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５年１２月

警察庁サイバー警察局 サイバー企画課

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

第１部 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 個人所有端末装置のセキュリティ対策【問5-1】 21
3.1.4 テレワークの実施状況 【問6】 24
3.1.5 テレワークの開始時期 【問6-1】 27
3.1.6 テレワーク業務の端末装置（パソコン、スマートフォン等）の利用環境【問6-2】 29
3.1.7 テレワークを行っていない理由 【問6-3】 31
3.1.8 事業体内のネットワーク利用状況 【問7】 34
3.1.9 クラウドサービスの利用状況 【問8】 36
3.1.10 外部からの接続許可状況 【問9】 38
3.1.11 情報セキュリティ対策の必要性の理由【問10】 41
3.1.12 過去に受けたことのある被害状況 【問10-1-1】 45
3.1.13 攻撃手段 【問10-1-2】 48
3.1.14 関連会社や取引先等に被害を与えてしまったことがあるか 【問10-2】 50
3.1.15 被害を受けたことによる対策 【問10-3】 52
3.1.16 届出先機関等 【問10-4-1】 55
3.1.17 届出した理由 【問10-4-2】 58
3.1.18 届出を躊躇させる要因 【問10-5】 61
3.1.19 届出先機関を知っているか 【問11】 64
3.1.20 不正アクセス禁止法でアクセス管理者による防御措置についての努力義務【問12】 67
3.1.21 情報セキュリティ対策の実施状況 【問13】 67
3.1.22 情報セキュリティ運用・管理専門部署の有無 【問13-1】 70

3.1.23　情報セキュリティ管理体制　【問13-2】 74
3.1.24　セキュリティポリシーの策定状況　【問13-3】 77
3.1.25　セキュリティ関連事項の定期的な議論の状況【問13-3-1】 79
3.1.26　情報セキュリティ侵害事案発生時の対応マニュアル等の策定状況【問13-4】 81
3.1.27　第三者機関の認証制度等の利用状況　【問13-5】 83
3.1.28　次年期の情報セキュリティ対策の投資計画　【問13-6】 85
3.1.29　情報セキュリティ対策への投資に関する問題点　【問13-7】 88
3.1.30　情報セキュリティ対策を行っていない理由　【問13-8】 92
3.1.31　サプライチェーンリスク対策として対策を行っているか　【問14】 93
3.1.32　情報セキュリティ対策に関する考え方　【問15】 95
3.1.33　投資に関する考え方　【問15-1】 98
3.1.34　事後的対応と予防的対応に関する考え方　【問15-2】 100
3.1.35　保険への意識　【問15-3】 103
3.1.36　規制・罰則への考え方　【問15-4】 105
3.1.37　プライバシーの考慮に関する考え方　【問15-5】 107
3.1.38　利便性とのバランスに関する考え方　【問15-6】 109
3.2　技術的対策 112
3.2.1　セキュリティパッチの適用状況　【問16】 112
3.2.1　利用しているセキュリティサービス　【問17】 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17-1】 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18】 118
3.2.4　VPN機器のセキュリティ対策　【問18-1】 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19】 123
3.2.6　外部からの接続に対するセキュリティ対策　（通信路に対する対策）【問20-A】 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20-B】 129
3.2.8　社外等からのインターネット接続経由の認証方法　【問21】 131
3.2.9　ID・パスワードの管理方法　【問21-1】 133
3.2.10　不正ログイン対策　【問21-2】 135
3.2.11　フィッシング対策【問22】 138
3.2.11　各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）の利用状況【問23】 141
3.2.12　各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）の管理環境【問23-1】 143
3.2.13 各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）のセキュリティ対策【問23-2】 145
3.2.14　ぜい弱性調査（ペネトレーションテスト）実施の有無　【問23-3】 147
3.2.15　ログの取得状況　【問23-4】 150
3.2.16　ログの保管期間　【問23-4A】 152
3.2.17　ログの保管方法　【問23-4B】 153

3.2.18　ログを取得・保管している理由　【問23-4-1】 154
3.2.19　電子メールに関するセキュリティ対策　【問24】 155
3.2.20　添付ファイルの取り扱い　【問25】 159
3.2.21　重要システムの不正アクセス対策状況　【問26】 162
3.2.22　不正アクセス等への対策状況　【問27】 166
3.2.23　不正プログラムへの対策状況　【問28】 169
3.3　人的対策 171
3.3.1　情報セキュリティ教育の実施状況　【問29】 171
3.3.2　情報セキュリティ教育の内容　【問29-1】 175
3.3.3　情報セキュリティ教育の頻度　【問29-2】 177
3.3.4　情報セキュリティ教育を実施しない理由　【問29-3】 180
3.3.5　セキュリティ人材を確保するための施策　【問30】 181
3.3.6　セキュリティ対策の問題点や不安等 182
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 186
4.調査概要 188
4.1　調査の目的 188
4.2　調査の対象と調査方法 188
4.3　調査内容 189
4.4　送付・回収状況、集計対象件数 190
4.5　報告書を見る際の留意点 190
5.調査結果（概要と考察） 191
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 191
5.1.1　現在、取り組んでいる分野　【A-問2】 192
5.1.2　今後、もっとも力を入れたい分野　【A-問3】 195
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 198
5.2.1　現在、実用化(製品化)されている分野　【A-問4】 199
5.2.2　今後、実用化(製品化)を見込んでいる分野　【A-問5】 202
5.3　研究開発体制 205
5.3.1　年間の研究開発費　【A-問6】 206
5.3.2　研究開発に携わっている人数　【A-問7】 209
5.4　実用化された製品及び研究開発中の技術・サービス 212
5.4.1　何を守るか？ 213
5.4.2　何から保護するか？ 215
5.4.3　どのようなセキュリティ上の効果があるか？ 217
5.4.4　どのような機能を持つか？ 219
5.4.5　どのようなレイヤーのセキュリティを守るか？ 221
5.4.6　不正アクセスからの防御対象 223
5.4.7　どのようなサービスか？ 225

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？ 227
5.6　研究開発の進捗状況 228
5.7　発売時期の分布 229
5.8　研究開発期間の分布 230
5.9　実用化された製品及び研究開発中の技術・サービス 231
5.9.1　「技術の実用化（製品化）状況」について 233
5.9.2　「技術の研究開発状況」について 245
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

第１部

不正アクセス行為対策等の実態調査

1. 調査概要

1.1 調査の目的

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

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

1.2 調査の対象と調査方法

調査対象は、市販のデータベース（四季報）に掲載された企業、教育機関（国公立、私立の大学等）、医療機関、地方公共団体（県・市区町村等）、独立行政法人（教育機関及び医療機関に掲げるものを除く。）、特殊法人から特定の業種、地域に偏りのないよう2,951件を無作為に抽出した。

調査は、調査票を郵送で配付し、次の2つの方法で回収することで実施した。

① 電子メールでの回答

調査票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5年8月23日(水)（発送日）～9月15日(金)（締切日））

1.3 調査内容

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

1.4 送付、回収状況

調査票の送付総数は2,951件、回収総数は618件であった。回収率は20.9％である。

業種	発送数	回収数	回収率
農林・水産・鉱業	10	3	30.0%
製造業	901	168	18.6%
不動産・建築	187	42	22.5%
金融	108	38	35.2%
エネルギー	15	6	40.0%
運輸業	75	9	12.0%
情報通信	291	15	5.2%
サービス	837	116	13.9%
教育	290	131	45.2%
行政サービス	237	83	35.0%
無回答		7	－
合計	2,951	618	20.9%

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5年度の調査結果については、次のような特徴がみられる。

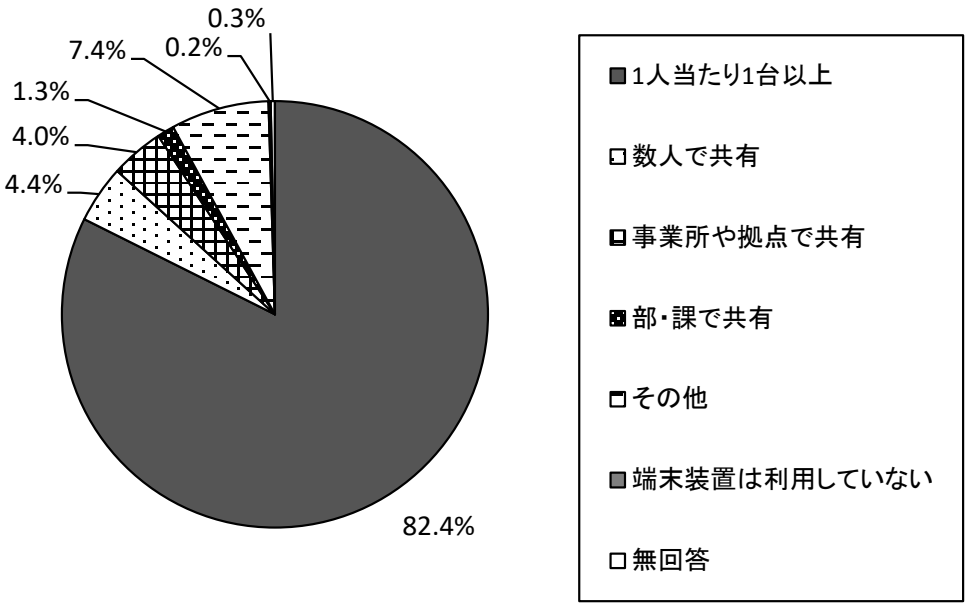
1　組織的対策状況

【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、82.4%で「1人当たり1台以上」で整備されており、「数人で共有」が4.4%、「事業所や拠点で共有」が4.0%となっている。テレワークの実施状況については、「行っている」が63.4%となっている。

事業体内のネットワーク利用状況については、「有線ネットワークと無線ネットワークを併用」が91.1%で最も高く、次いで「全て有線ネットワークで構築」が6.1%となっている。「全て無線ネットワークで構築」を含めるとほぼ全ての事業所でネットワークが導入されている。外部からの接続に対する許可についても、「許可している」が66.0%で、半数以上が外部からの接続を許可している。

【全体】端末装置（タブレット・スマートフォン等）の整備環境(SA,n=618)



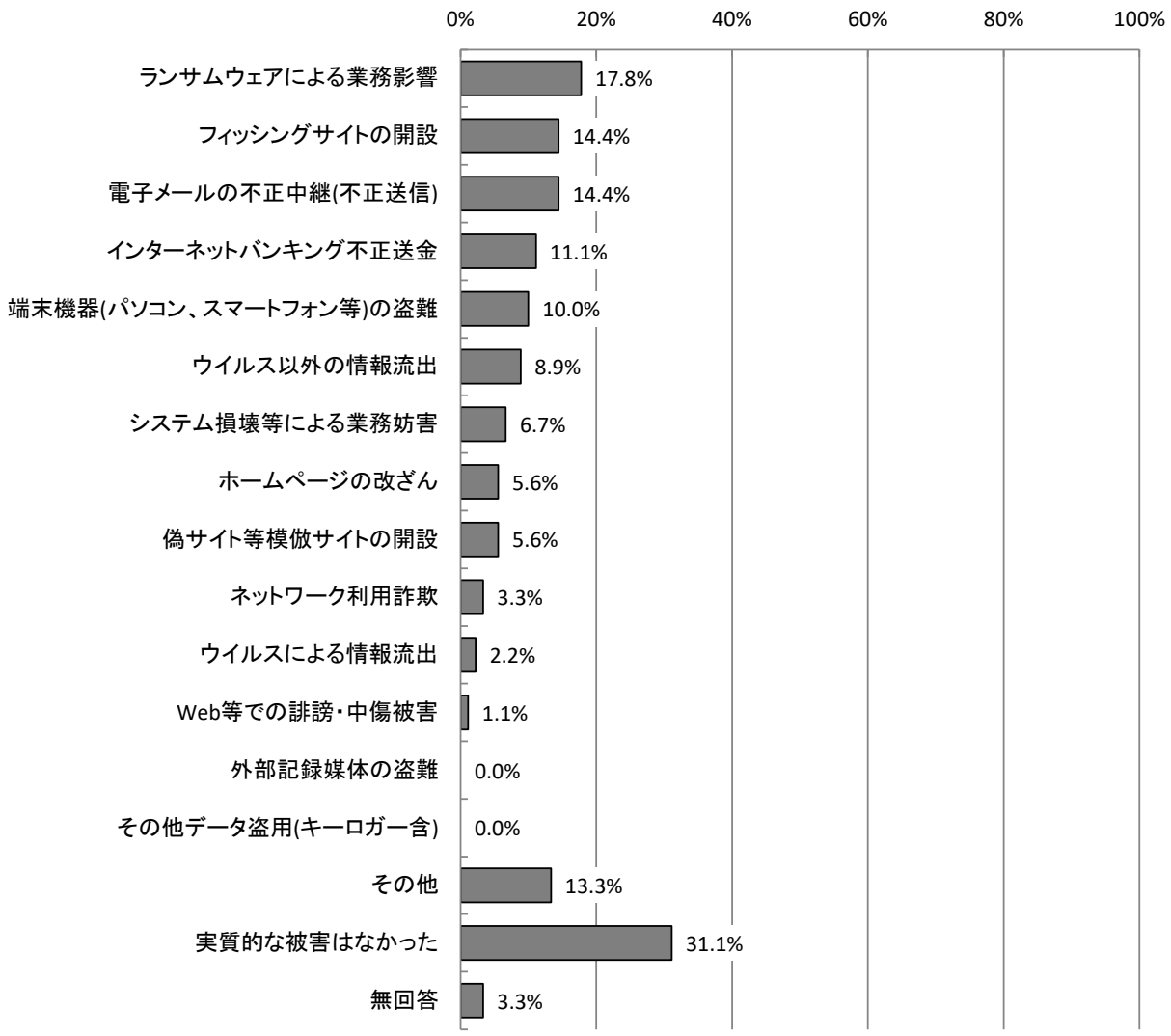
【不正アクセス等の被害状況】

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（90団体）について、被害内容をみると「ランサムウェアによる業務影響」が17.8%で高い。

届出先機関等については、「警察」が42.2%、「監督官庁」が22.2%、「個人情報保護委員会」が15.6%となっている。「届け出なかった」は35.6%と3割を超えている。

届出を躊躇させる要因は、「実質的な被害が無かったので」が68.8%で高く、次いで「社・団体内で対応できたので」が18.8%、「届出義務がないので」が9.4%で、被害が無かったと感じた場合や、自社以外に被害が及ばなかった場合、届出を躊躇する傾向が見られる。

【全体】過去に受けたことのある被害状況（MA,n=90）



【情報セキュリティの運用・管理体制】

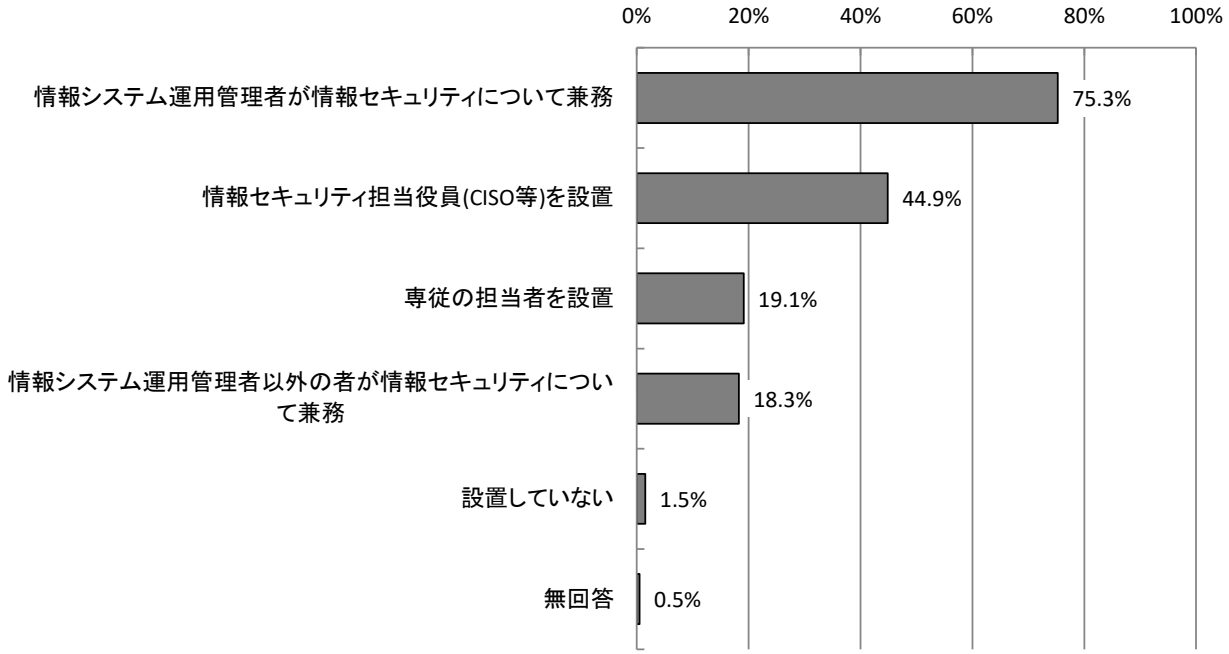
情報セキュリティ対策を行っている社・団体等（586団体）のうち、情報セキュリティ運用・管理専門部署の有無については、「ある」が72.5%であり、管理体制は「情報システム運用管理者が情報セキュリティについて兼務」が75.3%で最も多くなっており、「情報セキュリティ担当役員(CISO等)を設置」は44.9%となっている。

セキュリティポリシーの策定状況は、「策定している」が87.4%で高く、「今のところ、策定する予定はない」は2.2%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95.6%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となっている。

情報セキュリティ侵害事案発生時の対応マニュアル等の策定状況については、「策定している」が56.8%と過半数で、「策定することを検討」が28.0%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74.7%となっている。

【全体】情報セキュリティ管理体制（MA, n=586）

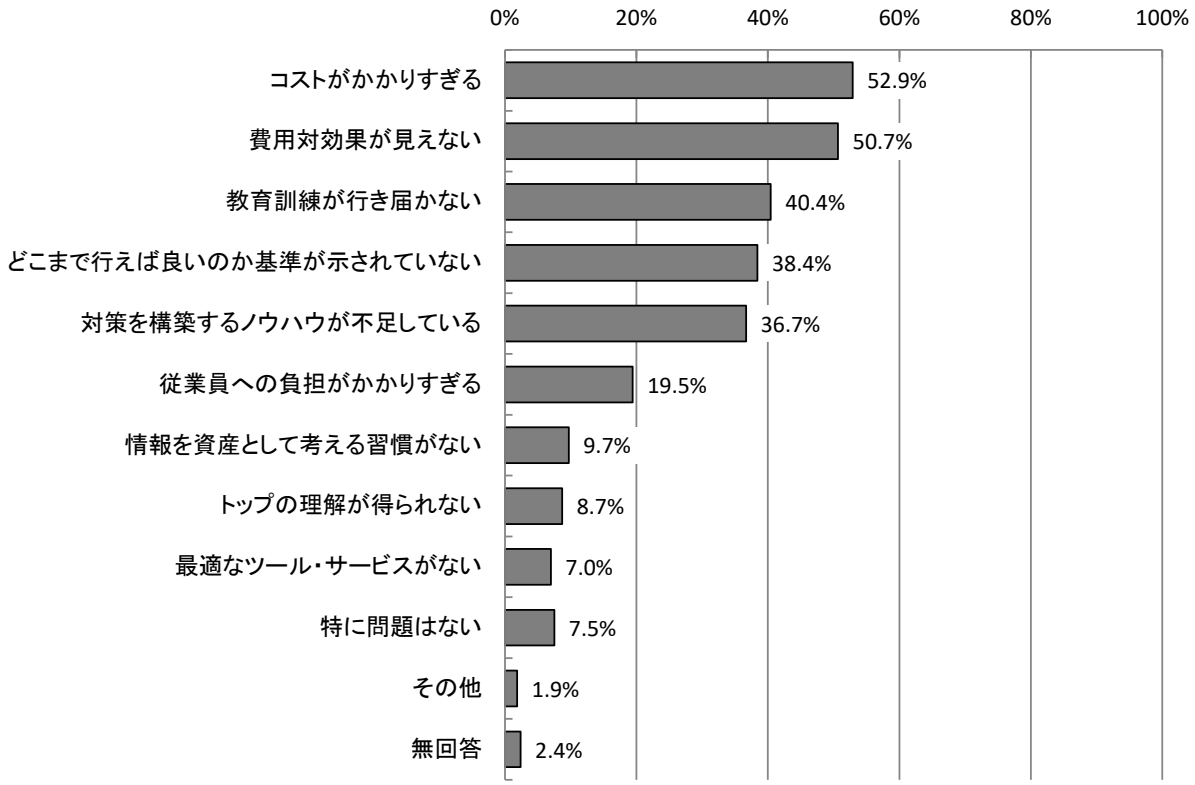


【情報セキュリティ対策への投資】

令和６年度の情報セキュリティ対策の投資計画については、令和５年度と比較して「現状どおりの予定」が59.0%で最も高く、「増額する予定」が30.4%、「減額する予定」は1.5%となっている。

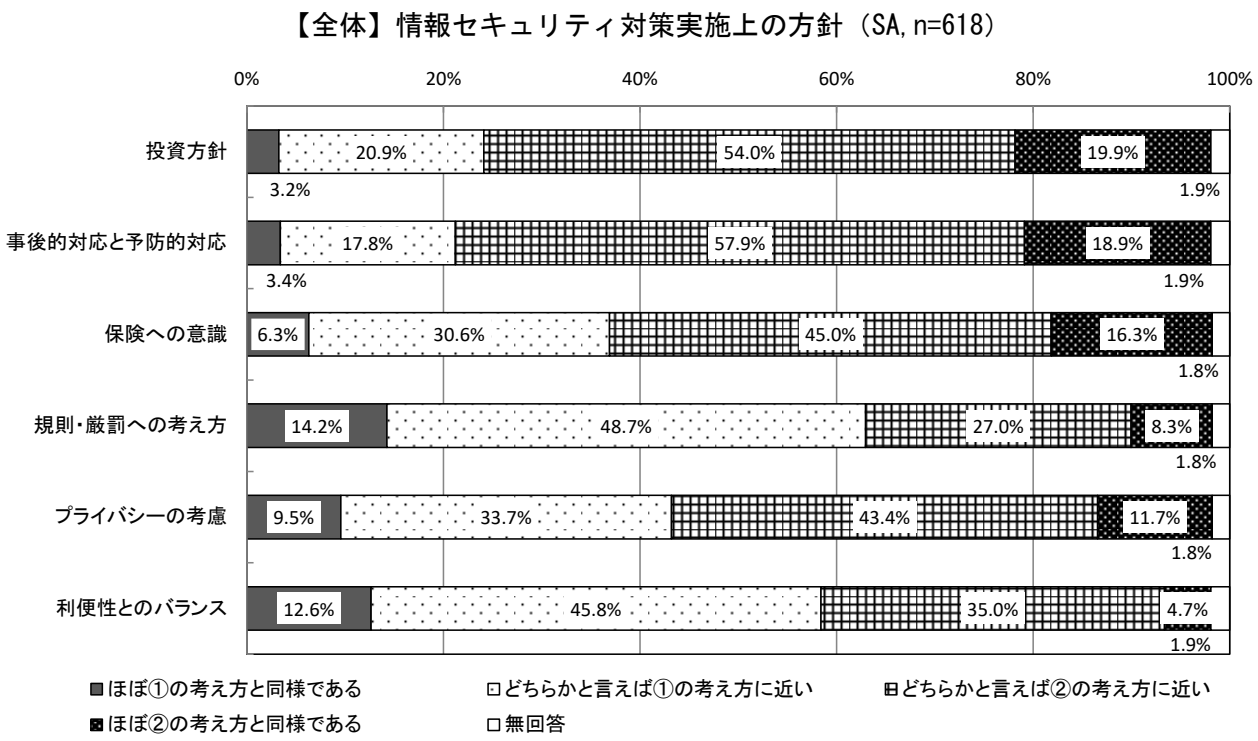
情報セキュリティ対策への投資に関する問題点は、「コストがかかりすぎる」が52.9%、「費用対効果が見えない」が50.7%で高くなっている。次いで「教育訓練が行き届かない」が40.4%、「どこまで行えば良いのか基準が示されていない」が38.4%となっている。

【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=586)



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



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。
規則・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	業務実態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

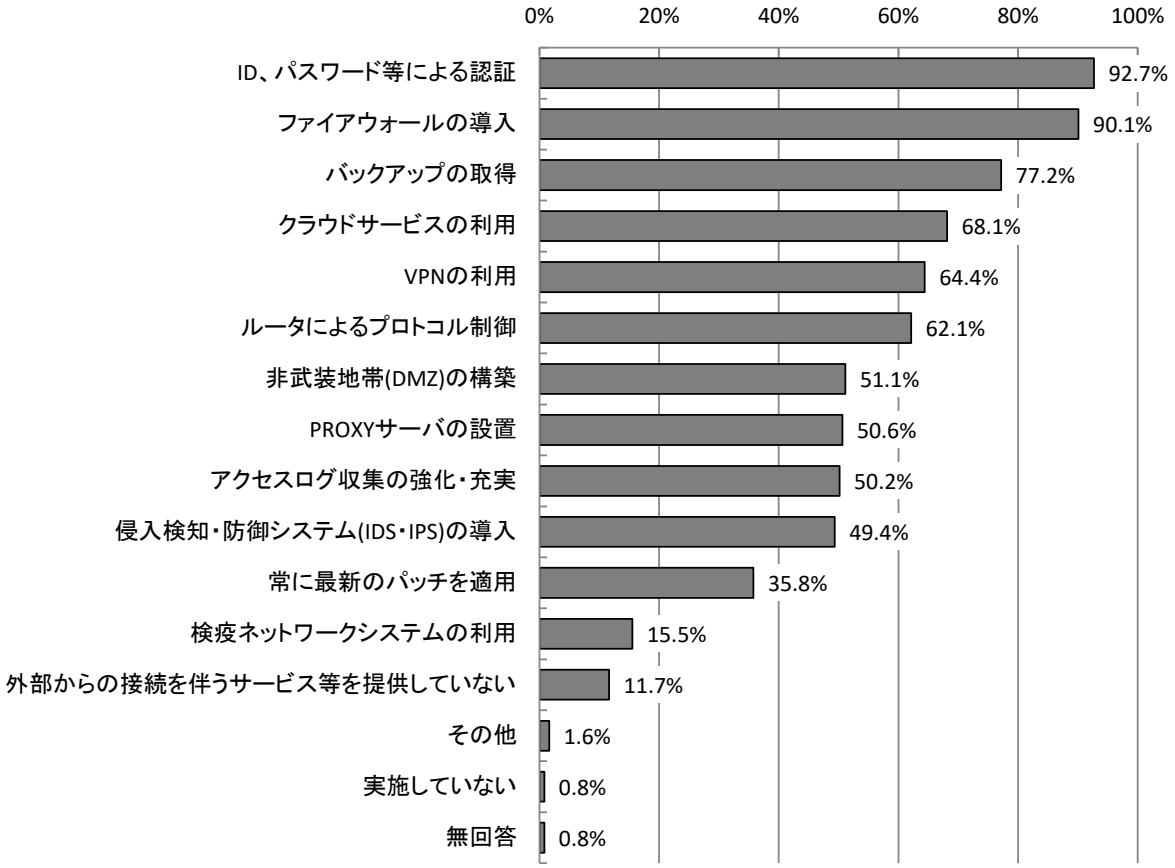
【ネットワークに対する情報セキュリティ対策】

安全なアクセス環境を維持するための対策については、「ID、パスワード等による認証」が92.7%で最も高く、次いで「ファイアウォールの導入」が90.1%、「バックアップの取得」が77.2%となっている。

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87.7%で最も高く、次いで「通信の暗号化」が69.6%、となっている。

端末に対する対策については、「ウイルス対策ソフト等の導入」が86.5%で最も高く、次いで「各種ログの保管」が45.6%となっている。

【全体】安全なアクセス環境を維持するための対策（MA,n=618）

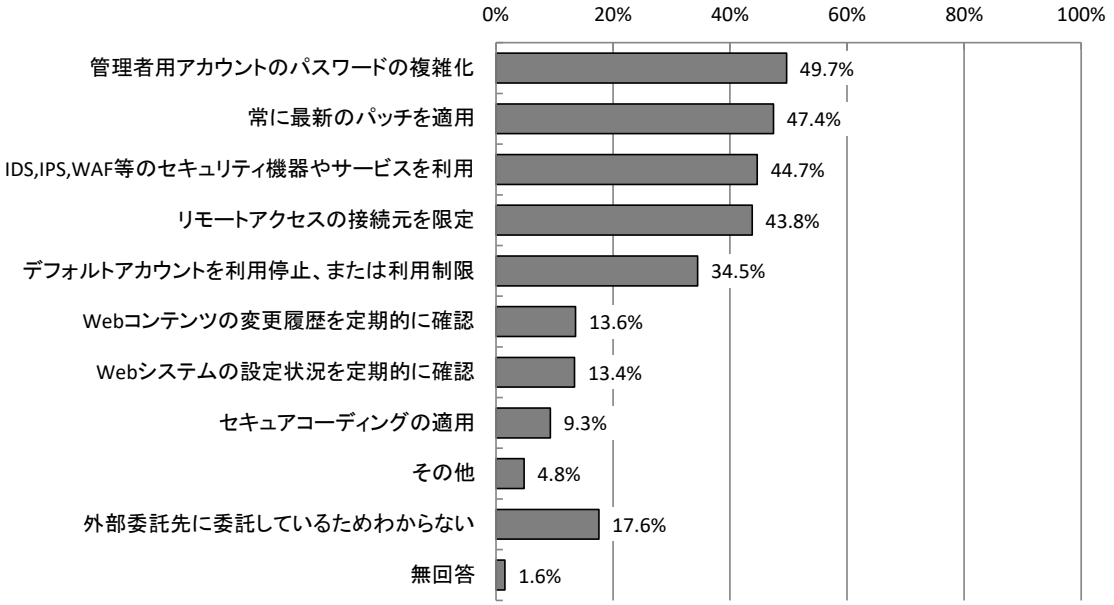


【各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）のセキュリティ対策】

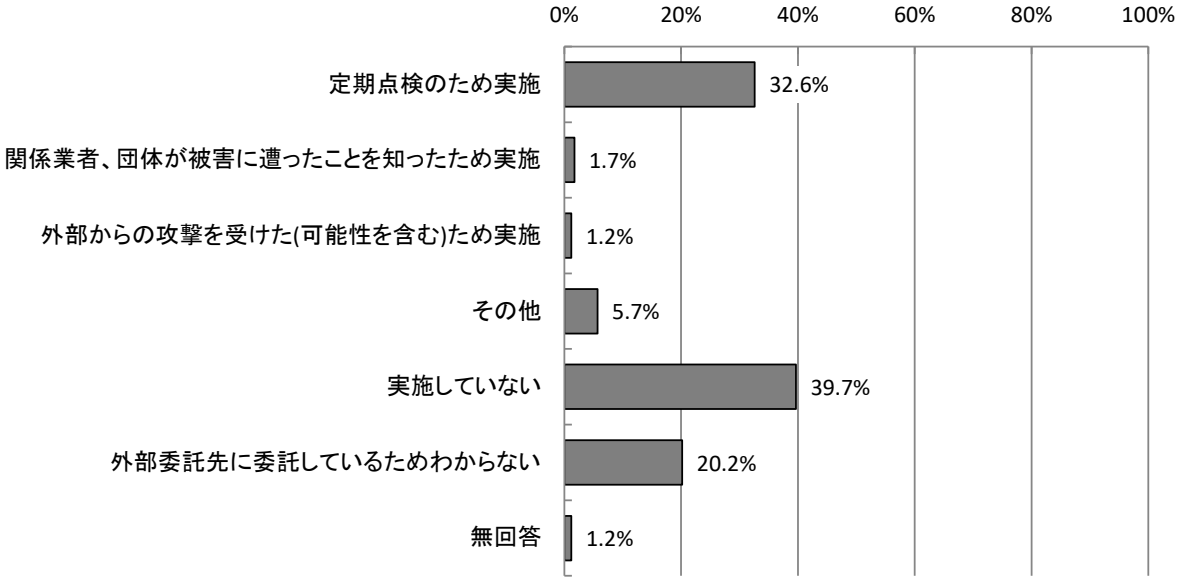
各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）のセキュリティ対策については、「管理者用アカウントのパスワードの複雑化」が49.7%で最も多く、次いで「常に最新のパッチを適用」が47.4%、「IDS,IPS,WAF等のセキュリティ機器やサービスを利用」が44.7%となっている。

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39.7%と最も多く、次いで「定期点検のため実施」が32.6%となっている。

【全体】各種サービスのセキュリティ対策（MA,n=580）



【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=580）

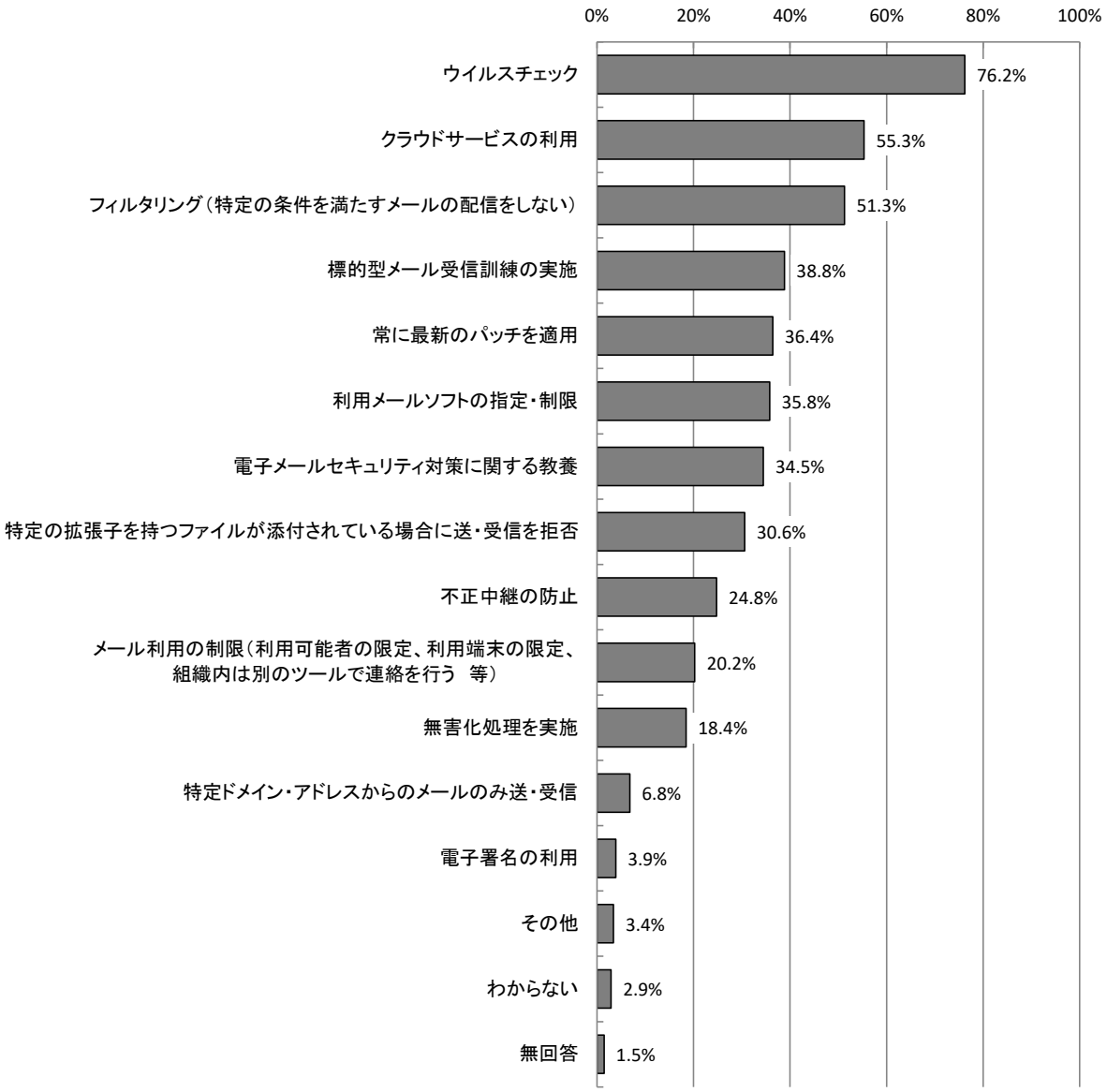


【電子メールに関するセキュリティ対策】

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76.2%で最も高く、次いで「クラウドサービスの利用」が55.3%、「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）」が51.3%となっている。

添付ファイルの取り扱いについては、「ウイルスチェックをしてから受信」が74.9%で最も高い。一方、「特にチェック等はしていない」は10.5%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=618）

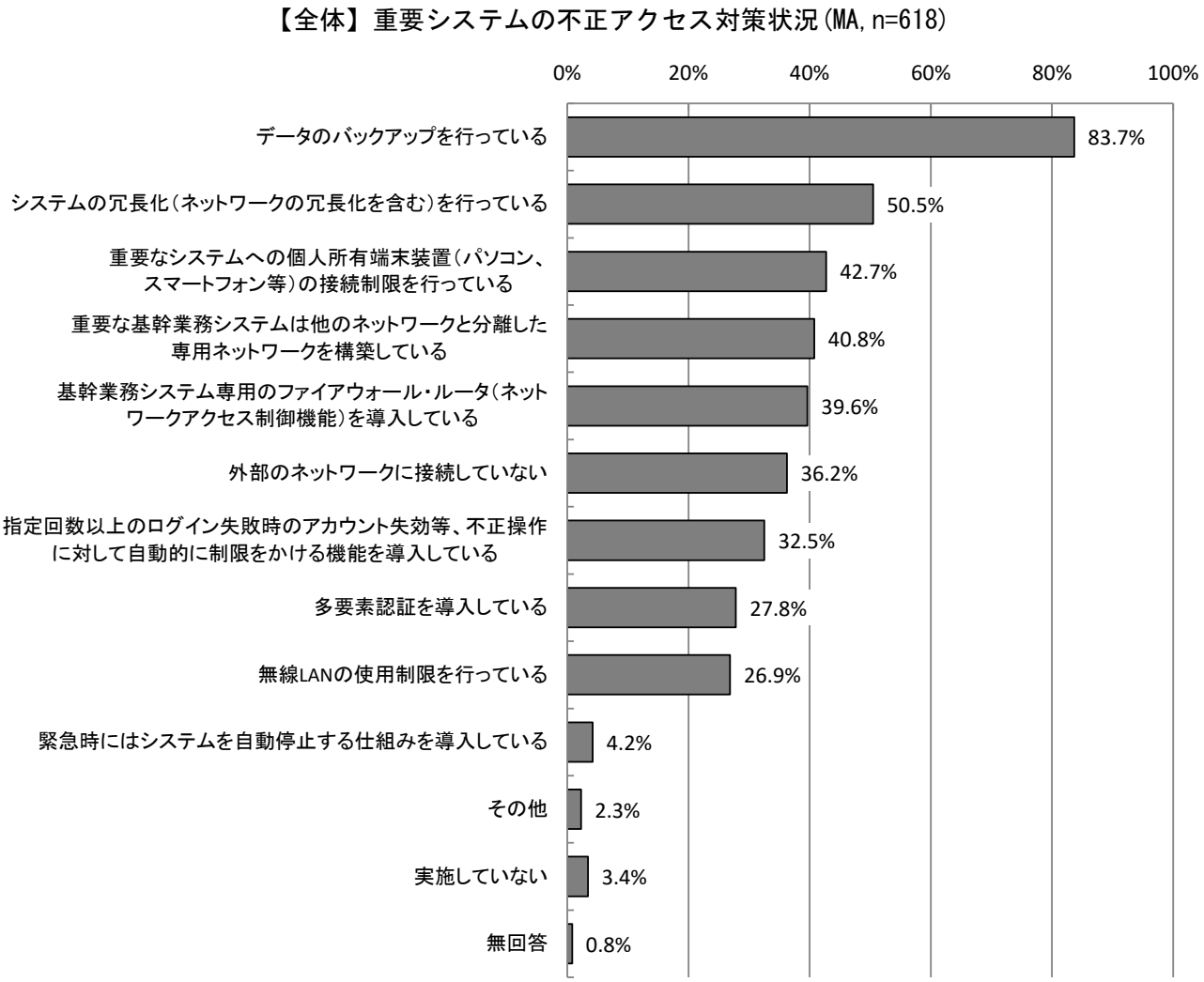


【不正アクセス、情報漏えい等に対する情報セキュリティ対策】

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83.7%で最も高く、「システムの冗長化（ネットワークの冗長化を含む）を行っている」が50.5%、「重要なシステムへの個人所有端末装置（パソコン、スマートフォン等）の接続制限を行っている」が42.7%、「重要な基幹業務システムは他のネットワークと分離した専用ネットワークを構築している」が40.8%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79.3%で最も高く、次いで「情報資産へのアクセス権の設定」が73.1%「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68.6%、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91.1%で最も高く、次いで「ウイルス対策ソフト（サーバ）の使用」が77.5%、「パターンファイルを定期的に更新する（自動更新システムを利用）」が72.0%となっている。



３　人的対策

【情報セキュリティ教育】

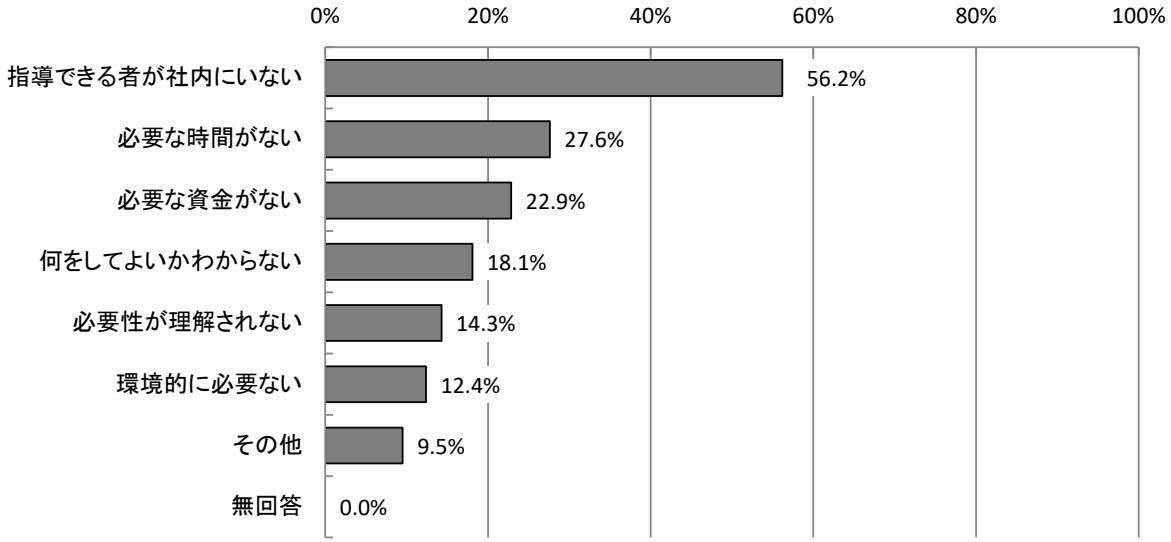
情報セキュリティ教育の実施状況は「実施している」が76.4%、「実施していない」が17.0%、「実施を予定している」が4.4%となっている。実施状況は従業員規模で違いがみられ、従業員数100人未満の社・団体では41.2%と実施率が低い。

なお、情報セキュリティ教育を実施しない理由については、「指導できる者が社内にいない」が56.2%で最も多く、次いで「必要な時間がない」が27.6%となっている。

情報セキュリティ教育の内容については、「ITリテラシー教育(インターネット・電子メール・SNS等の利用)」が80.6%、「情報セキュリティポリシー」が68.9%、「個人情報の保護・管理」が67.1%で高くなっている。

教育の頻度については、「年に１回」が44.3%で最も高く、次いで「年に数回」が38.3%、「採用、異動時等に実施」が25.9%となっている。

【全体】情報セキュリティ教育を実施しない理由(MA,n=105)

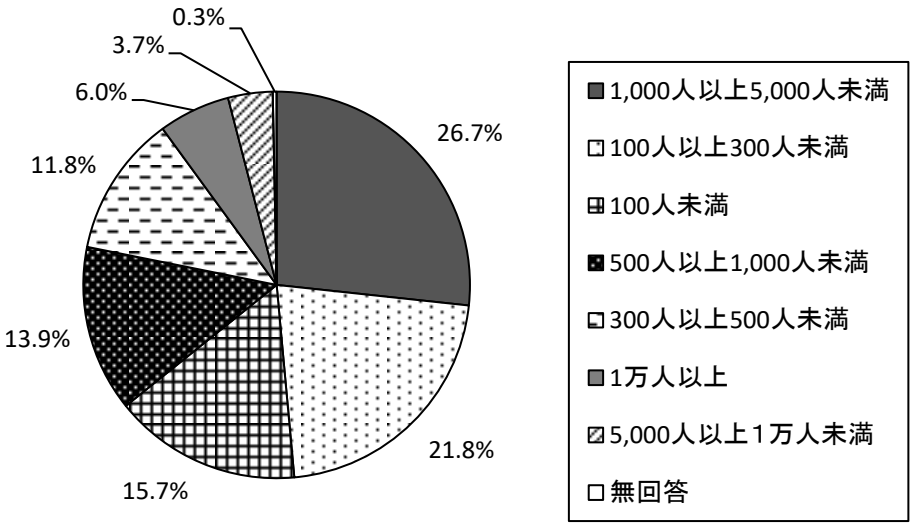


今回の調査結果では、情報セキュリティポリシーが、全体の８割以上で制定されており、情報セキュリティに関する教育においても、全体の７割以上で実施されている等、情報セキュリティに関する意識について一定の浸透が図られていることがうかがえる。その一方で、小規模組織におけるセキュリティ教育の実施率が低いことや、情報セキュリティ対策についてコストがかかりすぎる・費用対効果が見えない等の問題意見が出されるなど、問題点も明らかになった。

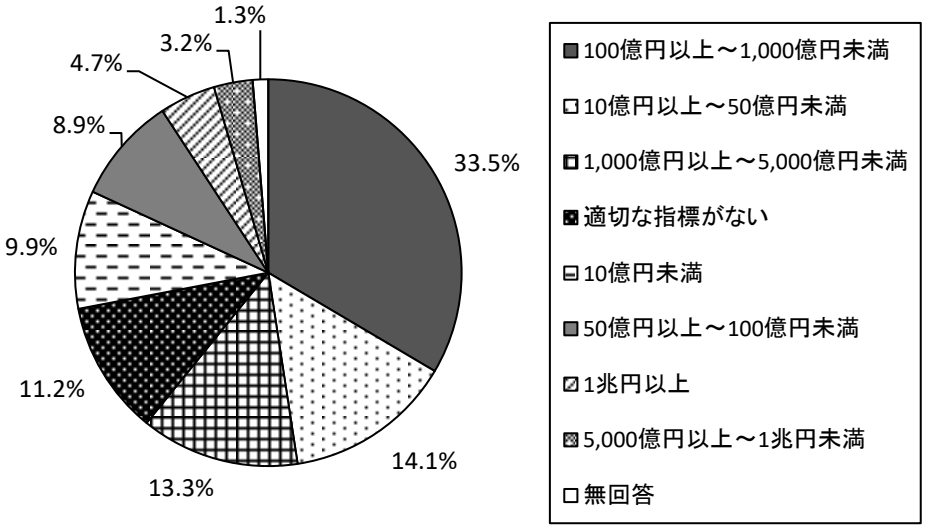
また、過去１年間に攻撃・被害を受けた社・団体等が全体の14.6%と依然として少なくない。そのうちランサムウェアによる業務影響が最も高い割合であり、セキュリティ対策が重要と認められる。セキュリティ侵害事案発生時における対応マニュアルの策定が、半数程度にとどまっている状況であり、事案発生の際の被害拡大防止のため、これら対策意識の浸透が今後の課題といえよう。

2.2 回答事業体の属性等

【全体】従業員規模（SA, n=618）【問2】



【全体】予算規模（SA, n=618）【問3】



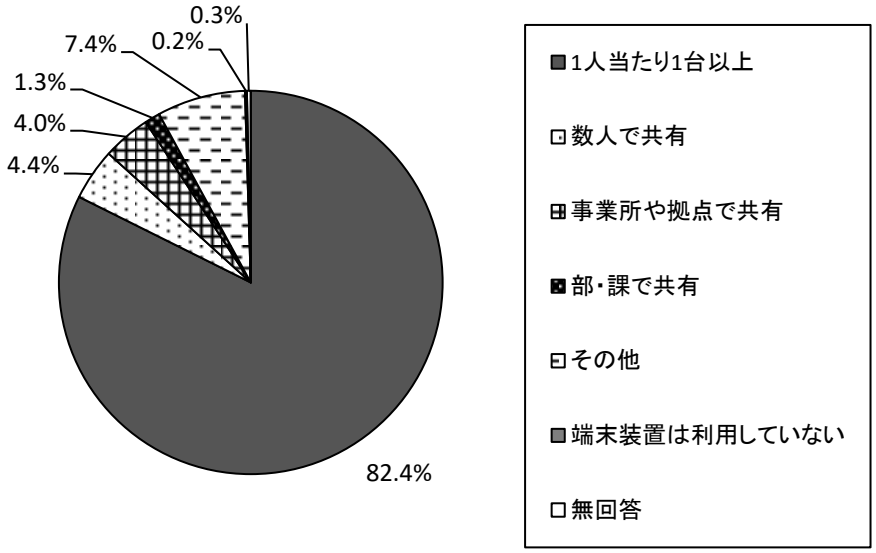
3. 調査結果

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】

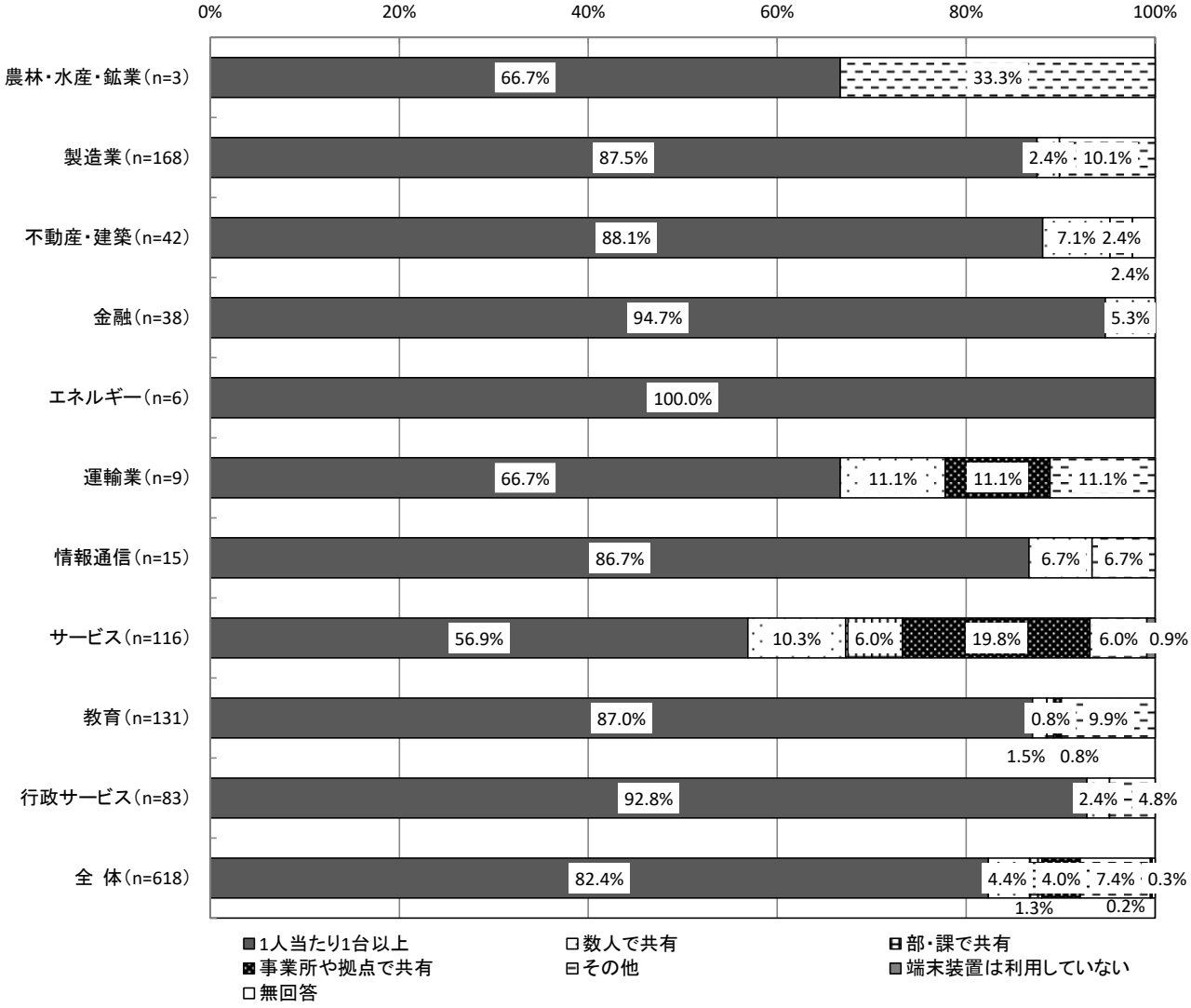
端末装置（パソコン）の整備環境については、「1人当たり1台以上」が82.4%で最も高く、「数人で共有」が4.4%、「事務所や拠点で共有」が4.0%となっている。

【全体】端末装置（パソコン、スマートフォン等）の整備環境（SA,n=618）



【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」が100.0%、「金融」が94.7%、「行政サービス」が92.8%で9割を超えて高い割合となっている。一方、「サービス」で56.9%と最も低く、「運輸業」で66.7%と低くなっている。

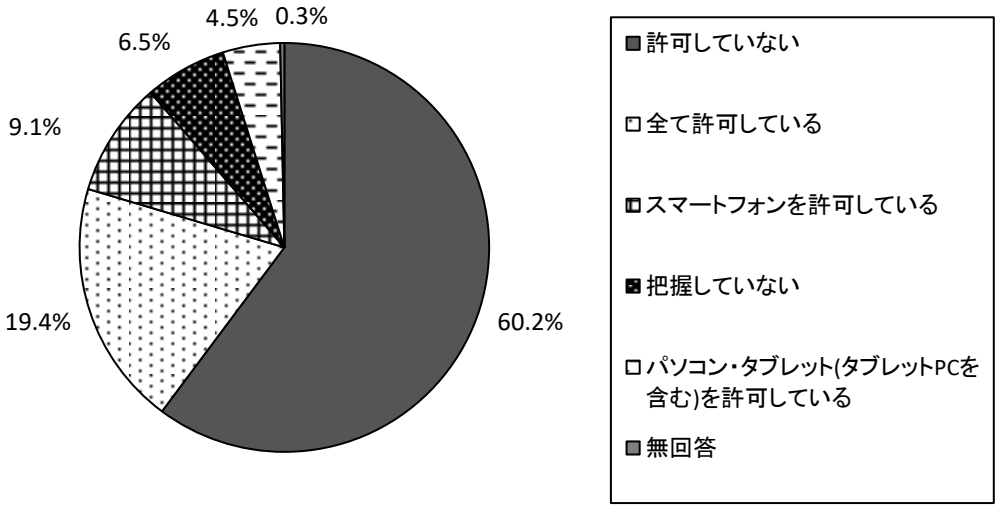
【業種別分析】端末装置（パソコン、スマートフォン等）の整備環境



3.1.2　業務における個人所有端末装置の扱い　【問5】

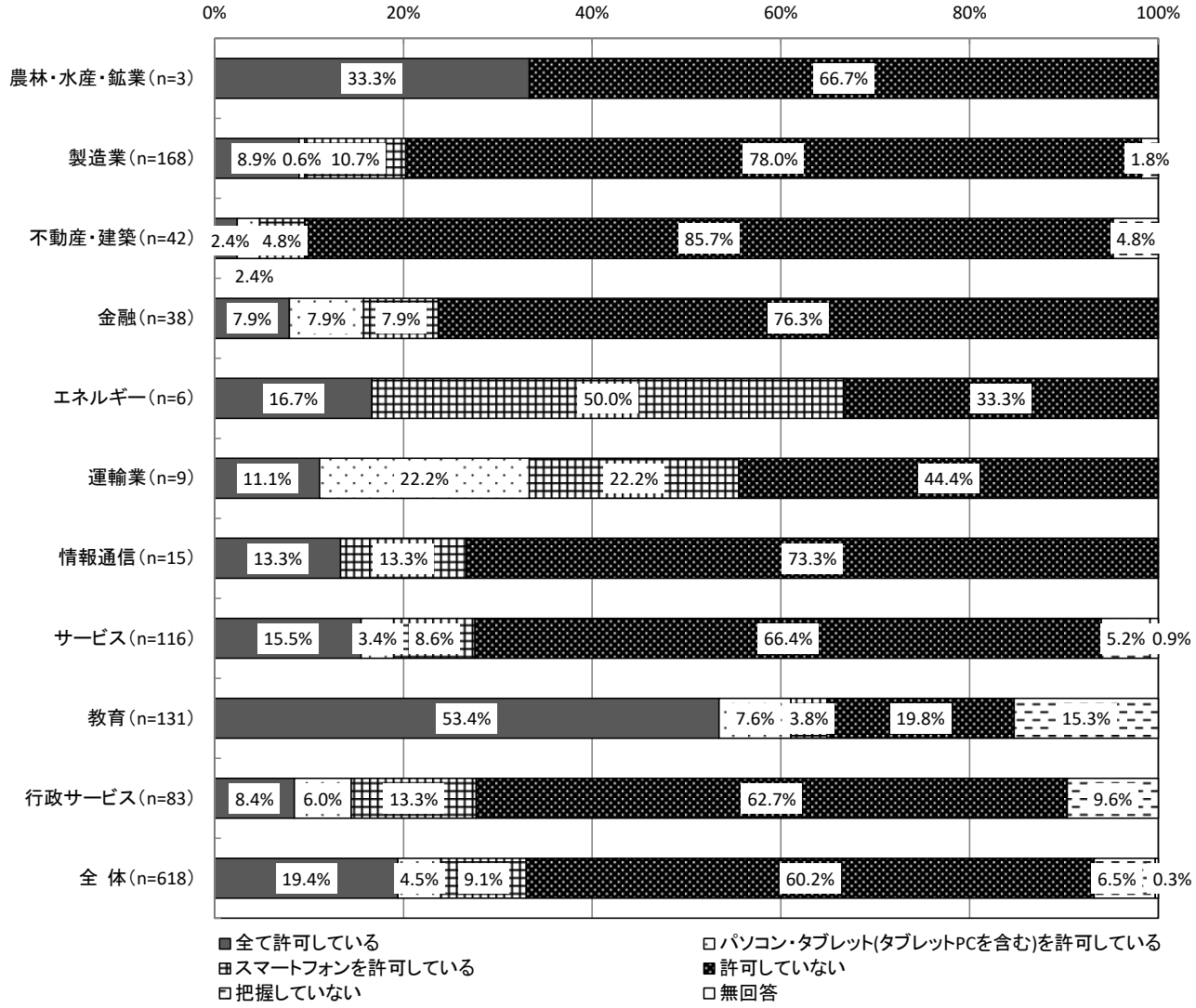
業務における個人所有端末装置の扱いについては、「許可していない」が60.2%で最も高く、「全て許可している」が19.4%、「スマートフォンを許可している」が9.1%となっている。

【全体】業務における個人所有端末装置の扱い（SA,n=618）

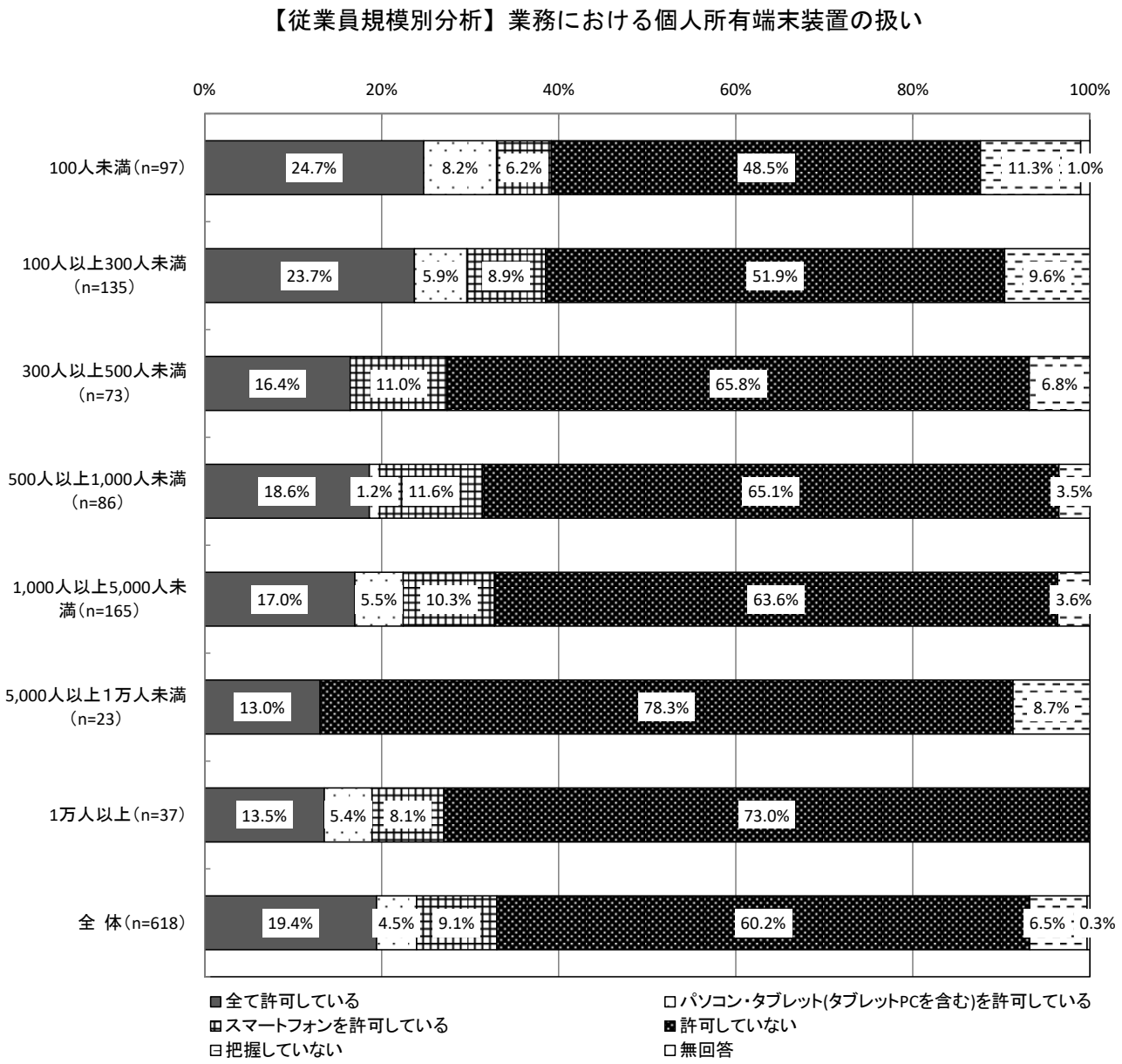


【業種別分析】業種別にみると、「許可していない」では、「不動産・建築」が85.7%で最も高く、次いで「製造業」が78.0%、「金融」が76.3%となっている。一方、最も低いのは「教育」で19.8%となっている。

【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、「5,000人以上１万人未満」が78.3%で最も高く、次いで「1万人以上」が73.0%で7割を超えている。一方、最も低いのは「100人未満」48.5%、次いで「100人以上300人未満」51.9%となっている。

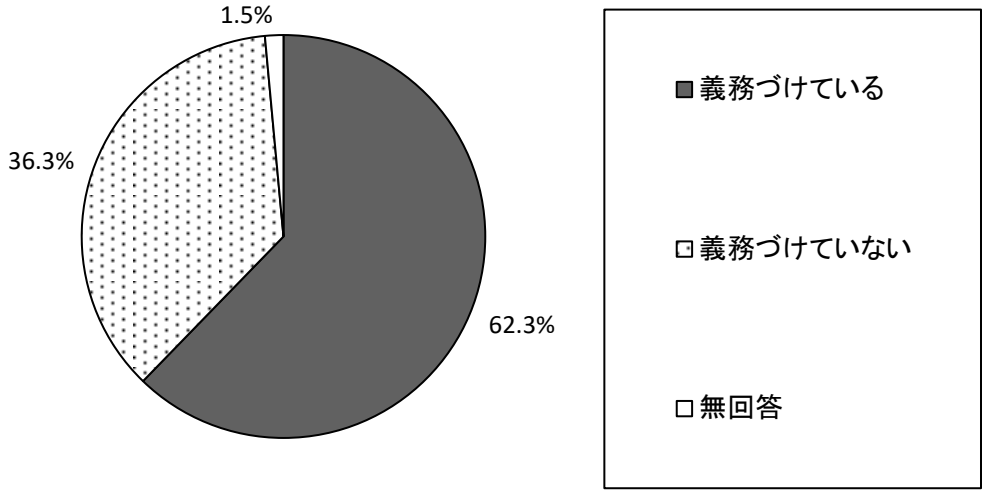


3.1.3　個人所有端末装置のセキュリティ対策【問5-1】

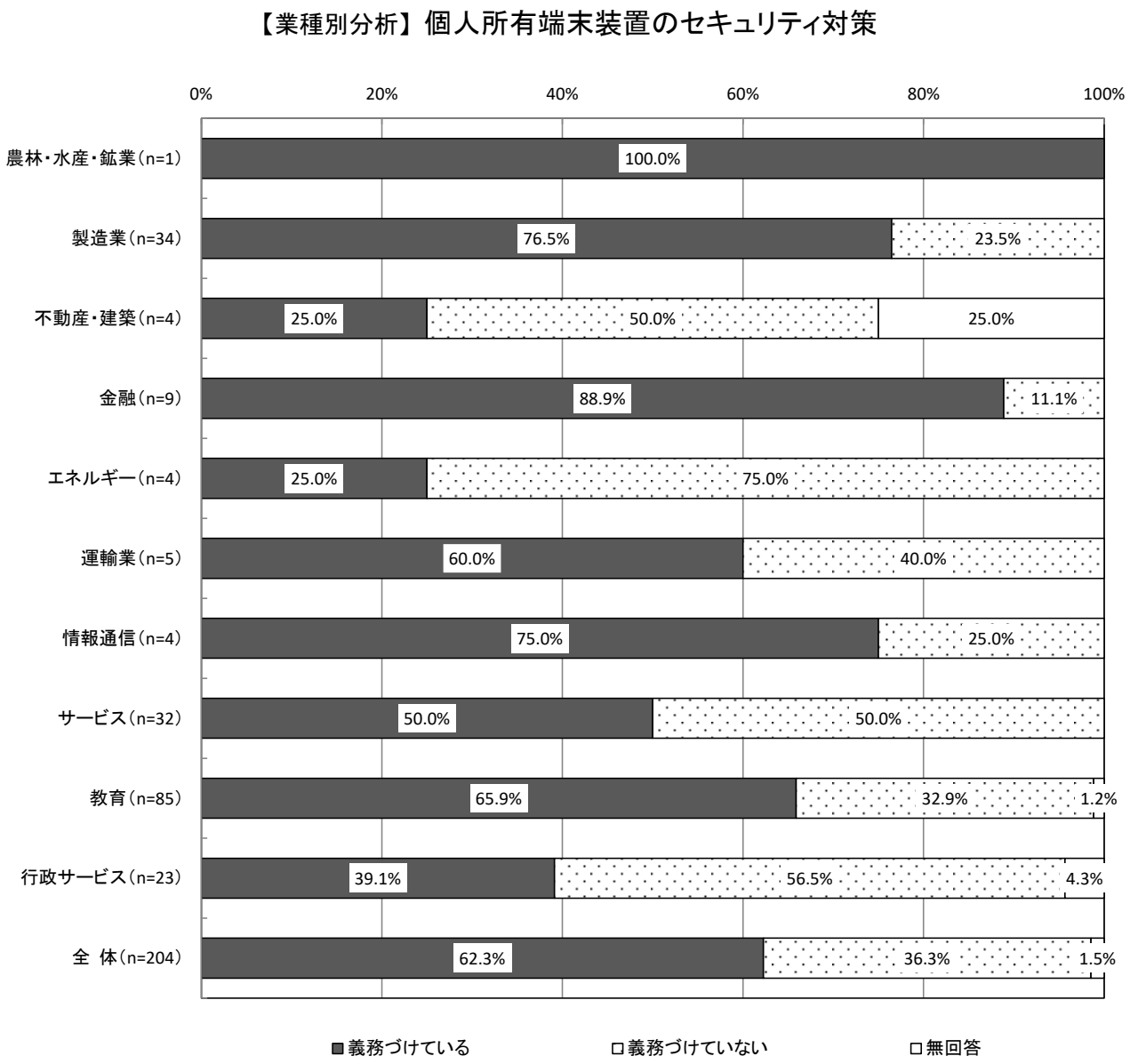
個人所有端末装置のセキュリティ対策については「義務づけている」が62.3%で高くなっている。これに対して「義務づけていない」は36.3%となっている。

※本項目は、個人所有端末装置を許可している社・団体等を対象としている。

【全体】個人所有端末装置のセキュリティ対策（SA,n=204）

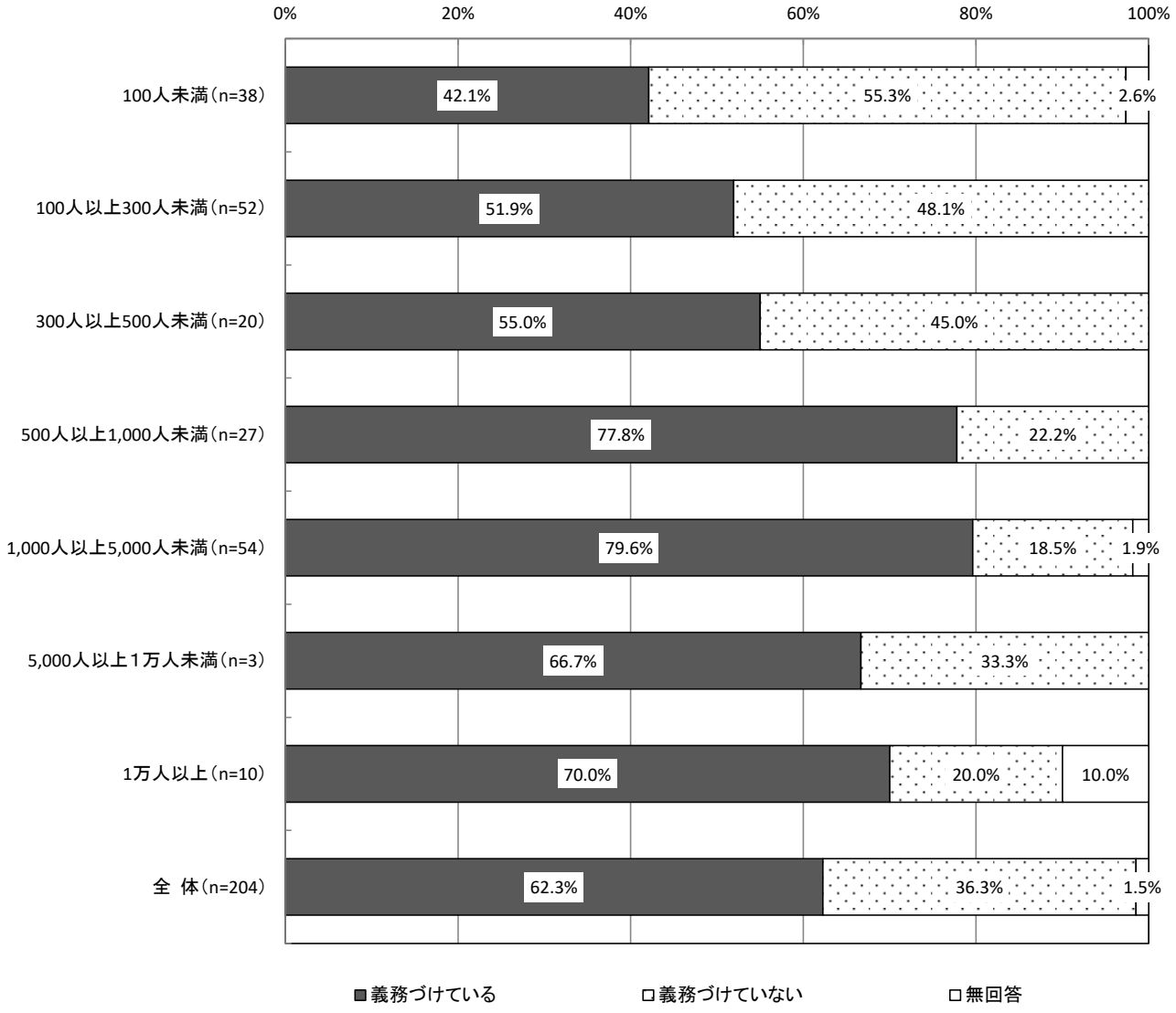


【業種別分析】業種別にみると、「義務づけている」は「金融」が88.9%、「製造業」が76.5%でいずれも高い。一方「行政サービス」が39.1%で低くなっている。



【従業員規模別分析】従業員規模別にみると、「義務づけている」は「1,000人以上5,000人未満」が79.6%、「500人以上1,000人未満」が77.8%で高くなっている。これに対して「100人未満」は42.1%と低くなっている。

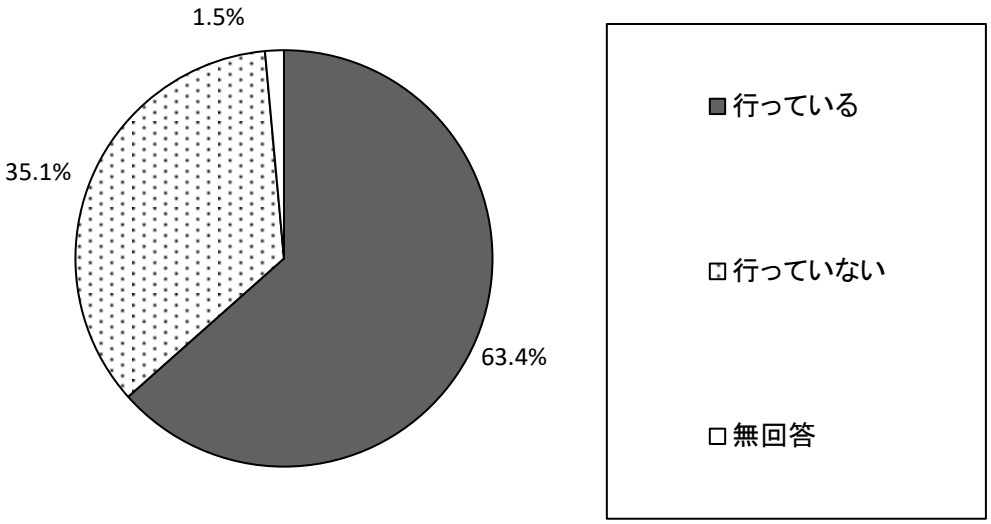
【従業員規模別分析】個人所有端末装置のセキュリティ対策



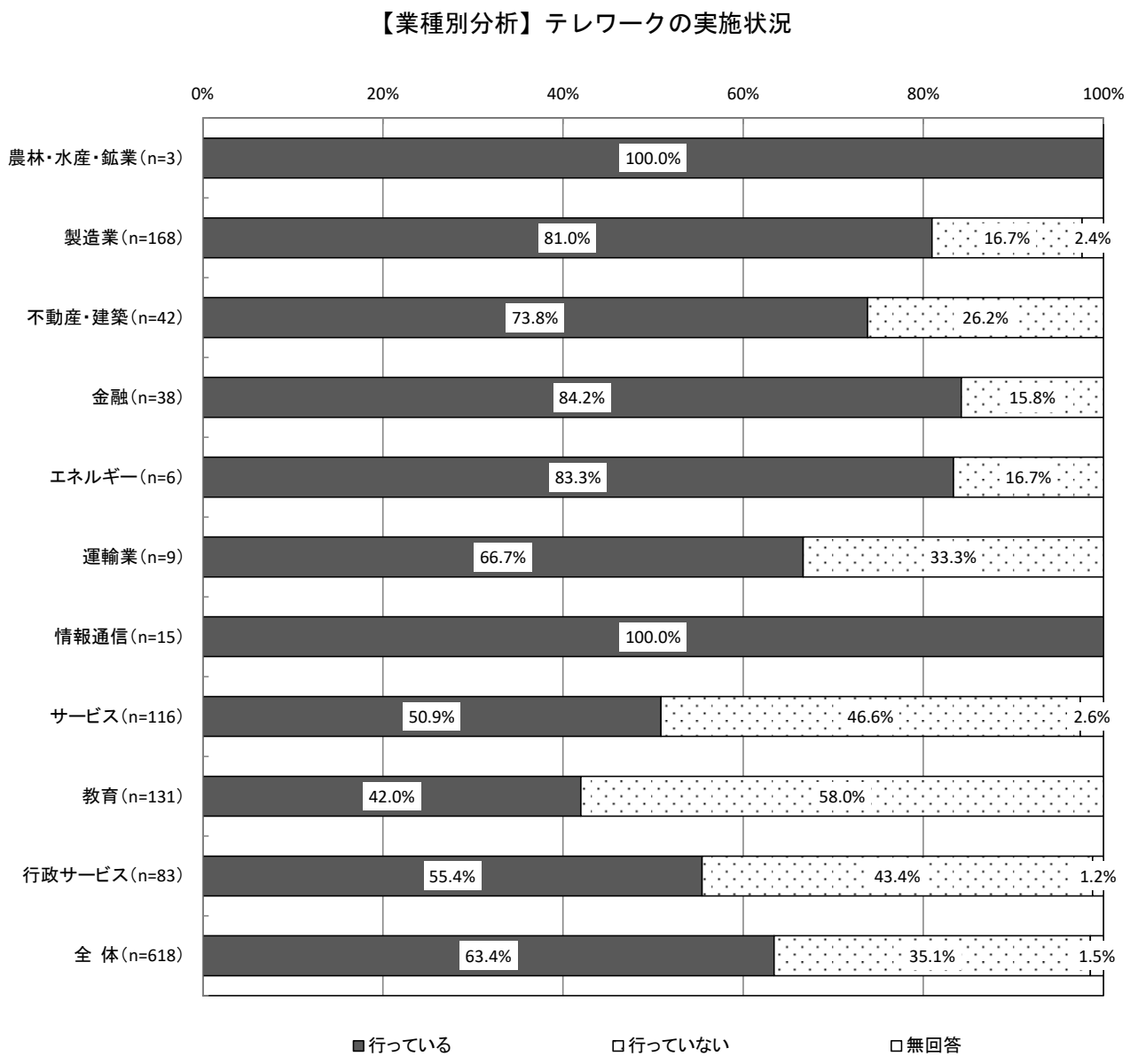
3.1.4　テレワークの実施状況　【問6】

テレワークの実施状況については、「行っている」が63.4%と高くなっている。これに対して、「行っていない」は、35.1%となっている。

【全体】テレワークの実施状況（SA,n=618）

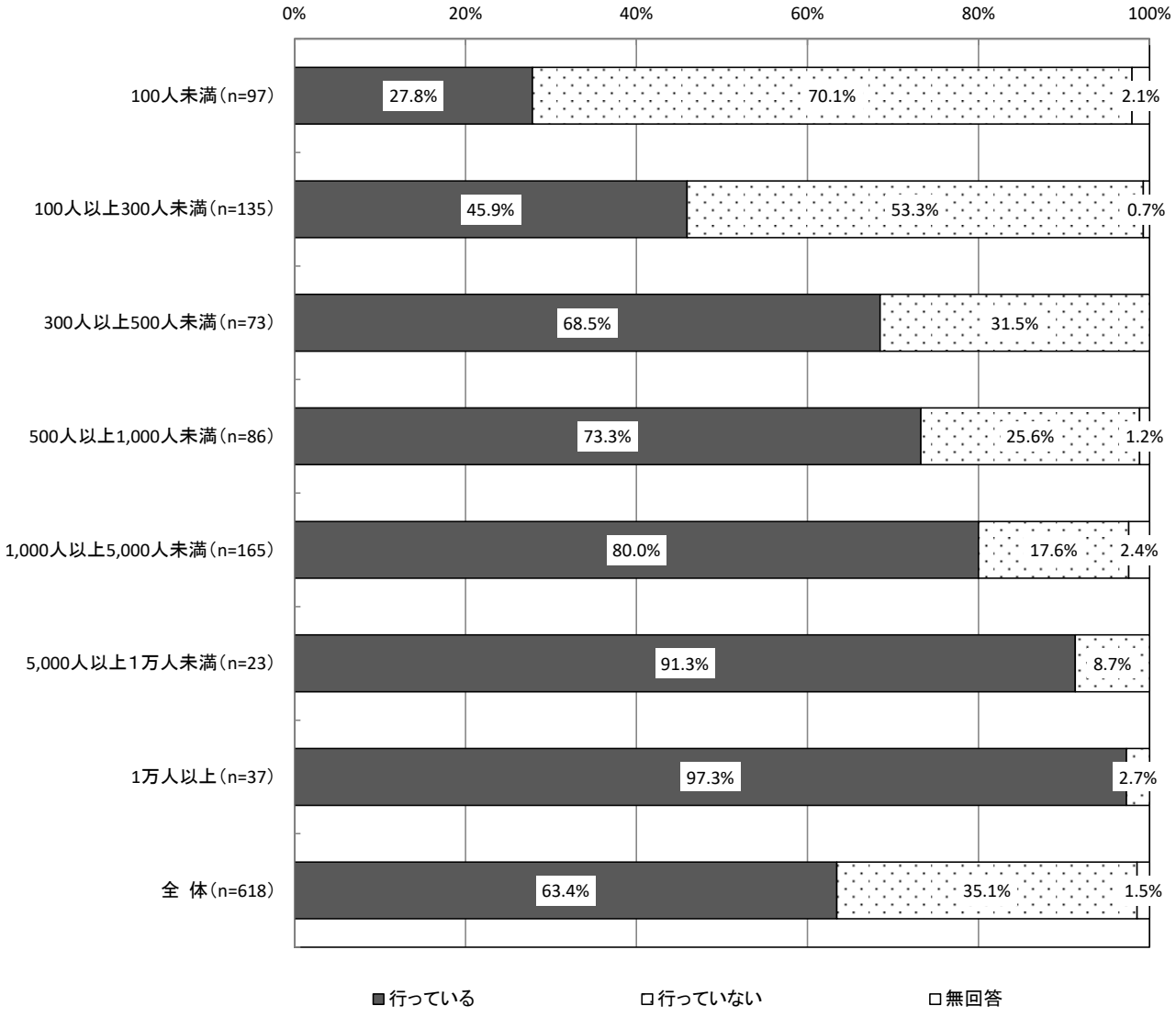


【業種別分析】業種別にみると、「行っている」は、「情報通信」が100.0%で高く、次いで「金融」が84.2%、「エネルギー」が83.3%となっている。一方、最も低いのは「教育」で42.0%となっている。



【従業員規模別分析】従業員規模別にみると、「行っている」では、「1万人以上」が97.3%、「5,000人以上１万人未満」が91.3%で9割を超えて高くなっている。「行っている」割合は従業員数規模が大きいほど高くなっており、従業員規模が「100人未満」で27.8%と最も低くなっている。

【従業員規模別分析】テレワークの実施状況

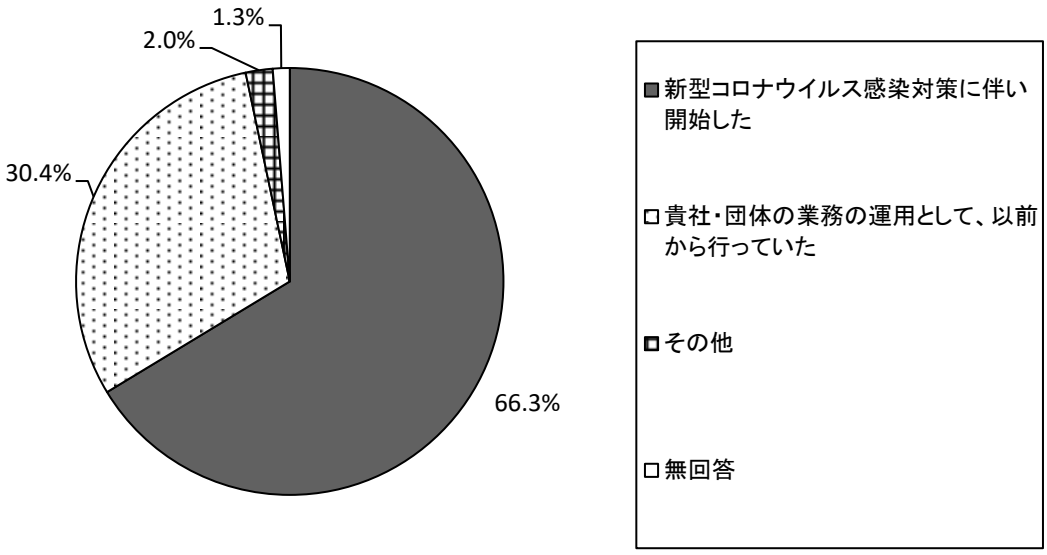


3.1.5　テレワークの開始時期　【問6-1】

テレワークの開始時期については、「新型コロナウイルス感染対策に伴い開始した」が66.3%、「貴社・団体の業務の運用として、以前から行っていた」が30.4%となっている。

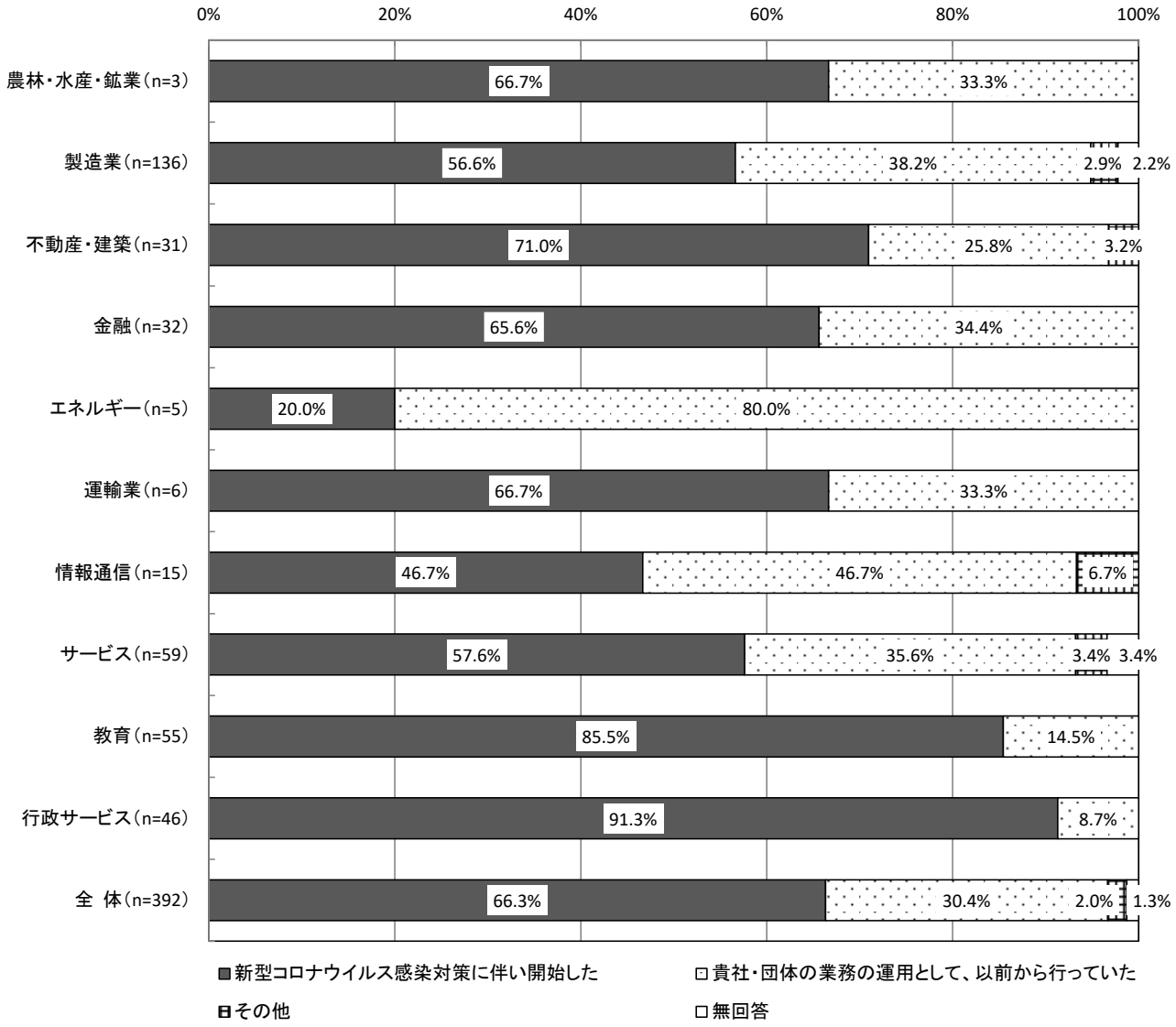
※本項目は、テレワークを実施している社・団体等を対象としている。

【全体】テレワークの開始時期（SA,n=392）



【業種別分析】業種別にみると、「新型コロナウイルス感染対策に伴い開始した」では、「行政サービス」が91.3%、「教育」が85.5%と高くなっている。一方、最も低いのは「エネルギー」で、20.0%となっている。

【業種別分析】テレワークの開始時期

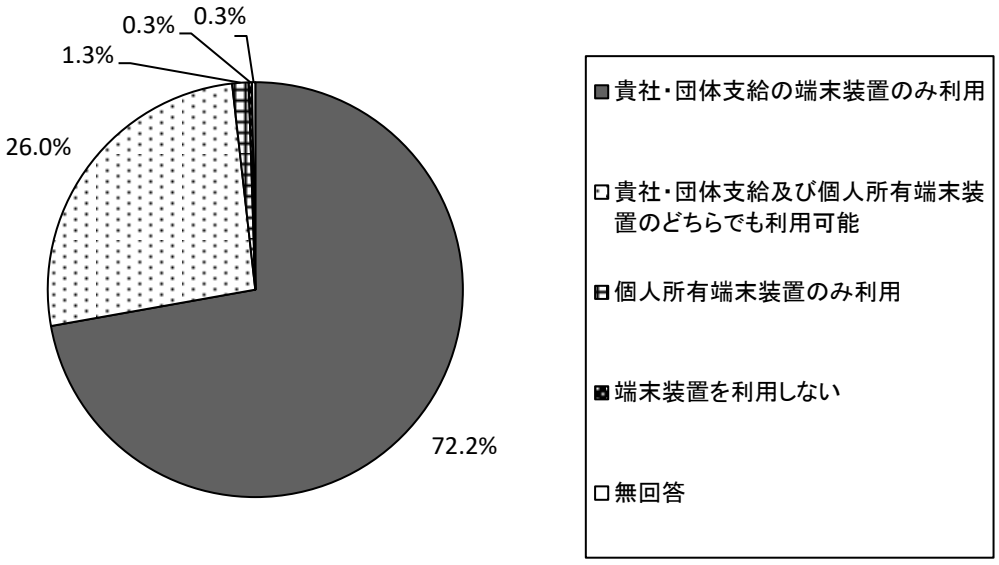


3.1.6　テレワーク業務の端末装置（パソコン、スマートフォン等）の利用環境　【問6-2】

テレワーク業務の端末装置（パソコン、スマートフォン等）の利用環境については、「貴社・団体支給の端末装置のみ利用」が72.2%で最も高く、「貴社・団体支給及び個人所有端末装置のどちらでも利用可能」が26.0%、「個人所有端末装置のみ利用」が1.3%となっている。

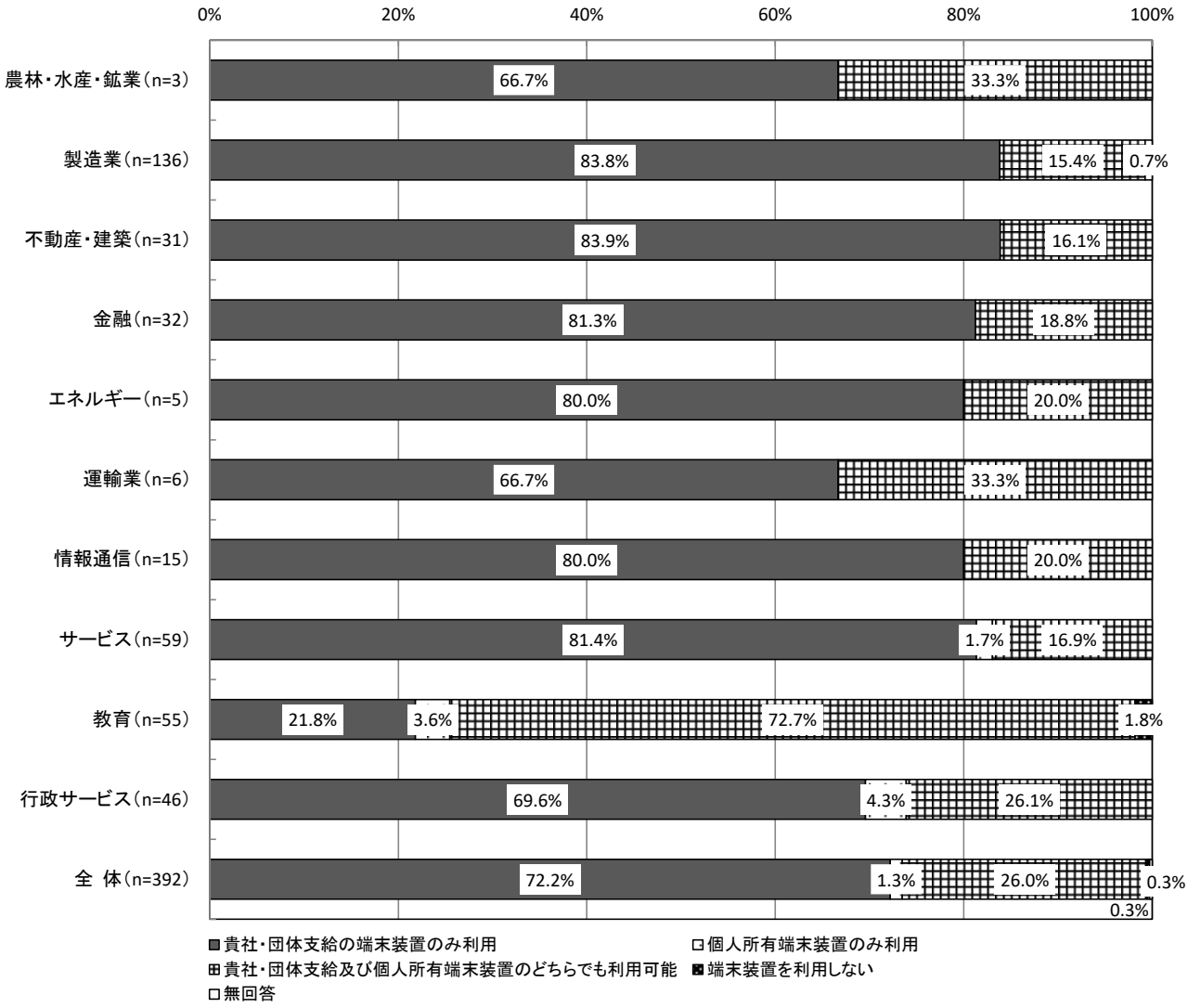
※本項目は、テレワークを実施している社・団体等を対象としている。

【全体】テレワーク業務の端末装置（パソコン、スマートフォン等）の利用環境（SA,n=392）



【業種別分析】業種別にみると、「貴社・団体支給の端末装置のみ利用」では、「不動産・建築」が83.9%、「製造業」が83.8%で高い。一方で、「教育」は21.8%で最も低くなっている。

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

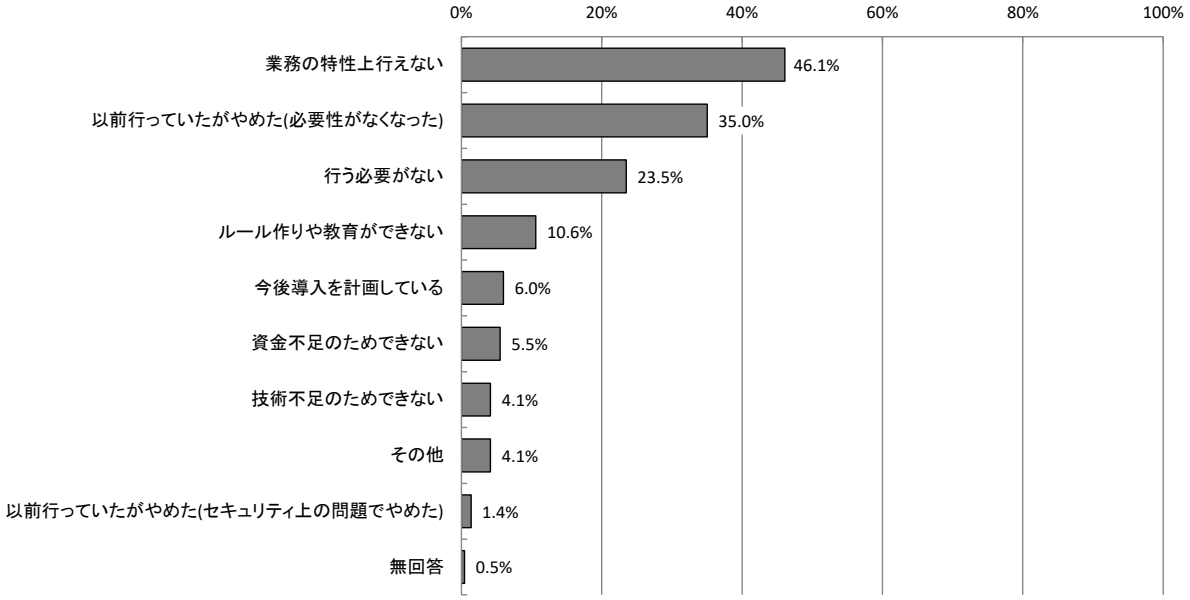


3.1.7　テレワークを行っていない理由　【問6-3】

テレワークを行っていない理由については、「業務の特性上行えない」が46.1%で最も高くなっている。次いで「以前行っていたがやめた(必要性がなくなった)」が35.0%、「行う必要がない」が23.5%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。

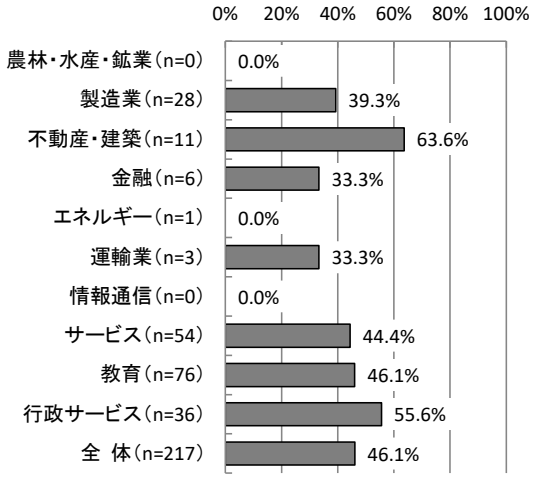
【全体】テレワークを行っていない理由（MA, n=217）



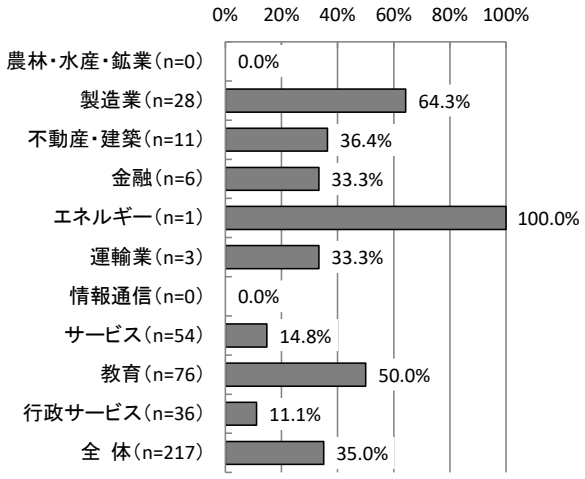
【業種別分析】業種別にみると、「業務の特性上行えない」では、「不動産・建築」が63.6%で最も高く、次いで「行政サービス」も55.6%と高くなっている。一方、「金融」では33.3%、「製造業」では39.3%で4割未満と低くなっている。

【業種別分析】テレワークを行っていない理由

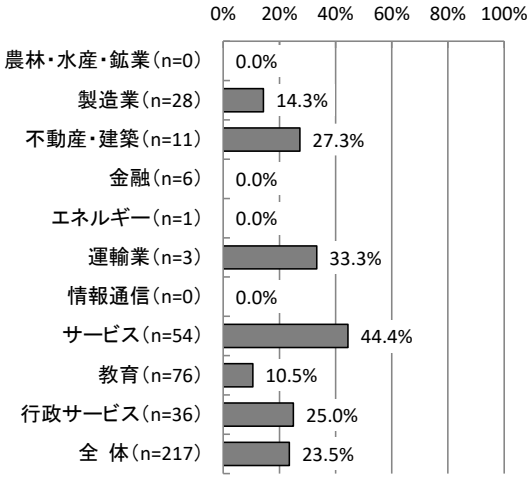
業務の特性上行えない



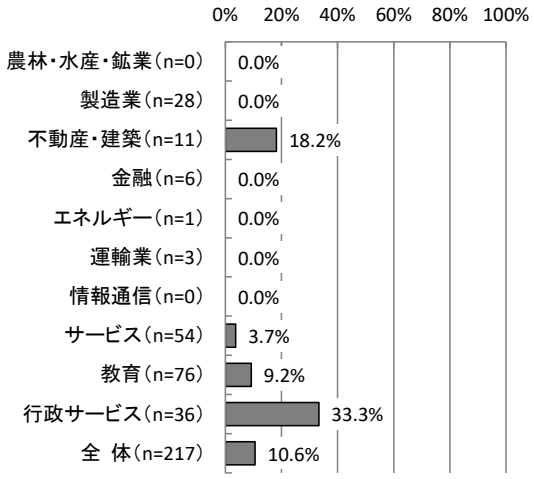
以前行っていたがやめた(必要性がなくなった)



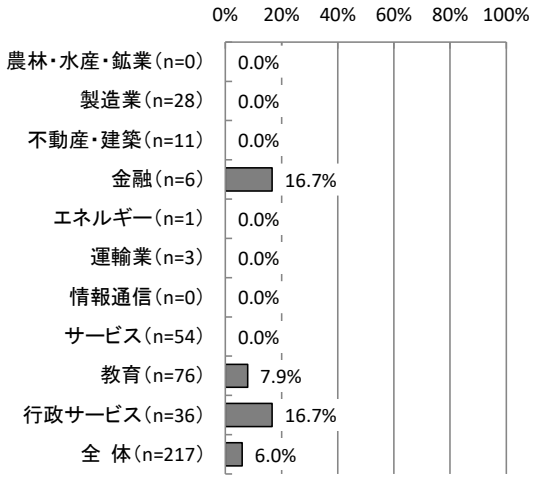
行う必要がない



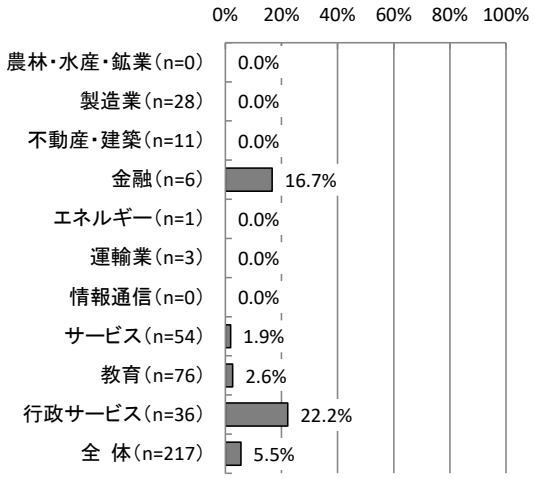
ルール作りや教育ができない



今後導入を計画している



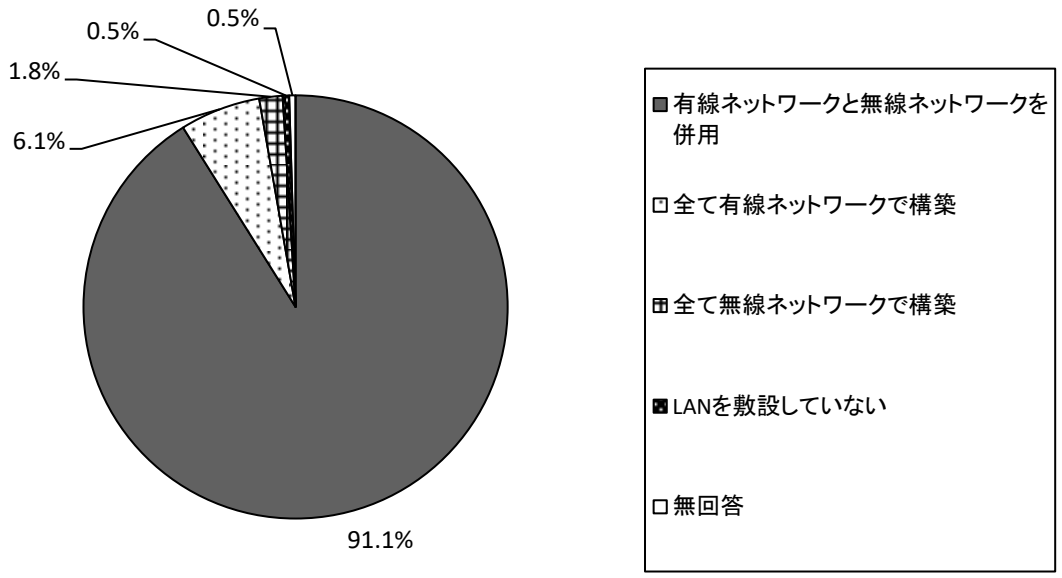
資金不足のためできない



3.1.8　事業体内のネットワーク利用状況　【問7】

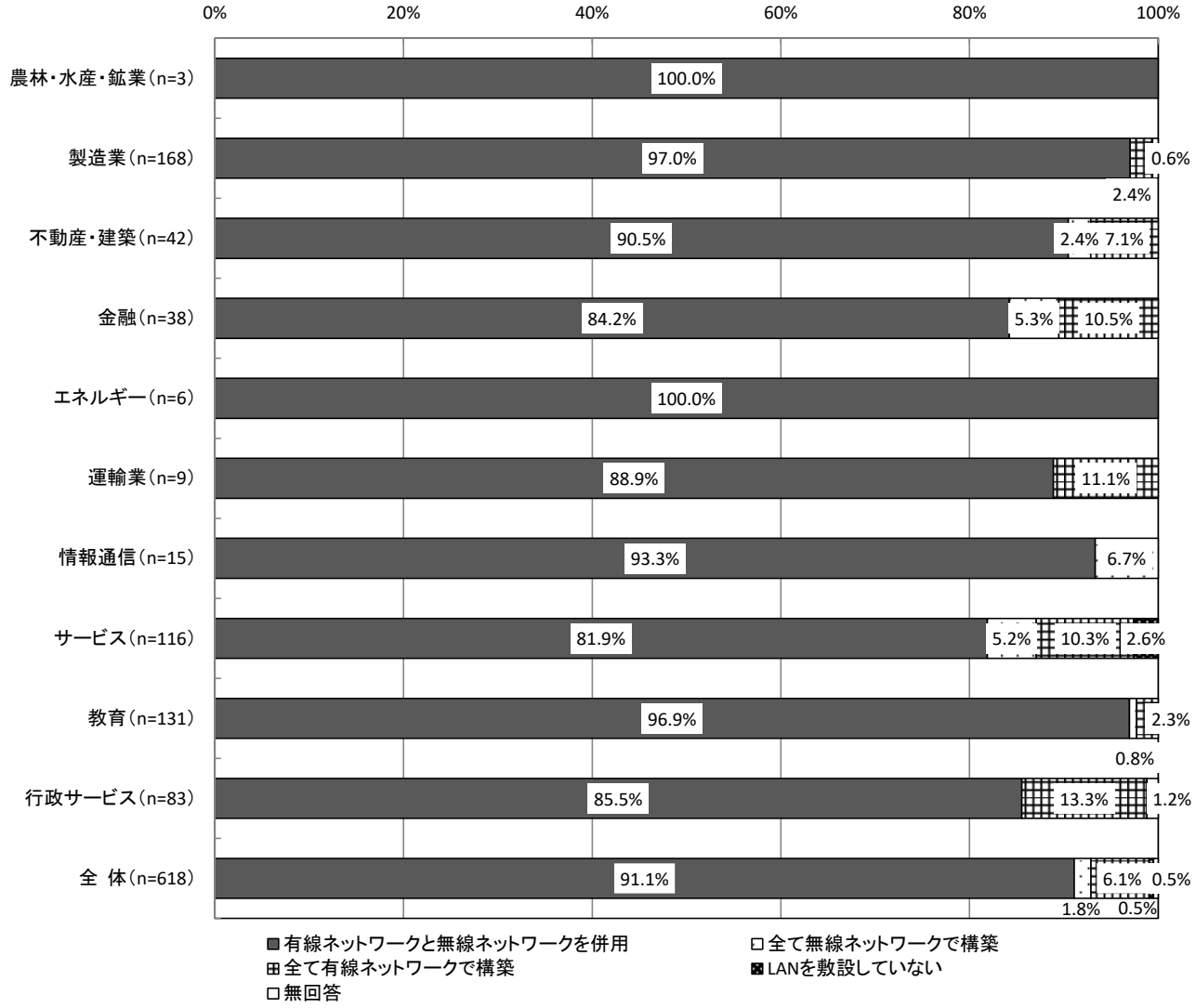
事業体内のネットワーク利用状況については、「有線ネットワークと無線ネットワークを併用」が91.1%で最も高く、次いで「全て有線ネットワークで構築」が6.1%となっている。

【全体】事業体内のネットワーク利用状況（SA,n=618）



【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」で100.0%、「製造業」で97.0%、「教育」で96.9%と高くなっている。「全て有線ネットワークで構築」は「行政サービス」が13.3%で高くなっている。

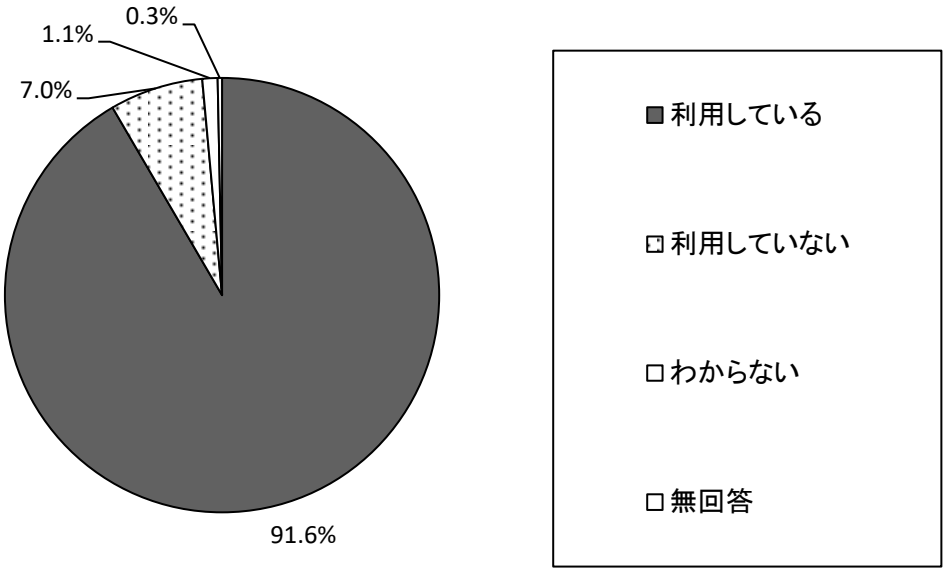
【業種別分析】事業体内のネットワーク利用状況



3.1.9　クラウドサービスの利用状況　【問8】

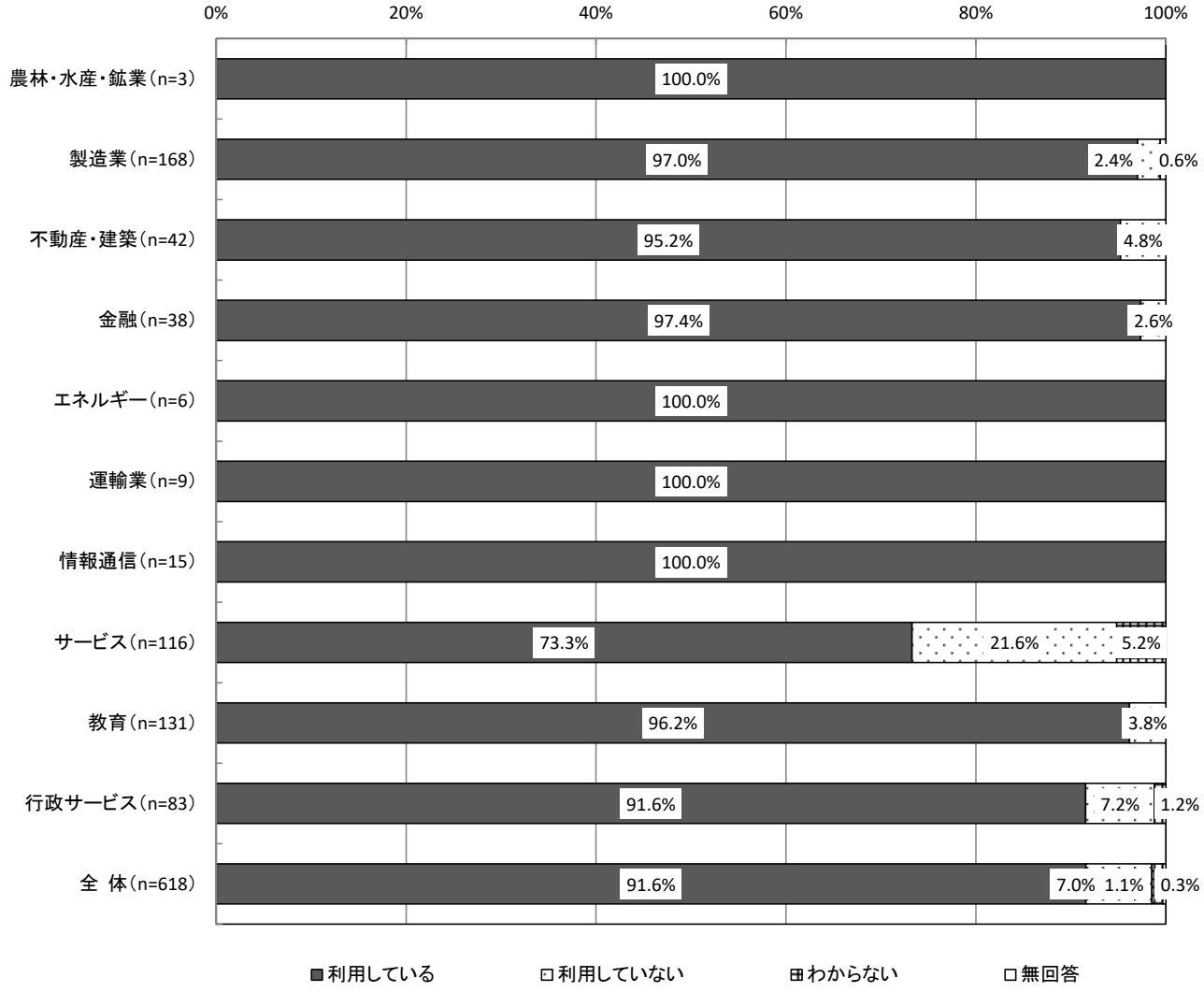
クラウドサービスの利用状況については、「利用している」が91.6%で最も高く、「利用していない」が7.0%、「わからない」が1.1%となっている。

【全体】クラウドサービスの利用状況（SA,n=618）



【業種別分析】業種別にみると、「使用している」については、「エネルギー」「運輸業」「情報通信」で100.0％と高く、次いで「金融」で97.4％、「製造業」で97.0％と高くなっている。一方で「サービス」では73.3％と低くなっている。

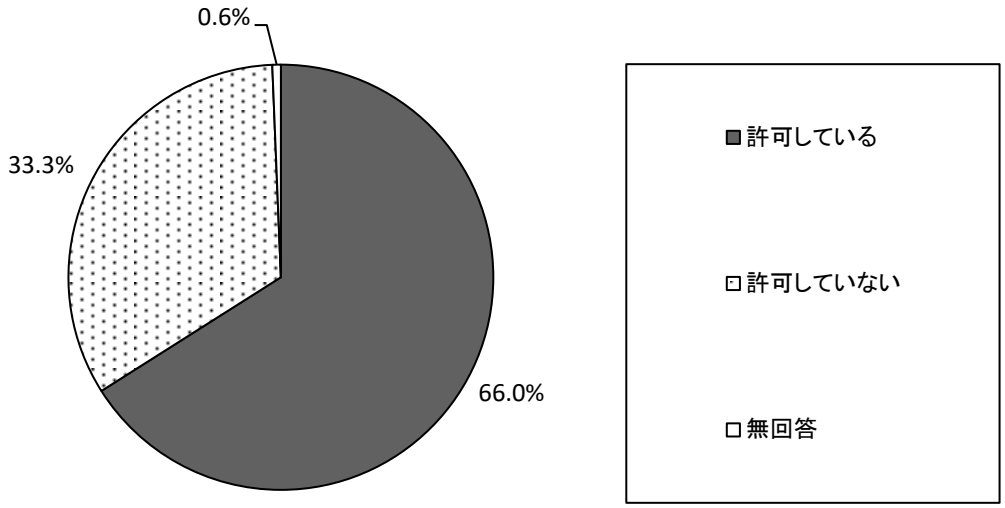
【業種別分析】クラウドサービスの利用状況



3.1.10　外部からの接続許可状況　【問9】

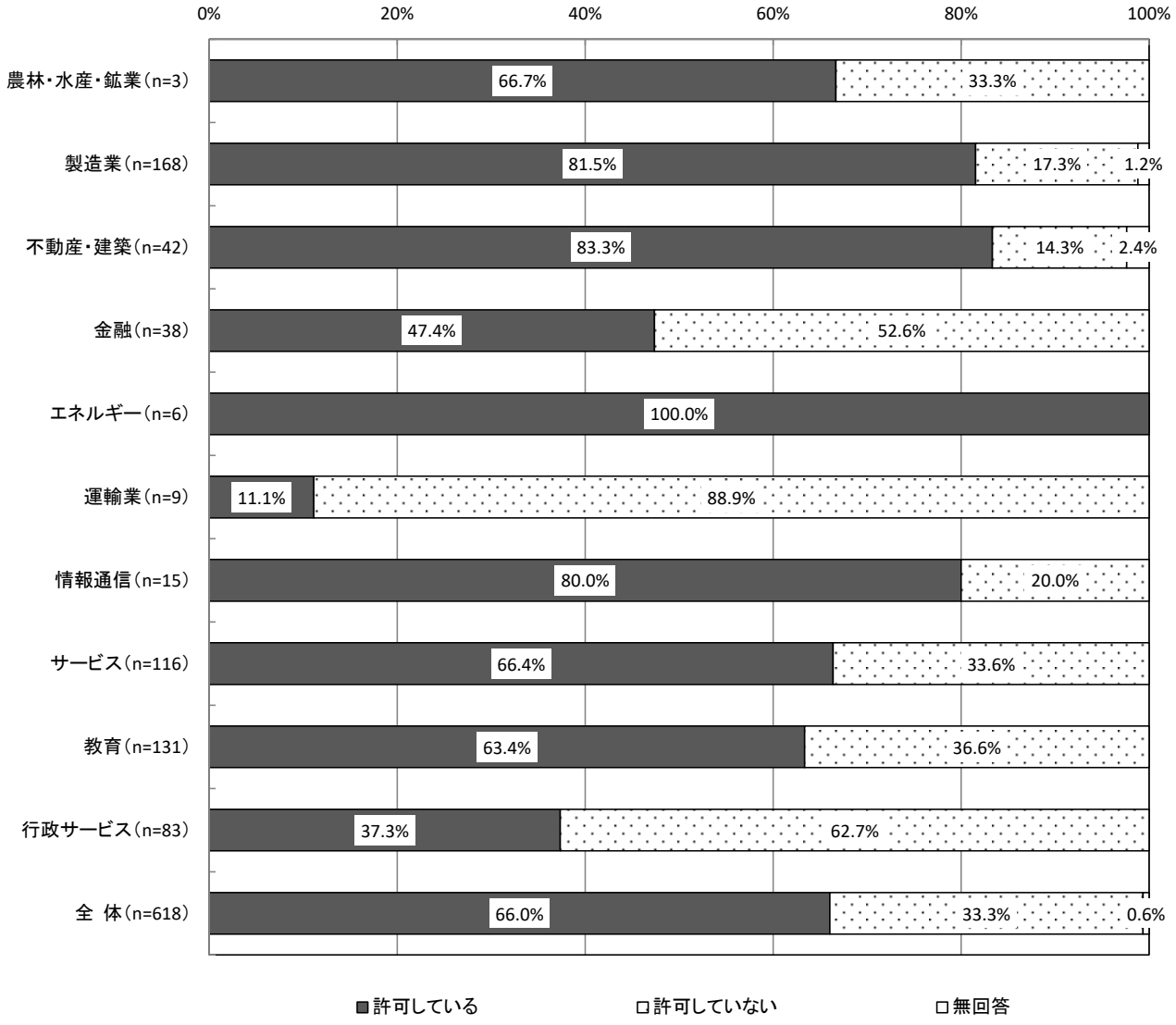
外部から事業体内ネットワークへの接続許可状況については、「許可している」が66.0%で高く、「許可していない」は33.3%となっている。

【全体】外部からの接続許可状況（SA,n=618）



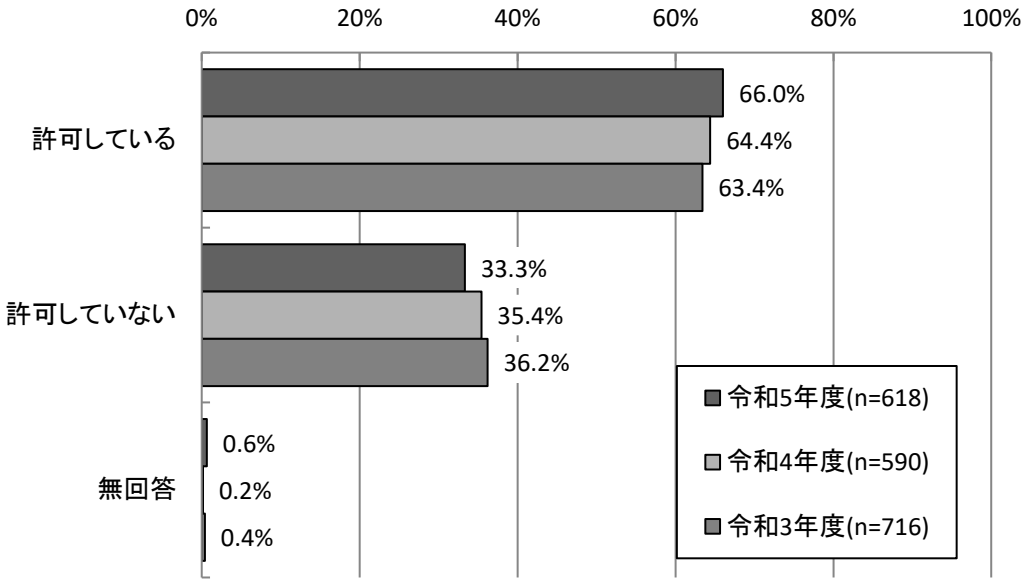
【業種別分析】業種別にみると、「許可している」では、「エネルギー」が100.0%、「不動産・建築」が83.3%、「製造業」が81.5%、「情報通信」が80.0%で高くなっている。一方「許可していない」は「運輸業」が88.9%で最も高く、次いで「行政サービス」が62.7%となっている。

【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、「許可していない」が2.1ポイントの減少、「許可している」が1.6ポイントの増加となっており、大きな変化はみられない。

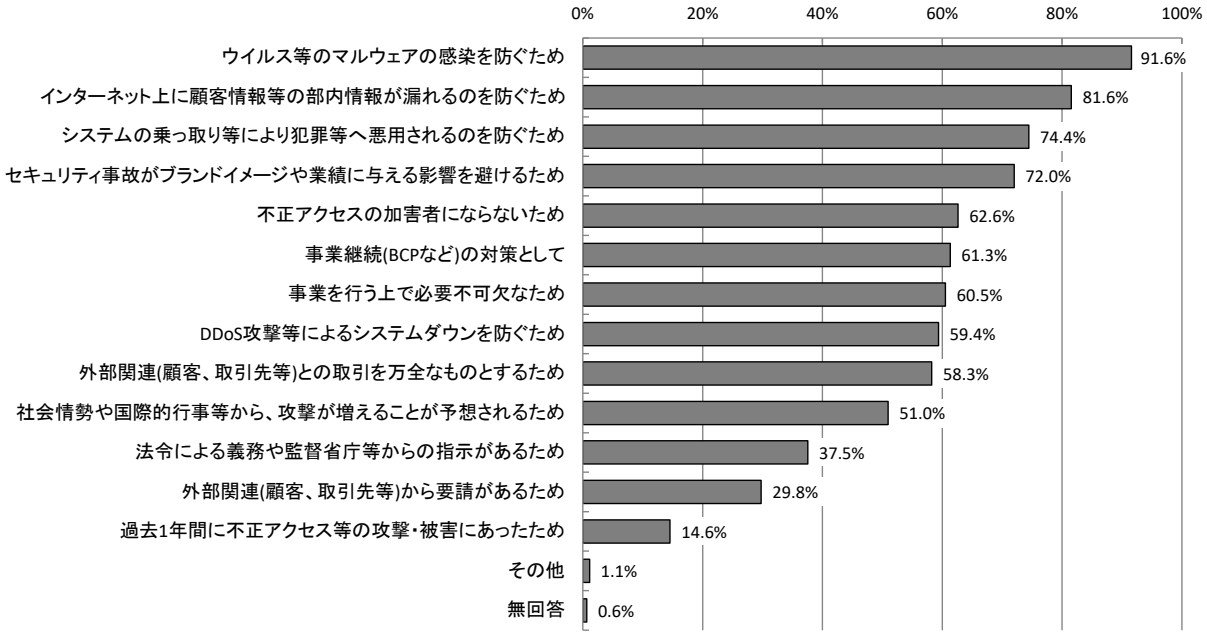
【経年変化】外部からの接続許可状況



3.1.11　情報セキュリティ対策の必要性の理由【問10】

情報セキュリティ対策の必要性の理由については、「ウイルス等のマルウェアの感染を防ぐため」が91.6%で最も高く、次いで「インターネット上に顧客情報等の部内情報が漏れるのを防ぐため」が81.6%、「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74.4%、「セキュリティ事故がブランドイメージや業績に与える影響を避けるため」が72.0%となっている。

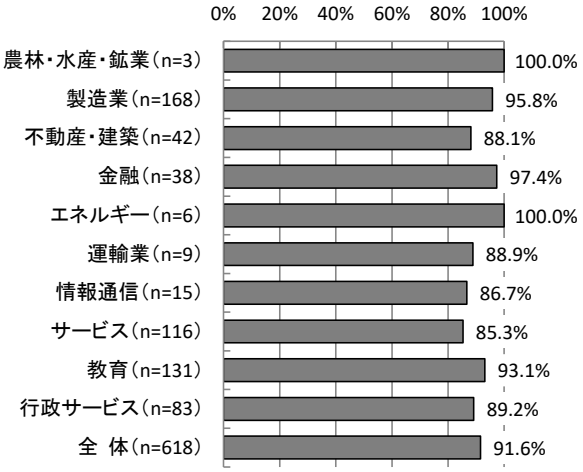
【全体】情報セキュリティ対策の必要性の理由（MA,n=618）



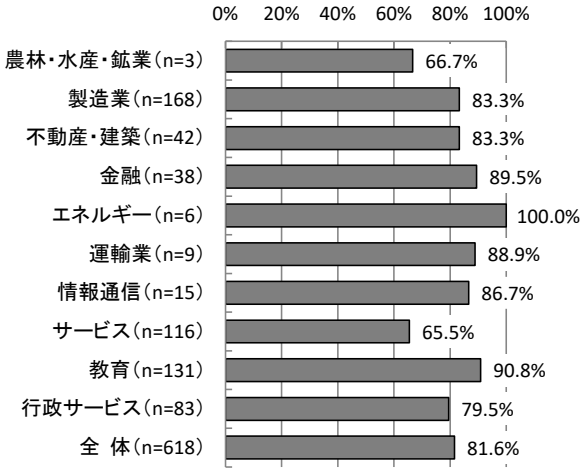
【業種別分析】業種別にみると、「ウイルス等のマルウェアの感染を防ぐため」では「エネルギー」が100.0%、「製造業」が95.8%と高い。「インターネット上に顧客情報等の部内情報が漏れるのを防ぐため」では「エネルギー」が100.0%、「教育」が90.8%で高い。一方で、「サービス」は65.5%と他の業種と比較して低くなっている。

【業種別分析】情報セキュリティ対策の必要性の理由

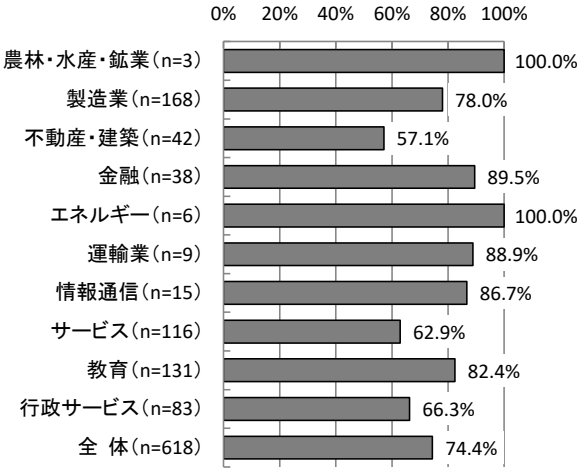
ウイルス等のマルウェアの感染を防ぐため



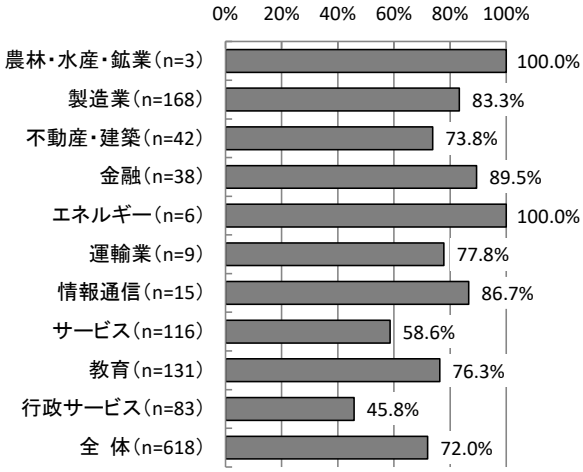
インターネット上に顧客情報等の部内情報が漏れるのを防ぐため



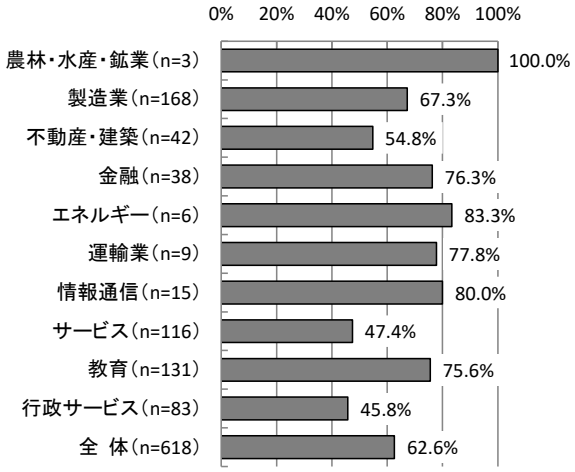
システムの乗っ取り等により犯罪等へ悪用されるのを防ぐため



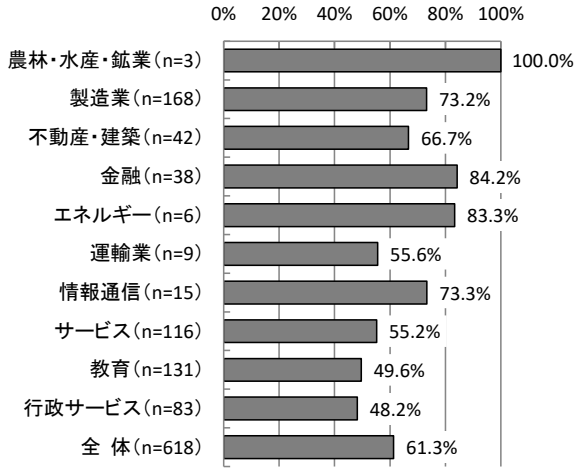
セキュリティ事故がブランドイメージや業績に与える影響を避けるため



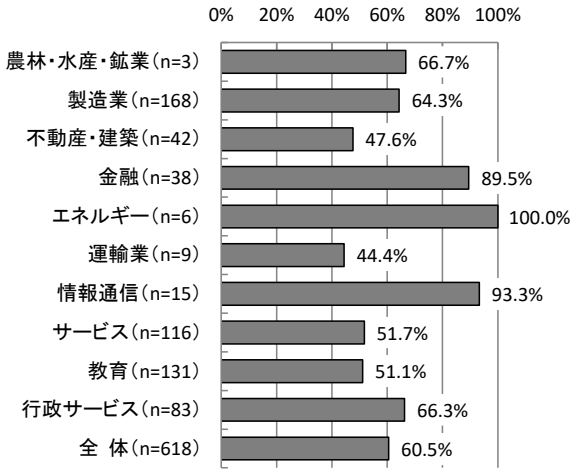
不正アクセスの加害者にならないため



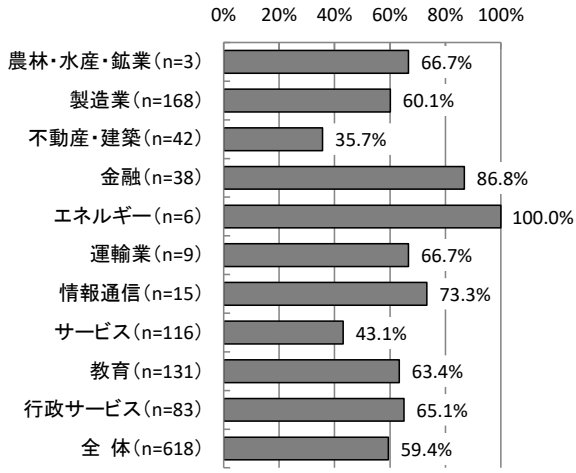
事業継続(BCPなど)の対策として



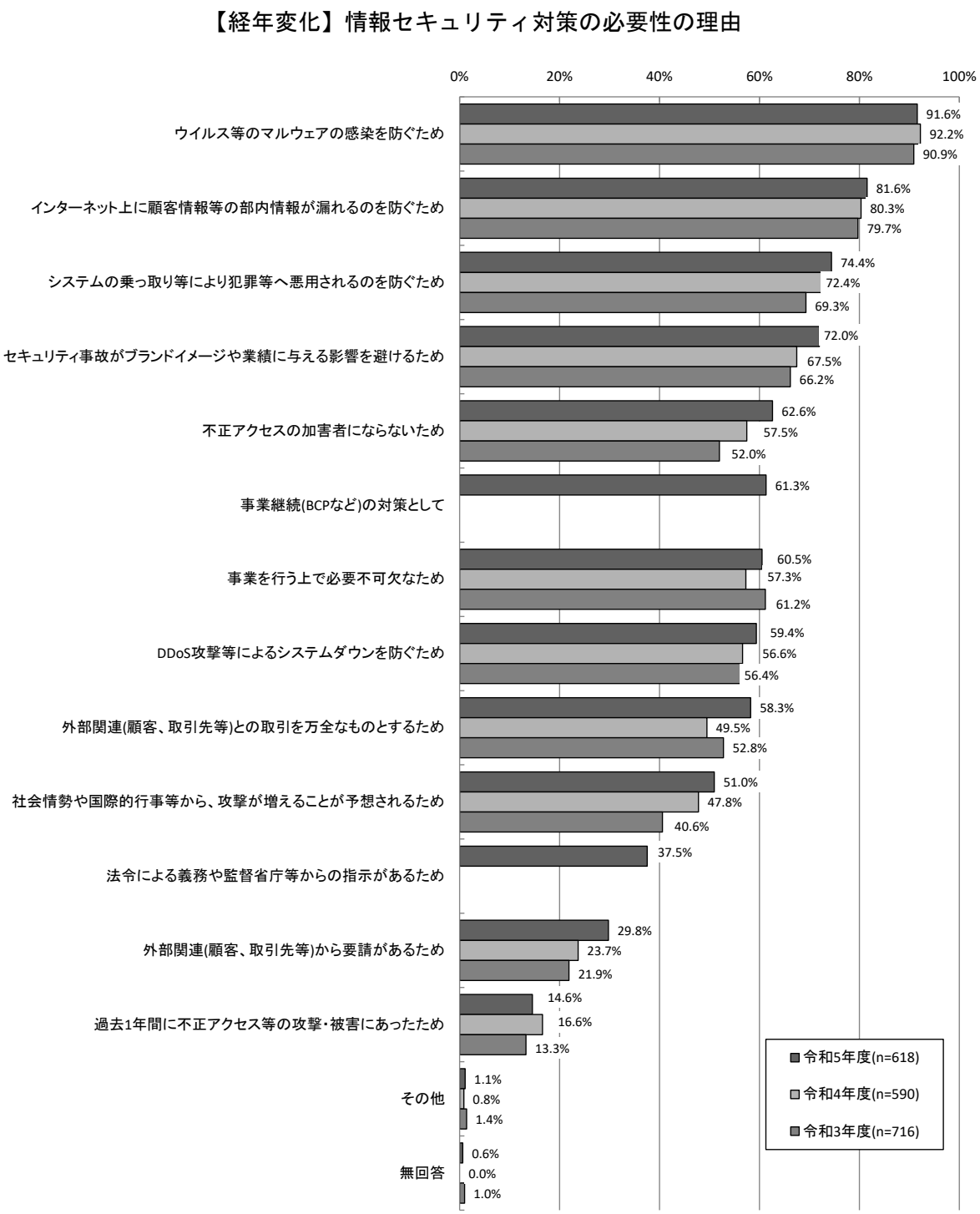
事業を行う上で必要不可欠なため



DDoS攻撃等によるシステムダウンを防ぐため



【経年変化】昨年度と比較すると、「外部関連(顧客、取引先等)との取引を万全なものとするため」が8.8ポイント、「外部関連(顧客、取引先等)から要請があるため」が6.1ポイント増加している。



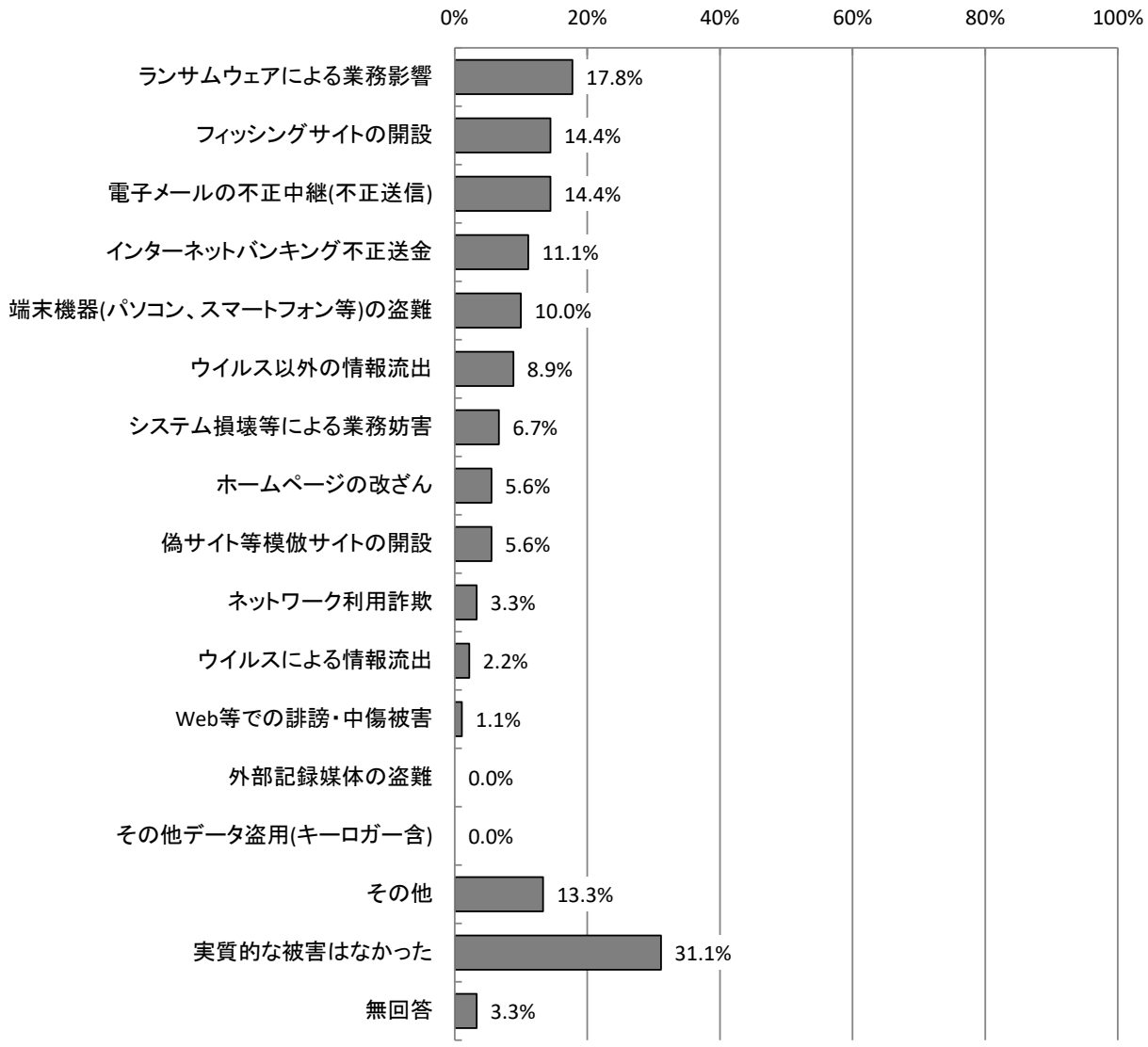
※令和５年度調査で「事業継続(BCPなど)の対策として」「法令による義務や監督省庁等からの指示があるため」を新設

3.1.12　過去に受けたことのある被害状況　【問10-1-1】

過去に受けたことのある被害状況については、「ランサムウェアによる業務影響」が17.8%で最も高く、次いで「フィッシングサイトの開設」「電子メールの不正中継(不正送信)」が14.4%となっている。また、「実質的な被害はなかった」が31.1%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。

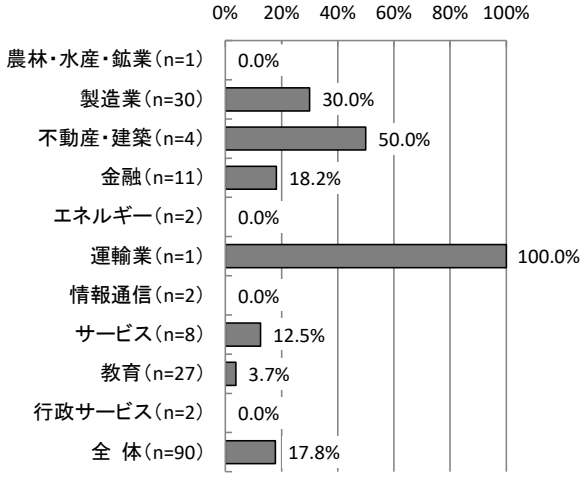
【全体】過去に受けたことのある被害状況（MA,n=90）



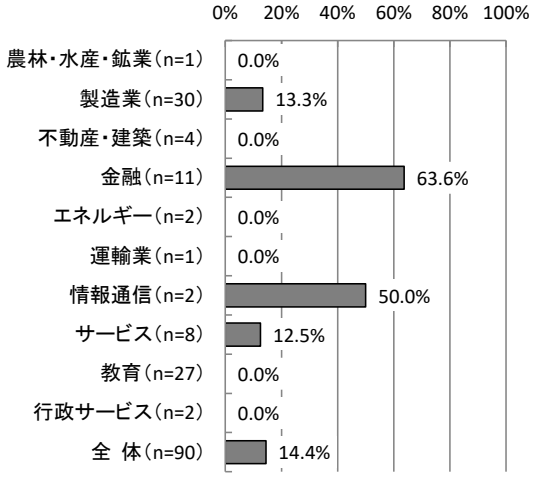
【業種別分析】業種別にみると、「ランサムウェアによる業務影響」については、「製造業」が30.0%で高い。「フィッシングサイトの開設」については、「金融」が63.6%で高くなっている。また、「電子メールの不正中継(不正送信)」については、「教育」が33.3%で高くなっている。

【業種別分析】過去に受けたことのある被害状況

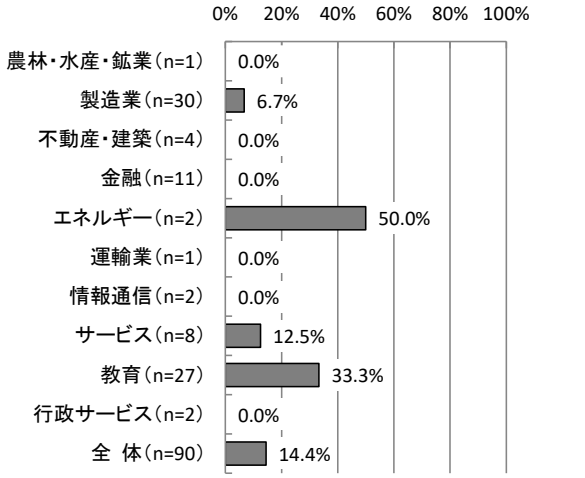
ランサムウェアによる業務影響



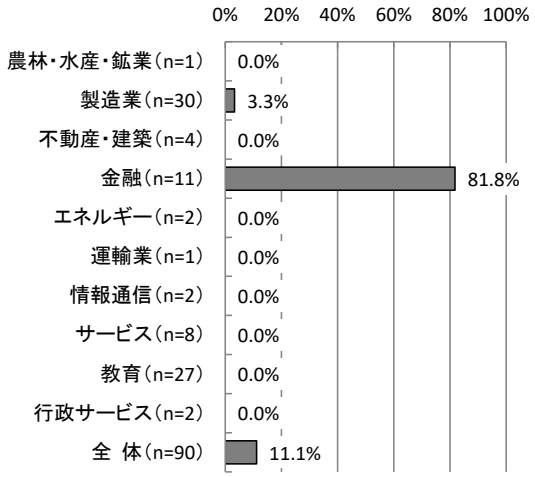
フィッシングサイトの開設



電子メールの不正中継(不正送信)



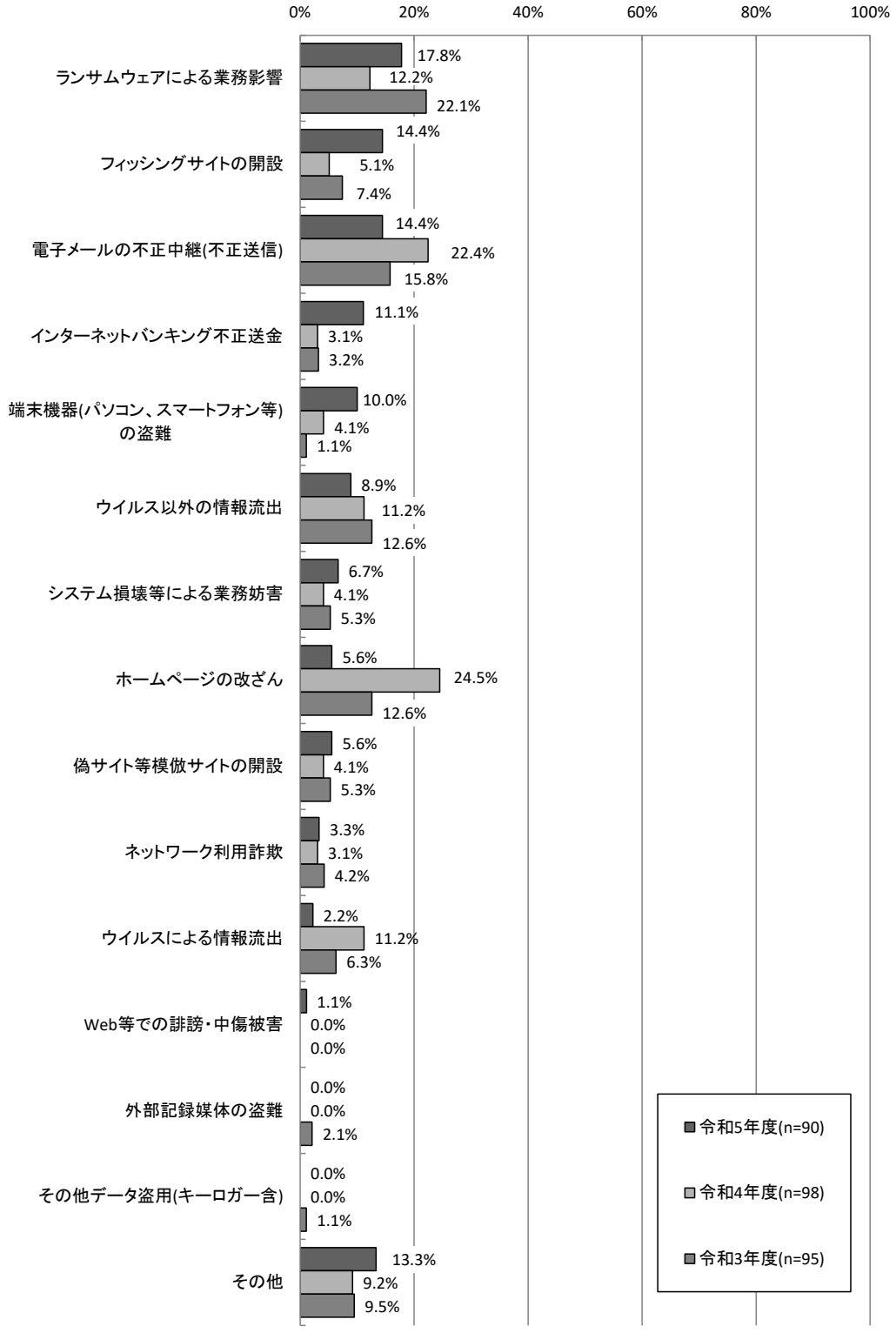
インターネットバンキング不正送金



【経年変化】昨年度と比較すると、「ホームページの改ざん」が18.9ポイント、「ウイルスによる情報流出」が9.0ポイント減少している。一方、「フィッシングサイトの開設」が9.3ポイントの増加となっている。

※「無回答」を除いた総数で比較している。

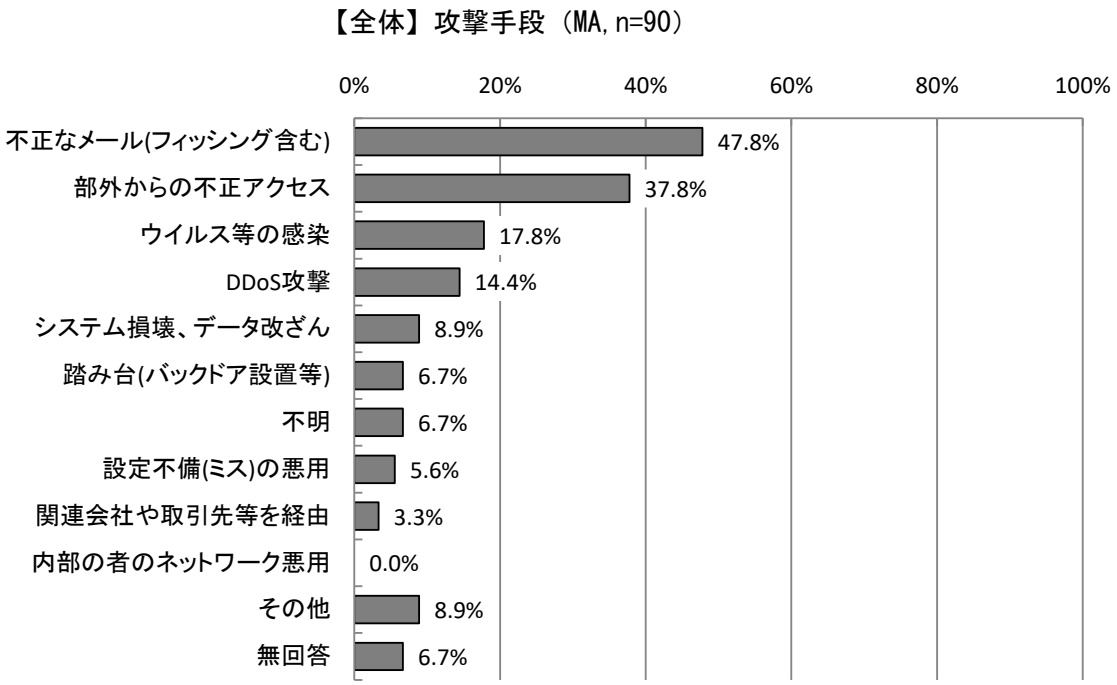
【経年変化】過去に受けたことのある被害状況



3.1.13　攻撃手段　【問10-1-2】

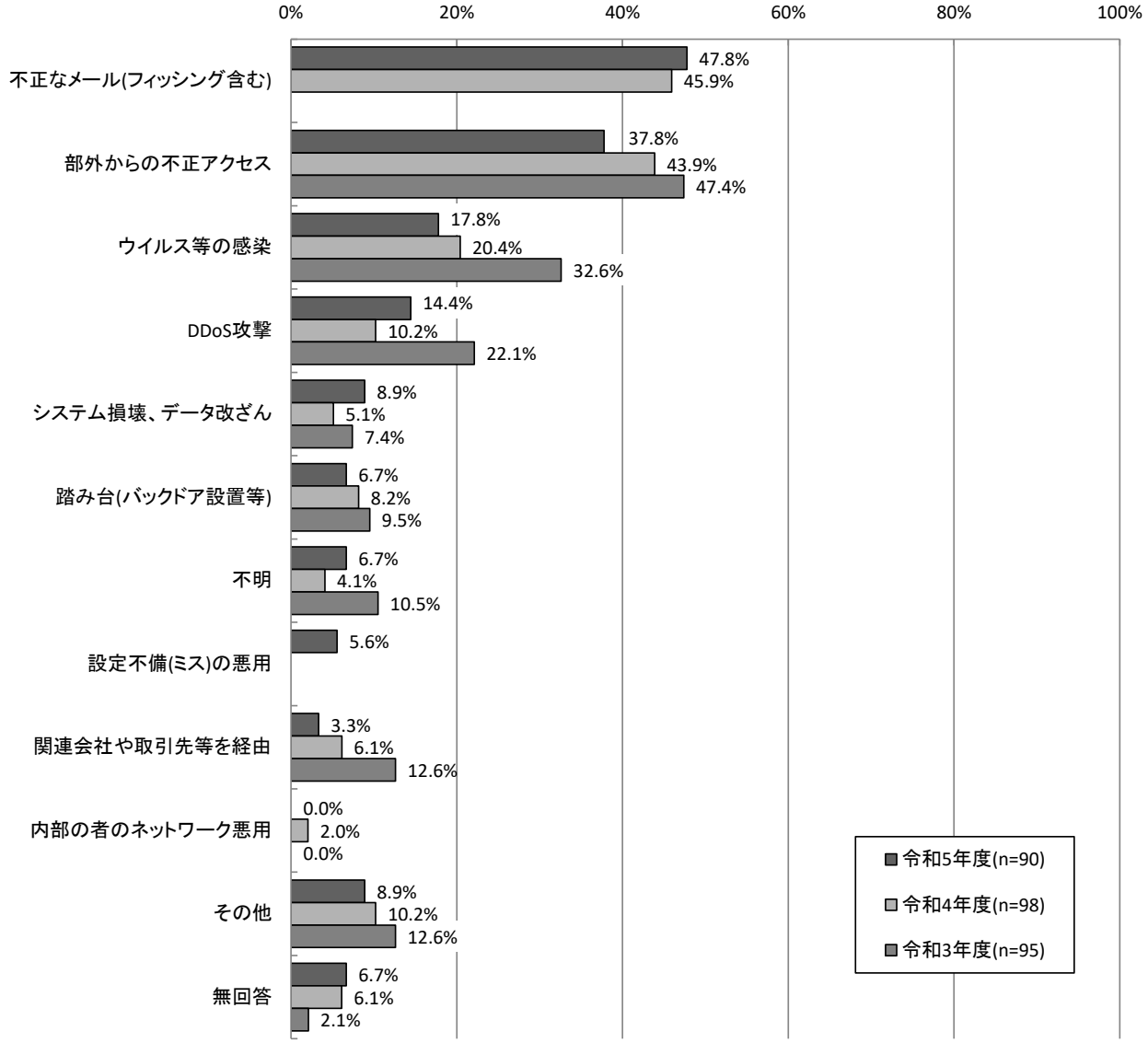
攻撃手段については、「不正なメール(フィッシング含む)」が47.8%で最も高く、次いで「部外からの不正アクセス」が37.8%となっている。

※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。



【経年変化】昨年度と比較すると、「設定不備(ミス)の悪用」が5.6ポイント、「DDoS攻撃」が4.2ポイント増加している。一方で、「部外からの不正アクセス」が6.1ポイント減少している。

【経年変化】攻撃手段



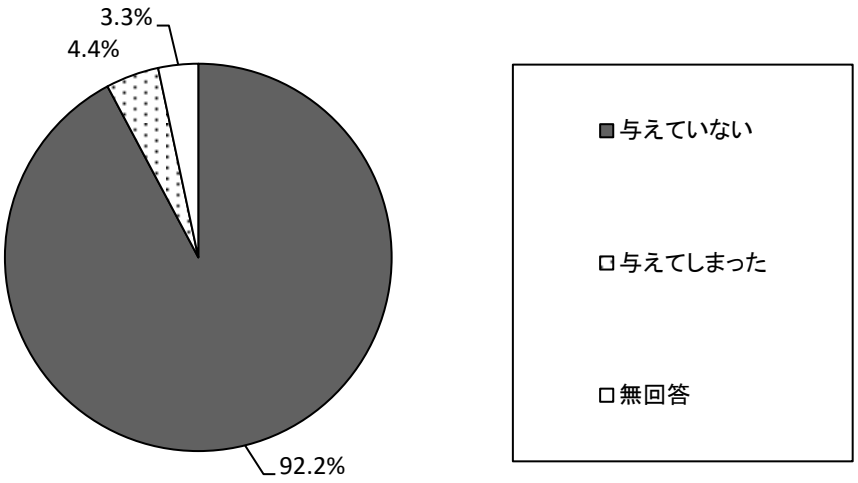
※令和４年度調査で「不正なメール（フィッシング含む）」を新設
※令和５年度調査で「設定不備(ミス)の悪用」を新設

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

不正アクセス等の被害によって被害を与えてしまったことがあるかについて、「与えていない」が92.2%で高くなっている。一方で「与えてしまった」は4.4%と低くなっている。

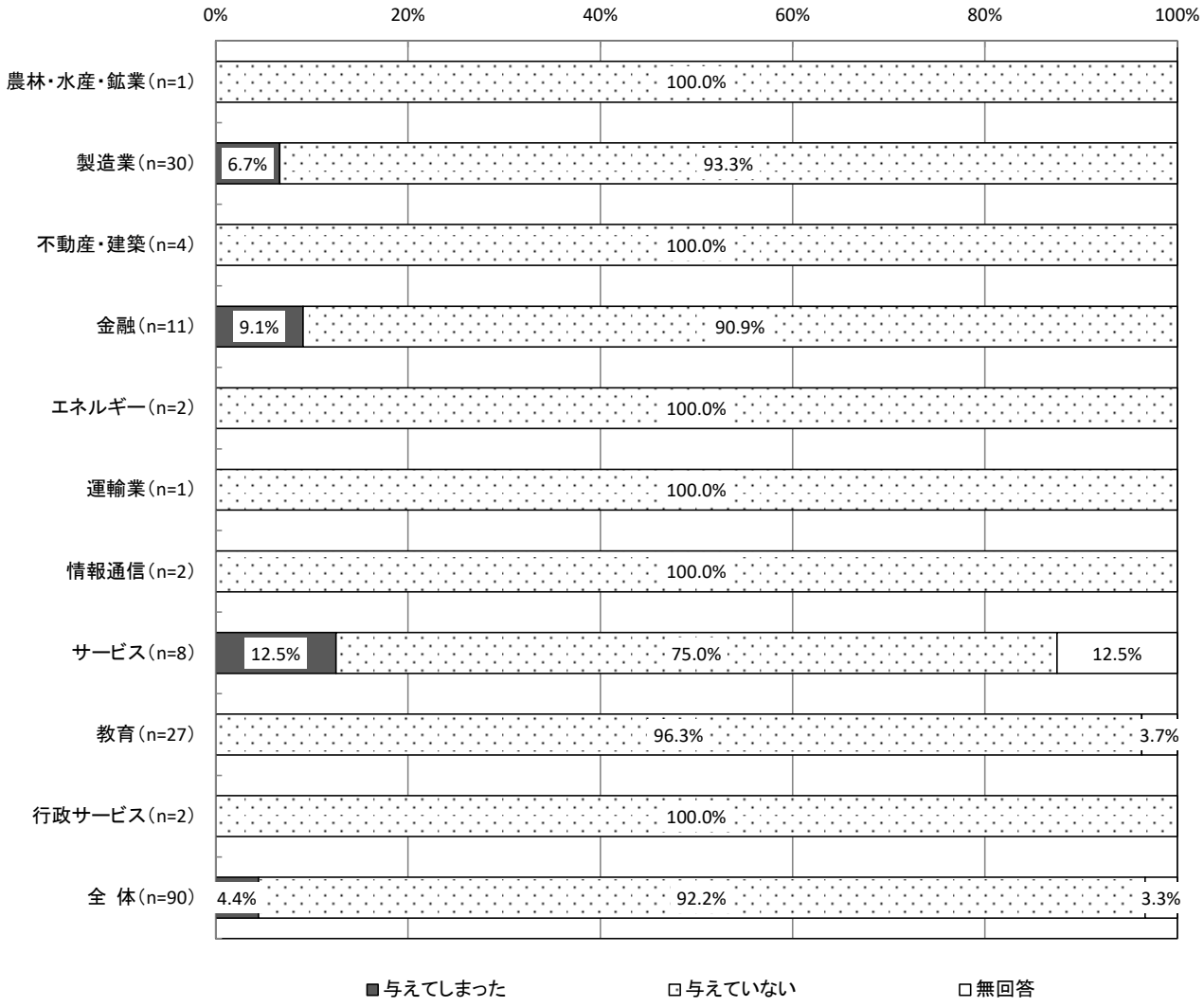
※本項目は、過去に不正アクセス等の被害にあった社・団体等を対象としている。

【全体】関連会社や取引先等に被害を与えてしまったことがあるか（MA,n=90）



【業種別分析】業種別にみると、「与えてしまった」が「サービス」で12.5%、「金融」で9.1%、「製造業」で6.7%となっている。

【業種別分析】関連会社や取引先等に被害を与えてしまったことがあるか

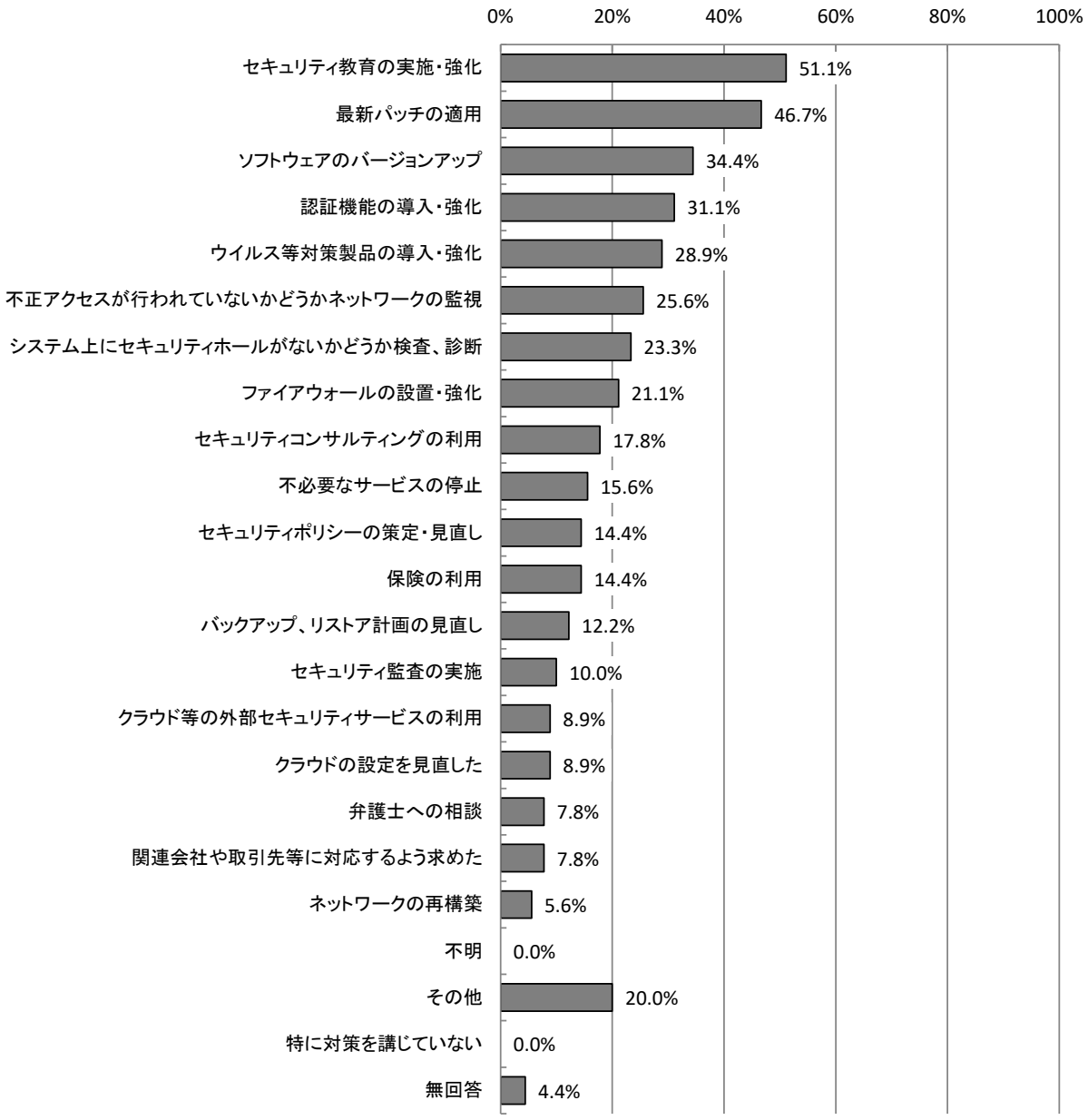


3.1.15　被害を受けたことによる対策　【問10-3】

被害を受けたことによる対策については、「セキュリティ教育の実施・強化」が51.1%、「最新パッチの適用」が46.7%、「ソフトウェアのバージョンアップ」が34.4%、「認証機能の導入・強化」が31.1%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。

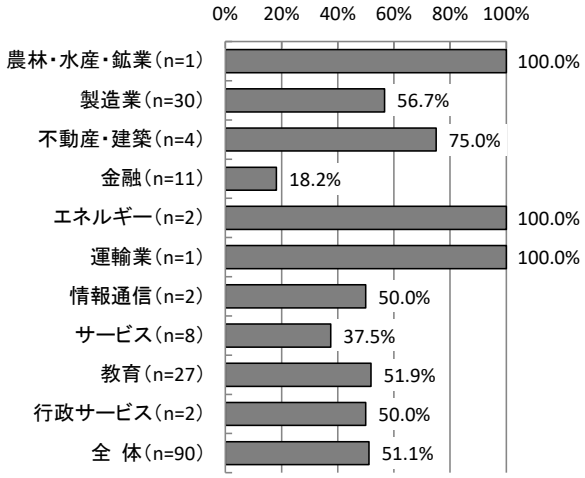
【全体】被害を受けたことによる対策（MA, n=90）



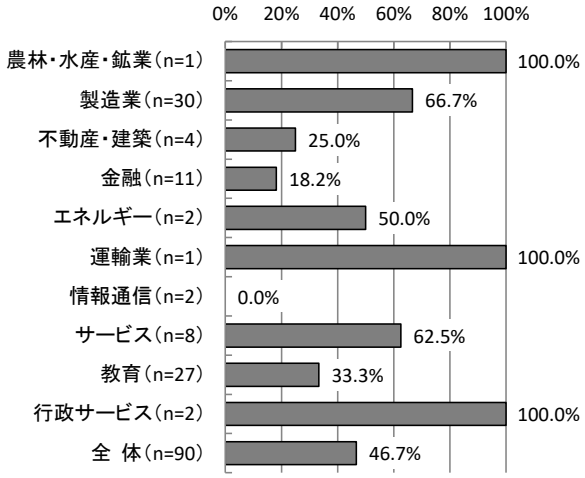
【業種別分析】業種別にみると、「セキュリティ教育の実施・強化」では「製造業」の56.7%と「教育」の51.9%が高く、「最新パッチの適用」については、「製造業」の66.7%と「サービス」の62.5%が高くなっている。

【業種別分析】被害を受けたことによる対策

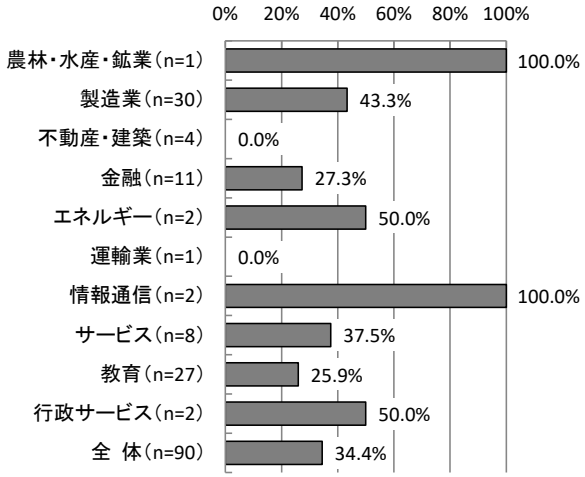
セキュリティ教育の実施・強化



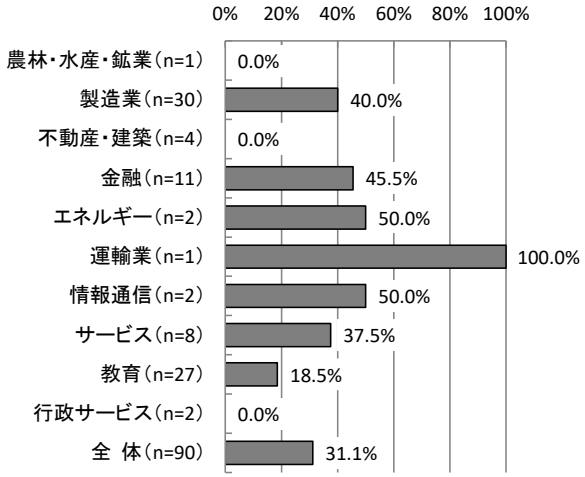
最新パッチの適用



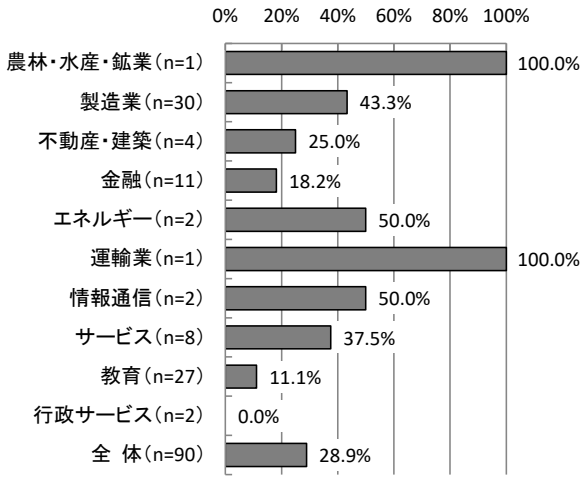
ソフトウェアのバージョンアップ



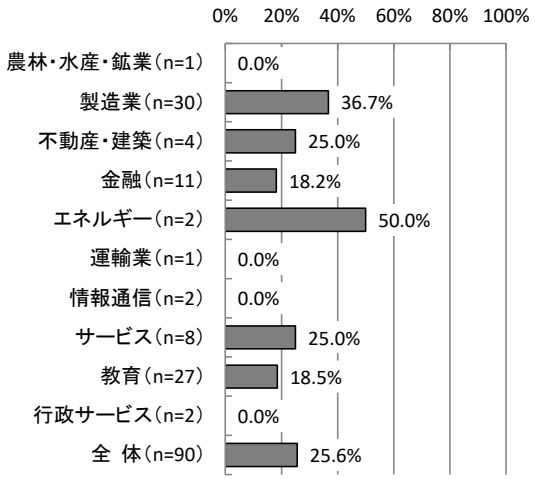
認証機能の導入・強化



ウイルス等対策製品の導入・強化



不正アクセスが行われていないかどうか
ネットワークの監視

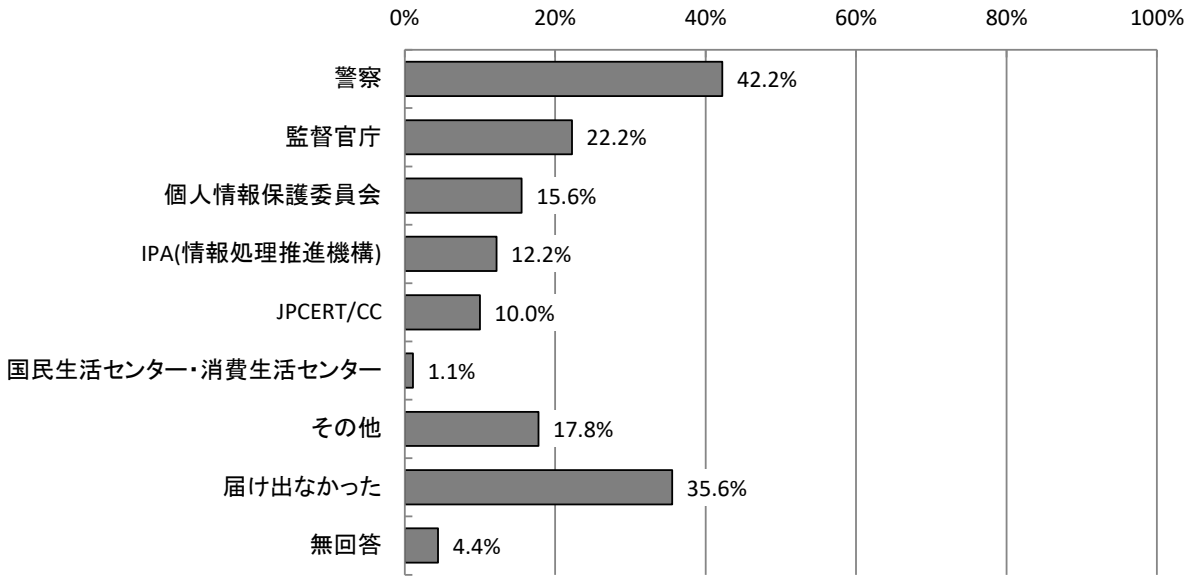


3.1.16　届出先機関等　【問10-4-1】

届出先機関等については、「警察」が42.2%で最も高く、次いで「監督官庁」が22.2%、「個人情報保護委員会」が15.6%となっている。一方、「届け出なかった」は35.6%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。

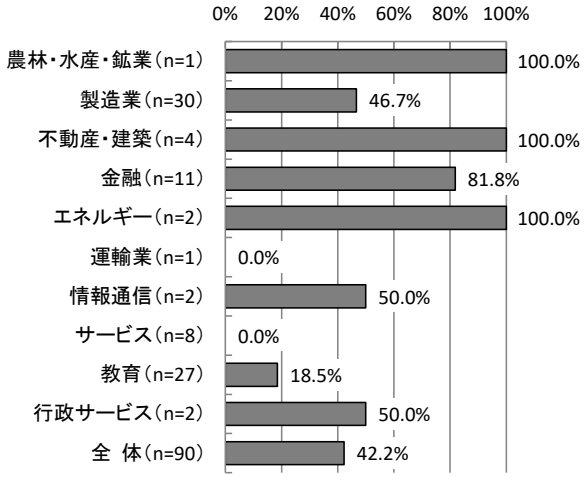
【全体】届出先機関等（MA, n=90）



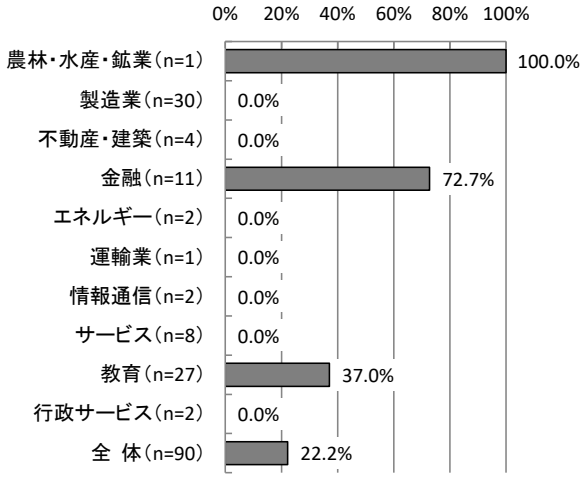
【業種別分析】業種別にみると、「警察」と「監督官庁」については「金融」がいずれも7割を超えて高くなっている。一方、「届け出なかった」については、「サービス」が62.5%と高くなっている。

【業種別分析】届出先機関等

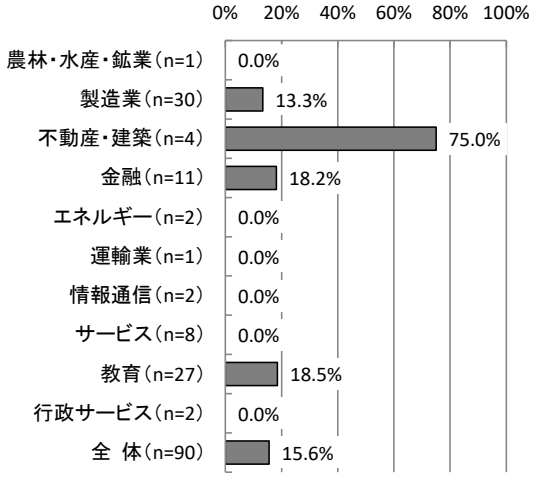
警察



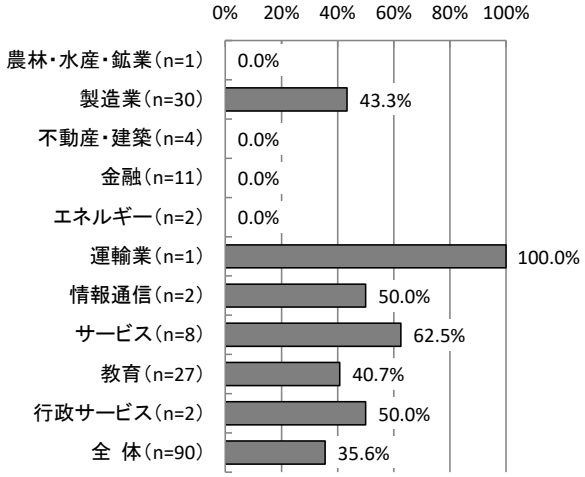
監督官庁



個人情報保護委員会



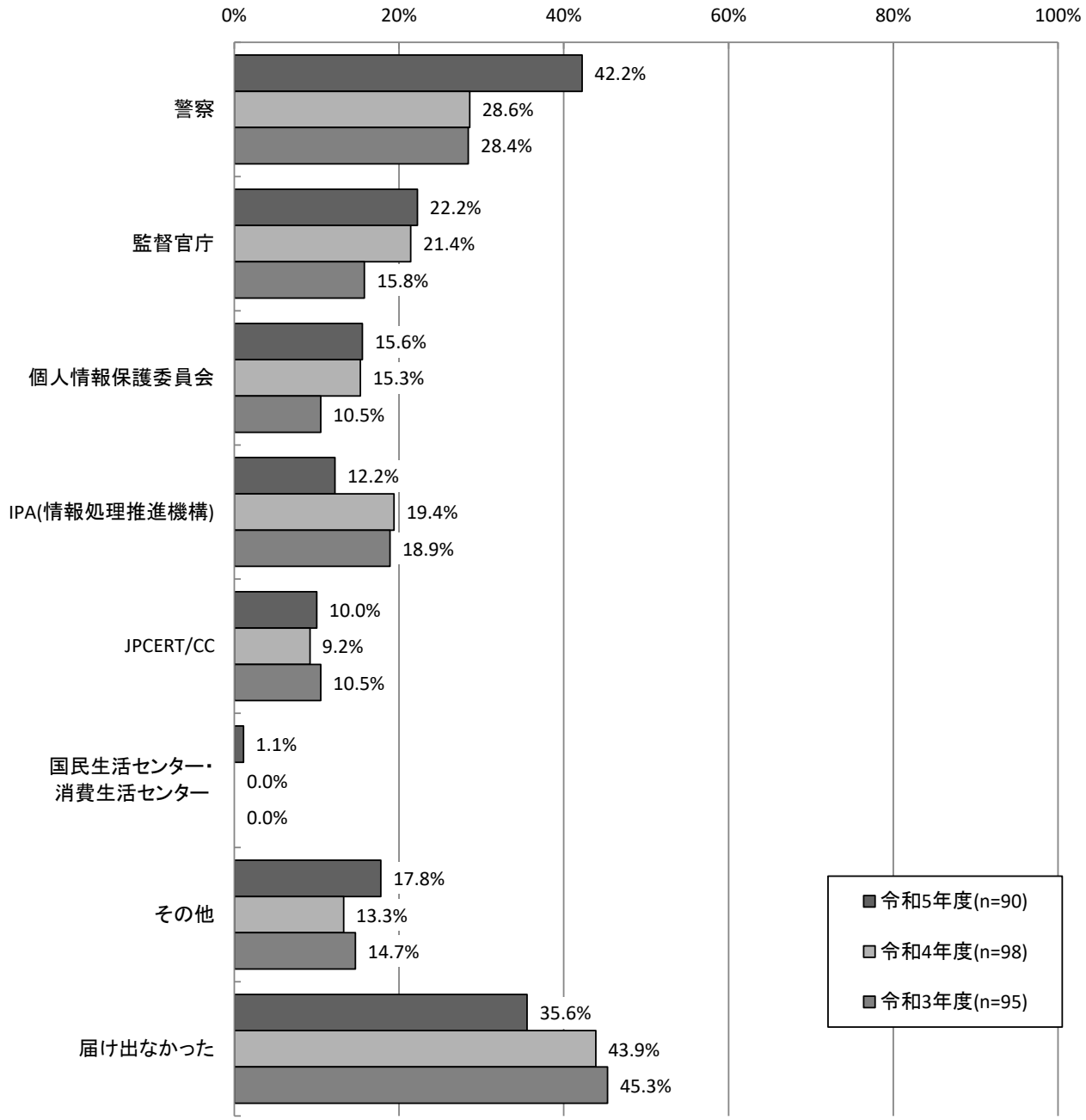
届け出なかった



【経年変化】昨年度と比較すると、「警察」が13.6ポイント増加した一方で、「IPA(情報処理推進機構)」が7.2ポイント減少している。「届け出なかった」は8.3ポイント減少している。

※「無回答」を除いた総数で比較している。

【経年変化】届出先機関等

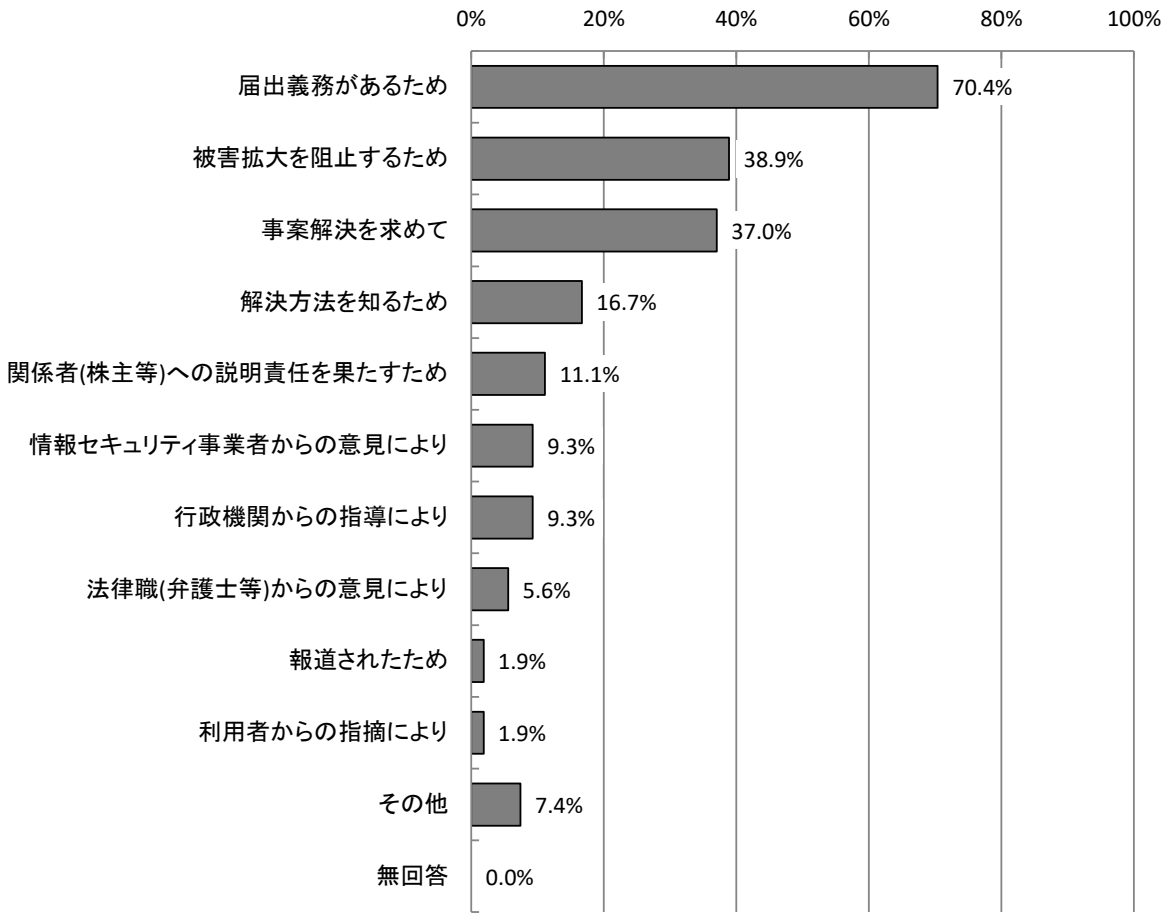


3.1.17　届出した理由　【問10-4-2】

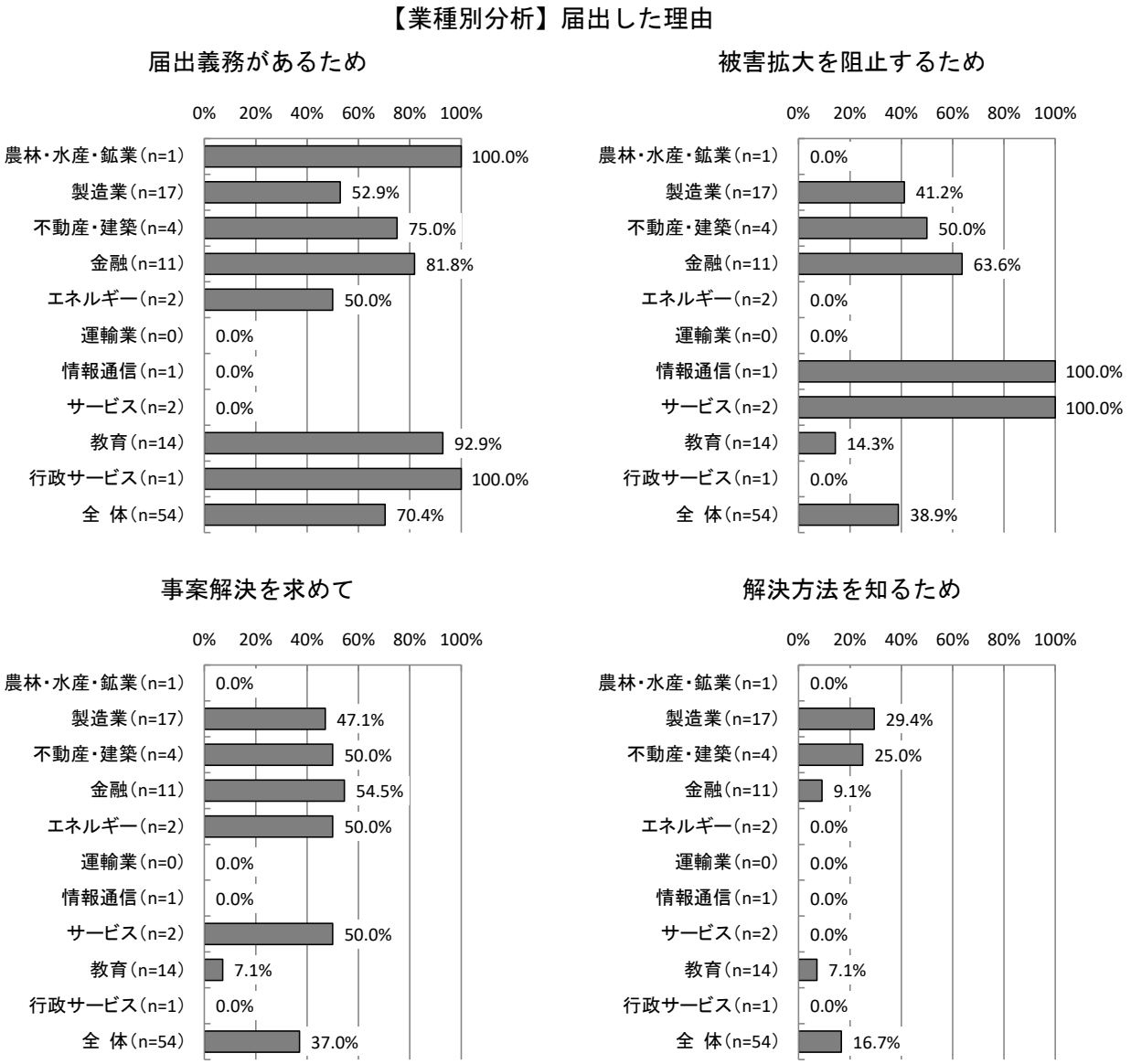
届出した理由については、「届出義務があるため」が70.4%で最も多く、次いで「被害拡大を阻止するため」が38.9%、「事案解決を求めて」が37.0%となっている。

※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=54）

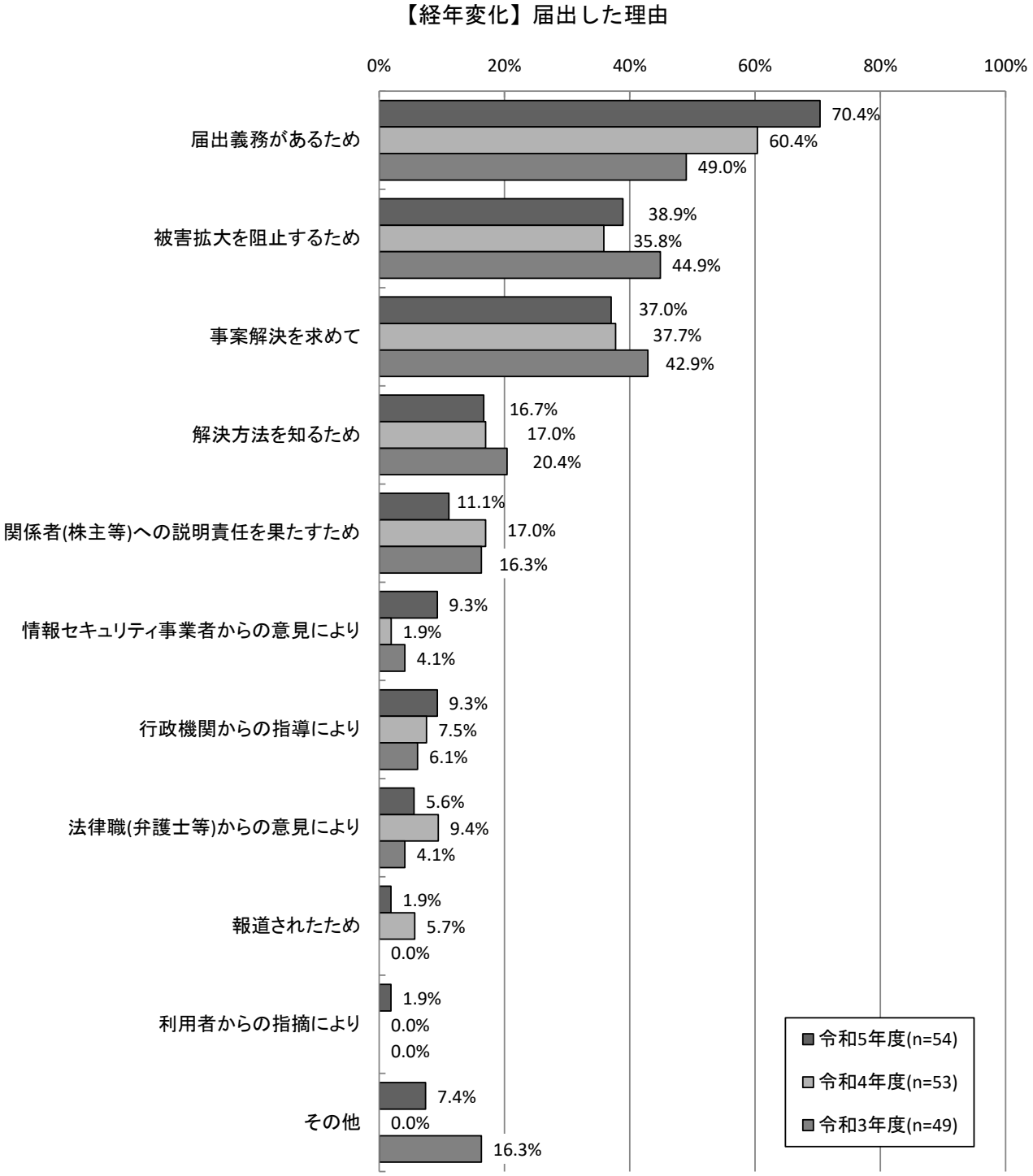


【業種別分析】業種別にみると、「届出義務があるため」は「教育」が92.9%で高く、「被害拡大を阻止するため」では「金融」が63.6%で高い。「事案解決を求めて」については「金融」が54.5%で高い。



【経年変化】昨年度と比較すると、「届出義務があるため」が10.0ポイント、「情報セキュリティ事業者からの意見により」が7.4ポイント増加し、「関係者(株主等)への説明責任を果たすため」が5.9ポイント減少となっている

※「無回答」を除いた総数で比較している。

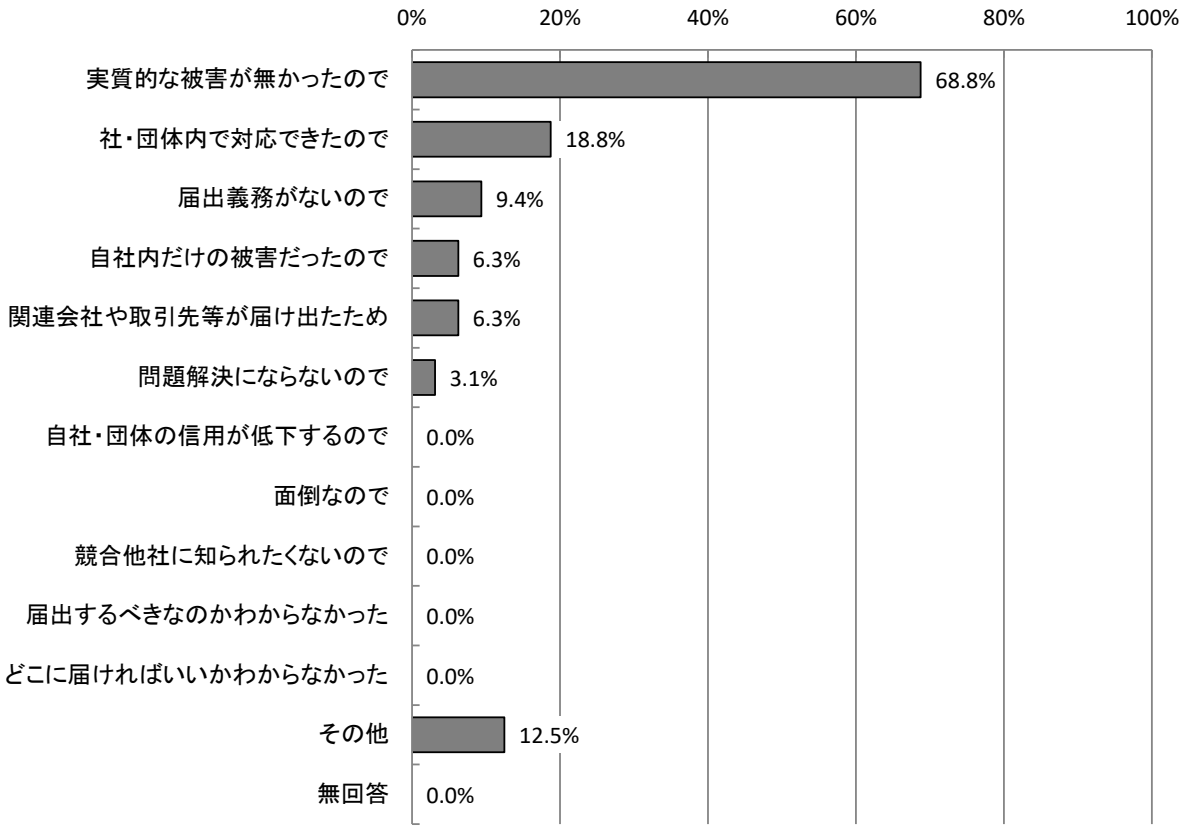


3.1.18　届出を躊躇させる要因　【問10-5】

届出を躊躇させる要因については、「実質的な被害が無かったので」が68.8%で最も高く、次いで「社・団体内で対応できたので」が18.8%、「届出義務がないので」が9.4%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。

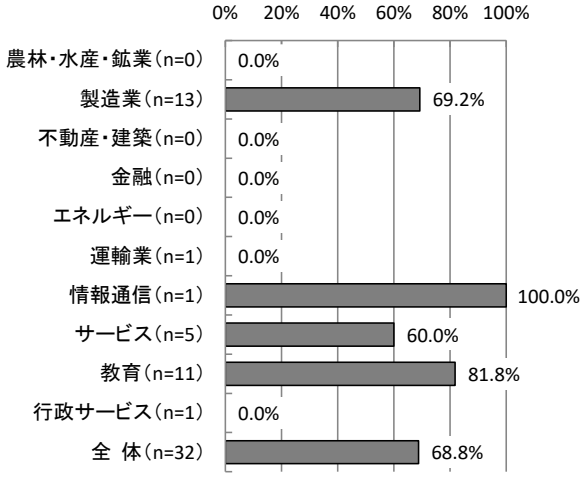
【全体】届出を躊躇させる要因（MA, n=32）



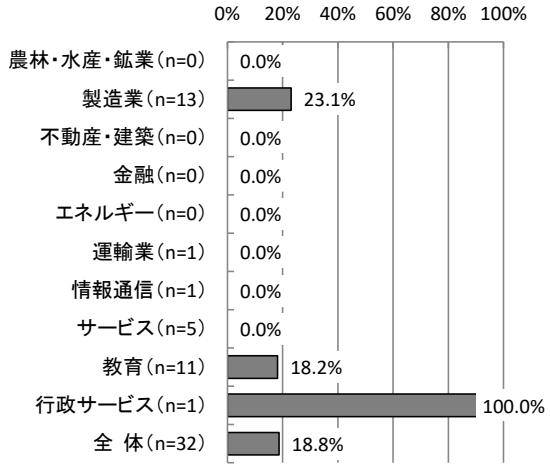
【業種別分析】業種別にみると、「実質的な被害が無かったので」については、「教育」が81.8%、「製造業」が69.2%となっている。「社・団体内で対応できたので」については、「製造業」が23.1%、「教育」が18.2%となっている。

【業種別分析】届出を躊躇させる要因

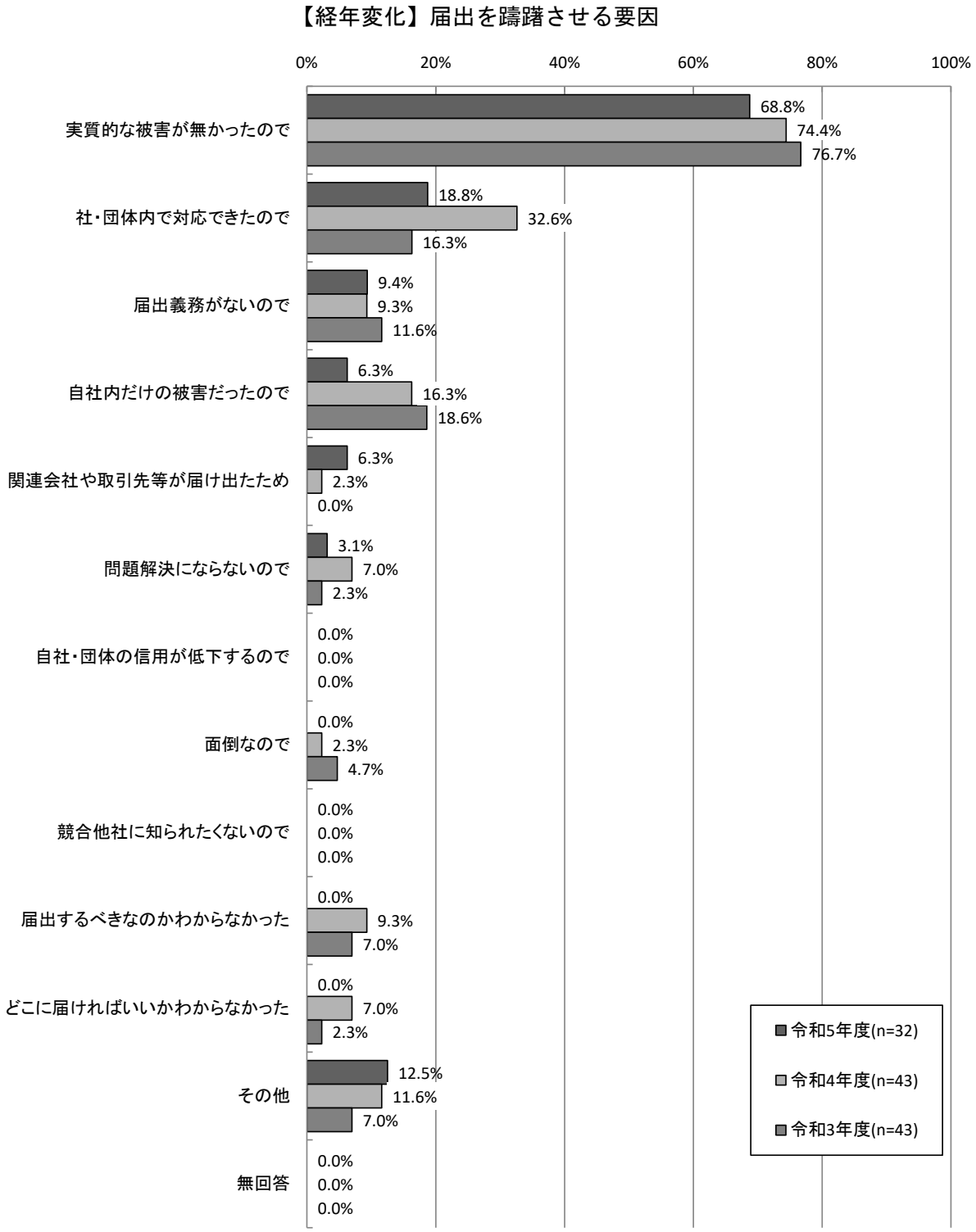
実質的な被害が無かったので



社・団体内で対応できたので



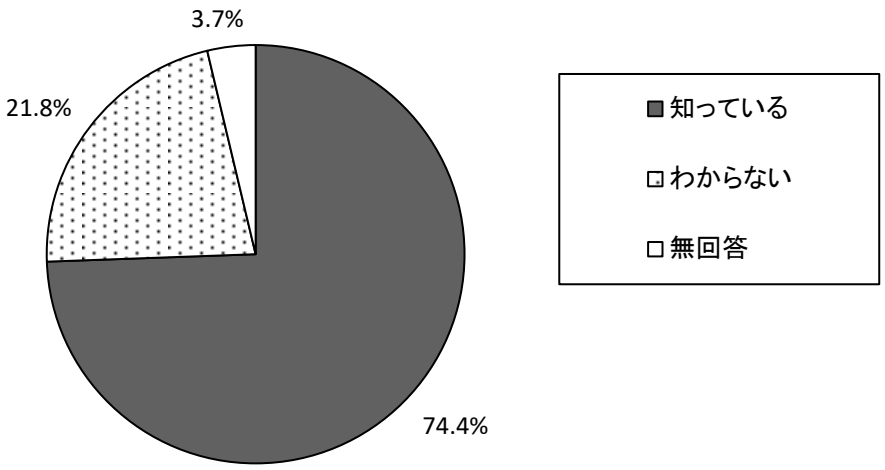
【経年変化】昨年度と比較すると、「社・団体内で対応できたので」が13.8ポイント、「自社内だけの被害だったので」が10.0ポイント、「届出するべきなのかわからなかった」が9.3ポイント減少している。



3.1.19　届出先機関を知っているか　【問11】

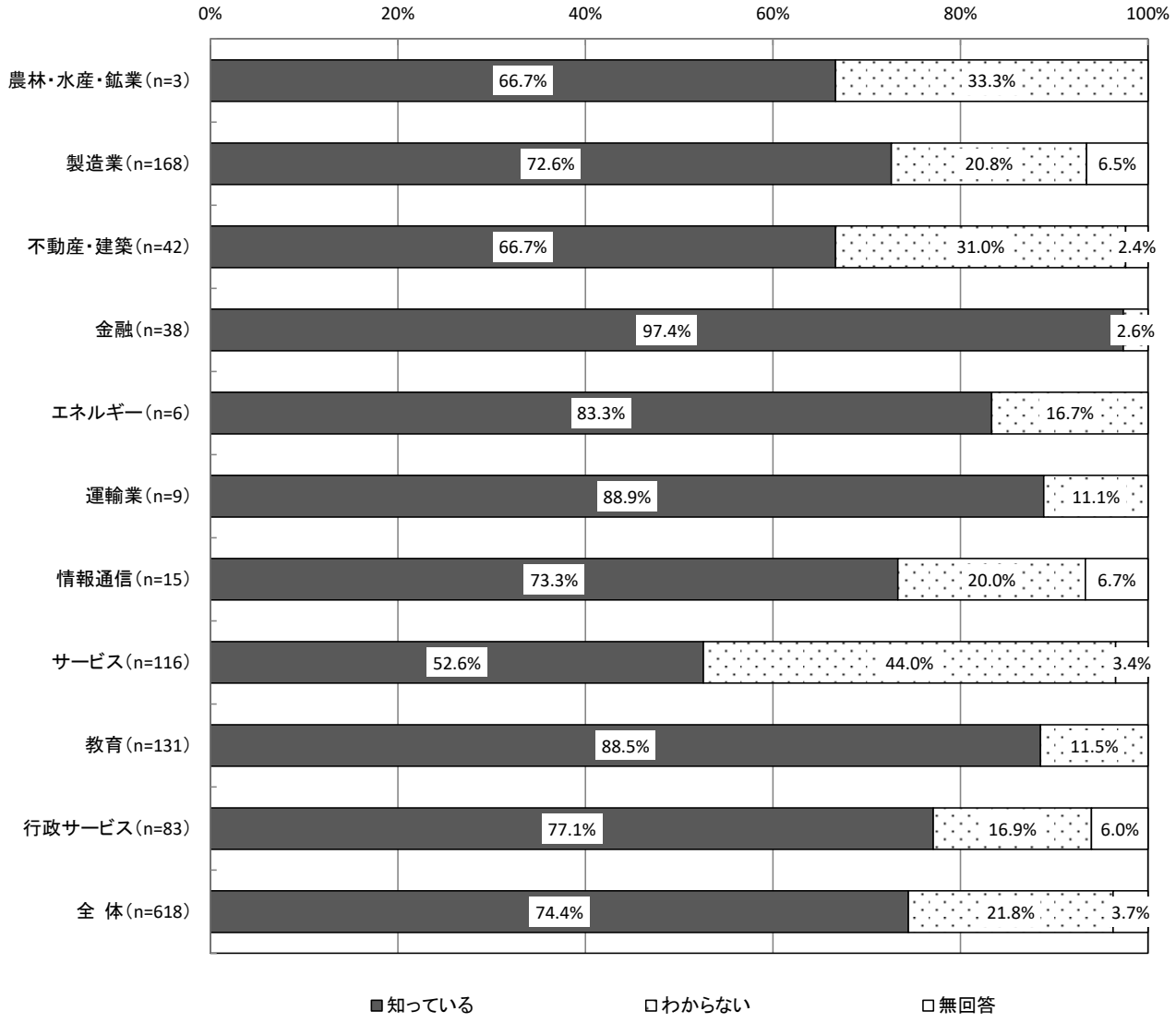
届出先機関を知っているかについては、「知っている」が74.4%と高く、「わからない」は21.8%となっている。

【全体】届出先機関を知っているか（SA,n=618）



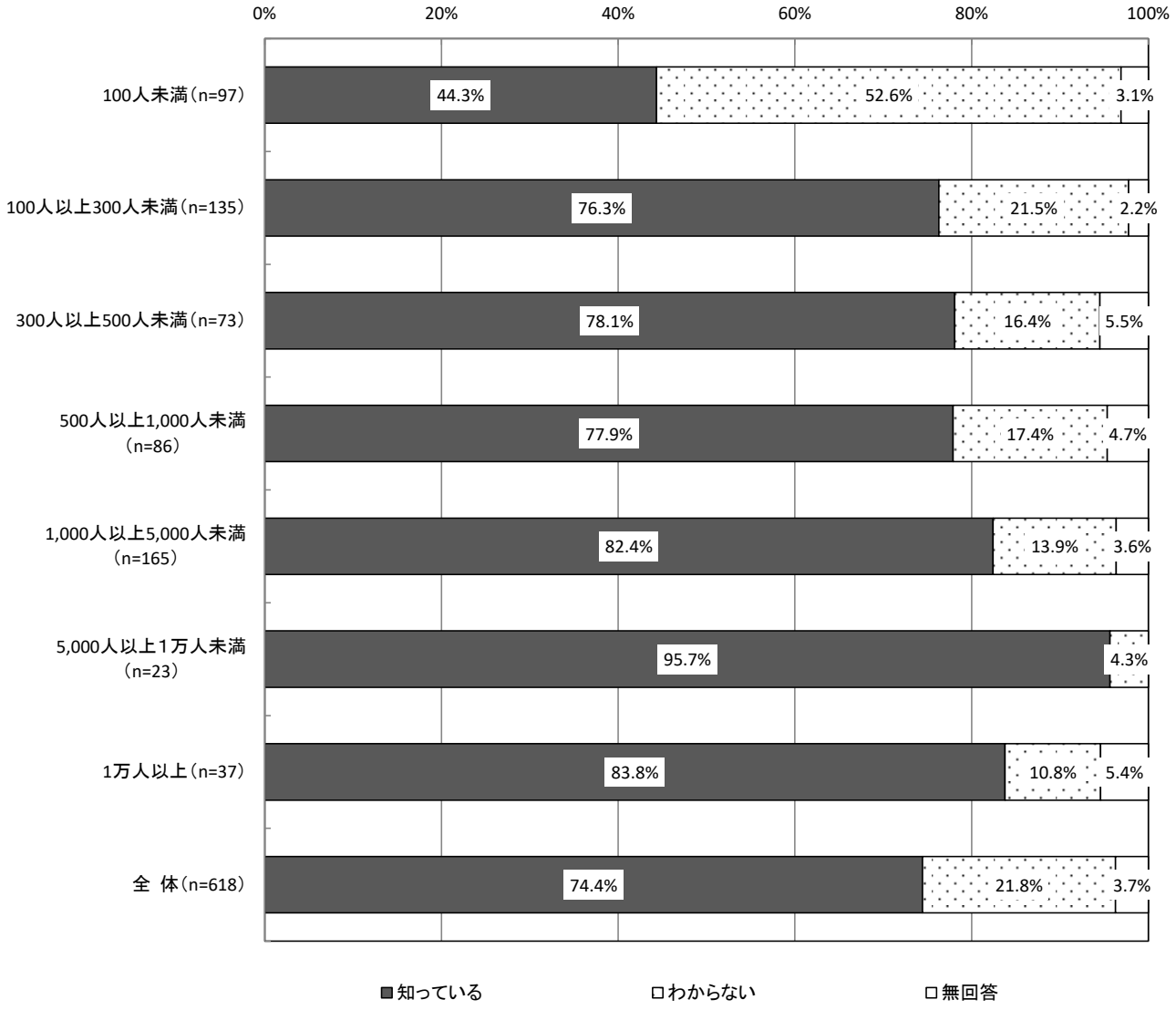
【業種別分析】業種別にみると、届出先機関を「知っている」については、「金融」が 97.4%、「運輸業」が 88.9%で高い。一方、「わからない」については、「サービス」が 44.0%、「不動産・建築」が 31.0%となっている。

【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、100人以上では「知っている」が「わからない」より高くなっている。「100人未満」では52.6%が「わからない」と回答しており、「知っている」より高くなっている。

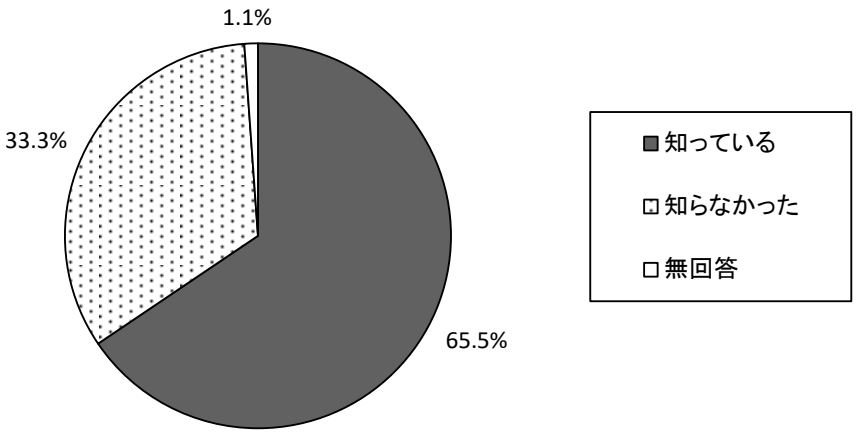
【従業員規模別分析】届出先機関を知っているか



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

アクセス管理者による防御措置についての努力義務については、「知っている」が65.5%、「知らなかった」は33.3%となっている。

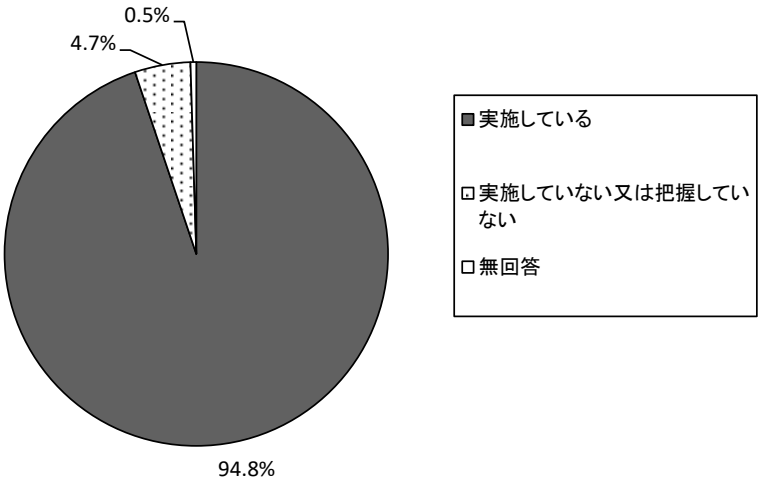
【全体】不正アクセス禁止法でアクセス管理者による防御措置についての努力義務（SA,n=618）



3.1.21　情報セキュリティ対策の実施状況　【問13】

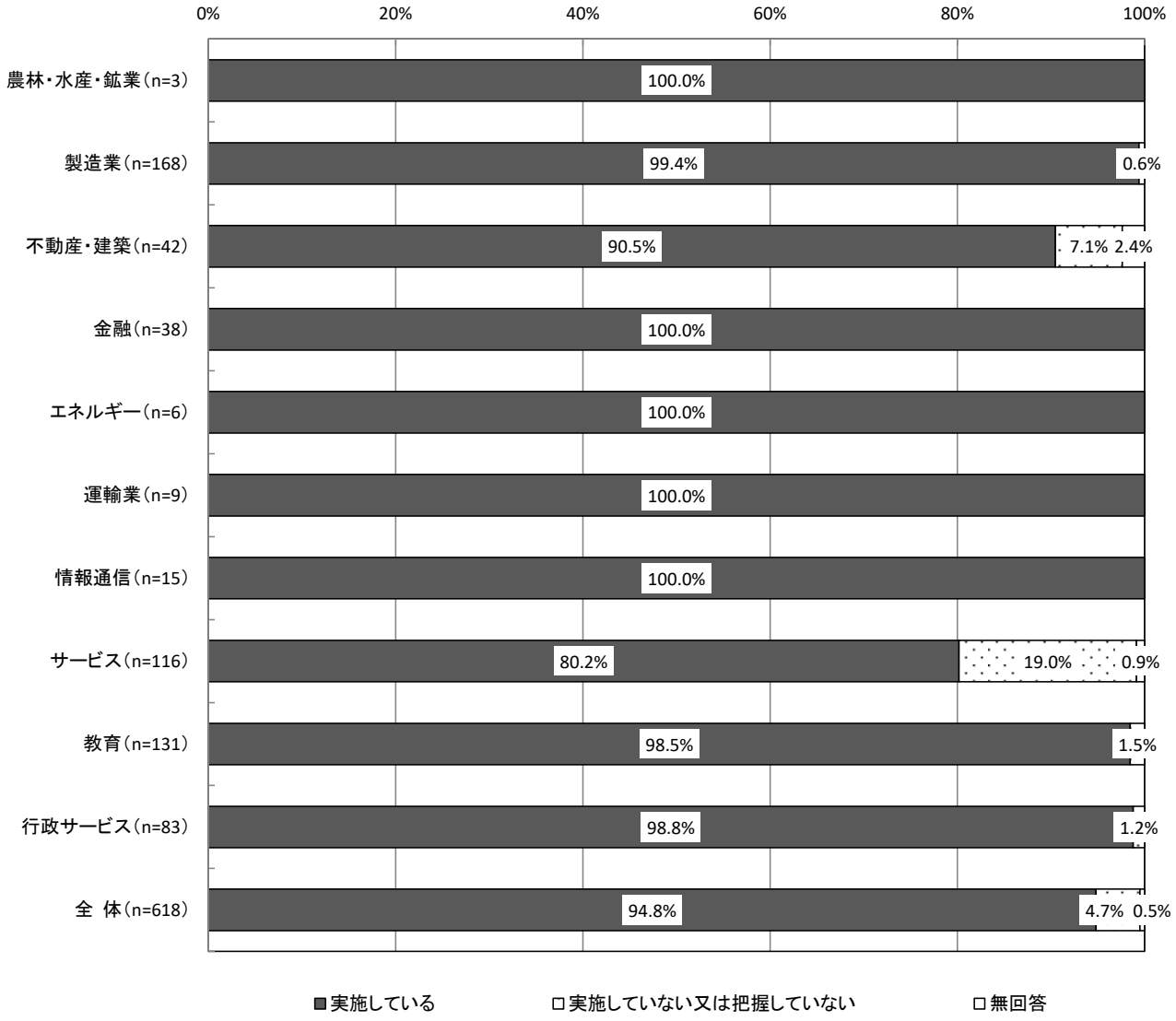
情報セキュリティ対策の実施状況については、「実施している」が94.8%、「実施していない又は把握していない」が4.7%となっている。

【全体】情報セキュリティ対策の実施状況（SA,n=618）

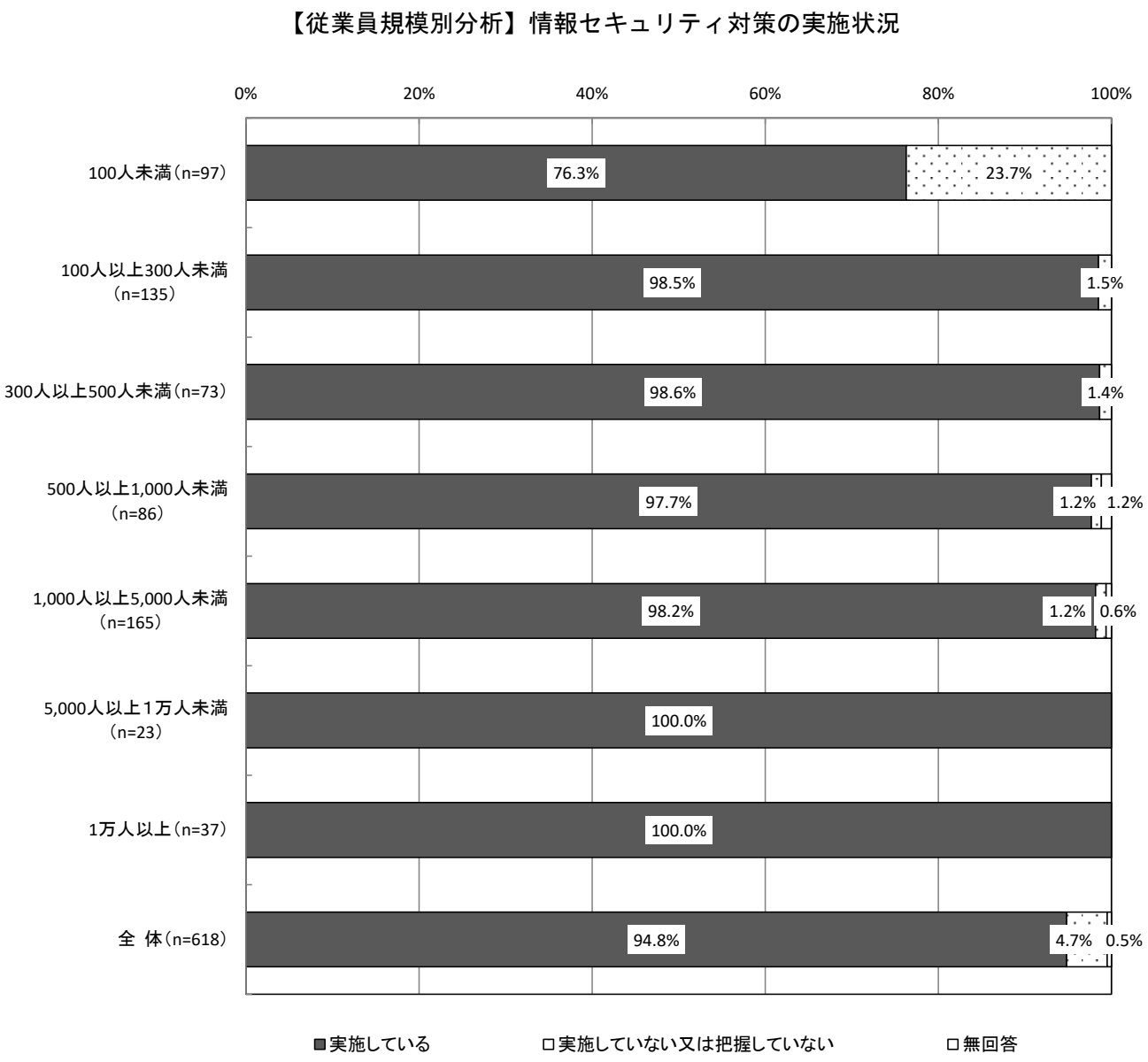


【業種別分析】業種別では情報セキュリティ対策を「実施している」がいずれも 8 割を超えている。このうち「金融」「エネルギー」「運輸業」「情報通信」は 100.0%と高い割合である。最も低いのは「サービス」の 80.2%となっている。

【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「実施している」が95%以上であるのに対して、「100人未満」では「実施していない又は把握していない」が23.7%となっている。

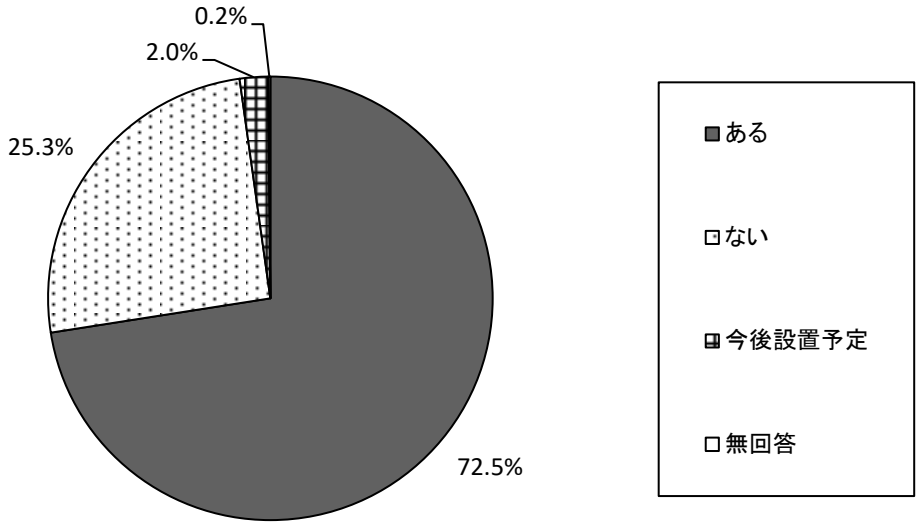


3.1.22　情報セキュリティ運用・管理専門部署の有無　【問13-1】

情報セキュリティ運用・管理専門部署の有無については、「ある」が72.5%と高く、「ない」は25.3%となっている。

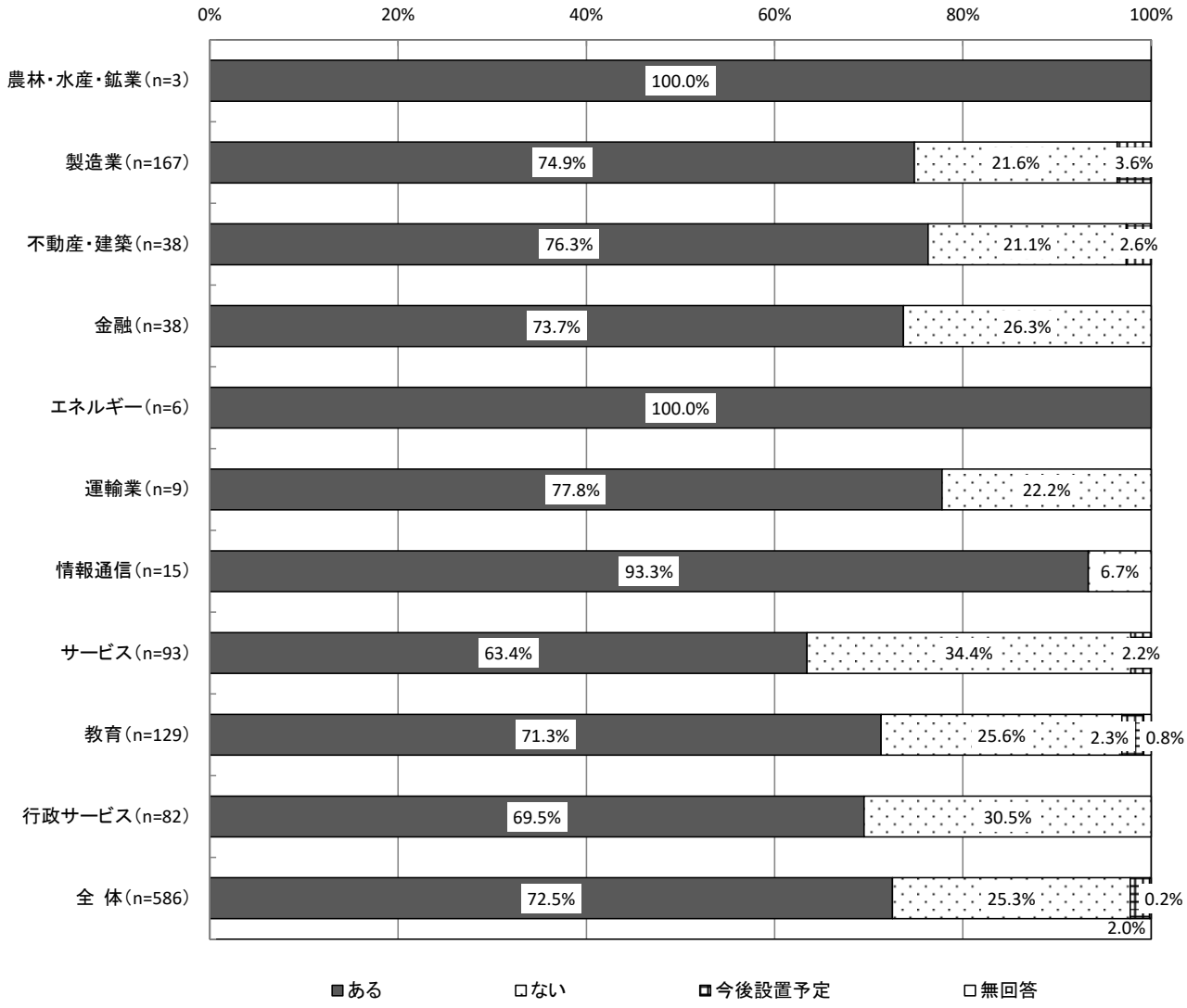
※本項目は、情報セキュリティ対策を行っている社・団体等を対象としている。

【全体】情報セキュリティ運用・管理専門部署の有無（SA,n=586）



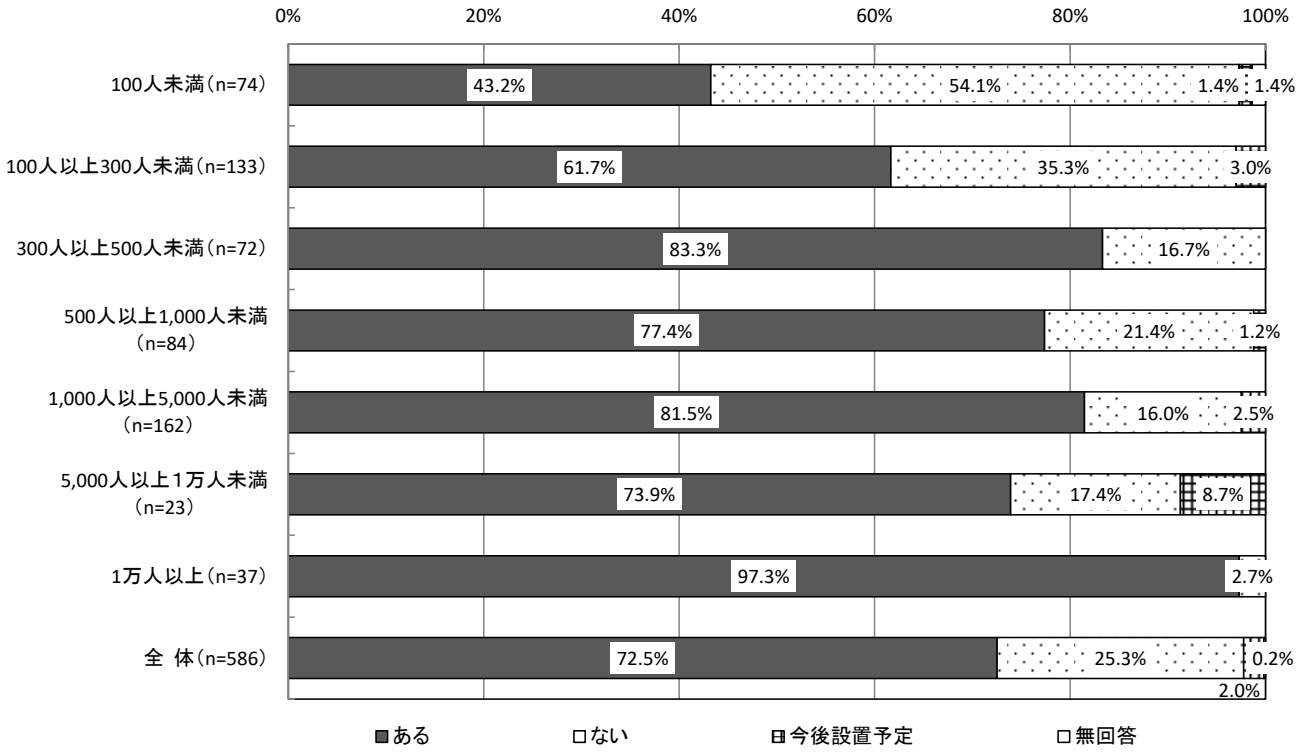
【業種別分析】業種別にみると、情報セキュリティ運用・管理専門部署が「ある」については、「エネルギー」が 100.0%、「情報通信」が 93.3%などで高くなっている。一方、情報セキュリティ運用・管理専門部署が「ない」については、「サービス」が 34.4%、「行政サービス」が 30.5%で高くなっている。

【業種別分析】情報セキュリティ運用・管理専門部署の有無



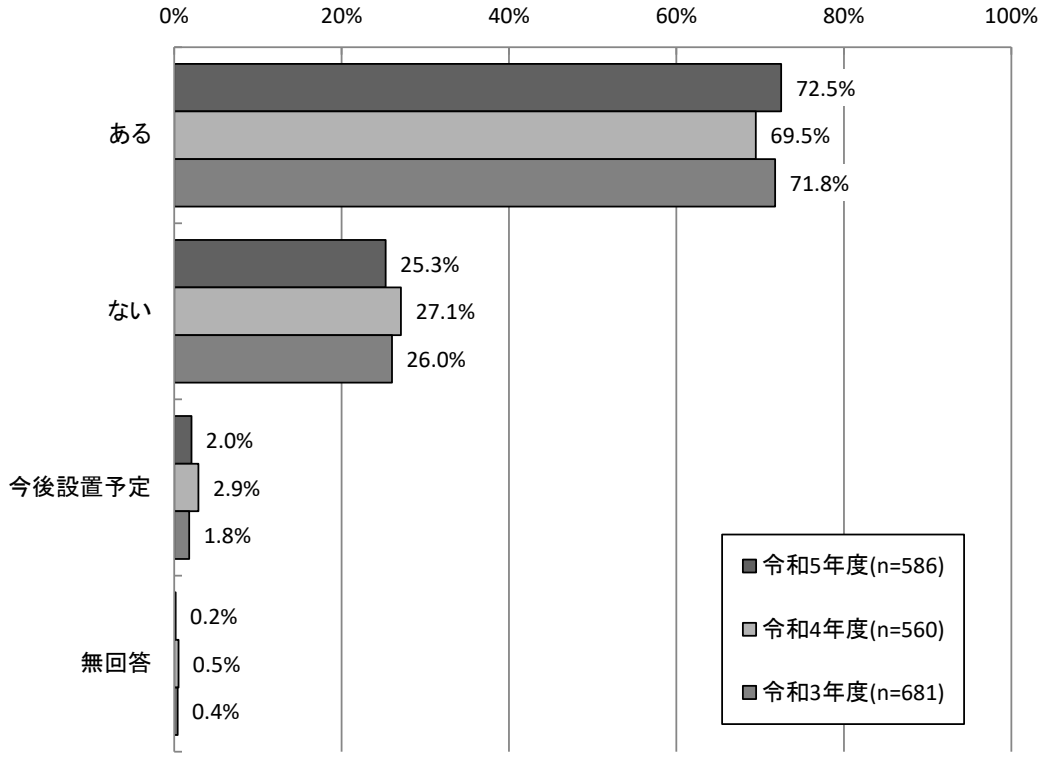
【従業員規模別分析】従業員規模別にみると、「ある」は「１万人以上」で97.3%と高くなっている。一方、「ない」は「100人未満」で54.1%と最も高くなっている。

【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、情報セキュリティ運用・管理専門部署が「ある」が3.0ポイント増加し、「ない」が1.8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

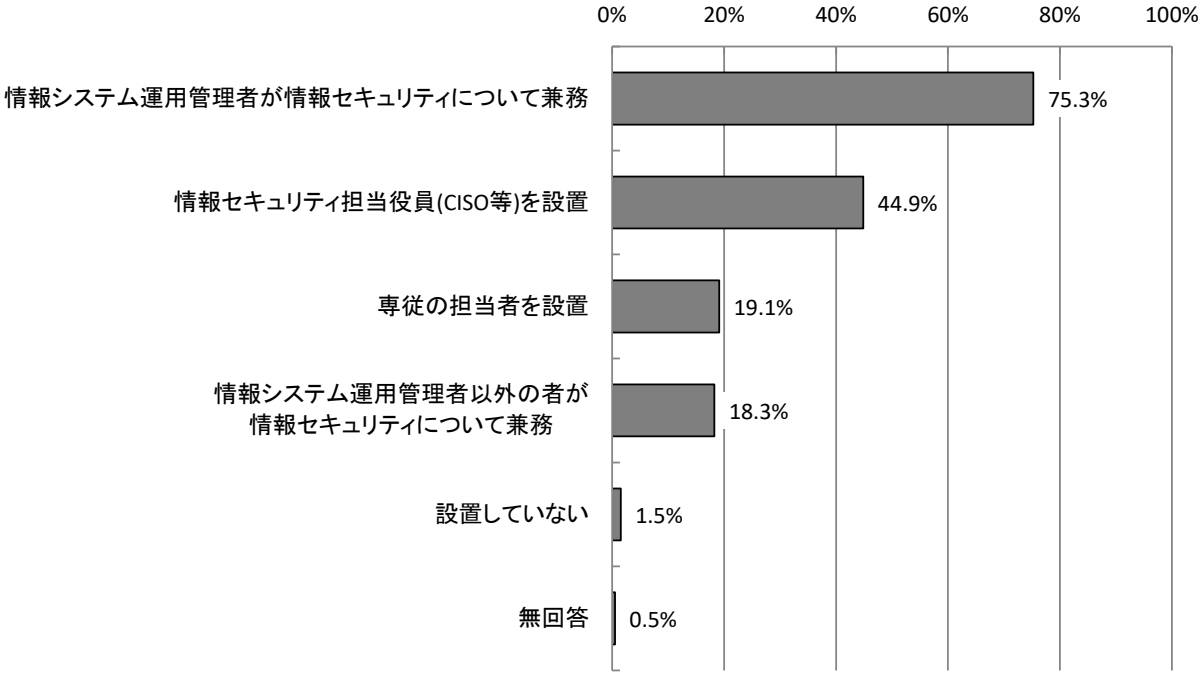


3.1.23　情報セキュリティ管理体制　【問13-2】

情報セキュリティ管理体制については、「情報システム運用管理者が情報セキュリティについて兼務」が75.3%で最も高く、次いで「情報セキュリティ担当役員(CISO等)を設置」が44.9%、「専従の担当者を設置」が19.1%となっている。

※本項目は、情報セキュリティ対策を行っている社・団体等を対象としている。

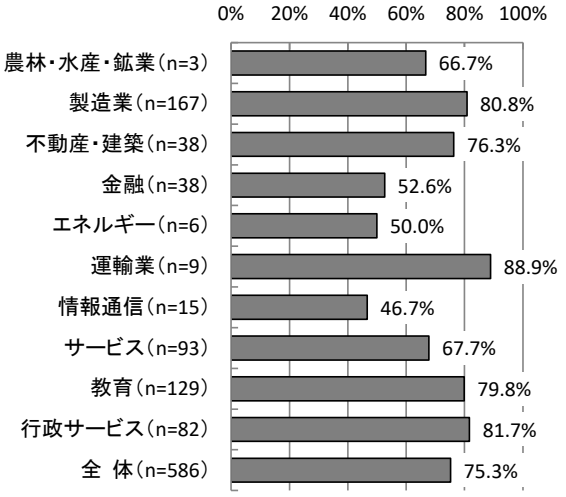
【全体】情報セキュリティ管理体制（MA, n=586）



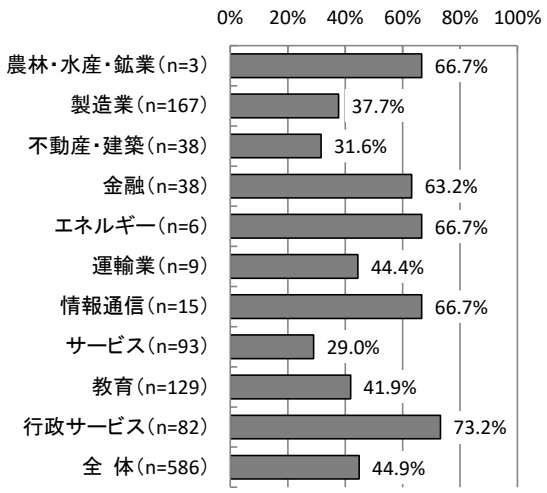
【業種別分析】業種別にみると、「情報システム運用管理者が情報セキュリティについて兼務」については、「運輸業」が88.9%、「行政サービス」が81.7%、「製造業」で80.8%と高くなっている。「情報セキュリティ担当役員(CISO等)を設置」については、「行政サービス」が73.2%で最も高い。「専従の担当者を設置」では、「情報通信」が60.0%で最も高い。

【業種別分析】情報セキュリティ管理体制

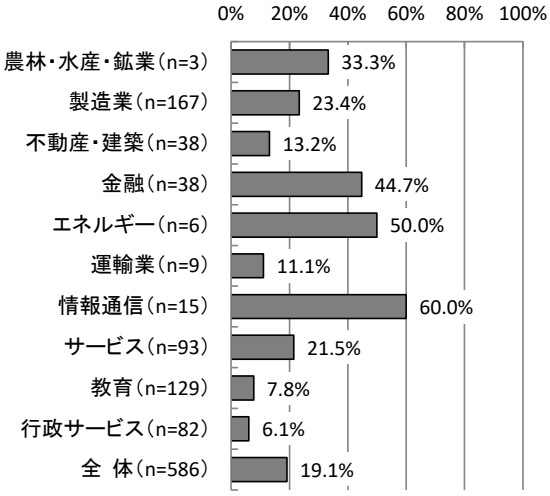
情報システム運用管理者が情報セキュリティについて兼務



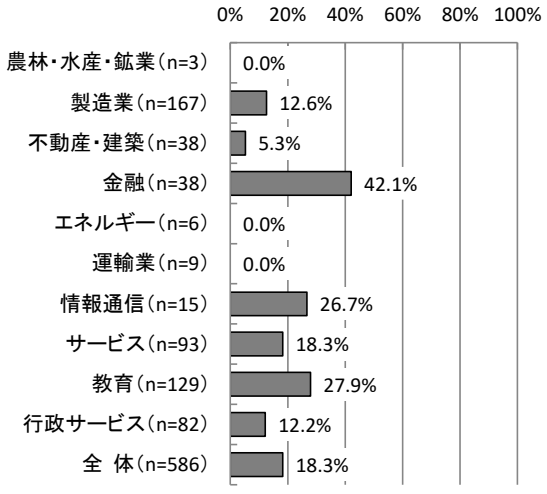
情報セキュリティ担当役員(CISO等)を設置



専従の担当者を設置

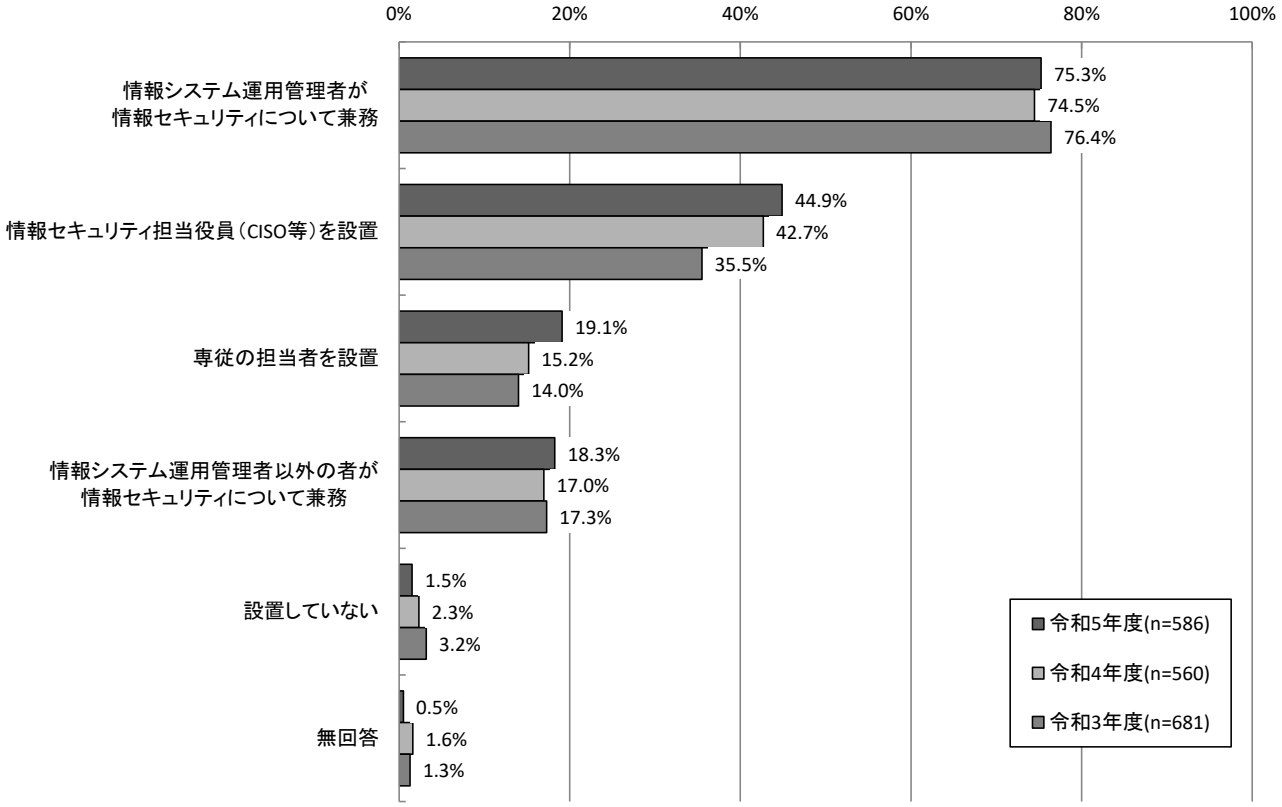


情報システム運用管理者以外の者が情報セキュリティについて兼務



【経年変化】昨年度と比較すると、「専従の担当者を設置」が3.9ポイント、「情報セキュリティ担当役員（CISO等）を設置」が2.2ポイント増加している。「設置していない」は昨年度に続き減少している。

【経年変化】情報セキュリティ管理体制

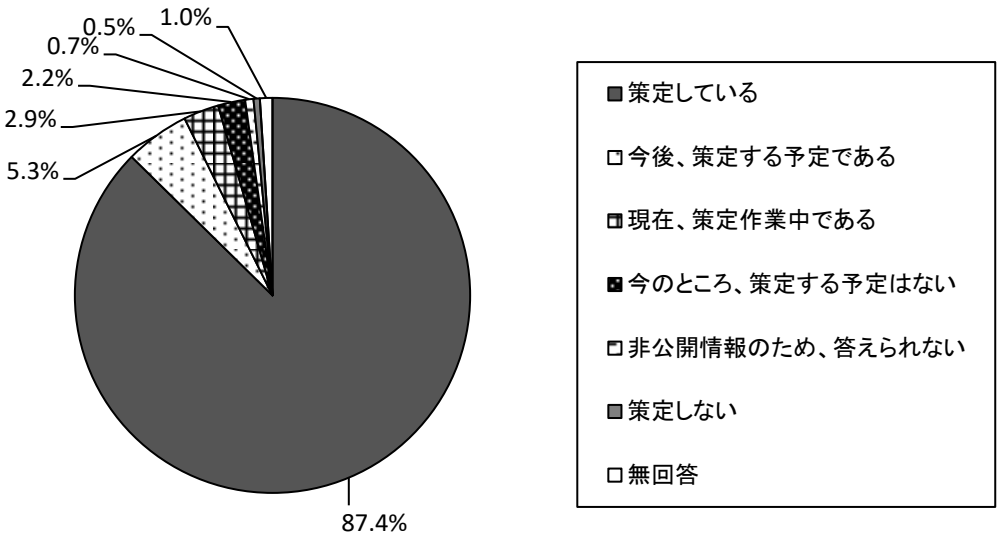


3.1.24　セキュリティポリシーの策定状況　【問13-3】

セキュリティポリシーの策定状況については、「策定している」が87.4%で最も高く、次いで「今後、策定する予定である」が5.3%、「現在、策定作業中である」が2.9%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95.6%となっている。

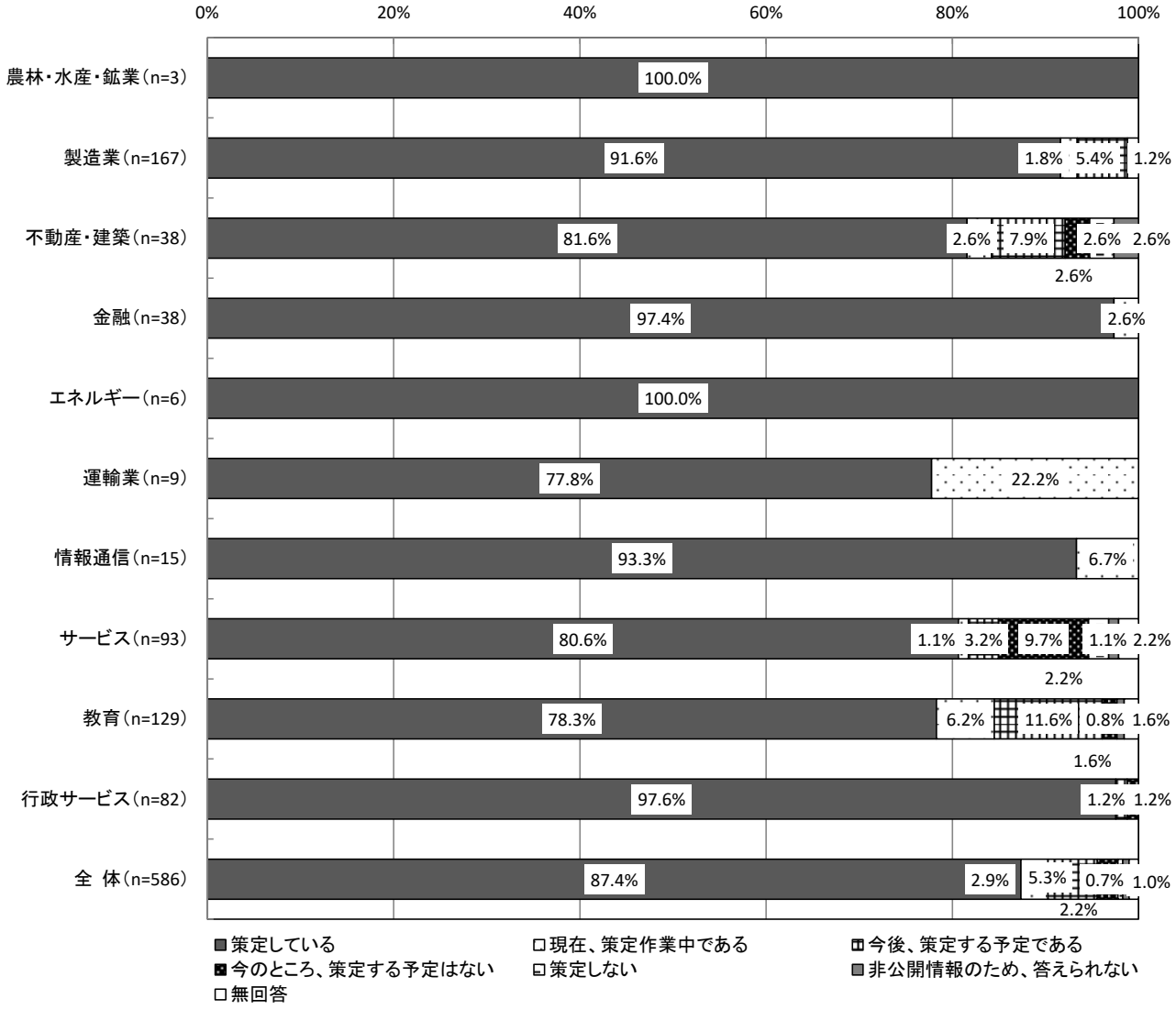
※本項目は、情報セキュリティ対策を行っている社・団体等を対象としている。

【全体】セキュリティポリシーの策定状況（SA,n=586）



【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%、「行政サービス」が97.6%、「金融」が97.4%、「情報通信」が93.3%、「製造業」が91.6%と9割を超えている。一方「策定している」が低いのは、「運輸業」の77.8%、「教育」の78.3%となっている。

【業種別分析】セキュリティポリシーの策定状況

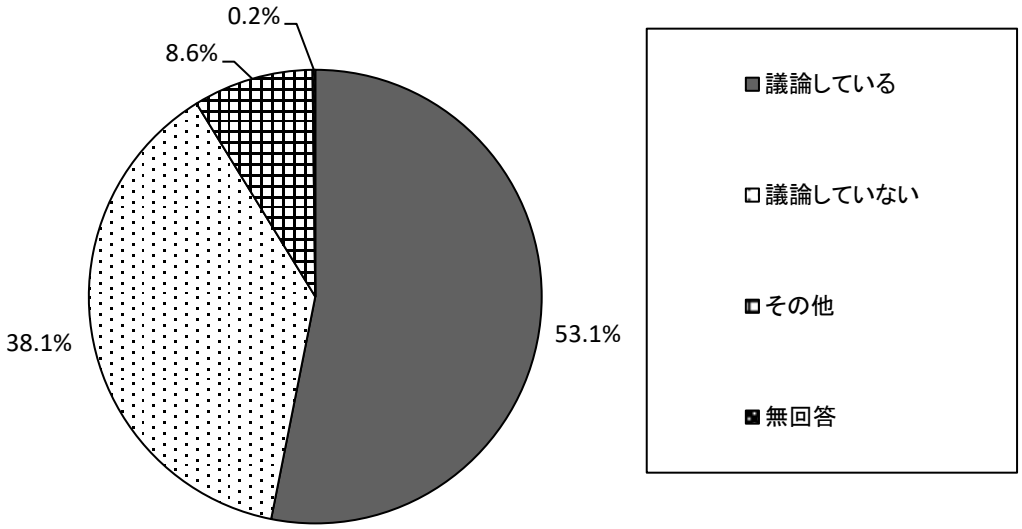


3.1.25　セキュリティ関連事項の定期的な議論の状況【問13-3-1】

セキュリティの関連事項を役員会議や経営会議等の議題として定期的に議論しているかについては、「議論している」が53.1%、「議論していない」が38.1%となっている。

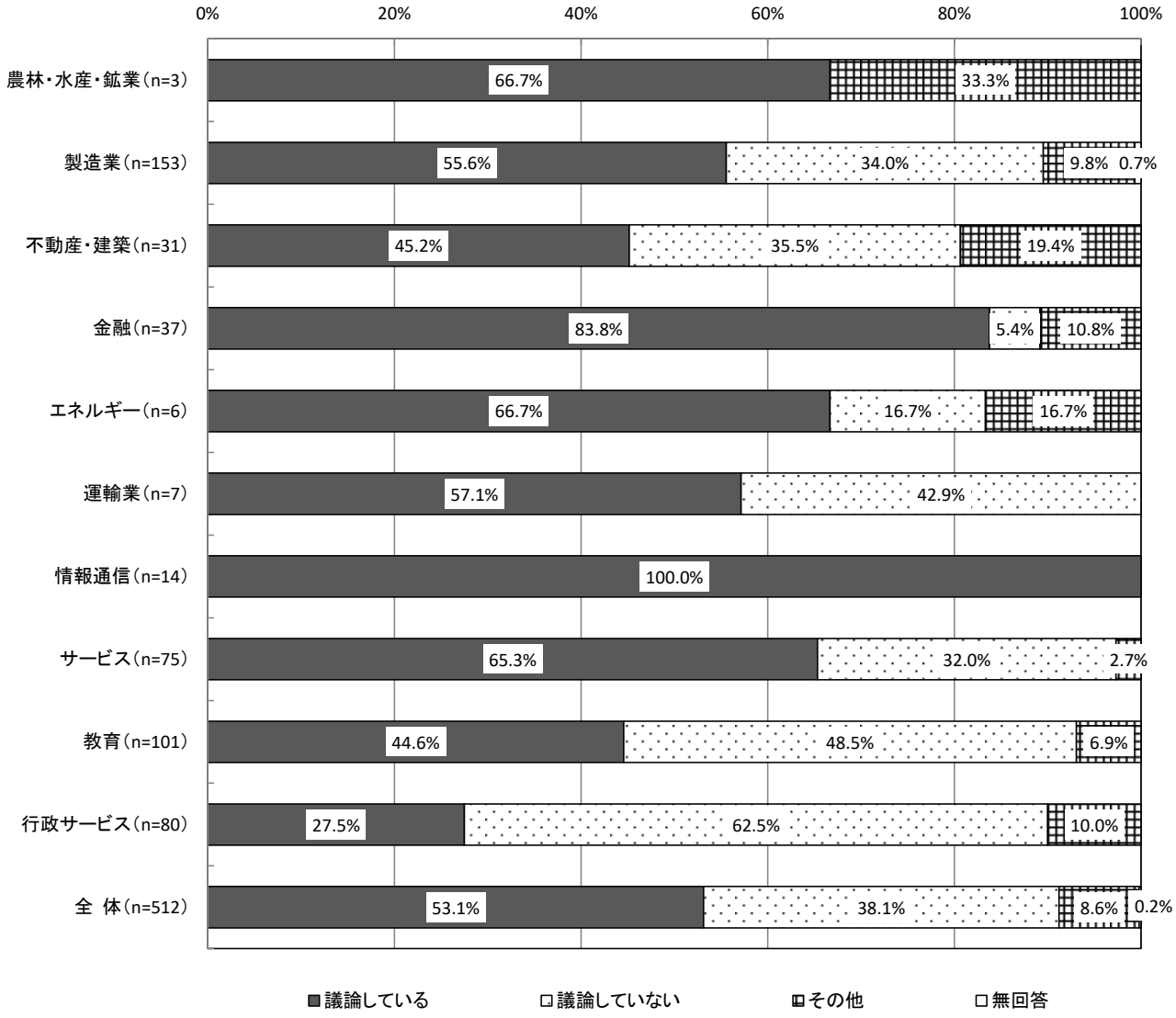
【全体】セキュリティの関連事項を役員会議や経営会議等の議題として定期的に議論しているか

(SA,n=512)



【業種別分析】業種別にみると、セキュリティの関連事項を役員会議や経営会議等の議題として定期的に議論しているかについては、「議論している」では「情報通信」の100.0%が最も高く、次いで「金融」が83.8%となっている。

【業種別分析】セキュリティの関連事項を役員会議や経営会議等の議題として定期的に議論しているか

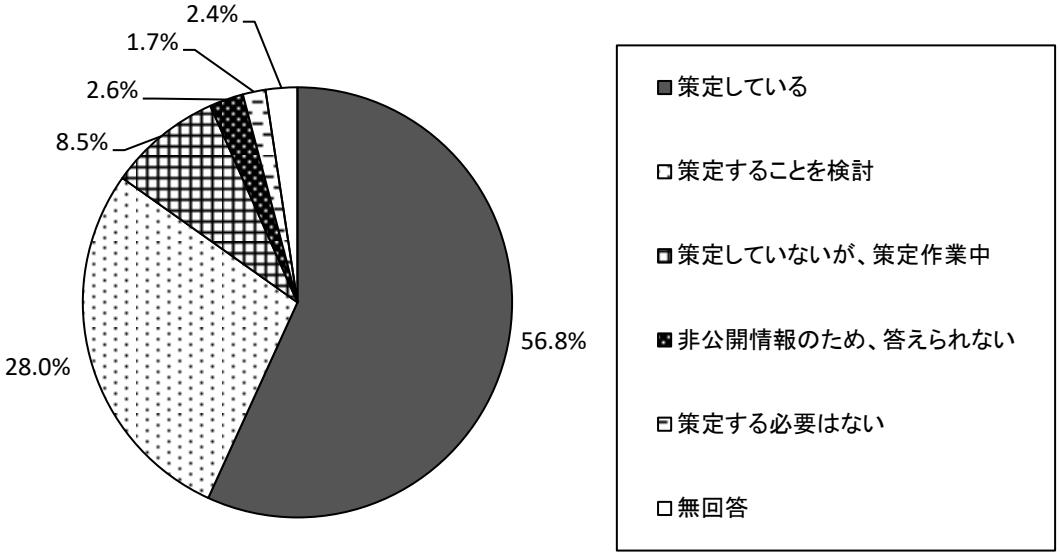


3.1.26　情報セキュリティ侵害事案発生時の対応マニュアル等の策定状況　【問13-4】

情報セキュリティ侵害事案発生時の対応マニュアル等の策定状況については、「策定している」が56.8%で過半数となっている。次いで「策定することを検討」が28.0%、「策定していないが、策定作業中」が8.5%となっている。

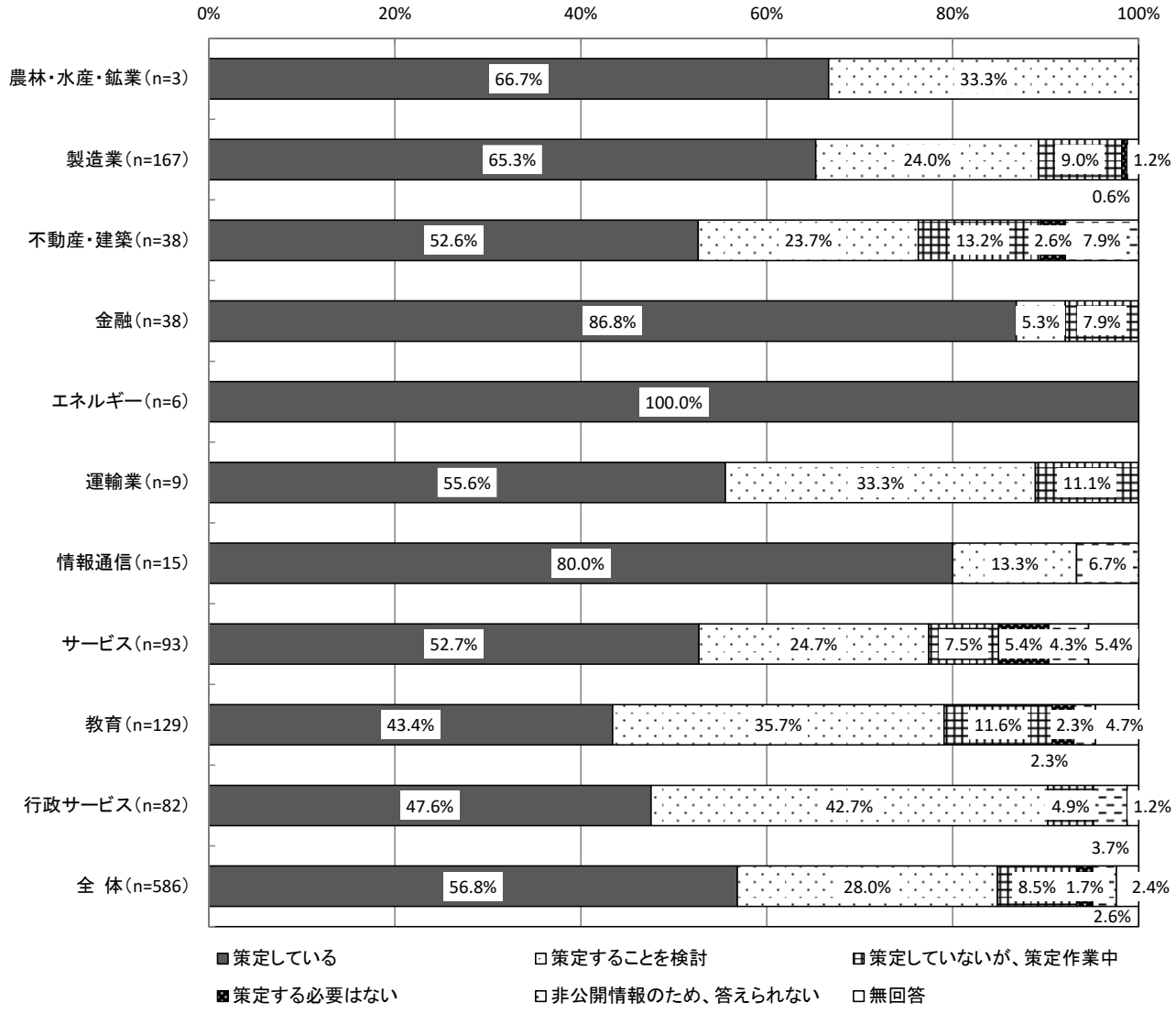
※本項目は、情報セキュリティ対策を行っている社・団体等を対象としている。

【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=586）



【業種別分析】業種別にみると、「策定している」については、「エネルギー」の100.0%、「金融」の86.8%などが高い。これに対して「教育」が43.4%、「行政サービス」が47.6%と低くなっている。

【業種別分析】情報セキュリティ侵害事案発生時の対応マニュアル等の策定状況

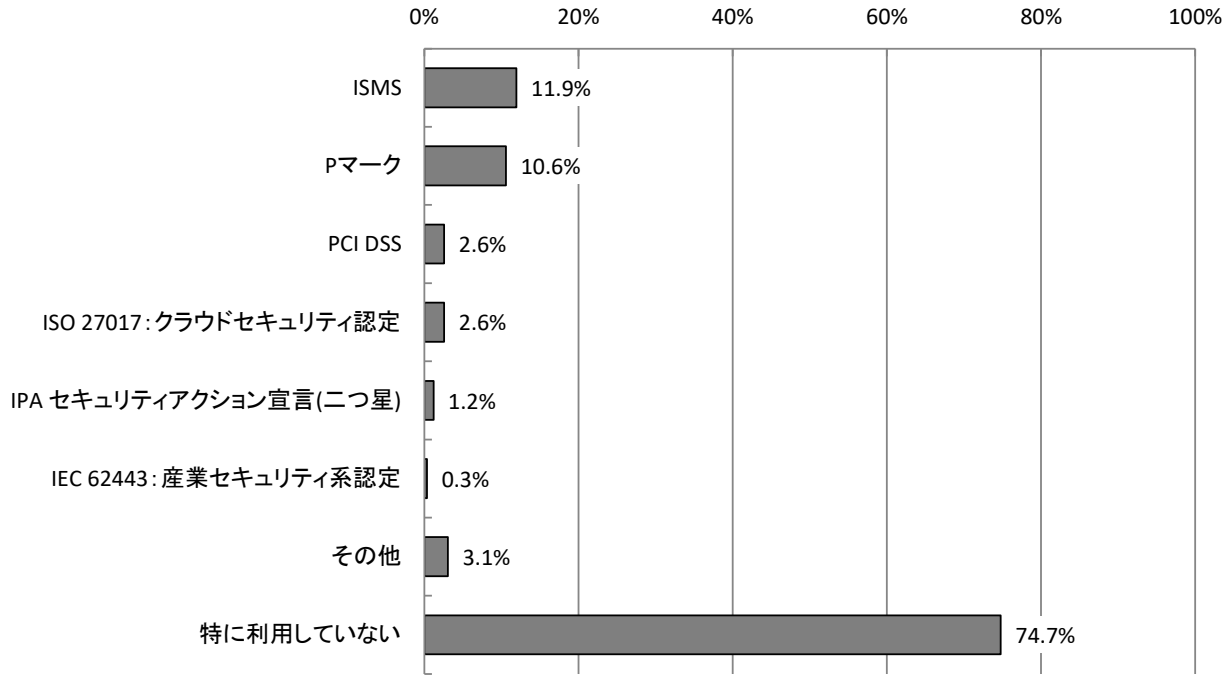


3.1.27　第三者機関の認証制度等の利用状況　【問13-5】

第三者機関の認証制度等の利用状況については、「特に利用していない」が74.7%で最も高い。次いで「ISMS」が11.9%、「Ｐマーク」が10.6%となっている。

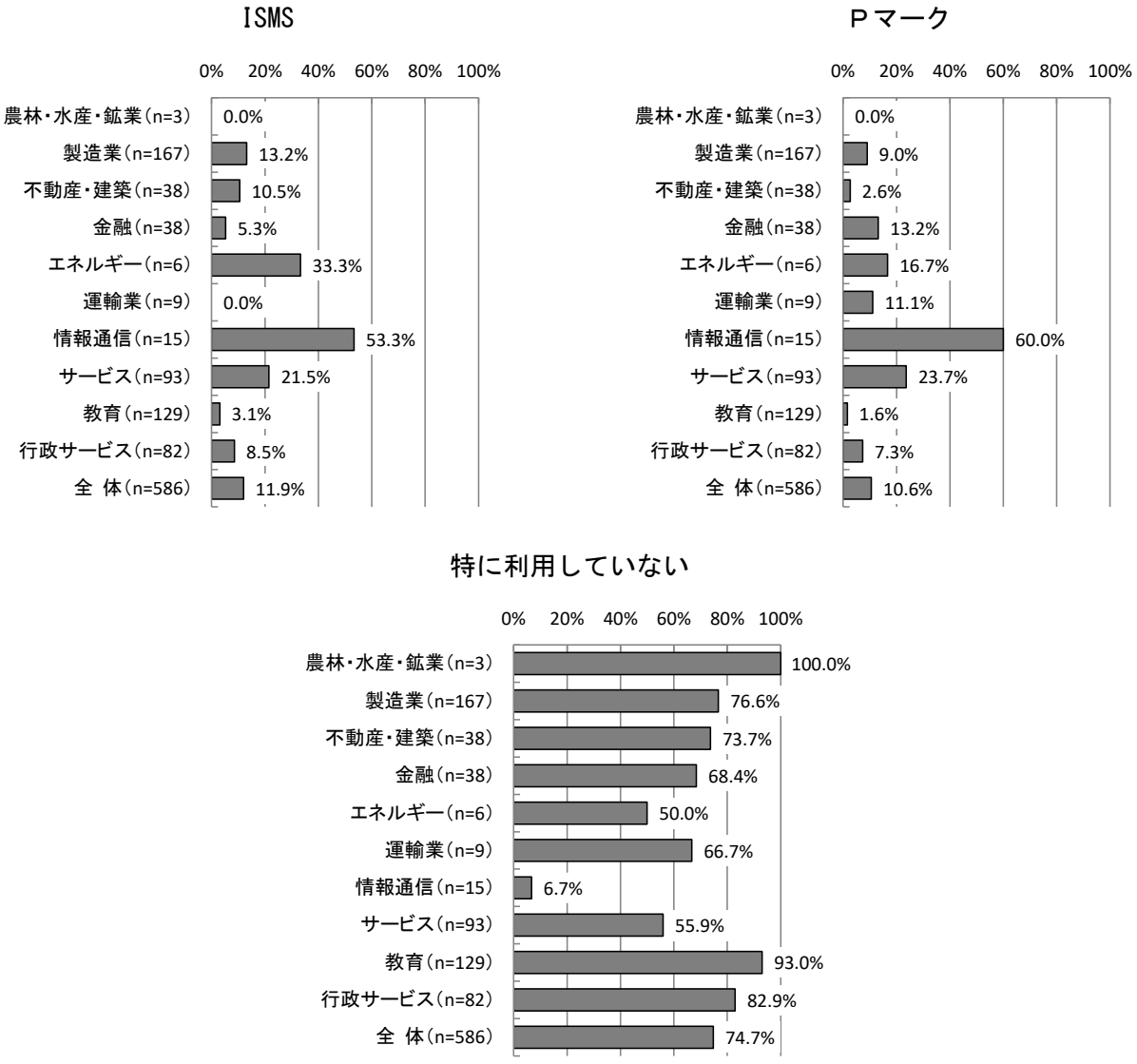
※本項目は、情報セキュリティ対策を行っている社・団体等を対象としている。

【全体】第三者機関の認証制度等の利用状況（MA, n=586）



【業種別分析】業種別にみると、「ISMS」については、「情報通信」が53.3%で高くなっている。「特に利用していない」については、「教育」で93.0%と高くなっている。

【業種別分析】第三者機関の認証制度等の利用状況

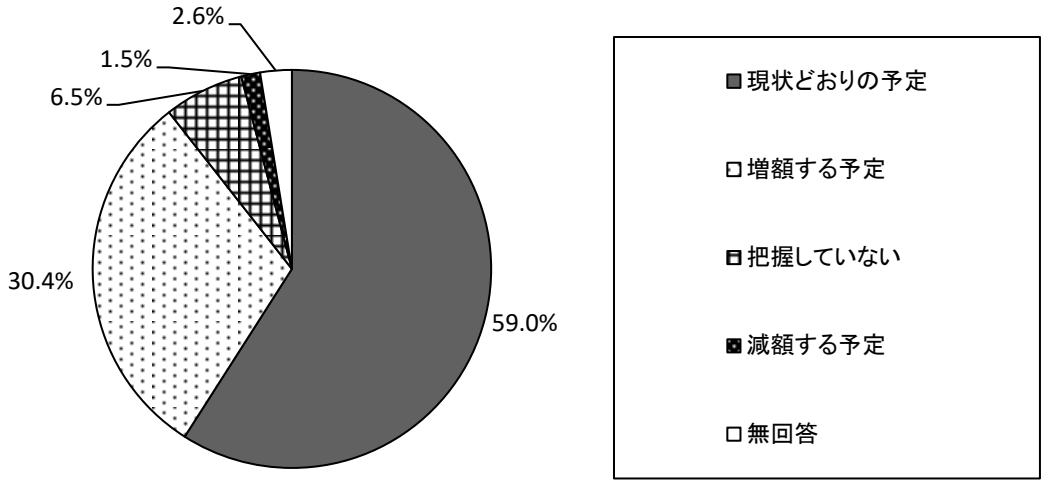


3.1.28　次年期の情報セキュリティ対策の投資計画　【問13-6】

次年期（年単位）の情報セキュリティ対策の投資計画については、「現状どおりの予定」が59.0%で最も高く、次いで「増額する予定」が30.4%となっている。これに対して「減額する予定」は1.5%とわずかな割合にとどまっている。

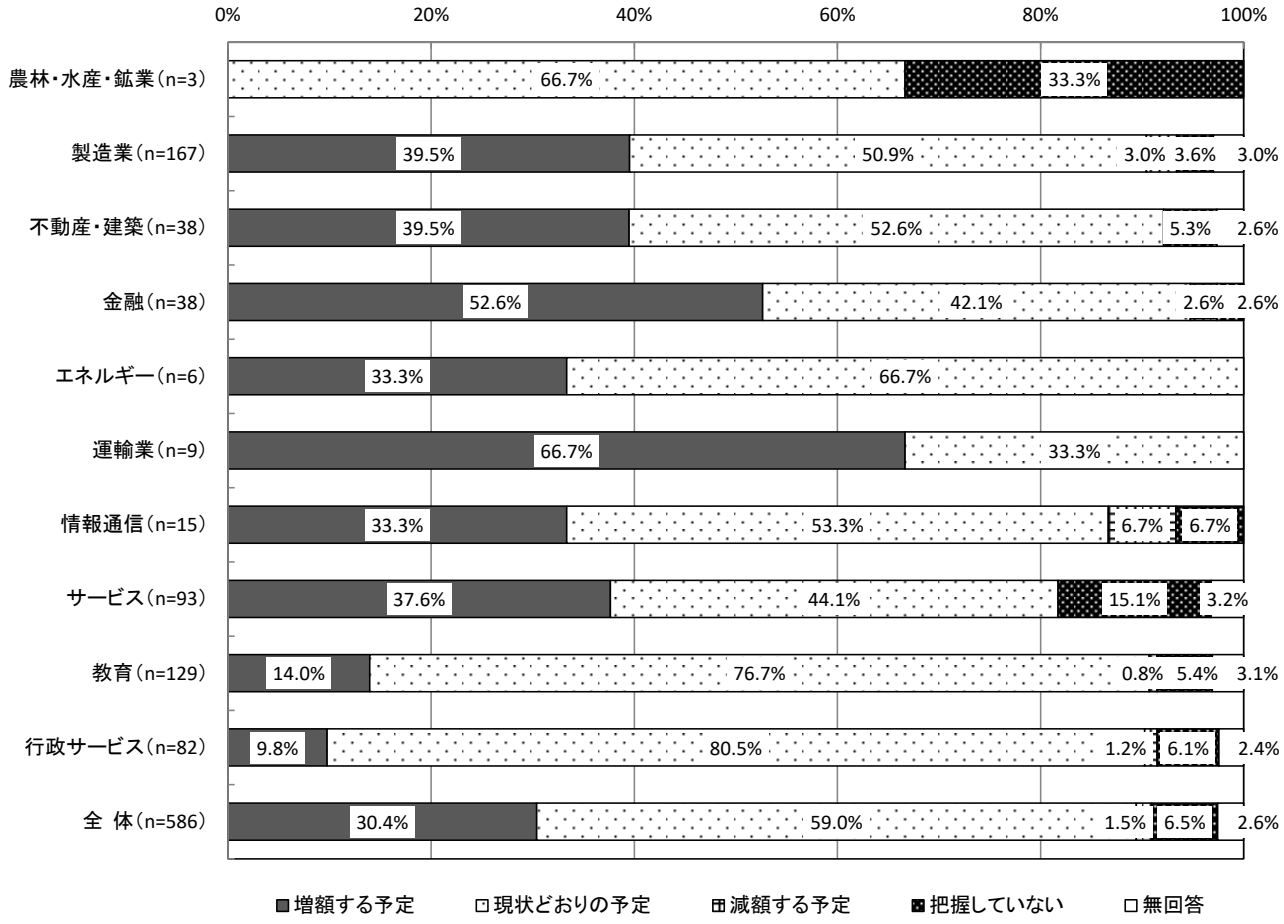
※本項目は、情報セキュリティ対策を行っている社・団体等を対象としている。

【全体】次年期の情報セキュリティ対策の投資計画（SA,n=586）



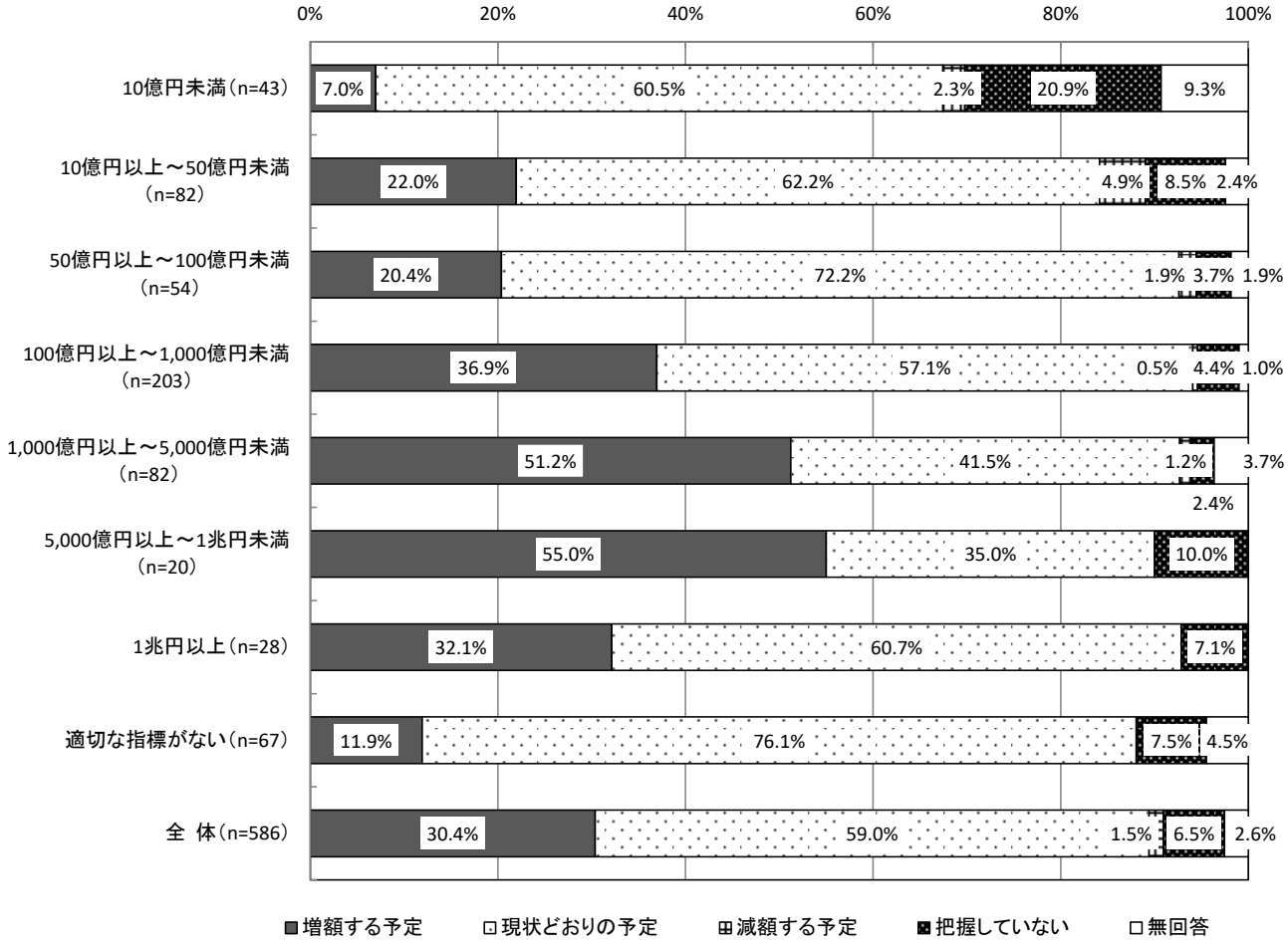
【業種別分析】業種別にみると、今期と比較して投資額を「増額する予定」については、「運輸業」が66.7%、「金融」が52.6%となっている。「現状どおりの予定」については、「行政サービス」が80.5%で最も高く、次いで「教育」が76.7%となっている。

【業種別分析】次年期の情報セキュリティ対策の投資計画



【予算規模別分析】予算規模別にみると、今期と比較して投資額を「増額する予定」については、「5,000億円以上～1兆円未満」が55.0%で最も高く、次いで「1,000億円以上～5,000億円未満」が51.2%となっている。これに対して「10億円未満」では7.0%と低くなっている。

【予算規模分析】次年期の情報セキュリティ対策の投資計画

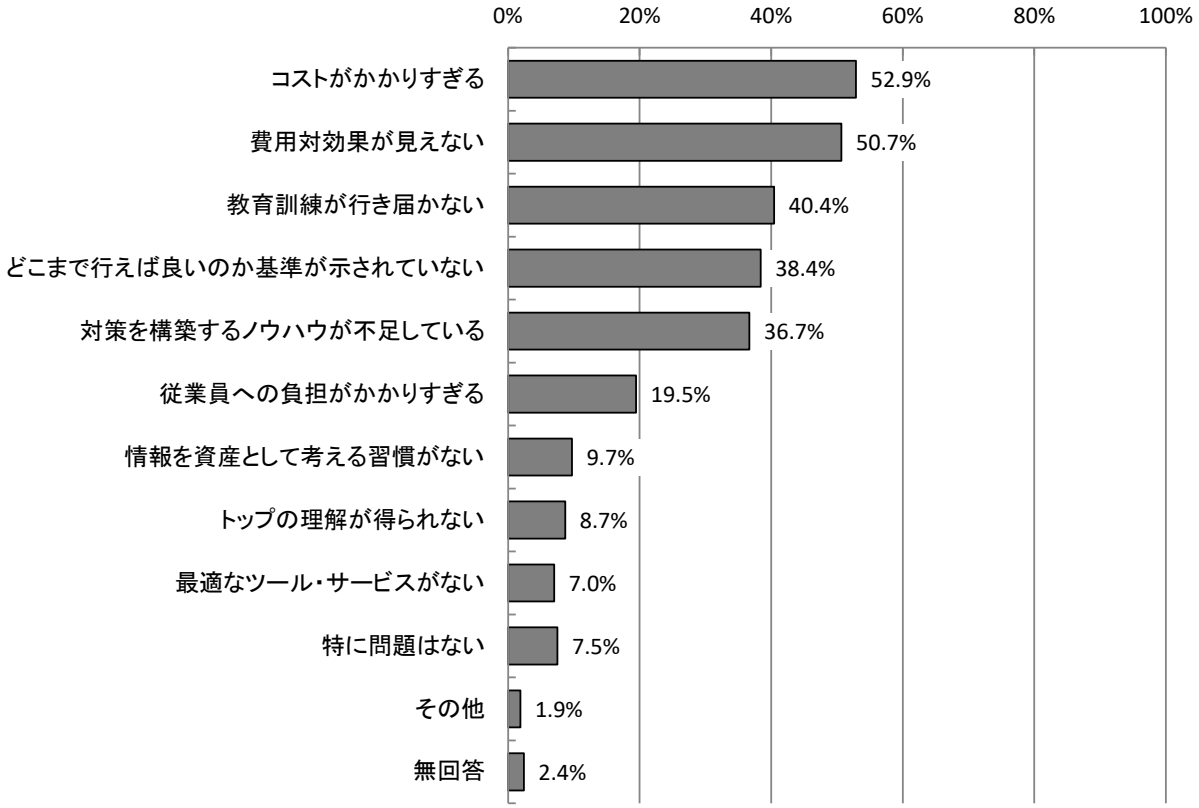


3.1.29　情報セキュリティ対策への投資に関する問題点　【問13-7】

情報セキュリティ対策への投資に関する問題点については、「コストがかかりすぎる」が52.9%、「費用対効果が見えない」が50.7%で高く、過半数となっている。次いで「教育訓練が行き届かない」が40.4%、「どこまで行えば良いのか基準が示されていない」が38.4%、「対策を構築するノウハウが不足している」が36.7%となっている。

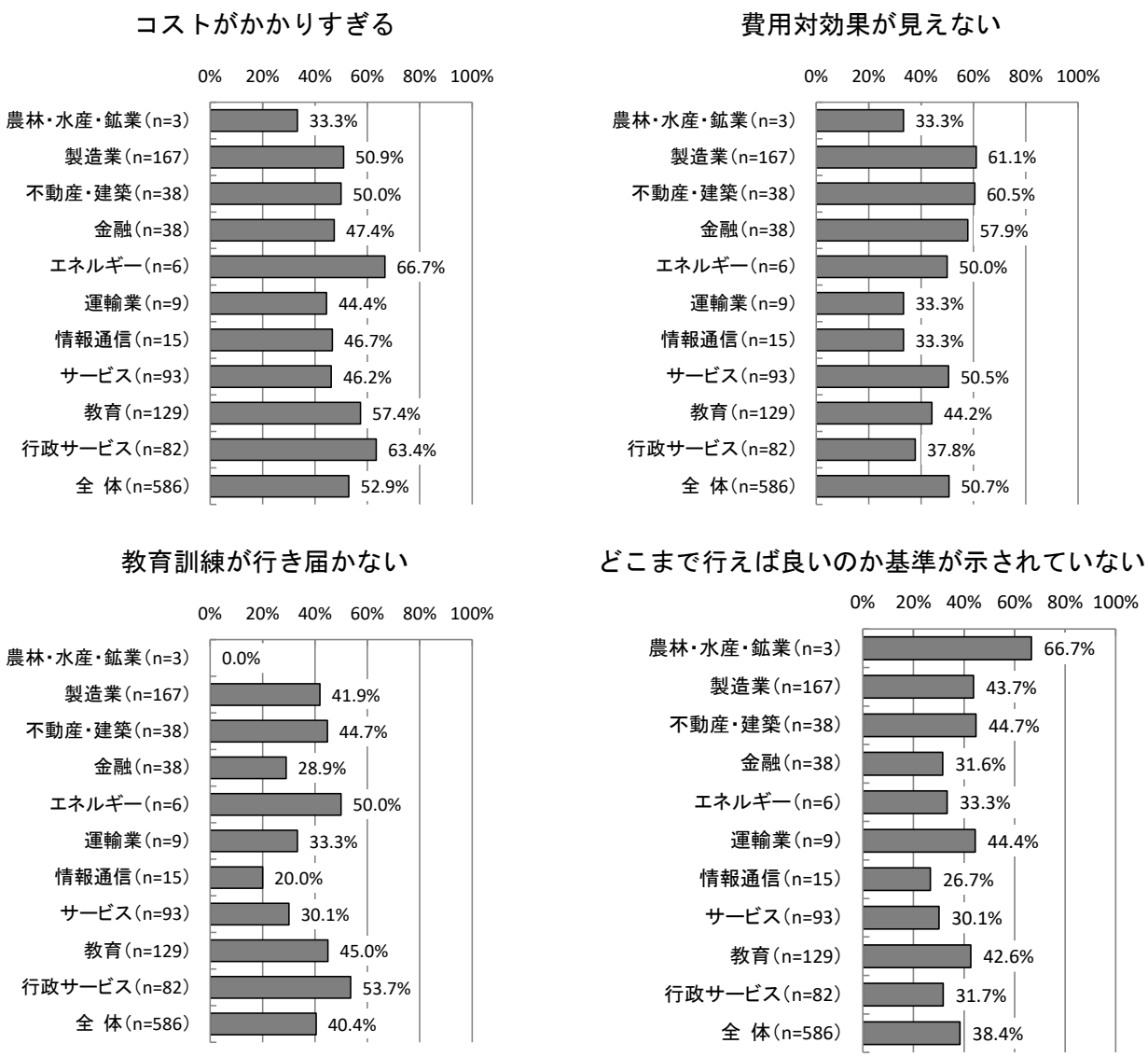
※本項目は、情報セキュリティ対策を行っている社・団体等を対象としている。

【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=586）



【業種別分析】業種別にみると、「コストがかかりすぎる」については、「エネルギー」が66.7%、「行政サービス」が63.4%で高くなっている。「費用対効果が見えない」については、「製造業」が61.1%、「不動産・建築」が60.5%で高い。「教育訓練が行き届かない」については、「行政サービス」が53.7%、「エネルギー」が50.0%で高く、「どこまで行えば良いのか基準が示されていない」では、「不動産・建築」が44.7%、「運輸業」が44.4%で高くなっている。

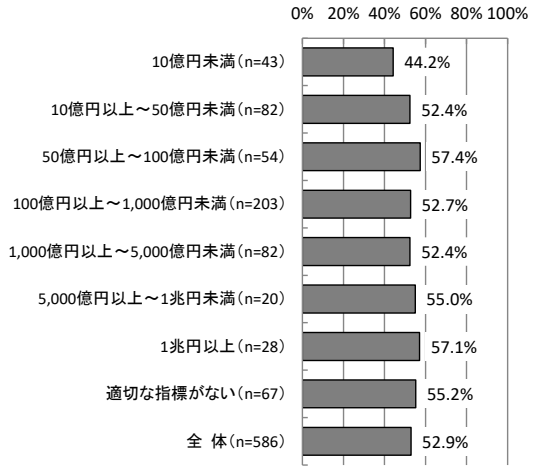
【業種別分析】情報セキュリティ対策への投資に関する問題点



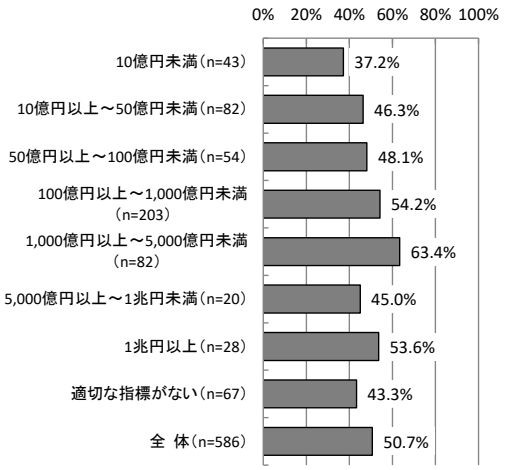
【売上・予算規模別分析】売上・予算規模別にみると、「コストがかかりすぎる」については、「50億円以上～100億円未満」が57.4%で最も高く、次いで「1兆円以上」が57.1%となっている。「費用対効果が見えない」については、「1,000億円以上～5,000億円未満」が63.4%で高い。「教育訓練が行き届かない」については、「50億円以上～100億円未満」が59.3%で最も高くなっている。

【売上・予算規模別分析】情報セキュリティ対策への投資に関する問題点

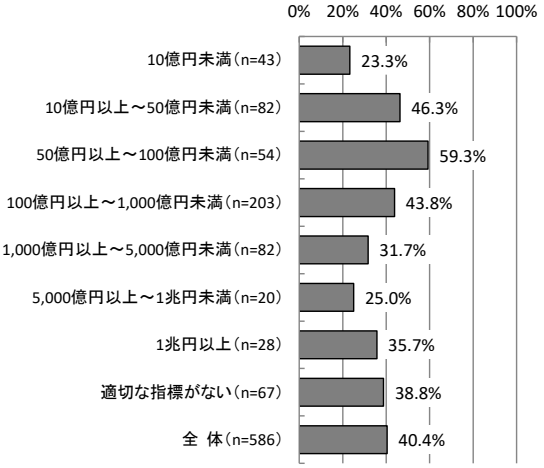
コストがかかりすぎる



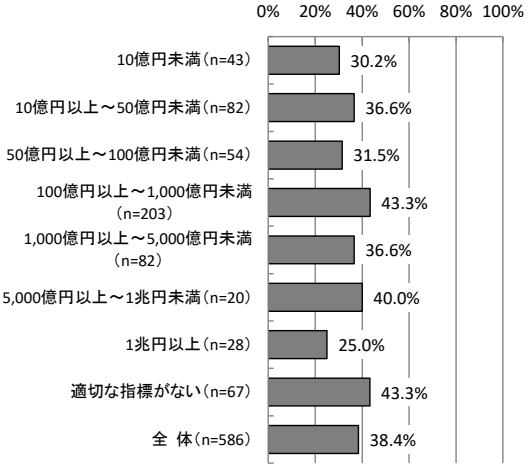
費用対効果が見えない



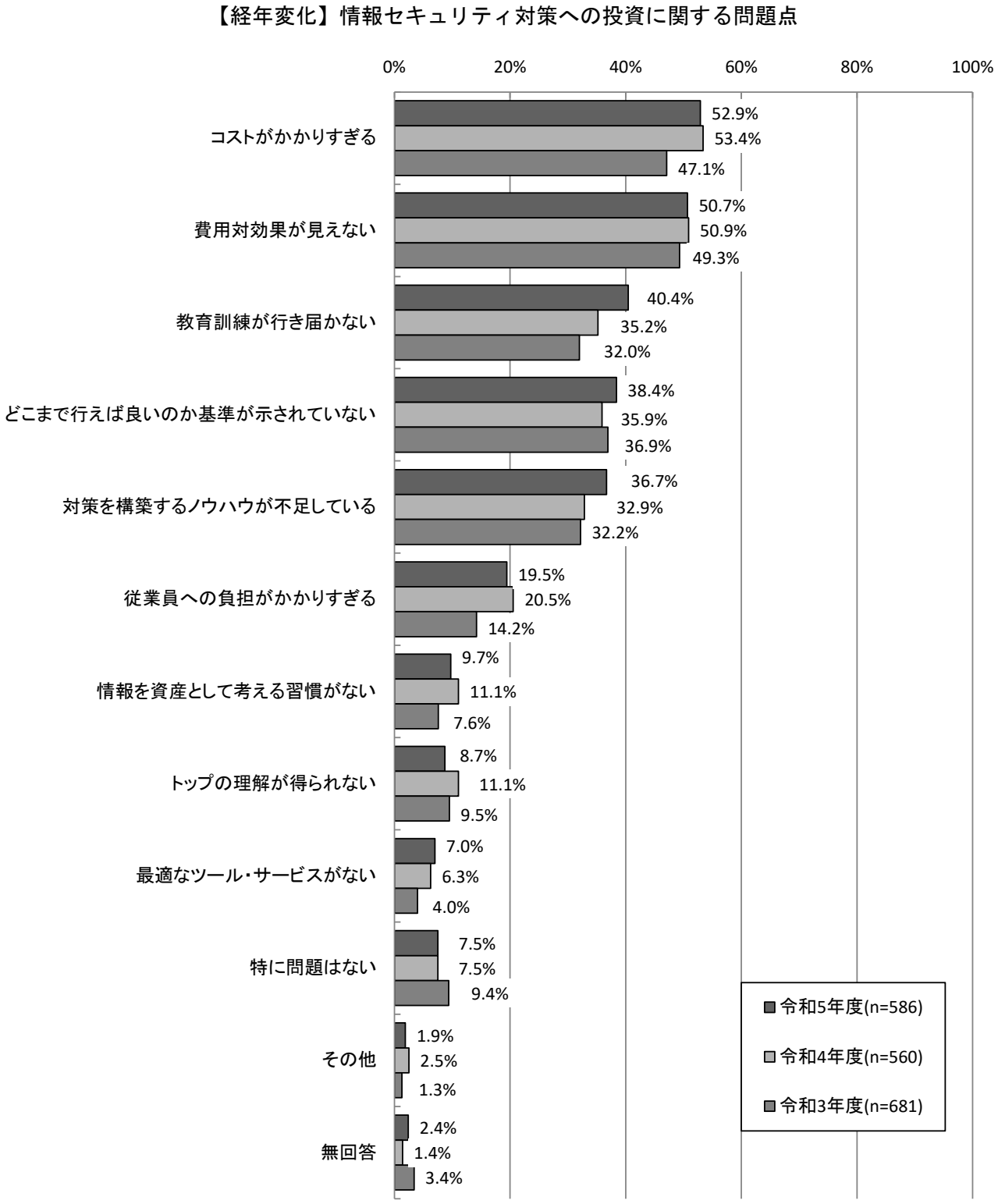
教育訓練が行き届かない



どこまで行えば良いのか基準が示されていない



【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5.2ポイント、「対策を構築するノウハウが不足している」が3.8ポイント増加している。一方、「トップの理解が得られない」が2.4ポイント減少している。

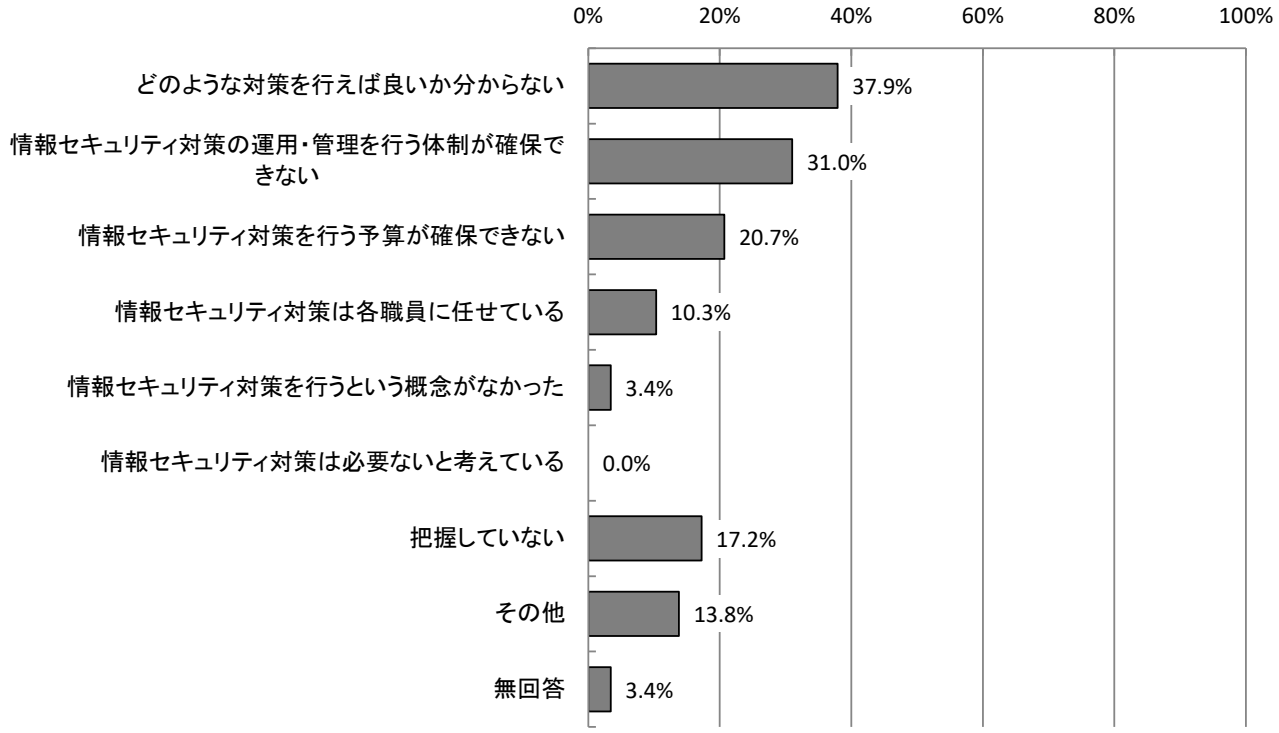


3.1.30　情報セキュリティ対策を行っていない理由　【問13-8】

情報セキュリティ対策を行っていない理由については、「どのような対策を行えば良いか分からない」が37.9%で最も高く、次いで「情報セキュリティ対策の運用・管理を行う体制が確保できない」が31.0%となっている。

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

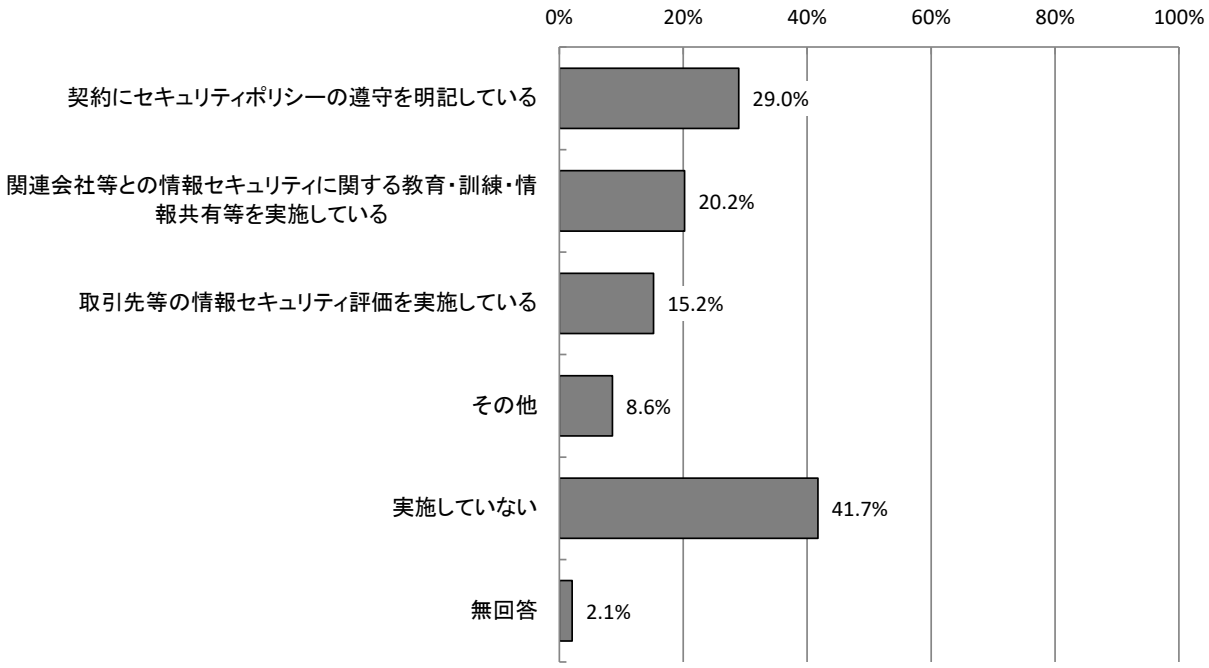
【全体】情報セキュリティ対策を行っていない理由（MA,n=29）



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

サプライチェーンリスク対策については「契約にセキュリティポリシーの遵守を明記している」が29.0%と高く、次いで「関連会社等との情報セキュリティに関する教育・訓練・情報共有等を実施している」が20.2%となっている。

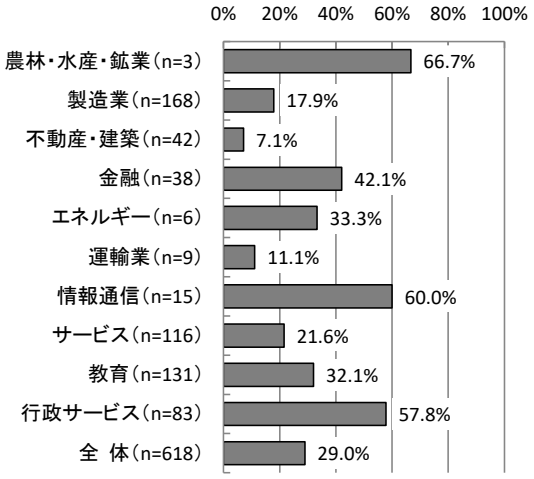
【全体】サプライチェーンリスク対策として対策を行っているか（MA, n=618）



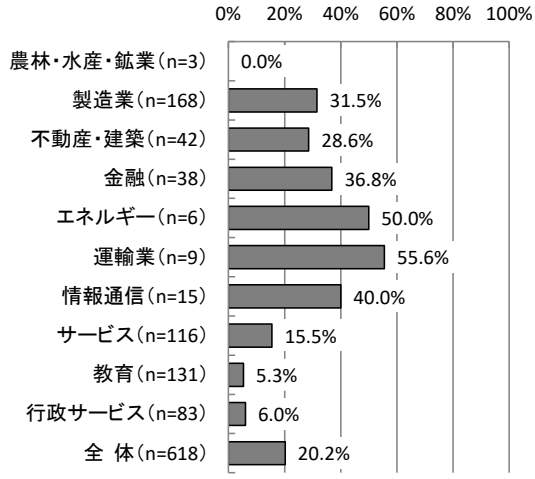
【業種別分析】業種別では、「契約にセキュリティポリシーの遵守を明記している」は「情報通信」が60.0%、「行政サービス」が57.8%で高くなっている。一方、「不動産・建築」は7.1%で最も低くなっている。

【業種別分析】サプライチェーンリスク対策として対策を行っているか

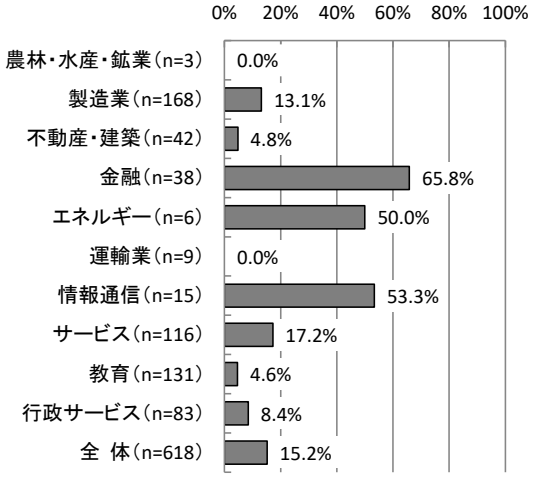
契約にセキュリティポリシーの遵守を明記している



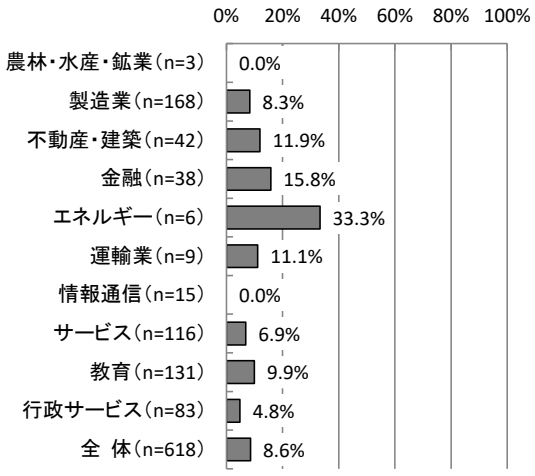
関連会社等との情報セキュリティに関する教育・訓練・情報共有等を実施している



取引先等の情報セキュリティ評価を実施している



実施していない



3.1.32 情報セキュリティ対策に関する考え方 【問15】

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

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

調査対象とした基本的な考え方と相対する2つの考え

①として提示した考え方	②として提示した考え方
1. 投資方針	
セキュリティ投資は必要最低限に抑えるべきである。	来るべき問題事案に備えて、積極的に投資を行うべきである。
2. 事後的対応と予防的対応	
情報セキュリティ対策としては、問題発生に対しての応急対応や、再発防止・被害拡大防止に注力すべきである。	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することに加え、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。	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	
業務実態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に抑えるべきである」に近いとする割合が24.1%、「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73.9%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49.8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べきである」に近いとする割合が21.2%、「②情報セキュリティ対策としては、リスクの検知など、予防上の対策に注力すべきである」に近いとする割合が76.8%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55.6ポイントと大幅に上回っている。

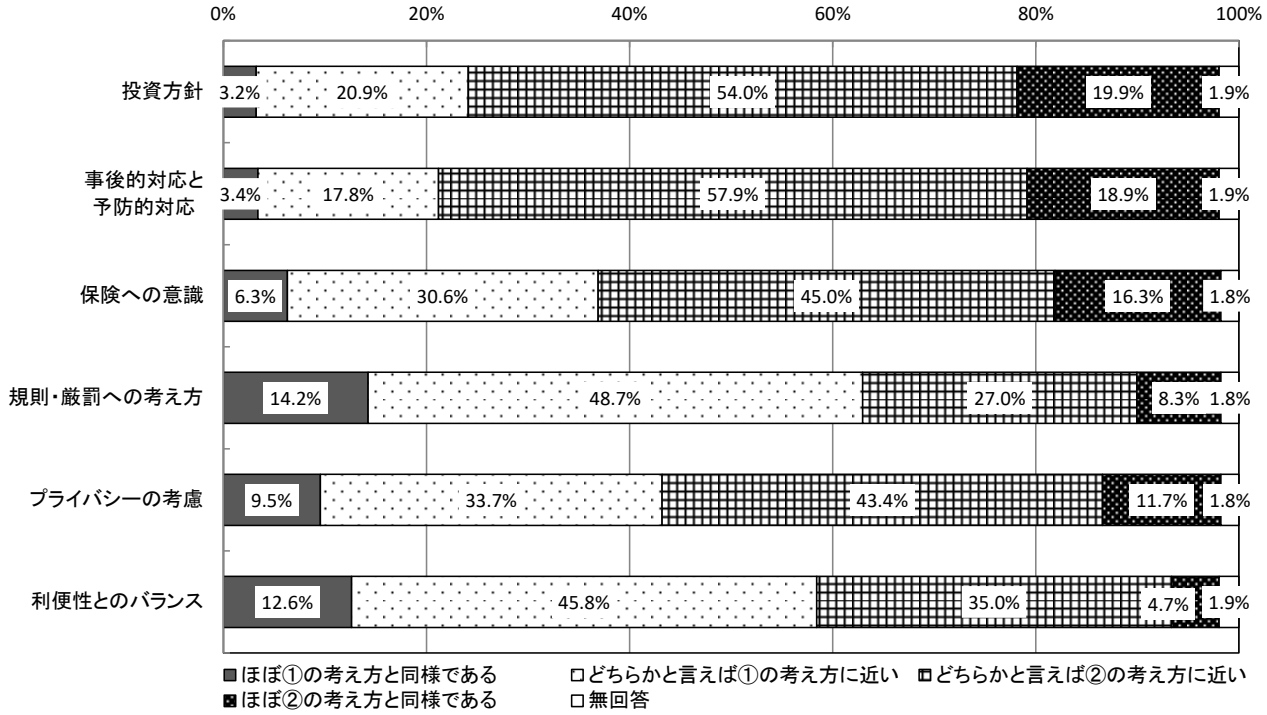
「保険への意識」については、「①情報セキュリティ対策としては、人的・技術的な対策によりカバーできるところを対策すれば十分である」に近いとする割合が36.9%、「②情報セキュリティ対策としては、人的・技術的対策によりカバーすることに加え、保険によりまかなうべきである」に近いとする割合が61.3%で、「保険的な対応が必要」とする割合が「人的・技術的な対策で十分」を24.4ポイント上回っている。

「規制・罰則への考え方」については、「①技術以外の面での対策としては、従業員等への教育と、適切な情報提供により対策を促すことが重要である」に近いとする割合が62.9%、「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35.3%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27.6ポイント上回っている。

「プライバシーの考慮」については、「①職場とはいえ、従業員等のプライバシーは保護された上で、情報セキュリティ対策は行われるべきである」に近いとする割合が43.2%、「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保護の制約はやむをえない」に近いとする割合が55.1%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11.9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業務実態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58.4%、「②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」とする39.7%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18.7ポイント上回っている。

【全体】情報セキュリティ対策に関する考え方（SA,n=618）



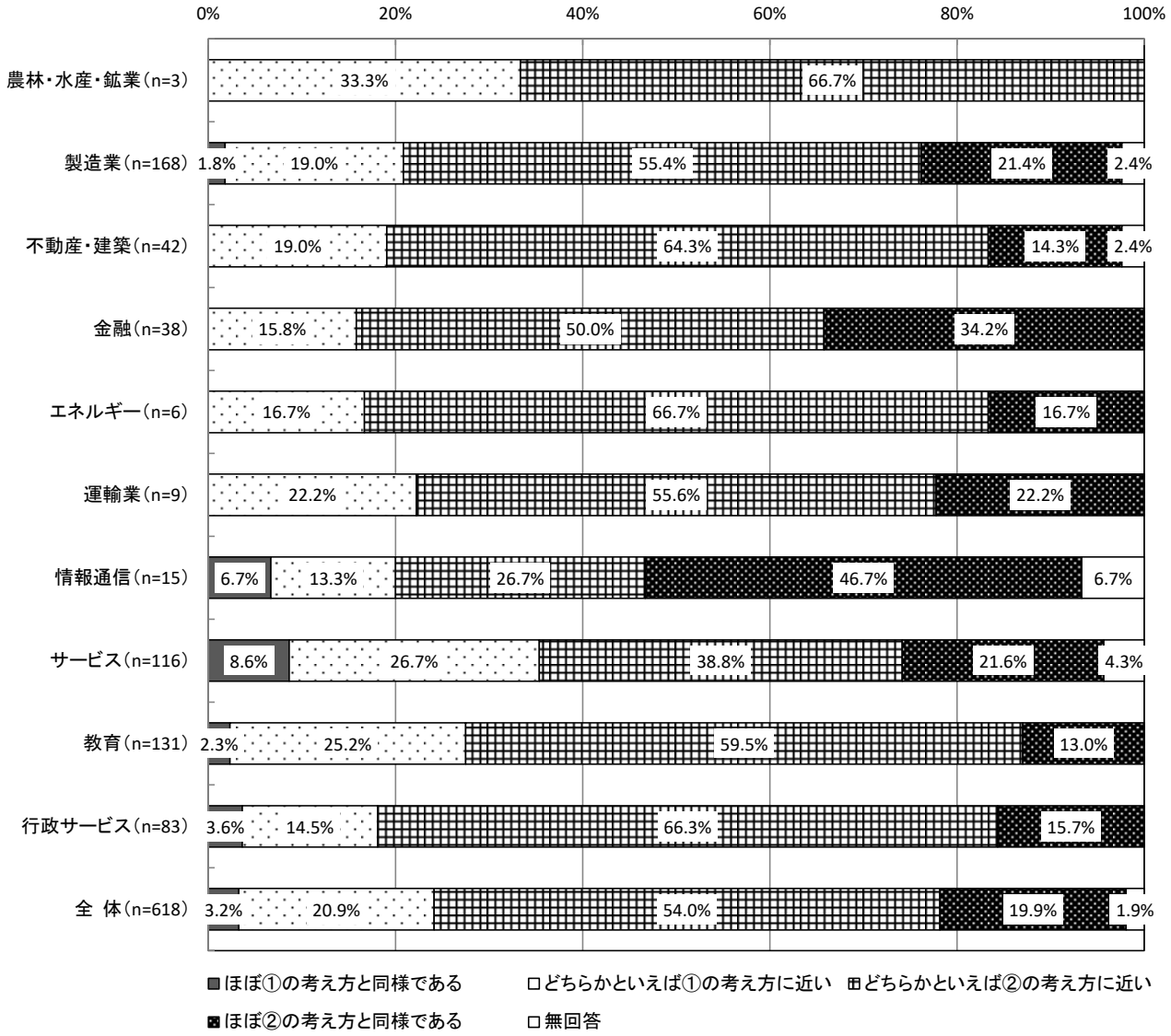
3.1.33　投資に関する考え方　【問15-1】

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

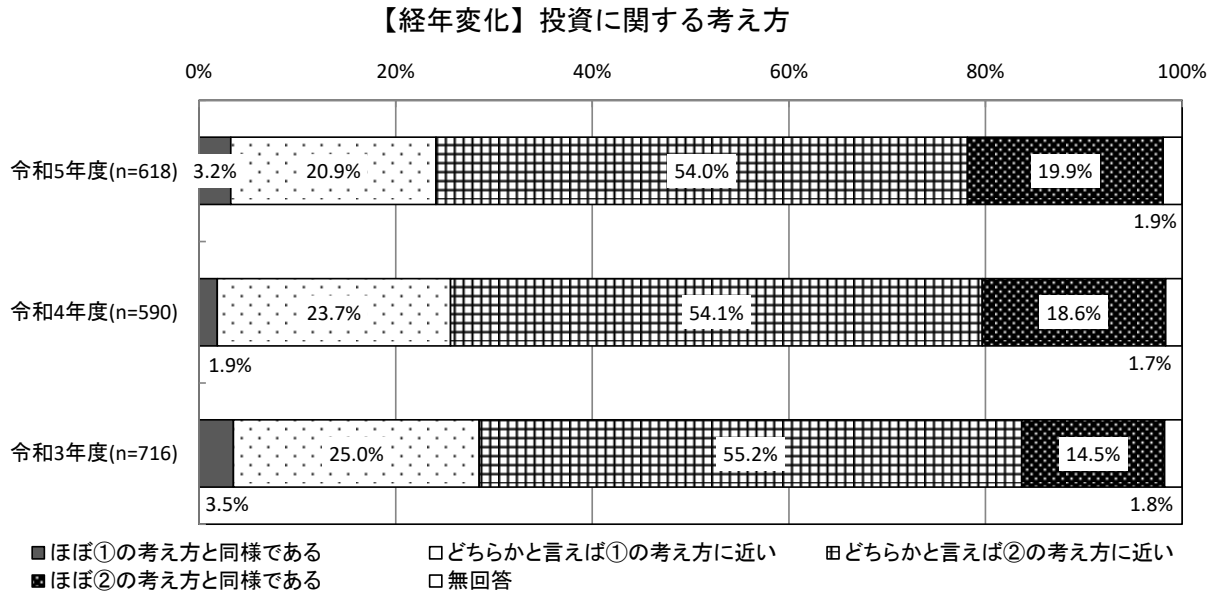
①として提示した考え方	②として提示した考え方
セキュリティ投資は必要最低限に抑えるべきである。	来るべき問題事案に備えて、積極的に投資を行うべきである。

【業種別分析】業種別にみると、投資方針に関して全ての業種で、「②積極的投資」の割合が多く、特に「金融」が84.2%、「行政サービス」が82.0%と高くなっている。

【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1.5ポイントの減少、「②積極的投資」は1.2ポイントの増加となっている。



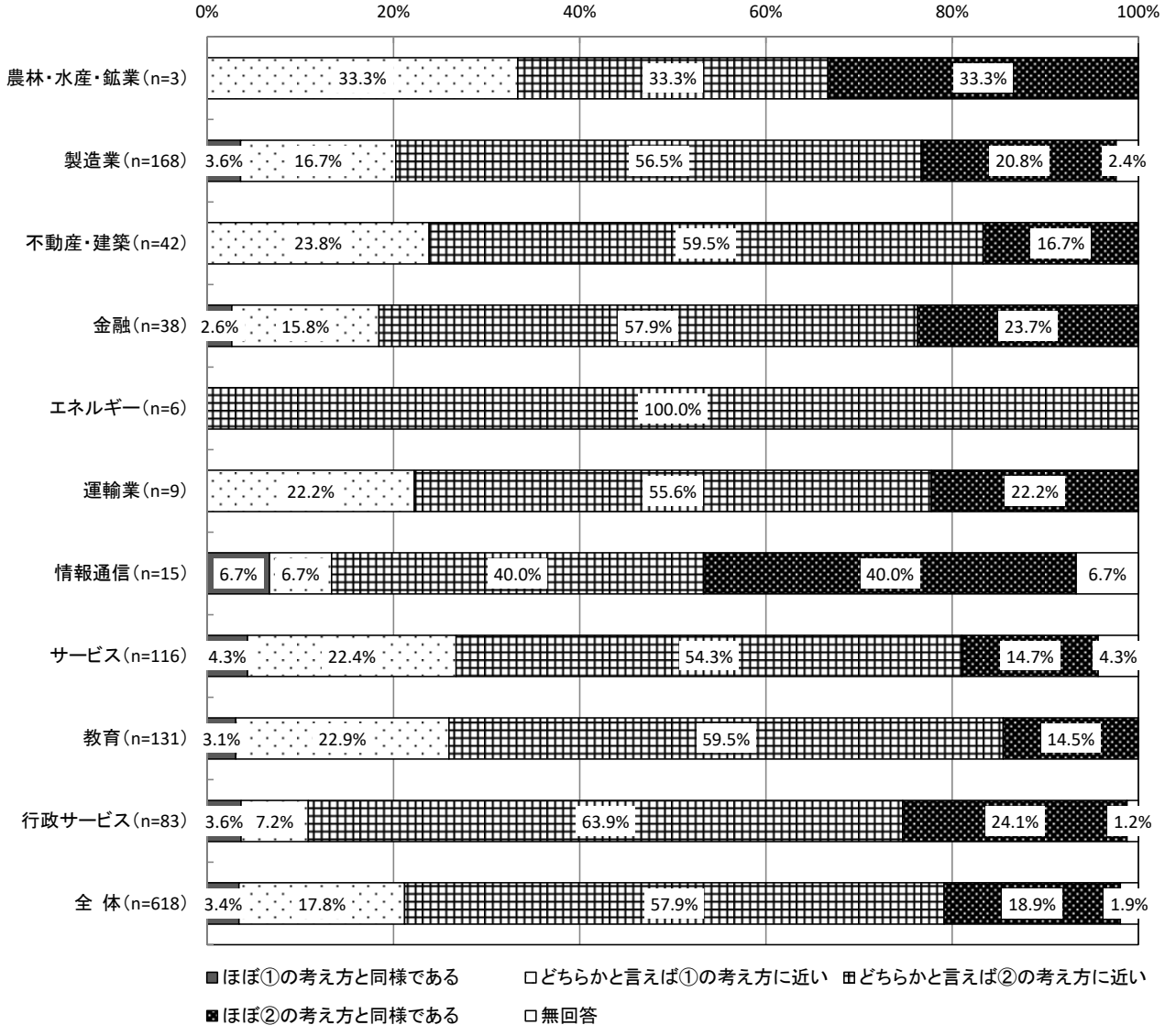
3.1.34　事後的対応と予防的対応に関する考え方　【問15-2】

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

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

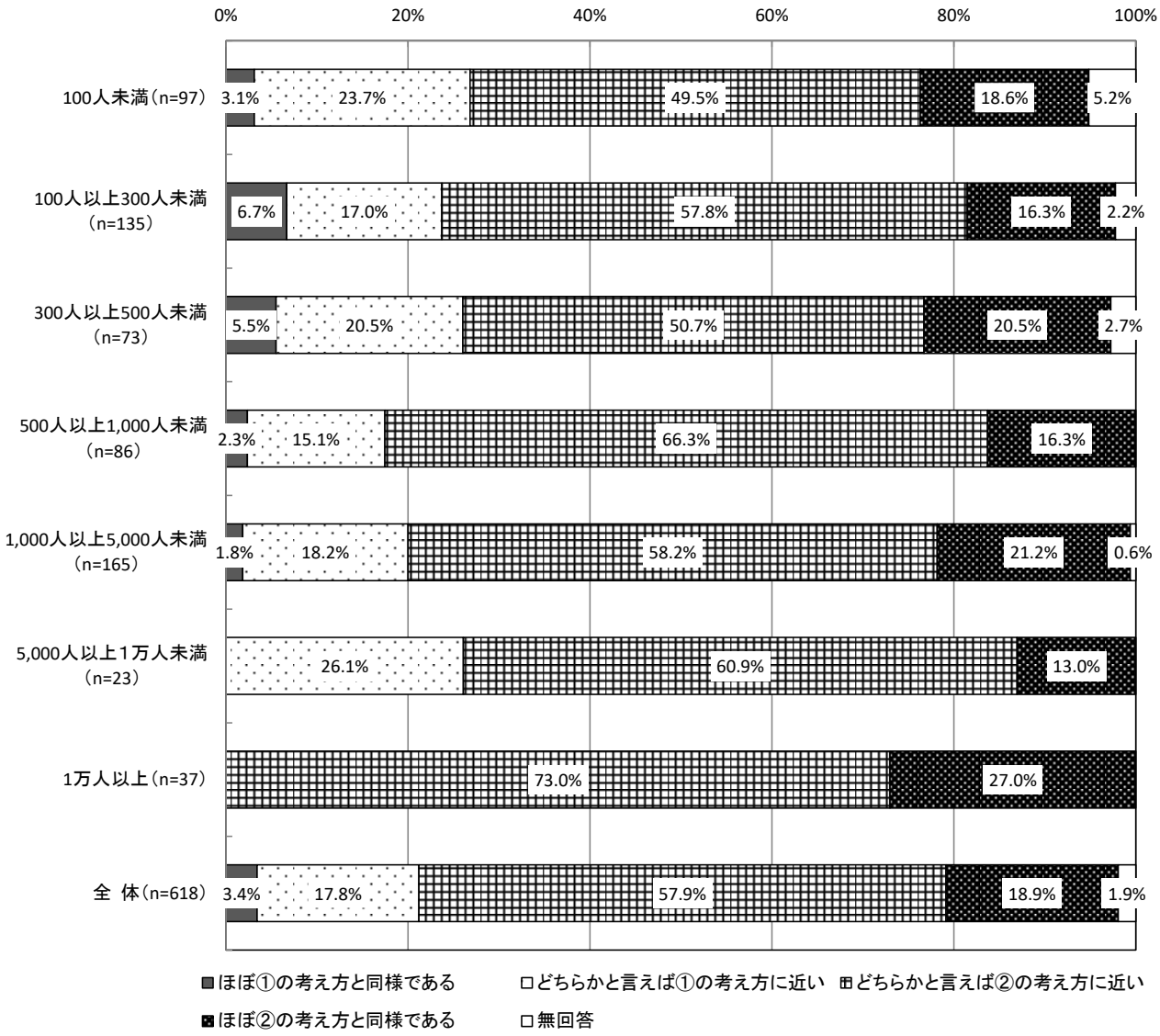
【業種別分析】業種別にみると、全ての業種で「②予防的対応」の割合が多く、「エネルギー」が100%、「行政サービス」が88.0%、「金融」が81.6%と高くなっている。

【業種別分析】事後的対応と予防的対応に関する考え方

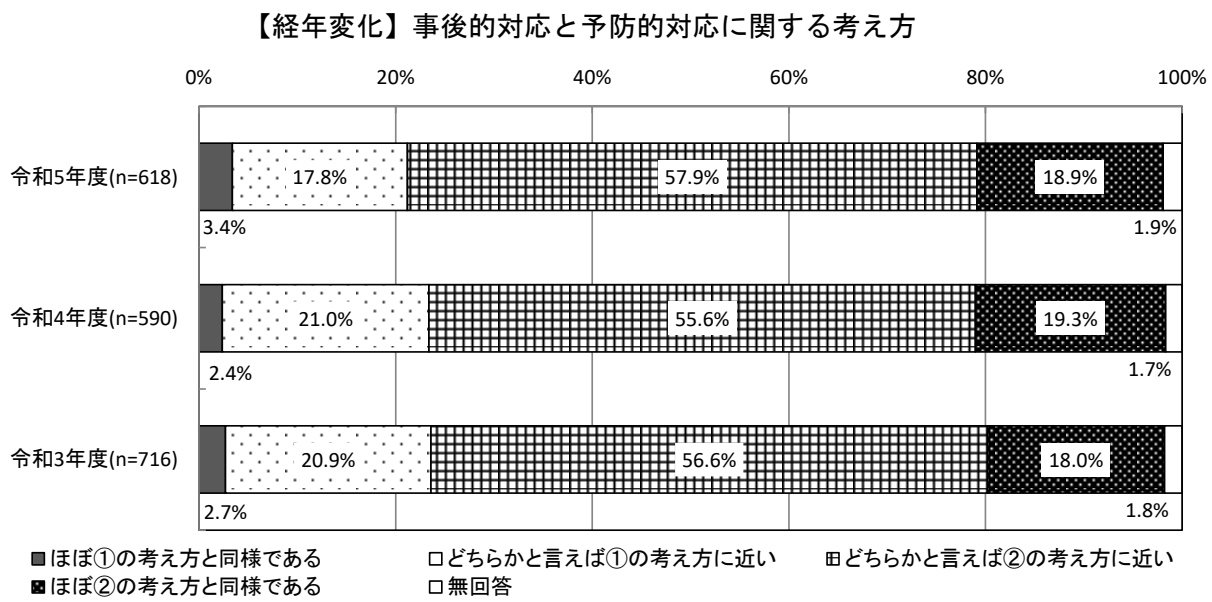


【従業員規模別分析】従業員規模別にみると、全ての従業員規模で「②予防的対応」が「①問題発生への適切な対応」を上回っている。

【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2.2ポイントの減少、「②予防的対応」は1.9ポイントの増加となっている。



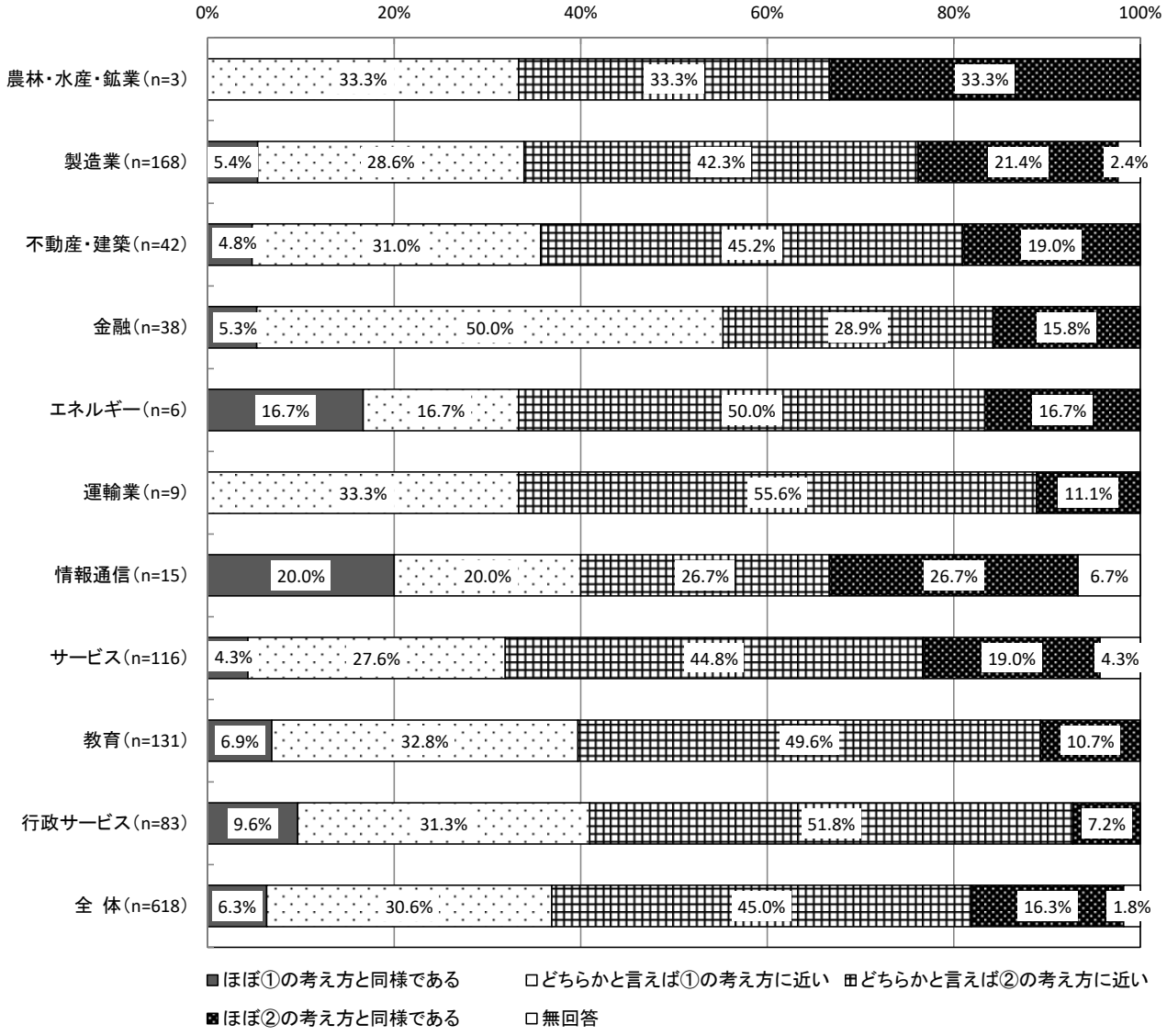
3.1.35　保険への意識　【問15-3】

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

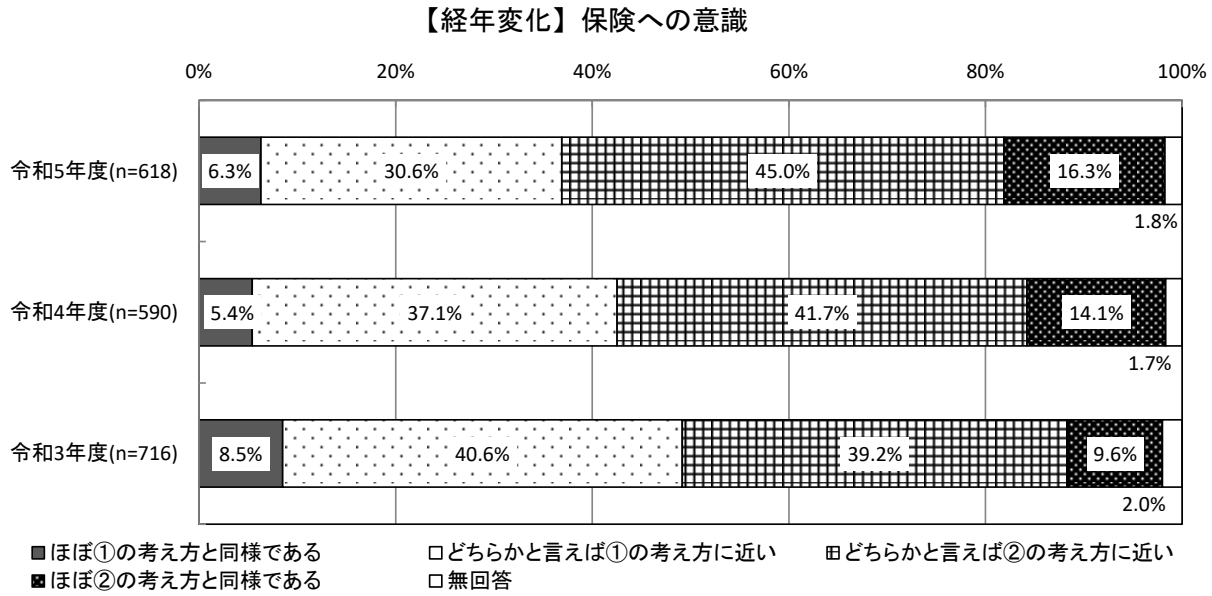
①として提示した考え方	②として提示した考え方
情報セキュリティ対策としては、人的・技術的な対策により カバーできるところを対策すれば十分である。	情報セキュリティ対策としては、人的・技術的対策により カバーすることに加え、保険によりまかなうべきである。

【業種別分析】業種別にみると、「金融」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、55.3%と高い。一方、この他の業種では「②保険的な対応が必要」が「①人的・技術的な対策で十分」を上回っている。

【業種別分析】保険への意識



【経年変化】昨年度と比較すると、「①人的・技術的な対策で十分」は5.6ポイントの減少となり、「②保険的な対応が必要」は5.5ポイントの増加となっている。



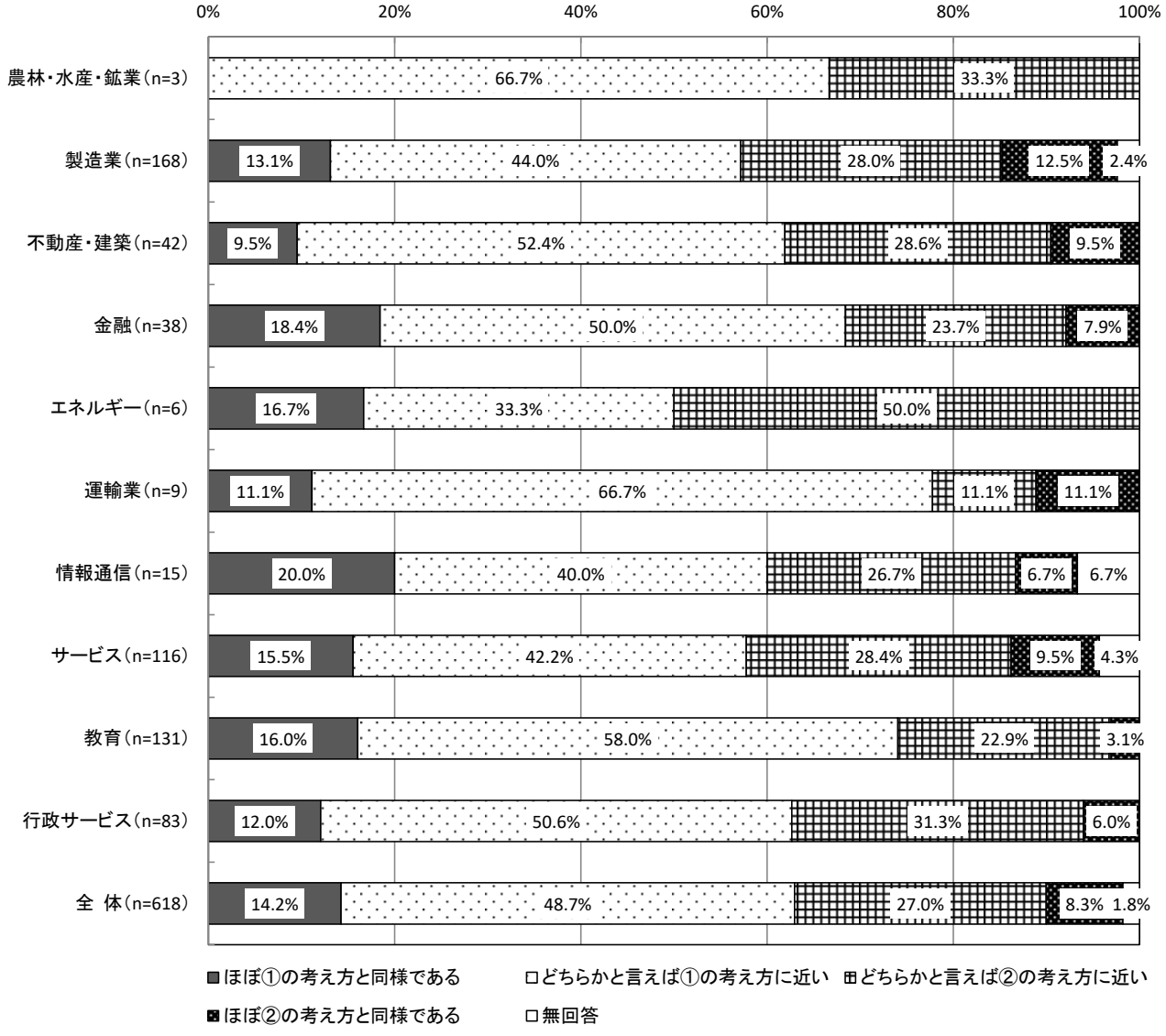
3.1.36　規制・罰則への考え方　【問15-4】

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

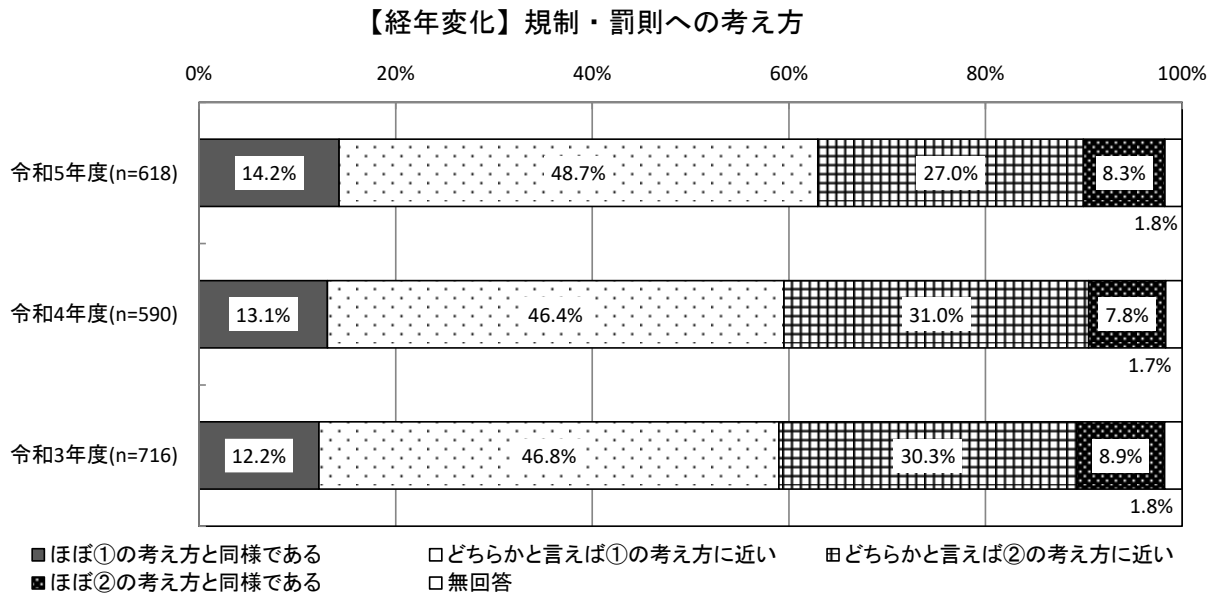
①として提示した考え方	②として提示した考え方
技術以外の面での対策としては、従業員等への教育と、適切な情報提供により対策を促すことが重要である。	技術以外の面での対策としては、教育はもちろんのこと、規制・罰則などの強制力のある制度的対応を行うことが重要である。

【業種別分析】業種別にみると、「エネルギー」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「運輸業」では「①教育と情報提供を中心とした対応」が55.6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3.4ポイントの増加、「②規則・罰則も含む強制力のある対応」は3.5ポイントの減少となっている。



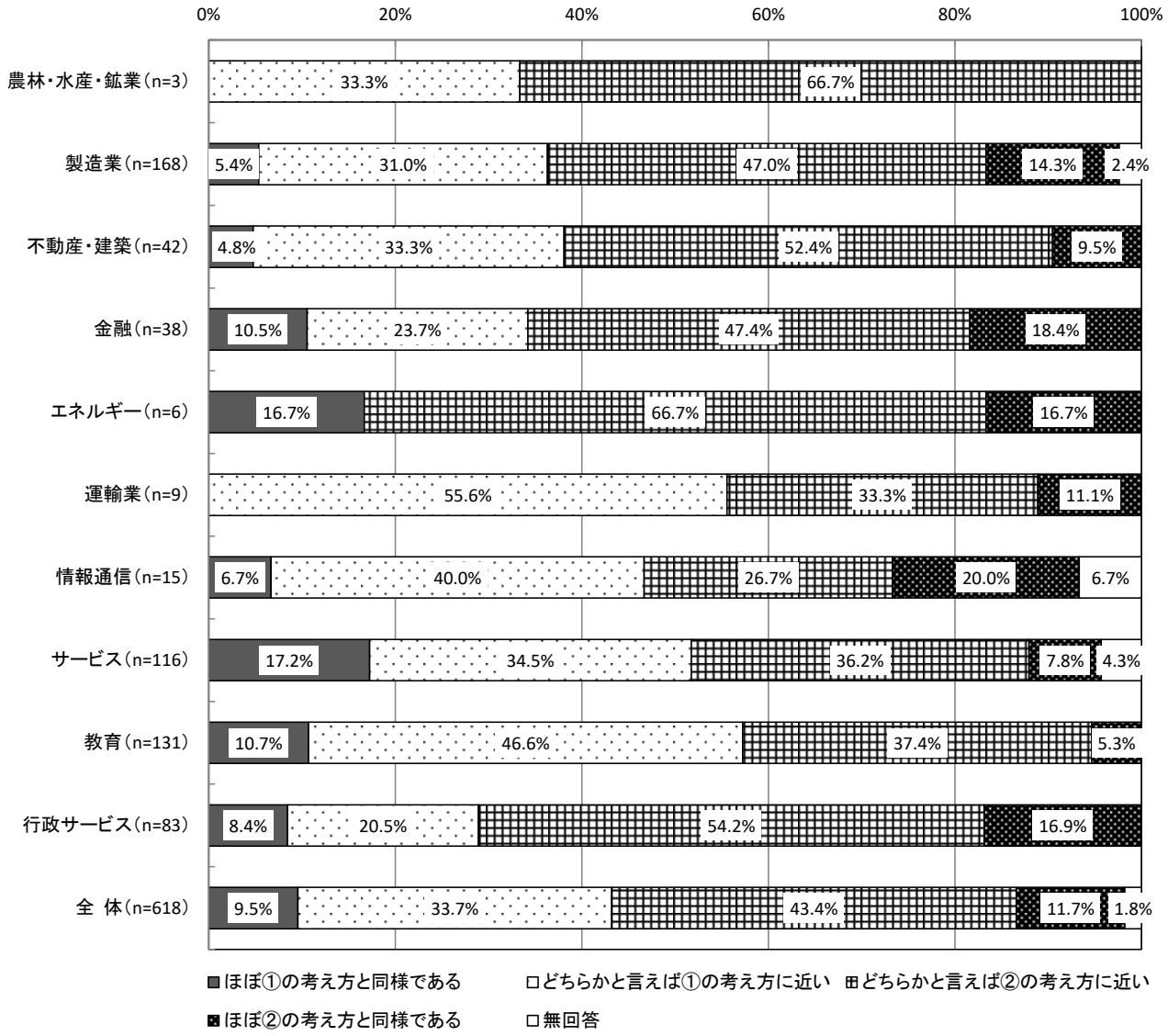
3.1.37　プライバシーの考慮に関する考え方　【問15-5】

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

①として提示した考え方	②として提示した考え方
職場とはいえ、従業員等のプライバシーは保護された上で、情報セキュリティ対策は行われるべきである。	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。

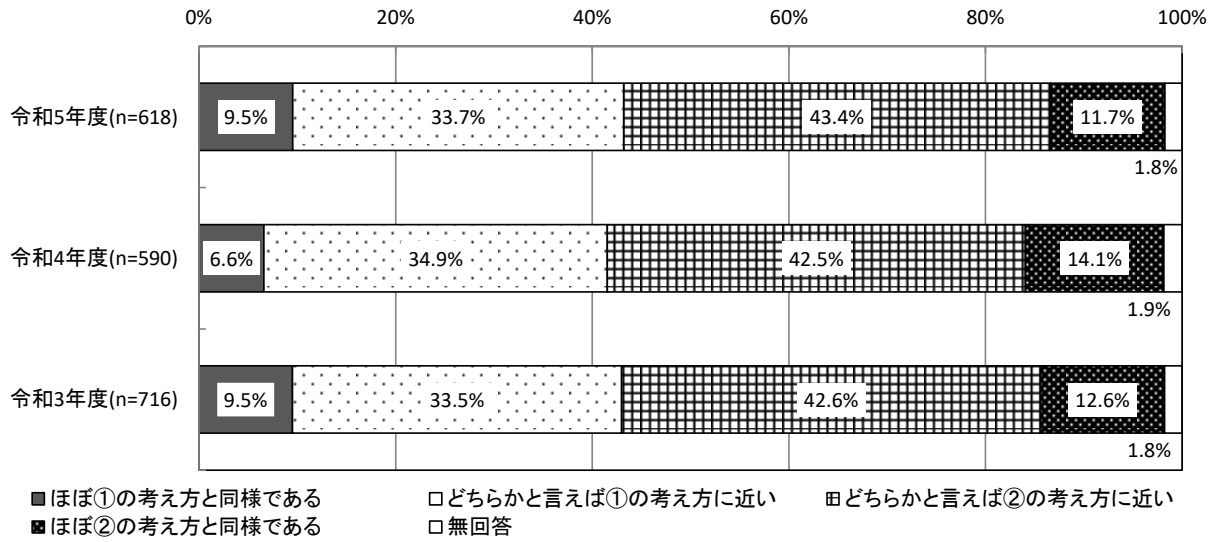
【業種別分析】業種別を見ると、「運輸業」「サービス」「教育」を除くすべての業種で「②プライバシー保護の制約はやむをえない」が「①プライバシーはある程度考慮すべき」を上回っている。特に「エネルギー」で66.7ポイント「②プライバシー保護の制約はやむをえない」が多くなっている。

【業種別分析】プライバシーの考慮に関する考え方



【経年変化】昨年度と比較すると、「①プライバシーはある程度考慮すべき」は1.7ポイントの増加、「②プライバシー保護の制約はやむをえない」は1.5ポイントの減少となっている。

【経年変化】プライバシーの考慮に関する考え方



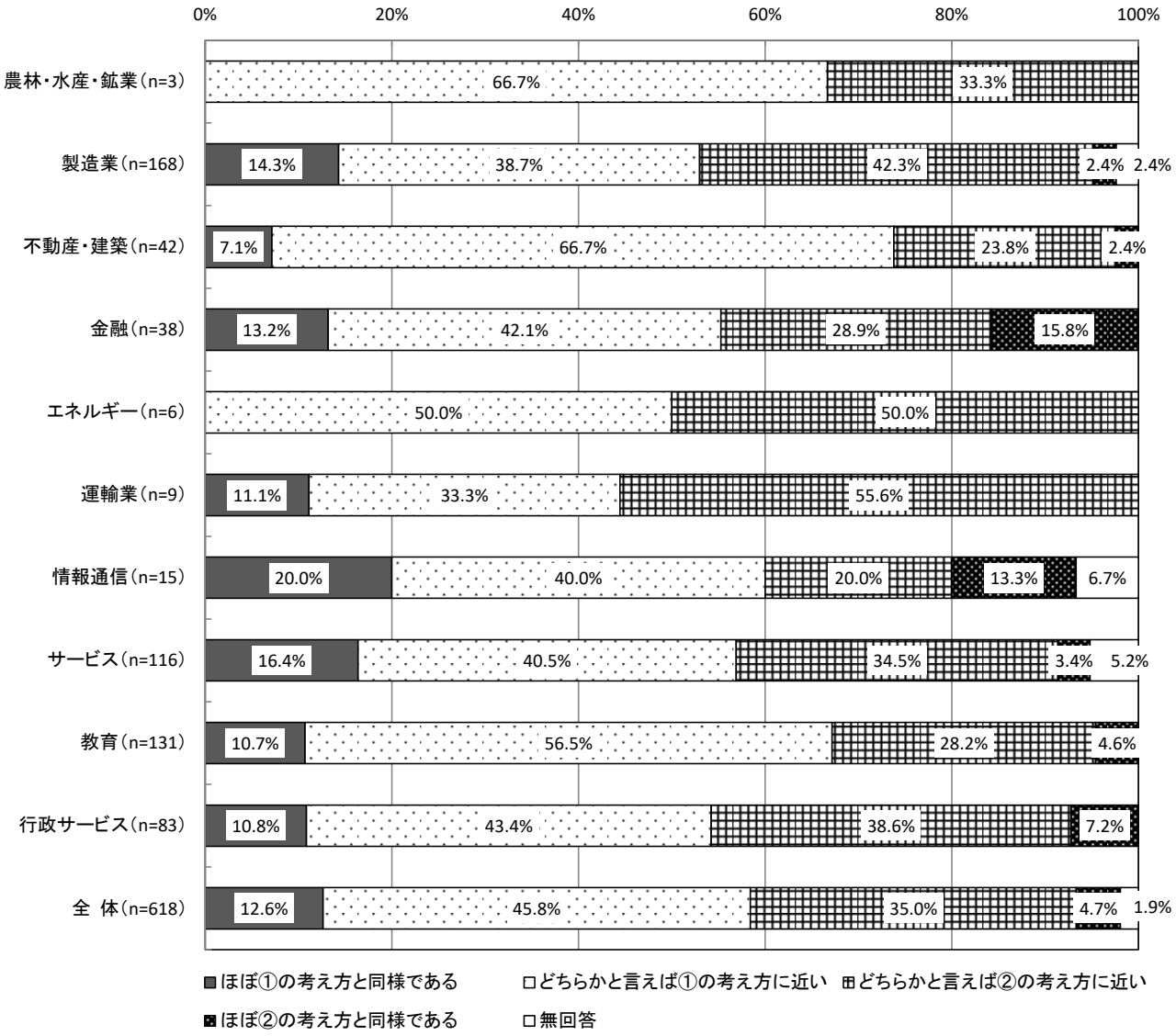
3.1.38　利便性とのバランスに関する考え方　【問15-6】

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

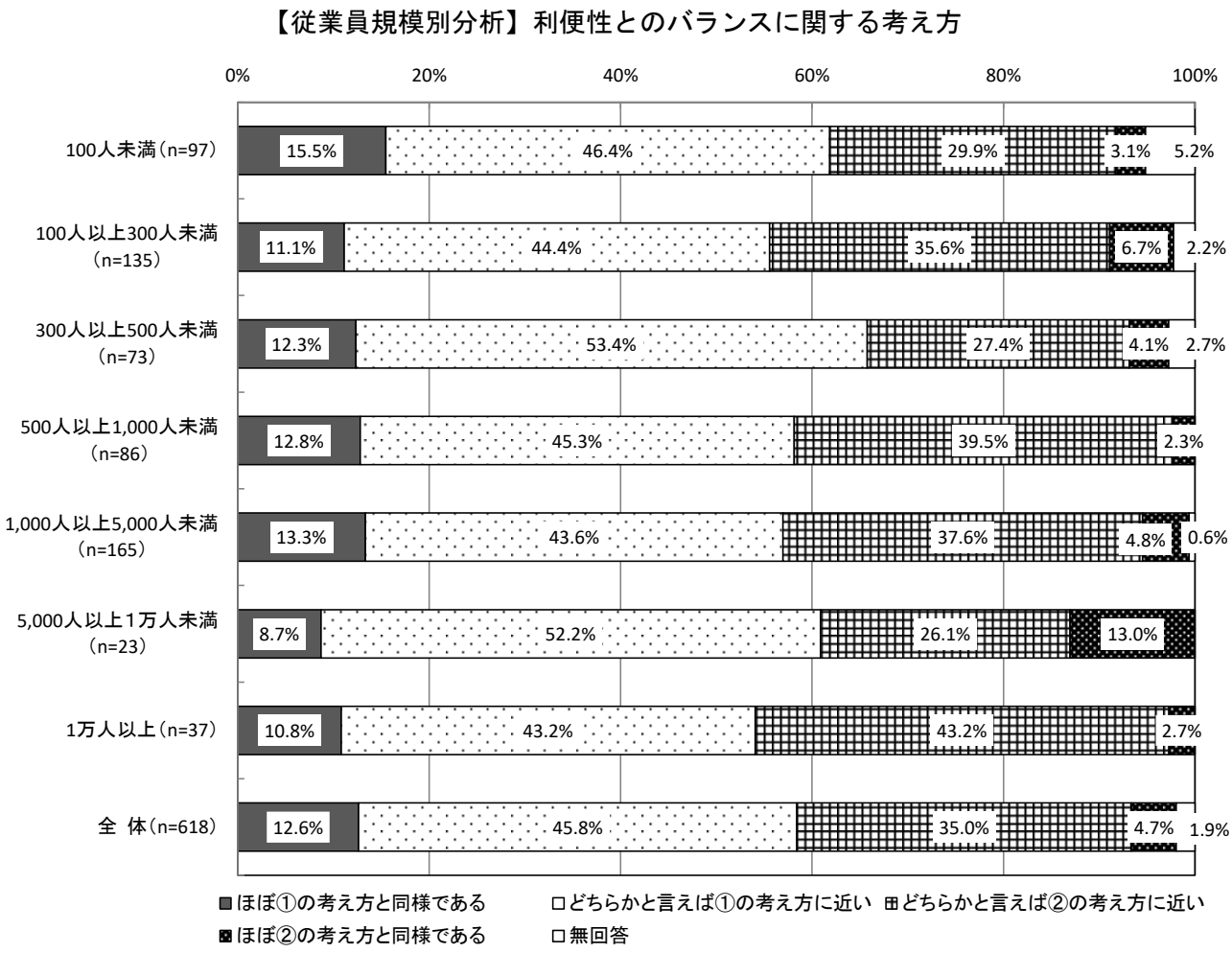
①として提示した考え方	②として提示した考え方
業務実態に負担をかけるほどのセキュリティ対策は不適当であり、利便性とのバランスを考慮すべきである。	ユーザにシステム利用上・業務上の負担を強いてでもセキュリティを守るべきである。

【業種別分析】業種別にみると、「エネルギー」「運輸業」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「不動産・建築」で47.6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。

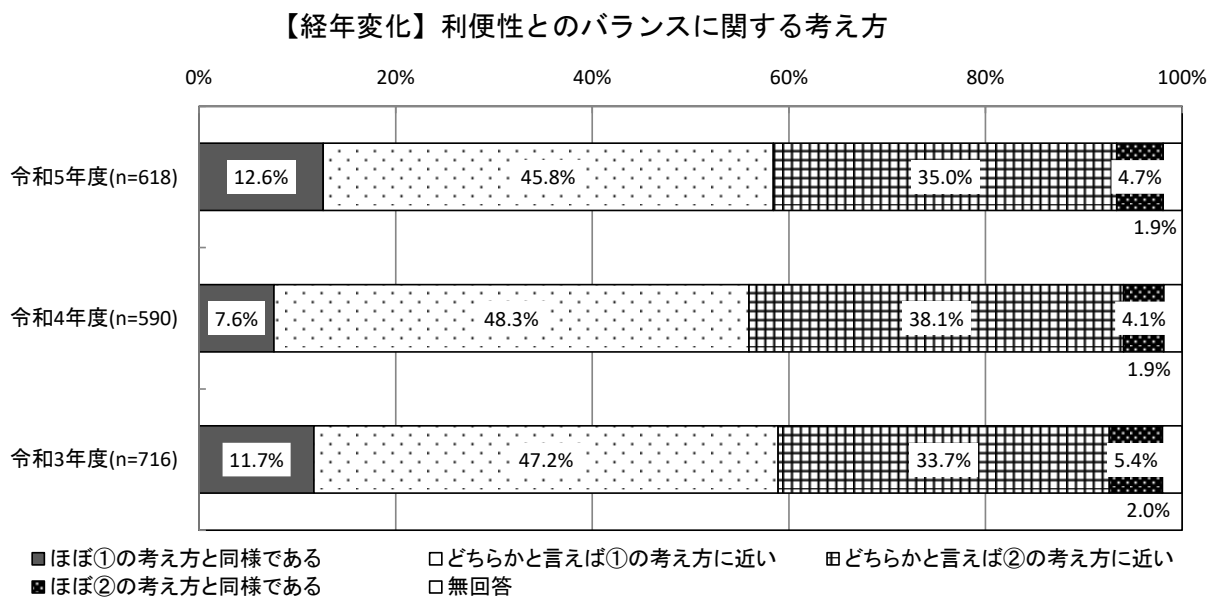
【業種別分析】利便性とのバランスに関する考え方



【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。「1万人以上」では「②負担を強いてでもセキュリティを守る」がやや高くなっている。



【経年変化】昨年度と比較すると、「①利便性とのバランスを考慮」は2.5ポイントの増加、「②負担を強いてでもセキュリティを守る」は2.5ポイントの減少となっている。

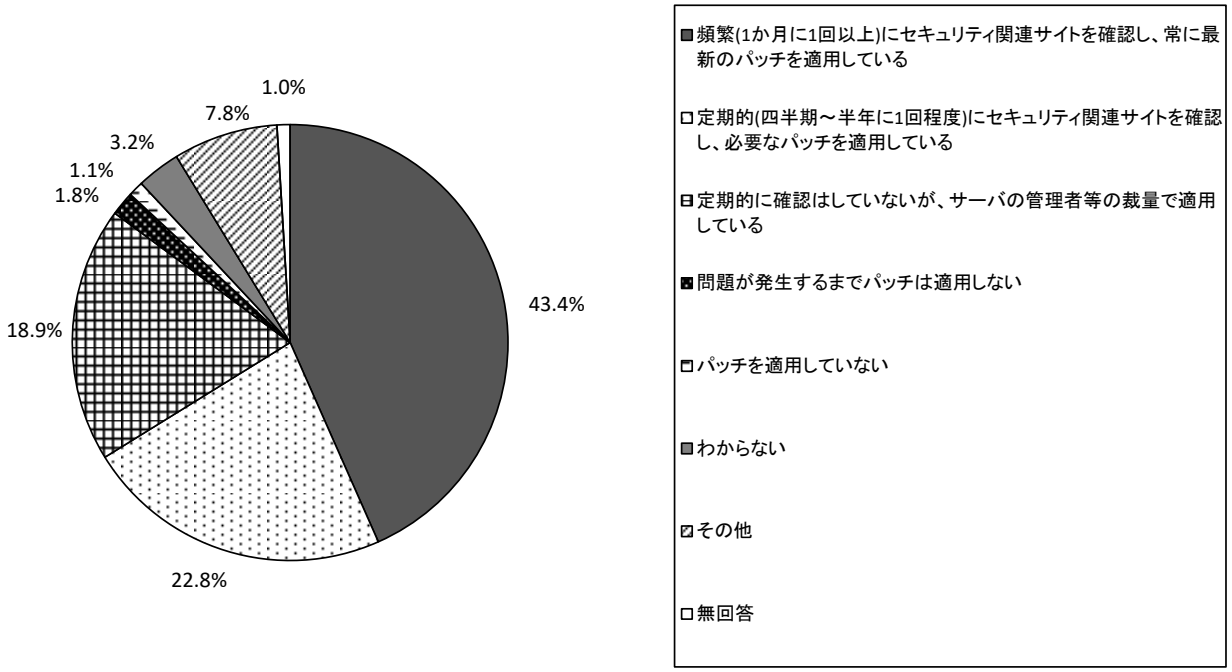


3.2 技術的対策

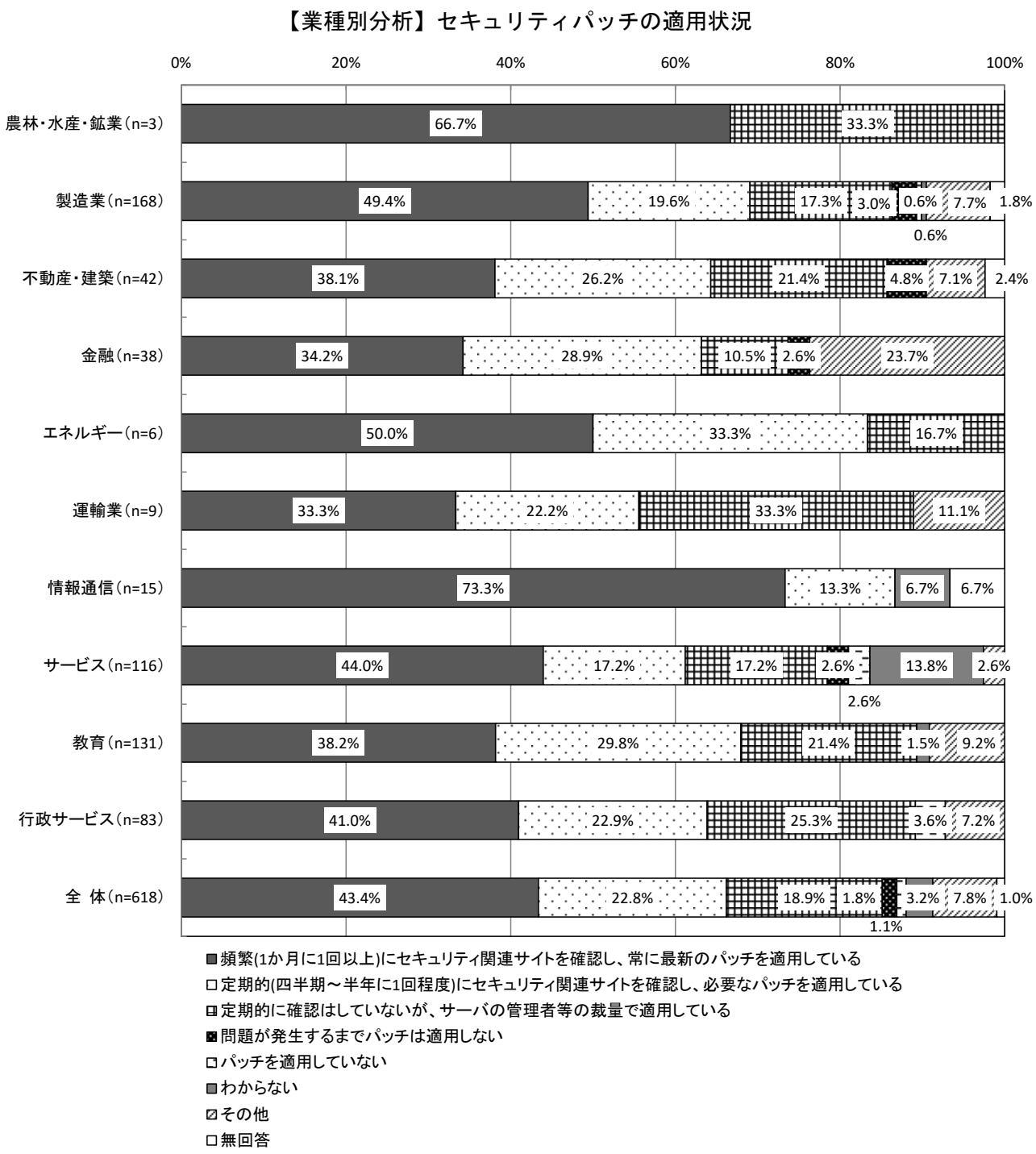
3.2.1 セキュリティパッチの適用状況 【問16】

セキュリティパッチの適用状況については、「頻繁(1か月に1回以上)にセキュリティ関連サイトを確認し、常に最新のパッチを適用している」が43.4%で最も高く、次いで「定期的(四半期～半年に1回程度)にセキュリティ関連サイトを確認し、必要なパッチを適用している」が22.8%、「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18.9%となっている。

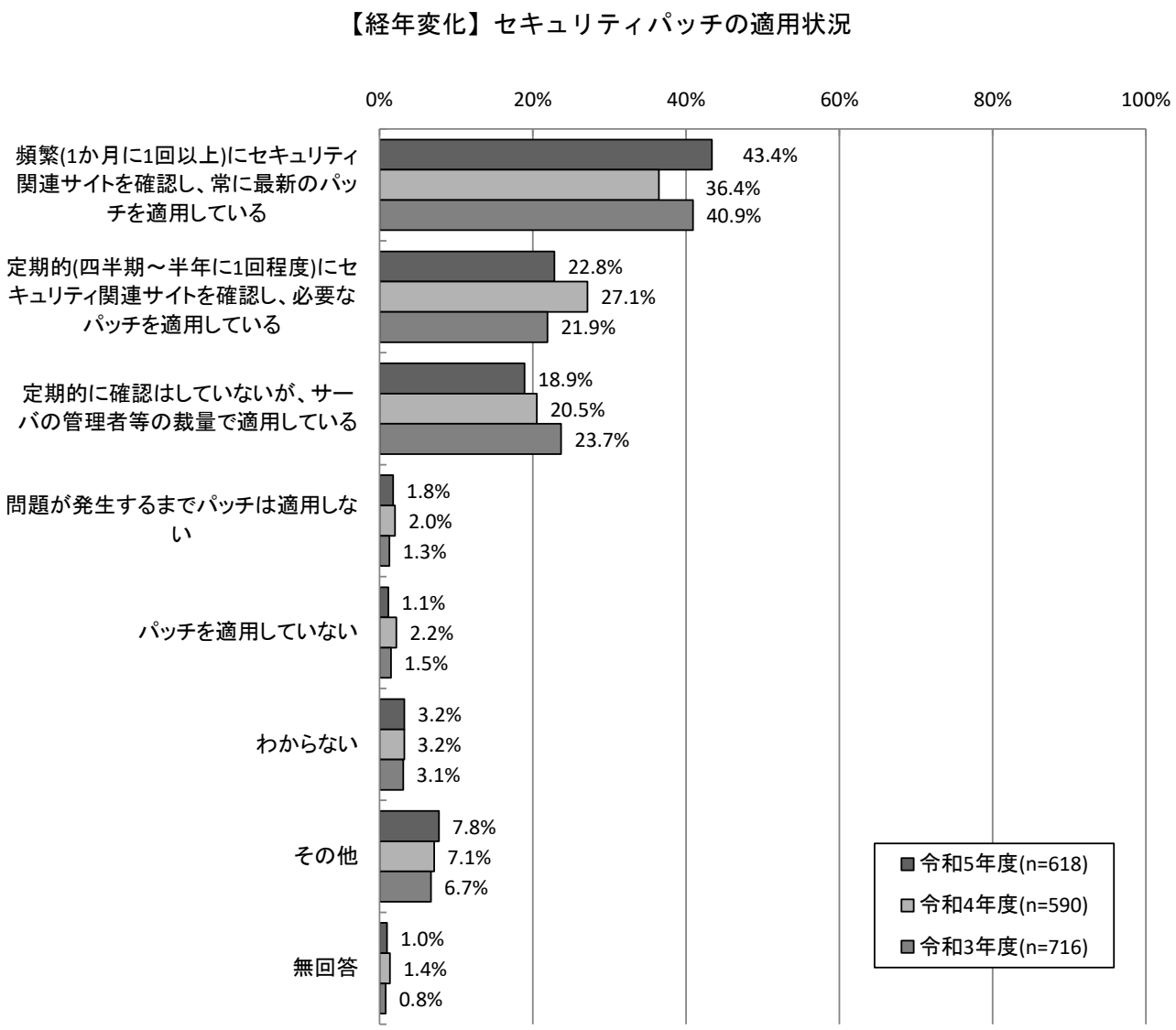
【全体】セキュリティパッチの適用状況 (SA,n=618)



【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73.3%と最も高くなっている。



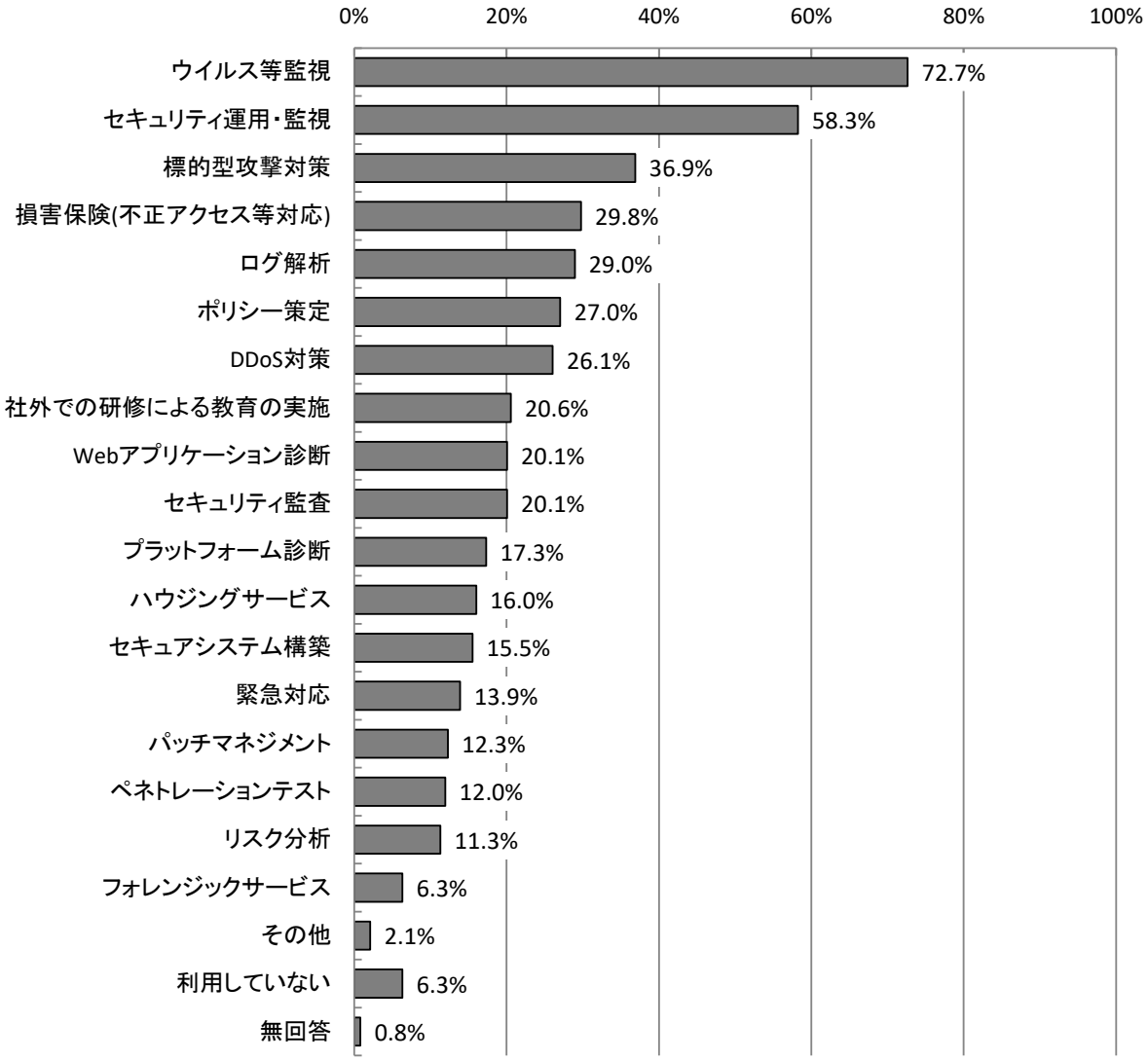
【経年変化】昨年度と比較すると、「頻繁(1か月に1回以上)にセキュリティ関連サイトを確認し、常に最新のパッチを適用している」が7.0ポイント増加している。



3.2.1　利用しているセキュリティサービス　【問17】

利用しているセキュリティサービスについては、「ウイルス等監視」が72.7%で最も高く、次いで「セキュリティ運用・監視」が58.3%となっている。一方「利用していない」は6.3%となっている。

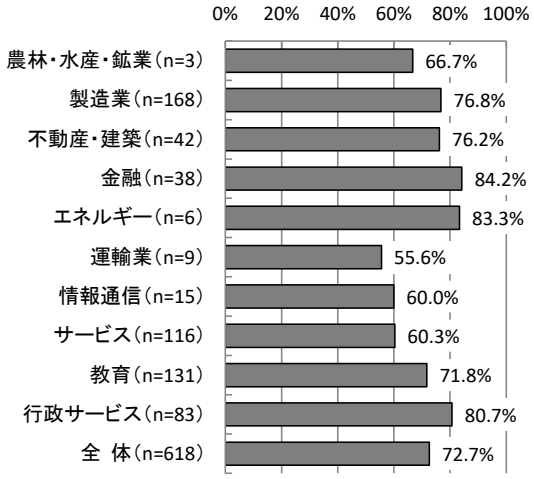
【全体】利用しているセキュリティサービス（MA, n=618）



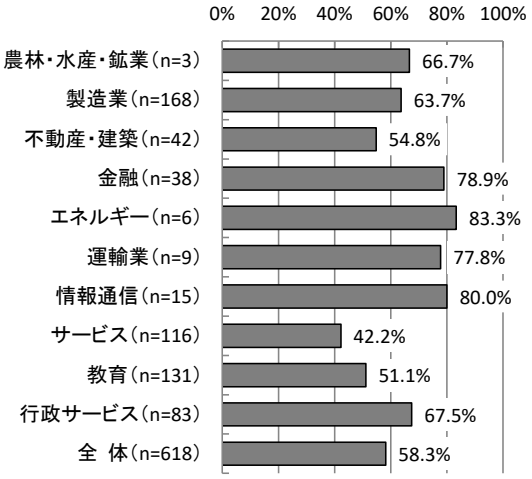
【業種別分析】業種別にみると、「ウイルス等監視」については、「金融」が84.2%、「エネルギー」が83.3%で高い。「セキュリティ運用・監視」については、「エネルギー」が83.3%、「情報通信」が80.0%で高くなっている。

【業種別分析】利用しているセキュリティサービス

ウイルス等監視



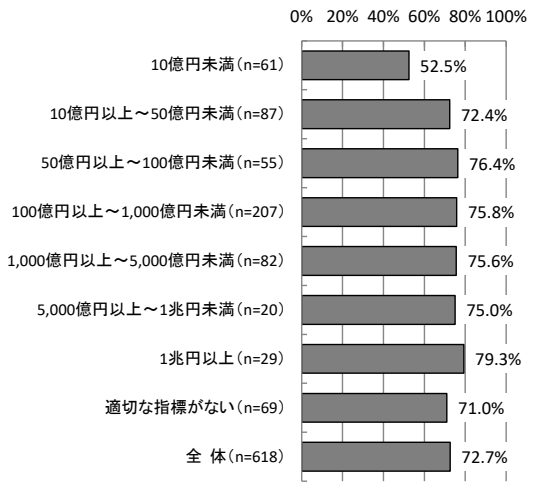
セキュリティ運用・監視



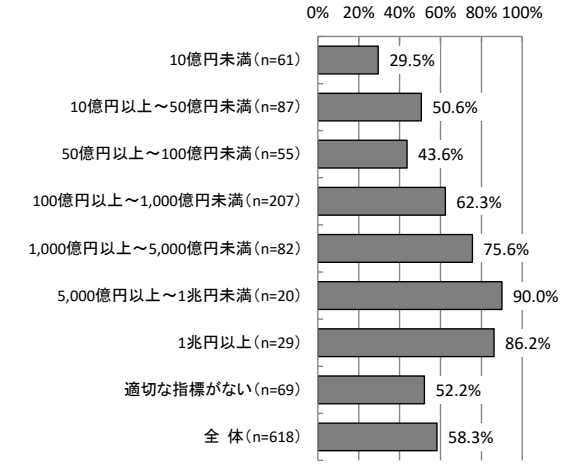
【予算規模別分析】予算規模別にみると、「ウイルス等監視」については、「1兆円以上」が79.3%で最も高くなっている。「セキュリティ運用・監視」については、「5,000億円以上～1兆円未満」が90.0%で最も高くなっている。

【予算規模別分析】利用しているセキュリティサービス

ウイルス等監視



セキュリティ運用・監視

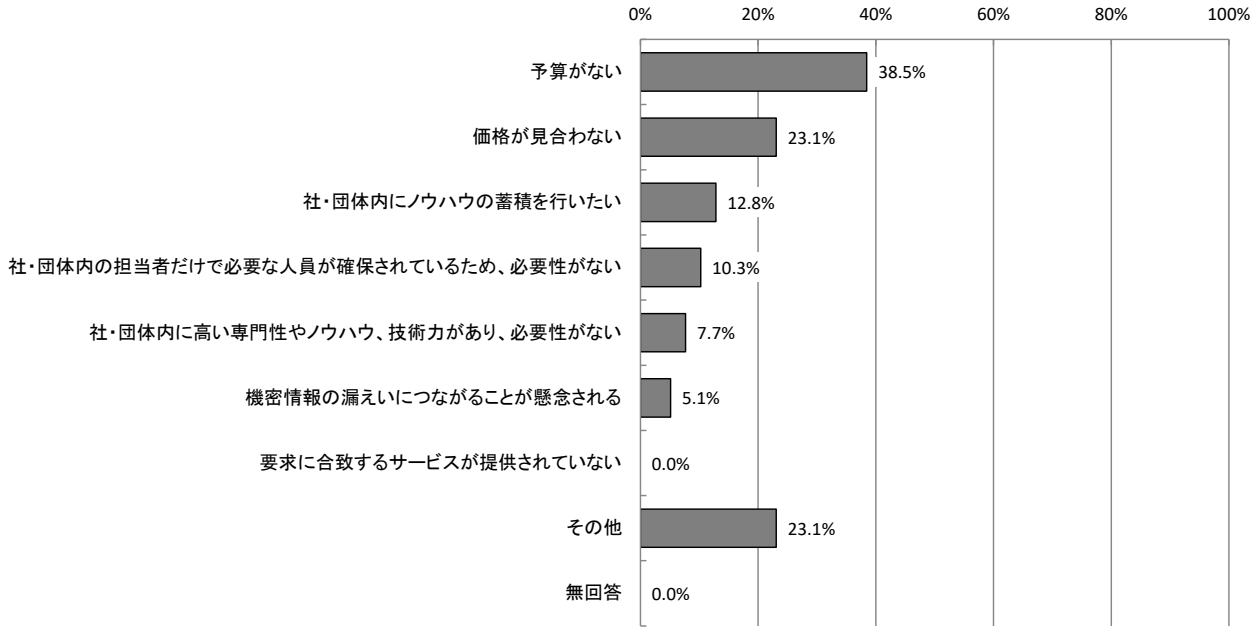


3.2.2　セキュリティサービスを利用していない理由　【問17-1】

セキュリティサービスを利用していない理由については、「予算がない」が38.5%で最も高く、次いで「価格が見合わない」が23.1%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。

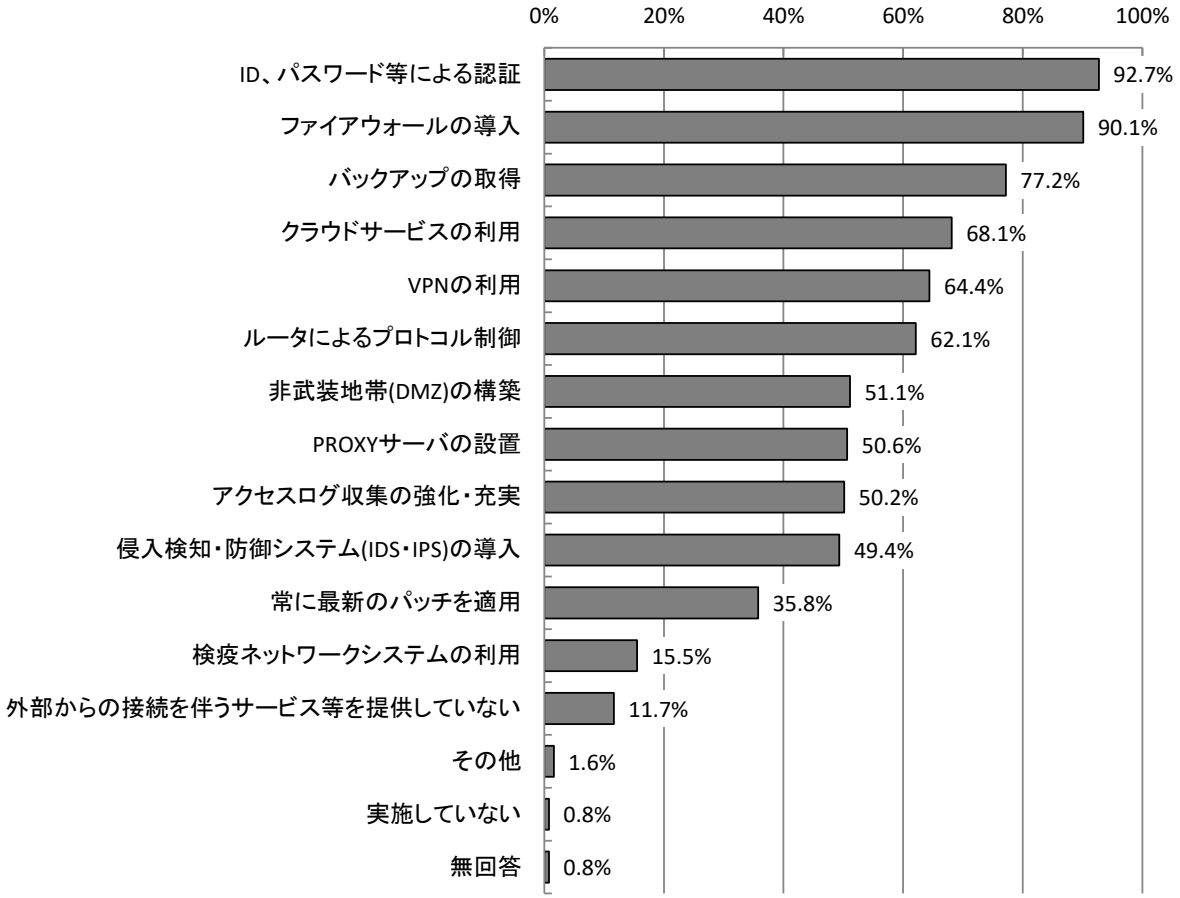
【全体】セキュリティサービスを利用していない理由（MA,n=39）



3.2.3　インターネット接続に対するセキュリティ対策　【問18】

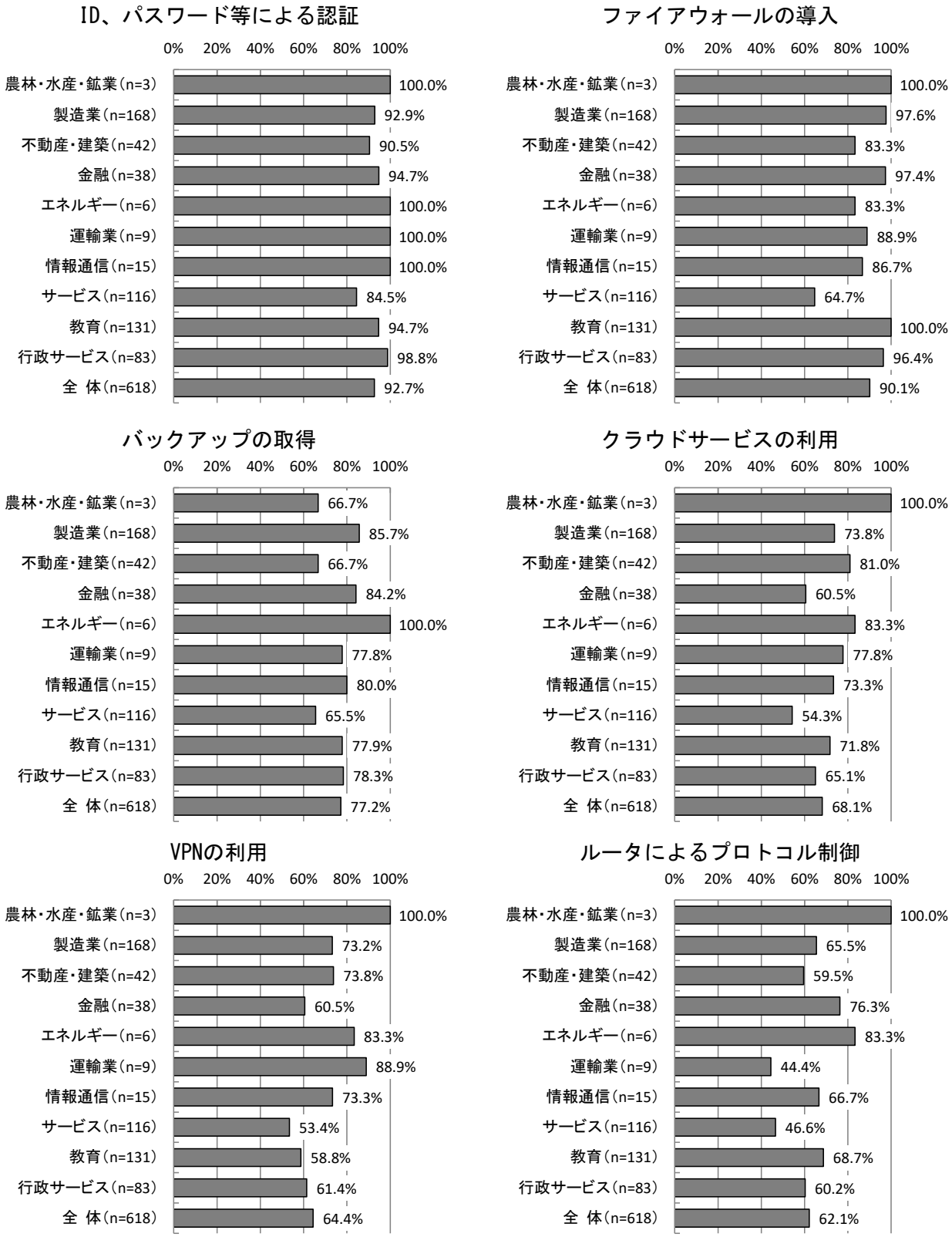
インターネット接続に対するセキュリティ対策については、「ID、パスワード等による認証」が92.7%で最も高く、次いで「ファイアウォールの導入」が90.1%となっている。

【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=618）



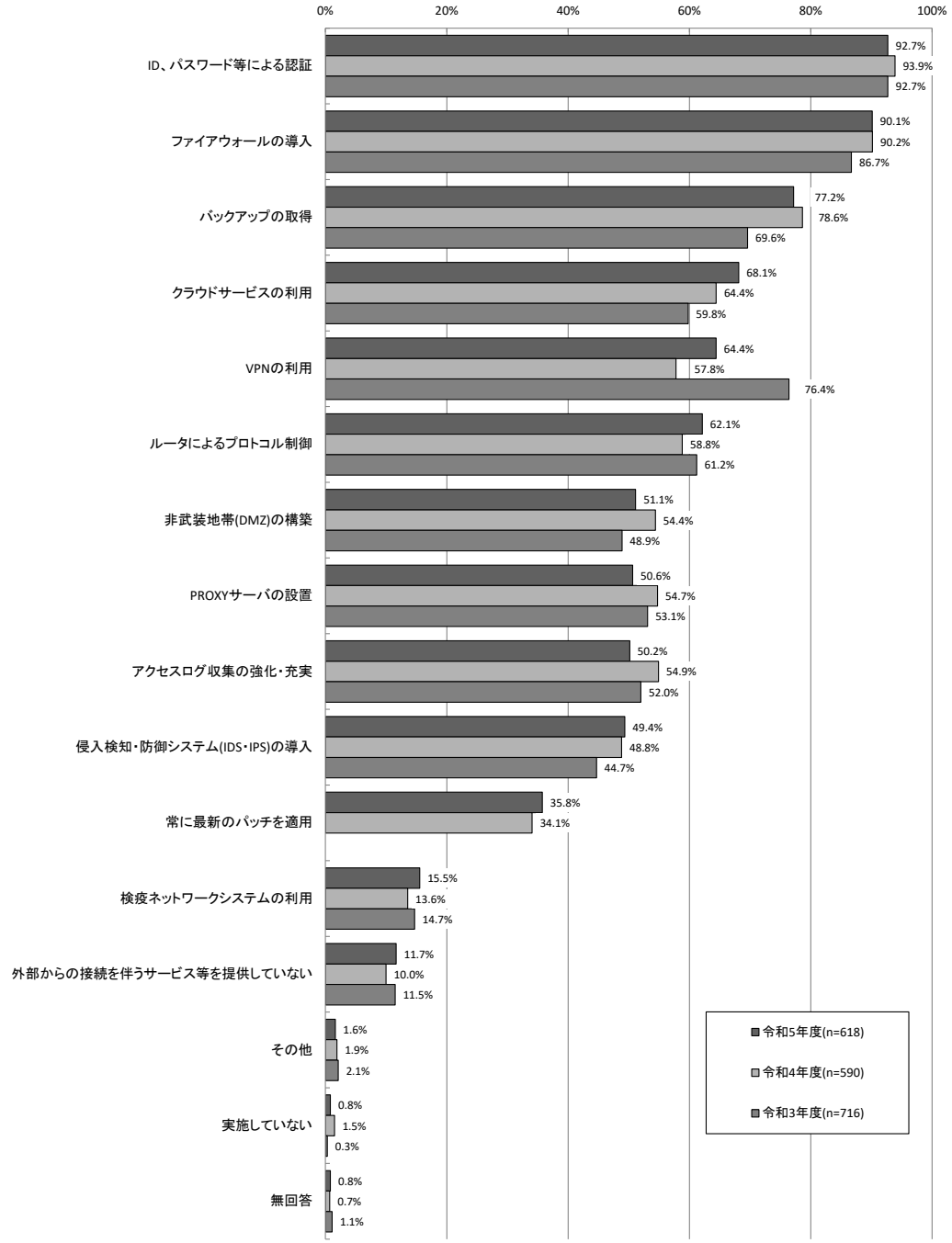
【業種別分析】業種別にみると、「ID、パスワード等による認証」については、「サービス」の84.5%を除き、いずれも90%以上と高くなっている。「ファイアウォールの導入」についても「サービス」の64.7%を除き、いずれも80%以上と高くなっている。

【業種別分析】インターネット接続に対するセキュリティ対策



【経年変化】昨年度と比較すると、「VPNの利用」が6.6ポイント、「クラウドサービスの利用」が3.7ポイント、「ルータによるプロトコル制御」が3.3ポイント増加している。一方で、「アクセスログ収集の強化・充実」が4.7ポイント、「PROXYサーバの設置」が4.1ポイント、「非武装地帯(DMZ)の構築」が3.3ポイント減少している。

【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



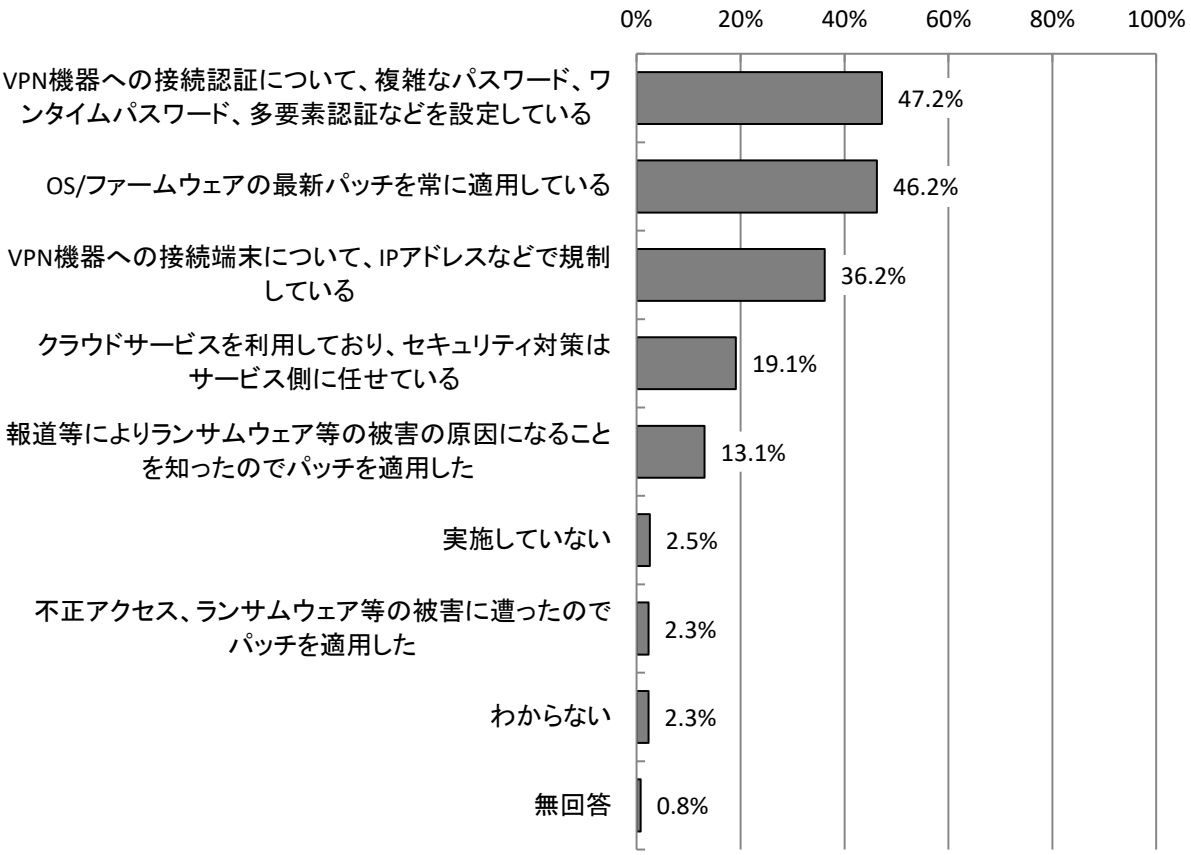
※令和３年度調査で「バックアップの取得」を新設
※令和４年度調査で「常に最新のパッチを適用」を新設

3.2.4 VPN機器のセキュリティ対策 【問18-1】

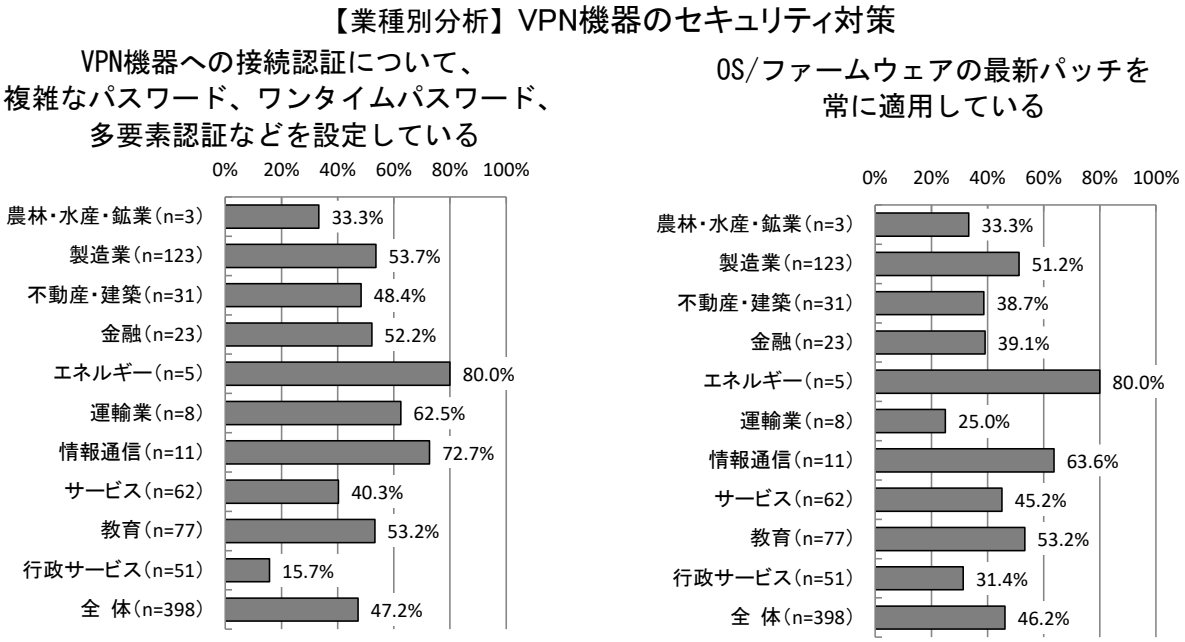
VPN機器のセキュリティ対策は、「VPN機器への接続認証について、複雑なパスワード、ワンタイムパスワード、多要素認証などを設定している」が47.2%で最も高い。「OS/ファームウェアの最新パッチを常に適用している」も46.2%と高くなっている。「実施していない」は2.5%と1割未満となっている。

※本項目は、VPNを利用している社・団体等を対象としている。

【全体】VPN機器のセキュリティ対策 (MA, n=398)



【業種別分析】業種別にみると、「VPN機器への接続認証について、複雑なパスワード、ワンタイムパスワード、多要素認証などを設定している」は「エネルギー」「情報通信」の順に高くなっている。「OS/ファームウェアの最新パッチを常に適用している」も同様に「エネルギー」「情報通信」の順に高い。

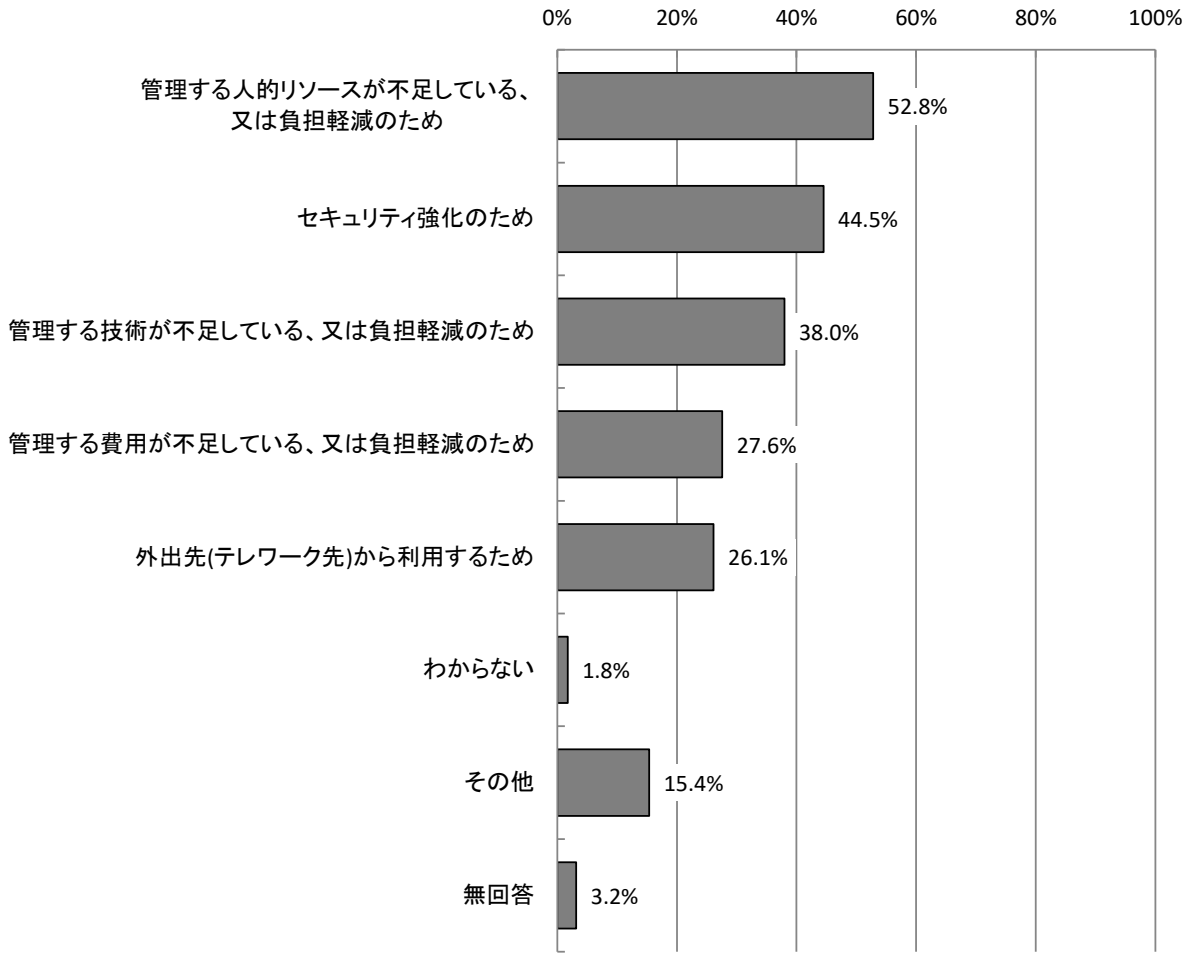


3.2.5　クラウドサービスを使用することになった理由　【問19】

クラウドサービスを使用することになった理由については、「管理する人的リソースが不足している、又は負担軽減のため」が52.8%で最も高く、次いで「セキュリティ強化のため」が44.5%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。

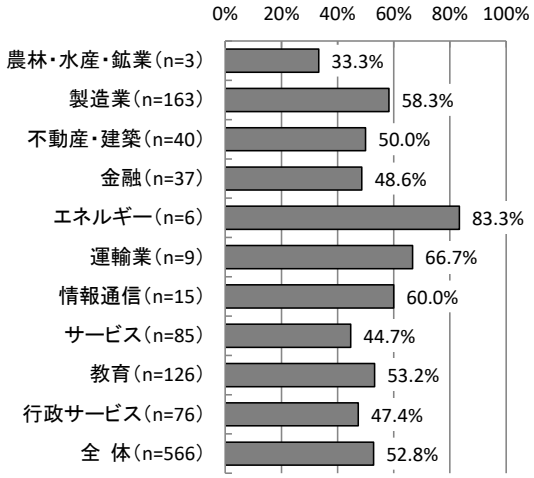
【全体】クラウドサービスを使用することになった理由（MA,n=566）



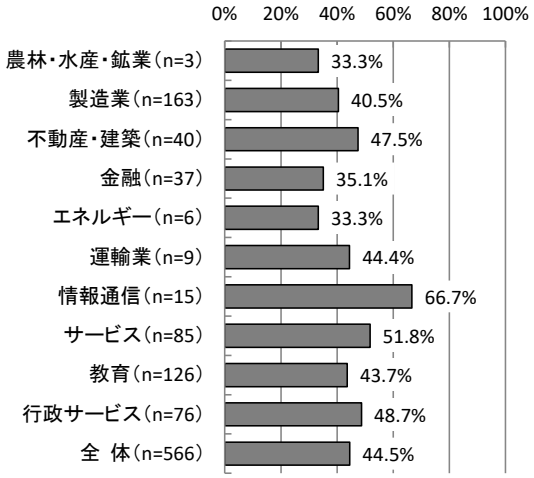
【業種別分析】業種別にみると、「管理する人的リソースが不足している、又は負担軽減のため」については、「エネルギー」が83.3%、「運輸業」が66.7%、「情報通信」が60.0%で高い。「セキュリティ強化のため」については、「情報通信」が66.7%で高くなっている。

【業種別分析】クラウドサービスを使用することになった理由

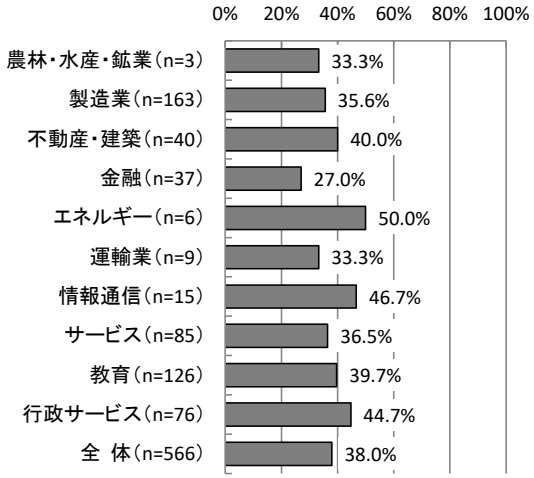
管理する人的リソースが不足している、又は負担軽減のため



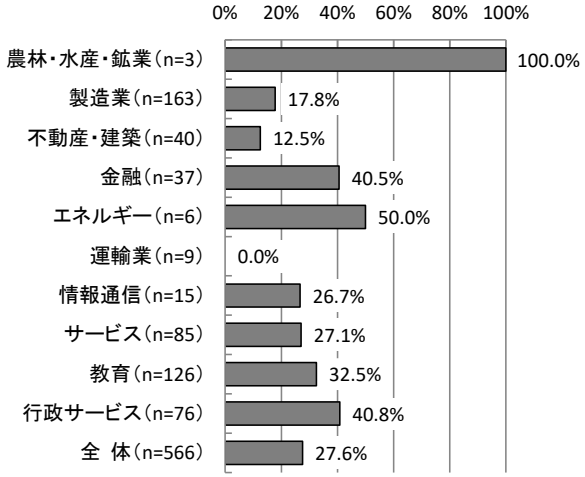
セキュリティ強化のため



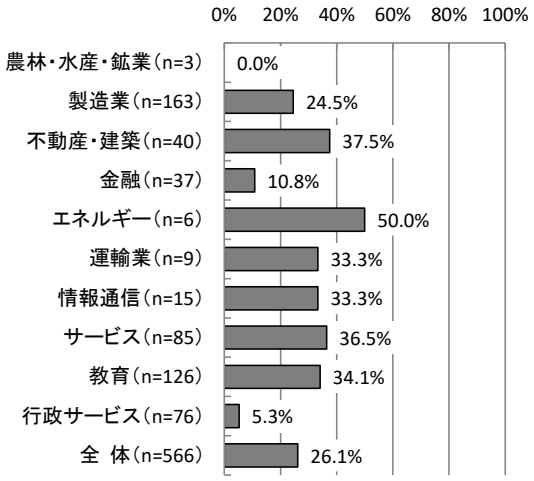
管理する技術が不足している、又は負担軽減のため



管理する費用が不足している、又は負担軽減のため



外出先（テレワーク先）から利用するため

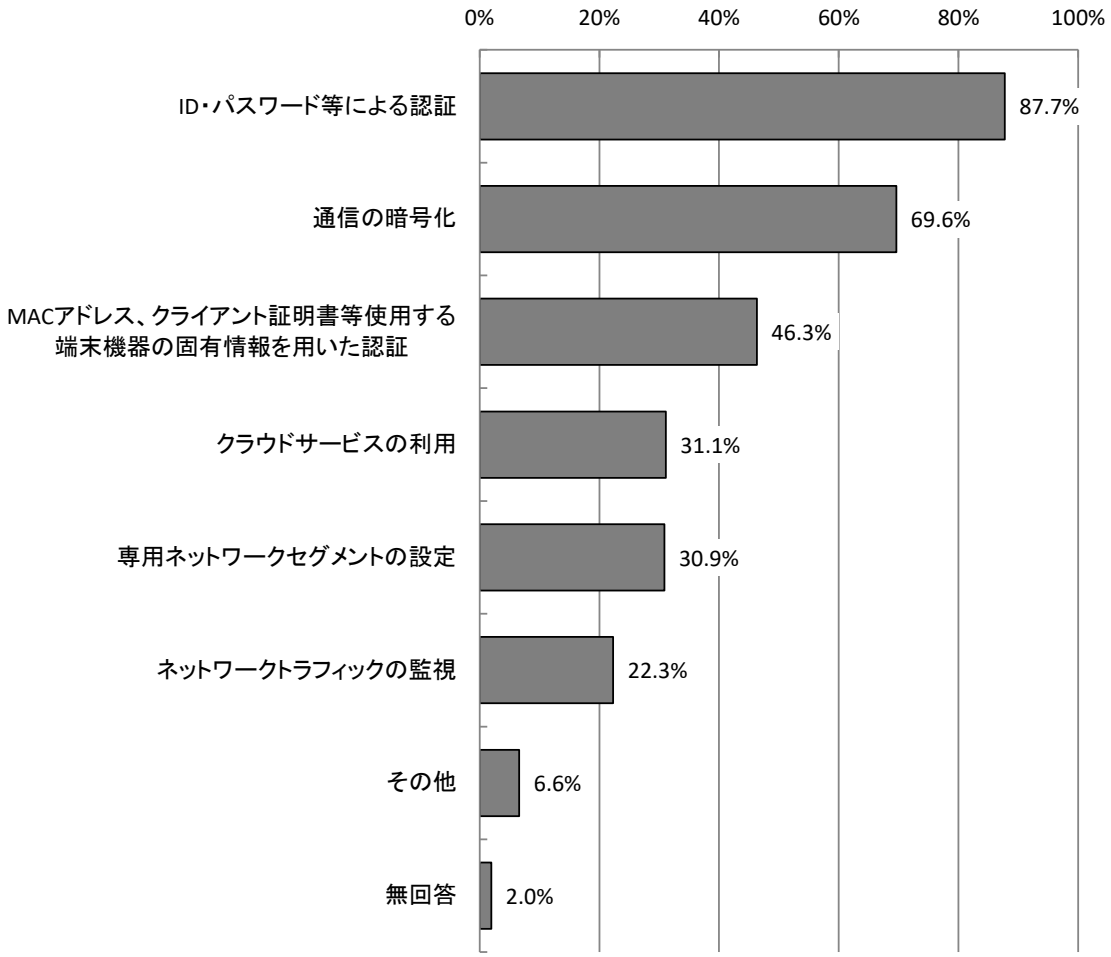


3.2.6　外部からの接続に対するセキュリティ対策　（通信路に対する対策）　【問20-A】

外部からの接続に対するセキュリティ対策（通信路に対する対策）については、「ID・パスワード等による認証」が87.7%で最も高く、次いで「通信の暗号化」が69.6%、「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46.3%となっている。

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

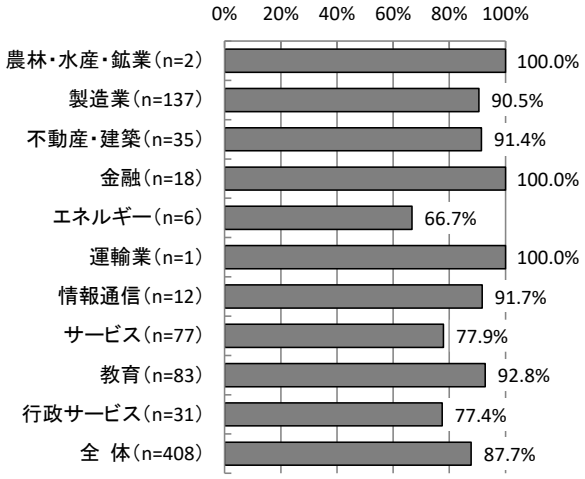
【全体】外部からの接続に対するセキュリティ対策（通信路に対する対策）（MA, n=408）



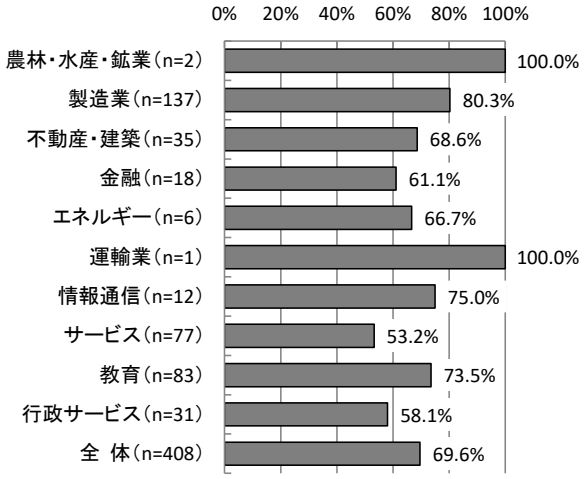
【業種別分析】業種別にみると、「ID・パスワード等による認証」では「金融」が100.0%と最も高く、「通信の暗号化」では「製造業」が80.3%で最も高い。

【業種別分析】外部からの接続に対するセキュリティ対策（通信路に対する対策）

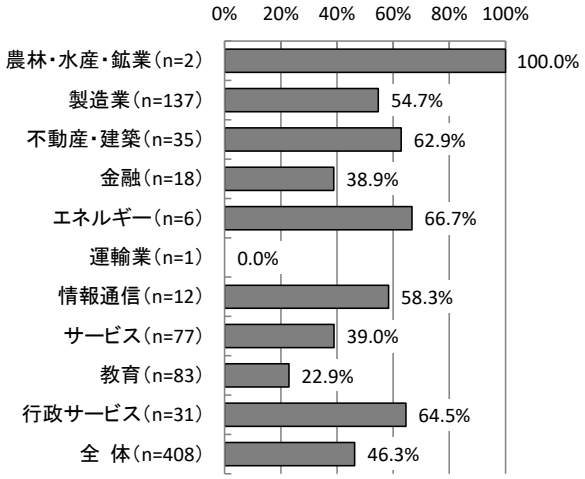
ID・パスワード等による認証



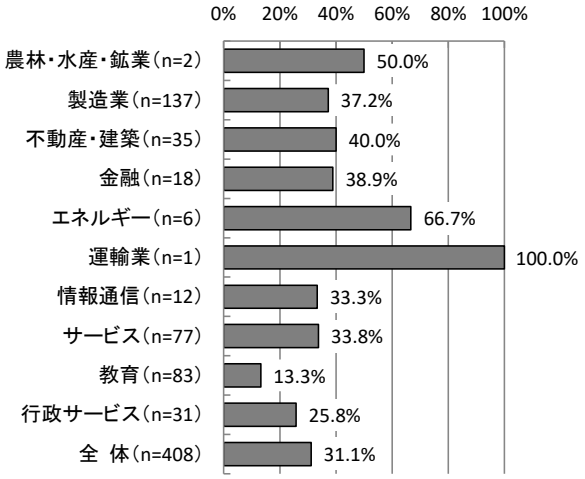
通信の暗号化



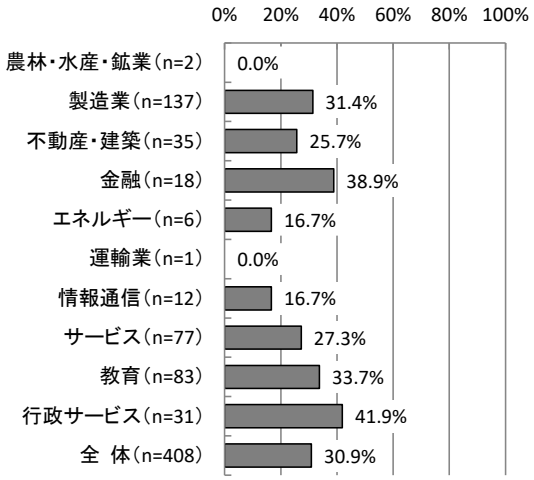
MAC アドレス、クライアント証明書等使用する端末機器の固有情報を用いた認証



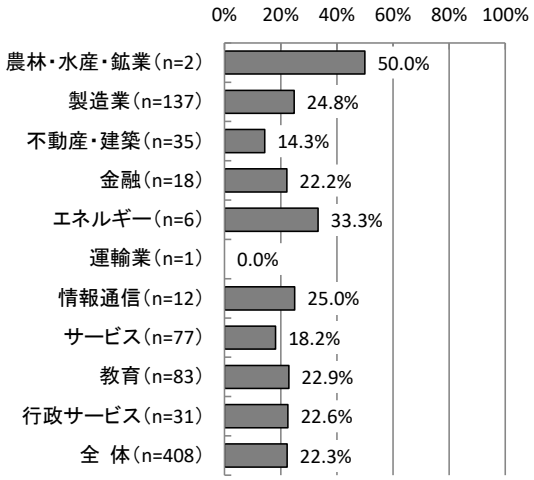
クラウドサービスの利用



専用ネットワークセグメントの設定



ネットワークトラフィックの監視

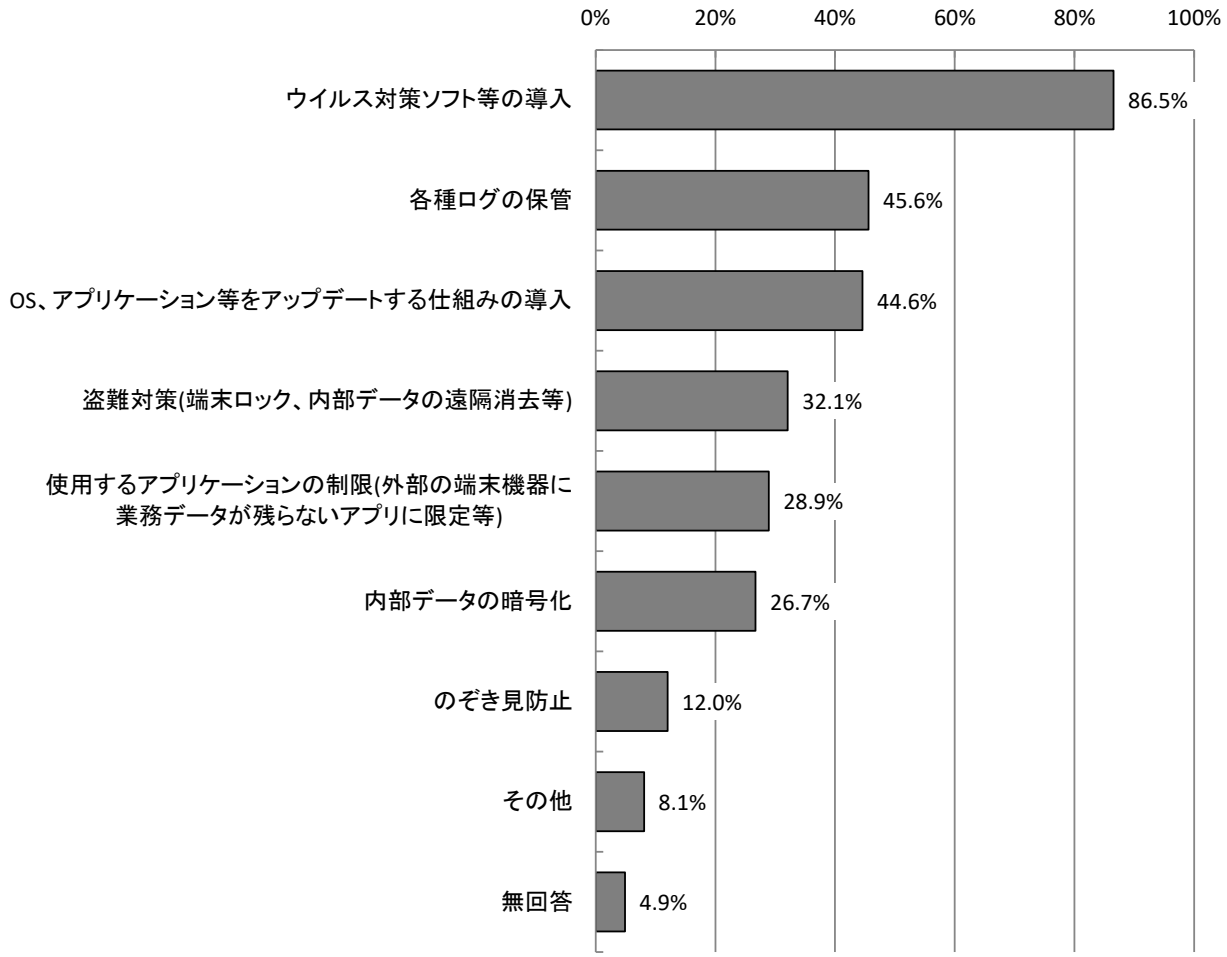


3.2.7　外部からの接続に対するセキュリティ対策　（端末に対する対策）　【問20-B】

外部からの接続に対するセキュリティ対策（端末に対する対策）については、「ウイルス対策ソフト等の導入」が86.5%で最も高く、次いで「各種ログの保管」が45.6%、「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44.6%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。

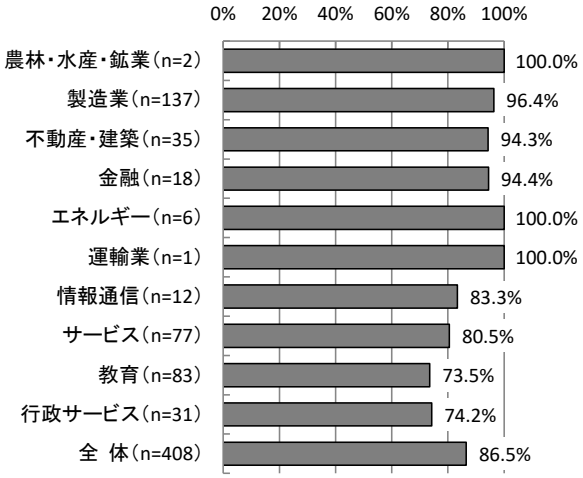
【全体】外部からの接続に対するセキュリティ対策（端末に対する対策）（MA, n=408）



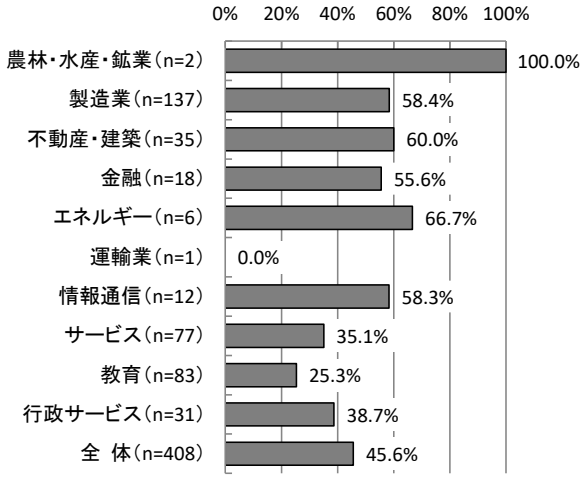
【業種別分析】業種別にみると、業種別にみると、「ウイルス対策ソフト等の導入」では「エネルギー」が100.0%と最も高く、「製造業」「不動産・建築」「金融」で90%以上と高くなっている。「各種ログの保管」では「エネルギー」が66.7%で最も高い。

【業種別分析】外部からの接続に対するセキュリティ対策（端末に対する対策）

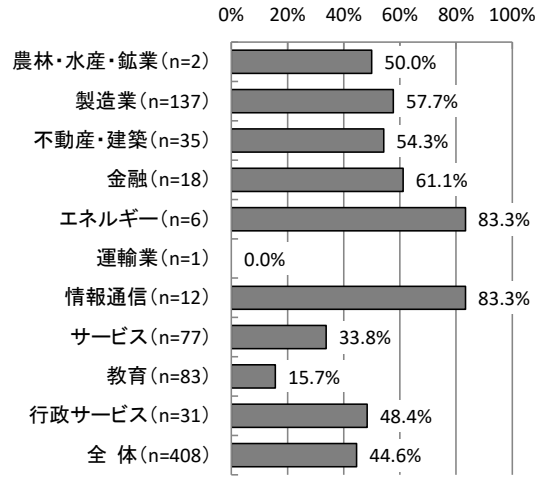
ウイルス対策ソフト等の導入



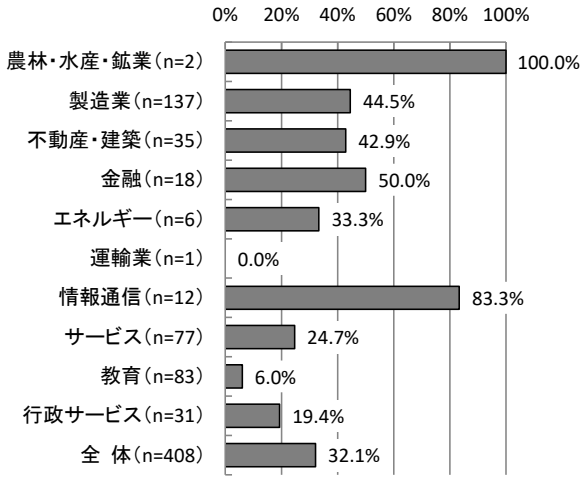
各種ログの保管



OS、アプリケーション等を
アップデートする仕組みの導入



盗難対策
（端末ロック、内部データの遠隔消去等）

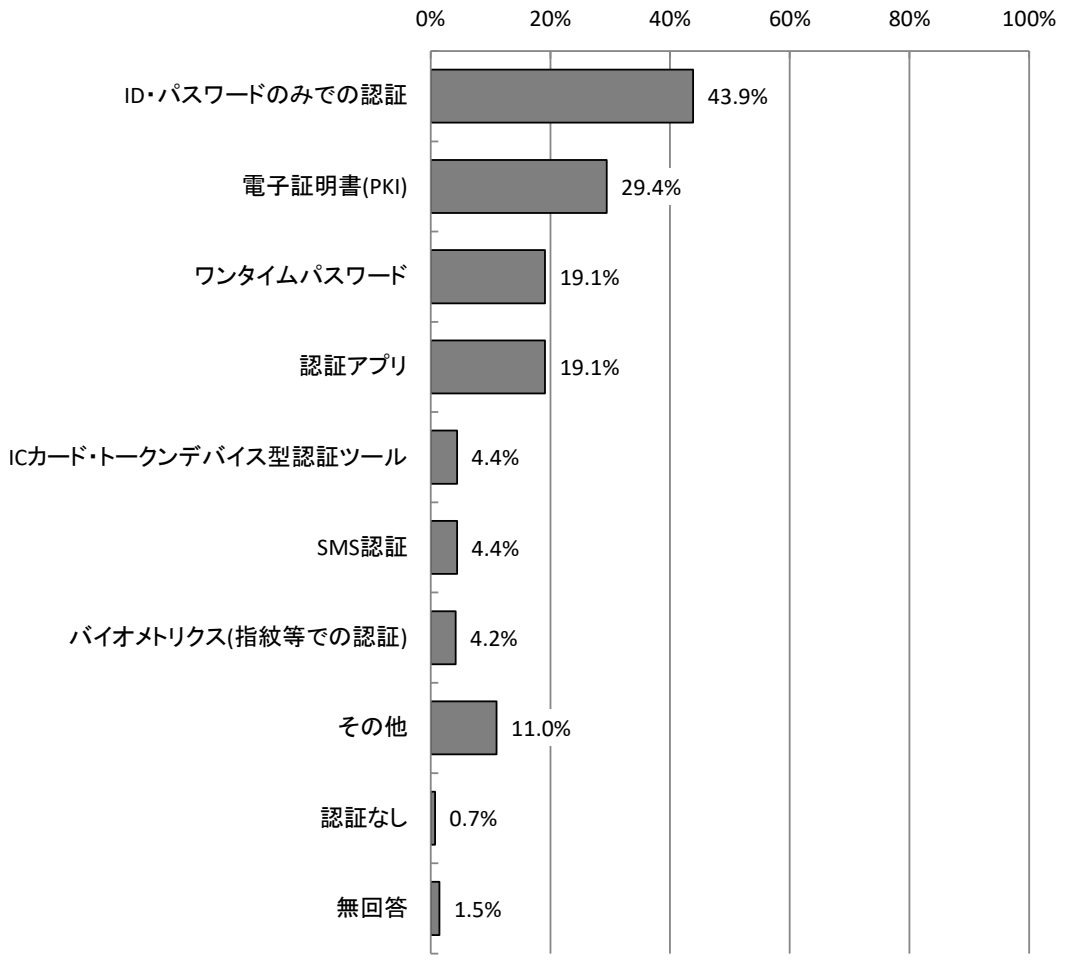


3.2.8　社外等からのインターネット接続経由の認証方法　【問21】

社外等からのインターネット接続経由の認証方法については、「ID・パスワードのみでの認証」が43.9%で最も高い。次いで「電子証明書(PKI)」が29.4%となっている。一方、「認証なし」は0.7%と1割未満となっている。

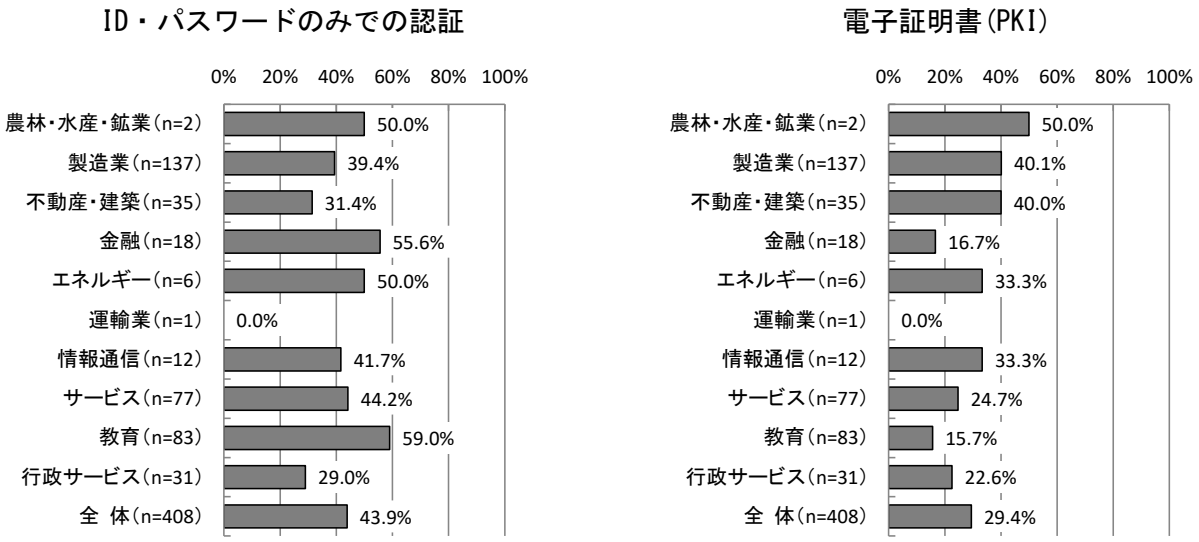
※本項目は、外部から内部ネットワークへの接続を許可している社・団体等を対象としている。

【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=408）



【業種別分析】業種別にみると、「ID・パスワードのみでの認証」については、「教育」が59.0%、「金融」が55.6%と高くなっている。

【業種別分析】社外等からのインターネット接続経由の認証方法

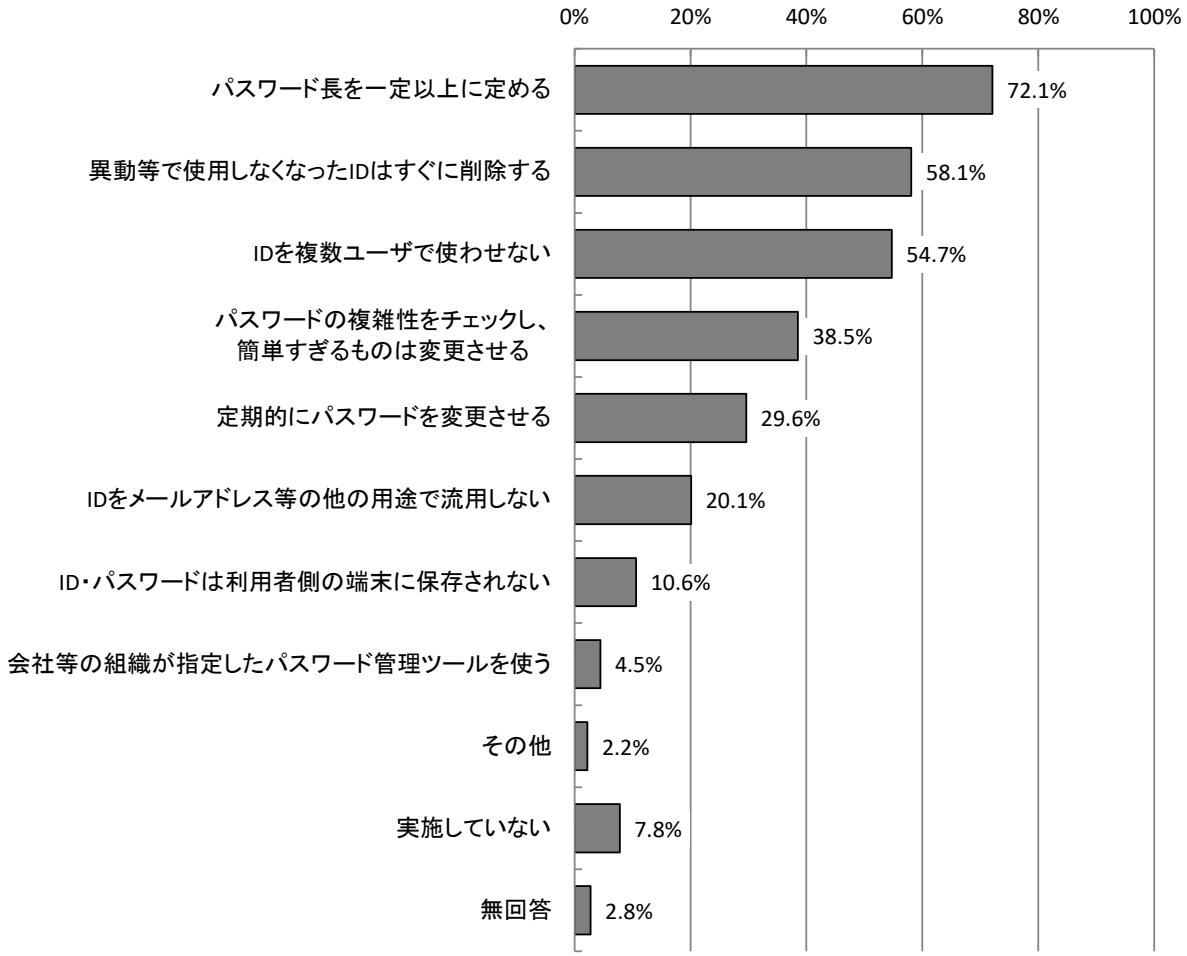


3.2.9　ID・パスワードの管理方法　【問21-1】

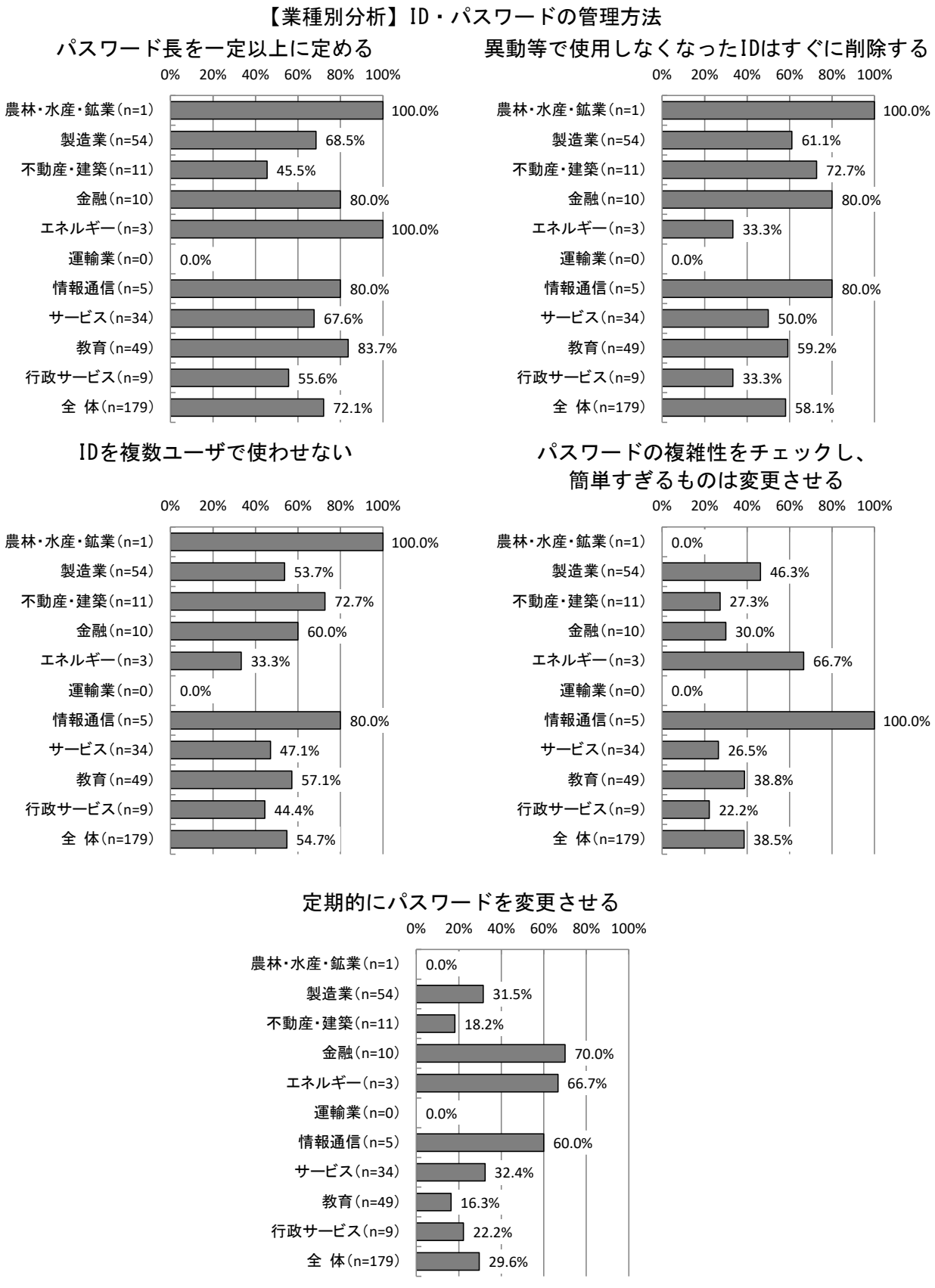
ID・パスワードの管理方法については、「パスワード長を一定以上に定める」が72.1%で最も高く、次いで「異動等で使用しなくなったIDはすぐに削除する」が58.1%となっている。

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

【全体】ID・パスワードの管理方法（MA,n=179）



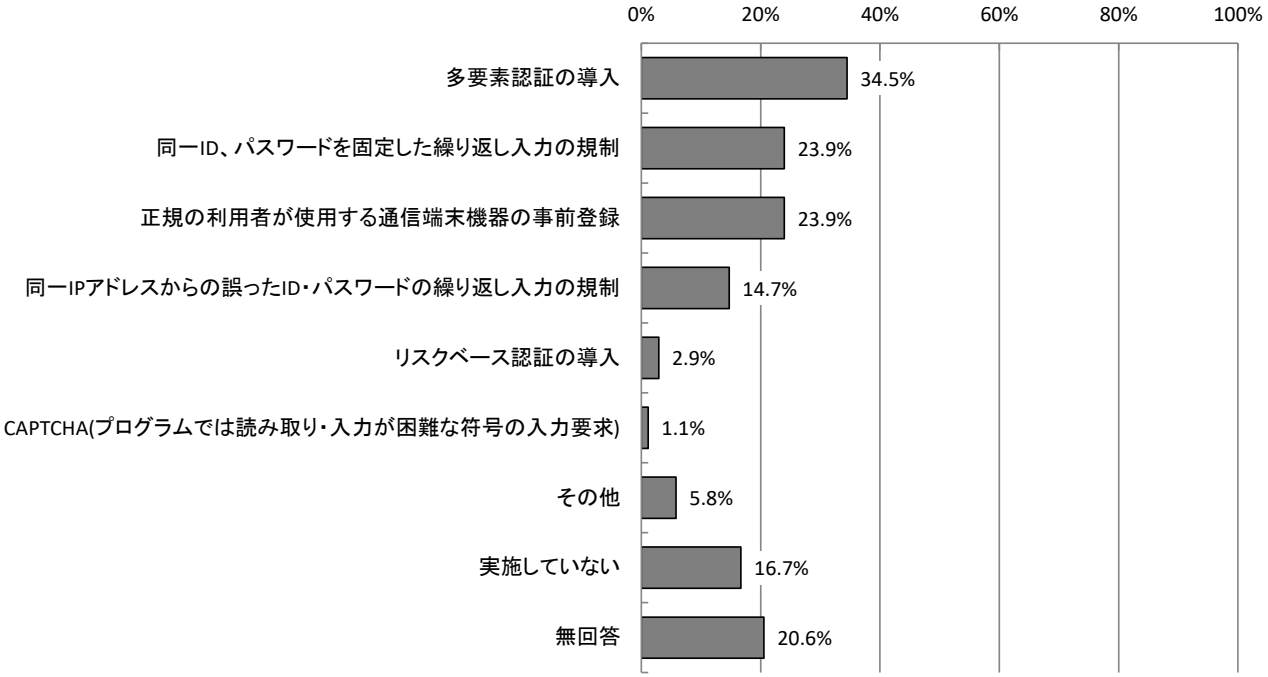
【業種別分析】業種別にみると、「パスワード長を一定以上に定める」については、「教育」が83.7%、「金融」「情報通信」が80.0%で高くなっている。「異動等で使用しなくなったIDはすぐに削除する」については、「金融」「情報通信」が80.0%で高い。



3.2.10　不正ログイン対策　【問21-2】

不正ログイン対策については、「多要素認証の導入」が34.5%で最も高くなっている。次いで「同一ID、パスワードを固定した繰り返し入力の規制」「正規の利用者が使用する通信端末機器の事前登録」がいずれも23.9%となっている。一方、「実施していない」は16.7%となっている。

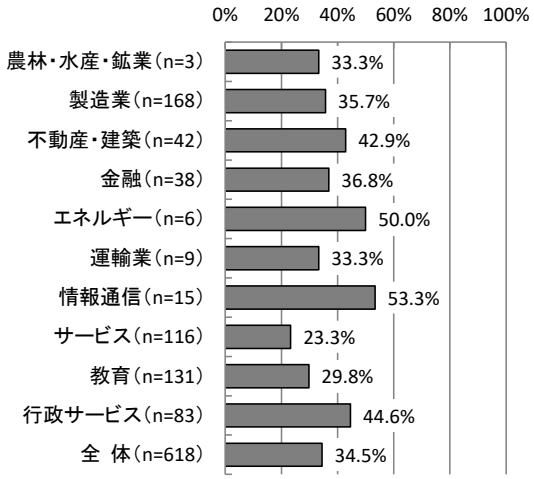
【全体】不正ログイン対策（MA,n=618）



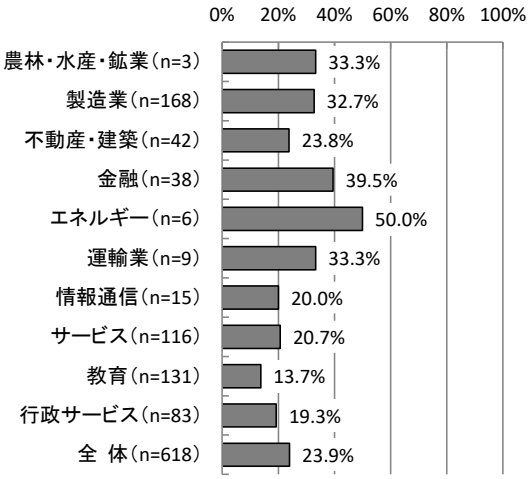
【業種別分析】業種別にみると、「多要素認証の導入」については、「情報通信」が53.3%、「エネルギー」が50.0%で高くなっている。「同一ID、パスワードを固定した繰り返し入力の規制」については、「エネルギー」が50.0%で最も高くなっている。「正規の利用者が使用する通信端末機器の事前登録」については、「エネルギー」が50.0%、「情報通信」が40.0%で高くなっている。

【業種別分析】不正ログイン対策

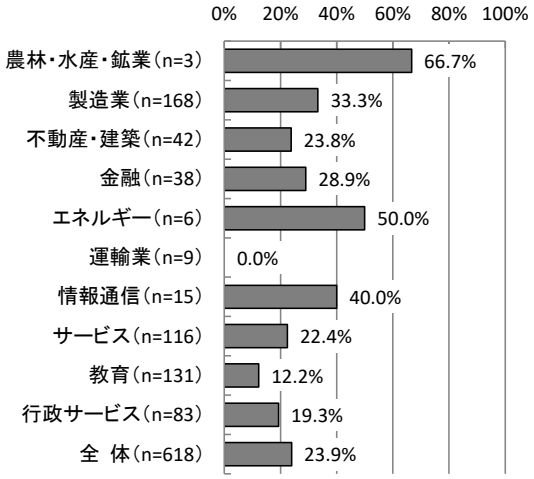
多要素認証の導入



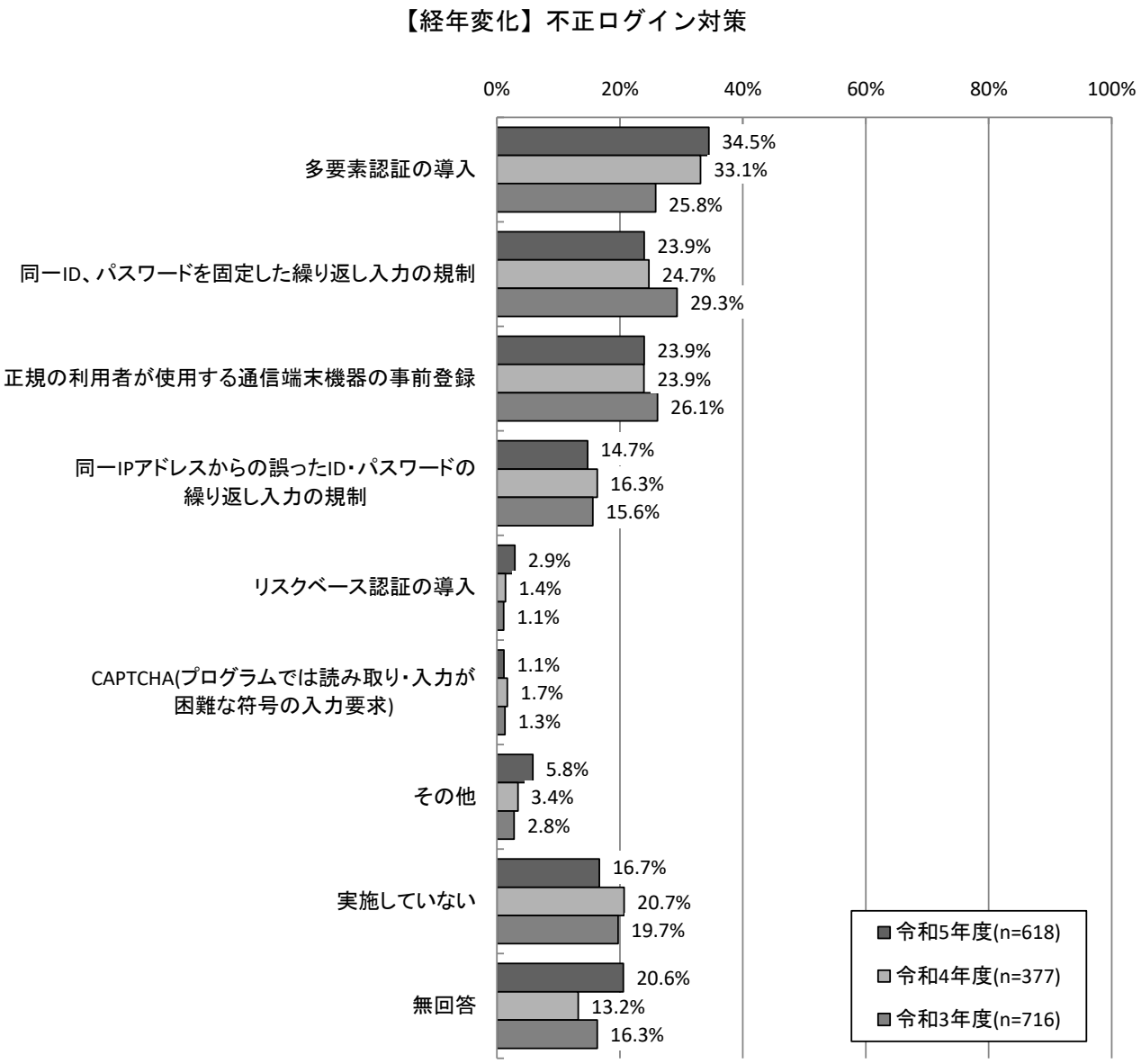
同一ID、パスワードを固定した繰り返し入力の規制



正規の利用者が使用する通信端末機器の事前登録



【経年変化】３年間を比較したところ、「同一IPアドレスからの誤ったID･パスワードの繰り返し入力の規制」が1.6ポイント、「同一ID･パスワードを固定した繰り返し入力の規制」が0.8ポイント減少している。一方で、「リスクベース認証の導入」が1.5ポイント、「多要素認証の導入」が1.4ポイント増加している。

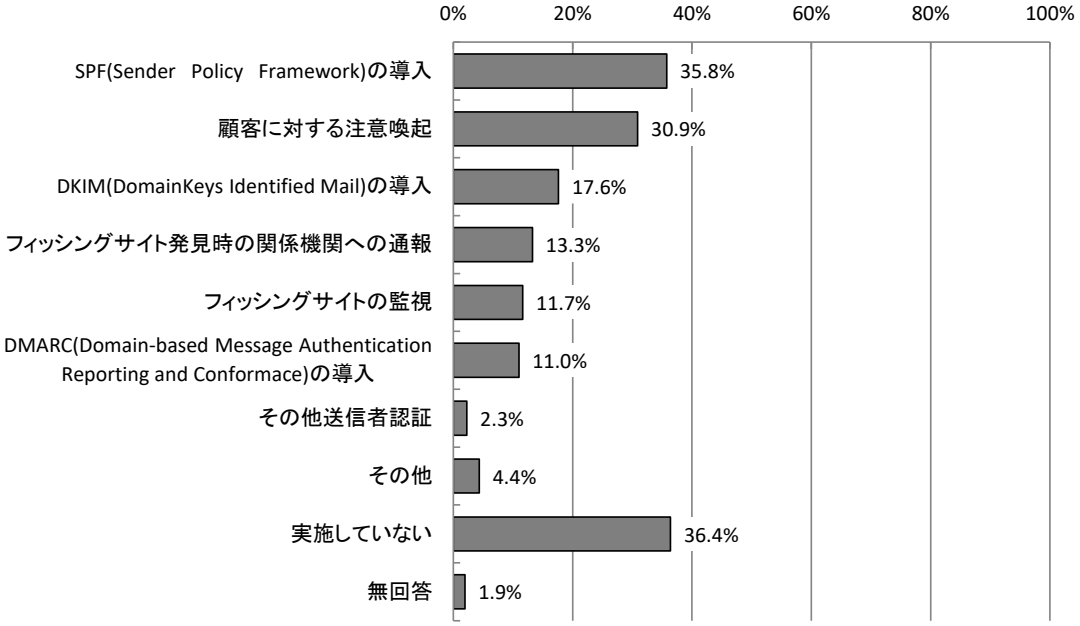


※令和３年度調査で「多要素認証の導入」「リスクベース認証の導入」を新設

3.2.11　フィッシング対策【問22】

フィッシング対策については、送信ドメイン認証（SPF、DKIM、DMARC）をみると、「SPF(Sender Policy Framework)の導入」が35.8%、「DKIM（DomainKeys Identified Mail）の導入」が17.6%、「DMARC(Domain-based Message Authentication Reporting and Conformace）の導入」が11.0%となっている。「顧客に対する注意喚起」が30.9%と、最も高い「SPF(Sender Policy Framework)の導入」に次いで高くなっている。一方で、「実施していない」は36.4%となっている。

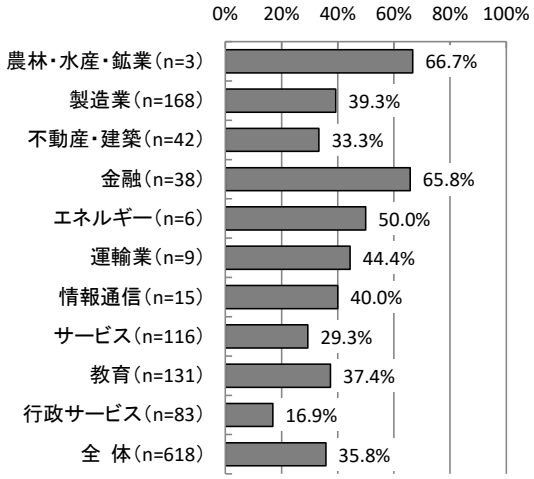
【全体】フィッシング対策(SA,n=618)



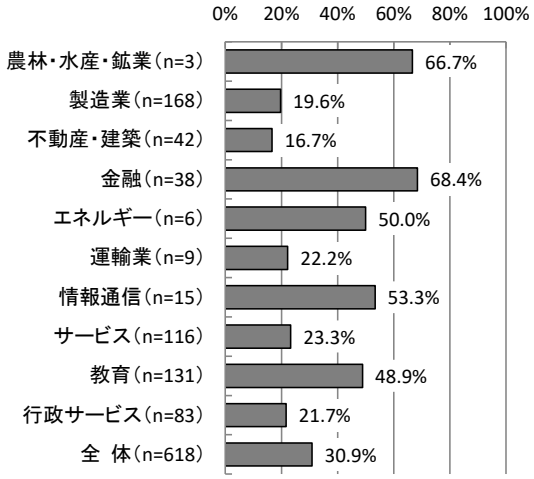
【業種別分析】業種別にみると、送信ドメイン認証（SPF、DKIM、DMARC）については、「SPF(Sender Policy Framework)の導入」では「金融」が65.8%、「エネルギー」が50.0%、「DKIM（DomainKeys Identified Mail）の導入」では「情報通信」が40.0%、「運輸業」が33.3%、「DMARC（Domain-based Message Authentication Reporting and Conformace）の導入」では「金融」が21.1%、「情報通信」が20.0%で高くなっている。「顧客に対する注意喚起」では「金融」が68.4%、「情報通信」が53.3%で高くなっている。

【業種別分析】フィッシング対策

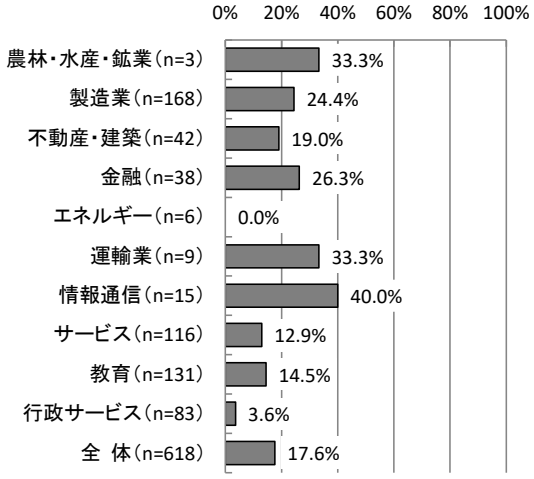
SPF(Sender Policy Framework)の導入



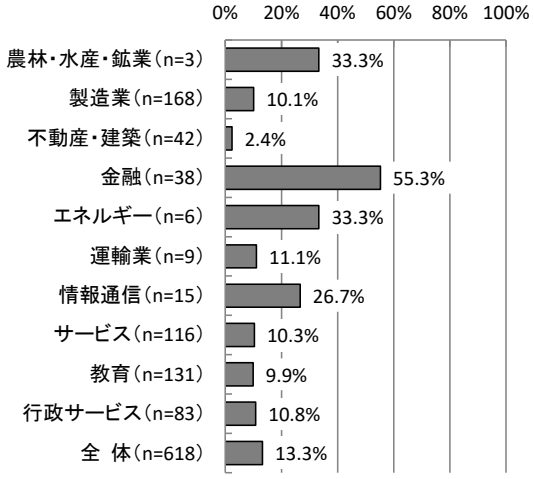
顧客に対する注意喚起



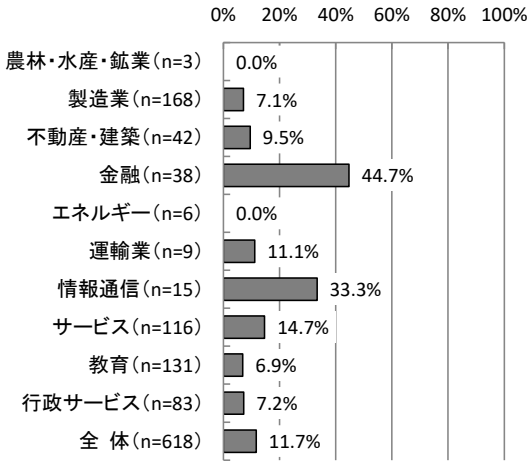
DKIM(DomainKeys Identified Mail)の導入



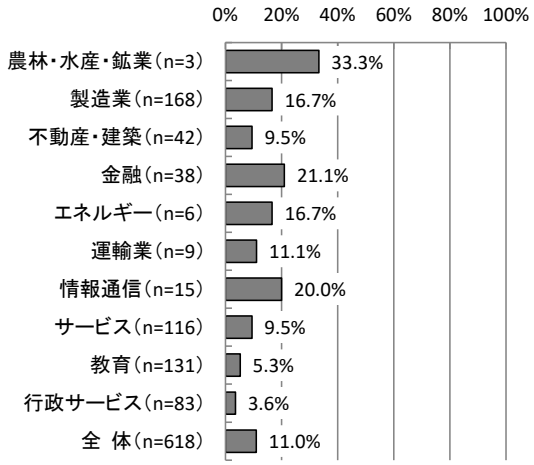
フィッシングサイト発見時の関係機関への通報



フィッシングサイトの監視



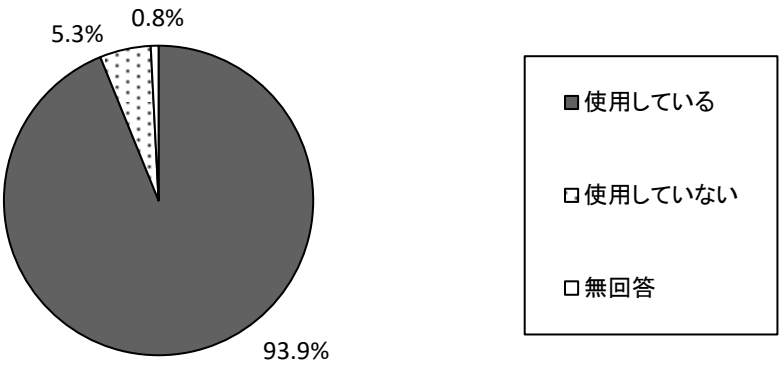
DMARC(Domain-based Message Authentication Reporting and Conformace)の導入



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

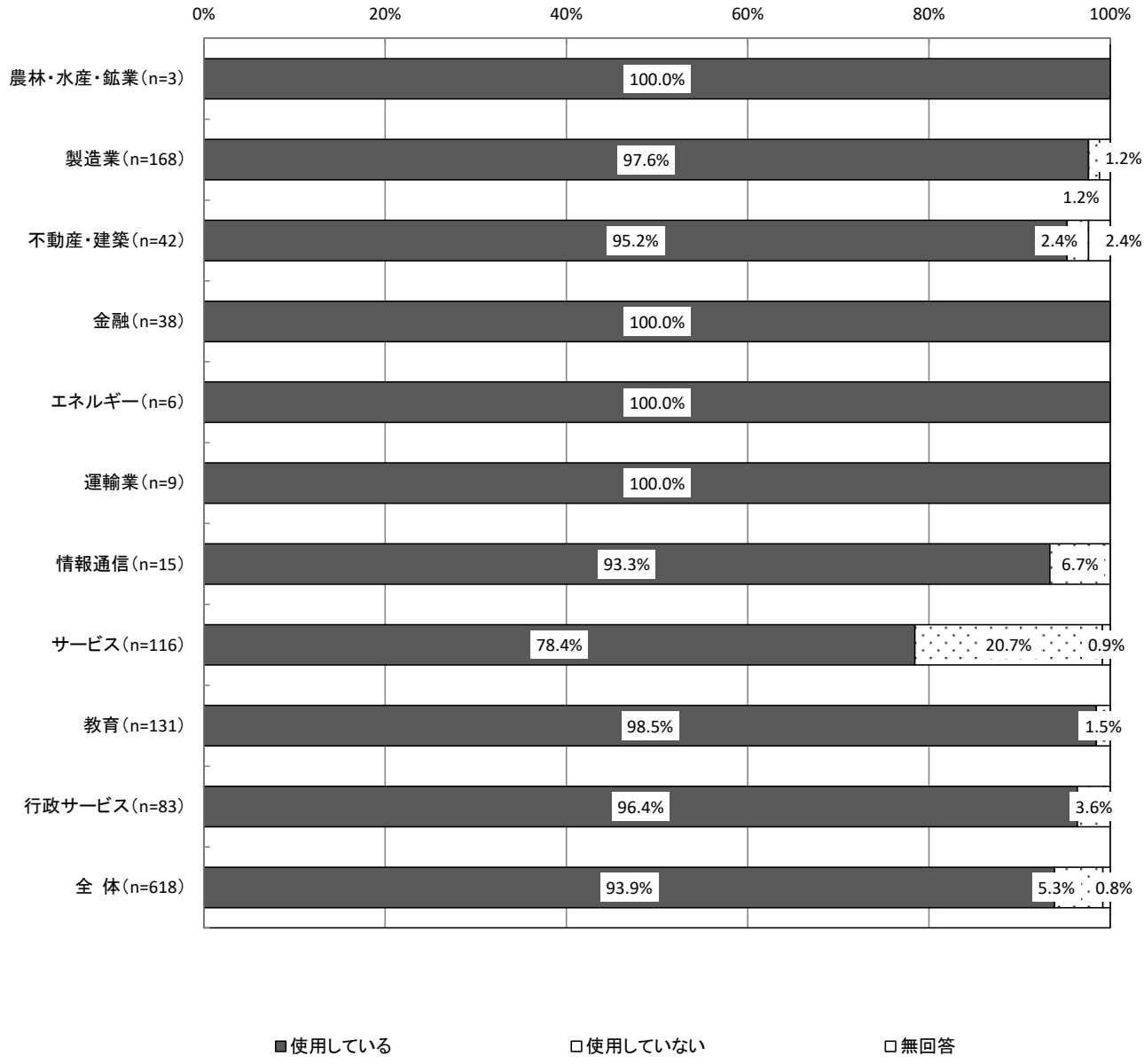
各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）の利用状況については、「使用している」が93.9%、「使用していない」が5.3%となっている。

【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=618）



【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」「エネルギー」「運輸業」で100.0％と高くなっている。90％を下回っているのは「サービス」の78.4％で「使用していない」が20.7％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）の利用状況

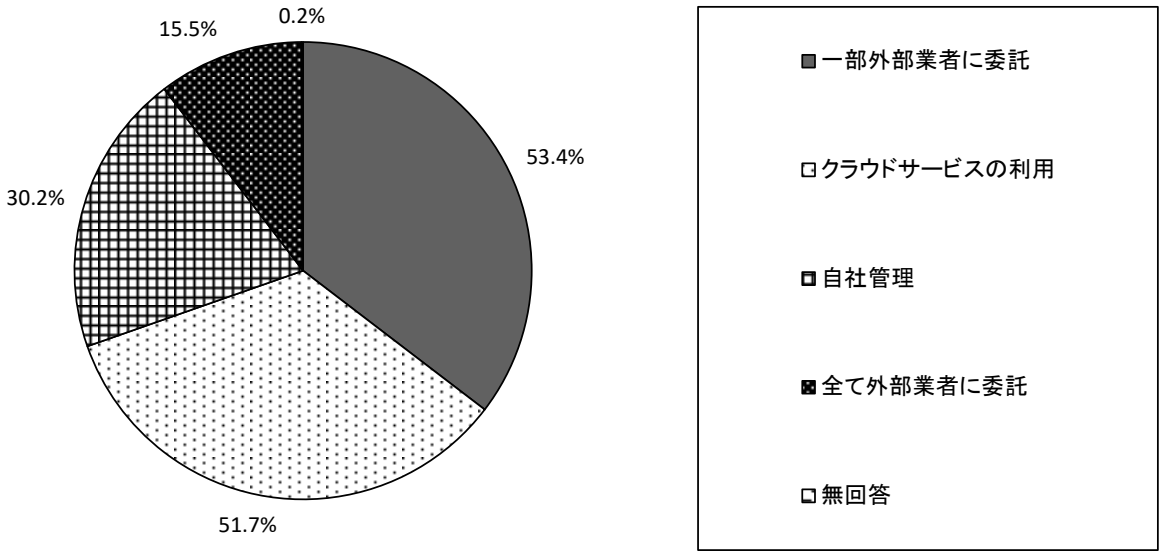


3.2.12　各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）の管理環境【問23-1】

各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）の管理環境については、「一部外部業者に委託」が53.4%で最も高く、次いで「クラウドサービスの利用」が51.7%、「自社管理」が30.2%となっている。

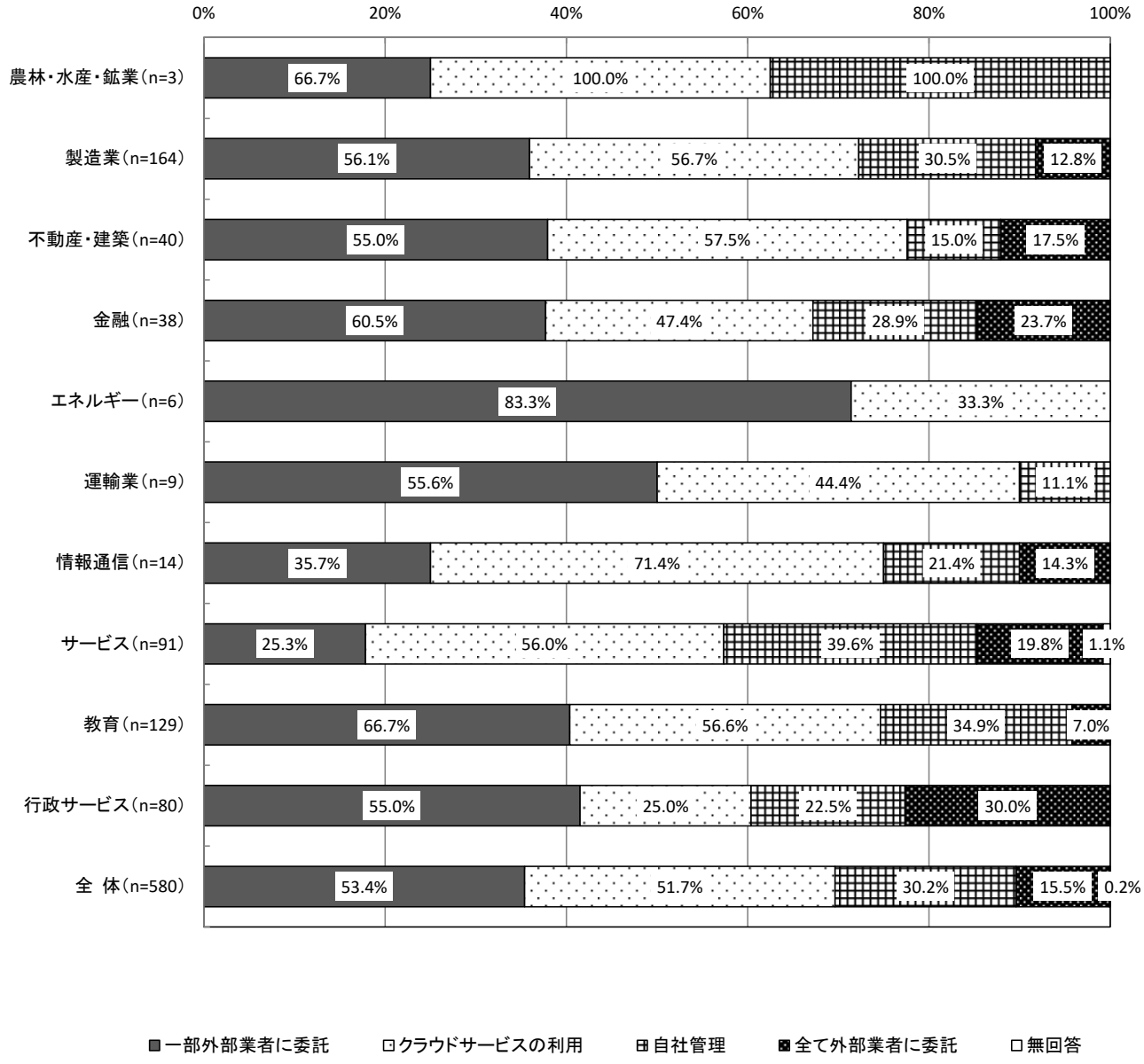
※本項目は、各種サービス（Webサイト、メール管理、ファイル管理等）を使用している社・団体等を対象としている。

【全体】各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）の管理環境（SA,n=580）



【業種別分析】業種別にみると、「一部外部業者に委託」については、「エネルギー」が83.3%で最も高く、「サービス」が25.3%で少なくなっている。「クラウドサービスの利用」については、「情報通信」が71.4%で最も高く、「行政サービス」が25.0%で最も少なくなっている。

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

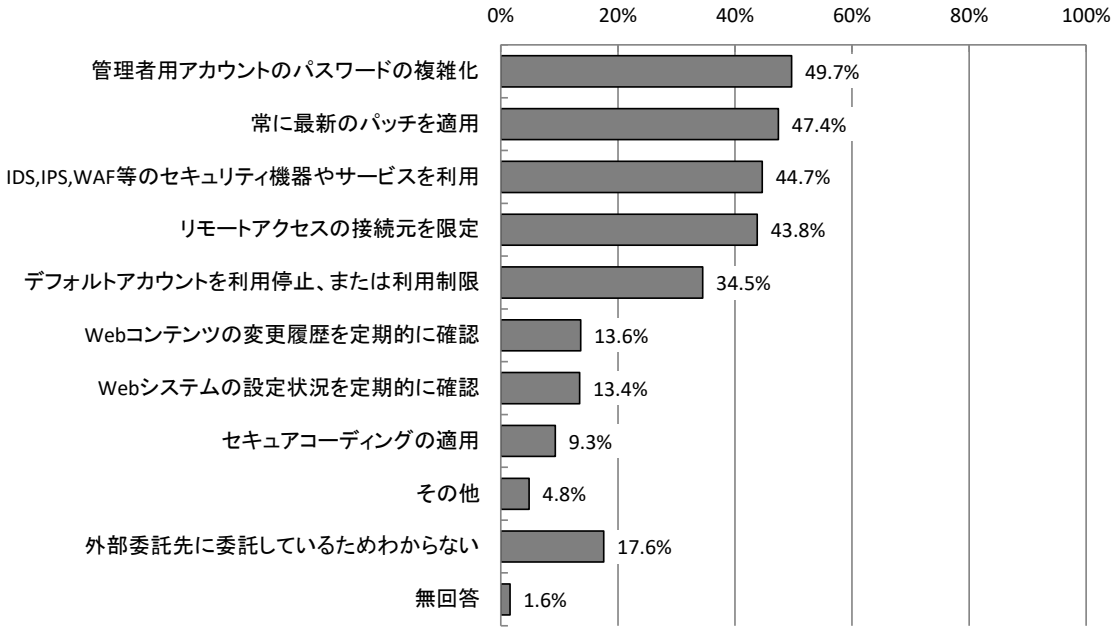


3.2.13 各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）のセキュリティ対策【問23-2】

各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）のセキュリティ対策については、「管理者用アカウントのパスワードの複雑化」が49.7%で最も高く、次いで「常に最新のパッチを適用」が47.4%、「IDS,IPS,WAF等のセキュリティ機器やサービスを利用」が44.7%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。

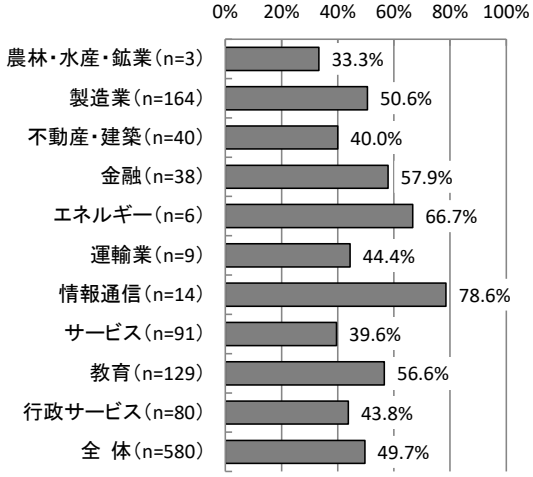
【全体】各種サービス（Ｗｅｂサイト、メール管理、ファイル管理等）のセキュリティ対策（MA,n=580）



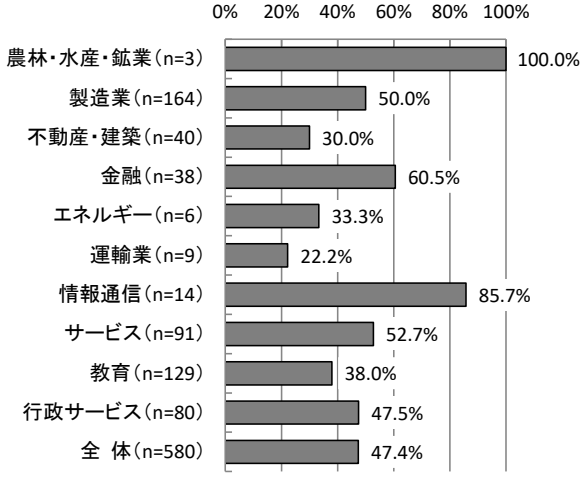
【業種別分析】業種別に見ると、「管理者用アカウントのパスワードの複雑化」については、「情報通信」が78.6%、「エネルギー」が66.7%で高くなっている。「常に最新のパッチを適用」については、「情報通信」が85.7%、「金融」が60.5%で高くなっている。

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

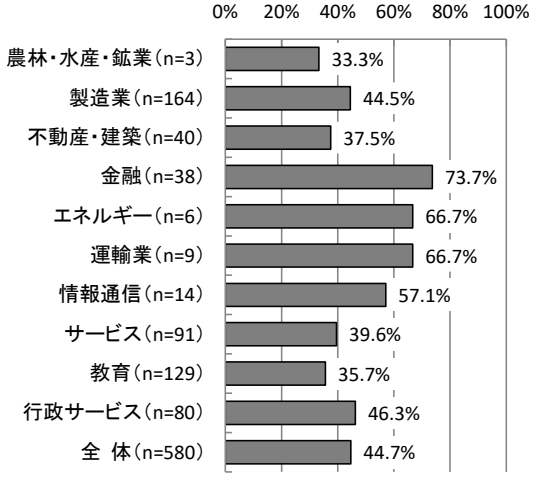
管理者用アカウントのパスワードの複雑化



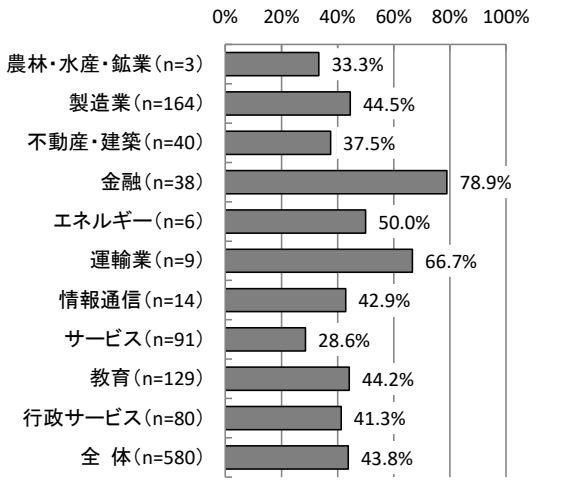
常に最新のパッチを適用



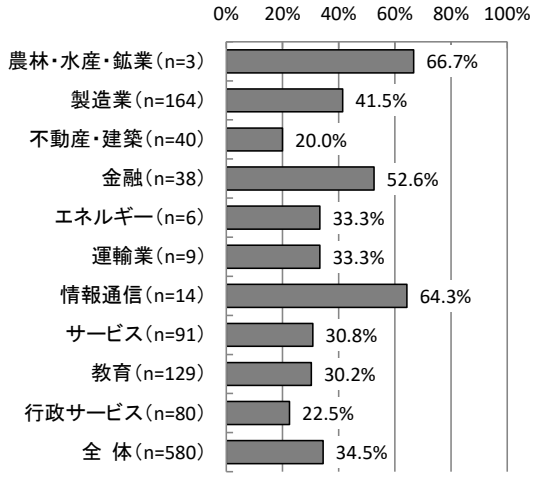
IDS,IPS,WAF等のセキュリティ機器やサービスを利用



リモートアクセスの接続元を限定



デフォルトアカウントを利用停止、または利用制限

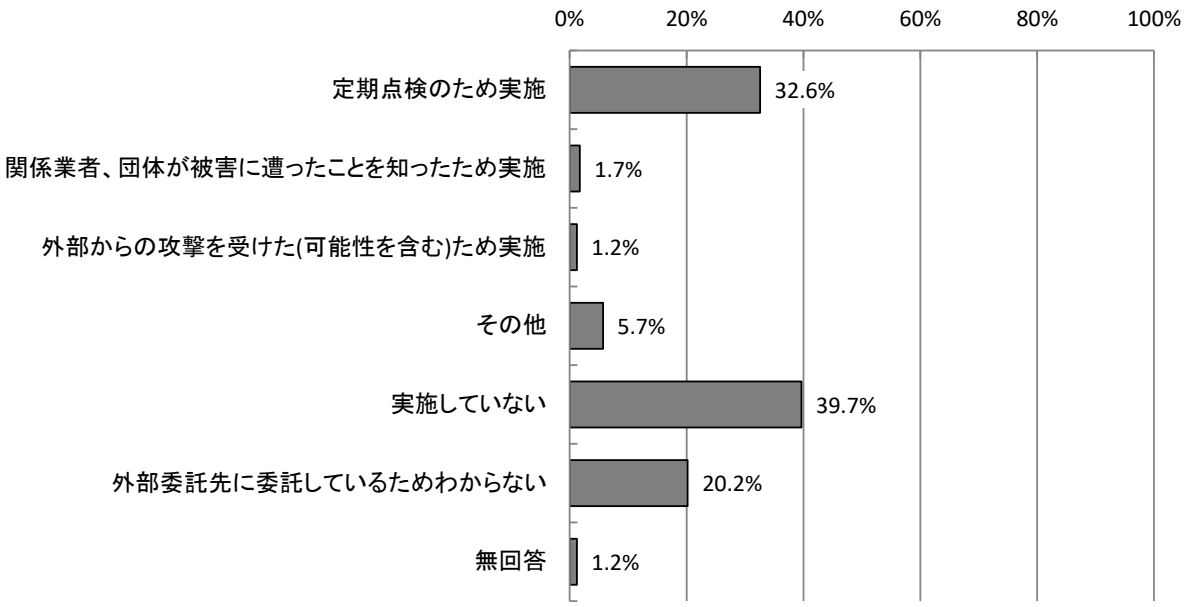


3.2.14　ぜい弱性調査（ペネトレーションテスト）実施の有無　【問23-3】

ぜい弱性調査（ペネトレーションテスト）実施の有無については、「実施していない」が39.7%と4割近くで最も高い。実施しているとの回答では、「定期点検のため実施」が32.6%と多くなっている。

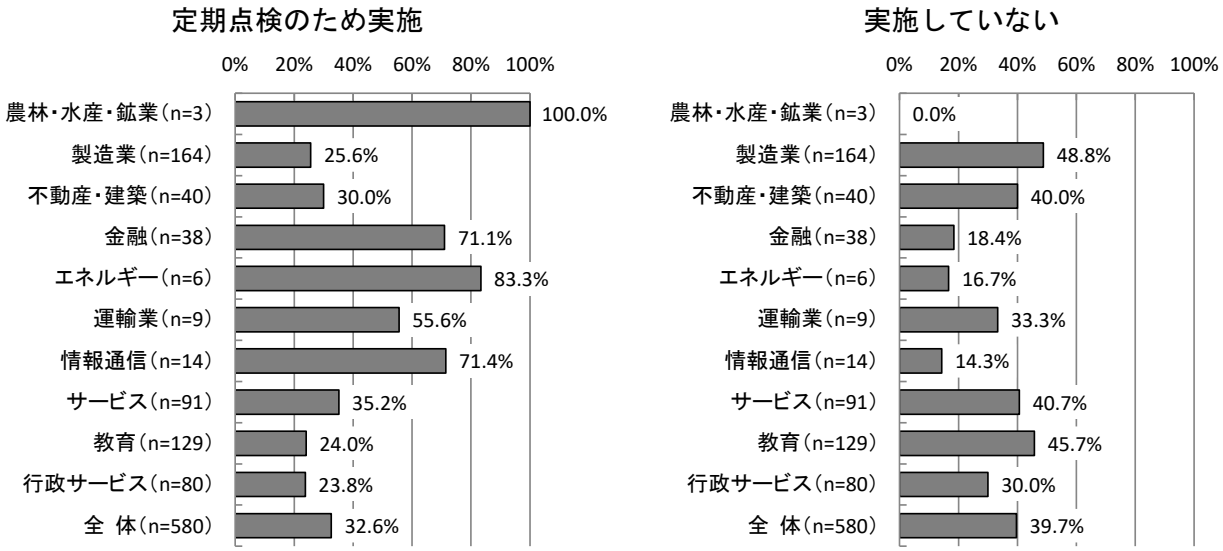
※本項目は、各種サービスの全部又は一部を自社で管理している社・団体等を対象としている。

【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=580）



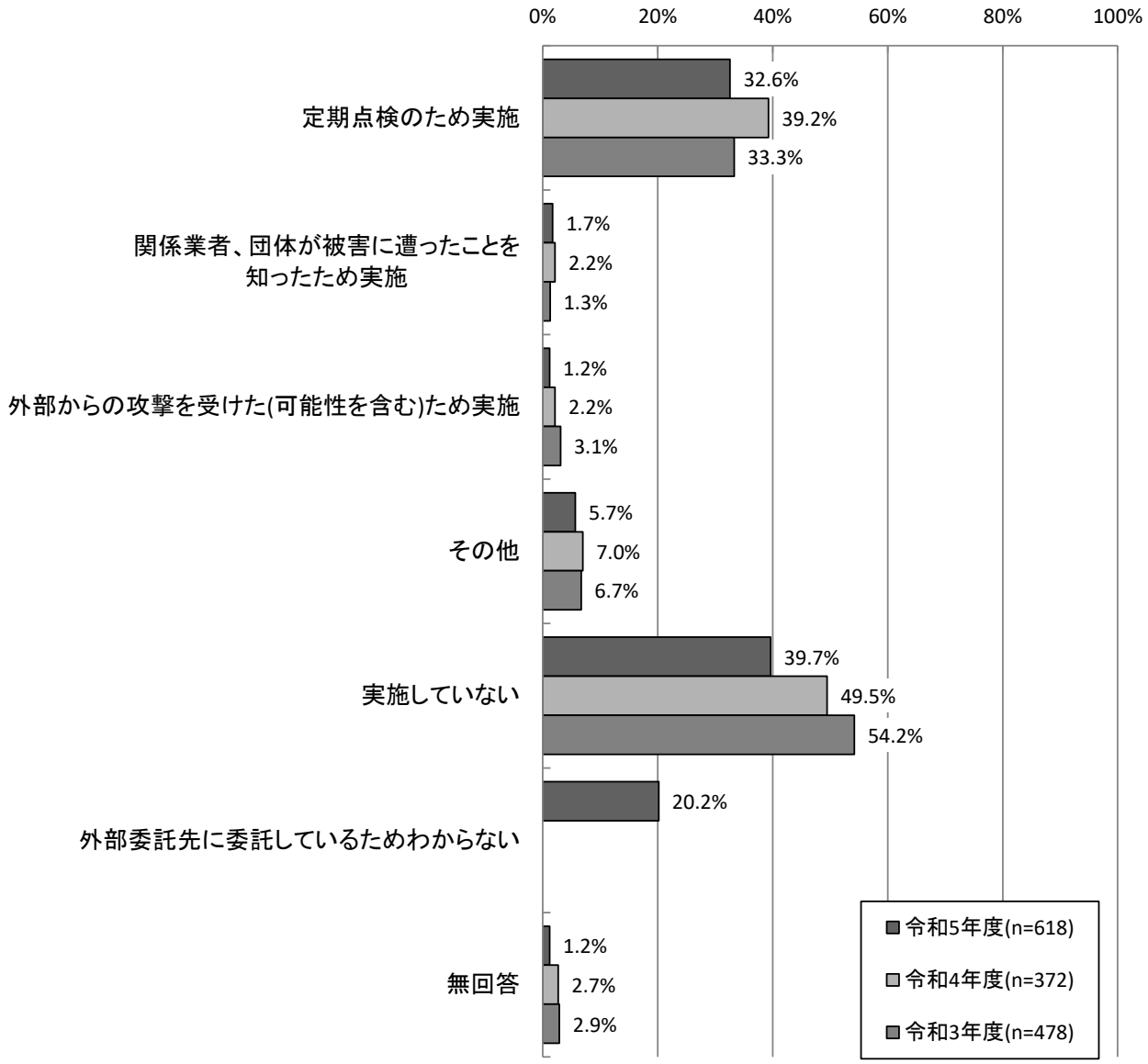
【業種別分析】業種別にみると、「定期点検のため実施」については、「エネルギー」が83.3%で最も高く、次いで「情報通信」が71.4%となっている。一方、「実施していない」については、「製造業」が48.8%、「教育」が45.7%で高くなっている。

【業種別分析】ぜい弱性調査（ペネトレーションテスト）実施の有無



【経年変化】昨年度と比較すると、「実施していない」が 9.8 ポイント、「定期点検のため実施」が 6.6 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



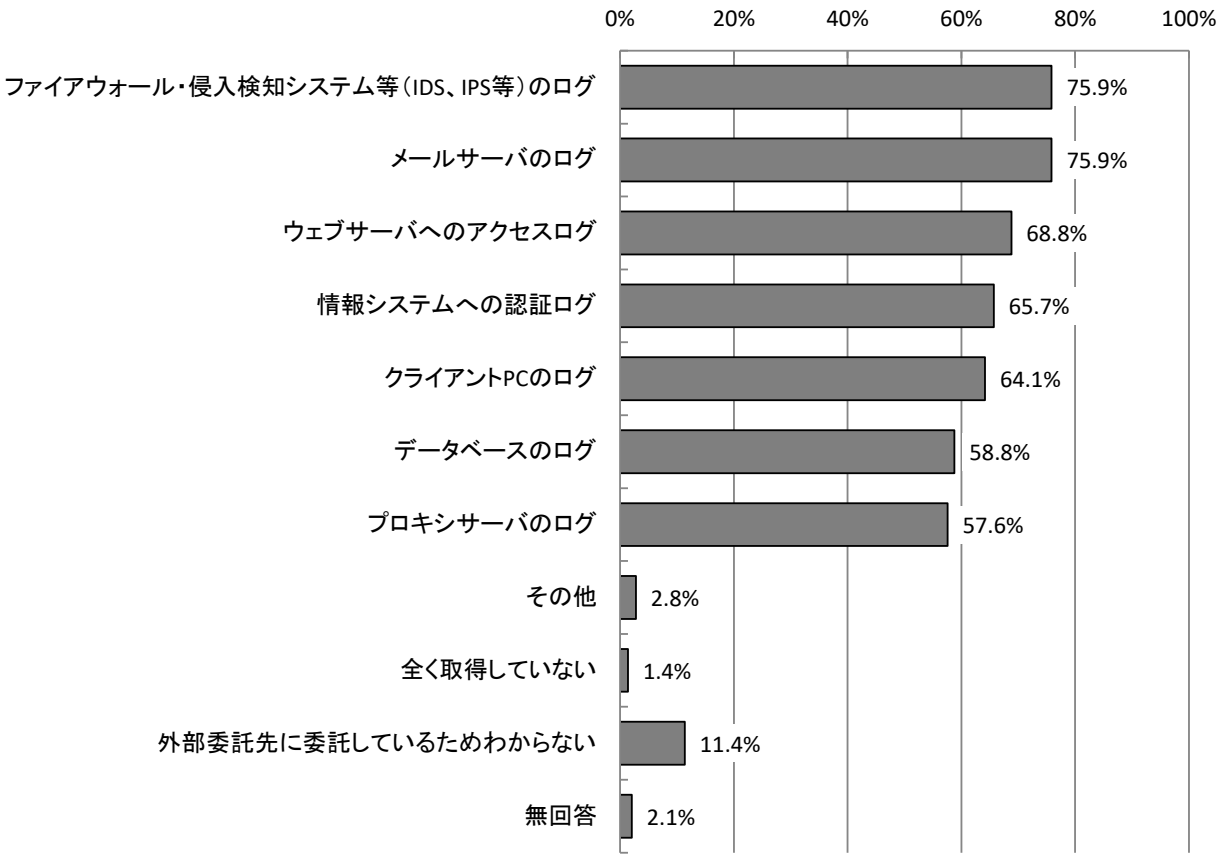
※令和5年度調査で、「外部委託先に委託しているためわからない」を新設。

3.2.15　ログの取得状況　【問23-4】

ログの取得状況については、「ファイアウォール・侵入検知システム等（IDS、IPS等）のログ」「メールサーバのログ」がいずれも75.9%で最も高く、「ウェブサーバへのアクセスログ」が68.8%、「情報システムへの認証ログ」が65.7%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。

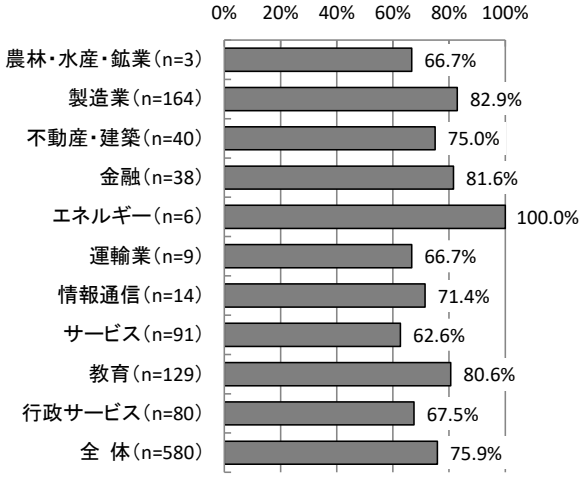
【全体】ログの取得状況（MA, n=580）



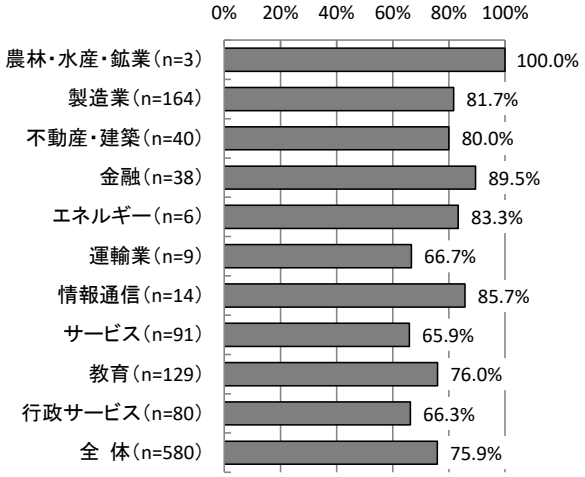
【業種別分析】業種別にみると、「ファイアウォール・侵入検知システム等（IDS、IPS等）のログ」では、「エネルギー」が100.0%、「製造業」が82.9%、「金融」が81.6%、「教育」が80.6%で高い。「メールサーバのログ」では「金融」が89.5%、「情報通信」が85.7%で高くなっている。

【業種別分析】ログの取得状況

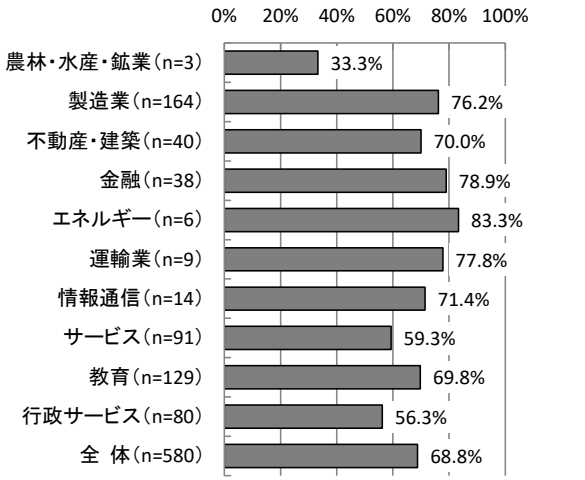
ファイアウォール・侵入検知システム等（IDS、IPS等）のログ



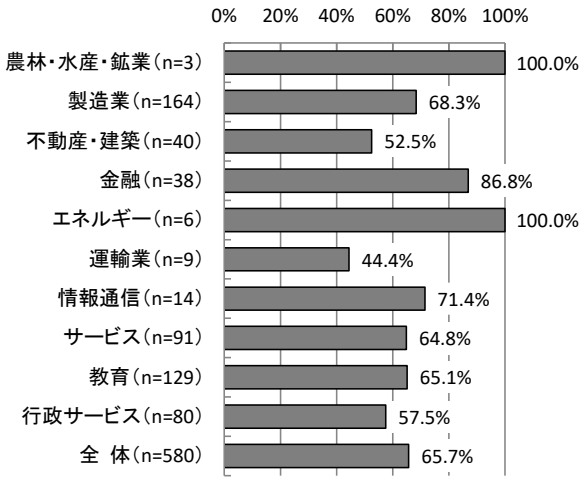
メールサーバのログ



ウェブサーバへのアクセスログ



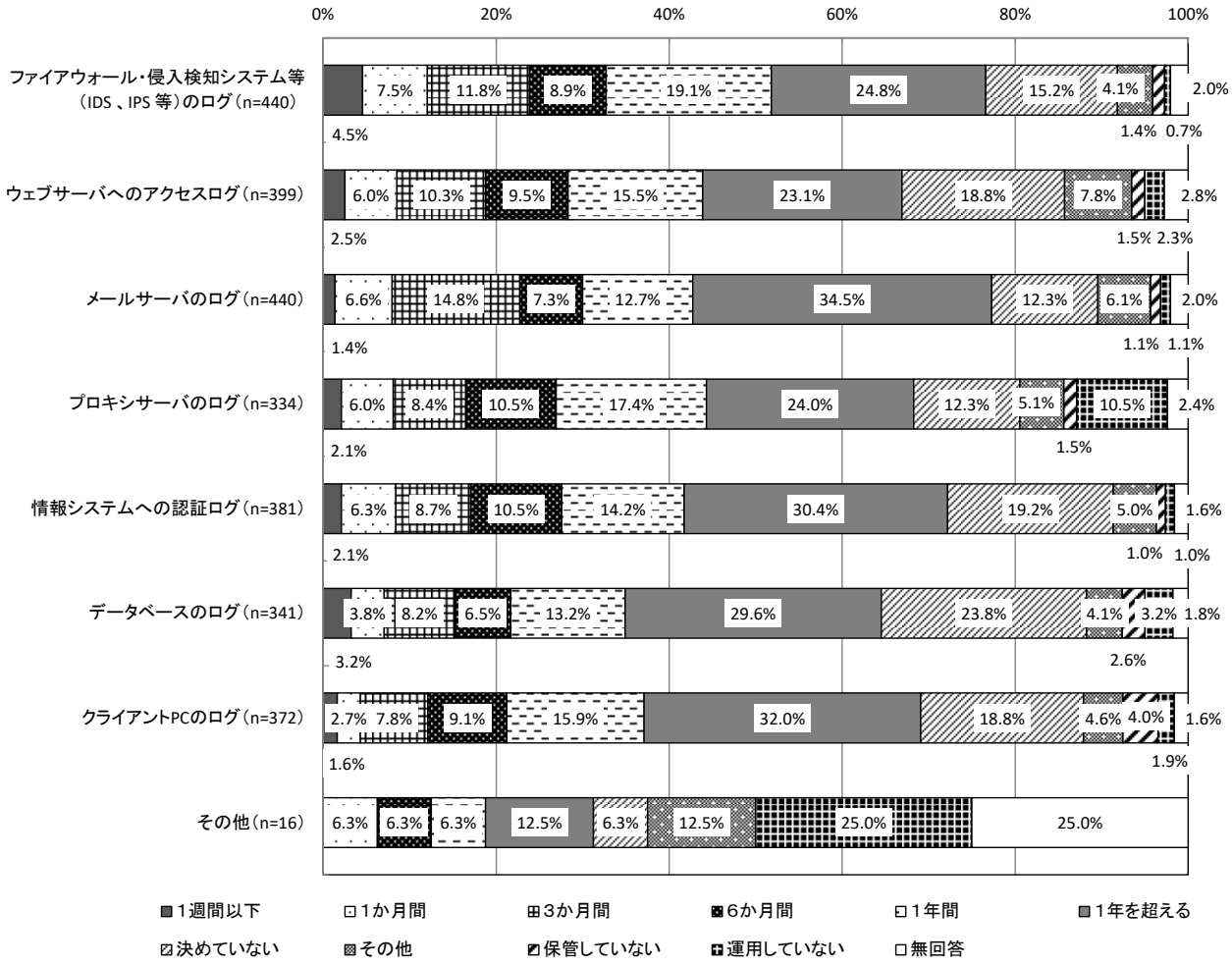
情報システムへの認証ログ



3.2.16　ログの保管期間　【問23-4A】

ログの保管期間については、いずれも「１年を超える」が最も高い割合となっている。

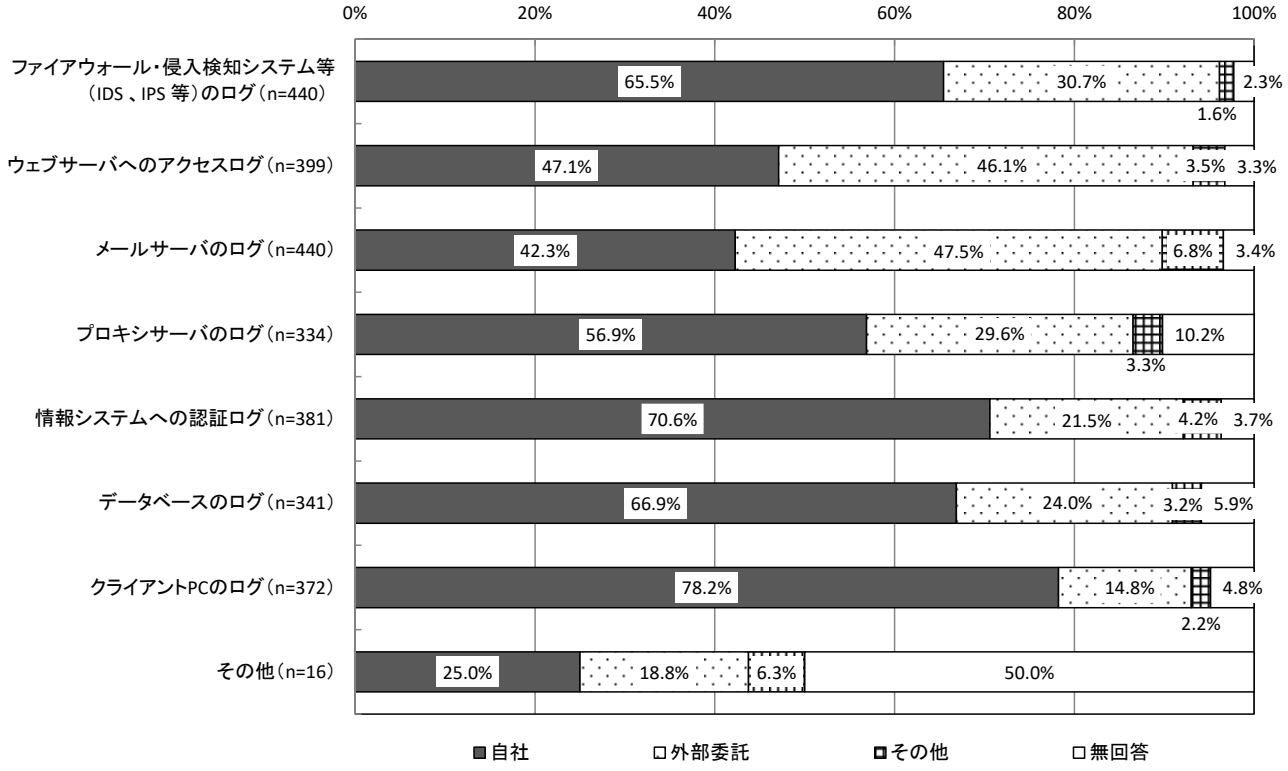
【全体】ログの保管期間



3.2.17　ログの保管方法　【問23-4B】

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

【全体】ログの保管方法

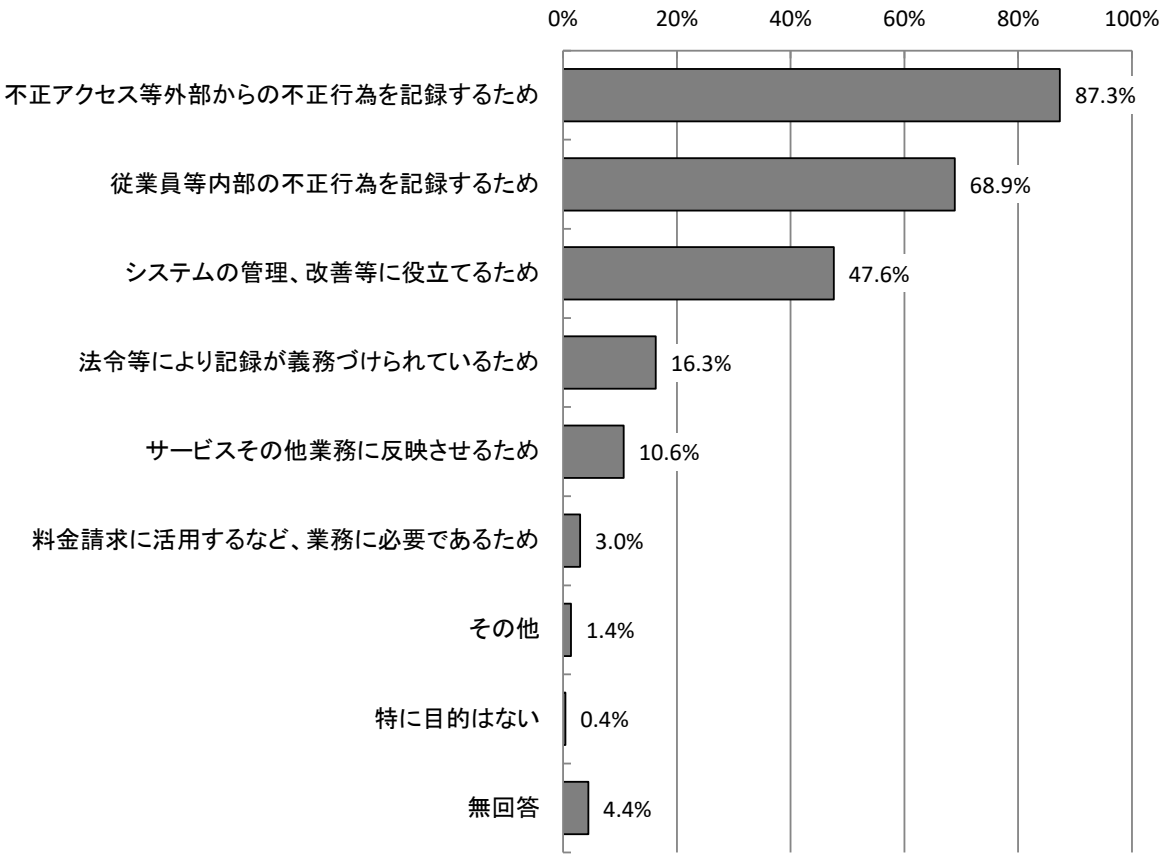


3.2.18　ログを取得・保管している理由　【問23-4-1】

ログを取得・保管している理由については、「不正アクセス等外部からの不正行為を記録するため」が87.3%と最も高く、次いで「従業員等内部の不正行為を記録するため」が68.9%、「システムの管理、改善等に役立てるため」が47.6%となっている。

※本項目は、ログを取得している社・団体等を対象としている。

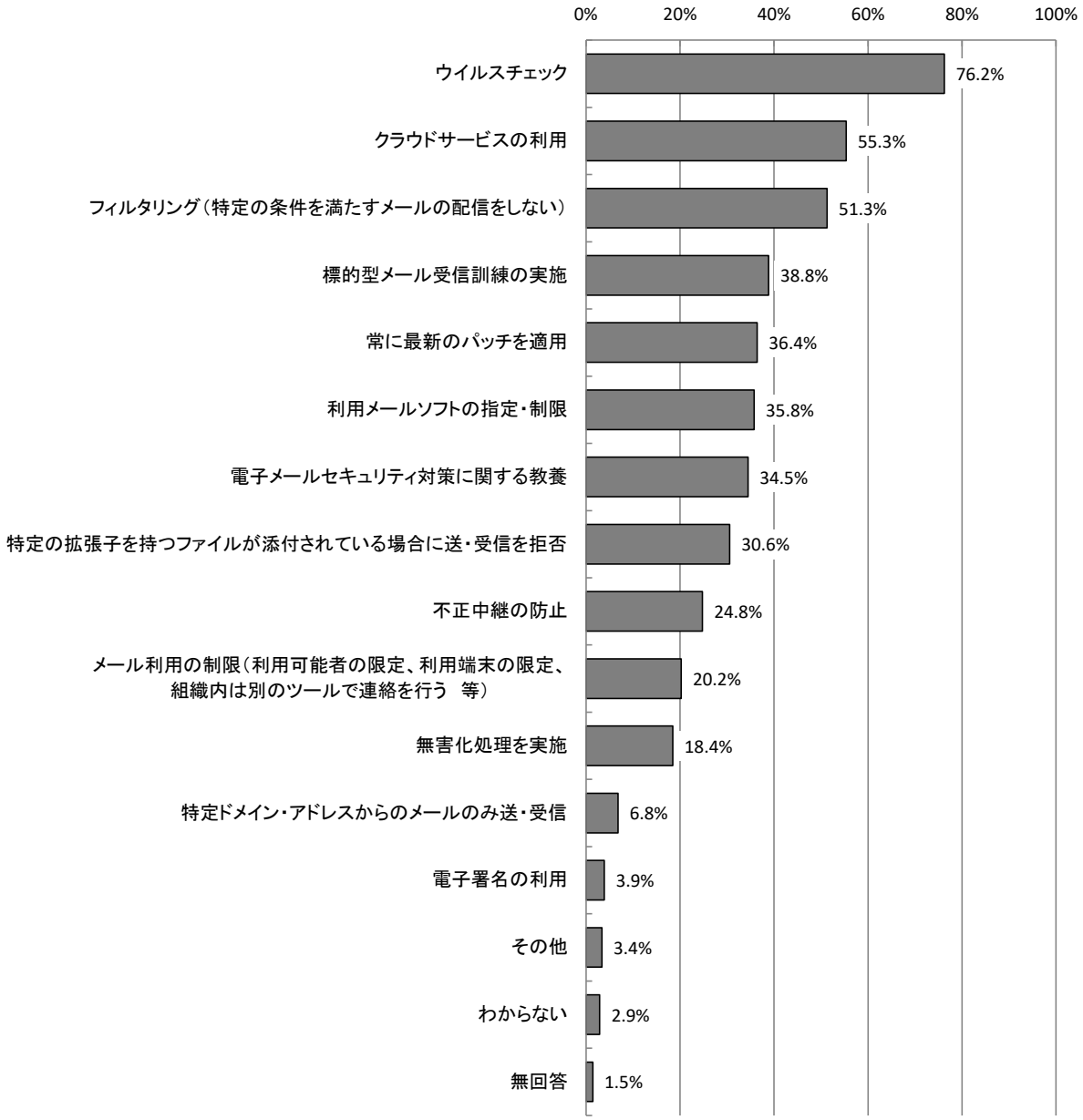
【全体】ログを取得・保管している理由（MA,n=498）



3.2.19　電子メールに関するセキュリティ対策　【問24】

電子メールに関するセキュリティ対策については、「ウイルスチェック」が76.2%で最も高く、次いで「クラウドサービスの利用」が55.3%、「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）」が51.3%となっている。

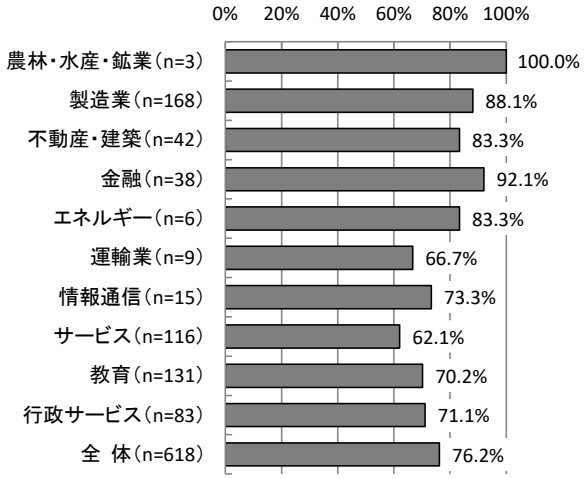
【全体】電子メールに関するセキュリティ対策（MA,n=618）



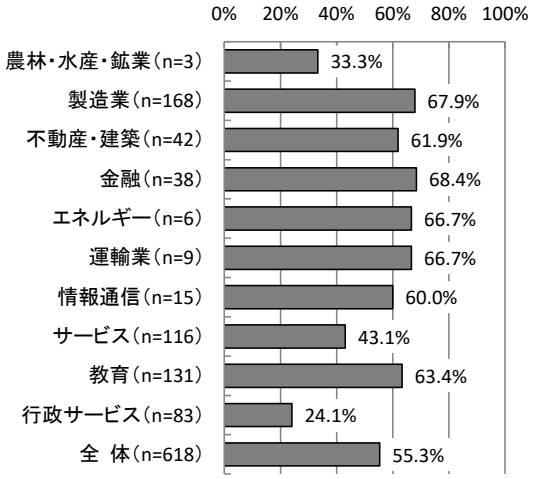
【業種別分析】業種別にみると、「ウイルスチェック」については、「金融」が92.1%と高く、次いで「製造業」が88.1%と高くなっている。「クラウドサービスの利用」については「金融」が68.4%、「フィルタリング（特定の条件を満たすメールの配信をしない）」については「エネルギー」が83.3%と高くなっている。

【業種別分析】電子メールに関するセキュリティ対策

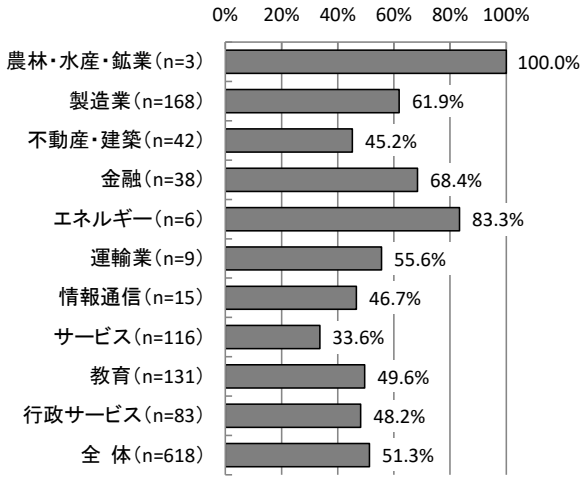
ウイルスチェック



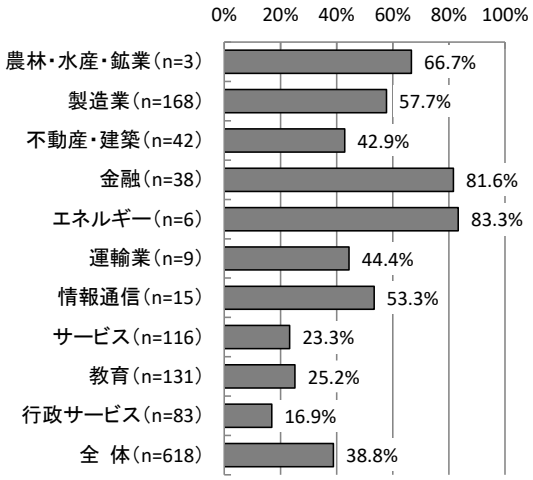
クラウドサービスの利用



フィルタリング
（特定の条件を満たすメールの配信をしない）



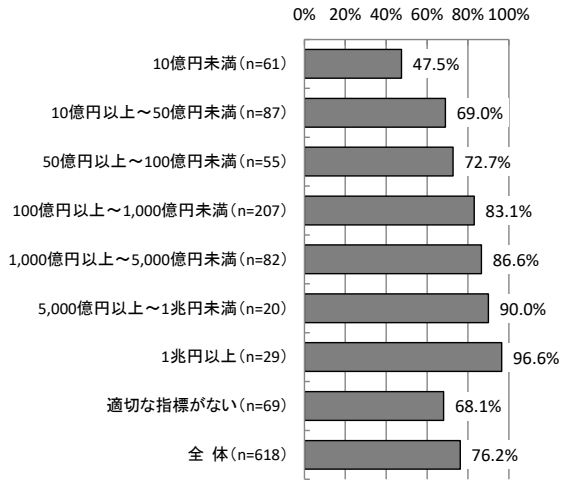
標的型メール受信訓練の実施



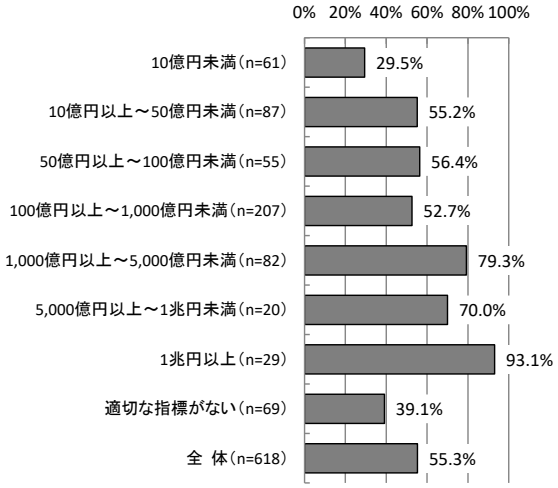
【予算規模別分析】予算規模別にみると、「ウイルスチェック」については、「1兆円以上」が96.6%で最も高く、次いで「5,000億円以上～1兆円未満」が90.0%となっている。「クラウドサービスの利用」についても「1兆円以上」が93.1%で最も高い。

【予算規模別分析】電子メールに関するセキュリティ対策

ウイルスチェック

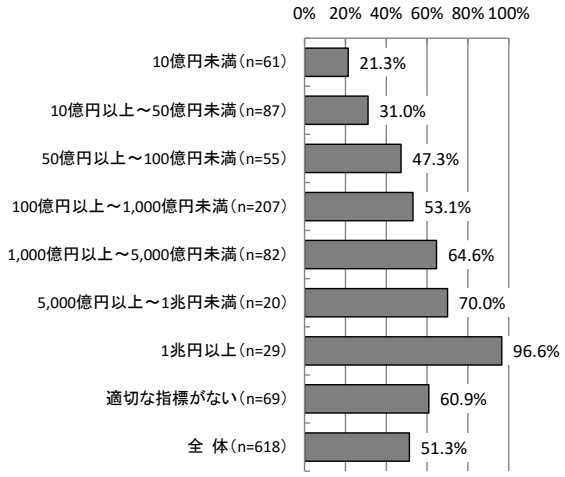


クラウドサービスの利用

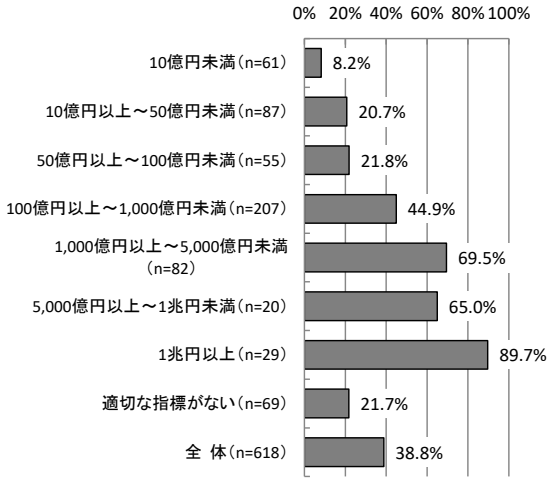


フィルタリング

（特定の条件を満たすメールの配信をしない）

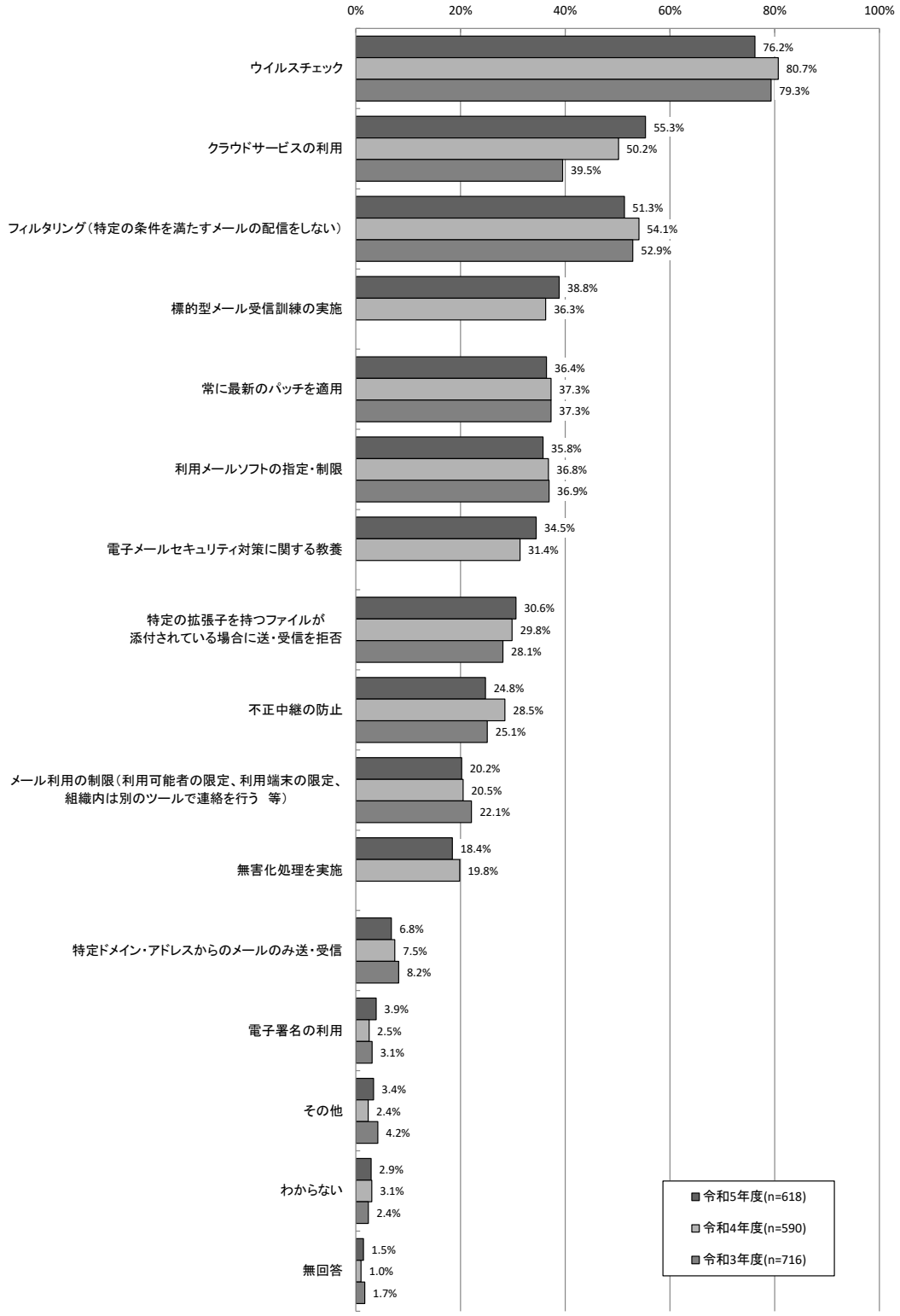


標的型メール受信訓練の実施



【経年変化】昨年度と比較すると、「クラウドサービスの利用」が5.1ポイント、「電子メールセキュリティ対策に関する教養」が3.1ポイント増加している。

【経年変化】電子メールに関するセキュリティ対策

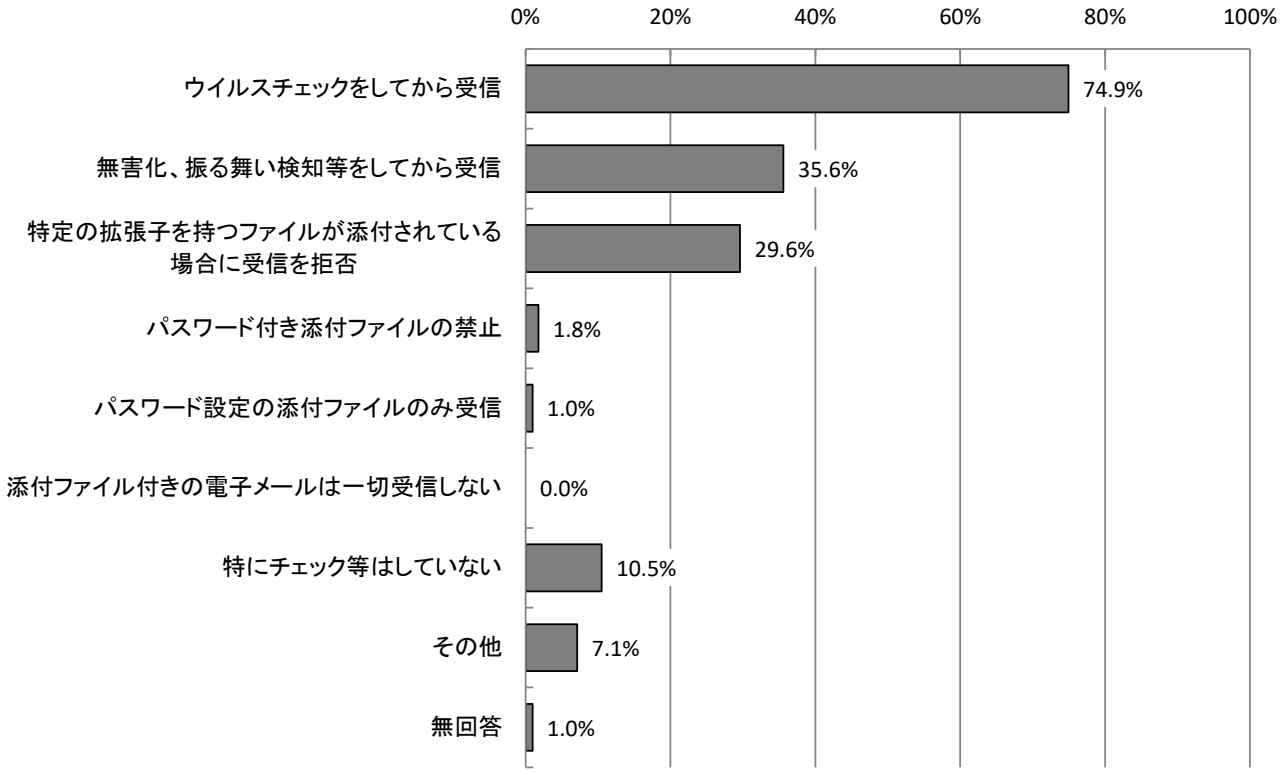


※令和４年度調査で、「無害化処理を実施」「標的型メール受信訓練の実施」「電子メールセキュリティ対策に関する教養」を新設。

3.2.20　添付ファイルの取り扱い　【問25】

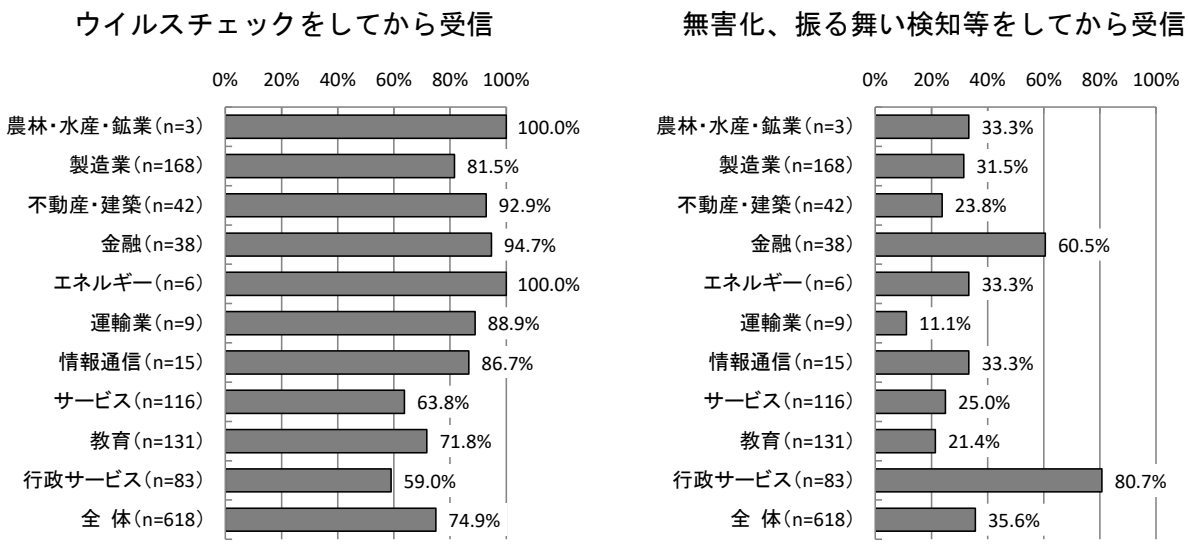
添付ファイルの取り扱いについては、「ウイルスチェックをしてから受信」が74.9%で最も高い。一方、「特にチェック等はしていない」は10.5%であった。

【全体】添付ファイルの取り扱い（MA,n=618）



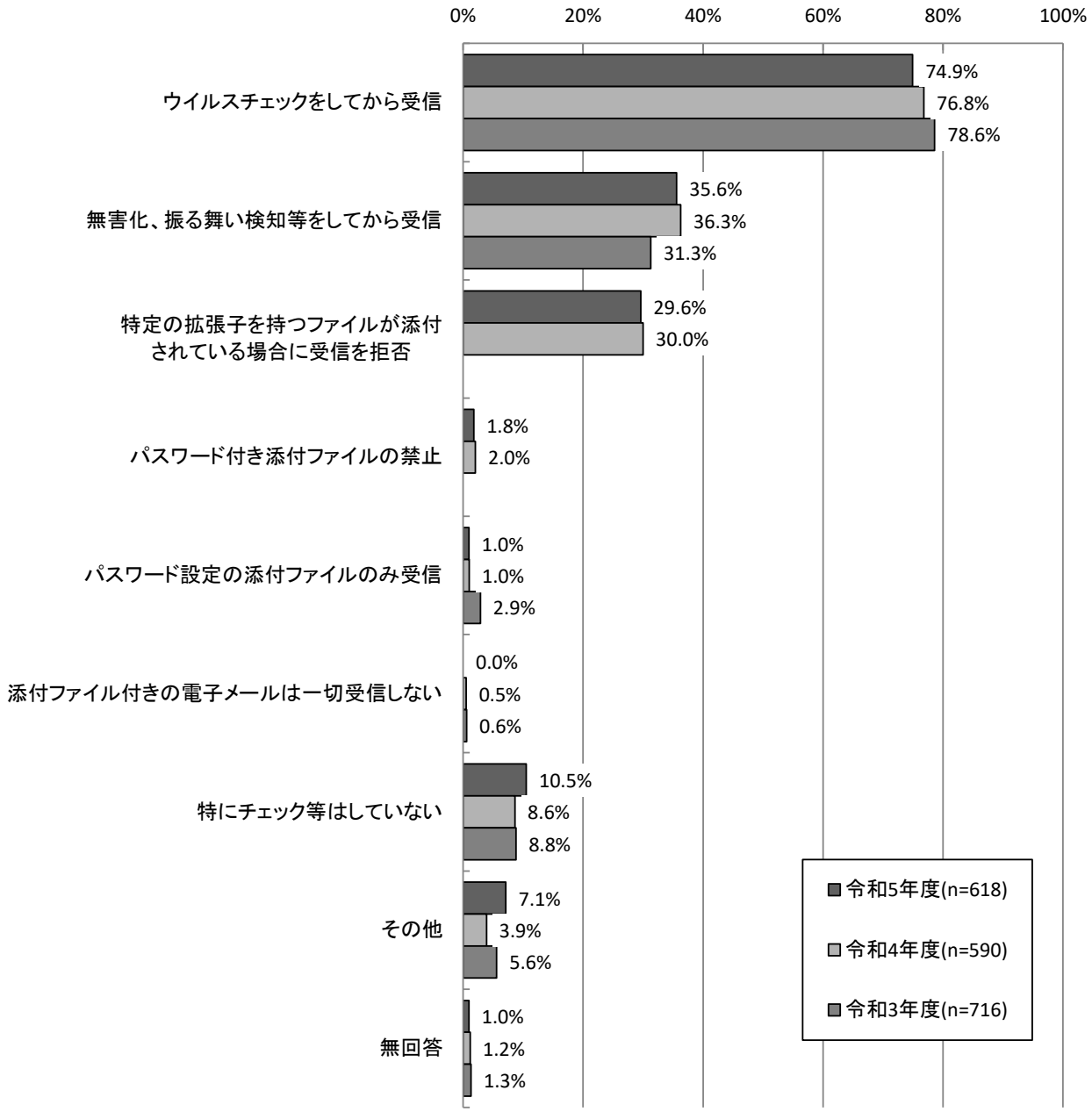
【業種別分析】業種別にみると、「ウイルスチェック等をしてから受信」は「エネルギー」で 100.0%、「金融」で 94.7%、「不動産・建築」で 92.9%となっている。

【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、「ウイルスチェックをしてから受信」が1.9ポイント減少し、「特にチェック等はしていない」が1.9ポイント増加している。

【経年変化】添付ファイルの取り扱い

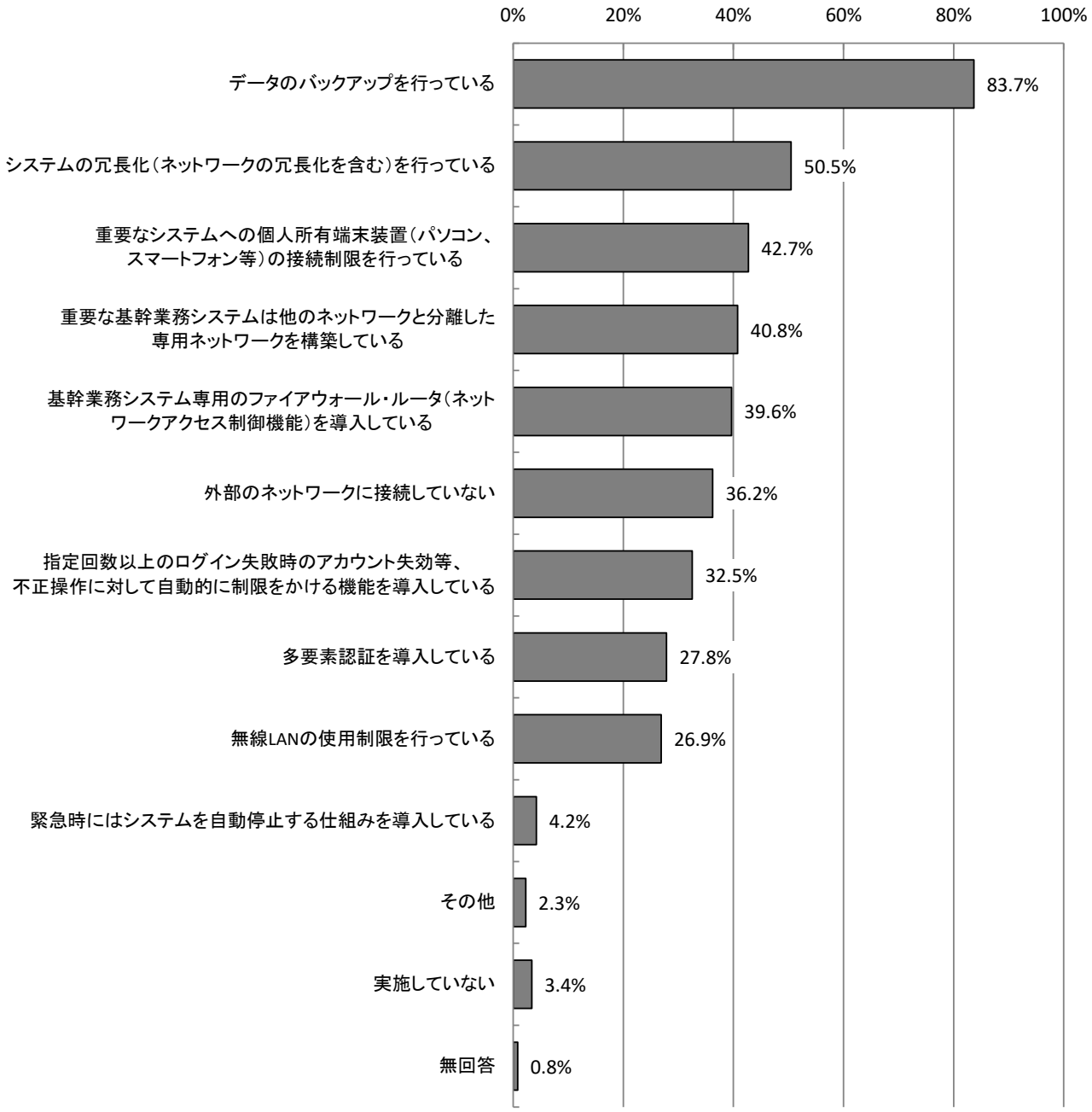


※令和４年度調査で、「特定の拡張子を持つファイルが添付されている場合に受信を拒否」「パスワード付き添付ファイルの禁止」を新設。

3.2.21　重要システムの不正アクセス対策状況　【問26】

重要システムの不正アクセス対策状況については、「データのバックアップを行っている」が83.7%で最も高く、「システムの冗長化（ネットワークの冗長化を含む）を行っている」が50.5%、「重要なシステムへの個人所有端末装置（パソコン、スマートフォン等）の接続制限を行っている」が42.7%、「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」が40.8%となっている。

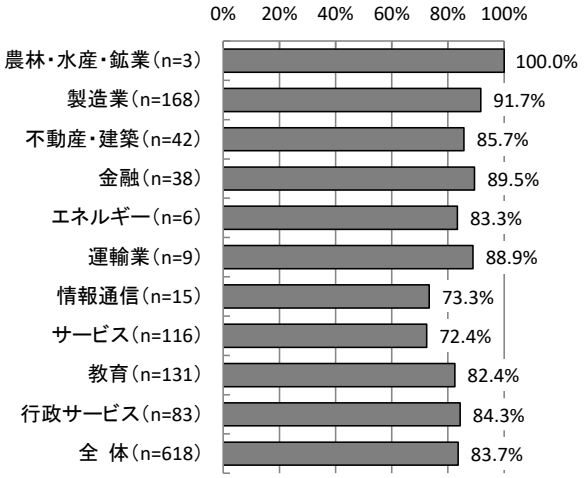
【全体】重要システムの不正アクセス対策状況（MA,n=618）



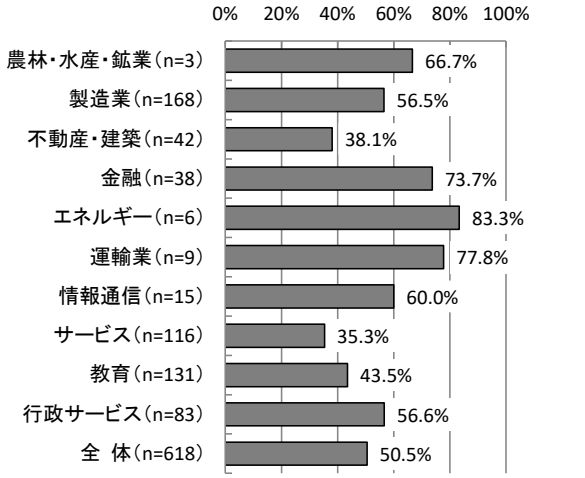
【業種別分析】業種別にみると、「データのバックアップを行っている」については、「製造業」が91.7%で高くなっている。「システムの冗長化（ネットワークの冗長化を含む）を行っている」については、「エネルギー」が83.3%、「運輸業」が77.8%、「金融」が73.7%で高くなっている。

【業種別分析】重要システムの不正アクセス対策状況

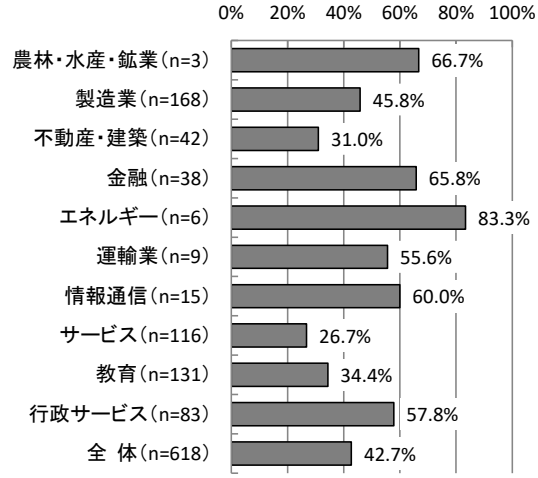
データのバックアップを行っている



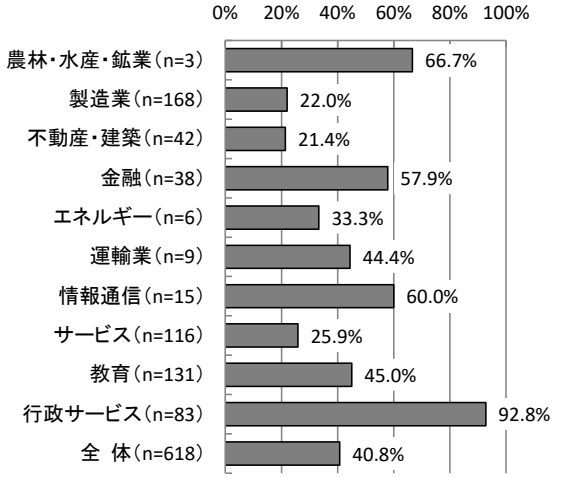
システムの冗長化
（ネットワークの冗長化を含む）を行っている



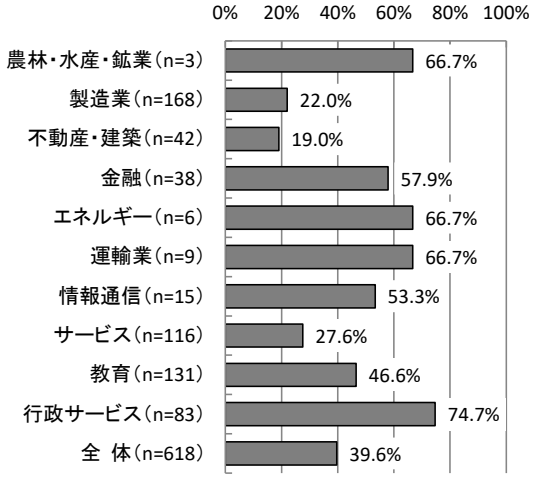
重要なシステムへの個人所有端末装置（パソコン、スマートフォン等）の接続制限を行っている



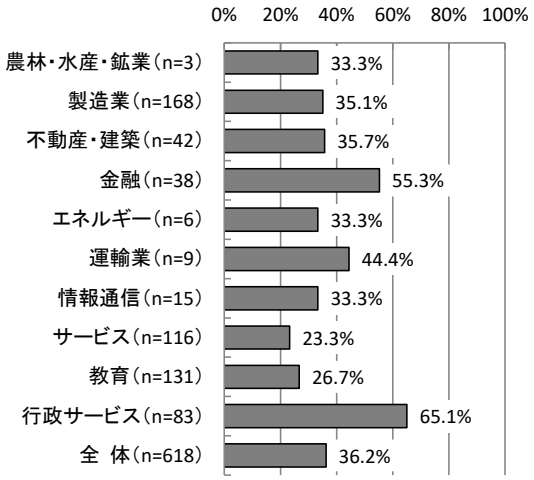
重要な基幹業務システムは他のネットワークと分離した専用ネットワークを構築している



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

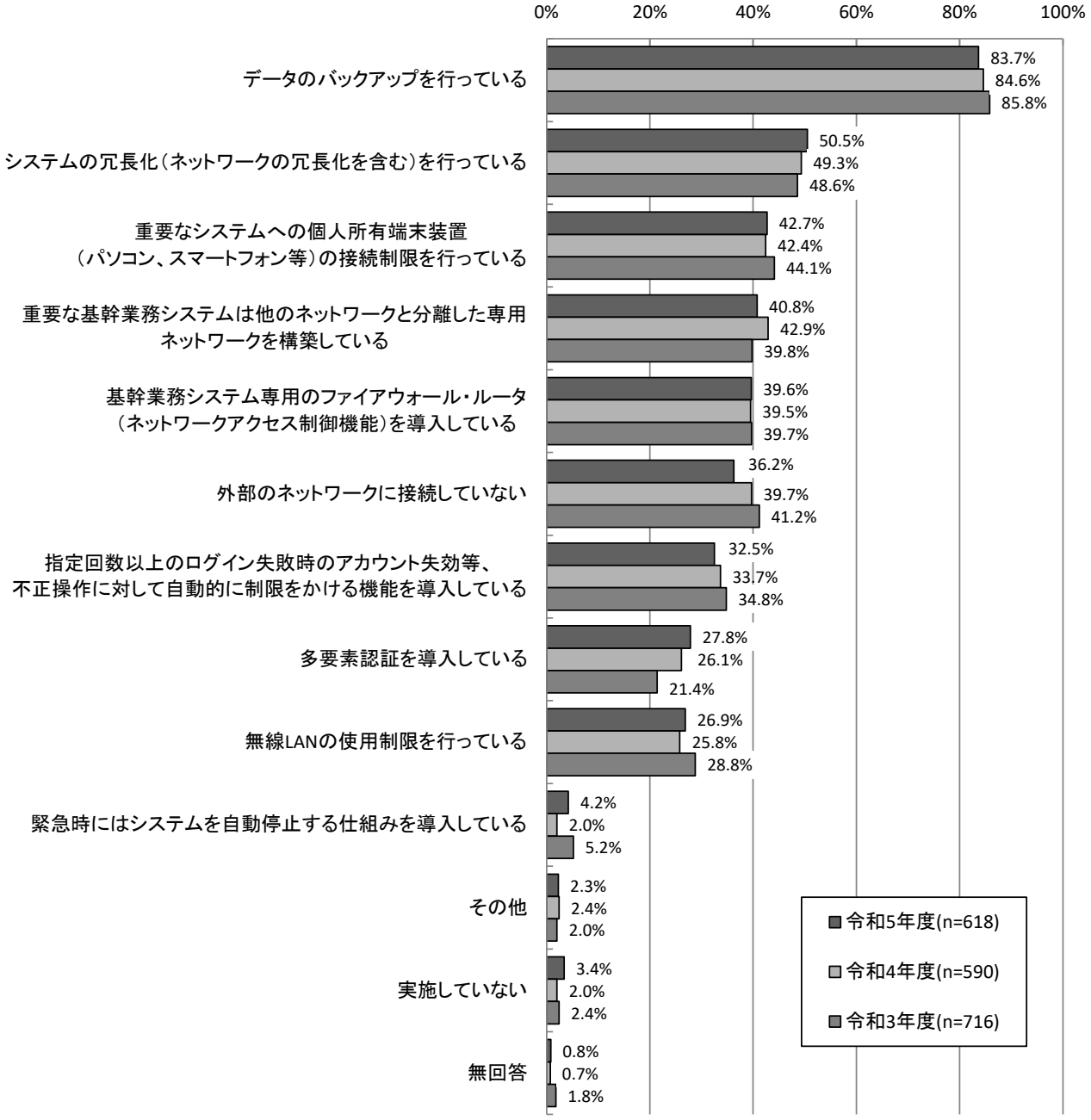


外部のネットワークに接続していない



【経年変化】昨年度と比較すると、「外部のネットワークに接続していない」が 3.5 ポイント減少している。一方、「緊急時にはシステムを自動停止する仕組みを導入している」が 2.2 ポイント、「多要素認証を導入している」が 1.7 ポイントの増加となっている。

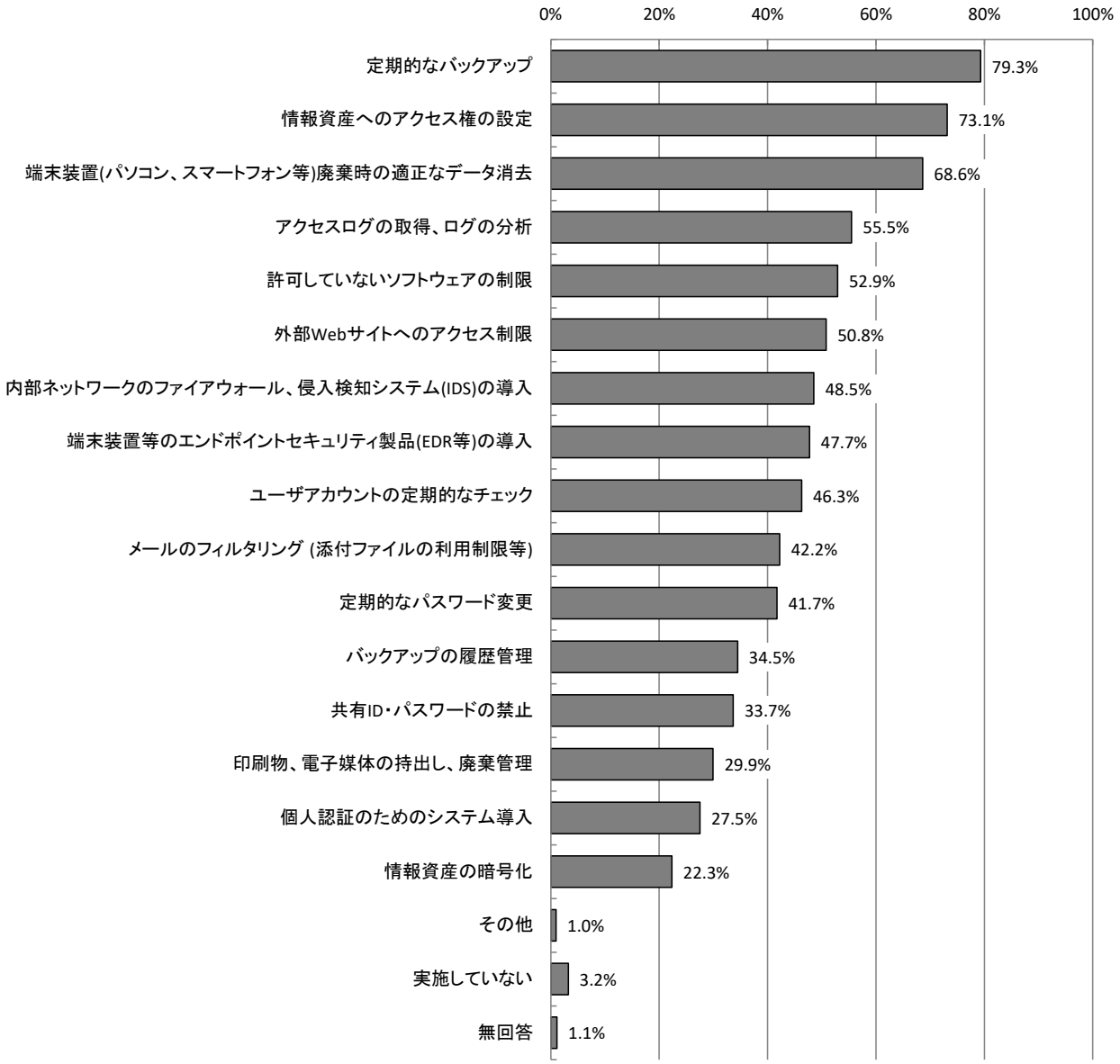
【経年変化】重要システムの不正アクセス対策状況



3.2.22　不正アクセス等への対策状況　【問27】

不正アクセス等への対策状況については、「定期的なバックアップ」が79.3%で最も高く、次いで「情報資産へのアクセス権の設定」が73.1%、「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68.6%となっている。

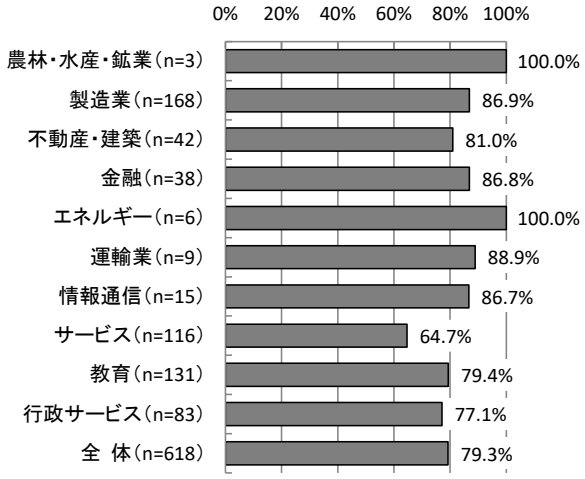
【全体】不正アクセス等への対策状況（MA, n=618）



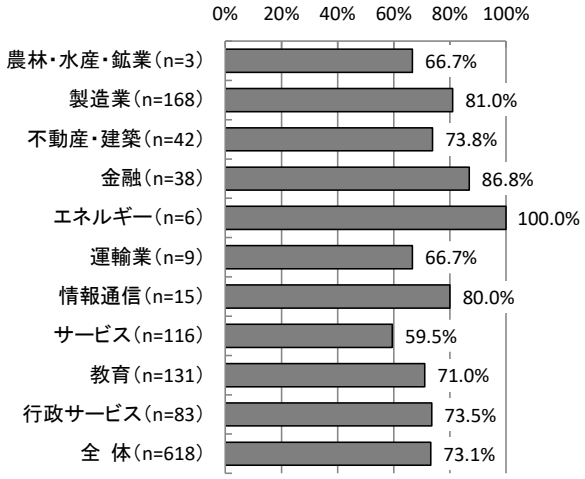
【業種別分析】業種別にみると、「定期的なバックアップ」は「エネルギー」が100.0%で高く、「製造業」「不動産・建築」「金融」「運輸業」「情報通信」で80%以上となっている。「情情報資産へのアクセス権の設定」は「エネルギー」が100.0%、「金融」が86.8%で高くなっている。

【業種別分析】不正アクセス等への対策状況

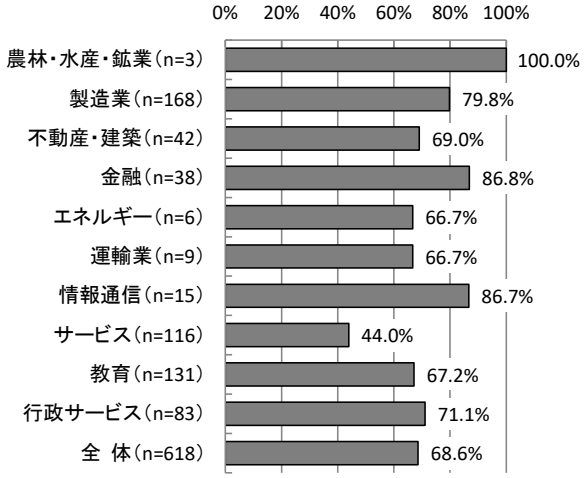
定期的なバックアップ



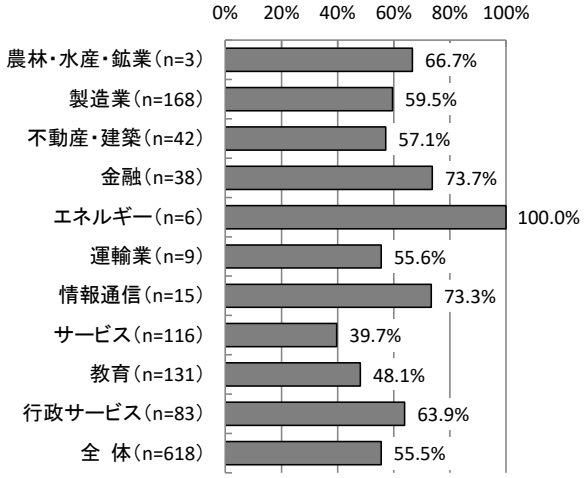
情報資産へのアクセス権の設定



端末装置(パソコン、スマートフォン等)廃棄時の適正なデータ消去

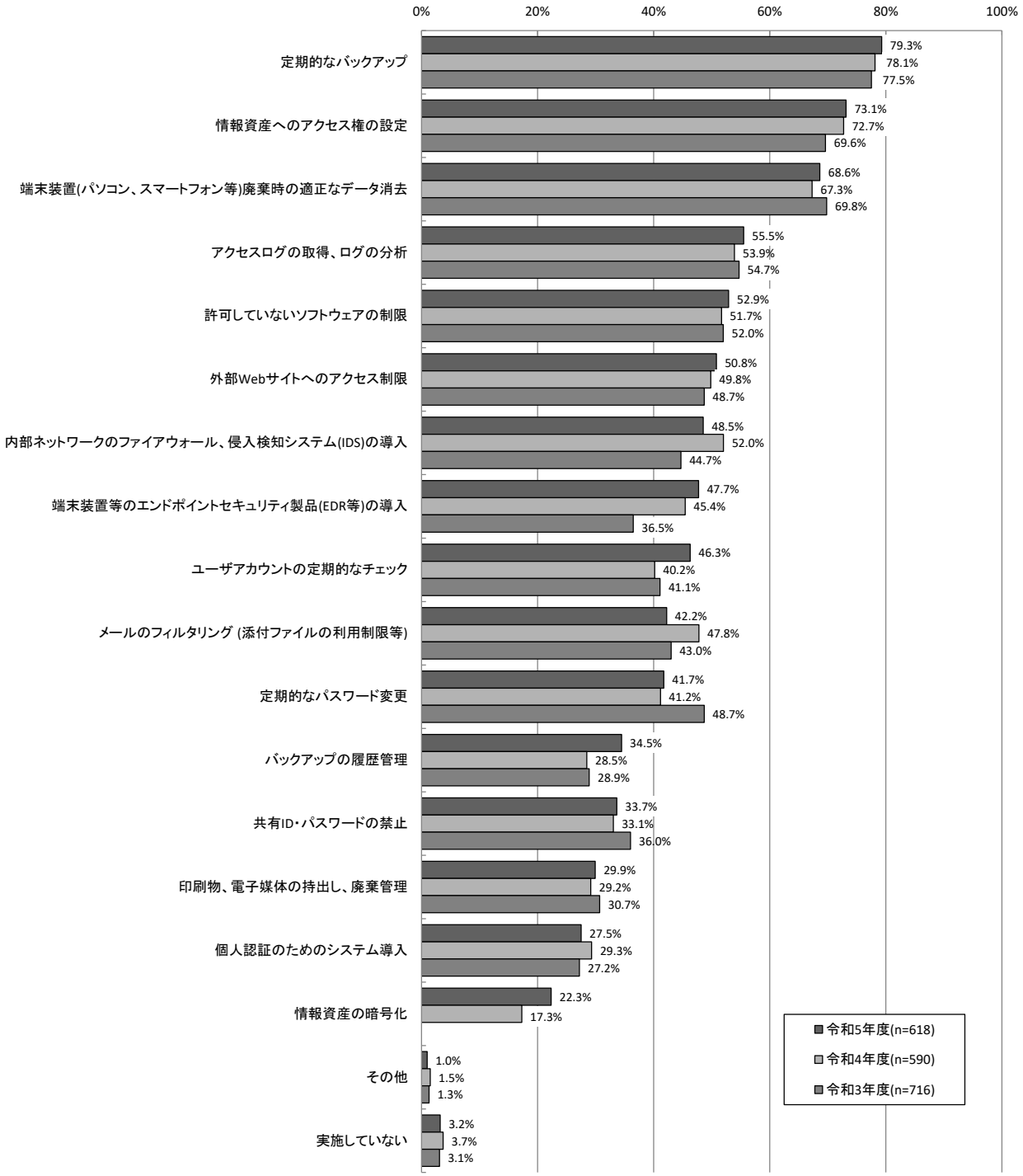


アクセスログの取得、ログの分析



【経年変化】昨年度と比較すると、「ユーザアカウントの定期的なチェック」が 6.1 ポイント、「バックアップの履歴管理」が 6.0 ポイント、「情報資産の暗号化」が 5.0 ポイント増加している。一方、「メールのフィルタリング（添付ファイルの利用制限等)」が 5.6 ポイント減少している。

【経年変化】不正アクセス等への対策状況

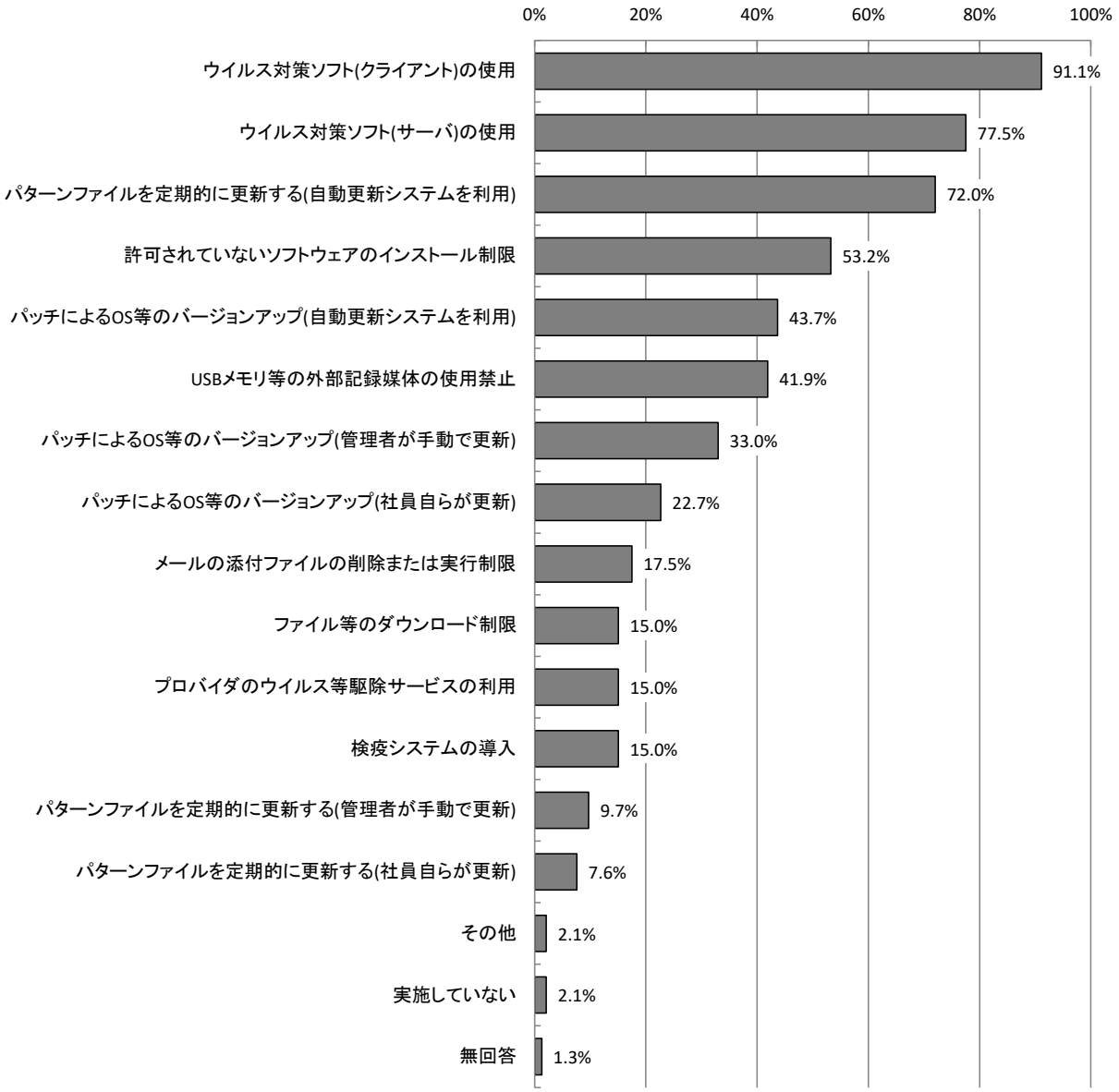


※令和３年度調査で、「端末装置等のエンドポイントセキュリティ製品（EDR等）の導入」を新設。
※令和４年度調査で、「情報資産の暗号化」を新設。

3.2.23　不正プログラムへの対策状況　【問28】

不正プログラムへの対策状況については、「ウイルス対策ソフト(クライアント)の使用」が91.1%で最も高く、次いで「ウイルス対策ソフト(サーバ)の使用」が77.5%、「パターンファイルを定期的に更新する(自動更新システムを利用)」が72.0%となっている。

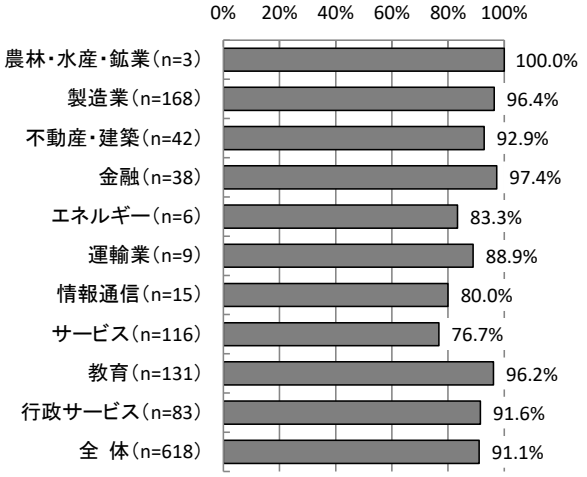
【全体】不正プログラムへの対策状況（MA, n=618）



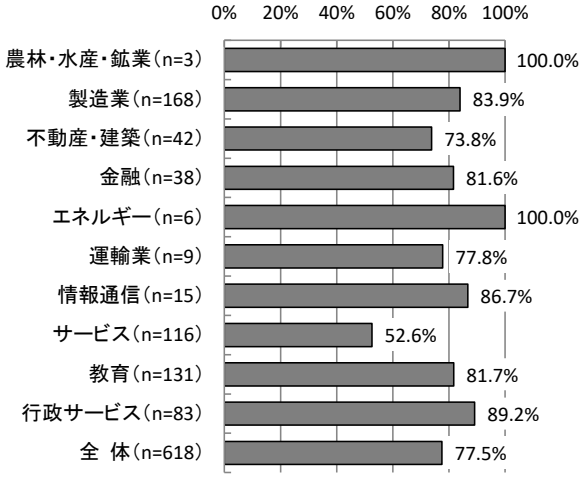
【業種別分析】業種別にみると、「ウイルス対策ソフト(クライアント)の使用」については、すべての業種で70%以上と高くなっている。「ウイルス対策ソフト(サーバ)の使用」については、「エネルギー」が100.0%、「行政サービス」が89.2%で高くなっている。

【業種別分析】不正プログラムへの対策状況

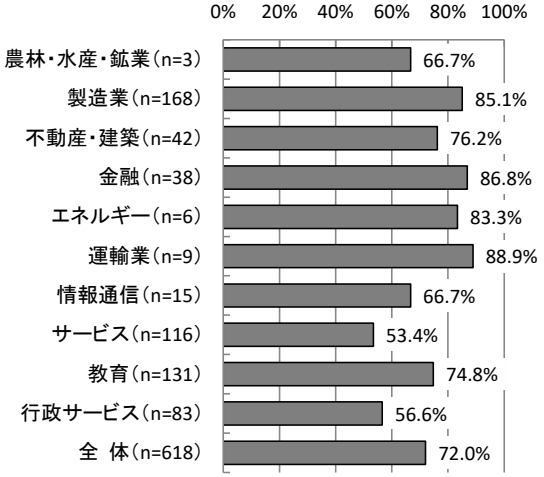
ウイルス対策ソフト(クライアント)の使用



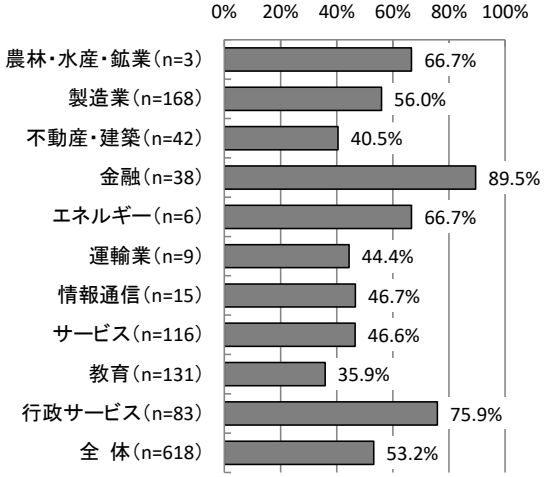
ウイルス対策ソフト(サーバ)の使用



パターンファイルを定期的に更新する(自動更新システムを利用)



許可されていないソフトウェアのインストール制限

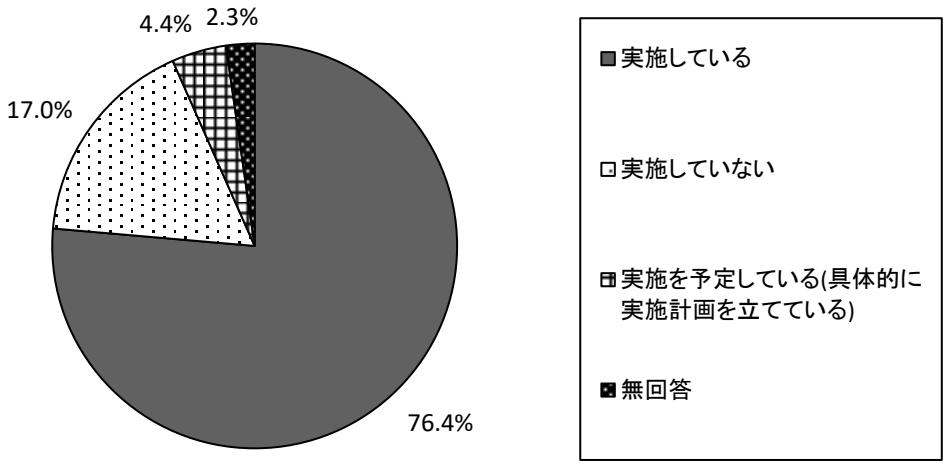


3.3 人的対策

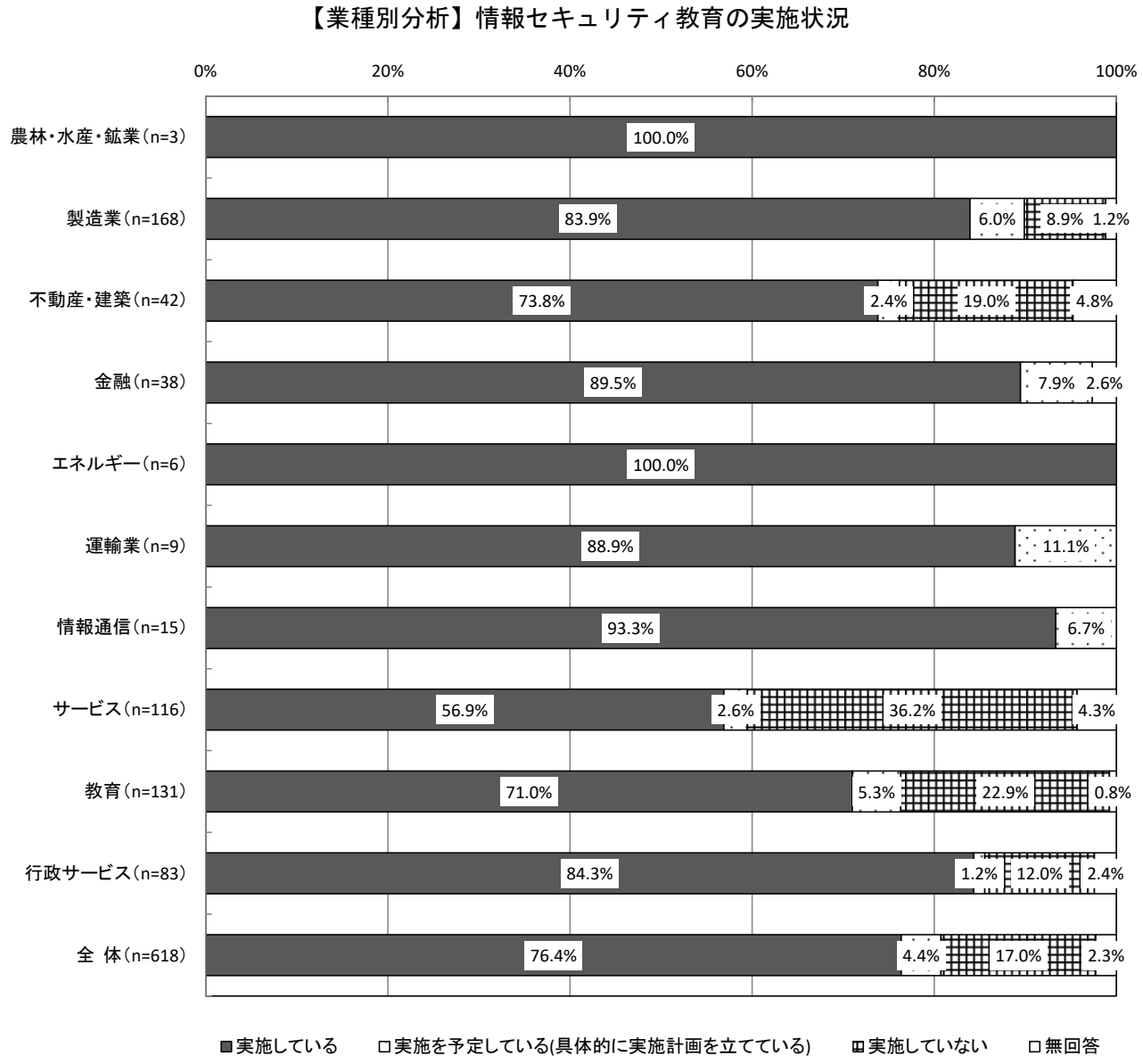
3.3.1 情報セキュリティ教育の実施状況 【問29】

情報セキュリティ教育の実施状況は「実施している」が76.4%、「実施していない」が17.0%、「実施を予定している(具体的に実施計画を立てている)」が4.4%となっている。

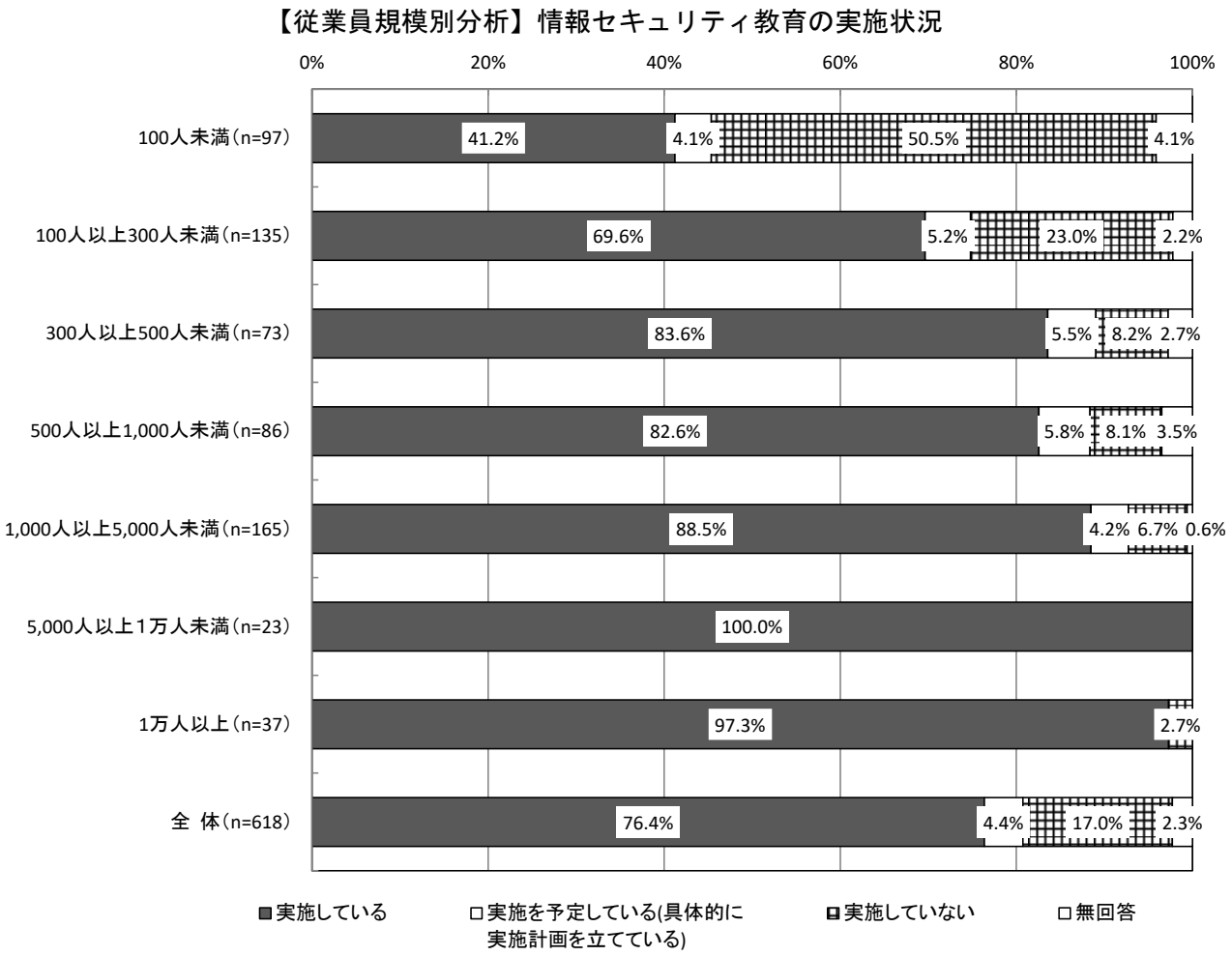
【全体】情報セキュリティ教育の実施状況 (SA,n=618)



【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%、「情報通信」が93.3%となっている。一方、「実施していない」は「サービス」が36.2%、「教育」が22.9%となっている。

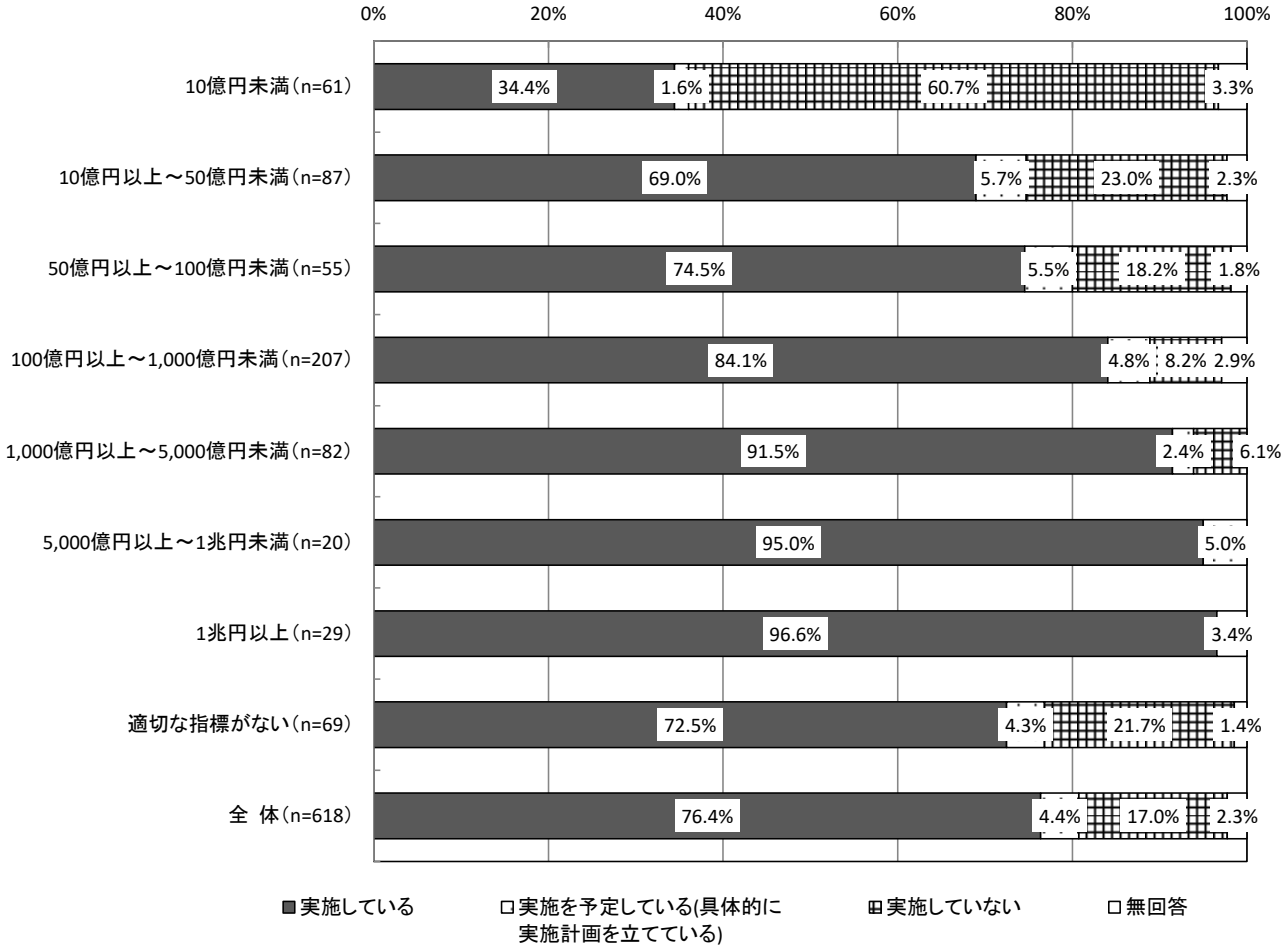


【従業員規模別分析】従業員規模別にみると、「実施している」については、概ね従業員規模が大きくなるにつれて高くなる傾向にあり、「5,000人以上１万人未満」「1万人以上」で9割を超えている。



【予算規模別分析】予算規模別にみると、「実施している」については「10億円未満」では34.4%で、予算規模が大きくなるにつれて高くなる傾向にあり、「1,000億円以上～5,000億円未満」「5,000億円以上～1兆円未満」「1兆円以上」で9割を超えている。

【予算規模別分析】情報セキュリティ教育の実施状況

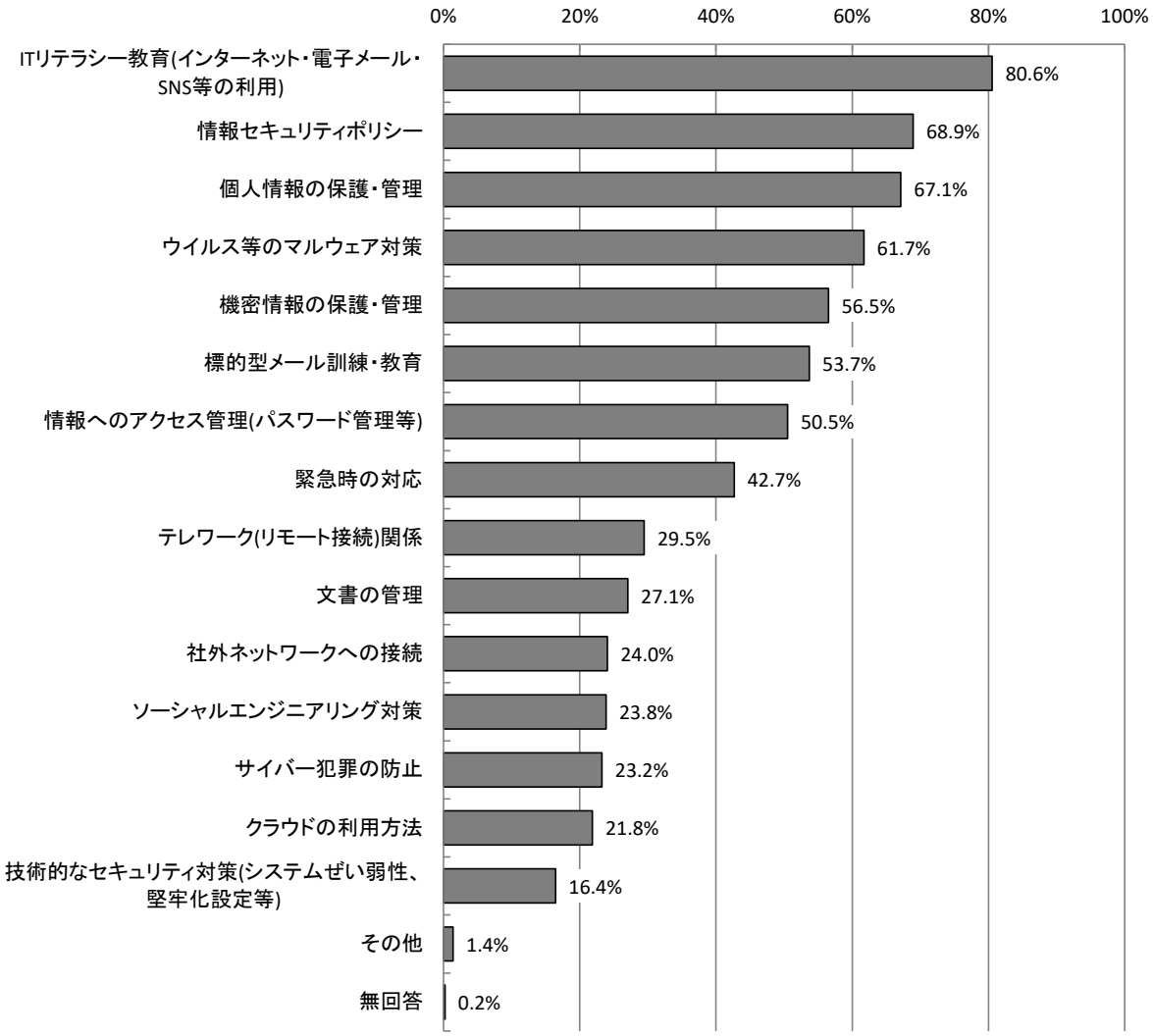


3.3.2　情報セキュリティ教育の内容　【問29-1】

情報セキュリティ教育の内容については、「ITリテラシー教育(インターネット・電子メール・SNS等の利用)」が80.6%、「情報セキュリティポリシー」が68.9%で高くなっている。

※本項目は、情報セキュリティ教育を行っている社・団体等を対象としている。

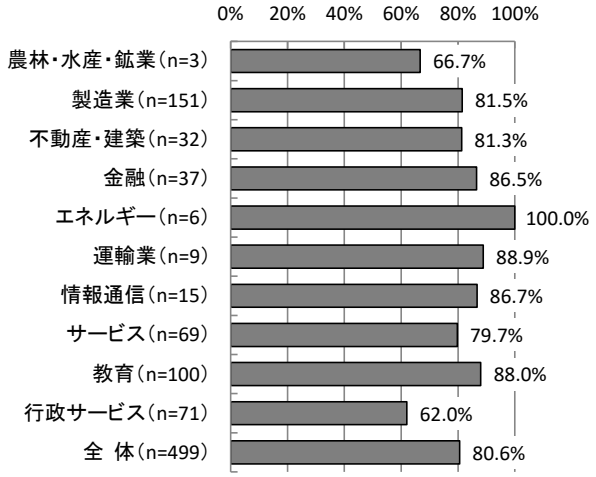
【全体】情報セキュリティ教育の内容（MA, n=499）



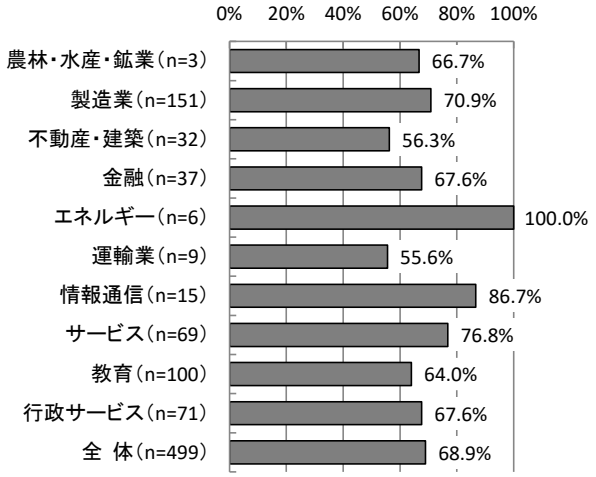
【業種別分析】業種別にみると、「ITリテラシー教育(インターネット・電子メール・SNS等の利用)」は、「エネルギー」が100.0%、「運輸業」が88.9%と高くなっている。「情報セキュリティポリシー」は「エネルギー」が100.0%、「情報通信」が86.7%で高い。「個人情報の保護・管理」は「エネルギー」が100.0%、「情報通信」が93.3%で高くなっている。

【業種別分析】情報セキュリティ教育の内容

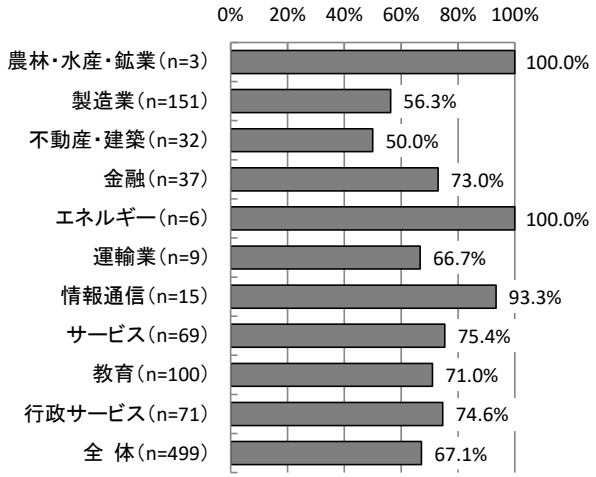
ITリテラシー教育(インターネット・電子メール・SNS等の利用)



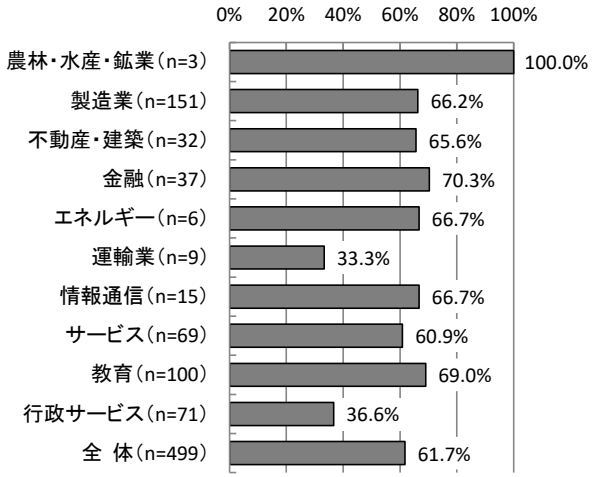
情報セキュリティポリシー



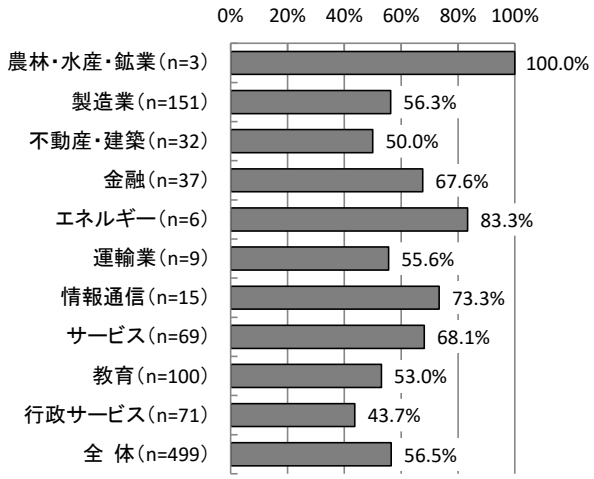
個人情報の保護・管理



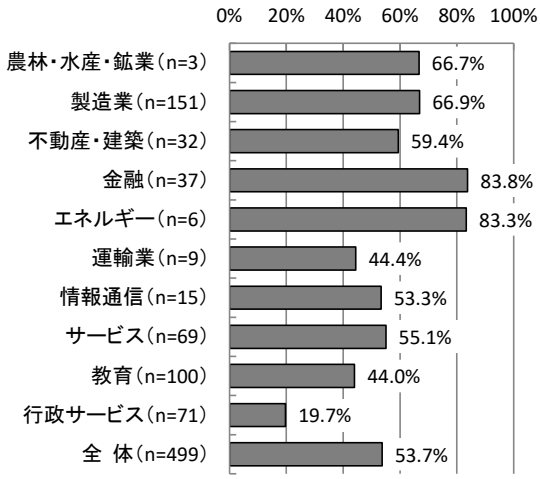
ウイルス等のマルウェア対策



機密情報の保護・管理



標的型メール訓練・教育

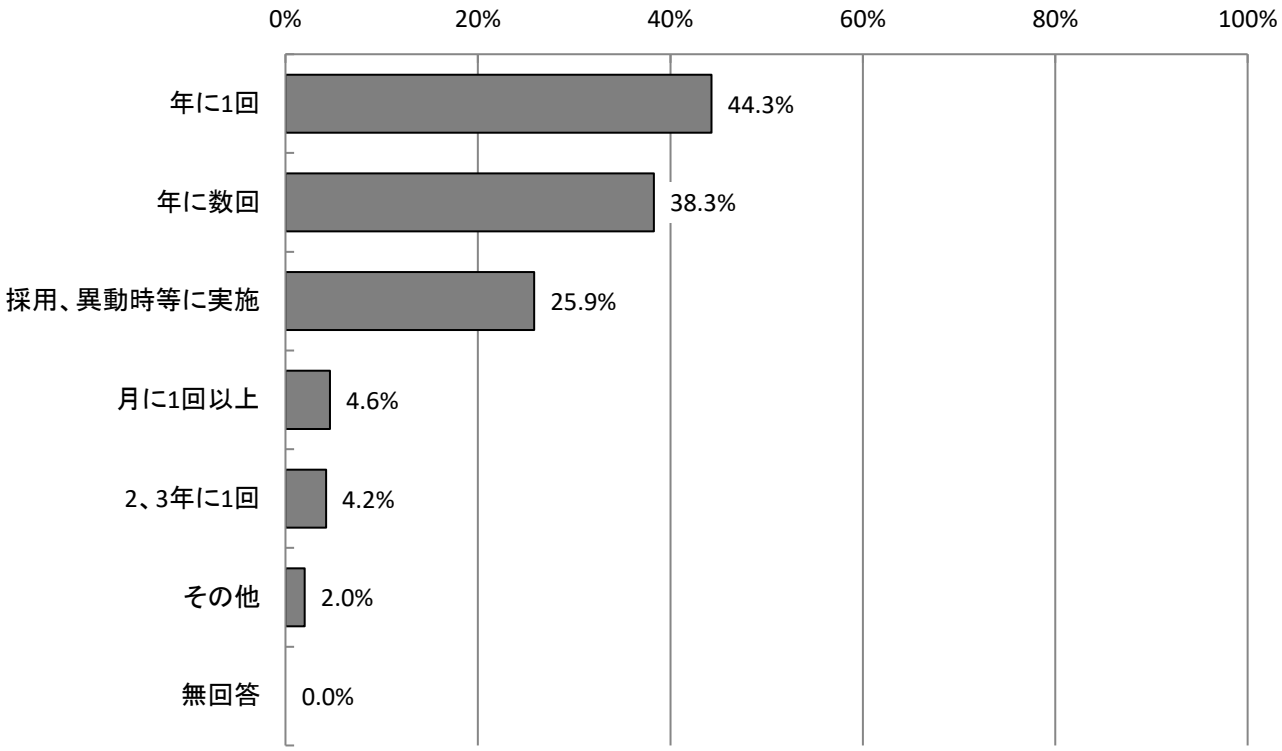


3.3.3 情報セキュリティ教育の頻度 【問29-2】

情報セキュリティ教育の頻度については、「年に１回」が44.3%で最も高く、次いで「年に数回」が38.3%、「採用、異動時等に実施」が25.9%となっている。

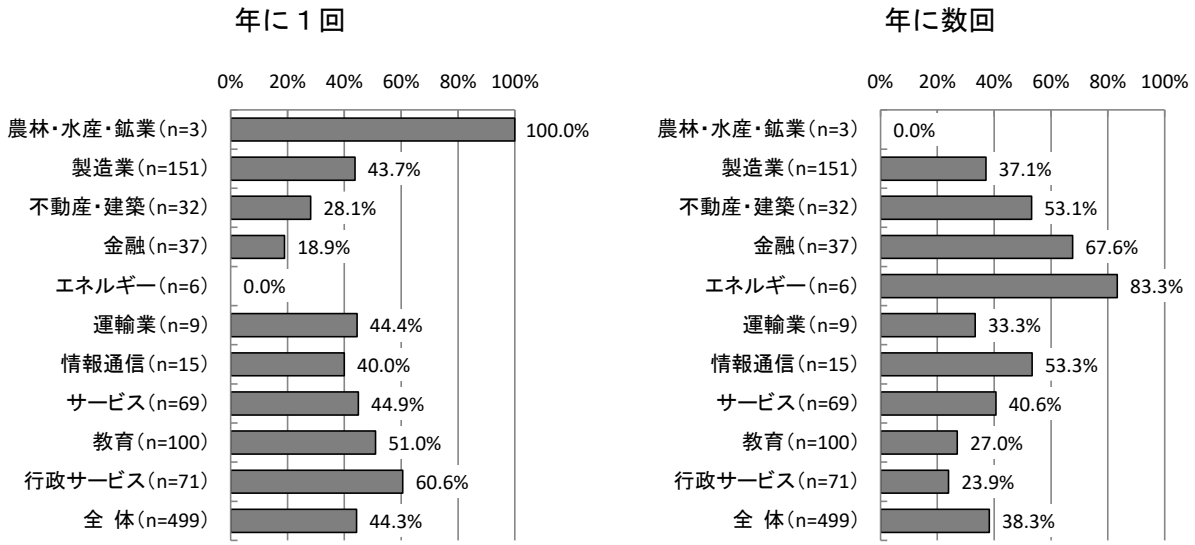
※本項目は、情報セキュリティ教育を行っている社・団体等を対象としている。

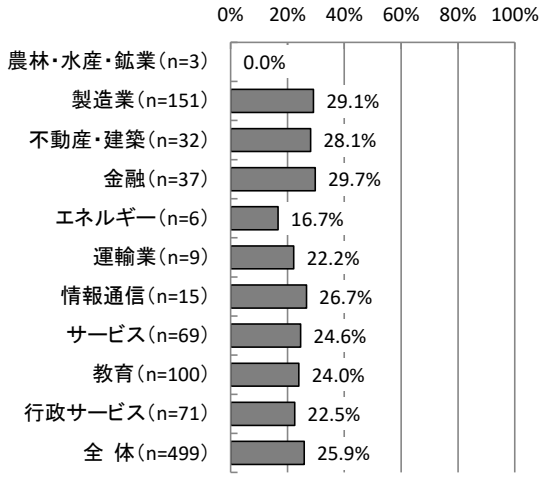
【全体】情報セキュリティ教育の実施頻度（MA, n=499）



【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60.6%で最も高く、「年に数回」については、「エネルギー」が83.3%となっている。「採用、異動時等に実施」については、「金融」で29.7%となっている。

【業種別分析】情報セキュリティ教育の実施頻度

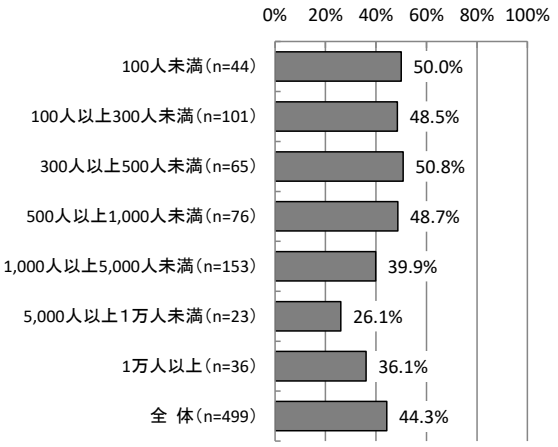




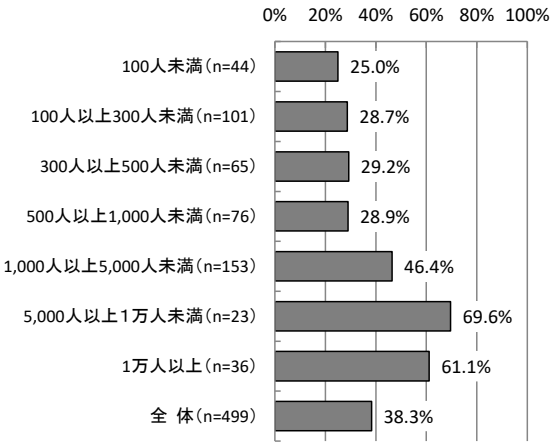
【従業員規模別分析】従業員規模別にみると、「年に１回」については「300人以上500人未満」が50.8%、「年に数回」については、「5,000人以上１万人未満」が69.6%と最も高くなっている。

【従業員規模別分析】情報セキュリティ教育の実施頻度

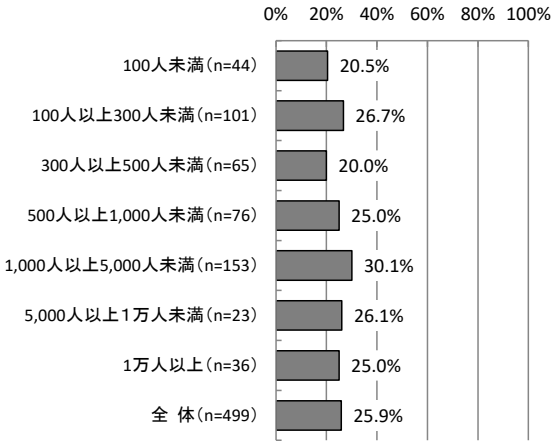
年に１回



年に数回



採用、異動時等に実施

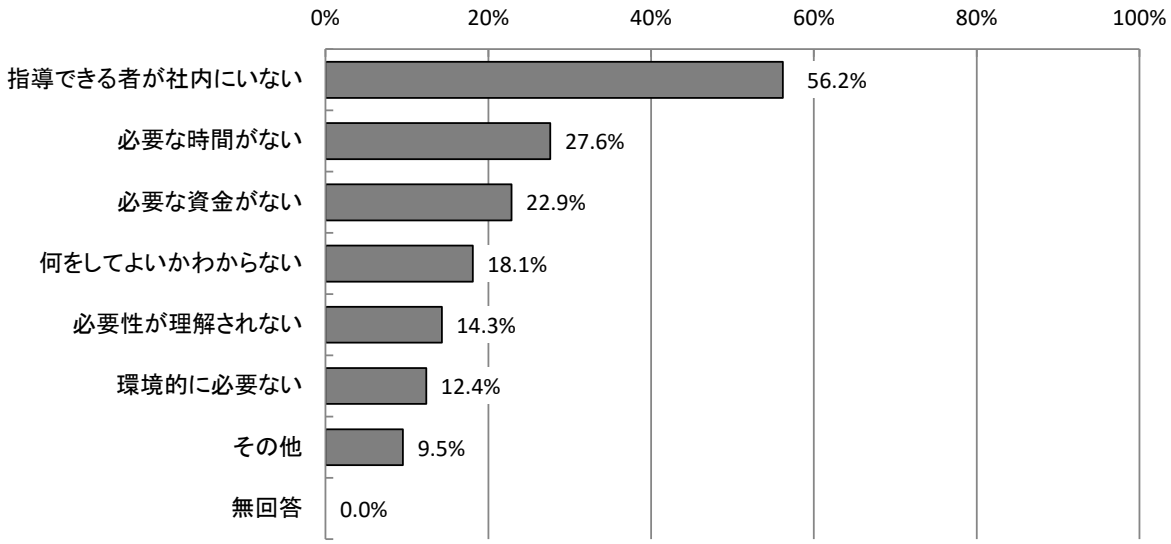


3.3.4　情報セキュリティ教育を実施しない理由　【問29-3】

情報セキュリティ教育を実施しない理由については、「指導できる者が社内にいない」が56.2%で最も高く、次いで「必要な時間がない」が27.6%となっている。

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

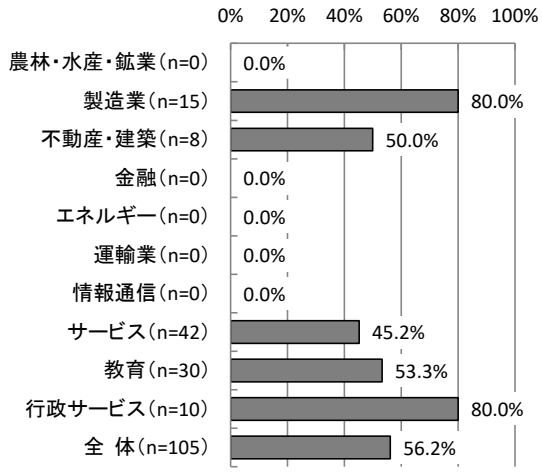
【全体】情報セキュリティ教育を実施しない理由（MA,n=105）



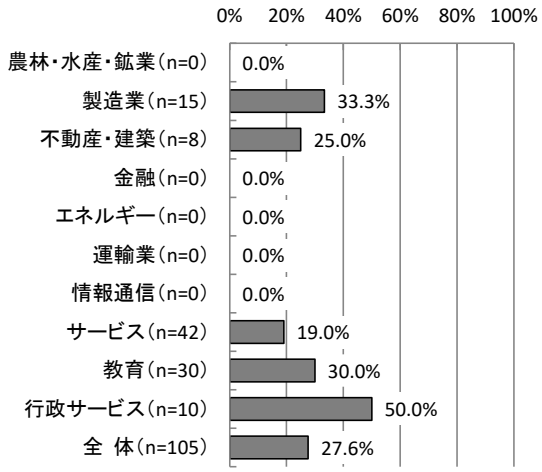
【業種別分析】業種別にみると、「指導できる者が社内にいない」は、「製造業」「行政サービス」で80.0%、「必要な時間がない」は、「行政サービス」で50.0%と高くなっている。

【業種別分析】情報セキュリティ教育を実施しない理由

指導できる者が社内にいない



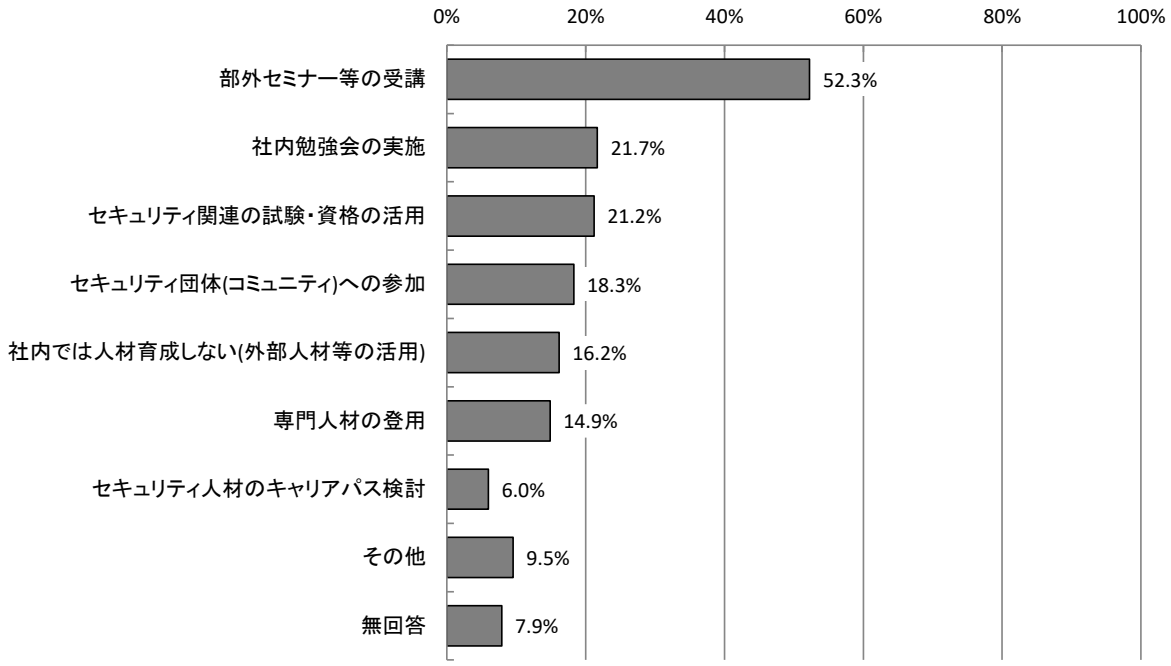
必要な時間がない



3.3.5　セキュリティ人材を確保するための施策 【問30】

セキュリティ人材を確保するための施策は「部外セミナー等の受講」が52.3%で最も高く、次いで「社内勉強会の実施」が21.7%、「セキュリティ関連の試験・資格の活用」が21.2%となっている。

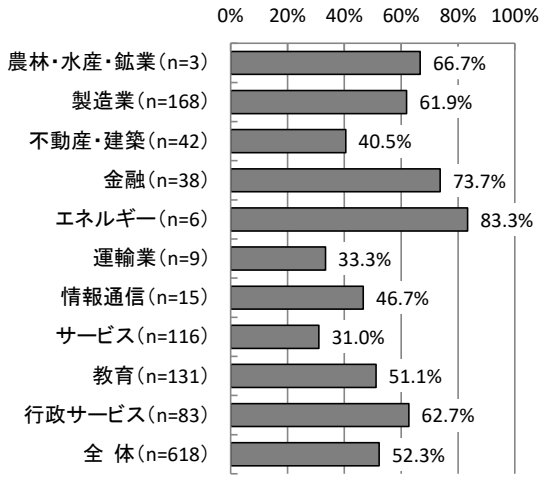
【全体】セキュリティ人材を確保するための施策（MA, n=618）



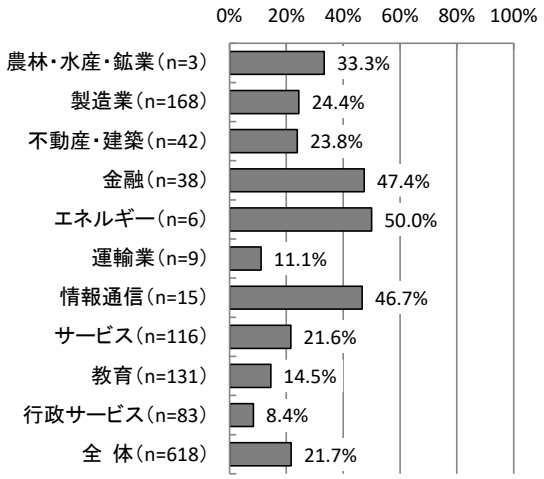
【業種別分析】業種別にみると、「部外セミナー等の受講」は、「エネルギー」が83.3%、「金融」が73.7%で高い。「社内勉強会の実施」の実施は、「エネルギー」で50.0%、「金融」で47.4%、「情報通信」で46.7%と高くなっている。

【業種別分析】セキュリティ人材を確保するための施策

部外セミナー等の受講



社内勉強会の実施



3.3.6　セキュリティ対策の問題点や不安等

- 自発的な危機感の譲成が出来るよう育みたい。
- ①不正アクセスに対する不安はきりがないが、外部委託業者がきちんとしてくれていると信頼するしかない。②不正アクセスする者を厳罰化すべし。
- Web入力式にしてほしい
- 従業員を使用せず1人で治療をしています。netには極力つながないようにしていてPCはオフラインで使用する事が多いです。
- 標的型メール訓練では、部長層以上のヒット率が、一般層よりも明らかに高い。(倍の確率で、ヒットする。)多忙は理由にならないので、どうやって意識を高めるかがチャレンジである。
- 同様のアンケートが多方面より送付されてくる。(総務省等)これだけの内容を解答するには時間をかかるので、できれば統一するなどしてほしい。
- セキュリティ対策に万全はない･費用対効果も見えにくい。･継続的なアップデートが必要
- 不正アクセス、特に不正購買、クレジットマスターなどの犯人をつかまえてほしいと思うが、何をどうしたらよいかわからない。(防御対策を行っているのみである。)
- 人的資源、金銭的資源の不足　電子カルテベンダ、医療機器ベンダのセキュリティ対策への認識欠如。☆対策を求めると有償対応として高額な費用を求められる　システムの複雑化、細分化に伴う管理コストの増大　業界的にオンプレミス前提のシステムが多く、クラウド化に踏みきれない。Windows個人ログオンがなじまない(PCの共用が前提の職場環境)
- web回答できると良いと思います。
- セキュリティ関連予算･人材の獲得が困難。
- 社内メンバーの理解を得ることが難しい。充分な予算および人材が確保できない。
- 基幹ネットワークは固定IPアドレスの改定を行い、認証外機器は接続させない。TV会議は全く別のネットワークで構築し、期間ネットワークへは接続させない。
- NIST対応の基準が確定されないことが不安。
- 年配社員との意識のへだたりが有る。セキュリティに関しては、海外の方が｢本場｣で、日本国内で流通するサービスで太刀打ちできるか心配。
- 問9はもう少し具体的に記述した方が良いと思います。
- 高額の費用が必要な対策について、経営陣の理解を得るのに手間がかかる事。
- 費用対効果がわからないため、投資額が決めづらい。
- セキュリティ対策は保険的な要素が強く、何らかのインシデントが発生するなどしない限り予算が付きにくい。また、対応する人材の確保も困難になってきている。
- マルウェア、ウイルス感染時、個体感染は受容するが、他のキキへの拡大を防止できる対策を行ないたい。拡大してしまうと対応できない。
- どこまで対策してよいのか基準がなく不明瞭なため、ベンダーに過剰な提案を受けることが多い。各企業の規模や仕組はさまざまであるが国をあげた取組みとして、セキュリティ対策の義務化等を検討して欲しい。
- 中国のように、国単位でUTMによるマルウェアフィルタリングを行った上で、日本国民にネットワークを提供することはできないのかどうか知りたい。中小企業が投資するには、コストがかかりすぎる。
- 費用対効果が見えないので、予算確保が困難である。
- ほぼ、外部からアクセスできない設定で運用しているが、外部へ公開しているサーバー等のシステム更新をなかなか行えていない。クラウドに対する不安からなかなかPPAP等から脱却できていない。旧態前のセキュリティ的に問題のある、慣れた操作法から安全な新しい操作法に移ってもらえないでいる。
- 本アンケートの真贋が不明だった。御庁ホームページ等にアンケート実施を表記していただければと思います。ご検討のほどお願い申し上げます。
- 回答しづらいアンケート項目があり、改善していただけたらと思います(例　問5.6条件つきで許可や義務でなく推奨など)
- 昨今進めているデジタル化対応(システムのクラウド化等)やデータ利活用推進と並行して、セキュリティ対策を強化する必要がある。その中で将来を見据えた十分なセキュリティ対策を進められる人材の育成が課題。コスト増大にも不安感を感じている。サイバー攻撃の高度化に対して業務バランスを保ちつつセキュリティ対策を行うのは高いレベルの専門性が求められ中長期的な人材育成が課題。
- 人材の不足(セキュリティ全般をファシリテーションできる人材)･ダークサイトの確認出来るようなスキルが不足
- 専問用語ばかりで何にか何だかわかりません。スミマセン。
- セキュリティ人材不足　コストの2点が悩み。
- 国策として実施してほしい。
- 「いかにして攻撃に気づけるのか?」「気づいた時の初動を正しく実行できるか」という点に不安があります。
- 予算、人材の確保が困難。　・「どこまで対策すれば良いか」のゴールが明確にならない。
- 費用対効果がハッキリしない。どこまで対策すればよいのか明確な答えがない。
- 社内に情報セキュリティ対策を行うための人材や体制、スキルが十分でない

- クライアント側にエンドポイント、EDRを導入してソフトウェアで入口と感染後対策をしています。特定部門にはハードウェアのSubgateで感染しても横展開しないように追加対策しています。ルータ側では不正サーバへの接続を監視するためSSLインスペクションを導入しています。これらの対策を今期実施しましたが、導入費用が高額であり正直費用対効果の面ではやりすぎ感はあります。ルータの年間更新費用がもうすぐ発生しますが、今のセキュリティレベルを維持するだけでもコストがかかるので費用と効果のバランスがとても難しくなってくると思っています。
- 情報セキュリティ対策の企画立案を行う人材が不足している。また、情報セキュリティに関しての意識や理解が少ない組織のため、早急な対応が求められるが意思決定まで時間がかかる実情がある。
- 当社では当社のITパートナー様にご協力いただき、情報システム・情報セキュリティを運営しているが、日々、変化する脅威に迅速に対応することは難しく、基本的な対策を行っているものの、いつ被害に遭ってもおかしくない状況であり、そのことが不安材料
- 法に基づかず任意で個人情報の提供を強いる地方警察に困惑している。
- 弊社はグローバル企業ですが、日本国内の内容で回答しました。　問5-1の回答について補足です。 個人所有端末は社内利用不可、VDIを利用する場合にのみ許可しています。なお、VDIのセキュリティ対策は実施しています。（問20の回答を参照下さい）
- 情報セキュリティ対策の必要性については、十分に感じているが、専門性が高く職員のノウハウが不足しているのが実情。また、他業務と兼務しているため情報セキュリティに対する時間的、心理的余裕がない。現状はベンダーに頼らないとわからないことが多い。
- グループ全体へのセキュリティガバナンスの浸透
- 組織のシステム管理者、組織の利用者、顧客の情報セキュリティ意識が低い。 情報セキュリティ対策は投資効果が見えにくい上に割高。事象が発生しないと必要性が認識されない。 情報資産を持たない（＝リスク低減）という考え方もあるので、保存期間が到来した情報は積極的に削除する事も重要であると考える。
- 本来であれば回答は出来ない領域のアンケートであるため、警察庁から直接回答依頼するか外部委託関係を証明できるようにしてほしい。
- 事前の防衛のための予算をとりずらい。提案方法が不明。
- 一番の課題はセキュリティ施策を計画し実行する人員（専任）不足です。社内の人員だけでは対応が非常に難しい。いざ施策を実行しようにも、システム担当者側の理解、協力も必要なため、常に最新のパッチが適用されたサーバでの運用も難しい。 サイバーセキュリティに対する施策についても、親会社よりアドバイスはあるものの、何をどこまで実施すれば良いか不明な点も多い。
- 海外での事案の場合、当該国の警察との連携も必要になってくるが、日本の警察とは違ってどこまでその国の警察を信用すべきかという点で難しさを感じることもある。インターネットの世界は国境がないので、グローバルにはどう対応すべきかといったことのガイドラインが欲しい。
- グループ企業各社でセキュリティ対策の水準や、セキュリティへの感受性が異なり、そのギャップを多々感じることがある。そうしたギャップをケアしながらの対策推進の難しさがある。
- セキュリティ人材を社内で育成・確保が難しい　高度な知識と経験が必要だが、いざという時の待機要員だけというわけにもいかず、また、セキュリティ対策は無尽蔵に対策を上乗せするものではない事から、専門能力人材を自社で確保する事が困難（スキルアップ経験が獲得しずらい。ある程度整ってくるとモチベーションが保てない）
- 個人情報等に関与するデータは専用回線で取り扱う状況にありますが、セキュリティ対策をある程度の知識を持って行う職員がいないため運営につき概ね導入時の設定のまま継続しています。職員合計で１０名に満たない規模の診療所です。導入したマイナンバーカードを用いた個人認証に正しくセキュリティがかかっているのかも判然としません。大きな企業ならともかく個人で営む小事業所に高度なセキュリティ対策を求めることの限界を認識して欲しいものです。
- 社内で検討すべき内容のアンケートだったので、当社の取り組みが間違っていないことを認識できました。
- そもそもセキュリティのアンケートなのに紙もしくはExcelでの提出とは、一番セキュアではないと思われます。匿名アンケートであれば、それなりのクラウドサービスもありますので、今後はそちらを利用してはいかがでしょうか？
- 情報セキュリティ対策を実施するにあたり、攻撃手法が変化している中で、未知のウイルスや新たなサイバー攻撃、顧客データや機密情報を守る責任、不適切なアクセス、内部者の悪意ある行動、外部からの侵入など、様々な対策の強化が必要があると考えるが、どれだけの費用をかけてどこまでの対策が必要か、費用対効果分析はどうすればよいのか、予算不足やスキル不足が問題点となっております。 また、不正アクセス等の侵害事案が発生した場合等の事後対応マニュアルを早急に作成する必要があると考えています。
- 情報セキュリティ対策については日ごとに対応すること増えており ①対応するための情報収集の方法 ②収集した情報の活用 ③運用管理における教育方法具体的実施 ④対応するための人材確保 が課題となっている
- 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 ・セキュリティスキルを持つ人材不足、社内評価制度のあり方 ・セキュリティ対策の実施と利便性のバランス確保 ・社員のセキュリティ意識の向上、浸透に要する多大な時間　・ランサムウェア対策（ネットワーク分離やデータバックアップ等の備え）
- セキュリティ一辺倒に構築すると費用も青天井となり、業務効率の悪化や、見合った人材を確保することも困難となるため、どこまでのセキュリティを構築するかというレベル感が難しいと考えています。
- セキュリティ投資はどちらかというと守りの投資。経営層になかなか理解が得られなかったが、最近は随分マシ

に。ただやはり、ハイエンドを目指すと投資が青天井になってしまうため、落としどころを探すのが難しい。セキュリティに関する営業も多いが、サービスのわりに高額であったりすることから、信頼できるベンダーを探しも大変かと思われる。 セキュリティ人材は社内育成も考えたが、人材そのもの採用、技術の維持や最新情報への知識のアップデート等の労力を考えると、それを専門にされている企業にお任せするほうが対効果があるのではと考えている。 他社との交流が乏しいので、他の企業ではどのくらいの対策を実施しているかは知りたい。 本アンケートについてですが、当社はEXCELにて提出いたしますが、次回以降はWEBサイトで行っていただきたい。 当社からみて取引実績のない企業様が提供されるファイルを利用するのは抵抗があります。 調査協力は惜しむつもりはありませんが、セキュリティ調査を謳っている本件の取り組み手段に問題はありませんか。

- セキュリティ人材（専門家）の確保。 問13-7.にあるように、情報セキュリティ対策に関する投資については費用対効果が見えづらく、また何をどこまで対策すれば良いという正解が無いため、導入面でも運用面でも困難であると感じている。
- アンケートの作成、ありががとうございます。参考にさせていただいております。 要望としまして、メール誤送信対策、特にPPAP対応について、アンケートデータが欲しいと思います。 セキュリティ対策はコストがかかるため、他の組織がどのていど実施しているのか、新しい対策、ソリューションの全体の普及状況を把握しつつ、対策をとりたいと思います。EDRや、XDRなどの普及状況、DMARCなどの復旧状況、SEIMやセキュリティ監視などの普及率、とくに、業種別の普及率の情報がほしいところです。
- ○情報セキュリティ対策および不正アクセス対策ともに、１００％防御できる仕組み（組織体制を含め）が存在しないこと。 ○守るべき情報資産に対し、どれだけの資金をセキュリティ対策に投資すればいいのか判断が困難であること。 ○未知のサイバー攻撃などに対してＡＩを使うなど、どんな高度なセキュリティ技術を導入しても、ヒューマンリスクが残ること。
- 異なる種類のセキュリティ対策でも、経営層に理解を得られないことがある。
- 情報セキュリティの重要性に関して経営陣とかなりの温度差を感じていることに不安を抱いています。
- 情報セキュリティ人財が高齢化しており、後継者の確保／育成が課題。 ・本アンケートの集計結果、並びに、サイバー警察局から我々民間企業への具体的なサポート内容をご教示いただきたい。
- 情報システム及び情報セキュリティに関する人材が少ない。
- メールの添付でExcelファイルを送るのは少々時代錯誤な気がします。
- 行っている様々な施策の関係性（それぞれがなぜ必要か？など）の理解が進みにくい ・情報セキュリティに関する研修・訓練等の受講率・実施率向上
- 当方、大学のため学生の BYOD での端末利用を検討しておりますが、学校関係では学生経由の情報漏洩が多いにも関わらず、セキュリティ教育やデバイス管理など課題が多く、教職員とはまた違った難しさがあります。
- セキュリティ対策ソフト、セキュリティ対策機器を導入しているので、他に必要性を感じていませんでした。これを機に考えてみようと注意喚起になりました。ありがとうございます。
- 学校法人であるため、教職員＝従業員、学生＝顧客と読み替え、回答しています。 本学では主要な情報システムはすべてクラウド化されており（MS365及びGoogleWorkspace）、メールやファイル共有サービス上でのウイルスの検知や防御はクラウドサービス側で実施されています。 クラウドサービスの認証は多要素認証を必須化しており、管理者が定期的にログを確認できるようになっております。
- 市直営の診療所に届いたため、市のシステムと電子カルテシステムどちらに関して回答すべきか不明確であった。（今回は主に電子カルテシステムについて回答。） 市の組織としての担当部署は存在するが、電子カルテシステムに関しては、診療所自体の事業規模が小さく、複数診療所の管理を行っているため、不正アクセスや情報セキュリティに精通した担当者を設置することは現状難しい。
- 情報セキュリティに対する組織の統制、理解の不足、何から着手すれば良いか優先順位、明示されたポリシーの策定などシステム導入の前にやるべきことが、人材不足によりできていないと感じている。
- 専門的人材確保が困難であること。
- 国の方針でαモデルやβモデルが存在するため町にあった提案をしてくれるベンダーが少ない。どこまでセキュリティをあげるべきなのかという指標がない。
- 費用面との折り合いが合わず、優先度をつけながら対策をしていく必要があるため、不十分な対策となっている可能性があり、解決について困難だと感じる。
- 本当にセキュリティ人材の担い手確保に苦労していることに尽きる。
- 人材などを含むリソースが不足しがちなため、全ての課題に速やかに対応することは、かなり難しい状況となっております。
- 投資は有限であり、リスクは多様にわたる中で、実績できることも絞らざるをえなくなるだけではなく、実施すべきと提案される内容も、年々増えていく中での優先順位付けが課題。
- 業種別のアンケートになっていないので、質問と答えがあわないところがあり答えに迷います。 機材やシステム、サービスへの質問に対して全体を指しているのか、一部でいいのか対象範囲がわかりずらいです。 ひとつのシステムに対して自社と委託がある場合に答えに困ります。

- 不正アクセス事件とランサムウェア感染が区別されず報道がわかりにくくなっている。最大リスクはランサムウェア感染でほかはピンピンしているのに、自社だけ数か月のダメージを受ける可能性がある。 サプライチェーンを踏み台にした攻撃も含めると全方位に対するセキュリティコストは膨大で会社の利益を圧迫する勢い。今はコロナ前とコロナ以降では複雑で多面的ですっかり様変わりした。つぎはぎで行ってきた回線インフラもリセットする必要がある。セキュリティ機器は表面は日本語でも中は英語コマンドなので理解が難しい。 他国からは侵されない国産OSは作れないものか？必ずトロンのOS領域を経ないとデータ利用ができないような。
- 「終わりなき戦い」をやっている感覚です。　　丸の内警察署様はじめ、引続き連携を密にして対応させて頂きたいたいと考えております。　諸々御協力賜りたく、何卒宜しくお願い申し上げます。
- 不正アクセスや情報漏えいに対する対策を強化すると、職員の業務フローに情報を持ち出すための手順が増えるため、業務効率が低下する可能性がある。業務効率を維持しつつ、不正アクセス等の対策の強化を図る方法があれば知りたい。
- 日々、技術が変化しているため、目指している防御網の見直しが十分に出来ていない。また、内部人材が限定されており、外部との折衝、内部への周知等が追いつかないと共に、穴を塞げていることの確証が持てない。
- 上場した時にJSOX法対応において、情報セキュリティ対策を外部監査法人の協力のもとルールや計画を策定し、運用を実施した。しかし、経営層での情報セキュリティリスクを軽視している経営者もおり、情報セキュリティ対策は、情報システム部門からのボトムアップにて対策などを承認してもらう形となっている。そのため、対策を理解してもらうための労力とスピード感など問題があり、対策が講じられにくくなっている。分からないから、今まで起きていないから対策しなくても良いといった考えが、経営層の一部にある。 また、情報セキュリティ対策担当は、だれもやりたがらないため、情報システム部門のボトムアップでの対策実施には限界を感じている。
- セキュリティ対策全般として、以下の問題があり、実施までに時間がかかる場合がある。　①製品、サービス選定に時間がかかる　②導入コストが高い　③明示的な導入効果が算出できない　・所管部門の要員の問題もあり、運用上のすべての対応を賄いきれず、エンドユーザに移管しているものもあり　完全な対応ができない部分が残る
- 情報漏洩などのインシデントは発生していないが、本当に発生していないのか我々が気づいていないだけなのか不安に感じることがある。
- 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

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

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

■お手数ですが、令和５年９月１５日(金) までに、ご返送ください。
◆郵送での回答：同封の返信用封筒をご利用ください（切手は不要です。）。
◆電子メールでの回答：「cyber@researchworks.co.jp」までお送りください。
なお、Excelファイルのダウンロード方法は同封の「調査ご協力のお願い」に記載しておりますので、恐れ入りますが、記載内容をご確認ください。

１． 組織的対策

【貴社・団体について伺います】

問１． 貴社・団体は、どの業種に該当しますか。（○は一つ）

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

（太枠線内にご回答ください）

問２． 貴社・団体の従業員は、どのくらい在籍されていますか。（○は一つ）

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

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

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

【情報システム等の環境について伺います】

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

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

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

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

４．許可していない
５．把握していない
→ 問６へお進みください

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

１．義務づけている　　２．義務づけていない

問６．　貴社・団体においてテレワークを行っていますか。（○は一つ）

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

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

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

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

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

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

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

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

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

問８．　クラウドサービスを利用していますか。（○は一つ）

１．利用している　　２．利用していない　　３．わからない

問９．　外部から内部ネットワークへの接続を許可していますか。（○は一つ）

１．許可している　　２．許可していない

【情報セキュリティの運用・管理体制について伺います】

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

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

2．ウイルス等のマルウェアの感染を防ぐため
3．DDoS 攻撃等によるシステムダウンを防ぐため
4．システムの乗っ取り等により犯罪等へ悪用されるのを防ぐため
5．外部関連（顧客、取引先等）との取引を万全なものとするため
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．外部関連（顧客、取引先等）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. 事業継続（BCP など）の対策として
12. 不正アクセスの加害者にならないため
13. 法令による義務や監督省庁等からの指示があるため
14. その他（　　）

→ 問11へお進みください

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

【→被害は？】

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

【→攻撃手段は？】

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

問10-2.　過去1年間に攻撃・被害を受けられた方にお伺いします。攻撃・被害を受けた結果、サプライチェーンに被害を与えてしまったことはありますか。与えてしまった場合はどのような被害を与えてしまいましたか。（○は一つ）

1．与えてしまった（　　）
2．与えていない

問10-3.　過去１年間に攻撃・被害を受けられた方にお伺いします。攻撃・被害を受けた結果、実際に講じられた対応策はどのようなものですか。（○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．保険の利用
19．バックアップ、リストア計画の見直し
20．不明
21．その他（　　）
22．特に対策を講じていない

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

〈届出・相談先機関等〉

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

〈届出・相談した理由〉へお進みください

〈届出・相談した理由〉

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

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

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

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

1．具体的な届出先（　　）
2．わからない

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

1．知っている　　2．知らなかった

問13.　情報セキュリティ対策を実施していますか。（○は一つ）

1．実施している → 問13-1～13-7へお進みください

2．実施していない又は把握していない → 問13-8へお進みください

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

1．ある　　2．ない　　3．今後設置予定

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

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

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

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

→ 問13-4へお進みください

問13-3-1.　問13-3で「１．策定している」と回答された方に伺います。日々変化する状況の中で、情報セキュリティポリシー等の変更などセキュリティの関連事項を役員会議や経営会議等の議題として定期的に議論していますか。（○は一つ）

1．議論している
2．議論していない
3．その他（　　）

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

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

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

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

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

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

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

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

問13-8.　問13で「２．実施し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ないのですか。（○はいくつでも）

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

問14.　サプライチェーンリスク対策として、関連会社や取引先に情報セキュリティ対策を求めるなど何らかの対策を実施されていますか。（○はいくつでも）

１．契約にセキュリティポリシーの遵守を明記している
２．取引先等の情報セキュリティ評価を実施している
３．関連会社等との情報セキュリティに関する教育・訓練・情報共有等を実施している
４．その他（　　）
５．実施していない

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

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

２． 技術的対策

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

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

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

【情報セキュリティサービスの利用状況について伺います】

問17.　現在、どのようなサービスを利用されていますか。（○はいくつでも）

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

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

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

【ネットワークに対する情報セキュリティ対策について伺います】

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

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

→ 問18-1へお進みください　　↓ 問19へお進みください

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

1．OS/ファームウェアの最新パッチを常に適用している
2．不正アクセス、ランサムウェア等の被害に遭ったのでパッチを適用した
3．報道等によりランサムウェア等の被害の原因になることを知ったのでパッチを適用した
4．VPN 機器への接続認証について、複雑なパスワード、ワンタイムパスワード、多要素認証などを設定している
5．VPN 機器への接続端末について、IP アドレスなどで規制している
6．実施していない
7．クラウドサービスを利用しており、セキュリティ対策はサービス側に任せている
8．わからない

問19.　問８でクラウドサービスを「１．利用している」と回答された方に伺います。
クラウドサービスを利用することになった理由は何ですか。（○はいくつでも）
※　問８で「２．利用していない」「３．わからない」と回答された方は、問20へお進みください。

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

問20.　問９で外部から内部ネットワークへの接続を「１．許可している」と回答された方に伺います。どのような情報セキュリティ対策を実施されていますか。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）

※　問９で「２．許可していない」と回答された方は、問22へお進みください。

【回答群Ａ（通信路に対する対策）】

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

【回答群Ｂ（端末に対する対策）】

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

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

→ 問21-1～21-2へお進みください

１．ID・パスワードのみでの認証
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．認証アプリ
８．その他（　　）
９．認証なし

→ 問21-2へお進みください

問21-1.　問21で「１．ＩＤ・パスワードのみでの認証」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、どのような対策を実施されていますか。（○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．実施していない

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

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

1．顧客に対する注意喚起
2．フィッシングサイトの監視
3．フィッシングサイト発見時の関係機関への通報
4．SPF（Sender Policy Framework）の導入
5．DKIM（DomainKeys Identified Mail）の導入
6．DMARC（Domain-based Message Authentication Reporting and Conformace）の導入
7．その他送信者認証
8．その他（　　）
9．実施していない

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

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

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

問23-1.　当該サービスは、どのように管理されていますか。（○はいくつでも）

1．自社管理
2．一部外部業者に委託
3．全て外部業者に委託
4．クラウドサービスの利用

問23-2.　セキュリティ対策は、どのような取組みを実施されていますか。（○はいくつでも）

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

問23-3.　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：　　）
6．外部委託先に委託しているためわからない。

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

該当する選択肢の番号に○

ログの種類	回答群A	回答群B
回答例		
４．プロキシサーバのログ	5	1
１．ファイアウォール・侵入検知システム等（IDS、IPS 等）のログ		
２．ウェブサーバへのアクセスログ		
３．メールサーバのログ		
４．プロキシサーバのログ		
５．情報システムへの認証ログ		
６．データベースのログ		
７．クライアント PC のログ		
８．その他（　　）		
９．全く取得していない		
10．外部委託先に委託しているためわからない。		

各解答欄に該当する回答群から当てはまる番号を記入

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

回答群　B
１．自社
２．外部委託
３．その他
（　　）

問23-4-1へお進みください

問24へお進みください

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

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

【電子メールに対する情報セキュリティ対策について伺います】

問24.　電子メールに関するセキュリティ対策では、どのような取組みを実施されていますか。（○はいくつでも）
※　送信ドメイン認証（SPF、DKIM、DMARC）等については、問22に記載しています。

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．電子署名の利用
10. クラウドサービスの利用
11. 無害化処理を実施
12. 標的型メール受信訓練の実施
13. 電子メールセキュリティ対策に関する教養
14. その他（　　）
15. わからない

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

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

【不正アクセス、情報漏えい等に対する情報セキュリティ対策について伺います】

問26.　重要なシステム（基幹業務、製造　等に関わるシステム）への侵入阻止や侵入時における被害軽減に向けて、どのような対策を実施されていますか。（○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. 実施していない

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

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

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

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

３．人的対策

【情報セキュリティ教育に関する取り組みについて伺います】

問29.　現在、情報セキュリティ教育を実施されていますか。（○は一つ）

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

３．実施していない　→ 問29-3へお進みください

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

１．情報セキュリティポリシー
２．IT リテラシー教育
（インターネット・電子メール・SNS 等の利用）
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．標的型メール訓練・教育
16．その他（　　）

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

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

→ 問29-2を回答後、問30へお進みください

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

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

問30.　セキュリティ人材（専門家）を確保するための施策を実施されていますか。（○はいくつでも）

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

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

アンケートはこれで終わりです。ご協力ありがとうございました。
お手数ですが、令和5年9月15日(金) までに、ご返送ください。

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

付録2

問1. 貴社・団体は、どの業種に該当しますか。

農林・水産・鉱業	
農林・水産	0
鉱業	1
その他	2
小計	3
製造業	
食品	13
繊維	6
紙・パルプ	1
化学	35
薬品	7
ゴム・窯業	7
非鉄金属	6
機械	30
電気機器	19
造船	1
輸送機器	11
精密機器	4
その他	28
小計	168
不動産・建築	
不動産	9
建築	23
その他	10
小計	42
金融	
銀行	21
証券	4
保険	4
クレジット	0
消費者金融	1
信用金庫・組合	0
その他	8
小計	38
エネルギー	
電力	2
ガス	0
水道	0
石油製造(精製)	1
その他	3
小計	6

運輸業	
鉄道・地下鉄	3
航空	2
陸運	1
海運	1
倉庫	1
その他	1
小計	9
情報通信	
新聞	0
放送	1
通信	6
ISP	0
その他	8
小計	15
サービス	
流通・卸売	33
小売	10
娯楽・アミューズメント	0
飲食	0
ホテル・旅行	2
情報処理・ソフトウェア	13
警備	1
医療・福祉	39
その他	18
小計	116
教育	
大学	126
短大	1
専門学校	0
その他	4
小計	131
行政サービス	
都道府県	1
政令指定都市	3
市町村	79
小計	83
無回答	7
合計	618

第２部

アクセス制御機能に関する技術の研究開発の状況等に関する調査

4.調査概要

4.1 調査の目的

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

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

4.2 調査の対象と調査方法

調査対象：以下に該当する調査対象から無作為に1,884件抽出した。

・企業（1,599社）

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

・大学（285校）

国公立・私立大学のうち、理工系学部又はこれに準ずるものを設置するもの

調査方法は、次の方法で実施した。

① 電子メールでの回答

調査票のファイルに直接回答内容を入力してもらい、電子メールにて回答

② 郵送等での回答

配付した調査票を、郵送で送付してもらい回答

（調査期間：令和5年8月23日（水）（発送日）～9月15日（金）（締切日））

4.3 調査内容

本調査では次の2つを調査した。

① 研究開発の傾向

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

質問項目は次の通りである。

・研究開発体制
・アクセス制御機能に関する技術研究開発に係る現状と今後の展望
・アクセス制御機能に関する実用化（製品化）に係る現状と今後の展望

調査票：付録資料にある『回答用紙A』を参照

【アクセス制御機能の分類表】

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

② 実用化された製品及び研究開発中の技術・サービス

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

質問項目は以下の通りである。

・何を守るか
・何から保護するのか
・どのようなセキュリティ上の効果があるか
・どのような機能を持っているか
・どのようなレイヤーのセキュリティを守るか
・不正アクセスからの防御対象
・どのようなサービスか

調査票：付録資料の『回答用紙B』、『回答用紙C』を参照

4.4 送付・回収状況、集計対象件数

全体では、1,884件を送付して、214件を回収し、回収率は11.4%であった。

全体での回収数214件のうち、回答用紙A「アクセス制御機能に関する技術の研究開発の現状と方向性に係る調査」の問１「アクセス制御機能に関する技術の研究開発を行っていますか」に「はい」と回答した有効回答数は34件であった。また、回答用紙B「実用化（製品化）されているアクセス制御機能に関する技術」に対する回答は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24件であった。

4.5 報告書を見る際の留意点

・集計結果の比率は、小数点第二位を四捨五入し、小数点第一位までを百分率（%）で表示しているため、その数値の合計が100%を前後する場合がある。
・本文やグラフ中の選択肢は、調査票の言葉を短縮しているものがある。

5.調査結果(概要と考察)

5.1 アクセス制御機能に関する技術研究開発に係る現状と今後の展望

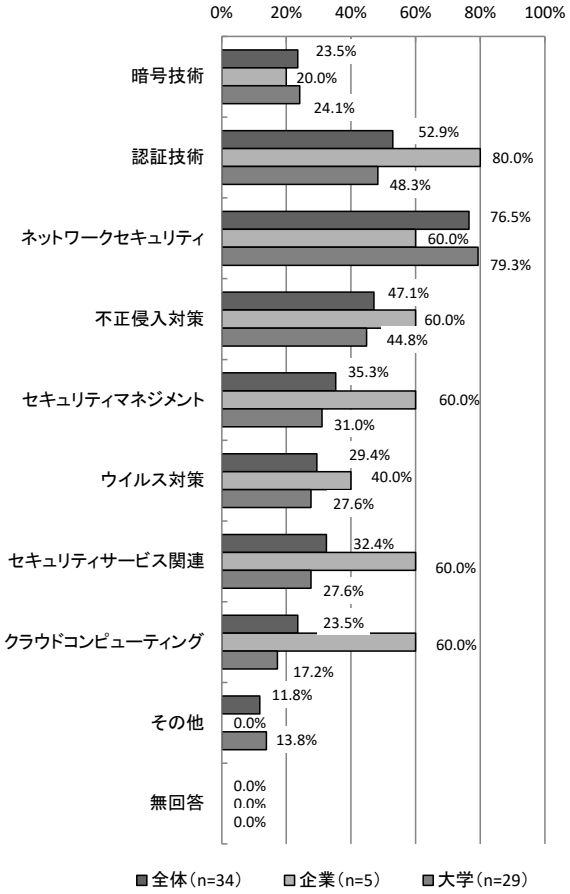
現在、取り組んでいる分野について、全体では「ネットワークセキュリティ」が最も高い。企業では「暗号技術」が高く、大学では「ネットワークセキュリティ」が高くなっている。

今後、取り組んでいく分野について、全体ではネットワークセキュリティ」が最も高い。企業では「認証技術」「セキュリティマネジメント」「セキュリティサービス関連」「クラウドコンピューティング」が高く、大学では「ネットワークセキュリティ」が高い。

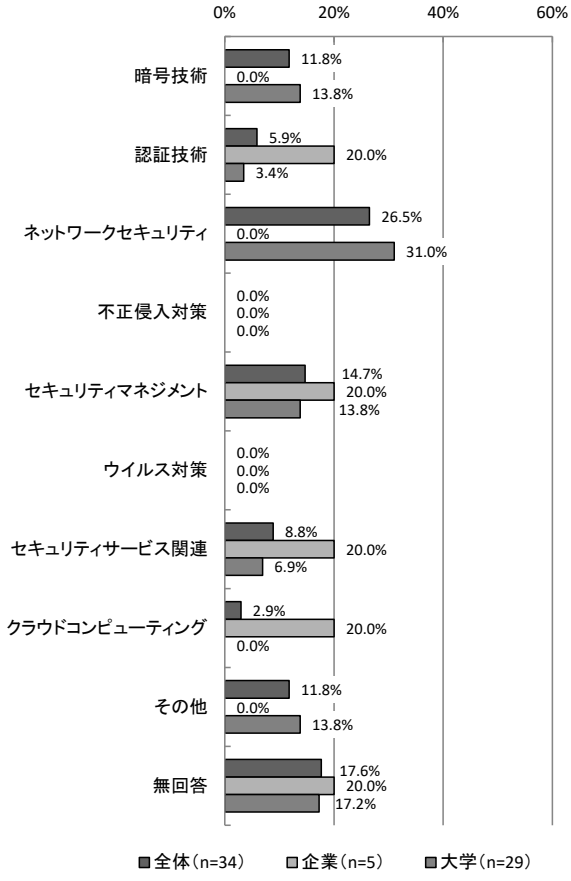
現在、取り組んでいる分野については、「ネットワークセキュリティ」が76.5%（26件）で最も多く、次いで「認証技術」が52.9%（18件）となっている。企業では「暗号技術」が80.0%（4件）で最も多く、大学では「ネットワークセキュリティ」が79.3%（23件）で最も多い。

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26.5%（9件）で最も多くなっている。企業では「認証技術」「セキュリティマネジメント」「セキュリティサービス関連」「クラウドコンピューティング」がそれぞれ20.0%（1件）、大学では「ネットワークセキュリティ」が31.0%（9件）と最も多くなっている。

【本調査】現在、取り組んでいる分野（MA）【A-問2】



【本調査】今後、もっとも力を入れたい分野（SA）【A-問3】

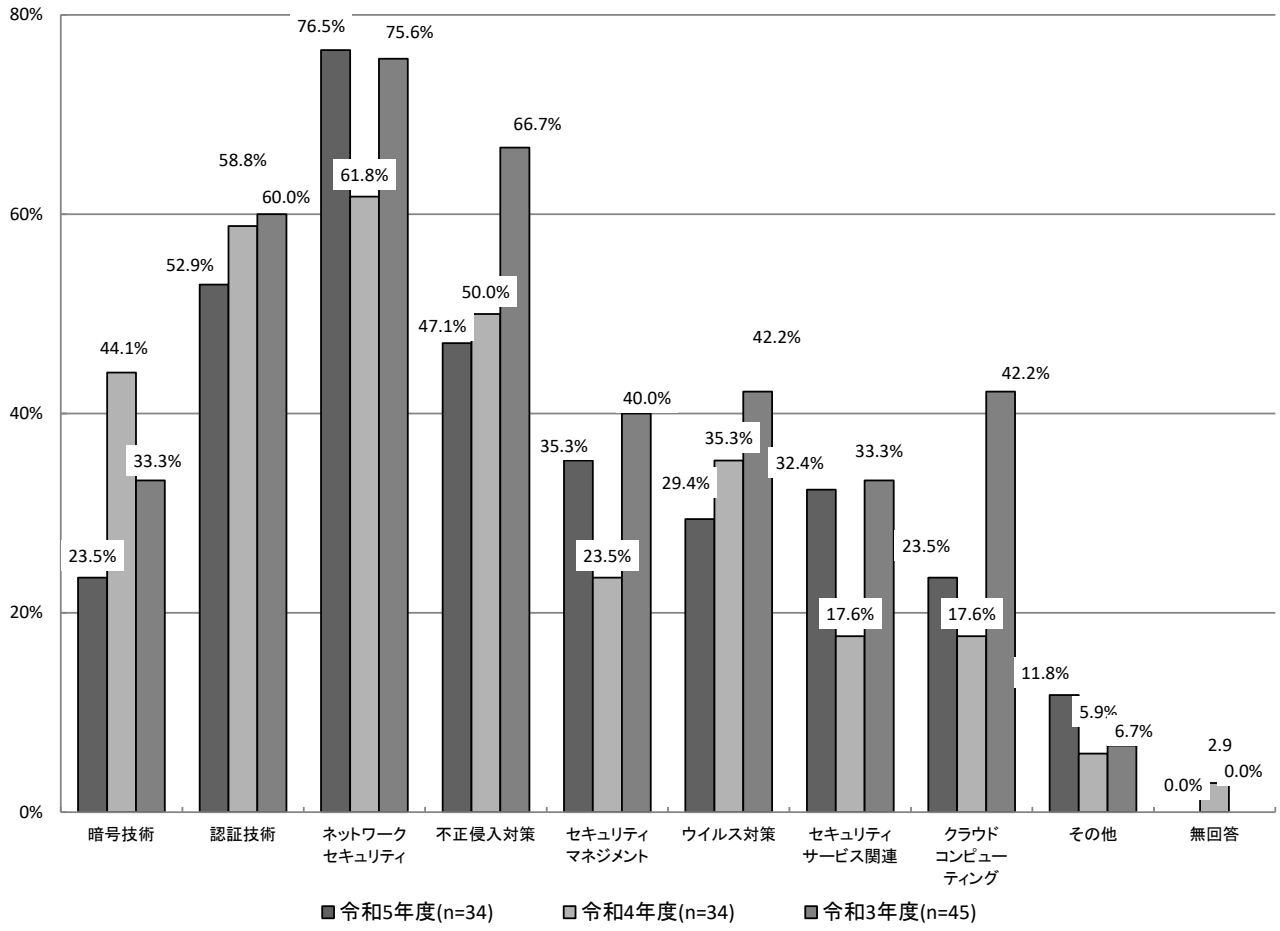


5.1.1　現在、取り組んでいる分野　【A-問2】

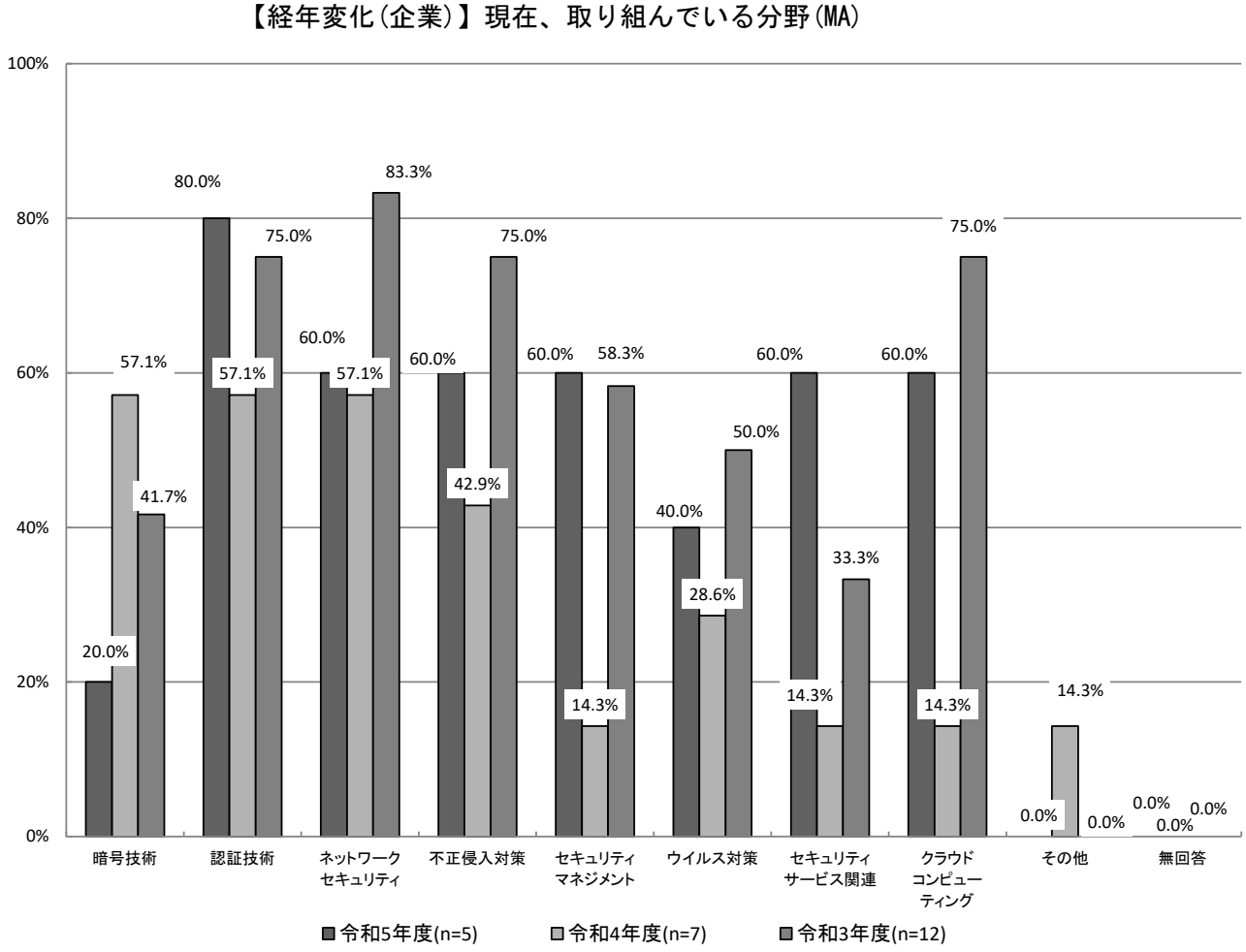
【経年変化】
　全体では、特に「暗号技術」が大きく減少している一方で、「ネットワークセキュリティ」「セキュリティサービス関連」が増加している。
　企業では、「暗号技術」が減少し、「セキュリティマネジメント」「セキュリティサービス関連」「クラウドコンピューティング」が増加している。大学では、「暗号技術」が減少し、「セキュリティサービス関連」が増加している。

【経年変化(全体)】
　昨年度と比較すると全体では、「暗号技術」が20.6ポイント減少しており、「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14.7ポイント増加している。

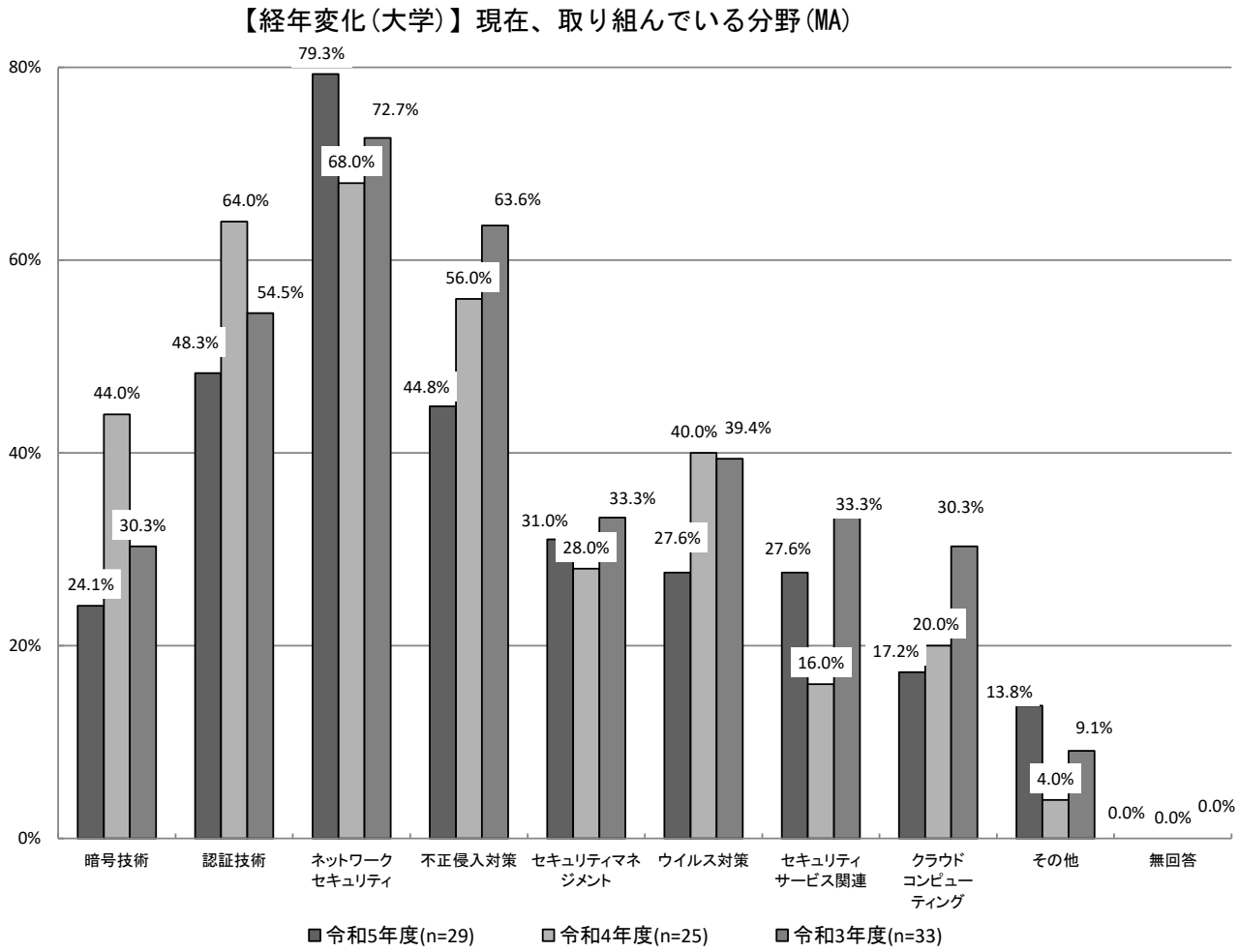
【経年変化(全体)】現在、取り組んでいる分野(MA)



【経年変化(企業)】
昨年度と比較すると企業では、「暗号技術」が37.1ポイント減少しており、「セキュリティマネジメント」「セキュリティサービス関連」「クラウドコンピューティング」が45.7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、「暗号技術」が19.9ポイント減少しており、「セキュリティサービス関連」が11.6ポイント増加している。

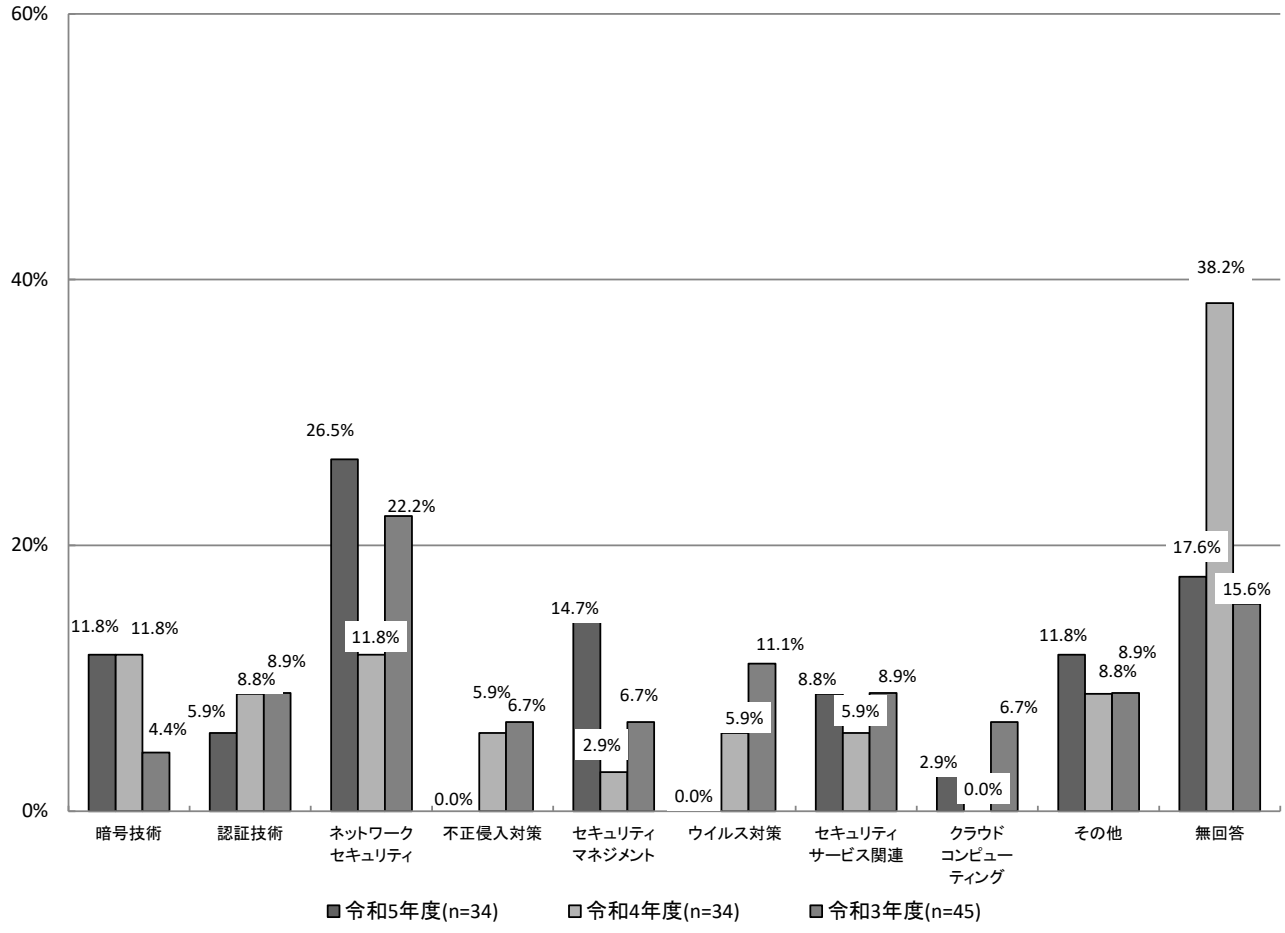


5.1.2 今後、もっとも力を入れたい分野 【A-問3】

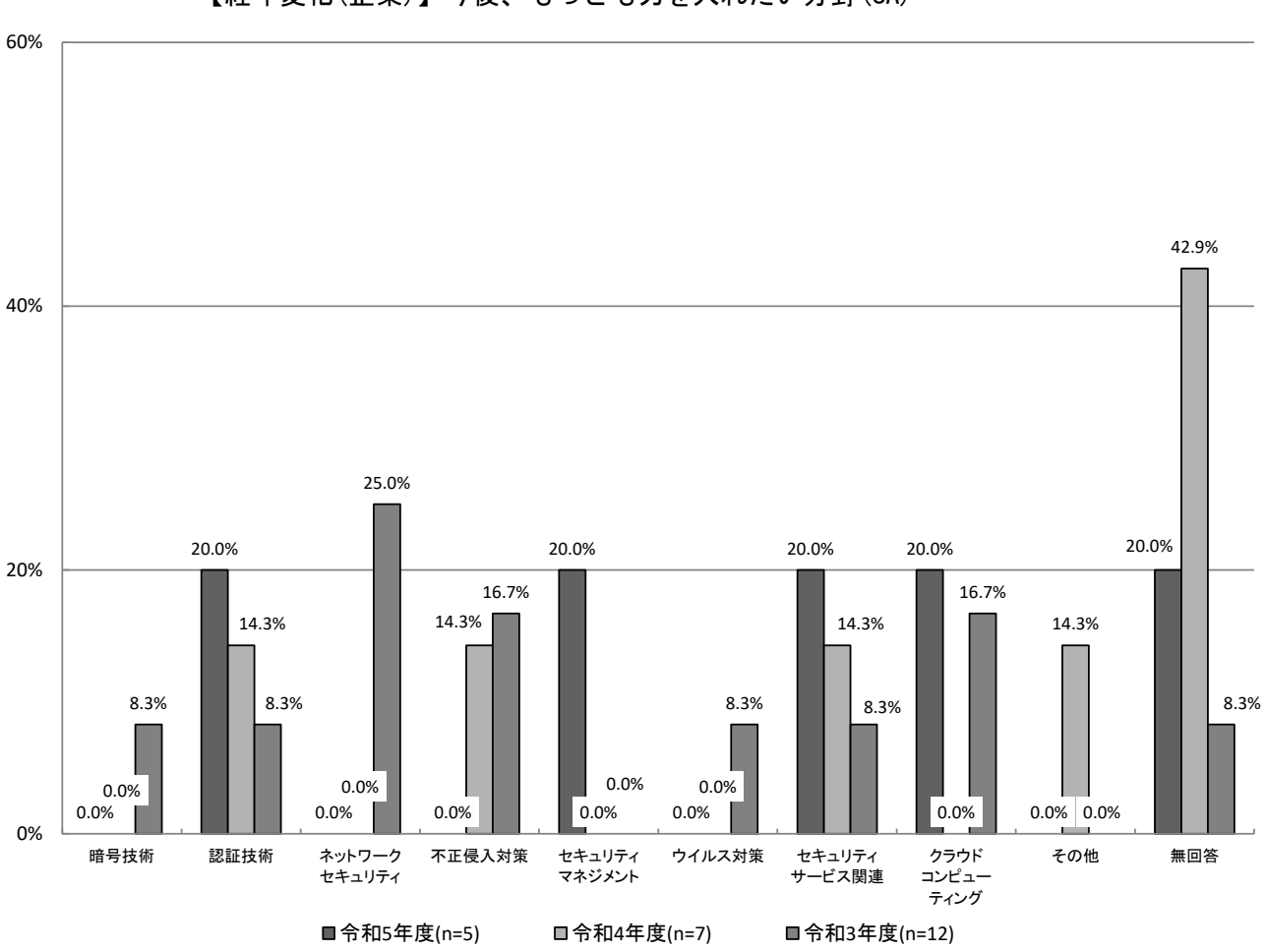
【経年変化】
全体では、「ネットワークセキュリティ」が増加しているが、一方、「不正侵入対策」「ウイルス対策」が減少している。
企業では、「セキュリティマネジメント」「クラウドコンピューティング」が増加しており、大学では「ネットワークセキュリティ」が昨年度よりも増加している。

【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14.7ポイント増加している。一方、「不正侵入対策」「ウイルス対策」が5.9ポイント減少している。

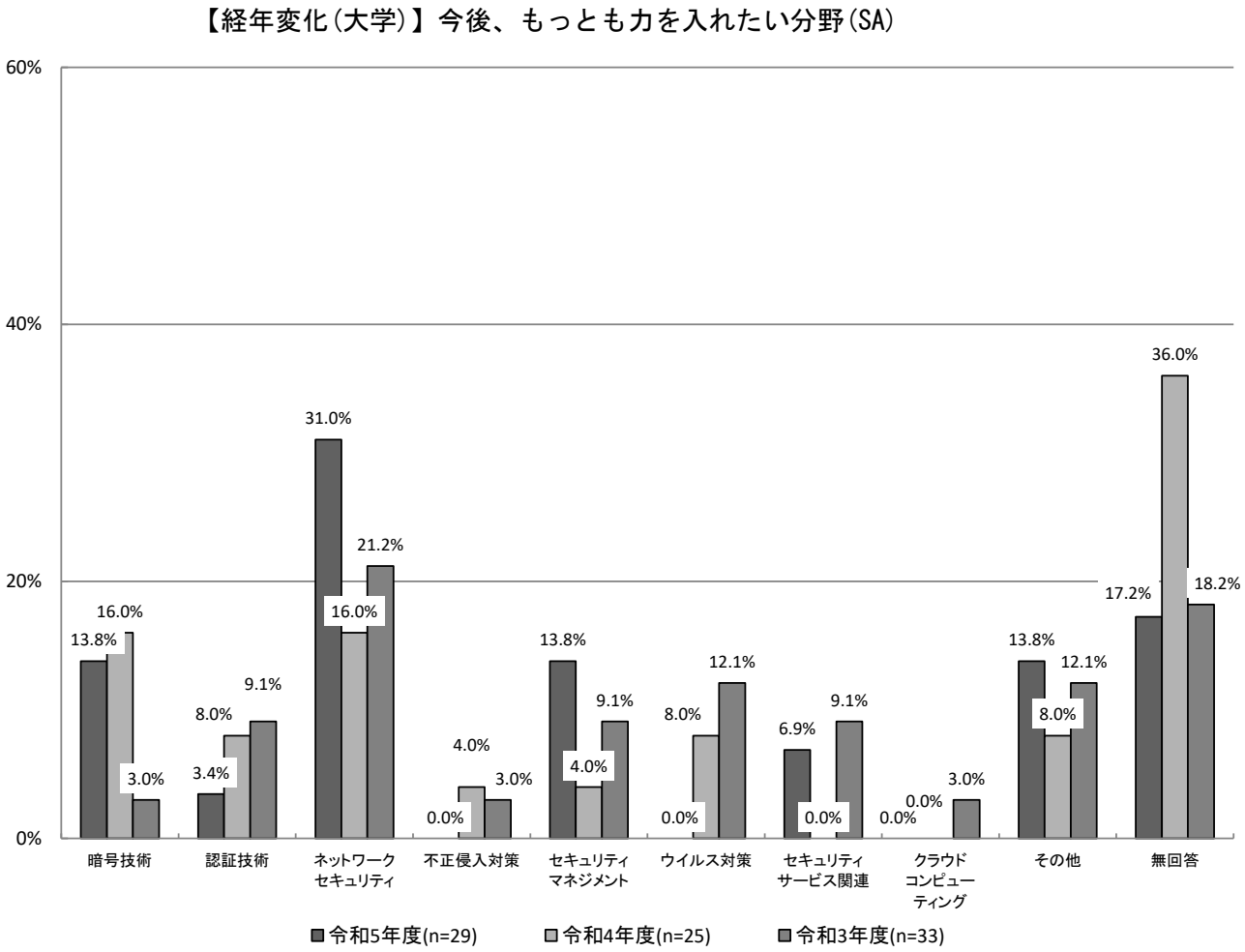
【経年変化(全体)】今後、もっとも力を入れたい分野(SA)



【経年変化(企業)】
昨年度と比較すると企業では、「セキュリティマネジメント」「クラウドコンピューティング」がそれぞれ20.0ポイント増加している。一方、「不正侵入対策」が14.3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、「ネットワークセキュリティ」が15.0ポイント増加している。一方、「ウイルス対策」は8.0ポイント減少している。



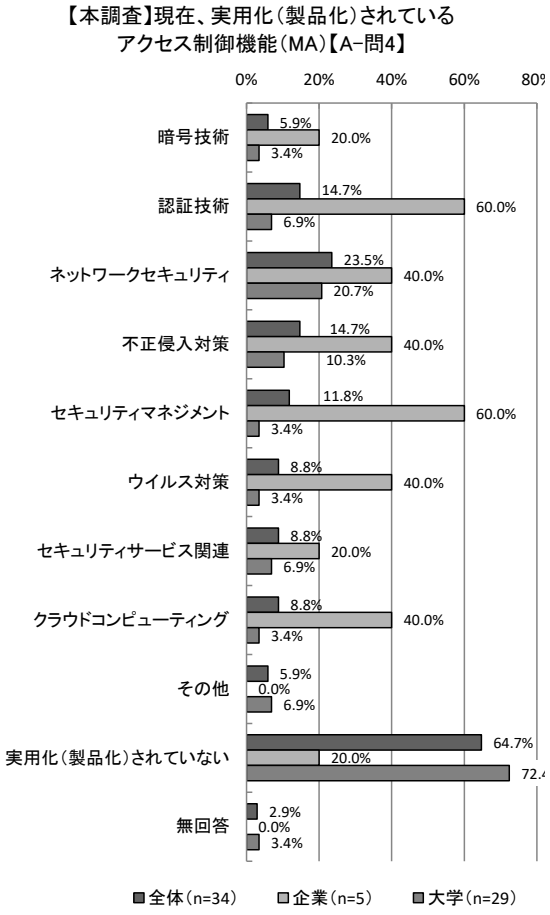
5.2 アクセス制御機能に関する実用化(製品化)に係る現状と今後の展望

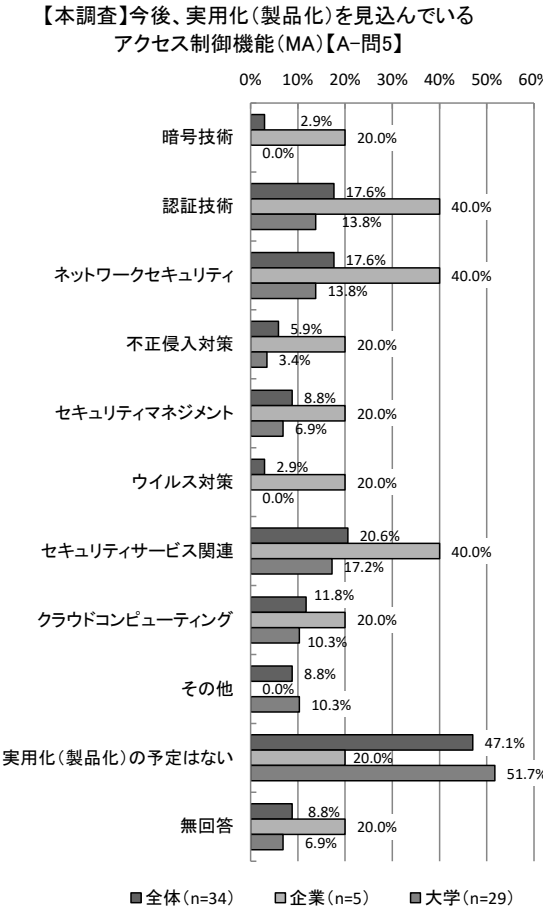
実用化（製品化）の現状については、「ネットワークセキュリティ」が最も多くなっている。

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、「セキュリティサービス関連」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23.5%（8件）で最も多く、次いで「認証技術」「不正侵入対策」がそれぞれ14.7%（5件）となっている。企業では「認証技術」「セキュリティマネジメント」が60.0%（3件）で最も多く、大学では「ネットワークセキュリティ」が20.7%（6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「セキュリティサービス関連」が20.6%（7件）で最も多く、次いで「認証技術」「ネットワークセキュリティ」がそれぞれ17.6%（6件）となっている。企業では「認証技術」「ネットワークセキュリティ」「セキュリティサービス関連」がそれぞれ40.0%（2件）で最も多く、大学では「セキュリティサービス関連」が17.2%（5件）で最も多くなっている。



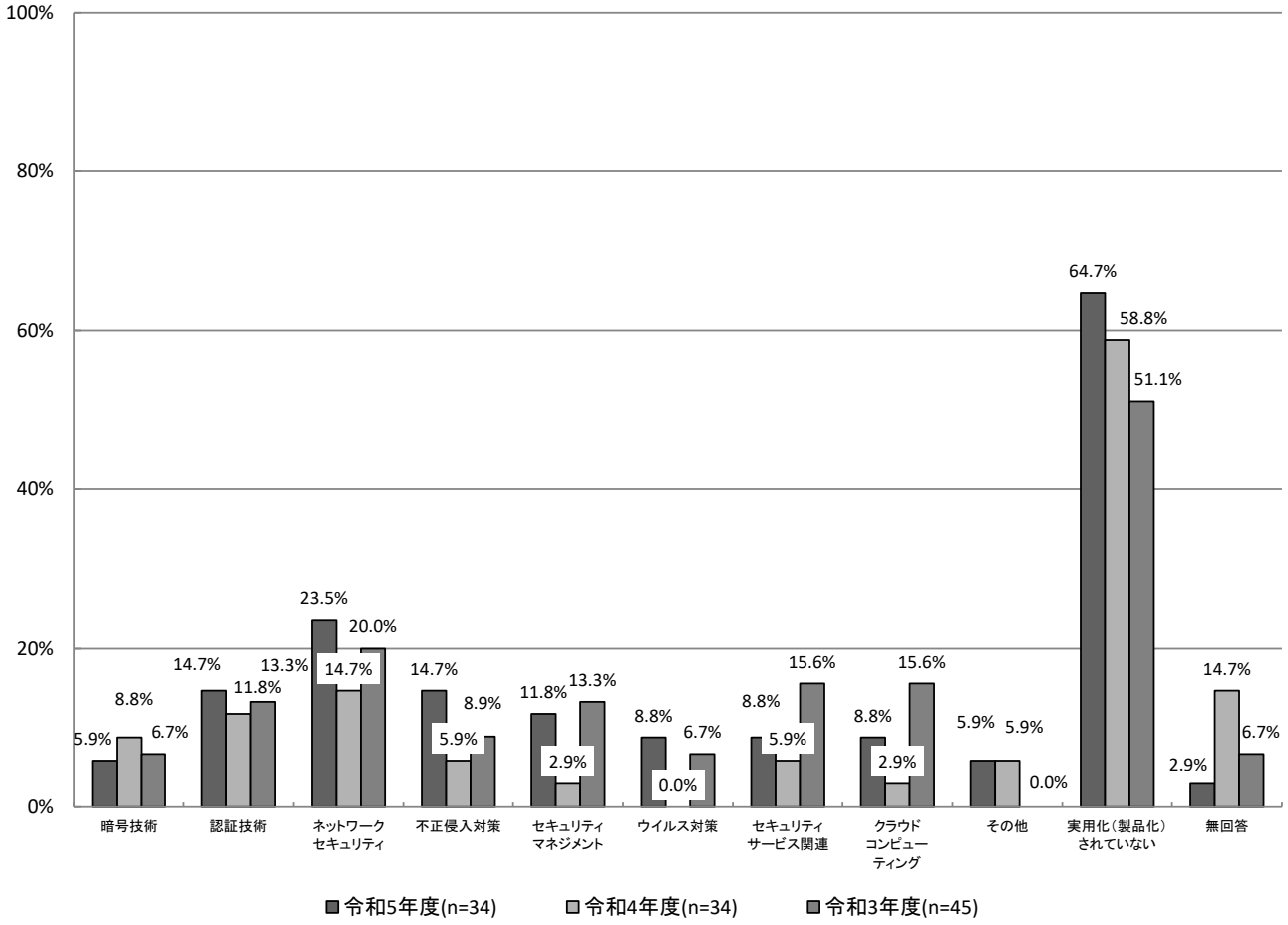


5.2.1　現在、実用化(製品化)されている分野　【A-問4】

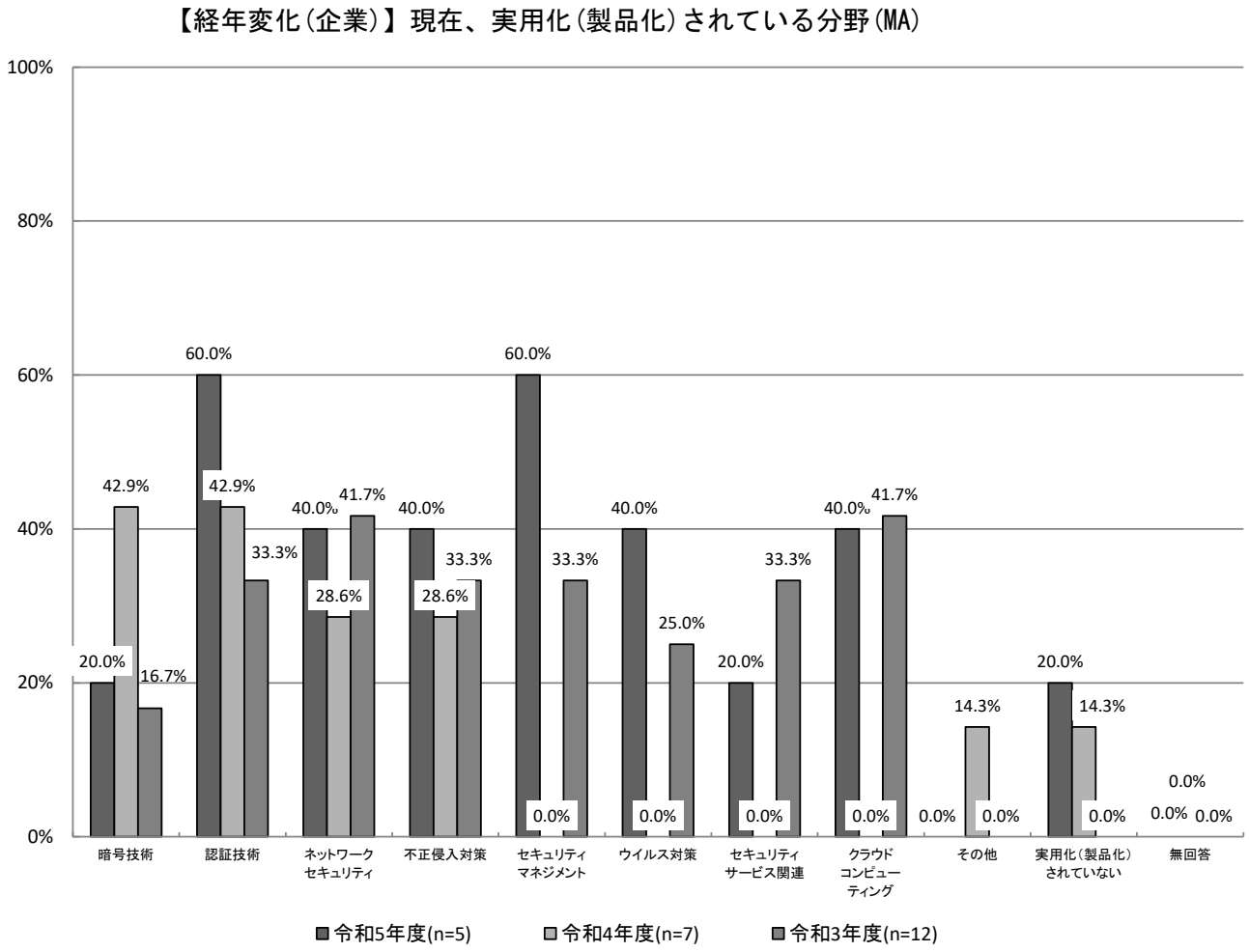
【経年変化】
　全体では、「暗号技術」の分野以外で増加している。
　企業では、「セキュリティマネジメント」が60.0ポイント増加し、大学では「不正侵入対策」が10.3ポイント、「ネットワークセキュリティ」が8.7ポイント増加している。

【経年変化(全体)】
　昨年度と比較すると「暗号技術」が2.9ポイント減少しており、それ以外の分野ではすべて増加している。

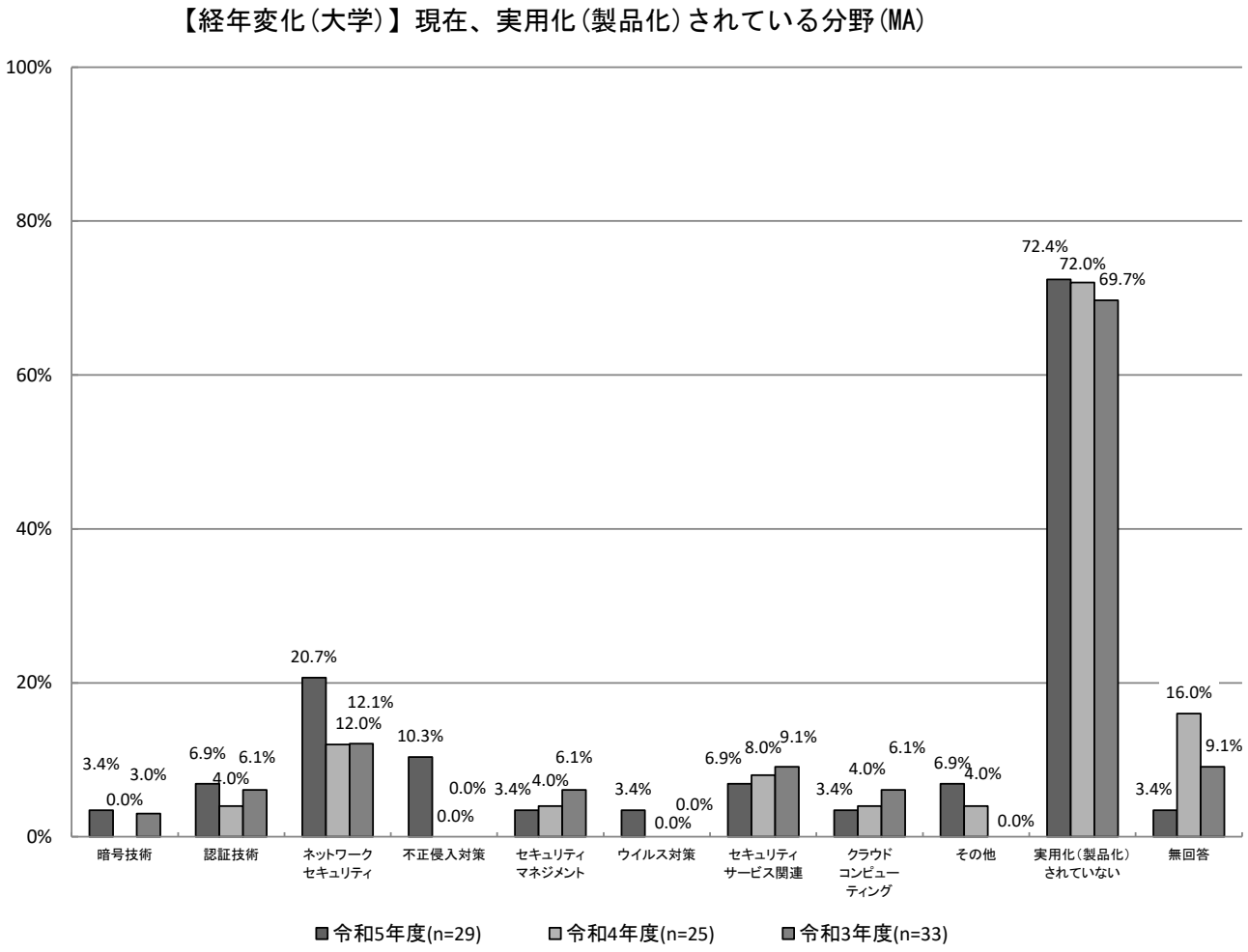
【経年変化(全体)】現在、実用化(製品化)されている分野(MA)



【経年変化(企業)】
昨年度と比較すると企業では、「セキュリティマネジメント」が60.0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企業では、「不正侵入対策」が10.3ポイント、「ネットワークセキュリティ」が8.7ポイント増加している。

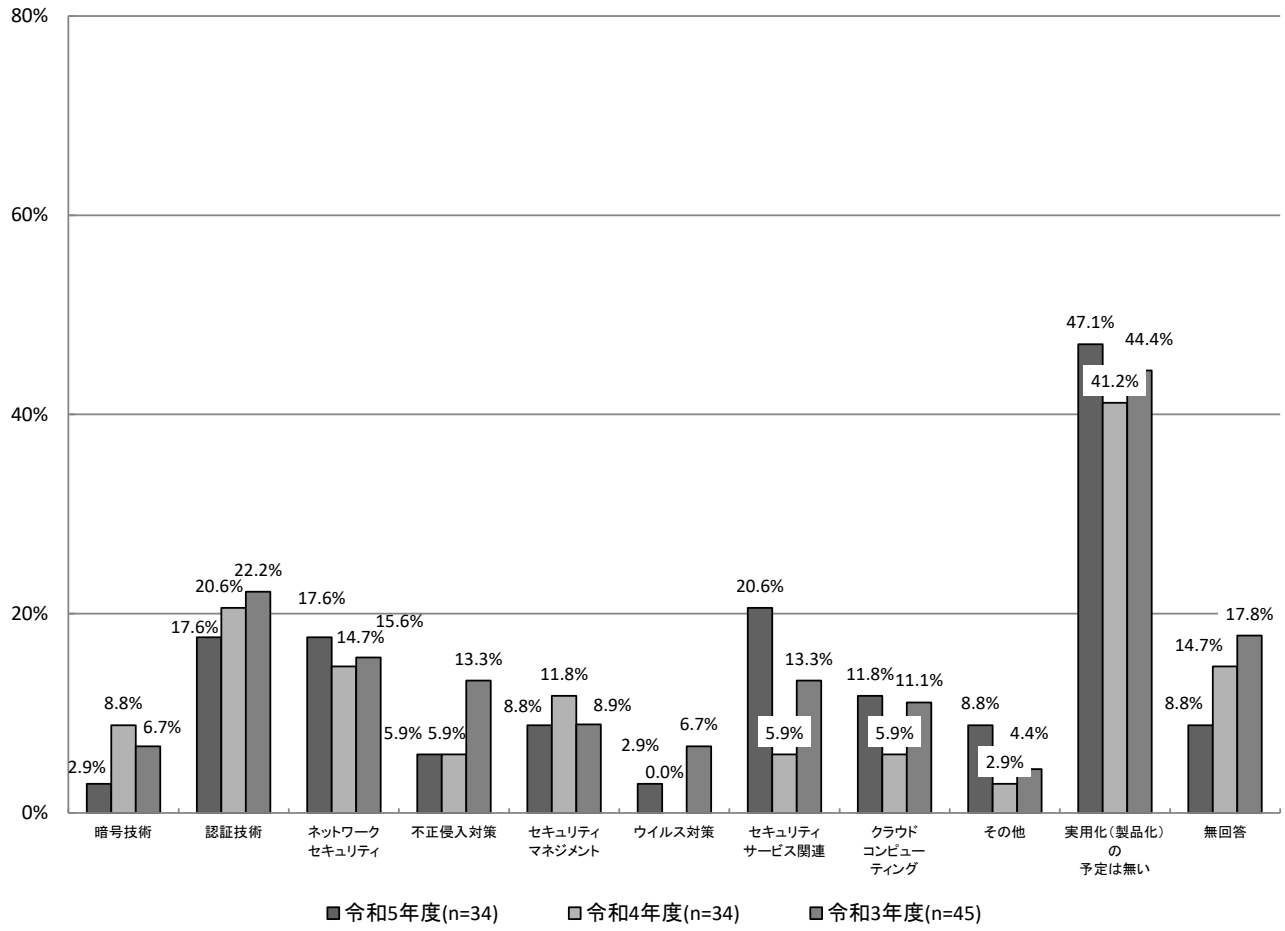


5.2.2　今後、実用化(製品化)を見込んでいる分野　【A-問5】

【経年変化】
　全体では、「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」などが増加している。
　企業では「セキュリティサービス関連」「ウイルス対策」「クラウドコンピューティング」などが増加しており、大学では「セキュリティサービス関連」が最も増加している。

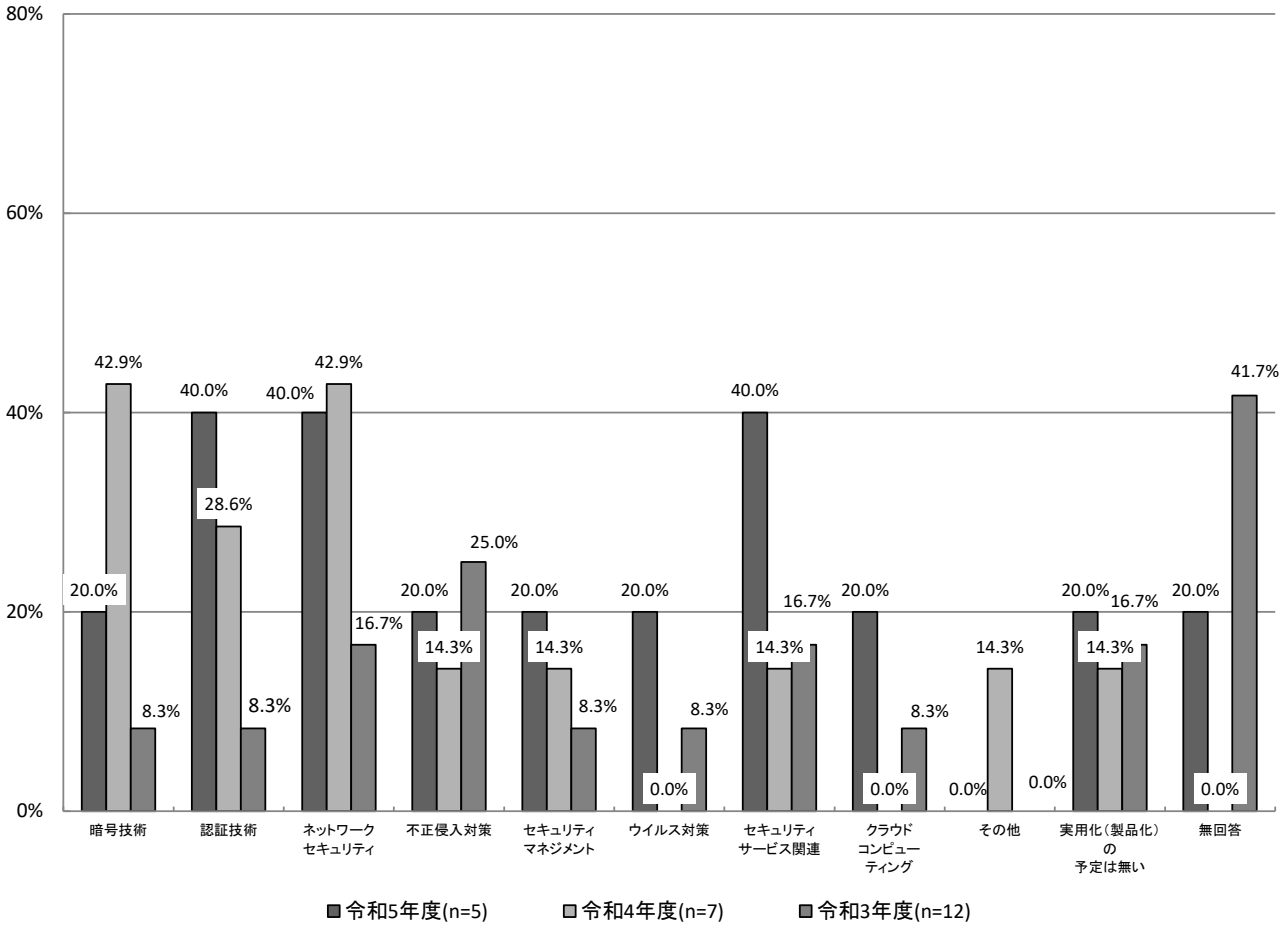
【経年変化(全体)】
　昨年度と比較すると全体では、「セキュリティサービス関連」が14.7ポイント増加している。次いで、「クラウドコンピューティング」が5.9ポイント増加している。

【経年変化(全体)】今後、実用化(製品化)を見込んでいる分野(MA)



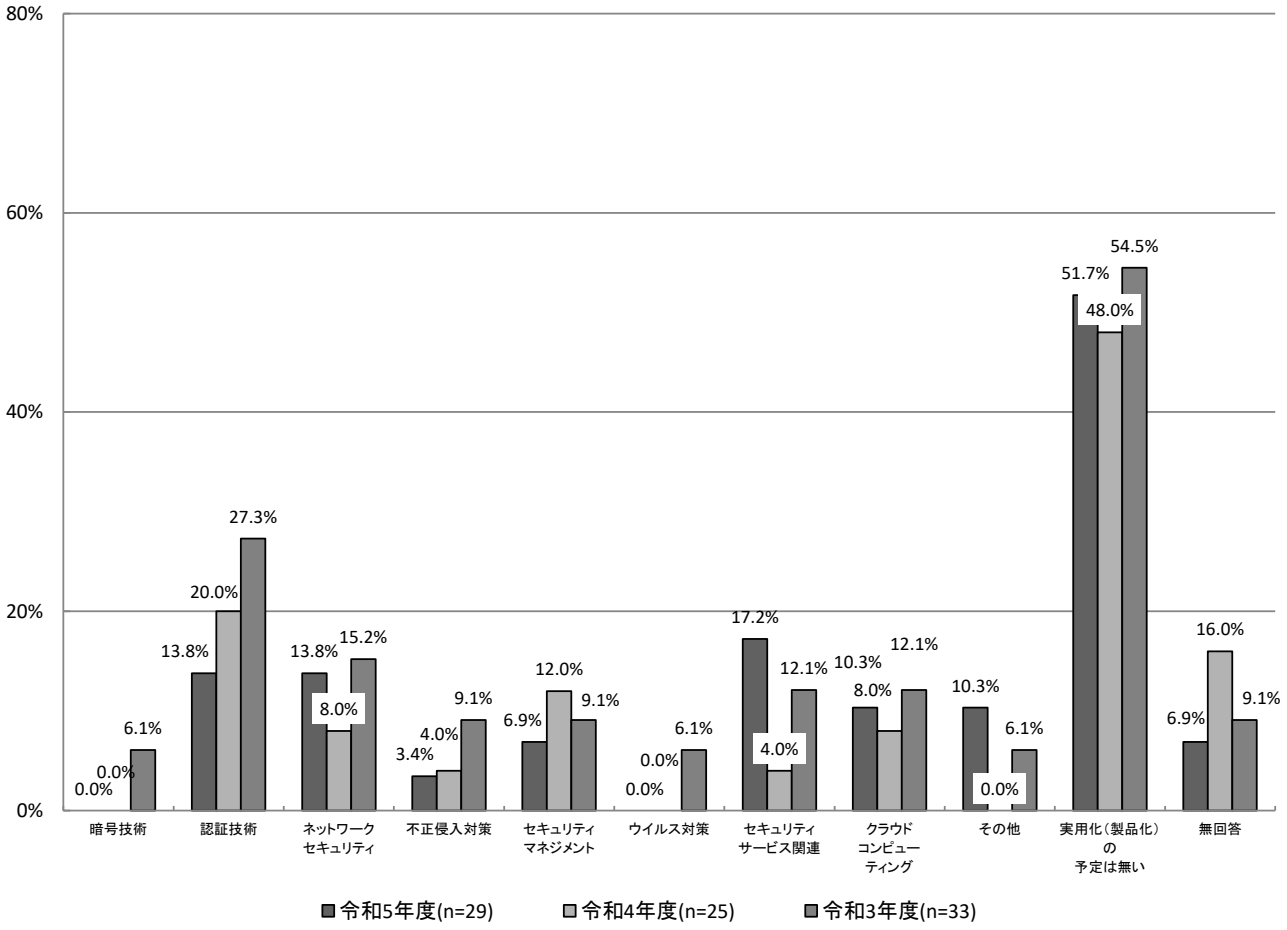
【経年変化(企業)】
昨年度と比較すると企業では、「セキュリティサービス関連」が25.7ポイントと最も増加しており、次いで「ウイルス対策」「クラウドコンピューティング」がそれぞれ20.0ポイント増加している。

【経年変化(企業)】今後、実用化(製品化)を見込んでいる分野(MA)



【経年変化(大学)】
昨年度と比較すると大学では、「セキュリティサービス関連」が13.2ポイントと最も増加している。一方、「認証技術」が6.2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)

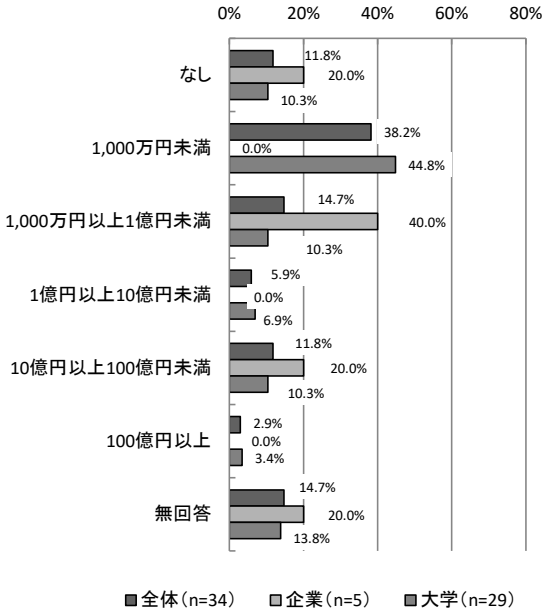


5.3 研究開発体制

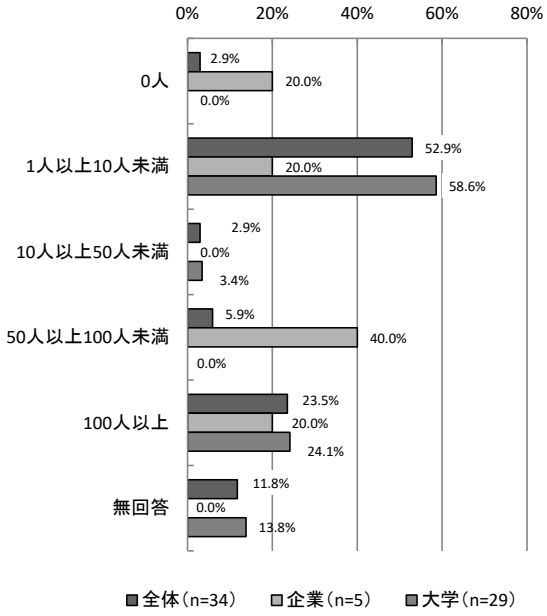
研究開発費について、企業は1,000万円以上1億円未満」が最も多く、大学は「1,000万円未満」が最も多くなっている。
研究開発人数について、企業は「50人以上100人未満」、大学は「1人以上10人未満」が最も多くなっている。

年間の研究開発費については、全体では「1,000万円未満」が38.2%（13件）で最も多くなっている。企業では「1,000万円以上1億円未満」が40.0%（2件）で最も多く、大学では「1,000万円未満」が44.8%（13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52.9%（18件）と最も多くなっている。企業では「50人以上100人未満」が40.0%（2件）で最も多く、大学では「1人以上10人未満」が58.6%（17件）で最も多くなっている。

【本調査】年間の研究開発費（SA）【A-問6】



【本調査】研究開発に携わっている人数（SA）【A-問7】

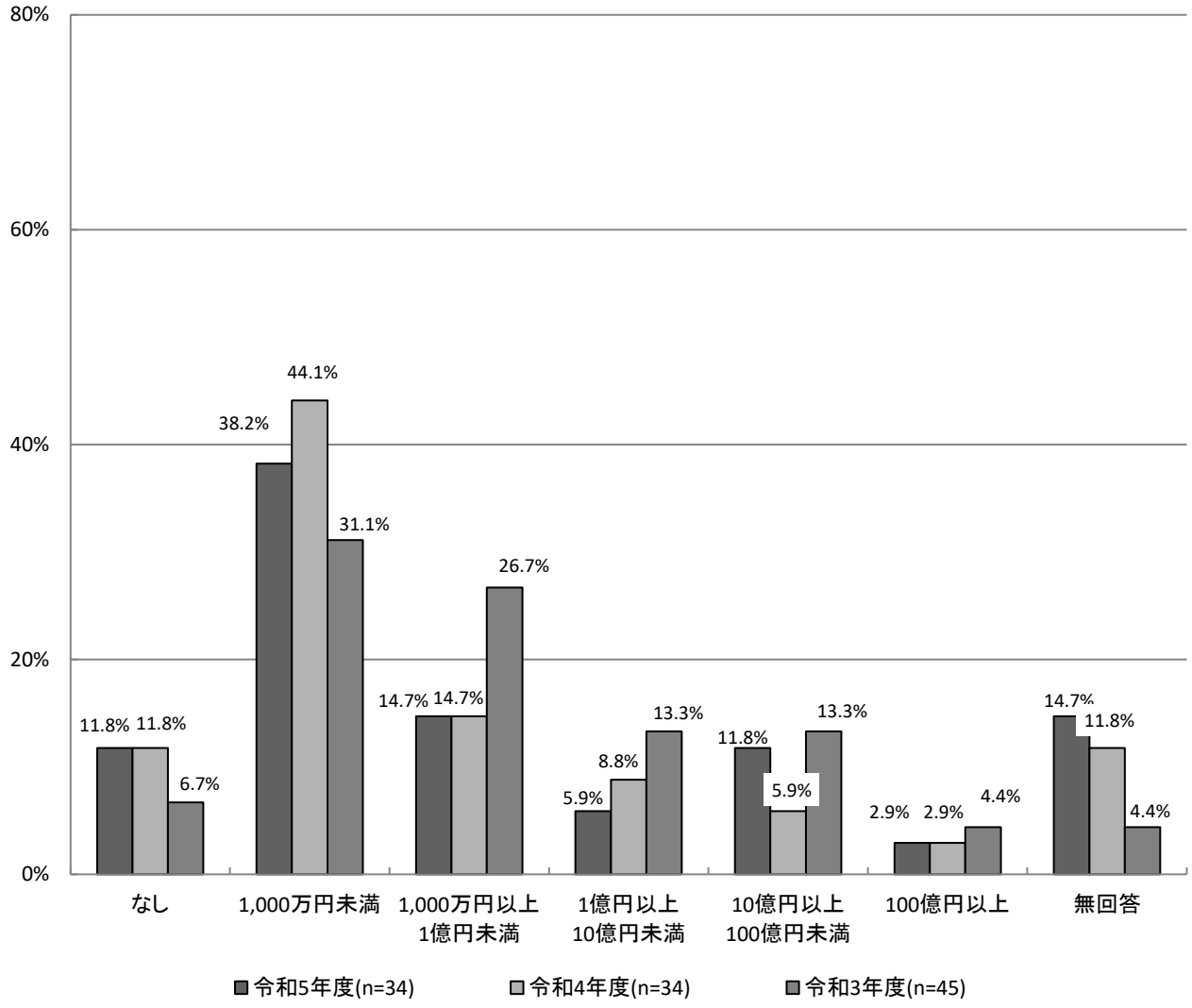


5.3.1　年間の研究開発費　【A-問6】

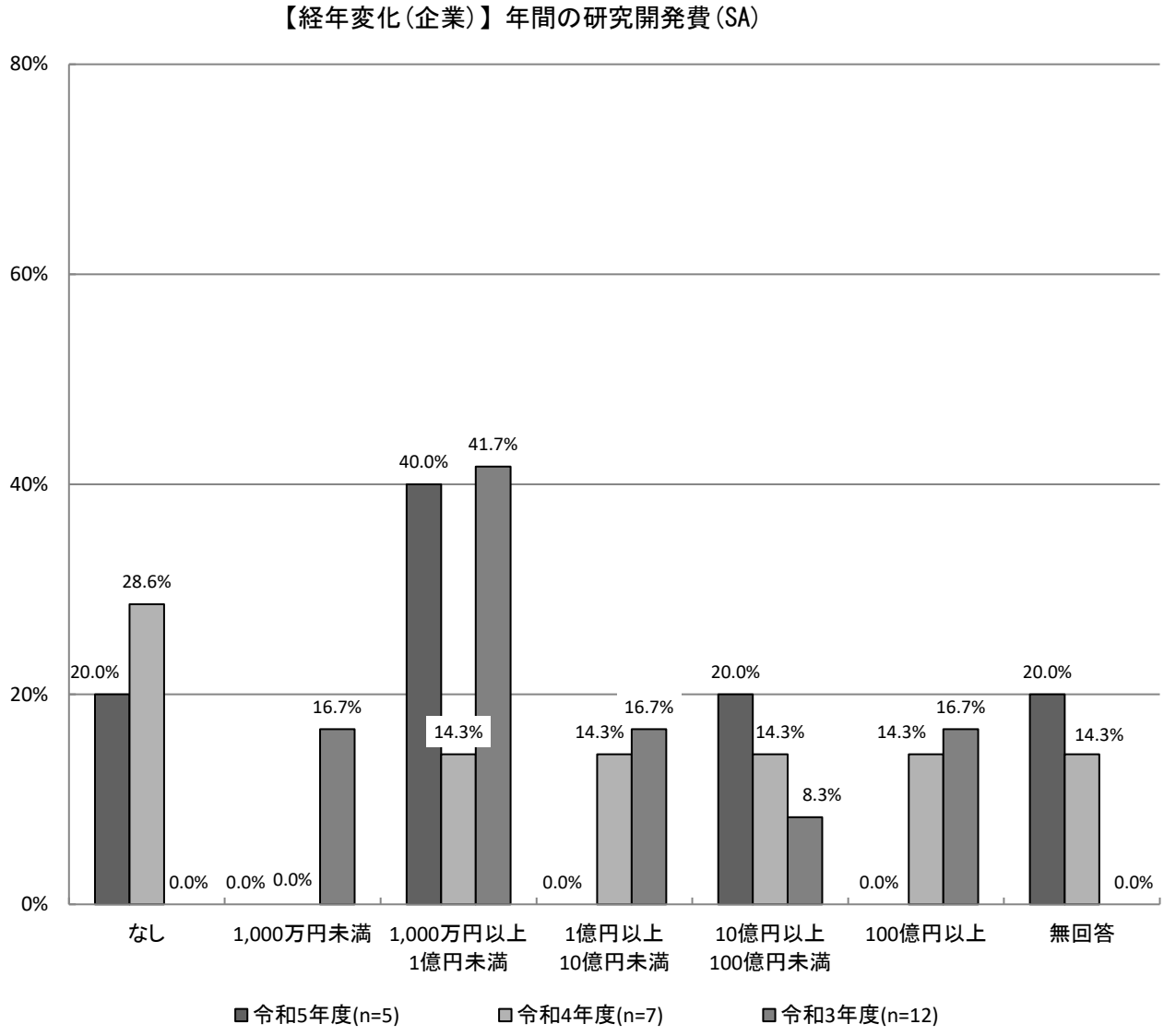
【経年変化】
　全体では「10億円以上100億円未満」が、企業では「1,000万円以上1億円未満」が最も増加している。
　大学では「1,000万円未満」が最も減少している。

【経年変化(全体)】
　昨年度と比較すると全体では、「10億円以上100億円未満」が5.9ポイント増加している。一方、「1,000万円未満」が5.9ポイント減少している。

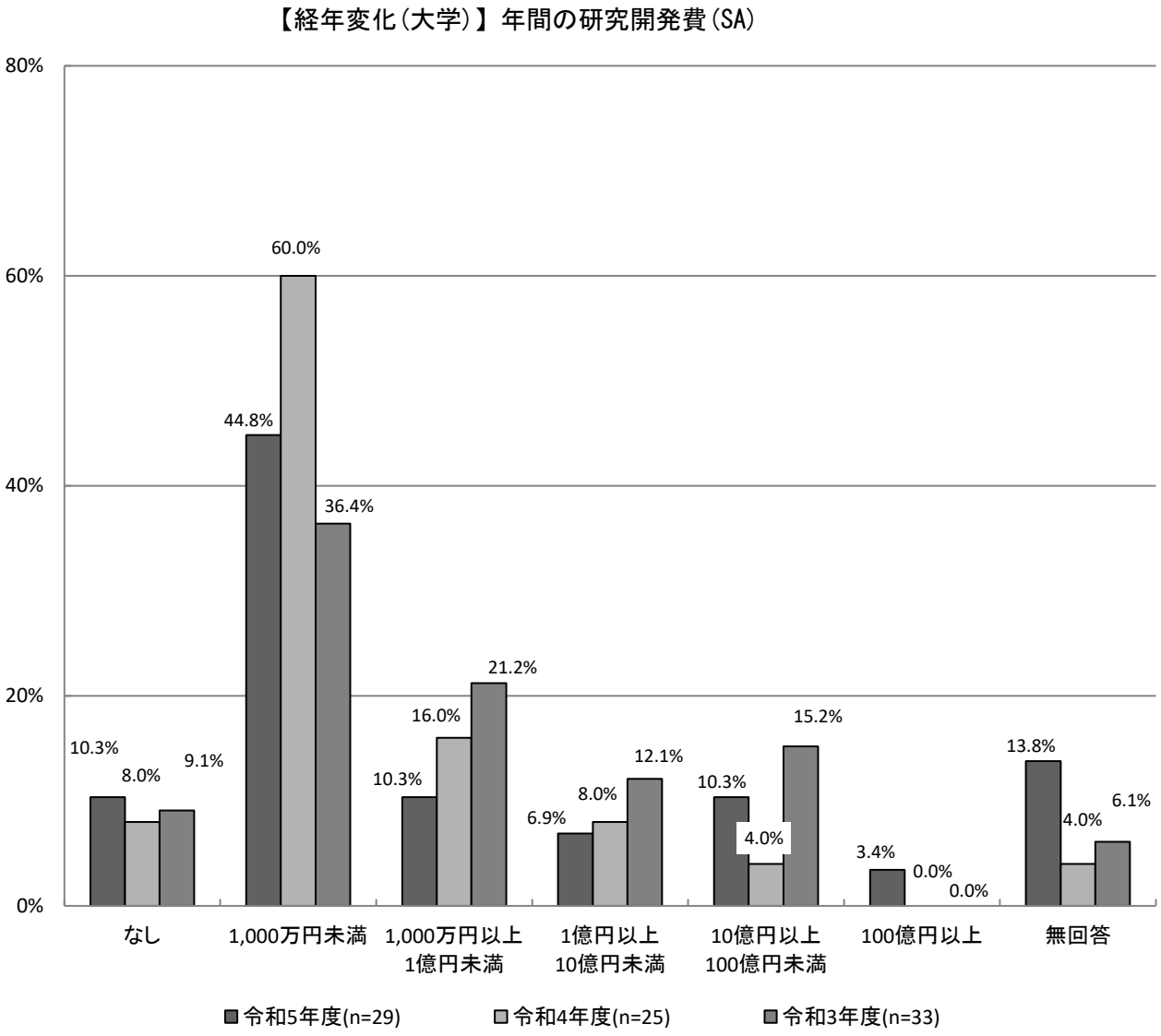
【経年変化(全体)】年間の研究開発費(SA)



【経年変化(企業)】
昨年度と比較すると企業では、「1,000万円以上1億円未満」が25.7ポイント増加している。一方、「1億円以上10億円未満」「100億円以上」がそれぞれ14.3ポイント減少している。



【経年変化(大学)】
昨年度と比較すると大学では、「1,000万円未満」が15.2ポイント減少している。一方、「10億円以上100億円未満」が6.3ポイントと最も増加している。

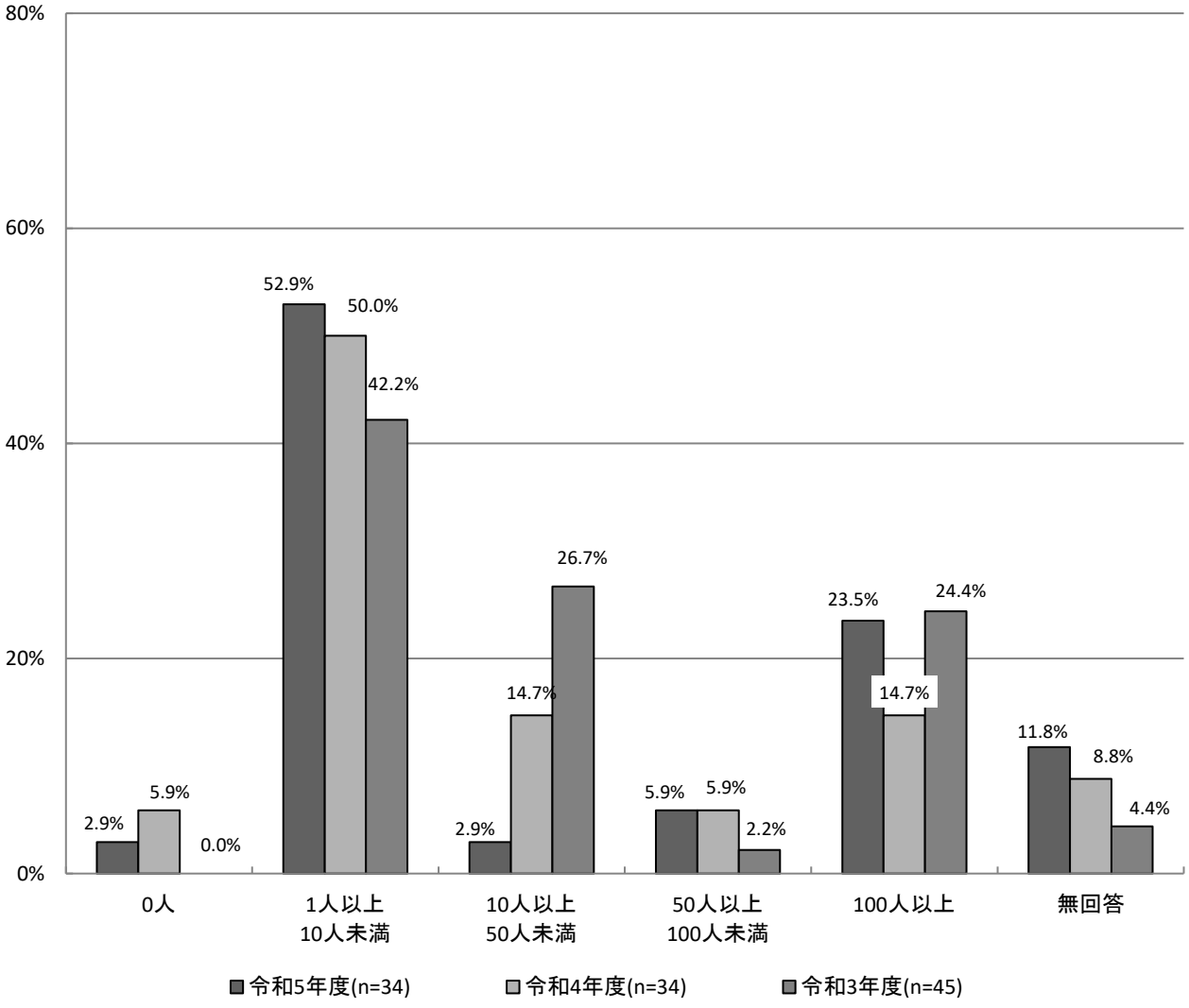


5.3.2　研究開発に携わっている人数　【A-問7】

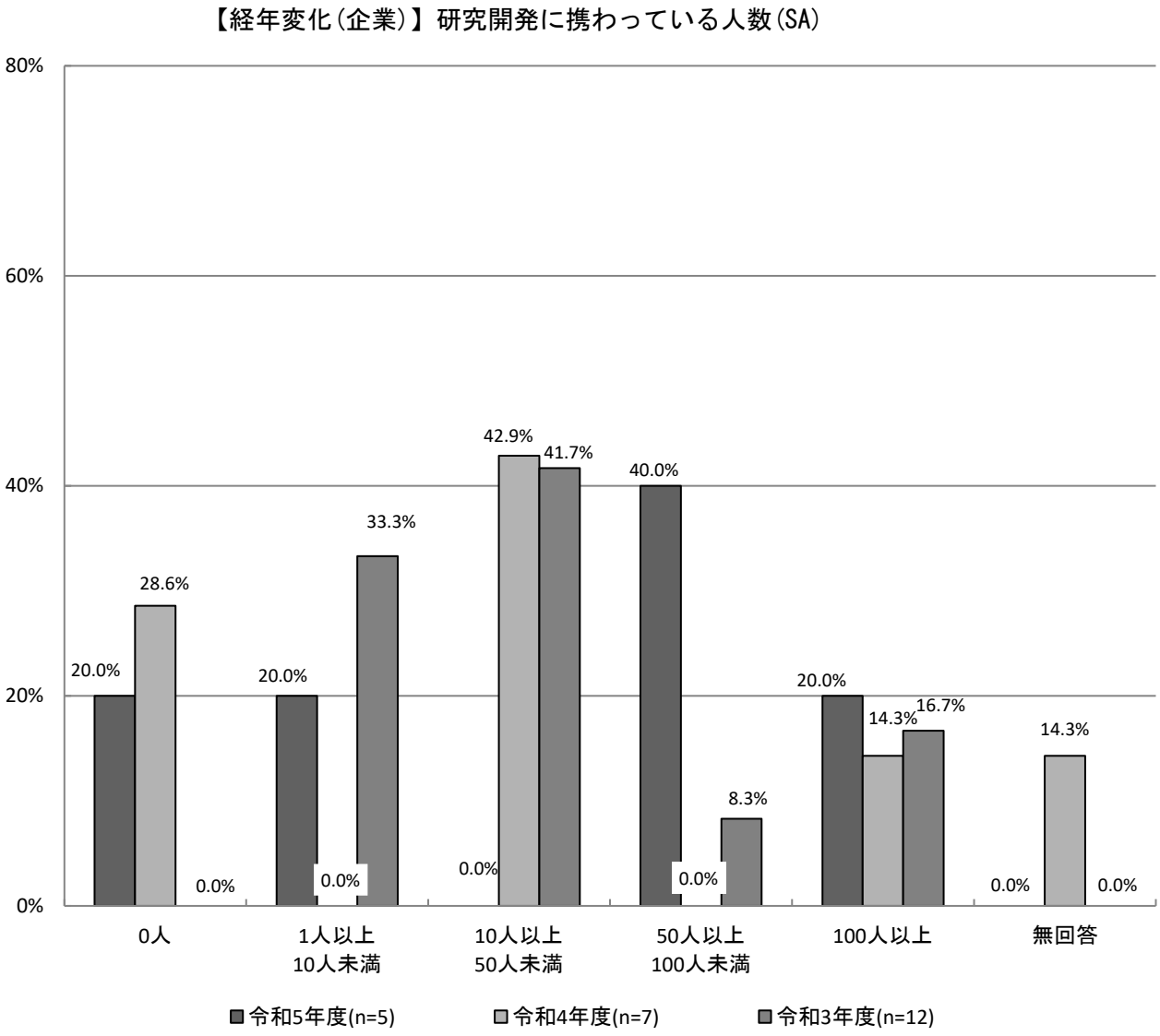
【経年変化】
　全体では「10人以上50人未満」が最も減少している。企業では「10人以上50人未満」減少している一方、「50人以上100人未満」が増加している。大学では、「「1人以上10人未満」」などが減少している。

【経年変化(全体)】
　昨年度と比較すると全体では、「10人以上50人未満」が11.8ポイント減少している。一方、「100人以上」が8.8ポイント増加している。

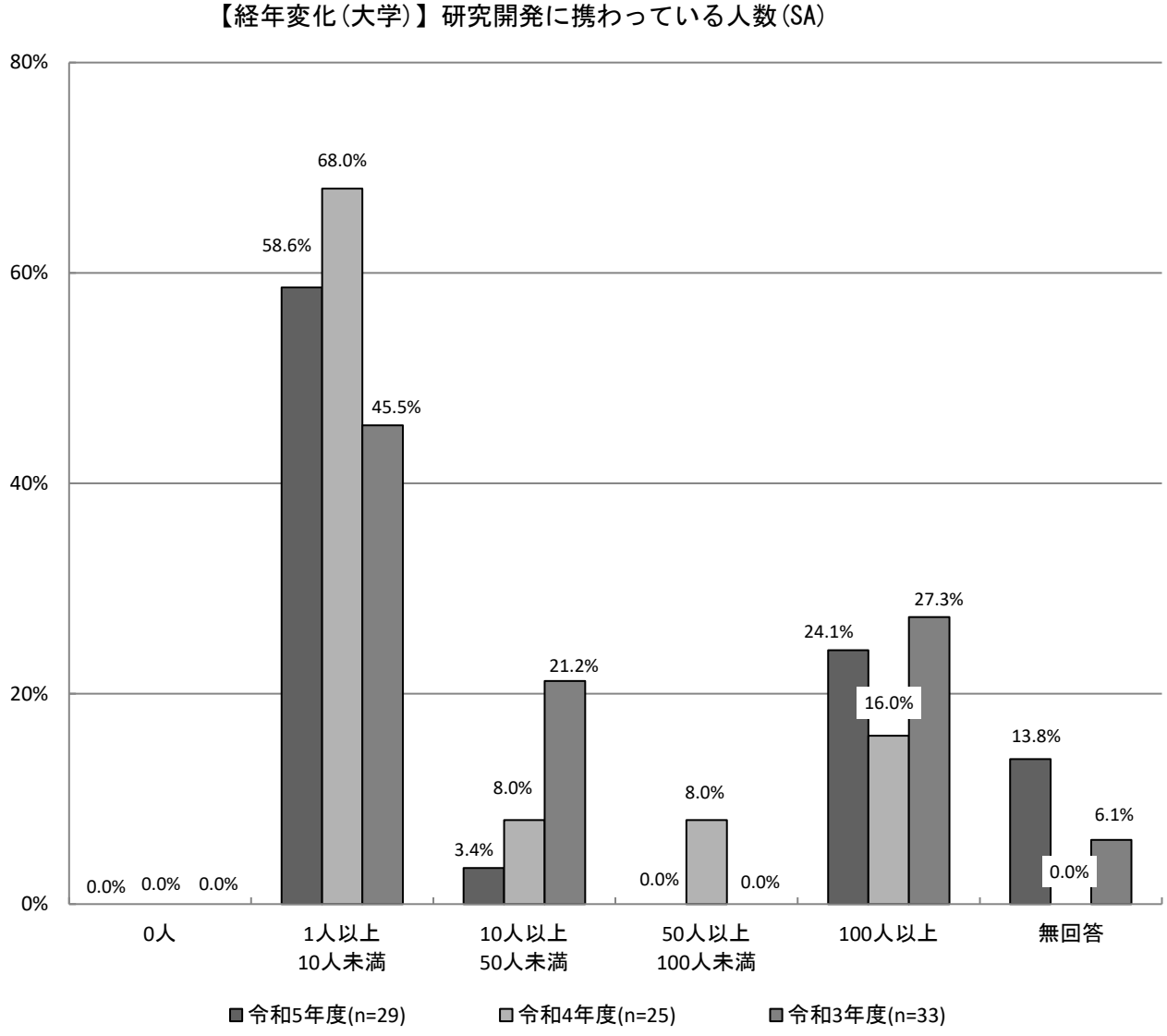
【経年変化(全体)】研究開発に携わっている人数(SA)



【経年変化(企業)】
昨年度と比較すると企業では、「10人以上50人未満」が42.9ポイント減少している。一方、「50人以上100人未満」が40.0ポイント増加している。



【経年変化(大学)】
昨年度と比較すると大学では、「1人以上10人未満」が9.4ポイント減少しており、次いで「50人以上100人未満」が8.0ポイント減少している。一方、「100人以上」は8.1ポイント増加している。



5.4 実用化された製品及び研究開発中の技術・サービス

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

(1)何を守るか？
- ・どのコンポーネントを守るのか、という観点から見た分類。
- ・ネットワーク、サーバ、クライアント等の大きなくくりの視点で見る。

(2)何から保護するか？
- ・どのような脅威から守るのか、という観点から見た分類。
- ・買う側の立場から見て、どのような対策をしたいかという視点でもある。

(3)どのようなセキュリティ上の効果があるか？
- ・どのような効果を狙ったものか、という観点から見た分類。
- ・事前対応、事中・事後対応という視点でもある。

(4)どのような機能を持っているか？
- ・どのような技術要素を使って守るのか、という観点から見た分類。
- ・売る側や開発する側の立場から見た、機能要素という視点でもある。

(5)どのようなレイヤーのセキュリティを守るか？
- ・どのようなレイヤーでセキュリティを守るのか、という観点から見た分類。

(6)どのようなサービスか？
- ・サービスの場合、どのような内容か、という観点から見た分類。

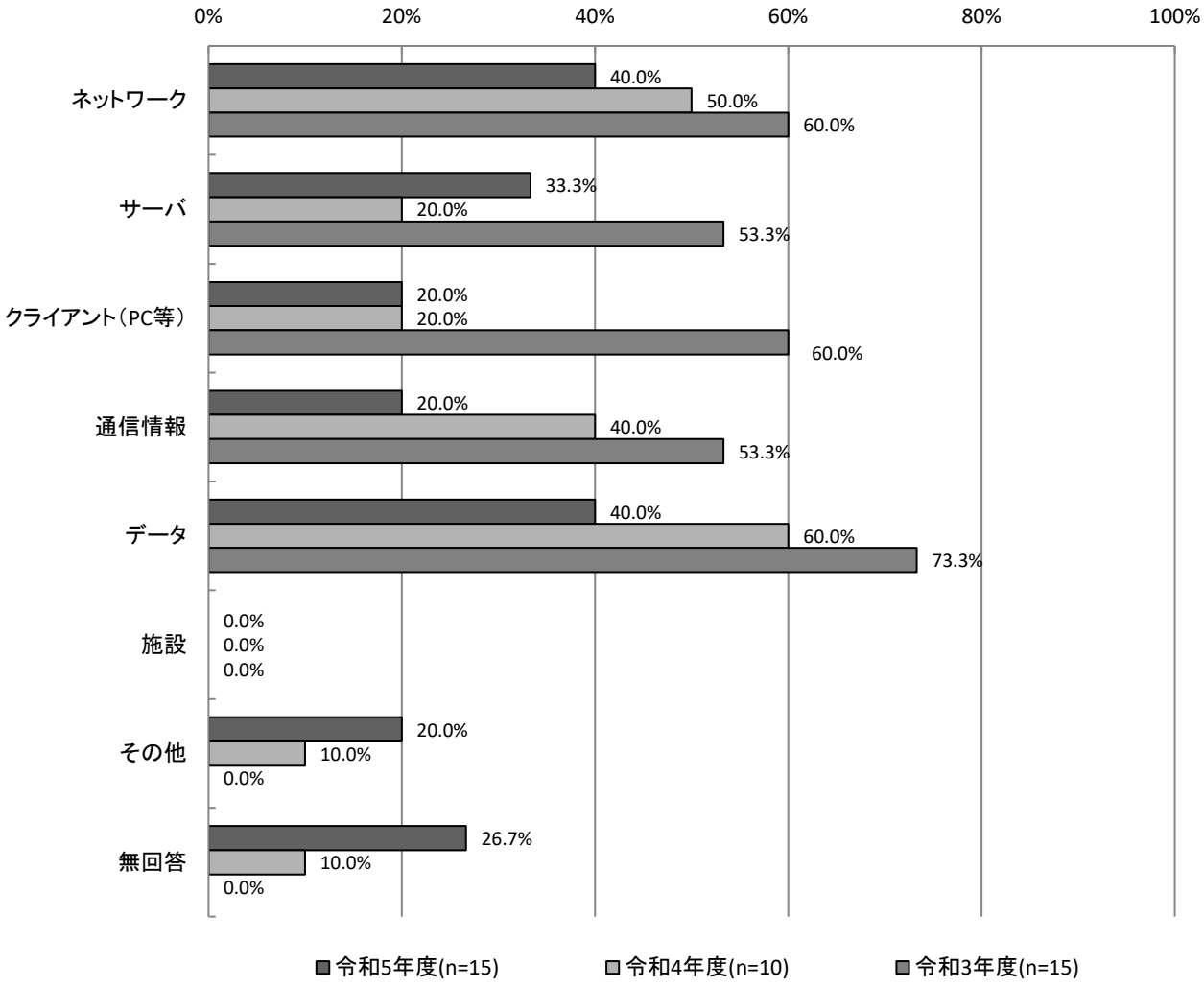
5.4.1　何を守るか？

Ⅰ.実用化(製品化)されているもの

実用化（製品化）されているものについては、「ネットワーク」「データ」がそれぞれ40.0%（6件）で最も多く、次いで「サーバ」が33.3%（5件）となっている。

昨年度と比較すると、「通信情報」「データ」がそれぞれ20.0ポイント減少している。

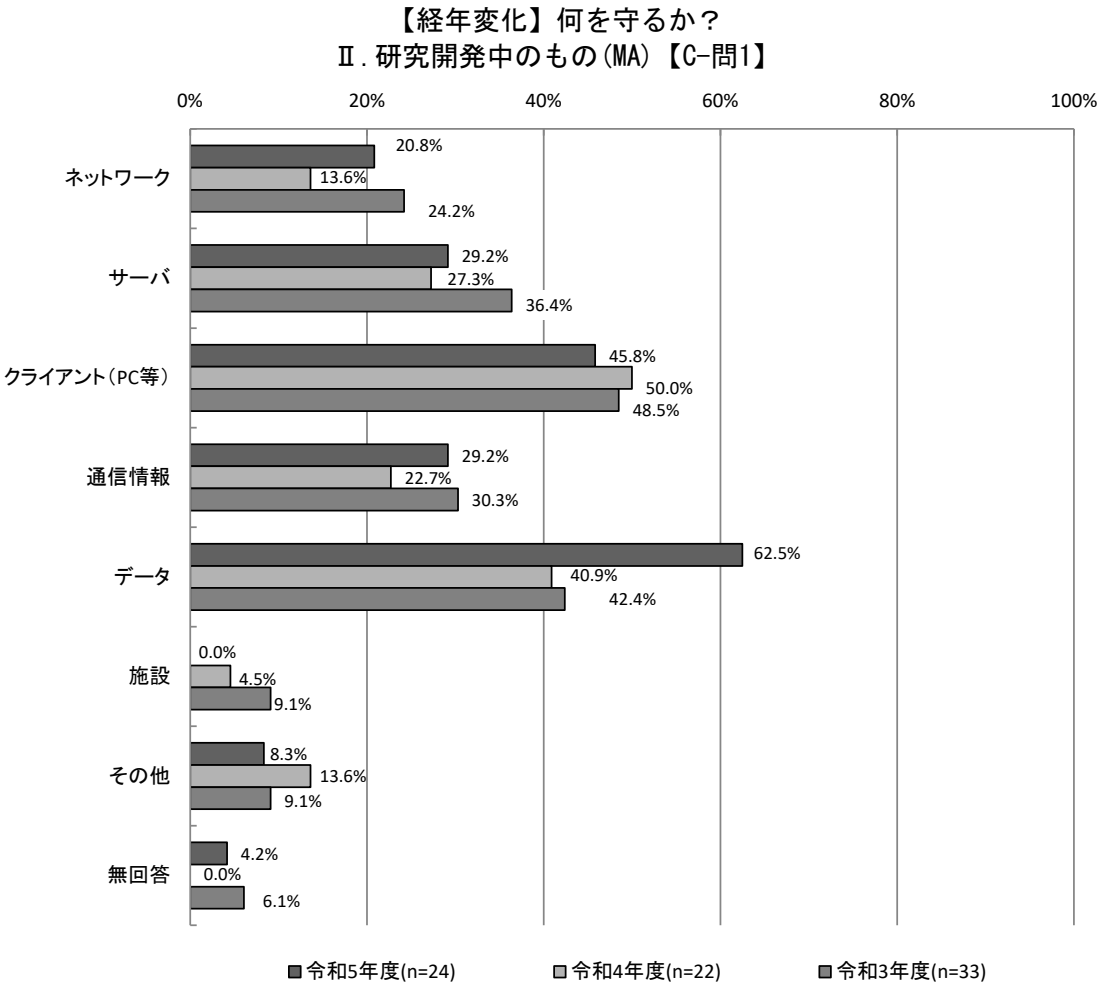
Ⅰ.実用化(製品化)されているもの(MA)【B-問1】



Ⅱ.研究開発中のもの

研究開発中のものについては、「データ」が62.5%（15件）で最も多く、次いで「クライアント(PC等)」が45.8%（11件）、「サーバ」「通信情報」が29.2%（7件）となっている。

昨年度と比較すると、「データ」が21.6ポイント増加しており、次いで「ネットワーク」が7.2ポイント増加している。



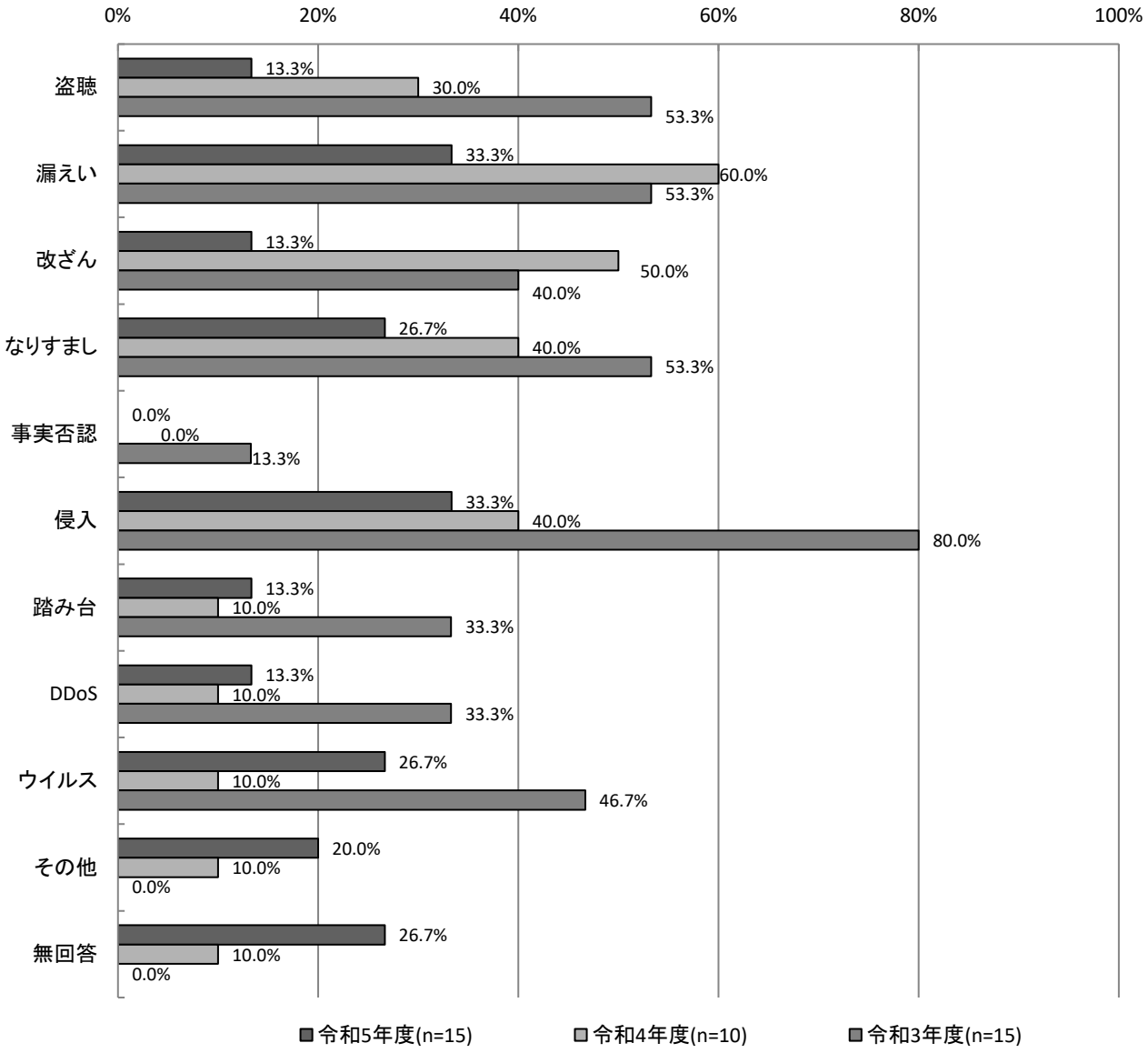
5.4.2　何から保護するか？

Ⅰ.実用化(製品化)されているもの

実用化（製品化）されているものについては、「漏えい」「侵入」が33.3%（5件）で最も多く、次いで「なりすまし」「ウイルス」が26.7%（4件）となっている。

昨年度と比較すると、「改ざん」が36.7ポイント、「漏えい」が26.7ポイント減少している。一方、「ウイルス」が16.7ポイント増加している。

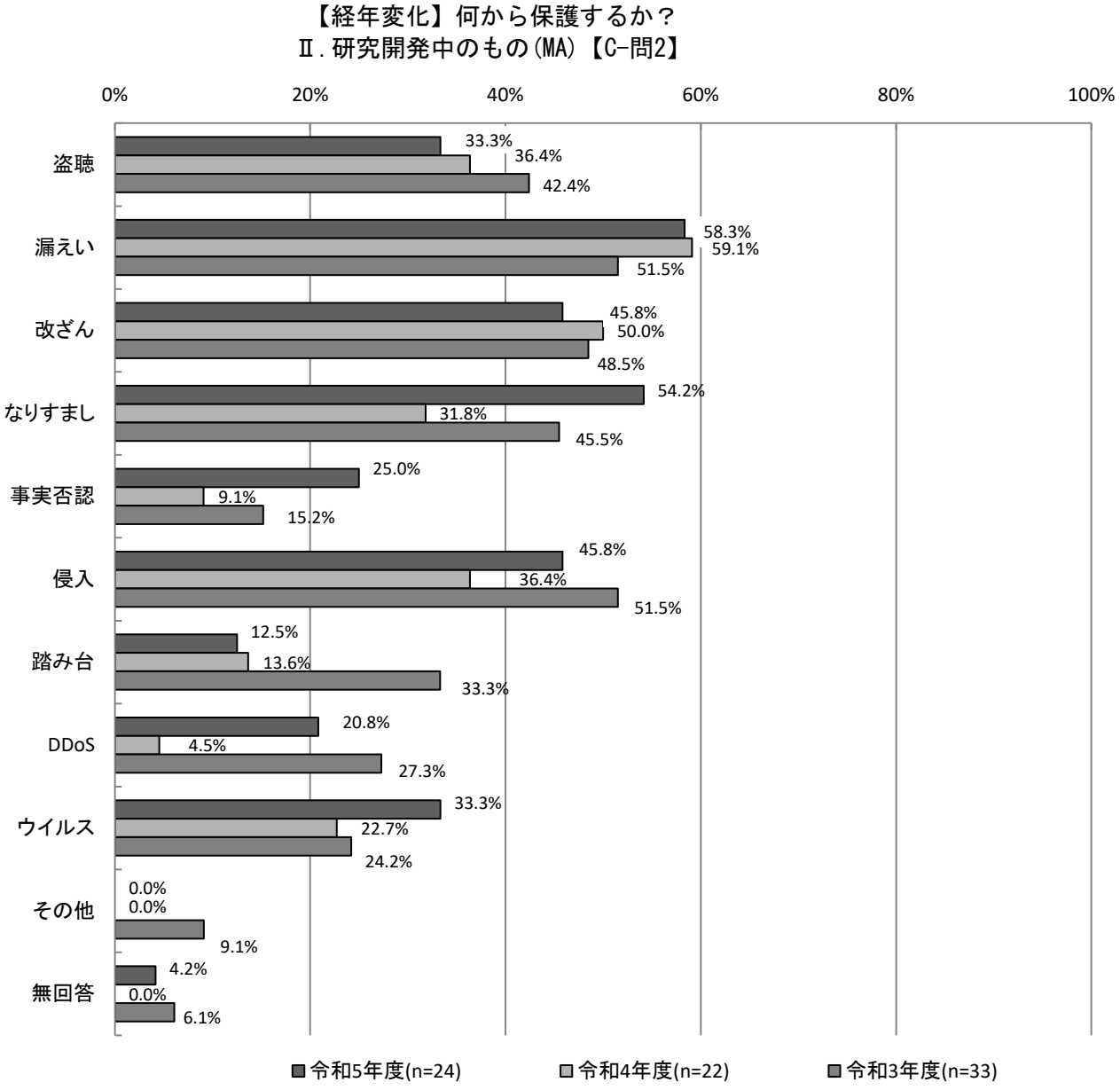
【経年変化】何から保護するか？
Ⅰ.実用化(製品化)されているもの(MA)【B-問2】



Ⅱ.研究開発中のもの

研究開発中のものについては、「漏えい」が58.3%（14件）で最も多く、次いで「なりすまし」が54.2%（13件）となっている。

昨年度と比較すると、「なりすまし」が22.4ポイント増加しており、次いで「DDoS」が16.3ポイント、「事実否認」が15.9ポイント増加している。



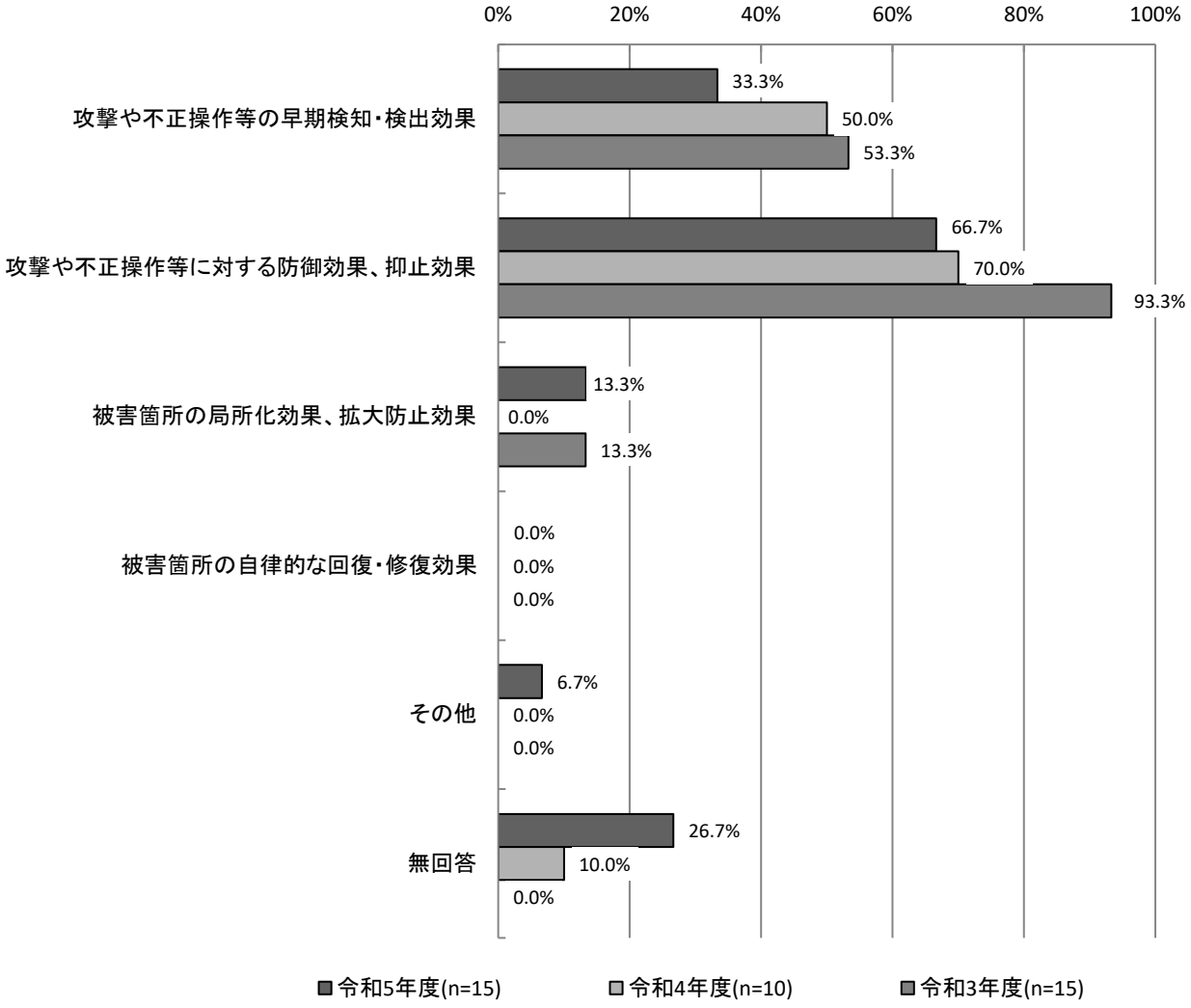
5.4.3　どのようなセキュリティ上の効果があるか？

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66.7%（10件）で最も多くなっている。

昨年度と比較すると、「攻撃や不正操作等の早期検知・検出効果」が16.7ポイント減少している。一方、「被害箇所の局所化効果、拡大防止効果」が13.3ポイント増加している。

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

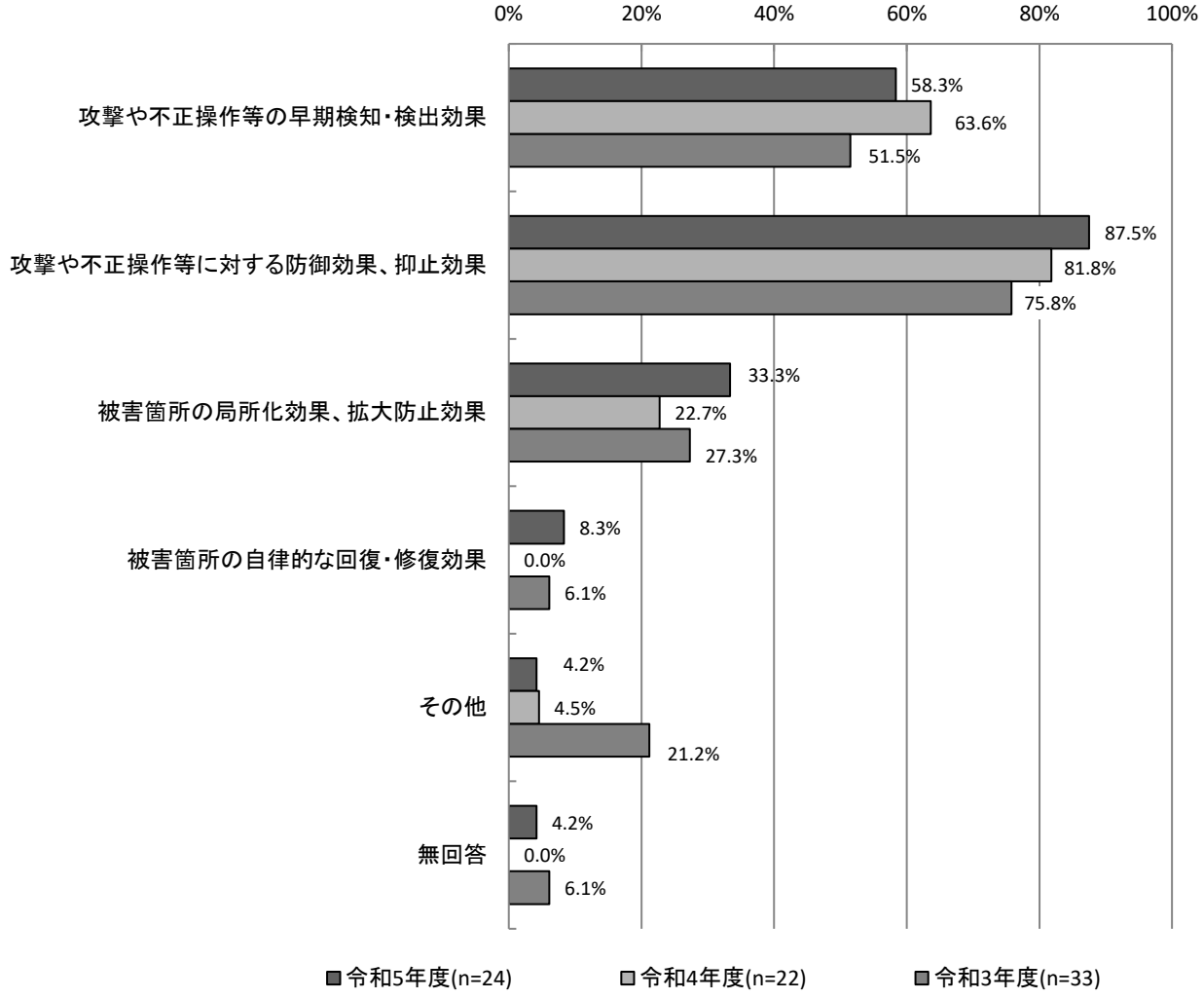


Ⅱ.研究開発中のもの

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87.5%（21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58.3%（14件）となっている。

昨年度と比較すると、「被害箇所の局所化効果、拡大防止効果」が10.6ポイント、「被害箇所の自律的な回復・修復効果」が8.3ポイント増加している。

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



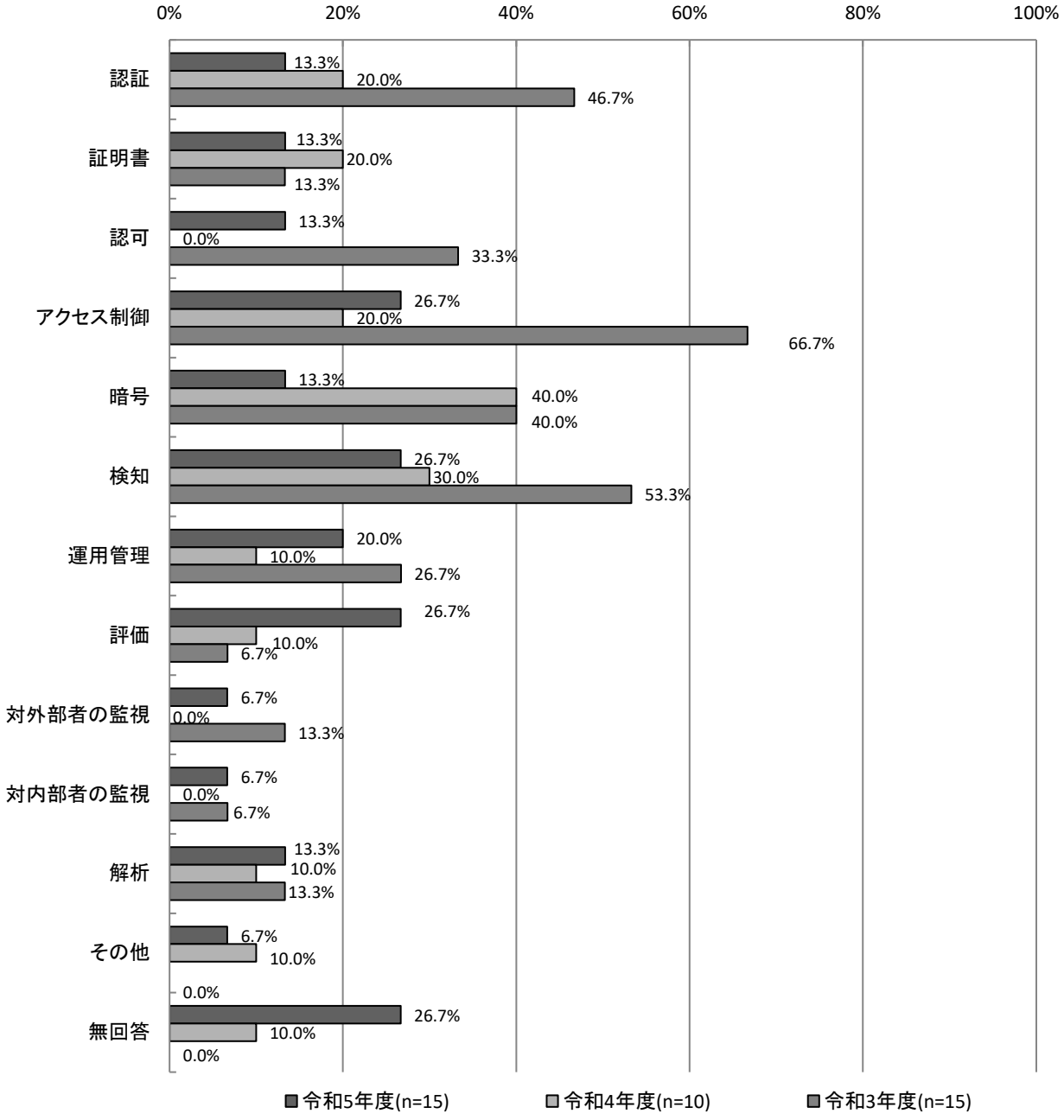
5.4.4　どのような機能を持つか？

Ⅰ.実用化(製品化)されているもの

実用化（製品化）されているものについては、「アクセス制御」「検知」「評価」がそれぞれ26.7%（4件）で最も多くなっている。

昨年度と比較すると、「暗号」が26.7ポイント減少している。一方、「評価」が16.7ポイント、「認可」が13.3ポイント増加している。

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

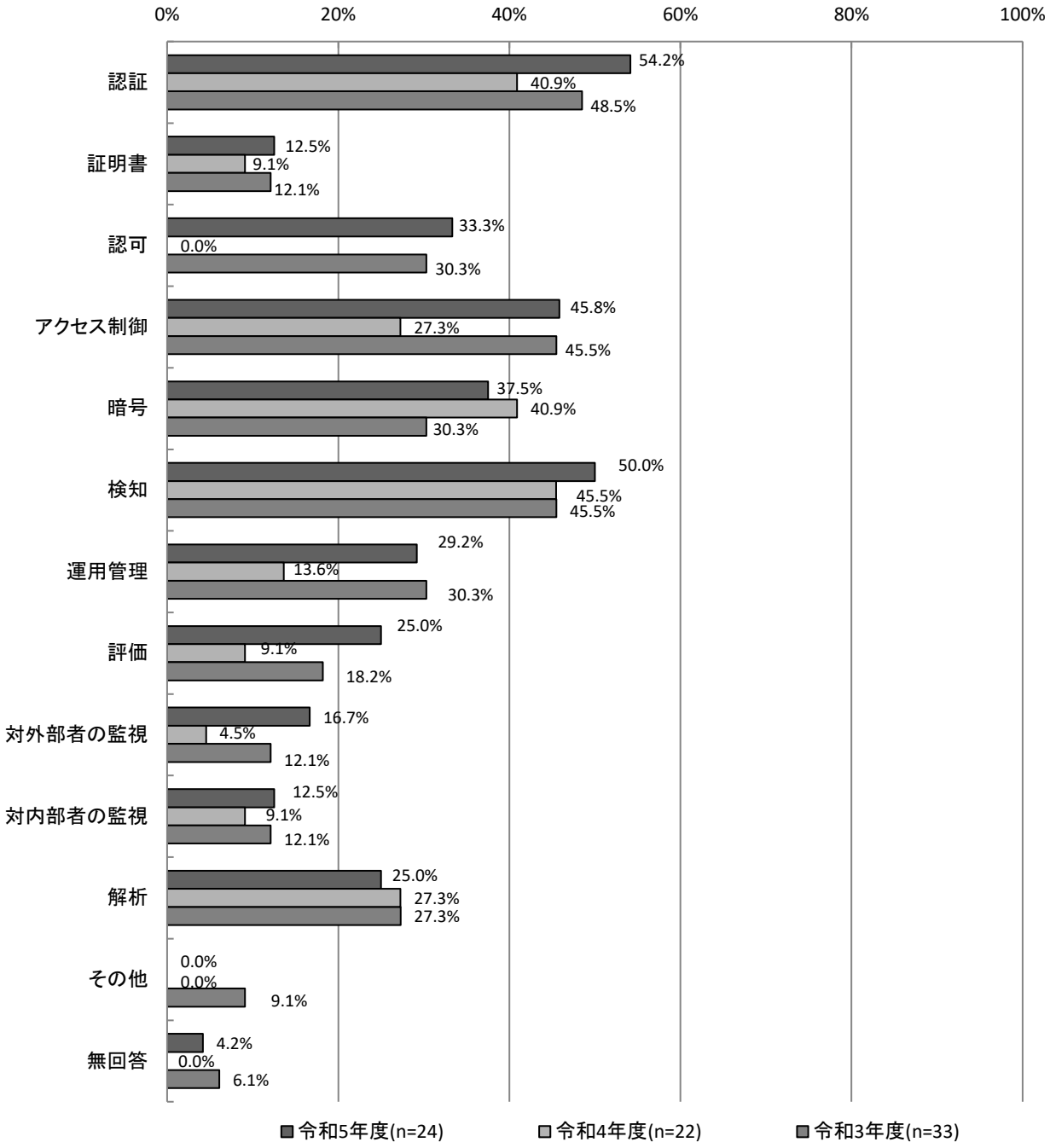


Ⅱ.研究開発中のもの

研究開発中のものについては、「認証」が54.2%（13件）で最も多く、次いで「検知」が50.0%（12件）となっている。

昨年度と比較すると、「認可」が33.3ポイント、「アクセス制御」が18.5ポイント増加している。

【経年変化】どのような機能を持つか？
Ⅱ.研究開発中のもの(MA)【C-問4】



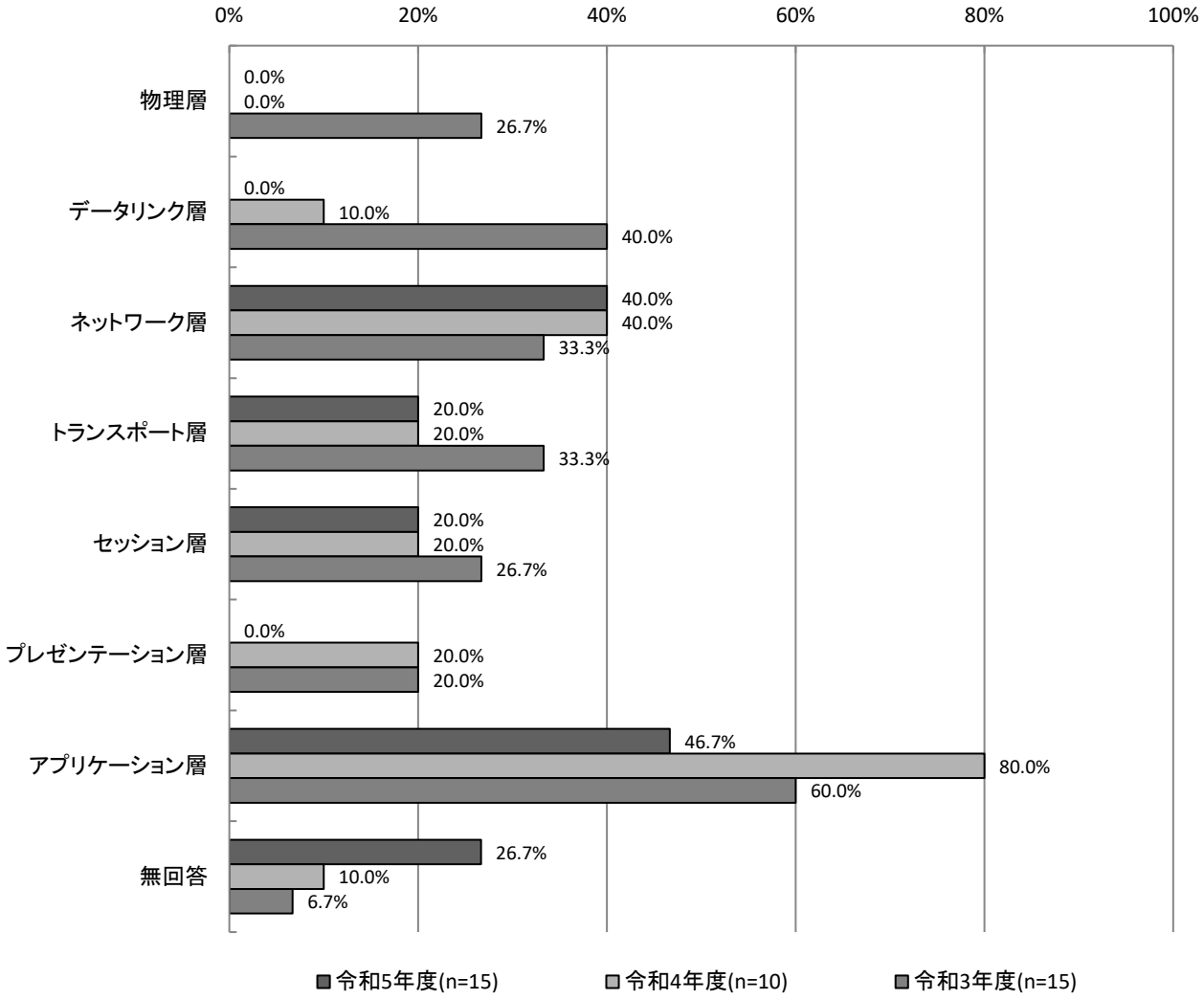
5.4.5　どのようなレイヤーのセキュリティを守るか？

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46.7%（7件）で最も多く、次いで「ネットワーク層」が40.0%（6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33.3ポイント減少しており、次いで「プレゼンテーション層」が20.0ポイント減少している。

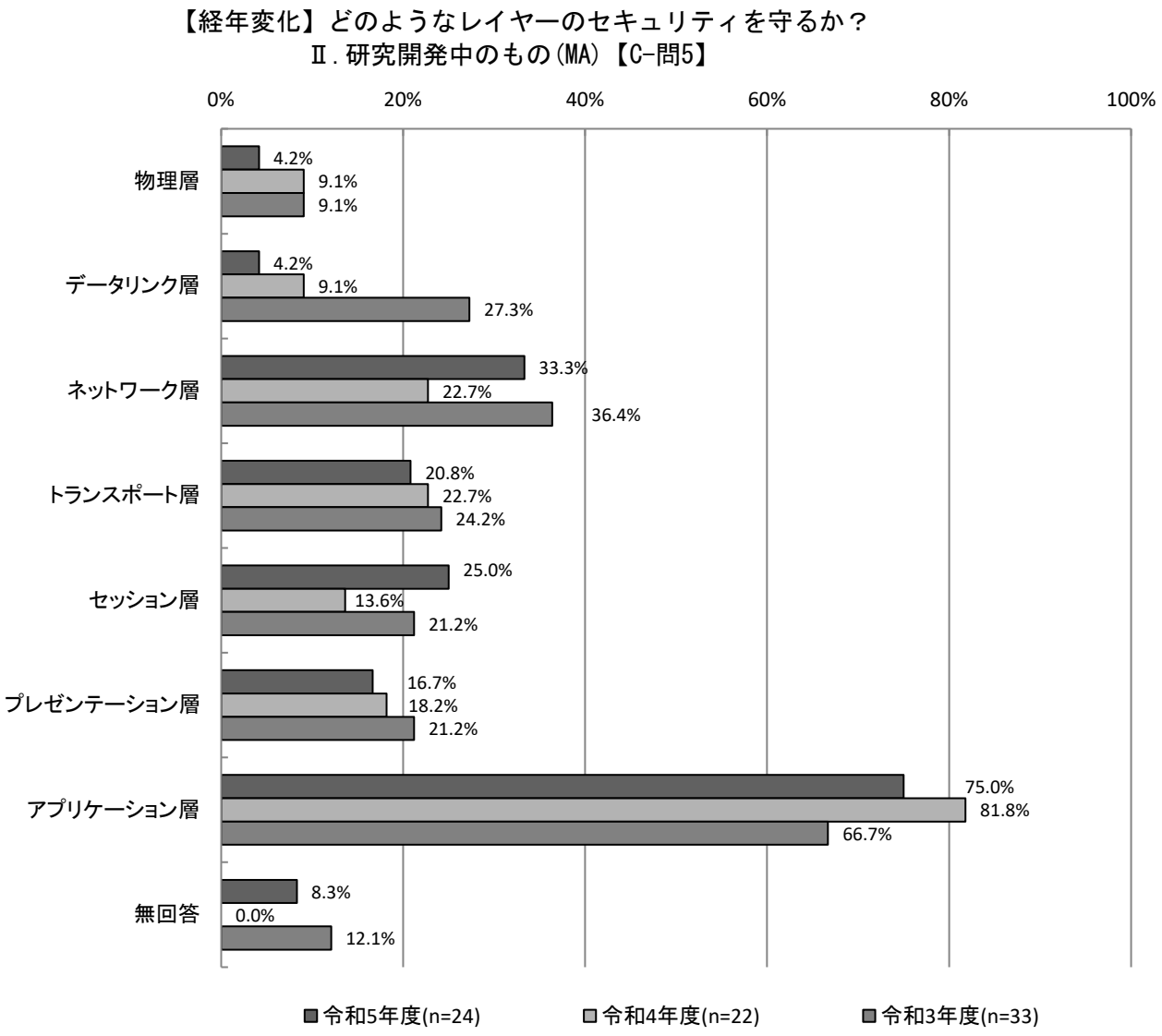
【経年変化】どのようなレイヤーのセキュリティを守るか？
Ⅰ.実用化(製品化)されているもの(MA)【B-問5】



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75.0%（18件）で最も多く、次いで「ネットワーク層」が33.3%（8件）となっている。

昨年度と比較すると、「セッション層」が11.4ポイント、「ネットワーク層」が10.6ポイント増加している。一方、「アプリケーション層」が6.8ポイント減少している。



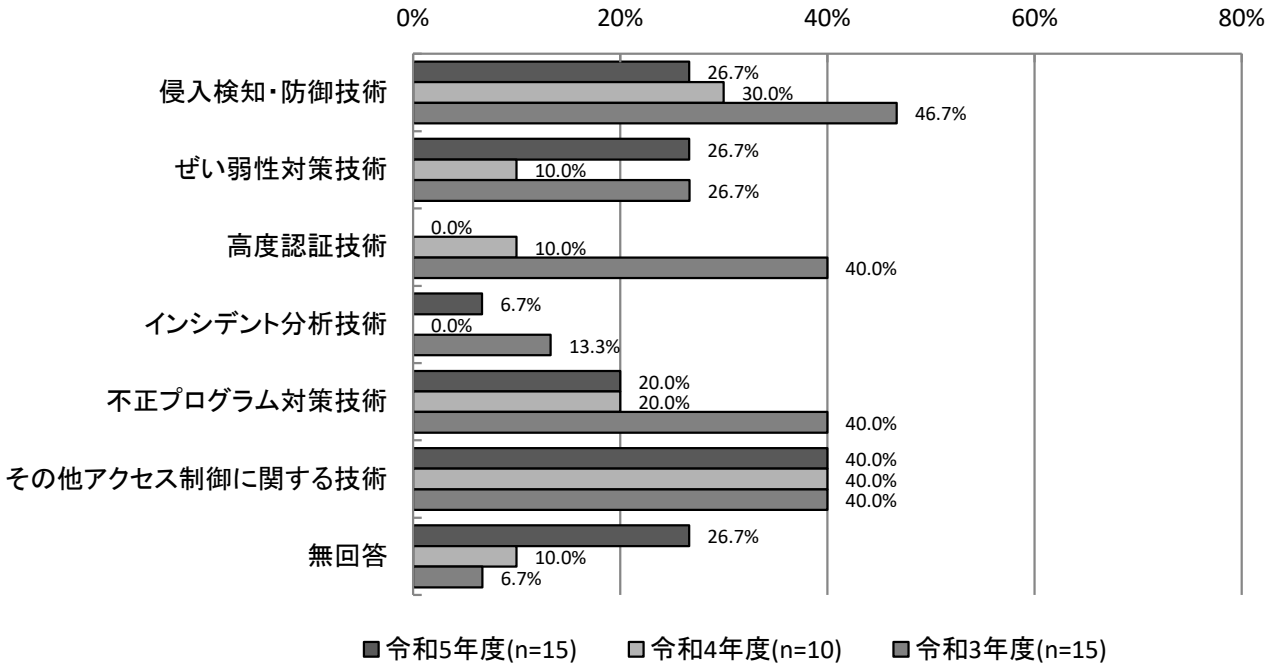
5.4.6　不正アクセスからの防御対象

Ⅰ.実用化(製品化)されているもの

実用化（製品化）されているものについては、「その他アクセス制御に関する技術」が40.0%（6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16.7ポイント増加している。一方、「高度認証技術」が10.0ポイント減少している。

【全体】不正アクセスからの防御対象
Ⅰ.実用化(製品化)されているもの(MA)【B-問6】

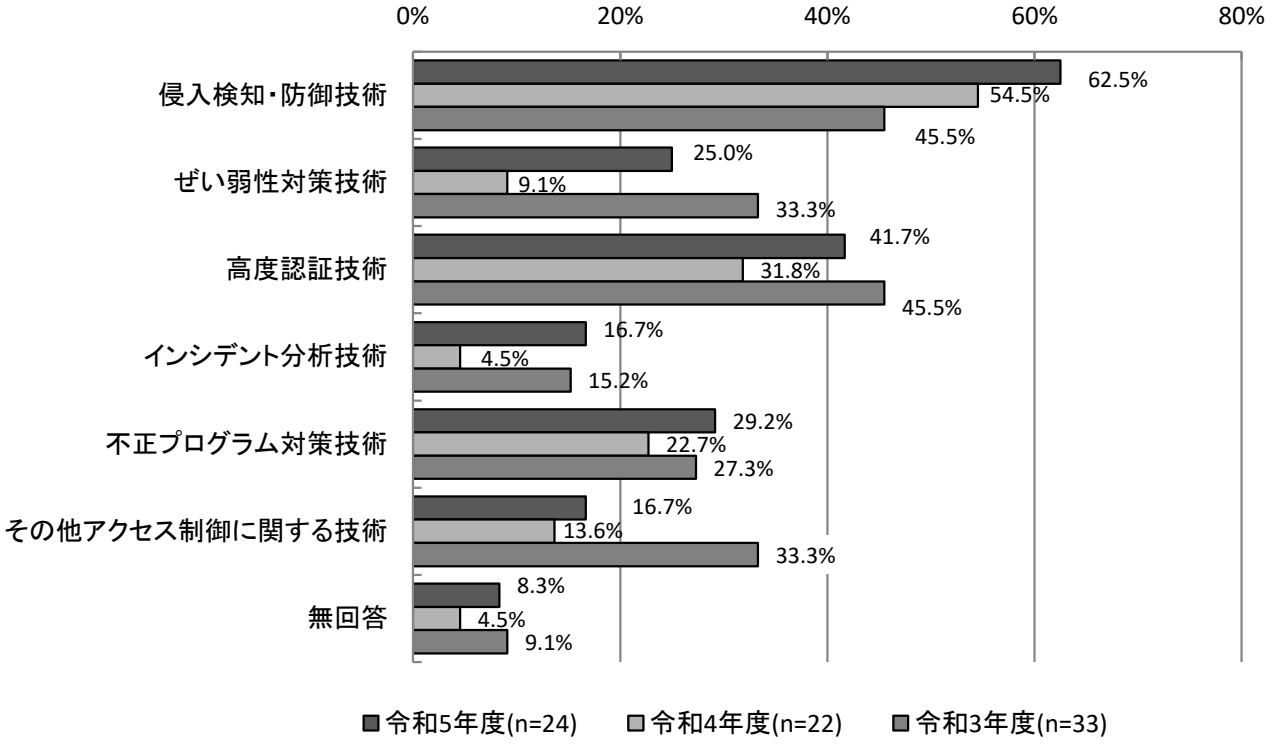


Ⅱ.研究開発中のもの

研究開発中のものについては、「侵入検知・防御技術」が62.5%（15件）で最も多くなっている。次いで、「高度認証技術」が41.7%（10件）となっている。

昨年度と比較すると、「ぜい弱性対策技術」が15.9ポイント、「インシデント分析技術」が12.2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】



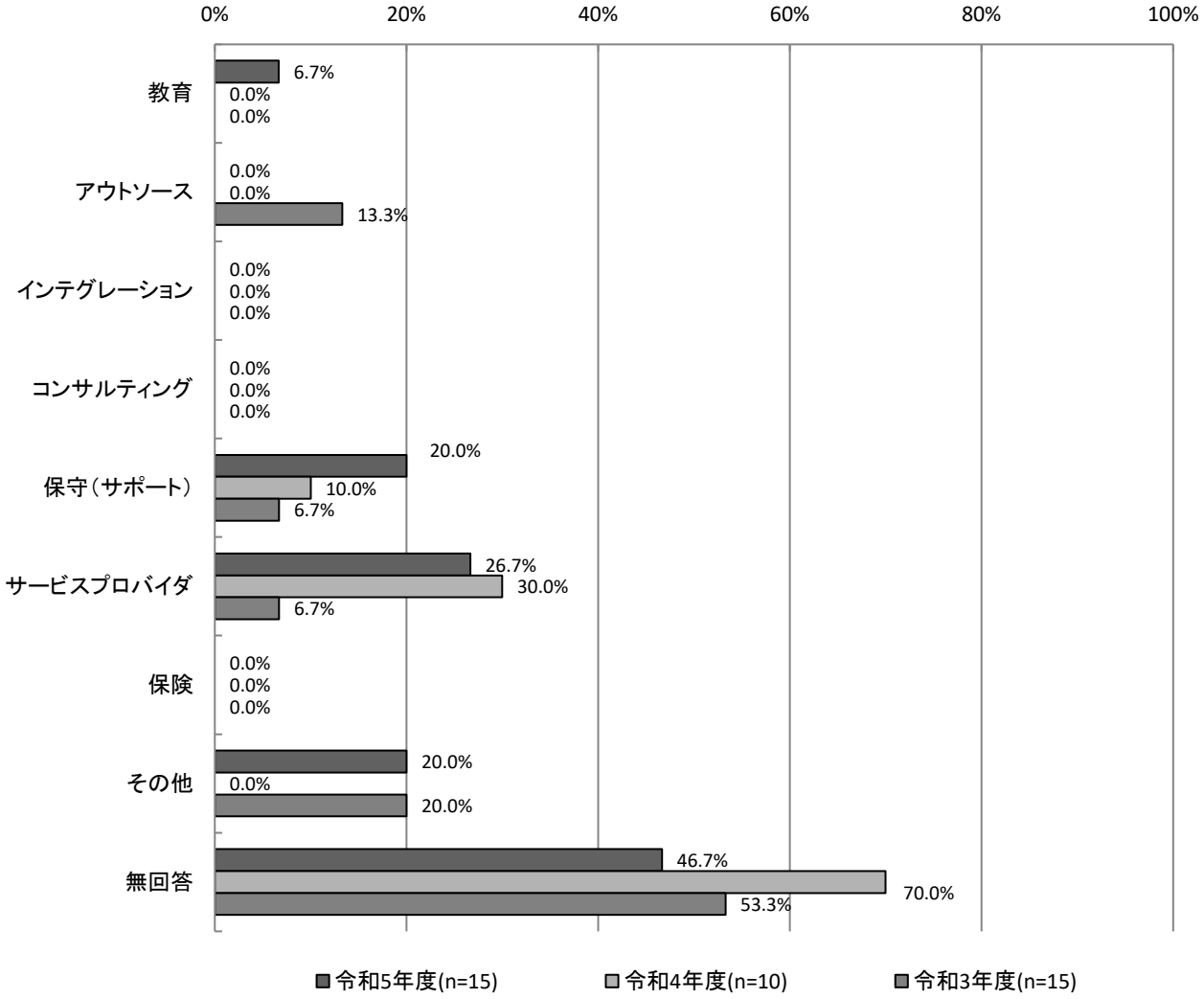
5.4.7　どのようなサービスか？

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、「サービスプロバイダ」が26.7%（4件）、「保守（サポート）」「その他」がそれぞれ20.0%（3件）となっている。

昨年度と比較すると、「保守（サポート）」が10.0ポイント増加している。次いで「教育」が6.7ポイント増加している。

【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】

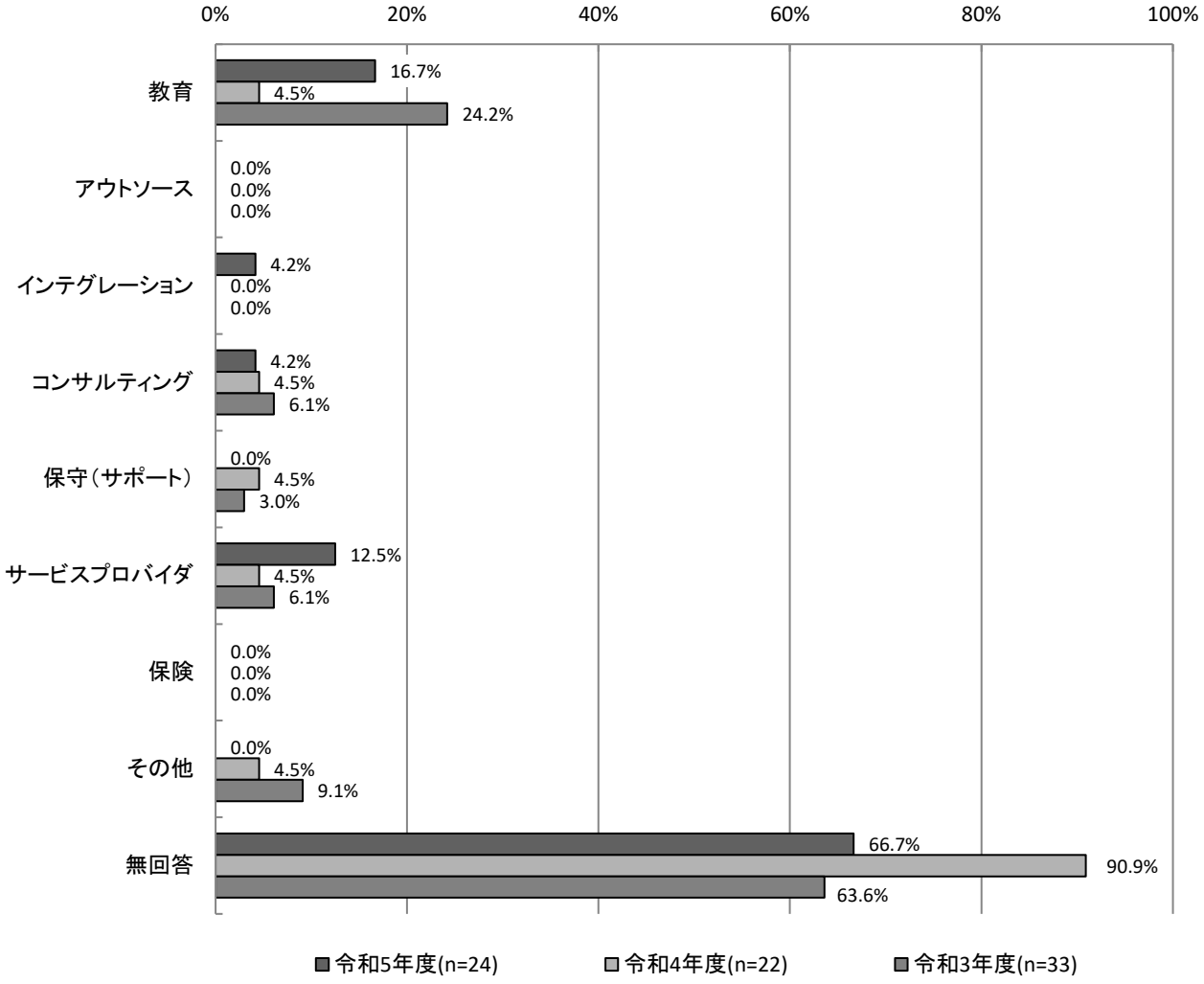


Ⅱ.研究開発中のもの

研究開発中のものについては、「教育」が16.7%（4件）となっている。

昨年度と比較すると、「教育」が12.2ポイント、「サービスプロバイダ」が8.0ポイント増加している。一方、「保守（サポート）」は4.5ポイント減少している。

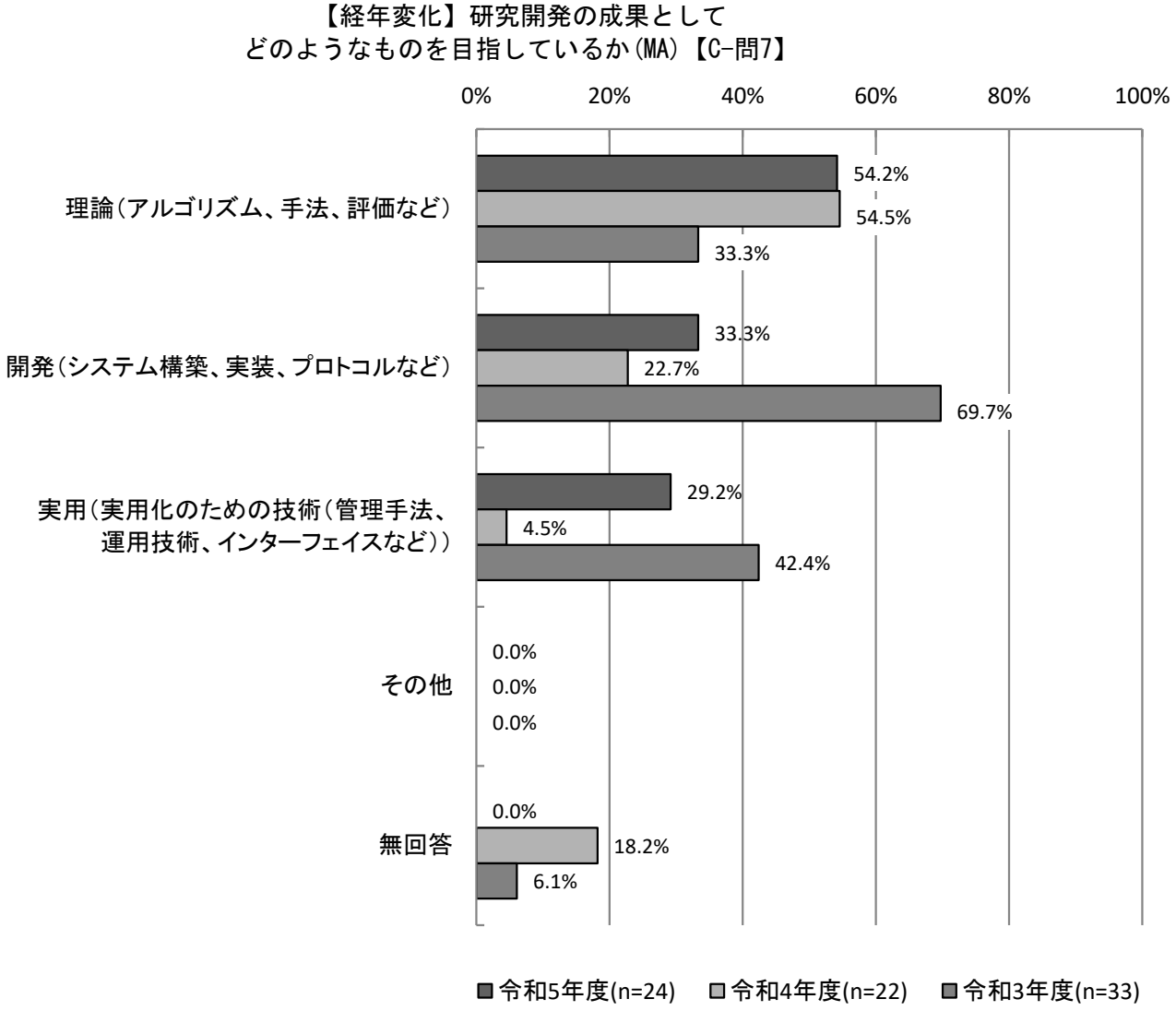
【経年変化】どのようなサービスか？
Ⅱ.研究開発中のもの(MA)【C-問8】



5.5 研究開発の成果としてどのようなものを目指しているか？

研究開発の目指す成果については、「理論(アルゴリズム、手法、評価など)」が54.2%（13件）で最も多く、次いで「開発(システム構築、実装、プロトコルなど)」が33.3%（8件)、「実用(実用化のための技術(管理手法、運用技術、インターフェイスなど))」が29.2%（7件）となっている。

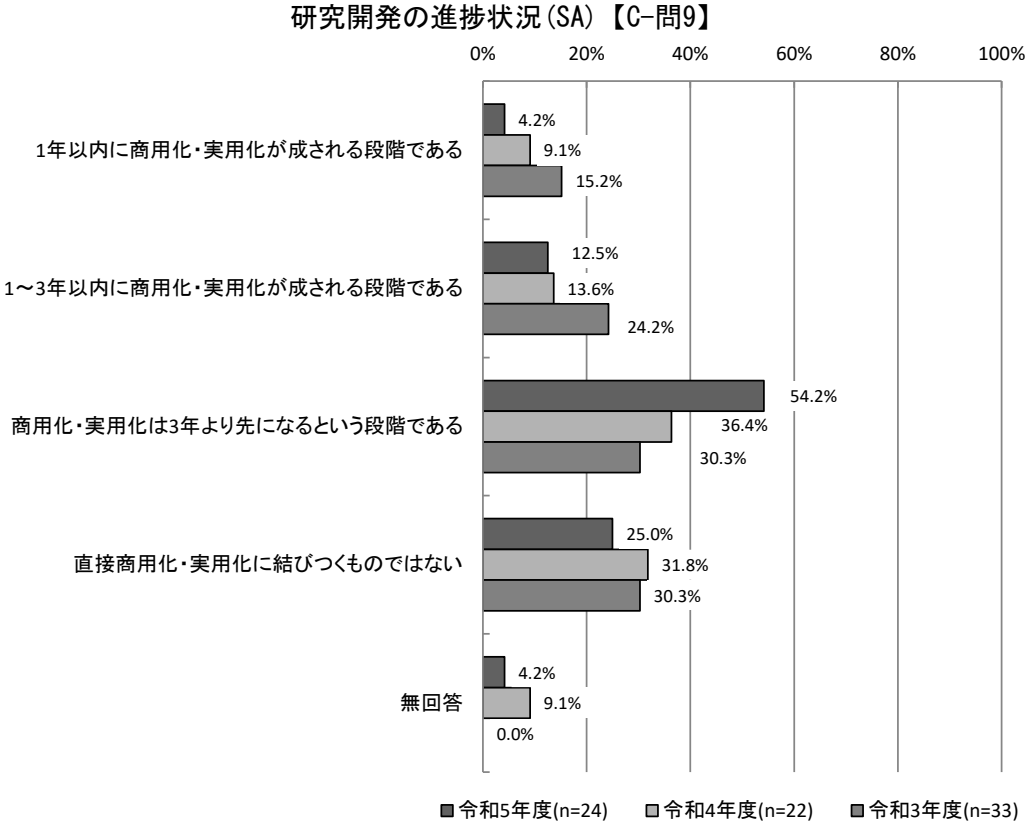
昨年度と比較すると、「実用（実用化のための技術（管理手法、運用技術、インターフェイスなど))」が24.7ポイント増加しており、次いで「開発（システム構築、実装、プロトコルなど)」が10.6ポイント増加している。



5.6 研究開発の進捗状況

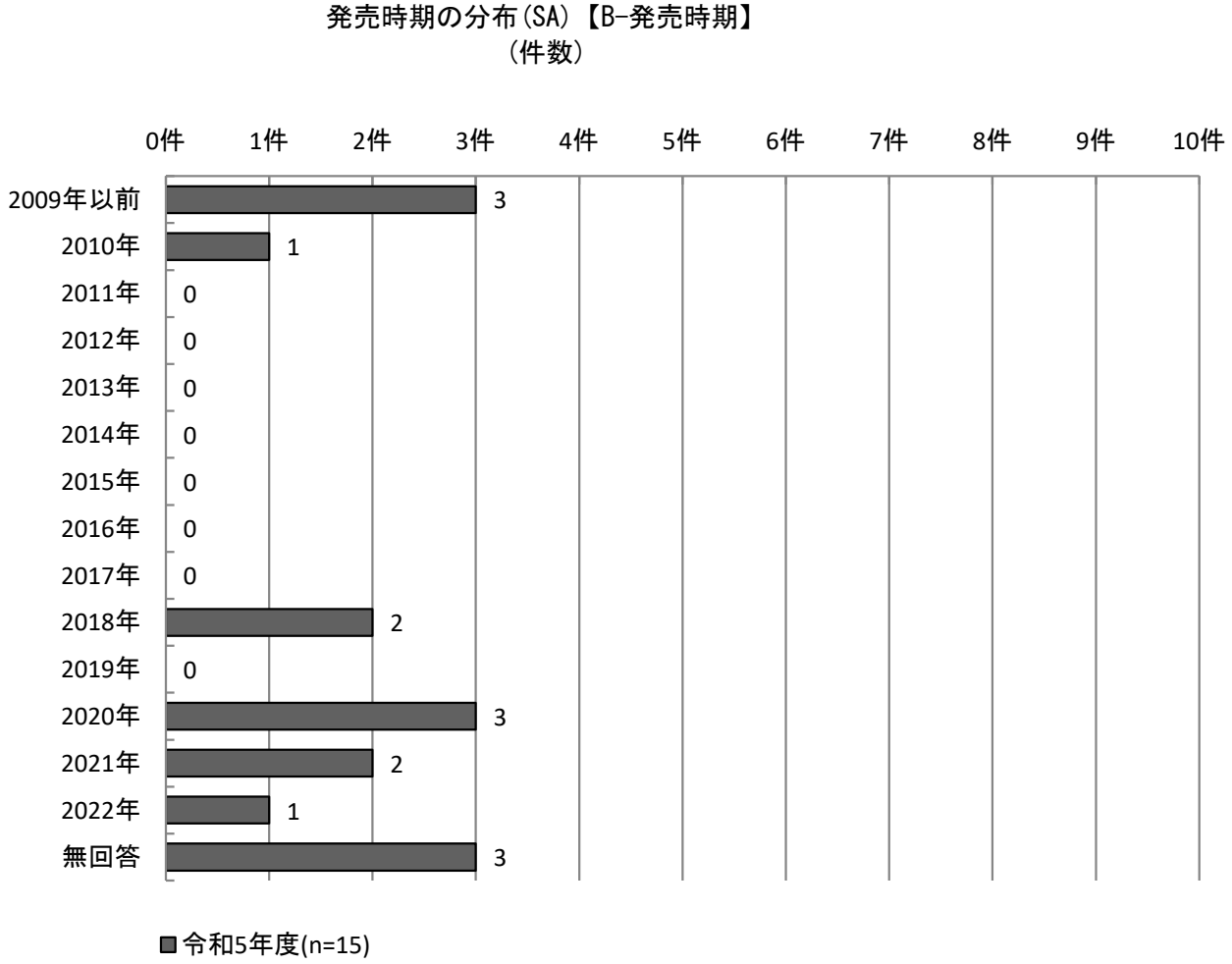
研究開発の進捗状況については、「商用化・実用化は3年より先になるという段階である」が54.2%（13件）と最も多い。次いで「直接商用化・実用化に結びつくものではない」が25.0%（6件）となっている。

昨年度と比較すると、「商用化・実用化は3年より先になるという段階である」が17.8ポイント増加している。一方、「直接商用化・実用化に結びつくものではない」が6.8ポイント、「1年以内に商用化・実用化が成される段階である」は4.9ポイント減少している。



5.7 発売時期の分布

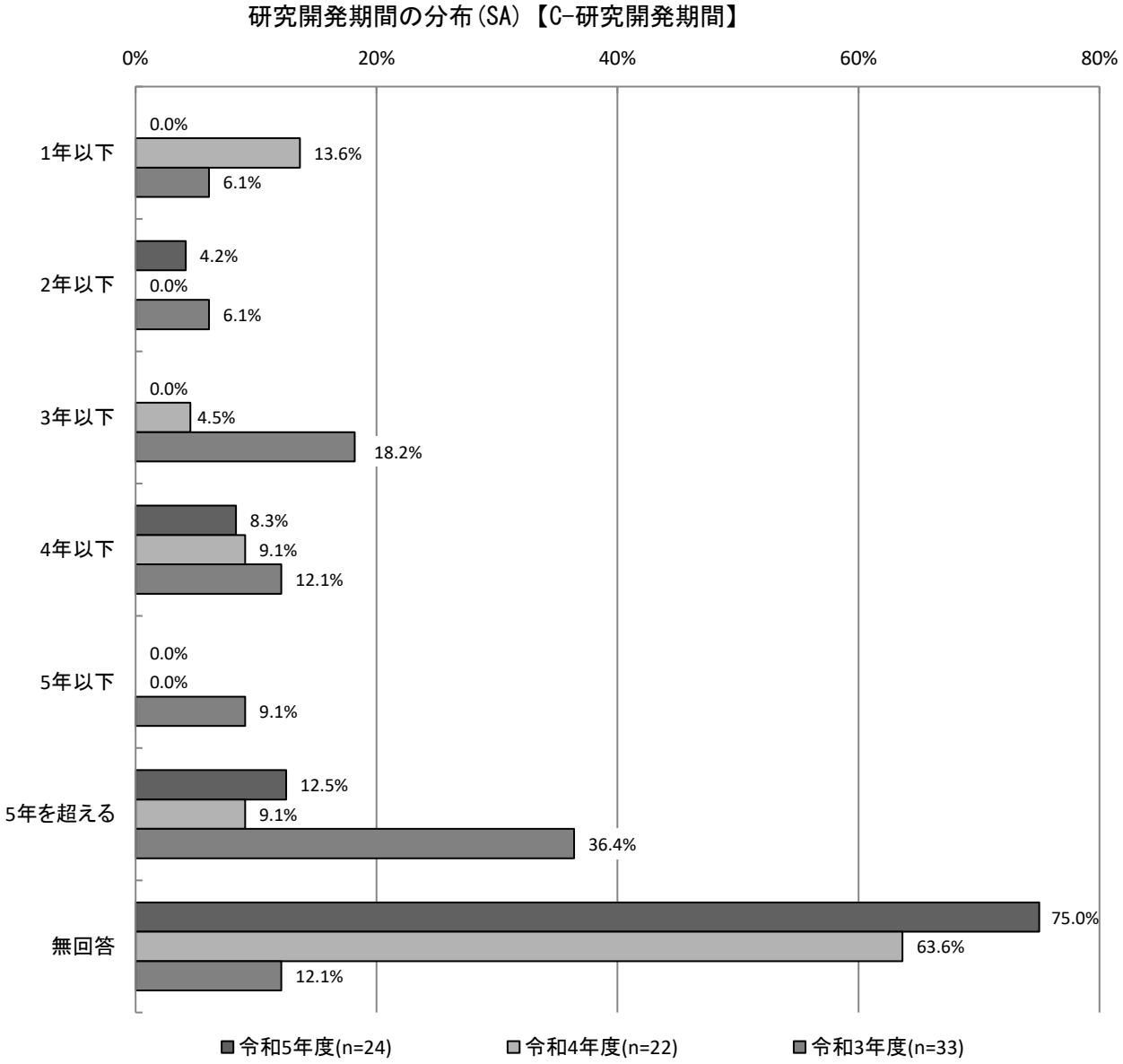
発売時期については、「2009年以前」「2020年」が3件となっている。



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12.5%（3件）で最も多く、次いで「4年以下」が8.3%（2件）となっている。

昨年度と比較すると、「1年以下」が13.6ポイント、「3年以下」が4.5ポイント減少している。一方「2年以下」が4.2ポイント増加している。



5.9 実用化された製品及び研究開発中の技術・サービス

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

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

■ 技術の実用化（製品化）状況

製品名	企業・大学名	開発元(メーカー名等)	侵入検知・防御技術	ぜい弱性対策技術	高度認証技術	インシデント分析技術	不正プログラム対策技術	その他アクセス制御に関する技術
Trend Vision One	トレンドマイクロ株式会社	トレンドマイクロ株式会社	○	○		○	○	
Fortigate 500E	公立大学法人公立諏訪東京理科大学	Fortinet	○					
Cavirin	株式会社ＳＲＡ	Cavirin Systems, Inc		○				
セキュリティ診断サービス	株式会社ＳＲＡ	SRA						
セキュリティ運用サービス	株式会社ＳＲＡ	SRA						
セキュリティ情報提供サービス	株式会社ＳＲＡ	SRA						
Camellia	三菱電機株式会社	NTTと三菱電機による共同開発						○
MistyGuard<CERTMANAGER>	三菱電機株式会社	三菱電機インフォメーションシステムズ						○
IoTハニーポット	三菱電機株式会社	三菱電機					○	
パスワード共有サービスPASSPATH	学校法人福岡大学	福岡大学情報基盤センター中國研究室						○
Nulab Pass	株式会社ヌーラボ	株式会社ヌーラボ						
Opengate	国立大学法人佐賀大学	佐賀大学						○

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

■　技術の研究開発状況

研究開発名称	企業・大学名	関連部門名	侵入検知・防御技術	ぜい弱性対策技術	高度認証技術	インシデント分析技術	不正プログラム対策技術	その他アクセス制御に関する技術
セキュリティインテリジェンス提供サービス	国立大学法人 横浜国立大学	先端科学高等研究院　情報・物理セキュリティ研究ユニット						
FIDO/WAF連携システム構築	株式会社ＳＲＡ	プロダクトサービス事業部			○			
認証暗号アルゴリズム	三菱電機株式会社	情報技術総合研究所	○					
耐量子計算機暗号	三菱電機株式会社	情報技術総合研究所	○					
秘匿検索(検索可能暗号)	三菱電機株式会社	情報技術総合研究所	○					
センサーセキュリティ	三菱電機株式会社	情報技術総合研究所	○					○
イントラネットにおけるデバイスの柔軟なアクセス制御に関する研究	学校法人　東北工業大学	工学部情報通信工学科 角田研究室	○					
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			○			
(特にプロジェクト名は無い)	国立大学法人東海国立大学機構名古屋大学	情報学研究科 情報システム学専攻 嶋田研究室	○			○	○	○
生体から得られる電磁気情報を用いた個人認証システム	日本大学	理工学部応用情報工学科	○	○	○		○	
ブロックチェーン技術を用いた単一医療機関向け診療記録システム	日本大学	理工学部応用情報工学科	○	○	○		○	
標的型メール対策訓練支援システム	日本大学	理工学部応用情報工学科	○	○	○	○	○	
デジタルフォレンジック技術の学習支援システム	日本大学	理工学部応用情報科学科	○	○	○	○	○	
セキュリティー研究センター	神奈川工科大学	神奈川工科大学　研究推進機構	○	○	○		○	
身体的特徴量、行動的特徴量、知識を組み合わせた認証方式の開発	国立大学法人佐賀大学	理工学部電気電子工学部門			○			

※　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	トレンドマイクロ株式会社
代表者名	
所在地	
窓口部署名	
電話番号	
ホームページのURL	
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： Trend Vision One 開発元(メーカー名等)： トレンドマイクロ株式会社 開発国： アメリカ合衆国 *CBP(米国国土安全保障省 税関・国境取締局）の規定 に基づき、「ソフトウェアがオブジェクトコードに変換される場所」を製造国（Country of Origin）と定義しています 価格： 弊社営業までお問合せください 発売時期： 2021年3月 出荷数： 非公開	トレンドマイクロが提供するXDR（Extended Detection and Response）は、エンドポイントに加え、メール、サーバ、クラウドワークロード、ネットワーク等の複数のセキュリティレイヤから正・不正問わずファイルやプロセスに対するアクティビティデータであるテレメトリを収集し、サイバー攻撃の有無や対処すべき事項を見出します。 Trend Vision Oneでは、法人組織が平時からリスクの把握、評価、軽減を行う「アタックサーフェスリスクマネジメント」とマルウェア等の脅威や、脅威とは断定できない不審な挙動の抽出を行い、影響範囲や感染経路の特定、攻撃の全体像の可視化など、迅速な対処を行うことを支援する「XDR」を提供します。 詳細は以下をご覧ください https://www.trendmicro.com/ja_jp/business/products/one-platform.html

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

企業・大学名	公立大学法人公立諏訪東京理科大学
代表者名	北原　政彦
所在地	391-0292 長野県茅野市豊平5000-1
窓口部署名	事務局総務課
電話番号	0266-73-1201
ホームページのURL	https://www.sus.ac.jp/
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： Fortigate 500E 開発元(メーカー名等)： Fortinet 開発国： アメリカ 価格： 830万円（本体のみの価格） 発売時期： 2018年3月1日 出荷数： 不明	FortiGate 500E シリーズは、中規模から大規模の企業向けに次世代ファイアウォール（NGFW）機能を提供します。キャンパスや大規模企業の支社への展開に最適な柔軟性も備えています。独自の強力なセキュリティプロセッサによって、ネットワークパフォーマンスの最適化、セキュリティの有効性、詳細な可視性が実現しており、巧妙なサイバー脅威からお客様を保護します。フォーティネットのセキュリティ ドリブン ネットワーキングのアプローチにより、新世代のセキュリティがネットワークへと緊密に統合されます。

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	株式会社ＳＲＡ
代表者名	平田淳史
所在地	171-0022 東京都豊島区南池袋2丁目32番8号
窓口部署名	プロダクトサービス事業部
電話番号	03-5979-2111
ホームページのURL	https://www2.sra.co.jp/
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： Cavirin 開発元(メーカー名等)： Cavirin Systems, Inc 開発国： United States 価格： 月額150,000円～ 発売時期： 2018年1月 出荷数： 非公開	・ Cavirin は CSPM 領域の製品で、クラウドにおける不適切な設定、人為的な設定ミスによるリスクを監視・修復する製品 ・ CSPM 製品ですが、オンプレミスの OS・コンテナの脆弱性対策・コンプライアンス準拠を監視可能 ・ NIST, CIS, PCI DSS、HIPPA 等、複数の基準で監視可能

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ＳＲＡ
代表者名	平田淳史
所在地	171-0022 東京都豊島区南池袋2丁目32番8号
窓口部署名	プロダクトサービス事業部
電話番号	03-5979-2111
ホームページのURL	https://www2.sra.co.jp/
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： セキュリティ診断サービス 開発元(メーカー名等)： SRA 開発国： 日本 価格： 50万円～(ライト/128IP) 発売時期： 2020年～ 出荷数：	・Nessusを用いた外部(インターネット)からの脆弱性診断サービス ・複数拠点の診断も可能 ・128 IP まで同一価格(以降64IP単位) ・対象IP数と診断回数のシンプルな価格体系 ・2種類(スタンダード、ライト)の診断タイプ(日本語による診断報告書の有無) ・無償での再診断可

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ＳＲＡ
代表者名	平田淳史
所在地	171-0022 東京都豊島区南池袋2丁目32番8号
窓口部署名	プロダクトサービス事業部
電話番号	03-5979-2111
ホームページのURL	https://www2.sra.co.jp/
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： セキュリティ運用サービス 開発元(メーカー名等)： SRA 開発国： 日本 価格： 20万円～（初期費用別途） 発売時期： 2022年～ 出荷数：	・セキュリティの専門知識をもった人材による運用サービス ・24x365の運用体制 ・マルチベンダーサポート(メーカー限定無し) ・アラートなどの検知の報告のみではなく、セキュリティ向上のための設定変更などのご提案も可能 ・オプションにてパッチ適用作業やWebアプリケーション脆弱性診断なども実施可

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ＳＲＡ
代表者名	平田淳史
所在地	171-0022 東京都豊島区南池袋2丁目32番8号
窓口部署名	プロダクトサービス事業部
電話番号	03-5979-2111
ホームページのURL	https://www2.sra.co.jp/
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： セキュリティ情報提供サービス 開発元(メーカー名等)： SRA 開発国： 日本 価格： 40万円～(初期＋年額) 発売時期： 2020年～ 出荷数：	・お客様環境にあったプロダクトを選択し、ピンポイントに脆弱性情報を収集 ・CVSS評価値や危険度レベル、影響範囲などのフィルタを用いて必要な情報のみ厳選して取得することが可能

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

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

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

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

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

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

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

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

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

企業・大学名	株式会社ヌーラボ
代表者名	橋本正徳
所在地	810-0041 福岡県福岡市中央区大名1丁目8-6 HCC BLD.
窓口部署名	情報統括部品質保証課
電話番号	092-752-5231
ホームページのURL	https://nulab.com
製品説明のURL	
対象技術	技術の概要・特徴など
製品名： Nulab Pass 開発元(メーカー名等)： 株式会社ヌーラボ 開発国： 日本 価格： ¥990～ 発売時期： 2020年8月4日 出荷数：	Nulab Pass（ヌーラボパス）は、株式会社ヌーラボが提供するサービス（Backlog、Cacoo、Typetalk）を利用する際のセキュリティとガバナンスを強化するサービスです。 組織の管理者による統合的なアカウント管理、SAML認証によるシングルサインオン、組織のメンバーの操作を記録する監査ログを提供します。

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

企業・大学名	国立大学法人佐賀大学
代表者名	兒玉浩明
所在地	840-8502 佐賀市本庄町１番地
窓口部署名	佐賀大学総合情報基盤センター
電話番号	0952-28-8149
ホームページのURL	https://www.saga-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： Opengate 開発元(メーカー名等)： 佐賀大学 開発国： 日本 価格： 無償 発売時期： 2005年 出荷数： 不明（ウェブサイトで公開）	背景： インターネットが社会に浸透してきた現在、携帯型コンピュータを接続できる情報コンセントや多人数共用の公開端末など、ネットワーク利用環境を広 く整備することが要望されている。一方、インターネット上では、侵入破壊行為や誹謗中傷行為等のトラブルが頻発しており、公開端末や情報コンセン ト等を無制限で開放することは許されなくなっている。しかし、公開端末ではシステムの認証機構不足や管理負担のため、また情報コンセントでは利用者本人が所有する機器を対象とするため、適切な認証を一律に適用することは困難である。 目的： 公開端末や情報コンセント・無線LAN等においても、利用資格を持つ者のみがネットワークを利用できるように制限するとともに、トラブル時の個人 特定を可能とするシステムの構築を目的とする。 利用： ブラウザを立ち上げて任意のサイトをアクセスする。すると認証要求ページが送られてくるので、ユーザIDとパスワードを返答する。許可ページ が表示されればネットワークが利用できる。ブラウザを終了するとネットワークが閉鎖される。 機能と構成： 本システムは、端末群と利用ネットワークとの間にゲートウエイを設置し、そこを通過するパケットをフィルタリングするシステムとして実現する。 端末にはWebブラウザが必要である。OS等は特に制限しない。また事前設定も不要である。ゲートウェイには、Webサーバとファイアウオー ルソフトが必要である。現状のプログラムは、FreeBSD上のApacheとipfwを利用している。また利用者認証のためには、FTP, POP3, POP3S, FTPS, RADIUS, LDAP, PAM, Shibboleth, HttpBasicをサポートしている。Opengateは CGIとして起動し、端末にAjaxスクリプトを送り、ブラウザの生存を監視する。

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

5.9.2 「技術の研究開発状況」について

※一覧表の下には対象となる防御対象について〇を付与している

企業・大学名	国立大学法人 横浜国立大学
代表者名	学長　梅原　出
所在地	240-8501 横浜市保土ヶ谷区常盤台79-1
窓口部署名	研究・学術情報部　情報企画課　情報企画係
電話番号	045-339-4472
関連部門名	先端科学高等研究院　情報・物理セキュリティ研究ユニット
ホームページのURL	https://www.ynu.ac.jp/
研究説明のURL	https://sec.ynu.codes/iot/ https://sec.ynu.codes/dos http://yoshioka.ynu.ac.jp/research.html https://ipsr.ynu.ac.jp/outcome.html
対象技術	技術の概要・特徴など
研究開発名称： セキュリティインテリジェンス提供サービス 研究開発国： 日本 研究開発時期： 2015年1月1日～2025年12月31日	サイバー攻撃やその原因となっている脅威アクターの動向をインターネット上のクロールやハニーポットにより観測し、情報を蓄積しており、そのデータを外部に提供する形でのサービスを提供する可能性がある。ハニーポットによる観測は８年間の研究開発を行っており、脅威アクタ分析については昨年度から開発を実施している。

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

企業・大学名	株式会社ＳＲＡ
代表者名	平田淳史
所在地	171-0022 東京都豊島区南池袋2丁目32番8号
窓口部署名	プロダクトサービス事業部
電話番号	03-5979-2111
関連部門名	プロダクトサービス事業部
ホームページのURL	https://www2.sra.co.jp/
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： FIDO/WAF連携システム構築 研究開発国： 日本 研究開発時期： 2022年10月1日～2023年12月31日	昨年度POCと市場調査を実施し、有効と判断しため、製品化開発中。

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

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

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

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

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

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

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

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

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

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： イントラネットにおけるデバイスの柔軟なアクセス制御に関する研究 研究開発国： 日本 研究開発時期： 2022年4月～	要素技術としてeBPF(extended Berkley Packet Filter)に着目しており，eBPFを利用したアイディアの実現性の検証を進めている状況にある.

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

企業・大学名	学校法人福岡大学
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～2024年3月31日	現段階では少数の被験者の協力による認証精度を確認している。 極めて高い認証精度を確認しており、近々、多くの被験者を用いて認証精度を検証する計画である。 現在は、国内のセキュリティ製品を開発するメーカーと共同研究開発を推進することについて協議しており、同メーカーから日本国内に向けて販売することを目指している。

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

企業・大学名	国立大学法人東海国立大学機構名古屋大学
代表者名	
所在地	
窓口部署名	
電話番号	
関連部門名	情報学研究科 情報システム学専攻 嶋田研究室
ホームページのURL	
研究説明のURL	https://www.net.itc.nagoya-u.ac.jp/member/shimada/researches/network_security.html https://www.net.itc.nagoya-u.ac.jp/member/shimada/researches/cyber_security.html https://www.net.itc.nagoya-u.ac.jp/member/shimada/researches/network.html
対象技術	技術の概要・特徴など
研究開発名称： （特にプロジェクト名は無い） 研究開発国： 日本 研究開発時期：	以下のような研究を過去数年の間に実施している。 - 悪性通信の解析/検知 　- HTTP(S)通信を使うC&C通信の検出 　- FPGAを利用した悪性通信からの特徴量抽出 - マルウェアの検知/分類 　- マルウェアバイナリのCFG特徴のGINによる圧縮を利用した分類 　- カスタム損失関数を導入したGBDTによるマルウェア検知精度向上 　- 潜在表現の時系列差分を用いた亜種マルウェア検知精度向上 　- APIコールログからのマルウェアプロセス推定 - セキュアなネットワーク運用 　- 攻撃の進捗と業務継続性を両立するネットワーク遮断 　- OS間のIPv6実装状態の差を悪用する攻撃と検証 　- バックボーン遅延ヒストグラムからの無線LAN Rogue AP(偽AP)検知 　- SRv6による組織内ネットワークにおける攻撃由来通信の隔離ネットワーク誘導 - 自動リンク処理などにおける国際化ドメイン名などのセキュリティ問題 - セキュリティナレッジの構築 　- SNSや議論系Webサイトから脆弱性情報の収集とランク分け 　- SNSの脆弱性話題からのWeb Application Firewallルール生成 - ハニーポットとIDS 　- IoT向け通信プロトコルのためのハニーポットとその観測結果 　- ハニーポット通信ログ解析からのIDSシグネチャ自動選択 - 標的型攻撃対策 　- 攻撃者の意図の解析を目的としたOpenFlowによる組織内感染端末通信の解析用仮想環境への誘導 　- ログ統合によるサイバー攻撃推定手法 　- ユーザの信用度を考慮したテレワーク通信へのアクセス制御手法 　- 通信遮断による標的型攻撃対応のための影響範囲VR可視化システム - 機械学習/深層学習応用システムへの攻撃 　- MalGANと強化学習による本命の検知率を低下させる学習用おとりマルウェアデータ生成 　- 研究用IDS作成学習データセットに対する偽学習データ付与 　- 勾配情報変化量を利用したSVMベースのマルウェア検知を標的にする中毒攻撃データの検知

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： 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	理工学部応用情報科学科
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	神奈川工科大学
代表者名	小宮山　一三
所在地	243-0292 神奈川県厚木市下荻野1030
窓口部署名	研究推進機構 広報部門
電話番号	046-291-3109
関連部門名	神奈川工科大学　研究推進機構
ホームページのURL	https://www.kait.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： セキュリティー研究センター 研究開発国： 日本 研究開発時期： 2021年3月～2024年8月	「分散型機械学習モデルに基づいた安全なIoTサービスを実現するための統合セキュリティー対策技術に関する研究」 本研究の目的は、誰もが安心して暮らせる超スマートな社会を実現するために、フィジカル空間とサイバー空間を融合したすべての部分で安全性と信頼性を確保することができる高度かつ検漏なIoTセキュリティー総合対策を確率する事である。　具体的には、超スマート社会実現におけるサイバー攻撃の脅威を明確に分析し、フィジカル空間からサイバー空間まで一貫して安全性を提供可能となる高度なIoTセキュリティーシステム構築技術の確立について検討する。　そして、不正デバイスと不正アップリケ―ションを見分けることができるデバイス認証技術とユーザー認証技術を開発するとともに、不正データ・異常データをより早く検知することができる信頼性の高い分散機械学習モデル構築手法の研究開発を行う。 今年度は、これまで検討・提案してきたスマートフォンとスマートウオッチのようなウエアラブル端末を用いた個人認証方式の有効性を検討する。　さらに、スマートフォンの行動的特徴量による個人識別に関する検討と文章作成中の打鍵情報による継続的な本人認証について検討を行っている。

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	国立大学法人佐賀大学
代表者名	兒玉浩明
所在地	840-8502 佐賀市本庄町１番地
窓口部署名	佐賀大学総合情報基盤センター
電話番号	0952-28-8149
関連部門名	理工学部電気電子工学部門
ホームページのURL	https://www.saga-u.ac.jp/
研究説明のURL	http://www.bioengineering.saga-u.ac.jp/research/douzono.html
対象技術	技術の概要・特徴など
研究開発名称： 身体的特徴量、行動的特徴量、知識を組み合わせた認証方式の開発 研究開発国： 日本 研究開発時期： 1996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４：集計表

付録３

本アンケート用紙は回答用紙Ａ・Ｂ・Ｃの３パートに分かれています。
内容をご確認頂き、回答頂けるパートのみご回答ください。

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５年９月１５日(金)までに、ご返送ください。
◆郵送での回答：同封の返信用封筒をご利用ください（切手は不要です。）。
◆電子メールでの回答：「cyber@researchworks.co.jp」までお送りください。
なお、Excelファイルのダウンロード方法は同封の「調査ご協力のお願い」に記載しておりますので、恐れ入りますが、記載内容をご確認ください。

問１．アクセス制御機能に関する技術の研究開発を行っていますか。（○は一つ）

１．はい
２．いいえ

※以下の設問には「1．はい」と答えた方のみお進みください。

問２．現在、取り組んでいるのは、どのような分野ですか。（○はいくつでも）

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

問３．今後、もっとも力を入れたいのは、どのような分野ですか。（○は一つ）

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

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

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

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

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

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

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

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

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

問８.貴事業所（研究所）は、どの業種にあてはまりますか。（○は一つ）

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

（太枠線内にご回答ください）

回答用紙B

実用化（製品化）されているアクセス制御機能に関する技術の個別調査

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

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

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

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

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

回答用紙C

研究開発中のアクセス制御機能に関する技術の個別調査

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

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

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

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

＜別紙＞　アクセス制御機能について

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

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

＜参考＞

「不正アクセス行為の禁止等に関する法律」第２条第３項

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

＜回答用紙Aの補足＞表１　アクセス制御機能の分類表

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

＜回答用紙B・Cの補足＞表２　用語説明

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

公開情報及びご連絡先記入用紙

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

【公開用情報】

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

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

【ご担当者様のご連絡先】

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

【個人情報のお取り扱いについて】

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