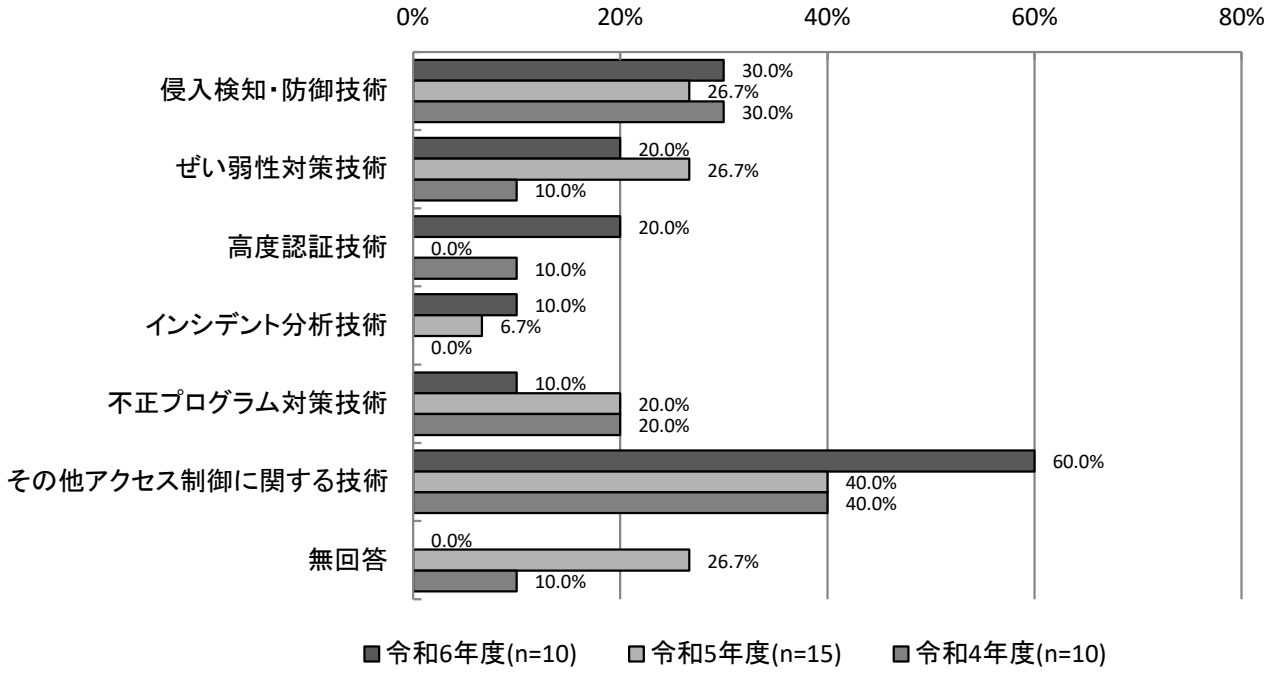
5.4.6　不正アクセスからの防御対象

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、「その他アクセス制御に関する技術」が60.0%（6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」「その他アクセス制御に関する技術」がそれぞれ20.0ポイント増加している。一方、「不正プログラム対策技術」が10.0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】

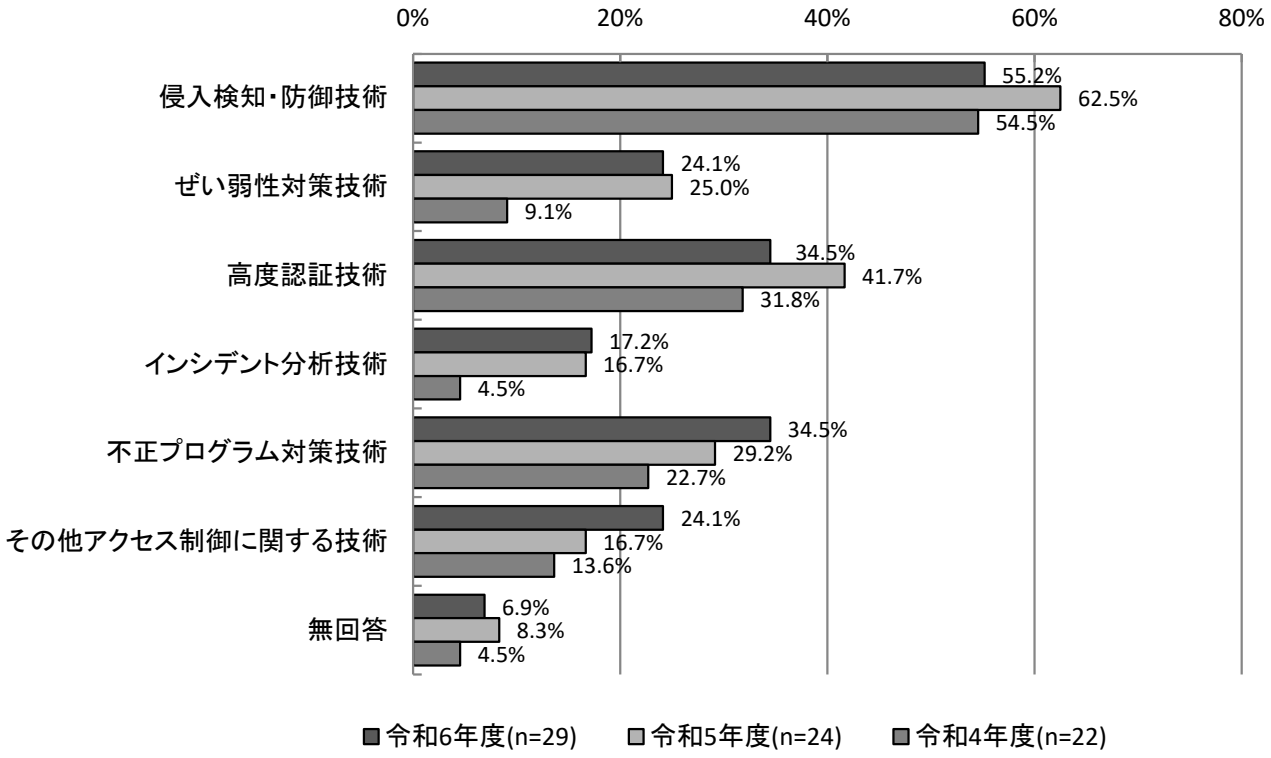


Ⅱ.研究開発中のもの

研究開発中のものについては、「侵入検知・防御技術」が55.2%（16件）で最も多くなっている。次いで、「高度認証技術」「不正プログラム対策技術」がそれぞれ34.5%（10件）となっている。

昨年度と比較すると、「侵入検知・防御技術」が7.3ポイント、「高度認証技術」が7.2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
Ⅱ.研究開発中のもの(MA)【C-問6】



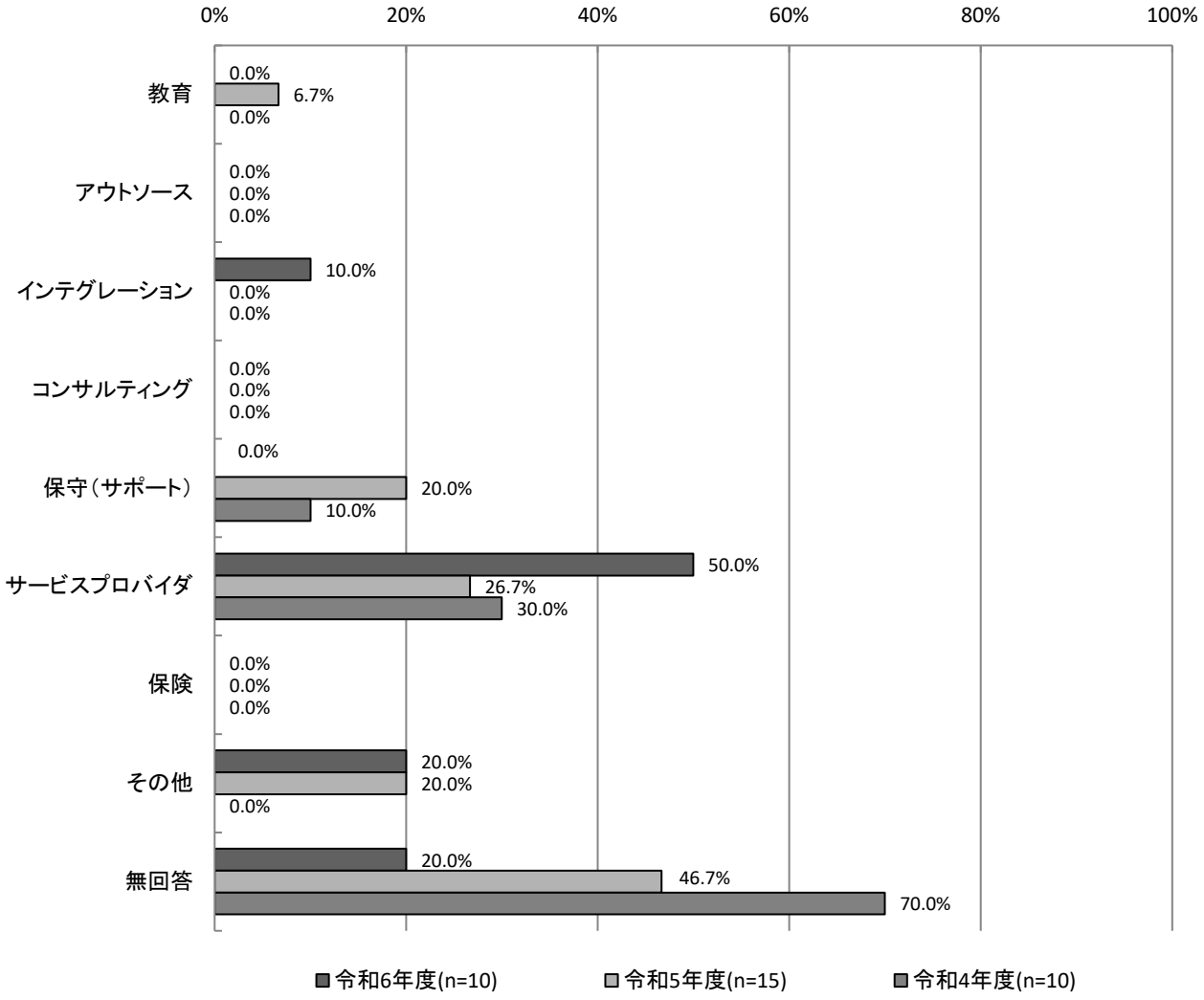
5.4.7　どのようなサービスか？

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50.0%（5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ポイント増加している。一方で、「保守（サポート）」が20.0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】

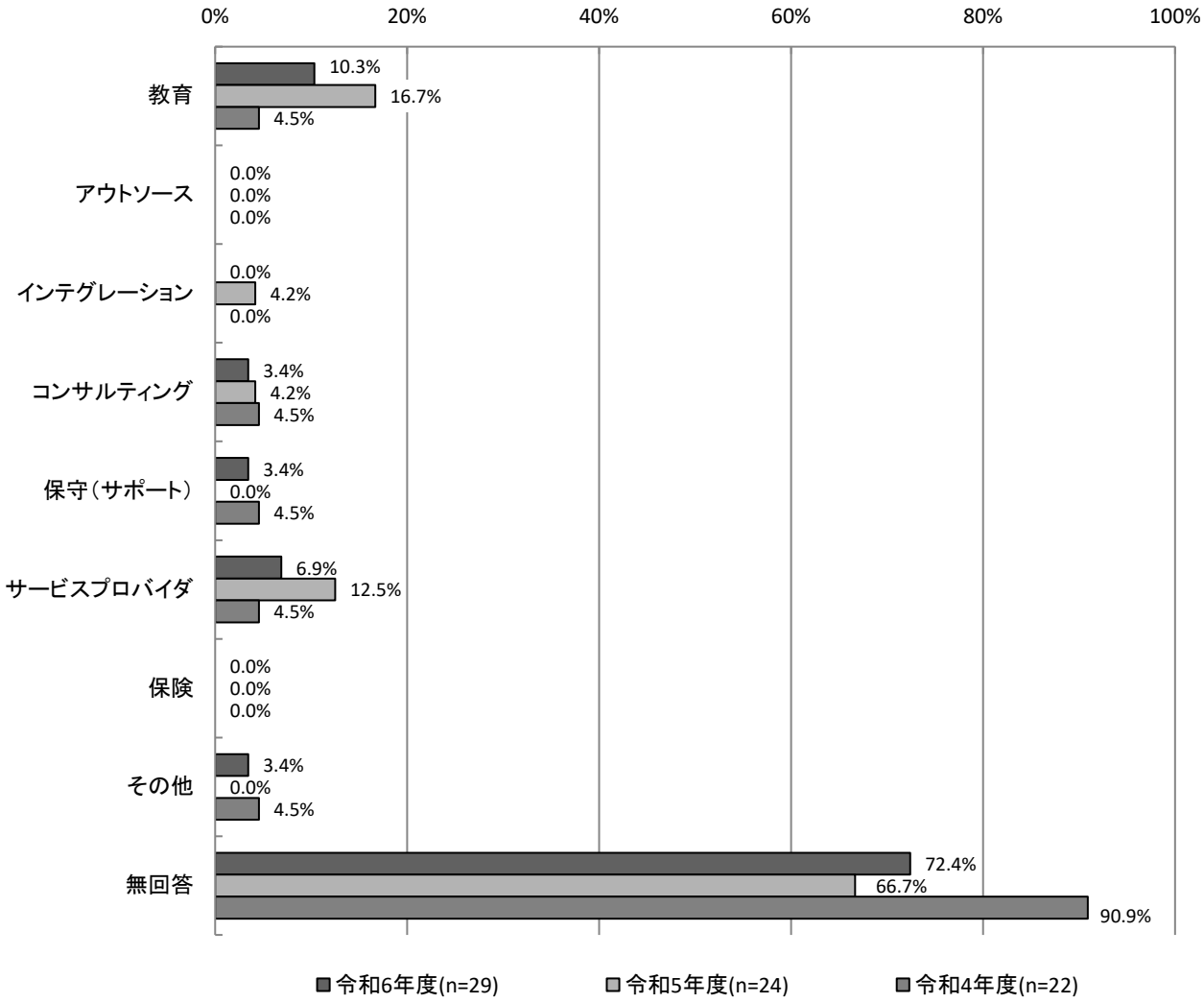


Ⅱ.研究開発中のもの

研究開発中のものについては、「教育」が10.3%（3件）となっている。

昨年度と比較すると、「教育」が6.4ポイント、「サービスプロバイダ」が5.6ポイント減少している。一方、「保守（サポート）」は3.4ポイント増加している。

【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】

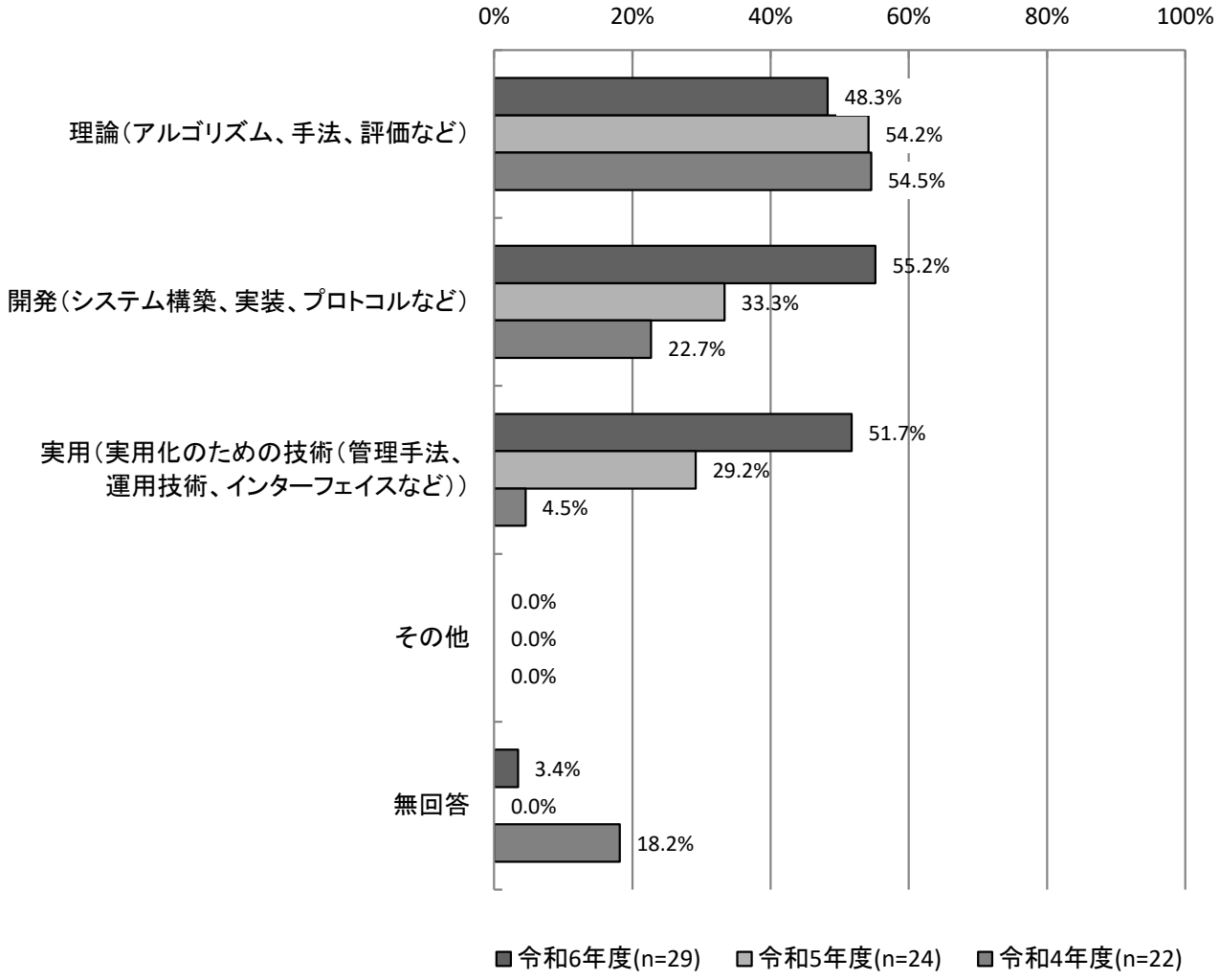


5.5 研究開発の成果としてどのようなものを目指しているか？

研究開発の目指す成果については、「開発（システム構築、実装、プロトコルなど)」が55.2%（16件）で最も多く、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51.7%（15件)、「理論（アルゴリズム、手法、評価など)」が48.3%（14件）となっている。

昨年度と比較すると、「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22.5ポイント増加しており、次いで「開発（システム構築、実装、プロトコルなど)」が21.9ポイント増加している。

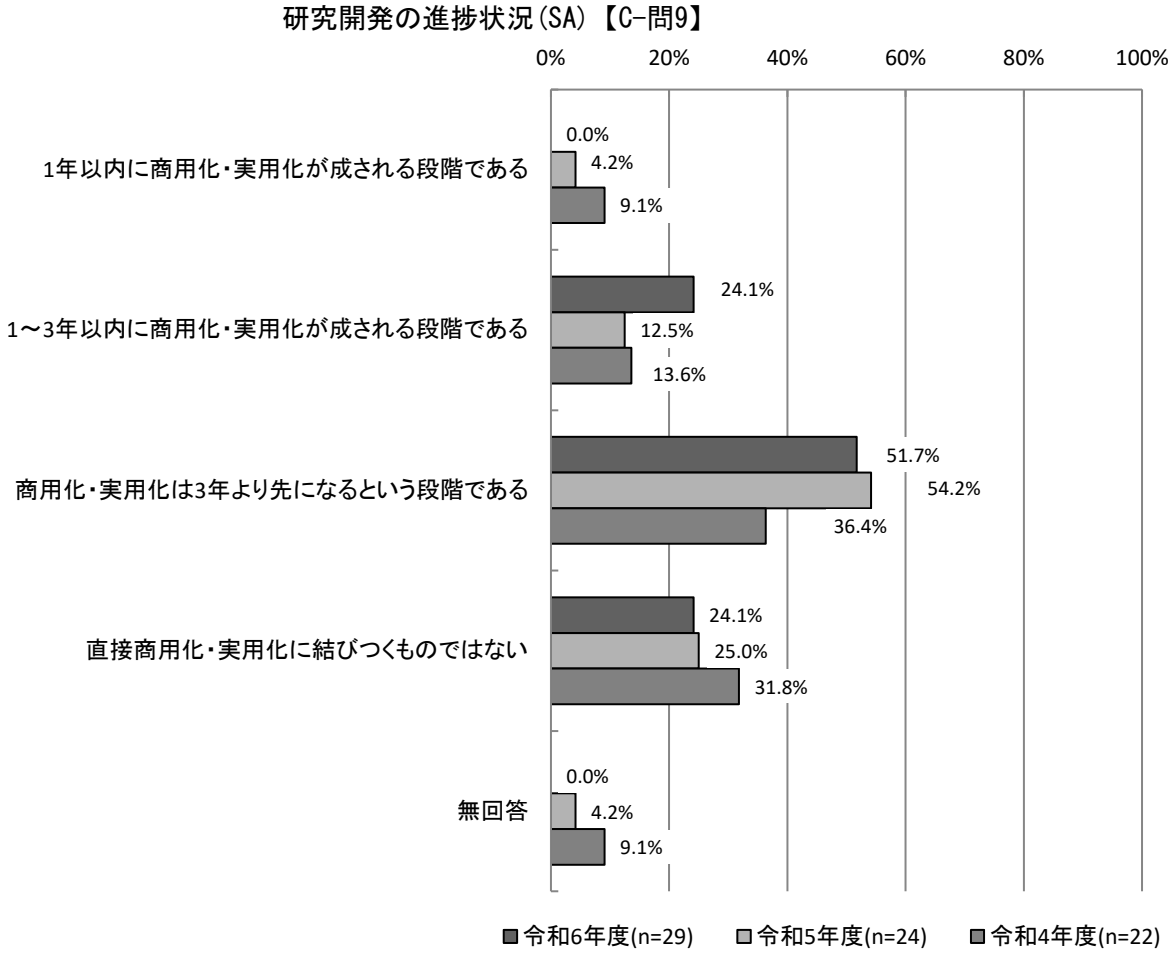
【経年変化】研究開発の成果として
どのようなものを目指しているか(MA)【C-問7】



5.6 研究開発の進捗状況

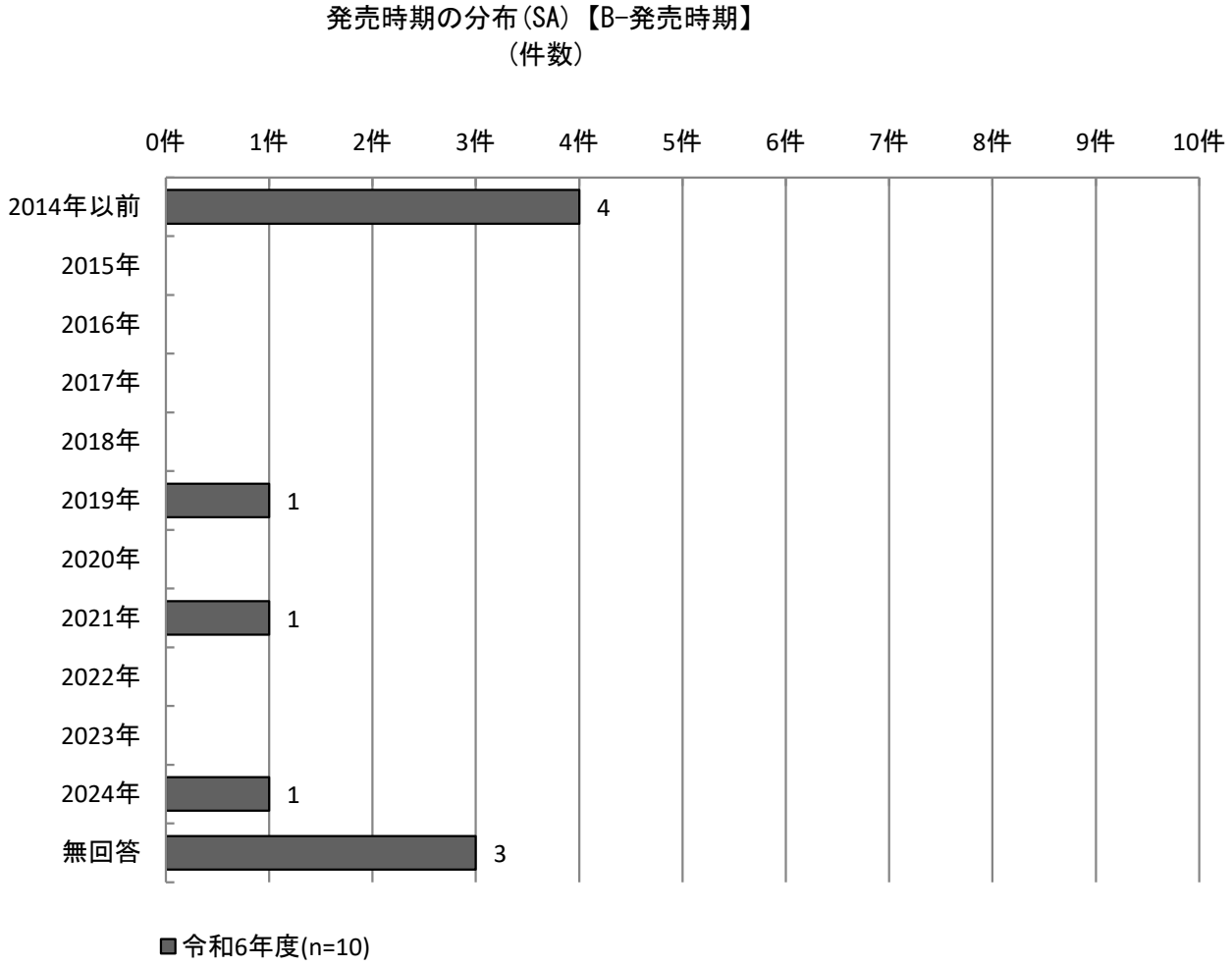
研究開発の進捗状況については、「商用化・実用化は3年より先になるという段階である」が51.7%（15件）と最も多い。次いで「1～3年以内に商用化・実用化が成される段階である」が24.1%（7件）となっている。

昨年度と比較すると、「1～3年以内に商用化・実用化が成される段階である」が11.6ポイント増加している。



5.7 発売時期の分布

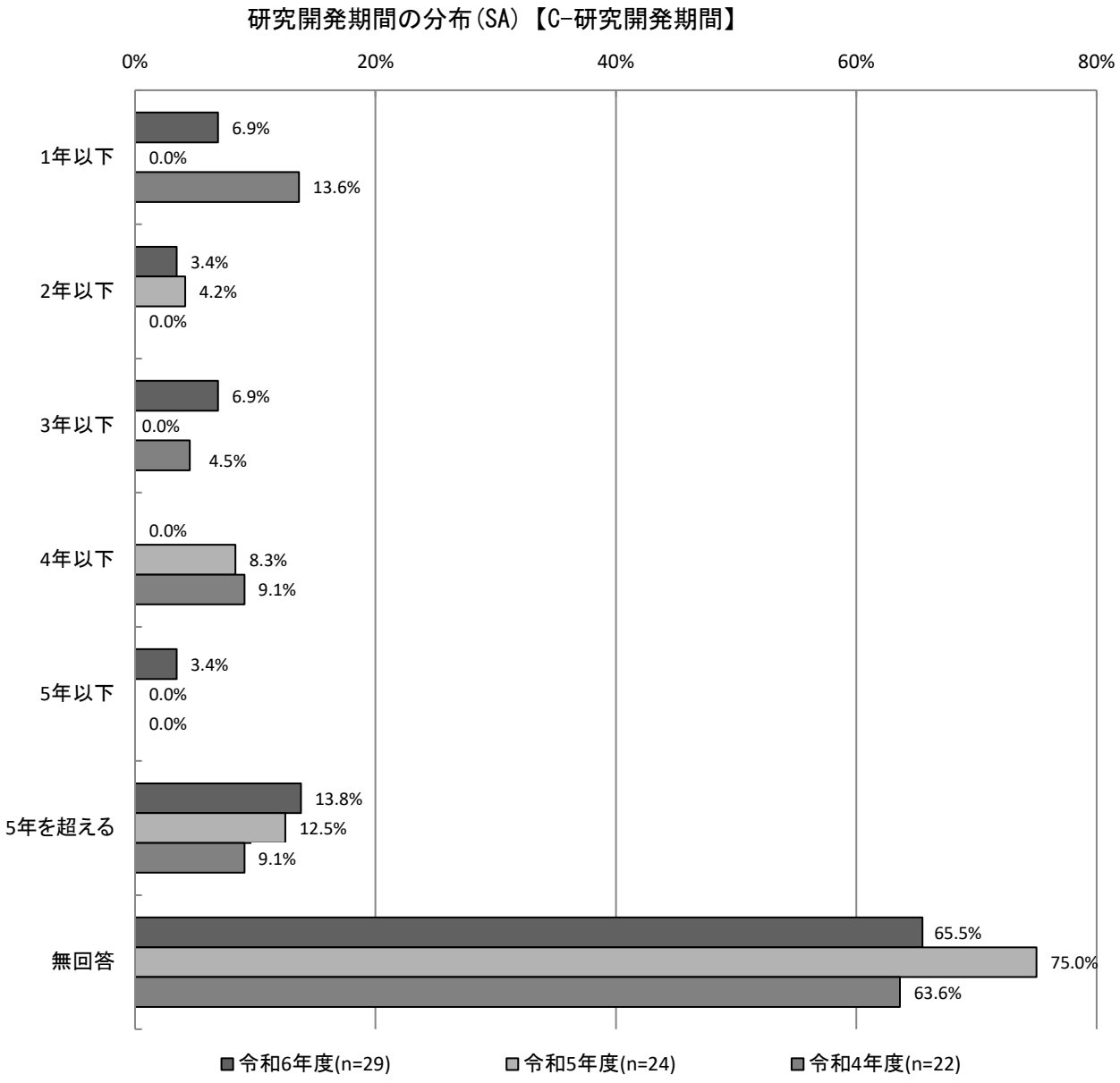
発売時期については、「2014年以前」が4件となっている。



5.8 研究開発期間の分布

研究開発期間については、「5年を超える」が13.8%（4件）で最も多く、次いで「1年以下」「3年以下」がそれぞれ6.9%（2件）となっている。

昨年度と比較すると、「4年以下」が8.3ポイント減少している。



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
Fit SDM	株式会社アイ・エス・ビー	(株)アイ・エスビー				○		
Soliton OneGate	株式会社ソリトンシステムズ	株式会社ソリトンシステムズ			○			
NetAttest EPS	株式会社ソリトンシステムズ	株式会社ソリトンシステムズ			○			
Microsoft AZURE	国立大学法人東海国立大学機構岐阜大学	Microsoft						○
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
セキュリティインテリジェンス提供サービス	国立大学法人 横浜国立大学	先端科学高等研究院　情報・物理セキュリティ研究ユニット						
USBメモリ紛失時の情報漏えい検知技術に関する研究開発	国立大学法人　琉球大学	工学部						○
高速処理と柔軟なポリシー記述を可能にする次世代フィルタの開発	公立大学法人前橋工科大学	-	○					○
CYPHONIC	学校法人名古屋電気学園愛知工業大学	情報科学部 情報科学科 モバイルコンピューティング研究室		○				
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	○					
情報危機管理教育サービス	和歌山大学	情報セキュリティ						
可読文字列と画像化技術を併用したマルウェア判別手法	明星大学 情報学部	情報学部 情報学科 丸山研究室					○	
覗き見耐性を持つジャイロと音を用いた認証手法	明星大学 情報学部	情報学部 情報学科 丸山研究室			○			
暗号技術・認証技術	明星大学 情報学部	情報学部　情報学科　小暮研究室	○		○			
オープンイノベーションサーバー	国立大学法人東海国立大学機構岐阜大学	研究推進部						○
(特にプロジェクト名は無い)	国立大学法人東海国立大学機構名古屋大学	情報学研究科 情報システム学専攻 嶋田研究室	○			○	○	○
高度生体認証システム	公立大学法人北九州市立大学	情報システム工学科　山崎恭研究室	○		○			
非記号情報による環境状況推定	日本文理大学	日本文理大学・工学部・情報メディア学科	○		○			
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			○			
情報システムに対する攻撃・不正アクセスの予測・検知・防御・分析・可視化に関する基盤技術の確立	東京情報大学	総合情報学部 共創ラボ（ネットワーク・セキュリティLab）	○	○		○	○	
生体から得られる電磁気情報を用いた個人認証システム	日本大学	理工学部応用情報工学科	○	○	○		○	
ブロックチェーン技術を用いた単一医療機関向け診療記録システム	日本大学	理工学部応用情報工学科	○	○	○		○	
標的型メール対策訓練支援システム	日本大学	理工学部応用情報工学科	○	○	○	○	○	
デジタルフォレンジック技術の学習支援システム	日本大学	理工学部応用情報工学科	○	○	○	○	○	
ネットワークトラフィック及びログ解析に基づく異常検知	公立大学法人大阪	情報学研究科	○					

※ 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	株式会社アイ・エス・ビー
代表者名	代表取締役社長　岩尾一史
所在地	141-0032 東京都品川区大崎5-1-11
窓口部署名	総務部
電話番号	03-3490-1761
ホームページのURL	https://www.isb.co.jp
対象技術	技術の概要・特徴など
製品名： Fit SDM 開発元（メーカー名等）： (株)アイ･エスビー 開発国： 価格： 150円～800円/月額 発売時期： 出荷数： 	MDMです　クライドサービスとして提供

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	株式会社ソリトンシステムズ
代表者名	鎌田 理
所在地	160-0022 東京都新宿区新宿２－４－３
窓口部署名	ITセキュリティ事業部
電話番号	03-5360-3811
ホームページのURL	https://www.soliton.co.jp/
対象技術	技術の概要・特徴など
製品名： Soliton OneGate 開発元(メーカー名等)： 株式会社ソリトンシステムズ 開発国： 日本 価格： PKIプラン 100円/月、Basicプラン 300円/月、Standardプラン 600円/月など。詳細はお問い合わせください。 発売時期： 2019年12月2日 出荷数： 非開示	Soliton OneGateは、デジタル証明書をはじめとする多彩な多要素認証（MFA）とシングルサインオン（SSO）でクラウドに点在する組織の情報資産を不正アクセスから守る、多要素認証サービスです。 クラウドからデータを持ち出さずに活用することができるセキュアブラウザ機能を使った「データ保護」（情報漏えい対策）や、セキュアな無線LAN認証やVPN/SASE認証の強化、Windowsサインインの認証強化にも対応し、セキュリティ強化で組織のDX推進を支援します。 ※政府情報システムのためのセキュリティ評価制度（ISMAP）に登録済み。

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	株式会社ソリトンシステムズ
代表者名	鎌田 理
所在地	160-0022 東京都新宿区新宿２－４－３
窓口部署名	ITセキュリティ事業部
電話番号	03-5360-3811
ホームページのURL	https://www.soliton.co.jp/
対象技術	技術の概要・特徴など
製品名： NetAttest EPS 開発元(メーカー名等)： 株式会社ソリトンシステムズ 開発国： 日本 価格： NetAttest EPS(EPS-SX15A-Aモデル) 定価23万円～、物理・仮想アプライアンスで複数のラインナップがあり、ご利用機能に応じたライセンスと保守費用が必要です。詳細はお問い合わせください。 発売時期： 2002年 出荷数： 累計33,000台以上	NetAttest EPSは、オールインワン認証アプライアンスです。ネットワーク機器と連携して強固な認証環境を実現し、悪意ある攻撃者の不正侵入をシャットアウトします。 デジタル証明書を利用したネットワーク認証に必要となる機能を搭載し、正しい端末・正しいユーザーのみネットワークに接続できる安全な環境を実現することができます。無線LANセキュリティとして求められているIEEE802.1XのEAP-TLS認証、VPNの多要素認証（MFA）を実現する認証サーバーとして、多くの実績があります。

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	国立大学法人東海国立大学機構岐阜大学
代表者名	松尾　清一
所在地	501-1193 岐阜市柳戸１－１
窓口部署名	研究推進部研究推進課
電話番号	058-293-3140
ホームページのURL	https://ari.gifu-u.ac.jp/
対象技術	技術の概要・特徴など
製品名： Microsoft AZURE 開発元(メーカー名等)： Microsoft 開発国： アメリカ 価格： https://azure.microsoft.com/ja-jp/pricing/details/cognitive-services/openai-service/?msockid=2c44f817717566f51281eb5a70fe6745 発売時期： 2010年1月1日 出荷数： 増加中 https://www.nikkei.com/article/DGXZQOGN27EC70X20C21A7000000/?msockid=2c44f817717566f51281eb5a70fe6745	https://azure.microsoft.com/ja-jp/

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	
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： 現在は無料 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は下記のとおり。 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	国立大学法人 横浜国立大学
代表者名	学長　梅原　出
所在地	240-8501 横浜市保土ヶ谷区常盤台79-1
窓口部署名	研究・学術情報部　情報企画課　情報企画係
電話番号	045-339-4472
関連部門名	先端科学高等研究院　情報・物理セキュリティ研究ユニット
ホームページのURL	https://www.ynu.ac.jp/
研究説明のURL	https://sec.ynu.codes/iot/ https://sec.ynu.codes/dos http://yoshioka.ynu.ac.jp/research.html https://ipsr.ynu.ac.jp/outcome.html
対象技術	研究開発状況
研究開発名称： セキュリティインテリジェンス提供サービス 研究開発国： 日本 研究開発時期： 2015年1月1日～2025年12月31日	サイバー攻撃やその原因となっている脅威アクターの動向をインターネット上のクロールやハニーポットにより観測し、情報を蓄積しており、そのデータを外部に提供する形でのサービスを提供する可能性がある。ハニーポットによる観測は９年間の研究開発を行っており、脅威アクタ分析については2022年度から開発を実施している。

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	国立大学法人　琉球大学
代表者名	西田　睦
所在地	903-0213 沖縄県中頭郡西原町字千原１
窓口部署名	工学部総務係
電話番号	098-895-8589
関連部門名	工学部
ホームページのURL	https://www.tec.u-ryukyu.ac.jp/
研究説明のURL	
対象技術	研究開発状況
研究開発名称： USBメモリ紛失時の情報漏えい検知技術に関する研究開発 研究開発国： 日本 研究開発時期： 2024年4月1日～	USBメモリを紛失して拾得された際に、デバイス内の情報にアクセスされたことを検知する技術を研究している。 現在その有効性やユースシーンについて情報収集、検証を行っている。

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	公立大学法人前橋工科大学
代表者名	理事長　福田尚久
所在地	371-0816 群馬県前橋市上佐鳥町460番地1
窓口部署名	学務課　地域貢献・研究支援係
電話番号	027-265-7361
関連部門名	-
ホームページのURL	https://www.maebashi-it.ac.jp/
研究説明のURL	https://kaken.nii.ac.jp/ja/grant/KAKENHI-PROJECT-23K11104/
対象技術	研究開発状況
研究開発名称： 高速処理と柔軟なポリシー記述を可能にする次世代フィルタの開発 研究開発国： 日本 研究開発時期： 2023年4月1日～2026年3月31日	パケット分類アルゴリズムの開発状況について、現在、領域分割アルゴリズムと連分割トライアルゴリズムとの融合に関する実装を完了している段階である。提案アルゴリズムについて、理論的な評価では、非常に高速な分類処理速度を達成している一方で、ランダムに抽出したデータで構成される疑似ネットワーク環境において要求メモリ量が莫大であり、実用上問題がある段階である。今後は、実際のネットワーク環境を模倣した作成されたデータを使用して、提案アルゴリズムの調整を進めていく予定である。

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	
その他アクセス制御に関する技術	○

企業・大学名	学校法人名古屋電気学園愛知工業大学
代表者名	後藤 泰之
所在地	470-0392 愛知県豊田市八草町八千草1247
窓口部署名	総務課
電話番号	0565-48-8121
関連部門名	情報科学部 情報科学科 モバイルコンピューティング研究室
ホームページのURL	https://www.ait.ac.jp/
研究説明のURL	https://researchmap.jp/katsuhiro.naito/published_papers
対象技術	研究開発状況
研究開発名称： CYPHONIC 研究開発国： 日本 研究開発時期： 2018年4月1日～	管理クラウド機能と端末機能の実装は概念実証は終えておりマネージメント機能の強化及びクラウド側のDDoS対策などを検討中

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	学校法人　東北工業大学
代表者名	樋口　龍雄
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	研究開発状況
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～	要素技術としてLinuxカーネルに搭載されているeBPF（extended Berkeley Packet Filter）に着目している．eBPFは，デバイスの様々な情報を精密に監視する手段として近年注目されている．現在は，eBPFを活用し，通信情報を構成するパケットと、パケットを送受信したアプリケーションを関連付けるシステムの実現性と有効性を検証している．今後，パケットに関連付けられたアプリケーション情報を利用した，柔軟かつ細粒度なアクセス制御システムの開発を進める．

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	和歌山大学
代表者名	
所在地	640-8510 和歌山県和歌山市栄谷930
窓口部署名	
電話番号	
関連部門名	情報セキュリティ
ホームページのURL	https://www.wakayama-u.ac.jp/
研究説明のURL	（なし）
対象技術	研究開発状況
研究開発名称： 情報危機管理教育サービス 研究開発国： 日本 研究開発時期： 2024年4月1日～2026年3月31日	当方は、「情報危機管理コンテスト」を19年間実施しており、その運用を担当している。当該コンテストは、情報セキュリティに関するインシデントを当方が発生させ、コンテスト参加側がインシデント対応し、その技量を競うものである。 上記コンテスト運用は、一種の教育システムとして設計しており、和歌山大学内外での情報セキュリティ実践演習としても活用している。しかし、同様にリソースの限度によって展開が困難となっており、これを解決するための研究開発としている。 現在、クラウド化について、いくつかのインシデント・シナリオを実装しており、現在は生成AIによる人的資源のリプレースを設計している。今後は、100人を受け入れるためのシステム設計、インタフェースの開発を実施する予定である。

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	
その他アクセス制御に関する技術	

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	明星大学　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 丸山研究室
ホームページのURL	（明星大学情報学部） https://www.is.meisei-u.ac.jp/ （明星大学） https://www.meisei-u.ac.jp/
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 可読文字列と画像化技術を併用したマルウェア判別手法 研究開発国： 日本 研究開発時期： 2024年6月～	マルウェア解析における表層解析は，補助的な役割に限定して利用されてきた．ファイルの可読文字列やバイナリデータなどを調査する表層解析は，実際にマルウェアを動かしているわけではない．そのため，解析にかかる時間が短く，簡単に行うことができる一方，得られる情報が少ない．しかし，自然言語処理技術や深層学習などの発達により，表層解析は再評価された．現在では，可読文字列やバイナリデータなど表層解析から得られる情報のみを利用して，マルウェアの検知や分類を行う手法が提案されている． 本研究では，可読文字列と画像化技術の併用によるマルウェア検知率及び判別率の向上を目的とする．

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	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	明星大学　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 丸山研究室
ホームページのURL	（明星大学情報学部） https://www.is.meisei-u.ac.jp/ （明星大学） https://www.meisei-u.ac.jp/
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 覗き見耐性を持つジャイロと音を用いた認証手法 研究開発国： 日本 研究開発時期： 2024年6月～	スマートフォンのロック解除において覗き見攻撃を防ぐために振動やジェスチャーを用いた認証がこれまで提案されてきているが，覗き見されてしまい，パスワードが盗まれてしまう可能性が残っている．また，画面の視覚情報を用いない認証方式については，検討がされていない現状がある． 本研究ではスマートフォンに内蔵されているジャイロセンサと，常時装着することが増えているヒアラブルデバイス（完全ワイヤレスイヤホン）からの音を用いた，画面の視覚情報を用いない新たな認証手法について検討する．

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	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	明星大学　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　小暮研究室
ホームページのURL	（明星大学情報学部） https://www.is.meisei-u.ac.jp/ （明星大学） https://www.meisei-u.ac.jp/
研究説明のURL	https://www.iag.meisei-u.ac.jp/meuhp/KgApp?resId=S001191&_gl=1*14z5mzy*_ga*MTEzODYxMzY3NS4xNjUzNDQ5OTcx*_ga_FWWP82PEWW*MTcyNjY0MTAxMS41NC4xLjE3MjY2NDEwNjMuMC4wLjA.*_ga_EB871D7KTK*MTcyNjY0MTAxMS41NC4xLjE3MjY2NDEwNjMuMC4wLjA.*_ga_9XN59YCSYK*MTcyNjY0MTAxMS41MS4xLjE3MjY2NDEwNjMuMC4wLjA.
対象技術	研究開発状況
研究開発名称： 暗号技術・認証技術 研究開発国： 日本 研究開発時期： 2021年7月1日～2027年3月31日	誰でもインターネットにアクセスすることのできる現代社会においては、デジタルデータで表現される情報を安全に守る必要があります。デジタルデータの秘匿に用いられる暗号技術の安全性を、数学を用いた解読計算量の観点から保証する研究を行っています。世界中で通用する仮想通貨を初めて実現したブロックチェーン等、コンピューターを通じて数学と社会とをつなぐアプリケーションの研究開発も行っています。

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	国立大学法人東海国立大学機構岐阜大学
代表者名	松尾　清一
所在地	501-1193 岐阜市柳戸１－１
窓口部署名	研究推進部研究推進課
電話番号	058-293-3140
関連部門名	研究推進部
ホームページのURL	https://ari.gifu-u.ac.jp/
研究説明のURL	特になし
対象技術	研究開発状況
研究開発名称： オープンイノベーションサーバー 研究開発国： 日本 研究開発時期： 2022年9月1日～2023年3月20日	研究データのオリジナル性を担保するために、ブロックチェーンの仕組みを使っています。

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	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	情報学研究科 情報システム学専攻 嶋田研究室
ホームページのURL	
研究説明のURL	https://www.net.itc.nagoya-u.ac.jp/member/shimada/researches/network_security.html https://www.net.itc.nagoya-u.ac.jp/member/shimada/researches/cyber_security.html https://www.net.itc.nagoya-u.ac.jp/member/shimada/researches/network.html
対象技術	研究開発状況
研究開発名称： （特にプロジェクト名は無い） 研究開発国： 日本 研究開発時期：	以下のような研究を過去数年の間に実施している。継続的に研究開発を続けているため、研究開発期間は特に記さない。 - 悪性通信の解析/検知 - HTTP(S)通信を使うC&C通信の検出 - NFA型シグネチャ検知のFPGAによるハードウェア化 - FPGAを利用したペイロードの周波数領域特徴量抽出とホストPCでの機械学習系検知 - マルウェアの検知/分類 - マルウェアバイナリのCFG特徴のGINによる圧縮を利用した分類 - カスタム損失関数を導入したGBDTによるマルウェア検知精度向上 - 潜在表現の時系列差分を用いた亜種マルウェア検知精度向上 - セキュアなネットワーク運用 - 攻撃の進捗と業務継続性を両立するネットワーク遮断 - OS間のIPv6実装状態の差を悪用する攻撃と検証 - バックボーン遅延ヒストグラムからの無線LAN Rogue AP(偽AP)検知 - 自動リンク処理などにおける国際化ドメイン名などUTF文字処理上のセキュリティ問題 - Physically Unclonable Functionを利用したIoT向けプロトコルの多要素認証化 - セキュリティナレッジの構築 - SNSや議論系Webサイトから脆弱性情報の収集とランク分け - SNSの脆弱性話題からのWeb Application Firewallルール生成 - ハニーポットとIDS - IoT向け通信プロトコルのためのハニーポットとその観測結果 - 標的型攻撃対策 - ログ統合によるサイバー攻撃推定手法 - ユーザの信用度を考慮したテレワーク通信へのアクセス制御手法 - 通信遮断による標的型攻撃対応のための影響範囲VR可視化システム - 機械学習/深層学習応用システムへの攻撃 - 研究用IDS作成学習データセットに対する偽学習データ付与 - 勾配情報変化量を利用したSVMベースのマルウェア検知を標的にする中毒攻撃データの検知 - 悪性URLクエリを検知する機械学習システムに対する細工されたURLクエリ学習による中毒攻撃とその対策

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	公立大学法人北九州市立大学
代表者名	理事長　津田　純嗣
所在地	802-8577 福岡県北九州市小倉南区北方四丁目２番１号
窓口部署名	企画管理課　企画・研究支援係
電話番号	093-695-3367
関連部門名	情報システム工学科　山崎恭研究室
ホームページのURL	https://www.kitakyu-u.ac.jp/
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 高度生体認証システム 研究開発国： 日本 研究開発時期： 2020年4月1日～2025年3月31日	科学研究費助成事業の研究課題において，携帯端末を対象とした安全性および利便性の高い生体認証システム（高度生体認証システム）を実現するための要素技術を開発中.

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	日本文理大学
代表者名	学長　橋本　堅次郎
所在地	870-0397 大分県大分市一木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	日本文理大学・工学部・情報メディア学科
ホームページのURL	https://www.nbu.ac.jp/
研究説明のURL	www.nbu.ac.jp/~fukushima/fukushima.html
対象技術	研究開発状況
研究開発名称： 非記号情報による環境状況推定 研究開発国： 日本 研究開発時期： 2024年4月1日～2025年3月31日	企業との共同研究として進行している

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	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	研究開発状況
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～2025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、近々、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について協議しており、同メーカーから日本国内に向けて販売することを目指している。

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	東京情報大学
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	総合情報学部 共創ラボ（ネットワーク・セキュリティ Lab）
ホームページのURL	https://www.tuis.ac.jp/
研究説明のURL	
対象技術	研究開発状況
研究開発名称： 情報システムに対する攻撃・不正アクセスの予測・検知・防御・分析・可視化に関する基盤技術の確立 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	日本大学
代表者名	
所在地	102-8275 東京都千代田区九段南4-8-24
窓口部署名	研究推進部　研究事務課
電話番号	03-5275-8137
関連部門名	理工学部応用情報工学科
ホームページのURL	http://www.nihon-u.ac.jp/
研究説明のURL	https://53lab.jp/
対象技術	研究開発状況
研究開発名称： 生体から得られる電磁気情報を用いた個人認証システム 研究開発国： 日本 研究開発時期： 2016年12月1日～	実験用のシステムを構築し，有効性の検証を行っている。

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	日本大学
代表者名	
所在地	102-8275 東京都千代田区九段南4-8-24
窓口部署名	研究推進部　研究事務課
電話番号	03-5275-8137
関連部門名	理工学部応用情報工学科
ホームページのURL	http://www.nihon-u.ac.jp/
研究説明のURL	https://53lab.jp/
対象技術	研究開発状況
研究開発名称： ブロックチェーン技術を用いた単一医療機関向け診療記録システム 研究開発国： 日本 研究開発時期： 2017年12月1日～	実験用のシステムを構築し，有効性の検証を行っている。

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	日本大学
代表者名	
所在地	102-8275 東京都千代田区九段南4-8-24
窓口部署名	研究推進部　研究事務課
電話番号	03-5275-8137
関連部門名	理工学部応用情報工学科
ホームページのURL	http://www.nihon-u.ac.jp/
研究説明のURL	https://53lab.jp/
対象技術	研究開発状況
研究開発名称： 標的型メール対策訓練支援システム 研究開発国： 日本 研究開発時期： 2017年12月15日～	実験用のシステムを構築し，有効性の検証を行っている。

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	日本大学
代表者名	
所在地	102-8275 東京都千代田区九段南4-8-24
窓口部署名	研究推進部　研究事務課
電話番号	03-5275-8137
関連部門名	理工学部応用情報工学科
ホームページのURL	http://www.nihon-u.ac.jp/
研究説明のURL	https://53lab.jp/
対象技術	研究開発状況
研究開発名称： デジタルフォレンジック技術の学習支援システム 研究開発国： 日本 研究開発時期： 2018年9月1日～	実験用のシステムを構築し，有効性の検証を行っている。

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	公立大学法人大阪
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	情報学研究科
ホームページのURL	
研究説明のURL	なし
対象技術	研究開発状況
研究開発名称： ネットワークトラフィック及びログ解析に基づく異常検知 研究開発国： 日本 研究開発時期： 2006年4月1日～2024年	基礎研究を継続しており、研究成果は国内の学会等で継続的に発表している。

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	