

サイバーセキュリティおよび
プライバシー業界における
多様なキャリアパス
実態調査2024

目次

1. はじめに	p.2
2. 日米セキュリティ業界で働く専門家の「12の傾向」	p.4
(1) セキュリティ業界で働く日米専門家は「文系」出身者の割合が高い	p.6
(2) 転職経験者の前職は「IT・セキュリティベンダー」「製造業」「サービス業」「金融・保険業」の順で多い	p.9
(3) 転職・部門異動経験者の前所属部門は、文系出身専門家で「営業部門」、理系出身専門家で「情報セキュリティ部門」がトップ	p.11
(4) セキュリティ業界における女性の割合は、ゆるやかに増加傾向	p.12
(5) 文系出身専門家は「ガバナンス・マネジメント」業務、理系出身専門家は「エンジニアリング」業務に携わる傾向	p.13
(6) セキュリティ業界で実際に働いた印象は、「専門性を高められる業界」がトップ	p.15
(7) ロールモデルがいる日米専門家は7割。多くが「セキュリティ業務に満足」とポジティブな評価	p.18
(8) 専門家の考える「活躍の定義」は「時間内に効率よく高品質な成果を出せる」がトップ。一方、社内の期待は「管理職になる」がトップと乖離がみられる	p.20
(9) 「業務に有益」とする資格は「クラウドセキュリティ関連資格」が上位	p.22
(10) ロールモデルがいる日米専門家は「セキュリティ業界で長く働きたい」意向が8割	p.27
(11) 昇進意欲のある米国専門家は8割で日本専門家より多い	p.28
(12) セキュリティ関連CxOを目指すなら、最も有益とする経験は「IT・セキュリティ実務」と「コンサルティング」	p.32
3. 今後「セキュリティ業界」を目指す学生や転職者に向けたメッセージ	p.34
4. 国内大学における「セキュリティ教育者」のキャリアパス	p.41
5. おわりに	p.45
6. アンケート調査概要	p.47
Appendix. 回答者の属性とその他のデータ	p.49

1. はじめに



1. はじめに

皆さんは「セキュリティ業界で働くこと」を想像したことがあるでしょうか。

世界的に、DXやAI利活用などビジネスのデジタル化が浸透する中、高度化するサイバー脅威から情報資産や人権を保護するため、サイバーセキュリティやプライバシー（以下「セキュリティ」という）業界へのビジネス需要は一層高まっています。比例して専門家の需要も高まり、セキュリティ業界では、優秀でポテンシャルのある学生や他専門分野経験を持つ転職者を多く求めています。

一方で、セキュリティ業界は歴史が浅く、「どのような経歴を持つ者」が「どのように活躍」しているか見えづらいという声も多く聞かれます。そのような声を受け、PwCコンサルティング合同会社では、学生や転職活動者が「セキュリティ業界で働く自分」をより具体的に想像できるよう、2022年より、セキュリティ業界で働く専門家のキャリアパス調査を実施しています。2回目となる今回の業界動向調査では、日本だけでなく、同業界を牽引する米国のセキュリティ専門家も調査対象に加え、日米セキュリティ専門家600名（男性専門家：300名、女性専門家：300名）からアンケート調査の回答を得ました。

本調査が、皆さんにとってセキュリティ業界を目指すきっかけとなれば心より嬉しく思います。

2022年度調査の詳細は「[サイバーセキュリティおよびプライバシー業界で働く女性の実態調査2022](#)」
(以下、「初回業界調査」という)をご参照ください。

2.日米セキュリティ業界で働く 専門家の「12の傾向」



2. 日米セキュリティ業界で働く専門家の「12の傾向」

今回の調査では、日米セキュリティ業界で働く専門家の12の傾向を確認することができました(図表1)。なお、本調査では「対話と発展のための世界文化多様性デー¹」に合わせて、セキュリティ業界で働く専門家のキャリアパスを「日米」「男女」「最終学歴(文系または理系)」「転職経験有無」「ロールモデルの有無」など多様なグループ属性から傾向を分析しました。

図表1: 日米セキュリティ業界で働く専門家の「12の傾向」

1. セキュリティ業界で働く日米専門家は「文系」出身者の割合が高い
2. 転職経験者の前職は「IT・セキュリティベンダー」「製造業」「サービス業」「金融・保険業」の順で多い
3. 転職・部門異動経験者の前所属部門は、文系出身専門家で「営業部門」、理系出身専門家で「情報セキュリティ部門」がトップ
4. セキュリティ業界における女性の割合は、ゆるやかに増加傾向
5. 文系出身専門家は「ガバナンス・マネジメント」業務、理系出身専門家は「エンジニアリング」業務に携わる傾向
6. セキュリティ業界で実際に働いた印象は、「専門性を高められる業界」がトップ
7. ロールモデルがいる日米専門家は7割。多くが「セキュリティ業務に満足」とポジティブな評価
8. 専門家の考える「活躍の定義」は「時間内に効率よく高品質な成果を出せる」がトップ。一方、社内の期待は「管理職になる」がトップと乖離がみられる
9. 「業務に有益」とする資格は「クラウドセキュリティ関連資格」が上位
10. ロールモデルがいる日米専門家は「セキュリティ業界で長く働きたい」意向が8割
11. 昇進意欲のある米国専門家は8割で、日本専門家より多い
12. セキュリティ関連CxOを目指すなら、最も有益とする経験は「IT・セキュリティ実務」と「コンサルティング」



1. United Nations, "World Day for Cultural Diversity for Dialogue and Development, 21 May" <https://www.un.org/en/observances/cultural-diversity-day>

【日米セキュリティ業界で働く：「過去」の傾向】

「過去の傾向」において最も注目したいのは、セキュリティ専門家の最終学歴や前職の業種・所属部門について、日米で同じような傾向がみられたことです。

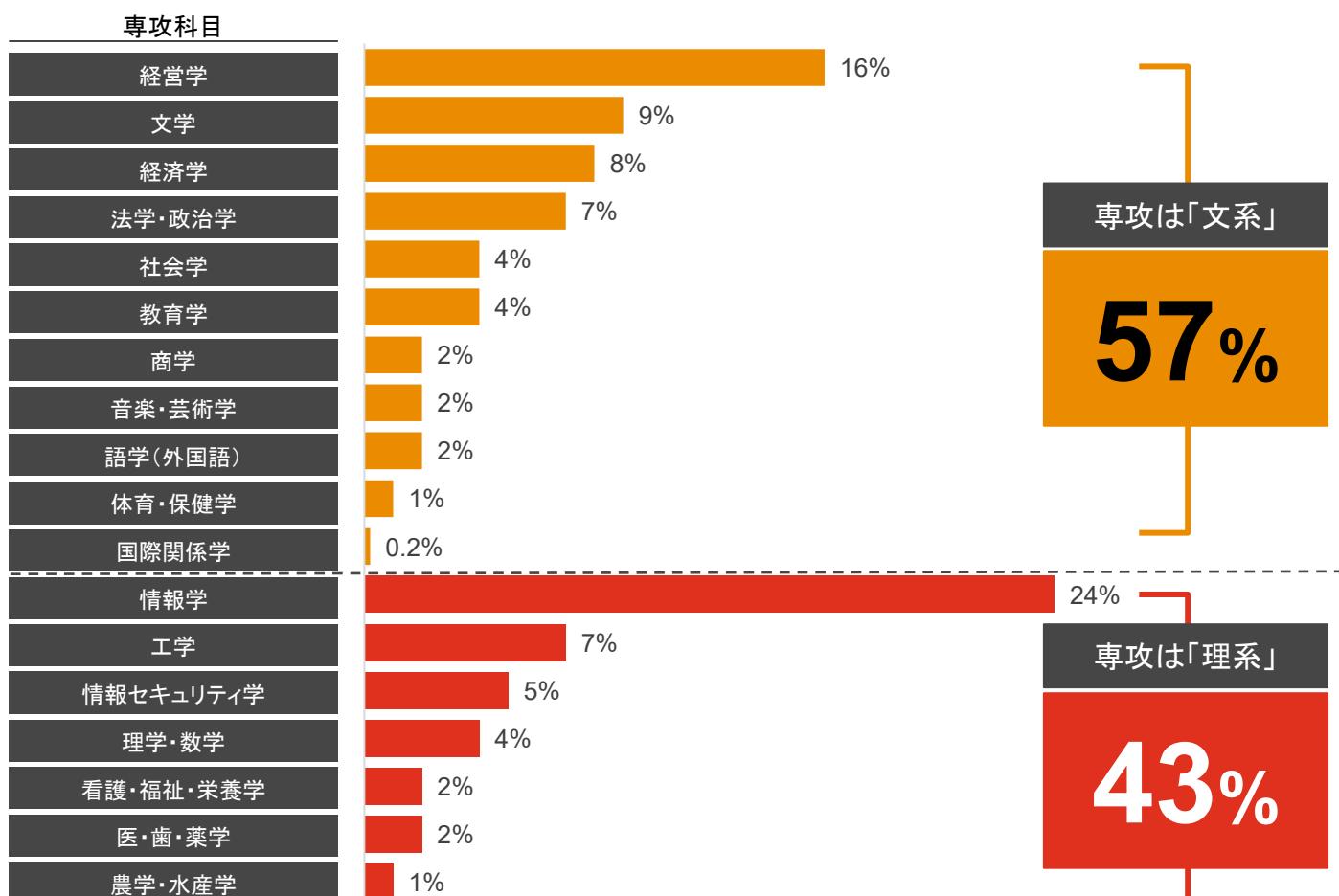
(1) セキュリティ業界で働く日米専門家は「文系」出身者の割合が高い

まず、最終学歴(大学・大学院)の専攻をみると、日米セキュリティ専門家(n=582)は「文系出身専門家」が約6割、「理系出身専門家」が約4割と、本業界で「文系出身専門家」がより多く活躍していることが分かります(図表2)。

具体的に文系出身専門家の専攻をみると、「経営学」が最も多く16%、次いで「文学」が9%、「経済学」が8%、「法学・政治学」が7%、「社会学」「教育学」がそれぞれ4%の順になりました。続いて理系出身専門家の専攻では、「情報学」を専攻した専門家が最も多く24%、次いで「工学」が7%、「情報セキュリティ学」が5%、「理学・数学」が4%の順となりました。

これらのことから、セキュリティ専門家としてのキャリアは文系・理系専攻者ともに開かれており、特に「情報学」「経営学」出身者が日米専門家として活躍していることが確認できました。

図表2: 日米セキュリティ業界で働く専門家の最終学歴の専攻(n=582)



Q. あなたの最終学歴における専攻分野を教えてください。

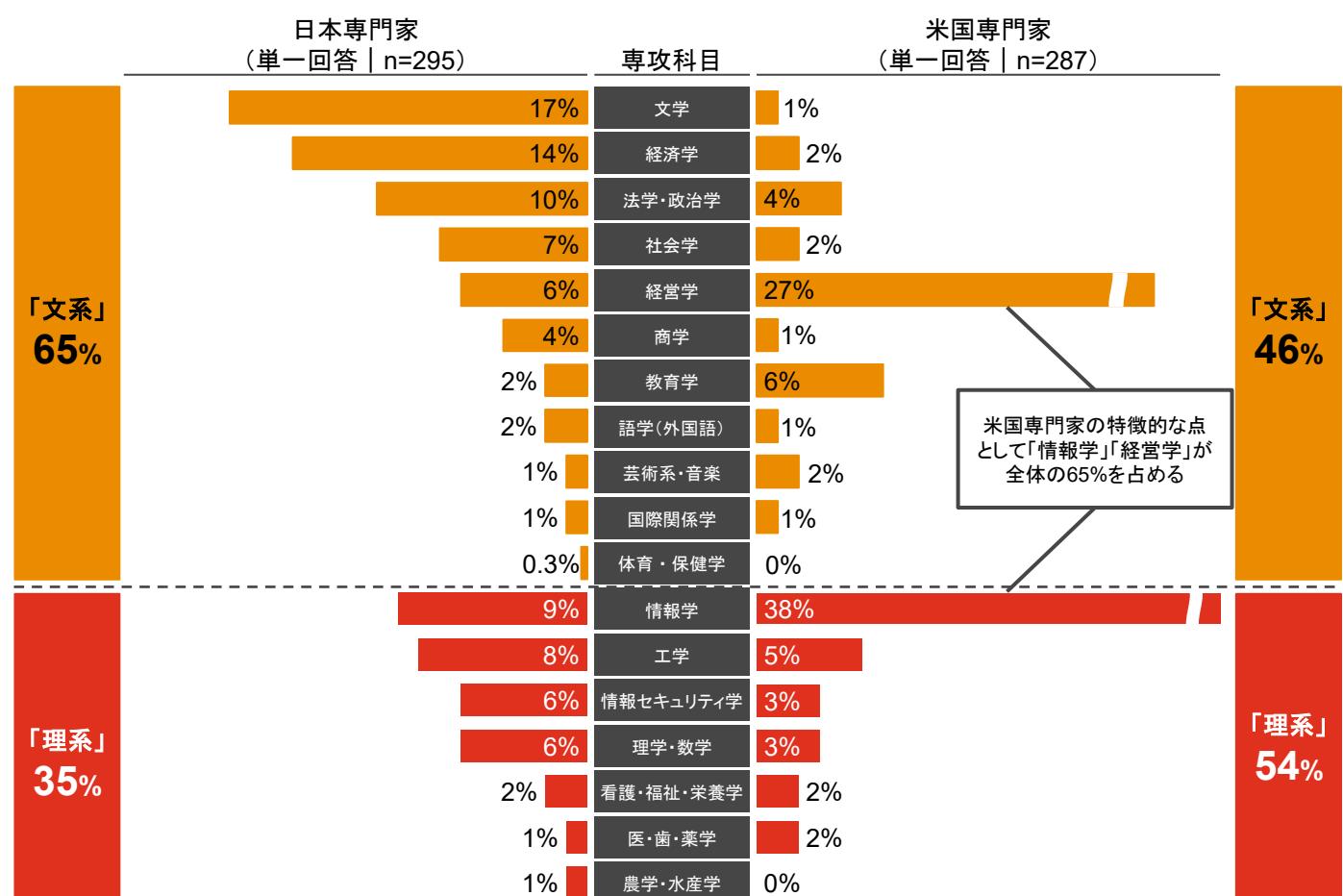
次に、日米専門家を国別に比較すると、日本専門家(n=295)では文系出身者が65%、理系出身者が35%と文系出身専門家が高い割合となったのに対し、米国専門家(n=287)では文系出身者が46%、理系出身専門家が54%と、ほぼ同じ割合となりました(図表3)。

具体的に各国の専攻科目の上位5科目をみると、日本専門家では、「文学」が最も多く17%、次いで「経済学」が14%、「法学・政治学」が10%、「情報学」が9%、「工学」が8%の順であり、上位3位の専攻が文系となりました。なお、2年前の初回業界調査と比較すると、「工学」の順位に変動あるものの、上位を占める専攻科目は同様の傾向にあり、2024年業界調査では文系出身専門家がより高い割合を占める結果となりました(初回業界調査:日本専門家では、「工学」が最も多く26%、次いで「文学」16%、「理学」13%、「経済学」12%、「法学・政治学」「社会学」それぞれ6%の順)。

続いて米国専門家における上位5科目の専攻科目をみると、「情報学」が最も多く38%、次いで「経営学」が27%、「教育学」が6%、「工学」が5%、「法学・政治学」が4%の順となりました。

これらのことから、最終学歴において日本専門家は幅広い専攻科目の履修者がセキュリティ業界へ参入するのに対し、米国専門家は「情報学(情報セキュリティ学含む)」や「経営学」など特定科目履修者が参画する傾向にあります。

図表3: 日米セキュリティ業界で働く専門家の最終学歴の専攻(日米比較 | n=582)



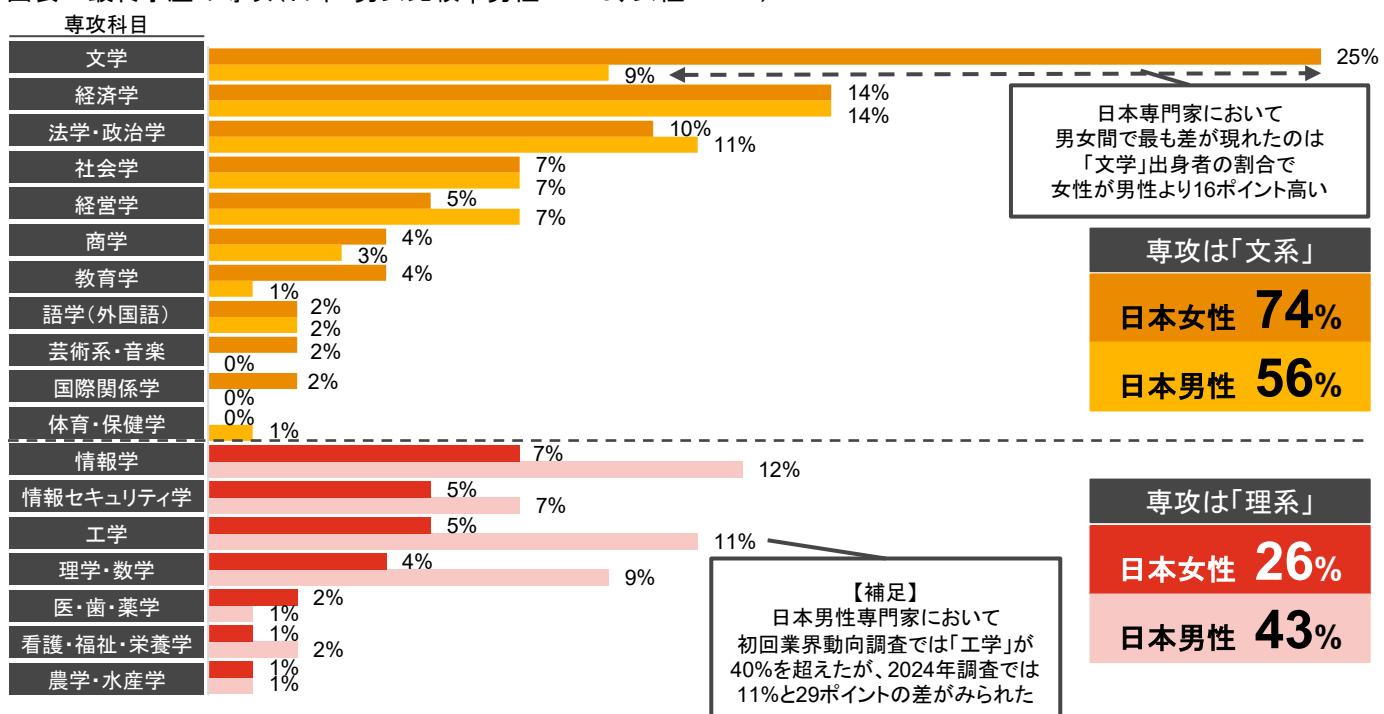
Q. あなたの最終学歴における専攻分野をお知らせください。

【補足】本調査において米国専門家の「体育・保健学」「農学・水産学」専攻者は確認できなかった

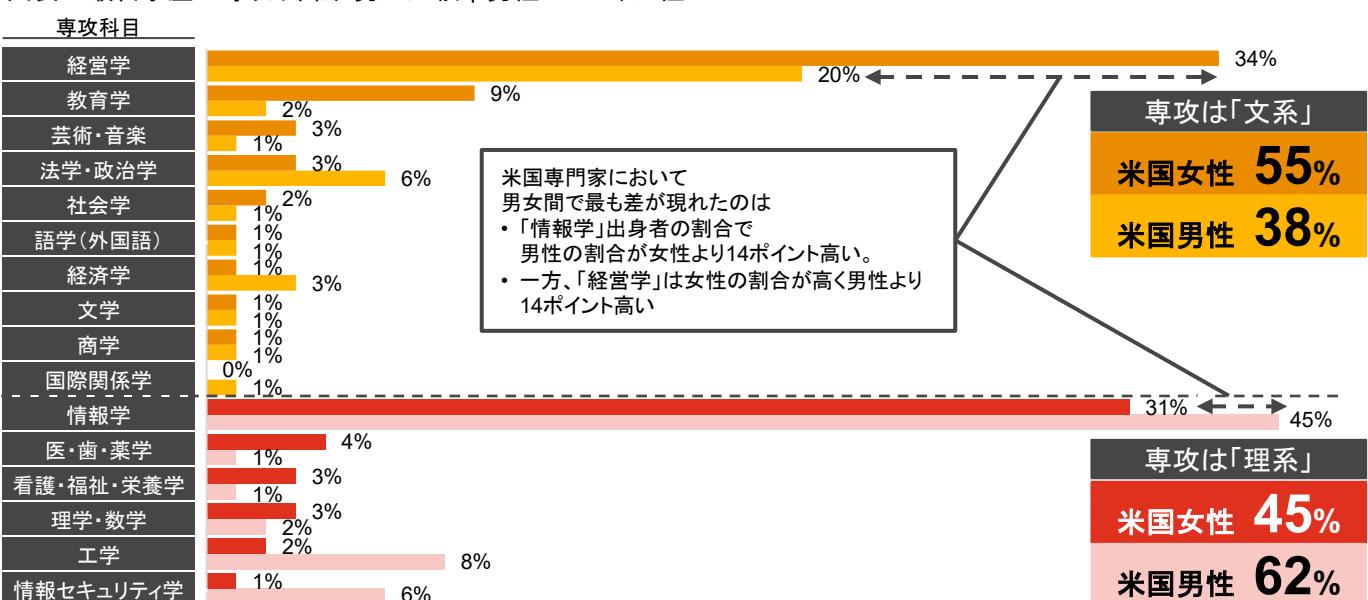
さらに、各国を男女別に比較すると、日本の女性専門家は「文系」出身の割合が74%と、他グループ（日本男性56%、米国女性55%、米国男性38%）よりも高いことが確認されました（図表4・図表5）。

男女の差が確認できた専攻科目は日米で異なります。まず日本の女性専門家（n=147）と男性専門家（n=148）間で最も差が確認できた専攻科目は「文学」で、女性専門家は16ポイントも高くなりました。また、米国では女性専門家（n=143）と男性専門家（n=144）間で最も差が確認できた専攻科目は「情報学」と「経営学」で、「情報学」は男性の割合が女性より14ポイント高く、「経営学」は女性の割合が男性より14ポイント高くなりました。

図表4：最終学歴の専攻（日本・男女比較 | 男性n=148、女性n=147）



図表5：最終学歴の専攻（米国・男女比較 | 男性n=144、女性n=143）



■(参考)セキュリティ業界へ就職する学生の傾向

今回の調査では、サイバーセキュリティ人材の育成を担う、日本のサイバーセキュリティ関連の教授・講師にセキュリティ業界を目指す学生の傾向について伺い、以下の回答を得ました。

図表6:セキュリティ業界へ就職する学生の傾向(インタビュー)

	セキュリティ業界を学ぶ学生の傾向	目指す職種の傾向
大学講師A	<ul style="list-style-type: none"> 身の回りでセキュリティ被害にあった人がいて興味を持つ学生 実際の事案から問題意識を持つ学生(警察官を目指している場合等) アニメやゲームが好きでセキュリティに興味を持つ学生 	<ul style="list-style-type: none"> マルウェア解析やフォレンジック・製品開発など 暗号関連の技術職 CSIRT(Computer Security Incident Response Team)
大学教授B	<ul style="list-style-type: none"> 生活の中でセキュリティに課題意識を持つ学生 仕事をする中で直面したセキュリティ上の課題への答えを見つけたい学生 企業から派遣されてセキュリティについて学ぶ学生 	<ul style="list-style-type: none"> 社会人学生においては現在の職種でのキャリアアップ
大学教授C	<ul style="list-style-type: none"> 数学系の学部出身者 電気系の学部出身者 	<ul style="list-style-type: none"> セキュリティコンサルティング AI、データサイエンス関連のセキュリティ
大学教授D	<ul style="list-style-type: none"> セキュリティに対して「かっこいい」「面白そう」「社会課題を解決できる」などのイメージを持つ学生 CTF等をきっかけにセキュリティ業界に興味を持つ学生 	<ul style="list-style-type: none"> 技術系職 上流工程・マネジメント コンサルティング

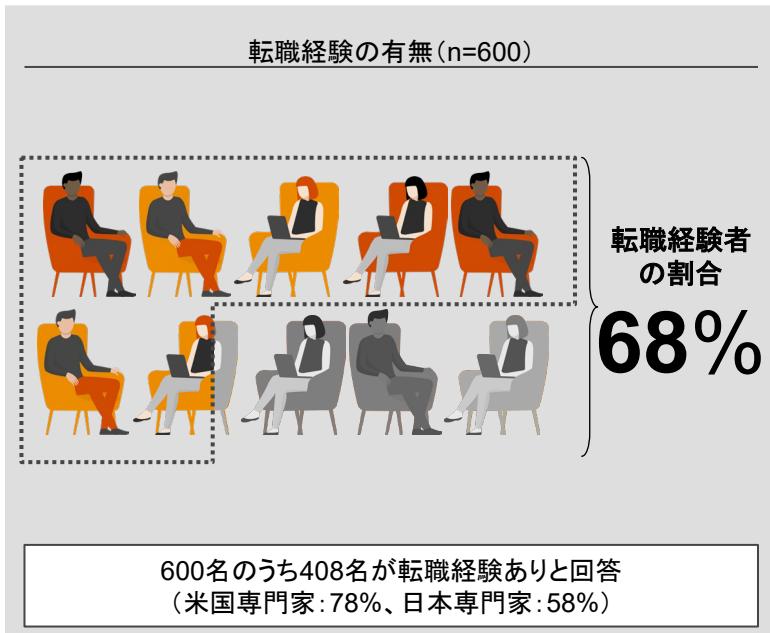
(2)転職経験者の前職は「IT・セキュリティベンダー」「製造業」「サービス業」「金融・保険業」の順で多い

続いて、転職や部署異動経験者をみていきます。

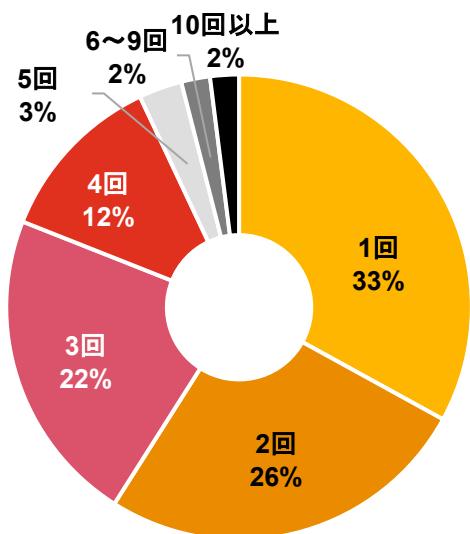
日米専門家(n=600)に転職経験を確認したところ、転職経験者は約7割を占めました(図表7)。とりわけ米国専門家の転職経験割合が78%と多く、日本専門家(58%)と比較し20ポイント多くなりました。また、転職経験を有する日米専門家(n=408)に転職回数を確認したところ、「1回」は33%、「2回」26%、「3回」22%、「4回」12%、「5回」3%、「6~9回」2%、「10回以上」2%となっており、転職を2回以上経験する人が65%と多数派となりました。

さらに転職や部署異動経験者(n=426)に対して前職(または異動前)での業種について確認したところ、業種では「IT・セキュリティベンダー」が最も多く約3割、次いで「製造業」「サービス業」「金融業、保険業」の順に多くなりました(図表8:左)。なお、前職の業種については日米専門家間において有意な差は確認できませんでしたが、理系出身専門家は「IT・セキュリティベンダー」を経験後に転職する割合が43%と約半数を占め、文系出身専門家(17%)と比較し26ポイント多くなっています(図表8:右)。

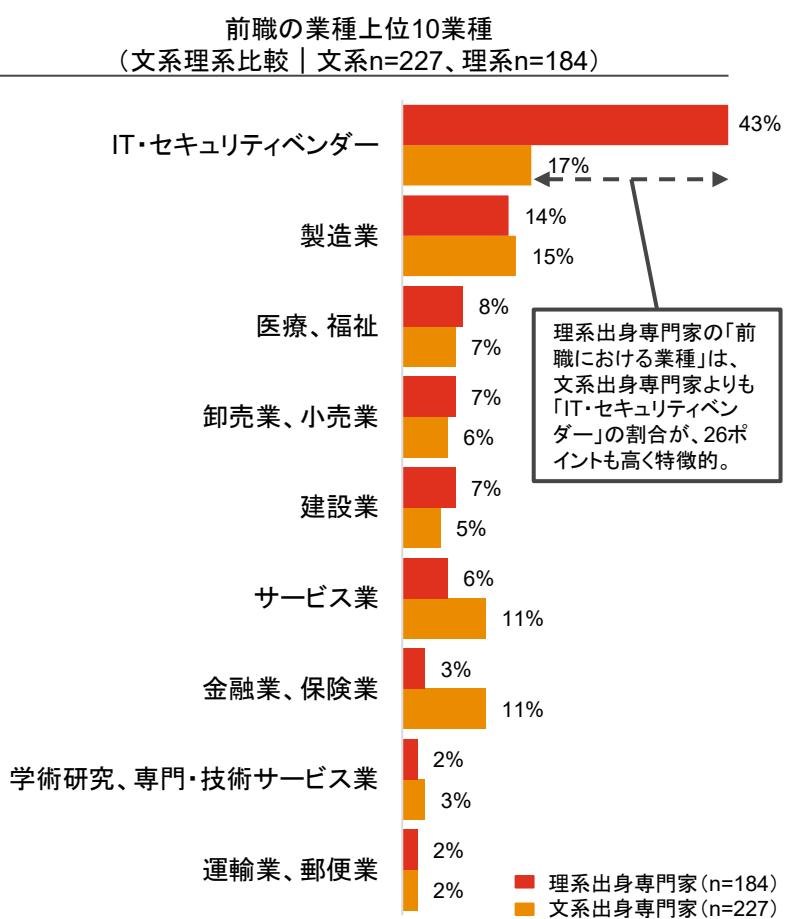
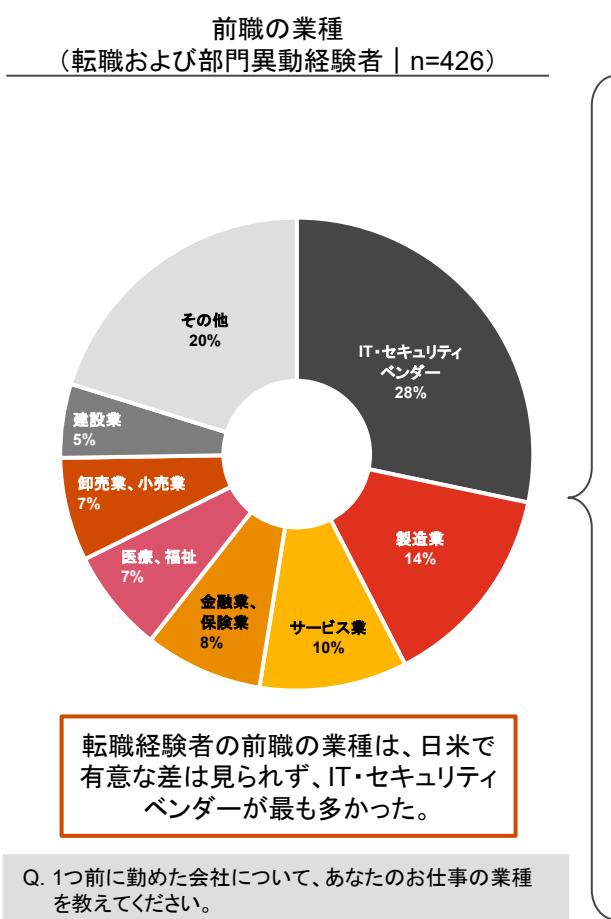
図表7:日米専門家における転職経験の割合と転職回数



転職経験者の転職回数(日米専門家 | n=408)



図表8:転職経験者および部門異動経験者の前職における業種



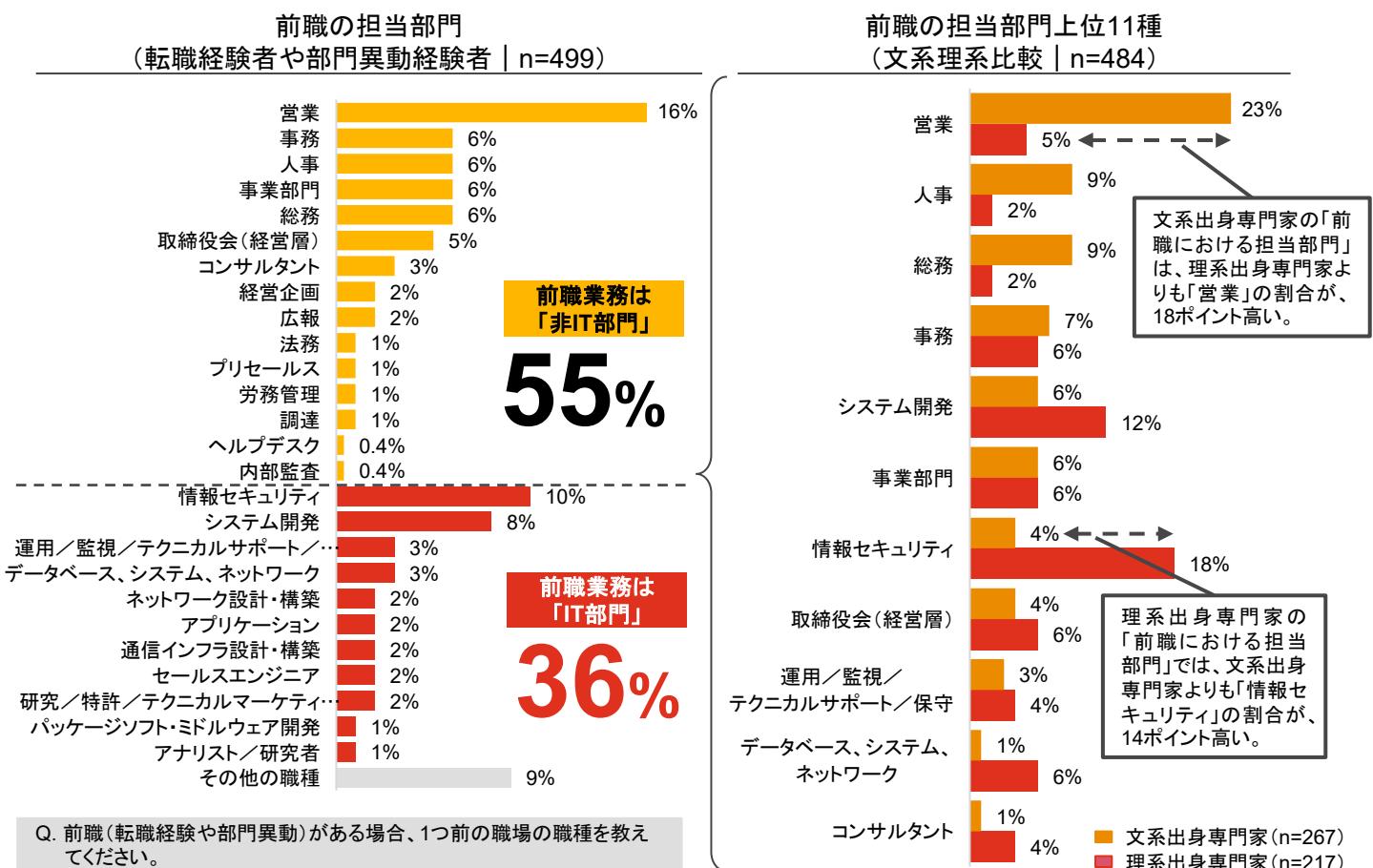
(3) 転職・部門異動経験者の前所属部門は、文系出身専門家で「営業部門」、理系出身専門家で「情報セキュリティ部門」がトップ

前職や部門異動前の担当部門では、「非IT部門」が約6割、「IT部門」は約4割となり、日本を対象とした初回業界調査結果²とは逆転して、「非IT部門」出身者の割合が高い傾向にあることが分かりました(図表9:左)。

具体的にみると「非IT部門」では、「営業」が最も多く16%、次いで「事務」「人事」「事業部門」「総務」がそれぞれ6%、「取締役会(経営層)」が5%の順に多くなりました。「IT部門」では、「情報セキュリティ」が最も多く10%、次いで「システム開発」が8%、「運用／監視／テクニカルサポート／保守」「データベース、システム、ネットワーク」が3%の順に多くなっています。

これらを文系出身専門家(n=267)および理系出身専門家(n=217)で比較すると、最も差が表れたのは「営業」で、文系出身専門家の23%に対し理系出身専門家は5%と、18ポイントの差が確認されました。対して、「情報セキュリティ」では文系出身専門家(4%)に対し理系出身専門家は18%と、14ポイントの差が確認されています。

図表9: 転職経験者および部門異動経験者の前職における担当部門



これらのことから、セキュリティ業界は最終学歴の専攻では「理系」「文系」、また転職においては「IT部門」「非IT部門」出身者双方に開かれており、同業界を牽引する米国でもこの傾向が認められることから、日本のセキュリティ業界においても本傾向は今後も続くと言えるでしょう。

2. 初回業界調査では、「IT部門(50%)」「非IT部門(42%)」「その他(8%)」となり、「IT部門」出身者が高く出ています。

【日米セキュリティ業界で働く:「現在」の傾向】

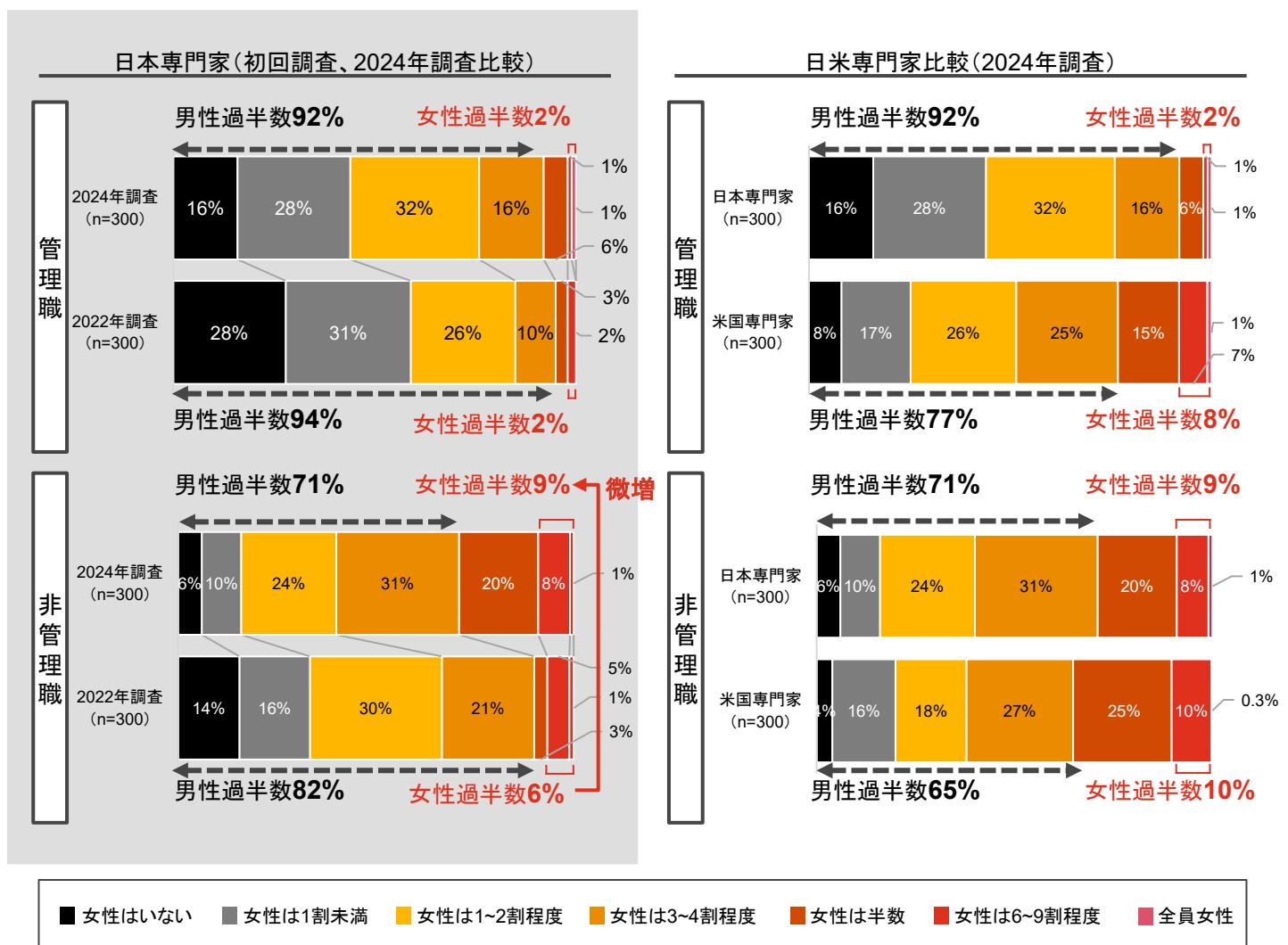
前章ではセキュリティ専門家のキャリアパスにおける「過去」をみてきました。本章では、「現在」の傾向をみていきましょう。

(4) セキュリティ業界における女性の割合は、ゆるやかに増加傾向

セキュリティ業界では、日本では女性専門家は少ないと言われており、初回業界調査においても当該傾向はデータとして裏付けられています。

今年度調査においても「職場でセキュリティ・プライバシー業務に携わる女性の割合」を日米専門家(n=600)に確認した結果、日本においては、女性の割合は2年前の初回業界調査からゆるやかに増加傾向を示し(図表10:左)、米国においても、女性の割合が日本よりもやや多いものの、全体として男性の割合が多い業界であることが確認できました(図表10:右)

図表10: 日米専門家の職場でセキュリティ・プライバシー業務に携わる女性の割合

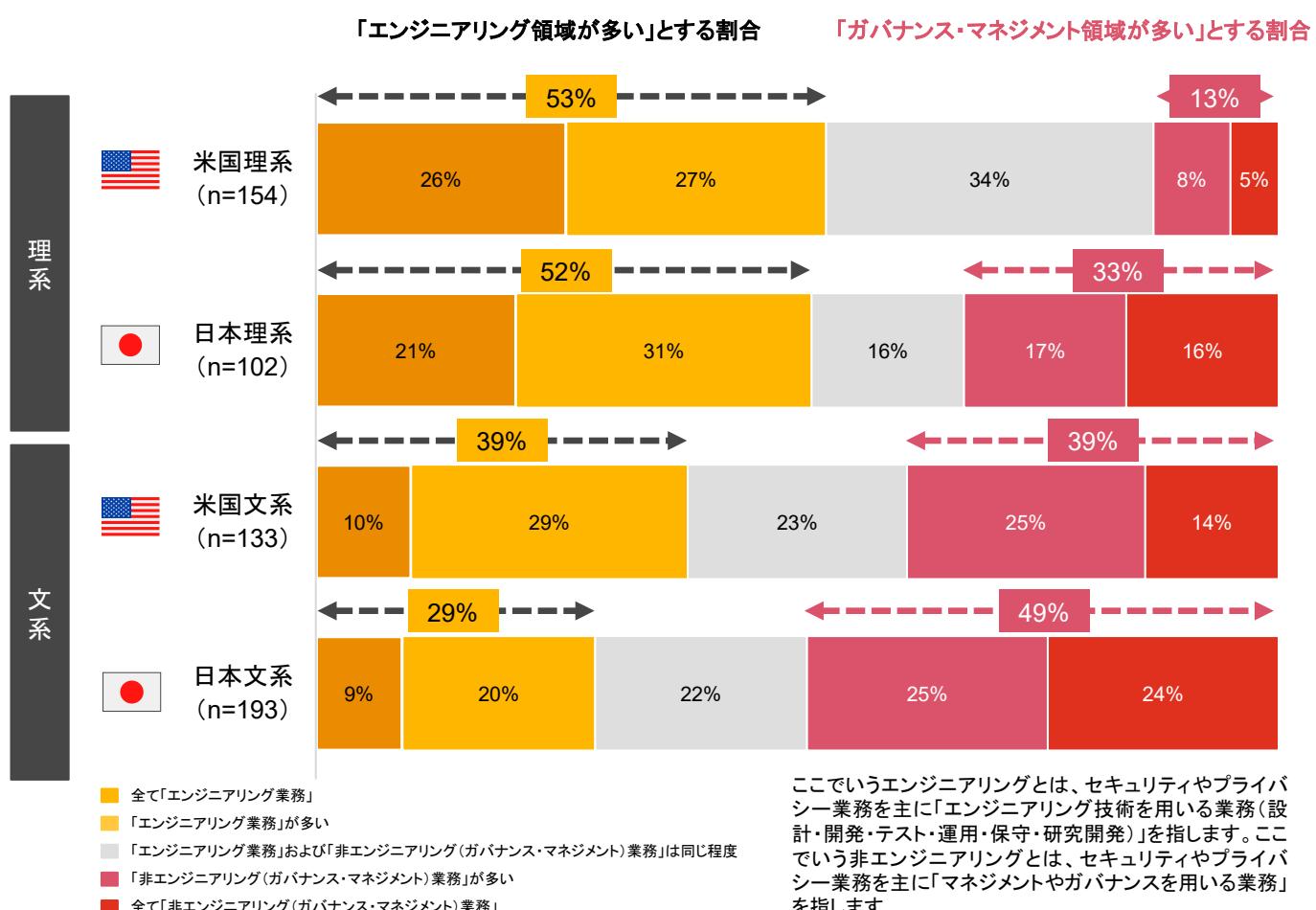


Q. あなたの職場で、セキュリティ・プライバシー業務に携わる女性の割合(管理職(課長・マネージャー以上)/非管理職)を教えてください。

(5) 文系出身専門家は「ガバナンス・マネジメント」業務、理系出身専門家は「エンジニアリング」業務に携わる傾向

日米専門家におけるキャリアパスの「現在の傾向」として、「携わる業務領域」について最終学歴の専攻グループ(理系、文系)で傾向が確認できました(図表11)。理系出身専門家は「エンジニアリング業務が多い」割合が高く、日米ともに過半数を占めますが、日米で比較すると日本は「ガバナンス・マネジメント業務が多い」とする割合が33%と米国よりも20ポイントも高くなっています。また、文系出身専門家をみると、理系出身専門家よりも「ガバナンス・マネジメント業務が多い」割合が日米それぞれで高く、日本の文系出身専門家では約5割を占め、最も多くなっています。

図表11: 日米専門家における「エンジニアリング業務、非エンジニアリング(ガバナンス・マネジメント)業務に携わる割合」(最終学歴の専攻グループ比較)



Q. あなたの現在の勤務先での主な業務は、エンジニアリング業務ですか、非エンジニアリング(ガバナンス・マネジメント)業務ですか。最もあてはまるものを教えてください。

さらに、具体的な業務タスクの項目を、「過去」「現在」「将来」のタイムラインでみると、日米専門家は、「過去」になんらかのセキュリティ業務またはプライバシー業務を経験している割合が約8割います。また、「将来」においても米国文系出身専門家を除き、日米専門家の約8割がセキュリティ業務担当を希望しており、セキュリティ業務関連のキャリアパスを構築していることが分かります(図表12)。

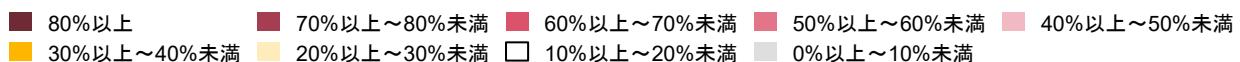
まず、日本専門家は、過去の傾向では、「セキュリティ経営」に携わるとした割合が最も高く32%、次いで「セキュリティ監査」23%、「経営リスクマネジメント」「セキュリティ統括」がそれぞれ18%の順に高くなっています。現在および将来希望する業務タスクの傾向にも同じ傾向がみられ、日本専門家は同じ業務タスク延長線でのキャリアパスを描く傾向があると言えます。

続いて米国専門家では、過去の傾向では、日本専門家と同じく「セキュリティ経営」が最も多く51%、続いて「経営リスクマネジメント」が35%、「セキュリティ統括」が30%、「セキュリティ監査」「デジタルシステム／事業戦略・企画・調達」がそれぞれ27%となっています。現在の傾向としては、米国専門家は、ほぼ全ての項目が30%越えとなっており、日本専門家と比較し複数の業務タスクを兼任していることが分かります。将来の傾向では、米国文系出身専門家に特徴が表れており、ほぼ全ての項目が6割越えとなっています。なかでも回答者の8割が「セキュリティ経営」「経営リスクマネジメント」、7割以上が「セキュリティ監視運用」「セキュリティ調査分析・研究開発」業務に意欲を示しています。一方、米国理系出身専門家は日本専門家と同じような割合にとどまり、「セキュリティ経営」が最も高く29%、「経営リスクマネジメント」が28%、「システムアーキテクチャ」「セキュリティ監視運用」「セキュリティ調査分析・研究開発」がそれぞれ25%と続きます。

図表12:現在の業務タスク(複数回答 | n=600)

回答者数	過去						現在						将来					
	米国			日本			米国			日本			米国			日本		
	全体	文系	理系															
セキュリティ経営	51%	45%	56%	32%	31%	35%	47%	38%	56%	30%	32%	28%	36%	81%	29%	26%	26%	25%
セキュリティ監査	27%	30%	24%	23%	20%	28%	37%	29%	44%	24%	21%	29%	26%	59%	21%	17%	15%	23%
経営リスクマネジメント	35%	35%	32%	18%	18%	18%	46%	47%	45%	18%	19%	16%	35%	80%	28%	17%	16%	19%
セキュリティ統括	30%	28%	31%	18%	17%	21%	47%	46%	49%	19%	19%	20%	31%	69%	24%	16%	17%	16%
デジタルシステム／事業戦略・企画・調達	27%	25%	29%	15%	12%	22%	40%	38%	43%	19%	14%	28%	26%	59%	19%	16%	14%	22%
システムアーキテクチャ	24%	24%	23%	12%	7%	21%	33%	24%	42%	13%	8%	24%	30%	68%	25%	10%	7%	17%
デジタルプロダクト開発	22%	20%	25%	11%	9%	16%	32%	25%	39%	11%	8%	17%	31%	69%	19%	12%	11%	15%
デジタルプロダクト運用・脆弱性診断／ペネトレーションテスト・セキュリティ監視運用	19%	17%	21%	12%	11%	15%	35%	29%	41%	13%	9%	21%	30%	68%	22%	13%	11%	18%
セキュリティ監視運用	24%	22%	26%	12%	11%	15%	39%	32%	46%	16%	16%	16%	34%	77%	25%	15%	15%	15%
セキュリティ調査分析・研究開発	21%	23%	19%	9%	7%	13%	36%	30%	42%	10%	6%	17%	33%	74%	25%	11%	9%	15%
その他のセキュリティ・プライバシー業務	13%	13%	14%	18%	20%	15%	25%	29%	21%	27%	27%	25%	23%	51%	19%	15%	15%	17%
セキュリティ・プライバシー以外の業務	22%	20%	23%	23%	24%	20%	0%	0%	0%	0%	0%	0%	18%	40%	21%	22%	23%	17%

セキュリティ専門家の前職・前担当部門で「セキュリティに業務に携わっていた割合」は日米ともに約8割が多い



Q. あなたの現在の勤務先での業務タスクとして、あてはまるものを全て教えてください。過去に担当されていたもの、また将来的に担当してみたいものも併せてご回答ください。

「セキュリティ業界はハッキング技術やコーディングなどのエンジニアリング技術領域のスキルや経験が必要なのではないか」と考える学生や他業界・他部門からの転職者も多いと思いますが、データが示すように、サイバーセキュリティ戦略や体制構築・規程策定・教育業務などガバナンス業務や、必ずしもエンジニアリングの知識を要しない地政学リスク・法規制対応やOSINT³など調査に関する業務も多く存在します。そのため、エンジニアリング業務の経験がなくても、セキュリティ業界に関心があるのであれば、安心して挑戦していただきたいと考えます。

3. OSINT(Open Source Intelligence)とは、ダークウェブを含むインターネット上の公開情報を対象として情報を収集・分析するリサーチ方法の一種です。

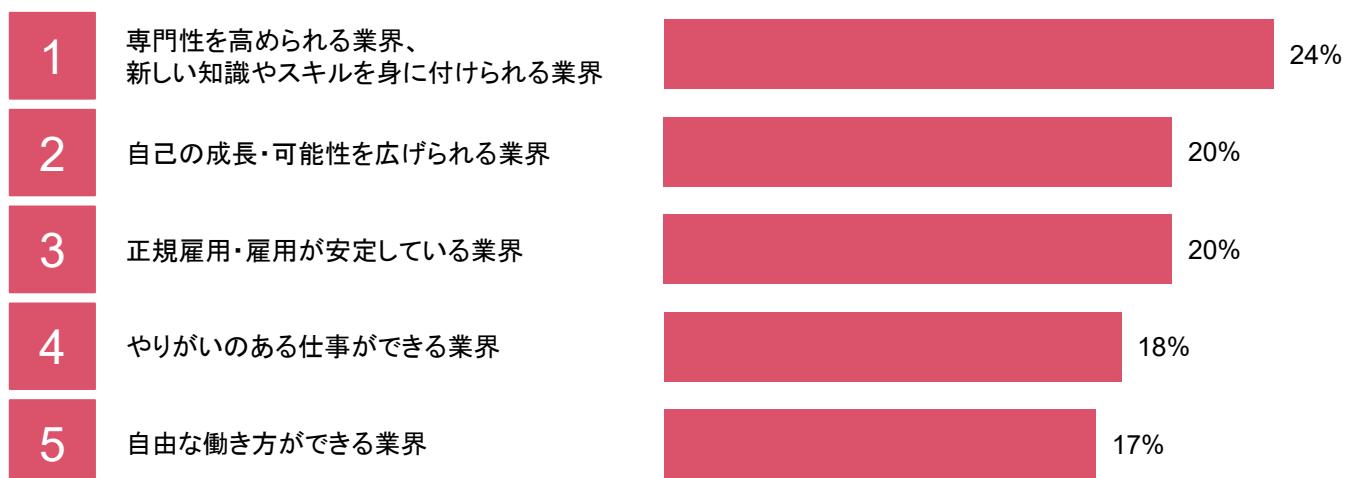


(6)セキュリティ業界で実際に働いた印象は、「専門性を高められる業界」がトップ

日米専門家(n=600)にセキュリティ業界に対する「実際に働いた後の印象」を確認したところ、「専門性を高められる業界、新しい知識やスキルを身に付けられる業界」が24%で最も多く、次いで「自己の成長・可能性が広げられる業界」「正規雇用・雇用が安定している業界」がそれぞれ20%、「やりがいのある仕事ができる業界」が18%、「自由な働き方ができる業界」が17%と続いている(図表13)。

のことから、セキュリティ業界は雇用が安定した中で自己実現をできるだけでなく、それが自分に合った働き方ができる業界と言えるでしょう。

図表13:セキュリティ業界で働いた後の同業界に抱く印象(上位5項目 | n=600)



Q. あなたが実際に働いてみたあなたのセキュリティ・プライバシー業務のイメージとして、あてはまるものをそれぞれ3つずつお知らせください。

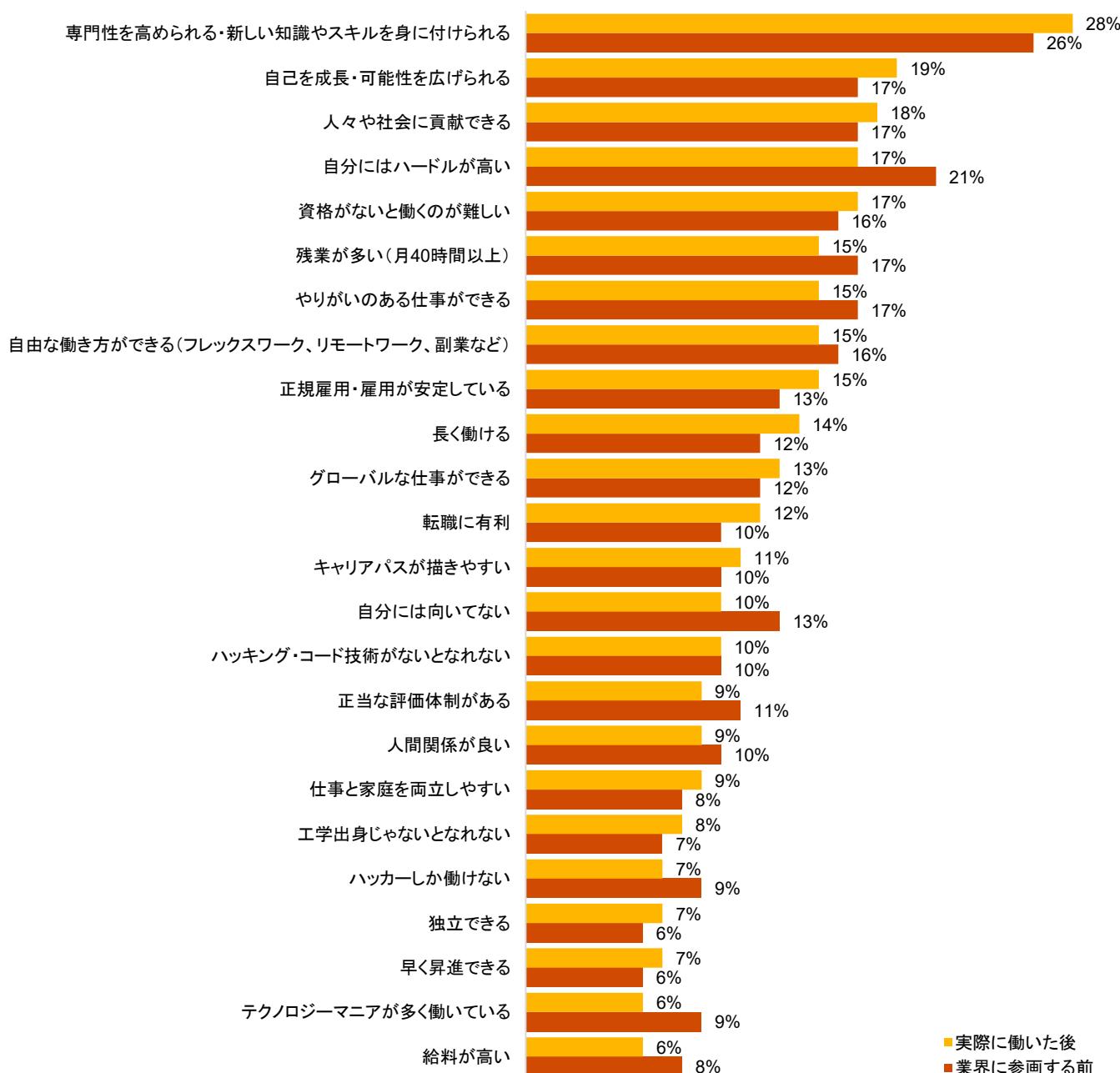
続いて、各国専門家の実際に働いた印象について具体的に傾向をみていきましょう。

日本専門家(n=300)の実際に働いた後の印象の上位3項目をみると、「専門性や新たな知識・スキルを身に付けられる」が最も高く28%、次いで「自己を成長・可能性を広げられる」が19%、「人々や社会に貢献できる」が18%の順となりました(図表14)。米国専門家(n=300)の実際に働いた後の印象の上位3項目では「正規雇用・雇用が安定している」が最も高く24%、次いで「自己を成長・可能性を広げられる」「やりがいのある仕事ができる」がそれぞれ21%となりました(図表15)。なお、日本男女専門家比較、米国男女専門家比較の詳細データはAppendix 図表42～図表45を参照ください。

またこれらのポジティブな回答はいずれも、セキュリティ業界に参画する「前の印象」よりも実際に働いた「後の印象」として回答した専門家が多くなりました。これらからセキュリティ業界は、日米ともに業界参画前に想像するよりも自己実現ができる業界だと言えます。

一方で、セキュリティ業界に入る「前の印象」の懸念点として、日本専門家は「自分にはハードルが高すぎる」と印象を抱く割合が21%と、米国専門家(6%)と比較し高く、特に日本女性専門家(24%)に顕著に表れています。このことから本業界未経験の就職活動者にとって、就職先としてセキュリティ業界が選択肢から漏れているのではないかと危惧します(詳細はAppendix図表42・図表43・図表44・図表45参照)。なお、同じ項目について、実際に働いた「後の印象」は日本女性専門家において約10ポイントも低いことから、「想像していたよりもハードルは低い業界」とも言えます。このため、就職先として関心があれば「私には難しい業界だ」など壁をつくらず、思い切って挑戦いただくとよいと考えます。

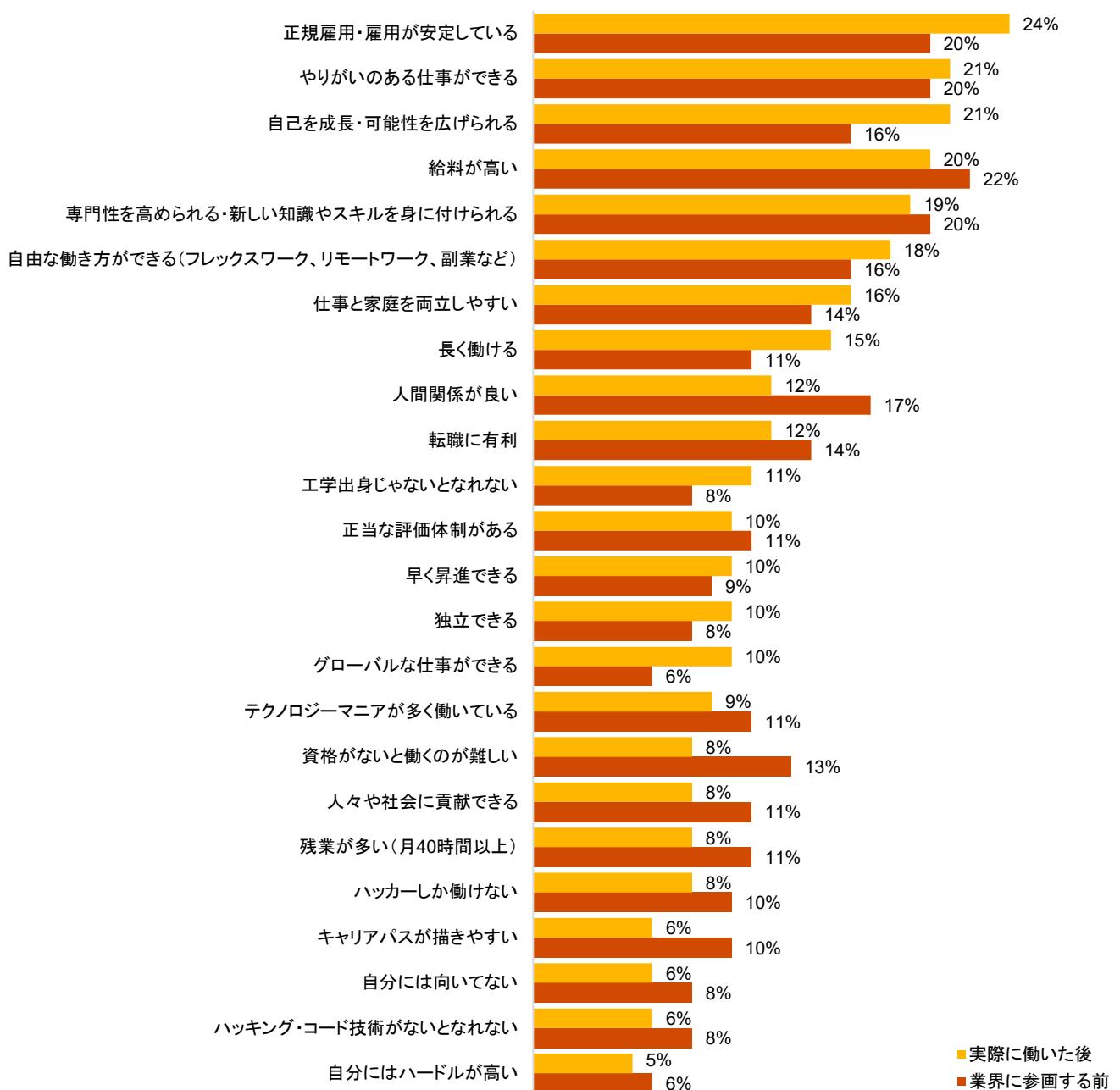
図表14: 働く「前」と実際に働いた「後」のセキュリティ業界に対する印象の比較(日本)



Q. あなたが実際に働いてみたあなたのセキュリティ・プライバシー業務のイメージとして、あてはまるものをそれぞれ3つずつお知らせください。



図表15: 働く「前」と実際に働いた「後」のセキュリティ業界に対する印象の比較(米国)



Q. あなたが実際に働いてみたあなたのセキュリティ・プライバシー業務のイメージとして、あてはまるものをそれぞれ3つずつお知らせください。

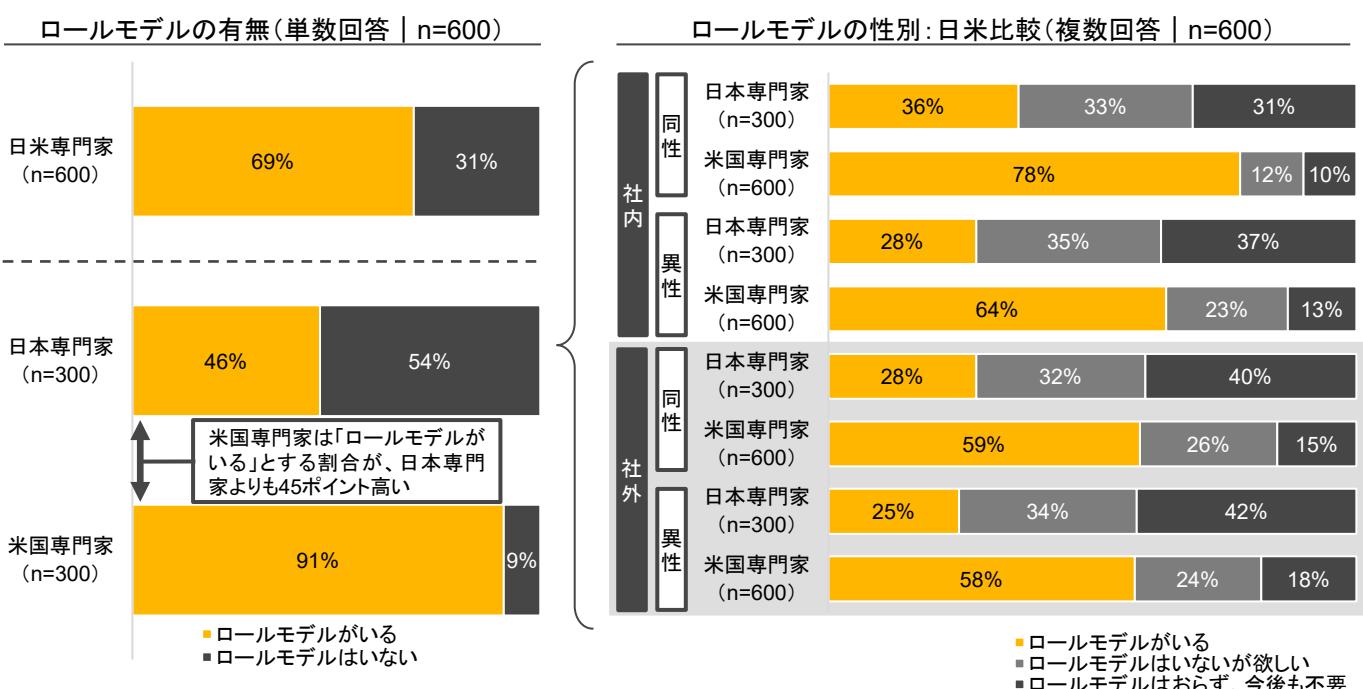
(7) ロールモデルがいる日米専門家は7割。多くが「セキュリティ業務に満足」とポジティブな評価

続いて「仕事への満足度」について確認したところ、日米専門家ともに、「ロールモデルがいる」グループ(n=415)は「ロールモデルはいない」グループ(n=185)より、仕事への満足度が顕著に高くなることが確認できました(図表16・図表17)。

まず、ロールモデルの有無についてみていきます。

日米専門家(n=600)に「あなたのキャリアパスを検討・設計する上での、ロールモデル(お手本となる人物または人物像)の有無」を確認したところ、69%が「ロールモデルがいる」と回答しました(図表16:左)。日米で比較すると、日本専門家(n=300)では「ロールモデルがいる」割合が46%に対し、米国専門家(n=300)では「ロールモデルがいる」割合が91%と、45ポイントも高くなりました。具体的にみると、「社内に同性のロールモデルがいる」割合が日米専門家においてともに最も高く、米国専門家では78%を占め、日本専門家では36%となりました(図表16:右)。

図表16: 日米専門家における「ロールモデルの有無」



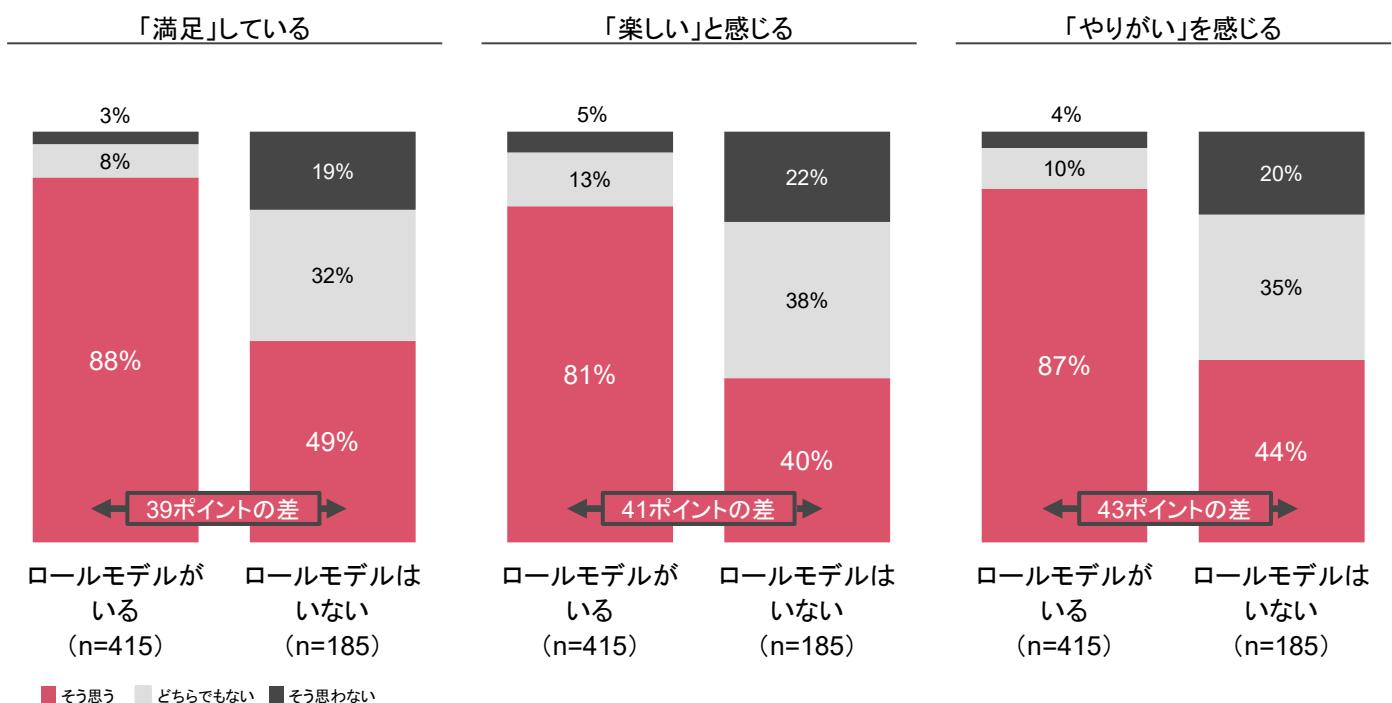
Q. あなたがセキュリティ・プライバシー業界で働くにあたり、あなたのキャリアパスを検討・設計する上で、ロールモデル(お手本となる人物または人物像)は存在しますか。

続いて「担当するセキュリティ業務に満足(楽しい・やりがい)しているか」確認したところ、「ロールモデルがいる」グループ(n=415)は、業務に満足する割合が8割以上と高いことが示されました(図表17)。

具体的には「ロールモデルがいる」グループは、業務に対し「満足している」と回答した割合は88%、「楽しいと感じる」は81%、「やりがいを感じる」は87%と、いずれも8割以上がポジティブな回答をしました。対して「ロールモデルはいない」グループ(n=185)は、業務に対し「満足している」と回答した割合は49%('ロールモデルがいる'グループと39ポイント差)、「楽しいと感じる」は40%(同41ポイント差)、「やりがいを感じる」は44%(同43ポイント差)と、いずれも半数に届きませんでした。



図表17: 担当するセキュリティ業務における満足度(楽しい・やりがい)(ロールモデルの有無で比較)



Q. あなたは、現在の仕事に対して満足していますか。または、「楽しさ」や「やりがい」を感じていますか。

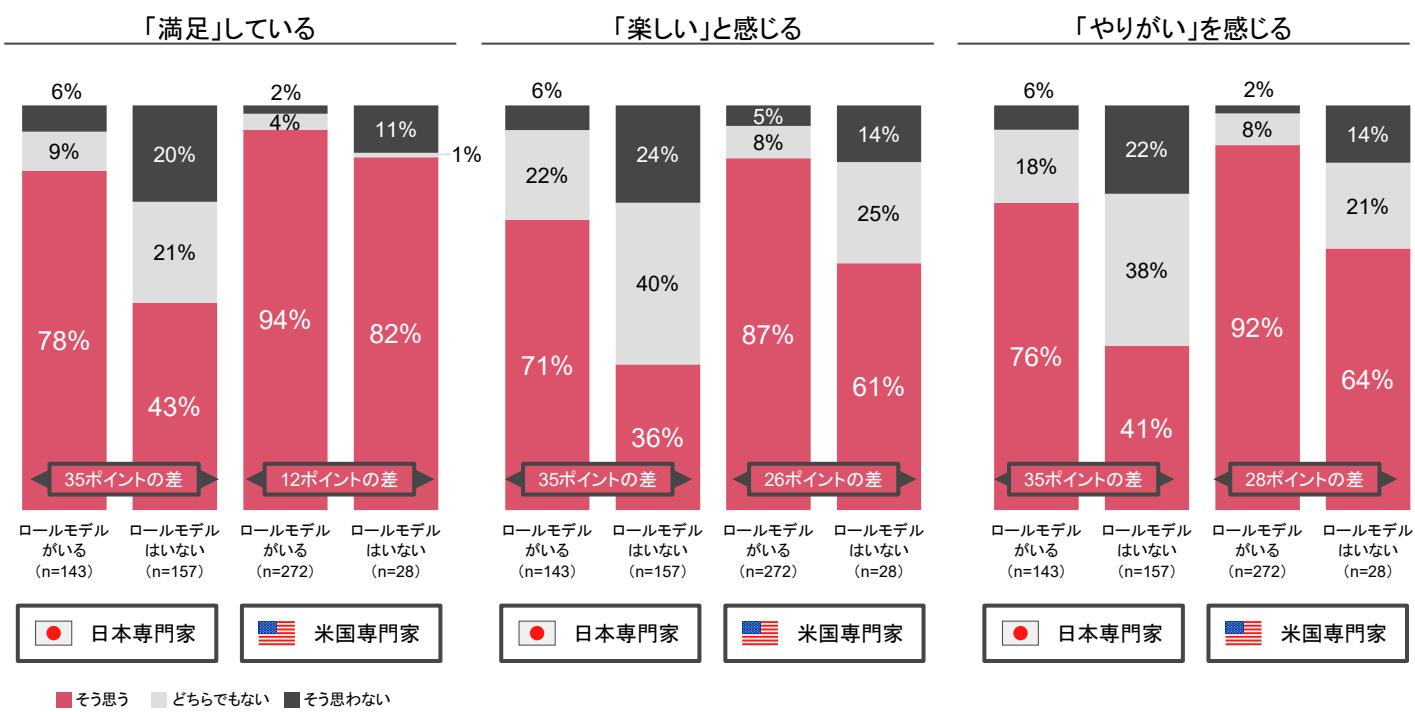
さらに「ロールモデルの有無」を日米専門家で分析します(図表18)。

日本専門家においては、ロールモデルのいるグループ(n=143)がいずれも高い傾向が表れています。まず、業務に「満足している」と回答した割合は、ロールモデルのいるグループは78%、ロールモデルのいないグループ(n=157)は43%、「楽しいと感じる」は、ロールモデルのいるグループは71%、ロールモデルのいないグループは36%、「やりがいを感じる」は、ロールモデルのいるグループは76%に対し、ロールモデルのいないグループは41%と、各項目で35ポイントの差が確認できました。

米国専門家においてはロールモデルの有無にかかわらず業務に「満足している」割合が高く、ロールモデルのいるグループ(n=272)は94%、ロールモデルのいないグループ(n=28)は82%となりました。一方で、「楽しさ」「やりがい」の項目では顕著な差が確認できました。「楽しいと感じる」は、ロールモデルのいるグループが87%に対し、ロールモデルのいないグループは61%と26ポイントの差があり、「やりがいを感じる」では、ロールモデルのいるグループが92%、ロールモデルのいないグループが64%と28ポイントの差が確認できました。

これらのことから、セキュリティ業界で、仕事にやりがいや楽しさを感じて働く上では、自身のロールモデルを見つけることが有用であると言えます。

図表18: 担当するセキュリティ業務における満足度(楽しい・やりがい)(ロールモデルの有無で比較、日米比較)



(8) 専門家の考える「活躍の定義」は「時間内に効率よく高品質な成果を出せる」がトップ。一方、社内の期待は「管理職になる」がトップと乖離がみられる

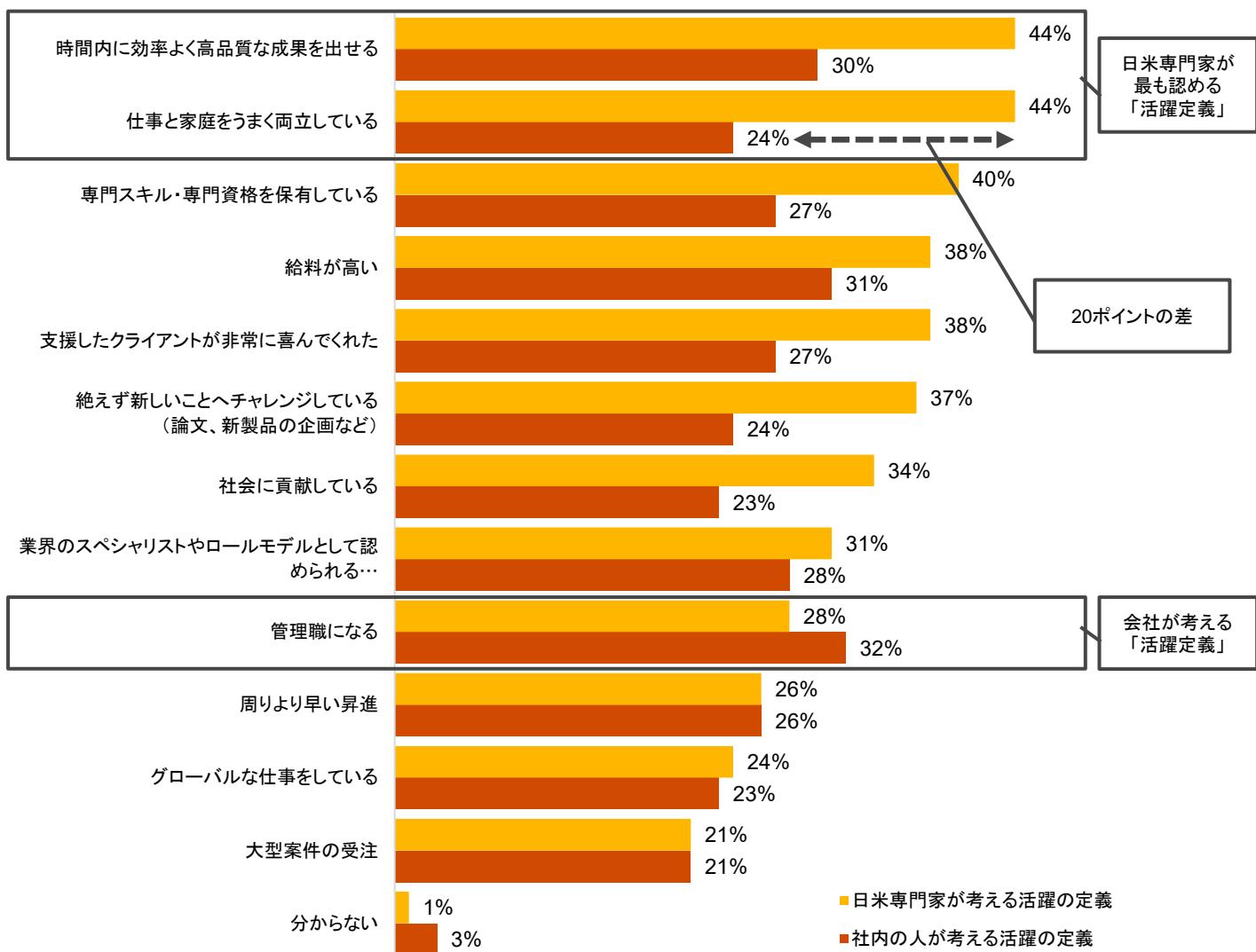
しばしば、日本では「活躍の定義」として管理職(や経営層)になることが挙げられますが、実際、日米専門家の考える「活躍」とは何を指すのでしょうか。今回の調査で、専門家が考える「活躍の定義」に加え、社内が期待する「活躍の定義」を確認したところ、この2つの定義に乖離がみられました(図表19)。

日米専門家(n=600)に「あなたの考える活躍の定義」を確認したところ、「時間内に効率よく高品質な成果を出せる」「仕事と家庭をうまく両立している」がそれぞれ44%と最も多く、続いて「専門スキル・専門資格を保有している」が40%、「給料が高い」「支援したクライアントが非常に喜んでくれた」がそれぞれ38%の順に多くなっています。

次に「社内の人と考える活躍の定義」について確認したところ、「管理職になる」が最も高く32%、次いで「給料が高い」が31%、「時間内に効率よく高品質な成果を出せる」が30%、「業界のスペシャリストやロールモデルとして認められる(メディアに取り上げられる)」が28%、「専門スキル・専門資格を保有している」「支援したクライアントが非常に喜んでくれた」がそれぞれ27%の順に高くなりました。専門家自身が考える活躍の定義において、「管理職になる」(28%)は全体の9番目で、専門家自身が考える活躍の定義と社内で期待される活躍の定義には乖離があることが分かります。

このことからセキュリティ業界で働く専門家は、ワークライフバランスや限られた時間の中で成果を出すことを重視する一方で、会社が考える活躍の定義として最も多く選択された「管理職になる」ことはあまり重視していない傾向があると言えます。

図表19: 日米専門家の考える「活躍の定義」と社内が考える「活躍の定義」比較(複数回答 | n=600)



Q. あなたにとって、仕事で活躍するとは具体的にどのような条件を満たした場合と考えますか。また会社で評価されている人の特徴も併せて、あてはまるものを全て教えてください。

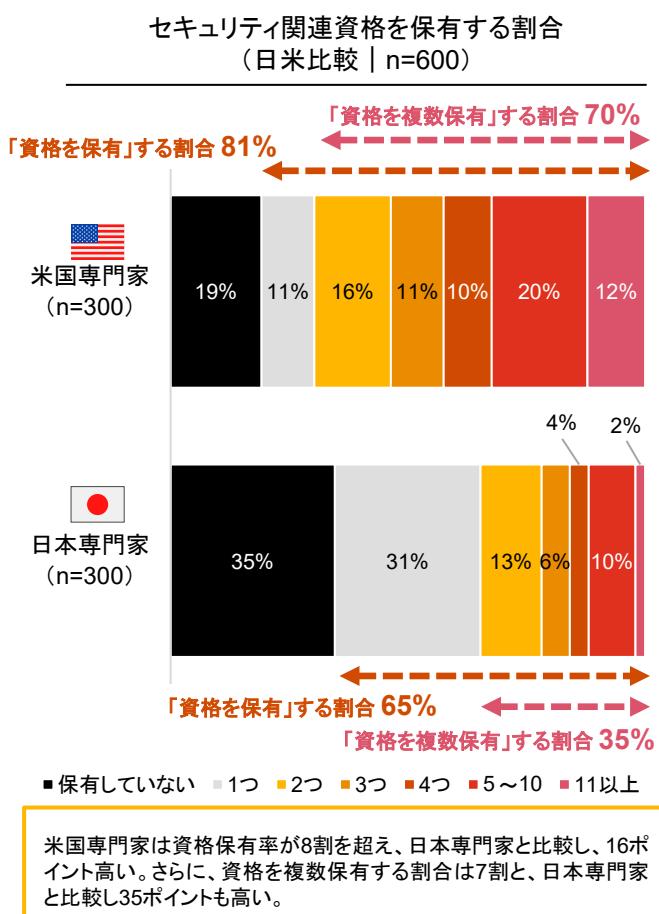
(9) 「業務に有益」とする資格は「クラウドセキュリティ関連資格」が上位

次に、日米専門家のセキュリティ関連資格の「保有状況」と「有益性」についてみていきます。

日米専門家の資格保有状況は、米国専門家の割合は81%と、日本専門家の資格保有率65%よりも16ポイント高く、また米国専門家は複数資格を保有する傾向にあり(70%)、日本専門家の35%と比較して高くなりました(図表20:左)。

具体的に保有資格をみると、資格を保有する米国専門家(n=223)においては、「AWS Certified Security - Specialty」が最も多く42%、次いで「Certified Cloud Security Professional (CCSP)」が38%、「Certified Information Privacy Manager (CIPM)」「Certified Information Security Manager (CISM)」が31%、「Certified Information Privacy Professional (CIPP) (iapp)」が29%の順に高くなりました(図表20:右)。資格を保有する日本専門家(n=197)においても「AWS Certified Security - Specialty」が最も多く36%、次いで「IPA情報処理技術者」が22%、「Certified Cloud Security Professional (CCSP)」が21%、「情報セキュリティマネジメント」「Certified Ethical Hacker (CEH)」「IPA応用情報技術者」がそれぞれ15%と続きます。

図表20: 日米専門家のセキュリティ関連資格の保有状況



保有資格上位10項目日米比較
(日米比較 | n=420)

資格を保有する 米国専門家(n=223)	資格を保有する 日本専門家(n=197)
1 AWS Certified Security – Specialty 42 %	1 AWS Certified Security – Specialty 36 %
2 Certified Cloud Security Professional (CCSP) 38 %	2 IPA情報処理技術者 22 %
3 Certified Information Privacy Manager (CIPM) 31 %	3 Certified Cloud Security Professional (CCSP) 21 %
3 Certified Information Security Manager (CISM) 31 %	4 情報セキュリティマネジメント 15 %
5 Certified Information Privacy Professional (CIPP) (iapp) 29 %	4 Certified Ethical Hacker (CEH) 15 %
6 Certified Information Systems Security Professional (CISSP) 27 %	4 IPA応用情報技術者 15 %
6 Certified Data Privacy Solutions Engineer 27 %	7 Certified Data Privacy Solutions Engineer 14 %
8 Certified Ethical Hacker (CEH) 25 %	8 情報セキュリティマネジメント 11 %
9 Certified in Risk and Information Systems Control (CRISC) 22 %	8 Certified Information Privacy Professional (CIPP) (iapp) 11 %
10 Project Management Professional (PMP) 21 %	8 Certified Information Privacy Manager (CIPM) 11 %

米国および日本専門家の保有資格上位10項目に重複して確認できた資格

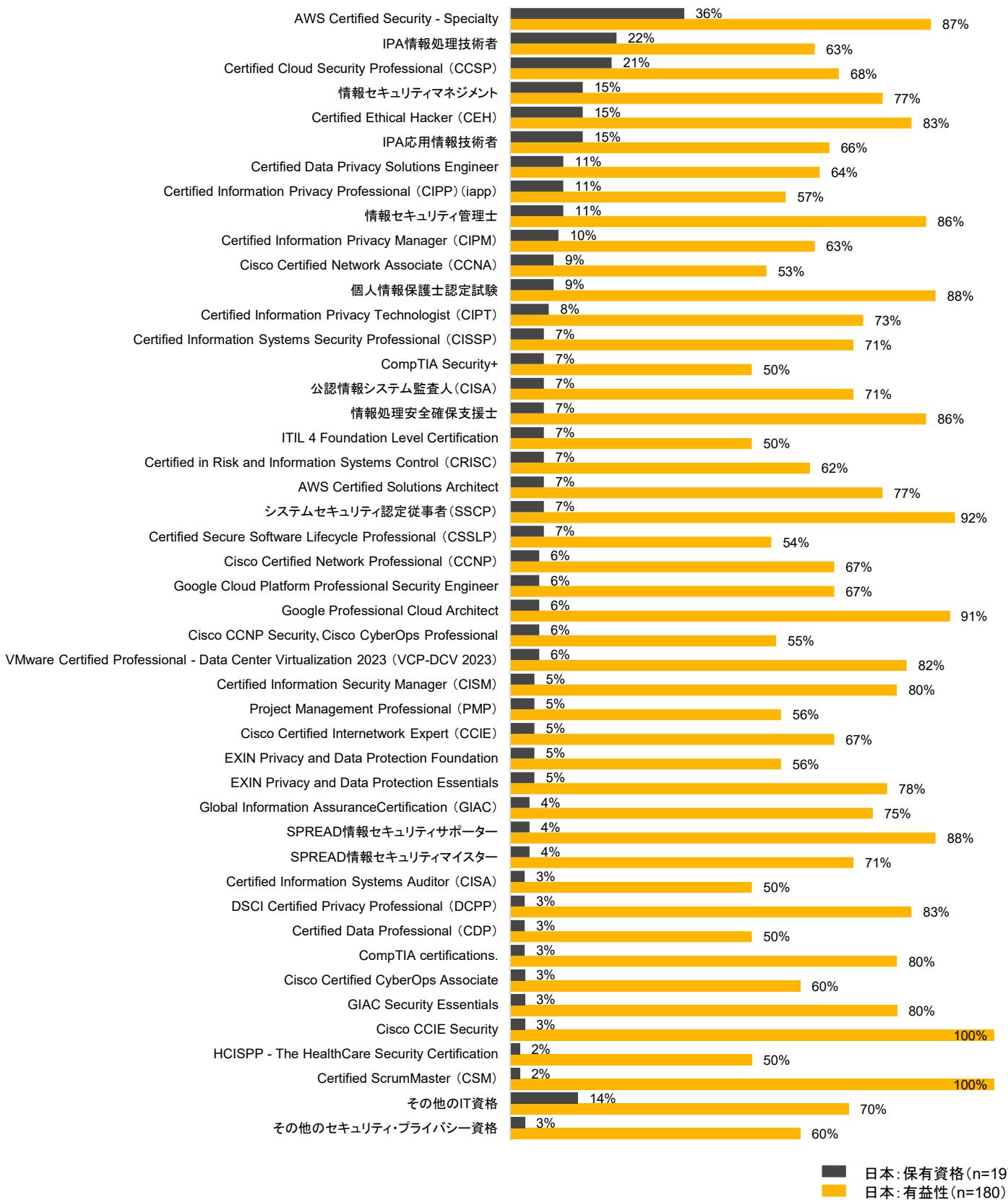
Q. あなたは、セキュリティ・プライバシー業務に関連するどのような資格を保有していますか。



さらに、取得した資格が業務に有益だったかを確認したところ、日米専門家ともにほぼ全ての資格において半数以上が有益性を感じていることが分かりました(図表21・図表22)。

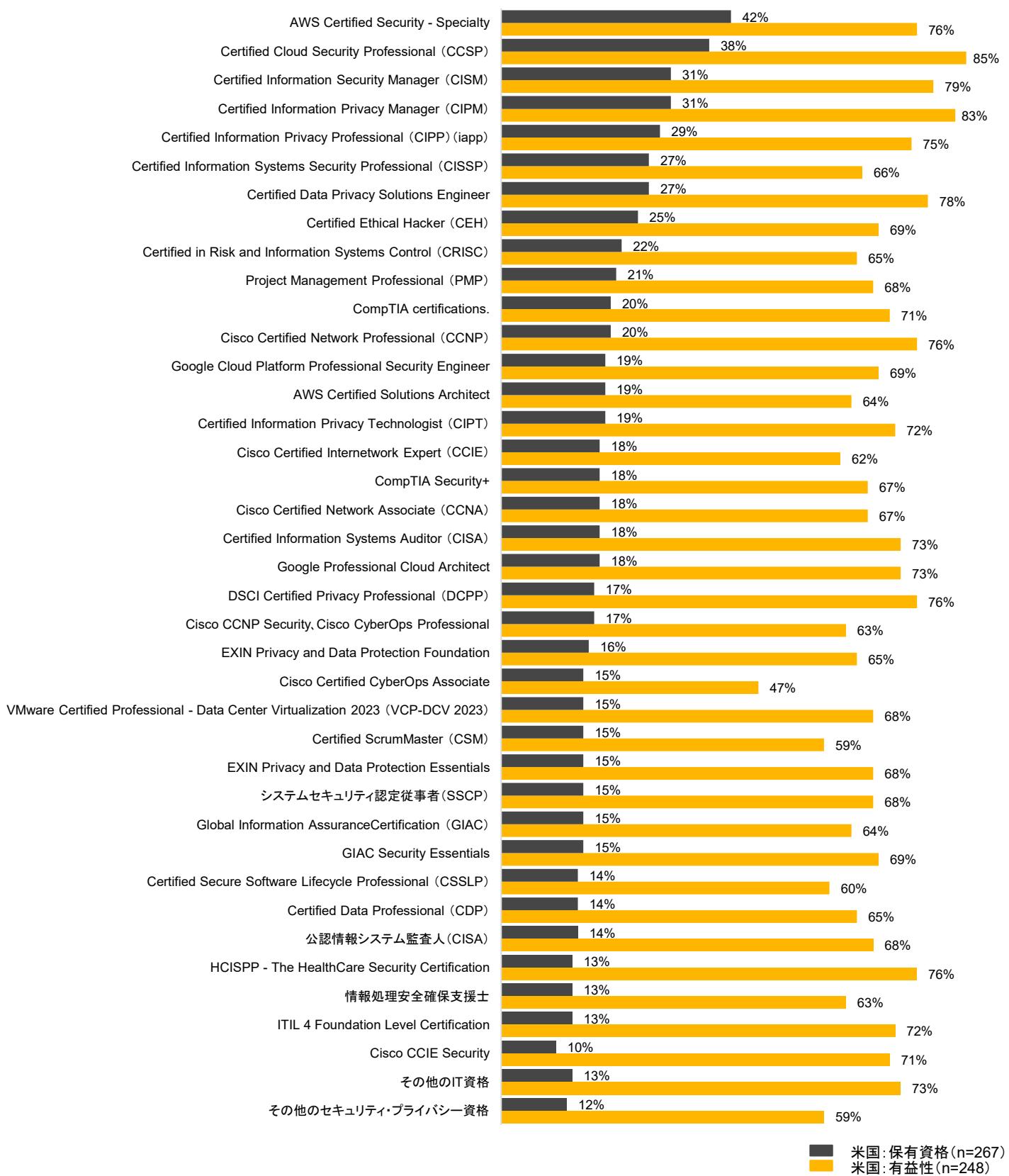
具体的にみると、保有する資格に有益性を認める日本専門家(n=180)において、資格保有者数が10名以上で「業務に有益」とした資格は「システムセキュリティ認定従事者(SSCP)」が最も多く92%、次いで「Google Professional Cloud Architect」が91%、「個人情報保護士認定試験」が88%、「AWS Certified Security - Specialty」が87%、「情報処理安全確保支援士」「情報セキュリティ管理士」がそれぞれ86%と順に高くなっています(図表21)。次に、保有する資格に有益性を認める米国専門家(n=248)においては「Certified Cloud Security Professional (CCSP)」が最も多く85%、次いで「Certified Information Privacy Manager (CIPM)」が83%、「Certified Information Security Manager (CISM)」が79%、「Certified Data Privacy Solutions Engineer」が78%、「AWS Certified Security - Specialty」「DSCI Certified Privacy Professional (DCPP)」「HCISPP - The HealthCare Security Certification」「Cisco Certified Network Professional (CCNP)」がそれぞれ76%となっています(図表22)。

図表21: 日米専門家の保有資格と有益性(日本)



Q. あなたは、セキュリティ・プライバシー業務に関連するどのような資格を保有していますか。またその中で業務に有益だったものを教えてください。

図表22: 日米専門家の保有資格と有益性(米国)



Q. あなたは、セキュリティ・プライバシー業務に関連するどのような資格を保有していますか。またその中で業務に有益だったものを教えてください。



Past

Present

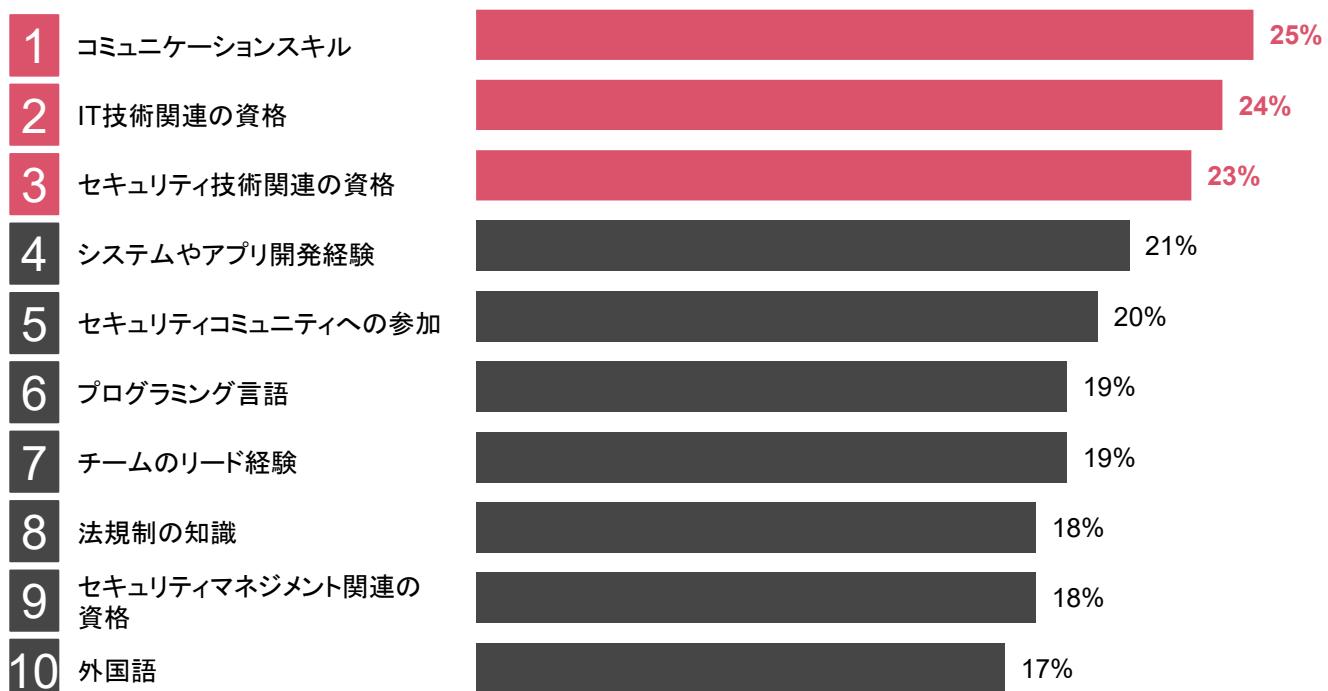
Future

(参考)日米専門家が推奨するスキルや経験

また、本調査において、将来セキュリティ業界を目指す学生や転職者へ推奨する研鑽すべきスキルや経験として、日米専門家は「コミュニケーションスキル」「IT技術関連の資格」「セキュリティ技術関連の資格」を挙げました(図表23)。今後セキュリティ業界を目指す際に参考としていただければ幸いです。

図表23: 日米専門家が学生や転職者へ推奨する、セキュリティ業務に携わる前に学ぶべきスキル・経験

(上位10項目 | n=523)



Q. 未来のセキュリティ専門家を目指す学生や転職者へ、あなたが推奨する、事前に勉強・経験しておくと有利だと考えるスキル・経験を全て教えてください。

【日米セキュリティ業界で働く：「将来」の傾向】

本章では、日米専門家のキャリアパスにおいて「将来」をどのように描くのかをみていきましょう。

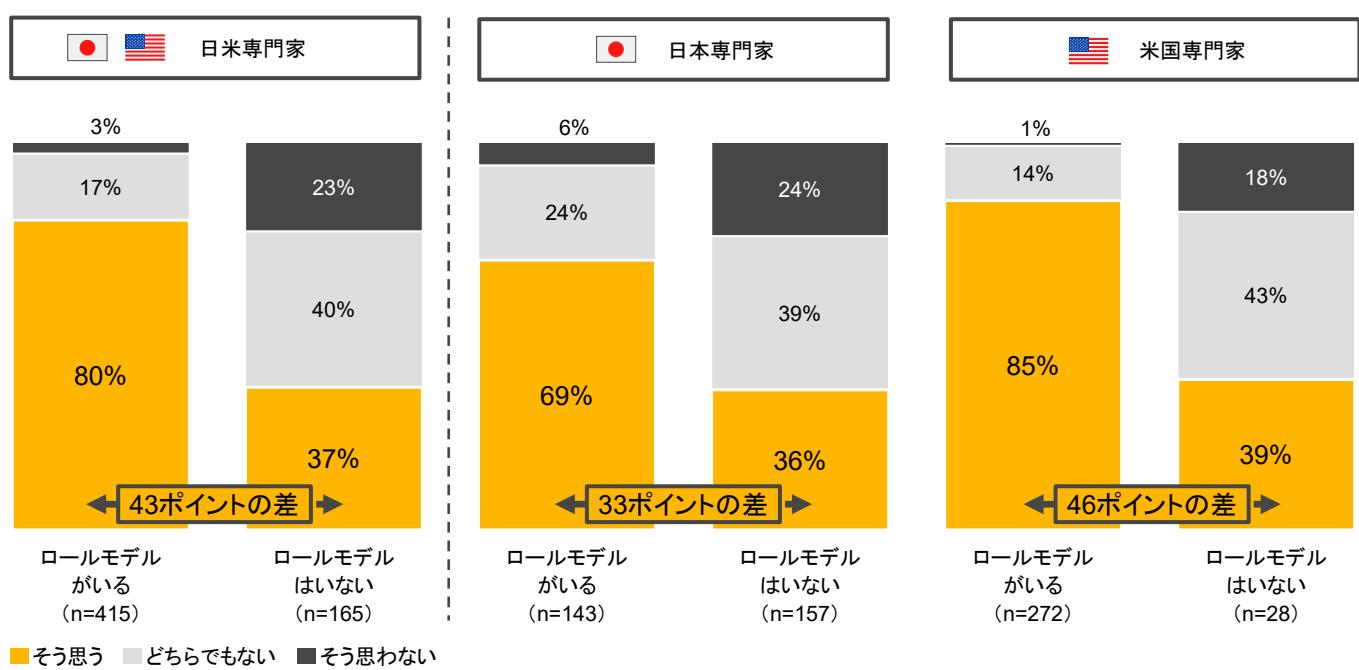
(10) ロールモデルがいる日米専門家は「セキュリティ業界で長く働きたい」意向が8割

前章「現在の傾向」で「ロールモデルがいる」グループは、業務にやりがいや楽しさを感じ満足する割合が全て8割以上と高い傾向を確認しましたが、「セキュリティ業界で長く働きたい」と回答した割合も8割と、「ロールモデルはない」グループ(4割未満)よりも高くなりました(図表24)。

日本専門家を分析すると「セキュリティ業界で長く働きたい」と考える「ロールモデルがいる」グループは69%と、「ロールモデルはない」グループの36%と比較して33ポイント多くなりました。米国専門家においても同様の傾向がみられ、「セキュリティ業界で長く働きたい」と考える「ロールモデルがいる」グループは85%と非常に高いものの、「ロールモデルはない」グループは39%にとどまり、46ポイントの差が確認できました。

このため、セキュリティ業界でのキャリアパスを描く際には、自身が目指したいロールモデルを見つけておくと、セキュリティ業界で長く、充実した業務経験を得ることができると言えるでしょう。

図表24:セキュリティ業界で長く働きたいと考える割合(ロールモデルの有無、日米比較)





Past

Present

Future

(11) 昇進意欲のある米国専門家は8割で日本専門家より多い

続いて、日米専門家の将来の意向として、「昇進」「目指す領域(スペシャリスト／ジェネラリスト)」「転職」についてみていきましょう。

■ 昇進意欲

日米専門家に「管理職または経営層への昇進意欲(同職階に就く者は継続意欲)」を確認したところ、「昇進意欲がある」と回答した米国専門家は約9割と、日本専門家の約7割より多くなりました(図表25)。昇進を希望する理由はAppendix図表46・図表47、昇進する上での不安や課題はAppendix図表48・図表49をご参照ください)。

具体的にみると、「管理職または経営層への昇進意欲がある」日本専門家は66%、「管理職または経営層どちらにもなりたくない」とした日本専門家は34%でした。

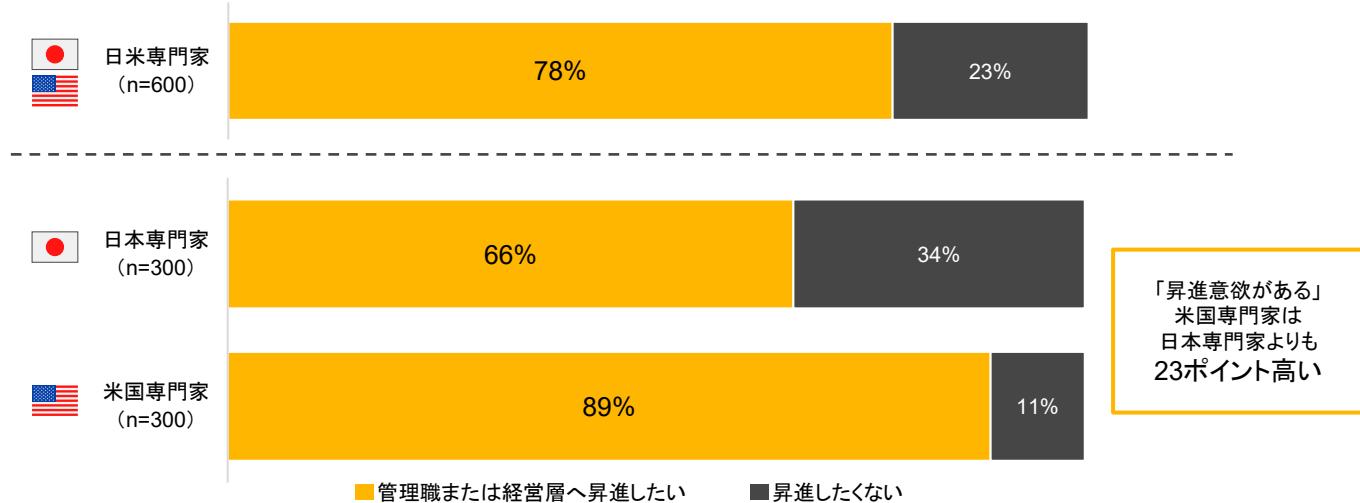
男女間で比較すると、「管理職または経営層への昇進意欲がある」と回答した日本男性専門家は74%であるのに対し、日本女性専門家は57%にとどまり、男性専門家の方が17ポイントも多いことが分かります(図表26)。昇進意欲の性別による傾向は、初回業界調査でも確認されていますが、2年前調査と比べ男女ともに昇進意欲は高まっていると言えます。

※初回業界調査では、「管理職または経営層への昇進意欲がある」と回答した日本男性専門家は60%(今年度調査では+14ポイント)、日本女性専門家は45%(今年度調査では+12ポイント)。

続いて米国専門家では、89%が「管理職または経営層への昇進意欲がある」と回答し、「管理職または経営層どちらにもなりたくない」とした米国専門家は11%にとどまりました。

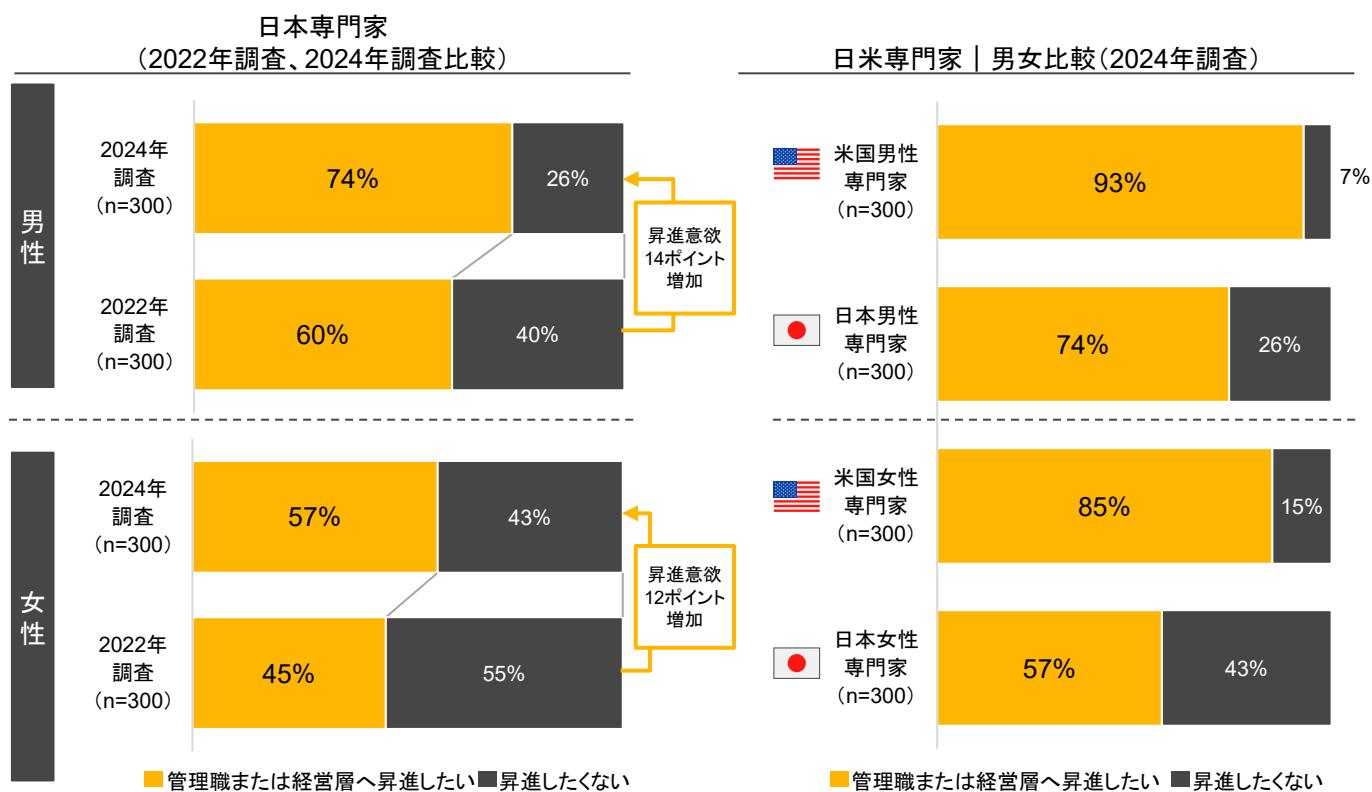
男女間で比較すると、「管理職または経営層への昇進意欲がある」と回答した米国男性専門家は93%、米国女性専門家は85%と双方高くなり、日本と異なり男女間の昇進意欲の差は8ポイントにとどまりました。

図表25: 管理職または経営層への昇進意欲(日米比較)



Q. あなたの今後のキャリアステップとして、経営層や管理職になりたいと思いますか？現在、管理職以上の方は今後も続けたいと思いますか。

図表26: 管理職または経営層への昇進意欲(男女比較)

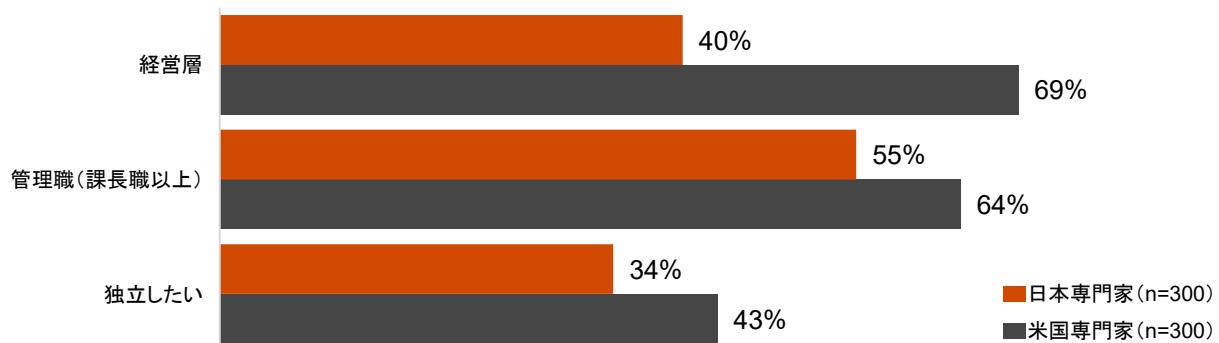


Q. あなたの今後のキャリアステップとして、経営層や管理職になりたいと思いますか？現在、管理職以上の方は今後も続けたいと思いますか。

■独立の意向

さらに、独立の意欲について分析すると、米国専門家では43%が独立したいと回答し、日本専門家は34%となり、各国男女間での差は特段確認されませんでした(図表27)。

図表27: 昇進の意向と独立の意向

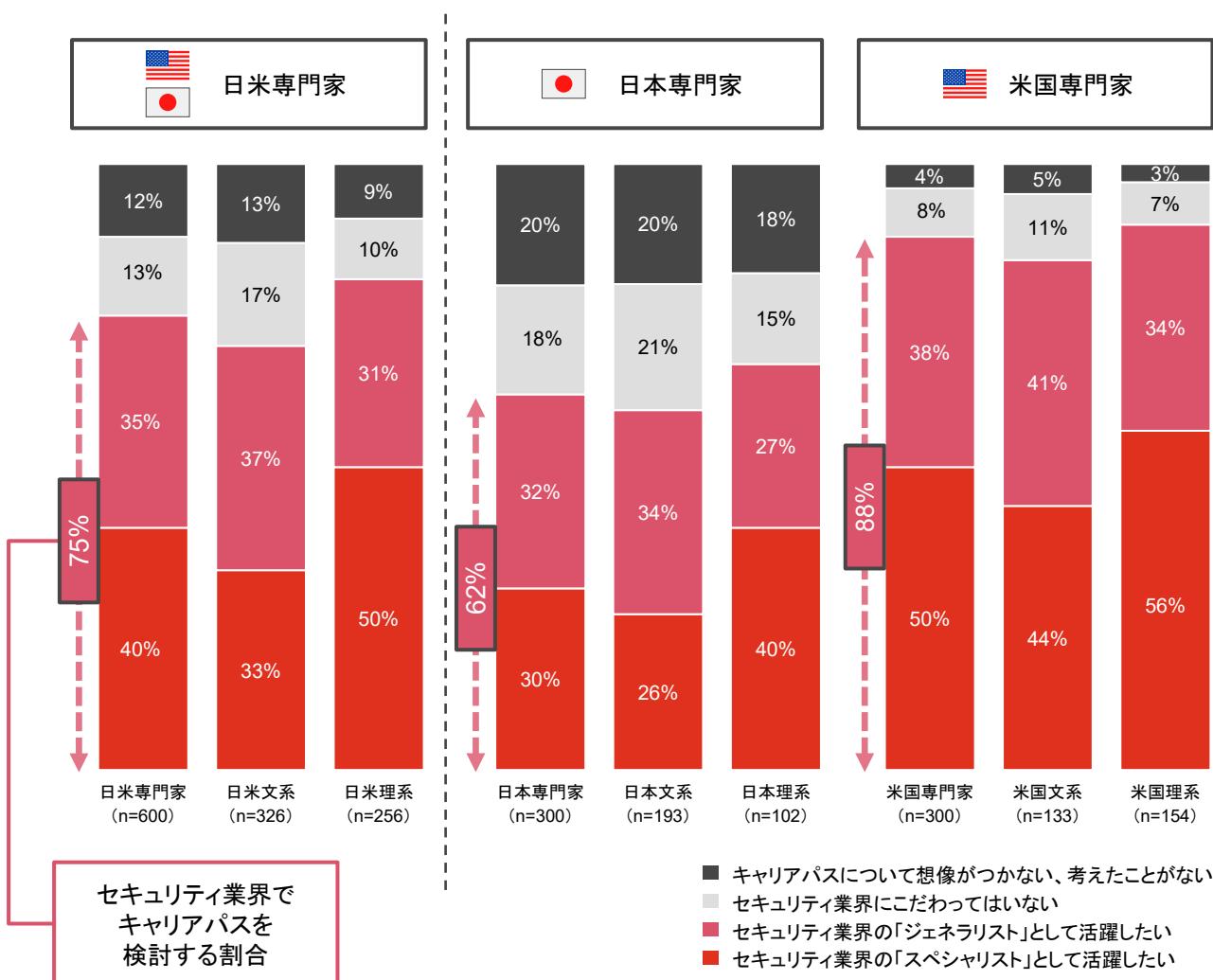


Q. あなたの今後のキャリアステップとして、経営層や管理職になりたい、または独立したいと思いますか。

■「スペシャリスト」「ジェネラリスト」への意向

日米専門家へ、セキュリティ業界でのキャリアパスについて検討状況を確認したところ、「セキュリティ業界でキャリアパスを検討している」と回答した割合は75%と多数派となり、そのうち「スペシャリスト」を目指す割合は40%、「ジェネラリスト」を目指す割合は35%となりました(図表28)。理系／文系出身グループで比較すると、理系出身専門家(n=256)は「セキュリティ業界でスペシャリスト」を目指す割合が多く半数を占め、文系出身専門家(n=326)の33%よりも17ポイント多くなりました。

図表28: 日米専門家の将来の意向: スペシャリスト／ジェネラリスト



Q. あなたが、セキュリティ業界で働くにあたり、将来のキャリアパスの意向で最もあてはまるものを教えてください。



■転職の意向

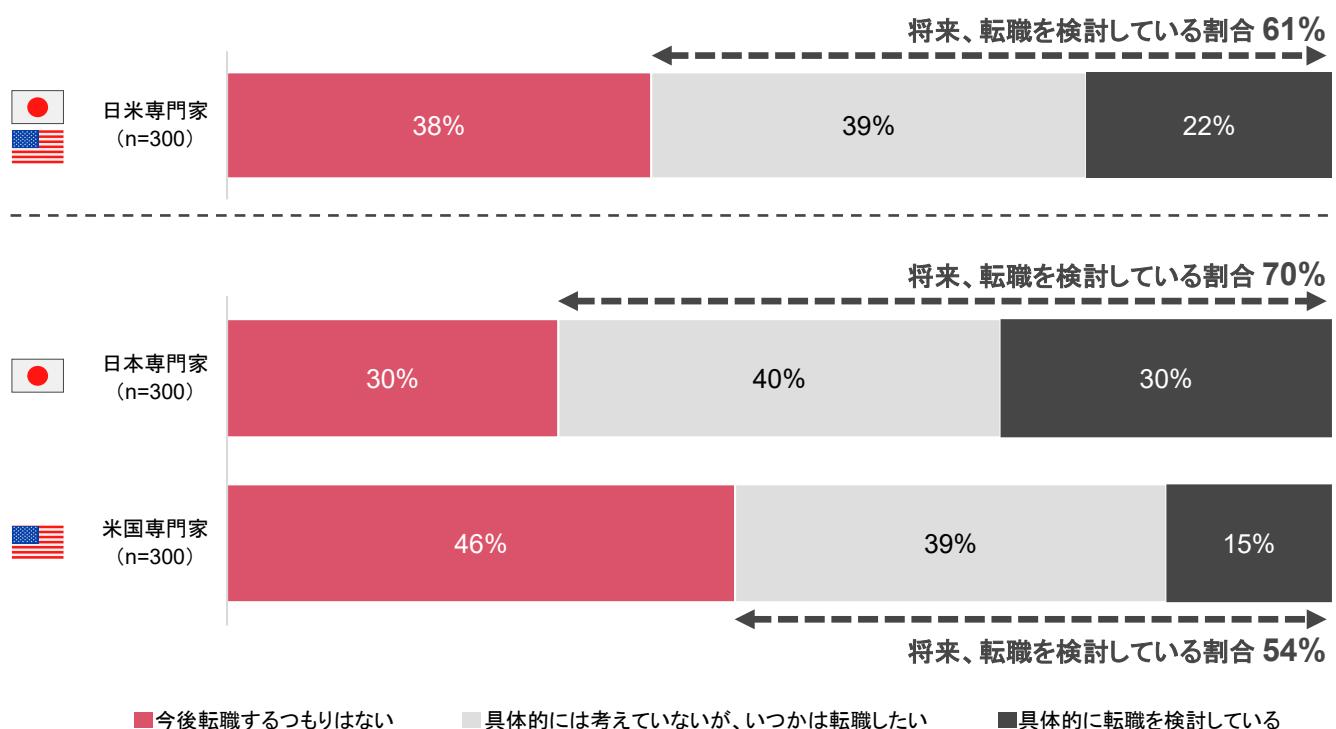
続いて、日米専門家へ転職の意向を確認すると「将来、転職を検討している」と回答した割合は約6割に上りました。この傾向は、米国専門家(約5割)よりも、日本専門家(7割)にやや強く意向が確認できました(図表29。なお、過去の「転職理由」および将来の「転職希望理由」はAppendix図表50をご参照ください)。

具体的にみると、日本専門家では「今後転職するつもりはない」と回答した割合は30%、「具体的には考えていないが、いつかは転職したい」が40%、「具体的に転職を検討している」が30%となりました。続いて、米国専門家では、「今後転職するつもりはない」と回答した割合は46%と高く、「具体的には考えていないが、いつかは転職したい」が39%、「具体的に転職を検討している」が15%となり、日本専門家より現在の企業でのキャリア構築を目指す専門家が多い傾向が確認されました。

日本専門家においては、初回業界調査⁴と比較すると、具体的に転職を検討する割合がやや増加傾向にあり、この背景には日本企業の終身雇用文化が徐々に薄れ、ジョブホップによりキャリア構築するモデルが浸透しつつあることがあるのではないかと推察します。

将来のキャリアとして、転職時にどのような経験を積むべきかも検討し、キャリアデザインしていくと良いでしょう。

図表29: 将来における転職の検討状況(日米比較)



Q. あなたの転職の意向を教えてください。

4. 初回業界調査では、日本専門家の転職意向は、「今後転職するつもりはない」「具体的には考えていないが、いつかは転職したい」「具体的に転職を検討している」がそれぞれ39%、23%でした。



(12) セキュリティ関連CxOを目指すなら、最も有益とする経験は「IT・セキュリティ実務」と「コンサルティング」

また、将来CxOレベルを目指す方においては、日米専門家は「IT・セキュリティ実務」や「セキュリティ関連のコンサルティング」経験が最も有益としていることが明らかになりました。なお、本項では、回答数の多かった米国専門家を主軸に置いてみていきます。

具体的にみると、「最高情報セキュリティ責任者(CISO)」を目指す上で最も有益とする経験は、米国専門家は「IT・セキュリティ実務」が最も高く66%(日本:32%)、続いて「コンサルティング(セキュリティガバナンス・エンジニアリングを含む)」が39%(日本:31%)、「コンプライアンス・法務」が37%(日本:25%)と続きます(図表30)。

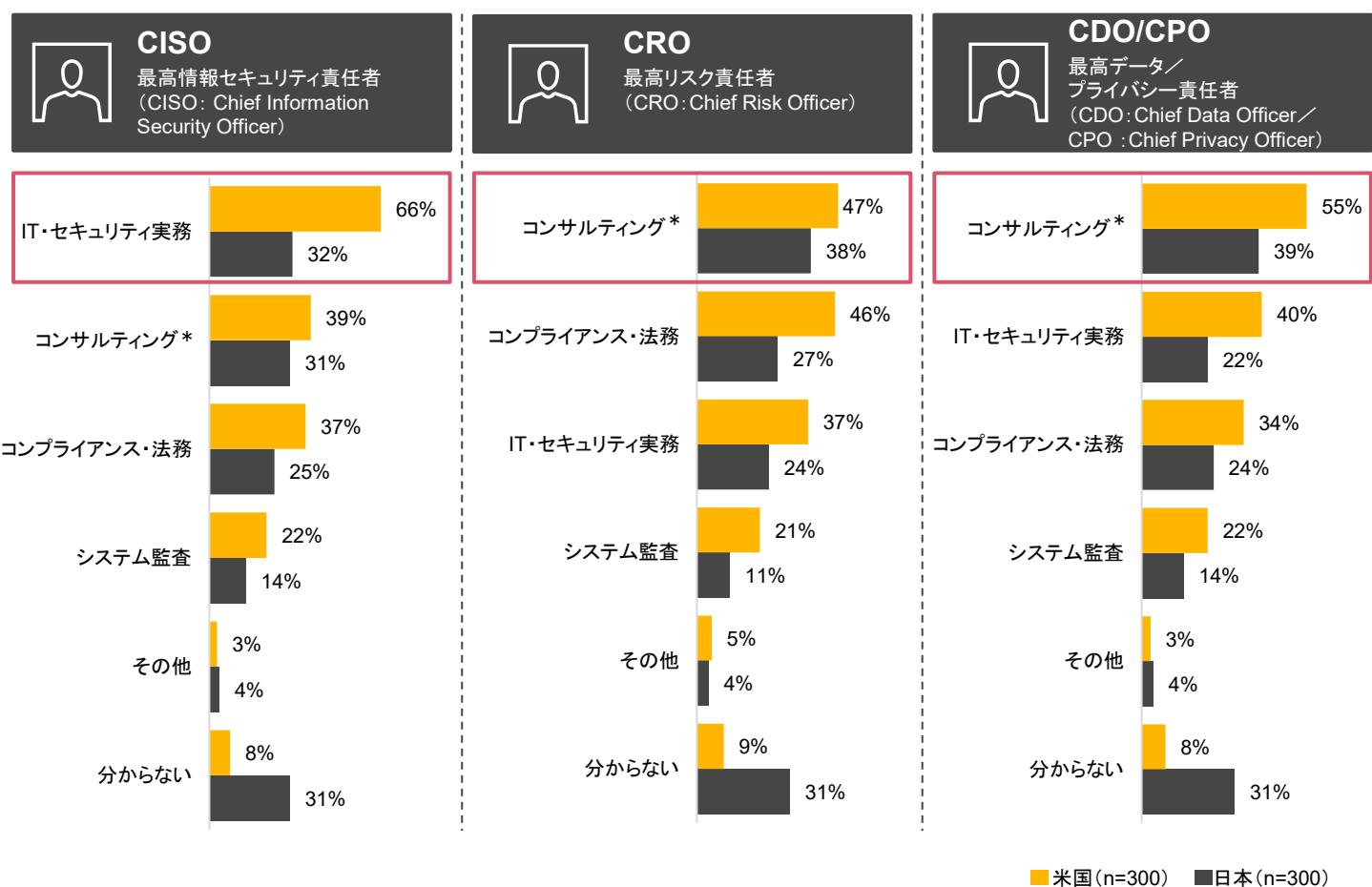
続いて「最高リスク責任者(CRO)」では「コンサルティング」が最も高く47%(日本:38%)、次いで「コンプライアンス・法務」が46%(日本:27%)、「IT・セキュリティ実務」が37%(日本:24%)となりました。「最高データ／プライバシー責任者(CDO/CPO)」においても、「コンサルティング」が最も高く55%(日本:39%)、次いで「IT・セキュリティ実務」が40%(日本:22%)、「コンプライアンス・法務」が34%(日本:24%)となりました。

特にCISOにおいて多くの米国専門家が「IT・セキュリティ実務」を選択した背景としては、実務経験がなく責任をとり・指示・判断することが難しいことや、多くのCISOキャリアモデルが存在することの他、米国投資家がCISOには実務経験者を評価傾向にあることから⁵、特に上場企業におけるCISO職へのキャリアモデルがある程度成熟していることがあると推察します。一方で、日本専門家は「分からない」を選択する割合が約3割と多く、CISOへのキャリアパスが見えづらい状況にありますが、今後、本業界を牽引する米国と同じようなキャリアモデルが日本でも構築されていくでしょう。

これらの傾向から、CISOやCRO、CDO/CPOの役職を目指す方で、「IT・セキュリティ実務」や「コンサルティング」業務が未経験である場合には、次のキャリアパスとしてこれらの業務経験を検討すると良いでしょう。

5. PwC「サイバーセキュリティおよびプライバシー情報開示」に関する日米投資家の意識調査2024
<https://www.pwc.com/jp/ja/knowledge/thoughtleadership/digital-trust-investor-survey2024.html>

図表30: 日米セキュリティ専門家が、CISO、CRO、CDO/CPOを目指す上で有利だと考える「セキュリティ業務経験」



Q. あなたは、セキュリティ人材がCISO、CRO、CDOなどの経営層を目指す場合、「どのような業務経験」があると有利と考えますか。それぞれあてはまるものを、全て教えてください。



3. 今後「セキュリティ業界」 を目指す学生や転職者 に向けたメッセージ

3. 今後「セキュリティ業界」を目指す学生や転職者に向けたメッセージ

日本でサイバーセキュリティ人材を多く輩出してきた大学教員から、今後セキュリティ業界で働くことを検討されている方々へメッセージをいただきました。

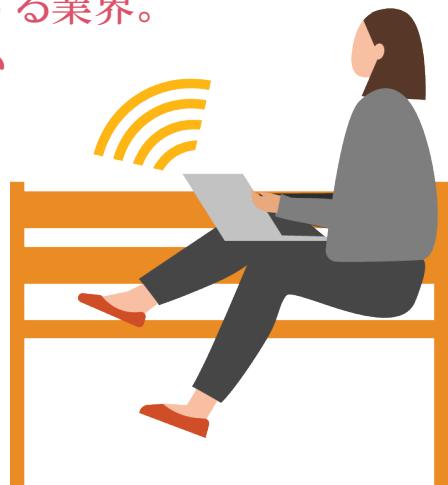
PwCコンサルティング合同会社（以下、PwCコンサルティング）のインクルージョン＆ダイバーシティ（I&D）リーダーであるSean King、林恵子、PwC Japan有限責任監査法人のインクルージョン＆ダイバーシティ（I&D）リーダーである綾部泰二からのメッセージと併せ、ぜひご覧ください。

Message



セキュリティ業界は文系の学生も活躍できる。
実態としても、理系より文系が多く就職する業界。
興味があればぜひチャレンジしてほしい

大学講師A氏



「セキュリティ業界は理系でないと就職できない」というイメージが今も学生の中に根強くあると感じています。このためか、文系の学生は「セキュリティ業界には行けない」と考え、職業選択から外す傾向にあります。しかし実際はセキュリティ業界へ就職する学生の半数以上が文系であることを伝えると、文系の学生たちから大きな反響があり、その気付きをきっかけに就職先の候補とする学生もいます。現在の学生は小中高等学校でプログラミング教育を受け、大学でも情報学が必修科目となっていることから、文系の学生でも基礎知識としてITやプログラミングについて学んでおり、セキュリティ業界で活躍できるポテンシャルを十分に持っています。「セキュリティ業界は理系でなければ目指せない」という考えは間違った固定観念であり、「セキュリティ業界は、文系も目指せる」ことを業界全体で訴求していく必要があると強く思います。

セキュリティ業界は非常に専門性の高い職種ではありますが、幅広い知識や多様な経験、人脈を持っていることが将来とも役に立つことの多い領域でもあります。「文系だから難しい」などとは考えず、興味があればぜひチャレンジしてみてほしいと思います。



Message

“

自分なりに興味や意義を感じることを大事にしてほしい

大学教授B氏



私たちの大学院では、ストレートマスター（大学卒業後すぐに大学院へ進学する学生）だけではなく、社会人学生としてセキュリティを学ぶ方多くいます。学びの目的の傾向としては、ストレートマスターの学生は「学部+α」の強みを培うためであることが多い一方で、社会人学生は自身の業務や生活の中でセキュリティに関する課題意識を持って研究を希望する方が多く、修了後の進路は、セキュアなシステム設計ができる技術者やビジネスコンサルタントなど多岐にわたっています。また、企業から派遣される形でご自身のキャリア強化や自社製品・サービス開発のために学ぶ方も多くいます。大学院という「場」は、バックグラウンドが異なる学生間でのディスカッションを通じて新たな気付きが芽生え、学生にとって刺激や学びになるものであり、卒業後も「意見交換できる多様なネットワークを持っている」ことが非常に大きな強みになります。

これからセキュリティ業界を目指す皆さんが大学院でキャリア強化を図られる場合においては、「自分なりに意義を感じる研究を見つける」ことが非常に大事だと思います。短期間で学位を取得することは決して容易ではない中で、自分が興味や意義を感じる研究を通して、学ぶことの楽しさやさまざまな発見を得ることが支えになるでしょう。



Message

“

困っている方たちと目線を合わせ支援ができる
専門家になっていただきたい

大学教授C氏



私の研究室はセキュリティ系の研究室のため、通信やセキュリティに興味がある学生が多いです。暗号理論から、システムや組織のセキュリティ等へと研究分野が変わる学生もいます。私自身は学際的に興味を持ち、どのような課題やリスクがあるかをみつけることが最も大事だと考えています。

就職においては、ハードウェアセキュリティ関連職種は一人の学生に対して多くの募集があり、就職に強みがあります。一方で、学生たちに人気の高い職種はセキュリティコンサルタントやAI、データサイエンス関連のセキュリティで、学生たちはさまざまな人たちや先輩の雰囲気をみて、自分が思い描くキャリアプランや楽しみを実現できそうな進路を決定している傾向にあります。

将来セキュリティ業界を目指す学生の皆さんには、悪意を持つサイバー攻撃者からの防御だけでなく、本当に困っている方たち、いわゆるセキュリティ弱者が置き去りにされないよう支援できる専門家になっていただきたいです。このためには、学生のうちから困っている人たちと目線を合わせることが重要です。



Message

“

技術を理解した上で、技術を世の中にどう使うのかという
一步引いた目線を養えるような学びや経験を積んでほしい。
きっと将来のキャリアパスが広がるはず

大学教授D氏



ここ数年で就職戦線の状況は大きく変わり、企業ではなく学生側が就職先を選ぶ立場、いわゆる売り手市場となりました。その中で、「セキュリティ業界からマネジメントへの感覚を磨き、コンサルティング業界に進む」というキャリアパスは学生にも認識されている王道のルートになりつつあります。

セキュリティ業界のキャリアパスは特定の技術を磨き上げた先にあるセキュリティエンジニアという方向性と、セキュリティ全体を見るジェネラリストという方向性があると思いますが、企業でセキュリティを任されるのは一般的に後者だと考えます。

これからセキュリティ業界を目指す皆さんには、大学での学びはもちろん、技術を理解した上で、技術を世の中にどう使うのかという、一步引いた目線を養えるような学びや経験を積んでいただきたいです。また、学生の間には企業に入ってからではできないつながりがあります。学内外問わず、将来同じ業界で働くであろう方たちとのつながりを大事にしてください。さらに、IT業界全体に言えることですが、特にセキュリティはインプットを怠ってはなりません。社会人になってからも自己研鑽を続けることがとても重要です。世の中やセキュリティに対するさまざまな見方を持つよう意識すると、将来のキャリアパスが広がると思います。



PwCのInclusion and Diversity(I&D)のセキュリティリーダーからのメッセージ

“

セキュリティ業界におけるダイナミックで充実したキャリア

“A Dynamic and Enriching Career in Cybersecurity”

Sean King(PwCコンサルティング セキュリティ&プライバシー I&Dリードパートナー)

セキュリティ専門家の需要は依然として高く、ある推計⁶によると350万件以上の求人が埋まっていないとされ、人材不足が大きな課題となっています。現在、世界のセキュリティ業界では男性が主流で、女性の労働力は全体のわずか25%にとどまります⁷。セキュリティ業界により多くの女性が参加することは、人材と需要とのギャップを埋める大きなチャンスだと確信しています。

不思議なことに、セキュリティ業界には依然として偏見があります。メディアは、この業界は技術者と謎めいた元ハッカーだけで構成されているというステレオタイプを誇張する傾向にあります。これは非常に多様な側面を持つセキュリティという職業に対する限定的で時代遅れの見方と言わざるを得ません。

セキュリティ業界は「新しいキャリア」を求める男女にとって素晴らしい選択肢の1つです。戦略、コンプライアンス、リスク管理、ガバナンス、人材、プロセス、そしてデータとテクノロジーを網羅する豊かな領域です。さらに、サイバーは非常に動的であり、現在の出来事や地政学的状況と密接に関連しています。セキュリティ業界でのキャリアを通じて得られる幅広い知識やスキル、経験はあなたのキャリアを大いに前進させることができます。ぜひセキュリティ業界でのキャリアを検討してみてください。

The growing need for cybersecurity professionals continues to be a huge issue. By some estimates there are more than 3.5 million cyber security jobs unfilled. The field continues to be dominated by males. Currently women make up only about 25% of the cybersecurity workforce globally. There is a huge opportunity to bridge the talent gap by involving more women in the arena of cybersecurity.

Oddly enough, there is still a stigma with cybersecurity. The media continues to perpetuate stereotypes that represent the industry as one consisting of only techies and mysterious ex-hackers. However, this is a pretty narrow and antiquated view of an extremely diverse profession.

Cybersecurity is a great option for women seeking a new career. It's a rich domain which encompasses strategy, compliance, risk management, governance, people, and process, as well as data and technology. What's more, cyber is very dynamic and closely aligned with current events and the geopolitical landscape. The broad range of knowledge, skills, and exposure you will gain through a cybersecurity career can take you very far. We encourage you to have a look.

6. Cybersecurity Ventures, "Cybercrime Magazine: Cybersecurity Jobs Report: 3.5 Million Unfilled Positions In 2025" (2023/4/14)
<https://cybersecurityventures.com/jobs/>

7. ISC2, "Women in Cybersecurity: Women in the Profession" <https://www.isc2.org/Insights/2024/04/Women-in-Cybersecurity-Report-Women-in-the-Profession>



“

社会全体から期待される 『セキュリティ人財』としての活躍

綾部 泰二(PwC Japan有限責任監査法人 I&Dリードパートナー)

皆さん、セキュリティ業界での仕事に対してどのようなイメージを持たれているでしょうか？何か特別なスキルを持った人たちによる特殊な仕事というイメージを持たれていないでしょうか？確かに専門家による仕事なのですが、セキュリティにはさまざまな分野があり、それぞれの専門家がいます。例えばセキュリティ技術に強いエンジニア、サイバーリスクを可視化するリスクの専門家、またリスクマネジメントを実現するために必要なルールやガバナンスを確立するガバナンスの専門家等々の分野があり、多様なバックボーンの方が活躍するフィールドがあります。

一方ビジネス面を鑑みると、私たちの業務は止まることなくデジタル化されていき、安心・安全に業務を遂行していくためにサイバーセキュリティは必要不可欠な領域となっています。また業務だけでなく、私たちの生活もデジタル化が進んでいることから、セキュリティ人財の活躍は社会全体から期待されるところです。

しかしながらセキュリティという領域で、特に日本では人材不足であると言われて久しい状況です。

社会全体から期待され、さまざまなバックボーンを持つ方が活躍できるセキュリティという領域に、多くの方に興味を持っていただき、セキュリティの専門家をしていただければ幸いです。



“

多様な人材が志高く参画する セキュリティ業界を目指して

林 恵子(PwCコンサルティング テクノロジー&デジタルコンサルティング／トラストコンサルティング部門I&Dリードシニアマネージャー)

サイバーセキュリティとプライバシーの業界のキャリアについて、この業界のリーダー位置にあるPwCコンサルティングとして、今回もこのような発信ができるこをたいへん嬉しく思います。

セキュリティ業界ではテクノロジーによるイノベーションも日々推進されていますが、そのイノベーションを起こす源泉となるのは「人」です。セキュリティ業界でのキャリアが皆さんにとって魅力的なキャリアであることをお伝えすることで、今後日本でもグローバルでも重要となるセキュリティ分野に多くの人が参画してくださることを期待しています。

また日本ではまだまだ道半ばのI&Dを推進する一人として、キャリア・性別・専攻を超えた多様な人材が志高くセキュリティ業界に参画し、よりイノベーティブな社会となるよう、お手伝いしていけたらと思っています。



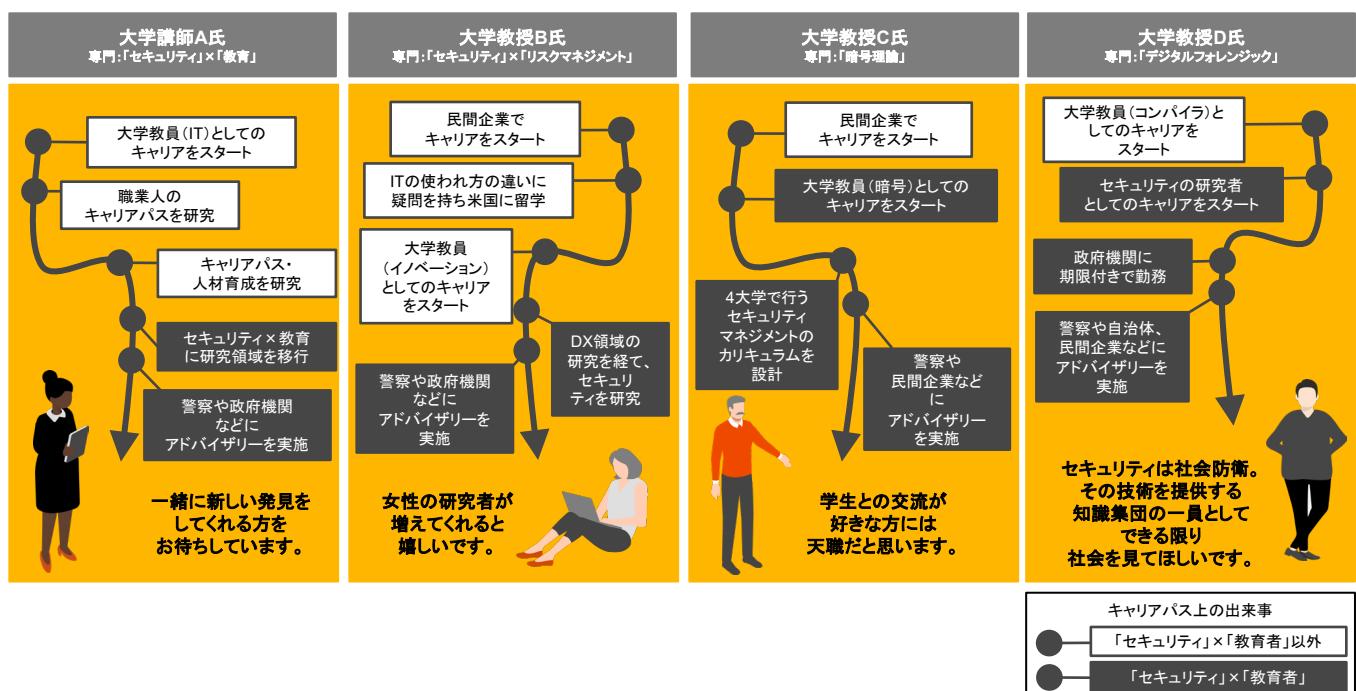
4. 国内大学における 「セキュリティ教育者」の キャリアパス



4. 国内大学における「セキュリティ教育者」のキャリアパス

セキュリティの専門家の需要が高まり、人材の育成を担う次世代の大学教授・講師の人材不足も日本のセキュリティ業界における課題となりつつあります。そこで、2024年業界調査では、初の試みとして日本でサイバーセキュリティに携わる大学教員4名にキャリアパスについてインタビューを行いました(図表31)。本章が大学教員としてのキャリアを目指すきっかけとなれば幸いです。

図表31:サイバーセキュリティ人材育成を担う大学教員4名のキャリアパス



セキュリティ教育に携わるきっかけや経緯はそれぞれ異なるものの、今回のインタビューから興味深い共通点が確認できました。

■インタビューから確認できた「セキュリティ教育者」のキャリアパスの傾向

- ① ITやイノベーションなどの強みを生かしてセキュリティへキャリアパスを移行した
- ② 民間での社会人経験や他分野での研究経験がセキュリティの大学教員のキャリアパスにポジティブな影響を与えている
- ③ 「学生とともに新しい発見をすること」「学生を後押しできること」を大学教員のやりがいや楽しみとして挙げている
- ④ 大学での授業や研究以外に、警察や国の機関のアドバイザリーや民間企業のインシデント委員会などの社会貢献活動をしている

図表32:「セキュリティ」×「教育者」のキャリアパスの傾向

01 ITやイノベーションなどの強みを生かしてセキュリティへキャリアパスを移行した

学生時代の経験やキャリアパスを構築する中で獲得した強味をベースとして、セキュリティ領域へキャリアの軸を移行した

02 民間企業での経験や他分野での研究経験がキャリアパスにポジティブな影響を与えている

民間企業での経験や、研究者としてセキュリティ以外の分野を研究した経験が、現在の研究領域や大学での教育プログラムの設計等で役立った

03 「学生とともに新しい発見をすること」「学生を後押しできること」がやりがいや楽しみ

大学教員は学生とのやり取りから新たな気づきを得るなど、大いに刺激を受けて研究を行っている他、学生たちが新しいもの・考えを生み出す際の手伝いができる

04 大学での授業や研究以外で社会貢献活動に携わっている

社会貢献活動として警察や国の機関等でのアドバイザリーや、民間企業でのインシデント委員会などの活動をしている

傾向から推測される
大学教員に向いている方

- 学生との交流があるキャリアを送りたい方
- 知的好奇心の高い方
- 社会貢献に関心のあるセキュリティ専門家
- セキュリティ分野以外のバックグラウンドを持つ方や社会人経験のある方



— 大学における「セキュリティ教育者」というキャリアパスに至る経緯 —

今回のインタビュー調査で特筆すべき点は、国内大学における「セキュリティ教育者」は4名中2名が民間企業でキャリアをスタートさせていたことです。また、4名中3名が大学教授としてのキャリアを歩み始めた段階では「セキュリティ」に特化しておらず、「IT」や「イノベーション」、「コンパイラ」といった分野から、徐々にセキュリティへと研究領域を移行していました。

加えて、研究領域が他分野からセキュリティへと移行した大学教員はいずれも、他分野での研究経験が、自らの研究においてさまざまな視点の獲得などのポジティブな影響を与えていたと考えていました。また、民間企業での勤務経験から、セキュリティ担当者が技術用語を使わずに経営層などとのコミュニケーションを取る必要性を感じ、セキュリティ教育のカリキュラム設計にセキュリティマネジメントを反映した例も確認できました。

これらのことから、民間企業での経験や他分野での研究経験が「セキュリティ」×「教育者」のキャリアパスにポジティブな影響を与えていると言えるでしょう。したがって、民間企業等で社会人経験を積んだ方や他分野の研究者にとって、セキュリティ教育者のキャリアパスは大いに活躍の可能性がある選択肢の1つとなりそうです。

— 大学教員の活動・やりがい —

大学教員の主要な取り組みの1つである「学生の育成」については、「学生一人一人の伸びしろが面白い」「学生たちが新たなもの・考え方を生み出すのをサポートできるのが一番の楽しみ」「学生との関わりやその中で受ける刺激が教員の新たな気づきや研究につながっている」といった意見がありました。また、「世の中の変化を学生の変化を通してみることで、10年先の課題を先読みできることは、研究者としても教育者としても面白いと感じる」といった声もありました。これらから、学生の成長をサポートすることそのものが楽しみややりがいになっているとともに、教員も学生から刺激を受けて自身の研究を進めていくと言えそうです。



インタビュー対象者は、教職の他にも、警察や自治体のセキュリティアドバイザリーや政府機関等のセキュリティ関連の委員会への参加、民間企業でのインシデント発生時に外部有識者として知見の提供などさまざまな社会貢献活動をしており、社会全体のセキュリティレベルの向上などに寄与していることが確認できました。このことから、社会貢献活動を重視するセキュリティ専門家や学生は、大学の教員というキャリアパスも視野に入れられるかもしれません。

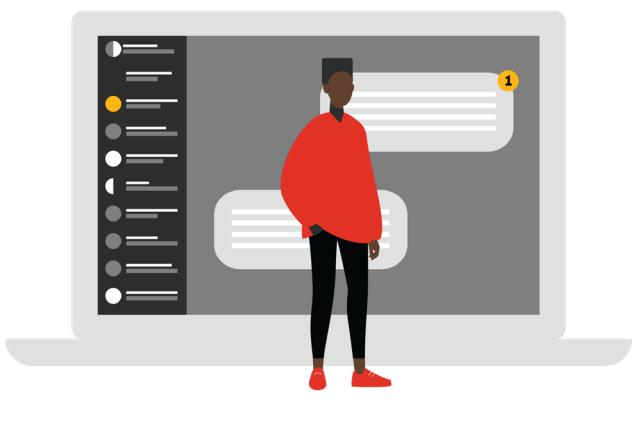
—これから「セキュリティ」×「教育者」のキャリアパスを目指す方に向けて—

大学教員はセキュリティ専門家を育成する重要な役割を担うものの、志望者が少なく、現職の大学教員でも、いわゆる団塊世代が退職する時期を迎えつつあります。そのような中で、次の世代に「日本のインターネットを作ってきた世代」からバトンをつながなくてはならない、といった危機感も教育現場にあるようです。

大学教員に向いている方

セキュリティに関しては、領域の新しさから「開拓されきっていない領域」であるとともに、今日の日進月歩の技術革新により、「常に新しくなっていく領域」でもあります。今回インタビューを実施した教員からは「先が見えないからこそ面白い」といった意見も出ました。また、教職以外に外部有識者としての活動など社会貢献活動も行っているなど、セキュリティ分野以外での経験や社会人経験が生かせるキャリアパスであることも今回のインタビューからみえてきました。

このことから、「学生を育てたい」「次の世代に技術などを伝えたい」といった志のある方や、「新しいことを発見したい」といった知的好奇心の高い方、社会貢献を重視するセキュリティ専門家、セキュリティ分野以外でのバックグラウンドを持つ方、社会人経験のある方にとって、大学教員は希望を叶える職種と言えるでしょう。



大学教員を目指す方への推奨事項

「博士号の取得」については、「セキュリティ」×「教育者」のキャリアパスを目指す方々はどのような取り組みをしておくとよいのでしょうか。

今回のインタビューから「博士号を取得する」という共通のアドバイスがありました。博士号は自らの専門性を第三者が評価するための指標と言え、特に海外では博士号の取得有無によりコミュニケーションの取り方に差異があるそうです。社会人学生が博士号を取得するために仕事と両立させる生活を送るのはハードな印象があるかもしれません、仕事での取り組み 자체が論文の題材として十分であり、適切に論文にまとめれば短期間での学位取得も可能といった、社会人ならではのチャンスがあることも明らかになりました。

今回インタビューを実施した教員のキャリアパスからも傾向がみられるように、大学卒業後、大学院へ進学しそのまま研究者・教育者としてのキャリアを積む以外に、社会人経験を経て大学教授になるというキャリアパスもあります。

今後、皆さんのキャリアパスに大学における「セキュリティ教育者」の選択肢が入れば嬉しく思います。



5. おわりに



5. おわりに

今回の調査で、セキュリティ業界は、同業界を世界的に牽引する米国および日本において、最終学歴が「文系」「理系」出身者双方とも活躍する業界であることが、データとして裏づけられました。また、ロールモデルを持つグループの約8割は、自身の業務に「やりがい」「楽しさを感じ、「長く働きたい」と考えています。

セキュリティ業界は、他業界に比べて歴史が浅いことから、残念ながらキャリアパスやキャリアモデルが成熟していません。ですが、これは裏を返せば、あなた自身で日本のセキュリティ専門家のキャリアモデルをつくれる業界であるとも言えます。皆さんにセキュリティ業界を就職先の1つとしてご検討いただければ、心より嬉しく思います。

就職先を検討されている学生の皆さんへ

セキュリティ業界には、理系出身だけでなく文系出身の学生も多く就職しています。文系の学部を専攻している学生の皆さんにもぜひ一度、就職先の1つとしてセキュリティ業界をご検討いただければ幸いです。

PwC Japanグループにおいても、語学(外国語)、国際関係、法律関係の学部出身者を中心に、多くの文系出身の専門家が活躍しています。セキュリティ業界は、国を超えるサイバー攻撃や、データに関する国をまたいだ法規制など、目まぐるしく変化する動向に対応することが求められます。そのため、グローバルに活躍できる仕事やグローバルな犯罪者から人や社会を「守る」仕事が数多くあります。

調査結果からも分かるように、「専門性を高めたいや新しい知識やスキルを身に付けたい」方、「社会貢献したい」方、「正規雇用や安定した雇用」を求める方は、その希望をセキュリティ業界で叶えることができます。

あなたのやりたいことを「セキュリティ専門家」や「プライバシー専門家」として叶えていきませんか。セキュリティ業界自体の歴史はまだ浅く、頑張り次第では「あなた」が、セキュリティ業界の第一人者となれる可能性を秘めています。



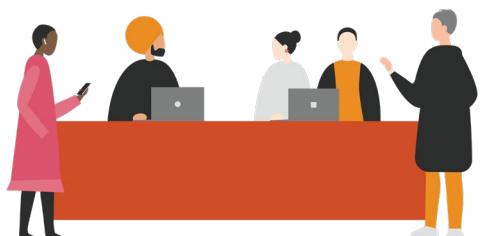
転職を検討している、または転職活動をされている皆さんへ

日本におけるセキュリティ業界は正規雇用率が9割超⁸と高く、「専門スキルを得られた」「売り手市場である」と実感できる、転職先として魅力のある業界の1つです。

また、今回の調査から、セキュリティ業界で働く専門家の過半数が「非IT部門」であり、営業や人事、総務などからの転身者であることが明らかになりました。実際、PwCコンサルティングにおいても「[Talents in Cyber Security and Privacy](#)」で紹介されているとおり、営業やマーケティング、法務など非IT部門出身専門家が数多く活躍しています。現在「IT部門」で活躍されている方はもちろん、「非IT部門」に所属されている皆さんもご活躍いただける業界と言えます。

特にセキュリティ業界の経験がなくても、「製造業には詳しい」「金融業には詳しい」といったスペシャリティがあるのであれば、それに「セキュリティ」をかけ合わせることで、セキュリティ業界における「×製造業」や「×金融業」のスペシャリストとして、他者にはない自分だけの専門領域を築くことができます。

「自分だけの専門領域」を持つことで、国内における先駆者、ひいては世界的な先駆者として活躍できる未来が切り開けるでしょう。皆さんのご活躍を心より期待しています。



8. 図表38参照

6. アンケート調査概要



6. アンケート調査概要

調査名 サイバーセキュリティおよびプライバシー業界における多様なキャリアパス実態調査2024

調査対象	<ul style="list-style-type: none">・ サイバーセキュリティまたはプライバシー関連業務従事者・ 日本または米国在住者・ 所属組織:従業員規模300名以上・ 部署:取締役会、営業、事業部門、総務、事務、人事、広報、調達、内部監査、経営企画、労務管理、法務、コンサルタント、アナリスト／研究者、プリセールス、システム開発、パッケージ・ソフト・ミドルウェア開発、ネットワーク設計・構築、運用／監視／テクニカルサポート／保守、研究／特許／テクニカルマーケティング／品質管理、データベースシステムネットワーク、アプリケーション開発、情報セキュリティ、ヘルプデスク、セールスエンジニア、その他・ サイバーセキュリティまたはプライバシー関連業務での業務経験:1年以上
調査期間	<ul style="list-style-type: none">・ アンケート調査:2024年1月9日(火)～2024年1月18日(木)・ インタビュー調査:2024年4月17日(水)～5月10日(金)
調査方法	<ul style="list-style-type: none">・ インターネットにおけるアンケート調査・ インタビュー調査
アンケート回答者数	600名 (米国:男性150名、女性150名、日本:男性150名、女性150名)



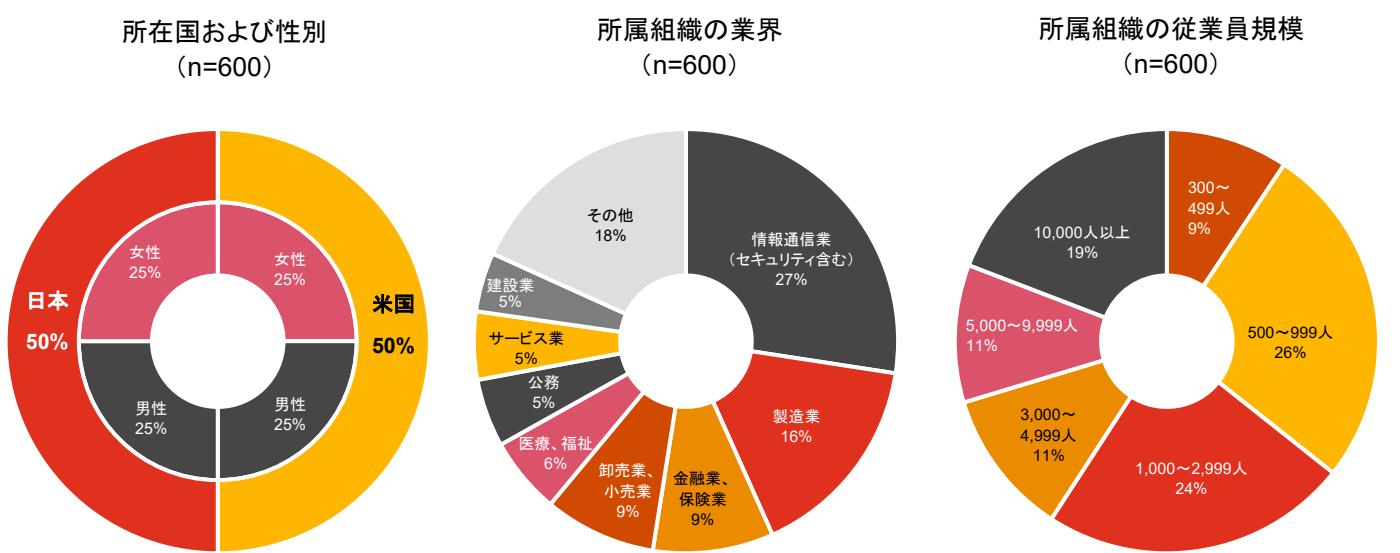
Appendix: 回答者の属性とその他のデータ



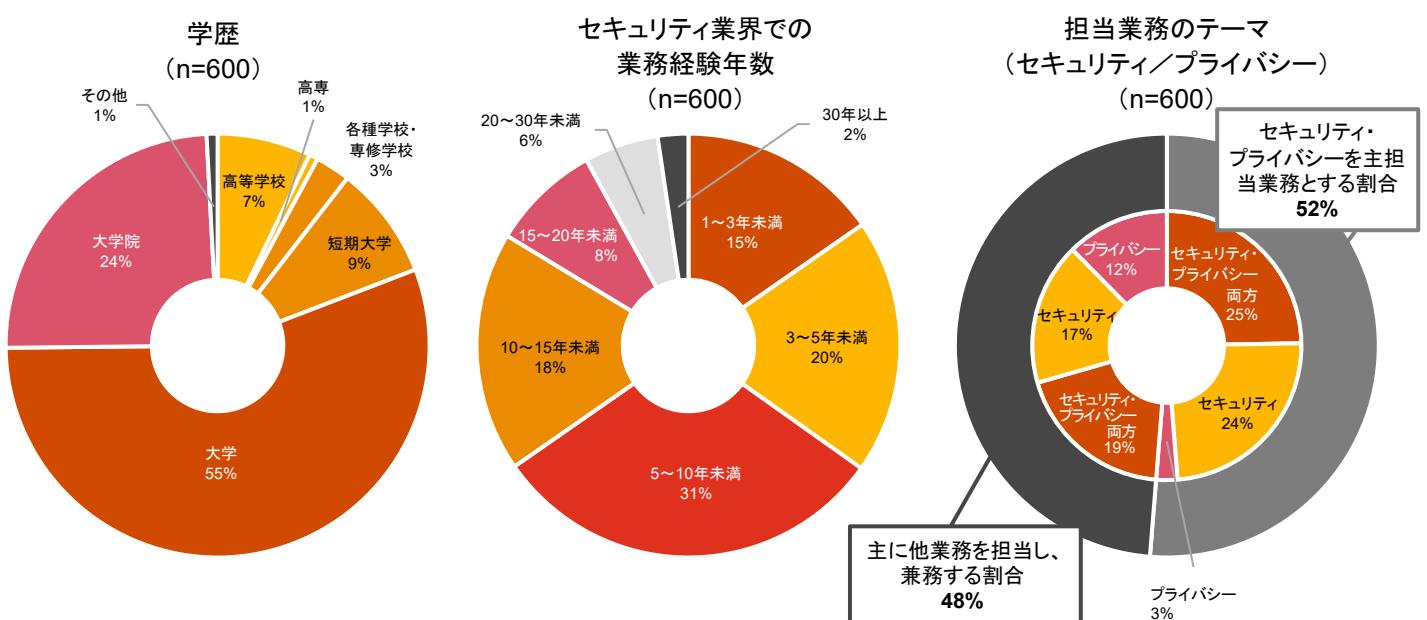
a) 回答者の属性

今回のアンケート調査では、セキュリティ業界で働く日米専門家各300名、計600名から回答を得られました。回答者の属性データ(図表33)をみると、所属組織の業界は情報通信業(セキュリティ含む)が最も多く、製造業、金融・保険業、卸売・小売業が上位を占め、所属組織の従業員規模は1,000名を超える組織が全体の65%を占めます。また、回答者の最終学歴は大学・大学院卒が全体の約8割となっています(図表34)。回答者の勤務地については、日本は東京都が最も多く、米国ではさまざまな州に分散していることが分かります(図表35)。また所属組織の属性(図表36)、所属部署(図表37)、現在の雇用形態(図表38)の割合は記載のとおりです。

図表33:回答者の属性①所在国および性別、所属組織の業界、所属組織の従業員規模

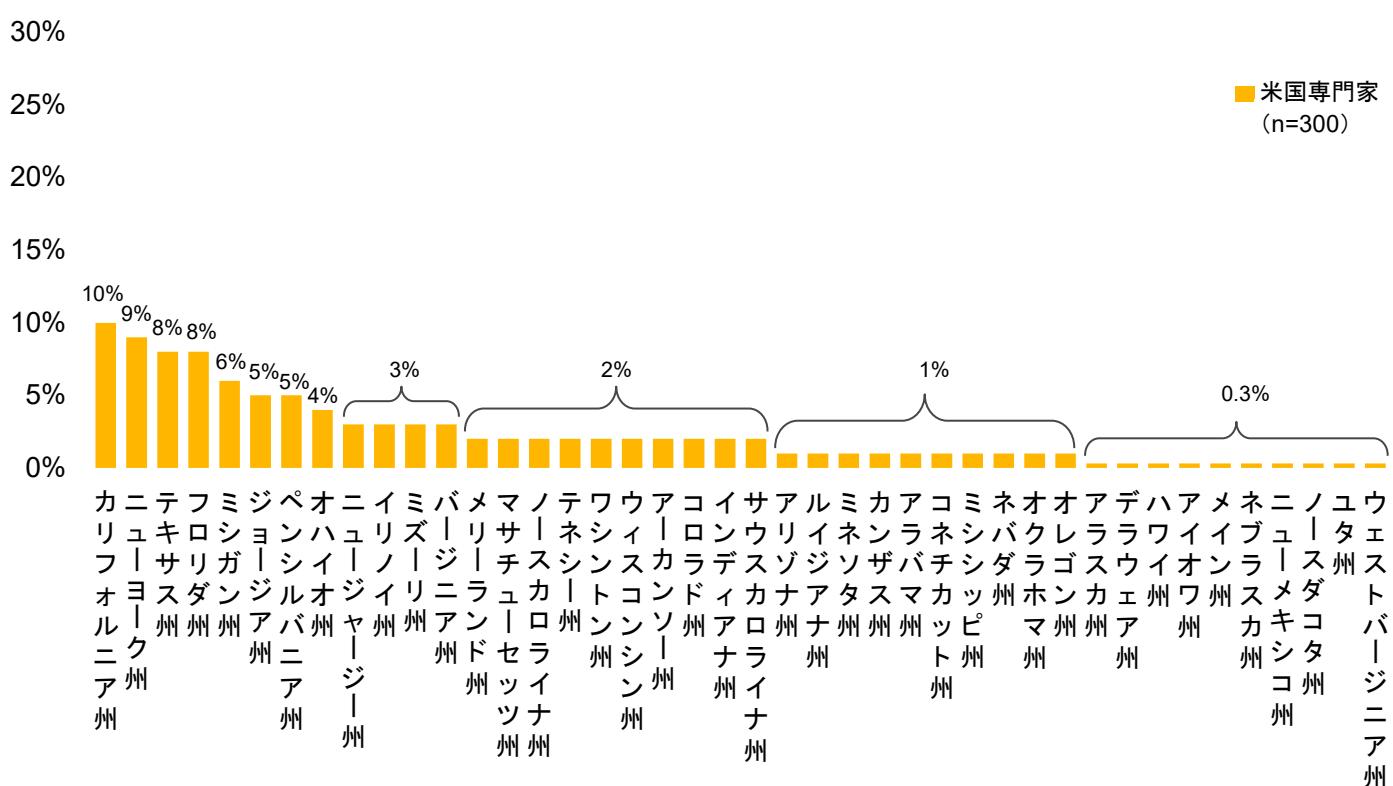
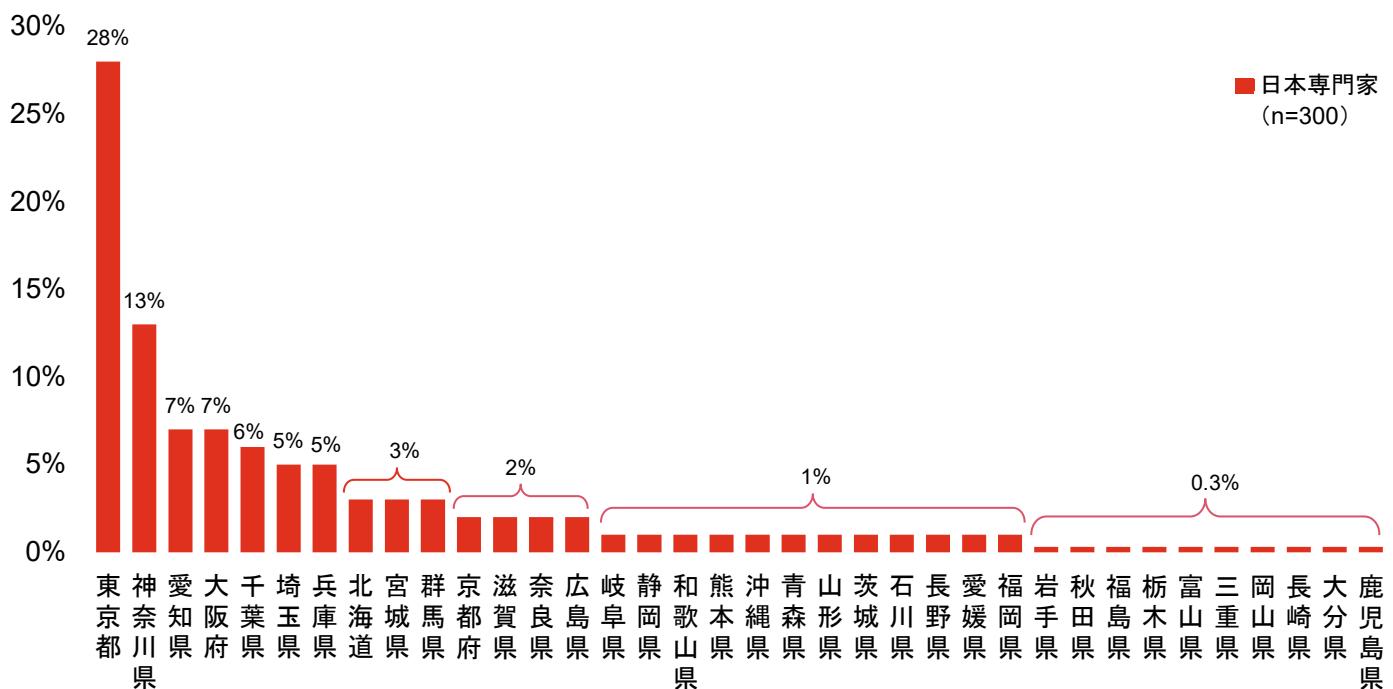


図表34:回答者の属性②学歴、業務経験年数、業務のテーマ

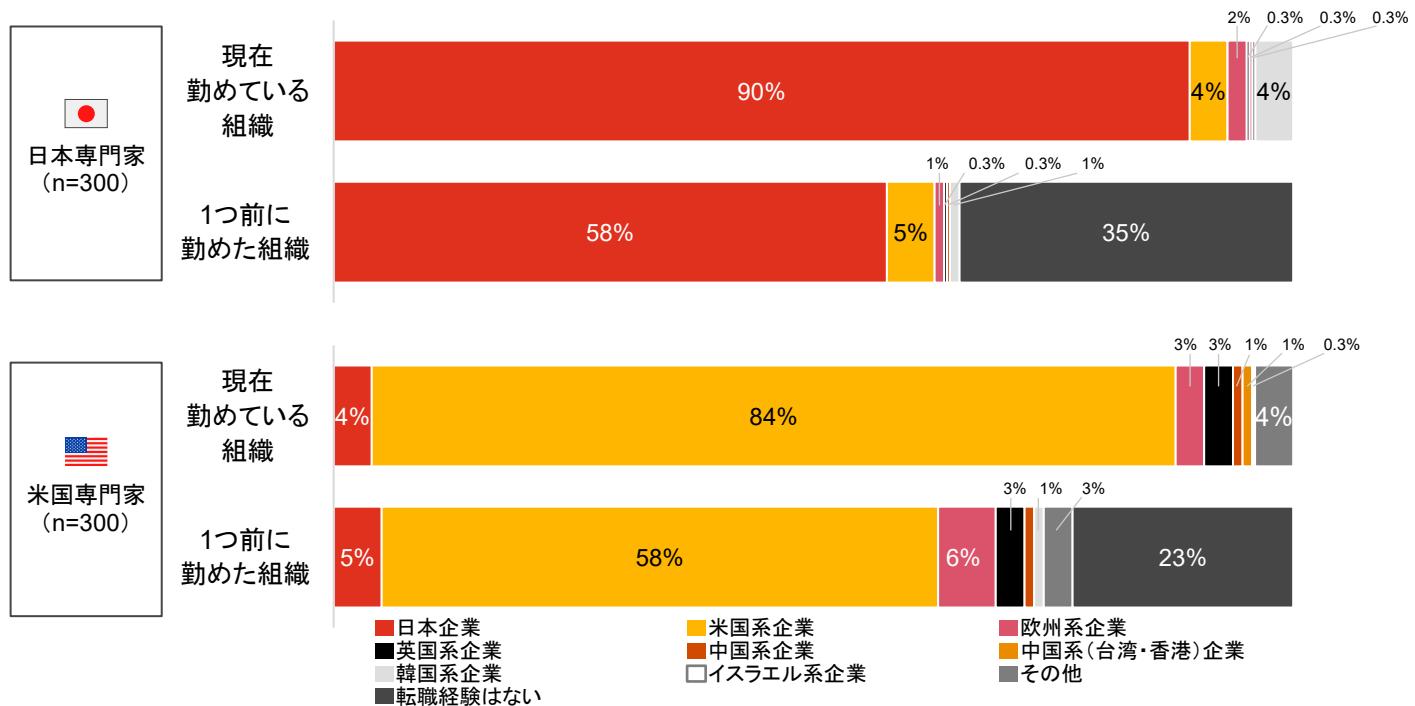




図表35:回答者の属性③勤務地(日本・米国)



図表36:回答者の属性④所属組織の属性(日米:過去・現在)

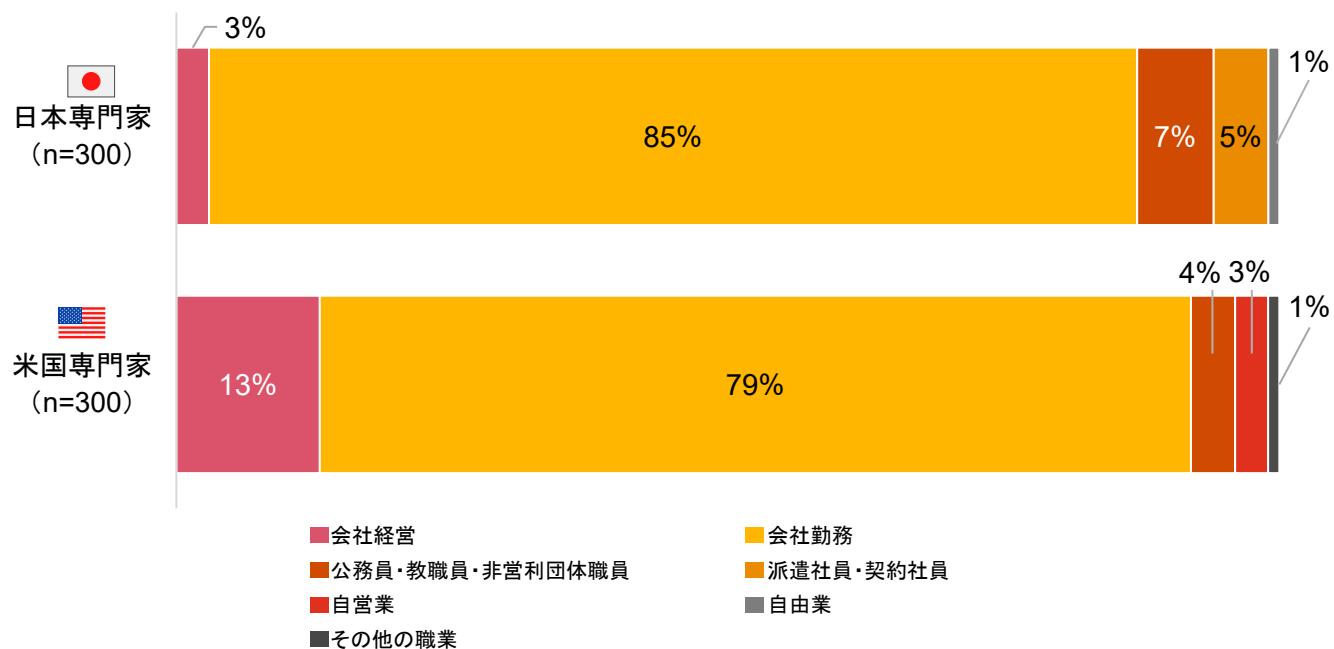


図表37:回答者の属性⑤所属部署

		営業	総務	事務	セキュリティ	情報	人事	事業部門	(経営層)	取締役会	テクニカルサポート/運用/監視/保守	システム開発	セールス	エンドユーザー	経営企画	通信インフラ	設計・構築	法務	パッケージソフト
日本	文系	文系	21%	15%	8%	7%	7%	5%	5%	5%	5%	4%	3%	3%	3%	2%	2%	2%	
		理系	7%	4%	9%	20%	1%	5%	4%	4%	4%	14%	2%	0%	3%	0%	4%	4%	
米国	文系	文系	8%	7%	11%	14%	8%	5%	8%	3%	3%	2%	0%	2%	2%	4%	4%	2%	
		理系	3%	2%	5%	34%	4%	5%	10%	3%	3%	5%	0%	1%	3%	1%	1%	2%	
		設計・構築	ネットワーク	データベース、システム	アプリケーション	労務管理	研究者	アーリースト/アナリスト	プリセールス	内部監査	ヘルプデスク	コンサルタント	調達	広報	研究/マーケティング/品質管理ほか	特許/技術/テクニカル	その他の職種		
日本	文系	文系	2%	1%	1%	1%	1%	1%	1%	1%	1%	0%	0%	0%	0%	7%			
		理系	4%	3%	1%	1%	1%	1%	0%	0%	0%	2%	2%	1%	1%	8%			
米国	文系	文系	2%	2%	2%	2%	2%	0%	0%	2%	1%	2%	4%	1%	2%	7%			
		理系	1%	5%	2%	1%	1%	0%	1%	1%	1%	5%	2%	2%	1%	2%			

■ : 30%以上 ■ : 20~29% ■ : 10~19% ■ : 5~9% ■ : 1~4% ■ : 0%

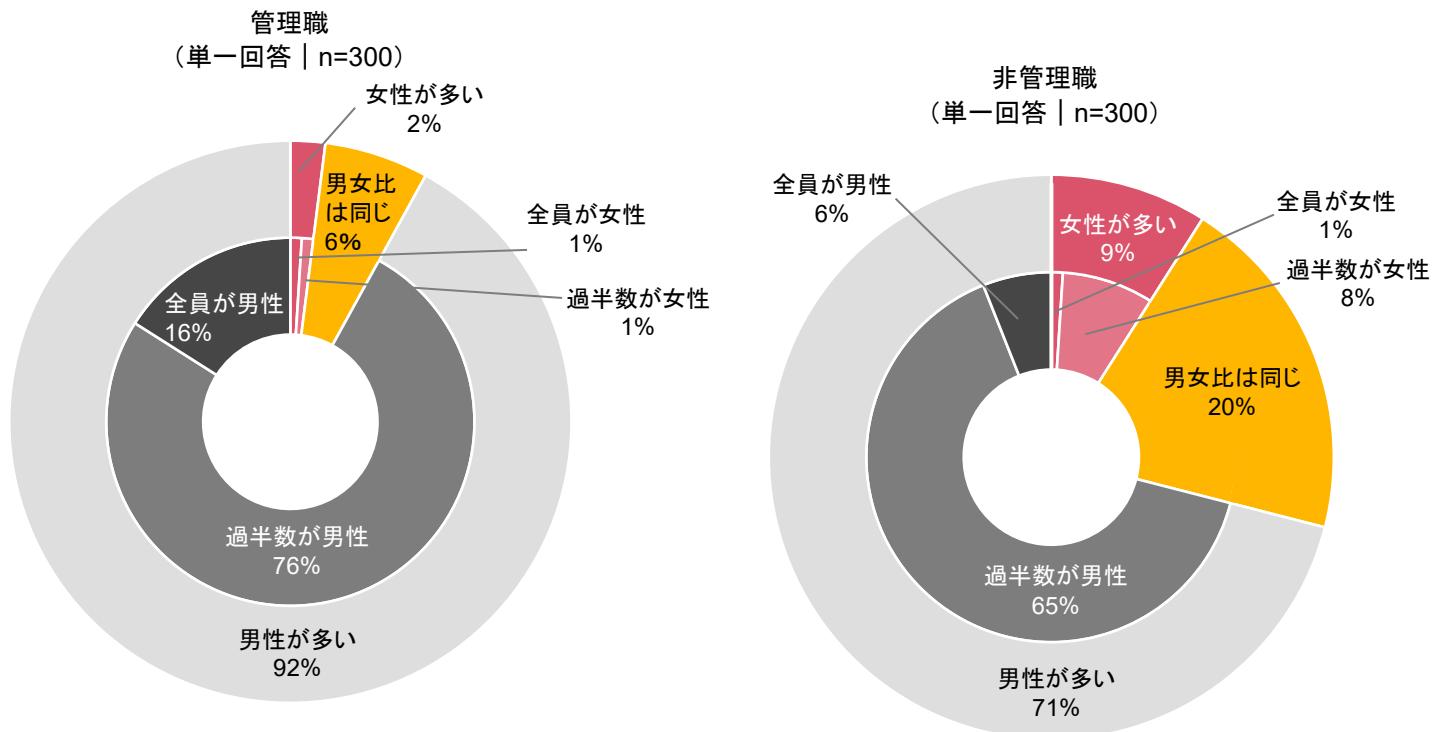
図表38:回答者の属性⑥現在の雇用形態



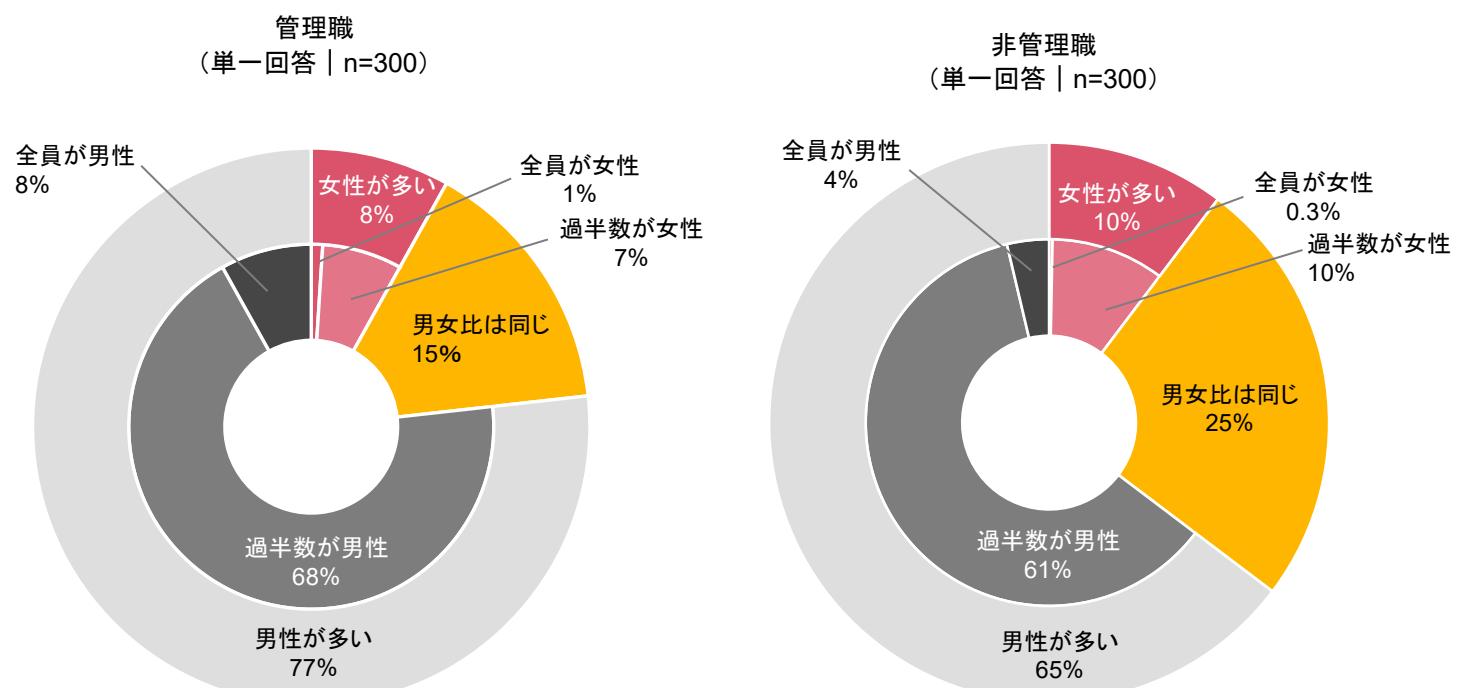
b) その他のデータ

本調査で得られた関連データを記載します。必要に応じてデータポイントとしてご活用ください。

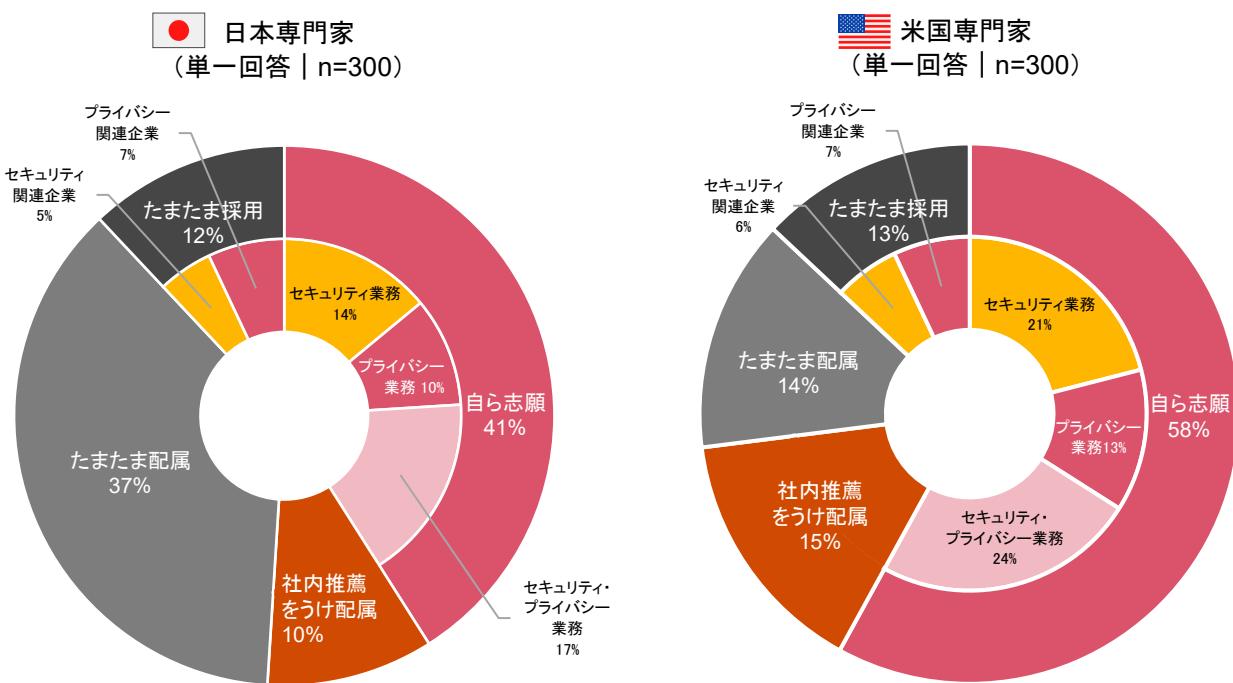
図表39:セキュリティ業界で働く女性の割合(管理職、非管理職)(日本)



図表40:セキュリティ業界で働く女性の割合(管理職、非管理職)(米国)

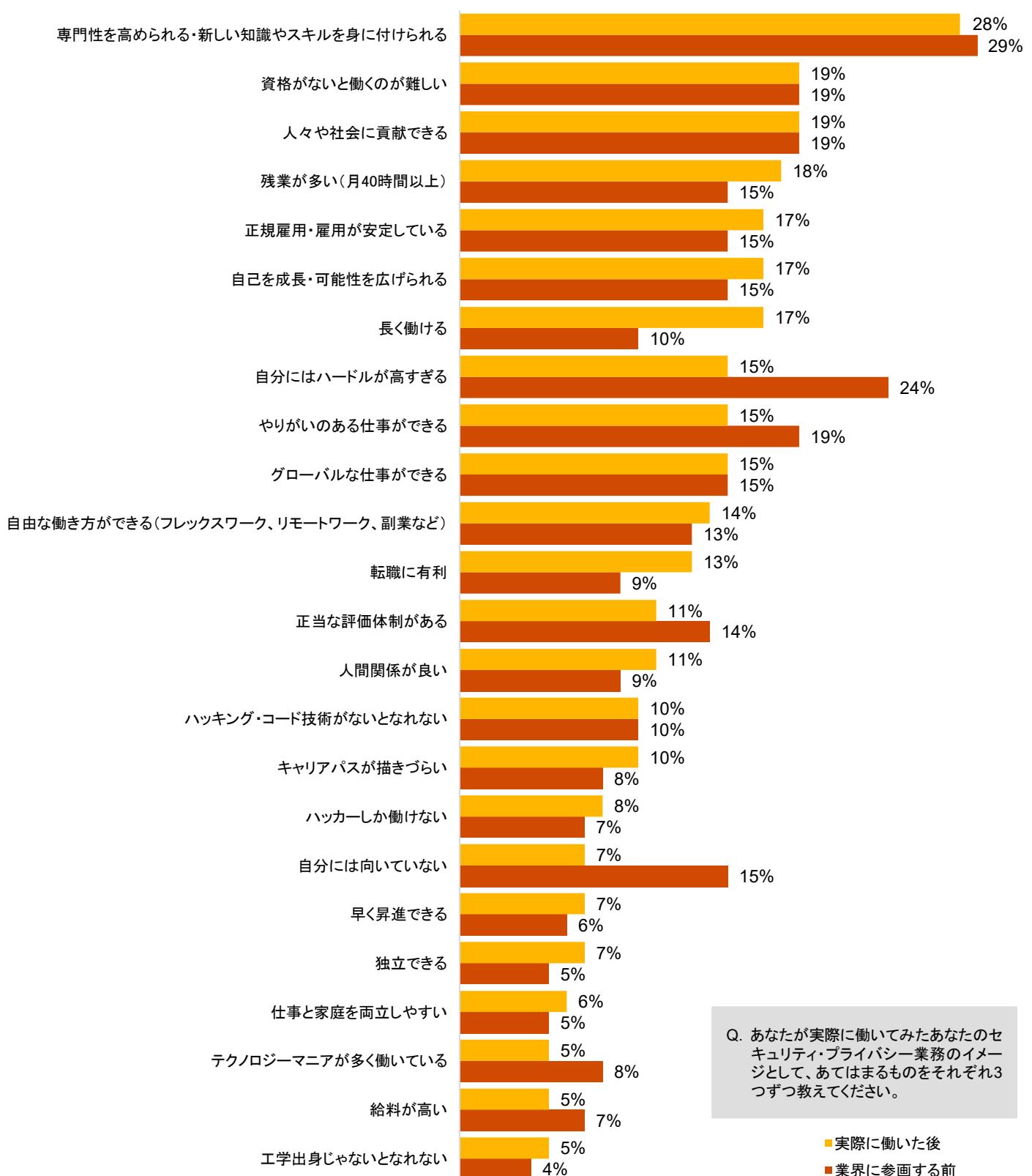


図表41:セキュリティ・プライバシー業務に携わることになったきっかけ(日米比較)

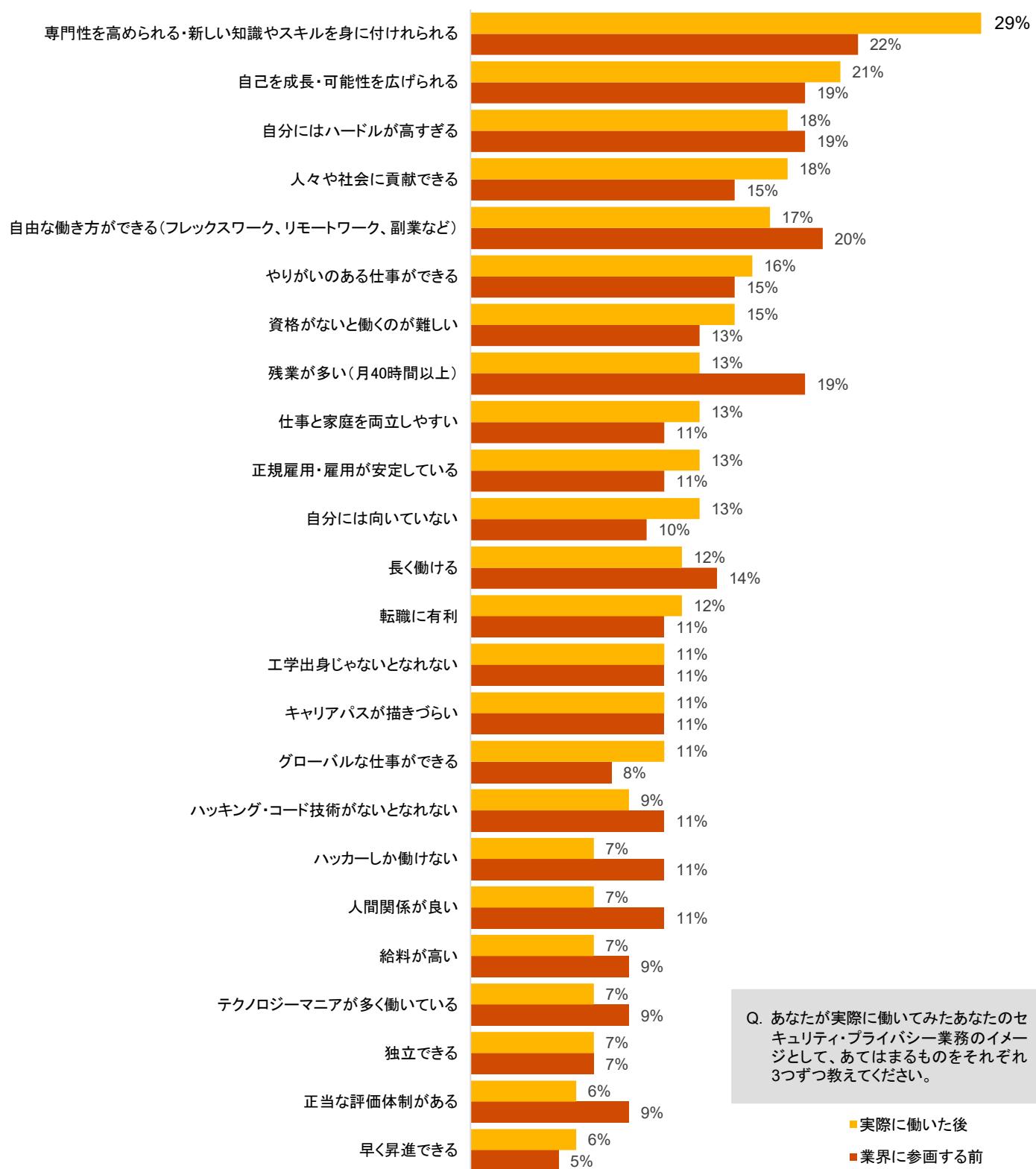




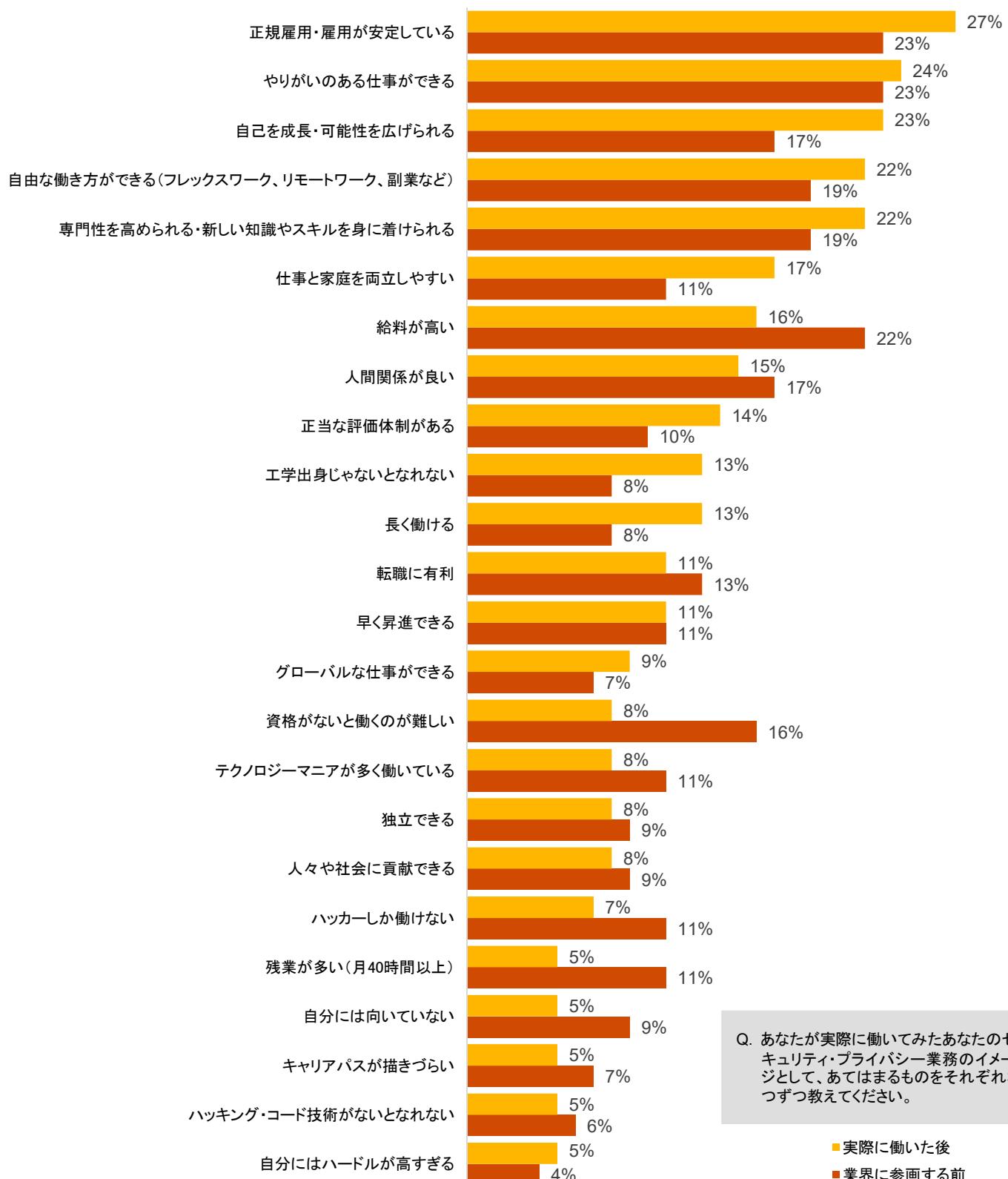
図表42: 働く「前」と実際に働いた「後」のセキュリティ業界に対する印象の比較(日本女性専門家)



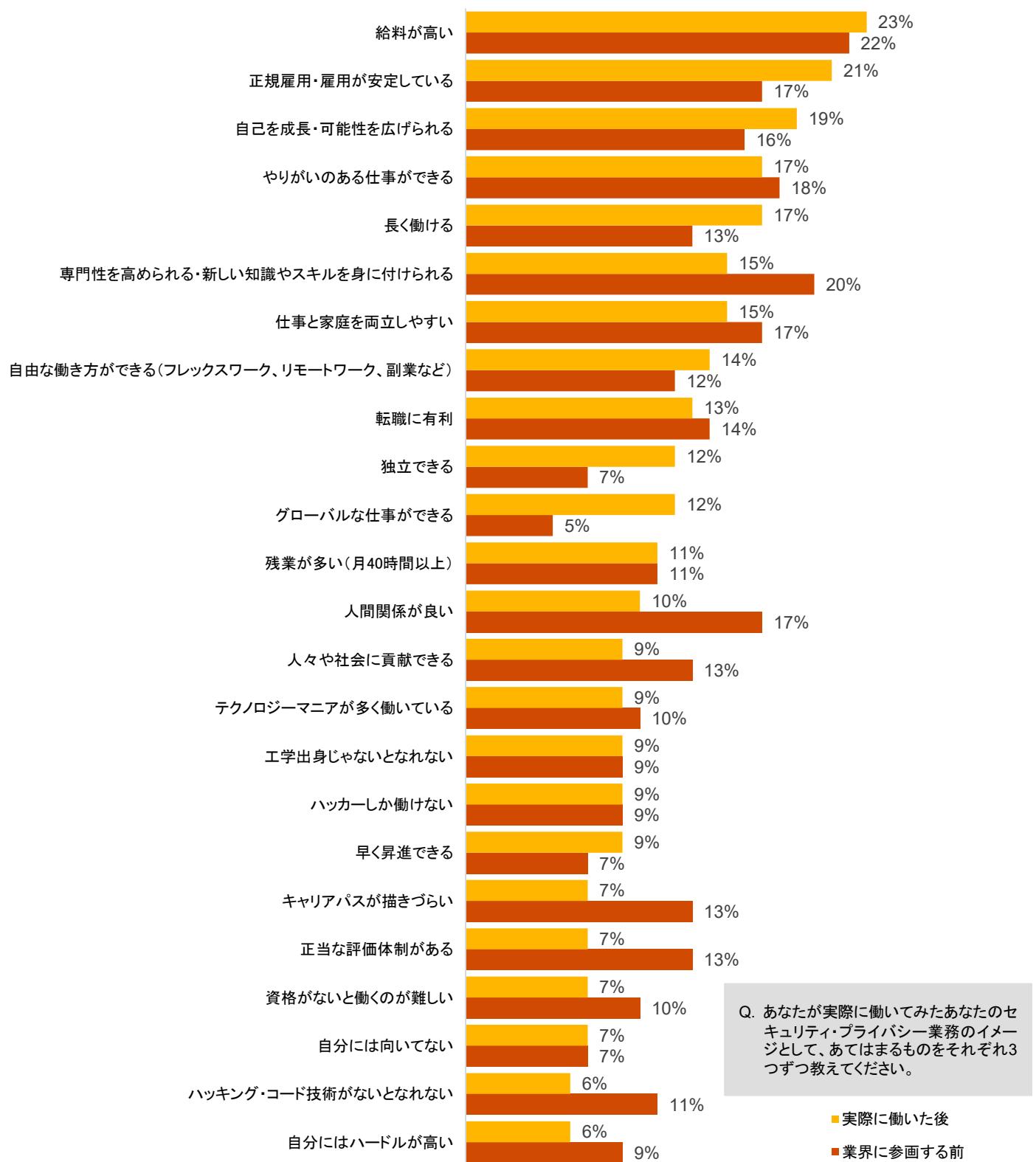
図表43: 働く「前」と実際に働いた「後」のセキュリティ業界に対する印象の比較(日本男性専門家)



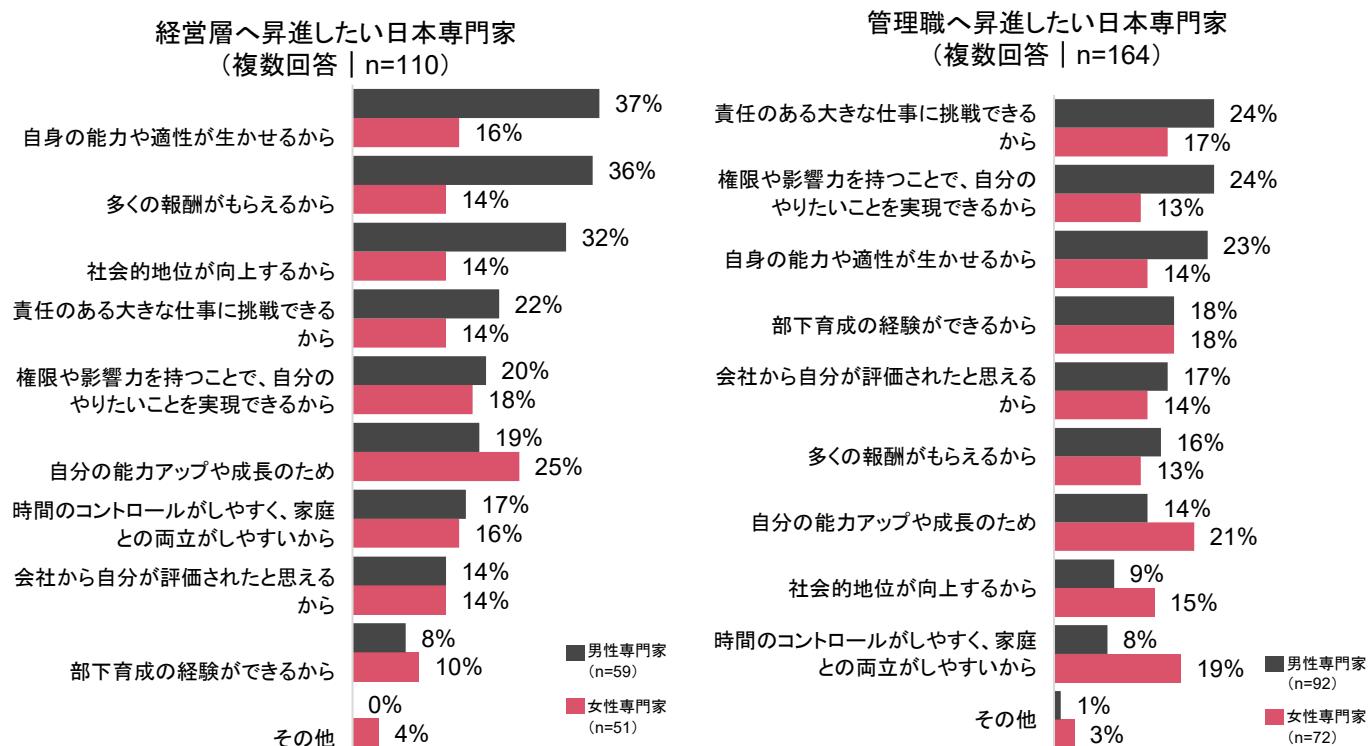
図表44: 働く「前」と実際に働いた「後」のセキュリティ業界に対する印象の比較(米国女性専門家)



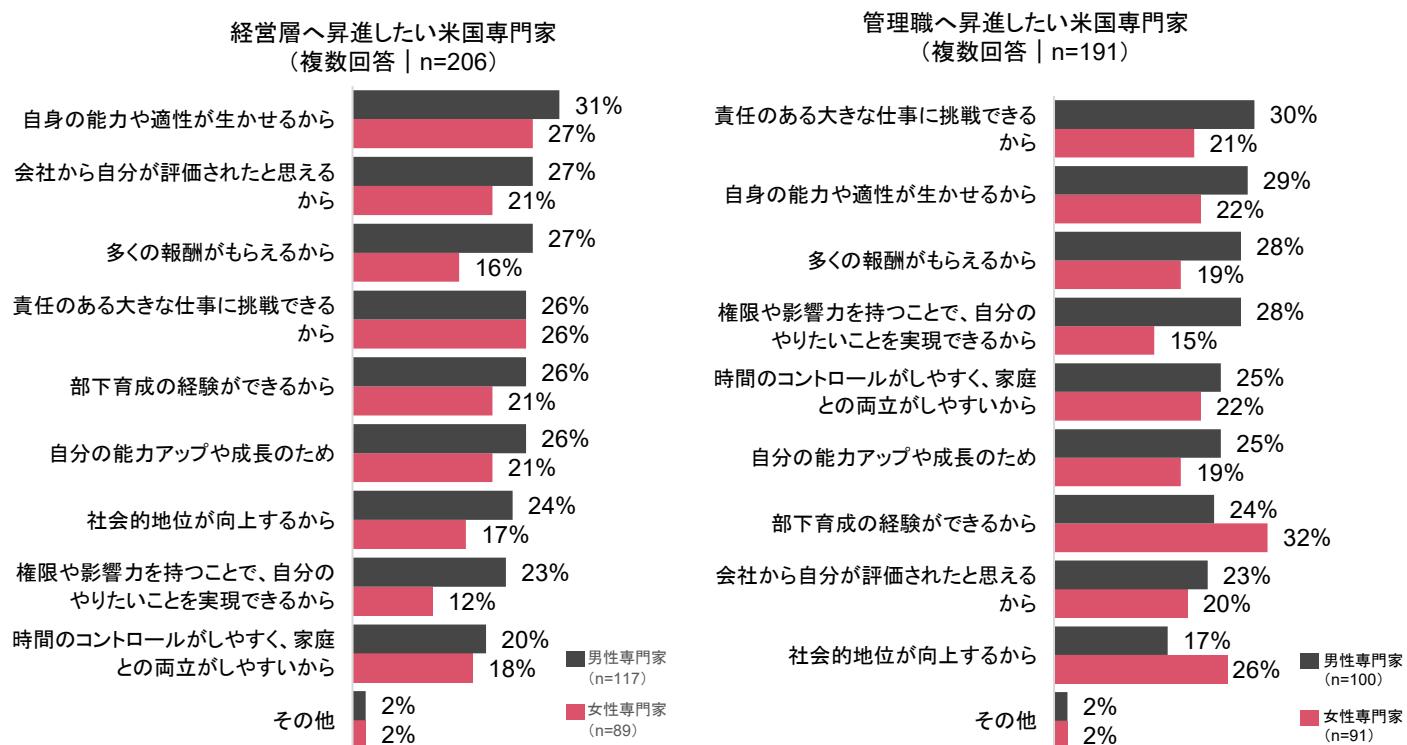
図表45: 働く「前」と実際に働いた「後」のセキュリティ業界に対する印象の比較(米国男性専門家)



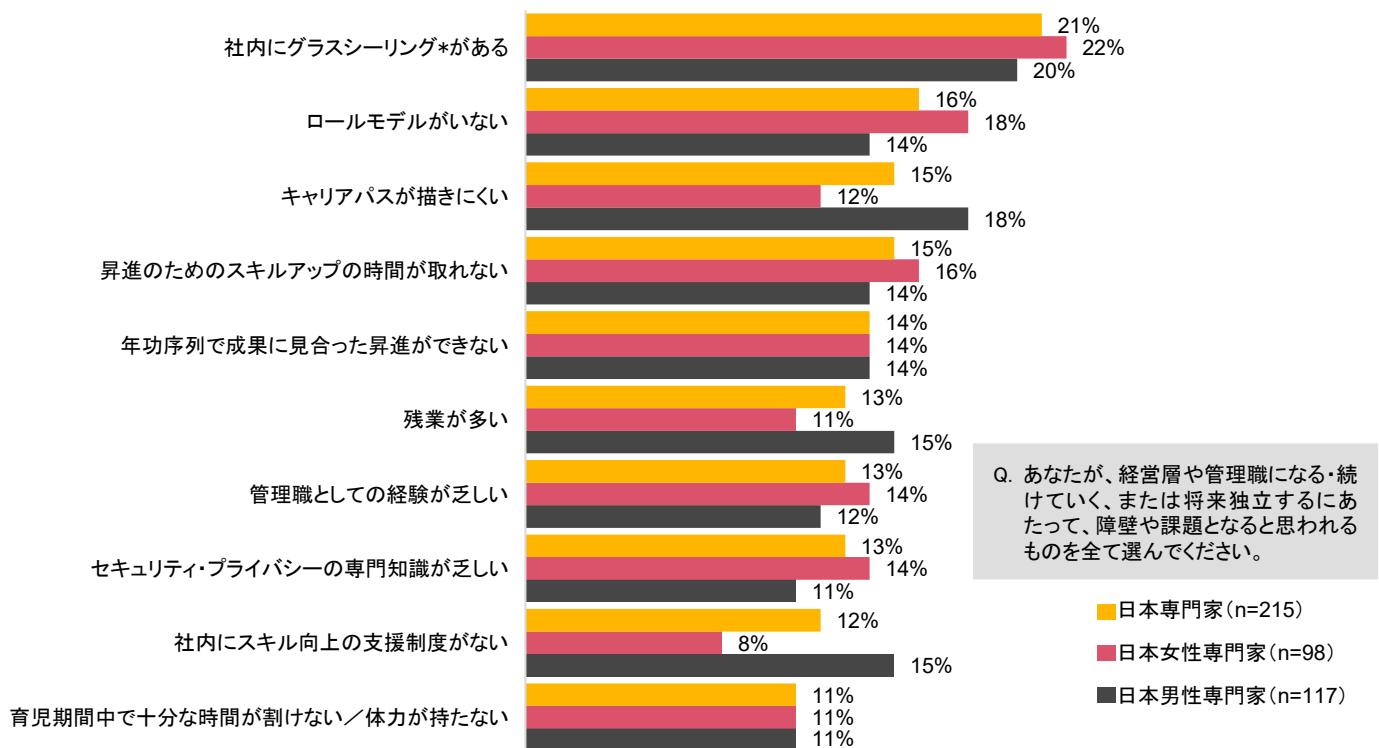
図表46: 昇進を希望する理由(日本)



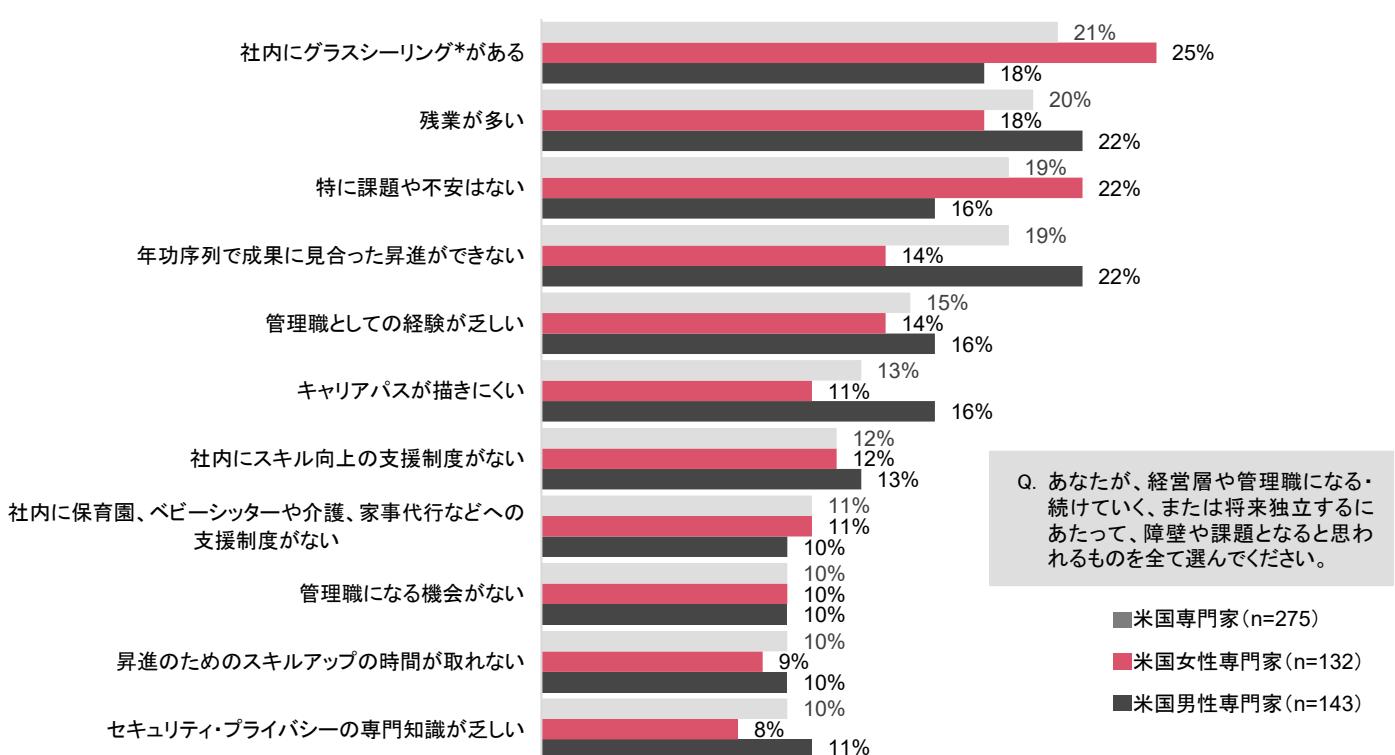
図表47: 昇進を希望する理由(米国)



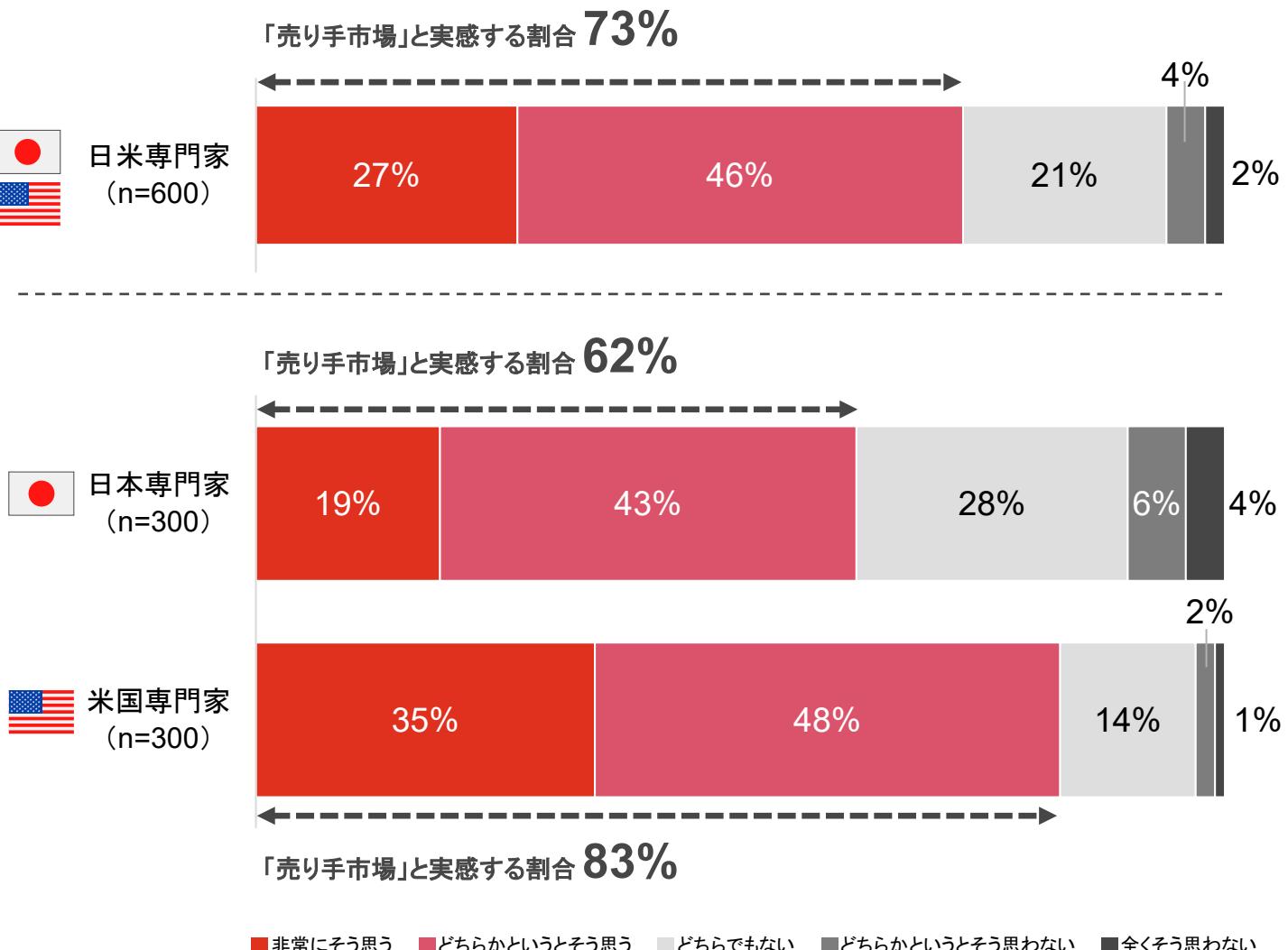
図表48: 昇進する上での不安や課題(日本上位10項目)



図表49: 昇進する上での不安や課題(米国上位10項目)

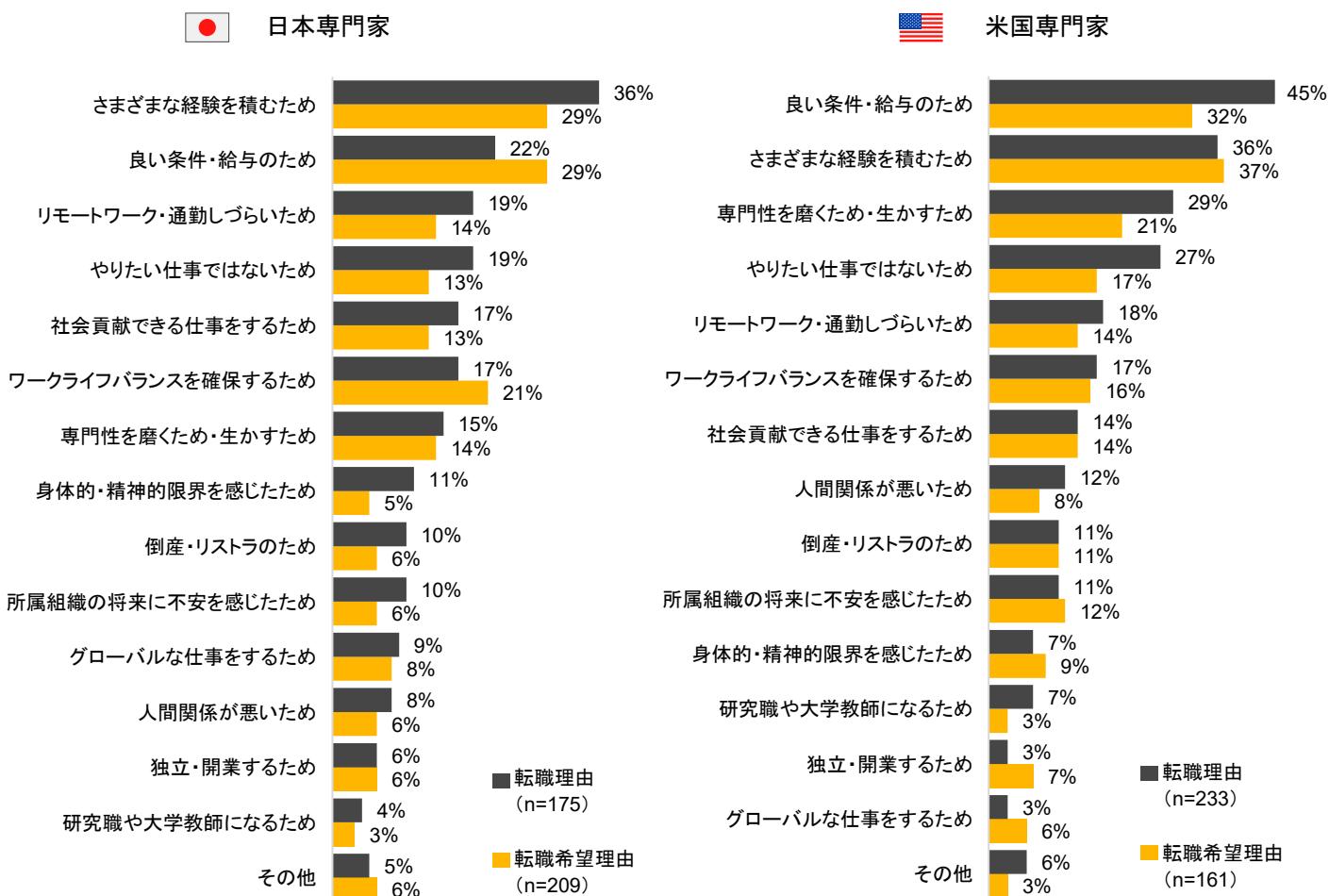


図表50:セキュリティ人材は「売り手市場」と実感する割合(日米比較)

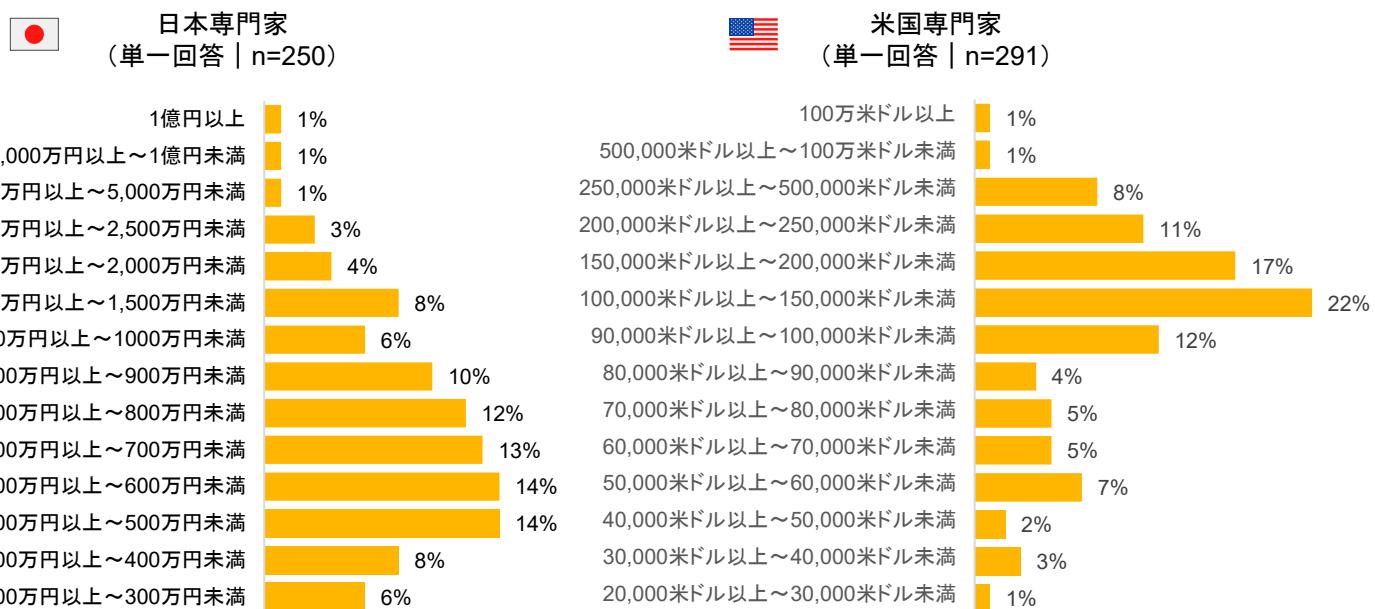


Q. あなたはセキュリティ・プライバシー業界の人材は売り手市場(就職・転職に有利)だと思いますか。最もあてはまるものを教えてください。

図表51:過去の「転職理由」および将来の「転職希望理由」の割合(日米)



図表52:現在希望する年収(日米比較)



監修

ショーン キング

PwCコンサルティング合同会社
パートナー

綾部 泰二

PwC Japan有限責任監査法人
パートナー

執筆

林 恵子

PwCコンサルティング合同会社
シニアマネージャー

愛甲 日路親

PwCコンサルティング合同会社
マネージャー

牧 言美

PwCコンサルティング合同会社
アソシエイト

お問い合わせ先

PwC Japanグループ

www.pwc.com/jp/ja/contact.html





www.pwc.com/jp

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwC Japan有限責任監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立した別法人として事業を行っています。複雑化・多様化する企業の経営課題に対し、PwC Japanグループでは、監査およびブローダーアシュアランスサービス、コンサルティング、ディールアドバイザリー、税務、そして法務における卓越した専門性を結集し、それらを有機的に協働させる体制を整えています。また、公認会計士、税理士、弁護士、その他専門スタッフ約11,500人を擁するプロフェッショナル・サービス・ネットワークとして、クライアントニーズにより的確に対応したサービスの提供に努めています。PwCは、社会における信頼を構築し、重要な課題を解決することをPurpose（存在意義）としています。私たちは、世界151カ国に及ぶグローバルネットワークに約364,000人のスタッフを擁し、高品質な監査、税務、アドバイザリーサービスを提供しています。詳細は www.pwc.com をご覧ください。

電子版はこちらからダウンロードできます。www.pwc.com/jp/ja/knowledge/thoughtleadership.html

発刊年月：2024年6月 改訂：2024年7月 管理番号：I202404-05

© 2024 PwC. All rights reserved.

PwC refers to the PwC network member firms and/or their specified subsidiaries in Japan, and may sometimes refer to the PwC network. Each of such firms and subsidiaries is a separate legal entity. Please see www.pwc.com/structure for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.