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２年12月

警察庁生活安全局情報技術犯罪対策課

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2,928件を無作為に抽出した。

調査は、調査票を郵送で配付し、次の2つの方法で回収することで実施した。

① 電子メールでの回答

調査票のファイルに直接回答内容を入力してもらい、電子メールにて回答

② 郵送等での回答

配付した調査票を、郵送やFAXなどで送付してもらい回答

（調査期間：令和2年8月26日(水)(発送日)～9月25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2,928件、回収総数は622件であった。回収率は21.2%である。

業種	発送数	回収数	回収率
農林・水産・鉱業	10	3	30.0%
製造業	902	155	17.2%
不動産・建築	187	40	21.4%
金融	108	29	26.9%
エネルギー	15	8	53.3%
運輸業	75	20	26.7%
情報通信	291	10	3.4%
サービス	839	148	17.6%
教育	267	81	30.3%
行政サービス	234	115	49.1%
無回答		13	-
合計	2,928	622	21.2%

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３〕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

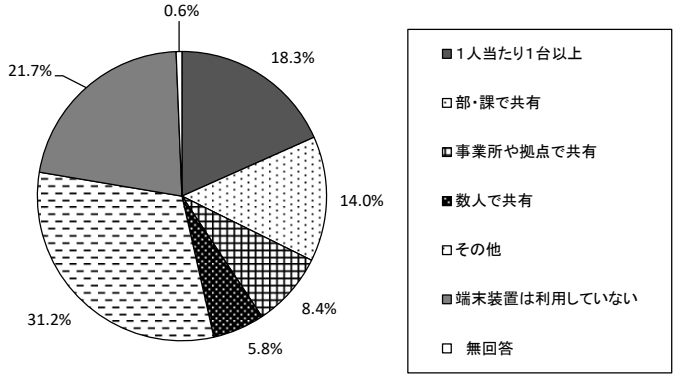
令和2年度の調査結果については、次のような特徴がみられる。

1　組織的対策状況

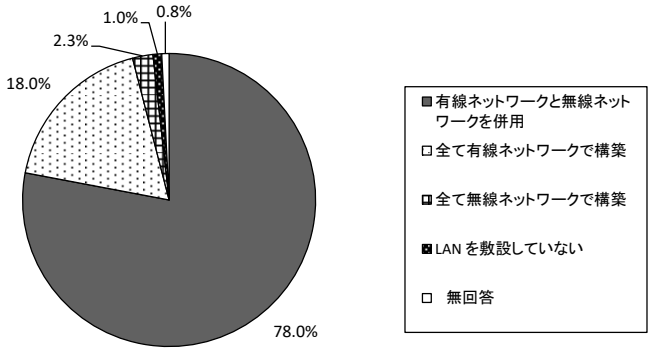
【情報システム等の環境】

パソコンの整備環境については、80.2%で「1人当たり1台以上」で整備されており、タブレット・スマートフォン等の整備環境については、「1人当たり1台以上」が18.3%で最も多く、「部・課で共有」が14.0%、「事業所や拠点で共有」が8.4%となっている。タブレット・スマートフォン等は、金融や情報通信で整備率が高く、行政サービスや教育では、「利用していない」割合が高い。「事業所内でのネットワーク利用状況」については、「有線ネットワークと無線ネットワークを併用」が78.0%と高く、「全て有線ネットワークで構築」「全て無線ネットワークで構築」を含めるとほぼ全ての事業所でネットワークが導入されている。インターネット環境については、98.1%で導入されており、「外部からの接続に対する許可」についても、「許可している」が59.8%であり、半数以上が外部からの接続を許可している。

【全体】端末装置（タブレット・スマートフォン等）の整備環境(SA,n=622)



【全体】事業体内のネットワーク利用状況（SA,n=622）

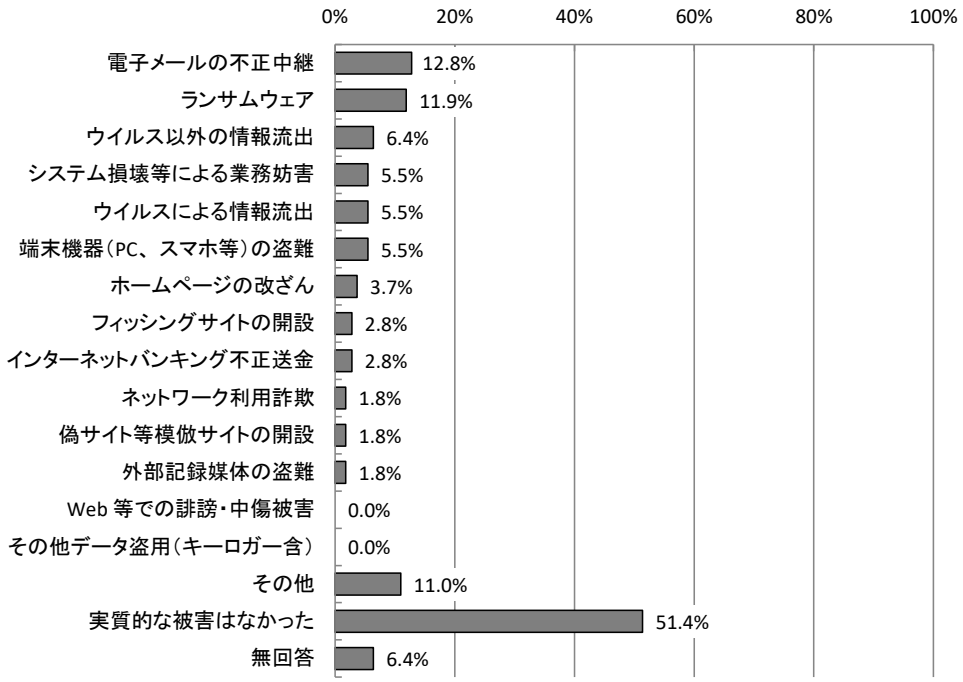


【不正アクセス等の被害状況】

過去の被害状況については、「電子メールの不正中継」が12.8%で最も多く、次いで「ランサムウェア」が11.9%となっている。届出先機関等については、「警察」が17.4%で最も多く、次いで「監督官庁」が14.7%となっている。

また、届出を躊躇させる要因としては、「実質的な被害が無かったので」が68.6%で最も多く、次いで「社・団体内で対応できたので」が25.5%であり、被害が無かったと感じた場合や、自社以外に被害が及ばなかった場合、届出を躊躇する傾向が見られる。

【全体】過去に受けたことのある被害状況（MA, n=109）



【情報セキュリティの運用・管理体制】

情報セキュリティ運用・管理専門部署の有無については、「ある」が65.8%であり、「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69.3%で最も多くなっており、「情報セキュリティ担当役員（ＣＩＳＯ等）を設置」は36.3%となっている。

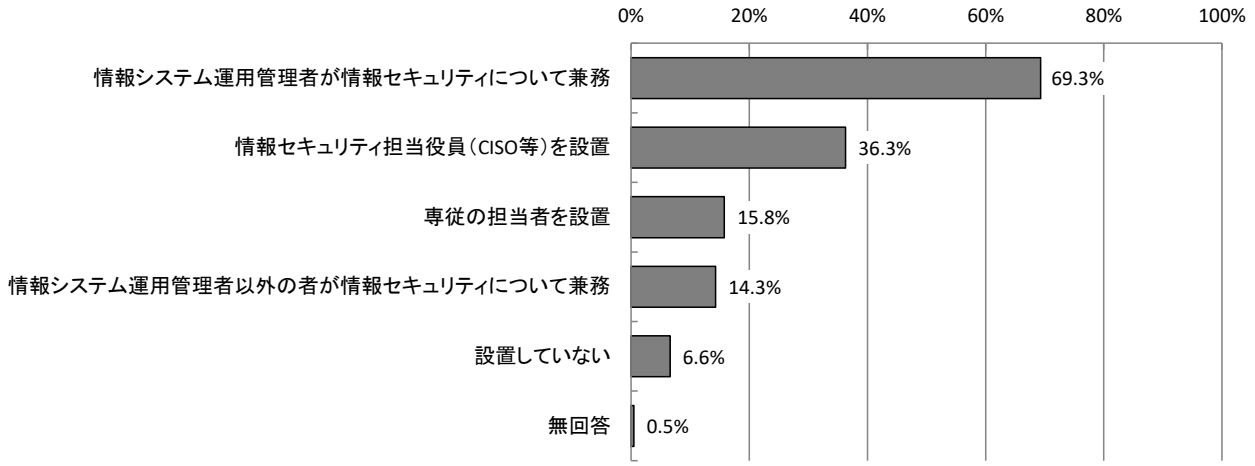
セキュリティポリシーの策定状況については、「策定している」が83.3%で最も多く、「今のところ、策定する予定はない」は3.5%となっている。今後予定と策定作業中を入れると92.1%であり、情報セキュリティポリシーの策定が浸透している状況が窺える。

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47.6%で最も多く、次いで「策定することを検討」が31.8%となっている。

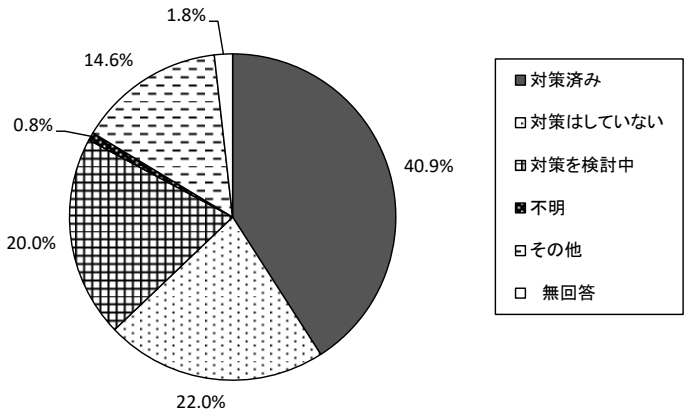
一方、第三者認証機関制度の利用は、「特に利用していない」が79.1%であり、ペネトレーションテストの実施も「実施していない」が60.1%と半数以上を占めている。

また、ビジネスメール詐欺については、80.5%が「知っていた」と回答しているが、「対策済み」は、40.9%であり、「対策はしていない」が22.0%となっている。

【全体】情報セキュリティ管理体制（MA,n=622）



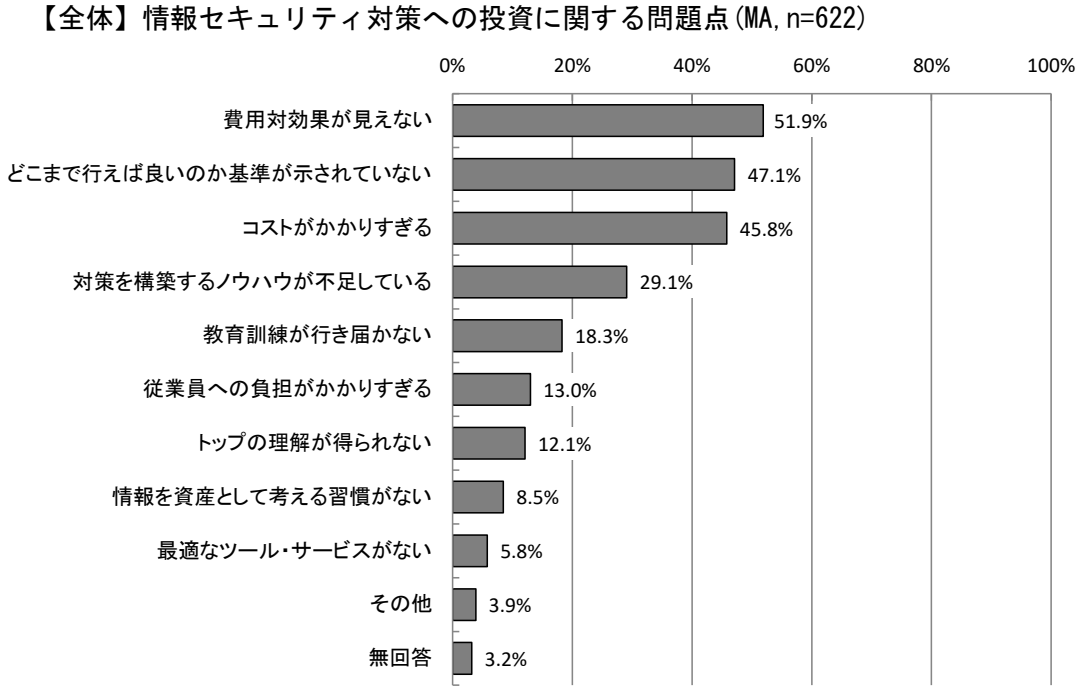
【全体】ビジネスメール詐欺への対策（SA,n=501）



【情報セキュリティ対策への投資】

2021年度情報セキュリティ対策の投資計画については、今期と比較して、「ほぼ同額とする計画」であるとする割合が72.8%で最も多く、増やす計画であるとする各項目の合計は23.5%で、減らすとする各項目の合計は1.6%となっている。

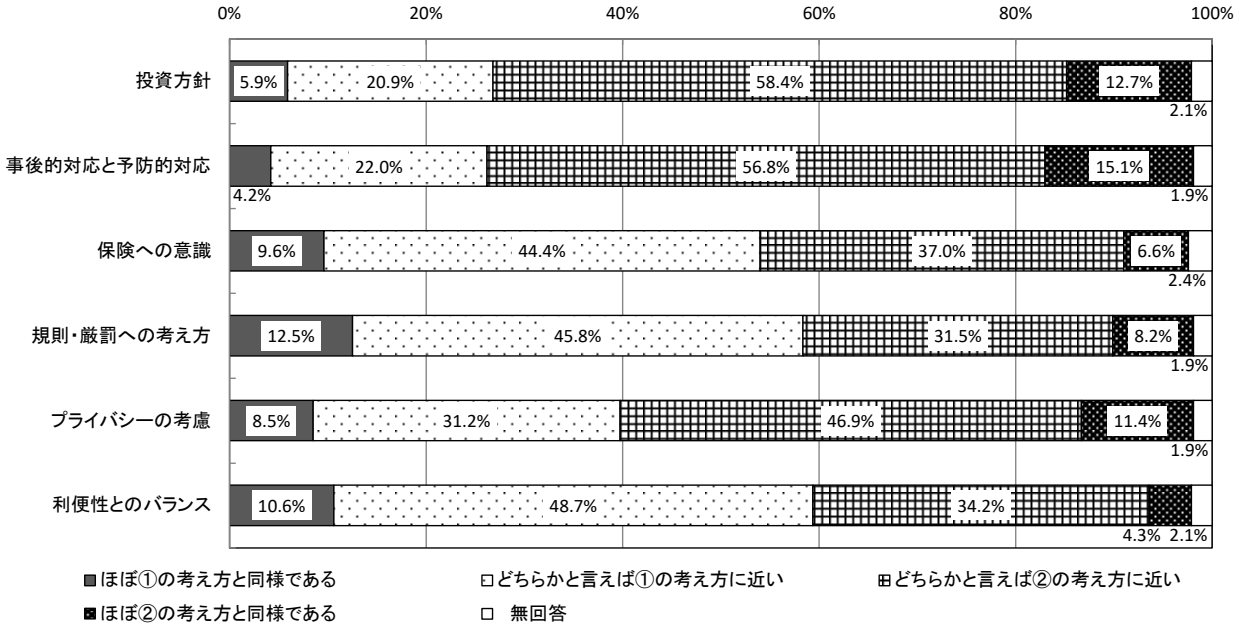
情報セキュリティ対策への投資に関する問題点については、「費用対効果が見えない」が51.9%で最も多く、次いで「どこまで行えば良いのか基準が示されていない」が47.1%、「コストがかかりすぎる」が45.8%となっている。



【情報セキュリティ対策に関する考え方】

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

【全体】情報セキュリティ対策実施上の方針（SA, n=622）



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

２　技術的対策

【ネットワークに対する情報セキュリティ対策】

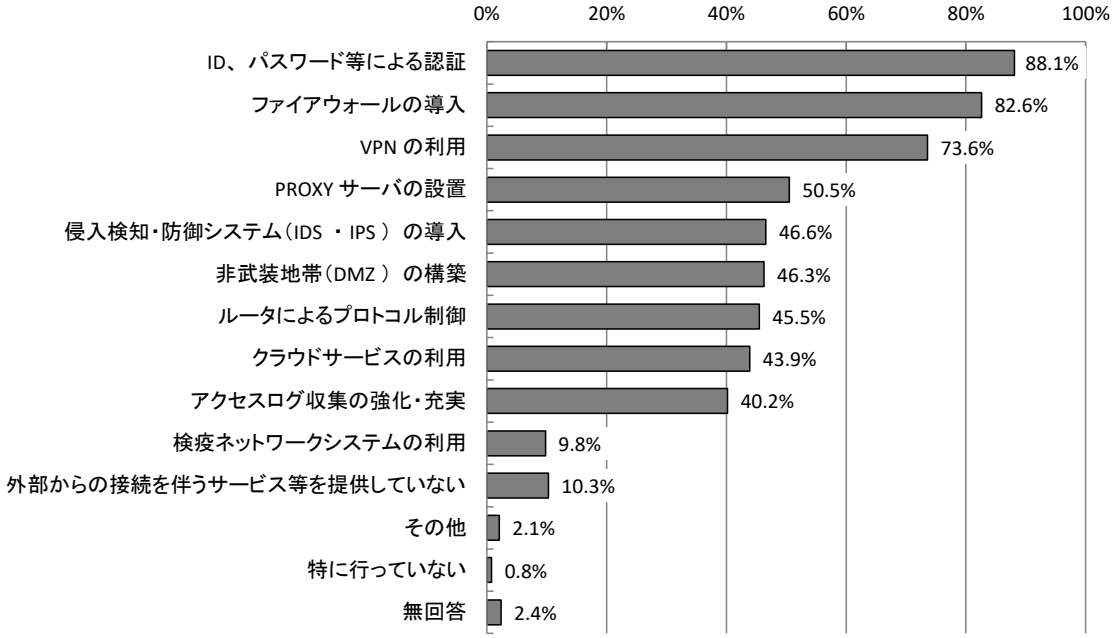
外部からの接続に対するセキュリティ対策（通信路に対する対策）については、「ID・パスワードに対する認証」が58.8%で最も多く、次いで、「通信の暗号化」が48.1%、「MACアドレス等の端末機器の固有情報を用いた認証」「専用ネットワークセグメントの設定」がこれに続いている。

端末に対する対策については、「ウイルス対策ソフト等の導入」が64.5%で最も多く、次いで「OS、アプリケーション等をアップデートする仕組みの導入」が41.8%となっている。

インターネット接続に対するセキュリティ対策については、「ID・パスワード等による認証」が88.1%で最も多く、次いで「ファイアウォールの導入」が82.6%となっている。「VPNの利用」「PROXYサーバの設置」については半数以上が実施している状況である。

無線LANネットワークのセキュリティ対策については、「WPA2又はWPA3による暗号化」が62.7%で導入されており、28.9%で「MACアドレス認証」が実施されているが、ぜい弱性が指摘されている「WEPによる暗号化」も10.8%で使用されている。

【全体】インターネット接続に対するセキュリティ対策（MA,n=622）



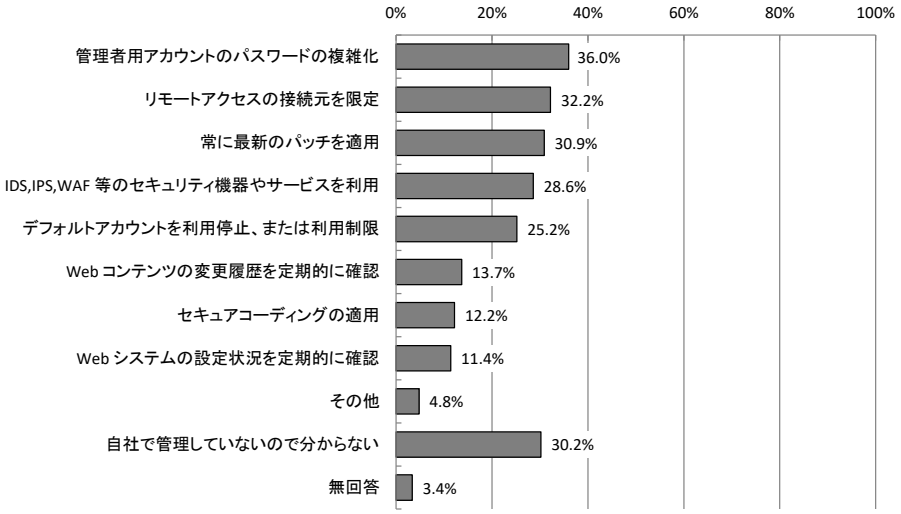
【Webサービスに対するセキュリティ対策】

Webサーバ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」「リモートアクセスの接続元を限定」「常に最新のパッチを適用」「IDS・IPS等の利用」等が実施されているが、いずれも30%前後の実施状況である。

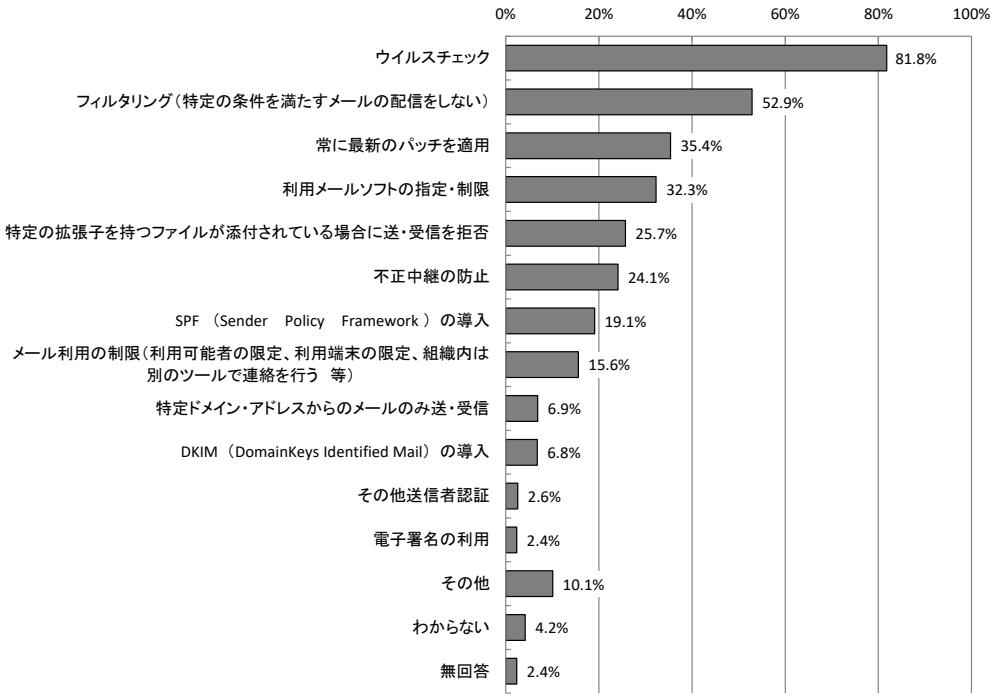
電子メールに関するセキュリティ対策については、「ウイルスチェック」が81.89%で最も多く、次いで「フィルタリング」52.9%、「常に最新のパッチを適用」35.4%という状況である。

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78.1%で最も多い。「特にチェックもせず受信」は、7.1%であった。

【全体】Webサーバのセキュリティ対策（MA,n=622）



【全体】電子メールに関するセキュリティ対策（MA,n=622）

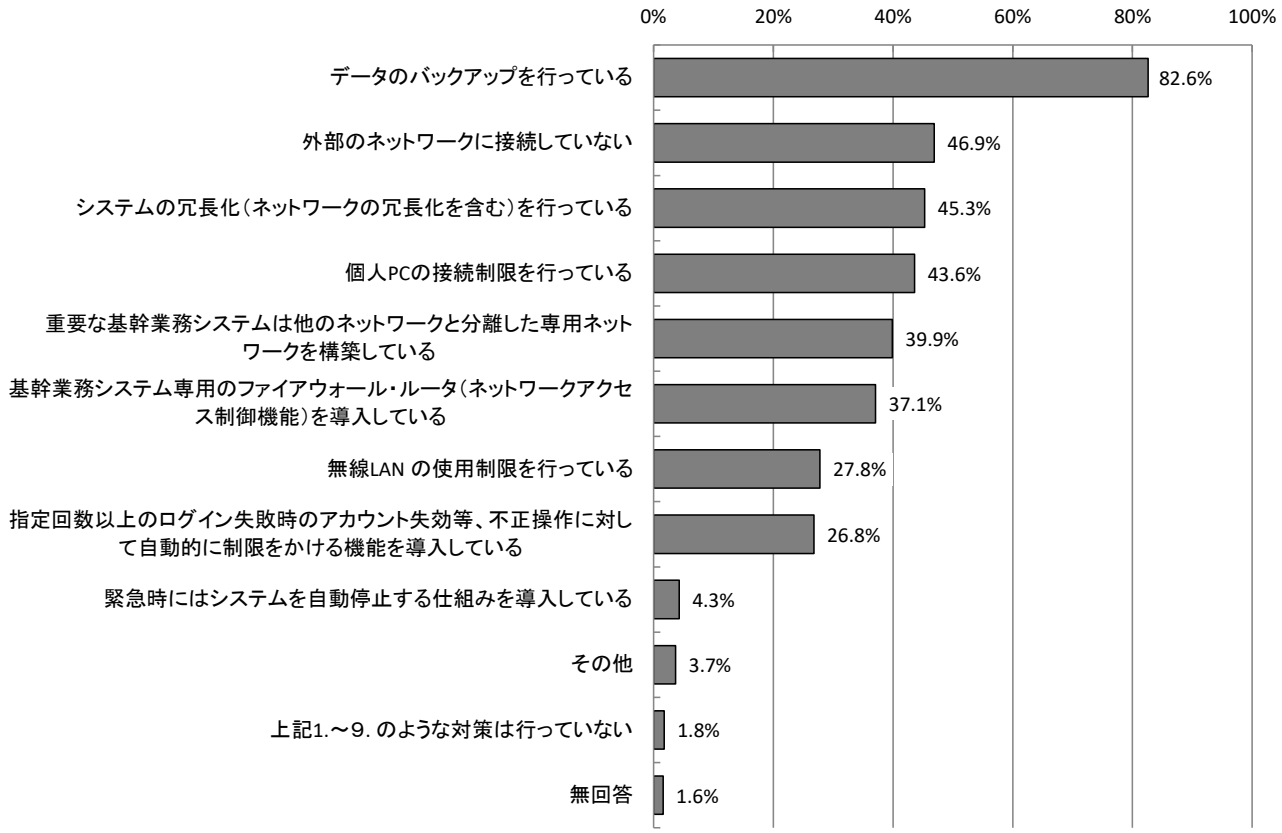


【不正アクセス、情報漏えい等に対する情報セキュリティ対策】

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82.6%で最も多く、次いで「外部のネットワークに接続していない」が46.9%、「システムの冗長化（ネットワークの冗長化含む）が45.3%となっている。

不正アクセス等への対策状況については、「パソコン廃棄時の適正なデータ消去」が81.0%で最も多く、「定期的なバックアップ」が74.8%、「情報資産へのアクセス権の設定」が71.4%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93.1%で最も多くなっており、次いで「ウイルス対策ソフト(サーバ)の使用」83.6%、「パターンファイルを定期的に更新（自動更新システムを利用）」が76.2%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=622)



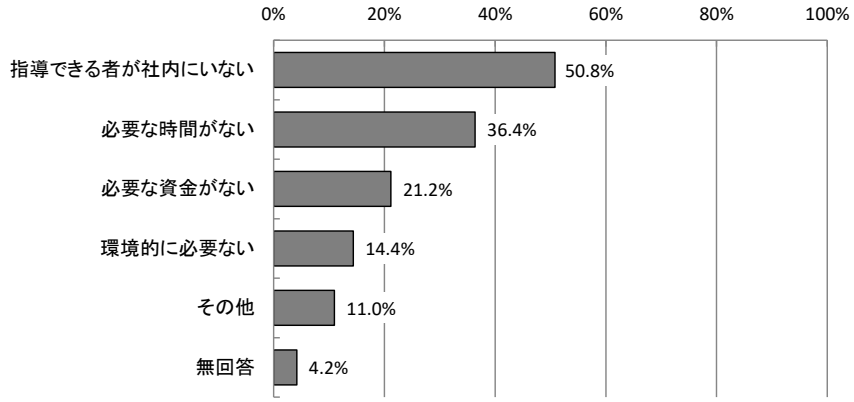
３　人的対策

【情報セキュリティ教育】

情報セキュリティ教育の実施状況については、「実施している」が72.2%で最も多く、「実施をしていない」が19.0%である。実施していない理由については、「指導できる者が社内にいない」が50.8%で最も多く、「必要な時間がない」36.4%、「必要な資金がない」21.2%となっている。

また、情報セキュリティ教育の内容については、「情報セキュリティポリシー」が61.6%で最も多く、次いで「個人情報の保護・管理」が61.3%、「ウイルス等のマルウェア対策」が55.3%となっている。教育の頻度については、「年に１回」が36.7%で最も多く、次いで「年に数回」が24.0%、「採用・異動時等に実施」が21.5%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=118)

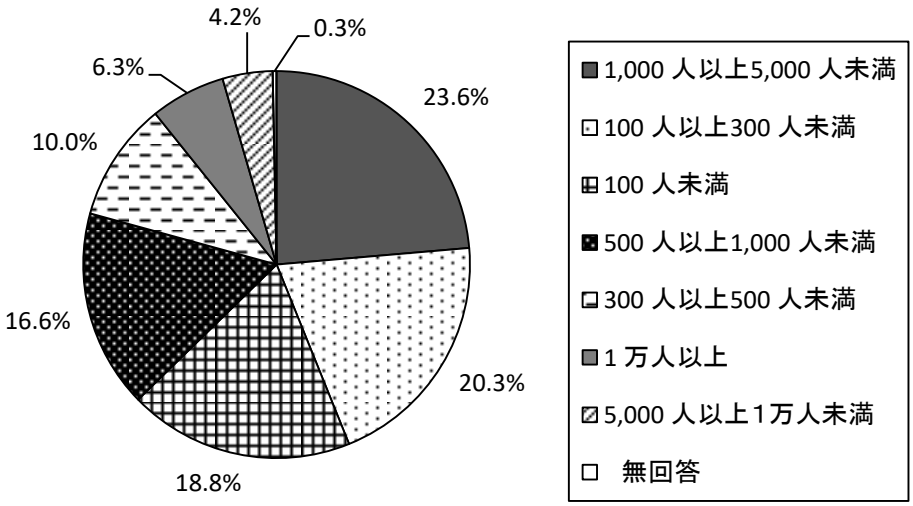


今回の調査結果では、情報セキュリティポリシーが、全体の８割以上で制定されており、情報セキュリティに関する教育においても、全体の７割で実施されている等情報セキュリティに関する意識について一定の浸透が図られていることがうかがえるが、その一方で、情報セキュリティ対策について費用対効果が見えづらいことや基準が示されていないこと等が多くの組織で問題点として認識されていることが認められた。

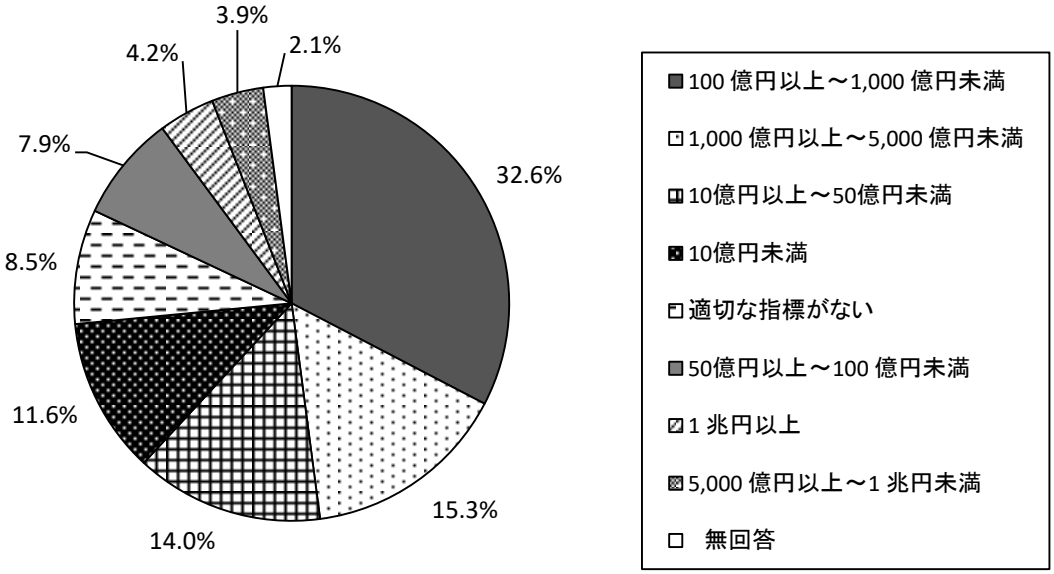
また、セキュリティ侵害事案発生時における対策マニュアルの策定が、依然半数に満たない状況であり、事案発生の際の被害拡大防止のため、これら対策意識の浸透が今後の課題の一つといえる。

2.2　回答事業体の属性等

【全体】従業員規模（SA,n=622）【問2】



【全体】予算規模（SA,n=622）【問3】



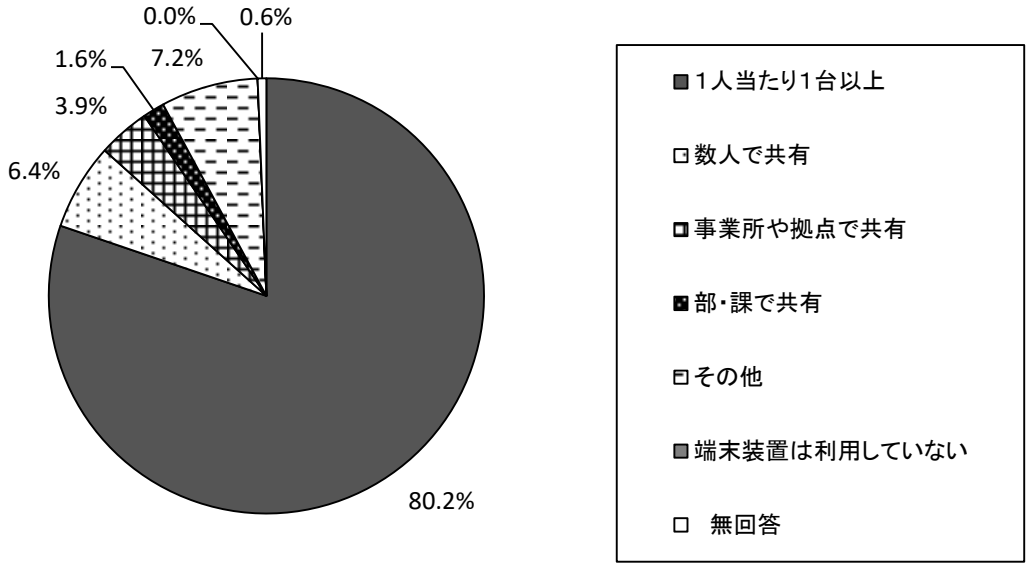
3. 調査結果

3.1　組織的対策

3.1.1　端末装置（パソコン）の整備環境　【問4】

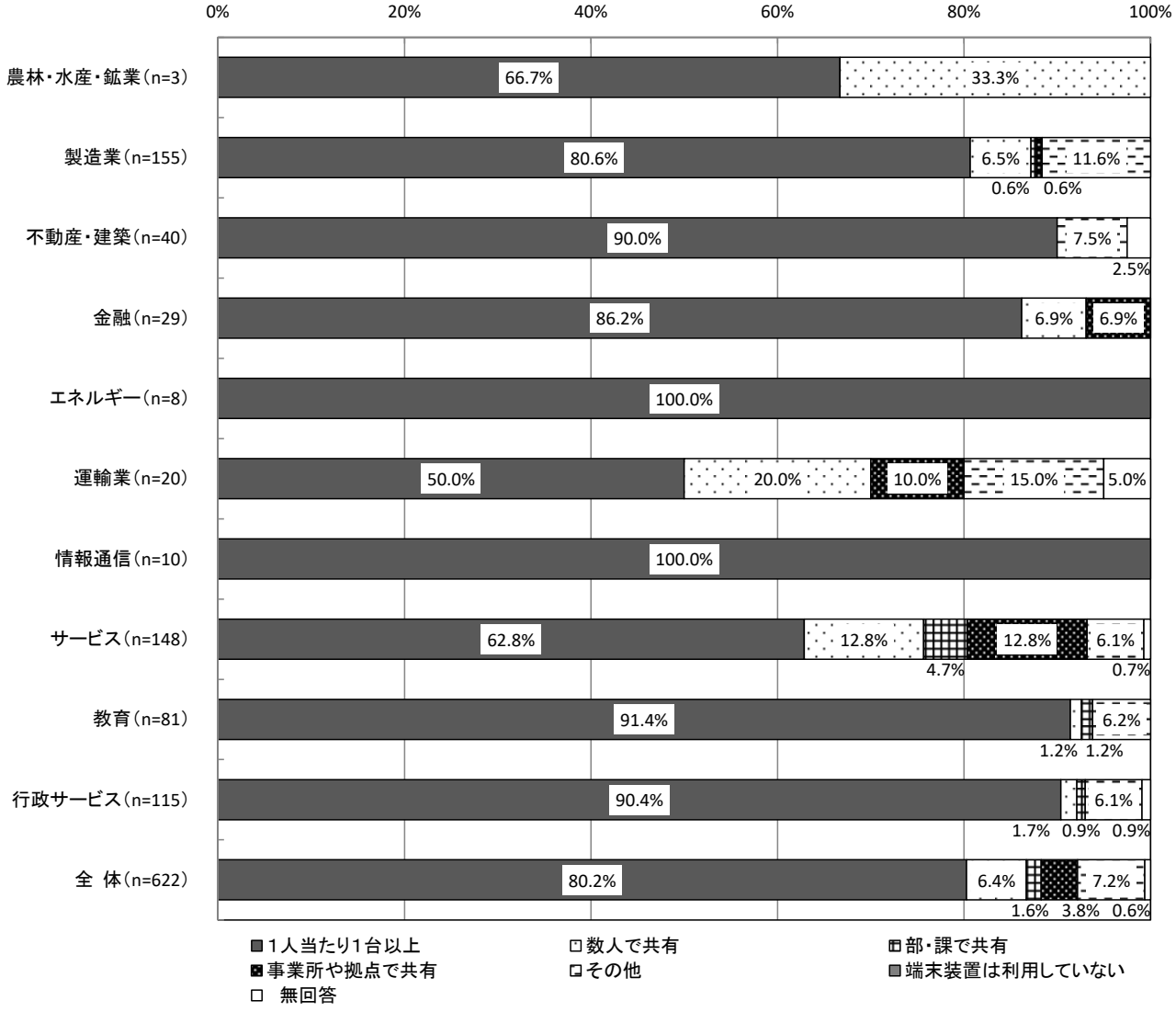
端末装置（パソコン）の整備環境については、「1人当たり1台以上」が80.2%で最も多く、「数人で共有」が6.4%、「事業所や拠点で共有」が3.9%となっている。

【全体】端末装置（パソコン）の整備環境（SA,n=622）



【業種別分析】業種別にみると、「1人当たり1台以上」では、「エネルギー」「情報通信」が100.0%で最も多く、次いで「教育」が91.4%、「行政サービス」が90.4%、「不動産・建築」が90.0%となっている。一方、最も少ないのは「運輸業」で50.0%となっている。

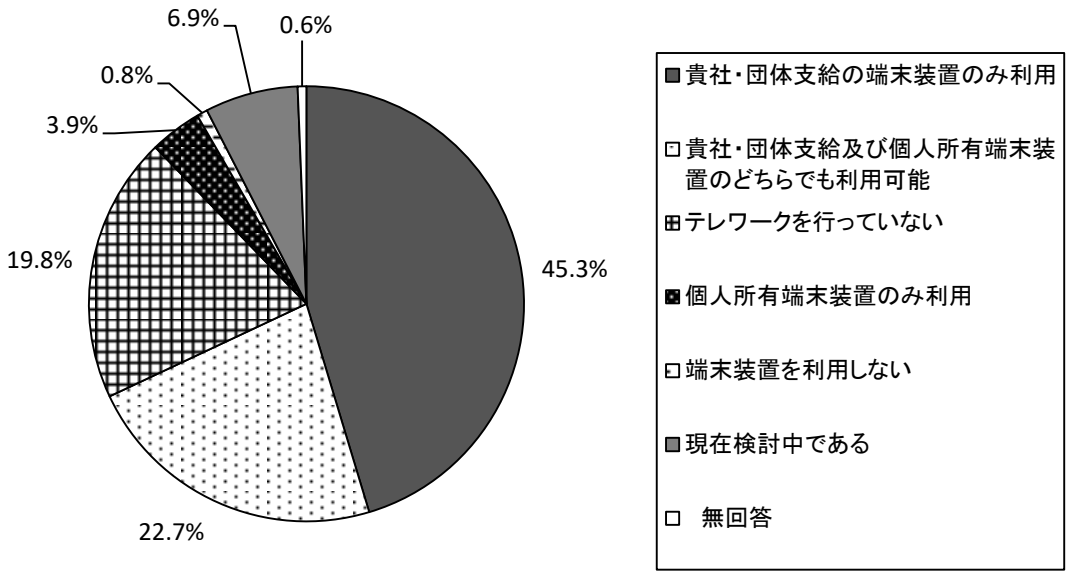
【業種別分析】端末装置（パソコン）の整備環境



3.1.2　テレワーク業務の端末装置（パソコン）の利用環境　【問4-1】

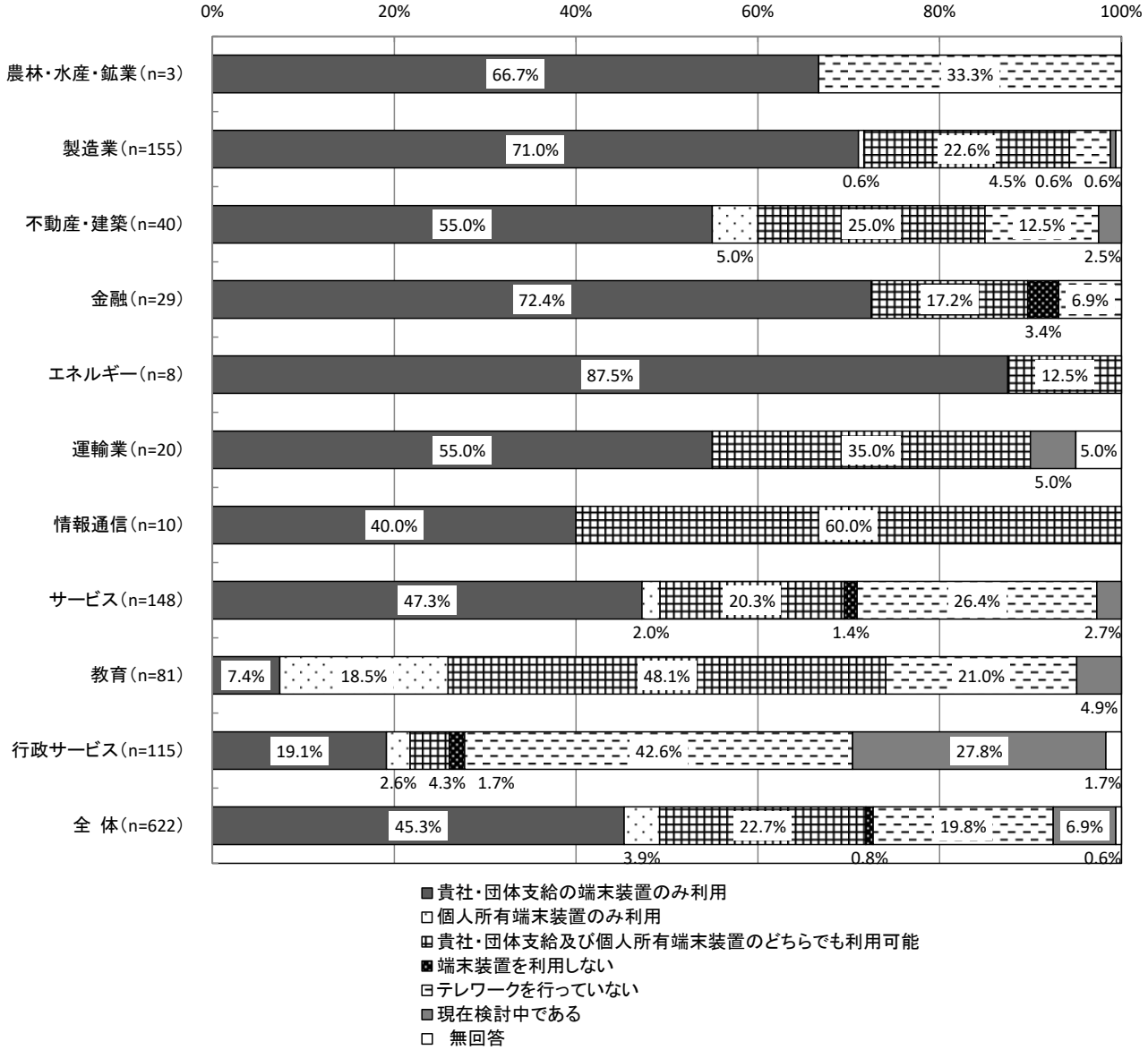
テレワーク業務の端末装置（パソコン）の整備環境については、「貴社・団体支給の端末装置のみ利用」が45.3%で最も多く、「貴社・団体支給及び個人所有端末装置のどちらでも利用可能」が22.7%、「テレワークを行っていない」が19.8%となっている。

【全体】テレワーク業務の端末装置（パソコン）の利用環境（SA,n=622）



【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、「エネルギー」が87.5%で最も多く、次いで「金融」が72.4%、「製造業」が71.0%となっている。一方、最も少ないのは「教育」で7.4%となっている。

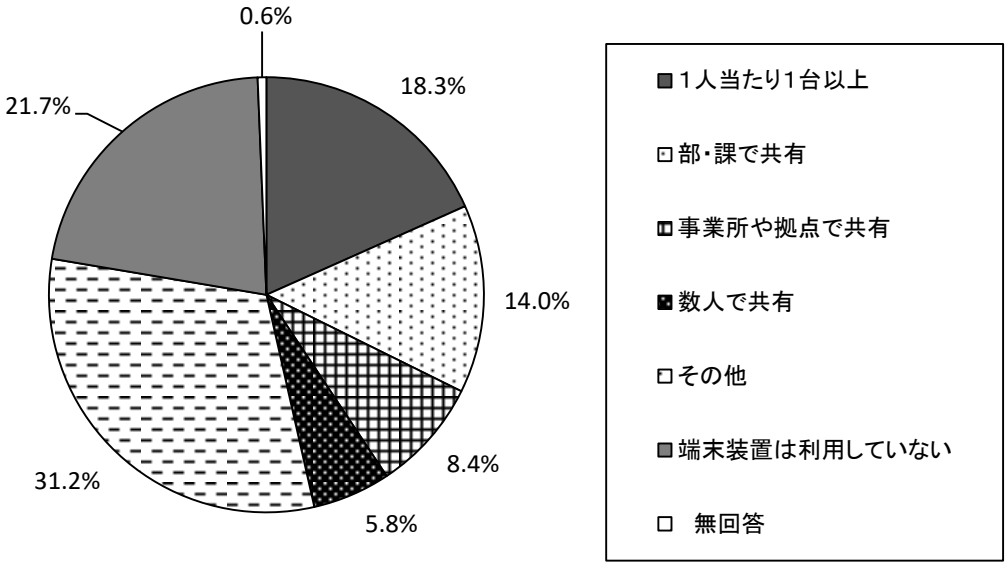
【業種別分析】テレワーク業務の端末装置（パソコン）の利用環境



3.1.3　端末装置（タブレット・スマートフォン等）の整備環境　【問5】

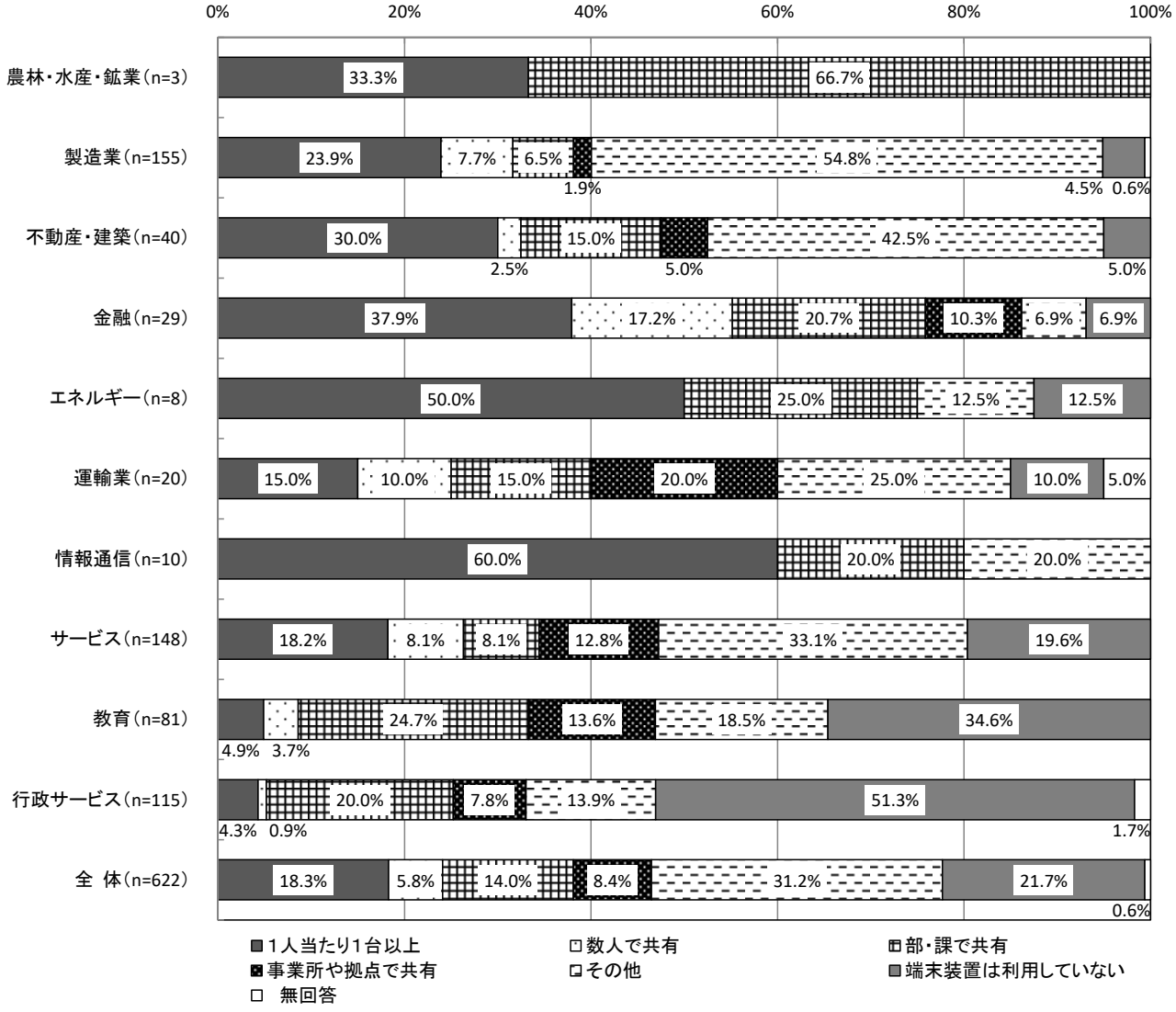
端末装置（タブレット・スマートフォン等）の整備環境については、「1人当たり1台以上」が18.3%で最も多く、「部・課で共有」が14.0%、「事業所や拠点で共有」が8.4%となっている。

【全体】端末装置（タブレット・スマートフォン等）の整備環境（SA,n=622）



【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60.0%で最も多く、次いで「エネルギー」が50.0%となっている。一方「端末装置は利用していない」では、「行政サービス」が51.3%で最も多く、「教育」が34.6%となっている。

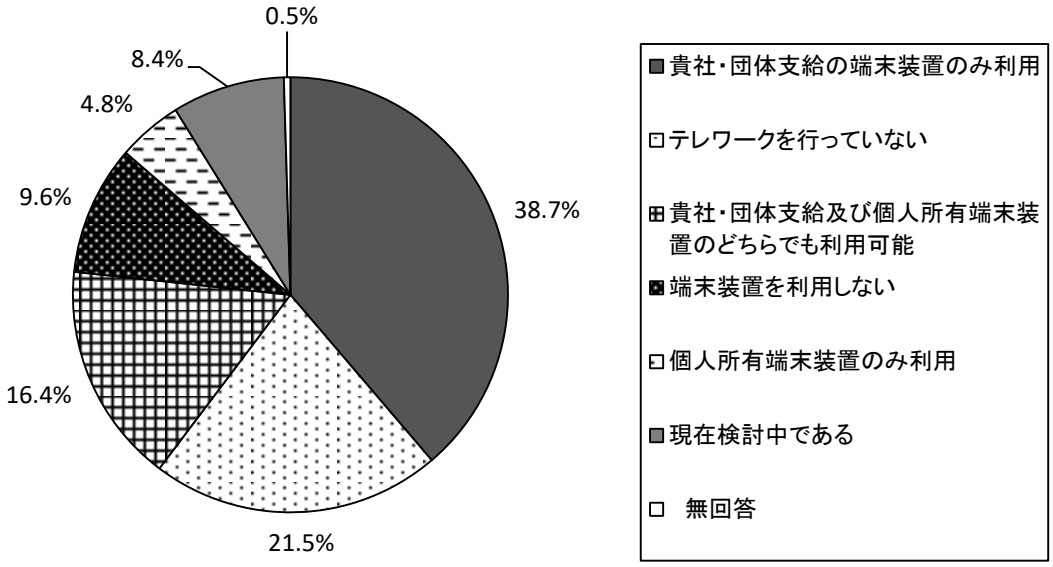
【業種別分析】端末装置（タブレット・スマートフォン等）の整備環境



3.1.4　テレワーク業務の端末装置（タブレット・スマートフォン等）の整備環境　【問5-1】

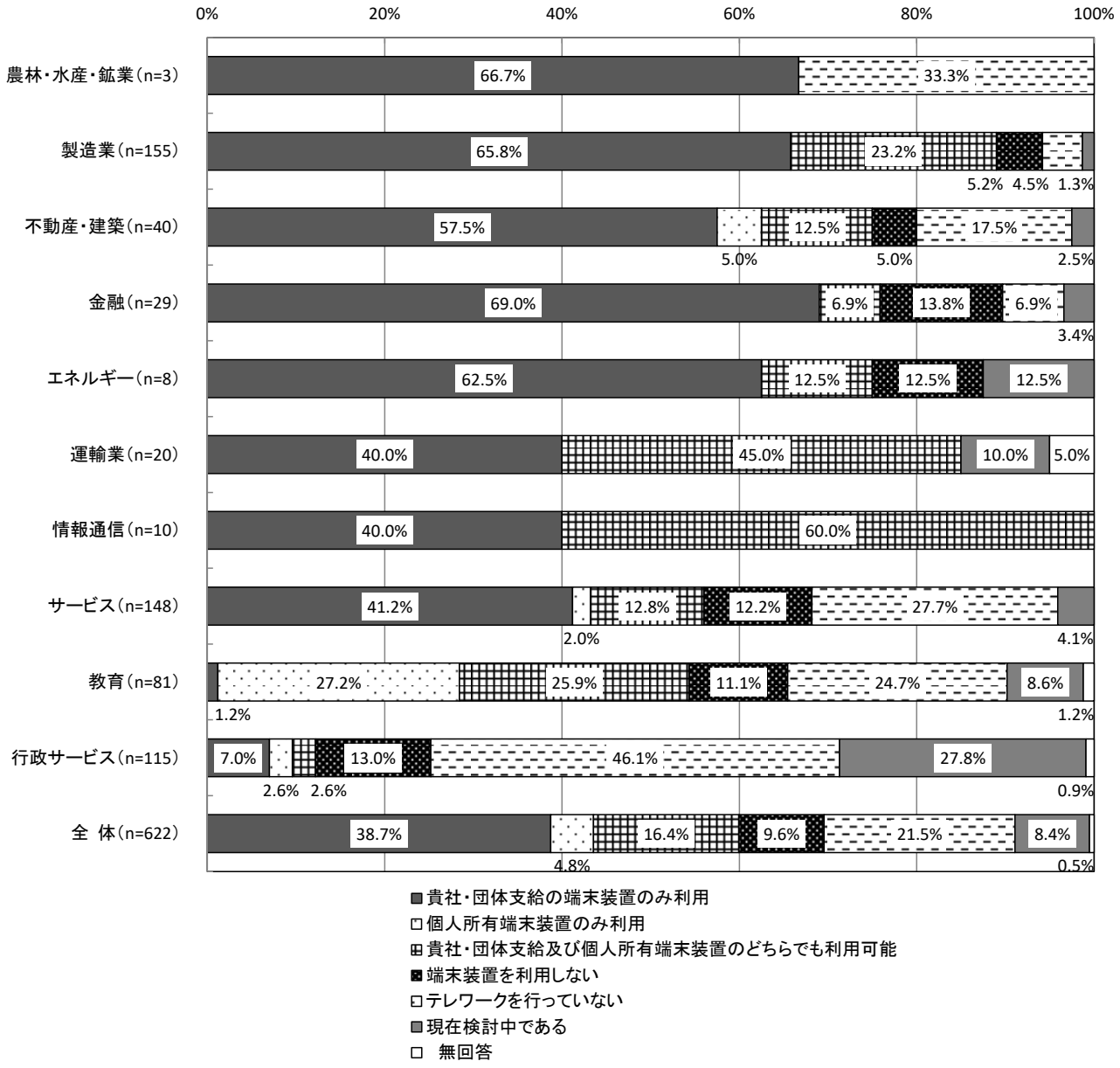
テレワーク業務の端末装置（タブレット・スマートフォン等）の整備環境については、「貴社・団体支給の端末装置のみ利用」が38.7%で最も多く、「テレワークを行っていない」が21.5%、「貴社・団体支給及び個人所有端末装置のどちらでも利用可能」が16.4%となっている。

【全体】テレワーク業務の端末装置（タブレット・スマートフォン等）の利用環境（SA,n=622）



【業種別分析】業種別にみると、「貴社・団体支給の端末装置のみ利用」では、「金融」が69.0%で最も多く、次いで、「製造業」が65.8%「エネルギー」が62.5%となっている。一方、最も少ないのは「教育」で1.2%となっている。

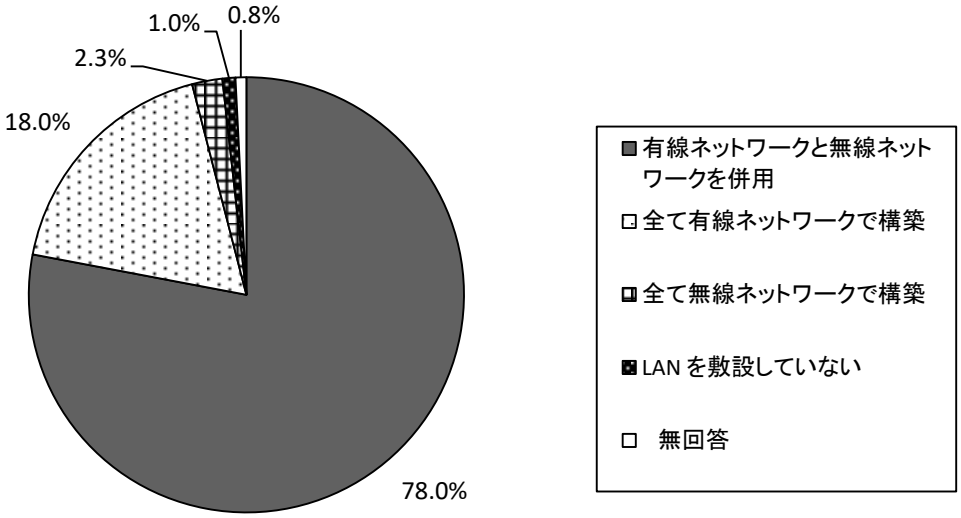
【業種別分析】テレワーク業務の端末装置（タブレット・スマートフォン等）の利用環境



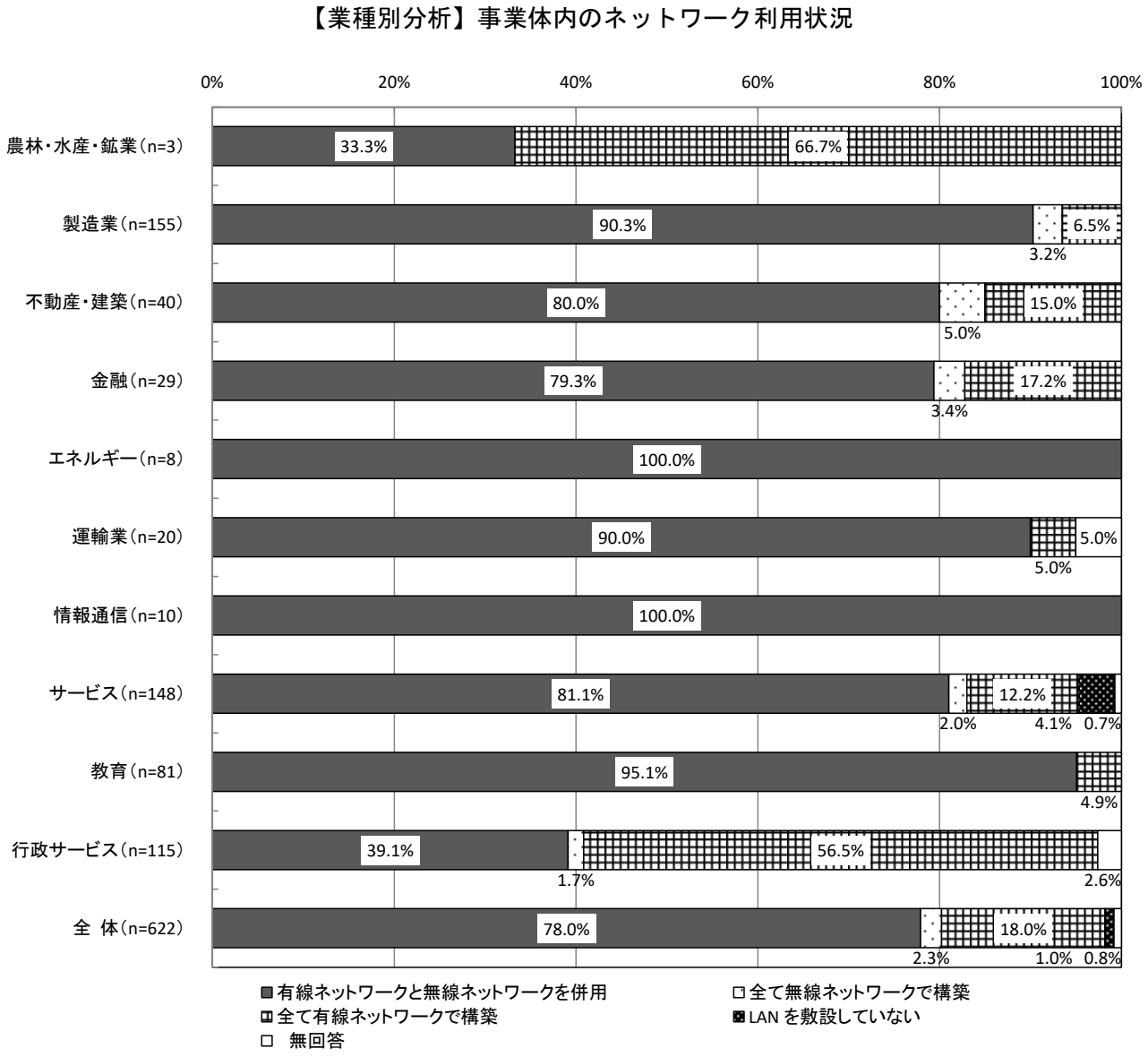
3.1.5　事業体内のネットワーク利用状況　【問6】

事業体内のネットワーク利用状況については、「有線ネットワークと無線ネットワークを併用」が78.0%で最も多く、次いで「全て有線ネットワークで構築」が18.0%となっている。

【全体】事業体内のネットワーク利用状況（SA,n=622）



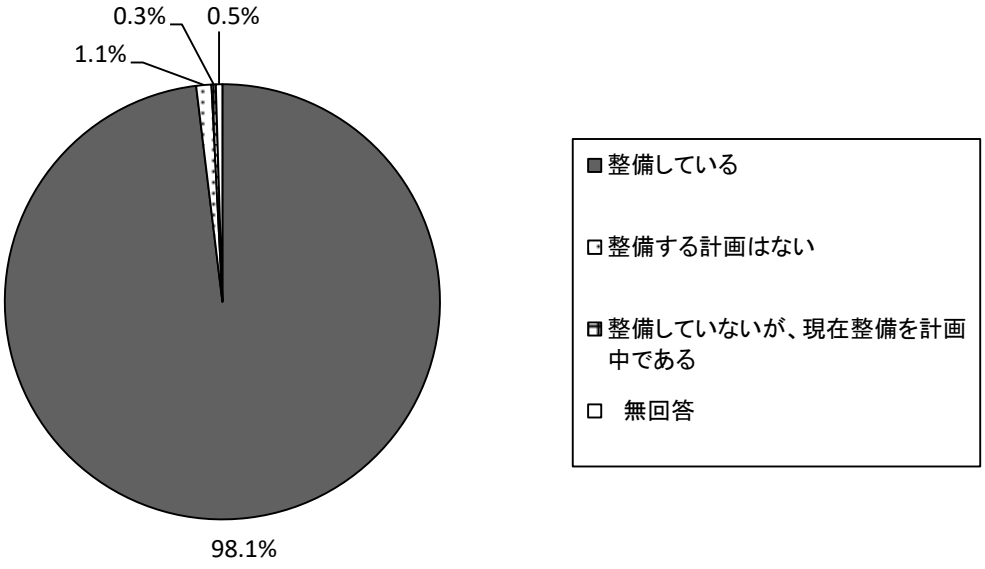
【業種別分析】業種別にみると、「有線ネットワークと無線ネットワークを併用」については、「エネルギー」「情報通信」が100.0%で最も多く、次いで「教育」が95.1%、「製造業」が90.3%、「運輸業」が90.0%となっている。



3.1.6　インターネット環境の整備　【問7】

インターネット環境の整備については、「整備している」が98.1%で最も多く、「整備する計画はない」は1.1%であった。

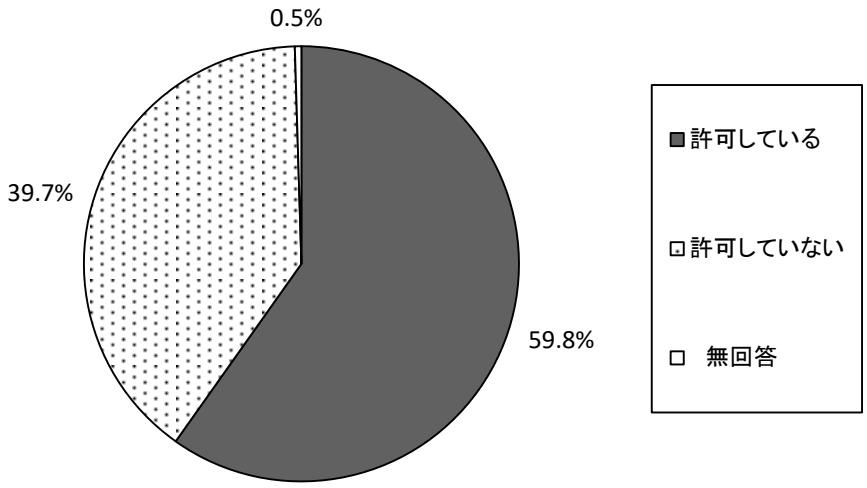
【全体】インターネット環境の整備（SA,n=622）



3.1.7　外部からの接続許可状況　【問8】

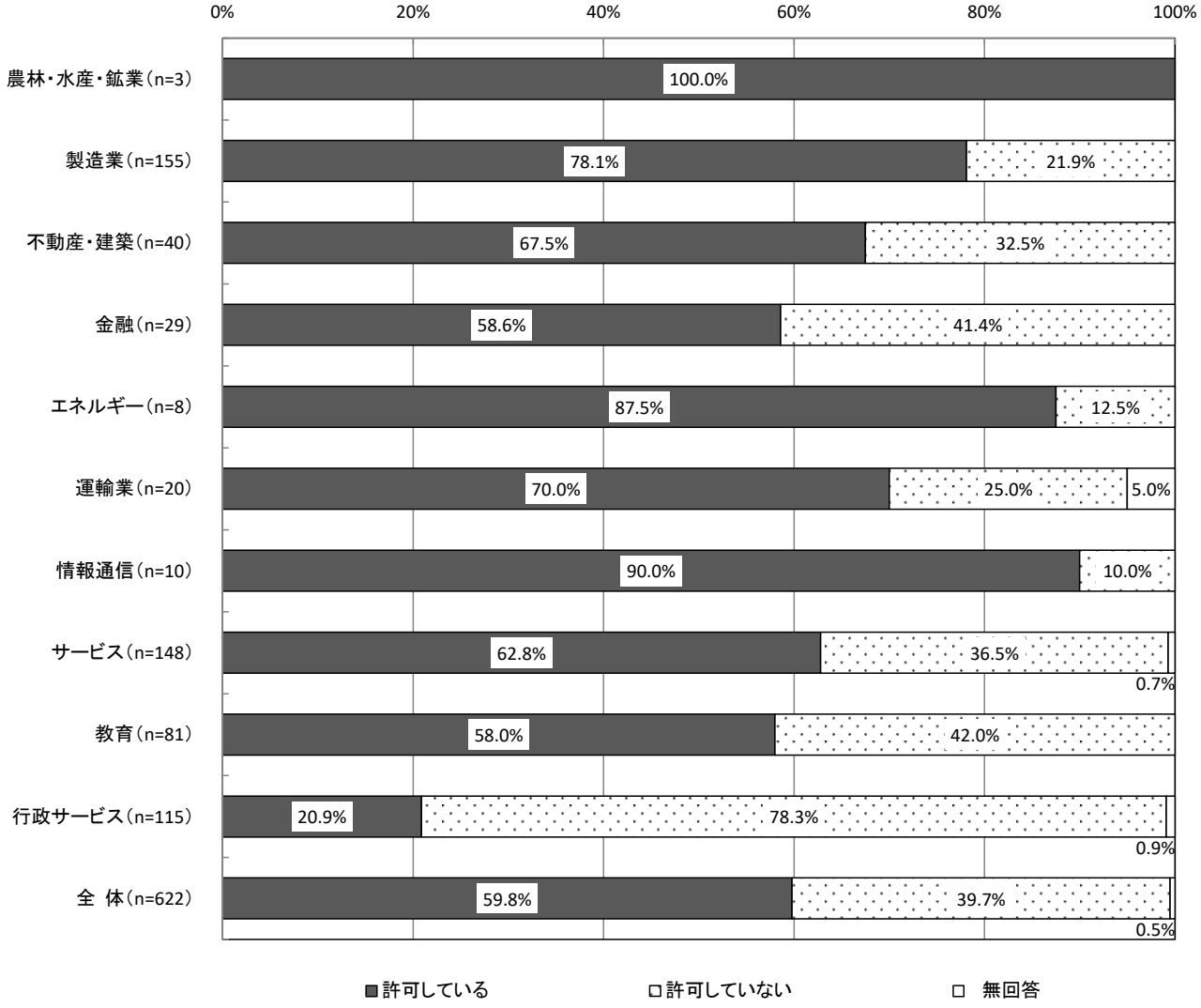
外部から事業体内ネットワークへの接続については、「許可している」が59.8%、「許可していない」は39.7%となっている。

【全体】外部からの接続許可状況（SA,n=622）



【業種別分析】業種別にみると、「許可している」では、「情報通信」が90.0%で最も多く、次いで「エネルギー」が87.5%、「製造業」が78.1%となっている。また、「許可していない」は「行政サービス」が78.3%で最も高い。

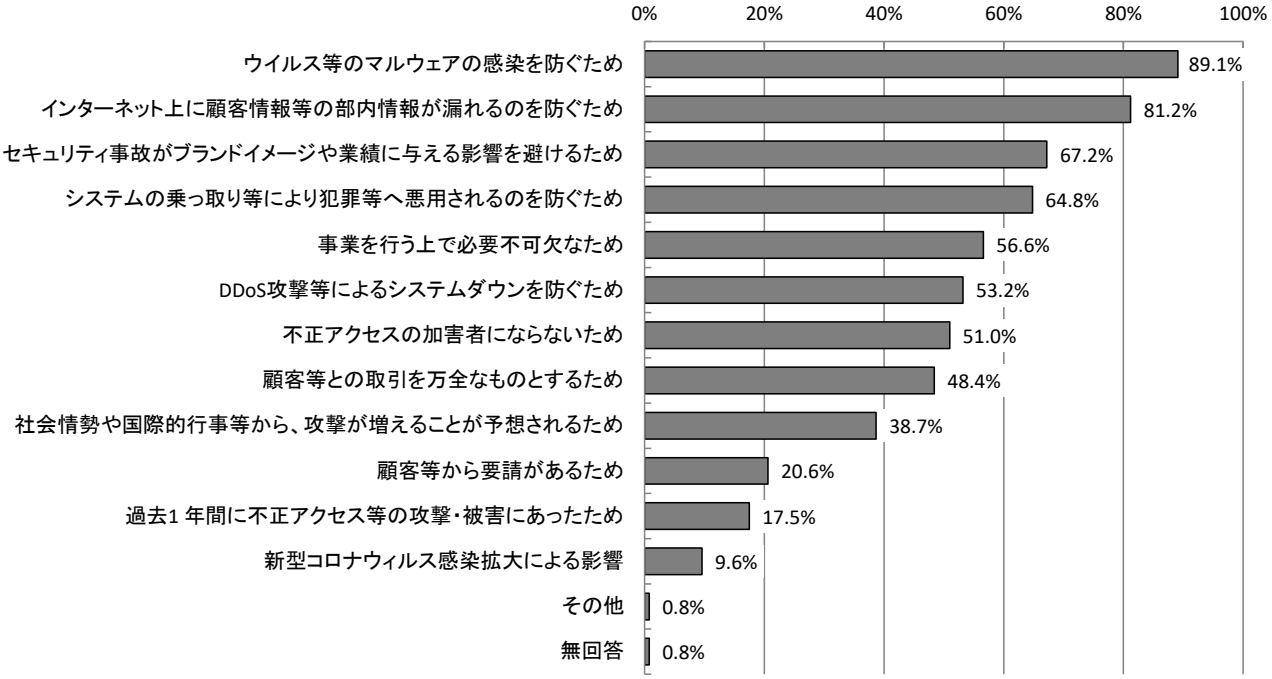
【業種別分析】外部からの接続許可状況



3.1.8　情報セキュリティ対策の必要性の理由【問9】

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89.1%で最も多く、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81.2%、「セキュリティ事故がブランドイメージや業績に与える影響を避けるため」が67.2%、「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64.8%となっている。

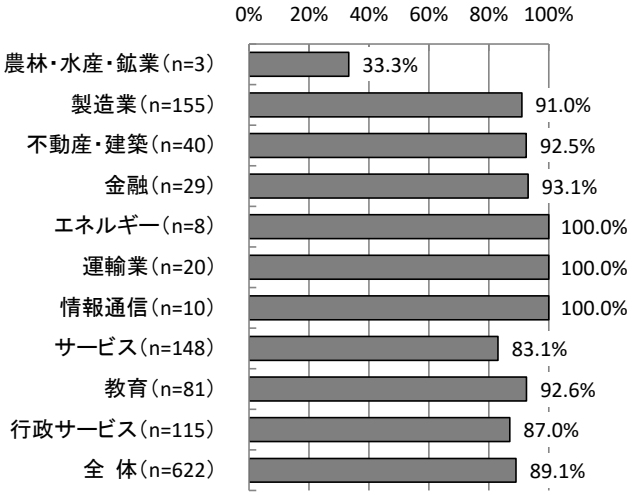
【全体】情報セキュリティ対策の必要性の理由（MA,n=622）



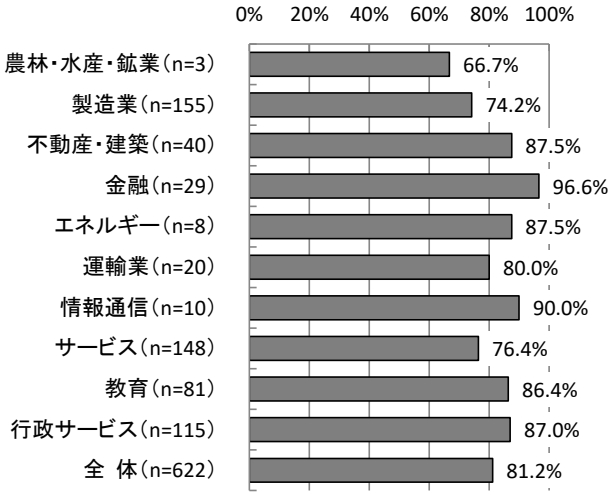
【業種別分析】業種別にみると、「ウイルス等のマルウェアの感染を防ぐため」については、「エネルギー」「運輸業」「情報通信」が100.0%、「インターネット上に顧客情報等の部内情報が漏れるのを防ぐため」については、「金融」が96.6%、「セキュリティ事故がブランドイメージや業績に与える影響を避けるため」については、「情報通信」が100.0%、「システムの乗っ取り等により犯罪等へ悪用されるのを防ぐため」では「運輸業」が95.0%と多くなっている。また、「事業を行う上で必要不可欠なため」については、「情報通信」が80.0%、「DDoS攻撃等によるシステムダウンを防ぐため」については、「金融」が86.2%、「不正アクセスの加害者にならないため」については、「情報通信」が80.0%、「顧客等との取引を万全なものとするため」については、「金融」が82.8%と多くなっている。

【業種別分析】情報セキュリティ対策の必要性の理由

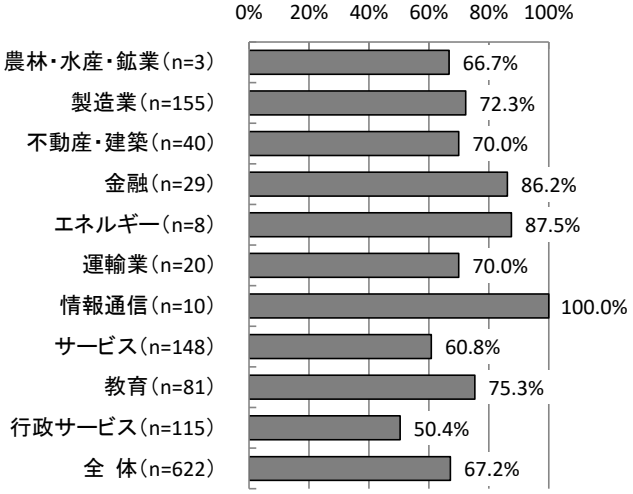
ウイルス等のマルウェアの感染を防ぐため



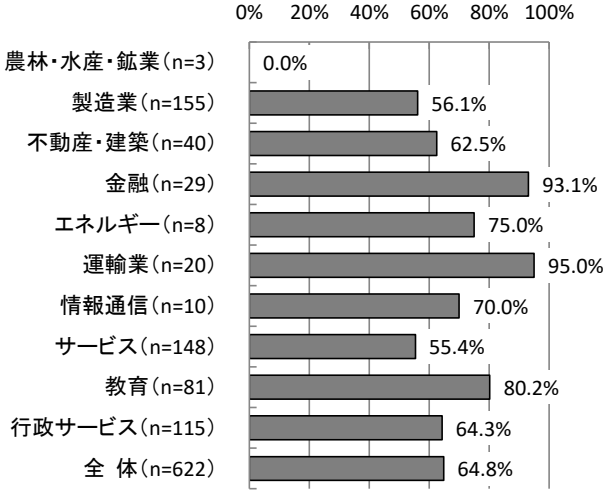
インターネット上に顧客情報等の部内情報が漏れるのを防ぐため



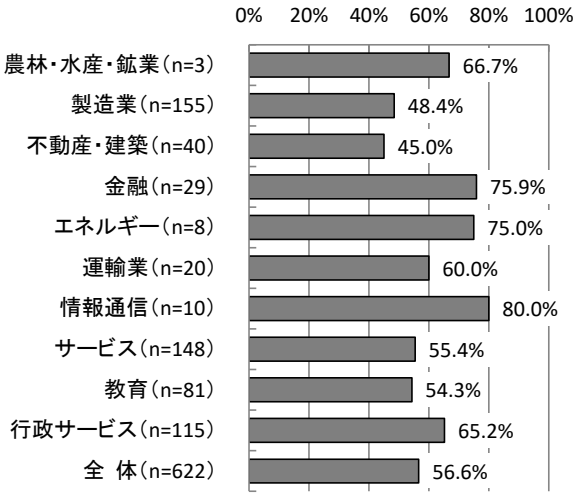
セキュリティ事故がブランドイメージや業績に与える影響を避けるため



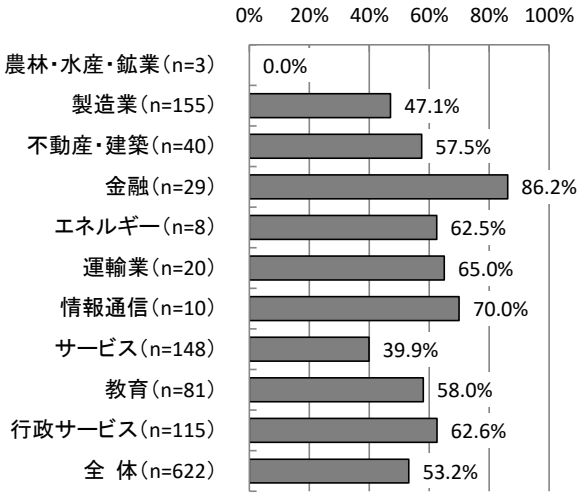
システムの乗っ取り等により犯罪等へ悪用されるのを防ぐため



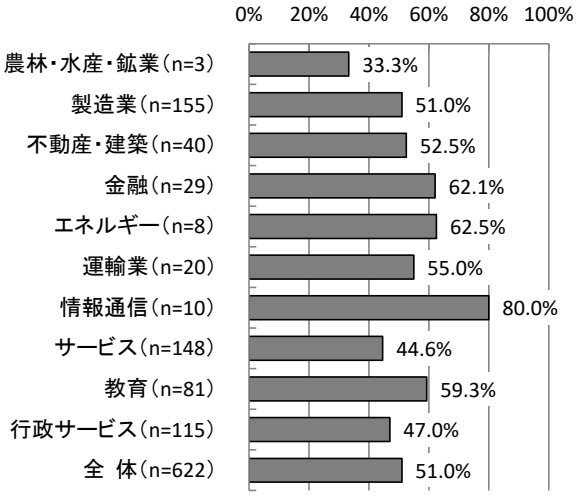
事業を行う上で必要不可欠なため



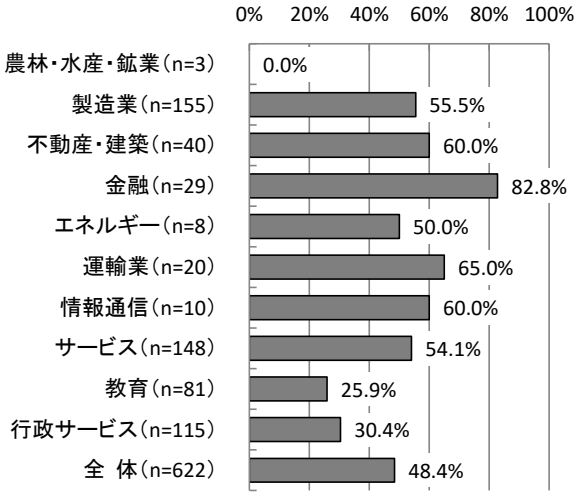
DDoS攻撃等によるシステムダウンを防ぐため



不正アクセスの加害者にならないため



顧客等との取引を万全なものとするため



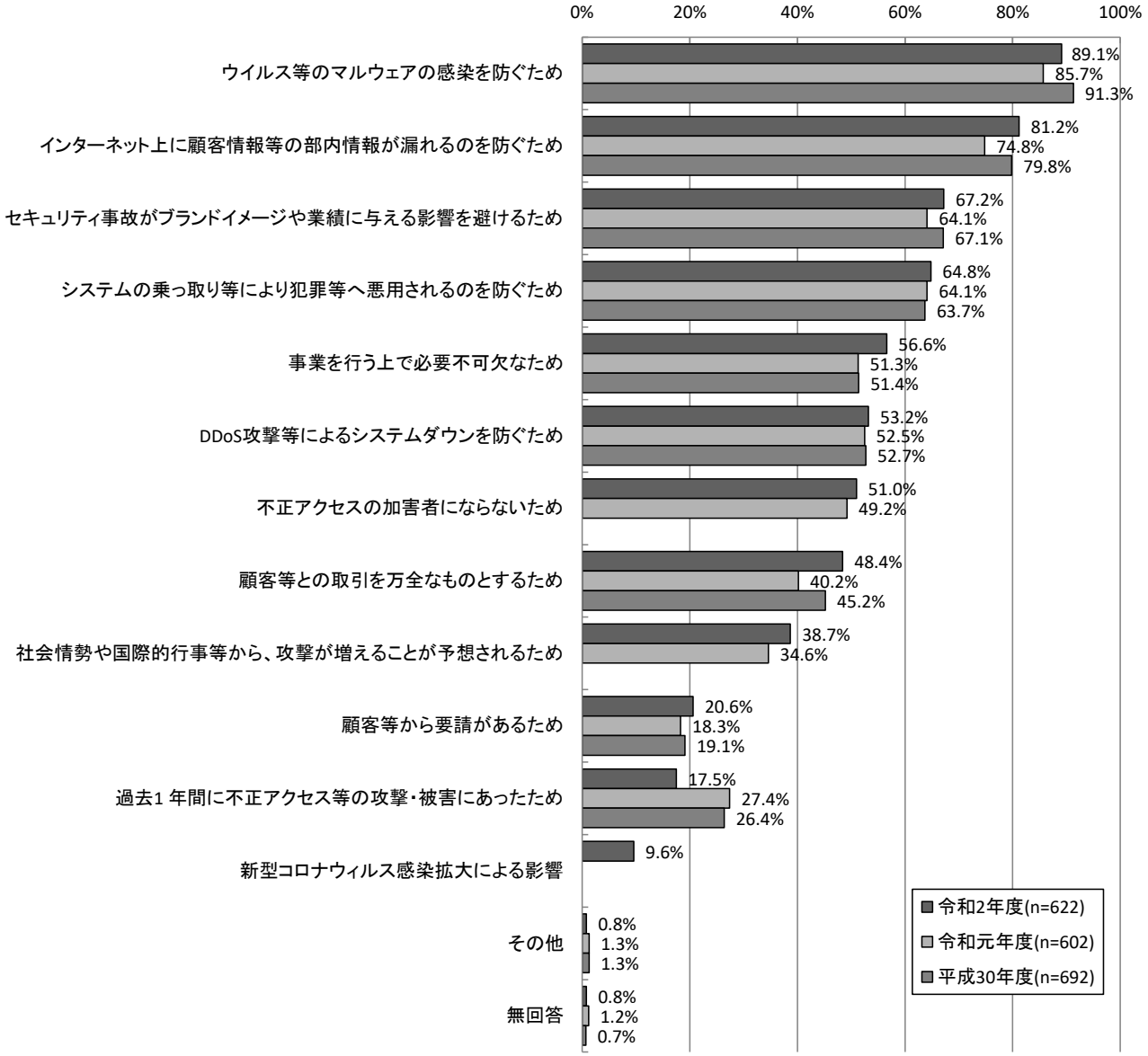
【経年変化】昨年度と比較すると、「顧客等との取引を万全なものとするため」が若干増加し、「過去１年間に不正アクセス等の攻撃・被害にあったため」が9.9ポイント減少している。

※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。

※令和元年度調査で、「社会情勢や国際的行事等から、攻撃が増えることが予想されるため」「不正アクセスの加害者にならないため」を新設。

※令和２年度調査で、「新型コロナウィルス感染拡大による影響」を新設。

【経年変化】情報セキュリティ対策の必要性の理由

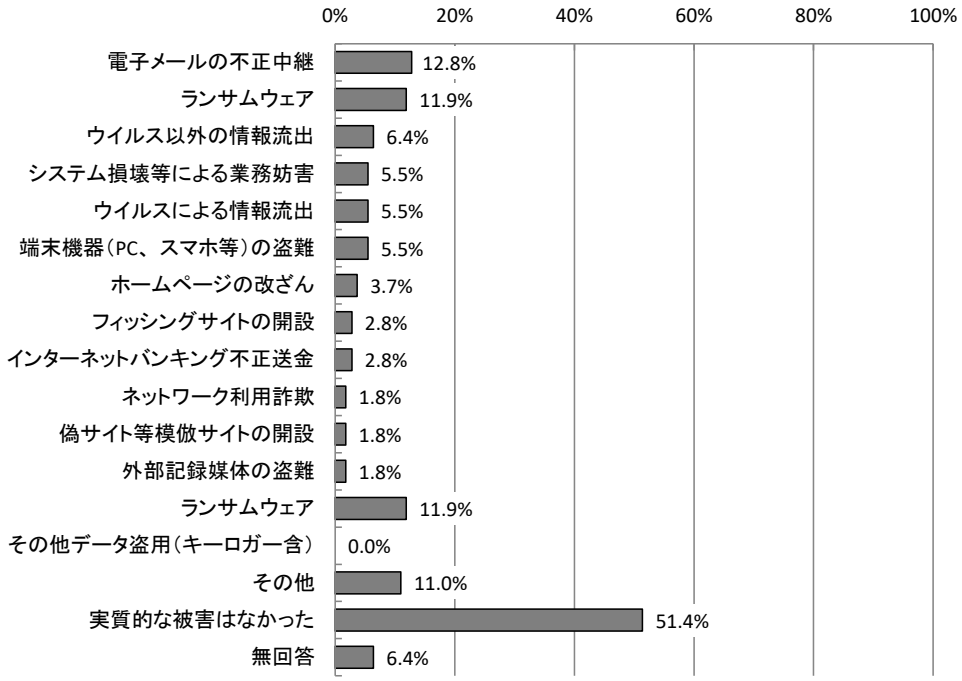


3.1.9　過去に受けたことのある被害状況　【問9-1-1】

過去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」が12.8%で最も多く、次いで「ランサムウェア」が11.9%、「ウイルス以外の情報流出」が6.4%となっている。また、「実質的な被害はなかった」が51.4%となっている。

※本項目は、過去に不正アクセス等の被害にあった社・団体等を対象としている。

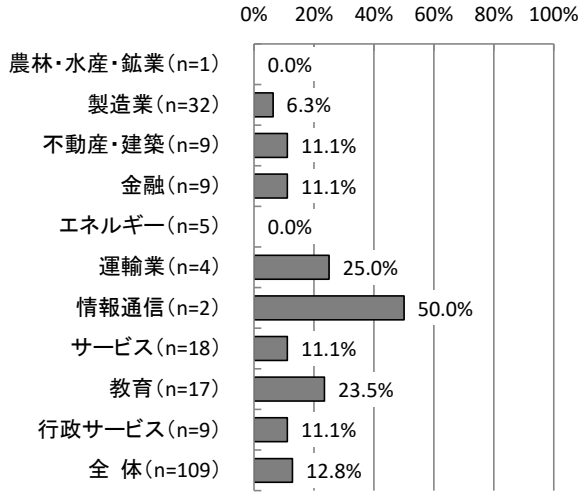
【全体】過去に受けたことのある被害状況（MA, n=109）



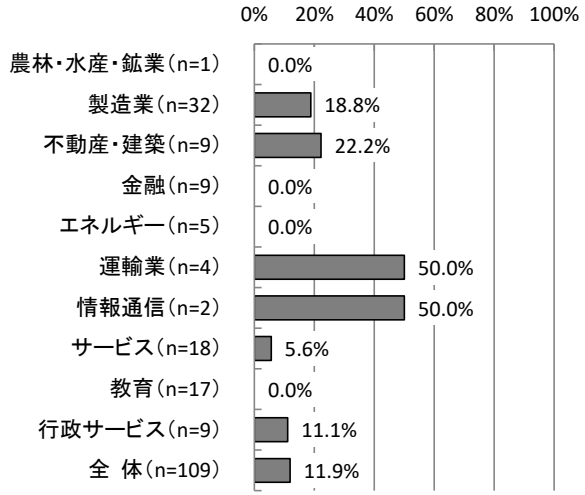
【業種別分析】業種別にみると、「電子メールの不正中継」については、「教育」が23.5%となっている。「ランサムウェア」については、「不動産・建築」が22.2%で最も多くなっている。また、「ウイルス以外の情報流出」については、「エネルギー」が20.0%と最も多くなっている。

【業種別分析】過去に受けたことのある被害状況

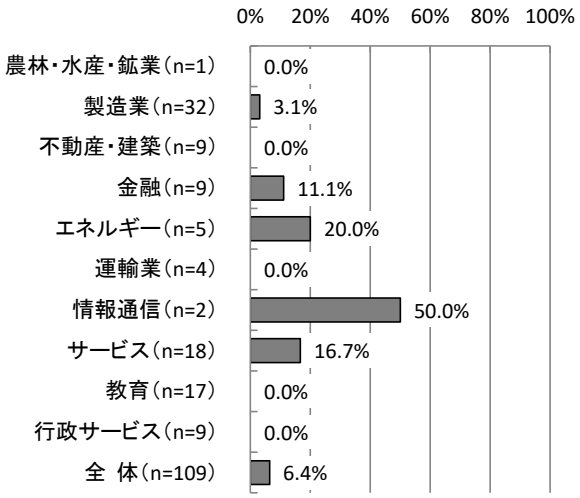
電子メールの不正中継



ランサムウェア

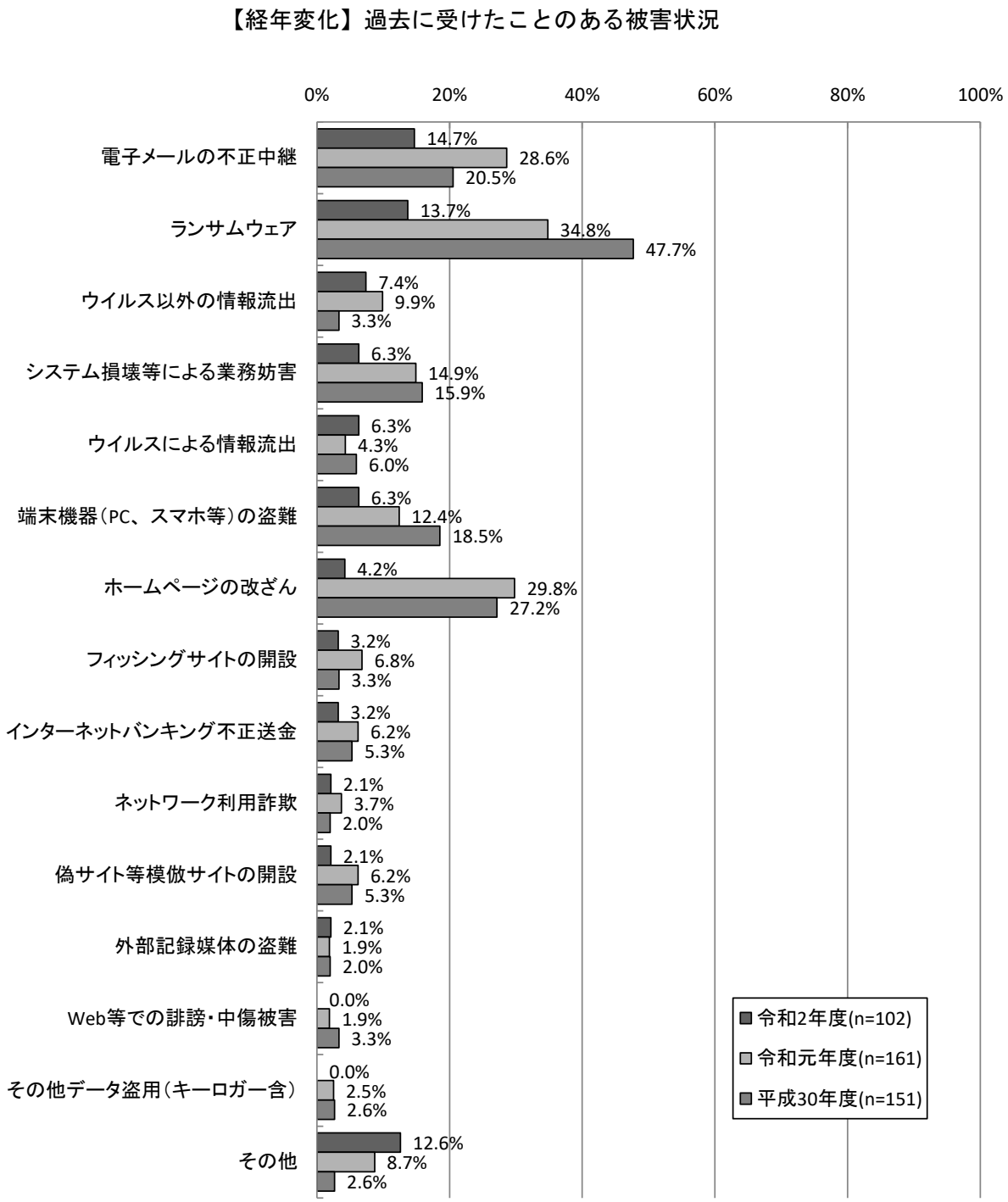


ウイルス以外の情報流出



【経年変化】昨年度と比較すると、「ウイルスによる情報流出」を除く全項目で減少しており、「ランサムウェア」が21.1ポイント、「ホームページの改ざん」が25.6ポイント減少している。

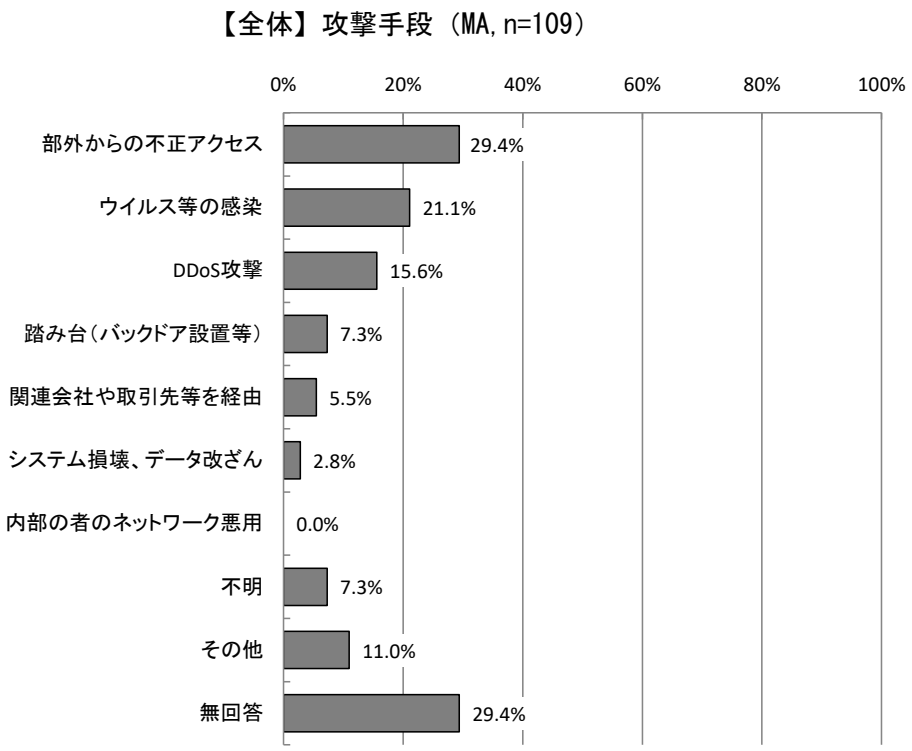
※「無回答」を除いた総数で比較している。



3.1.10　攻撃手段　【問9-1-2】

攻撃手段については、「部外からの不正アクセス」が29.4%で最も多く、次いで「ウイルス等の感染」が21.1%、「DDoS攻撃」が15.6%となっている。

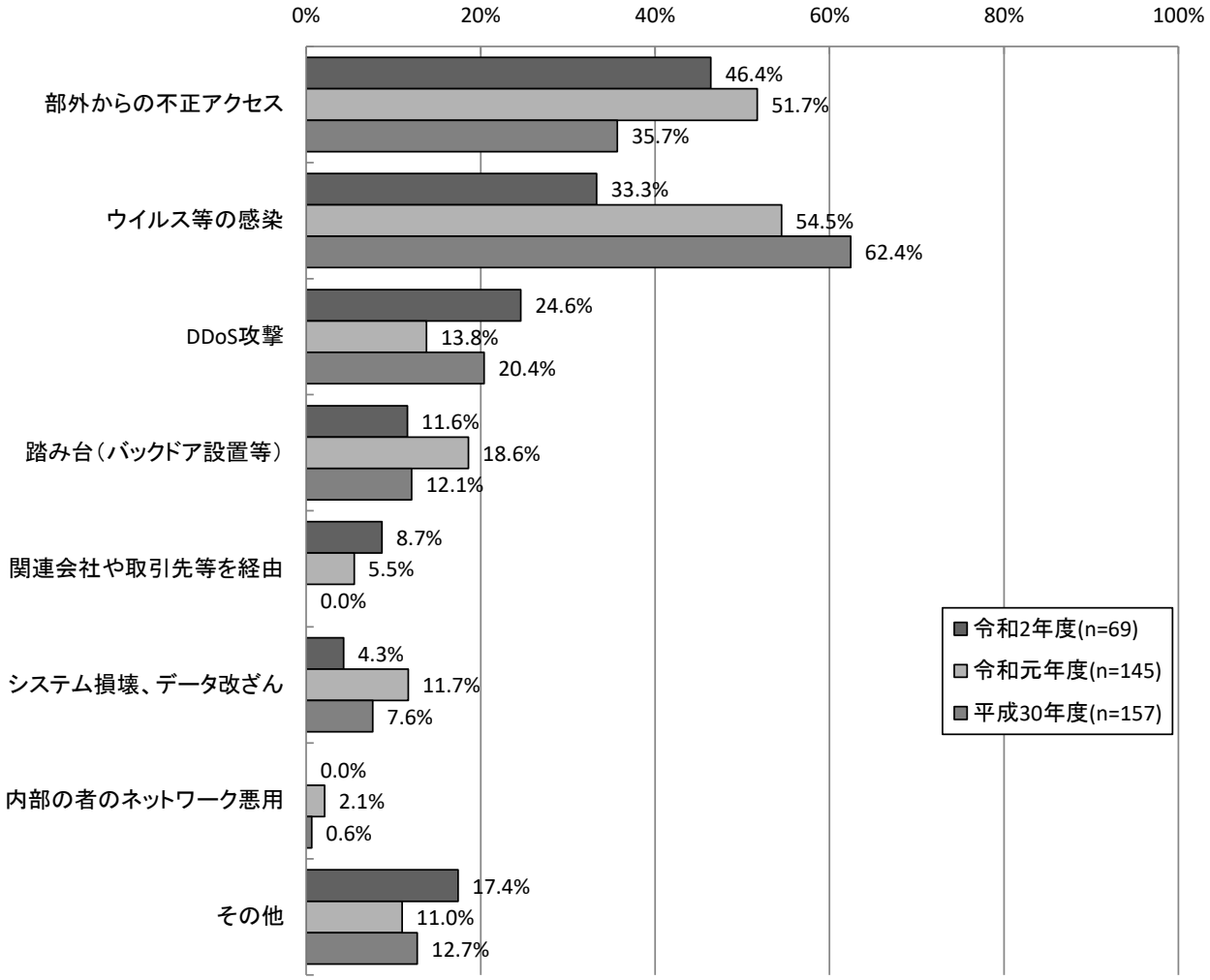
※本項目は、過去に不正アクセス等の被害にあった社・団体等を対象としている。



【経年変化】昨年度と比較すると、8項目中3項目で増加しており、「DDoS攻撃」が10.8ポイント増加し、「ウイルス等の感染」は21.2ポイント減少している。

※「不明」「無回答」を除いた総数で比較している。
※令和元年度調査で「関連会社や取引先等を経由」を新設。

【経年変化】攻撃手段

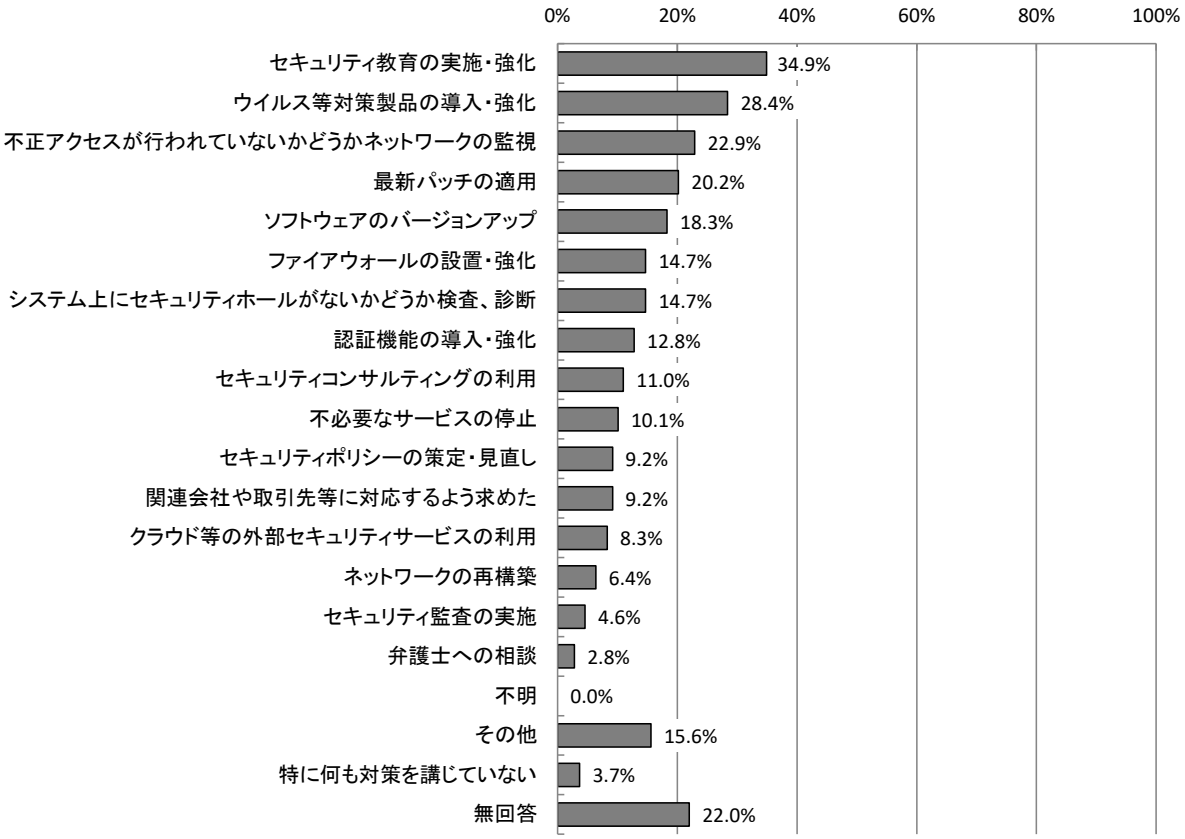


3.1.11　被害を受けたことによる対策　【問9-2】

被害を受けたことによる対策については、「セキュリティ教育の実施・強化」が34.9%で最も多く、次いで「ウイルス等対策製品の導入・強化」が28.4%、「不正アクセスが行われていないかどうかネットワークの監視」が22.9%となっている。

※本項目は、過去に不正アクセス等の被害にあった社・団体等を対象としている。

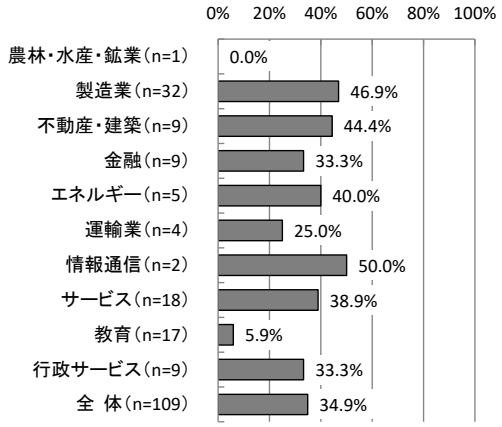
【全体】被害を受けたことによる対策（MA, n=109）



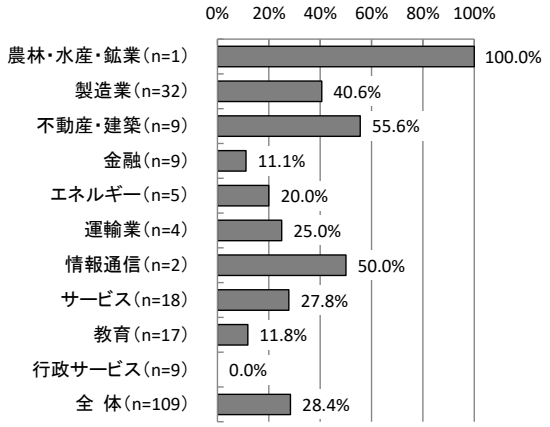
【業種別分析】業種別にみると、「セキュリティ教育の実施・強化」については、「製造業」が46.9%で最も多くなっている。「ウイルス等対策製品の導入・強化」については、「不動産・建築」が55.6%で最も多く、「不正アクセスが行われていないかどうかネットワーク監視」については、「エネルギー」が40.0%で最も多くなっている。

【業種別分析】被害を受けたことによる対策

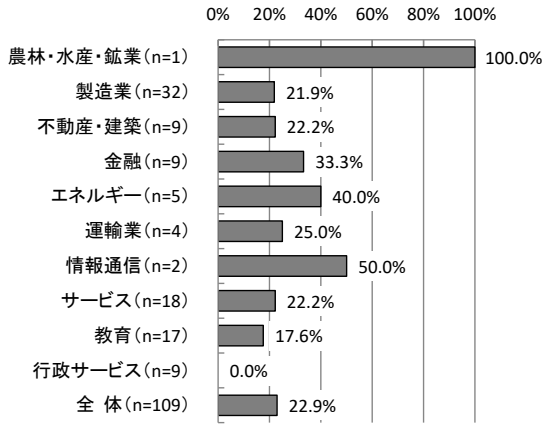
セキュリティ教育の実施・強化



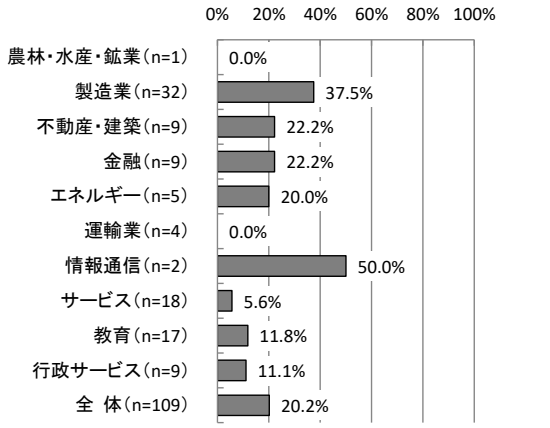
ウイルス等対策製品の導入・強化



不正アクセスが行われていないかどうか
ネットワークの監視

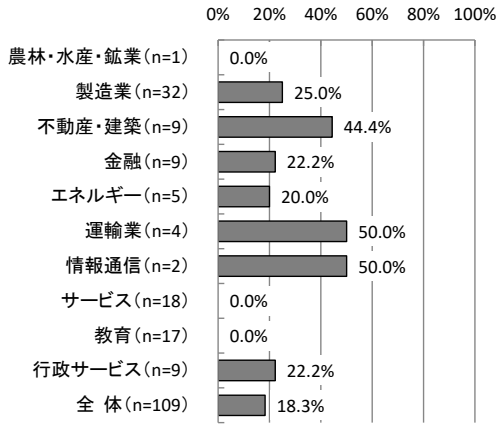


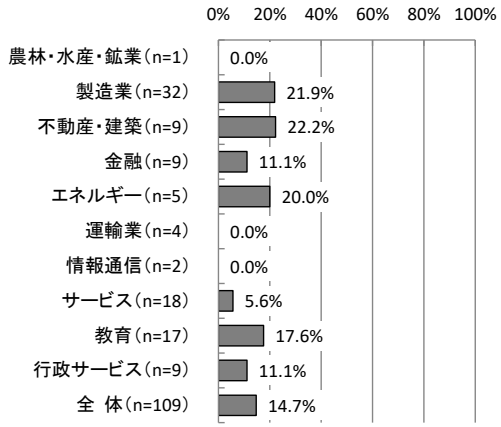
最新パッチの適応



ソフトウェアのバージョンアップ

ファイアウォールの設置・強化



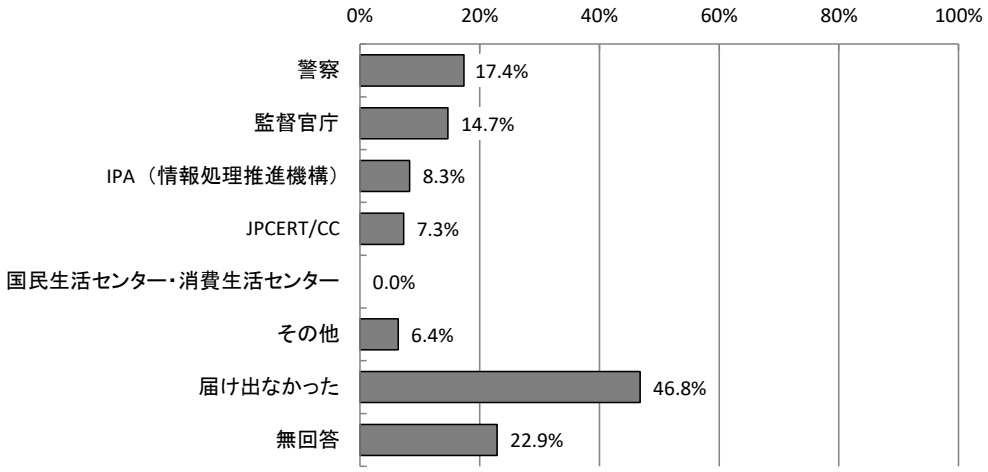


3.1.12 届出先機関等 【問9-3-1】

届出先機関等については、「警察」が17.4%で最も多く、次いで「監督官庁」が14.7%となっている。一方、「届け出なかった」は46.8%となっている。

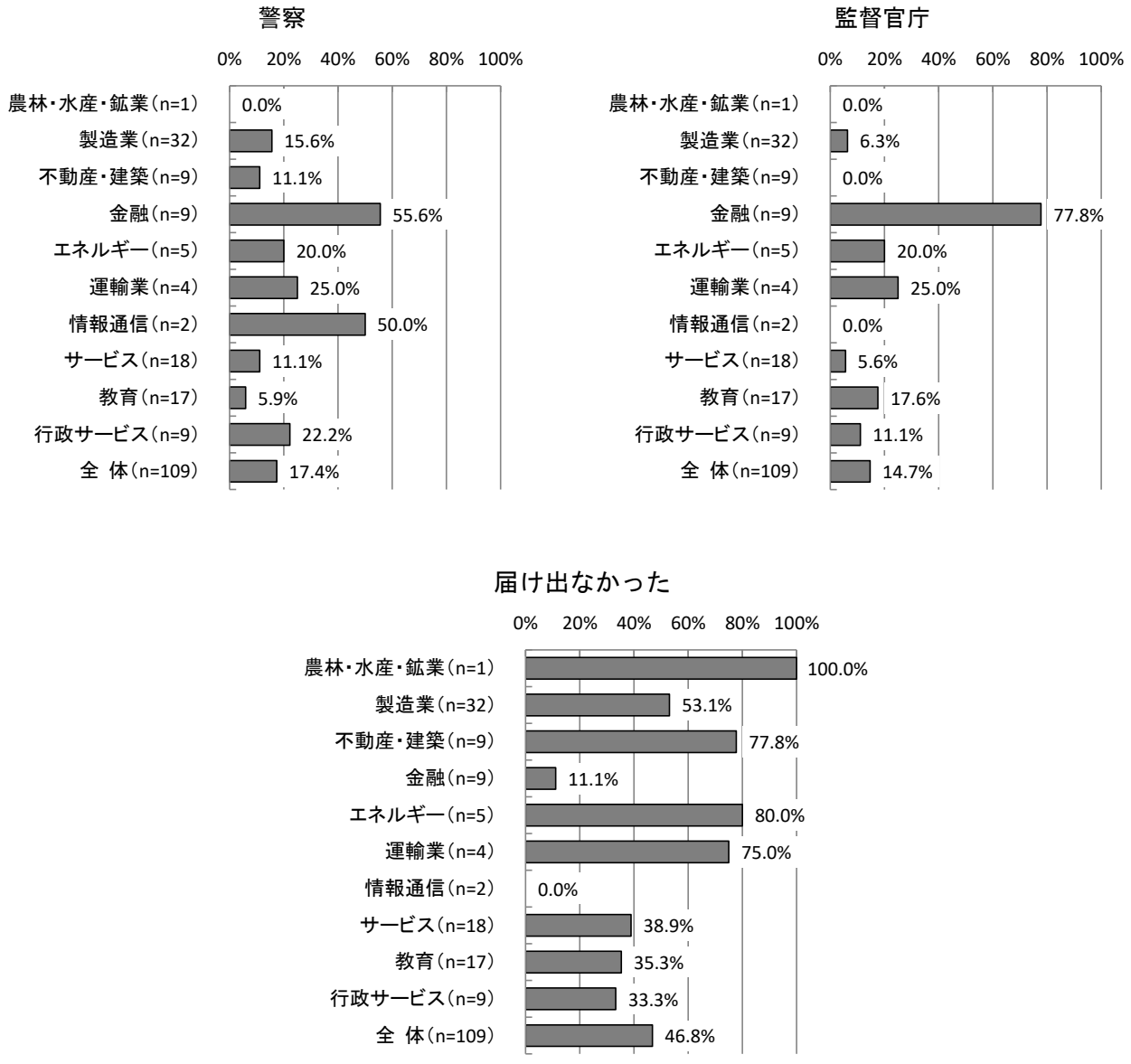
※本項目は、過去に不正アクセス等の被害にあった社・団体等を対象としている。

【全体】届出先機関等（MA, n=109）



【業種別分析】業種別にみると、「警察」については「金融」が55.6%で最も多く、「監督官庁」でも「金融」が77.8%で最も多くなっている。「届け出なかった」については、「エネルギー」が80.0%となっている。

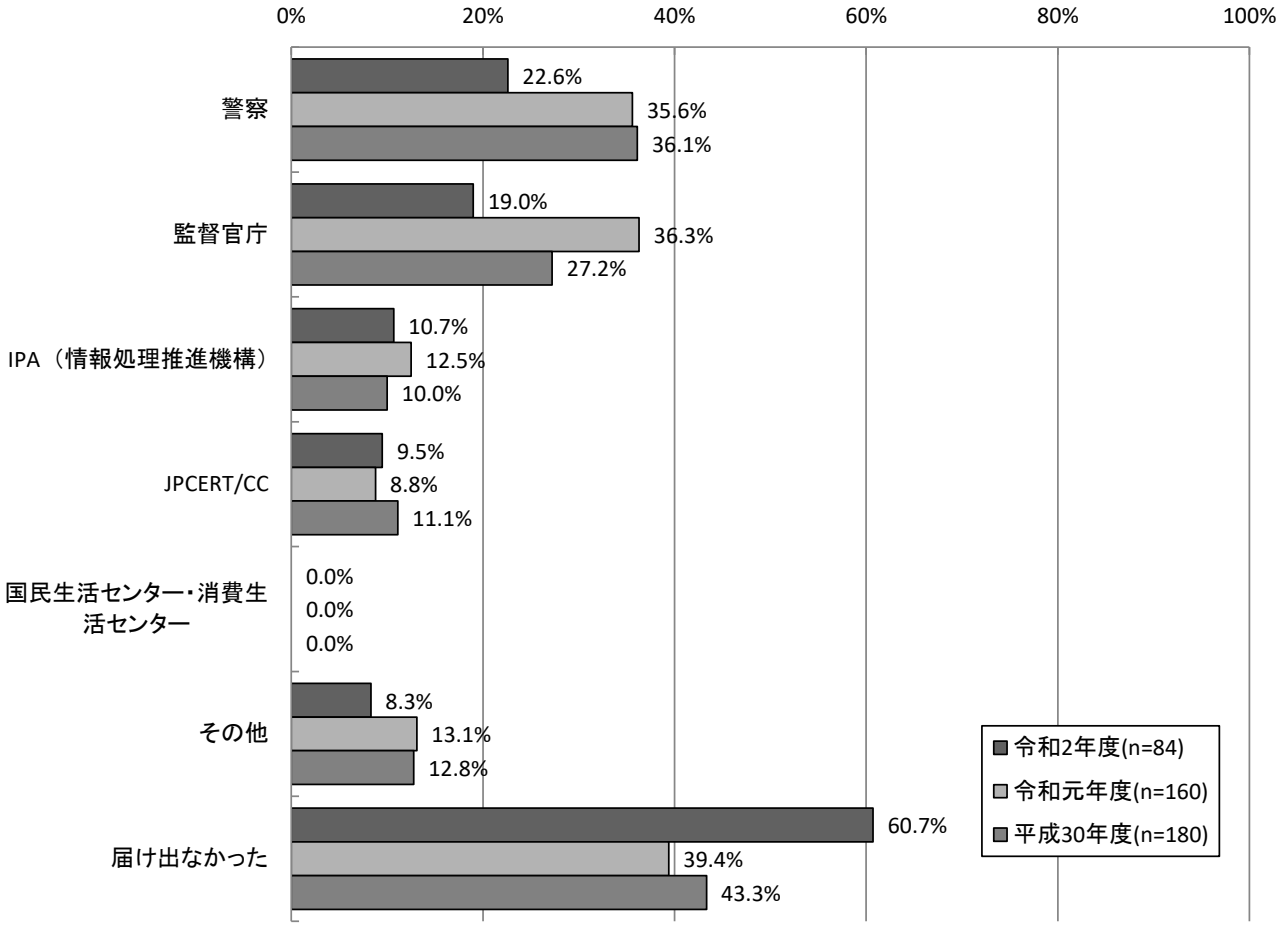
【業種別分析】届出先機関等



【経年変化】昨年度と比較すると、全体的に減少している項目が多く、「警察」は13.0ポイント、「監督官庁」は17.3ポイント、それぞれ減少している。一方で、「届け出なかった」は21.3ポイント増加している。

※「無回答」を除いた総数で比較している。

【経年変化】届出先機関等

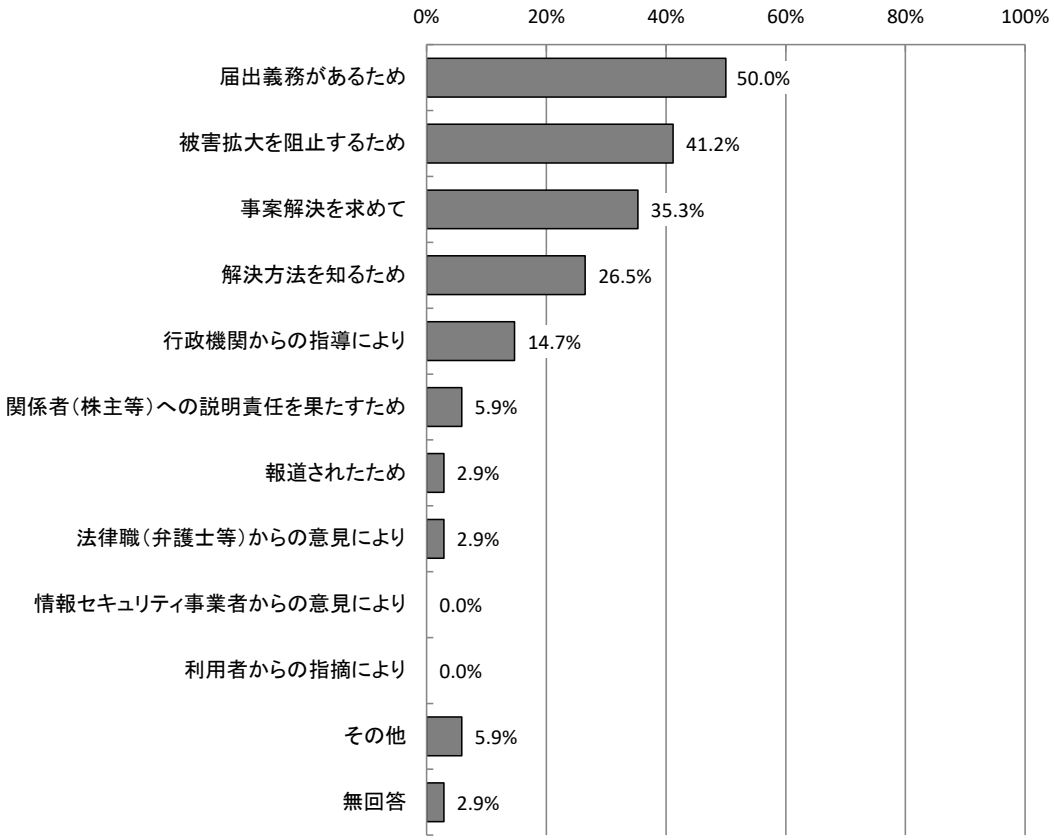


3.1.13　届出した理由　【問9-3-2】

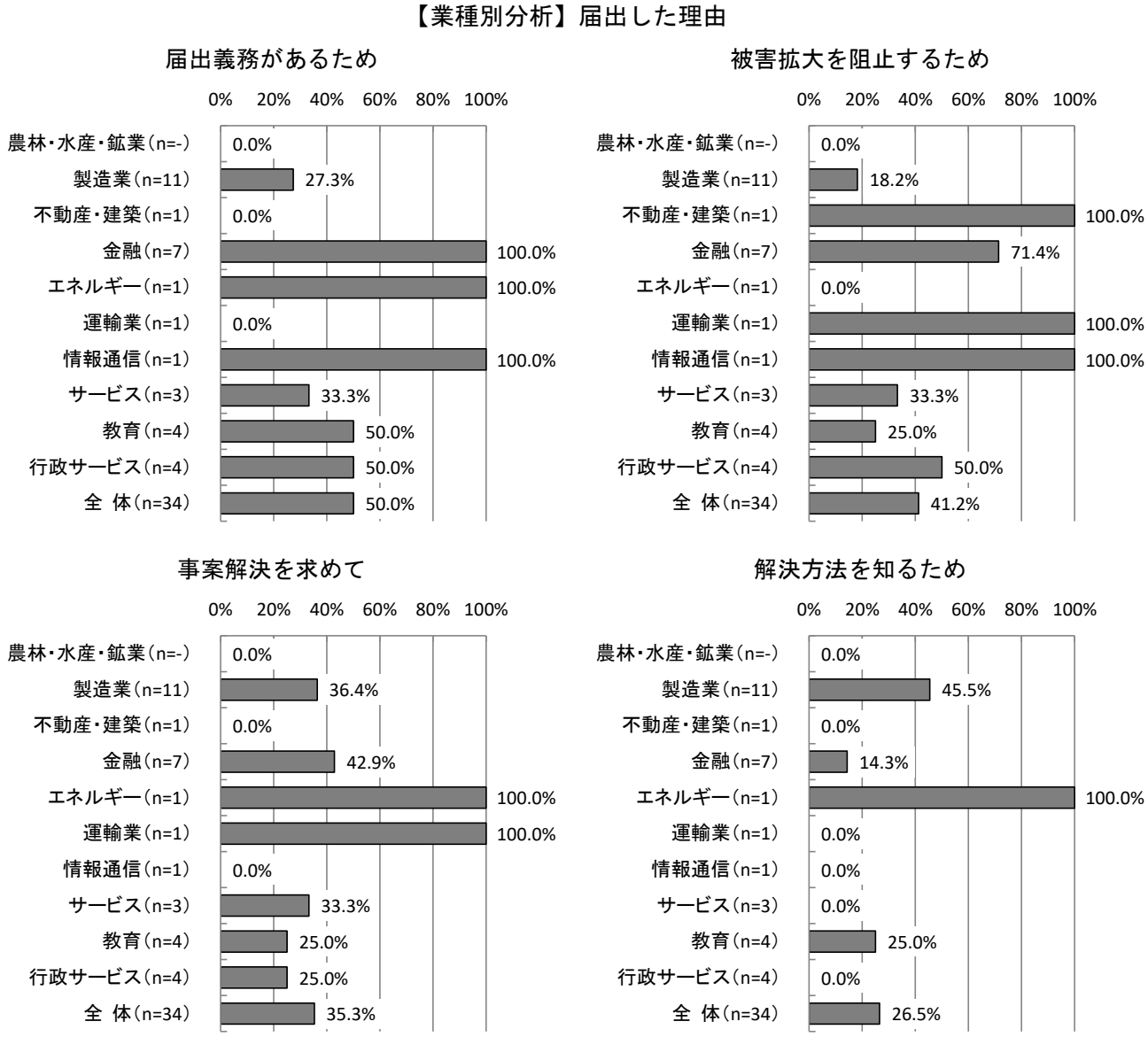
届出した理由については、「届出義務があるため」が50.0%で最も多く、次いで「被害拡大を阻止するため」が41.2%、「事案解決を求めて」が35.3%となっている。

※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=34）

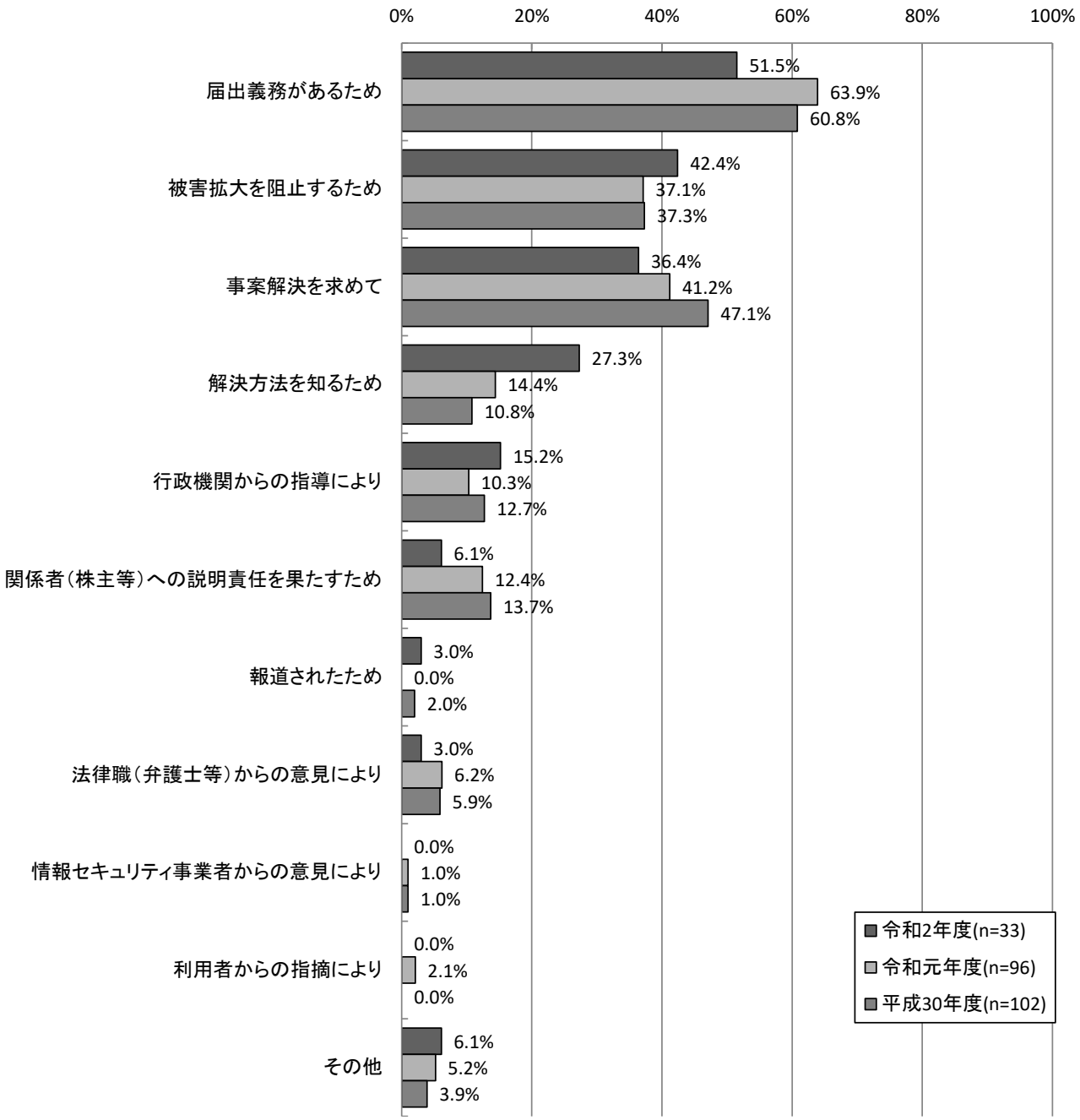


【業種別分析】業種別にみると、「届出義務があるため」については「金融」が100.0%と最も多くなっている。「被害拡大を阻止するため」については「金融」が71.4%と最も多く、次いで「製造業」が18.2%となっている。「事案解決を求めて」については「金融」が42.9%と最も多くなっている。



【経年変化】昨年度と比較すると、「解決方法を知るため」が12.9ポイント増加し、「届出義務があるため」が12.4ポイント減少となっている

※「無回答」を除いた総数で比較している。

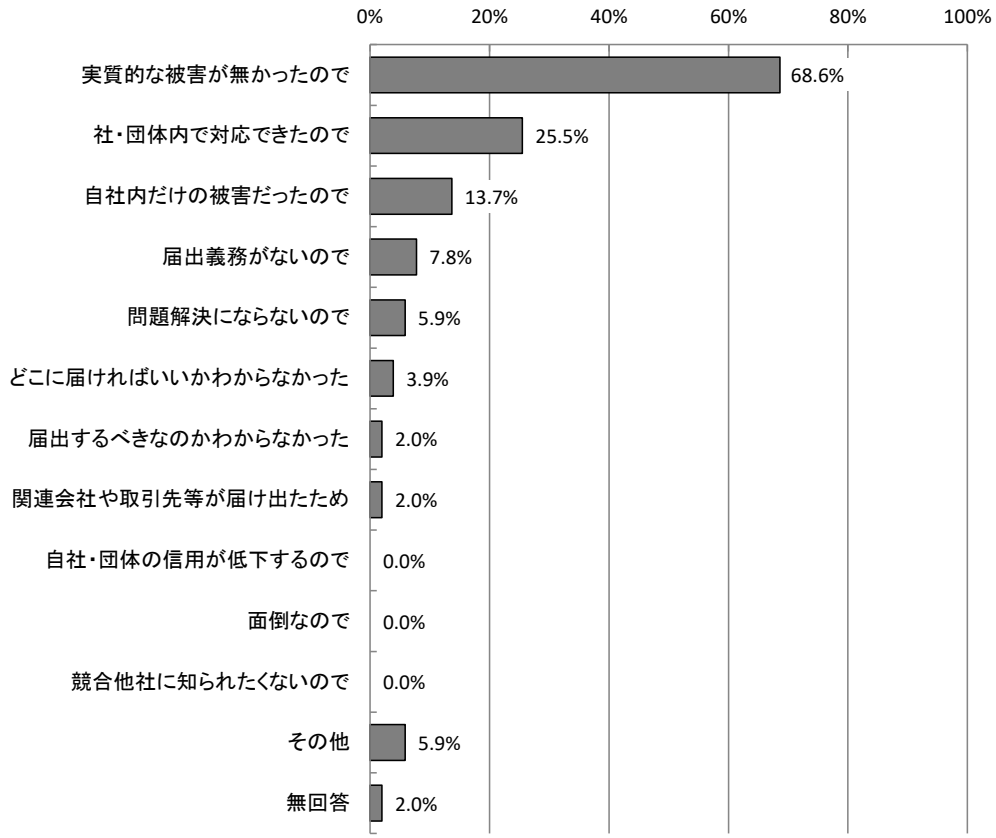


3.1.14　届出を躊躇させる要因　【問9-4】

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68.6%で最も多く、次いで「社・団体内で対応できたので」が25.5%となっている。

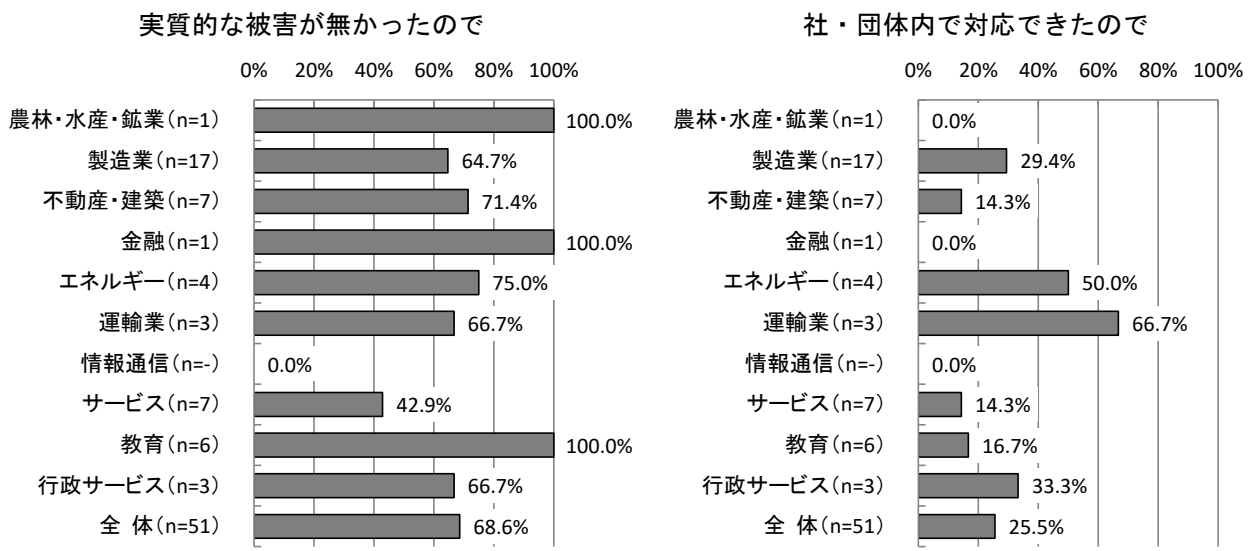
※本項目は、被害の届出を行わなかった社・団体等を対象としている。

【全体】届出を躊躇させる要因（MA, n=51）



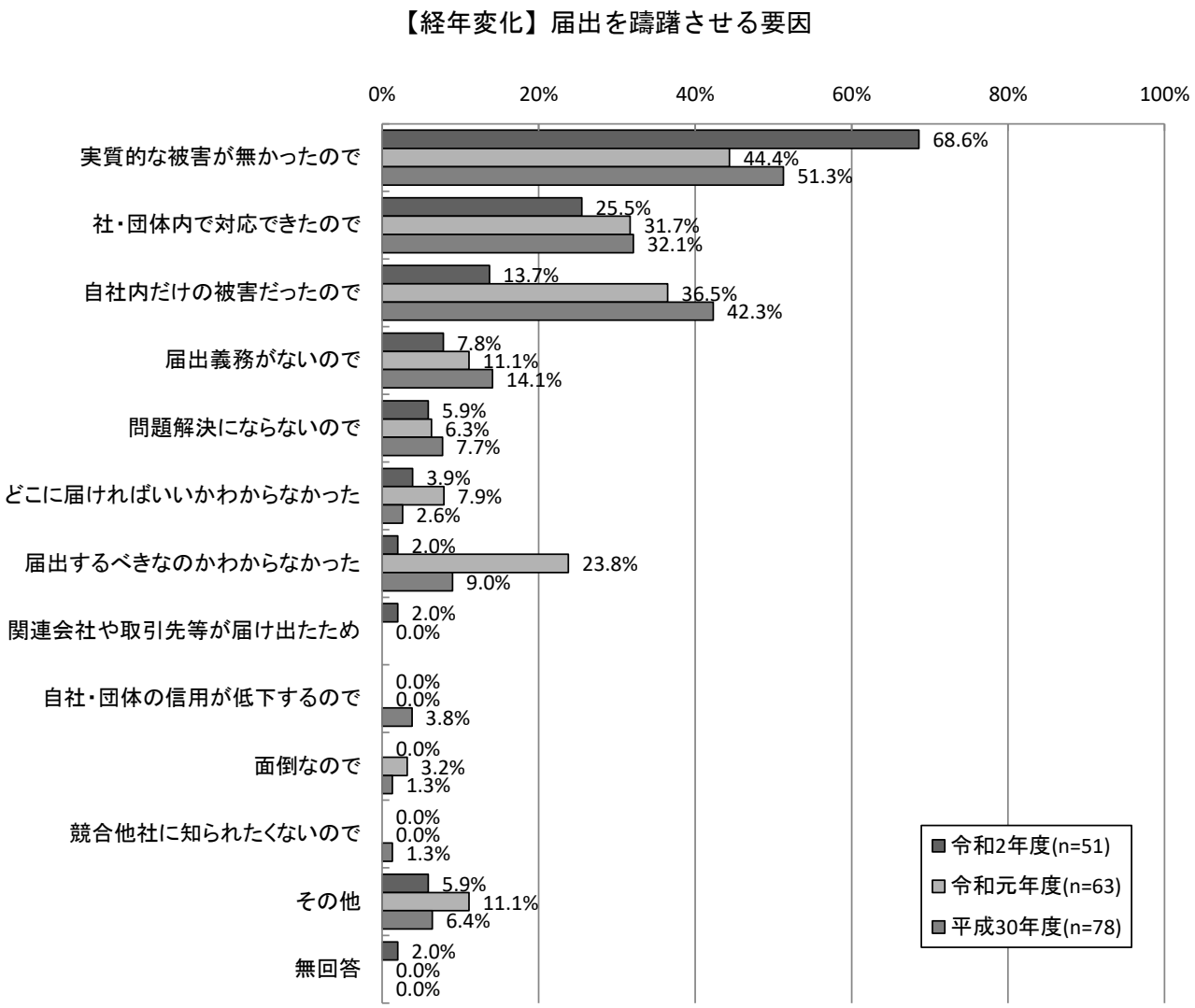
【業種別分析】業種別にみると、「実質的な被害が無かったので」については、「教育」が100.0%、「不動産・建築」が71.4%となっている。「社・団体内で対応できたので」については、「製造業」が29.4%、「教育」が16.7%となっている。

【業種別分析】届出を躊躇させる要因



【経年変化】昨年度と比較すると、「実質的な被害が無かったので」が24.2ポイントの増加であった。一方、「自社内だけの被害だったので」は22.8ポイント、「届出するべきなのかわからなかった」は21.8ポイント減少している。

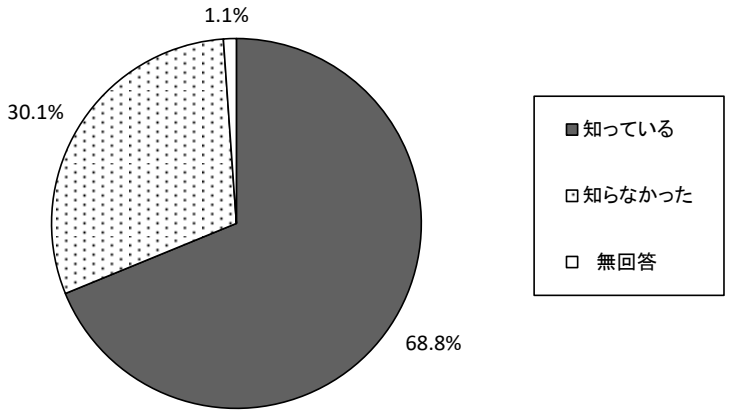
※令和元年度調査で「関連会社や取引先等が届け出たため」を新設



3.1.15　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10】

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68.8%、「知らなかった」は30.1%となっている。

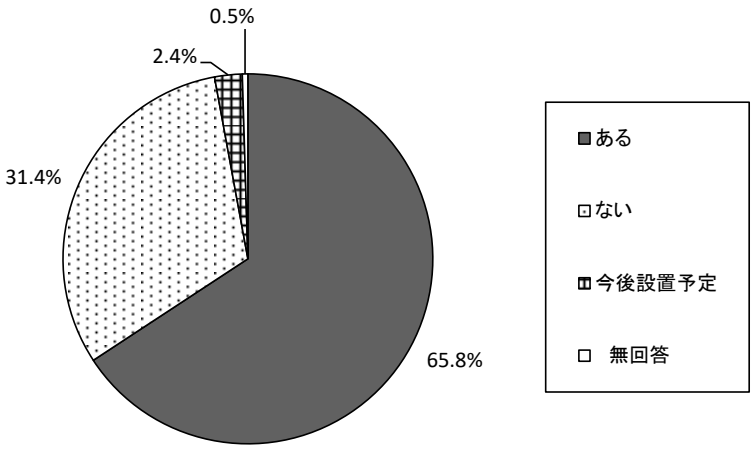
【全体】不正アクセス禁止法でアクセス管理者による防御措置についての努力義務（SA,n=622）



3.1.16　情報セキュリティ運用・管理専門部署の有無　【問11】

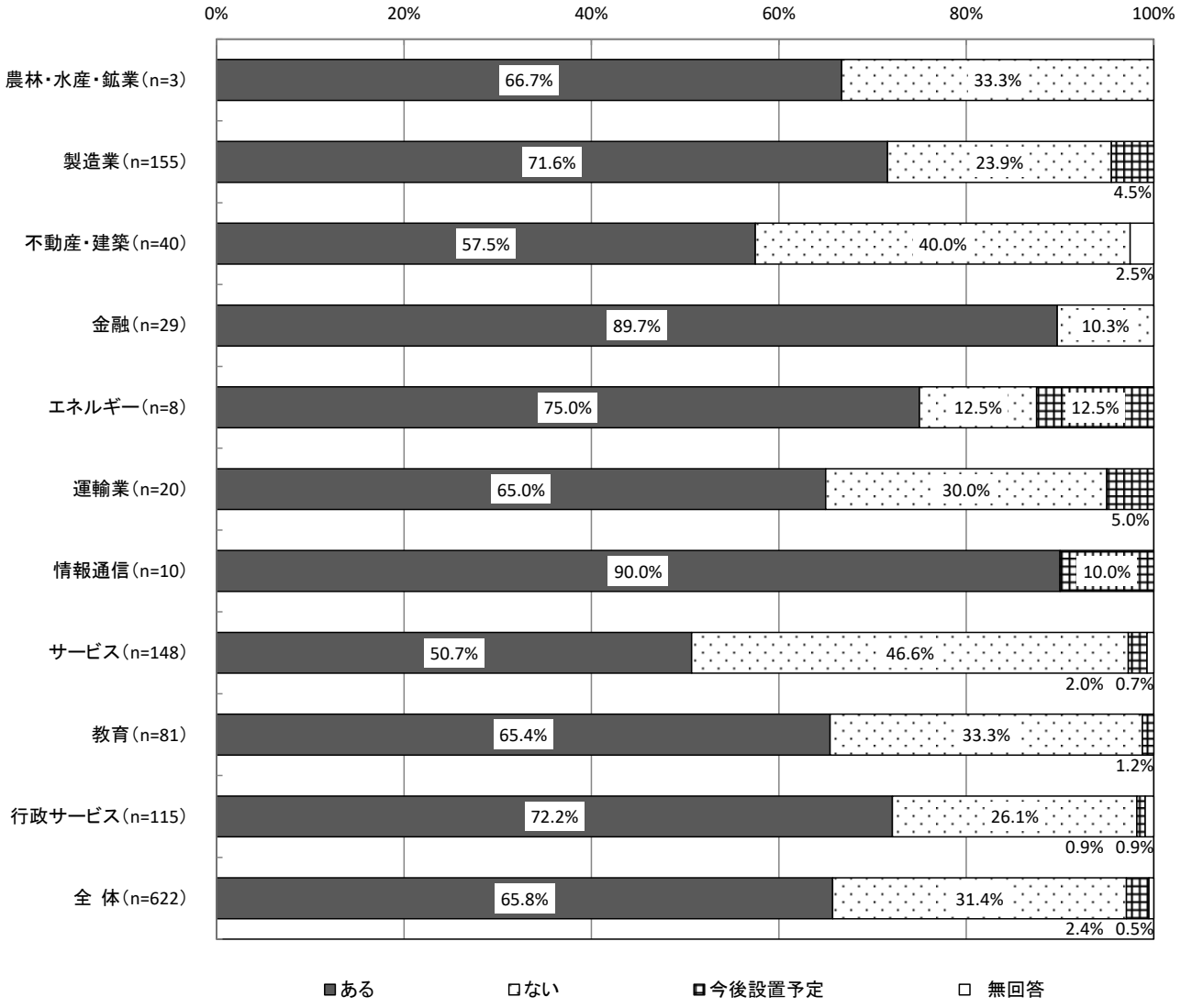
情報セキュリティ運用・管理専門部署の有無については、「ある」が65.8%、「ない」が31.4%となっている。

【全体】情報セキュリティ運用・管理専門部署の有無（SA,n=622）

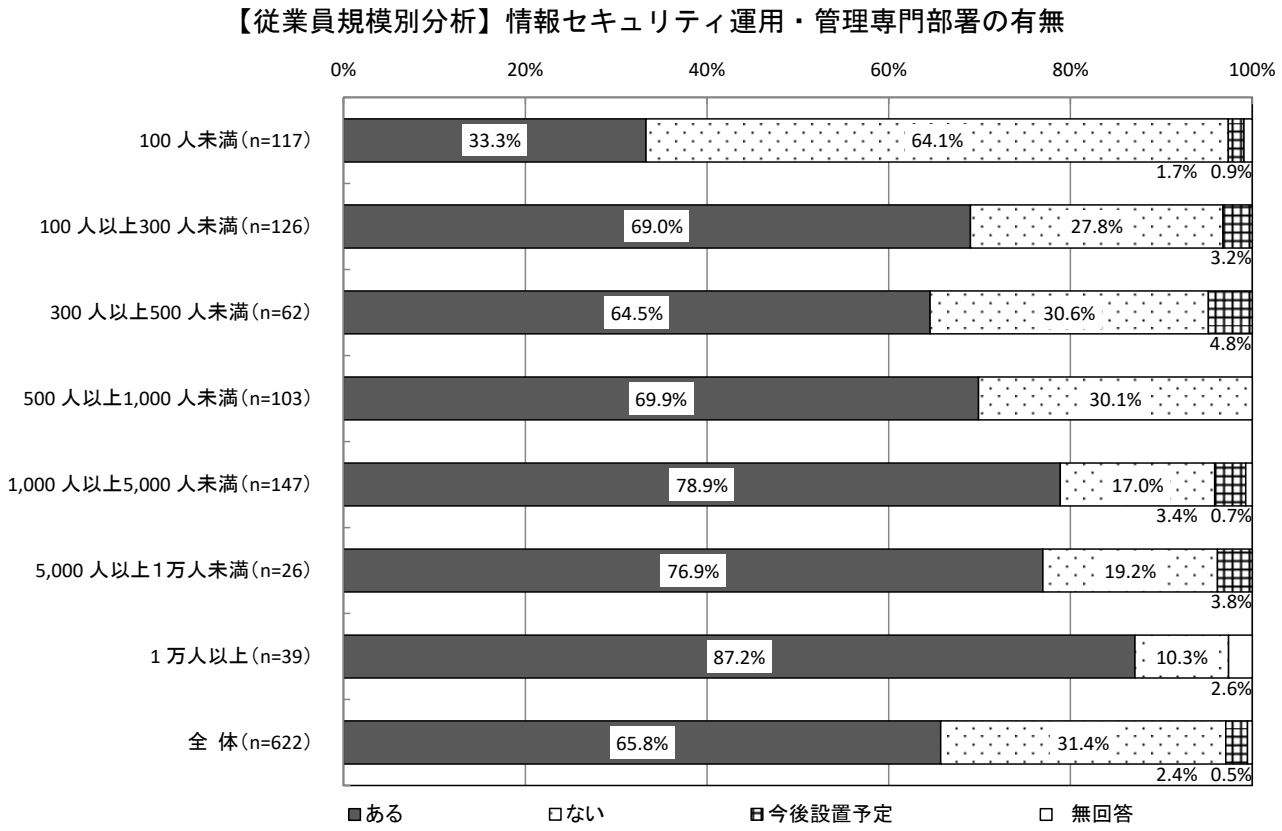


【業種別分析】業種別にみると、情報セキュリティ運用・管理専門部署が「ある」については、「情報通信」が 90.0%で最も多く、次いで「金融」が 89.7%となっている。一方、情報セキュリティ運用・管理専門部署が「ない」については、「サービス」が 46.6%となっている。

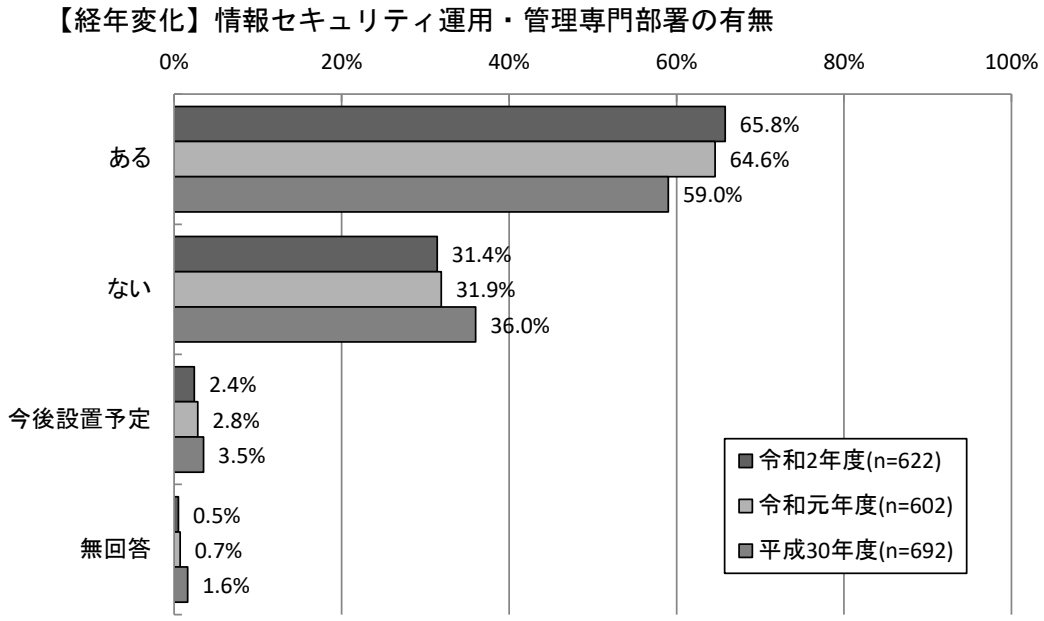
【業種別分析】情報セキュリティ運用・管理専門部署の有無



【従業員規模別分析】従業員規模別にみると、「ある」は「１万人以上」で87.2%と最も多くなっている。一方、「ない」は「100人未満」で64.1%と最も多くなっている。



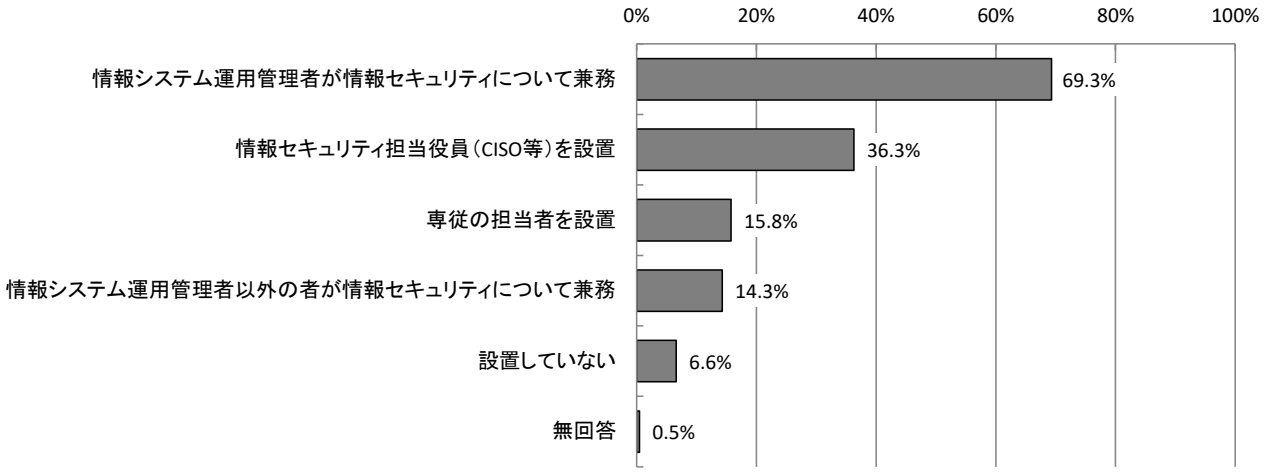
【経年変化】昨年度と比較すると、「ある」が1.2ポイント増加している。



3.1.17　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69.3%で最も多く、次いで「情報セキュリティ担当役員（ＣＩＳＯ等）を設置」が36.3%、「専従の担当者を設置」は15.8%となっている。

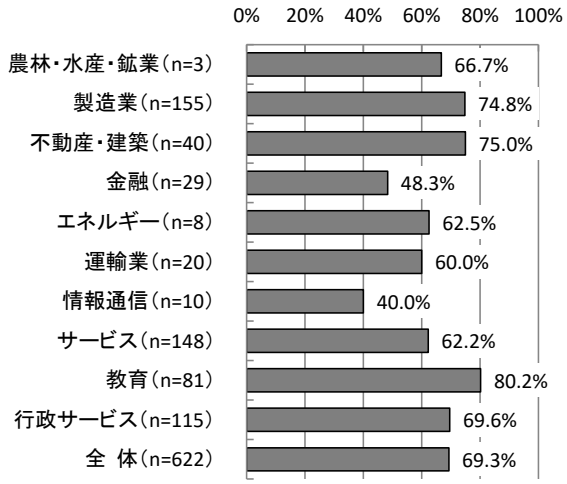
【全体】情報セキュリティ管理体制（MA, n=622）



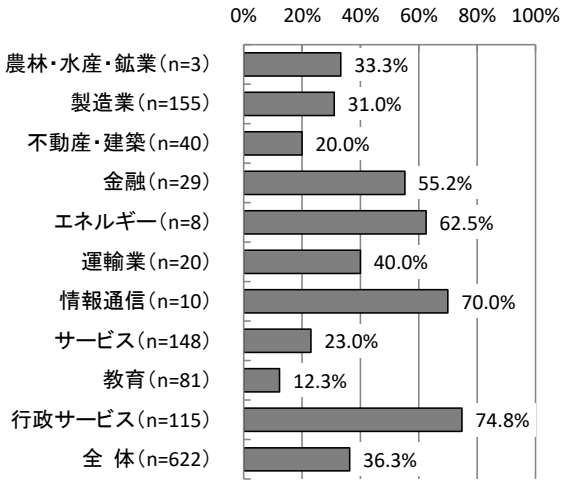
【業種別分析】業種別にみると、「情報システム運用管理者が情報セキュリティについて兼務」については、「教育」が80.2%で最も多く、次いで「不動産・建築」が75.0%となっている。「情報セキュリティ担当役員（ＣＩＳＯ等）を設置」については、「行政サービス」が74.8%で最も多く、次いで「情報通信」が70.0%となっている。「専従の担当者を設置」では、「エネルギー」が62.5%で最も多い。

【業種別分析】情報セキュリティ管理体制

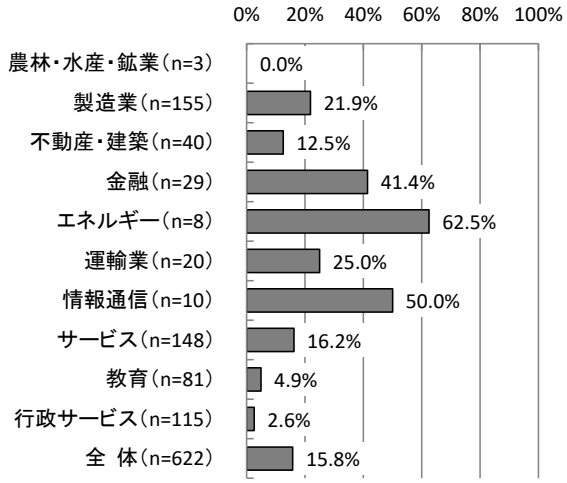
情報システム運用管理者が情報セキュリティについて兼務



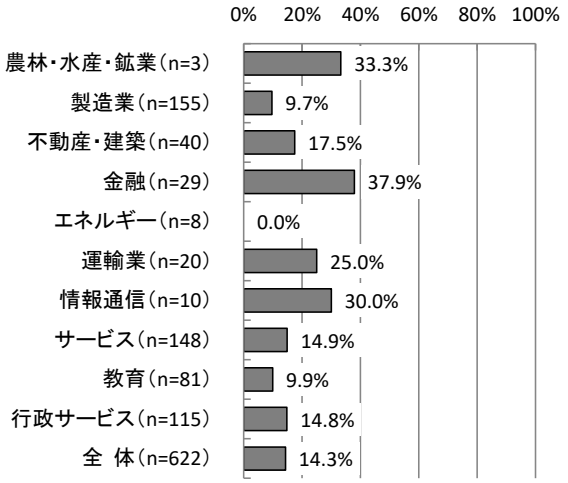
情報セキュリティ担当役員（ＣＩＳＯ等）を設置



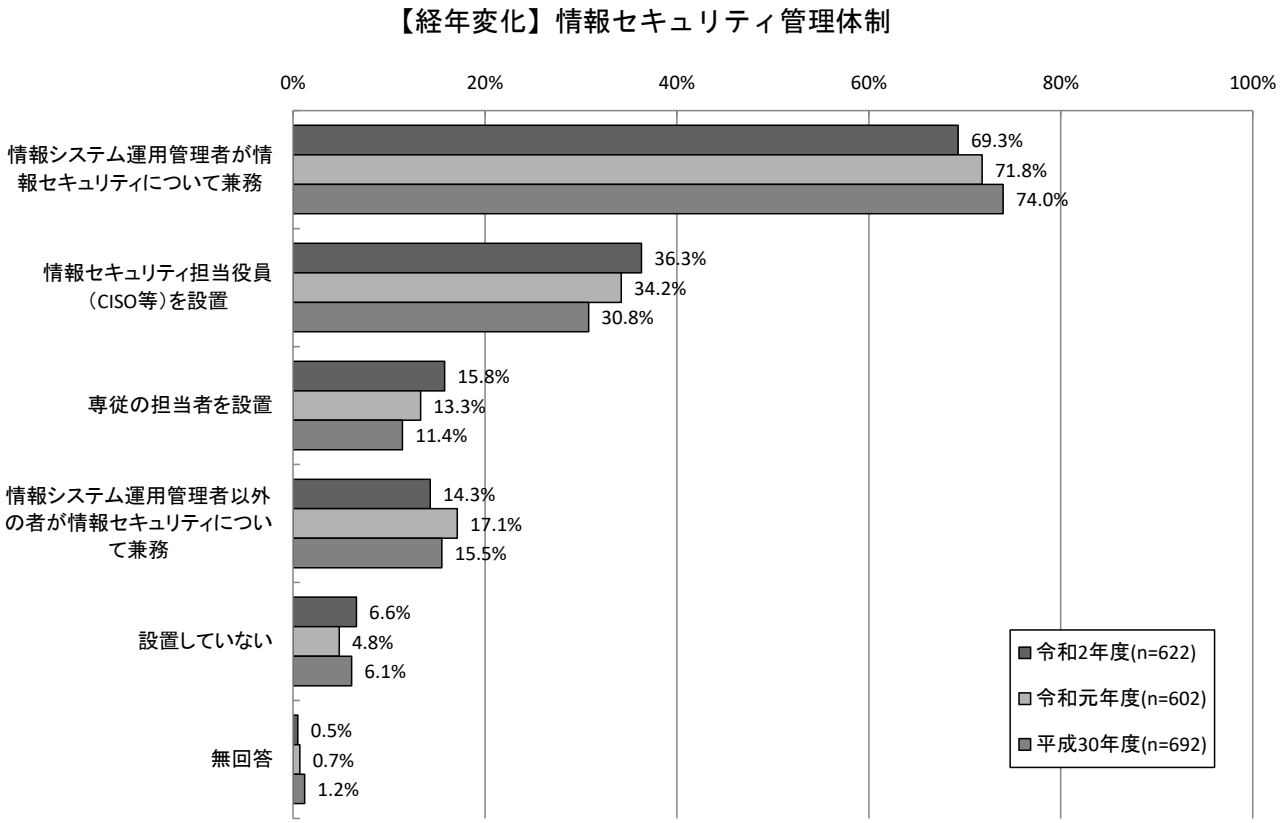
専従の担当者を設置



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



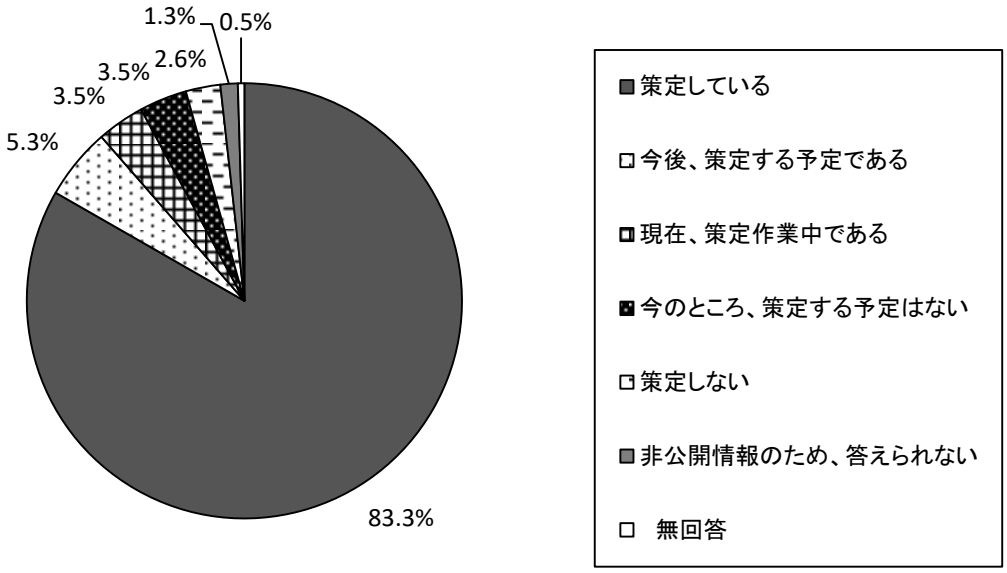
【経年変化】昨年度と比較すると、「専従の担当者を設置」が2.5ポイント増加している。一方、「情報システム運用管理者以外の者が情報セキュリティについて兼務」は2.8ポイント減少している。



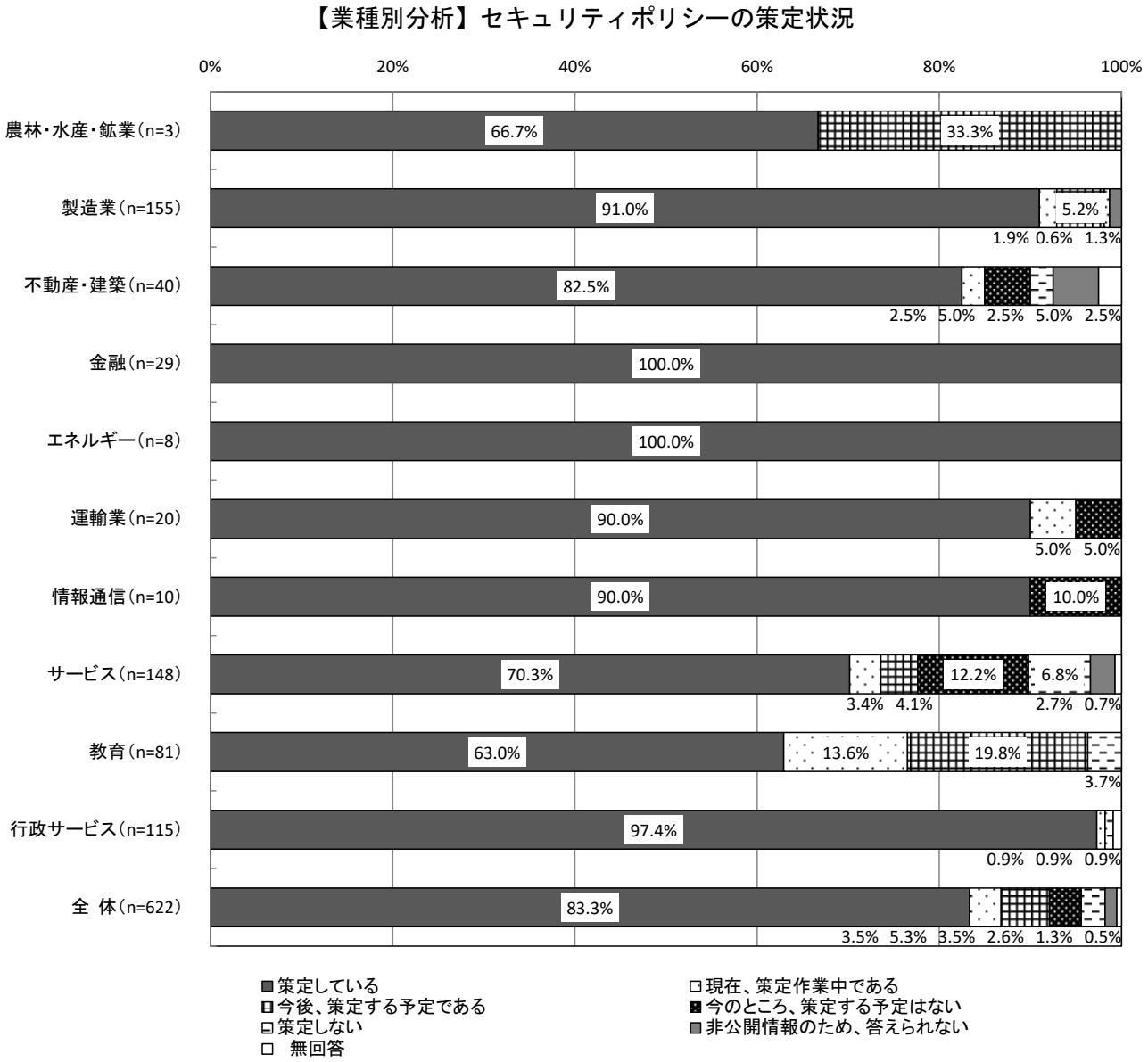
3.1.18　セキュリティポリシーの策定状況　【問13】

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」が83.3%で最も多く、次いで「今後、策定する予定である」が5.3%、「現在、策定作業中である」「今のところ、策定する予定はない」が3.5%となっている。「策定している」「今後、策定する予定である」「現在、策定作業中である」を加えた「策定（予定）」は、全体の92.1%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=622）



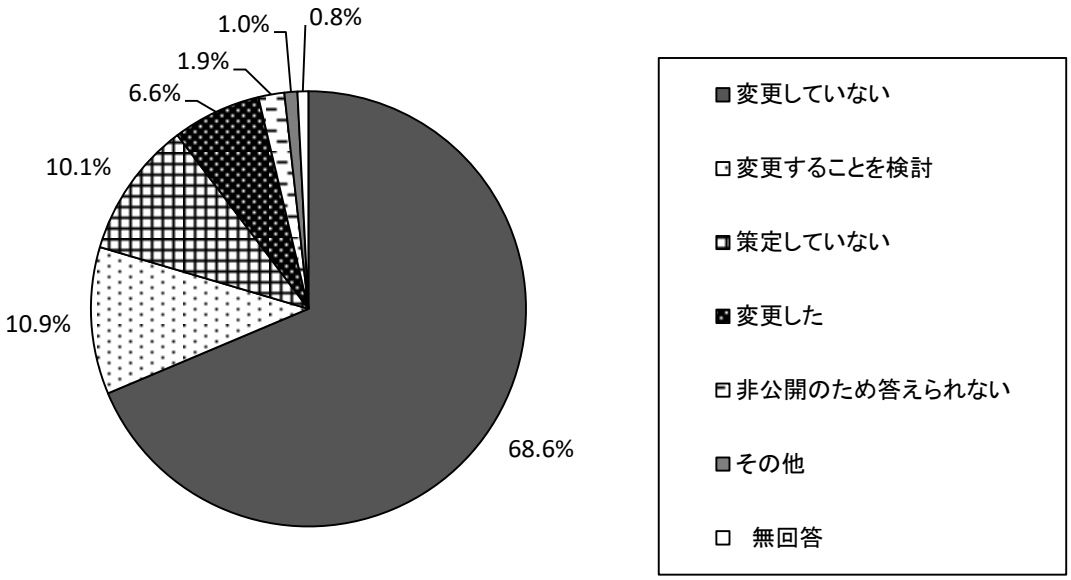
【業種別分析】業種別にみると、セキュリティポリシーを「策定している」については「金融」「エネルギー」が100.0%、「行政サービス」が97.4%、「製造業」が91.0%、「運輸業」「情報通信」が90.0%と9割を超えている。



3.1.19　新型コロナウィルスの影響によるセキュリティポリシーの策定変更状況　【問13-1】

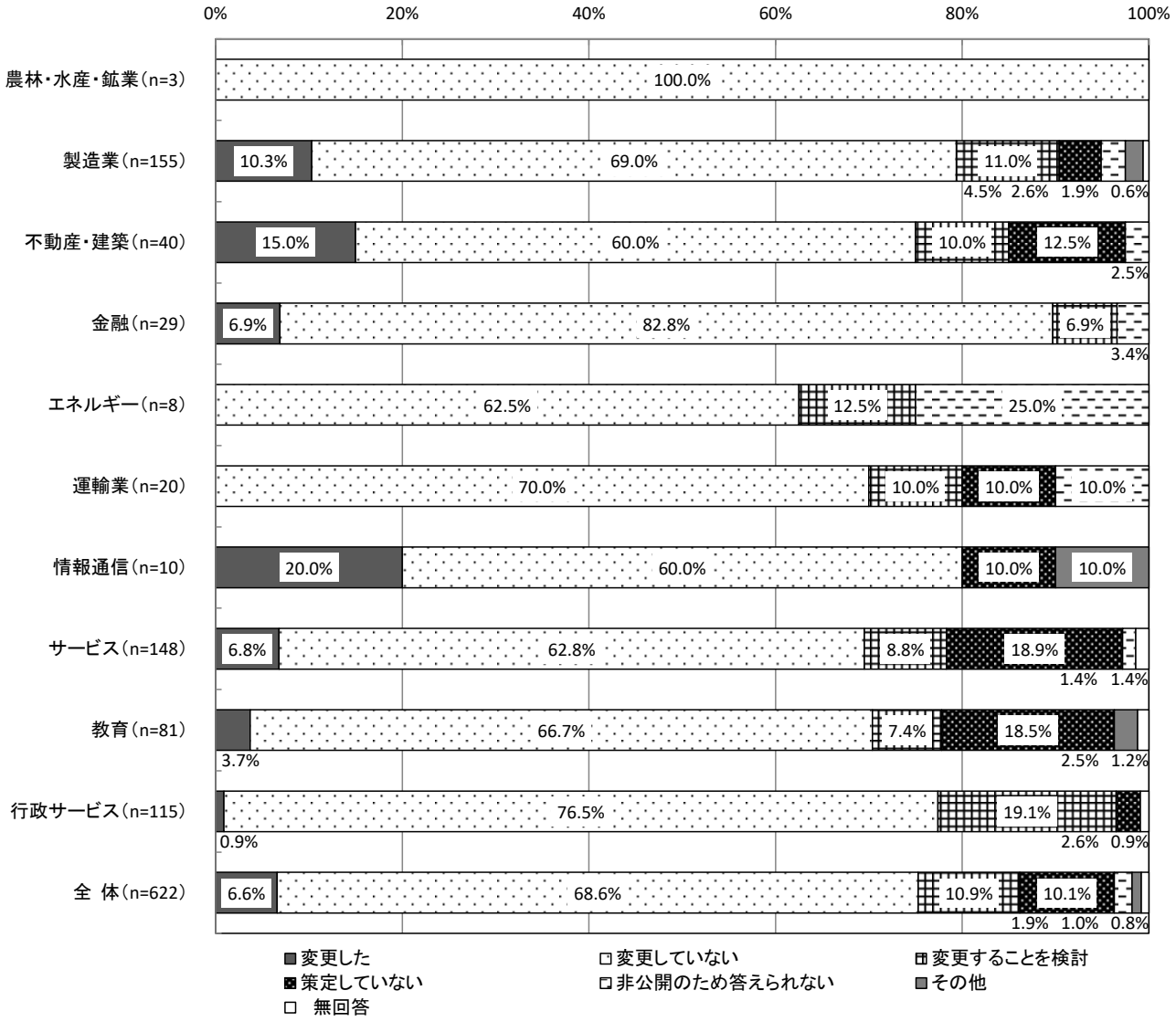
新型コロナウィルスの影響によるセキュリティポリシーの策定変更状況については、「変更していない」が68.6%で最も多く、次いで「変更することを検討」が10.9%、「策定していない」が10.2%となっている。

【全体】新型コロナウィルスの影響による**セキュリティポリシーの策定**変更**状況**（SA,n=622）



【業種別分析】業種別にみると、新型コロナウィルスの影響によるセキュリティポリシーの策定変更を「変更していない」については「金融」が82.8%で最も多く、次いで「行政サービス」が76.5%となっている。

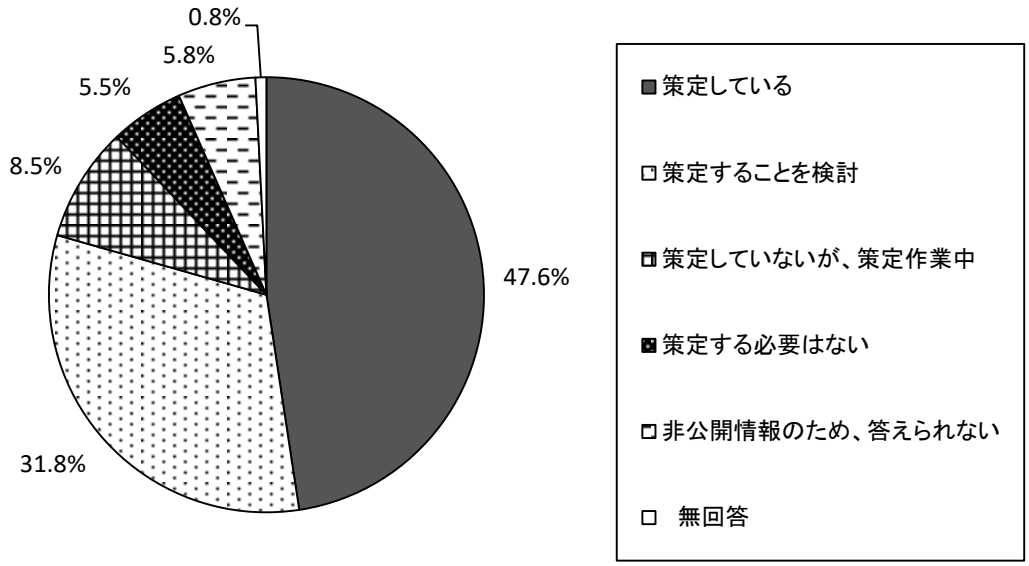
【業種別分析】新型コロナウィルスの影響によるセキュリティポリシーの策定変更状況



3.1.20　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14】

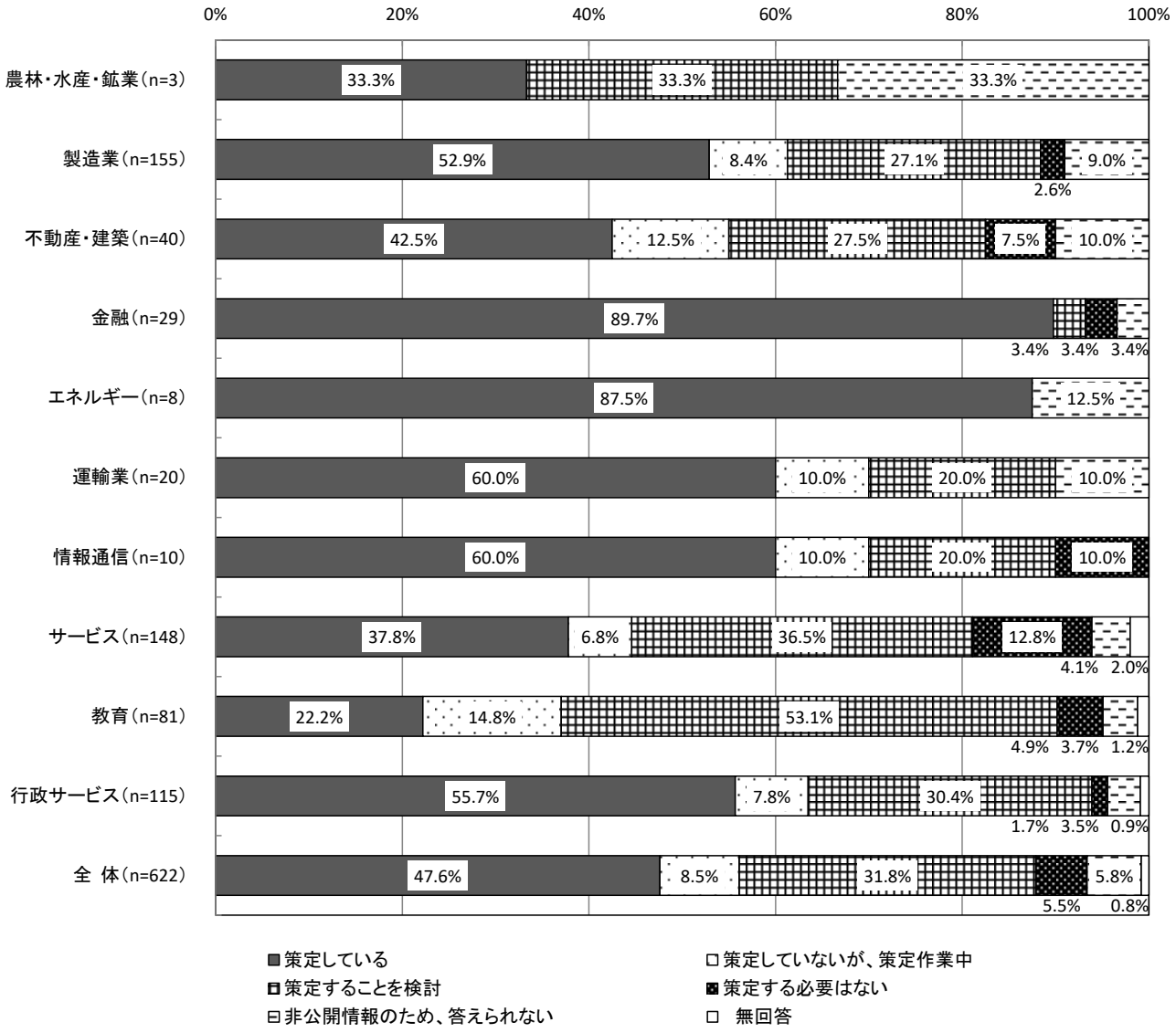
情報セキュリティ侵害事案発生時の対応マニュアル等の策定状況については、「策定している」が47.6%で最も多く、次いで「策定することを検討」が31.8%となっている。

【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=622）



【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」が89.7%で最も多く、次いで「エネルギー」が87.5%となっている。

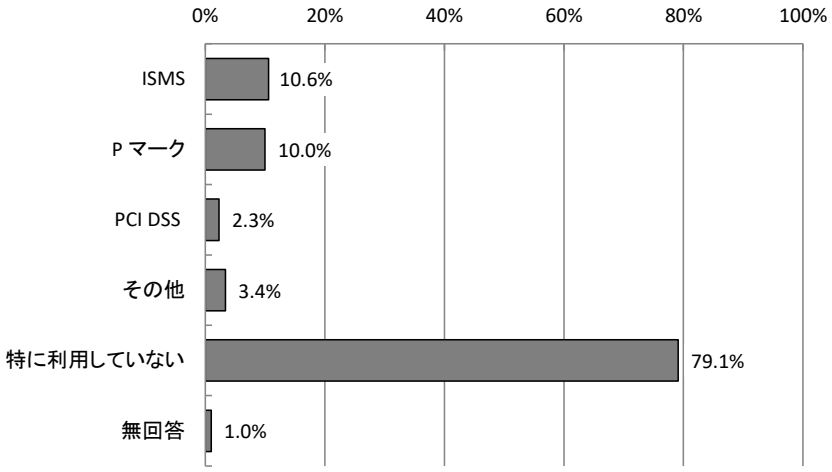
【業種別分析】情報セキュリティ侵害事案発生時の対応マニュアル等の策定状況



3.1.21　第三者機関の認証制度等の利用状況　【問15】

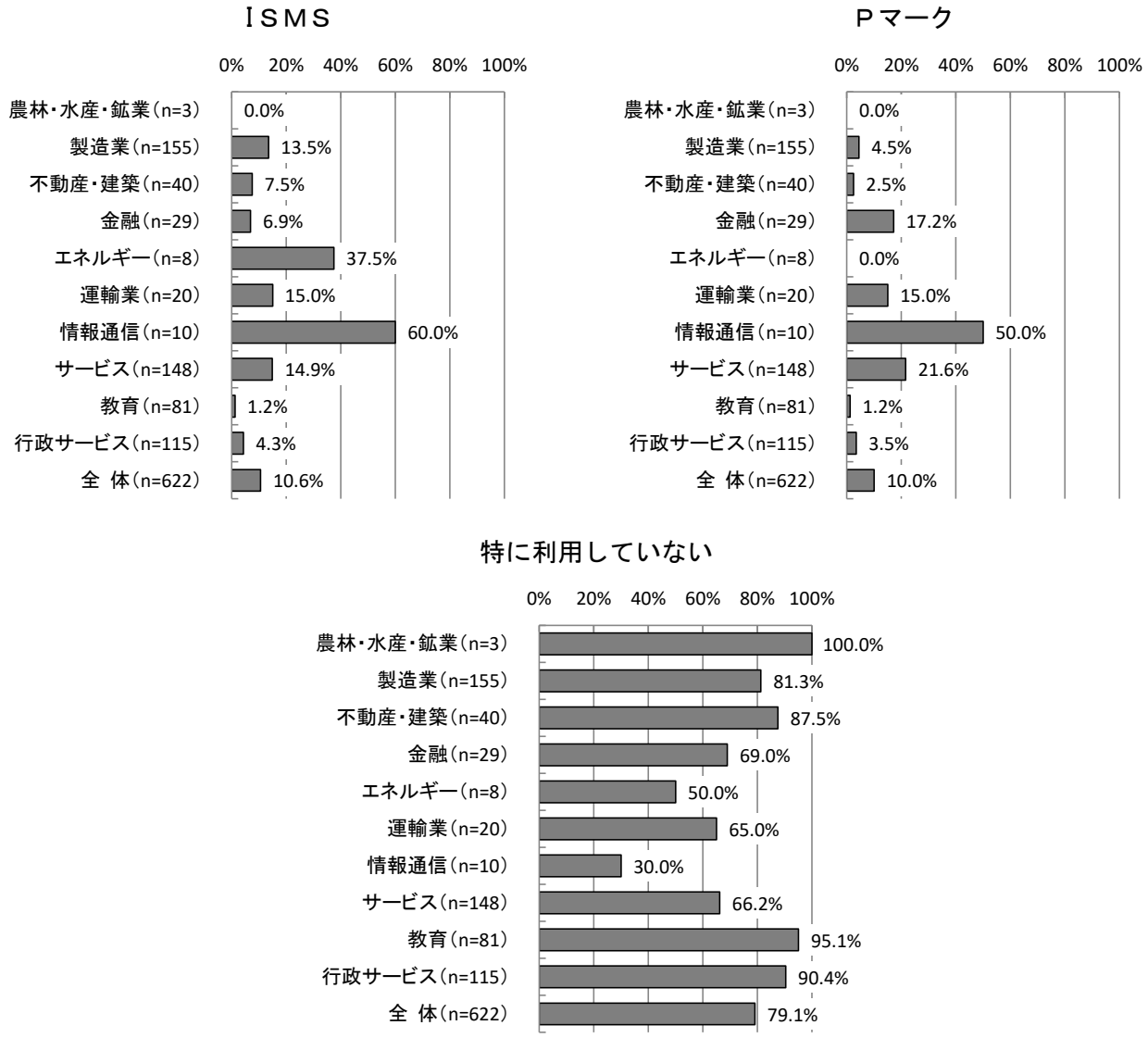
第三者機関の認証制度等の利用状況については、「特に利用していない」が79.1％で最も多く、次いで「ＩＳＭＳ」が10.6％、「Ｐマーク」が10.0％となっている。

【全体】第三者機関の認証制度等の利用状況（MA, n=622）



【業種別分析】業種別にみると、「ＩＳＭＳ」については、「情報通信」が60.0％で最も多くなっている。「特に利用していない」については、「教育」が95.1％で最も多く、次いで「行政サービス」が90.4％となっている。

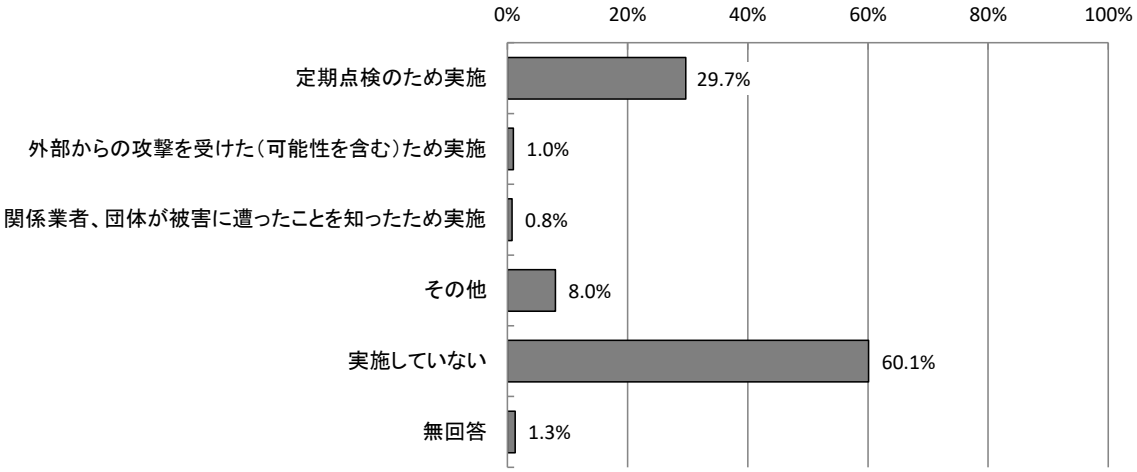
【業種別分析】第三者機関の認証制度等の利用状況



3.1.22　ぜい弱性調査（ペネトレーションテスト）実施の有無　【問16】

ぜい弱性調査（ペネトレーションテスト）実施の有無については、「実施していない」が60.1%で最も多い。実施しているとの回答では、「定期点検のため実施」が29.7%と多くなっている。

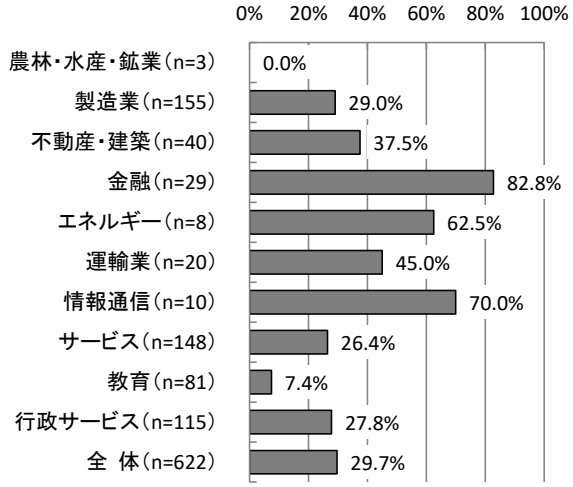
【全体】ぜい弱性調査（ペネトレーションテスト）実施の有無（MA,n=622）



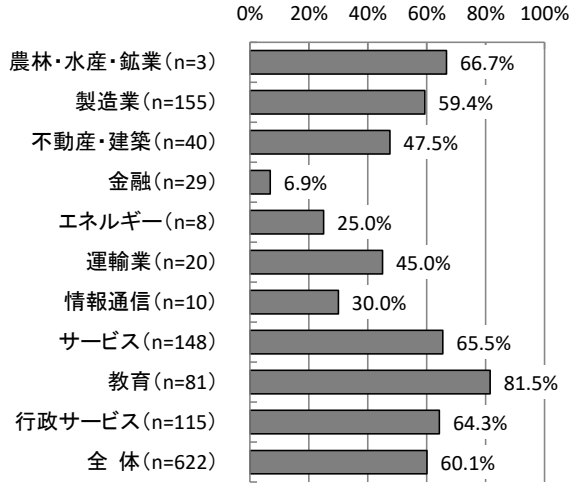
【業種別分析】業種別にみると、「定期点検のため実施」については、「金融」が82.8%となっている。一方、「実施していない」については、「教育」が81.5%で最も多く、次いで「サービス」が65.5%となっている。

【業種別分析】ぜい弱性調査（ペネトレーションテスト）実施の有無

定期点検のため実施

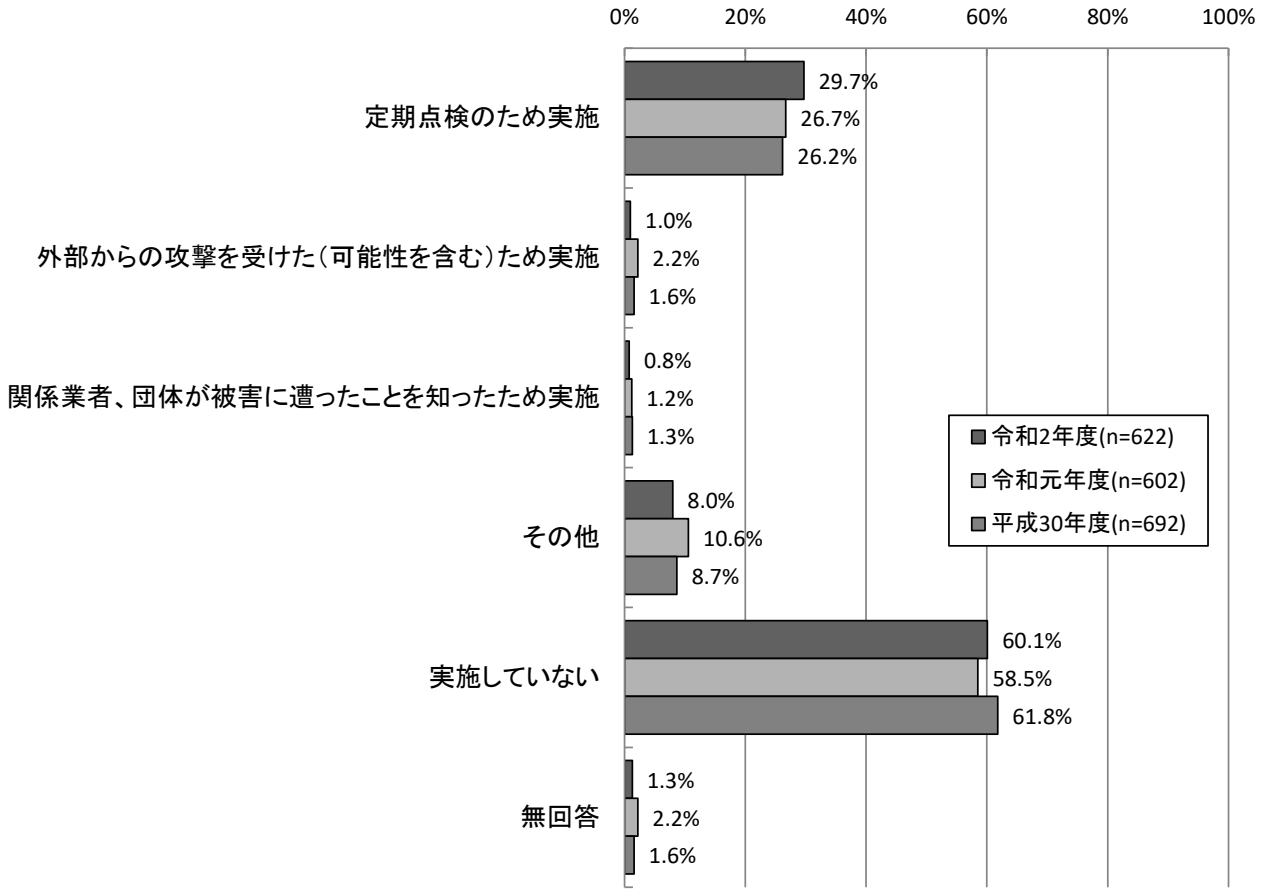


実施していない



【経年変化】昨年度と比較すると、「定期点検のための実施」が 3.0 ポイント増加している。

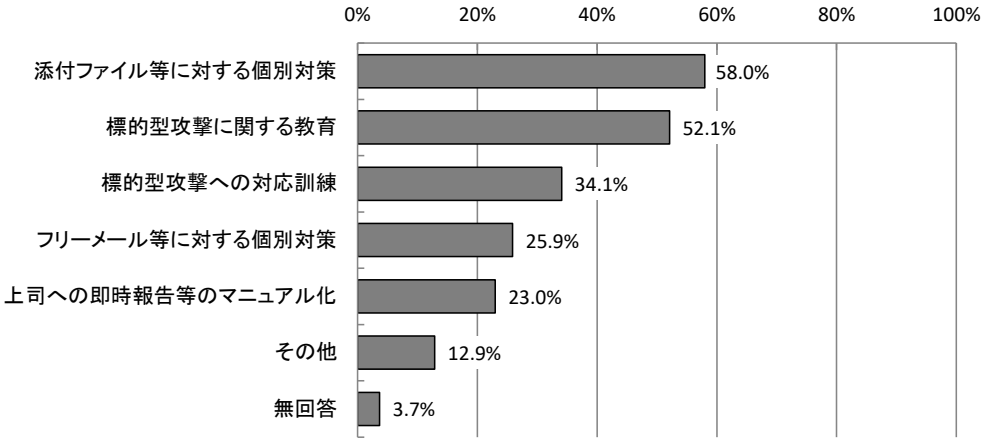
【経年変化】ぜい弱性調査（ペネトレーションテスト）実施の有無



3.1.23　標的型攻撃への対策状況　【問17】

標的型攻撃への対策状況については、「添付ファイル等に対する個別対策」が58.0%で最も多く、次いで「標的型攻撃に関する教育」が52.1%となっている。

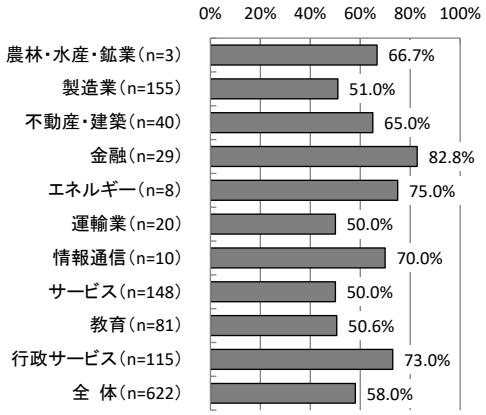
【全体】標的型攻撃への対策状況（MA, n=622）



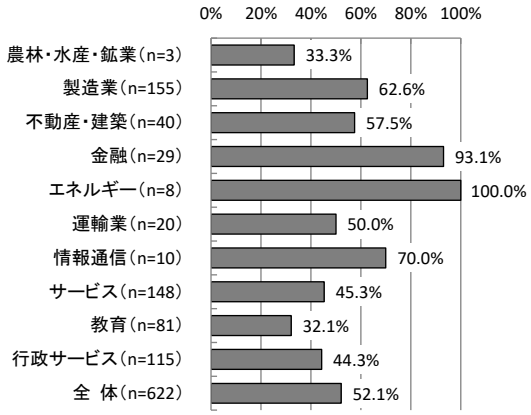
【業種別分析】業種別にみると、「添付ファイル等に対する個別対策」については、「金融」が82.8%で最も多く、次いで「エネルギー」が75.0%となっている。「標的型攻撃に関する教育」については、「エネルギー」が100.0%で最も多く、次いで「金融」が93.1%となっている。

【業種別分析】標的型攻撃への対策状況

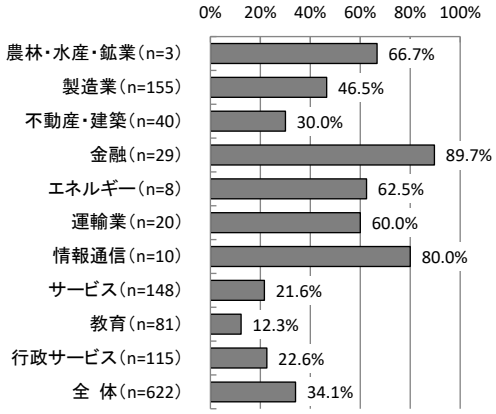
添付ファイル等に対する個別対策



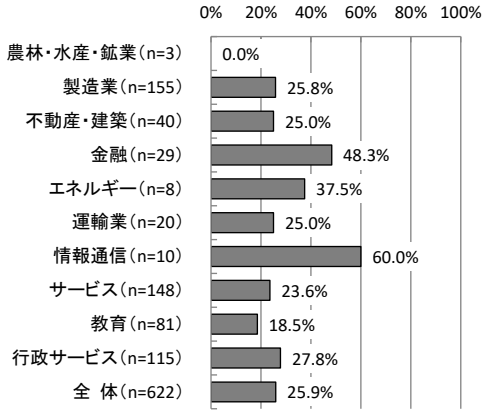
標的型攻撃に関する教育



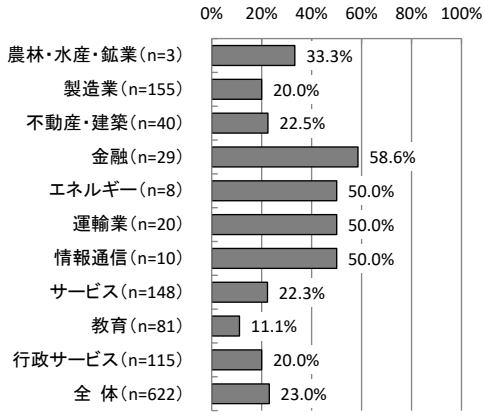
標的型攻撃への対応訓練



フリーメール等に対する個別対策



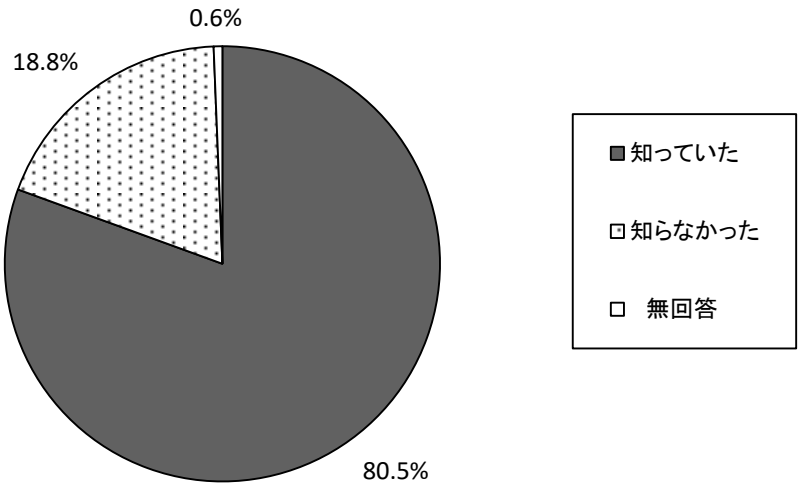
上司への即時報告等のマニュアル化



3.1.24　ビジネスメール詐欺の認知状況　【問18】

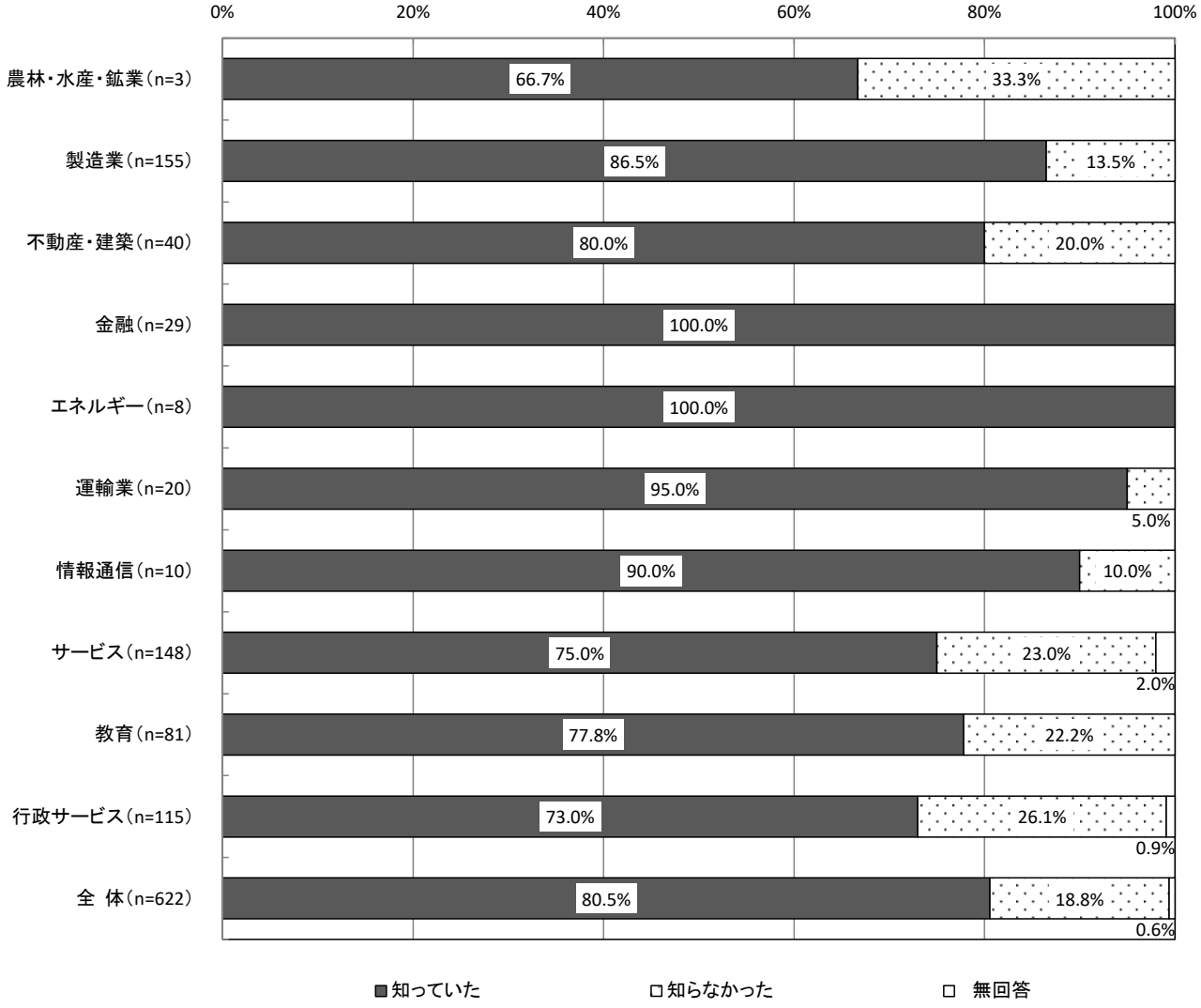
ビジネスメール詐欺の認知状況については、「知っていた」が80.5%、「知らなかった」が18.8%となっている。

【全体】ビジネスメール詐欺の認知状況（SA,n=622）



【業種別分析】業種別にみると、「知っていた」については、「金融」「エネルギー」が100.0%で最も多く、次いで「運輸業」が95.0%となっている。一方、「知らなかった」については、「行政サービス」が26.1%と最も多くなっている。

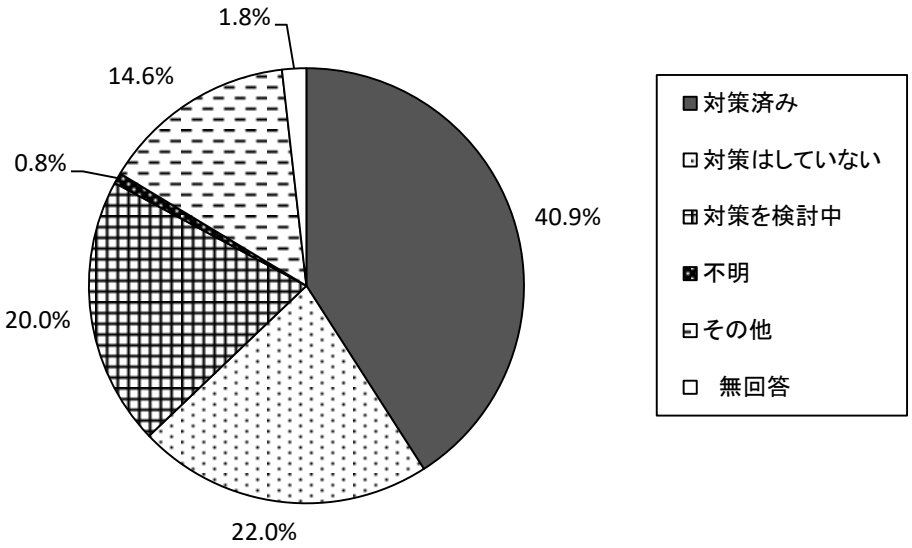
【業種別分析】ビジネスメール詐欺の認知状況



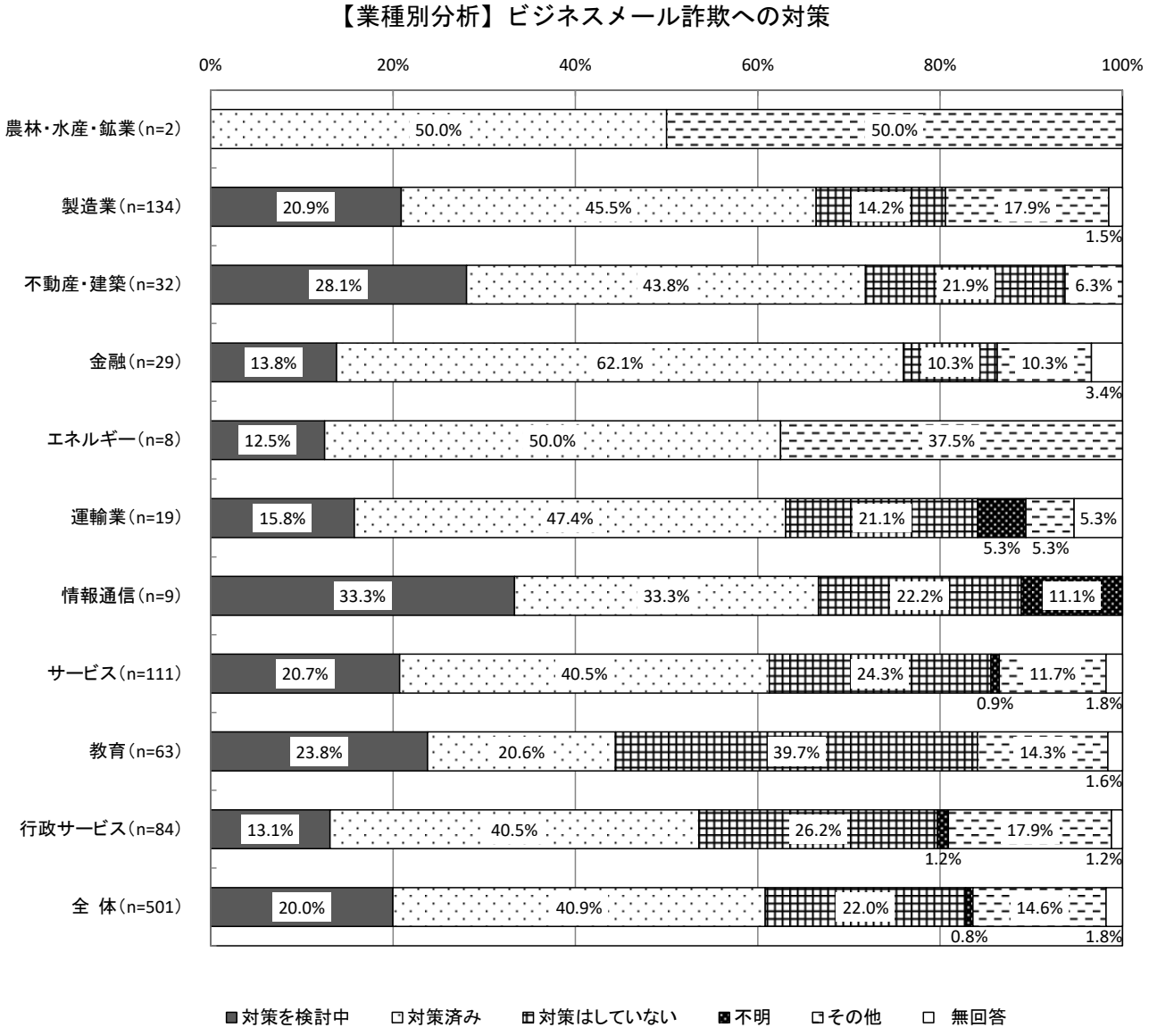
3.1.25　ビジネスメール詐欺への対策　【問19】

ビジネスメール詐欺への対策については、「対策済み」が40.9%で最も多く、次いで「対策はしていない」が22.0%、「対策を検討中」が20.0%となっている。

【全体】ビジネスメール詐欺への対策（SA,n=503）



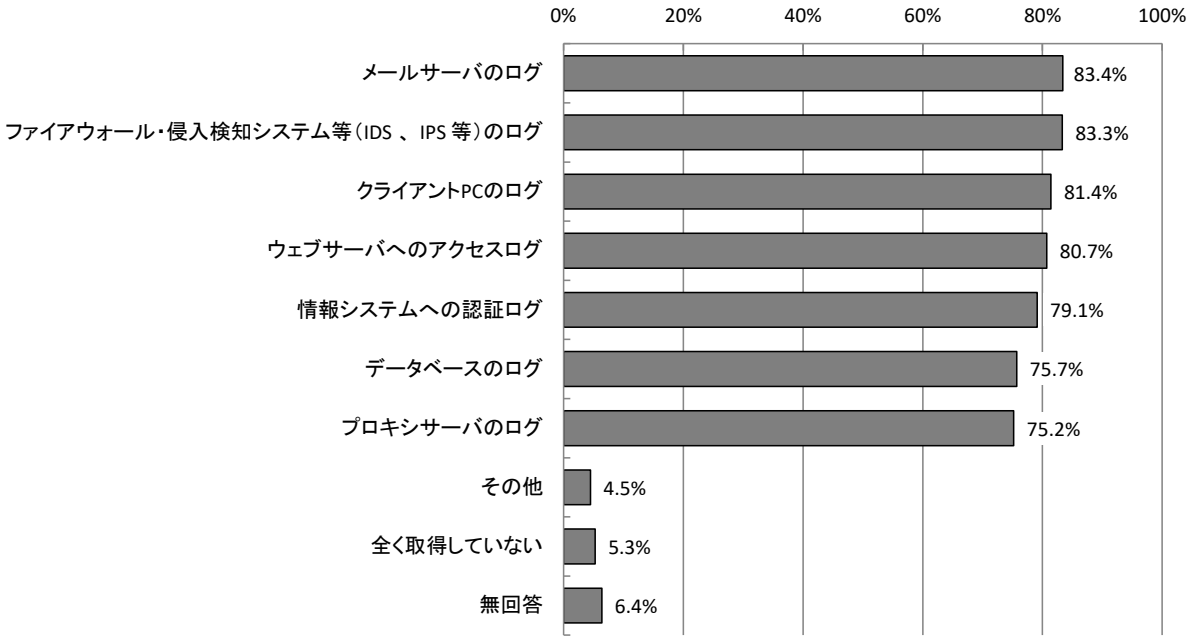
【業種別分析】業種別にみると、「対策済み」については、「金融」が62.1%と最も多く、次いで「エネルギー」が50.0%、「運輸業」が47.4%となっている。「対策はしていない」については、「教育」が39.7%と最も多くなっている。



3.1.26　アクセスログの取得状況　【問20】

ログの取得状況については、「メールサーバのログ」が83.4%で最も多く、次いで「ファイアウォール・侵入検知システム等（IDS、IPS等）のログ」が83.3%、「クライアントPCのログ」が81.4%、「ウェブサーバへのアクセスログ」が80.7%となっている。

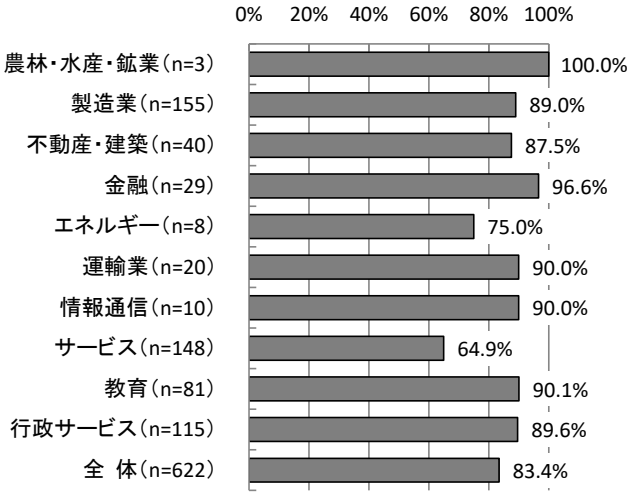
【全体】ログの取得状況（MA,n=622）



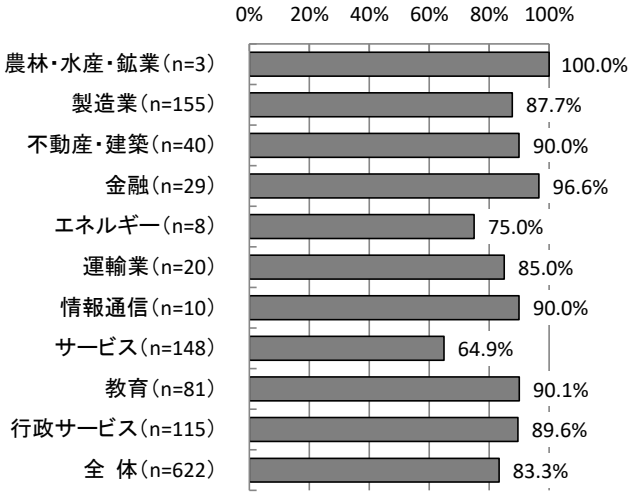
【業種別分析】業種別にみると、「メールサーバのログ」及び「ファイアウォール・侵入検知システム等（IDS、IPS等）のログ」「クライアントPCのログ」「ウェブサーバへのアクセスログ」については、「金融」がそれぞれで最も多くなっている。

【業種別分析】ログの取得状況

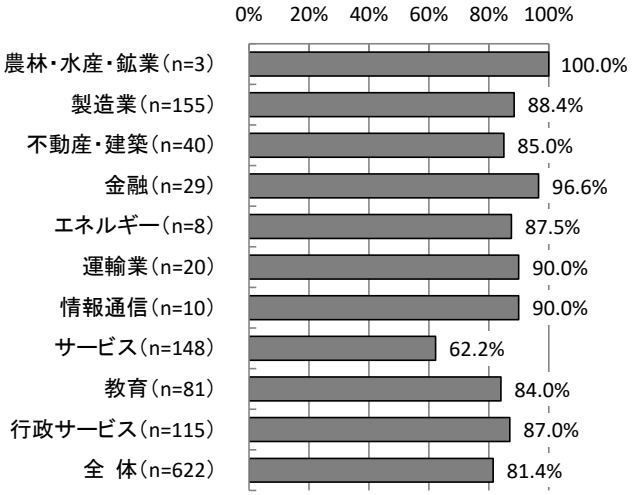
メールサーバのログ



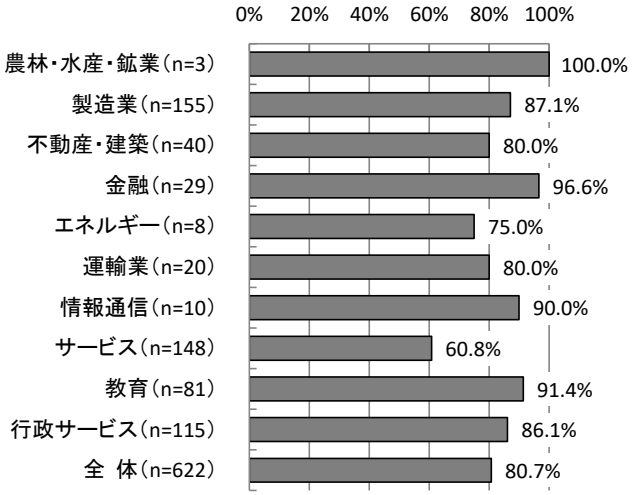
ファイアウォール・侵入検知システム等（IDS 、IPS 等）のログ



クライアントＰＣのログ

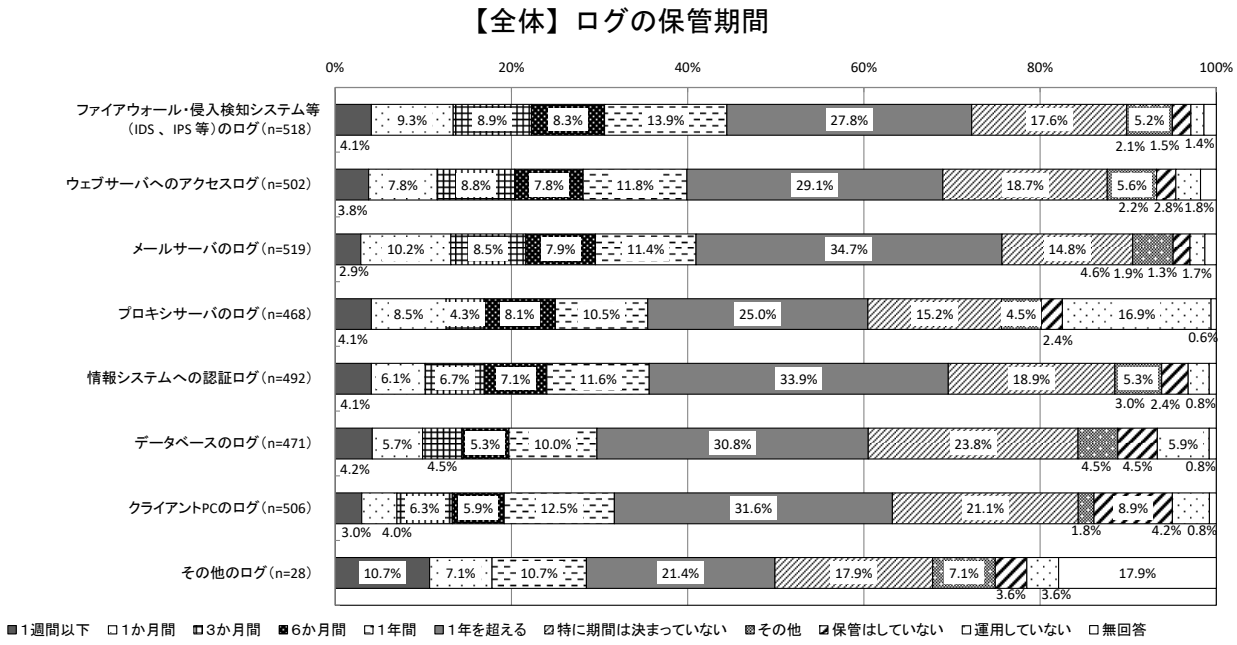


ウェブサーバへのアクセスログ



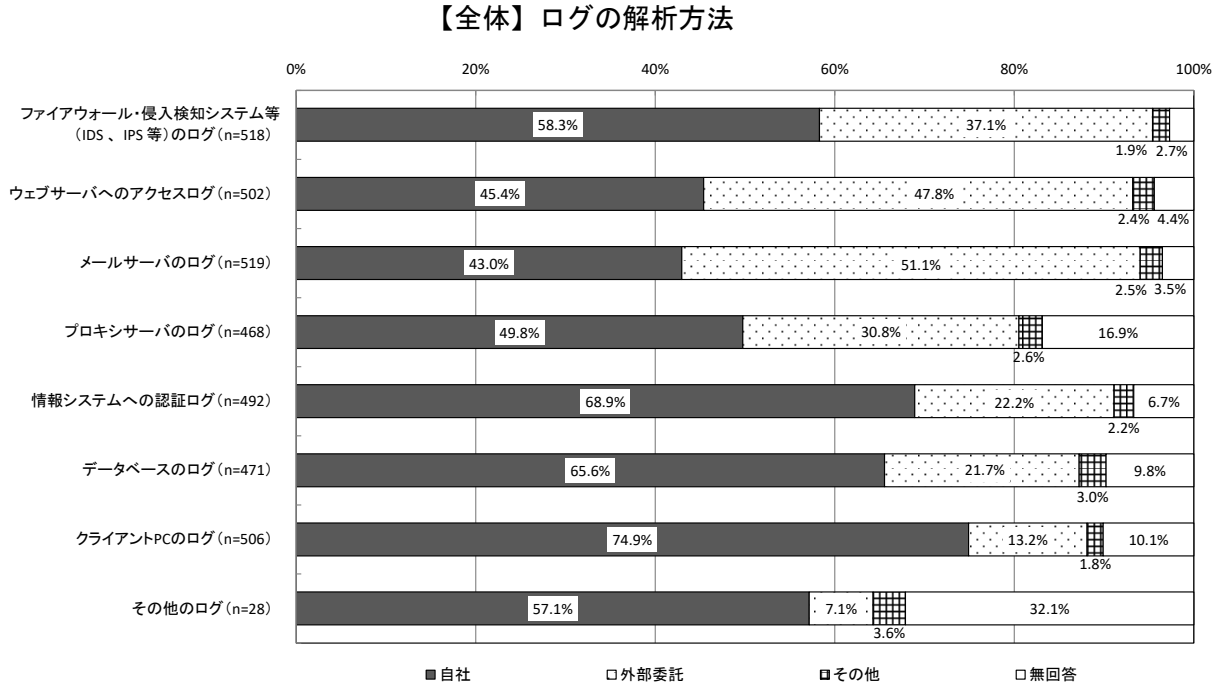
3.1.27　ログの保管期間　【問20A】

ログの保管期間については、すべてのログの種類で「１年を超える」が最も多くなっている。



3.1.28　ログの解析方法　【問20B】

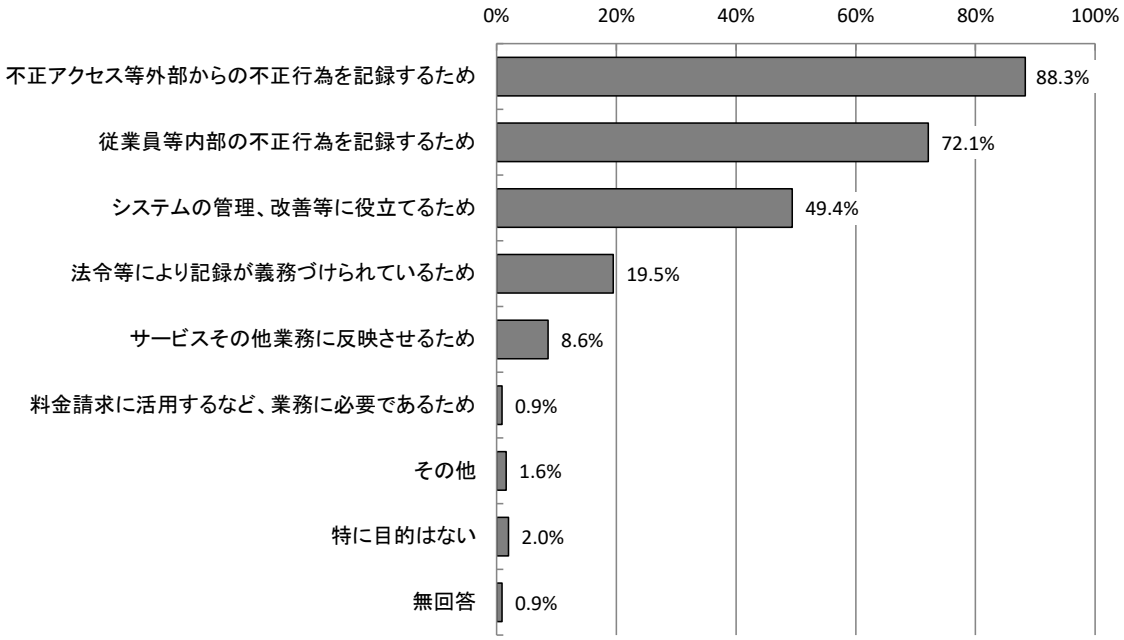
ログの解析方法については、ほとんどのログの種類で「自社」が最も多くなっているが、「ウェブサーバへのアクセスログ」「メールサーバのログ」では「外部委託」が最も多くなっている。



3.1.29　ログを取得・保管している理由　【問21】

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88.3%で最も多く、次いで「従業員等内部の不正行為を記録するため」が72.1%、「システムの管理、改善等に役立てるため」が49.4%となっている。

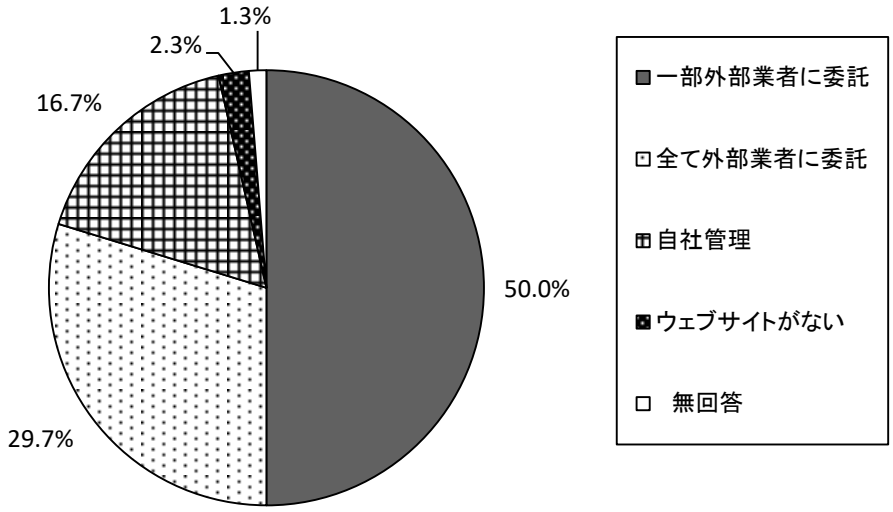
【全体】ログを取得・保管している理由（MA,n=549）



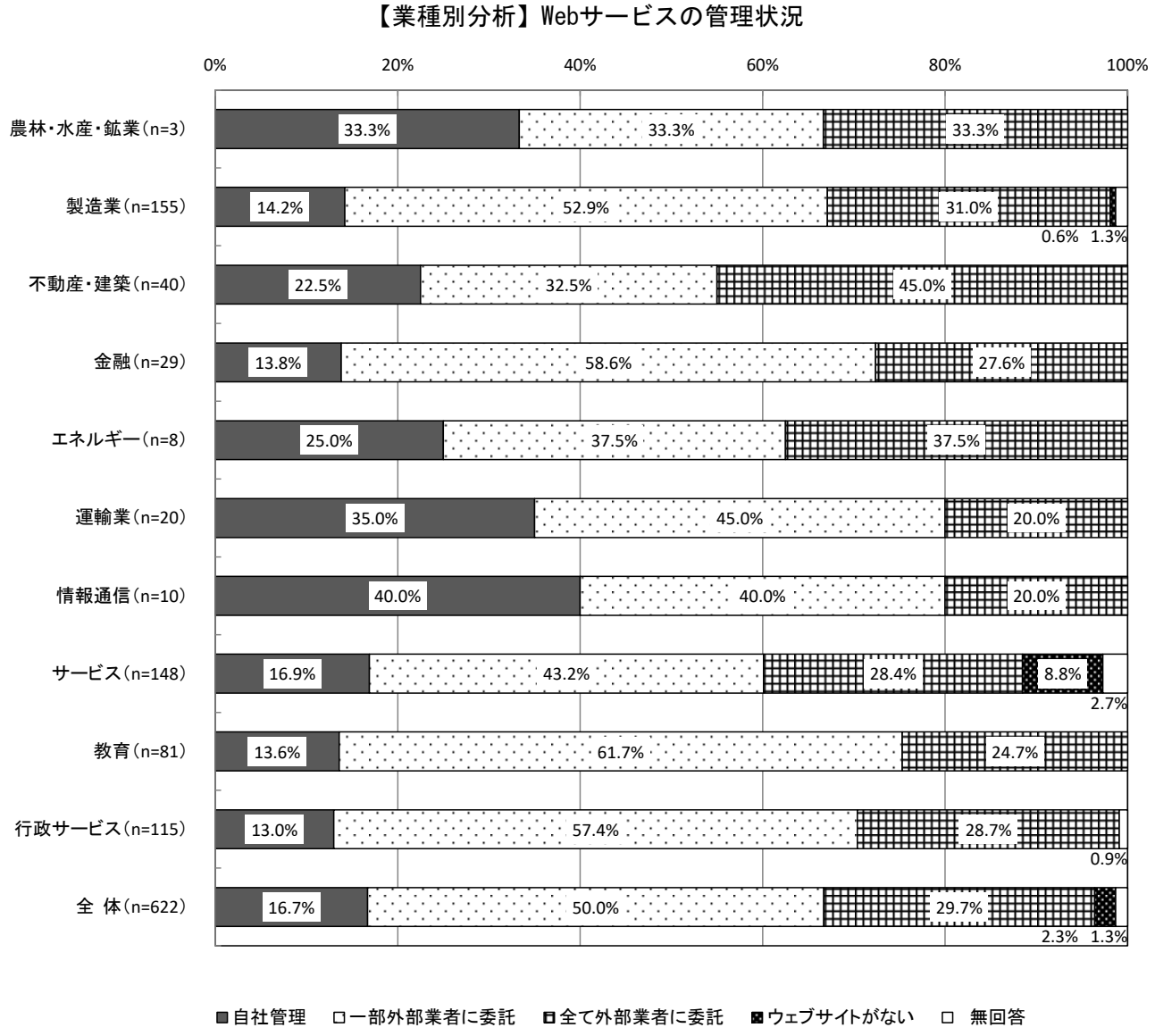
3.1.30　Webサービスの管理環境【問22】

Webサービス（サイト、メール等）の管理状況については、「一部外部業者に委託」が50.0%で最も多く、次いで「全て外部業者に委託」が29.7%、「自社管理」が16.7%となっている。

【全体】Webサービスの管理状況（SA,n=622）



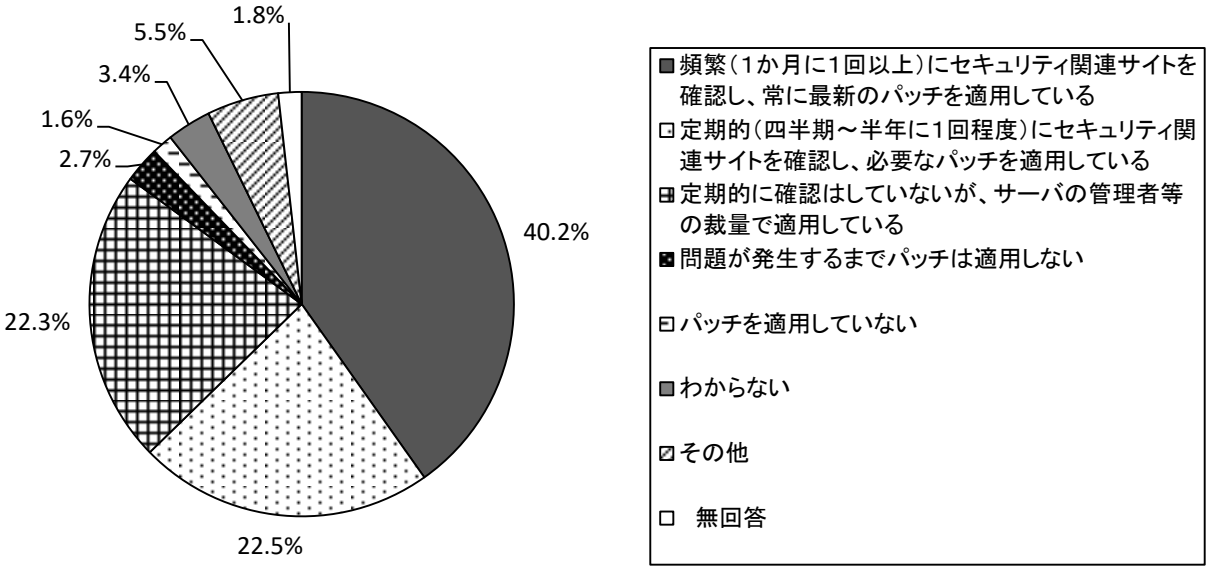
【業種別分析】業種別にみると、「不動産・建築」では「全て外部業者に委託」が最も多く、「エネルギー」では「一部外部業者に委託」「全て外部業者に委託」がそれぞれ37.5%で同率、それ以外の業種では「一部外部業者に委託」が最も多くなっている。



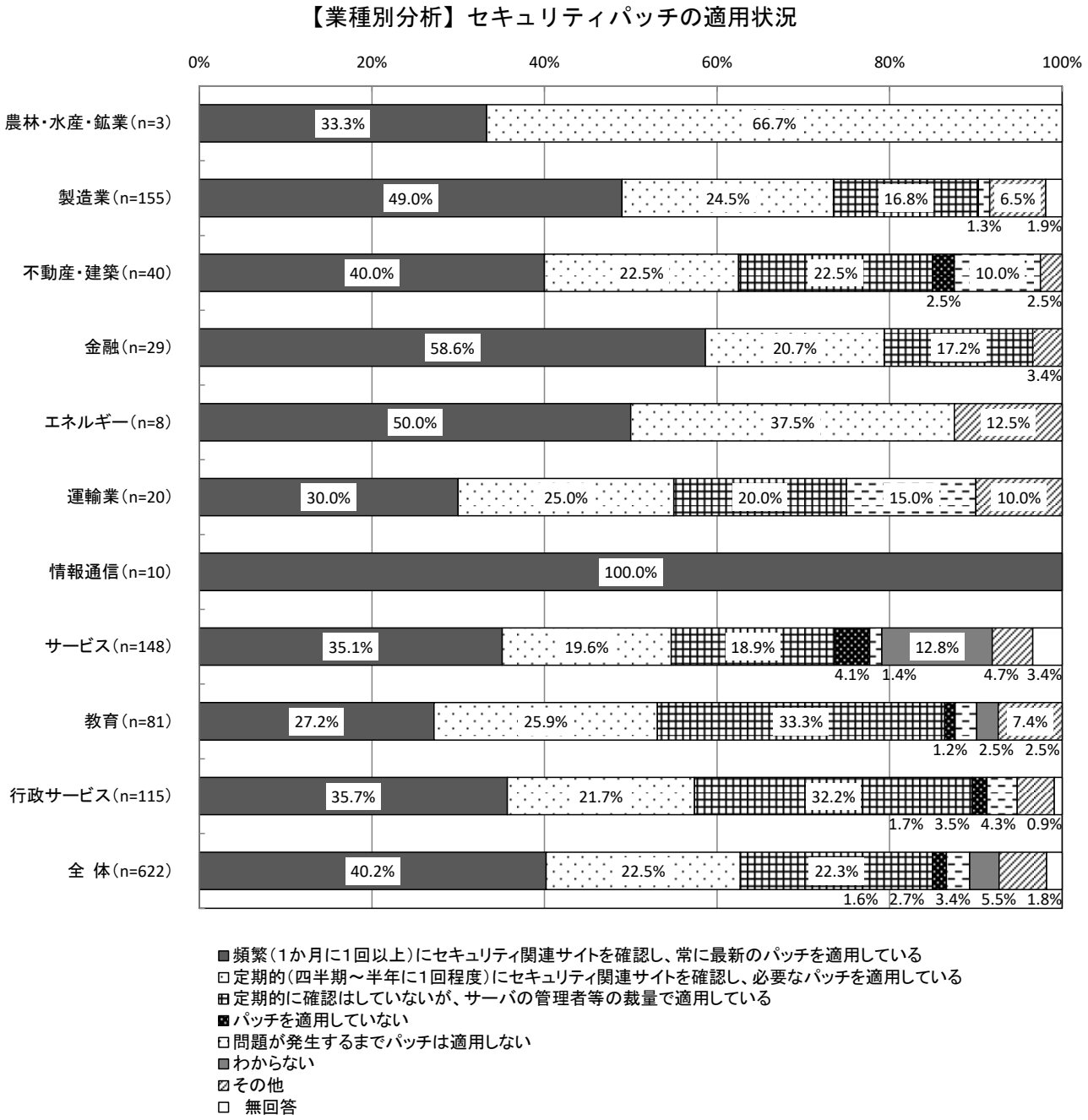
3.1.31　セキュリティパッチの適用状況　【問23】

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40.2%で最も多く、次いで「定期的（四半期～半年に１回程度）にセキュリティ関連サイトを確認し、必要なパッチを適用している」が22.5%、「定期的に確認はしていないが、サーバの管理者等の裁量で適用している」が22.3%となっている。

【全体】セキュリティパッチの適用状況（SA,n=622）

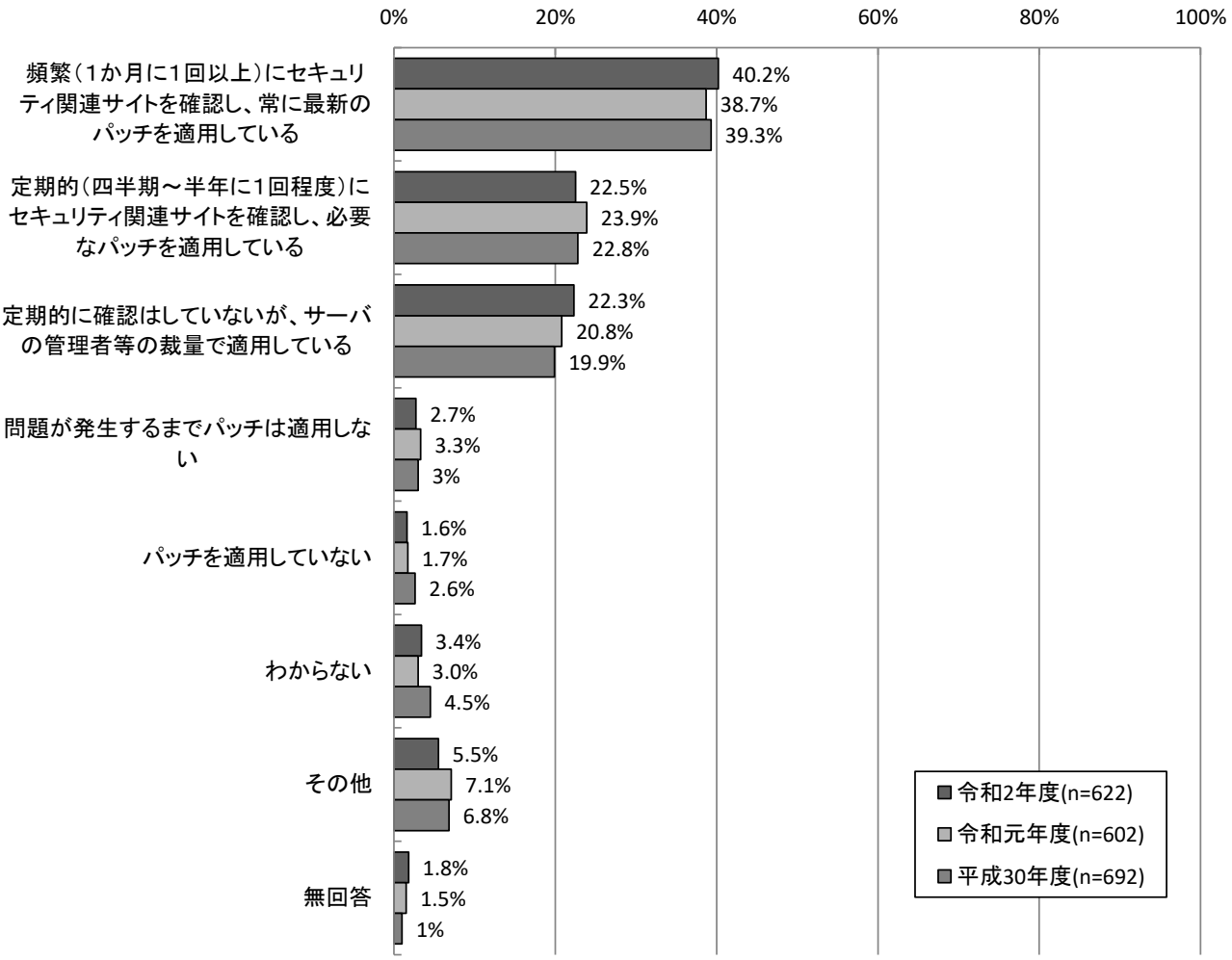


【業種別分析】業種別にみると、「頻繁（１か月に１回以上）にセキュリティ関連サイトを確認し、常に最新のパッチを適用している」については、「情報通信」が100.0%と最も多く、次いで「金融」が58.6%となっている。



【経年変化】昨年度と比較すると、「頻繁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」「定期的に確認はしていないが、サーバの管理者等の裁量で適用している」がそれぞれ1.5ポイント増加している。

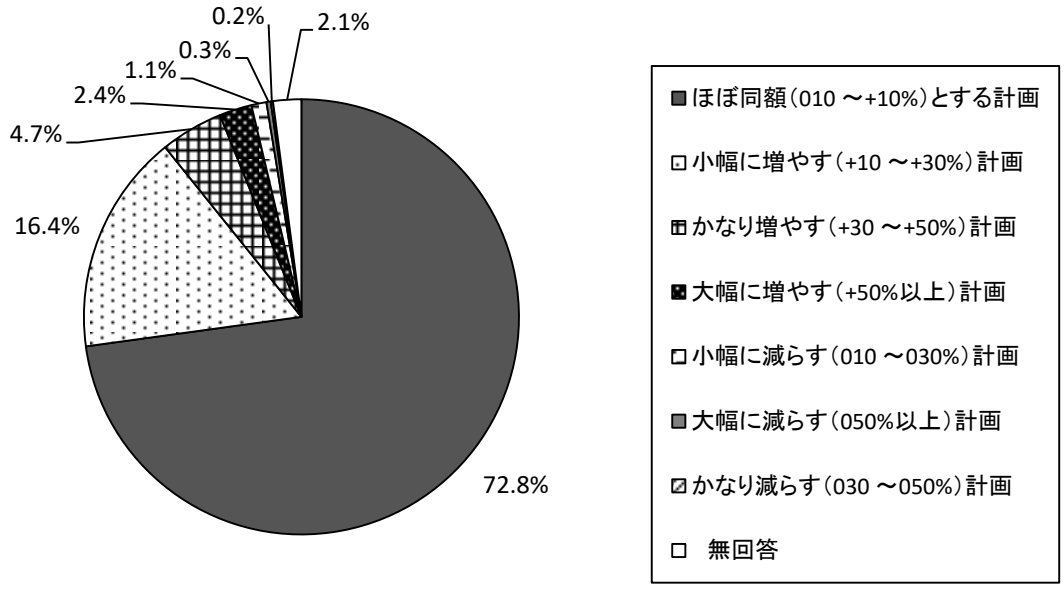
【経年変化】セキュリティパッチの適用状況



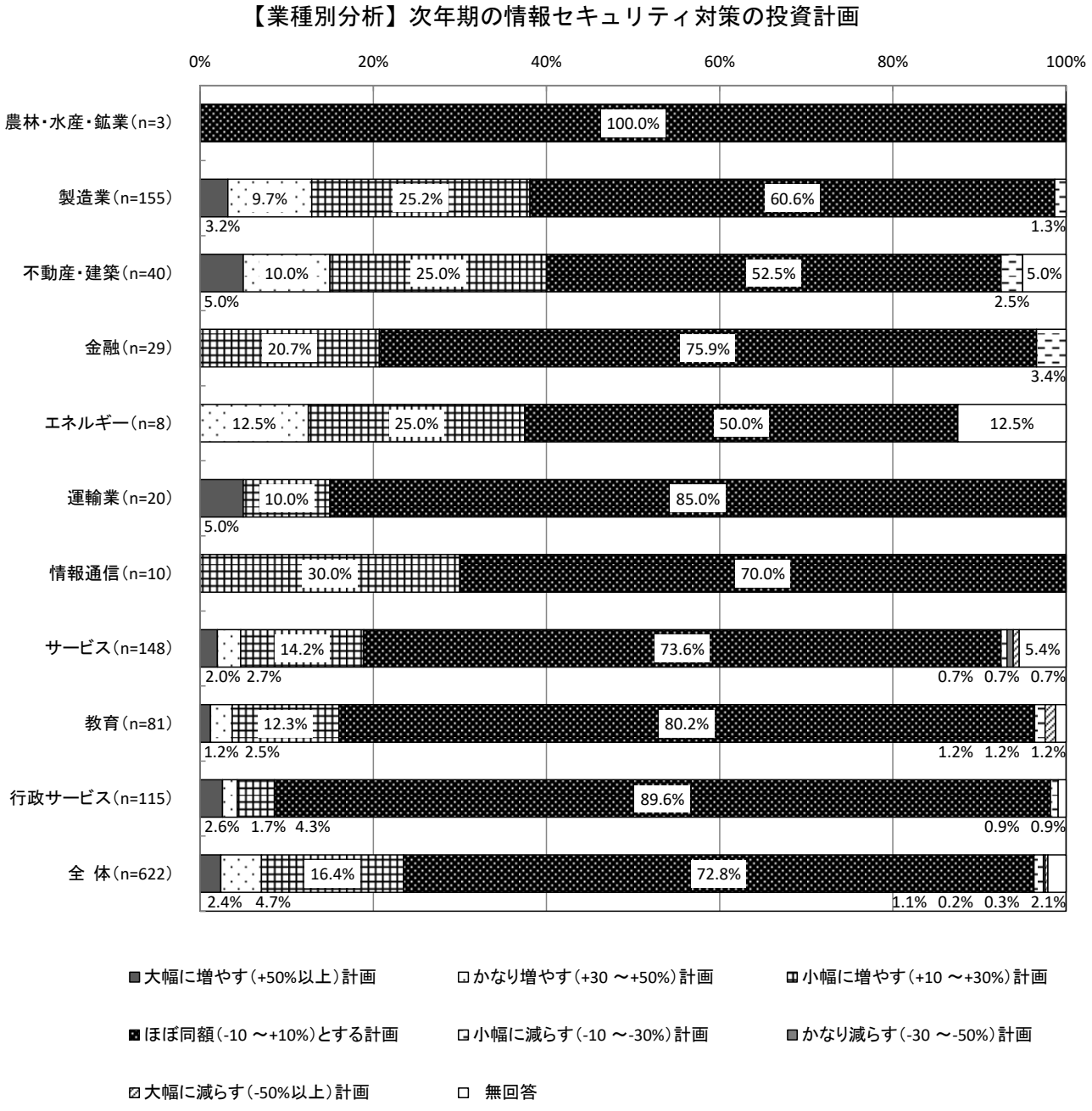
3.1.32　次年期の情報セキュリティ対策の投資計画　【問24】

次年期（年単位）の情報セキュリティ対策の投資計画については、「ほぼ同額（010～+10%）とする計画」が72.8%で最も多く、次いで「小幅に増やす（+10～+30%）計画」が16.4%、「かなり増やす（+30～+50%）計画」が4.7%となっている。

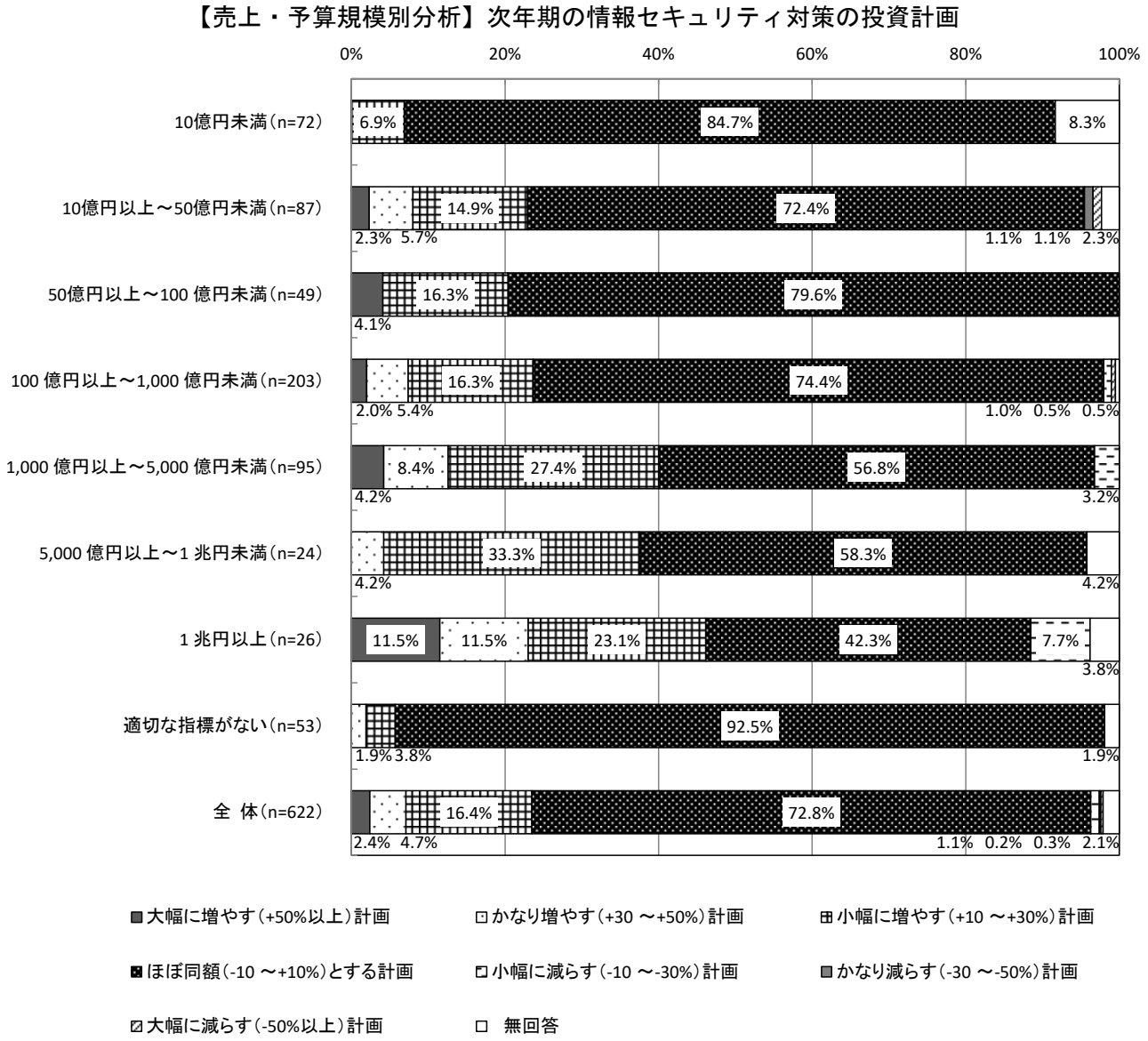
【全体】次年期の情報セキュリティ対策の投資計画（SA,n=622）



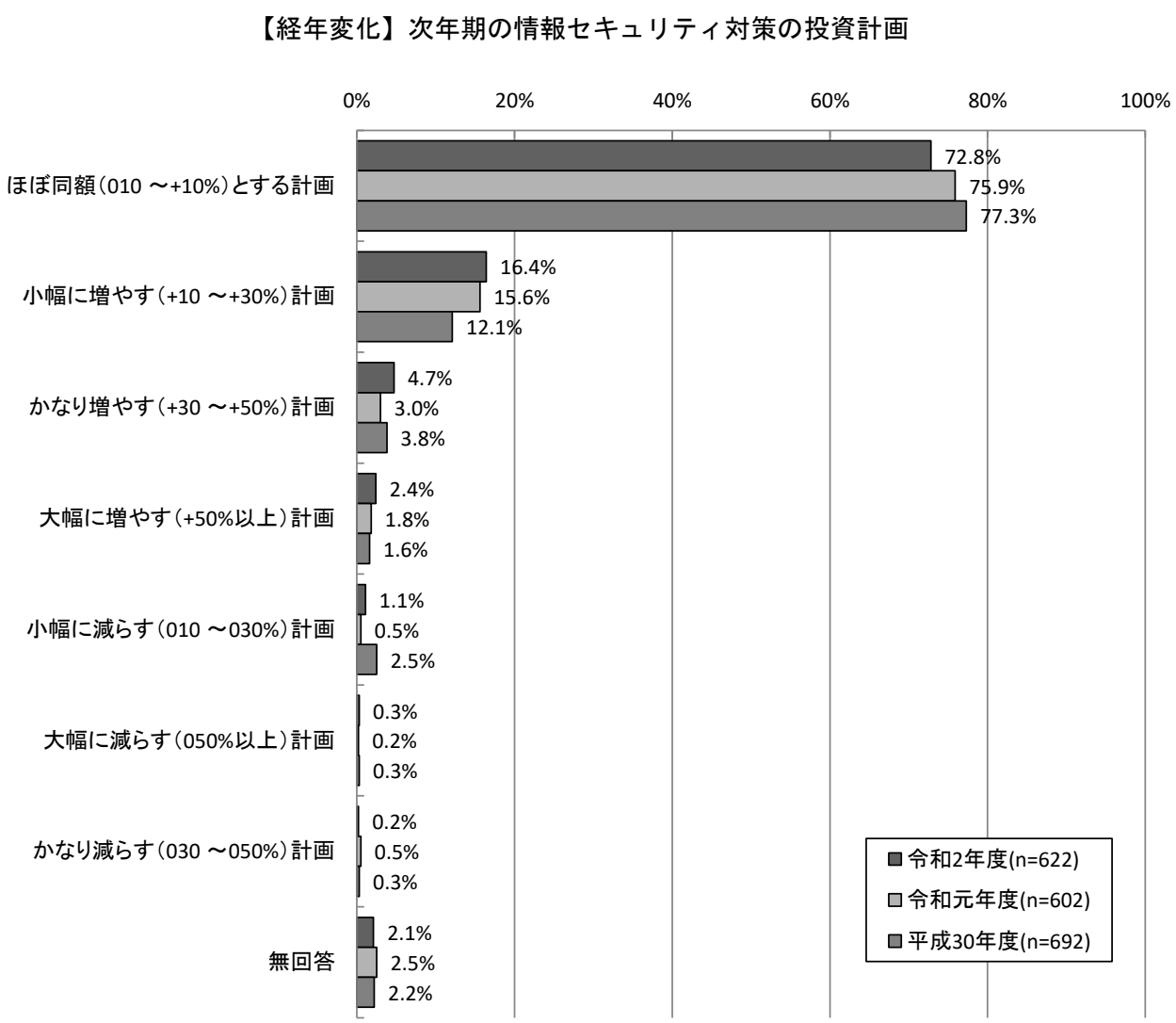
【業種別分析】業種別にみると、今期と比較して投資額を「増やす計画」については、「不動産・建築」が合計40.0%で最も多く、次いで「製造業」が38.1%、「エネルギー」が37.5%となっている。今期と比較して、「ほぼ同額とする計画」については、「行政サービス」が89.6%で最も多く、次いで「運輸業」が85.0%、「教育」が80.2%で続いている。



【売上・予算規模別分析】売上・予算規模別にみると、今期と比較して投資額を「増やす計画」については、「1兆円以上」が46.1%で最も多く、次いで「1000億円以上～5,000億円未満」が40.0%、「5,000億円以上～1兆円未満」が37.5%となっている。今期と比較して、「ほぼ同額とする計画」は、「適切な指標がない」が92.5%で最も多くなっている。



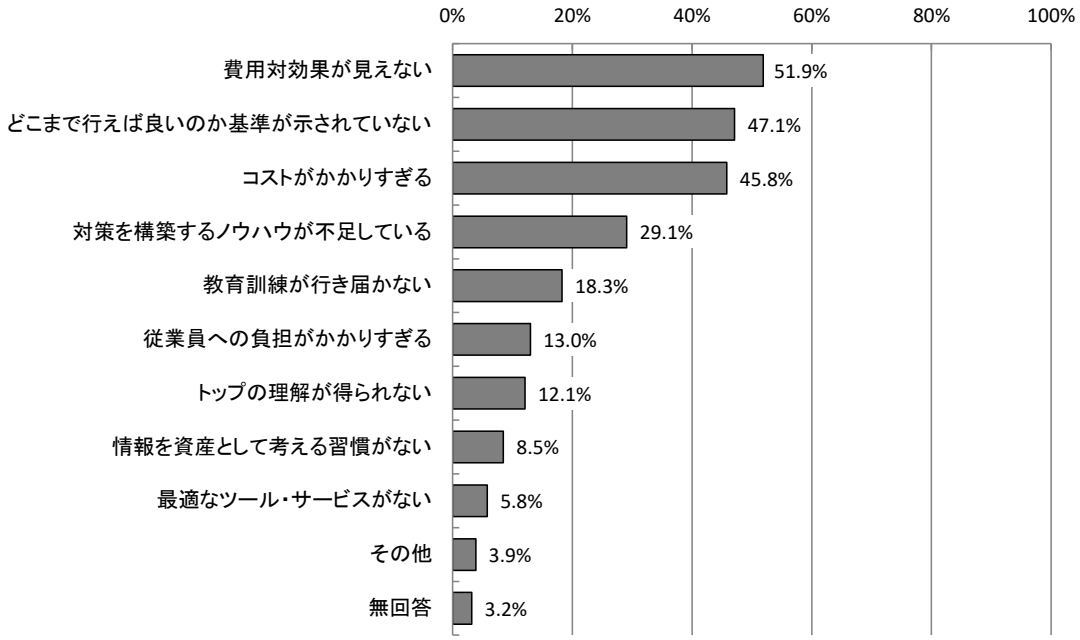
【経年変化】昨年度と比較すると、「ほぼ同額とする計画」が 3.1 ポイント減少している。



3.1.33　情報セキュリティ対策への投資に関する問題点　【問25】

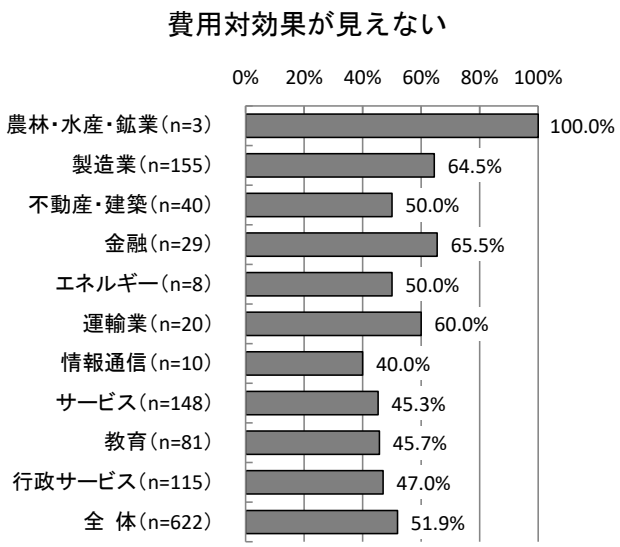
情報セキュリティ対策への投資に関する問題点については、「費用対効果が見えない」が51.9%で最も多く、次いで「どこまで行えば良いのか基準が示されていない」が47.1%、「コストがかかりすぎる」が45.8%となっている。

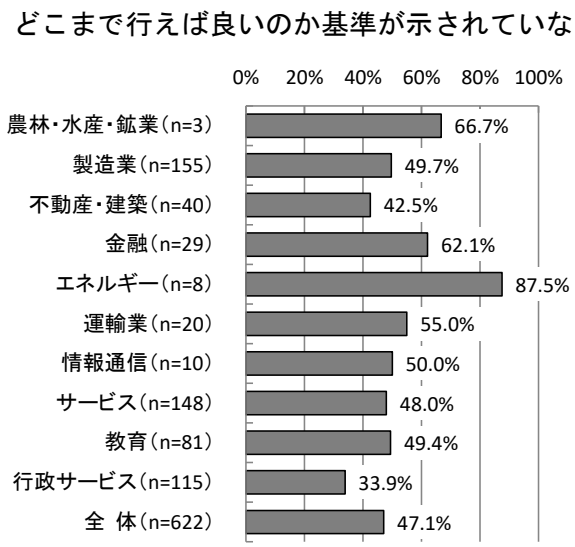
【全体】情報セキュリティ対策への投資に関する問題点（MA,n=622）

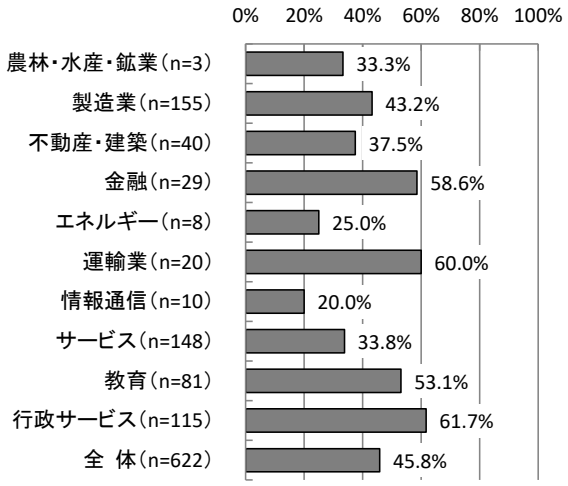


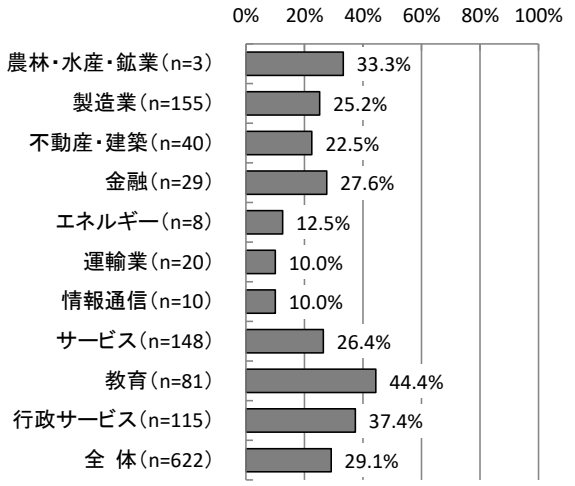
【業種別分析】業種別にみると、「費用対効果が見えない」については、「金融」が65.5%で最も多くなっている。「どこまで行えば良いのか基準が示されていない」については、「エネルギー」が87.5%、「コストがかかりすぎる」については、「行政サービス」が61.7%で最も多くなっている。

【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





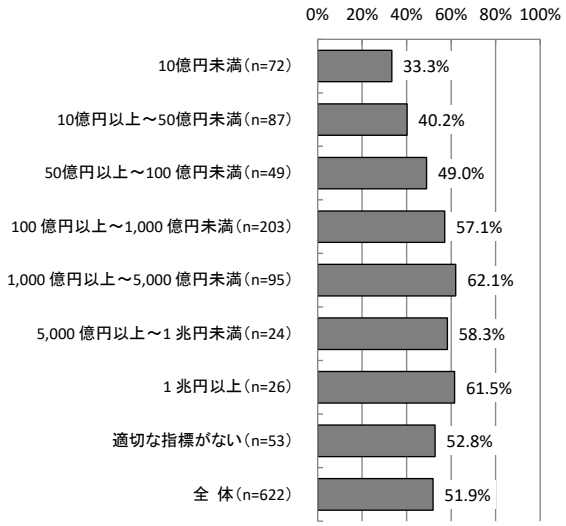




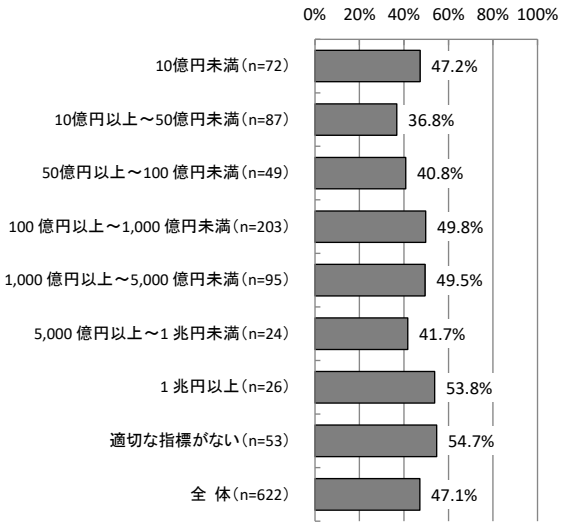
【売上・予算規模別分析】売上・予算規模別にみると、「費用対効果が見えない」については、「1,000億円以上～5,000億円未満」が62.1％で最も多く、次いで「1兆円以上」が61.5％となっている。「どこまで行えば良いのか基準が示されていない」については、「適切な指標がない」が54.7％で最も多く、次いで「1兆円以上」が53.8％となっている。「コストがかかりすぎる」については、「50億円以上～100億円未満」が59.2％で最も多く、次いで「5,000億円以上～1兆円未満」が50.0％となっている。

【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

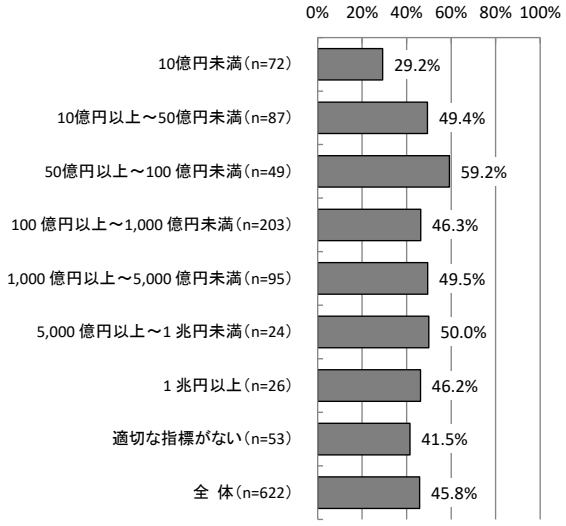
費用対効果が見えない



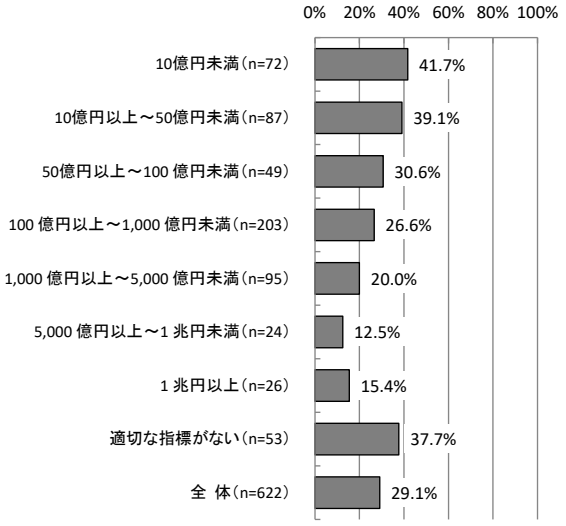
どこまで行えば良いのか基準が示されていない



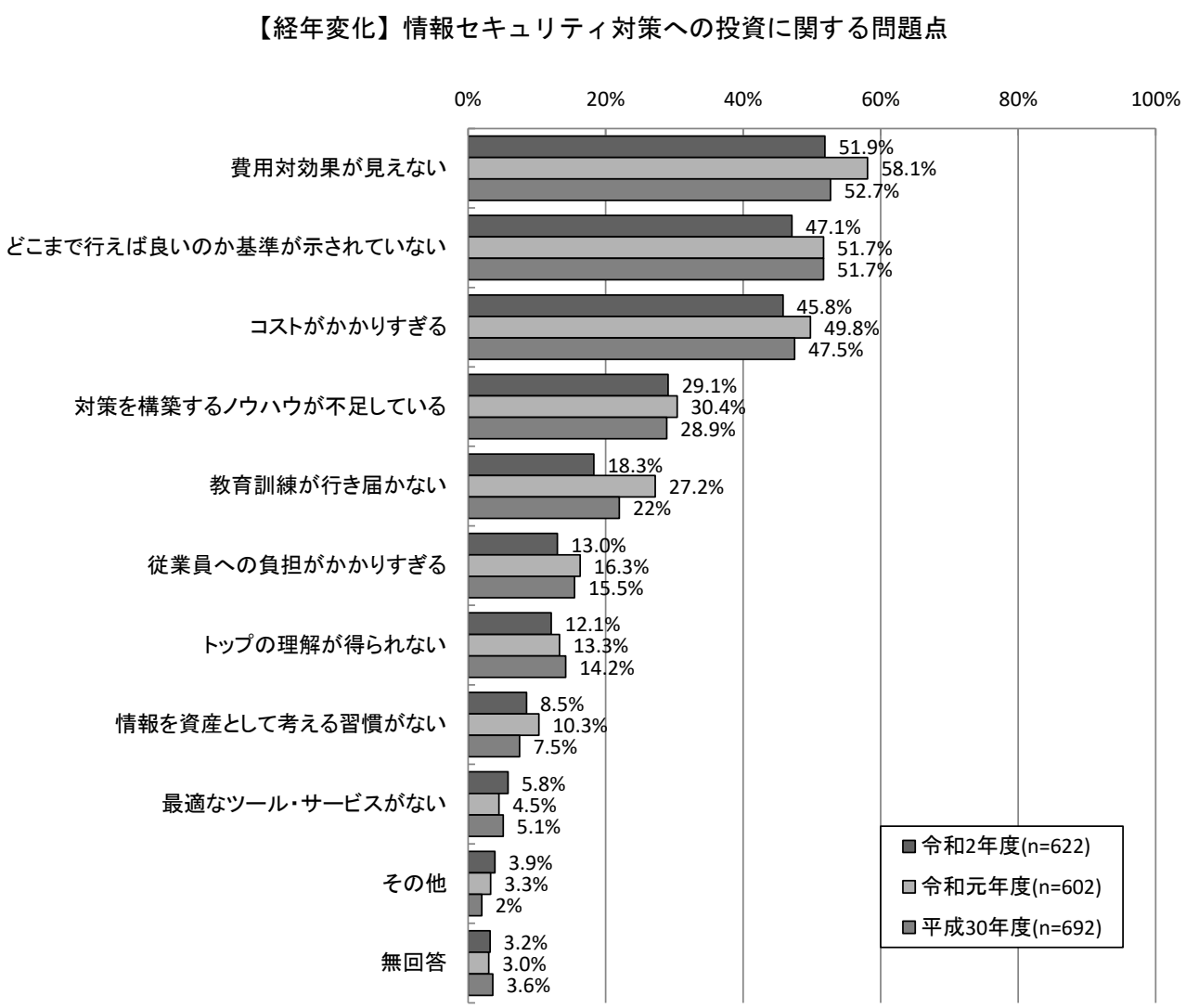
コストがかかりすぎる



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、「最適なツール・サービスがない」を除いて減少している。



3.1.34 情報セキュリティ対策に関する考え方 【問26】

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

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

調査対象とした基本的な考え方と相対する2つの考え

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

【全体】「投資方針」については、「①セキュリティ投資は必要最低限度に抑えるべきである」に近いとする割合が26.8%、「②来るべき問題事案に備えて、積極的に投資を行うべきである」に近いとする割合が71.1%となっており、「積極的」とする割合が「必要最低限」とする割合を44.3ポイント上回っている。

「事後的対応と予防的対応」については、「①情報セキュリティ対策としては、問題発生に対しての応急対応や、再発防止・被害拡大防止に注力するべきである」に近いとする割合が26.2%、「②情報セキュリティ対策としては、リスクの検知など、予防上の対策に注力するべきである」に近いとする割合が71.9%となっており、「予防的対応」とする割合が「問題発生への適切な対応」とする割合を45.7ポイントと大幅に上回っている。

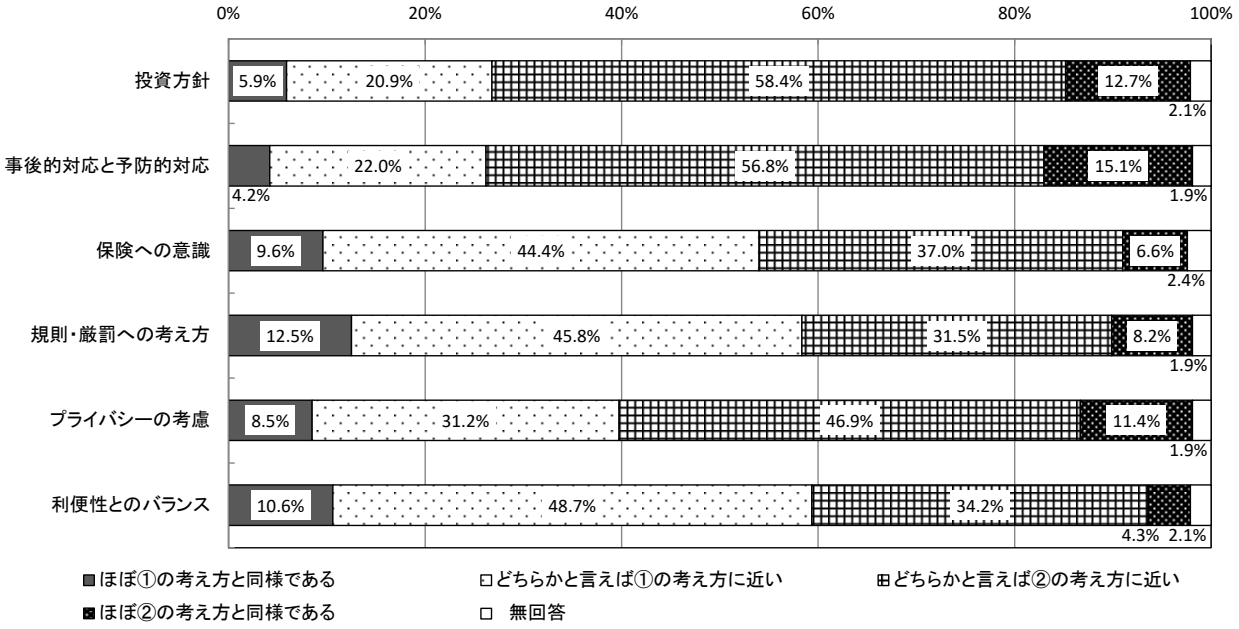
「保険への意識」については、「①情報セキュリティ対策としては、人的・技術的な対策によりカバーできるところを対策すれば十分である」に近いとする割合が54.0%、「②情報セキュリティ対策としては、人的・技術的対策によりカバーできないリスクは保険によりまかなうべきである」に近いとする割合が43.6%となっており、「人的・技術的な対策で十分」とする割合が「保険的対応が必要」を10.4ポイント上回っている。

「規制・罰則への考え方」については、「①技術以外の面での対策としては、従業員等への教育と、適切な情報提供により対策を促すことが重要である」に近いとする割合が58.3%、「②技術以外の面での対策としては、教育はもちろんのこと、規制・罰則などの強制力のある制度的対応を行うことが重要である」に近いとする割合が39.7%となっており、「教育と情報提供を中心とした対応」とする割合が「規則・罰則も含む強制力のある対応」を18.6ポイント上回っている。

「プライバシーの考慮」については、「①職場とはいえ、従業員等のプライバシーはある程度考慮したうえで、情報セキュリティ対策は行われるべきである」に近いとする割合が39.7%、「②職場のセキュリティ保護のためにはシステム利用状況のモニタリングなどによるプライバシーの侵害はやむをえない」に近いとする割合が58.3%となっており、「ある程度のプライバシーの侵害はやむをえない」とする割合が「プライバシーはある程度考慮されるべきだ」とする割合を18.6ポイント上回っている。

「利便性とのバランス」については、「①業務実施に負担をかけるほどのセキュリティ対策は不適当であり、利便性とのバランスを考慮すべきである」に近いとする割合が59.3%、「②ユーザーにシステム利用上・業務上の負担を強いてでもセキュリティを守るべきである」とする38.5%となっており、「利便性とのバランスを考慮」とする割合が「負担を強いてでもセキュリティを守る」とする割合を20.8ポイント上回っている。

【全体】情報セキュリティ対策に関する考え方（SA,n=622）

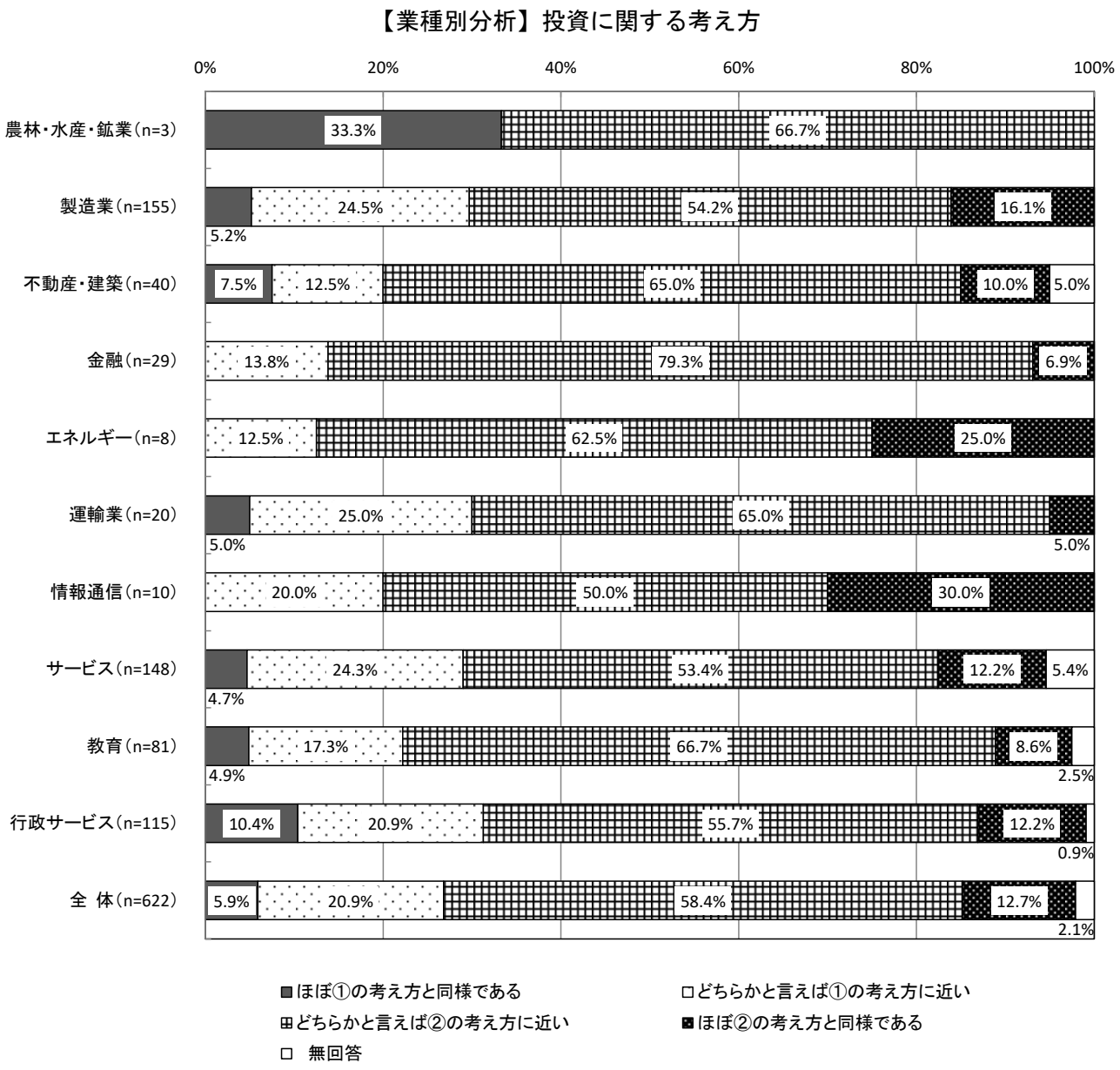


3.1.35　投資に関する考え方　【問26-1】

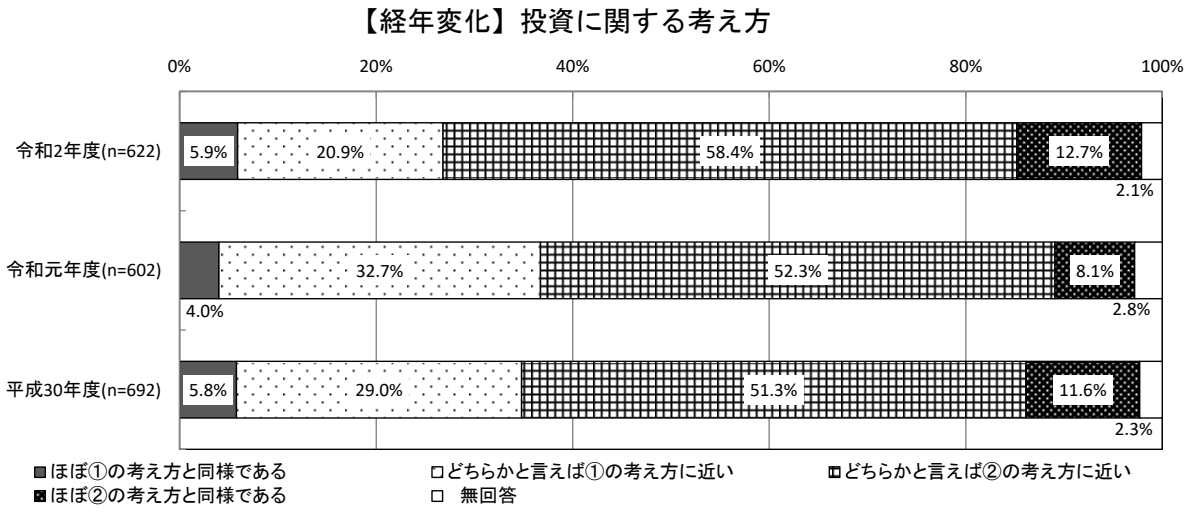
情報セキュリティに対する投資方針については、下記に挙げる2つの考え方のいずれに近いかを尋ねている。

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

【業種別分析】業種別にみると、投資方針に関して全ての業種で、「②積極的投資」の割合が多く、特に「エネルギー」が87.5%、「金融」が86.2%、「情報通信」が80.0%で8割以上となっている。



【経年変化】昨年度と比較すると、「①必要最低限」は9.9ポイントの減少、「②積極的投資」は10.7ポイントの増加となっている。

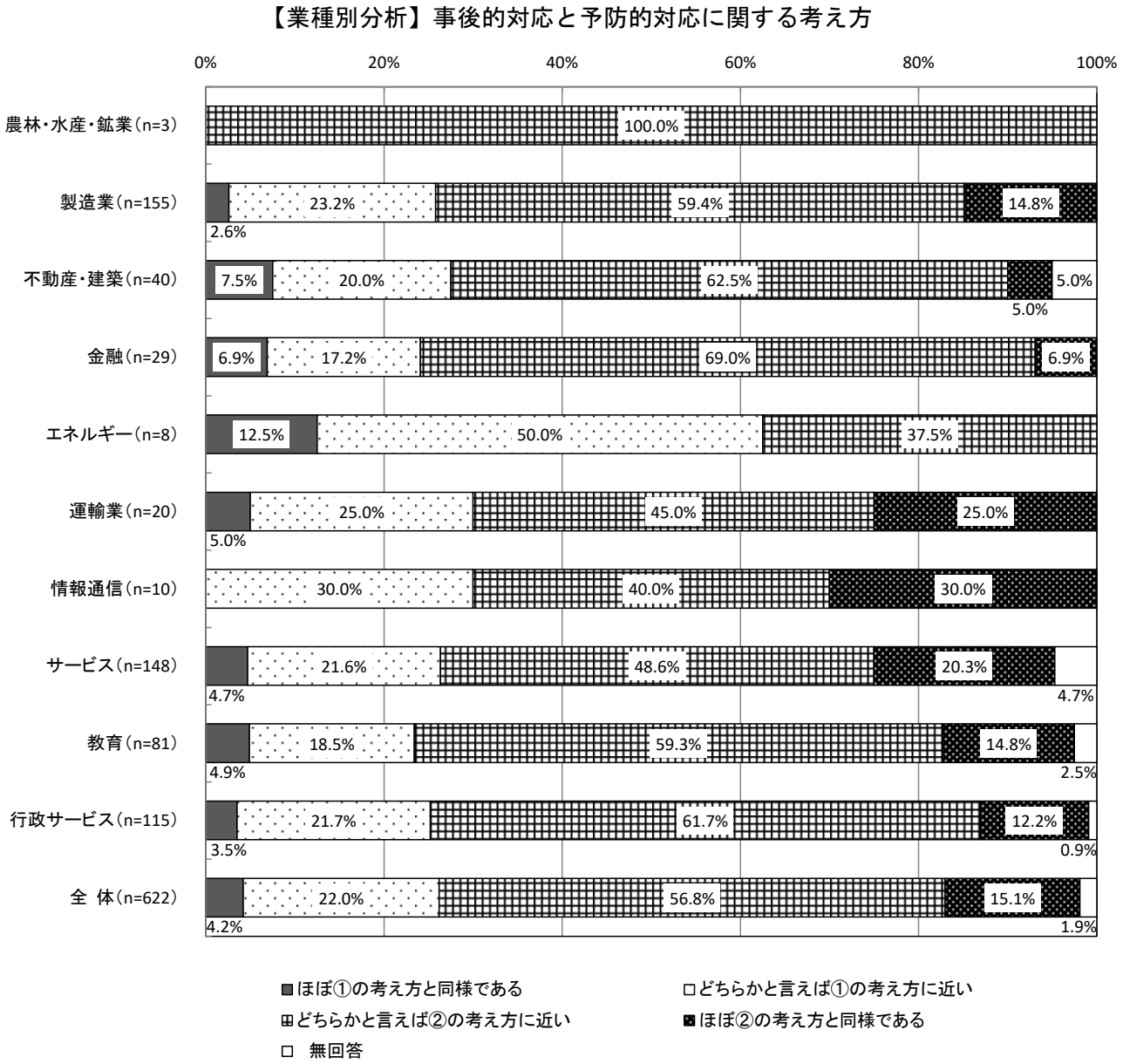


3.1.36　事後的対応と予防的対応に関する考え方　【問26-2】

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

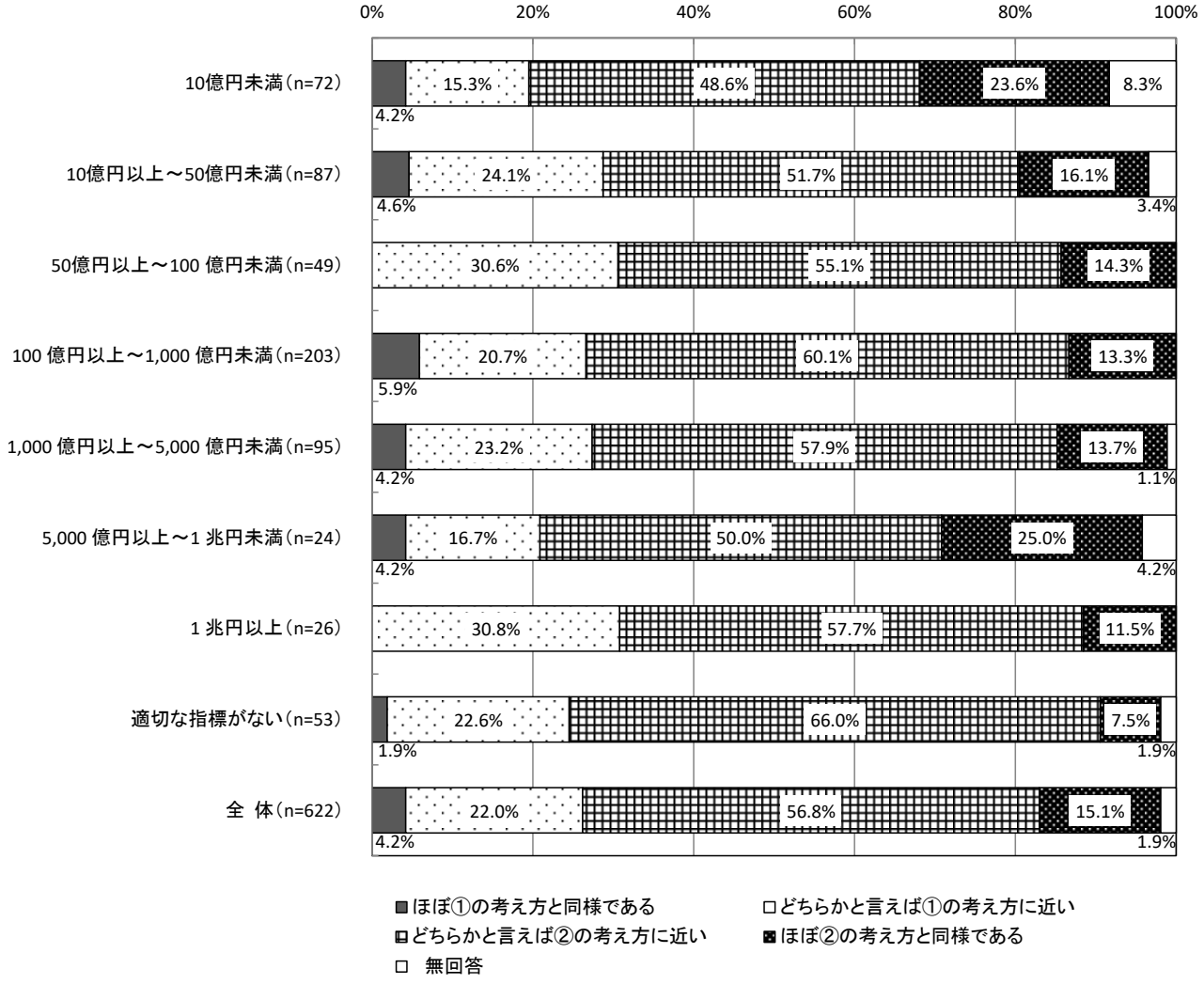
①として提示した考え方	②として提示した考え方
情報セキュリティ対策としては、問題発生に対しての応急対応や、再発防止・被害拡大防止に注力するべきである。	情報セキュリティ対策としては、リスクの検知など、予防上の対策に注力するべきである。

【業種別分析】業種別にみると、「エネルギー」を除く全ての業種で「②予防的対応」が「①事後的対応」と比べて多くなっている。特に「金融」で51.8ポイント、「教育」で50.7ポイント「②予防的対応」が多くなっている。

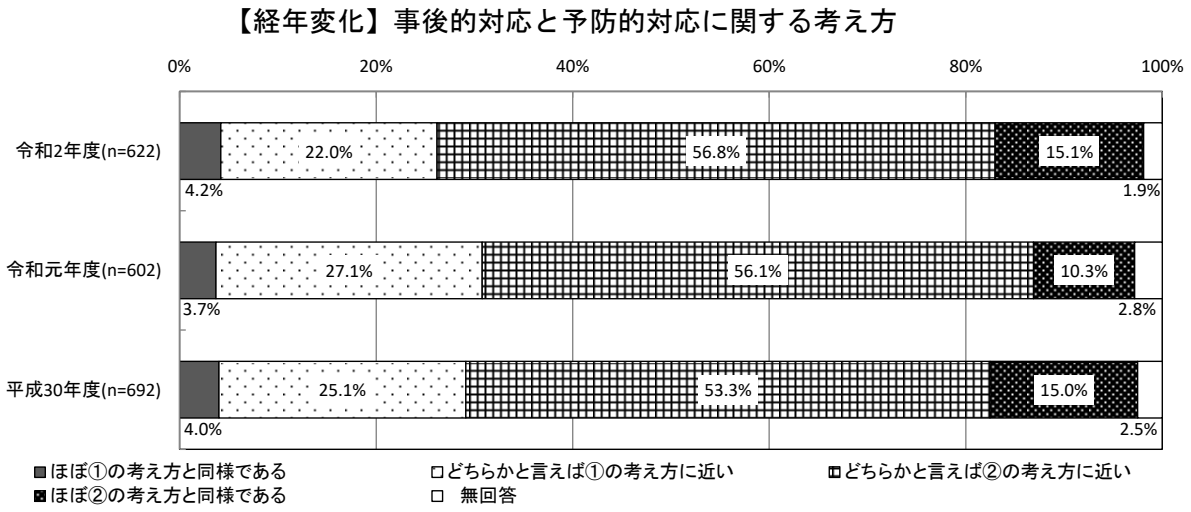


【売上・予算規模別分析】売上・予算規模別にみると、全ての売上・予算規模で「②予防的対応」が「①事後的対応」に比べて多くなっている。特に「②予防的対応」が多いのは、「5,000 億円以上～1 兆円未満」の75.0%、「100 億円以上～1,000 億円未満」の73.7%、「適切な指標がない」の73.5%である。

【売上・予算規模別分析】事後的対応と予防的対応に関する考え方



【経年変化】昨年度と比較すると、「①事後的対応」は4.6ポイントの減少、「②予防的対応」は5.5ポイントの増加となっている。



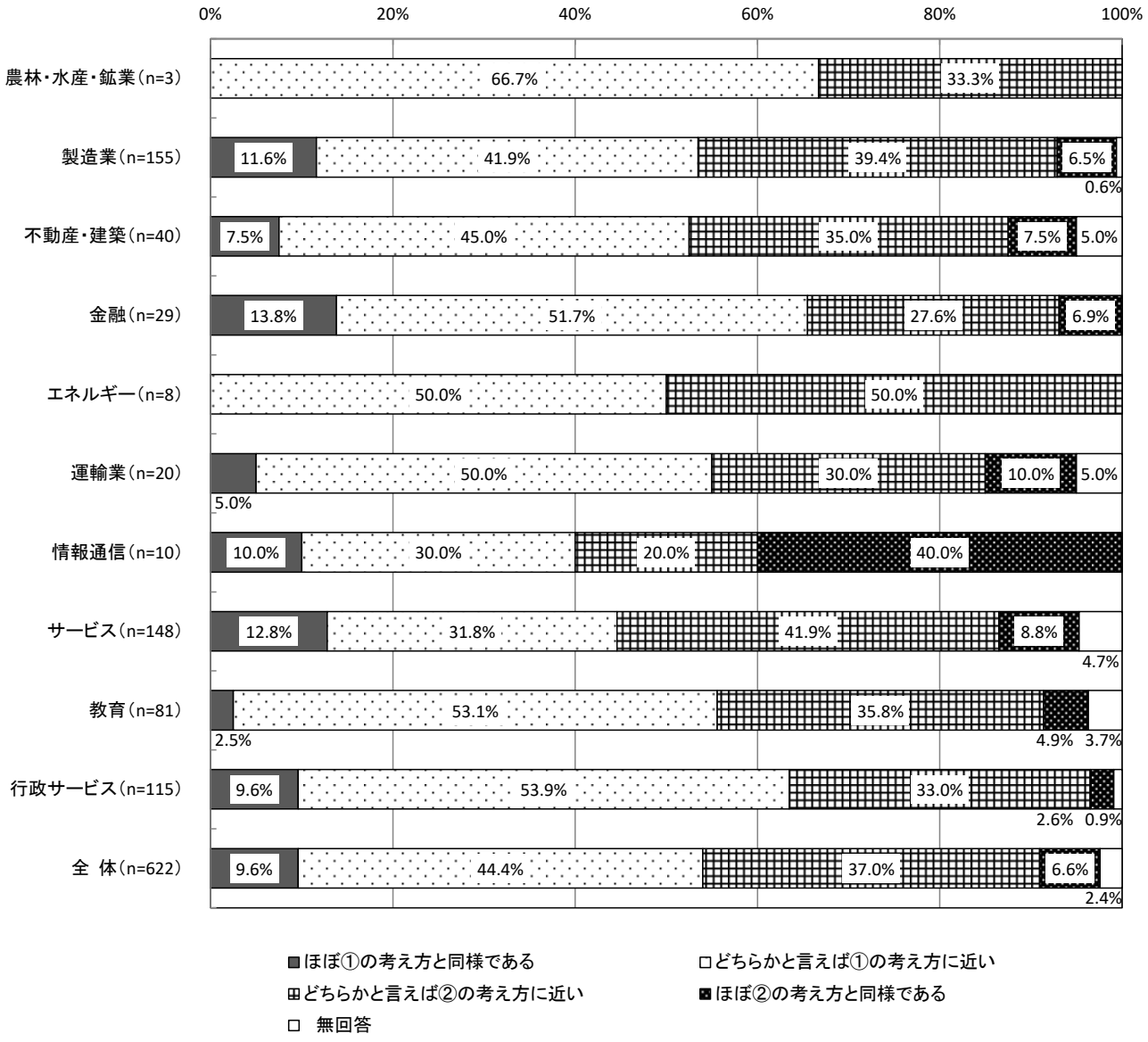
3.1.37　保険への意識　【問26-3】

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

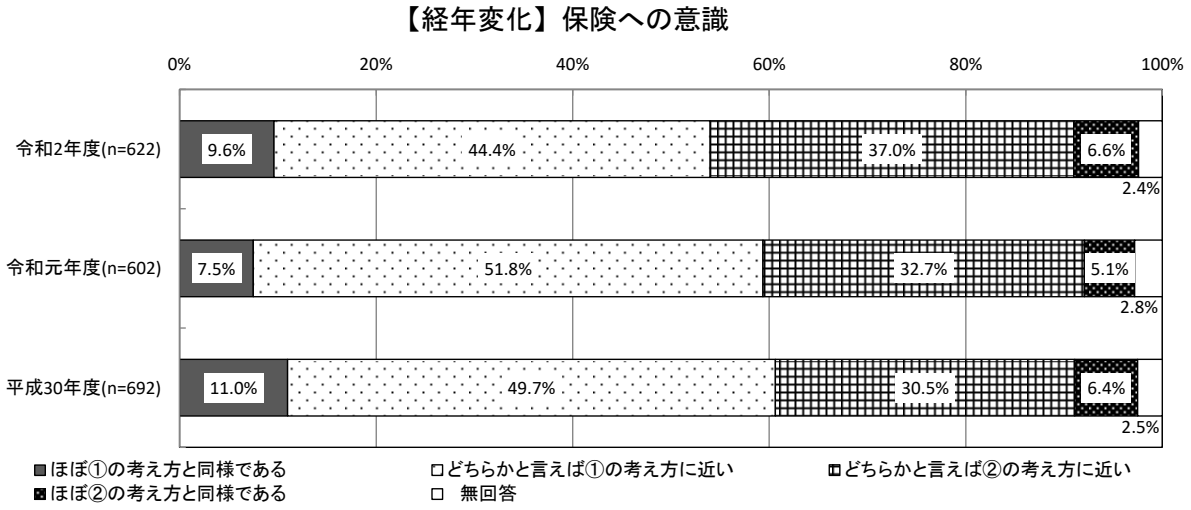
①として提示した考え方	②として提示した考え方
情報セキュリティ対策としては、人的・技術的な対策によりカバーできるところを対策すれば十分である。	情報セキュリティ対策としては、人的・技術的対策によりカバーできないリスクは保険によりまかなうべきである。

【業種別分析】業種別にみると、「情報通信」「サービス」を除くすべての業種で「①人的・技術的な対策で十分」が「②保険的な対応が必要」を上回っている。特に「金融」で65.5%、「行政サービス」で63.5%と「①人的・技術的な対策で十分」が多くなっている。

【業種別分析】保険への意識



【経年変化】昨年度と比較すると、「①人的・技術的な対策で十分」は5.3ポイントの減少となり、「②保険的な対応が必要」は5.8ポイントの増加となっている。

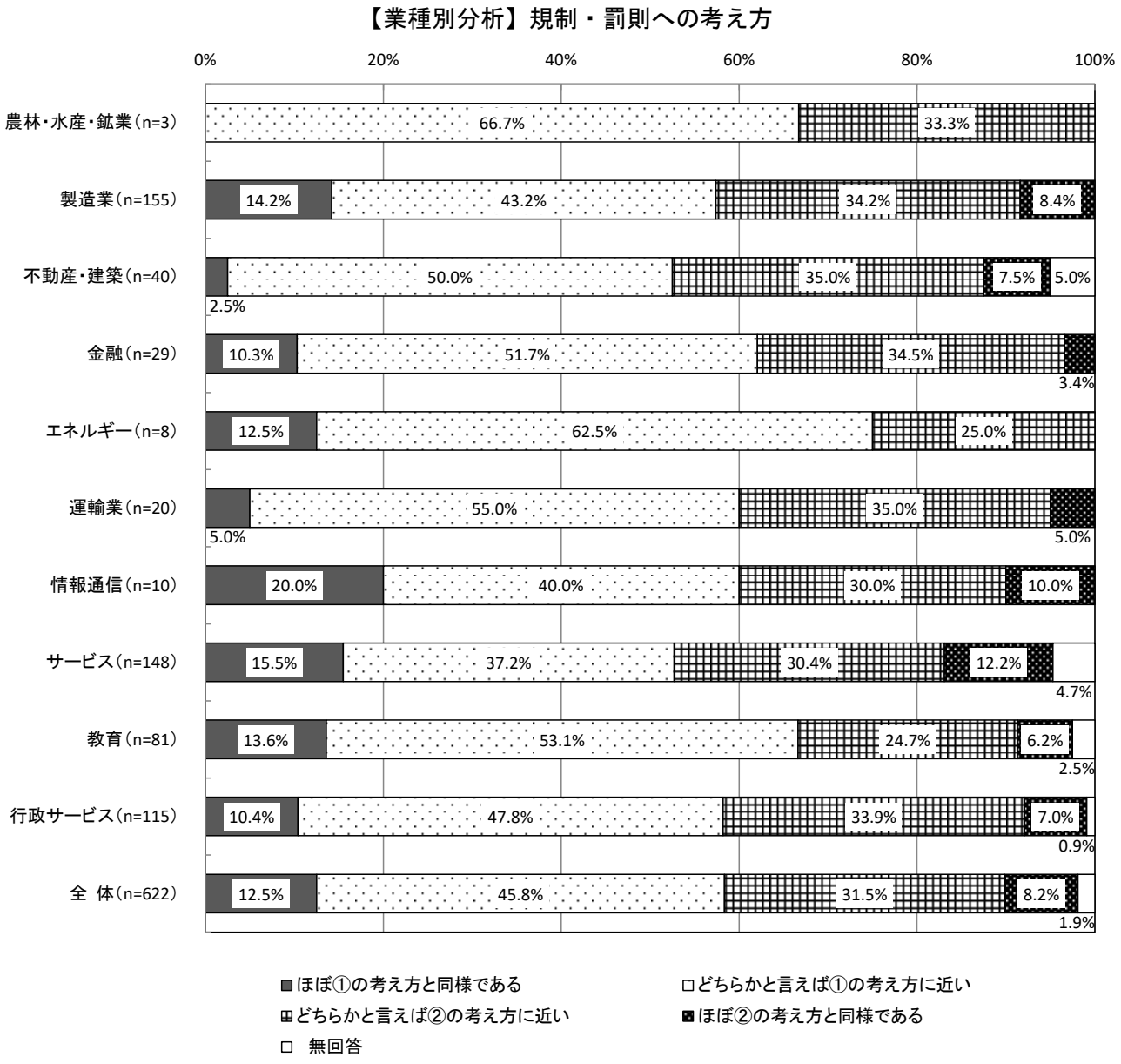


3.1.38　規制・罰則への考え方　【問26-4】

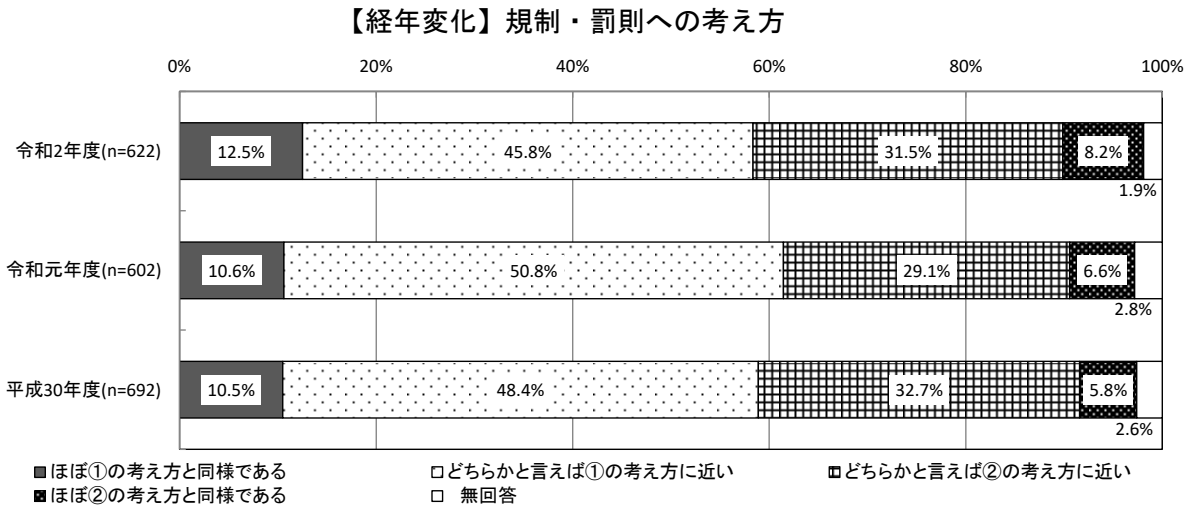
規制・罰則への考え方については、下記に挙げる2つの考え方のいずれに近いかを尋ねている。

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

【業種別分析】業種別にみると、すべての業種で「①教育と情報提供を中心とした対応」が「②規則・罰則も含む強制力のある対応」を上回っている。特に「エネルギー」では50.0ポイント「①人的・技術的な対策で十分」が多くなっている。



【経年変化】昨年度と比較すると、「①教育と情報提供を中心とした対応」は3.1ポイントの減少、「②規則・罰則も含む強制力のある対応」は4.0ポイントの増加となっている。



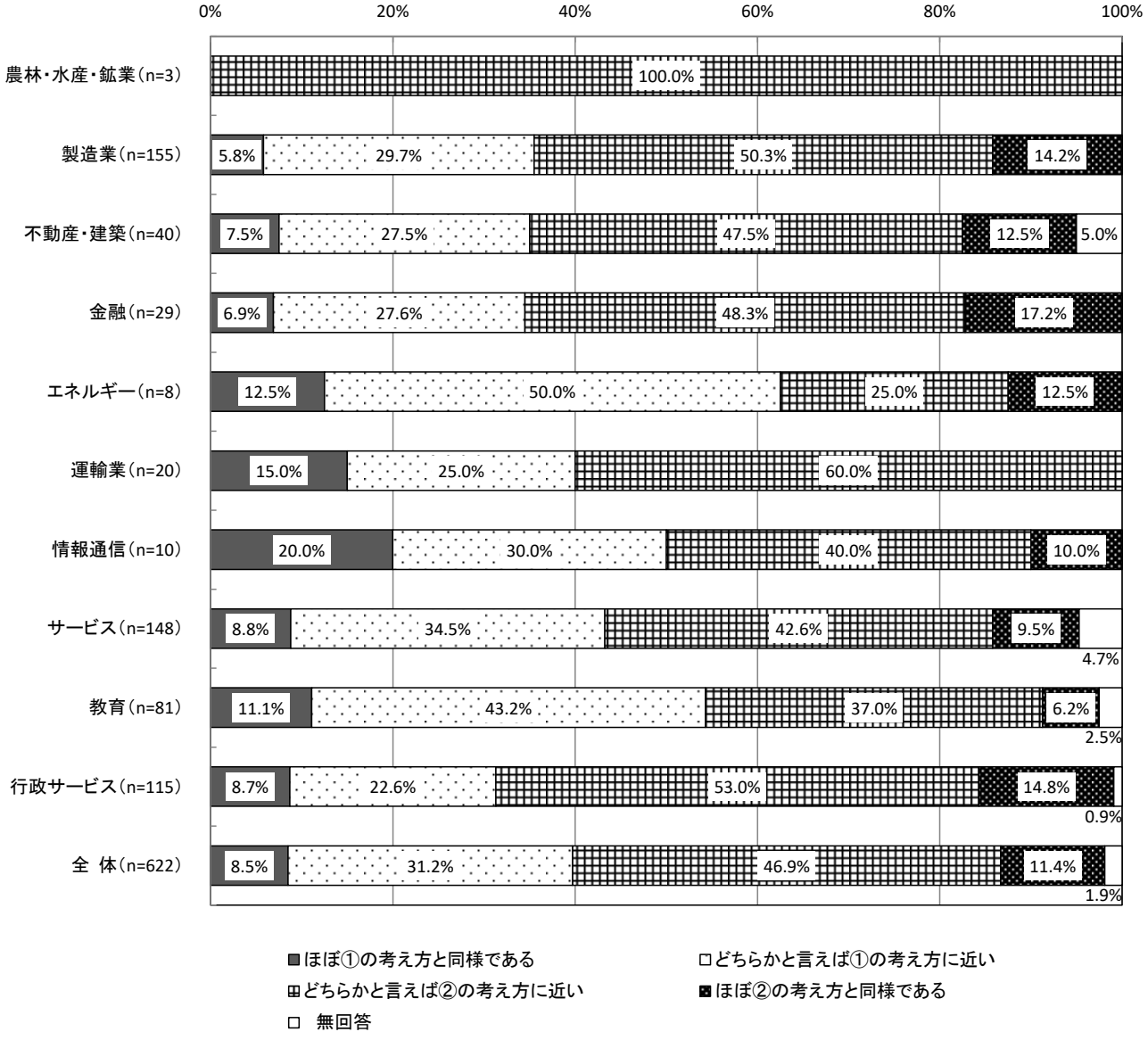
3.1.39　プライバシーの考慮に関する考え方　【問26-5】

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

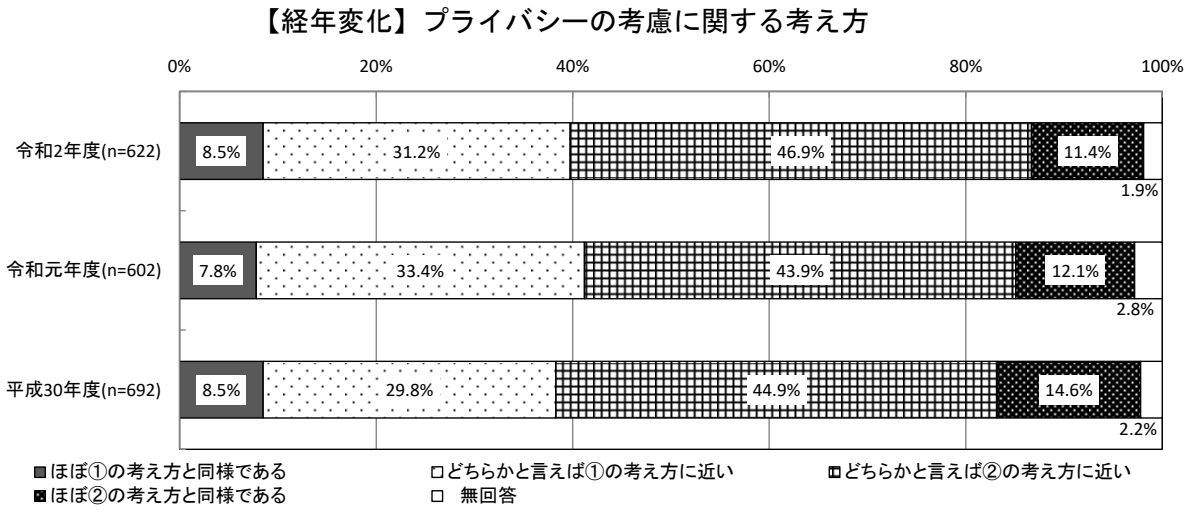
①として提示した考え方	②として提示した考え方
職場とはいえ、従業員等のプライバシーはある程度考慮したうえで、情報セキュリティ対策は行われるべきである。	職場のセキュリティ保護のためにはシステム利用状況のモニタリングなどによるプライバシーの侵害はやむをえない。

【業種別分析】業種別を見ると、「エネルギー」、「情報通信」、「教育」を除くすべての業種で「②プライバシーの侵害はやむをえない」が「①プライバシーはある程度考慮すべき」を上回っている。特に「行政サービス」で36.5ポイントと「②プライバシーの侵害はやむをえない」が多くなっている。

【業種別分析】プライバシーの考慮に関する考え方



【経年変化】昨年度と比較すると、「①プライバシーはある程度考慮すべき」は1.5ポイントの減少、「②プライバシーの侵害はやむをえない」は2.3ポイントの増加となっている。



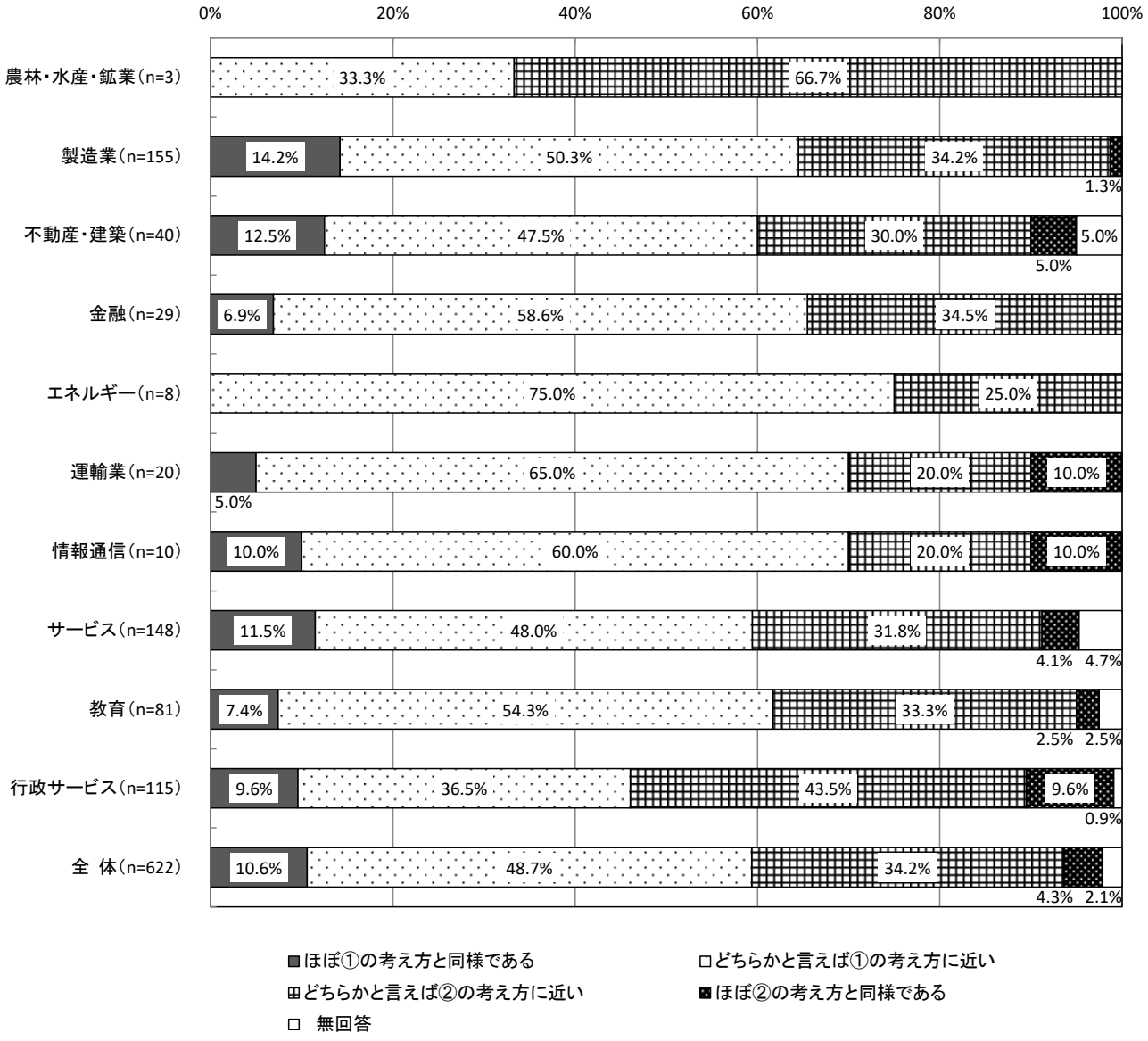
3.1.40　利便性とのバランスに関する考え方　【問26-6】

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

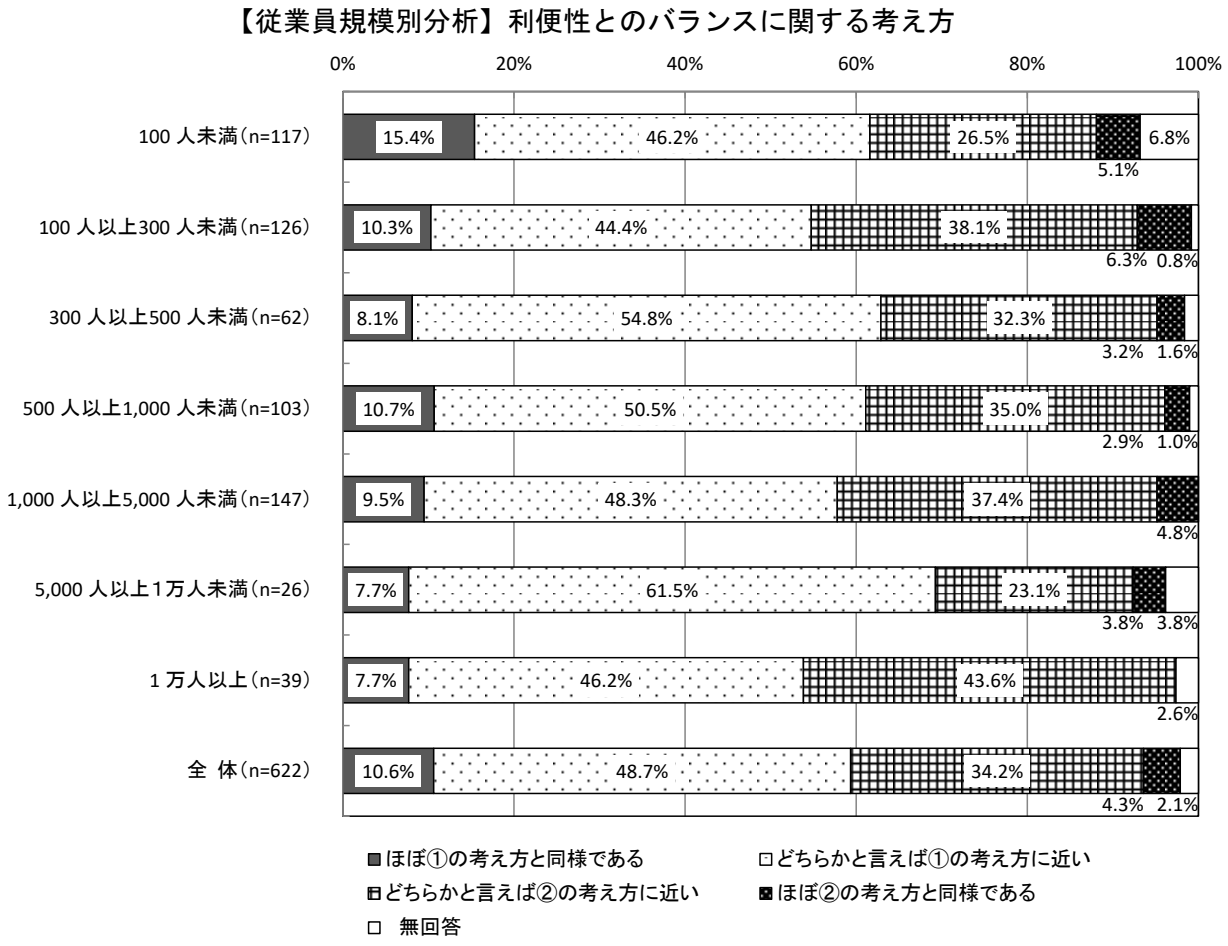
①として提示した考え方	②として提示した考え方
業務実施に負担をかけるほどのセキュリティ対策は不適当であり、利便性とのバランスを考慮すべきである。	ユーザーにシステム利用上・業務上の負担を強いてでもセキュリティを守るべきである。

【業種別分析】業種別にみると、「行政サービス」を除くすべての業種で「①利便性とのバランスを考慮」が「②負担を強いてでもセキュリティを守る」を上回っている。特に「エネルギー」で75.0%、「運輸業」「情報通信」でそれぞれ70.0%と「①利便性とのバランスを考慮」が多くなっている。

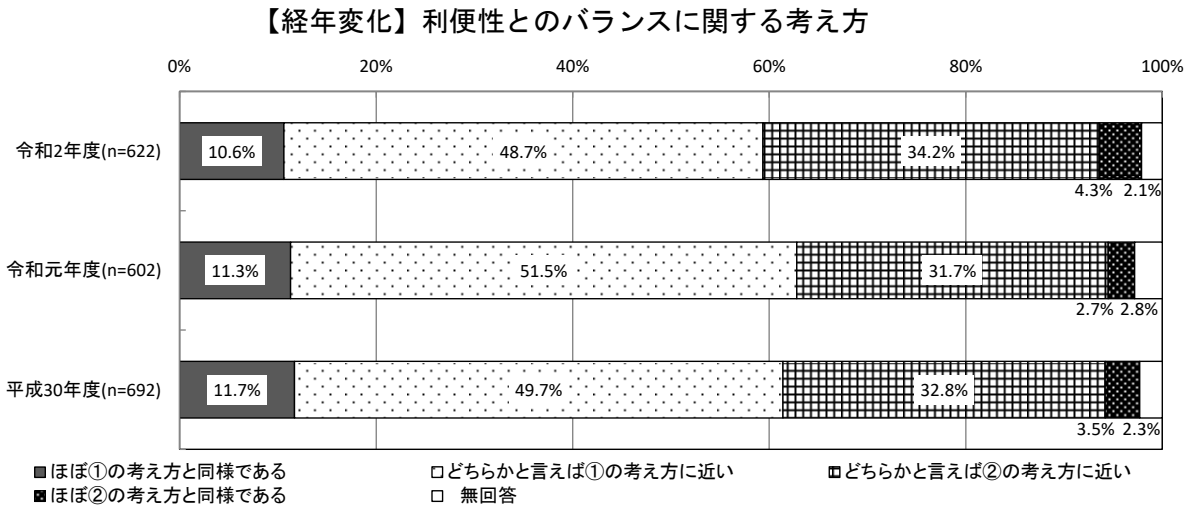
【業種別分析】利便性とのバランスに関する考え方



【従業員規模別分析】従業員規模別にみると、すべての従業員規模で「①利便性とのバランスを考慮」が「②負担を強いてでもセキュリティを守る」を上回っている。



【経年変化】昨年度と比較すると、「①利便性とのバランスを考慮」は3.5ポイントの減少、「②負担を強いてでもセキュリティを守る」は4.1ポイントの増加となっている。

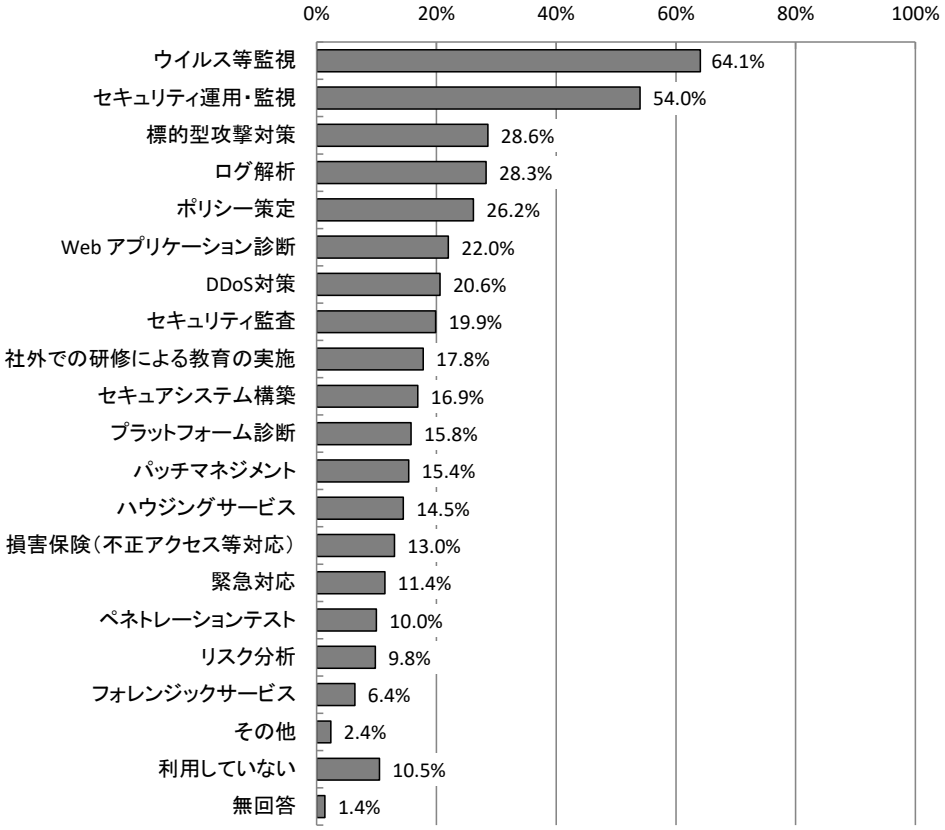


3.2　技術的対策

3.2.1　利用しているセキュリティサービス　【問27】

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64.1%で最も多く、次いで「セキュリティ運用・監視」が54.0%となっており、一方「利用していない」は10.5%となっている。

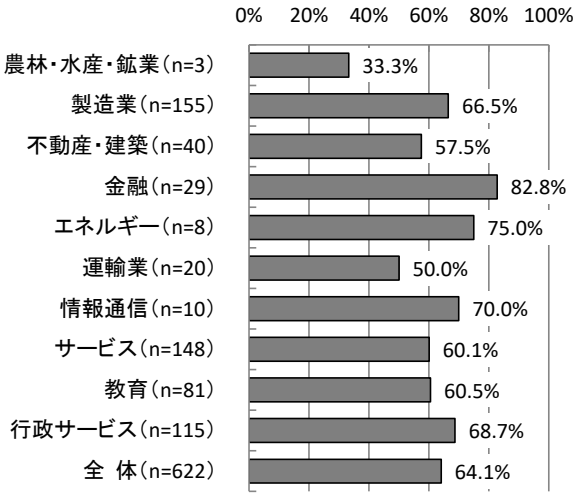
【全体】利用しているセキュリティサービス（MA,n=622）



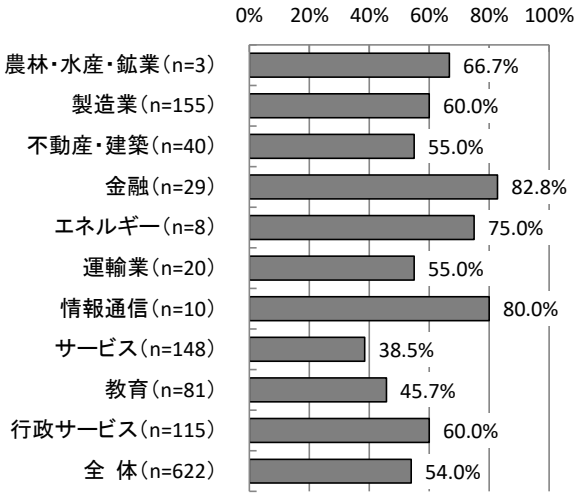
【業種別分析】業種別にみると、「ウイルス等監視」については、「金融」が82.8%で最も多く、次いで「エネルギー」が75.0%と7割を超えている。「セキュリティ運用・監視」については、「金融」が82.8%で最も多く、次いで「情報通信」が80.0%と8割を超えている。

【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



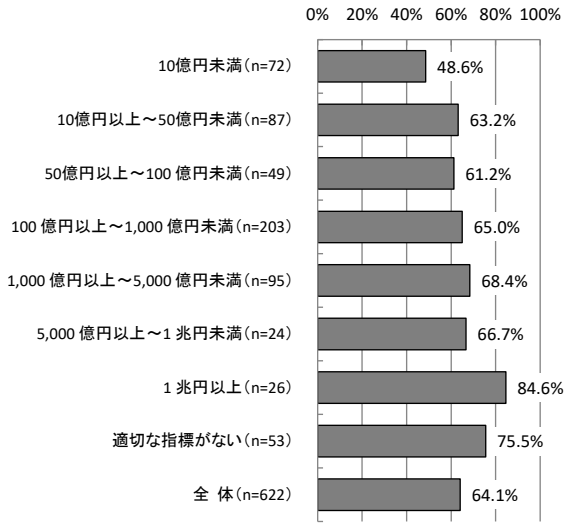
セキュリティ運用・監視



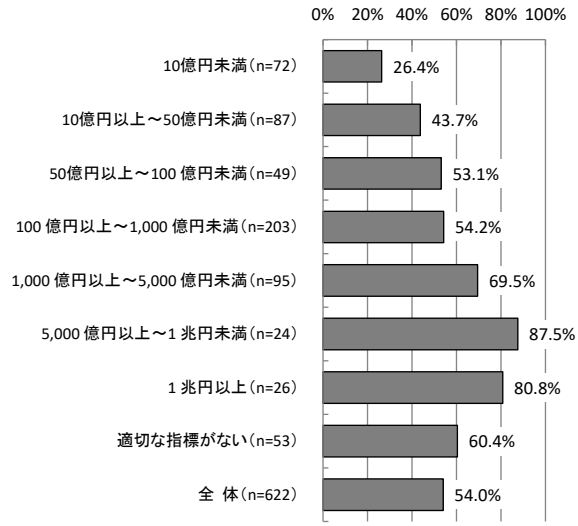
【売上・予算規模別分析】売上・予算規模別にみると、「ウイルス等監視」については、「1兆円以上」が84.6%で最も多くなっている。「セキュリティ運用・監視」については、「5,000億円以上～1兆円未満」が87.5%で最も多く、次いで「1兆円以上」が80.8%となっている。

【売上・予算規模別分析】利用しているセキュリティサービス

ウイルス等監視



セキュリティ運用・監視

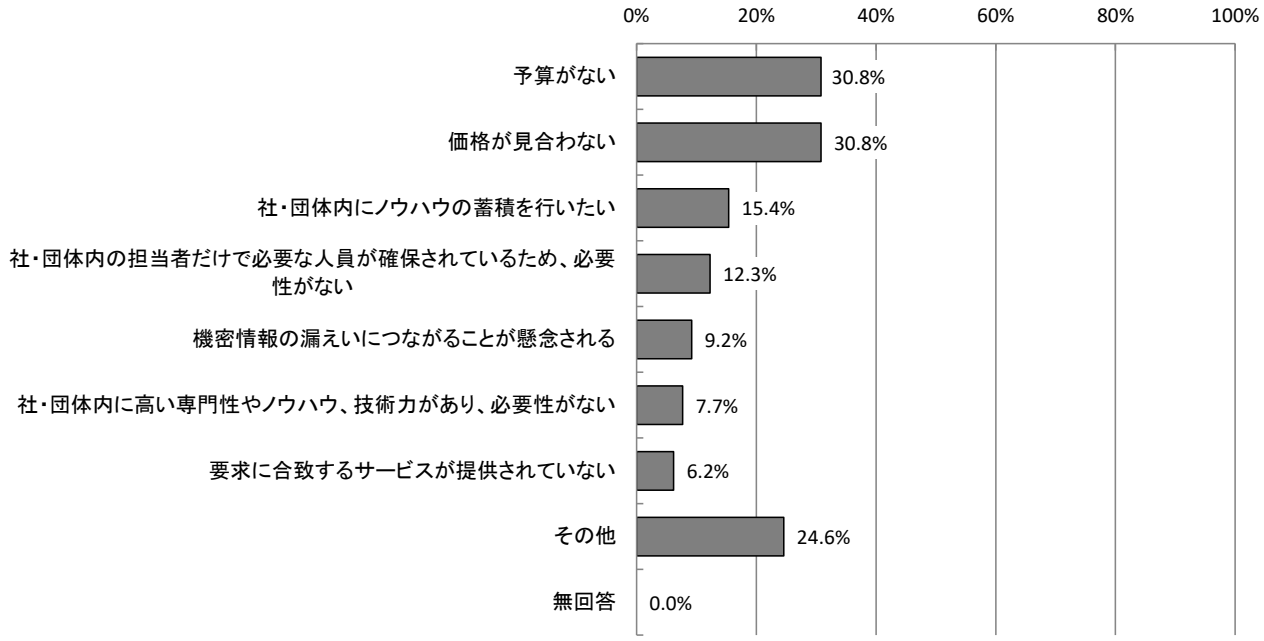


3.2.2　セキュリティサービスを利用していない理由　【問28】

セキュリティサービスを利用していない理由については、「予算がない」と「価格が見合わない」がともに30.8%で最も多く、金銭面の理由が上位に挙げられている。

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

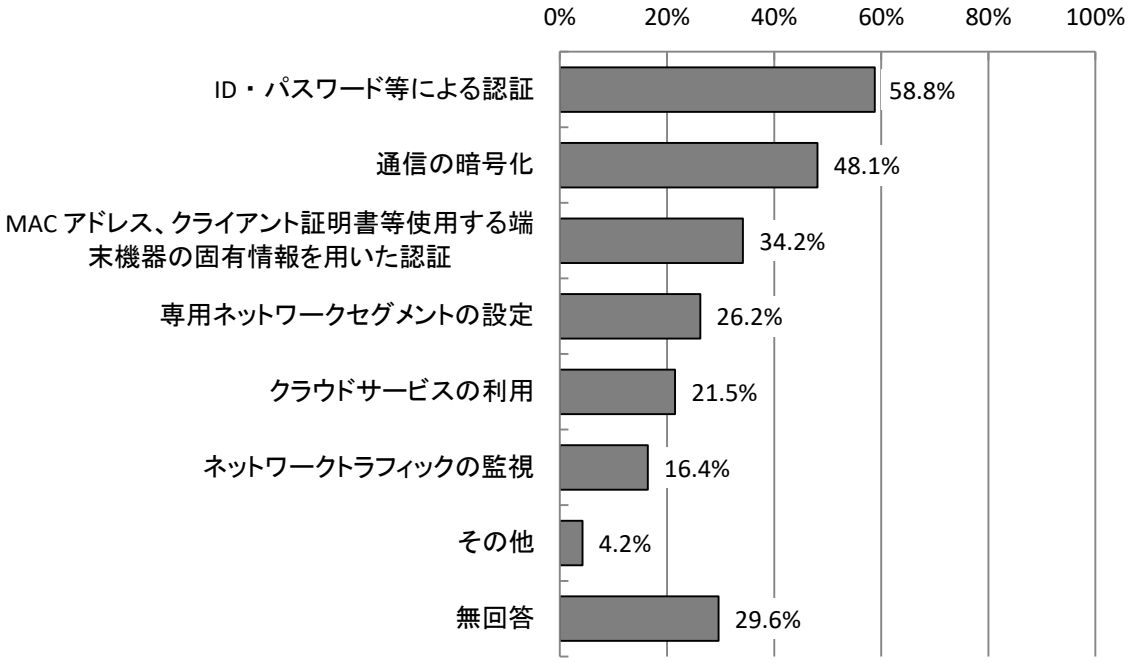
【全体】セキュリティサービスを利用していない理由（MA, n=65）



3.2.3　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29-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・パスワードによる認証」が58.8%で最も多く、次いで「通信の暗号化」が48.1%、「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34.2%、「専用ネットワークセグメントの設定」が26.2%となっている。

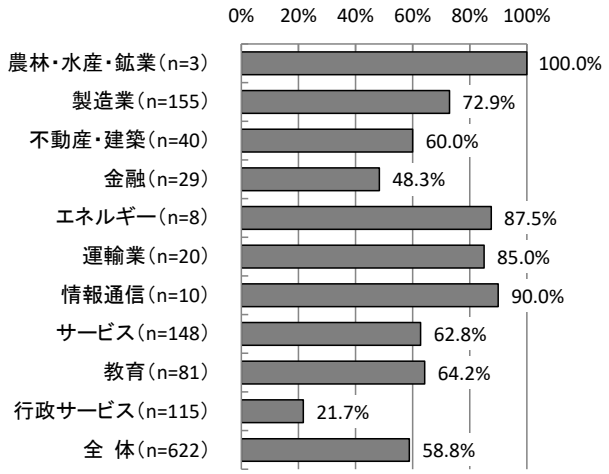
【全体】外部からの接続に対するセキュリティ対策（通信路に対する対策）（MA, n=622）



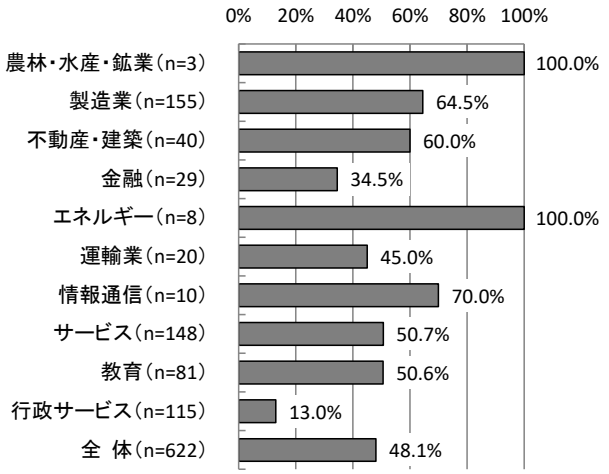
【業種別分析】業種別にみると、「ID・パスワードによる認証」及び「専用ネットワークセグメントの設定」は「情報通信」がそれぞれ90.0%、50.0%で最も多く、「通信の暗号化」及び「MACアドレス、クライアント証明書等使用する端末機器の固有情報を用いた認証」は「エネルギー」がそれぞれ100.0%、75.0%と最も多くなっている。

【業種別分析】外部からの接続に対するセキュリティ対策（通信路に対する対策）

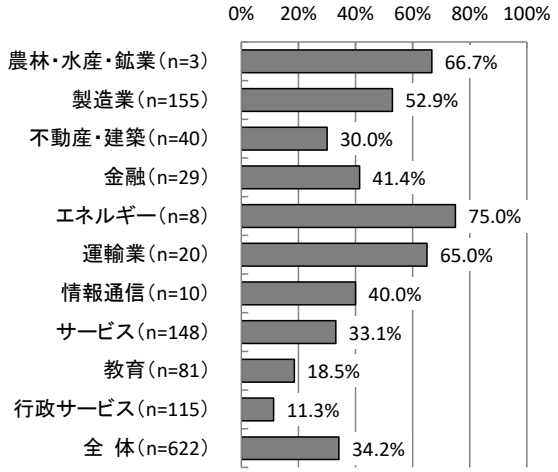
ID・パスワードによる認証



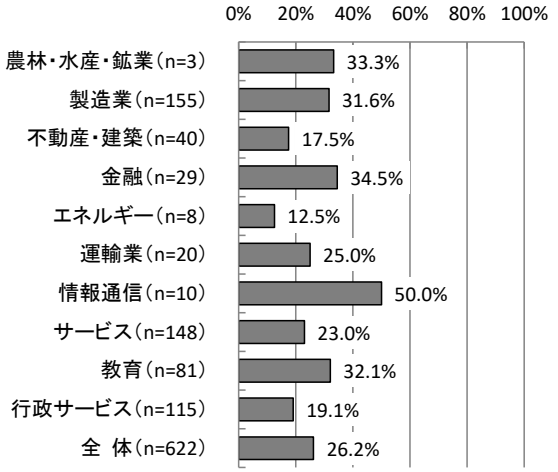
通信の暗号化



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



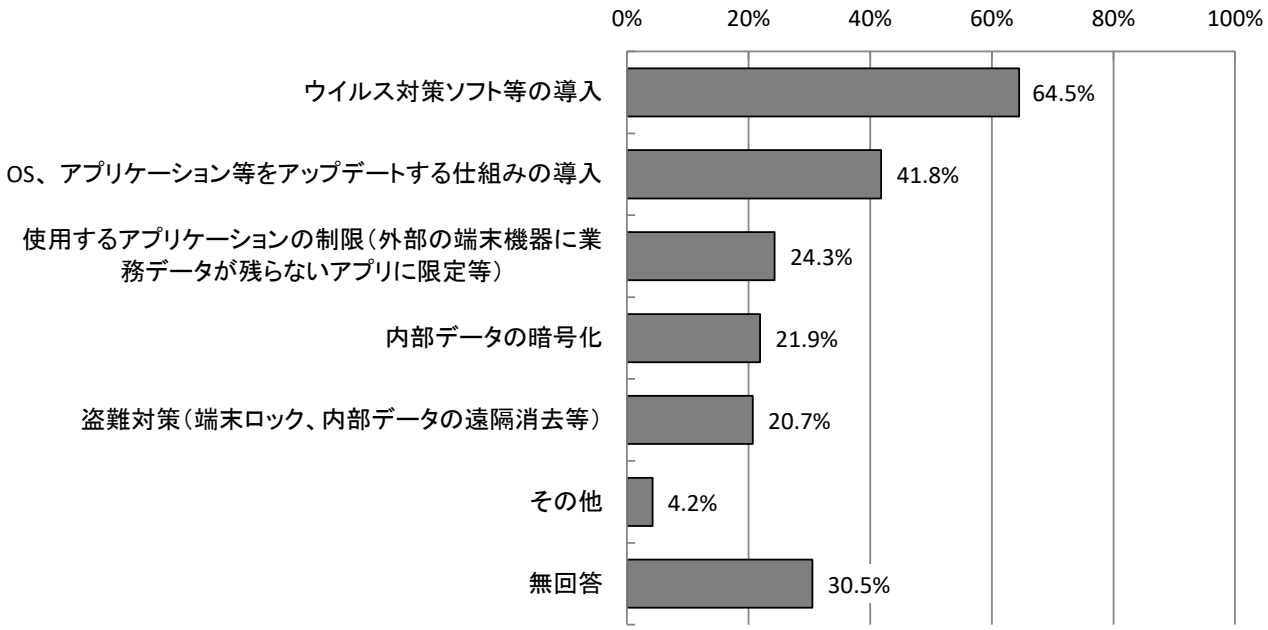
専用ネットワークセグメントの設定



3.2.4　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29-B】

外部からの接続に対するセキュリティ対策（端末に対する対策）については、「ウイルス対策ソフト等の導入」が64.5%で最も多く、次いで「OS、アプリケーション等をアップデートする仕組みの導入」が41.8%となっている。

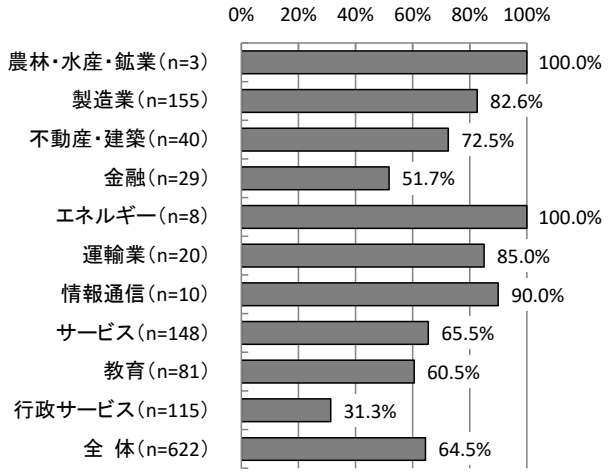
【全体】外部からの接続に対するセキュリティ対策（端末に対する対策）（MA, n=622）



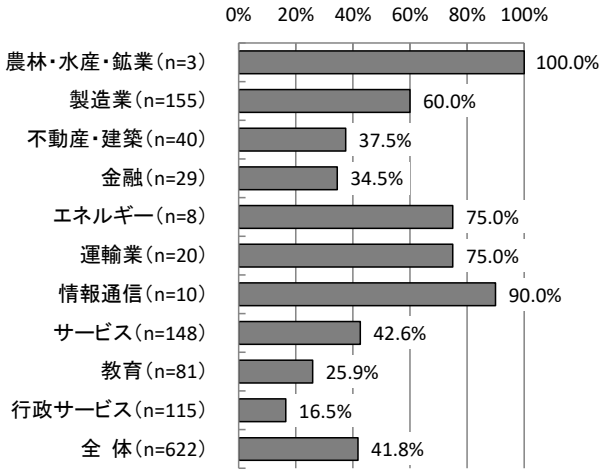
【業種別分析】業種別にみると、「ウイルス対策ソフト等の導入」及び「内部データの暗号化」では「エネルギー」がそれぞれ100.0%、62.5%と最も多く、「OS、アプリケーション等をアップデートする仕組みの導入」及び「使用するアプリケーションの制限」では「情報通信」がそれぞれ90.0%、70.0%と最も多くなっている。

【業種別分析】外部からの接続に対するセキュリティ対策（端末に対する対策）

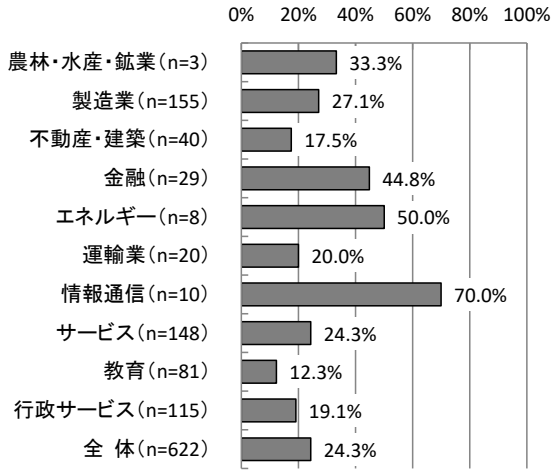
ウイルス対策ソフト等の導入



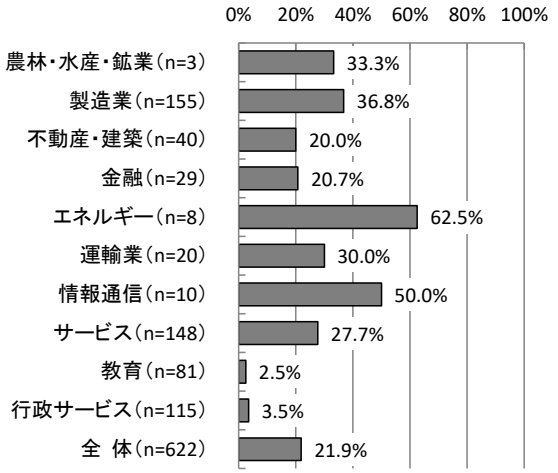
OS、アプリケーション等をアップデートする仕組みの導入



使用するアプリケーションの制限（外部の端末機器に業務データが残らないアプリに限定等）



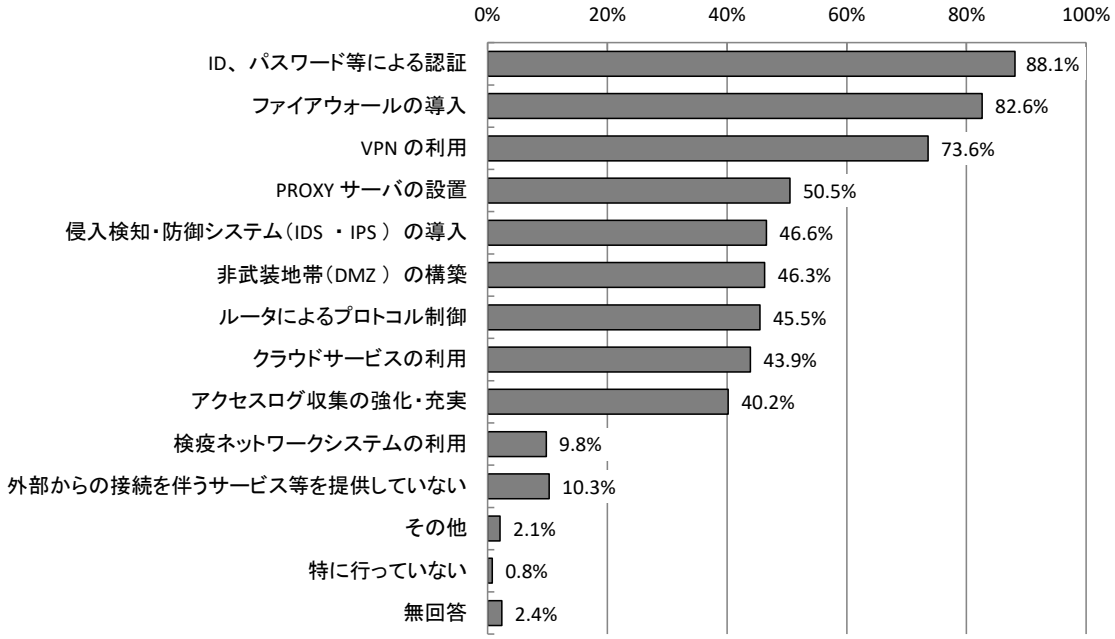
内部データの暗号化



3.2.5　インターネット接続に対するセキュリティ対策　【問30】

インターネット接続に対するセキュリティ対策については、「ID、パスワード等による認証」が88.1%で最も多く、次いで「ファイアウォールの導入」が82.6%となっている。

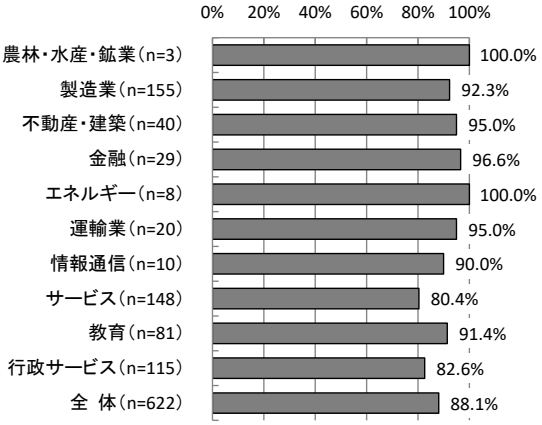
【全体】インターネット接続に対するセキュリティ対策（MA, n=622）



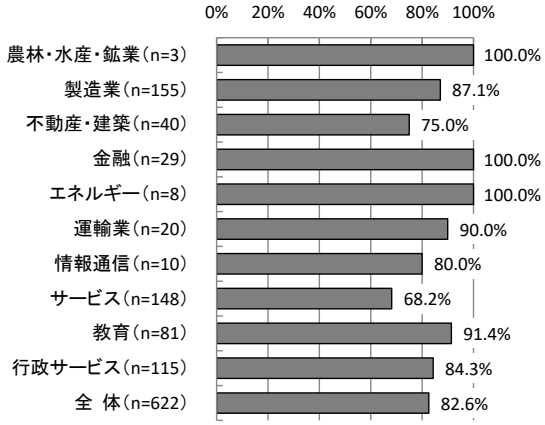
【業種別分析】業種別にみると、「ID、パスワード等による認証」については、「エネルギー」が100.0%で最も多くなっている。「ファイアウォールの導入」については、「金融」「エネルギー」がそれぞれ100.0%で最も多くなっている。

【業種別分析】インターネット接続に対するセキュリティ対策

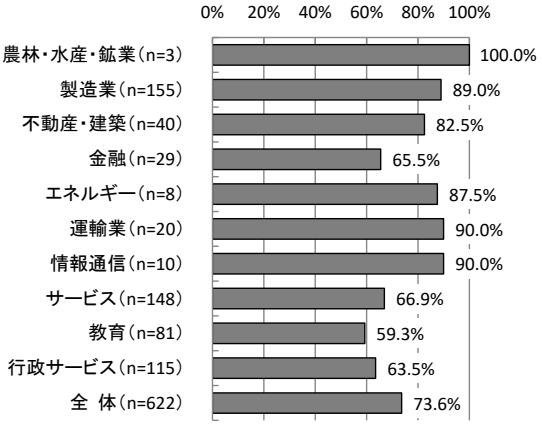
ID、パスワード等による認証



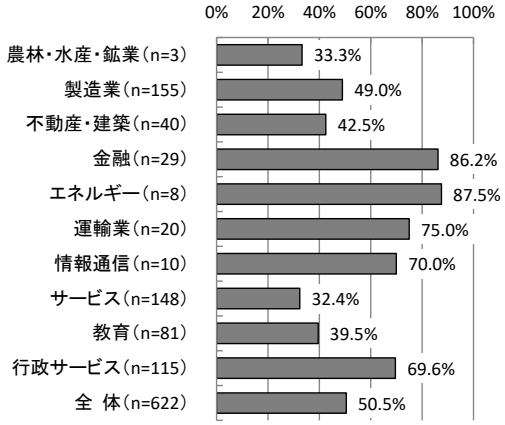
ファイアウォールの導入



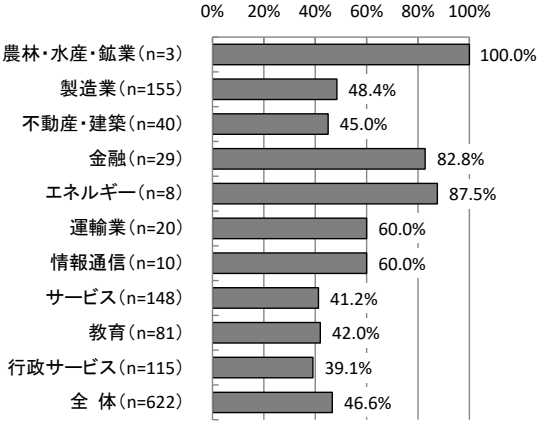
VPN の利用



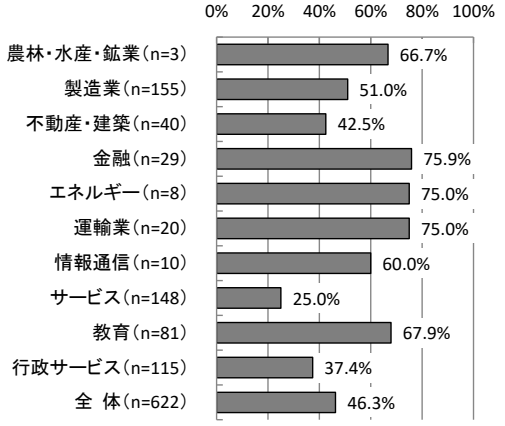
PROXY サーバの設置



侵入検知・防御システム（IDS・IPS）の導入

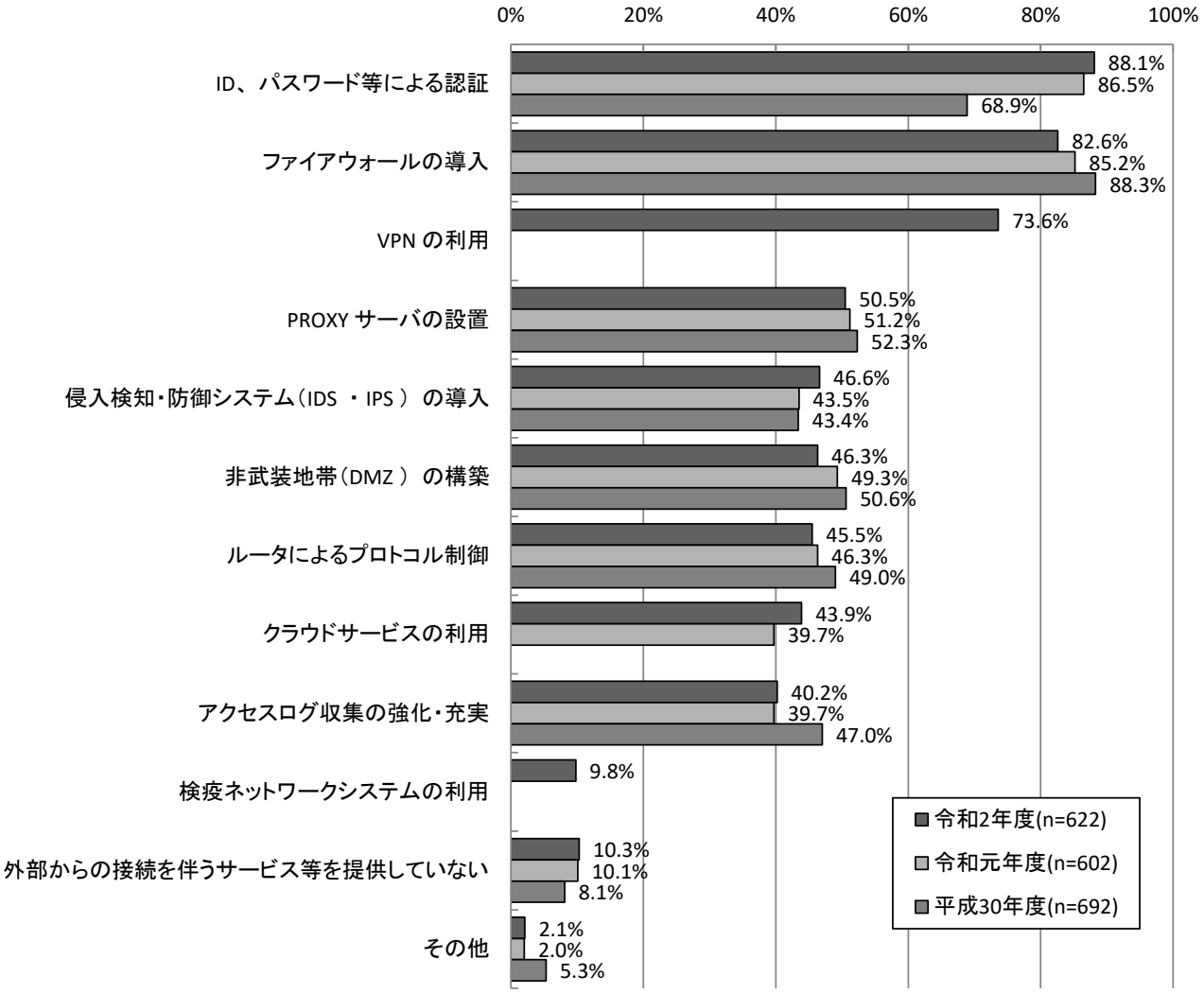


非武装地帯（DMZ）の構築



【経年変化】昨年度と比較すると、概ね増加傾向にあり、「クラウドサービスの利用」が4.2ポイント、「侵入検知・防御システム（IDS・IPS）の導入」が3.1ポイント増加している。一方「非武装地帯（DMZ）の構築」は3.0ポイント減少となっている。

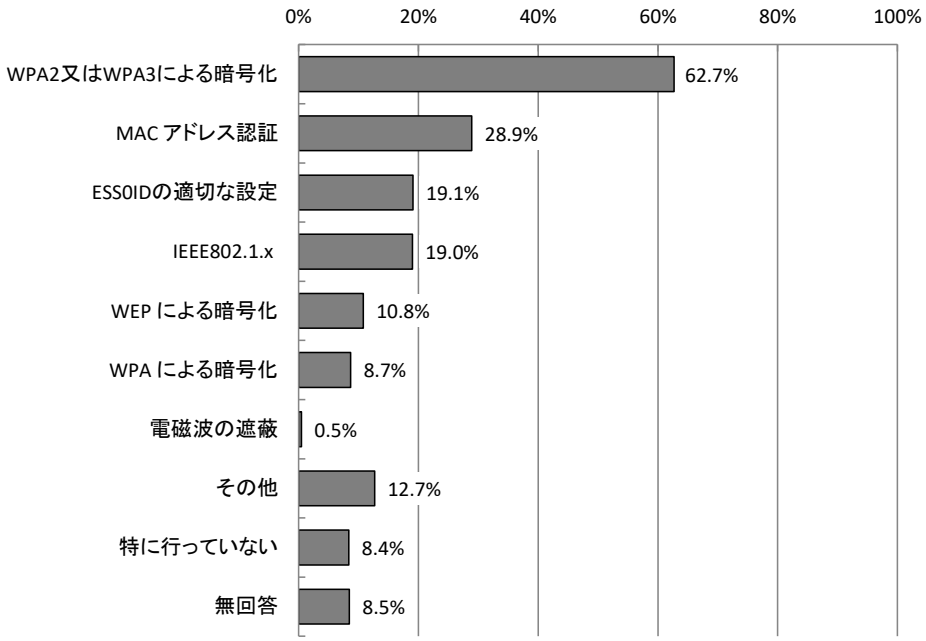
【経年変化】インターネット接続に対するセキュリティ対策



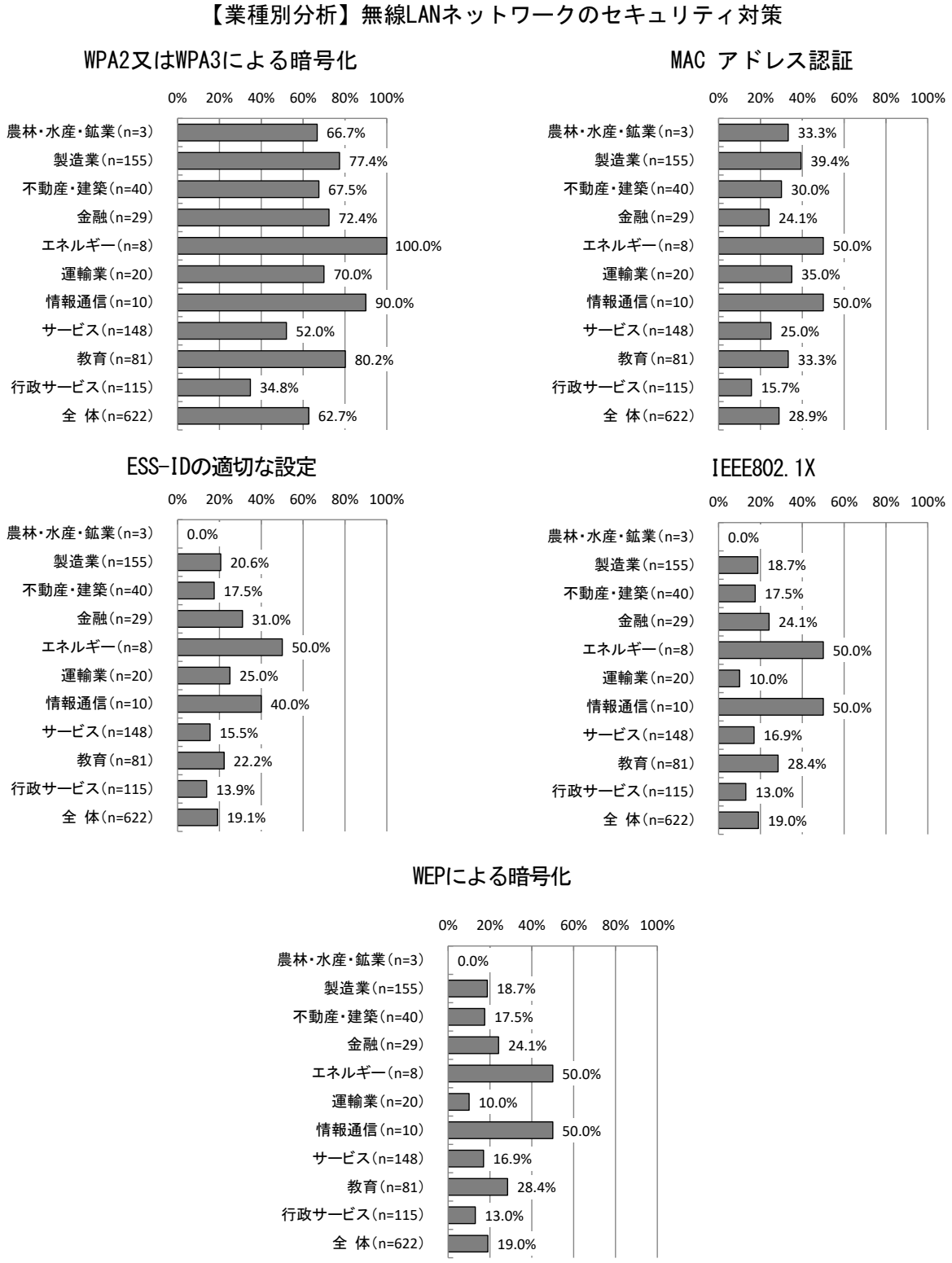
3.2.6　無線LANネットワークのセキュリティ対策　【問31】

無線LANネットワークのセキュリティ対策については、「WPA2又はWPA3による暗号化」が62.7%で最も多く、次いで「MACアドレス認証」が28.9%となっている。

【全体】無線LANネットワークのセキュリティ対策（MA,n=622）

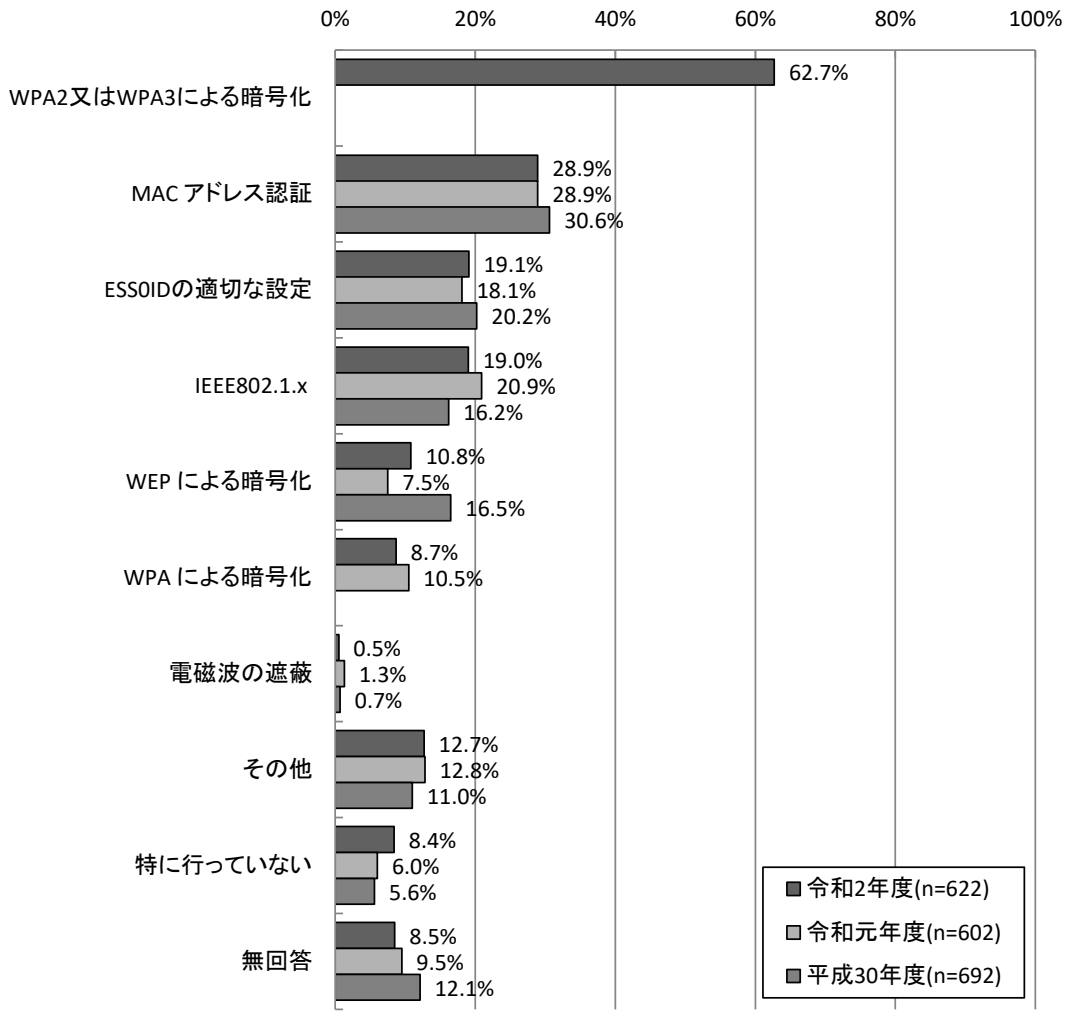


【業種別分析】業種別にみると、「WPA2又はWPA3による暗号化」については、「エネルギー」が100.0%で最も多く、次いで「情報通信」が90.0%となっている。「MACアドレス認証」については、「エネルギー」「情報通信」がそれぞれ50.0%で最も多くなっている。



【経年変化】昨年度と比較すると、「WEPによる暗号化」が3.3ポイントの増加、「IEEE802.1.x」が1.9ポイントの減少となっている。

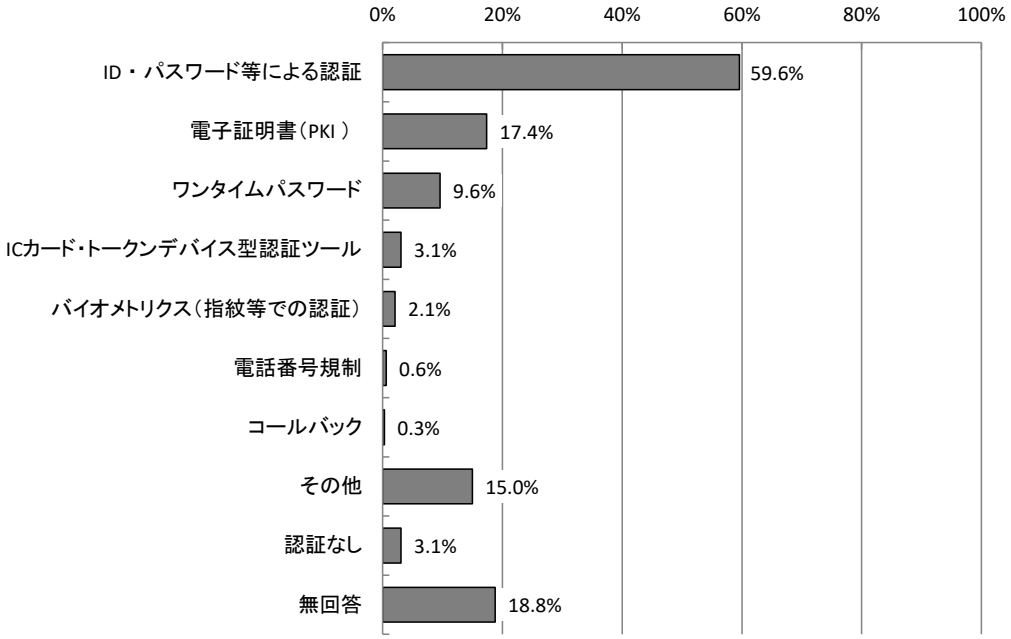
【経年変化】無線LANネットワークのセキュリティ対策



3.2.7　社外等からのインターネット経由接続における認証方法　【問32】

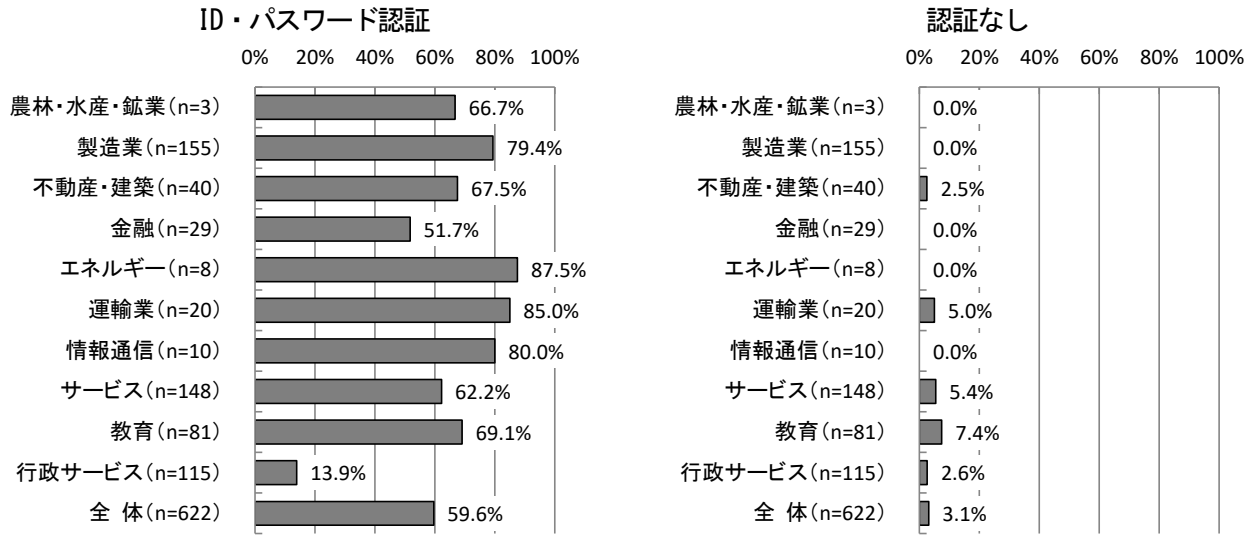
インターネットへの接続の認証方法については、「ID・パスワード認証」が59.6%で最も多く、「認証なし」は3.1%となっている。

【全体】インターネットへの接続の認証方法（MA, n=622）



【業種別分析】業種別にみると、「ID・パスワード認証」については、「エネルギー」が87.5%で最も多く、次いで「運輸業」が85.0%、「情報通信」が80.0%で続いている。「認証なし」については、「教育」が7.4%、「サービス」が5.4%、「運輸業」が5.0%で多くなっている。

【業種別分析】インターネットへの接続の認証方法

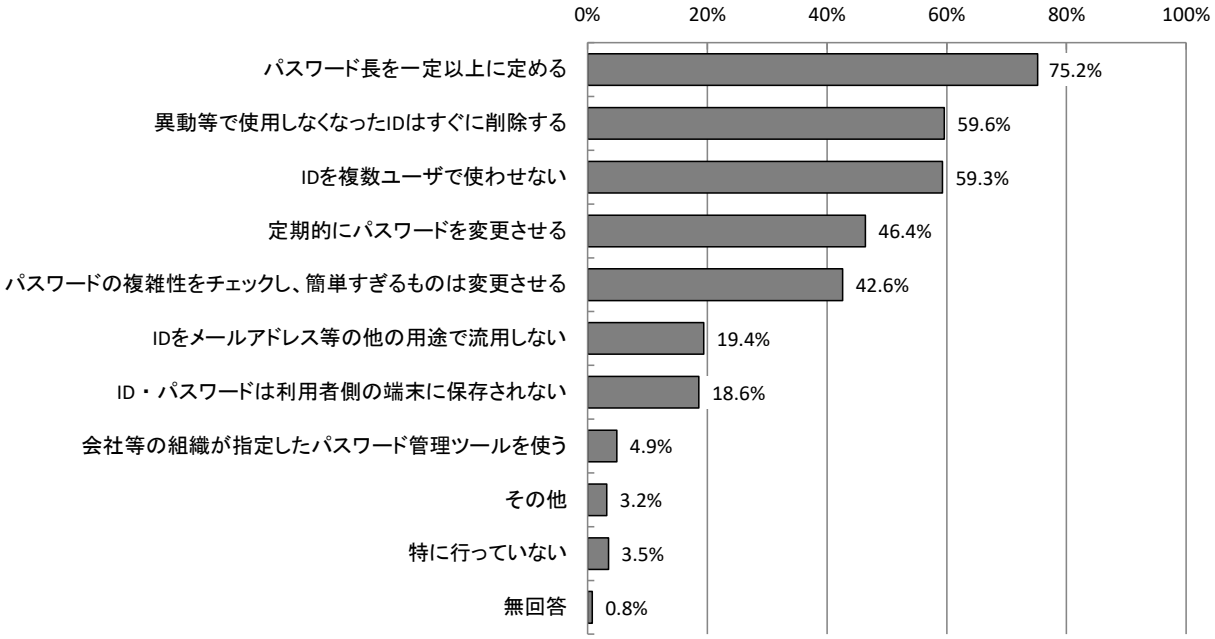


3.2.8　ID・パスワードの管理方法　【問33】

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75.2%で最も多く、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59.6%となっている。

※本項目は、インターネット接続を行う際に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。

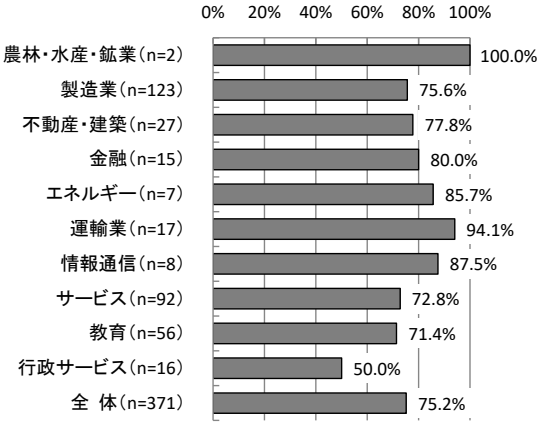
【全体】ID・パスワードの管理方法（MA, n=371）



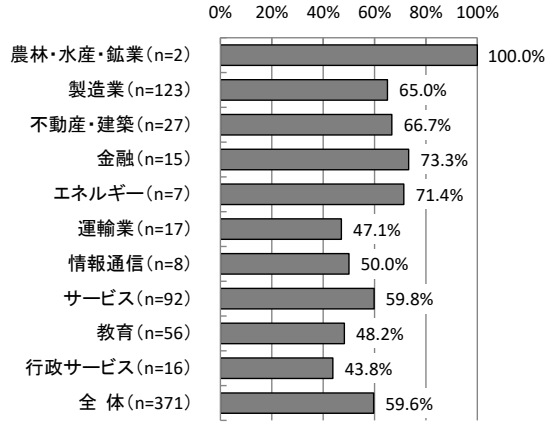
【業種別分析】業種別にみると、「パスワード長を一定以上に定める」については、「運輸業」が94.1%で最も多く、次いで「情報通信」が87.5%となっている。「異動等で使用しなくなったIDはすぐに削除する」については、「金融」が73.3%で最も多く、次いで「エネルギー」が71.4%となっている。

【業種別分析】ID・パスワードの管理対策

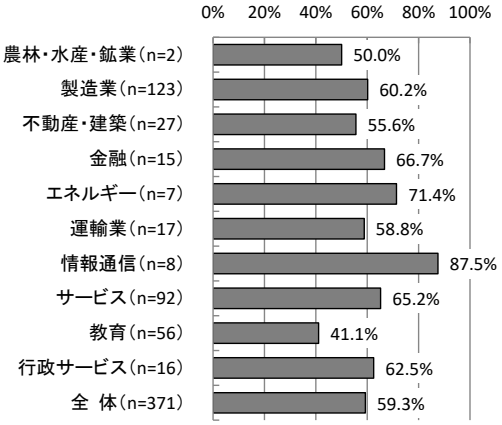
パスワード長を一定以上に定める



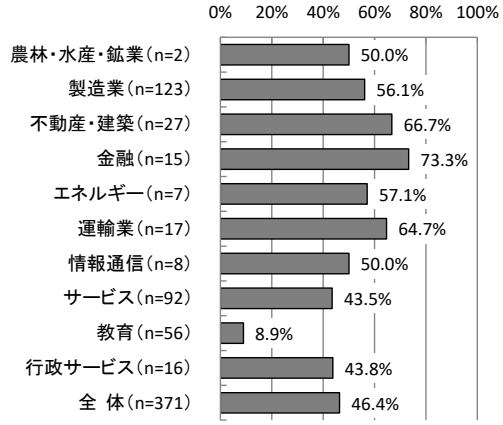
異動等で使用しなくなったIDはすぐに削除する



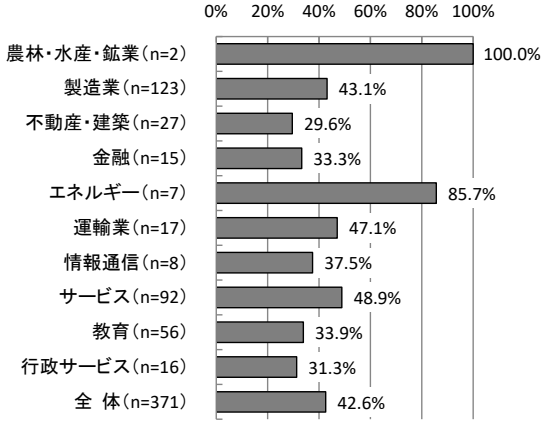
IDを複数ユーザーで使わせない



定期的にパスワードを強制的に変更させる



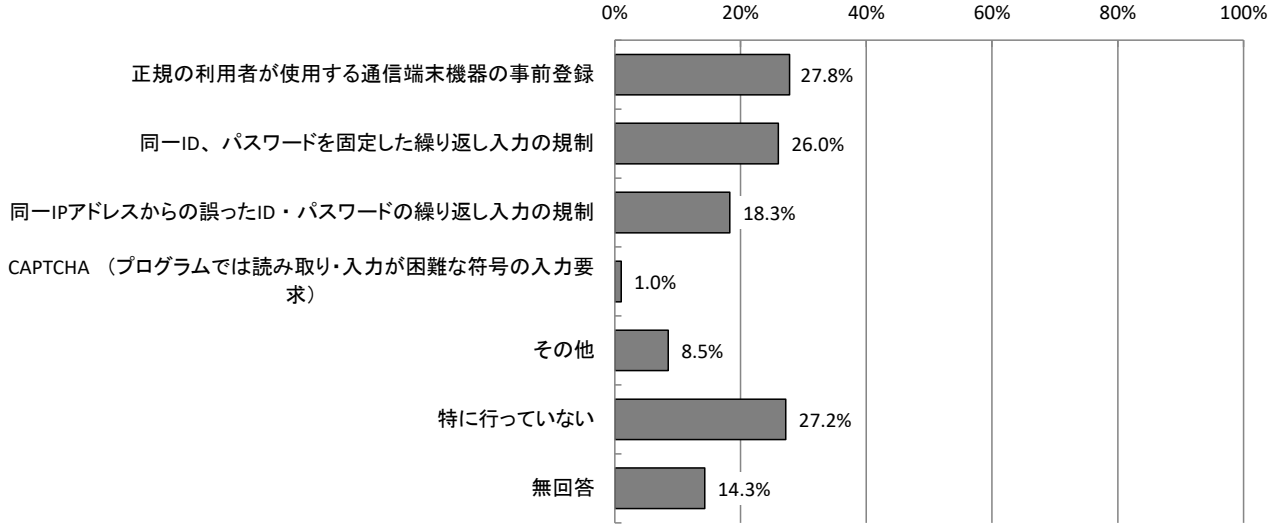
パスワードの複雑性をチェックし、簡単すぎるものは変更させる



3.2.9　不正ログイン対策　【問34】

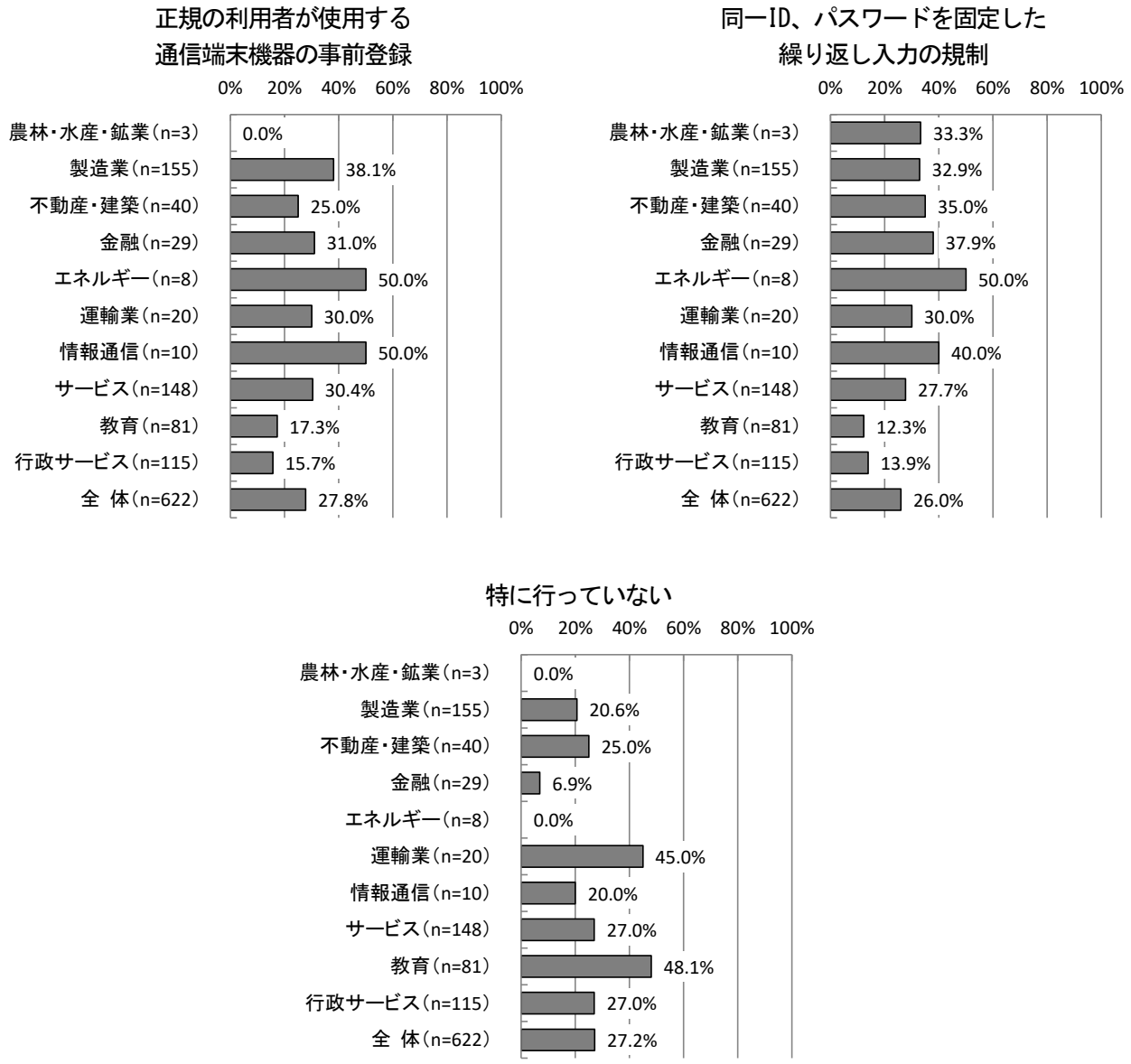
不正ログイン対策については、「正規の利用者が使用する通信端末機器の事前登録」が27.8%で最も多く、次いで「同一ID、パスワードを固定した繰り返し入力の規制」が26.0%、「同一IPアドレスからの誤ったID・パスワードの繰り返し入力の規制」が18.3%となっている。一方、「特に行っていない」は27.2%となっている。

【全体】不正ログイン対策（MA, n=622）

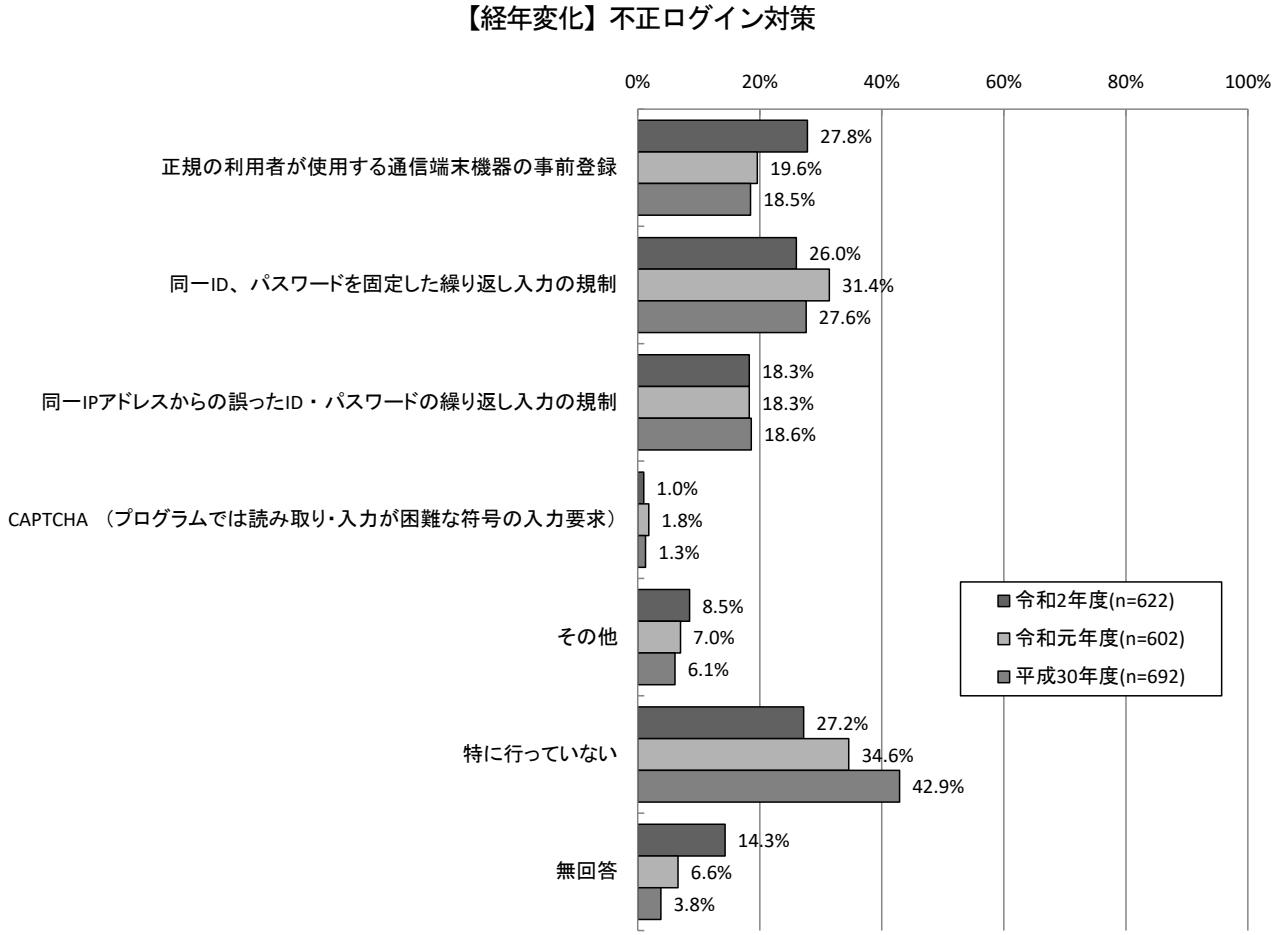


【業種別分析】業種別にみると、「正規の利用者が使用する通信端末機器の事前登録」については、「エネルギー」「情報通信」がそれぞれ50.0%と最も多くなっている。「同一ID、パスワードを固定した繰り返し入力の規制」については、「エネルギー」が50.0%で最も多く、次いで「情報通信」が40.0%となっている。「特に行っていない」については、「教育」が48.1%で最も多く、次いで「運輸業」が45.0%と多くなっている。

【業種別分析】不正ログイン対策



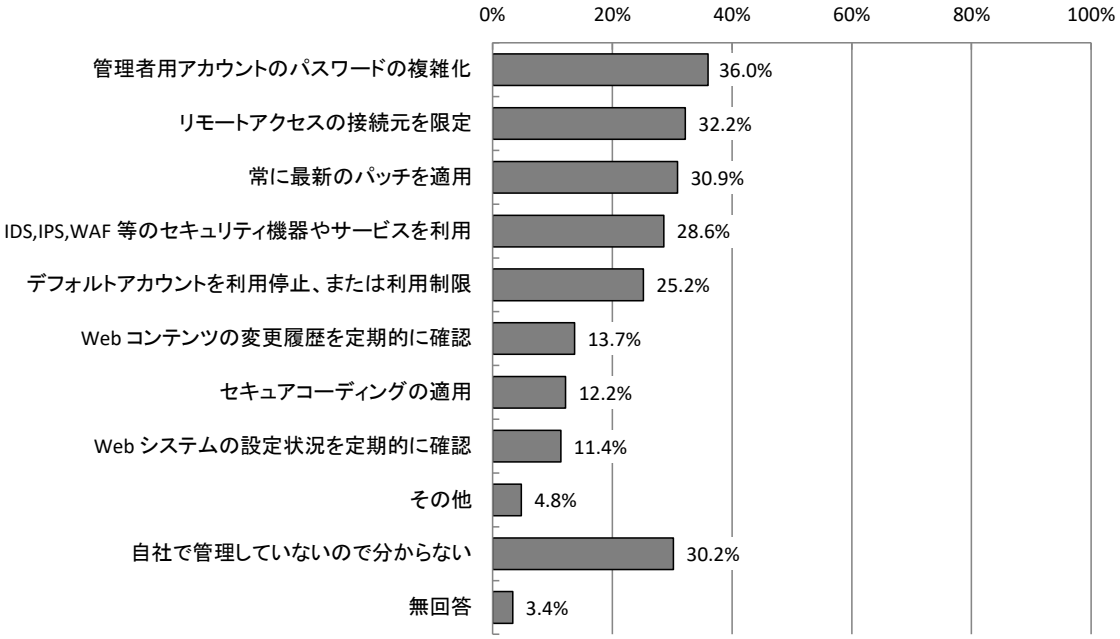
【経年変化】昨年度と比較すると、「正規の利用者が使用する通信端末機器の事前登録」は8.2ポイントの増加、「同一ID、パスワードを固定した繰り返し入力の規制」は5.4ポイントの減少となっている。また、「特に行っていない」は7.4ポイント減少している。



3.2.10 Webサーバのセキュリティ対策 【問35】

Webサーバ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36.0%で最も多く、次いで「リモートアクセスの接続元を限定」が32.2%、「常に最新のパッチを適用」が30.9%となっている。

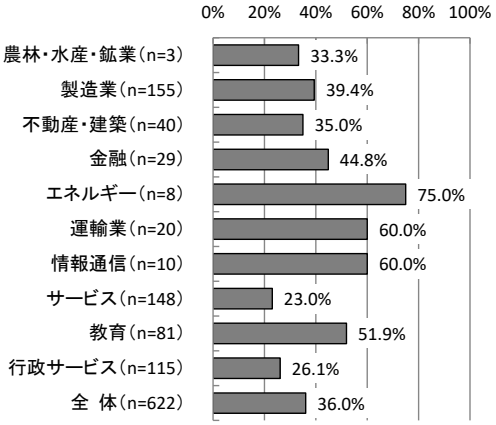
【全体】Webサーバのセキュリティ対策 (MA, n=622)



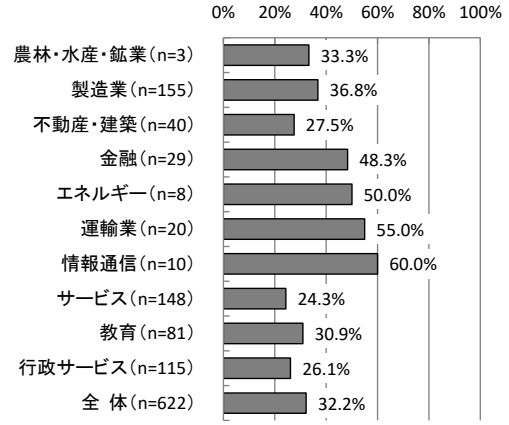
【業種別分析】業種別に見ると、「管理者用アカウントのパスワードの複雑化」については、「エネルギー」が75.0%と最も多く、次いで「運輸業」、「情報通信」がともに60.0%となっている。「リモートアクセスの接続元を限定」については、「情報通信」が60.0%と最も多く、次いで「運輸業」が55.0%、「エネルギー」が50.0%となっている。

【業種別分析】Webサーバのセキュリティ対策

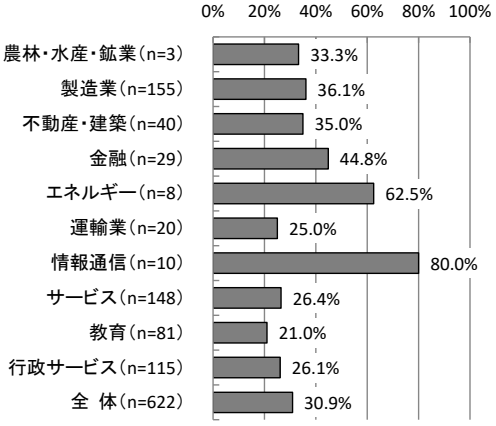
管理者用アカウントのパスワードの複雑化



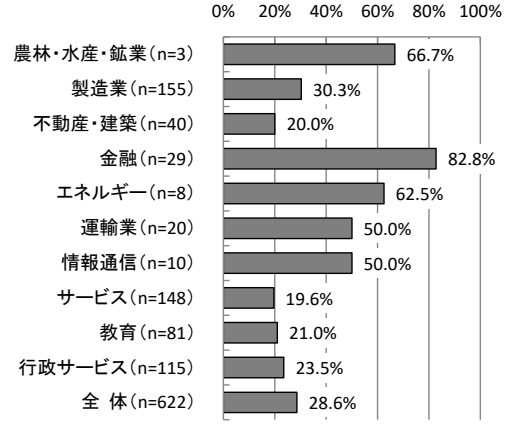
リモートアクセスの接続元を限定



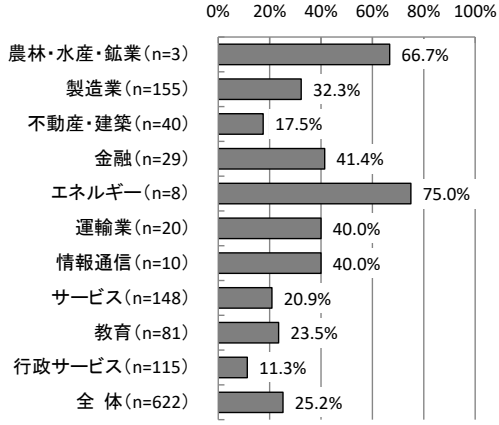
常に最新のパッチを適用



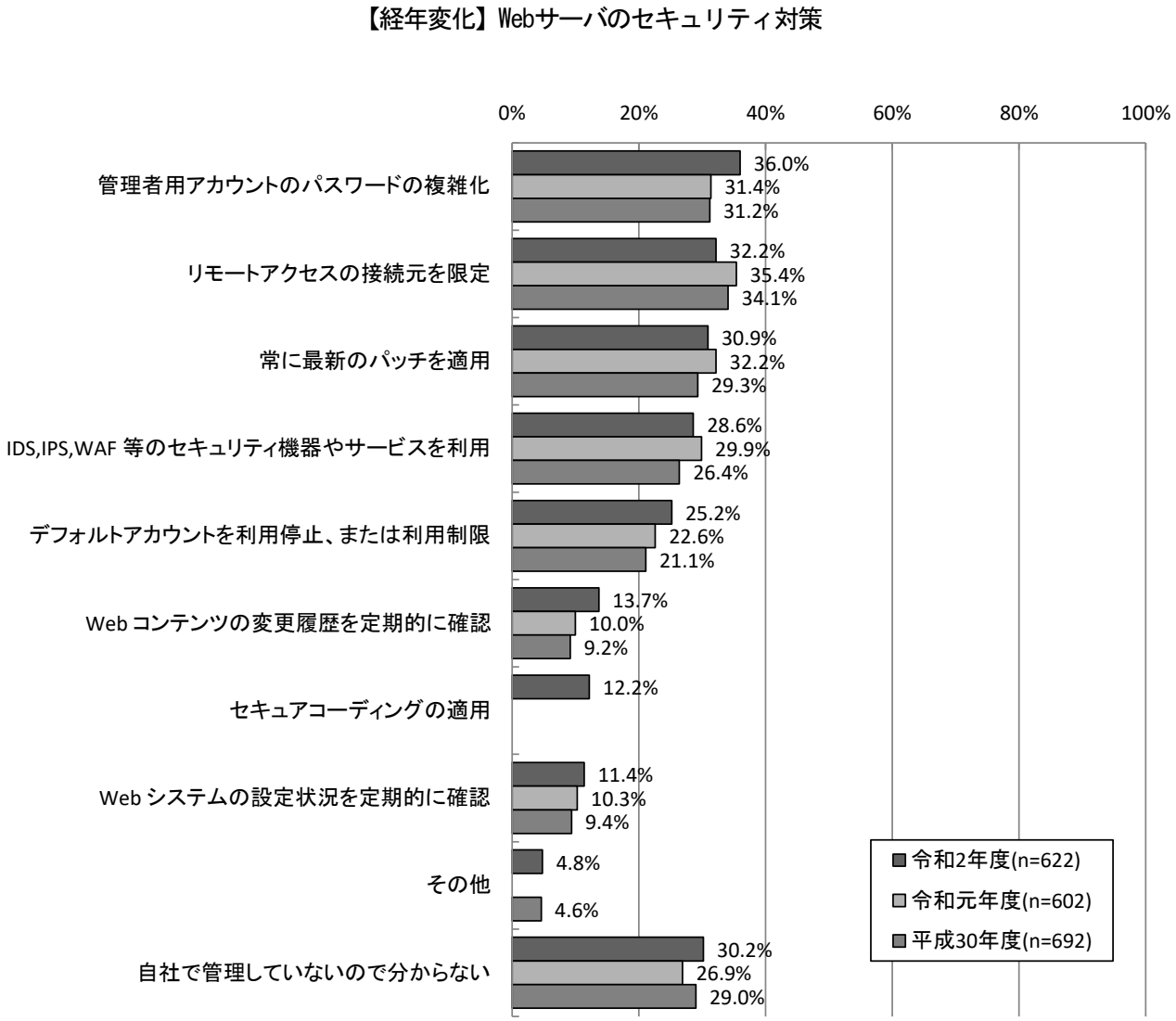
IDS, IPS, WAF 等のセキュリティ機器やサービスを利用



デフォルトアカウントを利用停止、または利用制限



【経年変化】昨年度と比較すると、「管理者用アカウントのパスワードの複雑化」が 4.6 ポイント、「Web コンテンツの変更履歴を定期的に確認」が 3.7 ポイント増加となっている。

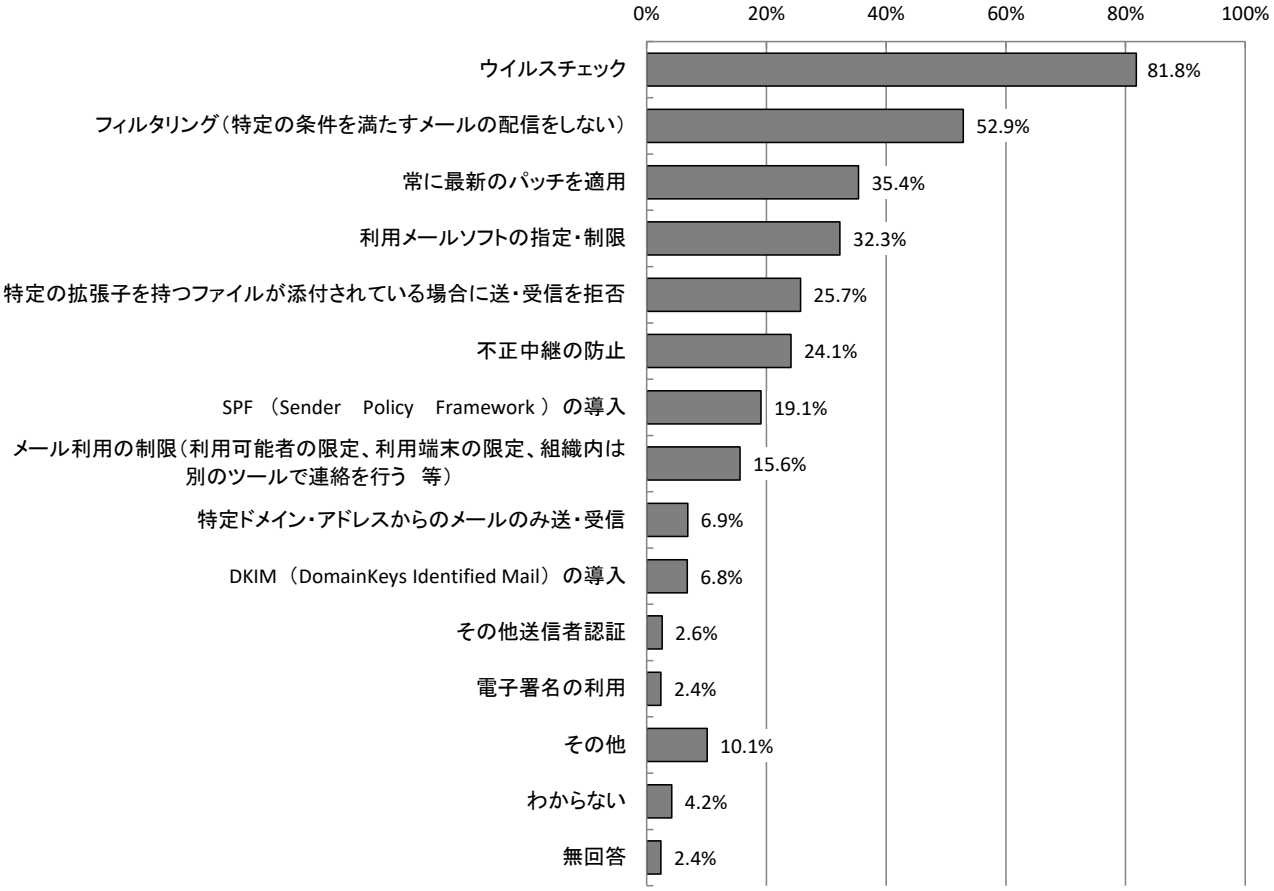


※令和２年度調査で「セキュアコーディングの適用」を新設

3.2.11　電子メールに関するセキュリティ対策　【問36】

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81.8%で最も多く、次いで「フィルタリング（特定の条件を満たすメールの配信をしない）」が52.9%、「常に最新のパッチを適用」が35.4%となっている。

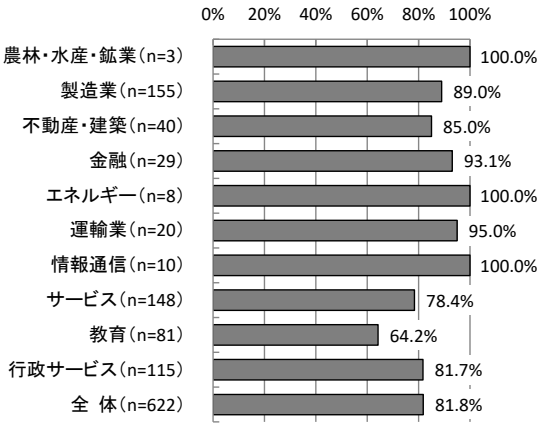
【全体】電子メールに関するセキュリティ対策（MA, n=622）



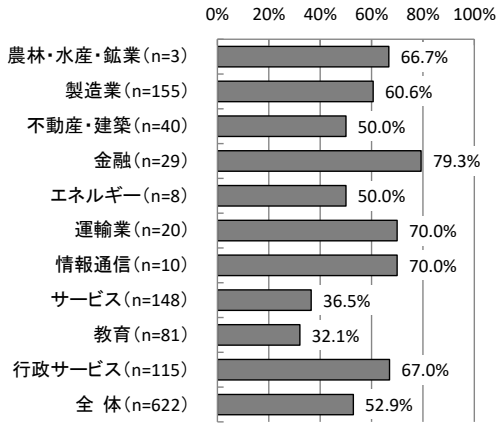
【業種別分析】業種別にみると、「ウイルスチェック」については、「エネルギー」「情報通信」がそれぞれ100.0%で最も多く、次いで「運輸業」が95.0%となっている。「フィルタリング」については、「金融」が79.3%、「常に最新のパッチを適用」については「情報通信」が70.0%と最も多くなっている。

【業種別分析】電子メールに関するセキュリティ対策

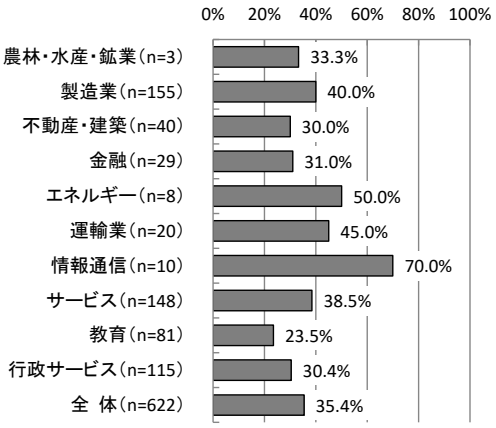
ウイルスチェック



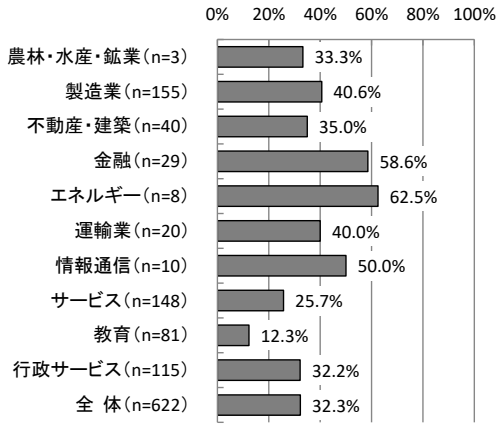
フィルタリング
（特定の条件を満たすメールの配信をしない）



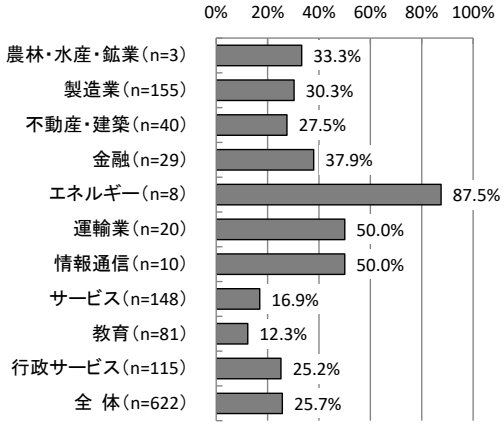
常に最新のパッチを適用



利用メールソフトの指定・制限



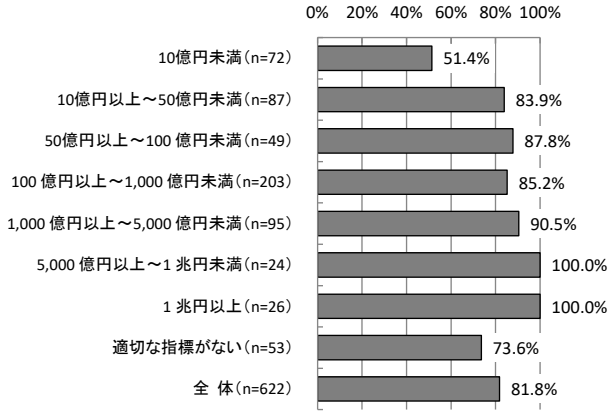
特定の拡張子を持つファイルが添付
されている場合に送・受信を拒否



【売上・予算規模別分析】売上・予算規模別にみると、すべての売上・予算規模で「ウイルスチェック」の実施率が最も高くなっている。

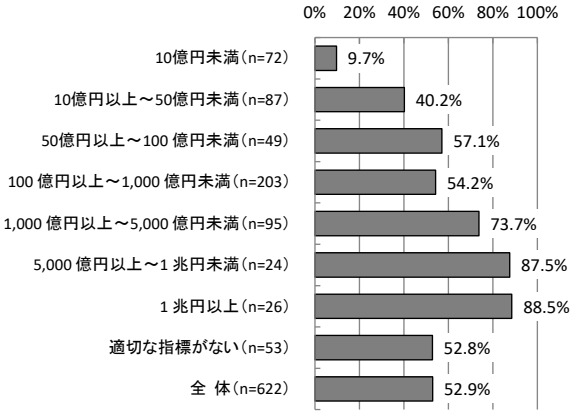
【売上・予算規模別分析】電子メールに関するセキュリティ対策

ウイルスチェック

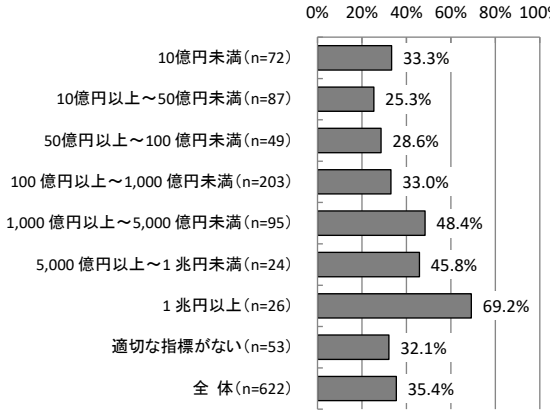


フィルタリング

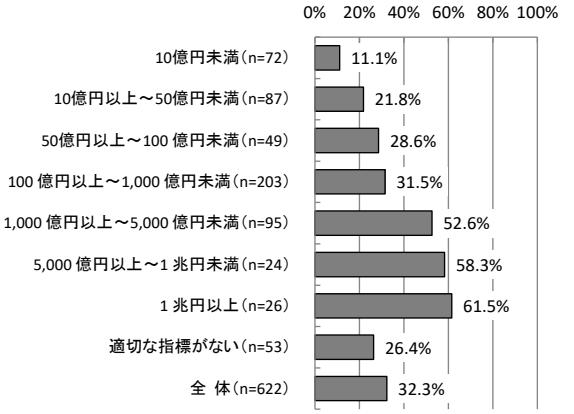
（特定の条件を満たすメールの配信をしない）



常に最新のパッチを適用

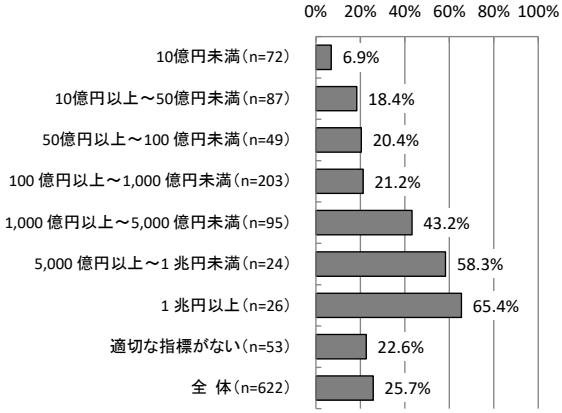


利用メールソフトの指定・制限



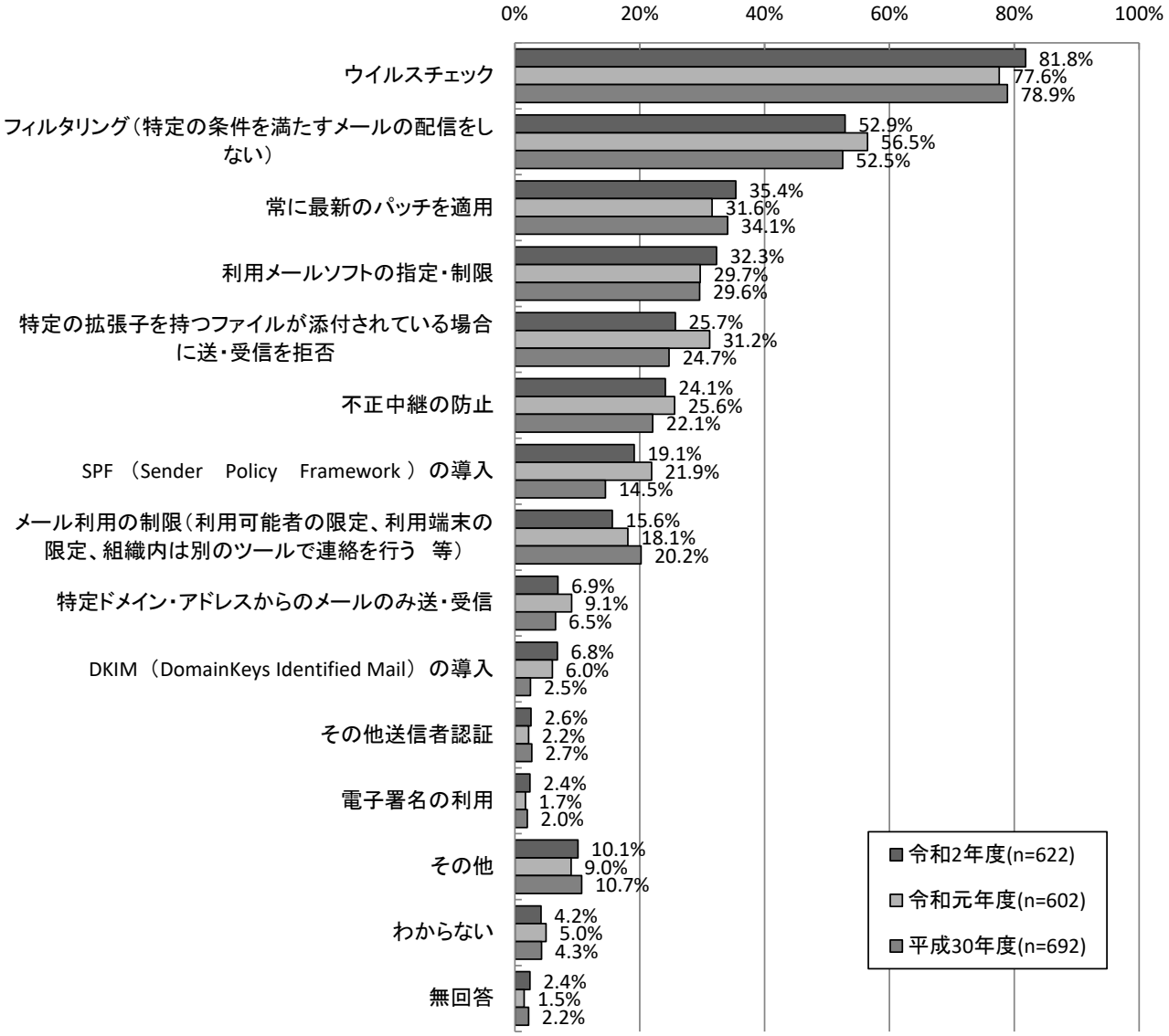
特定の拡張子を持つファイルが

添付されている場合に送・受信を拒否



【経年変化】昨年度と比較すると、「特定の拡張子を持つファイルが添付されている場合に送・受信を拒否」が5.5ポイント減少、「ウイルスチェック」が4.2ポイント増加している。

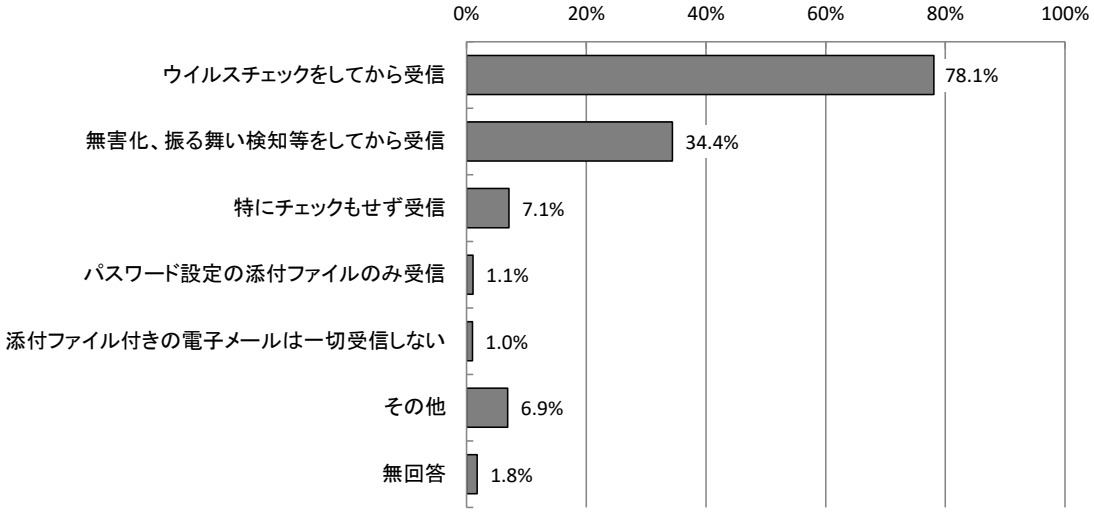
【経年変化】電子メールに関するセキュリティ対策



3.2.12　添付ファイルの取り扱い　【問37】

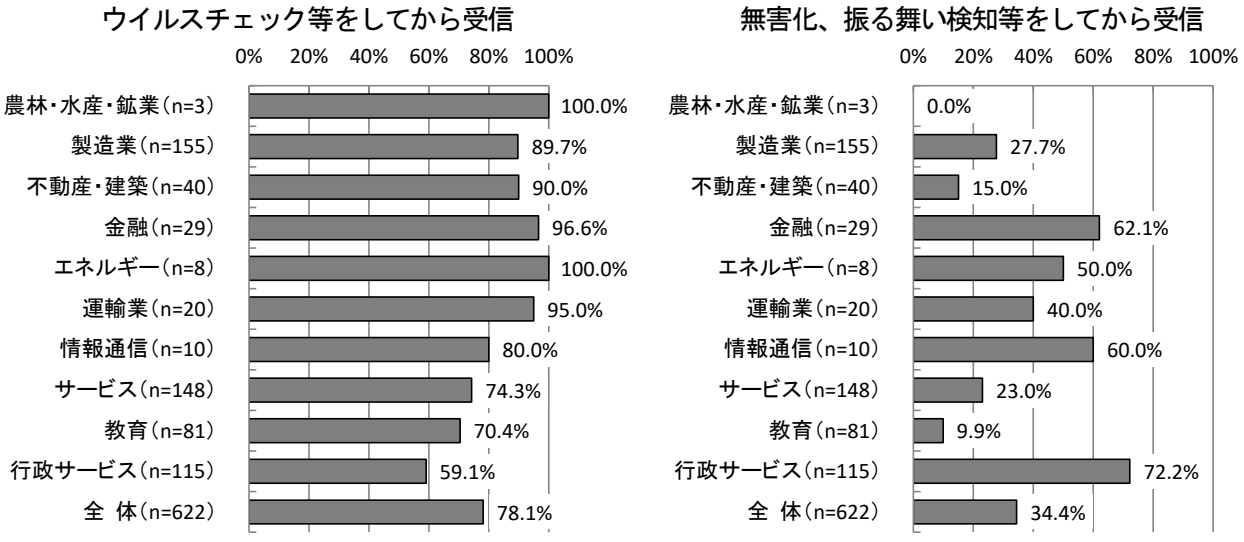
添付ファイルの取り扱いについては、「ウイルスチェックをしてから受信」が78.1%で最も多い。一方、「特にチェックもせずに受信」は7.1%であった。

【全体】添付ファイルの取り扱い（SA, n=622）

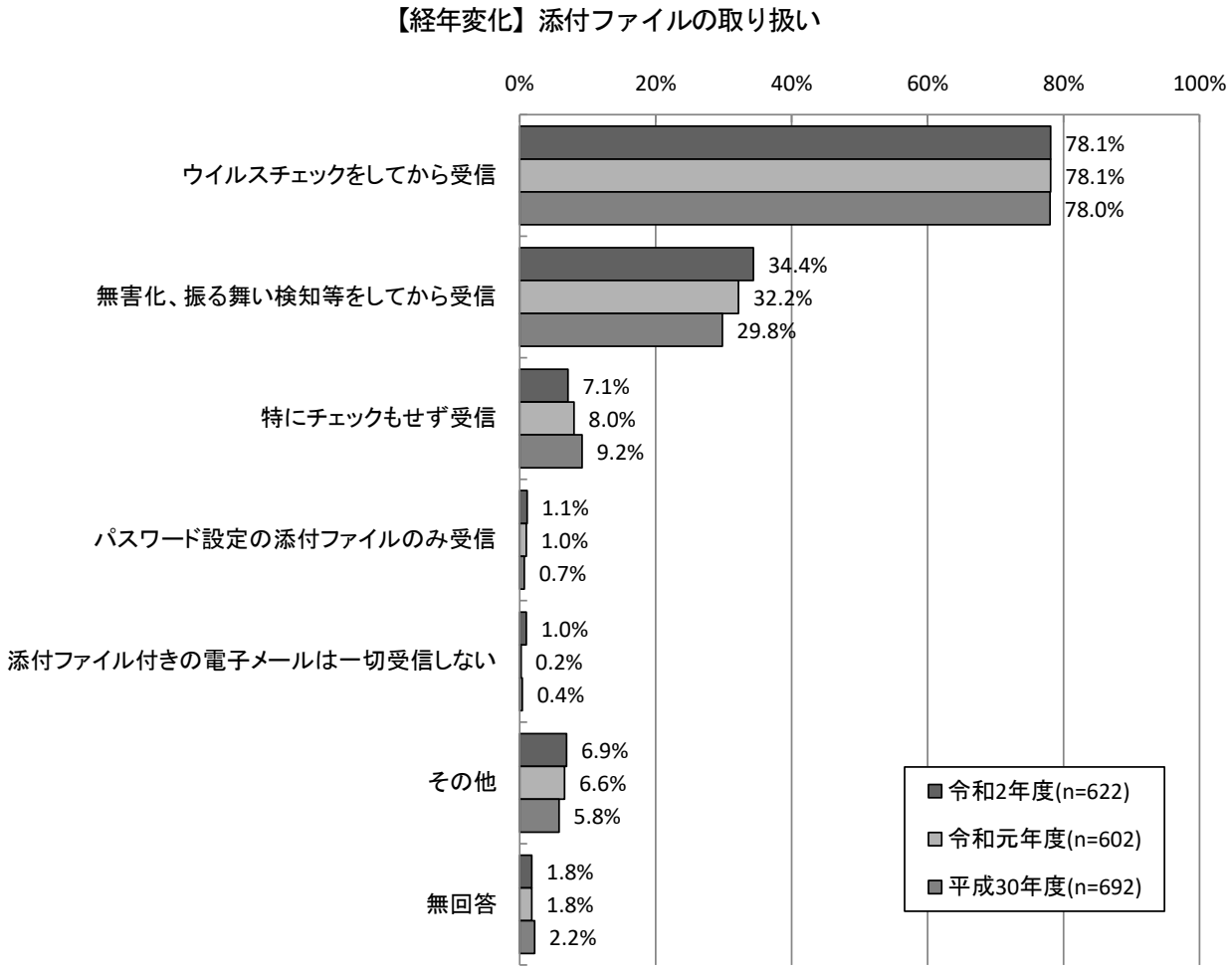


【業種別分析】業種別にみると、「ウイルスチェック等をしてから受信」は「エネルギー」で100.0%、「金融」で96.6%、「運輸業」で95.0%、「不動産・建築」で90.0%と、9割以上となっている。

【業種別分析】添付ファイルの取り扱い



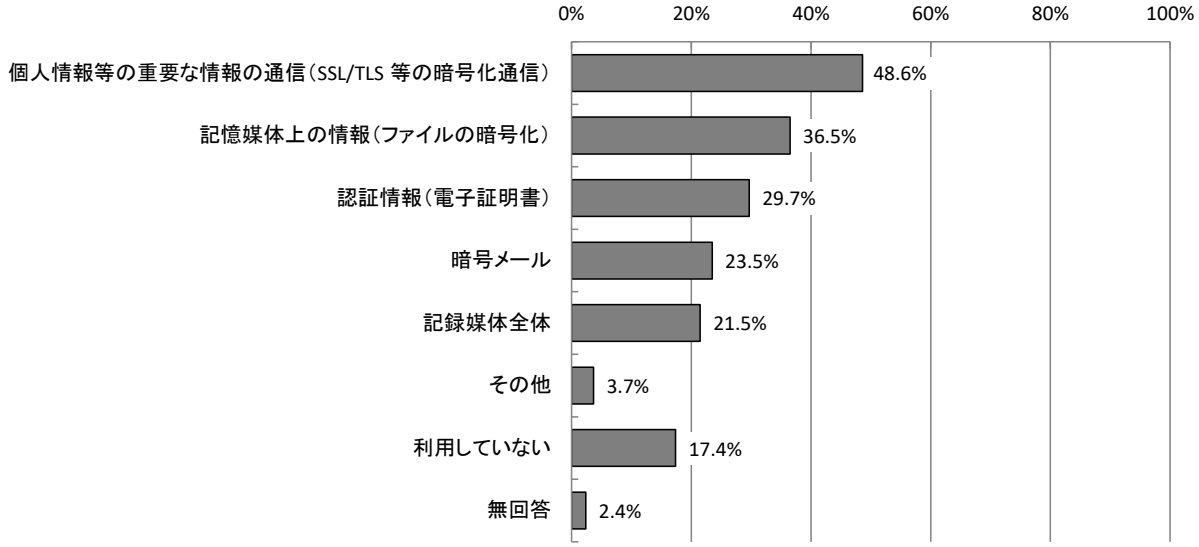
【経年変化】経年変化をみると、「無害化、振る舞い検知等ををしてから受信」が2.2ポイント増加し、「特にチェックもせず受信」が0.9ポイント減少している。



3.2.13　暗号化技術の用途　【問38】

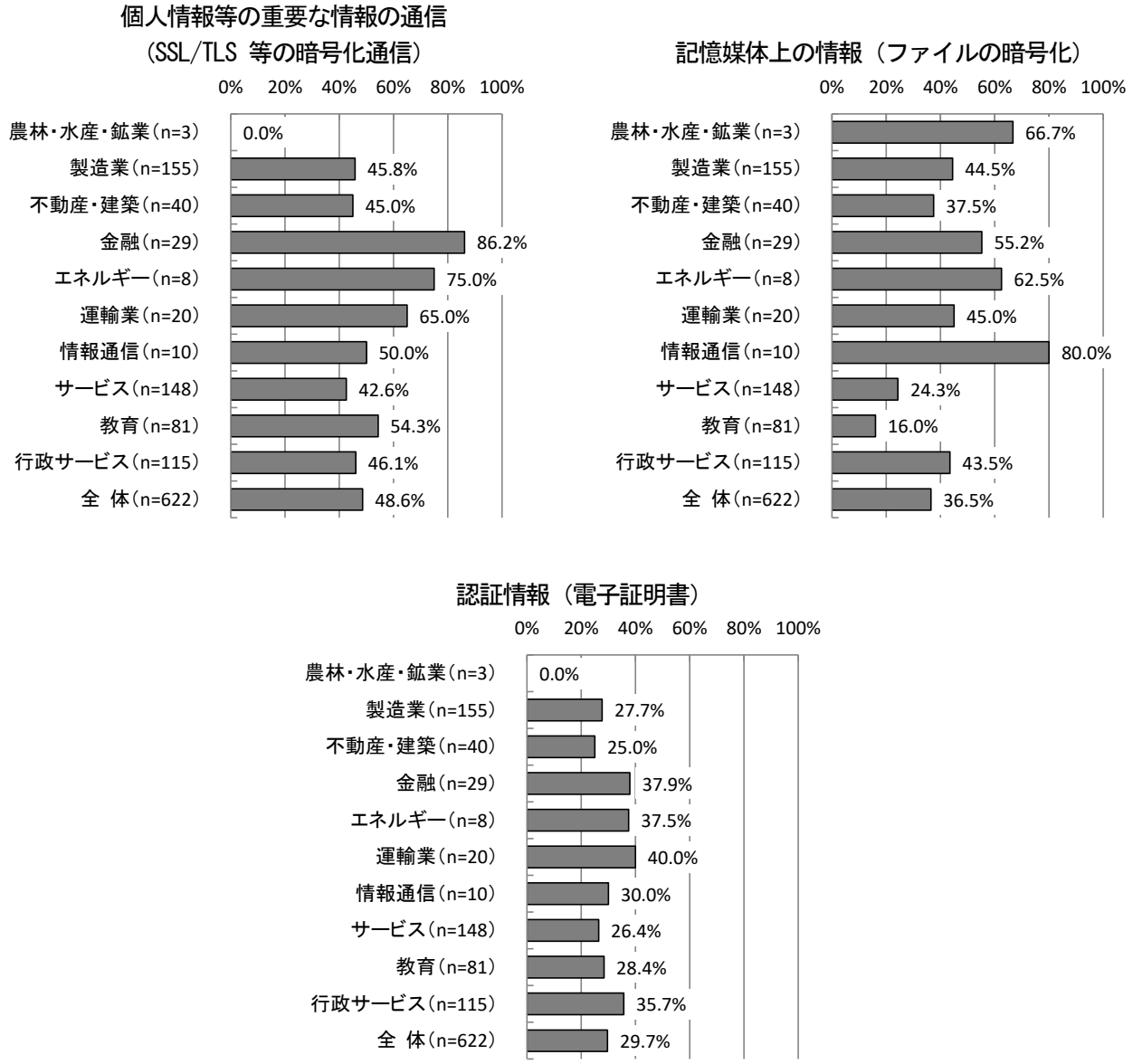
暗号化技術の用途については、「個人情報等の重要な情報の通信（SSL 等の暗号化通信）」が48.6%で最も多く、次いで「記憶媒体上の情報（ファイルの暗号化）」が36.5%、「認証情報（電子証明書）」が29.7%となっている。

【全体】暗号化技術の用途（MA, n=622）



【業種別分析】業種別にみると、「個人情報等の重要な情報の通信（SSL等の暗号化通信）」については、「金融」が86.2%で最も多く、次いで「エネルギー」が75.0%となっている。「記憶媒体上の情報（ファイルの暗号化）」については、「情報通信」が80.0%で最も多く、「認証情報（電子証明書）」については、「運輸業」が40.0%で最も多くなっている。

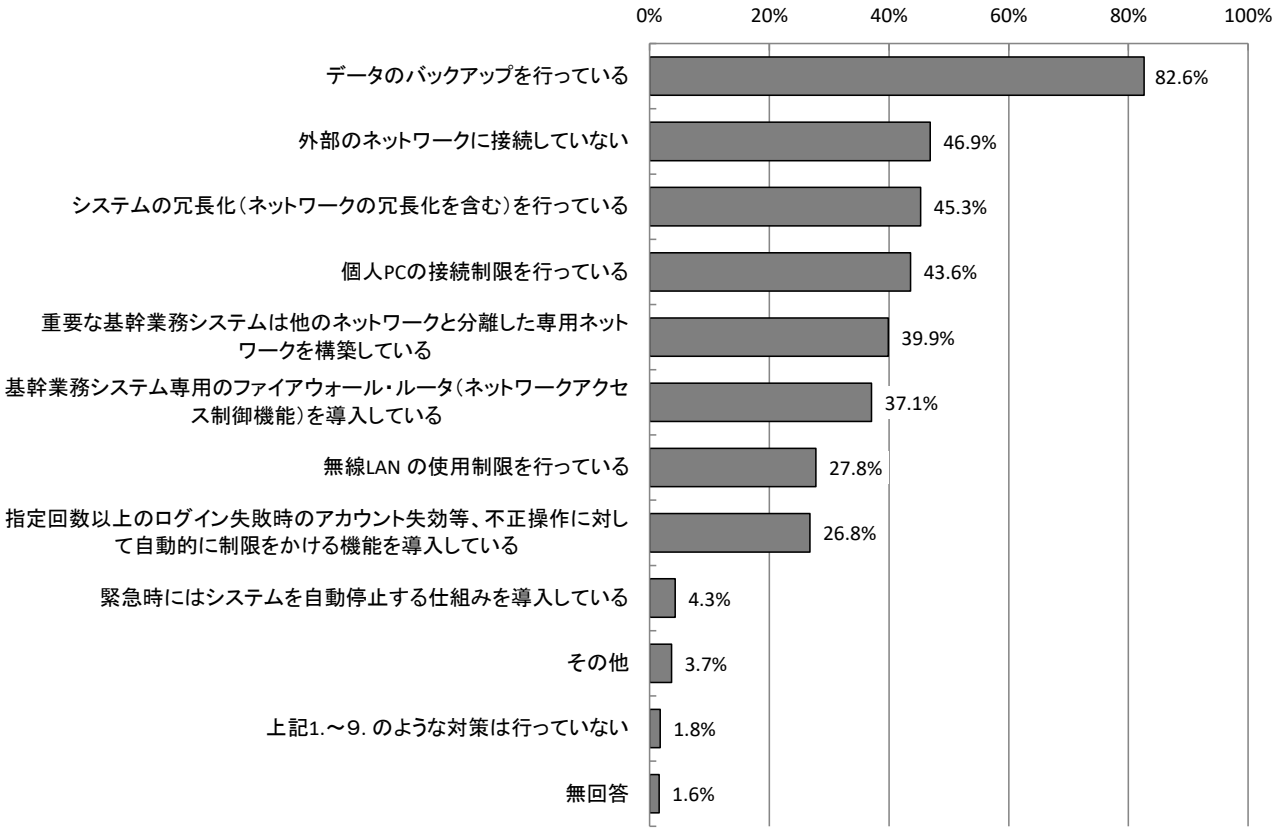
【業種別分析】暗号化技術の用途



3.2.14　重要システムの不正アクセス対策状況　【問39】

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82.6%で最も多く、「外部のネットワークに接続していない」が46.9%、「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45.3%で続いている。

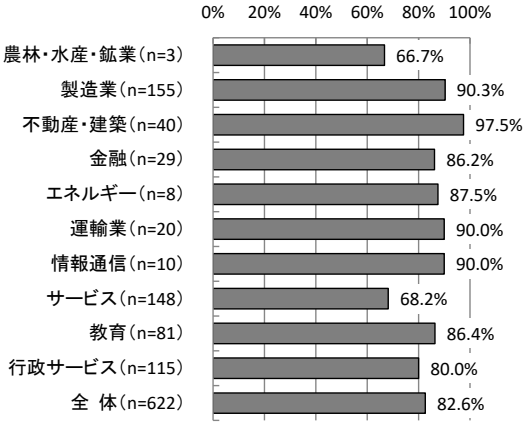
【全体】重要システムの不正アクセス対策状況（MA, n=622）



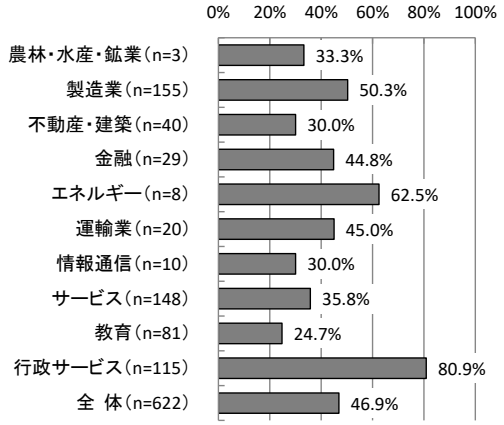
【業種別分析】業種別にみると、「データのバックアップを行っている」については、「不動産・建築」が97.5%で最も多く、次いで「製造業」が90.3%となっている。「外部のネットワークに接続していない」については、「行政サービス」が80.9%で最も多くなっている。

【業種別分析】重要システムの不正アクセス対策状況

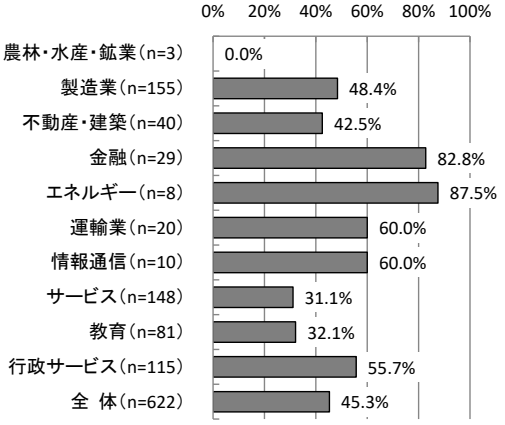
データのバックアップを行っている



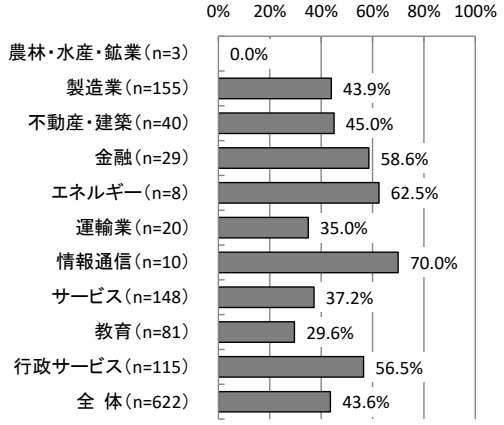
外部のネットワークに接続していない



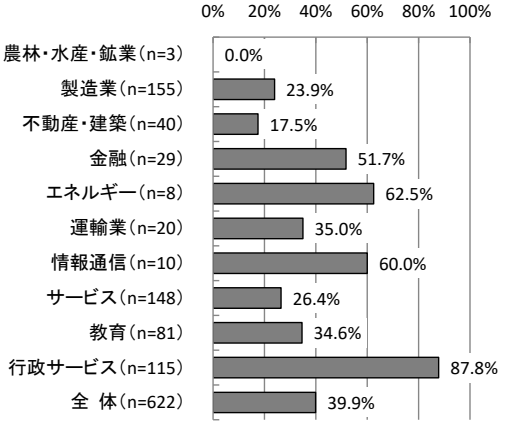
システムの冗長化
（ネットワークの冗長化を含む）を行っている



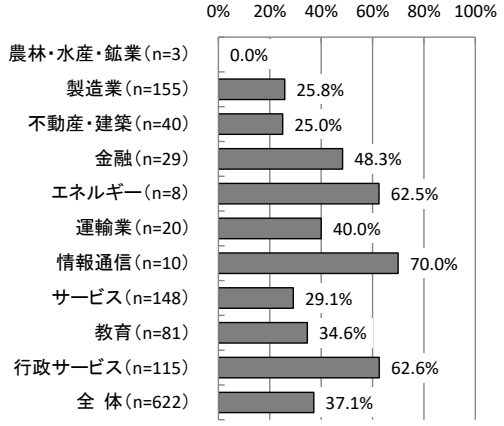
個人PCの接続制限を行っている



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

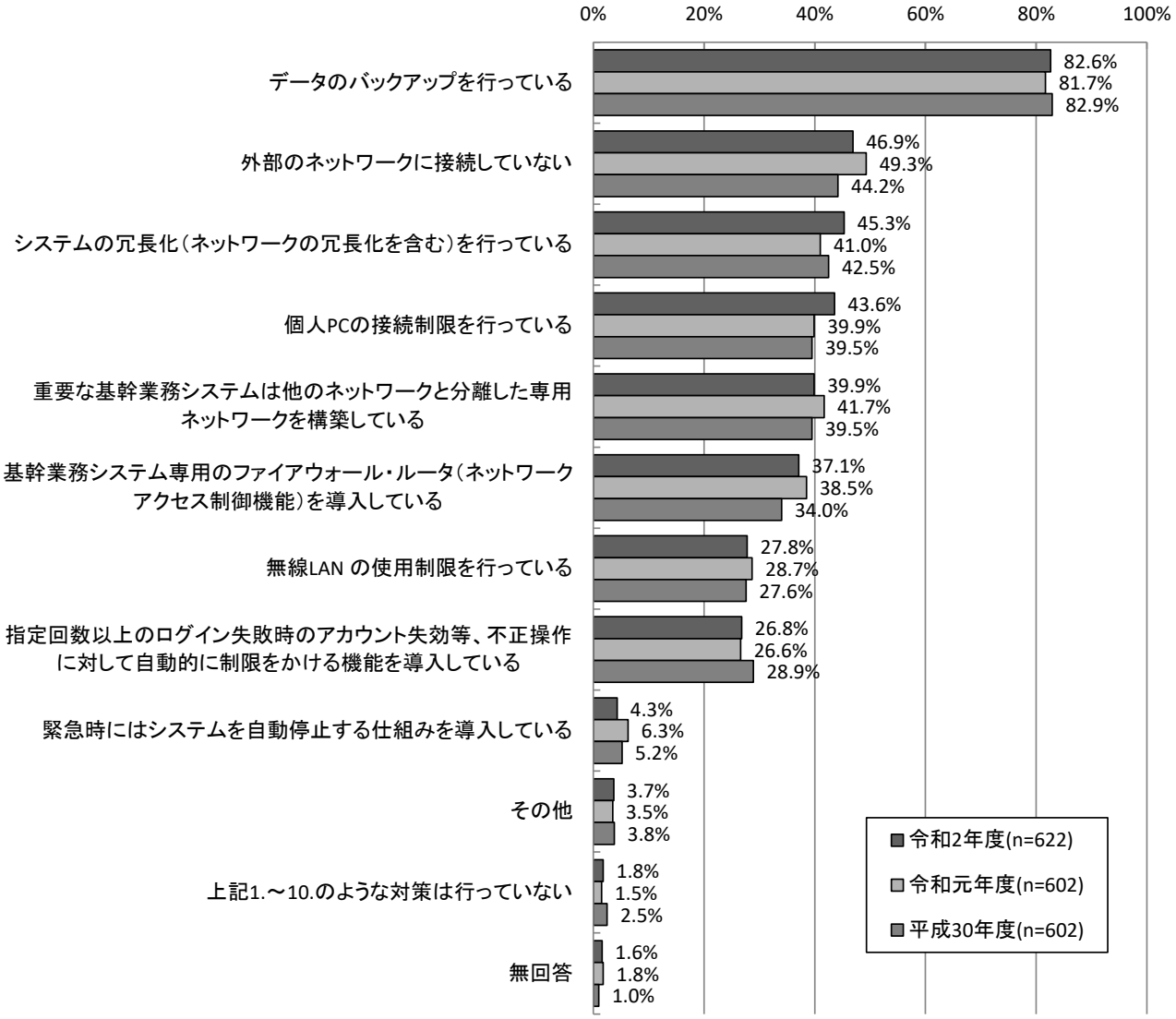


基幹業務システム専用のファイアウォール・ルーター
（ネットワークアクセス制御機能）を導入している



【経年変化】昨年度と比較すると、「特定の拡張子を持つファイルが添付されている場合に送・受信を拒否」が4.3ポイント、「個人PCの接続制限を行っている」が3.7ポイント増加している。

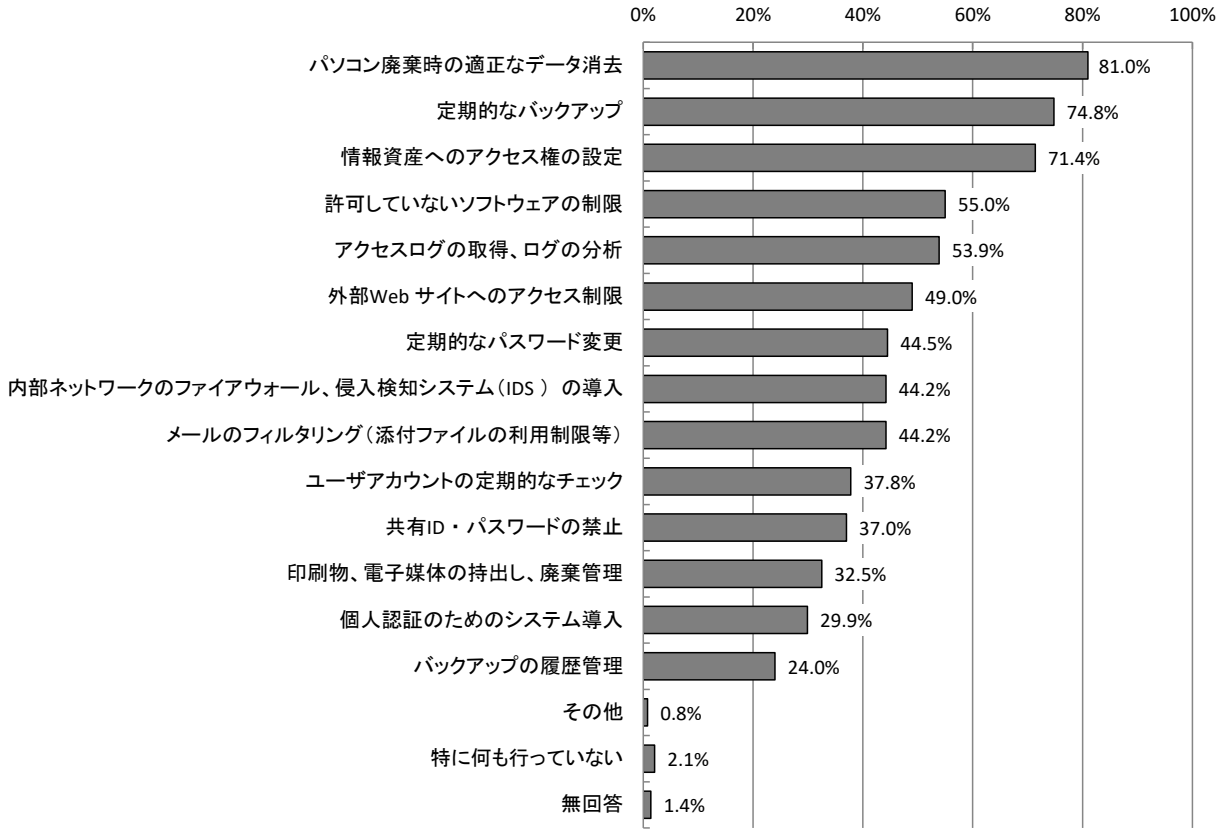
【経年変化】重要システムの不正アクセス対策状況



3.2.15　不正アクセス等への対策状況　【問40】

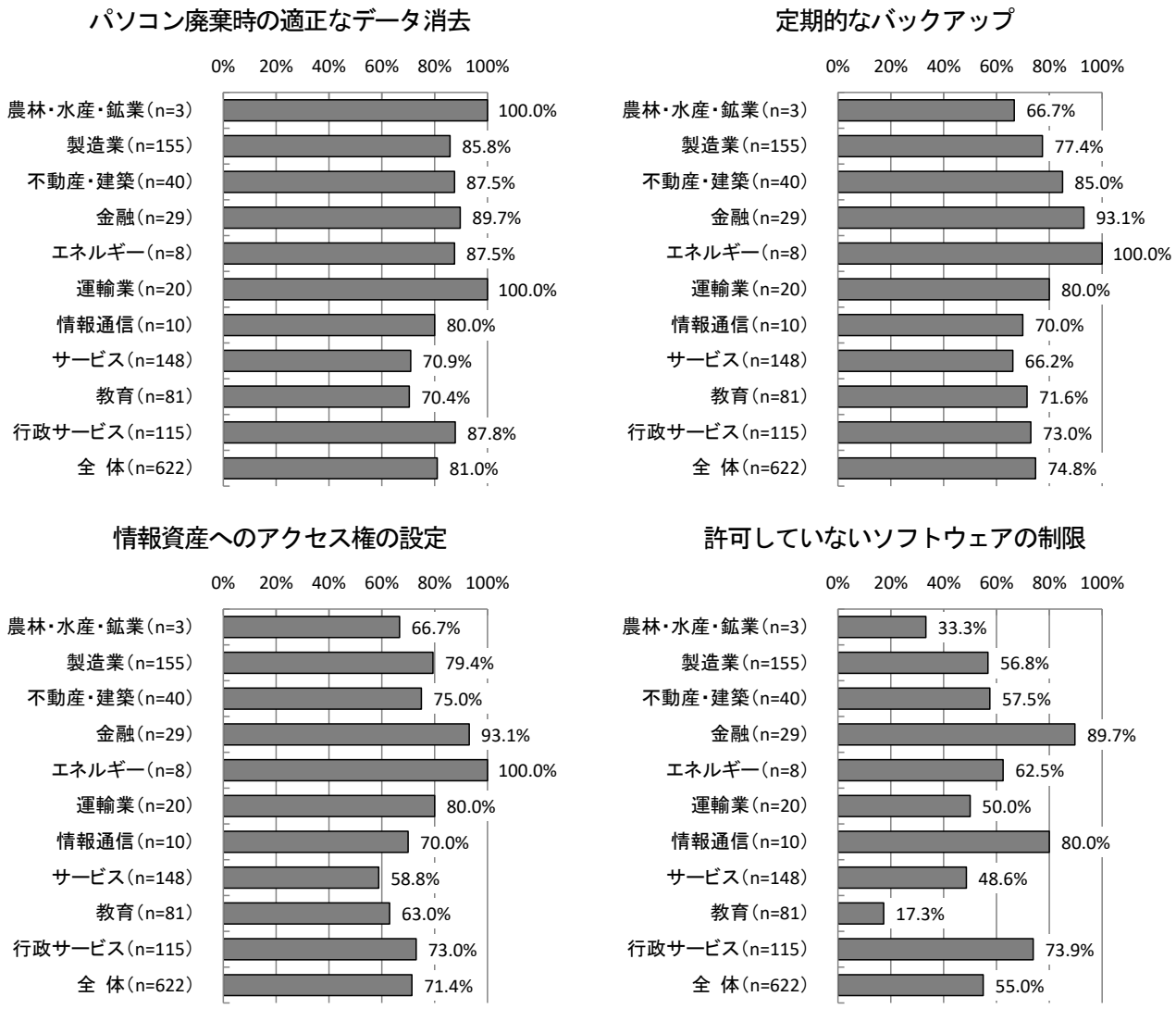
不正アクセス等への対策状況については、「パソコン廃棄時の適正なデータ消去」が81.0%で最も多く、次いで「定期的なバックアップ」が74.8%、「情報資産へのアクセス権の設定」が71.4%となっている。

【全体】不正アクセス等への対策状況（MA,n=622）



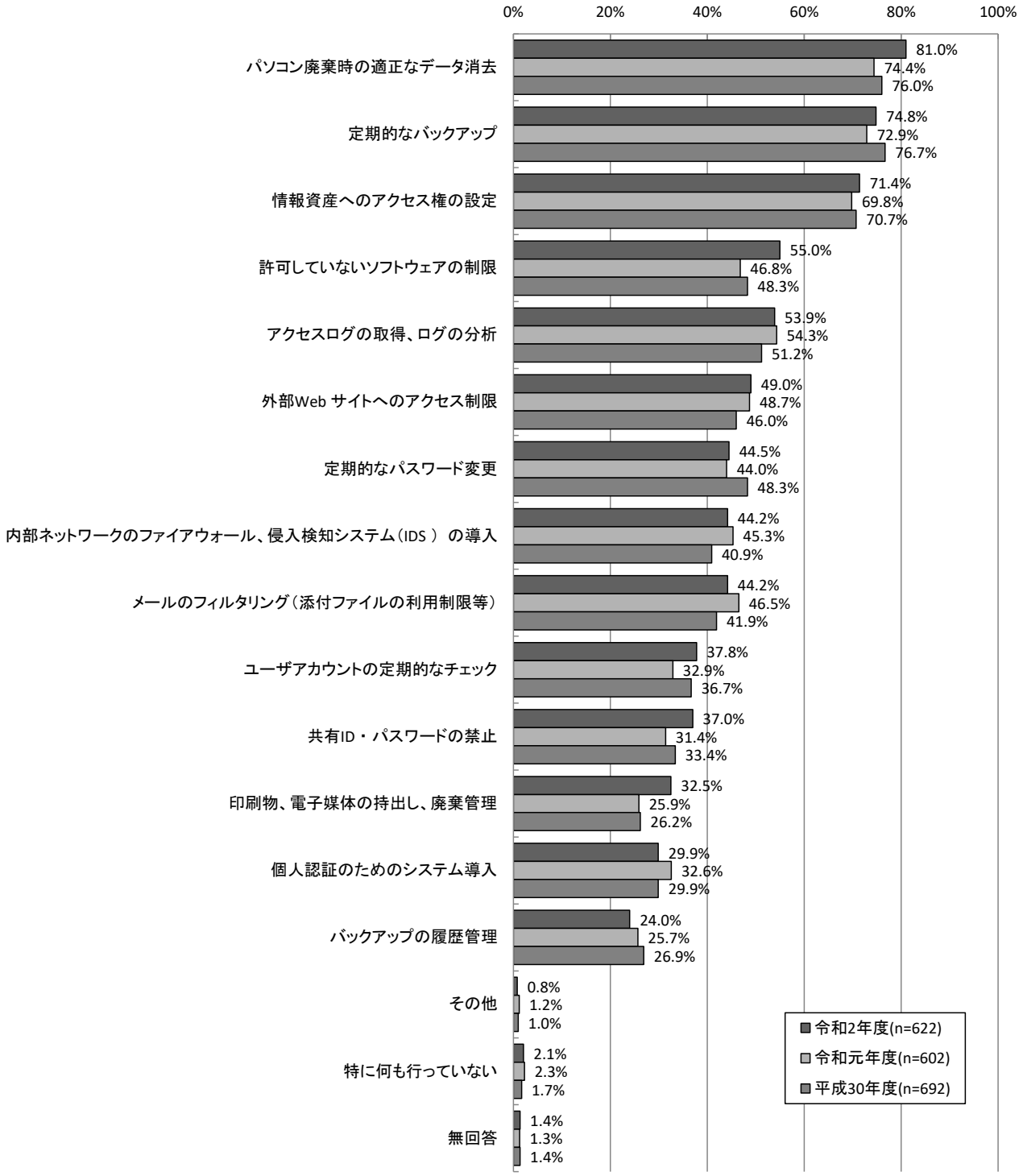
【業種別分析】業種別にみると、「パソコン廃棄時の適正なデータの消去」については、「運輸業」が100.0%で最も多く、次いで「金融」が89.7%、「行政サービス」が87.8%となっている。「定期的なバックアップ」及び「情報資産へのアクセス権の設定」については、「エネルギー」がともに100.0%で最も多く、「許可していないソフトウェアの制」については、「金融」が89.7%で最も多くなっている。

【業種別分析】不正アクセス等への対策状況



【経年変化】昨年度と比較すると、ほとんどの対策項目で増加となっており、「許可していないソフトウェアの制限」が 8.2 ポイント、「パソコン廃棄時の適正なデータ消去」「印刷物、電子媒体の持出し、廃棄管理」がそれぞれ 6.6 ポイント増加している。

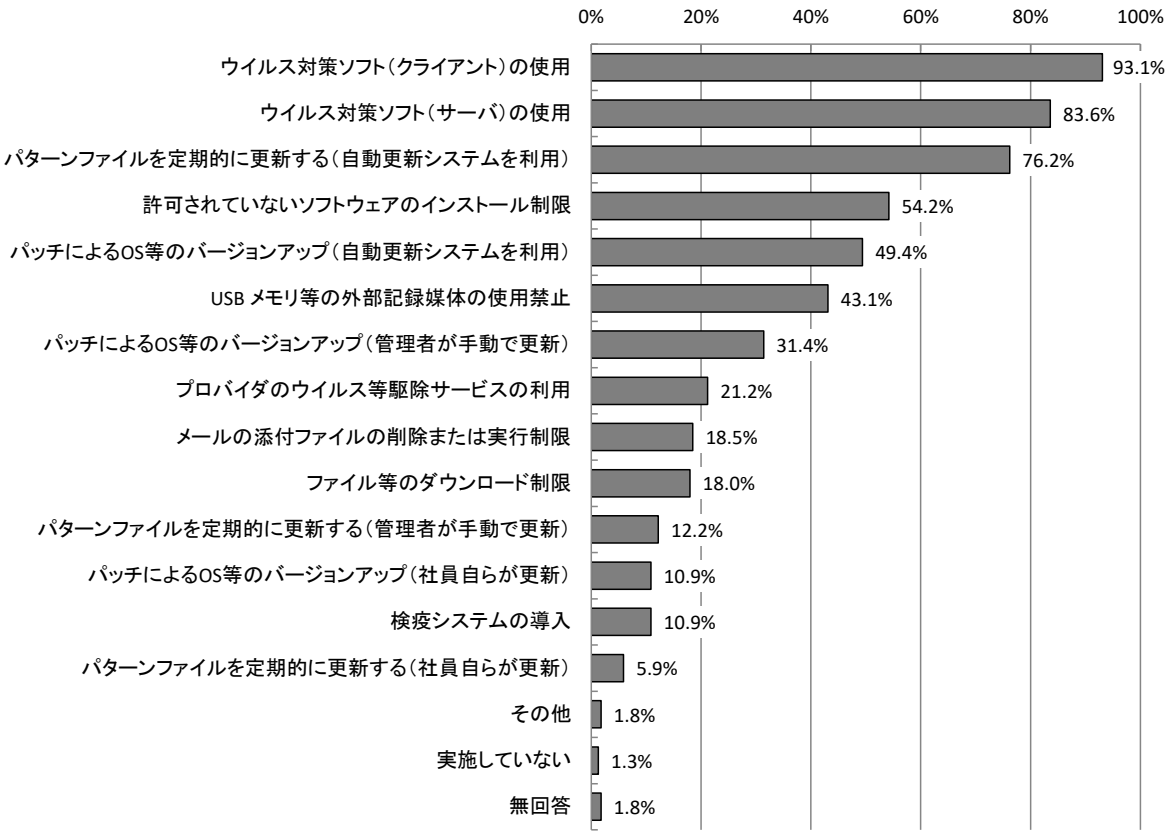
【経年変化】不正アクセス等への対策状況



3.2.16　不正プログラムへの対策状況　【問41】

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93.1%で最も多く、次いで「ウイルス対策ソフト（サーバ）の使用」が83.6%、「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76.2%となっている。

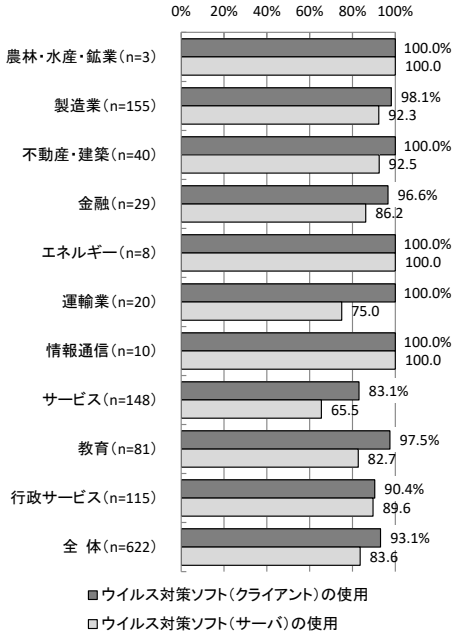
【全体】不正プログラムへの対策状況（MA, n=622）



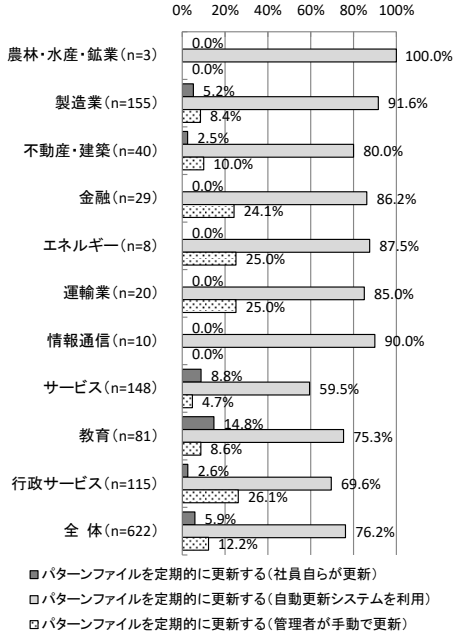
【業種別分析】業種別にみると、「ウイルス対策ソフトの使用」については、「サービス」以外の業種でそれぞれの項目で7割を超えている。また、「パターンファイルの定期的な更新」については、「製造業」「不動産・建築」「金融」「エネルギー」「運輸業」「情報通信」で「パターンファイルを定期的に更新する（自動更新システムを利用）」が8割を超えている。

【業種別分析】不正プログラムへの対策状況

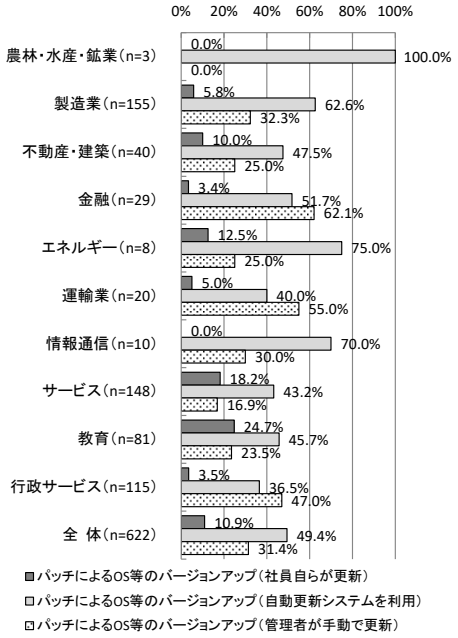
ウイルス対策ソフトの使用



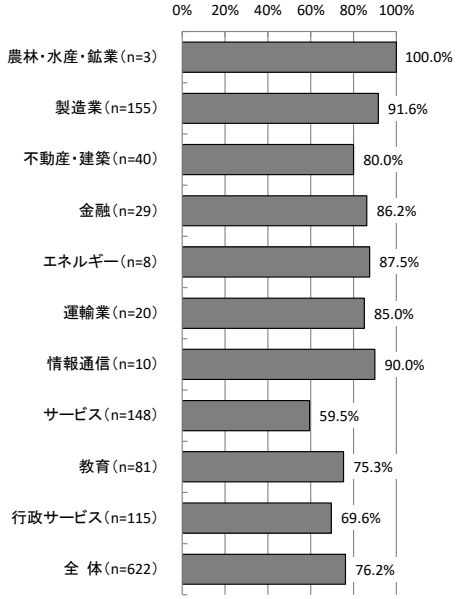
パターンファイルの定期的な更新



パッチによるOS等のバージョンアップ



許可されていないソフトウェアのインストール制限

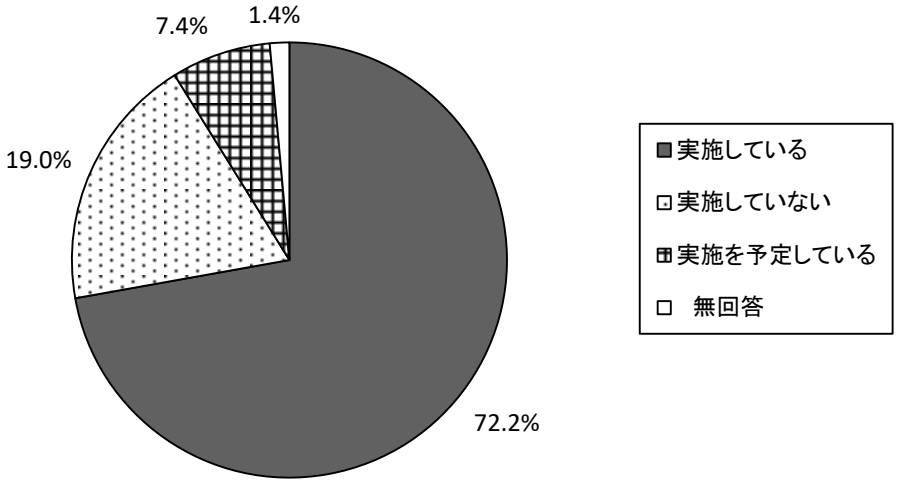


3.3　人的対策

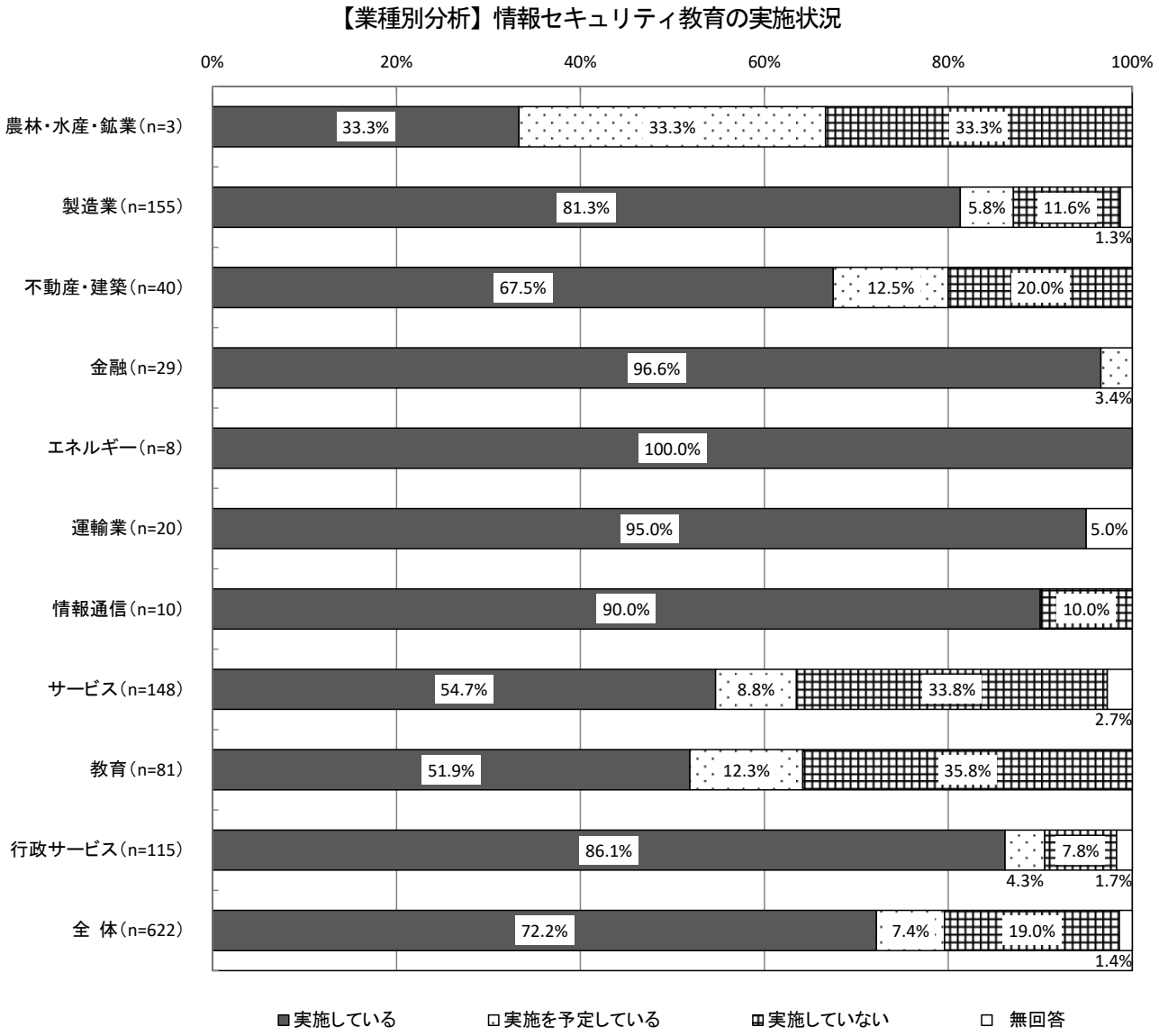
3.3.1　情報セキュリティ教育の実施状況　【問42】

情報セキュリティ教育の実施状況については、「実施している」が72.2%、「実施していない」が19.0%、「実施を予定している」が7.4%、となっている。

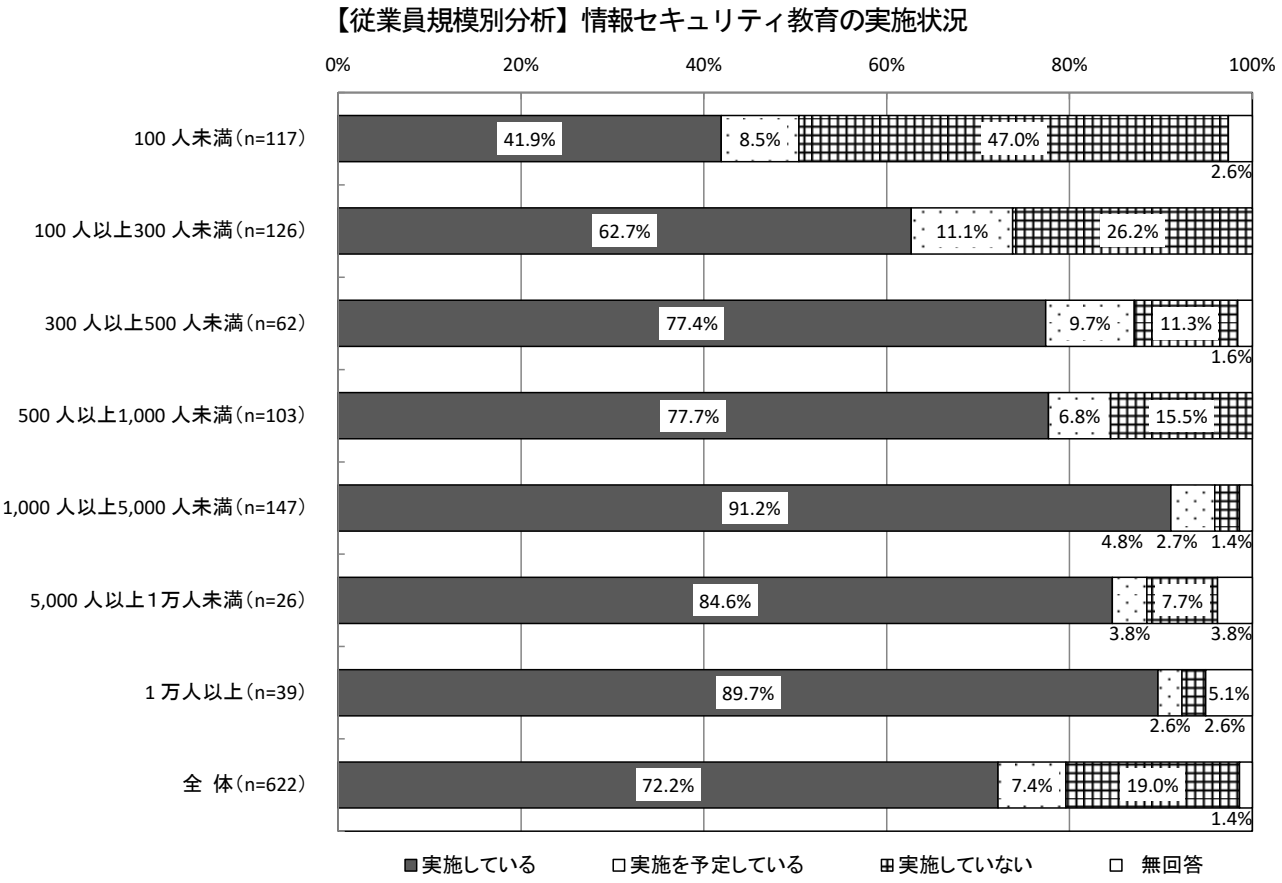
【全体】情報セキュリティ教育の実施状況（SA,n=622）



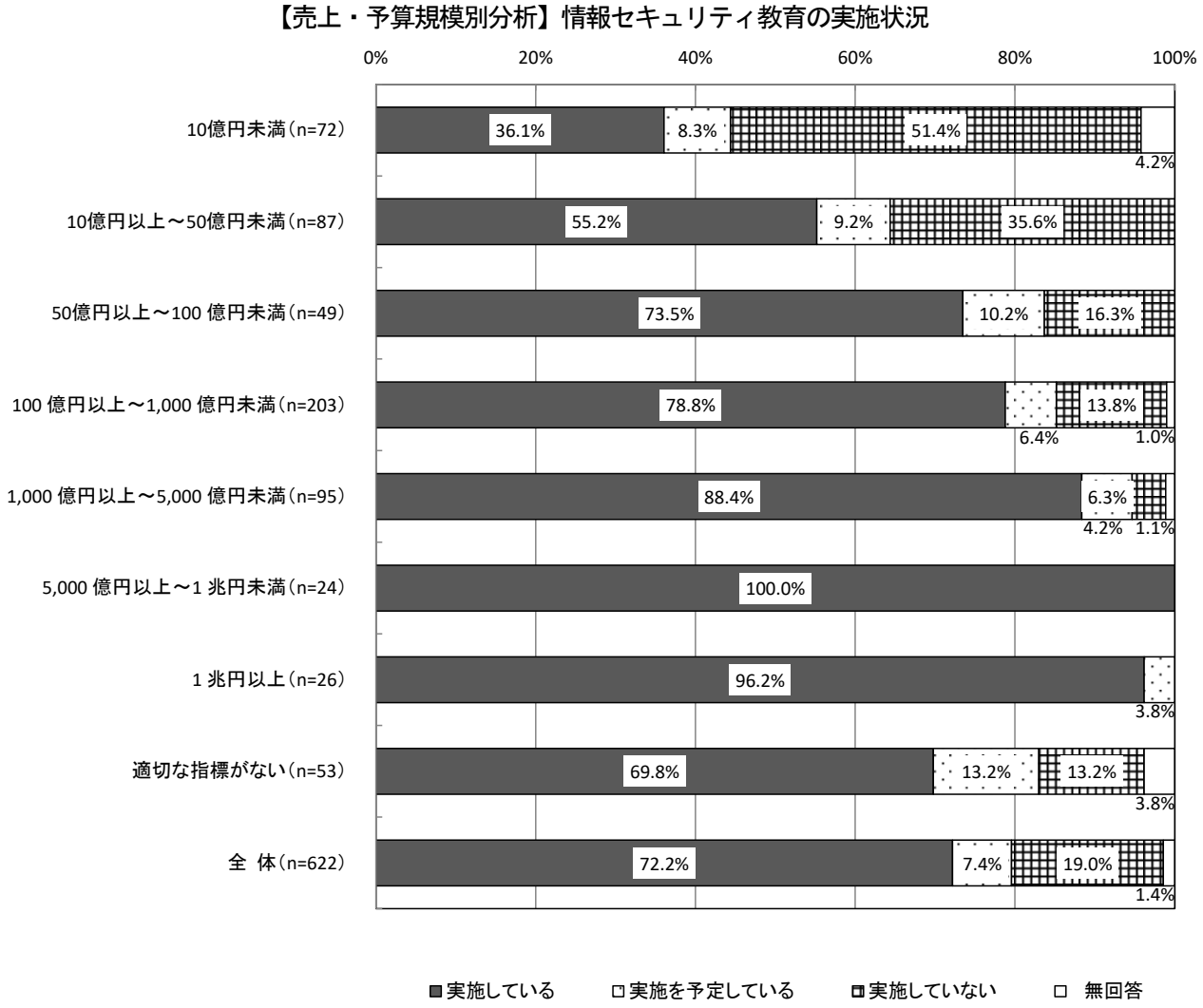
【業種別分析】業種別にみると、「実施している」については、「エネルギー」が100.0%で最も多く、次いで「金融」が96.6%となっている。一方、「実施していない」は「教育」で35.8%となっている。



【従業員規模別分析】従業員規模別にみると、「実施している」については、概ね従業員規模が大きくなるにつれて多くなる傾向にあり、「1,000 人以上5,000 人未満」で91.2%となっている。



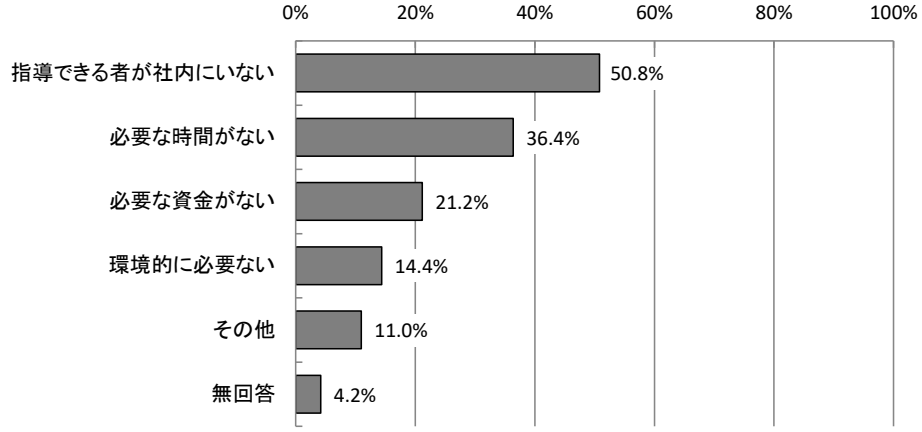
【売上・予算規模別分析】売上・予算規模別にみると、「実施している」については、概ね売上・予算規模が大きくなるにつれて多くなり、「5,000億円以上～1兆円未満」では100.0%となっている。



3.3.2 情報セキュリティ教育を実施しない理由 【問43】

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50.8%で最も多く、次いで「必要な時間がない」が36.4%、「必要な資金がない」が21.2%となっている。

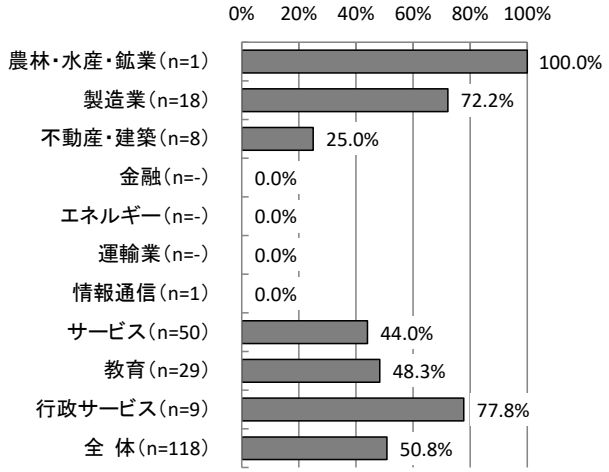
【全体】情報セキュリティ教育を実施しない理由 (MA, n=118)



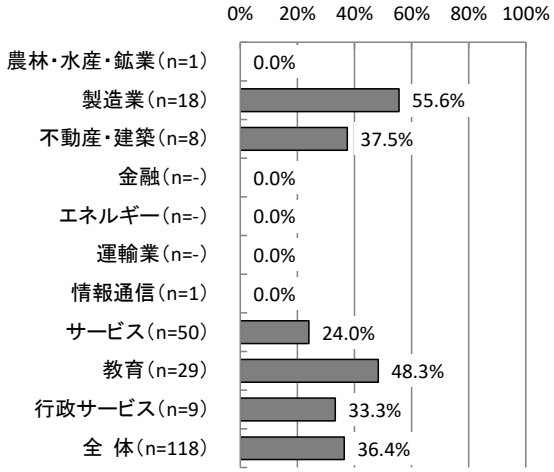
【業種別分析】業種別にみると、「指導できる者が社内にいない」については、「行政サービス」が77.8%で最も多くなっている。

【業種別分析】情報セキュリティ教育を実施しない理由

指導できる者が社内にいない



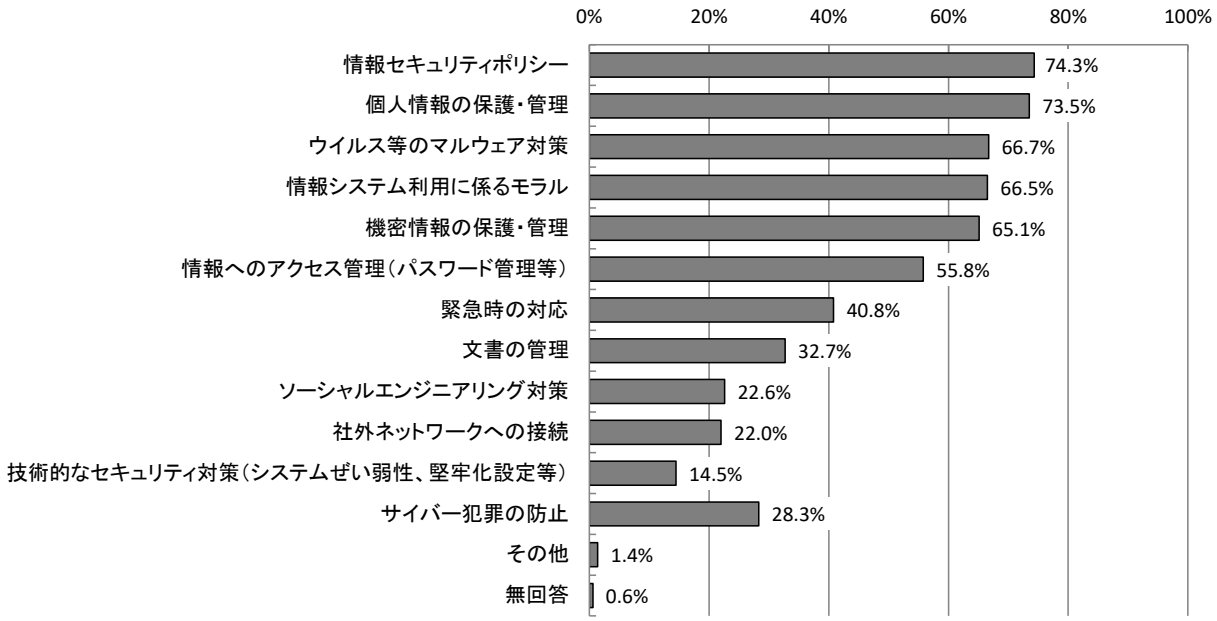
必要な時間がない



3.3.3 情報セキュリティ教育の内容 【問44】

情報セキュリティ教育の内容については、「情報セキュリティポリシー」が74.3%で最も多く、次いで「個人情報の保護・管理」が73.5%、「情報システム利用に係るモラル」が66.7%となっている。

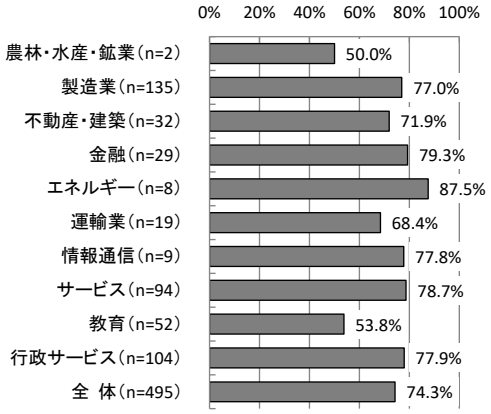
【全体】情報セキュリティ教育の実施内容（MA, n=495）



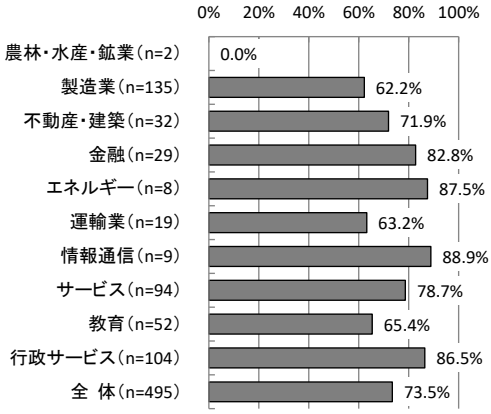
【業種別分析】業種別にみると、「情報セキュリティポリシー」については、「エネルギー」が87.5%で最も多く、次いで「金融」が79.3%となっている。「個人情報の保護・管理」については、「情報通信」が88.9%で最も多く、次いで「エネルギー」が87.5%となっている。

【業種別分析】情報セキュリティ教育の実施内容

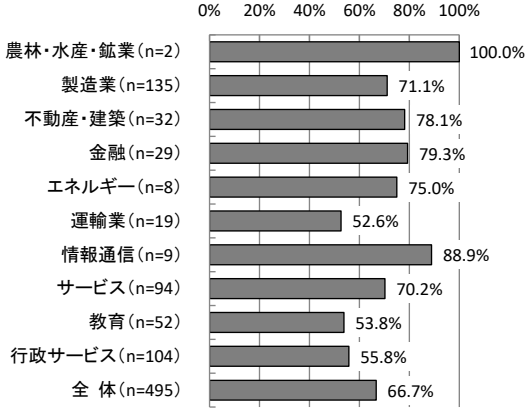
情報セキュリティポリシー



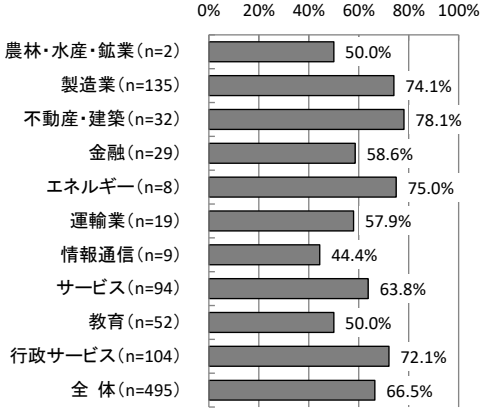
個人情報の保護・管理



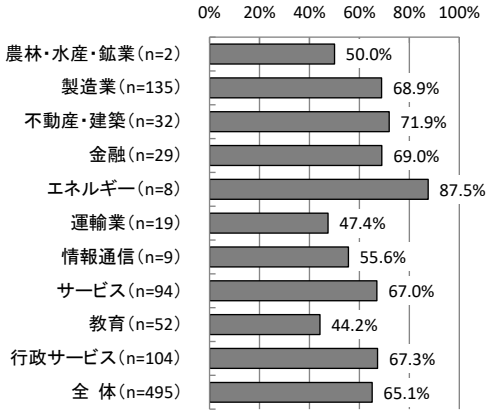
ウイルス等のマルウェア対策



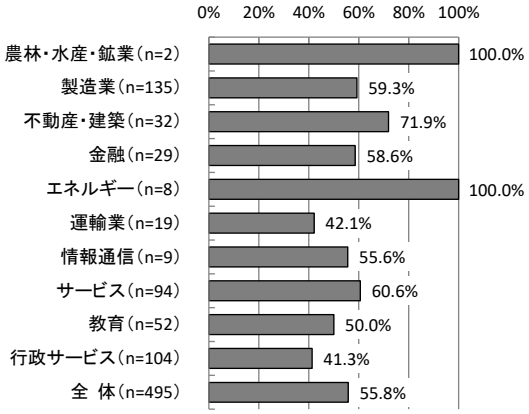
情報システム利用に係るモラル



機密情報の保護・管理



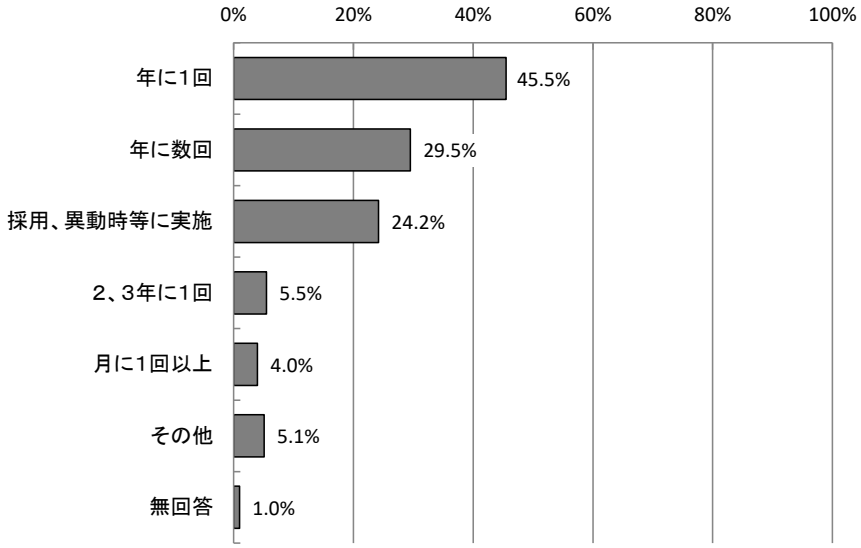
情報へのアクセス管理（パスワード管理等）



3.3.4　情報セキュリティ教育の頻度　【問45】

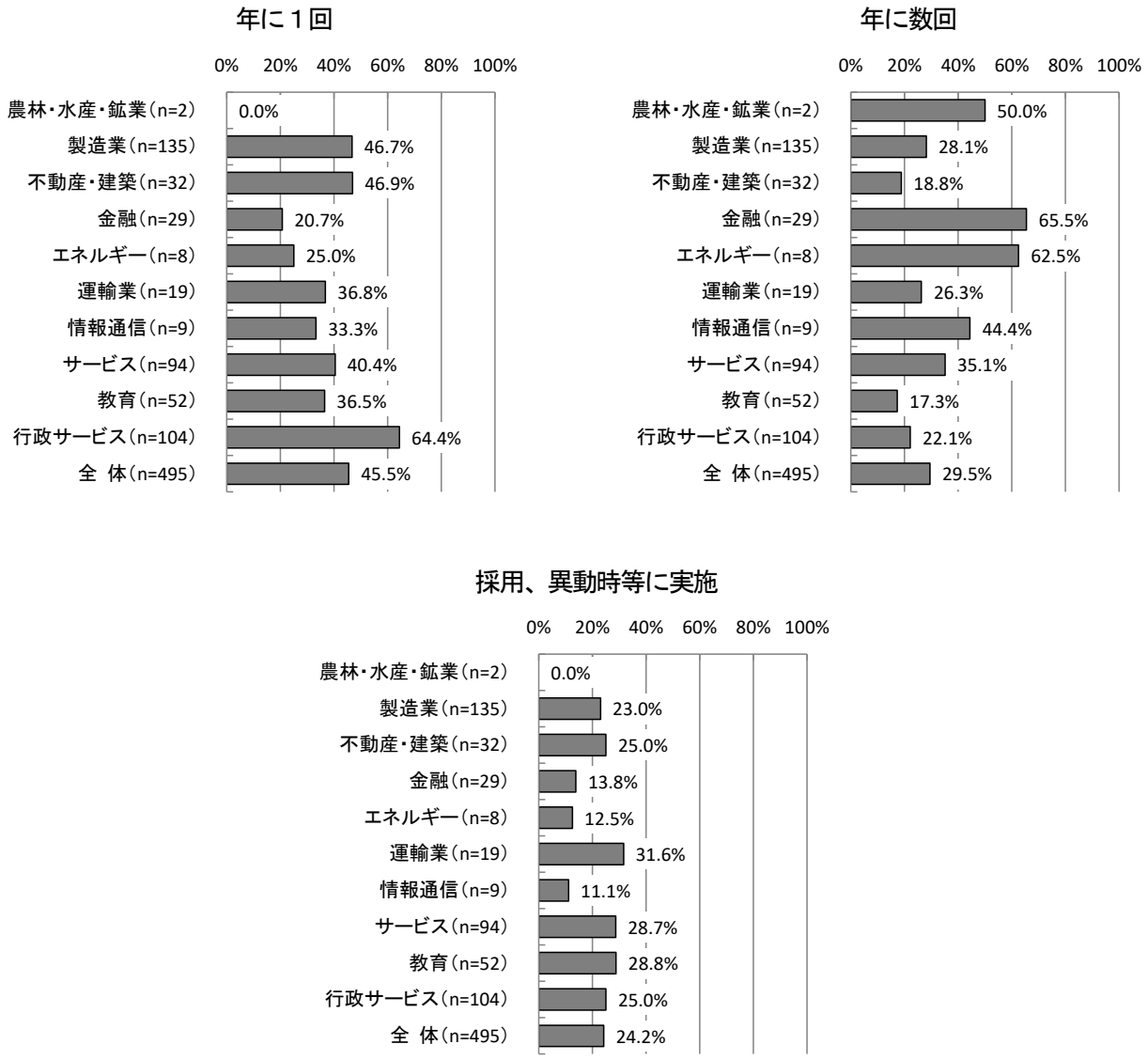
情報セキュリティ教育の頻度については、「年に１回」が45.5%で最も多く、次いで「年に数回」が29.5%、「採用、異動時等に実施」が24.2%となっている。

【全体】情報セキュリティ教育の実施頻度（MA, n=495）



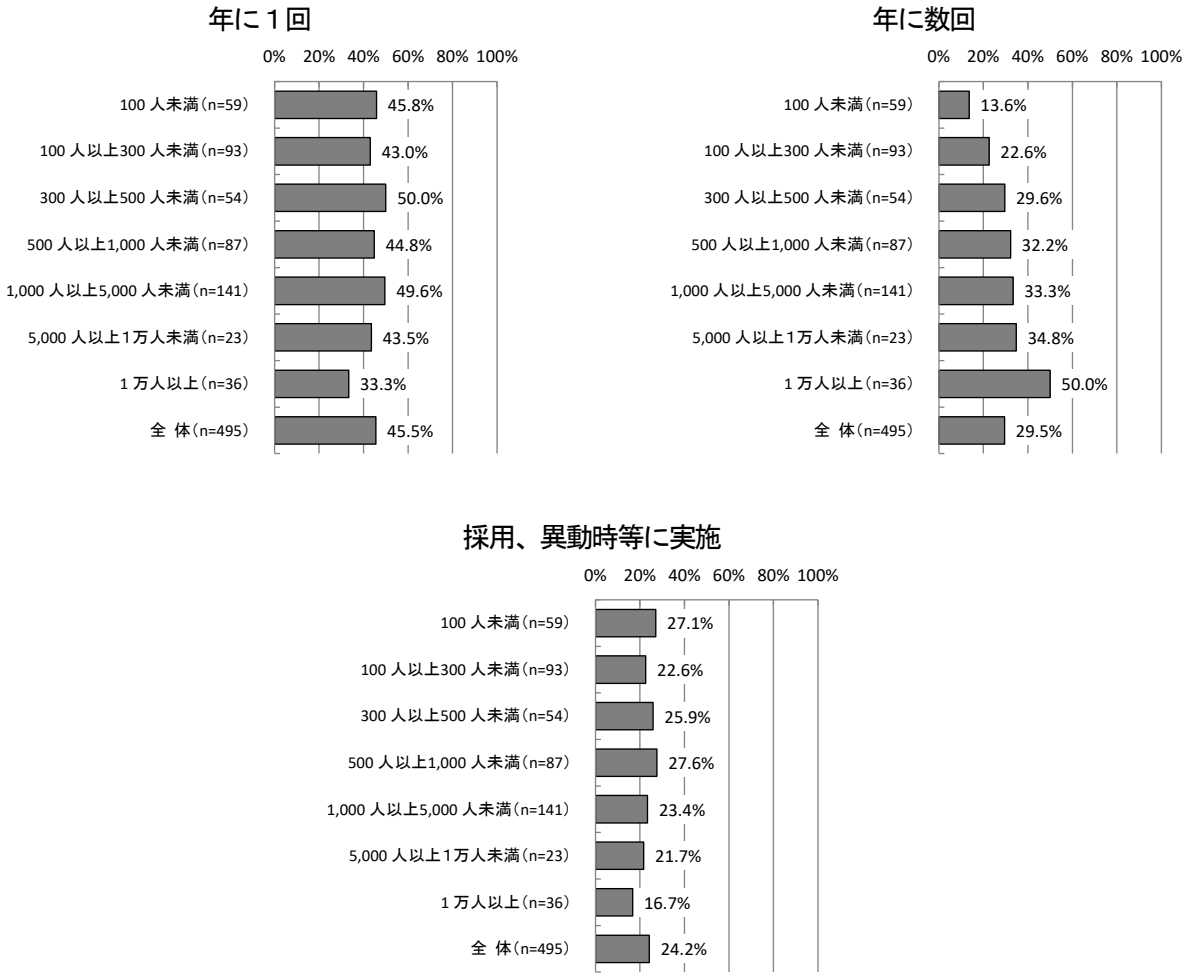
【業種別分析】業種別にみると、「年に1回」については、「行政サービス」が64.4%で最も多く、「年に数回」については、「金融」が65.5%となっている。「採用、異動時等に実施」については、「運輸業」が31.6%となっている。

【業種別分析】情報セキュリティ教育の実施頻度



【従業員規模別分析】従業員規模別にみると、「年に1回」については「300人以上500人未満」が50.0%、「年に数回」については、「1万人以上」が50.0%が最も多くなっている。

【従業員規模別分析】情報セキュリティ教育の実施頻度



3.3.5　セキュリティ対策の問題点や不安等

１．組織的対策

●どこまで行うべきか限られた予算では、対応に苦慮する。
●経営者の理解が得にくい
●ｉＴリテラシー向上による効率化とセキュリティ教育が不十分である認識はあるが、時間と費用を捻出しないのが現状。社内お知らせで定期に提示する程度が現状である。
●当診療所はレセプト請求以外で外部ネットワークに接続する必然性がほとんどないのだが、ゼロではないため　そこにコストをかける必要性が生じる。小さな事業所では何かと困難に思う。
●費用をかければセキュリティの強化はされるが、その有用性についてなかなか上層部の理解を得られない。
●リスクと、対策への費用対効果のレビューなど、必要だが、その工数をあてる人員の確保が難しい。（網羅する範囲が広い為）
●情報セキュリティ対策の為の予算が取得しにくい。
●レセプトコンピューターのみでインターネット環境にまだないため対策は今のところしてない。
●セキュリティについては際限がないので、どこまで実施すべきなのか分からない。従って投資判断が難しい
●費用対効果を表しずらく経営層への説明が困難
●どこまで行っていけば良いのか、上限がない内容のため、いつも不安です。大学ですので、個人の情報を保有しており、ねらわれてしまえば、まず間違いなく、もれてしまいます。セキュリティ投資についても、上層部は、理解していますが、提案するこちらも、どこまでが、最適なのか、いつも難しいです。１人情シスなので、とにかくクラウドに預けてしまい、何か起きたときは、あやまるように考えています。
●セキュリティ対策を強化すると業務効率が低下するリスクがあり、バランスが難しい。
●セキュリティ対策に割ける人員が少ない。運用すべきシステムは増加するが全体をまとめて管理できる仕組みがない
●・人材不足
●・予防対策としてシステム導入したいが、その有用性・費用対効果からの必要性の説明が難しく、社内予算の確保が難しい。　・人的及び技術的リソースの確保が難しい。
●情報セキュリティ対策は、費用対効果の説明が難しいため、経営層の理解を得るのが非常に難しい。また全構成員に関わる事項であり、業務方法・文書管理・就業規則等にも関連するが、経営判断を得られず全く進まずにいる。
所轄官庁等から、より具体的な基準や、認証評価の標準項目とするなどしないかぎり、組織としえ動かないと考えられる。〃
●ICTリテラシーの格差。組織内で築かれた文化等障害が多く、理解を得るのが難しい。コストの問題。短期間で費用対効果がでにくく、可視化し難い為、優先度が低くなりがち
●セキュリティ部門・セキュリティ関連費用を圧縮したい。・セキュリティ専任部署の人員が、非常に不足し、募集しても適切な人員が採用できない。・日本人は、不審メール開封への警戒心が薄く、教育だけでは意識向上は難しい。
●明らかに不正なアカウント取得を狙っているとしか思えないメールが毎日大量に届き、メールチェックが苦痛です。
●具体的な対策をどうしたらよいのかわらない。また経営層に費用をかけてでも実施しなければいけないと理解してもらうためにはどうすればよいのか教えてほしい。

２．技術的対策

●Ｅｍｏｔｅｔのようなユーザーに判断が困難なマルウエアに対しては、複数セキュリティシール組合わせで、システム側にも対応するしかない。しかしながら現状、いたちごっこであるため、コストが際限なく膨張してしまう。
●常に新しい攻撃への対応。どこまで対策すればよいか分からない。
●本町では、総務省が求める「三層の構え」を実施している為インターネットを介した不正アクセスは不可能と考えている。
●ソフトしか入っておらず、容易にウイルス感染して情報流出する危険がある。・ウイルス感染？フィッシングにより、メールアカウントが乗っとられた場合、乗っとられたことに気付かないまま長期間メールを監視されビジネスメール詐欺やウイルス発信源として使われてしまう。
●グループ関連会社や取引先等についても今後、セキュリティ強化に取り組んでいきたいと考えている。
●サーバやｗｅｂは、対応可能である。またＤＤＯＳ等の攻撃も汰応している。メールに添付しているファイルの対応はできていない。対策が大げさになり、高額なソフトが多い。

３．人的対策

●社員のレベルに応じた教育
●内部利用者の情報流出に対し、規定や、教育で抑止させておく必要がある。操作ミスは、コントロールできるが、悪意ある行動を未然にどう防ぐか。
●情報処理安全確保支援士の雇用を義務付けて欲しい。
●人事異動で情報分野に関する知識が蓄積されていない。
●・情報システム、情報セキュリティの知識に長けている者が数名しか居ない。・管理者が専任ではないため、システムを

導入しても、内容確認など、本当のセキュリティ運用ができていない。・経営側が、専任者を必要と考えていない。（考えてくれない）。

●従業員の業務に支障が出ないようにしつつ、安全性を担保することの難しさを感じます。パッチ適用についても、端末台数が多くなるほど徹底させることが難しいと感じます。

●情報セキュリティを守る事は、もはや、一般常識だと思うが、意識が低い人への対応。

●セキュリティ担当者の不足

●専従の社員がいないため、マンパワー不足を感じている。また、テレワークの普及に伴うセキュリティの在り方に不安がある。

●人員が足りない。

●ＩＴ部門とユーザー部門との意識情報リテラシーのギャップ、理解不足。

●教育や研修を行っても情報セキュリティへの意識がなかなか根付かない。

●職員等への教育・運用の徹底が難しいとかんじています。

●対策をどこまでやるべきかの判断、社員の情報セキュリティ意識の浸透が難しいと感じている

●セキュリティに対しての認識が薄い。

●経理者および従業員の理解を得るのが難しい

●セキュリティポリシーの策定をしてもパートアルバイトが多い業種のため、全ての従業員に徹底するのが難しいと感じています

●ICT利用者のリテラシー向上に苦慮している。社内教育や訓練だけでは限界があり、懲戒など社内規則の利用を結びつけないが反対意見もそれなりにある。

●ＩＴリテラシーのレベルが人によってバラつきがある。投資の効果が測りにくい

●・情報セキュリティ教育について、職員のパソコンスキルに差があるためアンケートを取ると、簡単に言う職員と難しいという職員がいる。

・本アンケートに関して、病院の場合、基幹システムである医療情報システムネットワーク（閉域）と情報系ネットワーク（インターネット接続環境）があり、対策方法が違うため、どちらについて答えてよいか悩ましい。

・コストがかかるが、情報セキュリティ対策は保険のようなものであり、予算時に必要性を説明してもなかなか理解が得られない。

●社員一人一人のITリテラシーの向上をいかに実現するかが最大の課題。

４．その他

●専門家でないとわからない内容が多かった。専門用語がわからない

●言葉の定義にあいまいさを感じた。

●専門用語が多く、設問の理解が困難。

●不正アクセス行為対策等については、区の単位ではなく市全体として実施しているため、問４以降回答できません。

●勝手に会社名を名乗られて、人材募集をＳＮＳ等で詐欺に使われている事例があり、困っている。

●当院ではインターネット環境がないため、今後の参考にさせて頂きます。

●マイクロソフト社の提唱を受け、パスワードの定期変更を停止しました。情報セキュリティの観点から、方向性が分かりません。

●日々新しい不正アクセス等の手口が出て来ており、一企業で全てに対策を取り対応していくことが困難になって来ている。名だたる大企業が被害にあっている現状を見せつけられるとどうして良いか分からなくなっている。

●３．人的対策は情シスメンバーに対してなのか、一般社員に対してなのかわかりません。今回は情シスメンバー対象ということで回答致しました。

●紙ベースではなくＥｘｃｅｌやＷｅｂで回答できるようにしてもらいたい

●海外拠点、サプライチェーンのセキュリティ対策の実施が困難。

●脅威情報が不足している。基本はネットのニュース等をチェックして該当すると思われるものに対して対策を講じるしかない状態。勿論、刑事事件になれば警察が対応してくれると思うし、社会的に影響の大きい事象になれば、ＮＩＳＣもＪＰＣＥＲＴも対応してくれると思うが、それは、何かが起きてからのこと。何かが起こる前に、脅威情報を共有する仕組みを作って欲しい。

●サイバーセキュリティは経営上の大きなリスクの１つであるとの認識でここ数年で投資額も増加させています。その一方で攻撃が高度化の一途をたどっているため個社での対策は難しくなっています。官民一体となっての取組みが、今後増々重要になってくると考えています。

●内容が一部門だけでは判断できない多岐の項目であるため各部署に問い合わせていて時間がかかり遅れてしまいました

申しわけありません
●Webを利用したアンケートだと手間がかからず楽だと思います。
●問26の二番めの設問に関して、当社の考えは「100%の防御[protect]は不可能であるとの認識の元、予防的対策である早期検知[detect]と事後的対応である迅速な対応[response]と復旧[recovery]に注力すべきである」というものとなる。そのため必ずしも予防的対応と事後的対応とどちらを重視するかという二択にはそぐわないが、右側の“リスクの検知”は、リスクの特定のことを述べられていると理解し、検知・対応・復旧という攻撃発生時から発生後の要素は左側に記載されていると理解した上で、左寄りに○をつけた。
●企業経営における情報セキュリティの重要性は年々高まっていると考えます。特に近年増加している犯罪者集団との闘いについては、一企業での対応が難しいため、警察関係者のご尽力には大変感謝しております。
●アンケートの回答方法において、数字の横に□と☑の方法での回答様式に変更可能でしょうか?
●困難に感じてることは、ホームページ等へのアクセスが急増した場合、それが攻撃なのかを判断の困難性である。また、電話よりメールでのコミュニケーションが増えていく中で、メールは便利である一方で、大きなトラブルをうむ要素であることの意識付けを高める必要性を感じている。
●一般従業員向けに法令遵守のための最低限の基礎に絞った情報セキュリティに関するｅ－Ｌｅａｒｎｉｎｇがあれば利用を検討したい。”法令でこう定められているので、こういうことをやってはいけない／やらないといけない”といった具合に、法令と具体的な取り組みの対応が分かるものが良い。さらに、不正アクセス禁止法、個人情報保護法、マイナンバー法、サイバーセキュリティ基本法等の諸法令の関係性が概観で良いのでわかるのもがあるとなお良い。なお、無料か格安のものが望ましいが、今のところ無料のものはきわめて少なく、適切なものは見つかっていない。
●セキュリティ対策はどこまでやってもキリが

不正アクセス行為対策等の実態調査　付録資料

付録１：調査票
付録２：集計表

付録１

１．組織的対策

【貴社・団体についてお伺いします】

問１．　貴社・団体は、どの業種に該当しますか。（○は一つ）

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

（太枠線内にご回答ください）

問２．　貴社・団体の従業員は、どのくらい在籍されていますか。（○は一つ）

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

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

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

【情報システム等の環境について伺います】

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

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

問４－１．　昨今の新型コロナウィルス感染拡大防止策等により、テレワーク業務が急激に普及しているが、テレワーク業務を行う際の端末装置（パソコン）の利用環境はどのようになっていますか。（○は一つ）

１．貴社・団体支給の端末装置のみ利用
２．個人所有端末装置のみ利用
３．貴社・団体支給及び個人所有端末装置のどちらでも利用可能
４．端末装置を利用しない
５．テレワークを行っていない
６．現在検討中である

問５．　貴社・団体支給の端末装置（タブレット、スマートフォン等）の整備環境は、どのようになっていますか。（○は一つ）

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

問５－１．　昨今の新型コロナウィルス感染拡大防止策等により、テレワーク業務が急激に普及しているが、テレワーク業務を行う際の端末装置（タブレット、スマートフォン等）の利用環境はどのようになっていますか。（○は一つ）

１．貴社・団体支給の端末装置のみ利用
２．個人所有端末装置のみ利用
３．貴社・団体支給及び個人所有端末装置のどちらでも利用可能
４．端末装置を利用しない
５．テレワークを行っていない
６．現在検討中である

問６．　貴社・団体内 LAN には、有線、無線のいずれかのネットワークを利用していますか。（○は一つ）

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

問７．　インターネット環境は、現在、整備されていますか。（○は一つ）

１．整備している
２．整備していないが、現在整備を計画中である
３．整備する計画はない

問８．　外部から内部ネットワークへの接続を許可していますか。（○は一つ）

１．許可している
２．許可していない

【情報セキュリティの運用・管理体制について伺います】

問９．　情報セキュリティ対策の必要性を感じるのは、どのような理由からですか。（○はいくつでも）

1．過去1年間に不正アクセス等の攻撃・被害にあったため ⟶ 問9-1～9-3へお進みください

2．ウイルス等のマルウェアの感染を防ぐため
3．DDoS 攻撃等によるシステムダウンを防ぐため
4．システムの乗っ取り等により犯罪等へ悪用されるのを防ぐため
5．顧客等との取引を万全なものとするため
6．インターネット上に顧客情報等の部内情報が漏れるのを防ぐため
7．セキュリティ事故がブランドイメージや業績に与える影響を避けるため
8．事業を行う上で必要不可欠なため
9．顧客等から要請があるため
10. 社会情勢や国際的行事等から、攻撃が増えることが予想されるため
11. 新型コロナウィルス感染拡大による影響
12. 不正アクセスの加害者にならないため
13. その他（　　）

問10へ
お進みください

問９－１．　過去1年間に攻撃・被害を受けられた方にお伺いします。それは、どのような被害であり、また、攻撃手段でしたか。（○はいくつでも）

【→被害は？】

1．ホームページの改ざん
2．システム損壊等による業務妨害
3．ウイルスによる情報流出
4．ウイルス以外の情報流出
5．ネットワーク利用詐欺
6．偽サイト等模倣サイトの開設
7．フィッシングサイトの開設
8．電子メールの不正中継
9．Web 等での誹謗・中傷被害
10. 端末機器（PC、スマホ等）の盗難
11. 外部記録媒体の盗難
12. インターネットバンキング不正送金
13. ランサムウェア
14. その他データ盗用（キーロガー含）
15. その他（　　）
16. 実質的な被害はなかった

【→攻撃手段は？】

1．DDoS 攻撃
2．踏み台（バックドア設置等）
3．部外からの不正アクセス
4．ウイルス等の感染
5．システム損壊、データ改ざん
6．内部の者のネットワーク悪用
7．関連会社や取引先等を経由
8．不明
9．その他（　　）

問9-2.　過去１年間に攻撃・被害を受けられた方にお伺いします。攻撃・被害を受けた結果、実際に講じられた対応策はどういったものですか。（○はいくつでも）

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

問9-3.　過去1年間に攻撃・被害を受けられた方にお伺いします。どこに届出・相談をなされましたか。また、その理由は何ですか。（○はいくつでも）

〈届出・相談先機関等〉

1．警察	5．監督官庁
2．IPA（情報処理推進機構）	6．その他（　　）
3．JPCERT/CC	7．届け出なかった → 問9-4へお進みください
4．国民生活センター・消費生活センター	

→ 〈届出・相談した理由〉へお進みください

〈届出・相談した理由〉

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

問9-4.　過去1年間に攻撃・被害を受けられたが、届け出なかった方にお伺いします。届出・相談を躊躇させる要因としては、どういったことがあげられますか。（○はいくつでも）

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

問10.　不正アクセス禁止法では第８条において、アクセス管理者による防御措置について《努力義務》が規定されていますが、そのことを知っておられましたか。（○は一つ）

1．知っている
2．知らなかった

問11.　情報セキュリティに関して、その運用、管理を専門に行う部署はありますか。（○は一つ）

1．ある
2．ない
3．今後設置予定

問12.　情報セキュリティに関する管理体制は、どのようになっていますか。（○はいくつでも）

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

問13.　情報セキュリティポリシー等は、策定されていますか。（○は一つ）

1．策定している
2．現在、策定作業中である
3．今後、策定する予定である
4．今のところ、策定する予定はない
5．策定しない
6．非公開情報のため、答えられない

問13-１．　新型コロナウィルス感染拡大の影響により、情報セキュリティポリシー等を変更しましたか。（〇は一つ）

１．変更した
２．変更していない
３．変更することを検討
４．策定していない
５．非公開のため答えられない
６．その他（　　）

問14.　不正アクセス等の侵害事案が発生した場合のために、現在、対応マニュアルや要領等を策定しておられますか。（〇は一つ）

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

問15.　情報システムのセキュリティ対策について、第三者機関の認証制度等を利用していますか。（〇はいくつでも）

１．ISMS
２．Pマーク
３．PCI DSS
４．その他（　　）
５．特に利用していない

問16.　過去1年間にシステムのぜい弱性検査（ペネトレーションテスト等）を実施しましたか。（〇はいくつでも）

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

問17.　標的型攻撃対策としては、どのような取組をされていますか。（〇はいくつでも）

１．添付ファイル等に対する個別対策
２．フリーメール等に対する個別対策
３．標的型攻撃への対応訓練
４．標的型攻撃に関する教育
５．上司への即時報告等のマニュアル化
６．その他（　　）

問18.　ビジネスメール詐欺について知っておられましたか。（〇は一つ）

１．知っていた　→ 問19へお進みください
２．知らなかった　→ 問20へお進みください

問19.　問18で「１．知っていた」と回答された方にお伺いします。ビジネスメール詐欺への対策としては、どのような取組をされていますか。（〇は一つ）

１．対策を検討中
２．対策済み
３．対策はしていない
４．不明
５．その他（　　）

問20.　ログは取得後、どれくらいの期間保管されていますか。また、どの様な方法で行っておられますか。
（下表の各欄に、取得しているログの種類は該当する番号に○を、ログの保管期間及び方法は回答群Ａ（保管期間）・Ｂ（方法）からそれぞれ回答を選び、番号をご記入ください。）
※　回答が複数あるときは、最も長い期間を選んでご記入ください。

ログの種類	回答群 Ａ	回答群 Ｂ
１．ファイアウォール・侵入検知システム等（IDS、IPS 等）のログ		
２．ウェブサーバへのアクセスログ		
３．メールサーバのログ		
４．プロキシサーバのログ		
５．情報システムへの認証ログ		
６．データベースのログ		
７．クライアント PC のログ		
８．その他（　　）		
９．全く取得していない　⟶　問22にお進みください。		

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

回答群　Ｂ
１．自社
２．外部委託
３．その他
（　　）

問21. ログを取得・保管されているのは、どのような理由からですか。（○はいくつでも）

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

問22.　Web サービス（サイト、メール等）は、どのように管理されていますか。（○は一つ）

１．自社管理
２．一部外部業者に委託
３．全て外部業者に委託
４．ウェブサイトがない

問23. OS やアプリケーションのセキュリティ・パッチの適用や更新状況をお答えください。（○は一つ）

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

問24.　次年期（年単位）の情報セキュリティ対策の投資総額については、今年期（年単位）と比較してどのようになりますか（未定の場合は見込みでご回答ください）。（○は一つ）

1．大幅に増やす（+50%以上）計画
2．かなり増やす（+30～+50%）計画
3．小幅に増やす（+10～+30%）計画
4．ほぼ同額（−10～+10%）とする計画
5．小幅に減らす（−10～−30%）計画
6．かなり減らす（−30～−50%）計画
7．大幅に減らす（−50%以上）計画

問25.　これらの経費に関しては、どういった問題点が考えられますか。（○はいくつでも）

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

問26.　今後、どのようなことに重点をおいて、情報セキュリティ対策を行うべきだと考えておられますか。
下表の各行に考え方①、②の内容を比較し、より考え方が近いものをお選びください。
（○は各項目一つ）

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

２．　技術的対策

【情報セキュリティサービスの利用状況について伺います】

問27.　現在、どのようなサービスを利用されていますか。（○はいくつでも）

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

→ **問28へお進みください**

→ **問29へお進みください**

問28.　問27で「20．利用していない」と回答された方に伺います。その理由は何故ですか。（○はいくつでも）

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

【ネットワークに対する情報セキュリティ対策について伺います】

問29.　問８で確認した内容について、外部から内部ネットワークへの接続を許可している場合、どのような情報セキュリティ対策を講じておられますか。
通信路に対する対策は、回答群Ａから、端末に対する対策は、回答群Ｂからそれぞれ選択してください。（○はいくつでも）

【回答群Ａ（通信路に対する対策）】

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

【回答群Ｂ（端末に対する対策）】

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

問30.　安全なアクセス環境を維持するために、どのような対策をされていますか。（○はいくつでも）

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

問31．組織内で利用する無線 LAN では、どのようなセキュリティ対策を行っていますか。（○はいくつでも）

1．WEP による暗号化
2．WPA による暗号化
3．WPA2又はWPA3による暗号化
4．ESS-ID の適切な設定
5．MAC アドレス認証
6．IEEE802.1.x
7．電磁波の遮蔽
8．その他（　　）
9．特に行っていない

問32.　従業員等が社外等からインターネット接続経由で業務アクセスを行う場合に利用しているのは、どういった認証方法ですか。（○はいくつでも）

→問33へお進みください

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

→ 問34へお進みください

問33.　問32で「ＩＤ・パスワード等による認証」と回答された方に伺います。ＩＤ・パスワード等の管理を徹底するために、どのような対策をされていますか。（○はいくつでも）

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

問34.　不正ログイン（他人のＩＤ・パスワードを無断で入力する不正アクセス行為）を防止するために、どのような対策をされていますか。（○はいくつでも）

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

【Ｗｅｂサービスに対するセキュリティ対策について伺います】

問35. Web サーバのセキュリティ対策では、どのような取組みをされていますか。（○はいくつでも）

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

問36. 電子メールに関するセキュリティ対策では、どのような取組みをされていますか。（○はいくつでも）

１．常に最新のパッチを適用
２．不正中継の防止
３．フィルタリング（特定の条件を満たすメールの配信をしない）
４．ウイルスチェック
５．特定ドメイン・アドレスからのメールのみ送・受信
６．特定の拡張子を持つファイルが添付されている場合に送・受信を拒否
７．利用メールソフトの指定・制限
８．メール利用の制限
（利用可能者の限定、利用端末の限定、組織内は別のツールで連絡を行う　等）
９．SPF（Sender　Policy　Framework）の導入
10. DKIM（DomainKeys Identified Mail）の導入
11. その他送信者認証
12. 電子署名の利用
13. その他（　　）
14. わからない

問37. 電子メールに添付されたファイルは、どのように取り扱っておられますか。（○はいくつでも）

１．ウイルスチェックをしてから受信
２．無害化、振る舞い検知等をしてから受信
３．パスワード設定の添付ファイルのみ受信
４．添付ファイル付きの電子メールは一切受信しない
５．特にチェックもせず受信
６．その他（　　）

【不正アクセス、情報漏えい等に対する情報セキュリティ対策について伺います】

問38. 現在、暗号化技術は、どのような用途で使用されていますか。（○いくつでも）

１．暗号メール
２．記憶媒体上の情報（ファイルの暗号化）
３．記録媒体全体
４．認証情報（電子証明書）
５．個人情報等の重要な情報の通信（SSL/TLS 等の暗号化通信）
６．その他（　　）
７．利用していない

問39.　重要なシステム（基幹業務、製造　等に関わるシステム）への侵入阻止や侵入時における被害軽減に向けて、どのような対策を導入されていますか。
（○はいくつでも）

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

問40.　不正アクセス、データ改ざん、情報漏えい等の行為に対して、どのような対策を実施されていますか。
（○はいくつでも）

1．情報資産へのアクセス権の設定
2．定期的なパスワード変更
3．許可していないソフトウェアの制限
4．ユーザアカウントの定期的なチェック
5．アクセスログの取得、ログの分析
6．個人認証のためのシステム導入
7．定期的なバックアップ
8．バックアップの履歴管理
9．印刷物、電子媒体の持出し、廃棄管理
10．パソコン廃棄時の適正なデータ消去
11．共有 ID・パスワードの禁止
12．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
13．メールのフィルタリング（添付ファイルの利用制限等）
14．外部 Web サイトへのアクセス制限
15．その他（　　）
16．特に何も行っていない

問41.　ウイルスやマルウェア等の不正プログラムに対して、どのような対策を実施されていますか。
（○はいくつでも）

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

３．人的対策

【情報セキュリティ教育に関する取り組みについて伺います】

問42.　現在、情報セキュリティ教育を行っておられますか。（○は一つ）

１．実施している
２．実施を予定している　→　問44へお進みください

３．実施していない　→　問43へお進みください

問43.　なぜ実施しないのですか。（○はいくつでも）

１．指導できる者が社内にいない
２．必要な資金がない
３．環境的に必要ない
４．必要な時間がない
５．その他（　　）

問44.　情報セキュリティに関する教育では、どのような内容を行っておられますか。（○はいくつでも）

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

問45.　情報セキュリティに関する教育は、どのくらいの頻度で行われていますか。（○はいくつでも）

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

問46.　情報セキュリティ対策を実施するに当たって、困難に感じていることや、不正アクセス行為対策に対する不安等、または、本アンケート調査に対するご意見等がございましたら、次の空欄に記載してください。

アンケートはこれで終わりです。ご協力ありがとうございました。
お手数ですが、令和2年9月25日(金) までに、ご返送ください。

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

付録２

集計表

問１．業種別回収数

農林・水産・鉱業	
農林・水産	2
鉱業	0
その他	1
小計	3
製造業	
食品	12
繊維	7
紙・パルプ	2
化学	25
薬品	7
ゴム・窯業	6
非鉄金属	12
機械	22
電気機器	15
造船	0
輸送機器	11
精密機器	12
その他	24
小計	155
不動産・建築	
不動産	13
建築	23
その他（不動産・建築）	4
小計	40
金融	
銀行	15
証券	5
保険	1
クレジット	2
消費者金融	1
信用金庫・組合	0
その他	5
小計	29
エネルギー	
電力	3
ガス	3
水道	1
石油製造(精製)	0
その他	1
小計	8

運輸業	
鉄道・地下鉄	7
航空	0
陸運	3
海運	1
倉庫	6
その他	3
小計	20
情報通信	
新聞	0
放送	4
通信	4
ＩＳＰ	0
その他	2
小計	10
サービス	
流通・卸売	22
小売	14
娯楽・アミューズメント	0
飲食	0
ホテル・旅行	1
情報処理・ソフトウェア	20
警備	1
医療・福祉	45
その他	45
小計	148
教育	
大学	74
短大	0
専門学校	1
その他	6
小計	81
行政サービス	
都道府県	2
政令指定都市	5
市町村	108
小計	115
無回答	13
合計	622

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1,822件抽出した。

・企業（1,600社）

市販のデータベース（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（222校）

国公立・私立大学のうち、理工系学部又はこれに準ずるものを設置するもの

調査方法は、次の方法で実施した。

① 電子メールでの回答

調査票のファイルに直接回答内容を入力してもらい、電子メールにて回答

② 郵送等での回答

配付した調査票を、郵送やFAXなどで送付してもらい回答

（調査期間：令和2年8月26日(水)(発送日)～9月25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7つの分野に分類し、企業や大学において力をいれている分野等を調査した。

質問項目は次の通りである。

・研究開発体制

・アクセス制御機能に関する技術研究開発に係る現状と今後の展望

・アクセス制御機能に関する実用化（製品化）に係る現状と今後の展望

調査票：付録資料にある『回答用紙A』を参照

【分類の票】

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

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、1,822件を送付して、204件を回収し、回収率は11.2%であった。

全体での回収数204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18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32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

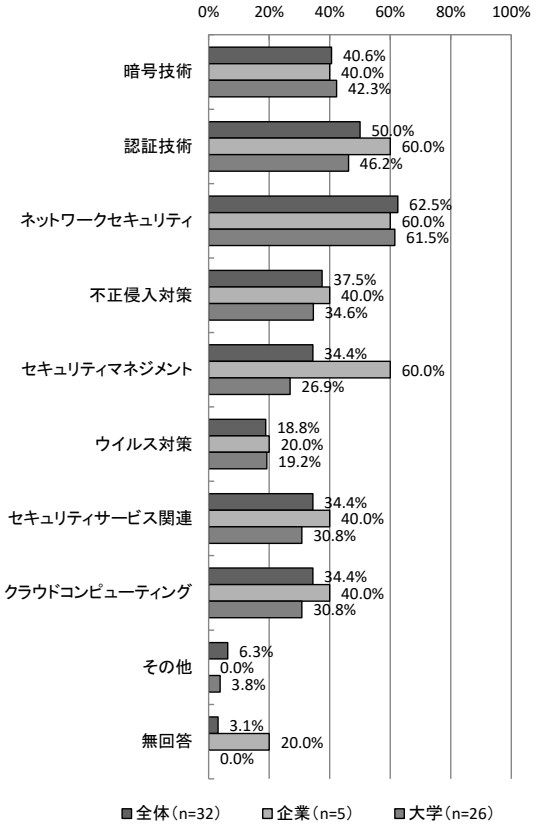
現在、取り組んでいる分野について、全体では「ネットワークセキュリティ」が最も多く、企業では「認証技術」「ネットワークセキュリティ」、大学では「ネットワークセキュリティ」が最も多くなっている。

今後、取り組んでいく分野について、全体では「暗号技術」が最も多く、企業では「不正侵入対策」「セキュリティサービス関連」、大学では「暗号技術」が最も多くなっている。

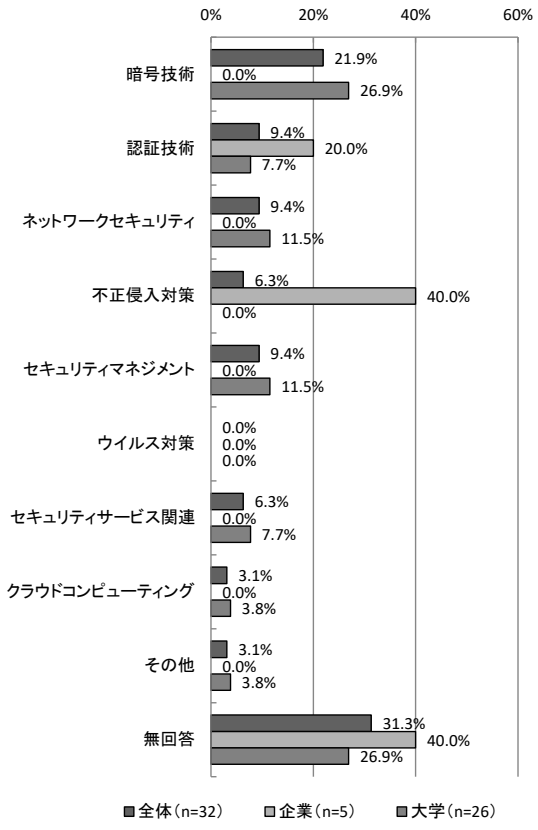
現在、取り組んでいる分野については、「ネットワークセキュリティ」が62.5%（20件）で最も多く、次いで「認証技術」が50.0%（16件）となっている。企業では「暗号技術」「ネットワークセキュリティ」が60.0%（3件）で最も多く、大学では「ネットワークセキュリティ」が61.5%（16件）で最も多い。

今後、もっとも力を入れたい分野については、「暗号技術」が21.9%（7件）で最も多く、次いで「認証技術」「ネットワークセキュリティ」「セキュリティマネジメント」が9.4%（3件）となっている。企業では「不正侵入対策」が40.0%（2件）、大学では「暗号技術」が26.9%（7件）と最も多くなっている。

【本調査】現在、取り組んでいる分野（MA）【A-問2】



【本調査】今後、もっとも力を入れたい分野（SA）【A-問3】



5.1.1　現在、取り組んでいる分野　【A-問2】

【経年変化】

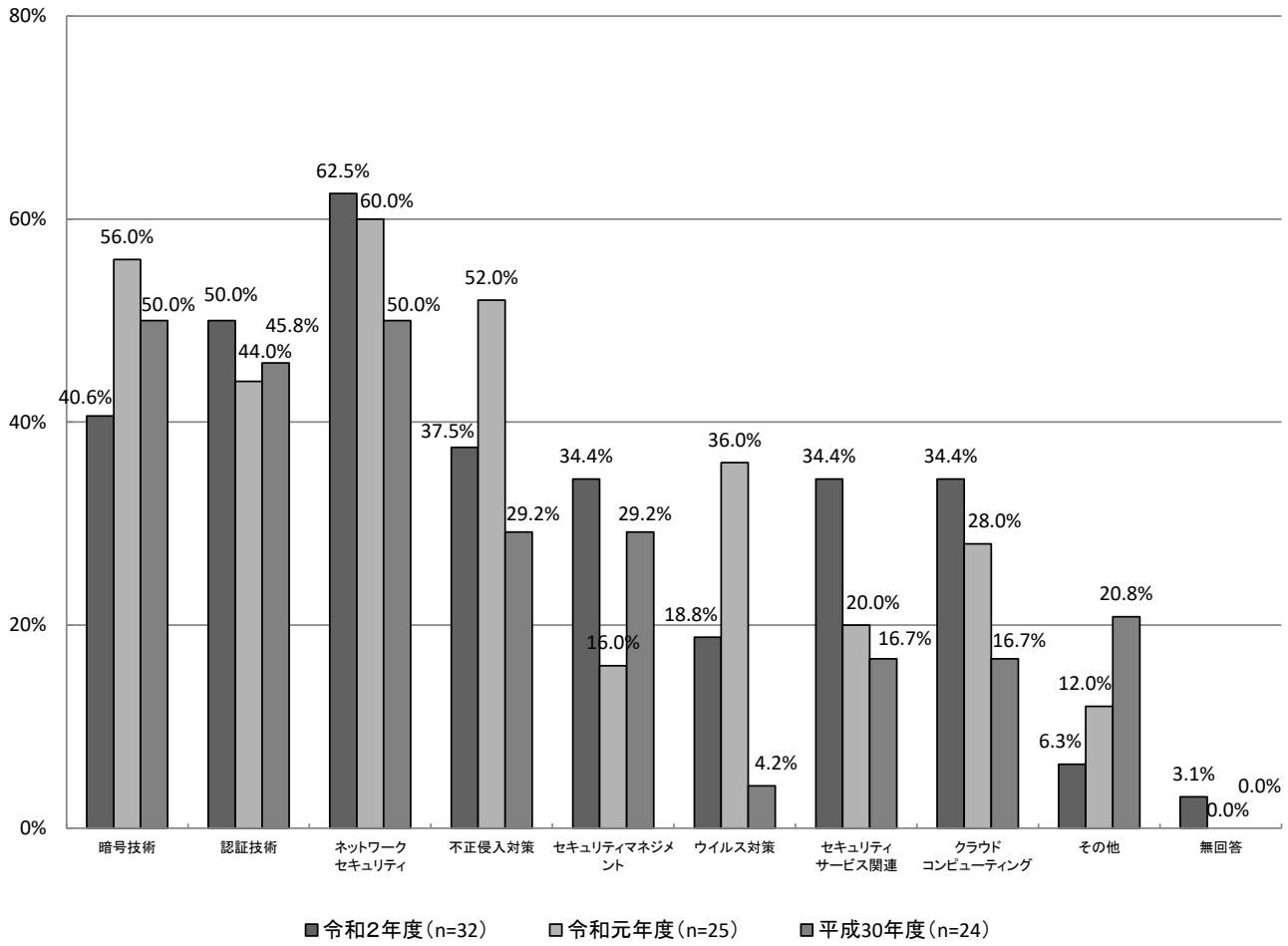
全体では、昨年度より全般的に増加する分野が多く、特に「セキュリティマネジメント」、「セキュリティサービス関連」が大きく増加している。

企業では、「認証技術」や「セキュリティマネジメント」が増加し、大学では、「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)】

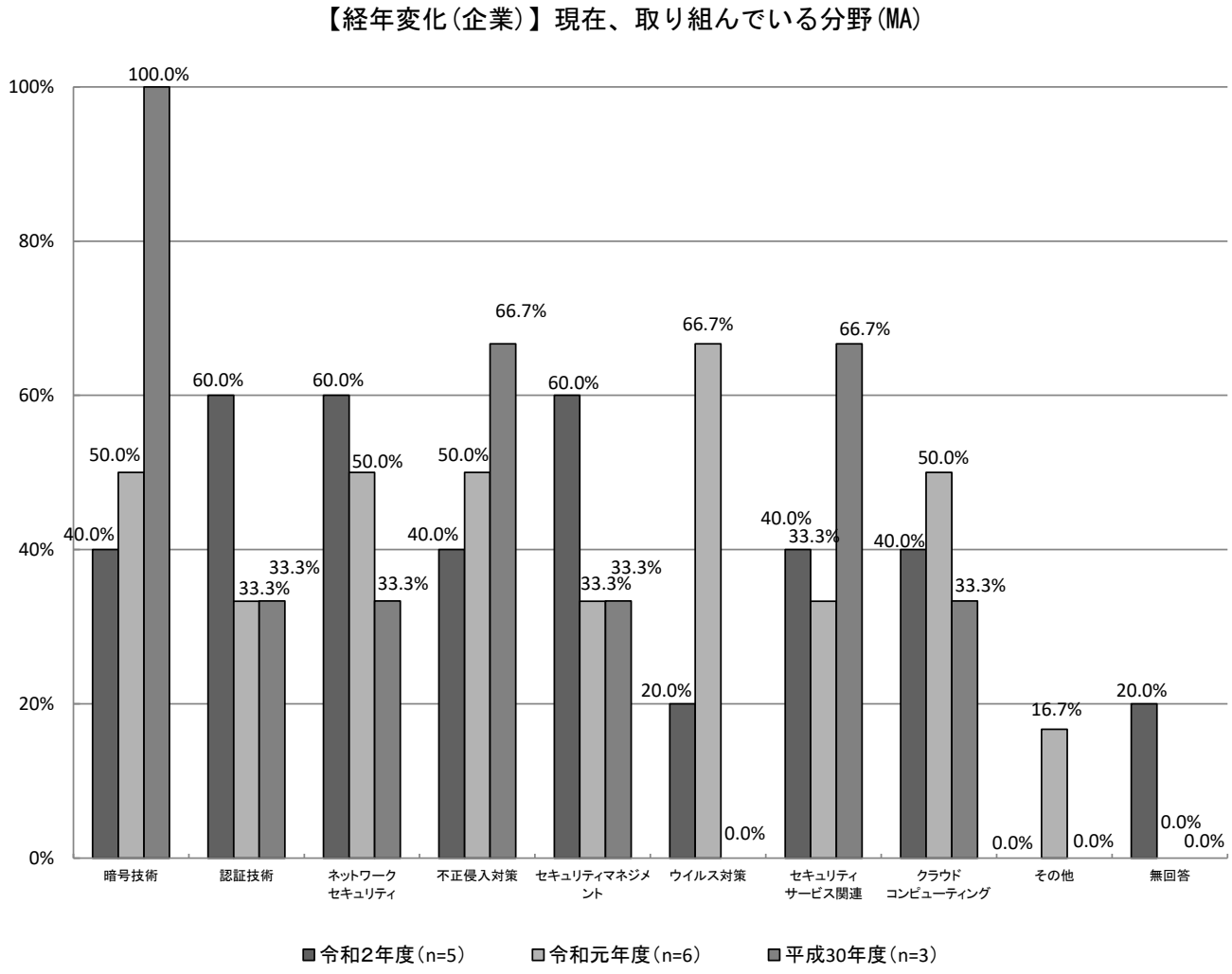
昨年度と比較すると全体では、「セキュリティマネジメント」が18.4ポイント、「セキュリティサービス関連」が14.4ポイント増加している。

【経年変化(全体)】現在、取り組んでいる分野(MA)



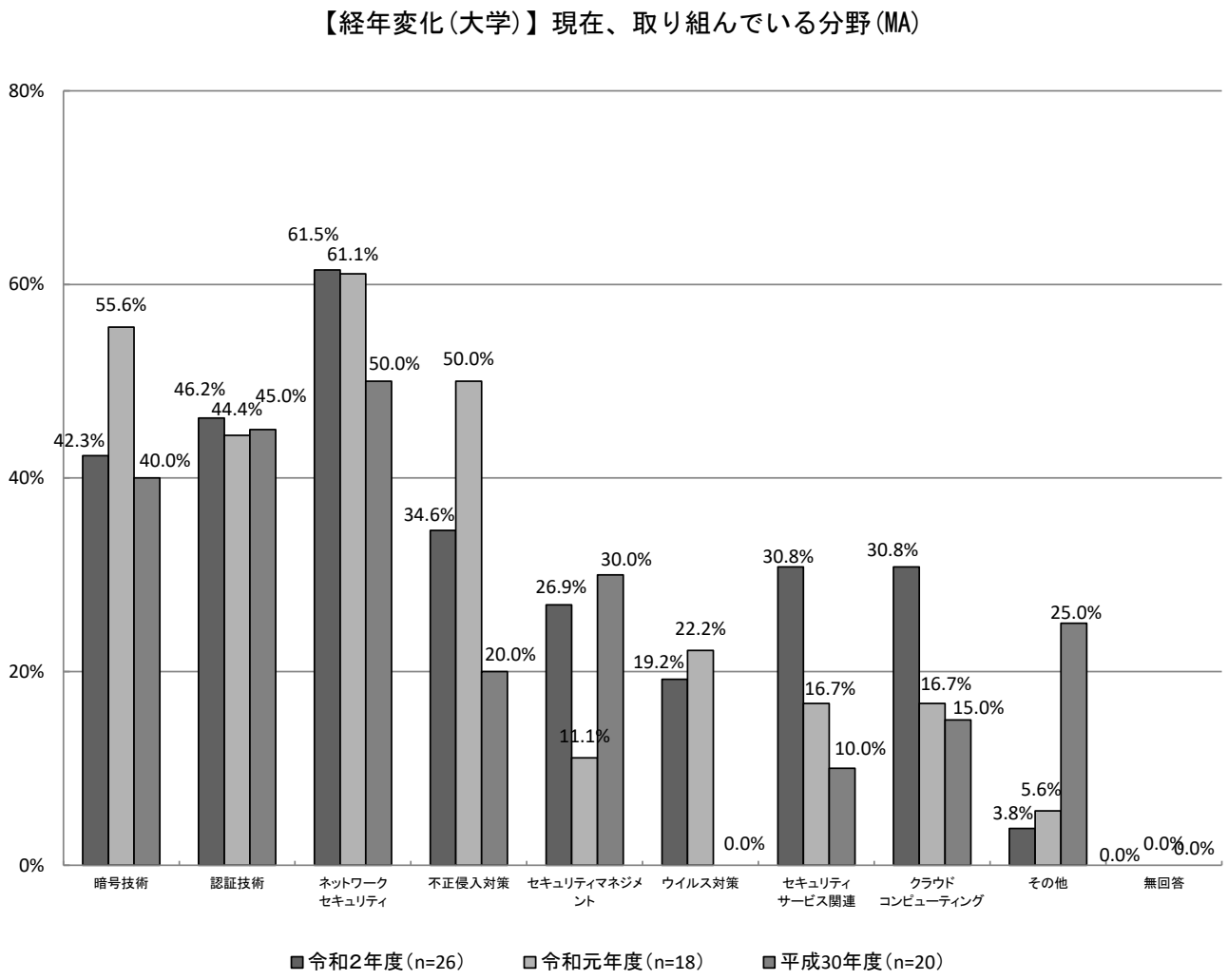
【経年変化(企業)】

昨年度と比較すると企業では、「認証技術」「セキュリティマネジメント」がそれぞれ26.7ポイントで最も増加している。一方「ウイルス対策」が46.7ポイント減少している。



【経年変化(大学)】

昨年度と比較すると大学では、「セキュリティマネジメント」が15.8ポイント、「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」がそれぞれ14.1ポイント増加している。



5.1.2　今後、もっとも力を入れたい分野　【A-問3】

【経年変化】

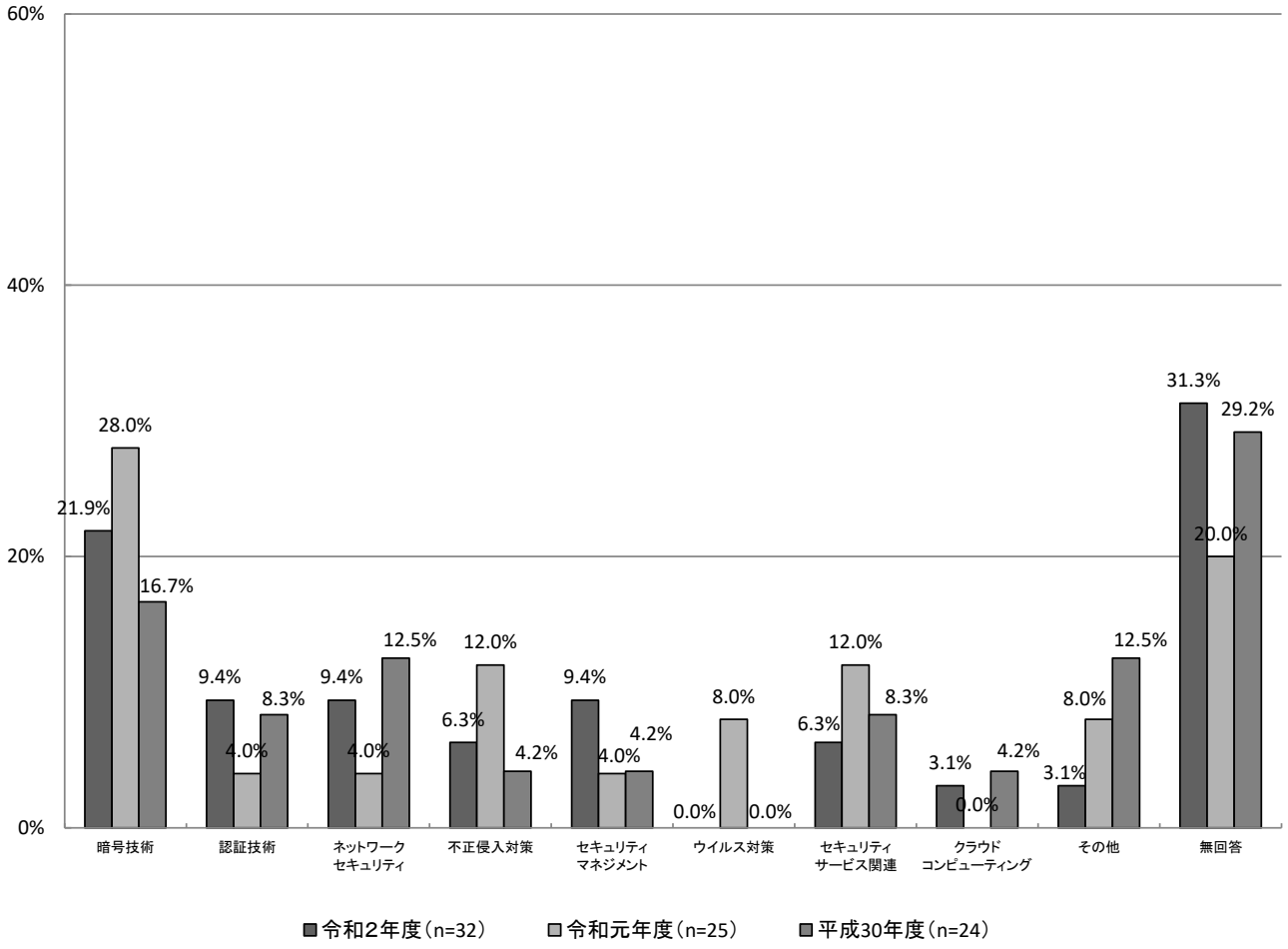
全体では、半数以上の分野で昨年度より減少しており、特に「ウイルス対策」、「暗号技術」で差が大きくなっている。

企業では、「不正侵入対策」が昨年度より最も増加しており、大学では、「ネットワークセキュリティ」が昨年度より最も増加している。

【経年変化(全体)】

昨年度と比較すると全体では、「ウイルス対策」が8.0ポイント、「暗号技術」が6.1ポイント減少している。一方、「認証技術」「ネットワークセキュリティ」「セキュリティマネジメント」はそれぞれ5.4ポイント増加している。

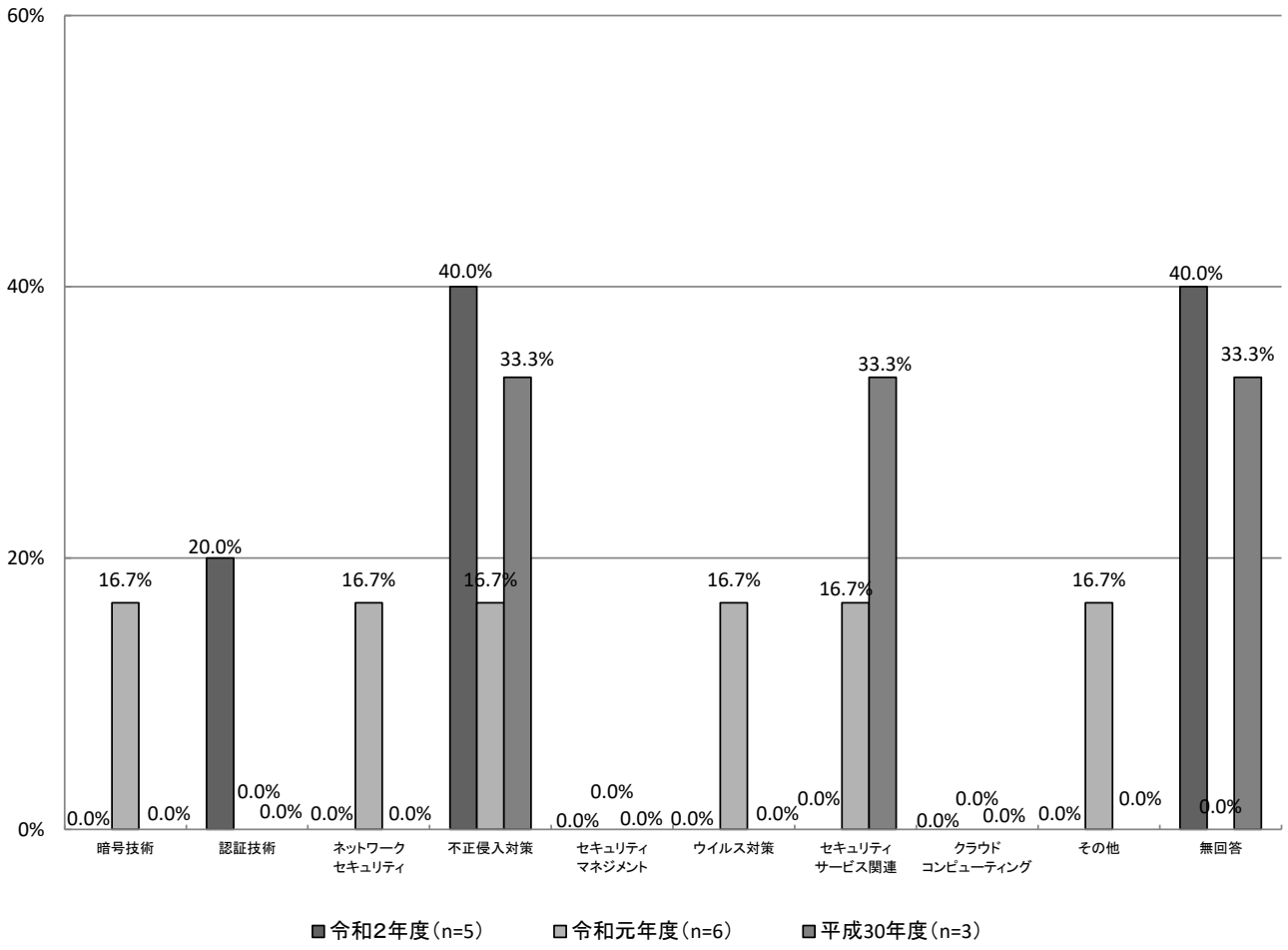
【経年変化(全体)】今後、もっとも力を入れたい分野(SA)



【経年変化(企業)】

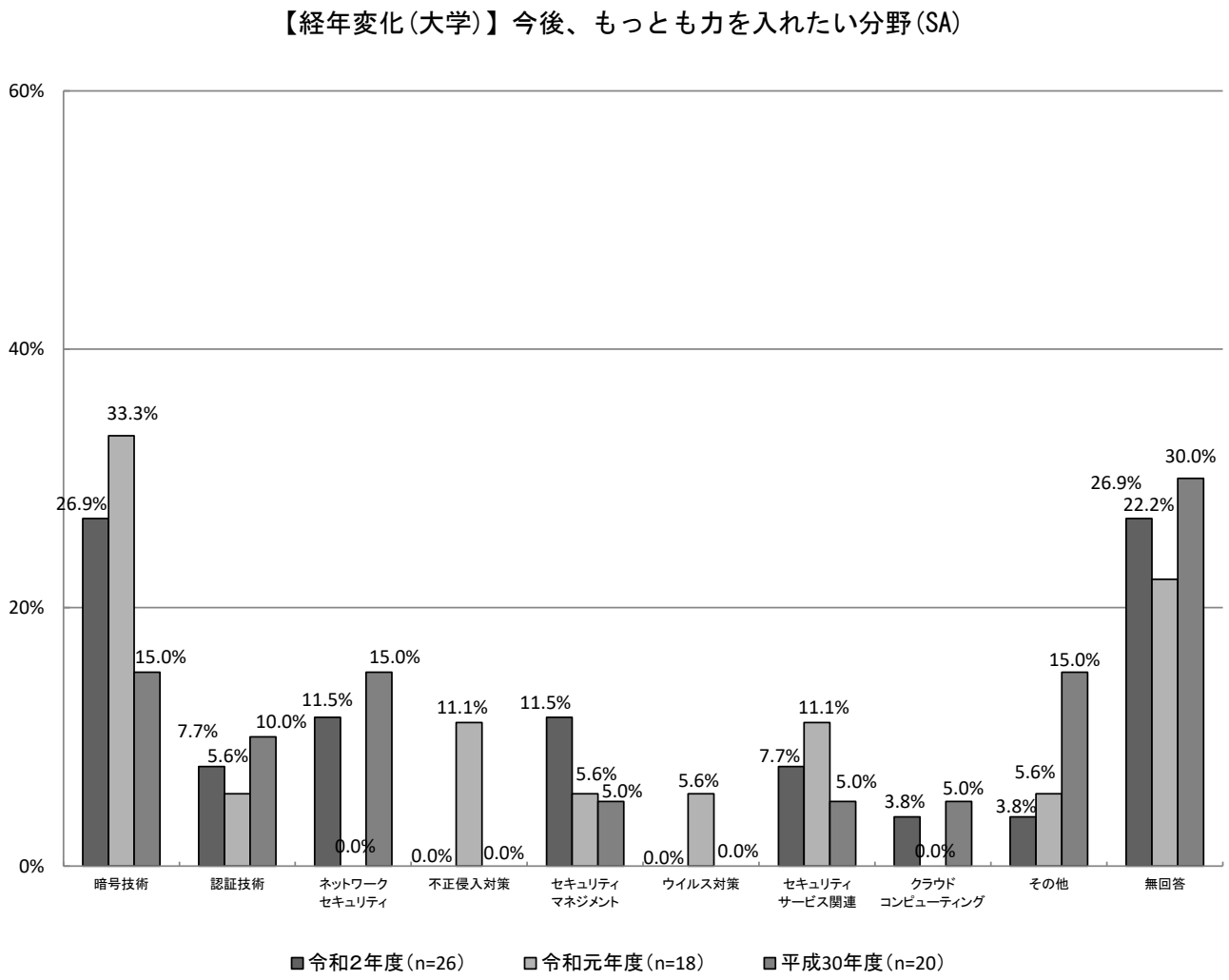
昨年度と比較すると企業では、「不正侵入対策」が23.3ポイント、「認証技術」が20.0ポイントと増加している。一方、増加した２項目以外の回答は得られなかった。

【経年変化(企業)】今後、もっとも力を入れたい分野(SA)



【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11.5ポイント増加している。



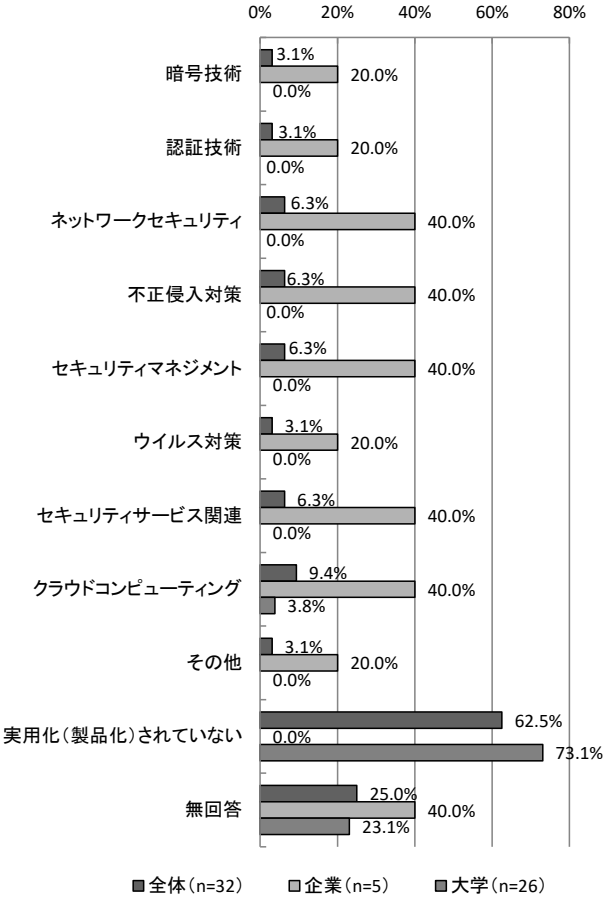
5.2　アクセス制御機能に関する実用化（製品化）に係る現状と今後の展望

実用化（製品化）の現状については、「クラウドコンピューティング」が最も多くなっている。
今後、実用化（製品化）を見込んでいるアクセス制御機能については、「認証技術」が最も多くなっている。

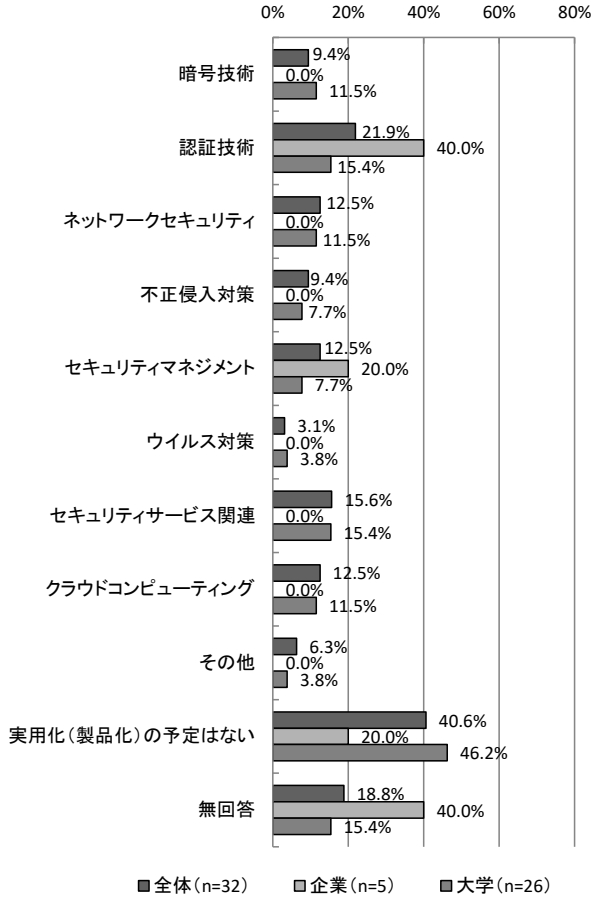
現在、実用化（製品化）されている分野については、全体では「クラウドコンピューティング」が9.4%（3件）で最も多く、次いで「ネットワークセキュリティ」「不正侵入対策」「セキュリティサービス関連」がそれぞれ6.3%（2件）となっている。企業では「ネットワークセキュリティ」「不正侵入対策」「セキュリティマネジメント」「セキュリティサービス関連」「クラウドコンピューティング」がそれぞれ40.0%（2件）で最も多く、大学では「クラウドコンピューティング」が3.8%（1件）で最も多くなっている。

今後、実用化（製品化）を見込んでいる分野については、全体及び企業では「認証技術」がそれぞれ21.9%（7件）、40.0%（2件）で最も多く、企業では「認証技術」「セキュリティサービス関連」がそれぞれ40.0%（2件）で最も多くなっている。

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



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

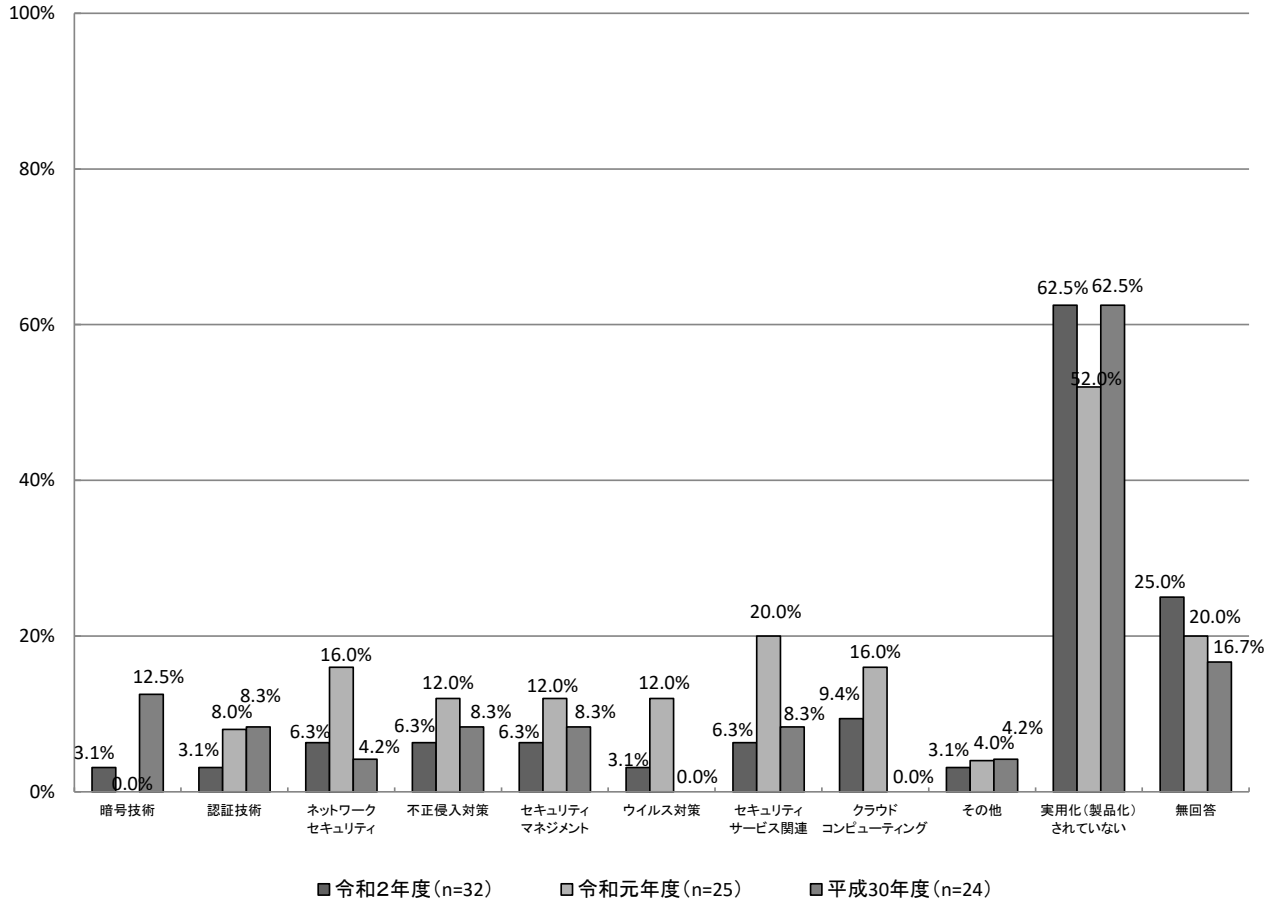


5.2.1　現在、実用化(製品化)されている分野　【A-問4】

【経年変化】
全体では、「暗号技術」を除くすべての分野で減少している。
企業では、「暗号技術」を除くすべての分野で減少し、大学では、「クラウドコンピューティング」以外の分野の回答は得られなかった。

【経年変化(全体)】
昨年度と比較すると全体では、「暗号技術」を除くすべての分野で減少している。

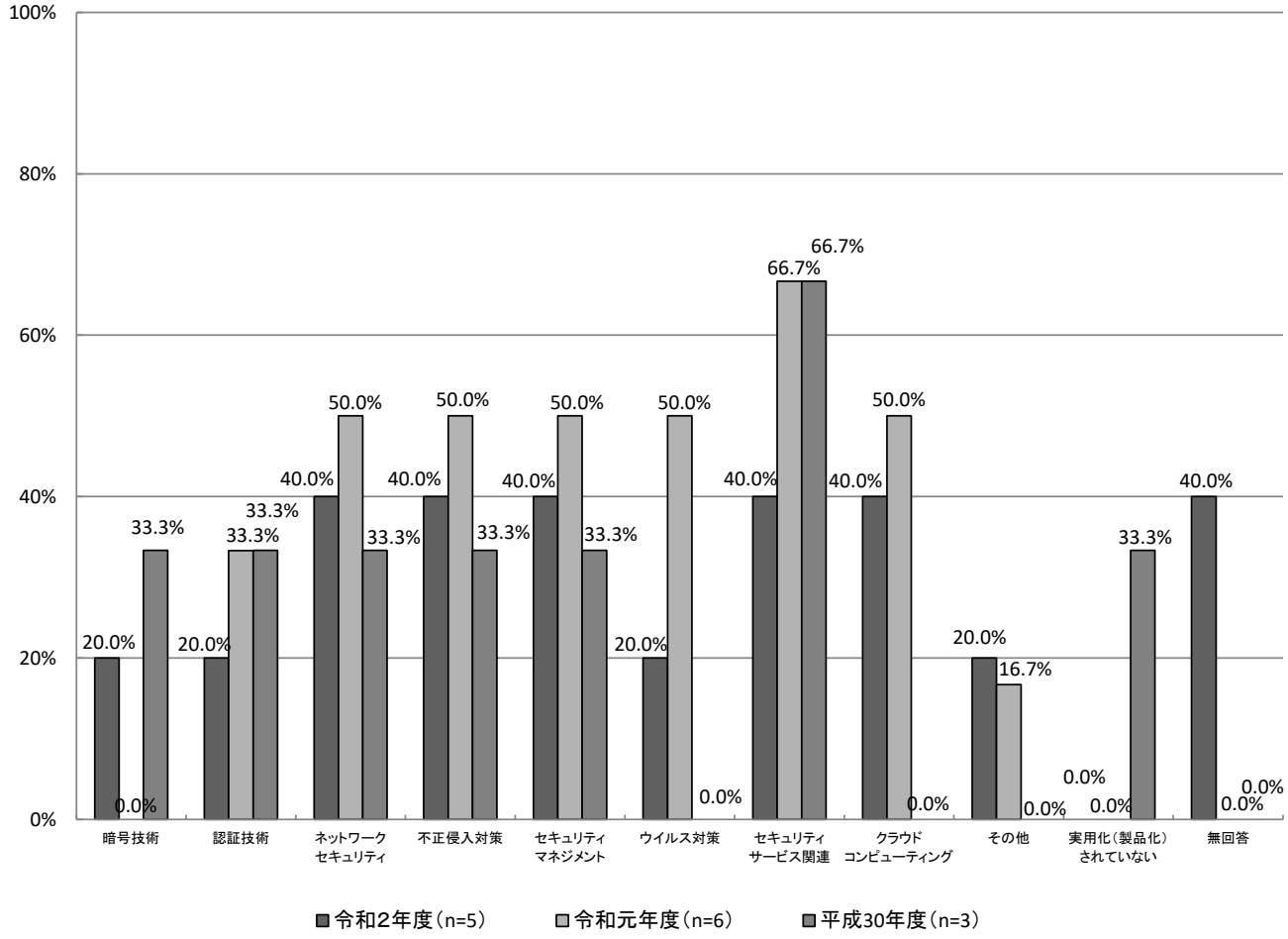
【経年変化(全体)】現在、実用化(製品化)されている分野(MA)



【経年変化(企業)】

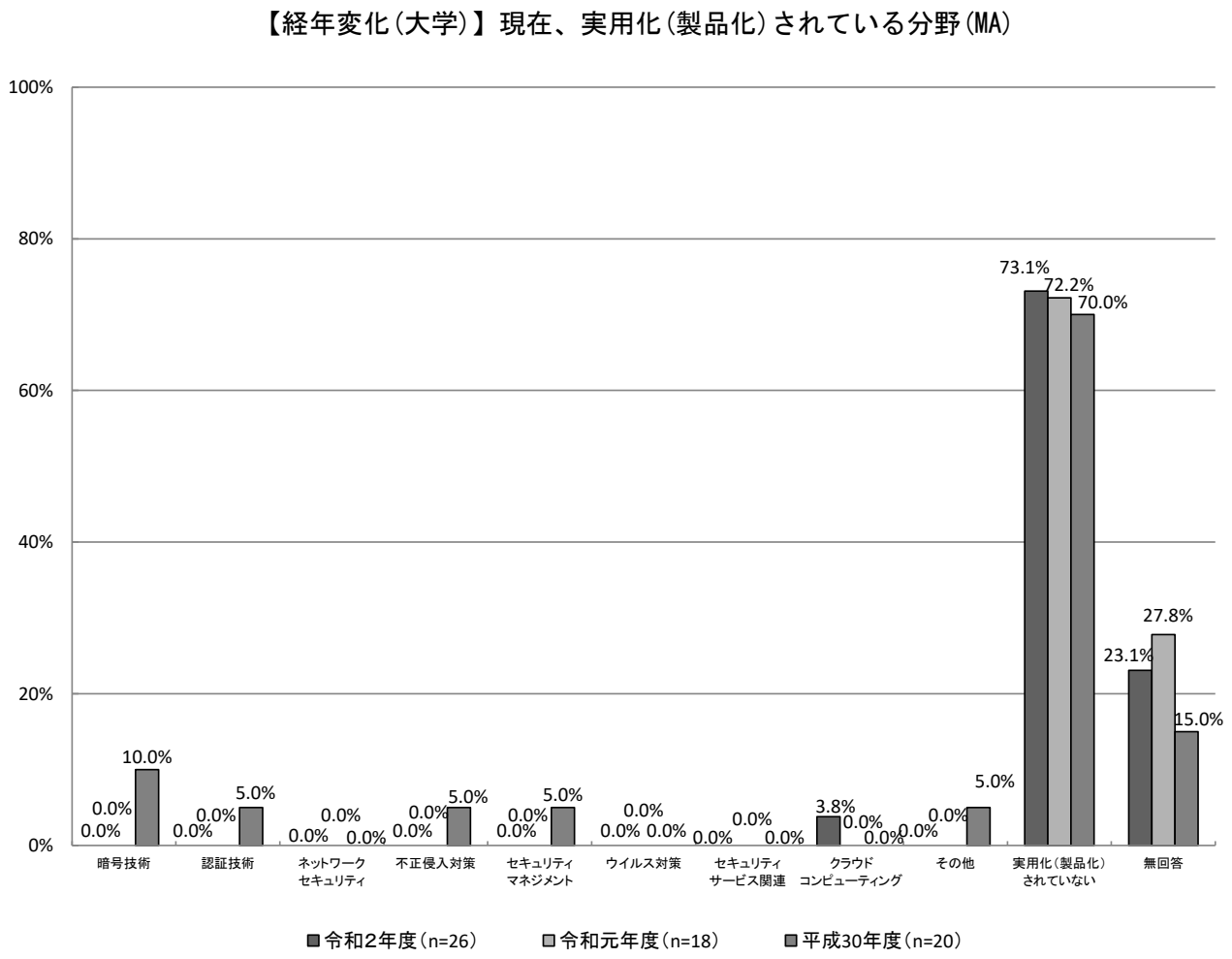
昨年度と比較すると企業では、「暗号技術」を除くすべての分野で減少しており、特に「ウイルス対策」が30.0ポイント減少している。

【経年変化(企業)】現在、実用化(製品化)されている分野(MA)



【経年変化(大学)】

昨年度と比較すると大学では、「クラウドコンピューティング」が3.8ポイント増加している。



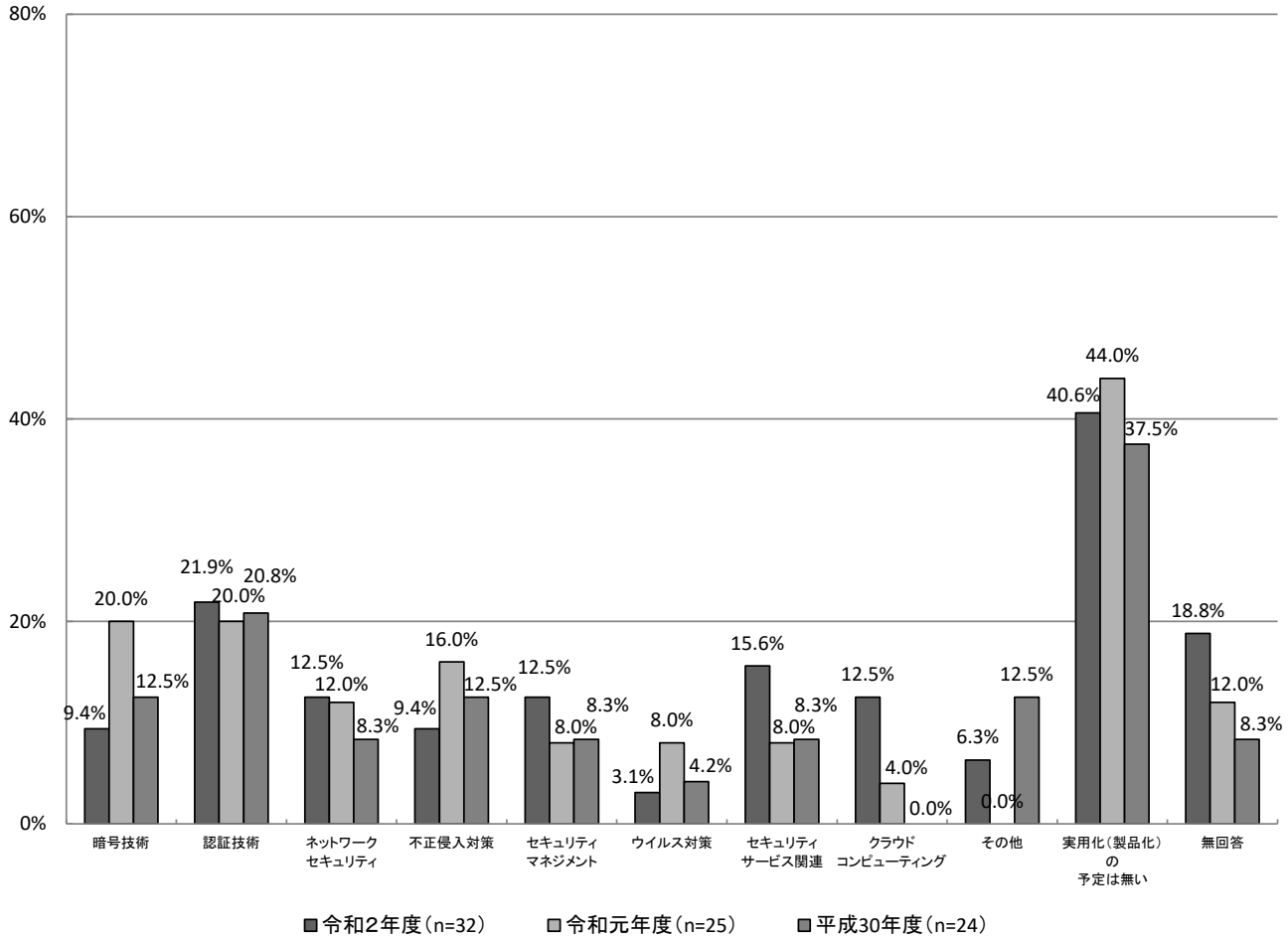
5.2.2　今後、実用化(製品化)を見込んでいる分野　【A-問5】

【経年変化】
全体では、「暗号技術」が大きく減少している。
企業では「「セキュリティマネジメント」、大学では「セキュリティ関連サービス」がそれぞれ最も増加している。

【経年変化(全体)】

昨年度と比較すると全体では、「暗号技術」が10.6ポイント、「不正侵入対策」が6.6ポイント減少している。一方、「クラウドコンピューティング」が8.5ポイント、「セキュリティサービス関連」が7.6ポイント増加している。

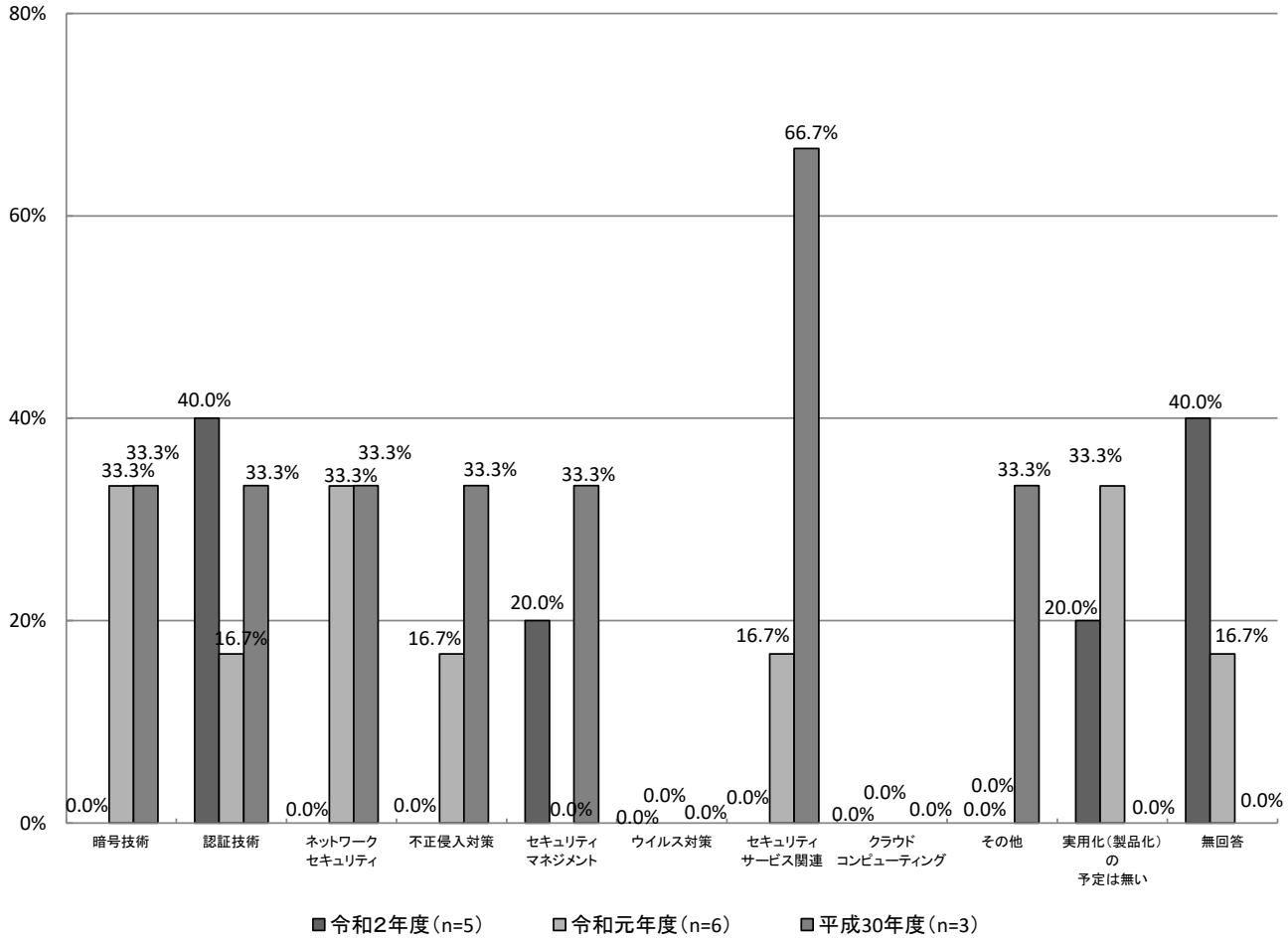
【経年変化(全体)】今後、実用化(製品化)を見込んでいる分野(MA)



【経年変化(企業)】

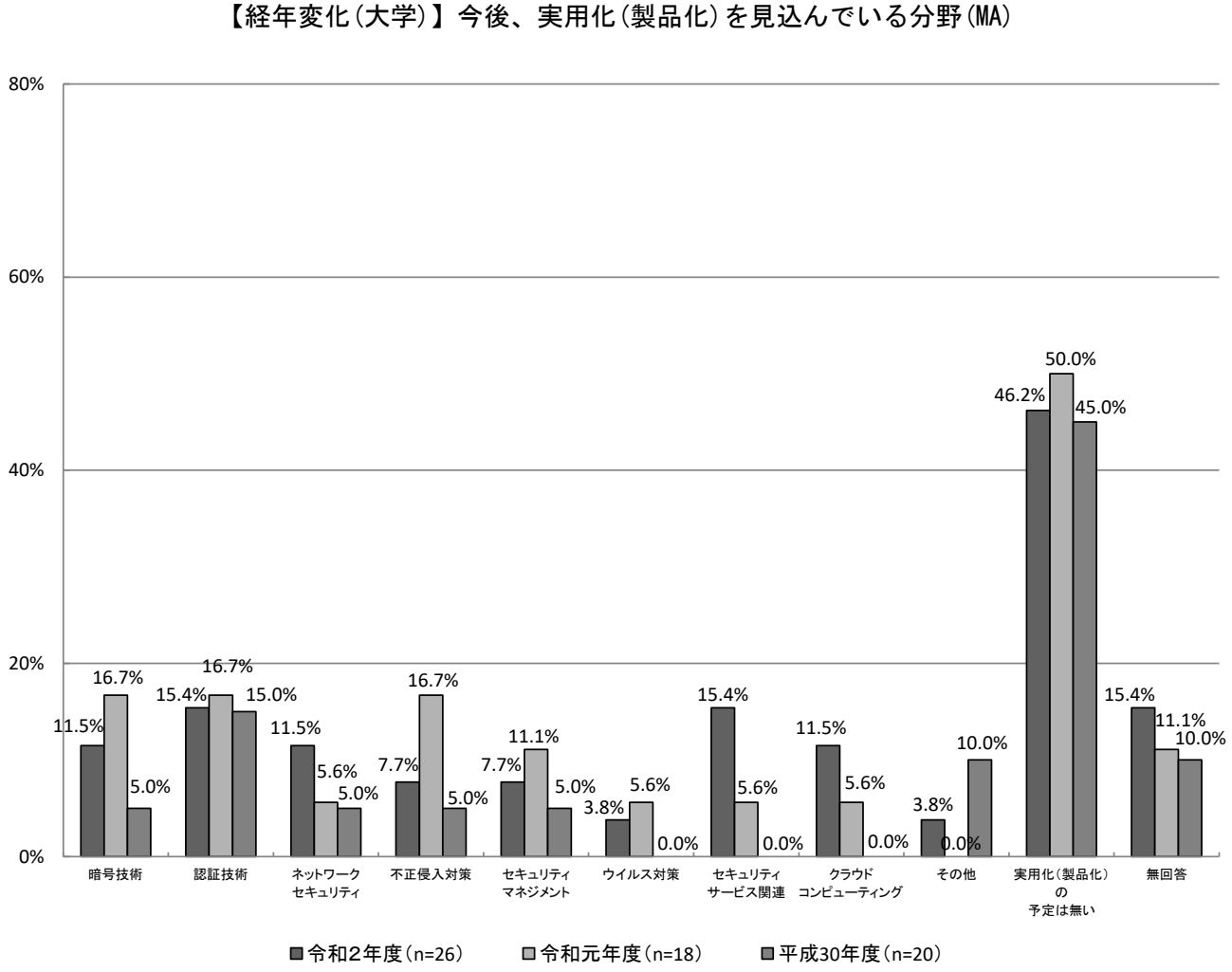
昨年度と比較すると企業では、「認証技術」が23.3ポイントと最も増加しており、次いで「セキュリティマネジメント」が20.0ポイント増加している。一方、「暗号技術」「ネットワークセキュリティ」はそれぞれ33.3ポイント減少している。

【経年変化(企業)】今後、実用化(製品化)を見込んでいる分野(MA)



【経年変化(大学)】

昨年度と比較すると大学では、「セキュリティサービス関連」が9.8ポイントと最も増加しており、次いで「ネットワークセキュリティ」「クラウドコンピューティング」が5.9ポイント増加している。一方「不正侵入対策」は9.0ポイント減少している。



5.3　研究開発体制

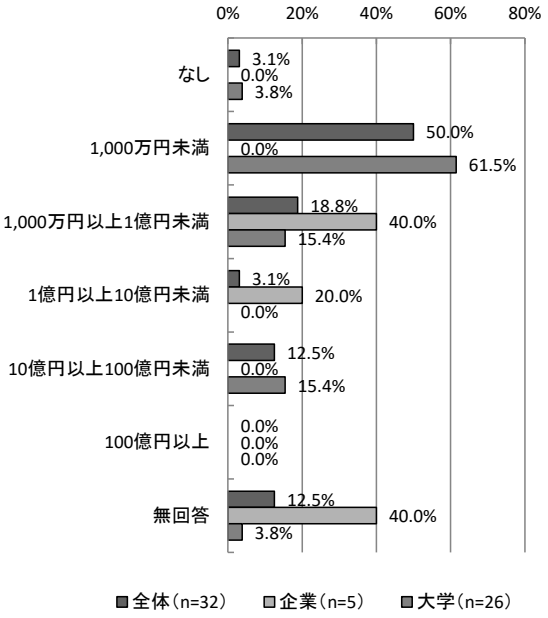
研究開発費について、企業では「1,000万円以上1億円未満」が最も多く、大学では「1,000万円未満」が最も多くなっている。

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

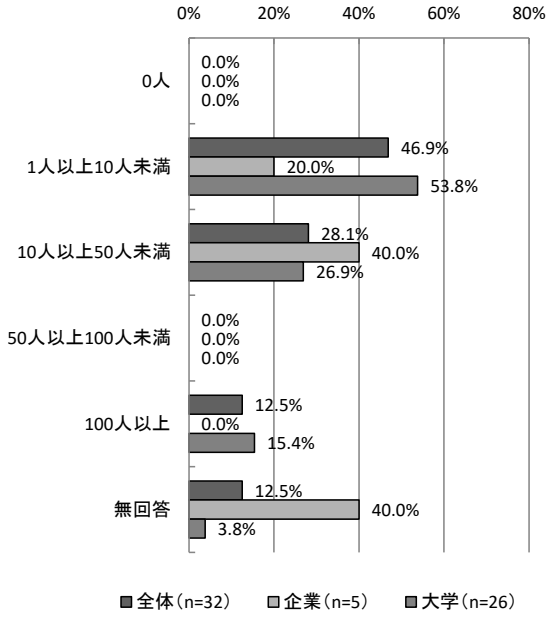
年間の研究開発費については、「1,000万円未満」が50.0%（16件）で最も多くなっている。企業では「1,000万円以上1億円未満」が40.0%（2件）で最も多く、大学では「1,000万円未満」が61.5%（16件）と最も多くなっている。

研究開発人員については、全体では「1人以上10人未満」が46.9%（15件）と最も多くなっている。企業では「10人以上50人未満」が40.0%（2件）で最も多く、大学では「1人以上10人未満」が53.8%（14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】

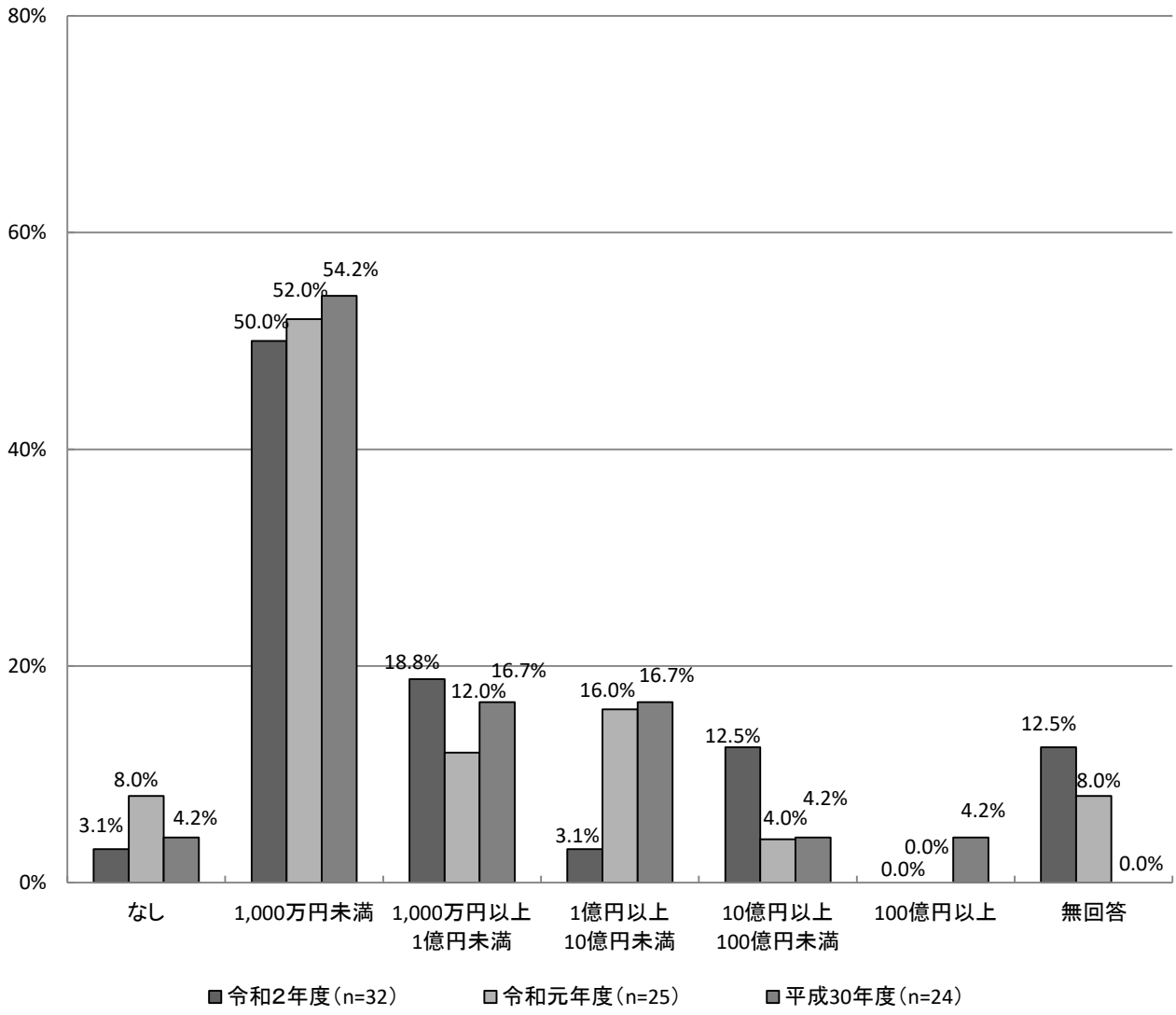


5.3.1　年間の研究開発費　【A-問6】

【経年変化】
　全体及び大学では「10億円以上100億円未満」が最も増加しており、企業では「1,000万円以上1億円未満」で最も増加している。

【経年変化(全体)】
昨年度と比較すると全体では、「10億円以上100億円未満」が8.5ポイント増加している。

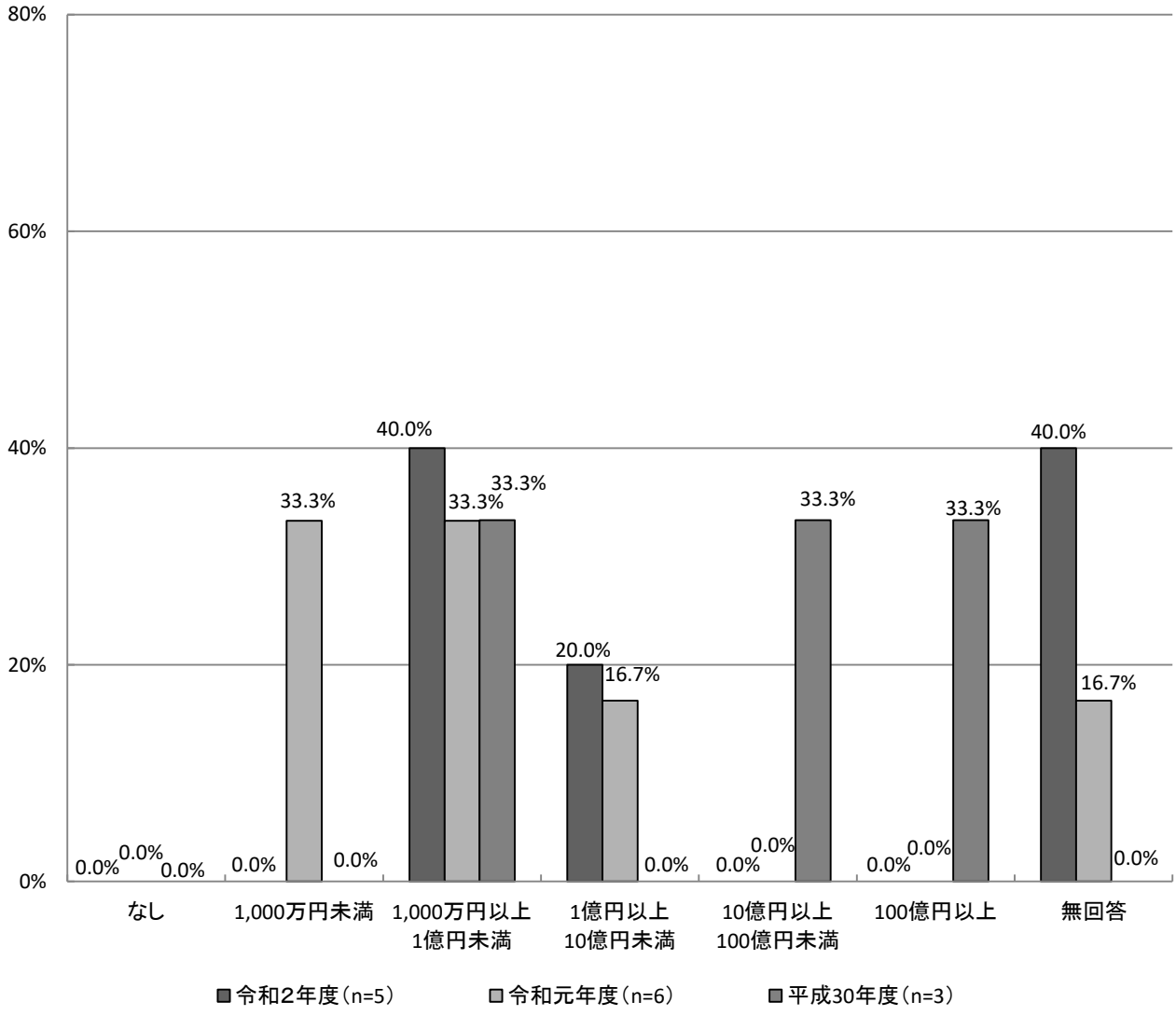
【経年変化(全体)】年間の研究開発費(SA)



【経年変化(企業)】

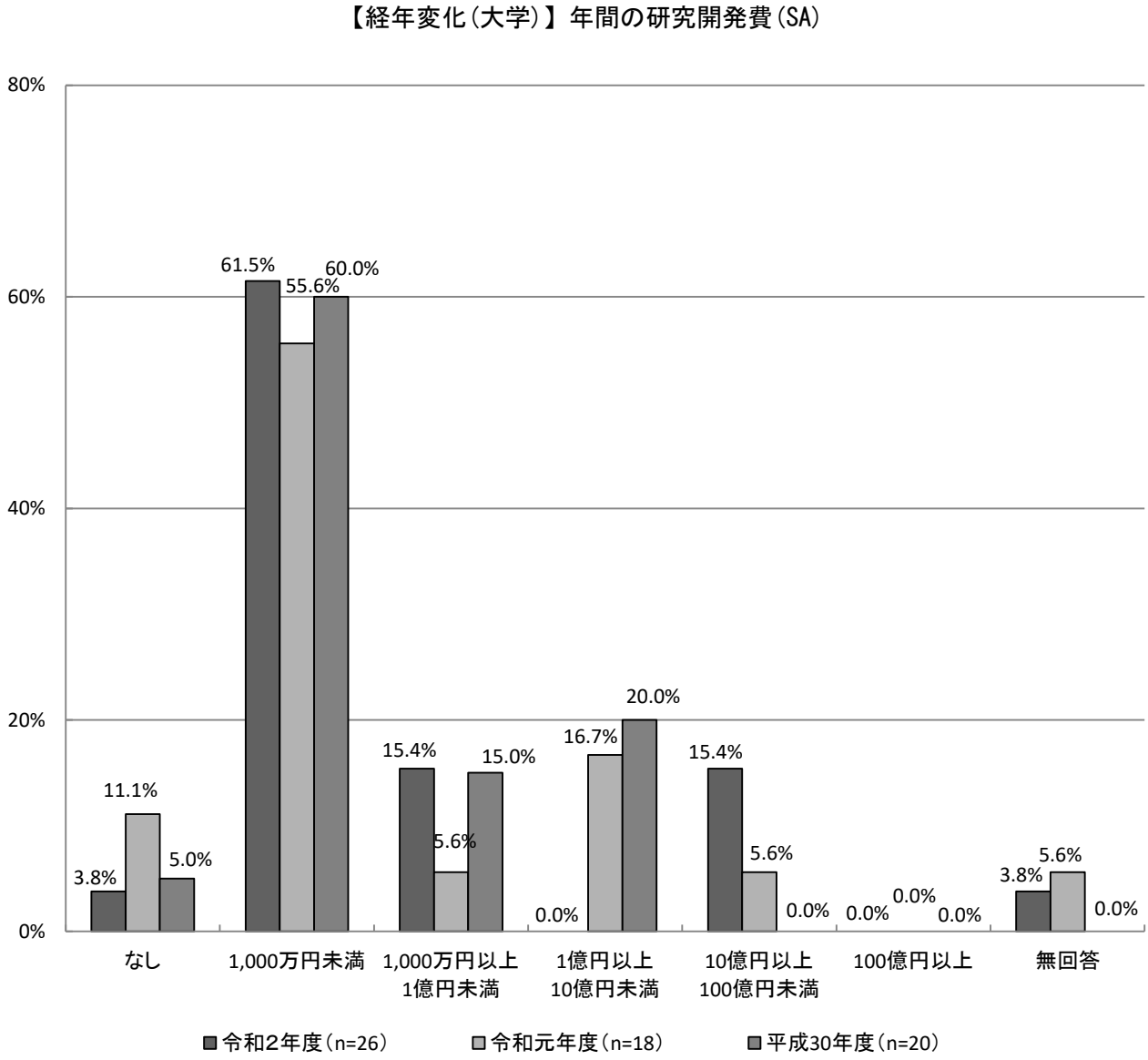
昨年度と比較すると企業では、「1,000万円以上1億円未満」が6.7ポイントと最も増加している。一方で「1,000万円未満」が33.3ポイント減少している。

【経年変化(企業)】年間の研究開発費(SA)



【経年変化(大学)】

昨年度と比較すると大学では、「1,000万円以上1億円未満」「10億円以上100億円未満」がそれぞれ9.8ポイントと最も増加しており、次いで「1,000万円未満」が5.9ポイント増加しており、それ以外の項目では減少している。

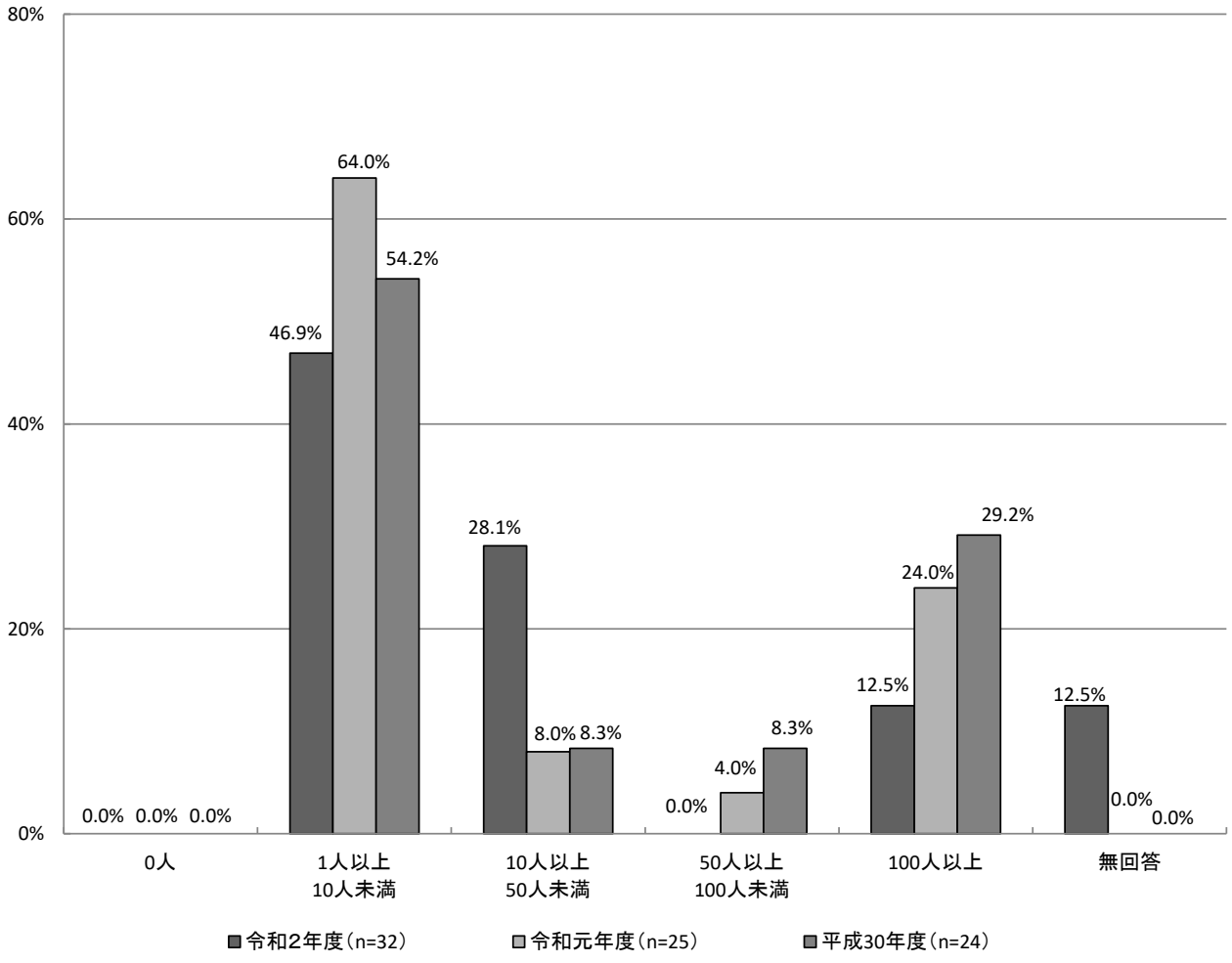


5.3.2　研究開発に携わっている人数　【A-問7】

【経年変化】
全体、企業及び大学では、昨年度より「10人以上50人未満」が最も増加している。

【経年変化(全体)】
昨年度と比較すると全体では、「10人以上50人未満」が20.1ポイント増加している。一方、「1人以上10人未満」は17.1ポイント減少している。

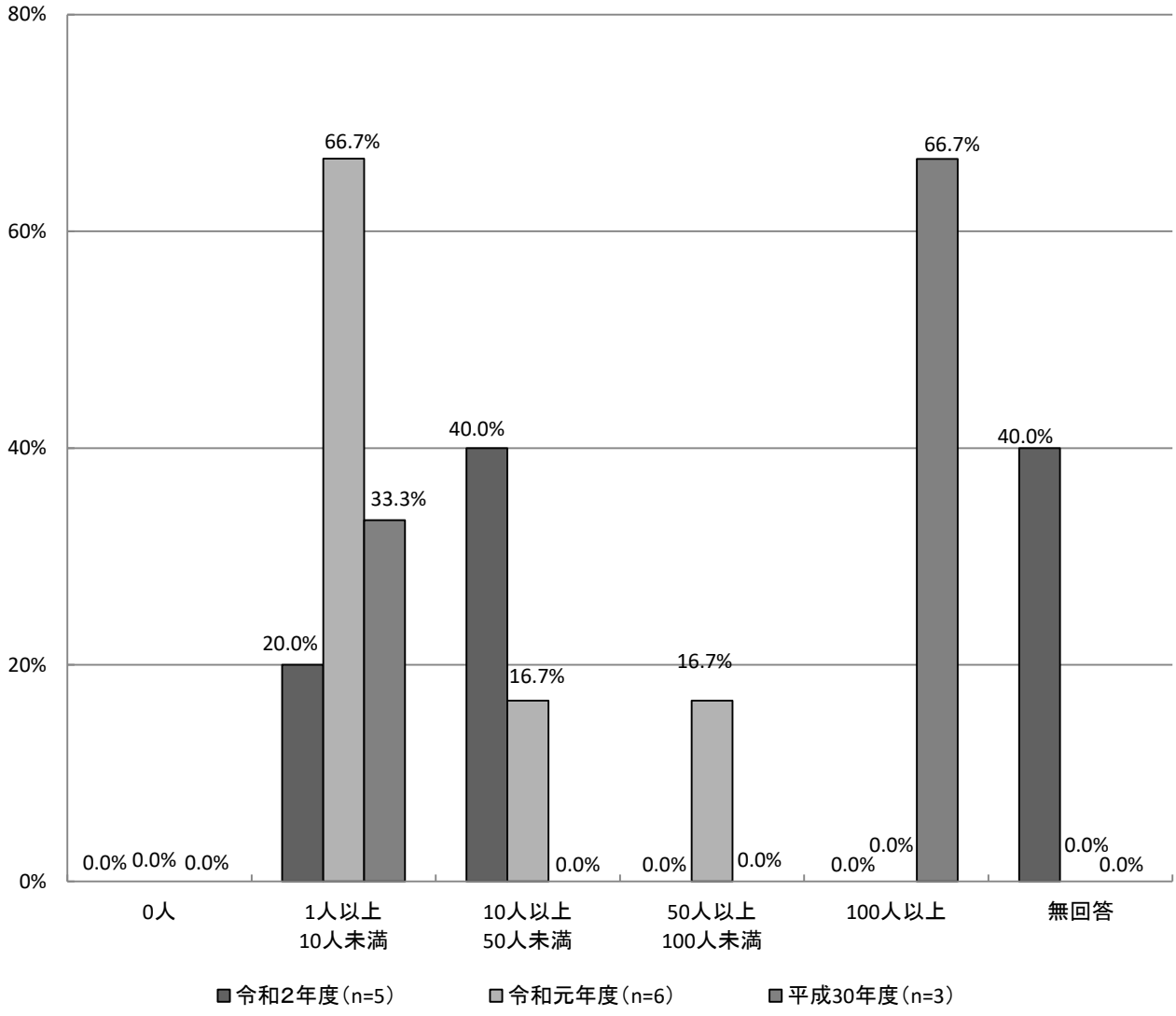
【経年変化(全体)】研究開発に携わっている人数(SA)



【経年変化(企業)】

昨年度と比較すると企業では、「10人以上50人未満」が23.3ポイント増加している。一方、「1人以上10人未満」は46.7ポイント減少している。

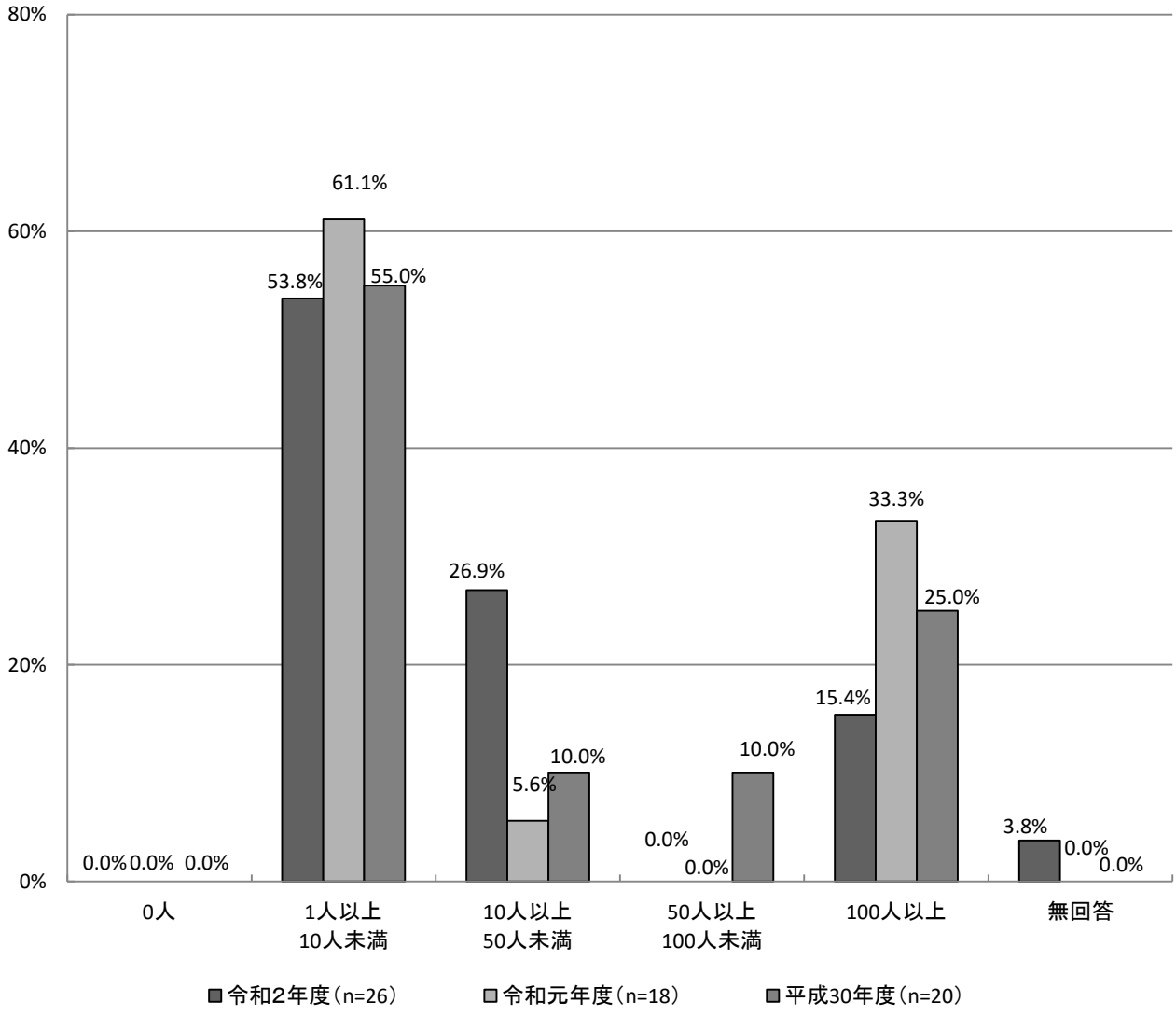
【経年変化(企業)】研究開発に携わっている人数(SA)



【経年変化(大学)】

昨年度と比較すると大学では、「10人以上50人未満」が21.3ポイントと最も増加している。一方「100人以上」は17.9ポイント減少している。

【経年変化(大学)】研究開発に携わっている人数(SA)



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。

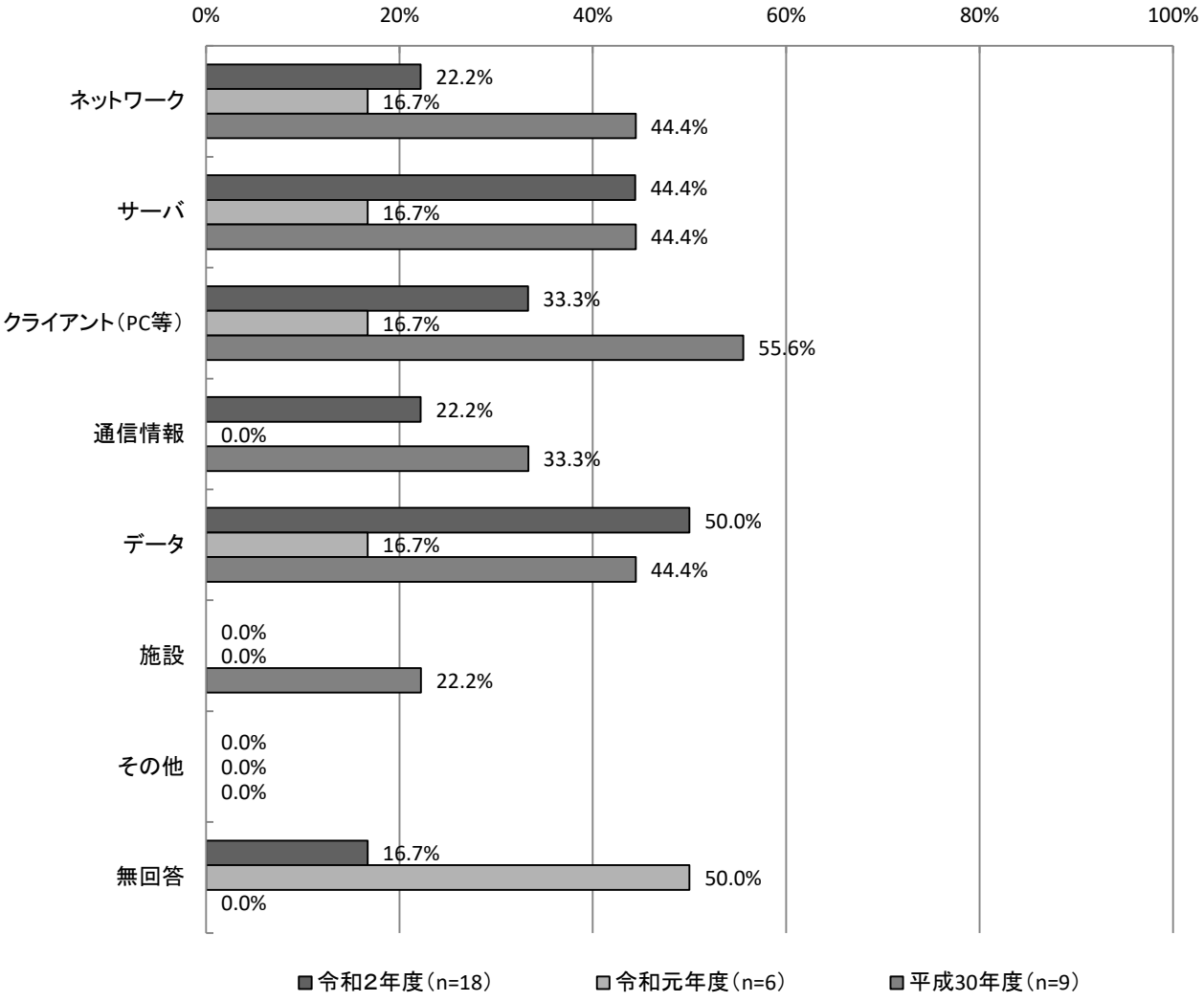
5.4.1　何を守るか？

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、「サーバ」が44.4％（8件）で最も多く、次いで「クライアント（PC等）」が33.3％（6件）となっている。

昨年度と比較すると、「データ」が33.3ポイント、「サーバ」が27.7ポイント、「通信情報」が22.2ポイント、「クライアント（PC等）」が16.6ポイント、「ネットワーク」が5.5ポイント増加しており、減少している項目はなかった。

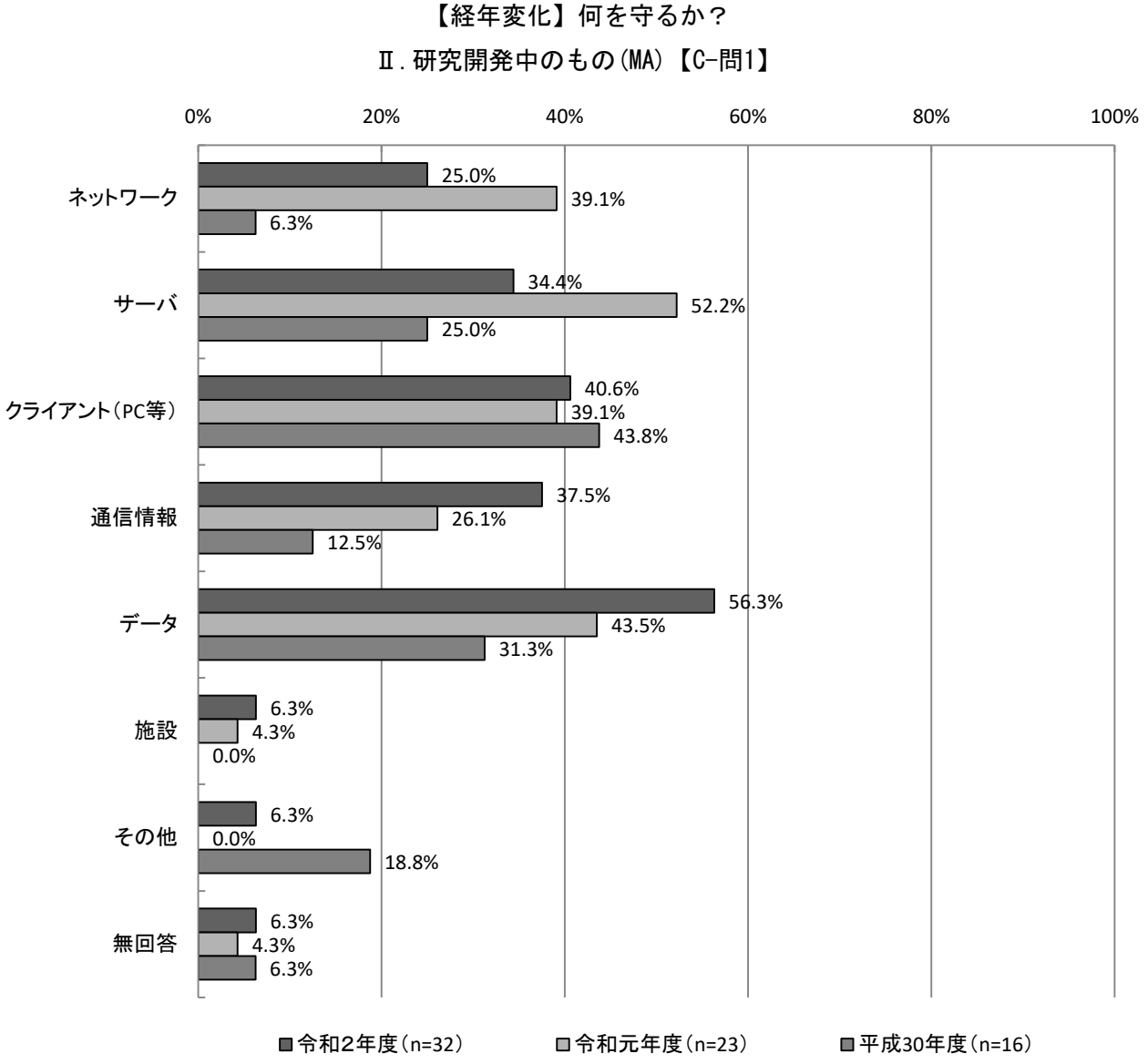
Ⅰ.実用化(製品化)されているもの(MA)【B-問1】



Ⅱ.研究開発中のもの

研究開発中のものについては、「データ」が56.3%（18件）で最も多く、次いで「クライアント（PC等）」が40.6%（13件）、「情報通信」が37.5%（12件）となっている。

昨年度と比較すると、「サーバ」が17.8ポイントと最も減少しており、次いで「ネットワーク」が14.1ポイント減少している。



5.4.2　何から保護するか？

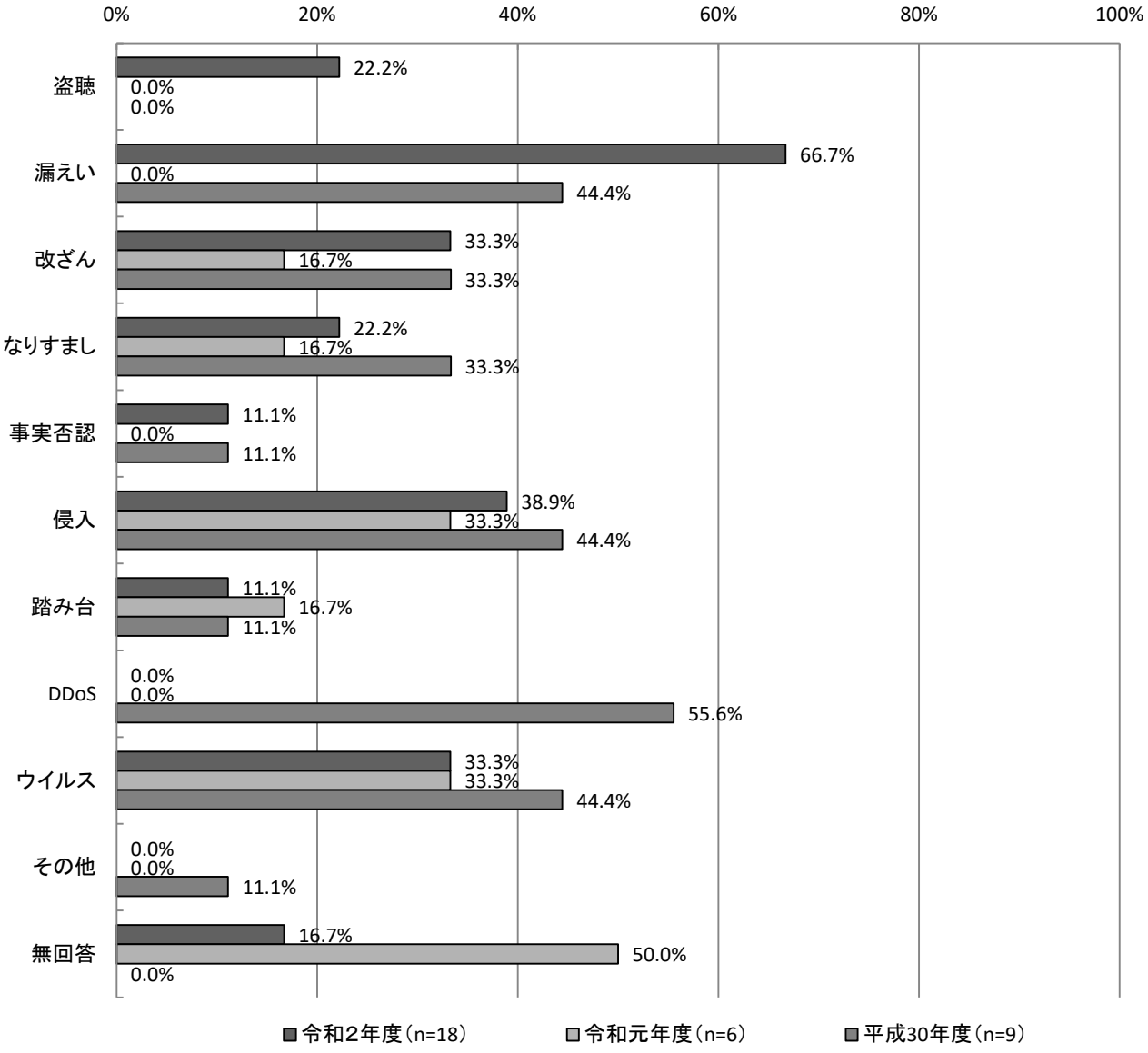
Ⅰ.実用化(製品化)されているもの

実用化（製品化）されているものについては、「漏えい」が66.7%（12件）で最も多く、次いで「侵入」が38.9%（7件）となっている。

昨年度と比較すると、「漏えい」が66.7ポイントで最も増加しており、次いで「盗聴」が22.2ポイント増加している。一方「踏み台」は5.6ポイント減少している。

【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】



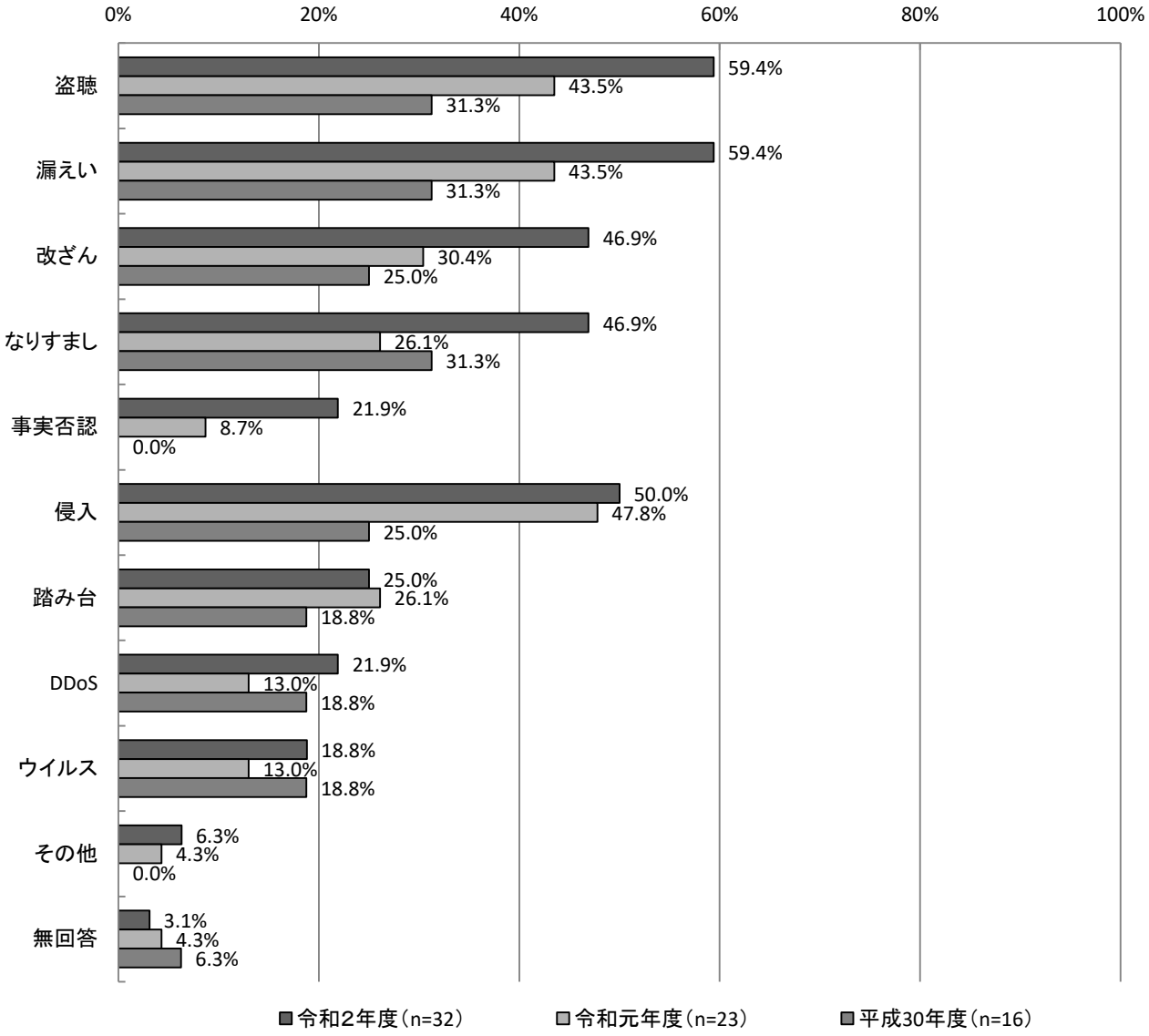
Ⅱ.研究開発中のもの

研究開発中のものについては、「盗聴」「漏えい」がそれぞれ59.4%（19件）で最も多く、次いで「侵入」が50.0%（16件）がとなっている。

昨年度と比較すると、「なりすまし」が20.8ポイントで最も増加しており、次いで「改ざん」が16.5ポイント増加している。一方「踏み台」は1.1ポイント減少している。

【経年変化】何から保護するか？

Ⅱ.研究開発中のもの(MA)【C-問2】



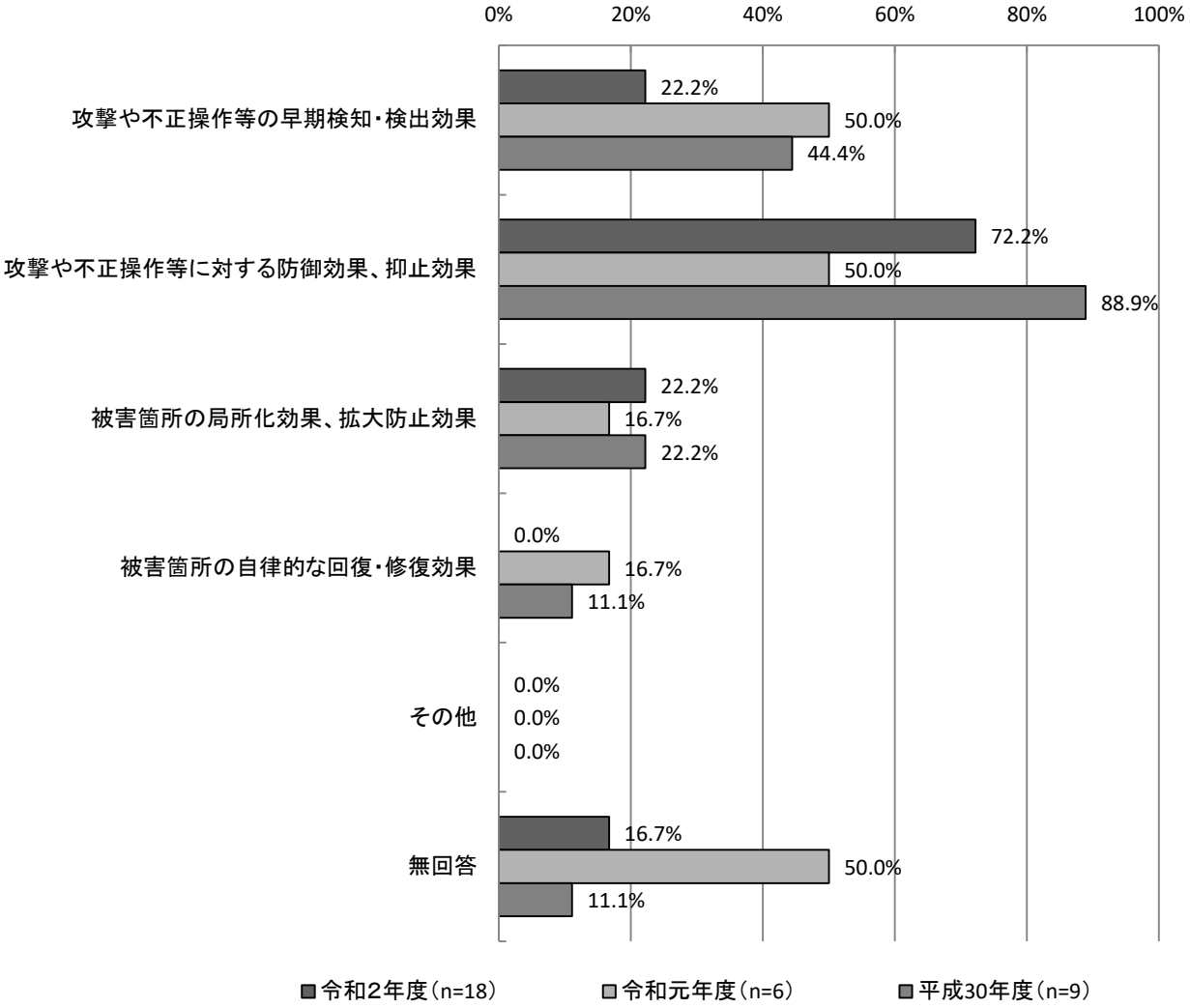
5.4.3　どのようなセキュリティ上の効果があるか？

Ⅰ.実用化(製品化)されているもの

実用化（製品化）されているものについては、「攻撃や不正操作等に対する防御効果、抑止効果」が72.2%（13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22.2ポイントと最も増加しており、一方「攻撃や不正操作等の早期検知・検出効果」が27.8ポイントと最も減少している。

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

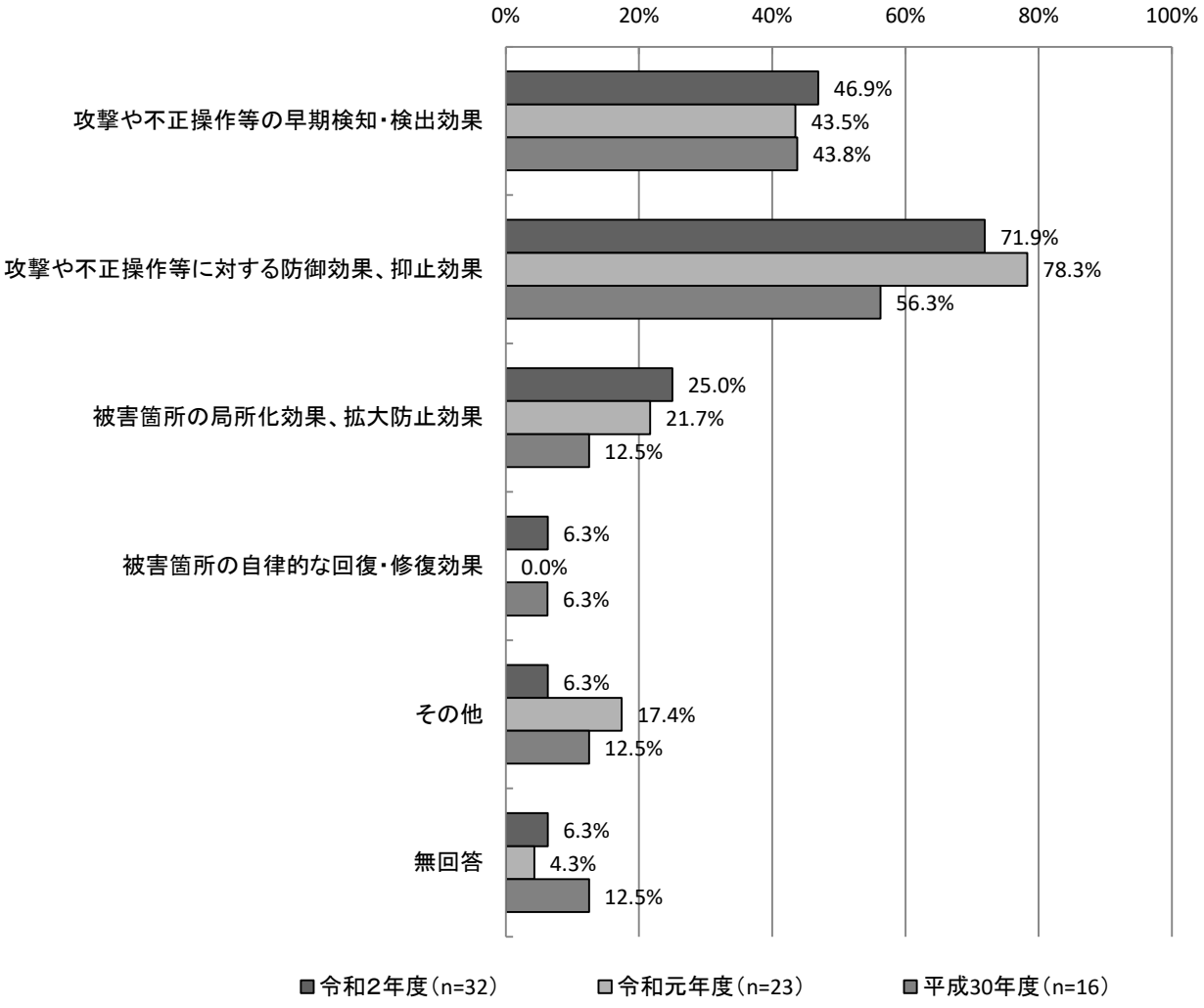


Ⅱ.研究開発中のもの

研究開発中のものについては、「攻撃や不正操作等に対する防御効果、抑止効果」が71.9%（23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46.9%（15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6.4ポイント減少している一方、「被害箇所の自律的な回復・修復効果」が6.3ポイント、「攻撃や不正操作等の早期検知・検出効果」が3.4ポイント、「被害箇所の局所化効果、拡大防止効果」が3.3ポイント増加している。

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



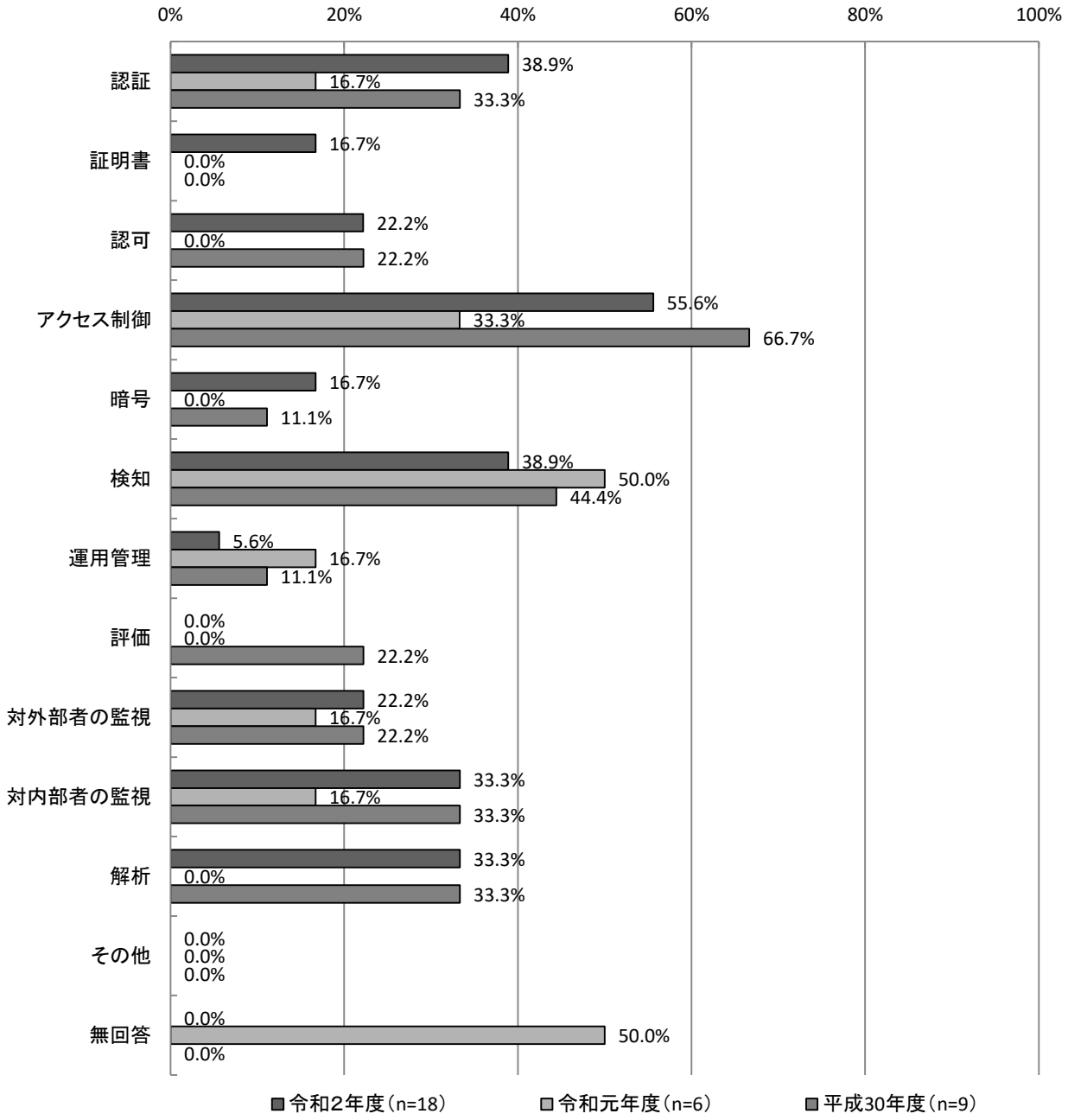
5.4.4　どのような機能を持つか？

Ⅰ.実用化(製品化)されているもの

実用化（製品化）されているものについては、「アクセス制御」が55.6%（10件）で最も多く、次いで「認証」「検知」がそれぞれ38.9%（7件）となっている。

昨年度と比較すると、「解析」が33.3ポイントと最も増加しており、次いで「アクセス制御」が22.3ポイント、「認証」「認可」がそれぞれ22.2ポイント増加している。一方「検知」「運用管理」はそれぞれ11.1ポイントと最も減少している。

【経年変化】どのような機能を持つか？
Ⅰ.実用化(製品化)されているもの(MA)【B-問4】



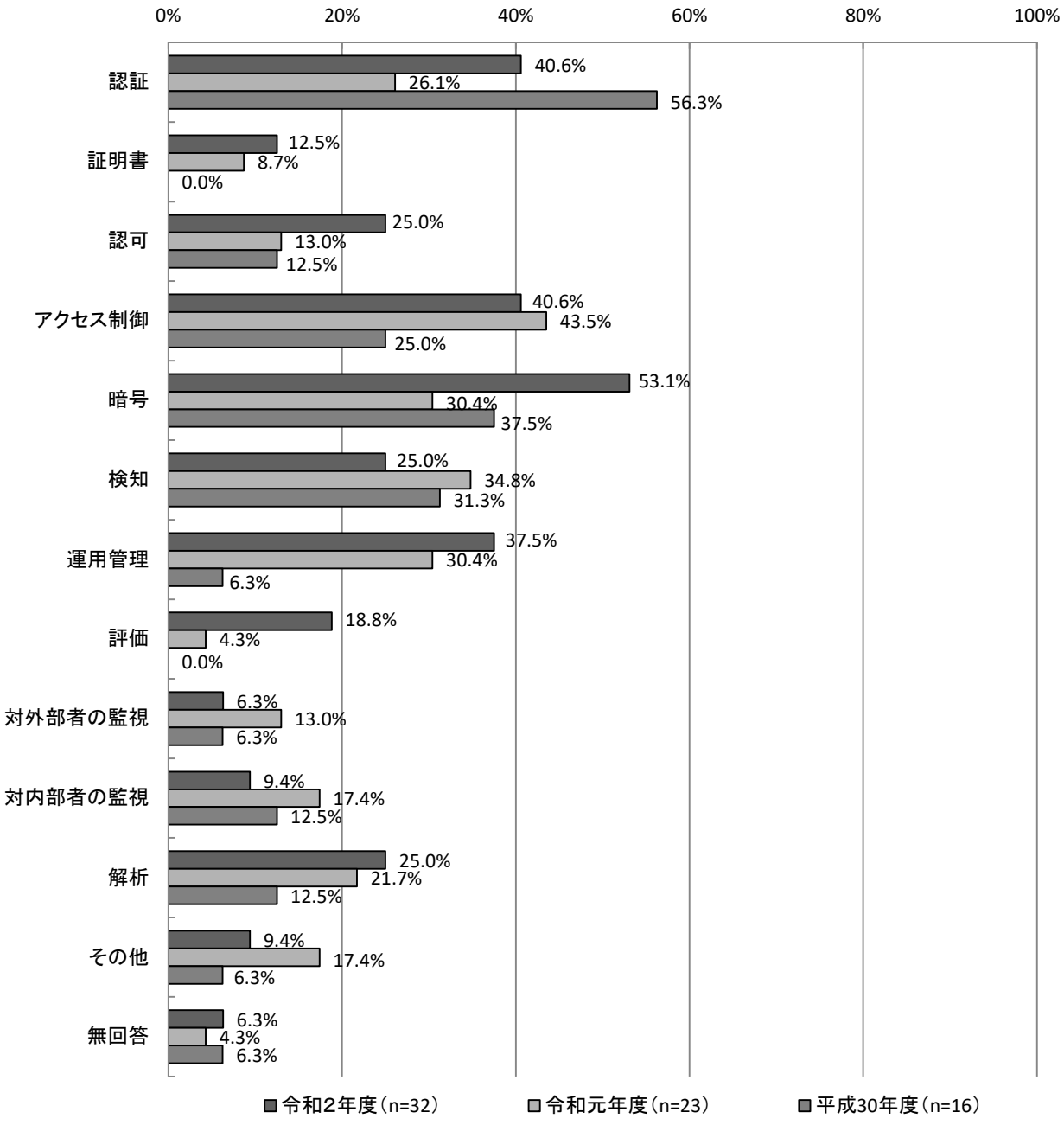
Ⅱ.研究開発中のもの

研究開発中のものについては、「暗号」が53.1%（17件）で最も多く、次いで「認証」「アクセス制御」がそれぞれ40.6%（13件）となっている。

昨年度と比較すると、「暗号」が22.7ポイントと最も増加しており、次いで「認証」「評価」が14.5ポイント増加している。一方「検知」が9.8ポイントと最も減少している。

【経年変化】どのような機能を持つか？

Ⅱ.研究開発中のもの(MA)【C-問4】



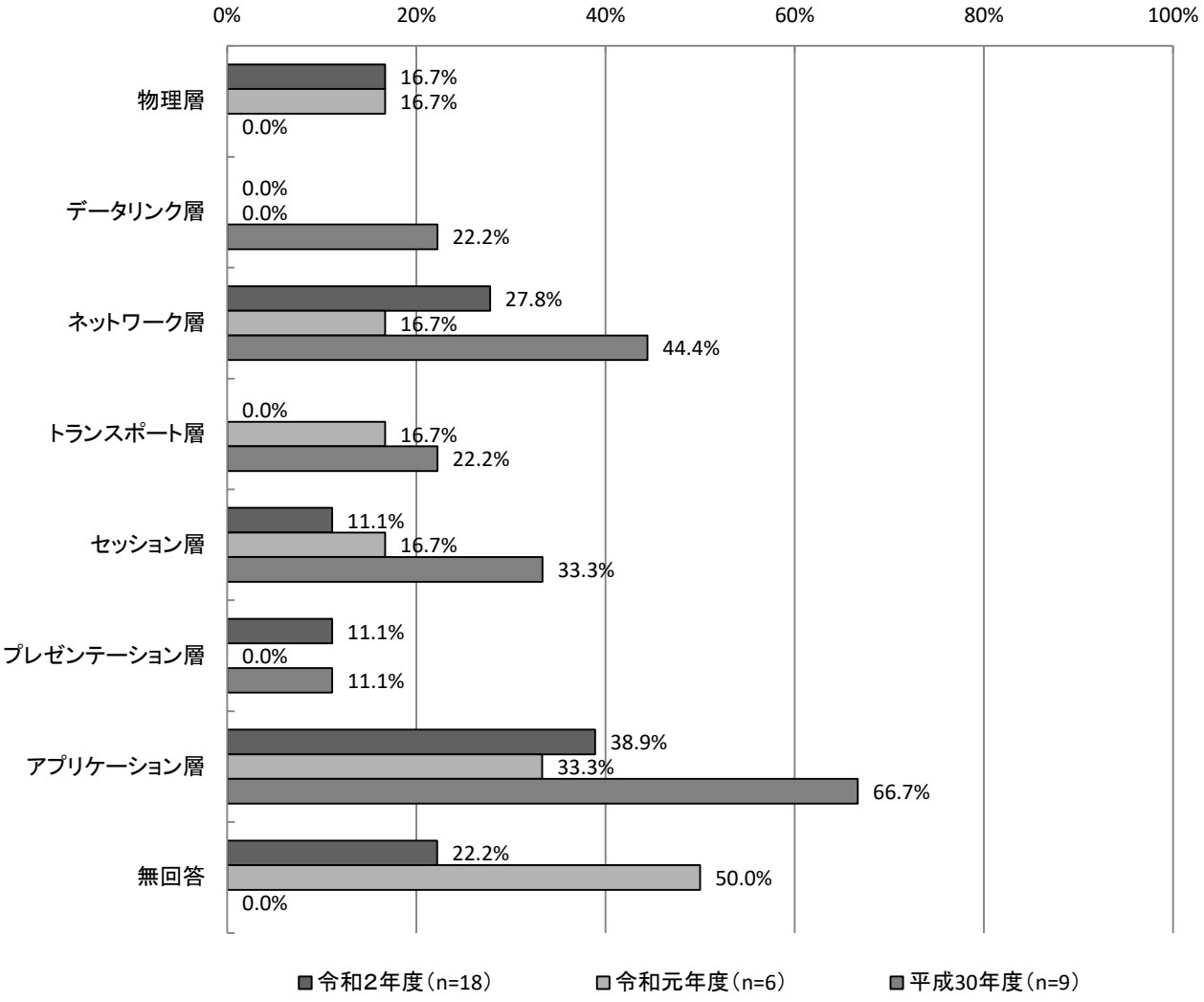
5.4.5　どのようなレイヤーのセキュリティを守るか？

Ⅰ.実用化(製品化)されているもの

実用化（製品化）されているものについては、「アプリケーション層」が38.9%（7件）で最も多く、次いで「ネットワーク層」が27.8%（5件）となっている。

昨年度と比較すると、「ネットワーク層」「プレゼンテーション層」がそれぞれ11.1ポイントと最も増加しており、「トランスポート層」は16.7ポイントと最も減少している。

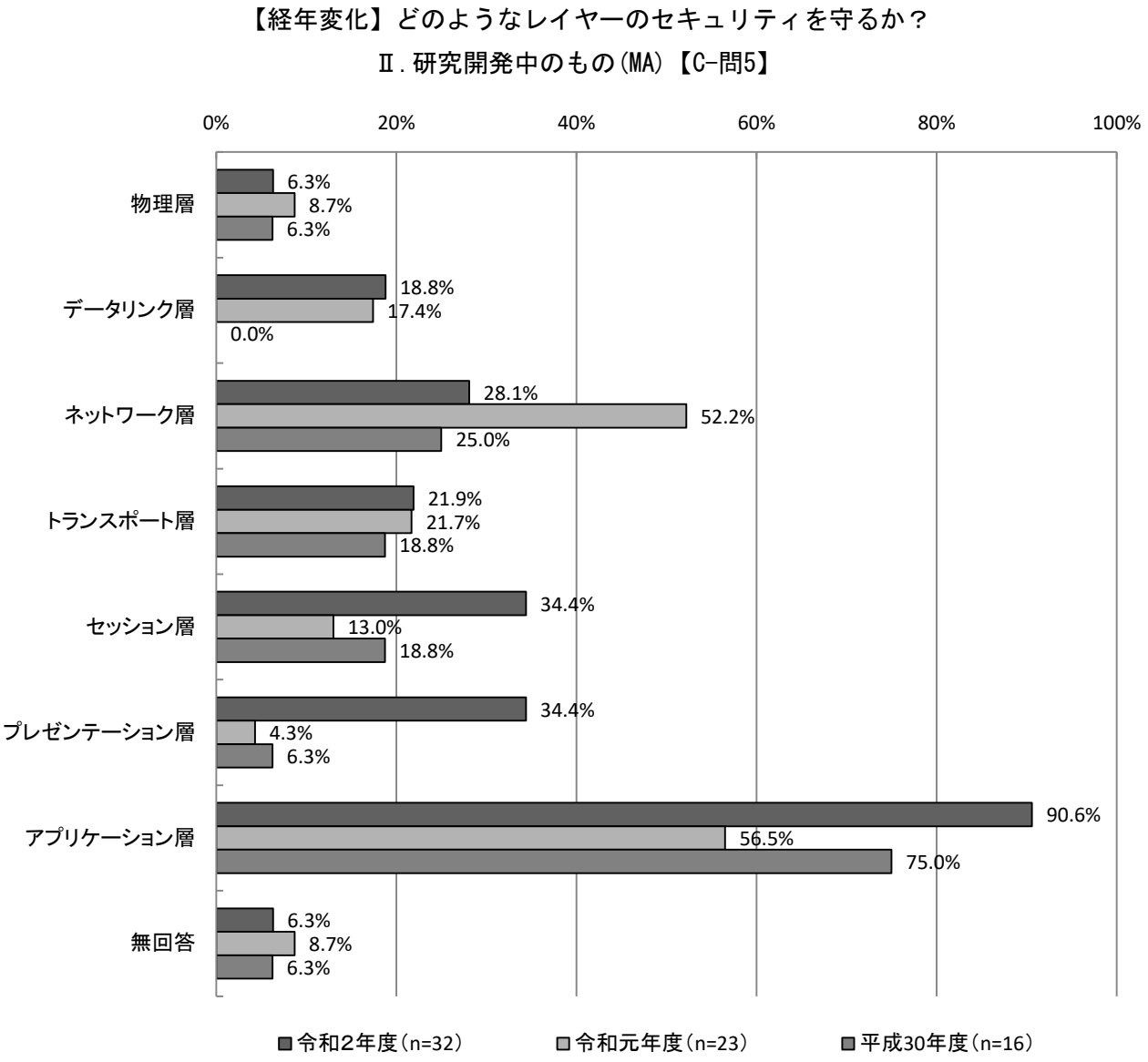
【経年変化】どのようなレイヤーのセキュリティを守るか？
Ⅰ.実用化(製品化)されているもの(MA)【B-問5】



Ⅱ.研究開発中のもの

研究開発中のものについては、「アプリケーション層」が90.6%（29件）で最も多く、次いで「セッション層」「プレゼンテーション層」がそれぞれ34.4%（11件）となっている。

昨年度と比較すると、「アプリケーション層」が34.1イントと最も増加しており、次いで「プレゼンテーション層」が30.1ポイント増加している。一方「ネットワーク層」が24.1ポイント減少している。



5.4.6　不正アクセスからの防御対象

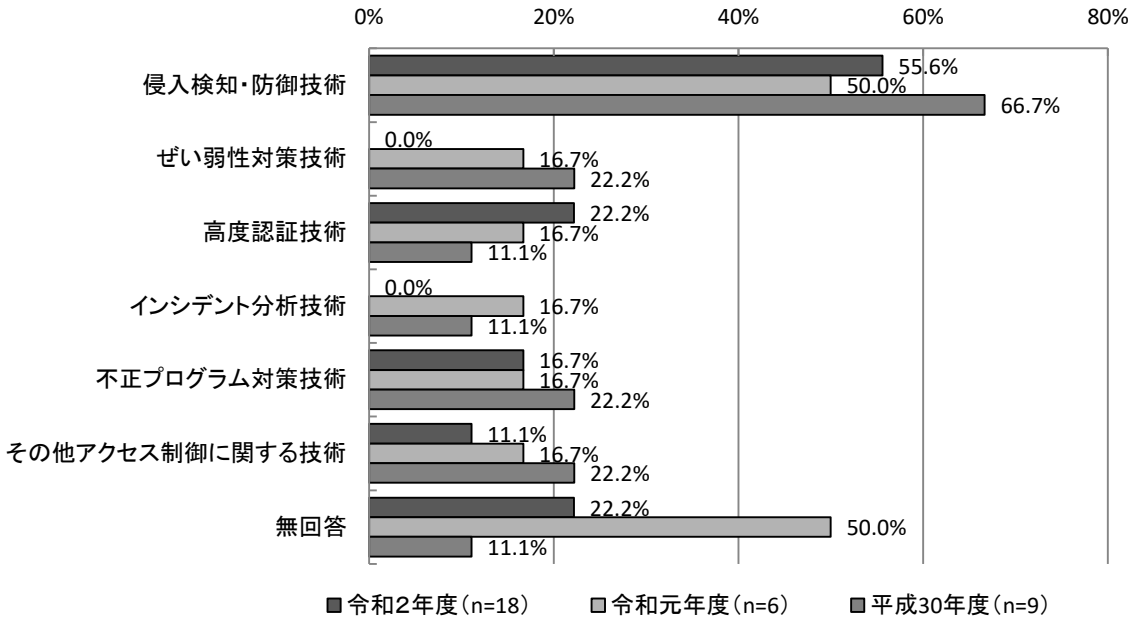
Ⅰ.実用化(製品化)されているもの

実用化（製品化）されているものについては、「侵入検知・防御技術」が55.6%（10件）で最も多くなっている。

昨年度と比較すると、「ぜい弱性対策技術」「インシデント分析技術」がそれぞれ16.7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】



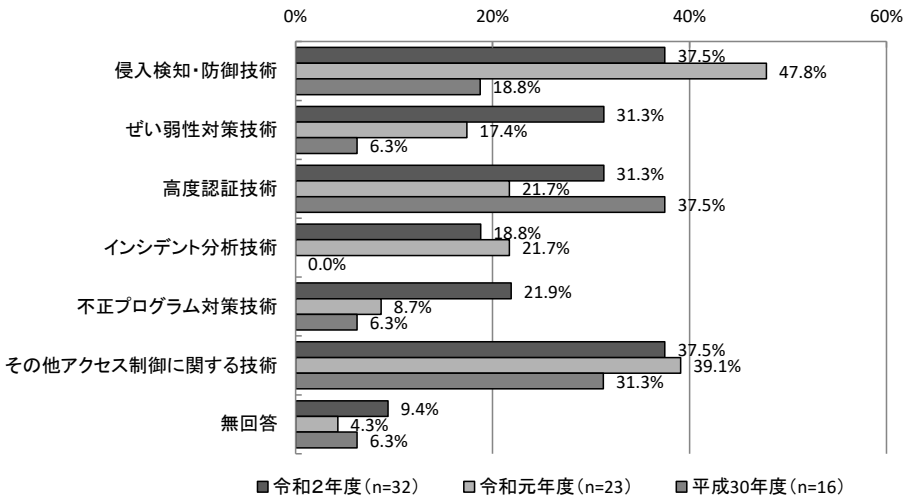
Ⅱ.研究開発中のもの

研究開発中のものについては、「侵入検知・防御技術」が37.5%（12件）で最も多くなっている。

昨年度と比較すると、「ぜい弱性対策技術」が13.9ポイントと最も増加しており、次いで「高度認証技術」が9.6ポイント増加している。

【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？

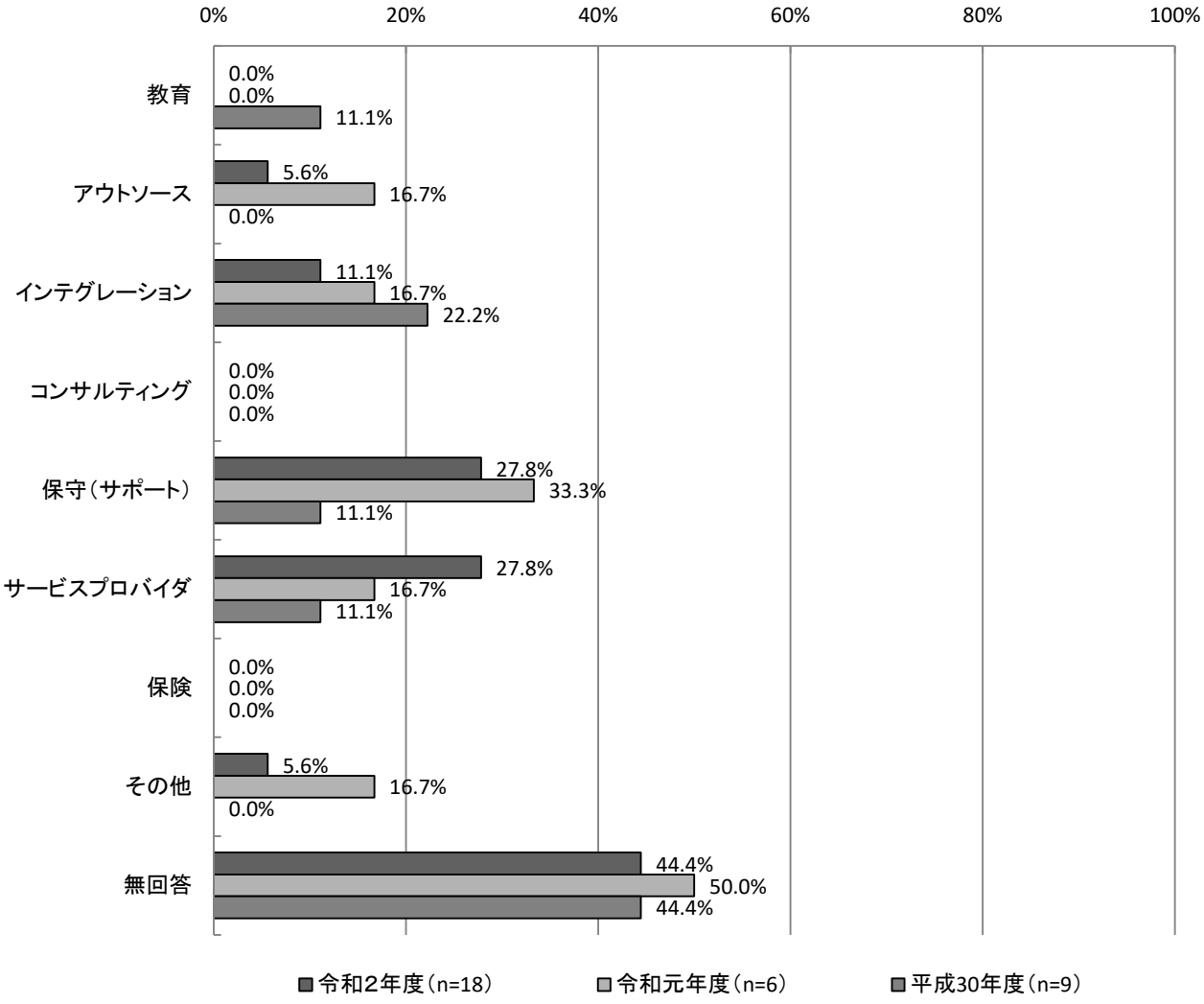
Ⅰ.実用化(製品化)されているもの

実用化（製品化）されているものについては、「保守（サポート）」「サービスプロバイダ」が27.8%（5件）、「インテグレーション」が11.1%（2件）、「アウトソース」が5.6%（1件）となっている。

昨年度と比較すると、「サービスプロバイダ」が11.1ポイントと最も増加している。

【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】



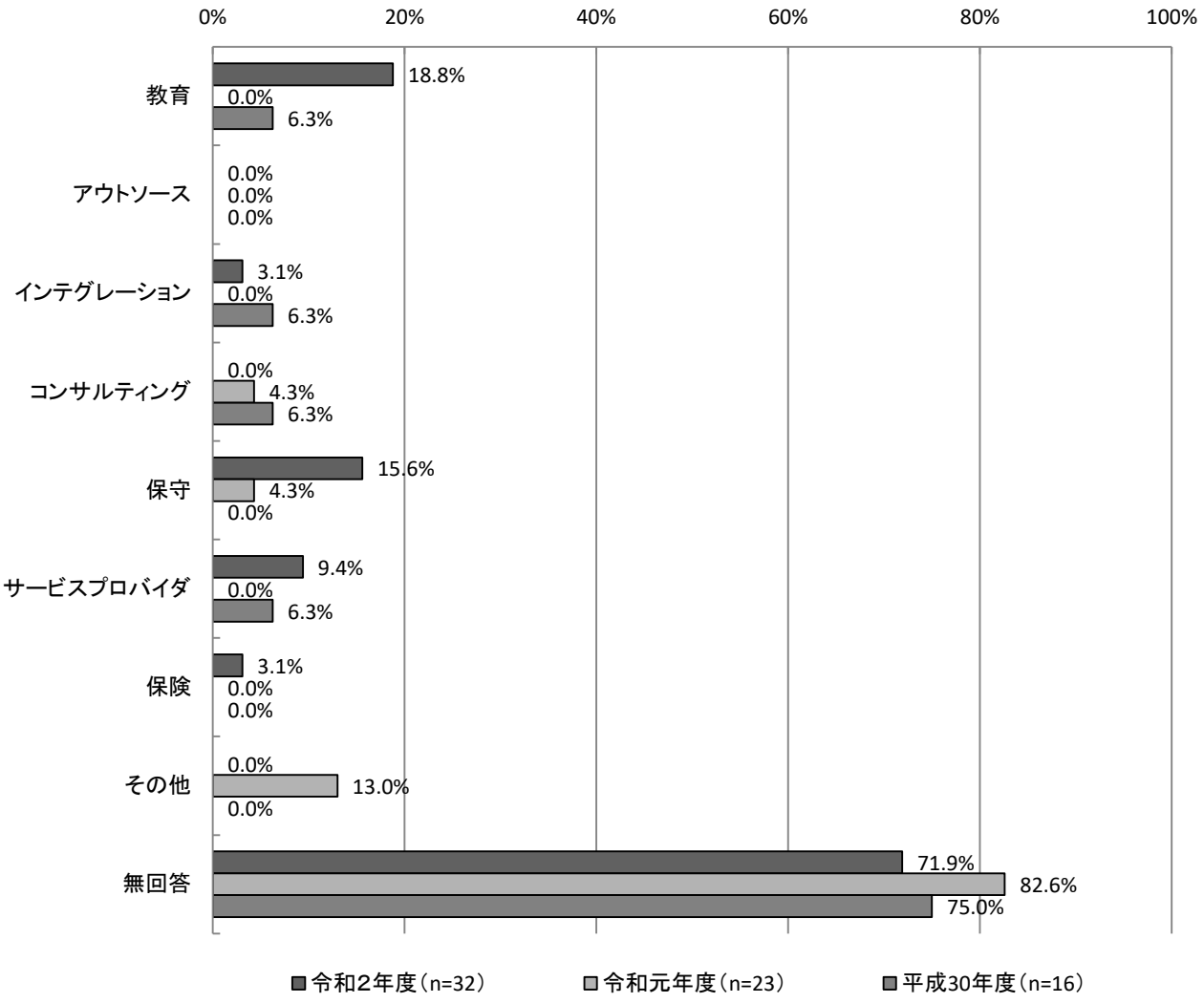
Ⅱ.研究開発中のもの

研究開発中のものについては、「教育」が18.8%（6件）、「保守」が15.6%（5件）、「サービスプロバイダ」が9.4%（3件）、「インテグレーション」が3.1%（1件）となっている。

昨年度と比較すると、「教育」が18.8ポイントと最も増加しており、次いで「保守」が11.3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】

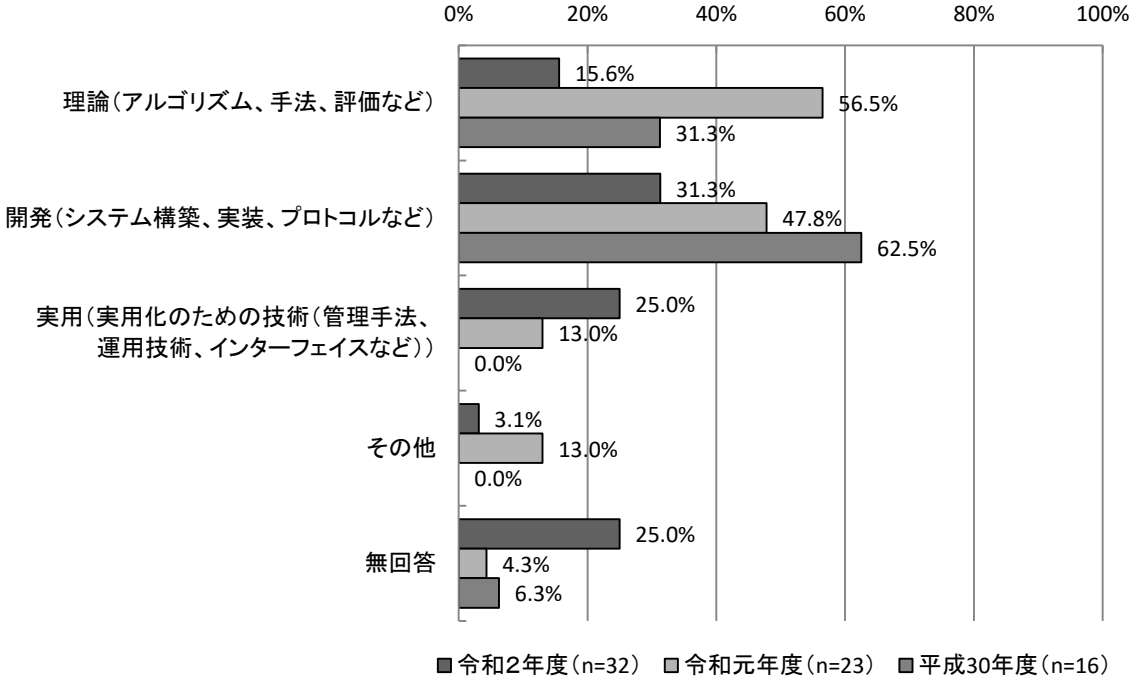


5.5　研究開発の成果としてどのようなものを目指しているか？

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31.3%（10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25.0%（8件)、「理論（アルゴリズム、手法、評価など)」が15.6%（5件）となっている。

昨年度と比較すると、「理論（アルゴリズム、手法、評価など)」が40.9ポイント減少しており、一方「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))」は12.0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】

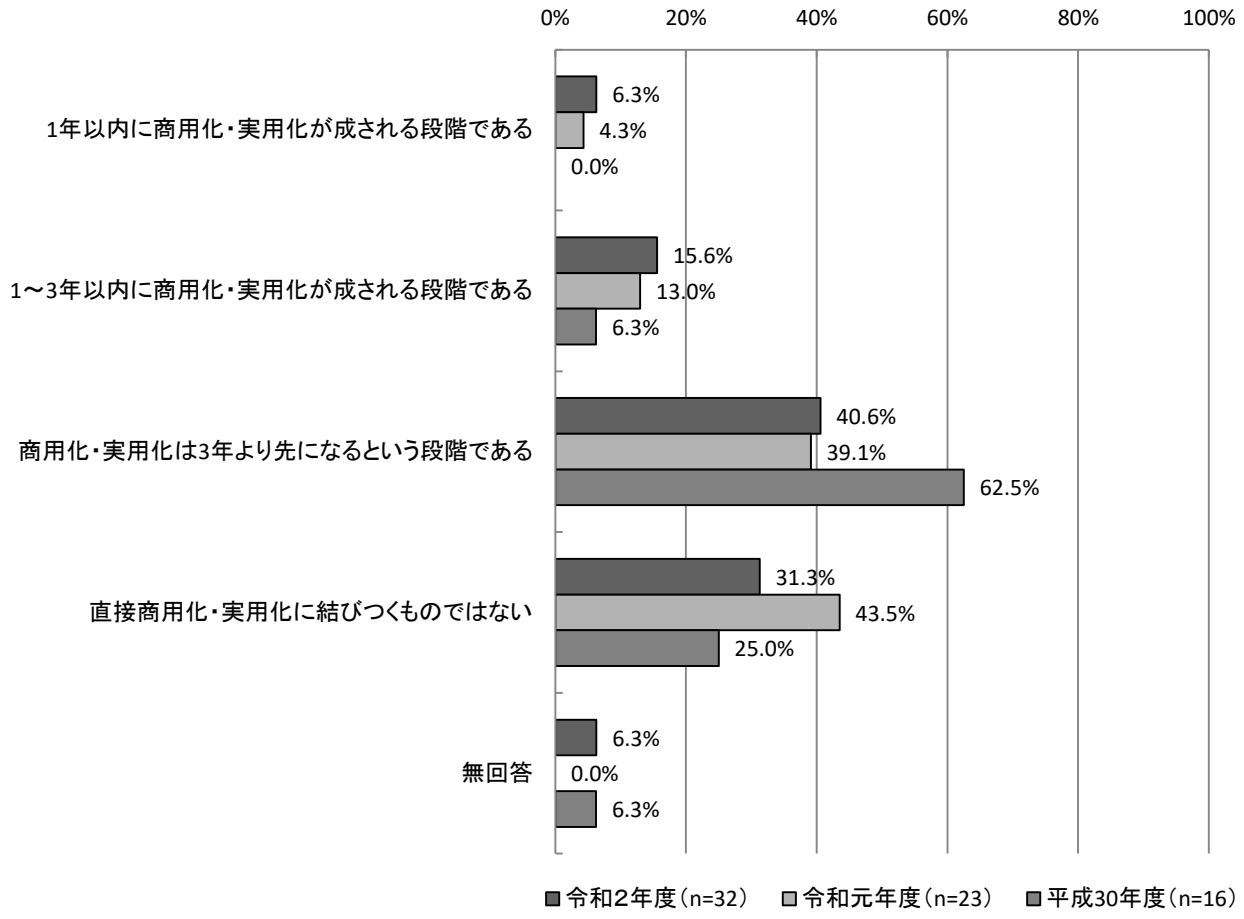


5.6　研究開発の進捗状況

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40.6%（13件）で最も多く、次いで「直接商用化・実用化に結びつくものではない」が31.3%（10件）となっている。

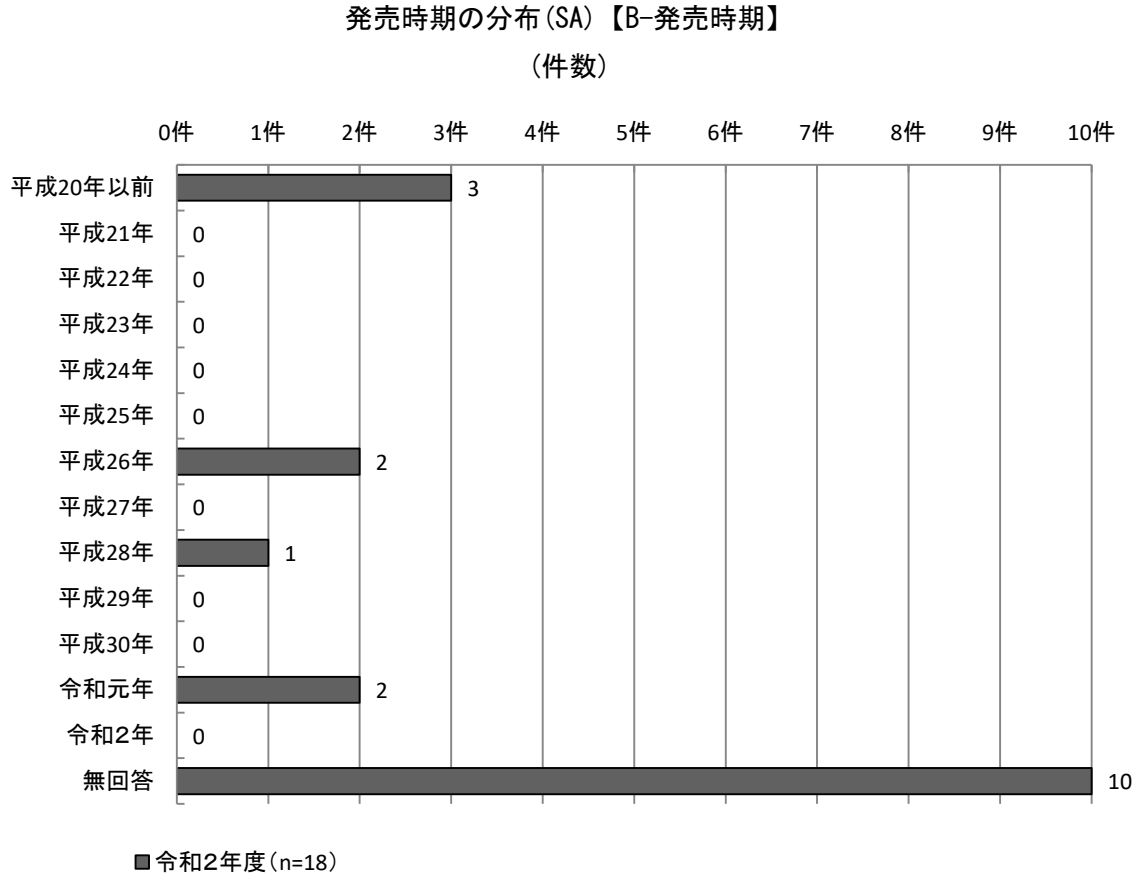
昨年度と比較すると、「1～3年以内に商用化・実用化が成される段階である」が2.6ポイントと最も増加している。一方「直接商用化・実用化に結びつくものではない」が12.2ポイントと最も減少している。

研究開発の進捗状況(SA)【C-問9】



5.7　発売時期の分布

発売時期については、「平成20年以前」が3件で最も多く、次いで「平成26年」「令和元年」が2件、「平成28年」が1件となっている。

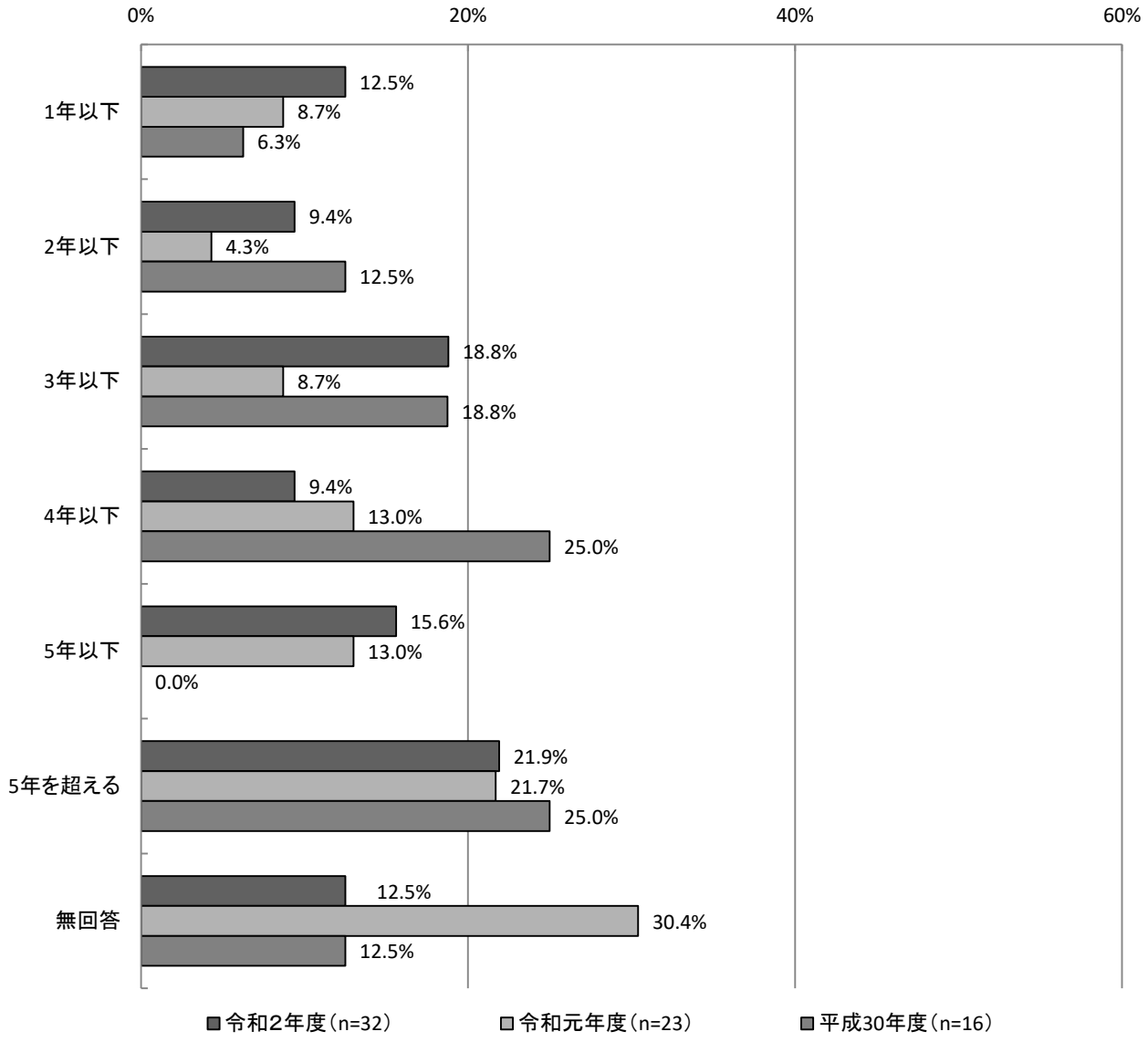


5.8　研究開発期間の分布

研究開発期間については、「5年を超える」が21.9%（7件）で最も多く、次いで「3年以下」が18.8%（6件）となっている。

昨年度と比較すると、「3年以下」が10.1ポイントと最も増加している。一方「4年以下」は3.6ポイント減少している。

研究開発期間の分布(SA)【C-研究開発期間】



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
ED-SV4	（株）アイオーデータ機器	アイオーデータ機器						
ED-HB3	（株）アイオーデータ機器	アイオーデータ機器			○			
ED-FP	（株）アイオーデータ機器	アイオーデータ機器			○			
トレンドマイクロ　ウィルスバスター	正栄食品工業株式会社	トレンドマイクロ	○				○	
ＺＡＣ／ＲｅｆｏｒｍａＰＳＡ	株式会社オロ	株式会社オロ						
Ａｃｃｏｕｎｔ@Ａｄａｐｔｅｒ	兼松株式会社	日立ソリューションズ株式会社	○					

※ 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
安全なＩｏＴサービスを実現するための総合セキュリティ対策技術	神奈川工科大学	セキュリティ研究センター	○	○	○			
名称　特になし	学校法人　上智学院	暗号						○
カオス暗号の研究	学校法人君が淵学園（崇城大学）	崇城大学情報学部						
ネットワークセキュリティ、情報ネットワーク技術に関する研究	東京情報大学	ネットワークシステム研究室	○	○		○	○	
多要素認証技術	学校法人　北海道科学大学	北海道科学大学			○			
耐量子計算機暗号プロトコル	佐賀大学理工学部	佐賀大学理工学部　廣友研究室			○			
（名前なし）	国立大学法人名古屋大学	情報基盤センター　情報基盤ネットワーク研究部門	○	○		○	○	○
セキュア電子メール秘密映像伝送、クラウドデータ保管	東京電機科学大学　総合研究所　サイバー・セキュリティ研究所	東京電機大学　総合研究所　サイバーセキュリティ―研究所						○
ストリーム暗号	石巻専修大学	理工学部情報電子工学科						○
遠隔健康支援システム	八戸工業大学	ネットワークセキュリティ	○					
JST CREST ビッグデータ統合利用のためのセキュアなコンテンツ共有・流通基盤の構築	国立大学法人お茶の水女子大学	お茶の水女子大学　小口研究室		○				
遠隔通信ロバストネステスト	学校法人 中央大学	国際情報学部		○				
パスワード共有システム	福岡大学	福岡大学情報基盤センター研究開発室（中國研究室）						○
Raspberry Gate	国立大学法人金沢大学	総合メディア基盤センター	○					
Privacy-preserving smart contracts on blockchains	国立大学法人金沢大学	理工研究域電子情報通信学系			○			
人間社会のセキュリティ構造を模倣したIoT向け運用モデルの開発	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						○

※ 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）アイオーデータ機器
代表者名	
所在地	
窓口部署名	
電話番号	
ホームページのURL	
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： ED-SV4 開発元(メーカー名等)： アイオーデータ機器 開発国： 価格： ¥9,200～￥32,200 （容量による） 発売時期： 平成26年6月～ 出荷数：	パスワードロックとアンチウイルス機能を備えたＵＳＢメモリー

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）アイオーデータ機器
代表者名	
所在地	
窓口部署名	
電話番号	
ホームページのURL	
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： ED-HB3 開発元(メーカー名等)： アイオーデータ機器 開発国： 価格： オープン 発売時期： 令和元年6月～ 出荷数：	パスワードボタン付きＵＳＢメモリー

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）アイオーデータ機器
代表者名	
所在地	
窓口部署名	
電話番号	
ホームページのURL	
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： ED-FP 開発元(メーカー名等)： アイオーデータ機器 開発国： 価格： オープン 発売時期： 令和元年6月～ 出荷数：	指紋認証によるログイン機能を備えたＵＳＢメモリー

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	正栄食品工業株式会社
代表者名	本多市郎
所在地	〒110-8723 東京都台東区秋葉原5番7号
窓口部署名	総務部総務課
電話番号	03-3253-1211
ホームページのURL	
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： 　　トレンドマイクロ　ウィルスバスター 開発元(メーカー名等)： 　　トレンドマイクロ 開発国： 　　日本 価格： 発売時期： 出荷数： 	

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	株式会社オロ
代表者名	川田　篤
所在地	〒153-0063 東京都目黒区目黒3-9-1　目黒須田ビル
窓口部署名	コーポレート本部
電話番号	03-5724-7001
ホームページのURL	https://www.oro.com
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： ＺＡＣ／ＲｅｆｏｒｍａＰＳＡ 開発元(メーカー名等)： アイオーデータ機器 開発国： 株式会社オロ 価格： 約3,200,000円 （ソフトウエア価格） 発売時期： 平成18年～ 出荷数： 1,000	Ｗｅｂブラウザから弊社サーバ（クラウド）にアクセスし、ＥＲＰ各種機能を利用。ＨＴＴＰＳ通信により、通信を暗号化。ログイン時は、ユーザ名・パスワードにより認証。アカウントロックの条件は、利用各社がマスタで設定。別途オプションとして、ＧｏｏｇｌｅアカウントＳＡＭＬ方式によるサインイン連携を提供。

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	兼松株式会社
代表者名	谷川　薫
所在地	〒105-8005 東京都港区芝浦1-2-1　シーバンスＮ館
窓口部署名	
電話番号	03-5440-8111
ホームページのURL	https://www.kanematsu.co.jp
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： Ａｃｃｏｕｎｔ＠Ａｄａｐｔｅｒ 開発元(メーカー名等)： 日立ソリューションズ株式会社 開発国： 日本 価格： オープン 発売時期： 出荷数： 不明	・ＭＡＣアドレス認証により、予め登録されたＰＣ端末以外の社内ネットワーク接続を防止する製品。 ・制御機能によるネットワーク遅延が発生しない仕様。

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○を付与している

企業・大学名	神奈川工科大学
代表者名	
所在地	〒243-0292 厚木市下荻野1030
窓口部署名	
電話番号	
関連部門名	セキュリティ研究センター
ホームページのURL	
研究説明のURL	
対象技術	技術の概要・特徴など
研究開発名称： 安全なＩｏＴサービスを実現するための総合セキュリティ対策技術 研究開発国： 研究開発時期： 令和2年4月1日～ 令和5年3月31日	

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　上智学院
代表者名	佐久間　勤
所在地	〒102-8554 千代田区紀尾井町7-1
窓口部署名	上智大学　総務局　広報グループ
電話番号	03-3238-3179
関連部門名	暗号
ホームページのURL	www.sophia.ac.jp
研究説明のURL	
対象技術	技術の概要・特徴など
研究開発名称： 名称　特になし 研究開発国： 日本 研究開発時期： 平成30年4月～	秘密分散法のデータサイズに関する理論的研究。・シェアの生成法。・シェアサイズの見積り）に関する基礎研究を行なっている。

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	学校法人君が淵学園（崇城大学）
代表者名	理事長　中山峰男
所在地	〒860-0082 熊本市西区池田4-22-1
窓口部署名	地域共創センター
電話番号	096-326-3418
関連部門名	崇城大学情報学部
ホームページのURL	https://www.sojo-u.ac.jp
研究説明のURL	
対象技術	技術の概要・特徴など
研究開発名称： カオス暗号の研究 研究開発国： 日本 研究開発時期： 平成24年4月1日～	簡単な規則に基づくカオスを応用したＩｏＴ向け暗号を設計中である。

不正アクセスからの防御対象	
侵入検知・防御技術	
ぜい弱性対策技術	
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
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	学長　鈴木　昌治
所在地	〒265-8501 千葉市若葉区御成台4-1
窓口部署名	総務課
電話番号	043-236-4603
関連部門名	ネットワークシステム研究室
ホームページのURL	http://www.tuis.ac.jp
研究説明のURL	
対象技術	技術の概要・特徴など
研究開発名称： ネットワークセキュリティ、情報ネットワーク技術に関する研究 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	学校法人　北海道科学大学
代表者名	北海道科学大学　学長　渡辺泰裕
所在地	〒006-8585 北海道札幌市手稲区前田7条15丁目4-1
窓口部署名	入試　地域連携部研究推進課
電話番号	011-688-2241
関連部門名	北海道科学大学
ホームページのURL	https://www.hus.ac.jp
研究説明のURL	
対象技術	技術の概要・特徴など
研究開発名称： 多要素認証技術 研究開発国： 日本 研究開発時期： 平成28年4月～令和2年9月	基礎的な技術の実現可能性に対する初期検討段階

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	佐賀大学理工学部
代表者名	理工学部長　豊田　一彦
所在地	〒840-8502 佐賀市本庄町1
窓口部署名	
電話番号	
関連部門名	佐賀大学理工学部　廣友研究室
ホームページのURL	
研究説明のURL	
対象技術	技術の概要・特徴など
研究開発名称： 耐量子計算機暗号プロトコル 研究開発国： 日本 研究開発時期： 平成31年4月1日～	量子コンピュータの解読に耐性のある暗号プロトコルを開発した。仕様は論文として発表している。計算量、通信量の評価を行っている

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	国立大学法人名古屋大学
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	情報基盤センター　情報基盤ネットワーク研究部門
ホームページのURL	
研究説明のURL	https://www.net.nagoya-u.ac.jp/menber/shimada./
対象技術	技術の概要・特徴など
研究開発名称： （名前なし） 研究開発国： 日本 研究開発時期： 平成25年4月1日～	ＵＲＬから概要や発表文献を見て下さい。

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

企業・大学名	東京電機科学大学総合研究所 サイバー・セキュリティ研究所
代表者名	
所在地	〒120-8551 東京都足立区千住旭町5番
窓口部署名	
電話番号	
関連部門名	東京電機大学総合研究所サイバーセキュリティ―研究所
ホームページのURL	http://www.dendai.ac.jp/crc/
研究説明のURL	http://www.lab.ine.aj.dendai.ac.jp/wordpress/
対象技術	技術の概要・特徴など
研究開発名称： セキュア電子メール秘密映像伝送、クラウドデータ保管 研究開発国： 日本 研究開発時期： 平成19年3月6日～ 令和2年12月31日	秘密電子メール、秘密映像伝送技術、ならびにクラウドを活用したデータの安全分散保管技術に関しては、プロトタイプソフトウェアを試作し、技術展開が出来るレベルに達している。

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	石巻専修大学
代表者名	学長　尾池　守
所在地	〒986-8580 宮城県石巻市南境新水戸1
窓口部署名	事務部　事務課（学務担当）研究支援係
電話番号	0225-22-7716
関連部門名	理工学部情報電子工学科
ホームページのURL	https://www.senshu-u.ac.jp/ishinomaki/
研究説明のURL	https://astesj.cam/v05/i05/p09
対象技術	技術の概要・特徴など
研究開発名称： ストリーム暗号 研究開発国： 日本 研究開発時期： 平成28年4月1日～	主にストリーム暗号に関する研究を行っている。カオス・ニューラルネットワークを用いた乱数発生器を様々な組込みシステムへの応用を試み、通信データの暗号化・複合化の高速化を目指す。最近では車載ネットワークCAN向けのストリーム暗号を提案した。詳細は「研究内容の説明がされているURL」の論文をご参照してください。

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

企業・大学名	八戸工業大学
代表者名	学長　坂本　禎智
所在地	〒031-8501 青森県八戸市大字妙字大開88-1
窓口部署名	事務部　学事課
電話番号	0178-25-8111
関連部門名	ネットワークセキュリティ
ホームページのURL	syomu@hi-tech.ac.jp
研究説明のURL	https://www.hi-tech.ac.jp/profile/database.cgi?cmd=dp&num=18
対象技術	技術の概要・特徴など
研究開発名称： 遠隔健康支援システム 研究開発国： 日本 研究開発時期： 令和2年7月1日～ 令和3年1月29日	◎遠隔システム：在宅勤務者、および高齢者の方と遠隔でコミュニケーション（ビデオ会会議機能／チャット機能／録音・録画機能）を取るシステム（アプリ）をおいて、クラウドネットワークのセキュリティ構築方法を研究している。施設のケアスタッフは、呼出しがあった時、端末に発信者情報が自動でポップアップ表示され、発信者を確認出来る。また、発信者の蓄積データを選択して閲覧し、健康状態を推察できるように構築する。 ◎医療情報連携機能：バイタル機器と端末が連携しバイタル情報の収集・グラフ化を行い、サーバに通知する事で蓄積データを作成する。施設では、発信者情報を基に、各種蓄積データを閲覧する。 ◎研究開発状況：遠隔システム機能との連携で、サーバおよび端末の最新セキュアOSに対応したサーバの多層防御を想定し、不正プログラム対策・Webレピュテーション・IPS／IDSが可能な既存の製品を選択し、テストを行っている。サーバ保護に必要な複数の機能がオールインワンのSaaS型総合サーバセキュリティ機能を組み込むために、既存システムの改修部分を特定し、テストを実施する段階である。

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	国立大学法人お茶の水女子大学
代表者名	学長　室伏きみ子
所在地	〒112-8610 東京都文京区大塚2-1-1
窓口部署名	研究・産学連携課
電話番号	03-5978-5503
関連部門名	お茶の水女子大学　小口研究室
ホームページのURL	http://www.ocha.ac.jp/
研究説明のURL	https://www.yama.info.waseda.ac.jp/crest/
対象技術	技術の概要・特徴など
研究開発名称： JST CREST ビッグデータ統合利用のためのセキュアなコンテンツ共有・流通基盤の構築 研究開発国： 日本 研究開発時期： 平成27年10月1日～ 令和3年3月3日	

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 中央大学
代表者名	大村雅彦
所在地	〒192-0393 東京都八王子市東中野742-1
窓口部署名	AI・データサイエンスセンター事務室
電話番号	03-3817-7463
関連部門名	国際情報学部
ホームページのURL	https://www.chuo-u.ac.jp/aboutus/efforts/ai_and_ds/
研究説明のURL	
対象技術	技術の概要・特徴など
研究開発名称： 遠隔通信ロバストネステスト 研究開発国： 日本 研究開発時期： 平成31年4月1日～	技術研究組合 制御システムセキュリティセンター との共同研究により実施している。ネットワークにつながる系統連系保護装置やスマート保安を実現する機器の設置時や更改時に遠隔からセキュリティ試験を実施できるようにする。試験実施手順の煩雑さと誤判定率の高さを課題として、現在研究開発を進めている。試験対象が遠隔地に多数存在するため、試験の遠隔・自動化を進め、試験実施の負担を軽減することを目的としてる。今後のスマート保安におけるセキュリティ評価のあり方を具体的に検討する際に、実用化段階にあることを目指す。

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

企業・大学名	福岡大学
代表者名	貫 正義（理事長）
所在地	〒814-0180 福岡県福岡市城南区七隈八丁目19-1
窓口部署名	情報基盤センター事務部 情報戦略室
電話番号	092-871-6631
関連部門名	福岡大学情報基盤センター研究開発室（中國研究室）
ホームページのURL	https://www.fukuoka-u.ac.jp/
研究説明のURL	https://passpath.net/ （現在は福岡大学内からのみアクセス可能）
対象技術	技術の概要・特徴など
研究開発名称： パスワード共有システム 研究開発国： 日本 研究開発時期： 令和元年12月1日～ 令和2年11月30日	研究開発はほぼ完了し、実装もほぼ完了している状況である。 研究開発成果をサービスとして学内外に無償で提供する計画である （本学の研究推進部などと協議中）。

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	国立大学法人金沢大学
代表者名	学長　　山崎　光悦
所在地	〒920-1192 石川県金沢市角間町
窓口部署名	研究・社会共創推進部研究推進課研究推進総務係
電話番号	076-264-5230
関連部門名	総合メディア基盤センター
ホームページのURL	https://www.kanazawa-u.ac.jp/
研究説明のURL	
対象技術	技術の概要・特徴など
研究開発名称： Raspberry Gate 研究開発国： 日本 研究開発時期： 平成27年4月1日～	Raspberry Gate は、IoTデバイスの集合体が構成する、小規模なローカルネットワークの対外接続点に設置するセキュリティゲートウェイであある。現在は、IPv4に対する実装と性能評価を終え、IPv6対応を進めている。

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

企業・大学名	国立大学法人金沢大学
代表者名	学長　　山崎　光悦
所在地	〒920-1192 石川県金沢市角間町
窓口部署名	研究・社会共創推進部研究推進課研究推進総務係
電話番号	076-264-5230
関連部門名	理工研究域電子情報通信学系
ホームページのURL	https://www.kanazawa-u.ac.jp/
研究説明のURL	
対象技術	技術の概要・特徴など
研究開発名称： Privacy-preserving smart contracts on blockchains 研究開発国： 日本 研究開発時期： 令和2年4月1日～ 令和5年3月31日	We aim to design, build, and analyze a complete system that allows smart contracts on a blockchain to handle private data stored off-chain without compromising the privacy of the data. The main idea is to use a combination of cryptographic commitment schemes and zero-knowledge proof techniques, which have been tested and validated in several academic papers. A major challenge for realizing a general-purpose system that supports privacy-preserving smart contracts is its efficiency, both in terms of contract development and execution costs. Thus, we are now in the process of designing and developing domain-specific languages tailored for privacy-preserving smart contracts, as well as their optimizing compilers that produce smaller, more efficient zero-knowledge proofs to reduce the execution cost.

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	技術の概要・特徴など
研究開発名称： 人間社会のセキュリティ構造を模倣したIoT向け運用モデルの開発 研究開発国： 日本 研究開発時期： 平成27年4月～	基本要素のモデル化と基本要件の分析が完了しており，インター ネット標準のネットワーク管理技術を活用したプロタイプ実装を 開発して，提案の概念実証と基本的実現性を確認している． 現在は，開発したプロトタイプ実装をベースとして実装の改良を 進めるとともに，実用性に関する検討のため様々なIoTデバイスを 対象とした実験を進めようとしている．

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	○

アクセス制御機能に関する技術の
研究開発の状況等に関する調査　　付録資料

付録３：調査票
付録４：集計表

付録３

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

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

■ お手数ですが、令和２年９月 25 日(金) までに、ご返送ください。
◆郵送での回答：同封の返信用封筒をご利用ください（切手は不要です）
◆電子メールでの回答：「cyber@astweb.co.jp」 までお送りください

問１．アクセス制御機能に関する技術の研究開発を行っていますか。（○は一つ）

１．はい
２．いいえ

※以下の設問には「１．はい」と答えた方のみお進みください。

問２．現在、取り組んでいるのは、どのような分野ですか。（○はいくつでも）

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

問３．今後、もっとも力を入れたいのは、どのような分野ですか。（○は一つ）

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

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

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

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

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

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

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

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

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

問８.貴事業所（研究所）は、どの業種にあてはまりますか。（○は一つ）

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

（太枠線内にご回答ください）

回答用紙B

実用化（製品化）されているアクセス制御機能に関する技術の個別調査

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

★ご回答内容の報告書への掲載及び警察庁ホームページでの公開につきまして、「公開情報及びご連絡先記入用紙」にもご回答ください。
※ 本調査票（回答用紙 B）に回答する製品がない場合は回答用紙 C へお進みください。

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

問6　この製品はどのような不正アクセスからの防御を対象としていますか。 **（○はいくつでも）**	1．侵入検知・防御技術 2．ぜい弱性対策技術 3．高度認証技術 4．インシデント分析技術 5．不正プログラム対策技術 6．その他アクセス制御に関する技術
問7　どのようなサービスですか（対象がサービスの場合） **（○はいくつでも）**	1．教育 2．アウトソース 3．インテグレーション 4．コンサルティング 5．保守（サポート） 6．サービスプロバイダ 7．保険 8．その他 （　　）
概要・特徴など	
価格	
発売時期	西暦　　年　　月　　日頃～
出荷数	累計

回答用紙C

研究開発中のアクセス制御機能に関する技術の個別調査

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

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

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

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

＜別紙＞　アクセス制御機能について

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

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

＜参考＞

「不正アクセス行為の禁止等に関する法律」第２条第３項

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

＜回答用紙Aの補足＞表１　アクセス制御機能の分類表

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

＜回答用紙B・Cの補足＞表２　用語説明

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

公開情報及びご連絡先記入用紙

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

【公開用情報】

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

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

【ご担当者様のご連絡先】

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

【個人情報のお取り扱いについて】

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