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３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 1
1. 調査概要 3
1.1　調査の目的 3
1.2　調査の対象と調査方法 3
1.3　調査内容 3
1.4　送付、回収状況 4
1.5　報告書を見る際の留意点 4
2. 調査結果の概要等 5
2.1　概要 5
2.2　回答事業体の属性等 15
3. 調査結果 16
3.1　組織的対策 16
3.1.1　端末装置（パソコン、スマートフォン等）の整備環境　【問4】 16
3.1.2　業務における個人所有端末装置の扱い　【問5】 18
3.1.3　テレワークの実施状況　【問6】 21
3.1.4　テレワークの開始時期　【問6-1】 24
3.1.5　テレワーク業務の端末装置（パソコン、スマートフォン等）の利用環境【問6-2】 26
3.1.6　テレワークを行っていない理由　【問6-3】 28
3.1.7　事業体内のネットワーク利用状況　【問7】 31
3.1.8 インターネット環境の整備　【問8】 33
3.1.9　クラウドサービスの利用状況　【問9】 34
3.1.10　外部からの接続許可状況　【問10】 36
3.1.11　情報セキュリティ対策の必要性の理由【問11】 39
3.1.12　過去に受けたことのある被害状況　【問11-1-1】 43
3.1.13　攻撃手段　【問11-1-2】 46
3.1.14　被害を受けたことによる対策　【問11-2】 48
3.1.15　届出先機関等　【問11-3-1】 51
3.1.16　届出した理由　【問11-3-2】 54
3.1.17　届出を躊躇させる要因　【問11-4】 57
3.1.18　届出先機関を知っているか　【問12】 60
3.1.19　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13】 63
3.1.20　情報セキュリティ対策の実施状況　【問14】 63
3.1.21　情報セキュリティ運用・管理専門部署の有無　【問14-1】 66
3.1.22　情報セキュリティ管理体制　【問14-2】 69
3.1.23　セキュリティポリシーの策定状況　【問14-3】 72

3.1.24　新型コロナウイルスの影響によるセキュリティポリシーの変更状況.....74
【問14-3-1】.....74
3.1.25　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14-4】.....76
3.1.26　第三者機関の認証制度等の利用状況　【問14-5】.....78
3.1.27　次年期の情報セキュリティ対策の投資計画　【問14-6】.....80
3.1.28　情報セキュリティ対策への投資に関する問題点　【問14-7】.....84
3.1.29　標的型攻撃への対策状況　【問14-8】.....88
3.1.30　情報セキュリティ対策を行っていない理由　【問14-9】.....90
3.1.31　ビジネスメール詐欺の認知状況　【問15】.....91
3.1.32　ビジネスメール詐欺への対策　【問15-1】.....93
3.1.33　情報セキュリティ対策に関する考え方　【問16】.....95
3.1.34　投資に関する考え方　【問16-1】.....98
3.1.35　事後的対応と予防的対応に関する考え方　【問16-2】.....100
3.1.36　保険への意識　【問16-3】.....103
3.1.37　規制・罰則への考え方　【問16-4】.....105
3.1.38　プライバシーの考慮に関する考え方　【問16-5】.....107
3.1.39　利便性とのバランスに関する考え方　【問16-6】.....109
3.1.40　セキュリティパッチの適用状況　【問17】.....112
3.2　技術的対策.....115
3.2.1　利用しているセキュリティサービス　【問18】.....115
3.2.2　セキュリティサービスを利用していない理由　【問18-1】.....117
3.2.3　インターネット接続に対するセキュリティ対策　【問19】.....118
3.2.4　無線LANネットワークのセキュリティ対策　【問20】.....121
3.2.5　クラウドサービスを使用することになった理由　【問21】.....124
3.2.6　外部からの接続に対するセキュリティ対策（通信路に対する対策）【問22-A】.....126
3.2.7　外部からの接続に対するセキュリティ対策（端末に対する対策)【問22-B】.....128
3.2.8　社外等からのインターネット接続経由の認証方法　【問23】.....130
3.2.9　ID・パスワードの管理方法　【問23-1】.....132
3.2.10　不正ログイン対策　【問23-2】.....134
3.2.11　各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）の利用状況【問24】.....137
3.2.12　各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）の管理環境【問24-1】.....139
3.2.13　各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）のセキュリティ対策【問24-2】.....141
3.2.14　ぜい弱性調査（ペネトレーションテスト）実施の有無　【問24-3】.....143
3.2.15　ログの取得状況　【問24-4】.....145
3.2.16　ログの保管期間　【問24-4A】.....147
3.2.17　ログの保管方法　【問24-4B】.....147

3.2.18　ログを取得・保管している理由　【問24-4-1】 148
3.2.19　電子メールに関するセキュリティ対策　【問25】 149
3.2.20　添付ファイルの取り扱い　【問26】 153
3.2.21　暗号化技術の用途　【問27】 155
3.2.22　重要システムの不正アクセス対策状況　【問28】 157
3.2.23　不正アクセス等への対策状況　【問29】 160
3.2.24　不正プログラムへの対策状況　【問30】 163
3.3　人的対策 165
3.3.1　情報セキュリティ教育の実施状況　【問31】 165
3.3.2　情報セキュリティ教育の内容　【問31-1】 169
3.3.3　情報セキュリティ教育の頻度　【問31-2】 171
3.3.4　情報セキュリティ教育を実施しない理由　【問31-3】 174
3.3.5　セキュリティ対策の問題点や不安等 175
不正アクセス行為対策等の実態調査　付録資料
調査票　付録１
集計表　付録２

第２部 179
4. 調査概要 181
4.1　調査の目的 181
4.2　調査の対象と調査方法 181
4.3　調査内容 182
4.4　送付・回収状況、集計対象件数 183
4.5　報告書を見る際の留意点 183
5. 調査結果（概要と考察） 184
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 184
5.1.1　現在、取り組んでいる分野　【A-問2】 185
5.1.2　今後、もっとも力を入れたい分野　【A-問3】 188
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 191
5.2.1　現在、実用化(製品化)されている分野　【A-問4】 192
5.2.2　今後、実用化(製品化)を見込んでいる分野　【A-問5】 195
5.3　研究開発体制 198
5.3.1　年間の研究開発費　【A-問6】 199
5.3.2　研究開発に携わっている人数　【A-問7】 202
5.4　実用化された製品及び研究開発中の技術・サービス 205
5.4.1　何を守るか？ 206
5.4.2　何から保護するか？ 208
5.4.3　どのようなセキュリティ上の効果があるか？ 210
5.4.4　どのような機能を持つか？ 212
5.4.5　どのようなレイヤーのセキュリティを守るか？ 214
5.4.6　不正アクセスからの防御対象 216
5.4.7　どのようなサービスか？ 218

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？ 220
5.6　研究開発の進捗状況 221
5.7　発売時期の分布 222
5.8　研究開発期間の分布 223
5.9　実用化された製品及び研究開発中の技術・サービス 224
5.9.1　「技術の実用化（製品化）状況」について 226
5.9.2　「技術の研究開発状況」について 233
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
調査票　付録３
集計表　付録４

第１部

不正アクセス行為対策等の実態調査

1. 調査概要

1.1　調査の目的

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

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

1.2　調査の対象と調査方法

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

調査は、調査票を郵送で配付し、次の2つの方法で回収することで実施した。

①　電子メールでの回答

調査票のファイルに回答内容を入力してもらい、電子メールにて回答

②　郵送等での回答

配付した調査票を、郵送で送付してもらい回答

（調査期間：令和3年8月23日（月）（発送日）～9月21日（火）（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2,950件、回収総数は716件であった。回収率は24.3%である。

業種	発送数	回収数	回収率
農林・水産・鉱業	10	1	10.0%
製造業	901	186	20.6%
不動産・建築	187	53	28.3%
金融	108	30	27.8%
エネルギー	15	10	66.7%
運輸業	75	16	21.3%
情報通信	291	11	3.8%
サービス	839	187	22.3%
教育	290	100	34.5%
行政サービス	234	112	47.9%
無回答		10	-
合計	2,950	716	24.3%

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

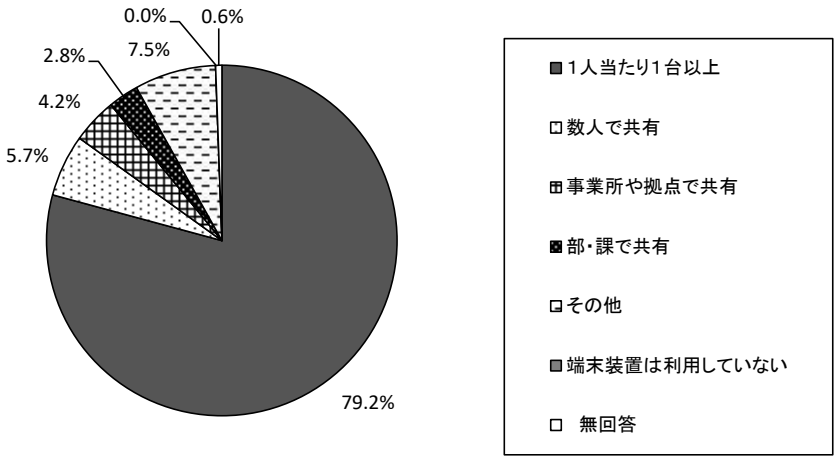
令和3年度の調査結果については、次のような特徴がみられる。

1　組織的対策状況

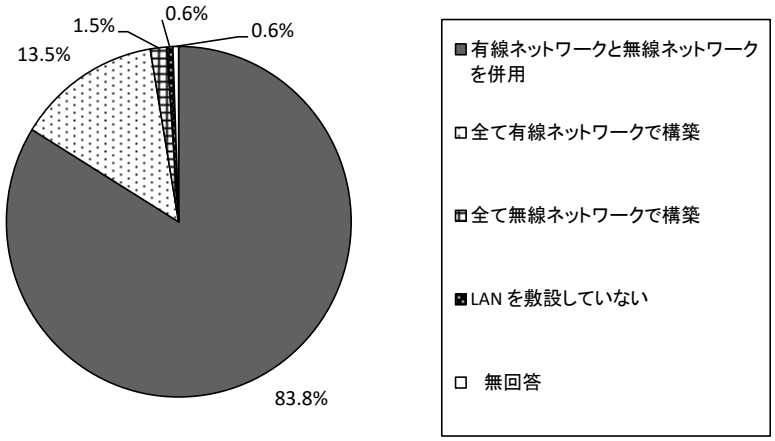
【情報システム等の環境】

パソコン・スマートフォン等の整備環境については、79.2%で「1人当たり1台以上」で整備されており、「数人で共有」が5.7%、「事業所や拠点で共有」が4.2%となっている。「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83.8%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、99.4%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63.4%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=716)



【全体】事業体内のネットワーク利用状況（SA, n=716）

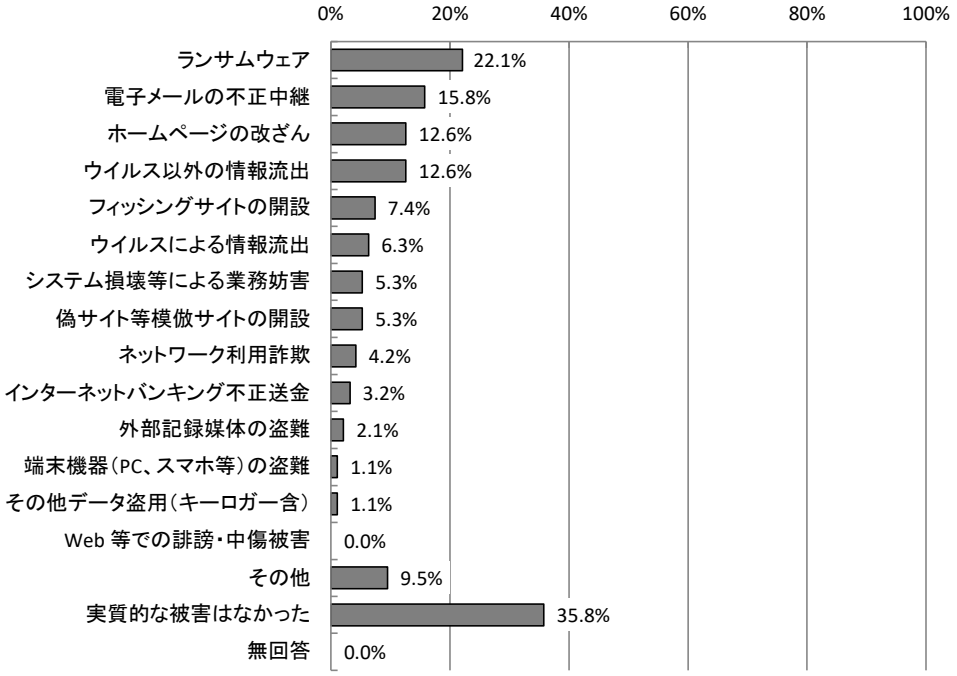


【不正アクセス等の被害状況】

過去１年間に不正アクセス等の攻撃・被害にあったと回答した社・団体等（95団体）について、その被害の種類は「ランサムウェア」が22.1％で最も多く、次いで「電子メールの不正中継」が15.8％となっている。届出先機関等については、「警察」が28.4％で最も多く、次いで「IPA （情報処理推進機構）」が18.9％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76.7％で最も多く、次いで「自社内だけの被害だったので」が18.6％となり、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=95）



【情報セキュリティの運用・管理体制】

情報セキュリティ対策を行っている社・団体等（681団体）のうち、情報セキュリティ運用・管理専門部署の有無については、「ある」が71.8%であり、管理体制は「情報システム運用管理者が情報セキュリティについて兼務」が76.4%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35.5%となっている。

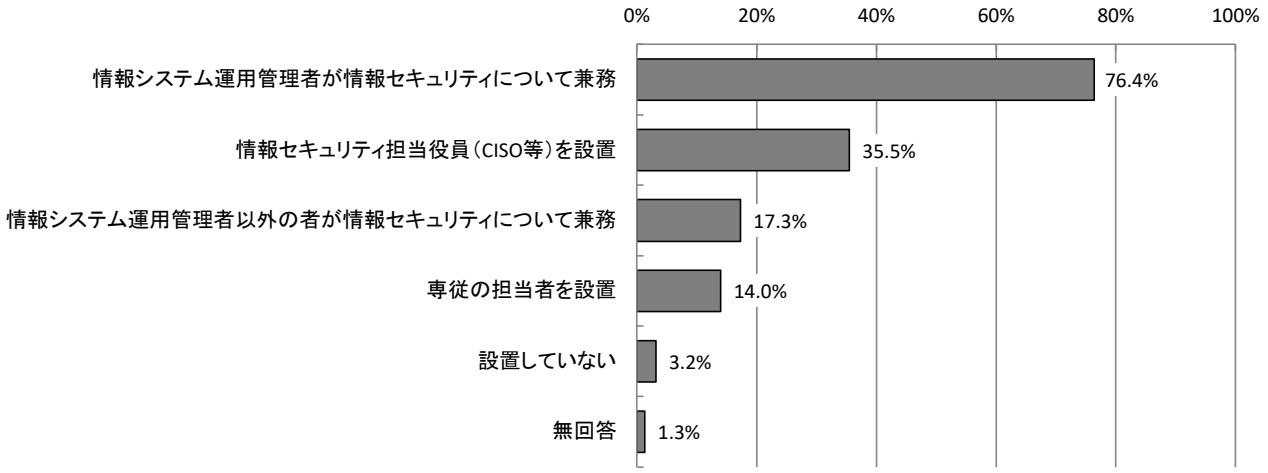
セキュリティポリシーの策定状況については、「策定している」が81.2%で最も多く、「今のところ、策定する予定はない」は4.1%となっている。策定済みに今後予定と策定作業中を入れると90.6%であり、情報セキュリティポリシーの策定が浸透している状況が窺える。

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48.6%で最も多く、次いで「策定することを検討」が31.9%となっている。

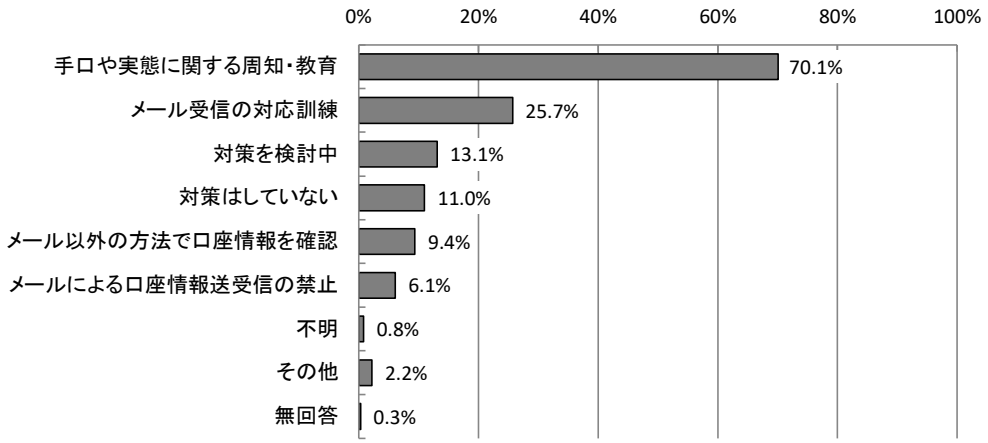
第三者認証機関制度の利用は、「特に利用していない」が80.5%となっている。

また、ビジネスメール詐欺については、88.7%が「知っていた」と回答しており、対策方法は「手口や実態に関する周知・教育」が70.1%で最も多くなった。一方、「対策はしていない」が11.0%となっている。

【全体】情報セキュリティ管理体制（MA, n=681）



【全体】ビジネスメール詐欺への対策（SA, n=635）

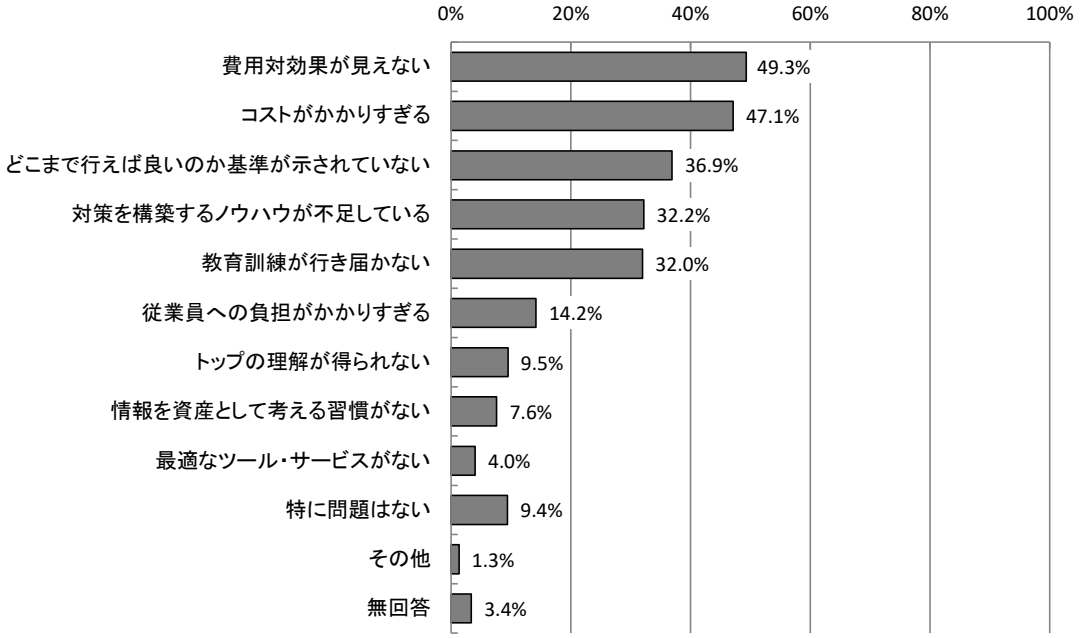


【情報セキュリティ対策への投資】

令和４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67.5%で最も多く、増やす計画であるとする各項目の合計は22.3%で、減らすとする各項目の合計は1.2%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49.3%で最も多く、次いで「コストがかかりすぎる」が47.1%、「どこまで行えば良いのか基準が示されていない」が36.9%となっている。

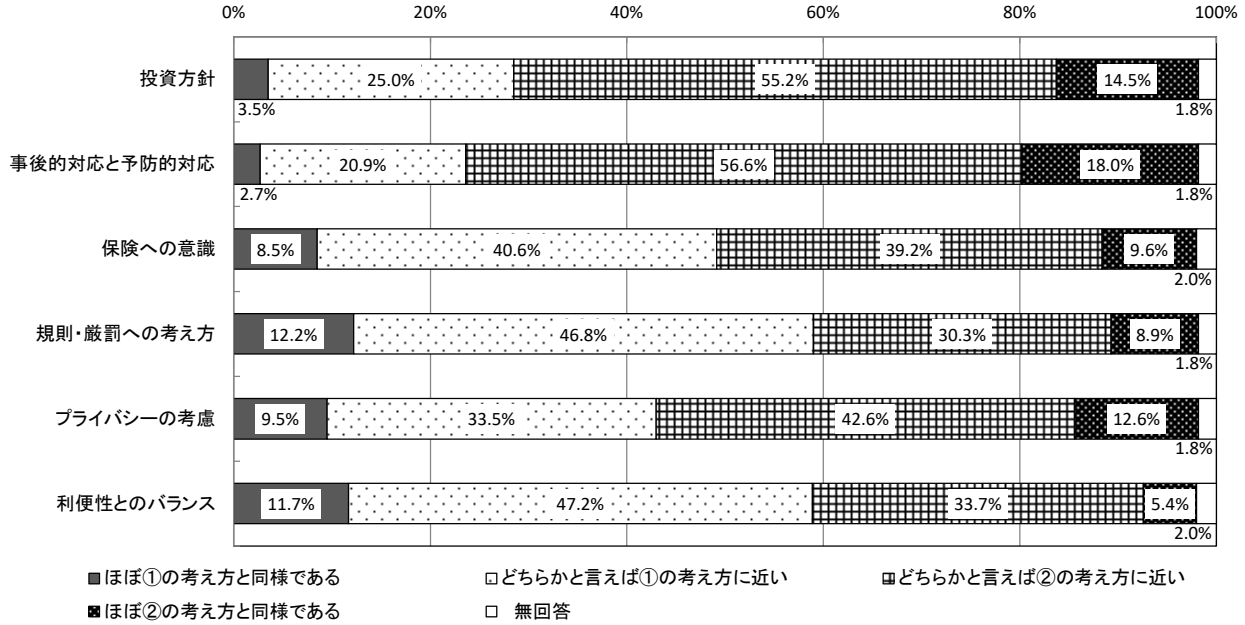
【全体】情報セキュリティ対策への投資に関する問題点(MA,n=681)



【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=716）



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】

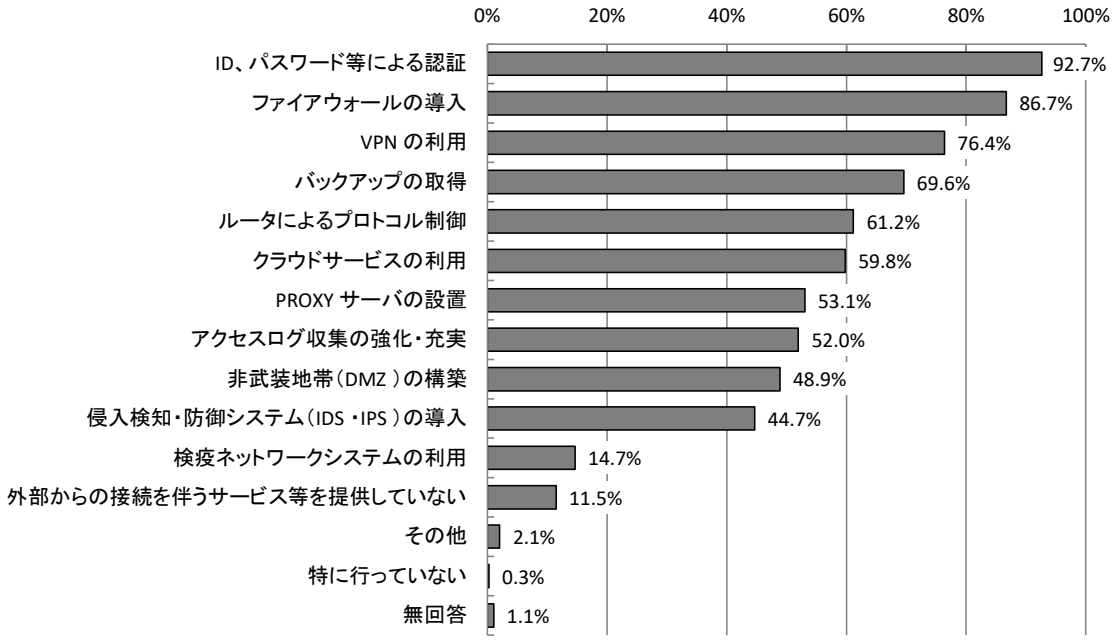
外部からの接続に対するセキュリティ対策（通信路に対する対策）については、「ID・パスワードに対する認証」が90.7%で最も多く、次いで、「通信の暗号化」が71.6%、「MACアドレス等の端末機器の固有情報を用いた認証」「専用ネットワークセグメントの設定」がこれに続いている。

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91.0%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55.9%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92.7%で最も多く、次いで「ファイアウォールの導入」が86.7%となっている。

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71.2%で導入されており、36.0%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11.0%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=716）

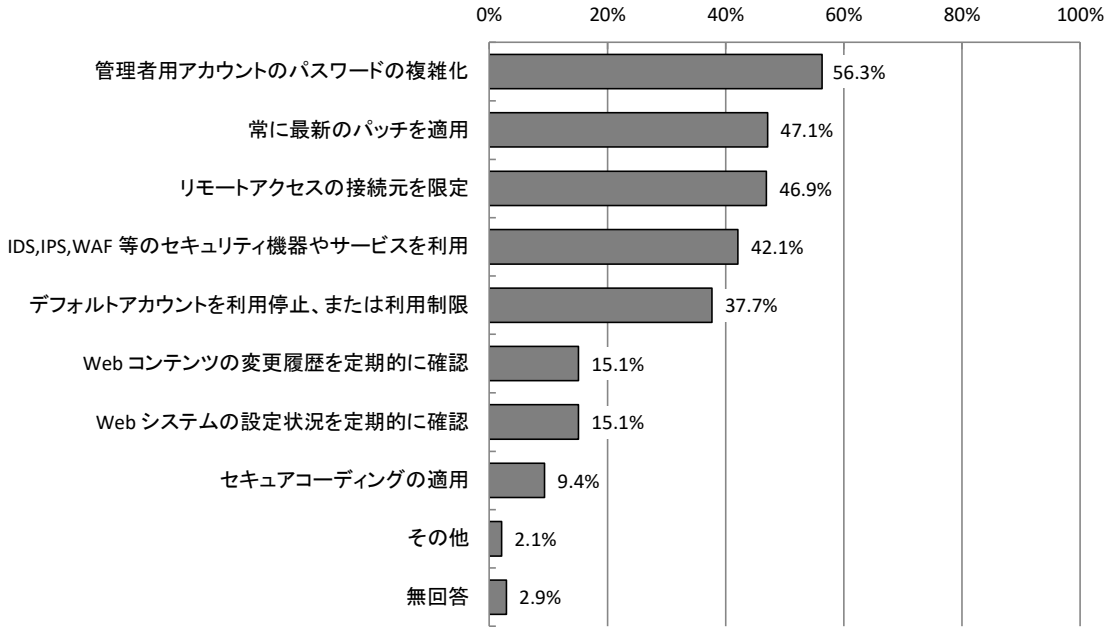


【各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）のセキュリティ対策】

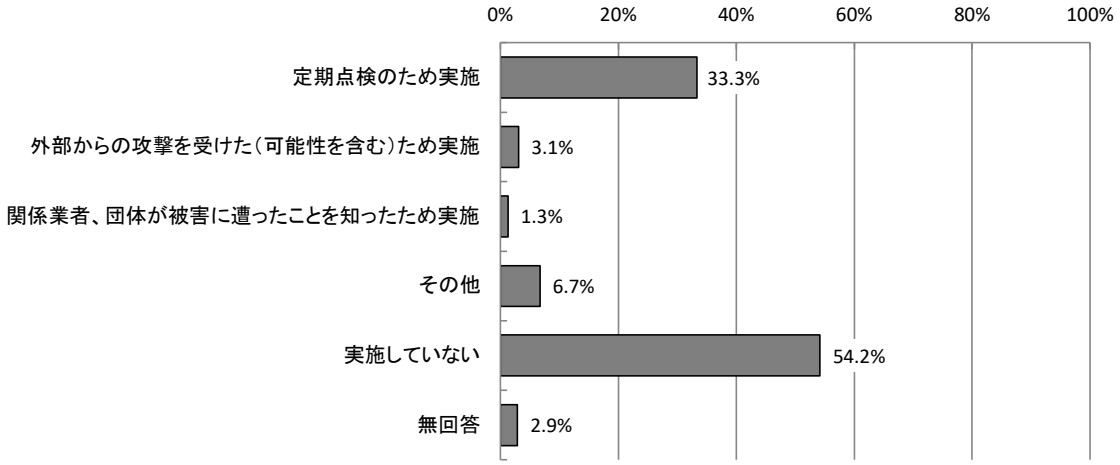
各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）のセキュリティ対策については、「管理者用アカウントのパスワードの複雑化」が56.3％で最も多く、次いで「常に最新のパッチを適用」が47.1％、「リモートアクセスの接続元を限定」が46.9％となっている。

ぜい弱性調査（ペネトレーションテスト）実施の有無については、「実施していない」が54.2％と最も多く、次いで「定期点検のため実施」が33.3％となっている。

【全体】Webサーバのセキュリティ対策（MA, n=478）



【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=478）

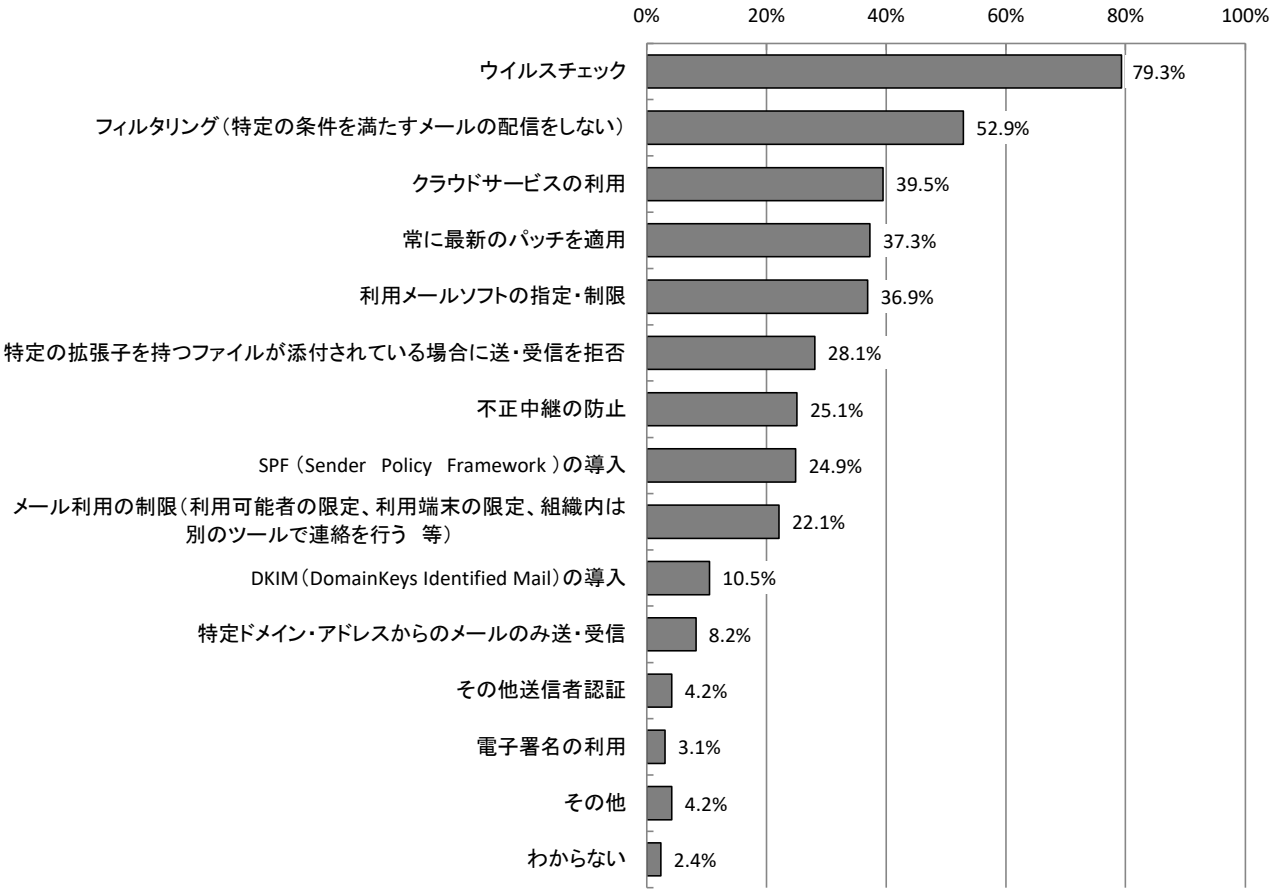


【電子メールに関するセキュリティ対策】

電子メールに関するセキュリティ対策については、「ウイルスチェック」が79.3%で最も多く、次いで「フィルタリング」が52.9%、「クラウドサービスの利用」が39.5%となっている。

添付ファイルの取り扱いについては、「ウイルスチェックをしてから受信」が78.6%で最も多くなった。一方、「特にチェックもせず受信」は、8.8%であった。

【全体】電子メールに関するセキュリティ対策（MA,n=716）

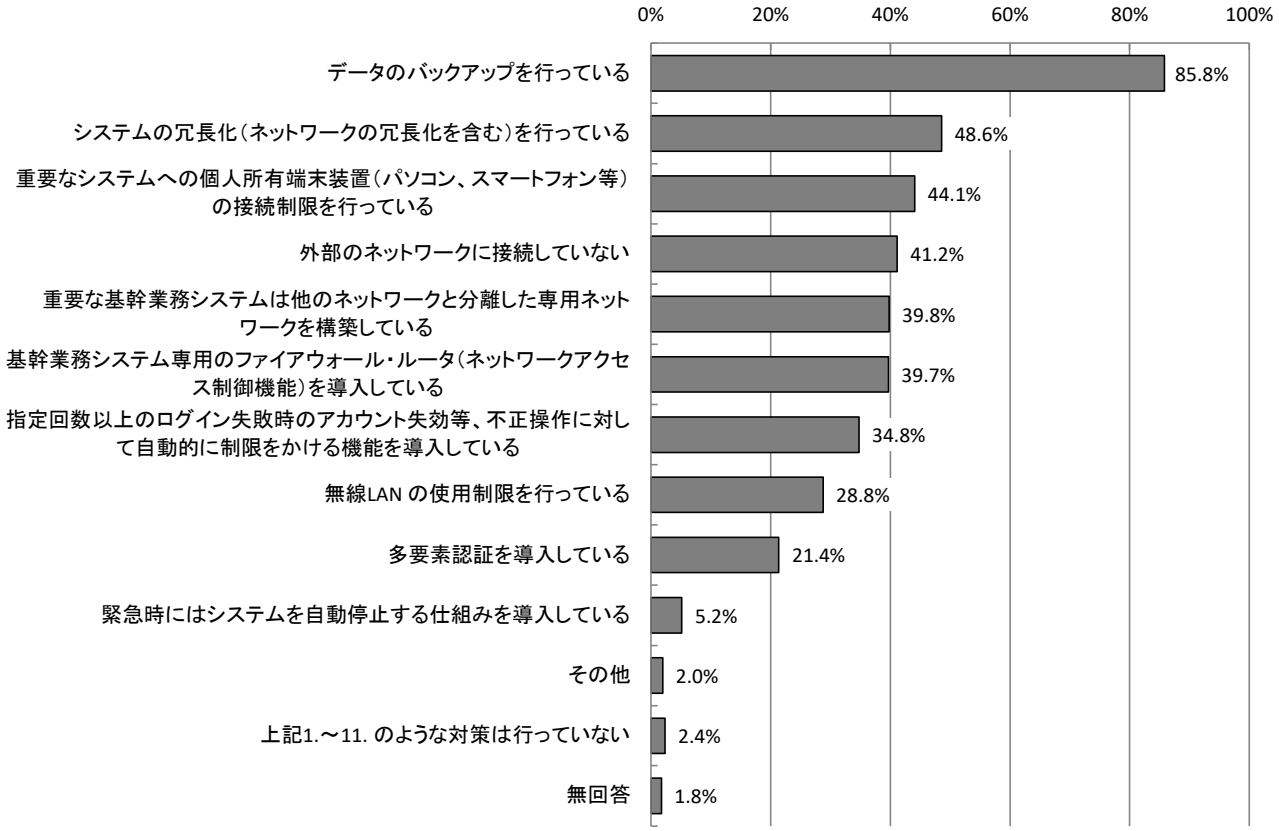


【不正アクセス、情報漏えい等に対する情報セキュリティ対策】

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85.8%で最も多く、次いで「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48.6%、「重要なシステムへの個人所有端末装置（パソコン、スマートフォン等）の接続制限を行っている」が44.1%となっている。

不正アクセス等への対策状況については、「定期的なバックアップ」が77.5%で最も多く、次いで「端末装置（パソコン、スマートフォン等）廃棄時の適正なデータ消去」が69.8%、「情報資産へのアクセス権の設定」が69.6%となっている。不正プログラムへの対策状況については、「ウイルス対策ソフト（クライアント）の使用」が91.8%で最も多く、次いで「ウイルス対策ソフト（サーバ）の使用」が79.7%、「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73.9%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=716)



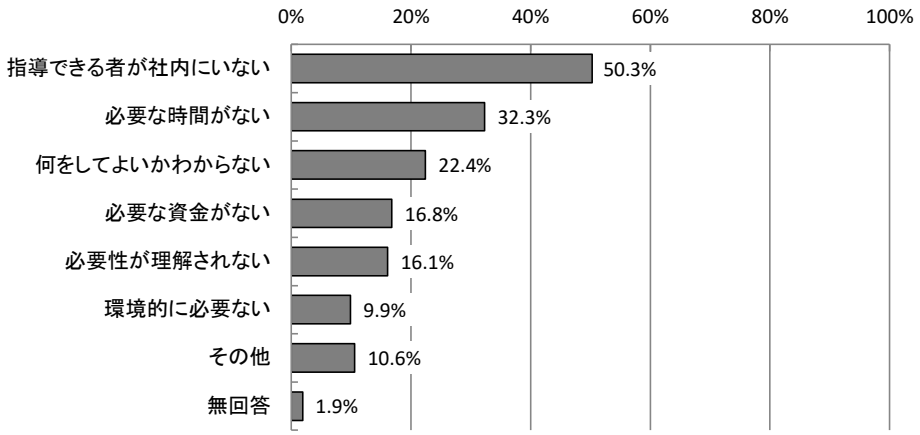
３　人的対策

【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71.2%、「実施していない」が22.5%、「実施を予定している」が4.7%となっている。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50.3%で最も多く、次いで「必要な時間がない」が32.3%、「何をしてよいかわからない」が22.4%となっている。また、従業員数100人未満の社・団体では41.4%であり小規模ほど実施率が低い状況にある。

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71.0%で最も多く、次いで「個人情報の保護・管理」が70.0%、「情報システム利用に係るモラル」が69.5%となっている。教育の頻度については、「年に１回」が42.8%で最も多く、次いで「年に数回」が36.4%、「採用、異動時等に実施」が28.1%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=161)

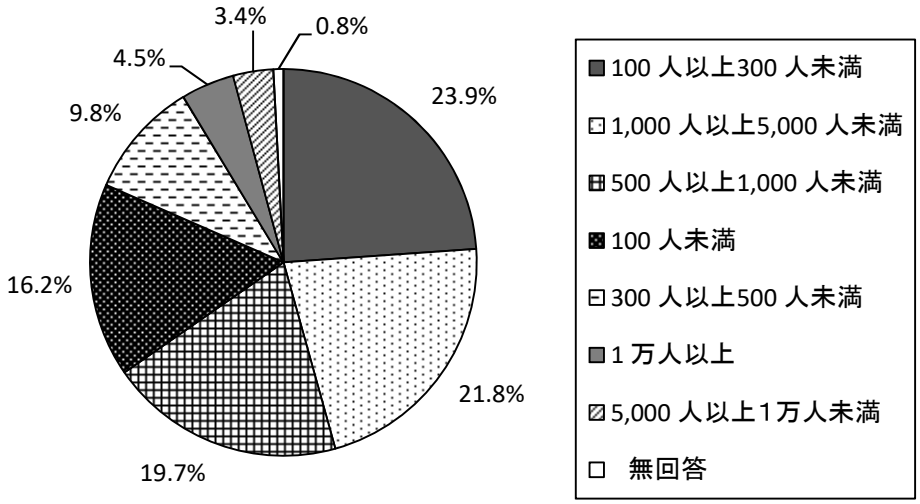


今回の調査結果では、情報セキュリティポリシーが、全体の８割以上で制定されており、情報セキュリティに関する教育においても、全体の７割で実施されている等情報セキュリティに関する意識について一定の浸透が図られていることがうかがえるが、その一方で、小規模組織におけるセキュリティ教育の実施率が低いことや、情報セキュリティ対策について費用対効果が見えづらい・基準が示されていない等の問題意見が出されるなど、問題点も明らかになった。

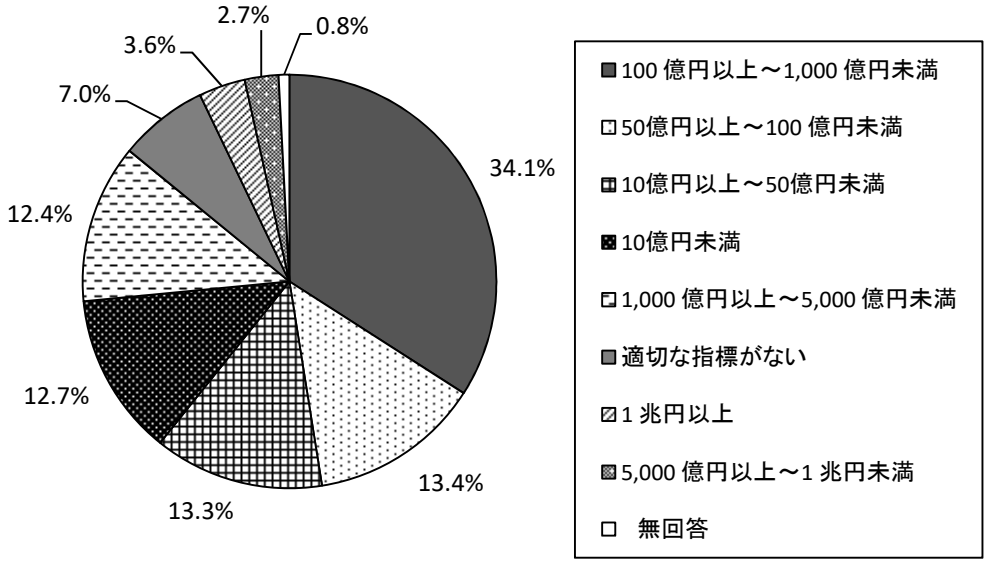
また、過去１年間に攻撃・被害を受けた社・団体等が全体の13.3%あり、そのうちランサムウェア被害が最も多く、インターネット接続に対するセキュリティ対策が重要と認められるほか、セキュリティ侵害事案発生時における対応マニュアルの策定が、依然半数に満たない状況であり、事案発生の際の被害拡大防止のため、これら対策意識の浸透が今後の課題といえる。

2.2　回答事業体の属性等

【全体】従業員規模（SA,n=716）【問2】



【全体】予算規模（SA,n=716）【問3】



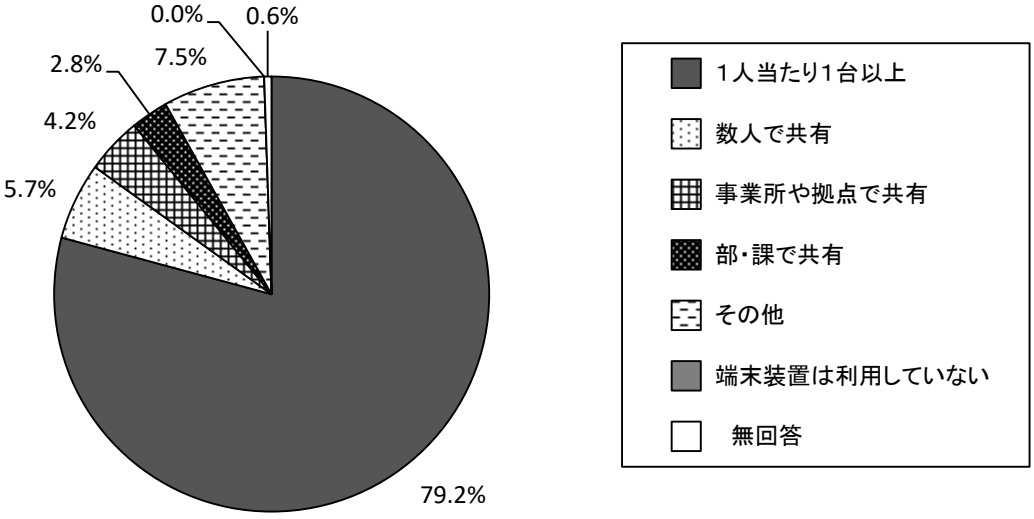
3. 調査結果

3.1　組織的対策

3.1.1　端末装置（パソコン、スマートフォン等）の整備環境　【問4】

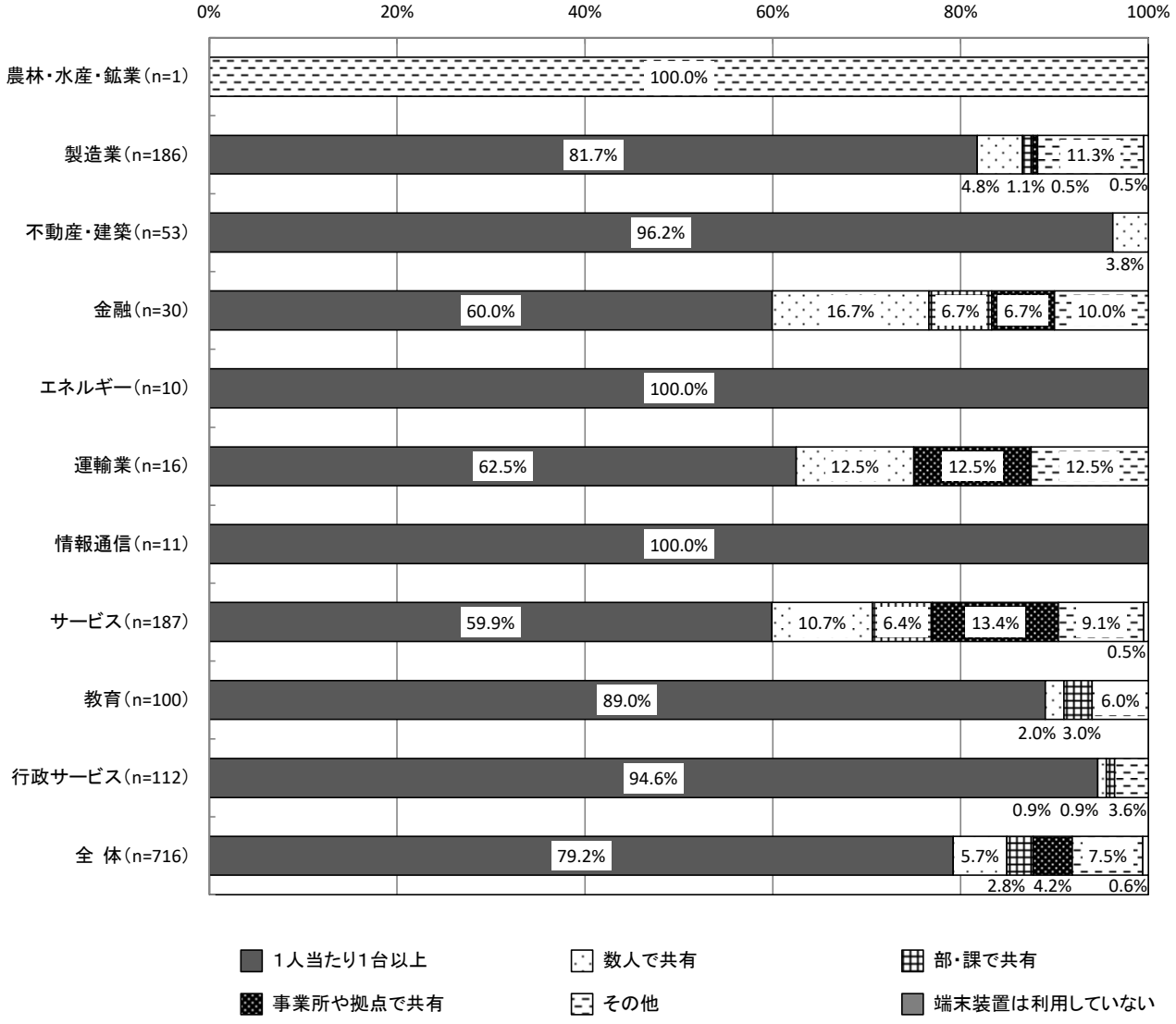
端末装置（パソコン）の整備環境については、「1人当たり1台以上」が79.2%で最も多く、「数人で共有」が5.7%、「事業所や拠点で共有」が4.2%となっている。

【全体】端末装置（パソコン、スマートフォン等）の整備環境（SA,n=716）



【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「不動産・建築」が96.2%、「行政サービス」が94.6%、「教育」が89.0%となっている。一方、最も少ないのは「サービス」で59.9%となっている。

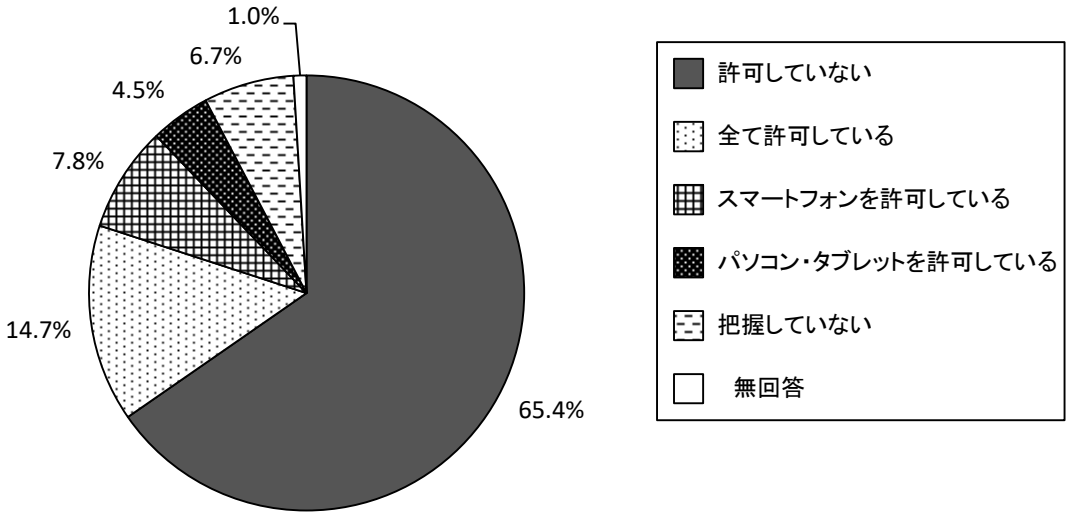
【業種別分析】端末装置（パソコン、スマートフォン等）の整備環境



3.1.2　業務における個人所有端末装置の扱い　【問5】

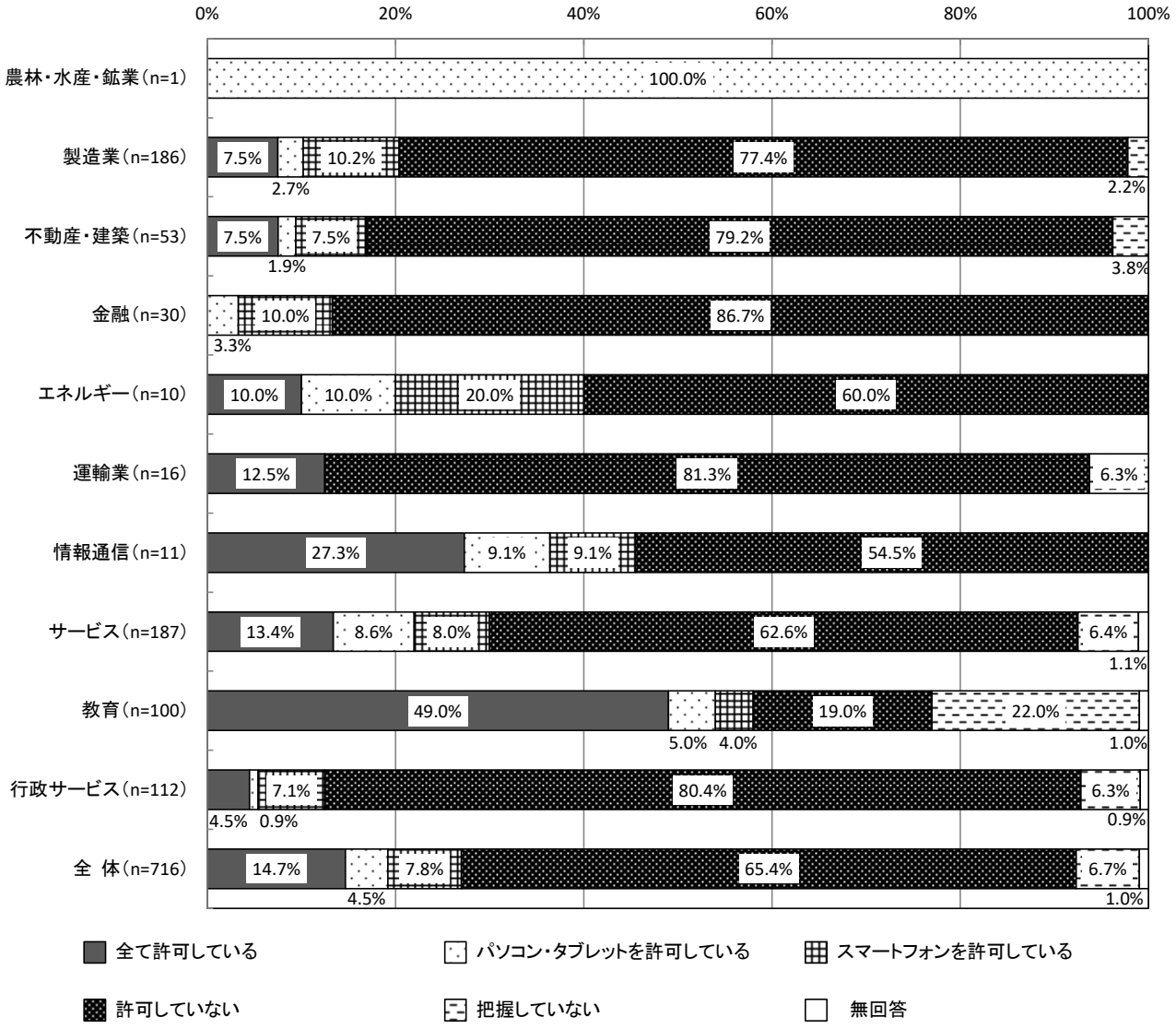
業務における個人所有端末装置の扱いについては、「許可していない」が65.4%で最も多く、「全て許可している」が14.7%、「スマートフォンを許可している」が7.8%となっている。

【全体】業務における個人所有端末装置の扱い（SA,n=716）



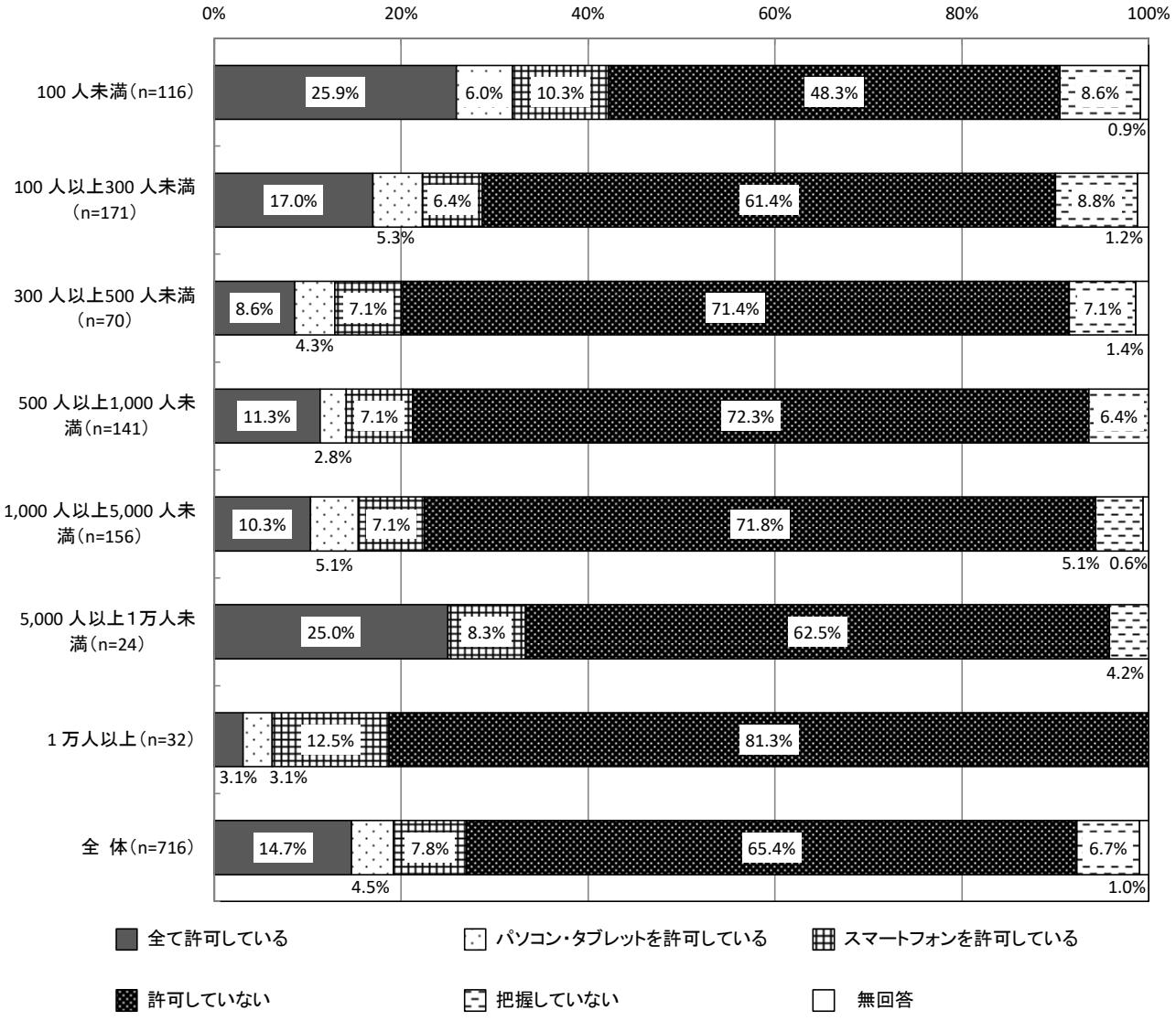
【業種別分析】業種別にみると、「許可していない」では、「金融」が86.7%で最も多く、次いで「運輸業」が81.3%、「行政サービス」が80.4%、「不動産・建築」が79.2%となっている。一方、最も少ないのは「教育」で19.0%となっている。

【業種別分析】業務における個人所有端末装置の扱い



【従業員規模別分析】従業員規模別にみると、「許可していない」では、「１万人以上」が81.3％で最も多く、次いで「500人以上1,000人未満」が72.3％、「1,000人以上5,000人未満」が71.8％、「5,000人以上１万人未満」が62.5％となっている。一方、最も少ないのは「100人未満」で48.3％となっている。

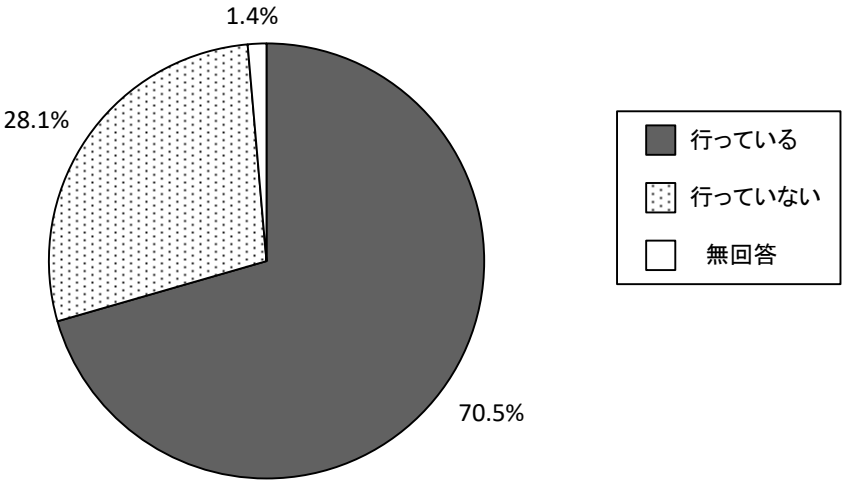
【従業員規模別分析】業務における個人所有端末装置の扱い



3.1.3　テレワークの実施状況　【問6】

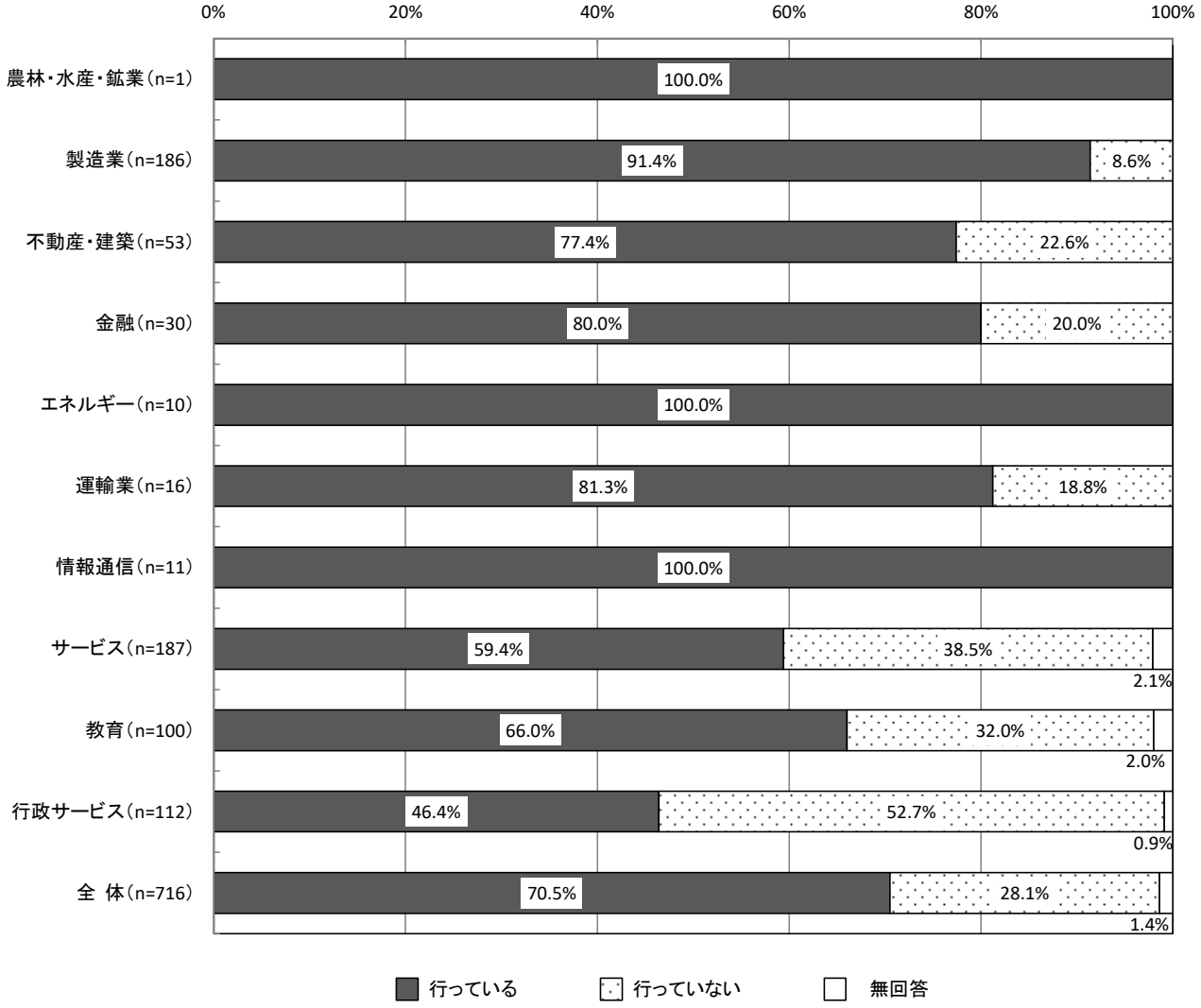
テレワークの実施状況については、「行っている」が70.5%、「行っていない」が28.1%となっている。

【全体】テレワークの実施状況（SA,n=716）



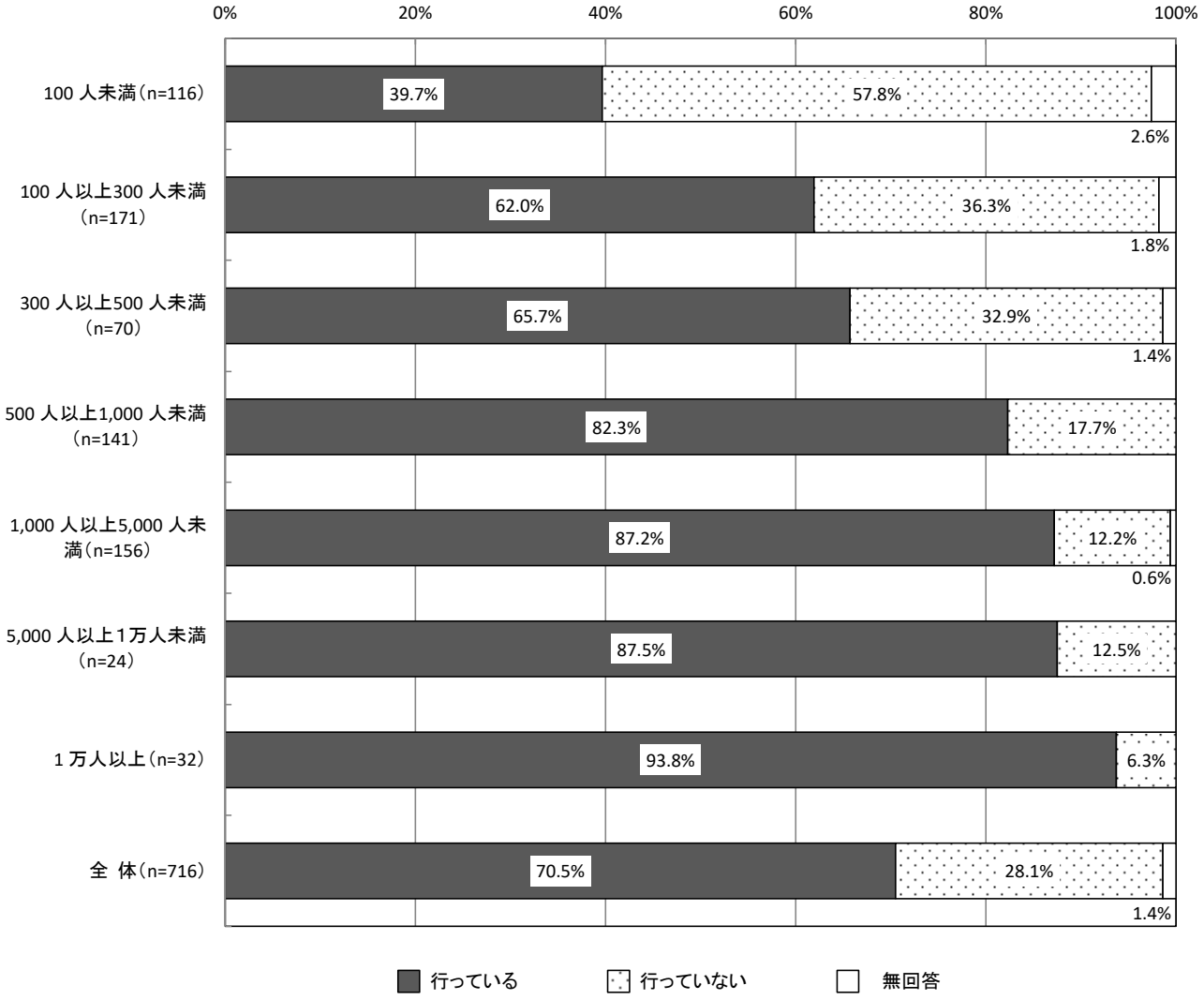
【業種別分析】業種別にみると、「行っている」では、「エネルギー」「情報通信」が100.0%で最も多く、次いで「製造業」が91.4%、「運輸業」が81.3%、「金融」が80.0%となっている。一方、最も少ないのは「行政サービス」で46.4%となっている。

【業種別分析】テレワークの実施状況



【従業員規模別分析】従業員規模別にみると、「行っている」では、「１万人以上」が93.8％で最も多く、次いで「5,000人以上１万人未満」が87.5％、「1,000人以上5,000人未満」が87.2％、「500人以上1,000人未満」が82.3％となっている。一方、最も少ないのは「100人未満」で39.7％となっている。

【従業員規模別分析】テレワークの実施状況

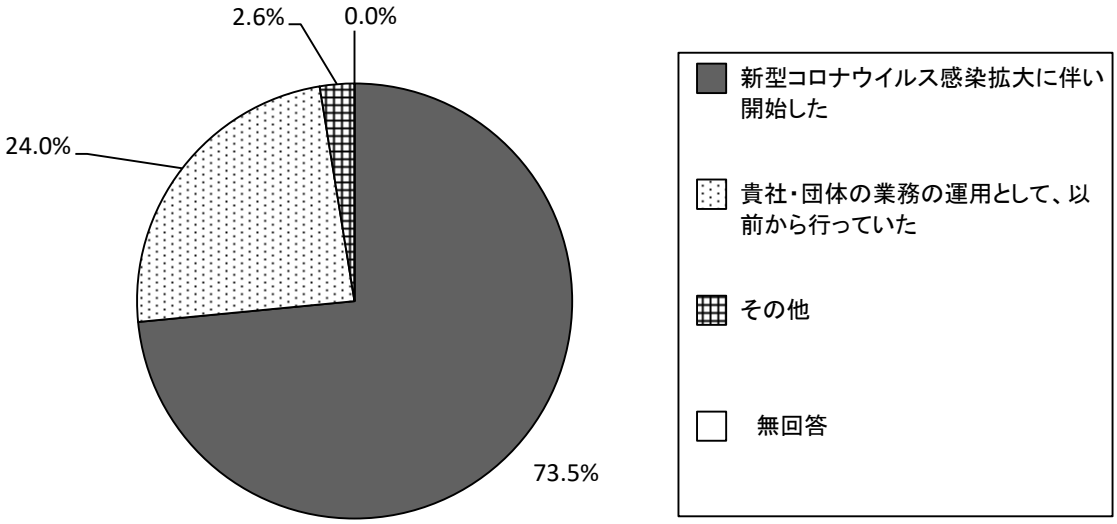


3.1.4　テレワークの開始時期　【問6-1】

テレワークの開始時期については、「新型コロナウイルス感染拡大に伴い開始した」が73.5%、「貴社・団体の業務の運用として、以前から行っていた」が24.0%となっている。

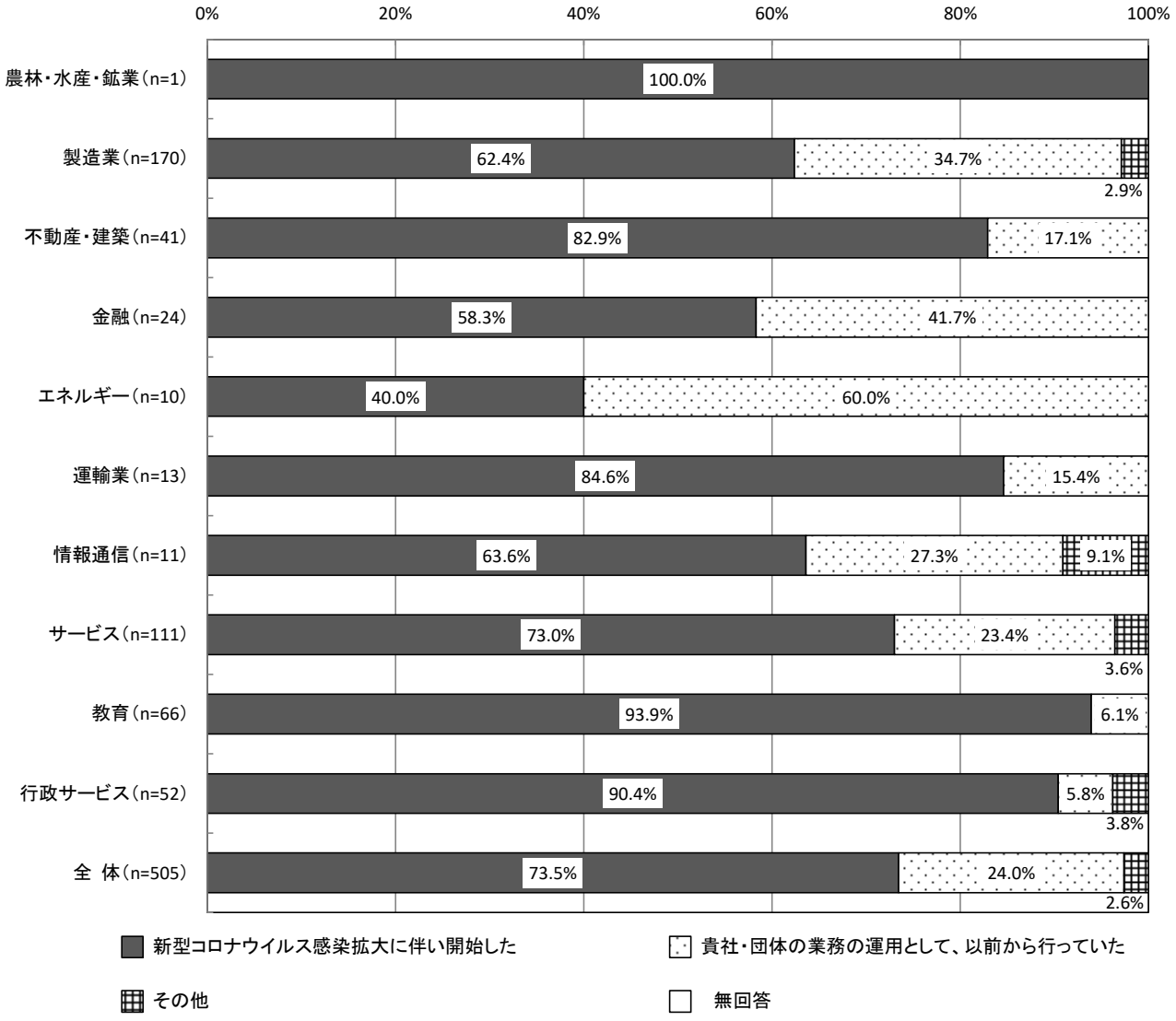
※本項目は、テレワークを実施している社・団体等を対象としている。

【全体】テレワークの開始時期（SA, n=505）



【業種別分析】業種別にみると、「新型コロナウイルス感染拡大に伴い開始した」では、「教育」が93.9%で最も多く、次いで「行政サービス」が90.4%、「運輸業」が84.6%、「不動産・建築」が82.9%となっている。一方、最も少ないのは「エネルギー」で40.0%となっている。

【業種別分析】テレワークの開始時期

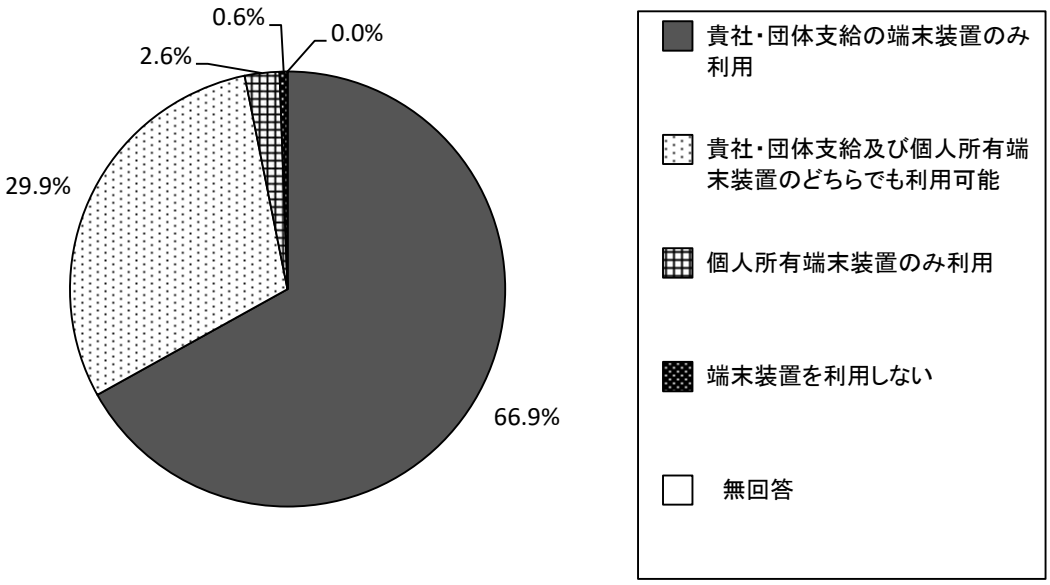


3.1.5　テレワーク業務の端末装置（パソコン、スマートフォン等）の利用環境　【問6-2】

テレワーク業務の端末装置（パソコン、スマートフォン等）の利用環境については、「貴社・団体支給の端末装置のみ利用」が66.9%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29.9%、「個人所有端末装置のみ利用」が2.6%となっている。

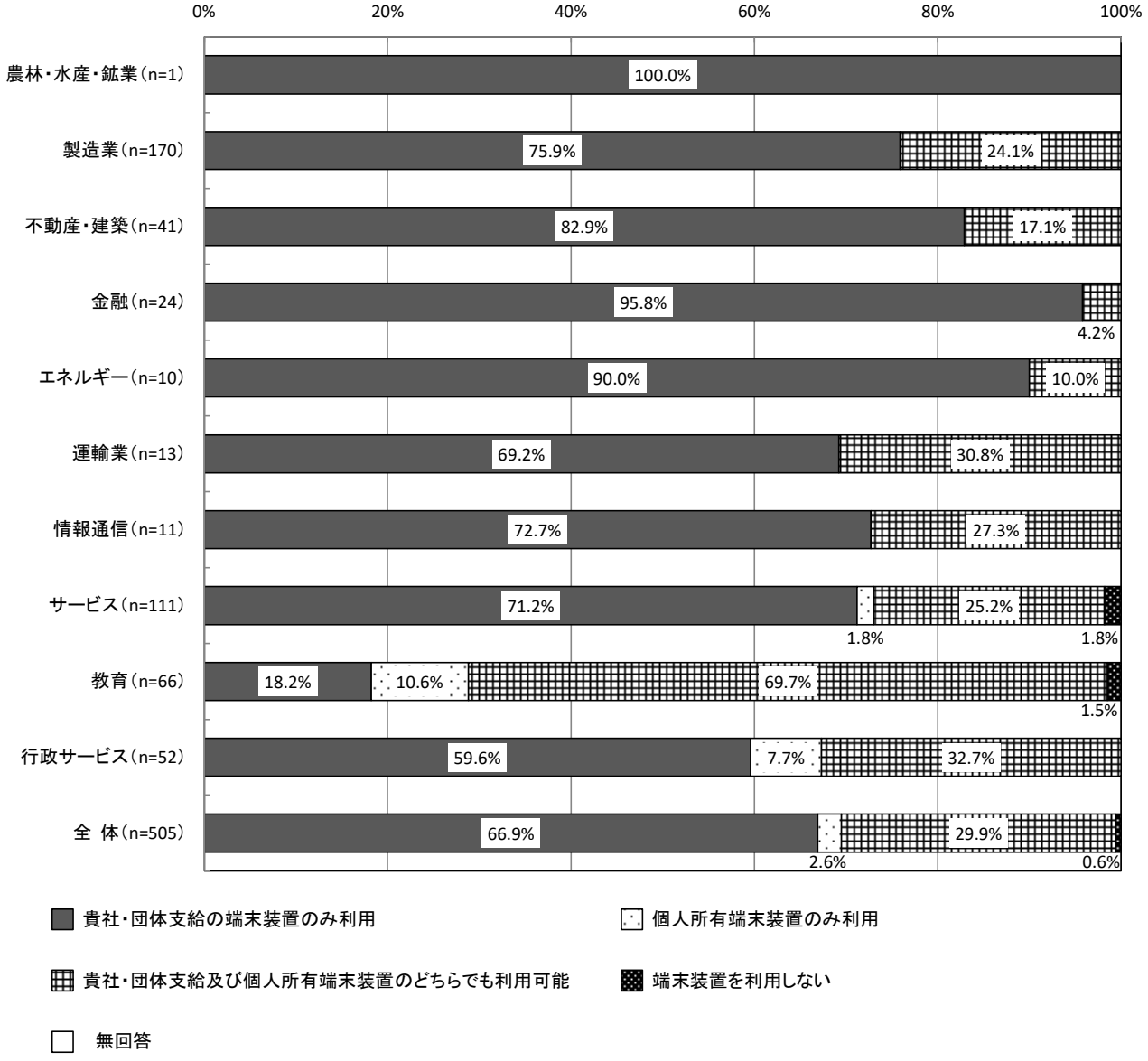
※本項目は、テレワークを実施している社・団体等を対象としている。

【全体】テレワーク業務の端末装置（パソコン、スマートフォン等）の利用環境（SA,n=505）



【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95.8%で最も多く、次いで「エネルギー」が90.0%、「不動産・建築」が82.9%となっている。一方、最も少ないのは「教育」で18.2%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、スマートフォン等）の利用環境

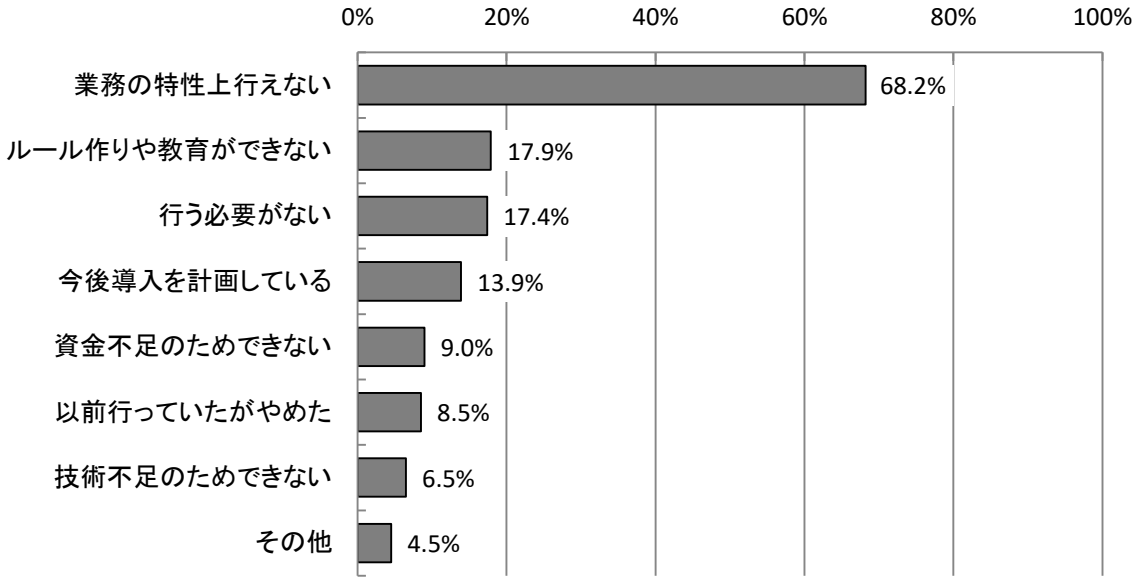


3.1.6　テレワークを行っていない理由　【問6-3】

テレワークを行っていない理由については、「業務の特性上行えない」が68.2%で最も多く、「ルール作りや教育ができない」が17.9%、「行う必要がない」が17.4%となっている。

※本項目は、テレワークを実施していない社・団体等を対象としている。

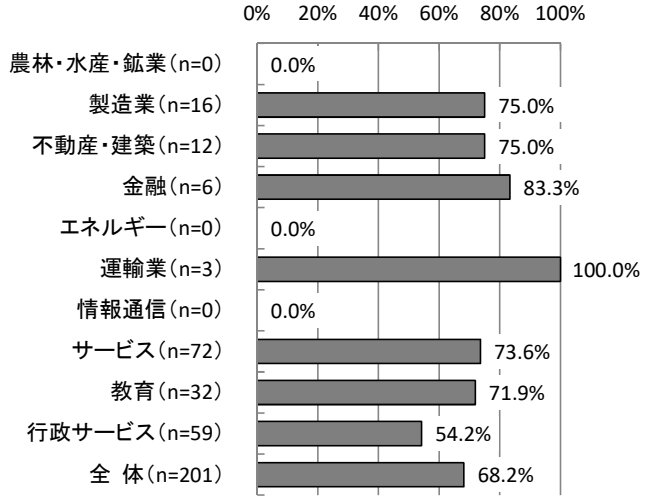
【全体】テレワークを行っていない理由（MA, n=201）



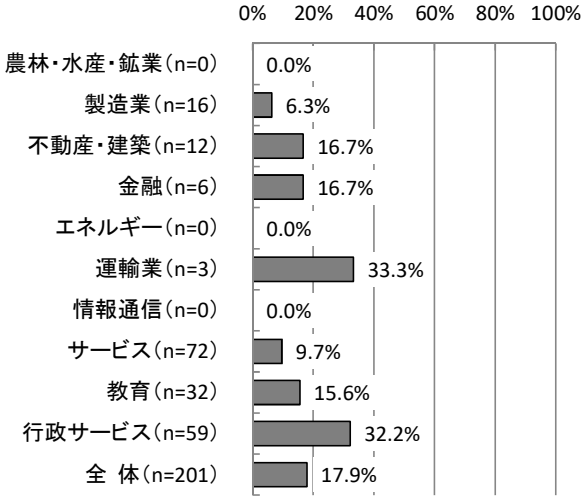
【業種別分析】業種別にみると、「業務の特性上行えない」では、「金融」が83.3%で最も多く、次いで「製造業」「不動産・建築」が75.0%、「サービス」が73.6%となっている。一方、最も少ないのは「行政サービス」で54.2%となっている。

【業種別分析】テレワークを行っていない理由

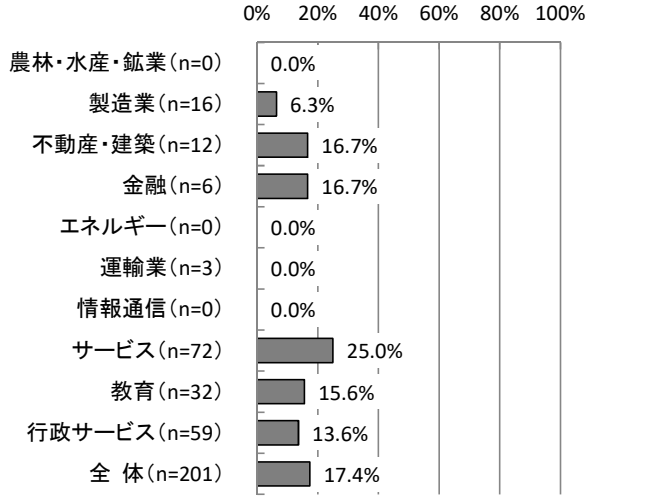
業務の特性上行えない



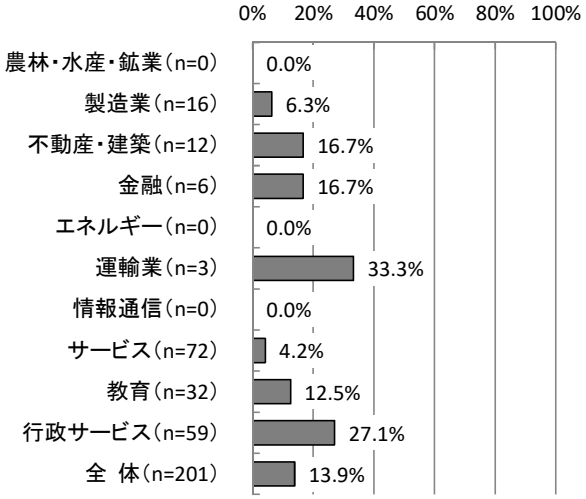
ルール作りや教育ができない



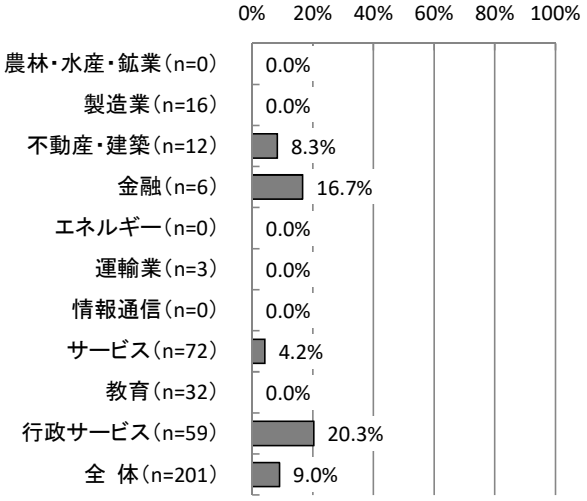
行う必要がない



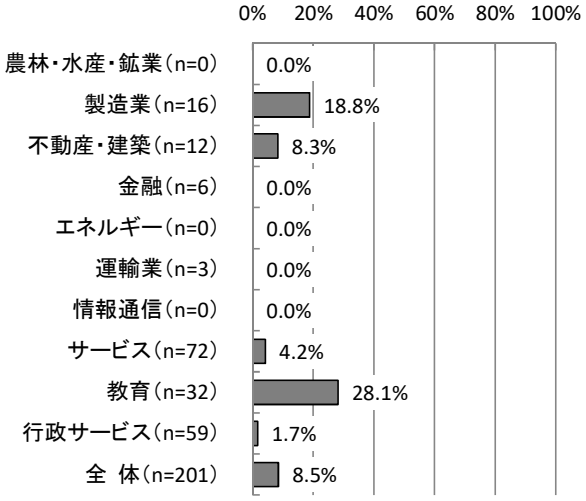
今後導入を計画している



資金不足のためできない



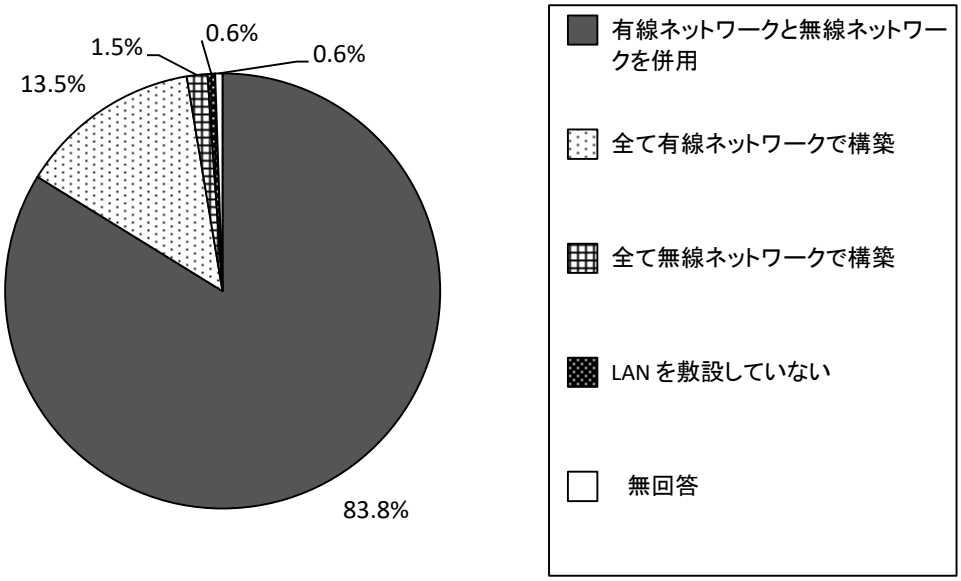
以前行っていたがやめた



3.1.7　事業体内のネットワーク利用状況　【問7】

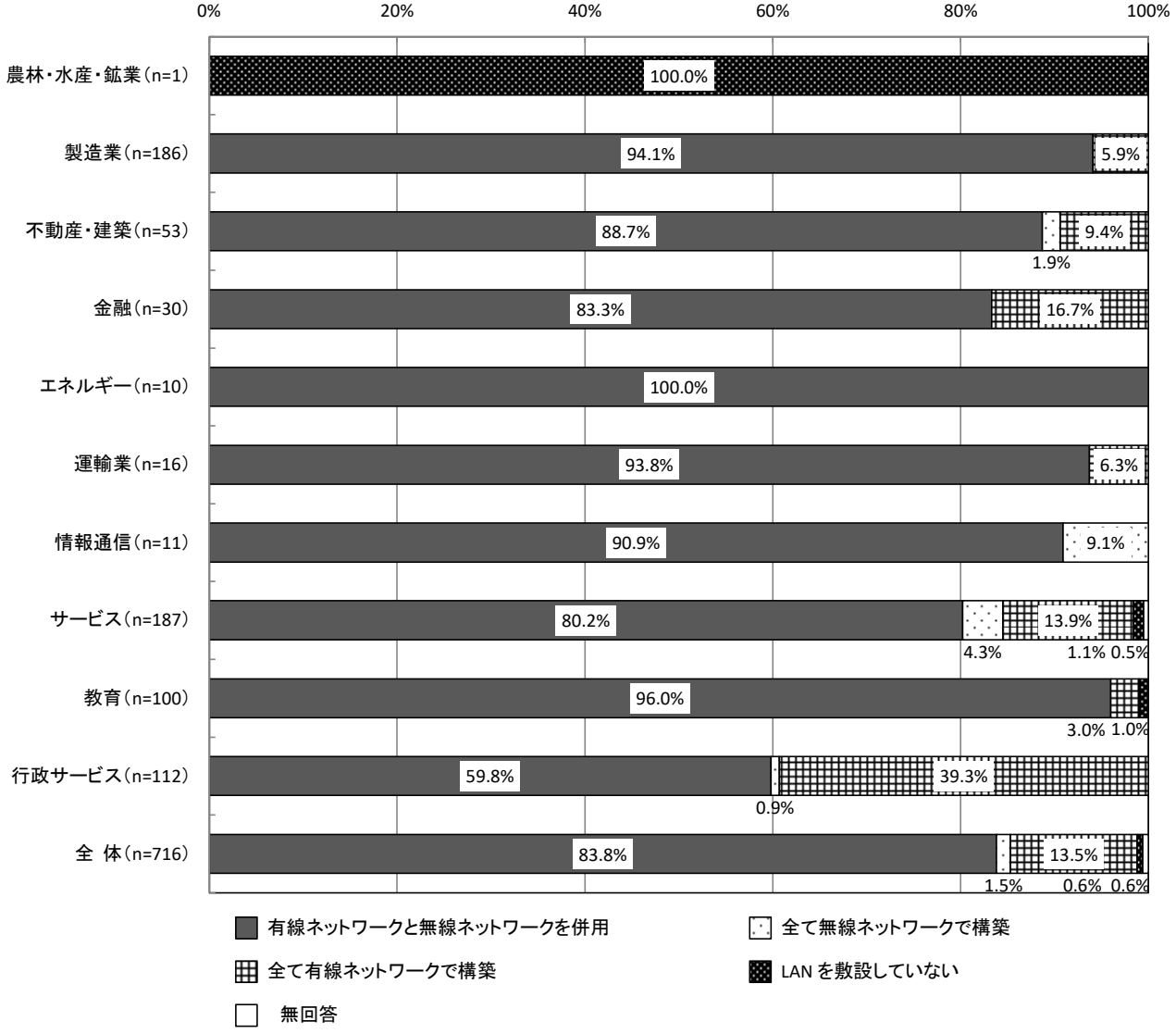
事業体内のネットワーク利用状況については、「有線ネットワークと無線ネットワークを併用」が83.8%で最も多く、次いで「全て有線ネットワークで構築」が13.5%となっている。

【全体】事業体内のネットワーク利用状況（SA, n=716）



【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」が100.0%で最も多く、次いで「教育」が96.0%、「製造業」が94.1%、「運輸業」が93.8%となっている。

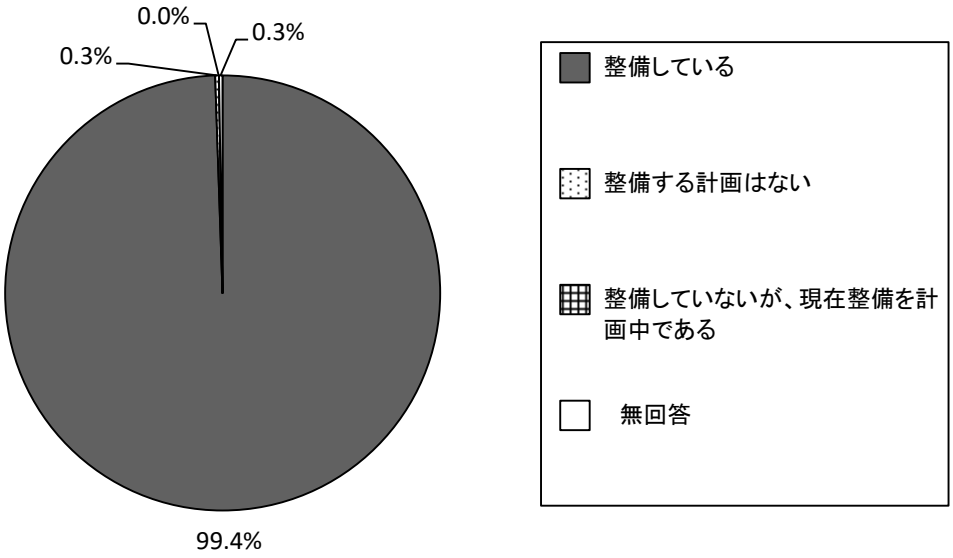
【業種別分析】事業体内のネットワーク利用状況



3.1.8 インターネット環境の整備　【問8】

インターネット環境の整備については、「整備している」が99.4%で最も多く、「整備する計画はない」は0.3%であった。

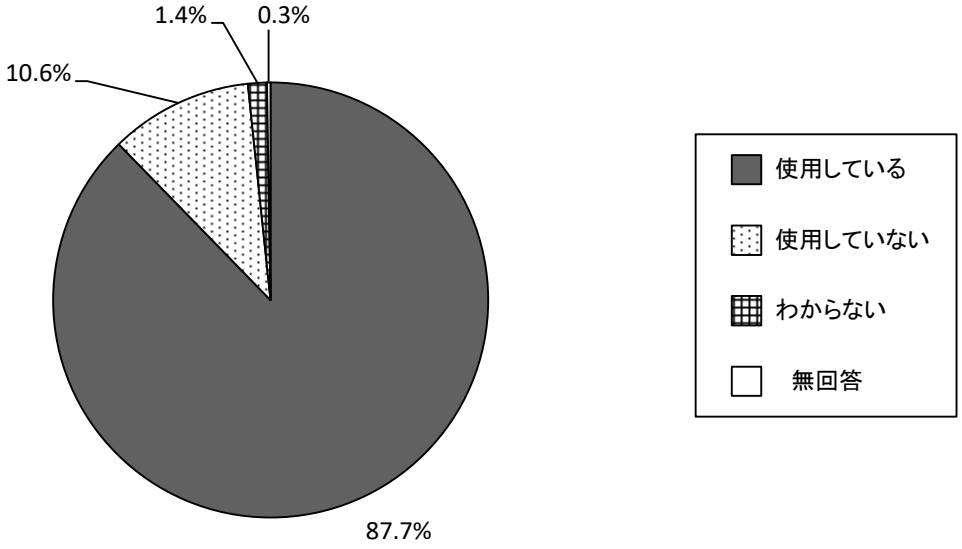
【全体】インターネット環境の整備（SA,n=716）



3.1.9　クラウドサービスの利用状況　【問9】

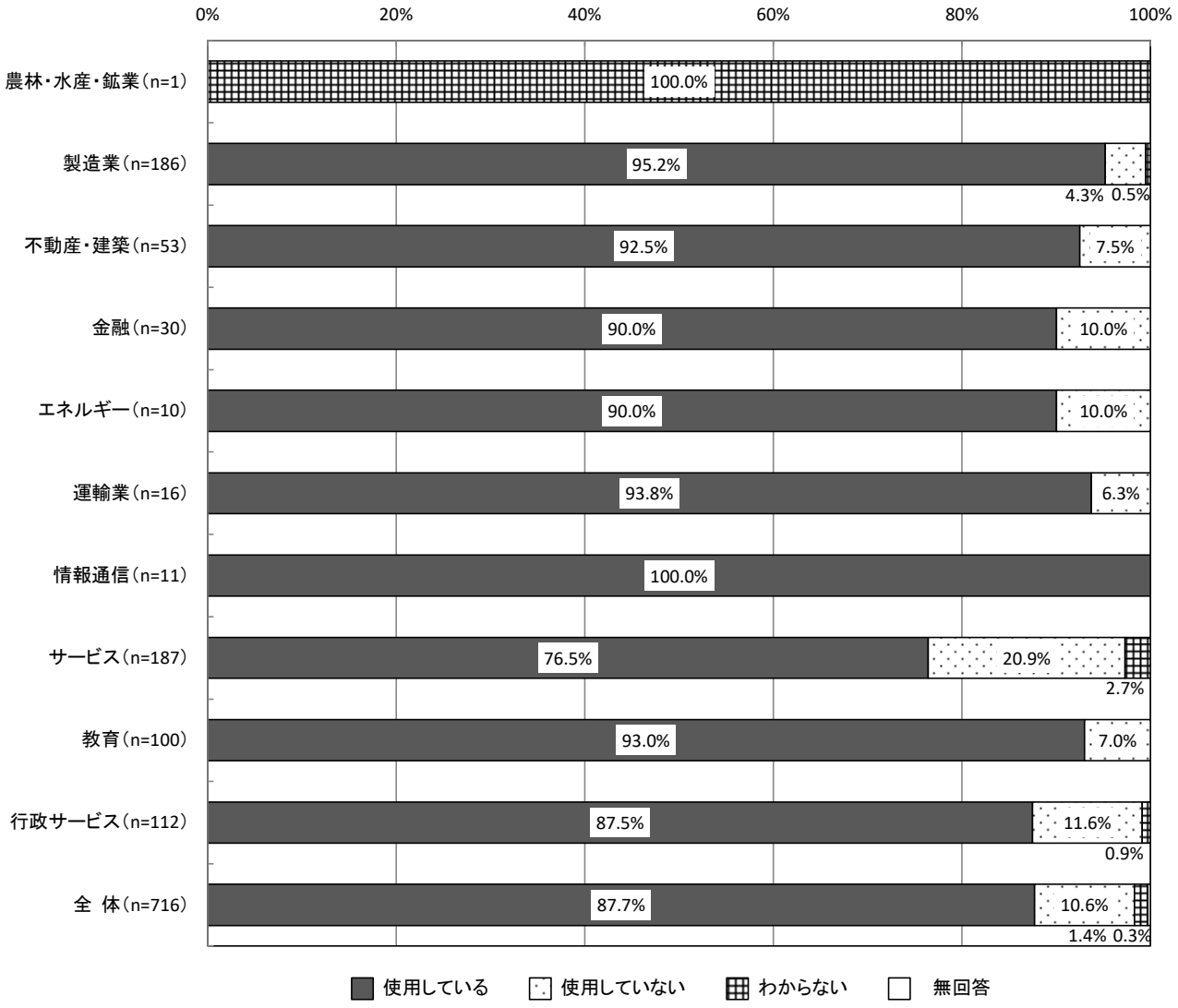
クラウドサービスの利用状況については、「使用している」が87.7%で最も多く、「使用していない」が10.6%、「わからない」が1.4%となっている。

【全体】クラウドサービスの利用状況（SA,n=716）



【業種別分析】業種別にみると、「使用している」については、「情報通信」が100.0%で最も多く、次いで「製造業」が95.2%、「運輸業」が93.8%、「教育」が93.0%となっている。

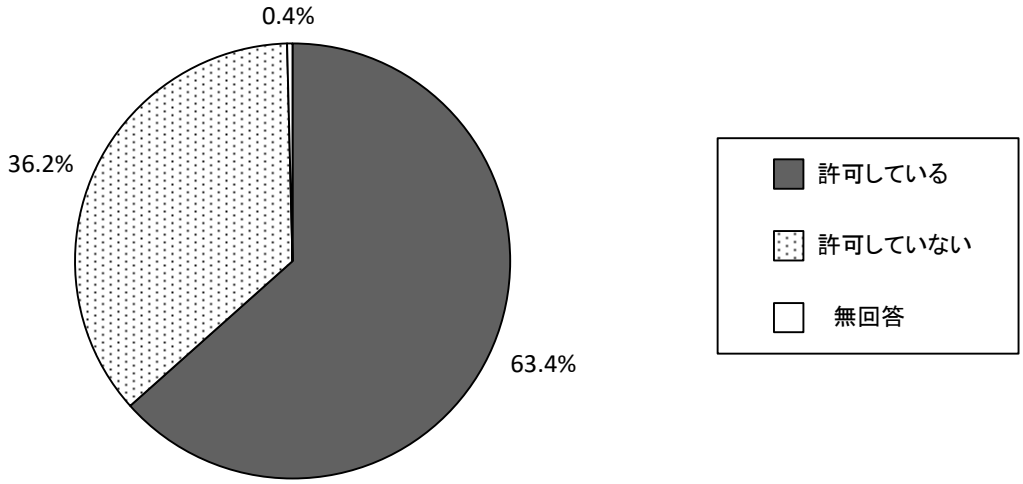
【業種別分析】クラウドサービスの利用状況



3.1.10　外部からの接続許可状況　【問10】

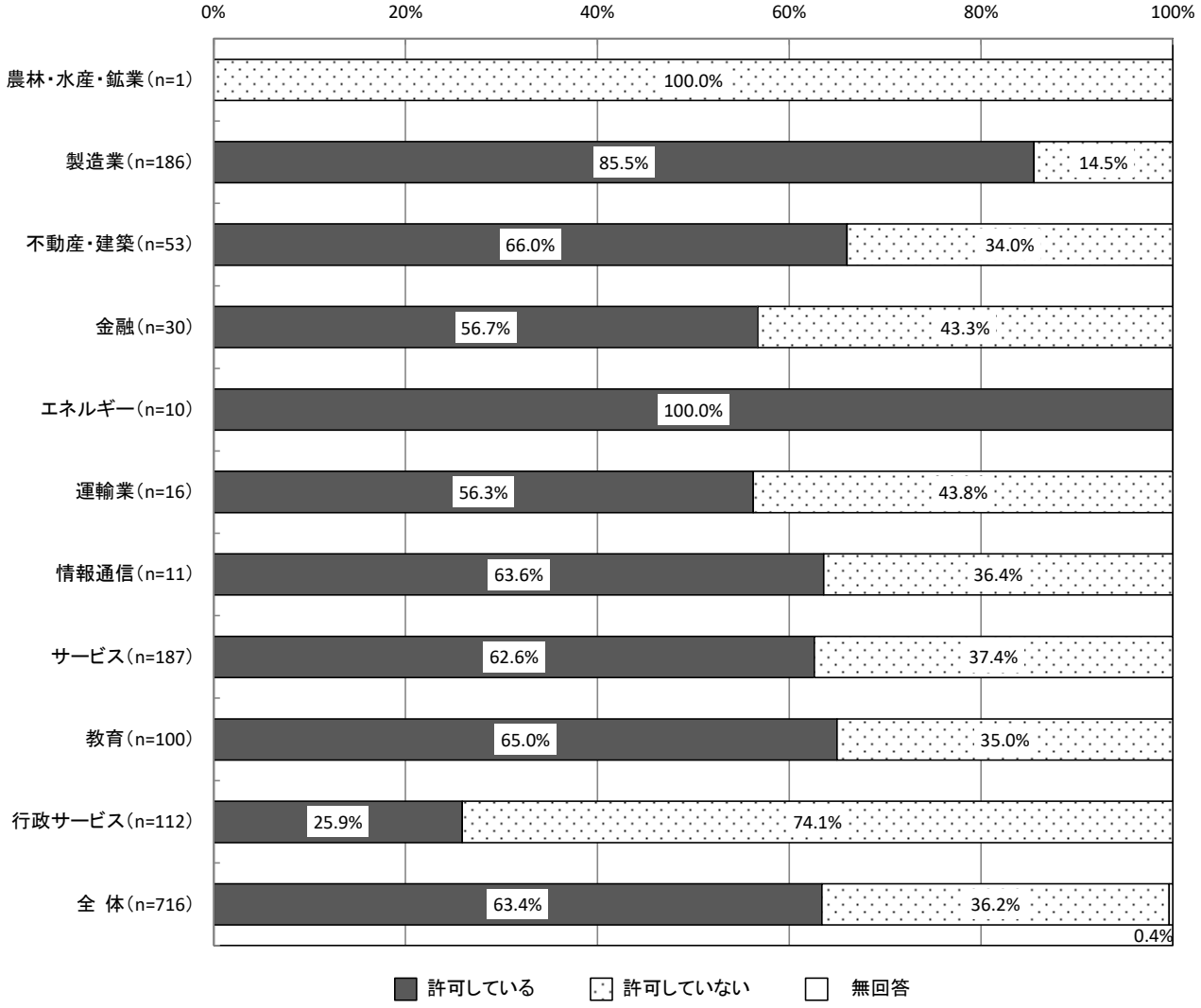
外部から事業体内ネットワークへの接続許可状況については、「許可している」が63.4%、「許可していない」は36.2%となっている。

【全体】外部からの接続許可状況（SA,n=716）

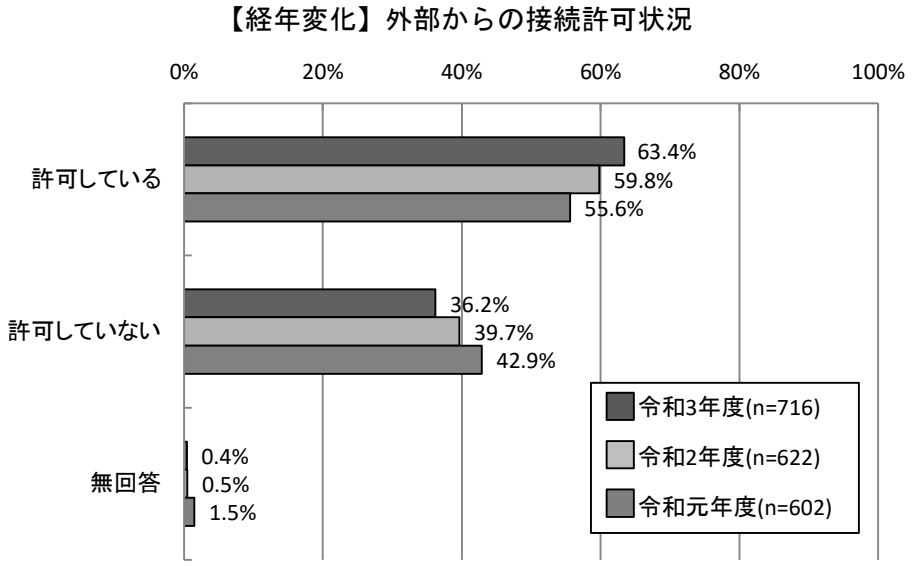


【業種別分析】業種別にみると、「許可している」では、「エネルギー」が100.0%で最も多く、次いで「製造業」が85.5%、「不動産・建築」が66.0%となっている。また、「許可していない」は「行政サービス」が74.1%で最も高い。

【業種別分析】外部からの接続許可状況



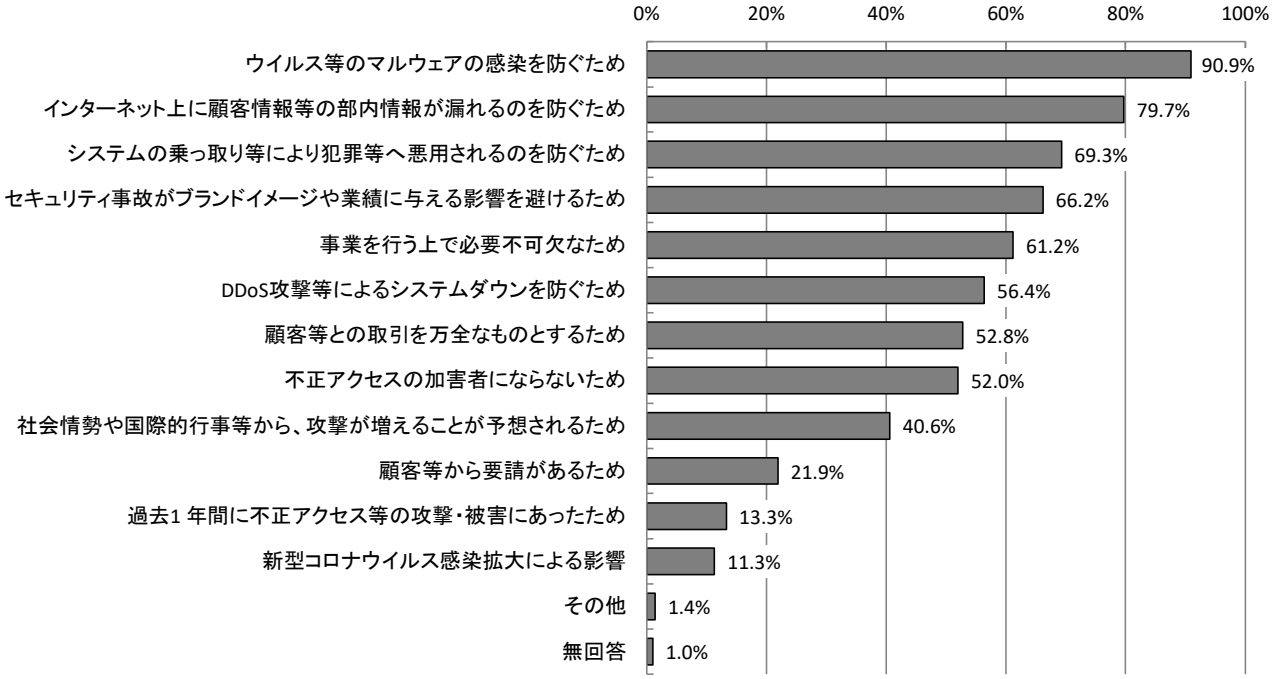
【経年変化】昨年度と比較すると、「許可している」が3.6ポイント増加し、「許可していない」が3.5ポイント減少している。



3.1.11　情報セキュリティ対策の必要性の理由【問11】

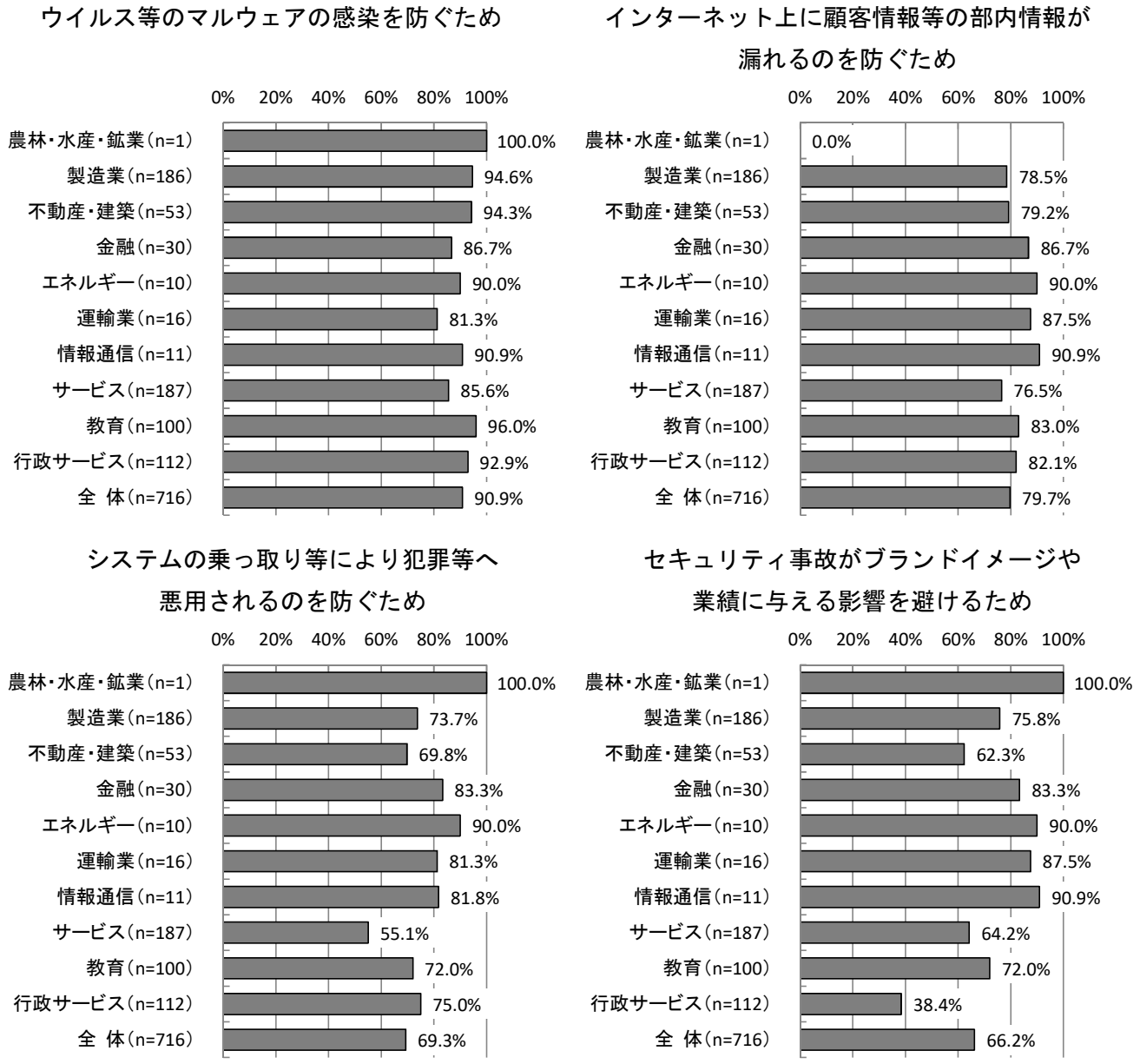
情報セキュリティ対策の必要性の理由については、「ウイルス等のマルウェアの感染を防ぐため」が90.9%で最も多く、次いで「インターネット上に顧客情報等の部内情報が漏れるのを防ぐため」が79.7%、「システムの乗っ取り等により犯罪等へ悪用されるのを防ぐため」が69.3%、「セキュリティ事故がブランドイメージや業績に与える影響を避けるため」が66.2%となっている。

【全体】情報セキュリティ対策の必要性の理由（MA, n=716）

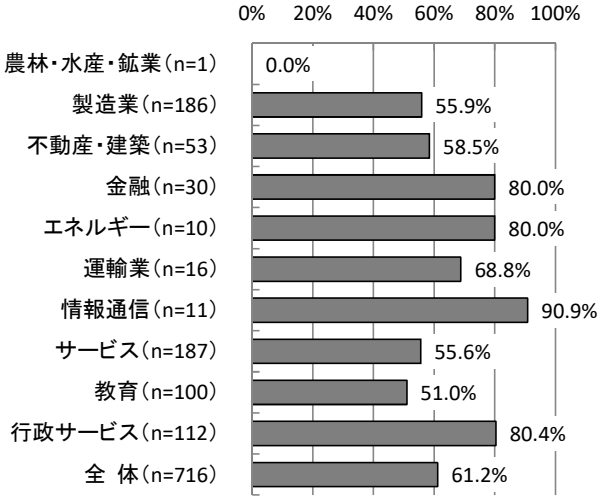


【業種別分析】業種別にみると、「ウイルス等のマルウェアの感染を防ぐため」については、「教育」が96.0%、「インターネット上に顧客情報等の部内情報が漏れるのを防ぐため」については、「情報通信」が90.9%、「システムの乗っ取り等により犯罪等へ悪用されるのを防ぐため」では「エネルギー」が90.0%、「セキュリティ事故がブランドイメージや業績に与える影響を避けるため」については、「情報通信」が90.9%と多くなっている。また、「事業を行う上で必要不可欠なため」については、「情報通信」が90.9%、「DDoS攻撃等によるシステムダウンを防ぐため」については、「エネルギー」が90.0%、、「顧客等との取引を万全なものとするため」については、「運輸業」が81.3%「不正アクセスの加害者にならないため」については、「エネルギー」が80.0%と多くなっている。

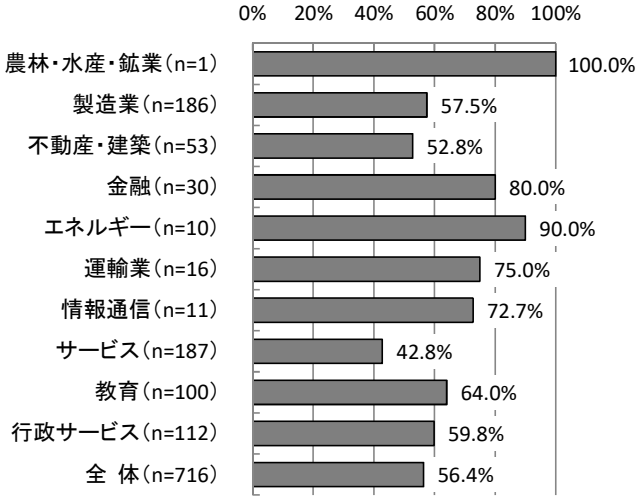
【業種別分析】情報セキュリティ対策の必要性の理由



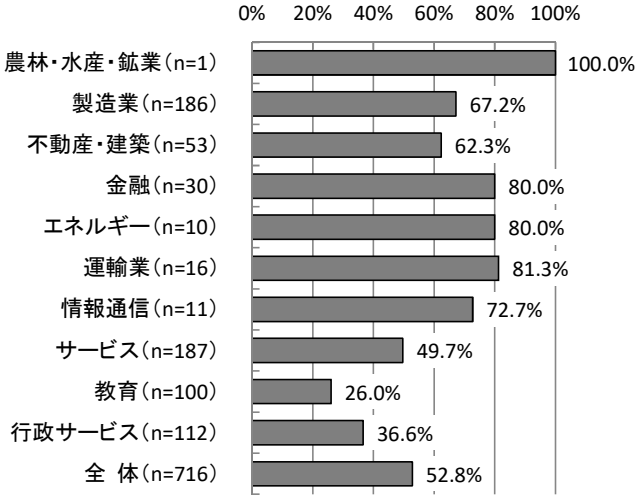
事業を行う上で必要不可欠なため



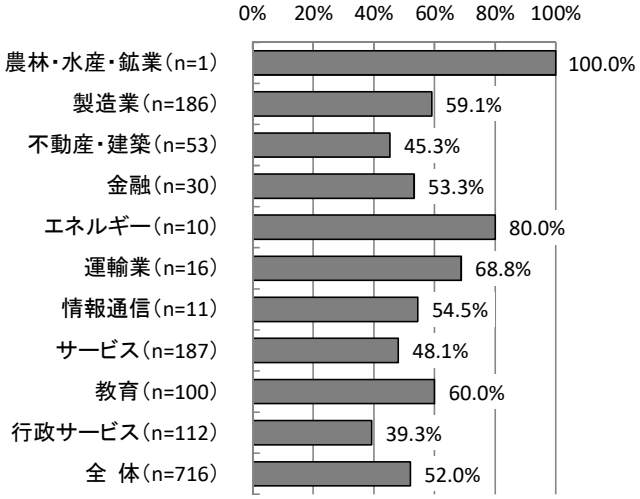
DDoS攻撃等によるシステムダウンを防ぐため



顧客等との取引を万全なものとするため

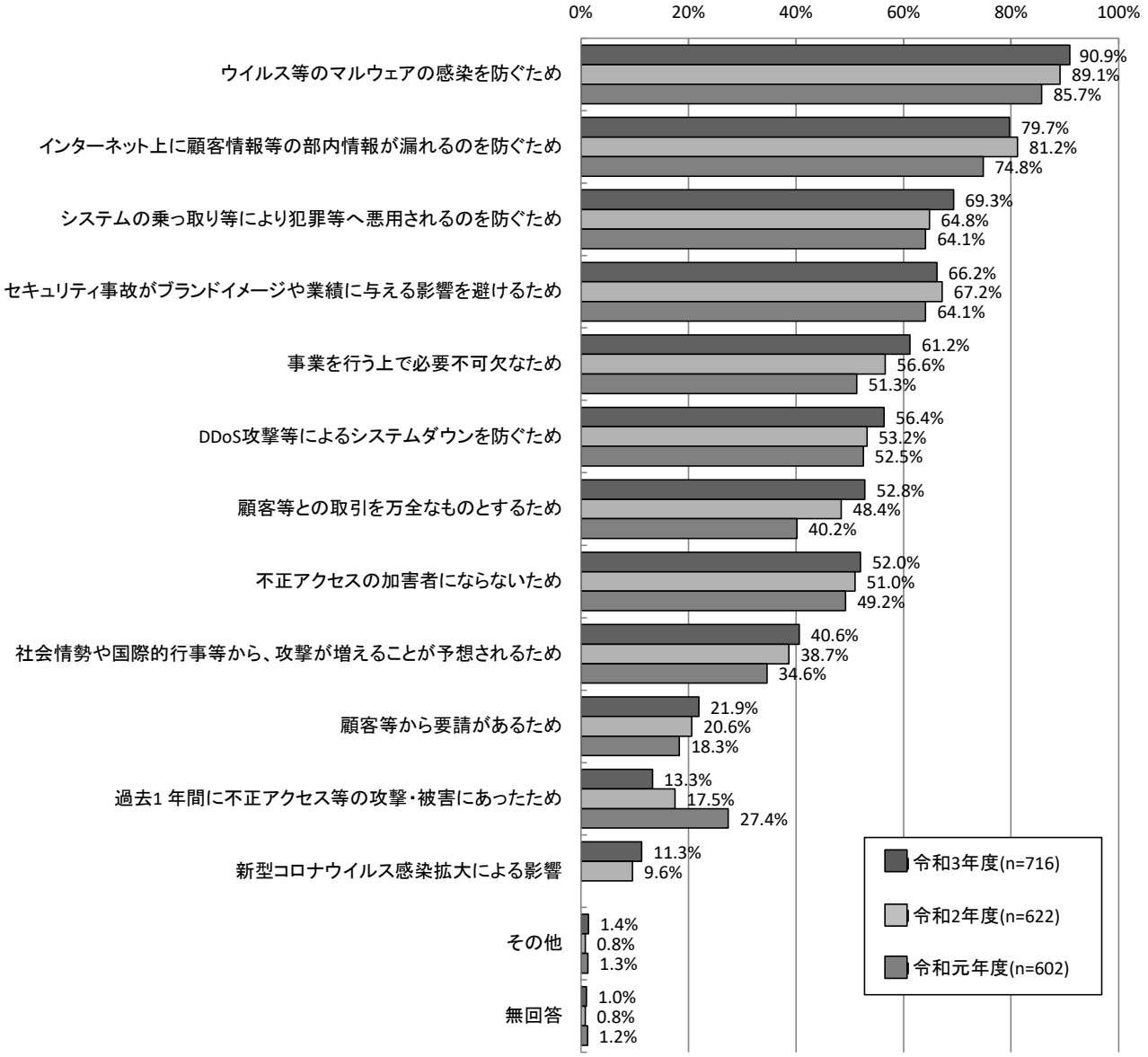


不正アクセスの加害者にならないため



【経年変化】昨年度と比較すると、「事業を行う上で必要不可欠なため」が4.6ポイント、「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4.5ポイント増加し、「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4.2ポイント減少している。

【経年変化】情報セキュリティ対策の必要性の理由



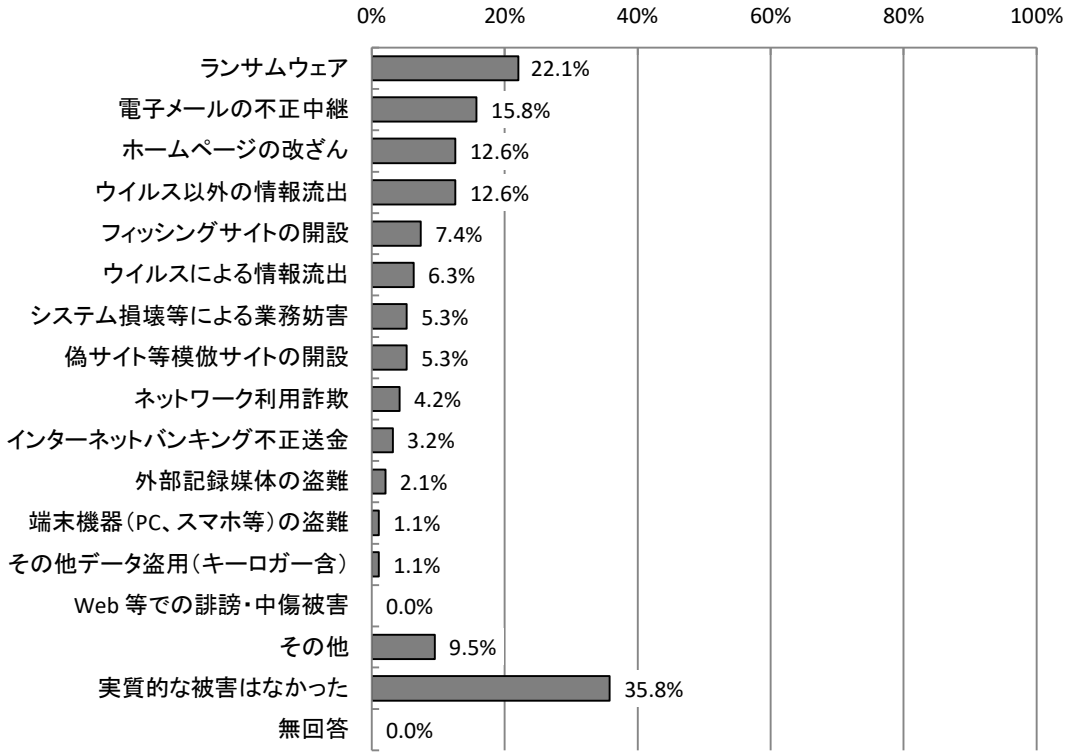
※令和２年度調査で、「新型コロナウィルス感染拡大による影響」を新設。

3.1.12　過去に受けたことのある被害状況　【問11-1-1】

過去に受けたことのある被害状況については、「ランサムウェア」が22.1%で最も多く、次いで「電子メールの不正中継」が15.8%、「ホームページの改ざん」と「ウイルス以外の情報流出」が12.6%となっている。また、「実質的な被害はなかった」が35.8%となっている。

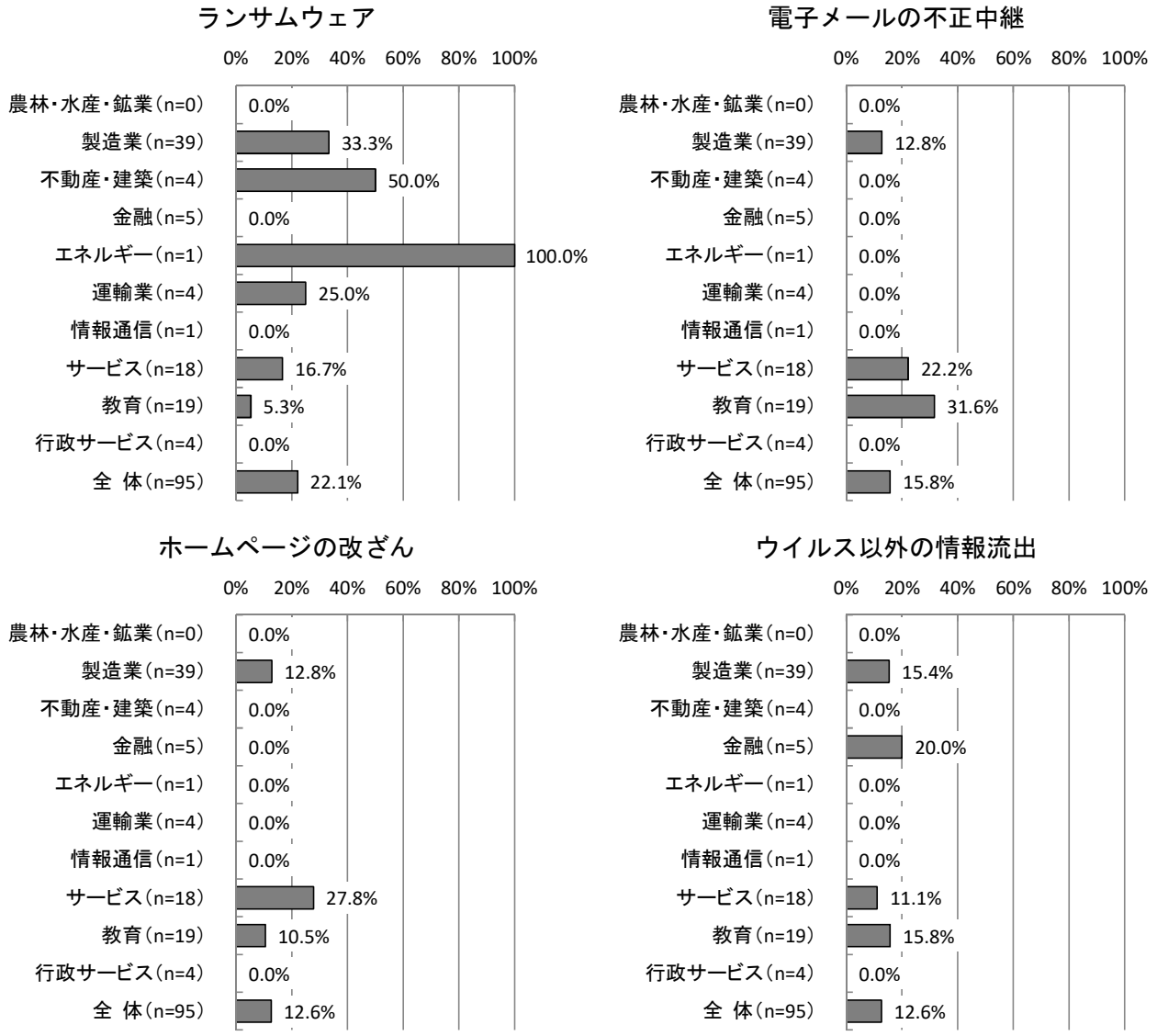
※本項目は、過去に不正アクセス等の被害にあった社・団体等を対象としている。

【全体】過去に受けたことのある被害状況（MA,n=95）



【業種別分析】業種別にみると、「ランサムウェア」については、「製造業」が33.3%で最も多くなっている。「電子メールの不正中継」については、「教育」が31.6%となっている。また、「ホームページの改ざん」については、「サービス」が27.8%と最も多くなっている。

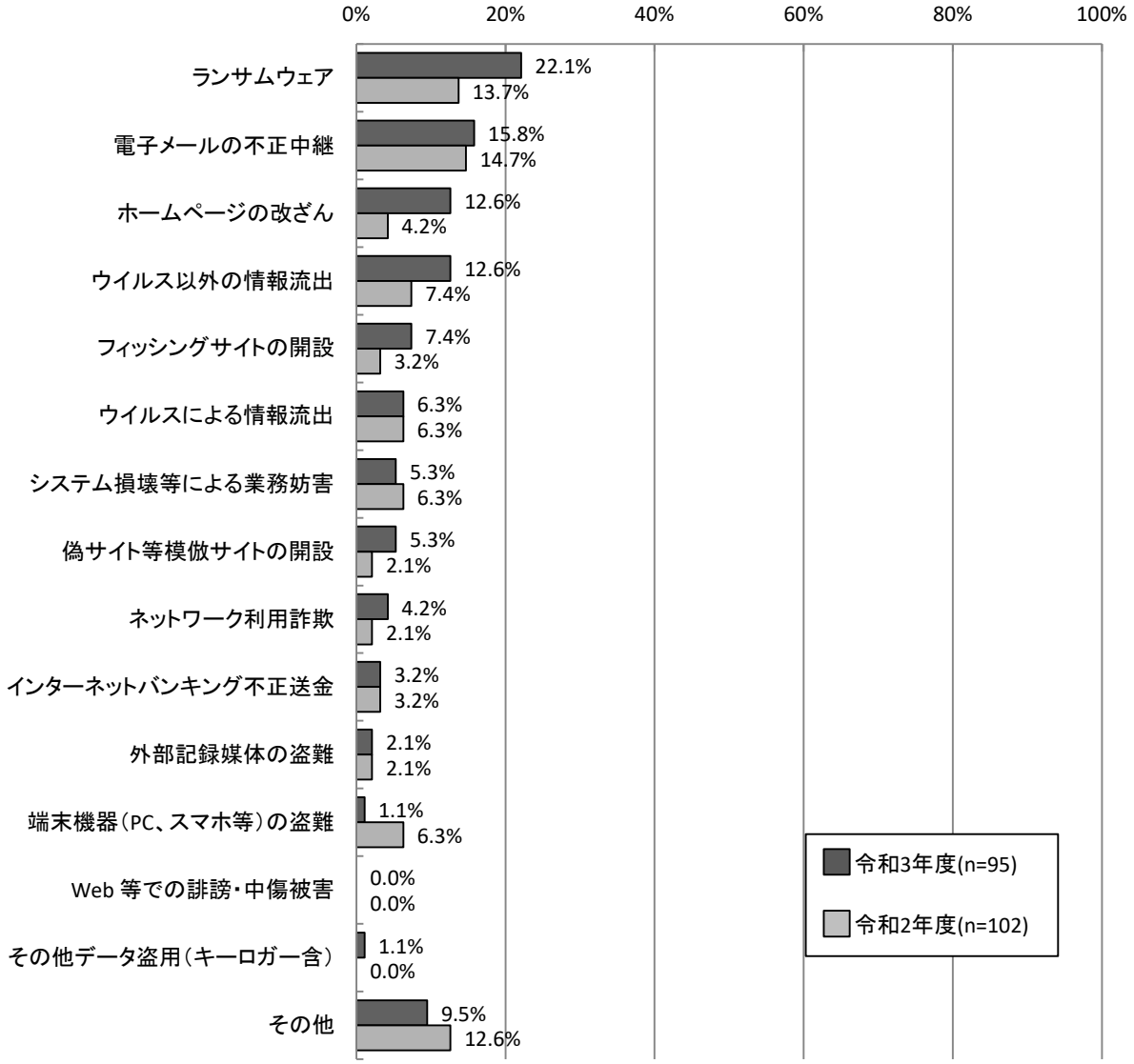
【業種別分析】過去に受けたことのある被害状況



【経年変化】昨年度と比較すると、「システム損壊等による業務妨害」を除く全項目で増加または横ばいとなっており、「ランサムウェア」と「ホームページの改ざん」が8.4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】過去に受けたことのある被害状況

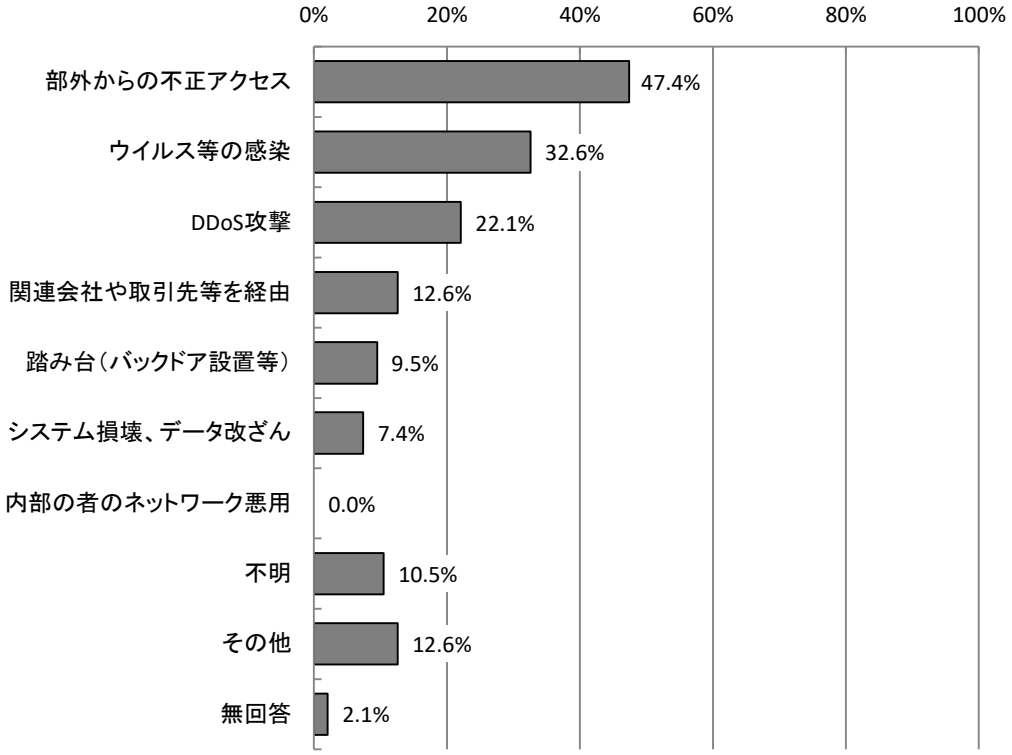


3.1.13　攻撃手段　【問11-1-2】

攻撃手段については、「部外からの不正アクセス」が47.4%で最も多く、次いで「ウイルス等の感染」が32.6%、「DDoS攻撃」が22.1%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。

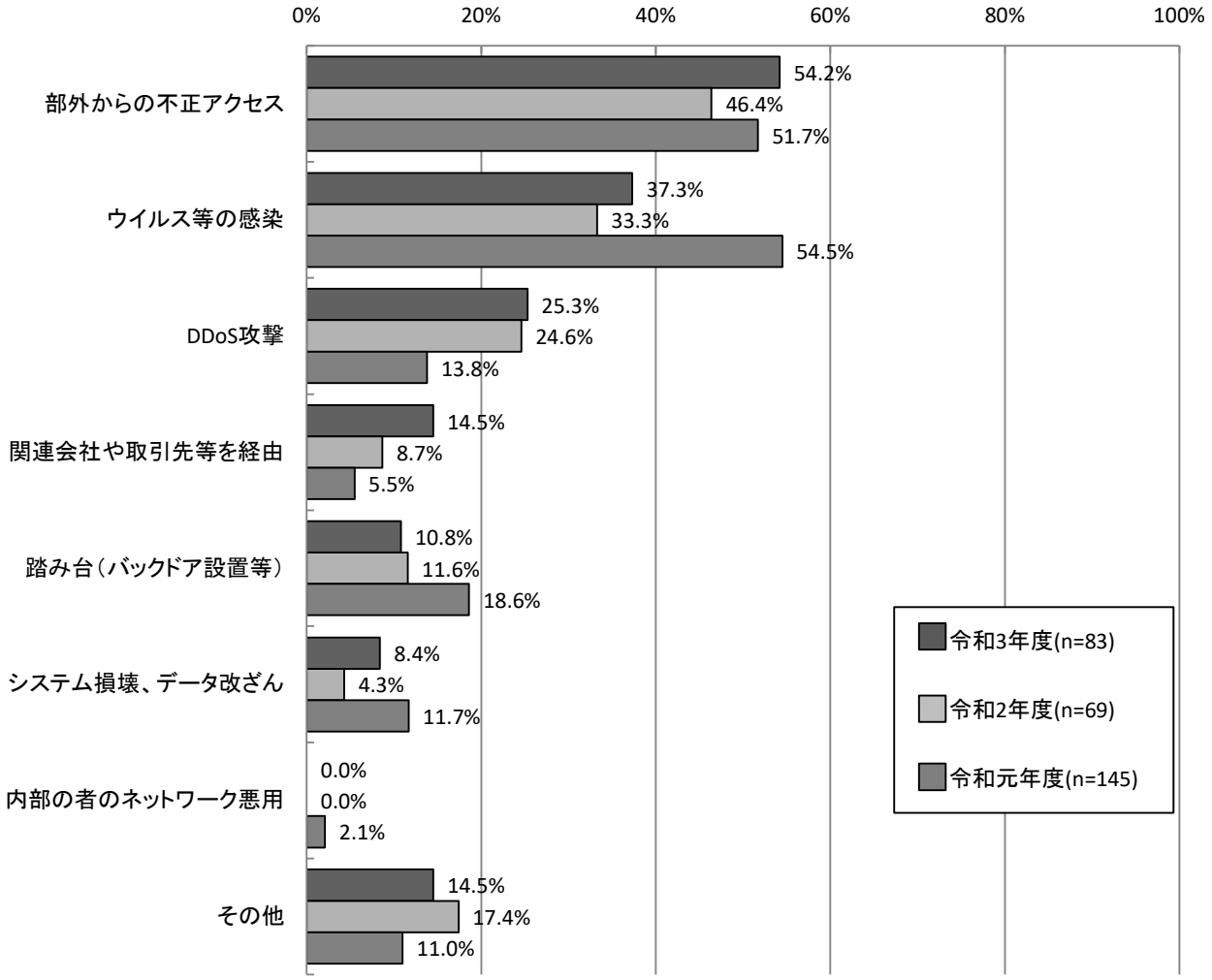
【全体】攻撃手段（MA,n=95）



【経年変化】昨年度と比較すると、「踏み台（バックドア設置等）」をのぞく全ての項目で増加または横ばいとなっており、「部外からの不正アクセス」は7.8ポイント増加している。

※「不明」「無回答」を除いた総数で比較している。

【経年変化】攻撃手段

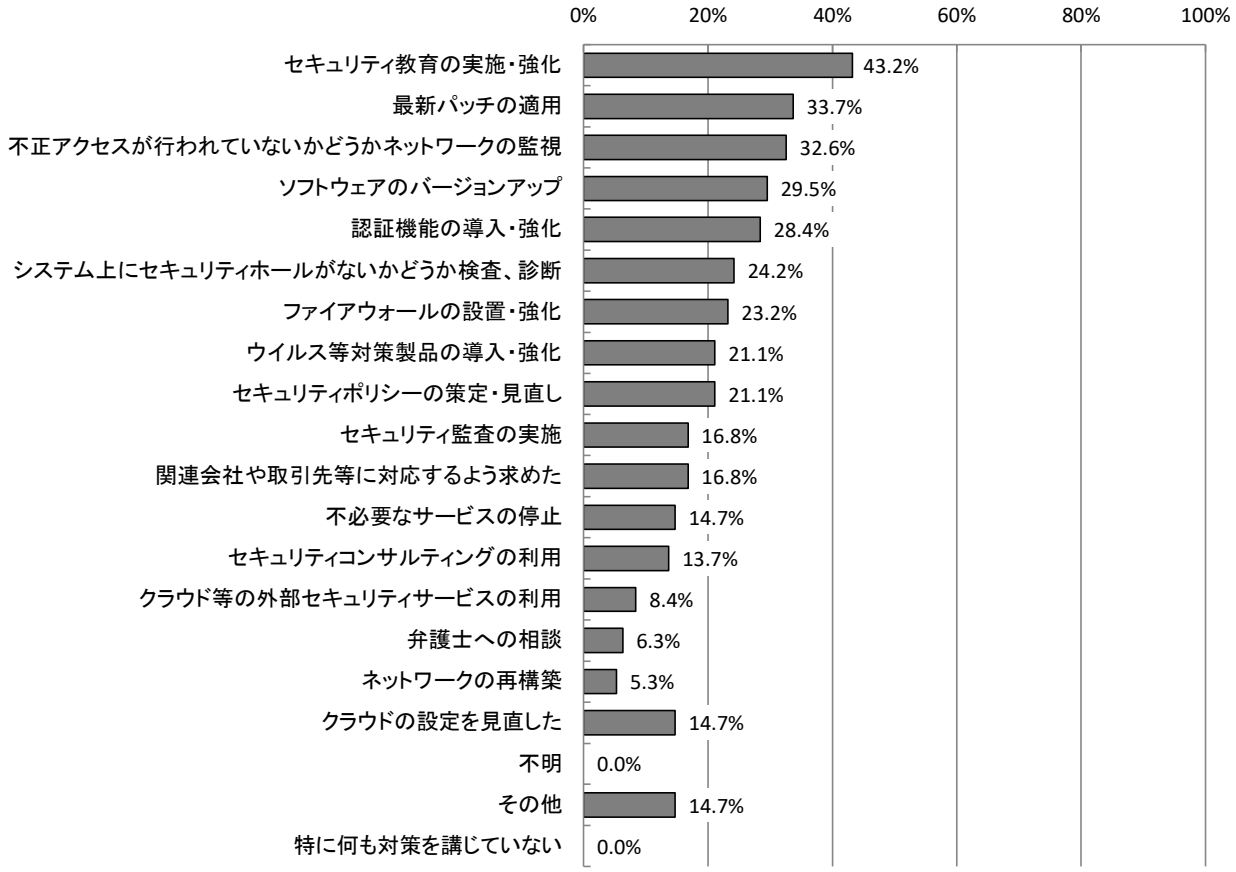


3.1.14　被害を受けたことによる対策　【問11-2】

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43.2%で最も多く、次いで「最新パッチの適用」が33.7%、「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32.6%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。

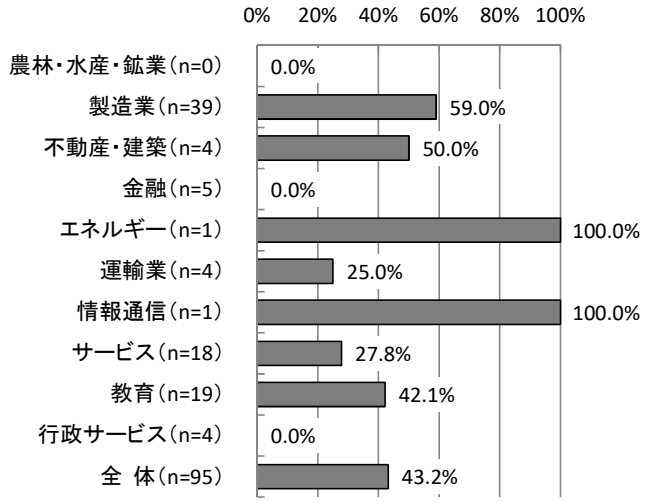
【全体】被害を受けたことによる対策（MA,n=95）



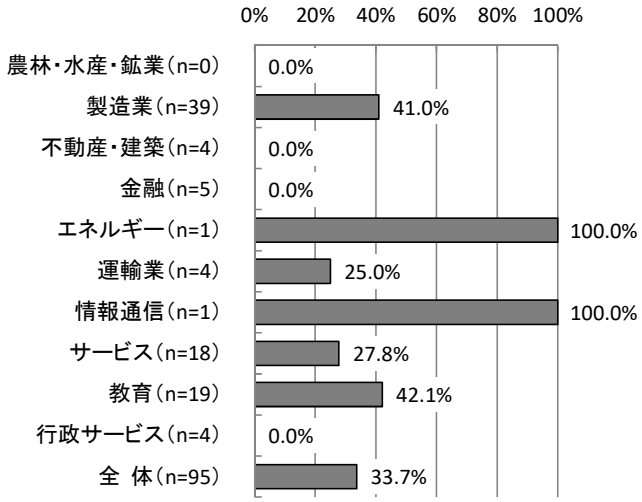
【業種別分析】業種別にみると、「セキュリティ教育の実施・強化」については、「製造業」が59.0%で最も多くなっている。また、「最近パッチの適用」では、「教育」が42.1%で最も多くなっている。

【業種別分析】被害を受けたことによる対策

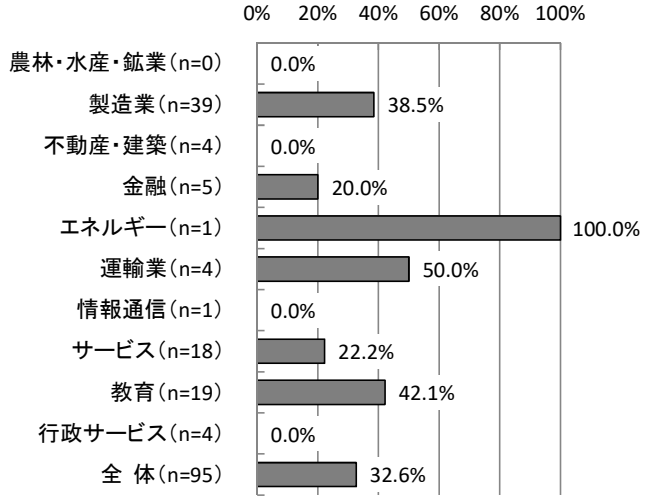
セキュリティ教育の実施・強化



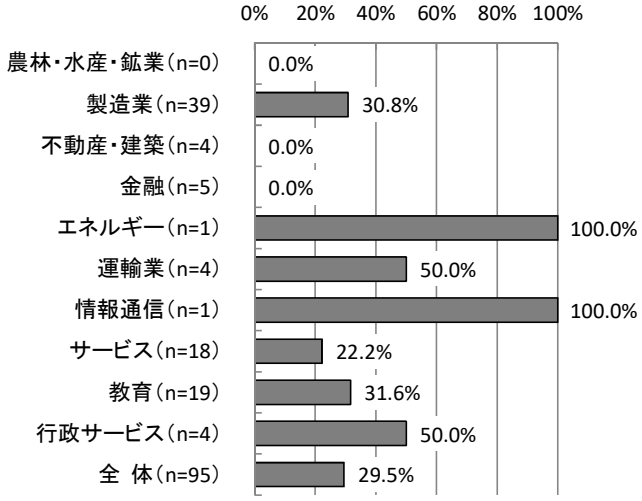
最新パッチの適用



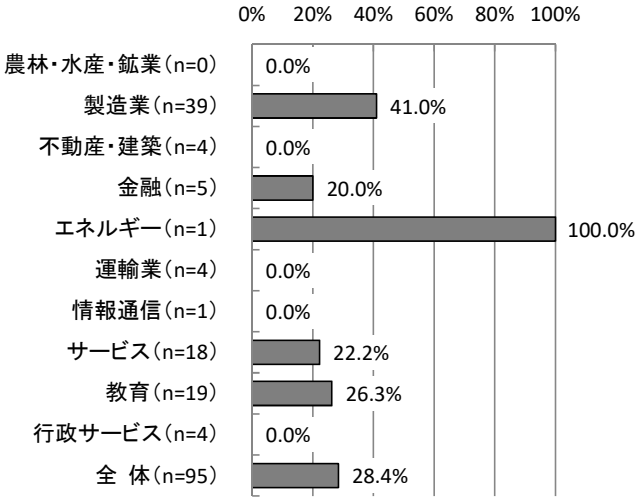
不正アクセスが行われていないかどうか
ネットワークの監視



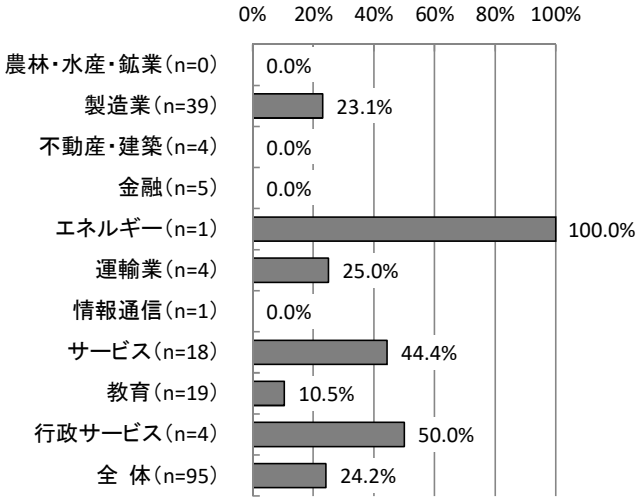
ソフトウェアのバージョンアップ



認証機能の導入・強化



システム上にセキュリティホールがないかどうか検査、診断

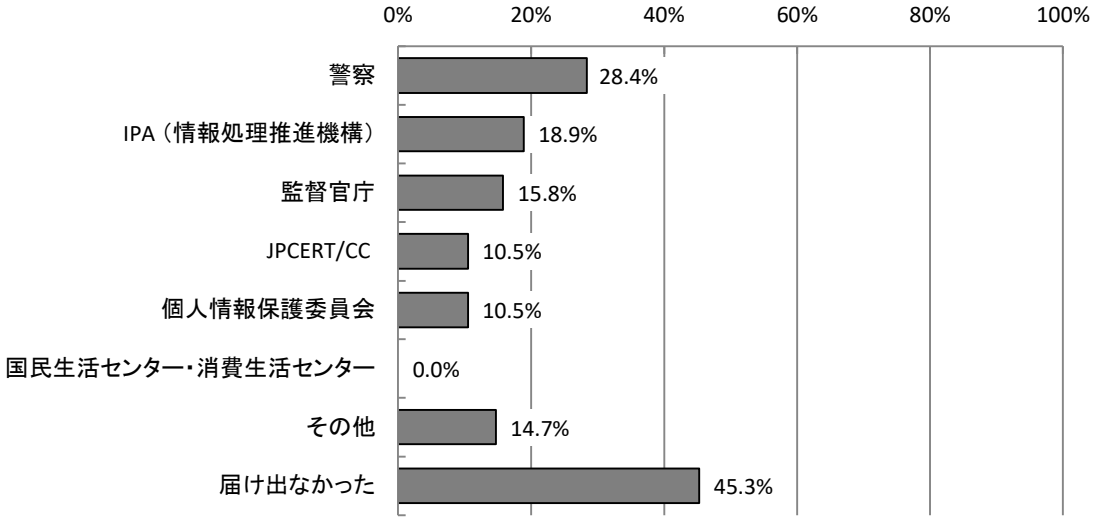


3.1.15　届出先機関等　【問11-3-1】

届出先機関等については、「警察」が28.4%で最も多く、次いで「IPA（情報処理推進機構）」が18.9%、「監督官庁」が15.8%となっている。一方、「届け出なかった」は45.3%となっている。

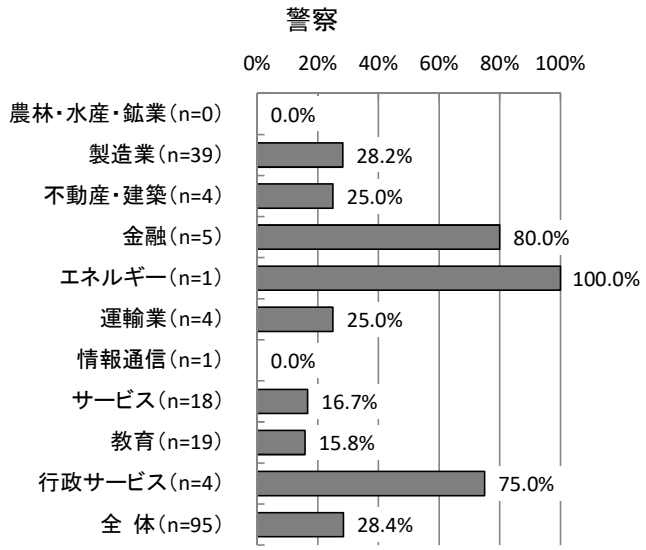
※本項目は、過去に不正アクセス等の被害にあった社・団体等を対象としている。

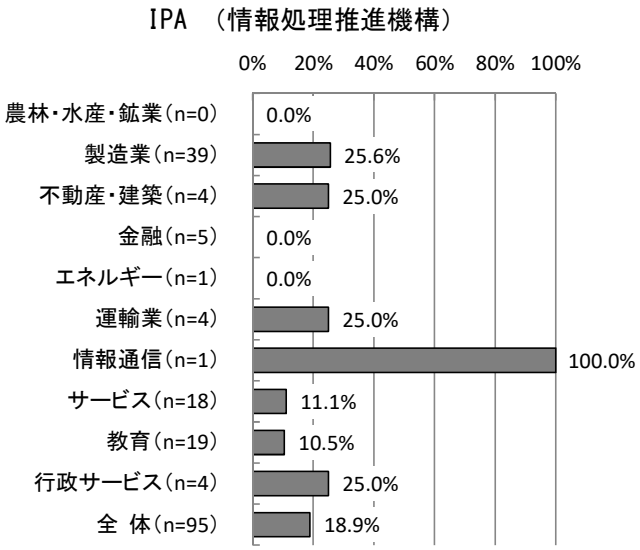
【全体】届出先機関等（MA, n=95）

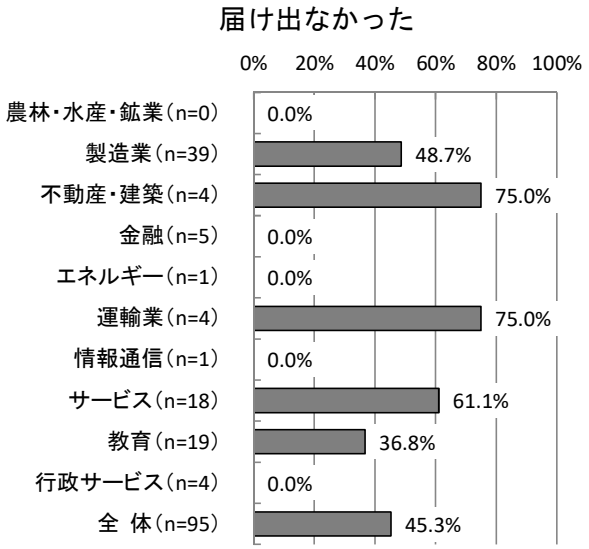


【業種別分析】業種別にみると、「警察」については「金融」が80.0%で最も多くなっている。「届け出なかった」については、「サービス」が61.1%と多くなっている。

【業種別分析】届出先機関等



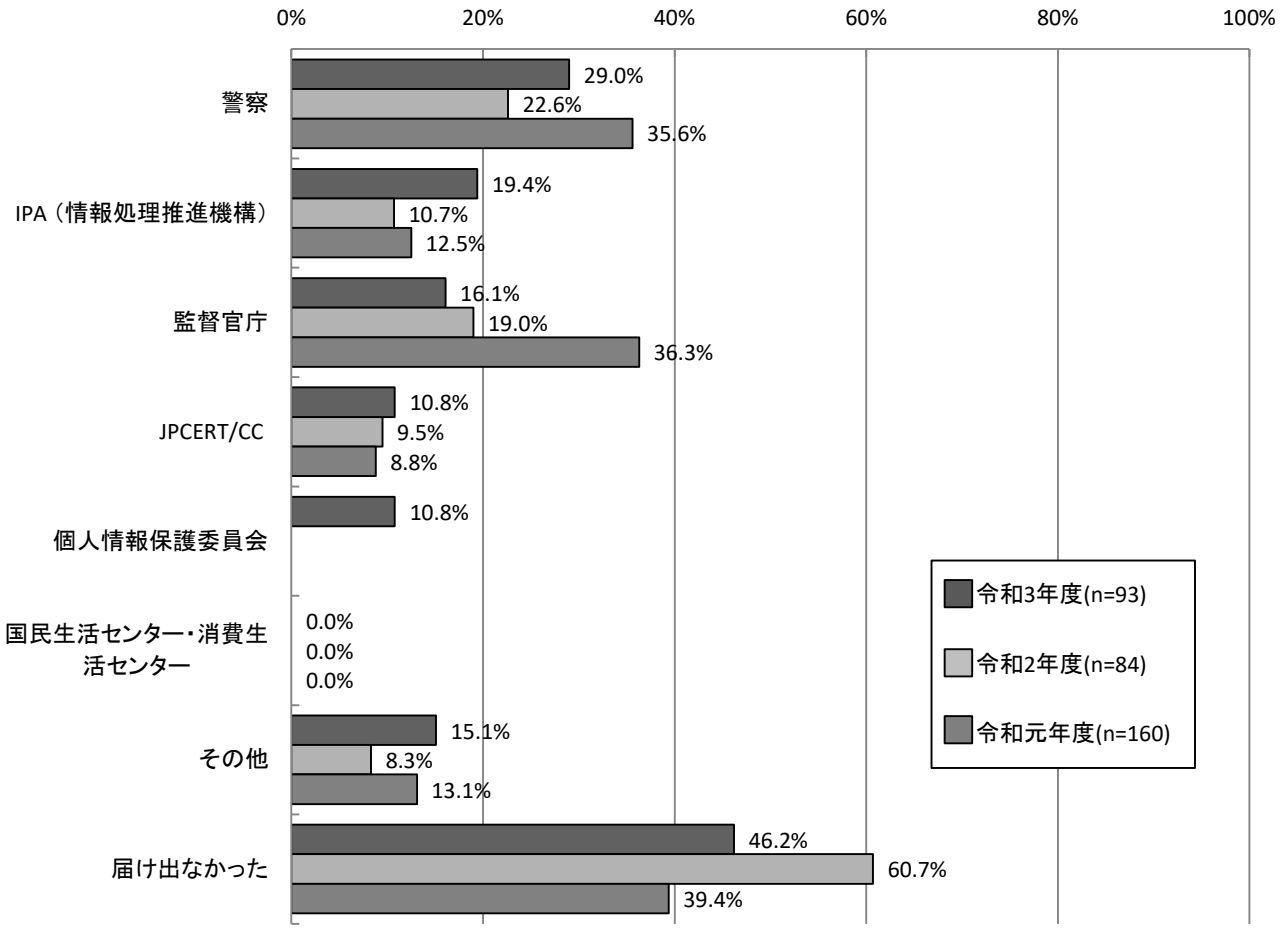




【経年変化】昨年度と比較すると、「警察」は6.4ポイント、「IPA （情報処理推進機構）」は8.7ポイント、「JPCERT/CC」は1.3ポイントそれぞれ増加している。一方で、「届け出なかった」は14.5ポイント減少している。

※「無回答」を除いた総数で比較している。

【経年変化】届出先機関等



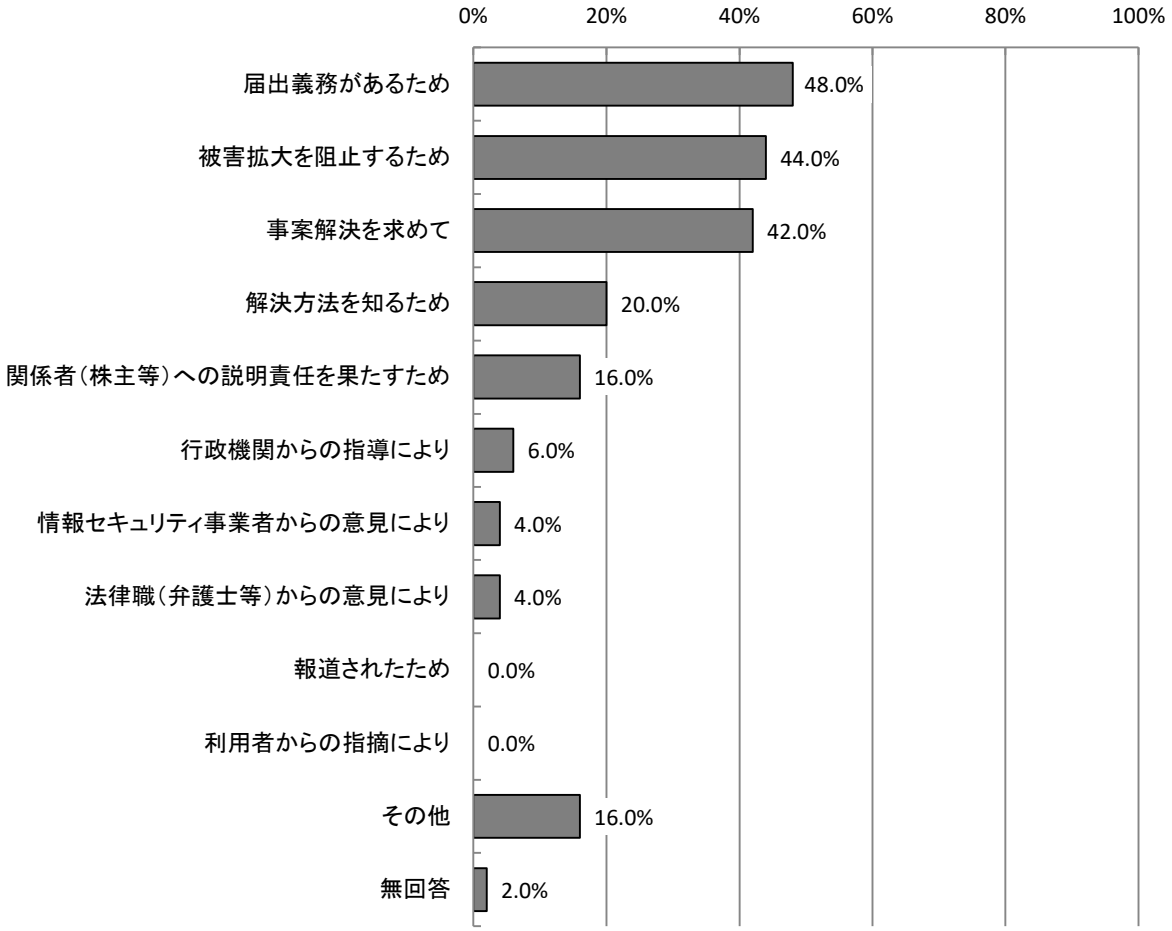
※令和３年度調査で、「個人情報保護委員会」を新設。

3.1.16　届出した理由　【問11-3-2】

届出した理由については、「届出義務があるため」が48.0%で最も多く、次いで「被害拡大を阻止するため」が44.0%、「事案解決を求めて」が42.0%となっている。

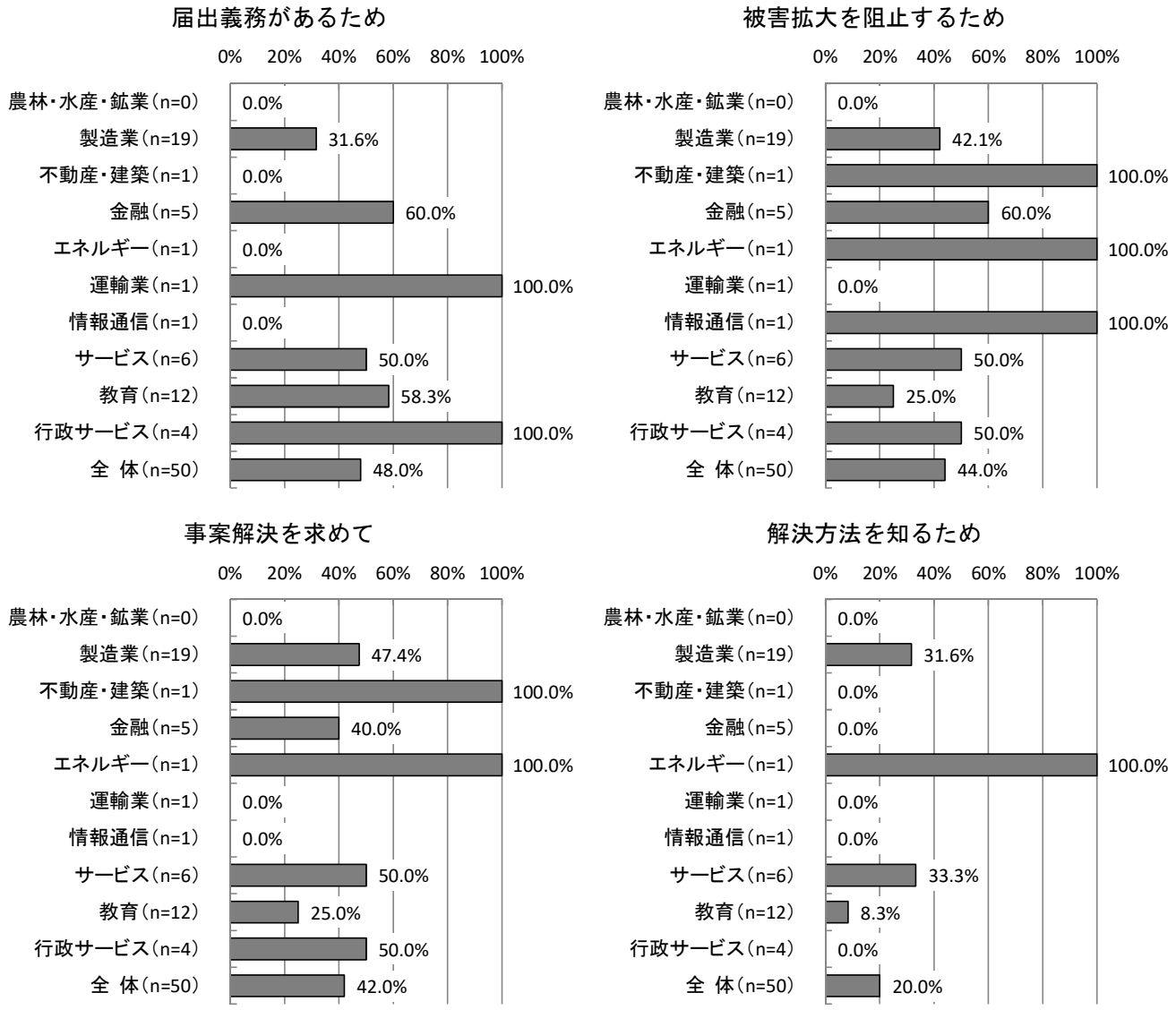
※本項目は、被害の届出を行った社・団体等を対象としている。

【全体】届出した理由（MA,n=50）



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

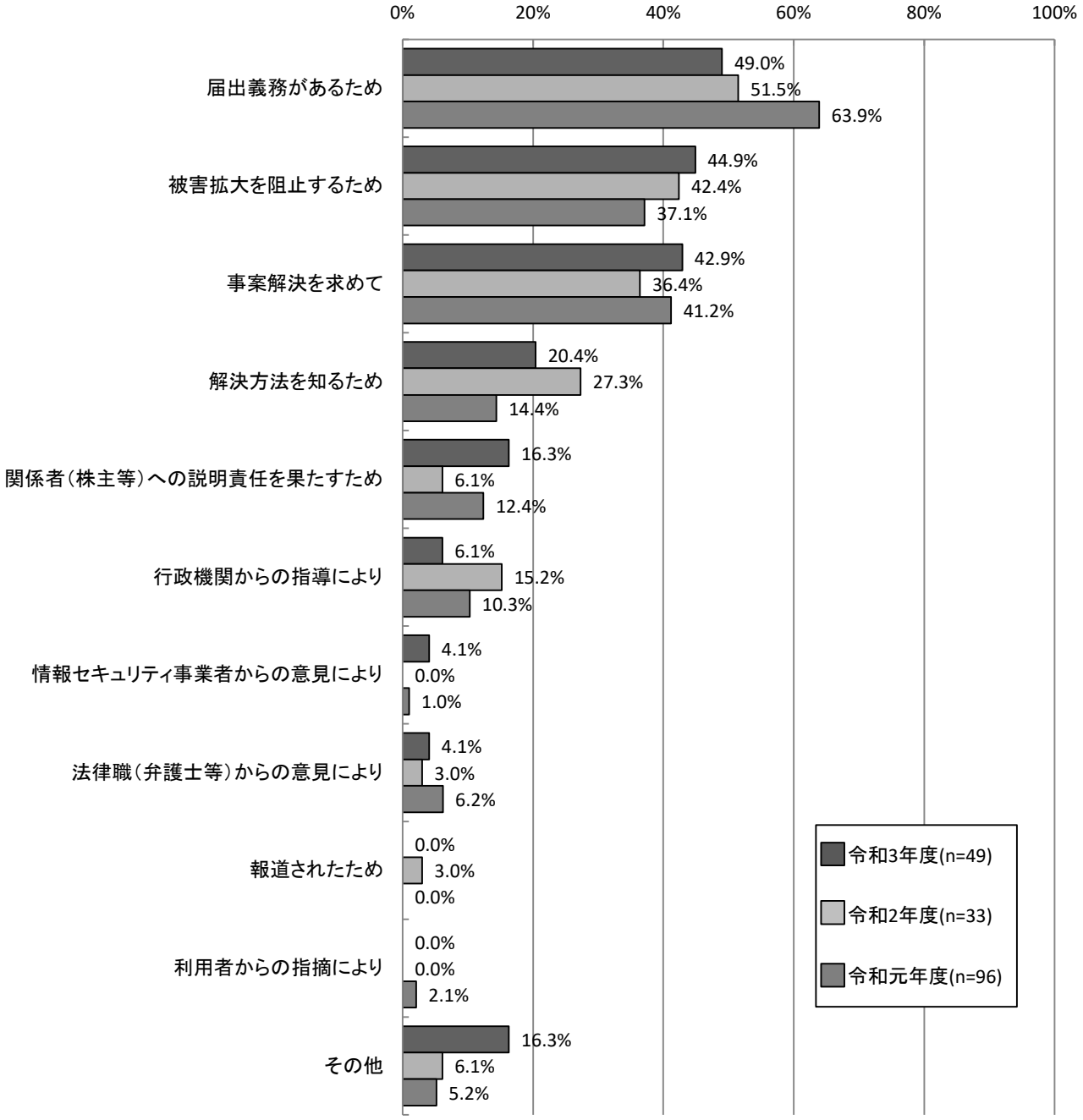
【業種別分析】届出した理由



【経年変化】昨年度と比較すると、「関係者（株主等）への説明責任を果たすため」が10.2ポイント増加し、「行政機関からの指導により」が9.1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。

【経年変化】届出した理由

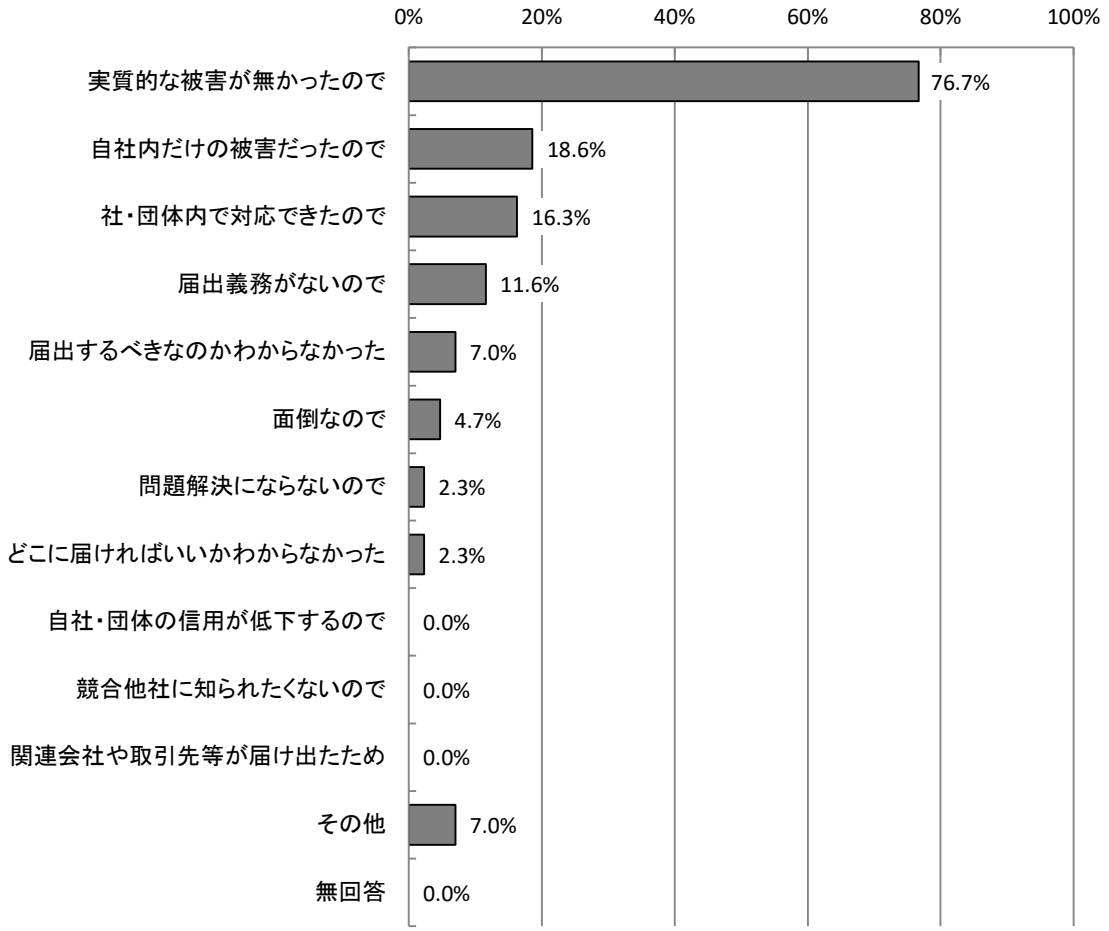


3.1.17　届出を躊躇させる要因　【問11-4】

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76.7%で最も多く、次いで「自社内だけの被害だったので」が18.6%、「社・団体内で対応できたので」が16.3%となっている。

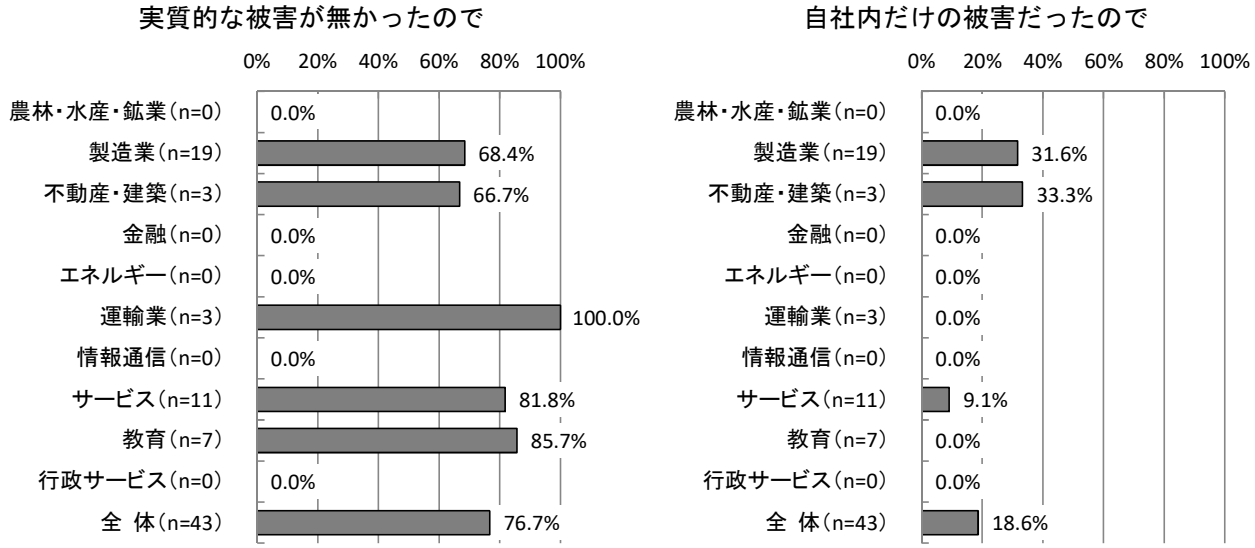
※本項目は、被害の届出を行わなかった社・団体等を対象としている。

【全体】届出を躊躇させる要因（MA,n=43）



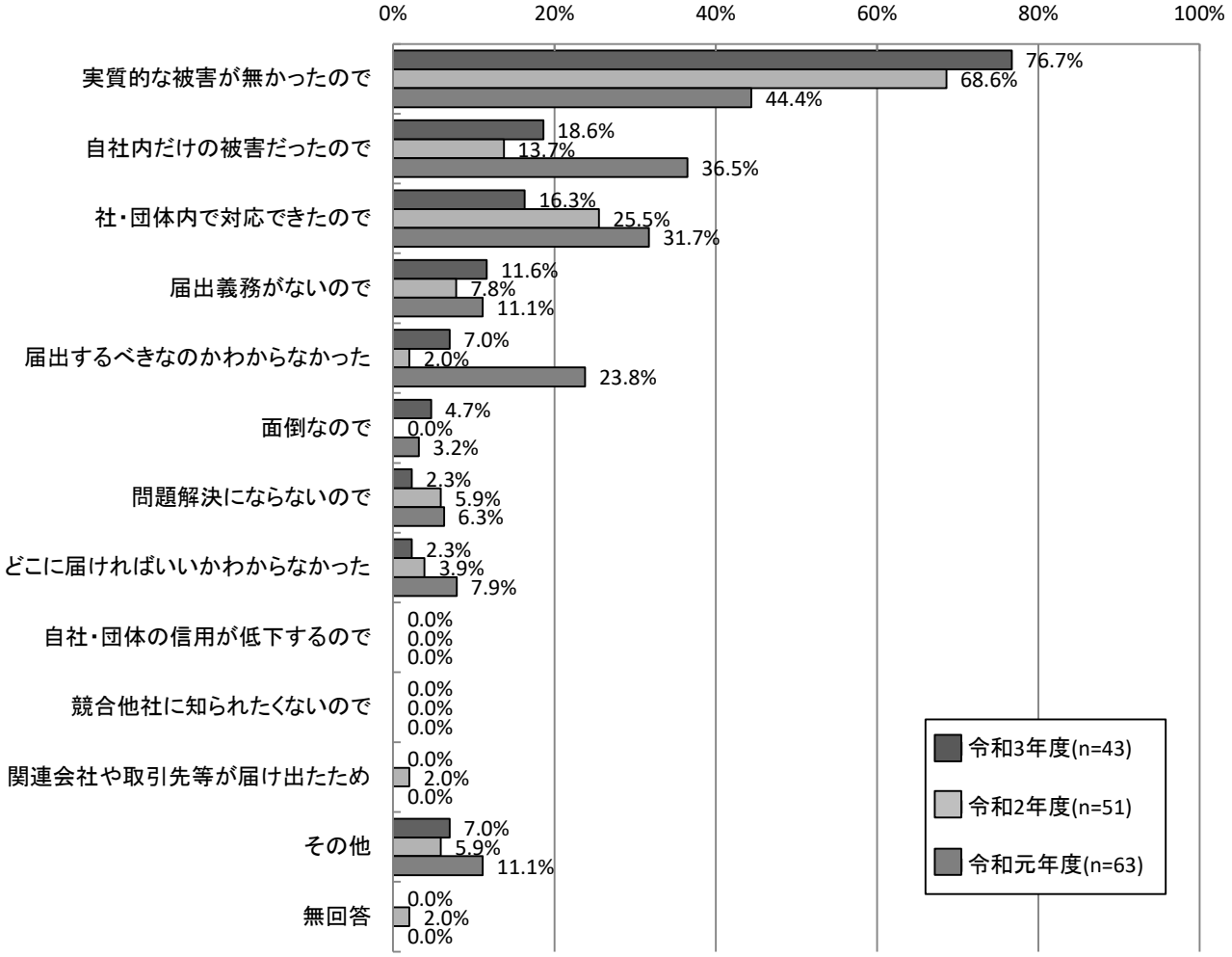
【業種別分析】業種別にみると、「実質的な被害が無かったので」については、「教育」が85.7%、「サービス」が81.8%となっている。「自社内だけの被害だったので」については、「製造業」が31.6%となっている。

【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8.1ポイントの増加であった。一方、「社・団体内で対応できたので」は9.2ポイント減少している。

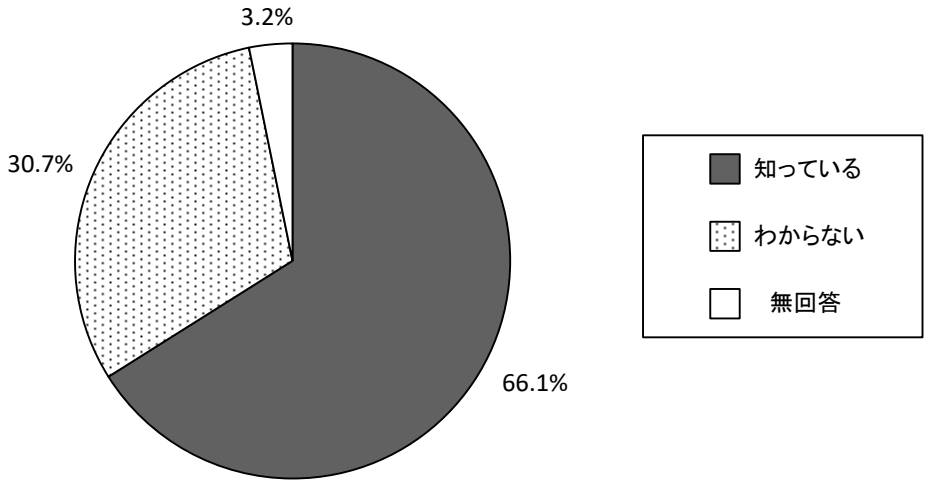
【経年変化】届出を躊躇させる要因



3.1.18　届出先機関を知っているか　【問12】

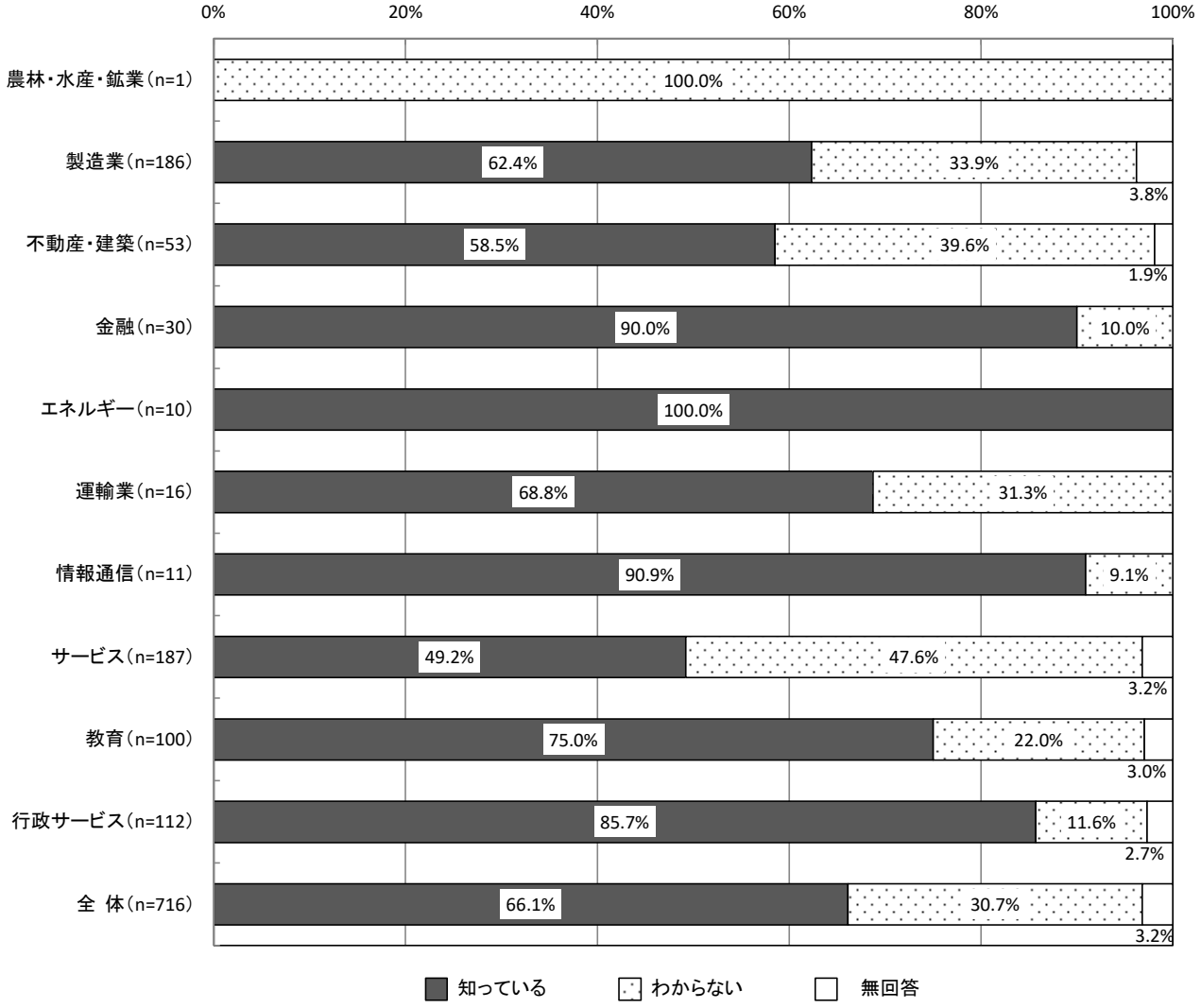
届出先機関を知っているかについては、「知っている」が66.1%、「わからない」が30.7%となっている。

【全体】届出先機関を知っているか（SA,n=716）



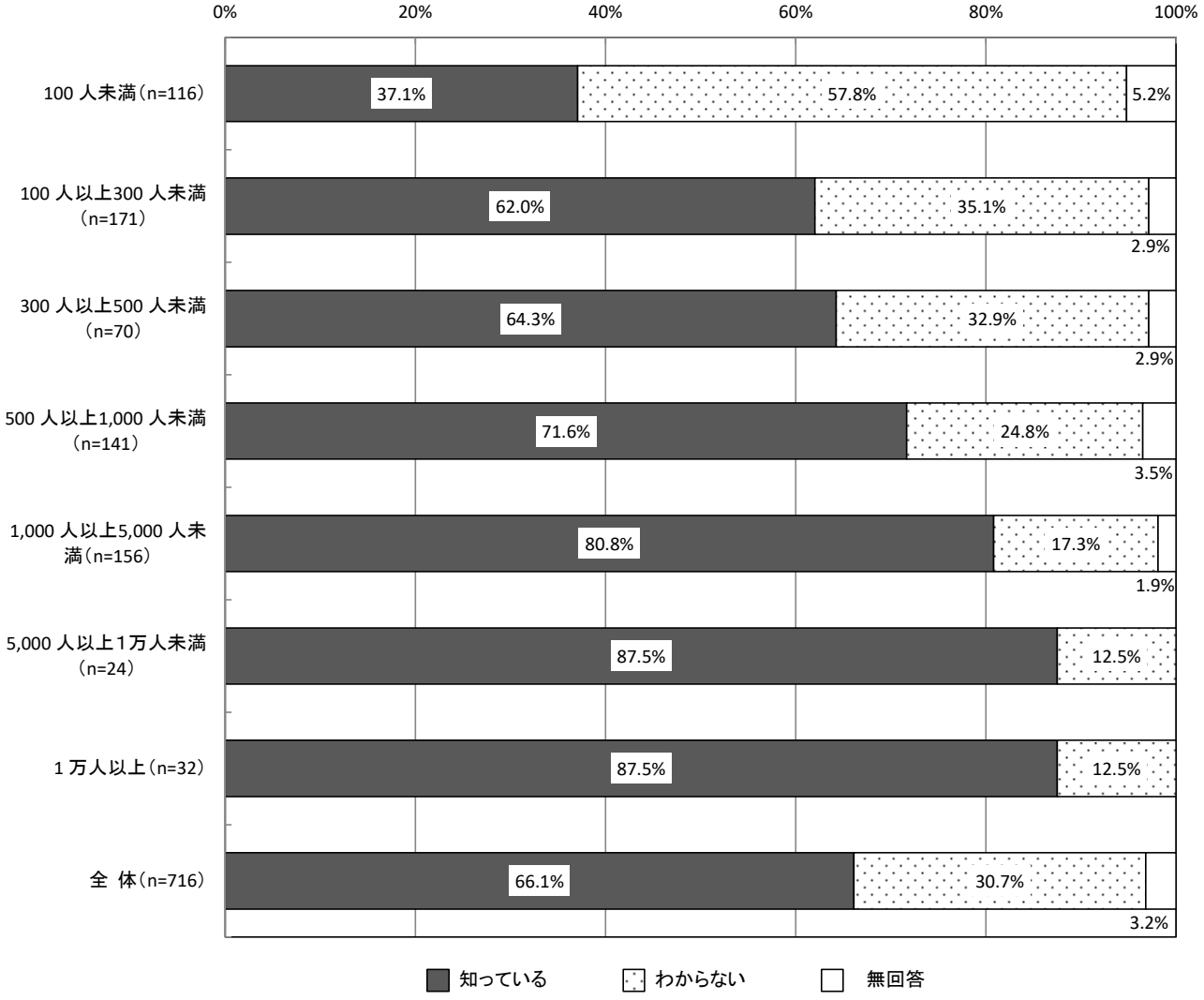
【業種別分析】業種別にみると、届出先機関を「知っている」については、「エネルギー」が 100.0%で最も多く、次いで「情報通信」が 90.9%となっている。一方、「わからない」については、「サービス」が 47.6%となっている。

【業種別分析】届出先機関を知っているか



【従業員規模別分析】従業員規模別にみると、従業員数が多くなるほど「知っている」の割合が高くなる傾向であり、「100人未満」では57.8%が「わからない」となっている。

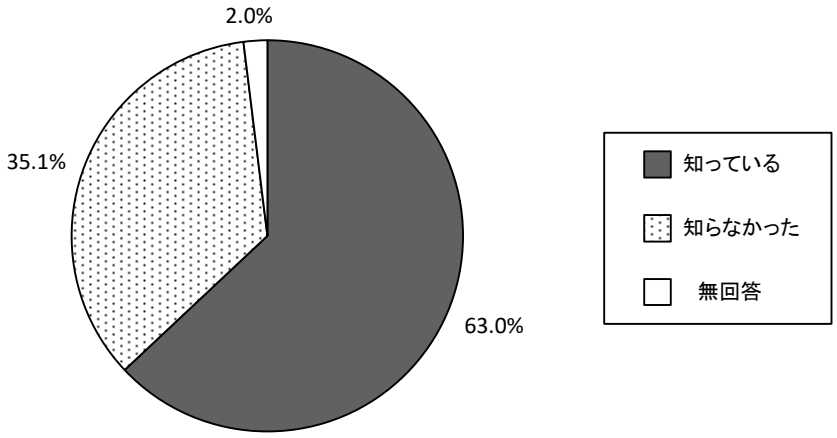
【従業員規模別分析】届出先機関を知っているか



3.1.19　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13】

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63.0%、「知らなかった」は35.1%となっている。

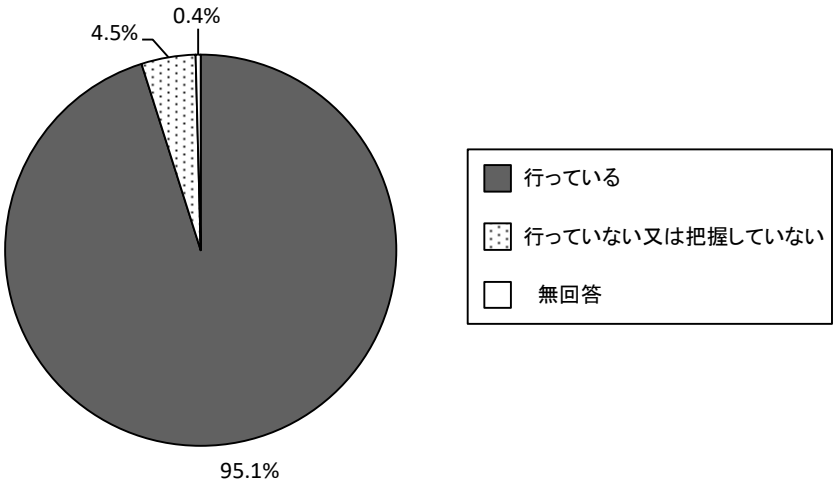
【全体】不正アクセス禁止法でアクセス管理者による防御措置についての努力義務（SA,n=716）



3.1.20　情報セキュリティ対策の実施状況　【問14】

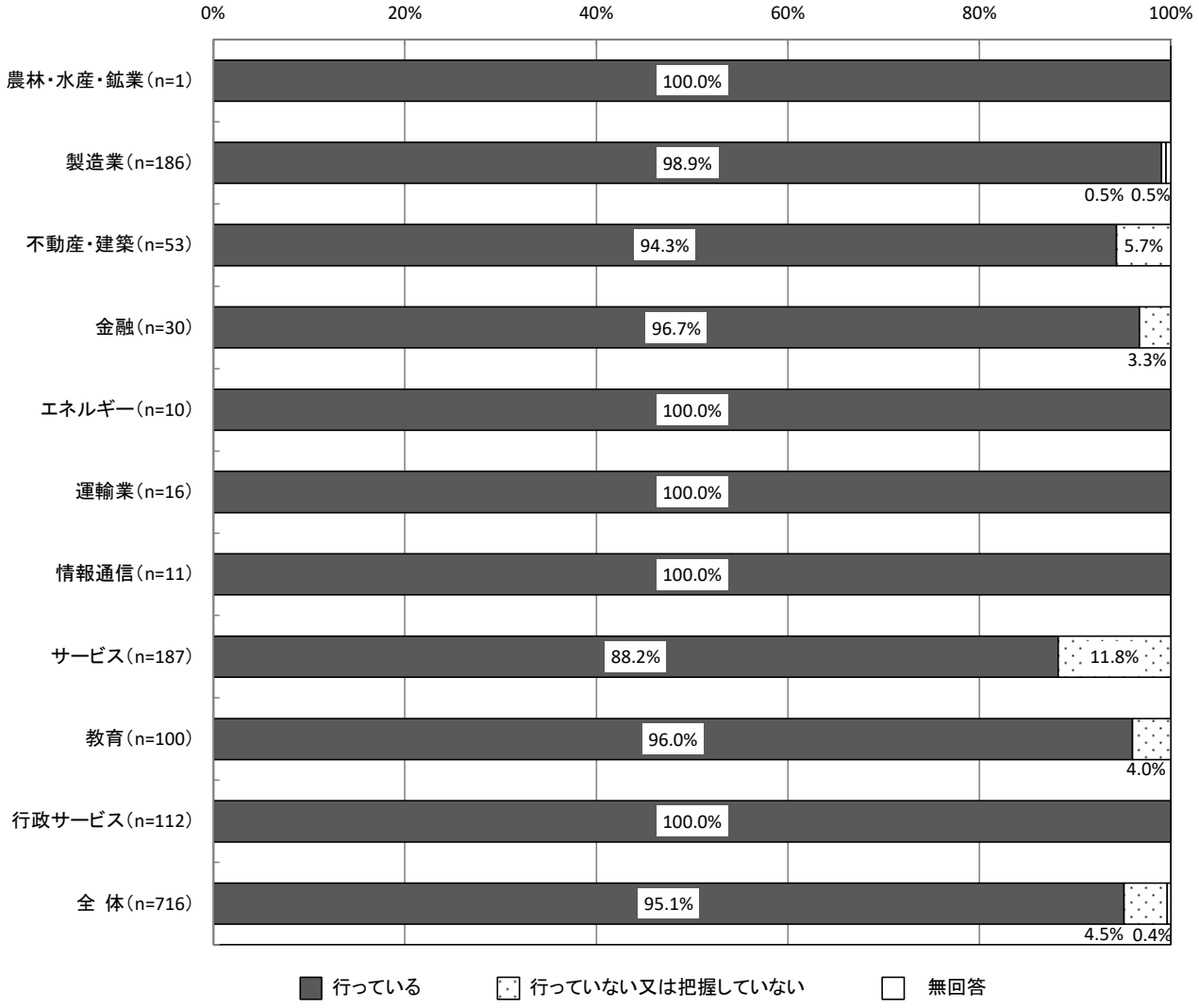
情報セキュリティ対策の実施状況については、「行っている」が95.1%、「行っていない又は把握していない」が4.5%となっている。

【全体】情報セキュリティ対策の実施状況（SA,n=716）



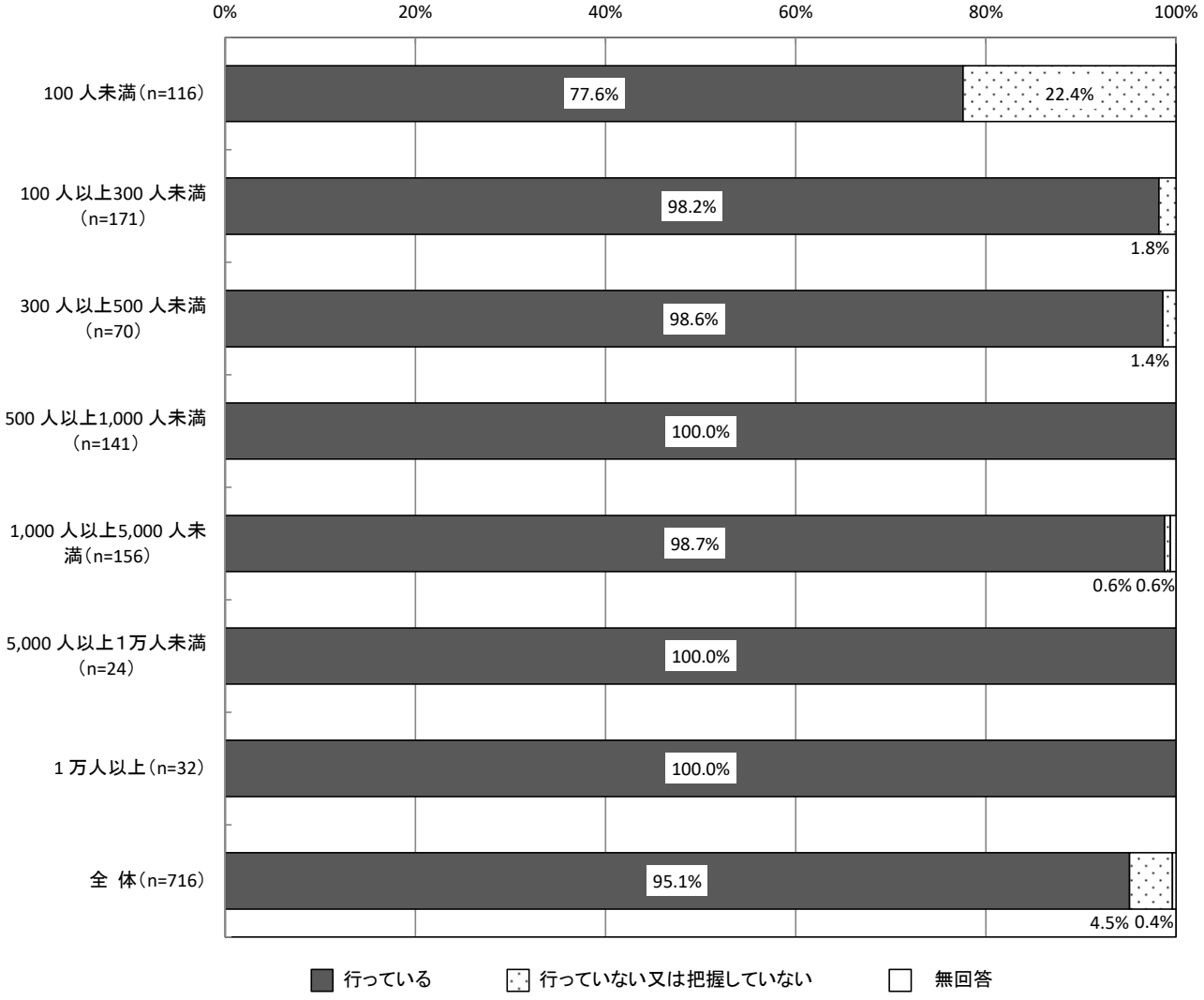
【業種別分析】業種別にみると、情報セキュリティ対策を「行っている」については、「エネルギー」「運輸業」「情報通信」「行政サービス」が 100.0%で最も多く、次いで「製造業」が 98.9%となっている。一方、情報セキュリティ対策を「行っていない又は把握していない」については、「サービス」が 11.8%となっている。

【業種別分析】情報セキュリティ対策の実施状況



【従業員規模別分析】従業員規模別にみると、従業員数100人以上は「行っている」が98%以上であるのに対して、「100人未満」では「行っていない又は把握していない」が22.4%となっている。

【従業員規模別分析】情報セキュリティ対策の実施状況

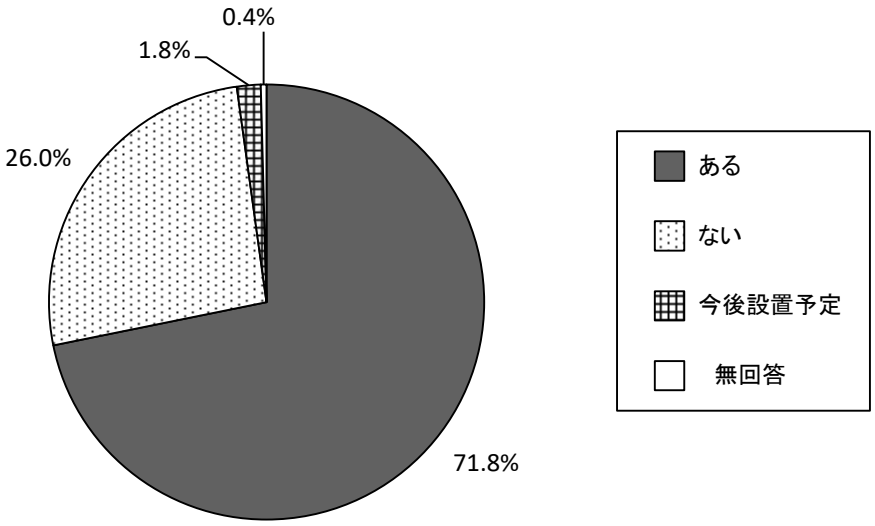


3.1.21　情報セキュリティ運用・管理専門部署の有無　【問14-1】

情報セキュリティ運用・管理専門部署の有無については、「ある」が71.8%、「ない」が26.0%となっている。

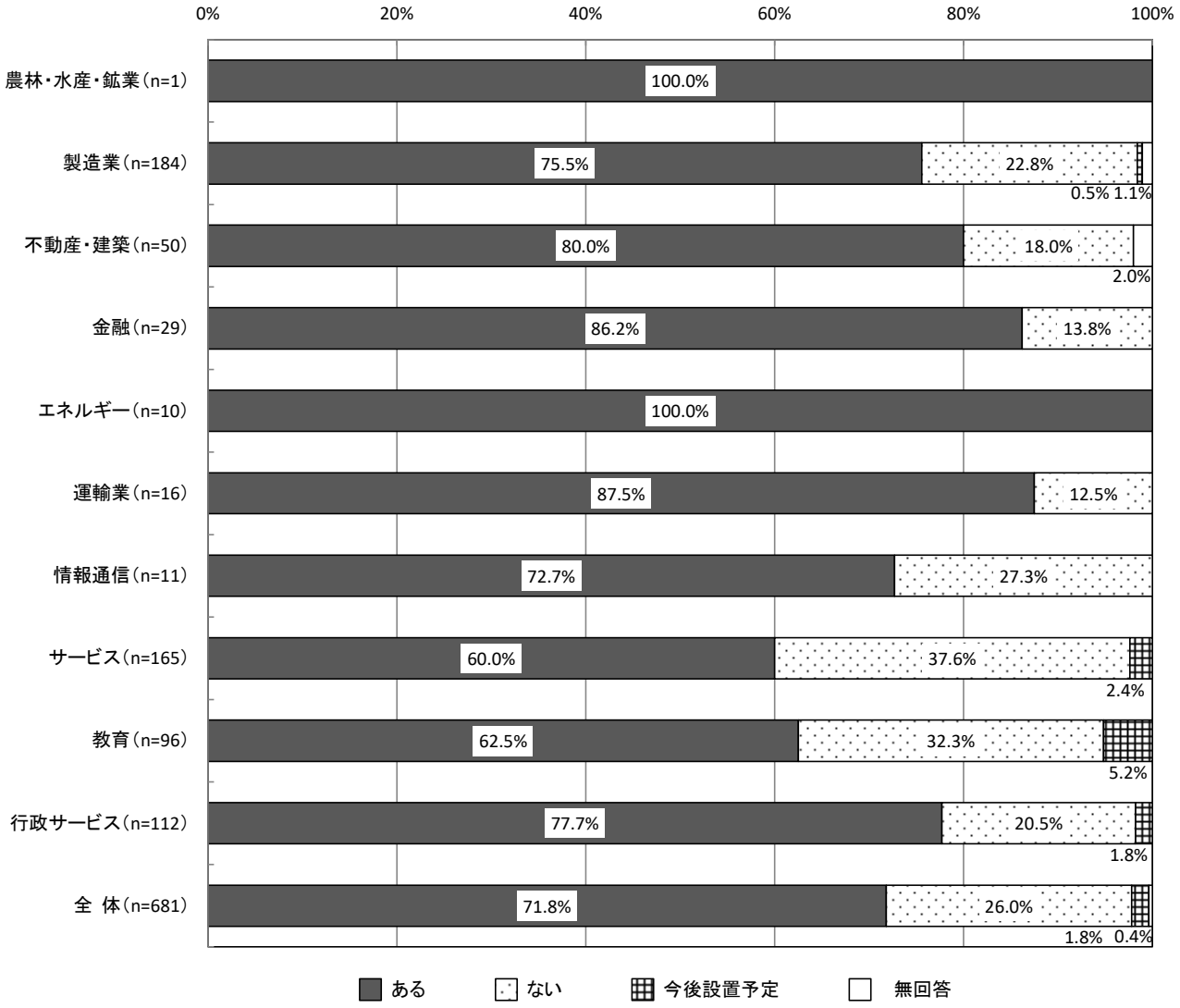
※本項目は、情報セキュリティ対策を行っている社・団体等を対象としている。

【全体】情報セキュリティ運用・管理専門部署の有無（SA,n=681）



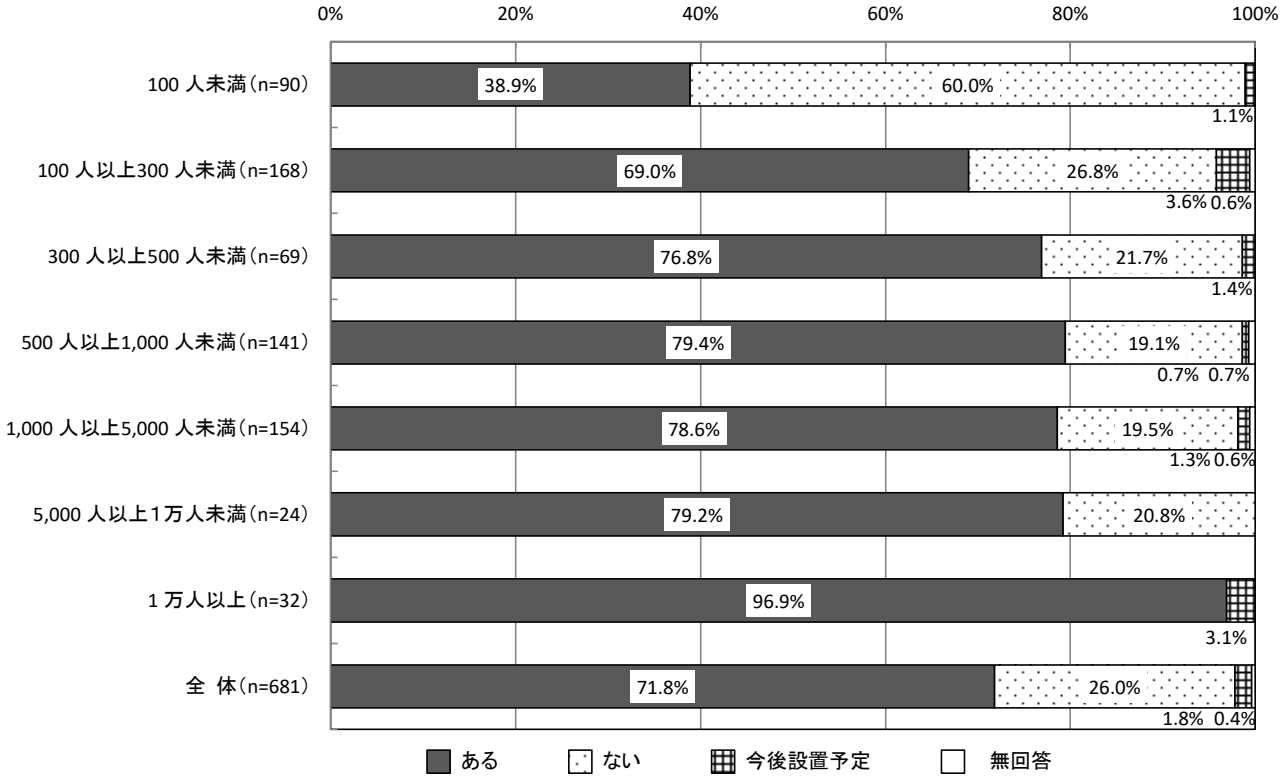
【業種別分析】業種別にみると、情報セキュリティ運用・管理専門部署が「ある」については、「エネルギー」が 100.0%で最も多く、次いで「運輸業」が 87.5%となっている。一方、情報セキュリティ運用・管理専門部署が「ない」については、「サービス」が 37.6%と最も多くなっている。

【業種別分析】情報セキュリティ運用・管理専門部署の有無



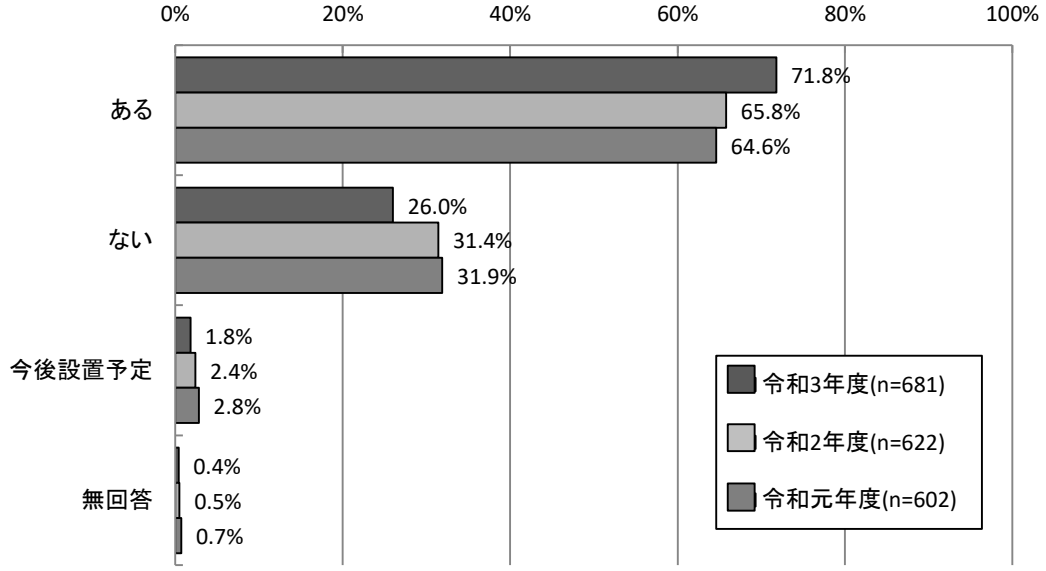
【従業員規模別分析】従業員規模別にみると、「ある」は「１万人以上」で96.9％と最も多くなっている。一方、「ない」は「100人未満」で60.0％と最も多くなっている。

【従業員規模別分析】情報セキュリティ運用・管理専門部署の有無



【経年変化】昨年度と比較すると、「ある」が6.0ポイント増加し、「ない」が5.4ポイント減少している。

【経年変化】情報セキュリティ運用・管理専門部署の有無

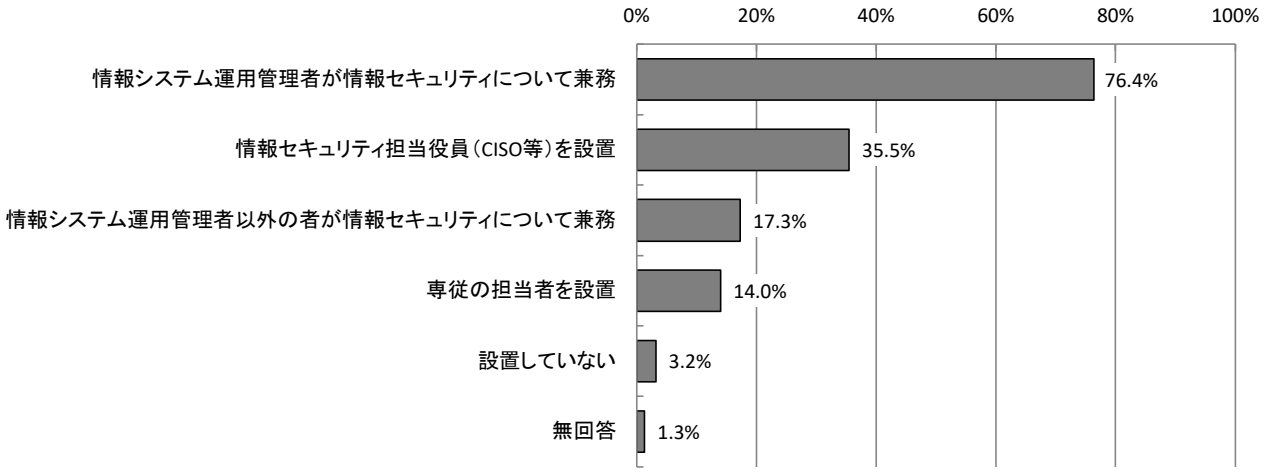


3.1.22　情報セキュリティ管理体制　【問14-2】

情報セキュリティ管理体制については、「情報システム運用管理者が情報セキュリティについて兼務」が76.4%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35.5%、「情報システム運用管理者以外の者が情報セキュリティについて兼務」が17.3%となっている。

※本項目は、情報セキュリティ対策を行っている社・団体等を対象としている。

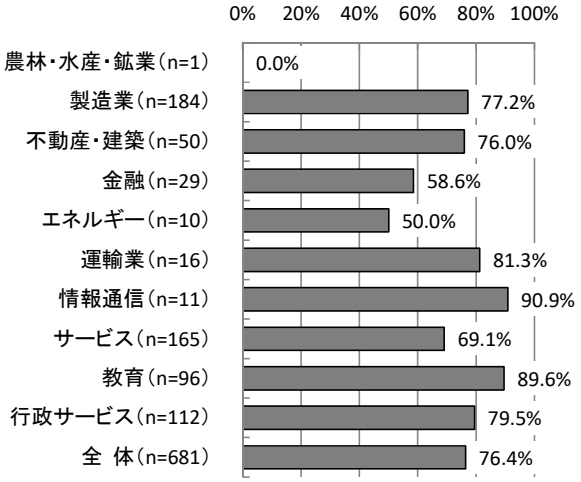
【全体】情報セキュリティ管理体制（MA, n=681）



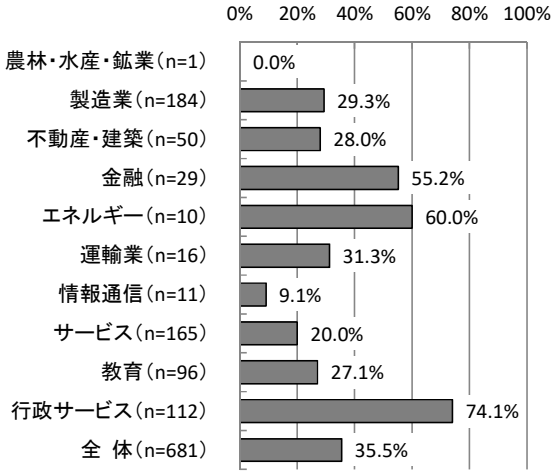
【業種別分析】業種別にみると、「情報システム運用管理者が情報セキュリティについて兼務」については、「情報通信」が90.9％で最も多く、次いで「教育」が89.6％となっている。「情報セキュリティ担当役員（ＣＩＳＯ等）を設置」については、「行政サービス」が74.1％で最も多く、次いで「エネルギー」が60.0％となっている。「情報システム運用管理者以外の者が情報セキュリティについて兼務」では、「金融」が34.5％で最も多い。

【業種別分析】情報セキュリティ管理体制

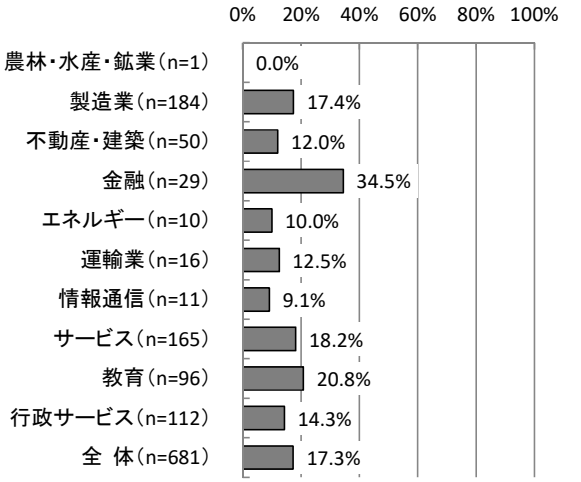
情報システム運用管理者が
情報セキュリティについて兼務



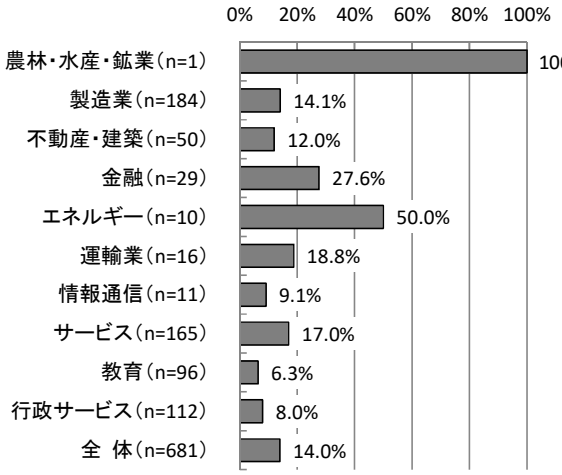
情報セキュリティ担当役員（ＣＩＳＯ等）を設置



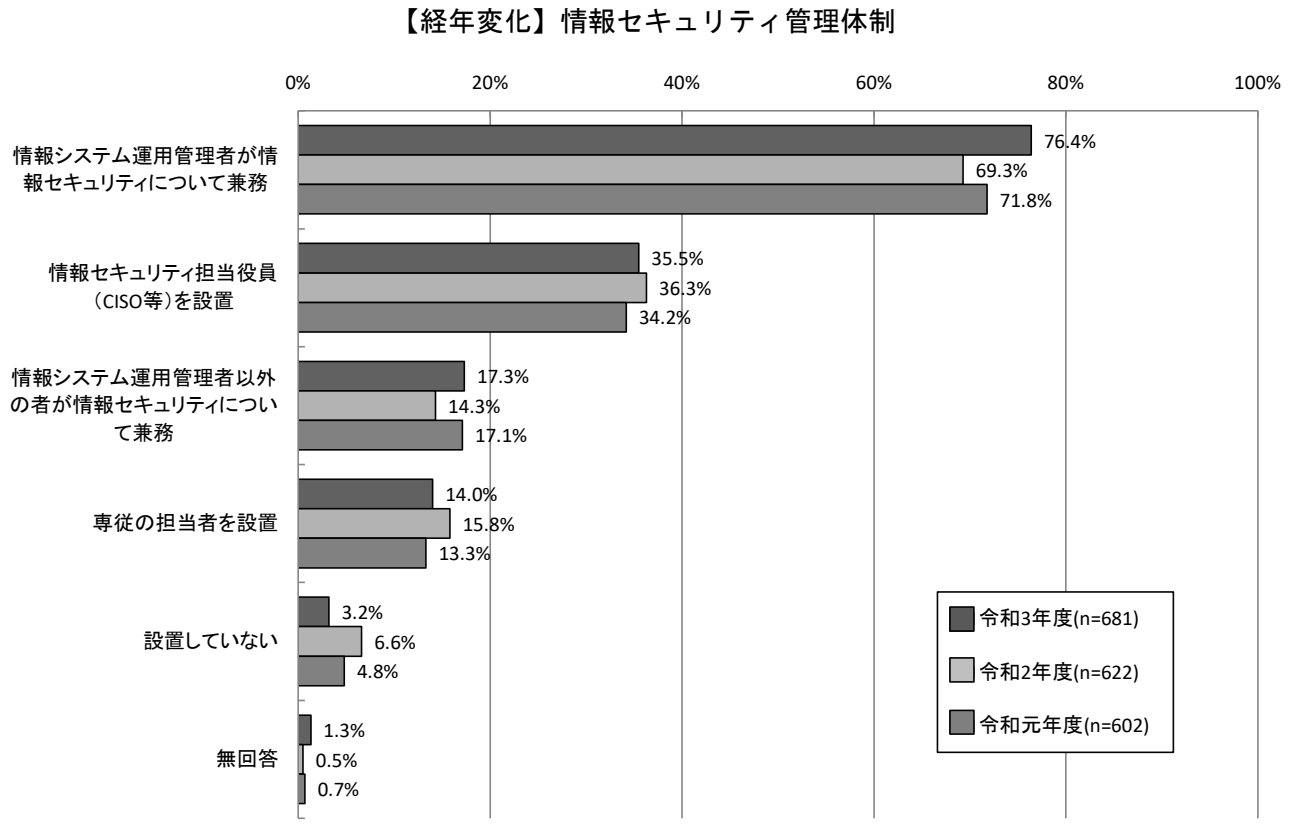
情報システム運用管理者以外の者が
情報セキュリティについて兼務



専従の担当者を設置



【経年変化】昨年度と比較すると、「情報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7.1ポイント増加している。

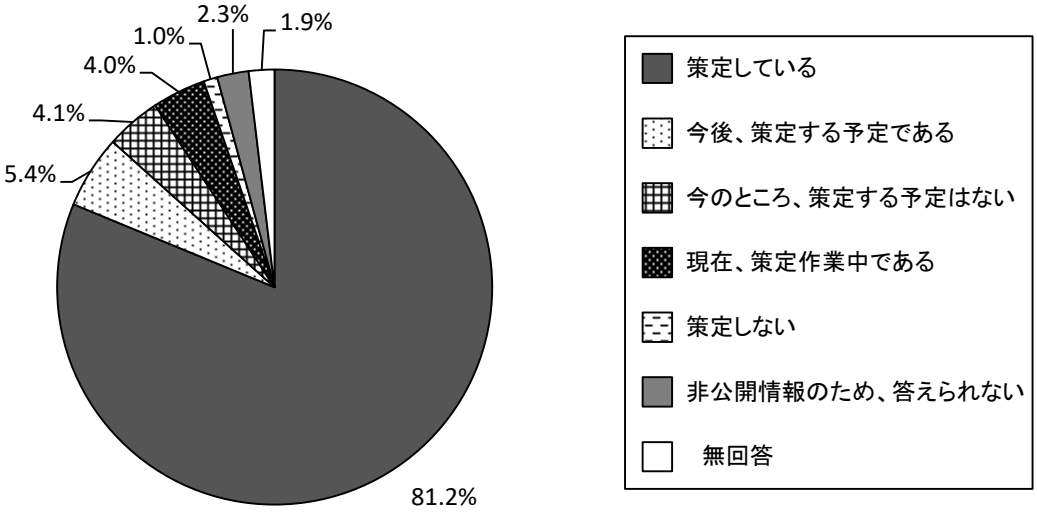


3.1.23　セキュリティポリシーの策定状況　【問14-3】

セキュリティポリシーの策定状況については、「策定している」が81.2%で最も多く、次いで「今後、策定する予定である」が5.4%、「今のところ、策定する予定はない」が4.1%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90.6%となっている。

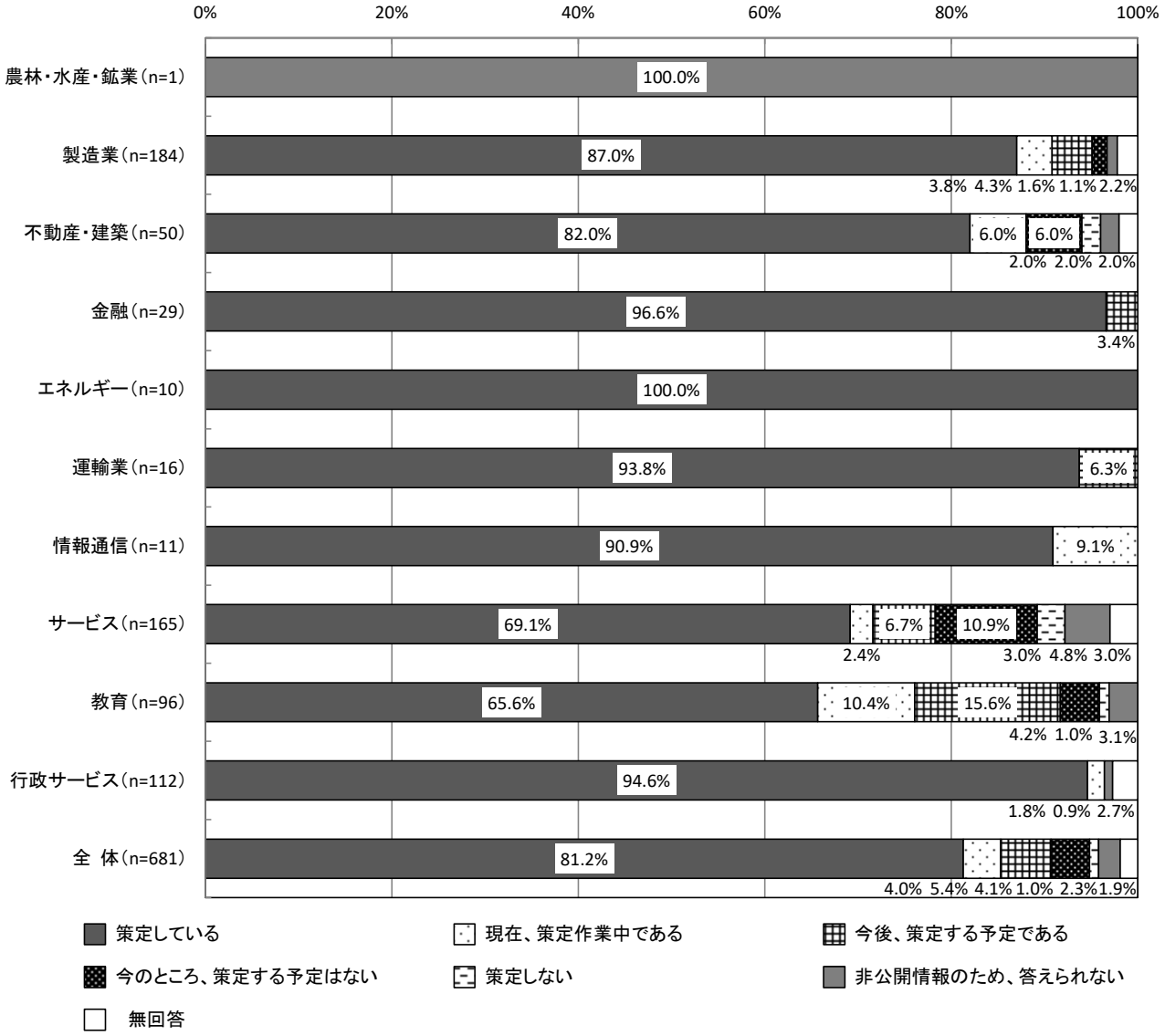
※本項目は、情報セキュリティ対策を行っている社・団体等を対象としている。

【全体】セキュリティポリシーの策定状況（SA,n=681）



【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「エネルギー」が100.0%、「金融」が96.6%、「行政サービス」が94.6%、「運輸業」が93.8%、「情報通信」が90.9%と9割を超えている。

【業種別分析】セキュリティポリシーの策定状況

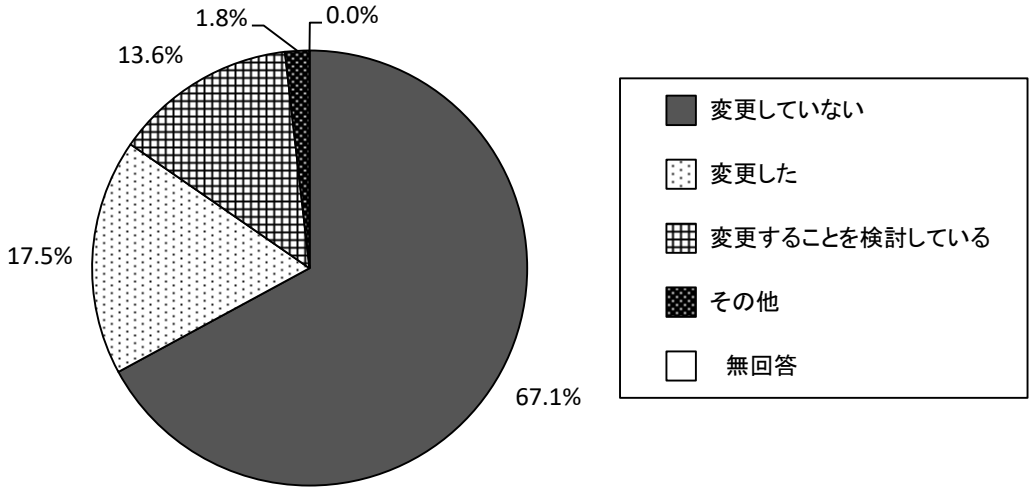


3.1.24　新型コロナウイルスの影響によるセキュリティポリシーの変更状況【問14-3-1】

新型コロナウイルスの影響によるセキュリティポリシーの変更状況については、「変更していない」が67.1%で最も多く、次いで「変更した」が17.5%、「変更することを検討している」が13.6%となっている。

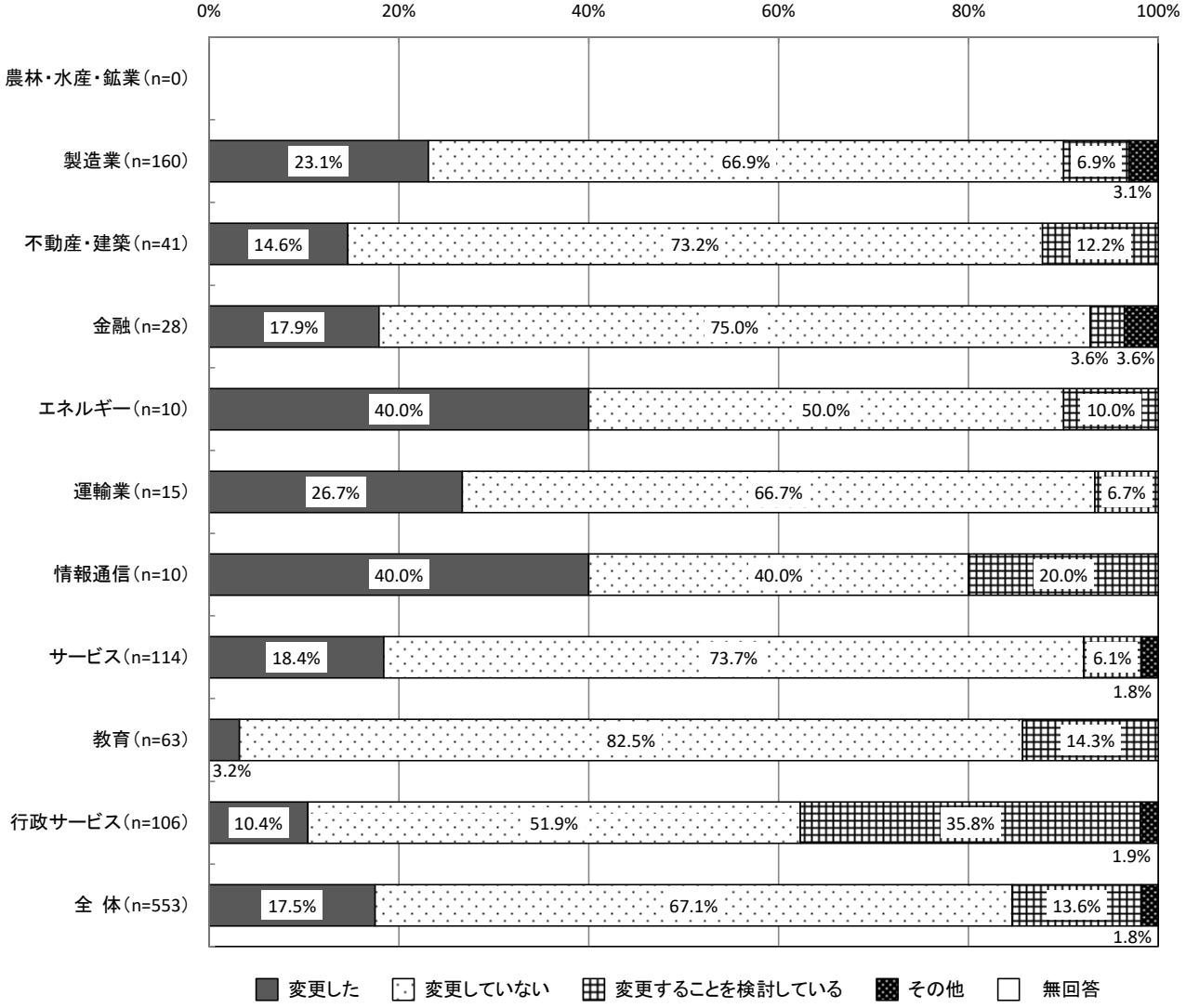
※本項目は、セキュリティポリシーを策定している社・団体等を対象としている。

【全体】新型コロナウイルスの影響によるセキュリティポリシーの変更状況（SA,n=553）



【業種別分析】業種別にみると、新型コロナウイルスの影響によるセキュリティポリシーの変更状況については、「変更していない」については「教育」が82.5%で最も多く、次いで「金融」が75.0%となっている。

【業種別分析】新型コロナウイルスの影響によるセキュリティポリシーの変更状況

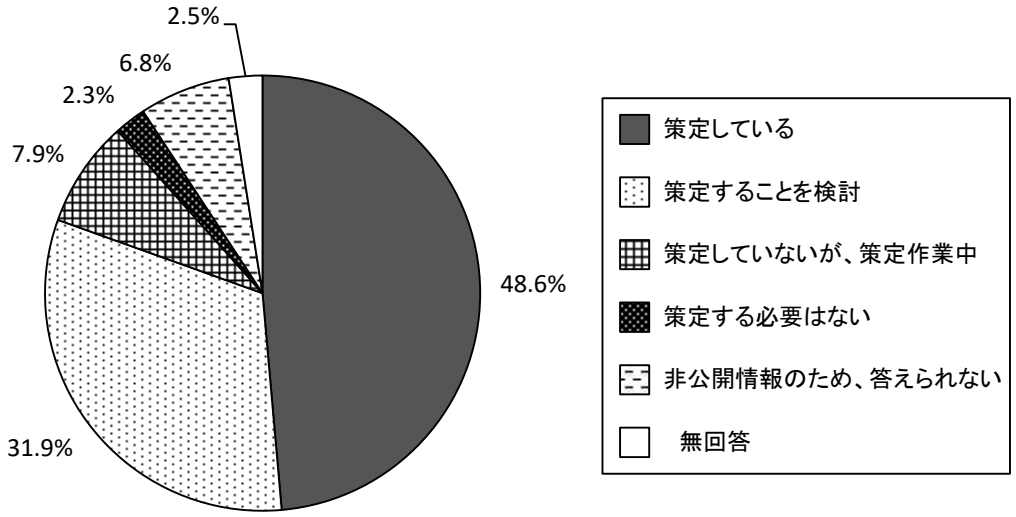


3.1.25　情報セキュリティ侵害事案発生時の対応マニュアル等の策定状況　【問14-4】

情報セキュリティ侵害事案発生時の対応マニュアル等の策定状況については、「策定している」が48.6%で最も多く、次いで「策定することを検討」が31.9%、「策定していないが、策定作業中」が7.9%となっている。

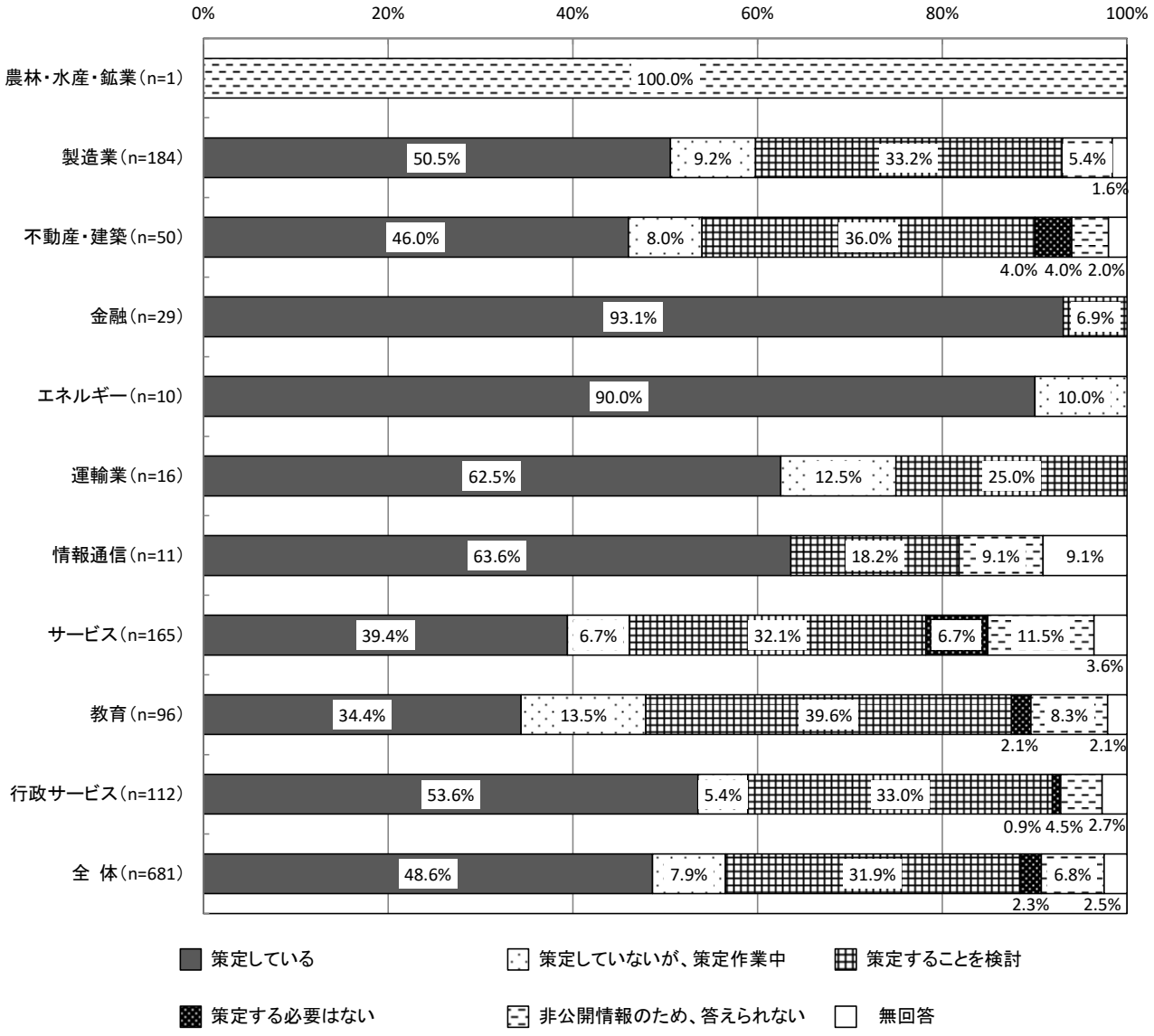
※本項目は、情報セキュリティ対策を行っている社・団体等を対象としている。

【全体】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=681）



【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93.1%で最も多く、次いで「エネルギー」が90.0%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

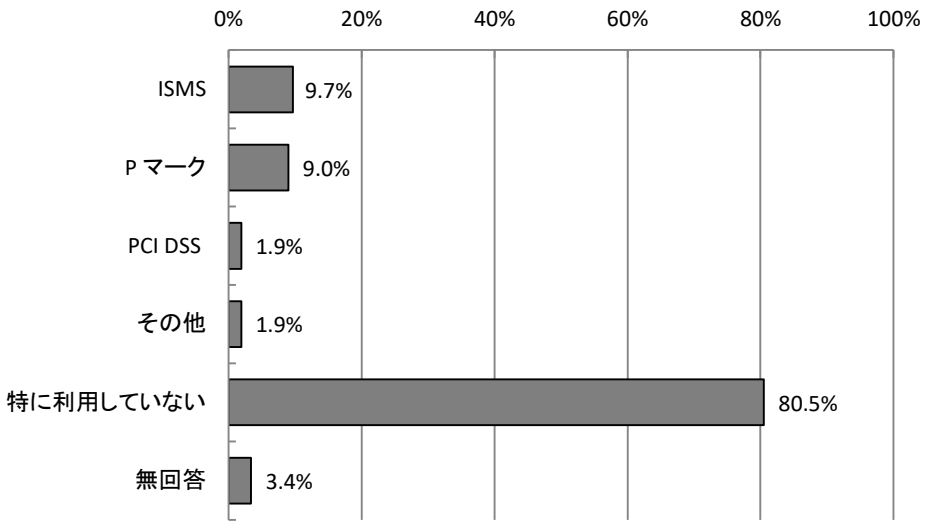


3.1.26　第三者機関の認証制度等の利用状況　【問14-5】

第三者機関の認証制度等の利用状況については、「特に利用していない」が80.5%で最も多く、次いで「ＩＳＭＳ」が9.7%、「Ｐマーク」が9.0%となっている。

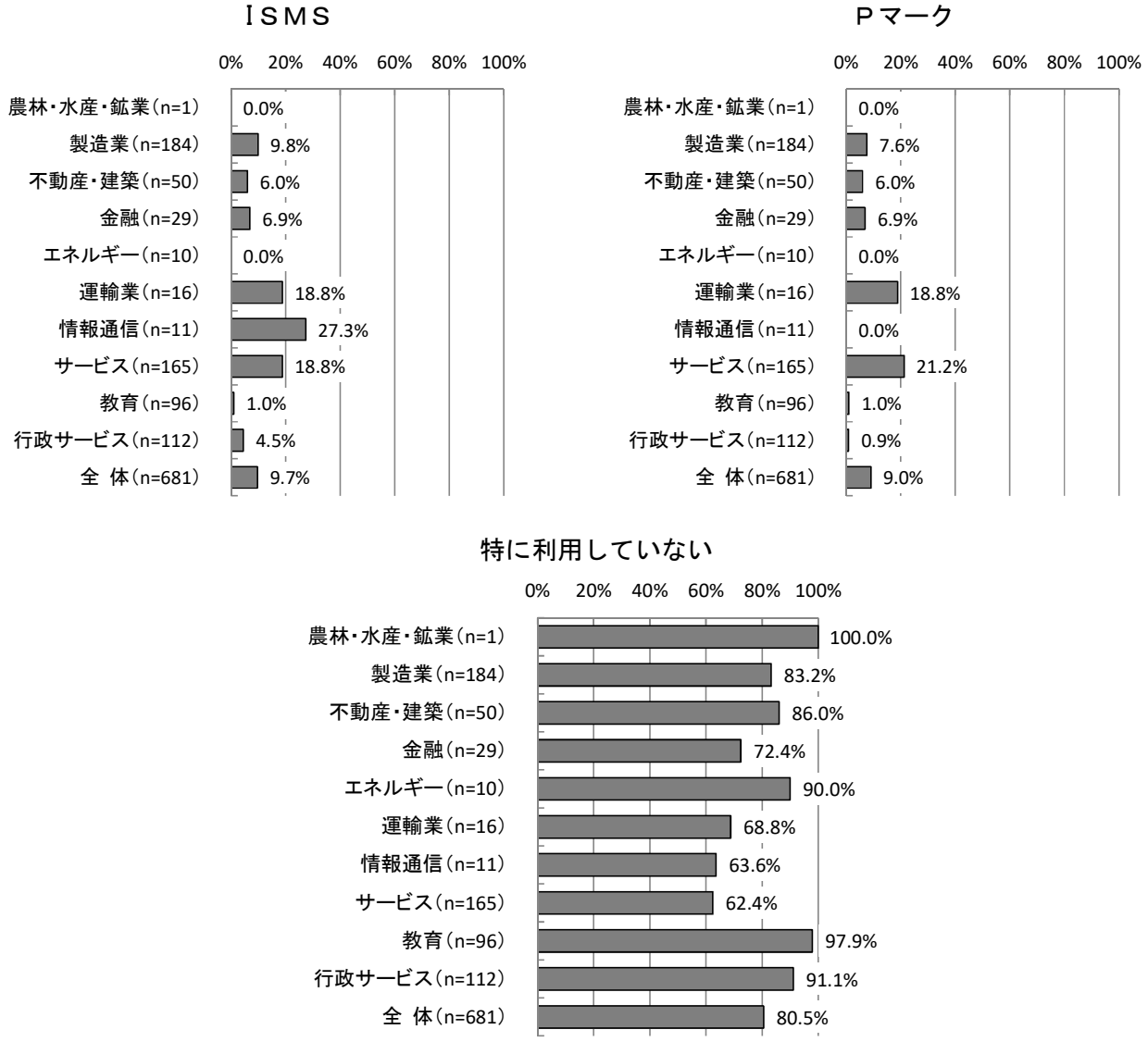
※本項目は、情報セキュリティ対策を行っている社・団体等を対象としている。

【全体】第三者機関の認証制度等の利用状況（MA, n=681）



【業種別分析】業種別にみると、「ＩＳＭＳ」については、「情報通信」が27.3％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97.9％で最も多く、次いで「行政サービス」が91.1％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

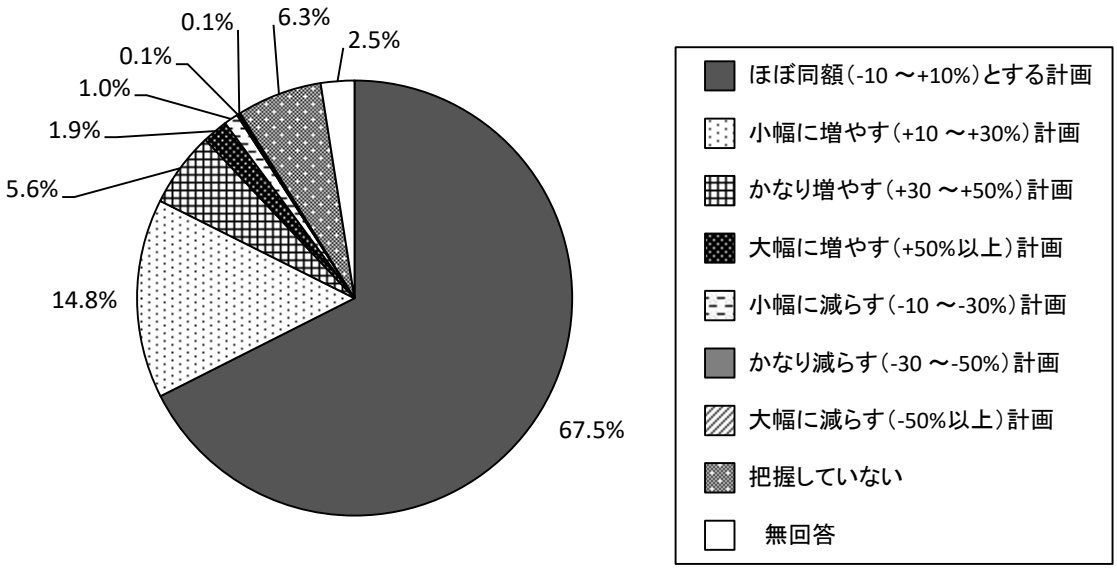


3.1.27　次年期の情報セキュリティ対策の投資計画　【問14-6】

次年期（年単位）の情報セキュリティ対策の投資計画については、「ほぼ同額（-10～+10%）とする計画」が67.5%で最も多く、次いで「小幅に増やす（+10～+30%）計画」が14.8%、「かなり増やす（+30～+50%）計画」が5.6%となっている。

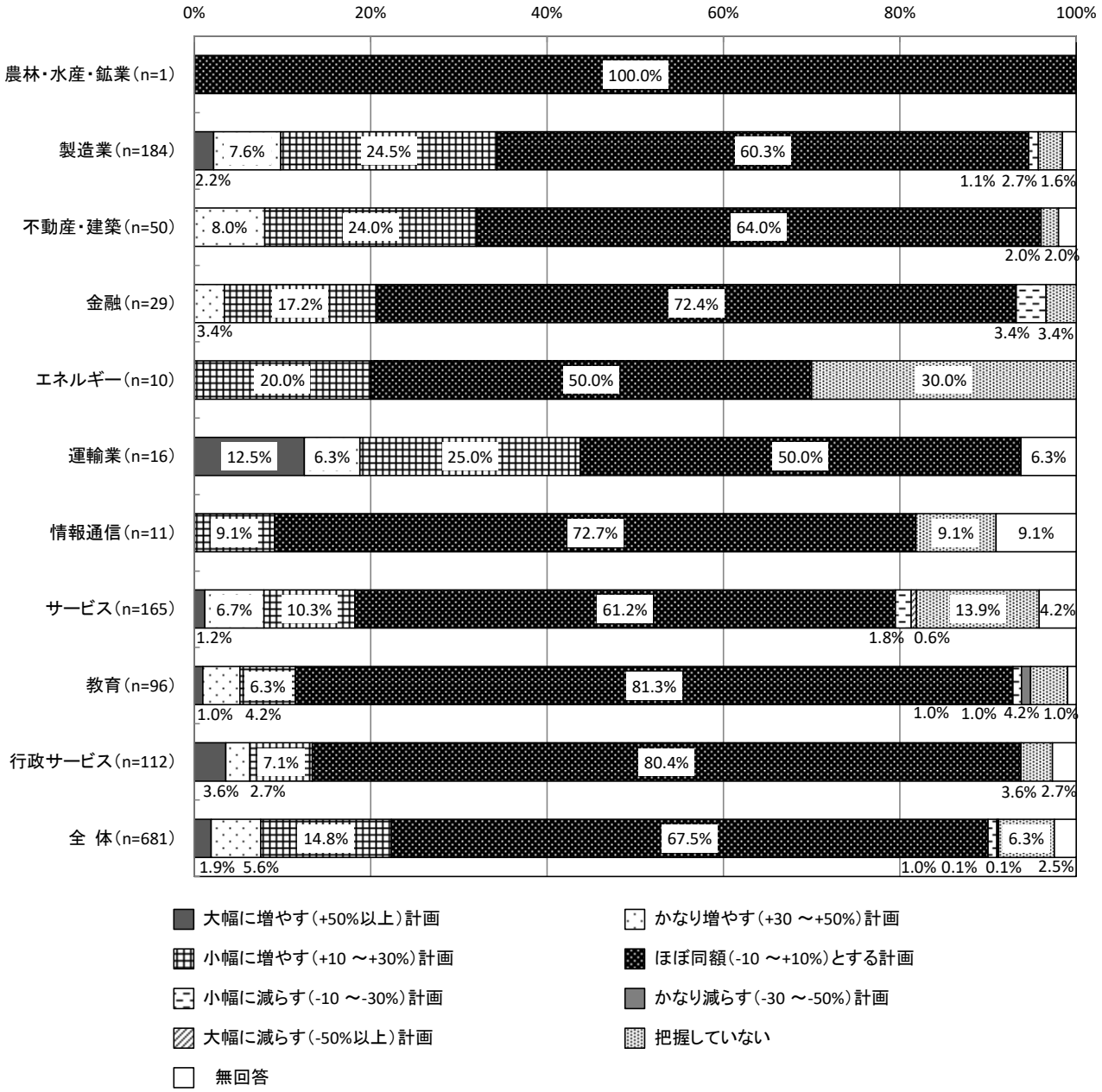
※本項目は、情報セキュリティ対策を行っている社・団体等を対象としている。

【全体】次年期の情報セキュリティ対策の投資計画（SA,n=681）



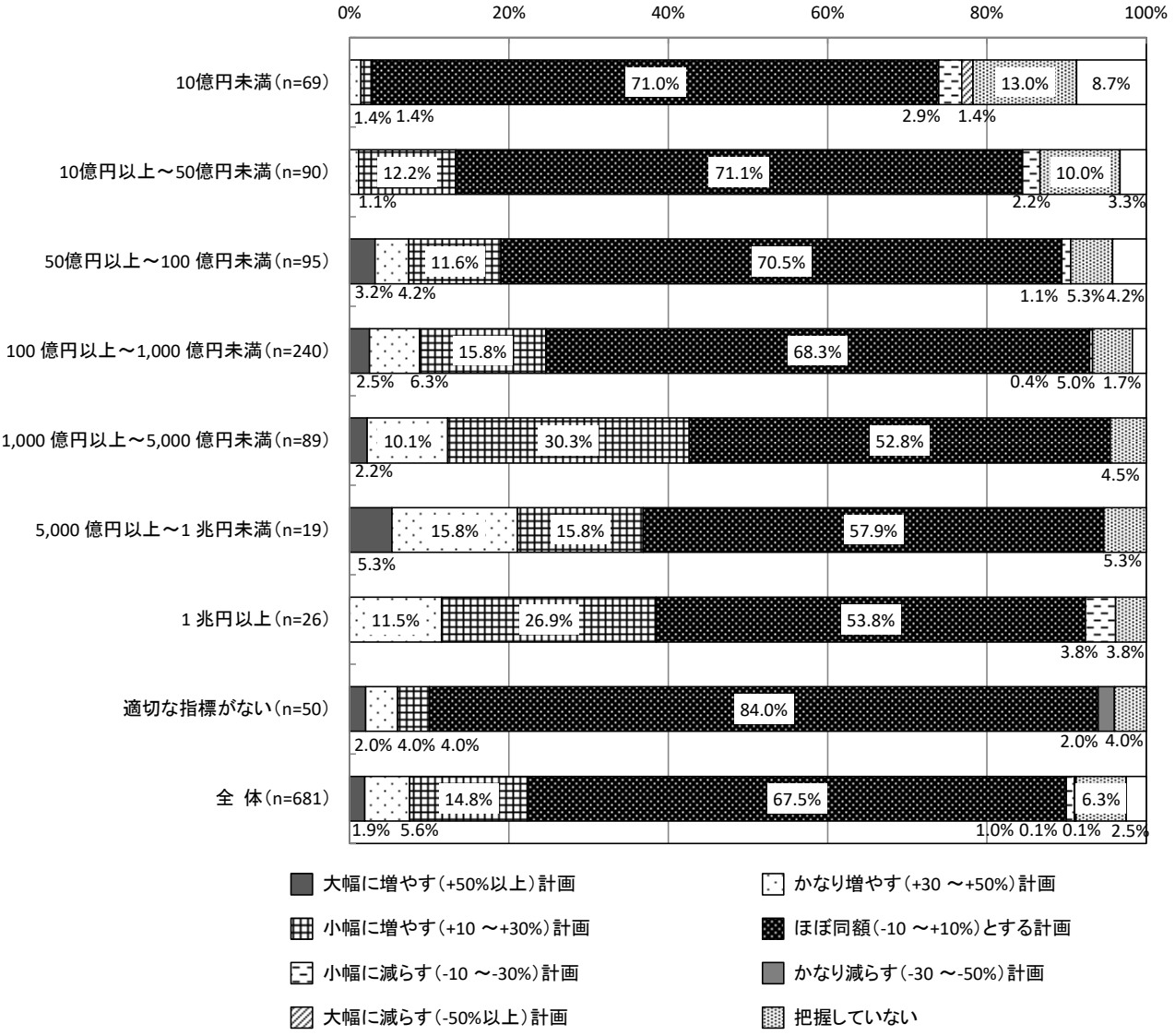
【業種別分析】業種別にみると、今期と比較して投資額を「増やす計画」については、「運輸業」が合計43.8%で最も多く、次いで「製造業」が34.3%、「不動産・建築」が32.0%となっている。今期と比較して、「ほぼ同額とする計画」については、「教育」が81.3%で最も多く、次いで「行政サービス」が80.4%、「情報通信」が72.7%で続いている。

【業種別分析】次年期の情報セキュリティ対策の投資計画



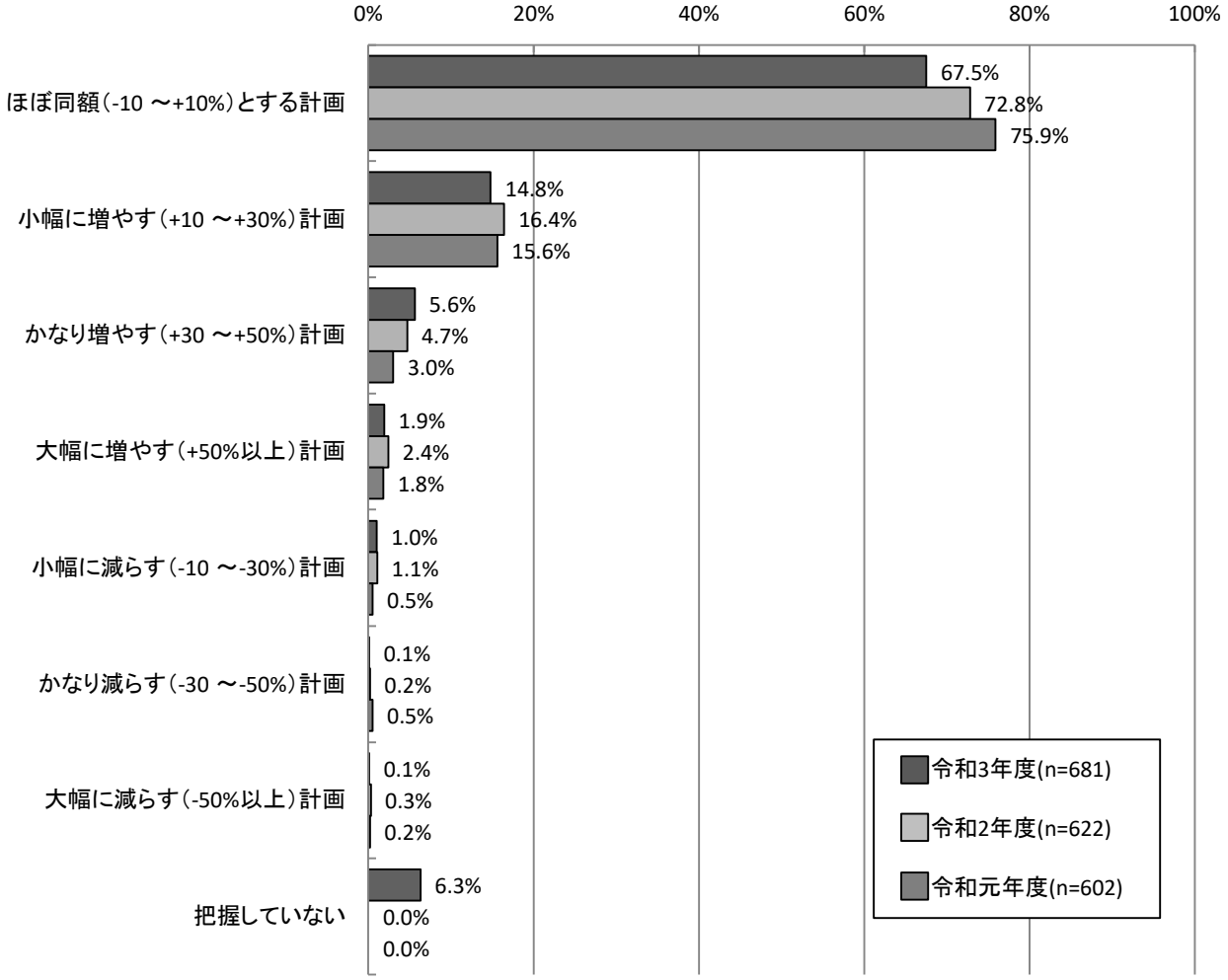
【売上・予算規模別分析】売上・予算規模別にみると、今期と比較して投資額を「増やす計画」については、「1,000億円以上～5,000億円未満」が計42.6%で最も多く、次いで「１兆円以上」が38.4%、「5,000億円以上～１兆円未満」が36.9%となっている。今期と比較して、「ほぼ同額とする計画」は、「適切な指標がない」が84.0%で最も多くなっている。

【売上・予算規模別分析】次年期の情報セキュリティ対策の投資計画



【経年変化】昨年度と比較すると、「ほぼ同額（−10～+10%）とする計画」が 5.3 ポイント減少している。

【経年変化】次年期の情報セキュリティ対策の投資計画

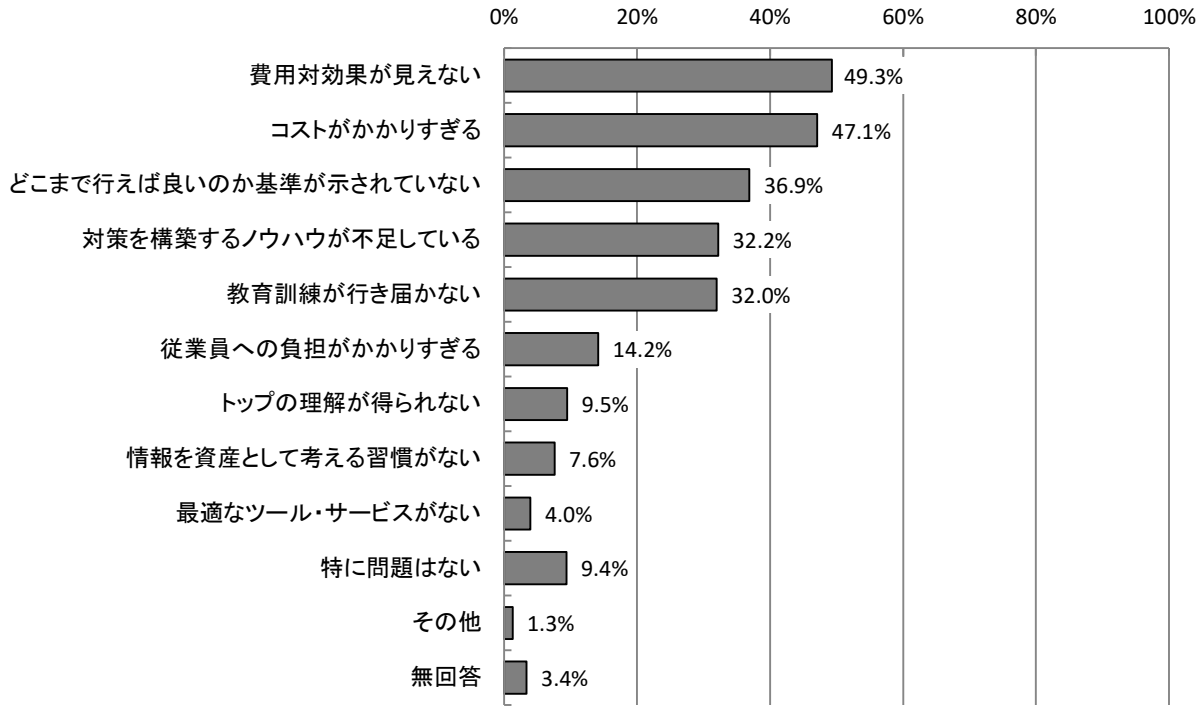


3.1.28　情報セキュリティ対策への投資に関する問題点　【問14-7】

情報セキュリティ対策への投資に関する問題点については、「費用対効果が見えない」が49.3%で最も多く、次いで「コストがかかりすぎる」が47.1%、「どこまで行えば良いのか基準が示されていない」が36.9%となっている。

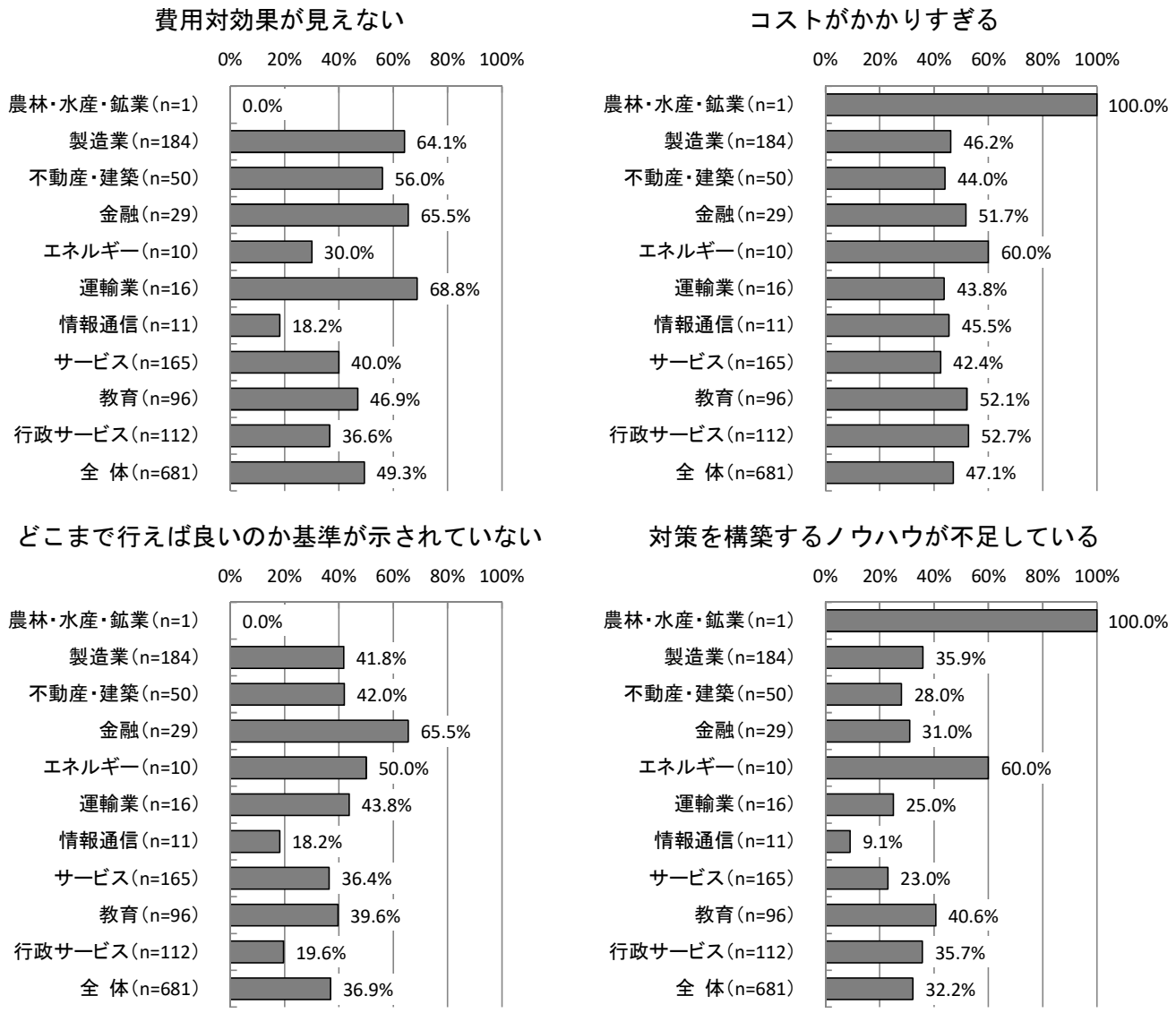
※本項目は、情報セキュリティ対策を行っている社・団体等を対象としている。

【全体】情報セキュリティ対策への投資に関する問題点（MA, n=681）



【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、「運輸業」が68.8%で最も多くなっている。「コストがかかりすぎる」については、「エネルギー」が60.0%、「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、「金融」が65.5%で最も多くなっている。

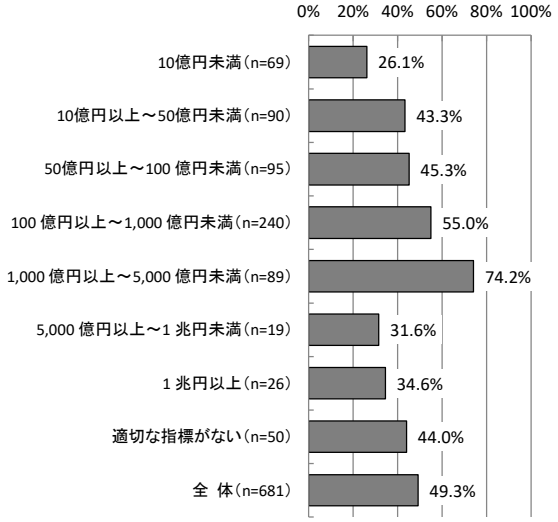
【業種別分析】情報セキュリティ対策への投資に関する問題点



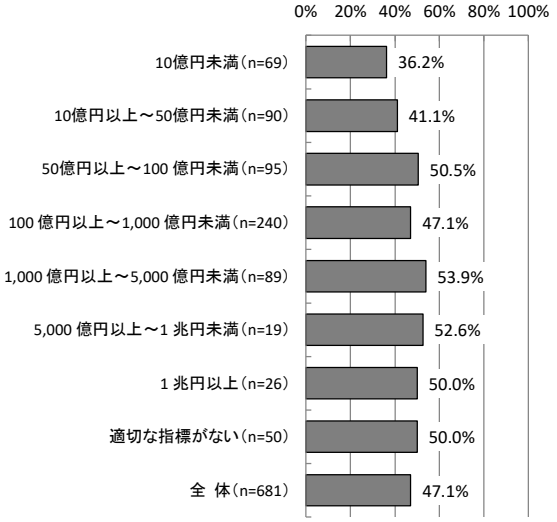
【売上・予算規模別分析】売上・予算規模別にみると、「費用対効果が見えない」については、「1,000億円以上～5,000億円未満」が74.2％で最も多く、次いで「100億円以上～1,000億円未満」が55.0％となっている。「コストがかかりすぎる」については、「1,000億円以上～5,000億円未満」が53.9％で最も多く、次いで「5,000億円以上～１兆円未満」が52.6％となっている。「どこまで行えば良いのか基準が示されていない」については、「5,000億円以上～１兆円未満」が47.4％で最も多く、次いで「1,000億円以上～5,000億円未満」46.1％となっている。

【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

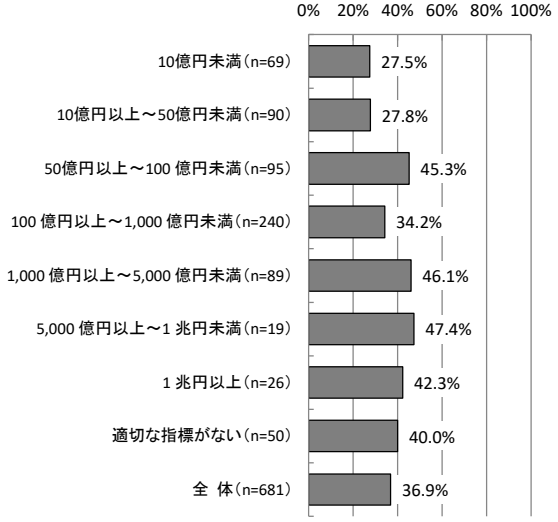
費用対効果が見えない



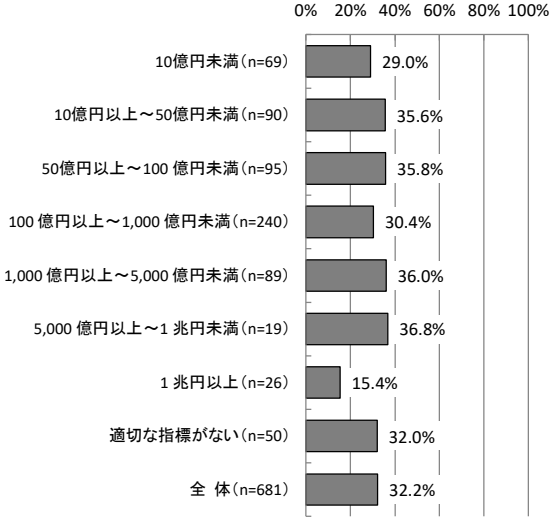
コストがかかりすぎる



どこまで行えば良いのか基準が示されていない

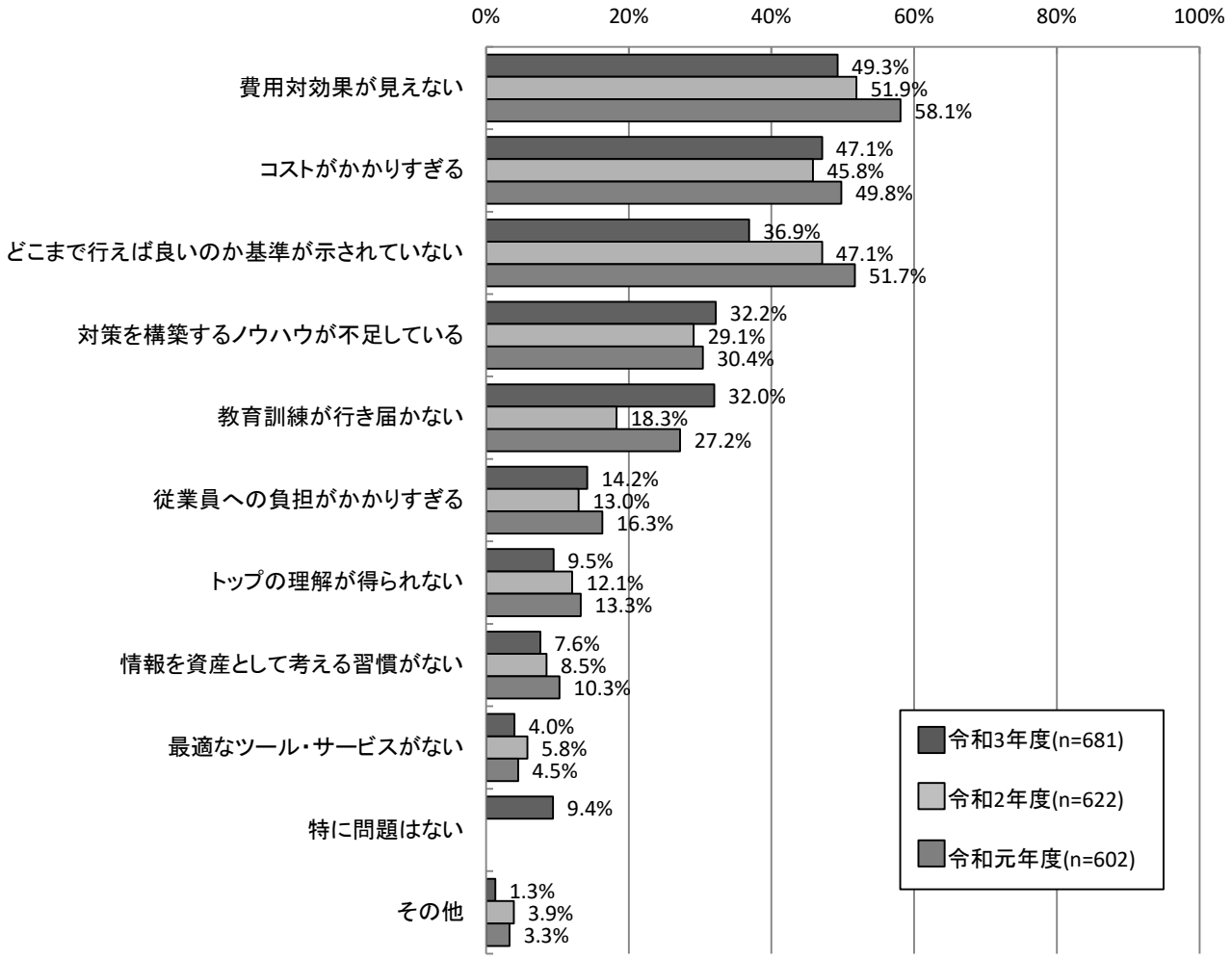


対策を構築するノウハウが不足している



【経年変化】昨年度と比較すると、「教育訓練が行き届かない」が13.7ポイント増加している。一方、「どこまで行えば良いのか基準が示されていない」が10.2ポイント減少している。

【経年変化】情報セキュリティ対策への投資に関する問題点



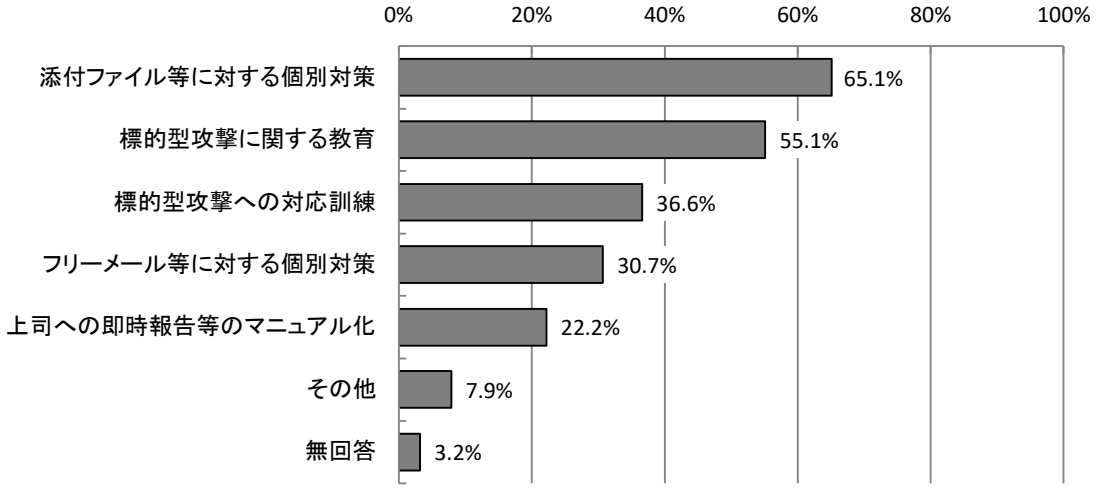
※令和３年度調査で、「特に問題はない」を新設。

3.1.29　標的型攻撃への対策状況　【問14-8】

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65.1%で最も多く、次いで「標的型攻撃に関する教育」が55.1%、「標的型攻撃への対応訓練」が36.6%となっている。

※本項目は、情報セキュリティ対策を行っている社・団体等を対象としている。

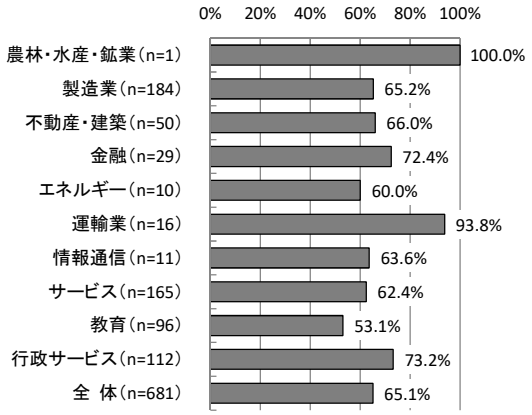
【全体】標的型攻撃への対策状況（MA, n=681）



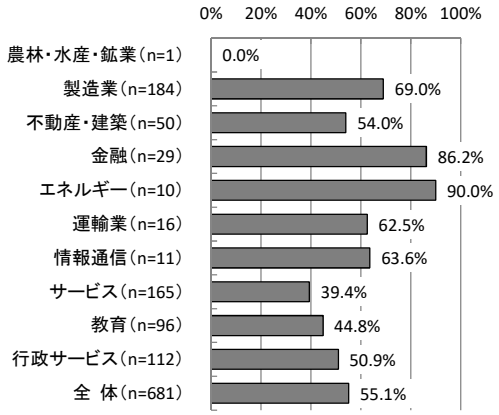
【業種別分析】業種別にみると、「添付ファイル等に対する個別対策」については、「運輸業」が93.8%で最も多く、次いで「行政サービス」が73.2%となっている。「標的型攻撃に関する教育」については、「エネルギー」が90.0%で最も多く、次いで「金融」が86.2%となっている。

【業種別分析】標的型攻撃への対策状況

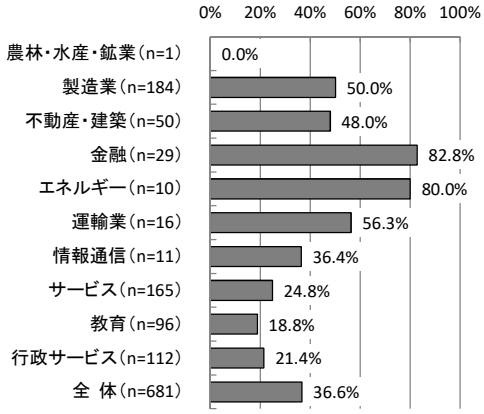
添付ファイル等に対する個別対策



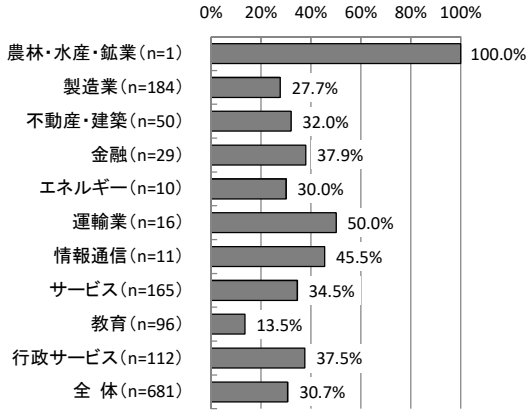
標的型攻撃に関する教育



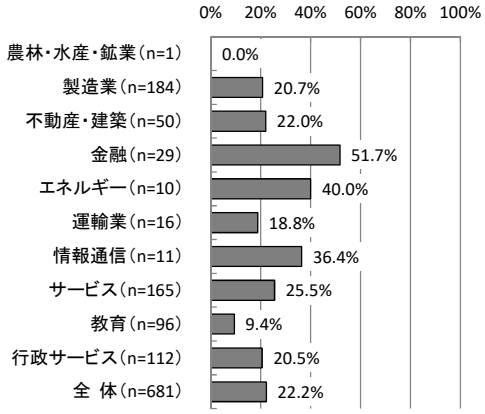
標的型攻撃への対応訓練



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

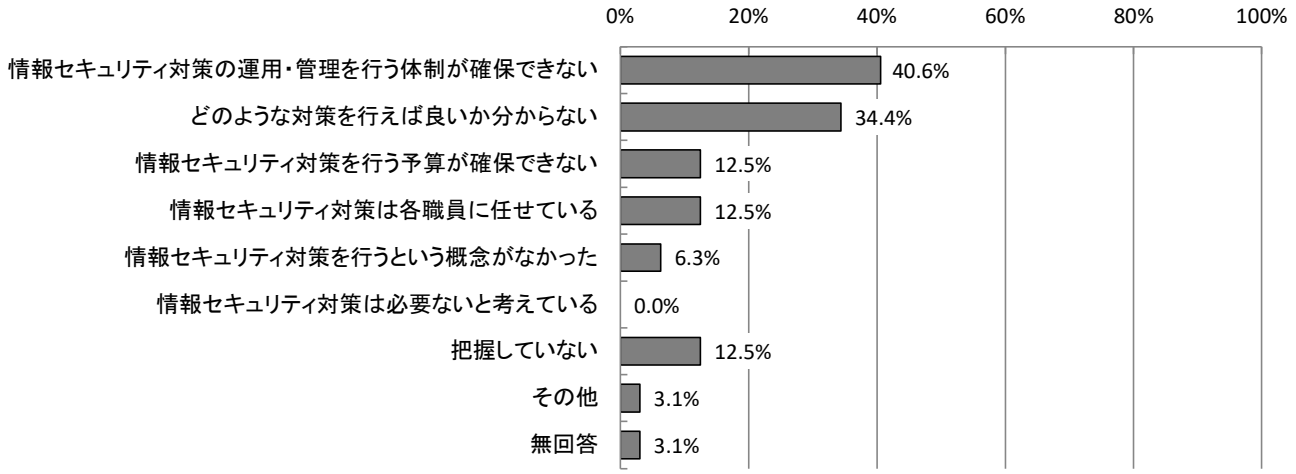


3.1.30　情報セキュリティ対策を行っていない理由　【問14-9】

情報セキュリティ対策を行っていない理由については、「情報セキュリティ対策の運用・管理を行う体制が確保できない」が40.6%で最も多く、次いで「どのような対策を行えば良いか分からない」が34.4%となっている。

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

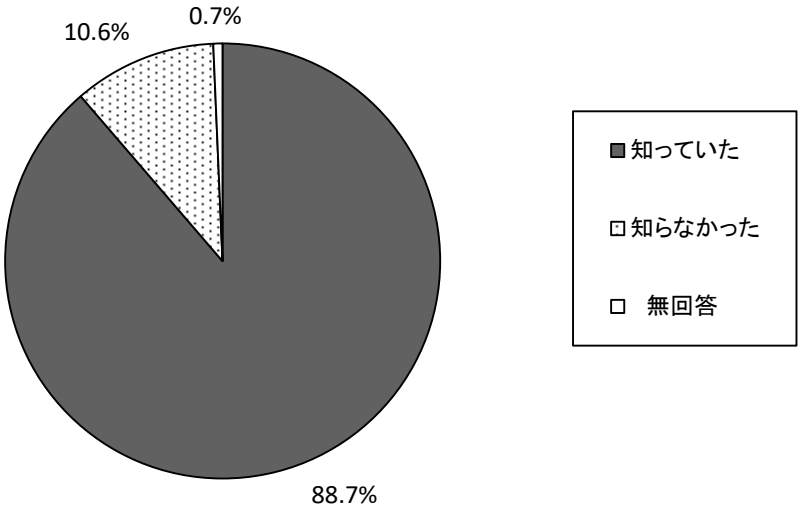
【全体】情報セキュリティ対策を行っていない理由（MA,n=32）



3.1.31　ビジネスメール詐欺の認知状況　【問15】

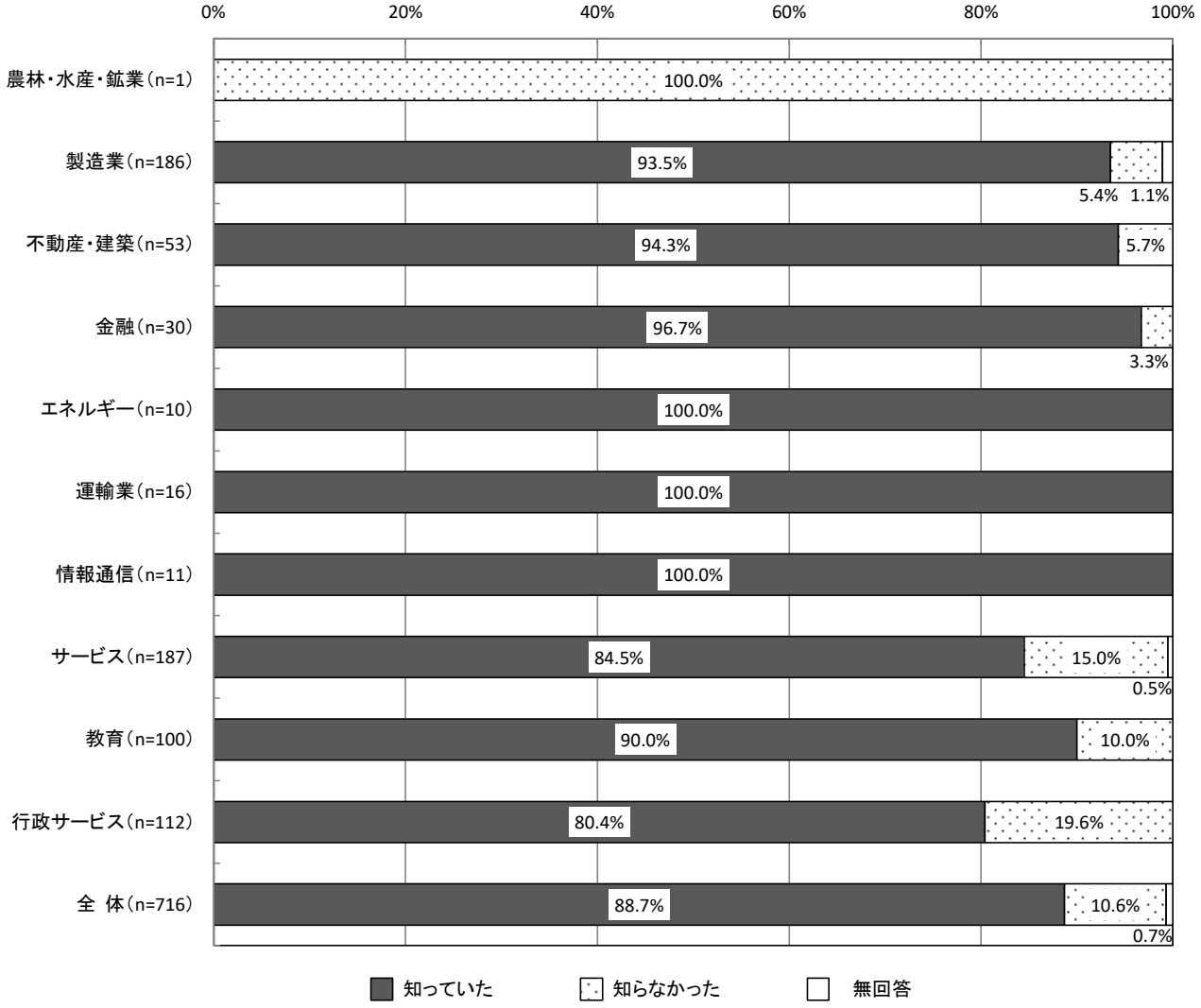
ビジネスメール詐欺の認知状況については、「知っていた」が88.7%、「知らなかった」が10.6%となっている。

【全体】ビジネスメール詐欺の認知状況（SA,n=716）



【業種別分析】業種別にみると、「知っていた」については、「エネルギー」「運輸業」「情報通信」が100.0%で最も多く、次いで「金融」が96.7%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19.6%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

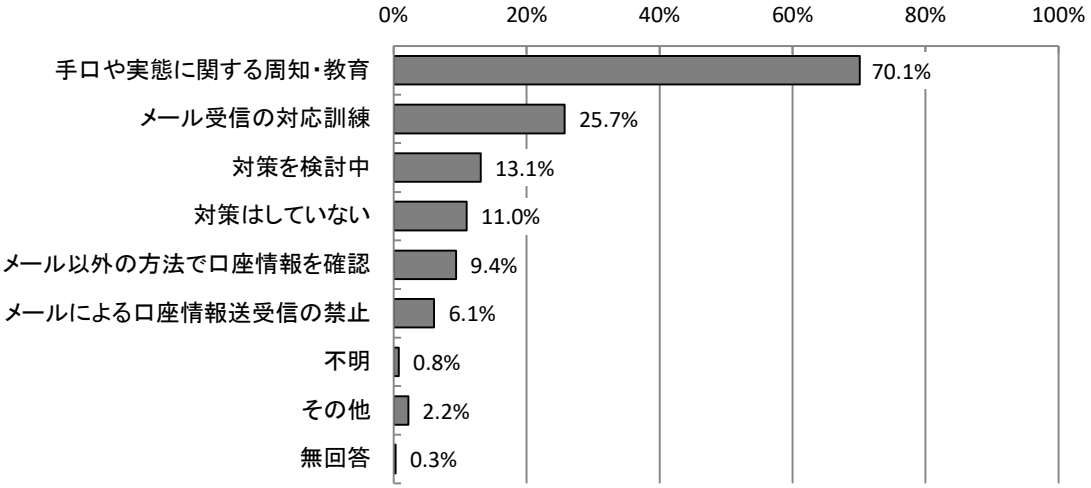


3.1.32　ビジネスメール詐欺への対策　【問15-1】

ビジネスメール詐欺への対策については、「手口や実態に関する周知・教育」が70.1%で最も多く、次いで「メール受信の対応訓練」が25.7%、「対策を検討中」が13.1%となっている。

※本項目は、ビジネスメール詐欺を知っている社・団体等を対象としている。

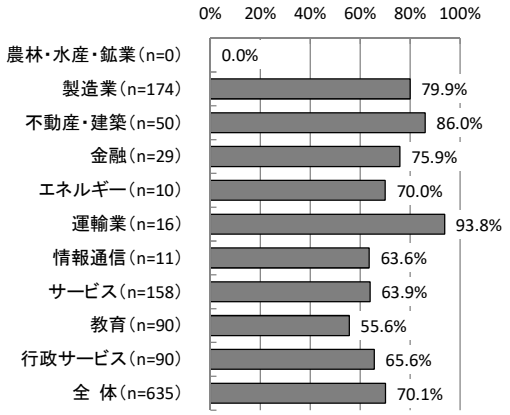
【全体】ビジネスメール詐欺への対策（MA, n=635）



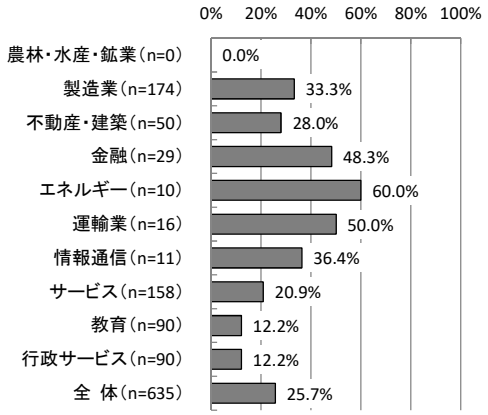
【業種別分析】業種別にみると、「手口や実態に関する周知・教育」については、「運輸業」が93.8%と最も多く、次いで「不動産・建築」が86.0%となっている。「メール受信の対応訓練」については、「エネルギー」が60.0%と最も多く、次いで「運輸業」が50.0%となっている。

【業種別分析】ビジネスメール詐欺への対策

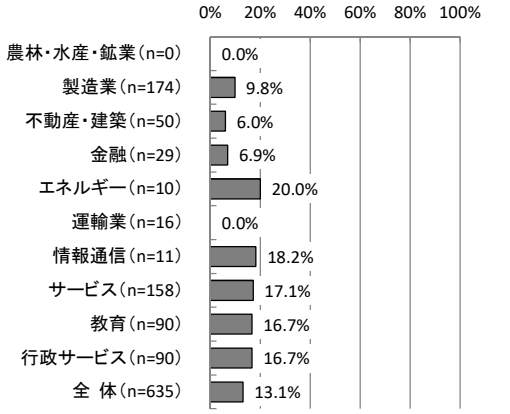
手口や実態に関する周知・教育



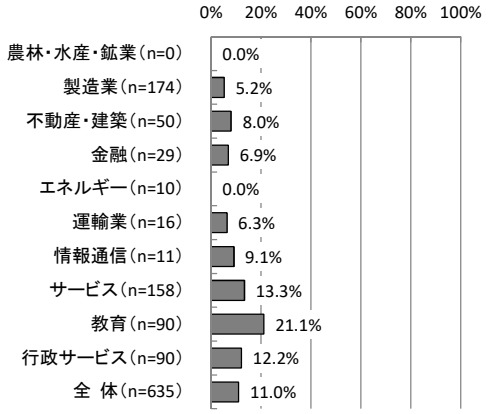
メール受信の対応訓練



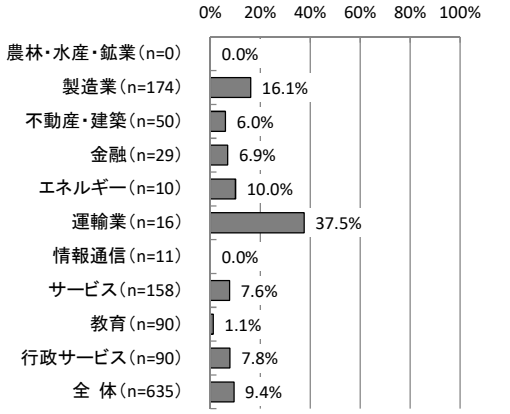
対策を検討中



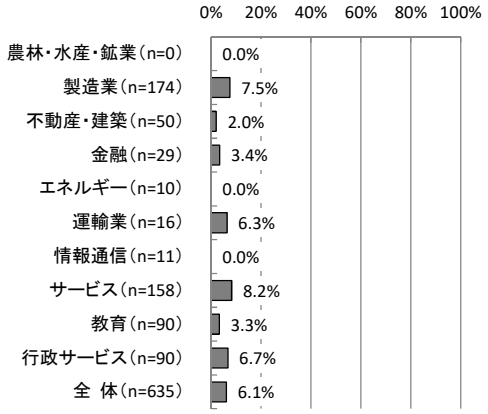
対策はしていない



メール以外の方法で口座情報を確認



メールによる口座情報送受信の禁止



3.1.33　情報セキュリティ対策に関する考え方 【問16】

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

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

調査対象とした基本的な考え方と相対する2つの考え

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

【全体】「投資方針」については、「①セキュリティ投資は必要最低限度に抑えるべきである」に近いとする割合が28.5%、「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69.7%となっており、「積極的」とする割合が「必要最低限」とする割合を41.2ポイント上回っている。

「事後的対応と予防的対応」については、「①情報セキュリティ対策としては、問題発生に対しての応急対応や、再発防止・被害拡大防止に注力するべきである」に近いとする割合が23.6%、「②情報セキュリティ対策としては、リスクの検知など、予防上の対策に注力するべきである」に近いとする割合が74.6%となっており、「予防的対応」とする割合が「問題発生への適切な対応」とする割合を51.0ポイントと大幅に上回っている。

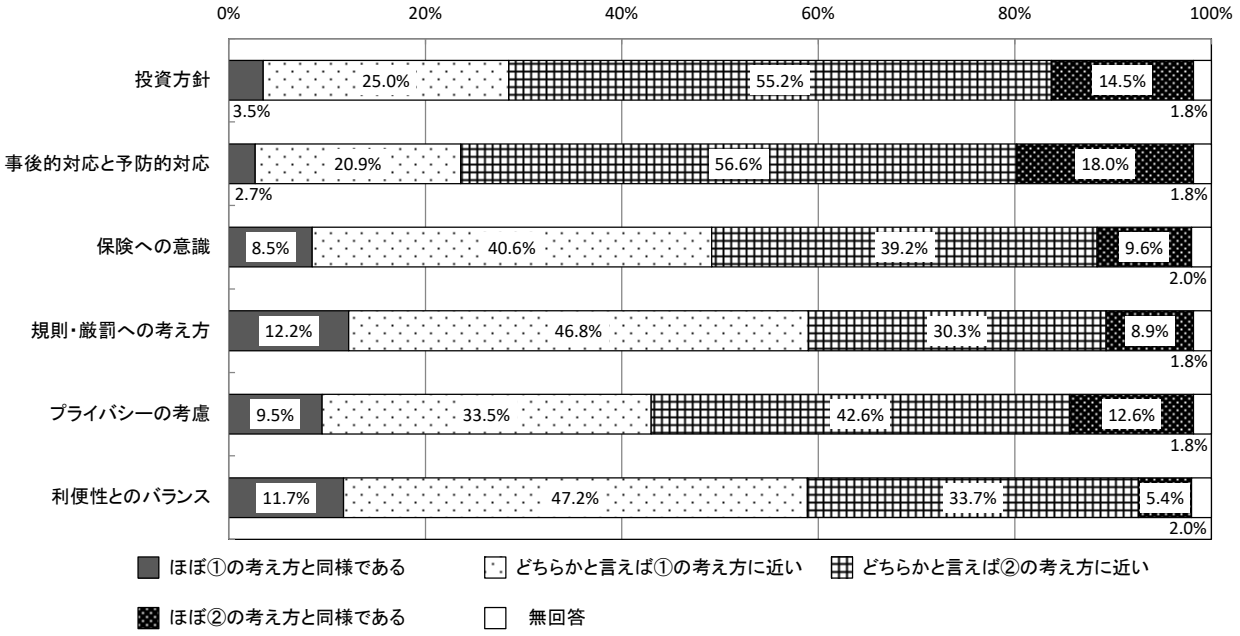
「保険への意識」については、「①情報セキュリティ対策としては、人的・技術的な対策によりカバーできるところを対策すれば十分である」に近いとする割合が49.1%、「②情報セキュリティ対策としては、人的・技術的対策によりカバーできないリスクは保険によりまかなうべきである」に近いとする割合が48.8%となっており、それぞれ同程度となっている。

「規制・罰則への考え方」については、「①技術以外の面での対策としては、従業員等への教育と、適切な情報提供により対策を促すことが重要である」に近いとする割合が59.0%、「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39.2%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19.8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43.0%、「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55.2%となっており、「ある程度のプライバシー保護の制約はやむをえない」とする割合が「プライバシーはある程度考慮されるべきだ」とする割合を12.2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58.9%、「②ユーザーにシステム利用上・業務上の負担を強いてでもセキュリティを守るべきである」とする39.1%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19.8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=716）



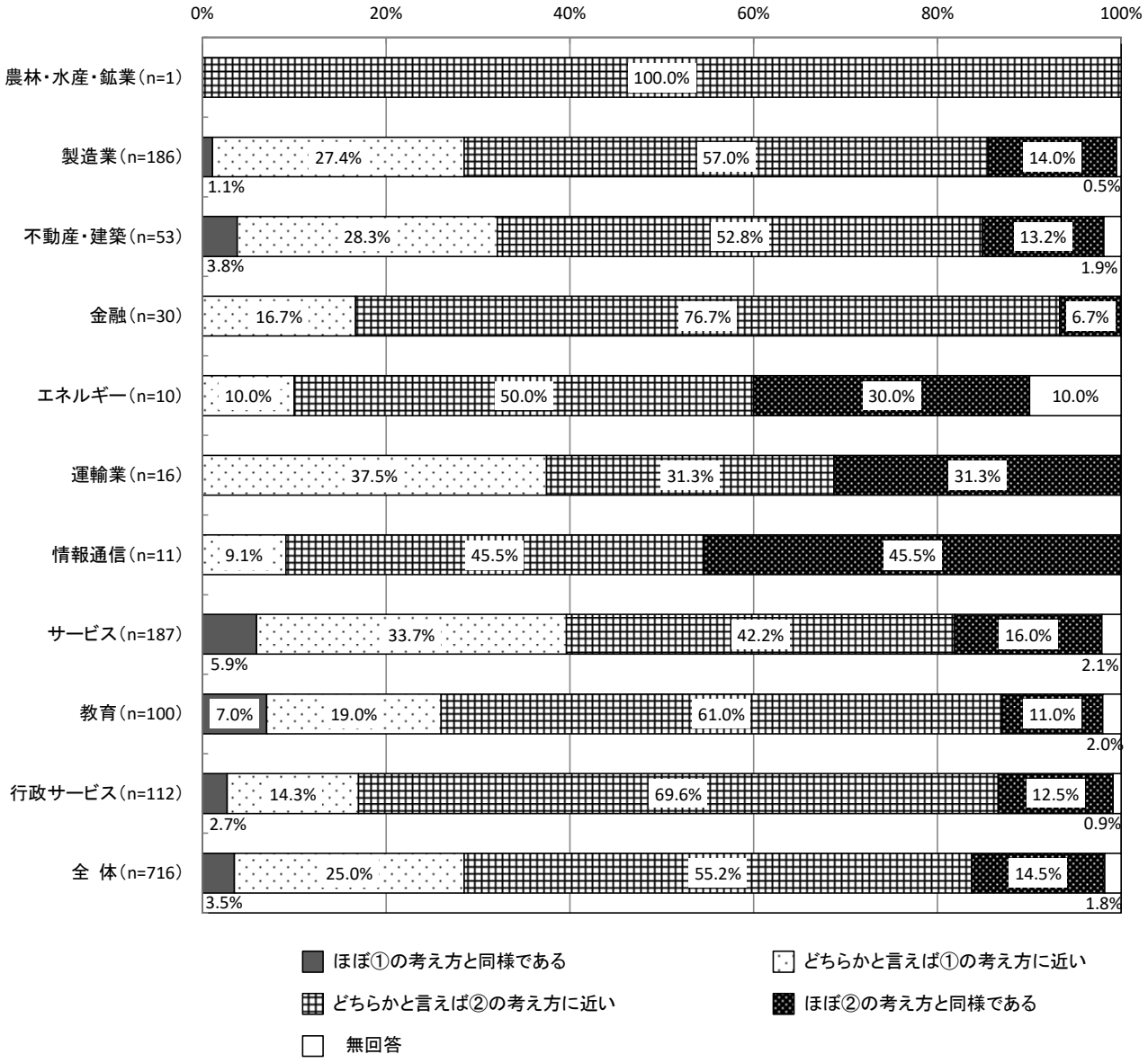
3.1.34　投資に関する考え方　【問16-1】

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。

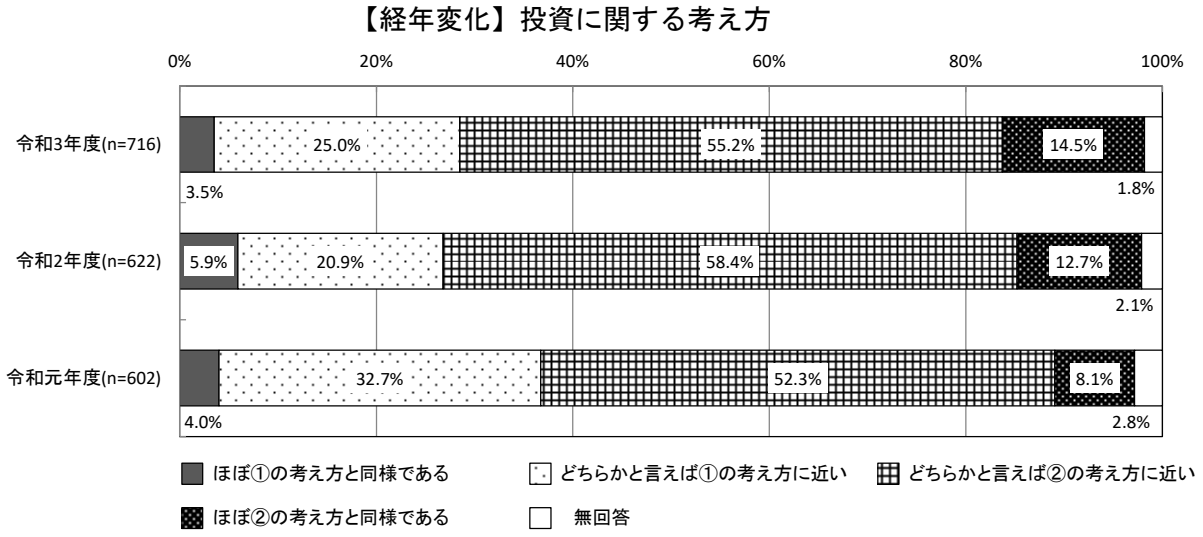
①として提示した考え方	②として提示した考え方
セキュリティ投資は必要最低限に抑えるべきである。	来るべき問題事案に備えて、積極的に投資を行うべきである。

【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「情報通信」が91.0%、「金融」が83.4%、「行政サービス」が82.1%となっている。

【業種別分析】投資に関する考え方



【経年変化】昨年度と比較すると、「①必要最低限」は1.7ポイントの増加、「②積極的投資」は1.4ポイントの減少となっている。



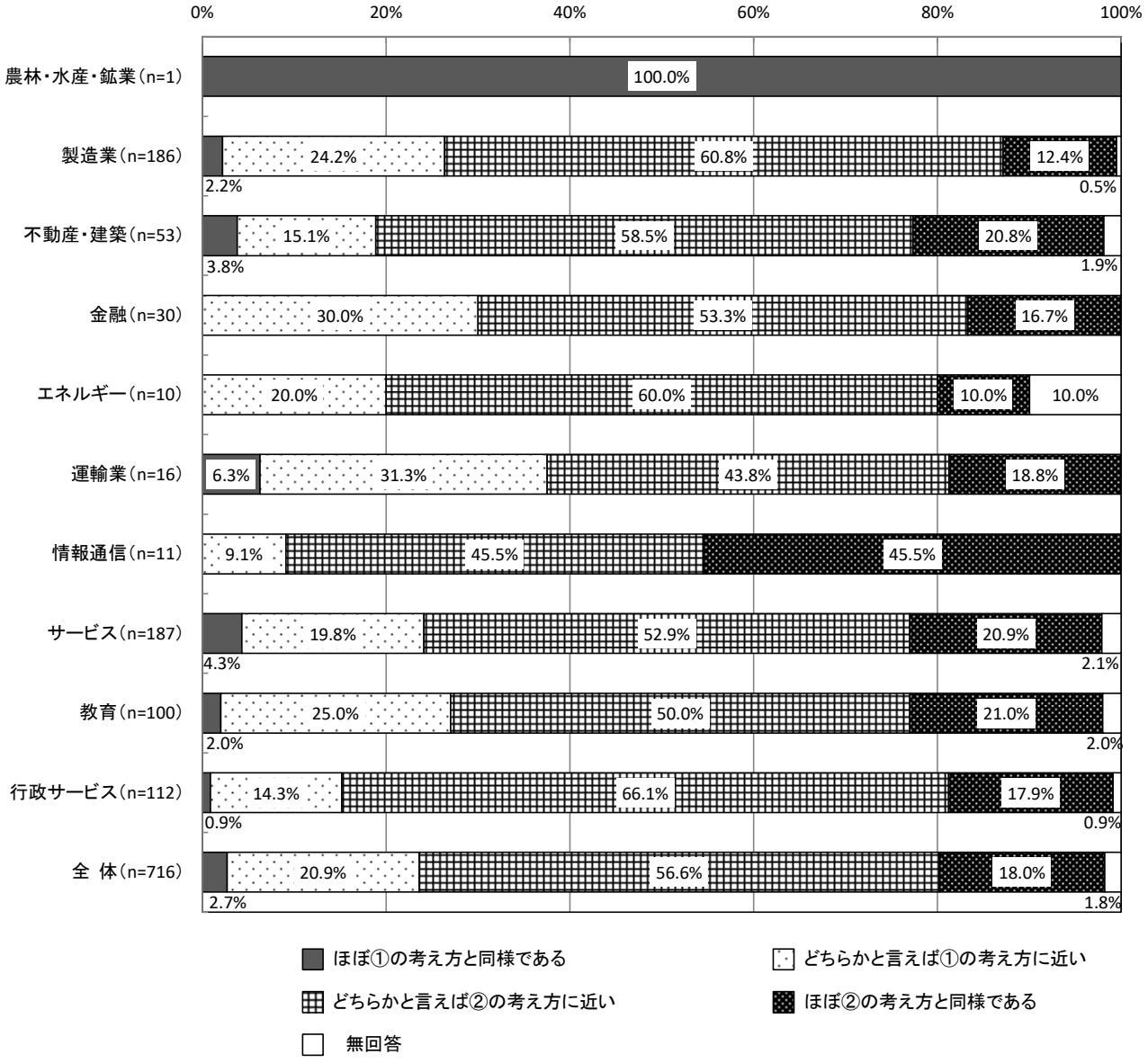
3.1.35　事後的対応と予防的対応に関する考え方　【問16-2】

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。

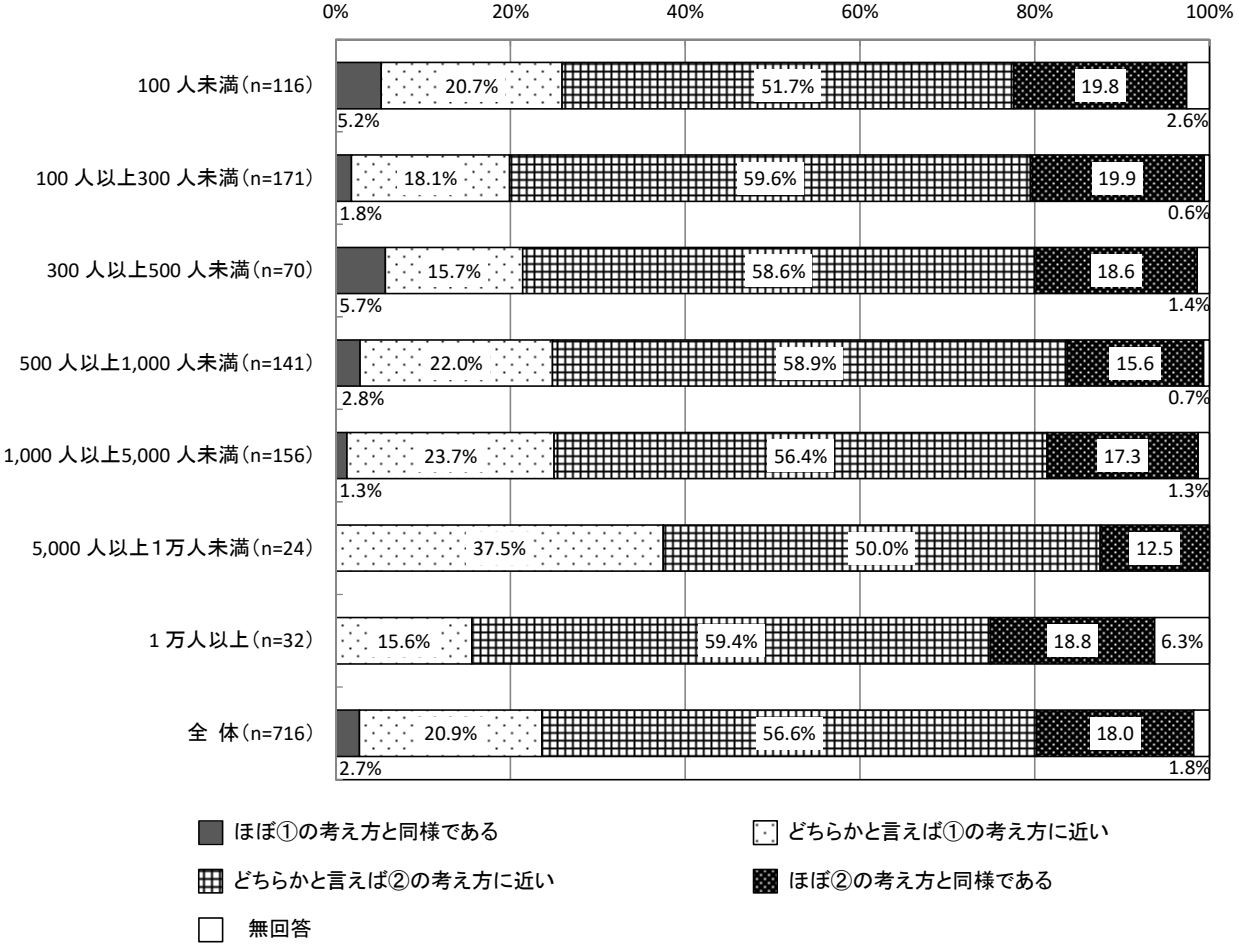
【業種別分析】業種別にみると、全ての業種で「②予防的対応」の割合が多く、特に「情報通信」が91.0%、「行政サービス」が84.0%、「不動産・建築」が79.3%となっている。

【業種別分析】事後的対応と予防的対応に関する考え方

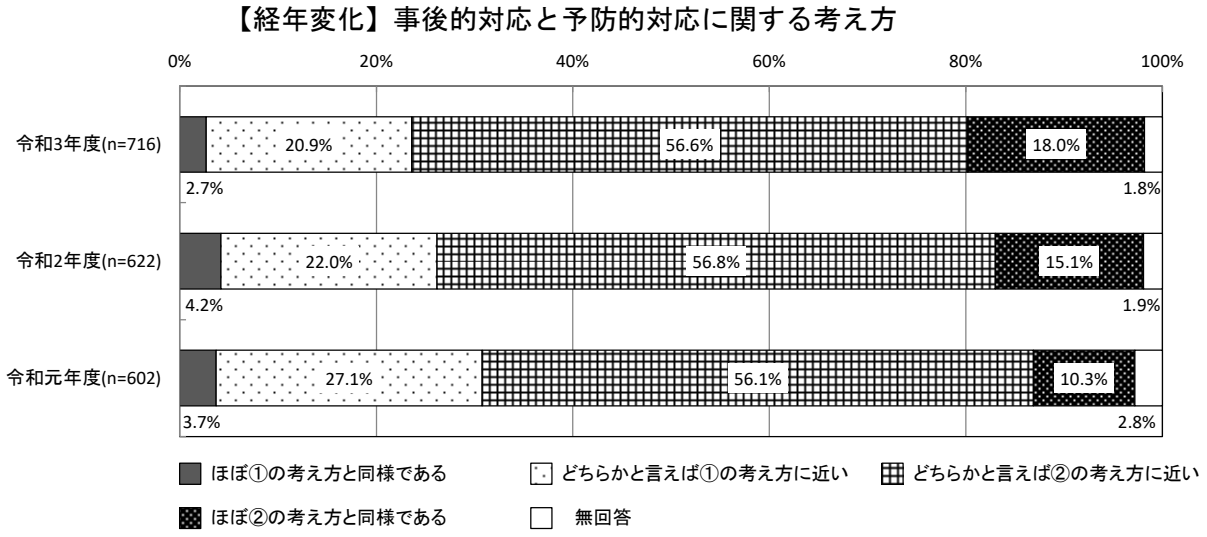


【従業員規模別分析】従業員規模別にみると、全ての従業員規模で「②予防的対応」が「①問題発生への適切な対応」を上回っている。

【従業員規模別分析】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2.6ポイントの減少、「②予防的対応」は2.7ポイントの増加となっている。



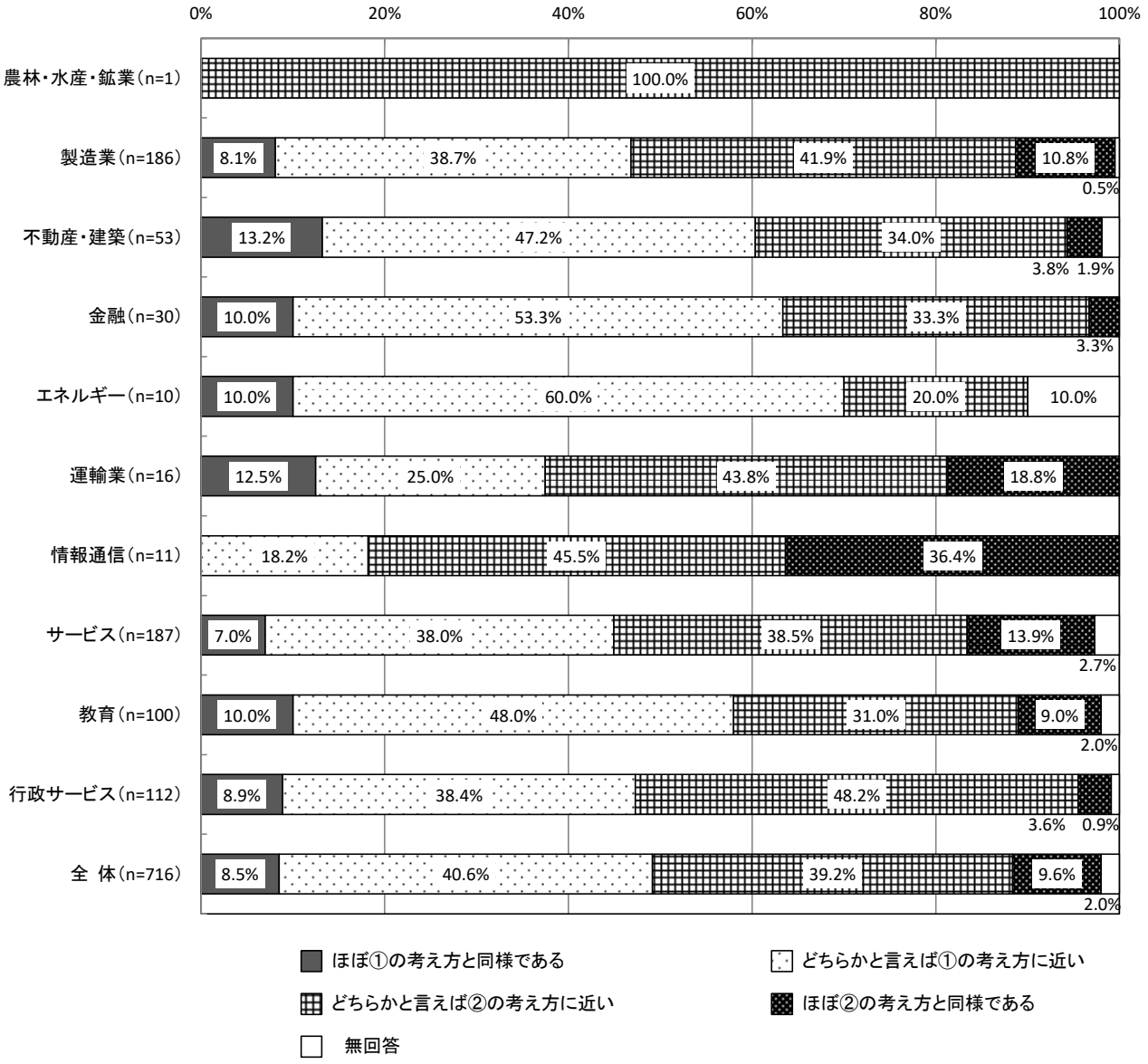
3.1.36　保険への意識　【問16-3】

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。

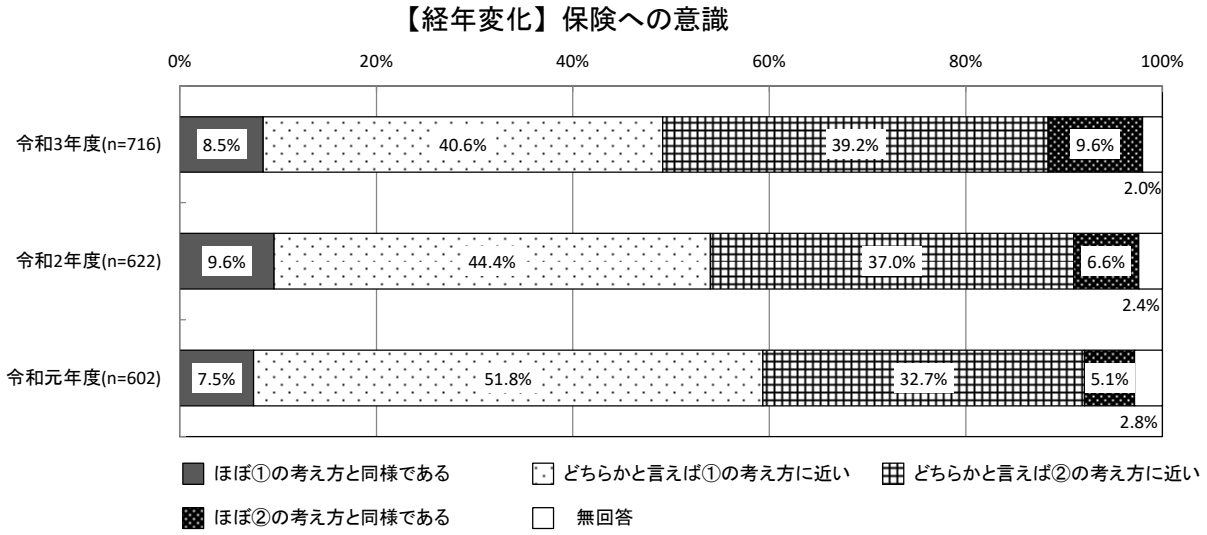
①として提示した考え方	②として提示した考え方
情報セキュリティ対策としては、人的・技術的な対策によりカバーできるところを対策すれば十分である。	情報セキュリティ対策としては、人的・技術的対策によりカバーできないリスクは保険によりまかなうべきである。

【業種別分析】業種別にみると、「不動産・建築」「金融」「エネルギー」「教育」で「①人的・技術的な対策で十分」が「②保険的な対応が必要」を上回っており、特に「エネルギー」で70.0%となっている。一方、「製造業」「運輸業」「情報通信」「サービス」「行政サービス」では「②保険的な対応が必要」が「①人的・技術的な対策で十分」を上回っており、特に「情報通信」で81.9%となっている。

【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4.9ポイントの減少となり、「②保険的な対応が必要」は5.2ポイントの増加となっている。



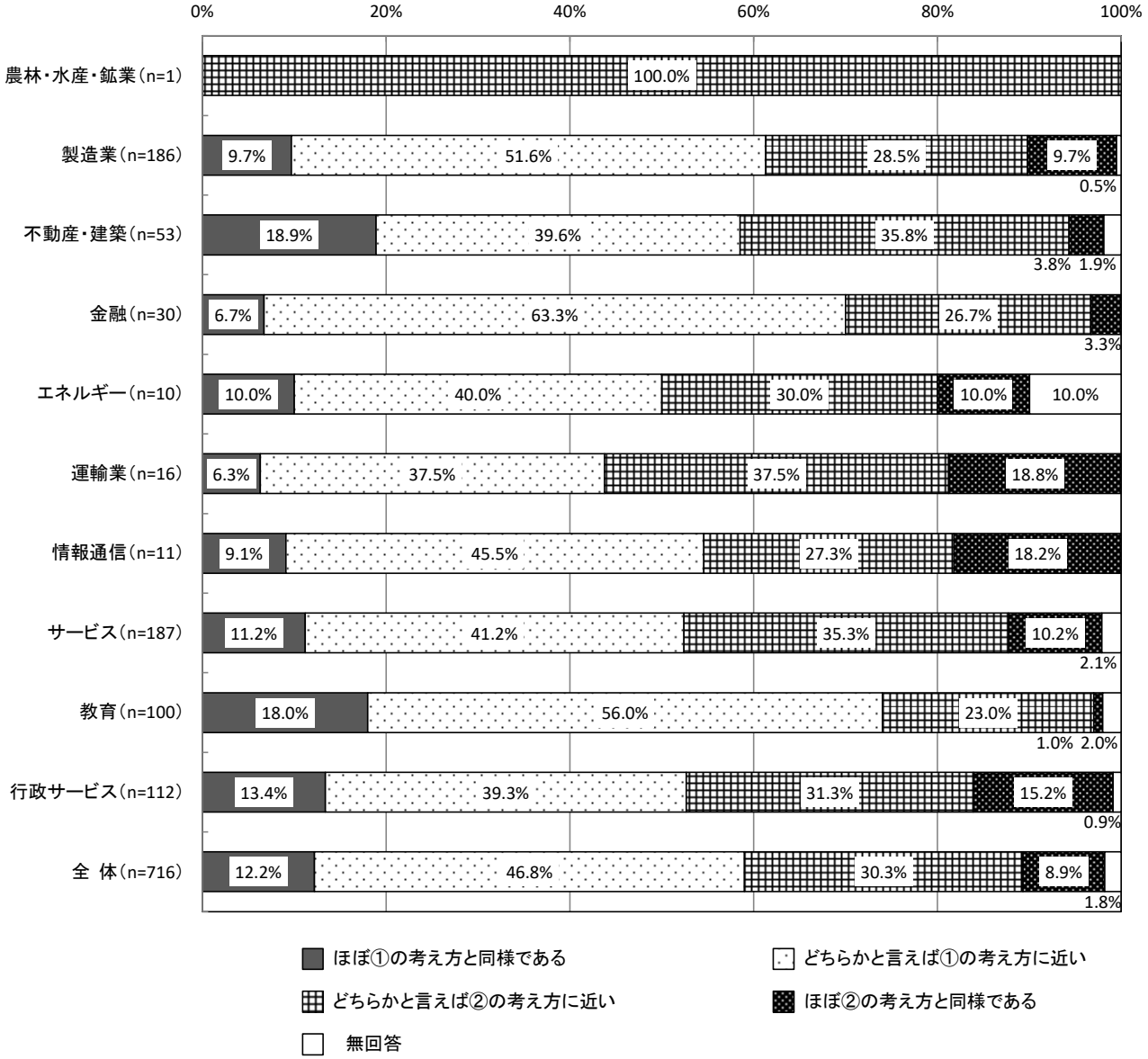
3.1.37　規制・罰則への考え方　【問16-4】

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。

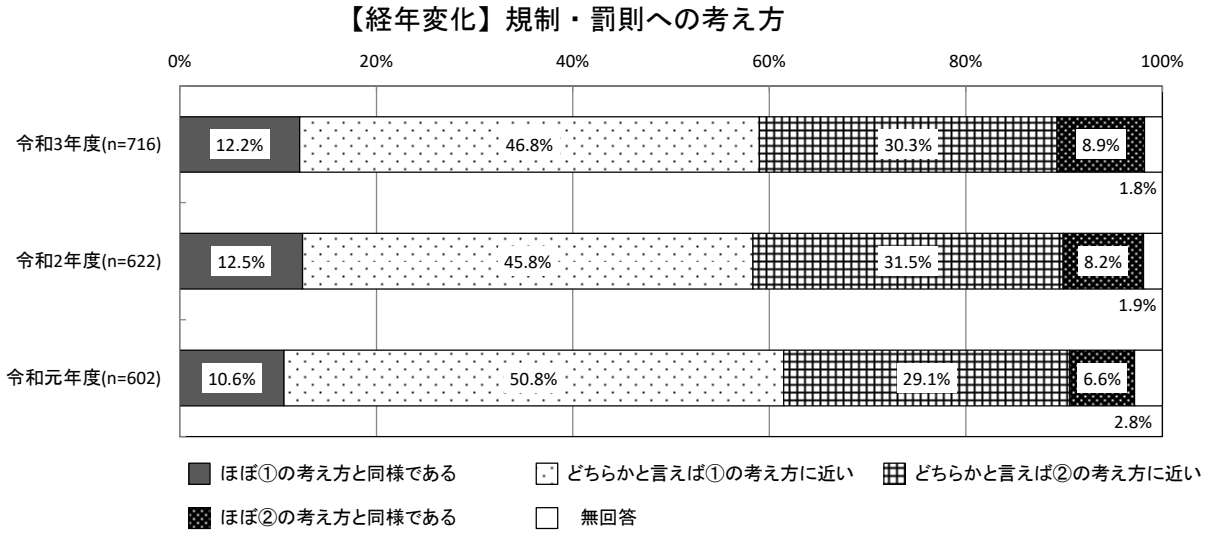
①として提示した考え方	②として提示した考え方
技術以外の面での対策としては、従業員等への教育と、適切な情報提供により対策を促すことが重要である。	技術以外の面での対策としては、教育はもちろんのこと、規制・罰則などの強制力のある制度的対応を行うことが重要である。

【業種別分析】業種別にみると、「運輸業」を除くすべての業種で「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「教育」では「①人的・技術的な対策で十分」が50.0ポイント上回っている。

【業種別分析】規制・罰則への考え方



【経年変化】昨年度と比較すると、「①教育と情報提供を中心とした対応」は0.7ポイントの増加、「②規則・罰則も含む強制力のある対応」は0.5ポイントの減少となっている。



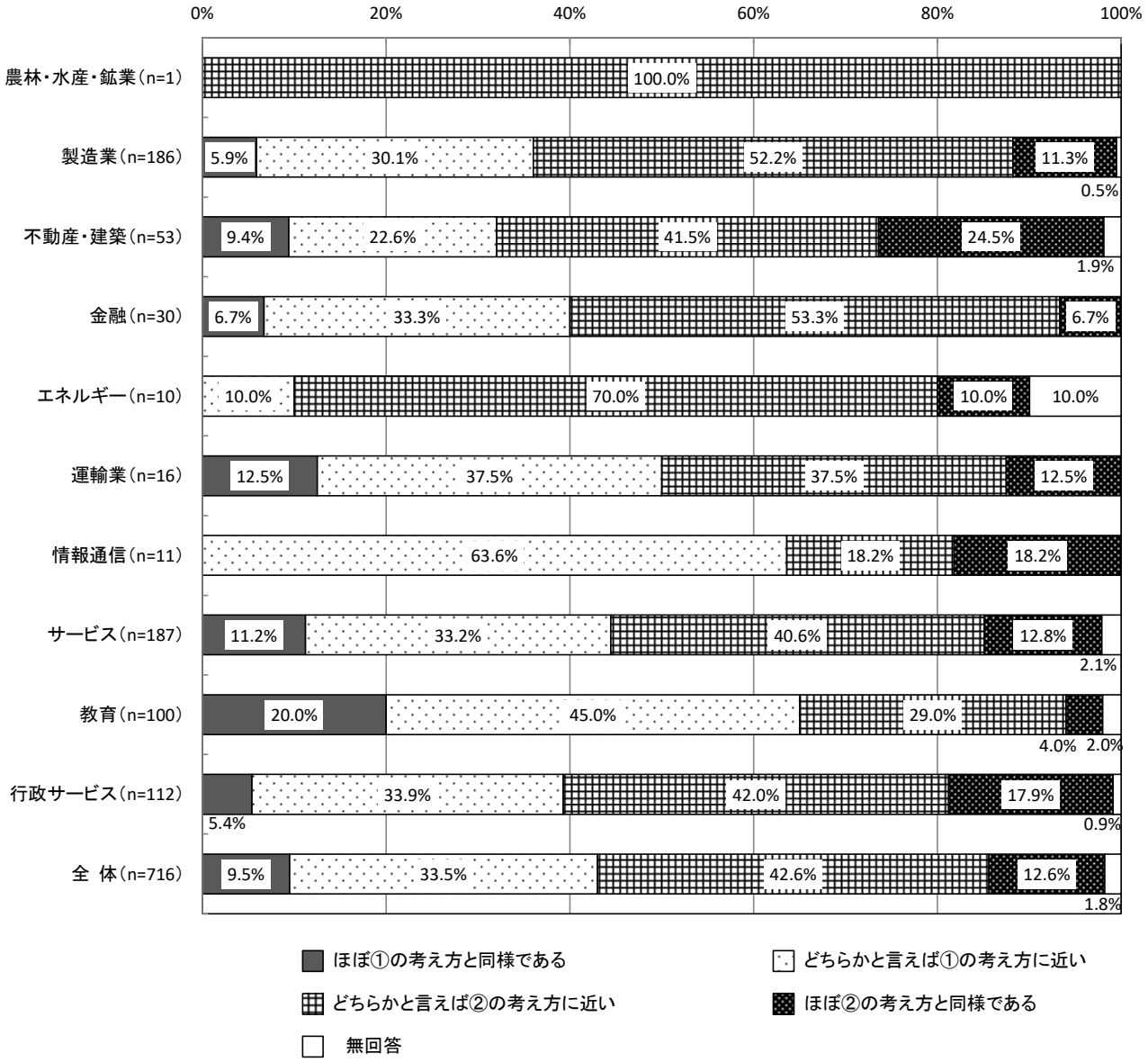
3.1.38　プライバシーの考慮に関する考え方　【問16-5】

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。

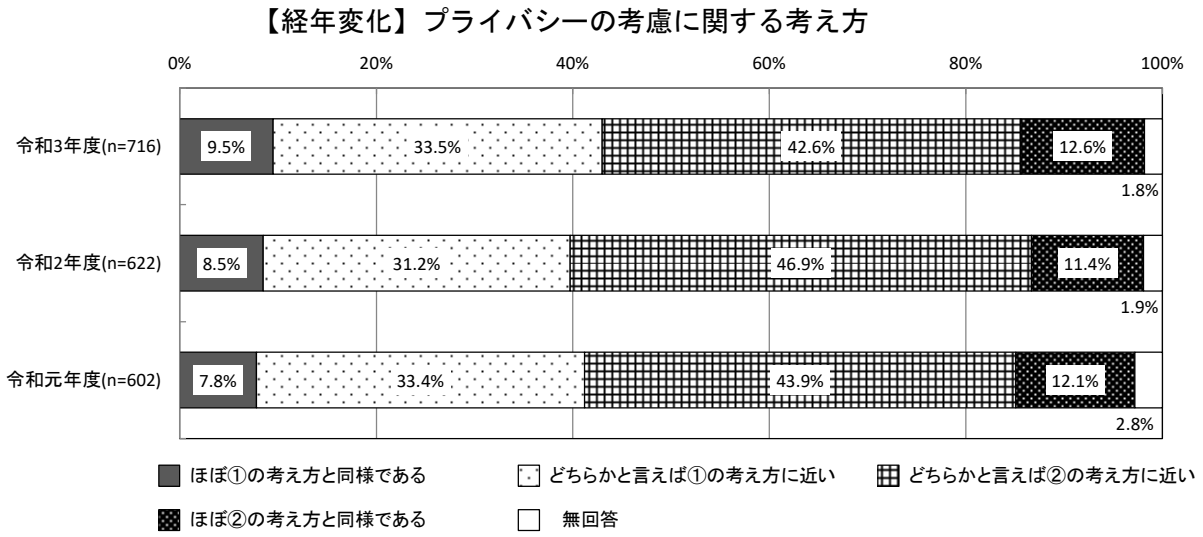
①として提示した考え方	②として提示した考え方
職場とはいえ、従業員等のプライバシーはある程度考慮したうえで、情報セキュリティ対策は行われるべきである。	職場のセキュリティ保護のためにはシステム利用状況のモニタリングなどによるプライバシー保護の制約はやむをえない。

【業種別分析】業種別を見ると、「運輸業」「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20.6ポイント「②プライバシー保護の制約はやむをえない」が多くなっている。

【業種別分析】プライバシーの考慮に関する考え方



【経年変化】昨年度と比較すると、「①プライバシーはある程度考慮すべき」は3.3ポイントの増加、「②プライバシーの保護の制約はやむをえない」は3.1ポイントの減少となっている。



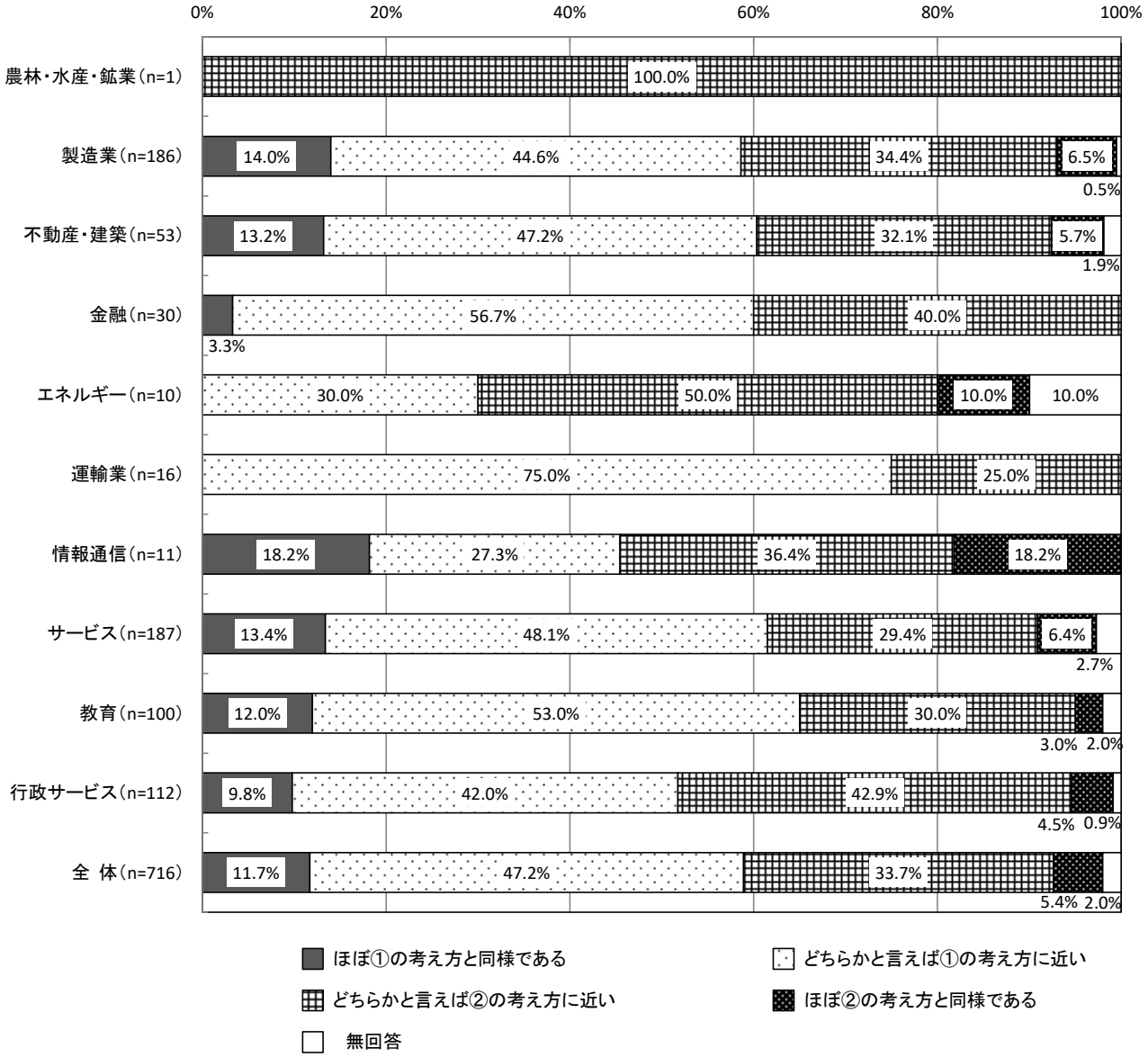
3.1.39　利便性とのバランスに関する考え方　【問16-6】

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。

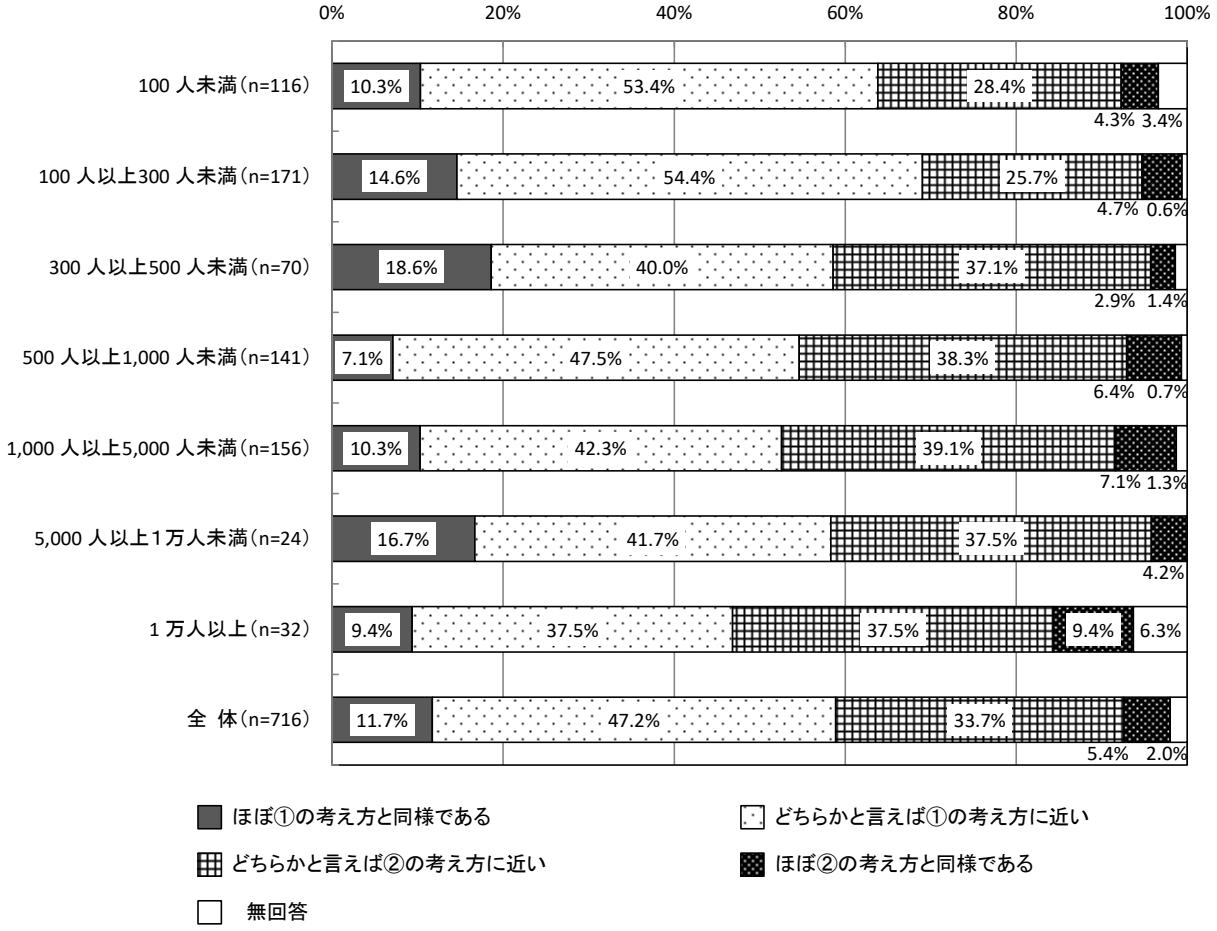
【業種別分析】業種別にみると、「エネルギー」「情報通信」を除くすべての業種で「①利便性とのバランスを考慮」が「②負担を強いてでもセキュリティを守る」を上回っている。特に「運輸業」で50.0ポイント、「教育」で32.0ポイント「①利便性とのバランスを考慮」が多くなっている。

【業種別分析】利便性とのバランスに関する考え方

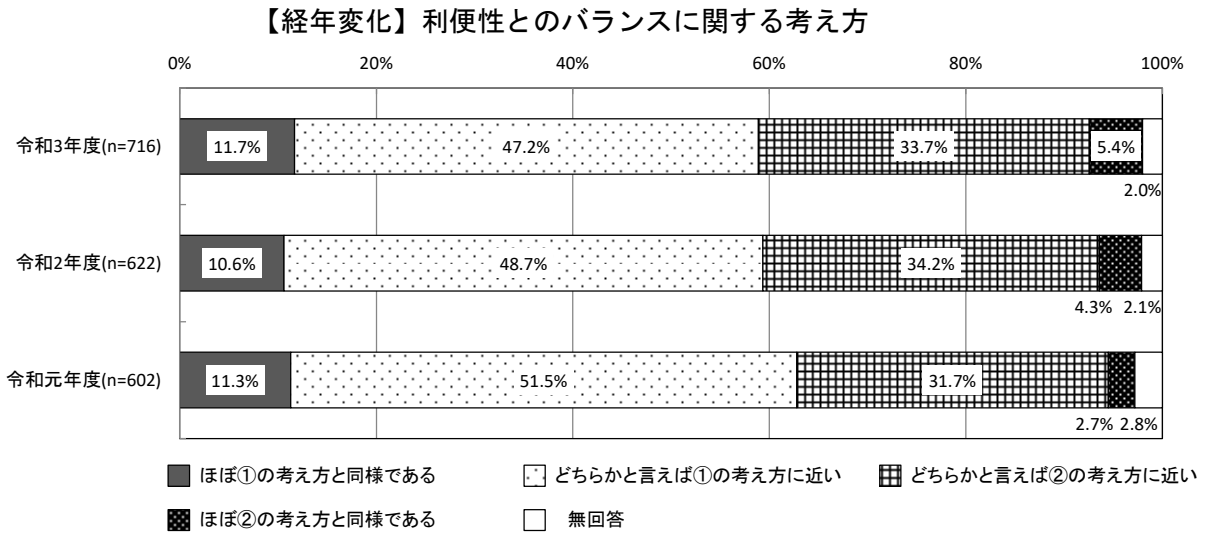


【従業員規模別分析】従業員規模別にみると、すべての従業員規模で「①利便性とのバランスを考慮」が「②負担を強いてでもセキュリティを守る」を上回っている。

【従業員規模別分析】利便性とのバランスに関する考え方



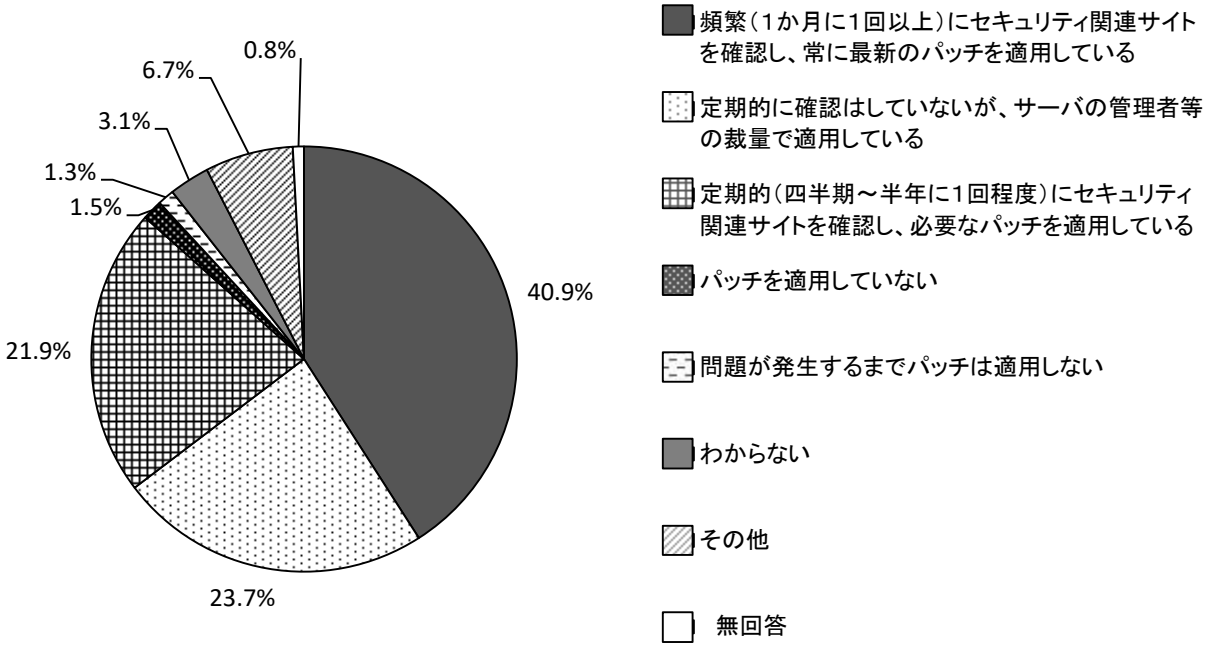
【経年変化】昨年度と比較すると、「①利便性とのバランスを考慮」は0.4ポイントの減少、「②負担を強いてでもセキュリティを守る」は0.6ポイントの増加となっている。



3.1.40　セキュリティパッチの適用状況　【問17】

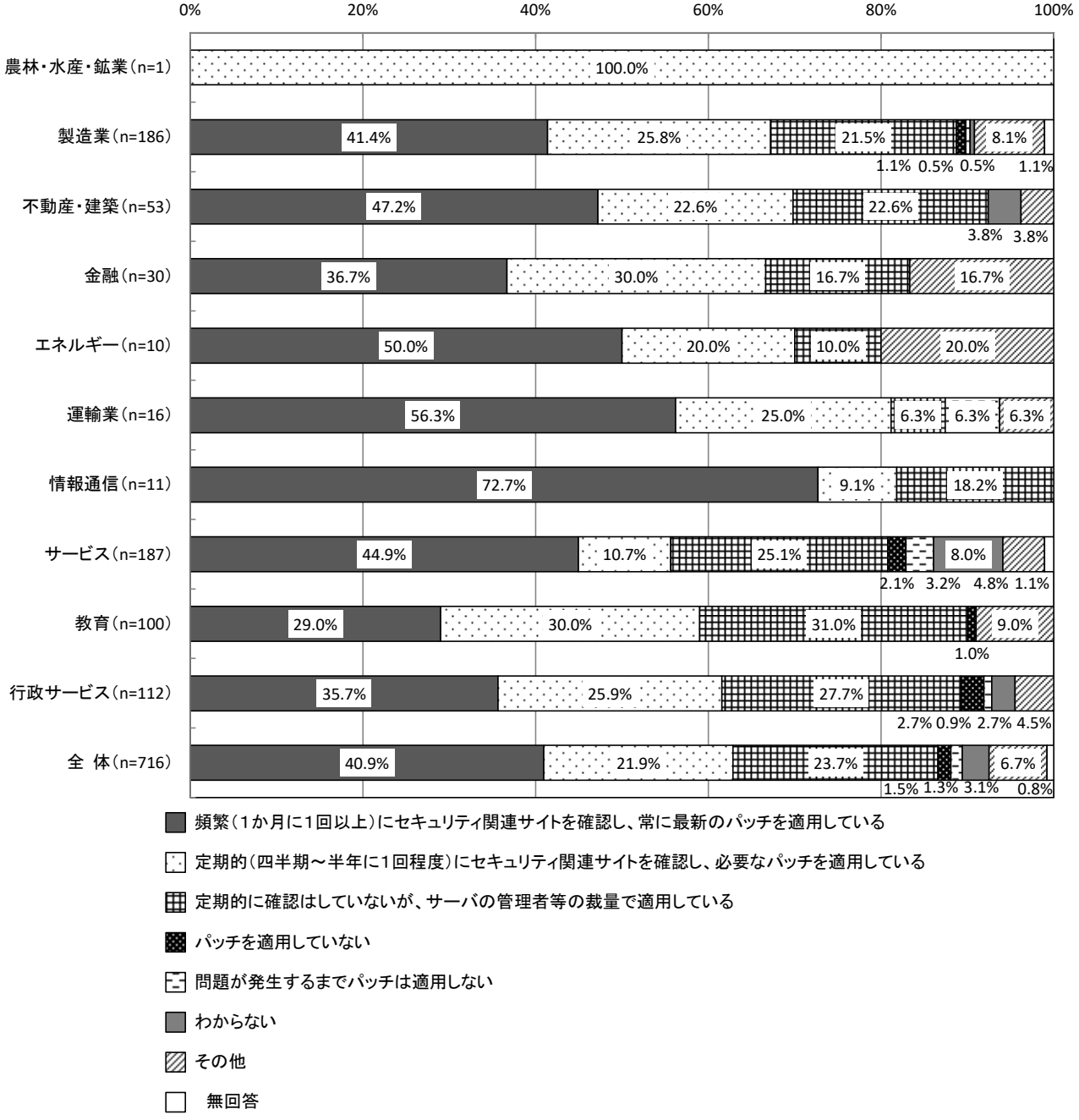
セキュリティパッチの適用状況については、「頻繁（１か月に１回以上）にセキュリティ関連サイトを確認し、常に最新のパッチを適用している」が40.9%で最も多く、次いで「定期的に確認はしていないが、サーバの管理者等の裁量で適用している」が23.7%、「定期的（四半期～半年に１回程度）にセキュリティ関連サイトを確認し、必要なパッチを適用している」が21.9%となっている。

【全体】セキュリティパッチの適用状況（SA,n=716）



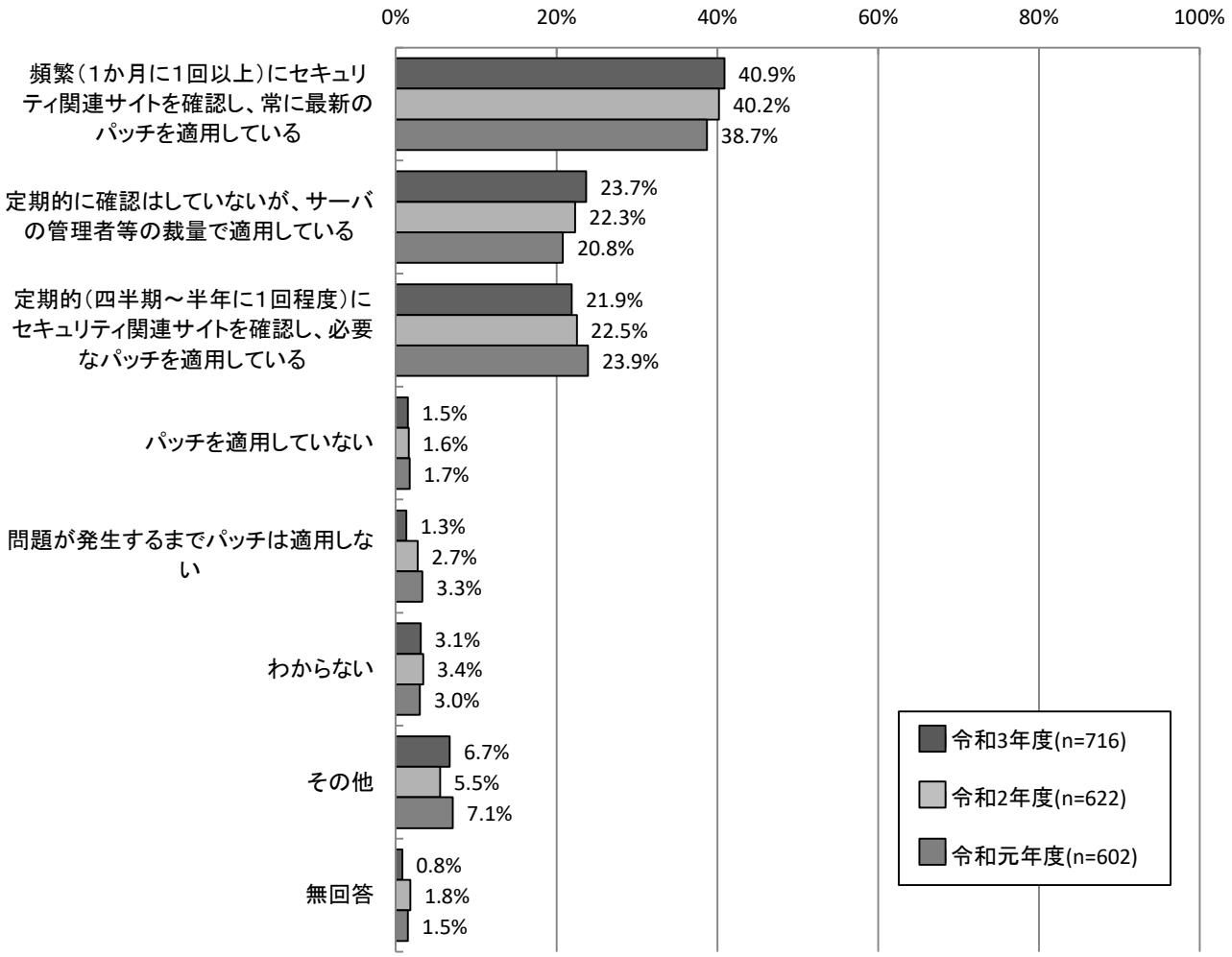
【業種別分析】業種別にみると、「頻繁（１か月に１回以上）にセキュリティ関連サイトを確認し、常に最新のパッチを適用している」については、「情報通信」が72.7％と最も多く、次いで「運輸業」が56.3％となっている。

【業種別分析】セキュリティパッチの適用状況



【経年変化】昨年度と比較すると、「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1.4ポイント、「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」が0.7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

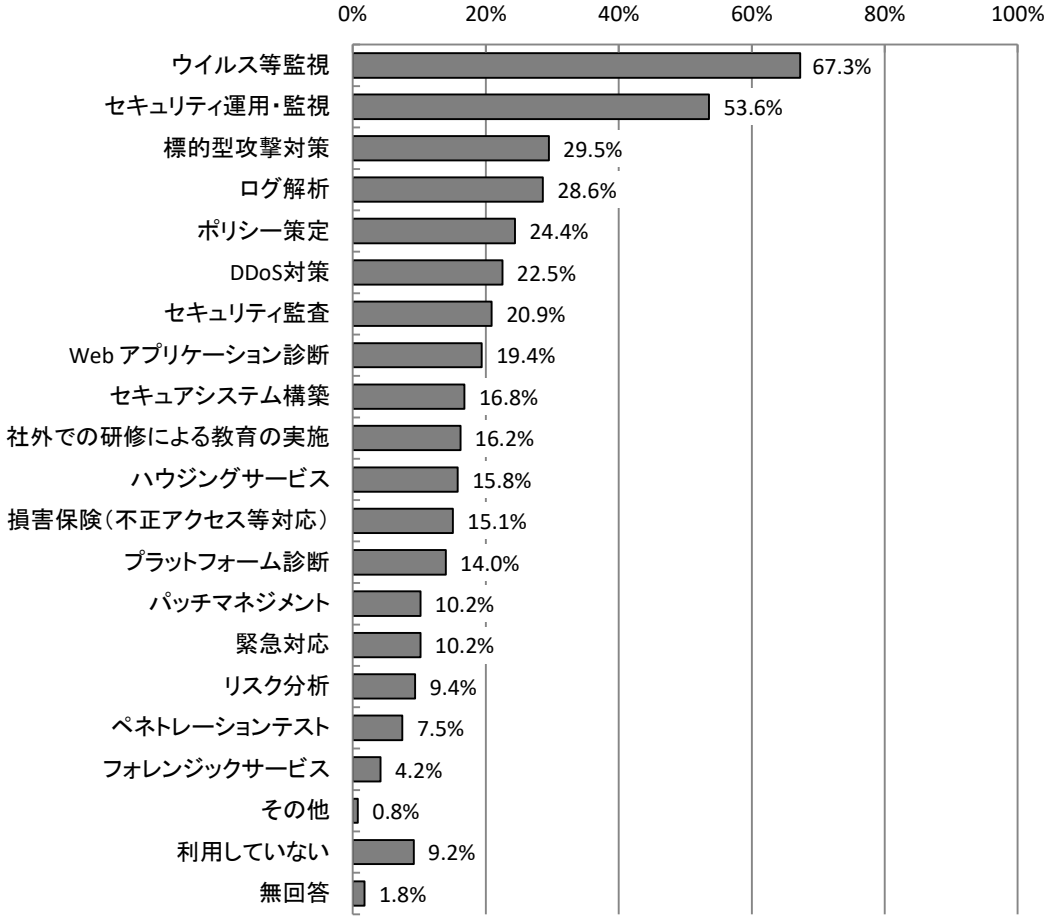


3.2　技術的対策

3.2.1　利用しているセキュリティサービス　【問18】

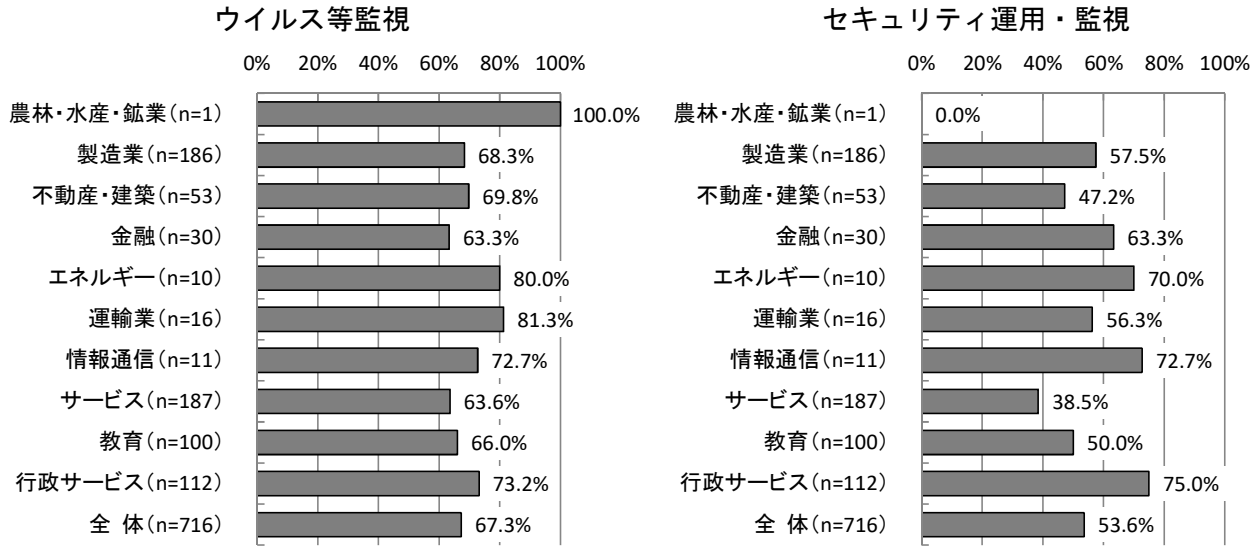
利用しているセキュリティサービスについては、「ウイルス等監視」が67.3%で最も多く、次いで「セキュリティ運用・監視」が53.6%となっている。一方「利用していない」は9.2%となっている。

【全体】利用しているセキュリティサービス（MA,n=716）



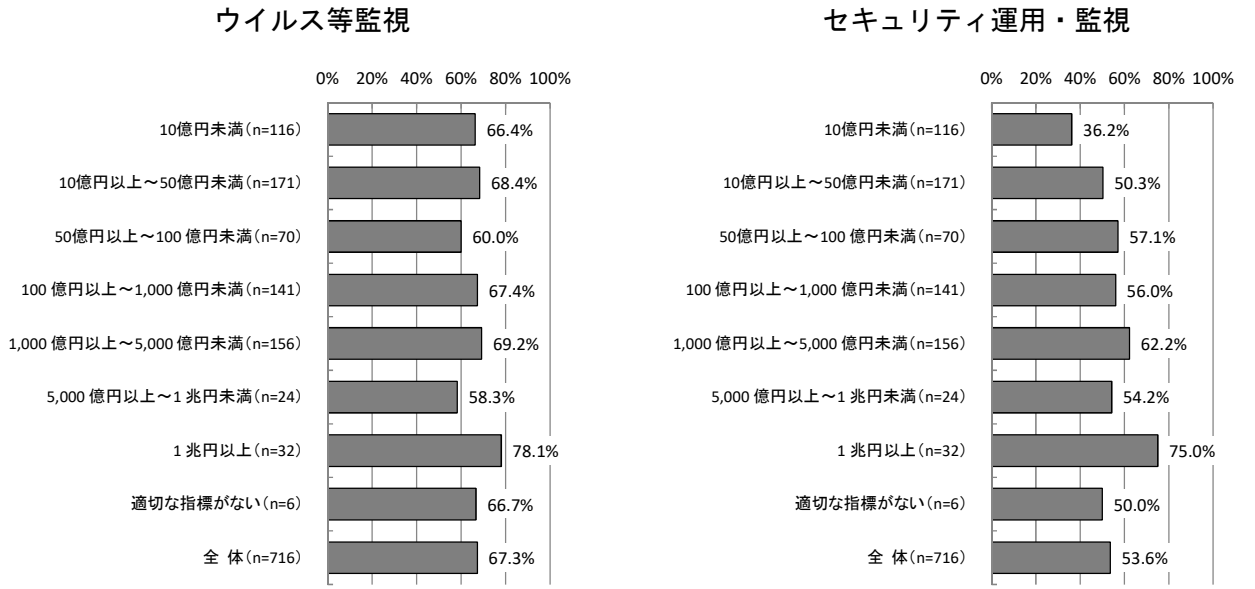
【業種別分析】業種別にみると、「ウイルス等監視」については、「運輸業」が81.3%で最も多く、次いで「エネルギー」が80.0%と8割を超えている。「セキュリティ運用・監視」については、「行政サービス」が75.0%で最も多く、次いで「情報通信」が72.7%となっている。

【業種別分析】利用しているセキュリティサービス



【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78.1%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、「１兆円以上」が75.0%で最も多くなっている。

【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

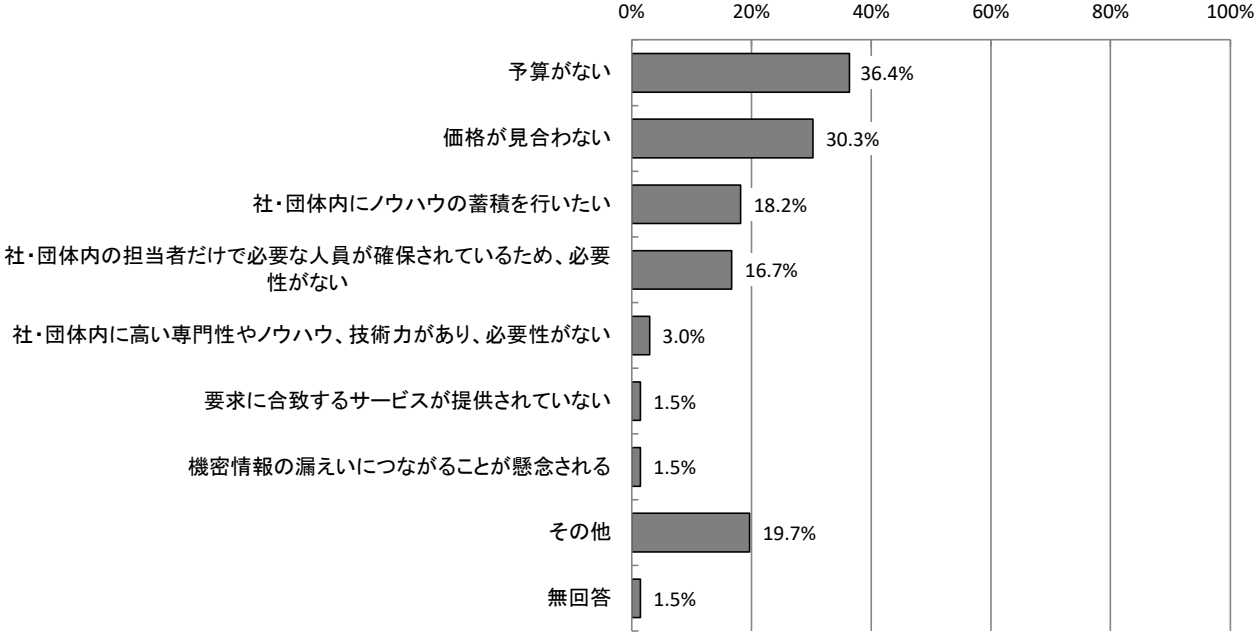


3.2.2　セキュリティサービスを利用していない理由　【問18-1】

セキュリティサービスを利用していない理由については、「予算がない」が36.4%で最も多く、次いで「価格が見合わない」が30.3%と、金銭面の理由が上位に挙げられている。

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

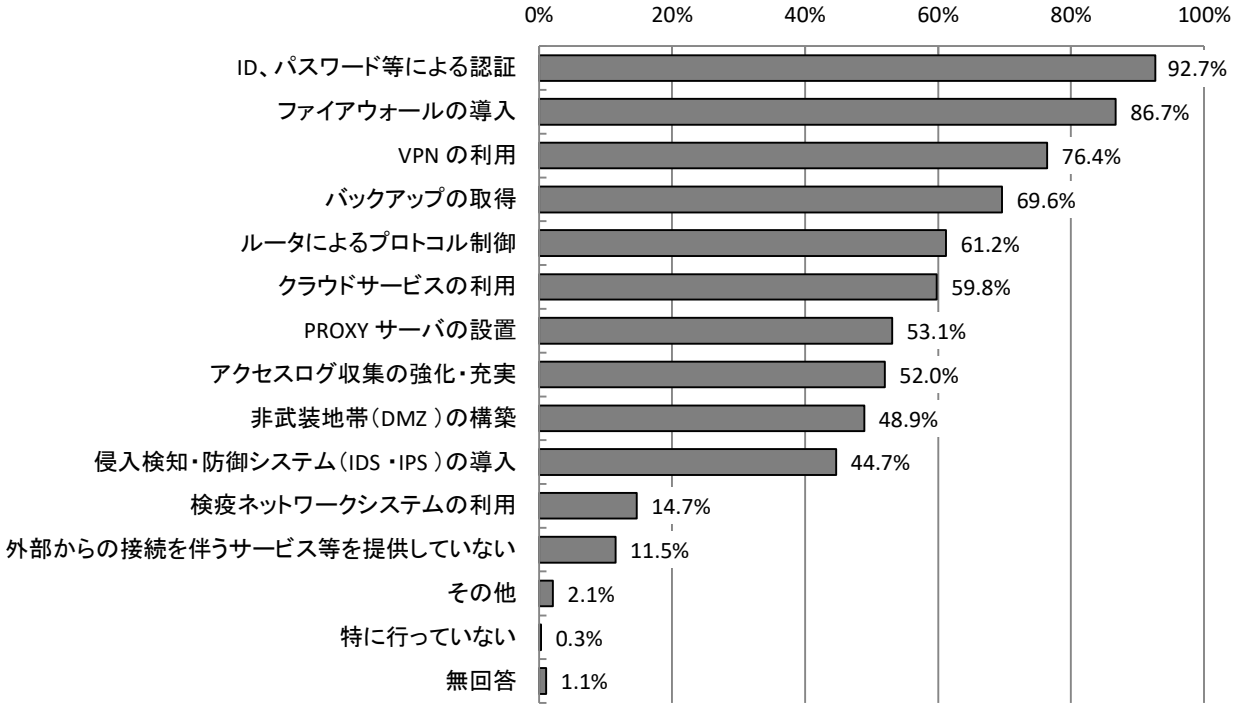
【全体】セキュリティサービスを利用していない理由（MA,n=66）



3.2.3　インターネット接続に対するセキュリティ対策　【問19】

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92.7%で最も多く、次いで「ファイアウォールの導入」が86.7%、「VPNの利用」が76.4%となっている。

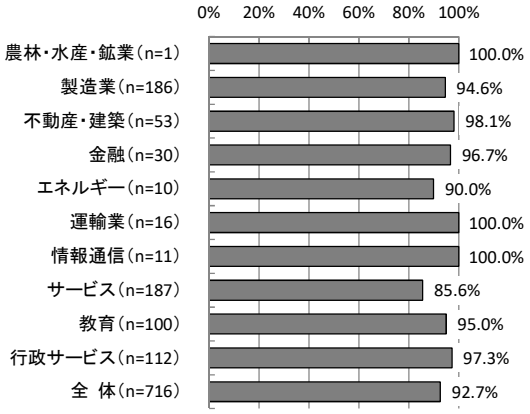
【全体】インターネット接続に対するセキュリティ対策（MA, n=716）



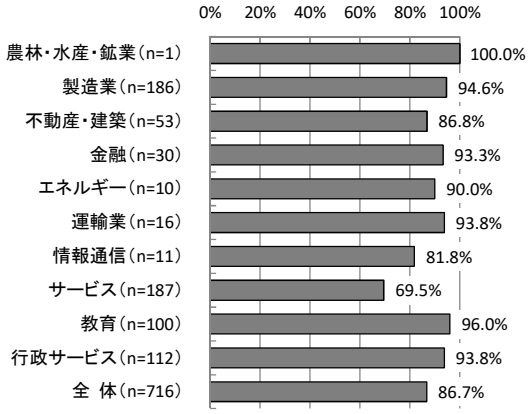
【業種別分析】業種別にみると、「ID、パスワード等による認証」については、「運輸業」「情報通信」が100.0%で最も多くなっている。「ファイアウォールの導入」については、「教育」が96.0%で最も多くなっている。

【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

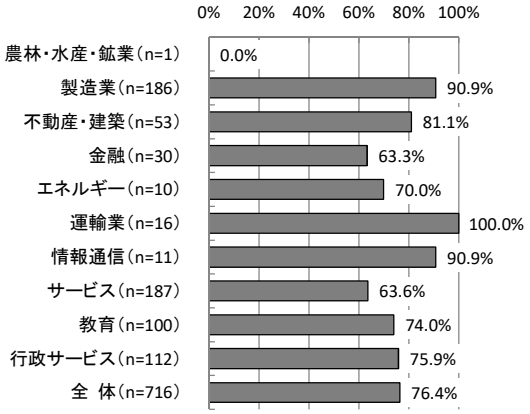
ID、パスワード等による認証



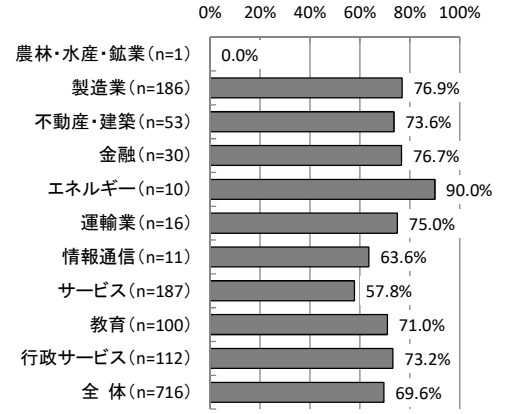
ファイアウォールの導入



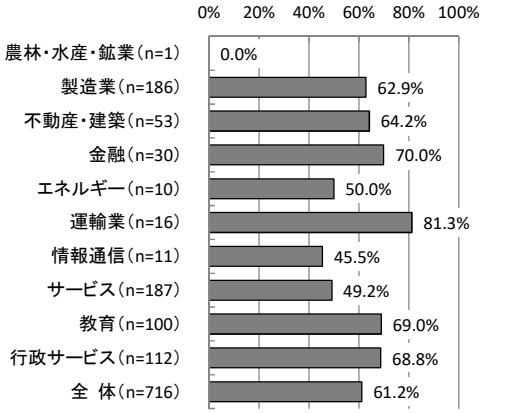
VPN の利用



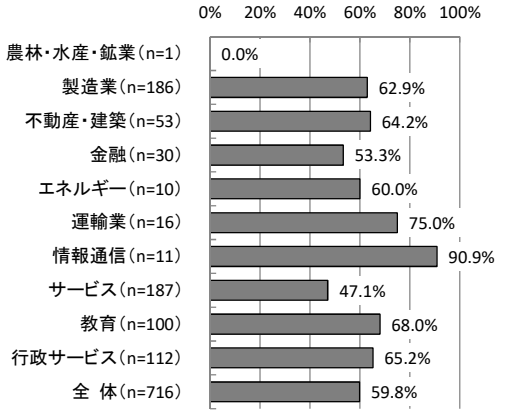
バックアップの取得



ルータによるプロトコル制御

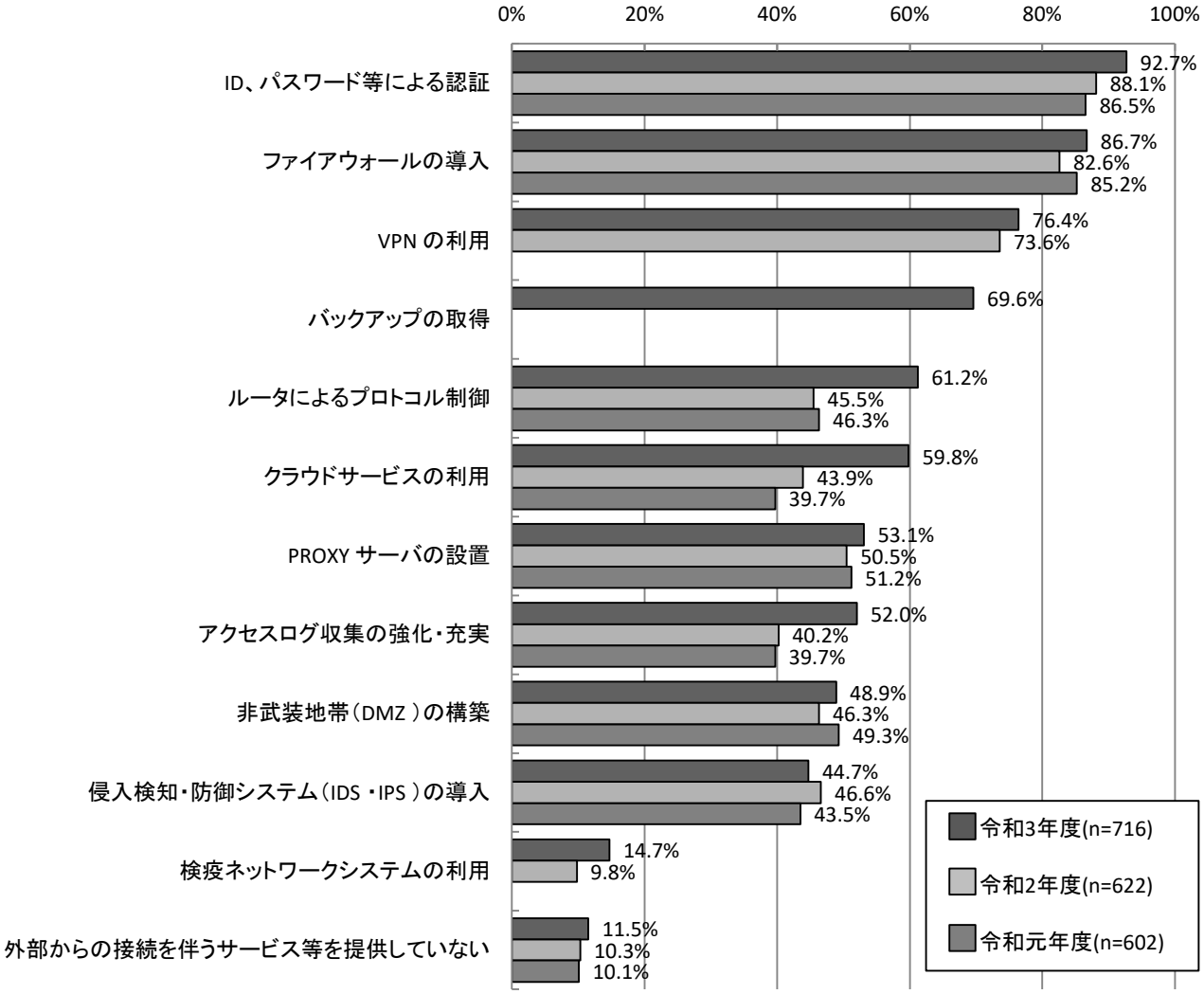


クラウドサービスの利用



【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15.9ポイント、「ルータによるプロトコル制御」が15.7ポイント増加している。

【経年変化】インターネット接続に対するセキュリティ対策



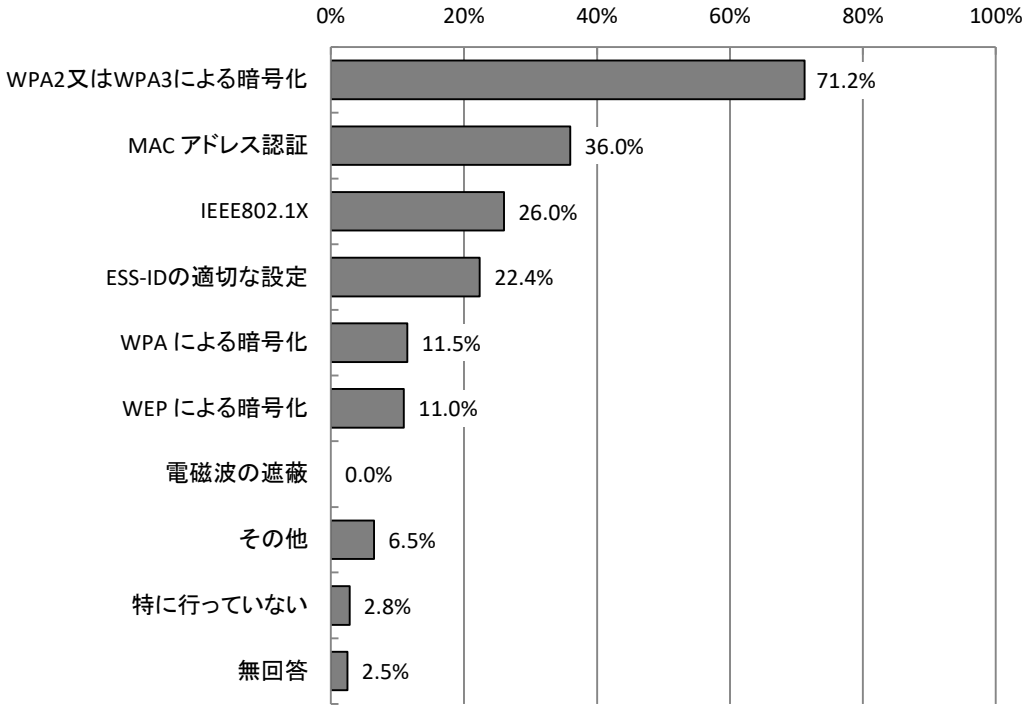
※令和２年度調査で「VPNの利用」「検疫ネットワークシステムの利用」を新設
※令和３年度調査で「バックアップの取得」を新設

3.2.4　無線LANネットワークのセキュリティ対策　【問20】

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71.2%で最も多く、次いで「MACアドレス認証」が36.0%となっている。

※本項目は、事業体内で無線LANを使用している社・団体等を対象としている。

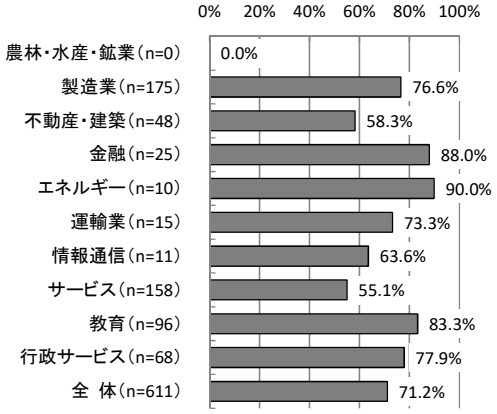
【全体】無線LANネットワークのセキュリティ対策（MA,n=611）



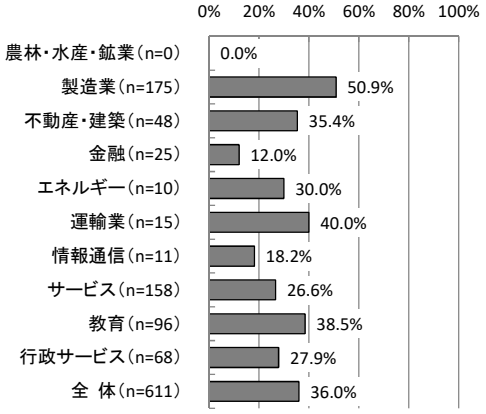
【業種別分析】業種別にみると、「WPA2又はWPA3による暗号化」については、「エネルギー」が90.0%で最も多く、次いで「金融」が88.0%となっている。「MACアドレス認証」については、「製造業」が50.9%で最も多くなっている。

【業種別分析】無線LANネットワークのセキュリティ対策

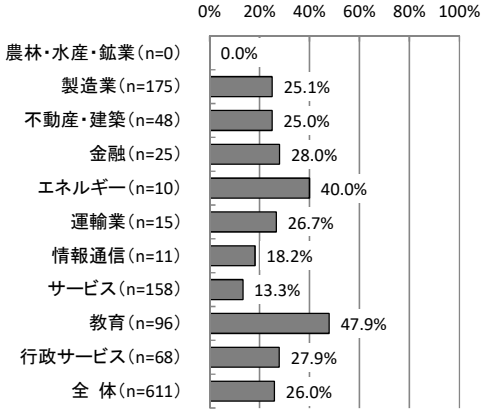
WPA2又はWPA3による暗号化



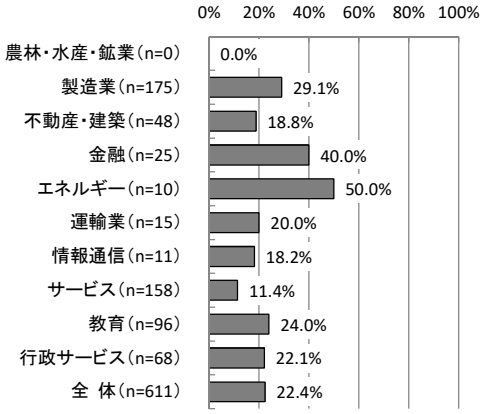
MAC アドレス認証



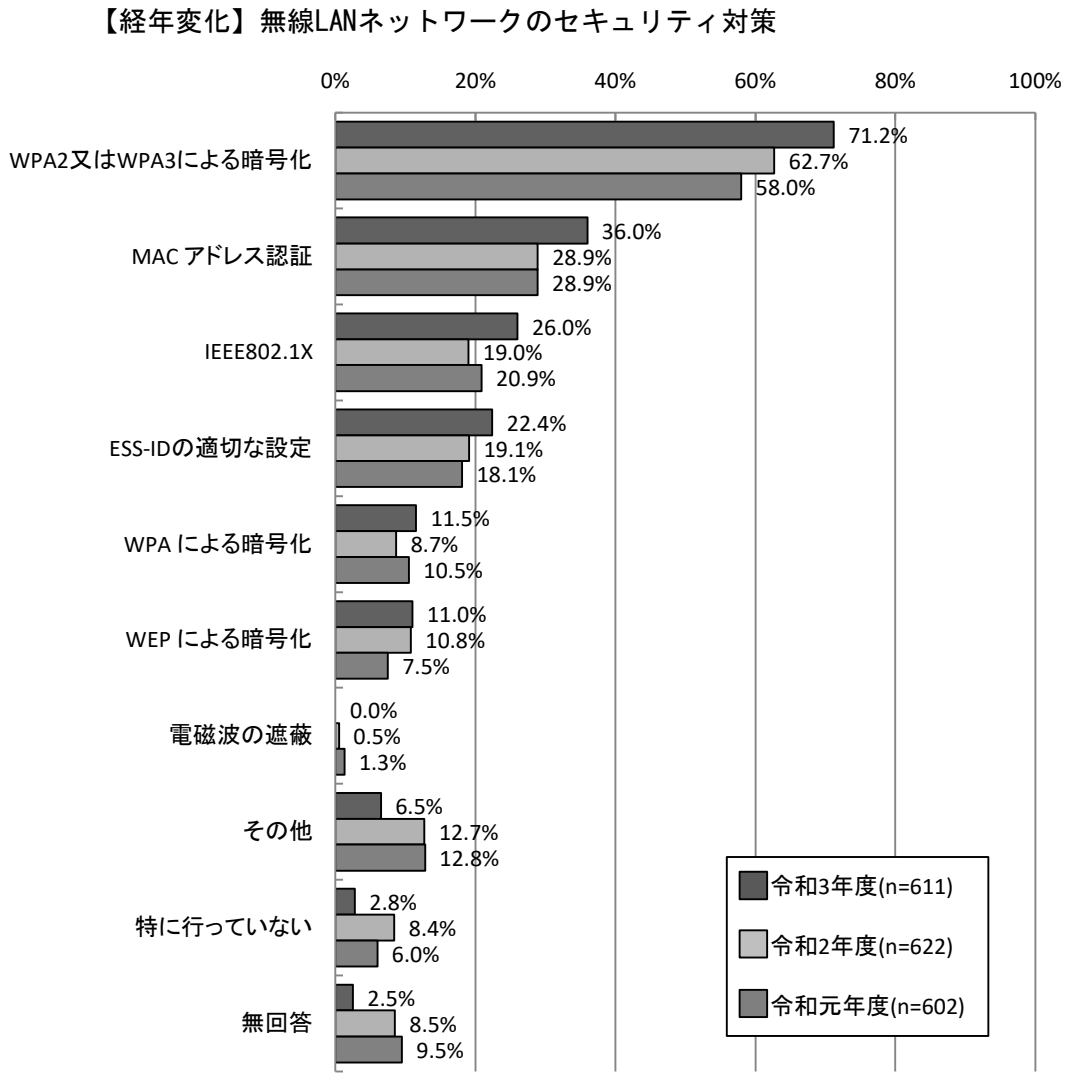
IEEE802.1X



ESS-IDの適切な設定



【経年変化】過去３年を比較すると、「WPA2又はWPA3による暗号化」が年々増加している傾向にある。

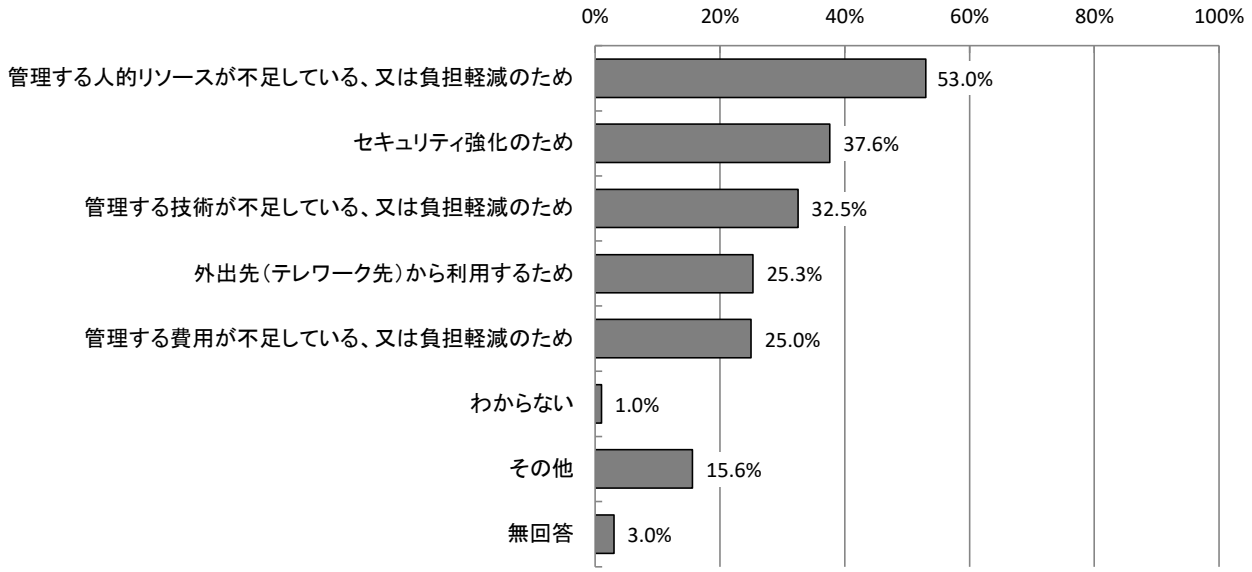


3.2.5　クラウドサービスを使用することになった理由　【問21】

クラウドサービスを使用することになった理由については、「管理する人的リソースが不足している、又は負担軽減のため」が53.0%で最も多く、次いで「セキュリティ強化のため」が37.6%となっている。

※本項目は、クラウドサービスを使用している社・団体等を対象としている。

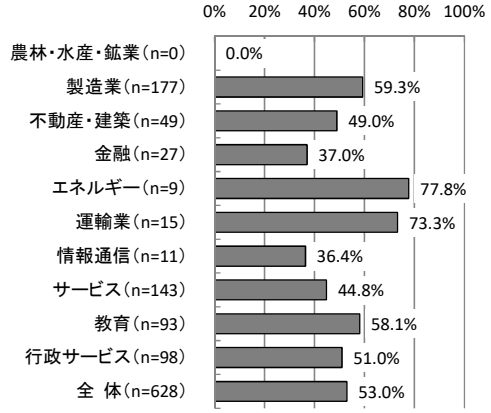
【全体】クラウドサービスを使用することになった理由（MA, n=628）



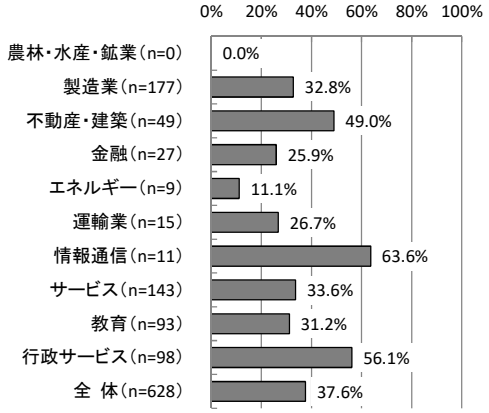
【業種別分析】業種別にみると、「管理する人的リソースが不足している、又は負担軽減のため」については、「エネルギー」が77.8%で最も多く、次いで「運輸業」が73.3%となっている。「セキュリティ強化のため」については、「情報通信」が63.6%で最も多くなっている。

【業種別分析】クラウドサービスを使用することになった理由

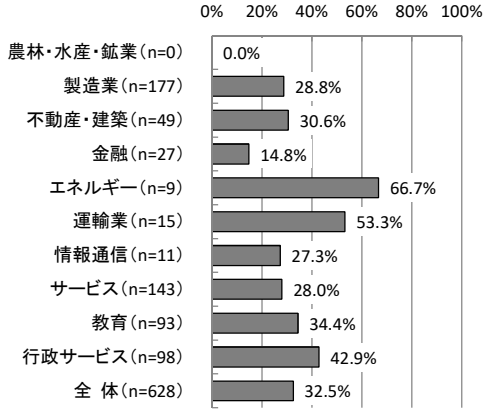
管理する人的リソースが不足している、又は負担軽減のため



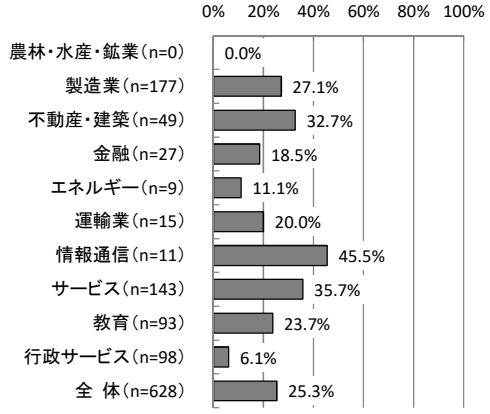
セキュリティ強化のため



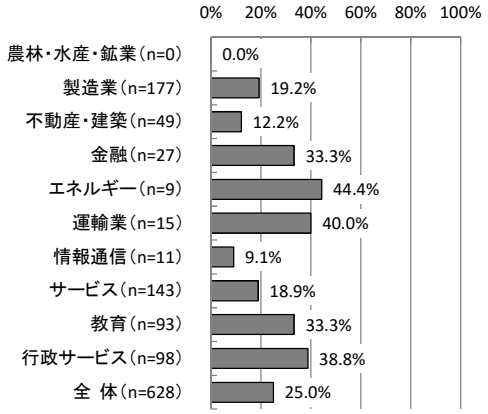
管理する技術が不足している、又は負担軽減のため



外出先（テレワーク先）から利用するため



管理する費用が不足している、又は負担軽減のため

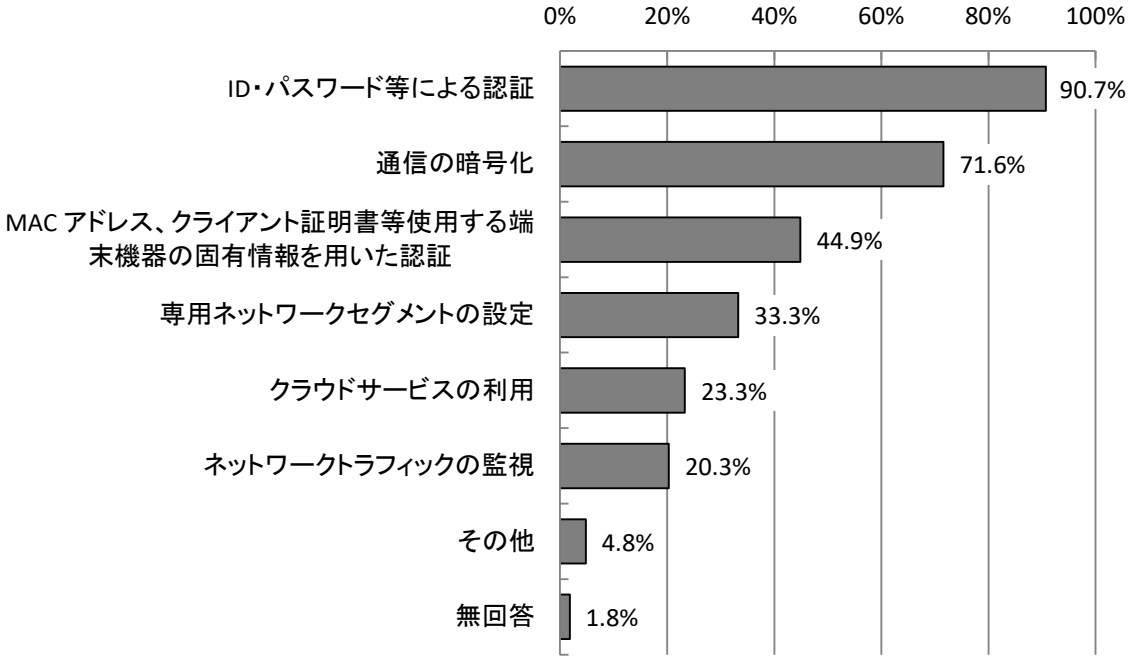


3.2.6　外部からの接続に対するセキュリティ対策　（通信路に対する対策）　【問22-A】

外部からの接続に対するセキュリティ対策（通信路に対する対策）については、「ID・パスワード等による認証」が90.7%で最も多く、次いで「通信の暗号化」が71.6%、「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44.9%となっている。

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

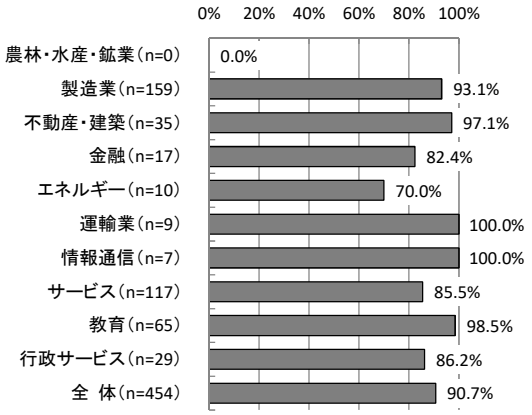
【全体】外部からの接続に対するセキュリティ対策（通信路に対する対策）（MA, n=454）



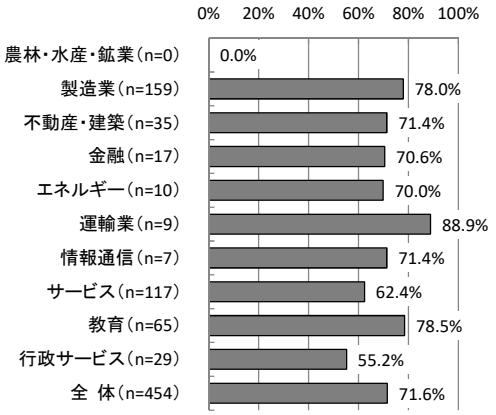
【業種別分析】業種別にみると、「ID・パスワード等による認証」では「運輸業」「情報通信」がそれぞれ100.0%と最も多く、「通信の暗号化」では「運輸業」が88.9%と最も多くなっている。

【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）

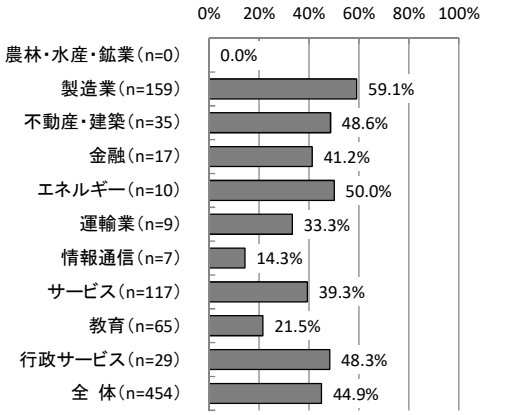
ID・パスワード等による認証



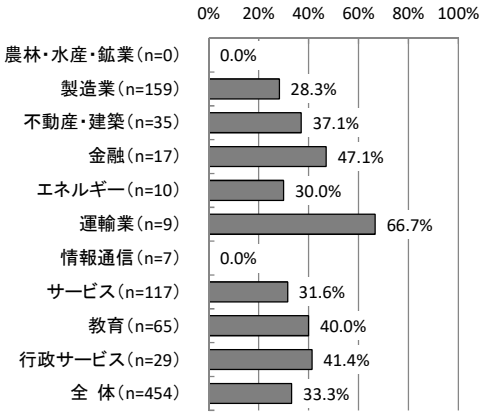
通信の暗号化



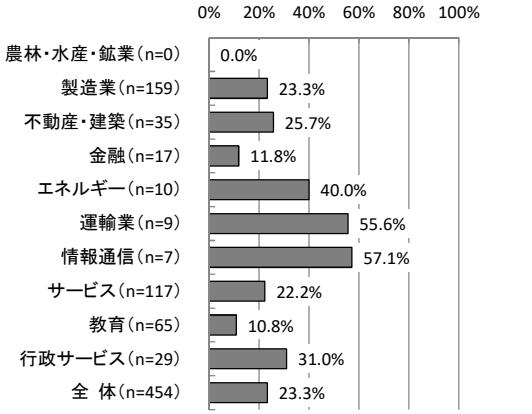
MAC アドレス、クライアント証明書等使用する端末機器の固有情報を用いた認証



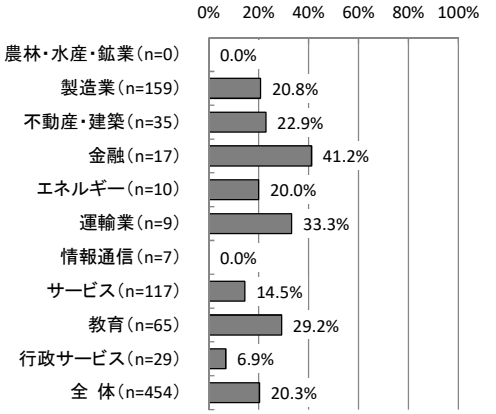
専用ネットワークセグメントの設定



クラウドサービスの利用



ネットワークトラフィックの監視

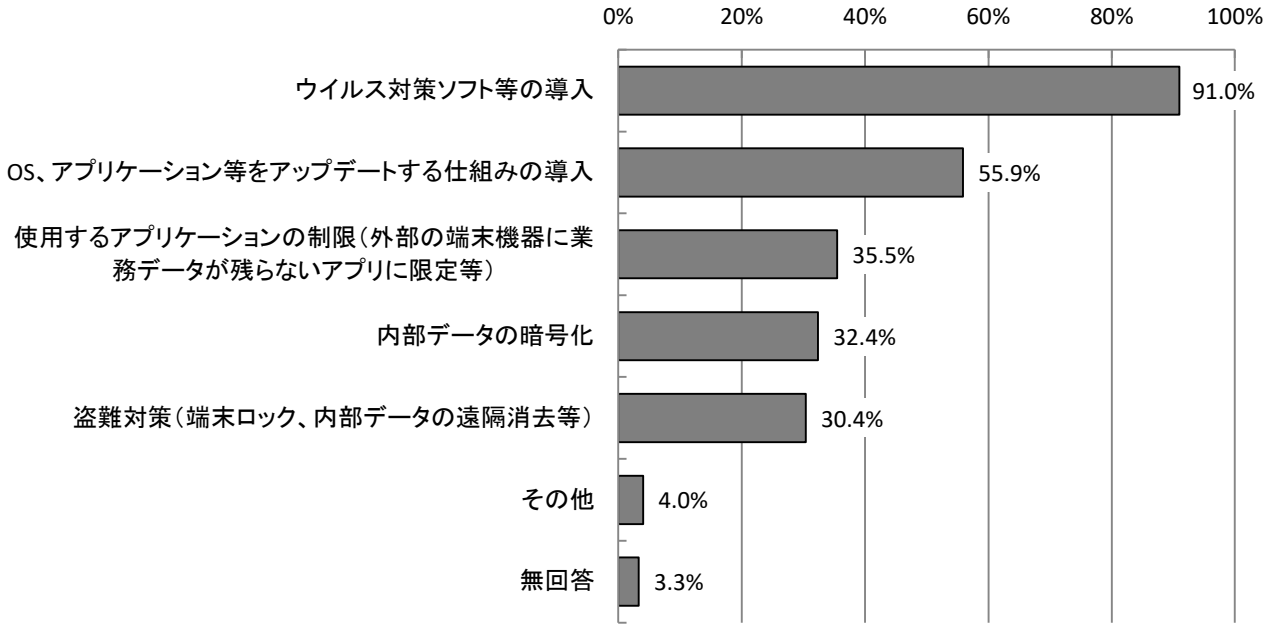


3.2.7　外部からの接続に対するセキュリティ対策　（端末に対する対策）　【問22-B】

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91.0%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55.9%、「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）」が35.5%となっている。

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

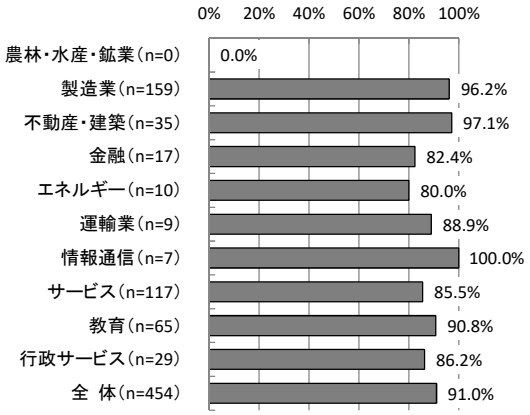
【全体】外部からの接続に対するセキュリティ対策（端末に対する対策）（MA, n=454）



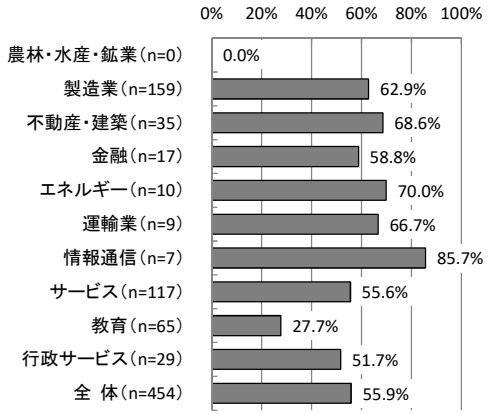
【業種別分析】業種別にみると、「ウイルス対策ソフト等の導入」「OS、アプリケーション等をアップデートする仕組みの導入」では「情報通信」がそれぞれ100.0%、85.7%で最も多く、「使用するアプリケーションの制限（外部の端末機器に業務データが残らないアプリに限定等）」及び「内部データの暗号化」では「エネルギー」がそれぞれ70.0%と最も多くなっている。

【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）

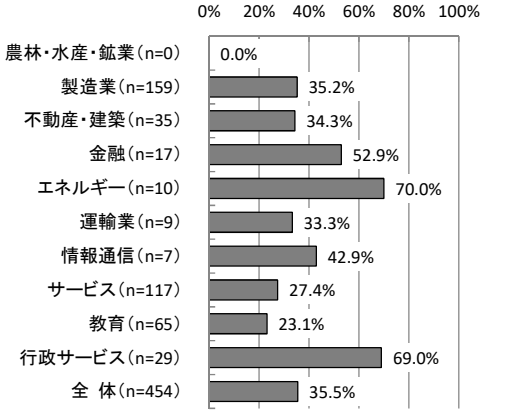
ウイルス対策ソフト等の導入



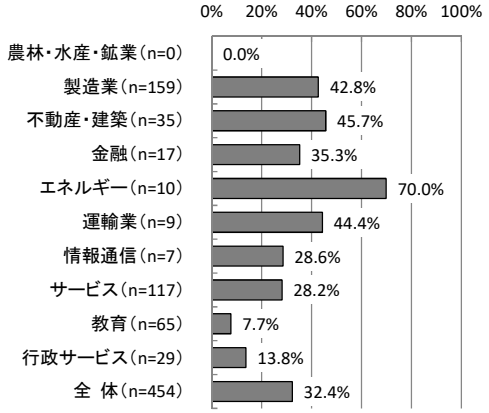
OS、アプリケーション等をアップデートする仕組みの導入



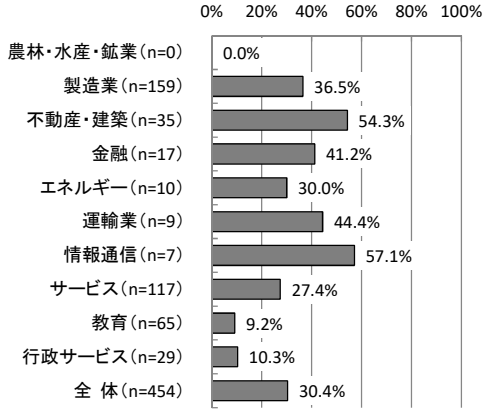
使用するアプリケーションの制限（外部の端末機器に業務データが残らないアプリに限定等）



内部データの暗号化



盗難対策（端末ロック、内部データの遠隔消去等）

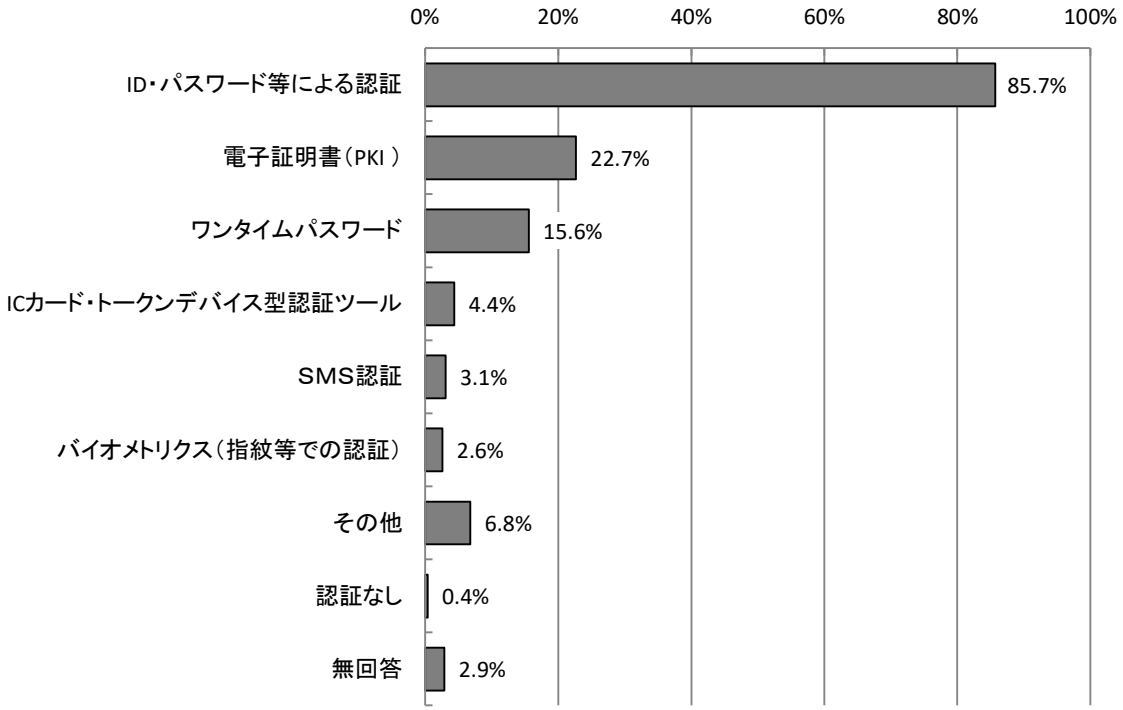


3.2.8　社外等からのインターネット接続経由の認証方法　【問23】

社外等からのインターネット接続経由の認証方法については、「ID・パスワード等による認証」が85.7%で最も多く、次いで「電子証明書（PKI）」が22.7%となっている。一方、「認証なし」は0.4%となっている。

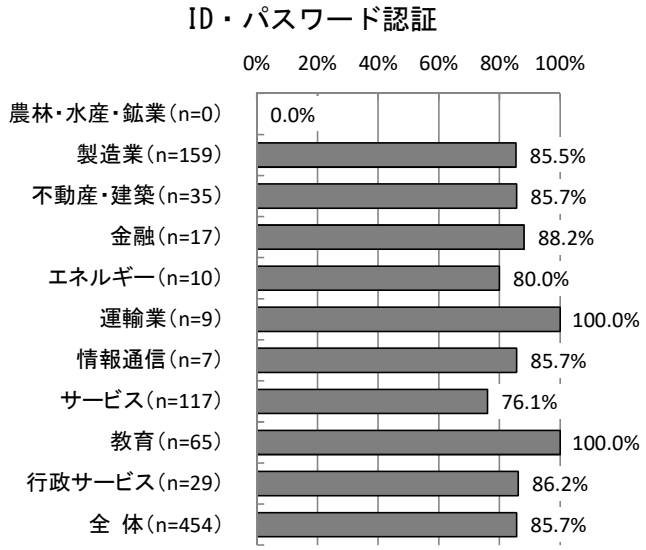
※本項目は、外部から内部ネットワークへの接続を許可している社・団体等を対象としている。

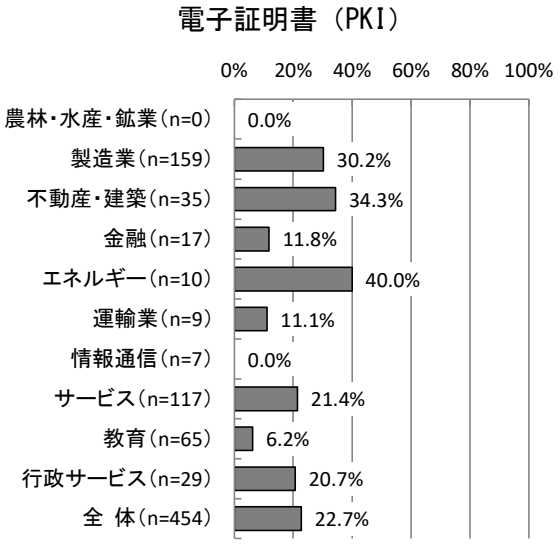
【全体】社外等からのインターネット接続経由の認証方法（MA, n=454）



【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、「運輸業」「教育」が100.0%で最も多くなっている。

【業種別分析】社外等からのインターネット接続経由の認証方法



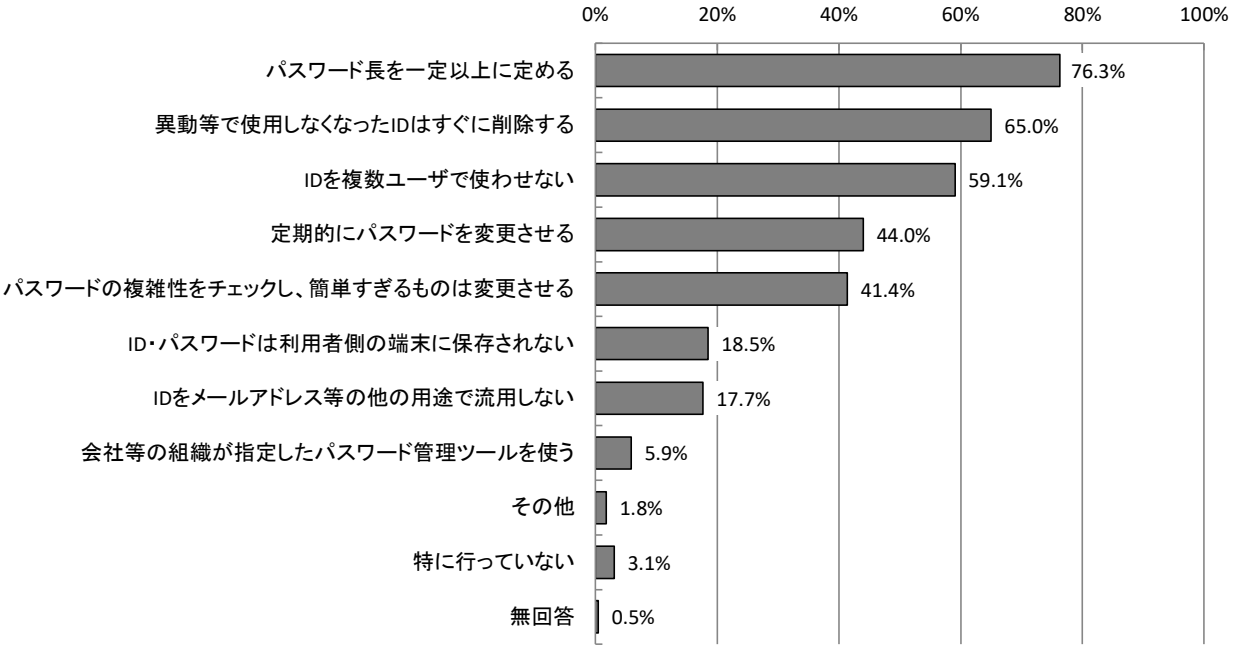


3.2.9　ID・パスワードの管理方法　【問23-1】

ID・パスワードの管理方法については、「パスワード長を一定以上に定める」が76.3%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65.0%となっている。

※本項目は、社外等からのインターネット接続を行う際に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。

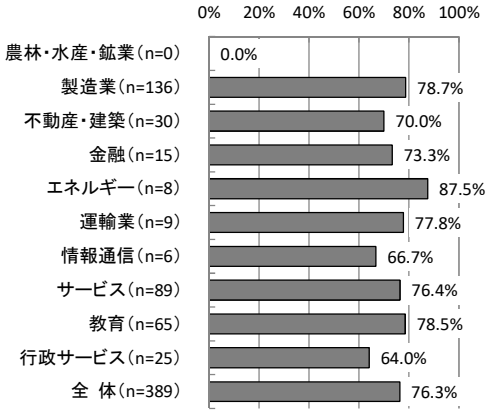
【全体】ID・パスワードの管理方法（MA,n=389）



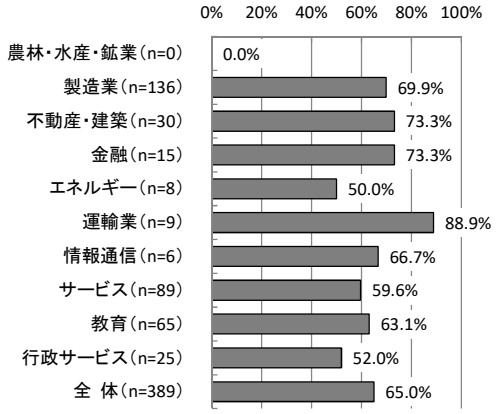
【業種別分析】業種別にみると、「パスワード長を一定以上に定める」については、「エネルギー」が87.5%で最も多く、次いで「製造業」が78.7%となっている。「異動等で使用しなくなったIDはすぐに削除する」については、「運輸業」が88.9%で最も多くなっている。

【業種別分析】ID・パスワードの管理方法

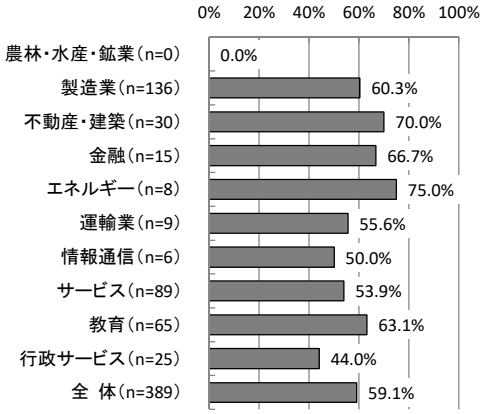
パスワード長を一定以上に定める



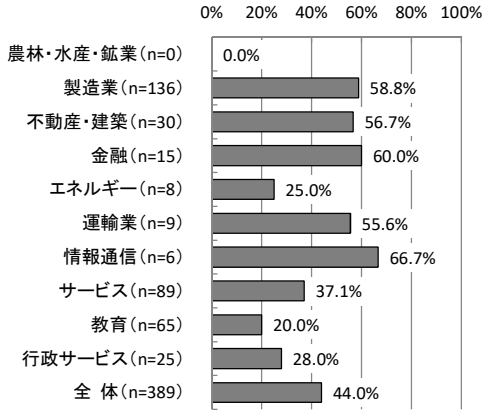
異動等で使用しなくなったIDはすぐに削除する



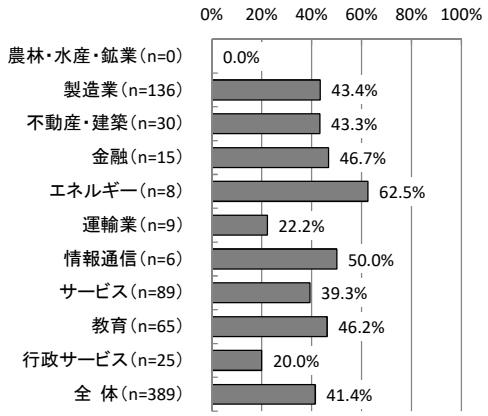
IDを複数ユーザーで使わせない



定期的にパスワードを変更させる



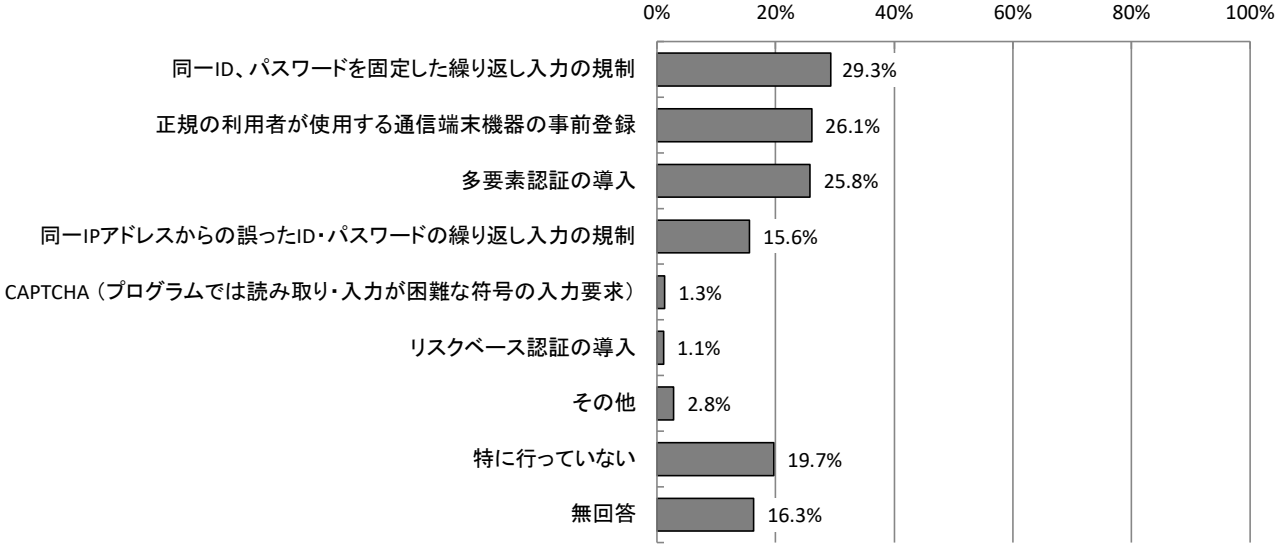
パスワードの複雑性をチェックし、簡単すぎるものは変更させる



3.2.10　不正ログイン対策　【問23-2】

不正ログイン対策については、「同一ID、パスワードを固定した繰り返し入力の規制」が29.3%で最も多く、次いで「正規の利用者が使用する通信端末機器の事前登録」が26.1%、「多要素認証の導入」が25.8%となっている。一方、「特に行っていない」は19.7%となっている。

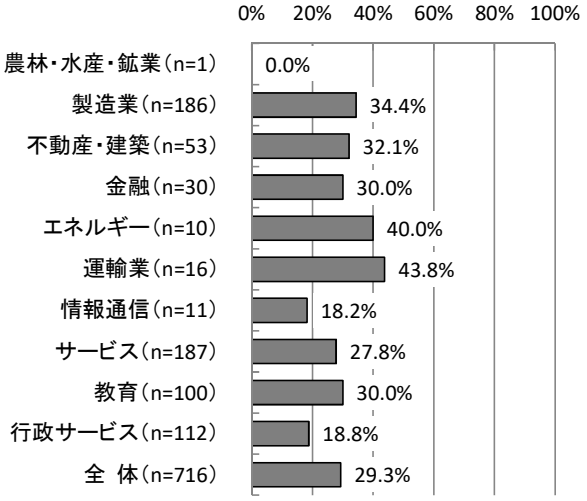
【全体】不正ログイン対策（MA, n=716）



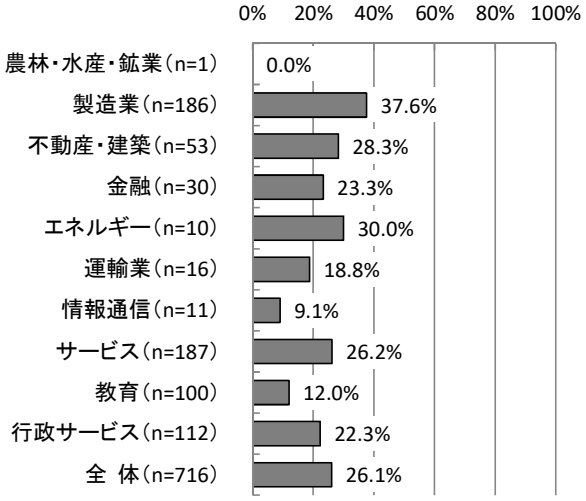
【業種別分析】業種別にみると、「同一ID、パスワードを固定した繰り返し入力の規制」については、「運輸業」が43.8%と最も多く、次いで「エネルギー」が40.0%となっている。「正規の利用者が使用する通信端末機器の事前登録」については、「製造業」が37.6%で最も多く、次いで「エネルギー」が30.0%となっている。

【業種別分析】不正ログイン対策

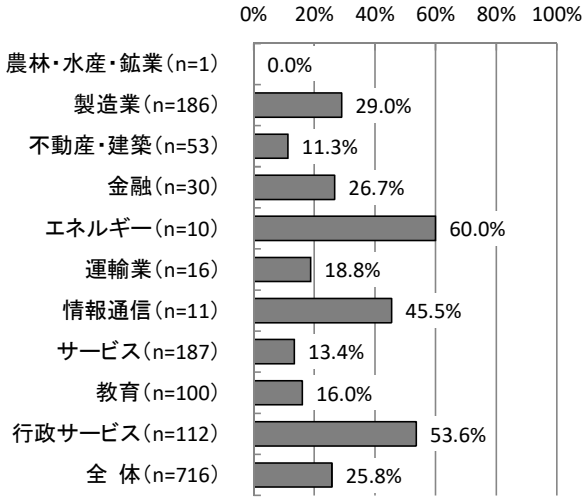
同一ID、パスワードを固定した繰り返し入力の規制



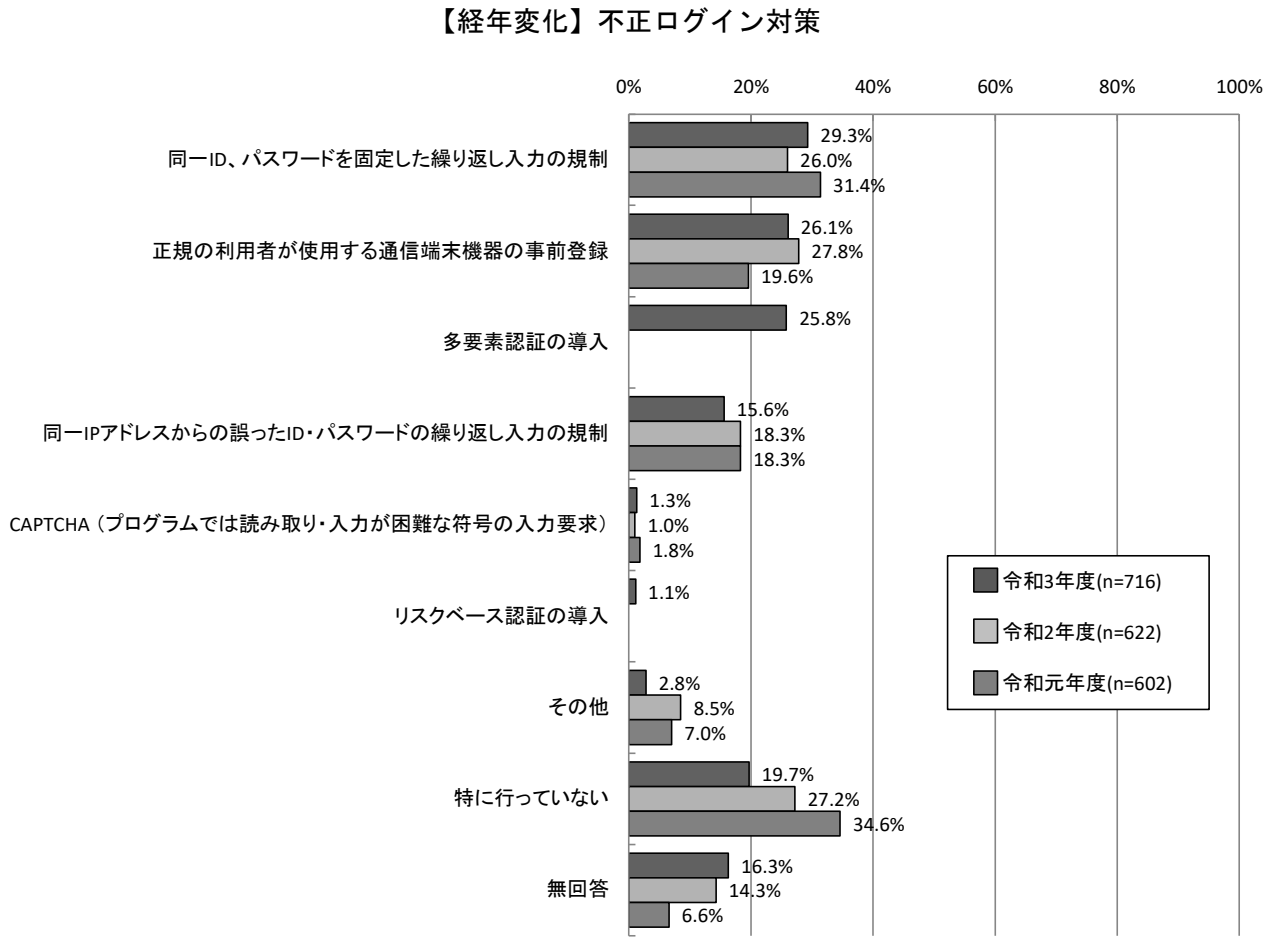
正規の利用者が使用する通信端末機器の事前登録



多要素認証の導入



【経年変化】３年間を比較したところ、行っている対策に大きな変化は見られないが、対策を「特に行っていない」とする社・団体等が減少傾向にある。

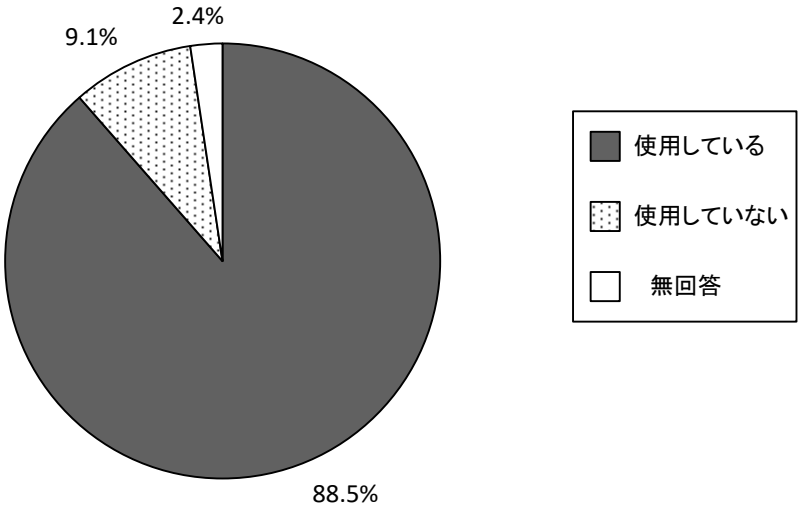


※令和３年度調査で「多要素認証の導入」「リスクベース認証の導入」を新設

3.2.11　各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）の利用状況【問24】

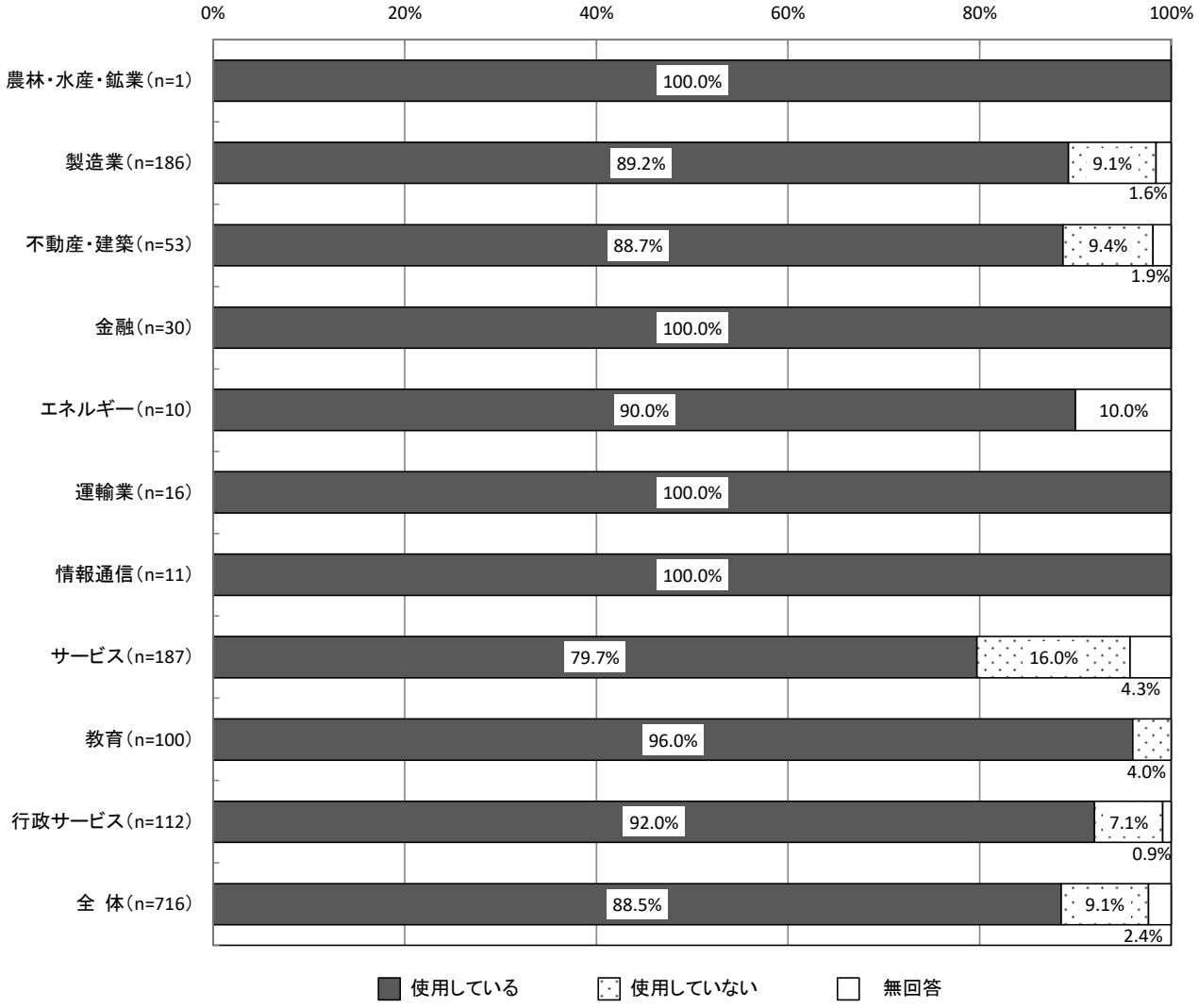
各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）の利用状況については、「使用している」が88.5%、「使用していない」が9.1%となっている。

【全体】各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）の利用状況（SA,n=716）



【業種別分析】業種別にみると、各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）を「使用している」については、「金融」「運輸業」「情報通信」がそれぞれ100.0％と最も多くなっている。「使用していない」については、「サービス」が16.0％で最も多くなっている。

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

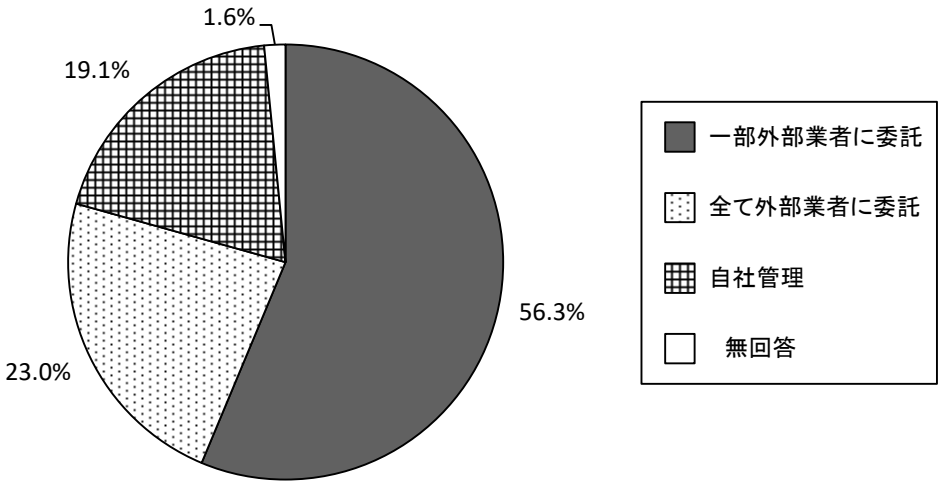


3.2.12　各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）の管理環境【問24-1】

各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）の管理環境については、「一部外部業者に委託」が56.3％で最も多く、次いで「全て外部業者に委託」が23.0％、「自社管理」が19.1％となっている。

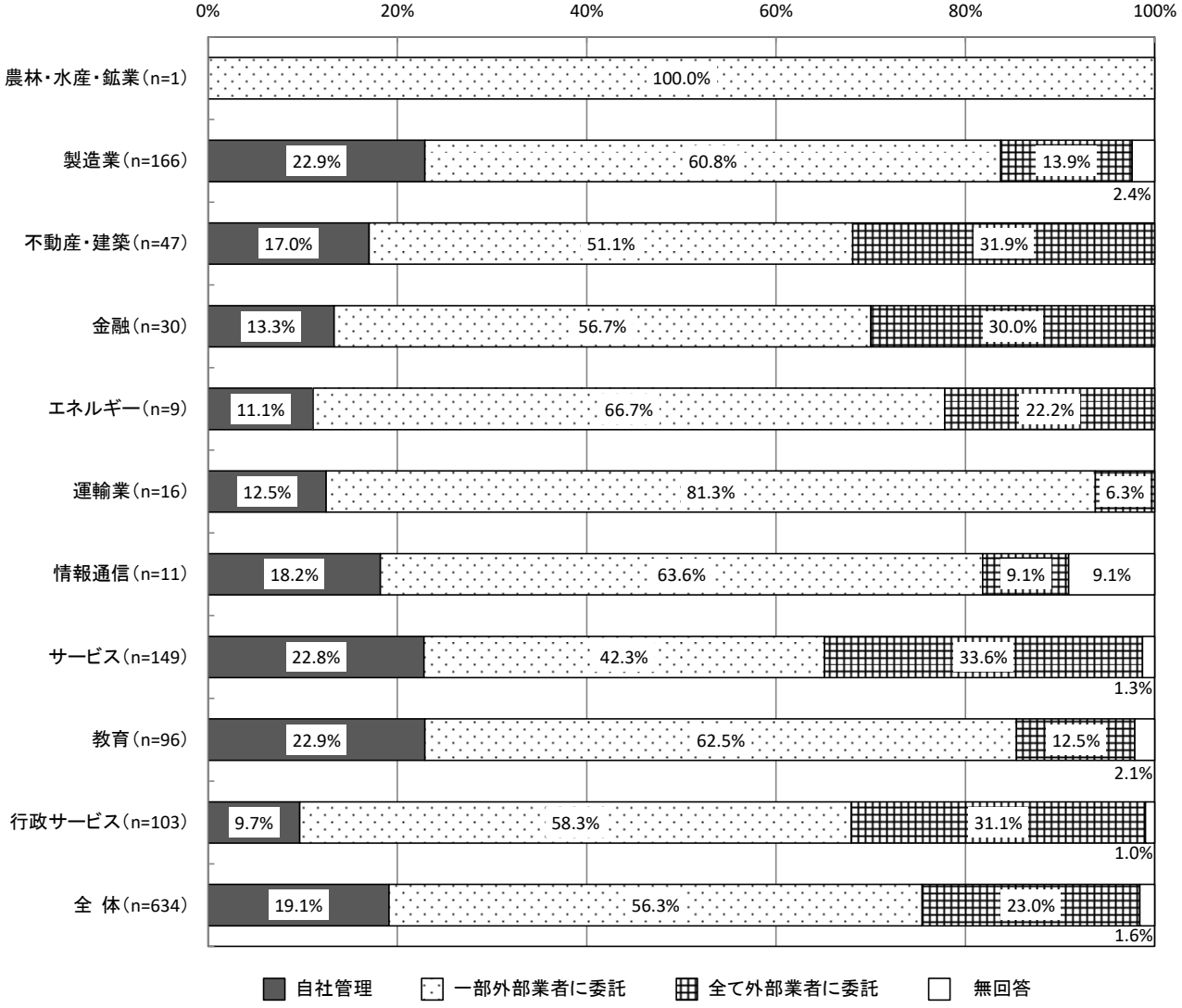
※本項目は、各種サービス（Webサイト、メール管理、ファイル管理等）を使用している社・団体等を対象としている。

【全体】各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）の管理環境（SA,n=634）



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

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

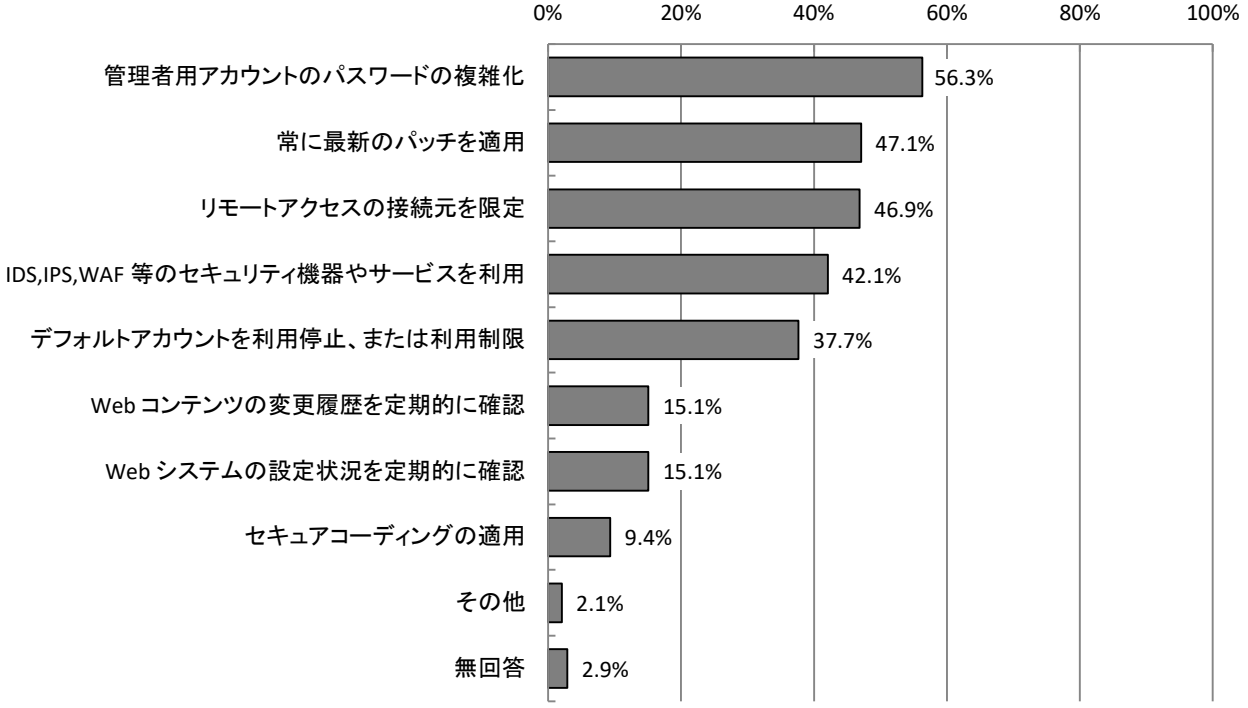


3.2.13　各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）のセキュリティ対策【問24-2】

各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）のセキュリティ対策については、「管理者用アカウントのパスワードの複雑化」が56.3％で最も多く、次いで「常に最新のパッチを適用」が47.1％、「リモートアクセスの接続元を限定」が46.9％となっている。

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

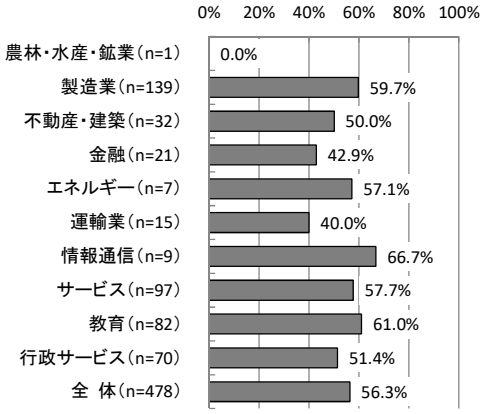
【全体】各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）のセキュリティ対策（MA,n=478）



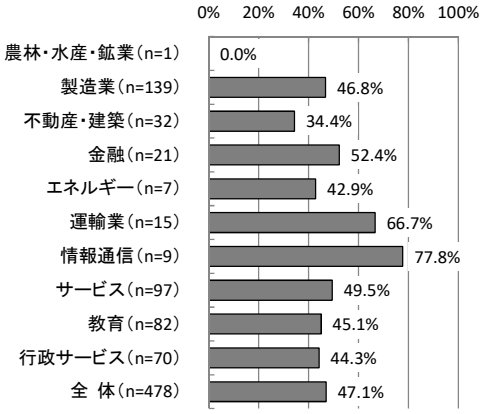
【業種別分析】業種別に見ると、「管理者用アカウントのパスワードの複雑化」については、「情報通信」が66.7%と最も多く、次いで「教育」が61.0%となっている。「常に最新のパッチを適用」については、「情報通信」が77.8%と最も多く、次いで「運輸業」が66.7%となっている。

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

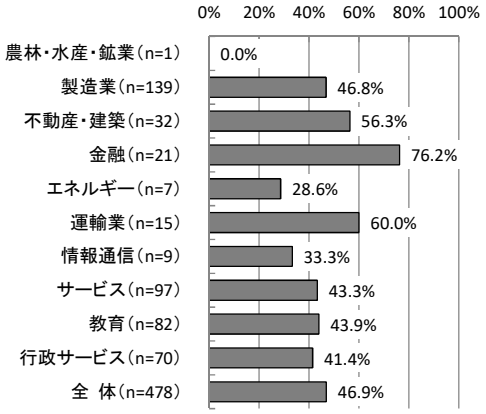
管理者用アカウントのパスワードの複雑化



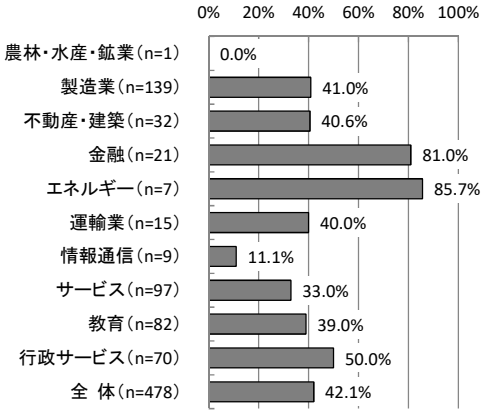
常に最新のパッチを適用



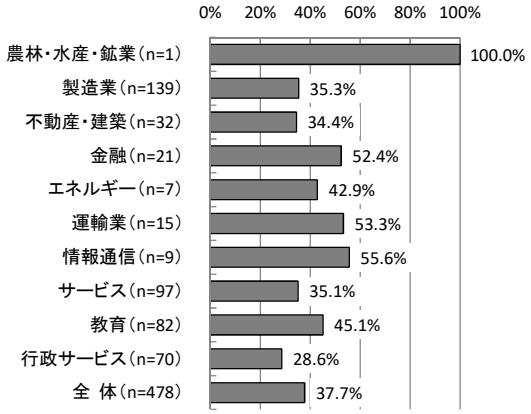
リモートアクセスの接続元を限定



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

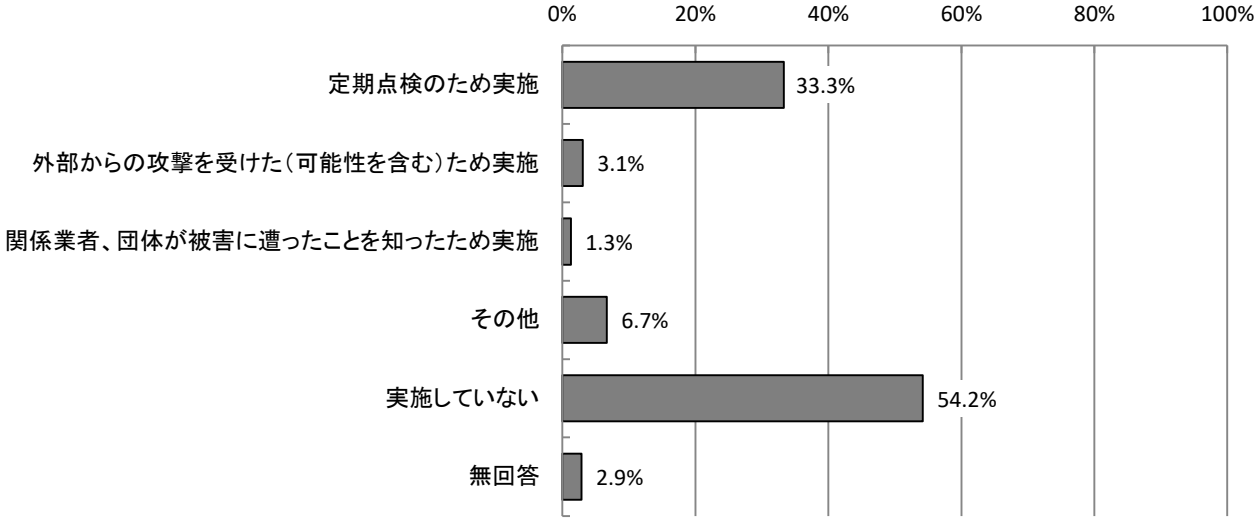


3.2.14　ぜい弱性調査（ペネトレーションテスト）実施の有無　【問24-3】

ぜい弱性調査（ペネトレーションテスト）実施の有無については、「実施していない」が54.2%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33.3%と多くなっている。

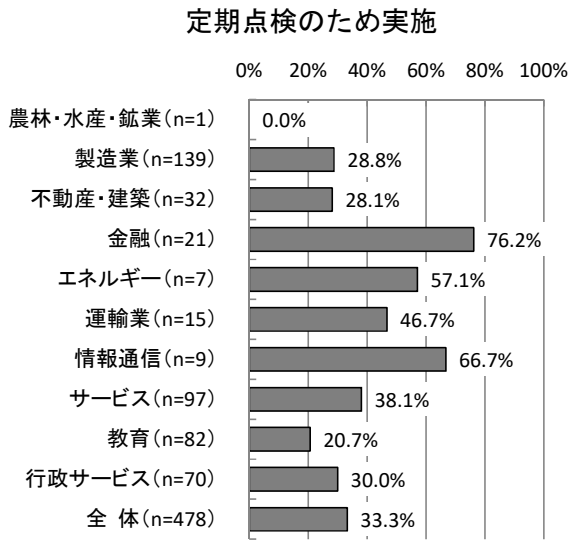
※本項目は、各種サービスの全部又は一部を自社で管理している社・団体等を対象としている。

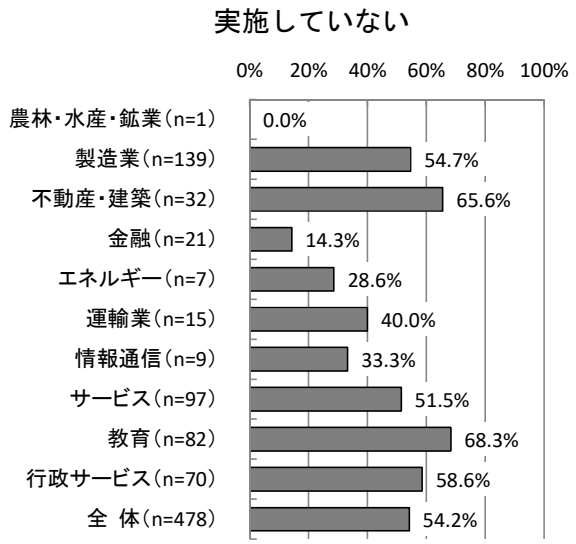
【全体】ぜい弱性調査（ペネトレーションテスト）実施の有無（MA, n=478）



【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76.2%で最も多く、次いで「情報通信」が66.7%となっている。一方、「実施していない」については、「教育」が68.3%で最も多く、次いで「不動産・建築」が65.6%となっている。

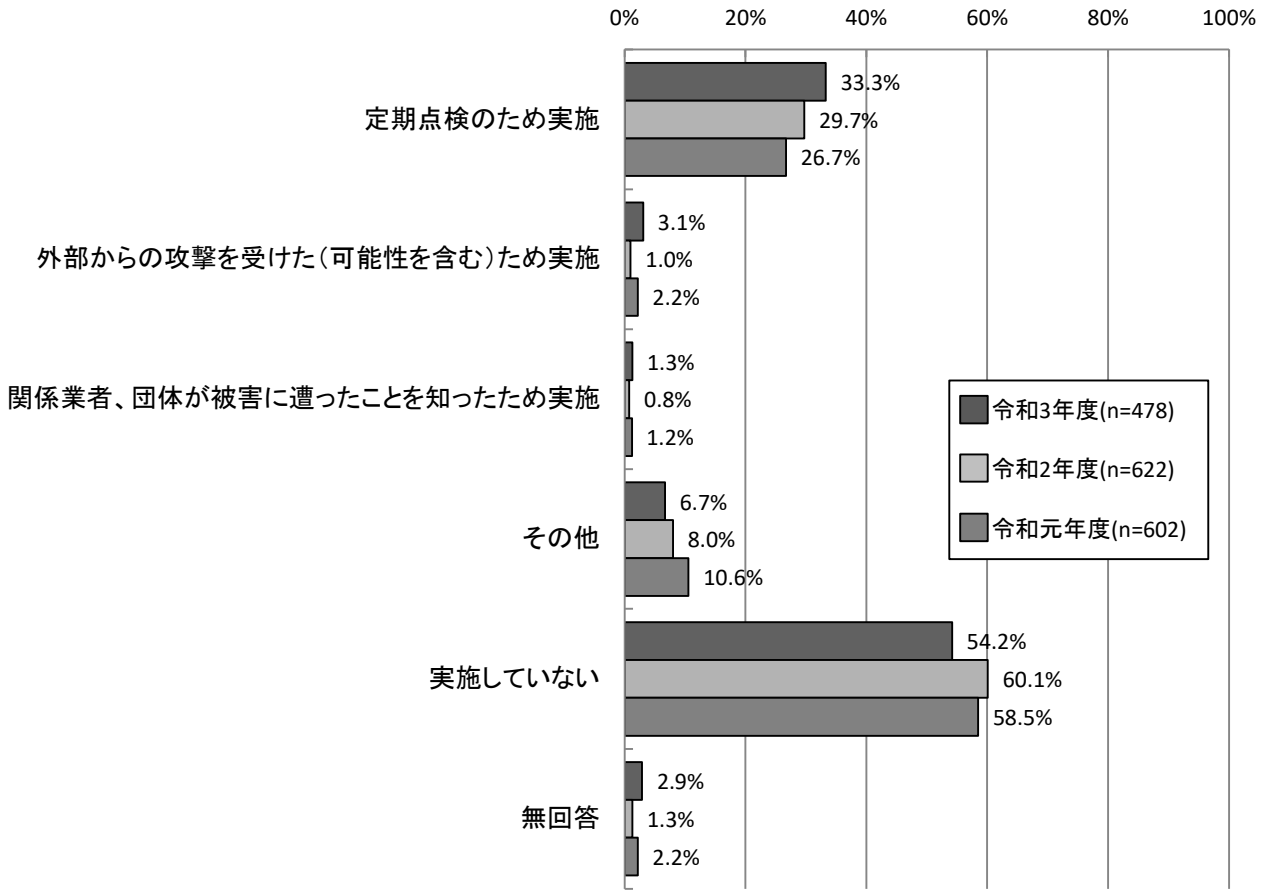
【業種別分析】ぜい弱性調査（ペネトレーションテスト）実施の有無





【経年変化】昨年度と比較すると、「定期点検のための実施」が 3.6 ポイント増加し、「実施していない」は 5.9 ポイント減少している。

【経年変化】ぜい弱性調査（ペネトレーションテスト）実施の有無

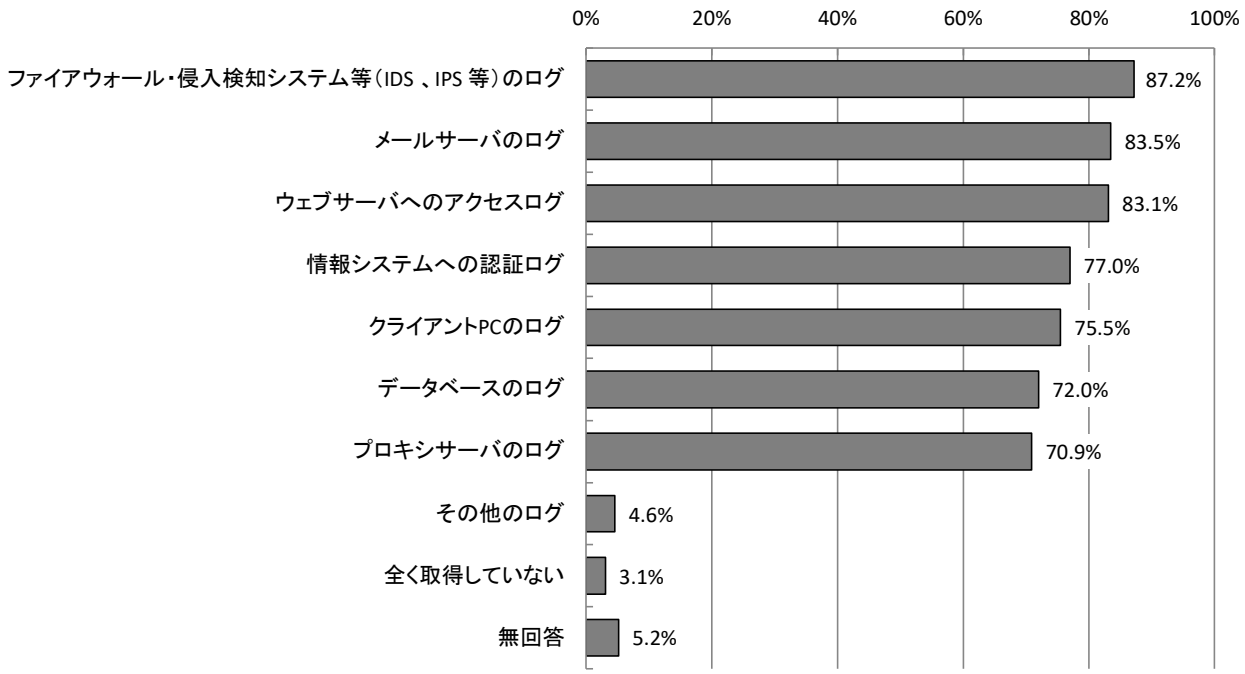


3.2.15　ログの取得状況　【問24-4】

ログの取得状況については、「ファイアウォール・侵入検知システム等（IDS、IPS等）のログ」が87.2%で最も多く、次いで「メールサーバのログ」が83.5%、「ウェブサーバへのアクセスログ」が83.1%、「情報システムへの認証ログ」が77.0%となっている。

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

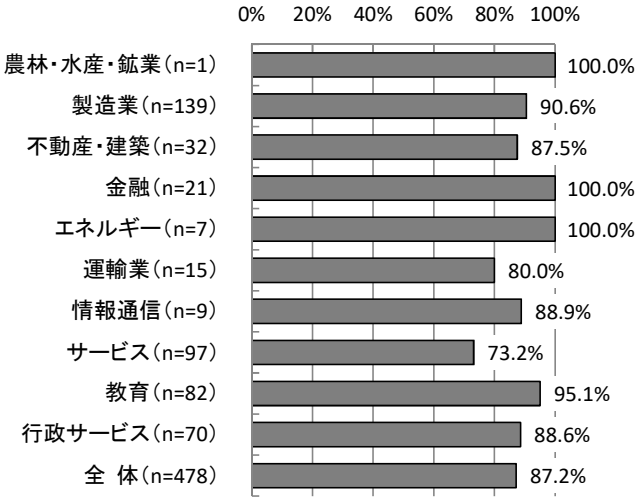
【全体】ログの取得状況（MA, n=478）



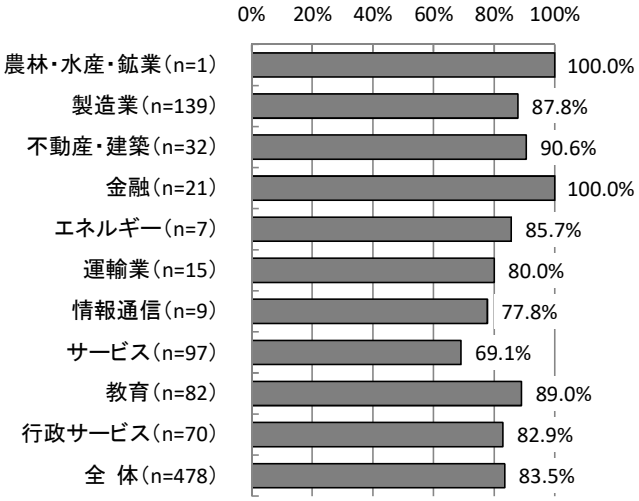
【業種別分析】業種別にみると、「ファイアウォール・侵入検知システム等（IDS、IPS等）のログ」では、「金融」「エネルギー」、「メールサーバのログ」「ウェブサーバへのアクセスログ」では「金融」、「情報システムへの認証ログ」では「情報通信」がそれぞれ100.0%で最も多くなっている。

【業種別分析】ログの取得状況

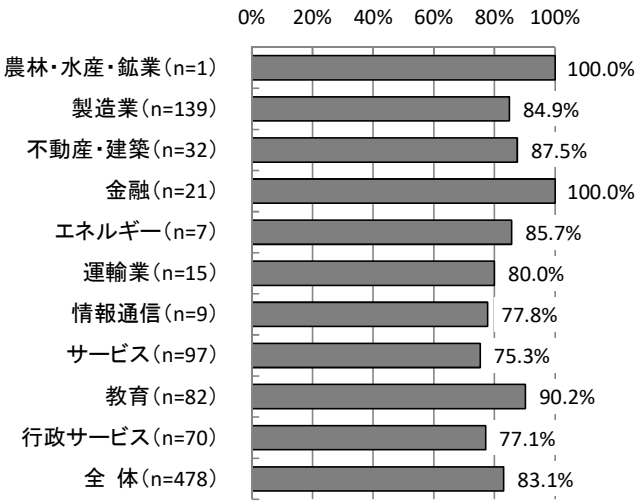
ファイアウォール・侵入検知システム等（IDS 、IPS 等）のログ



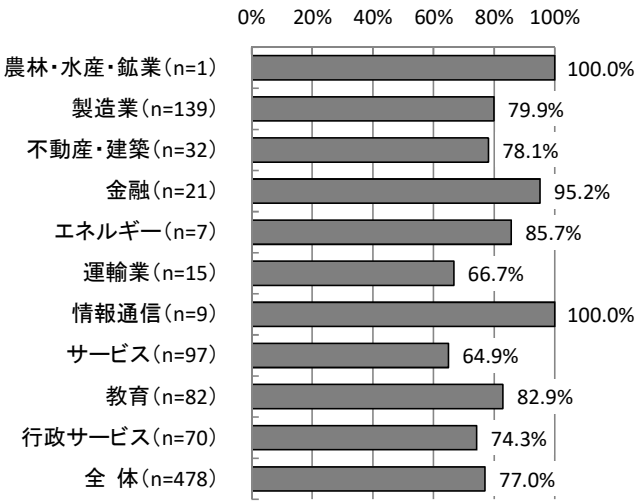
メールサーバのログ



ウェブサーバへのアクセスログ



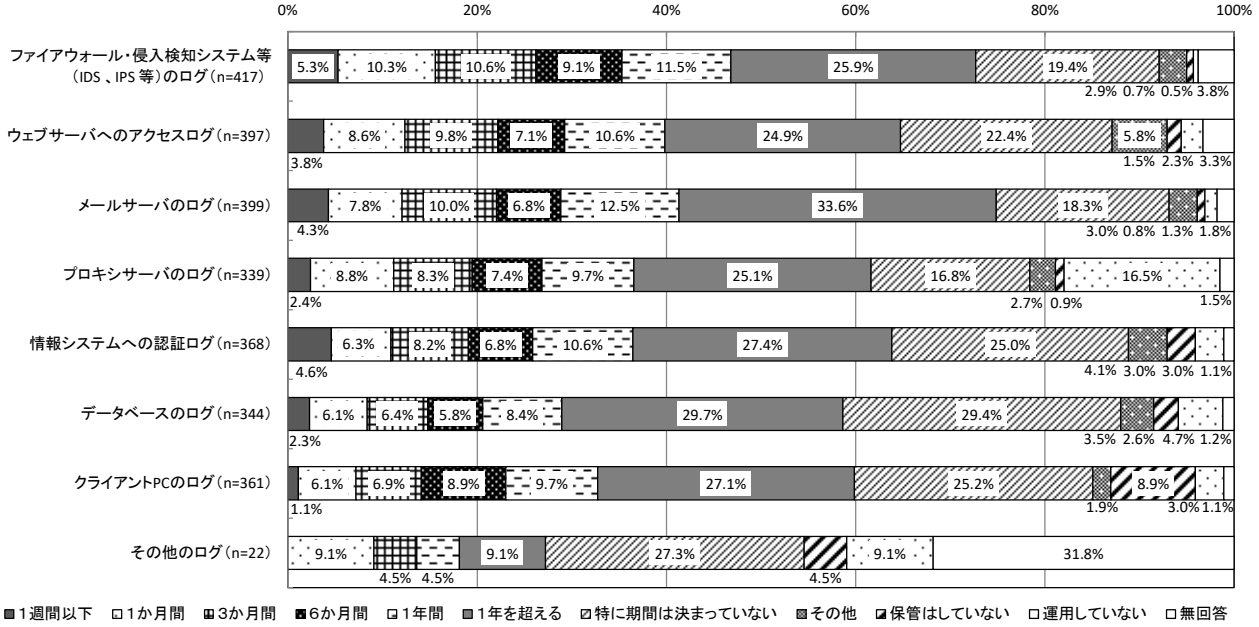
情報システムへの認証ログ



3.2.16　ログの保管期間　【問24-4A】

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。

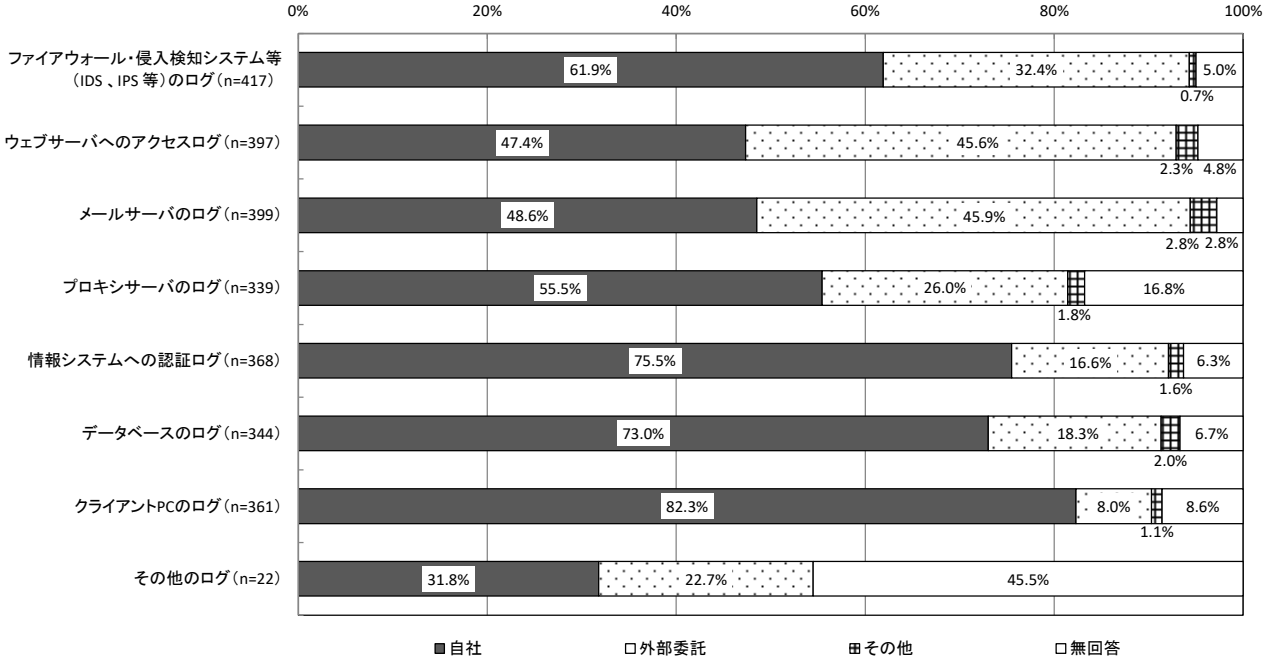
【全体】ログの保管期間



3.2.17　ログの保管方法　【問24-4B】

ログの保管方法については、すべてのログの種類で「自社」が最も多くなっている。

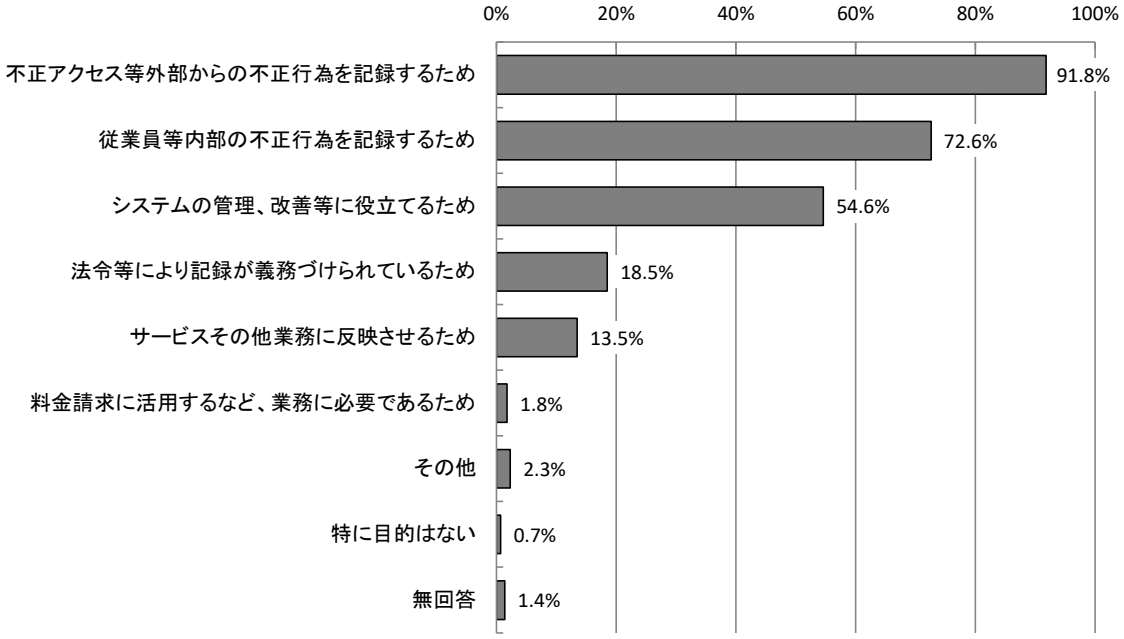
【全体】ログの保管方法



3.2.18　ログを取得・保管している理由　【問24-4-1】

ログを取得・保管している理由については、「不正アクセス等外部からの不正行為を記録するため」が91.8%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72.6%、「システムの管理、改善等に役立てるため」が54.6%となっている。

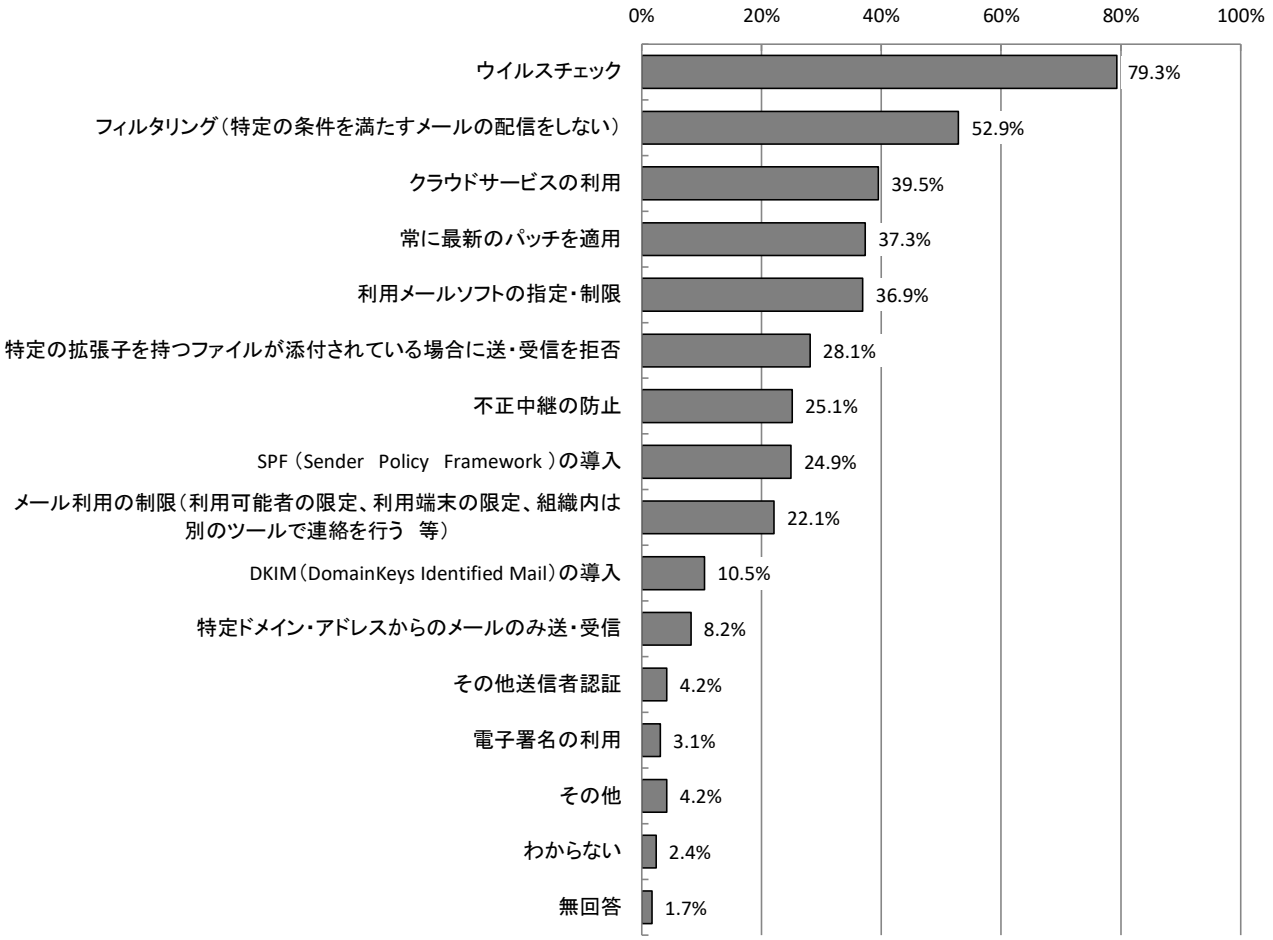
【全体】ログを取得・保管している理由（MA,n=438）



3.2.19　電子メールに関するセキュリティ対策　【問25】

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79.3%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%、「クラウドサービスの利用」が39.5%となっている。

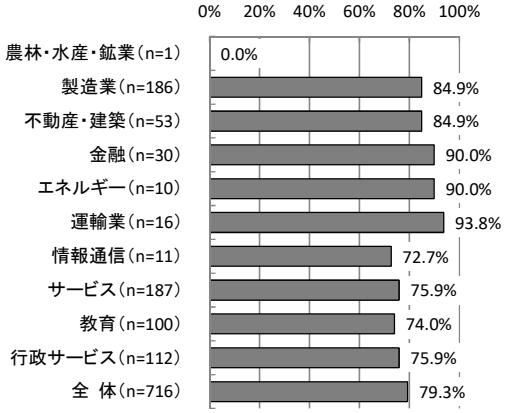
【全体】電子メールに関するセキュリティ対策（MA,n=716）



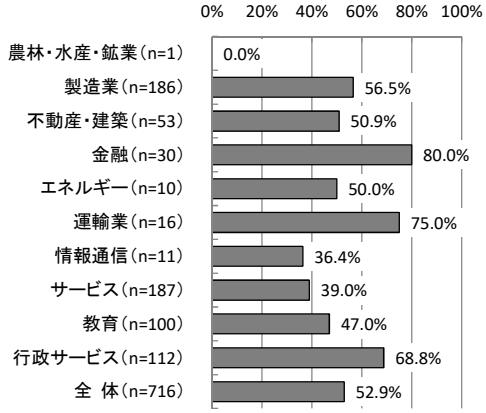
【業種別分析】業種別にみると、「ウイルスチェック」については、「運輸業」が93.8%で最も多く、次いで「金融」「エネルギー」がそれぞれ90.0%となっている。「フィルタリング」については「金融」が80.0%、「クラウドサービスの利用」については「運輸業」が56.3%と最も多くなっている。

【業種別分析】電子メールに関するセキュリティ対策

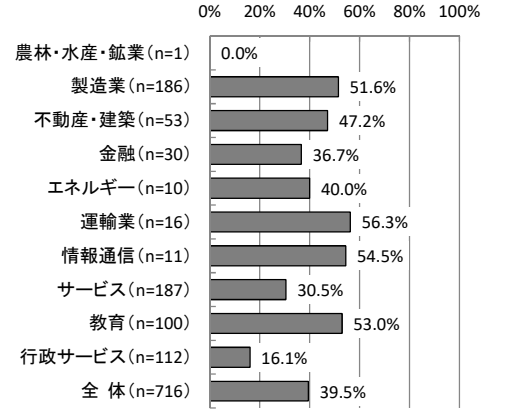
ウイルスチェック



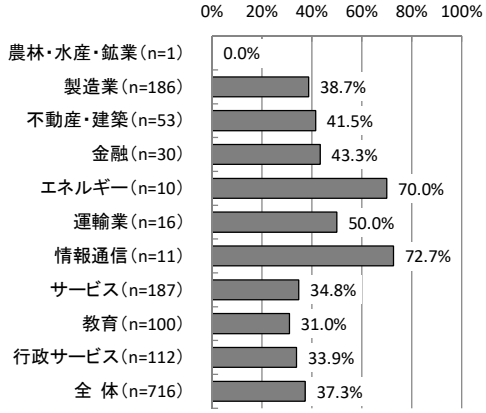
フィルタリング
（特定の条件を満たすメールの配信をしない）



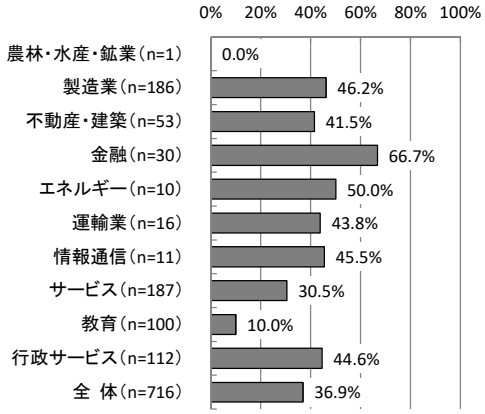
クラウドサービスの利用



常に最新のパッチを適用



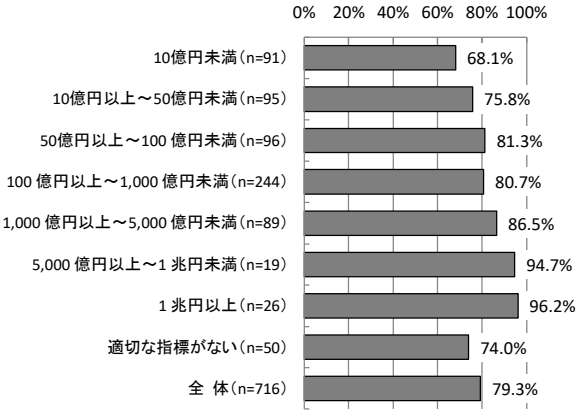
利用メールソフトの指定・制限



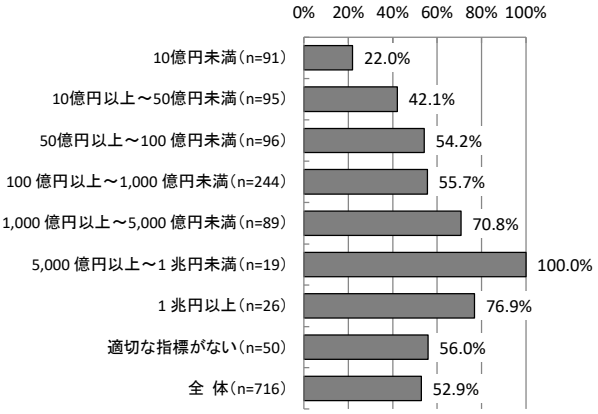
【売上・予算規模別分析】売上・予算規模別にみると、「ウイルスチェック」については、「１兆円以上」が96.2%で最も多く、次いで「5,000億円以上～１兆円未満」が94.7%となっている。「フィルタリング」については「5,000億円以上～１兆円未満」が100.0%で最も多く、次いで「１兆円以上」が76.9%となっている。

【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

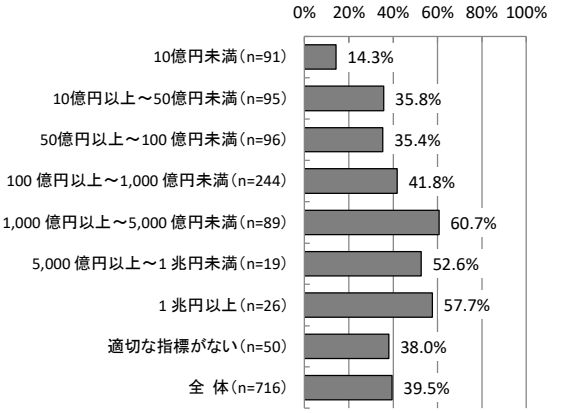
ウイルスチェック



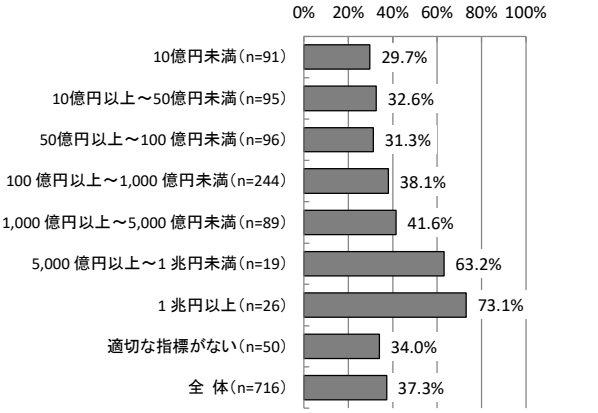
フィルタリング
（特定の条件を満たすメールの配信をしない）



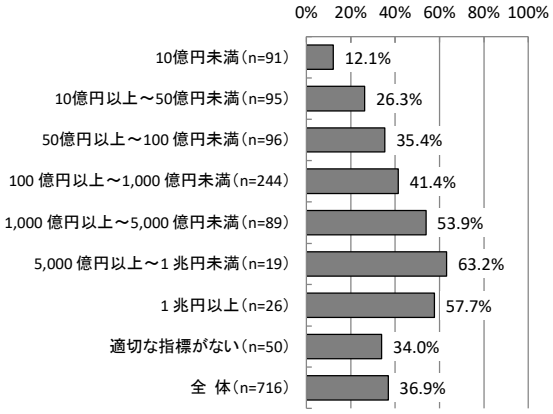
クラウドサービスの利用



常に最新のパッチを適用

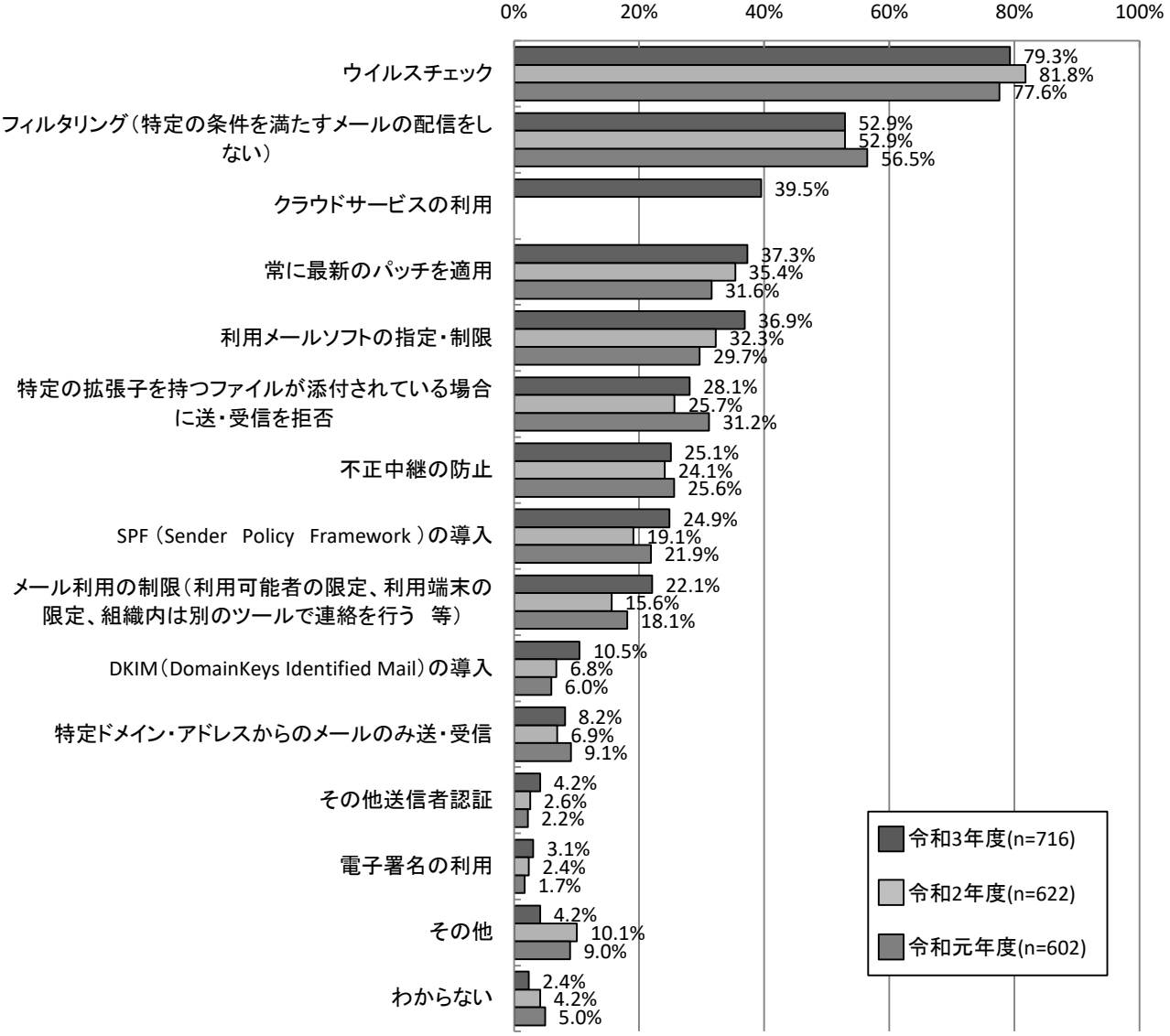


利用メールソフトの指定・制限



【経年変化】昨年度と比較すると、「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）」が6.5ポイント、「SPF（Sender Policy Framework ）の導入」が5.8ポイント増加し、「ウイルスチェック」が2.5ポイント減少している。

【経年変化】電子メールに関するセキュリティ対策

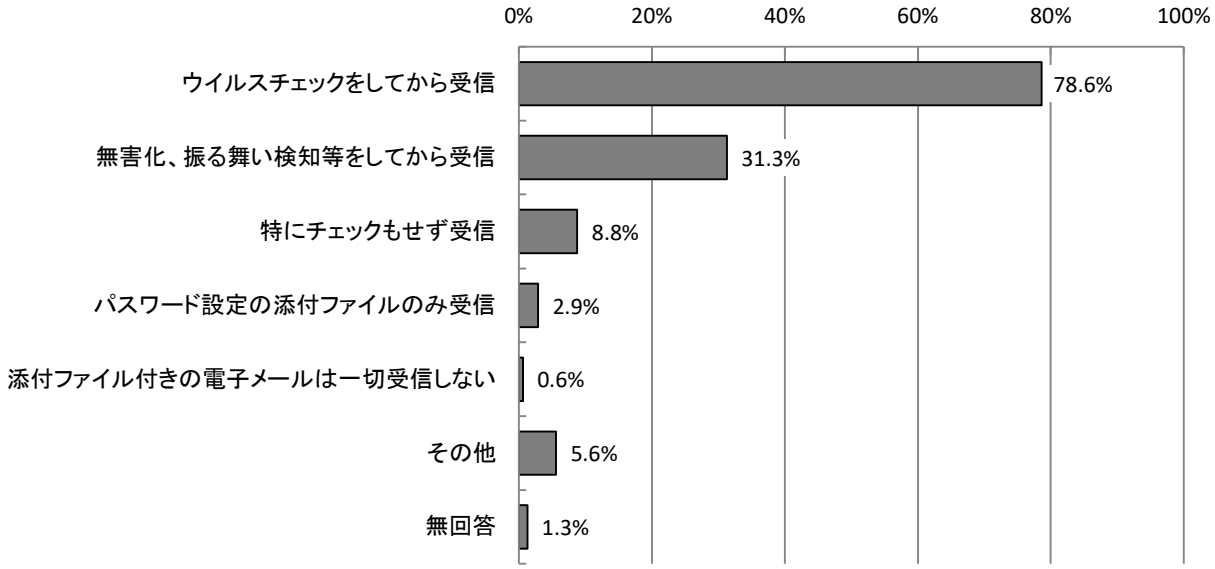


※令和３年度調査で、「クラウドサービスの利用」を新設。

3.2.20　添付ファイルの取り扱い　【問26】

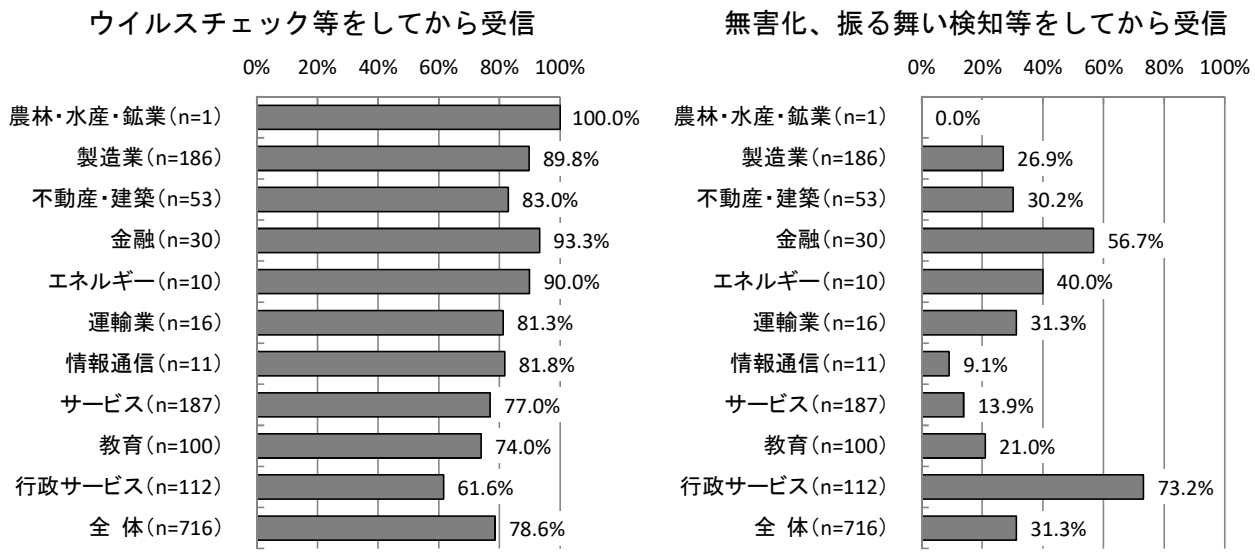
添付ファイルの取り扱いについては、「ウイルスチェックをしてから受信」が78.6%で最も多い。一方、「特にチェックもせずに受信」は8.8%であった。

【全体】添付ファイルの取り扱い（MA, n=716）



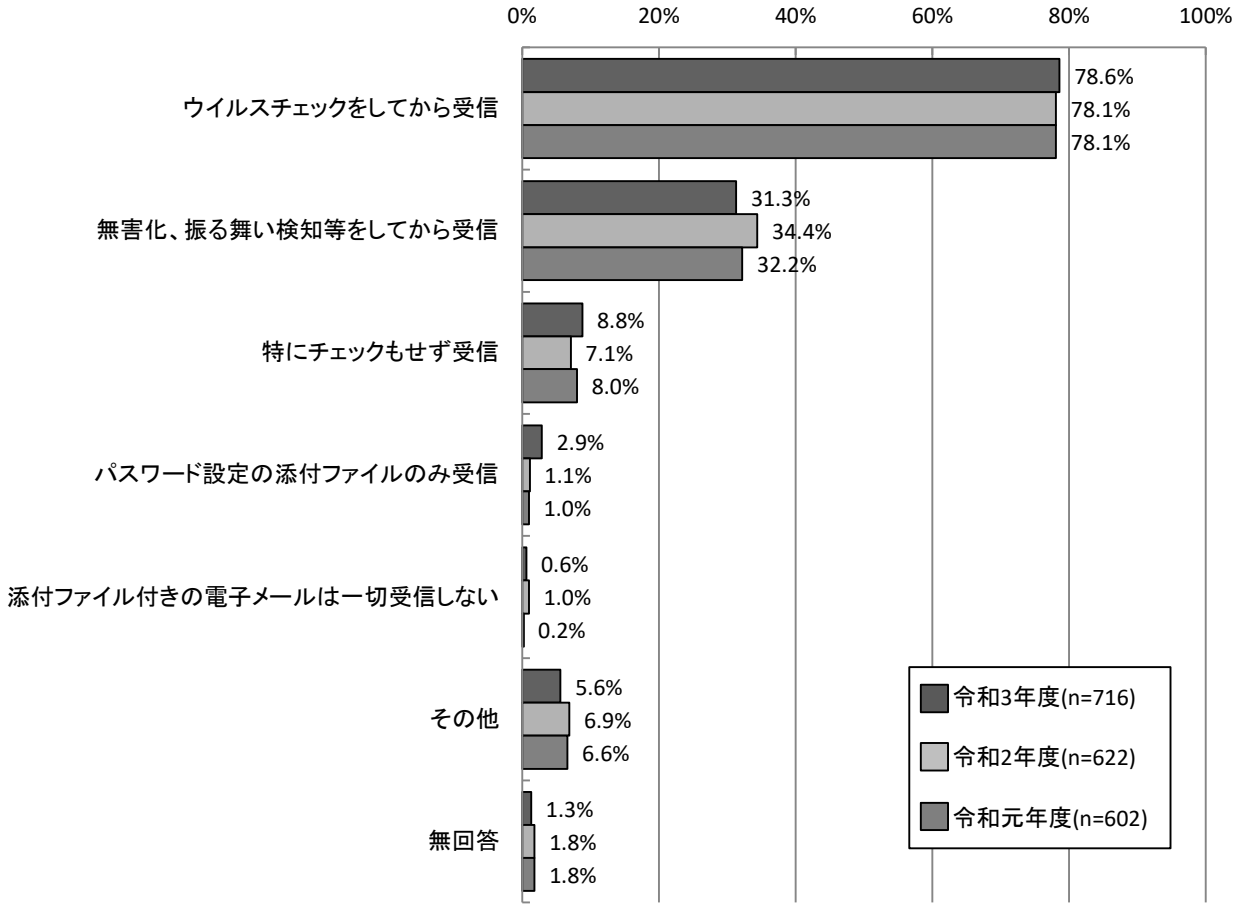
【業種別分析】業種別にみると、「ウイルスチェック等をしてから受信」は「金融」で93.3%と最も高く、次いで「エネルギー」で90.0%、「製造業」で89.8%となっている。

【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、「パスワード設定の添付ファイルのみ受信」が1.8ポイント、「特にチェックもせず受信」が1.7ポイント増加し、「無害化、振る舞い検知等をしてから受信」が3.1ポイント減少している。

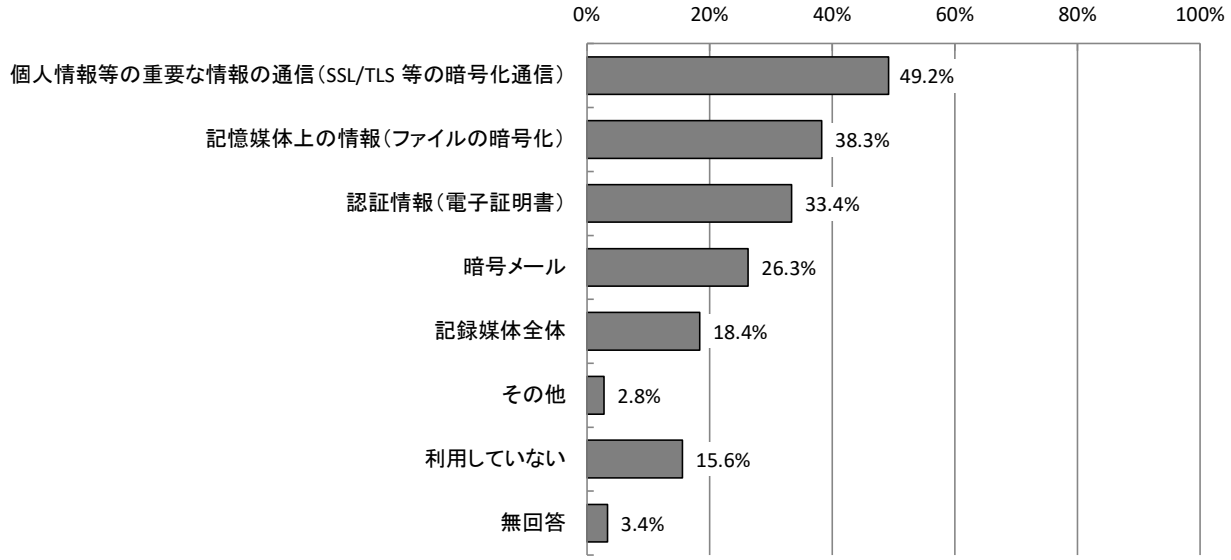
【経年変化】添付ファイルの取り扱い



3.2.21　暗号化技術の用途　【問27】

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/TLS等の暗号化通信）」が49.2%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38.3%、「認証情報（電子証明書）」が33.4%となっている。

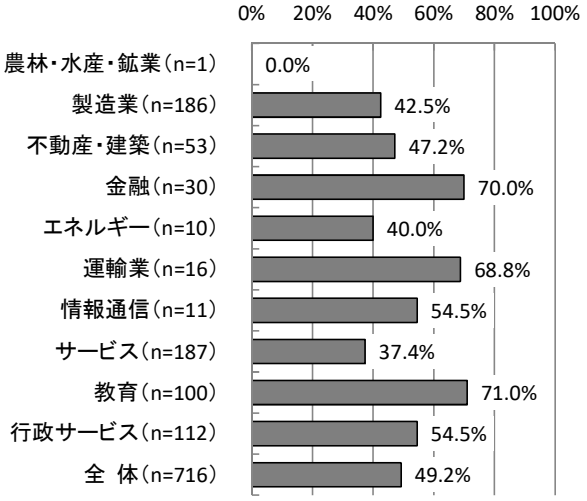
【全体】暗号化技術の用途（MA, n=716）



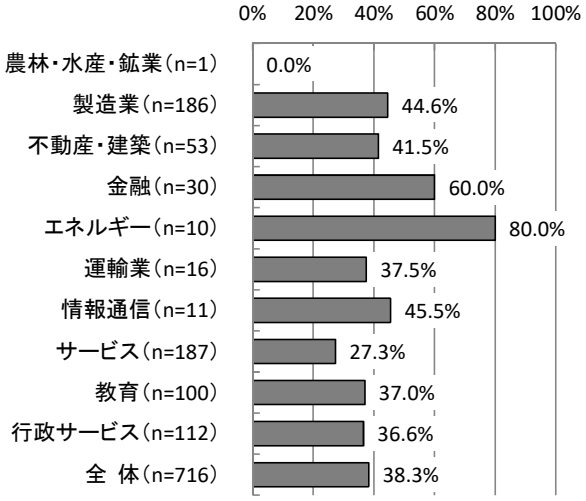
【業種別分析】業種別にみると、「個人情報等の重要な情報の通信（SSL等の暗号化通信）」については、「教育」が71.0%で最も多く、次いで「金融」が70.0%となっている。「記憶媒体上の情報（ファイルの暗号化）」については、「エネルギー」が80.0%で最も多く、「認証情報（電子証明書）」については、「金融」が53.3%で最も多くなっている。

【業種別分析】暗号化技術の用途

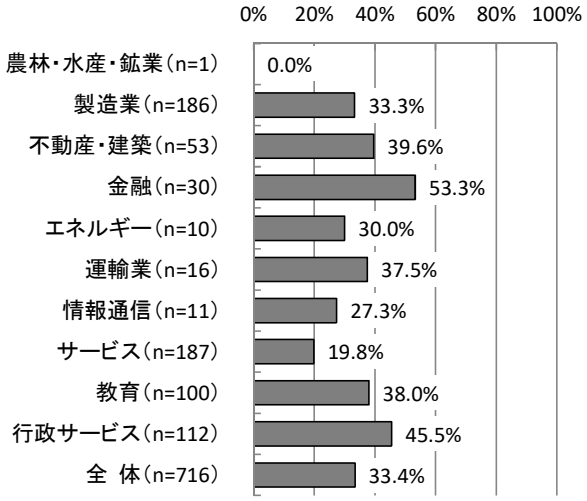
個人情報等の重要な情報の通信
（SSL/TLS 等の暗号化通信）



記憶媒体上の情報（ファイルの暗号化）



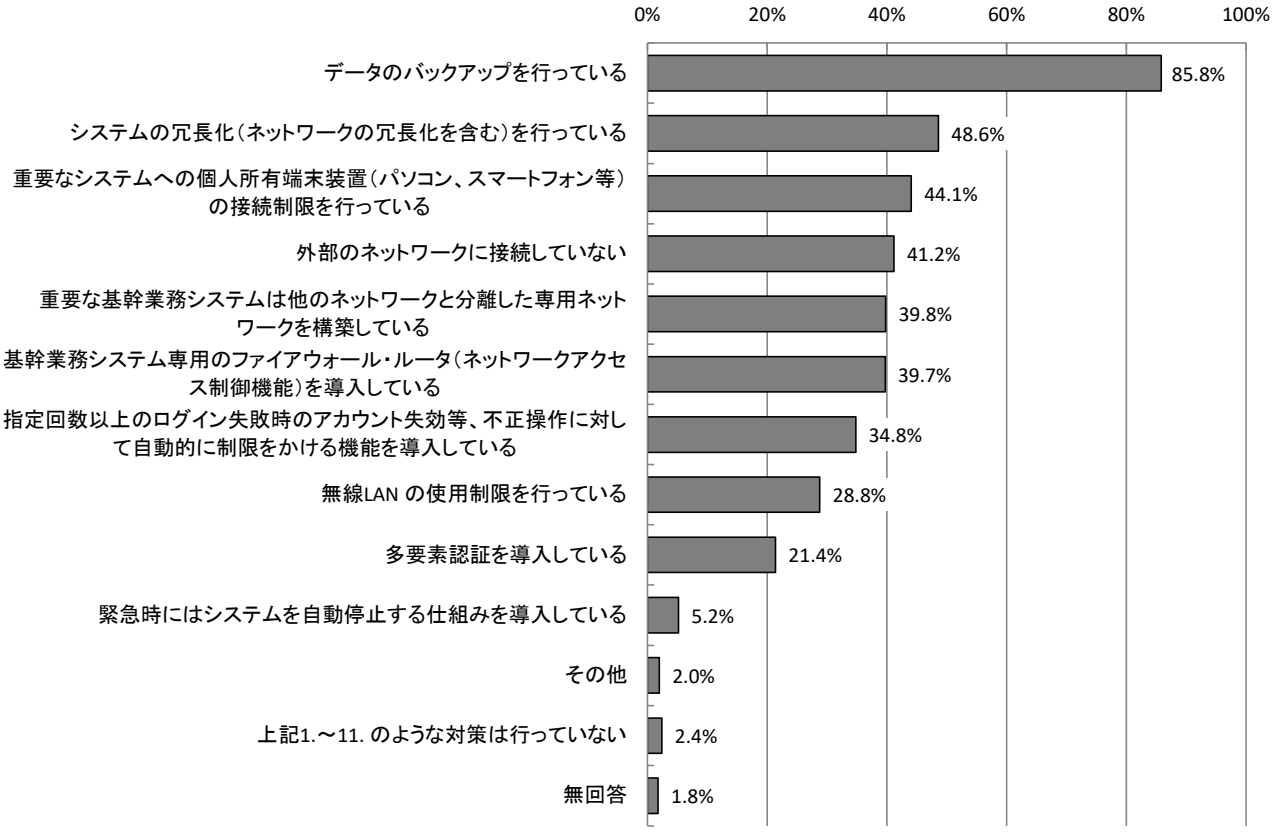
認証情報（電子証明書）



3.2.22　重要システムの不正アクセス対策状況　【問28】

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85.8%で最も多く、「システムの冗長化（ネットワークの冗長化を含む）を行っている」が48.6%、「重要なシステムへの個人所有端末装置（パソコン、スマートフォン等）の接続制限を行っている」が44.1%となっている。

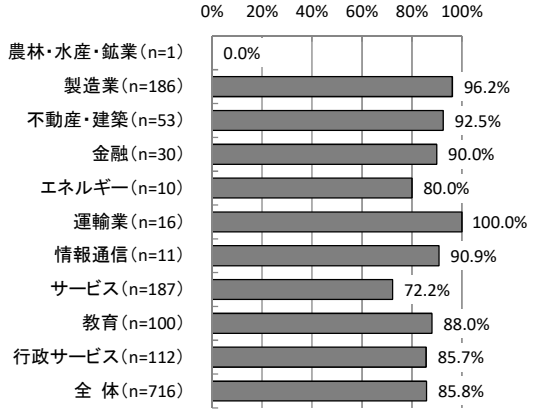
【全体】重要システムの不正アクセス対策状況（MA, n=716）



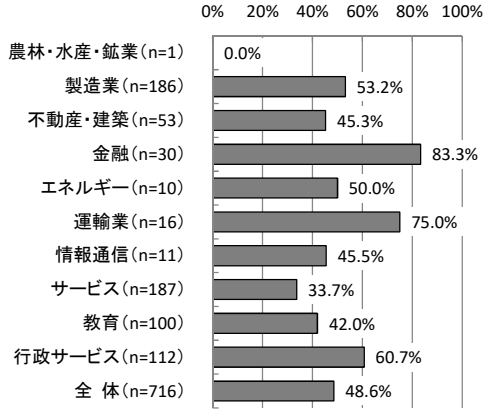
【業種別分析】業種別にみると、「データのバックアップを行っている」については、「運輸業」が100.0%で最も多く、次いで「製造業」が96.2%となっている。「システムの冗長化を行っている」については、「金融」が83.3%で最も多くなっている。

【業種別分析】重要システムの不正アクセス対策状況

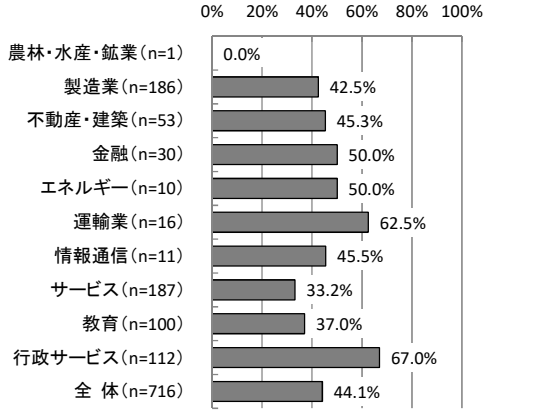
データのバックアップを行っている



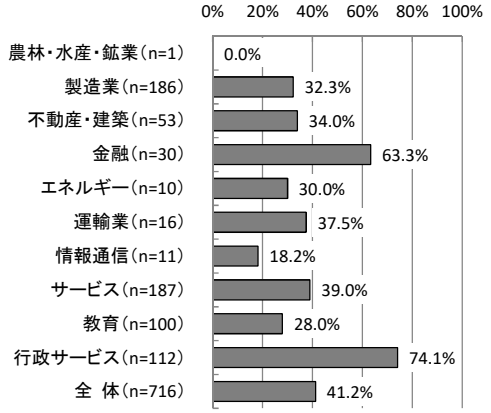
システムの冗長化（ネットワークの冗長化を含む）を行っている



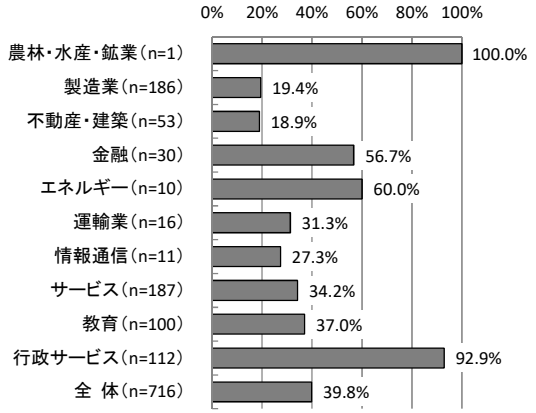
重要なシステムへの個人所有端末装置（パソコン、スマートフォン等）の接続制限を行っている



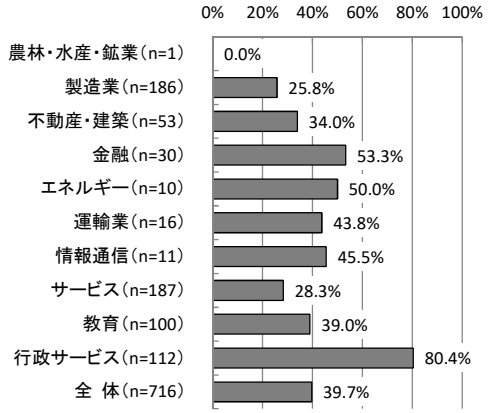
外部のネットワークに接続していない



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

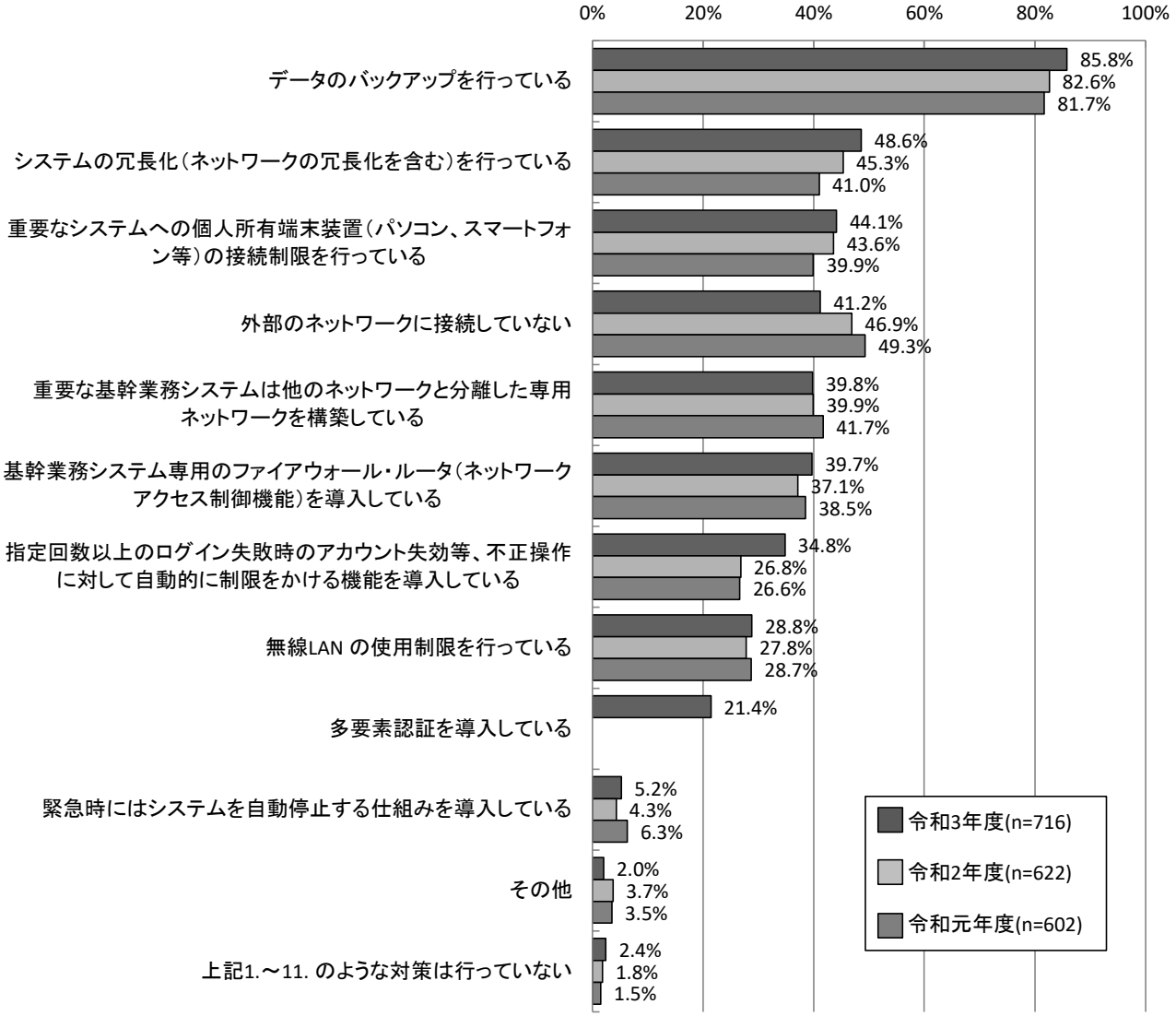


基幹業務システム専用のファイアウォール・ルーター（ネットワークアクセス制御機能）を導入している



【経年変化】昨年度と比較すると、「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」が 8.0 ポイント増加し、「外部のネットワークに接続していない」が 5.7 ポイント減少している。

【経年変化】重要システムの不正アクセス対策状況

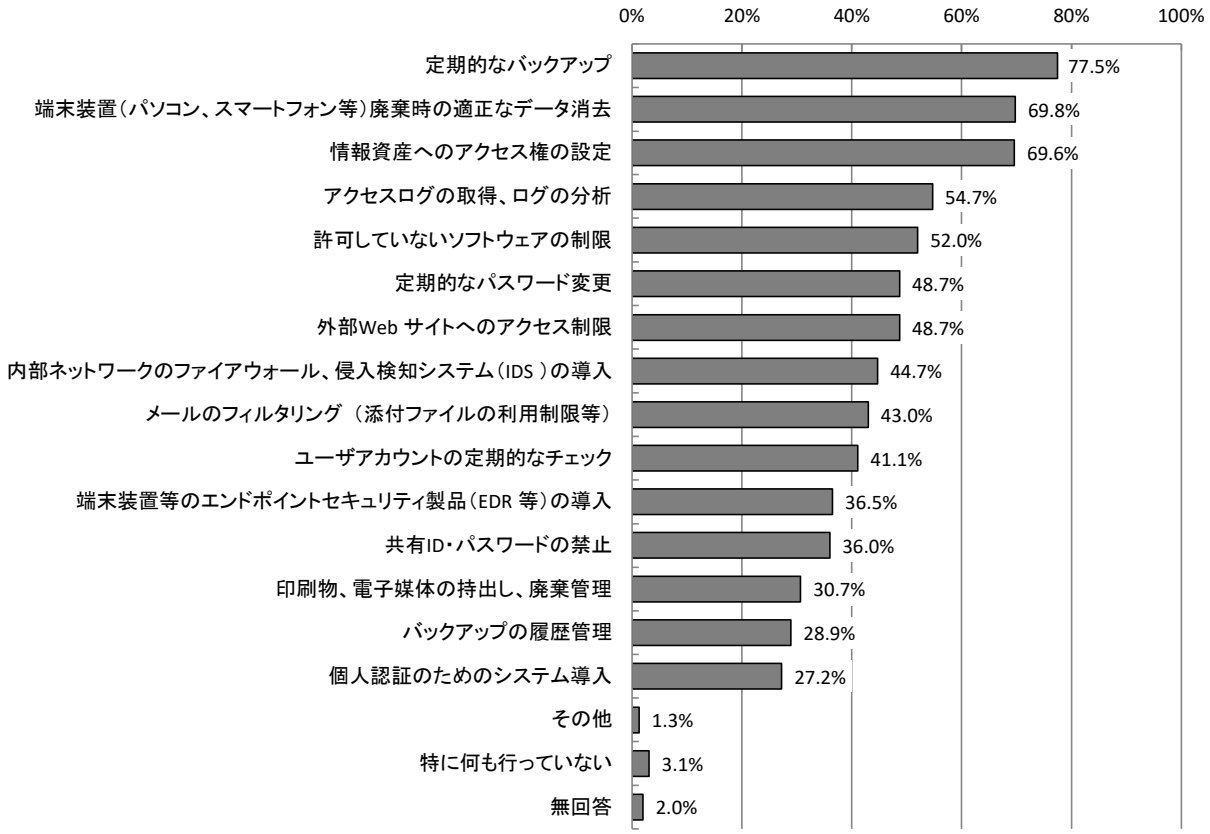


※令和３年度調査で、「多要素認証を導入している」を新設。

3.2.23　不正アクセス等への対策状況　【問29】

不正アクセス等への対策状況については、「定期的なバックアップ」が77.5%で最も多く、次いで「端末装置（パソコン、スマートフォン等）廃棄時の適正なデータ消去」が69.8%、「情報資産へのアクセス権の設定」が69.6%となっている。

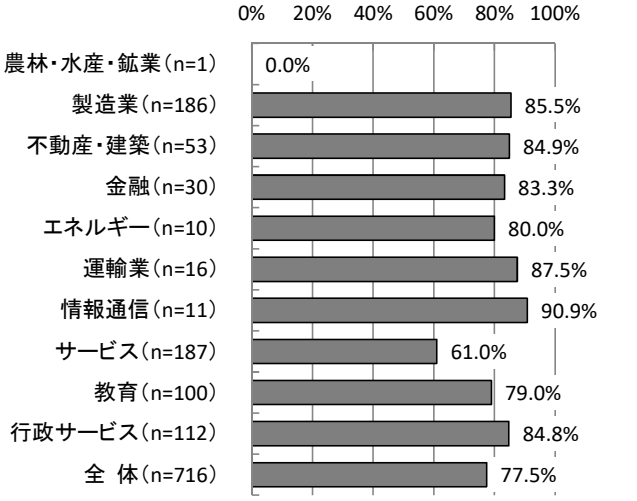
【全体】不正アクセス等への対策状況（MA,n=716）



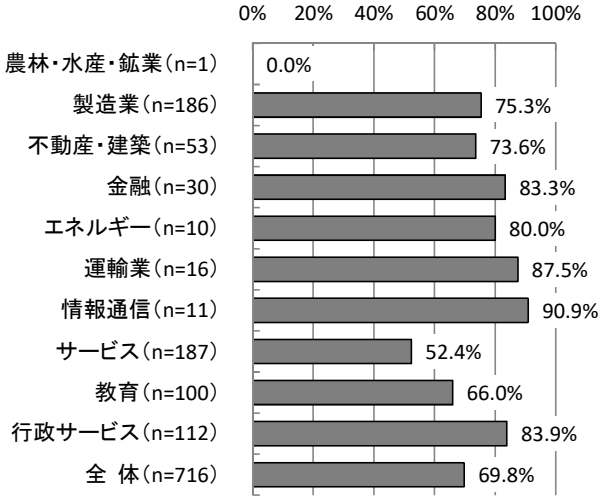
【業種別分析】業種別にみると、「定期的なバックアップ」「パソコン廃棄時の適正なデータの消去」については、「情報通信」が90.9%で最も多く、次いで「運輸業」が87.5%となっている。「情報資産へのアクセス権の設定」については、「情報通信」が100.0%で最も多く、次いで「金融」が90.0%となっている。

【業種別分析】不正アクセス等への対策状況

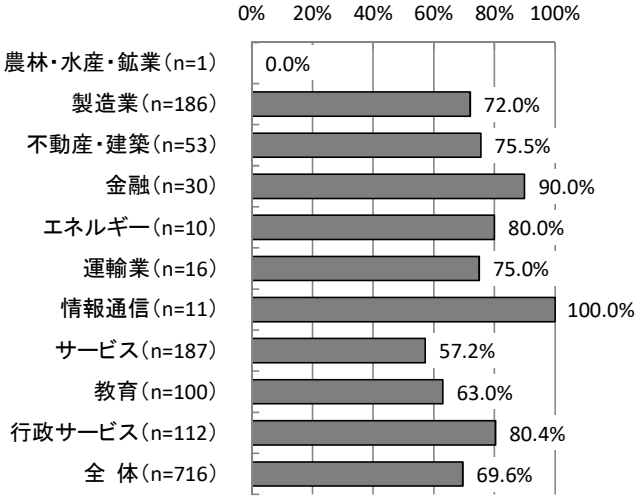
定期的なバックアップ



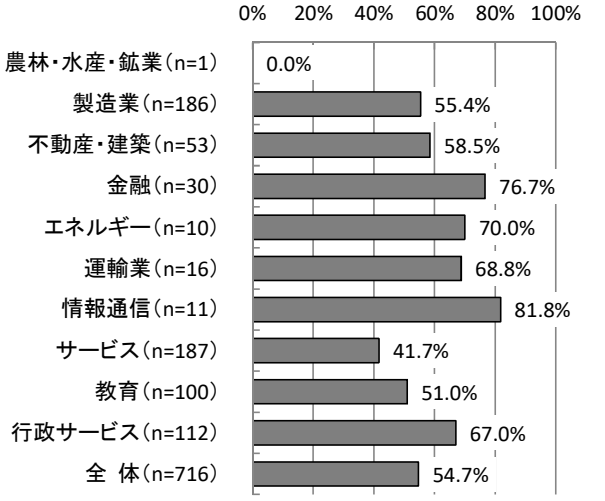
端末装置（パソコン、スマートフォン等）廃棄時の適正なデータ消去



情報資産へのアクセス権の設定

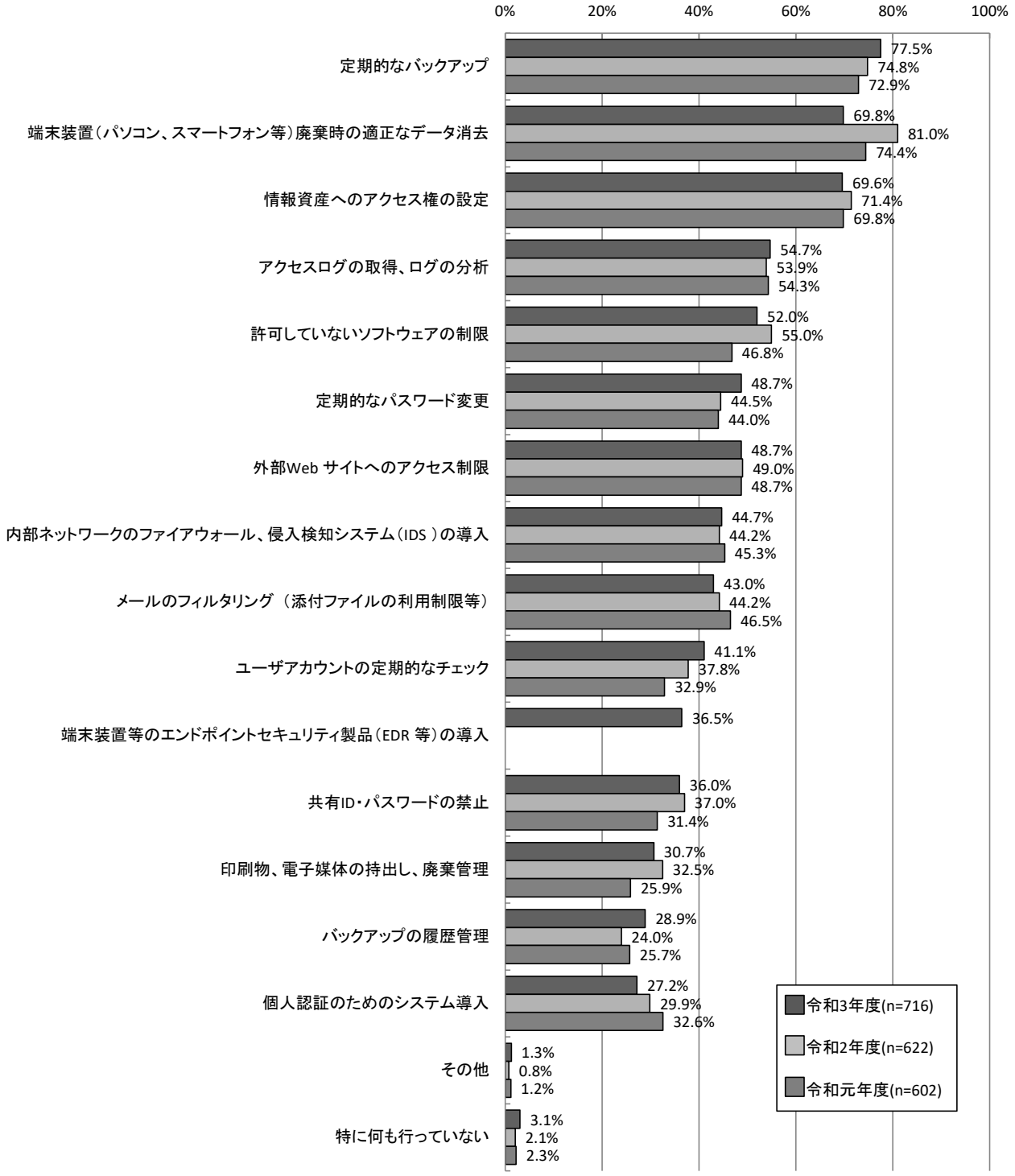


アクセスログの取得、ログの分析



【経年変化】昨年度と比較すると、「バックアップの履歴管理」が 4.9 ポイント、「定期的なパスワード変更」が 4.2 ポイント増加し、「端末装置（パソコン、スマートフォン等）廃棄時の適正なデータ消去」が 11.2 ポイント減少している。

【経年変化】不正アクセス等への対策状況

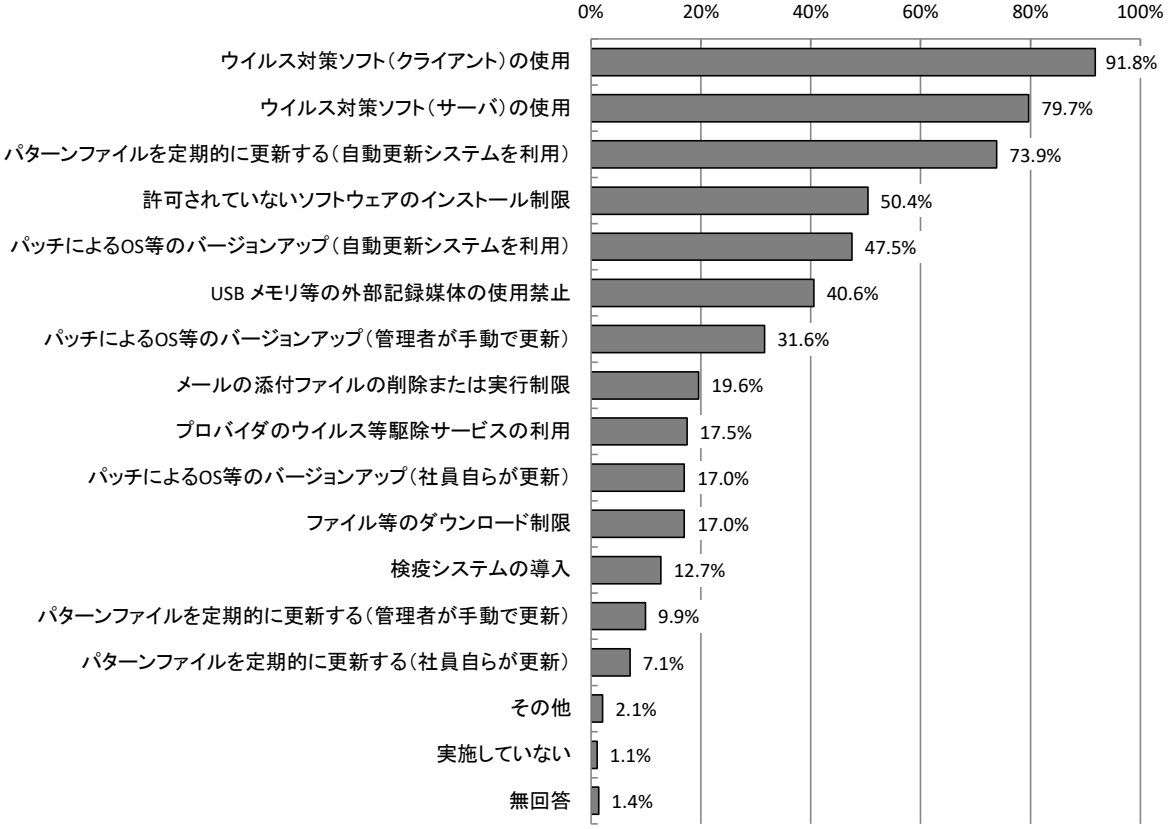


※令和３年度調査で、「端末装置等のエンドポイントセキュリティ製品（EDR等）の導入」を新設。

3.2.24　不正プログラムへの対策状況　【問30】

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91.8%で最も多く、次いで「ウイルス対策ソフト（サーバ）の使用」が79.7%、「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73.9%となっている。

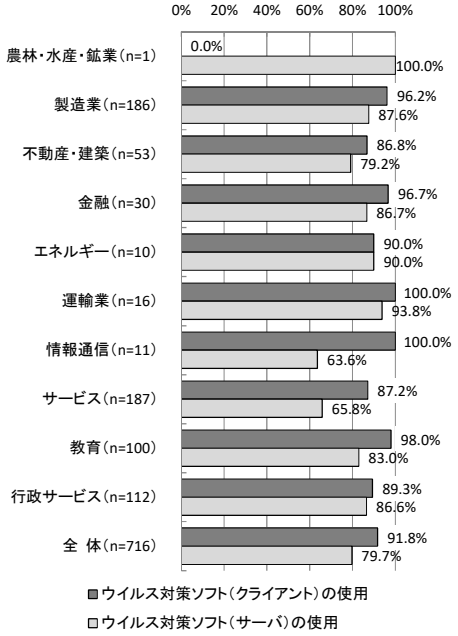
【全体】不正プログラムへの対策状況（MA,n=716）



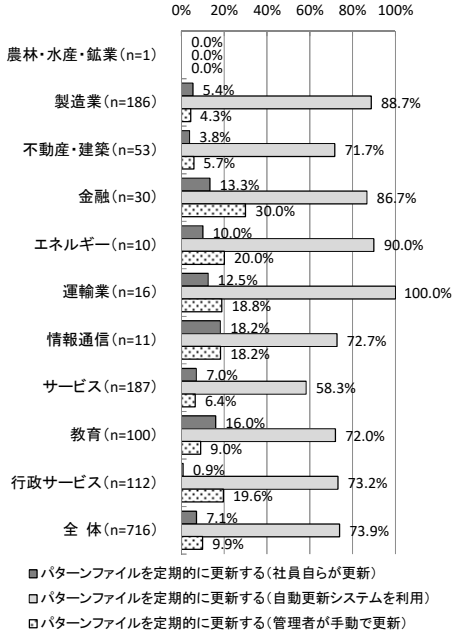
【業種別分析】業種別にみると、「ウイルス対策ソフトの使用」については、「情報通信」「サービス」以外の業種でそれぞれの項目が7割を超えている。また、「パターンファイルの定期的な更新」については、「製造業」「金融」「エネルギー」「運輸業」で「パターンファイルを定期的に更新する（自動更新システムを利用）」が8割を超えている。

【業種別分析】不正プログラムへの対策状況

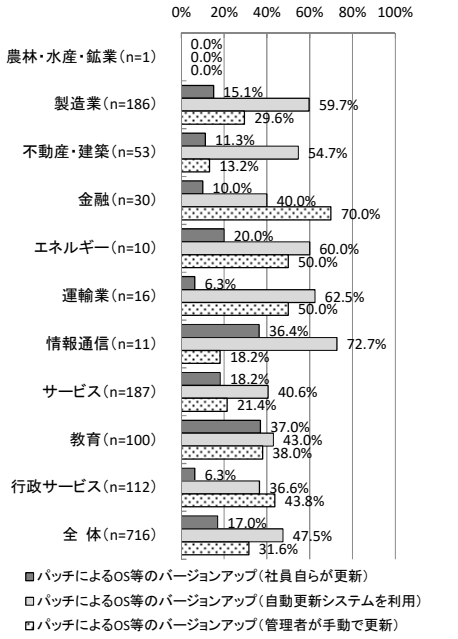
ウイルス対策ソフトの使用



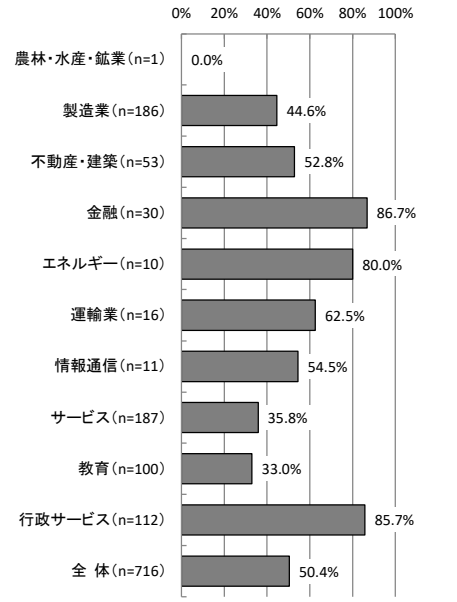
パターンファイルの定期的な更新



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

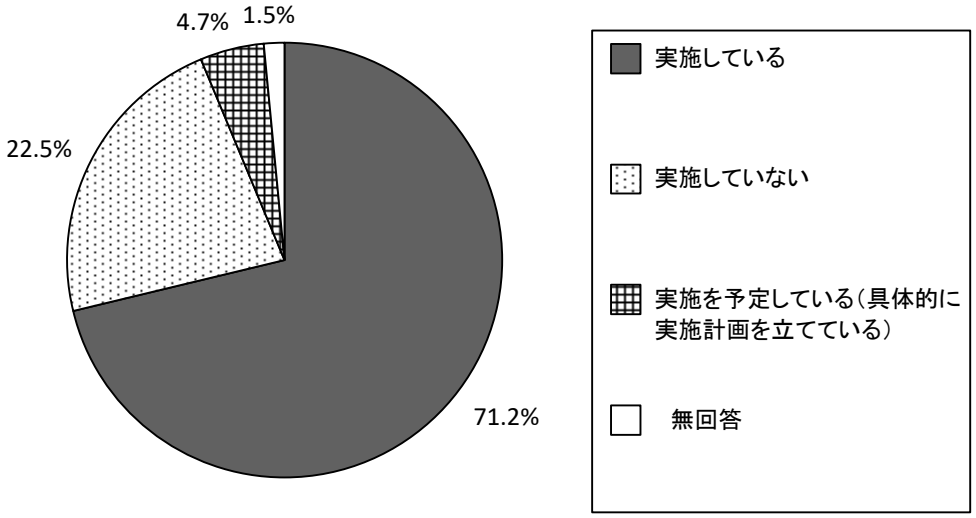


3.3　人的対策

3.3.1　情報セキュリティ教育の実施状況　【問31】

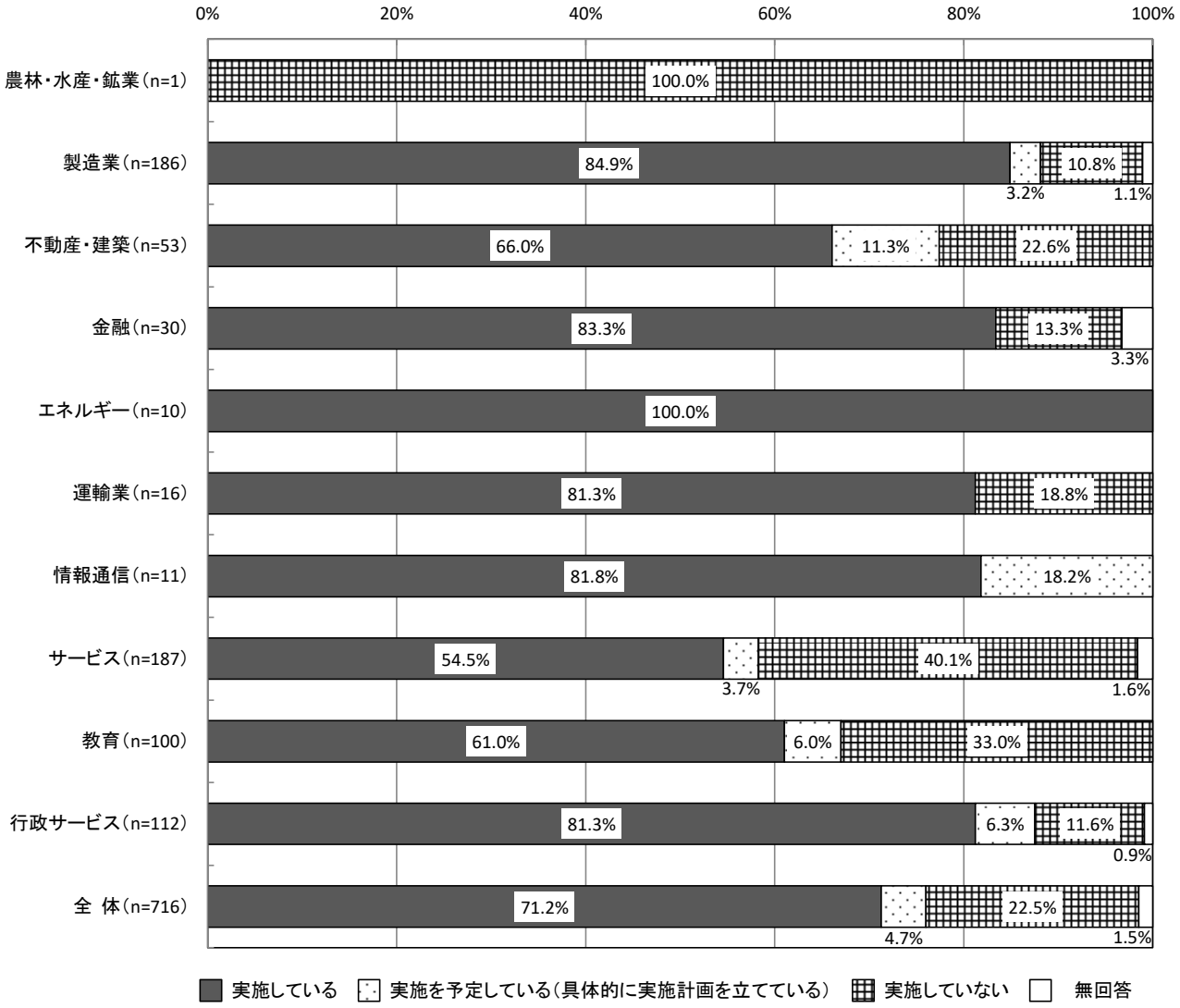
情報セキュリティ教育の実施状況については、「実施している」が71.2%、「実施していない」が22.5%、「実施を予定している」が4.7%となっている。

【全体】情報セキュリティ教育の実施状況（SA,n=716）



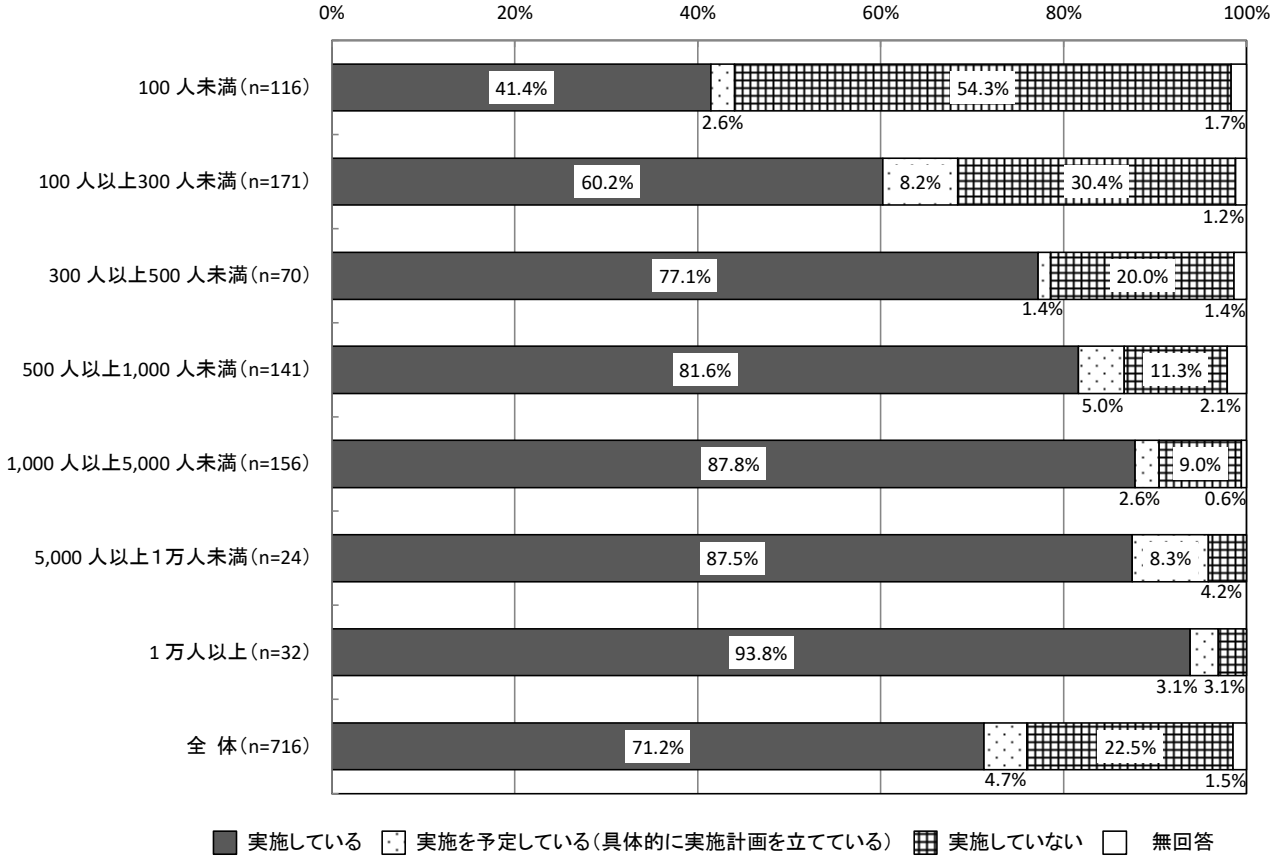
【業種別分析】業種別にみると、「実施している」については、「エネルギー」が100.0%で最も多く、次いで「製造業」が84.9%となっている。一方、「実施していない」は「サービス」で40.1%となっている。

【業種別分析】情報セキュリティ教育の実施状況



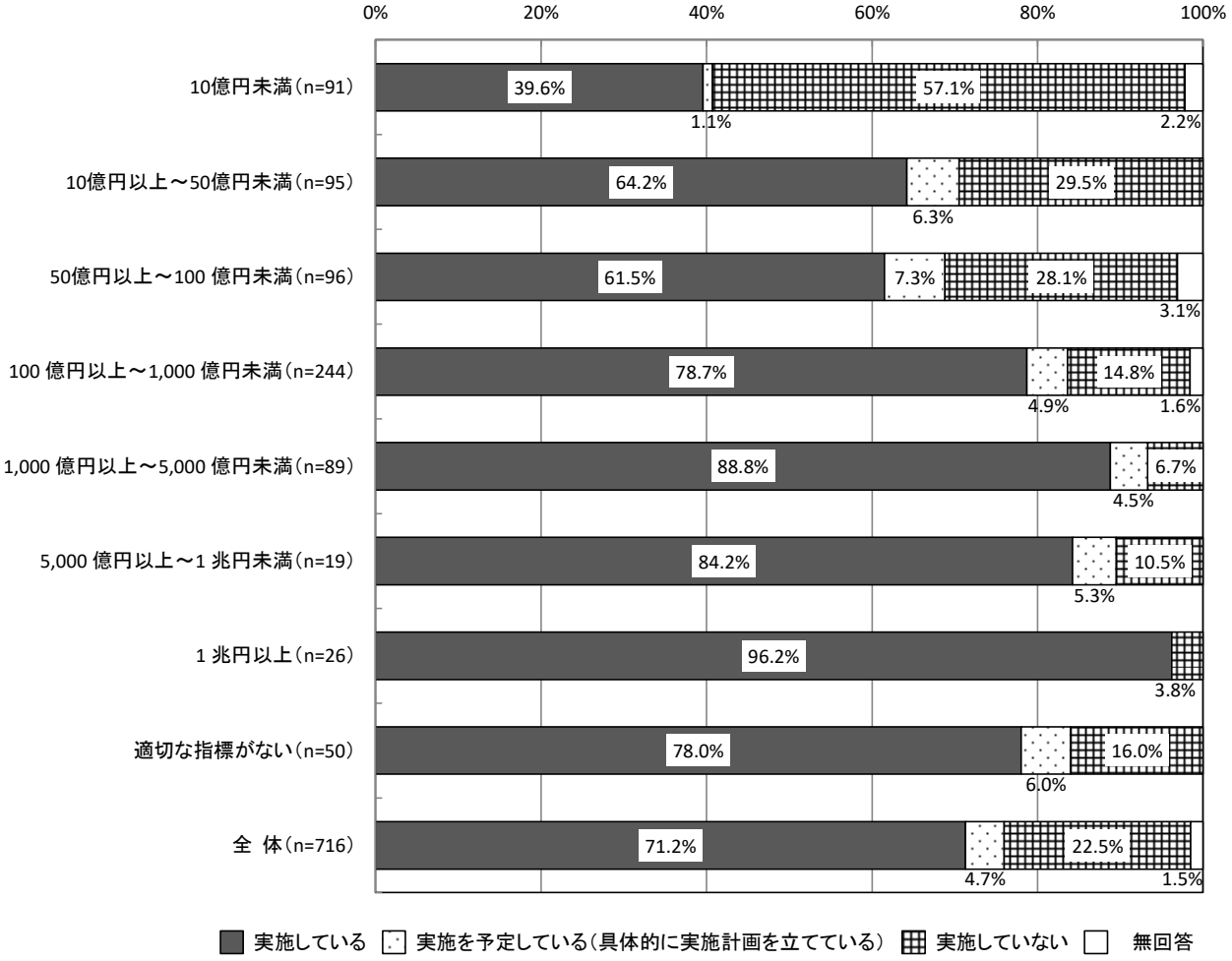
【従業員規模別分析】従業員規模別にみると、「実施している」については、概ね従業員規模が大きくなるにつれて多くなる傾向にあり、「１万人以上」で93.8%となっている。

【従業員規模別分析】情報セキュリティ教育の実施状況



【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「10億円未満」では39.6%だが、概ね売上・予算規模が大きくなるにつれて多くなる傾向にある。

【売上・予算規模別分析】情報セキュリティ教育の実施状況

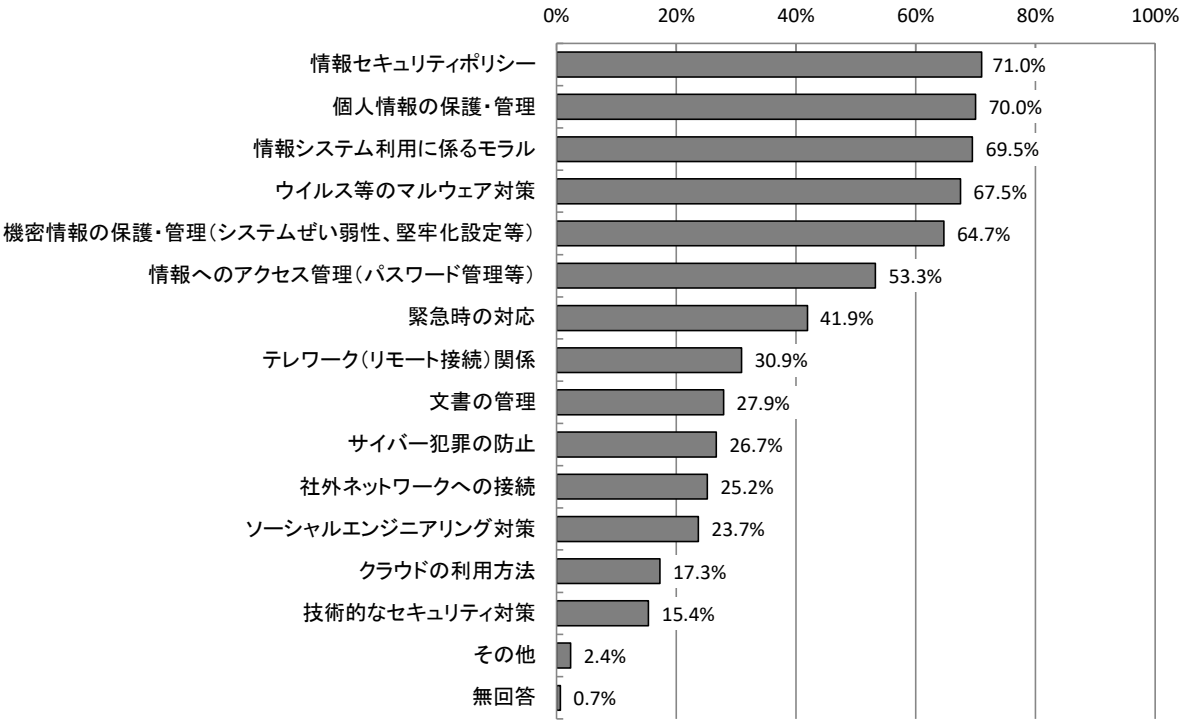


3.3.2　情報セキュリティ教育の内容　【問31-1】

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71.0%で最も多く、次いで「個人情報の保護・管理」が70.0%、「情報システム利用に係るモラル」が69.5%となっている。

※本項目は、情報セキュリティ教育を行っている社・団体等を対象としている。

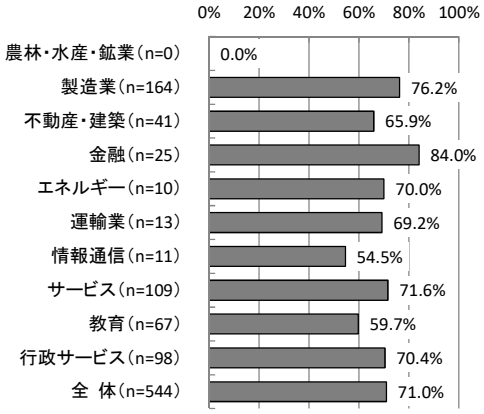
【全体】情報セキュリティ教育の内容（MA, n=544）



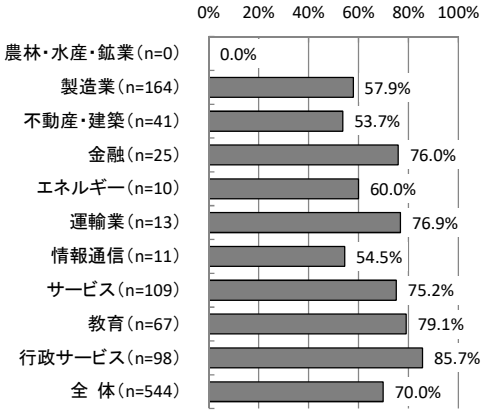
【業種別分析】業種別にみると、「情報セキュリティポリシー」については、「金融」が84.0%で最も多く、次いで「製造業」が76.2%となっている。「個人情報の保護・管理」については、「行政サービス」が85.7%で最も多く、次いで「教育」が79.1%となっている。

【業種別分析】情報セキュリティ教育の内容

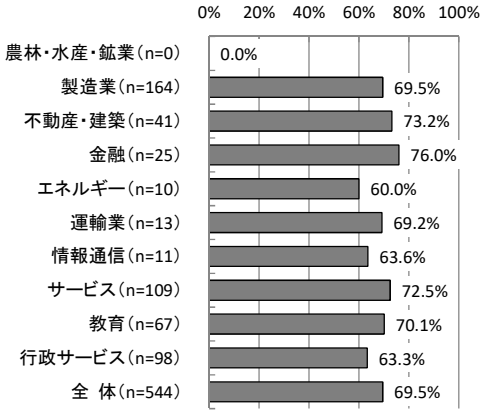
情報セキュリティポリシー



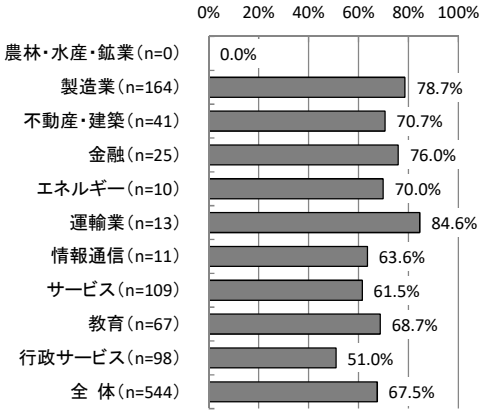
個人情報の保護・管理



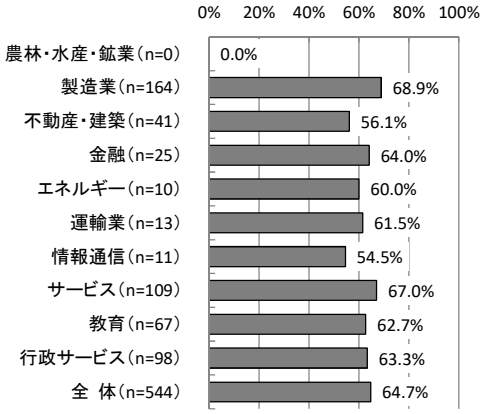
情報システム利用に係るモラル



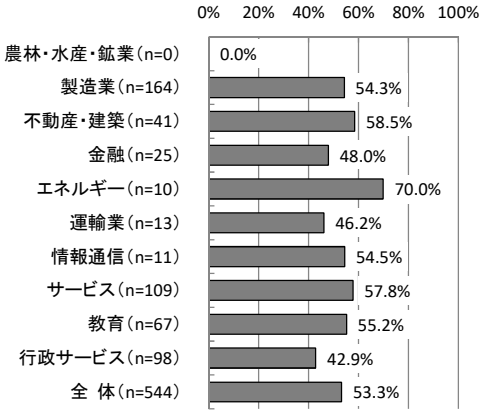
ウイルス等のマルウェア対策



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）

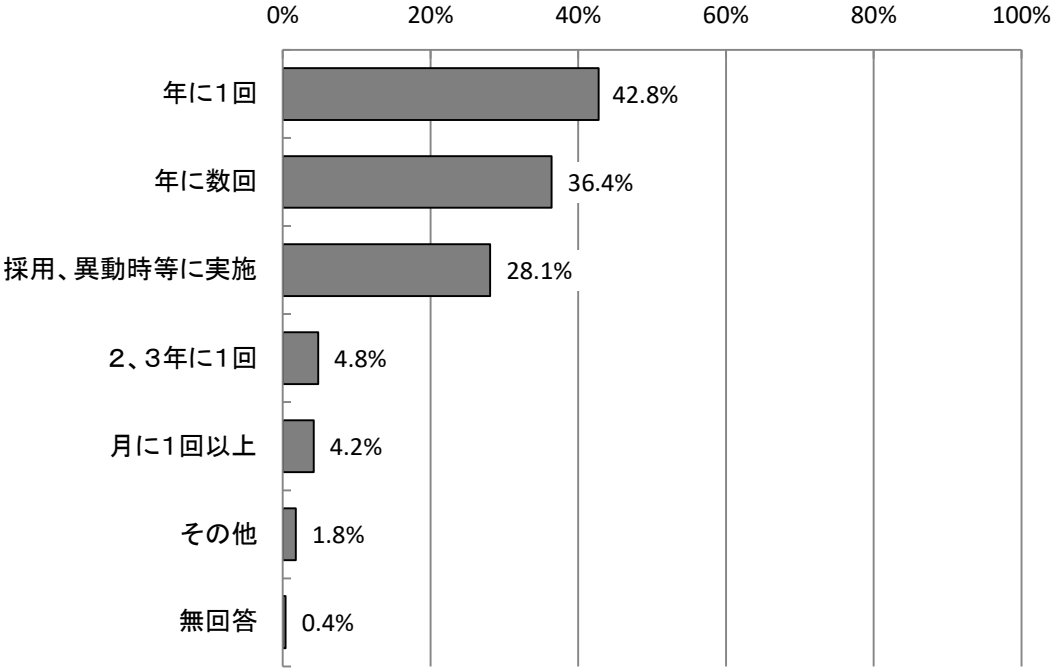


3.3.3　情報セキュリティ教育の頻度　【問31-2】

情報セキュリティ教育の頻度については、「年に１回」が42.8%で最も多く、次いで「年に数回」が36.4%、「採用、異動時等に実施」が28.1%となっている。

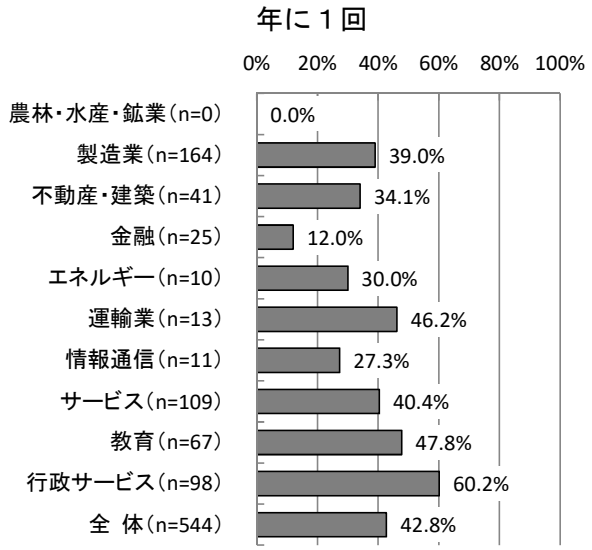
※本項目は、情報セキュリティ教育を行っている社・団体等を対象としている。

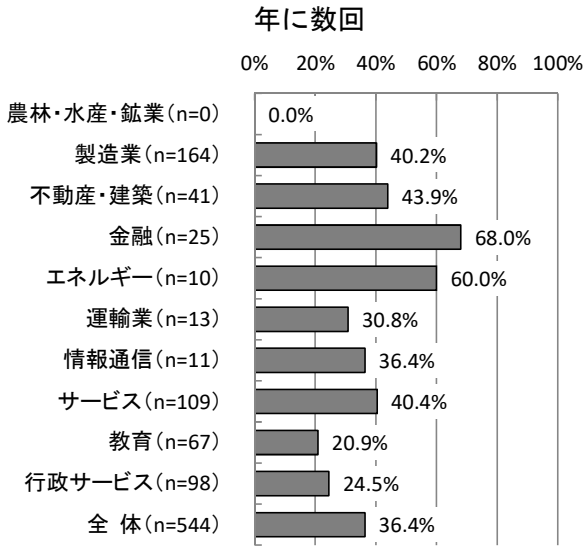
【全体】情報セキュリティ教育の実施頻度（MA, n=544）

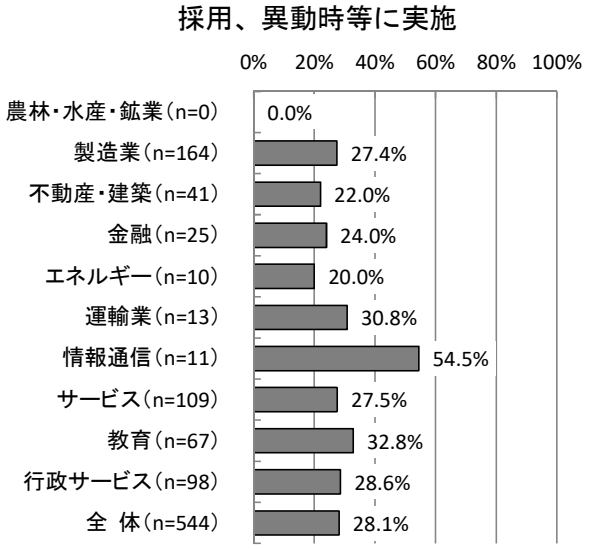


【業種別分析】業種別にみると、「年に１回」については、「行政サービス」が60.2%で最も多く、「年に数回」については、「金融」が68.0%となっている。「採用、異動時等に実施」については、「情報通信」が54.5%となっている。

【業種別分析】情報セキュリティ教育の実施頻度

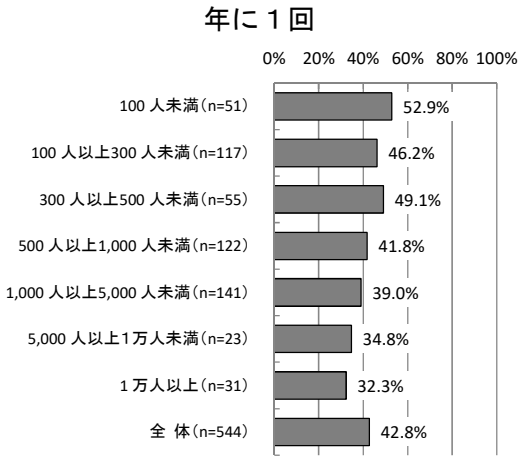


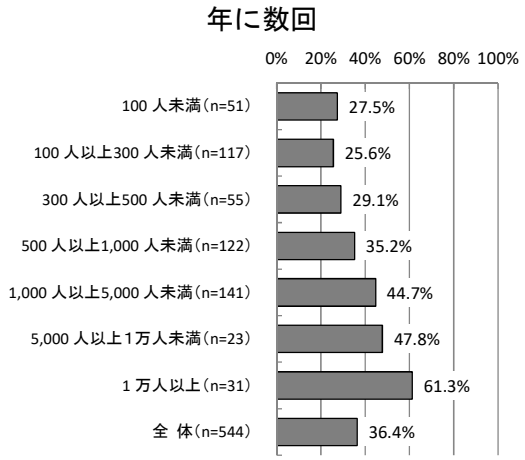


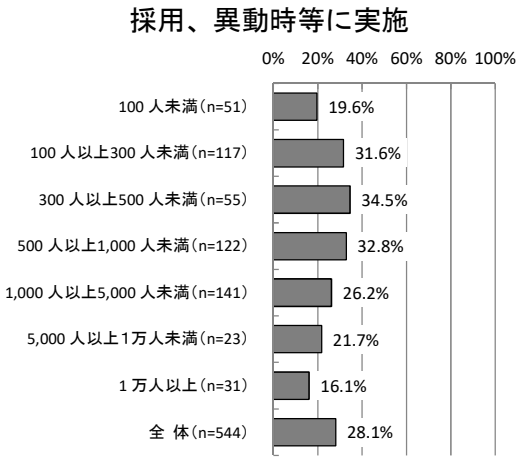


【従業員規模別分析】従業員規模別にみると、「年に１回」については「100人未満」が52.9%、「年に数回」については、「１万人以上」が61.3%と最も多くなっている。

【従業員規模別分析】情報セキュリティ教育の実施頻度





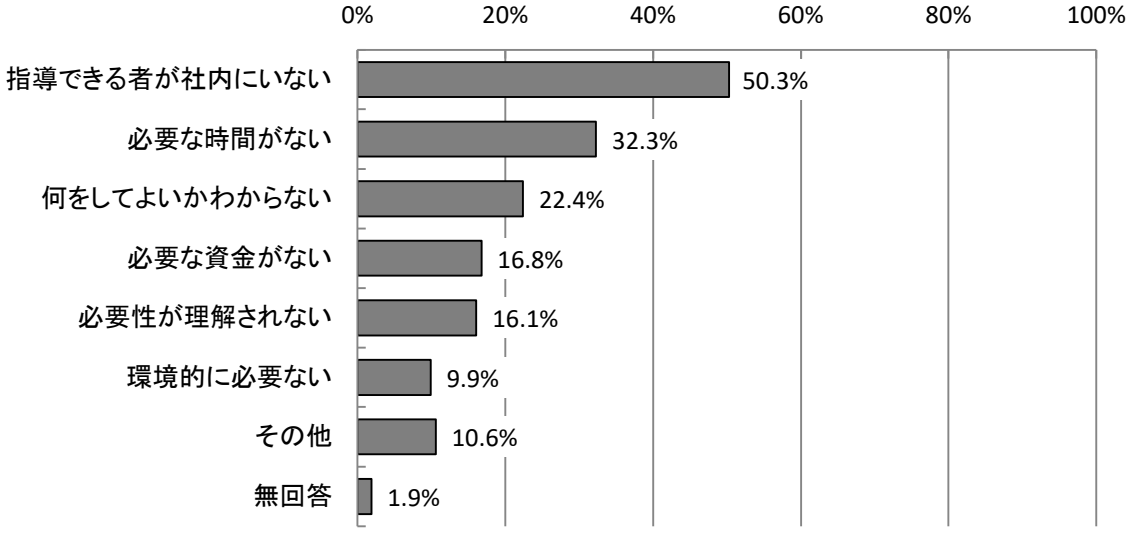


3.3.4　情報セキュリティ教育を実施しない理由　【問31-3】

情報セキュリティ教育を実施しない理由については、「指導できる者が社内にいない」が50.3%で最も多く、次いで「必要な時間がない」が32.3%、「何をしてよいかわからない」が22.4%となっている。

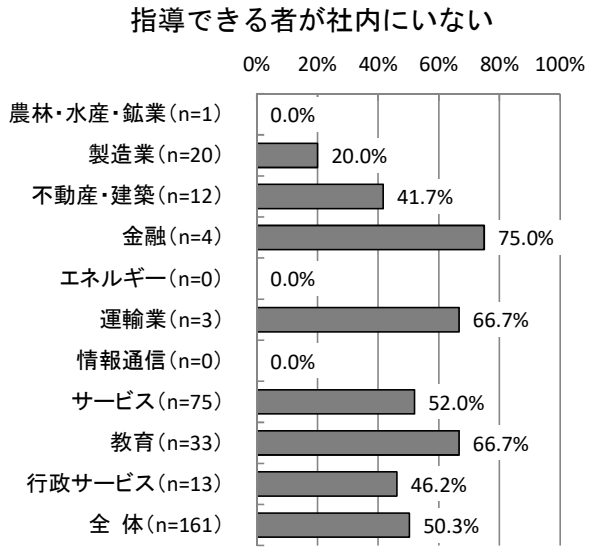
※本項目は、情報セキュリティ教育を実施していない社・団体等を対象としている。

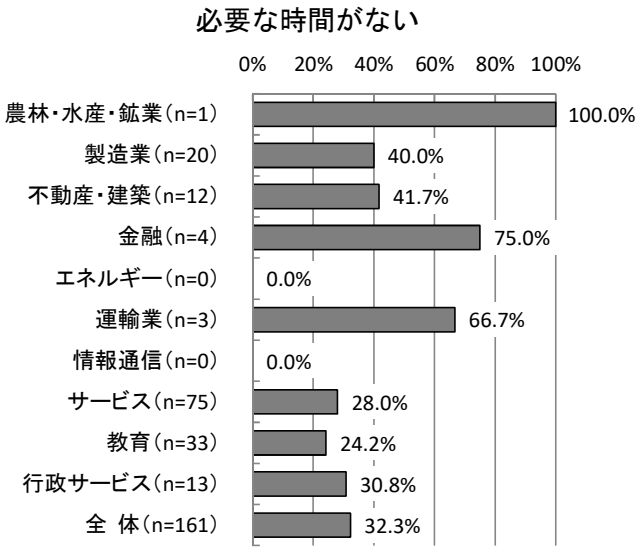
【全体】情報セキュリティ教育を実施しない理由（MA, n=161）



【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、「教育」が66.7%で最も多く、次いで「サービス」が52.0%となっている。

【業種別分析】情報セキュリティ教育を実施しない理由





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

●セキュリティ投資に関する目安がないため、会社の業務や経営者の意識によって、変化が生じる。
●・情報システム部門との兼務であり、情報やセキュリティに関する最新の動向をつかみ自社の対策に落としこむことがなかなか迅速に対応できない･監視など不正侵入などのインシデントに素早く気づく体制が整っていない・どこまですべきかわからず過剰投資になりがち。
●情報セキュリティ対策で、実施している業務に対して、どこまでコストをかけて実施していくべきかに悩みます。
●投資及び教育にかかわる費用、時間が増加の一途をたどっている。重要性も高まっているが、零細企業には負担が大きいと感じる。
●診療所の為、患者さんの情報が外部に漏れない為のセキュリティを外部の業者に依頼している
●役員における情報セキュリティに対するリテラシーが低く、法律的な強制力もないため、必要性があまり理解されない。法整備や実務担当の地位向上につながる様な施策を行ってほしい。
●利便性の追求と情報セキュリティのバランスを保つことに困難を感じる。
●アンケート内にもありましたが、情報セキュリティ対策は費用対効果が見えにくく、掛かる費用に対する納得を得られにくいこと。また、専門部署を組織できないこと。
●情報セキュリティ教育の大変さを感じています。ＩＴリテラシーの底上げは必須だが、全国の拠点に等しく行うことは難しいです。
●セキュリティ対策と運用の利便性のバランス。利便性を損なわないセキュリティ対策。
●予算面、体制面、スキル面において一般企業で対応するにはある程度、限界があると思う。一般企業のIT部門に情報セキュリティのスペシャリストは入社してこない。理想と現実の大きなギャップを感じます。
●従業員全体のリテラシー向上が難しい。
●必要なコストへの理解と、教育のコスト
●グループ会社との一体運用の業務が多く、海外を含めたグループ会社に対する教育が十分できていない。
●セキュリティ対策は重要であるが、毎年対策を変えて費用をかける必要があるが、なぜかけた費用で防御が不足するのかを説明するのが難しい。また、業務効率や売上の向上といった目に見える形での組織への貢献が見えにくく、予算申請しにくい。
●日々対策が変化しており、何が適正な対策か手探りで運用している。対策実施時に当然費用が掛かるが費用対効果の説明が難しく、システムの導入が思うように進まない。
●セキュリティは出来るだけ強化したいと考えていますが、費用対効果を会社へ説明しにくく、政府推奨または法整備による、明確な基準が指し示されれば導入しやすくなると思います。
●情報セキュリティ対策を専門とする部署がないこと。
●システムの導入や更新において、予算が限られていたり、予算により納期が縛られてしまっていたりしており、対策が十分に行えていないことを感じている。
●情報セキュリティ周知徹底可能な判り易い説明資料（ＩＴリテラシーが弱い方へもそのまま使えそうな資料）が１年更新される形であれば大変有難いです。
（特に、情報セキュリティ事故でどれだけ費用面および社会的インパクトがあるのか？、実際に会った情報セキュリティ事故事例などと共に、認識薄い方へもしっかりと危機感を煽れる内容の方がより判り易い、と考えます。）
●取引先や委託先での情報セキュリティ事故による自社情報漏洩への対策はコントロールできない。（契約時の賠償請求に関する取り決め程度しかできない）
●情報セキュリティ対策の対策規模は会社規模と余力にあった対応までが前提となる。
●情報資産の活用と情報セキュリティ対策のバランスをとるのが難しい。（利便性を確保しようとすると情報セキュリティリスクが増大する傾向がある。人的・金銭的コストをかけても完全な防御は難しい（コストに見合わない））
●セキュリティ対策は費用対効果が期待できないものとなっている。経営層に向け、セミナーやホワイトペーパなど、経営層が危機感を感じる資料がたくさんの種類があるとうれしい。
●各種協会、協議会、団体、メーカーなどがそれぞれセキュリティ対策に対するドキュメントやガイドラインを作っており、情報が散乱しているので収集に時間がかかります。そういった各種情報を一覧化してくれるような仕組みがあるとありがたいと思っています。
●セキュリティを強化すればそれに応じて職員に制限をかけ、不便をかけることとなり、なかなか理解いただけないこと。また、職員のセキュリティへの意識向上が難しいと考えており、職場のPCに使用のスマホやUSBを接続し、ウイルスを検知するような事例も報告されている。
●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。
●利便性とセキュリティの両立にはお金掛かる、また、電子申請ができる様に環境を構築する必要があるがお金が掛かる。将来的に予算が膨らんでいくこと。

●・活動予算の調整時に、費用対効果を説明するのに苦労する
・従業員全員の情報セキュリティリテラシーを向上させるための方法
●インターネットを介したセキュリティを脅かす各種の脅威は、一般的なユーザーの想定を超える程身近になっている半面、一般的な見方ではすでに脅威を認識できない。教育で対応できる範囲を超える部分もあると思われるが、そういった脅威に組織的に対応する必要性を理解いただくこともまた難しい情勢になっている。情報セキュリティ対策を実施するにあたって、不安や困難に感じていることは下記です。
・情報セキュリティ対策をどこまで行えばよいのか、企業や業種において社会通念上の基準がなく、各企業判断に委ねられており手探りの対応が必要であること
・業務効率とセキュリティレベル向上に伴う負担増となること
・ウイルス・不正通信発生時、最終的に問題なしと判断するための経験や知見が必要であること。ノウハウ不足による見逃しリスク有。
・セキュリティ分野の技術的な進展に伴う社内の対応知見・経験が追い付いていない。
・セキュリティを担保するための、現場含めた社内体制の構築が課題。事業拡大する中、知見・経験含めて対応が追い付いていない。
●社内の意識醸成をどうやっていくかが最優先の課題であって、仕掛けや仕組みを導入するのはその後の工程であると考えています

２．技術的対策

●クローズドの有線LANの為大きな対応は行なっていないが、気にはしている。
●いくら対策しても、攻撃者の技術のほうが上手で、常に不安である。
●・同規模以上の他社との導入レベルの比較がしづらい。（投資の一つの妥当性の目安としたい。）
・メールにおけるドッペルゲンガードメインに対しては自社だけの対策では情報漏洩を防げない。
●・利便性と情報セキュリティ対策のバランスが難しい。
・年々、不正アクセス等の攻撃が巧妙化していく中で、その対策を講じていくのが難しい。
●技術面、知識面が不十分であり、情報収集や対策の実施に不安を感じる
●ランサムウェア等に感染した場合の、備えと安全な復旧手順に不安があります

３．人的対策

●セキュリティ管理のための人的資源の確保。どのレベルまで、対策を行うべきかの見きわめ。
●・何から実施すればよいか分からない。
・人員不足（一緒に考えてくれる人がいない）
●費用・人材の不足　重要性の理解不足
●専属の担当者がいないので、従業員の負担が大きい。
●情報セキュリティの重要性がより多くの方々に理解されると対策を進めやすくなります。よろしくお願い致します。
●セキュリティ対策、DXなど必要は感じていても人的に対応できていないのが現状。この手のアンケートさえも多すぎて負担です。
●セキュリティ人材が不足している
●専任担当者がいないため、他の業務との兼ね合いから対策が後回しになってしまう場合がある。
●人的対応。
●利用している人の認識が薄く感じる為、教育や訓練が必要と感じる。
●事務局が小規模（常勤は3名）すぎて情報セキュリティは外部委託せざるを得ないが、その業務を監督できる人材が居ない。
●要員や予算の確保が難しい
●サイバー攻撃は日々巧妙化、高度化している。ピンポイントで弊社を狙ってこられた場合に、どこまで耐えられるか。また標的型攻撃でも、発信者の詐称でなく先方のメールアカウントが乗っ取られていた場合等は、発信元での識別などできる訳もなく、文脈にも不審な点が無ければ避けようがない。この様な攻撃に対しては、いくら訓練等行っても効果はない。また情報セキュリティ対策に掛けられるコスト・人的リソースも弊社では限られており、その対策・対応には限界がある。
●学内におけるセキュリティセミナーを行うことが理想だが、計画立案自体に係る人的リソースが不足している。
●情報セキュリティの脅威に対応するための人材育成や最新技術に対応した機材を導入するための予算確保が難しい
●・情報セキュリティのインシデント発生時においては、その調査を行うためにしばしばネットワークやオペレーティングシステム等に関する高度な知識が必要となるが、それらを有する人材が不足している。（即戦力となる人材の確保、あるいは組織内での育成が難しい）
・大学という特性上、個人の持ち込みＰＣの接続を許可しなければならず、その点においてセキュリティ対策に難しさがある。
●情報セキュリティ対策を行うための人材や体制、スキルが十分ではない

●サイバーセキュリティ関連ＩＴ製品の複雑化・高額化、サイバーセキュリティ対策を行う人材の確保
●セキュリティのe-ラーニングや標的型メール訓練など、ＩＴ部門としてセキュリティ教育の機会を多く提供しようとしているが、その目的や必要性が十分理解されていない状況。従業員１人１人が自分事として捉えていただかないと意味がないため、引き続き啓蒙活動を続けていく。また、いくら対策をしても脅威がゼロになることはないため、今後は被害にあったときにいかに元の状態に早く復旧できるかという点にも力を入れていかなければならない。こうした取組に対し、リソースが不足している。
●各企業や団体の技術者が自由に相談できる無料の窓口があるといい。
●セキュリティ対策の情報不足、人的・対策時間の確保、セキュリティ教育や啓蒙活動
●・情報セキュリティ教育を徹底したいのですが、学生、教員、事務様々な立場での都合や思惑があり、その機会の設け方に苦慮しています。
・アンケートにお答えすることで、見直しにつながっており御礼申しあげます。
●セキュリティエンジニアの不足、要員不足による業務過多が深刻
●・費用と人的リソースに対して、どこまで対策を実施するか。１人しか居ないので、出来る事が多くないが、かといって委託すると費用的に難しい。また、そもそもセキュリティ関連のサービスや物品が高価。
・セキュリティ対策と業務上の利便性とのバランス
●専門的知識を保有する職員が不足している。
●情報システム要員の不足
●理解度に格差があり、教育実施時のレベル設定が難しい
●業務の性格上、社員以外の常駐スタッフの出入りが多く、情報セキュリティ教育等を実施しても隙間が出来てしまう。
●個々人の認識レベルが違うため、同じ内容の教育を行っても、理解度に差が生じてしまう。

４．その他

●いろんな分野の対策に応じたソリューションや製品が山ほどあるので、選定が難しいと感じる。導入を検討している間にも、どんどん時間が過ぎてしまう。
●アンケート結果のまとめを公開、共有して下さい
●セキュリティツールの価格が適切か、割高なのか、判断がつかない
●設問の意味・専門用語がわからないのがあった
●専門用語が多すぎて何を言っているのかわからない。
●中国ハッカーの撲滅をよろしく
●経営者のセキュリティへの理解があまりにも乏しい。ＩＴ全般といっても過言ではないレベル。一般レベルのリテラシーも2000～2010年代から、そこまで上がっておらず、諸外国との格差は拡がるばかりだと感じる。
●用語が全く理解できず、当方が質問に当てはまっているのかがわからない。このような程度のいる事務所なので、何が必要かも全くわからない。
●情報セキュリティに関し、多くの対策を実施して、費用もかけているが、攻撃側が常に最新の手口を用いていることや、相手が組織として活動しているので、１民間企業だけの対策では、防御は困難と感じる（相手とはATP10などです）
●業種等によりシステムの設計思想が異なるため、システム構成等も異なると考えられ、回答しづらい事項があった。
●アンケートについて前提条件の設定が欠けているのに具体的回答を要する質問が多い。質問自体もかなり昔のセキュリティ対策を元にしたものを焼き直して作問しただけで、内容が古いと思う。
ＩＴ管理者向け調査かつコロナ禍で在宅勤務が多い状況なのに、オンライン化できないのか？紙やExcelでないと回答の統計解析が設定できないのか？効率が悪い手段を使っていることに疑問を感じる。また、アンケート冊子自体や封筒も送付されているが、紙と郵送代もかかるし紙で回収したものもパンチャーに委託すると思われるので、無駄遣い。
このような中身のないアンケートを漫然と繰り返すことに誰か意見を言う人はいなかったのか、税と資源の無駄遣いをしていると感じる。
●新型コロナウイルス感染症対策で在宅勤務が増え、場所にとらわれないセキュリティ対策の必要性を感じています。
●どこまで行えばよいか、判断がつかない。（行おうとすれば、際限がない）費用対効果が分かりにくい、見積りを受領しても、適切な価格設定か判断ができない。
●・セキュリティに関する情報源がバラバラであるため、情報収集に苦労している
●・世の中や他社の情報セキュリティの潮流・動向は多くの場合は開示されないが、成功事例や失敗事例などで、サイバー攻撃・犯罪に活かすことができるコミュニティーがあれば参加したい。
・情報が少なく、どのように情報セキュリティの運用をすべきか悩む場合がある。相談先やかけこみ寺のような相手先（業者）を求めているが、費用面もありなかなか見つからない。
●本アンケートの結果を教えてください
●どこまで対策をすれば良いのかを決めるのが難しい。

●国外との情報通信などは国策としてセキュリティ対策の実施を検討していただきたい。
●厚労省やAmazon、三井住友カード、楽天カードなどをかたるメールが毎日大量に届く。各社に確認した上で、削除などをしているが、各社も対応のしようが無いようだ。取引のある銀行などからのメールであれば間違えてメール文中のリンクをクリックしてしまう恐れもある。メインのメールアドレスのため、変更もできない。迷惑メールに設定しても、違うアドレスで再び送信してくるのでいたちごっこになっている。
●日々進化する外部環境について行くのが大変である。
●技術的対策などセキュリティ対策等に関する内容については、機微な情報が含まれるため、関連する問いに関して「未回答」とさせていただきます。事情をお察しいただきますようお願いいたします。
●情報セキュリティ対策は重要な事柄と認識をしているが、何から手を付ければ良いのか不明なところがあり、後手に回ってしまっている。
●総体的な情報セキュリティ教育の実施について

不正アクセス行為対策等の実態調査　付録資料

付録１：調査票
付録２：集計表

付録１

１． 組織的対策

【貴社・団体について伺います】

問１． 貴社・団体は、どの業種に該当しますか。（○は一つ）

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

（太枠線内にご回答ください）

問２． 貴社・団体の従業員は、どのくらい在籍されていますか。（○は一つ）

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

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

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

【情報システム等の環境について伺います】

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

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

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

１．全て許可している
２．パソコン・タブレットを許可している
３．スマートフォンを許可している
４．許可していない
５．把握していない

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

１．行っている
└→ 問6-1～6-2へお進みください

２．行っていない
└→ 問6-3へお進みください

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

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

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

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

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

１．行う必要がない
２．業務の特性上行えない
３．以前行っていたがやめた
４．技術不足のためできない
５．資金不足のためできない
６．ルール作りや教育ができない
７．今後導入を計画している
８．その他（　　）

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

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

問８．　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９．　クラウドサービスを利用していますか。（○は一つ）

１．使用している　　３．わからない

２．使用していない

問 10.　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 11.　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11-1～11-4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. 新型コロナウイ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12へ
お進みください

問 11-1.　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（パソコン、スマートフォン等）の盗難

11. 外部記録媒体の盗難

12. インターネットバンキング不正送金

13. ランサムウェア

14. その他データ盗用（キーロガー含）

15. その他（　　）

16. 実質的な被害はなかった

【→攻撃手段は？】

１．DDoS 攻撃

２．踏み台（バックドア設置等）

３．部外からの不正アクセス

４．ウイルス等の感染

５．システム損壊、データ改ざん

６．内部の者のネットワーク悪用

７．関連会社や取引先等を経由

８．不明

９．その他（　　）

問 11-2.　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. クラウドの設定を見直した
18. 不明
19. その他（　　）
20. 特に何も対策を講じていない

問 11-3.　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
２．IPA（情報処理推進機構）
３．JPCERT/CC
４．国民生活センター・消費生活センター
５．監督官庁
６．個人情報保護委員会
７．その他（　　）
８．届け出なかった　→　**問11-4へお進みください**

〈届出・相談した理由〉へお進みください

〈届出・相談した理由〉

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

問 11-4.　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 12.　不正アクセス等の攻撃・被害に遭われた場合の届出先を知っていますか。それはどこですか。（○は一つ）

１．具体的な届出先（　　）
２．わからない

問 13.　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 14.　情報セキュリティ対策を行っていますか。（○は一つ）

1．行っている　→ 問14-1～14-8へお進みください

2．行っていない又は把握していない　→ 問14-9へお進みください

問 14-1.　問 14 で「1．行っている」と回答された方に伺います。情報セキュリティに関して、その運用、管理を専門に行う部署はありますか。（○は一つ）

1．ある
2．ない
3．今後設置予定

問 14-2.　問 14 で「1．行っている」と回答された方に伺います。情報セキュリティに関する管理体制は、どのようになっていますか。（○はいくつでも）

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

問 14-3.　問 14 で「1．行っている」と回答された方に伺います。情報セキュリティポリシー等は、策定されていますか。（○は一つ）

1．策定している　→ 問14-3-1へお進みください
2．現在、策定作業中である
3．今後、策定する予定である。
4．今のところ、策定する予定はない
5．策定しない
6．非公開情報のため、答えられない

→ 問14-4へお進みください

問 14-3-1.　問 14-3 で「1．策定している」と回答された方に伺います。新型コロナウイルス感染拡大の影響又はテレワーク業務の開始により、情報セキュリティポリシー等を変更しましたか。（○は一つ）

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

問 14-4.　問 14 で「1．行っている」と回答された方に伺います。不正アクセス等の侵害事案が発生した場合のために、現在、対応マニュアルや要領等を策定しておられますか。（○は一つ）

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

問 14-5.　問 14 で「1．行っている」と回答された方に伺います。情報システムのセキュリティ対策について、第三者機関の認証制度等を利用していますか。
（○はいくつでも）

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

問 14-6.　問 14 で「1．行っている」と回答された方に伺います。次年期（年単位）の情報セキュリティ対策の投資総額については、今年期（年単位）と比較してどのようになりますか（未定の場合は見込みでご回答ください）。（○は一つ）

1．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
8．把握していない

問 14-7.　問 14 で「1．行っている」と回答された方に伺います。これらの経費に関しては、どういった問題点が考えられますか。（○はいくつでも）

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

問 14-8.　問 14 で「1．行っている」と回答された方に伺います。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。（○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14-8を回答後、問15へお進みください

問 14-9　問 14 で「2．行っていない又は把握していない」と回答された方に伺います。なぜ、情報セキュリティ対策を行っていませんか。

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

問 15.　ビジネスメール詐欺について知っておられましたか。（○は一つ）

１．知っていた　→ 問15-1へお進みください

２．知らなかった　→ 問16へお進みください

問 15-1.　問 15 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。（○はいくつでも）

１．手口や実態に関する周知・教育
２．メール受信の対応訓練
３．メールによる口座情報送受信の禁止
４．メール以外の方法で口座情報を確認
５．対策を検討中
６．対策はしていない
７．不明
８．その他（　　）

問 16.　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

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

問 17.　OS やアプリケーションのセキュリティ・パッチの適用や更新状況をお答えください。
（○は一つ）

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

【情報セキュリティサービスの利用状況について伺います】

問 18.　現在、どのようなサービスを利用されていますか。（○はいくつでも）

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

問 18-1.　問 18 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 19.　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．バックアップの取得
13．その他（　　）
14．特に行っていない

問 20.　問７で「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」と回答された方に伺います。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．IEEE802.1X
７．電磁波の遮蔽
８．その他（　　）
９．特に行っていない

問 21.　問９でクラウドサービスを「１．使用している」と回答された方に伺います。
クラウドサービスを使用することになった理由は何ですか。（○はいくつでも）

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

問 22.　問 10 で外部から内部ネットワークへの接続を「１．許可している」と回答された方に伺います。
どのような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 23.　問 10 で外部から内部ネットワークへの接続を「１．許可している」と回答された方に伺います。従業員等が社外等からインターネット接続経由で業務アクセスを行う場合に利用しているのはどういった認証方法ですか。

（○はいくつでも）

問23-1～23-2へお進みください

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

問23-2へお進みください

問 23-1.　問 23 で「１．ＩＤ・パスワード等による認証」と回答された方に伺います。ＩＤ・パスワード等の管理を徹底するために、どのような対策をされていますか。（○はいくつでも）

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

問 23-2　不正ログイン（他人のＩＤ・パスワードを無断で入力する不正アクセス行為）を防止するために、どのような対策をされていますか。（○はいくつでも）

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

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

問 24.　各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）を利用していますか。（○は一つ）

１．使用している　→　問24-1へお進みください。

２．使用していない　→　問25へお進みください。

問 24-1.　当該サービスは、どのように管理されていますか。（○は一つ）

１．自社管理

２．一部外部業者に委託　→　問24-2～24-4へお進みください。

３．全て外部業者に委託　→　問25へお進みください。

問 24-2.　問 24-1 で「１．自社管理」「２．一部外部業者に委託」と回答された方に伺います。セキュリティ対策は、どのような取組みをされていますか。（○はいくつでも）

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

問 24-3.　問 24-1 で「１．自社管理」「２．一部外部業者に委託」と回答された方に伺います。過去 1 年間にシステムのぜい弱性検査（ペネトレーションテスト等）を実施しましたか。（○はいくつでも）

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

問 24-4.　問 24-1 で「１．自社管理」「２．一部外部業者に委託」と回答された方に伺います。ログは取得後、どれくらいの期間保管されていますか。また、どの様な方法で行っておられますか。（下表の各欄に、取得しているログの種類は該当する番号に○を、ログの保管期間及び方法は回答群Ａ（保管期間）・Ｂ（方法）からそれぞれ回答を選び、番号をご記入ください。）

※　回答が複数あるときは、最も長い期間を選んでご記入ください。

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 25 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24-4-1へお進みください

問 24-4-1.　問 24-4 で１～８の選択肢を回答された方に伺います。ログを取得・保管されているのは、どのような理由からですか。（○はいくつでも）

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

【電子メールに対する情報セキュリティ対策について伺います】

問25.　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. クラウドサービスの利用
14. その他（　　）
15. わからない

問26.　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 27.　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 28.　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．重要なシステムへの個人所有端末装置（パソコン、スマートフォン等）の接続制限を行っている
９．無線 LAN の使用制限を行っている
10. 多要素認証を導入している
11. その他（　　）
12. 上記 1.～11. のような対策は行っていない

問 29.　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. 端末装置（パソコン、スマートフォン等）廃棄時の適正なデータ消去
11. 共有 ID・パスワードの禁止
12. 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. 端末装置等のエンドポイントセキュリティ製品（EDR 等）の導入
16. その他（　　）
17. 特に何も行っていない

問 30.　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31.　現在、情報セキュリティ教育を行っておられますか。（○は一つ）

１．実施している
２．実施を予定している（具体的に実施計画を立てている）
→ 問31-1～31-2へお進みください

３．実施していない
→ 問31-3へお進みください

問31-1.　問31で「１．実施している」「２．実施を予定している」と回答された方に伺います。情報セキュリティに関する教育では、どのような内容を行っておられますか。（○はいくつでも）

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

問31-2.　問31で「１．実施している」「２．実施を予定している」と回答された方に伺います。情報セキュリティに関する教育は、どのくらいの頻度で行われていますか。（○はいくつでも）

１．月に１回以上
２．年に数回
３．年に１回
４．２、３年に１回
５．採用、異動時等に実施
６．その他（　　）
→ 問31-2を回答後、問32へお進みください。

問31-3.　問31で「３．実施していない」と回答された方に伺います。なぜ実施しないのですか。（○はいくつでも）

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

問32.　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3年9月21日(火) 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@ccn-g.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	1
鉱業	0
その他	0
小計	1
製造業	
食品	14
繊維	4
紙・パルプ	3
化学	34
薬品	7
ゴム・窯業	9
非鉄金属	10
機械	29
電気機器	31
造船	0
輸送機器	11
精密機器	8
その他	26
小計	186
不動産・建築	
不動産	16
建築	29
その他（不動産・建築）	8
小計	53
金融	
銀行	21
証券	2
保険	2
クレジット	1
消費者金融	0
信用金庫・組合	0
その他	4
小計	30
エネルギー	
電力	4
ガス	3
水道	0
石油製造（ 精製）	2
その他	1
小計	10

運輸業	
鉄道・地下鉄	2
航空	1
陸運	4
海運	2
倉庫	4
その他	3
小計	16
情報通信	
新聞	0
放送	3
通信	4
ＩＳＰ	0
その他	4
小計	11
サービス	
流通・卸売	28
小売	25
娯楽・アミューズメント	0
飲食	4
ホテル・旅行	5
情報処理・ ソフトウェア	26
警備	1
医療・福祉	56
その他	42
小計	187
教育	
大学	90
短大	0
専門学校	0
その他	10
小計	100
行政サービス	
都道府県	2
政令指定都市	3
市町村	107
小計	112
無回答	10
合計	716

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1,843件抽出した。

・企業（1,595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（248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3年8月23日（月）（発送日）～9月21日（火）（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、1,843件を送付して、299件を回収し、回収率は16.2%であった。

全体での回収数299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45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15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33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

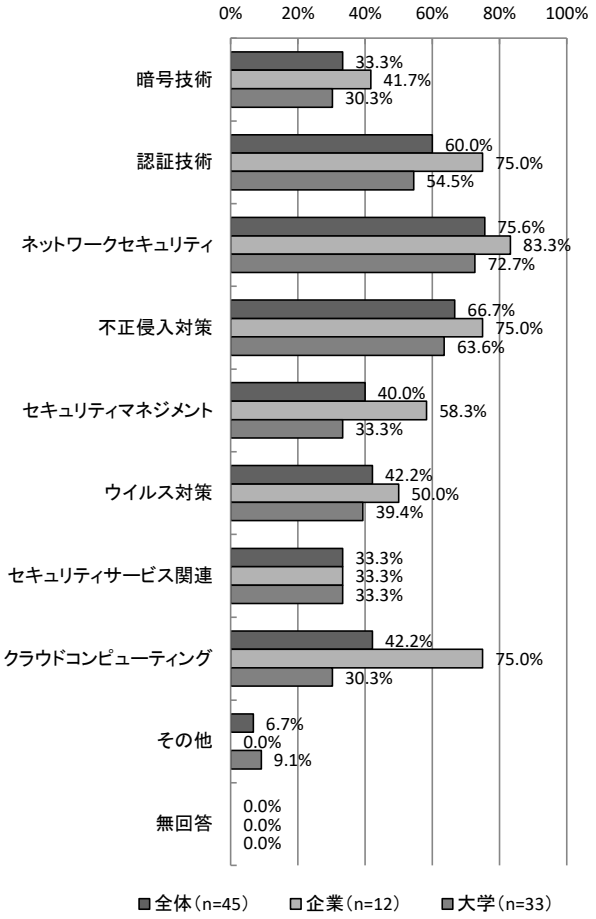
現在、取り組んでいる分野について、全体では「ネットワークセキュリティ」が最も多く、企業・大学いずれにおいても「ネットワークセキュリティ」が最も多くなっている。

今後、取り組んでいく分野について、全体では「ネットワークセキュリティ」が最も多く、企業・大学いずれにおいても「ネットワークセキュリティ」が最も多くなっている。

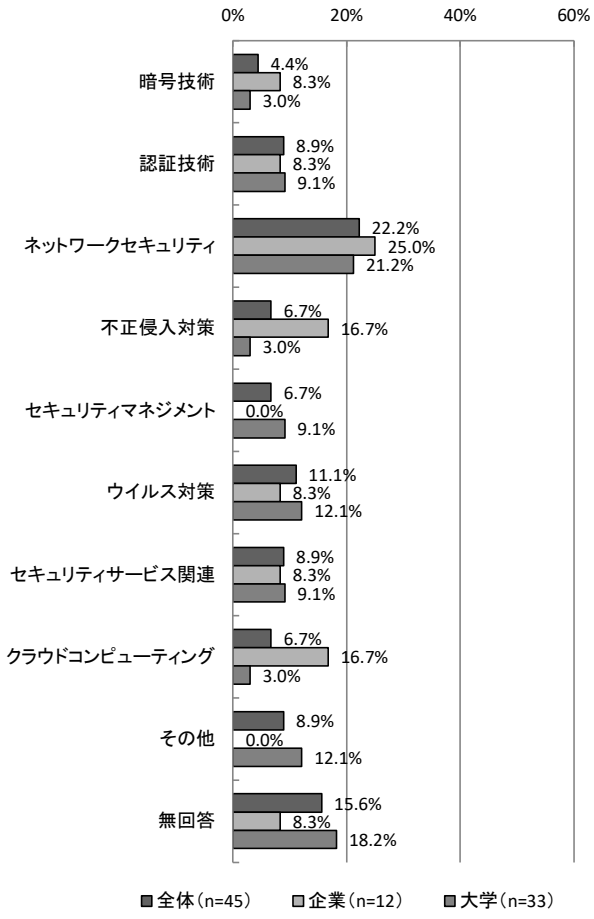
現在、取り組んでいる分野については、「ネットワークセキュリティ」が75.6%（34件）で最も多く、次いで「不正侵入対策」が66.7%（30件）となっている。企業では「ネットワークセキュリティ」が83.3%（10件）で最も多く、大学では「ネットワークセキュリティ」が72.7%（24件）で最も多い。

今後、もっとも力を入れたい分野については、「ネットワークセキュリティ」が22.2%（10件）で最も多く、次いで「ウイルス対策」が11.1%（5件）となっている。企業では「ネットワークセキュリティ」が25.0%（3件）、大学では「ネットワークセキュリティ」が21.2%（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】

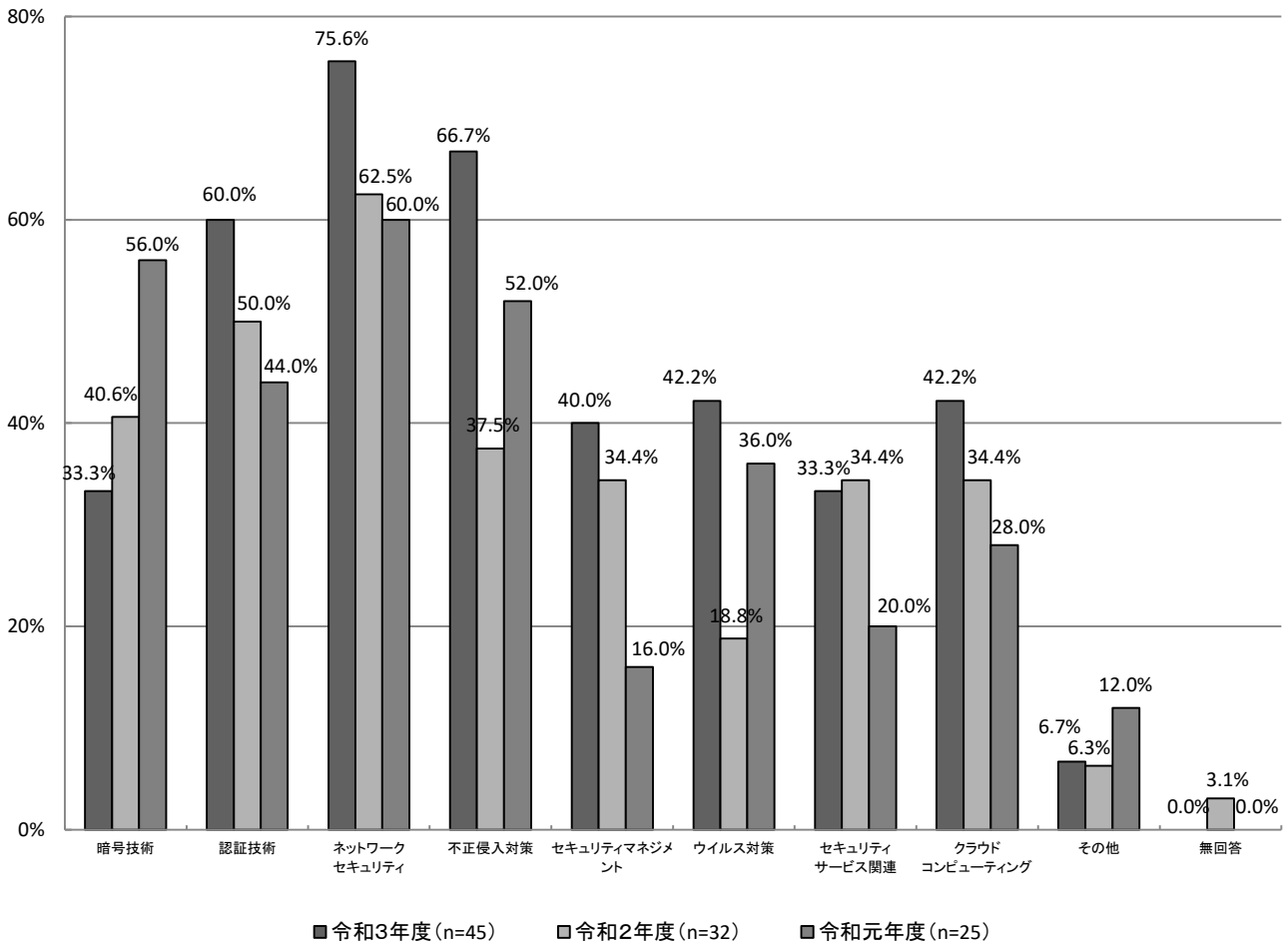
全体では、昨年度より増加または横ばいとなった分野が多く、特に「不正侵入対策」、「ウイルス対策」が大きく増加している。

企業では、「不正侵入対策」や「クラウドコンピューティング」が増加し、大学では、「不正侵入対策」や「ウイルス対策」が増加している。

【経年変化(全体)】

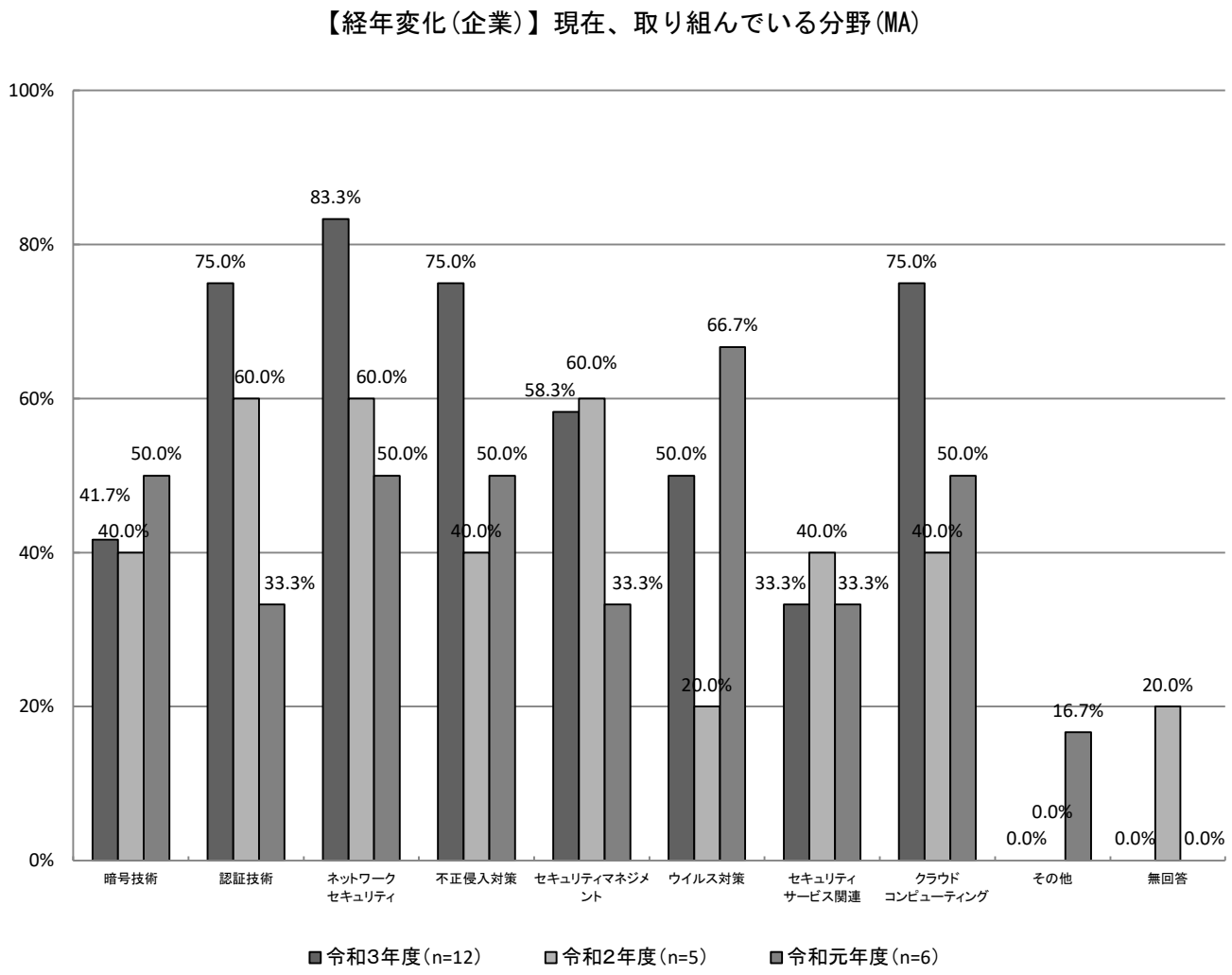
昨年度と比較すると全体では、「不正侵入対策」が29.2ポイント、「ウイルス対策」が23.4ポイント増加している。

【経年変化(全体)】現在、取り組んでいる分野(MA)



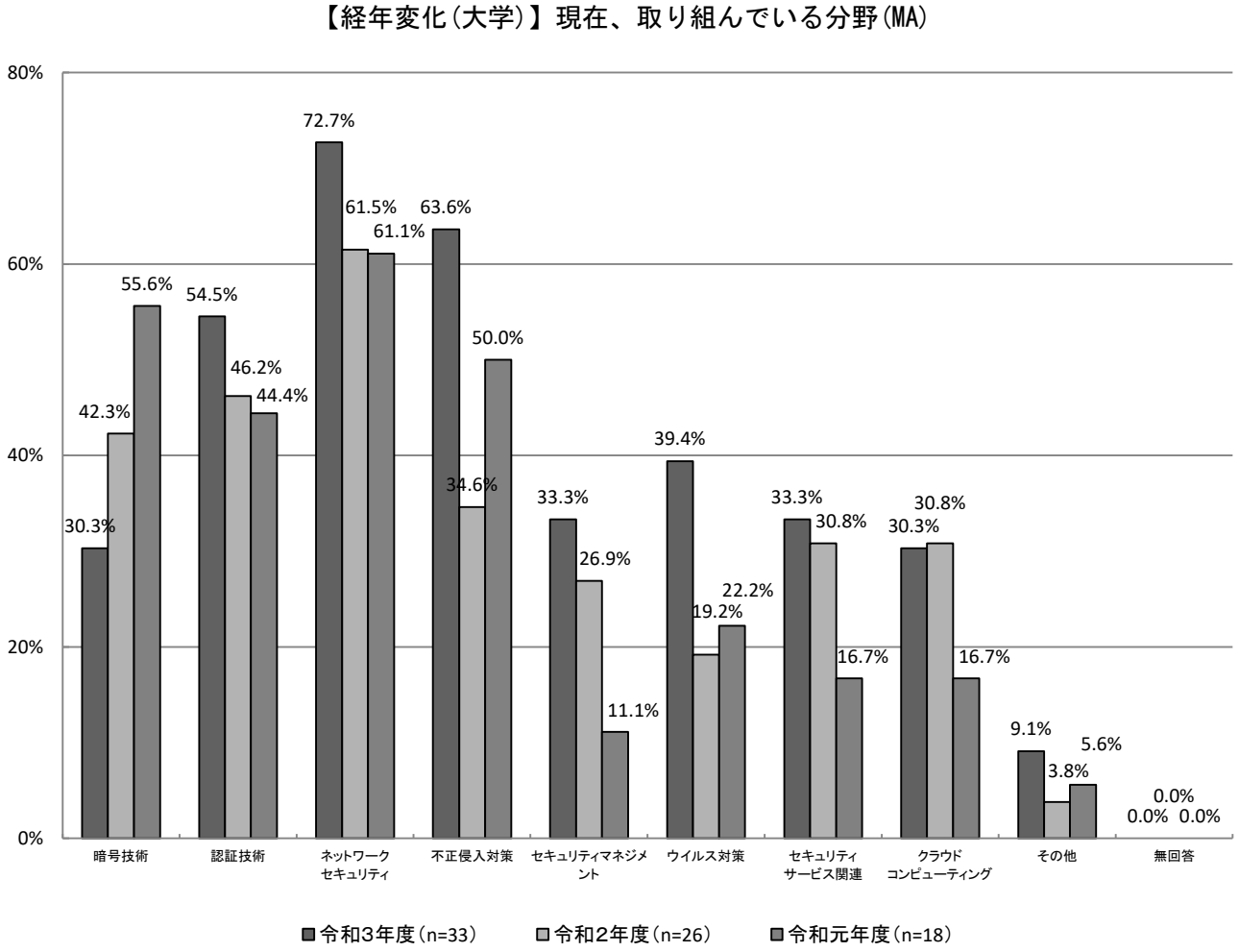
【経年変化(企業)】

昨年度と比較すると企業では、「不正侵入対策」「クラウドコンピューティング」が35.0ポイント増加している。



【経年変化(大学)】

昨年度と比較すると大学では、「不正侵入対策」が29.0ポイント、「ウイルス対策」が20.2ポイント増加している。

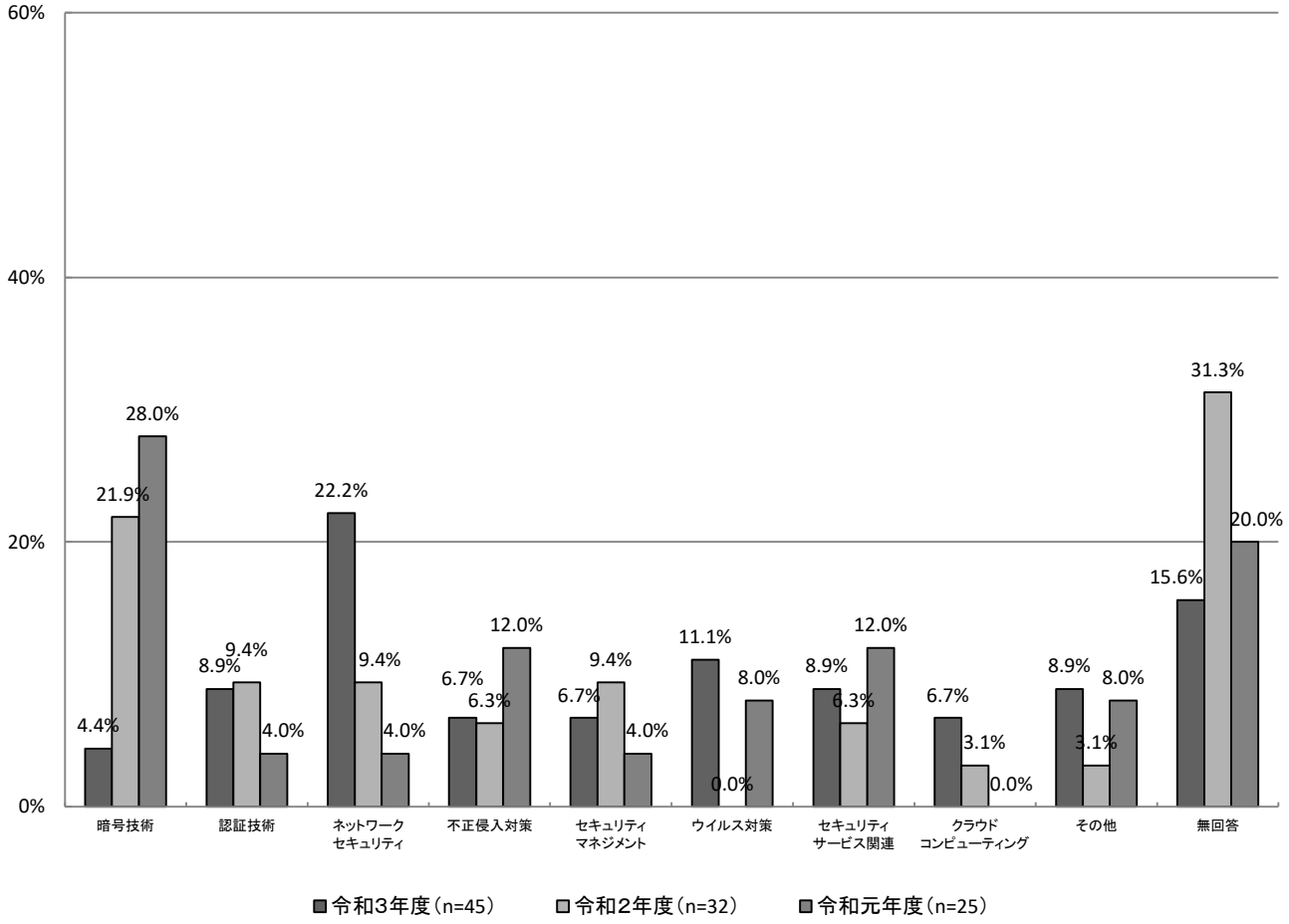


5.1.2　今後、もっとも力を入れたい分野　【A-問3】

【経年変化】
　全体では、「ネットワークセキュリティ」、「ウイルス対策」が増加し、「暗号技術」が減少している。
　企業では、「ネットワークセキュリティ」が昨年度より最も増加しており、大学では、「ウイルス対策」が昨年度より最も増加している。

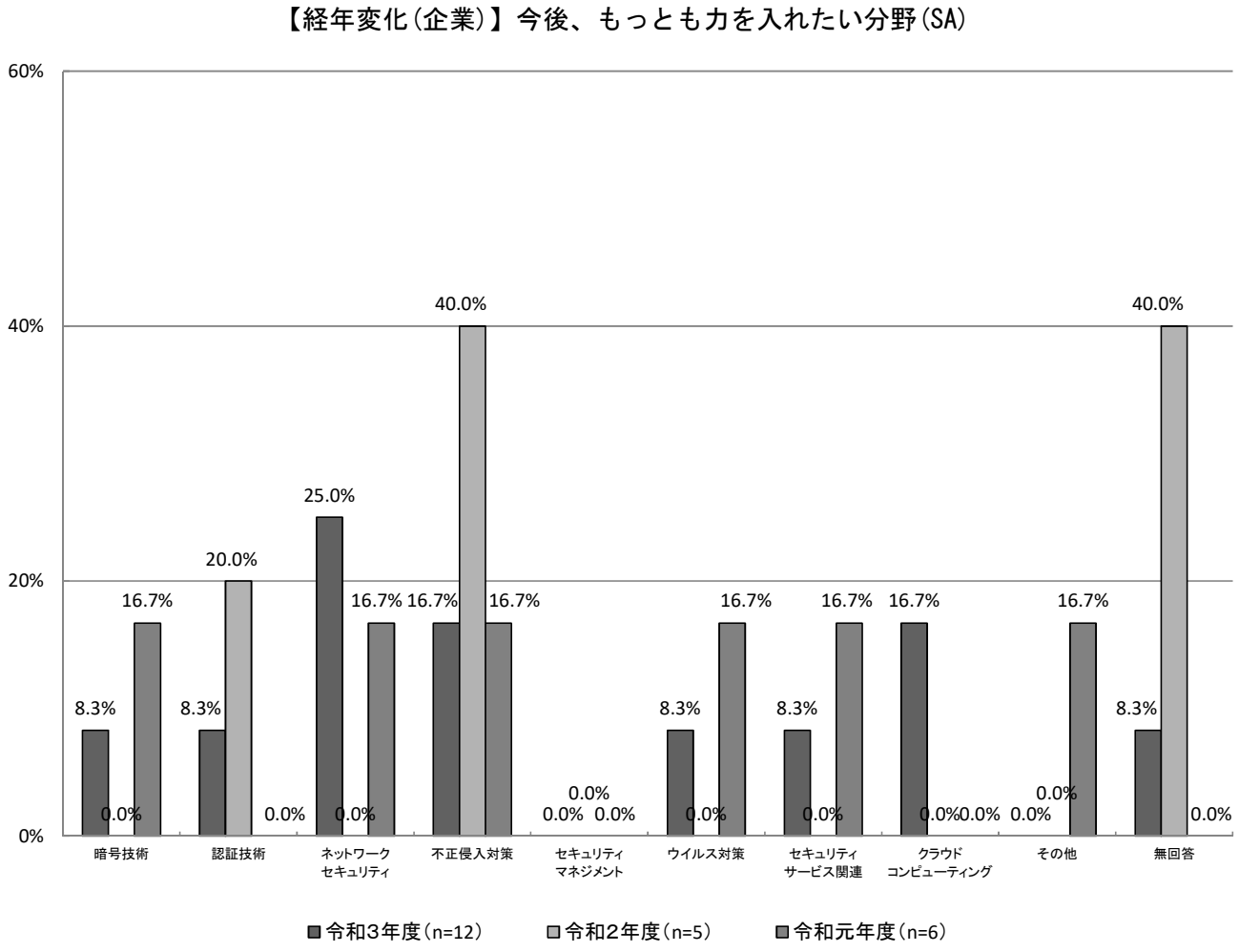
【経年変化(全体)】
　昨年度と比較すると全体では、「ネットワークセキュリティ」が12.8ポイント、「ウイルス対策」が11.1ポイント増加している。一方、「暗号技術」は17.5ポイント減少している。

【経年変化(全体)】今後、もっとも力を入れたい分野(SA)



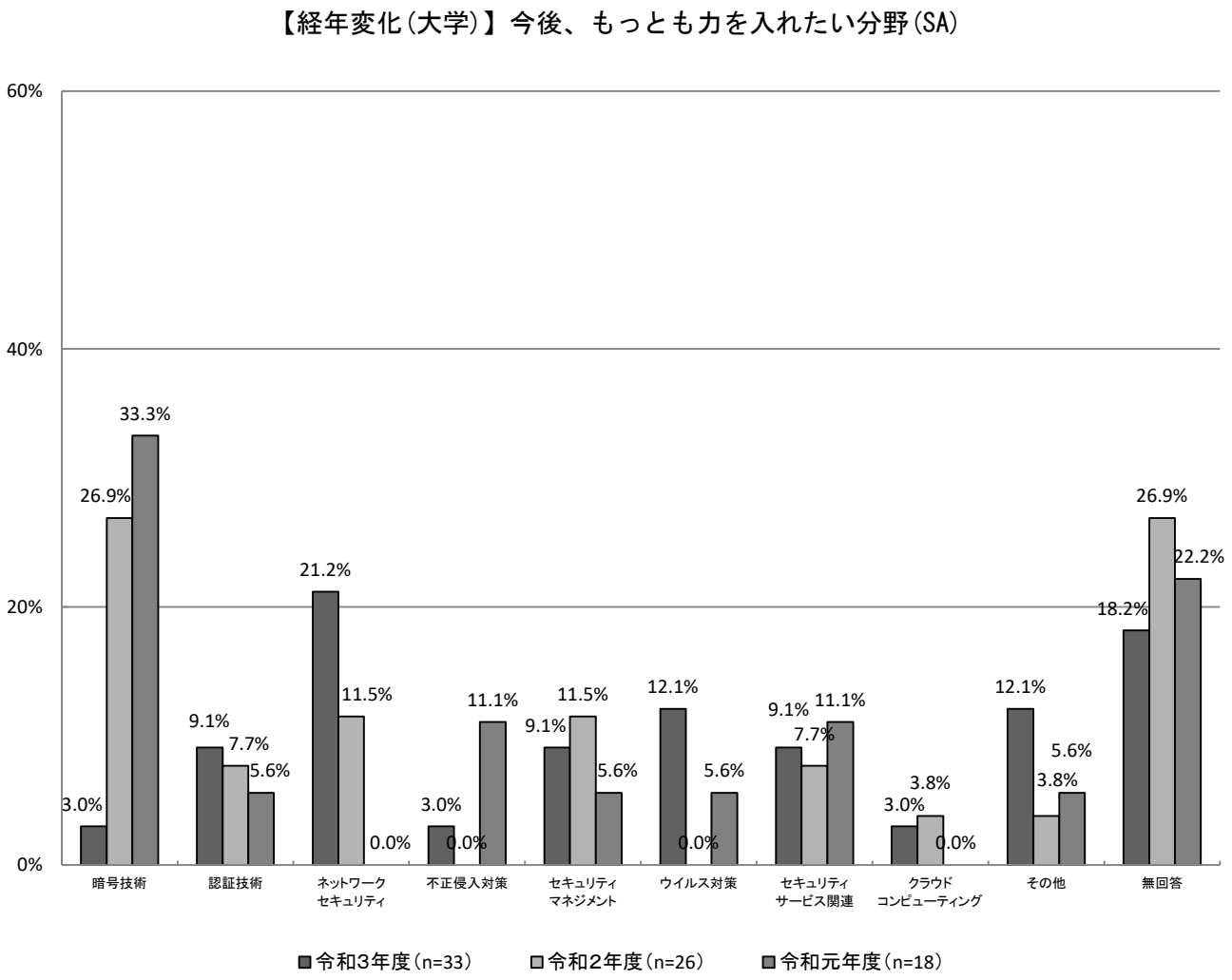
【経年変化(企業)】

昨年度と比較すると企業では、「ネットワークセキュリティ」が25.0ポイント、「クラウドコンピューティング」が16.7ポイントと増加している。一方、「不正侵入対策」は23.3ポイント減少している。



【経年変化(大学)】

昨年度と比較すると大学では、「ウイルス対策」が12.1ポイント増加している。一方、「暗号技術」は23.9ポイント減少している。

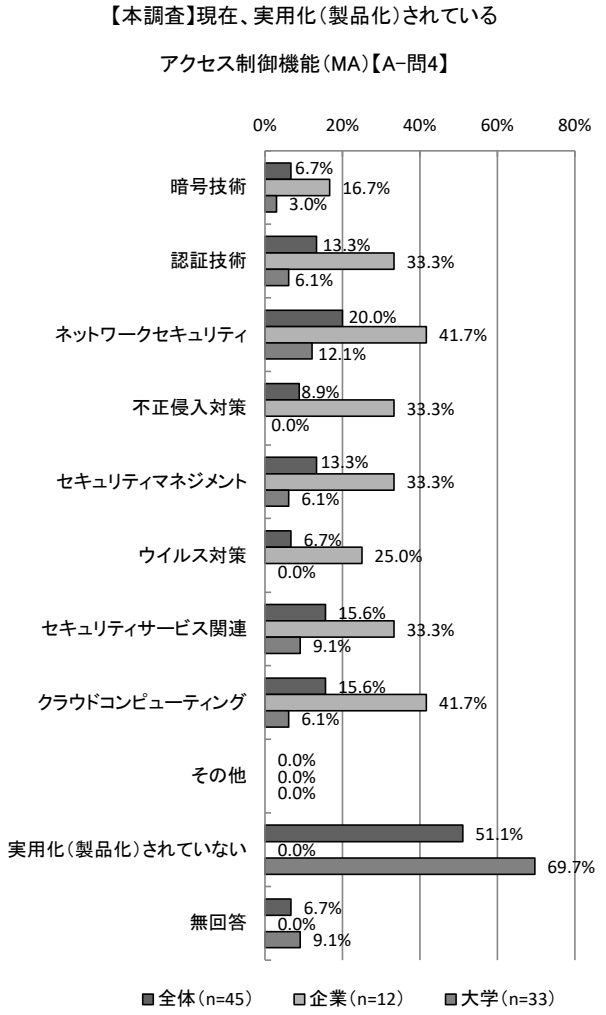


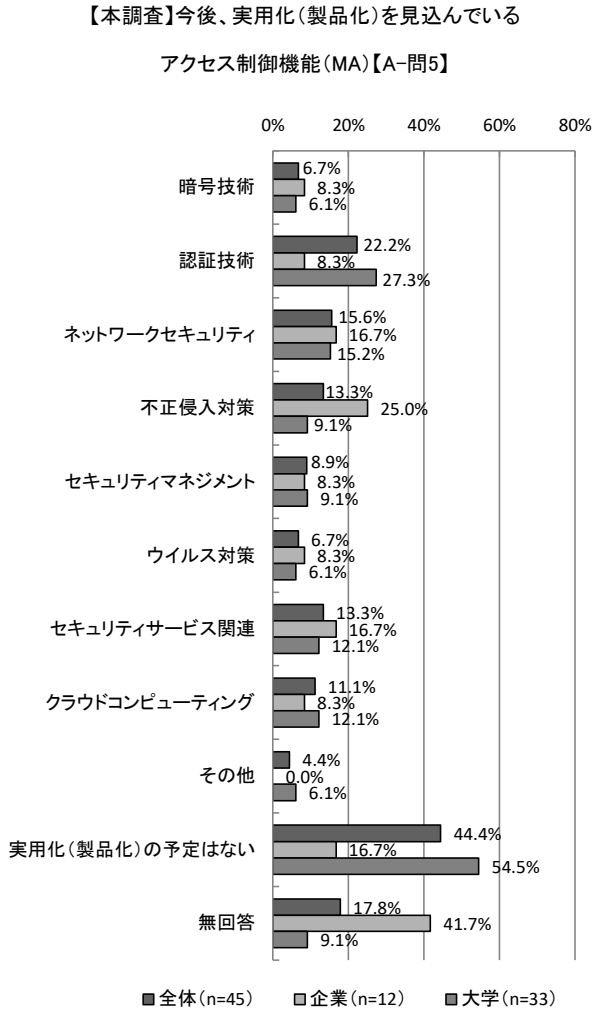
5.2　アクセス制御機能に関する実用化（製品化）に係る現状と今後の展望

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

現在、実用化（製品化）されている分野については、全体では「ネットワークセキュリティ」が20.0%（9件）で最も多く、次いで「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15.6%（7件）となっている。企業では「ネットワークセキュリティ」「クラウドコンピューティング」がそれぞれ41.7%（5件）で最も多く、大学では「ネットワークセキュリティ」が12.1%（4件）で最も多くなっている。

今後、実用化（製品化）を見込んでいる分野については、全体では「認証技術」が22.2%（10件）で最も多く、次いで「ネットワークセキュリティ」が15.6%（7件）となっている。企業では「不正侵入対策」が25.0%（3件）で最も多く、大学では「認証技術」が27.3%（9件）で最も多くなっている。



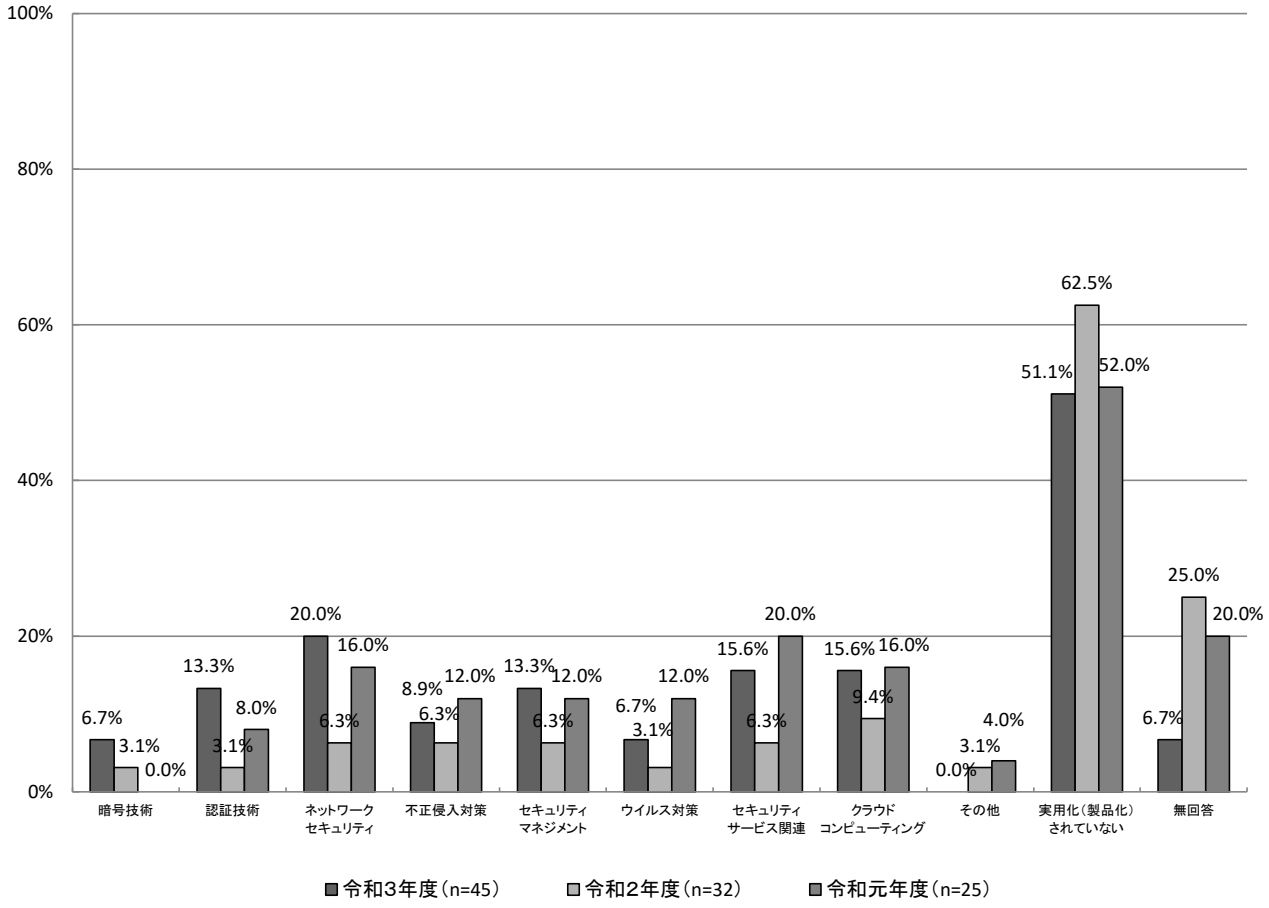


5.2.1　現在、実用化(製品化)されている分野　【A-問4】

【経年変化】
全体では、すべての分野で増加している。
企業では、「認証技術」が13.3ポイント増加し、大学では、すべての分野で増加または横ばいとなっている。

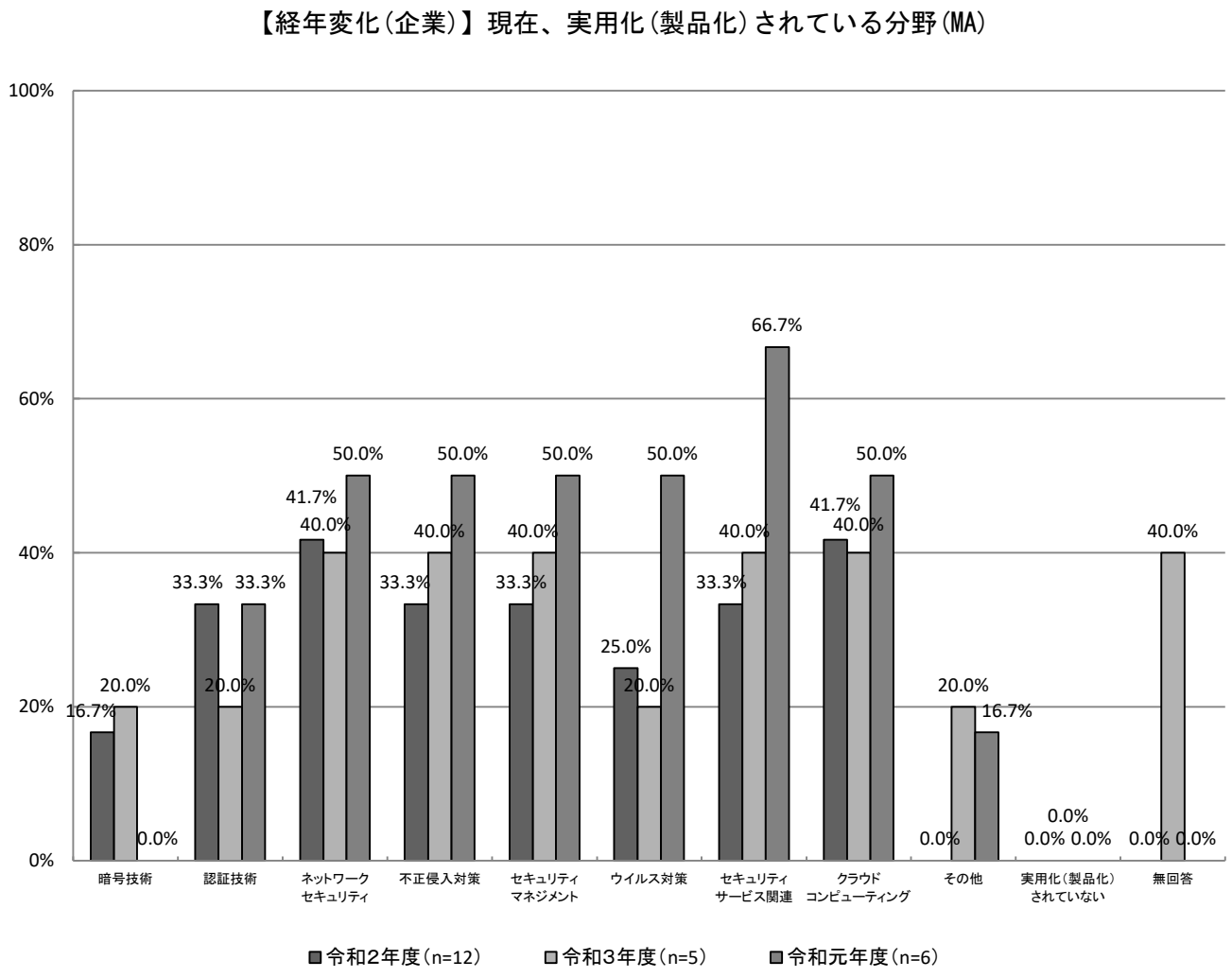
【経年変化(全体)】
昨年度と比較すると全体では、すべての分野で増加している。

【経年変化(全体)】現在、実用化(製品化)されている分野(MA)



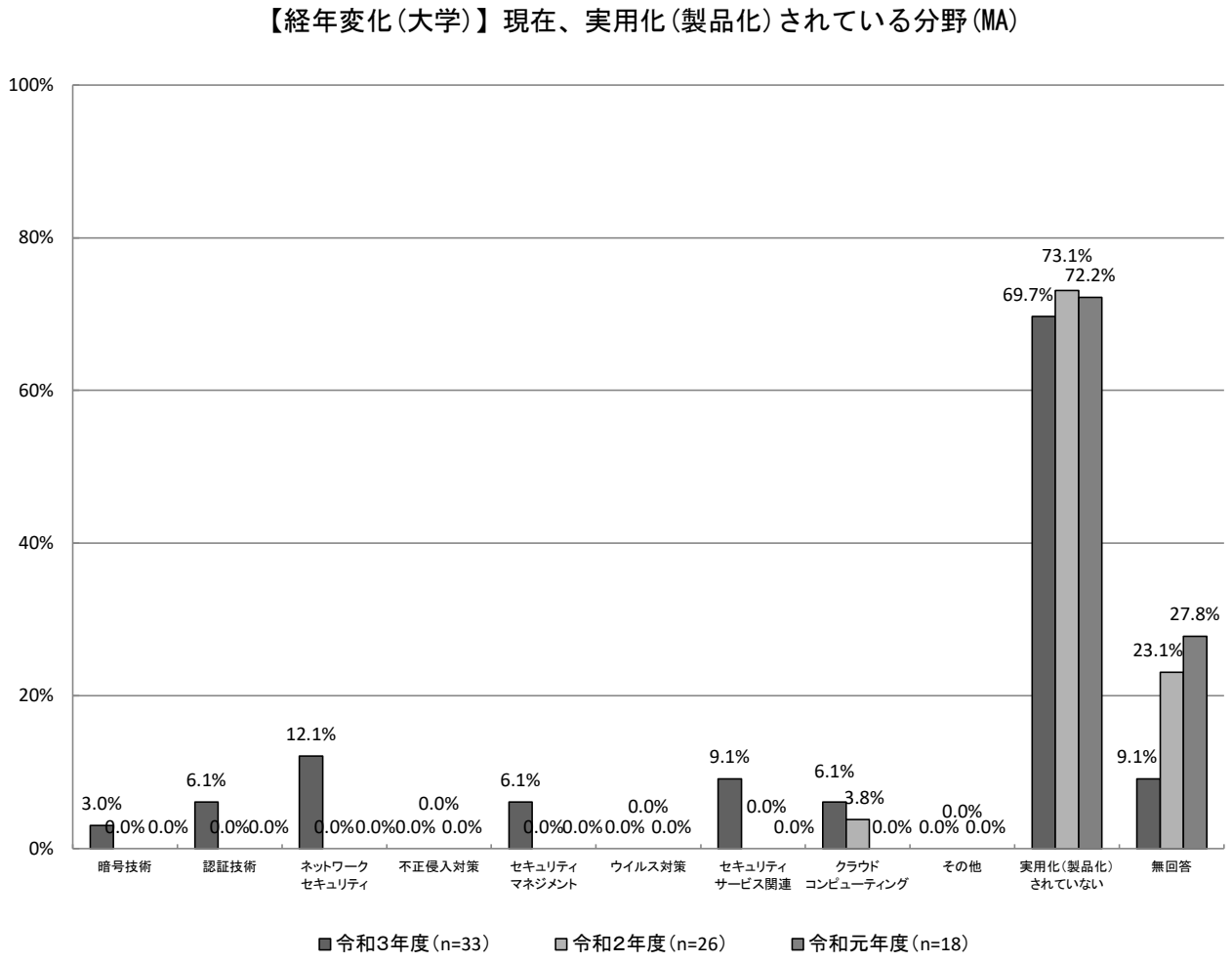
【経年変化(企業)】

昨年度と比較すると企業では、「認証技術」が13.3ポイント増加している。



【経年変化(大学)】

昨年度と比較すると大学では、すべての分野で増加または横ばいとなっている。

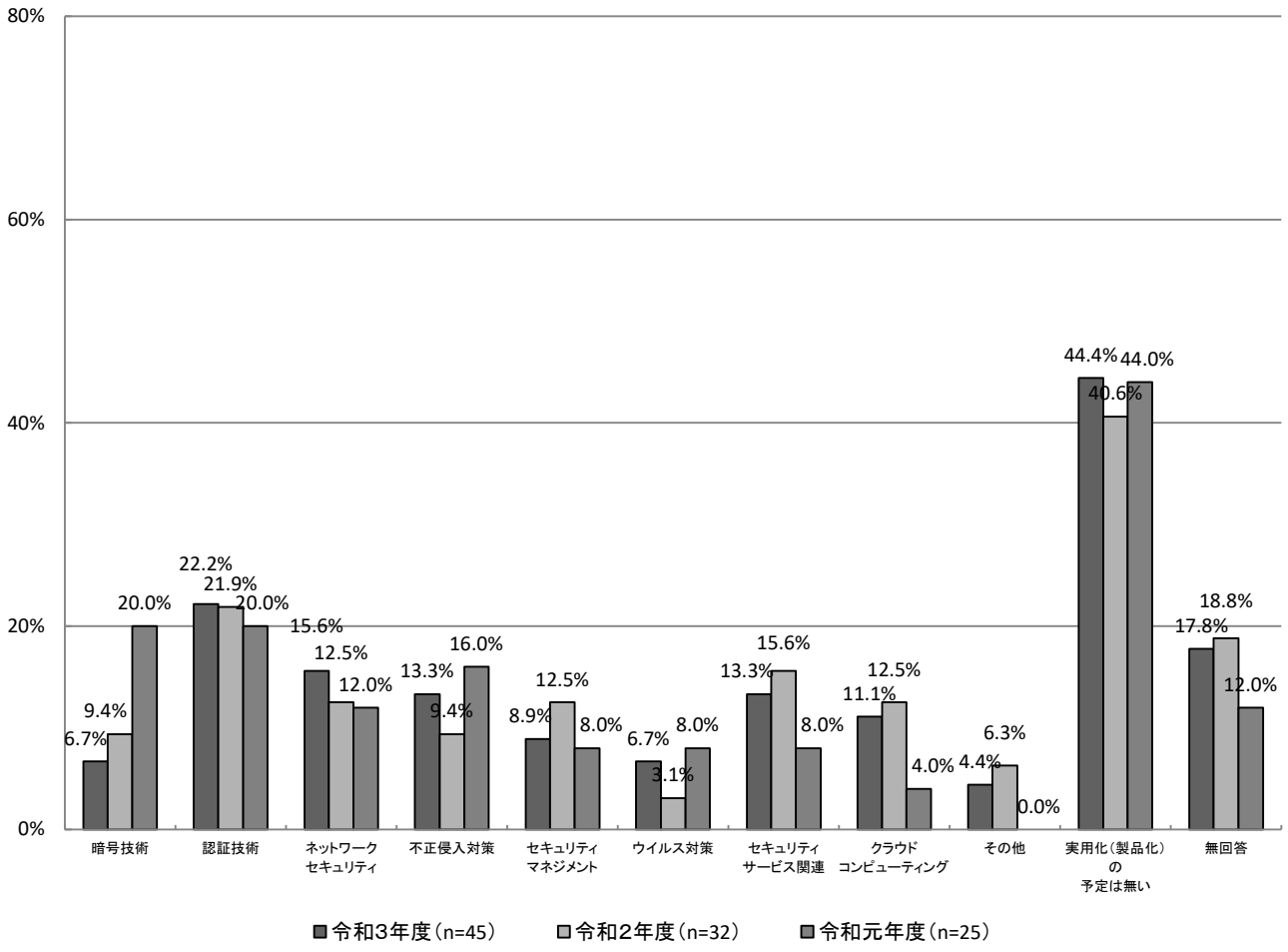


5.2.2　今後、実用化(製品化)を見込んでいる分野　【A-問5】

【経年変化】
全体では、「不正侵入対策」、「ウイルス対策」などが増加している。
企業では「不正侵入対策」、大学では「認証技術」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、「不正侵入対策」が3.9ポイント、「ウイルス対策」が3.6ポイント増加している。

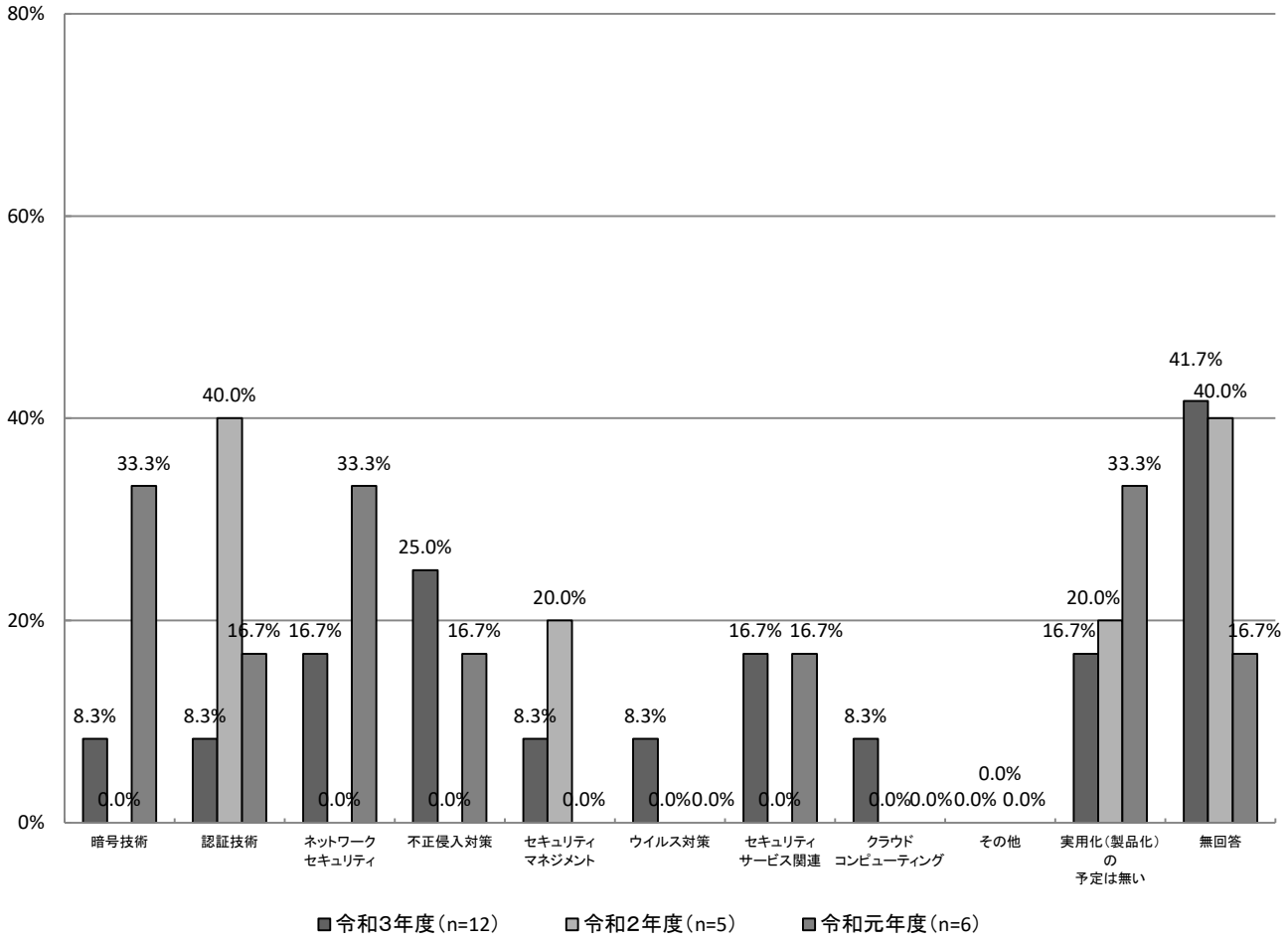
【経年変化(全体)】今後、実用化(製品化)を見込んでいる分野(MA)



【経年変化(企業)】

昨年度と比較すると企業では、「不正侵入対策」が25.0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」「セキュリティサービス関連」がそれぞれ16.7ポイント増加している。一方、「認証技術」は31.7ポイント減少している。

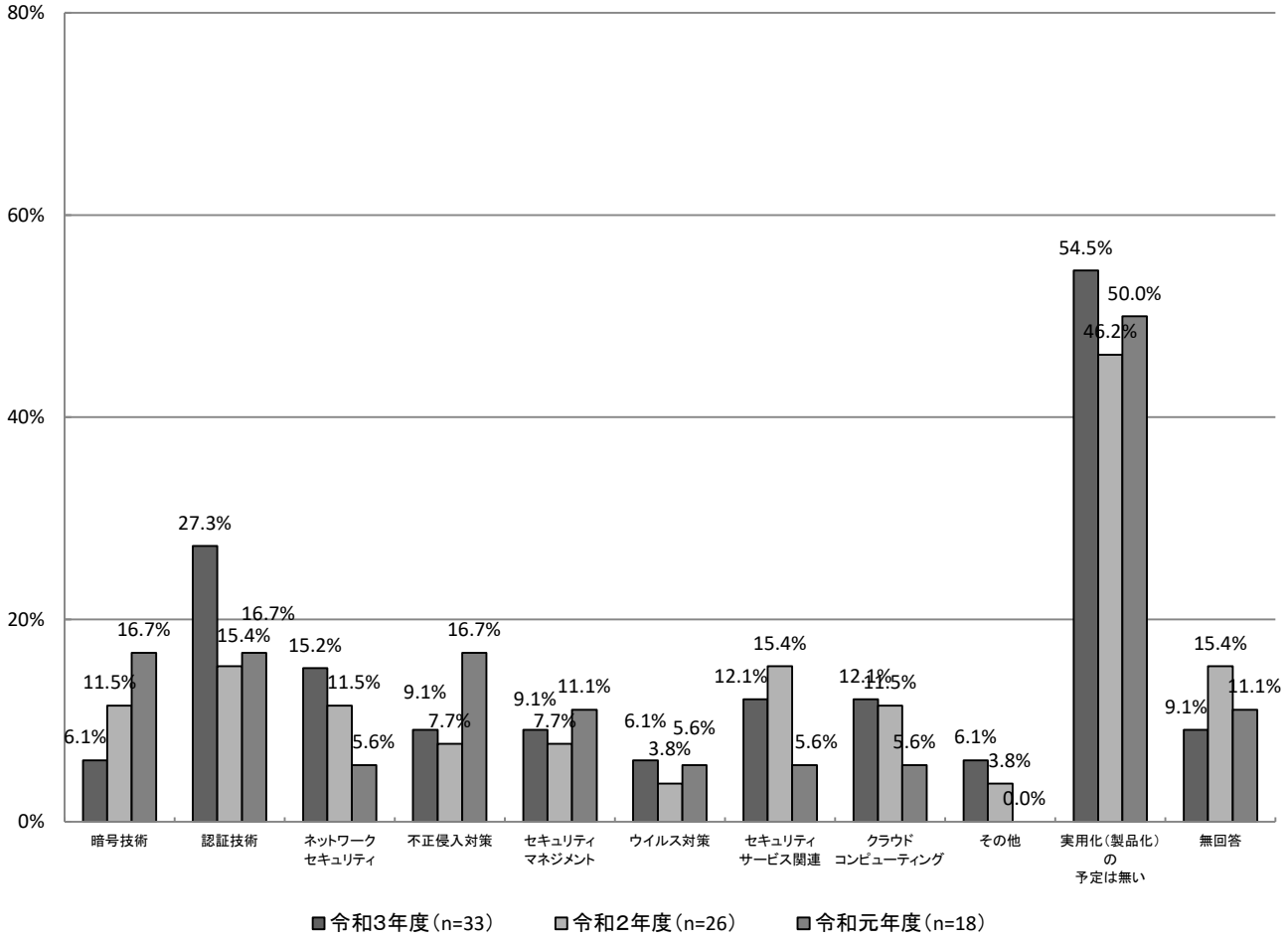
【経年変化(企業)】今後、実用化(製品化)を見込んでいる分野(MA)



【経年変化(大学)】

昨年度と比較すると大学では、「認証技術」が11.9ポイントと最も増加しており、次いで「ネットワークセキュリティ」が3.7ポイント増加している。一方、「暗号技術」は5.4ポイント減少している。

【経年変化(大学)】今後、実用化(製品化)を見込んでいる分野(MA)



5.3　研究開発体制

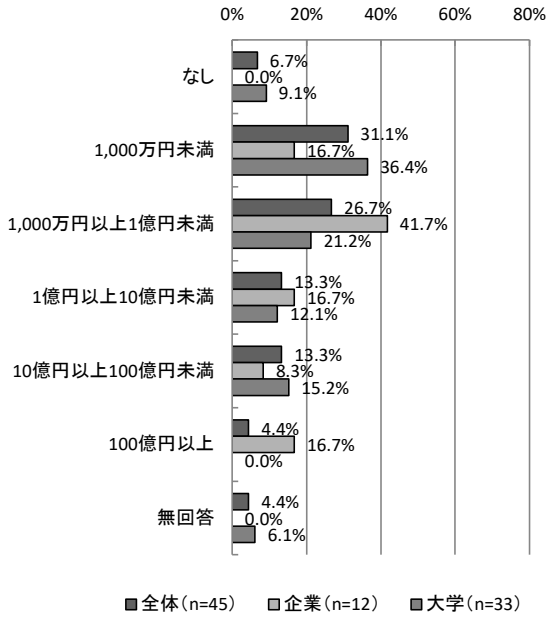
研究開発費について、企業は「1,000万円以上1億円未満」が最も多く、大学は「1,000万円未満」が最も多くなっている。

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

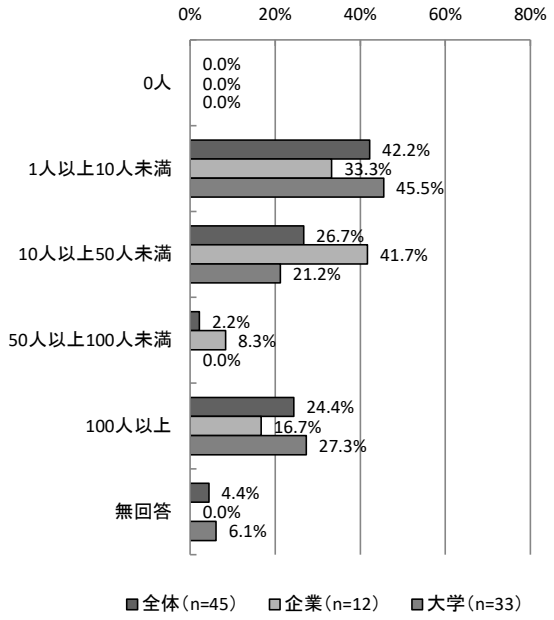
年間の研究開発費については、「1,000万円未満」が31.1%（14件）で最も多くなっている。企業では「1,000万円以上1億円未満」が41.7%（5件）で最も多く、大学では「1,000万円未満」が36.4%（12件）と最も多くなっている。

研究開発人員については、全体では「1人以上10人未満」が42.2%（19件）と最も多くなっている。企業では「10人以上50人未満」が41.7%（5件）で最も多く、大学では「1人以上10人未満」が45.5%（15件）で最も多くなっている。

【本調査】年間の研究開発費（SA）【A-問6】



【本調査】研究開発に携わっている人数（SA）【A-問7】

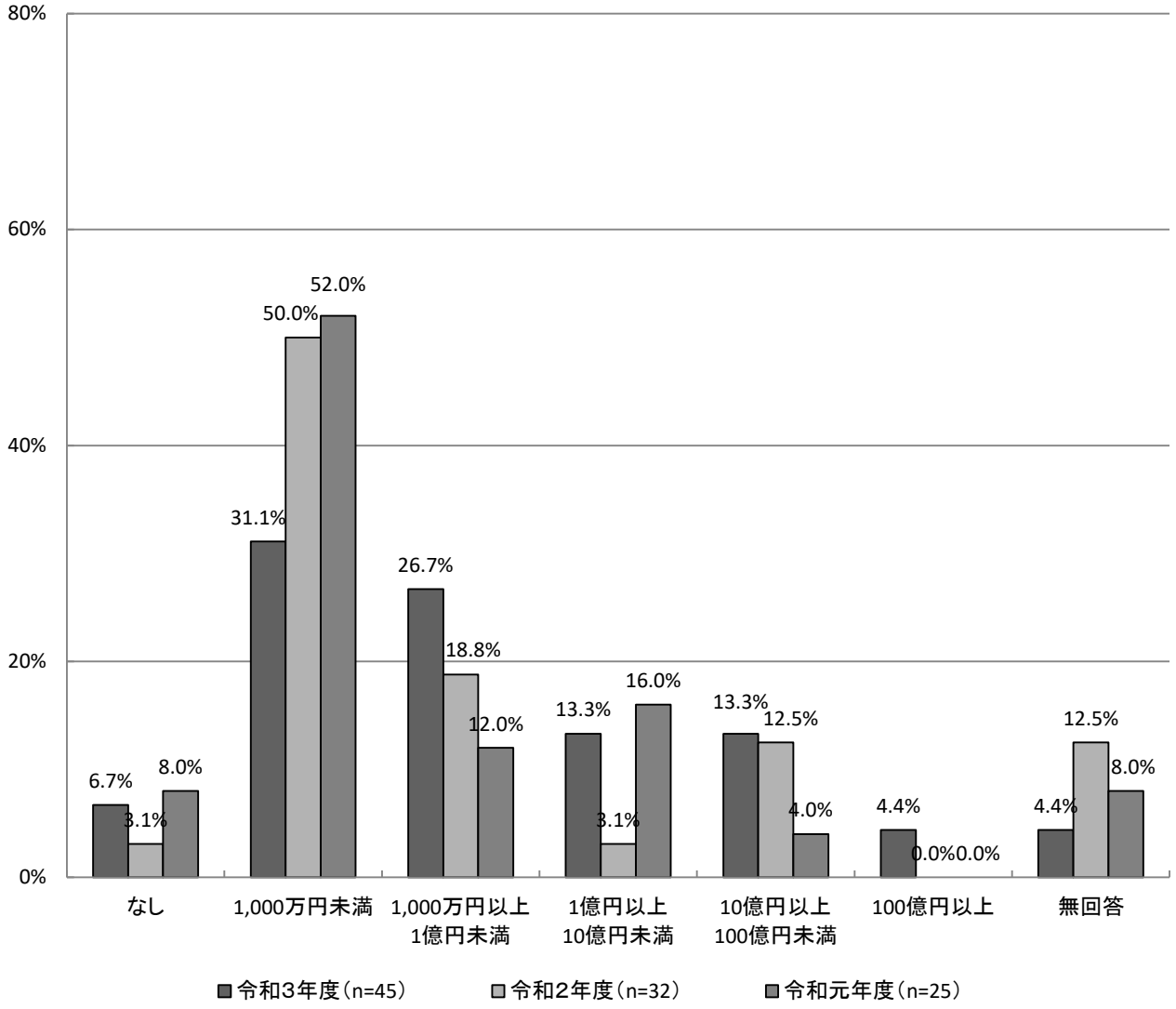


5.3.1　年間の研究開発費　【A-問6】

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

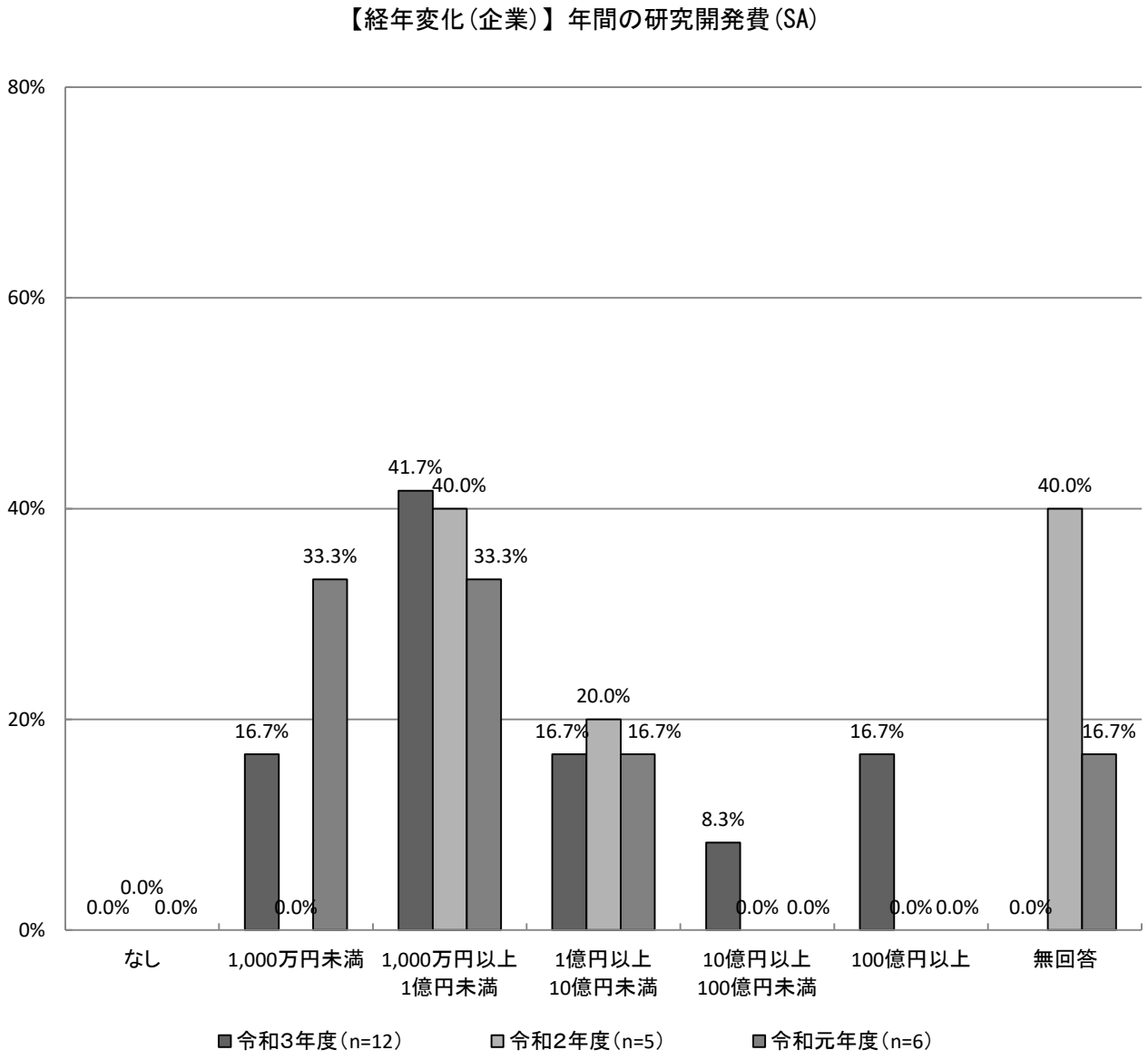
【経年変化(全体)】
昨年度と比較すると全体では、「1,000万円未満」が18.9ポイント減少している。一方、「1億円以上10億円未満」が10.2ポイント、「1,000万円以上1億円未満」が7.9ポイント増加している。

【経年変化(全体)】年間の研究開発費(SA)



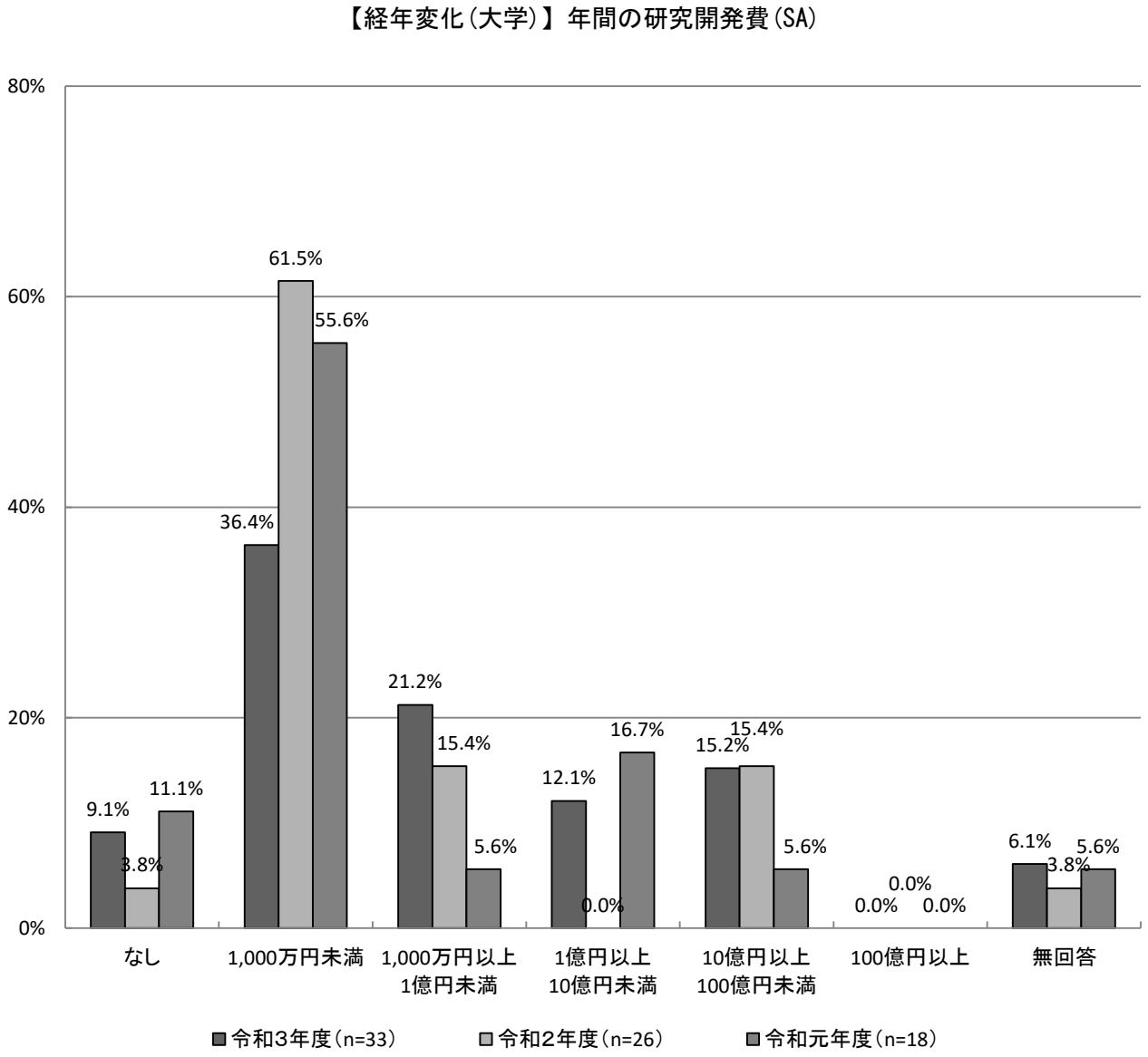
【経年変化(企業)】

昨年度と比較すると企業では、「1,000万円未満」「100億円以上」が16.7ポイントと最も増加している。



【経年変化(大学)】

昨年度と比較すると大学では、「1,000万円未満」が25.1ポイントと最も減少している。一方、「1億円以上10億円未満」が12.1ポイントと最も増加している。

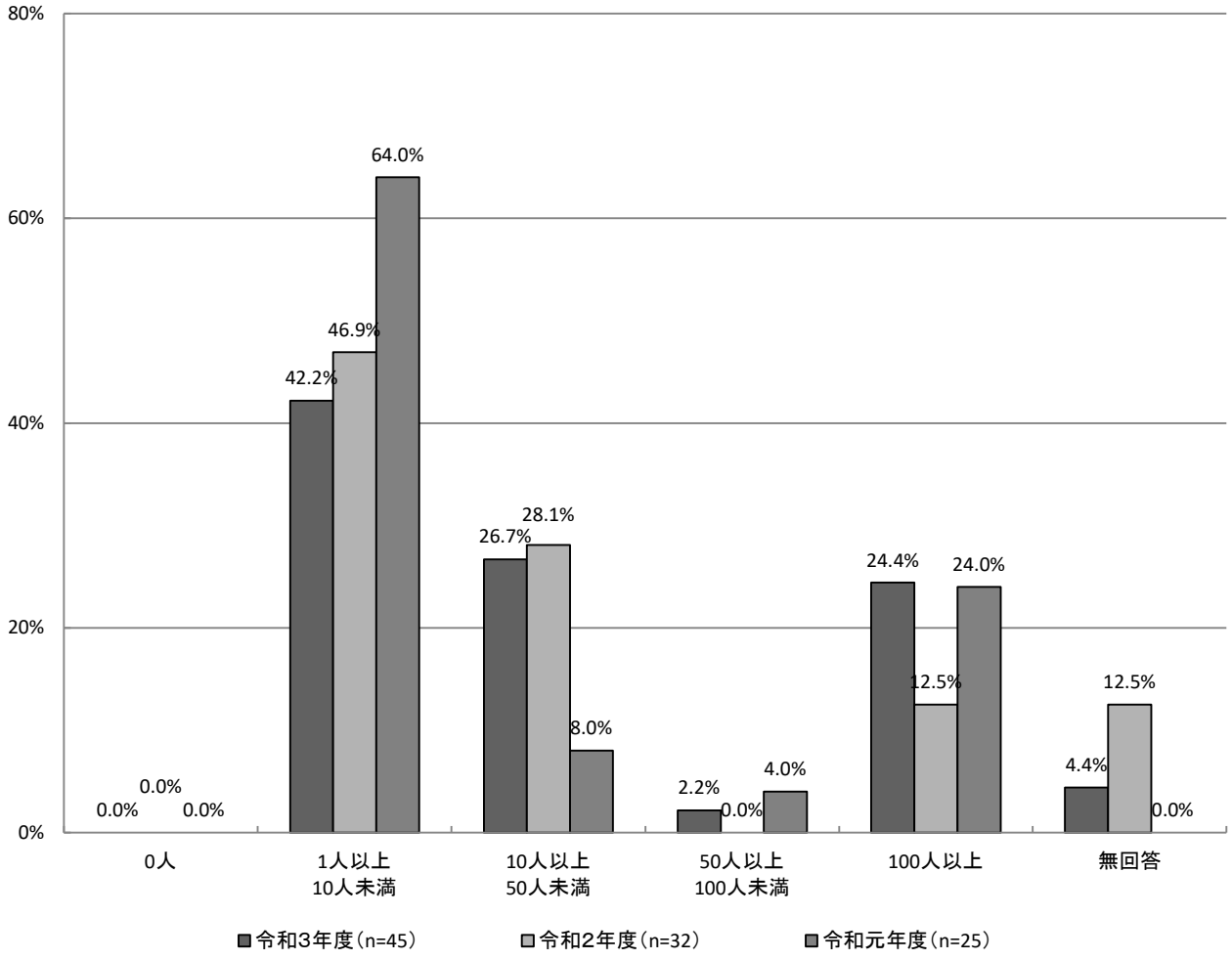


5.3.2　研究開発に携わっている人数　【A-問7】

【経年変化】
全体、企業及び大学では、昨年度より「100人以上」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、「100人以上」が11.9ポイント増加している。

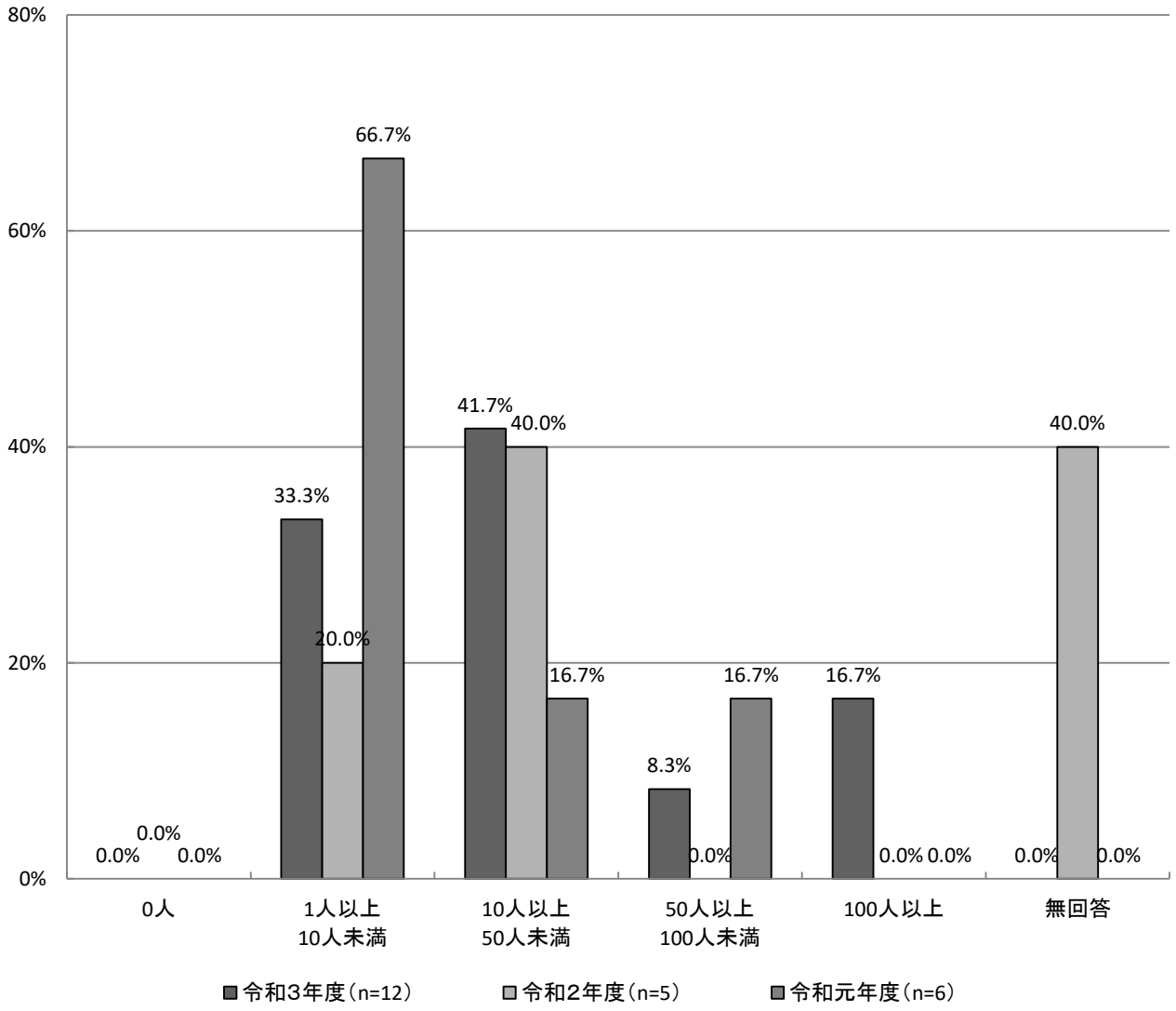
【経年変化(全体)】研究開発に携わっている人数(SA)



【経年変化(企業)】

昨年度と比較すると企業では、「100人以上」が16.7ポイント最も増加しており、次いで「1人以上10人未満」が13.3ポイント増加している。

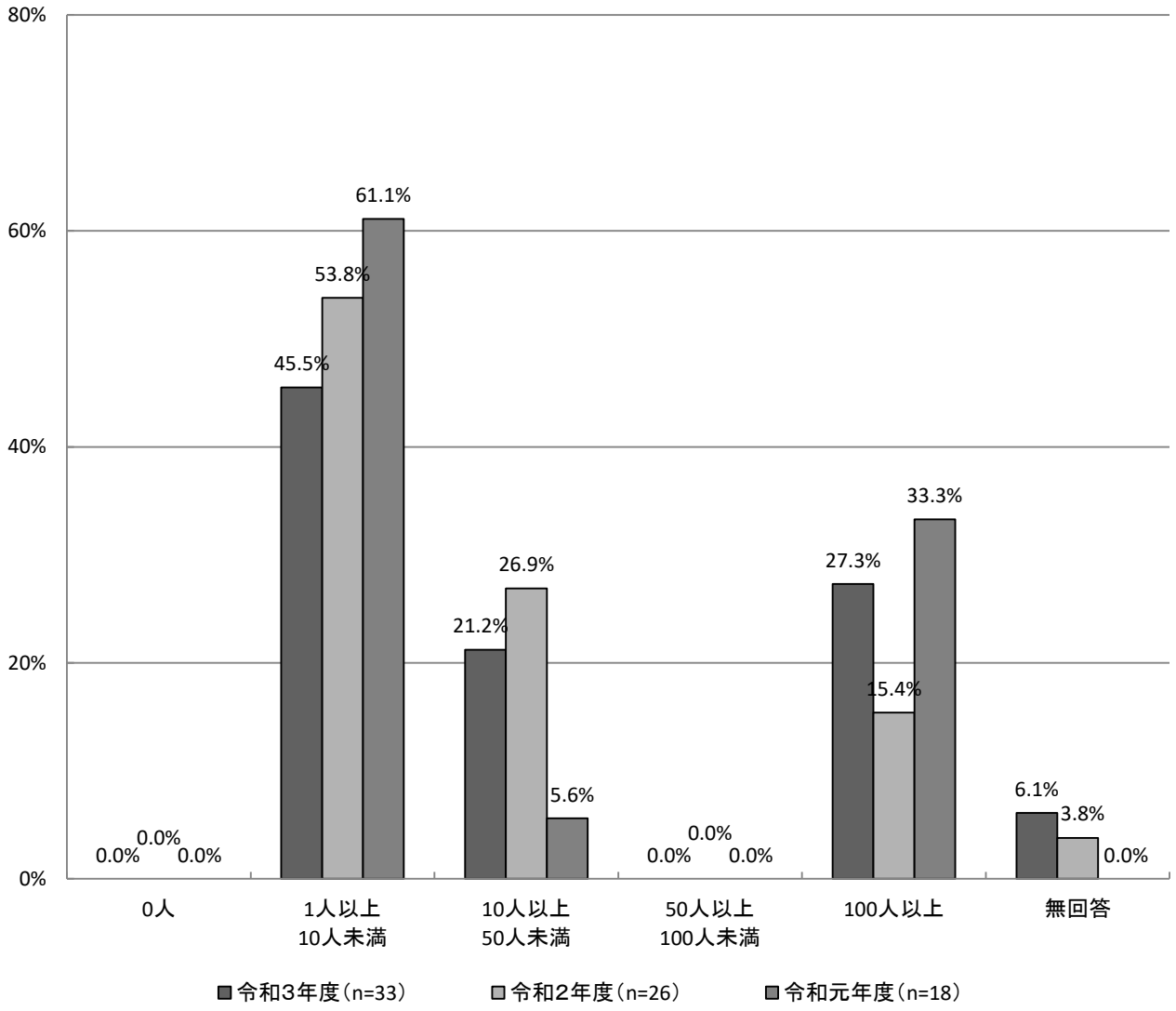
【経年変化(企業)】研究開発に携わっている人数(SA)



【経年変化(大学)】

昨年度と比較すると大学では、「100人以上」が11.9ポイントと最も増加している。一方「1人以上10人未満」は8.3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。

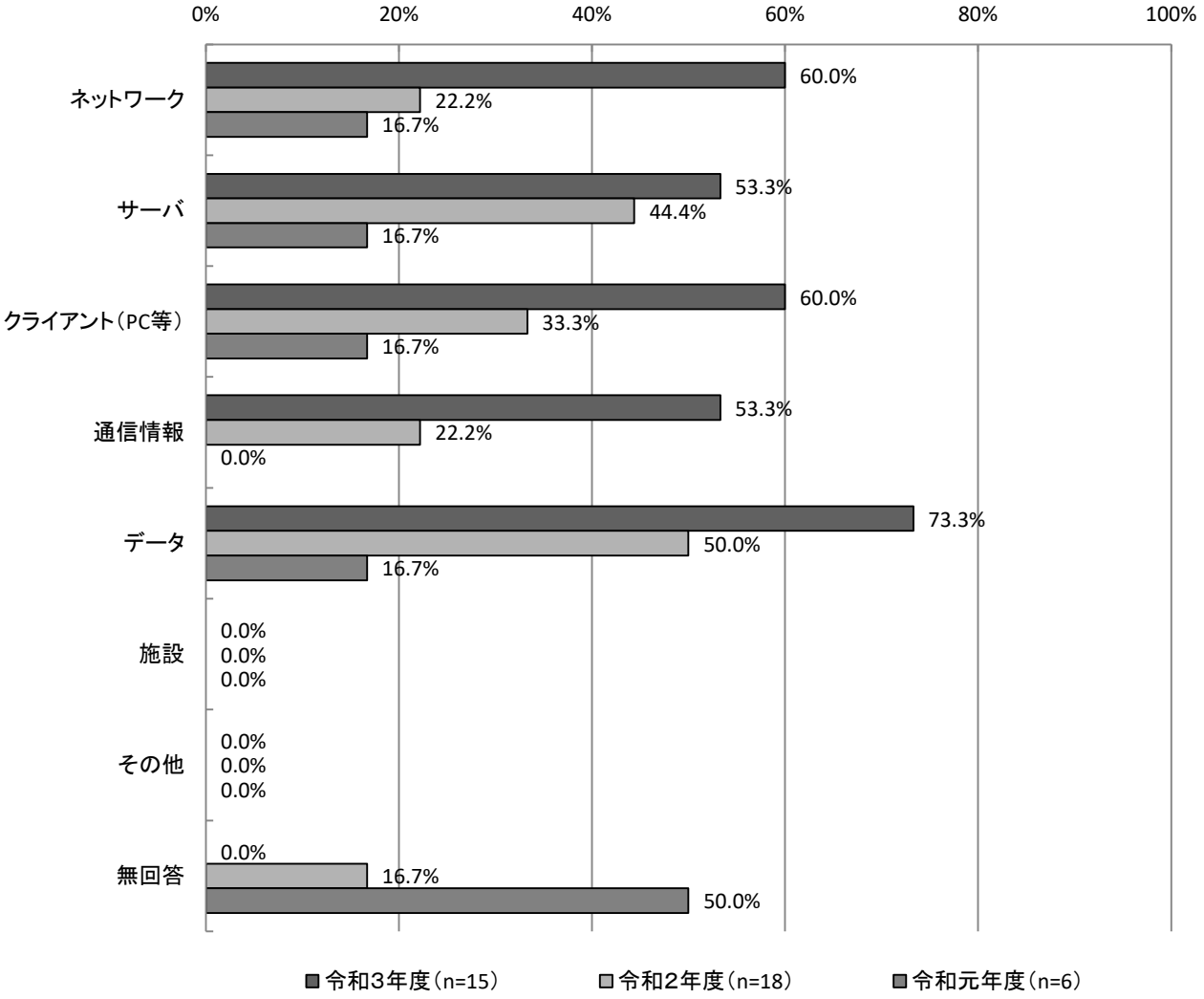
5.4.1　何を守るか？

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、「データ」が73.3%（11件）で最も多く、次いで「ネットワーク」「クライアント（PC等）」が60.0%（9件）となっている。

昨年度と比較すると、「ネットワーク」が37.8ポイント、「通信情報」が31.1ポイント、「クライアント（PC等）」が26.7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】



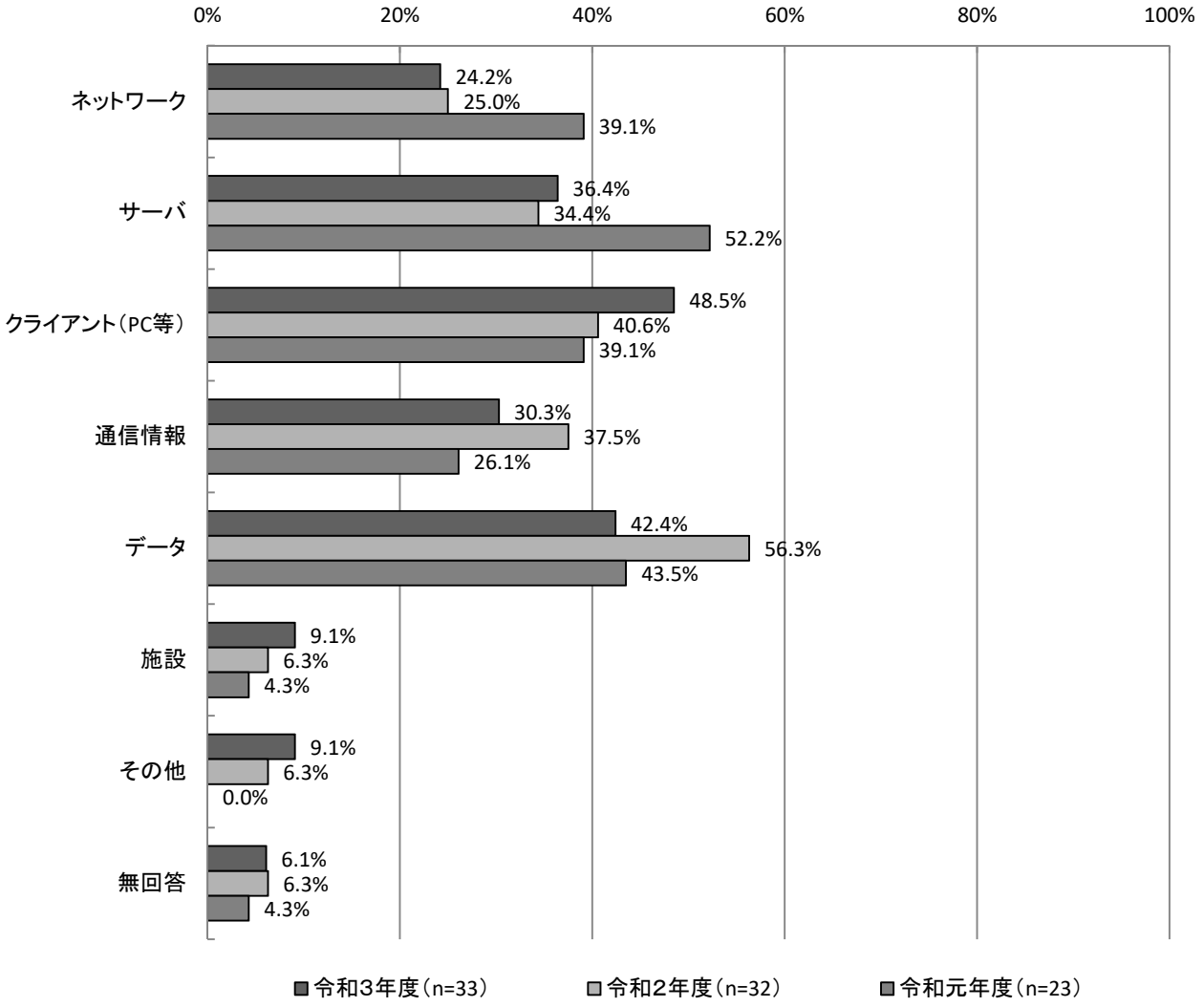
Ⅱ.研究開発中のもの

研究開発中のものについては、「クライアント（PC等）」が48.5%（16件）で最も多く、次いで「データ」が42.4%（14件）、「サーバ」が36.4%（12件）となっている。

昨年度と比較すると、「データ」が13.9ポイントと最も減少しており、次いで「通信情報」が7.2ポイント減少している。

【経年変化】何を守るか？

Ⅱ.研究開発中のもの(MA)【C-問1】



5.4.2　何から保護するか？

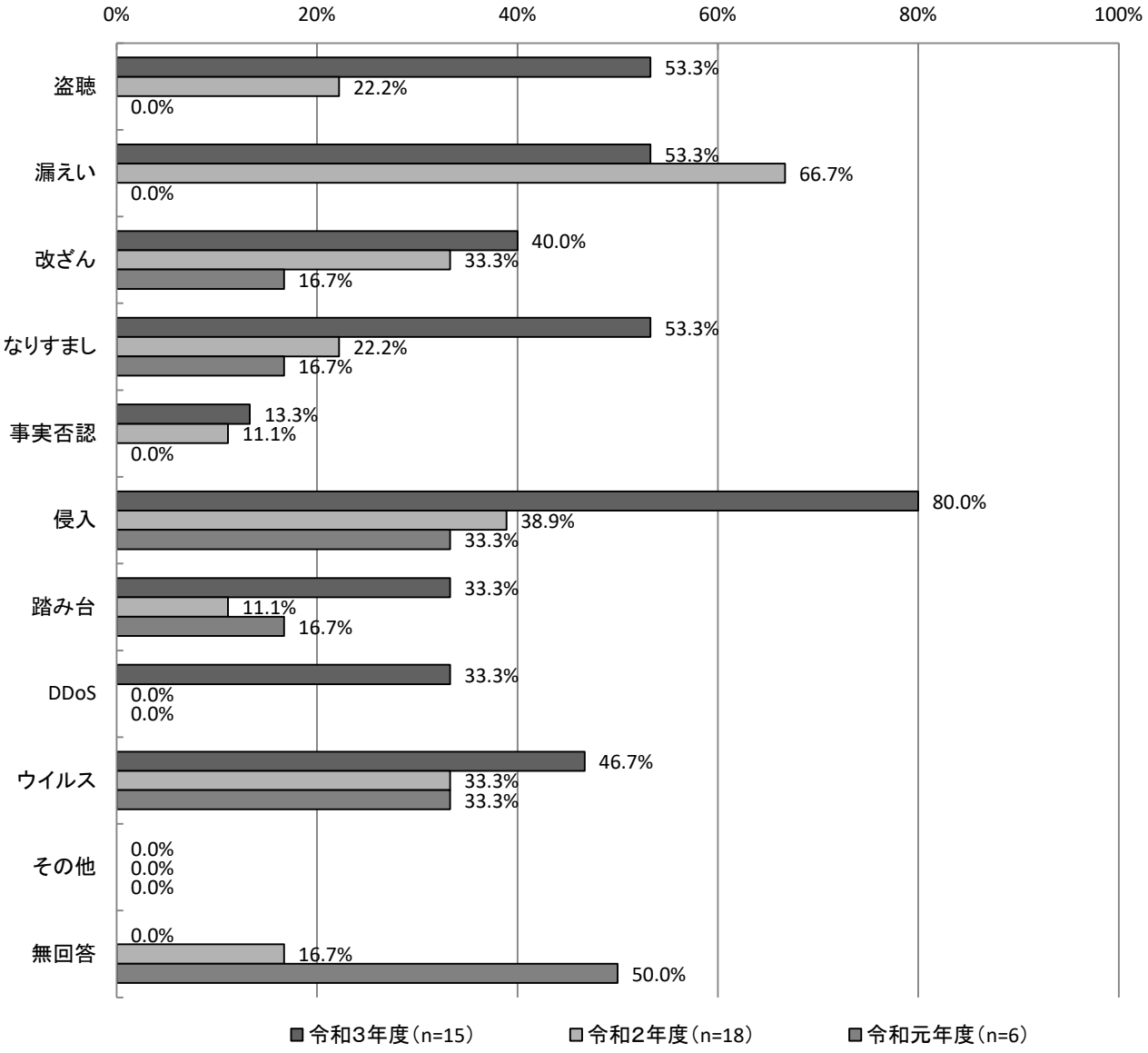
Ⅰ.実用化(製品化)されているもの

実用化（製品化）されているものについては、「侵入」が80.0%（12件）で最も多く、次いで「盗聴」「漏えい」「なりすまし」が53.3%（8件）となっている。

昨年度と比較すると、「侵入」が41.1ポイントで最も増加しており、次いで「DDoS」が33.3ポイント増加している。一方「漏えい」は13.4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】



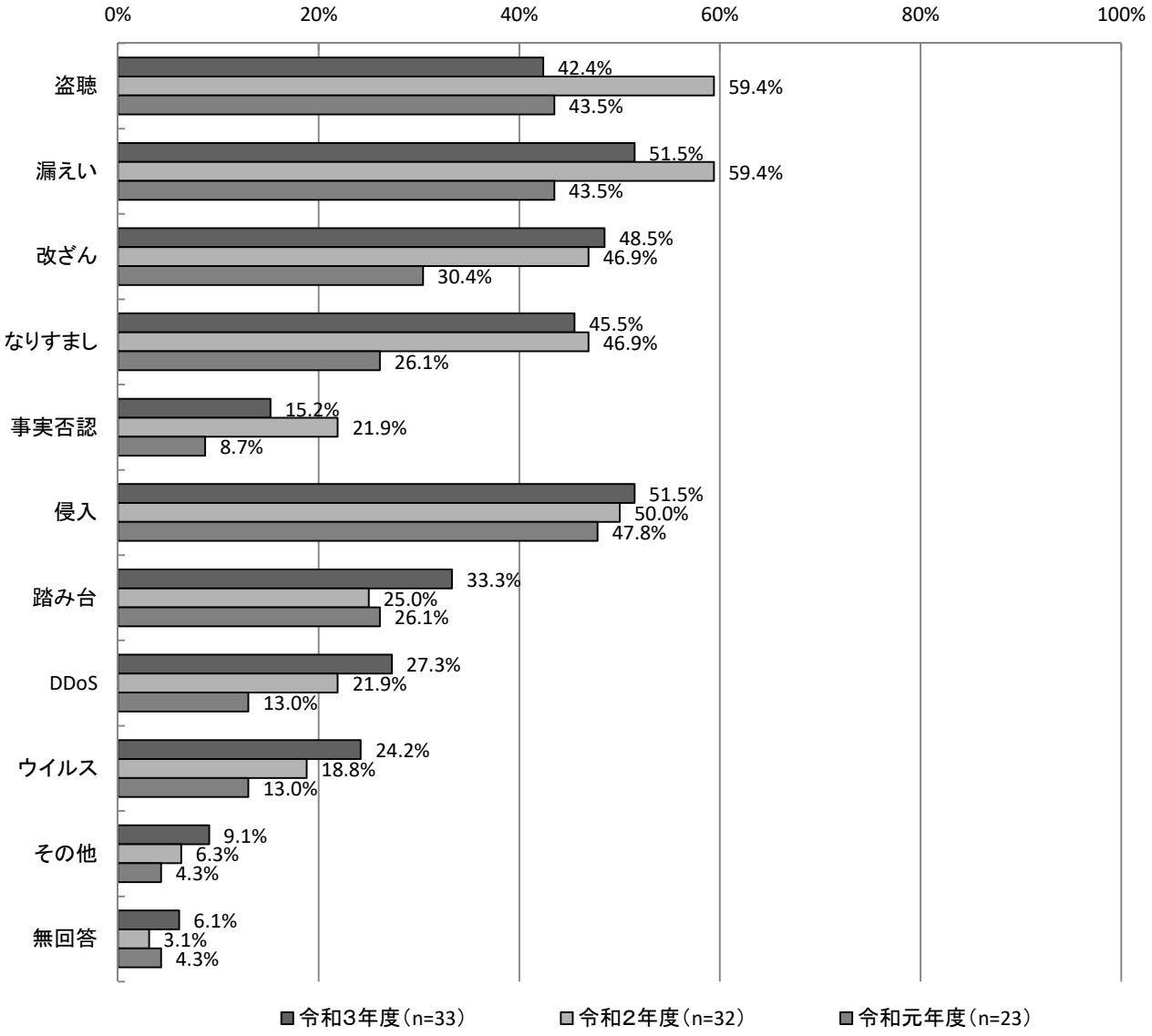
Ⅱ.研究開発中のもの

研究開発中のものについては、「漏えい」「侵入」がそれぞれ51.5%（17件）で最も多く、次いで「改ざん」が48.5%（16件）がとなっている。

昨年度と比較すると、「踏み台」が8.3ポイントで最も増加している。一方「盗聴」は17.0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？

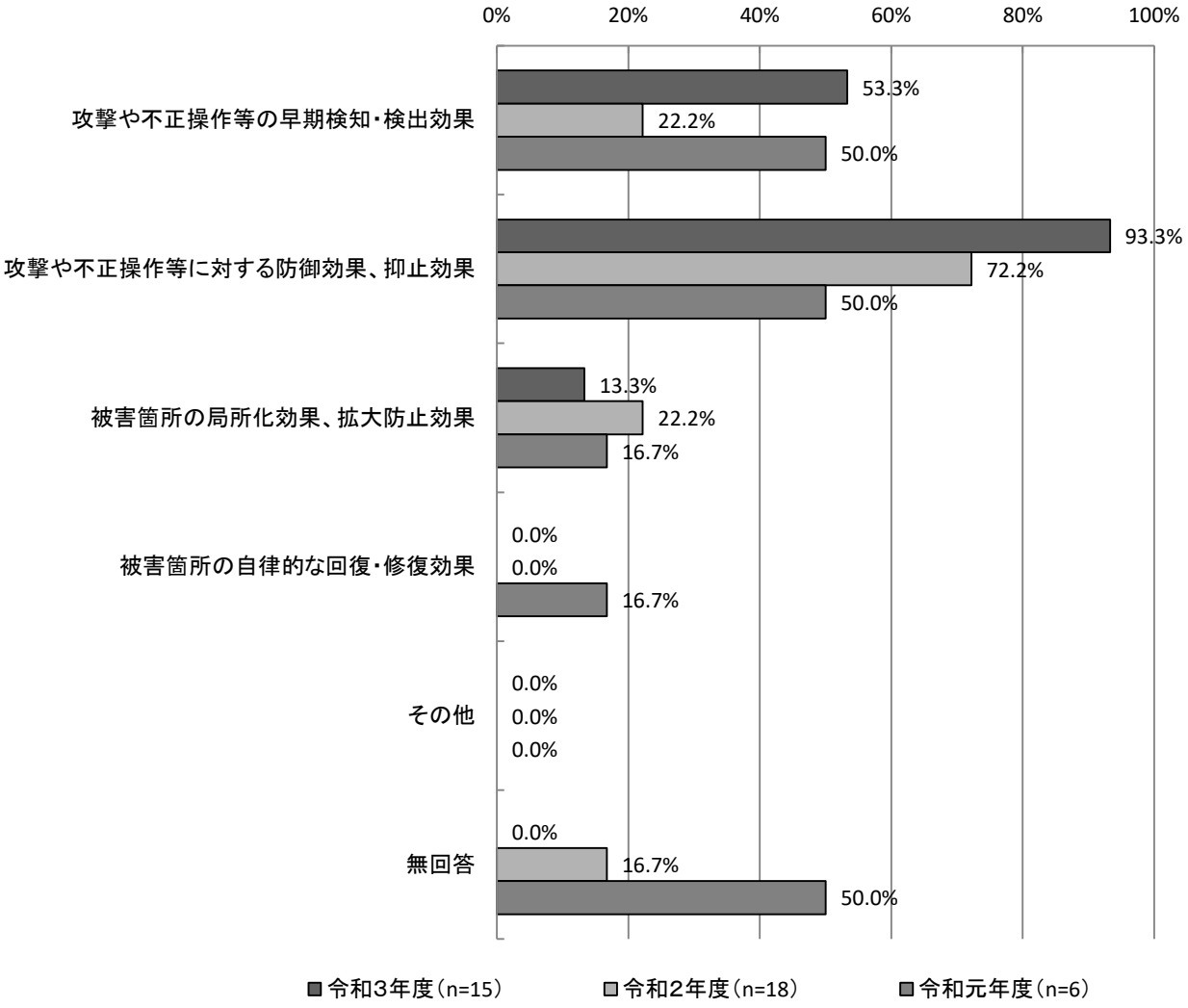
Ⅰ.実用化(製品化)されているもの

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93.3%（14件）で最も多くなっている。

昨年度と比較すると、「攻撃や不正操作等の早期検知・検出効果」が31.1ポイントで最も増加している。

【経年変化】どのようなセキュリティ上の効果があるか？

Ⅰ.実用化(製品化)されているもの(MA)【B-問3】

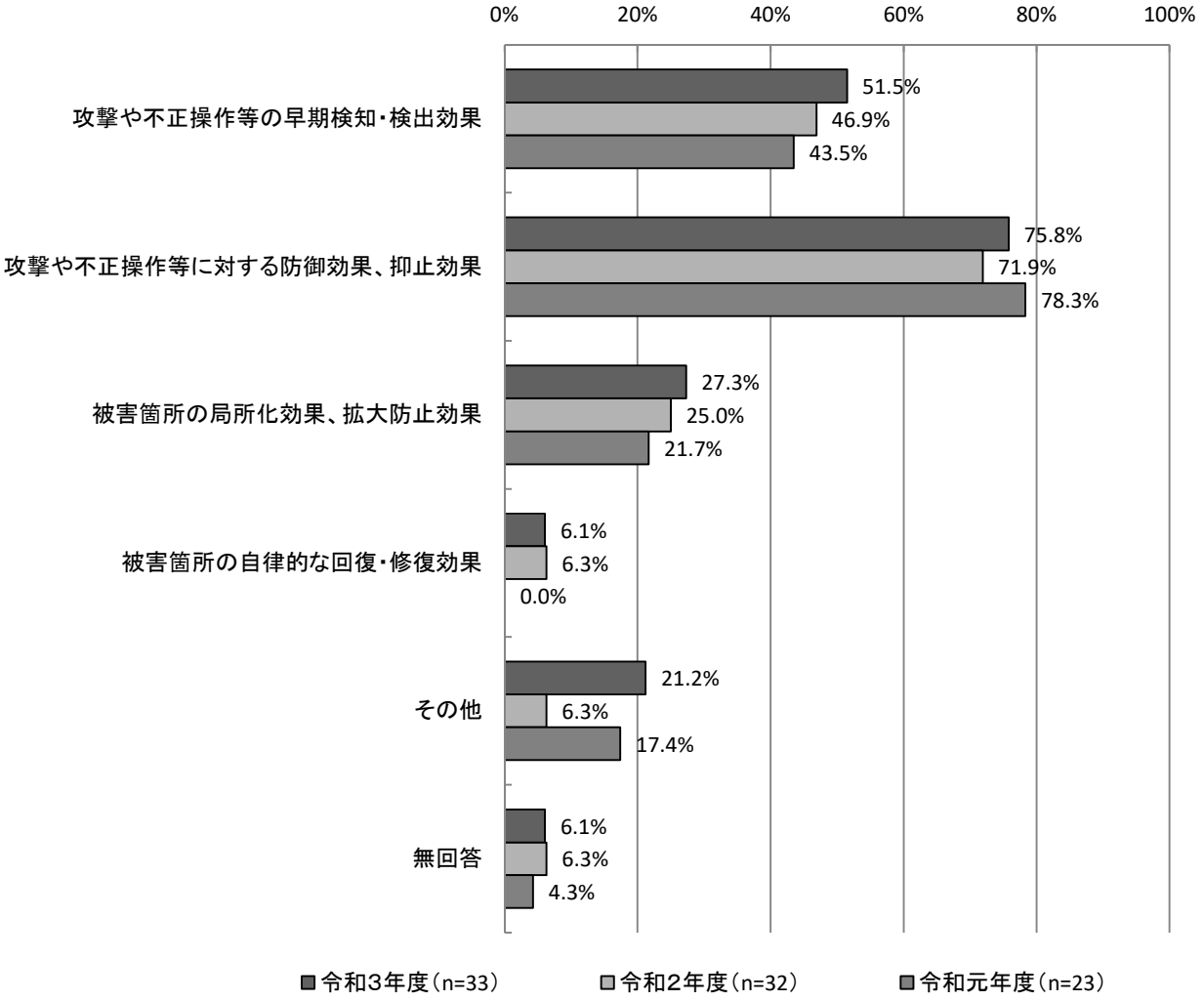


Ⅱ.研究開発中のもの

研究開発中のものについては、「攻撃や不正操作等に対する防御効果、抑止効果」が75.8%（25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51.5%（17件）となっている。

昨年度と比較すると、「攻撃や不正操作等の早期検知・検出効果」が4.6ポイント、「攻撃や不正操作等に対する防御効果、抑止効果」が3.9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？

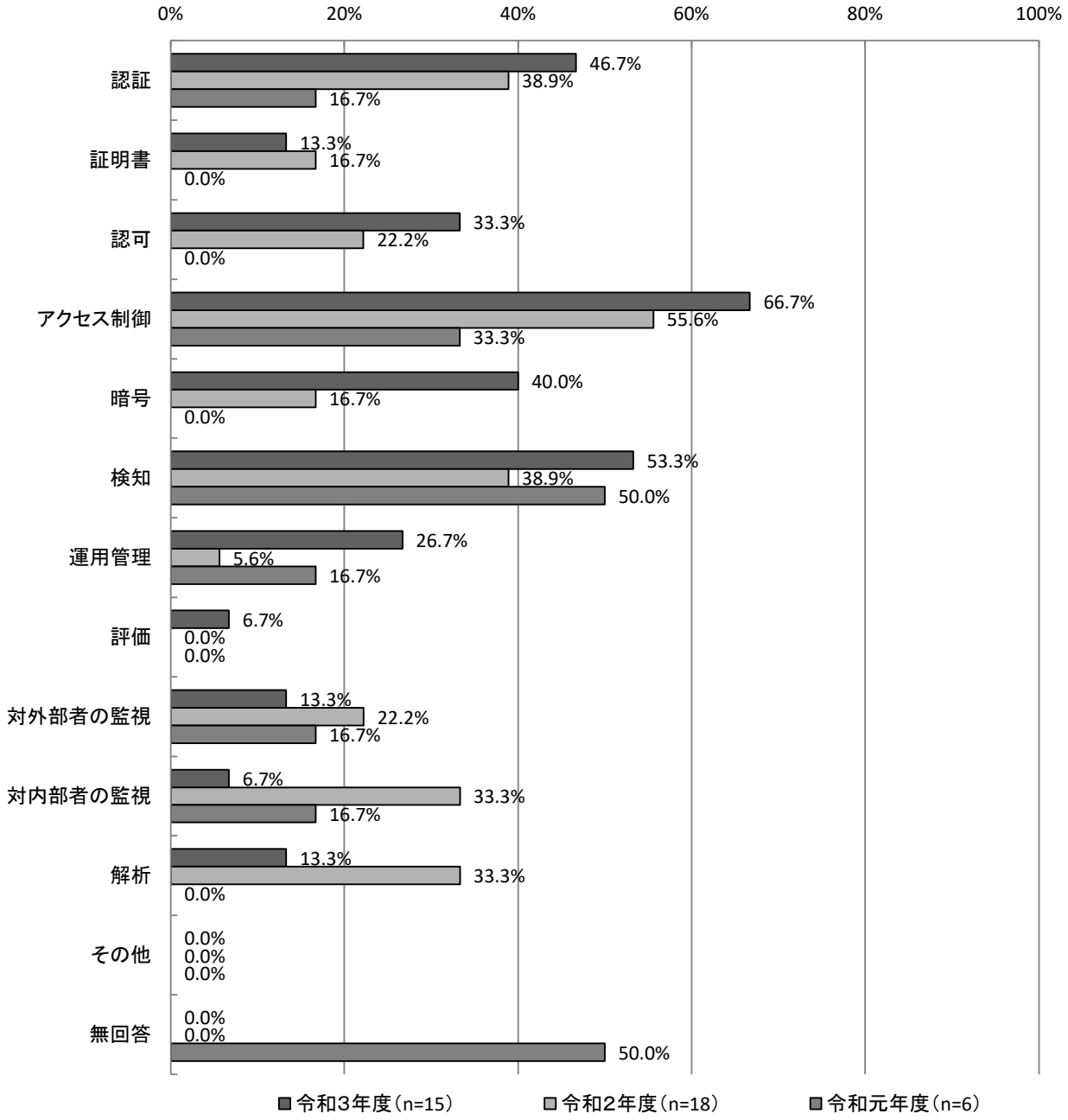
Ⅰ.実用化(製品化)されているもの

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66.7%（10件）で最も多く、次いで「検知」が53.3%（8件）となっている。

昨年度と比較すると、「暗号」が23.3ポイントと最も増加している。

【経年変化】どのような機能を持つか？

Ⅰ.実用化(製品化)されているもの(MA)【B-問4】



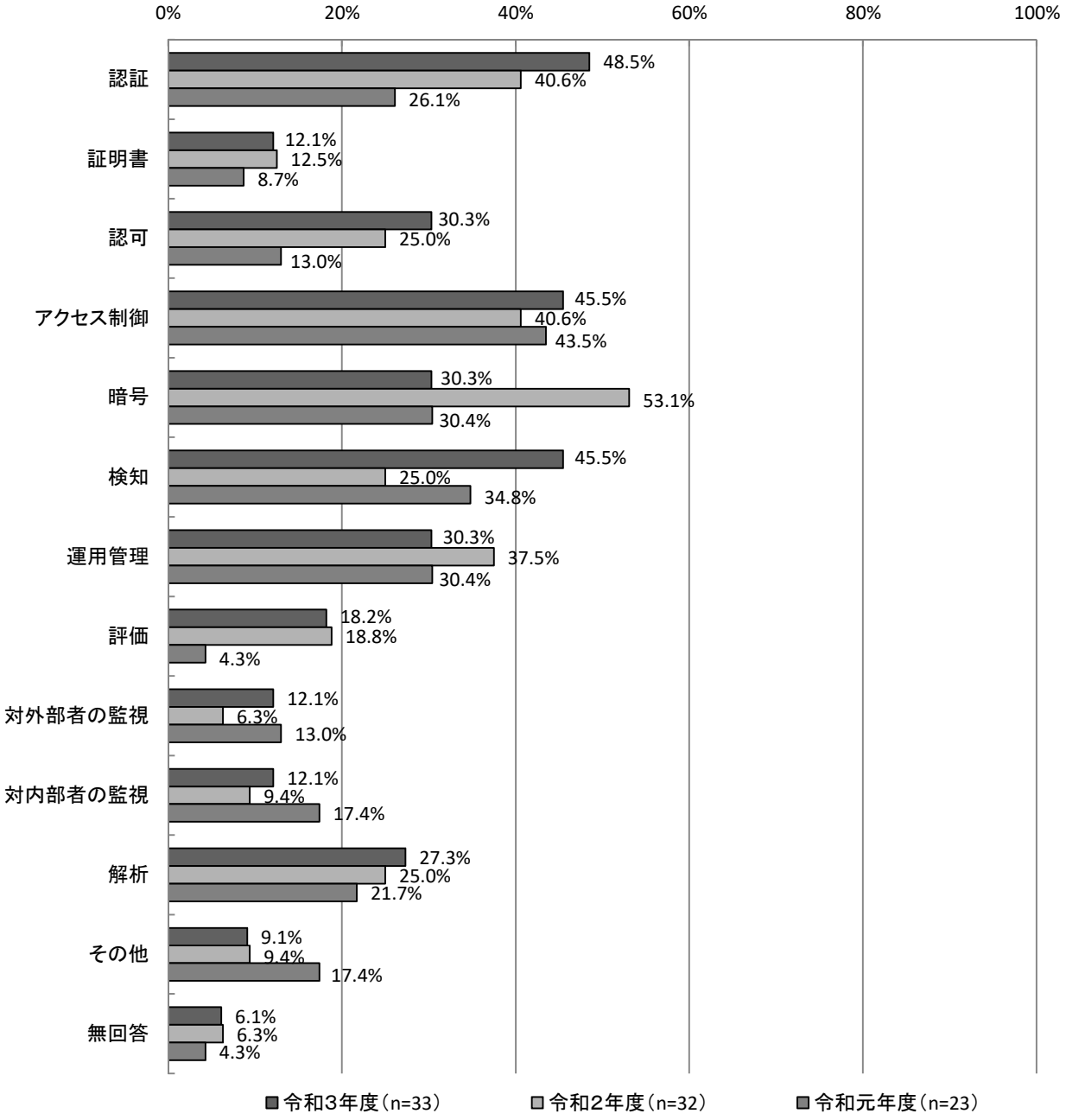
Ⅱ.研究開発中のもの

研究開発中のものについては、「認証」が48.5%（16件）で最も多く、次いで「アクセス制御」「検知」がそれぞれ45.5%（15件）となっている。

昨年度と比較すると、「検知」が20.5ポイントと最も増加している。一方、「暗号」は22.8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】



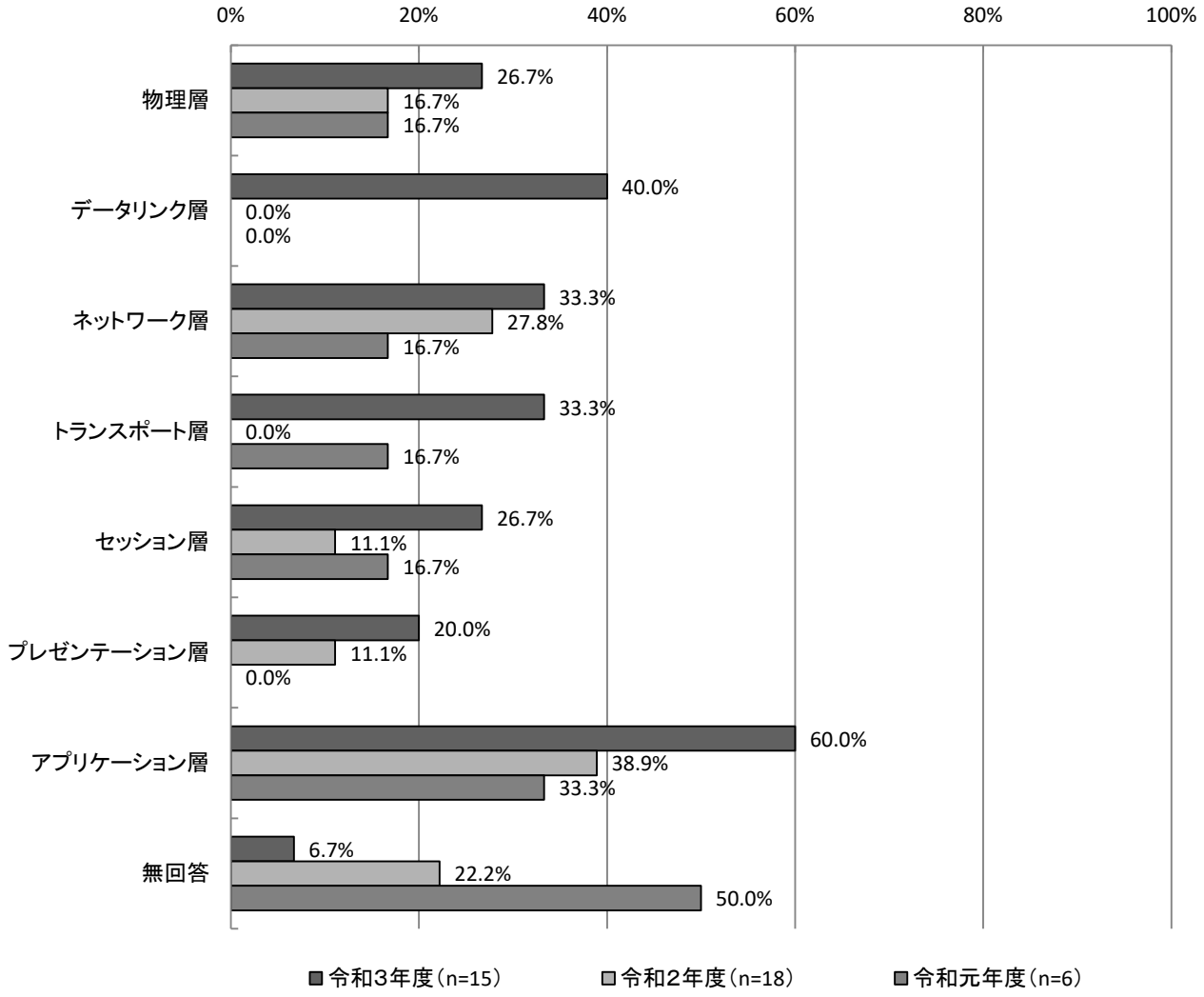
5.4.5　どのようなレイヤーのセキュリティを守るか？

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60.0％（9件）で最も多く、次いで「データリンク層」が40.0％（6件）となっている。

昨年度と比較すると、「データリンク層」が40.0ポイントと最も増加しており、減少している項目はなかった。

【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】

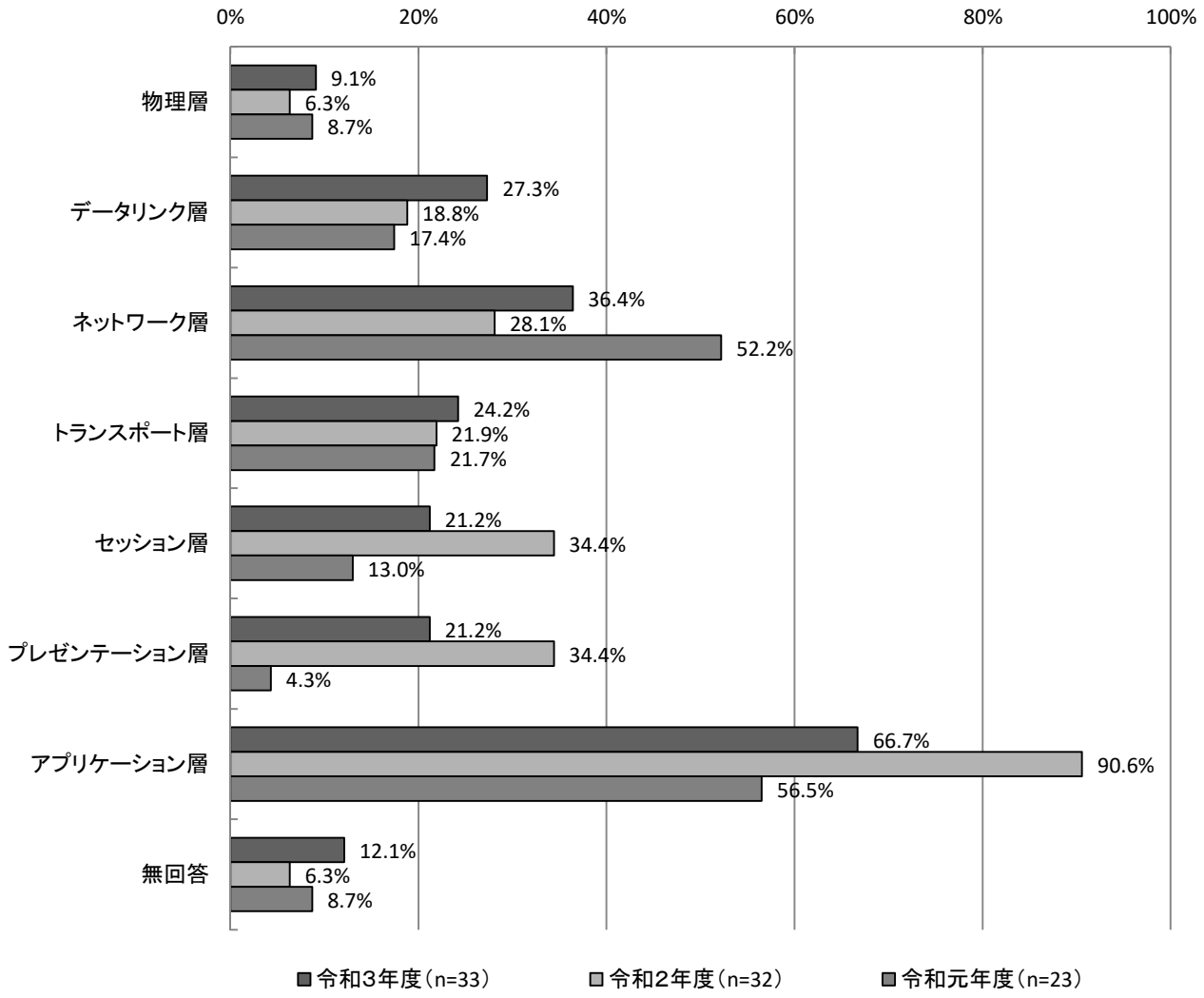


Ⅱ.研究開発中のもの

研究開発中のものについては、「アプリケーション層」が66.7%（22件）で最も多く、次いで「ネットワーク層」が36.4%（12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23.9ポイントと最も減少しており、次いで「セッション層」「プレゼンテーション層」がそれぞれ13.2ポイント減少している。一方、「データリンク層」は8.5ポイント増加している。

【経年変化】どのようなレイヤーのセキュリティを守るか？
Ⅱ.研究開発中のもの(MA)【C-問5】



5.4.6　不正アクセスからの防御対象

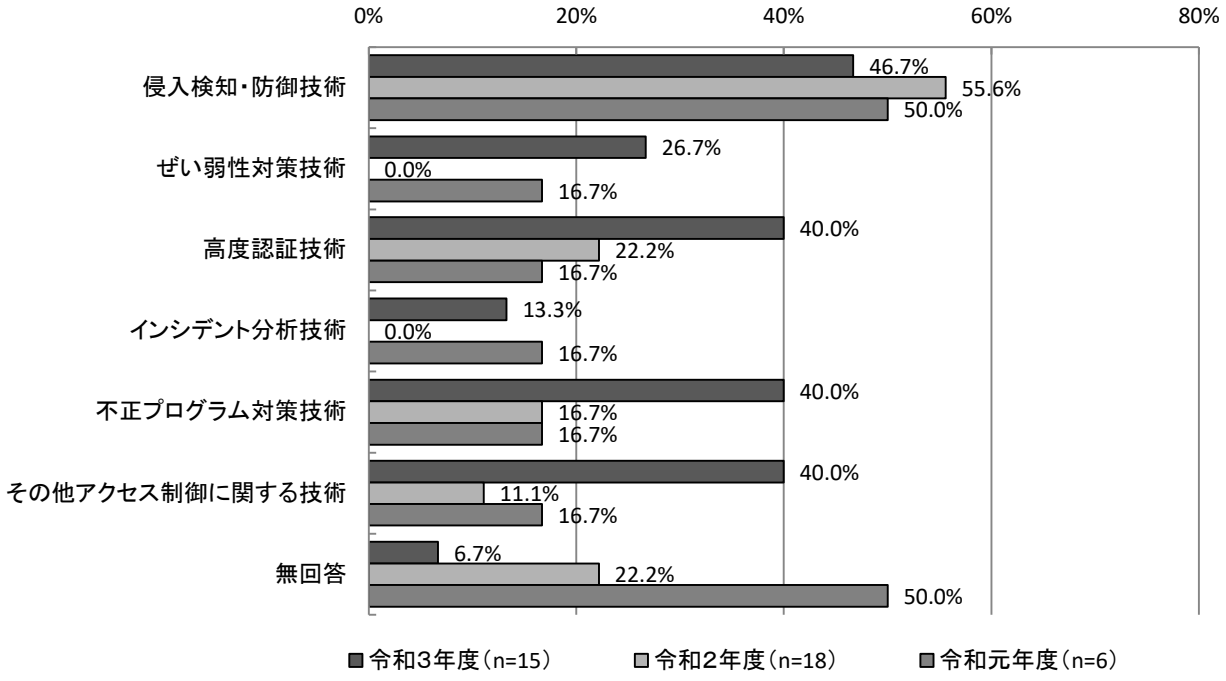
Ⅰ.実用化(製品化)されているもの

実用化（製品化）されているものについては、「侵入検知・防御技術」が46.7％（7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26.7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

Ⅰ.実用化(製品化)されているもの(MA)【B-問6】



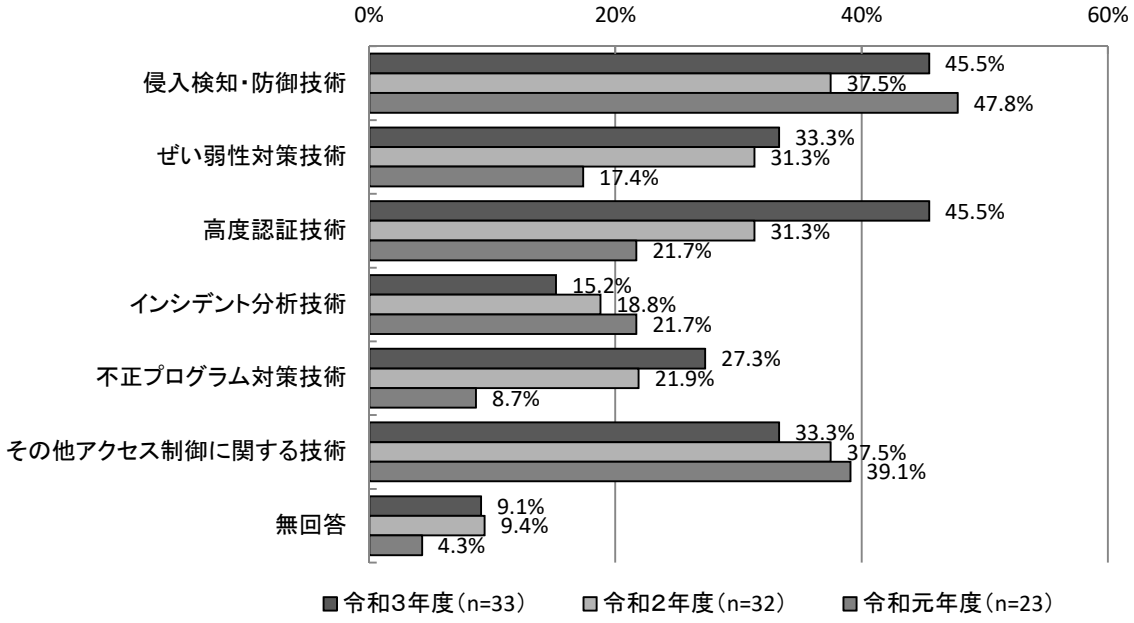
Ⅱ.研究開発中のもの

研究開発中のものについては、「侵入検知・防御技術」「高度認証技術」が45.5%（15件）で最も多くなっている。

昨年度と比較すると、「高度認証技術」が14.2ポイントと最も増加しており、次いで「侵入検知・防御技術」が8.0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？

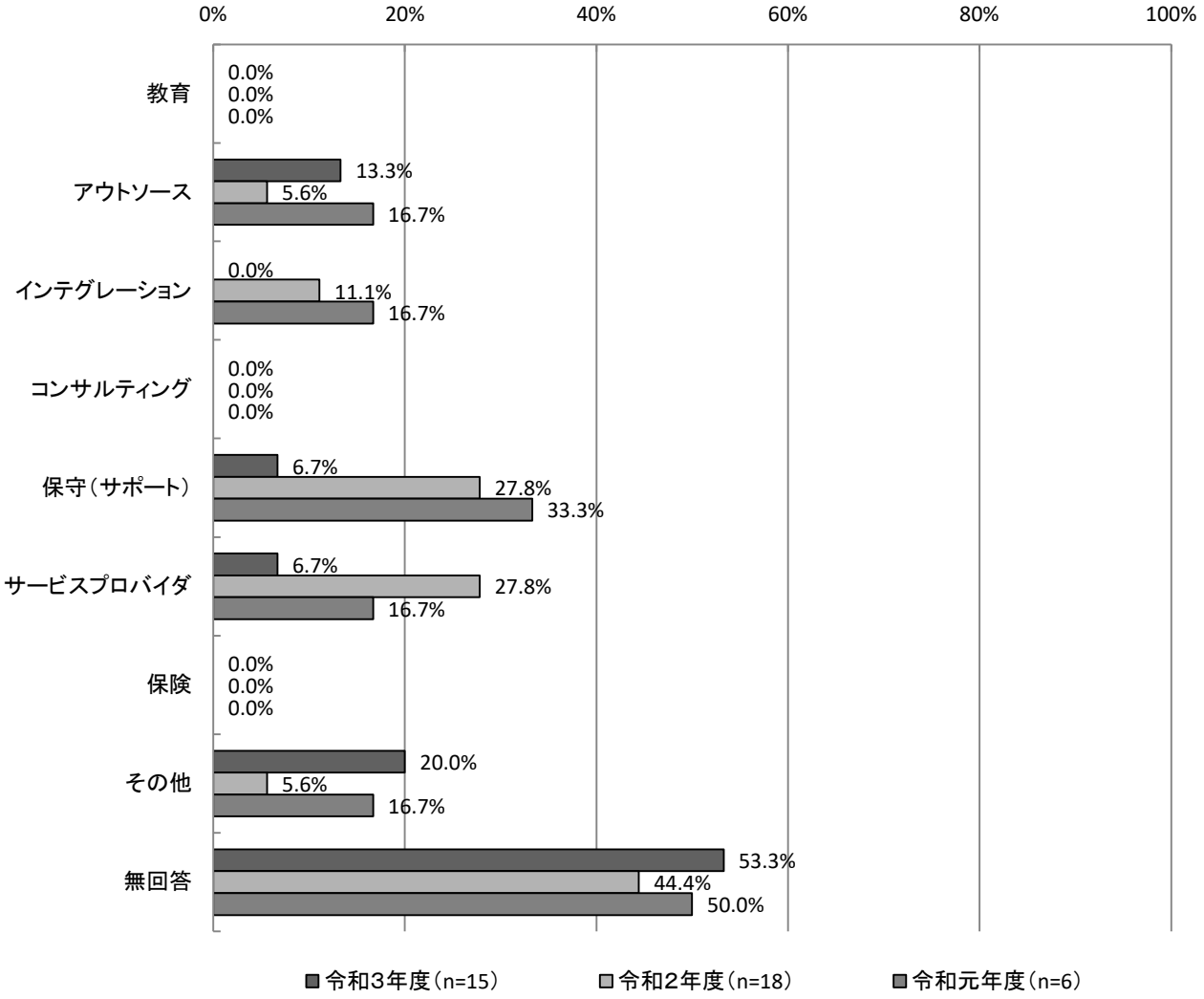
Ⅰ.実用化(製品化)されているもの

実用化（製品化）されているものについては、「アウトソース」が13.3％（2件）、「保守（サポート）」「サービスプロバイダ」が6.7％（1件）となっている。

昨年度と比較すると、「アウトソース」が7.7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】



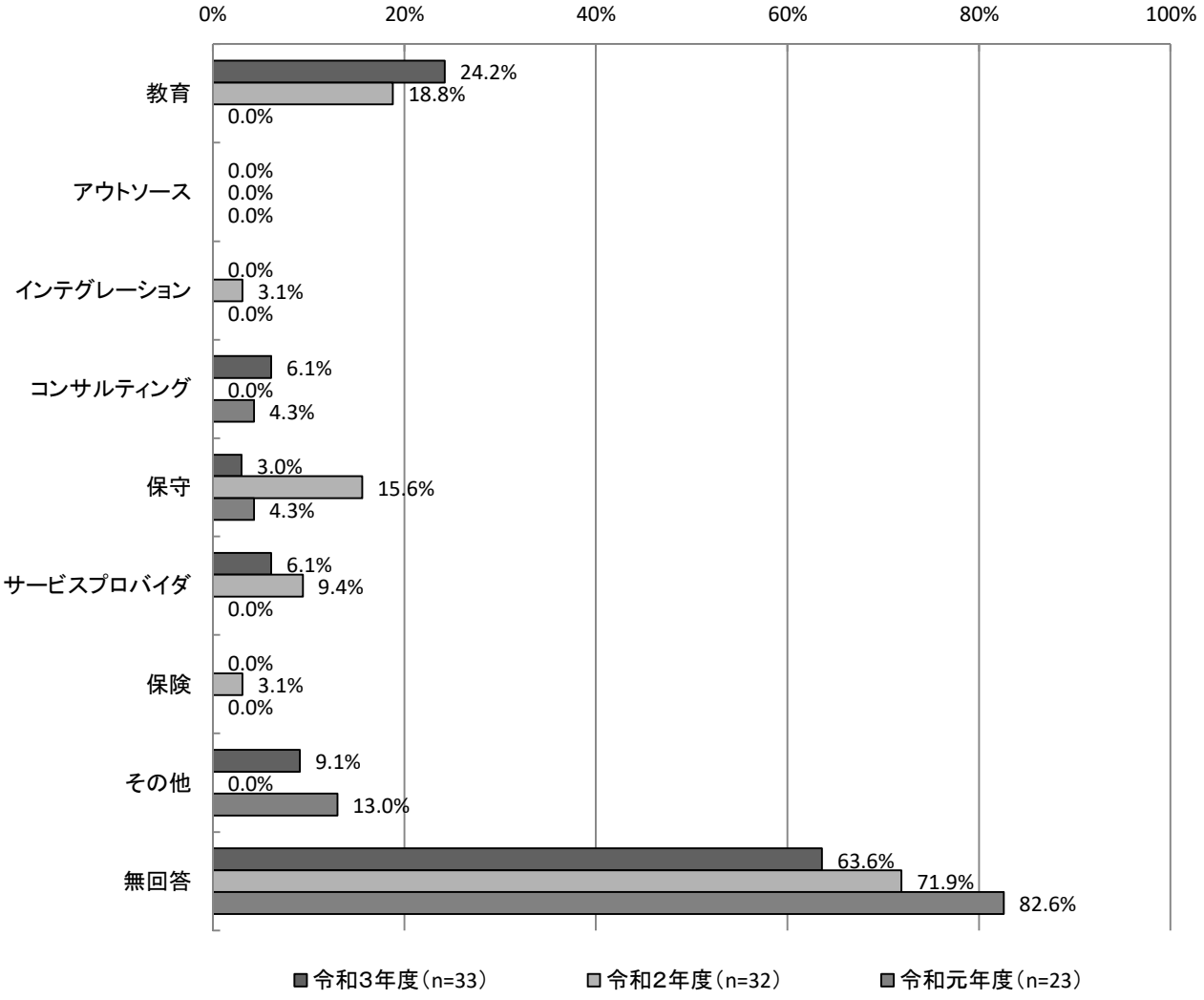
Ⅱ.研究開発中のもの

研究開発中のものについては、「教育」が24.2%（8件）、「コンサルティング」「サービスプロバイダ」が6.1%（2件）、「保守」が3.0%（1件）となっている。

昨年度と比較すると、「保守」が12.6ポイントと最も減少している。一方、「教育」は5.4ポイント増加している。

【経年変化】どのようなサービスか？

Ⅱ.研究開発中のもの(MA)【C-問8】

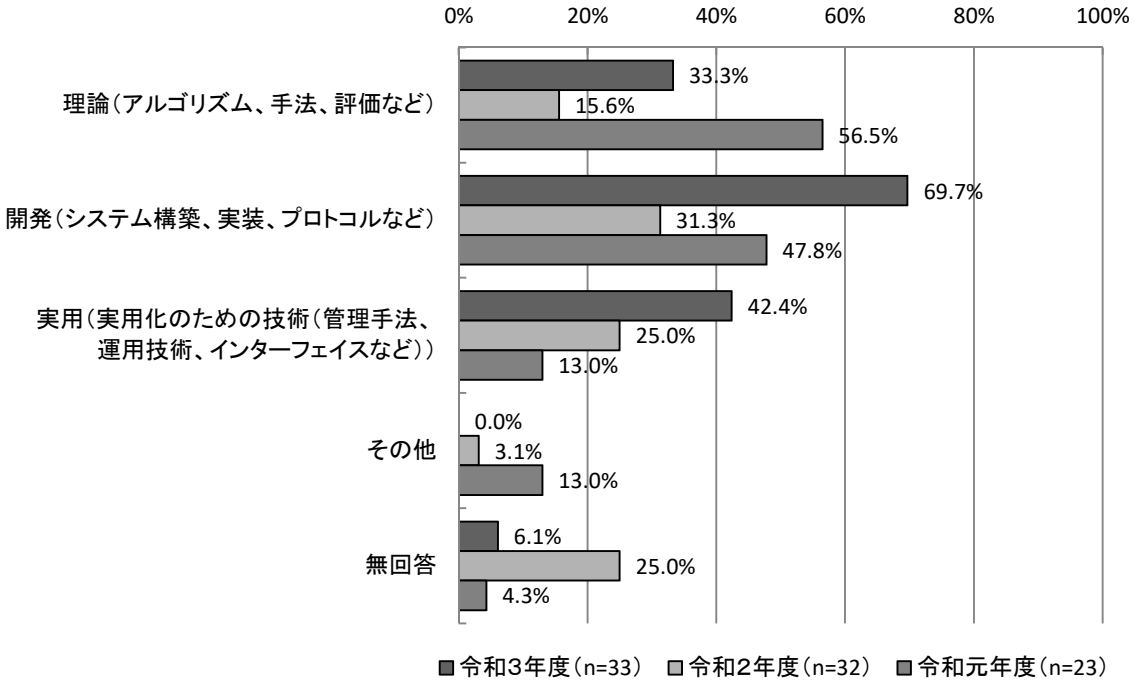


5.5　研究開発の成果としてどのようなものを目指しているか？

研究開発の目指す成果については、「開発（システム構築、実装、プロトコルなど）」が69.7%（23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42.4%（14件）、「理論（アルゴリズム、手法、評価など）」が33.3%（11件）となっている。

昨年度と比較すると、「開発（システム構築、実装、プロトコルなど）」が38.4ポイントと最も増加しており、次いで「理論（アルゴリズム、手法、評価など）」が17.7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】

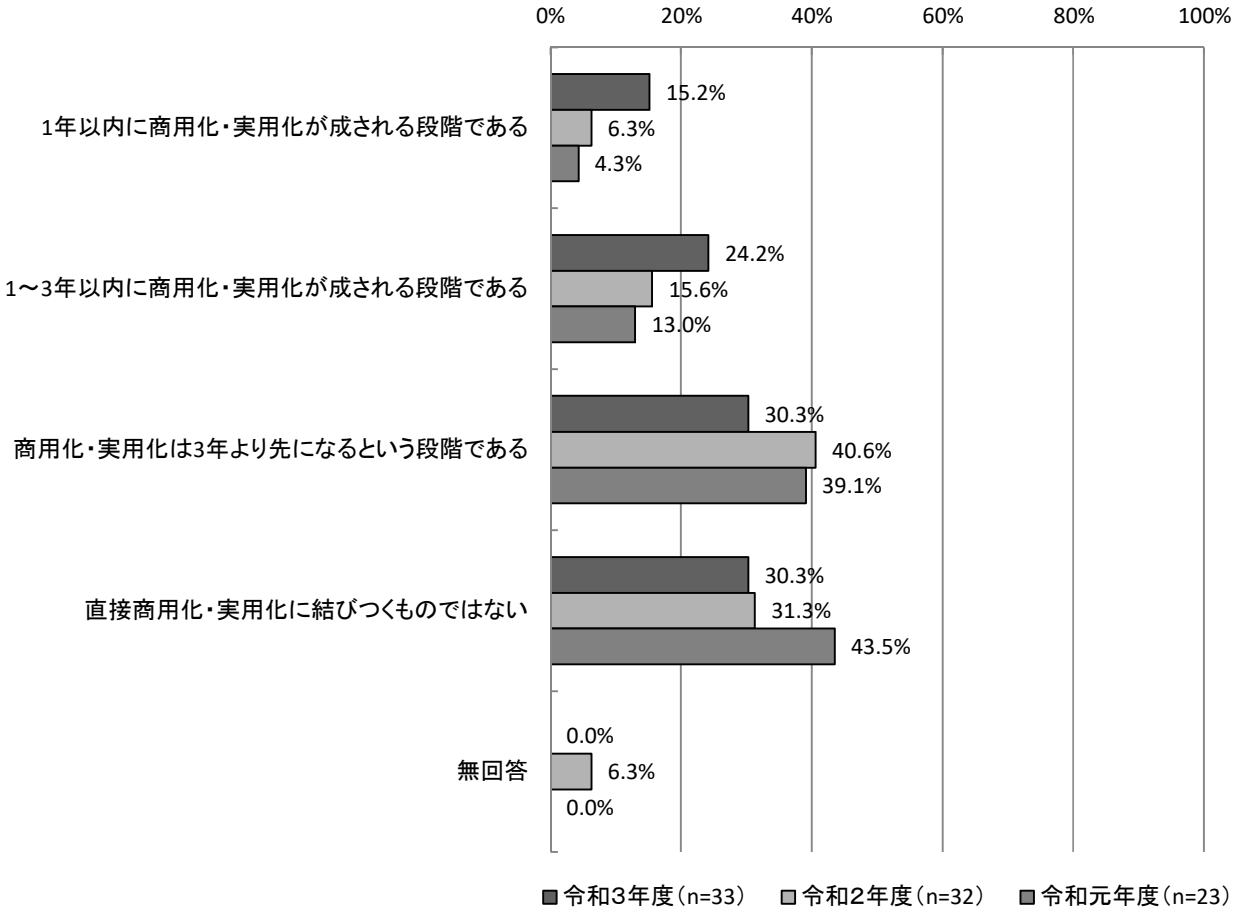


5.6　研究開発の進捗状況

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」「直接商用化・実用化に結びつくものではない」がそれぞれ30.3%（10件）となっている。

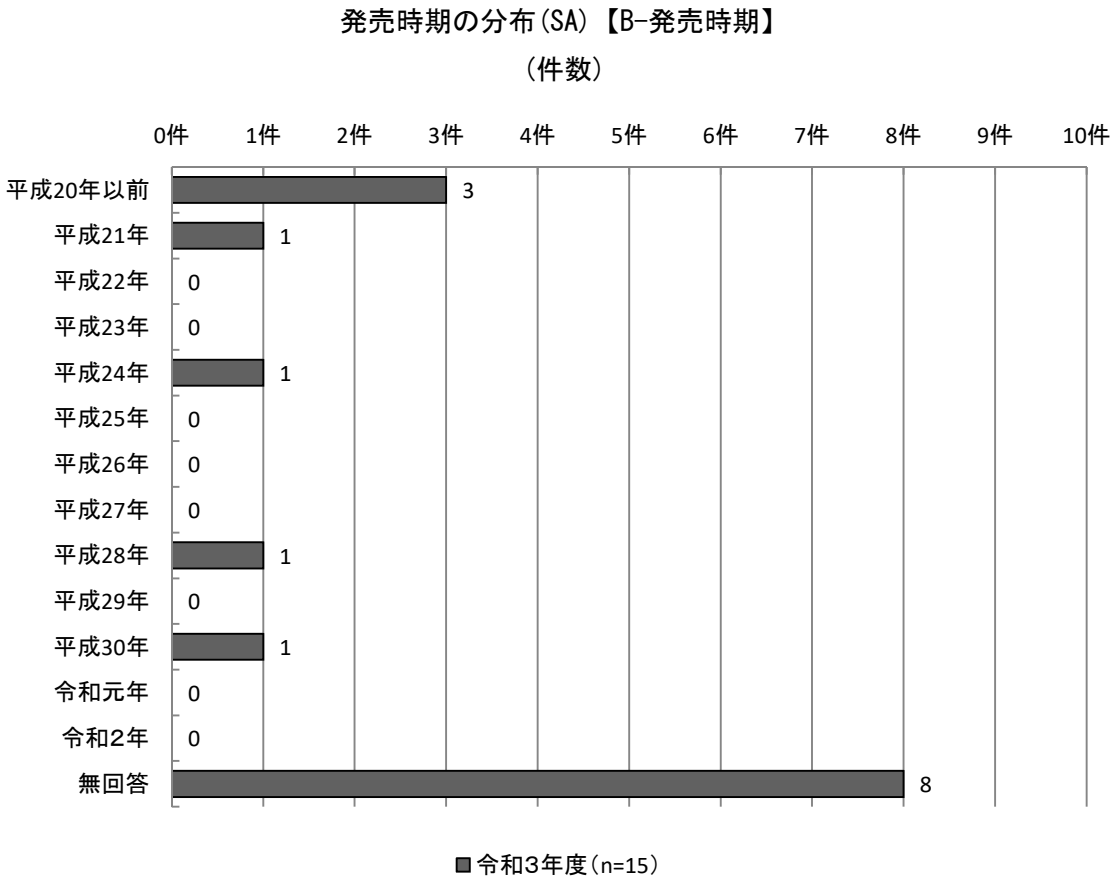
昨年度と比較すると、「1年以内に商用化・実用化が成される段階である」が8.9ポイントと最も増加している。一方、「商用化・実用化は3年より先になるという段階である」は10.3ポイントと最も減少している。

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4件で最も多く、次いで「平成21年」「平成23年」「平成24年」「平成28年」「平成30年」がそれぞれ1件となっている。

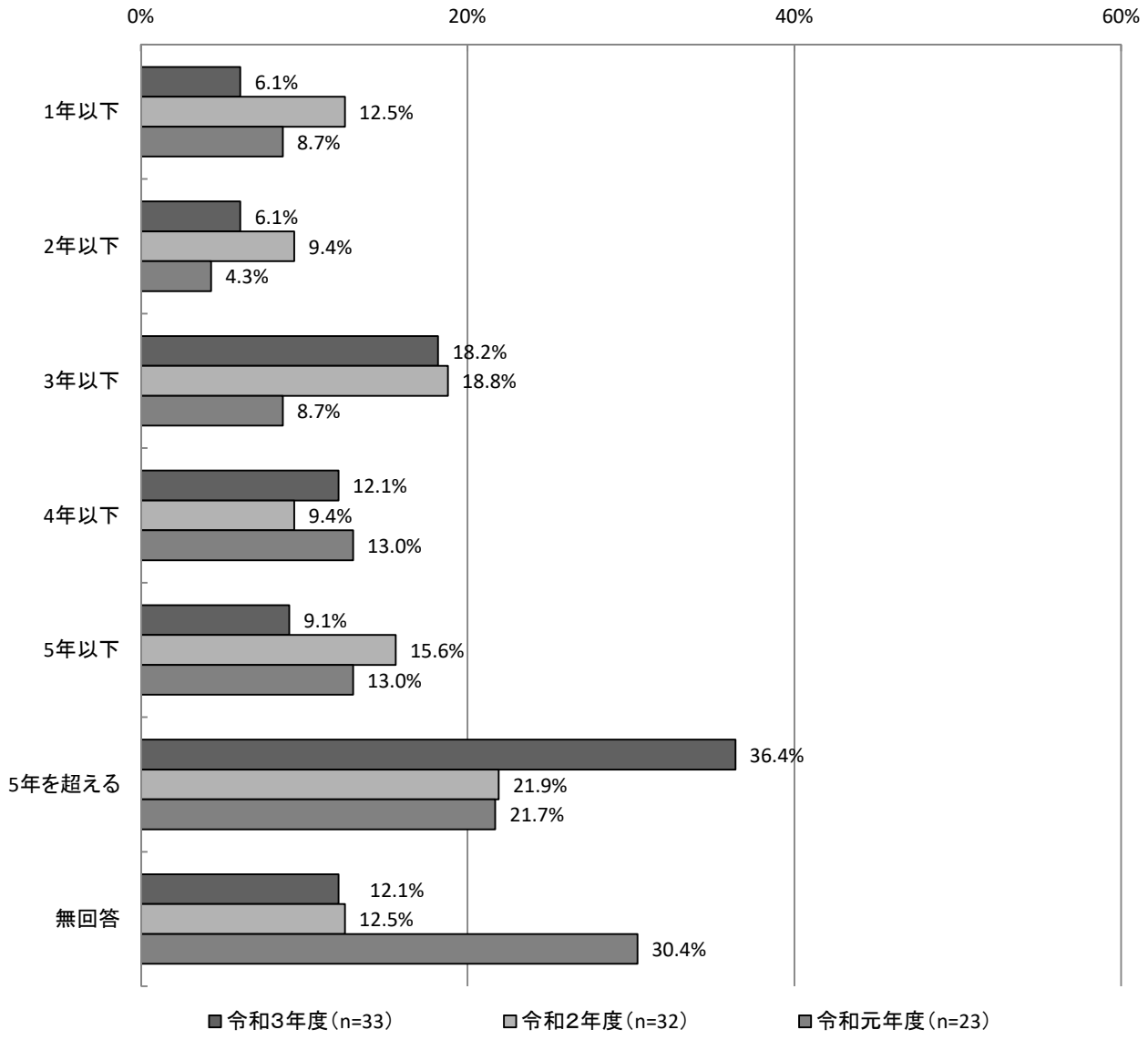


5.8　研究開発期間の分布

研究開発期間については、「5年を超える」が36.4%（12件）で最も多く、次いで「3年以下」が18.2%（6件）となっている。

昨年度と比較すると、「5年を超える」が14.5ポイントと最も増加している。一方「5年以下」は6.5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
クリプトボックス	東京理科大学	株式会社クリプト・ベーシック		○				
ZERO ウイルスセキュリティ	ソースネクスト株式会社	K7 Computing Pvt Ltd.	○	○			○	
eduroam JP	京都大学学術情報メディアセンター	国立情報学研究所			○			
学術認証フェデレーション　GakuNin	京都大学学術情報メディアセンター	国立情報学研究所			○			
imageRUNNER ADVANCE/DX シリーズ	キヤノン株式会社	キヤノン株式会社	○	○	○		○	○
IoTプラットフォーム	富士電機株式会社	富士電機株式会社	○		○		○	
VOIPセキュリティ診断サービス	株式会社ネクストジェン	株式会社ネクストジェン						○

※ 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
ウイルスの検出・分類に関する研究	国立大学法人岩手大学	理工学部システム創成工学科知能・メディア情報コース					○	
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						○
IoTマルウェアの解析技術の研究開発	神奈川工科大学	情報学部	○	○			○	
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						○
不正アクセスの経路及び手法に関する調査研究	株式会社アズジェント	セキュリティ・プラス本部						
サイバーフィジカルシステムのセキュリティに関する研究	創価大学　理工学部　情報システム工学科	創価大学　理工学部　情報システム工学科	○	○	○	○		
SDNにおける文脈型動的セキュリティプロトコル	学校法人中央大学	国際情報学部	○	○				○
新常態環境下の情報セキュリティに関する総合的研究（ユニット名）	学校法人中央大学	研究開発機構（ユニット代表者：趙晋輝）	○		○			○
産業用インターネットオブシングス(Industrial Internet of Things: IIoT)機器・システムに対する遠隔セキュリティ検証手法	学校法人中央大学	国際情報学部		○				
PDI認証	東京理科大学	認証技術			○			
生体から得られる電磁気情報を用いた個人認証システム	日本大学	理工学部応用情報化学科	○	○	○		○	
ブロックチェーン技術を用いた単一医療機関向け診療記録システム	日本大学	理工学部応用情報工学科	○	○	○		○	
標的型メール対策訓練支援システム	日本大学	理工学部応用情報工学科	○	○	○	○	○	
デジタルフォレンジック技術の学習支援システム	日本大学	理工学部応用情報工学科	○	○	○	○	○	
Raspberry Gate	国立大学法人金沢大学	学術メディア創成センター	○	○				
隠れオープンリゾルバスキャナ	中京大学	中京大学工学部		○				○
(特に名称をつけていない)	国立大学法人東海国立大学機構名古屋大学	情報基盤センター 情報基盤ネットワーク研究部門 基盤ネットワーク研究G	○	○		○	○	
新常態環境下の情報セキュリティに関する総合的研究（ユニット名）	国立大学法人東海国立大学機構名古屋大学	研究開発機構（ユニット代表者：趙晋輝）	○		○			○
対話的に通信制御が可能なマルウェア解析システム	京都大学学術情報メディアセンター	ネットワーク研究部門					○	
情報漏洩を防止するオペレーティングシステム	学校法人立命館（立命館大学）	情報理工学部						○
キーボード入力のタイミングを用いた生体認証	学校法人福岡大学	福岡大学情報基盤センター中國研究室			○			
改ざん検知・復旧技術開発	キヤノン株式会社	デジタルビジネスプラットフォーム開発本部	○					○
無線LANセキュリティ技術開発	キヤノン株式会社	デジタルビジネスプラットフォーム開発本部			○			
Canon ID(コンシューマ向け認証認可基盤)	キヤノン株式会社	デジタルビジネスプラットフォーム開発本部			○			
組込機器のセキュリティ技術	富士電機株式会社	技術開発本部　デジタルイノベーション研究所	○		○			○

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

5.9.1 「技術の実用化（製品化）状況」について

※一覧表の下には対象となる防御対象について○を付与している。

企業・大学名	東京理科大学
代表者名	本間　芳和
所在地	162-8601 東京都新宿区神楽坂1-3
窓口部署名	研究戦略・産学連携センター　企画管理部門
電話番号	03-5228-7440
ホームページのURL	https://www.tus.ac.jp
製品説明のURL	
対象技術	技術の概要・特徴など
製品名: クリプトボックス 開発元(メーカー名等): 株式会社クリプト・ベーシック 開発国: 日本 価格: 50万円 発売時期: 2012年4月1日～ 出荷数: 2	独自の鍵共有プロトコルと共通鍵暗号方式により従来と比較して10倍以上の鍵長を持つ暗号通信をもとに，強力なVPNを構築できる.

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	ソースネクスト株式会社
代表者名	代表取締役社長 兼 COO 小嶋智彰
所在地	105-7133 東京都港区東新橋1-5-2　汐留シティセンター33階
窓口部署名	
電話番号	
ホームページのURL	https://sourcenext.co.jp/
製品説明のURL	
対象技術	技術の概要・特徴など
製品名: ZERO ウイルスセキュリティ 開発元(メーカー名等): K7 Computing Pvt Ltd. 開発国: インド 価格: 1,980円・税込（1台用） 発売時期: 2003年11月14日～ 出荷数: 累計1000万台以上	「ZERO ウイルスセキュリティ」は、2006年より更新料0円で発売している製品。 「ウイルスセキュリティ」そのものは2003年の発売です。 「ウイルスセキュリティ」のエントリー数はのべ1000万台を突破しています。

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

企業・大学名	京都大学学術情報メディアセンター
代表者名	センター長　岡部　寿男
所在地	606-8501 京都府京都市左京区吉田本町
窓口部署名	情報部　情報推進課　総務掛
電話番号	075-753-7400
ホームページのURL	https://www.media.kyoto-u.ac.jp
製品説明のURL	
対象技術	技術の概要・特徴など
製品名: eduroam JP 開発元(メーカー名等): 国立情報学研究所 開発国: 日本（欧州と共同開発） 価格: 無料 発売時期: 2006年8月～ 出荷数: 国内310機関	教育、研究機関で提供されるキャンパス無線LANを相互に安全にローミングで利用できるようにする国際的な認証連携のしくみ　www.eduroam.jp

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

企業・大学名	京都大学学術情報メディアセンター
代表者名	センター長　岡部　寿男
所在地	606-8501 京都府京都市左京区吉田本町
窓口部署名	情報部　情報推進課　総務掛
電話番号	075-753-7400
ホームページのURL	https://www.media.kyoto-u.ac.jp
製品説明のURL	
対象技術	技術の概要・特徴など
製品名: 学術認証フェデレーション GakuNin 開発元(メーカー名等): 国立情報学研究所 開発国: 日本 価格: 無料 発売時期: 2009年4月～ 出荷数: 大学等258機関、サービス提供機関188	学術eリソースを利用する大学等と学術eリソースを提供する出社等が相互に認証連携を行うための国際的なしくみ www.gakunin.jp

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

企業・大学名	キヤノン株式会社
代表者名	御手洗冨士夫
所在地	146-8501 東京都大田区下丸子3-30-2
窓口部署名	
電話番号	03-3758-2111
ホームページのURL	https://global.canon
製品説明のURL	
対象技術	技術の概要・特徴など
製品名: imageRUNNER ADVANCE/DX シリーズ 開発元(メーカー名等): キヤノン株式会社 開発国: 日本 価格: 本体標準価格 67万円～500万円 発売時期: 2016年1月1日～ 出荷数:	弊社製品はオフィスにおけるネットワーク事務機器であり、顧客のオフィスネットワークインフラに接続され顧客情報が流通する為、セキュリティ脅威として、悪意や誤用による情報漏洩、他の情報機器へ攻撃踏み台としての悪用などの可能性に対して、高度な暗号化による盗聴防止、ユーザ認証機能による権限のある情報参照への認可、ファームウェアの改ざん防止・検知など、セキュリティに対して万全の備えを有している。

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	富士電機株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
ホームページのURL	https://www.fujielectric.co.jp/
製品説明のURL	
対象技術	技術の概要・特徴など
製品名: IoTプラットフォーム 開発元(メーカー名等): 富士電機株式会社 開発国: 日本 価格: 発売時期: 2018年9月1日～ 出荷数:	当社顧客サイトに設置されるエッジコントローラと、エッジコントローラにより収集したデータに基づきサービスを提供するクラウドから構成される。 提供サービスにはエネルギーマネジメント、稼働監視などが含まれる。

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	株式会社ネクストジェン
代表者名	大西　新二
所在地	108-0072 東京都港区白金1-27-6　白金高輪ステーションビル6F
窓口部署名	
電話番号	03-5793-3230
ホームページのURL	https://www.nextgen.co.jp
製品説明のURL	
対象技術	技術の概要・特徴など
製品名: VOIPセキュリティ診断サービス 開発元(メーカー名等): 株式会社ネクストジェン 開発国: 日本 価格: 実施内容による 発売時期: 2007年～ 出荷数: 200機器程度の診断実績	VIOP音声網に対するセキュリティ診断サービスです。新たな攻撃ツールや手法について継続的な調査を行っており、診断サービスでは、これらをもとに机上検討及び模擬攻撃を実施し、なりすましや改ざん、盗聴といった音声網へのリスクを可視化します。固定電話やモバイルなど通信事業者や、クラウドPBXサービス事業者、またはこれらに設備を導入するベンダが主な顧客です。国内の大手通信事業者が主な顧客ですが、詳細は当社HP（下記）をご覧ください。 https://www.nextgen.co.jp/solution/voip/service/sipvoip.html

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

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	国立大学法人岩手大学
代表者名	学長　小川　智
所在地	〒020-8550 岩手県盛岡市上田三丁目１８番８号
窓口部署名	理工学部事務部
電話番号	019-621-6305
関連部門名	理工学部システム創成工学科知能・メディア情報コース
ホームページのURL	https://www.iwate-u.ac.jp/
研究説明のURL	
対象技術	技術の概要・特徴など
研究開発名称： ウイルスの検出・分類に関する研究 研究開発国： 日本 研究開発時期： 2016年4月～	ウイルスの表層あるいは動的解析結果を利用した，機械学習による検出・分類手法の研究を行っている．

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

企業・大学名	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： 2015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	○

企業・大学名	神奈川工科大学
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	情報学部
ホームページのURL	
研究説明のURL	https://ipsj.ixsq.nii.ac.jp/ej/index.php?active_action=repository_view_main_item_detail&page_id=13&block_id=8&item_id=208504&item_no=1 https://ipsj.ixsq.nii.ac.jp/ej/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=211007&item_no=1&page_id=13&block_id=8
対象技術	技術の概要・特徴など
研究開発名称： IoTマルウェアの解析技術の研究開発 研究開発国： 日本 研究開発時期： 2019年10月1日～2022年3月1日	IoTマルウェアの解析の要となるライブラリ関数の特定が完了した。今後はライブラリ関数の情報を活用して、関数のトレースによる動的解析技術やIoTマルウェアの検知・亜種分類の研究開発を行う予定である。

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

企業・大学名	東京電機大学　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	https://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： 2007年3月6日～2021年12月31日	秘密電子メール、秘密映像伝達技術並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	株式会社アズジェント
代表者名	杉本　隆洋（代表取締役社長）
所在地	〒104-0044 東京都中央区明石町6-4　ニチレイ明石町ビル
窓口部署名	セキュリティ・プラス・ラボ
電話番号	03-6853-7406
関連部門名	セキュリティ・プラス本部
ホームページのURL	https://www.asgent.co.jp/
研究説明のURL	https://www.asgent.co.jp/press/releases/2014/20140117-000373.html
対象技術	技術の概要・特徴など
研究開発名称： 不正アクセスの経路及び手法に関する調査研究 研究開発国： 日本 研究開発時期： 2014年4月1日～継続中	セキュリティ・プラス・ラボ設立以来、世界中で横行する脅威の実態やその攻撃手法、またそれらの脅威からクラウド環境やモバイルデバイスを含めた情報資源を守るための対策技術の研究はもとより、国内外の有識者や組織との積極的な連携を図ることにより、技術だけでは守ることのできない「ソーシャルエンジニアリング」のような領域まで踏み込んだ広義での「セキュリティ」に関する調査、研究を継続して行っています。また、その調査・研究成果は講演活動、レポート、トレーニング等を通じて市場へ発信しています。

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

企業・大学名	創価大学　理工学部　情報システム工学科
代表者名	
所在地	〒192-0003 東京都八王子市丹木町1-236
窓口部署名	理工学部事務室
電話番号	042-691-9400
関連部門名	創価大学　理工学部　情報システム工学科
ホームページのURL	www.soka.ac.jp/science/infosys/
研究説明のURL	www.soka.ac.jp/science/infosys
対象技術	技術の概要・特徴など
研究開発名称： サイバーフィジカルシステムのセキュリティに関する研究 研究開発国： 日本 研究開発時期： 2017年4月1日～2023年3月31日	大学の研究室内での研究であり、実用等商品化は考えていない

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	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
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： SDNにおける文脈型動的セキュリティプロトコル 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
電話番号	03-3817-7463
関連部門名	研究開発機構（ユニット代表者：趙　晋輝）
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	ありません
対象技術	技術の概要・特徴など
研究開発名称： 新常態環境下の情報セキュリティに関する総合的研究（ユニット名） 研究開発国： 日本 研究開発時期： 2019年4月1日～2022年3月31日	企業秘密に関係するため開示は出来ません

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

企業・大学名	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
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	http://www.iperc.uec.ac.jp/datafile/annualreport/iPERC2019HP.pdf
対象技術	技術の概要・特徴など
研究開発名称： 産業用インターネットオブシングス（Industrial Internet of Things: IIoT)機器・システムに対する遠隔セキュリティ検証手法 研究開発国： 日本 研究開発時期： 2019年4月1日～	制御システムの模擬プラントにおいて評価を進める中で、実用化する上での課題に対処している。

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

企業・大学名	東京理科大学
代表者名	本間　芳和
所在地	〒162-8601 東京都新宿区神楽坂1-3
窓口部署名	研究戦略・産学連携センター　企画管理部門
電話番号	03-5228-7440
関連部門名	認証技術
ホームページのURL	https://www.tus.ac.jp
研究説明のURL	https://wakasapo.nedo.go.jp/seeds/seeds-0246/
対象技術	技術の概要・特徴など
研究開発名称： PDI認証 研究開発国： 日本 研究開発時期： 2016年4月1日～	理論及び研究実装，POC用プロトタイプが完成している．現在，サービス開始を目指し，サーバー安定稼働，API整備を進めている．

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	日本大学
代表者名	
所在地	〒102-8275 東京都千代田区九段南4-8-24
窓口部署名	研究推進部 研究事務課
電話番号	03-5275-8137
関連部門名	理工学部応用情報化学科
ホームページのURL	http://www.nihon-u.ac.jp/
研究説明のURL	https://53lab.jp/
対象技術	技術の概要・特徴など
研究開発名称： 生体から得られる電磁気情報を用いた個人認証システム 研究開発国： 日本 研究開発時期： 2016年12月1日～	実験用のシステムを構築し、有効性の検証を行っている。

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

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

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

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

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

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

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

企業・大学名	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	学術メディア創成センター
ホームページのURL	https://www.kanazawa-u.ac.jp/
研究説明のURL	ホームページでは公開しない
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： 2011年4月1日～	組み込み機器のセキュリティ研究の一環としてアクセス制御の技術開発も行っている

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	中京大学
代表者名	
所在地	〒466-8666 名古屋市昭和区八事本町１０１－２
窓口部署名	学園経営戦略部
電話番号	052-835-7138
関連部門名	中京大学工学部
ホームページのURL	https://www.chukyo-u.ac.jp/
研究説明のURL	http://www.e-ontap.com/blog/?date=20210331
対象技術	技術の概要・特徴など
研究開発名称： 隠れオープンリゾルバスキャナ 研究開発国： 日本 研究開発時期： 2021年3月1日～	試験運用中。すでに数千の脆弱なネットワークを発見し、JPCERT/CC へ報告している。商用化の計画は無し。研究発表は 1,2 年中に計画。

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

企業・大学名	国立大学法人東海国立大学機構名古屋大学
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	情報基盤センター 情報基盤ネットワーク研究部門 基盤ネットワーク研究G
ホームページのURL	
研究説明のURL	https://www.net.itc.nagoya-u.ac.jp/member/shimada/researches/network_security.html https://www.net.itc.nagoya-u.ac.jp/member/shimada/researches/cyber_security.html https://www.net.itc.nagoya-u.ac.jp/member/shimada/researches/network.html
対象技術	技術の概要・特徴など
研究開発名称： （特に名称をつけていない） 研究開発国： 日本 研究開発時期：	大学における継続的な研究であり、特に期間を区切って研究開発しているわけではない。

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	国立大学法人東海国立大学機構名古屋大学
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	研究開発機構（ユニット代表者：趙　晋輝）
ホームページのURL	
研究説明のURL	ありません
対象技術	技術の概要・特徴など
研究開発名称： 新常態環境下の情報セキュリティに関する総合的研究（ユニット名） 研究開発国： 日本 研究開発時期： 2019年4月1日～2022年3月31日	企業秘密に関係するため開示は出来ません

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

企業・大学名	京都大学学術情報メディアセンター
代表者名	センター長　岡部　寿男
所在地	〒606-8501 京都府京都市左京区吉田本町
窓口部署名	情報部　情報推進課　総務掛
電話番号	075-753-7400
関連部門名	ネットワーク研究部門
ホームページのURL	https://www.media.kyoto-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： 対話的に通信制御が可能なマルウェア解析システム 研究開発国： 日本 研究開発時期： 2020年4月～	マルウェア解析のためのサンドボックス上での通信制御の仕組みとして、対話的に制御が可能なシステムを開発している。

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

企業・大学名	学校法人立命館（立命館大学）
代表者名	森島朋三
所在地	〒604-8418 京都府京都市中京区西ノ京東栂尾町８番地
窓口部署名	BKCリサーチオフィス
電話番号	077-561-2802
関連部門名	情報理工学部
ホームページのURL	http://www.ritsumei.ac.jp/
研究説明のURL	https://www.asl.cs.ritsumei.ac.jp/研究プロジェクト:salvia
対象技術	技術の概要・特徴など
研究開発名称： 情報漏洩を防止するオペレーティングシステム 研究開発国： 日本 研究開発時期： 2003年4月1日～	情報漏洩を防止する基盤ソフトウェアというコンセプトに基づき，オーバヘッド，実現可能性，機能的限界などの各視点から，複数の実現手法について検討・開発を進めている．

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	学校法人福岡大学
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	福岡大学情報基盤センター中國研究室
ホームページのURL	
研究説明のURL	なし
対象技術	技術の概要・特徴など
研究開発名称： キーボード入力のタイミングを用いた生体認証 研究開発国： 日本 研究開発時期： 2016年9月1日～2022年3月31日	現段階では少数の被験者の協力による認証精度を確認している。 極めて高い認証精度を確認しており、近日中に多くの被験者を用いて、認認証精度を検証する計画である。 現在は、国内のセキュリティ製品を開発するメーカーと共同研究開発を推進することを協議しており、同メーカーから日本国内に向けて販売することを目指す。

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

企業・大学名	キヤノン株式会社
代表者名	御手洗冨士夫
所在地	〒146-8501 東京都大田区下丸子3-30-2
窓口部署名	
電話番号	03-3758-2111
関連部門名	デジタルビジネスプラットフォーム開発本部
ホームページのURL	https://global.canon
研究説明のURL	外部公開していません。
対象技術	技術の概要・特徴など
研究開発名称： 改ざん検知・復旧技術開発 研究開発国： 日本 研究開発時期： 2017年5月～2022年1月	改ざん検知、復旧の順に開発を進めております。改ざん検知については商用化済みでして、復旧について商用化を目指して開発を進めている状況です。

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	キヤノン株式会社
代表者名	御手洗冨士夫
所在地	〒146-8501 東京都大田区下丸子3-30-2
窓口部署名	
電話番号	03-3758-2111
関連部門名	デジタルビジネスプラットフォーム開発本部
ホームページのURL	https://global.canon
研究説明のURL	外部公開していません。
対象技術	技術の概要・特徴など
研究開発名称： 無線LANセキュリティ技術開発 研究開発国： 日本 研究開発時期： 2020年6月～2022年6月	無線LANセキュリティ技術開発として、1年以内の商用化を目指して、ハードウェアおよびソフトウェアの開発を進めております。

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

企業・大学名	キヤノン株式会社
代表者名	御手洗冨士夫
所在地	〒146-8501 東京都大田区下丸子3-30-2
窓口部署名	
電話番号	03-3758-2111
関連部門名	デジタルビジネスプラットフォーム開発本部
ホームページのURL	https://global.canon
研究説明のURL	外部公開していません。
対象技術	技術の概要・特徴など
研究開発名称： Canon ID(コンシューマ向け認証認可基盤) 研究開発国： 日本 研究開発時期： 2015年1月～2022年12月	コンシューマ向け認証認可基盤として開発を進めております。Canon IDとして商用化済みでして、現在は、Canon IDに対して多要素認証の導入などセキュリティを向上する機能を提供するべく開発を進めている状況です。

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	富士電機株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	技術開発本部　デジタルイノベーション研究所
ホームページのURL	https://www.fujielectric.co.jp/
研究説明のURL	https://www.fujielectric.co.jp/about/technology/fundamental/embedded_equipment.html
対象技術	技術の概要・特徴など
研究開発名称： 組込機器のセキュリティ技術 研究開発国： 日本 研究開発時期： 2019年4月1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	○

アクセス制御機能に関する技術の
研究開発の状況等に関する調査　　付録資料

付録３：調査票

付録３

回答用紙Ａ

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３年９月 21 日(火)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@ccn-g.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　　５．保守（サポート） 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 （　　）
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（サポート） 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
クラウドコンピューティング	ネットワークを経由してアクセスするサーバ、ストレージ等の資産管理、運用管理 クラウドサービス提供、利用に係るセキュリティ全般

＜回答用紙Ｂ･Ｃの補足＞表2　用語説明

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

公開情報及びご連絡先記入用紙

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

【公開用情報】

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

２．次にご記入いただいたお名前とご連絡先は、下記の「個人情報の取り扱いについて」により取り扱います。
なお、ご回答内容の確認のため、ご記入いただいたご連絡先に別途、株式会社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。