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

平成27年1月

警察庁生活安全局情報技術犯罪対策課

不正アクセス行為対策等の実態調査
目次

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、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、民間企業・各種団体において、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等を把握することにより、不正アクセス行為からの防御に関する意識の啓発や知識を普及させるとともに、今後の資料として活用しようとするものである。

1.2. 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1,450件抽出した。

・企業（1,282社）

市販のデータベース（四季報、IT総覧等）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（168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

アンケートを電子メールにて回答

②郵送での回答

調査票を郵送し、期日までに回答を郵送

（調査期間：平成26年11月6日（発送日）～11月28日（締切日））

1.3. 調査内容

本調査では次の2つを調査した。

① 研究開発の傾向

アクセス制御機能に関する技術サービスの研究開発の傾向を分析するために、アクセス制御機能を7つの分野に分類し、企業や大学において力をいれている分野等を調査した。

質問項目は次の通りである。

・研究開発体制

・アクセス制御機能に関する技術研究開発に係る現状と今後の展望

・アクセス制御機能に関する実用化（製品化）に係る現状と今後の展望

調査票：付録資料にある『回答用紙A』を参照

【分類の票】

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

② 実用化された製品及び研究開発中の技術・サービス

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

質問項目は以下の通りである。

・何を守るか

・何から保護するのか

・どのようなセキュリティ上の効果があるか

・どのような機能を持っているか

・どのようなレイヤーのセキュリティを守るか

・不正アクセスからの防御対象

・どのようなサービスか

調査票：付録資料の『回答用紙B』、『回答用紙C』を参照

1.4. 送付・回収状況、集計対象件数

全体では、1,450件を送付して、104件を回収し、回収率は7.2%であった。

調査対象となる企業1,282社に対して調査票を送付した。27社から調査票を回収し回収率は2.1%であった。

大学に対しては、理工系学部を設置する大学168校に対して調査票を送付した。38校から調査票を回収し、回収率は22.6%であった。

■送付数・回収数・回収率

	送付数	回収数	回収率（%）
企業	1,282	27	2.1%
大学	168	38	22.6%
不明※	－	39	－
合計	1,450	104	7.2%

全体での回収数104件のうち、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5件であった。また、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20件であった。

■各回答用紙別の集計対象件数

	回答用紙A	回答用紙B	回答用紙C
企業	27	5	2
大学	38	0	18
不明※	39	0	0
合計	104	5	20

※)「不明」は回答用紙に「企業」、「大学」いずれの記載も無かったものを示す。

1.5. 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。

・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。

2. 調査結果（概要と考察）

2.1. 研究開発の傾向

『回答用紙A』により調査した研究開発の傾向について、経年変化を含め考察している。

① 研究開発体制

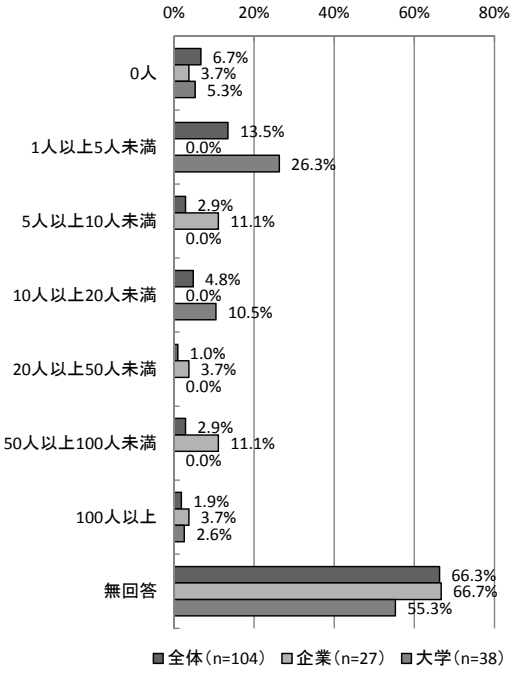
研究開発人数について、「0人」と回答があったものを除くと、企業では「5人以上10人未満」、「50人以上100人未満」が最も多くなっている。一方、大学では「1人以上5人未満」の小規模人員での研究開発が最も多くなっており、大学に比べて企業の方が人員体制は整っている。

研究開発費について、「なし」と回答があったものを除くと、企業では「1億円以上10億円未満」が最も多く、大学では「1,000万円未満」が最も多くなっており、大学に比べて企業の方が人員体制に続き予算に関しても整っている。

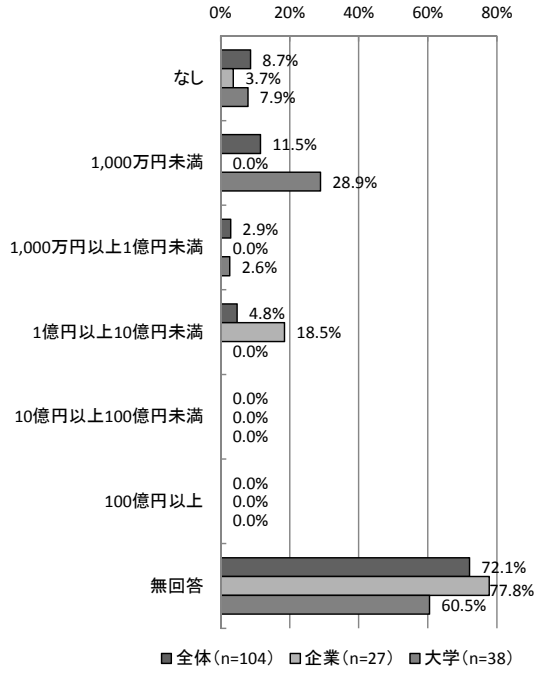
“研究開発に携わっている人数”について、全体では、「1人以上5人未満」が13.5%で最も多い。企業では、「5人以上10人未満」、「50人以上100人未満」が11.1%で最も多く、大学では、「1人以上5人未満」が26.3%で最も多い。

“年間の研究開発費”については、全体では、「1,000万円未満」が11.5%で最も多い。企業では、「1億円以上10億円未満」が18.5%で最も多く、大学では、「1,000万円未満」が28.9%で最も多い。

【本調査】研究開発に携わっている人数（SA）【A-問8】



【本調査】年間の研究開発費（SA）【A-問7】



② 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

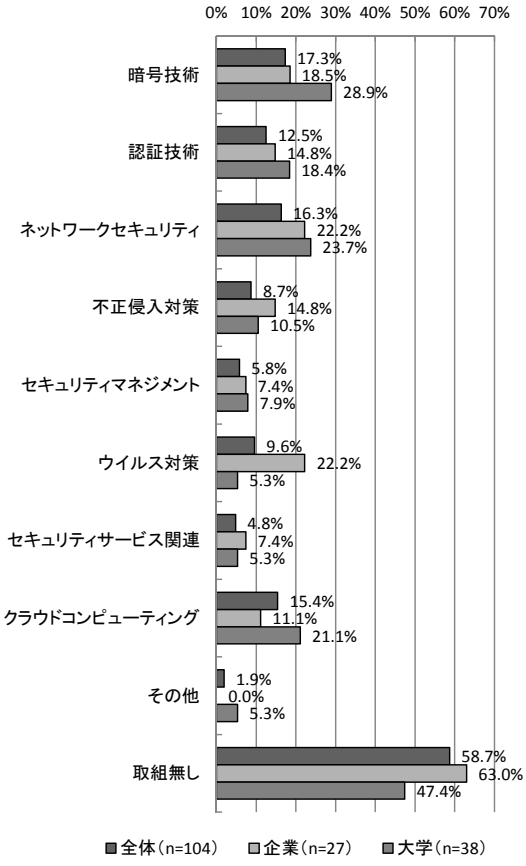
現在、取り組んでいる分野について、「取組無し」との回答を除くと、全体、大学ともに「暗号技術」が最も多く、企業は「ネットワークセキュリティ」、「ウイルス対策」が最も多い。

今後、取り組んでいく分野について、「取組無し」との回答を除くと、全体では「暗号技術」、「ネットワークセキュリティ」が最も多く、企業では「ネットワークセキュリティ」、「ウイルス対策」が最も多く、大学では「暗号技術」が最も多く、現在取り組んでいる分野と今後取り組んでいく分野の両方で相関がみられる。

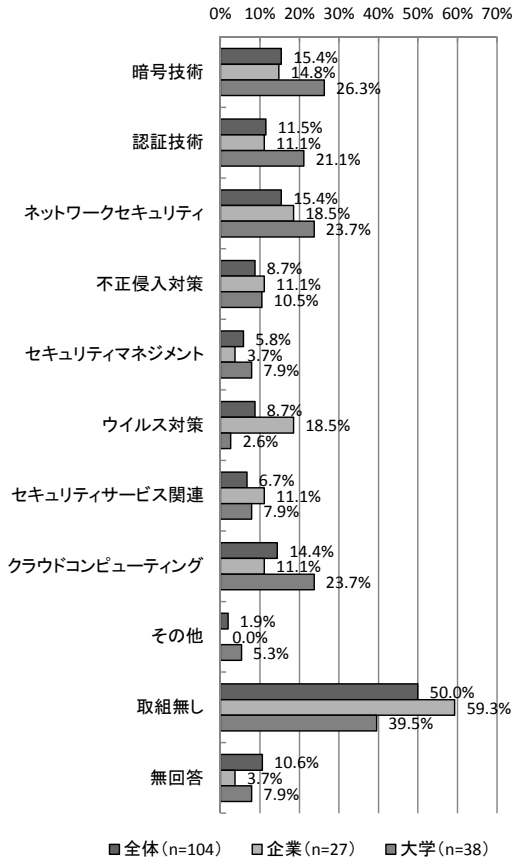
“現在、取り組んでいる分野”について、全体では、「取組無し」と回答があった58.7%を除くと、「暗号技術」が17.3%で最も多く、「ネットワークセキュリティ」が16.3%、「クラウドコンピューティング」が15.4%で続いている。「取組無し」との回答を除くと企業では、「ネットワークセキュリティ」、「ウイルス対策」が22.2%で最も多く、大学では、「暗号技術」が28.9%で最も多い。

“今後、取り組んでいく分野”について、全体では、「取組無し」と回答があった50.0%を除くと、「暗号技術」、「ネットワークセキュリティ」が15.4%で最も多く、「クラウドコンピューティング」が14.4%で続いている。「取組無し」との回答を除くと企業では、「ネットワークセキュリティ」、「ウイルス対策」が18.5%で最も多く、大学では、「暗号技術」が26.3%で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1】



【本調査】今後、取り組んでいく分野（MA）【A-問2】



③　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、「特になし」との回答を除くと、企業、大学ともに「暗号技術」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、「予定なし」との回答を除くと、企業では「ウイルス対策」が最も多く、大学では「暗号技術」が最も多くなっている。

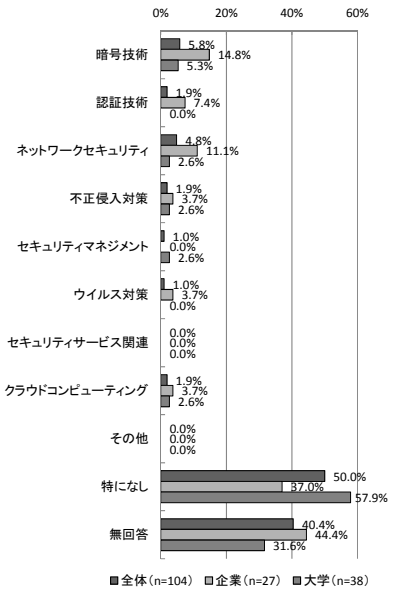
今後、最も力を入れていく分野について、企業では「暗号技術」、「ネットワークセキュリティ」が最も多く、大学では「暗号技術」が最も多くなっている。

“現在、実用化（製品化）されているアクセス制御機能”について、全体では、「特になし」と回答があった50.0%を除くと、「暗号技術」が5.8%で最も多い。企業では、「特になし」と回答があった37.0%を除くと、「暗号技術」が14.8%、大学では、「特になし」と回答があった57.9%を除くと、「暗号技術」が5.3%となっている。

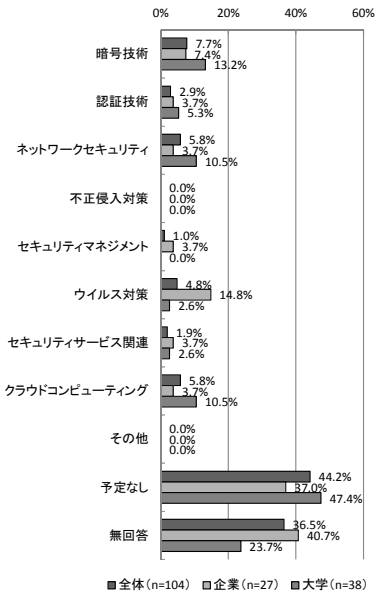
“今後、実用化（製品化）を見込んでいるアクセス制御機能”について、全体では、「予定なし」と回答があった44.2%を除くと、「暗号技術」が7.7%で最も多い。企業では、「予定なし」と回答があった37.0%を除くと、「ウイルス対策」が14.8%で最も多く、大学では、「予定なし」と回答があった47.4%を除くと、「暗号技術」が13.2%で最も多くなっている。

“今後、最も力を入れていく分野”について、全体では、「暗号技術」が22.0%、企業では、「暗号技術」、「ネットワークセキュリティ」が30.0%、大学では、「暗号技術」が25.0%で最も多くなっている。

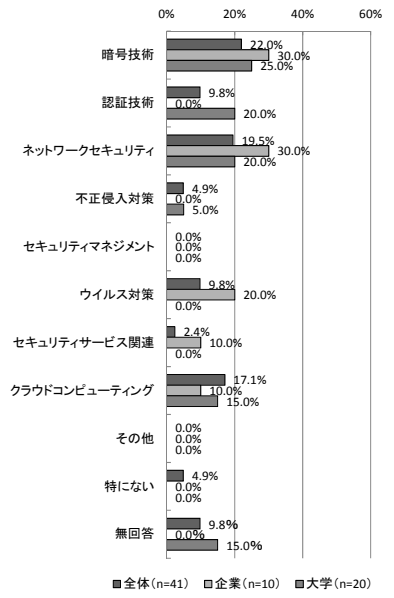
【本調査】現在、実用化（製品化）されている　アクセス制御機能（MA）【A-問4】



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



【本調査】今後、最も力を入れていく分野（SA）【A-問3】



2.2. 実用化された製品及び研究開発中の技術・サービス

① 研究開発・製品化事例の考察

『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。

(1) 何を守るか？

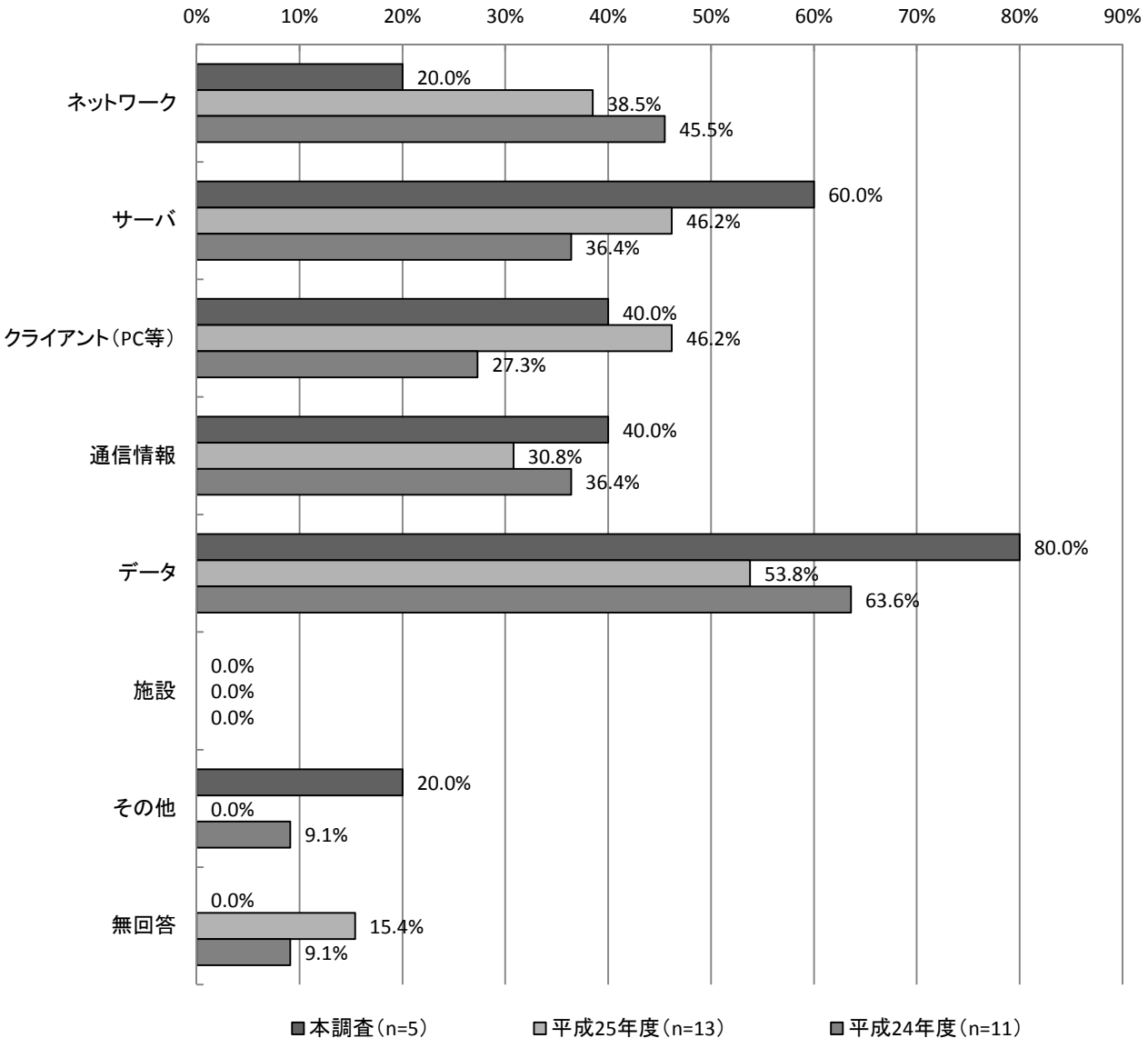
Ⅰ.実用化(製品化)されているもの

実用化（製品化）されているものについては「データ」の80.0%（4件）が最も多く、「サーバ」の60.0%（3件）が続いている。

昨年度と比較して、「ネットワーク」、「クライアント（PC等）」が減少しており、「サーバ」、「通信情報」、「データ」は増加している。

【経年変化】何を守るか？

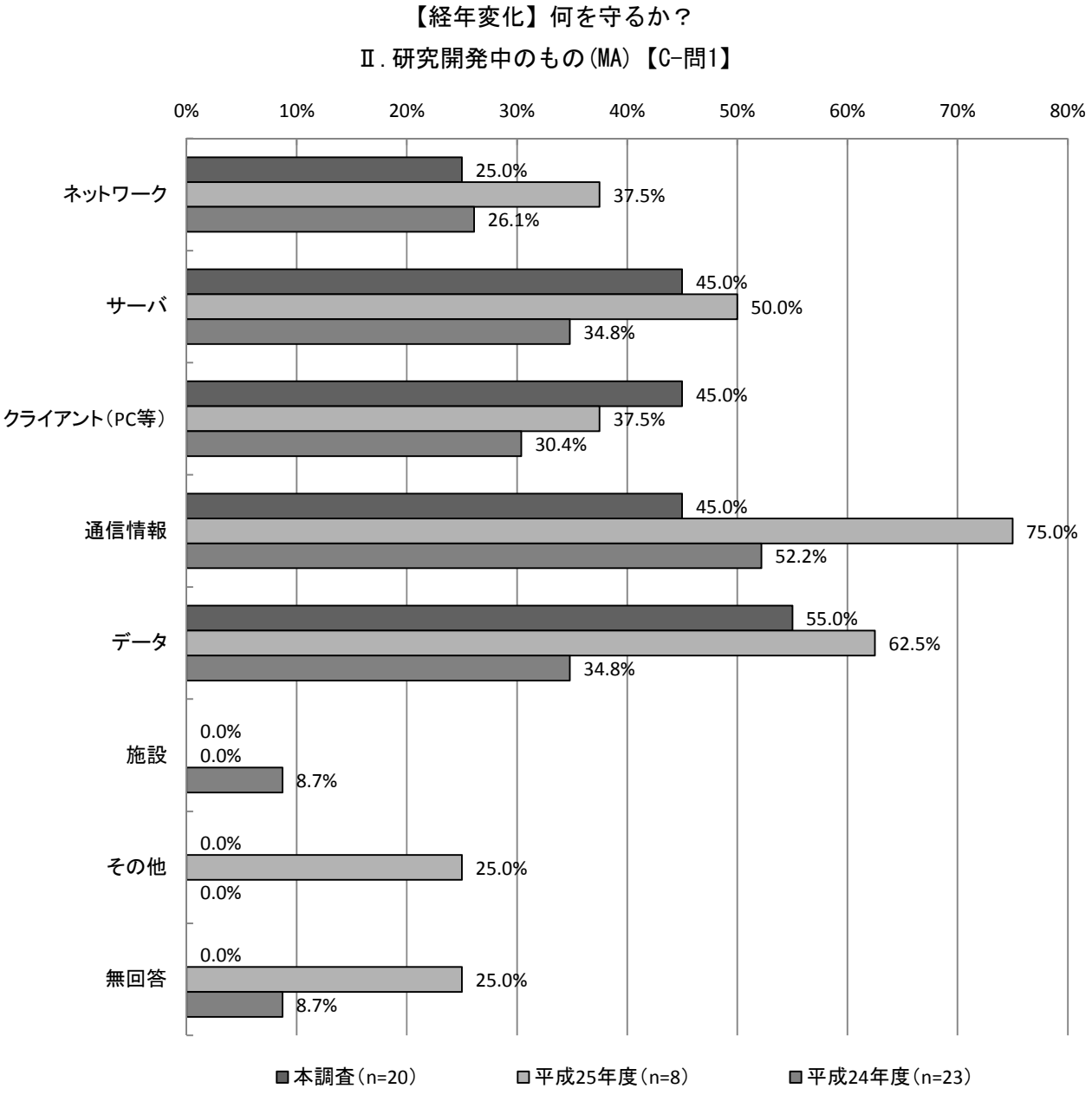
Ⅰ.実用化(製品化)されているもの(MA)【B-問1】



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55.0%（11件）と最も多く、「サーバ」、「クライアント(PC等)」、「通信情報」が45.0%（9件）で続いている。

経年変化を見ると、「クライアント(PC等)」を除き減少している。

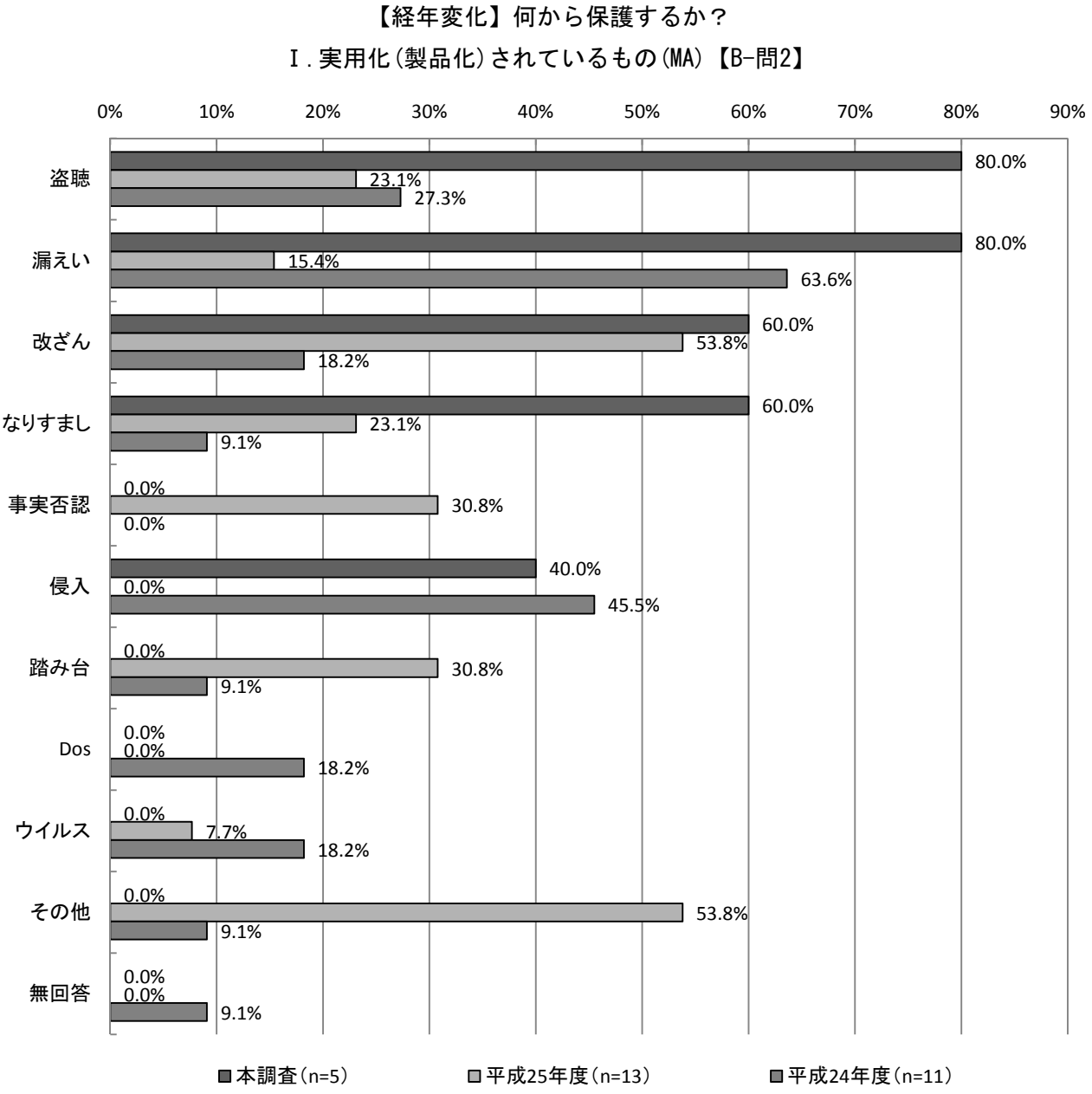


(2) 何から保護するか？

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、「盗聴」、「漏えい」の80.0%（4件）が最も多く、「改ざん」、「なりすまし」が60.0%（3件）で続いている。

経年変化を見ると「改ざん」、「なりすまし」は増加傾向にあり、実用化（製品化）が進んでいることが分かる。逆に昨年度と比較すると、「事実否認」、「踏み台」、「ウイルス」は減少している。

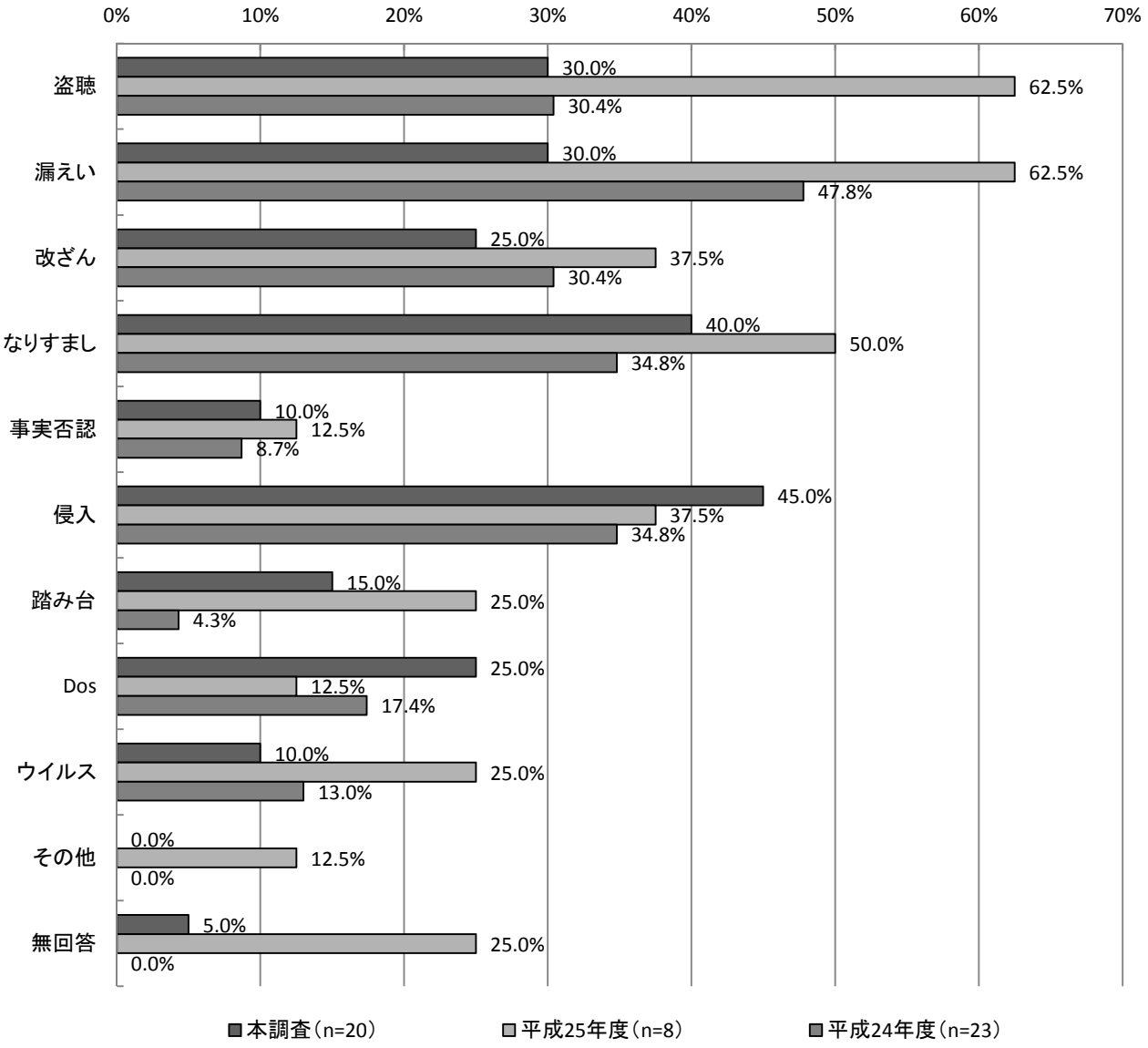


Ⅱ.研究開発中のもの

研究開発中のものについては、「侵入」の45.0%（9件）が最も多く、「なりすまし」の40.0%（8件）、「盗聴」、「漏えい」の30.0%（6件）が続いている。

経年変化を見ると、「侵入」、「Dos」が増加し、「盗聴」、「漏えい」、「改ざん」、「なりすまし」、「事実否認」、「踏み台」、「ウイルス」は減少している。

【経年変化】何から保護するか？
Ⅱ.研究開発中のもの(MA)【C-問2】



(3) どのようなセキュリティ上の効果があるか？

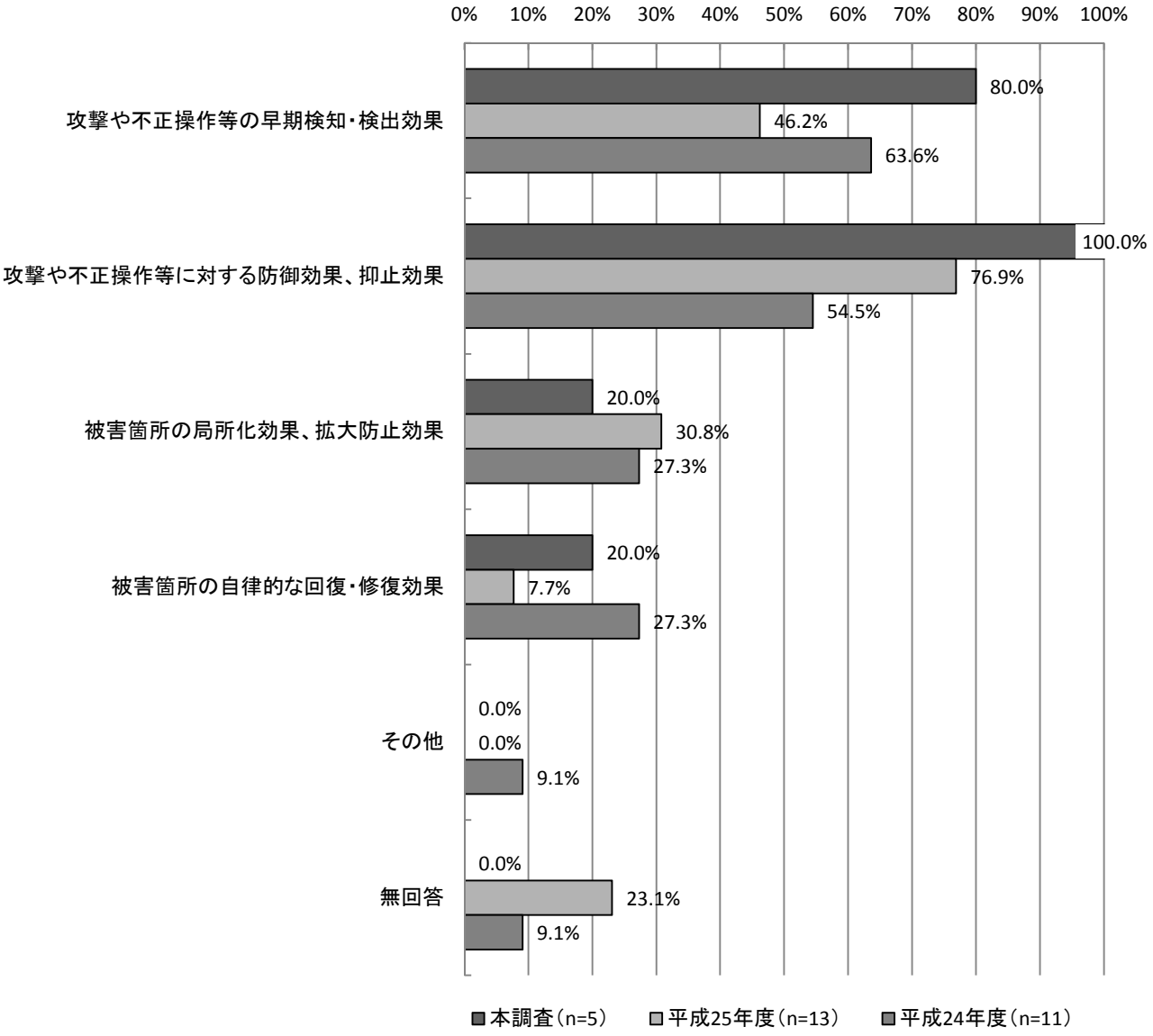
Ⅰ.実用化(製品化)されているもの

実用化（製品化）されているものについては、「攻撃や不正操作等に対する防御効果、抑止効果」が100.0%（5件）で最も多く、「攻撃や不正操作等の早期検知・検出効果」の80.0%（4件）が続いている。

他の項目と比較して、「攻撃や不正操作等に対する防御効果、抑止効果」、「攻撃や不正操作等の早期検知・検出効果」は高い割合を示しており、これらがセキュリティ上重要な役割を果たしていることが分かる。

【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】



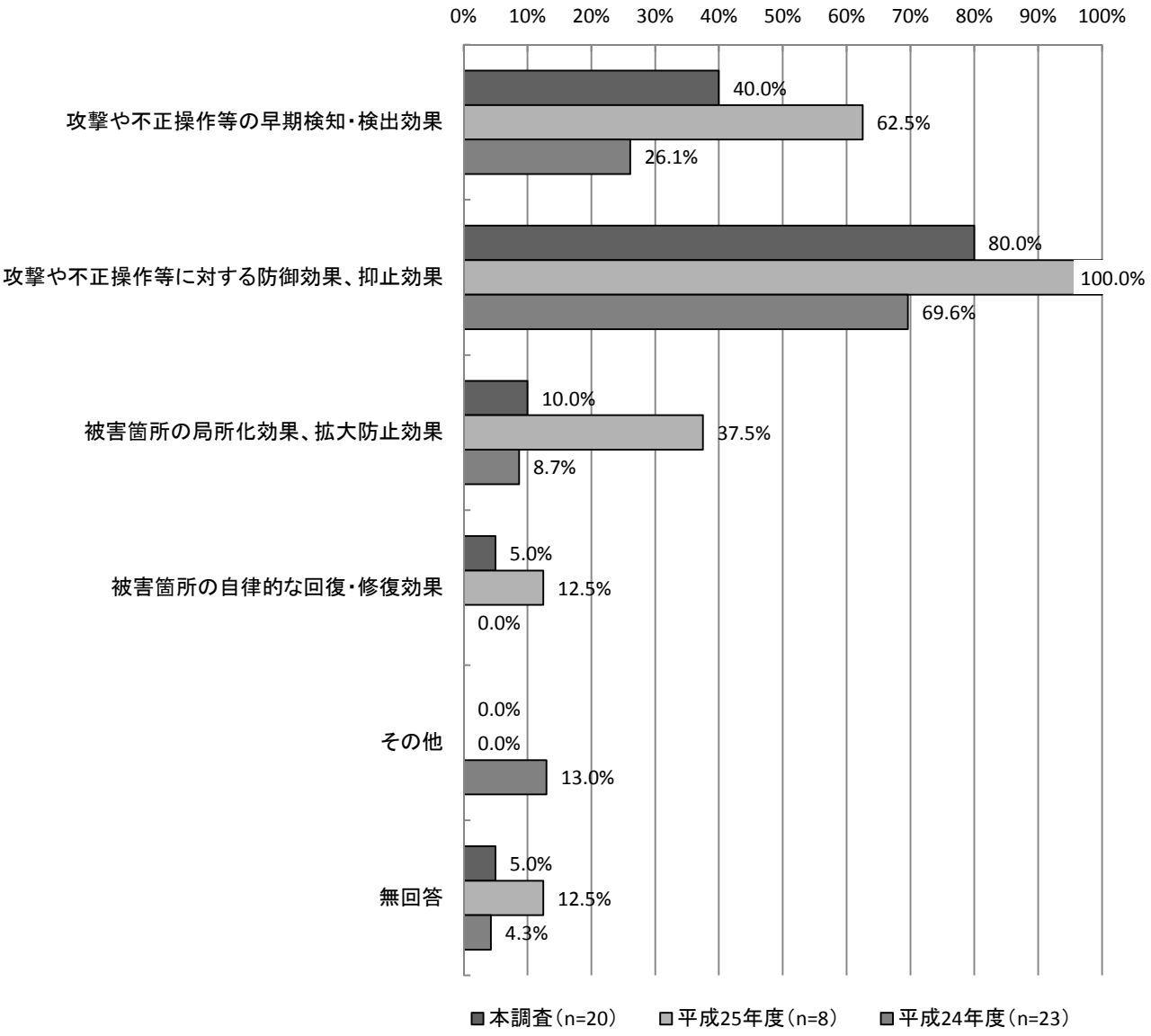
Ⅱ.研究開発中のもの

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80.0%（16件）と最も多く、「攻撃や不正操作等の早期検知・検出効果」の40.0%（8件）が続いている。

経年変化を見ると、「攻撃や不正操作等に対する防御効果、抑止効果」が常に高い割合を示しており、実用化（製品化）されているものの結果も含め、セキュリティ上重要な役割と考えられる。

【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】

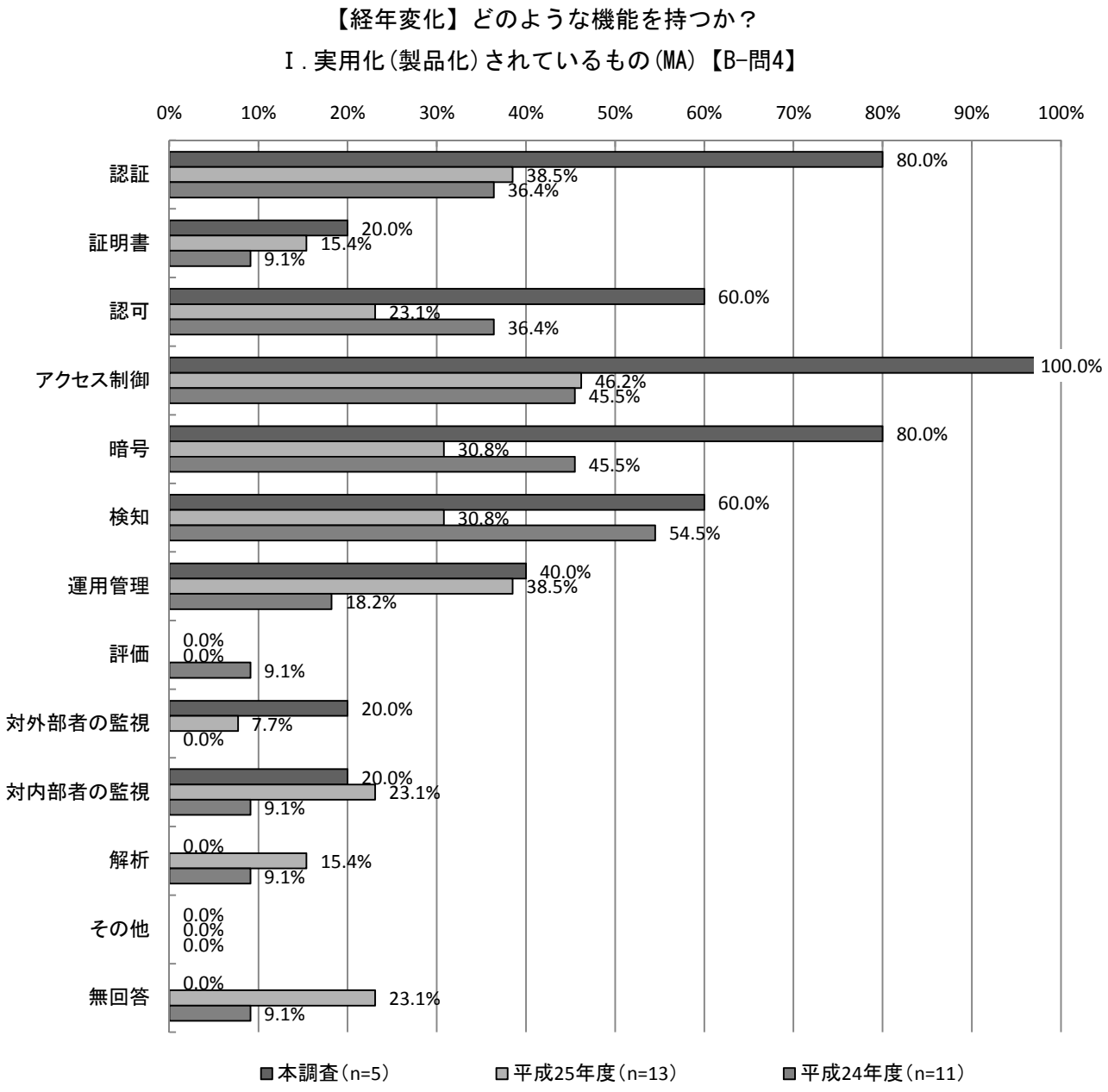


(4) どのような機能を持つか？

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」の100.0%（5件）が最も多く、「認証」、「暗号」の80.0%（4件）、「認可」、「検知」の60.0%（3件）が続いている。

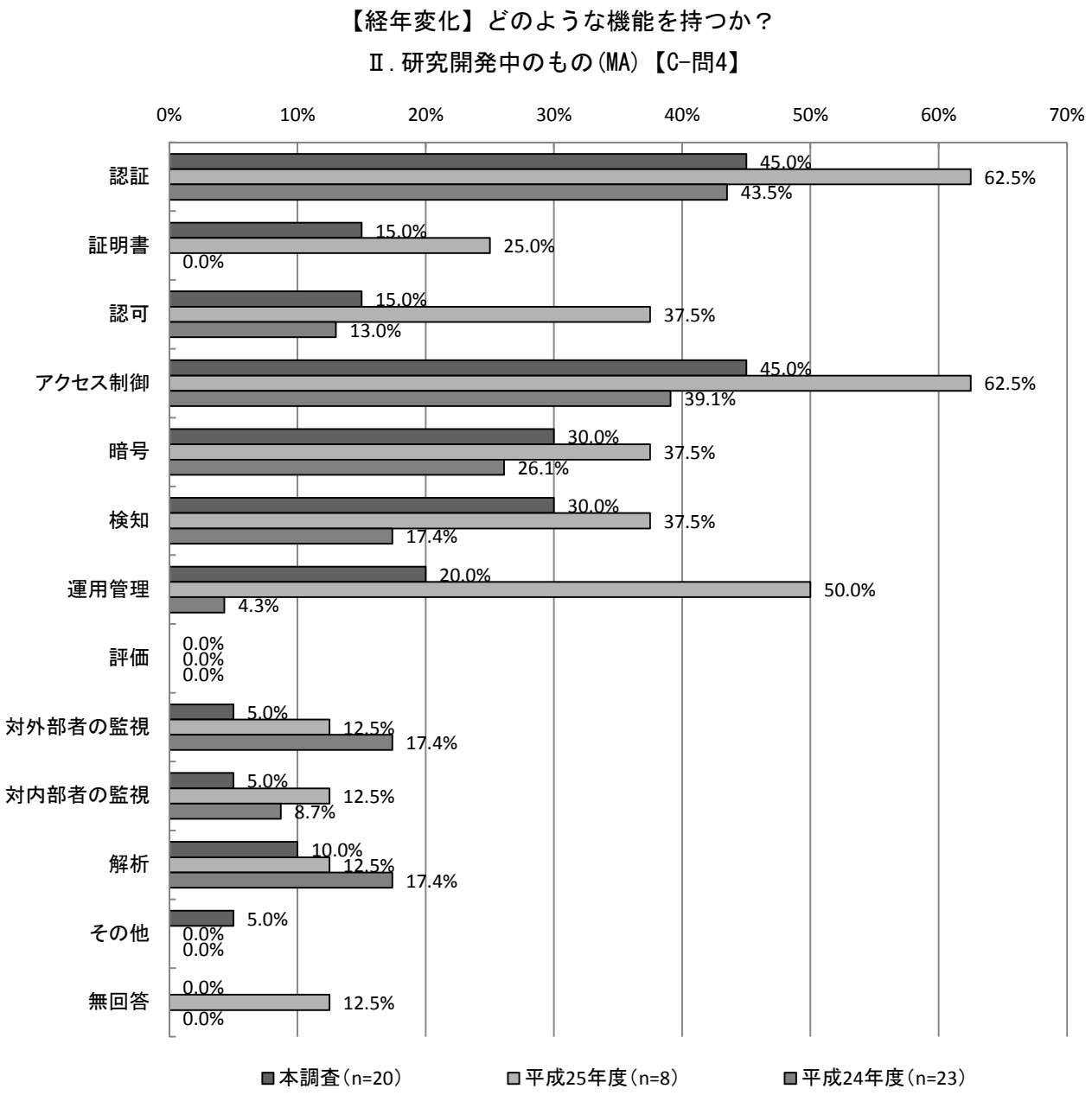
経年変化を見ると、「認証」、「証明書」、「アクセス制御」、「運用管理」、「対外部者の監視」で増加傾向がみられる。



Ⅱ.研究開発中のもの

研究開発中のものについては、「認証」、「アクセス制御」の45.0%（9件）が最も多く、「暗号」、「検知」の30.0%（6件）が続いている。

経年変化を見ると「認証」、「アクセス制御」が昨年度から引き続き高い割合を示しているが、すべての項目で昨年度と比較して減少している。



(5) どのようなレイヤーのセキュリティを守るか？

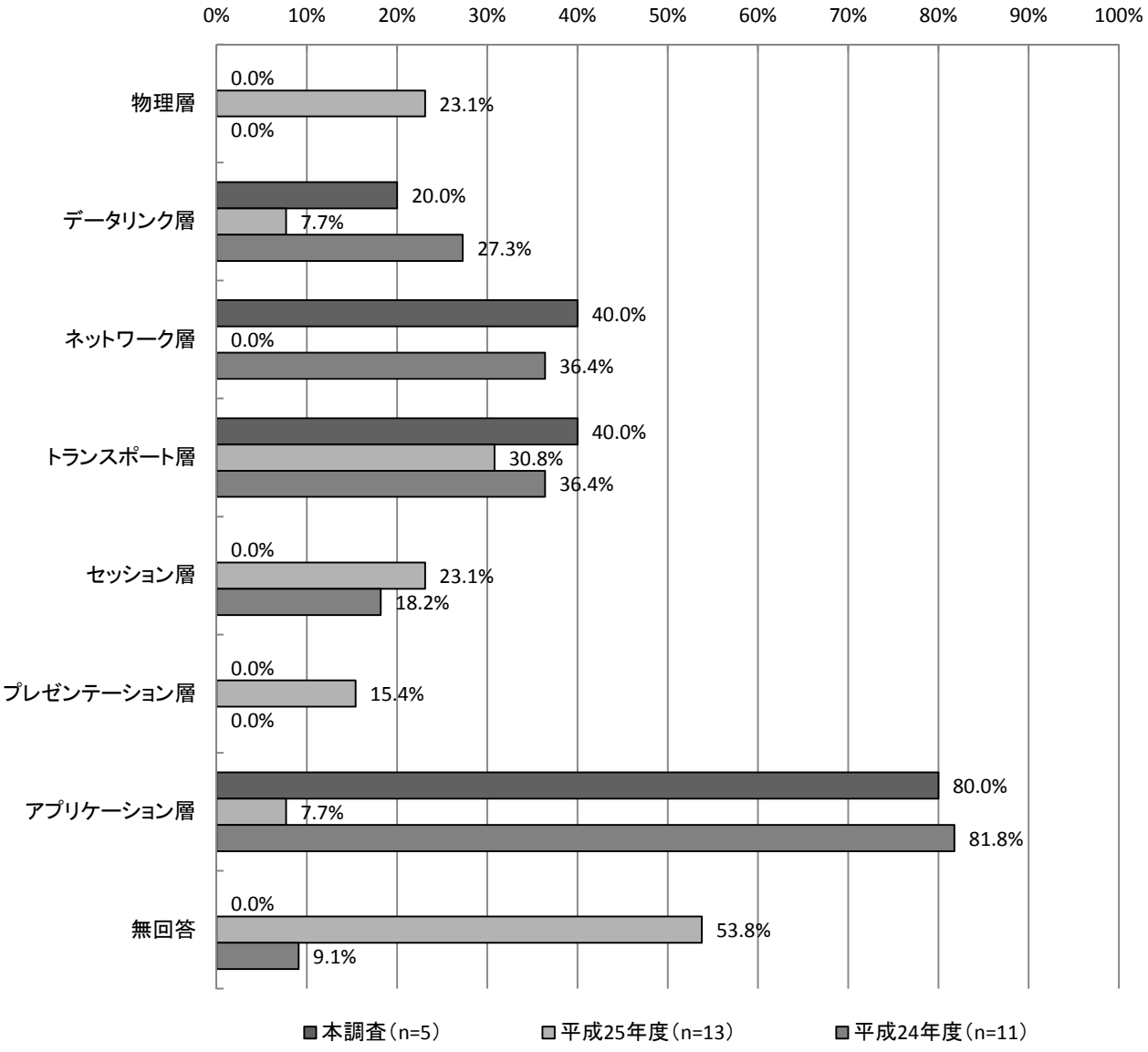
Ⅰ.実用化(製品化)されているもの

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」の80.0%（4件）が最も多く、「ネットワーク層」、「トランスポート層」が40.0%（2件）が続いている。

経年変化を見ると、「データリンク層」、「ネットワーク層」、「トランスポート層」、「アプリケーション層」は昨年度と比較して増加している。

【経年変化】どのようなレイヤーのセキュリティを守るか？

Ⅰ.実用化(製品化)されているもの(MA)【B-問5】

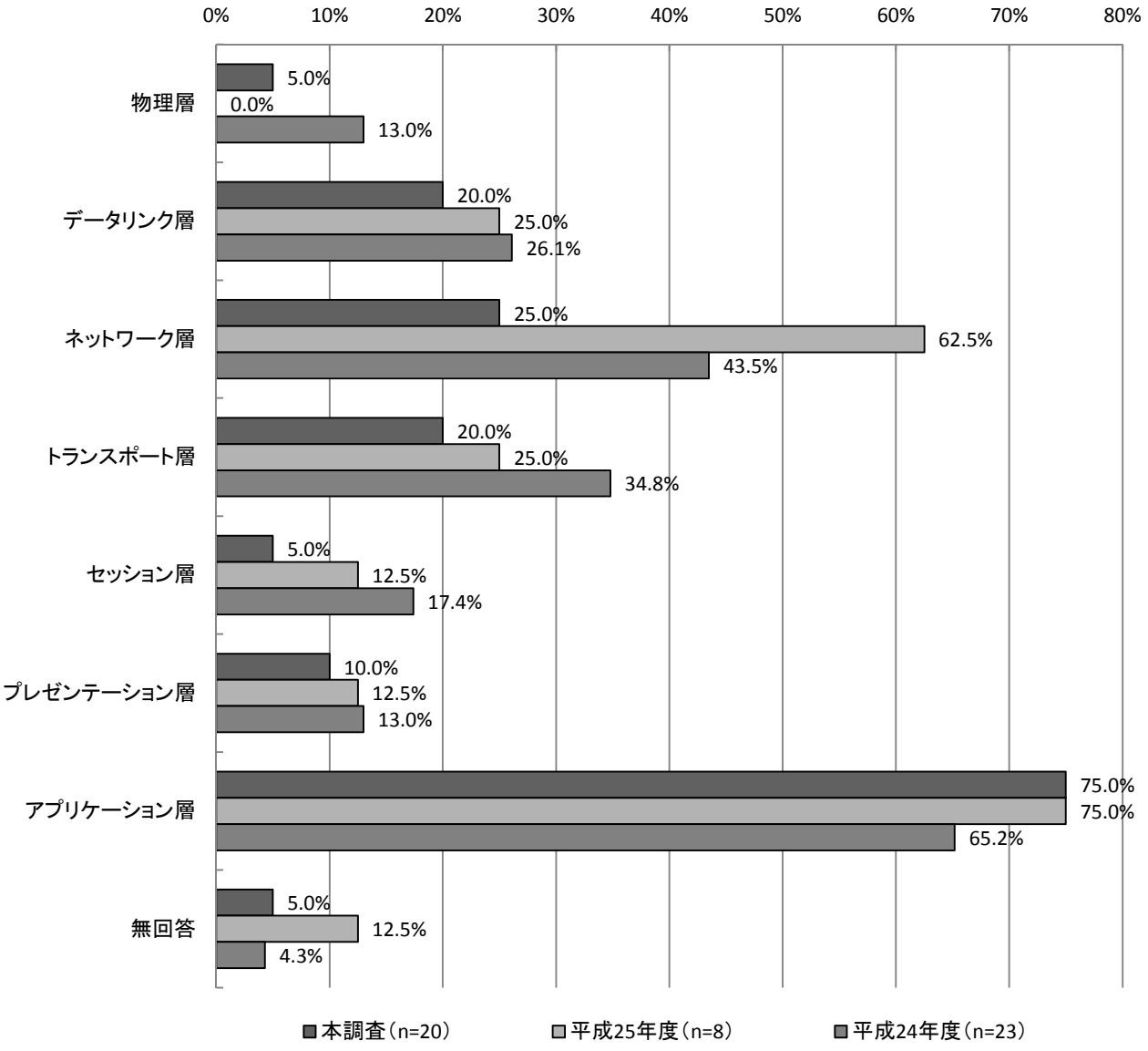


Ⅱ.研究開発中のもの

研究開発中のものについては、「アプリケーション層」が75.0%（15件）で最も多く、「ネットワーク層」の25.0%（5件）、「データリンク層」、「トランスポート層」の20.0%（4件）が続いている。

昨年度と比較すると、順位に目立った変動はないものの、昨年度と比較して減少している項目が多い。

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



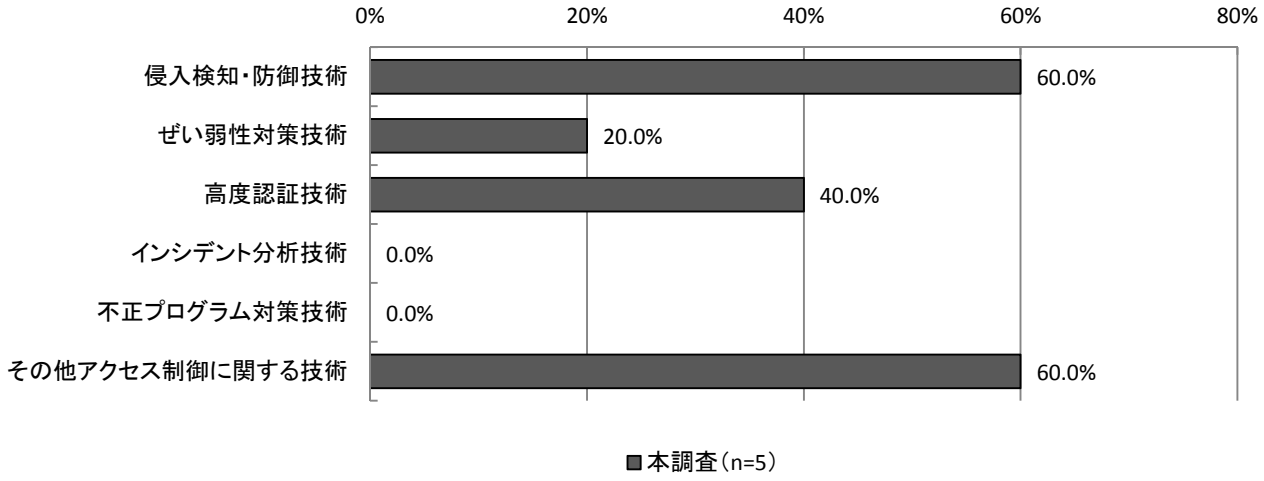
(6) 不正アクセスからの防御対象

Ⅰ.実用化(製品化)されているもの

実用化（製品化）されているものについては、「侵入検知・防御技術」が60.0%（3件）で最も多く、「高度認証技術」が40.0%（2件）、「ぜい弱性対策技術」が20.0%（1件）で続いている。

【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】

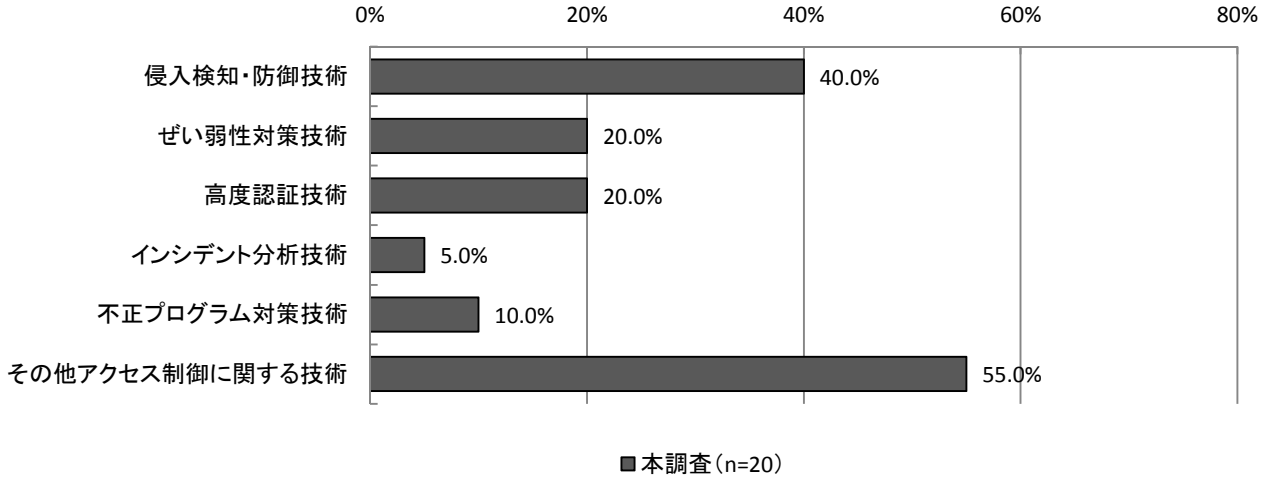


Ⅱ.研究開発中のもの

研究開発中のものについては、「侵入検知・防御技術」が40.0%（8件）で最も多く、「ぜい弱性対策技術」、「高度認証技術」が20.0%（4件）で続いている。

【全体】不正アクセスからの防御対象

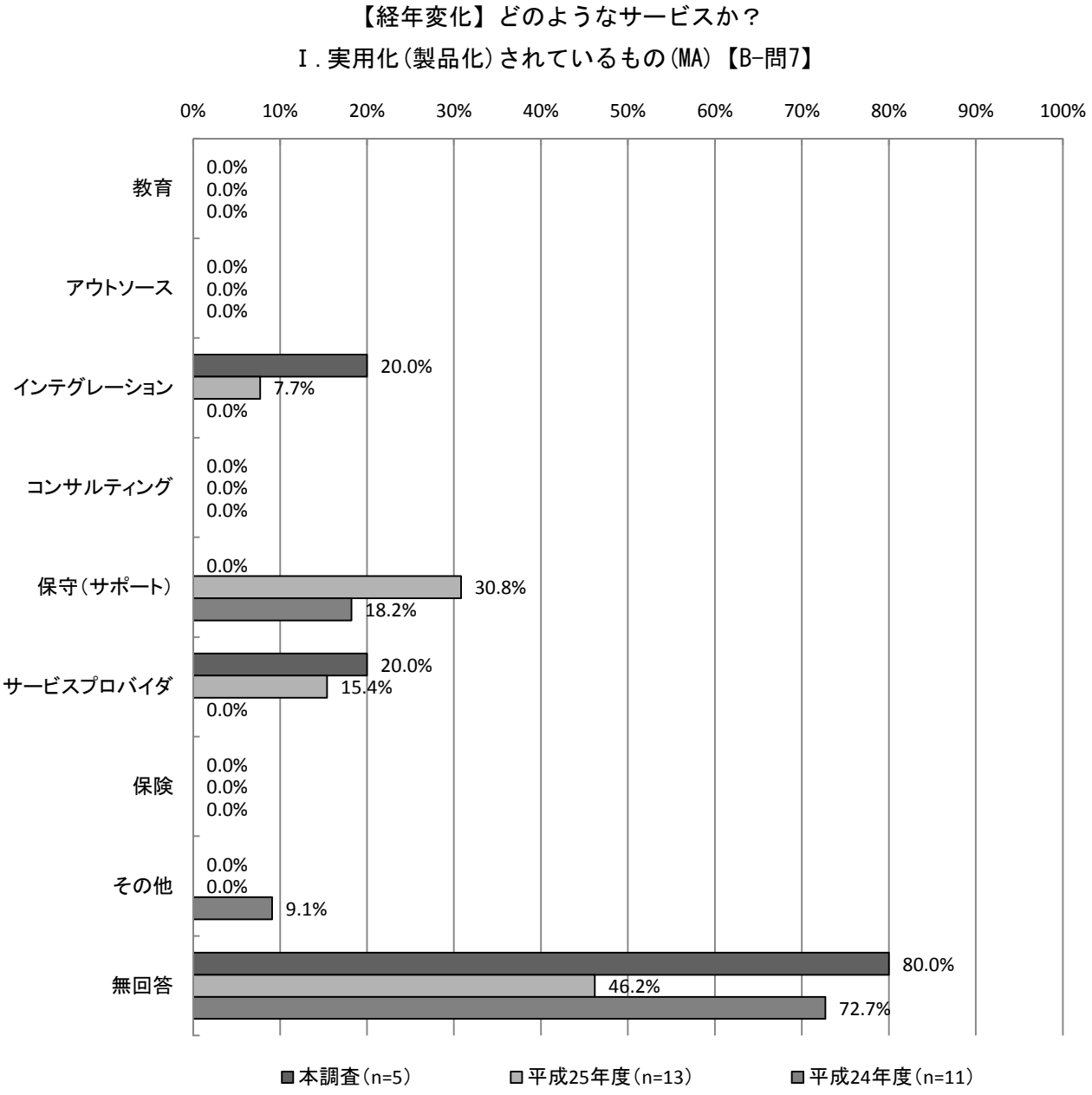
Ⅱ.研究開発中のもの(MA)【C-問6】



(7) どのようなサービスか？

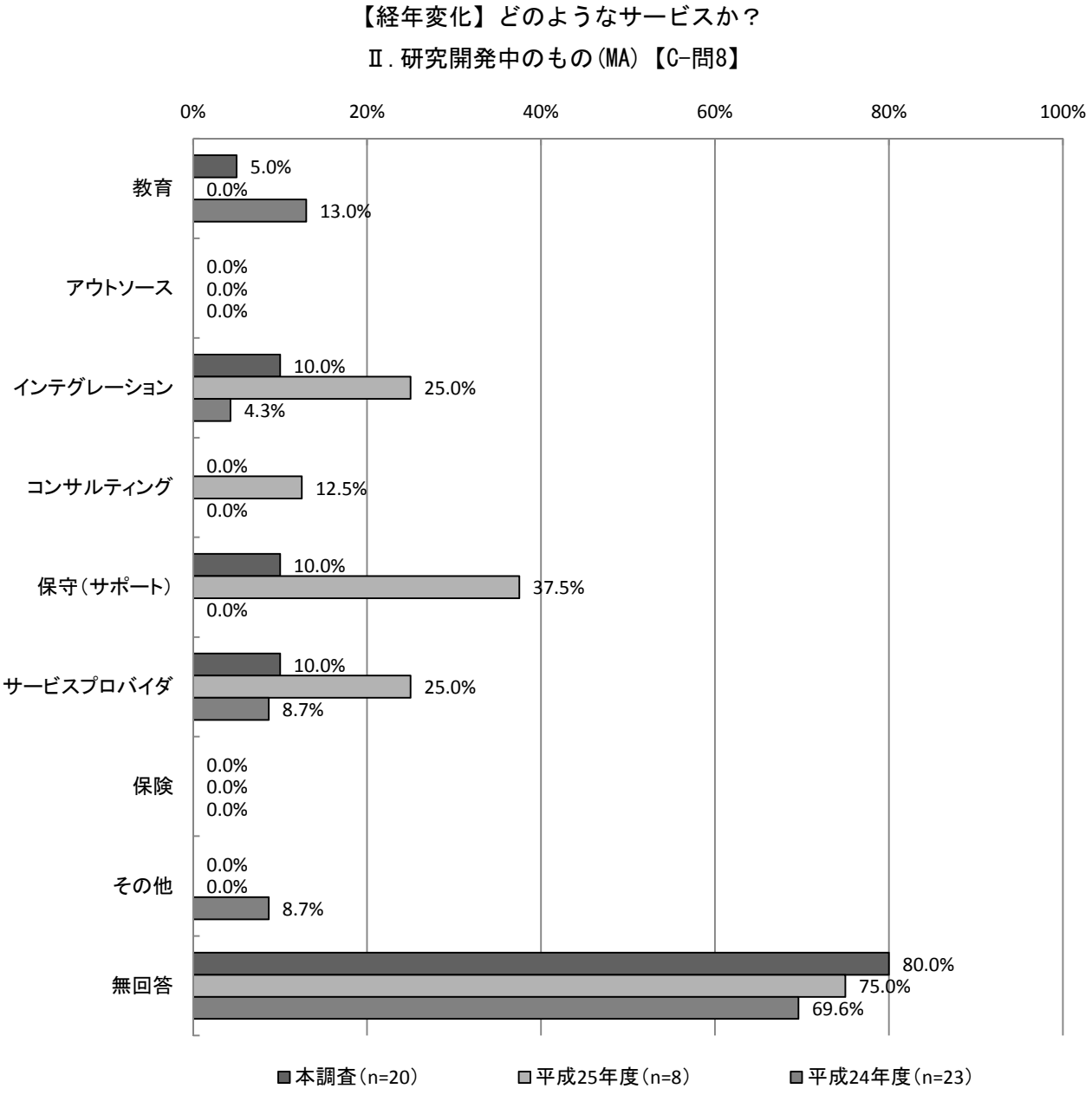
Ⅰ.実用化(製品化)されているもの

実用化（製品化）されているものについては、「インテグレーション」、「サービスプロバイダ」が20.0%（1件）となっている。



Ⅱ.研究開発中のもの

研究開発中のものについては、「インテグレーション」、「保守（サポート）」、「サービスプロバイダ」が10.0%（2件）で最も多く、「教育」が5.0%（1件）で続いているが、昨年度と比較すると、「保守（サポート）」が27.5ポイント減少している。

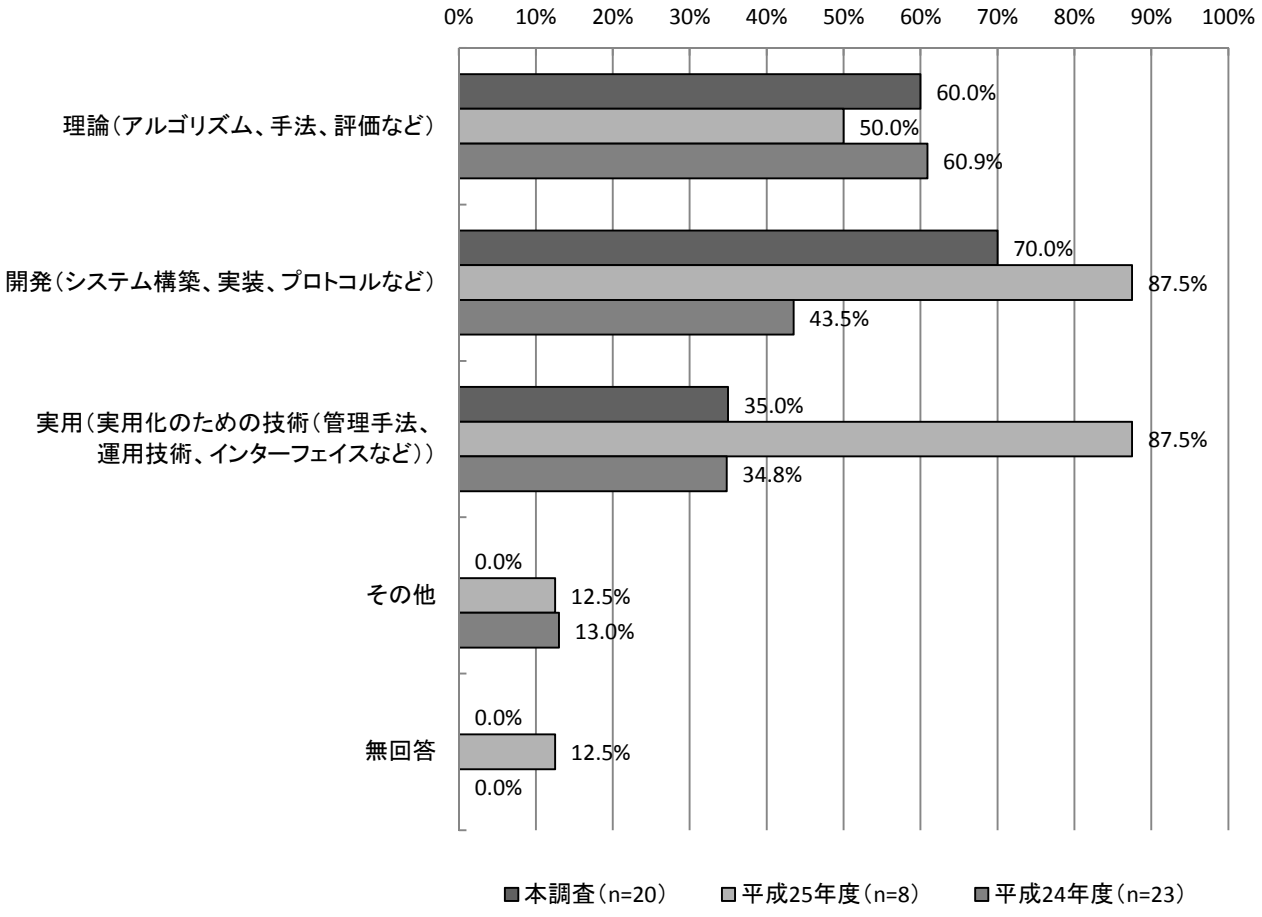


(8) 研究開発の成果としてどのようなものを目指しているか？

研究開発の成果として目指す項目については、「開発（システム構築、実装、プロトコルなど)」が 70.0%（14 件）で最も多く、「理論（アルゴリズム、手法、評価など)」が 60.0%（12 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 35.0%（7 件）となっている。

経年変化を見ると、昨年度と比較して「理論」は増加し、「開発」、「実用」は減少している。

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

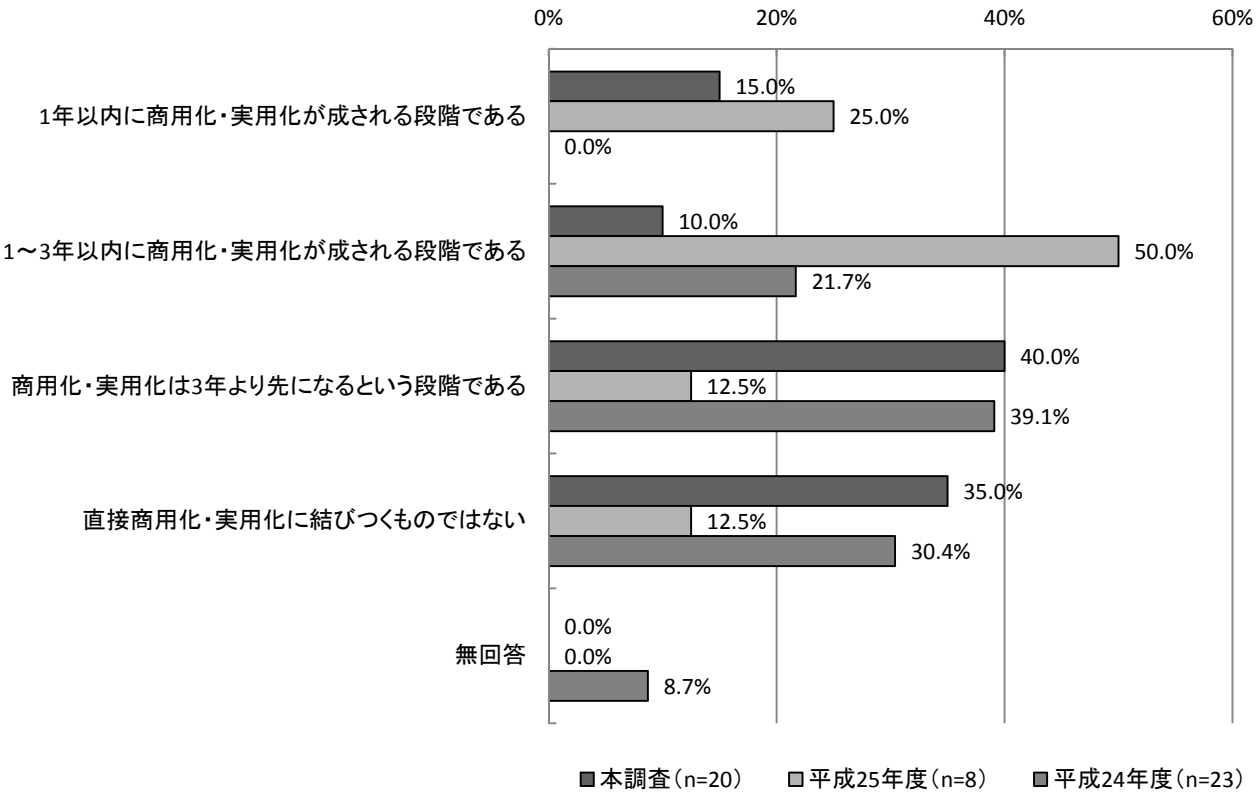


(9) 研究開発の進捗状況

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」の 40.0%（8 件）が最も多い。

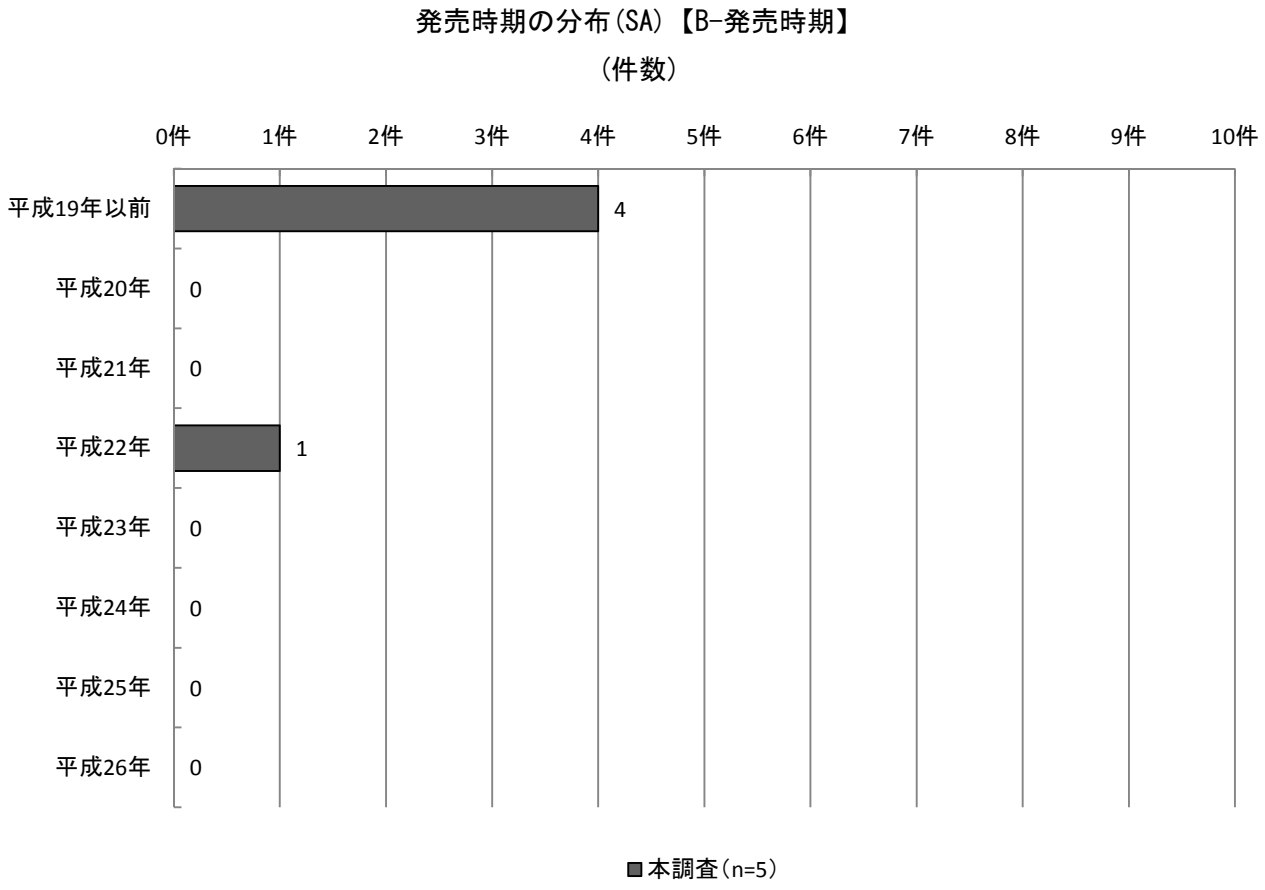
昨年度と比較すると、「商用化・実用化は 3 年より先になるという段階である」、「直接商用化・実用化に結びつくものではない」が増加し、「1 年以内に商用化・実用化が成される段階である」、「1～3 年以内に商用化・実用化が成される段階である」が減少している。

研究開発の進捗状況(SA)【C-問 9】



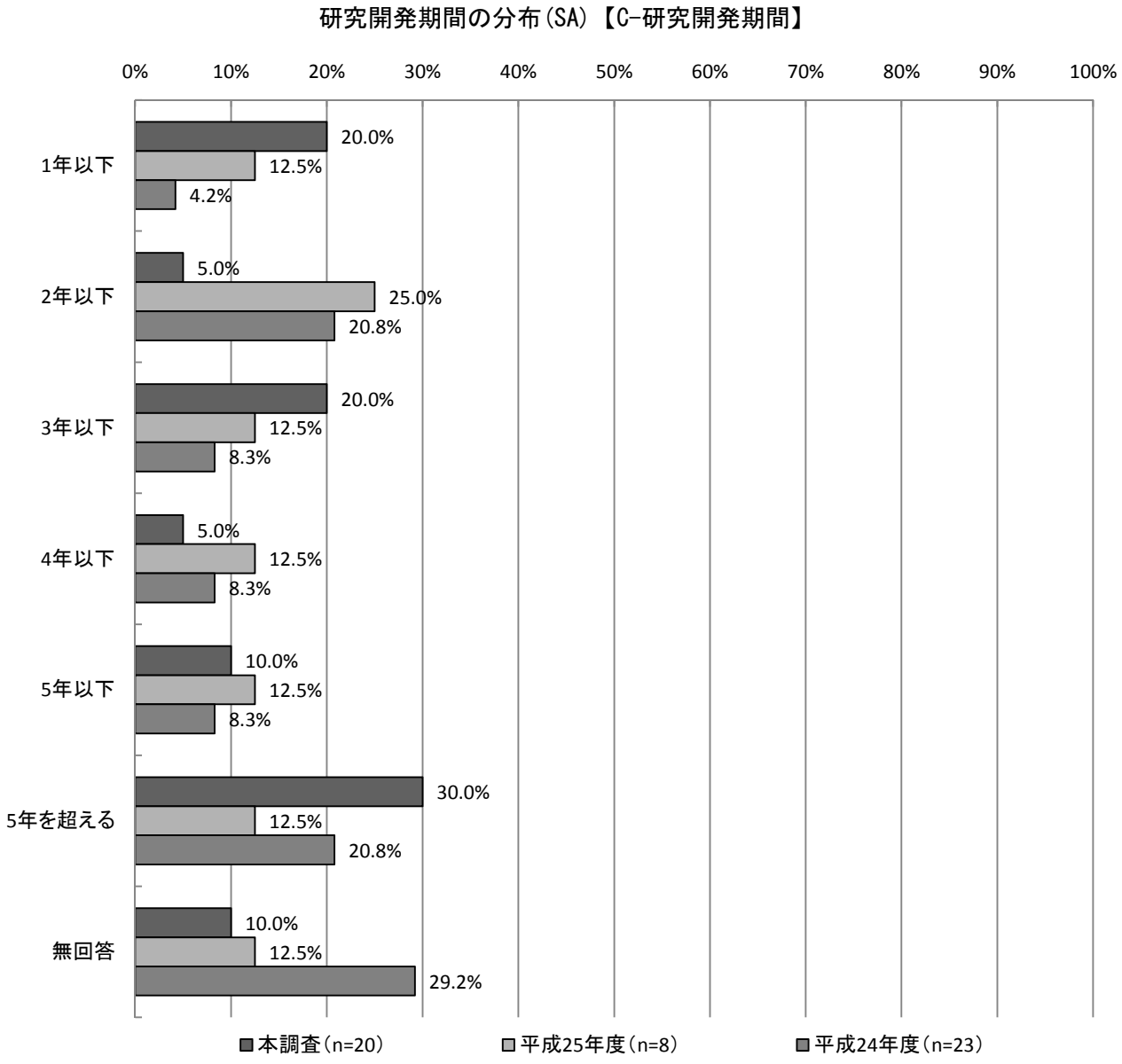
(10)　発売時期の分布

発売時期については、「平成 19 年以前」が 4 件で最も多く、「平成 22 年」が 1 件となっている。



（11） 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 30.0%（6 件）で最も多くなっており、開発期間が長くなっている。



3. 調査結果（データ）

3.1. 研究開発の傾向

『回答用紙A』により調査した研究開発の傾向について、個別データを示す。

3.1.1. 回答企業・大学の属性

(1) 研究開発に携わっている人数【A-問8】

【本調査】

全体では、「1人以上5人未満」が13.5%で最も多く、「0人」が6.7%で続いている。

企業では、「5人以上10人未満」、「50人以上100人未満」が多く、大学では、「1人以上5人未満」の小規模での研究開発が多くなっている。

【経年変化】

全体では、「1人以上5人未満」、「10人以上20人未満」、「50人以上100人未満」が増加している。

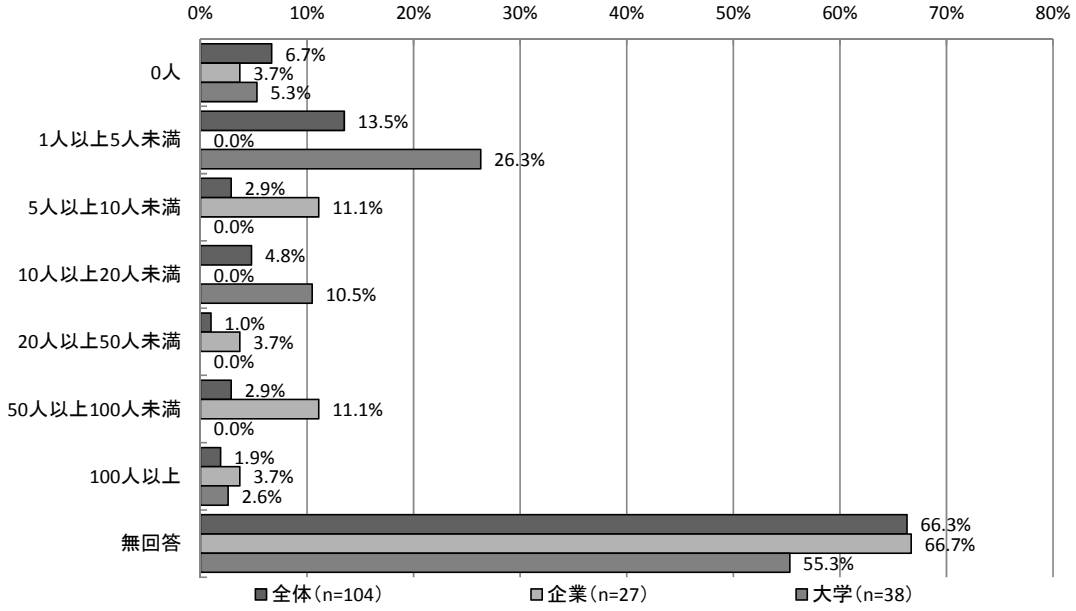
企業では、「5人以上10人未満」、「20人以上50人未満」、「50人以上100人未満」、「100人以上」、大学では、「1人以上5人未満」、「10人以上20人未満」が増加している。

【本調査】

研究開発人員について、全体では、「1 人以上 5 人未満」が 13.5%（14 件）であった。

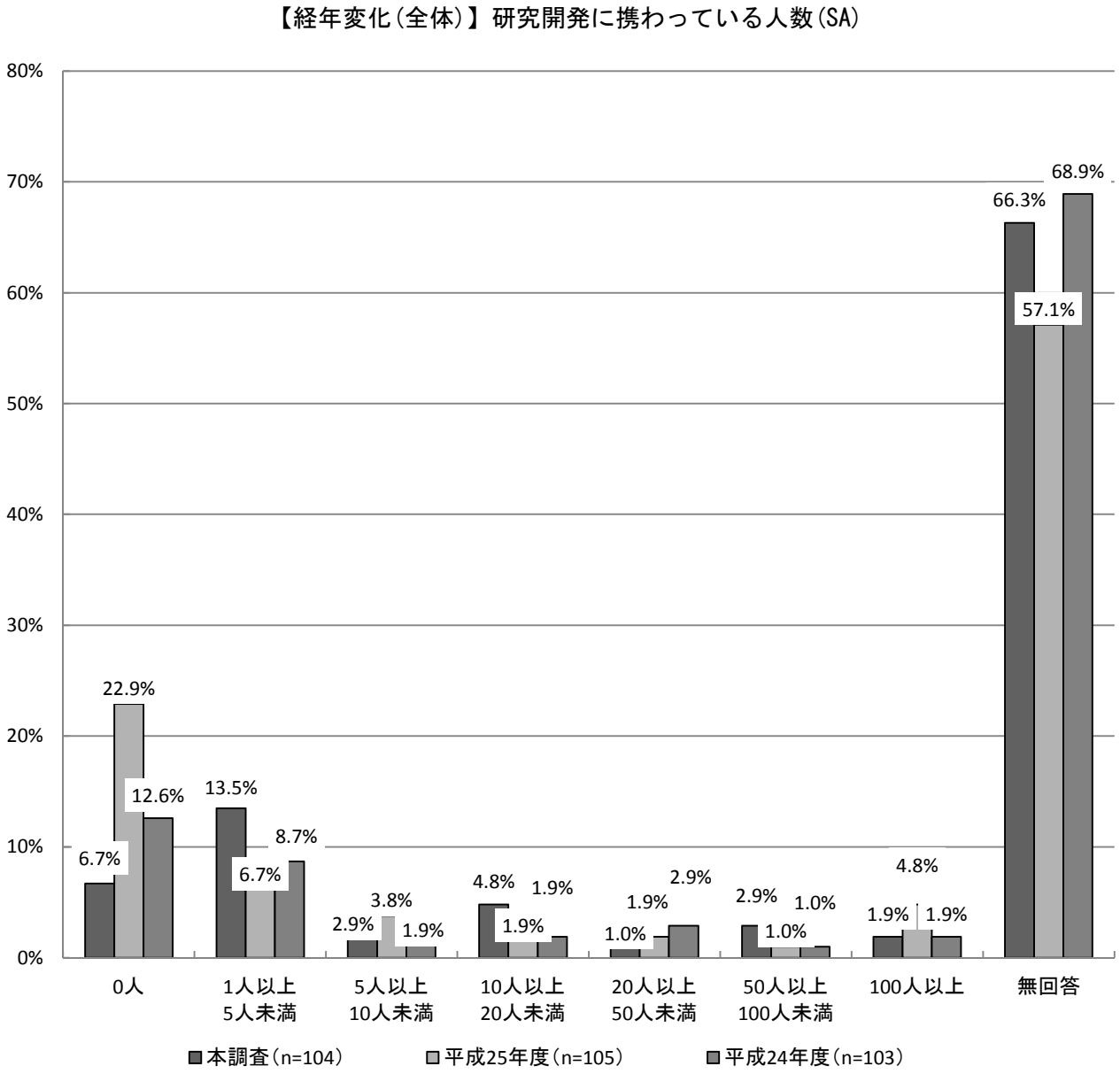
企業では、「5 人以上 10 人未満」、「50 人以上 100 人未満」が 11.1%（3 件）、大学では、「1 人以上 5 人未満」が 26.3%（10 件）で最も多くなっている。

【本調査】研究開発に携わっている人数(SA)



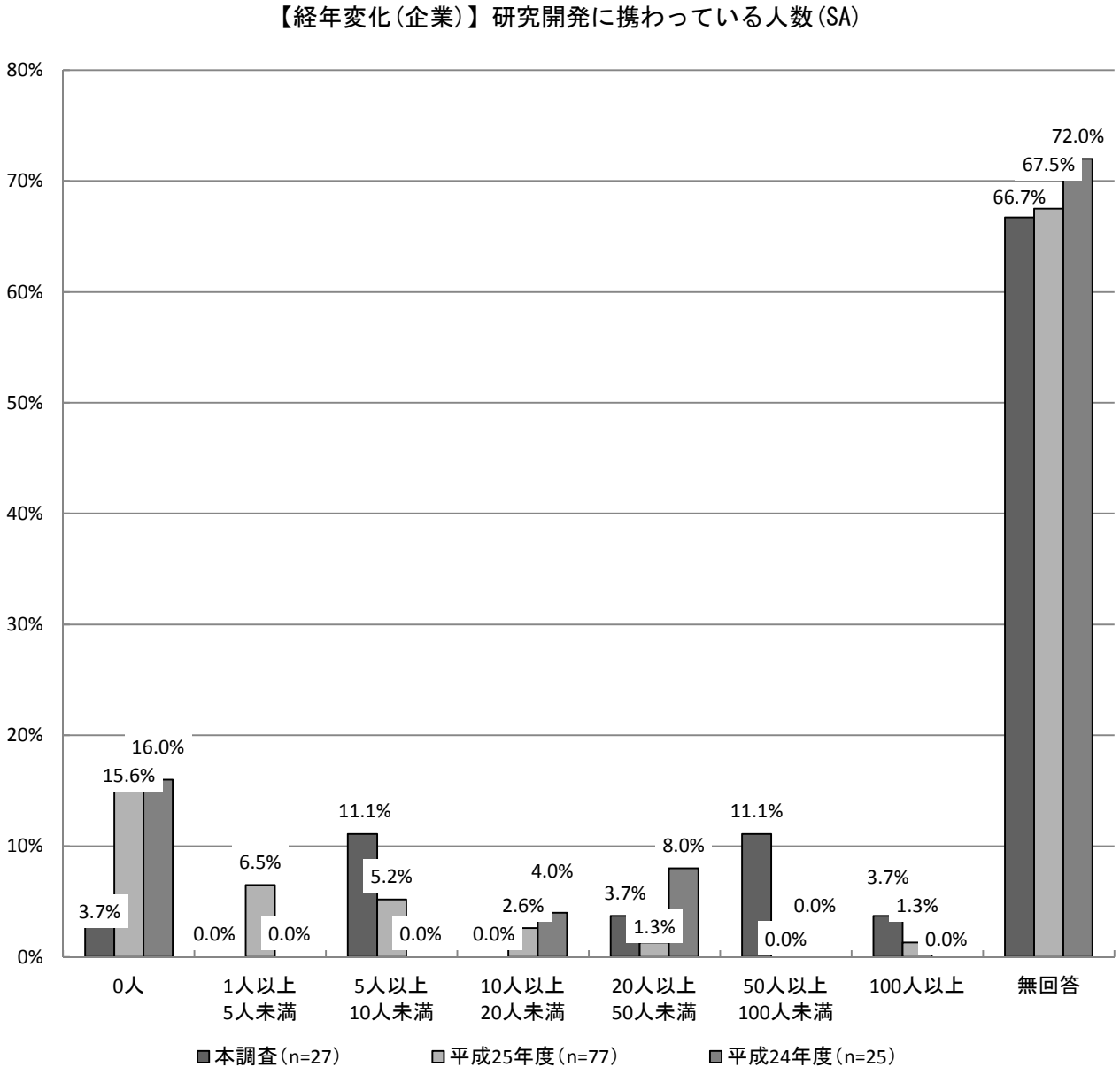
【経年変化(全体)】

全体の経年変化を見ると、「1 人以上 5 人未満」、「10 人以上 20 人未満」、「50 人以上 100 人未満」が増加している。



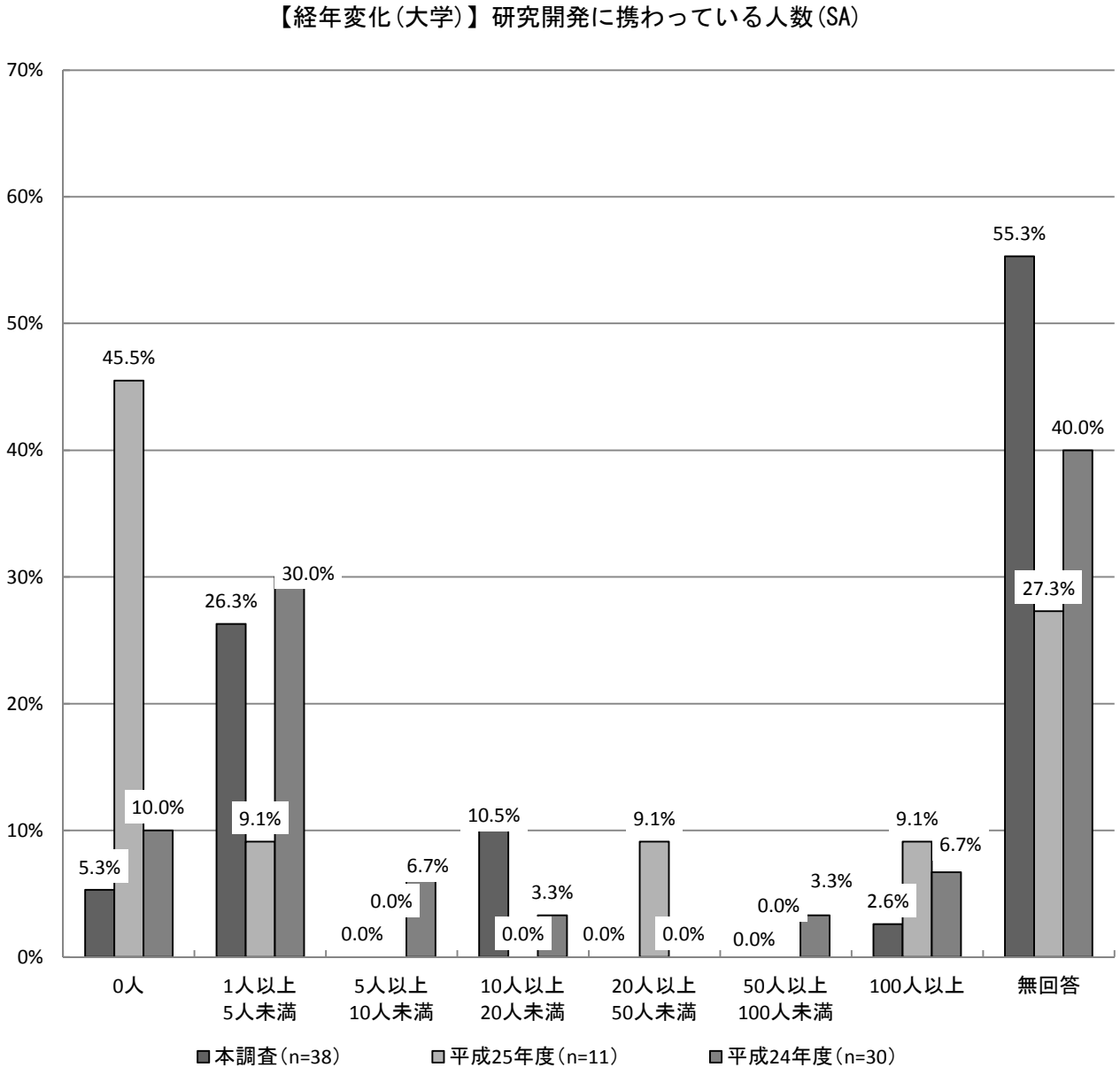
【経年変化(企業)】

企業の経年変化を見ると、「0 人」、「10 人以上 20 人未満」との回答が減少傾向にあり、「5 人以上 10 人未満」、「50 人以上 100 人未満」、「100 人以上」との回答に増加傾向がみられるため、小規模の研究開発と大規模の研究開発の 2 極化していると考えられる。



【経年変化(大学)】

大学の経年変化を見ると、小規模の「1 人以上 5 人未満」、中規模の「10 人以上 20 人未満」が増加しており、大規模の「100 人以上」が減少していることから、小規模や中規模での研究開発に取り組んでいることが分かる。



(2)年間の研究開発費【A-問7】

【本調査】

全体では、「1,000万円未満」が11.5%で最も多い。

企業では、「1億円以上10億円未満」が18.5%となっており、大学では、「1,000万円未満」が28.9%で最も多くなっている。

【経年変化】

全体では、「10億円以上100億円未満」が減少しており、「なし」及び「1,000万円未満」～「1億円以上10億円未満」の範囲で増加している。

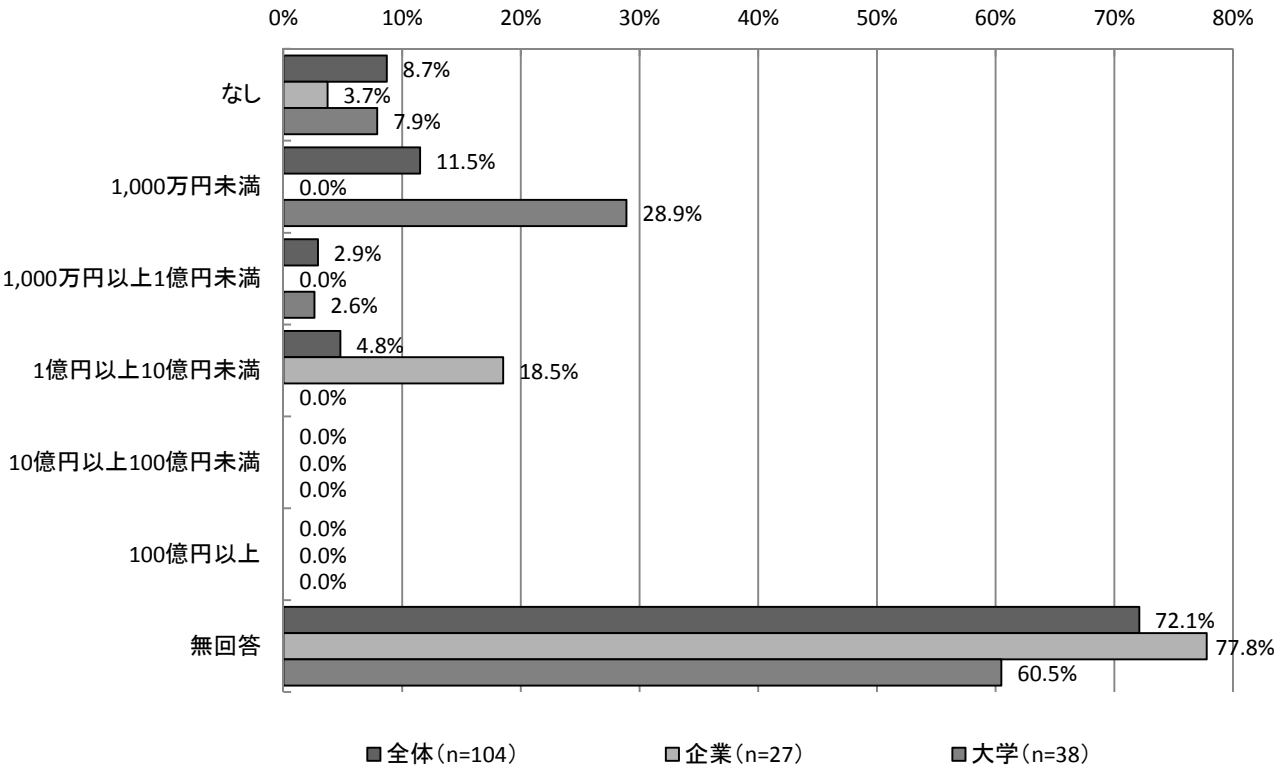
企業では、「1億円以上10億円未満」で増加しており、大学では「1,000万円未満」、「1,000万円以上1億円未満」で増加している。

【本調査】

年間の研究開発費について見ると、「1,000 万円未満」の 11.5%（12 件）が最も多い。

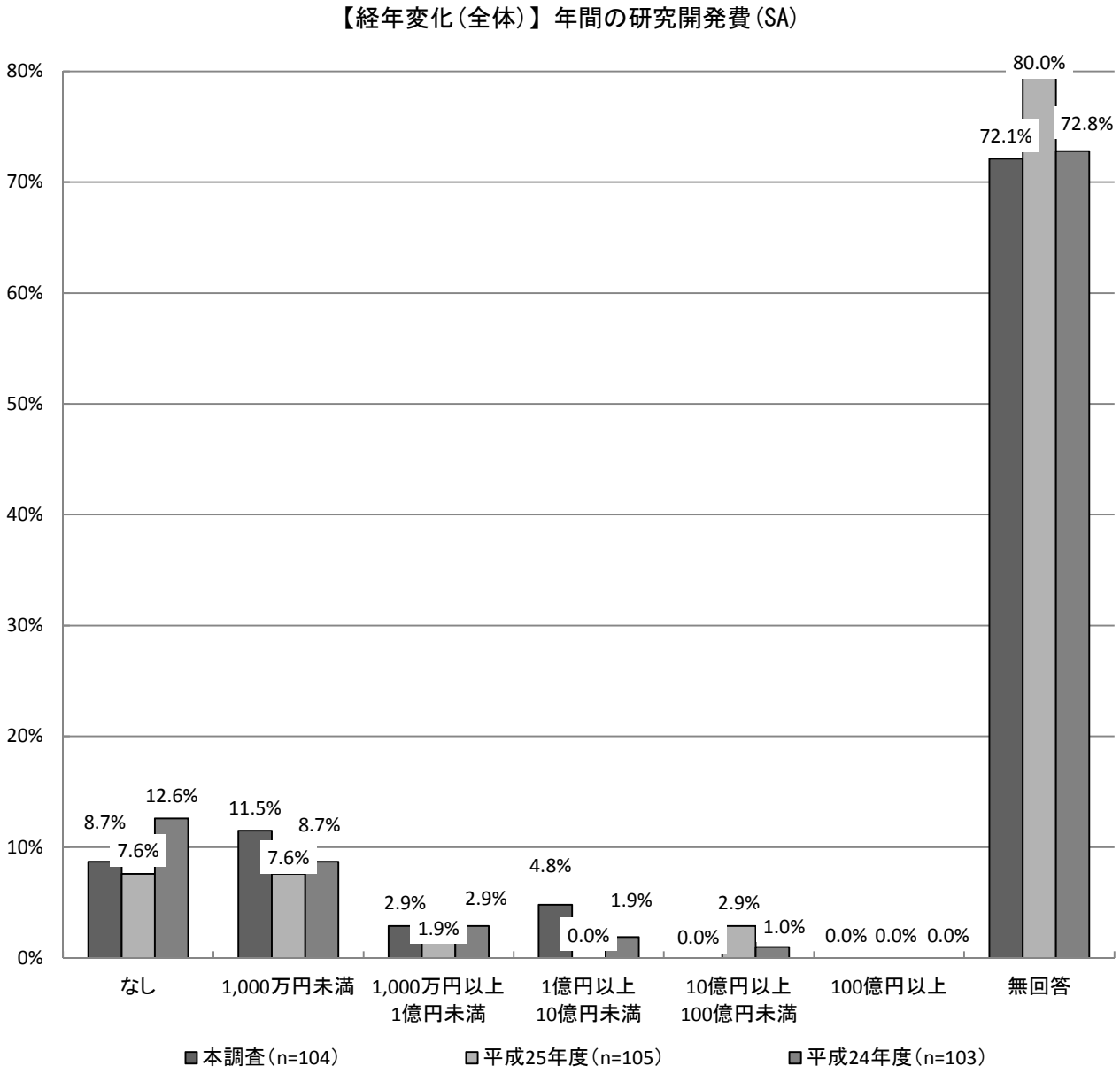
企業では、「1 億円以上 10 億円未満」の 18.5%（5 件）が最も多く、大学では、「1,000 万円未満」の 28.9%（11 件）が最も多い。

【本調査】年間の研究開発費(SA)



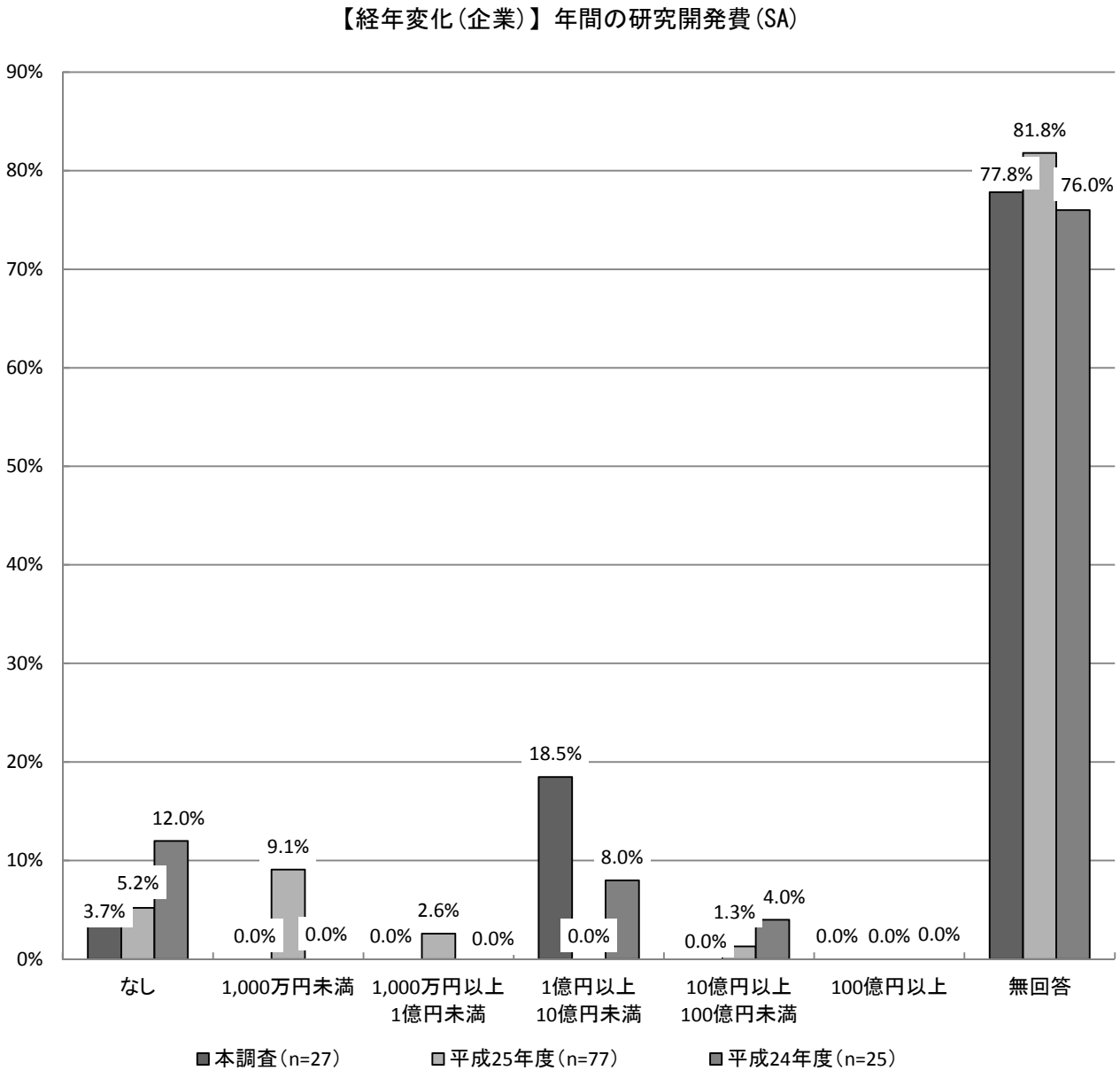
【経年変化(全体)】

全体の経年変化を見ると、年間の研究開発費が 10 億円未満で増加し、「10 億円以上 100 億円未満」で減少している。



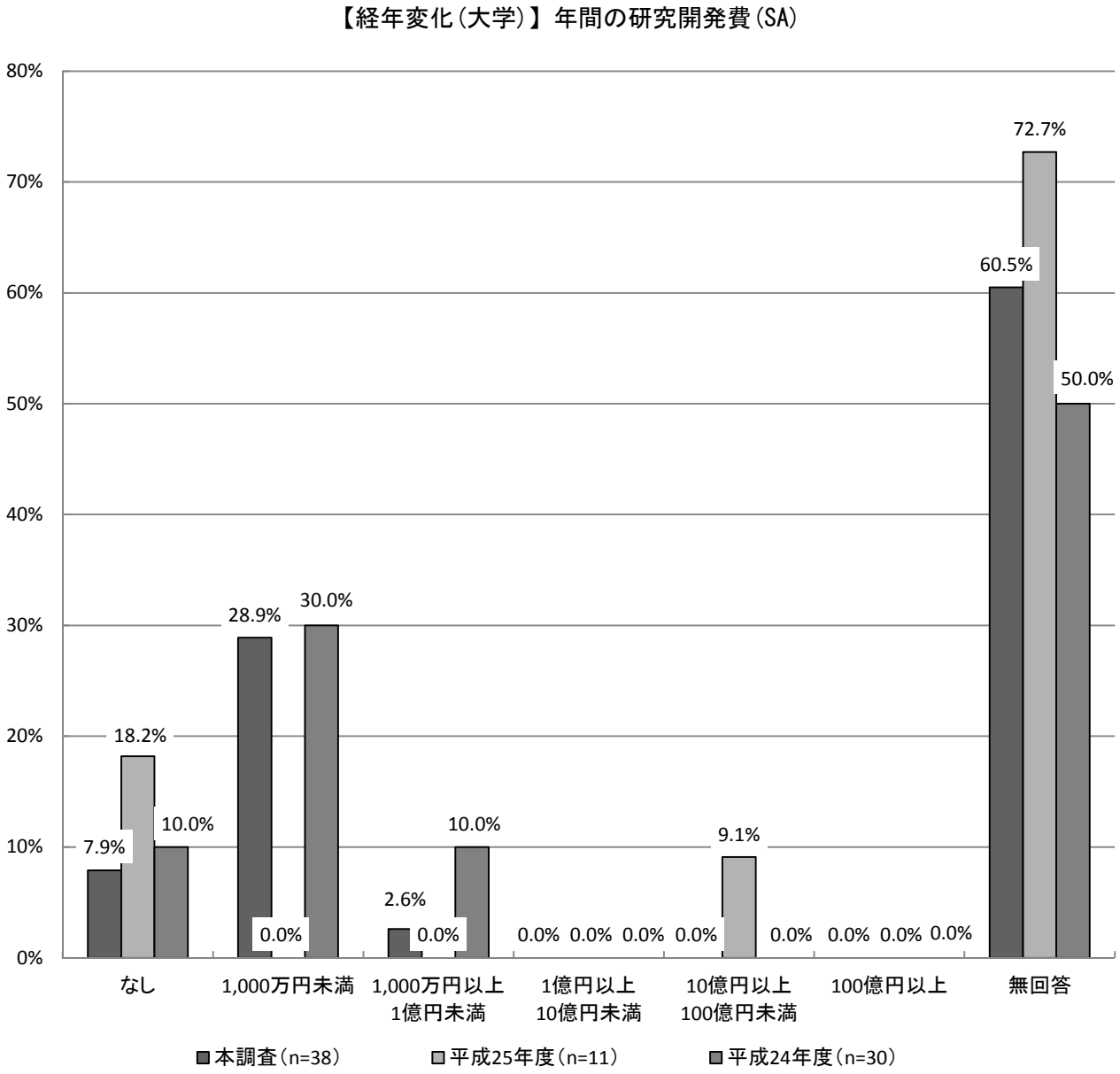
【経年変化(企業)】

企業の経年変化を見ると、「1 億円以上 10 億円未満」が増加しており、他の項目は減少している。



【経年変化(大学)】

大学の経年変化を見ると、「なし」、「10 億円以上 100 億円未満」が減少し、「1,000 万円未満」、「1,000 万円以上 1 億円未満」が増加している。

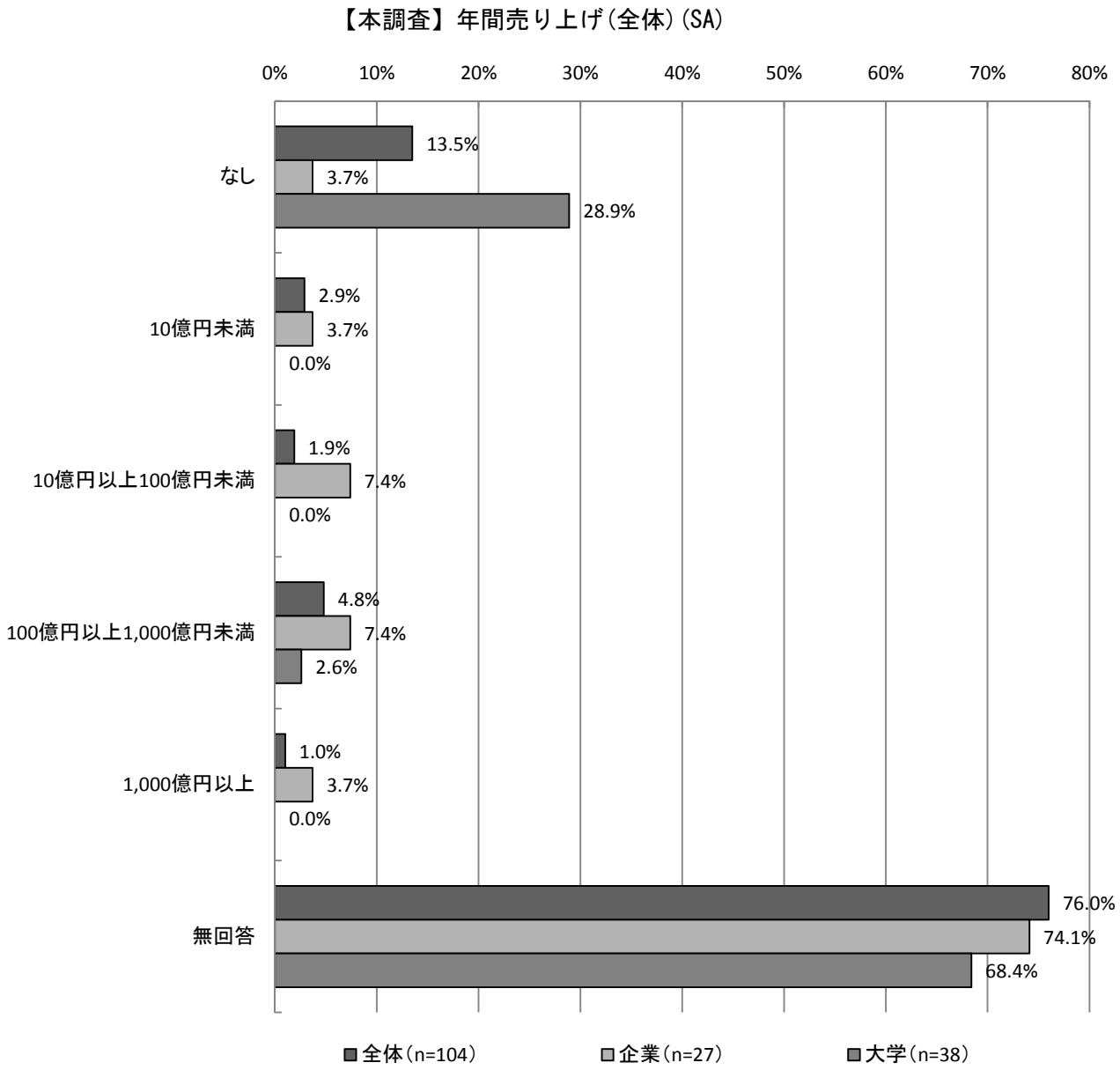


(3)年間売り上げ(全体) 【A-問 6.1】

【本調査】

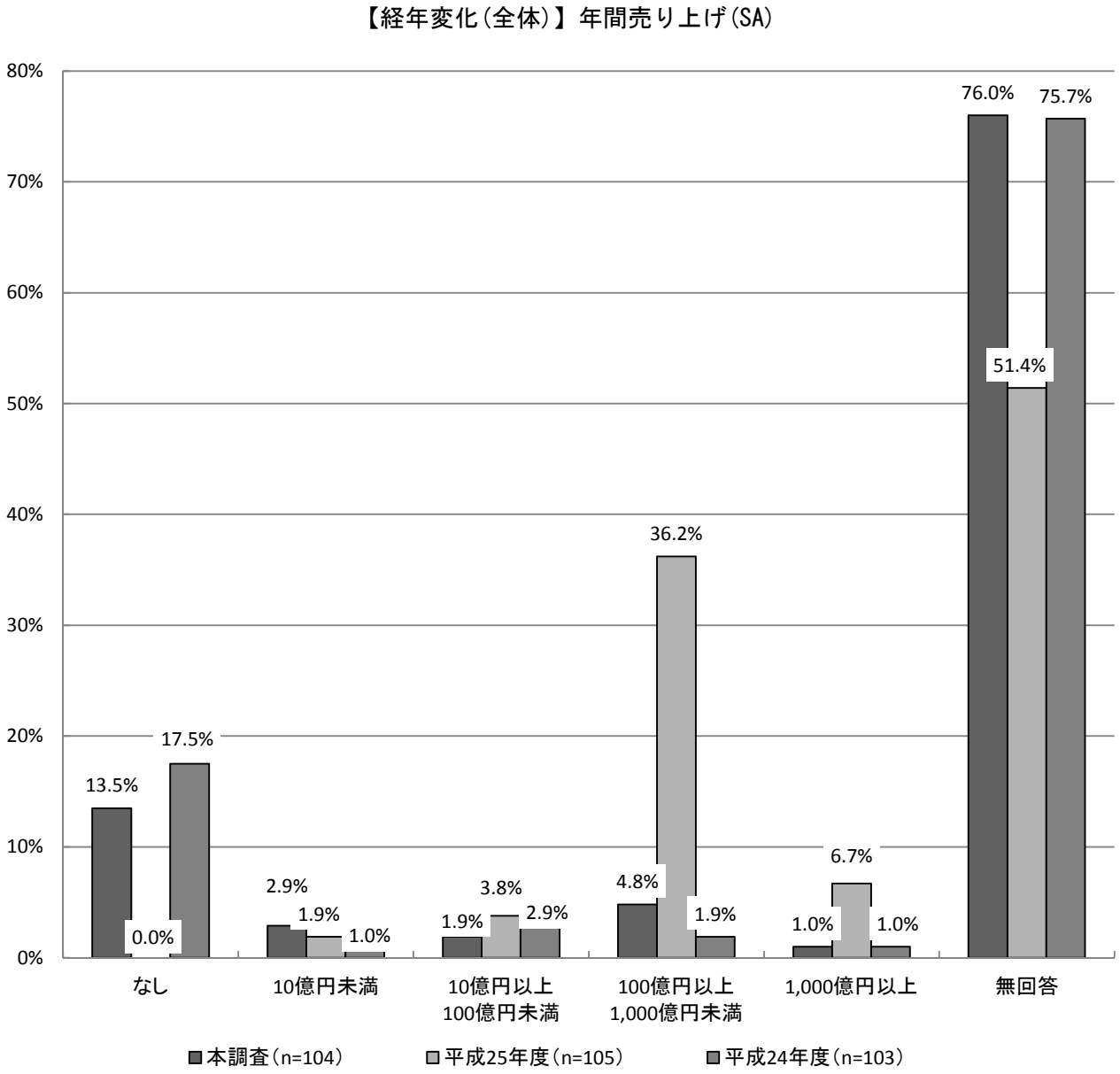
全体では、「なし」と回答した 13.5%（14 件）を除いて見ると、「100 億円以上 1,000 億円未満」が 4.8%（5 件）で最も多く、「10 億円未満」が 2.9%（3 件）で続いている。

企業では、「10 億円以上 100 億円未満」、「100 億円以上 1,000 億円未満」が 7.4%（2 件）で最も多く、大学では、「なし」を除くと「100 億円以上 1,000 億円未満」が 2.6%（1 件）となっている。



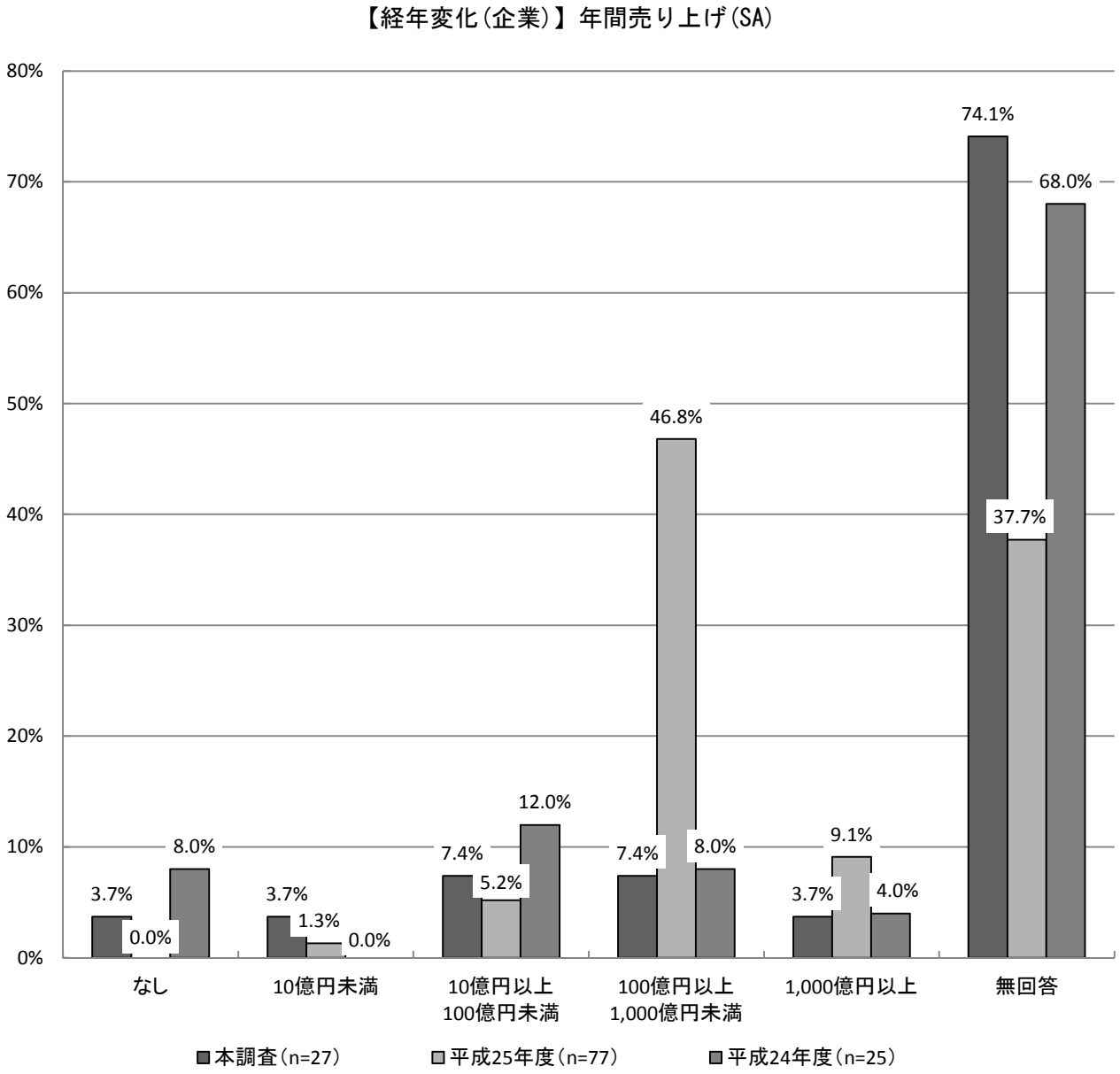
【経年変化(全体)】

全体の経年変化については、「なし」と回答したものを除いて見ると、昨年度と比較して、「10億円未満」を除くすべての項目で減少している。



【経年変化(企業)】

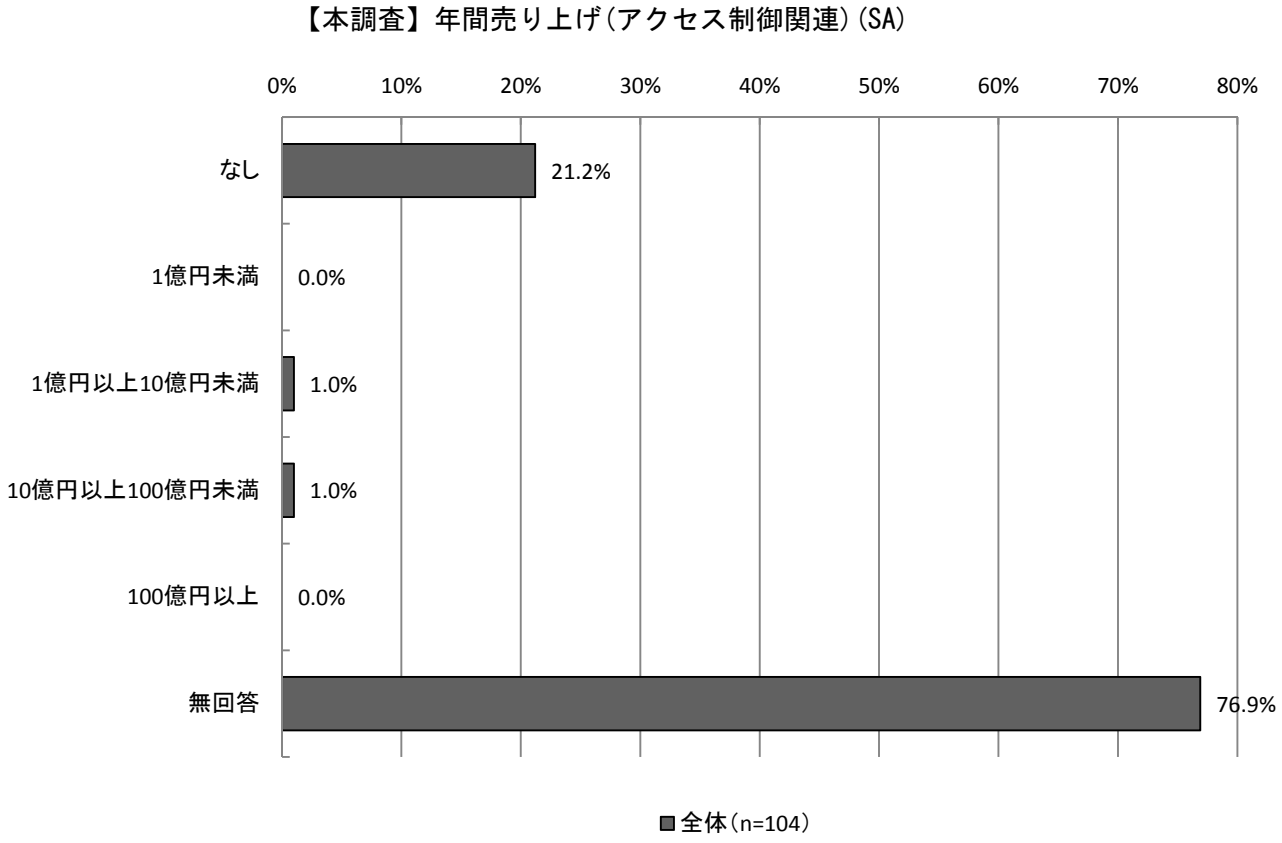
企業では、「なし」と回答したものを除いて見ると、昨年度と比較して、100 億円未満で増加し、100 億円以上で減少している。



(4)年間売り上げ(アクセス制御関連) 【A-問 6.2】

【本調査】

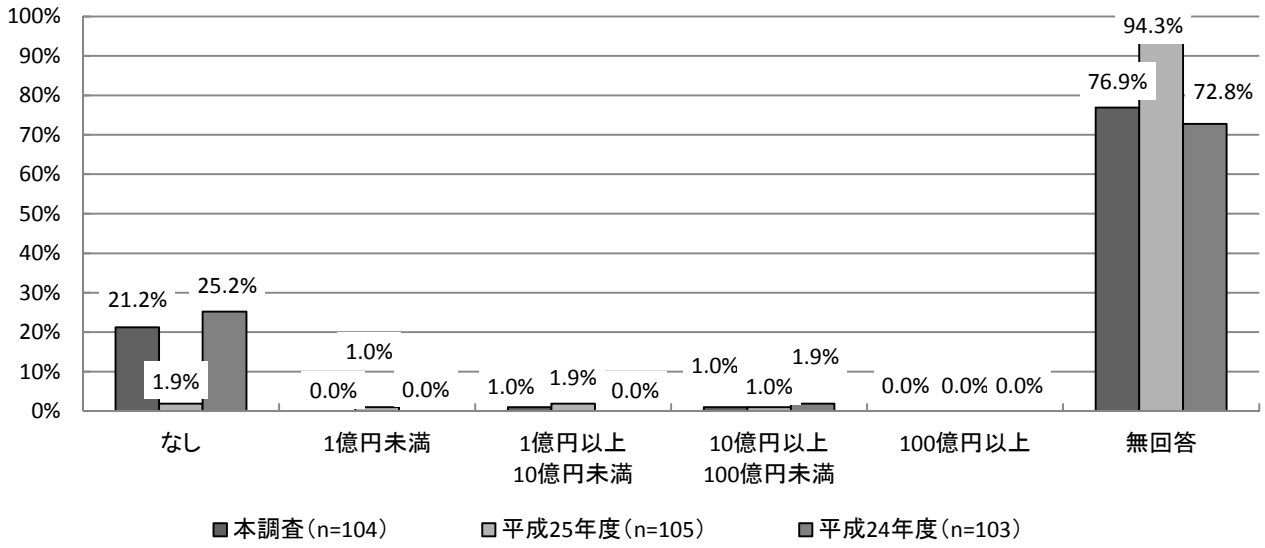
アクセス制御関連の年間の売り上げについては、「なし」と回答した 21.2%（22 件）を除いて見ると、「1 億円以上 10 億円未満」、「10 億円以上 100 億円未満」が 1.0%（1 件）となっている。



【経年変化(全体)】

全体の経年変化を見ると、「なし」と回答したものを除き、売り上げがある場合について見ると、「1 億円以上 10 億円未満」が昨年度と比較して減少している。

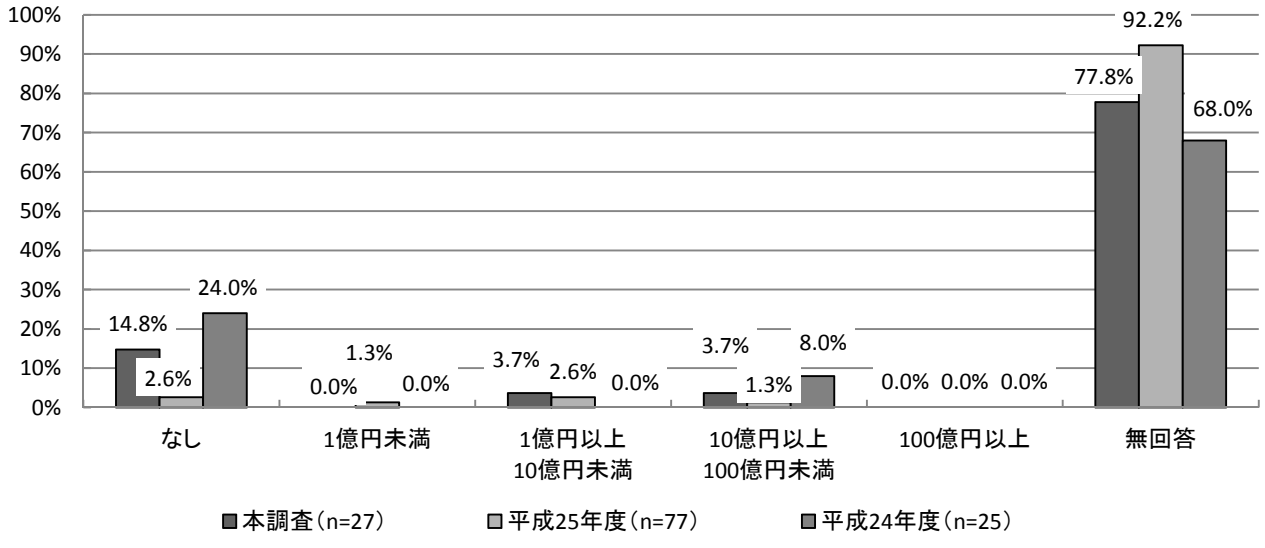
【経年変化(全体)】年間売り上げ(アクセス制御関連)(SA)



【経年変化(企業)】

企業について経年変化を見ると、「なし」と回答したものを除き、売り上げがある場合について見ると、「1 億円以上 10 億円未満」、「10 億円以上 100 億円未満」が昨年度と比較して増加している。

【経年変化(企業)】年間売り上げ(アクセス制御関連)(SA)



3.1.2. 現在、取り組んでいる分野【A-問1】

【本調査】

全体では、「取組無し」と回答のあった58.7%を除くと、「暗号技術」が17.3%で最も多く、「ネットワークセキュリティ」が16.3%、「クラウドコンピューティング」が15.4%で続いている。

企業では、「取組無し」と回答のあった63.0%を除くと、「ネットワークセキュリティ」、「ウイルス対策」が22.2%で最も多く、大学では、「取組無し」と回答のあった47.4%を除くと、「暗号技術」が28.9%で最も多くなっている。

【経年変化】

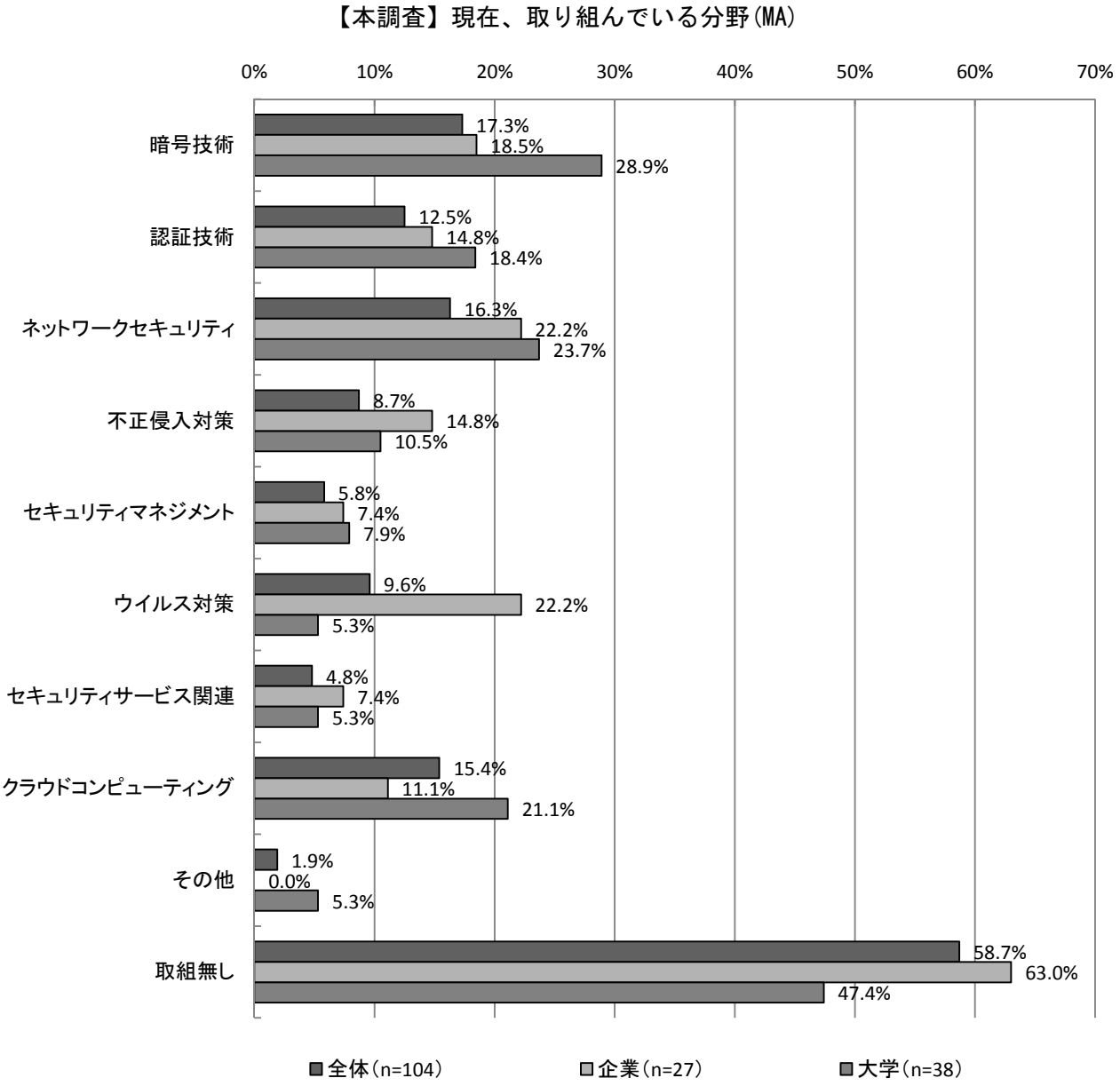
全体では、「暗号技術」、「認証技術」、「クラウドコンピューティング」が増加している。

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」を除く項目で増加しており、大学では、「暗号技術」、「認証技術」で増加している。

【本調査】

現在、取り組んでいる分野については、全体では「取組無し」と回答のあった 58.7%（61 件）を除くと、「暗号技術」が 17.3%（18 件）で最も多く、「ネットワークセキュリティ」が 16.3%（17 件）で続いている。

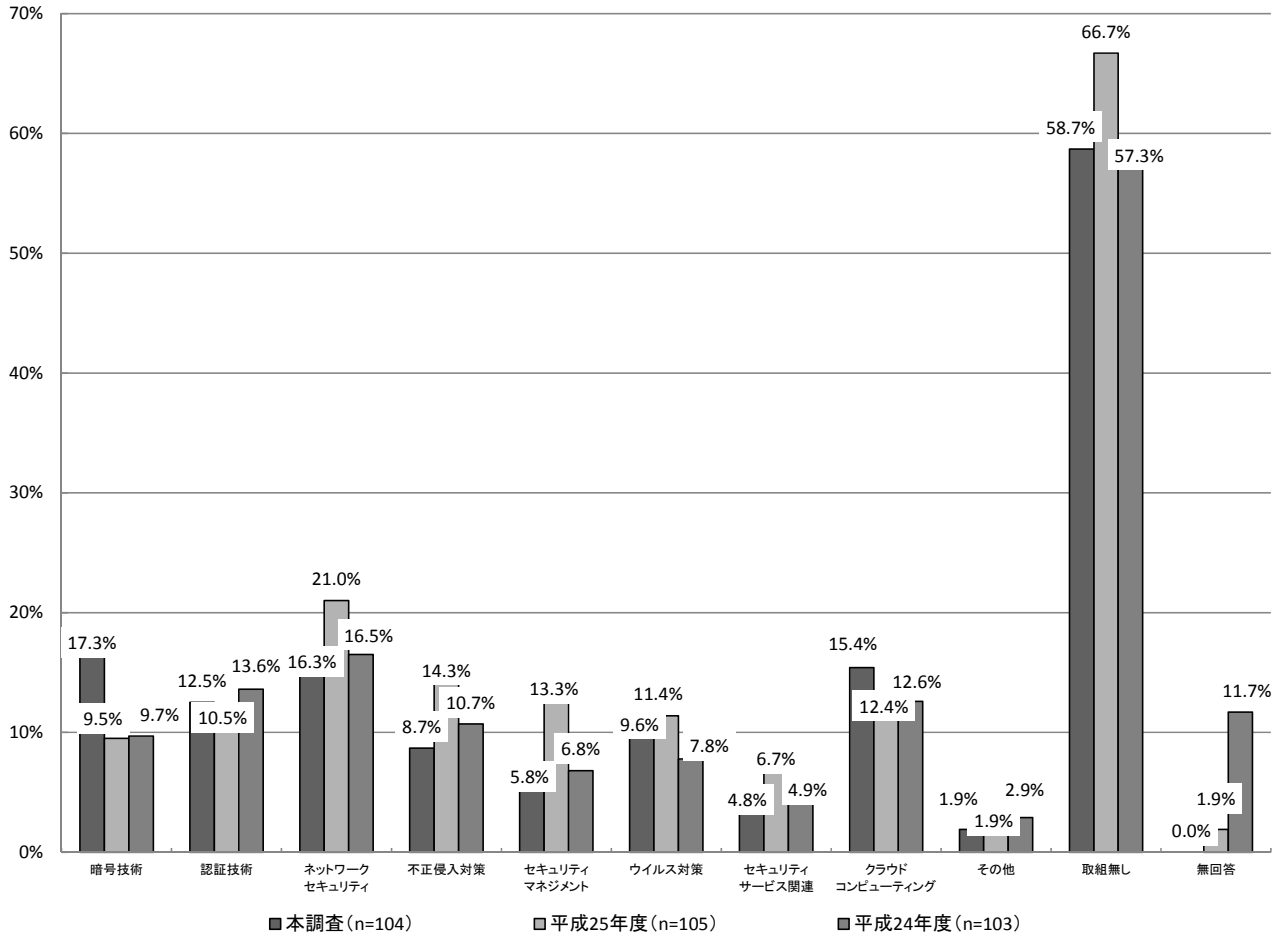
企業では、「取組無し」と回答のあった 63.0%（17 件）を除くと、「ネットワークセキュリティ」、「ウイルス対策」が 22.2%（6 件）で最も多く、大学では、「取組無し」と回答のあった 47.4%（18 件）を除くと、「暗号技術」が 28.9%（11 件）で最も多くなっている。



【経年変化(全体)】

全体の経年変化については、「取組無し」との回答を除くと、昨年度と比較して「暗号技術」、「認証技術」、「クラウドコンピューティング」が増加している。

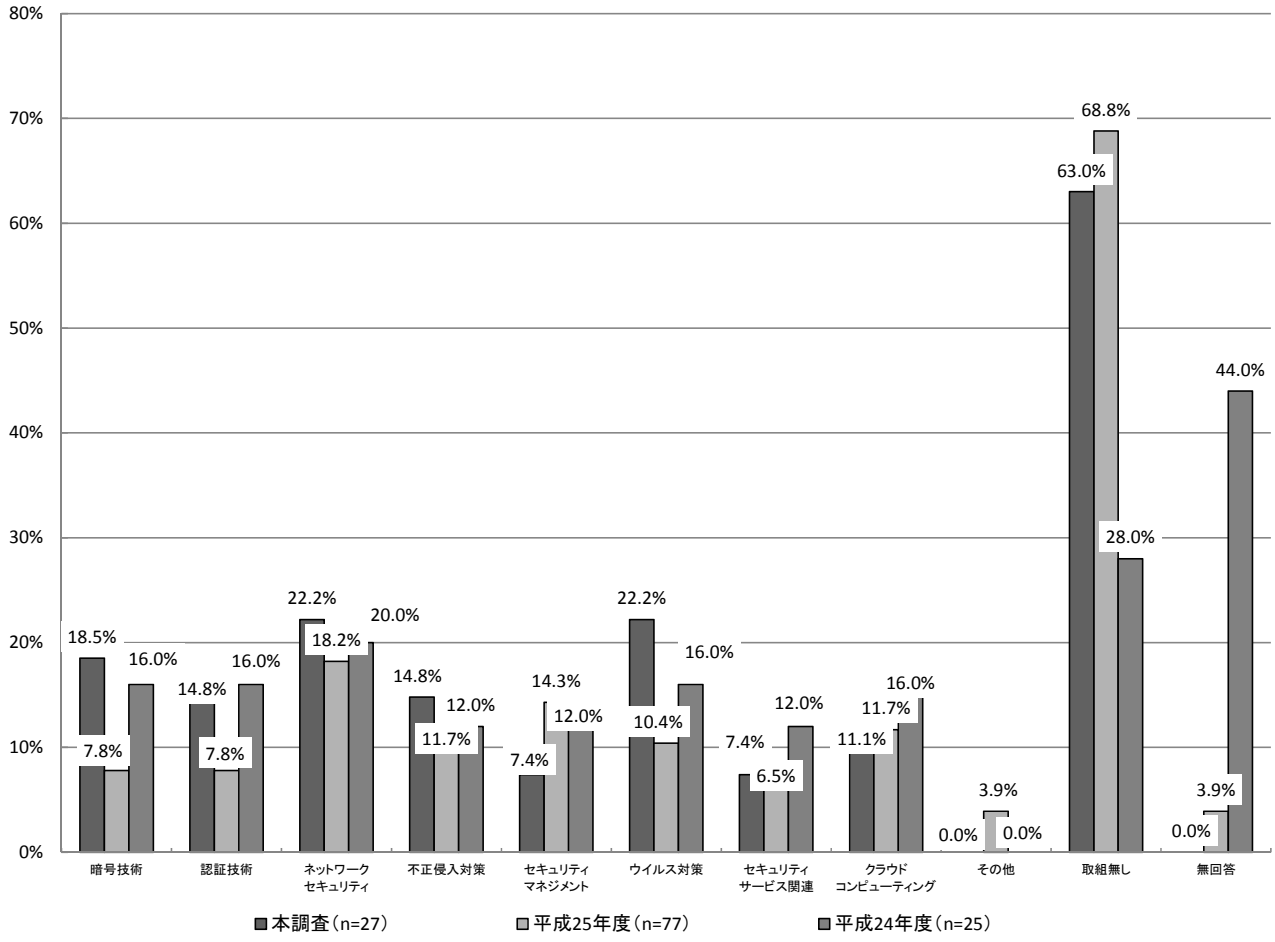
【経年変化(全体)】現在、取り組んでいる分野(MA)



【経年変化(企業)】

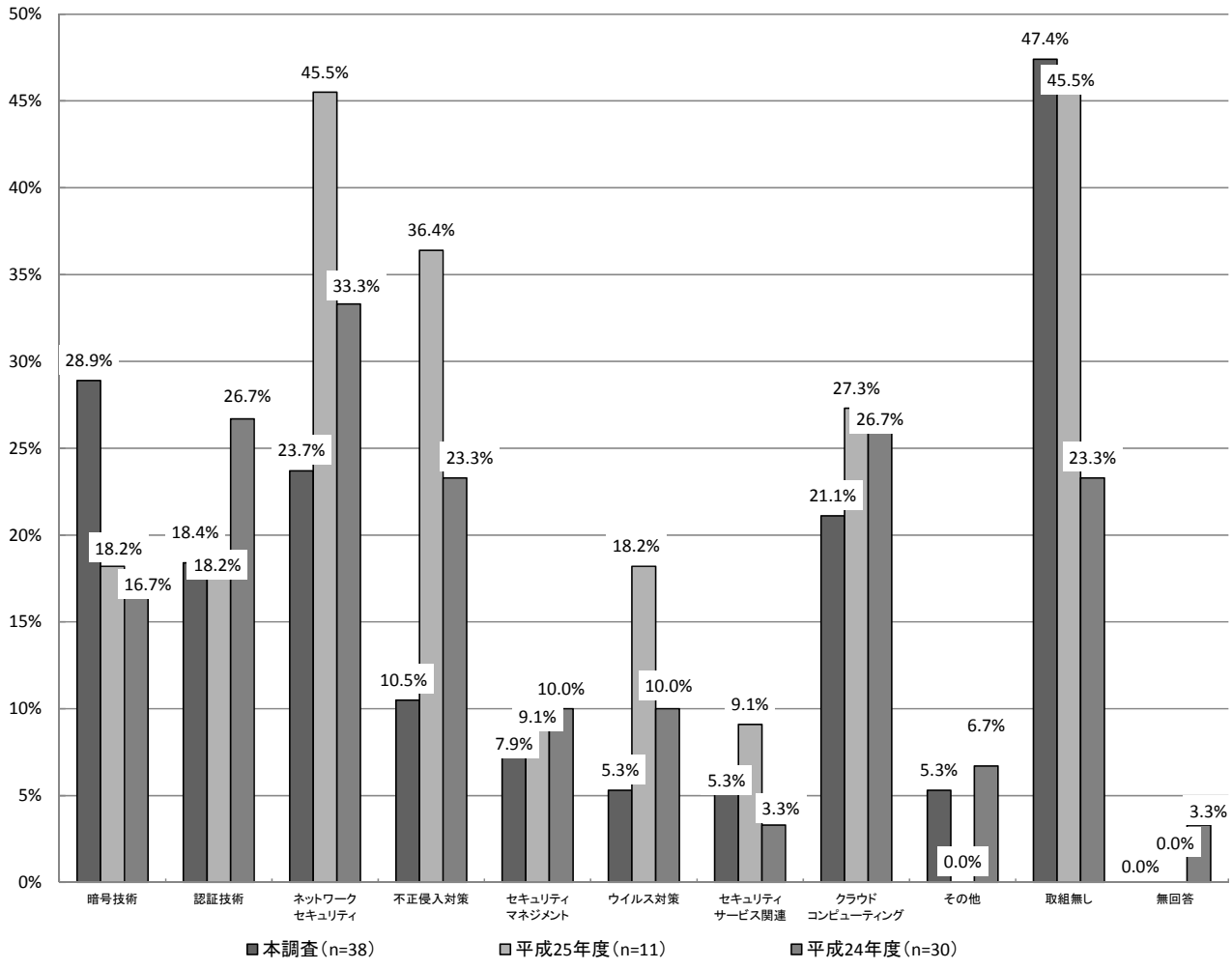
企業の経年変化を見ると、「取組無し」と回答したものを除くと、「セキュリティマネジメント」、「クラウドコンピューティング」を除く項目で昨年度と比較して増加している。

【経年変化(企業)】現在、取り組んでいる分野(MA)



【経年変化(大学)】

大学の経年変化を見ると、「取組無し」と回答したものを除くと、「暗号技術」、「認証技術」が増加している。



3.1.3. 今後、取り組んでいく分野【A-問2】

【本調査】

全体では、「取組無し」と回答があった50.0%を除くと、「暗号技術」、「ネットワークセキュリティ」が15.4%で最も多く、「クラウドコンピューティング」が14.4%で続いている。

企業では、「取組無し」と回答があった59.3%を除くと、「ネットワークセキュリティ」、「ウイルス対策」が18.5%で最も多く、大学では、「取組無し」と回答があった39.5%を除くと、「暗号技術」が26.3%で最も多くなっている。

【経年変化】

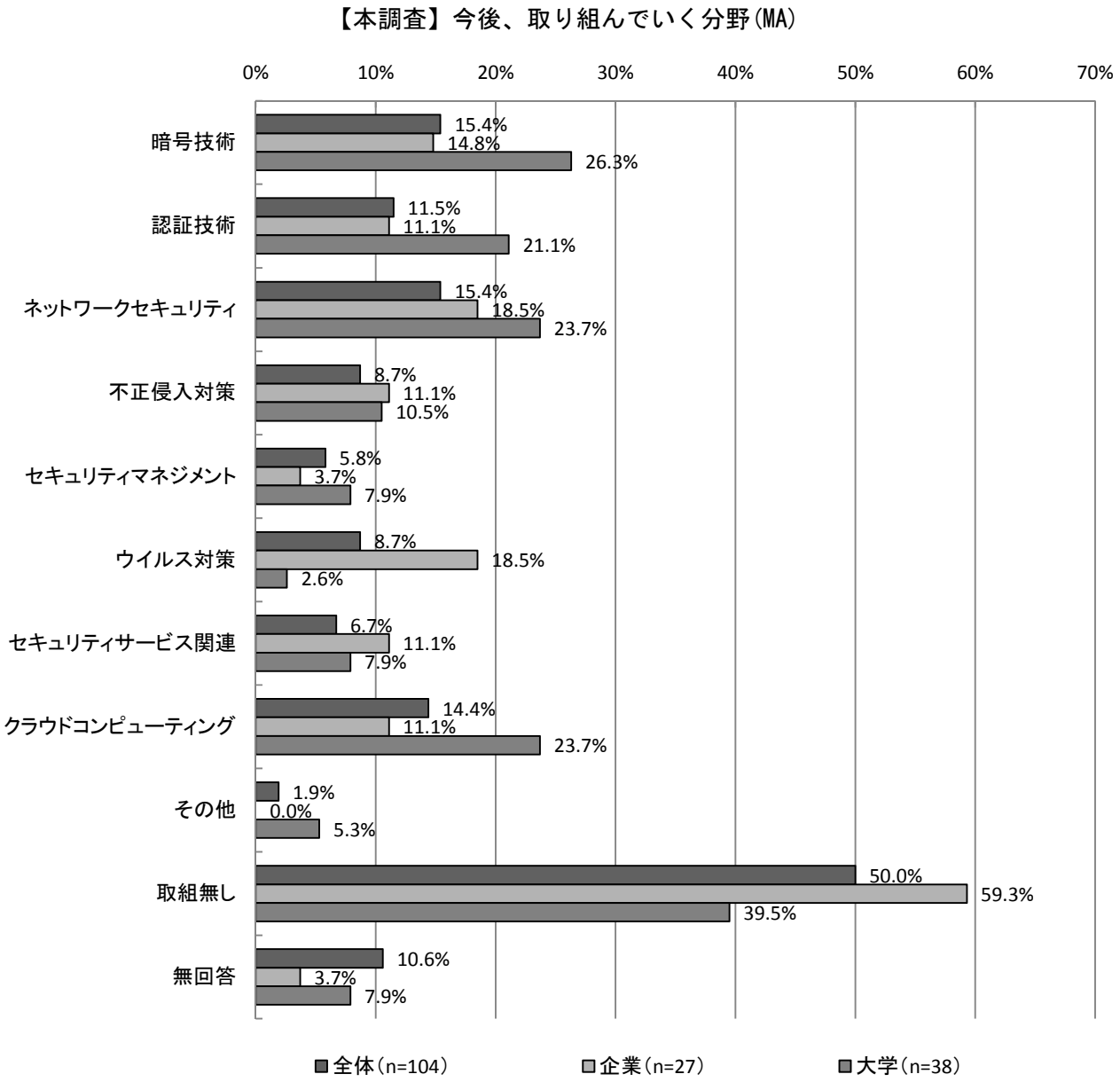
全体では、「セキュリティマネジメント」、「セキュリティサービス関連」、「クラウドコンピューティング」を除くすべての分野で増加している。

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」を除くすべての分野で増加しており、大学では、「暗号技術」が増加している。

【本調査】

全体では、「取組無し」と回答があった 50.0%（52 件）を除くと、「暗号技術」、「ネットワークセキュリティ」が 15.4%（16 件）で最も多く、「クラウドコンピューティング」が 14.4%（15 件）で続いている。

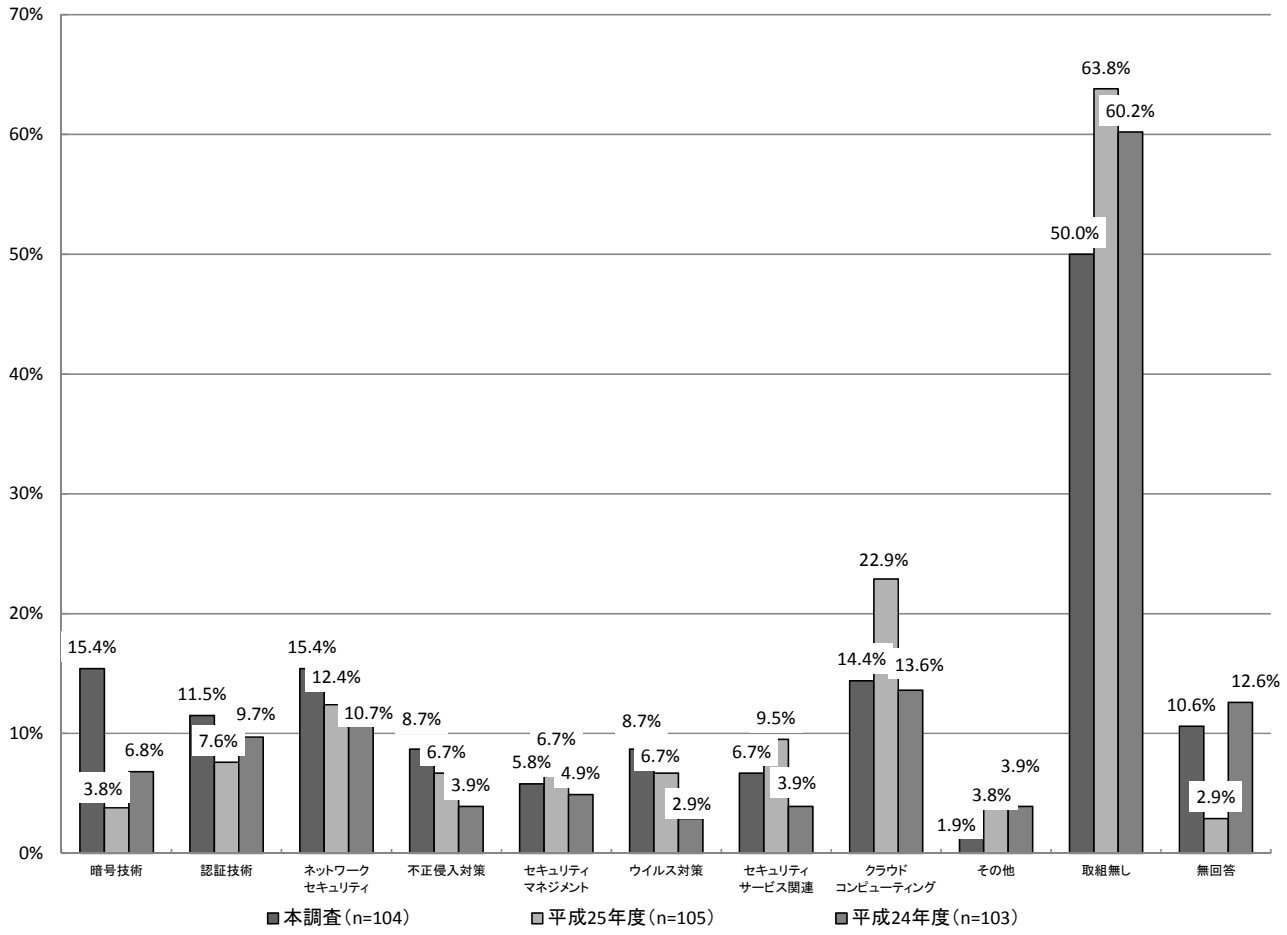
企業では、「取組無し」と回答があった 59.3%（16 件）を除くと、「ネットワークセキュリティ」、「ウイルス対策」が 18.5%（5 件）で最も多く、大学では、「取組無し」と回答があった 39.5%（15 件）を除くと、「暗号技術」が 26.3%（10 件）で最も多くなっている。



【経年変化(全体)】

全体の経年変化については、「取組無し」と回答したものを除くと、「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」を除くすべての分野で増加している。

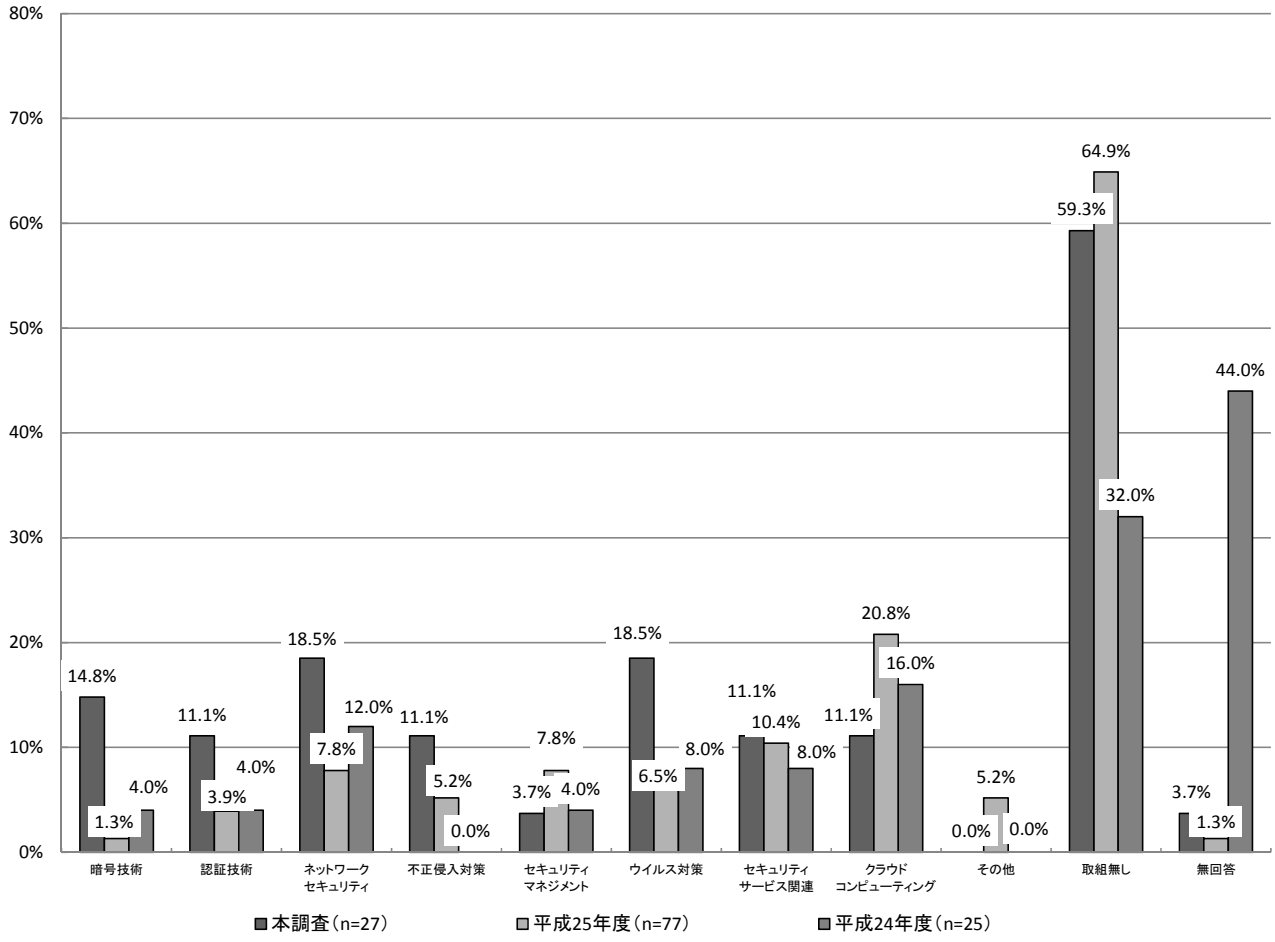
【経年変化(全体)】今後、取り組んでいく分野(MA)



【経年変化(企業)】

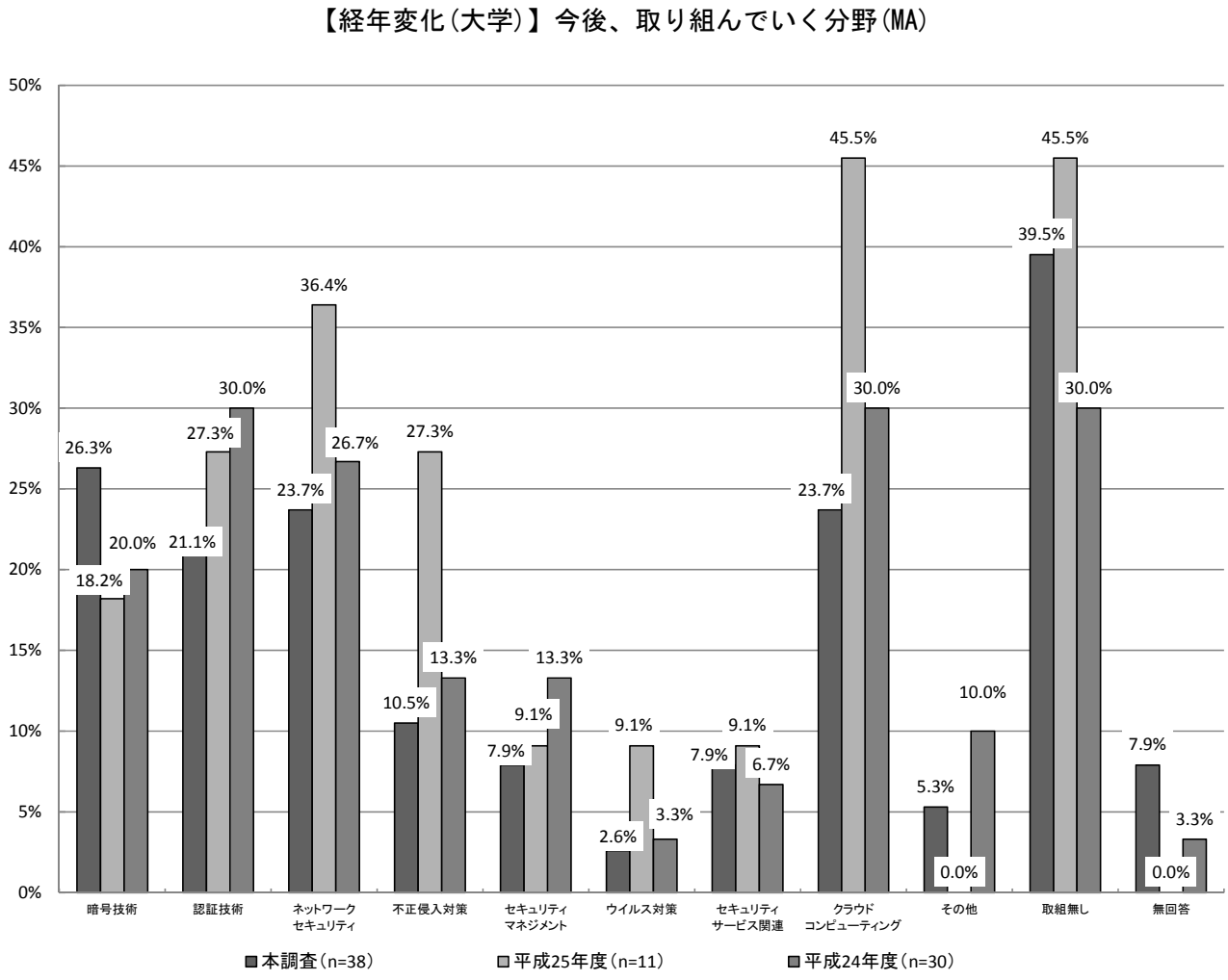
企業の経年変化を見ると、「取組無し」と回答したものを除くと、「セキュリティマネジメント」、「クラウドコンピューティング」を除くすべての分野で増加している。

【経年変化(企業)】今後、取り組んでいく分野(MA)



【経年変化(大学)】

大学の経年変化を見ると、「取組無し」と回答したものを除くと、「暗号技術」が増加している。



3.1.4. 今後、最も力を入れていく分野【A-問3】

【本調査】

全体では、「暗号技術」が22.0%で最も多く、「ネットワークセキュリティ」が19.5%、「クラウドコンピューティング」が17.1%で続いている。

企業では、「暗号技術」、「ネットワークセキュリティ」が30.0%で最も多く、大学では、「暗号技術」が25.0%で最も多くなっている。

【経年変化】

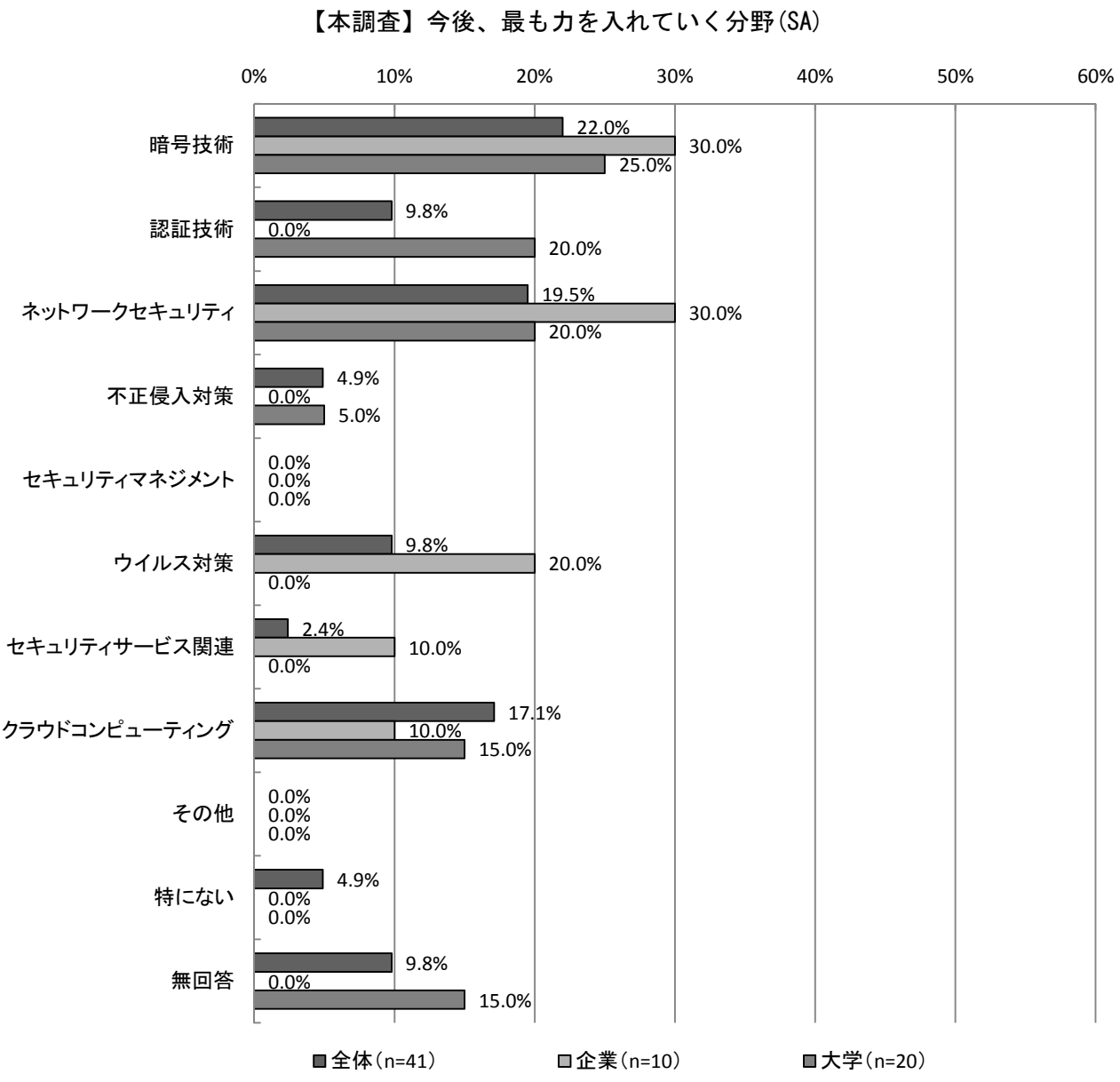
全体では、「セキュリティマネジメント」、「セキュリティサービス関連」を除くすべての分野で増加している。

企業では、「暗号技術」、「ネットワークセキュリティ」、「ウイルス対策」、「セキュリティサービス関連」が増加しており、大学では、「暗号技術」、「認証技術」、「ネットワークセキュリティ」、「クラウドコンピューティング」が増加している。

【本調査】

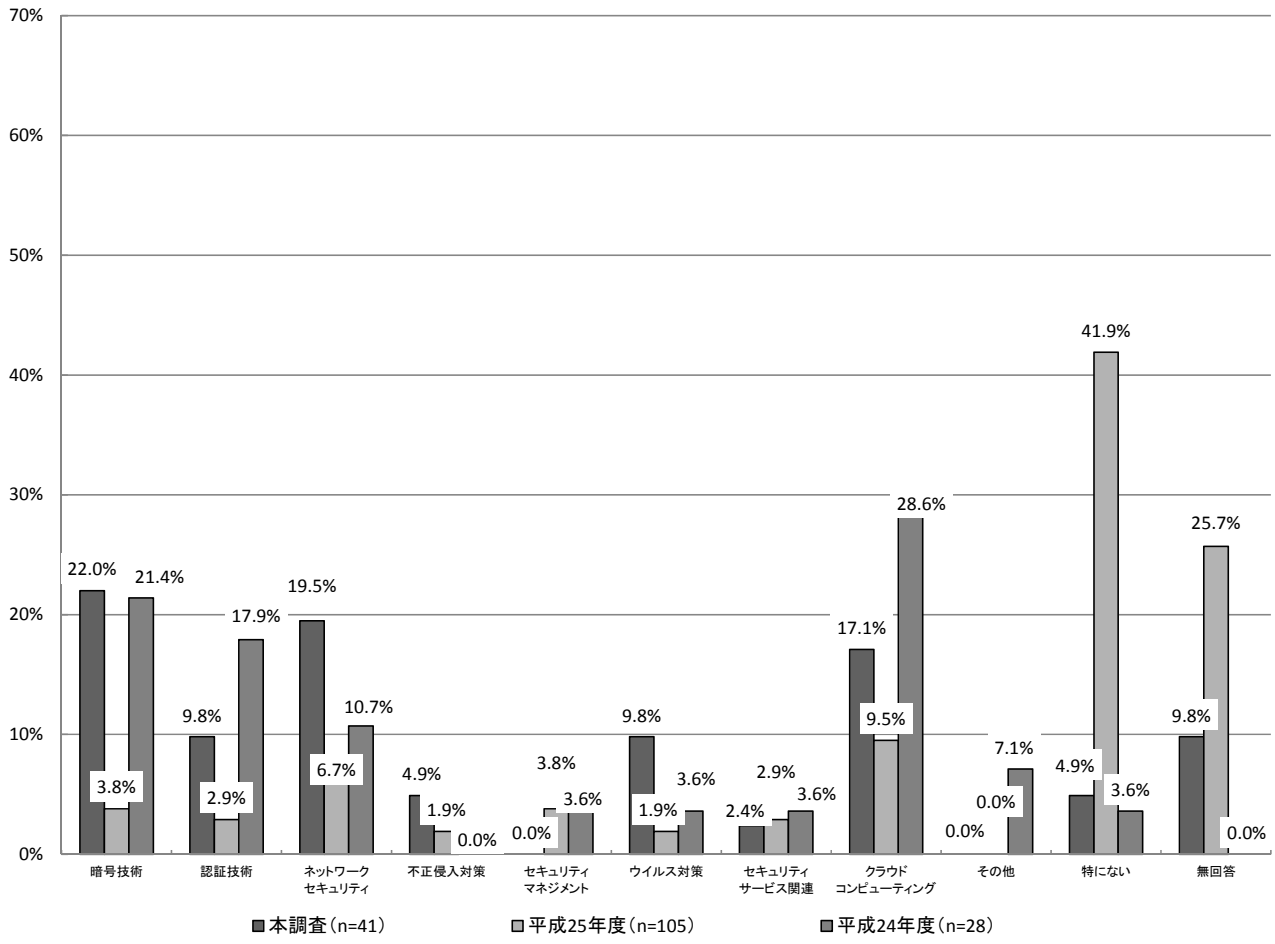
全体では、「暗号技術」が 22.0%（9 件）で最も多く、「ネットワークセキュリティ」が 19.5%（8 件）で続いている。

企業では、「暗号技術」、「ネットワークセキュリティ」が 30.0%（3 件）で最も多く、大学では、「暗号技術」が 25.0%（5 件）が最も多くなっている。



【経年変化(全体)】

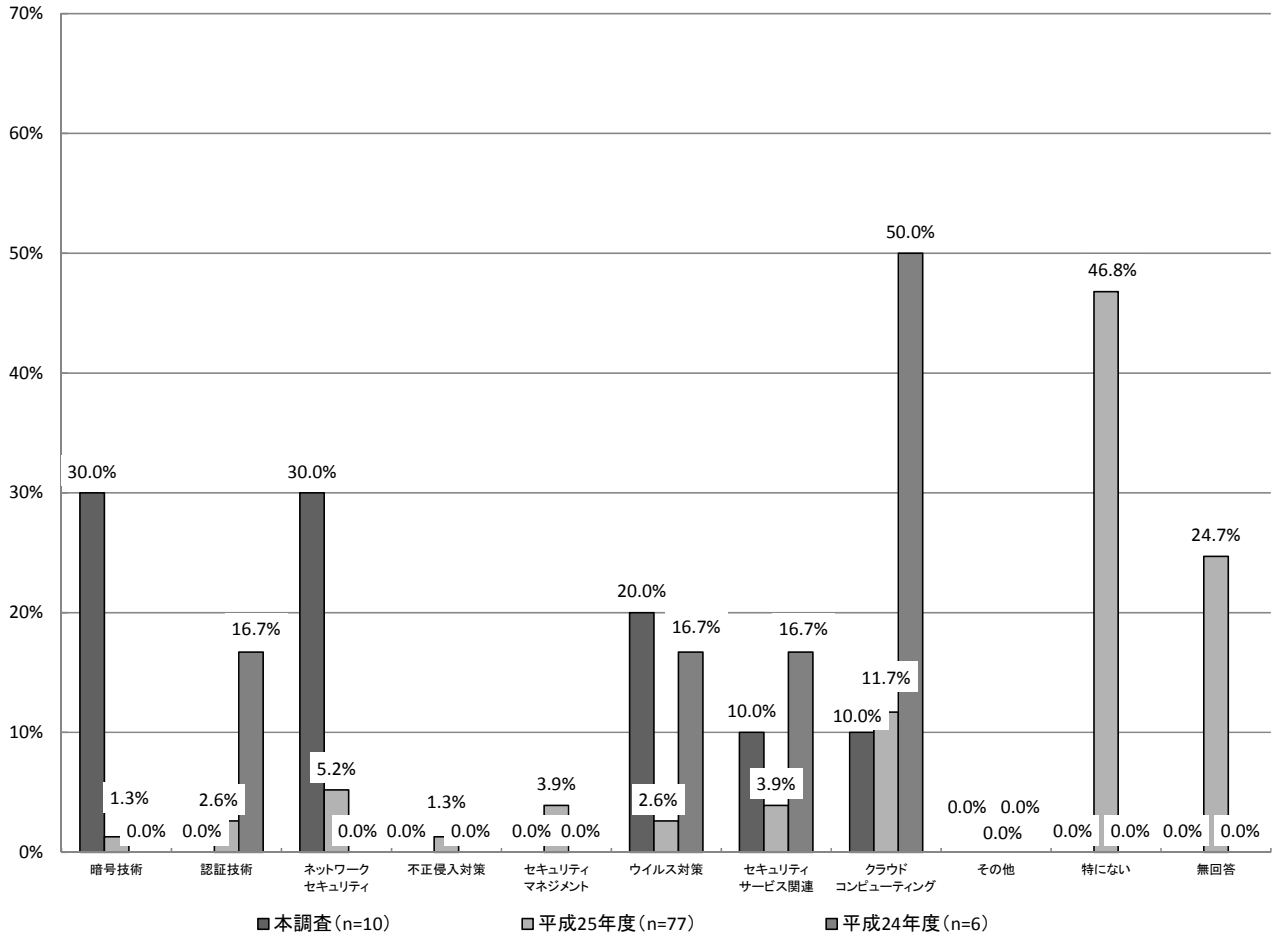
全体の経年変化を見ると、「セキュリティマネジメント」、「セキュリティサービス関連」を除くすべての分野で増加している。



【経年変化(企業)】

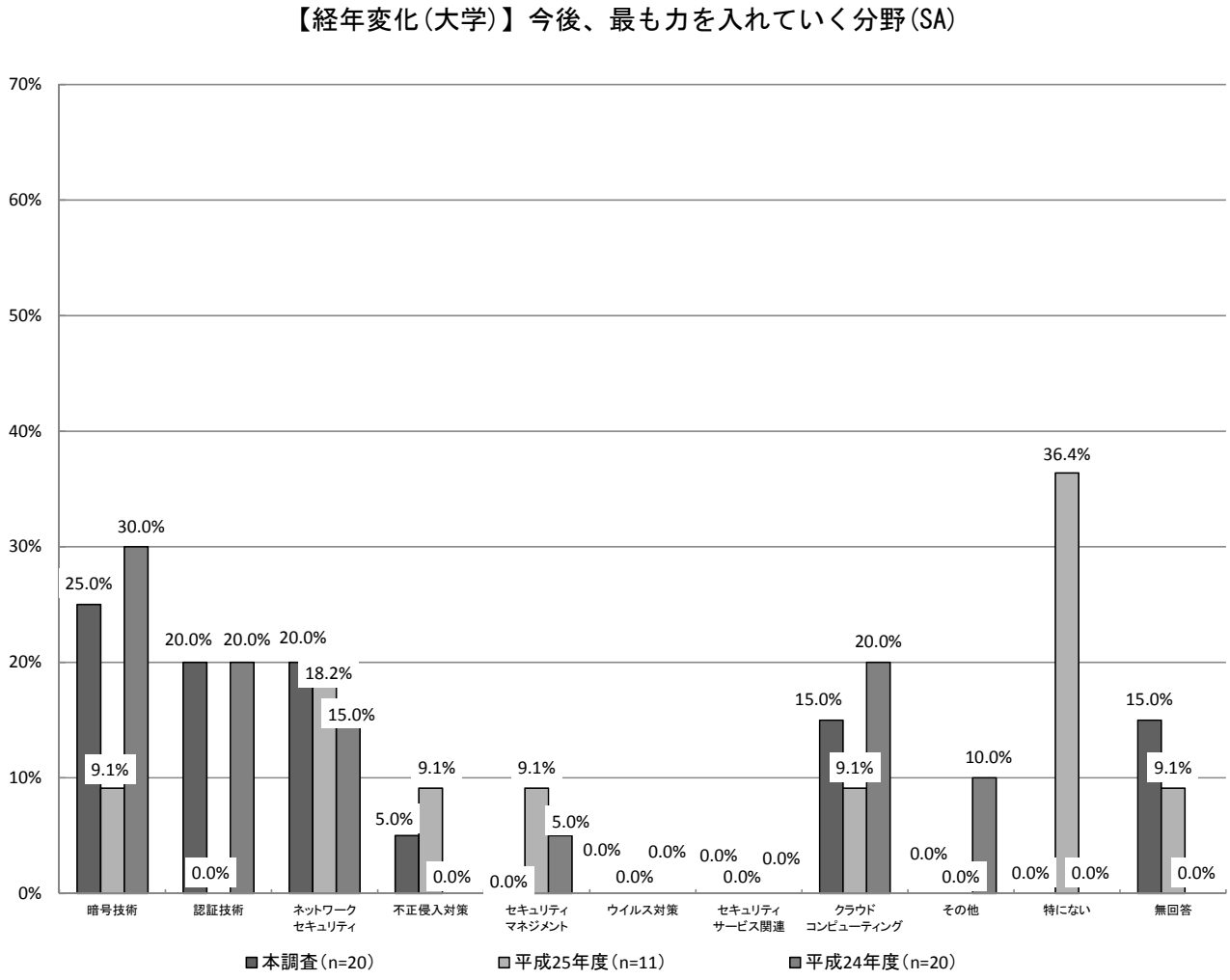
企業の経年変化を見ると、「暗号技術」、「ネットワークセキュリティ」、「ウイルス対策」、「セキュリティサービス関連」が増加している。

【経年変化(企業)】今後、最も力を入れていく分野(SA)



【経年変化(大学)】

大学の経年変化を見ると、「暗号技術」、「認証技術」、「ネットワークセキュリティ」、「クラウドコンピューティング」が増加している。



3.1.5. 現在、実用化(製品化)されているアクセス制御機能【A-問4】

【本調査】

全体では、「特になし」と回答のあった50.0%を除くと、「暗号技術」が5.8%で最も多く、「ネットワークセキュリティ」が4.8%で続いている。

企業では、「特になし」と回答のあった37.0%を除くと、「暗号技術」が14.8%で最も多く、大学では、「特になし」と回答のあった57.9%を除くと、「暗号技術」が5.3%で最も多くなっている。

【経年変化】

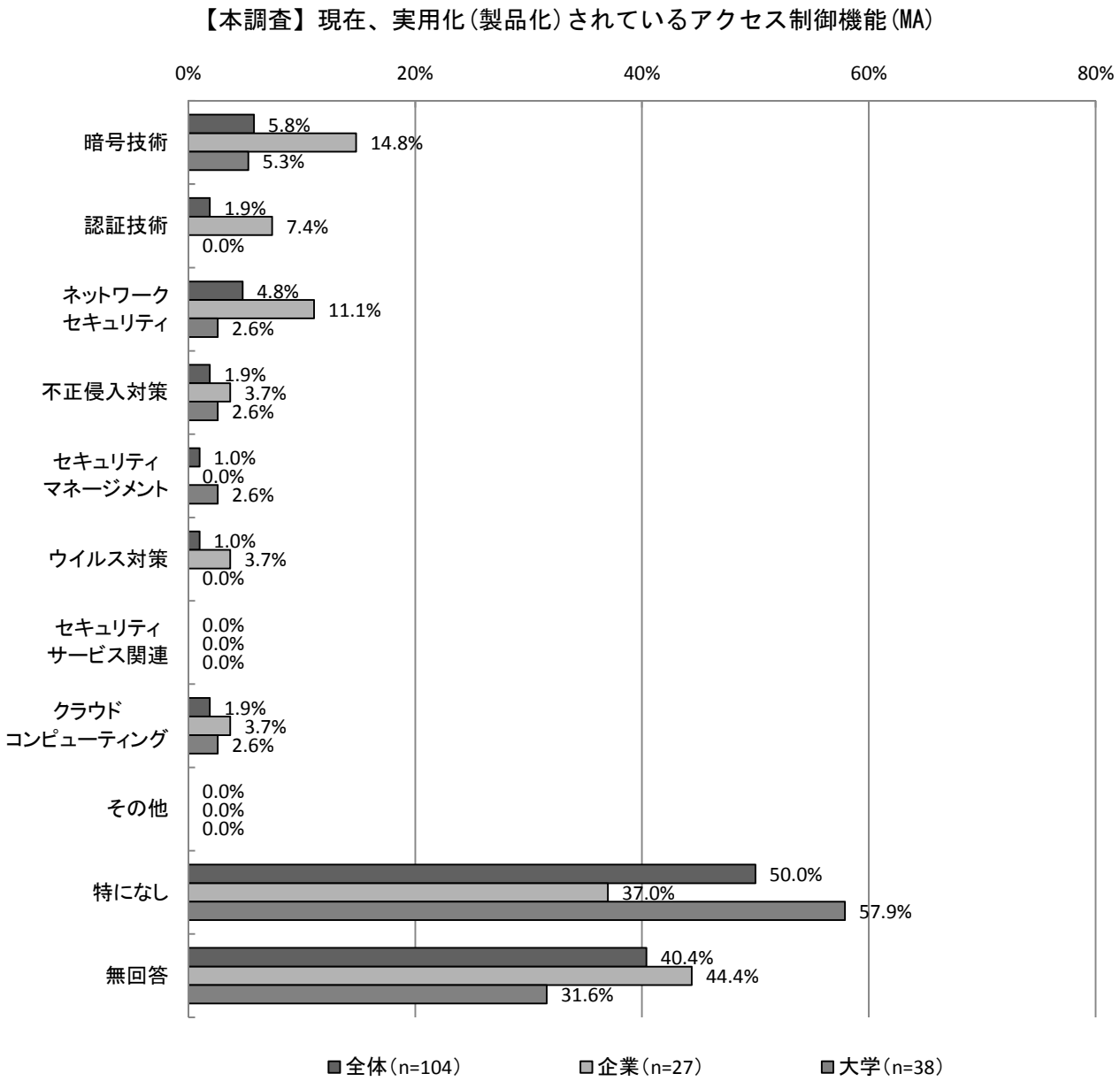
全体では、「暗号技術」が増加している。

企業では、「暗号技術」、「認証技術」、「ネットワークセキュリティ」、「不正侵入対策」が増加しており、大学では、「暗号技術」、「ネットワークセキュリティ」、「不正侵入対策」、「セキュリティマネジメント」、「クラウドコンピューティング」が増加している。

【本調査】

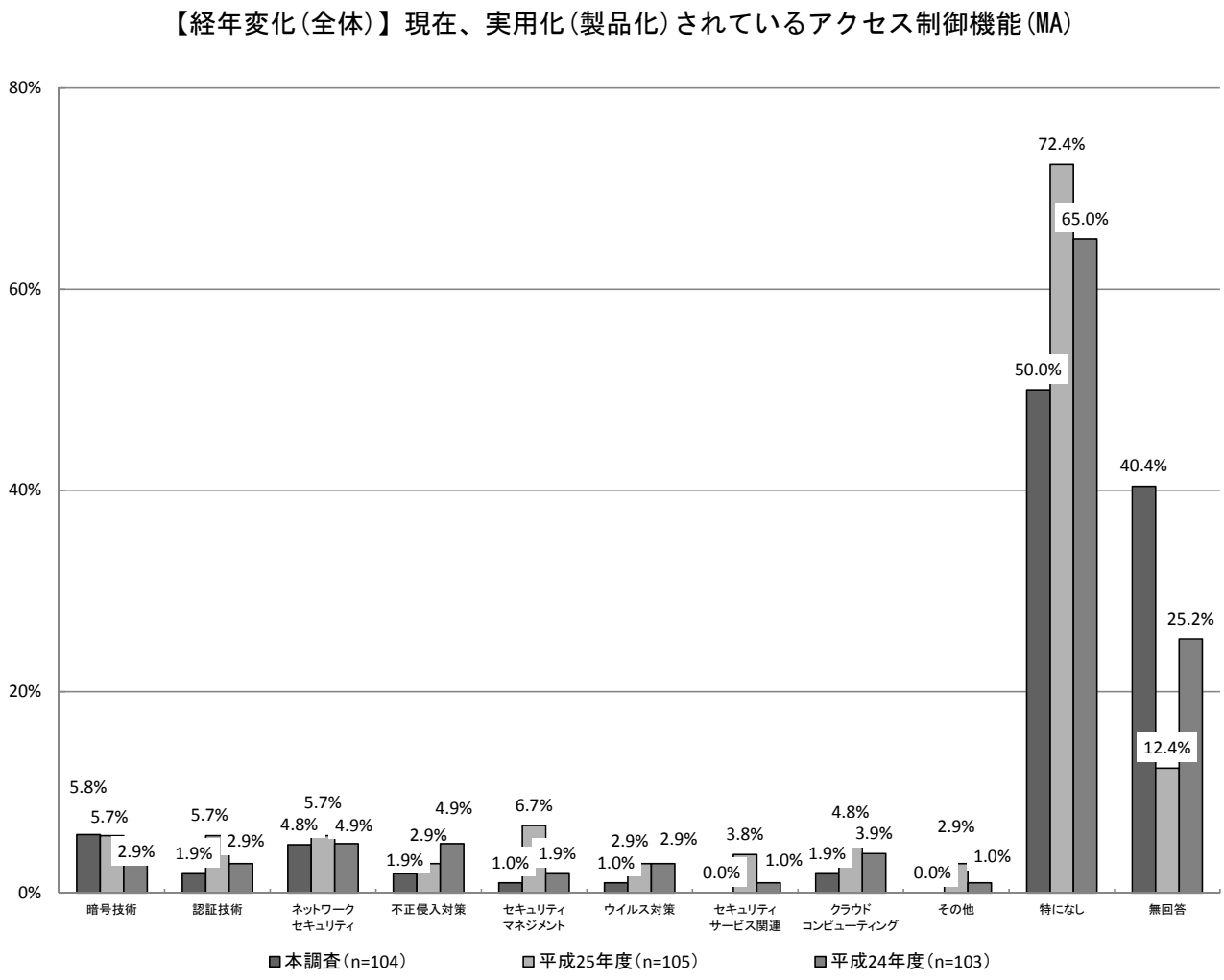
全体では、「特になし」と回答のあった 50.0%（52 件）を除くと、「暗号技術」が 5.8%（6 件）で最も多く、「ネットワークセキュリティ」が 4.8%（5 件）で続いている。

企業では、「特になし」と回答のあった 37.0%（10 件）を除くと、「暗号技術」が 14.8%（4 件）で最も多く、大学では、「特になし」と回答のあった 57.9%（22 件）を除くと、「暗号技術」が 5.3%（2 件）が最も多くなっている。



【経年変化(全体)】

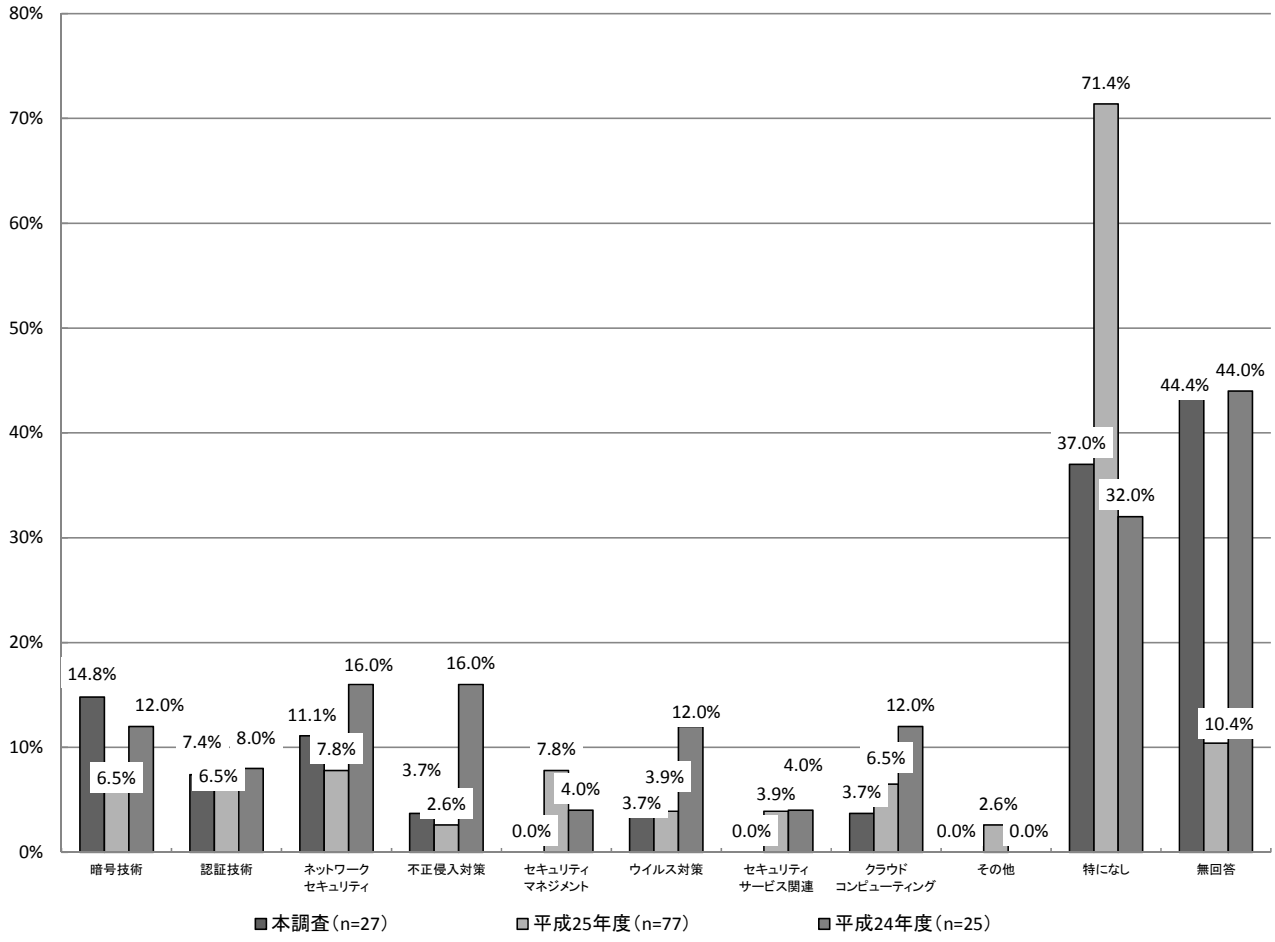
全体の経年変化を見ると、「暗号技術」を除くすべての分野で減少している。



【経年変化(企業)】

企業の経年変化を見ると、「暗号技術」、「認証技術」、「ネットワークセキュリティ」、「不正侵入対策」が増加している。

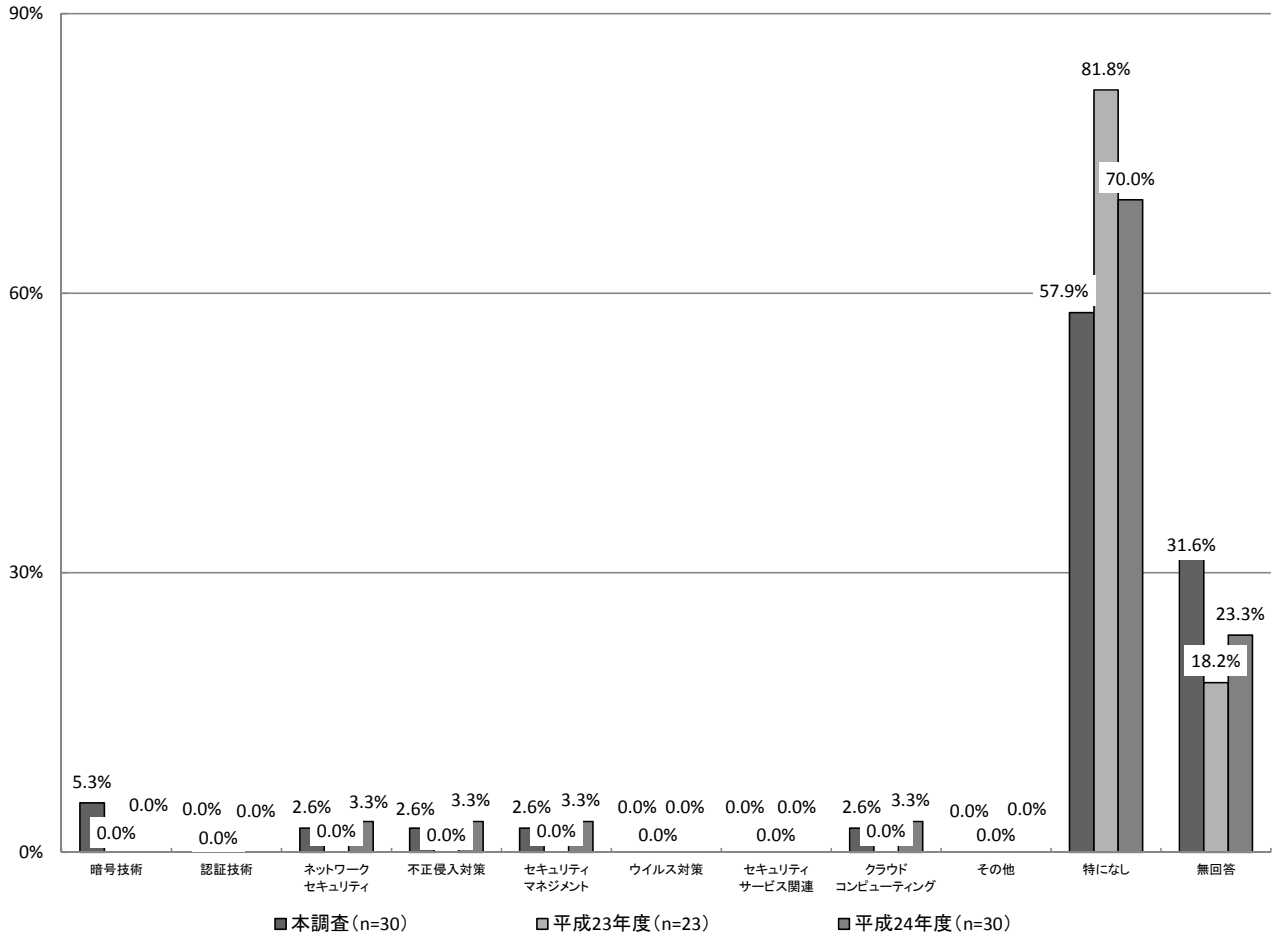
【経年変化(企業)】現在、実用化(製品化)されているアクセス制御機能(MA)



【経年変化(大学)】

大学の経年変化を見ると、「暗号技術」、「ネットワークセキュリティ」、「不正侵入対策」、「セキュリティマネジメント」、「クラウドコンピューティング」が増加している。

【経年変化(大学)】現在、実用化(製品化)されているアクセス制御機能(MA)



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

【本調査】

全体では、「予定なし」と回答のあった44.2%を除くと、「暗号技術」が7.7%で最も多く、「ネットワークセキュリティ」、「クラウドコンピューティング」が5.8%で続いている。

企業では、「予定なし」と回答のあった37.0%を除くと、「ウイルス対策」が14.8%で最も多く、大学では、「予定なし」と回答のあった47.4%を除くと、「暗号技術」が13.2%で最も多くなっている。

【経年変化】

全体では、「不正侵入対策」、「セキュリティマネジメント」、「セキュリティサービス関連」を除く分野で増加している。

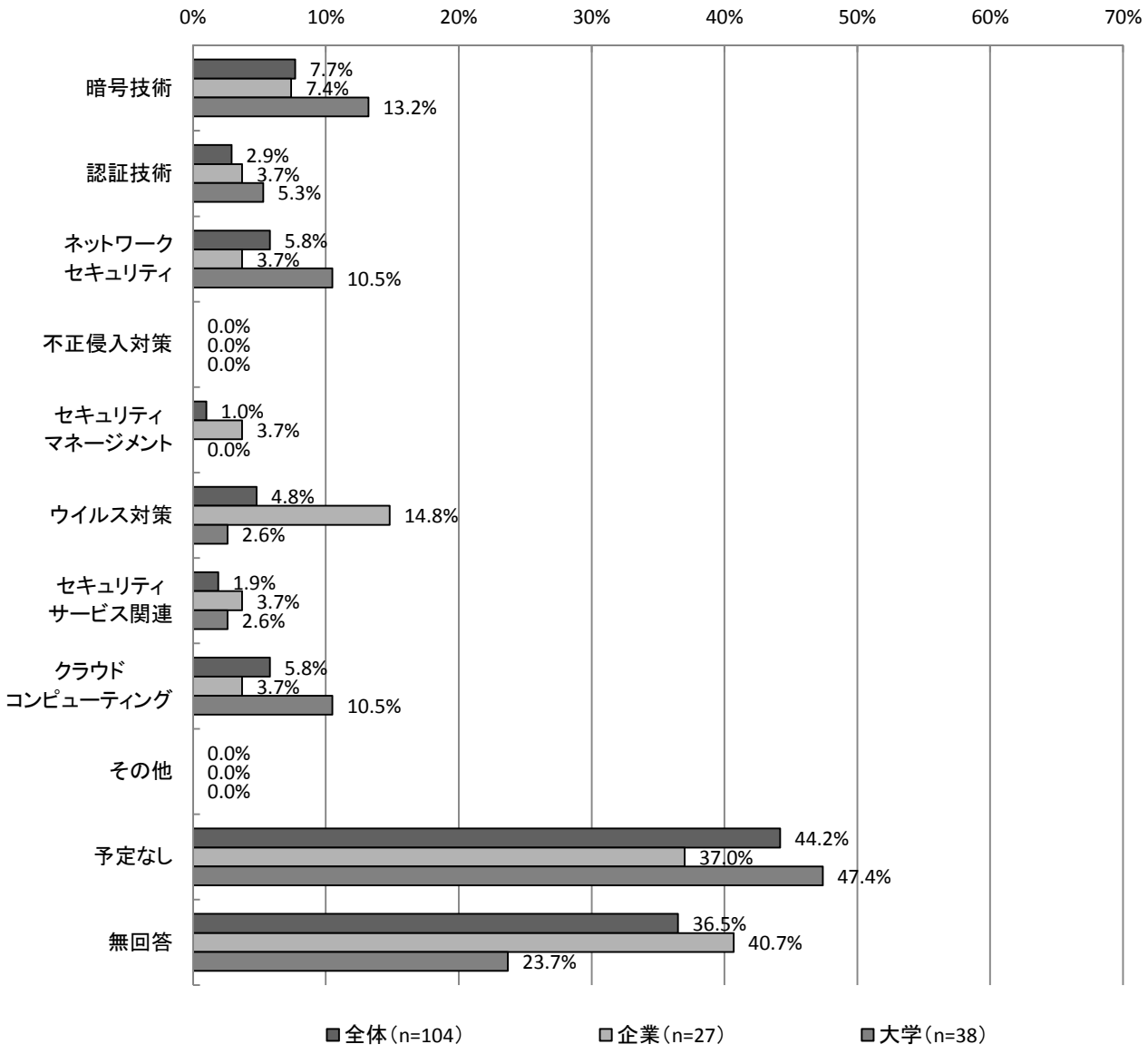
企業では、「不正侵入対策」、「セキュリティサービス関連」、「クラウドコンピューティング」を除く分野で増加しており、大学では、「ネットワークセキュリティ」、「不正侵入対策」、「セキュリティマネジメント」を除く分野で増加している。

【本調査】

全体では、「予定なし」と回答のあった 44.2%（46 件）を除くと、「暗号技術」が 7.7%（8 件）で最も多く、「ネットワークセキュリティ」、「クラウドコンピューティング」が 4.8%（5 件）で続いている。

企業では、「予定なし」と回答のあった 37.0%（10 件）を除くと、「ウイルス対策」が 14.8%（4 件）で最も多く、大学では、「予定なし」と回答のあった 47.4%（18 件）を除くと、「暗号技術」が 13.2%（5 件）で最も多くなっている。

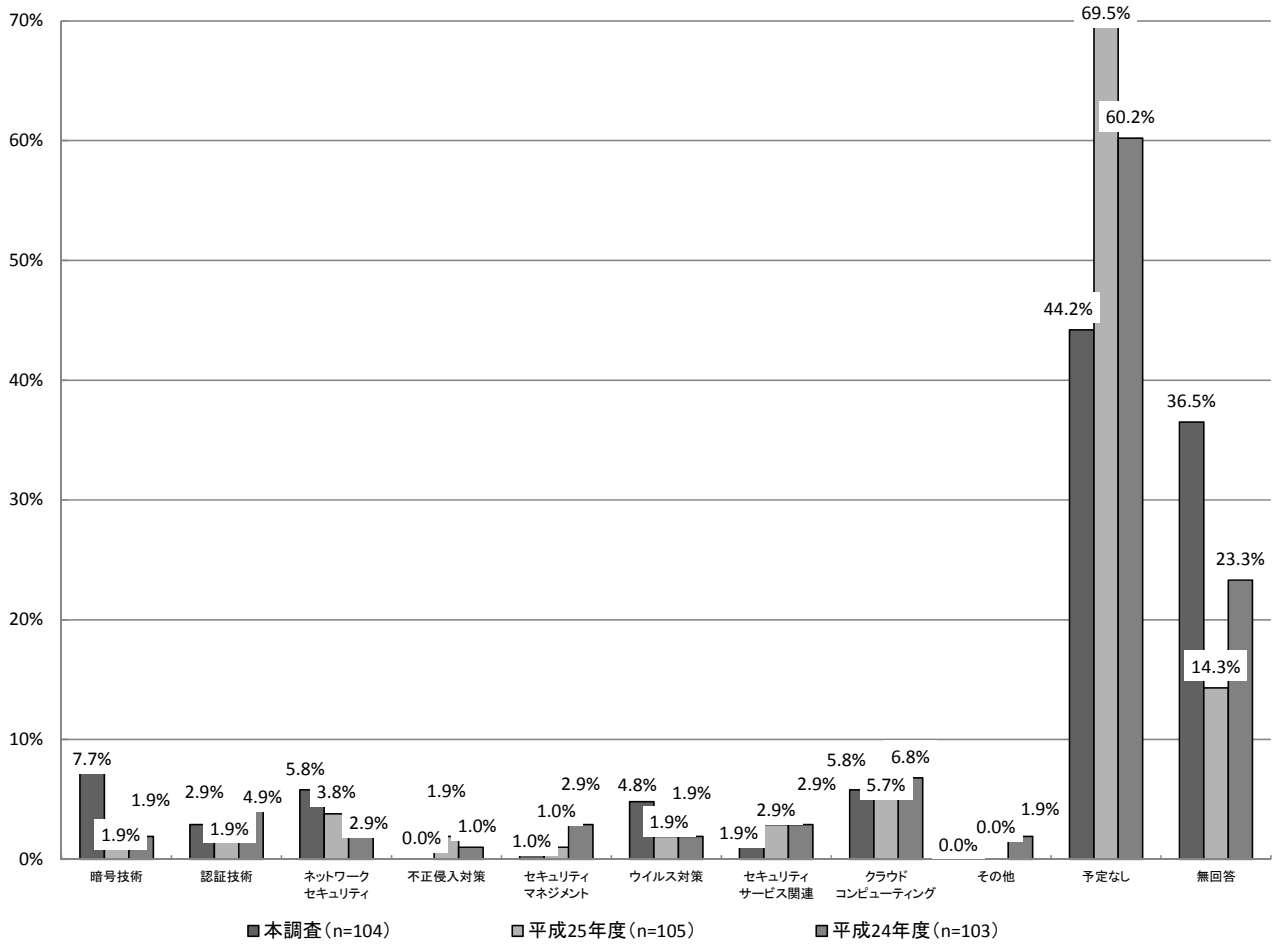
【本調査】今後、実用化（製品化）を見込んでいるアクセス制御機能（MA）



【経年変化(全体)】

全体の経年変化を見ると、「予定なし」と回答したものを除くと、「不正侵入対策」、「セキュリティマネジメント」、「セキュリティサービス関連」を除く分野で増加している。

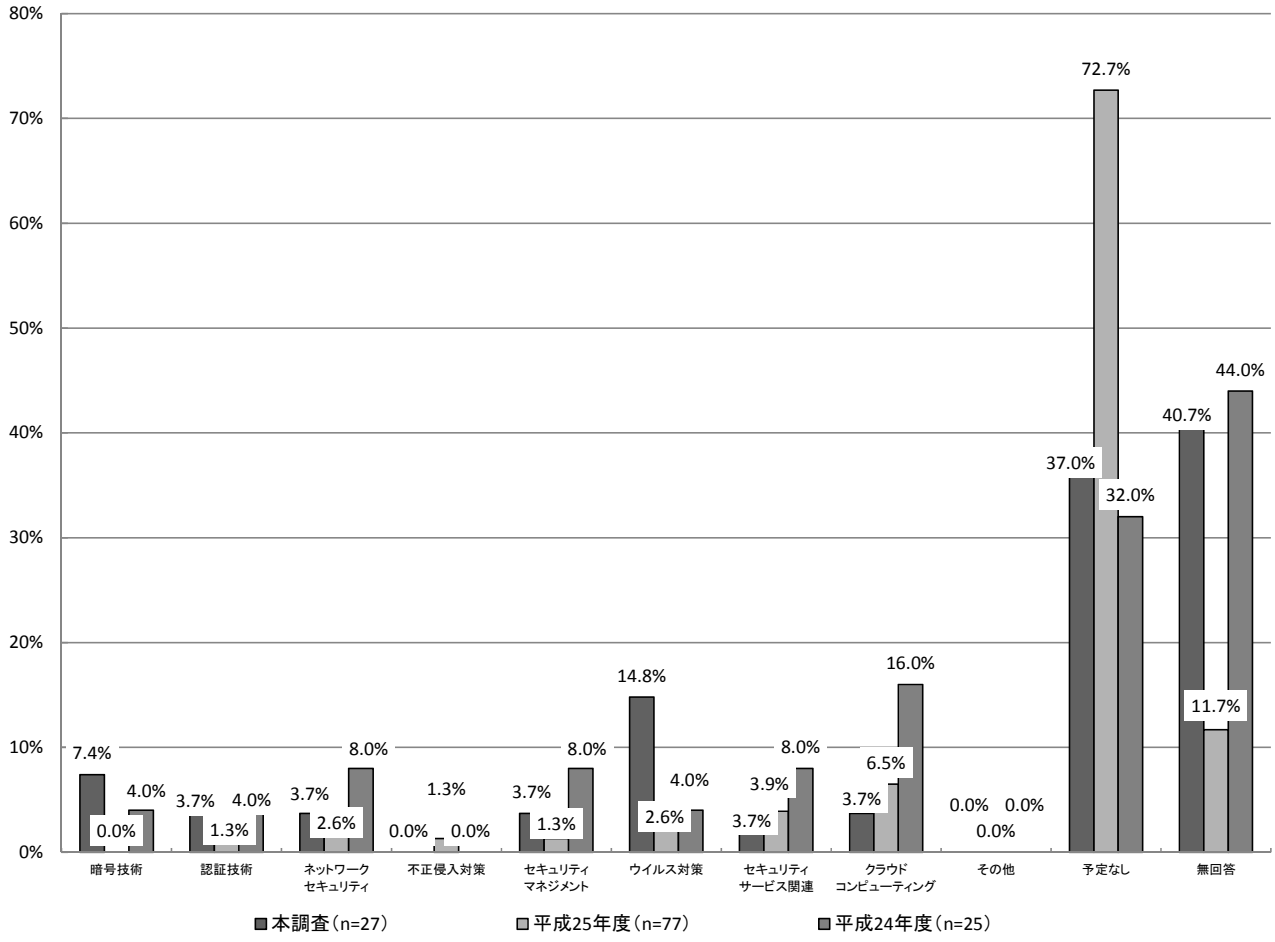
【経年変化(全体)】今後、実用化(製品化)を見込んでいるアクセス制御機能(MA)



【経年変化(企業)】

企業の経年変化を見ると、「予定なし」と回答したものを除くと、「不正侵入対策」、「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」を除く分野で増加している。

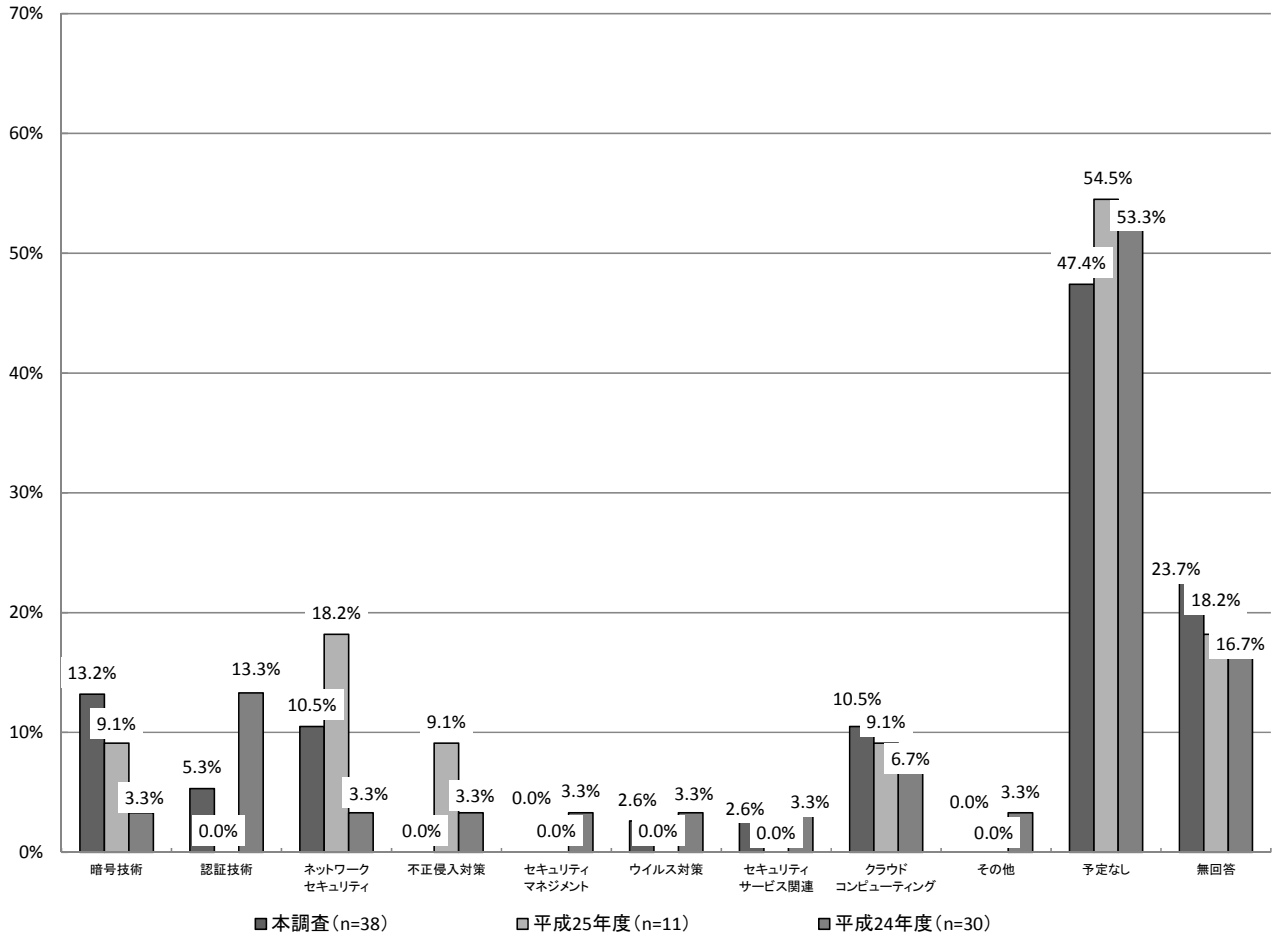
【経年変化(企業)】今後、実用化(製品化)を見込んでいるアクセス制御機能(MA)



【経年変化(大学)】

大学の経年変化を見ると、「予定なし」と回答したものを除くと、「ネットワークセキュリティ」、「不正侵入対策」、「セキュリティマネジメント」を除く分野で増加している。

【経年変化(大学)】今後、実用化(製品化)を見込んでいるアクセス制御機能(MA)



3.2. 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	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
A-Locky.net	株式会社インフィニテック	株式会社インフィニテック	○					○
FinalCode	デジタルアーツ株式会社	デジタルアーツ株式会社			○			
WebSAM SECUREMASTER	日本電気株式会社	日本電気株式会社			○			○
InfoCage	日本電気株式会社	日本電気株式会社	○	○				○
SG3600シリーズ	日本電気株式会社	日本電気株式会社	○					

「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
カオスを用いた暗号鍵の生成	八戸工業大学	秘匿通信		○				
	福井工業大学情報システムセンター	電子情報通信学会						○
ICカード等を用いた多要素web認証	宮崎大学情報基盤センター	情報基盤センター利用者支援部門			○			
ハードウェアベースIPSの研究	弘前大学総合情報処理センター	弘前大学総合情報処理センター	○					
軽量カオス暗号の研究	君が淵学園　崇城大学	崇城大学情報学部	○					
分散型ネットワークセキュリティ装置	東北工業大学工学部情報通信工学科松田研究室	工学部情報通信工学科松田研究室	○					○
不正防止可能秘密分散技術	法政大学情報科学部	法政大学情報科学部						○
属性証明書に基づくアクセス制御方式	大阪工業大学	情報科学部情報ネットワーク学科			○			
Webサーバセキュリティ	大阪工業大学	情報科学部情報ネットワーク学科		○	○			
IPV6における侵入検知	南山大学	理工学部	○					
Kソリューションズ(仮称)	デジタルアーツ株式会社	開発部　開発5課	○	○			○	○
ディレクトリ名を秘匿可能なクラウド向けファイル共有システム	広島大学情報メディア教育研究センター	広島大学情報メディア教育研究センター						○
ネットワークセキュリティに関する研究開発	九州工業大学 ネットワークデザイン研究センター		○					○
擬似乱数生成器に関する研究	九州工業大学	大学院　情報工学研究院						○
クラウドストレージに適した暗号技術	九州工業大学	大学院　情報工学研究院						○
認証暗号	日本電気株式会社　クラウドシステム研究所	クラウドシステム研究所						○
セキュリティマネジメント支援	公立大学法人会津大学							○
Webブラウザのための簡易PKI利用機能の実装	京都産業大学	コンピュータ理工学部			○			
通信記録の分析によるウイルス感染PCの検出	神戸大学大学院　工学研究科　電気電子工学専攻　森井研究室		○					

※回答票Cの回収数は20件となっているが、1件公開用情報が得られなかったため、技術の研究開発状況表は19件となっている

3.2.1. 「技術の実用化（製品化）状況」について

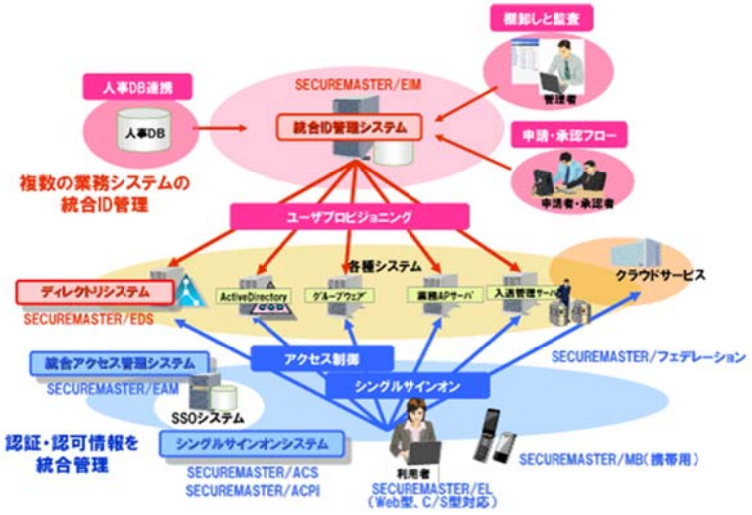
※一覧表の下には対象となる防御対象について○を付与している。

企業・大学名	株式会社インフィニテック
代表者名	芳賀　紳
所在地	〒141-0031　東京都品川区西五反田2-12-19　五反田NNビル3F
窓口部署名／電話番号	技術部／(03)5759-6810
ホームページのURL	http://www.infinitec.co.jp/
製品説明のURL	http://w3.infinitec.co.jp/modules/products/?page=category&cid=31
対象技術	技術の概要・特徴など
製品名: A-Locky.net 開発元: 株式会社インフィニテック 開発国: 日本 価格: 発売時期: 平成19年 出荷数:	A-LOCKY.netの基本機能 ●アクセス制御 ・USB認証キーが無いと、サーバの重要データ（情報金庫）にアクセスすることができません。 ・USB認証キーに権限をつけることで、利用できる重要情報を区別することができます。 ●暗号化 ・サーバ内の重要情報（情報金庫）は暗号化されていますので、万一、サーバ本体が盗難にあったとしても、サーバ内部の情報を閲覧することはできません。 ・サーバ内の暗号化された重要情報を閲覧するには、USB認証キーが必要です。 ●ログ管理 ・USB認証キーを利用している間の行動記録（ファイルの暗号化、複合化、印刷など）を取得し、サーバに一括管理します。 ・取得した記録から、必要に応じた（検索、抽出）記録を閲覧、印刷することができます。

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	デジタルアーツ株式会社
代表者名	道具　登志夫
所在地	〒100-0004 東京都千代田区大手町1-5-1　大手町ファーストスクエア　ウエストタワー14F
窓口部署名／電話番号	開発部／(03)5220-1110
ホームページのURL	http://www.daj.jp/
製品説明のURL	http://www.finalcode.com/jp/
対象技術	技術の概要・特徴など
製品名: FinalCode 開発元: デジタルアーツ株式会社 開発国: 日本 価格: 10Lic 25万円から 発売時期: 2010年6月～ 出荷数: 非公開	ファイルを自動的あるいは指定して暗号化すると共に、アクセス権をクラウドにて管理。いざとなったら、送ったファイルを後から削除することができるソリューション。 社外にファイルを送付した後も、ファイルの所在確認や、閲覧の許可・禁止、コピーや印刷の許可・禁止、閲覧期間制限、アクセス履歴のトラッキングが行える。 暗号化キーは利用者のハードウエアに紐付けられて自動的に生成され、クラウドで管理されるため、利用者はパスワードを意識することなく、通常のファイルと同様に扱うことができる。 この機能により、パスワード漏洩による情報漏洩の危険性から開放される。特に海外等の取引先に従来通りのパスワード保護したファイルを送付する際には、常にパスワード漏洩による情報漏洩がつきまとうが、そのような利用状況においても安全にファイルをやりとりできる。 また、サイバー攻撃など、マルウェアを利用した情報窃盗が行われた場合にも、明示的なパスワードが無いために、情報が漏洩することが無い。更には、ファイルの所在を確認することができるとともに、いざというときはリモートでファイルを削除することができる。

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

企業・大学名	日本電気株式会社
代表者名	遠藤 信博
所在地	〒108-8001　東京都港区芝五丁目7番1号
窓口部署名／電話番号	システムソフトウェア事業部
ホームページのURL	http://jpn.nec.com/infocage/index.html
製品説明のURL	http://jpn.nec.com/websam/securemaster
対象技術	技術の概要・特徴など
製品名: WebSAM SECUREMASTER 開発元: 日本電気株式会社 開発国: 日本 価格: ID管理　150万円～ アクセス管理・SSO　140万円 発売時期: 平成11年 出荷数: 約1,100システム	ID管理とアクセス管理を統合し、コスト削減と統制強化を図るとともに、情報の機密性を守ります。 ・ディレクトリから、ID管理、アクセス管理、シングルサインオン（SSO）まで、統合認証基盤構築に必要な製品を揃えたスイート製品です。共通的なインタフェースをご提供します。 ・GUIによる連携先システムの追加やアクセス制御ポリシ設定、お客さま固有の要件に対するAPIや開発言語による拡張など、種々の業務システムと柔軟に連携可能です。 ・自社製品で、国内にてソースコードを保有しているため、カスタマイズ要望、障害対応時なども迅速かつ柔軟なサポートが可能です。 

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

企業・大学名	日本電気株式会社
代表者名	遠藤 信博
所在地	〒108-8001　東京都港区芝五丁目7番1号
窓口部署名／電話番号	システムソフトウェア事業部
ホームページのURL	http://jpn.nec.com/infocage/index.html
製品説明のURL	http://jpn.nec.com/infocage/
対象技術	技術の概要・特徴など
製品名: InfoCage 開発元: 日本電気株式会社 開発国: 日本 価格: 発売時期: 平成14年12月24日 出荷数:	・電子ファイルにセキュリティ情報を持たせ暗号化し、情報漏えいを防止。 ・ファイル/HDD暗号、媒体制御、認証によりPCの統合セキュリティを実現。 ・webアプリケーションに渡されるデータをチェック。攻撃とみなしたアクセスをブロックすることで、通常のファイアウォールやIDS/IPSでは防ぎきれないWEBアプリケーション層への攻撃を防止。 ・社内ネットワークから持ち込みPCを排除し情報漏洩やウイルス感染のリスクを低減。 ・セキュリティ対策が不十分なPCを、業務ネットワークから隔離し、ウイルス感染などの危険性を低減。 ・ネットワーク内のPCのセキュリティ対策状況を把握し、効率的にセキュリティレベルを維持。

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	日本電気株式会社
代表者名	遠藤 信博
所在地	〒108-8001　東京都港区芝五丁目7番1号
窓口部署名／電話番号	システムソフトウェア事業部
ホームページのURL	http://jpn.nec.com/infocage/index.html
製品説明のURL	http://jpn.nec.com/sg/
対象技術	技術の概要・特徴など
製品名: SG3600シリーズ 開発元: 日本電気株式会社 開発国: 日本 価格: 85万円～ 発売時期: 平成15年7月 出荷数: 約1000台	概要：NEC独自エンジンを搭載したファイアウォール製品 特徴：・VPN機能（IPSec、SSL-VPN、IPSec）の標準搭載により公衆のネットワーク上でも改ざんや盗聴から守られたセキュアな通信を実現。 ・メール、DNS、プロキシ、NTP、DHCPといった各種サーバ機能を標準搭載しているため、別途サーバ導入が不要。 ・動的ルーティングをサポートしており、ネットワーク構成の変更にも柔軟に対応可能。 ・冗長化機能により、万が一の場合でも待機系に自動切り替え可能。

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	

3.2.2. 「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	八戸工業大学
代表者名	清水　能理
所在地	〒031-8501　青森県八戸市大字妙字大開88-1
窓口部署名／電話番号	工学部システム情報工学科／(0178)25-8135
関連部門名	秘匿通信
ホームページのURL	http://www.hi-tech.ac.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称: カオスを用いた暗号鍵の生成 研究開発国: 日本 研究開発期間: 平成26年4月1日～平成29年3月31日	自然界のカオス現象（振動）から人工的なカオス発振回路（モデリング）を構築し、得られるカオス信号と情報信号から暗号文を生成します。また、カオス発振回路は暗号化鍵（ワンタイムパスワードとして）の生成にも応用します。

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	〇
高度認証技術	
インシデント分析技術	
不正プログラム対策技術	
その他アクセス制御に関する技術	

企業・大学名	福井工業大学情報システムセンター
代表者名	情報システムセンター長　池田　岳史
所在地	〒910-8505　福井県福井市学園3丁目6番1号
窓口部署名／電話番号	情報システムセンター／(0776)29-7873
関連部門名	電子情報通信学会
ホームページのURL	http://www.fukui-ut.ac.jp
研究説明のURL	http://futredb.fukui-ut.ac.jp/html/100000242_ja.html?k=信川
対象技術	研究開発状況
研究開発名称: 研究開発国: 日本 研究開発期間:	我々はこれまでに、カオス性をもったニューラルネットワークにおける創発現象について解析を行ってきた。特に、カオス共鳴やカオス同期などについては、通信や認証技術への応用が期待できた。例えば、カオスにおける初期値鋭微性を利用し、共通パラメーターを鍵として設定した暗号化通信や認証技術などである。今後、ニューラルネットワークでの研究成果と知見に基づき、アクセス制御機能に関する分野に参入していく予定である。

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

企業・大学名	宮崎大学情報基盤センター
代表者名	廿日出　勇
所在地	〒889-2192　宮崎県宮崎市学園木花台西1丁目1番地
窓口部署名／電話番号	情報図書部／(0985)58-2867
関連部門名	情報基盤センター利用者支援部門
ホームページのURL	http://www.miyazaki-u.ac.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称: ICカード等を用いた多要素web認証 研究開発国: 日本 研究開発期間: 平成26年4月～	テストシステムを用いて実証実験を実行中

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	弘前大学総合情報処理センター
代表者名	葛西　真寿
所在地	〒036-8561　青森県弘前市文京町3番地
窓口部署名／電話番号	弘前大学研究推進部社会連携課／(0172)39-3726
関連部門名	弘前大学総合情報処理センター
ホームページのURL	http://www.cc.hirosaki-u.ac.jp/
研究説明のURL	
対象技術	研究開発状況
研究開発名称: 　ハードウェアベースIPSの研究 研究開発国: 　日本、タイ王国 研究開発期間: 　平成14年4月1日～	モバイル機器向けのIPS用のFPGAの開発を中心に行っている。

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	君が淵学園　崇城大学
代表者名	吉岡　大三郎
所在地	〒860-0082　熊本県熊本市西区池田4-22-1
窓口部署名／電話番号	情報学部/096-326-3111
関連部門名	崇城大学情報学部
ホームページのURL	http://www.sojo-u.ac.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称: 軽量カオス暗号の研究 研究開発国: 日本 研究開発期間: 平成24年4月1日～	これまで、ディジタルカオスに基づき暗号の主要部である非線形変換関数S-boxを設計した。今後、128bitのブロック暗号を設計する予定である。

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

企業・大学名	東北工業大学工学部情報通信工学科松田研究室
代表者名	松田　勝敬
所在地	〒982-8577　宮城県仙台市太白区八木山香澄町35-1
窓口部署名／電話番号	松田研究室／(022)305-3424
関連部門名	工学部情報通信工学科松田研究室
ホームページのURL	http://www.ice.tohtech.ac.jp/jp-ug/labs/matsuda.html
研究説明のURL	
対象技術	研究開発状況
研究開発名称: 分散型ネットワークセキュリティ装置 研究開発国: 日本 研究開発期間: 平成22年4月1日～	基本構成要素の開発、試験を実施中。

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	法政大学情報科学部
代表者名	理事長　田中　優子、学部長　雪田　修一
所在地	〒184-8584　東京都小金井市梶野町3-7-2
窓口部署名／電話番号	小金井事務部学務課情報科学部担当／(042)387-6023
関連部門名	法政大学情報科学部
ホームページのURL	http://cis.k.hosei.ac.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称: 不正防止可能秘密分散技術 研究開発国: 日本 研究開発期間: 平成18年4月1日～平成30年3月31日	保護対象となるデータを複数の部分情報に分けて複数のサーバで管理し、次の3つの安全性を保証する。 1.予め決められたグループのサーバが協力すると部分情報からデータが復元される 2.それ以外のグループが部分情報を持ちよってもデータに関する1ビットの情報も得られない 3.部分情報を改ざんしても高い確率で検知する 上記の性質を有する方式の開発を行い、世界最小の部分情報サイズを実現する方式を学会で発表。

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	大阪工業大学
代表者名	学長　井上　正崇
所在地	〒535-8585　大阪府大阪市旭区大宮5丁目16番1号
窓口部署名／電話番号	大阪工業大学企画課／(06)6954-4097
関連部門名	情報科学部情報ネットワーク学科
ホームページのURL	http://www.oit.ac.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称: 属性証明書に基づくアクセス制御方式 研究開発国: 日本 研究開発期間: 平成19年4月1日～平成28年3月31日	アクセス権限は個人に対し付与するものではなく、個人の所属や肩書などの属性に対し付与すべきであるとの考えに基づき、利用者登録を必要とせず、利用者属性に基づきアクセス条件を規定し、利用者が提示した属性に基づきサービス使用可否を判断する方式、およびそれに基づくシステムの研究試作を実施している。 利用者の属性を証明する手段として、ITU-T/ISO標準のX.509属性証明書を使用する。属性証明書の所有者であることの証明は、X.509属性証明書と対応付けされるX.509公開鍵証明書により行う。これらより、全体のシステムは、公開鍵証明書を発行する電子認証局（CA）、属性証明書を発行する電子認証局（AA）、サービスを提供するアクセス制御システムから構成される。CAやAAを試作すると共に、アクセス制御の例として、電子的な学生証や職員証に基づき大学Webページの閲覧可否を判断するシステム、および属性証明書の所有者確認をネットショップサーバとは独立させ、別組織で発行された電子的な社員証に基づきネットショップ匿名優待サービスを行うシステムを試作している。

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	大阪工業大学
代表者名	学長　井上　正崇
所在地	〒535-8585　大阪府大阪市旭区大宮5丁目16番1号
窓口部署名／電話番号	大阪工業大学企画課／(06)6954-4097
関連部門名	情報科学部情報ネットワーク学科
ホームページのURL	http://www.oit.ac.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称: Webサーバセキュリティ 研究開発国: 日本 研究開発期間: 平成22年4月1日～平成28年3月31日	Webサーバセキュリティとして、SQLインジェクション、クロスサイトスクリプティング、クロスサイトリクエストフォージェリに対する対策を研究試作している。 SQLインジェクションに関しては、SQL文で特別の意味を持つ特殊文字を検出し、その効果をなくすように行う文字の置換処理（サニタイジング）とSQL文のひな型の解析処理を事前に済ませておき、ひな型の変動箇所に、実際の値を割り当て実行する機能（バインド機構）の2手段を試作している。クロスサイトスクリプティングに関しては、スクリプトにおける特別な意味を持つ文字を別の文字に置き換えるエスケープ処理を試作しており、クロスサイトリクエストフォージェリに関しては、乱数をクライアントに送信するトークンとして使用し、トークンの確認により正常な利用者からの送信か否かを判断する方式を試作している。 今後もWebサーバに対するその他の攻撃に対する対策を研究していく予定である。

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

企業・大学名	南山大学
代表者名	学長　ミカエル・カルマノ
所在地	〒466-8673　愛知県名古屋市昭和区山里町18
窓口部署名／電話番号	総務部総務課／(052)832-3112
関連部門名	理工学部
ホームページのURL	http://www.nanzan-u.ac.jp
研究説明のURL	無し
対象技術	研究開発状況
研究開発名称: IPV6における侵入検知 研究開発国: 日本 研究開発期間: 平成24年4月～	IPV6固有の侵入検知のための統計的手法を確立するために、リースIPアドレスwp偽ったパケットを多数送信する疑似攻撃プログラムを開発してきた。ベイズ推定に基づく統計的分析もある程度進めてきたが、本格的な実験には至っていない。

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

企業・大学名	デジタルアーツ株式会社
代表者名	道具　登志夫
所在地	〒100-0004
窓口部署名／電話番号	開発部／(03)5220-1110
関連部門名	開発部　開発5課
ホームページのURL	http://www.daj.jp/
研究説明のURL	現時点ではなし
対象技術	研究開発状況
研究開発名称: Kソリューションズ（仮称） 研究開発国: 日本 研究開発期間: 2013年5月1日～2015年3月31日	主要な機能は研究開発が完了し、ユーザー・エクスペリエンスを高めるよう試験運用および、持続的なインテグレーションを実施中。 製品化のための、マニュアル等を含む製品付属品については、今後製作予定。

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

企業・大学名	広島大学情報メディア教育研究センター
代表者名	相原　玲二
所在地	〒739-8511　広島県東広島市鏡山1-4-2
窓口部署名／電話番号	ユーザサービス部門／(082)424-6252
関連部門名	広島大学情報メディア教育研究センター
ホームページのURL	http://www.media.hiroshima-u.ac.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称: ファイル名／ディレクトリ名を秘匿可能なクラウド向けファイル共有システム 研究開発国: 日本 研究開発期間: 平成26年4月1日～平成27年3月31日	属性ベース暗号を用いたシステムの試作および評価を行っている。科学研究費補助金による研究であり、未発表の内容も含まれているため詳細は記載しない。

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

企業・大学名	九州工業大学 ネットワークデザイン研究センター
代表者名	
所在地	
窓口部署名／電話番号	
関連部門名	
ホームページのURL	http://www.ndrc.kyutech.ac.jp
研究説明のURL	http://www.ndrc.kyutech.ac.jp
対象技術	研究開発状況
研究開発名称: ネットワークセキュリティに関する研究開発 研究開発国: 日本 研究開発期間: 平成22年4月1日～	外部ネットワークからの攻撃の早期検出を可能にする技術および，異常検出後の対処方法について研究開発を実施しており，現在は，実ネットワーク環境におけるデータの取得および取得したデータの分析を進めている。

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

企業・大学名	九州工業大学
代表者名	松永守央
所在地	〒820-8502　福岡県飯塚市川津680-4
窓口部署名／電話番号	大学院　情報工学研究院/0948-29-7654
関連部門名	大学院　情報工学研究院
ホームページのURL	http://www.kyutech.ac.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称: 　擬似乱数生成器に関する研究 研究開発国: 　日本 研究開発期間: 　平成18年～	暗号器を用いた一般的な構成とは異なる擬似乱数生成器の開発を目指している。カオス的に振る舞うロジスティック写像に着目し、計算器上に実装された写像の性質を調査している。擬似乱数生成器に求められるいくつかの設計上の指針を明らかにした。

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	九州工業大学
代表者名	松永守央
所在地	〒820-8502　福岡県飯塚市川津680-4
窓口部署名／電話番号	大学院　情報工学研究院/0948-29-7654
関連部門名	大学院　情報工学研究院
ホームページのURL	http://www.kyutech.ac.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称: 　クラウドストレージに適した暗号技術 研究開発国: 　日本 研究開発期間: 　平成26年11月～	アイディアの着想段階。状況設定と初歩的なプロトコルの考案が終了したところ。

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	日本電気株式会社　クラウドシステム研究所
代表者名	宮内　幸司
所在地	〒211-8666　川崎市中原区下沼部1753
窓口部署名／電話番号	044-431-7686
関連部門名	クラウドシステム研究所
ホームページのURL	http://jpn.nec.com/rd/crl/code/research/otr_jp.html
研究説明のURL	
対象技術	研究開発状況
研究開発名称: 　認証暗号 研究開発国: 　日本 研究開発期間:	特徴 ・暗号化レート1（1ブロックにつき1回のブロック暗号） ・オンライン処理可能、さらに並列処理可能 ・ブロック暗号の暗号化関数のみを利用し、復号関数を必要としない ・ブロック暗号の標準的な安全性をベースとした証明可能安全性保証

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	公立大学法人会津大学
代表者名	理事長　岡　隆一
所在地	〒965-8580　福島県会津若松市一箕町鶴賀上居合90
窓口部署名／電話番号	企画連携課／(0242)37-2511
関連部門名	
ホームページのURL	http://www.u-aizu.ac.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称: セキュリティマネジメント支援 研究開発国: 日本 研究開発期間: 平成16年5月～	基本部分については開発が完了している。今後はISO/IECの標準の変化や、認証に関する動向の変化に対応できる仕組みの検討と、システムの運用方法の検討を行う予定である。

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

企業・大学名	京都産業大学
代表者名	学長　大城光正
所在地	〒603-8555　京都府京都市北区上賀茂本山
窓口部署名／電話番号	コンピュータ理工学部/075-705-1531
関連部門名	コンピュータ理工学部
ホームページのURL	http://www.kyoto-su.ac.jp
研究説明のURL	
対象技術	研究開発状況
研究開発名称: Webブラウザのための簡易PKI利用機能の実装 研究開発国: 日本 研究開発期間: 平成26年4月1日～平成27年3月31日	WebRic技術などブラウザ間がP2Pで通信する事例が発生するなど、Webブラウザでの新たな通信形態における認証、暗号化等の要求が発生している。本研究ではWeb Cryptography APIなどの提案に伴い、検討が進められているWebアプリケーションでのPKI利用において、P2Pで用いられる簡易なPKI利用をサポートするために必要な機能拡張の調査ならびに実装を行う。成果はオープンソースとし製品化は検討していない。

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

企業・大学名	神戸大学大学院　工学研究科　電気電子工学専攻　森井研究室
代表者名	森井　昌克
所在地	〒657-8501　兵庫県神戸市灘区六甲台町1-1
窓口部署名／電話番号	神戸大学大学院　工学研究科／(078)803-6088
関連部門名	
ホームページのURL	http://srv.prof-morii.net/~morii/ http://bylines.news.yahoo.co.jp/moriimasakatsu/
研究説明のURL	なし
対象技術	研究開発状況
研究開発名称: 通信記録の分析によるウイルス感染PCの検出 研究開発国: 日本 研究開発期間: 平成24年4月1日～	HTTP通信など学内で収集している通信記録を総合的に分析してウイルス等に感染して遠隔操作される可能性があるPCなどの検出を行う。

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状況等に関する調査 調査報告書

付録資料

付録１：調査票
付録２：集計表

1.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

平成26年11月

調査ご協力のお願い

時下ますますご清祥のこととお慶び申し上げます。

この度、(株)タイム・エージェントは、警察庁生活安全局からの委託により、今後の不正アクセス行為からの防御に関する意識の啓発や知識の普及に役立てることを目的として、民間企業・各種団体のみなさま方の不正アクセス行為対策に関する取り組み状況をおうかがいするため、アンケート調査を実施することといたしました。

本アンケートは、貴社・団体において、**基幹業務システムを管理しておられる部署のご担当者**にお答えいただければ幸いに存じます。

回答をお願いしている民間企業・各種団体のみなさま方は全国より無作為に抽出させていただきました。また、ご回答いただいた内容につきましては、統計的に処理いたしますので、個々の方々のお名前や内容が外部に出るようなことはございません。

つきましては、ご多忙の折、誠に恐縮とは存じますが、上記の趣旨をご理解の上、本調査にご協力を賜りますようお願い申し上げます。

※　今回の調査結果は、報告書としてとりまとめた上、警察庁のホームページにて今年度中に公開する予定となっています。

過去に行った調査を、それぞれ取りまとめた報告書につきましては下記URLよりアクセスしてご覧いただけます。

過去の報告書：http://www.npa.go.jp/cyber/research/index.html

〈調査企画〉
〒100-8974　東京都千代田区霞ヶ関二丁目一番二号
警察庁　生活安全局　情報技術犯罪対策課
担当　小谷・藤田
TEL：03-3581-0141（内線 3443・3424）

〈調査実施（このアンケートに関するお問合せ先)〉
〒150-0044　東京都渋谷区円山町六番八号
㈱タイム・エージェント　担当 渡部
TEL／FAX：03-5459-1590／03-3770-6820
E-mail：access@timeagent.co.jp
（受付時間：平日 10 時から 17 時）

＜ご記入上のお願い＞

1　ご回答は、**貴社・団体内の基幹業務システムを管理されている部署の方**にお願いいたします。

2　ご回答方法は、「電子メールでの回答」、「郵送での回答」の中からお選び頂けます。
何れのご回答方法の場合も、**11月28日(金)**までにご返信頂くようお願い申し上げます。

3　質問の番号順にお答えください。質問によっては、一部の方だけにおうかがいするものがありますが、その場合は矢印等の指示にそってお進みください。

4　ご回答は、あてはまるものの番号を○印で囲んでください。なお、質問ごとに「○は一つ」「○はいくつでも」というように指定してありますので、ご注意ください。

5　「その他（　　）」に該当される場合は、お手数おかけいたしますが、なるべく詳しく（　　）内に回答内容をご記入ください。

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。

問1. 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（　　）
10. この分野の技術開発に取り組んでいない

問2. 今後、取り組む予定がある分野はどちらですか。（○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（　　）
10. この分野の技術開発に取り組む予定は無い

問3. 問2で回答いただいた中で、今後もっとも力を入れていく分野はどちらですか。（○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（　　）
10. 特に無い

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ご回答ください。（○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）の予定は無い

問6. 貴事業体（研究所）のおおよその年間売上と、おおよそのアクセス制御関連の年間売上をご回答ください。（単位にご注意ください）

年間売上全体　　およそ＿＿＿＿＿＿万円

その内、アクセス制御関連の年間売上　　およそ＿＿＿＿＿＿万円

問7. 貴事業体（研究所）のおおよその年間の研究開発費をご回答ください。（単位に注意）

年間研究開発費　　およそ＿＿＿＿＿＿万円

問8. 貴事業体（研究所）で研究開発に携わっているおおよその人員数をご回答ください。

研究開発人員　　およそ＿＿＿＿＿＿人

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．DoS（※）　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	平成　　年　　月　　日頃～
出荷数	累計
製品説明がされているURL	http://

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. DoS(※)　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	平成　年　月　日～平成　年　月　日
研究内容の説明がされているURL	http://

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いたします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	
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、株式会社タイム・エージェントからご連絡させていただくことがあります。

【ご担当者のご連絡先】

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

【個人情報のお取り扱いについて】

■　ご担当者の個人情報は、株式会社タイム・エージェント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。

＜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。次条第二項第一号及び第二号において同じ。）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、Secure Shellなど）、無線 LAN セキュリティ、ファイアウォール、パケットフィルタリング、コンテンツセキュリティ（コンテンツフィルタ、メールフィルタ）、ネットワーク管理
不正侵入対策	侵入検知（IDS）、ハニーポット、アクセスログ収集管理
セキュリティマネジメント	ログ解析、資産管理、情報保護、セキュリティ情報管理
ウイルス（不正プログラム）対策	ウイルス対策ソフト、スパイウェア対策ソフト
セキュリティサービス	セキュリティ診断、不正アクセスウイルス監視、コンサルティング、レスキューサービス

＜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。
DoS	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。

2. 集計表

2.1 回答用紙Ａの集計表

問1. 現在取り組んでいる分野

		調査数	暗号技術	認証技術	ネットワークセキュリティ	不正侵入対策	セキュリティマネジメント	ウイルス対策	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	その他	この分野の技術開発に取り組んでいない
全　体		104	18	13	17	9	6	10	5	16	2	61
		100.0	17.3	12.5	16.3	8.7	5.8	9.6	4.8	15.4	1.9	58.7
属性	企業	27	5	4	6	4	2	6	2	3	−	17
		100.0	18.5	14.8	22.2	14.8	7.4	22.2	7.4	11.1	−	63.0
	大学	38	11	7	9	4	3	2	2	8	2	18
		100.0	28.9	18.4	23.7	10.5	7.9	5.3	5.3	21.1	5.3	47.4

問2. 今後、取り組む予定がある分野

		調査数	暗号技術	認証技術	ネットワークセキュリティ	不正侵入対策	セキュリティマネジメント	ウイルス対策	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	その他	この分野の技術開発に取り組む予定は無い	無回答
全　体		104	16	12	16	9	6	9	7	15	2	52	11
		100.0	15.4	11.5	15.4	8.7	5.8	8.7	6.7	14.4	1.9	50.0	10.6
属性	企業	27	4	3	5	3	1	5	3	3	−	16	1
		100.0	14.8	11.1	18.5	11.1	3.7	18.5	11.1	11.1	−	59.3	3.7
	大学	38	10	8	9	4	3	1	3	9	2	15	3
		100.0	26.3	21.1	23.7	10.5	7.9	2.6	7.9	23.7	5.3	39.5	7.9

問3. 今後もっとも力をいれていく分野

		調査数	暗号技術	認証技術	ネットワークセキュリティ	不正侵入対策	セキュリティマネジメント	ウイルス対策	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	その他	特にない	無回答
全　体		41	9	4	8	2	−	4	1	7	−	2	4
		100.0	22.0	9.8	19.5	4.9	−	9.8	2.4	17.1	−	4.9	9.8
属性	企業	10	3	−	3	−	−	2	1	1	−	−	−
		100.0	30.0	−	30.0	−	−	20.0	10.0	10.0	−	−	−
	大学	20	5	4	4	1	−	−	−	3	−	−	3
		100.0	25.0	20.0	20.0	5.0	−	−	−	15.0	−	−	15.0

問4. 現在実用化（製品化）されている分野

		調査数	暗号技術	認証技術	ネットワークセキュリティ	不正侵入対策	セキュリティマネジメント	ウイルス対策	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	その他	実用化（製品化）されていない	無回答
全　体		104	6	2	5	2	1	1	−	2	−	52	42
		100.0	5.8	1.9	4.8	1.9	1.0	1.0	−	1.9	−	50.0	40.4
属性	企業	27	4	2	3	1	−	1	−	1	−	10	12
		100.0	14.8	7.4	11.1	3.7	−	3.7	−	3.7	−	37.0	44.4
	大学	38	2	−	1	1	1	−	−	1	−	22	12
		100.0	5.3	−	2.6	2.6	2.6	−	−	2.6	−	57.9	31.6

問5.実用化（製品化）を見込んでいる分野

		調査数	暗号技術	認証技術	ネットワークセキュリティ	不正侵入対策	セキュリティマネジメント	ウイルス対策	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	その他	実用化（製品化）の予定は無い	無回答
全体		104	8	3	6	－	1	5	2	6	－	46	38
		100.0	7.7	2.9	5.8	－	1.0	4.8	1.9	5.8	－	44.2	36.5
属性	企業	27	2	1	1	－	1	4	1	1	－	10	11
		100.0	7.4	3.7	3.7	－	3.7	14.8	3.7	3.7	－	37.0	40.7
	大学	38	5	2	4	－	－	1	1	4	－	18	9
		100.0	13.2	5.3	10.5	－	－	2.6	2.6	10.5	－	47.4	23.7

問6.1.年間売上

		調査数	なし	10億円未満	10億円以上100億円未満	11,000億円未満	1,000億円以上	無回答
全体		104	14	3	2	5	1	79
		100.0	13.5	2.9	1.9	4.8	1.0	76.0
属性	企業	27	1	1	2	2	1	20
		100.0	3.7	3.7	7.4	7.4	3.7	74.1
	大学	38	11	－	－	1	－	26
		100.0	28.9	－	－	2.6	－	68.4

問6.2.アクセス制御関連の年間売上

		調査数	なし	1億円未満	1億円以上10億円未満	10億円以上100億円未満	100億円以上	無回答
全体		104	22	－	1	1	－	80
		100.0	21.2	－	1.0	1.0	－	76.9
属性	企業	27	4	－	1	1	－	21
		100.0	14.8	－	3.7	3.7	－	77.8
	大学	38	12	－	－	－	－	26
		100.0	31.6	－	－	－	－	68.4

問7.年間の研究開発費

		調査数	なし	1,000万円未満	1億円,000万円未満	1億円以上10億円未満	10億円以上100億円未満	100億円以上	無回答
全体		104	9	12	3	5	－	－	75
		100.0	8.7	11.5	2.9	4.8	－	－	72.1
属性	企業	27	1	－	－	5	－	－	21
		100.0	3.7	－	－	18.5	－	－	77.8
	大学	38	3	11	1	－	－	－	23
		100.0	7.9	28.9	2.6	－	－	－	60.5

問8.研究開発人員

		調査数	0人	1人以上5人未満	5人以上10人未満	10人以上20人未満	20人以上50人未満	50人以上100人未満	100人以上	無回答
全体		104	7	14	3	5	1	3	2	69
		100.0	6.7	13.5	2.9	4.8	1.0	2.9	1.9	66.3
属性	企業	27	1	−	3	−	1	3	1	18
		100.0	3.7	−	11.1	−	3.7	11.1	3.7	66.7
	大学	38	2	10	−	4	−	−	1	21
		100.0	5.3	26.3	−	10.5	−	−	2.6	55.3

2.2 回答用紙Bの集計表

問1. 何を守るか

		調査数	ネットワーク	サーバ	クライアント（PC等）	通信情報	データ	施設	その他
全体		5 100.0	1 20.0	3 60.0	2 40.0	2 40.0	4 80.0	－ －	1 20.0
属性	企業	5 100.0	1 20.0	3 60.0	2 40.0	2 40.0	4 80.0	－ －	1 20.0
	大学	－ －	－ －	－ －	－ －	－ －	－ －	－ －	－ －

問2. 何から守るか

		調査数	盗聴	漏えい	改ざん	なりすまし	事実否認	侵入	踏み台	Dos	ウイルス	その他
全体		5 100.0	4 80.0	4 80.0	3 60.0	3 60.0	－ －	2 40.0	－ －	－ －	－ －	－ －
属性	企業	5 100.0	4 80.0	4 80.0	3 60.0	3 60.0	－ －	2 40.0	－ －	－ －	－ －	－ －
	大学	－ －	－ －	－ －	－ －	－ －	－ －	－ －	－ －	－ －	－ －	－ －

問3. セキュリティ上の効果

		調査数	攻撃や不正操作等の早期検知・検出効果	攻撃や不正操作等に対する防御効果、抑止効果	被害箇所の局所化効果、拡大防止効果	被害箇所の自律的な回復・修復効果	その他
全体		5 100.0	4 80.0	5 100.0	1 20.0	1 20.0	－ －
属性	企業	5 100.0	4 80.0	5 100.0	1 20.0	1 20.0	－ －
	大学	－ －	－ －	－ －	－ －	－ －	－ －

問4. どんな機能を持っているか

		調査数	認証	証明書	認可	アクセス制御	暗号	検知	運用管理	評価	対外部者の監視	対内部者の監視	解析	その他
全体		5 100.0	4 80.0	1 20.0	3 60.0	5 100.0	4 80.0	3 60.0	2 40.0	－ －	1 20.0	1 20.0	－ －	－ －
属性	企業	5 100.0	4 80.0	1 20.0	3 60.0	5 100.0	4 80.0	3 60.0	2 40.0	－ －	1 20.0	1 20.0	－ －	－ －
	大学	－ －	－ －	－ －	－ －	－ －	－ －	－ －	－ －	－ －	－ －	－ －	－ －	－ －

問5. どのようなレイヤーセキュリティを守るか

		調査数	物理層	データリンク層	ネットワーク層	トランスポート層	セッション層	プレゼンテーション層	アプリケーション層
全体		5 100.0	－ －	1 20.0	2 40.0	2 40.0	－ －	－ －	4 80.0
属性	企業	5 100.0	－ －	1 20.0	2 40.0	2 40.0	－ －	－ －	4 80.0
	大学	－ －	－ －	－ －	－ －	－ －	－ －	－ －	－ －

問6. 不正アクセスからの防御対象

		調査数	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
全体		5 100.0	3 60.0	1 20.0	2 40.0	－ －	－ －	3 60.0
属性	企業	5 100.0	3 60.0	1 20.0	2 40.0	－ －	－ －	3 60.0
	大学	－ －	－ －	－ －	－ －	－ －	－ －	－ －

問7. サービスについて

		調査数	教育	アウトソース	インテグレーション	コンサルティング	保守（サポート）	サービスプロバイダ	保険	その他	無回答
全体		5 100.0	－ －	－ －	1 20	－ －	－ －	1 20	－ －	－ －	4 80.0
属性	企業	5 100.0	－ －	－ －	1 20	－ －	－ －	1 20	－ －	－ －	4 80.0
	大学	－ －	－ －	－ －	－ －	－ －	－ －	－ －	－ －	－ －	－ －

2.3 回答用紙Cの集計表

問1. 何を守るか

		調査数	ネットワーク	サーバ	クライアント（PC等）	通信情報	データ	施設	その他
全体		20	5	9	9	9	11	−	−
		100.0	25.0	45.0	45.0	45.0	55.0	−	−
属性	企業	2	−	1	1	1	2	−	−
		100.0	−	50.0	50.0	50.0	100.0	−	−
	大学	18	5	8	8	8	9	−	−
		100.0	27.8	44.4	44.4	44.4	50.0	−	−

問2. 何から守るか

		調査数	盗聴	漏えい	改ざん	なりすまし	事実否認	侵入	踏み台	Dos	ウイルス	その他	無回答
全体		20	6	6	5	8	2	9	3	5	2	−	1
		100.0	30.0	30.0	25.0	40.0	10.0	45.0	15.0	25.0	10.0	−	5.0
属性	企業	2	1	−	1	1	−	1	1	−	1	−	−
		100.0	50.0	−	50.0	50.0	−	50.0	50.0	−	50.0	−	−
	大学	18	5	6	4	7	2	8	2	5	1	−	1
		100.0	27.8	33.3	22.2	38.9	11.1	44.4	11.1	27.8	5.6	−	5.6

問3. セキュリティ上の効果

		調査数	攻撃や不正操作等の早期検知・検出効果	攻撃や不正操作等に対する防御効果、抑止効果	被害箇所の局所化効果、拡大防止効果	被害箇所の自律的な回復・修復効果	その他	無回答
全体		20	8	16	2	1	−	1
		100.0	40.0	80.0	10.0	5.0	−	5.0
属性	企業	2	−	2	−	1	−	−
		100.0	−	100.0	−	50.0	−	−
	大学	18	8	14	2	−	−	1
		100.0	44.4	77.8	11.1	−	−	5.6

問4. どんな機能を持っているか

		調査数	認証	証明書	認可	アクセス制御	暗号	検知	運用管理	評価	対外部者の監視	対内部者の監視	解析	その他
全体		20	9	3	3	9	6	6	4	−	1	1	2	1
		100.0	45.0	15.0	15.0	45.0	30.0	30.0	20.0	−	5.0	5.0	10.0	5.0
属性	企業	2	2	−	−	1	1	−	−	−	1	−	−	−
		100.0	100.0	−	−	50.0	50.0	−	−	−	50.0	−	−	−
	大学	18	7	3	3	8	5	6	4	−	−	1	2	1
		100.0	38.9	16.7	16.7	44.4	27.8	33.3	22.2	−	−	5.6	11.1	5.6

問5. どのようなレイヤーのセキュリティを守るか

		調査数	物理層	データリンク層	ネットワーク層	トランスポート層	セッション層	プレゼンテーション層	アプリケーション層	無回答
全体		20 100.0	1 5.0	4 20.0	5 25.0	4 20.0	1 5.0	2 10.0	15 75.0	1 5.0
属性	企業	2 100.0	－ －	－ －	－ －	－ －	－ －	－ －	2 100.0	－ －
	大学	18 100.0	1 5.6	4 22.2	5 27.8	4 22.2	1 5.6	2 11.1	13 72.2	1 5.6

問6. 不正アクセスからの防御対象

		調査数	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
全体		20 100.0	8 40.0	4 20.0	4 20.0	1 5.0	2 10.0	11 55.0
属性	企業	2 100.0	1 50.0	1 50.0	－ －	－ －	1 50.0	2 100.0
	大学	18 100.0	7 38.9	3 16.7	4 22.2	1 5.6	1 5.6	9 50.0

問7. 目指している研究成果

		調査数	理論（アルゴリズム、手法、評価など）	開発（システム構築、実装、プロトコルなど）	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））	その他
全体		20 100.0	12 60.0	14 70.0	7 35.0	－ －
属性	企業	2 100.0	－ －	2 100.0	1 50	－ －
	大学	18 100.0	12 66.7	12 66.7	6 33.3	－ －

問8. サービスについて

		調査数	教育	アウトソース	インテグレーション	コンサルティング	保守（サポート）	サービスプロバイダ	保険	その他	無回答
全体		20 100.0	1 5.0	－ －	2 10.0	－ －	2 10.0	2 10.0	－ －	－ －	16 80.0
属性	企業	2 100.0	－ －	－ －	1 50	－ －	－ －	1 50	－ －	－ －	1 50.0
	大学	18 100.0	1 5.6	－ －	1 5.6	－ －	2 11.1	1 5.6	－ －	－ －	15 83.3

問9. 進捗状況

		調査数	1年以内に商用化・実用化が成される段階である	1～3年以内に商用化・実用化が成される段階である	商用化・実用化は3年より先になるという段階である	直接商用化・実用化に結びつくものではない
全体		20 100.0	3 15.0	2 10.0	8 40.0	7 35.0
属性	企業	2 100.0	1 50	1 50.0	－ －	－ －
	大学	18 100.0	2 11.1	1 5.6	8 44.4	7 38.9