「情報処理安全確保支援士（登録セキスペ）の活動に関する実態調査」

調査報告書

令和元年 7 月

独立行政法人情報処理推進機構

目次

1. 調査概要

1.1. 調査背景と目的

サイバー攻撃の増加・高度化に加え、社会的なIT依存度の高まりから、企業・組織におけるサイバーセキュリティ[1]対策の重要性が高まっている。それに伴い、企業・組織での安全なセキュリティ対策を高度なスキルを活かして推進できる人材が求められている。

このため、最新の知識・技能を備え、サイバーセキュリティ対策を推進する人材の育成と確保を目指し、サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律（平成28年法律第31号）が2016年10月21日に施行され、新たな国家資格「情報処理安全確保支援士」制度が創設された。

独立行政法人情報処理推進機構（以下「IPA」という。）では、情報処理安全確保支援士制度の運営機関として、試験、登録、講習の運営及び制度の普及活動を行っている。制度創設から3年が経過し、2019年4月1日には登録人数が合計で18,000名を超える規模となった。

本調査は、適切なサイバーセキュリティ対策の実現に必要となる制度や制度の在り方を検討することを将来課題とし、情報処理安全確保支援士の資格保持者（以下、登録セキスペという）に対して実態調査を実施したものである。

なお、アンケート調査の実施、集計・分析の一部をみずほ情報総研株式会社への委託事業として行った。

1.2. 調査内容

実施した調査内容を示す。

1.2.1. アンケート調査の実施概要

今回のアンケート調査では、登録セキスペ本人の他に、比較対象として高度IT人材（情報処理技術者試験のうち高度試験の合格者等）にも同様の質問を行った。また、登録セキスペが所属する組織の組織長にもアンケート調査を行った。3種類のアンケート調査の実施概要は次のとおりである。

(1) 登録セキスペを対象とした実態調査

アンケート調査の実施概要を表1-1に示す。

[1] 本報告書では、「サイバーセキュリティ」と「情報セキュリティ」は同義とする。

表 1-1 登録セキスペを対象とした実態調査

調査対象	登録セキスペ（2018 年 12 月時点。連絡が取れない者などを除く）
送付数	17,020 名
依頼方法	電子メールで個別に依頼
回答方法	Web アンケート調査画面又は Excel ワークシート形式の調査票への記入
実施期間	2018 年 12 月 26 日～2019 年 1 月 21 日
回収サンプル数	8,266 サンプル（回収率 48.6%）[2]

(2) 「高度IT人材」を対象とした実態調査

アンケート調査の実施概要を表 1-2 に示す。

表 1-2 「高度 IT 人材」を対象とした実態調査

調査対象	アンケートサービス企業にモニタ登録している企業等勤務者のうち、次のいずれかの条件を満たす人を「高度 IT 人材」として抽出: 条件①情報処理技術者試験のうち高度試験の合格者（登録セキスペを除く） 条件②IT 関連業務に従事しつつ、部下を指導できるチームリーダーレベル以上のスキル・能力を発揮している人
スクリーニング対象者	20,000 名
依頼方法	アンケートサービス企業から依頼
回答方法	Web アンケート調査画面への記入
実施期間	2019 年 2 月 8 日～2019 年 2 月 14 日
回収サンプル数	1,000 サンプル

※以降、本調査対象者を「高度 IT 人材」と呼ぶ

(3) 登録セキスペ所属組織の組織長を対象とした実態調査

アンケート調査の実施概要を表 1-3 に示す。

表 1-3 登録セキスペの所属組織の組織長を対象とした実態調査

調査対象	(1)のアンケートにおいて、「組織長を紹介可能」と回答した登録セキスペの所属組織の組織長（経営層と登録セキスペの双方に接点のある人。本人が登録セキスペである場合を除く）
送付数	561 名
依頼方法	電子メールで個別に依頼
回答方法	Web アンケート調査画面又は Excel ワークシート形式の調査票への記入
実施期間	2019 年 1 月 29 日～2019 年 2 月 13 日
回収サンプル数	170 サンプル（回収率 30.3%）

[2] 途中までの回答者を含む。全設問に回答した人数は、7,537 名（回収率 44.3%）。

1.2.2. 主な調査項目

主な調査項目は次のとおりである。

- 所属組織（企業・団体等）や部署について（業種、組織規模等）
- 担当業務や役割について（担当している IT 関連業務、セキュリティ対策関連業務等）
- 業務遂行における活用スキル
- 業務遂行におけるコミュニケーション状況（自組織内、自組織外）
- 業務遂行上の課題（業務の難易度とその要因等）
- 今後の展望（強化したい知識・スキルや取り組み等）
- 登録セキスペ制度の活用（登録のきっかけ、登録セキスペ制度のメリット等）

2. 調査結果の集計

次に、3 種類のアンケート調査において取得した回答内容の集計結果を示す。[3]

2.1. 登録セキスペの所属組織と役職

登録セキスペ及び高度 IT 人材に対し、職業、所属企業・団体、その規模（従業員数）、役職を質問した。

2.1.1. 回答者の職業

登録セキスペも高度 IT 人材も、回答者の 9 割程度が企業や民間の企業・団体で正社員や役員として勤務しており、個人事業主等は少なかった。

（設問文：あなたの職業として、最も近いものを 1 つ選択してください。兼業または出向されている方は、最も従事時間の長いものについてご回答ください）

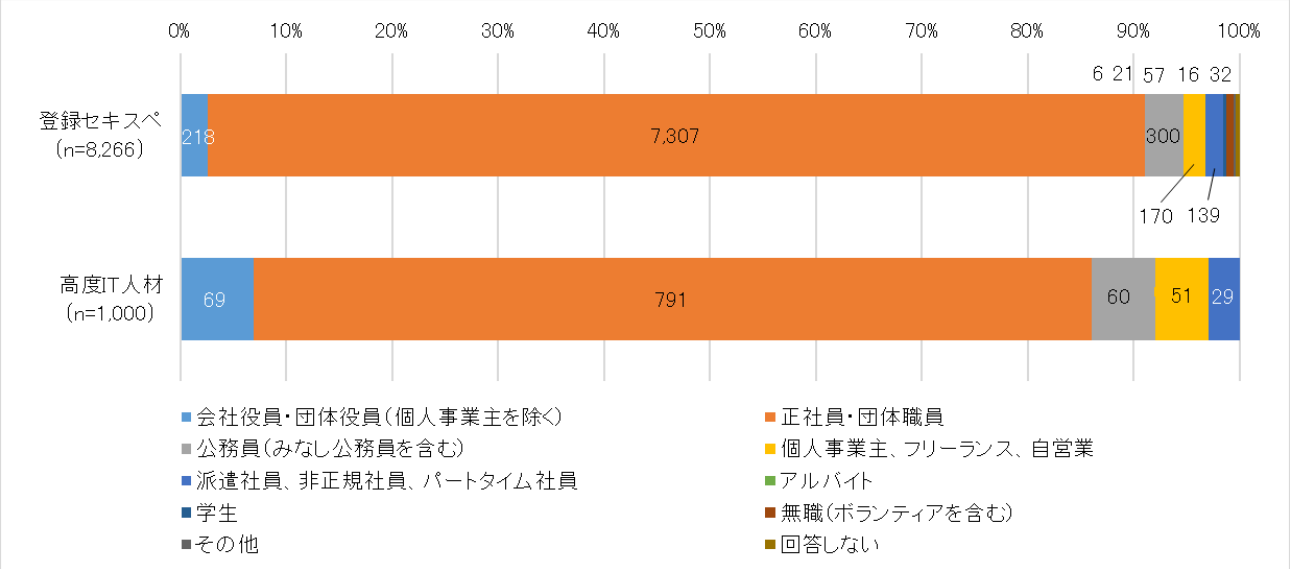


図 2-1 回答者の職業

[3] 本アンケート調査は、途中までの回答者を含むため、設問により n 値が異なる。

2.1.2. 所属組織の業種

（2.1.2, 2.1.3 の設問は、2.1.1 において、職業が「会社役員・団体役員、正社員・団体職員、公務員、個人事業主・フリーランス・自営業、派遣社員・非正規社員・パートタイム社員」と回答した人を対象に質問している）

登録セキスペは、IT 系の業種（情報処理・提供サービス業、ソフトウェア業、コンピュータ及び周辺機器製造または販売業）の所属者の割合が多く、3 業種合計で 67.2%を占めている。非 IT 系業種の所属者の割合は 32.3%であるが、業種別に見ると、例えば、「製造業」所属者の割合は 7.1%、576 名、「金融業・保険業、不動産業・物品賃貸業」所属者の割合は 2.9%、234 名となっている。

高度 IT 人材では、IT 系 3 業種の所属者の割合は 43.6%で、登録セキスペと比較して少ない割合である。

（設問文：従事されている業務の業種として、次の中から最も近いものを 1 つ選んでください。※複数の事業を行っている企業や団体に所属している場合は、あなたが所属している部署で行っている事業における業種として、最も近いものを 1 つご回答ください。）

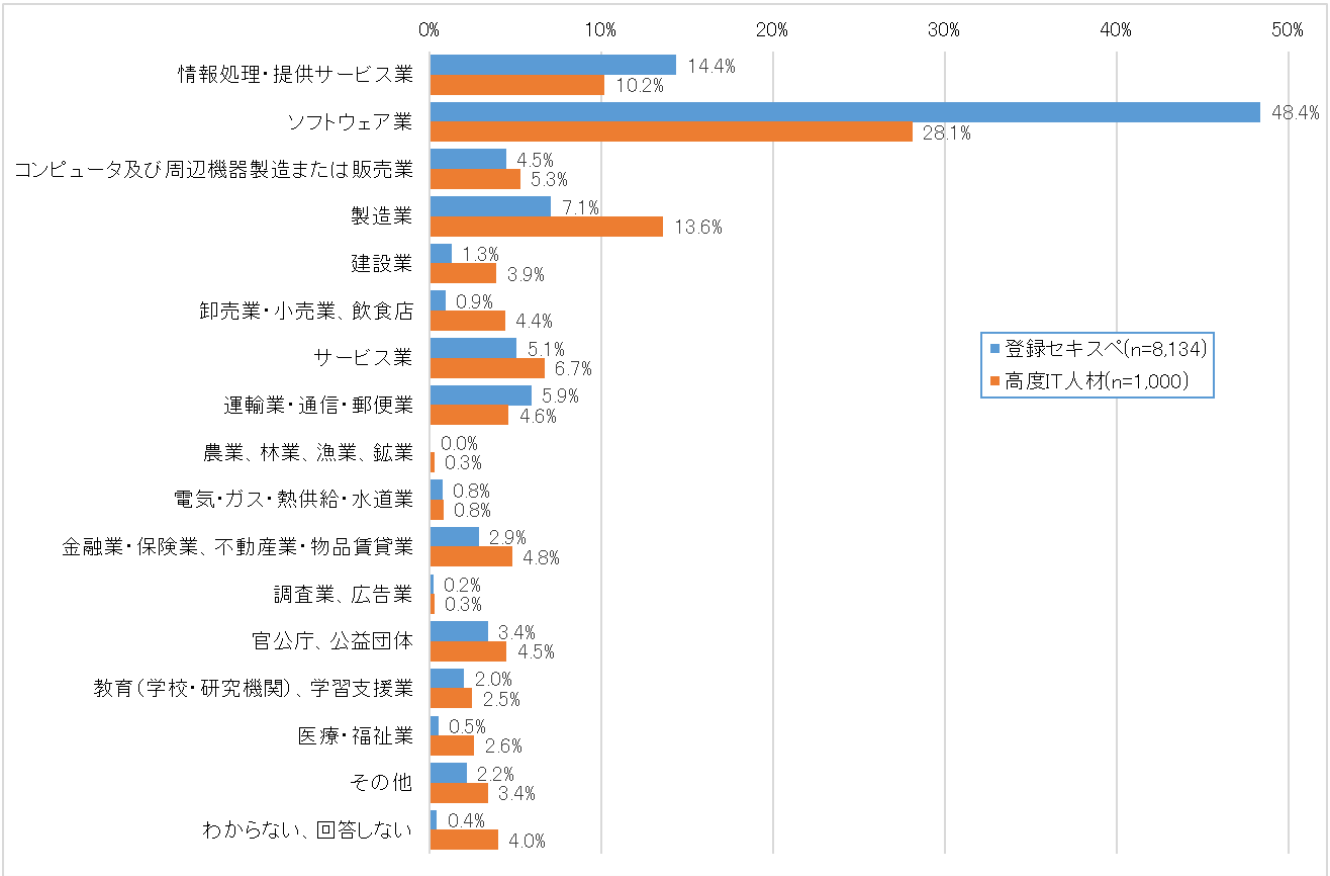


図 2-2 所属組織の業種

2.1.3. 所属組織の規模(従業員数)

登録セキスペは、高度 IT 人材と比較して 1,000 名以上の企業に所属している者の割合が 55.8%と高い。

(設問文:所属する企業・団体の総従業員数として、あてはまるものを 1 つ選んでください。※正社員以外の雇用形態の社員を含み、派遣社員を除いてください。※複数の事業を行っている企業や団体に所属している場合は、あなたが所属している部署の行っている事業に従事する人数をご回答ください。)

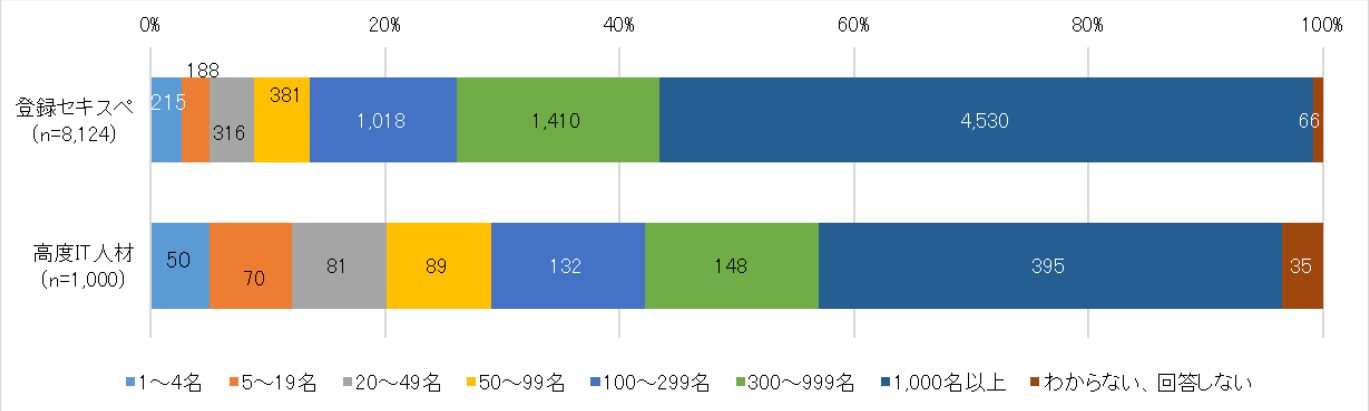


図 2-3 所属組織の規模

2.1.4. 役職

企業・団体に勤務する人を対象に、役職を確認した。登録セキスペは一般社員～係長・主任クラスの役職の人で約 7 割を占めた。これに対し、高度 IT 人材は一般社員～係長・主任クラスの役職の人は 5 割程度であり、課長職以上の役割を担う人が半数近くいた。

(設問文:あなたの役職として、最も近いものを 1 つ選択してください。なお、部下がいるかどうかは問いません。)

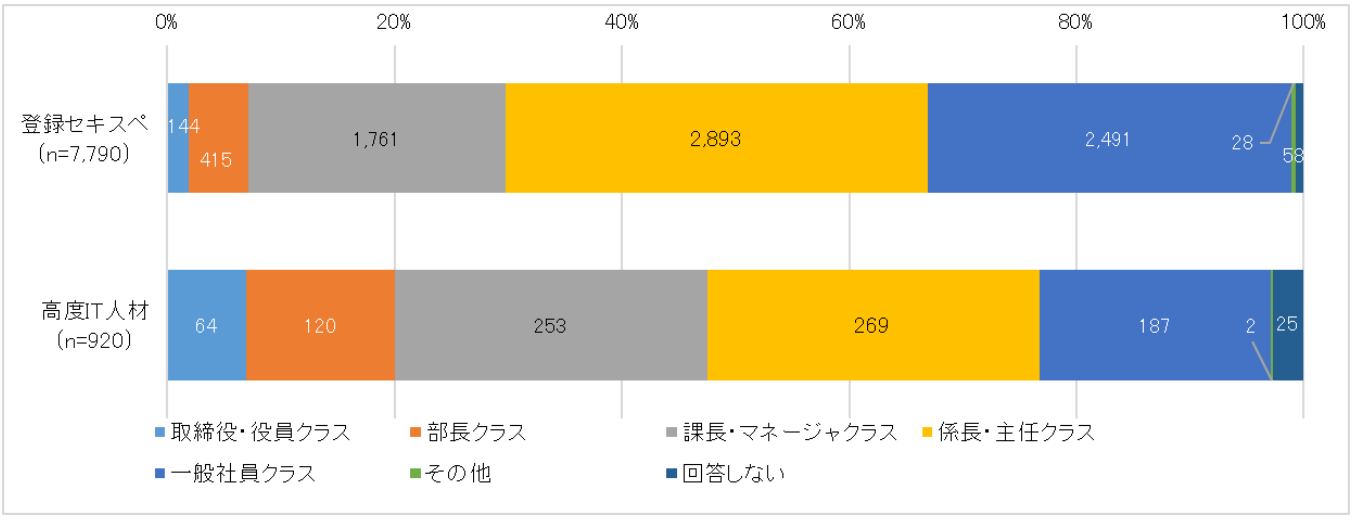


図 2-4 役職

高度 IT 人材回答者の平均年齢は、46.9 歳であった。これに対し、登録セキスペ回答者の平均年齢は、42.1 歳である。役職の分布の違いは、年齢層のずれなどが影響していると考えられる。

2.2. 登録セキスペの所属部署・ミッションについて

登録セキスペ及び高度 IT 人材の、所属部署について質問した。

（質問対象は、2.1.1 において、「会社役員・団体役員、正社員・団体職員、公務員、個人事業主・フリーランス・自営業、派遣社員・非正規社員・パートタイム社員」と回答した人）。

2.2.1. 所属部署

所属部署を、組織経営、スタッフ（間接部門）、事業遂行（直接部門）、その他に分類すると図 2-5 のとおりとなった。

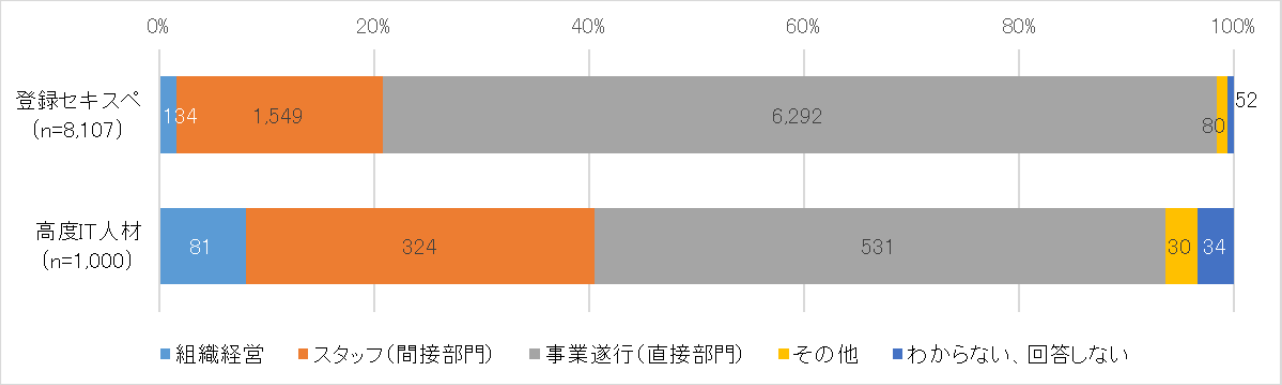


図 2-5 所属部署（分類別）

さらに所属部署別の人数を見ると、スタッフ（間接部門）所属の登録セキスペは自組織向け情報システム関連部門所属者が最も多く、高度 IT 人材では総務系の部門所属者が最も多かった。

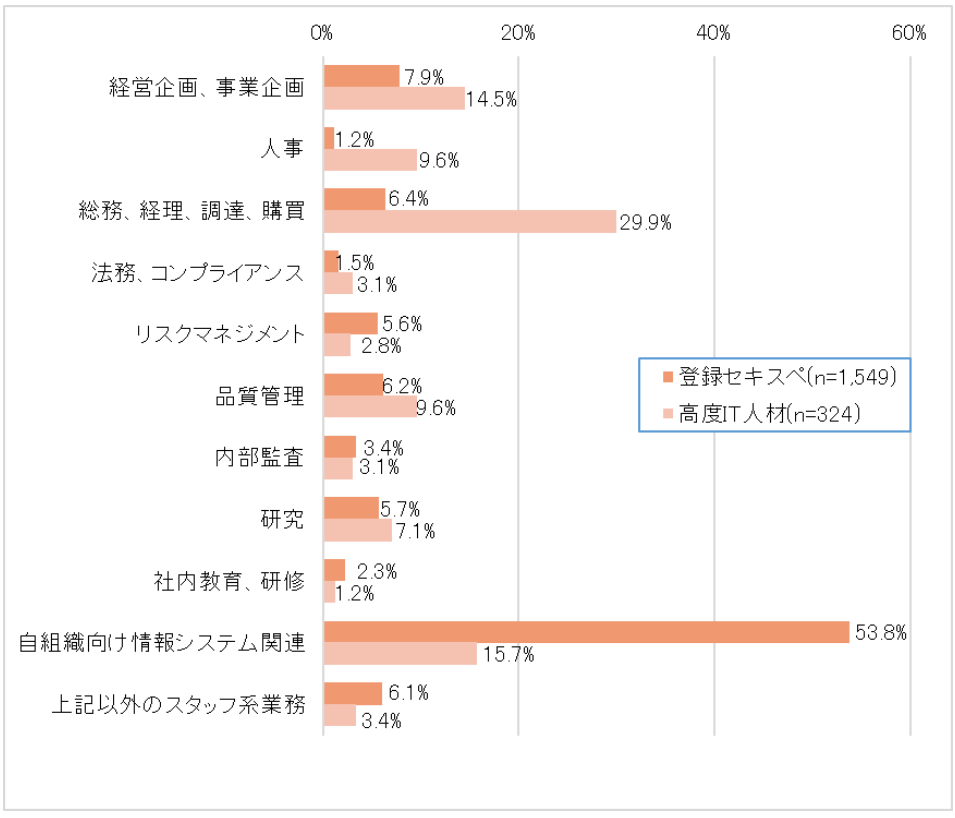


図 2-6 所属部署（スタッフ（間接部門）のみ）

事業遂行(直接部門)所属の登録セキスペ・高度 IT 人材は、どちらも IT システム・サービス関連部門所属者が最も多かった。

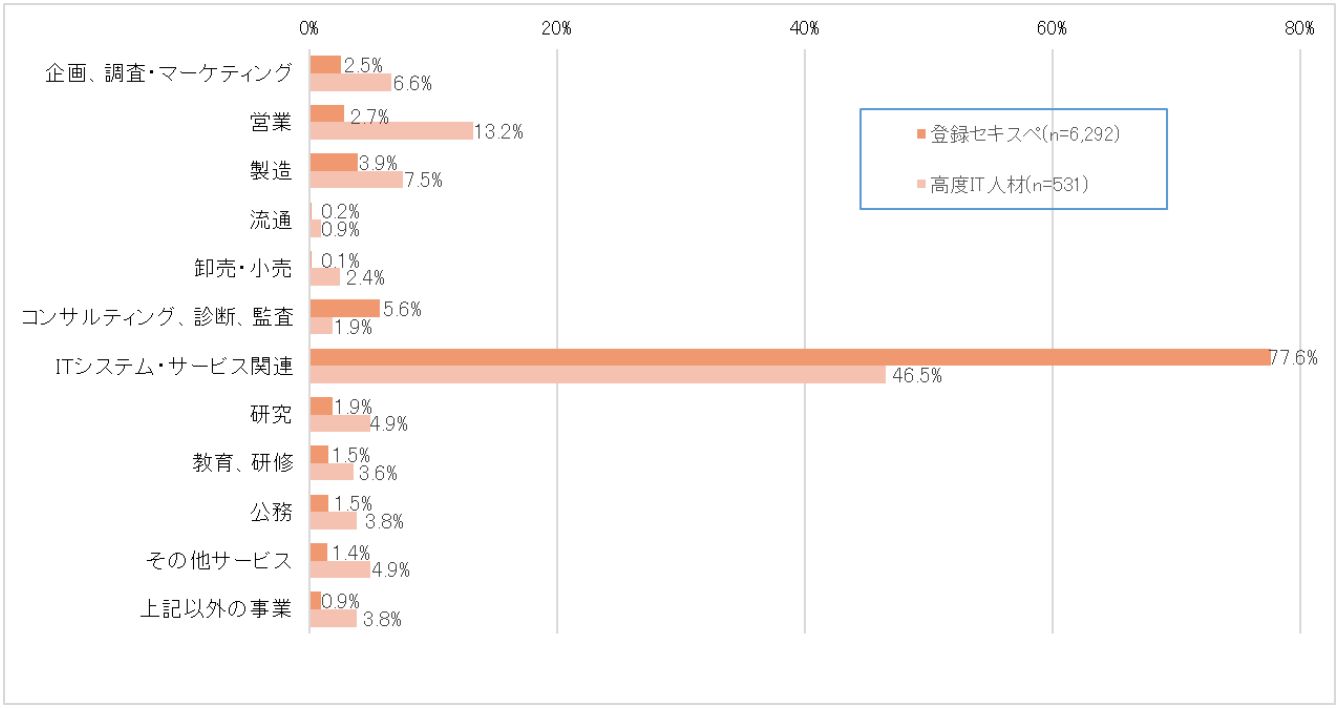


図 2-7 所属部署(事業遂行(直接部門)のみ)

2.2.2. 所属部署のサイバーセキュリティ対策との関わり

スタッフ(間接部門)と事業遂行(直接部門)の所属者に対し、所属部署のサイバーセキュリティ対策との関わりを確認した。

(設問文:あなたが所属している部署は、情報セキュリティ対策にどのような形で関わっていますか。最も近いものを 1 つ選択してください。)[4,5]

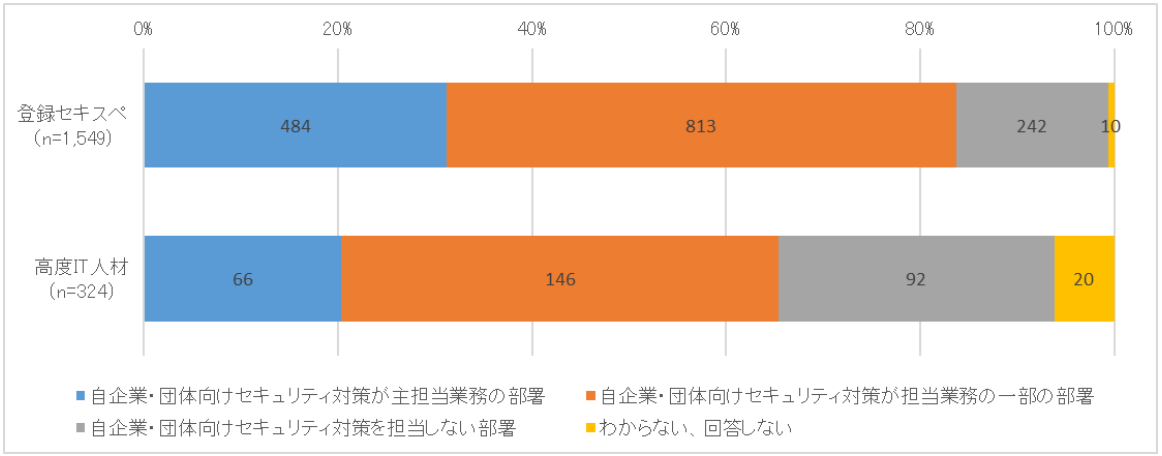


図 2-8 サイバーセキュリティ対策との関わり(スタッフ(間接部門))

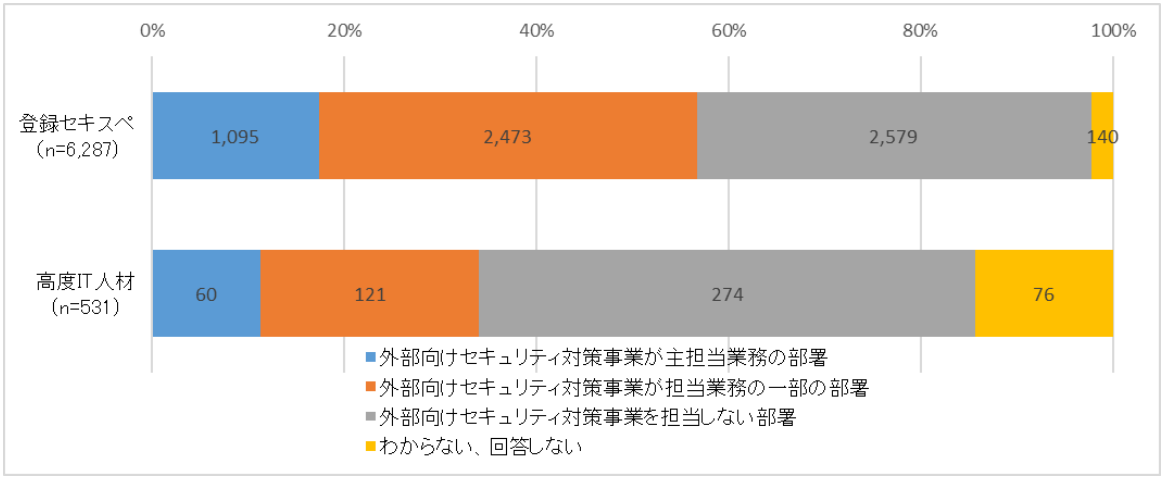


図 2-9 サイバーセキュリティ対策との関わり(事業遂行(直接部門))

図 2-9 から、事業遂行(直接部門)に所属する登録セキスペの約 4 割、高度 IT 人材の約 5 割が「サイバーセキュリティ対策に関するサービス提供や製品販売を行っていない部署に所属している」と回答している。この方々については、2.2.3 に追加の集計データを掲載する。

---

[4] 選択肢の文章は、次のとおり。
- 自企業・団体やグループの情報セキュリティ対策を主たる担当業務とする部署である
- 自企業・団体やグループの情報セキュリティ対策を担当業務の一部に含む部署である
- 情報セキュリティ対策に関わらない部署である
- わからない、回答しない

[5] 選択肢の文章は、次のとおり。
- 情報セキュリティ対策サービス提供や関連製品販売等の外部向け事業を主たる担当業務とする部署である
- 情報セキュリティ対策サービス提供や関連製品販売等の外部向け事業を担当業務の一部に含む部署である
- 情報セキュリティ対策の外部向け事業には関わらない部署である
- わからない、回答しない

所属部署の種別によって、サイバーセキュリティ対策との関わりがどのように異なるかを調べるために、クロス集計を行った（登録セキスペの回答データのみ）。

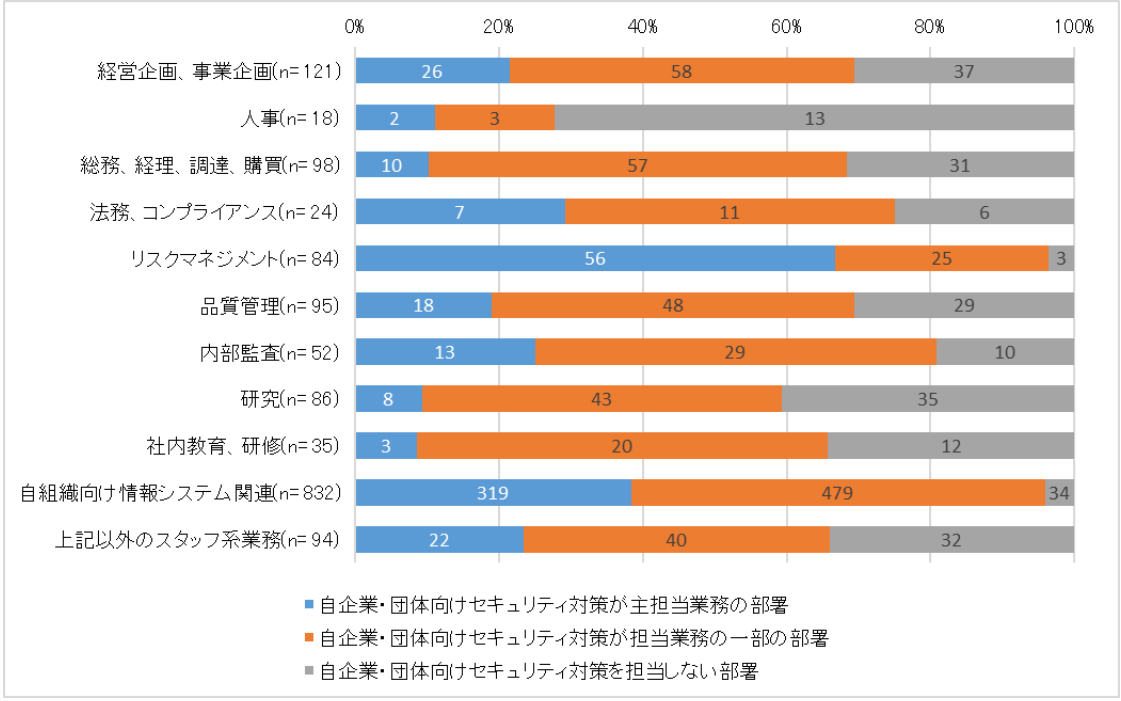


図 2-10 所属部署のサイバーセキュリティ対策との関わり（スタッフ（間接部門））

図 2-10 からは、リスクマネジメント部門は、自組織・団体のサイバーセキュリティ対策を主担当業務として担当していることが多い（6 割以上）ことが分かる。他の部門は、業務の一部に自組織・団体のサイバーセキュリティ対策が含まれていることの方が比較的多い。

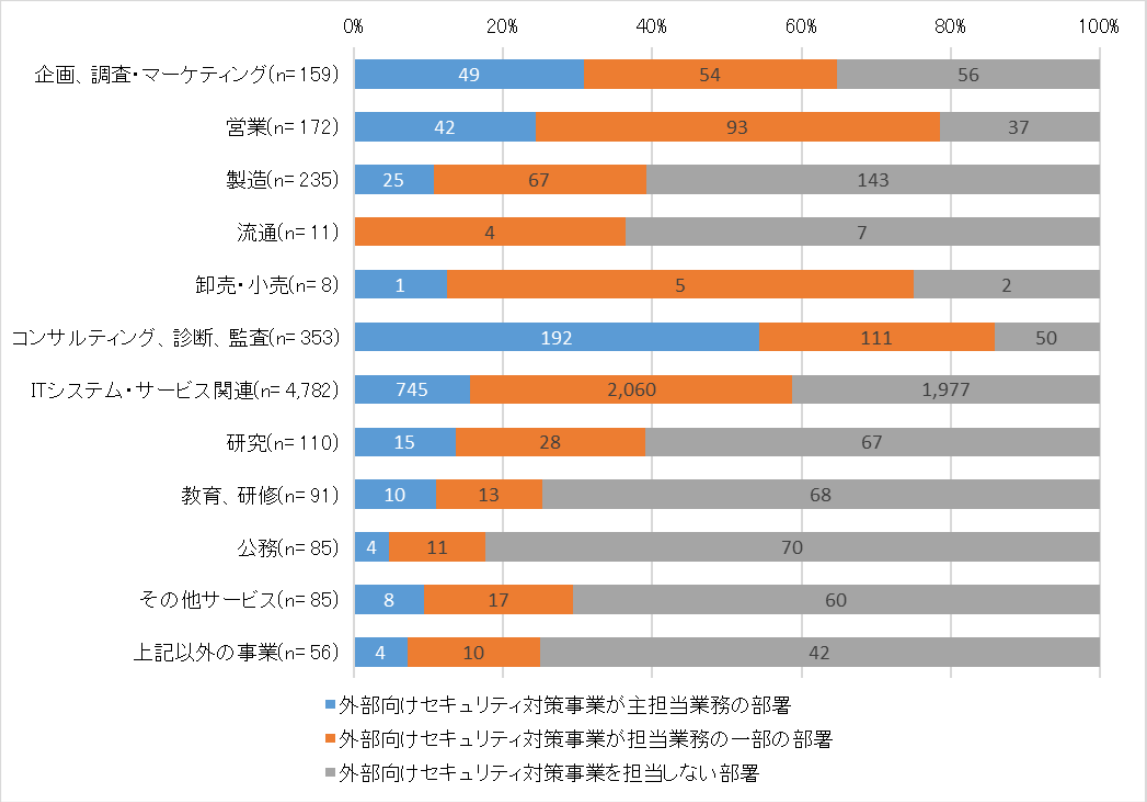


図 2-11 所属部署のサイバーセキュリティ対策との関わり(事業遂行(直接部門))

図 2-11 を見ると、「外部向けセキュリティ対策事業が主担当業務」と回答する割合が最も多かったのは、「コンサルティング、診断、監査」で約 5 割。セキュリティコンサルタントやセキュリティ監査などの部門であることが想定される。他の部門は、「外部向けセキュリティ対策事業が担当業務の一部」又は「外部向けセキュリティ対策事業を担当しない部署」と回答する割合が高い。これらから、セキュリティ対策事業を専門で行っている部署は少なく、主担当業務の一部としてサイバーセキュリティ対策サービスを提供していることが多いという実態がうかがえる。

2.2.3. サイバーセキュリティ対策を担当しない部署に所属する登録セキスペについて

スタッフ(間接部門)(図 2-10)及び事業遂行(直接部門)(図 2-11)の両方で、サイバーセキュリティ対策が部署のミッションに含まれていない登録セキスペの人が少なからずいる。これらの方々がサイバーセキュリティ対策関連業務を担当しているのかどうかを確認した。

スタッフ(間接部門)において「自組織・団体のサイバーセキュリティ対策を担当しない部署」に所属すると答えた 242 名について、サイバーセキュリティ対策業務の担当状況を確認したところ(本設問の詳細は 2.3.4 に記載)、図 2-12 のとおり、約半数が何らかのサイバーセキュリティ対策業務を担当していた。

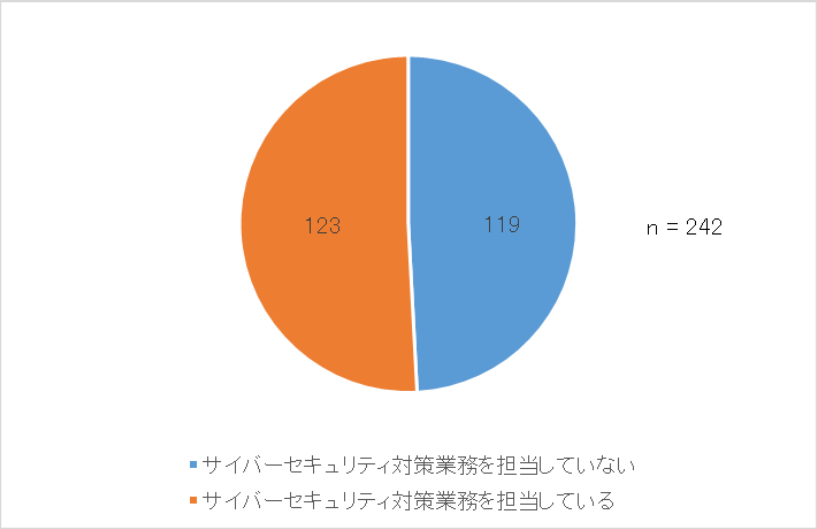


図 2-12　サイバーセキュリティ対策業務担当状況

(サイバーセキュリティ対策を担当しないスタッフ(間接部門)所属の登録セキスペ)

また、事業遂行(直接部門)において「外部向けセキュリティ対策事業を担当しない部署」に所属すると答えた 2,579 名についても同様に、サイバーセキュリティ対策業務の担当状況を確認したところ(本設問の詳細は 2.3.4 に記載)、図 2-13 のとおり、約 7 割が何らかのサイバーセキュリティ対策業務を担当していた。

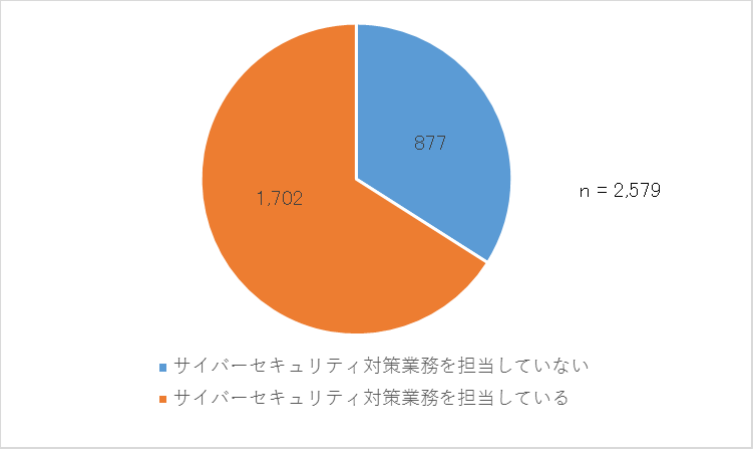


図 2-13　サイバーセキュリティ対策業務担当状況

(サイバーセキュリティ対策事業を行わない所属部署の登録セキスペ)

これらから、登録セキスペなどのサイバーセキュリティ対策に関わる人材は、サイバーセキュリティ対策をミッションとする部署だけでなく、サイバーセキュリティ対策がミッションに含まれない部署にもいることが分かる。業務遂行の中で、切り離せないものとしてサイバーセキュリティ対策が実行されており、それを高度なセキュリティの知識・スキルを持って支える人材が、様々な部門の中にいることが示されている。

2.3. 登録セキスペの担当業務

登録セキスペ及び高度 IT 人材に対し、IT やサイバーセキュリティ対策において担当する業務、CSIRT 担当状況を質問した（質問対象は、2.1.1 において、「会社役員・団体役員、正社員・団体職員、公務員、個人事業主・フリーランス・自営業、派遣社員・非正規社員・パートタイム社員」と回答した人）。

2.3.1. 担当業務の IT システム・サービスとの関わり

まず、担当業務において、IT システム・サービスとどのように関わっているかを確認した。本設問は複数選択可としている。

（設問文：あなたの担当業務では、どのような IT システム・サービスにどのように関わっていますか？関わりをすべて選択してください。：複数選択）[6]

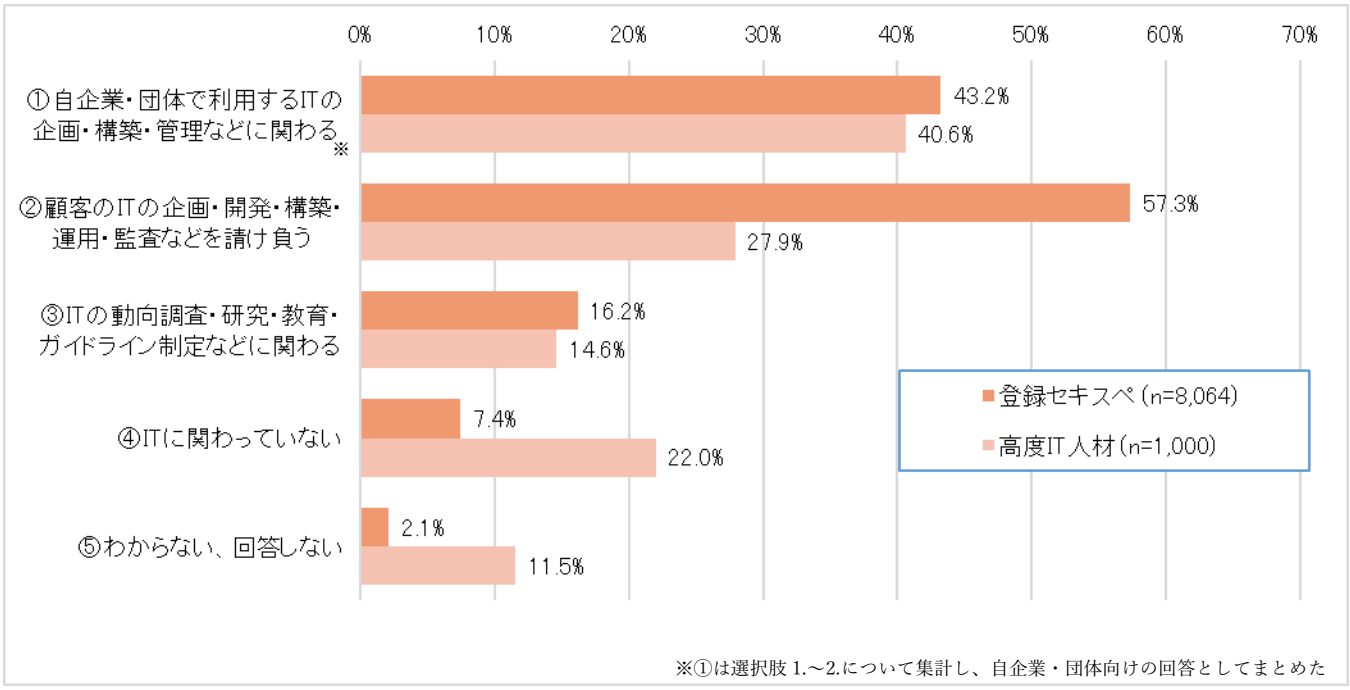


図 2-14 担当業務における IT システム・サービスとの関わり

[6] 選択肢の文章は、次のとおり。
1.自企業・団体の内部向け IT システム・サービス※の企画・構築・管理などに関わっている
（※内部向け IT システム・サービスとは、いわゆる「コーポレート IT」の分野で、人事、経理システム等の社内システムを指す）
2.自企業・団体の外部向け IT システム・サービス※の企画・構築・管理などに関わっている
（※外部向け IT システム・サービスとは、いわゆる「ビジネス IT」の分野で、オンラインショッピングサイト等の対外システムを指す）
3.顧客が使う IT システム・サービスの企画・開発・構築・運用・監査などを請け負っている（例：ベンダとしてのシステムの受託開発）
4.IT システム・サービスの動向調査、研究、教育、ガイドライン等の制定に関わっている
5.IT システム・サービスには関わっていない
6.わからない、回答しない

登録セキスペでは、顧客への IT システム・サービス提供に関わる、いわゆる IT ベンダ系の業務担当者(②)が 6 割弱と最も多く、次いで多かったのは、業務で活用する IT の企画・構築・管理に関わる人(①、4 割強)であった。つまり、顧客の IT を守る登録セキスペだけでなく、自組織・団体の IT を守る登録セキスペも多いことが分かる。

高度 IT 人材は、登録セキスペと比較して、IT ベンダ系の業務担当者の割合が大幅に少なかった。高度 IT 人材の業種分布(図 2-2)をみると IT 系企業の割合が登録セキスペと比較して少ないため、その影響が表れていると思われる。

図 2-14 の①を細分化し、業務で活用する IT の種別を、組織内で活用するシステム(以降、コーポレート IT と呼ぶ)と社外取引などの対外システム(以降、ビジネス IT と呼ぶ)に分けると、図 2-15 のようになる。

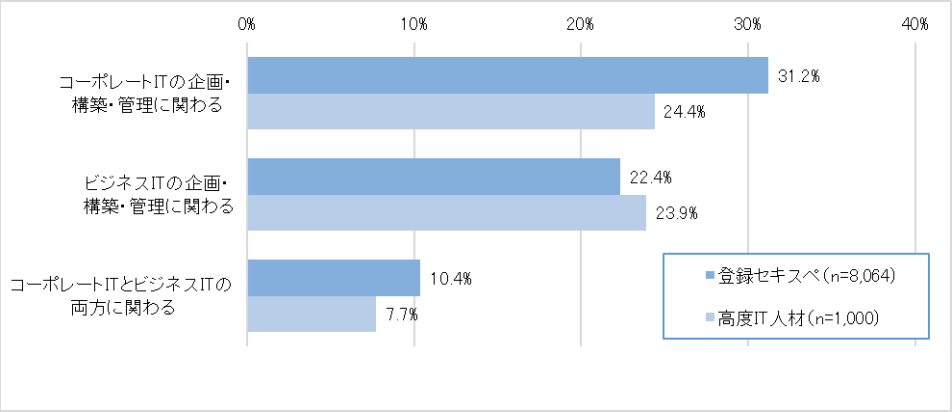


図 2-15 担当業務における IT システム・サービスとの関わり(図 2-14①の細分化)

登録セキスペの自組織で活用する IT に関わる人では、コーポレート IT に関わる人が回答者の 3 割と最も多かったが、ビジネス IT に関わる人も 22.4%いた。今後、デジタルトランスフォーメーション(通称:DX)[7]の進展によってお客様のフロントライン業務の IT 化が進むと、ビジネス IT のセキュリティ対策を担う登録セキスペが増えていくことが予測される。

IT システム・サービスとの関わりの違いによって、サイバーセキュリティ対策業務の目的が大きく異なるため、以降の分析は、次の(A)～(D)にグループ分けして実施する。

(A) コーポレート IT の企画・構築・管理に関わる人 (以下、コーポレート IT)

(B) ビジネス IT の企画・構築・管理に関わる人 (以下、ビジネス IT)

(C) 顧客 IT の企画・開発・構築・運用・監査などを請け負う人 (以下、IT ベンダ)

(D) IT の動向調査・研究・教育・ガイドライン制定などに関わる人 (以下、IT 調査研究・教育他)

補足するが、IT との関わりは複数選択できるため、各グループの間には重なりがある(同じ人が複数のグループに属している)。それぞれのグループの重なり具合は図 2-16 のとおりである。特に(B)ビジネス IT や(D)IT 調査研究・教育他において重なりが大きいため、(B)ビジネス IT は(A)コーポレート IT とまとめて担当している人が多いことや、他の業務を行いながら調査、研究、教育などを担当している人が多いことなどが分かる。

[7] 企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の有意性を確立すること(経済産業省:デジタルトランスフォーメーションを推進するためのガイドライン(DX 推進ガイドライン) Ver.1.0 https://www.meti.go.jp/press/2018/12/20181212004/20181212004-1.pdf)

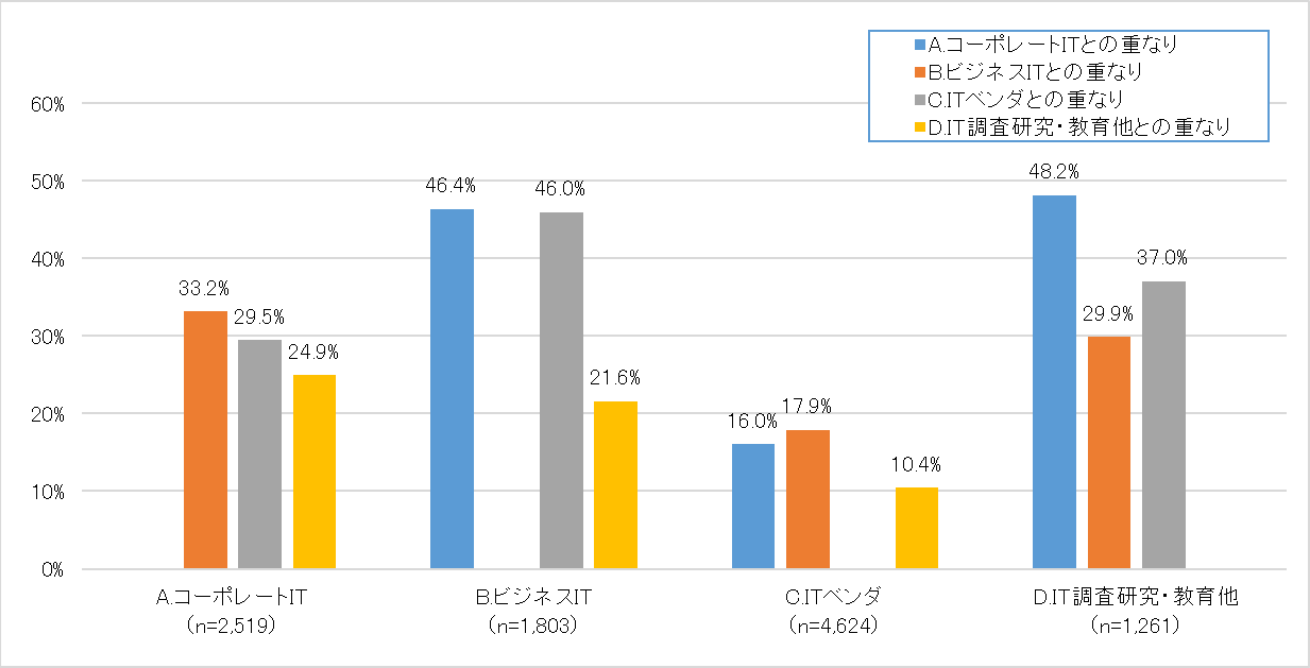


図 2-16　グループ間の重なりの割合（登録セキスペのみ）

2.3.2.　担当する IT 関連業務（主たる業務）

8 種類の IT 関連業務を定義し、登録セキスペ及び高度 IT 人材がどの業務を担当しているかを質問し、前述の(A)～(D)にグループ分けして集計した。質問対象は、2.3.1 の設問で、「IT システム・サービスには関わっていない」、「わからない、回答しない」の選択者及び無回答者以外で、登録セキスペは 7,289 名、高度 IT 技術者は 665 名である。

（設問文：以下の IT システム・サービスに関連する業務のうち、あなたが担当している役割として、以下の 2.～4.の中から最も近いものをそれぞれ 1 つ選択してください。なお、担当していない業務については「1.担当していない」を選択してください。）[8]

（設問文：前問でお答えの中で、主たる業務を 1 つ選択してください。）

まずは、主たる業務の回答内容を図 2-17 に示す。

[8] 役割の選択肢は次のとおり。
1.担当していない
2.責任者・管理者（実務より管理業務が主体）
3.主導的な実務者（責任者を兼ねる場合も含む）
4.補佐的な実務者
5.回答しない

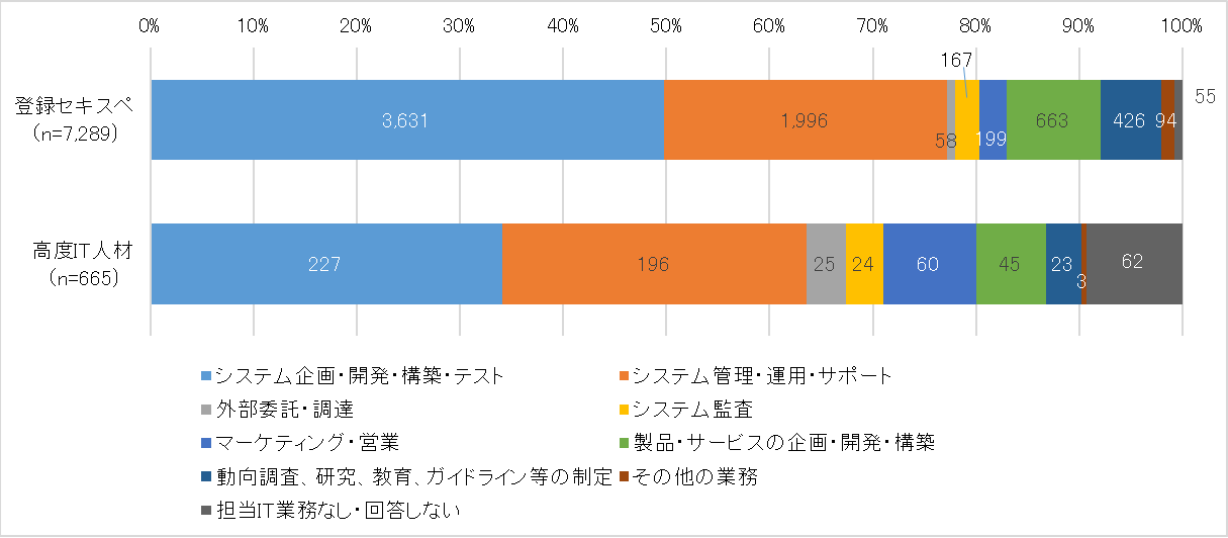


図 2-17 担当する IT 関連業務(主たる業務のみ／全体)

登録セキスペは、「システム企画・開発・構築・テスト」と「システム管理・運用・サポート」を合せると 8 割弱となり、過半数を占めた。その中でも「システム企画・開発・構築・テスト」を主担当業務とする人材の方が多かった。高度 IT 人材は、登録セキスペと比較すると「システム管理・運用・サポート」や「外部委託・調達」を主担当業務とする人材の割合が高かった。これは、高度 IT 人材は、顧客への IT システム・サービス提供に関わる人材の割合が比較的低いことによると考えられる。

図 2-18 に、2.3.1 であげたグループ(A)～(D)(担当業務における IT との関わり)ごとのグラフを示す(登録セキスペのみ)。(D)IT 調査研究・教育他は、システム企画・開発・構築・テストと管理・運用・サポート以外の業務の割合が大きく、他と違う分布を見せているが、グループ(A)～(C)は際立って大きな違いは見られなかった。(A)コーポレート IT と(B)ビジネス IT において、「外部委託・調達」を主担当業務とする人材が少ないことは想定外だったが、業務の一部として外部委託することはあっても、それ自身が主担当業務とならないという業務の性質を表していると考えている。

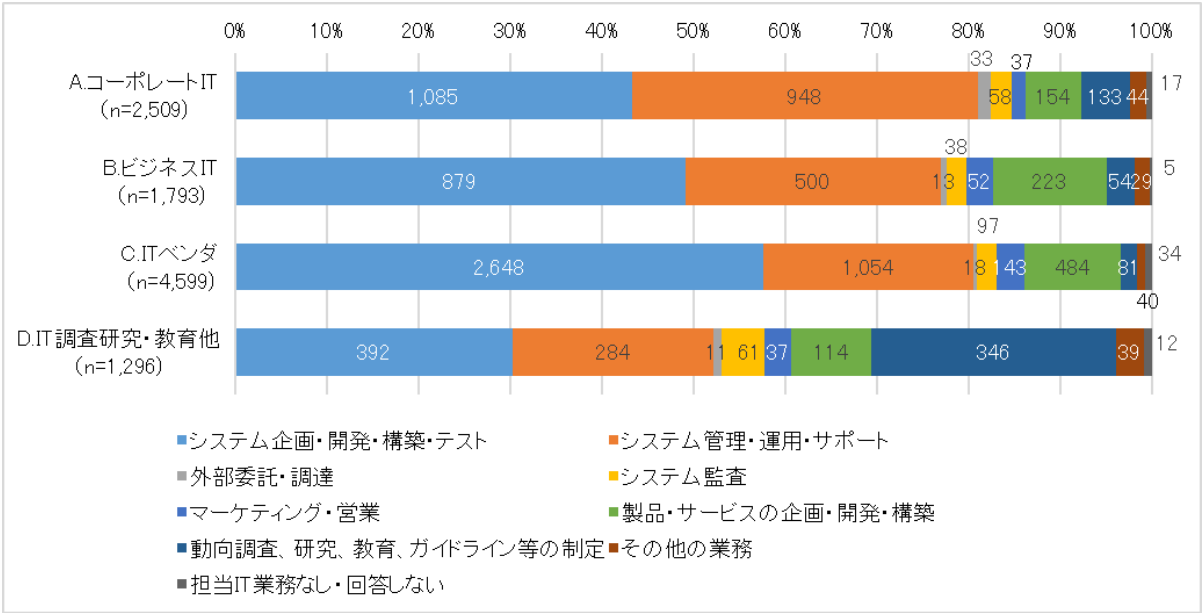


図 2-18 担当する IT 関連業務(主たる業務のみ／グループ別、登録セキスペのみ)

2.3.3. 担当する IT 関連業務（関わる業務すべて）

次に、担当する IT 関連業務すべてについて、グループ（A）～（D）ごとに図 2-19～図 2-22 に示す。全般的に、「主導的な実務者」として IT 関連業務を担っている人材が多いことが分かる。

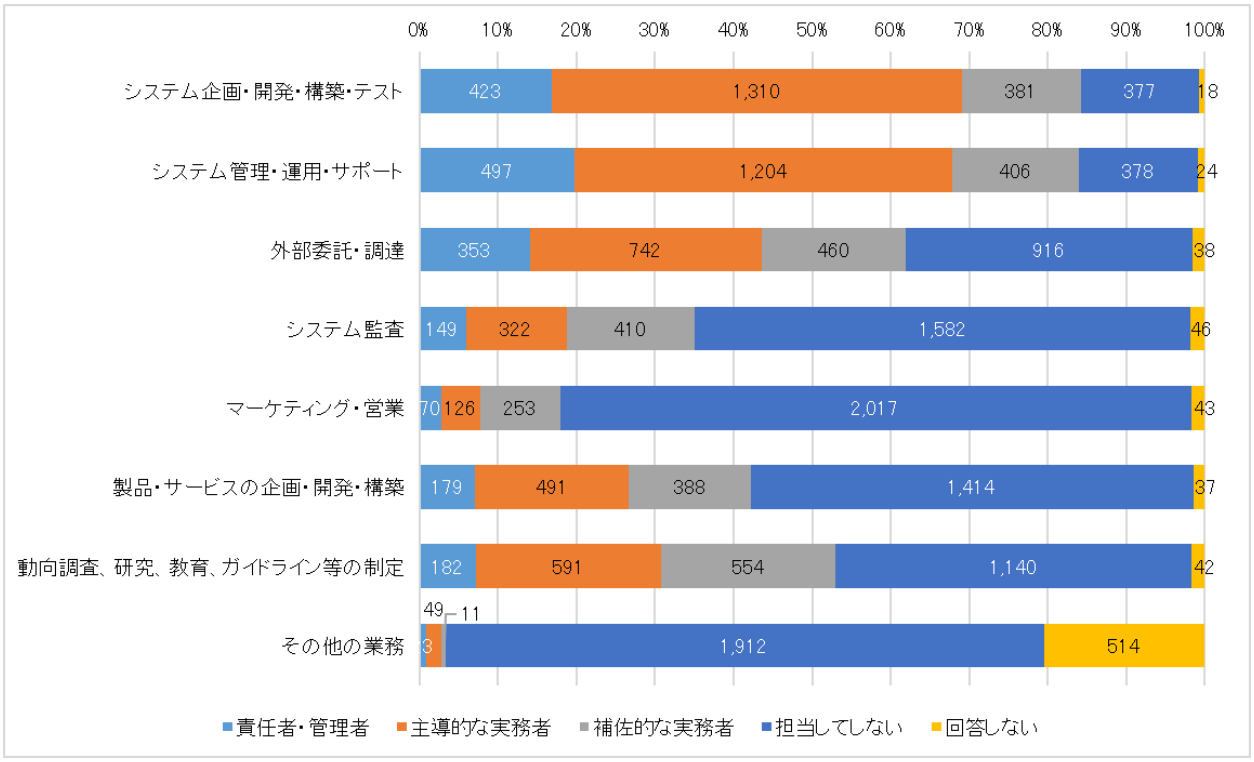


図 2-19 担当する IT 関連業務（関わるすべての業務／（A）コーポレート IT）（n=2,509）

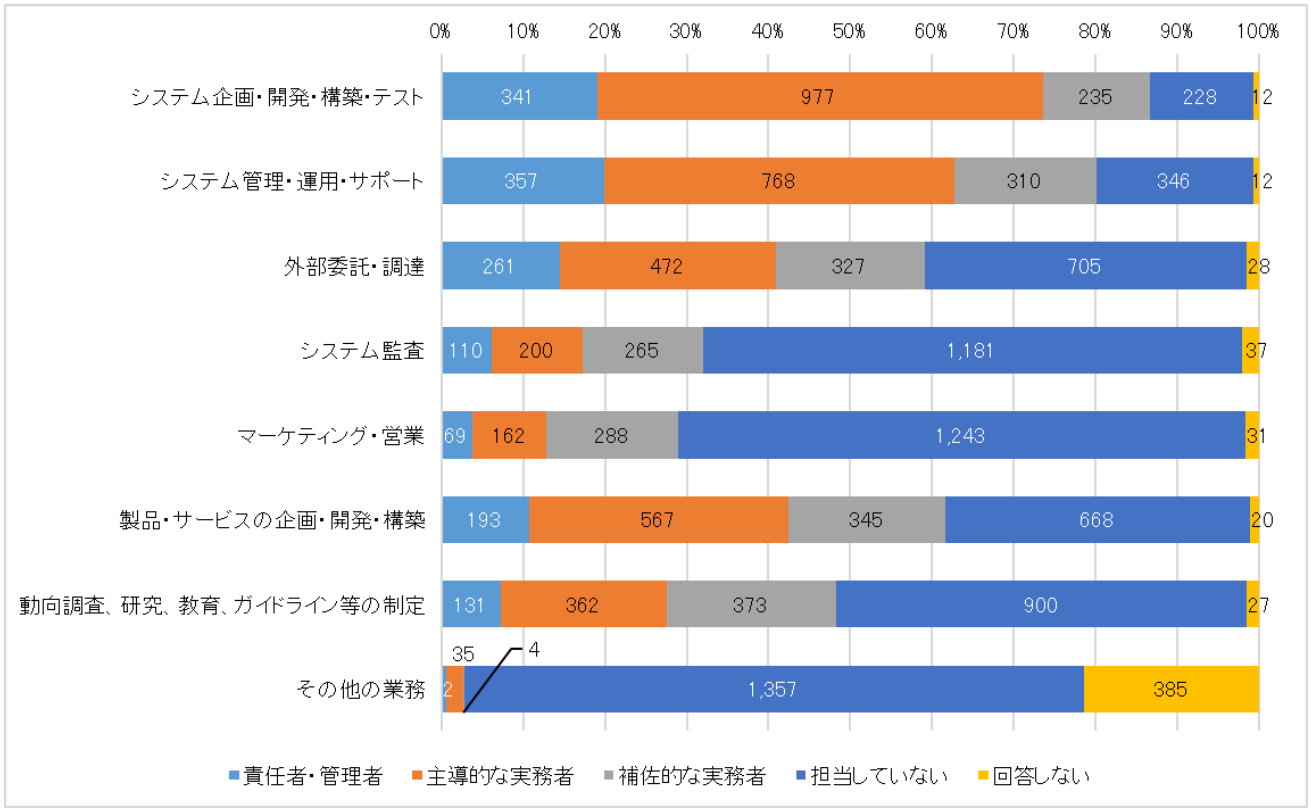


図 2-20 担当する IT 関連業務（関わるすべての業務／（B）ビジネス IT）（n=1,793）

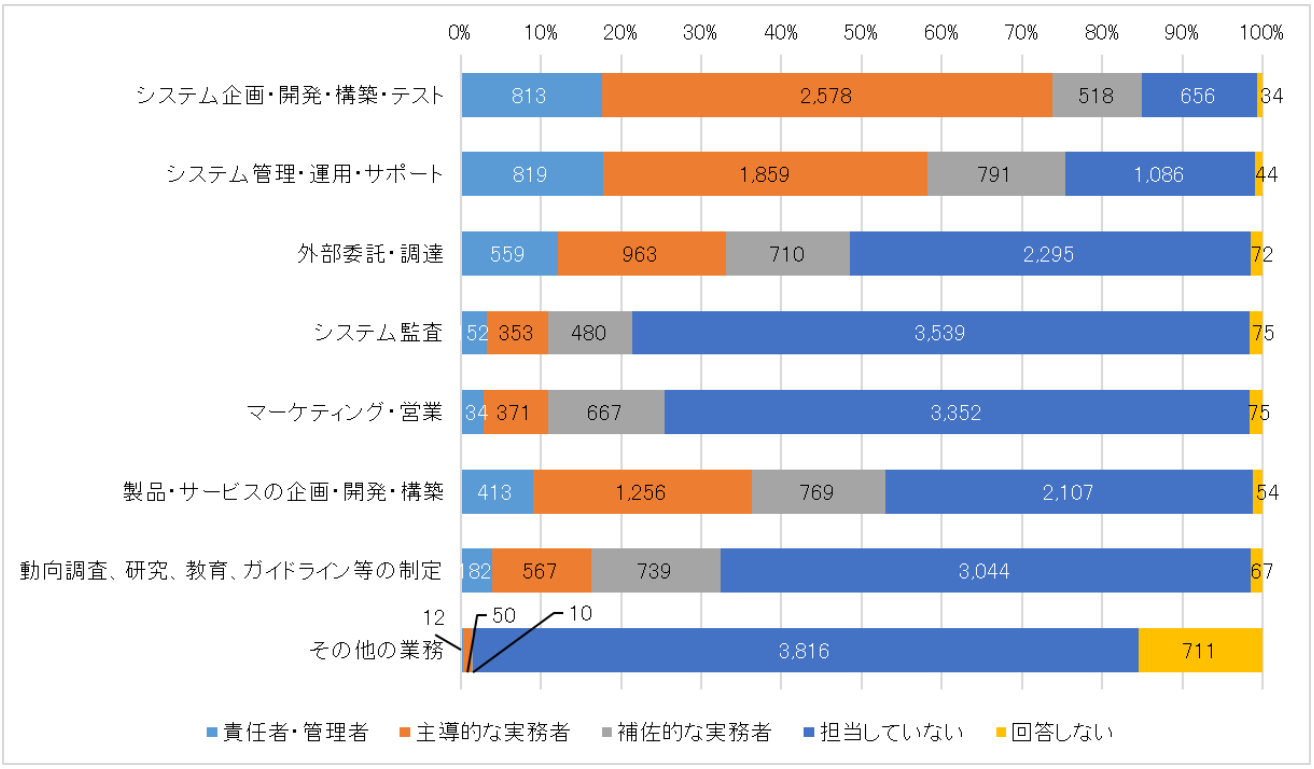


図 2-21 担当する IT 関連業務（関わるすべての業務／(C)IT ベンダ）(n=4,599)

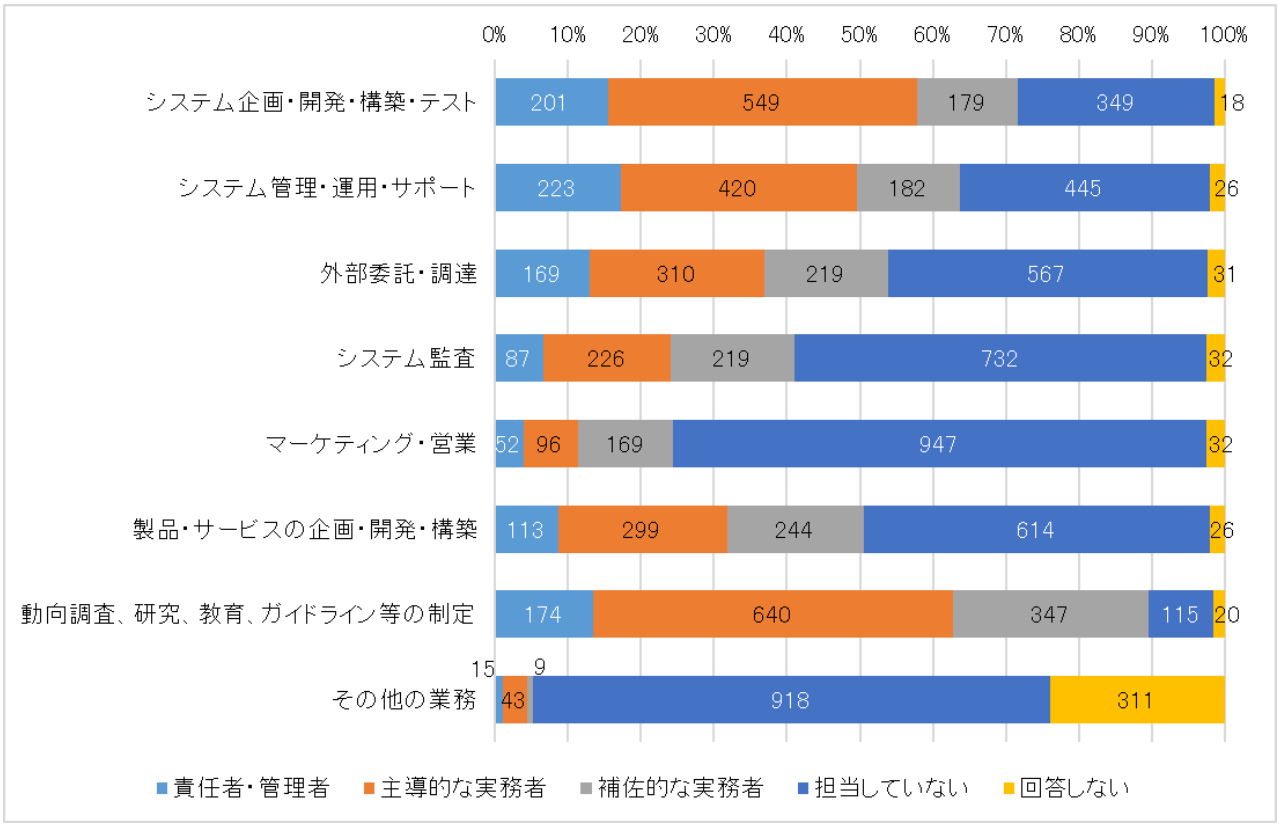


図 2-22 担当する IT 関連業務（関わるすべての業務／(D)IT 調査研究・教育他）(n=1,296)

2.3.4. 担当するサイバーセキュリティ対策関連業務（主たる業務）

12 種類のサイバーセキュリティ対策関連業務を定義し、登録セキスペ及び高度 IT 人材がどの業務を担当しているか質問し、前述の（A）～（D）にグループ分けの上、集計した。質問対象は、2.1.1 において、「会社役員・団体役員、正社員・団体職員、公務員、個人事業主・フリーランス・自営業、派遣社員・非正規社員・パートタイム社員」と回答した人とした。

（設問文：以下のサイバーセキュリティ対策に関連する業務のうち、あなたが担当している役割として、以下の 2.～4.の中から最も近いものをそれぞれ 1 つ選択してください。なお、担当していない業務については 1.を選択してください。）[9]

（設問文：前問でお答えの中で、主たる業務を 1 つ選択してください。）

選択肢として提示した 12 種類のサイバーセキュリティ対策関連業務を表 2-1 に示す。

表 2-1 確認したサイバーセキュリティ対策関連業務の一覧

No	サイバーセキュリティ対策関連業務（調査票掲載文章）	本報告書内で使う略称
1	サイバーセキュリティに関する経営判断	経営判断
2	サイバーセキュリティ管理体制の構築（コンサルティングを含む）	管理体制の構築
3	サイバーセキュリティ管理体制のマネジメント（コンサルティングを含む）	マネジメント
4	セキュア設計・開発・構築・評価（コンサルティングを含む）	セキュア設計
5	IT システム・サービスのセキュリティ面での運用・管理（外部委託・調達等を含む）	システム運用
6	サイバーセキュリティ対策機器の運用・保守	機器運用保守
7	監視・情報収集	監視・情報収集
8	脆弱性診断、情報セキュリティ監査	脆弱性／監査
9	インシデント対応（コンサルティングを含む）	インシデント
10	セキュリティ技術及びサイバーセキュリティ対策に関する調査・研究	調査研究
11	サイバーセキュリティに関する教育・人材育成	教育・人材育成
12	その他の業務	その他

登録セキスペ及び高度 IT 人材の主たる業務の回答内容を図 2-23 に示す。

[9] 役割の選択肢は次のとおり。
1.担当してしない
2.責任者・管理者（実務より管理業務が主体）
3.主導的な実務者（責任者を兼ねる場合も含む）
4.補佐的な実務者
5.回答しない

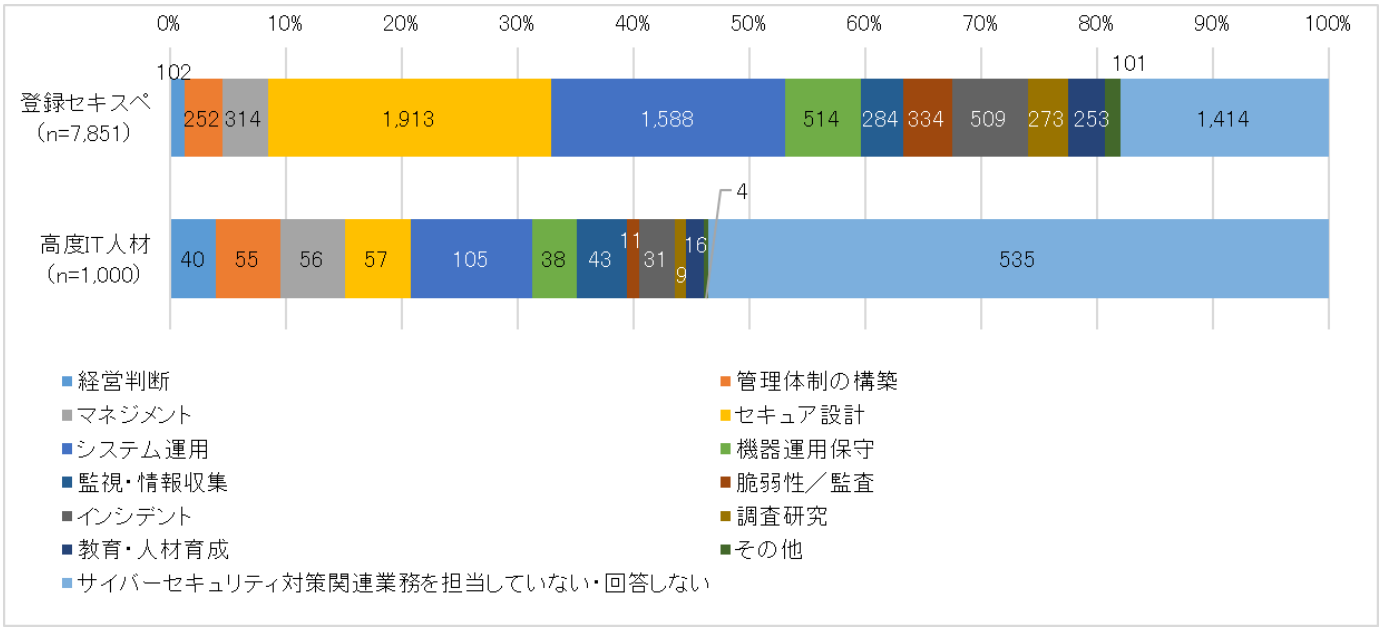


図 2-23 担当するサイバーセキュリティ対策関連業務(主たる業務のみ／全体)

サイバーセキュリティ対策に関する上流業務(「経営判断」、「管理体制の構築」、「マネジメント」)を主担当業務とする登録セキスペは 8.5%であった。主担当業務として多かったのは「セキュア設計」を主担当業務とする人で 24.4%、また運用系業務(「システム運用」、「機器運用保守」)も 26.8%と多かった。これと比較して、高度 IT 人材は上流業務担当者が多い(15.1%)など、登録セキスペとは違う傾向を示している。

また、担当しているサイバーセキュリティ対策関連業務を一つも選択しなかった割合は、登録セキスペで 22.1%、高度 IT 人材で 53.5%と高かった。そもそも業務遂行上 IT に関わらない人の割合は、図 2-14 によると登録セキスペで 7.4%、高度 IT 人材で 22.0%である。

図 2-24 に、2.3.1 であげたグループ(A)～(D)(担当業務における IT システム・サービスとの関わり)ごとのグラフを示す(登録セキスペのみ)。 (A)コーポレート IT や (B)ビジネス IT では、上流業務を担当する割合が全体と比較して大きいことや、(C)IT ベンダがサイバーセキュリティ対策関連業務を担当していない割合が大きいことが分かる。また、「セキュア設計」を担当する人材は、(C)IT ベンダに多いことも分かる。

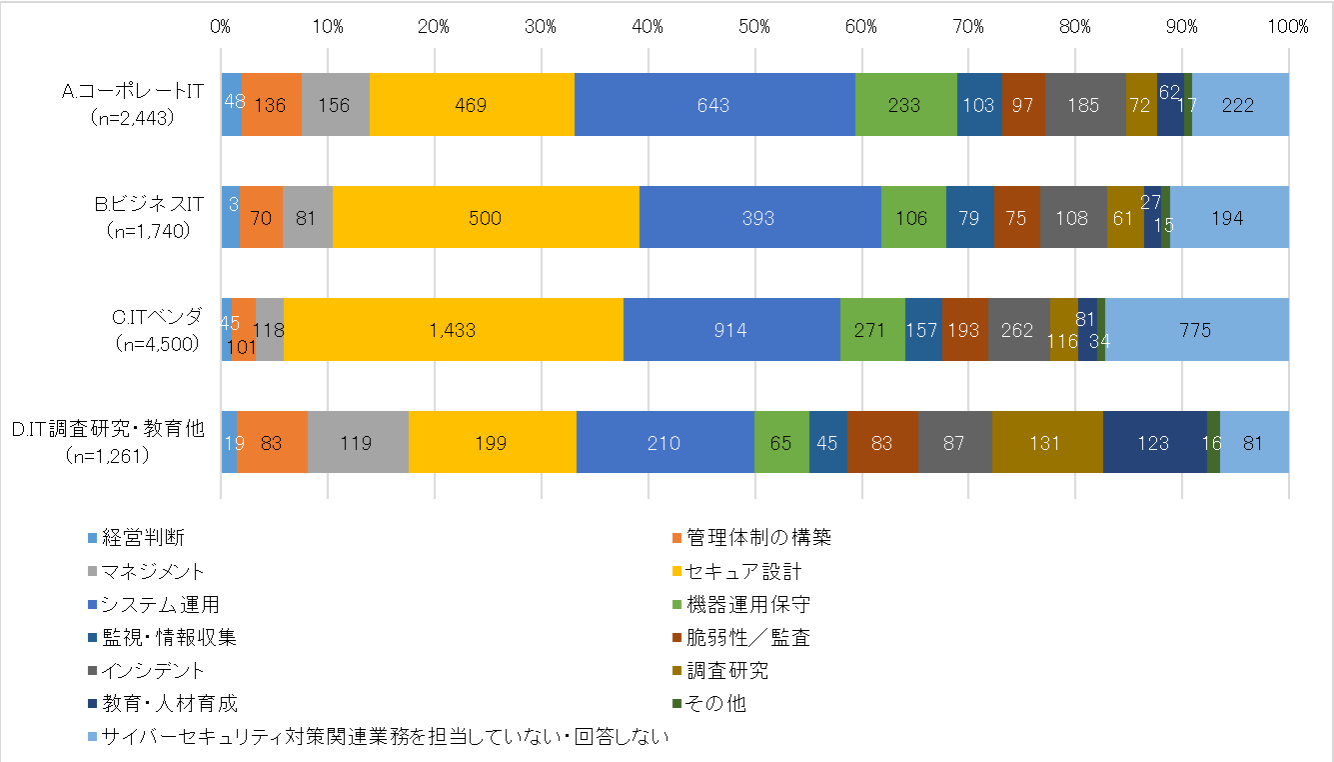


図 2-24 担当するサイバーセキュリティ対策関連業務（主たる業務のみ／グループ別、登録セキスペのみ）

2.3.5. 担当するサイバーセキュリティ対策関連業務（関わる業務すべて）

次に、担当するサイバーセキュリティ対策関連業務すべてについて、グループ（A）～（D）ごとに図 2-25～図 2-28 に示す。

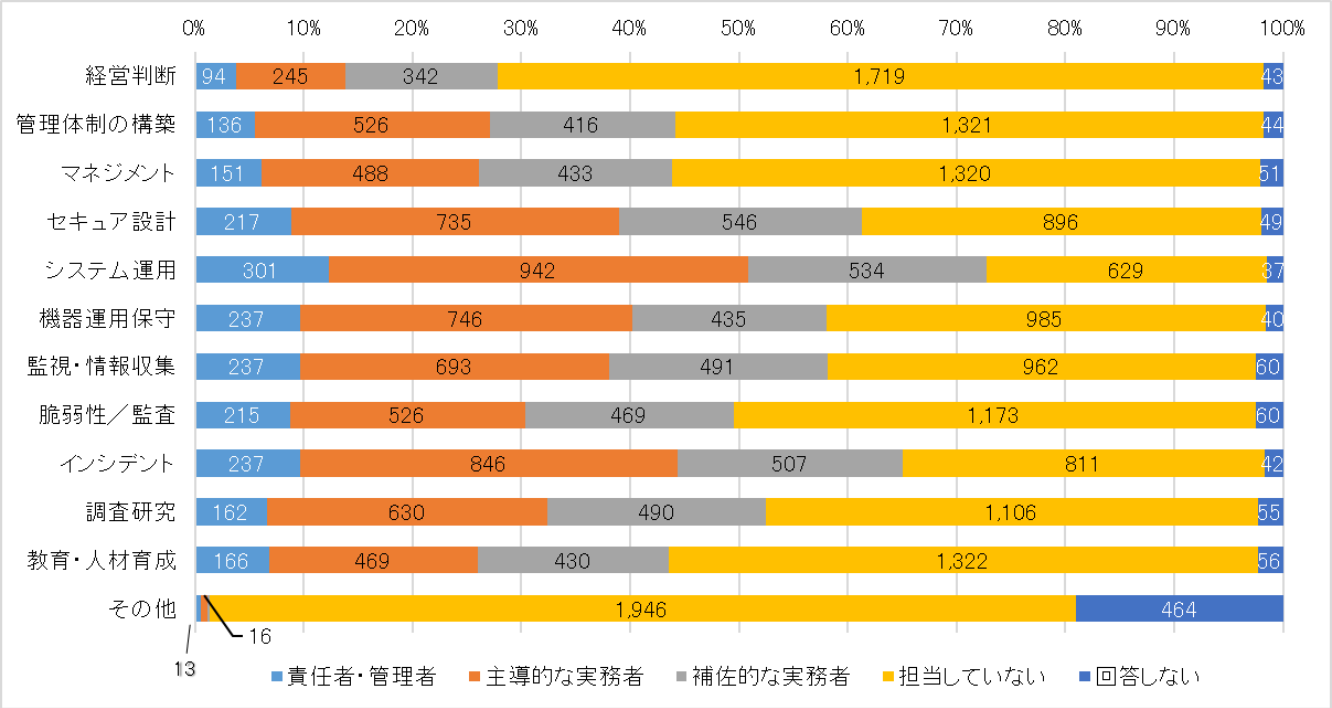


図 2-25 担当するサイバーセキュリティ対策関連業務（関わるすべての業務／（A）コーポレート IT）（n=2,443）

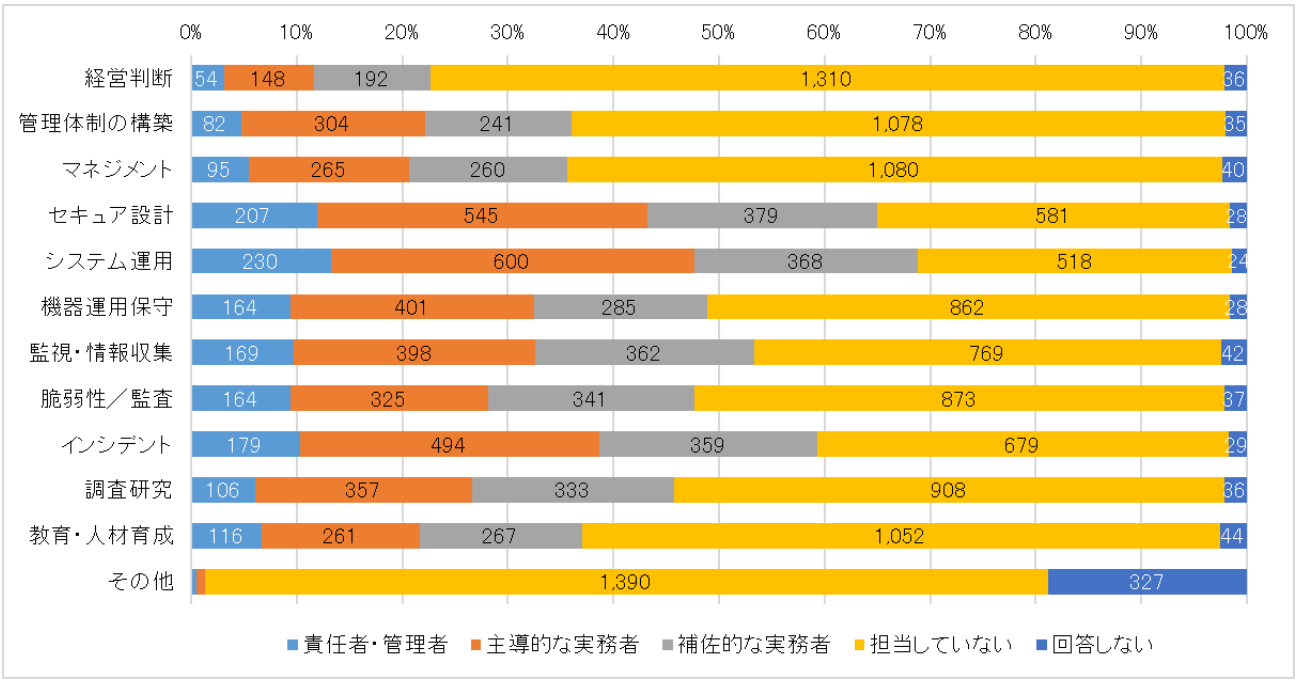


図 2-26 担当するサイバーセキュリティ対策関連業務（関わるすべての業務／(B)ビジネス IT）(n=1,740)

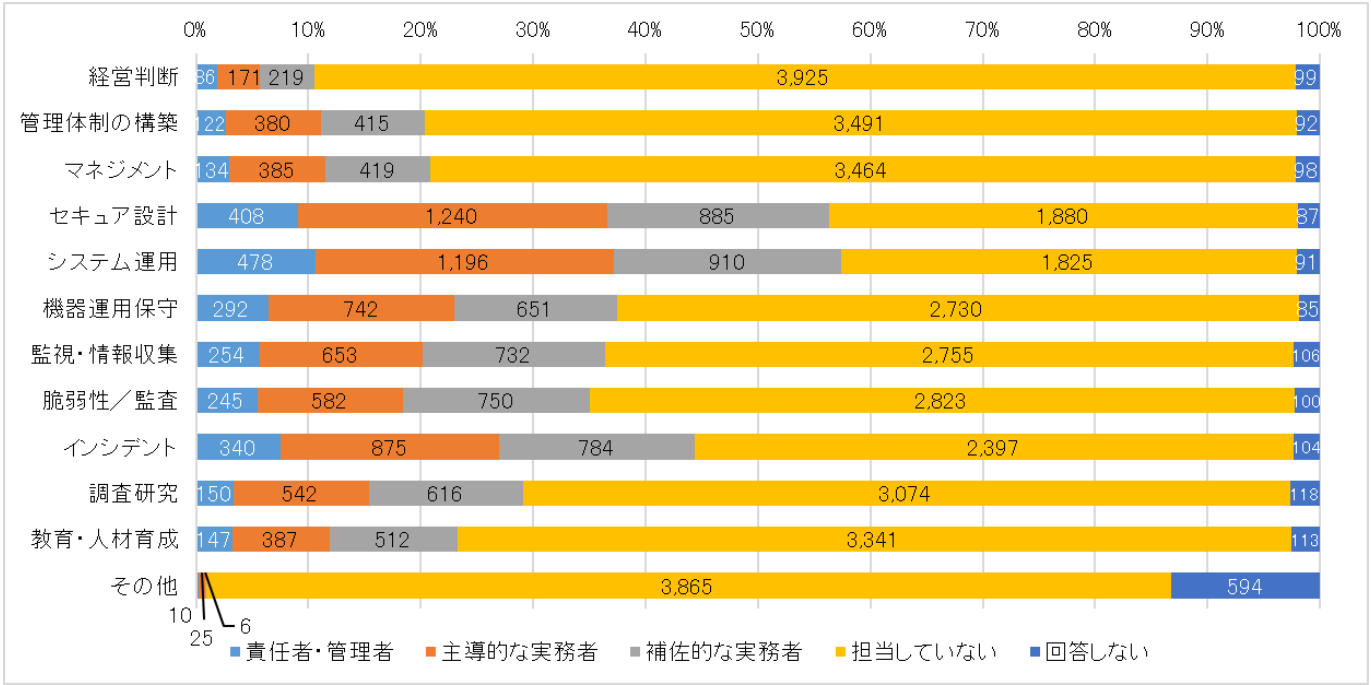


図 2-27 担当するサイバーセキュリティ対策関連業務（関わるすべての業務／(C)IT ベンダ）(n=4,500)

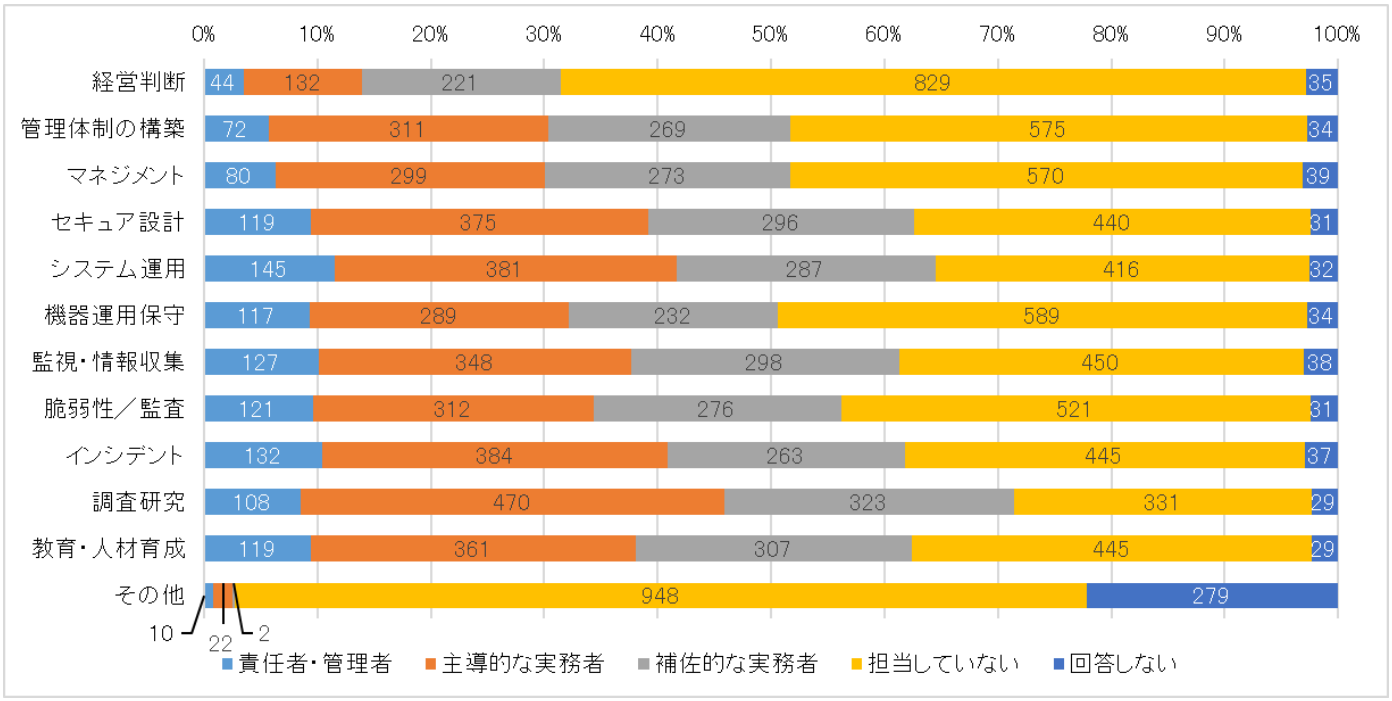


図 2-28 担当するサイバーセキュリティ対策関連業務（関わるすべての業務／(D)IT 調査研究・教育他）(n=1,261)

(A)コーポレート IT、(B)ビジネス IT において、運用系の業務担当者が多いことが分かる。また、(C)IT ベンダでは「担当していない」との回答が多いが、これは、1 人が担当する業務数が、他のグループと比較して少ないことを示している。表 2-2 に、グループごとの平均担当業務数を示す。

表 2-2 平均担当業務数（グループ別、登録セキスペ）

IT システム・サービスとの関わり	平均担当業務数
(A).コーポレート IT	5.6
(B).ビジネス IT	5.0
(C).IT ベンダ	3.6
(D) IT 調査研究・教育他	6.1

平均担当業務数は、グループごとの違いはあるにせよ、全般的に高かった。つまり、複数の業務を担当している登録セキスペが多いことになる。そこで、担当業務の組み合わせの傾向から登録セキスペの人材像の現状が見えてくると考え、この値を使ってクラスタ分析を行った。分析結果は、3.2 に記載する。

2.3.6. 担当業務が IT に関わりのない登録セキスペについて

2.3.1 の設問において、担当業務が「IT に関わっていない」と回答した登録セキスペの、サイバーセキュリティ対策関連業務の担当状況を集計した(n=591)。

サイバーセキュリティ対策関連業務の担当状況の設問では、1 つ以上担当業務があると回答した人は 288 名で 48.7%であった。IT に関わりのない業務を担当している登録セキスペの半数が、サイバーセキュリティ対策関連業務を担当しているということになる。興味深かったため、その 288 名の部署を調べた。その結果、IT に関わりのない業務担当者でも、様々な部門でサイバーセキュリティ対策業務を担当していることが分かった。図 2-29～図 2-31 にその結果を示す。

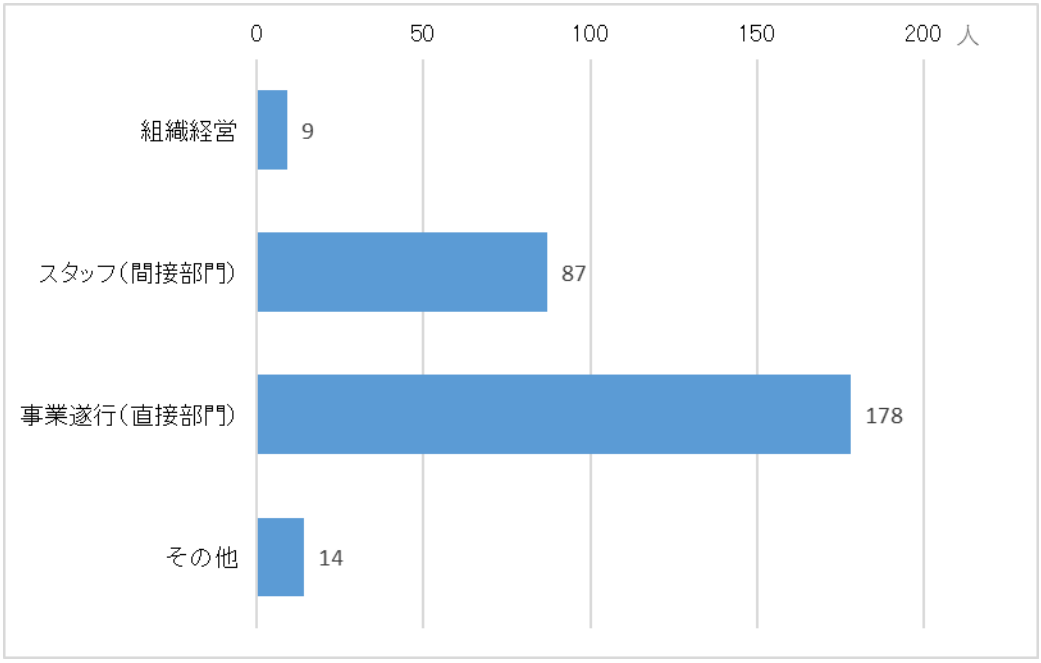


図 2-29 IT に関わりないがサイバーセキュリティ対策関連業務を担当する登録セキスペの部署(n=288)

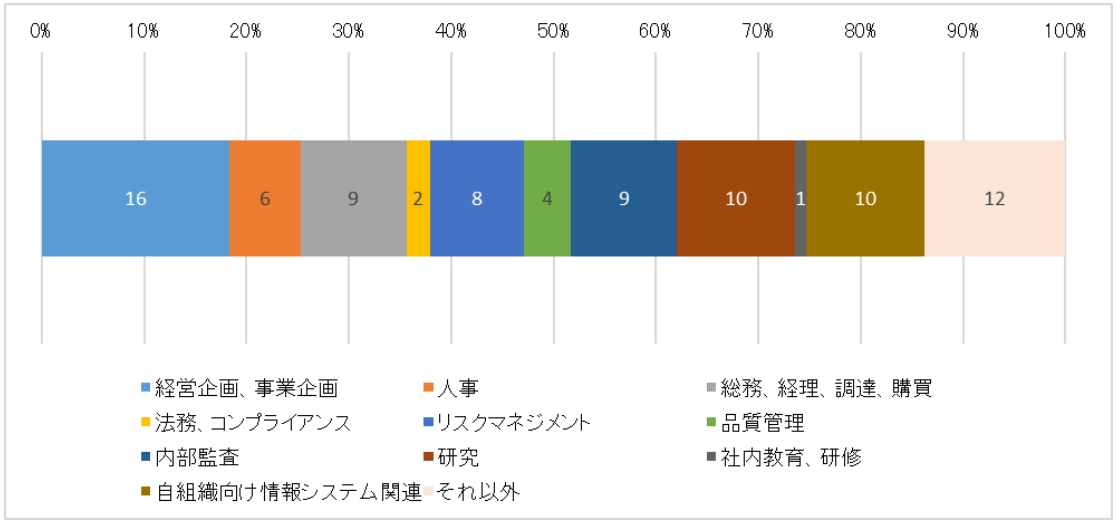


図 2-30 IT に関わりないがサイバーセキュリティ対策関連業務を担当する登録セキスペの部署(スタッフ(間接部門)のみ, n=87)

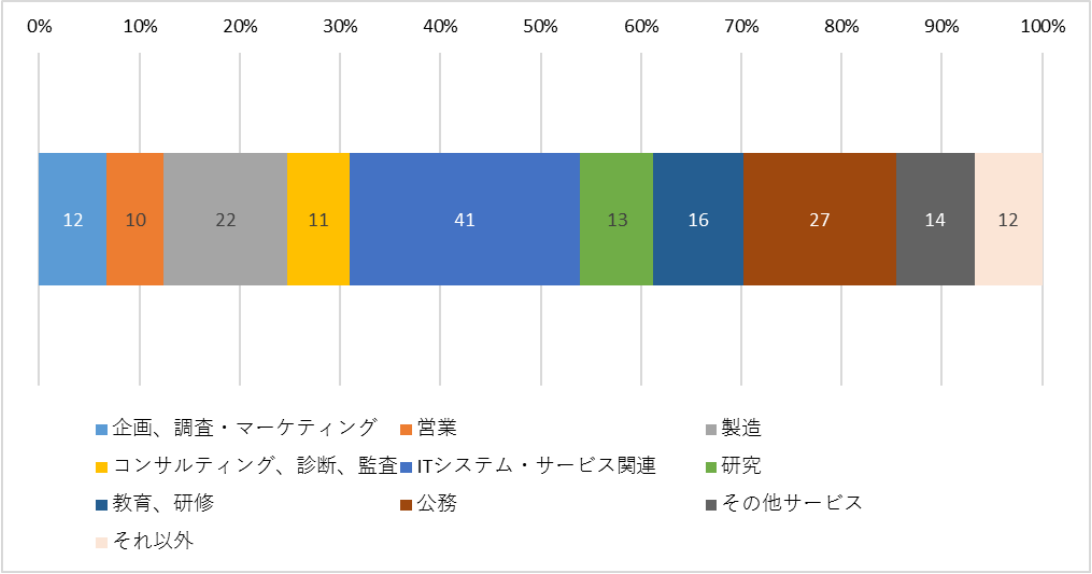


図 2-31 IT に関わりないがサイバーセキュリティ対策関連業務を担当する登録セキスペの部署(事業遂行(直接部門)のみ, n=178)

2.3.7. CSIRT 担当状況

CSIRT 担当状況は図 2-32 のとおりとなった。

(設問文:あなたは自企業・団体の CSIRT メンバーですか。次の中から最も近いものを 1 つ選択してください。)

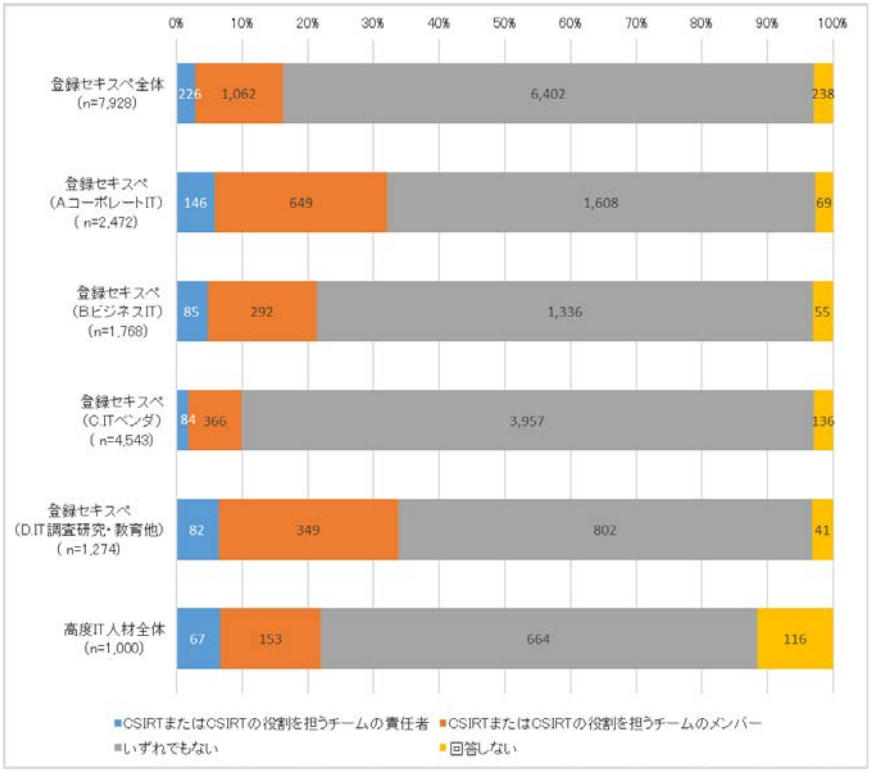


図 2-32 CSIRT 担当状況

CSIRT の担当状況を見ると(A)コーポレート IT で CSIRT の責任者やメンバーである割合が高く、(C)IT ベンダでは低い傾向であった。また、(D)IT 調査研究・教育他で CSIRT である割合が高い点については約半数が(A)コーポレート IT にも含まれるため、その影響が出ていると考える。

2.4. 登録セキスペの活用スキル

登録セキスペ及び高度 IT 人材の IT 関連業務やサイバーセキュリティ対策関連業務担当者に対し、業務遂行に必要な知識・スキルを確認した。

2.4.1. IT 業務における活用スキル

IT 関連業務を担当していると回答した人に、各業務遂行において必要な知識・スキルを確認した。

(設問文:ご回答いただいた IT システム・サービスに関連する業務に関して、業務を行う上で必要な知識・スキルのうち重要な順に上位 5 つまでを業務ごとに選択してください。なお、知識・スキルのレベルは問いません。
選択肢:
(1)アプリケーション／サービスに関するもの(業種固有のアプリケーション、ウェブ、グループウェア、オフィスアプリ、会計アプリ、SaaS、開発技術など)
(2)システム基盤／ハードウェアに関するもの(システムのアーキテクチャ、OS、仮想環境、IaaS・PaaS 等のクラウドサービス、IoT など)
(3)情報セキュリティ技術・情報セキュリティ対策の運用・マネジメントに関するもの
(4)先端技術に関するもの(AI、データサイエンス、ブロックチェーン など)
(5)開発や運用の管理に関するもの(プロジェクトマネジメント、サービスマネジメント、アジャイル手法 など)
(6)事業戦略に関するもの(経営、リスクマネジメント、財務、設備投資、設備管理、人材戦略など)
(7)倫理、コンプライアンス、法律やガイドライン、標準、規格等に関するもの
(8)人間力に関するもの(コミュニケーション、意識共有、人を動かす行動力 など)
(9)その他の知識・スキル
(10)上記(1)～(9)のいずれの知識も必要としない
(11)わからない、回答しない
)

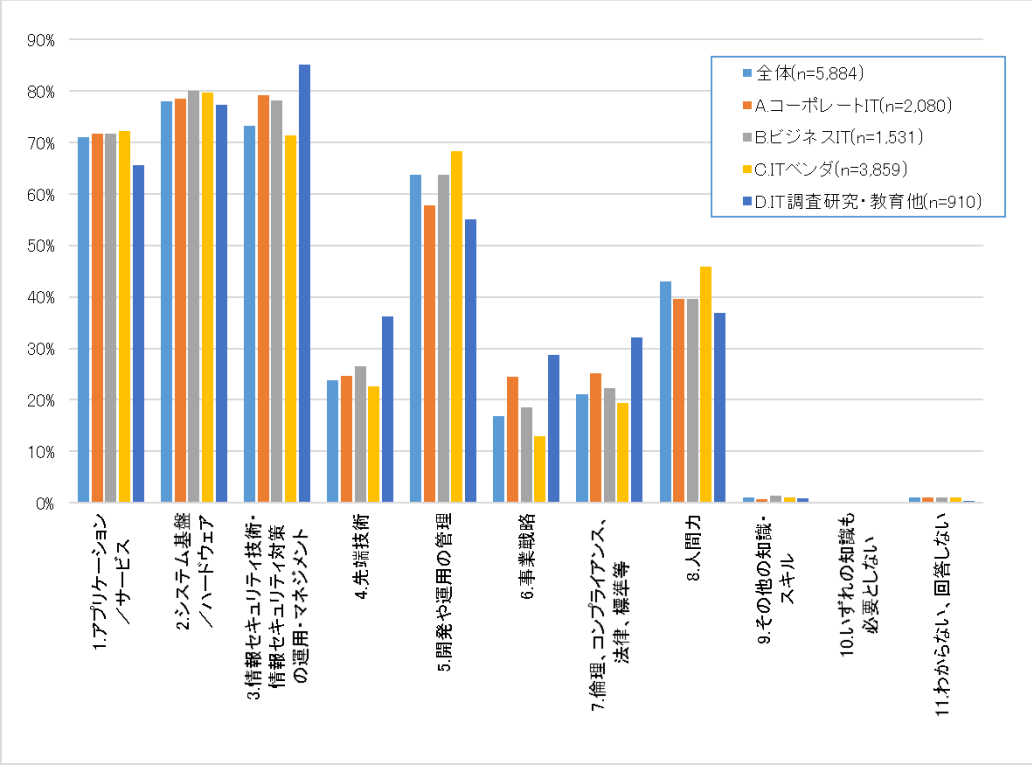


図 2-33 IT 関連業務遂行に必要な知識・スキル(「システム企画・開発・構築・テスト」業務)

いずれのグループも大きな相違はなく、8 割近くの人が「1.アプリケーション／サービス」、「2.システム基盤/ハードウェア」、「3.情報セキュリティ技術・情報セキュリティ対策の運用・マネジメント」、「5.開発や運用の管理」の知識・スキルを活用しており、「4.先端技術」や「6.事業戦略」などの知識・スキルを活用している割合は 2 割程度と低いことが分かる。

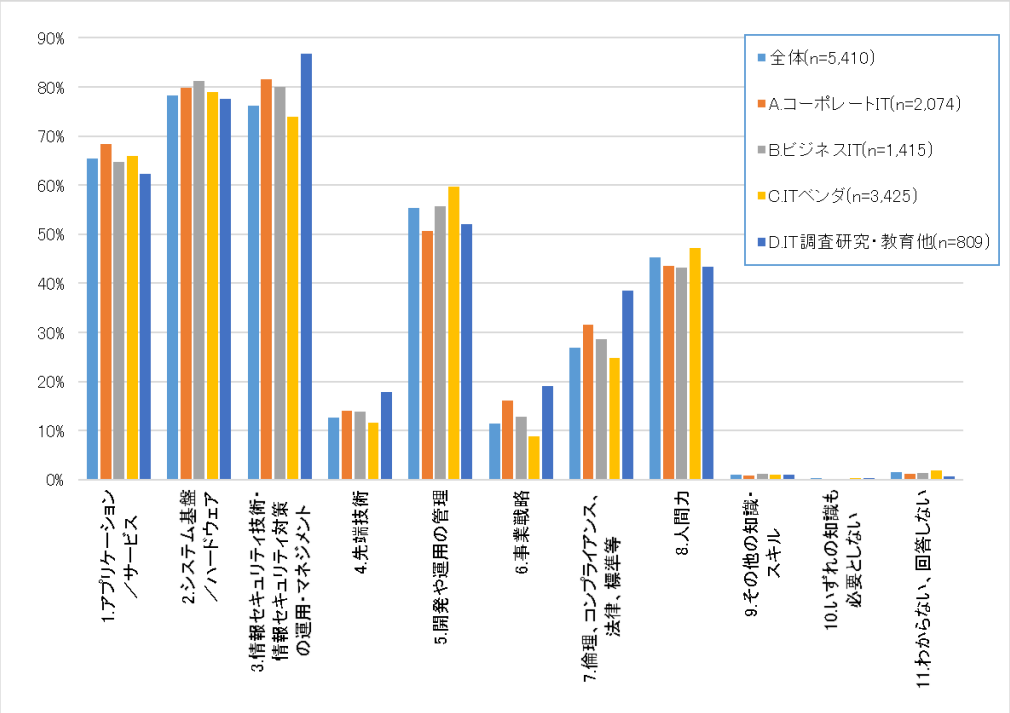


図 2-34　IT 関連業務遂行に必要な知識・スキル(「システム管理・運用・サポート」業務)

「システム企画・開発・構築・テスト」業務と比較して、「1. アプリケーション／サービス」知識・スキルを活用している人は若干少なくなっている。その他は大きな傾向の違いはない。

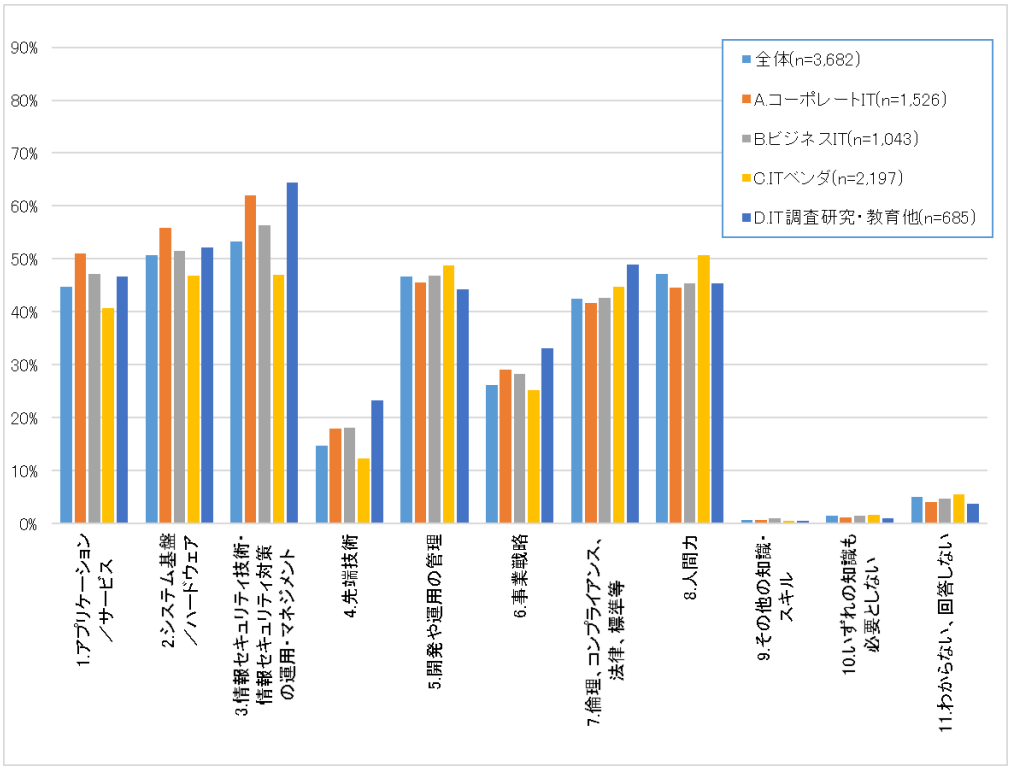


図 2-35　IT 関連業務遂行に必要な知識・スキル(「外部委託・調達」業務)

「外部委託・調達」業務では、前の 2 業務と比較して、1.～3.の知識・スキルを活用している人は少ない。ただし、「6.事業戦略」や「7.倫理、コンプライアンス、法律、標準等」の知識・スキルを活用する人の割合が高まる。

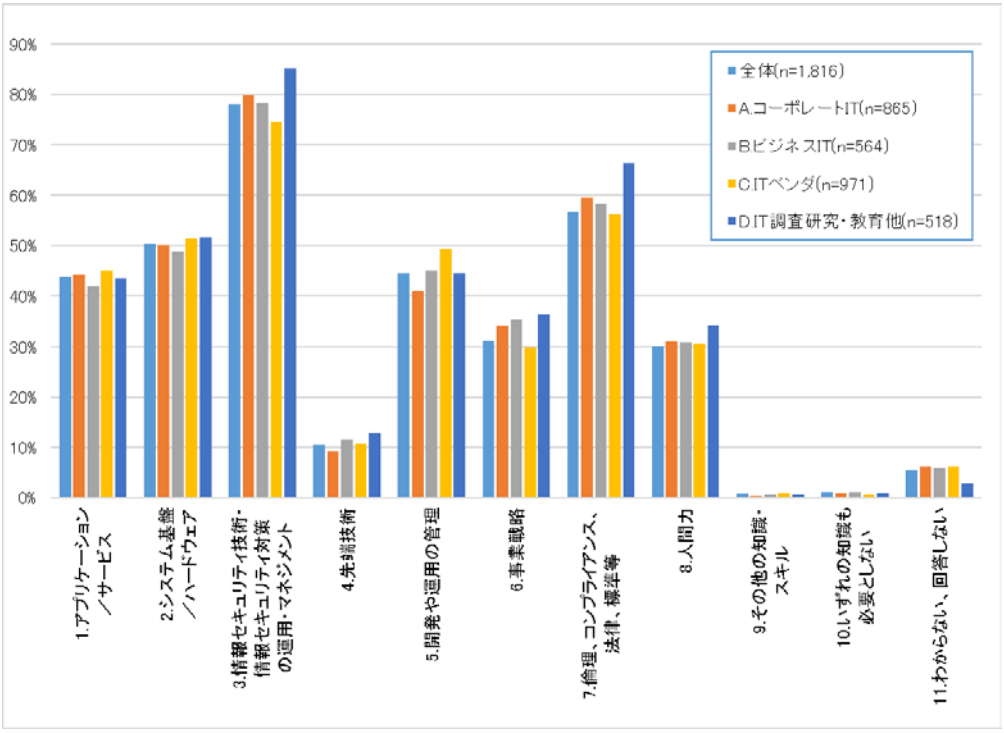


図 2-36　IT 関連業務遂行に必要な知識・スキル(「システム監査」業務)

「システム監査」業務担当者は、「3.情報セキュリティ技術・情報セキュリティ対策の運用・マネジメント」の知識・スキルや「7.倫理、コンプライアンス、法律、標準等」などの知識を活用していることが分かる。

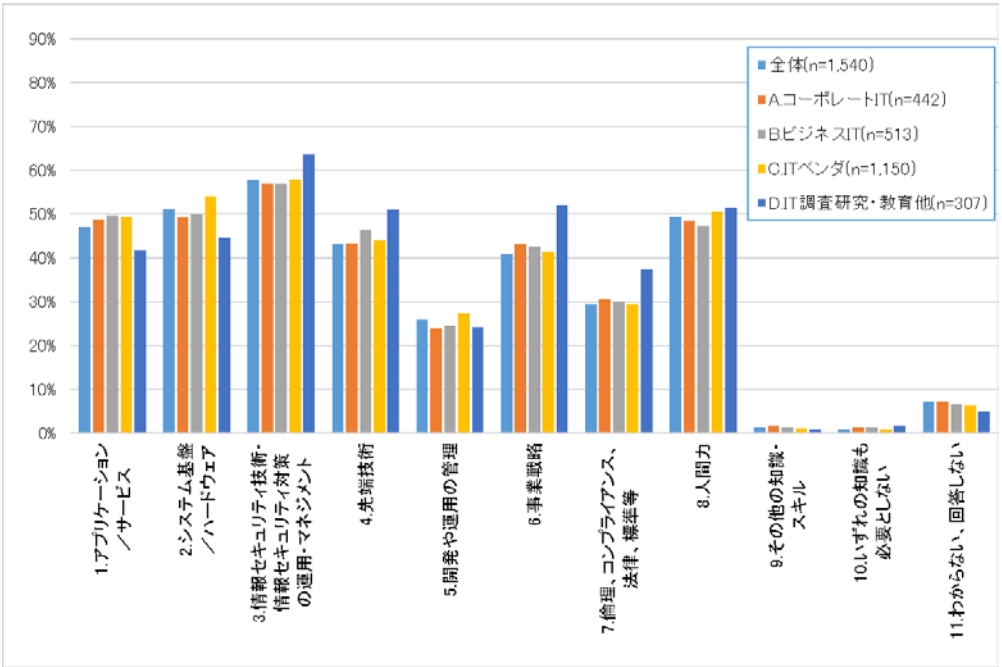


図 2-37　IT 関連業務遂行に必要な知識・スキル(「マーケティング・営業」業務)

「マーケティング・営業」業務担当者は、他の IT 関連業務と比較すると IT 系技術の知識・スキルを活用する割合は低いが、事業戦略の知識・スキルを活用する割合が 5 割近くあり、他業務と比べて高い。特に(D)IT 調査研究・教育他において高いことが特徴的である。更に「8.人間力」に関する知識・スキルも活用割合が若干高いが、極端に違うわけではない。

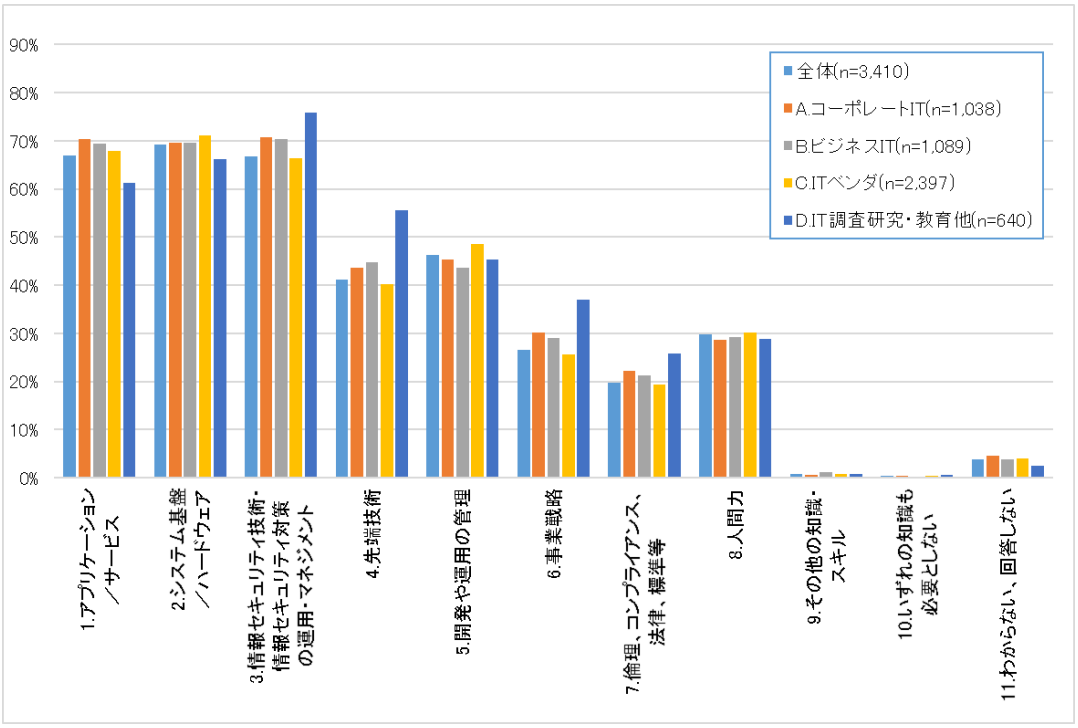


図 2-38　IT 関連業務遂行に必要な知識・スキル（「製品・サービスの企画・開発・構築」業務）

「製品・サービスの企画・開発・構築」業務担当者の活用知識・スキルは、情報セキュリティ技術・情報セキュリティ対策の運用・マネジメントの知識・スキルが突出しておらず、情報セキュリティに関する製品開発でも、全般的な技術知識が必要となることの表れではないかと考える。

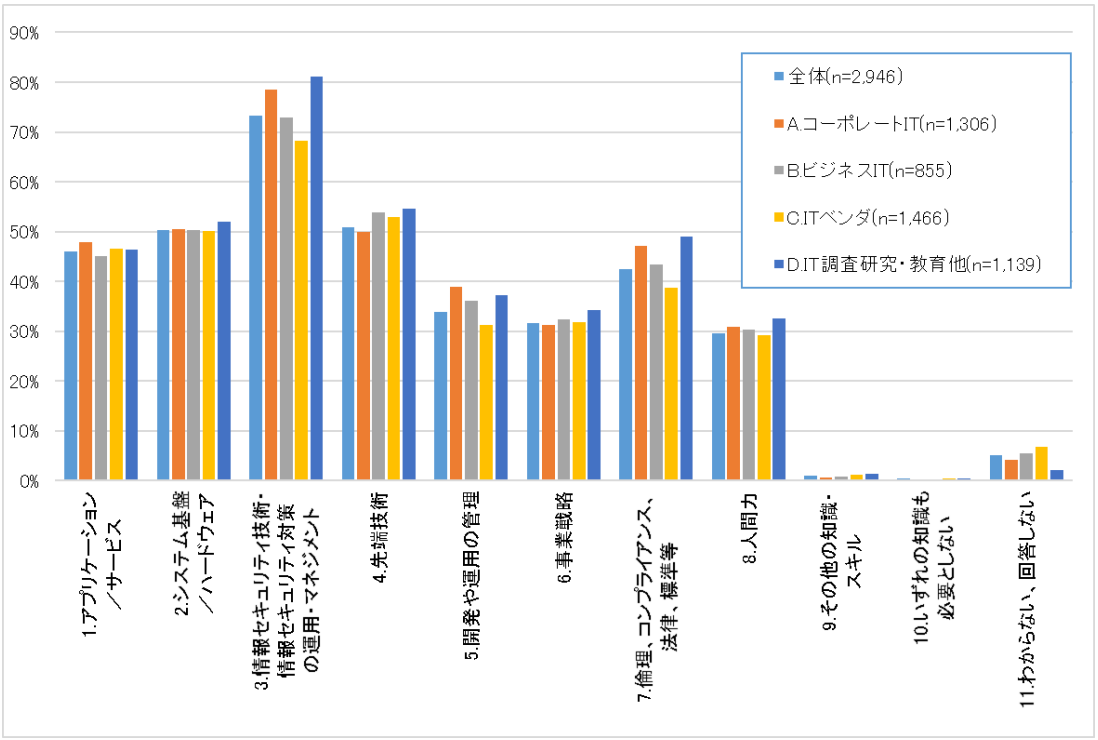


図 2-39　IT 関連業務遂行に必要な知識・スキル（「動向調査、研究、教育、ガイドライン等の制定」業務）

「動向調査、研究、教育、ガイドライン等の制定」業務では、情報セキュリティ以外の IT 技術系知識の活用度合いが低く、先端技術に関する知識・スキルの活用割合も高い。この傾向は業務内容を考えると納得感は高い。

2.4.2. サイバーセキュリティ対策関連業務における活用スキル

サイバーセキュリティ対策関連業務を担当していると回答した人に、その業務遂行に必要な知識・スキルを確認した。

（設問文：回答いただいたサイバーセキュリティ対策に関する業務に関して、業務を行う上で必要な知識・スキルの上位 5 つまでを選択してください。なお、知識・スキルのレベルは問いません。
選択肢：
1 情報セキュリティ分野／(1) 最新の脅威に関するもの（脆弱性、マルウェアなどの攻撃手法、攻撃主体　など）
2 情報セキュリティ分野／(2) 情報セキュリティ技術に関するもの（暗号や認証、電子署名、情報理論　など）
3 情報セキュリティ分野／(3) 情報セキュリティ対策の運用に関するもの（対策のオペレーション、監視、インシデントレスポンス　など）
4 情報セキュリティ分野／(4) 情報セキュリティマネジメントに関するもの（情報セキュリティポリシー、情報セキュリティガバナンス、情報セキュリティ監査等）
5 情報セキュリティ分野／(5) 情報セキュリティ機能の設計・実装に関するもの（セキュリティ要件定義、設計、実装、テスト、評価　など）
6.IT関連ほか全般／(6) アプリケーション／サービスに関するもの（業種、ウェブ、グループウェア、オフィスアプリ、会計アプリ、SaaS、開発技術　など）
7IT関連ほか全般／(7) システム基盤／ハードウェアに関するもの（システムのアーキテクチャ、OS、仮想環境、IaaS・PaaS 等のクラウドサービス、IoT 等）
8 IT関連ほか全般／(8) 先端技術に関するもの（AI、データサイエンス、ブロックチェーン　など）
9 IT関連ほか全般／(9) 開発や運用の管理に関するもの（プロジェクトマネジメント、サービスマネジメント、アジャイル手法　など）
10 IT関連ほか全般／(10) 事業戦略に関するもの（経営、リスクマネジメント、財務、設備投資、設備管理、人材戦略など）
11IT関連ほか全般／(11) 倫理、コンプライアンス、法律やガイドライン、標準、規格等に関するもの
12IT関連ほか全般／(12) 人間力に関するもの（コミュニケーション、意識共有、人を動かす行動力　など）
13 その他／(13) 上記 (1) ～ (12) のいずれの知識も必要としない
14 その他／(14) わからない、回答しない
）

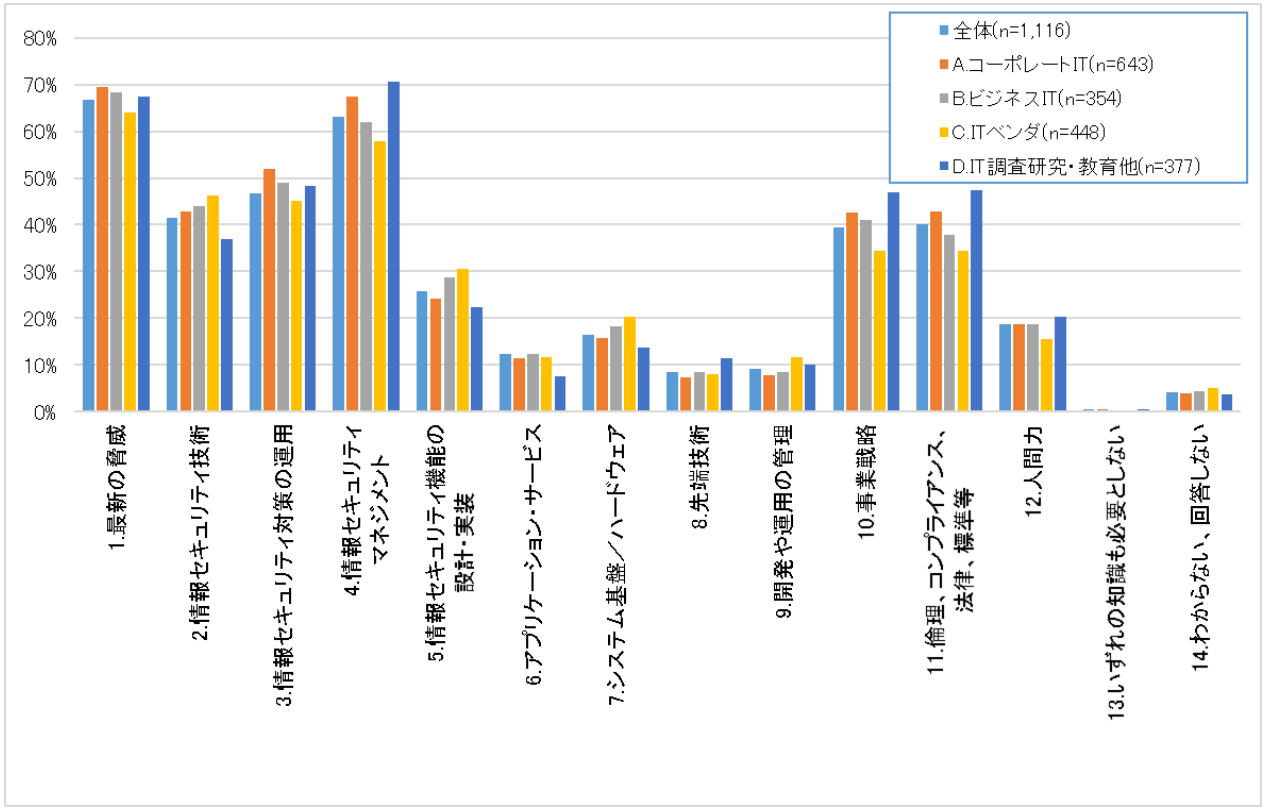


図 2-40 サイバーセキュリティ対策関連業務遂行に必要な知識・スキル（「経営判断」）

「経営判断」業務における活用知識・スキルは、(D)IT 調査研究・教育他を除くと、グループによる傾向の大きな違いはない。他の業務と比べて事業戦略や「11.倫理、コンプライアンス、法律、標準等」の知識を活用している割合が高いが、5 割弱と想定より低かった。

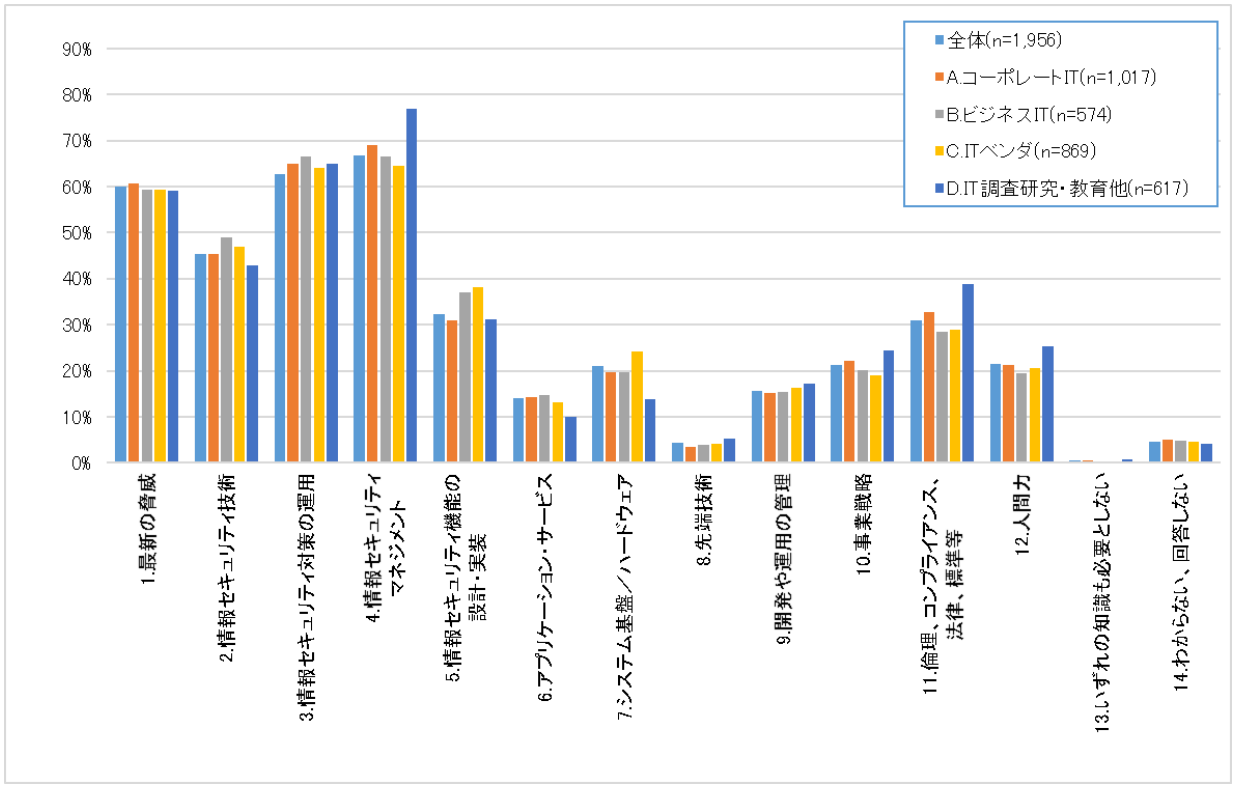


図 2-41 サイバーセキュリティ対策関連業務遂行に必要な知識・スキル(「管理体制の構築」)

「管理体制の構築」業務における活用知識・スキルは、「2.情報セキュリティ技術」や「3.情報セキュリティ対策の運用」の知識・スキルであり、IT 技術に関する知識・スキルはあまり活用していないことが分かる。また、事業戦略の知識・スキルの活用度合いも 2 割程度と低い。

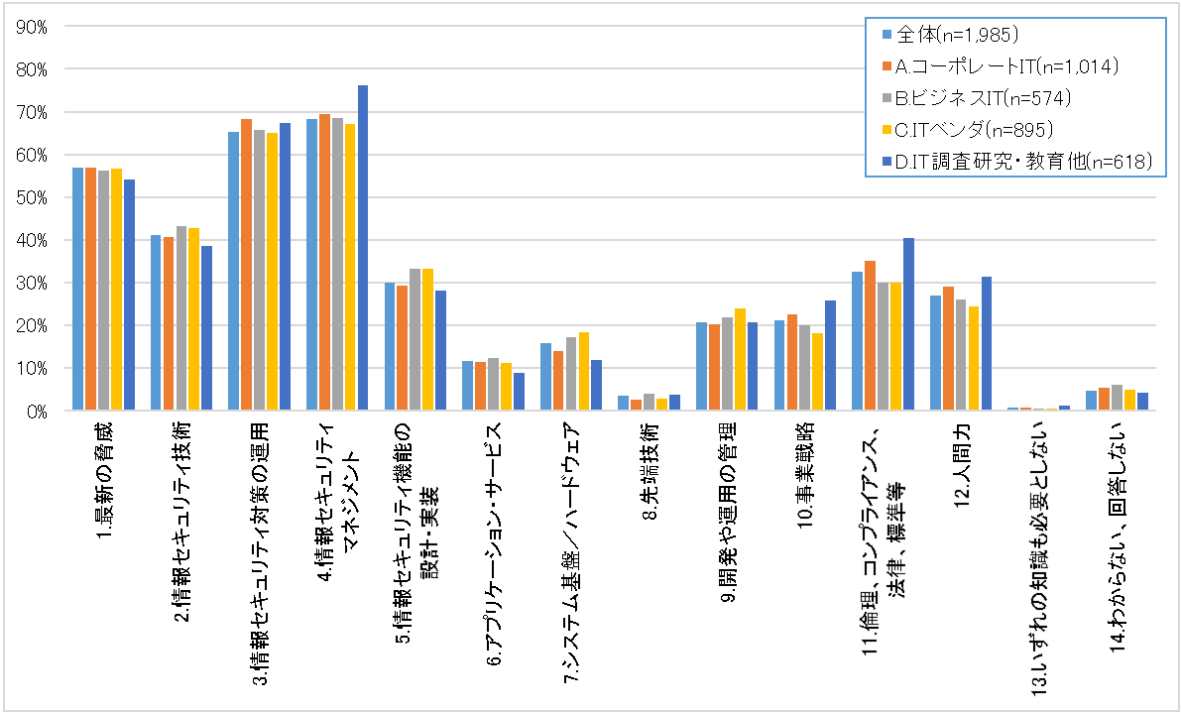


図 2-42 サイバーセキュリティ対策関連業務遂行に必要な知識・スキル(「マネジメント」)

「マネジメント」業務における活用知識・スキルは、「管理体制の構築」業務の傾向と大きな違いはなかった。

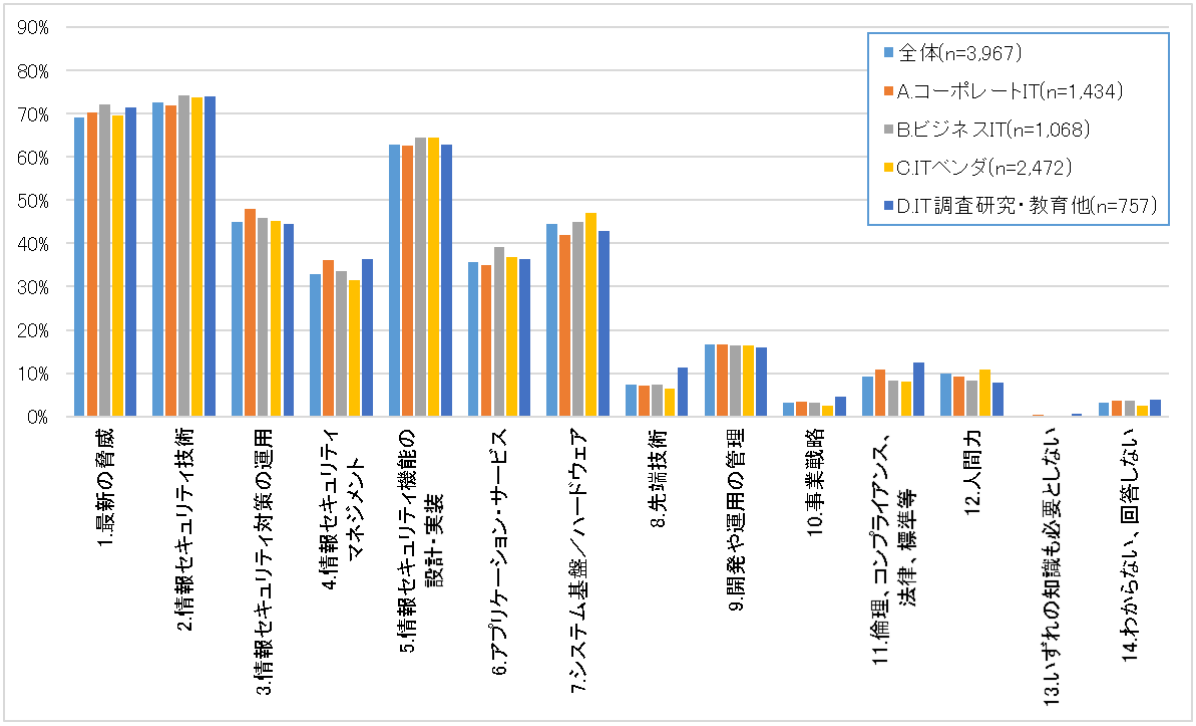


図 2-43 サイバーセキュリティ対策関連業務遂行に必要な知識・スキル(「セキュア設計」)

「セキュア設計」業務における活用知識・スキルは、「1.最新の脅威」、「2.情報セキュリティ技術」、「5.情報セキュリティ機能の設計・実装」など、セキュリティ関連の知識・スキルの活用割合が大きい。「11.倫理、コンプライアンス、法律、標準等」や「12.人間力」の知識・スキルの活用割合が他業務と比較して低い。

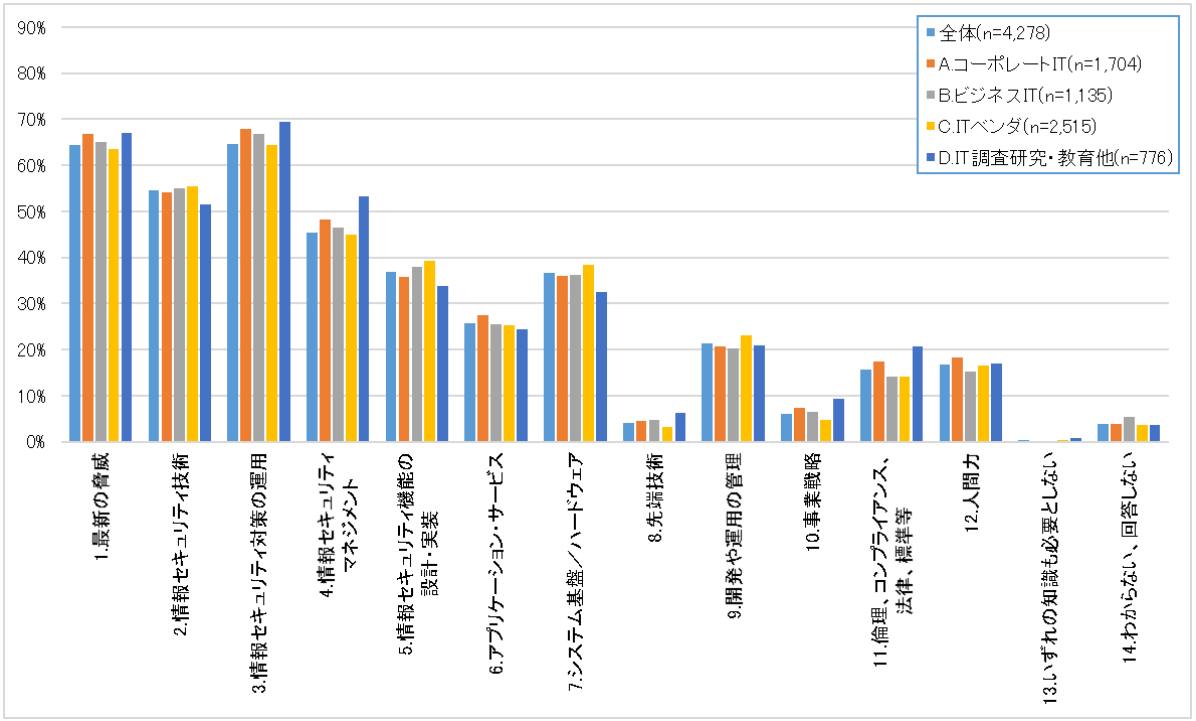


図 2-44 サイバーセキュリティ対策関連業務遂行に必要な知識・スキル(「システム運用」)

「システム運用」業務における活用知識・スキルは、運用に関わる知識・スキルの活用割合が大きいことは理解しやすい。加えて、「12.人間力」の知識・スキルの活用割合が「セキュア設計」業務の活用度合と比較すると若干高い。

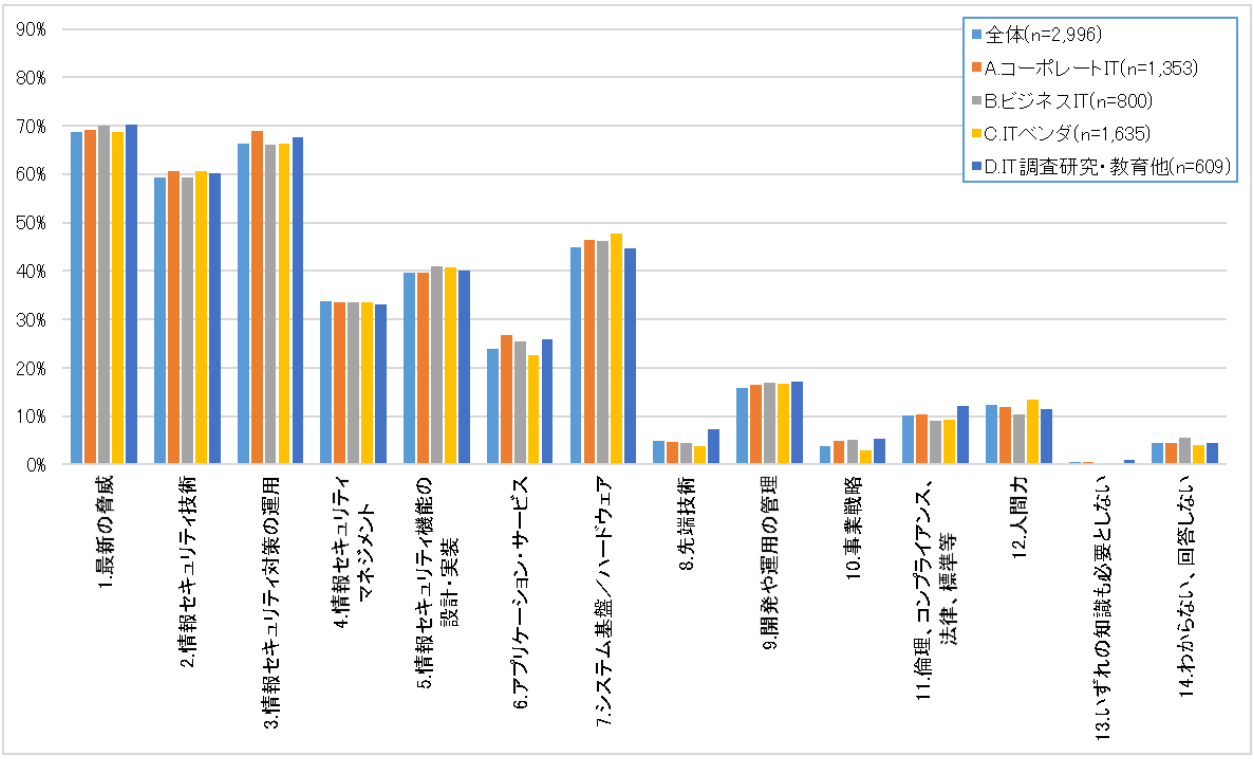


図 2-45 サイバーセキュリティ対策関連業務遂行に必要な知識・スキル(「機器運用保守」)

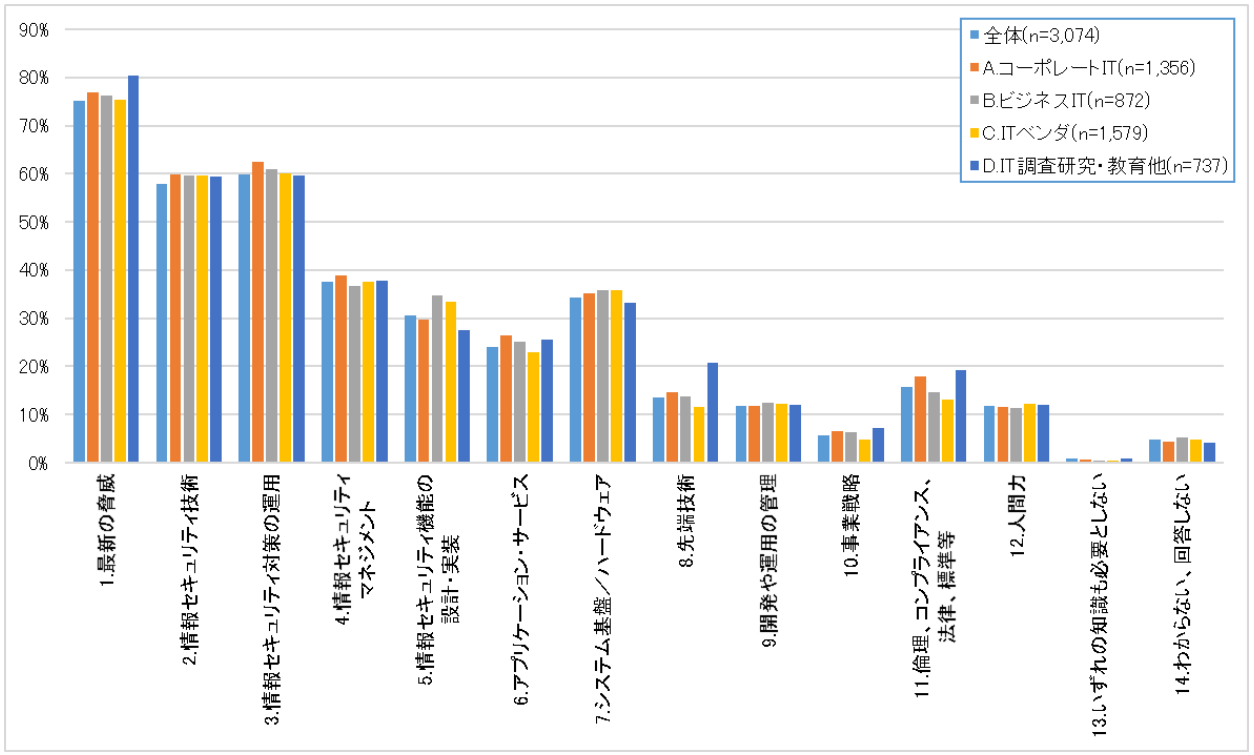


図 2-46 サイバーセキュリティ対策関連業務遂行に必要な知識・スキル(「監視・情報収集」)

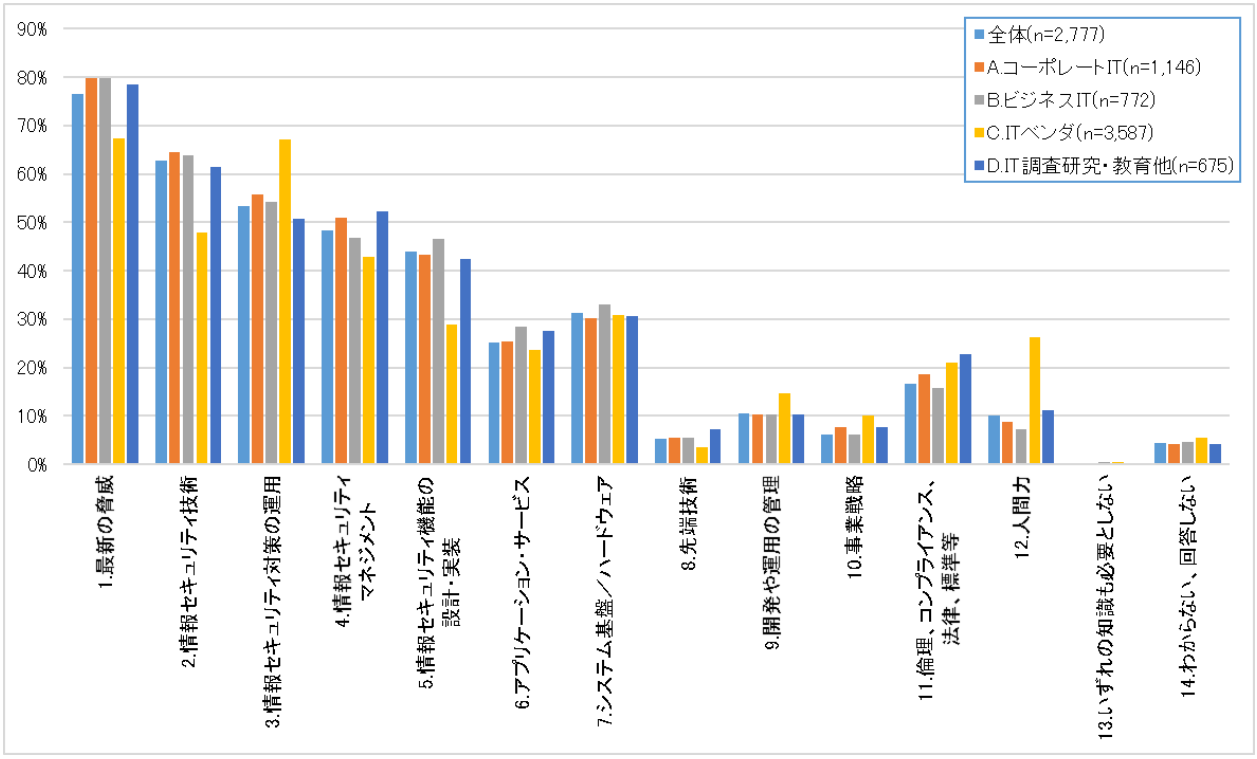


図 2-47 サイバーセキュリティ対策関連業務遂行に必要な知識・スキル(「脆弱性／監査」)

「脆弱性／監査」業務における活用知識・スキルは、(C)IT ベンダの傾向が他グループと異なっている。「脆弱性診断」の業務担当者と「情報セキュリティ監査」の業務担当者の割合の違いが影響している可能性がある。

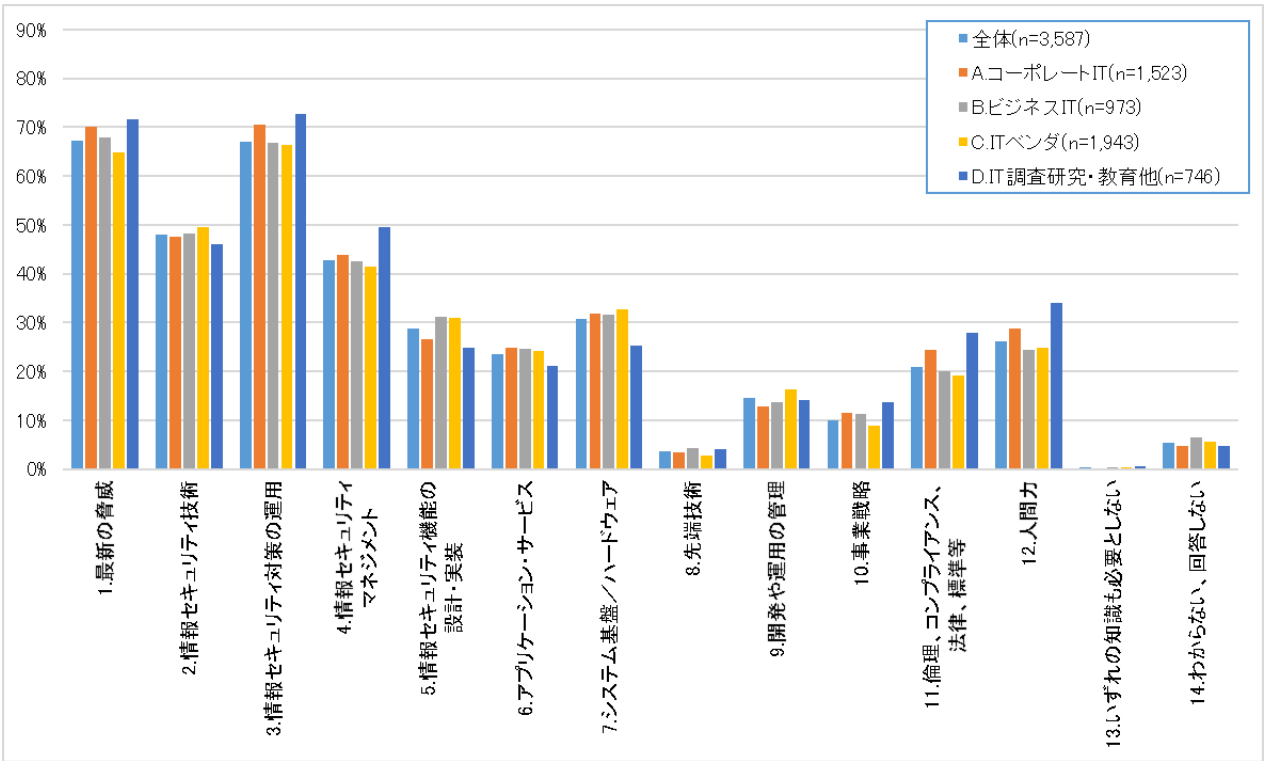


図 2-48 サイバーセキュリティ対策関連業務遂行に必要な知識・スキル(「インシデント」業務)

「インシデント」業務における活用知識・スキルは、「12.人間力」の知識・スキルの活用割合が比較的高い。インシデント対応は複数部署が連携して対応する業務であることを示していると考える。

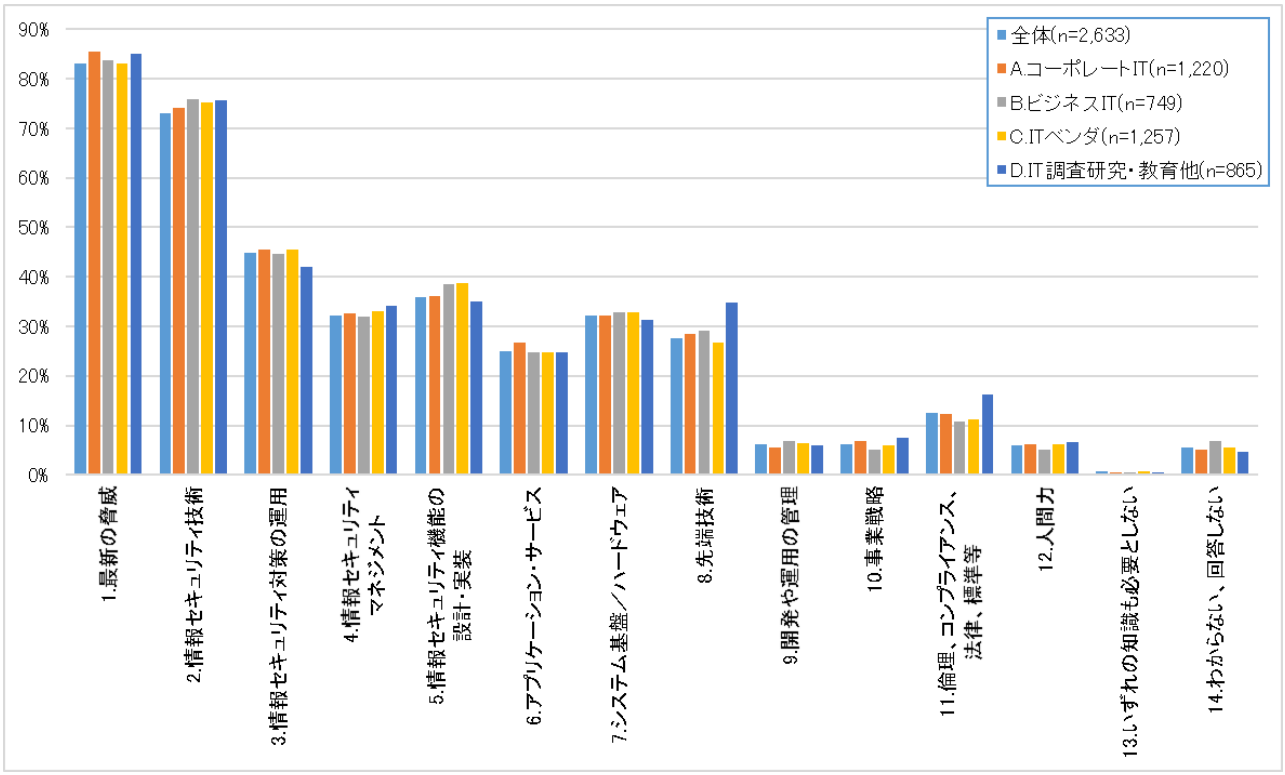


図 2-49 サイバーセキュリティ対策関連業務遂行に必要な知識・スキル(「調査研究」業務)

「調査研究」業務における活用知識・スキルは、技術系の知識・スキル(1.～8.以外)の活用割合が非常に低い。ここから、セキュリティに関する調査研究は、技術に特化した分野で行われているように思われる。

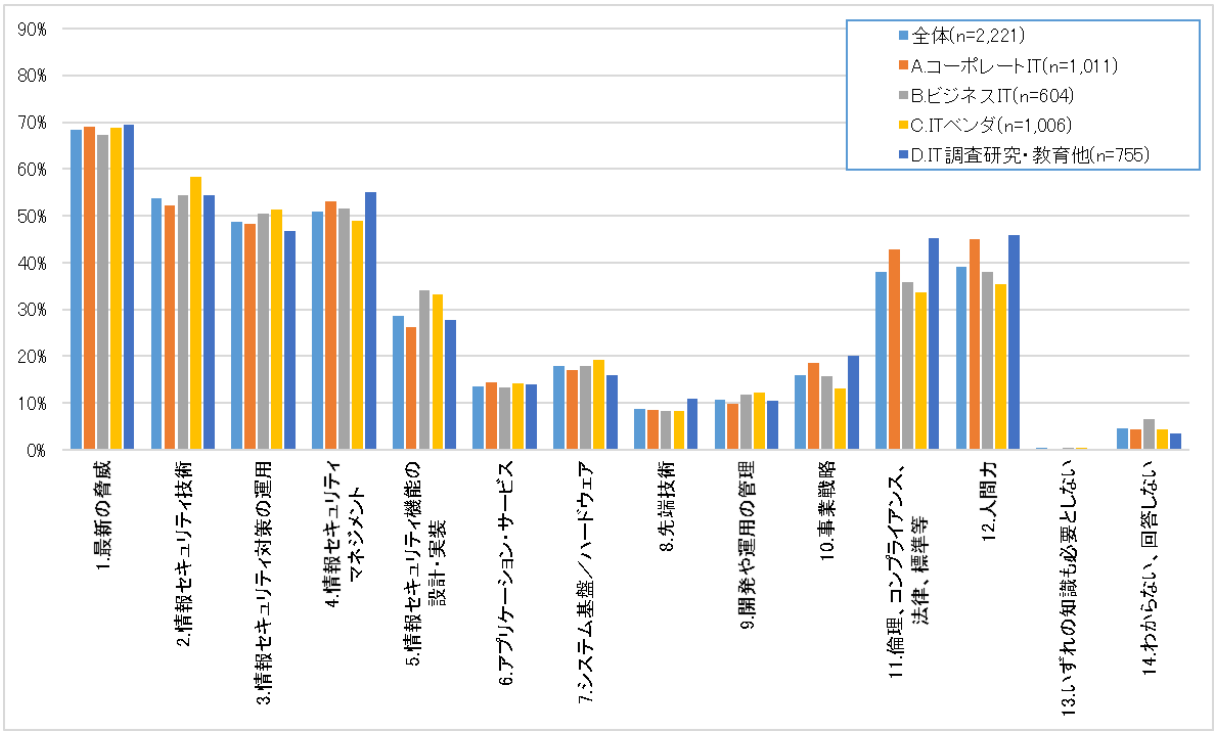


図 2-50 サイバーセキュリティ対策関連業務遂行に必要な知識・スキル(「教育・人材育成」業務)

「教育・人材育成」業務における活用知識・スキルを見ると、比較的幅広い知識・スキルが求められていることが分かる。

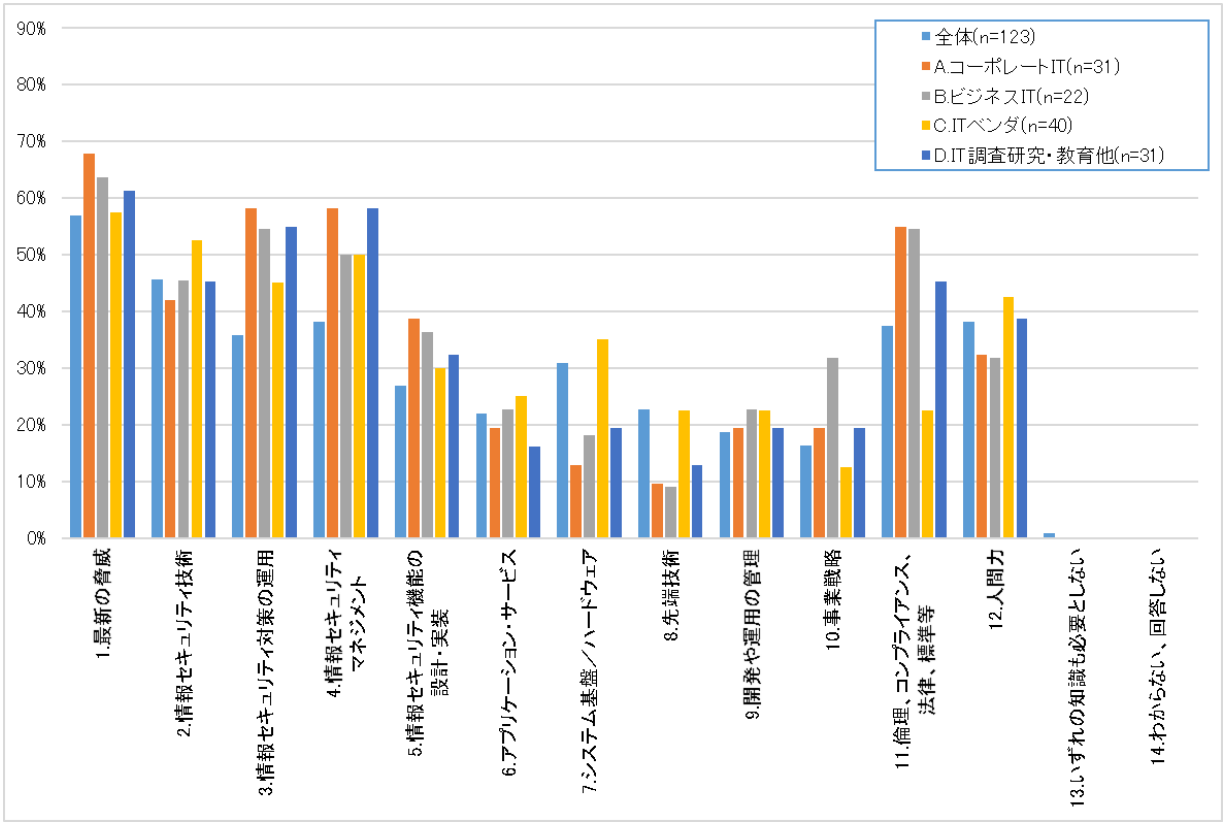


図 2-51 サイバーセキュリティ対策関連業務遂行に必要な知識・スキル(「その他」業務)

2.5. サイバーセキュリティ対策における部署間・組織間コミュニケーション

登録セキスペ及び高度 IT 人材のサイバーセキュリティ対策関連業務担当者に対し、業務の遂行の中でコミュニケーションを行う相手を確認した。

2.5.1. サイバーセキュリティ対策における部署間コミュニケーション

所属組織内のコミュニケーション相手を業務ごとに示す。全般的にコミュニケーション相手で多いのは「情報セキュリティマネジメント、CSIRT 等の担当者」及び「情報システム関連部門の担当者」であった。加えて、サイバーセキュリティの上流業務では、「経営層」とコミュニケーションをとる割合が高かった。

（設問文：あなたが所属する企業・団体の内部で、業務を通じて情報セキュリティ対策に関するコミュニケーション（会合での議論、依頼、情報提供、相談への対応等）を行う相手をすべて選択してください。※月 1 回以上のコミュニケーションがある相手をすべて選択してください。※間接的に情報セキュリティ対策に影響するもの（例：新技術を用いた製品の導入の相談）を含みます。※担当者同士が能動的にコミュニケーションを行うものに限定し、定期的な社内報の配信等は含めないでください。※ご自身がコミュニケーション相手に相当する場合や、自部署内の担当者の場合は選択しないでください。
選択肢：
(1) 経営層（代表者、取締役、執行役員、CIO、CISO、相談役等）
(2) 企画・人事・総務・経理・調達・購買等の部署の担当者
(3) 法務・コンプライアンスの担当者
(4) 情報セキュリティマネジメント、CSIRT、情報セキュリティ統括の担当者
(5) リスクマネジメントの担当者
(6) 品質管理の担当者
(7) 監査の担当者
(8) 研究所所属の担当者
(9) 教育・研修の担当者
(10) 情報システム関連部署の担当者
(11) 事業部門の担当者
(12) (1)～(11)以外の担当者
(13) 社内にはコミュニケーション相手が存在しない
(14) 回答しない）

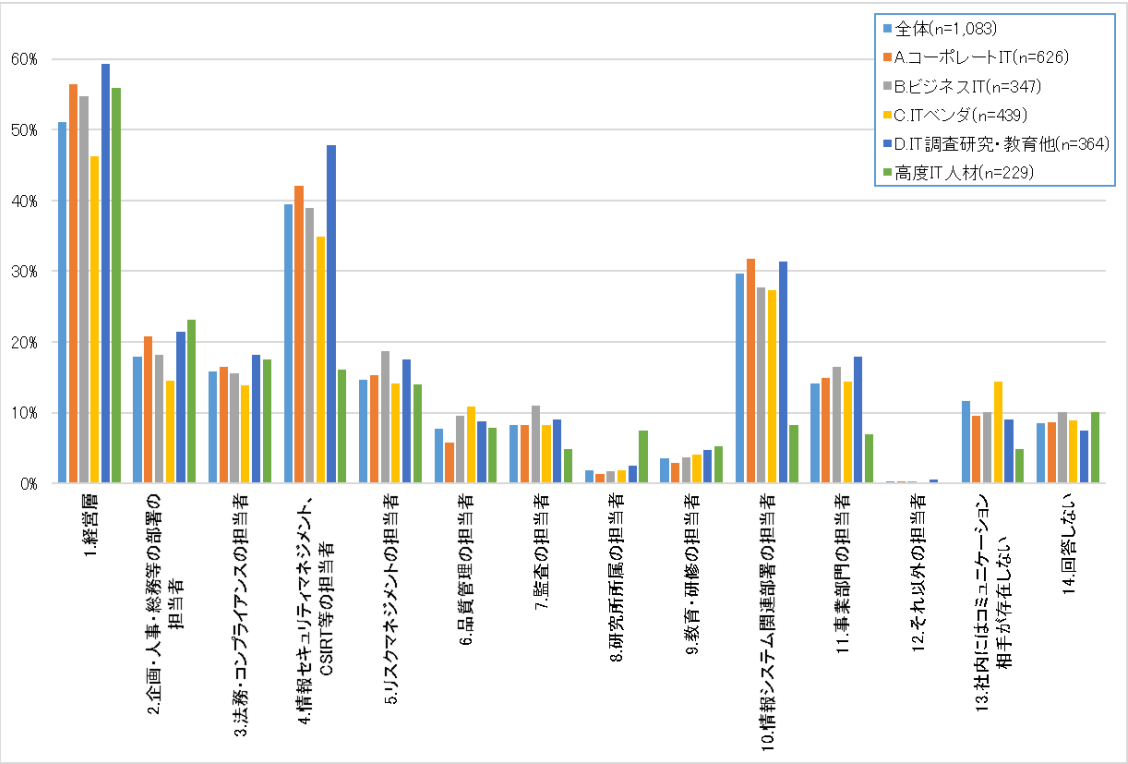


図 2-52 サイバーセキュリティ対策業務遂行上のコミュニケーション相手（自組織内、月 1 回以上）／「経営判断」

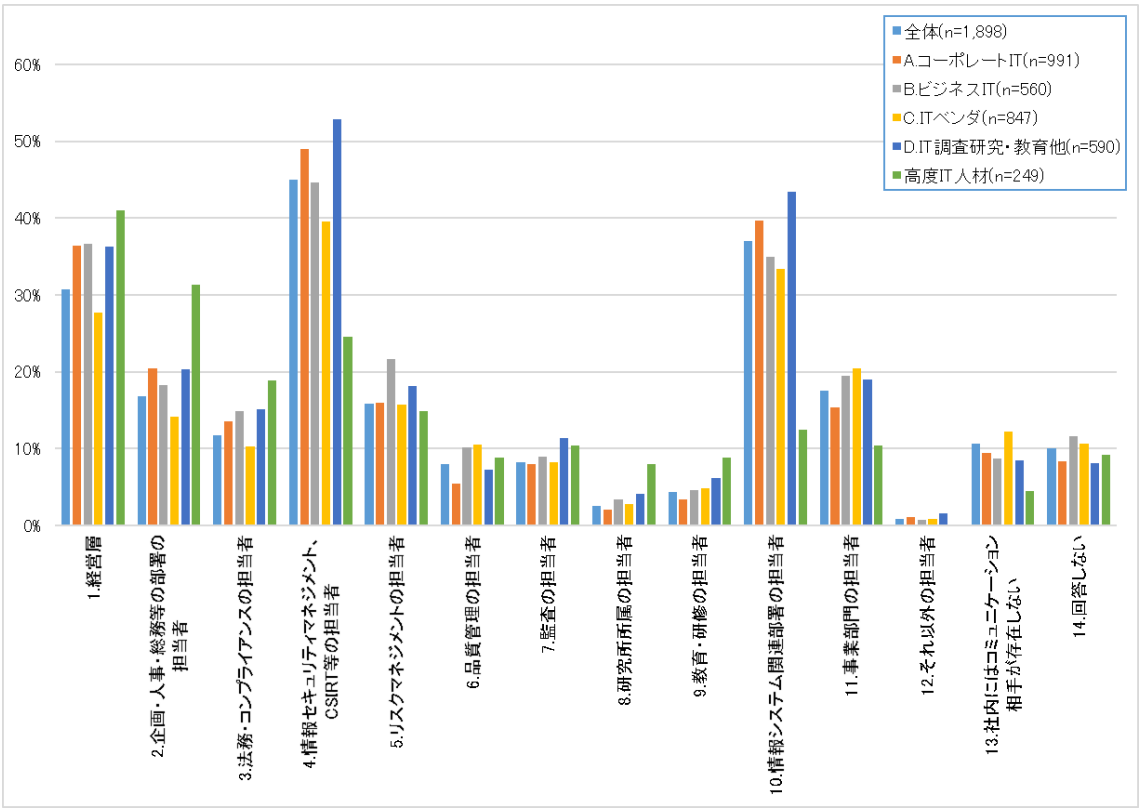


図 2-53 サイバーセキュリティ対策業務遂行上のコミュニケーション相手(自組織内、月 1 回以上)／「管理体制の構築」

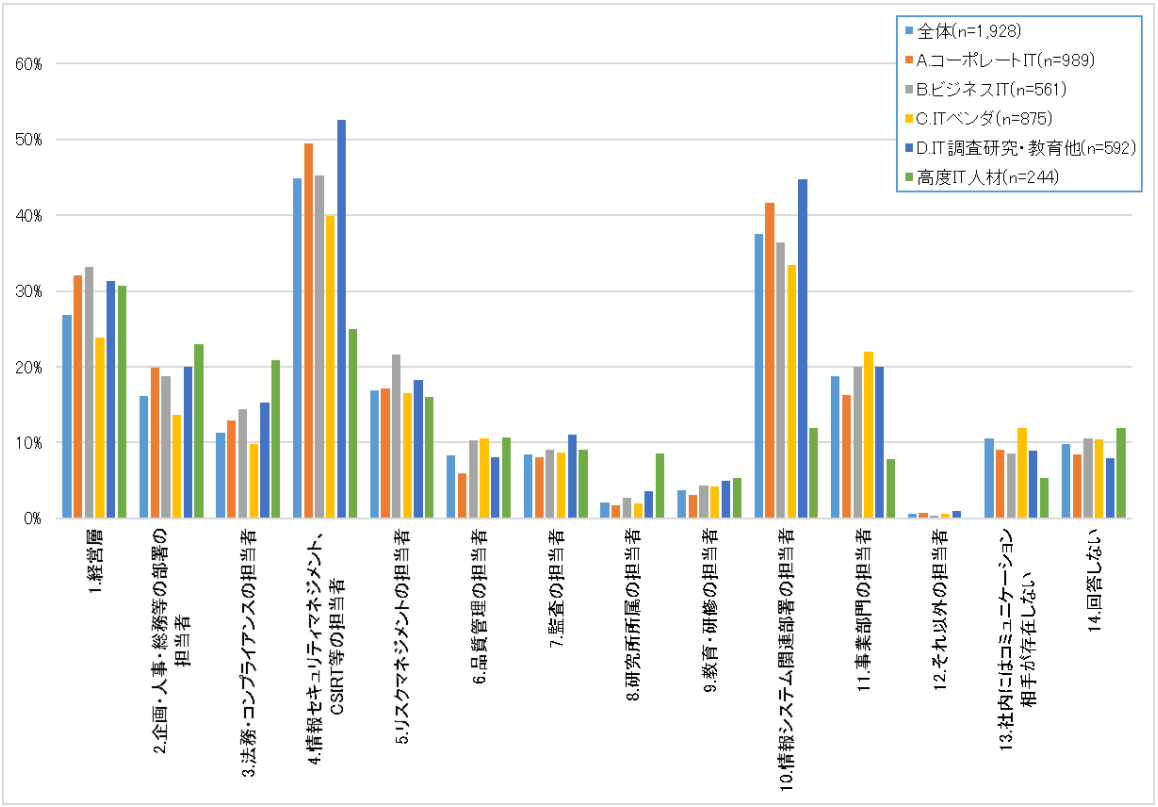


図 2-54 サイバーセキュリティ対策業務遂行上のコミュニケーション相手(自組織内、月 1 回以上)／「マネジメント」

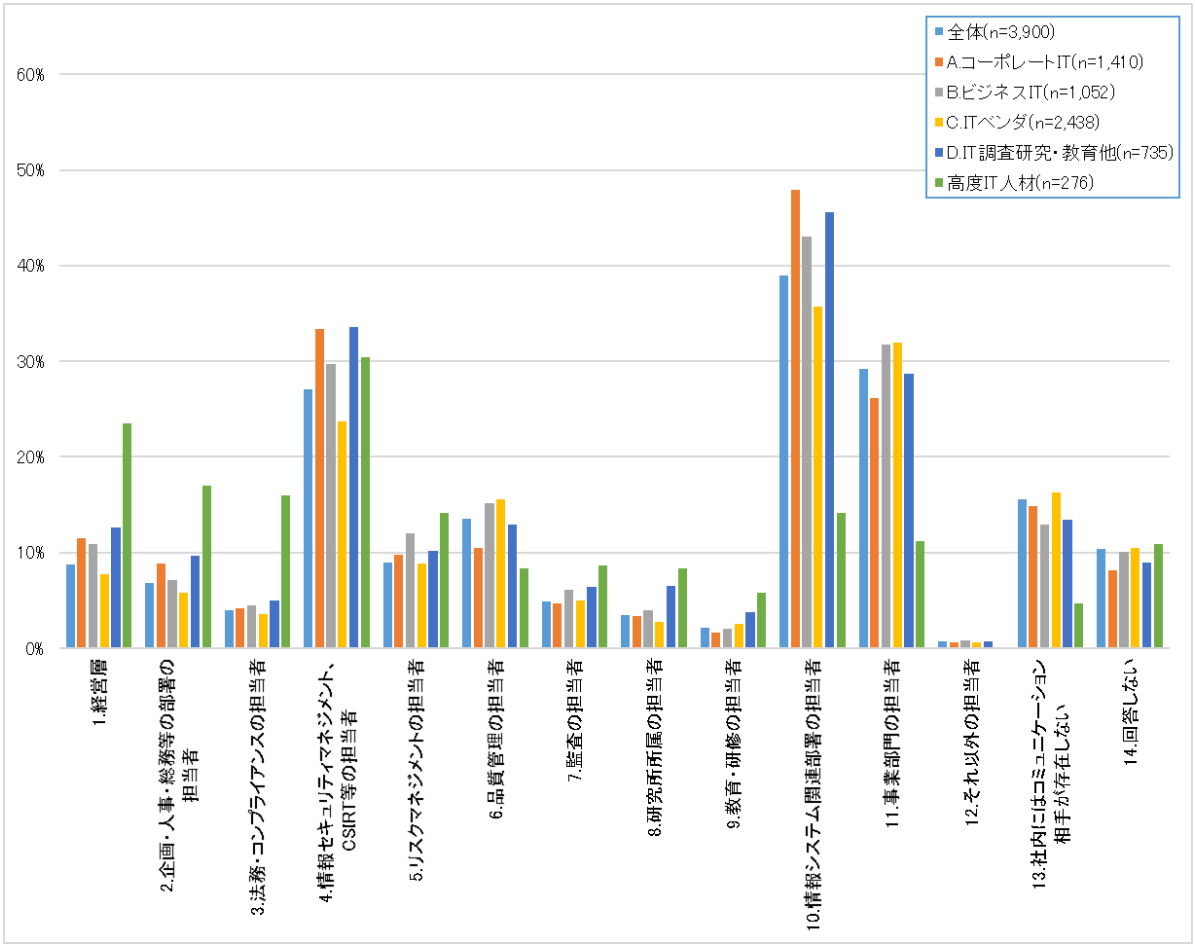


図 2-55 サイバーセキュリティ対策業務遂行上のコミュニケーション相手（自組織内、月 1 回以上）／「セキュア設計」

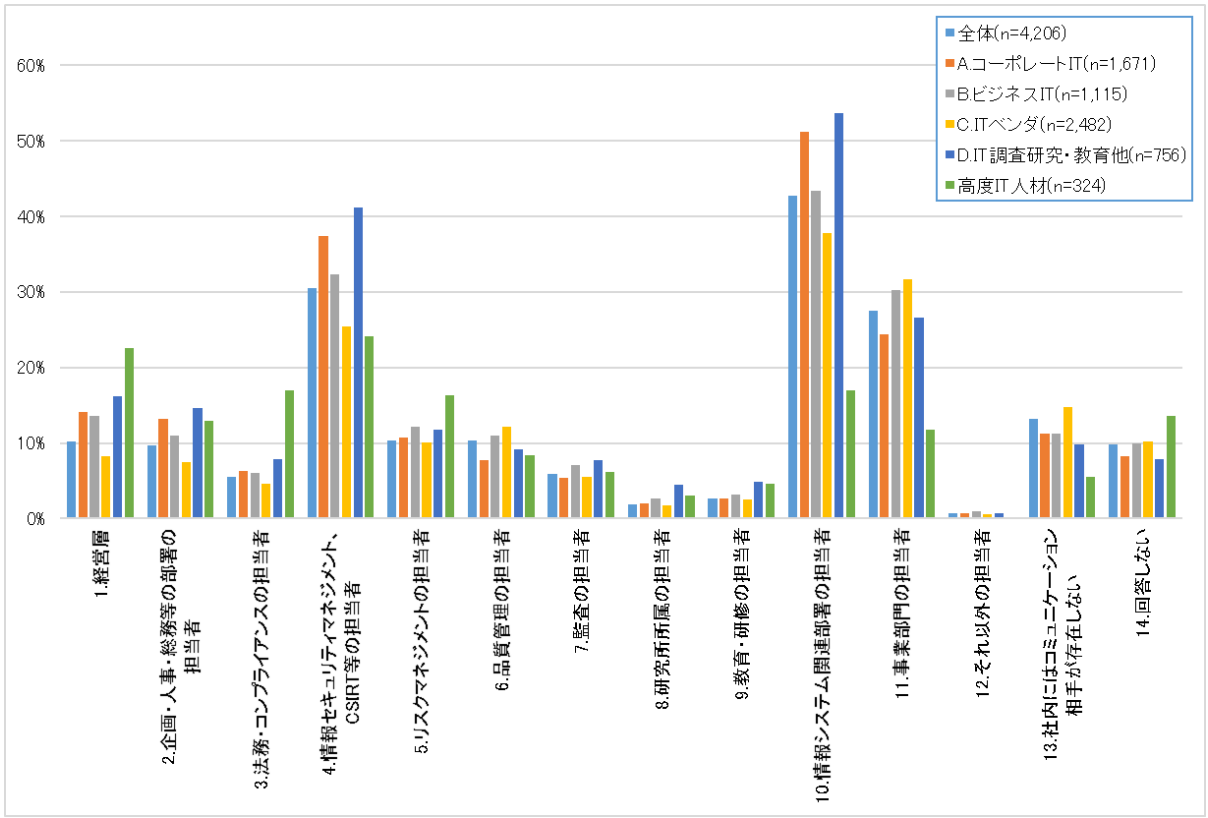


図 2-56 サイバーセキュリティ対策業務遂行上のコミュニケーション相手（自組織内、月 1 回以上）／「システム運用」

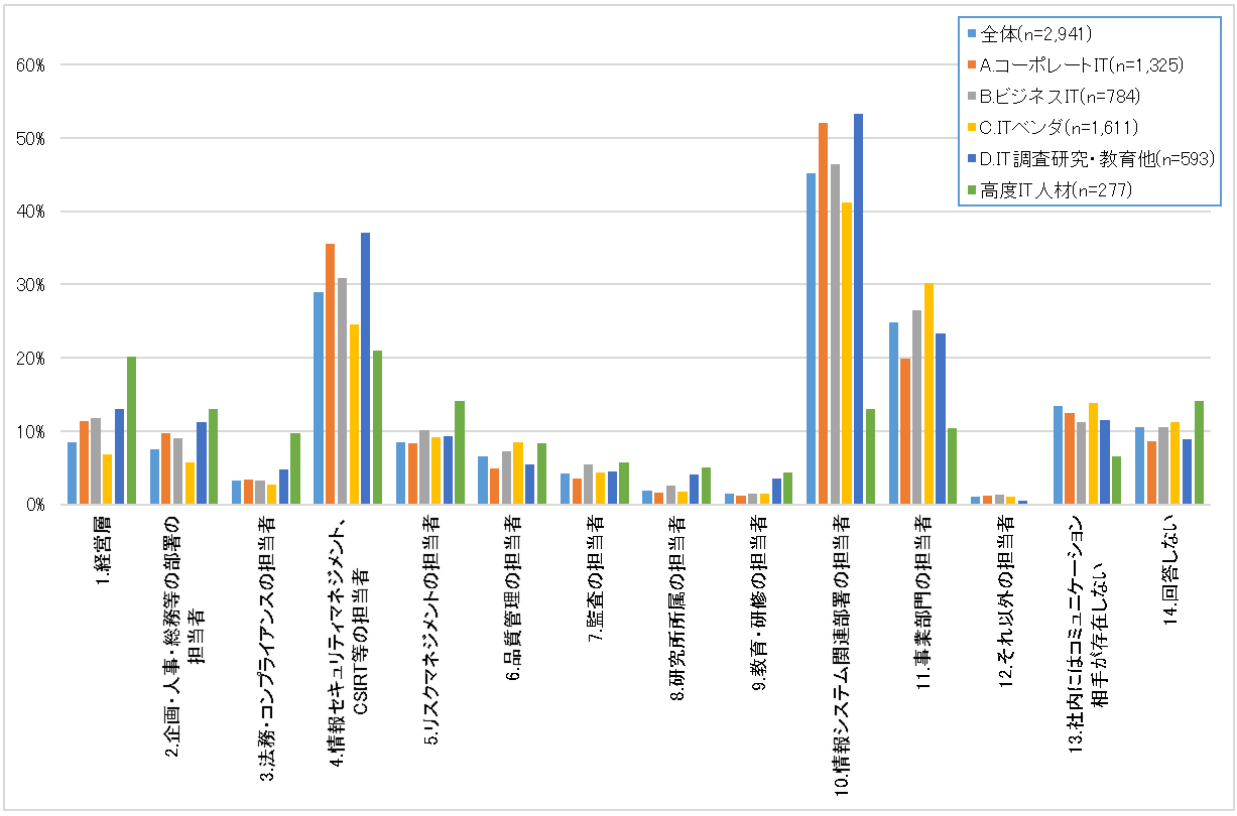


図 2-57 サイバーセキュリティ対策業務遂行上のコミュニケーション相手(自組織内、月 1 回以上)／「機器運用保守」

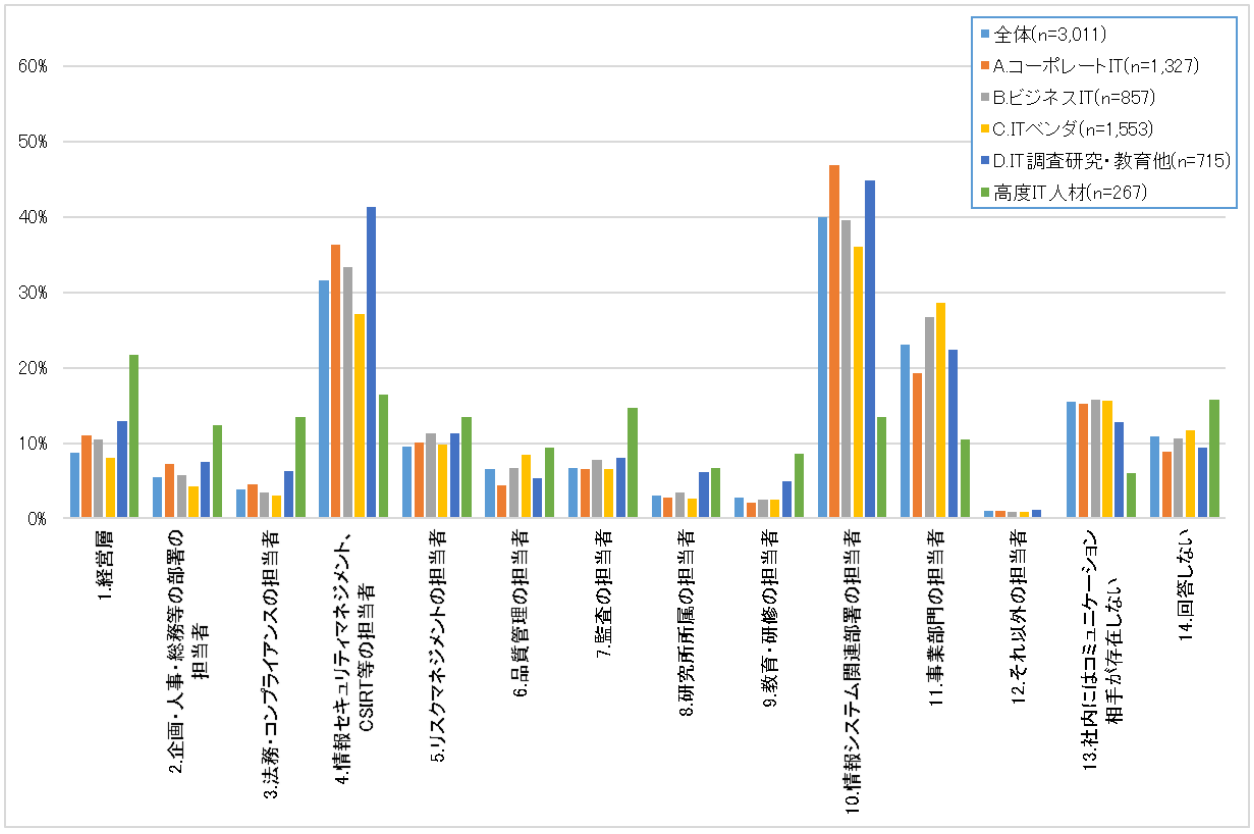


図 2-58 サイバーセキュリティ対策業務遂行上のコミュニケーション相手(自組織内、月 1 回以上)／「監視・情報収集」

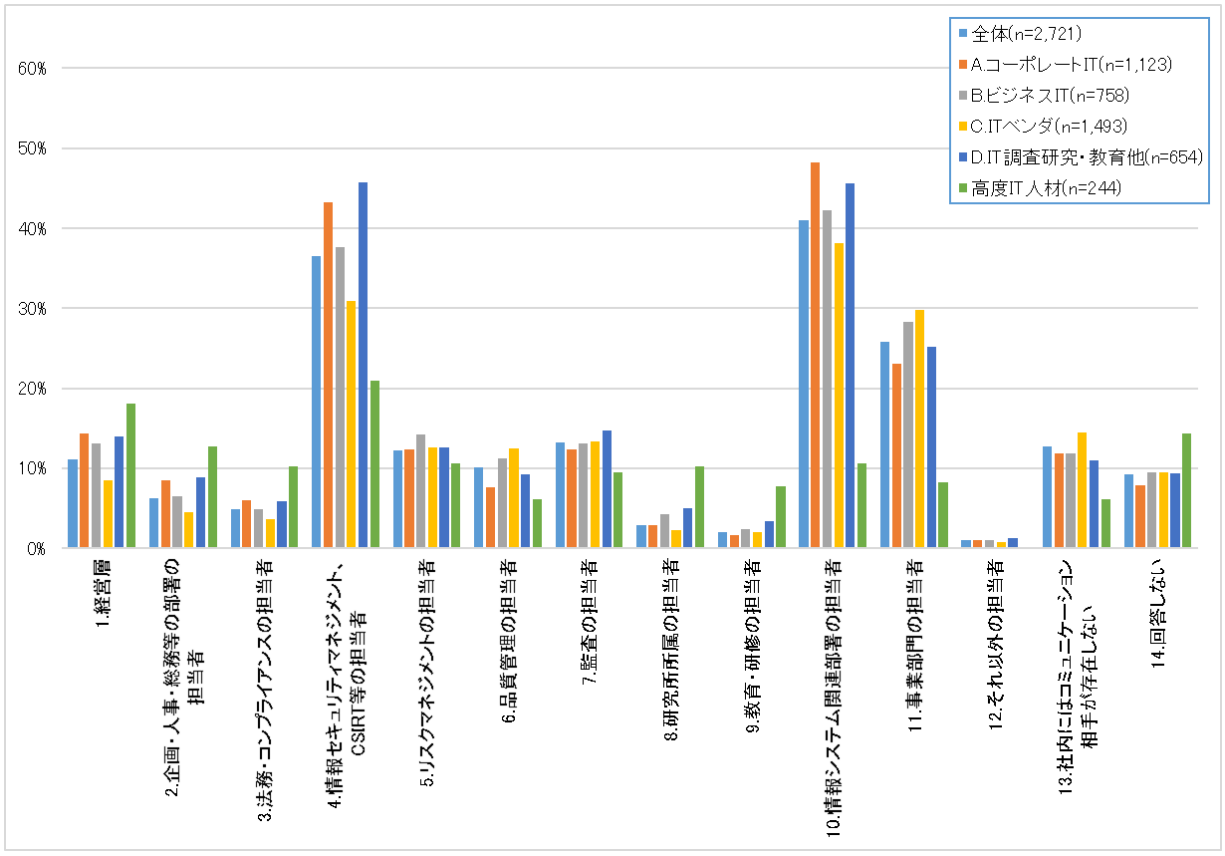


図 2-59 サイバーセキュリティ対策業務遂行上のコミュニケーション相手(自組織内、月 1 回以上)／「脆弱性／監査」

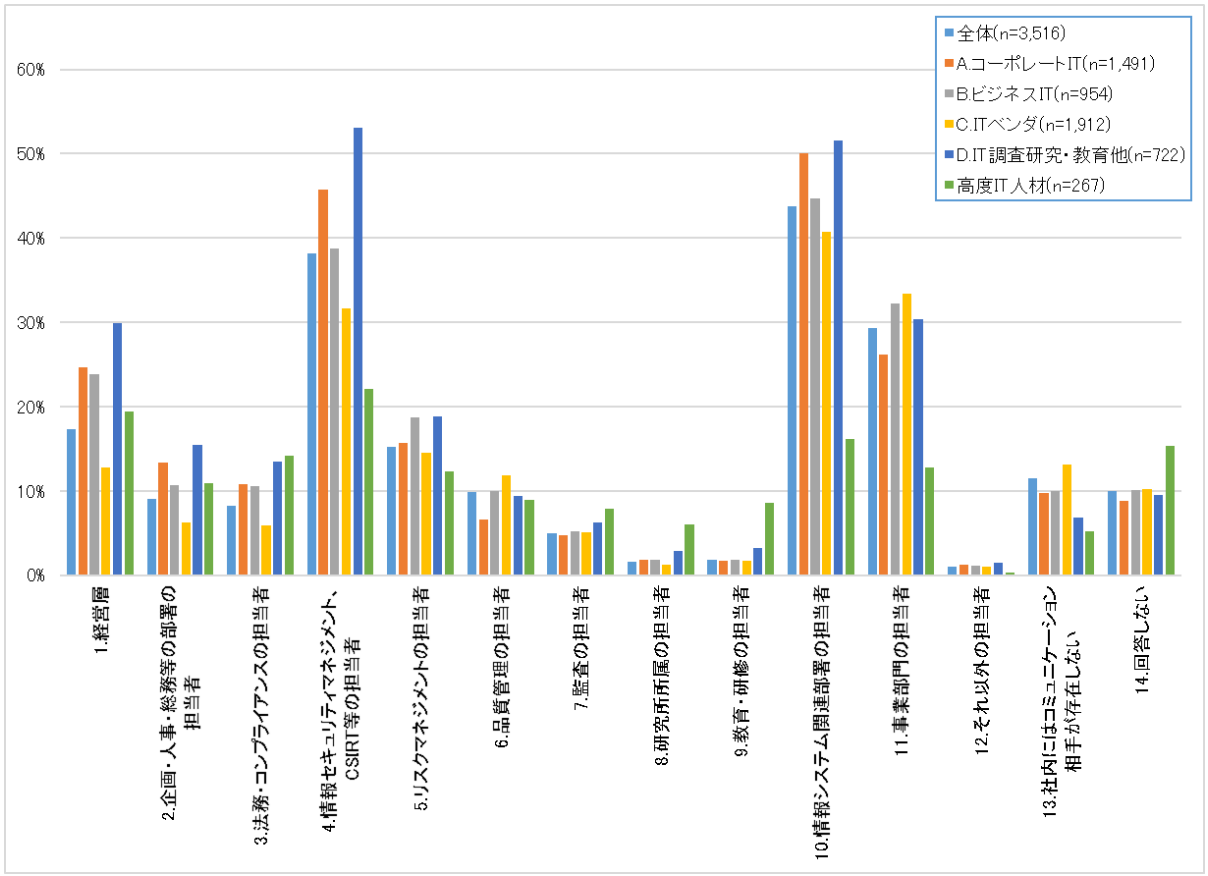


図 2-60 サイバーセキュリティ対策業務遂行上のコミュニケーション相手(自組織内、月 1 回以上)／「インシデント」

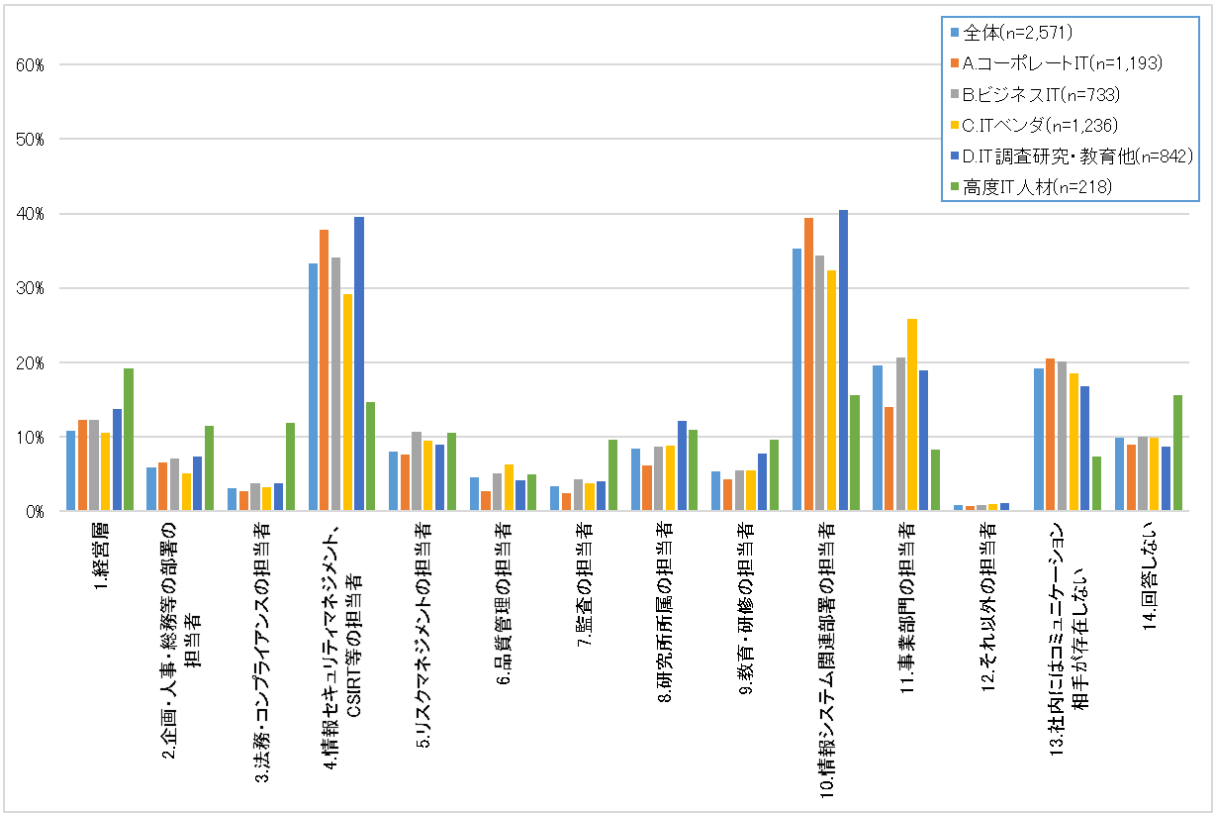


図 2-61 サイバーセキュリティ対策業務遂行上のコミュニケーション相手(自組織内、月 1 回以上)／「調査研究」

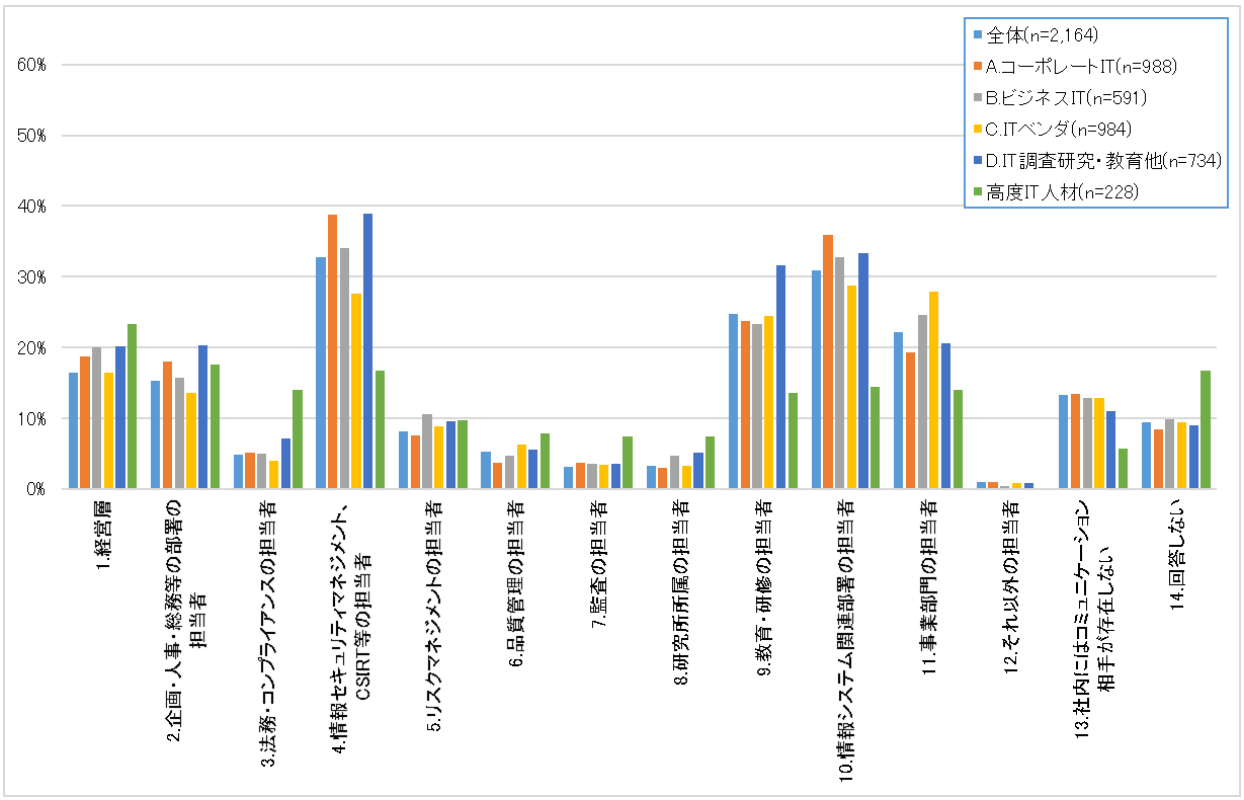


図 2-62 サイバーセキュリティ対策業務遂行上のコミュニケーション相手(自組織内、月 1 回以上)／「教育・人材育成」

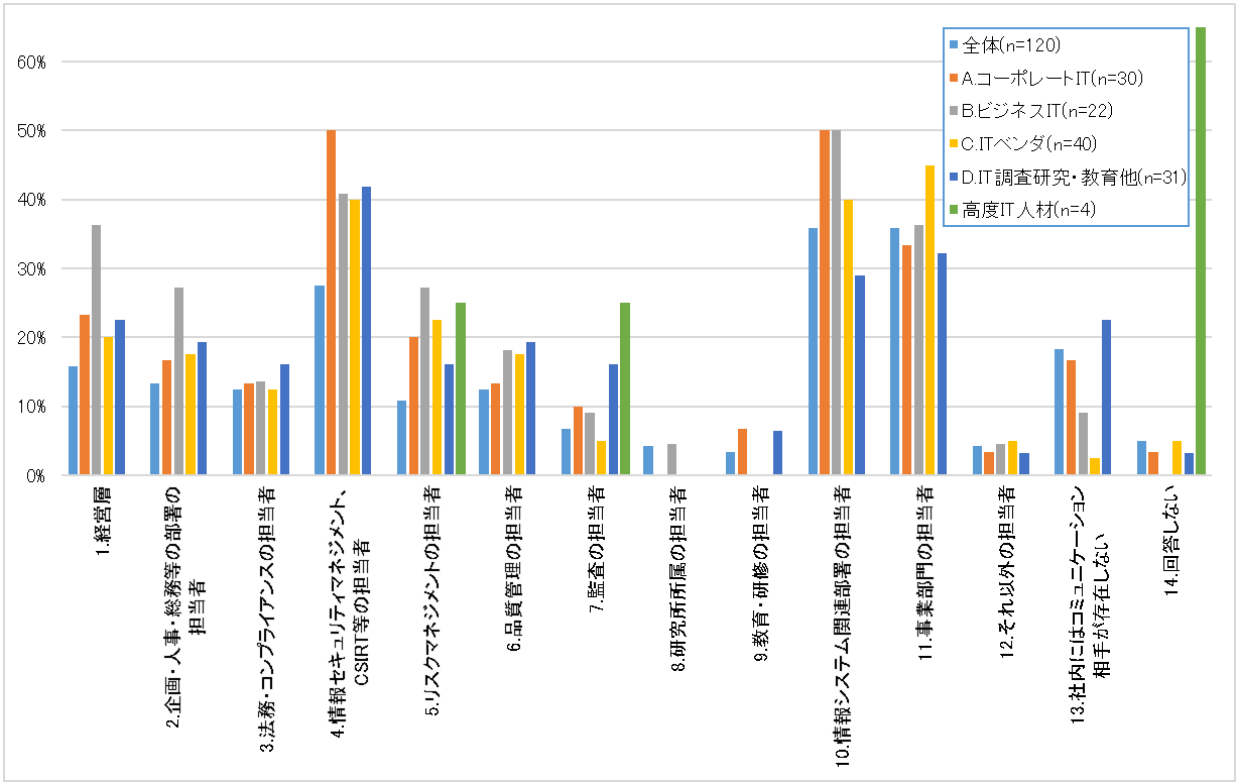


図 2-63 サイバーセキュリティ対策業務遂行上のコミュニケーション相手(自組織内、月 1 回以上)／「その他」

2.5.2. サイバーセキュリティ対策における組織間コミュニケーション

次に、自組織の外部とのコミュニケーション相手を担当業務ごとに示す。(C)IT ベンダは全般的に「顧客・業務委託元」とのコミュニケーションをとる割合が多く、「システム運用」や「機器の運用保守」、「監視・情報収集」業務では業務委託先やセキュリティサービスのベンダなどとやり取りする割合が高かった(3 割程度)。

(設問文:あなたが所属する企業・団体の外部で、情報セキュリティ対策に関するコミュニケーション(受発注、契約、相談、調整、意見交換等)を行う相手をすべて選択してください。
※月 1 回以上のコミュニケーションがある相手をすべて選択してください。
※コミュニケーションには、間接的に情報セキュリティ対策に影響するもの(例:新技術を用いた製品の導入の相談)を含みます。
※担当者同士が能動的にコミュニケーションを行うものに限定し、定期的なマルウェア警戒情報の配信等は含みません。
選択肢:
(1)顧客(BtoC 事業の顧客を除く)・業務委託元(親会社を除く)
(2)親会社
(3)子会社、グループ企業
(4)業務委託先(セキュリティサービスのベンダを除く)
(5)セキュリティサービスのベンダ
(6)製品ベンダ、販売店
(7)監督官庁、自治体窓口
(8)共同研究やコンソーシアムのパートナー(企業、大学など)
(9)(1)～(8)以外の方
(10)社外にはコミュニケーション相手が存在しない
(11)回答しない
)

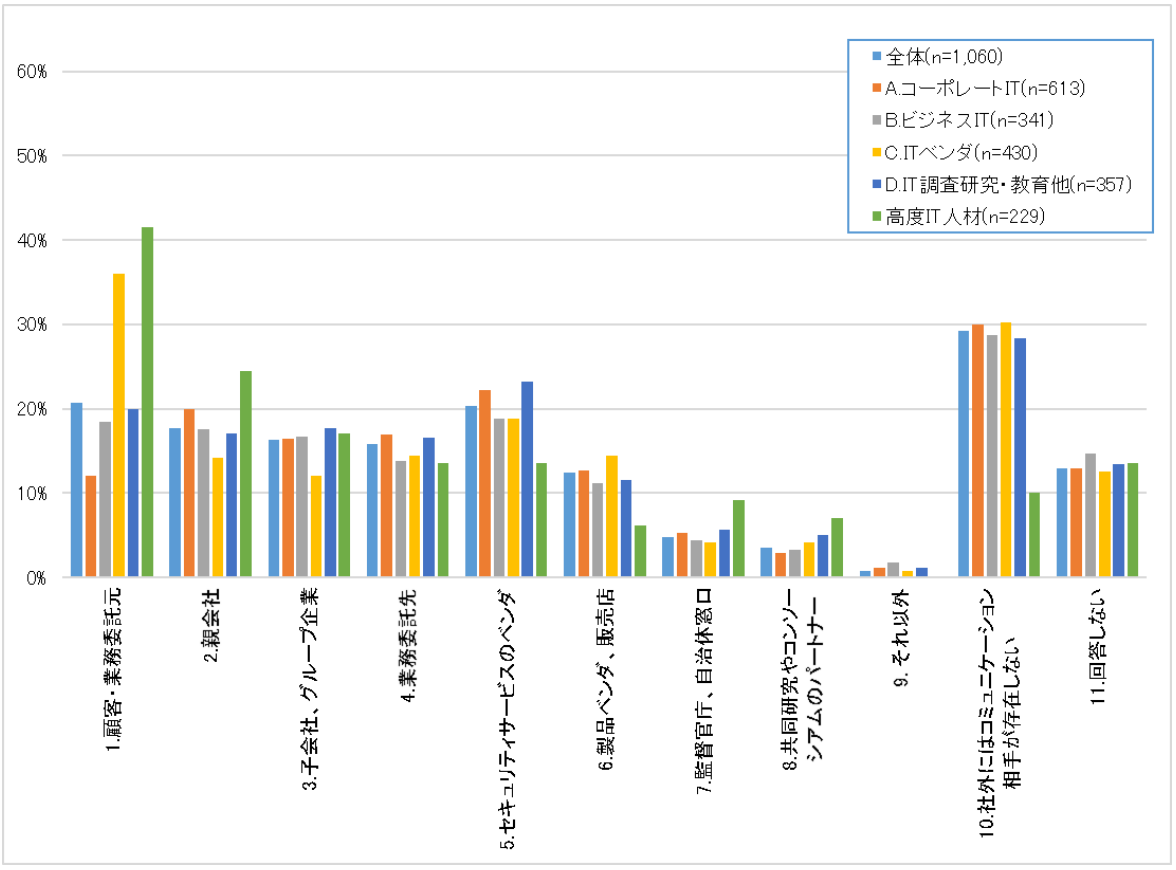


図 2-64 サイバーセキュリティ対策業務遂行上のコミュニケーション相手（自組織外、月 1 回以上）／「経営判断」

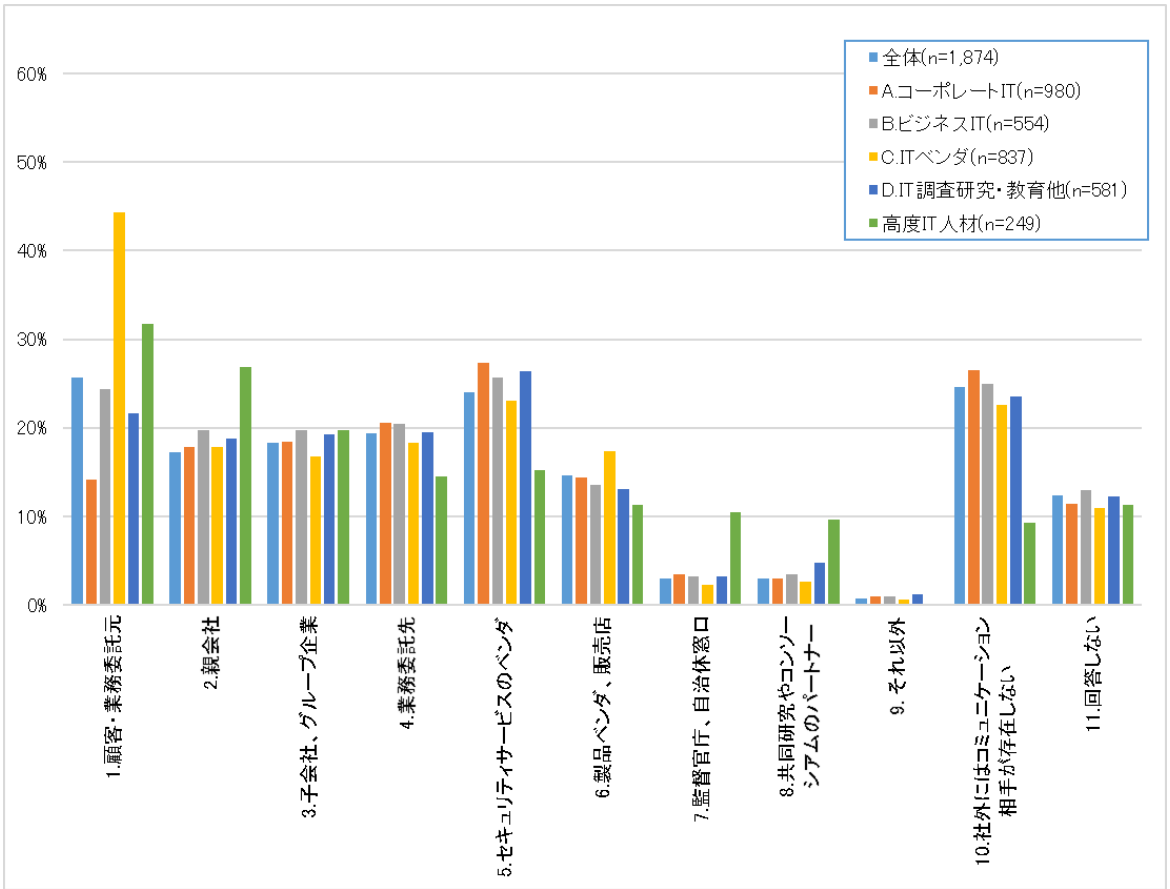


図 2-65 サイバーセキュリティ対策業務遂行上のコミュニケーション相手（自組織外、月 1 回以上）／「管理体制の構築」

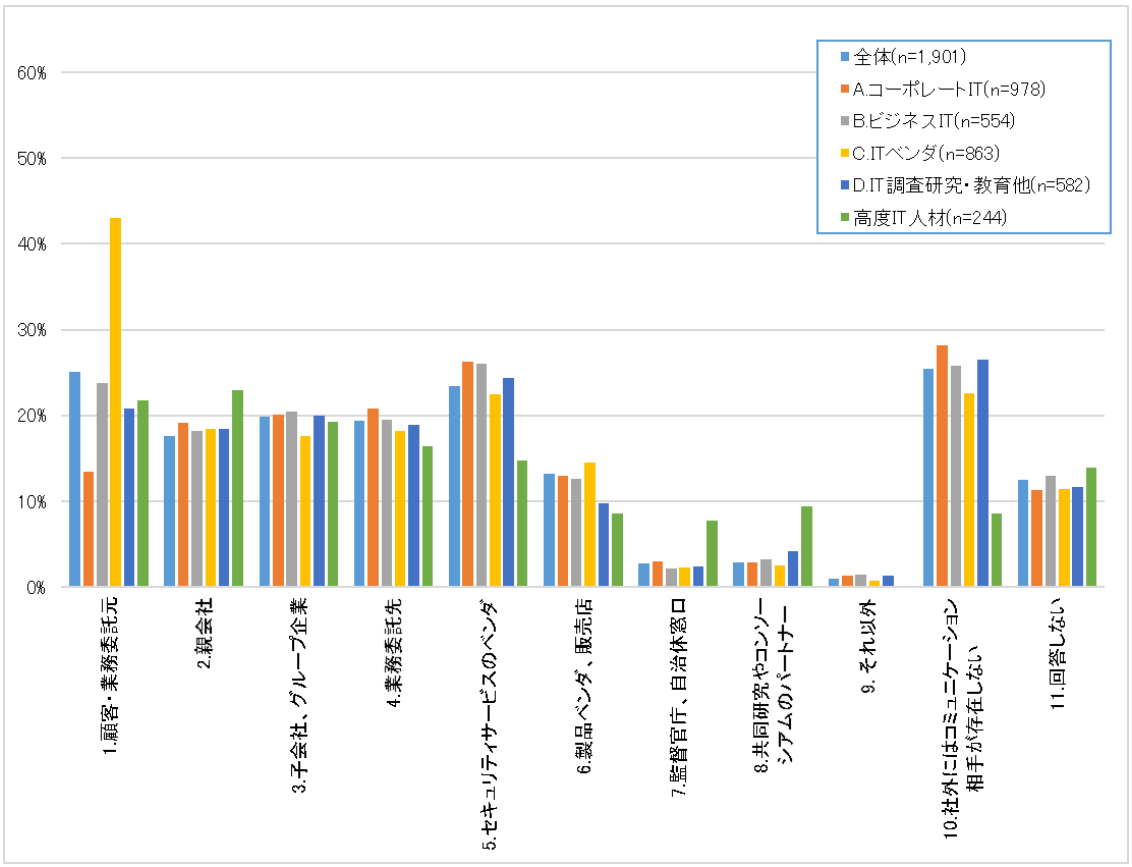


図 2-66 サイバーセキュリティ対策業務遂行上のコミュニケーション相手（自組織外、月 1 回以上）／「マネジメント」

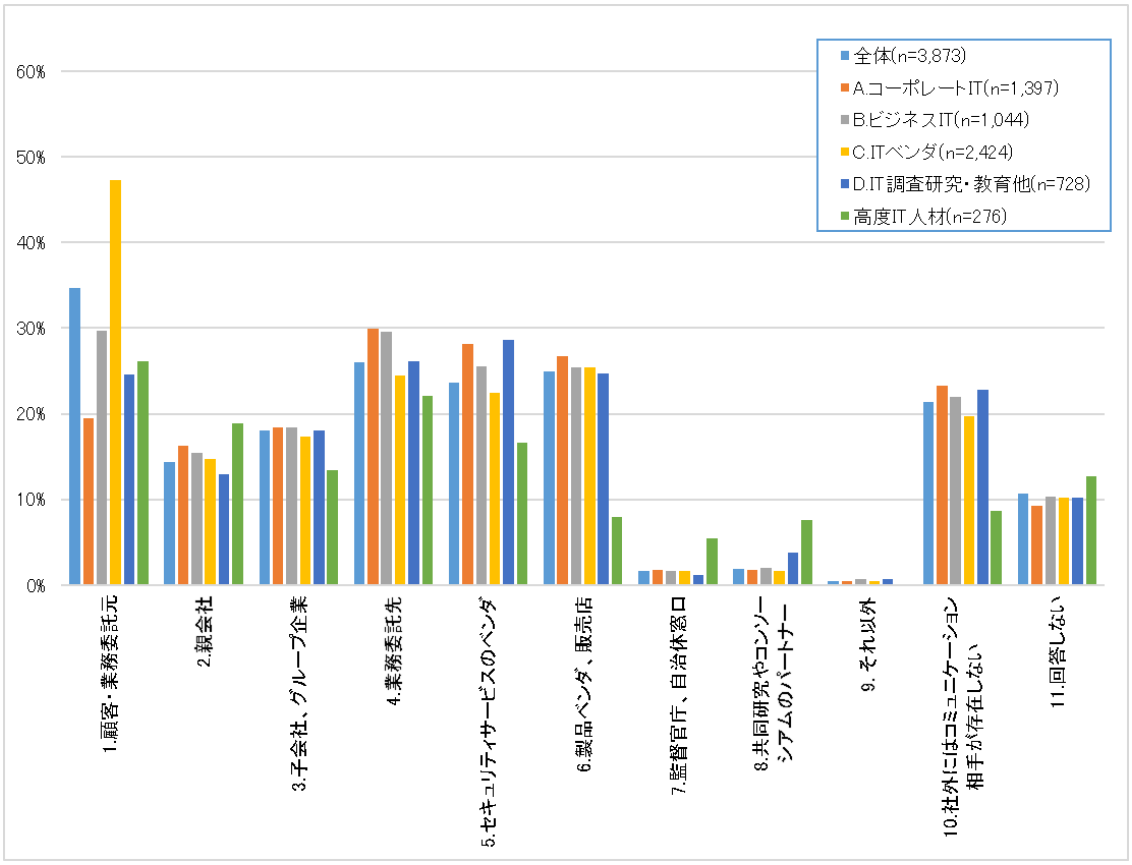


図 2-67 サイバーセキュリティ対策業務遂行上のコミュニケーション相手（自組織外、月 1 回以上）／「セキュア設計」

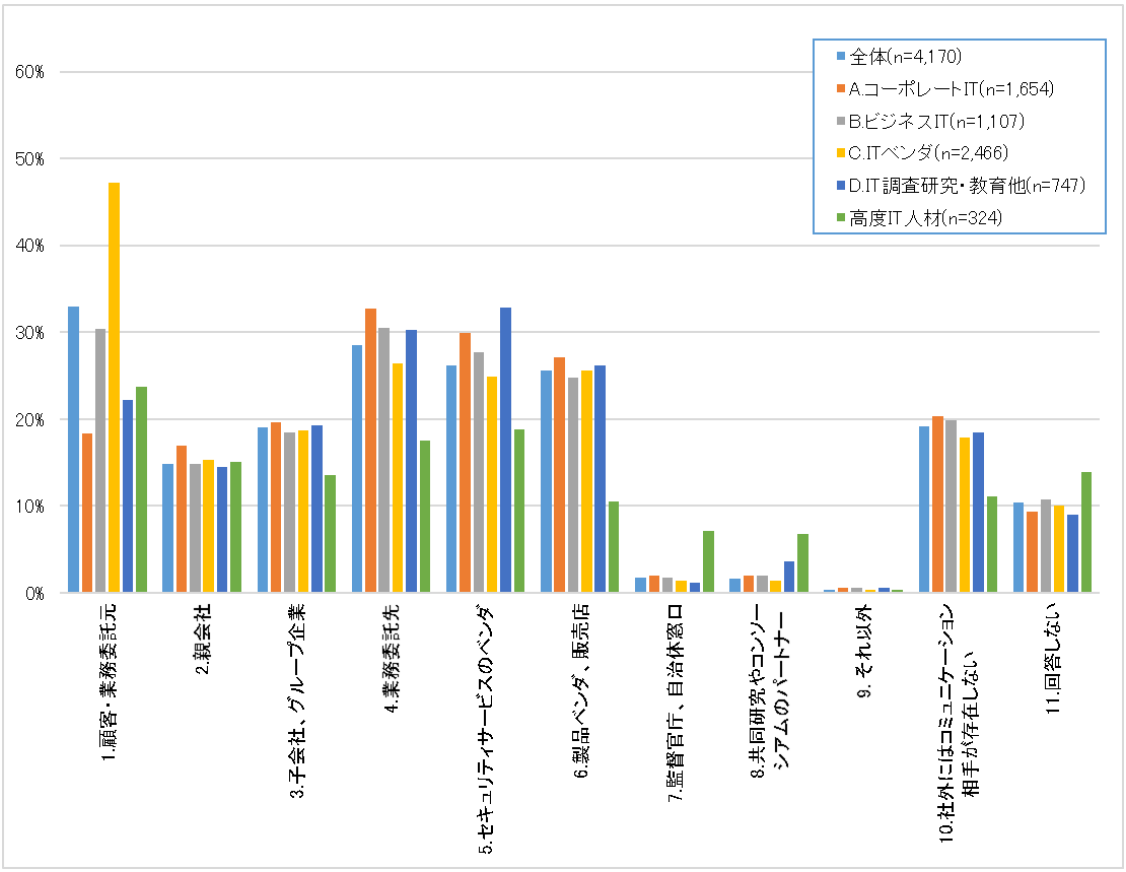


図 2-68 サイバーセキュリティ対策業務遂行上のコミュニケーション相手(自組織外、月 1 回以上)／「システム運用」

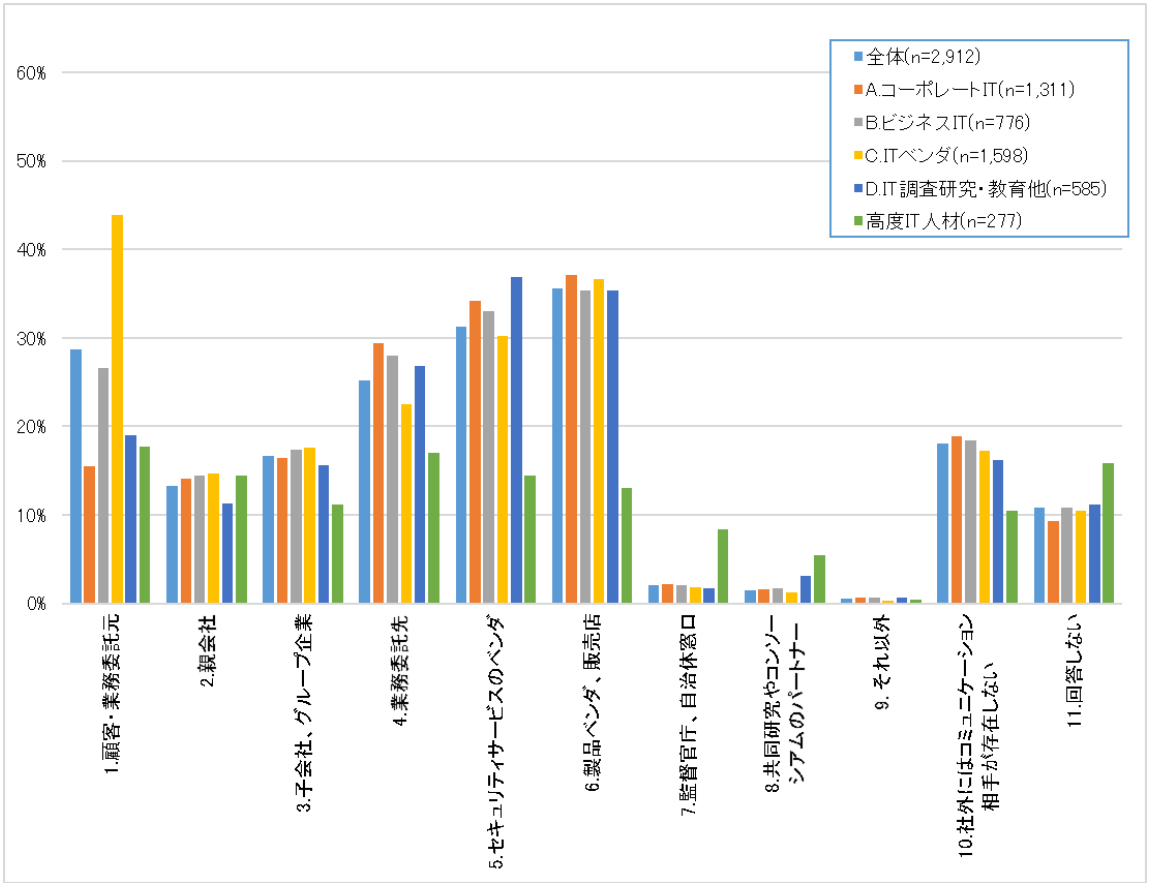


図 2-69 サイバーセキュリティ対策業務遂行上のコミュニケーション相手(自組織外、月 1 回以上)／「機器運用保守」

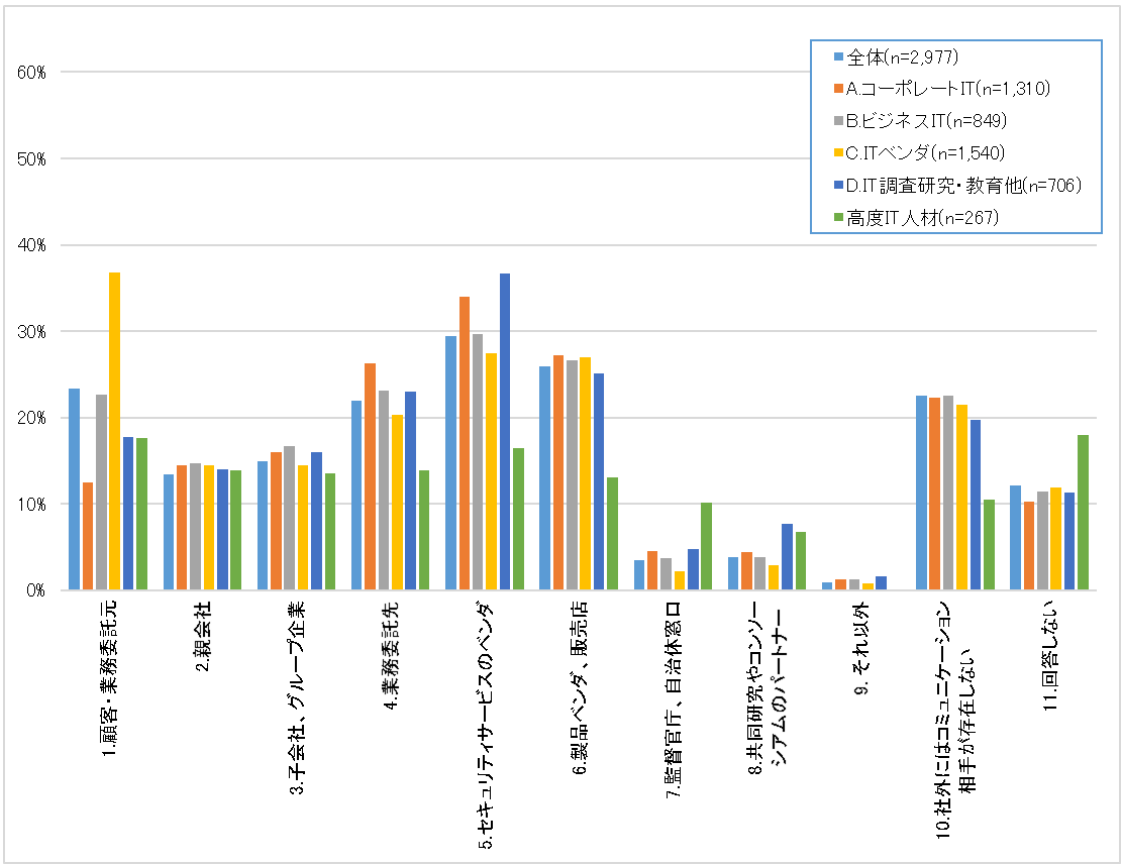


図 2-70 サイバーセキュリティ対策業務遂行上のコミュニケーション相手（自組織外、月 1 回以上）／「監視・情報収集」

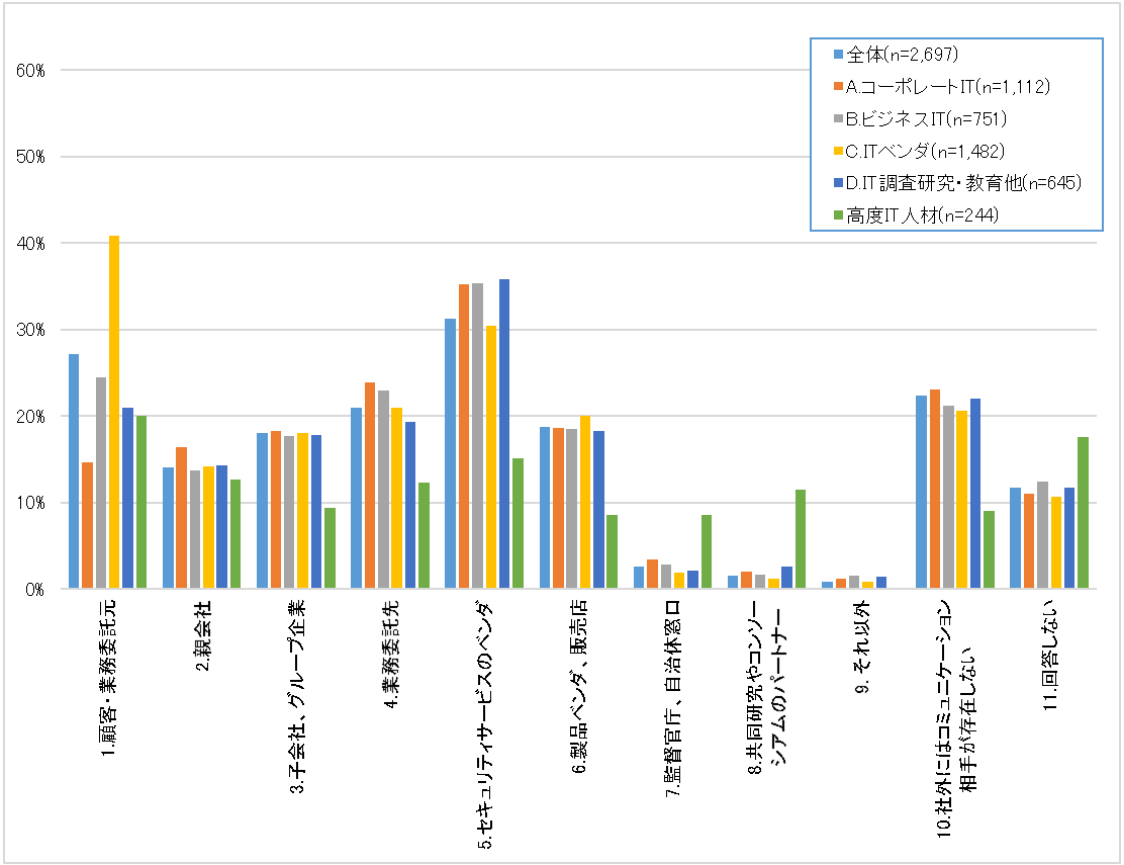


図 2-71 サイバーセキュリティ対策業務遂行上のコミュニケーション相手（自組織外、月 1 回以上）／「脆弱性／監査」

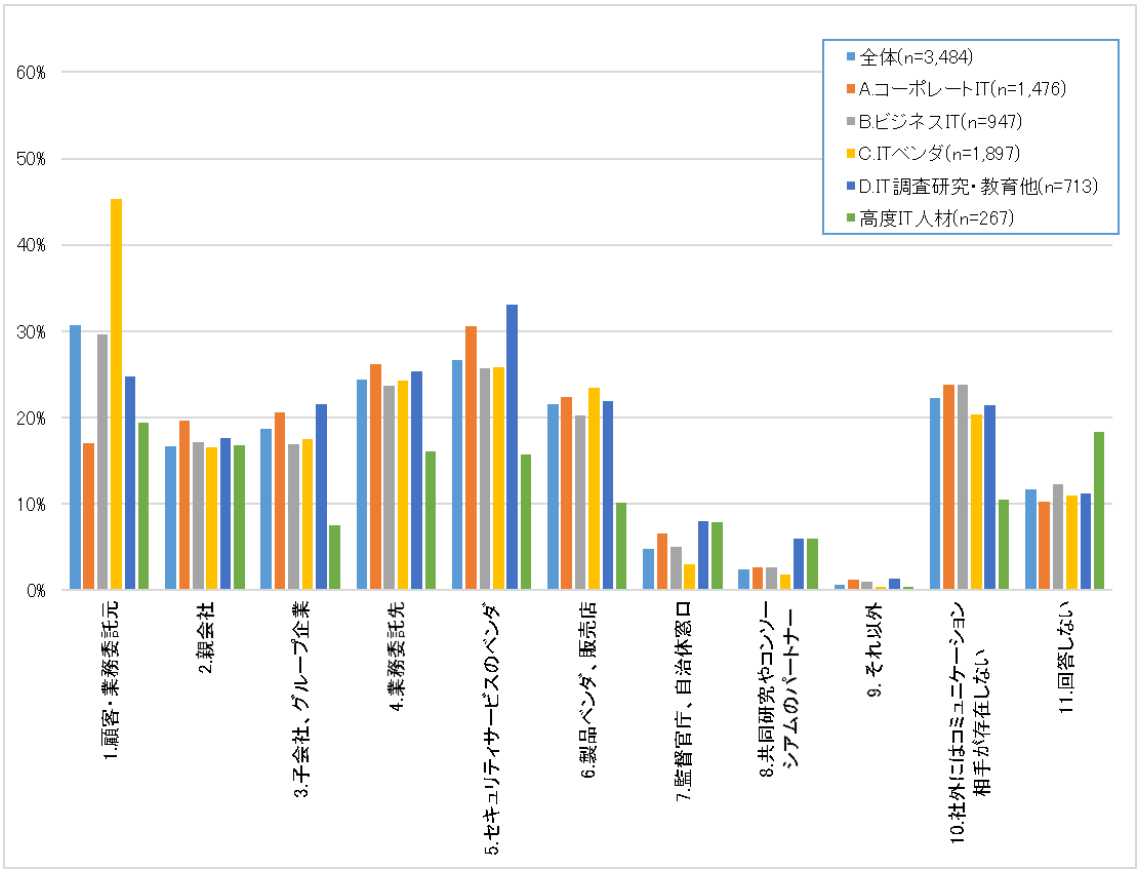


図 2-72 サイバーセキュリティ対策業務遂行上のコミュニケーション相手（自組織外、月 1 回以上）／「インシデント」

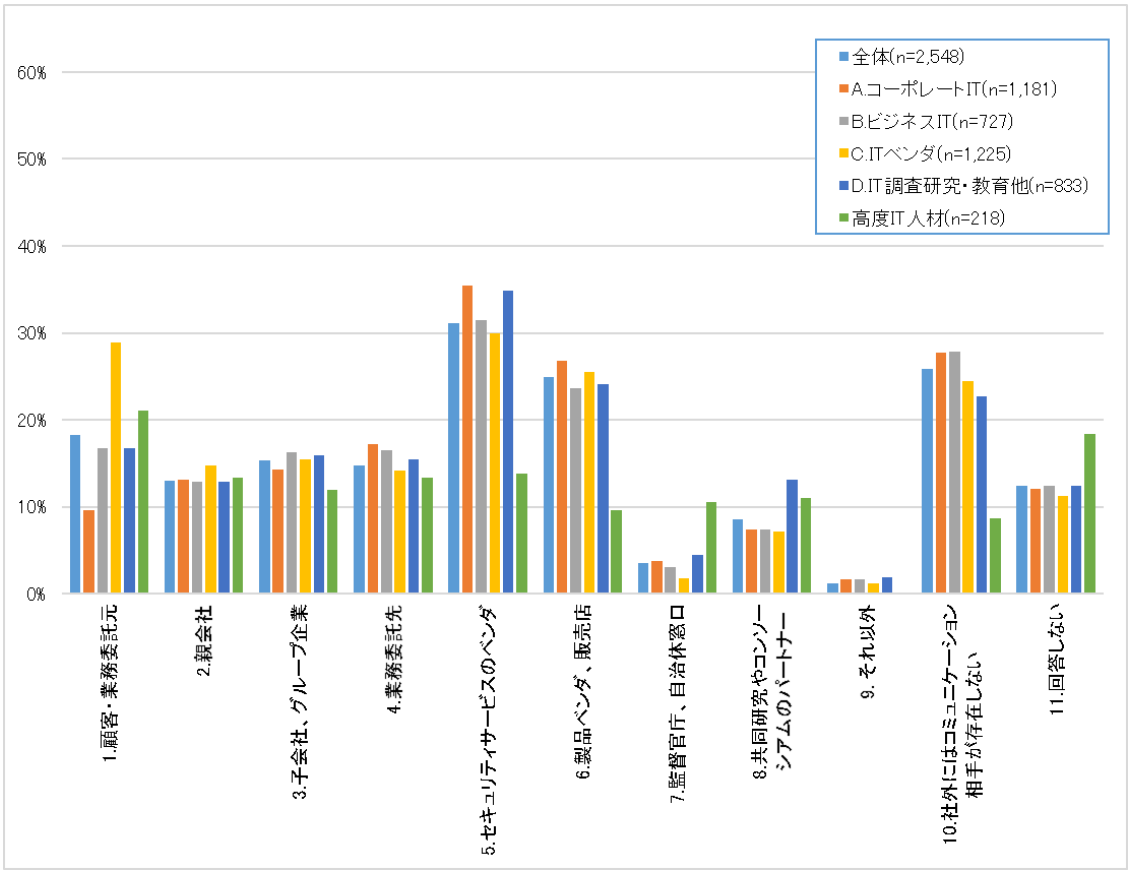


図 2-73 サイバーセキュリティ対策業務遂行上のコミュニケーション相手（自組織外、月 1 回以上）／「調査研究」

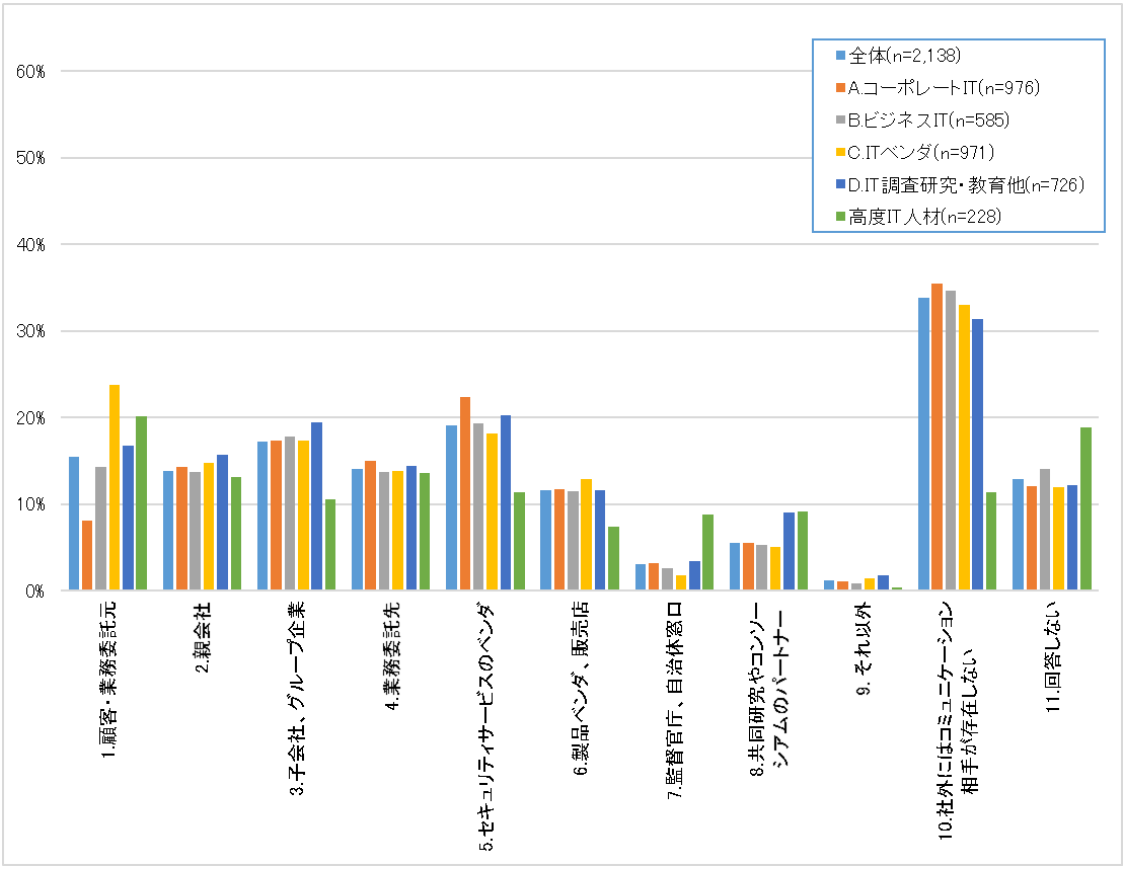


図 2-74 サイバーセキュリティ対策業務遂行上のコミュニケーション相手(自組織外、月 1 回以上)／「教育・人材育成」

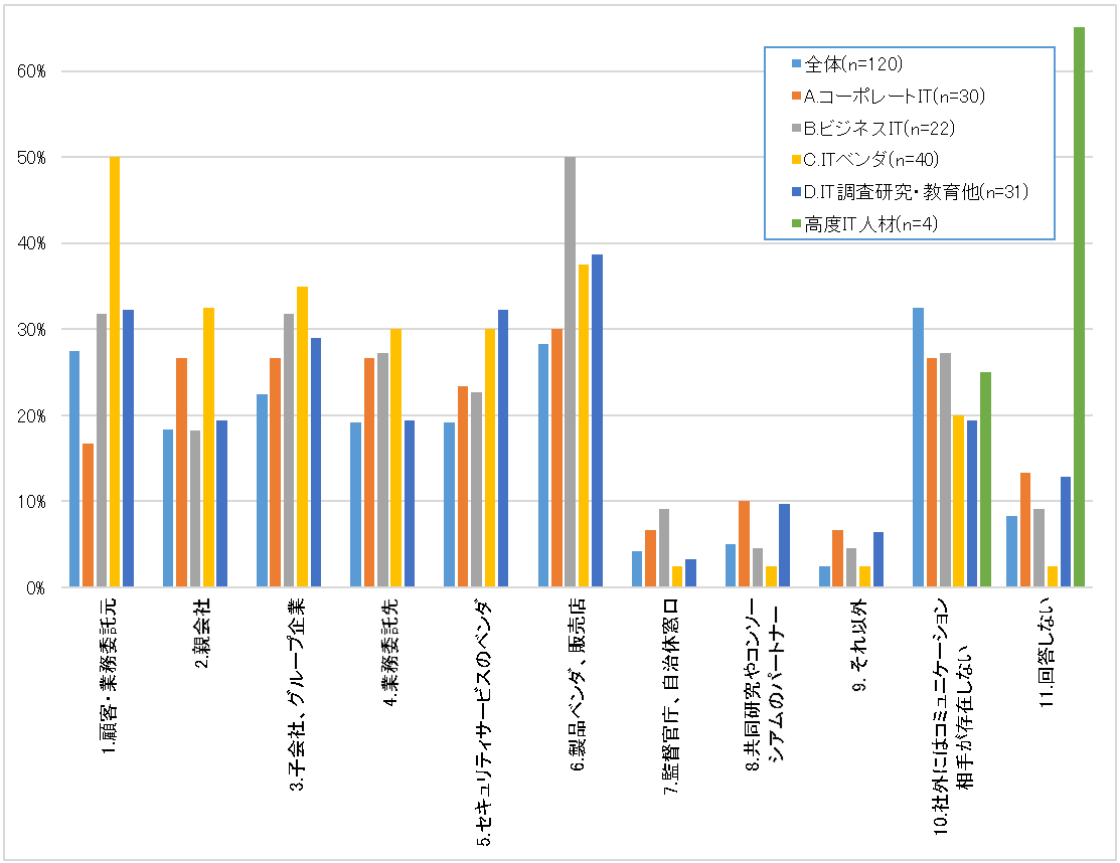


図 2-75 サイバーセキュリティ対策業務遂行上のコミュニケーション相手(自組織外、月 1 回以上)／「その他」

2.5.3. 頻繁にコミュニケーションをとる相手

前述のデータでは、「月 1 回以上」のコミュニケーション相手であったが、加えて、情報セキュリティ対策に関するコミュニケーションを頻繁にとる相手を確認した。

（設問文：回答いただいた業務でコミュニケーションをとる相手のうち、頻繁（概ね 2～3 日に 1 回以上）にコミュニケーションをとる相手をすべて選択してください。（いくつでも））

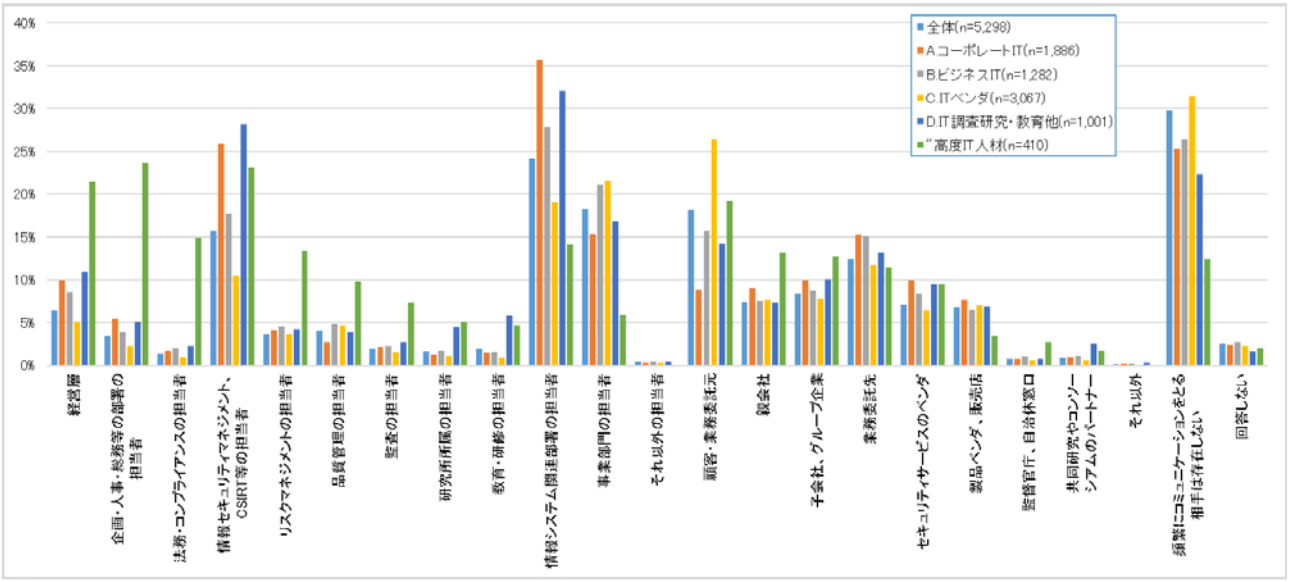


図 2-76 サイバーセキュリティ対策業務遂行上のコミュニケーション相手（自組織内外、2-3 日に 1 回以上）

全般的に、(A)コーポレート IT に関わる人がコミュニケーションをとる相手が多く、特に 3 割前後の人が「情報セキュリティマネジメント、CSIRT などの担当者」、「情報システム関係部署の担当者」と頻繁に情報セキュリティ対策に関するコミュニケーションをとっていることが分かった。「事業部門」とは、(B)ビジネス IT、(C)IT ベンダに関わる人の方がコミュニケーションをとる割合が 2 割程度と高かった。加えて、(C)IT ベンダでは、「顧客・業務委託元」とコミュニケーションをとる割合が高かった（約 25%）。また、高度 IT 人材の回答からは、経営層や企画・人事などの部門担当者とのコミュニケーションが多い。これについては 2.10.2 で述べる。

2.6. 業務遂行上の課題

登録セキスペ及び高度 IT 人材のサイバーセキュリティ対策関連業務担当者、及び登録セキスペ所属組織の組織長に対し、業務の遂行上抱える課題について、いくつかの観点から確認した。

2.6.1. 業務の難易度とその要因

サイバーセキュリティ対策関連業務を担当している人を対象に、その業務の難易度を確認した。

（設問文：あなたは、サイバーセキュリティ対策に関して担当している業務を、どの程度難しいものと考えていますか。Q12 で選択いただいた業務それぞれについて、(1)～(6)のうち、最も近いものを 1 つ選択してください。
選択肢：
(1)つねに難しいと感じる
(2)しばしば難しいと感じる
(3)たまに難しいと感じるときがある
(4)まったく難しさを感じない
(5)なんともいえない
(6)回答しない
）

(1)つねに難しい＝3、(2)しばしば難しい＝2、(3)たまに難しい＝1、(4)まったく難しさを感じない＝0 とし、平均値を算出した。図 2-77 にグラフを示す。

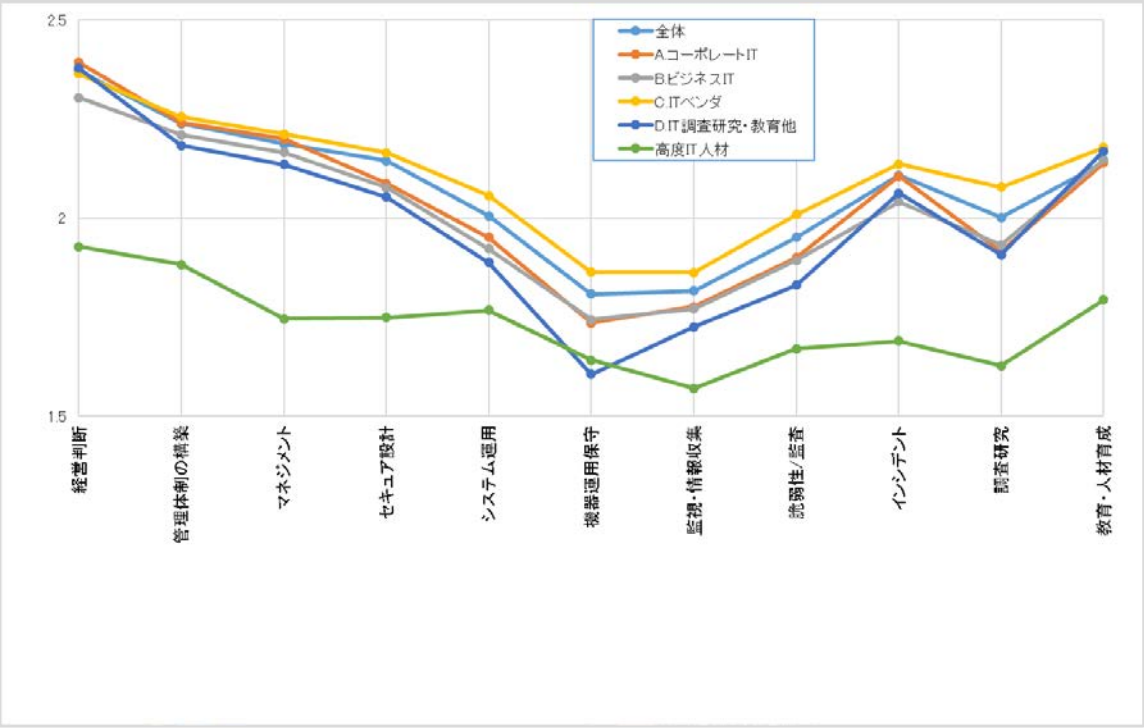


図 2-77 サイバーセキュリティ対策関連業務の難易度（平均値）

業務ごとに難易度の感じ方に差があり、上流業務及びインシデント対応・人材育成などの業務が、難易度が高いと感じられているようである。登録セキスペのグループ(A)～(D)ごとに算出したが、傾向に大きな違いは認められなかった。ただし、高度 IT 人材は全般的に難易度を低く感じている人が多い。

いずれかの業務について「難しい」と回答した人を対象に、難しいと感じる要因を確認した（なお、業務は特定せずに確認している）。

（設問文：最も難易度が高いと感じている業務について、そのように感じる要因として考えられるものをすべて選択してください。）

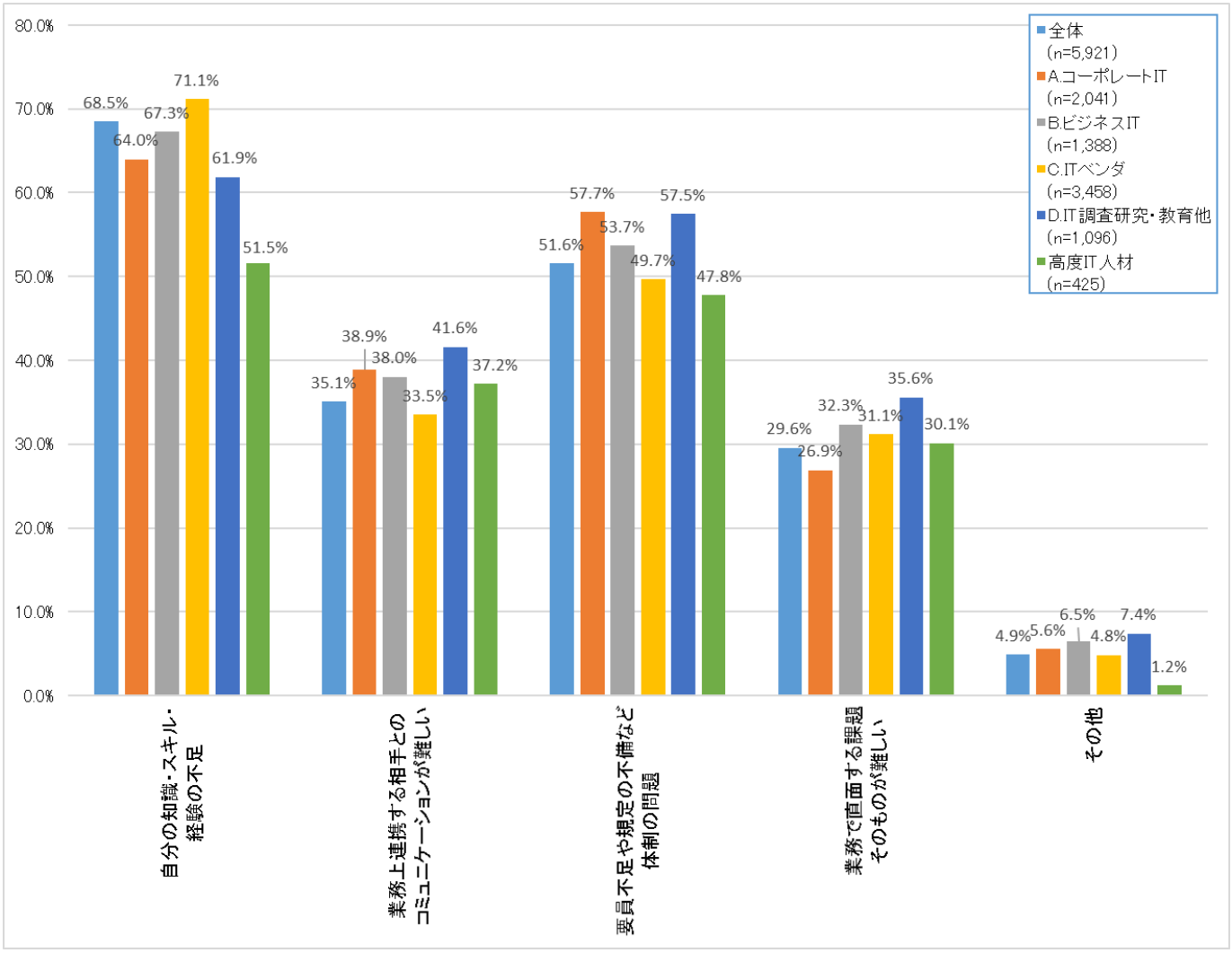


図 2-78 サイバーセキュリティ対策関連業務を難しいと感じる要因（複数回答）

6－7 割程度の登録セキスペが「自分の知識・スキル・経験の不足」が要因であると回答した。グループ（A）～（D）ごとの違いは大幅なものはなかった。高度 IT 人材は「自分の知識・スキル・経験の不足」を挙げる割合が登録セキスペと比較して低かったが、これは平均年齢が高いことなどが影響している可能性がある。

2.6.2. 組織長からみた業務遂行の評価

登録セキスペが所属する組織の組織長に、その組織で遂行されているサイバーセキュリティ対策関連業務の評価を確認した（数が少ないため、グループ分けをせず掲載する）。

（設問文：あなたの部署で遂行されているサイバーセキュリティ対策関連業務は、期待されている成果を上げていますか。選択いただいた業務それぞれについて、最も近いものを 1 つ選択してください。）

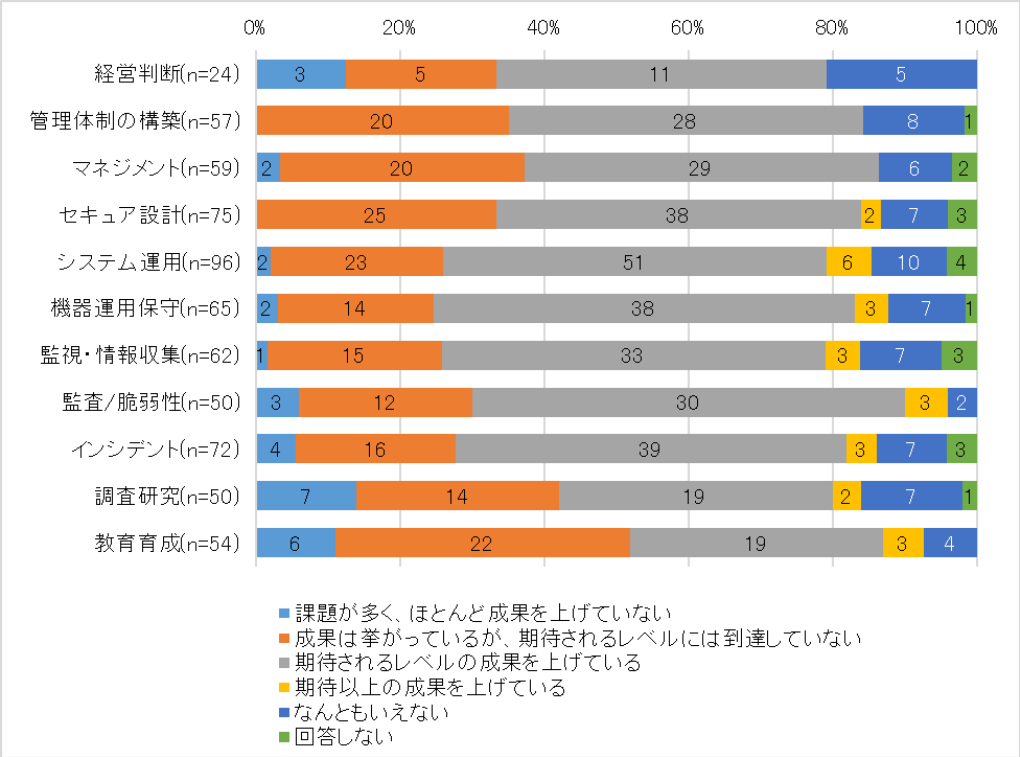


図 2-79 組織長からみた業務遂行の評価

全般的に、「期待されるレベルの成果を上げている」以上の割合が 5 割前後であった。ただし調査研究や教育・人材育成は「ほとんど成果を上げていない」、「期待されるレベルに到達していない」の選択の割合が多く、課題が大きい状態であることが推測される。

2.6.3. コミュニケーション相手に望む知識・スキルレベル

業務でコミュニケーションをとる相手に求めるサイバーセキュリティの知識・スキルレベルを確認した。加えて、現時点での相手の知識・スキルレベルを確認した。

(設問文:業務でコミュニケーションをとる相手に求めるサイバーセキュリティの知識・スキルのレベルとして、理想と考えるものを(1)～(5)から、現状を(6)～(10)から、それぞれ相手毎に 1 つ選択してください。
選択肢:
＜理想と考える相手の知識・スキルの選択肢＞
(1) 情報処理安全確保支援士試験レベル
(2) 情報セキュリティマネジメント試験レベル
(3) IT パスポート試験レベル
(4) サイバーセキュリティの知識・スキルは求めない
(5) わからない、回答しない
＜現状の相手の知識・スキルの選択肢＞
(6) 情報処理安全確保支援士試験レベル
(7) 情報セキュリティマネジメント試験レベル
(8) IT パスポート試験レベル
(9) サイバーセキュリティの知識・スキルを持っていない
(10) わからない、回答しない
)

次に、コミュニケーション相手に求めるサイバーセキュリティの知識・スキルの理想の平均値、現状の平均値、理想と現状のギャップをそれぞれグラフにした(平均値は、レベルを数値に変換し、コミュニケーション相手ごとに算出した。数値は、「情報処理安全確保支援士試験レベル」＝3、「情報セキュリティマネジメント試験レベル」＝2、「IT パスポート試験レベル」＝1、「サイバーセキュリティの知識・スキルは求めない」＝0 とした)。

① コミュニケーション相手に求めるサイバーセキュリティの知識・スキル（理想、平均値）

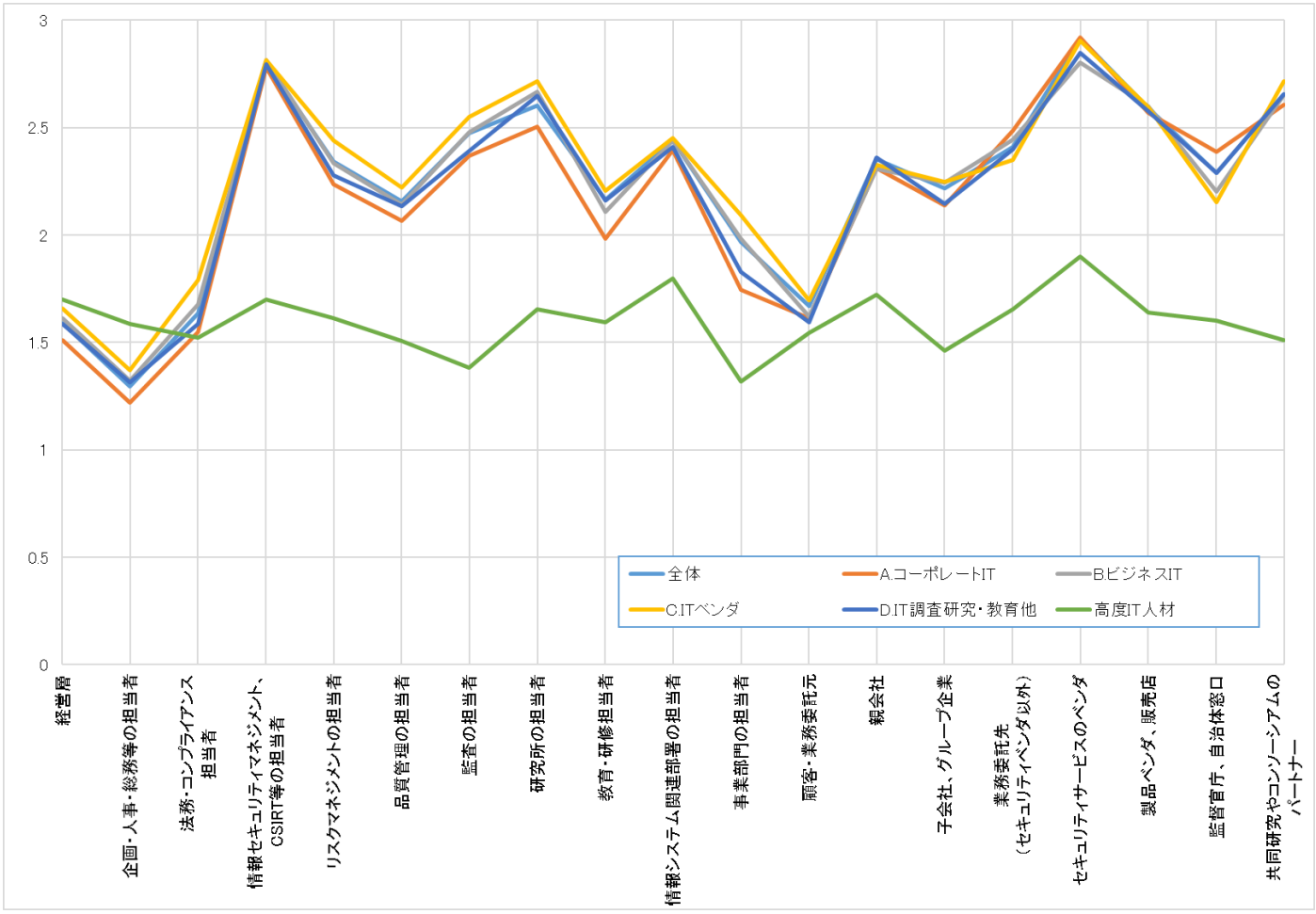


図 2-80 コミュニケーション相手の知識・スキルレベル平均値（理想）

表 2-3 コミュニケーション相手の知識・スキルレベル（理想） 回答数（「わからない・回答しない」と回答した人を除く）

	経営層	企画・人事・総務等の担当者	法務・コンプライアンス担当者	情報セキュリティマネジメント、CSIRT等の担当者	リスクマネジメントの担当者	品質管理の担当者	監査の担当者	研究所の担当者	教育・研修担当者	情報システム関連部署の担当者	事業部門の担当者	顧客・業務委託元	親会社	子会社、グループ企業	業務委託先（セキュリティベンダ以外）	セキュリティサービスのベンダ	製品ベンダ、販売店	監督官庁、自治体窓口	共同研究やコンソーシアムのパートナー
全体	1,153	944	688	2,261	1,017	906	720	318	673	2,784	2,110	2,109	1,065	1,305	1,771	1,908	1,882	295	303
A.コーポレートIT	622	487	346	996	442	280	293	115	275	1,180	723	437	453	514	746	812	778	150	122
B.ビジネスIT	365	263	205	590	323	260	207	90	166	719	567	483	278	339	481	536	482	75	80
C.ITベンダ	493	417	299	1,125	546	599	387	154	324	1,467	1,302	1,700	627	725	958	1,039	1,089	118	126
D.IT調査研究・教育他	367	280	203	553	240	174	176	119	249	609	432	313	206	282	345	465	385	87	136
高度IT人材	202	189	174	190	152	105	113	95	101	138	113	193	158	147	156	141	111	93	98

高度 IT 人材以外では、コミュニケーション相手に求める知識・スキルレベルの傾向はほぼ同じであった。つまり、IT への関わり方による違いはなかった。いわゆるサイバーセキュリティ担当となりやすい部門の所属者にはおおむね情報処理安全確保支援士試験レベルの知識・スキルレベルを求め、それ以外は情報セキュリティマネジメント試験レベルの知識・スキルレベルを求めることが多いようである。また、「経営層」、「企画・人事・総務等の担当者」、「法務・コンプライアンスの担当者」、「顧客・業務委託元」には IT パスポート試験レベルでもよいと考える担当者も多いようである。

② コミュニケーション相手のサイバーセキュリティの知識・スキルレベル（現状、平均値）

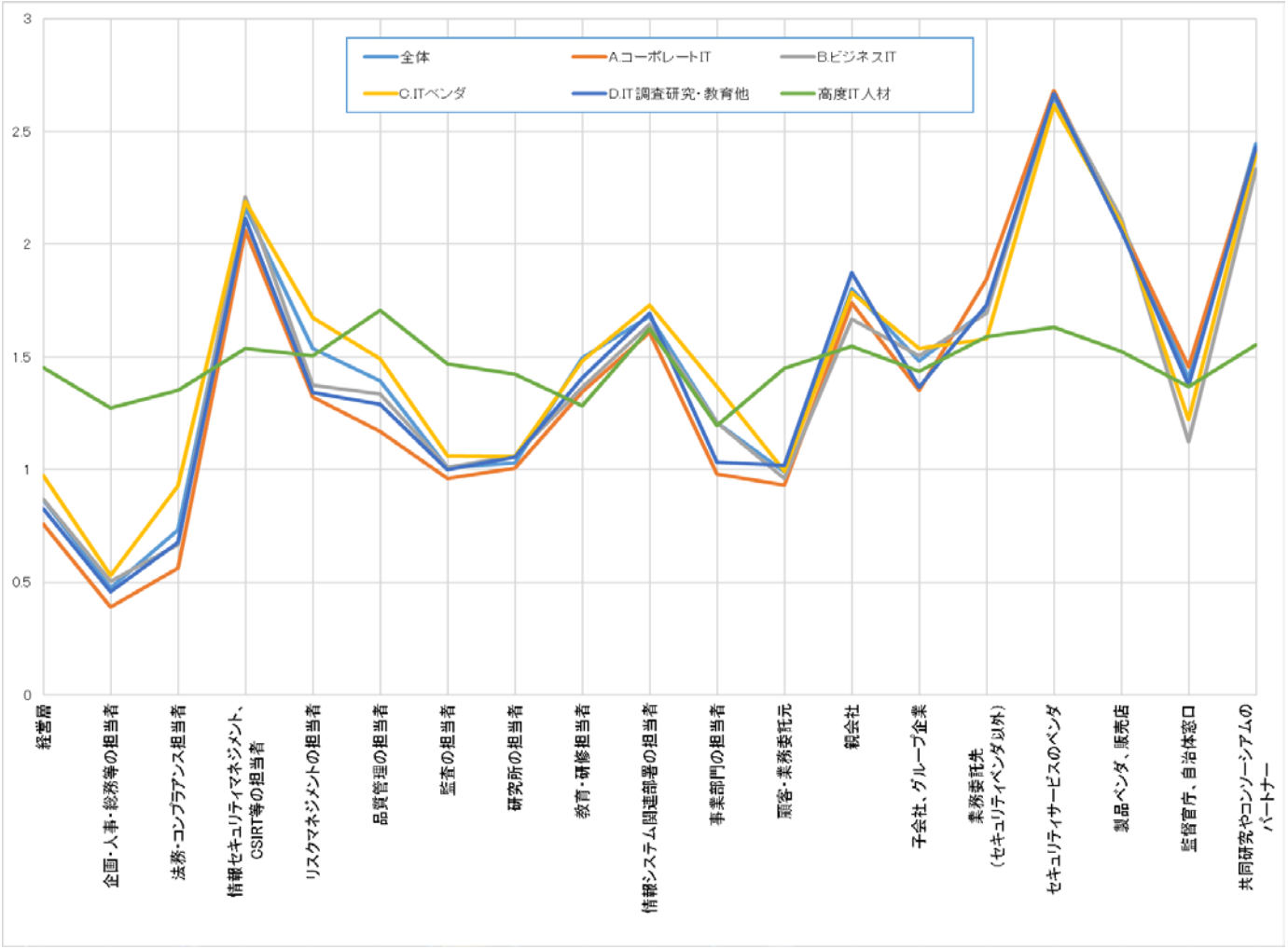


図 2-81 コミュニケーション相手の知識・スキルレベル平均値（現状）

表 2-4 コミュニケーション相手の知識・スキルレベル（現状） 回答数（「わからない・回答しない」と回答した人を除く）

	経営層	企画・人事・総務等の担当者	法務・コンプライアンス担当者	情報セキュリティマネジメント、CSIRT等の担当者	リスクマネジメントの担当者	品質管理の担当者	監査の担当者	研究所の担当者	教育・研修担当者	情報システム関連部署の担当者	事業部門の担当者	顧客・業務委託元	親会社	子会社、グループ企業	業務委託先（セキュリティベンダ以外）	セキュリティサービスのベンダ	製品ベンダ、販売店	監督官庁、自治体窓口	共同研究やコンソーシアムのパートナー
全体	909	725	487	1,760	743	641	526	244	524	2,142	1,628	1,532	779	918	1,187	1,300	1,132	164	206
A.コーポレートIT	494	384	254	800	340	203	220	77	208	953	554	313	328	370	506	548	456	77	80
B.ビジネスIT	298	209	147	459	249	195	159	74	132	571	438	363	208	234	325	365	298	49	54
C.ITベンダ	394	315	196	862	388	416	273	118	252	1,111	1,013	1,252	459	507	644	698	668	72	82
D.IT調査研究・教育他	305	223	167	450	193	138	145	97	204	487	330	228	156	203	234	305	232	48	100
高度IT人材	193	179	165	182	149	102	103	93	99	125	103	189	154	145	146	138	107	87	92

理想と異なり、高度 IT 人材の回答との違いが少なくなっていることが分かる。

③ コミュニケーション相手のサイバーセキュリティの知識・スキルのギャップ

加えて、理想と現状のギャップを算出した（①理想のレベル平均値－②現状のレベル平均値　とした）。

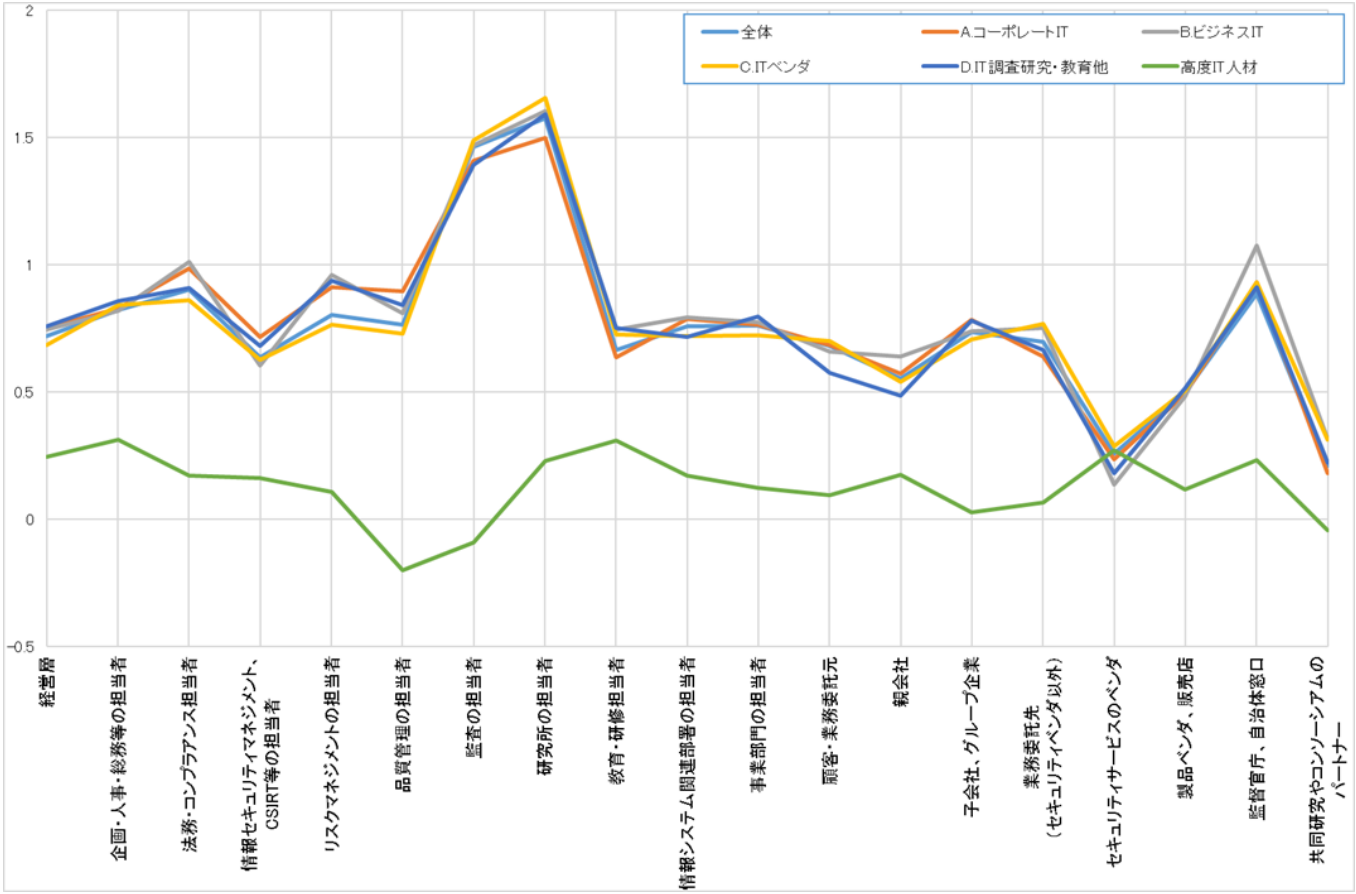


図 2-82 コミュニケーションをとる相手のスキルレベル平均値（理想と現状のギャップ）

監査、研究所など特にギャップの大きい相手もいるが、回答数が少ないため少し極端な値が出ている可能性もある。やり取りの多い部署である「情報セキュリティマネジメント、CSIRT 等」や「情報システム関連」、「業務委託元」、「業務委託先（セキュリティベンダ以外）」などでは、0.5～1 弱のギャップがあり、コミュニケーションの困難さにつながっている可能性がある。高度 IT 人材は理想が高くないことからギャップが小さく、全般的にほぼ 0 に近かった。

2.7. 今後の展望

登録セキスペ及び高度 IT 人材に対し、今後強化したい知識・スキルや今後担当したい業務と立場などについて確認した。

2.7.1. 強化したい知識・スキルや取り組み

今後強化したい知識・スキルを確認した。

（設問文：あなたが今後強化したいと思う必要な知識・スキルをすべて選択してください。
選択肢：
情報セキュリティ分野／(1)最新の脅威に関するもの（脆弱性、マルウェアなどの攻撃手法、攻撃主体　など）
情報セキュリティ分野／(2)情報セキュリティ技術に関するもの（暗号や認証、電子署名、情報理論　など）
情報セキュリティ分野／(3)情報セキュリティ対策の運用に関するもの（対策のオペレーション、監視、インシデントレスポンス　など）
情報セキュリティ分野／(4)情報セキュリティマネジメントに関するもの（情報セキュリティポリシー、情報セキュリティガバナンス、情報セキュリティ監査など）
情報セキュリティ分野／(5)情報セキュリティ機能の設計・実装に関するもの（セキュリティ要件定義、設計、実装、テスト、評価　など）
IT関連ほか全般／(6)アプリケーション／サービスに関するもの（業種、ウェブ、グループウェア、オフィスアプリ、会計アプリ、SaaS、開発技術　など）
IT関連ほか全般／(7)システム基盤／ハードウェアに関するもの（システムのアーキテクチャ、OS、仮想環境、IaaS・PaaS 等のクラウドサービス、IoT　など）
IT関連ほか全般／(8)先端技術に関するもの（AI、データサイエンス、ブロックチェーン　など）
IT関連ほか全般／(9)開発や運用の管理に関するもの（プロジェクトマネジメント、サービスマネジメント、アジャイル手法　など）
IT関連ほか全般／(10)事業戦略に関するもの（経営、リスクマネジメント、財務、設備投資、設備管理、人材戦略など）
IT関連ほか全般／(11)倫理、コンプライアンス、法律やガイドライン、標準、規格等に関するもの
IT関連ほか全般／(12)人間力に関するもの（コミュニケーション、意識共有、人を動かす行動力　など）
その他／(13)その他
その他／(14)強化したいと思う知識・スキルはない
その他／(15)回答しない
）

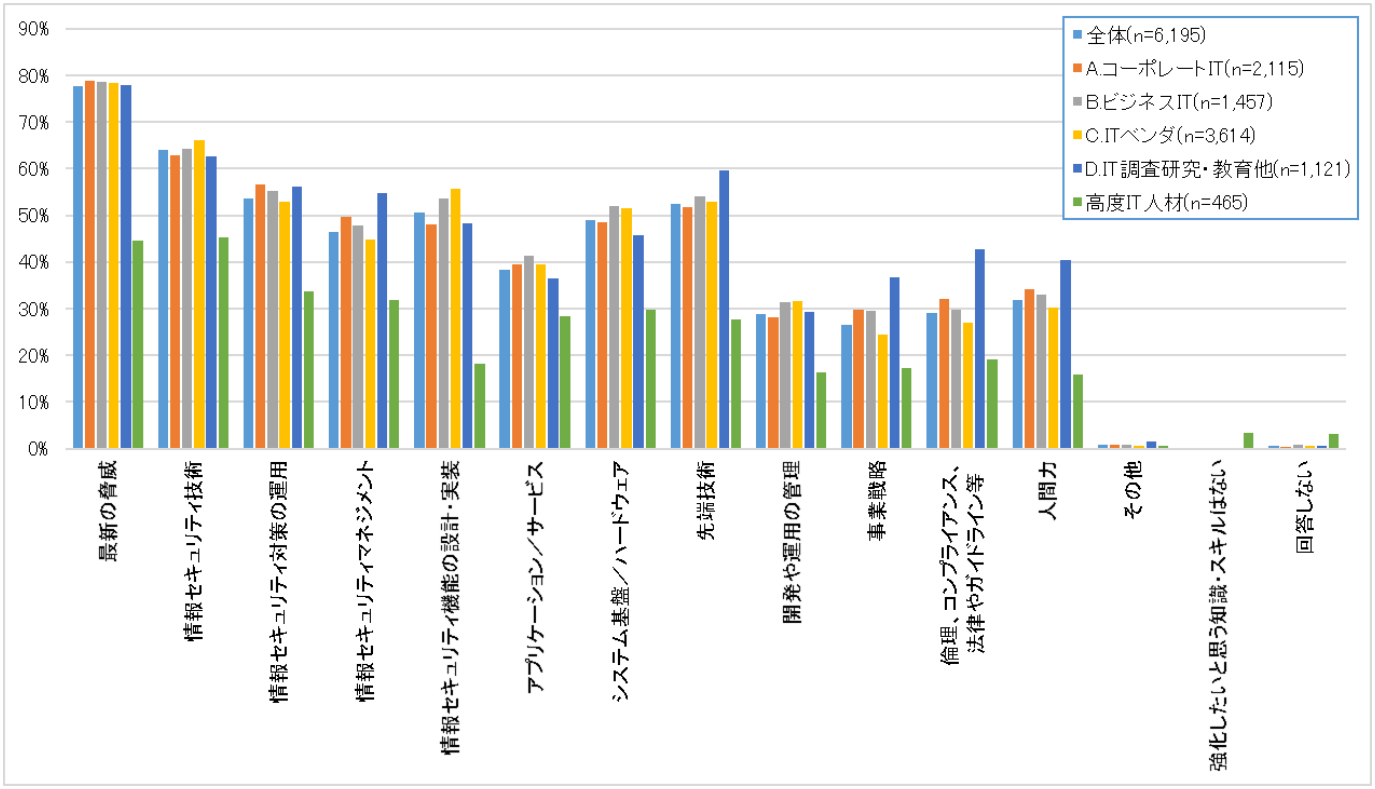


図 2-83 今後強化したい知識・スキル（複数選択）

IT との関わりによる違いは少なく、情報セキュリティ関連の知識・スキルを強化したいと考えている登録セキスペが多かった。加えて IT 関連の基盤や先端知識・スキルも強化の意向が強い。それに比べて、IT の開発や運用管理、事業戦略、人間力などは知識・スキルの強化を考える人が少なかった。

「今後強化したい知識・スキル」を 1 つ以上回答した人を対象に、知識・スキル向上のために現在行っている取組を確認した。

（設問文：あなたが現在実施している、知識・スキル向上のための取組をすべて選択してください。
選択肢：
実践を通じた OJT（On the Job Training）
社外の有償のセミナー、講座（e ラーニングを含む）、大学・大学院等の受講
社外の無償のセミナー、講座等（MOOC*を含む）の受講 ＊MOOC：無償で受講できるオープンな講座（Massive Open Online Courses）のこと
社内セミナー、社内向け e ラーニング等の受講
社外の勉強会（コミュニティ活動を含む）の開催、参加
書籍、雑誌、公開のウェブサイト等を用いた独学
その他
回答しない
）

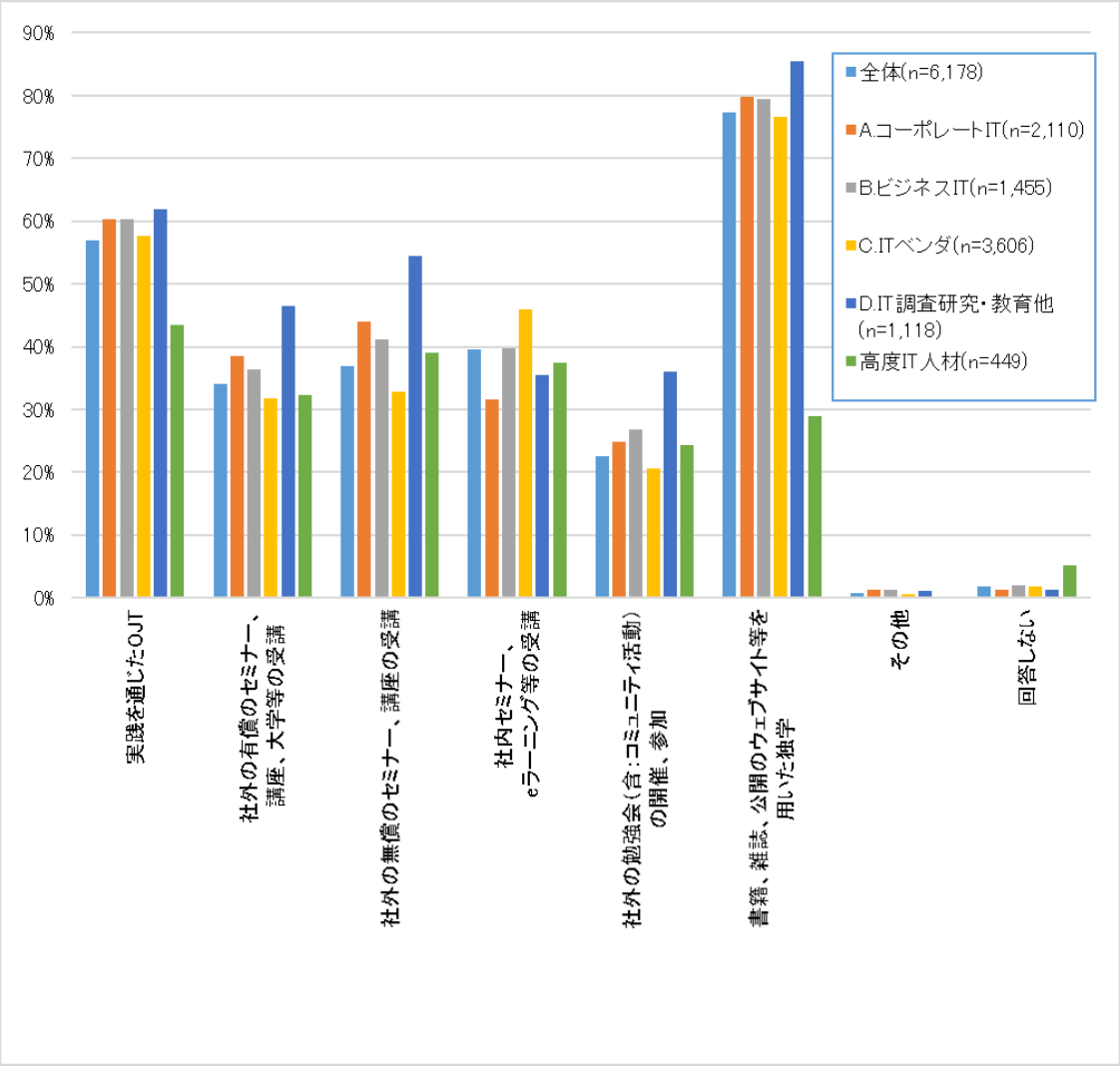


図 2-84 知識・スキル向上のための取り組み

登録セキスペは、高度 IT 人材と比較すると、知識・スキル向上に取り組む割合が高いと言える。特に、8 割程度が独学で知識・スキル向上を行っており、それに加えて有償無償の社外セミナーやコミュニティ活動などでスキル向上を図っている人が多いことが分かる。特に（D）IT 調査研究・教育他の人は取り組んでいる割合が高い。

2.7.2. 今後担当したい業務と立場

登録セキスペに対し、今後サイバーセキュリティの知識・スキルでどのように活躍していきたいかを確認した。

（設問文：あなたは今後、サイバーセキュリティの知識・スキルを活かして、どのように活躍していきたいですか。差し支えない範囲で結構ですので、担当したいサイバーセキュリティ業務について、あてはまるものをすべて選択ください。）

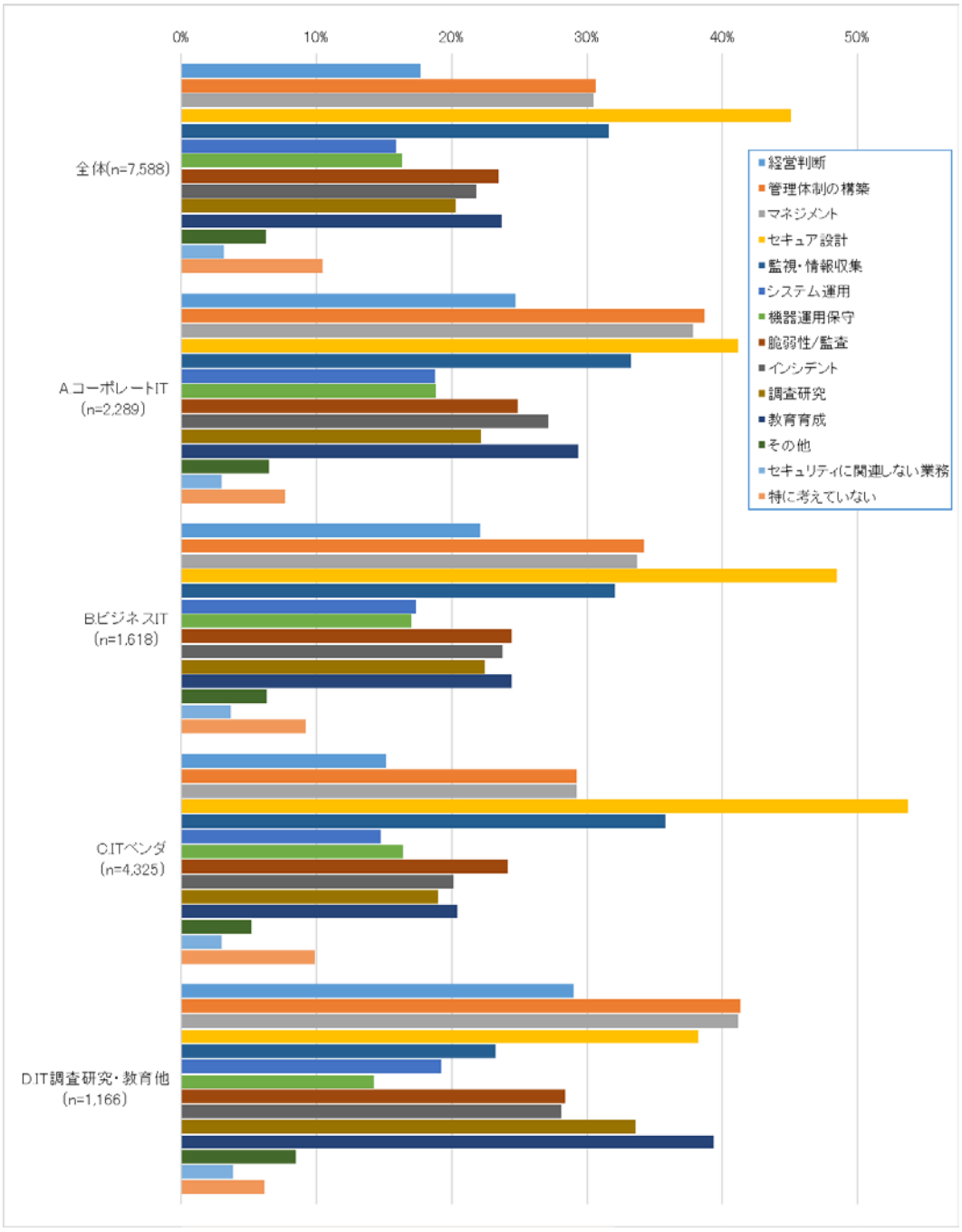


図 2-85 今後担当したい業務

図 2-85 は、現状その業務を担当していて「そのまま継続して担当したい」と選択している人数も含まれている。

そこで、現状は担当していないが、今後担当したいと考えている人数を算出するため、現状担当している人をカウントせずに集計した結果を図 2-86 に示す。これを見ると、「管理体制の構築」、「マネジメント」、「セキュア設計」などが人気であることが分かる。

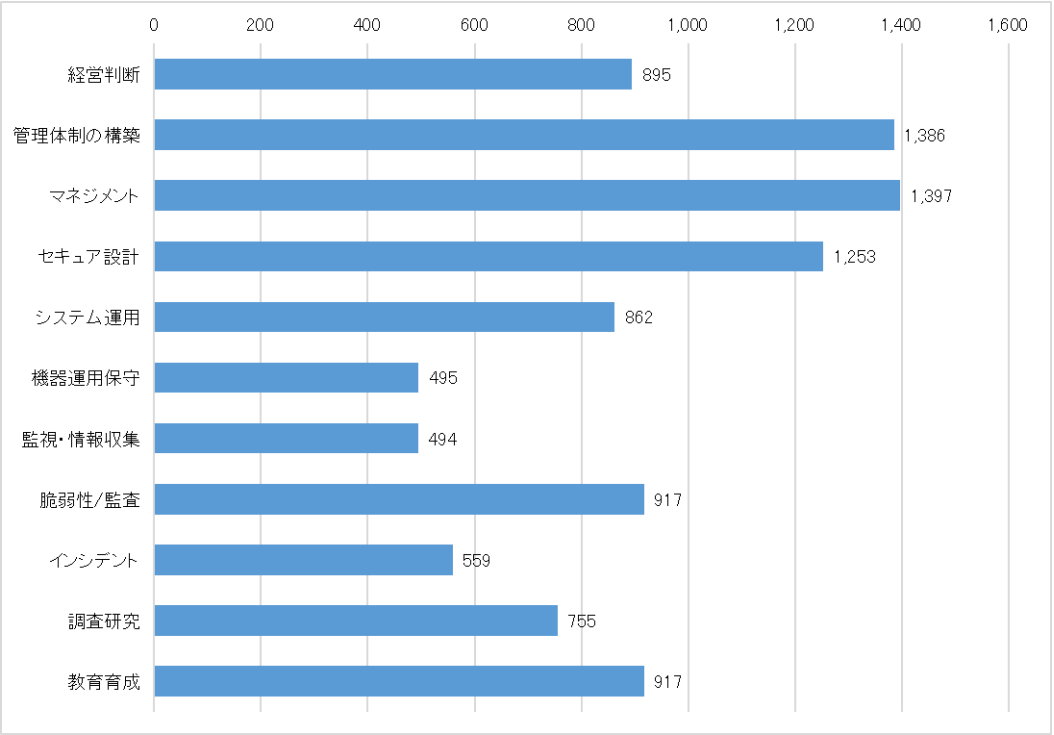


図 2-86 今後担当したい業務 選択人数(現状担当している人を除く) (n=7,588)

また、担当したい業務をどのような立場で行いたいかを確認した。

(設問文:あなたは今後、サイバーセキュリティの知識・スキルを活かして、どのように活躍していきたいですか。差し支えない範囲で結構ですので、担当したいサイバーセキュリティ業務とお立場のそれぞれについて、あてはまるものをすべて選択ください。)

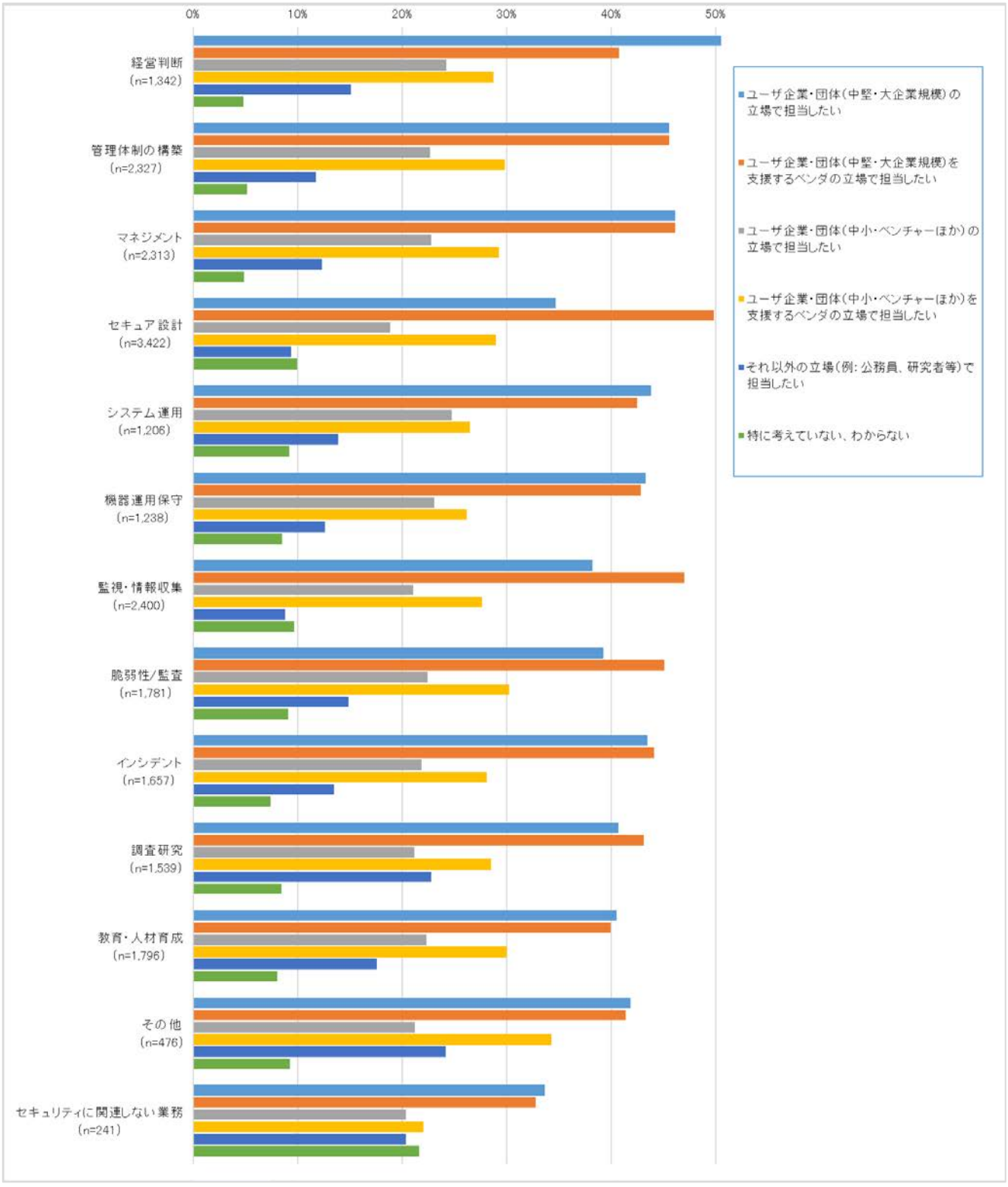


図 2-87 今後行いたい立場(担当したい業務ごと)

2.8. 登録セキスペ制度の活用

登録セキスペ及びその所属組織の組織長に対し、登録セキスペ制度の活用状況やメリットについて確認した。

2.8.1. 登録のきっかけ

情報処理安全確保支援士として登録をした理由は、図 2-88 のとおりであった。

（設問文:あなたが情報処理安全確保支援士として登録した理由として、次の中から最も近いものを 1 つ選択してください。）

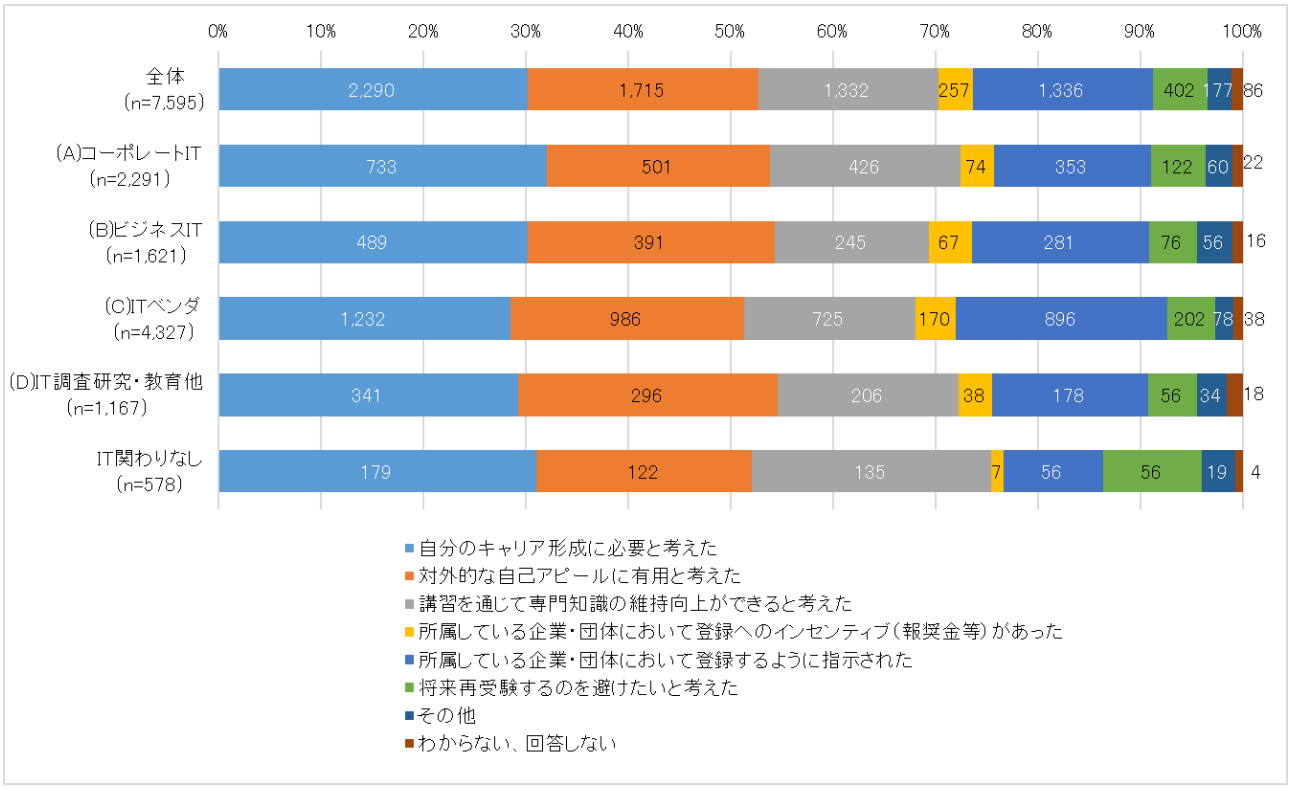


図 2-88 情報処理安全確保支援士への登録のきっかけ

キャリア形成のため、自己アピールのため、講習による専門知識の維持向上のため、という自身の目的によって登録した人がいずれのグループでも 7 割程度を占めており、所属組織の指示による登録の割合は 2 割前後であった。

役職別に集計した結果は、図 2-89 のとおりであった。

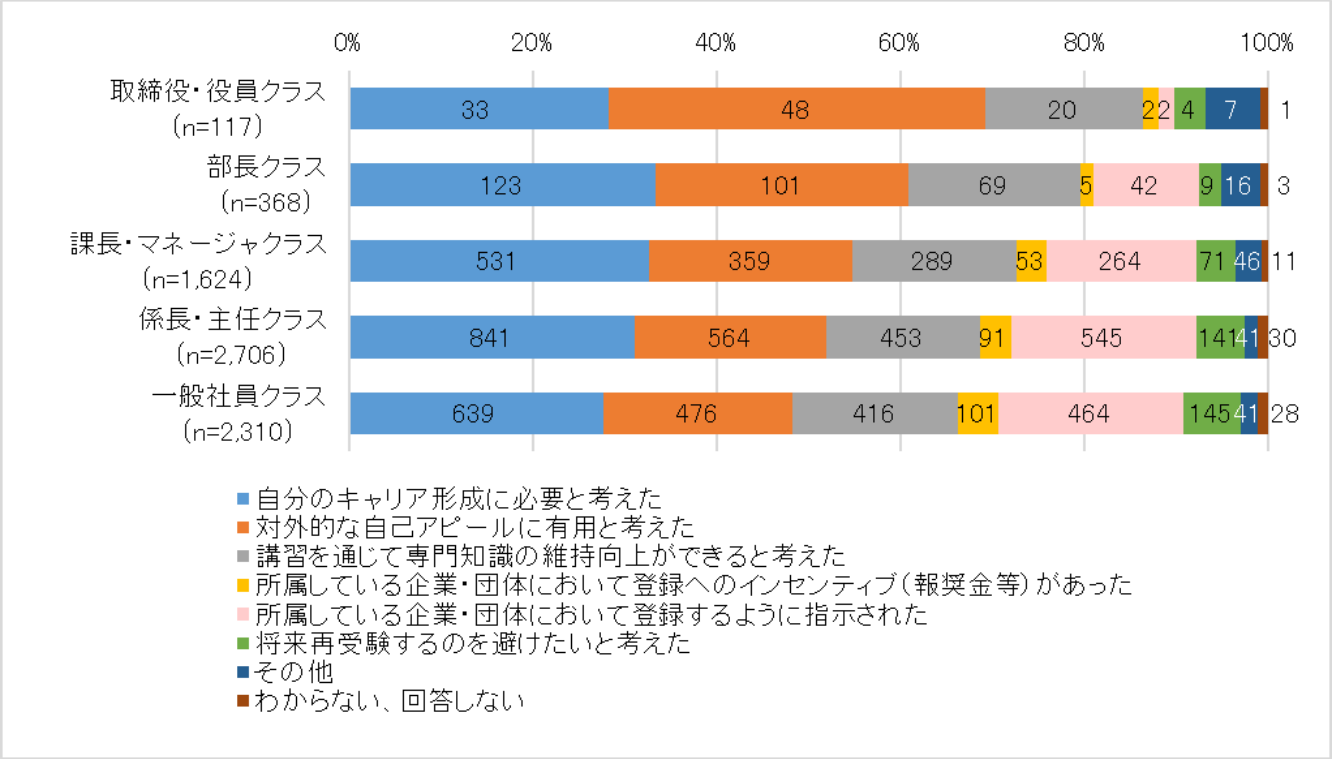


図 2-89 情報処理安全確保支援士への登録のきっかけ(役職別)

役職が高い人ほど「対外的な自己アピール」のために活用されている割合が高かった。

2.8.2. 登録・講習費用の負担者

登録セキスペの登録や講習受講にかかる費用負担について確認した。

（設問文：登録やこれまで受講した講習の費用を誰が負担していますか？次の中から最も近いものを 1 つ選択してください。
※以前所属していた企業・団体が負担した場合も、「所属している企業・団体」とみなしてご回答ください。
※まだ講習を受講しておらず、誰が負担するか不明の場合は推定で回答していただいて結構です。）

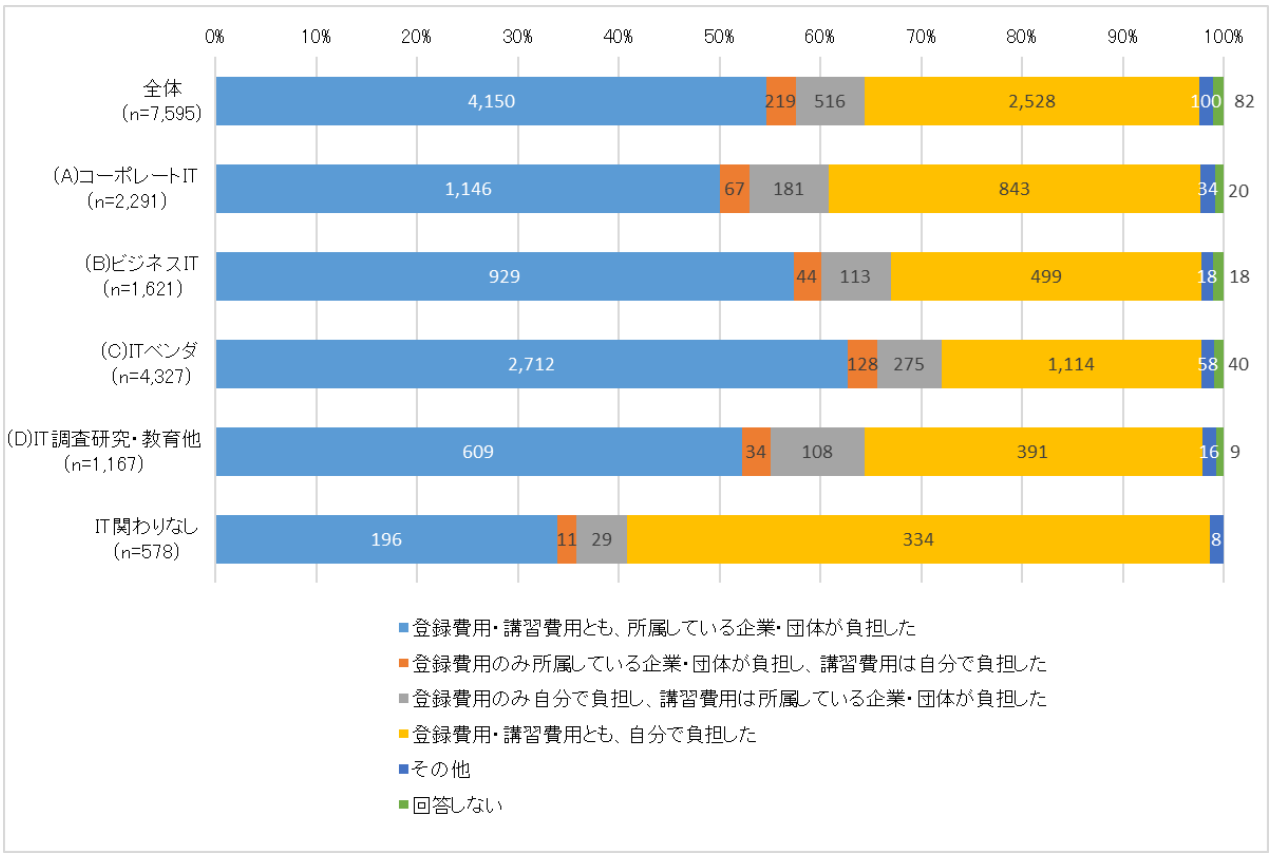


図 2-90 登録や講習受講にかかる費用負担

全体的には、5 割以上の登録セキスペにおいて、所属組織が登録・維持費用の全部又は一部を負担していることが分かった。ただし、IT への関わり方によって傾向が異なり、(A)コーポレート IT や(D)IT 調査研究・教育他に関わる部門に所属する登録セキスペは自己負担の比率が比較的高かった。また、IT に関わりのない部門に所属している登録セキスペは自己負担比率が 6 割近かった。これは、キャリアチェンジや異動などのために資格を取った方々が多いと推測できる。

2.8.3. 登録セキスペ制度のメリット

メリットとなること

登録セキスペと高度 IT 人材の両方に対し、情報処理安全確保支援士制度への登録によって得られるメリットは何かを確認した(今後実施される可能性のある施策も含めている)。

(設問文:情報処理安全確保支援士への登録によって得られることのうち、あなたにとってメリットとなることをすべて選択してください。なお、選択肢には現在実施されていないが、今後情報処理安全確保支援士を対象に実施される可能性のある施策を含めて挙げています。)

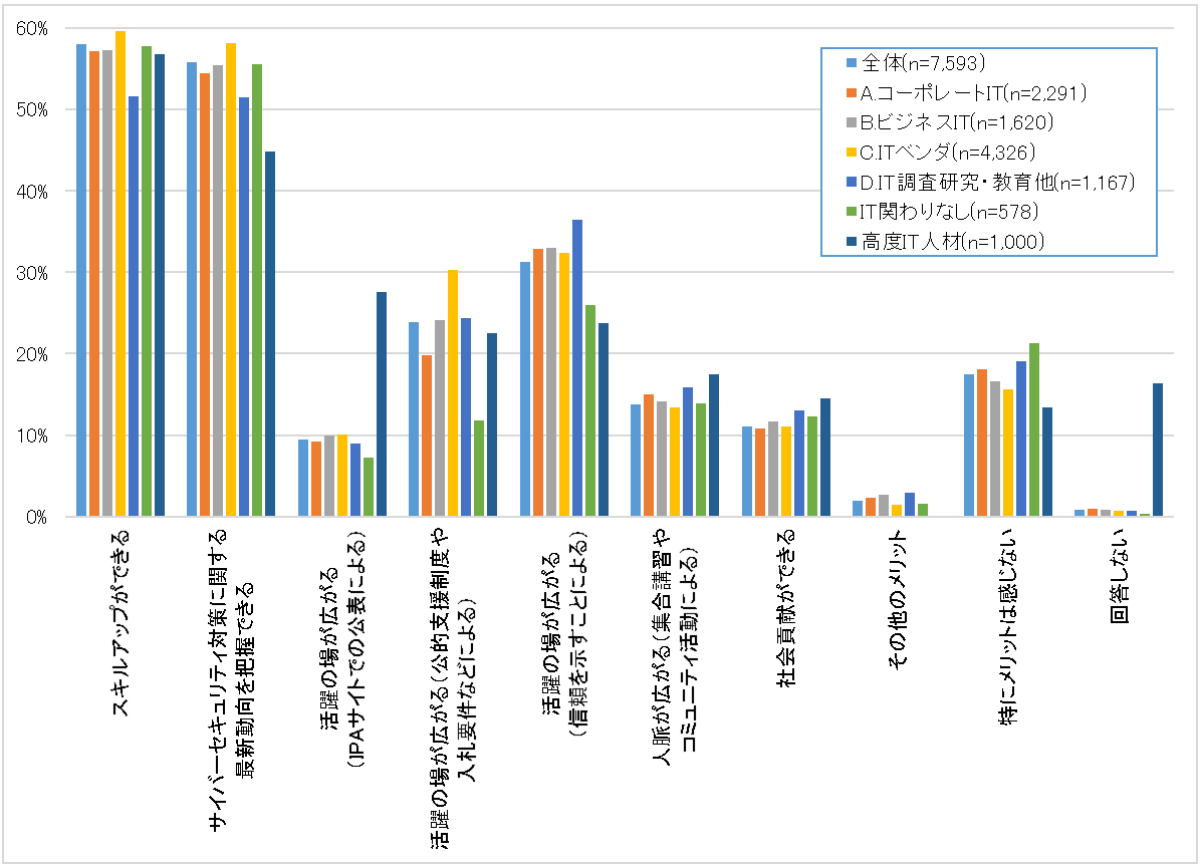


図 2-91 メリットとなること(登録セキスペ、高度 IT 人材)

すでに登録している人は、スキルアップや情報収集を最も大きなメリットと考えていることが分かった。また活躍の場が広がる、つまり仕事が得られることにメリットを感じている人はおおむね 3 割弱で、特に信頼を示すことによる活躍の場の広がりを重視していることが分かった。IPA サイトでの公表による活躍の場の広がりがメリットと考える割合が高度 IT 人材において高く登録セキスペにおいて低い点は、現時点での公表の仕方に課題があることを示していると考えられ、今後の改善が必要な点と考える。その他、人脈の広がりや社会貢献をメリットと考える人は 1 割程度であった。

組織における登録セキスペの活用のメリット

組織における登録セキスペの活用がメリットとなるかどうかを、組織長に対して確認した。

(設問文:情報処理安全確保支援士への登録によって得られるメリットは、以下のようなものが想定されています。これらの中であなたの部署にとってメリットとなるものをすべて選択してください。※なお、選択肢には現在実施されていないが、今後情報処理安全確保支援士を対象に実施される可能性のある施策を含めて挙げています。)

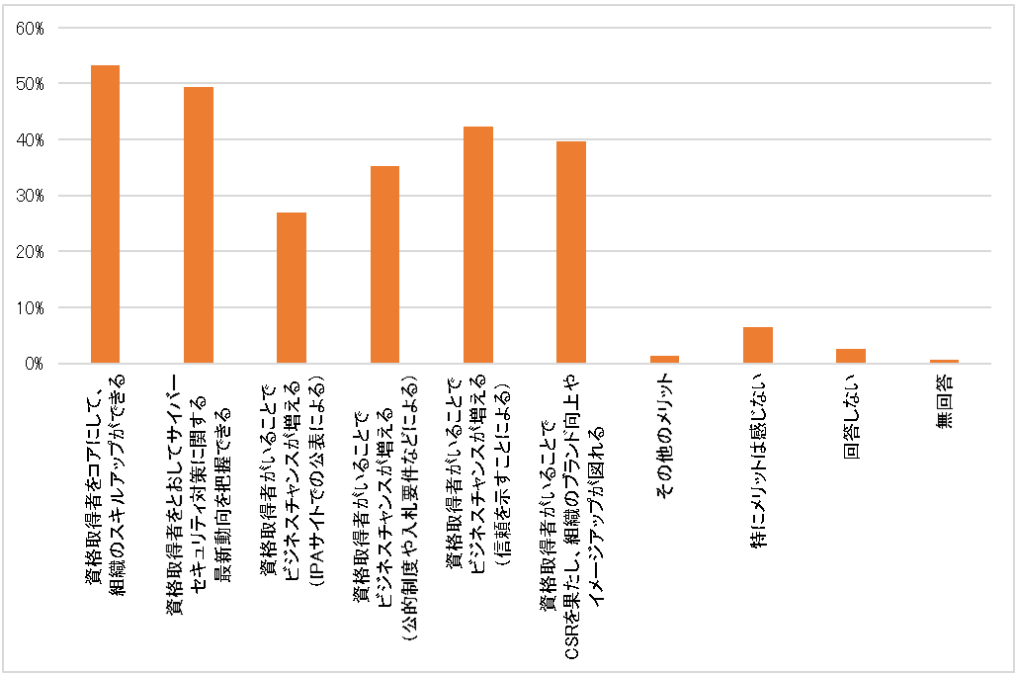


図 2-92 メリットとなること（組織長：n=156）

登録セキスペや高度 IT 人材と比較すると、「ビジネスチャンスが増える」ことがメリットと回答する割合が約 3.5 割と高い。また、組織のブランド向上やイメージアップをメリットと回答する割合も 4 割と高かった。

実際に得られたメリット

次に、登録したことで実際に得られたメリットを確認した。

（設問文：情報処理安全確保支援士に登録したことで得られた具体的なメリットがこれまでにあれば、あてはまるものをすべて選択してください。）

図 2-93 に、実際に得られたメリットがあったと答えた方と、ないと答えた方の割合を示す。全体的に 6 割弱の方が「実際に得られたメリットはない」と答えた。登録セキスペの活躍の場を増やすなど、メリットを増やす活動が今後必要であることが分かる。

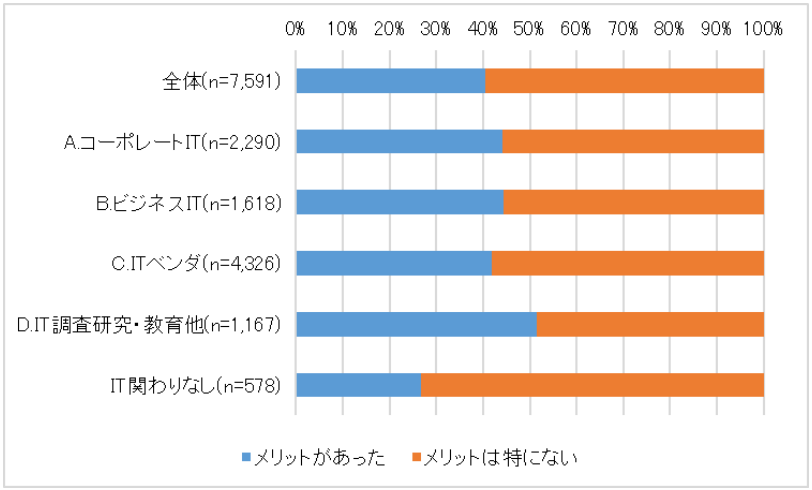


図 2-93 実際に得られたメリットの有無

具体的に得られたメリットとしては、「情報セキュリティ対応力をアピールできた」や「講習で得た知識が業務に活かせた」などの回答が多かった。

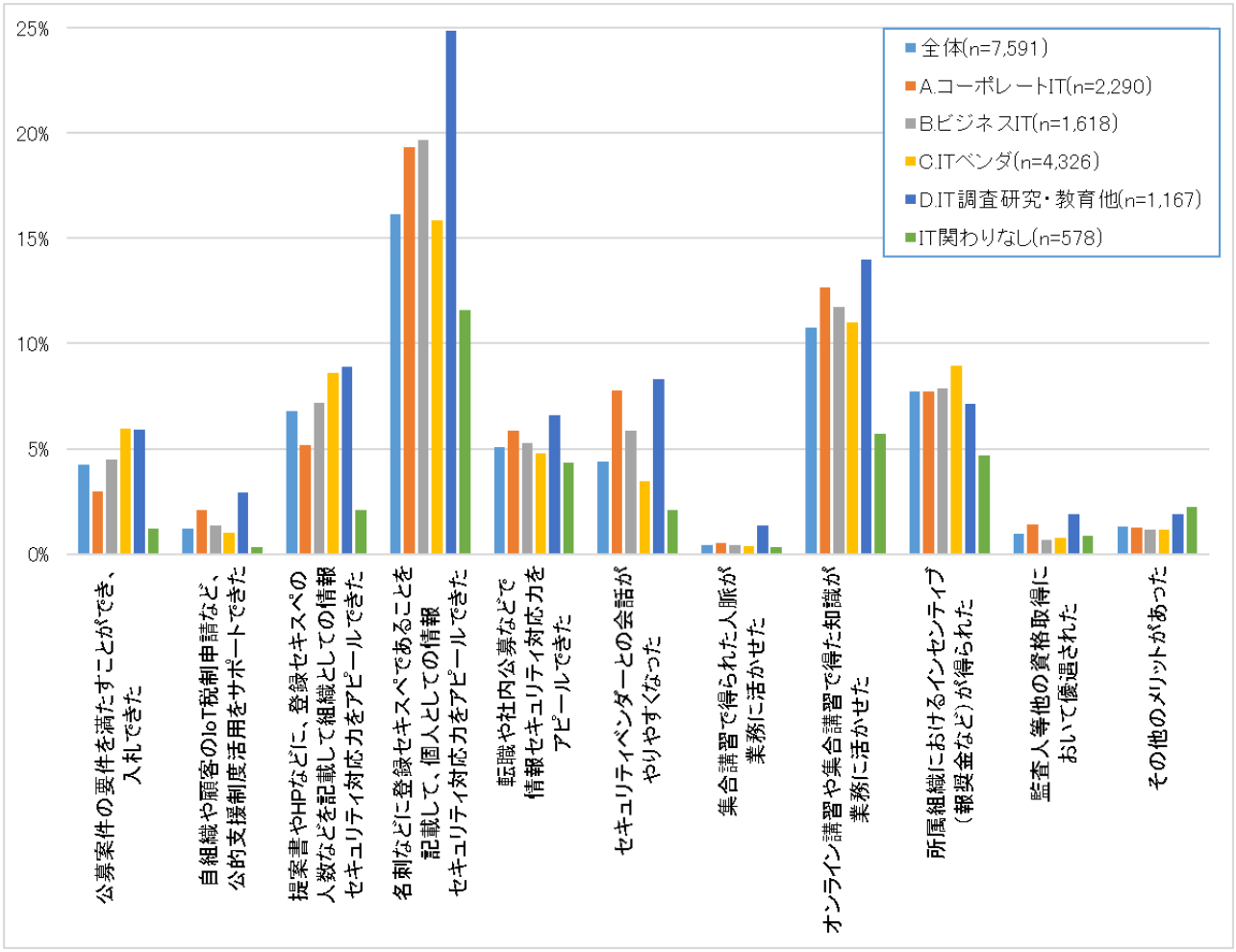


図 2-94 実際に得られたメリット（回答者の割合）

2.9. 登録セキスペ制度の認知度、必要性

高度 IT 人材及び登録セキスペ所属組織の組織長を対象に、登録セキスペ制度の認知度や必要性を確認した。

2.9.1. 高度 IT 人材における登録セキスペ制度の認知度、必要性

高度 IT 人材は、IT 関連業務に就いている若しくは過去就いていた人である。その方々の中で、登録セキスペ制度を正しく理解していた人は 2 割弱であった。

（設問文:あなたは、情報処理安全確保支援士制度を知っていましたか。最も近いものを 1 つ選択してください。）

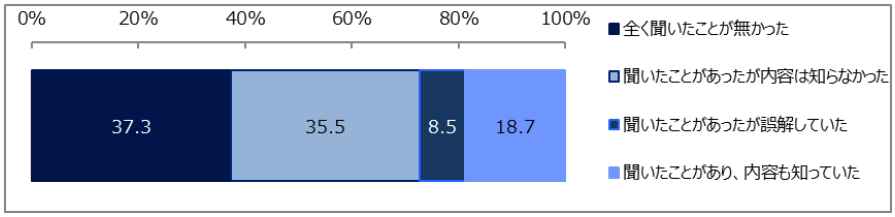


図 2-95 登録セキスペ制度の認知度（高度 IT 人材:n=1,000）

併せて、登録セキスペが所属組織に必要かどうかを確認すると、6 割が必要と回答した。

（設問文:情報処理安全確保支援士は、情報セキュリティに関する高度な知識・スキルを国が保証する資格です。あなたの所属されている部署に、情報処理安全確保支援士は必要と思われますか。最も近いものを 1 つ選択してください。）

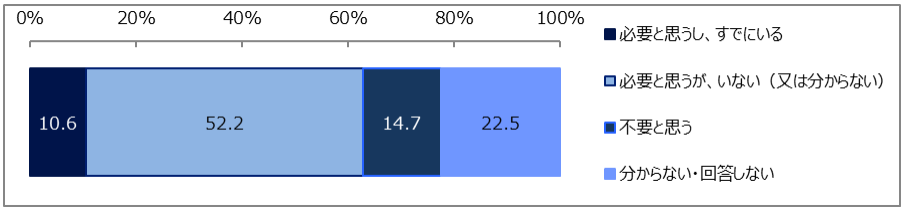


図 2-96 登録セキスペの必要性（高度 IT 人材:n=1,000）

必要であるが知らなかった、という人が一定数いることが推測され、制度活用に向けては認知度向上が必要であることが分かる。

2.9.2. 組織長における登録セキスペ制度の認知度、必要性

同様の確認を組織長に対しても行った。

（設問文:あなたは、情報処理安全確保支援士制度を知っていましたか？ 次の中から最も近いものを 1 つ選択してください。）

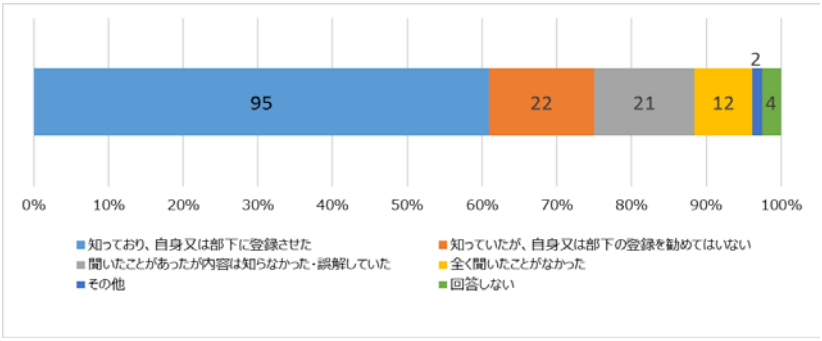


図 2-97 登録セキスペ制度の認知度（組織長、n=156）

（設問文：情報処理安全確保支援士は、情報セキュリティに関する高度な知識・スキルを国が保証する資格です。あなたの部署の役割において、情報処理安全確保支援士は必要と思われますか？ 次の中から最も近いものを 1 つ選択してください。）

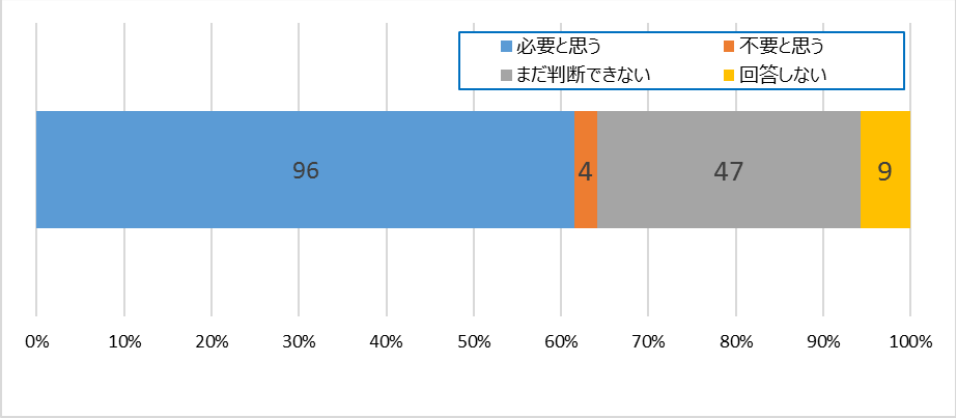


図 2-98 登録セキスペの必要性（組織長、n=156）

回答者は、自分の組織に登録セキスペがいる人なので、認知度は高かったが、「知らなかった」と答えた人も一部おり、自主的に登録している登録セキスペの所属組織の組織長であると推測する。必要性については「まだ判断できない」と答えた人が 3 割おり、判断に必要な情報を届ける活動が必要であることが分かる。

併せて、「情報処理安全確保支援士が必要」と答えた組織長には「どのように確保するのか」も確認したところ、「自部署の担当者の育成」が圧倒的に多かった。

（設問文：人材をどのように確保することが予想されますか？ あてはまるものをすべて選択してください。）

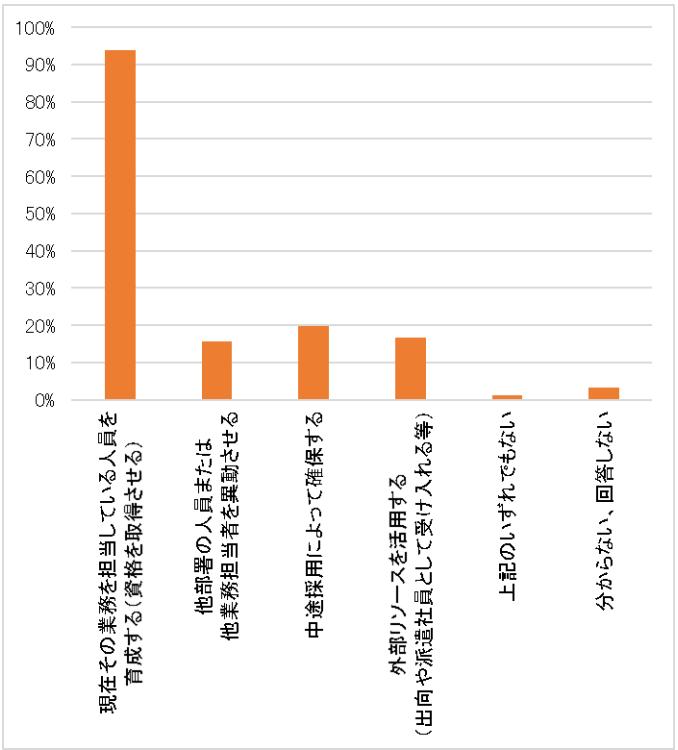


図 2-99 登録セキスペの確保方法（n=96）

2.10. その他の集計・分析

その他、実施した集計・分析内容を掲載する。

2.10.1. 所属部署の情報機器の活用状況やセキュリティ対策の管理状況について

多くの登録セキスペが、所属部署において情報技術やそれを用いた機器を活用して業務を行っている。

（設問文:あなたが所属している部署の行っている事業における情報技術やそれを用いた機器の状況として、最も近いものを1つ選択してください。）

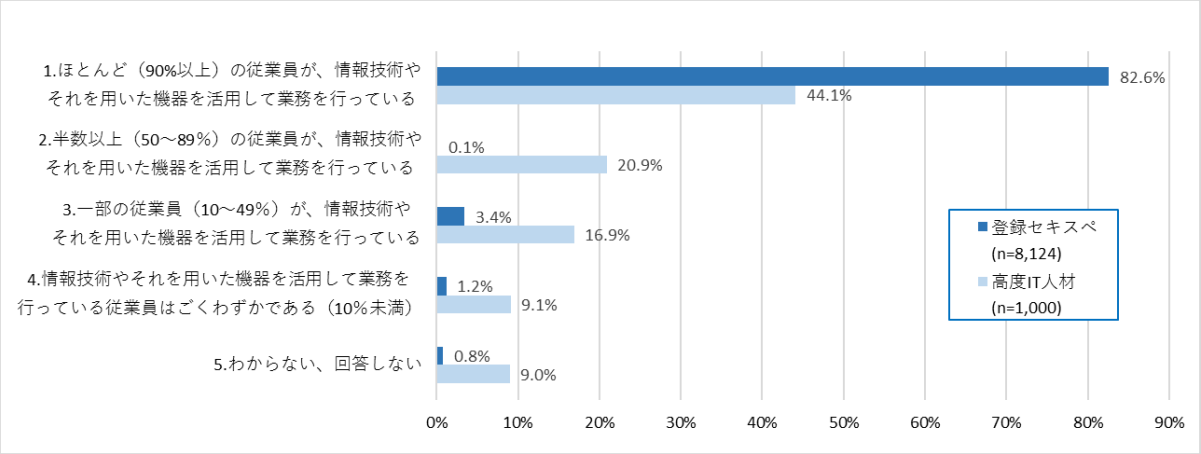


図 2-100 所属部署の行っている事業における情報技術やそれを用いた機器の状況（n=8,124）

また、所属部署における情報機器やそのセキュリティ対策の管理状況について、高度 IT 人材は適切な対策や改善が実施されている割合が 5 割程度なのに対し、登録セキスペは 7 割を超えている。

（設問文:あなたが所属している部署の行っている事業における情報機器やそのセキュリティ対策の管理状況として、最も近いものを1つ選択してください。）

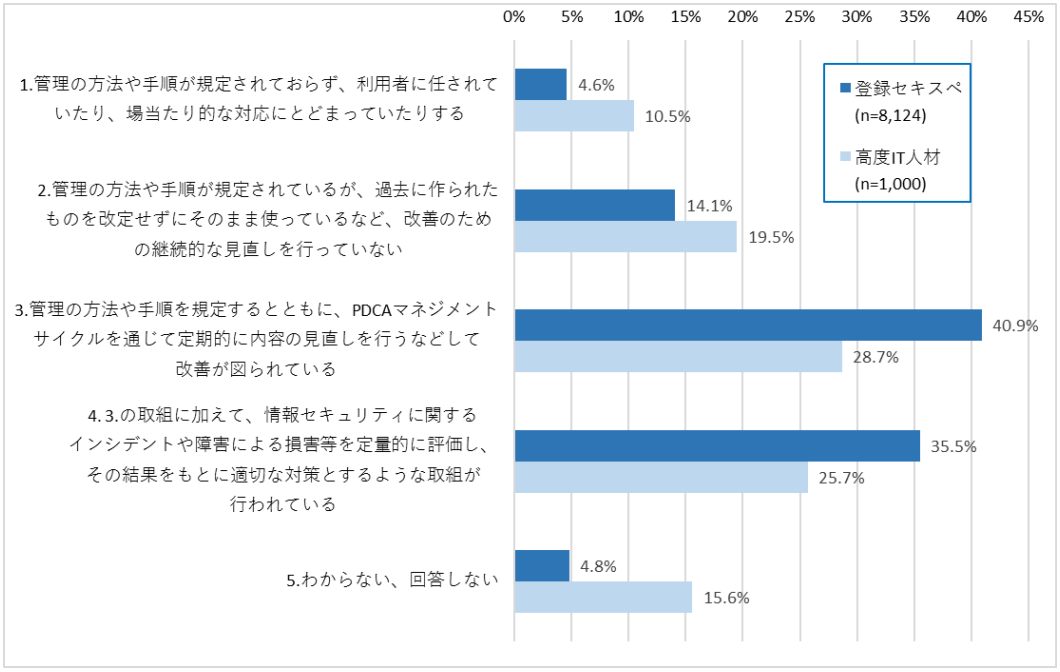


図 2-101 所属部署の行っている事業における情報機器やそのセキュリティ対策の管理状況（n=8,124）

2.10.2. 自組織の IT に関わる登録セキスペの組織規模・業種別分布

(A)コーポレート IT と(B)ビジネス IT のどちらかに属する、自組織の IT に関わる登録セキスペについて、その組織規模分布、及び業種別分布をまとめた。

値は人数であって、会社数ではない点に注意しなくてはならないが、組織規模が小さいほど、自組織の IT に関わる登録セキスペは少ないことが分かる。

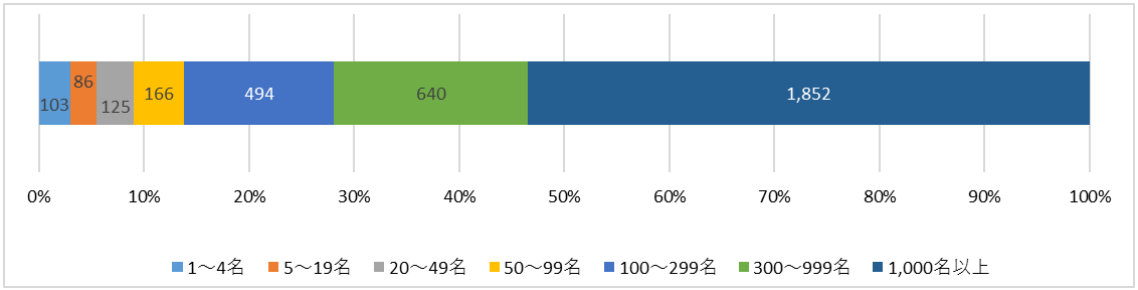


図 2-102 自組織の IT に関わる登録セキスペの組織規模別分布(n=3,466)

また業種別にみると、IT をビジネスで活用する業種(図 2-103 の 1.～3.)に所属する登録セキスペが多いが、それ以外の業種で見ると、製造業、サービス業、運輸・通信・郵便業、金融・保険業、官公庁などに 200 名前後又はそれ以上の登録セキスペがいることが分かる。登録セキスペが所属しているということは、それだけセキュリティ対策に取り組む意識が高いことを示しており、ビジネスでの IT 活用度合が高い業種とみることもできる。

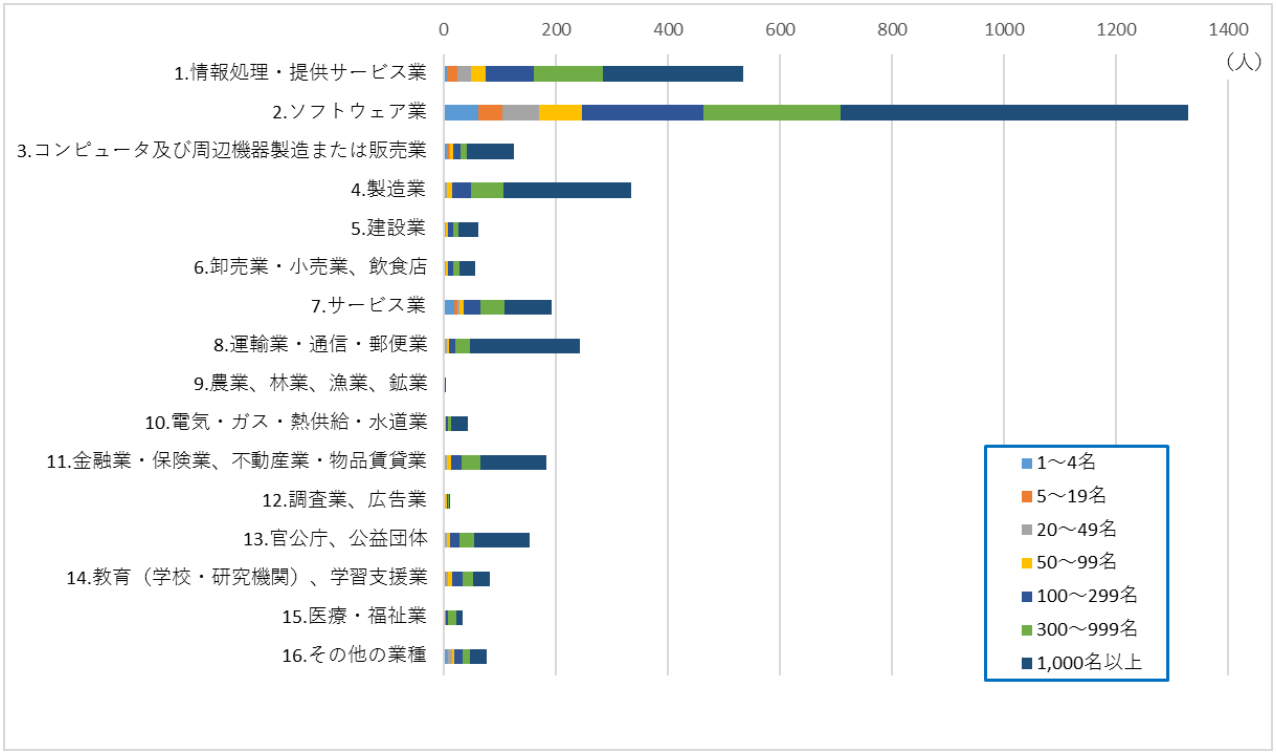


図 2-103 自組織の IT に関わる登録セキスペの業種分布(n=3,466)

また、業種によって、組織規模の分布が異なっていたため、99 名以下の組織に所属する登録セキスペの登録率を業種別に算出した。これから、製造業や運輸・通信・郵便業、金融・保険業では、登録セキスペが大規模組織に偏っていることが分かった。

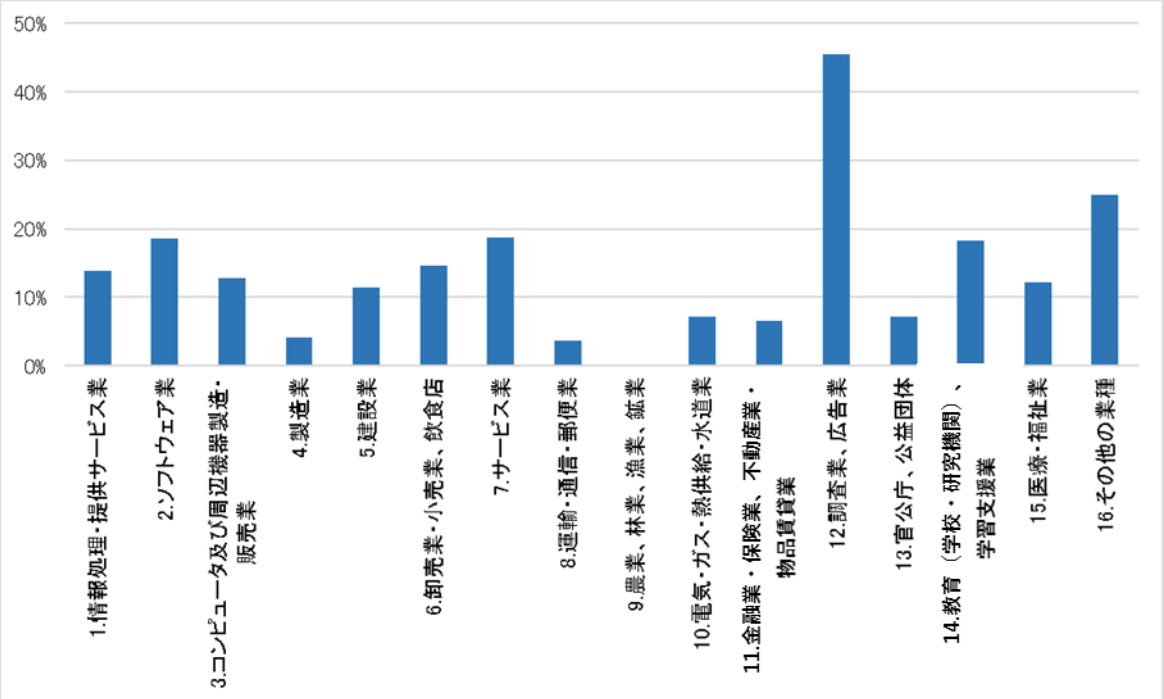


図 2-104 99 名以下の組織に所属する自組織の IT に関わる登録セキスペの業種別登録率

2.10.3. 「登録セキスペ」と「高度 IT 人材」の違い

高度 IT 人材（表 1 -2 参照）と登録セキスペの回答内容には大きく異なる点が多い。例えば、図 2-23 の担当するサイバーセキュリティ対策関連業務において、高度 IT 人材は上流業務の担当者が登録セキスペと比較して多い。また、図 2-76 を見るとサイバーセキュリティ業務遂行において経営層や企画関連部門と頻繁にコミュニケーションをとると答える割合が登録セキスペと比較して高い。この違いが発生する理由を考察した。

まず、図 2-14 から、高度 IT 人材は、登録セキスペと比較して（C）IT ベンダに所属する人数割合が低く、約半分程度である。したがって（A）コーポレート IT や（B）ビジネス IT の傾向に近いと考えられる。しかし、これだけでは差異が説明しきれないため、高度 IT 人材の抽出条件（表 1-2 参照）が登録セキスペのボリュームゾーンと差異がある可能性を考えた。抽出条件は 2 つあり、それぞれの合致人数を確認したところ、表 2-5 のとおりであった。

表 2-5 高度IT人材の抽出条件と合致人数[10]

抽出条件	合致人数(割合)
① 情報処理技術者試験のうち高度試験の合格者 （ただし、情報処理安全確保支援士登録者を除く）	385 名（38.5%）
② IT 関連業務に従事しつつ、部下を指導できるチームリーダー以上のスキル・能力を発揮している[11]	815 名（81.5%）

条件①は登録セキスペにも合致する条件となるため、これが差異につながることは考えにくい。したがって、条件②が登録セキスペのボリュームゾーンとのずれにつながっていると考える。平均年齢の差異（高度 IT 人材：46.9 歳、登録セキスペ：42.1 歳）、管理職以上の割合の差異（高度 IT 人材：47.5%、登録セキスペ：29.7%）を併せて考えると、登録セキスペのボリュームゾーンは「チームリーダーの一歩手前」と考えられる。

[10] ①と②両方を満たす高度 IT 人材もいるため、合算して 1,000 名にはならない。
[11] 次の選択肢のうち、4.以上を選択した人を抽出した。
1. 新人・初級者レベル／仕事に慣れ始めたレベル
2. 上位者の指導のもとに仕事ができる若手人材レベル
3. 独立して仕事ができる中堅人材レベル
4. 部下を指導できるチームリーダーレベル
5. 社内での指導者・幹部レベル
6. 国内で著名なレベル
7. 国際的に著名なレベル

3. サイバーセキュリティ対策業務の担当状況によるクラスタ分析[12]

2.3.5 で記載したとおり、登録セキスペは、複数のサイバーセキュリティ対策関連業務を担当していることが多い。更に、担当業務の組み合わせを調べてみると、「(A)コーポレート IT に関わる登録セキスペはサイバーセキュリティ対策関連業務を全般的に担当している人が多い」など、いくつかの傾向があった。

そこで、担当するサイバーセキュリティ対策関連業務に関する回答内容を基にクラスタ分析を行い、業務の組み合わせの似ているまとまり(クラスタ)を抽出した。更に、得られたクラスタの属性値を分析することで、サイバーセキュリティ対策を担う人材の現状が一部見えてきた。

本章では、3.1 に実施したクラスタ分析について述べ、3.2 に得られたデータを掲載し、3.3 に業務担当状況の分析内容と考察を記載している。

3.1. クラスタ分析手順

3.1.1. 分析に活用した設問

分析に使った設問は次のとおり。

設問文:
以下のサイバーセキュリティ対策に関連する業務のうち、あなたが担当している役割として、以下の(2)～(4)の中から最も近いものをそれぞれ 1 つ選択してください。なお、担当していない業務については(1)を選択してください。

選択肢1(業務の種類):
- サイバーセキュリティに関する経営判断
- サイバーセキュリティ管理体制の構築(コンサルティングを含む)
- サイバーセキュリティ管理体制のマネジメント(コンサルティングを含む)
- セキュア設計・開発・構築・評価(コンサルティングを含む)
- IT システム・サービスのセキュリティ面での運用・管理(外部委託・調達等を含む)
- サイバーセキュリティ対策機器の運用・保守
- 監視・情報収集
- 脆弱性診断、情報セキュリティ監査
- インシデント対応(コンサルティングを含む)
- セキュリティ技術及びサイバーセキュリティ対策に関する調査・研究
- サイバーセキュリティに関する教育・人材育成
- その他の業務

選択肢2(役割):
- (1)担当していない
- (2)責任者・管理者(実務より管理業務が主体)
- (3)主導的な実務者(責任者を兼ねる場合も含む)
- (4)補佐的な実務者
- (5)回答しない

[12] 本分析は、東京工業大学　情報理工学院　吉川厚特定教授と、東京工業大学 情報理工学院 情報工学系知能情報コース修士　青木亮磨氏にご支援いただいて実施した。

3.1.2. データの前処理

データの前処理として次の作業を実施した。

・「選択肢 2（役割）」は、各役割に応じて変換した（(2) 責任者・管理者→3、(3) 主導的な実務者→2、(4) 補佐的な実務者→1、(1) 担当していない・(5) 回答しない→0 に変換）。

・サイバーセキュリティ対策関連業務を 1 つも担当していないと回答した人は 1 つのクラスタとして扱う。

3.1.3. クラスタ数の推定シミュレーションと確定

前処理後のデータについて、BIC 基準によるクラスタ数推定シミュレーションを実施した。その結果、推定されたクラスタ数のうちいくつかを選択して実際にクラスタを生成させ、クラスタごとに属性値を算出・比較した。その結果を見て、分類の意味が理解しやすいクラスタ数に確定した。

3.2. クラスタ分析結果

クラスタ分析は、登録セキスペ回答者全員を対象に実施し、加えて IT との関わりのグループ（A）～（D）に分けても行った。

3.2.1. クラスタ数推定シミュレーション結果

クラスタ数推定シミュレーションは 100 回行い、結果は図 3-1 のとおりであったため、クラスタ数は 20 で確定した。

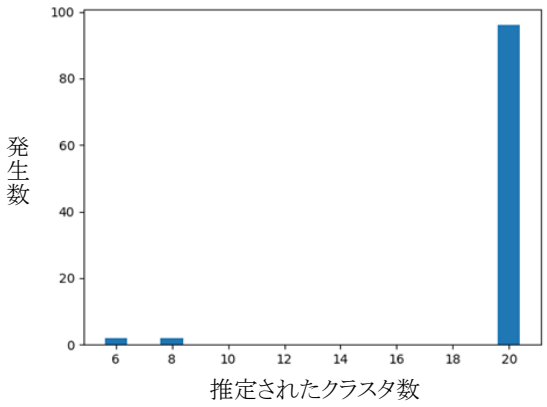


図 3-1 クラスタ数推定シミュレーション結果

3.2.2. クラスター一覧と属性値

20 個のクラスタについて、サイバーセキュリティ対策関連業務の担当状況と、いくつかの属性値（平均担当業務数、平均年齢、役職分布、組織規模分布など）を算出した。なお、サイバーセキュリティ対策関連業務の担当状況の詳細は図 6-5～図 6-7 を、また属性値の詳細は図 6-1～図 6-4 を参照のこと。

サイバーセキュリティ対策関連業務の担当状況と、いくつかの属性値を表 3-1 に示す。なお、記載する属性値の意味は次のとおりである。

- **平均担当業務数**

  「担当している」と回答したサイバーセキュリティ対策関連業務数の平均値。どのような役割で担当しているかは問わない。

- **平均年齢**

  クラスタを構成する人の年齢の平均値。

- **役職:管理職以上**

  役職が管理職以上と答えた人の割合。

- **組織規模:千人以上**

  所属する組織の人数規模が 1,000 名以上であると答えた人の割合。

- **セキュリティ対策が主業務部署**

  自組織のセキュリティ対策を主担当業務とする部署に所属している、と答えた人の割合。

- **セキュリティサービス提供が主業務部署**

  外部向けセキュリティ対策事業を主担当業務とする部署に所属している、と答えた人の割合。

表 3-1 クラスター一覧

クラスタ No.	人数	サイバー関連業務の担当状況(着色:8割以上、斜線:4割～8割)												クラスタの属性値					
		経営判断	管理体制の構築	マネジメント	セキュア設計	システム運用	機器運用保守	監視情報収集	脆弱性／監査	インシデント	調査研究	教育・人材育成	その他	平均担当業務数	平均年齢	役職:管理職以上	組織規模:千人以上	セキュリティ対策が主業務部署	セキュリティサービス提供が主業務部署
1	179	■	■	■	■	■	■	■	■	■	■	■		10.6	47.1	90.1%	31.8%	21.4%	26.2%
2	223	▨	■	■	▨	▨		▨	▨	■	■	■		8.1	46.7	58.3%	49.8%	22.4%	21.4%
3	429		■	■	■	■	■	■	■	■	■	■		10.4	45.4	58.2%	37.2%	21.0%	17.9%
4	215				■	■				■				4.1	42.7	45.2%	68.8%	1.9%	12.4%
5	234		■	■	■	■	■	■	▨	■	▨			8.6	43.3	43.8%	49.6%	15.0%	18.1%
6	298										▨	■		3.1	43.4	36.0%	56.6%	6.9%	22.1%
7	277		▨	▨	■	■	■	■	■	■	■	■		8.3	42.7	35.5%	59.2%	7.7%	20.1%
8	379				■	■								3.3	41.4	33.6%	67.5%	0.8%	18.0%
9	326	▨	■	■	■	■	▨	▨	▨	▨	▨			7.3	42.8	32.7%	53.8%	13.8%	22.2%
10	217				▨	■	▨	■	■	■				6.1	42.8	32.2%	63.0%	3.8%	11.7%
11	320					■								2.3	42.4	30.8%	67.2%	2.6%	11.9%
12	226		▨	▨		■	■	■	▨	■	■	■		8.1	42.2	28.8%	55.4%	20.7%	14.9%
13	190				▨				■					2.7	42.7	26.3%	63.3%	6.0%	27.7%
14	345		▨	▨	■	■	▨	■	■	■	■	▨		7.5	42.0	25.2%	59.1%	11.4%	18.0%
15	452				■									2.1	41.1	24.6%	59.4%	1.2%	15.2%
16	348				▨	■	■	■		■				5.3	40.9	21.5%	58.8%	3.8%	17.3%
17	1,414													0.0	41.2	21.2%	55.3%	2.1%	8.7%
18	927				▨	▨								1.7	41.4	20.1%	58.7%	1.9%	7.5%
19	516					▨				■				2.7	40.6	18.9%	55.0%	2.8%	7.3%
20	336					▨	■	■		▨				4.1	40.1	16.8%	52.6%	2.5%	17.2%

※「人数」及び「クラスタの属性値」は、色の濃さで値の大きさを表している。

※「役職:管理職以上」の値で降順に並べている

また、それぞれのクラスタ所属者が、グループ（A）～（D）に所属する割合を表 3-2 に示す。

表 3-2 クラスター一覧 各グループに属する割合

クラスタNo.	各グループ割合				
	(A)コーポレートIT	(B)ビジネスIT	(C)ITベンダ	(D)IT調査研究・教育他	IT業務無
1	65.9%	40.8%	38.5%	34.6%	1.7%
2	44.4%	24.2%	45.3%	45.3%	3.6%
3	66.4%	38.2%	38.2%	38.9%	1.2%
4	24.2%	22.8%	75.3%	3.7%	0.9%
5	55.1%	28.2%	48.7%	17.5%	0.4%
6	23.2%	14.1%	36.9%	48.7%	10.7%
7	47.3%	30.3%	57.4%	24.9%	1.4%
8	26.4%	26.1%	77.0%	7.1%	0.0%
9	37.4%	27.3%	53.4%	25.2%	4.0%
10	29.5%	28.1%	71.0%	9.7%	0.9%
11	28.4%	20.3%	68.4%	5.0%	1.3%
12	58.8%	23.9%	35.0%	32.7%	3.1%
13	21.1%	18.4%	60.5%	13.2%	8.4%
14	34.5%	27.8%	51.0%	33.0%	3.2%
15	17.7%	21.9%	74.6%	9.5%	4.9%
16	37.6%	26.1%	62.9%	6.9%	0.9%
17	15.7%	13.7%	54.8%	5.7%	21.6%
18	21.9%	16.5%	61.7%	9.4%	10.7%
19	28.5%	20.0%	60.9%	9.1%	7.4%
20	32.1%	20.5%	58.0%	8.0%	5.4%

※「各グループ割合」は、色の濃さで値の大きさを表している。

※グループの区別に関わる設問は複数選択可能のため、合計すると 100%を超える。

3.3. 登録セキスペの業務担当状況の分析

3.2 のデータをもとに、登録セキスペのサイバーセキュリティ対策関連業務担当状況を分析する。

3.3.1. 役割の分類

20 個のクラスタは、サイバーセキュリティ対策関連業務担当状況の類似性から、次のように分類した。これらは、登録セキスペがどのような役割を担っているかを表している。

- **経営課題ストラテジ**

  サイバーセキュリティ対策関連業務を全般的に担当している。

- **IT 全体デザイン**

  サイバーセキュリティ対策関連業務を全般的に担当しているが、上流業務（「経営判断」、「管理体制の構築」、「マネジメント」）は補助的に担当している、又は担当していない。

- **設計運用管理**

  IT ライフサイクル全般に幅広く関わりセキュリティ確保を担当している

- **設計開発**

  セキュアな設計・開発・構築・評価を担当している（運用系業務は担当していない）

- **運用管理**

  インシデント対応を含む運用系業務を担当している

- **運用**

  運用系業務を担当している

- **緊急対応**

  インシデント対応業務を担当している

- **監査・脆弱性診断**

  情報セキュリティ監査又は脆弱性診断業務を担当している

- **育成**

  サイバーセキュリティに関する人材育成業務を担当している

3.3.2. 役割の分類とレベル

3.3.1 の分類ごとにクラスタをまとめ、役職レベルを図示してみると、図 3-2 のようになった（縦に伸びる帯が一つのクラスタで、帯に記載される数字はクラスタ No を表す）。併せて、その役割の分類ごとの人数・割合も示した。

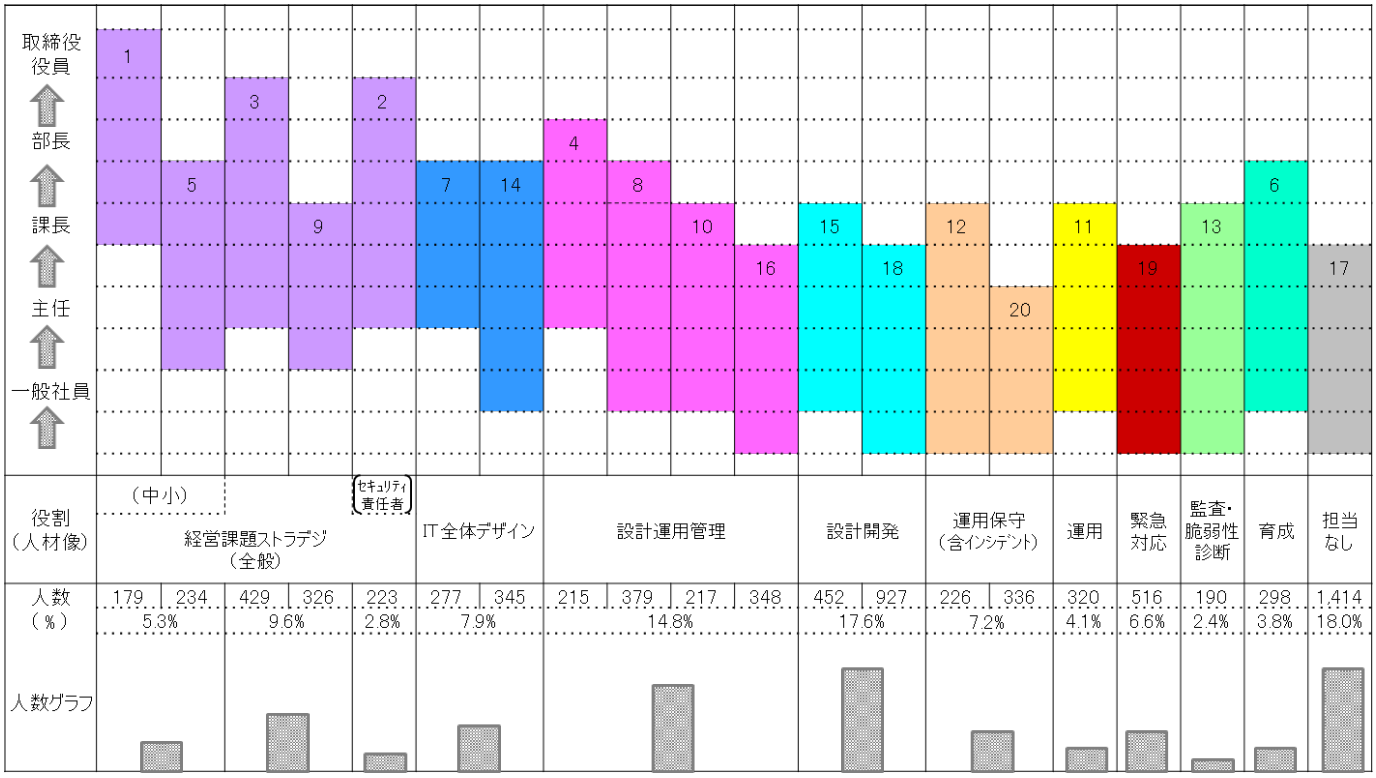


図 3-2 役割の分類とレベル（役職の分布） n=7,851

3.3.3. 役割の分類ごとに関する考察

役割の分類ごとに、主担当業務として選択した業務を調べた。

「経営課題ストラテジ」に分類されるクラスタ（No.1,2,3,5,9）

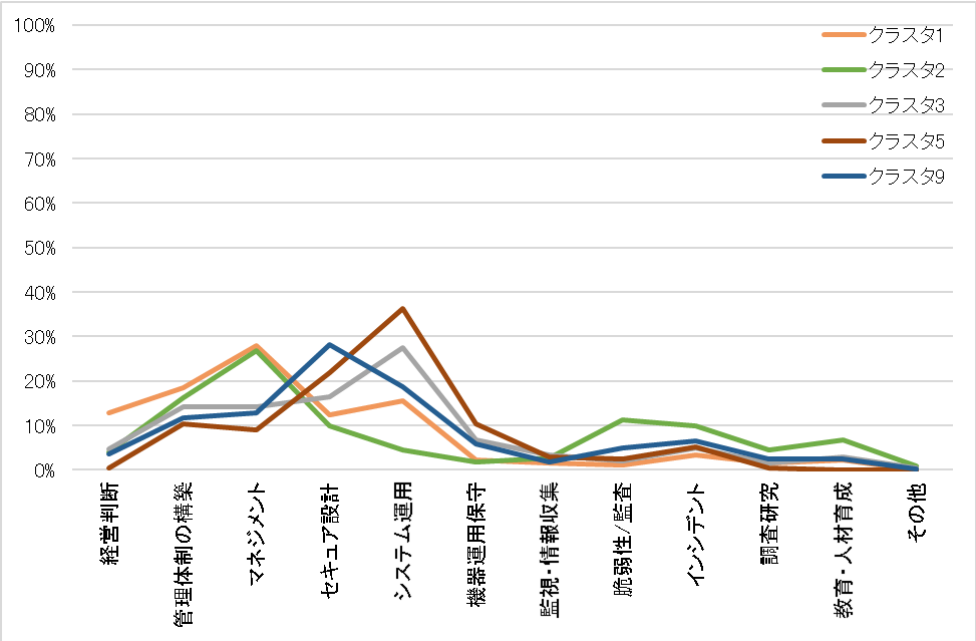


図 3-3 主担当業務の選択割合（「経営課題ストラテジ」のクラスタ）

「経営課題ストラテジ」に分類されるクラスタのうち、No.1 と No.3 は平均担当業務数が 10.6 及び 10.4 と極めて大きく、ほぼすべてのサイバーセキュリティ対策関連業務に関わっていると言える。両者の違いは、責任者・管理者としてであるか、主導的な実務者として担当しているかの違いである（図 6-5、図 6-6 参照）。どちらのクラスタも、所属組織の人数規模 300 名未満が半数近くを占めることから、比較的小さい規模の組織において、経営層又は経営層のサポートする組織がサイバーセキュリティ対策業務全般を担当していると考えられる。責任者（No.1）の主業務は「サイバーセキュリティ管理体制のマネジメント」を主業務とする人が多く、主導的な実務者（No.3）は「システムのセキュリティ面での運用」を主業務とする人が多いことが図 3-3 から分かる。

次に No.5、No.9 は、所属組織の人数規模 300 名未満はおよそ 1/3 であり、全体の分布と近い（図 6-2）。平均担当業務数は 8.6 及び 7.3 となり、大企業に近づくとある程度業務分担されることを示している。役職が高めのクラスタ（No.5）では主担当業務が「システムのセキュリティ面での運用」の人が多く、役職が低めのクラスタ（No.9）では主担当業務が「セキュア設計・開発」の人が多いことが、図 3-3 から分かる。また、どちらのクラスタも、（C）IT ベンダの割合が半数前後であり、セキュリティ分野のコンサルタントがこのクラスタに属していると考えられる。

No.2 は、この分類の他のクラスタと業務担当状況が異なり、「セキュア設計・開発」、「システム運用」を担当している割合が少なく、上流業務とインシデント対応が主な担当業務である。部長以上の役職に就く人が 2 割以上と、他のクラスタと比較して高く（図 6-3 参照）、（A）コーポレートITと（C）ITベンダの割合が同等で 5 割弱あることから、CISO などの組織のセキュリティ責任者、及びセキュリティ対策のコンサルタントと考えられる。

「IT 全体デザイン」に分類されるクラスタ（No.7, 14）

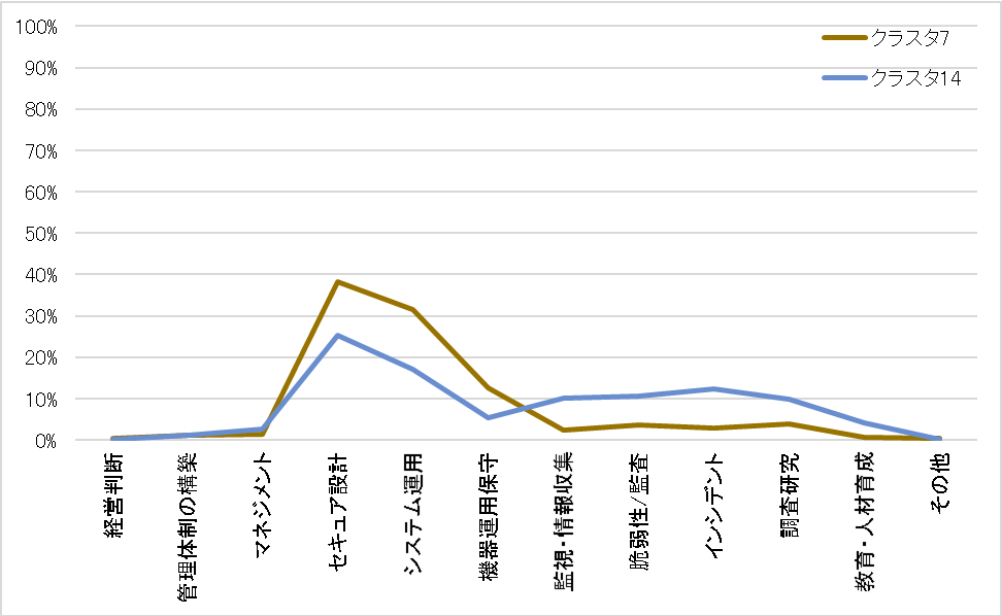


図 3-4 主担当業務の選択割合（「IT 全体デザイン」クラスタ）

「IT 全体デザイン」に分類されるクラスタは、「セキュア設計・開発」、「システムのセキュリティ面での運用」を主業務として担当し、上流業務は補助的に、それ以外の業務は全般的に担当している人である。役職分布においてあまり高くない（部長以上が 1 割弱）ことが特徴的である（図 6-3 参照）。

表 3-2 を見ると、(C)IT ベンダに所属する割合がそれぞれ 5 割以上と多いが、(A)コーポレート IT に所属する割合も No.7 で 5 割弱、No.14 で 3 割強と少なくない。ユーザ企業の情報システム部門などの若手で、サイバーセキュリティの管理よりは IT システムの構築や運用を中心に担当している人、及びそれを委託されている IT ベンダの方々がこのクラスタに属していると考えられる。

「設計運用管理」に分類されるクラスタ（No.4,8,10,16）

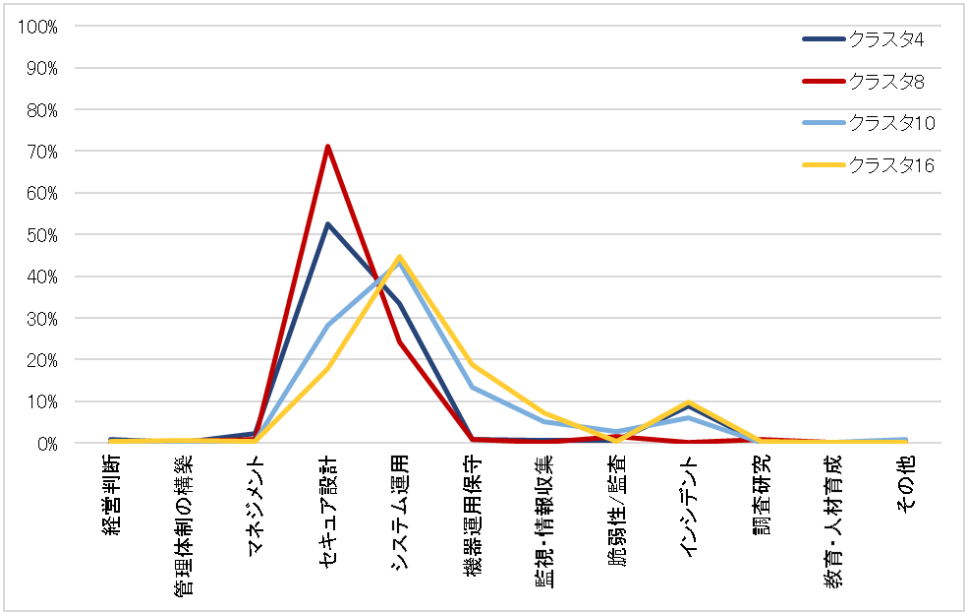


図 3-5 主担当業務の選択割合（「設計運用管理」クラスタ）

「設計運用管理」に分類されるクラスタは、設計系の業務と運用系の業務を両方担当している。図 3-5 で主担当業務を見ると、No.4、8 は「セキュア設計・開発」を主に担当しており、No.10、16 は「システムのセキュリティ面での運用」を主に担当している。設計中心の No4、8 は(C)IT ベンダの割合が最も高く、7-8 割を占める。運用中心の No.10、16 も(C)IT ベンダの割合が最も高いが、6-7 割であり、(A)コーポレート IT や(B)ビジネス IT の割合も 3-4 割ある。したがって、このクラスタの主な人材イメージは IT ベンダに所属して、システム設計・開発や運用・保守を顧客から受託して実施している技術者が想定できる。加えて、これらの業務を外部委託しないユーザ企業に所属する技術者も含まれているようである。設計中心のクラスタの役職分布は、運用中心のクラスタの分布よりも、役職の高い人の割合が大きい（図 6-3 参照）。

「設計開発」、「運用保守」、「運用」に分類されるクラスタ(No.15,18) (No.12,20) (No.11)

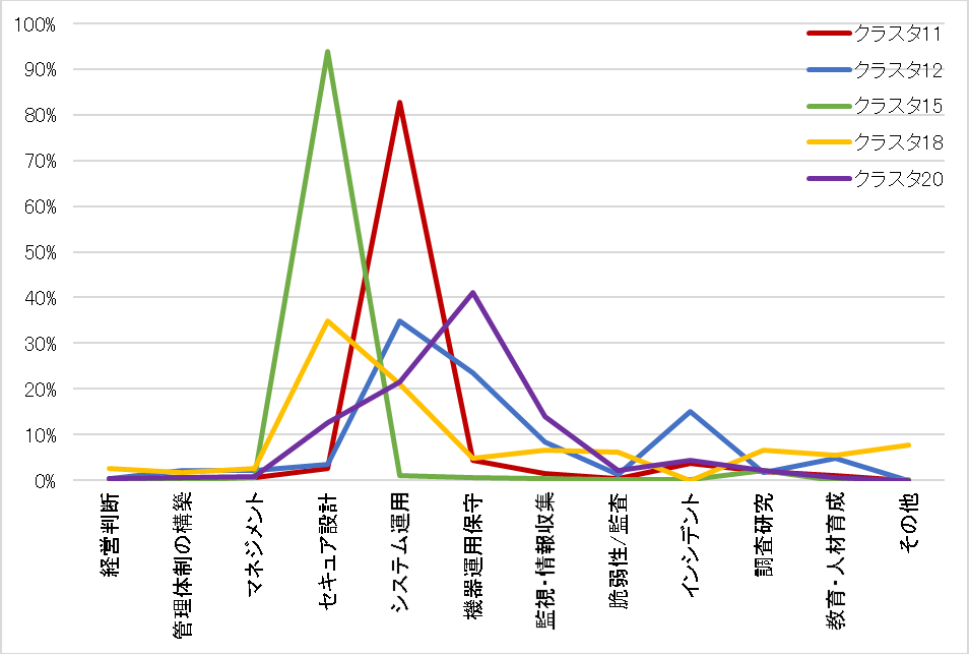


図 3-6 主担当業務の選択割合(「設計開発」「運用保守」「運用」クラスタ)

「設計開発」に分類されるクラスタのうち、No.15 は「セキュア設計・開発」を主に担当している人で、併せて「システムのセキュリティ面での運用」を担当しているが、それ以外はほぼ担当していない。ここから、特定のシステム担当者として開発から運用までを担当している人が想定される。No.18 は「セキュア設計」を中心にいくつかの業務を補助的な立場で担当しており、サイバーセキュリティ関連ではない他の業務を担当しながらサイバーセキュリティ対策関連業務を一部担当している人と考えられる。このクラスタは No.17 の「担当なし」以外では最も人数が多く、回答者全体の 11%を占める。No.15、18 どちらのクラスタも、(C)IT ベンダ所属の人の割合が 6-7 割と高く、役職分布をみると主任・担当レベルの人で 7-8 割である(図 6-3)。

「運用保守」に分類されるクラスタのうち、No.12 は「セキュア設計・開発」以外の業務を幅広く担当している人で、「システム運用」や「インシデント対応」を主担当業務としている人が多い。(A)コーポレート IT に属する割合が 6 割弱と高い。上流業務を担当することで、No.2 のクラスタに進む人の可能性がある。No.20 は、「機器運用保守」を中心に「システム運用」などを主業務としており、(C)IT ベンダに属する割合が 6 割弱で、課長以上の割合が 16.8%とクラスタの中では最も低い。ここから、セキュリティベンダや IT ベンダの若手技術者と考えられる。

「運用」に分類されるクラスタ No.11 は、「システム運用」以外の業務はほぼ担当していない。また、(C)IT ベンダに所属する割合が 7 割弱である。ここから、IT ベンダのシステム運用担当者と考えられる。課長以上が 3 割程度存在しており、「運用保守」のクラスタ(No.12、20)よりも値が高い。

「緊急対応」、「監査・脆弱性診断」、「育成」に分類されるクラスタ（No.19），（No.13），（No.6）

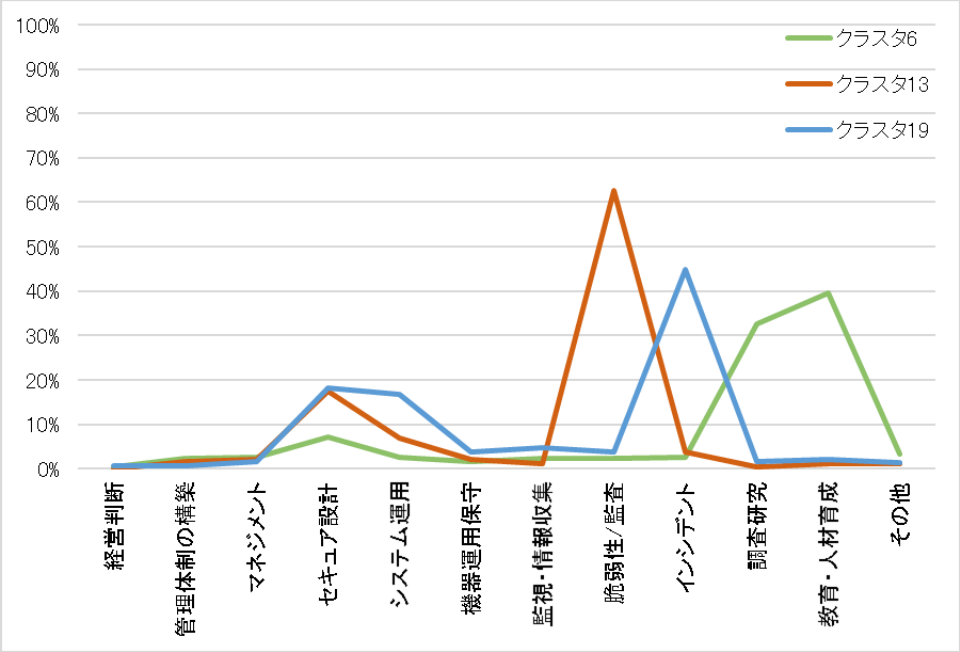


図 3-7 主担当業務の選択割合（「緊急対応」「監査・脆弱性診断」「育成」クラスタ）

「緊急対応」に分類されるクラスタ No.19 は、インシデント対応を主担当業務としている人が 5 割弱と多いが、「セキュア設計」や「システム運用」を主担当業務とする人もそれぞれ 2 割弱いる。課長以上の役職についている割合は 2 割弱と低い。ここから、インシデント対応に特化して担当している人材は若手であることが分かる。（C）IT ベンダに所属する割合が 6 割であるが、（A）コーポレート IT に所属する割合も 3 割弱いて他のクラスタと比較すると少なくない。

「監査・脆弱性診断」に分類されるクラスタ No.13 は、監査と脆弱性診断の各担当者が混在している。（C）IT ベンダに所属する割合が高く（6 割）、監査と脆弱性診断は外部委託することが多いことを表している。

「育成」に分類されるクラスタ No.6 は、「教育・人材育成」業務に加えて「調査研究」を担当している人が多いようである。また、課長以上の割合が 36.0％と他のクラスタと比較して高い。

「担当なし」に分類されるクラスタ（No.17）

クラスタ No.17 は、設問で提示した 12 のサイバーセキュリティ対策関連業務をすべて「担当していない」と回答した人である。このクラスタに属する全回答者の 22.1％の人は、セキュリティ知識・スキルを持ちながら、それを業務で活かせていないことを表している。

このクラスタに属する人のうち、業務上 IT に関わっていないと答えている人は 16.7％であり、逆に言うと 8 割以上の人（1,523 名，回答者の 18.4％）が IT に関わりながらもサイバーセキュリティ対策に関連する業務を行っていないことになる。

（参考に、高度 IT 人材の中でサイバーセキュリティ対策関連業務をすべて「担当していない」と回答した割合は 53.5％である。図 2-12 参照。）

4. 登録セキスペの現状

調査から見えてきた、登録セキスペの現状を述べる。

過半数は「プラス・セキュリティ人材」

「経営課題ストラテジ」(「セキュリティ責任者」を除く)、及び「IT 全体デザイン」、「設計運用管理」、「設計開発」、「運用保守」、「運用」に分類される人は、その業務遂行状況からセキュリティ業務のみを担当しているとは考えにくく、IT に関わる業務(IT 戦略立案から設計・開発、運用保守など)遂行の中でセキュリティスキルを活用している人が多いと考えられる。このような人材は「プラス・セキュリティ人材[13]」と呼ばれ、適切なサイバーセキュリティ対策実現の要となる人材である。本調査では、これらの分類に属する人の割合は回答者の約 6 割であった。

また、「経営課題ストラテジ」の「セキュリティ責任者」、及び「緊急対応」、「監査・脆弱性診断」等に分類される人は、セキュリティを主たる業務とする人材(以降、「セキュリティ専門人材」と呼ぶ)と考えられる。

セキュリティ人材に関する様々な議論があるが、「プラス・セキュリティ人材」と「セキュリティ専門人材」とで、その現状や課題は異なっていると考えられ、どちらをターゲットにした話なのか、切り分けて議論や検討を進める必要がある。

セキュリティに関わらない登録セキスペが約 2 割

明示的にサイバーセキュリティに関連する業務は担当していないと答えた人が登録セキスペの約 2 割であった点は、サイバーセキュリティ対策業務のある側面を表していると考える。セキュアな業務遂行は当たり前で非明示的に行われている可能性や、サイバーセキュリティ対策が必要ではない業務担当の人でもセキュリティ知識が必要と考えて資格を取得している可能性などが考えられる。

上位層の人材は事業を幅広く担当

「経営課題ストラテジ」及び「設計運用管理」には、部長以上の割合が 1 割以上ある分類が存在している(クラスタ No.1,2,3,4,5 を参照)。 ユーザ系企業で経営課題としてサイバーセキュリティ対策に取り組む上位層の人材と、IT ベンダ系企業で顧客の経営を支える IT を設計から運用まで全体的にサポートする上位層の人材を表していると推察する。

彼らは一種のキャリアゴールと考えられる。こういった方々は、対外的な自己アピールを主な目的として登録セキスペとなっている。(図 2-89 を参照)

中小規模の組織などで 1 人で活躍している登録セキスペは 5%

中小規模の組織などでは、平均担当業務数が 10 以上で、1 人でほぼすべての業務を担当している状況であった(クラスタ No.1,3 を参照)。更にこれらの分類は自組織で活用する IT の企画・構築・管理に関わる人が多く、中小規模の組織を中心に自組織で活用する IT のサイバーセキュリティを 1 人で支えている層がいることが分かった。この層は、回答者全体の 5%となる。

[13] 一般社団法人日本サイバーセキュリティ・イノベーション委員会:セキュリティ人材不足の真実と今なすべき対策とは～今必要なのは「プラス(+)・セキュリティ人材」だ～ https://www.j-cic.com/pdf/report/Human-Development-Plus-Security.pdf

ITとの関わりの違いに関する特長

IT との関わり区分（(A)コーポレートIT、(B)ビジネスIT、(C)IT ベンダ、(D)IT 調査研究・教育他）と 役割の分類 を分析する目的で、表 3-2 を再掲する。なお、役割の分類の単位にクラスタを並び替えている。

表 3-2 クラスター一覧 各グループに属する割合
〔 役割の分類の単位にクラスタを並び替えて 再掲 〕

役割の分類		クラスタNo.	各グループ割合				
			(A)コーポレートIT	(B)ビジネスIT	(C)ITベンダ	(D)IT調査研究・教育他	IT業務無
経営課題ストラテジ（全般）	（中小）	1	65.9%	40.8%	38.5%	34.6%	1.7%
		5	55.1%	28.2%	48.7%	17.5%	0.4%
		3	66.4%	38.2%	38.2%	38.9%	1.2%
		9	37.4%	27.3%	53.4%	25.2%	4.0%
	（セキュリティ責任者）	2	44.4%	24.2%	45.3%	45.3%	3.6%
IT全体デザイン		7	47.3%	30.3%	57.4%	24.9%	1.4%
		14	34.5%	27.8%	51.0%	33.0%	3.2%
設計運用管理		4	24.2%	22.8%	75.3%	3.7%	0.9%
		8	26.4%	26.1%	77.0%	7.1%	0.0%
		10	29.5%	28.1%	71.0%	9.7%	0.9%
		16	37.6%	26.1%	62.9%	6.9%	0.9%
設計開発		15	17.7%	21.9%	74.6%	9.5%	4.9%
		18	21.9%	16.5%	61.7%	9.4%	10.7%
運用保守（含インシデント）		12	58.8%	23.9%	35.0%	32.7%	3.1%
		20	32.1%	20.5%	58.0%	8.0%	5.4%
運用		11	28.4%	20.3%	68.4%	5.0%	1.3%
緊急対応		19	28.5%	20.0%	60.9%	9.1%	7.4%
監査・脆弱性診断		13	21.1%	18.4%	60.5%	13.2%	8.4%
育成		6	23.2%	14.1%	36.9%	48.7%	10.7%
担当なし		17	15.7%	13.7%	54.8%	5.7%	21.6%

※「各グループ割合」は、色の濃さで値の大きさを表している。
※グループの区分に関わる設問は複数選択可能のため、合計すると 100%を超える。

この特長を記すと以下のようになる。

(A)コーポレート IT　　主に「経営課題ストラテジ」と「運用保守」の分類に関わる人が多い。

(B)ビジネス IT　　特に多い分類はない。

(C)IT ベンダ　　「(A)コーポレート IT で多い分類」以外のほとんどにおいて、関わる人が多い。

(D)IT 調査研究・教育他　「経営課題ストラテジ」の中の「セキュリティ責任者」と「教育」の分類に関わる人が多い。

(B)ビジネス IT にて特に多い分類がなかったことは、現状ではビジネス IT のみを担当する人はあまり多くないことの表れかと思われる。 また「経営課題ストラテジ」の中の「セキュリティ責任者」については、(A)コーポレート IT と(C)IT ベンダの割合がほぼ同じであったが、これはその業務を 自組織で実施するか 外部ベンダとしても責任を持った対応とするのか の違いであり、どちらの立場で行っていても役割内容は変わらないことを示していると思われる。

5. おわりに

このたび得られた、「情報処理安全確保支援士（登録セキスペ）の活動に関する実態調査」のデータはすべて、「現状（As-Is）」を表しているものであり、今後の「あるべき姿（To-Be）」を表しているものではない。

登録セキスペをはじめとした高度なセキュリティ知識・スキルを持つ人材が活躍の場を広げていくことによって、サイバー空間における安心安全と経済発展の両立が浸透し、Society5.0 が進展する。従って、登録セキスペの活躍促進は重要課題と認識しており、自社（自組織）にとどまらず対外的な活動への展開を推進すべく、官民で連携した更なる調査や制度拡充等の取り組みが望まれる。

6. 補足資料:クラスタ属性値

3.2 で述べた、クラスタの属性値をグラフに示す。

年齢分布

各クラスタの年代別分布は図 6-1 のとおりである。平均年齢で昇順にソートしている。

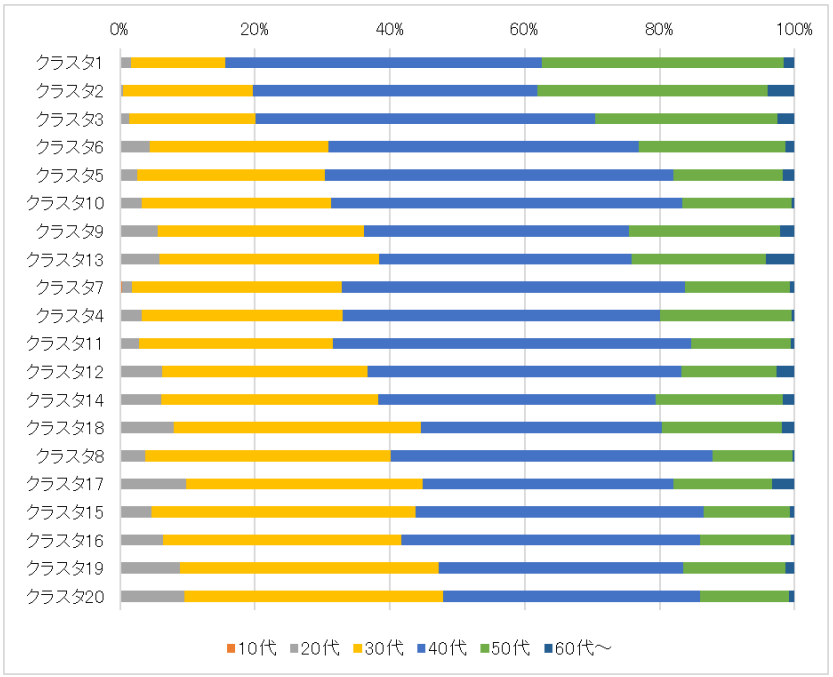


図 6-1 年齢分布

組織規模分布

各クラスタの組織規模別分布は図 6-2 のとおりである。組織規模 1,000 名以上の割合で昇順にソートしている。

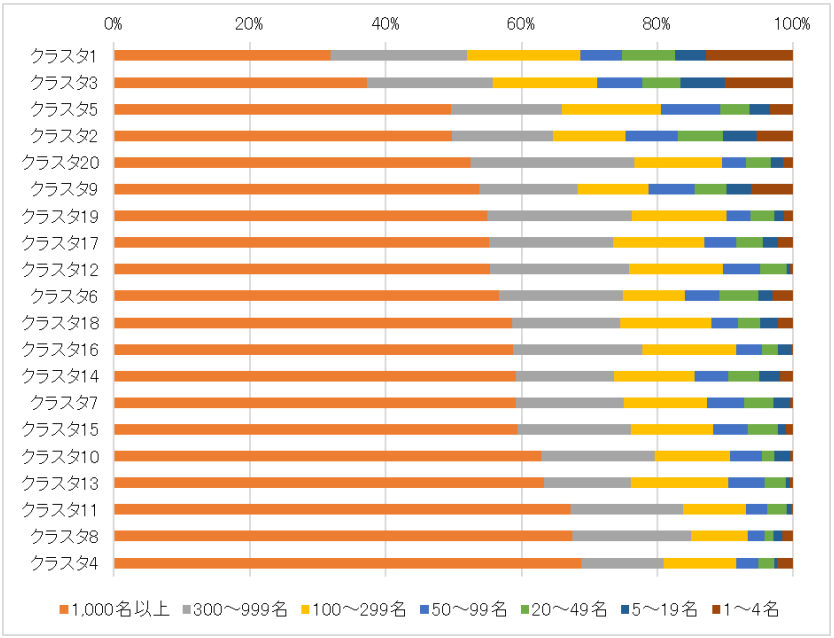


図 6-2 組織規模分布

役職分布

各クラスタの役職別分布は図 6-3 のとおりである。課長・マネージャクラス以上の割合の多い順にソートしている。

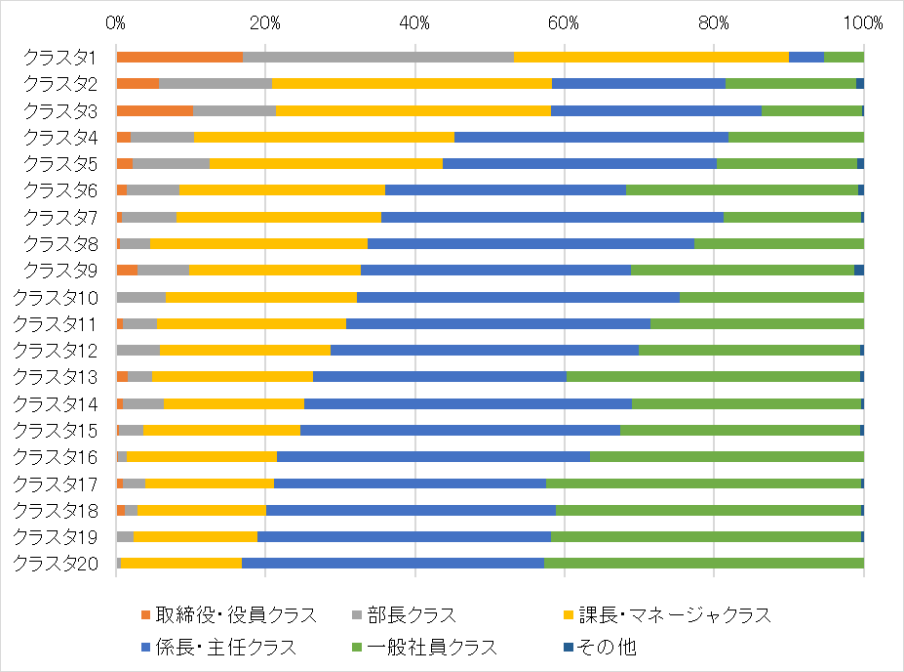


図 6-3 役職分布

所属組織のセキュリティ対策との関わり

セキュリティ対策とどのように関わっている組織に所属しているかで、分布をグラフ化した。

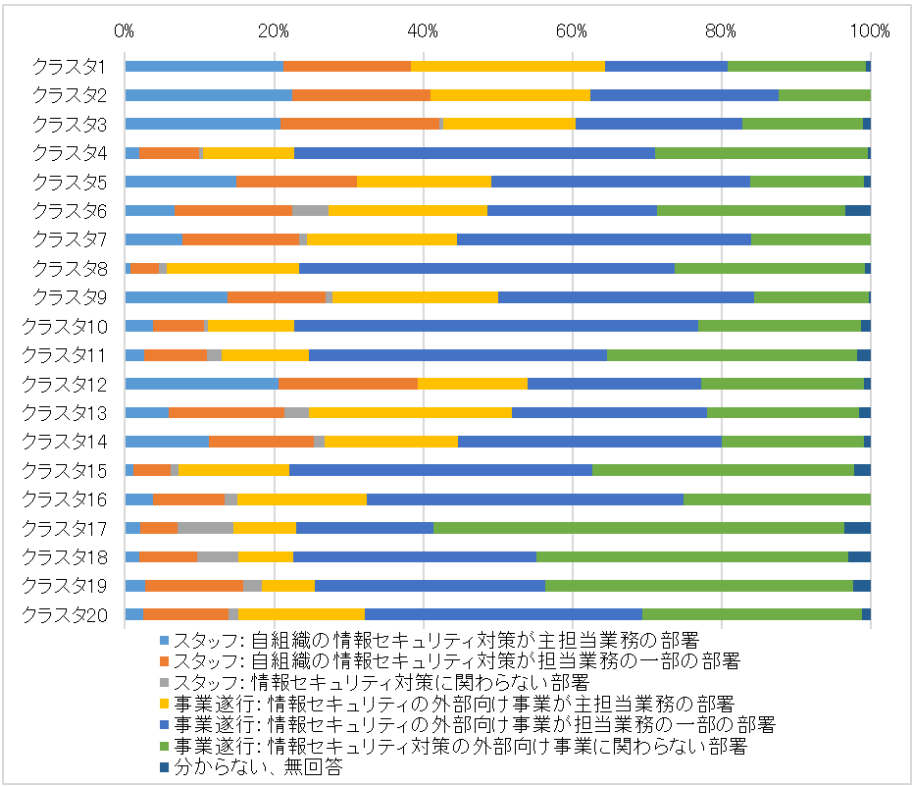


図 6-4 所属組織のセキュリティ対策との関わり

サイバーセキュリティ対策関連業務　担当状況

クラスタごとに、サイバーセキュリティ対策関連業務の担当状況をグラフ化した。縦軸はサイバーセキュリティ対策に関連する 12 業務を示しており、それぞれの業務について、責任者・管理者/主導的な実務者/補助的な実務者/担当していない　の選択をした人数を割合で示している。

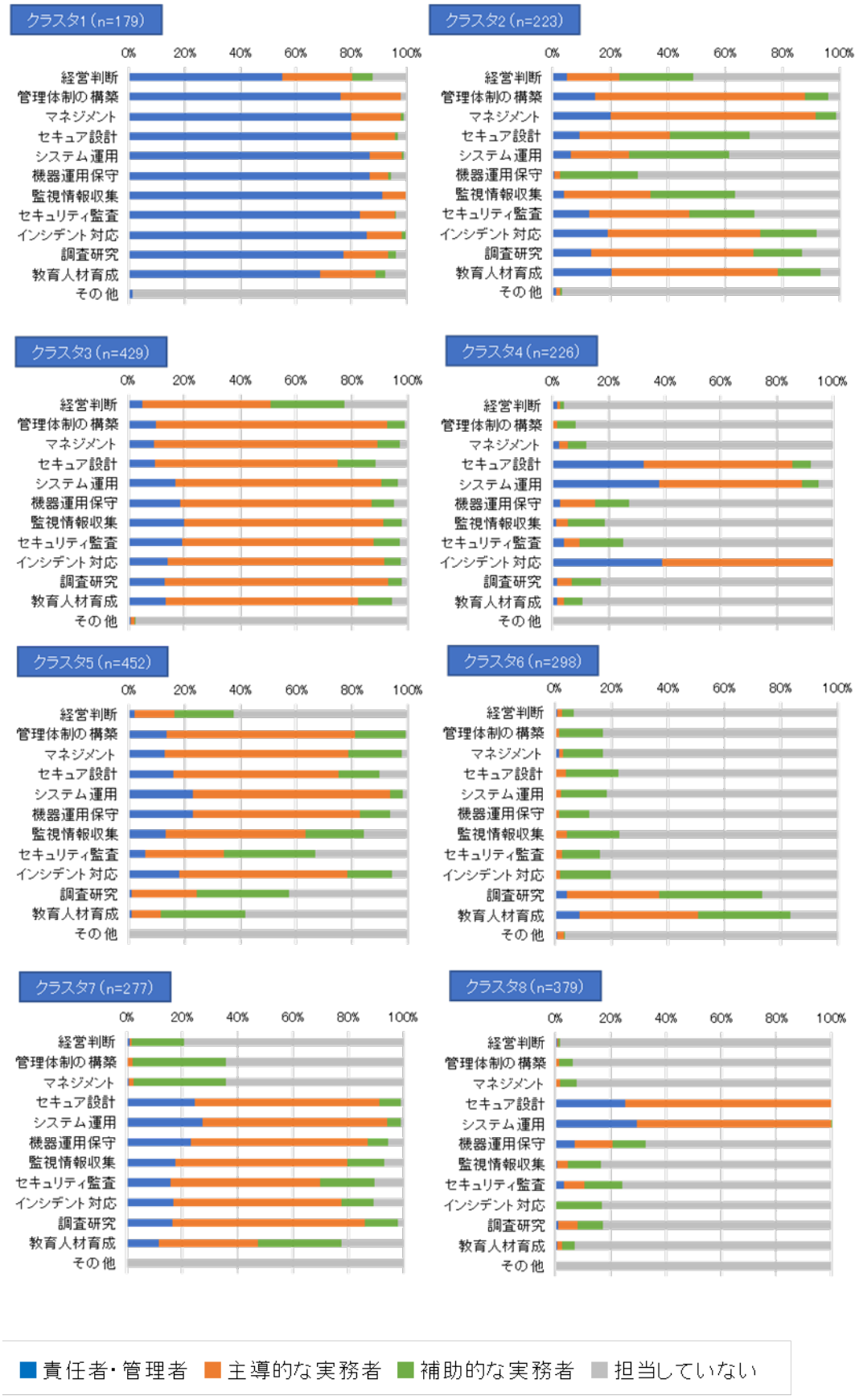


図 6-5 サイバーセキュリティ対策関連業務 担当状況（登録セキスペ回答者全員のクラスタ分析）クラスタ 1～8

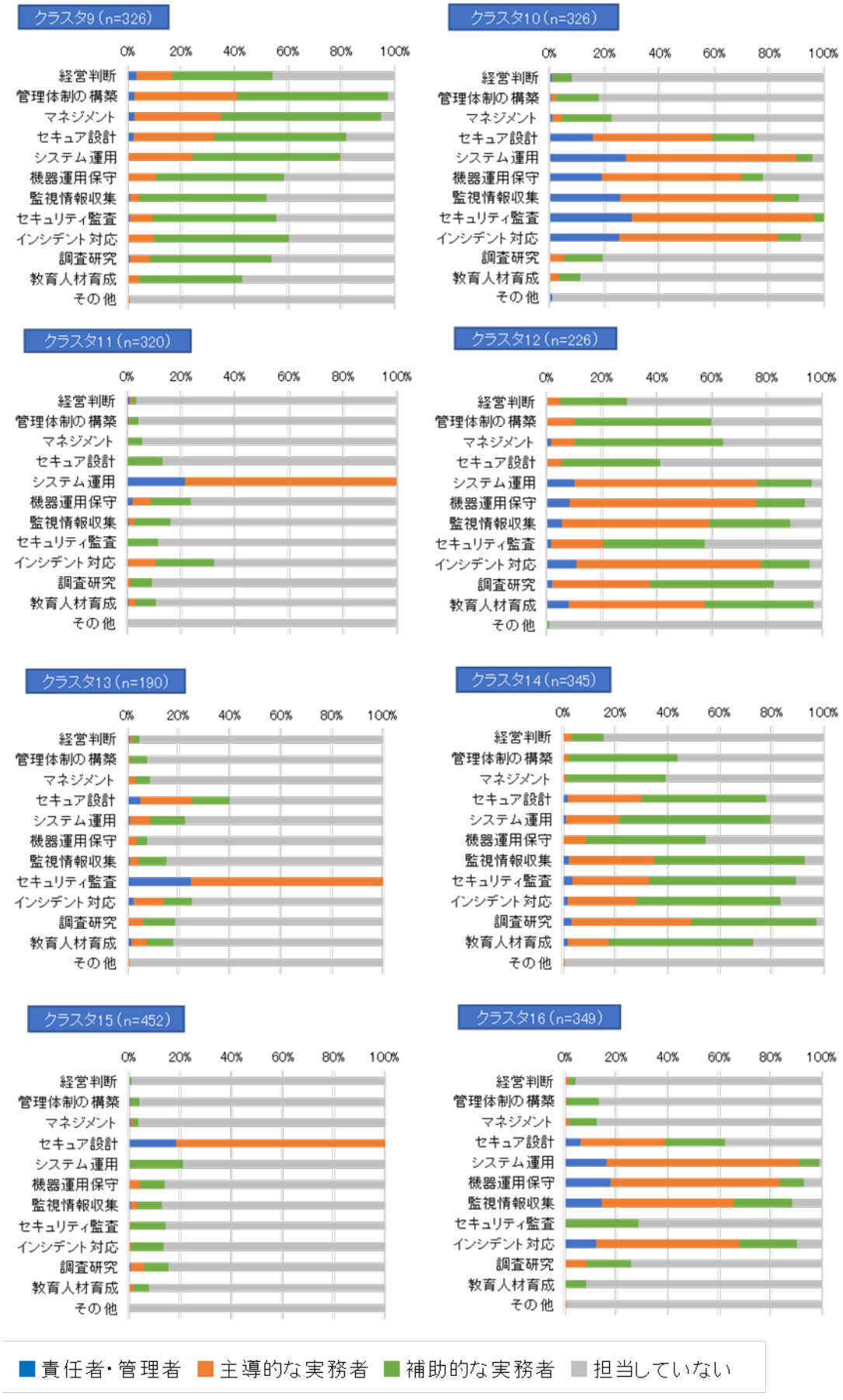
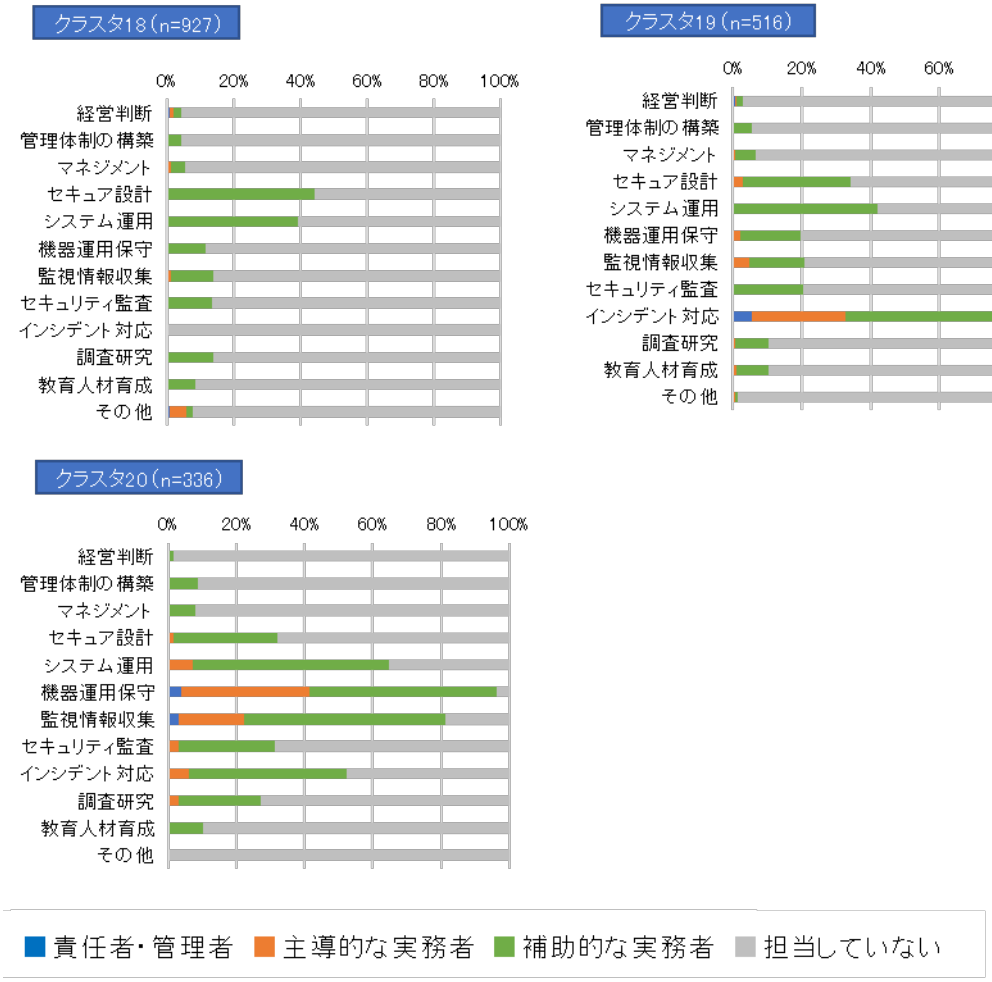


図 6-6 サイバーセキュリティ対策関連業務 担当状況（登録セキスペ回答者全員のクラスタ分析）クラスタ 9～16



※クラスタ 17 は担当業務がないためグラフを記載せず

図 6-7 サイバーセキュリティ対策関連業務 担当状況（登録セキスペ回答者全員のクラスタ分析）クラスタ 18～20

7. 補足資料:アンケート調査票(登録セキスペ向け)

登録セキスペに回答を依頼したアンケート調査票を示す。

＜用語の定義＞

本調査では、設問において次表の用語をそれぞれ表内のような意味で用います。

用語	定義および説明
サイバーセキュリティ	様々な定義が存在しますが、本調査では「情報セキュリティ」と同義として解釈して下さい。例えば、サイバーセキュリティ業務には情報セキュリティ管理に関する業務を含みます。
CISO	最高情報セキュリティ責任者（Chief Infomation Security Officer）
CIO	最高情報責任者（Chief Infomation Officer）
CSIRT	コンピュータセキュリティインシデント対応チーム（Computer Security Incident Response Team、コンピュータやネットワークを対象とするサイバーセキュリティ上の問題に対応するための組織）

【あなたの業務形態】

Q1　あなたの職業として、最も近いものを１つ選択してください。兼業又は出向されている方は、最も従事時間の長いものについてご回答ください（Q2以降も同様でお願いします）。

回答欄

1．会社役員・団体役員（個人事業主を除く）
2．正社員・団体職員
3．公務員（みなし公務員を含む）
4．個人事業主、フリーランス、自営業
5．派遣社員、非正規社員、パートタイム社員
6．アルバイト
7．学生
8．無職（ボランティアを含む）
9．その他
10．回答しない

「9. その他」を選択した場合は、下記に業務形態を記入してください。

【ご所属の企業・団体（事業）について】

Q2　［Q1で1～5を選択した回答者のみ］

Q1で回答した職業において従事されている、あなたがご所属の企業・団体の業種として、次の中から最も近いものを１つ選んでください。

※複数の事業を行っている企業や団体に所属している場合は、あなたが所属している部署で行っている事業における業種として、最も近いものを1つご回答ください。

回答欄

1．情報処理・提供サービス業（計算サービス、データエントリサービス、各種のデータを収集、加工、蓄積し、情報として提供する業種）
【例】受託計算サービス業、タイムシェアリングサービス業、データエントリ業、データベースサービス業など）

2．ソフトウェア業（プログラムの作成及びその作成に関して、調査、分析、助言などを行う業種）
【例】受託開発ソフトウェア業、パッケージソフトウェア業、システムインテグレータなど）

3．コンピュータ及び周辺機器製造または販売業
4．製造業（選択肢2, 3にあてはまるものを除く）
5．建設業
6．卸売業・小売業、飲食店
7．サービス業（選択肢1, 2, 3にあてはまるものを除く）
8．運輸業・通信・郵便業（倉庫業を含む）
9．農業、林業、漁業、鉱業
10．電気・ガス・熱供給・水道業
11．金融業・保険業、不動産業・物品賃貸業
12．調査業、広告業
13．官公庁、公益団体
14．教育（学校・研究機関）、学習支援業
15．医療・福祉業
16．その他（上記選択肢1～15で分類不能の業種）
17．わからない、回答しない

Q3　［Q1で1～5を選択した回答者のみ］

Q1で回答した職業に関して、所属する企業・団体の総従業員数として、あてはまるものを１つ選んでください。

※正社員以外の雇用形態の社員を含み、派遣社員を除いてください。

※複数の事業を行っている企業や団体に所属している場合は、あなたが所属している部署の行っている事業に従事する人数をご回答ください。

回答欄

1．1～4名
2．5～19名
3．20～49名
4．50～99名
5．100～299名
6．300～999名
7．1,000名以上
8．わからない、回答しない

Q4　［Q1で1～5を選択した回答者のみ］
あなたが所属している部署の行っている事業における情報技術やそれを用いた機器の状況として、最も近いものを１つ選択してください。

回答欄

1．ほとんど（90%以上）の従業員が、情報技術やそれを用いた機器を活用して業務を行っている
2．半数以上（50～89%）の従業員が、情報技術やそれを用いた機器を活用して業務を行っている
3．一部の従業員(10～49%)が、情報技術やそれを用いた機器を活用して業務を行っている
4．情報技術やそれを用いた機器を活用して業務を行っている従業員はごくわずかである(10%未満)
5．わからない、回答しない

Q5　［Q1で1～5を選択した回答者のみ］
あなたが所属している部署の行っている事業における情報機器やそのセキュリティ対策の管理状況として、最も近いものを１つ選択してください。

回答欄

1．管理の方法や手順が規定されておらず、利用者に任されていたり、場当たり的な対応にとどまっていたりする
2．管理の方法や手順が規定されているが、過去に作られたものを改定せずにそのまま使っているなど、改善のための継続的な見直しを行っていない
3．管理の方法や手順を規定するとともに、PDCAマネジメントサイクルを通じて定期的に内容の見直しを行うなどして改善が図られている
4．3.の取組に加えて、情報セキュリティに関するインシデントや障害による損害等を定量的に評価し、その結果をもとに適切な対策とするような取組が行われている
5．わからない、回答しない

【ご所属の部署について】

Q6　［Q1で1～5を選択した回答者のみ］
あなたが所属している部署の主たる業務内容について、次の中から最も近いものを１つ選択してください。
※Q1で公務員を選択した方で、ご所属の部署の業務が選択肢2～21に相当する場合は、22でなく2～21を選択してください。

回答欄

＜経営＞
1．組織経営（代表者、取締役、執行役員、相談役等）

＜スタッフ(間接部門)＞
2. 経営企画、事業企画
3. 人事
4. 総務、経理、調達、購買
5. 法務、コンプライアンス
6. リスクマネジメント
7. 品質管理
8. 内部監査
9. 研究
10. 社内教育、研修
11. 自組織向け情報システム関連
12. 上記以外のスタッフ系業務

＜事業遂行(直接部門)＞
13. 企画、調査・マーケティング
14. 営業
15. 製造
16. 流通
17. 卸売・小売
18. コンサルティング、診断、監査
19. ITシステム・サービス関連
20. 研究
21. 教育、研修
22. 公務(13～21以外)
23. その他サービス
24. 上記以外の事業

＜その他＞
25. 上記のいずれにもあてはまらない
26. わからない、回答しない

Q7-1　［Q6で2～12を選択した回答者のみ］
あなたが所属している部署は、情報セキュリティ対策にどのような形で関わっていますか。最も近いものを１つ選択してください。

回答欄

1．自企業・団体やグループの情報セキュリティ対策を主たる担当業務とする部署である
2．自企業・団体やグループの情報セキュリティ対策を担当業務の一部に含む部署である
3．情報セキュリティ対策に関わらない部署である
4．わからない、回答しない

Q7-2　［Q6で13～24を選択した回答者のみ］
あなたが所属している部署は、情報セキュリティ対策にどのような形で関わっていますか。最も近いものを１つ選択してください。

回答欄

1．情報セキュリティ対策サービス提供や関連製品販売等の外部向け事業を主たる担当業務とする部署である
2．情報セキュリティ対策サービス提供や関連製品販売等の外部向け事業を担当業務の一部に含む部署である
3．情報セキュリティ対策の外部向け事業には関わらない部署である
4．わからない、回答しない

Q7-3　［Q1で1～3を選択した回答者のみ］
あなたの役職として、最も近いものを１つ選択してください。なお、部下がいるかどうかは問いません。

回答欄

1．取締役・役員クラス
2．部長クラス
3．課長・マネージャークラス
4．係長・主任クラス
5．一般社員クラス
6．その他
7．回答しない

「6. その他」を選択した場合は、下記に役職を記入してください。

【あなたの担当業務について（IT関連）】

Q8　［Q1で1～5を選択した回答者のみ］

あなたの担当業務では、どのようなITシステム・サービスにどのように関わっていますか？関わりをすべて選択してください。

回答欄

- ☐ 1．自企業・団体の内部向けITシステム・サービス※の企画・構築・管理などに関わっている
  （※内部向けITとは、いわゆる「コーポレートIT」の分野で、人事、経理システム等の社内システムを指す）
- ☐ 2．自企業・団体の外部向けITシステム・サービス※の企画・構築・管理などに関わっている
  （※外部向けITとは、いわゆる「ビジネスIT」の分野で、オンラインショッピングサイト等の対外システムを指す）
- ☐ 3．顧客が使うITシステム・サービスの企画・開発・構築・運用・監査などを請け負っている（例：ベンダとしてのシステムの受託開発）
- ☐ 4．ITシステム・サービスの動向調査、研究、教育、ガイドライン等の制定に関わっている
- ☐ 5．ITシステム・サービスには関わっていない
- ☐ 6．わからない、回答しない

Q9　［Q8で1～4を選択した回答者のみ］

以下のITシステム・サービスに関連する業務のうち、あなたが担当している役割として、以下の②～④の中から最も近いものをそれぞれ1つ選択してください。なお、担当していない業務については①を選択して下さい。

業務内容	回答欄（プルダウンメニューから選択）
1．システム企画・開発・構築・テスト（コンサルティングを含む）	
2．システム管理・運用・サポート	
3．外部委託・調達	
4．システム監査	
5．マーケティング・営業	
6．製品・サービスの企画・開発・構築	
7．動向調査、研究、教育、ガイドライン等の制定	
8．その他の業務	

＜プルダウンメニューの選択肢＞

① 担当していない
② 責任者・管理者（実務より管理業務が主体）
③ 主導的な実務者（責任者を兼ねる場合も含む）
④ 補佐的な実務者
⑤ 回答しない

「8. その他の業務」で②～⑤を選択した場合は、下記に具体的に記入してください。

複数選択した方は、上記のうち主たる業務を1つ選択してください（番号を選択）：

Q10　［Q9で②～④を1つ以上選択した回答者のみ］

Q9でご回答いただいたITシステム・サービスに関連する業務に関して、業務を行う上で必要な知識・スキルの上位５つまでを業務ごとに選択してください。なお、知識・スキルのレベルは問いません。

		ITシステム・サービスに関連する業務							
		1 システム企画・開発・構築・テスト（コンサルティングを含む）	2 システム管理・運用・サポート	3 外部委託・調達	4 システム監査	5 マーケティング・営業	6 製品・サービスの企画・開発・構築	7 動向調査、研究、教育、ガイドライン等の制定	8 その他の業務
必要な知識・スキル	① アプリケーション／サービスに関するもの（業種固有のアプリケーション、ウェブ、グループウェア、オフィスアプリ、会計アプリ、SaaS、開発技術　など）	□	□	□	□	□	□	□	□
	② システム基盤／ハードウェアに関するもの（システムのアーキテクチャ、OS、仮想環境、IaaS・PaaS等のクラウドサービス、IoT　など）	□	□	□	□	□	□	□	□
	③ 情報セキュリティ技術・情報セキュリティ対策の運用・マネジメントに関するもの	□	□	□	□	□	□	□	□
	④ 先端技術に関するもの（AI、データサイエンス、ブロックチェーン　など）	□	□	□	□	□	□	□	□
	⑤ 開発や運用の管理に関するもの（プロジェクトマネジメント、サービスマネジメント、アジャイル手法　など）	□	□	□	□	□	□	□	□
	⑥ 事業戦略に関するもの（経営、リスクマネジメント、財務、設備投資、設備管理、人材戦略など）	□	□	□	□	□	□	□	□
	⑦ 倫理、コンプライアンス、法律やガイドライン、標準、規格等に関するもの	□	□	□	□	□	□	□	□
	⑧ 人間力に関するもの（コミュニケーション、意識共有、人を動かす行動力　など）	□	□	□	□	□	□	□	□
	⑨ その他の知識・スキル	□	□	□	□	□	□	□	□
	⑩ 上記①～⑨のいずれの知識も必要としない	□	□	□	□	□	□	□	□
	⑪ わからない、回答しない	□	□	□	□	□	□	□	□

「⑨その他の知識・スキル」を選択した方は、具体的内容をご記入ください。

【あなたの担当業務について（サイバーセキュリティ対策関連）】

Q11　［Q1で1～5を選択した回答者のみ］

あなたは自企業・団体のCSIRTメンバーですか？　次の中から最も近いものをそれぞれ１つ選択してください。

回答欄

1．CSIRTまたはCSIRTの役割を担うチームの責任者である
2．CSIRTまたはCSIRTの役割を担うチームのメンバーである
3．いずれでもない
4．回答しない

Q12　［Q1で1～5を選択した回答者のみ］

以下のサイバーセキュリティ対策に関連する業務のうち、あなたが担当している役割として、以下の②～④の中から最も近いものをそれぞれ1つ選択してください。なお、担当していない業務については①を選択して下さい。

※Q8でITシステム・サービスに関わると回答した方は、自分の関わるITシステム・サービスのサイバーセキュリティ対策に関する担当業務を含めてください。

業務内容	回答欄（プルダウンメニューから選択）
1．サイバーセキュリティに関する経営判断	
2．サイバーセキュリティ管理体制の構築（コンサルティングを含む）	
3．サイバーセキュリティ管理体制のマネジメント（コンサルティングを含む）	
4．セキュア設計・開発・構築・評価（コンサルティングを含む）	
5．ITシステム・サービスのセキュリティ面での運用・管理（外部委託・調達等を含む）	
6．サイバーセキュリティ対策機器の運用・保守	
7．監視・情報収集	
8．脆弱性診断、情報セキュリティ監査	
9．インシデント対応（コンサルティングを含む）	
10．セキュリティ技術及びサイバーセキュリティ対策に関する調査・研究	
11．サイバーセキュリティに関する教育・人材育成	
12．その他の業務	

＜プルダウンメニューの選択肢＞

① 担当していない
② 責任者・管理者（実務より管理業務が主体）
③ 主導的な実務者（責任者を兼ねる場合も含む）
④ 補佐的な実務者
⑤ 回答しない

「12. その他の業務」で②～⑤を選択した場合は、下記に具体的に記入してください。

複数選択した方は、上記のうち主たる業務を1つ選択してください（番号を選択）：

Q13　［Q12で②～④を1つ以上選択した回答者のみ］

Q12で回答いただいたサイバーセキュリティ対策に関する業務に関して、業務を行う上で必要な知識・スキルの上位５つまでを選択してください。なお、知識・スキルのレベルは問いません。

			サイバーセキュリティ対策に関連する業務											
			1 サイバーセキュリティに関する経営判断	2 サイバーセキュリティ管理体制の構築（コンサルティングを含む）	3 サイバーセキュリティ管理体制のマネジメント（コンサルティングを含む）	4 セキュア設計・開発・構築・評価（コンサルティングを含む）	5 ITシステム・サービスのセキュリティ面での運用・管理（外部委託・調達等を含む）	6 サイバーセキュリティ対策機器の運用・保守	7 監視・情報収集	8 脆弱性診断、情報セキュリティ監査	9 インシデント対応（コンサルティングを含む）	10 セキュリティ技術及びサイバーセキュリティ対策に関する調査・研究	11 サイバーセキュリティに関する教育・人材育成	12 その他の業務
必要な知識・スキル	情報セキュリティ分野	① 最新の脅威に関するもの（脆弱性、マルウェアなどの攻撃手法、攻撃主体など）	□	□	□	□	□	□	□	□	□	□	□	□
		② 情報セキュリティ技術に関するもの（暗号や認証、電子署名、情報理論など）	□	□	□	□	□	□	□	□	□	□	□	□
		③ 情報セキュリティ対策の運用に関するもの（対策のオペレーション、監視、インシデントレスポンス　など）	□	□	□	□	□	□	□	□	□	□	□	□
		④ 情報セキュリティマネジメントに関するもの（情報セキュリティポリシー、情報セキュリティガバナンス、情報セキュリティ監査　など）	□	□	□	□	□	□	□	□	□	□	□	□
		⑤ 情報セキュリティ機能の設計・実装に関するもの（セキュリティ要件定義、設計、実装、テスト、評価　など）	□	□	□	□	□	□	□	□	□	□	□	□
	ＩＴ関連ほか全般	⑥ アプリケーション／サービスに関するもの（業種、ウェブ、グループウェア、オフィスアプリ、会計アプリ、SaaS、開発技術　など）	□	□	□	□	□	□	□	□	□	□	□	□
		⑦ システム基盤／ハードウェアに関するもの（システムのアーキテクチャ、OS、仮想環境、IaaS・PaaS等のクラウドサービス、IoT　など）	□	□	□	□	□	□	□	□	□	□	□	□
		⑧ 先端技術に関するもの（AI、データサイエンス、ブロックチェーン　など）	□	□	□	□	□	□	□	□	□	□	□	□
		⑨ 開発や運用の管理に関するもの（プロジェクトマネジメント、サービスマネジメント、アジャイル手法　など）	□	□	□	□	□	□	□	□	□	□	□	□
		⑩ 事業戦略に関するもの（経営、リスクマネジメント、財務、設備投資、設備管理、人材戦略など）	□	□	□	□	□	□	□	□	□	□	□	□
		⑪ 倫理、コンプライアンス、法律やガイドライン、標準、規格等に関するもの	□	□	□	□	□	□	□	□	□	□	□	□
		⑫ 人間力に関するもの（コミュニケーション、意識共有、人を動かす行動力　など）	□	□	□	□	□	□	□	□	□	□	□	□
	その他	⑬ 上記①～⑫のいずれの知識も必要としない	□	□	□	□	□	□	□	□	□	□	□	□
		⑭ わからない、回答しない	□	□	□	□	□	□	□	□	□	□	□	□

Q14　［Q12で②～④を1つ以上選択した回答者のみ］
あなたは、サイバーセキュリティ対策に関して担当している業務を、どの程度難しいものと考えていますか。Q12で選択いただいた業務それぞれについて、①～⑥のうち、最も近いものを１つ選択してください。

業務内容	回答欄（プルダウンメニューから選択）
1．　サイバーセキュリティに関する経営判断	
2．　サイバーセキュリティ管理体制の構築（コンサルティングを含む）	
3．　サイバーセキュリティ管理体制のマネジメント（コンサルティングを含む）	
4．　セキュア設計・開発・構築・評価（コンサルティングを含む）	
5．　ITシステム・サービスのセキュリティ面での運用・管理（外部委託・調達等を含む）	
6．　サイバーセキュリティ対策機器の運用・保守	
7．　監視・情報収集	
8．　脆弱性診断、情報セキュリティ監査	
9．　インシデント対応（コンサルティングを含む）	
10．　セキュリティ技術及びサイバーセキュリティ対策に関する調査・研究	
11．　サイバーセキュリティに関する教育・人材育成	
12．　その他の業務	

＜プルダウンメニューの選択肢＞
① つねに難しいと感じる
② しばしば難しいと感じる
③ たまに難しいと感じるときがある
④ まったく難しさを感じない
⑤ なんともいえない
⑥ 回答しない

Q15　［Q14で①～③を1つ以上選択した回答者のみ］
最も難易度が高いと感じている業務について、そのように感じる要因として考えられるものを<u>すべて</u>選択してください。

回答欄	
□	1．　自分の知識・スキル・経験の不足
□	2．　業務上連携する相手とのコミュニケーションが難しい
□	3．　要員不足や規定の不備など体制の問題
□	4．　業務で直面する課題そのものが難しい
□	5．　その他
□	6．　回答しない

「5. その他」を選択した場合は、下記に具体的に記入してください。

Q16　［Q12で②～④を1つ以上選択した回答者のみ］
あなたが今後強化したいと思う必要な知識・スキルをすべて選択してください。

		回答欄
情報セキュリティ分野	① 最新の脅威に関するもの（脆弱性、マルウェアなどの攻撃手法、攻撃主体など）	☐
	② 情報セキュリティ技術に関するもの（暗号や認証、電子署名、情報理論など）	☐
	③ 情報セキュリティ対策の運用に関するもの（対策のオペレーション、監視、インシデントレスポンス　など）	☐
	④ 情報セキュリティマネジメントに関するもの（情報セキュリティポリシー、情報セキュリティガバナンス、情報セキュリティ監査　など）	☐
	⑤ 情報セキュリティ機能の設計・実装に関するもの（セキュリティ要件定義、設計、実装、テスト、評価　など）	☐
IT関連ほか全般	⑥ アプリケーション／サービスに関するもの（業種、ウェブ、グループウェア、オフィスアプリ、会計アプリ、SaaS、開発技術　など）	☐
	⑦ システム基盤／ハードウェアに関するもの（システムのアーキテクチャ、OS、仮想環境、IaaS・PaaS等のクラウドサービス、IoT　など）	☐
	⑧ 先端技術に関するもの（AI、データサイエンス、ブロックチェーン　など）	☐
	⑨ 開発や運用の管理に関するもの（プロジェクトマネジメント、サービスマネジメント、アジャイル手法　など）	☐
	⑩ 事業戦略に関するもの（経営、リスクマネジメント、財務、設備投資、設備管理、人材戦略など）	☐
	⑪ 倫理、コンプライアンス、法律やガイドライン、標準、規格等に関するもの	☐
	⑫ 人間力に関するもの（コミュニケーション、意識共有、人を動かす行動力　など）	☐
その他	⑬ その他	☐
	⑭ 強化したいと思う知識・スキルはない	☐
	⑮ 回答しない	☐

「⑬その他」を選択した場合は、下記に具体的に記入してください。

Q17　［Q16で⑭以外を選択した回答者のみ］
あなたが現在実施している、知識・スキル向上のための取組をすべて選択してください。

回答欄

- ☐ 1．実践を通じたOJT（On the Job Training）
- ☐ 2．社外の有償のセミナー、講座（eラーニングを含む）、大学・大学院等の受講
- ☐ 3．社外の無償のセミナー、講座等（MOOC*を含む）の受講
  * MOOC：無償で受講できるオープンな講座（Massive Open Online Courses）のこと
- ☐ 4．社内セミナー、社内向けeラーニング等の受講
- ☐ 5．社外の勉強会（コミュニティ活動を含む）の開催、参加
- ☐ 6．書籍、雑誌、公開のウェブサイト等を用いた独学
- ☐ 7．その他
- ☐ 8．回答しない

「7. その他」を選択した場合は、下記に具体的に記入してください。

【あなたのサイバーセキュリティ対策関連業務における連携について】

Q18　［Q12で②～④を1つ以上選択した回答者のみ］

あなたが所属する企業・団体の内部で、業務を通じて情報セキュリティ対策に関するコミュニケーション（会合での議論、依頼、情報提供、相談への対応等）を行う相手をすべて選択してください。

※月1回以上のコミュニケーションがある相手をすべて選択してください。
※間接的に情報セキュリティ対策に影響するもの（例：新技術を用いた製品の導入の相談）を含みます。
※担当者同士が能動的にコミュニケーションを行うものに限定し、定期的な社内報の配信等は含めないでください。
※ご自身がコミュニケーション相手に相当する場合や、自部署内の担当者の場合は選択しないでください。

		サイバーセキュリティ対策に関連する業務											
		1 サイバーセキュリティに関する経営判断	2 サイバーセキュリティ管理体制の構築（コンサルティングを含む）	3 サイバーセキュリティ管理体制のマネジメント（コンサルティングを含む）	4 セキュア設計・開発・構築・評価（コンサルティングを含む）	5 ITシステム・サービスのセキュリティ面での運用・管理	6 サイバーセキュリティ対策機器の運用・保守	7 監視・情報収集	8 脆弱性診断、情報セキュリティ監査	9 インシデント対応（コンサルティングを含む）	10 セキュリティ技術及びサイバーセキュリティ対策に関する調査・研究	11 サイバーセキュリティに関する教育・人材育成	12 その他の業務
社内のコミュニケーション相手	① 経営層（代表者、取締役、執行役員、CIO、CISO、相談役等）	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	② 企画・人事・総務・経理・調達・購買等の部署の担当者	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	③ 法務・コンプライアンスの担当者	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	④ 情報セキュリティマネジメント、CSIRT、情報セキュリティ統括の担当者	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	⑤ リスクマネジメントの担当者	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	⑥ 品質管理の担当者	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	⑦ 監査の担当者	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	⑧ 研究所所属の担当者	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	⑨ 教育・研修の担当者	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	⑩ 情報システム関連部署の担当者	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	⑪ 事業部門の担当者	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	⑫ ①～⑪以外の担当者	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	⑬ 社内にはコミュニケーション相手が存在しない	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	⑭ 回答しない	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

「⑫ ①～⑪以外の担当者」を選択した場合は、下記に具体的に記入してください。

Q19　［Q12で②～④を1つ以上選択した回答者のみ］

あなたが所属する企業・団体の外部で、情報セキュリティ対策に関するコミュニケーション（受発注、契約、相談、調整、意見交換等）を行う相手をすべて選択してください。

※月1回以上のコミュニケーションがある相手をすべて選択してください。
※コミュニケーションには、間接的に情報セキュリティ対策に影響するもの（例：新技術を用いた製品の導入の相談）を含みます。
※担当者同士が能動的にコミュニケーションを行うものに限定し、定期的なマルウェア警戒情報の配信等は含みません。

		サイバーセキュリティ対策に関連する業務											
		1 サイバーセキュリティに関する経営判断	2 サイバーセキュリティ管理体制の構築（コンサルティングを含む）	3 サイバーセキュリティ管理体制のマネジメント（コンサルティングを含む）	4 セキュア設計・開発・構築・評価（コンサルティングを含む）	5 ITシステム・サービスのセキュリティ面での運用・管理	6 サイバーセキュリティ対策機器の運用・保守	7 監視・情報収集	8 脆弱性診断、情報セキュリティ監査	9 インシデント対応（コンサルティングを含む）	10 セキュリティ技術及びサイバーセキュリティ対策に関する調査・研究	11 サイバーセキュリティに関する教育・人材育成	12 その他の業務
社外のコミュニケーション相手	① 顧客（BtoC事業の顧客を除く）・業務委託元（親会社を除く）	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	② 親会社	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	③ 子会社、グループ企業	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	④ 業務委託先（セキュリティサービスのベンダを除く）	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	⑤ セキュリティサービスのベンダ	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	⑥ 製品ベンダ、販売店	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	⑦ 監督官庁、自治体窓口	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	⑧ 共同研究やコンソーシアムのパートナー（企業、大学など）	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	⑨ ①～⑧以外の方	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	⑩ 社外にはコミュニケーション相手が存在しない	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
	⑪ 回答しない	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

「⑨ ①～⑧以外の担当者」を選択した場合は、下記に具体的に記入してください。

Q20-1　［Q12で②～④を1つ以上選択した回答者のみ］
Q18とQ19で選択した、業務でコミュニケーションをとる相手のうち、頻繁（概ね2～3日に1回以上）にコミュニケーションをとる相手をすべて選択してください。

社内のコミュニケーション相手	1. 経営層（代表者、取締役、執行役員、相談役）	☐
	2. 企画・人事・総務・経理・調達・購買等の部署の担当者	☐
	3. 法務・コンプライアンスの担当者	☐
	4. 情報セキュリティマネジメント、CSIRT、情報セキュリティ統括の担当者	☐
	5. リスクマネジメントの担当者	☐
	6. 品質管理の担当者	☐
	7. 監査の担当者	☐
	8. 研究所所属の担当者	☐
	9. 教育・研修の担当者	☐
	10. 情報システム関連部署の担当者	☐
	11. 事業部門の担当者	☐
	12. 1～11以外の担当者	☐
社外のコミュニケーション相手	13. 顧客（BtoC事業の顧客を除く）・業務委託元（親会社を除く）	☐
	14. 親会社	☐
	15. 子会社、グループ企業	☐
	16. 業務委託先（セキュリティサービスのベンダを除く）	☐
	17. セキュリティサービスのベンダ	☐
	18. 製品ベンダ、販売店	☐
	19. 監督官庁、自治体窓口	☐
	20. 共同研究やコンソーシアムのパートナー（企業、大学など）	☐
	21. 13～20以外の方	☐
頻繁にコミュニケーションをとる相手は存在しない		☐
回答しない		☐

Q20-2　［Q12で②～④を1つ以上選択した回答者のみ］
Q18とQ19で選択した、業務でコミュニケーションをとる相手に求めるサイバーセキュリティの知識・スキルのレベルとして、理想と考えるものを①～⑤から、現状を⑥～⑩から、それぞれ相手毎に１つ選択してください。

		理想と考える相手の知識･スキル回答欄	実態の相手の知識･スキル回答欄
社内のコミュニケーション相手	1. 経営層（代表者、取締役、執行役員、相談役）		
	2. 企画･人事･総務･経理･調達･購買等の部署の担当者		
	3. 法務･コンプライアンスの担当者		
	4. 情報セキュリティマネジメント、CSIRT、情報セキュリティ統括の担当者		
	5. リスクマネジメントの担当者		
	6. 品質管理の担当者		
	7. 監査の担当者		
	8. 研究所所属の担当者		
	9. 教育･研修の担当者		
	10. 情報システム関連部署の担当者		
	11. 事業部門の担当者		
	12. 1～11以外の担当者		
社外のコミュニケーション相手	13. 顧客（BtoC事業の顧客を除く）･業務委託元（親会社を除く）		
	14. 親会社		
	15. 子会社、グループ企業		
	16. 業務委託先（セキュリティサービスのベンダを除く）		
	17. セキュリティサービスのベンダ		
	18. 製品ベンダ、販売店		
	19. 監督官庁、自治体窓口		
	20. 共同研究やコンソーシアムのパートナー（企業、大学など）		
	21. 13～20以外の方		

＜理想と考える相手の知識・スキルの選択肢＞
① 情報処理安全確保支援士試験レベル※
② 情報セキュリティマネジメント試験レベル※
③ ITパスポート試験レベル※
④ サイバーセキュリティの知識･スキルは求めない
⑤ わからない、回答しない

＜現状の相手の知識・スキルの選択肢＞
⑥ 情報処理安全確保支援士試験レベル※
⑦ 情報セキュリティマネジメント試験レベル※
⑧ ITパスポート試験レベル※
⑨ サイバーセキュリティの知識･スキルを持っていない
⑩ わからない、回答しない

※各試験の合格者に相当する知識・スキルのレベルについては、次の資料をご覧ください。
ITパスポート試験のレベルについて： https://www.jitec.ipa.go.jp/1_11seido/ip.html
情報セキュリティマネジメント試験のレベルについて： https://www.jitec.ipa.go.jp/1_11seido/sg.html
情報処理安全確保支援士試験のレベルについて： https://www.jitec.ipa.go.jp/1_11seido/sc.html

Q21　［Q12で②～④を1つ以上選択した回答者のみ］

あなたが経験したサイバーセキュリティ対策に関わる業務遂行の中で、印象に残った事例・ことがら（過去に苦労したこと、うまくいったこと、困ったこと、嬉しかったこと等）があれば挙げてください。軽微なものでもかまいません。

※ここで記載いただいた内容は、個人や組織を特定できるような形で公表することはありません。

※特に記載することがなければ、空白のままでも構いません。

事例1：

印象に残った要因（例：厳重なセキュリティ対策を課せられている部署で業務効率が低迷）：

実施した内容（例：リスク分析を行い、その結果をもとに合理的な対策を提案）：

結果（例：事故発生を抑制しつつ業務効率化を実現）：

事例2：

印象に残った要因：

実施した内容：

結果：

事例3：

印象に残った要因：

実施した内容：

結果：

【情報処理安全確保支援士制度の活用について他】

Q22　あなたが情報処理安全確保支援士として登録した理由として、次の中から最も近いものを１つ選択してください。

回答欄

1．自分のキャリア形成に必要と考えた
2．対外的な自己アピールに有用と考えた
3．講習を通じて専門知識の維持向上ができると考えた
4．所属している企業・団体において登録へのインセンティブ（報奨金等）があった
5．所属している企業・団体において登録するように指示された
6．将来再受験するのを避けたいと考えた
7．その他
8．わからない、回答しない

「7. その他」を選択した場合は、下記に具体的に記入してください。

Q23　登録やこれまで受講した講習の費用を誰が負担していますか？　次の中から最も近いものを１つ選択してください。
※以前所属していた企業・団体が負担した場合も、「所属している企業・団体」とみなしてご回答ください。
※まだ講習を受講しておらず、誰が負担するか不明の場合は推定で回答していただいて結構です。

回答欄

1．登録費用・講習費用とも、所属している企業・団体が負担した
2．登録費用のみ所属している企業・団体が負担し、講習費用は自分で負担した
3．登録費用のみ自分で負担し、講習費用は所属している企業・団体が負担した
4．登録費用・講習費用とも、自分で負担した
5．その他
6．回答しない

「5. その他」を選択した場合は、下記に具体的に記入してください。

Q24　情報処理安全確保支援士への登録によって得られることのうち、あなたにとってメリットとなることをすべて選択してください。その上で、あなたにとって最も大きなメリットを1つ選択ください。なお、選択肢には現在実施されていないが、今後情報処理安全確保支援士を対象に実施される可能性のある施策を含めて挙げています。

回答欄

☐ 1．スキルアップができる
☐ 2．サイバーセキュリティ対策に関する最新動向を把握できる
☐ 3．活躍の場が広がる（IPAサイトでの公表による）
☐ 4．活躍の場が広がる（情報処理安全確保支援士を要件とする公的支援制度や入札要件などによる）
☐ 5．活躍の場が広がる（信頼を示すことによる）
☐ 6．人脈が広がる（集合講習やコミュニティ活動による）
☐ 7．社会貢献ができる
☐ 8．その他のメリット
☐ 9．特にメリットは感じない
☐ 10．回答しない

「8. その他のメリット」を選択した場合は、下記に具体的に記入してください。

複数選択した方は、最も大きなメリットを1つ選択してください（番号を選択）：

Q25- 情報処理安全確保支援士に登録したことで得られた具体的なメリットがこれまでにあれば、あてはまるものをすべて選択してください。

回答欄

- ☐ 1． 公募案件の要件を満たすことができ、入札できた
- ☐ 2． 自組織や顧客のIoT税制※申請など、公的支援制度活用をサポートできた
- ☐ 3． 提案書やホームページなどに、情報処理安全確保支援士の人数などを記載することで組織としての情報セキュリティ対応力をアピールできた
- ☐ 4． 名刺などに情報処理安全確保支援士であることを記載して、個人としての情報セキュリティ対応力をアピールできた
- ☐ 5． 転職や社内公募などで情報セキュリティ対応力をアピールできた
- ☐ 6． セキュリティベンダーとの会話がやりやすくなった
- ☐ 7． 集合講習で得られた人脈が業務に活かせた
- ☐ 8． オンライン講習や集合講習で得た知識が業務に活かせた
- ☐ 9． 所属組織におけるインセンティブ（報奨金など）が得られた
- ☐ 10． 監査人等他の資格取得において優遇された
- ☐ 11． その他のメリットがあった
- ☐ 12． メリットは特にない
- ☐ 13． 回答しない

※参考：コネクテッド・インダストリーズ税制（IoT税制）
http://www.meti.go.jp/policy/it_policy/data-katsuyo/iot-zeisei/iot-zeisei.html

「11. その他のメリットがあった」を選択した場合は、下記に具体的に記入してください。

Q25-2　あなたは今後、サイバーセキュリティの知識・スキルを活かして、どのように活躍していきたいですか。差し支えない範囲で結構ですので、担当したいサイバーセキュリティ業務とお立場のそれぞれについて、あてはまるものをすべて選択ください。

※本回答内容は、コミュニティ活動の促進や情報処理安全確保支援士向け情報配信のしくみの検討につながります。ぜひ積極的にご回答ください。

＜今後担当したい業務＞

回答欄	
☐	1．　サイバーセキュリティに関する経営判断
☐	2．　サイバーセキュリティ管理体制の構築（コンサルティングを含む）
☐	3．　サイバーセキュリティ管理体制のマネジメント（コンサルティングを含む）
☐	4．　セキュア設計・開発・構築・評価（コンサルティングを含む）
☐	5．　監視・情報収集
☐	6．　サイバーセキュリティ対策機器の運用・保守
☐	7．　ITシステム・サービスのセキュリティ面での運用・管理
☐	8．　脆弱性診断、情報セキュリティ監査
☐	9．　インシデント対応（コンサルティングを含む）
☐	10．　セキュリティ技術及びサイバーセキュリティ対策に関する調査・研究
☐	11．　サイバーセキュリティに関する教育・人材育成
☐	12．　その他のサイバーセキュリティ関連業務
☐	13．　サイバーセキュリティに関連しない業務
☐	14　　特に考えていない、わからない
☐	15．　回答しない

＜今後担当したい業務をどのような立場で行いたいか＞

回答欄	
☐	1．　ユーザ企業・団体（中堅・大企業規模）の立場で担当したい
☐	2．　ユーザ企業・団体（中堅・大企業規模）を支援するベンダーの立場で担当したい
☐	3．　ユーザ企業・団体（中小・ベンチャーほか）の立場で担当したい
☐	4．　ユーザ企業・団体（中小・ベンチャーほか）を支援するベンダーの立場で担当したい
☐	5．　1～4以外の立場（例：公務員、研究者等）で担当したい
☐	6．　特に考えていない、わからない
☐	7．　回答しない

Q26　本アンケート調査や、情報処理安全確保支援士検索サービス（*）についてのご意見がございましたら、下欄に記入してください。なお、本設問に対してご質問やご要望等をご記入いただいても、個別のご回答はできないことがありますので予めご了承ください。

＊ https://riss.ipa.go.jp/

Q27　本調査では、情報処理安全確保支援士本人への調査とあわせて、情報処理安全確保支援士が所属する組織の組織長（部長クラスの方を想定）を対象に、アンケート調査を実施する予定です（アンケート調査の詳細は別記をご参照ください）。
つきましては、Q6でお答えいただいたあなたの所属する部署の長をご紹介いただくことは可能でしょうか？　次の中であてはまるものを１つ選択してください。
※ご紹介いただいた場合は、アンケート回答依頼の電子メールをお送りしますが、そのアンケートへの回答は必須ではございません。

回答欄

１．紹介可能（後日、ご紹介依頼のご連絡をいたします）
２．紹介はできない
３．ご自身が部署の長である（後日、組織長へのアンケート依頼をお送りいたします）

【別記】組織長アンケートについて

IPAが実施する「サイバーセキュリティ対策に関わる人材の実態調査」の一環として、情報処理安全確保支援士が所属する組織等の組織長様を対象として、次の要領でアンケート調査を実施いたします。

◎アンケート調査実施要領

(1) 目的:　サイバーセキュリティ対策に関わる人材が所属する組織等における同人材の実態について、現場と経営を繋ぐ立場からの把握を行う。
(2) 時期:　2019年1月中旬～下旬を予定
(3) 対象者:　部長または事業部長クラスの方を想定しますが、組織によって役職名は異なりますので、以下の両方の要件を満たす方を想定してください。
・現場の業務内容をおおまかに把握している（サイバーセキュリティ対策に限定しません）。
・経営層を対象とした会議等への参加機会があるなど、経営層と直接コミュニケーションをする機会がある（自らが経営層に相当する方でもかまいません）。
(4) 調査内容: 次のような内容についてお尋ねする予定です（回答の所要時間は15分程度）。
・組織におけるITシステム・サービスに関する方針とサイバーセキュリティ対策の位置づけ
・サイバーセキュリティ対策の位置づけに関わる人材の確保・育成に関する方針
・サイバーセキュリティ対策の位置づけに関わる人材の保有すべき知識・スキル、資格等に関する認識
・情報処理安全確保支援士制度に関する認知及び考え方（メリット、効果、費用負担等）
(5) 調査方法: ウェブアンケートまたは調査票（電子ファイル形式）のうちご都合のよい方法でご回答いただきます。
(6) 調査結果: ご回答いただきました場合は、後日分析結果をご連絡させていただく予定です。

以上、お忙しいところご協力いただきありがとうございました。