THE LINUX FOUNDATION | Research

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

2024年 セキュア ソフトウェア 開発教育調査

現在のニーズを理解する

Marco Gerosa, Ph.D., *Northern Arizona University*
David A. Wheeler, Ph.D., *The Linux Foundation*
Stephen Hendrick, *The Linux Foundation*

序文
Christopher Robinson, *Intel*
Dave Russo, *Red Hat*

2024 年 6 月

2024年 セキュア ソフトウェア開発教育調査

ソフトウェア開発に直接携わる専門家の28%が、セキュアなソフトウェア開発に関する知識が不足しています。

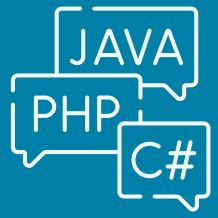
経験年数1年未満のソフトウェア開発者が最も知識不足であると回答しました(75%)。

専門家の69%は、セキュアなソフトウェア開発の教材として実務経験を重視していますが、知識を習得するまでに**5年以上の実務経験**が必要です。

専門家の50%が、セキュアなソフトウェア開発における**主な課題はトレーニング不足**と考えており、特にデータサイエンス職で顕著です(73%)。

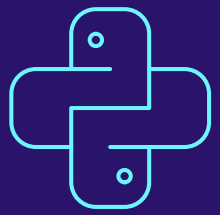
53%の専門家、特にシステム運用担当者(72%)は、セキュアなソフトウェア開発に関するコースを受講していません。その主な理由は、**優れたコースに関する認識不足** (44%) です。

79%の専門家は、プログラミング言語に依存しないコースを非常に重要だと考えています。一方、プログラミング言語固有のコースについて54%の専門家が重要視していました。

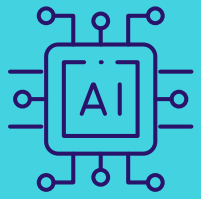


プログラミング言語に依存しないコースとして人気があるコンテンツは、**セキュリティ アーキテクチャー**(64%)、**セキュリティ教育とガイダンス**(64%)、**セキュアな実装**(63%)でした。

トレーニングの必要性については、**専門性と経験値**によって考え方に違いがありました。

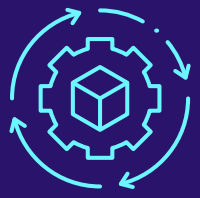


プログラミング言語固有のトレーニングで人気が高かったのは Pythonで、回答者の71%が選択しましたが、重要な言語として上位の選択肢に多く選ばれたのは、CとJavaでした。



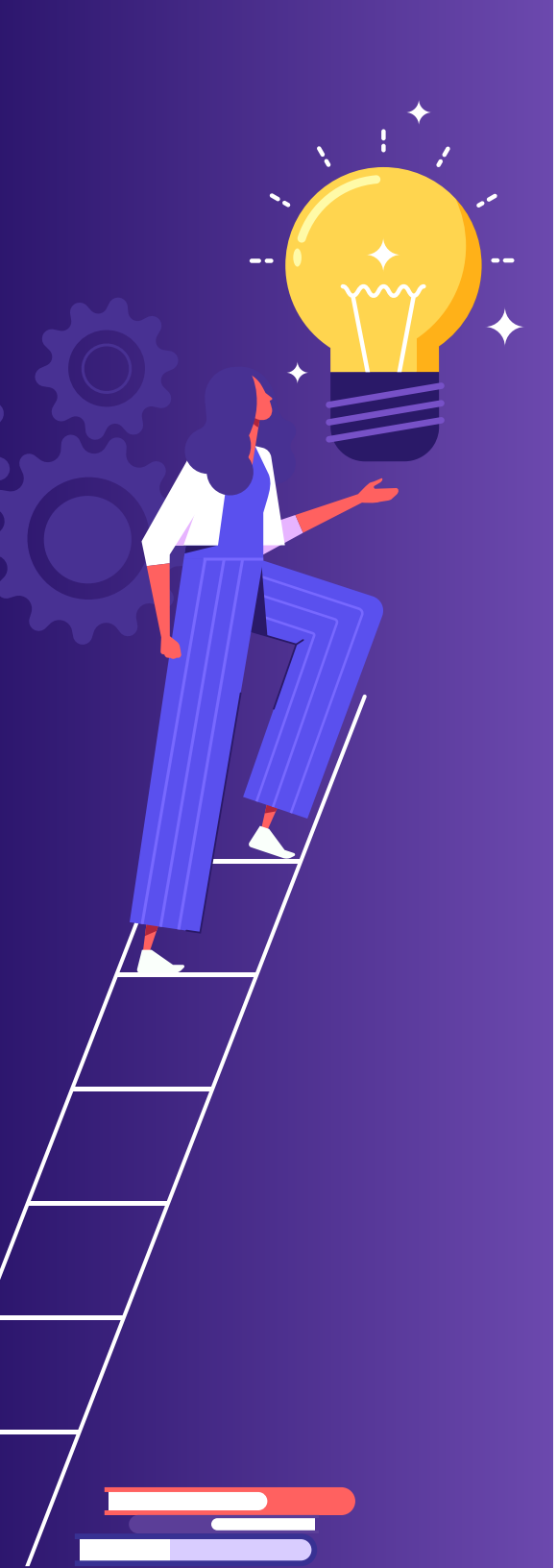
回答者の57%が、今後、セキュアなソフトウェア開発において、イノベーションが必要な注目分野は**AIとMLのセキュリティ**であると考えています。

回答者の56%が、**サプライチェーンのセキュリティ**は、より一層の注力とイノベーションが必要な重要分野だと考えています。



セキュアなソフトウェア開発に対する教育を充実させるため、OpenSSFは**新しいコースのトピックとしてセキュリティ アーキテクチャー**を選択しました。

もくじ



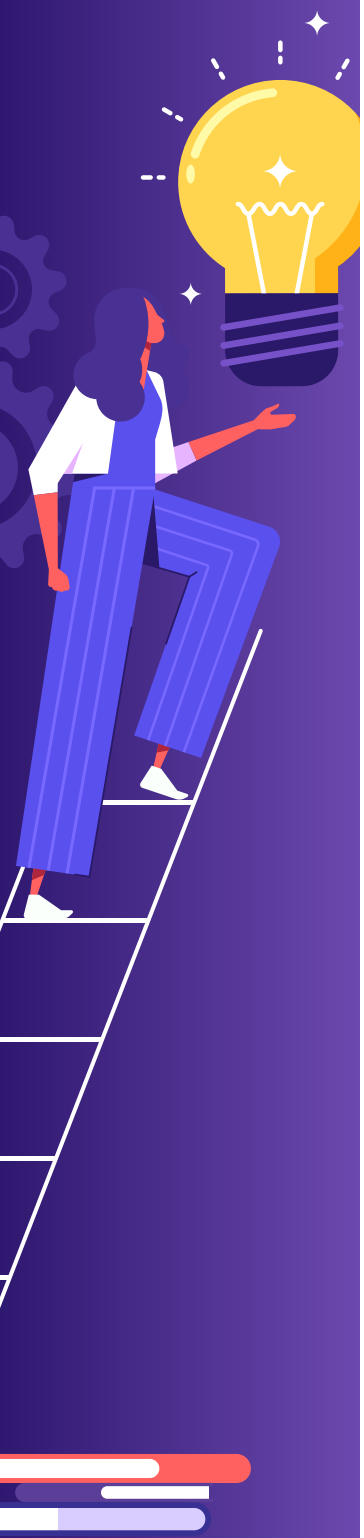
序文

知識というのは、一度習得してしまえば、開発者がどのようなプログラミング言語、開発環境、スキャナで作業していても、また、どのような環境にアクセスしても、いつでも活用できるツールです。このセキュア ソフトウェア開発教育調査に参加できたこと、そして Linux Foundation（LF）の調査結果をコミュニティへ公開できることを嬉しく思います。私たちはすでに、調査結果に基づいて対策を始めています。レポートが公開された今、コミュニティからのフィードバックを受け、さらにさまざまなスキルレベル、経験、経歴の開発者を支援できることを楽しみにしています。

Christopher Robinson, *Intel,* Co-Chair of the OpenSSF Education Special Interest Group and Chair of the OpenSSF Technical Advisory Council

開発ツールがどれほど洗練されたものになったとしても、特にセキュアな開発という点においては、コードを設計・実装する個人の知識と考え方がコード全体の品質に非常に大きな影響を与えます。開発者がセキュアな開発の実践方法を常に意識し、それを活用するためには、何を知るべきかを明らかにし、その情報を分かりやすく提供したいと考えています。OpenSSF のセキュア ソフトウェア開発教育調査の結果を活用することで、よりニーズにあった、学習効果の高い教材を提供できるでしょう。さらに、この情報を使って、オープンソース コミュニティに対するトレーニング全体の可用性や質を改善・拡大し、他のメンバにも展開していきます。

Dave Russo, *Red Hat,* Co-Chair of the OpenSSF Education Special Interest Group



第 1 章：はじめに

セキュアなソフトウェア開発は非常に重要であるにもかかわらず、多くの開発者は、セキュアなソフトウェア開発を効果的に実施するための知識やスキルが不足しています。多くの教育プログラムは、機能性と効率性に重点を置いており、セキュリティのトレーニングは軽視されがちです。ソフトウェアの安全性が、かつてないほど重要になっています。金融取引や医療管理から国家安全保障や日常的なコミュニケーションに至る多くの分野で、ソフトウェアの脆弱性が大惨事をもたらす可能性があります。IBM の報告書（2023 年）[1] によると、米国においてデータ侵害に対してかかったコストは、1 件あたり平均 944 万ドルです。Verizon の報告書（2021 年）[2] によると、情報漏えいの 43%は、ソフトウェア開発の不備に起因するソフトウェア脆弱性に関連しています。

サイバー脅威の進化は、攻撃者が絶えずソフトウェアの弱点を突く方法を見つけ出していることを意味しています。セキュアなコーディング プラクティス、定期的なセキュリティ評価、プロアクティブな脅威モデリングを実践することで、開発者は、機密データを保護し、ユーザーの信頼が得られる回復力のあるシステムを構築することができます。セキュアなソフトウェア開発は、ソフトウェア開発プロセスの単なる追加要素ではなく、不可欠な要件です。

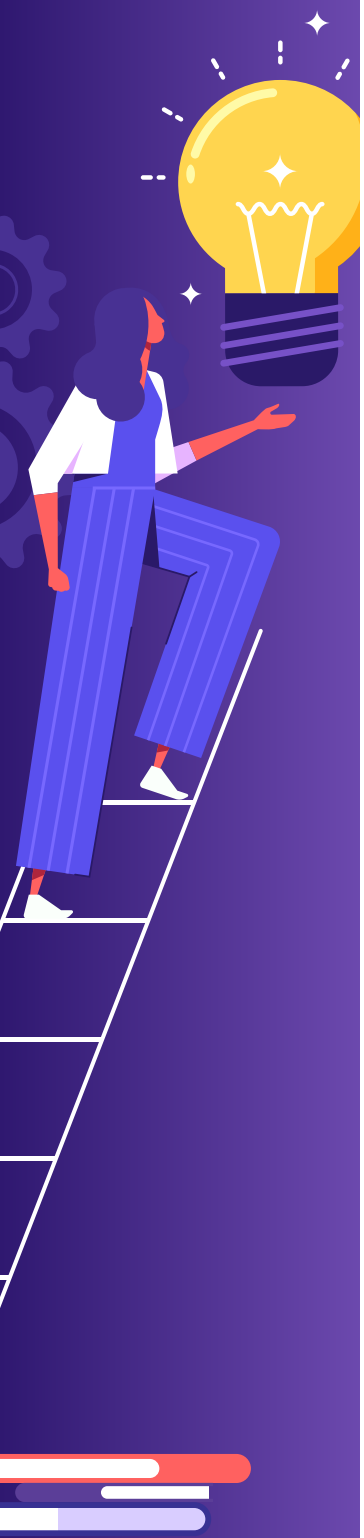
セキュアなソフトウェア開発は非常に重要であるにもかかわらず、多くの開発者は、セキュアなソフトウェア開発を効果的に実践するための知識やスキルが不足しています。多くの教育プログラムは、主に機能性と効率性を重視しており、セキュリティのトレーニングがおろそかになりがちです。歴史的に広く浸透している、セキュリティよりも機能性を重視するという文化は、ソフトウェア開発においての課題です。この考え方は、コンピューティングの黎明期まで遡ることができ、その頃の目的は、特定のタスクを実行するための機能的で信頼性の高いシステムを作成することでした。セキュリティは、考慮されたとしても、後回しにされることが多くありました。

セキュアなソフトウェア開発は非常に重要であるにもかかわらず、多くの開発者は、セキュアなソフトウェア開発を効果的に実践するための知識やスキルが不足しています。多くの教育プログラムは、主に機能性と効率性を重視しており、セキュリティのトレーニングがおろそかになりがちです。

セキュアなソフトウェア開発に取り組むための最初のステップは、既存の知識ギャップを認識し、トレーニングを強化すべき分野を特定することです。この目標を念頭に置いて、Open Source Security Foundation（OpenSSF）と Linux Foundation（LF）Research は提携し、セキュアソフトウェア開発教育のニーズを評価するために、ソフトウェア開発の専門家を対象とした世界規模の調査を実施しました。この調査は、ソフトウェア開発者教育に対する「セキュリティ バイ デザイン」のアプローチを促進し、セキュリティ教育プログラムを強化することを目的としています。

1 https://www.ibm.com/reports/data-breach

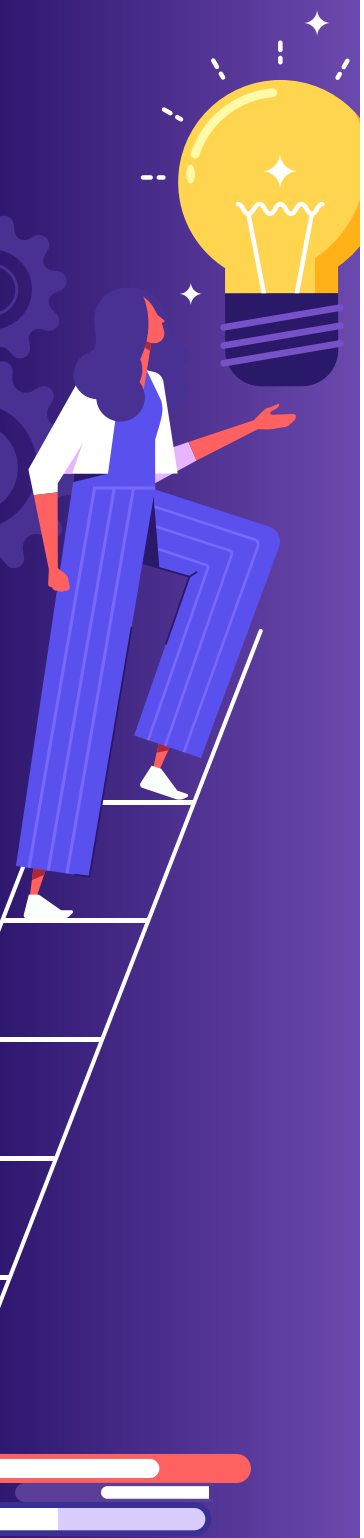
2 https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report



本調査では、2024 年 3 月 1 日から 4 月 29 日にかけて、ソフトウェア開発に携わる専門家から 398 件の有効回答を得ました。この調査には、セキュアなソフトウェア開発に関する回答者の属性、経験、および現在の考え方に関する設問と、セキュアなソフトウェア開発に関する教育ニーズに焦点を当てた設問が含まれています。調査手法と属性分布の詳細については、第 5 章を参照してください。

主な調査結果は以下のとおりです。

1. システム運用、ソフトウェア開発者、コミッター、メンテナーなど、ソフトウェアの開発・デプロイに直接携わる専門家の大部分（28%）が、セキュアなソフトウェア開発をよく知らないと回答しました。
2. 経験年数が 1 年未満のソフトウェア開発者が最も知識不足であると回答しました（75%）。
3. 専門家の 69%が、主な教材として実務経験を重視していますが、最低限のレベルの知識を習得するために、少なくとも 5 年の経験が必要と回答しました。
4. 多くの専門家(50%)、特にデータ サイエンスの専門家(73%)にとっての大きな課題はトレーニング不足です。
5. 多くの専門家（53%）、特にシステム運用の専門家（72%）は、セキュアなソフトウェア開発に関するコースを受講していません。
6. ほとんどの専門家（79%）は、セキュアなソフトウェア開発にはプログラミング言語に依存しないコースが非常に重要であると考えており、プログラミング言語固有のコースが非常に重要と考えている割合（54%）を上回っています。
7. プログラミング言語に依存しないコースの中では、セキュリティ アーキテクチャー、セキュリティ教育とガイダンス、セキュアな実装などが人気です。
8. トレーニングのニーズは、専門性や経験値によって大きく異なるため、セキュアなソフトウェアのプラクティスに関するさまざまな教育が必要であることがわかりました。
9. プログラミング言語固有のトレーニングでは、回答者の 71%が Python を選択しており、高い人気があります。しかし、重要度の上位を見ると、C と Java がより多く選択されており、プログラミング言語別教育における複雑な需要を示しています。
10. 今後のイノベーションが求められる注目すべき重要分野として、新しいセキュリティの懸念分野である AI や ML におけるセキュリティと、サプライ チェーンにおけるセキュリティが挙げられています。回答者の 57%が AI や ML におけるセキュリティ、回答者の 56%がサプライ チェーンのセキュリティが重要であると認識しています。
11. これらの調査結果に基づき、OpenSSF は、第 4 章で説明するように、セキュリティ アーキテクチャーに関する新しいコースを設置することを決めました。ここではいくつかの分析結果を紹介しましたが、すべてのデータを公開していますので、ぜひご覧ください。

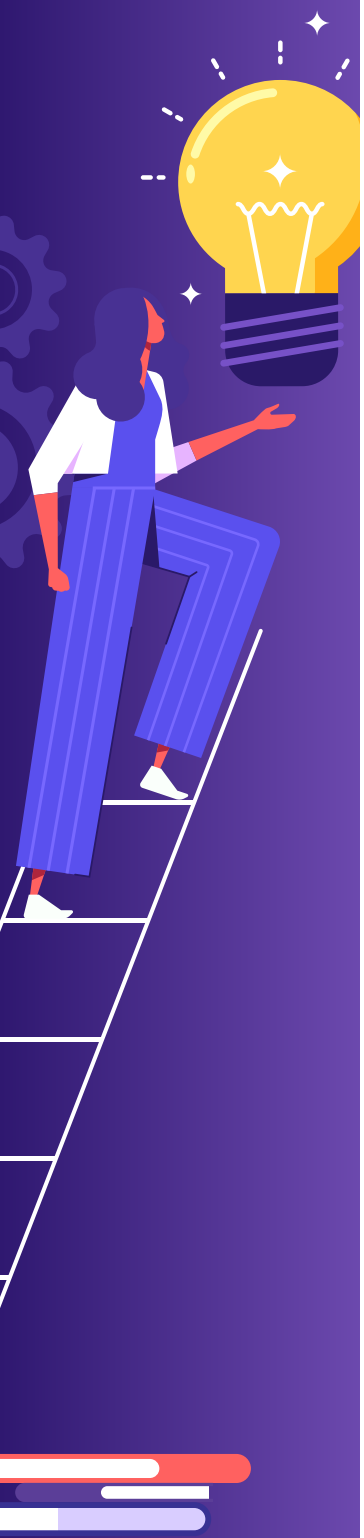


第 2 章：さらなるトレーニングの必要性

本章では、さらなるトレーニングの必要性を探ります。回答者がセキュアな開発手法について知識があるか、これらの手法を実践する際の課題は何か、そして専門家がどんな教材を活用しているかを分析しています。この分析は、どのようなトレーニングが今後必要かを理解するためのベースとなります。

本章の主な調査結果は以下のとおりです。

1. ソフトウェア開発に携わる多くの専門家（28%）が、セキュアなソフトウェア開発の知識が不足しています。
2. システム運用 (39%)、ソフトウェア開発者 (27%) など、ソフトウェア開発・デプロイにおいて主要な役割のメンバに、セキュアなソフトウェア開発をよく知らない専門家が多くいます。特にオープンソース ソフトウェア (OSS) においては、オープンソース プログラム オフィス (OSPO) メンバー (38%)、コミッター (29%)、メンテナー (23%) などが十分な知識がないと回答しています。
3. セキュリティ チームのメンバーでさえ（16%）、セキュアなソフトウェア開発をよく知らない場合があります。
4. ソフトウェア開発経験者であることは、セキュアなソフトウェア開発ができることを意味しておらず、経験年数に関係なく、少なくとも 20%はセキュアなソフトウェア開発に関して知識が不足しています。
5. 90%以上の専門家は、セキュアなソフトウェア開発ができるようになるためには、少なくとも 5 年間の実務経験が必要であると回答しています。
6. セキュアなソフトウェア開発コースを受講していない人のうち、受講しない理由が、すでに十分な知識があるからだと答えた人はごくわずか（13%）でした。
7. 組織がセキュアなソフトウェア開発の技術を取り入れる際の課題として、「認識不足とトレーニングの欠如」（50%）が、「時間不足」（58%）に次いで 2 番目に多く回答されました。
8. データ サイエンスの専門家においては「認識不足とトレーニングの欠如」と 73%が回答しており、大きな課題です。
9. 独学（74%）や実務経験（69%）といった教育機関以外での学習が主流となっています。
10. セキュリティ チームのメンバーの過半数（60%）がセキュアなソフトウェア開発に関するコースを受講していますが、ソフトウェア開発者（48%）やシステム運用の専門家（28%）など、他の重要な役割の専門家では受講している人は少数でした。
11. コースを受講しない理由のトップは、「セキュアなソフトウェア開発に関する良いコースを知らないため」（44%）でした。
12. セキュアなソフトウェア開発に関するコースが必要ないと答えた専門家はほとんどいませんでした（最大でも 13%）。
13. OpenSSF の教材を使用していると回答した組織はわずか 25%で、その理由のトップは認知度の低さでした。
14. ほとんどの回答者（74%）が、自分のペースで進められるトレーニング教材を望んでいます。



多くの専門家は、セキュアなソフトウェア開発の知識が不足している

図 1 に見られるように、ソフトウェア開発の専門家のほぼ 3 分の 1 が、セキュアなソフトウェア開発をよく知らないと感じています。また、セキュアなソフトウェア開発の知識があると回答した人であっても、それを実際にどのように適用すればよいかを知らない場合もあります。この傾向は図 2 の結果でも裏付けられています。「自分はこのテーマについてすでに十分知識があるため、トレーニングは必要ない」と回答した人はわずか 13%しかいませんでした。懸念すべき点は、図 1 のとおり、開発プロセスにおいて重要な役割を担っている専門家が、セキュアなソフトウェア開発のプラクティスを知らないことです。

ソフトウェア開発を主な職務とする人の 27%が、セキュアなソフトウェア開発のプラクティスをよく知らないと答えています。ソフトウェア開発者が、アプリケーションやシステムのコードを実装・保守する最前線にいることを考えると、この事実は大きな問題です。開発者の 4 分の 1 以上が十分な知識がないということは、開発者間の基本的な知識のギャップが大きく、それによって開発課程でセキュリティの脆弱性を生み出してしまう可能性が高いことを示しています。企業の標準的な開発者育成カリキュラムに、包括的なセキュリティ トレーニングを導入し、セキュアなコーディングのためのプラクティスをソフトウェア開発ライフサイクルの基本的な要素として取り込むことが急務であると言えます。

また、他の報告書のデータを考慮すると、どちらかといえばさらに事態は深刻かもしれません。Secure Code Warrior による 2022 年の調査では、開発者の 89% が、セキュア コーディング スキルについて「十分な」トレーニングを受けていると回答しました。しかし、具体的な内容について質問したところ、回答者の大半が、一般的なソフトウェアの脆弱性、その回避方法、脆弱性の悪用方法についてよく知らないと答えています。実際、この調査では、86%の開発者が、セキュア コーディングを実践するのが難しいと回答しています。[3]

これは、セキュアなソフトウェアの開発方法に関する情報が乏しいため、開発者は自分の知識を過大評価し、間違った知識をもとに知識があると回答していたことが原因と考えられます。大学を出た開発者であっても、その方法を学んでいない場合が多いことを考えると、あまり驚くべきことではありません。2021 年の調査では、U.S. News 誌の上位 24 校のコンピュータ サイエンス スクールのうち、学生にセキュリティについての学習を義務付けているのはカリフォルニア大学サンディエゴ校の 1 校だけであることが示されました。[4] つまり、基本的な事柄に対する理解さえも広範に欠如しているため、私たちのデータは、状況を現実よりも好意的に示している可能性が高いのです。

また、このデータにおいて、セキュアなソフトウェア開発について「よく知らない」と回答した人が、システム運用の専門家と OSPO のチーム メンバーで最も多いことが明らかになりました（それぞれ 39%と 38%）。これらの職務は、ソフトウェア インフラとオープンソース イニシアチブを管理・維持する上で重要な職務であり、いずれも企業全体のセキュリティ態勢の基礎であるため、この事実は大きな問題です。セキュリティ チームのメンバが「よく知らない」と回答した割合は最も低く、16% でした。セキュリティに特化した担当者は、セキュアな開発プラクティスに関する知識が豊富であることを示している一方で、セキュリティの専門家全員が知識を十分に持っていると考えていないことは懸念材料です。この結果から、企業ではセキュアなソフトウェア開発を意識する文化を醸成するために、部門横断的なトレーニング プログラムや取り組みが重要であると言えます。

3 The State of Developer-Driven Security Survey, Secure Code Warrior, 2022, https://discover.securecodewarrior.com/state-of-developer-driven-security-2022.html

4 https://www.appsecengineer.com/blog/developer-security-at-universities

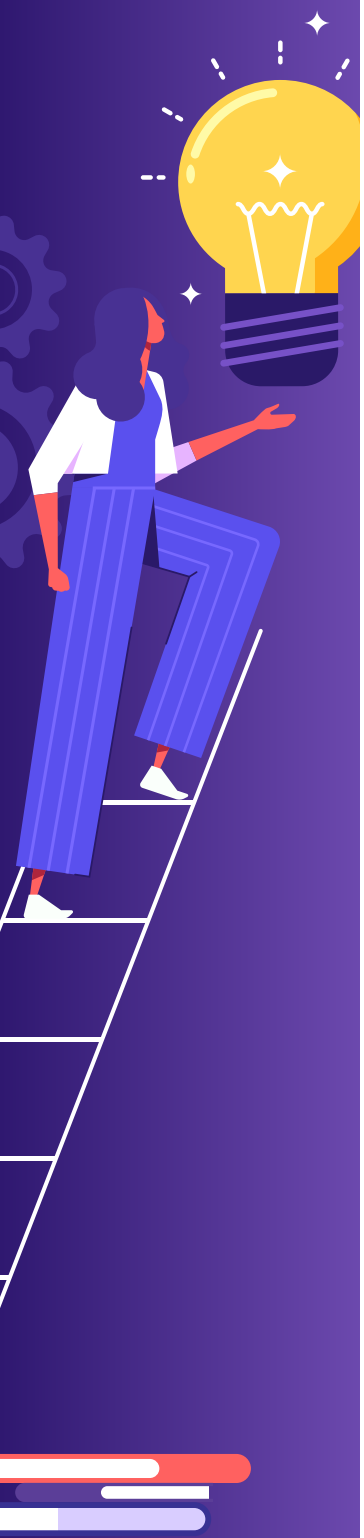
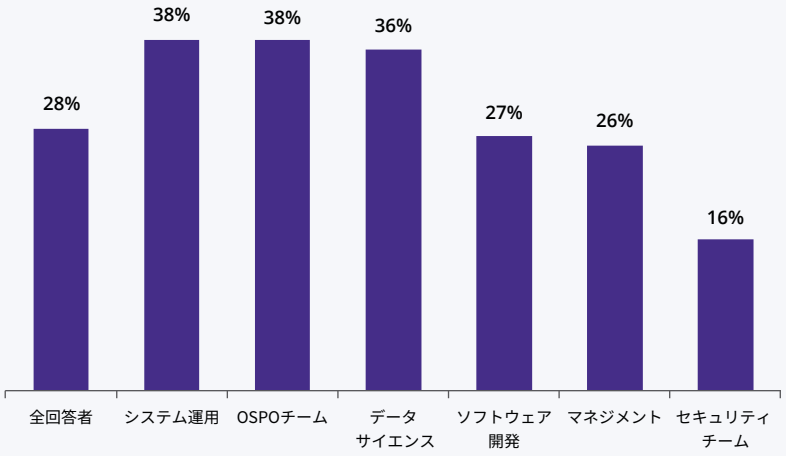


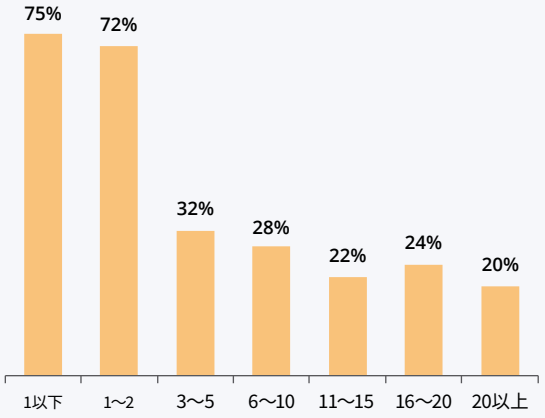
図 1

セキュアなソフトウェア開発についてよく知らないと回答した人の割合

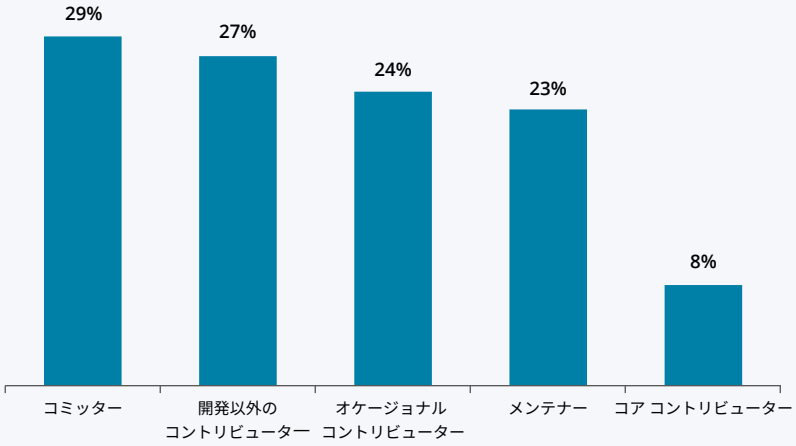
職務で区分



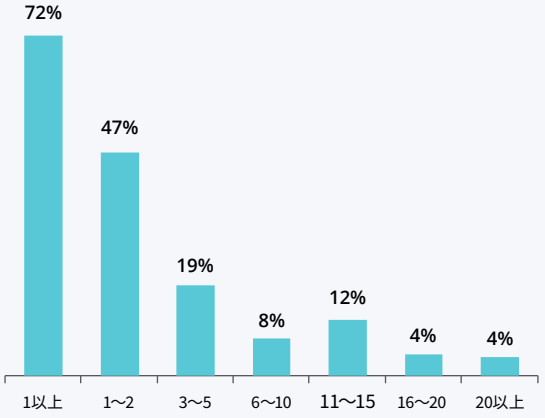
ソフトウェア開発経験年数による区分



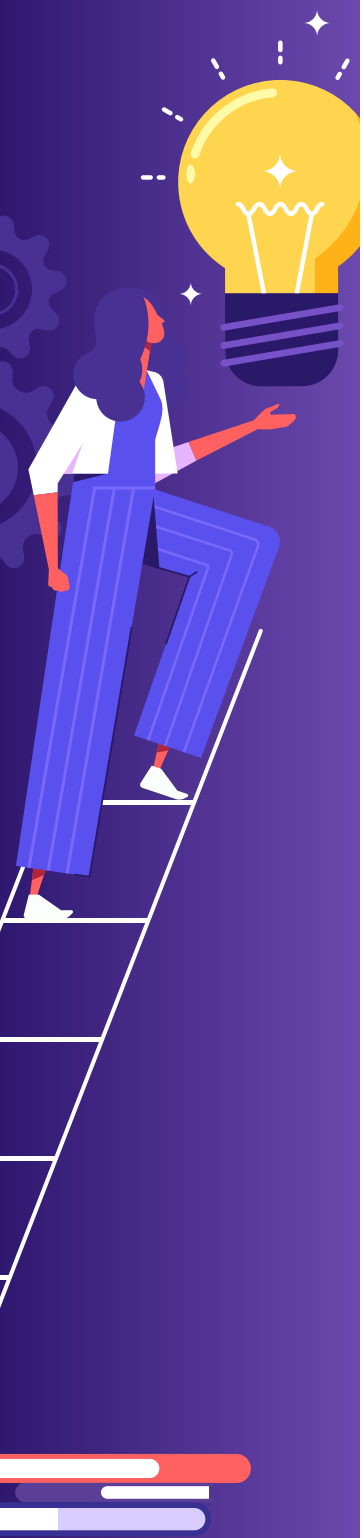
オープンソース ソフトウェアの役割別で区分



セキュア ソフトウェア開発の経験年数で区分



2024 年 SecEd 調査、問 14、問 5、問 8、問 15、問 16、サンプル数＝ 396、よく知らないは「まったく理解していない」または「ある程度は知識がある」と答えた人を示す。

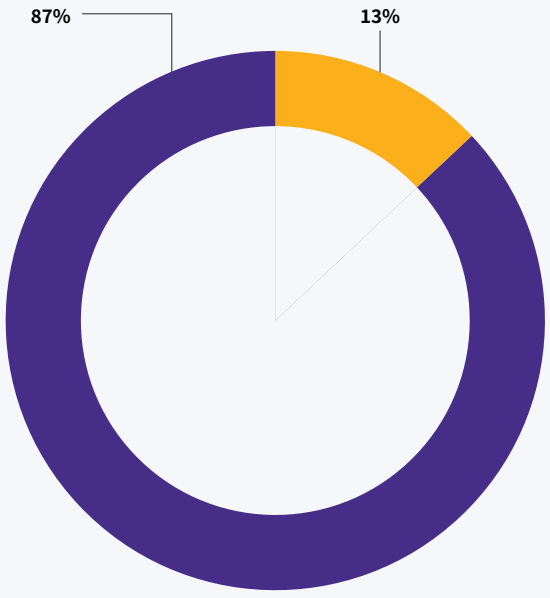


OSS のコントリビューターに絞ると、コミッターとメンテナーの 4 分の 1 以上が、セキュアなソフトウェア開発をよく知らないと考えていることがわかります。この事実は、オープンソースのリポジトリに直接コードを書いたり、他の人の成果物をレビューしたりする開発者の多くが、この分野についてよく知らないことを示しています。このようなセキュリティ知識の乏しい開発者が、OSS の技術を利用する多くの最新システムに対し、よく目にするような一般的な脅威を埋め込んでしまう可能性があります。

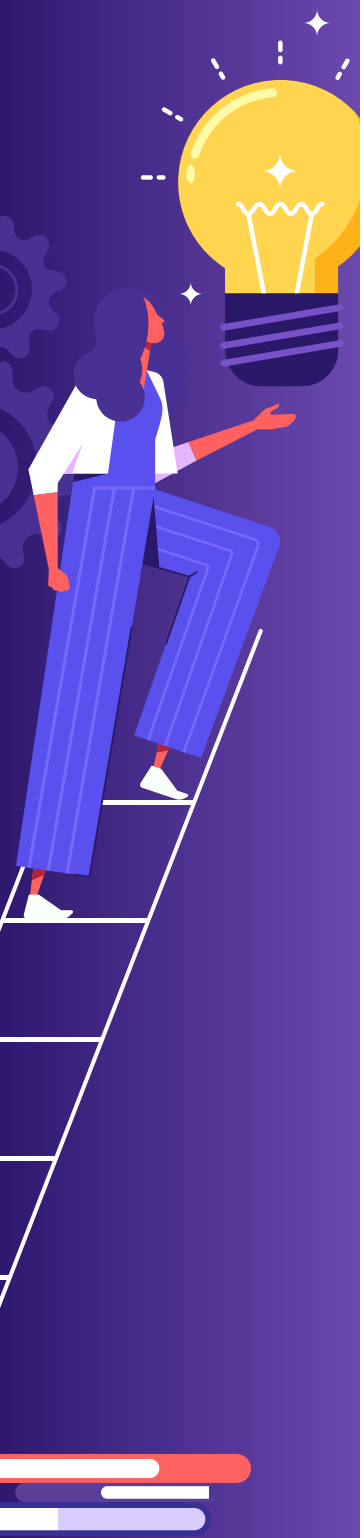
この調査では、経験年数による知識の違いも浮き彫りになりました。経験年数が 1 年未満のソフトウェア開発者は、「知識がない」と回答した割合が 75%と最も高く、経験年数が 1 ～ 2 年の場合は 72%に低下しています。同様に、セキュア ソフトウェア開発に関する経験が 1 年未満の人の 72%が「知識がない」と回答していますが、この数字は 1 ～ 2 年の経験者では 47%に低下しています。経験年数が長くなるにつれてこの数字は減少するものの、20 年以上の一般的な経験を持つ専門家の 20% は、依然としてこの分野の知識がないと回答しています。このことは、経験豊富な開発者であっても、必ずしもセキュアなソフトウェア開発の知識があるとは限らず、熟知するためには多くの場合、長年の特定の実務経験が必要なことを示しています。このことは、企業にとって、ソフトウェア専門家のキャリアの早い段階でセキュア ソフトウェア開発のトレーニングを取り入れることが重要であることを示しています。また、企業は、セキュア コーディングのプラクティスを習得できる育成プログラムに投資し、この知識を補うような継続的な教育を提供すべきであることを示しています。

図 2

セキュアなソフトウェア開発に関するコースを受講していないと回答した人のうち、すでにセキュアなソフトウェア開発に十分な知識があると考えている人の割合



2024 年 SecEd 調査、問 31、サンプルサイズ= 150



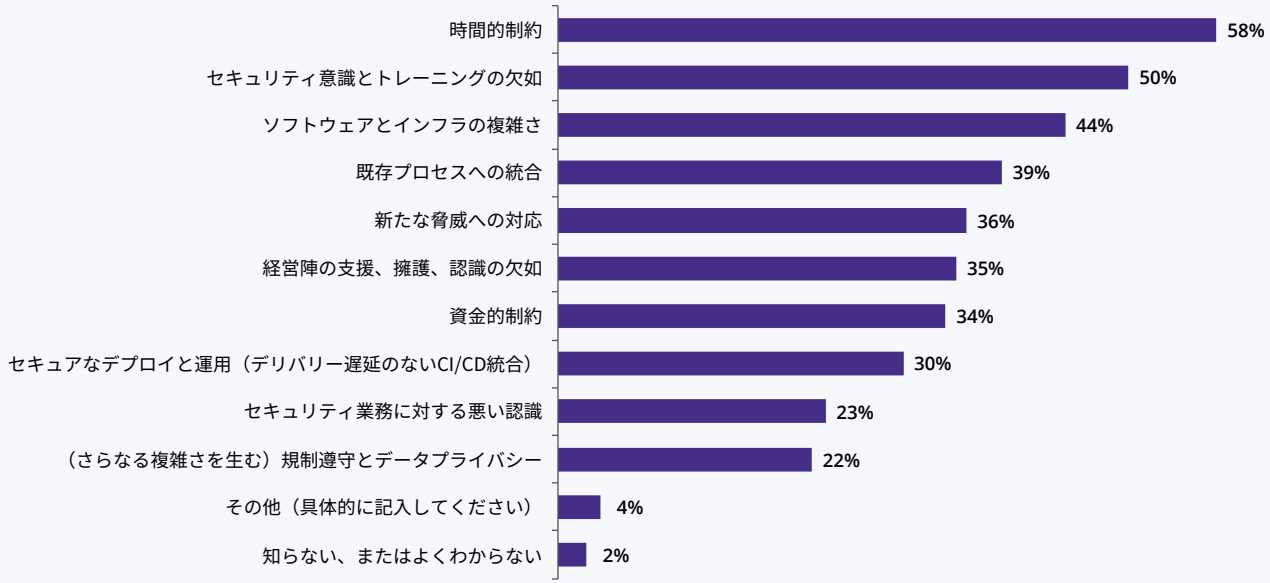
セキュアなソフトウェア開発の大きな課題は、意識向上とトレーニングの欠如

効果的にセキュアなソフトウェア開発とデプロイを実施するためには、多くの課題があります。調査の結果でも、セキュリティ意識とトレーニングの欠如が、組織にとっての最重要課題の 1 つであることが示されました。図 3 に示すように、回答者の半数がこの課題を挙げており、時間的制約に続き第 2 位にランクしています。時間的制約は多くの組織に共通する問題であるため、これらのニーズにうまく対応するためには、ほとんどの組織で、体系的かつ構造的な教育プログラムによってセキュリティ意識の向上とトレーニングに取り組む必要があります。これらのプログラムを、組織文化やワークフローにあわせて取り込み、定期的かつ強制的に、全部門で学習を継続し、セキュリティ意識を高める文化を醸成することで、このような教育活動の効果を高めることができます。

図 4 に示すように、セキュアなソフトウェア開発とデプロイに対し、セキュリティ意識とトレーニングを改善すべきという課題認識は、業務の専門性によっても異なります。最も懸念しているのはデータ サイエンスの専門家で、回答者の 73%が重大な課題であると回答しました。

図 3

セキュアなソフトウェア開発とデプロイにおける組織の最大の課題



2024 年 SecEd 調査、問 28、サンプル数＝ 324、総回答数＝ 1,224

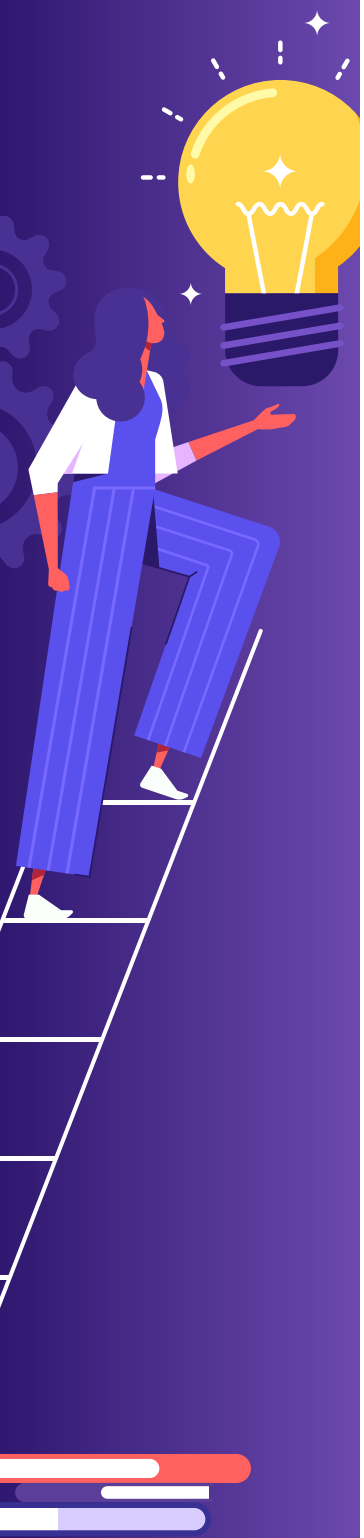
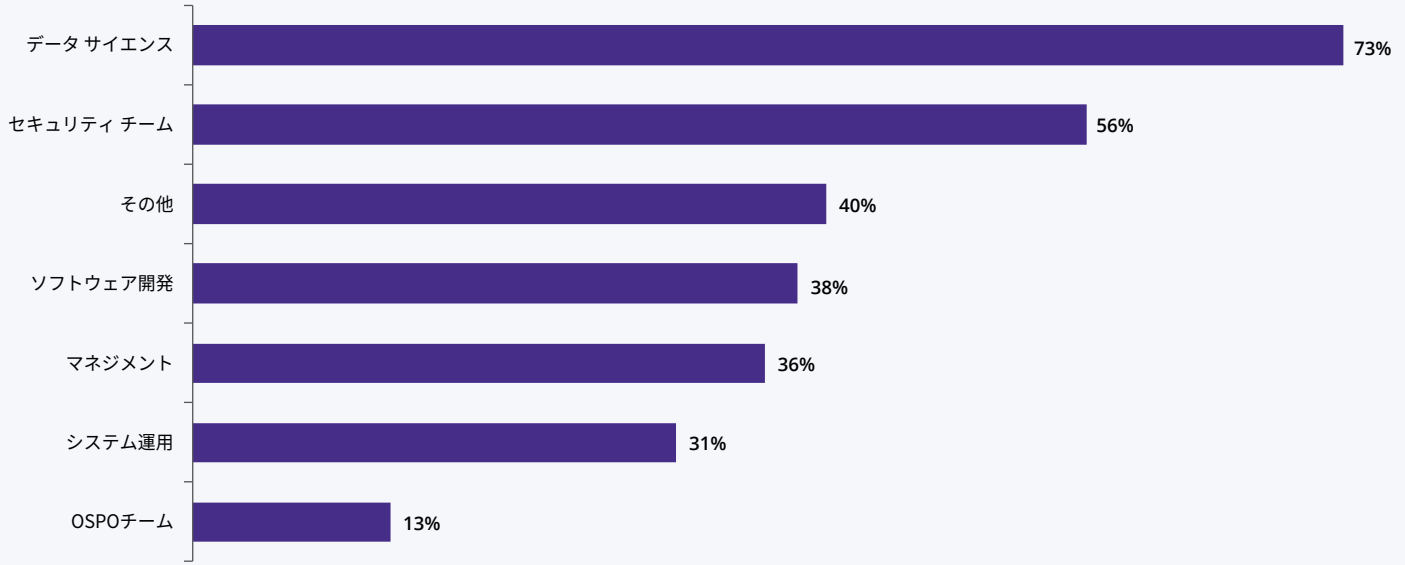


図 4

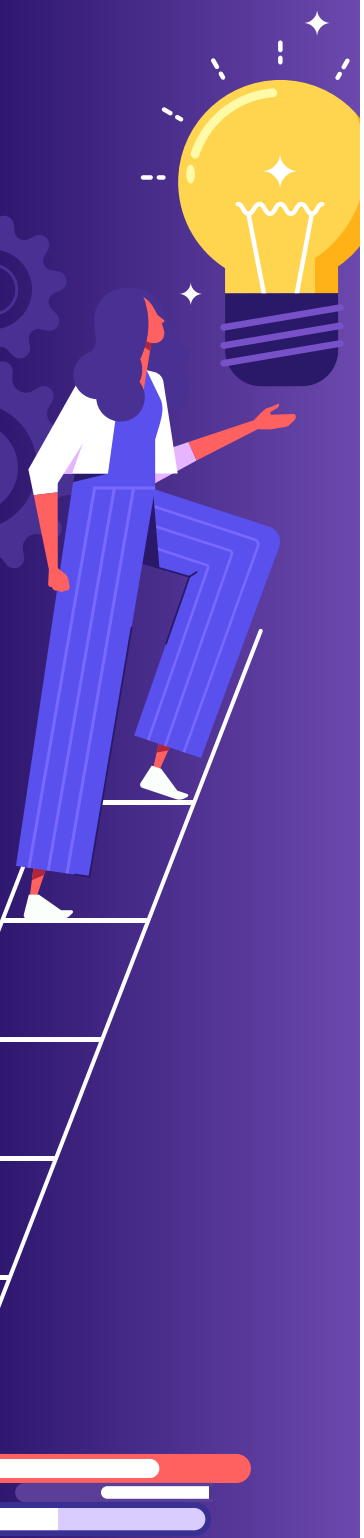
セキュアなソフトウェア開発とデプロイを実施する上での課題として、「セキュリティ意識の改善とトレーニングの欠如」を挙げた回答者の割合（回答者の職務別）



2024 年 SecEd 調査、問 28 と問 5 より構成、サンプルサイズ= 398

この結果は、データ サイエンスの専門家が、セキュア コーディングの標準や方法などのソフトウェア エンジニアリングの実践知識に乏しいアカデミックな分野の出身者が多いことを反映していると考えられます。データ サイエンスの専門家は、モデルやアルゴリズムを本番環境に直接導入することが増えており、セキュリティの実践知識の不足により、脆弱性を埋め込み、大量の機密データを流出してしまうリスクがあります。特に機械学習（ML）システムで使用する場合には、本番システムに直接導入されるモデルの訓練データとして使用される場合もあります。今回の結果は、データ保護の観点で、より強固で実践的なトレーニングが必要であることを示しています。

セキュリティ チームのメンバーも、セキュリティ意識とトレーニングの欠如が、セキュアなソフトウェア開発を実施する上での懸念事項であると感じており、56% がこの課題を挙げています。この結果は、組織



全体の体制に対するセキュリティ チーム独自の視点を反映しています。彼らは、サイバーの脅威に対する対策の主担当者として、理想的なセキュリティ プロトコルと、ソフトウェア開発時の実際の適用結果との違いを痛感しています。またそれにより、組織のセキュリティ インフラにおいても理想と現実のギャップが生じています。このギャップは、組織全体でセキュアなソフトウェア開発に関する教育を強化し、開発ライフサイクル全体にわたってセキュリティ意識を向上させ、脆弱性を防止する必要があることを物語っています。より高い意識付けとトレーニングの強化は、ソフトウェア開発（38%）、マネジメント（36%）、システム運用（31%）など、他の職務に就く多くの専門家でも必要とされています。

回答者の多くが、セキュアなソフトウェア開発に関するコースを受講していない

多くのソフトウェア開発の専門家は、依然として、大学での教育よりも教育機関以外での学習方法が人気です。図 5 では、セキュアなソフトウェア開発の学習方法として最も人気があったのは独学でした。回答者の 74%が、オンライン チュートリアル、ビデオ、書籍などを主な学習方法として利用していると回答しています。この方法に僅差で続いているのが、現場経験の蓄積（69%）です。これらの学習方法には欠点もあります。独学は個人の自主性に大きく依存し、講義のような包括的なカリキュラムや専門家の指導がないことが多く、知識にばらつきがでる可能性があります。現場経験に基づく学習は、実践的ではあるものの、現場で利用可能な専門知識、特定のプロジェクト、職場で遭遇するセキュリティ課題などに大きく左右されるため、一貫性に欠けることもあります。さらに、現場での学習では、不注意で本番環境に脆弱性を埋め込むんでしまうことにより、システム セキュリティを損なってしまう恐れがあります。

セキュアなソフトウェア開発に関するコースは、ソフトウェアのセキュリティ脆弱性を特定し、軽減したり予防したりするためのスキルと知識を専門家に提供することができ、それによって製品のセキュリティを強化し、潜在的なサイバーの脅威から組織を守ることができます。しかし、今回の調査結果によると、専門家の多くは、まだそのような講座を受講していません。図 6 に示すように、回答者の 47% しか、セキュアなソフトウェア開発に関する講座を受講したことがありませんでした。属性により分類すると、セキュリティ チームが 60%の受講率でトップであり、サイバー セキュリティの取り組みの中心的な役割を担っていることが確認できます。他のほとんどの職種においては、その割合は 44% から 50% であり、これらの職種のほとんどがトレーニングを受けていないことを意味しています。特に割合が低いのは、システム運用の専門家で 28%です。現代の多くの IT 環境では、DevOps 現象といわれるように、システム運用担当者が業務の一環としてソフトウェアを作成することが増えています。このようなアプリケーションでセキュリティ対策を怠ると、セキュリティの脆弱性を埋め込み、エコシステム全体が危険にさらされる可能性があります。また、このような専門家を育成することも不可欠です。セキュアなソフトウェア開発に関する知識をシステム運用担当者が習得することで、ソフトウェア開発チームとさらに協調して作業できるようになり、開発・サポート中のシステムに対しライフサイクル全体を通じたセキュリティ対策が行われ、組織全体のセキュリティが強化されるようになるからです。

図 5 に示すように、正式なアカデミック コース（大学など）を通じてセキュアなソフトウェア開発について学んだことのある回答者は、全体の 4 分の 1 未満でした。この結果は、スキル不足の原因が教育環境によるものであり、専門家がソフトウェア開発プロジェクトに参加する際には、事前に追加のトレーニングが必要であることを示しています。前述したように、この問題は単に、ほとんどの大学の教育課程で必修科目として導入されていないことが原因と思われます。追加トレーニングを実施することで、ソフトウェア開発における最新のセキュリティ要件に十分対応できるようになるでしょう。

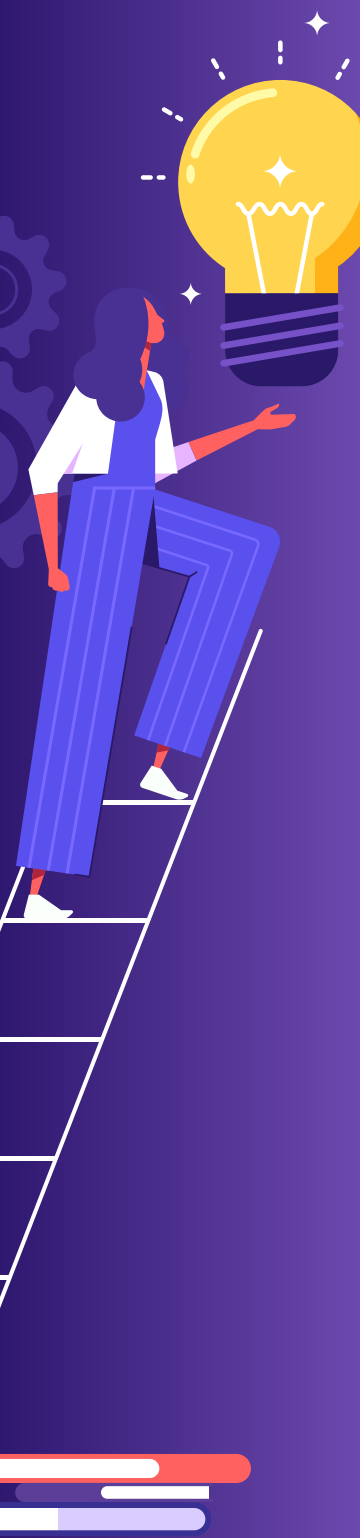
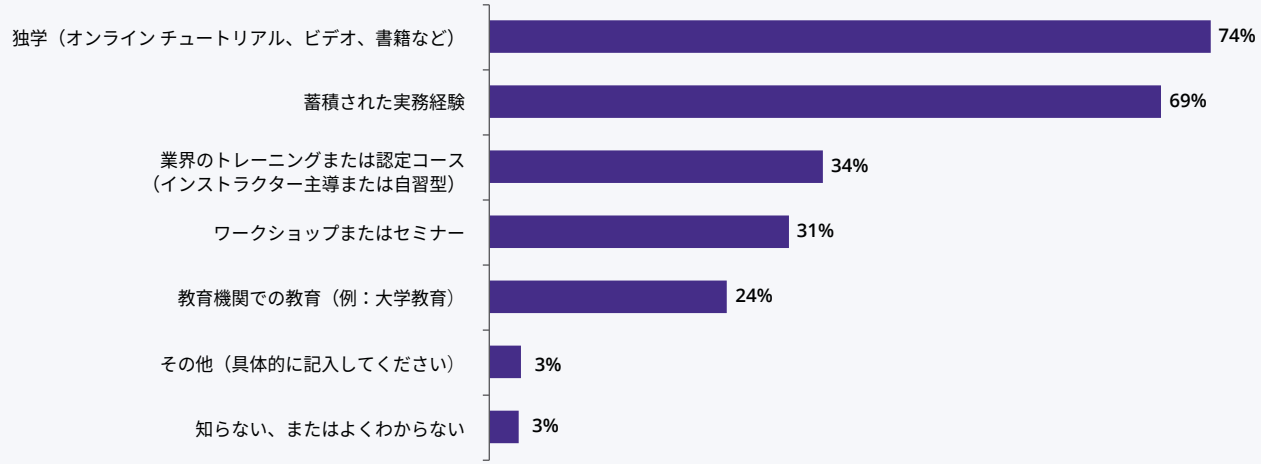


図 5

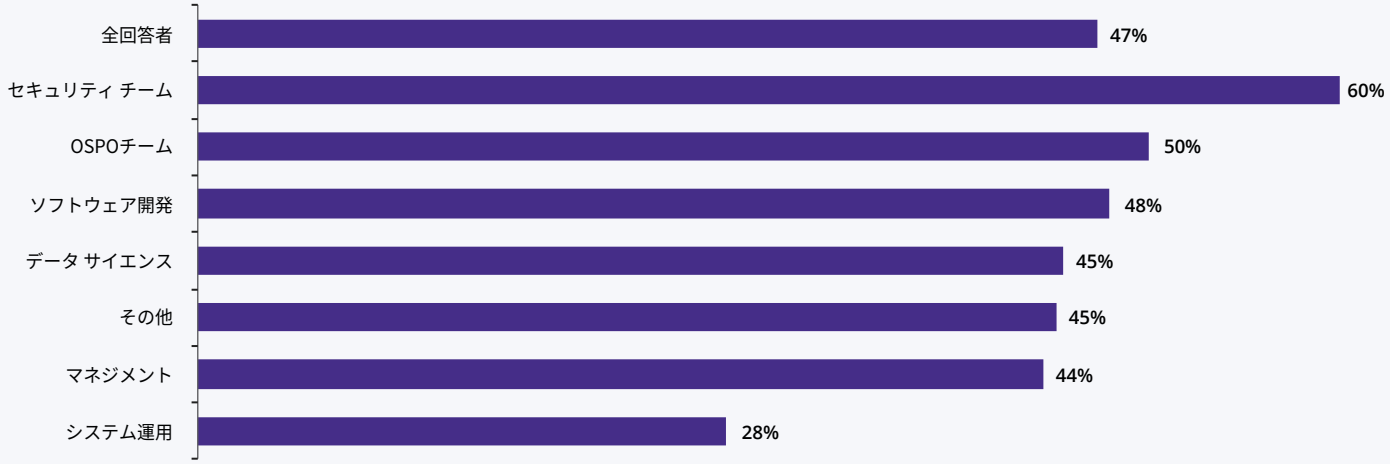
セキュアなソフトウェア開発のための主な学習教材



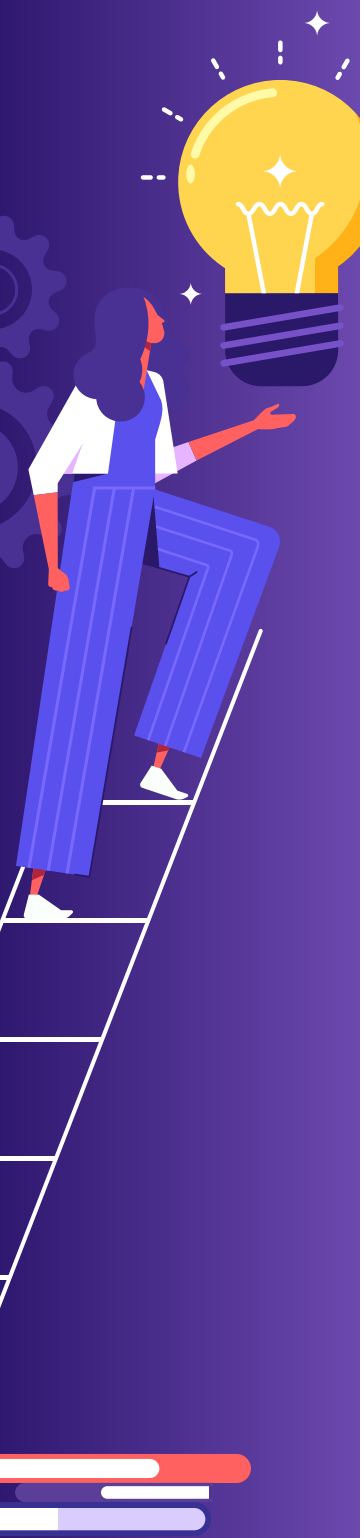
2024 年 SecEd 調査、問 17、サンプル数＝ 398、総回答数＝ 948

図 6

セキュアなソフトウェア開発に関するコースを受講したことがあると回答した人の割合



2024 年 SecEd 調査、問 20 と問 5 から構成、サンプル数＝ 383、DKNS (= 知らない、またはよくわからない）は分析から除外



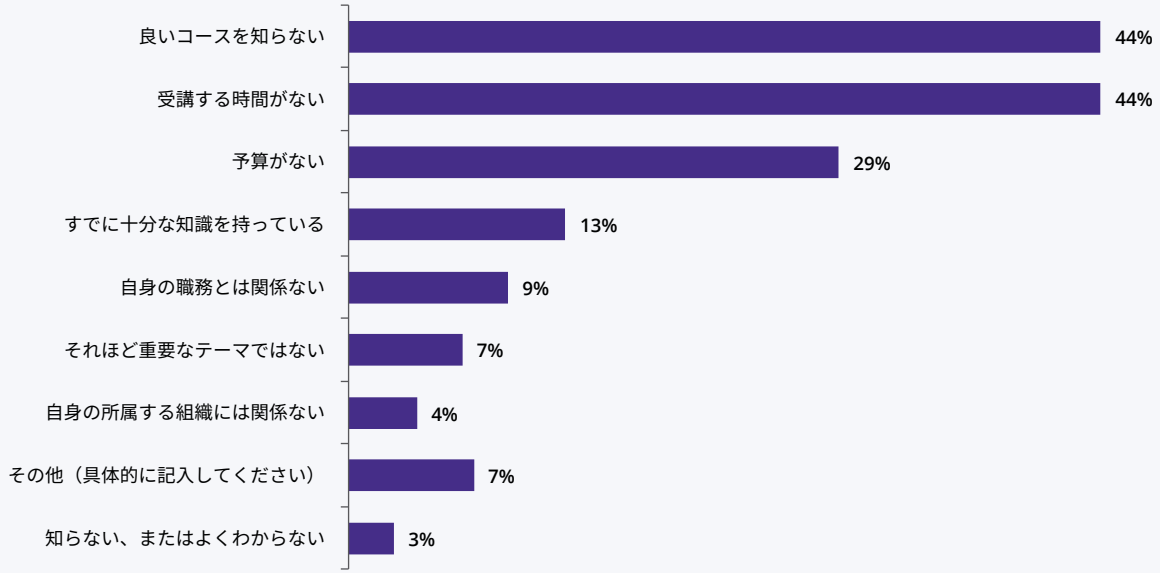
回答者は良いコースを知らないから受講していない

図 7 に示すように、セキュアなソフトウェア開発のコースを受講しない理由のトップは、「良いコースを知らないため」でした。この回答はいくつかの解釈ができます。まず、予算がないと答えた回答者は 29%であり、予算は制約事項ではありませんでした。また、研修を望んでいない、必要ないという理由の回答者がほとんどいませんでした。たとえば、自分は十分な知識がある (13%)、自分の役割に関係ない (9%)、それほど重要ではない (7%)、自分の組織に関係ない (4%) などの回答は少数でした。

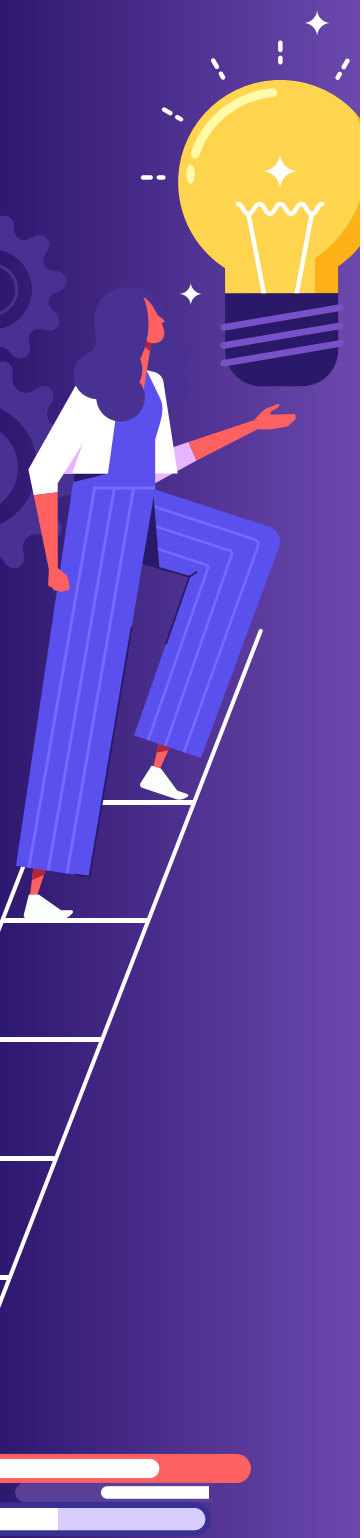
図 7 では、時間的制約が、良いコースを知らないことと僅差の上位の課題として挙げられていることにも気づくでしょう。この結果は、ソフトウェア開発の専門家が直面しているタイトなスケジュールを反映しています。この分野のトレーニングは、専門家が生産性を妨げることなく学習できるようにするため、柔軟で客観的であるべきでしょう。

図 7

セキュアなソフトウェア開発のコースを受講しない理由



2024 年 SecEd 調査、問 31、サンプル数＝ 150、総回答数＝ 239、問 20 で「いいえ」と答えた人のみが回答した質問



回答者は OpenSSF が無料の教材を提供していることを知らない

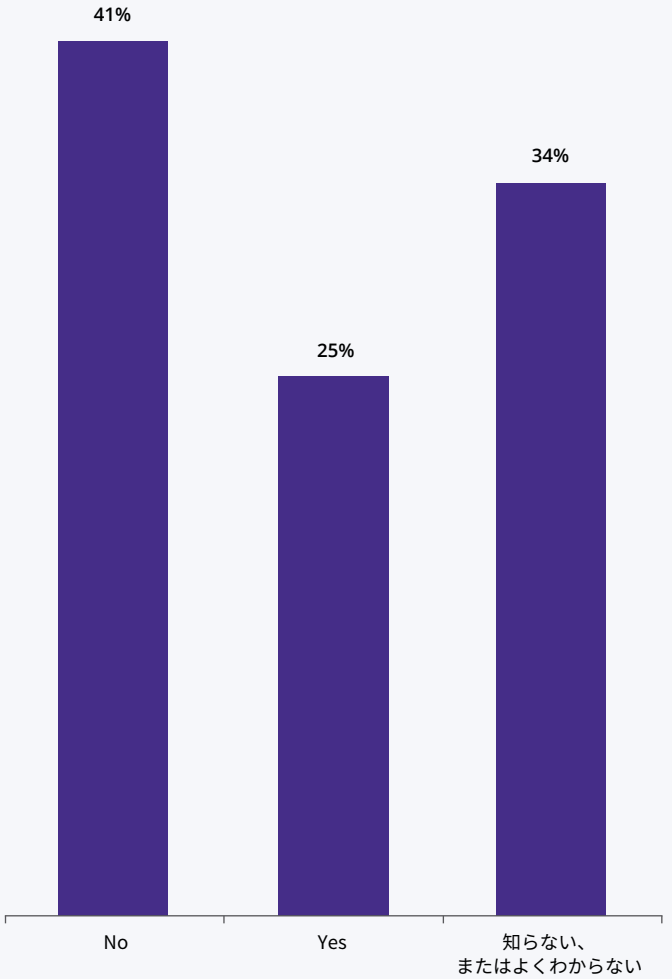
OpenSSF を含め、多くの組織がセキュアなソフトウェア開発に特化したトレーニングを提供しています。OpenSSF は、Linux Foundation が主催する OSS のセキュリティ向上を目的とした取り組みです。多くの取り組みの中で、OpenSSF は、開発者がセキュア コーディングに必要な知識とスキルを身につけるためのトレーニング プログラム、教材、リソースを提供しています。OpenSSF は、セキュアなソフトウェア開発の基礎知識に関するコースを無料で提供しています。しかし、図 8 で示すように、回答者の 4 分の 1 しか、所属組織で OpenSSF の教材を利用していないと回答しています。

OpenSSF は、Linux Foundation が主催する、OSS のセキュリティ向上を目的とした取り組みです。多くの取り組みの中で、OpenSSF は、開発者がセキュア コーディングに必要な知識とスキルを身につけるためのトレーニング プログラム、教材、リソースを提供しています。

どの教材も利用していない回答者の利用しない主な理由は、図 9 に示すように、OpenSSF がそのような教材を提供していることを知らないからでした。OpenSSF は、この調査結果を受け、セキュアなソフトウェア開発に関するトレーニングの提供を続け、宣伝活動を強化することを決めました。

図 8

OPENSSF のセキュアなソフトウェア開発に関する教材を使用している組織の割合



2024 年 SecEd 調査、問 21、サンプル数= 398

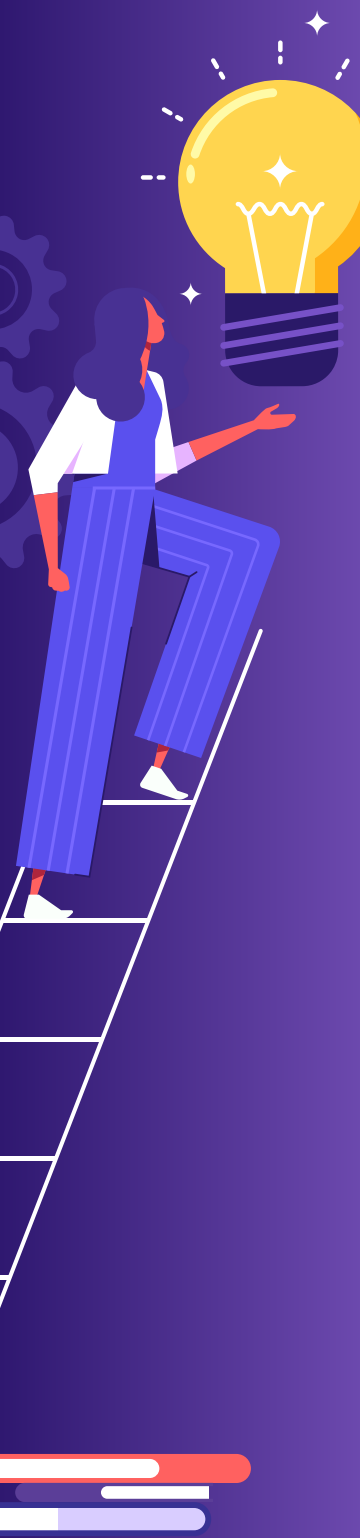
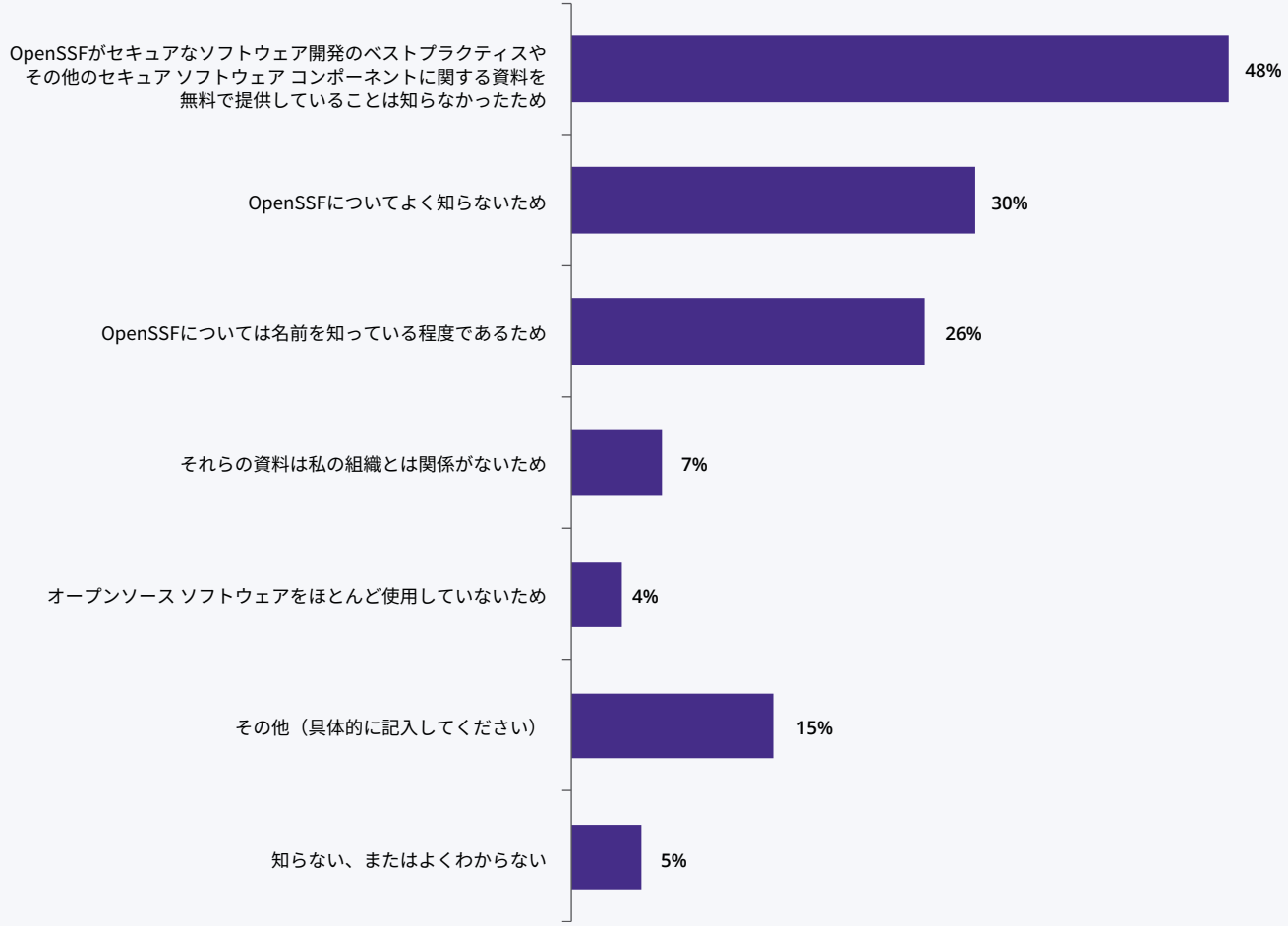
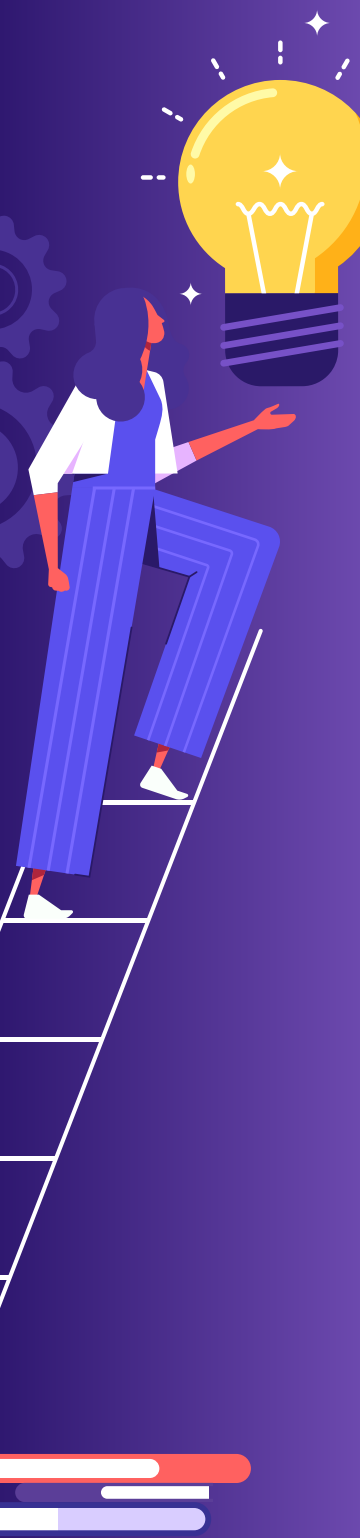


図 9

OPENSSF の教材を利用していない理由



2024 年 SecEd 調査、問 32、サンプル数＝ 135、総回答数＝ 181、問 32 で「いいえ」と答えた人のみが回答した質問

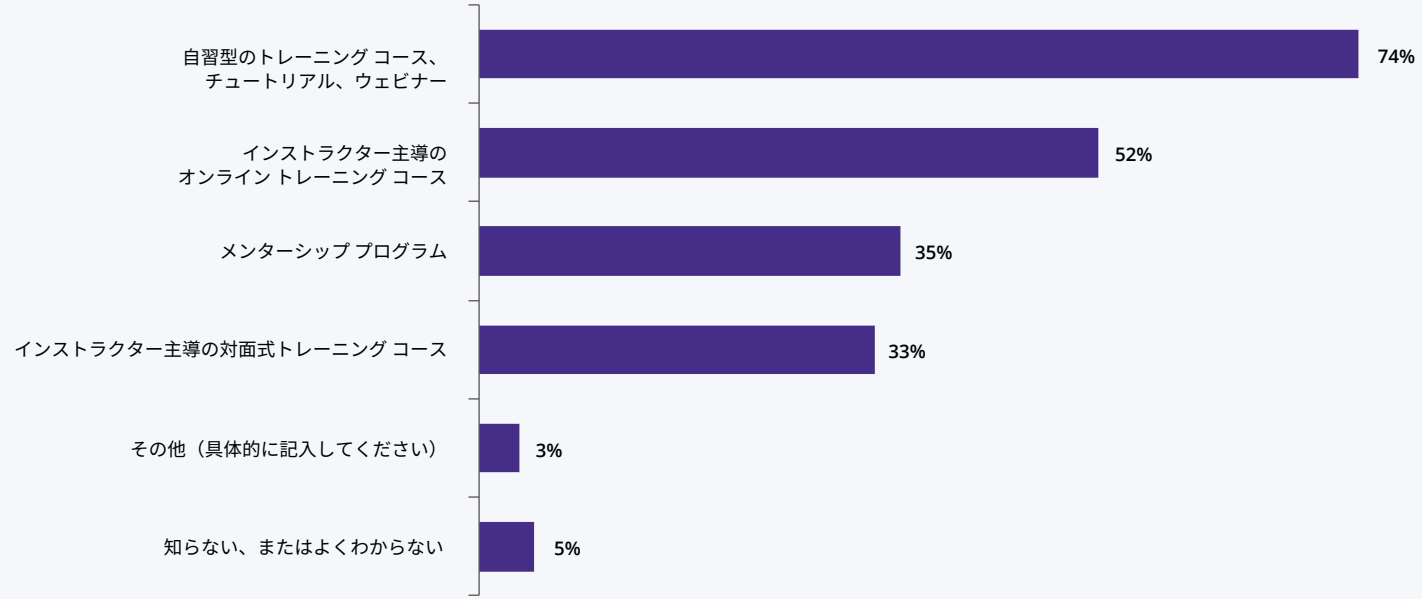


自習型トレーニングが人気

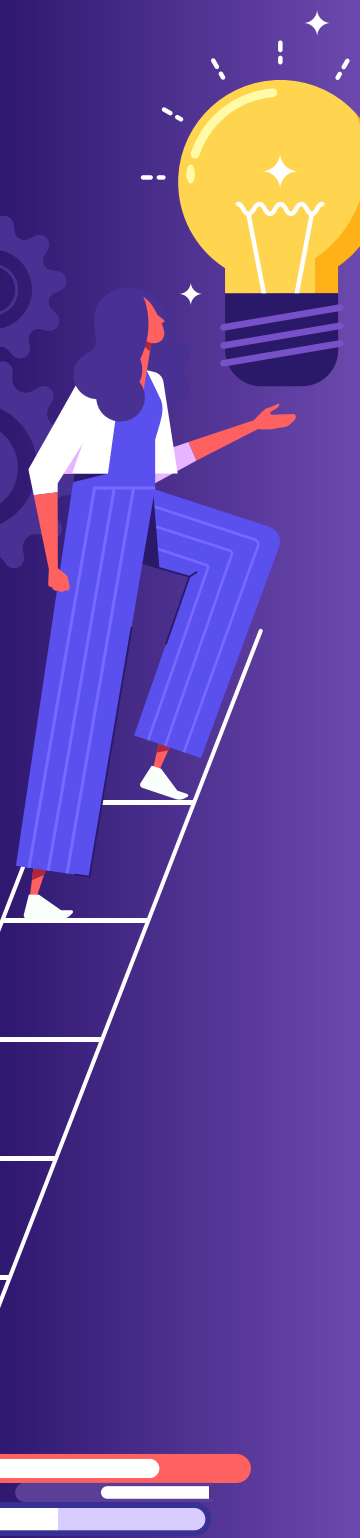
図 10 にあるように、組織が好む研修スタイルは、回答者の 74%が選択した自習型でした。この傾向は、多忙なスケジュールに合わせた柔軟な学習機会の提供が必要であることを示しています。インストラクターによるオンライン トレーニング コースも高く評価されており、回答者の 52%が有用であると回答しています。メンターシップ プログラムは回答者の 35% が利用しており、セキュリティ スキルを習得する上で、個別指導やサポートが重要であることを示しています。さらに、回答者の 33% がインストラクターによる対面式トレーニング コースが有益と考えており、対面式の学習環境の価値の高さを示しています。この結果から、セキュリティ教育の受け方に対する多様な好みとさまざまな学習ニーズに対応するため、組織は多様なトレーニング プログラムを提供する必要があると考えられます。

図 10

セキュリティに特化した教育プログラムやリソースで最も役に立ったもの



2024 年 SecEd 調査、問 30、サンプル数= 324、総回答数= 658

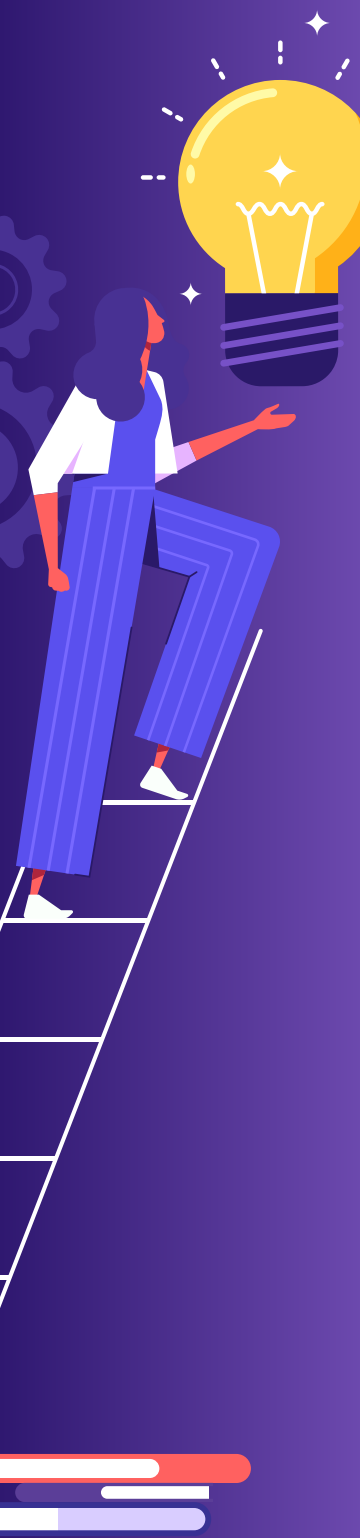


第 3 章：トレーニングにおいて優先度の高い分野

前章で述べたように、セキュアなソフトウェア開発には全般的なニーズがあり、より多くのトレーニングが必要です。ただ、この分野の範囲は広いため、トレーニングの取り組みや新しいコースの開発のためには何を優先すべきか理解する必要があります。本章では、受講者がプログラミング言語に依存しないトレーニングを好むか、プログラミング言語固有のトレーニングを好むかを分析し、最も必要とされるトピックを特定することにより、優先度の高い分野は何なのかを探ります。

本章の主な結果は以下のとおりです。

1. 回答者の 79%が、プログラミング言語に依存しないコースを非常に重要視しているのに対し、プログラミング言語固有のコースを重要視している回答者は 54%でした。
2. プログラミング言語診断コースの重要度が高いことは、職務、OSS との関わり方、地域、組織の種類、組織の規模にかかわらず一貫していました。
3. 回答者の間では、セキュリティ アーキテクチャー（64%）が最も人気が高く、セキュリティ教育とガイダンス（64%）、セキュアな実装（63%）がそれに続いています。
4. 専門性、OSS への関わり方、経験年数によってトレーニングのニーズに大きなばらつきがありました。最も人気があったのは、セキュリティ アーキテクチャー（ソフトウェア開発者とシステム運用）、セキュアな実装（マネジメントとデータ サイエンス）、脅威の評価（セキュリティ チーム）、ポリシーとコンプライアンス（OSPO チーム）でした。
5. 全体として、回答者はセキュリティ教育とガイダンスを最優先事項としています（ただし、この順位に関する注意点については以下を参照）。
6. Python に特化したコースは回答者の 71% があげており需要が高いです。一方、プログラミング言語の相対的な順位を考慮しない場合、2 位は JavaScript（クライアント側）で 49%でした。
7. Python コースは、OSS コミッターを除くすべての職務で最も高いニーズがありました。OSS コミッターは、C 言語コースのニーズが高いですが、Python も僅差の 2 位でした。
8. Python の全体的な人気の一方で、参加者に選択肢の中での重要度を聞いたところ、C（22%）と Java（18%）が Python（17%）よりも上位に選ばれました。
9. また、回答者は各組織でニーズのあるコースとして、認証、テスト、セキュアなコーディング プラクティス、サプライ チェーン セキュリティなどさまざまな専門的なトレーニングを挙げています。
10. 57%の回答者が AI と ML のセキュリティに対し、今後注目し技術革新が必要と指摘しています。また、サプライ チェーン セキュリティは 56%で、それに続いています。

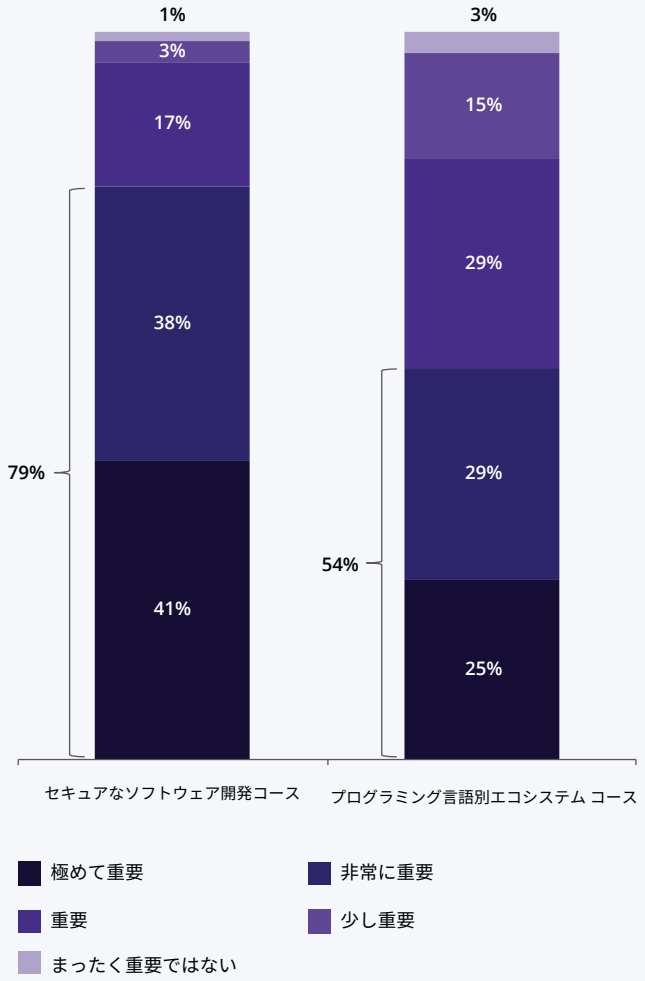


専門家は、特定のプログラミング言語に焦点を当てたトレーニングよりも、プログラミング言語に依存しないトレーニングの方が重要だと考えている

図 11 に示すように、回答者の 79%が、プログラミング言語に依存しないセキュアなソフトウェア開発トレーニングを「極めて重要」または「非常に重要」と考えているのに対し、プログラミング言語に特化したトレーニングを同レベルの重要度とした回答者は 54%しかいませんでした。プログラミング言語に依存しないセキュアなソフトウェア開発に関するコースは、プログラミング言語に特化したコースと比較すると、いくつかの利点があります。まず、さまざまなプログラミング言語やプラットフォームに適用されるセキュリティの原則を幅広く理解できるため、さまざまなエコシステムに適用できるようになります。プログラミング言語に依存しないコースでは、脅威のモデリング、セキュアな設計の原則、リスク評価など、セキュリティの基礎となるプラクティスを重視しています。このように普遍性があるため、知識の汎用性が高まり、多様な職場環境で応用できるようになるだけでなく、開発者は将来出現するかもしれない新しい技術やプログラミング言語にも対応できるようになります。

図 11

プログラミング言語に依存しないセキュアなソフトウェア開発コースとプログラミング言語固有のエコシステム コースの重要性



2024 年 SecEd 調査、問 27、サンプル数= 316、DKNS を除く

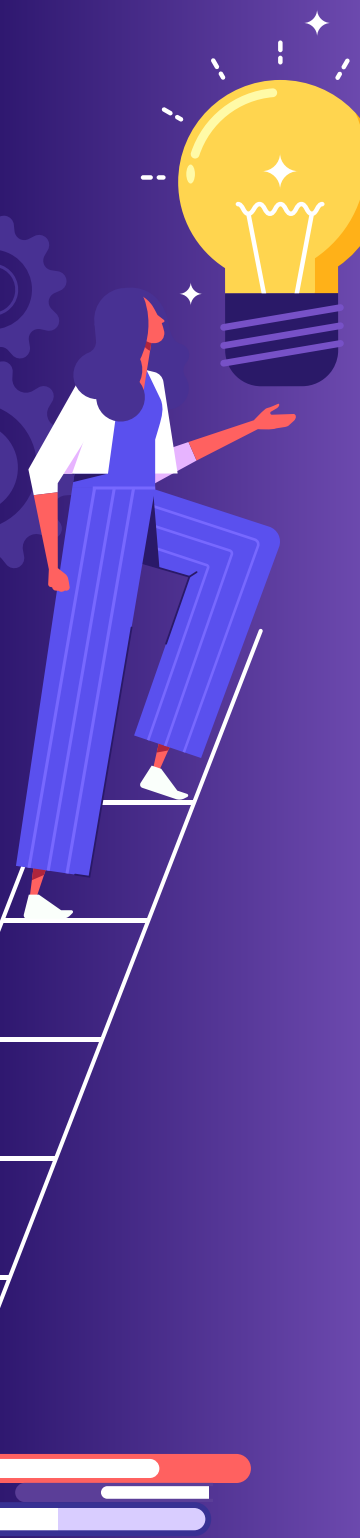
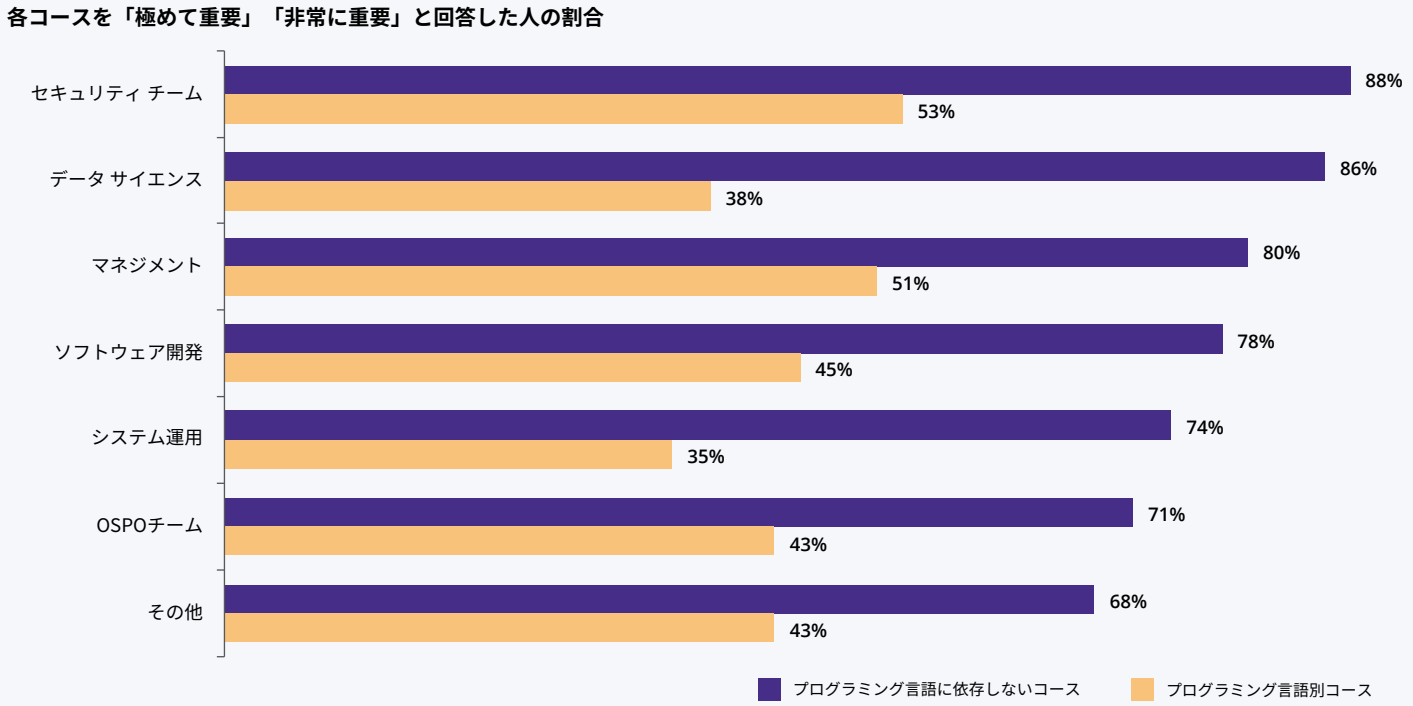


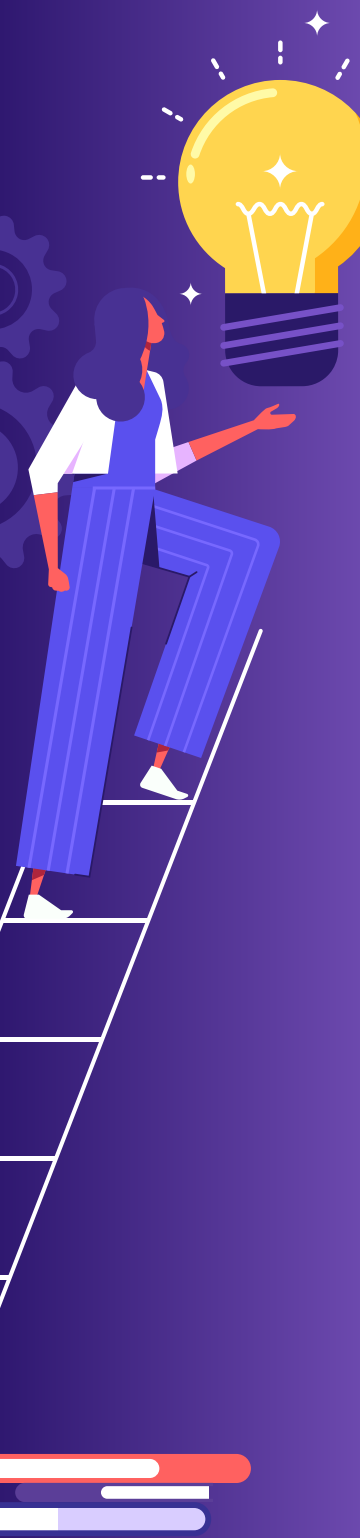
図 12

役割別に区分した、各種コースの重要度の比較



2024 年 SecEd 調査、問 27 と問 5 より構成、サンプル数=プログラミング言語に依存しない 316、プログラミング言語固有 318、DKNS は除く。

図 12 によると、プログラミング言語に依存しないコースへの人気は職種に関わらず一貫して高く、なかでも、複数のプログラミング言語で開発されたシステムに対応することが多いセキュリティ チームのメンバーから最も支持されています。さらに、OSS への貢献度、OSS での役割、地域、組織の種類、組織の規模によって区分した差異を分析しました。これらすべてのセグメントにおいて、回答者は一貫して、プログラミング言語に依存しないコースの方が、特定のプログラミング言語に特化したコースよりも重要であると評価しています。



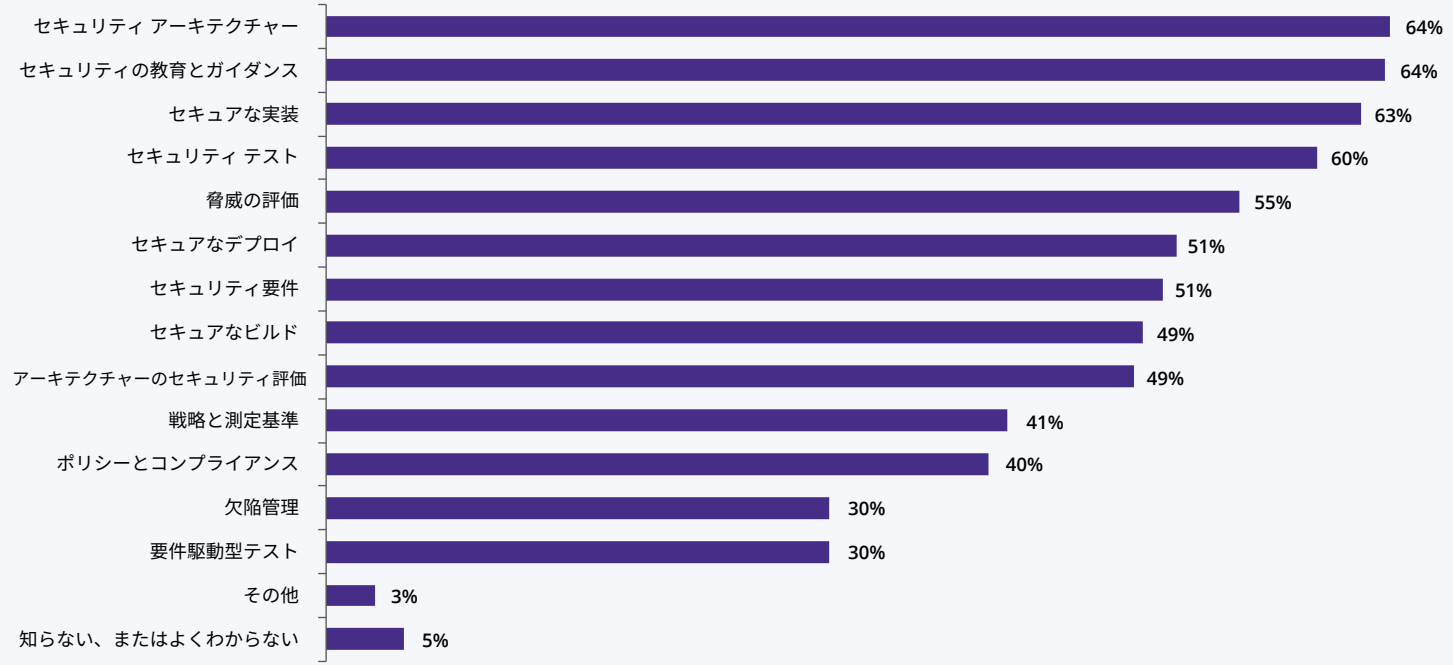
組織ではプログラミング言語に依存しない多種多様なコースを必要としており、セキュリティ アーキテクチャーは最も人気

組織は、教育格差を埋め、IT スタッフがセキュアなソフトウェア開発によりよく対処できるようにするために、プログラミング言語に依存しないさまざまなコースを必要としています。図 13 に示すように、「セキュアなアーキテクチャー」「セキュリティ教育とガイダンス」「セキュアな実装」「セキュリティ テスト」「脅威の評価」「セキュアなデプロイ」「セキュリティ要件」「セキュアなビルド」「アーキテクチャーのセキュリティ評価」の 9 つのコースが、回答者の 49% 以上から選ばれました。回答者が最も多く選択したのは「セキュリティ アーキテクチャー」（64.3%）で、僅差で「セキュリティ教育とガイダンス」（64.0%）、「セキュアな実装」（62.6%）が続いています。

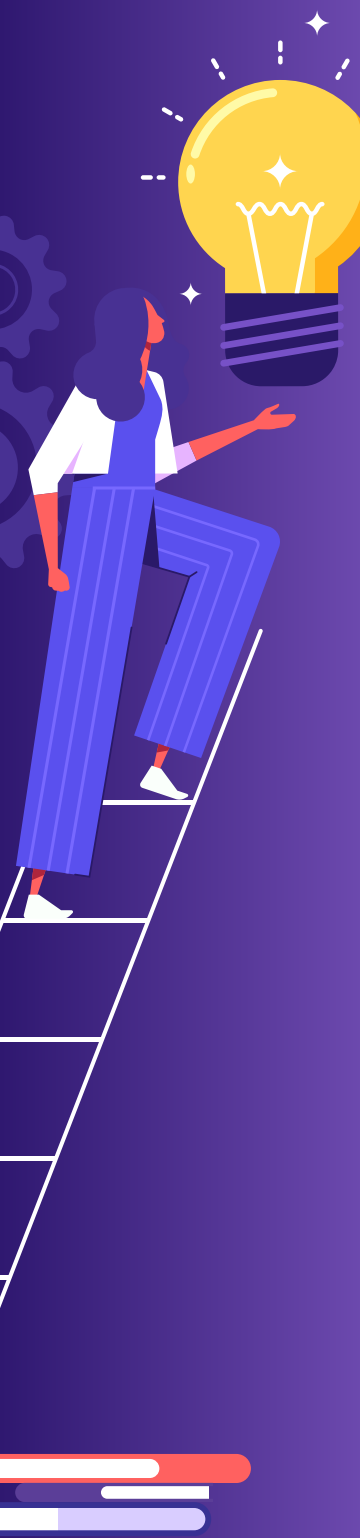
セキュリティ アーキテクチャーでは、セキュアなソフトウェア システムを構築・維持するために必要なプロセス、ツール、プロトコルを定義する構造化された枠組みを提供しています。セキュリティ アーキテク

図 13

プログラミング言語に依存しないコースは、企業の IT スタッフがセキュアなソフトウェア開発を行う上での知識の格差を埋めることができる



2024 年 SecEd 調査、問 25、サンプル数＝ 342、総回答数＝ 2,244



チャーにより、すべてのプロジェクトに一貫したセキュリティ標準を適用することができ、組織の目標やコンプライアンス要件に沿ったセキュリティ対策を実施するための青写真の役割を果たしています。このコースでは、セキュリティ要件を満たすために、ソフトウェアのアーキテクチャー設計、開発、デプロイの各段階で、コンポーネントや技術に関連するセキュリティ上の懸念に対処する方法について学習することができます。

選択肢の 1 つである「セキュリティ教育とガイダンス」の目的は、「従業員のセキュリティ意識を高め、セキュアなソフトウェアの設計、開発、デプロイにおいて、この知識とその他のガイダンスを活用するためのトレーニングを提供する」です。振り返ると、この選択肢は複数の解釈ができたため、もっと明確な定義が必要でした。ひとつの解釈として、この選択肢は「従業員に対する、最も適切なトレーニング順序をどう考案すべきか決めるための組織への支援」が目的と解釈できます。経験を積んだ回答者ほど、この選択肢を選ばなかった（予想されることとは正反対である）ことから、回答者の多くは、この解釈をしていないと思われます。別の解釈として、この選択肢は、セキュリティ教育とガイダンスに関する一般的な知識に焦点を当てた基礎的なことを学ぶコースだと解釈したと考えられます。他のデータを考慮すると、ほとんどの回答者が意図したのは後者の解釈であったと考えられます。OpenSSF には、セキュアなソフトウェア開発の基礎に関するコースはすでに他にありますが、前述のように、多くの回答者はそれを知らなかったと考えられます。

最後に、ソフトウェア開発におけるセキュアな実装コースでは、一般的な脆弱性を回避し、攻撃に対して堅牢なソースコードを実装する技術を学習します。このアプローチにより、ソフトウェア製品のコードには最初からセキュリティが埋め込まれることで、異次元の防御力が保証されます。開発者は、セキュアな実装を通してセキュアなコーディング プラクティスを適用することで、SQL インジェクション、クロスサイト スクリプティング、バッファ オーバーフローなどの脆弱性を防止することができます。コースの目的は、開発サイクルの序盤でリスクを軽減し、デプロイ後にセキュリティ問題を修正するコストと複雑さを軽減することです。セキュアな実装の基本は、プログラミング言語に依存せずに学習することができるものの、一般的に、より高度な能力を身に着けるためには特定のプログラミング言語に絞って学習する必要がある点には注意が必要です。

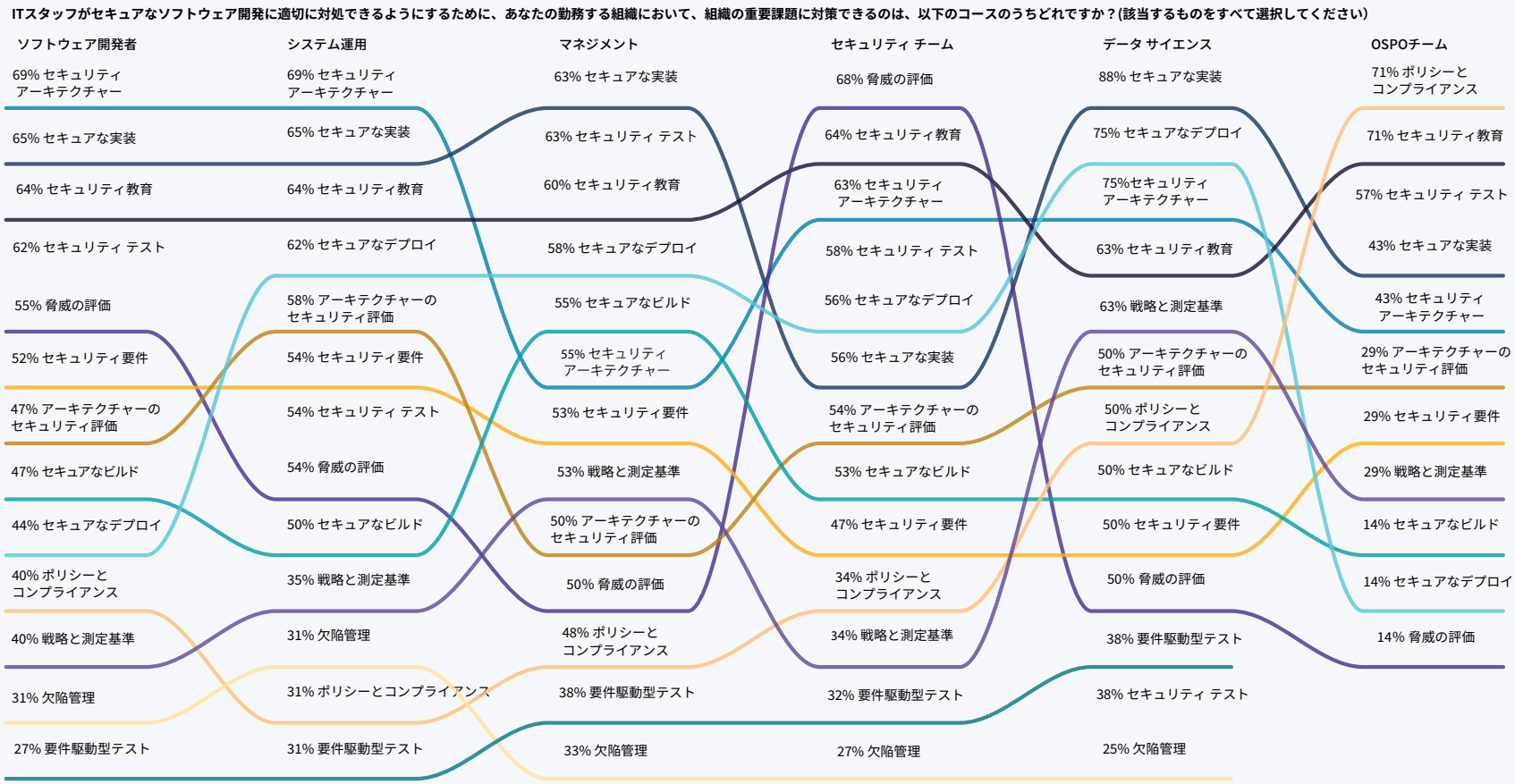
職務によってニーズは異なる

図 14 が示すように、各職務で求められる研修ニーズにはかなりのばらつきがありました。ソフトウェアの開発とデプロイに直接携わるソフトウェア開発者と運用担当者では、セキュリティ アーキテクチャーが最も人気でした。しかし、マネジメント（6 位）、セキュリティ チーム（3 位）、データ サイエンス（3 位）、OSPO チーム（5 位）では下位にランクされています。セキュアな実装は、マネジメントの専門家や、特にデータ サイエンスの専門家にとって人気がありました。セキュリティ チームにとっては、脅威の評価が最も人気の高いコースとしてランクインしており、一方、OSPO チーム メンバーではポリシーとコンプライアンスがトップでした。

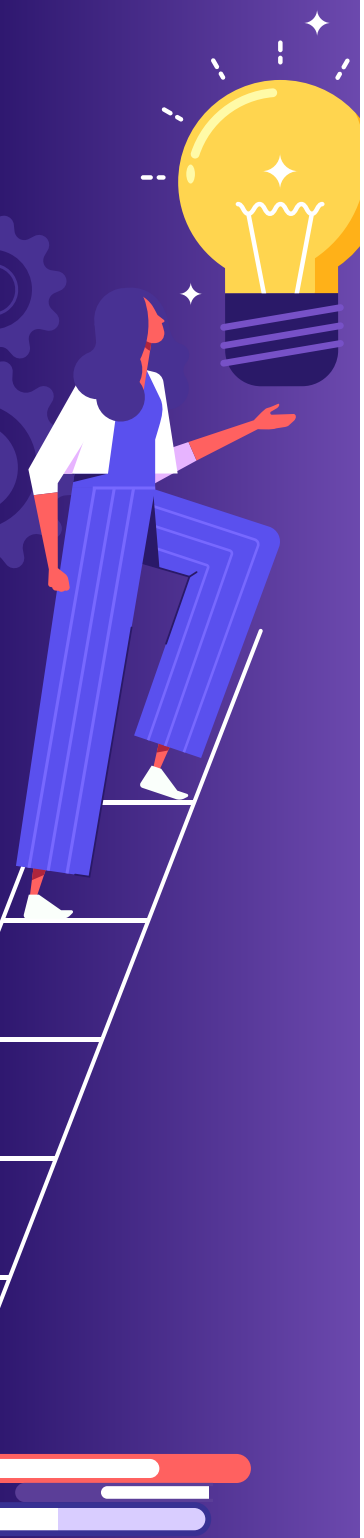
また、本分析を多角的にセグメント化したさまざまなランキングを、付録 B に掲載しています。OSS への貢献度（図 27）、地域（図 29）、組織の種類（図 30）、組織の規模（図 31）、セキュアなソフトウェア開発に関する知識の深さ（図 32）については、多少のばらつきはありますが、概ねセキュア アーキテクチャーやセキュリティ教育とガイダンスが上位を占めており、回答者の割合に大きな差はありませんでした。逆に、OSS での役割（図 28）や専門性（図 14）は、教育コースの人気に影響を及ぼすことがわかりました。さらに、経験年数もコースの選択に影響するようで、経験年数 5 年未満では「セキュリティ テスト」、5 年以上 20 年未満では「セキュリティ アーキテクチャー」、20 年以上では「セキュアな実装」の順位が高い結果となりました。

図 14

プログラミング言語に依存しないコースの職務別人気ランキング



2024 年 SecEd 調査、問 25 と問 5 より構成、サンプル数＝ 312、総回答数＝ 2,035、名前の前の数字は回答者の割合を表し、各列はこの数字でソートされています。



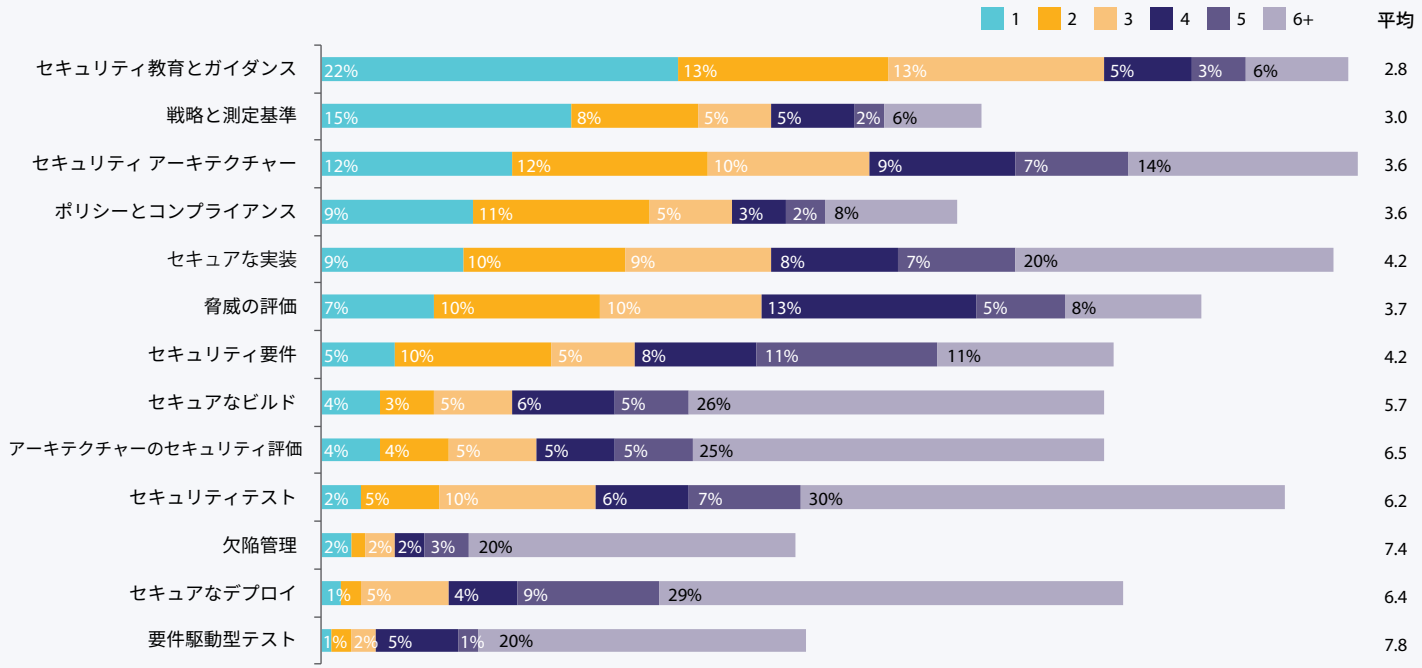
回答者は、セキュリティ教育とガイダンスが最重要事項と考えている

また、図 15 に示したコースの選択肢について、回答者に重要な順に順位付けをしてもらいました。図 15 を見ると、「セキュリティ教育とガイダンス」が最も重要なコースとして選択されている割合が高いことがわかります。

このコースは、選択肢から必要な 5 つを選択する重要度ランキングにおいても、トップでした。さらに、図 15 の右側に表示されている平均順位を考慮しても、このコースは他のコースを上回っています。平均順位でソートしても（図 15 の右側に表示）、1 位の割合でソートしても順位はほとんど変わらない点も重要なポイントです。

図 15

プログラミング言語に依存しないコースに対する重要度ランキング



2024 年 SecEd 調査、問 26、サンプル数= 308、順位 1 位の割合でソート

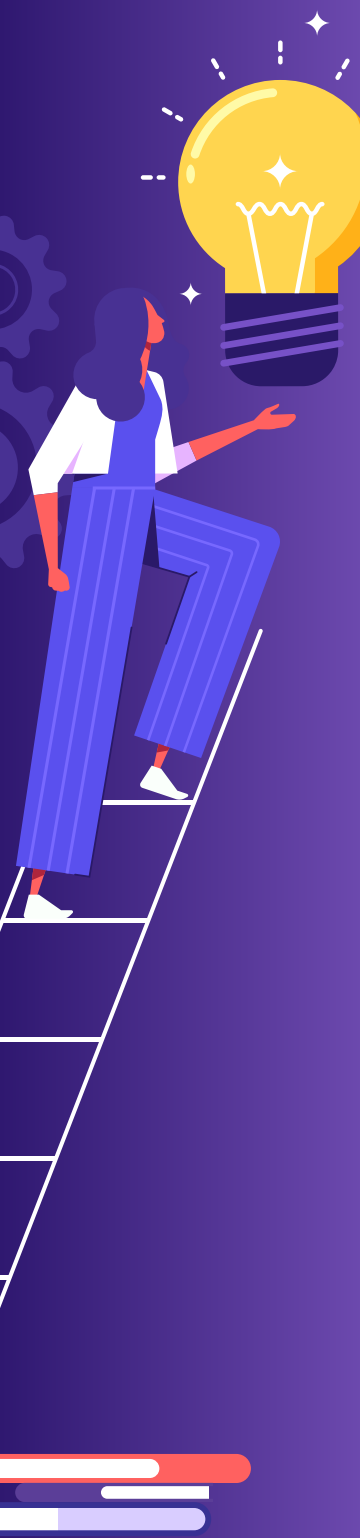


図 13 に示すように、人気度では 10 位以下であるにもかかわらず、図 15 では、戦略と測定基準が、人気上位の選択肢内の重要度ランキングとその平均順位の両方で 2 位となっています。この差は、「戦略と測定基準」が多くの人に注目されていないものの、重視する人にとっては高い価値を感じることができるコンテンツであり、より深い戦略や測定基準が求められる特定のニーズのある人にとって高く評価されていることを示しています。この分析結果は、教育プロバイダーにとっても有益な情報です。最も高い評価を示すユーザ層に向けカスタマイズし、効果的にマーケティングすることが可能になるでしょう。私たちのデータによると、戦略と測定基準を最重要選択肢に挙げる人は、主に大規模な組織（従業員数 20,000 人以上）に所属し、セキュアなソフトウェア開発に深い知識がありました。この傾向は、基本的なセキュリティの概念、ツール、プロセスを超えた、より複雑な組織環境に属する人が、セキュアなソフトウェアを効果的に開発・評価するために一定の戦略と評価基準を必要としていることを示しています。

Python に特化したコースが人気

プログラミング言語別コースの中では、Python に特化した教育への需要が高く、図 16 に示すように、重要度を考慮しない場合、回答者の 71%が需要があると回答しています。この需要は、回答者の 49%が支持する 2 番目に人気のある JavaScript（クライアント側）の需要を大きく上回っています。クライアント側とサーバー側の両方の JavaScript を選択した人の数値を合わせても、JavaScript の合計は 53% とわずかな違いしかなく、Python よりかなり低い数値となりました。これは主に、クライアントで JavaScript を使う人とサーバーで JavaScript を使う人が大きく重複しているためであると考えられます。

Python の人気はいくつかの要因が考えられます。Python は初心者にとってアクセスしやすいプログラミング言語として知られています。Python は、他のプログラミング言語から移行してきた人であれ、教育の過程で利用した人であれ、多くのプロフェッショナルがよく使うプログラミング言語になっています。特に、Python は GitHub[5] で

Python は GitHub で JavaScript に次いで 2 番目に人気のあるプログラミング言語であり、その使用率は前年比で 22% 以上も急増しています。Python は、AI や ML といった急速に成長している分野で注目されています。

JavaScript に次いで 2 番目に人気のあるプログラミング言語であり、その使用率は前年比で 22% 以上急増しており、AI や ML といった急速に成長している分野で注目されています。開発者が Python にシフトしていることと、Python のセキュアなソフトウェア開発に焦点を当てた教材が比較的少ないことが重なって、Python のコースの需要が高くなっているのでしょう。Python のコードを悩ませる一般的な脆弱性には、インジェクションや任意のコマンドの実行、安全でないファイル操作、古い依存関係、ディレクトリ トラバーサル、不適切なパッケージ管理などがあります。

とはいえ、2 番目の選択肢である JavaScript も、GitHub のリポジトリで最も人気のプログラミング言語であり、ソフトウェア開発の重要な要素であることに変わりはありません。クライアント側の JavaScript は、クロスサイト スクリプティングや機密データの流出といった脆弱性にさらされています。

5 https://github.blog/2023-03-02-why-python-keeps-growing-explained/

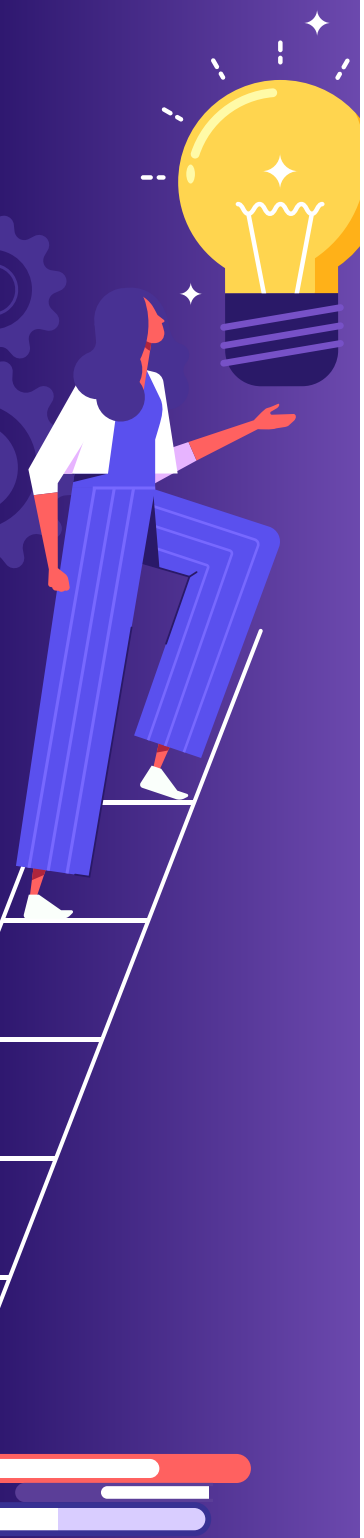
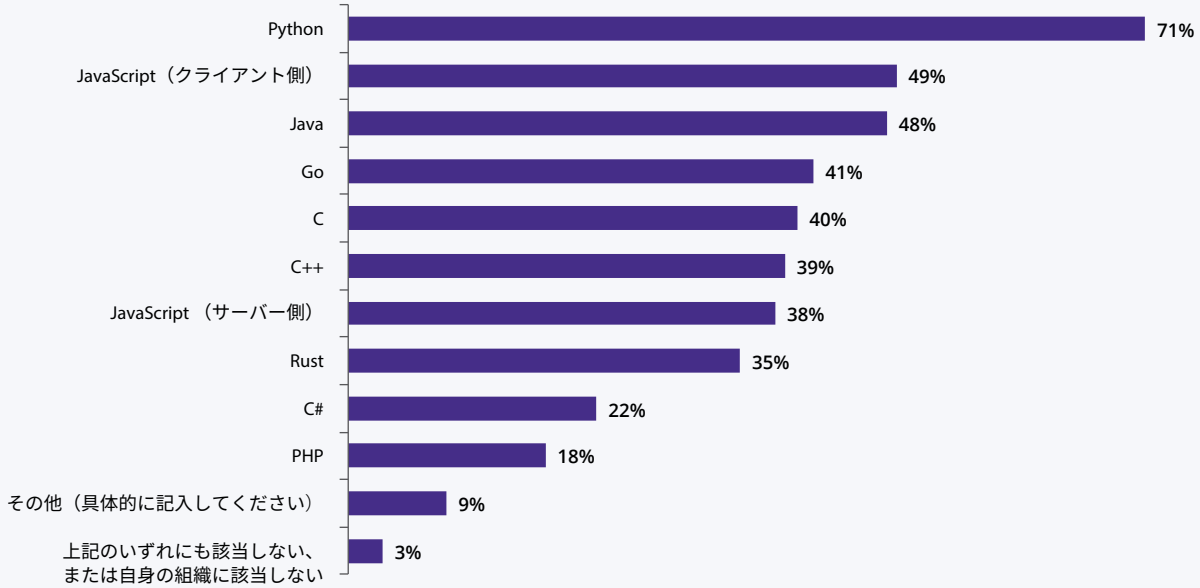


図 16

組織が開発者に提供すべきプログラミング言語別エコシステム コース



2024 年 SecEd 調査、問 23、サンプル数＝ 352、総回答数＝ 1,454

Python はさまざまなチームに人気がある

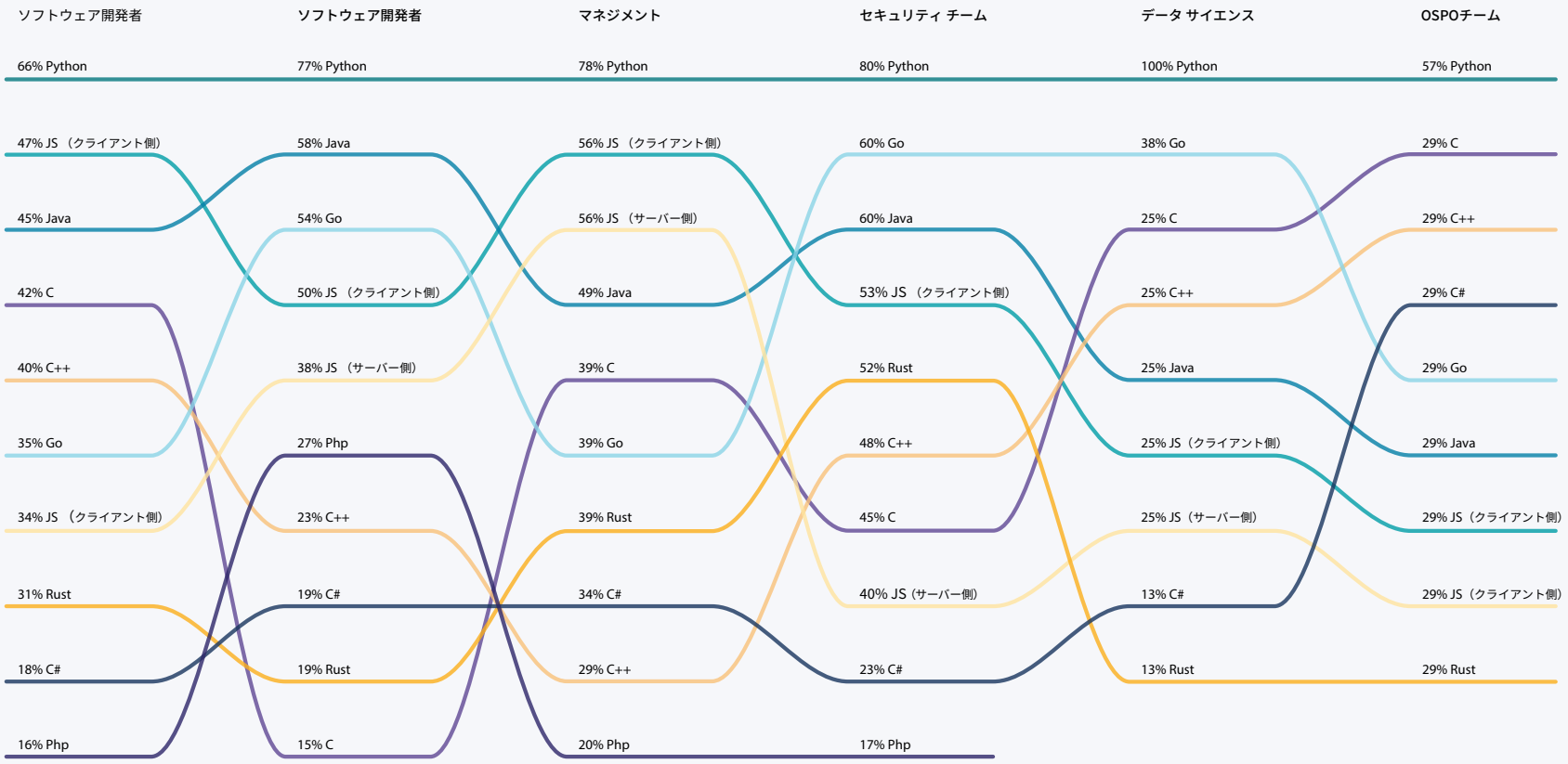
図 17 に示すように、重要度を無視した場合、プログラミング言語固有のコースの中で、Python に特化したセキュリティ コースが、すべての職務で最も人気がありました。図 17 は、データ サイエンスの専門家における Python の人気を示しており、データ サイエンスの専門家は、Python に特化したコースが自分たちのニーズと関連が強いことをよく認識しています。

プログラミング言語別のコースのランキングをセグメント化した付録 C にも示されるように、Python は、OSS コミッターを除くすべての職務で最も人気がありました。OSS コミッターは、Python は僅差で 2 位で、C 言語のコースに高い人気があります。これは、より低レベルのプログラミング課題に対処する機会が多い OSS コミッター特有の要求を反映しています。対照的に、Python の広範な人気は、さまざまな分野での広範な有用性と魅力を反映しています。

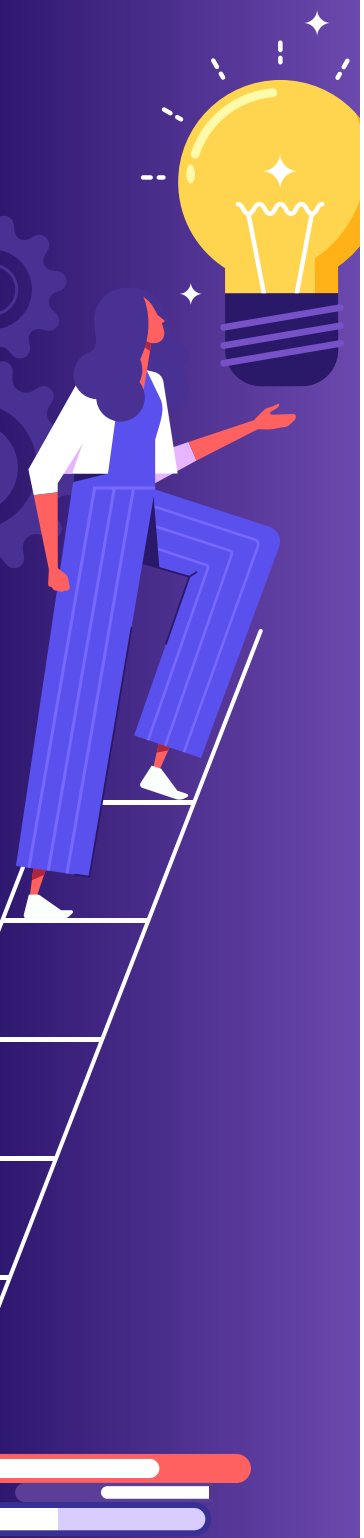
図 17

職務別に見たプログラミング言語別コースの人気ランキング

セキュア ソフトウェア開発に関する言語固有のエコシステム コースのうち、あなたの所属組織が開発者に提供すべきものはどれですか？（該当するものをすべて選択してください）



2024 年 SecEd 調査、問 23 と問 5 より構成、サンプル数＝ 321、合計回答数＝ 1,320、名前の前の数字は回答者の割合を表し、各列はこの数字でソートされています。



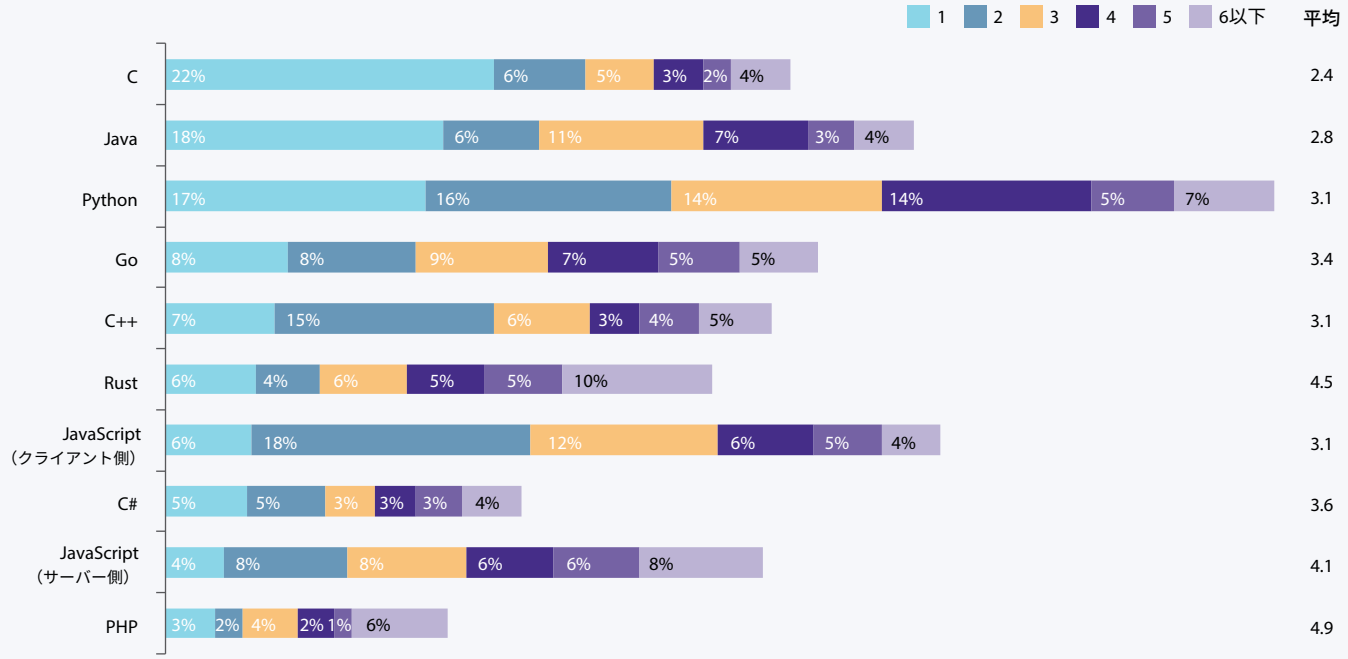
C と Java はトップの選択コースとして頻繁に選択されている

全体的な人気とは対照的に、回答者に選択肢をランク付けするように求めたところ、C と Java が Python よりも頻繁にトップの選択肢として選ばれました（図 18 参照）。

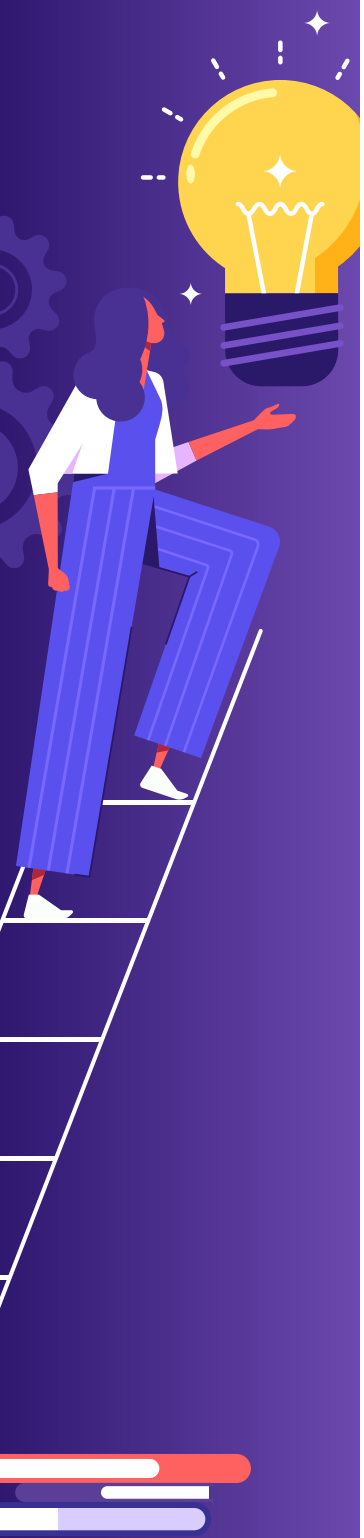
しかし、上位 2 つまたは 3 つの選択肢まで考慮すると、Python がリードしています。これは、Python が他の言語と一緒に選ばれることが多いことを示しており、Python がプログラミング言語のより大きなエコシステムの一部としての役割を果たしているのに対し、C 言語と Java は単独で選ばれることが多いという可能性があります。

図 18

選択した各プログラミング言語別コースに対する回答者の重要度ランキング



2024 年 SecEd 調査、問 24、サンプル数＝ 331、順位 1 位の割合で並べ替え



C 言語は重要なインフラを構築するために使用されており、この言語のセキュアなソフトウェア開発コースには学ぶべき点が多くあります。C 言語では、バッファー オーバーフロー、初期化されていない変数、ヌル ポインターの再参照、不適切な型変換、free 後の使用、二重 free などの脆弱性の影響を受けやすいです。Java もまた多くの用途で使用される言語であり、さまざまな種類のシステムやアプリケーションで広く使われています。TIOBE[6] での調査によると、若干 Java の人気は低下つつありますが、依然としてさまざまな新しいシステムの構築に極めて重要な状況です。また、数十年にわたって利用されてきたため、市場の Java を使用した生産システムもたくさんあるでしょう。

組織にはさまざまなニーズがある

回答者には自由記述の質問で、コースに対するニーズを自由に回答してもらいました。表 1 は、回答を分類したものです。回答の多くは、これまでの質問ですでに取り上げられているものですが、いくつかの興味深いトピックがありました。

まず、認定資格が高く評価されました。特定のトピックに関するプロフェッショナルな専門知識を認証し、標準化された知識ベースを確立することができます。組織にとって、認定資格は、ソフトウェア セキュリティの担当者個人がベストプラクティスや最新手法の知識があることを保証するものです。CSSLP（Certified Secure Software Lifecycle Professional）や CEH（Certified Ethical Hacker）などの認定資格は、個人の専門知識とセキュリティ分野へのコミットメントを証明するものであり、多くの場合、雇用主から要求されます。さらに、認定資格は継続的な教育や更新を義務付けていることが多いため、継続的な学習文化を維持するのに役立ち、進化する脅威や技術に遅れを取らないようにすることができます。

また、「検証」も回答が多かったテーマでした。定期的かつ包括的な検証は、攻撃者に悪用される可能性のあるバグを回避するのに役立つだけでなく、特定のセキュリティ課題に対する演習にもなります。静的アプリケーション セキュリティ テスト（SAST）は、ソースコードを実行することなく、脆弱性を発見するためにソースコードを検証する手法です。単体テストは、プログラムの一部（「ユニット」）に特定の入力を与え、その結果が期待されるものかどうかを判断します。ファジングは、「ランダムに」入力を生成してソフトウェアを実行し、望ましくない動作（クラッシュなど）を検出します。ウェブ アプリケーション スキャナーは、攻撃者のブラウザをシミュレートし、ウェブ アプリケーションのウェブ ページをクロールし、セキュリティの脆弱性がないかどうかを調べます。「動的アプリケーション セキュリティ テスト」（DAST）という用語には、さまざまな意味があり、ウェブ アプリケーション スキャナー[7,8] の同義語として使われることもあれば、ウェブ アプリケーション スキャナーやファジング[9,10] を含む意味で使われることもあります。このような技術は、ソフトウェア開発ライフサイクルのさまざまな段階において、広範な脆弱性を見つけ出すことができます。重要なのは、セキュリティ テストの自動化と、継続的インテグレーション／継続的デプロイメント（CI/CD）パイプラインの統合にフォーカスすることが重要だと強調する回答があったことです。

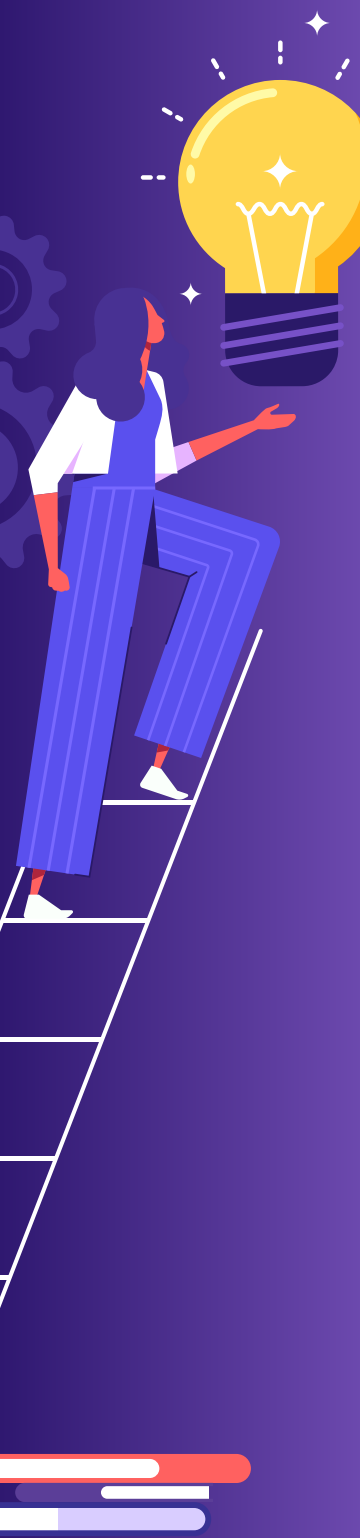
6 https://www.tiobe.com/tiobe-index/

7 https://www.veracode.com/security/dast-test

8 https://www.csoonline.com/article/3487708/9-top-fuzzing-tools-finding-the-weirdest-application-errors.html

9 https://insights.sei.cmu.edu/sei_blog/2018/07/10-types-of-application-security-testing-tools-when-and-how-to-use-them.html

10 https://blog.code-intelligence.com/what-is-fast



実装プロセスにおいては、セキュリティを直接組み込むことの重要性が示されました。なかでも、実装のベストプラクティスと防御的プログラミングに焦点を当てた教育プログラムが重要と示されています。このようなコースでは、開発者がソフトウェア開発の初期段階からセキュリティ対策を取り入れ、潜在的な脅威に対してより堅牢なコードを作成できるように指導しています。

また、サプライ チェーン セキュリティに関するコースも多くのリクエストがありました。現代のソフトウェアは個々に存在するのではなく、外部パッケージとの相互依存の広大なネットワークに接続されています。最近のサイバーセキュリティにおける大きな問題にも見られるように、現代のソフトウェア サプライ チェーンは複雑で相互につながっているため、どのコンポーネントの脆弱性であっても、システム全体を危険にさらす可能性があります。そのため、開発者は、サプライ チェーン全体で厳格なセキュリティ対策を行うことが不可欠です。これには、サードパーティ ベンダーを吟味すること、検証済みの安全なオープンソース ライブラリを使用すること、サードパーティ製コンポーネントの脆弱性を継続的に監視することなどが含まれます。ソフトウェアに使用されるすべてのコンポーネントの透明性を確保し、潜在的なリスクをより適切に管理することを可能にするため、最新のソフトウェア部品表（SBOM）を正確に維持することが極めて重要です。

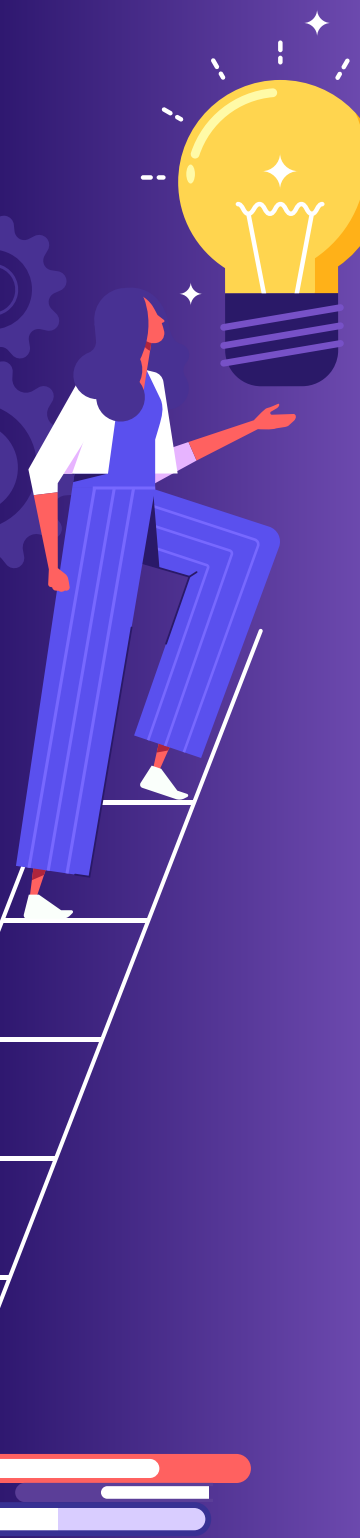
まとめると、表 1 にはセキュア ソフトウェア開発に関してリクエストの多かった教育分野を分類しており、IT セキュリティの多面的な課題に合わせた専門的なトレーニングの必要性が示されています。

表 1

自由記述のアンケートで回答者の要求が多かったコース内容

トピック	例
認定	CEH, CASE, CSSLP, CISA, CISSP, CSSE, CSSLP, OSP
テスト	自動セキュリティ テスト、レガシー コードへの最新テスト、コード セキュリティ テスト、DAST、SAST、ファジング、侵入テスト、ユニット テスト
コーディング プラクティス	実装のベストプラクティス、コーディング ルール、防御的プログラミング、エラー処理、コードにセキュリティを組み込む方法、OWASP トップ 10 に基づくコーディング
サプライチェーン	サプライ チェーン セキュリティ、SBOM、依存関係管理、使用前パッケージのスクリーニング、Sigstore、サプライ チェーン攻撃、ツーリング
脅威のモデリング	アジャイル脅威モデリング、脅威分析、脅威インテリジェンス、信頼境界の効果的な定義による脅威モデリング、脆弱性分析
セキュアなアーキテクチャー	セキュアな設計、セキュアな API 開発、セキュアな設計パターン、テストに重点を置いたセキュアなソフトウェアの設計
クラウド セキュリティ	クラウドネイティブ セキュリティのベストプラクティス、クラウド構成、パブリック クラウド、AWS、AZ-500
セキュアなソフトウェア開発（全般）	キャリア初期のエンジニアのためのセキュアなソフトウェア開発、セキュアなソフトウェア開発の基礎、全体的なセキュリティの視点
アイデンティティとアクセス管理	アクセス制御、アクセス管理、認証、IAM

2024 年 SecEd 調査、問 22、サンプルサイズ= 558、各回答者は 2 つの回答を記述、表は重複した回数順にソート、上位トピックのみ表示



今後現れる新しい分野

セキュアなソフトウェア開発は、多くの要素で構成されており、絶え間ない進化をしているため、変化し続けています。私たちは、図 19 に示すように、セキュアなソフトウェア開発において、今後さらに注目と革新が必要となる領域について、回答者に調査を行いました。

AI と ML のセキュリティは顕著な懸念事項であり、回答者の 57%が、セキュアなソフトウェア開発の観点から、より高い関心とイノベーションが必要な分野であると認識しています。これらの技術がさまざまな産業で不可欠になるにつれて、そのセキュリティへの影響はますます重要になっています。AI や ML システムでは、データを集約し運用するという特性と相まって、データ ポイズニング、モデルの盗用、敵対的攻撃といった独自の脆弱性にさらされています。現時点では、セキュアな ML システム（「敵対的機械学習」）の開発には多くの未解決の研究すべき課題があり、現在知られている緩和策は、一般的に敵対者に対してまだ十分なものではありません。[11] これらのテクノロジーが進化し、拡大するにつれて、AI や ML の堅牢なセキュリティ対策がますます重要になります。

AI と ML のセキュリティに次いで重要な分野は、サプライ チェーンのセキュリティであると回答者の 56%が回答しており、これは前節で説明した自由記述の質問の結果とも一致しています。ソフトウェア開発エコシステムの複雑化、相互接続性、グローバル化の進展により、サプライ チェーンのセキュリティ確保は今後ますます重要になります。企業がライブラリやフレームワークから開発ツールに至るまで、多数のサードパーティ コンポーネントやサービスを利用するにつれて、潜在的な脆弱性を狙った攻撃のターゲットが大幅に拡大しています。さらに、ソフトウェア セキュリティとデータ保護規制の要求が世界的に厳しくなるにつれて、コンプライアンスがより困難になっています。

ソフトウェア開発エコシステムの複雑化、相互接続性、グローバル化の進展により、サプライ チェーンのセキュリティは今後ますます重要になるでしょう

11 https://csrc.nist.gov/pubs/ai/100/2/e2023/final

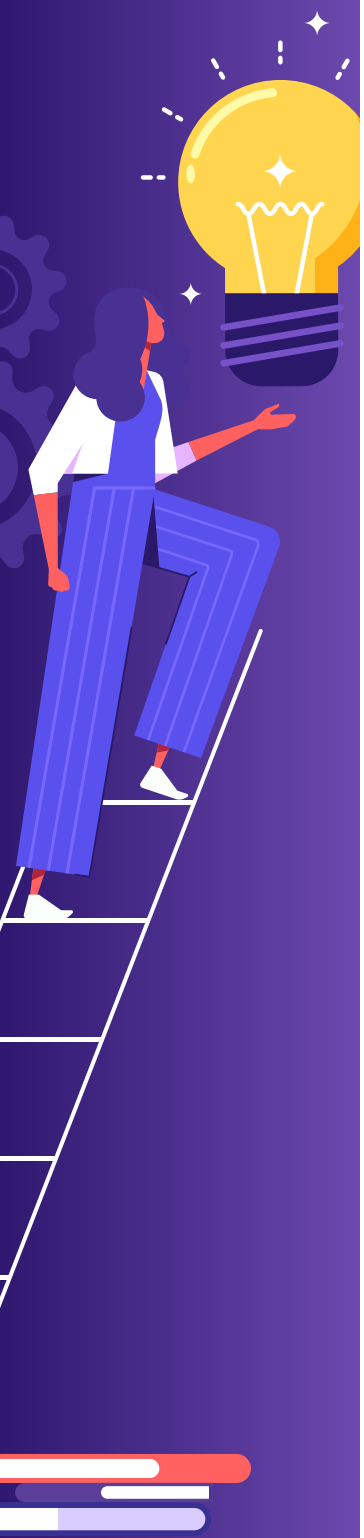
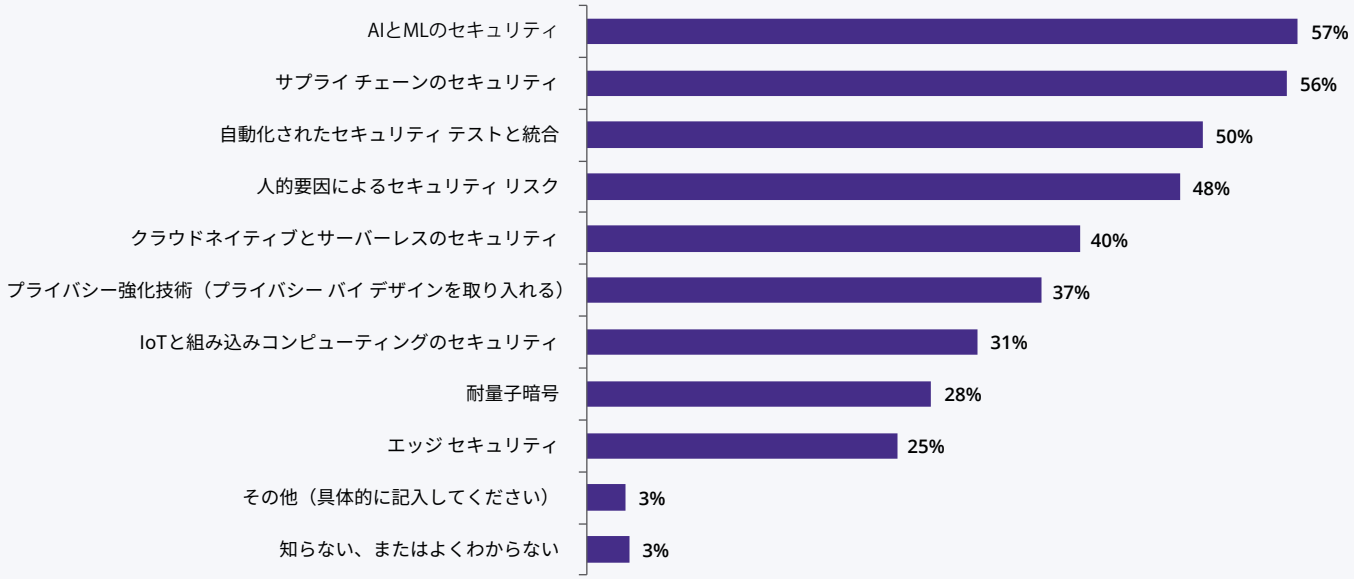


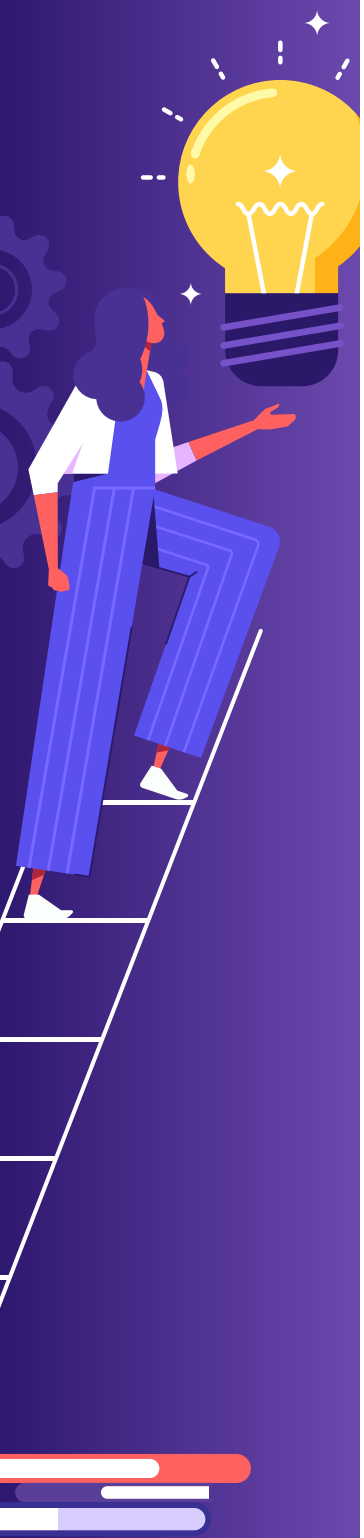
図 19

セキュアなソフトウェア開発において、今後さらに注目と革新が必要な分野



2024 年 SecEd 調査、問 29、サンプル数＝ 324、総回答数＝ 1,227

この調査では、他にもいくつかの懸念事項が浮き彫りになりました。自動化されたテストと統合については、回答者の 50%が、自動化により、継続的に脆弱性を特定し対処する強固な仕組みが必要だと回答しています。半数近く（48%）が人的要因によるセキュリティ リスクを挙げており、サイバーセキュリティ侵害において人的ミスが重要な懸念材料であることを反映しています。クラウドネイティブとサーバーレスのセキュリティに関する懸念は、参加者の 40% が挙げており、最新のコンピューティング パラダイムへの移行と、それらに特有のセキュリティ要求を反映しています。プライバシー強化技術は 37% が重要と挙げており、プライバシー規制が強化される中で個人データ保護の重要性が高まっていることを物語っています。その他の懸念分野としては、モノのインターネット（IoT）および組み込みコンピューティングのセキュリティ（31%）、耐量子暗号（28%）、エッジ セキュリティ（25%）が挙げられました。



第 4 章：OpenSSF におけるコース選択

この OpenSSF セキュリティ教育アンケートを実施した重要な目的の 1 つは、OpenSSF が次にどのようなコースを開発すべきかを特定するためでした。OpenSSF では、推測や数人へのヒアリングだけでなく、大規模な調査から得られる定量的なデータに基づいて意思決定をしたいと考えました。調査の結果、OpenSSF は、以下に説明する理由から、セキュリティ アーキテクチャーを開発対象として選択しました。

このアンケートを実施する前に、OpenSSF は、一般的に C、Java、Python のようなプログラミング言語固有のコースが回答者に人気があるのではないかと考えていました。実際、54%がプログラミング言語固有のコースを「非常に重要」または「重要」と回答しており、多くの人がそれらの教材に関心を持っていることが分かります。しかし、79% はプログラミング言語に依存しないコースを「非常に重要」または「重要」と回答しています。この結果を受けて、OpenSSF はプログラミング言語エコシステムに依存しないコースの作成に注力すべきであると考えを改めました。

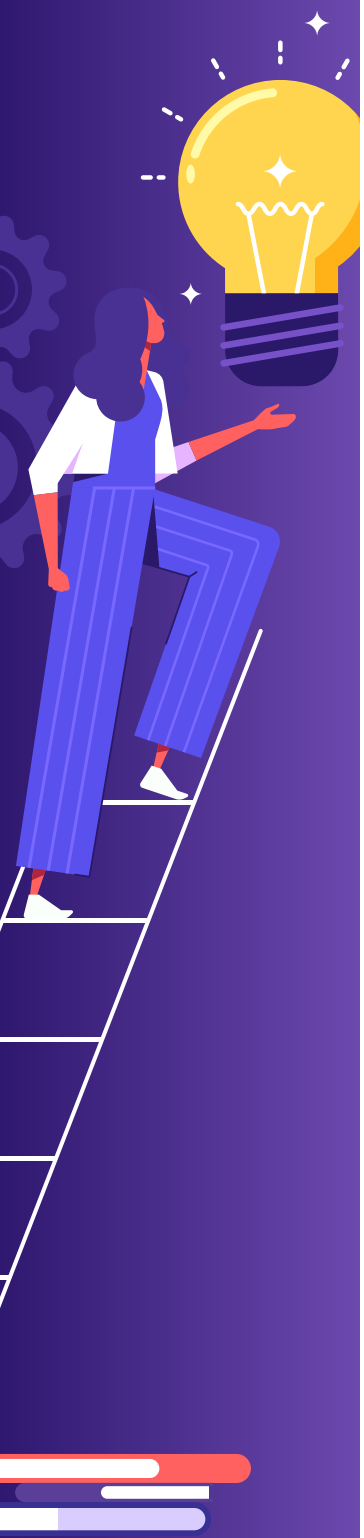
厳密には、考え方により「トップ」とされる分野はさまざまで、非常に複雑でした。

- 人気では、セキュリティ アーキテクチャー、セキュリティ教育とガイダンスが最も人気が高く、次いでセキュアな実装、セキュリティ テスト、脅威の評価が続きました。
- 最も重要度の高い選択肢だけを見ると、セキュリティ教育とガイダンスが最も多く、次いで、戦略と測定基準、セキュリティ アーキテクチャーの順となりました。
- 人気度を考慮した平均重要度ランキングでは、セキュリティ教育とガイダンスがトップで、セキュリティ アーキテクチャーとセキュアな実装がそれに続きました。

このばらつきが意思決定をより複雑にしました。職務別の分析の結果、職務によって重視される分野に傾向があることがわかりました。セキュリティ アーキテクチャーは、ソフトウェア開発者とシステム運用者において最も重要と評価されており、セキュリティ チームでは第 3 位でした。マネジメント、データ サイエンス、OSPO それぞれ、重要度の順位が異なります。このように、複数の「トップ」回答があることが理解できるかと思います。

地域別に分けてみると、興味深い違いがありました：米国とカナダ以外では、セキュリティ アーキテクチャーがトップでした。一方、米国とカナダでは、上位 2 つはセキュリティ教育とガイダンス、セキュアな実装でした。これは、米国とカナダでは、さまざまな職務の回答者が混在しているため、回答者のばらつきが大きくなっていることを示していると考えられます。

経験年数も大きな影響がありました。経験年数が 5 年未満の人はセキュリティ テストを最重視し、経験年数が 5 ～ 20 年の人はセキュリティ アーキテクチャーを最重視しました。経験年数が 20 年以上の人は、セキュリティ実装を最重要項目とし、セキュリティ アーキテクチャーを 2 位としています。我々は以下のような仮説を立てています：経験の浅い開発者は、セキュリティ テストによって欠陥の全部または大部分が発見されると期待しているのではないかと思います。開発者は経験を積むにつれて、テストによるアプローチが重要である一方で、テストが偽陽性や偽陰性を引き起こすということが、セキュリティ アーキテクチャーに起因しており、それらがセキュリティに与える影響が非常に大きいと気づくため、開発者はセキュリティ アーキテクチャーについてもっと知りたいと思うようになります。経験年数が 20 年になるころには、セキュリティ アーキテクチャーを習得しており、まだ興味が尽きない人はセキュリティ実装の知識をつけようとしていると考えられます。



OpenSSF ではこれらのすべてのコースを開発したいですが、リソースに限りがあり、どのコースを開発するか選択を迫られました。有望に思える分野でも、検討するとそうでないものもありました。

1. セキュリティ教育とガイダンスが上位にランクされていますが、これは概念的なものを指していると思われます。この定義は教育システムの構築に焦点を当てたものでしたが、初心者がこの項目を高く評価していました（図 33）。これは、多くの回答者が質問に記載された定義ではなく、一般的に教育やガイダンスが欲しいというイメージをもとに回答しているものと考えられます。

2. セキュアな実装も高く評価されていますが、既存の OpenSSF の基礎コースに、プログラミング言語に依存しないセキュアな実装コースがすでに設置されています。セキュアな実装についてより深く掘り下げることもできますが、その場合、基本的にプログラミング言語ごとのコースが必要になります。別の回答では、プログラミング言語固有の教材の多くは、重要ではあるものの最重要ではないことが示されています。プログラミング言語固有の教材の重要度が低かったことから、セキュアな実装の重要度はそれほど高くなく、フォーカスすべきでないと考えました。

3. セキュリティ テストは、自由記述のフィードバックや初心者からの回答において高い評価でした。これは有用な情報であり、将来的には素晴らしいコースの提供につながるかもしれません。一方、経験者においては回答者の評価はさまざまで、高く評価されている分野もあれば、かなり低い分野もありました。このトピックは、間違いなく今後検討を進めるべきトピックですが、直近のコースの創設という観点では期待薄と判断しました。

マネジメント職の回答者は、他の職務の回答者と異なる優先順位でした。しかし、OpenSSF はすでにマネジメントに焦点を当てたコースを提供しており、OpenSSF では、このコースが、マネジメント職の回答者の優先順位に適合していると考えています。そのため 201 コース（ある程度の知識のある人向けのコース）としては、マネジメント以外の人にフォーカスすることにしました。

現在は、OpenSSF はセキュリティ アーキテクチャーにフォーカスすることを考えています。この分野は、全体の人気でトップ、ソフトウェア開発者やシステム運用者の重要度のランキングでもトップに選ばれた分野です。また、トップに選ばなかった多くの職種の回答でも高い順位に選ばれています。さらに、多くの人が「脅威の評価」も重要であると回答していることから、OpenSSF ではこの内容もセキュリティ アーキテクチャーのコースの内容に含めようと考えています。特定のトピックがすべての人にとって最重要となることはありませんが、トレードオフを考慮すると、このコースが最適な選択と考えています。

OpenSSF にセキュリティ アーキテクチャーのコースはいくつかありますが、それほど多くは提供できていません。現在、OpenSSF が提供している基礎コースでは、セキュリティ アーキテクチャーについて扱っていますが、他のコースと同様に、基本的な概念を簡単に解説する内容にとどまっています。そのため、既存の教材を発展させた、セキュリティ アーキテクチャーの応用コースを新設することができると考えています。

以上のように、OpenSSF では、セキュリティ アーキテクチャー コースの強化が、回答者のニーズに最も合致すると考えています。

第 5 章：
調査と回答者について

本調査は、Linux Foundation とそのパートナーが 2024 年 3 月 1 日から 4 月 19 日まで実施したウェブ アンケートに基づいています。有効回答数は 398 件で、そのうち完全回答は 318 件でした。さらに、アンケートの構成については表 2 に記載のとおり、一部の質問は回答者全員を対象としていません。そのため、本レポート中の図表のキャプションにあるように、それぞれの分析サンプル サイズは異なります。

以下では、回答者の属性と調査方法を示しています。調査の全質問文は、**http://www.data.world/thelinuxfoundation** で入手できます。

属性分布

図 20 は、回答者の所属組織の統計です。従業員数に基づく組織規模の観点で、回答者を小規模組織（1 ～ 249 名）、中規模組織（250 ～ 999 名）、大規模組織（20,000 名以上）に分類しました。各組織規模から同数の回答者が調査に参加しており、小規模が 31%、中規模が 35%、大規模が 33%でした。企業のタイプ別では、IT 製品やサービスを利用して他の分野で事業を展開する組織（47%）と、IT 製品やサービスを主な収益源とする組織（41%）のバランスが取れています。また、政府機関、非営利団体、財団法人、学術機関など、その他のタイプの組織（12%）も調査に含まれています。右のパネルでは、組織の主な業種を見ることができます。全体では、情報技術（IT ベンダー、サービス・プロバイダー、メーカー）が 48%、その他の業界が 52%を占めています。この調査の目的を考えると、情報技術の回答者が多いことは当然でしょう。また、小売、教育、公共事業、運輸、その他（合計 3%未満）をまとめて、「その他の業種」としており、22% を占めています。

表 2

調査の構成

ページ	質問	質問カテゴリー	質問の回答者
P1		はじめに	全回答者
P2-P3	問 1 ～問 6	あなた自身について教えてください	全回答者（N ＝ 398）
P4	問 7 ～問 8	オープンソースへの関わり方	オープンソース貢献者（N ＝ 270）
P5	問 9 ～問 13	あなたが勤務する組織について教えてください	雇用されているプロフェッショナルのみ（N ＝ 362）
P6	問 14 ～問 21	セキュアなソフトウェア開発に対する考え方	全回答者（N ＝ 398）
P7 ～ P9	問 22 ～問 30	セキュアなソフトウェア開発のための教育ニーズ	全回答者（N ＝ 322 ～ 352）
P9	問 31 ～問 32	教材を利用していない理由	受講していない回答者（N ＝ 135-150）
P10	問 33	LFR 委員と報酬に関する情報	全回答者

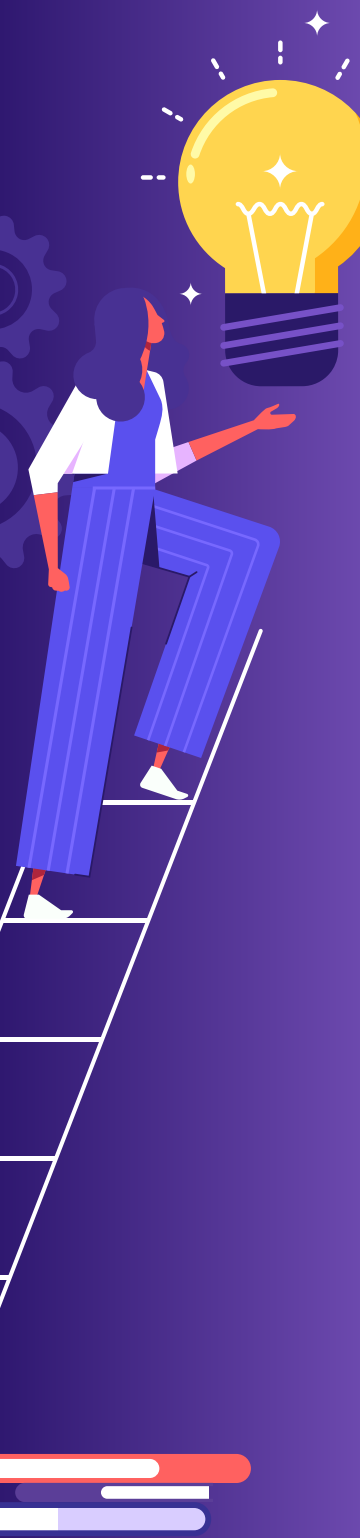
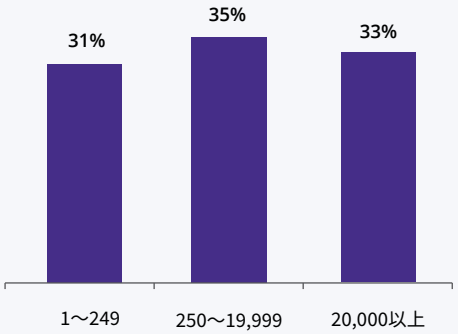


図 20

組織の分布

組織規模

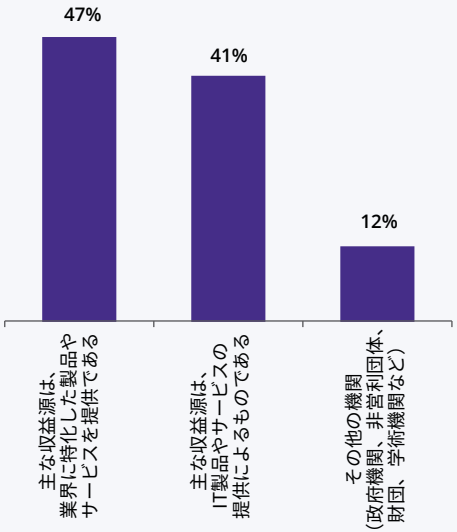
あなたの勤務先の従業員数をお答えください。



2024 年 SecEd 調査、問 12、サンプル数= 356、
DKNS を除く、その他の回答を再グループ化

会社の種類

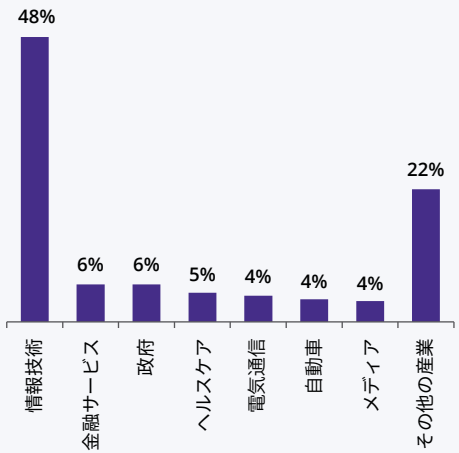
あなたはどのような企業や機関にお勤めですか？



2024 年 SecEd 調査、問 10、サンプルサイズ= 362

産業

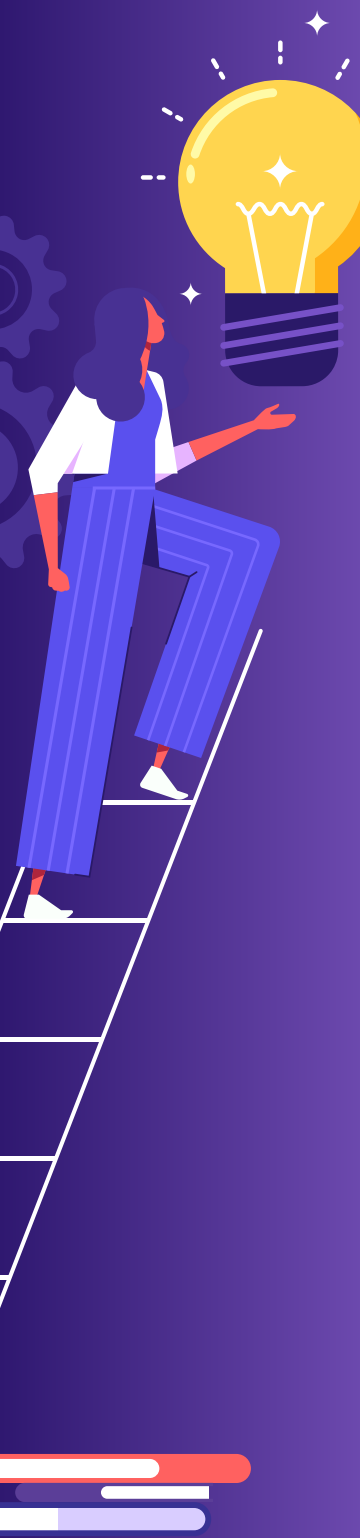
あなたの会社や機関の主要産業について、
最も適切なものは次のうちどれですか。



2024 年 SecEd 調査、問 11、サンプルサイズ= 362

図 21 は、回答者の属性を示しています。ソフトウェア開発者がサンプルの半数（50%）を占め、セキュリティ チーム（16%）、マネジメント（12%）、システム運用（9%）、その他と続きます。ほとんどの回答者はフルタイムで雇用されており（82%）、回答者の視点は個人（37%）、部門（28%）、会社（20%）、業界（16%）を代表した回答で、さまざまな視点が含まれています。ほとんどの参加者は OSS に一定程度関与しており、その貢献度は週 1 時間未満が 17%、それ以上が 51%でした。

最も多かった役割はオケージョナル コントリビューター（39%）、次いでメンテナー（28%）、開発以外のコントリビューター（14%）、コア コントリビューター（9%）、コミッター（8%）でした。地域別では、ヨーロッパ（41%）、米国とカナダ（36%）が多く、アジア太平洋地域が 13%、残りの 9%はその他の地域でした。調査データでは、各回答者の経験レベルは多様で、20%が 5 年未満、53%が 5 年〜20 年、残りの 27%が 20 年以上のソフトウェア開発経験者であることがわかりました。



しかし、セキュアなソフトウェア開発に関しては、経験年数は 2 年未満が 30%、3 年から 10 年が 48%、10 年以上が 22%となっています。最後に、知識の有無については、回答者の半数近く（47%）がセキュア ソフトウェア開発について「かなり知識がある」または「熟知している」と考えており、28%が「まったく理解していない」または「ある程度は知識がある」、25%が「知識がある」と回答しています。

調査方法と結果公開

調査データは、ソーシャルメディア、Linux Foundation、Linux.com の Web サイト、Linux Foundation のニュースレター、OpenSSF の支援によるオンライン調査によって収集されました。786 件の回答を得ましたが、388 件はスクリーニング基準を満たさないか、品質チェックを通過しなかったために破棄されています。参加者のスクリーニング基準には、ソフトウェア アプリケーションの開発に携わっていること、ボットを除外するように設計された質問で人間であることを確認できたこと、質問について回答できることなどが含まれています。品質チェックでは、回答された質問数と「知らない、またはよくわからない」（DKNS）の回答頻度に基づき、分析に必要十分なデータ数を確保できていることを確認しています。さらに、自由記述の回答、調査に費やした時間、提供された回答のパターンなどを、手作業で徹底的にチェックしてます。最終的に分析されたサンプル数は 398 件でした。調査データセットへのアクセスは、**http://www.data.world/thelinuxfoundation** で確認できます。

調査への参加は任意だったため、自己選択バイアスが生じた可能性があることは考慮が必要です。この種のバイアスは、参加者が調査に参加する際、関心のある結果が優位になるような選択をすることで、結果を歪めている可能性があります。

欠落データの扱い方

回答者はアンケートのほぼすべての質問に回答しなければなりませんでした（例外は一部の自由記述の質問のみ）。しかし、回答者の職務や経験の範囲外で質問に回答できない場合があるため、一部の質問の回答には選択肢として DKNS を選択できるようにしました。しかし、DKNS が選択されている場合、DKNS 回答をどう集計するかという問題が生じます。集計方法の 1 つは、他の回答と同様に DKNS を集計する方法を採用しています。この方法では、レポートの読者は、DKNS と回答した回答者の割合を見ることができます。また、収集したデータの正確な分布を確認できるというメリットがあります。この方法の問題点は、有効回答（回答者が質問に答えることができた回答）の分布を歪めてしまうことがあります。

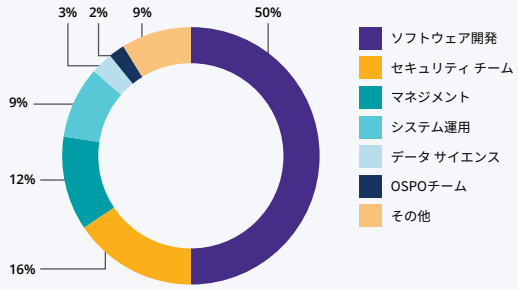
本調査結果の一部の分析では、DKNS を除外しています。これは、欠落データが無作為欠落または完全欠落に分類できるためです。ある質問から DKNS のデータを除外しても、他の回答のデータ（カウント）の分布は変わりませんが、残りの回答全体のパーセンテージを計算するために使用する分母のサイズが変わります。これは、DKNS の回答数に応じて、残りの回答のパーセント値を比例して増加させる効果があります。また、有効回答数も調整されます。DKNS のデータを除外した場合は、図の脚注をよく見れば、サンプル数（DKNS を含む）と有効回答数（DKNS を除外）の差から DKNS の回答数を確認することができます。最後に、本レポートにおけるパーセンテージの値は、四捨五入の関係で正確に 100%にならない場合があります。

図 21

回答者の属性分布

職務

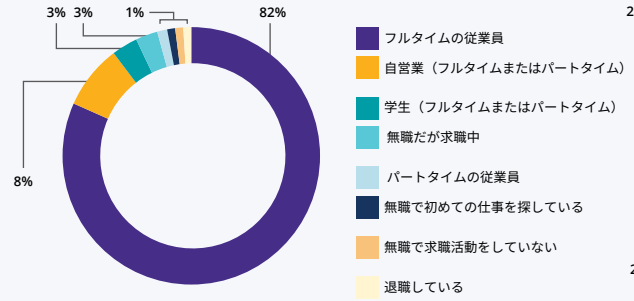
あなたの仕事上の立場に最も近い職務・領域は、以下のどれですか？



サンプル数＝398、カテゴリの名称は簡略化しており、
IT開発-ディレクターまたはバイスプレジデント、I
T運用-ディレクターまたはバイスプレジデント、プロダクト/プロジェクト管理、
Cレベルをマネジメントカテゴリに統合。その他はすべてその他

雇用形態

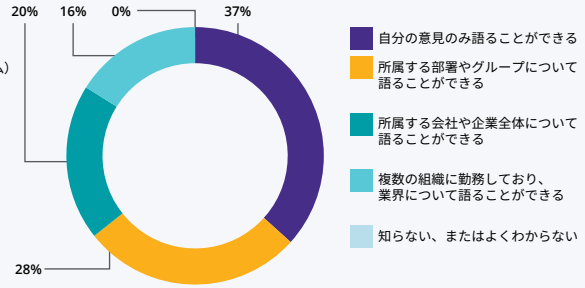
あなたの現在の雇用形態は次のうちどれですか？



2024年SecEd調査、問3、サンプルサイズ＝398

視点

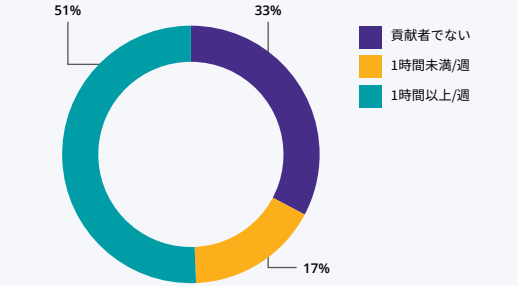
この調査で、あなたはどのような立場から意見を述べますか？



2024年SecEd調査、問4、サンプルサイズ＝398

OSSへの貢献

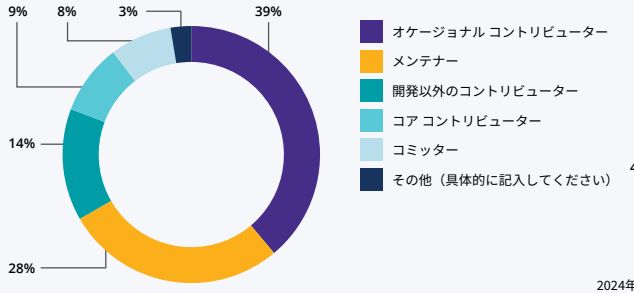
あなたは週に平均何時間、オープンソース プロジェクトに貢献していますか？



2024年SecEd調査、問6と問7より構成、サンプル数＝391、DNKSを除く

OSSでの役割

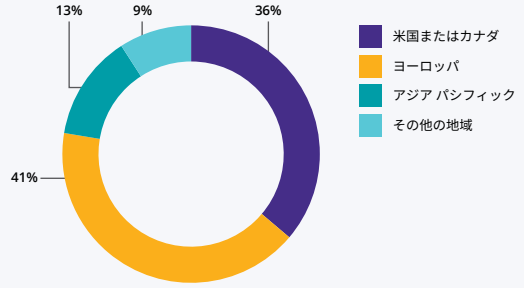
ご自身がかかわっているオープンソース プロジェクトで、
あなたはどのような役割にほとんどの時間を割いていますか？



2024年SecEd調査、問8、サンプル数＝270

地域

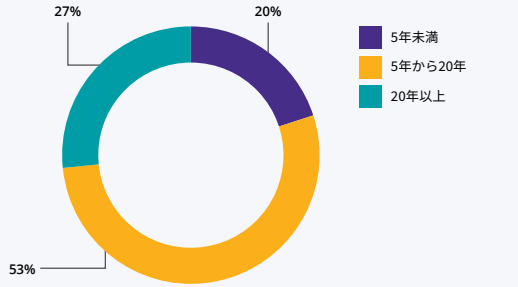
お住まいの国または地域はどこですか？



2024年SecEd調査、問9、サンプル数＝362、
アジア パシフィック＝中国、インド、日本、オセアニア、アジア太平洋地域
（中国、インド、日本、オセアニアを除く）。
その他の地域＝メキシコ、中米、カリブ海諸国、南米、中東、その他（具体的に記入してください）。

ソフトウェア開発経験

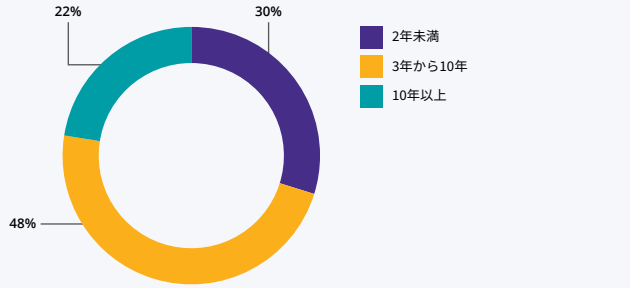
ソフトウェア開発の経験は何年ですか？



2024年SecEd調査、問15、サンプル数＝395、
DKNSを除外、より詳細な回答を再グループ化

セキュアなソフトウェア開発の経験

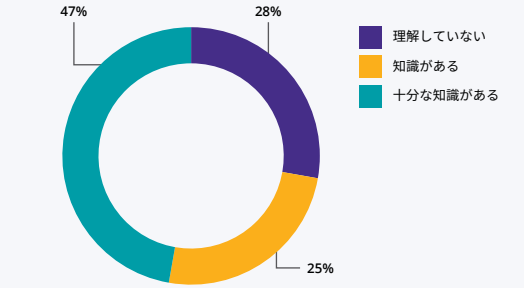
セキュア ソフトウェア開発の経験は具体的に何年ですか？



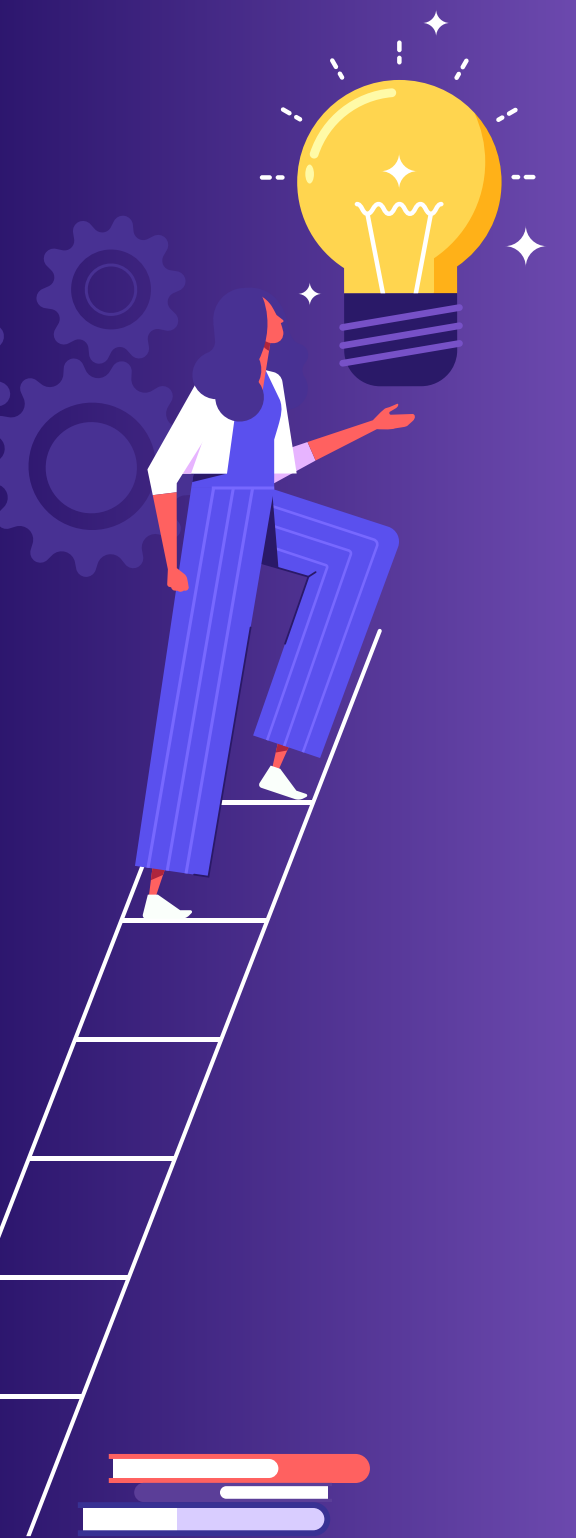
2024年SecEd調査、問16、サンプル数＝369、
DKNSを除外、より詳細な回答を再グループ化

セキュアなソフトウェア開発に関する知識

セキュア ソフトウェア開発についてどの程度ご存知ですか？



2024年SecEd調査、問14、サンプル数＝396、DKNSを除く。
理解していない＝まったく理解していない＋ある程度は知識がある
十分な知識がある＝かなり知識がある＋熟知している



結論

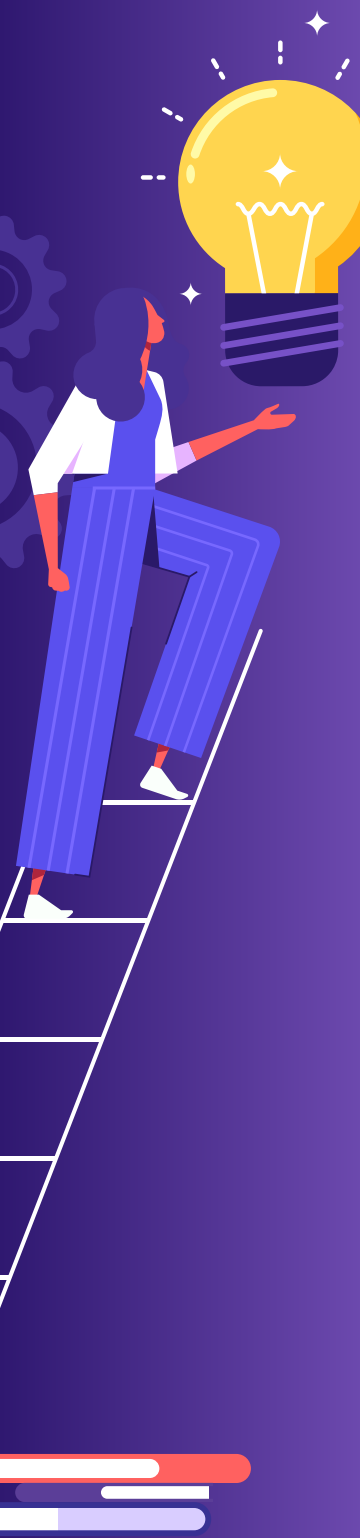
結論として、本調査により、セキュアなソフトウェア開発の知識とトレーニングの現状において、専門家の間に大きなギャップがあることが明らかになりました。豊富な経験を持つ開発者を含め、かなりの開発者はセキュアな開発手法の知識が不足しています。ほとんどの専門家は、現場での経験に頼っていますが、最低限の習熟度を達成するには何年もの経験が必要です。コースの新設により、このプロセスを加速させることで、回答者が指摘したように、セキュアなソフトウェア開発における主要課題に対処することができるようになるでしょう。

調査結果では、特にセキュリティ アーキテクチャー、セキュリティ教育とガイダンス、セキュアな実装などの分野で、プログラミング言語に依存しないコースの重要性が示されました。さらに、Python に特化したトレーニングに対して高い需要があることが明確になりました。これは Python が多くの分野で使用され、ソフトウェアのエコシステムにおいて重要な役割を担っていることを反映しています。しかし、トレーニングのニーズは専門性や経験値によって大きく異なるため、セキュアなソフトウェアの実践に関する多様な教育が必要であることがわかりました。

調査において、最も人気が高く、重要分野であることが明らかになった、セキュリティ アーキテクチャーに関するコースを OpenSSF は新設することにしました。これは業界のニーズに合致したものとなるでしょう。また、OpenSSF は、他の Linux Foundation のニュースレターや資料を活用し、OpenSSF の教材の情報を発信することで、現在の OpenSSF の教材の認知度を高める活動を行っていきます。

ソフトウェア開発教育において「セキュリティ バイ デザイン」の文化を醸成するために、すべての調査データを公開します。この分析結果をさらに研究し、ぜひ活用してください。セキュアなソフトウェア開発を効果的に活用するためのスキルと知識を開発者が確実に身につけることで、機密データは守られ、ユーザーの信頼を維持できる強靭なシステム構築につなげることができます。

.



付録 A：組織におけるサイバーセキュリティ

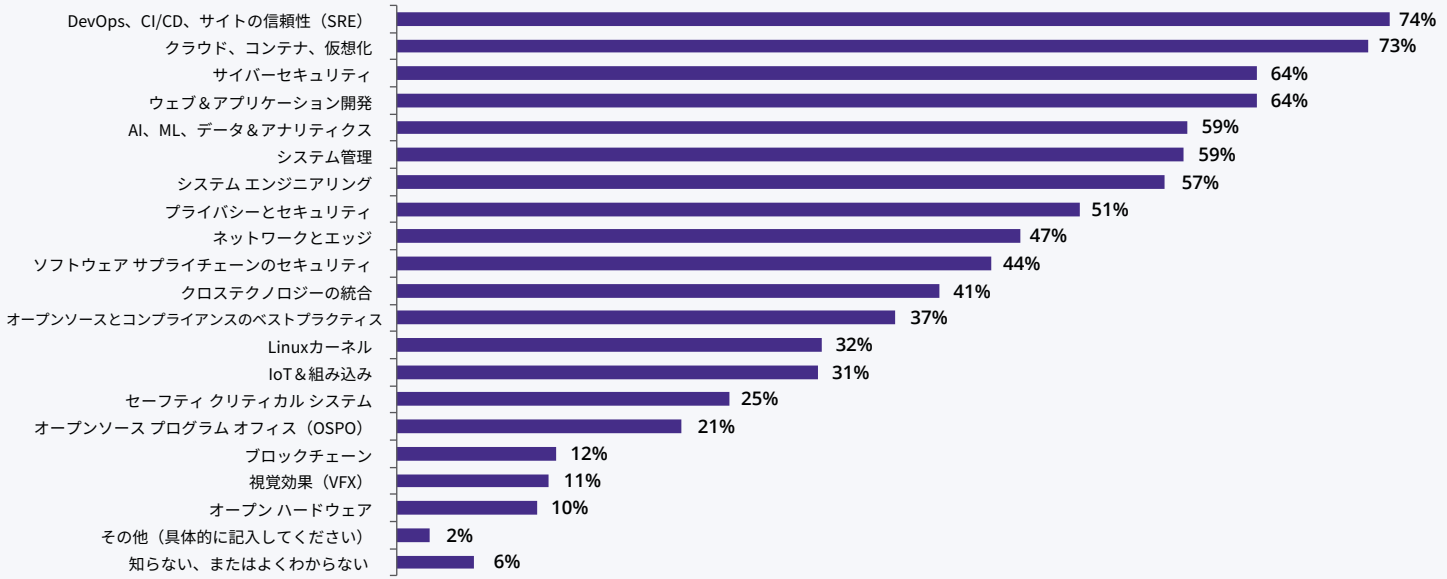
セキュアなソフトウェア開発におけるトレーニングのニーズと優先分野に関する分析、および、組織におけるサイバーセキュリティに関するトピックについて調査しました。この付録では、技術者数、組織が採用している活動、最新のセキュリティ脆弱性や脅威に対応するためのリソースについて説明します。

サイバーセキュリティは組織の優先事項

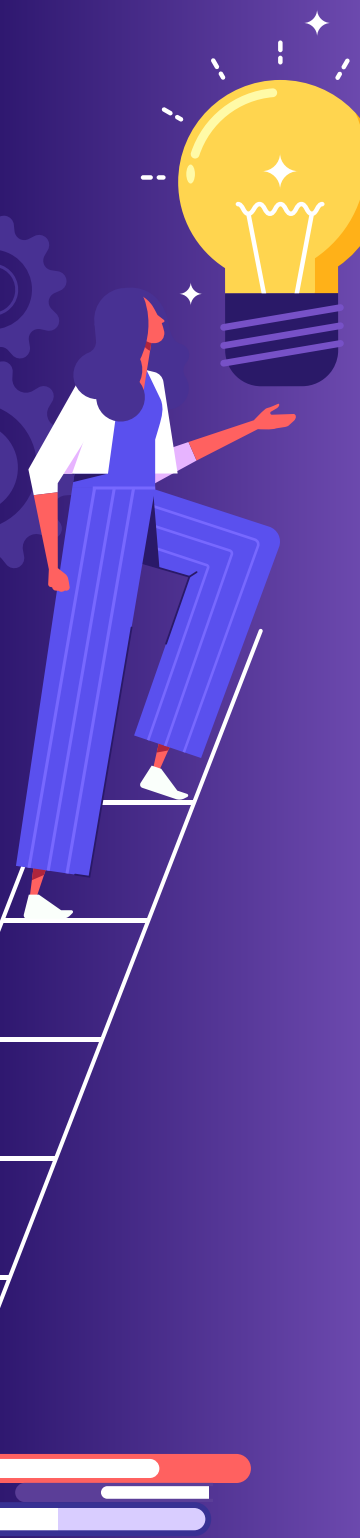
サイバーセキュリティは、ほとんどの組織にとって優先事項であり、図 22 に示すように、64%の組織がこの分野に技術者を配置しており、3 番目に多い分野となっています。図 23 によると、サイバーセキュリティは IT エンドユーザー企業でも重視されており、64% がこの分野に人員を配置しているのに対し、IT プロバイダー企業では 65% にとどまっています。小規模な組織であっても、サイバーセキュリティは重要で、従業員数が 250 人未満の組織の 51% が、この分野に専任のスタッフを配

図 22

回答組織における技術部門の人員数



2024 年 SecEd 調査、問 13、サンプル数＝ 362、総回答数＝ 2,978



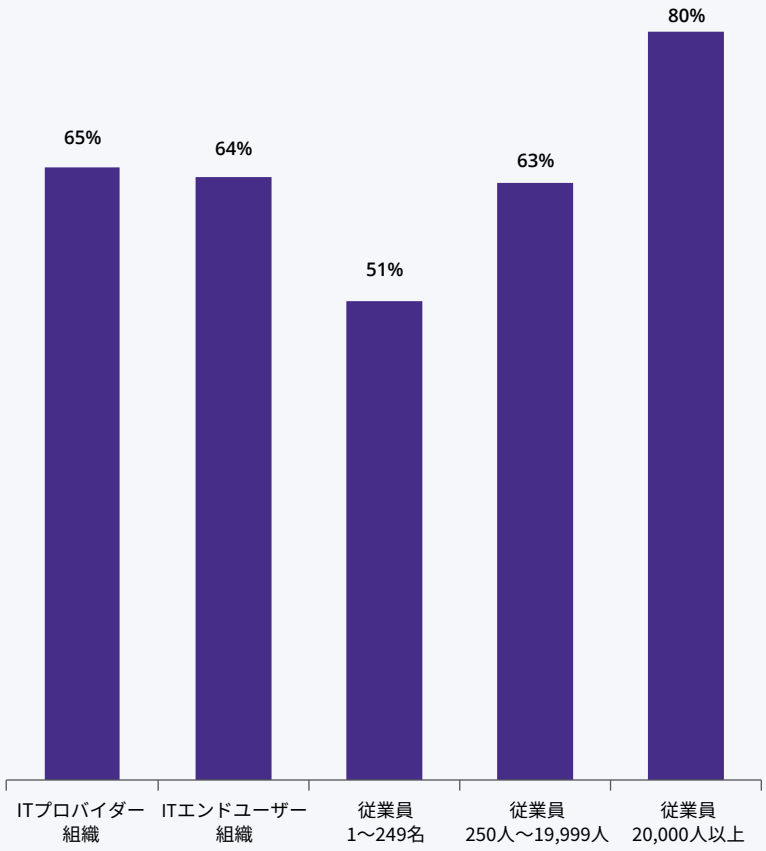
置しています。従業員数が 250 人～ 1 万 9,999 人の組織の 63%がサイバーセキュリティに人員を割いており、従業員数が 2 万人を超える組織では 80%にのぼります。

サイバーセキュリティ要員に対する高水準の投資は、日々進化するサイバー脅威からデジタル資産を保護することへの意識の高まりと緊急性を反映しています。今日、世界中のアタッカーがサイバー攻撃により組織を脅かす可能性があります。法規制やコンプライアンス基準にも後押しされ、サイバーセキュリティの専門家の必要性が増しており、場合によっては厳格なデータ保護プロトコルが義務付けられています。これらの基準を確実に遵守することは、機密情報を保護するだけでなく、組織の評価や信頼性にも影響を与えます。

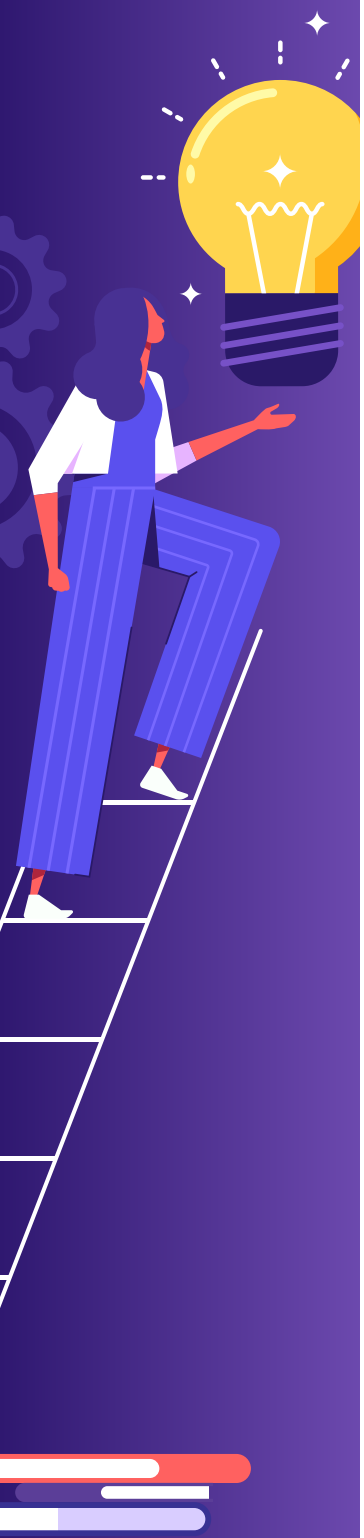
しかし、サイバーセキュリティの専門家を配置することは極めて重要ですが、それだけでは十分ではありません。サイバーセキュリティをソフトウェア開発プロセスに深く組み込む必要があります。セキュリティは、設計、実装、検証、デプロイなど、ソフトウェア開発全体を通して考慮される必要があります。セキュリティ プラクティスと思想を開発ライフサイクルに組み込むことで、組織は脆弱性をプロアクティブに特定して対処し、侵害のリスクを低減し、より柔軟性のあるソフトウェアを作成することができます。ソフトウェア開発ライフサイクル プロセスにセキュリティの観点をうまく組み込むには、ソフトウェアの専門家がセキュアなソフトウェア開発の技法と技術を熟知している必要があります。

図 23

サイバーセキュリティ分野の人員を配置している割合



2024 年 SecEd 調査、それぞれ問 13 と問 10、問 13 と問 12 より構成、サンプル数＝ 362



組織はさまざまなサイバーセキュリティ活動を採用している

図 24 は、組織のソフトウェア開発およびデプロイ プロセスに組み込まれているサイバーセキュリティ活動を示しています。組み合わせた利用を含めて考えると、CI または CI/CD が最も広く採用されているプラクティスであり、回答者の 75% がワークフローにこのプラクティスを組み込んでいます。このような高い採用率になっている理由は、セキュアなソフトウェア開発のためのツールやプラクティスを、安全なインフラの構築だけでなく、本番稼動前のコード チェックにも活用しているからでしょう。ロギング（68%）、機密情報管理（67%）、監視と警告（66%）も数多く採用されており、セキュリティ インシデントをリアルタイムに追跡・対処することも重視されているということが明らかになりました。

ほとんどの組織でユニット テストを実施しており（66%）、コードの完全性の確認を重視していることがわかります。また、ほとんどの組織がアイデンティティとアクセス管理を実施しており（65%）、ユーザー権限を管理したいという要望が広く浸透していることを示しています。それ以外に、コンフィギュレーション管理、セキュリティ パッチ、ソフトウェアの安全な設計と実装は、重要な活動であり、それぞれ回答者の 60%以上が挙げています。その一方で、ファズ テスト（26%）やサイバー脅威インテリジェンス（28%）のような活動はあまり実施されておらず、さらなる改善と投資の余地があることが示されています。

オンライン コースは組織にとって重要な学習教材

組織がデジタル資産を保護し、業務の質を保ち続けるためには、最新のセキュリティ脆弱性や脅威に対応することが重要です。システムを積極的に更新し、パッチを適用することで、多額の損失や信用の失墜につながる潜在的な侵害を防ぐことができます。

サイバー犯罪の被害額は、2023 年には 8 兆 1,500 億ドル（USD）に上ると推定されており、この数字は今後も増加すると予想されています。さらに、分野によっては、コンプライアンスのためにセキュリティ プラクティスを厳格に遵守することが義務付けられているケースもあり、継続的な警戒はオプションではなく、むしろ必須となっています。

サイバー犯罪の被害額は、2023 年には 8 兆 1,500 億ドル（USD）に上ると推計されており、この数字は今後も増加すると予想されています。[12] さらに、一部の分野では、コンプライアンスのため、セキュリティ プラクティスの厳格な遵守が義務付けられており、継続的な警戒はオプションではなく必須となっています。しかし、ほとんどの脆弱性は過去数十年と同じ種類のものであるというのが実態です。例えば、2023 年には、メジャーで重要なソフトウェアに対し攻撃が確認されたゼロデイ攻撃の 75%がメモリの安全性に関する脆弱性を狙ったものでした。[13,14] これはもともと 1970 年代に特定され、議論されていた問題です。一方、特定の製品では、新たな脆弱性が定期的に発生しており、多くは従来と同じ種類の脆弱性であるものの、早急な対処が必要です。さらに、2021 年の依存関係かく乱攻撃の発見のように、新しいタイプの脆弱性（または、脆弱性をより容易に悪用する方法）が発見されることもあり、その結果、脆弱性への最適な対策方法が変化することもあります。[15]

12 https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027

13 https://googleprojectzero.blogspot.com/2022/04/the-more-you-know-more-you-know-you.html

14 75% (42/56) of the 2023 entries in https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit

15 https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610

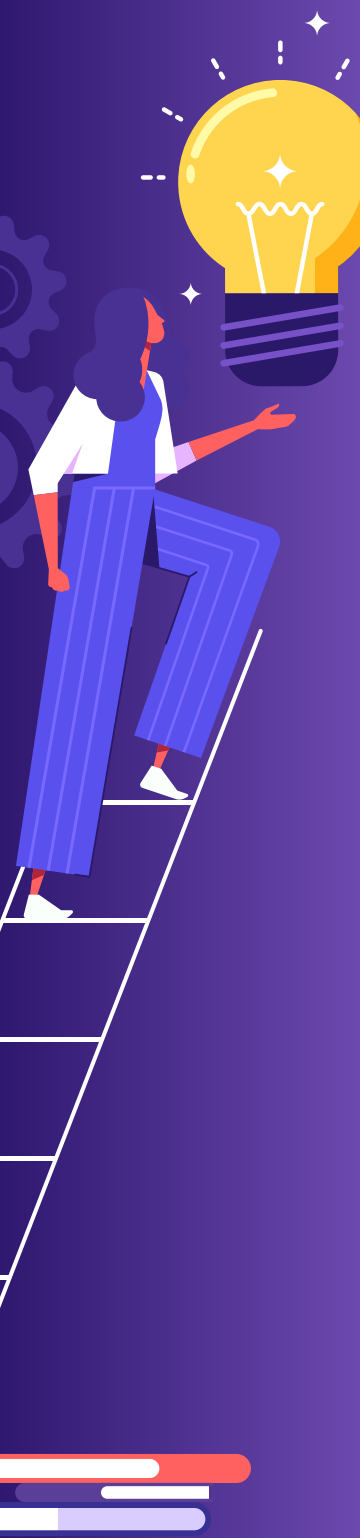
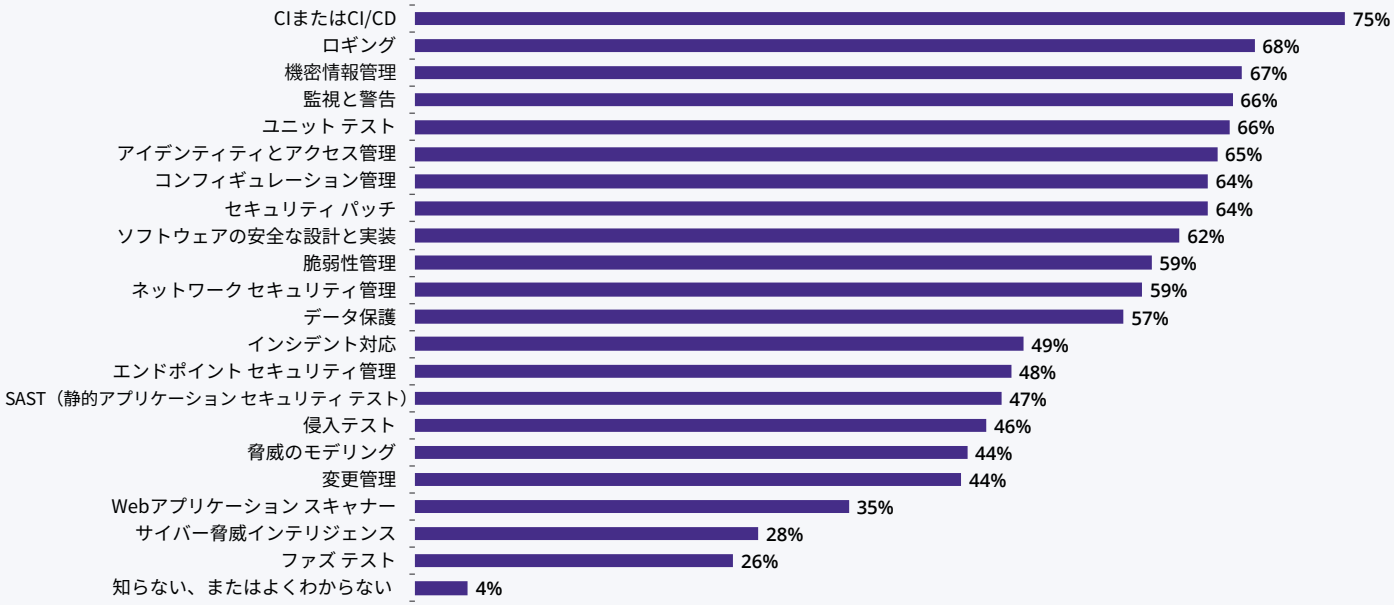


図 24

組織がソフトウェア開発・デプロイ プロセスの一環として採用している サイバーセキュリティ活動



2024 年 SecEd 調査、問 18、サンプル数= 398、総回答数= 4,538

したがって、組織は、常に情報を収集し、新たなセキュリティ課題に対応する必要があります。

セキュリティ関連の Web サイト、データベース、ブログ、メーリング リストが、最新情報の入手に多く利用されていることは意外に知られていない事実です。一方で、回答者の間では継続的な学習や資格取得への関心が非常に高いことがわかり、図 25 に示すように、40% の組織が、セキュリティ関連の最新動向の把握に活用しています。

従業員に継続的な教育と専門資格の取得を奨励することで、組織はサイバーセキュリティの知識とスキルを常に最新の状態に保つことができます。このような積極的なアプローチにより、担当者は組織のリスクを軽減し、新たな脆弱性に対し適切に特定して対応することができます。さらに、継続的な学習と資格取得により、組織のセキュリティ態勢を強化するだけでなく、セキュリティに対する意識や心構えを醸成することができます。このことは、日々変化する環境下でリスク対策を継続するために重要です。

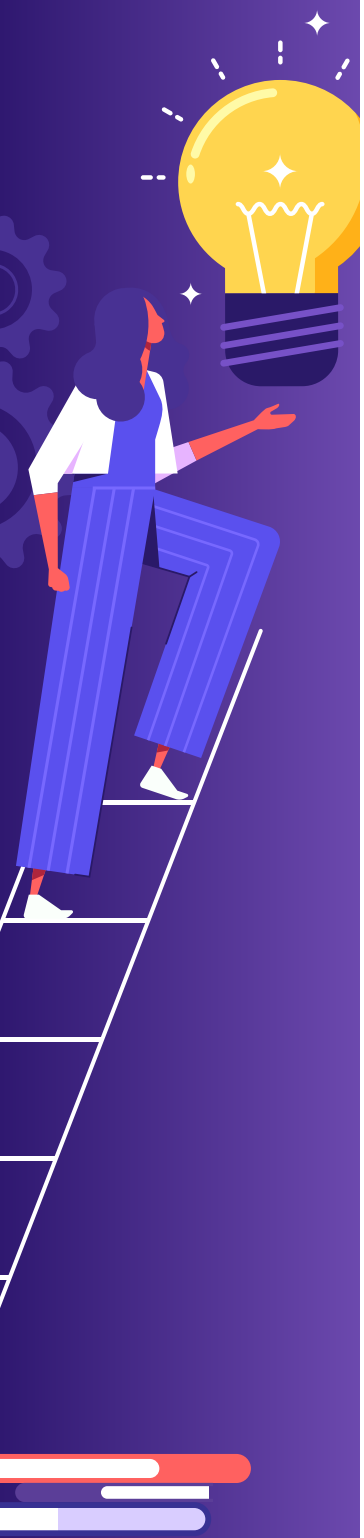
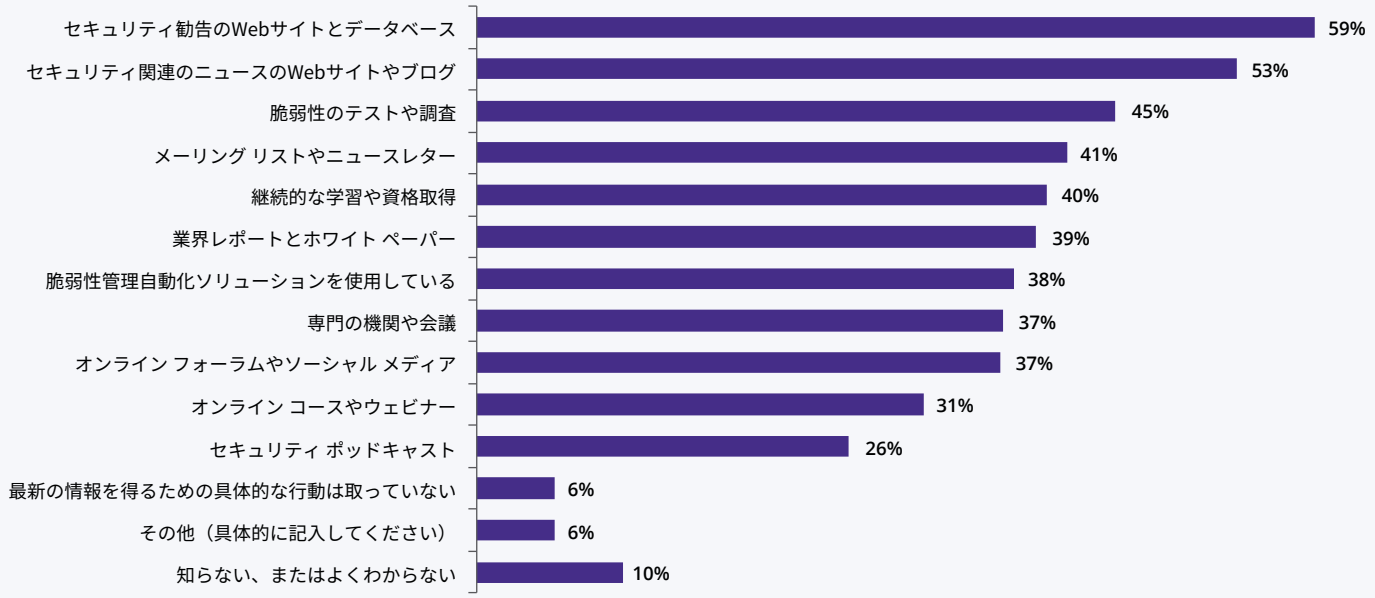


図 26 に見られるように、継続的な学習と資格取得に対しての考え方は、組織の部門によって異なります。OSPO チームが最も高い関心を示しており、回答者の 63%が重要と回答しています。僅差でセキュリティ チーム（56%）とマネジメント（55%）が続き、継続的な学習の価値を高く評価しています。しかし、その他の職務では、このトピックへの評価は低く、システム運用は 36%、ソフトウェア開発は 31%でした。図 26 は、大規模な組織ほど、この教育リソースを採用する傾向が高いことも明らかになっています。

具体的には、従業員 2 万人以上の組織の 57%が、継続的な学習と資格取得を重要な教育リソースとして利用していると回答しています。この数字は、従業員数が 250 人～19,999 人の組織では 40% に低下し、さらに従業員数が 1 人～249 人の小規模組織では 25% に低下します。この傾向は、組織の規模と、継続的な教育により最新のセキュリティ対策を維持する姿勢との間に相関関係があることを浮き彫りにしています。

図 25

使用している技術に関するセキュリティ脆弱性や脅威の最新情報を得るためのリソース



2024 年 SecEd 調査、問 19、サンプル数＝ 398、総回答数＝ 1,861

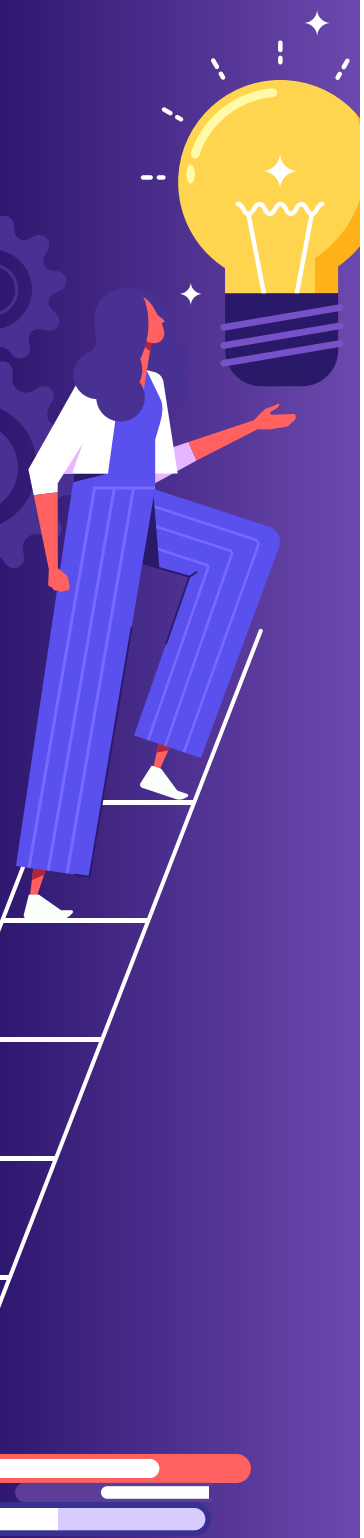
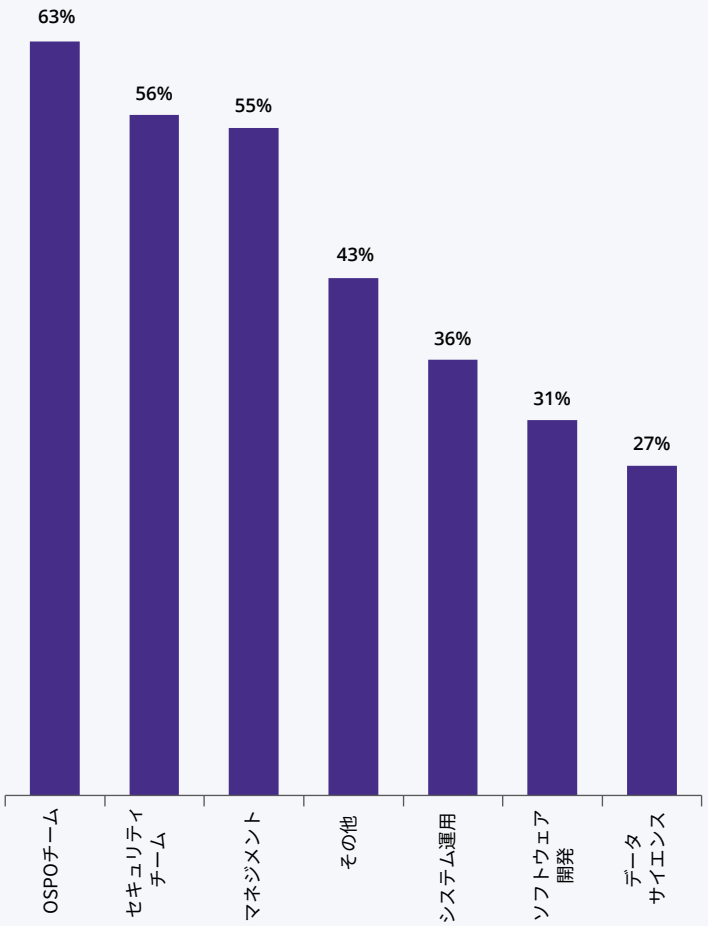


図 26

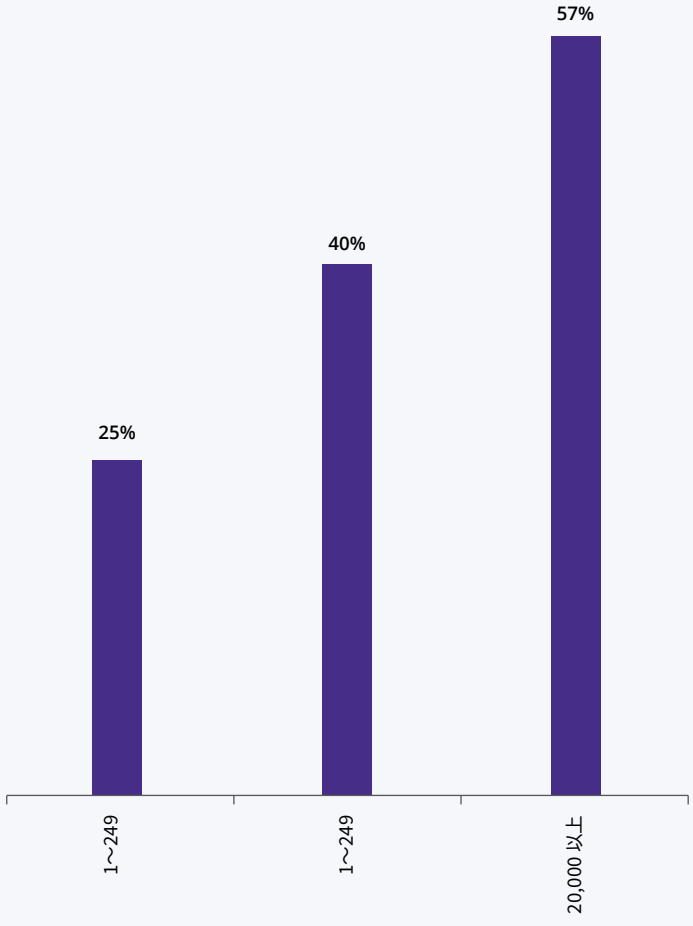
セキュリティの脆弱性や脅威に関する最新情報を得るためのリソースとして、継続的な学習や資格取得を挙げた回答者の割合

役割別にセグメント化



2024 年 SecEd 調査、Q19 と Q5 より構成、サンプル数＝ 398、「あなたの組織では、使用している技術に関連する最新のセキュリティ脆弱性や脅威の最新情報をどのように入手していますか」という質問に対して、「継続的な学習と資格取得」と回答した人の割合

組織内の従業員数でセグメント化



2024 年 SecEd 調査、Q19 と Q12 より構成、サンプル数＝ 356、「あなたの組織では、使用している技術に関連する最新のセキュリティ脆弱性や脅威の最新情報をどのように入手していますか」という質問に対して、「継続的な学習と資格取得」と回答した人の割合

付録 B：プログラミング言語に依存しないコースのカテゴリー別ランキング

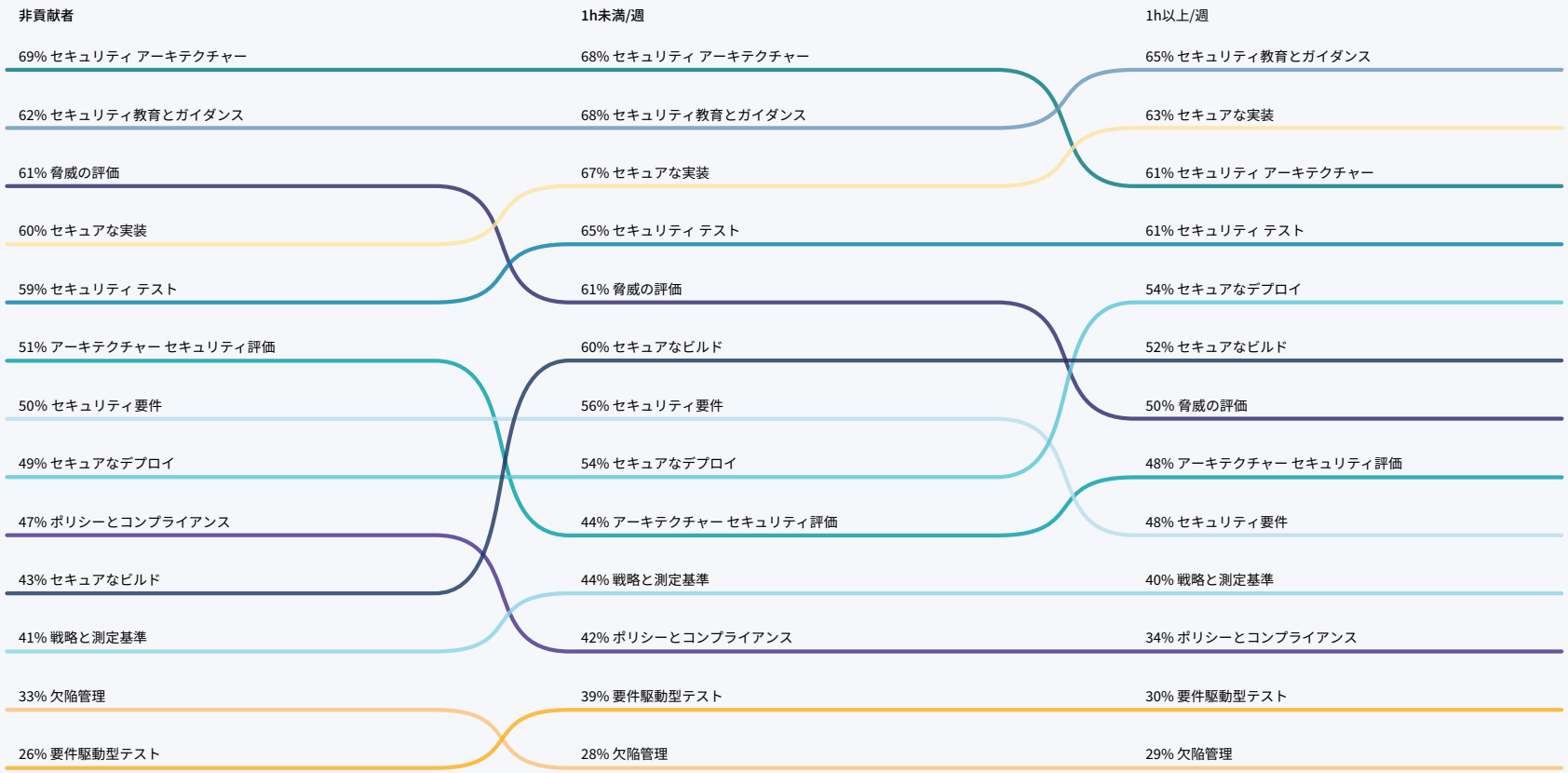
以下の図は、さまざまな基準によってセグメント化された、プログラミング言語に依存しないコースのランキングを示しています。

当然のことながら、コースの相対的な重要度は、さまざまな要因によって異なります。

図 27

プログラミング言語に依存しないコース（OSS への貢献度別）

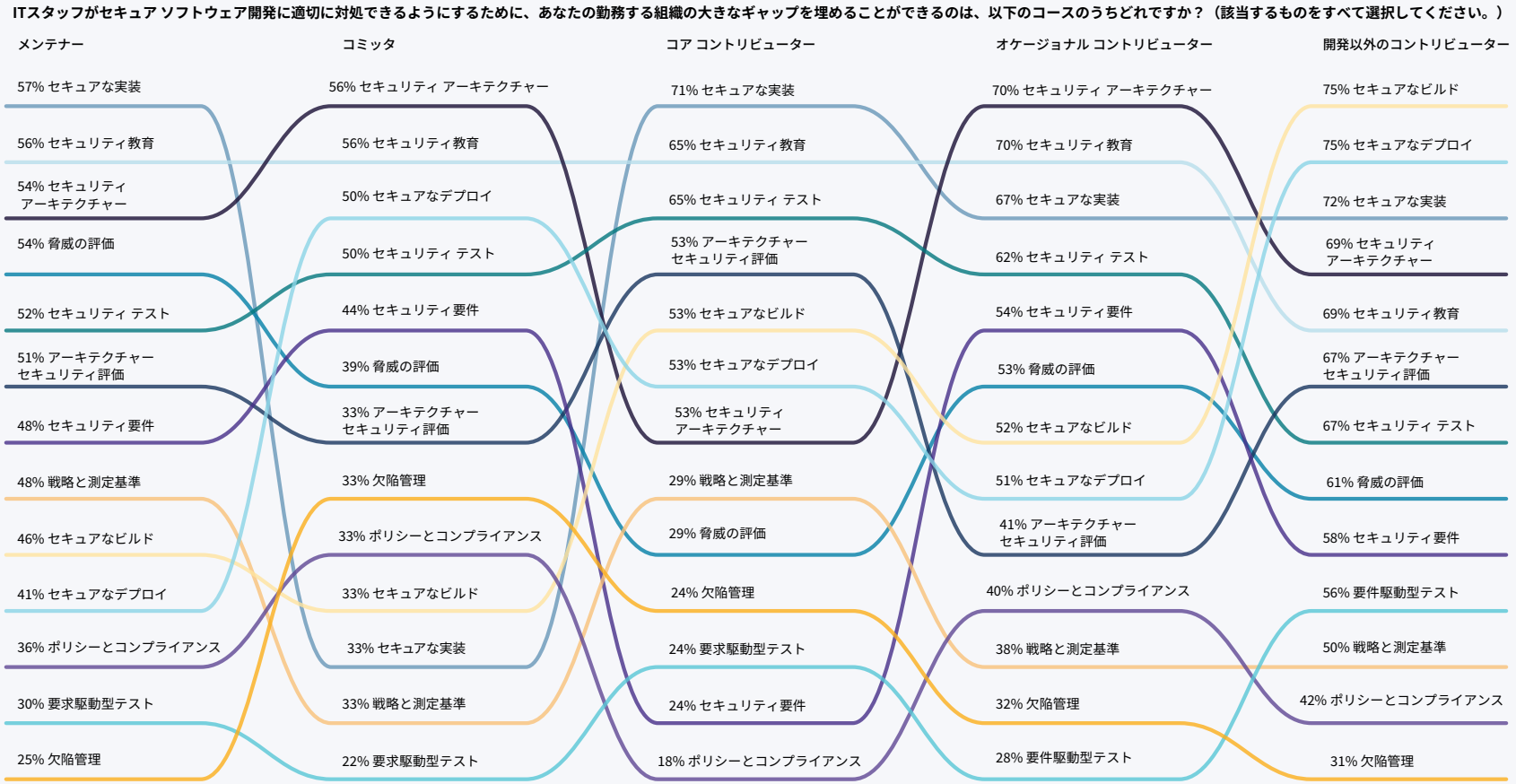
ITスタッフがセキュア ソフトウェア開発に適切に対処できるようにするために、あなたの勤務する組織の大きなギャップを埋めることができるのは、以下のコースのうちどれですか？（該当するものをすべて選択してください。）



2024 年 SecEd 調査、問 25 と問 7 で構成、サンプル数＝ 319、総回答数＝ 2,105、名前の前の数字は回答者の割合を表し、各列はこの数字でソートされています。

図 28

プログラミング言語に依存しないコース（OSS での役割別）

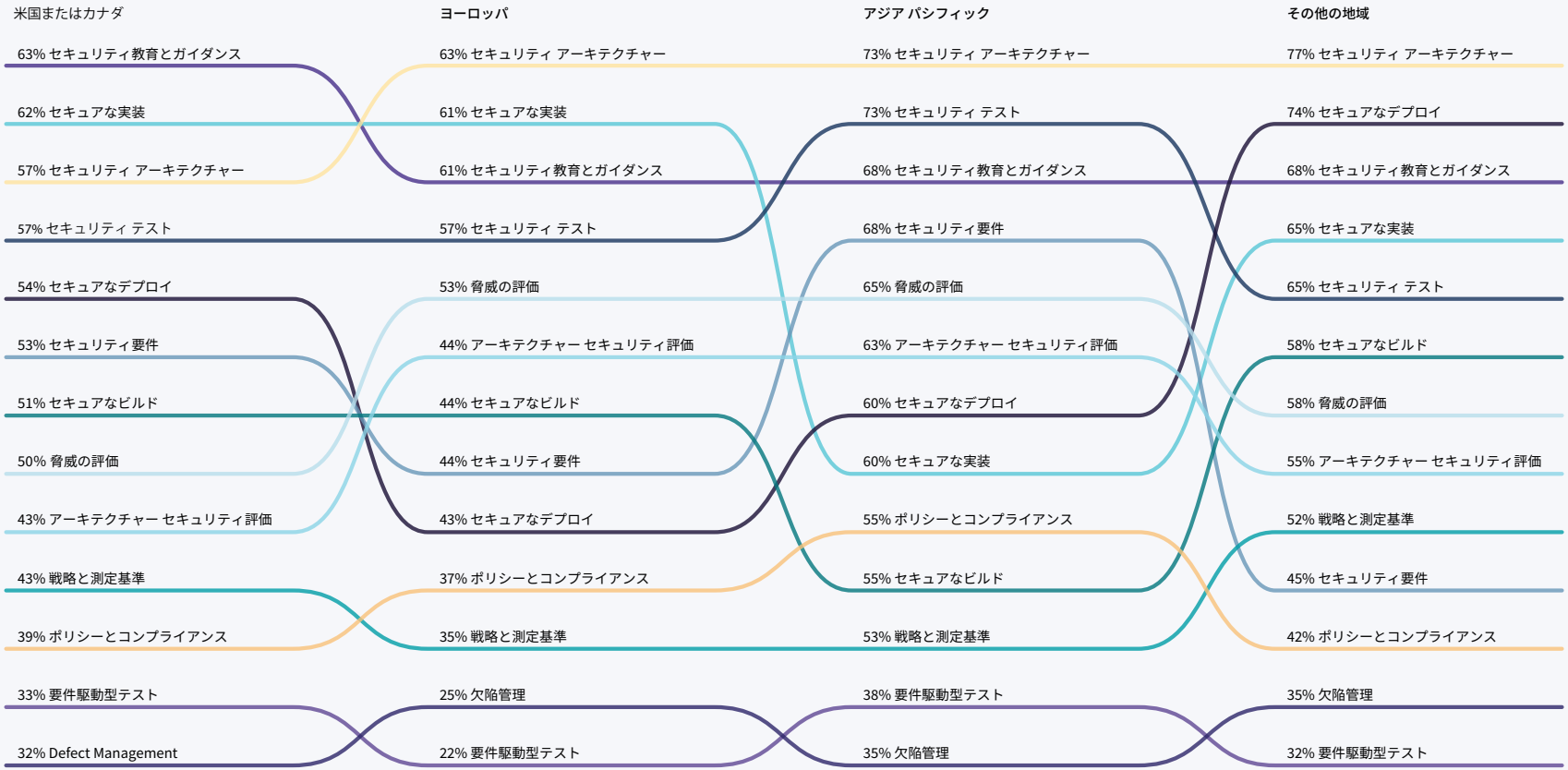


2024 年 SecEd 調査、問 25 と問 8 から構成、サンプル数＝ 231、総回答数＝ 1,512、名前の前の数字は回答者の割合を表し、各列はこの数字でソートされています。

図 29

プログラミング言語に依存しないコース（地域別）

ITスタッフがセキュア ソフトウェア開発に適切に対処できるようにするために、あなたの勤務する組織の大きなギャップを埋めることができるのは、以下のコースのうちどれですか？（該当するものをすべて選択してください。）

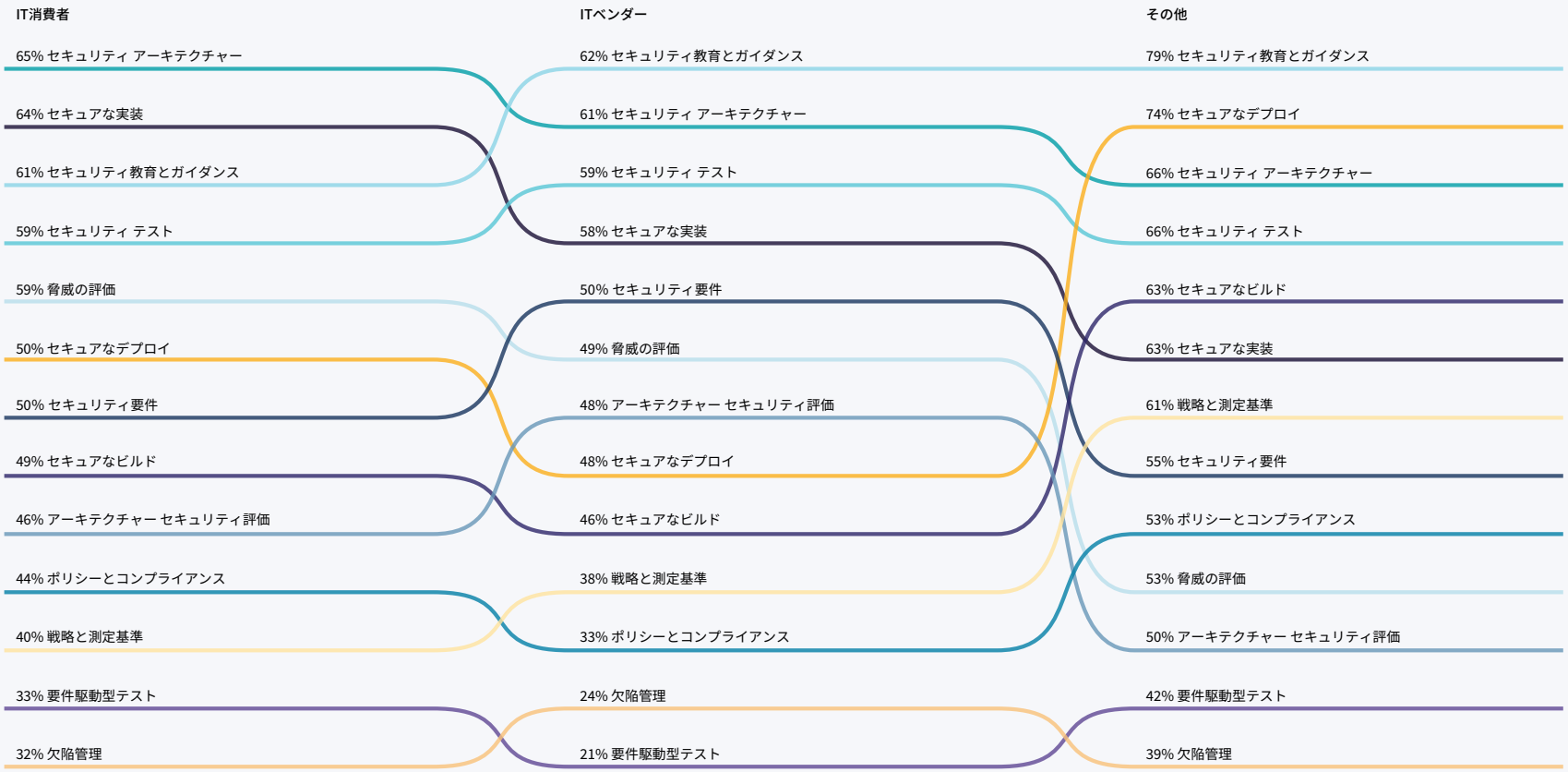


2024 年 SecEd 調査、問 25 と問 9 から構成、サンプル数＝ 312、総回答数＝ 2,028、名前の前の数字は回答者の割合を表し、各列はこの数字でソートされています。

図 30

プログラミング言語に依存しないコース（組織タイプ別）

ITスタッフがセキュア ソフトウェア開発に適切に対処できるようにするために、あなたの勤務する組織の大きなギャップを埋めることができるのは、以下のコースのうちどれですか？（該当するものをすべて選択してください。）

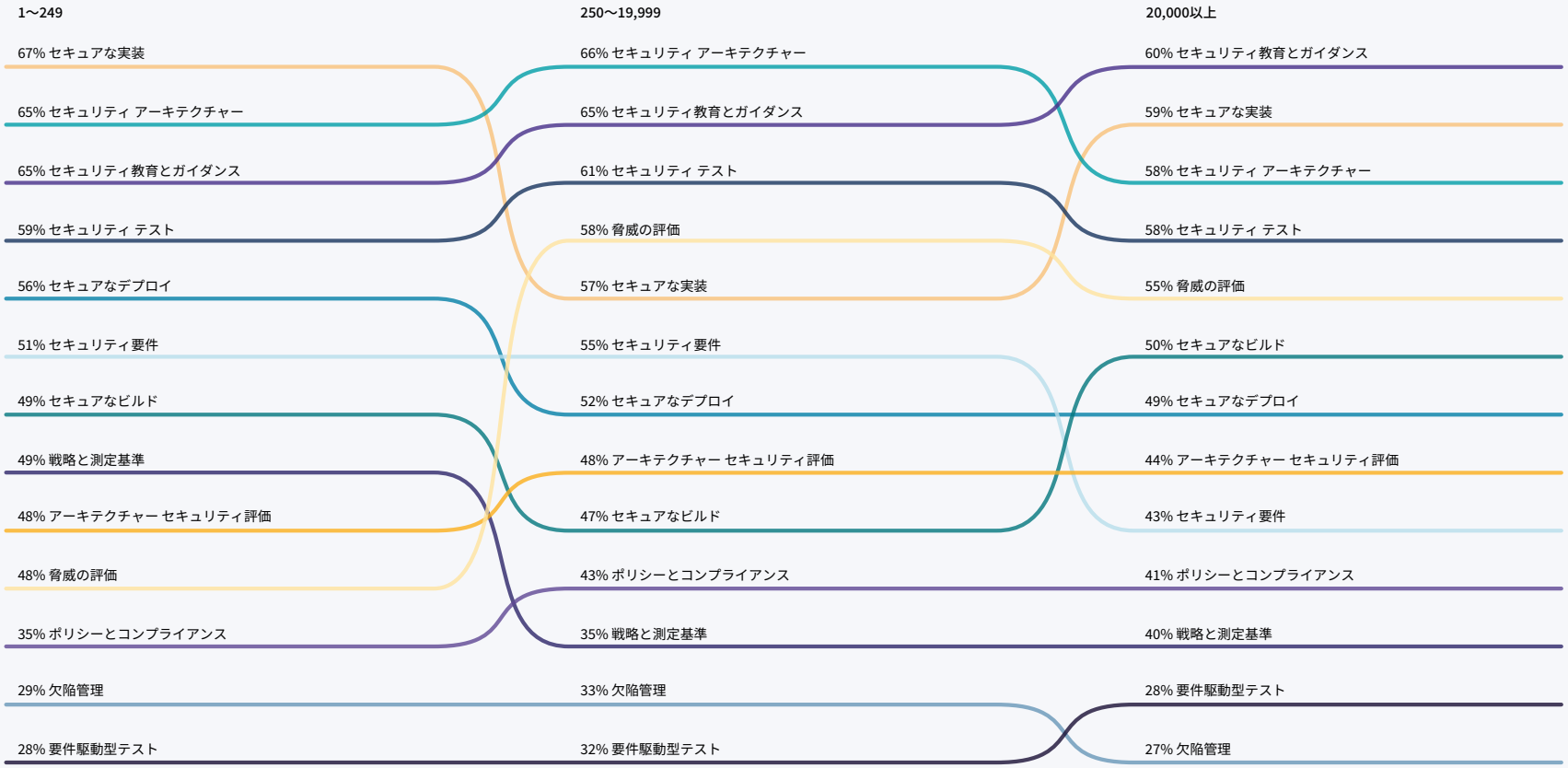


2024 年 SecEd 調査、問 25 と問 10 から構成、サンプル数＝ 312、総回答数＝ 2,028、名前の前の数字は回答者の割合を表し、各列はこの数字でソートされています。

図 31

プログラミング言語に依存しないコース（組織規模別）

ITスタッフがセキュア ソフトウェア開発に適切に対処できるようにするために、あなたの勤務する組織の大きなギャップを埋めることができるのは、以下のコースのうちどれですか？（該当するものをすべて選択してください。）

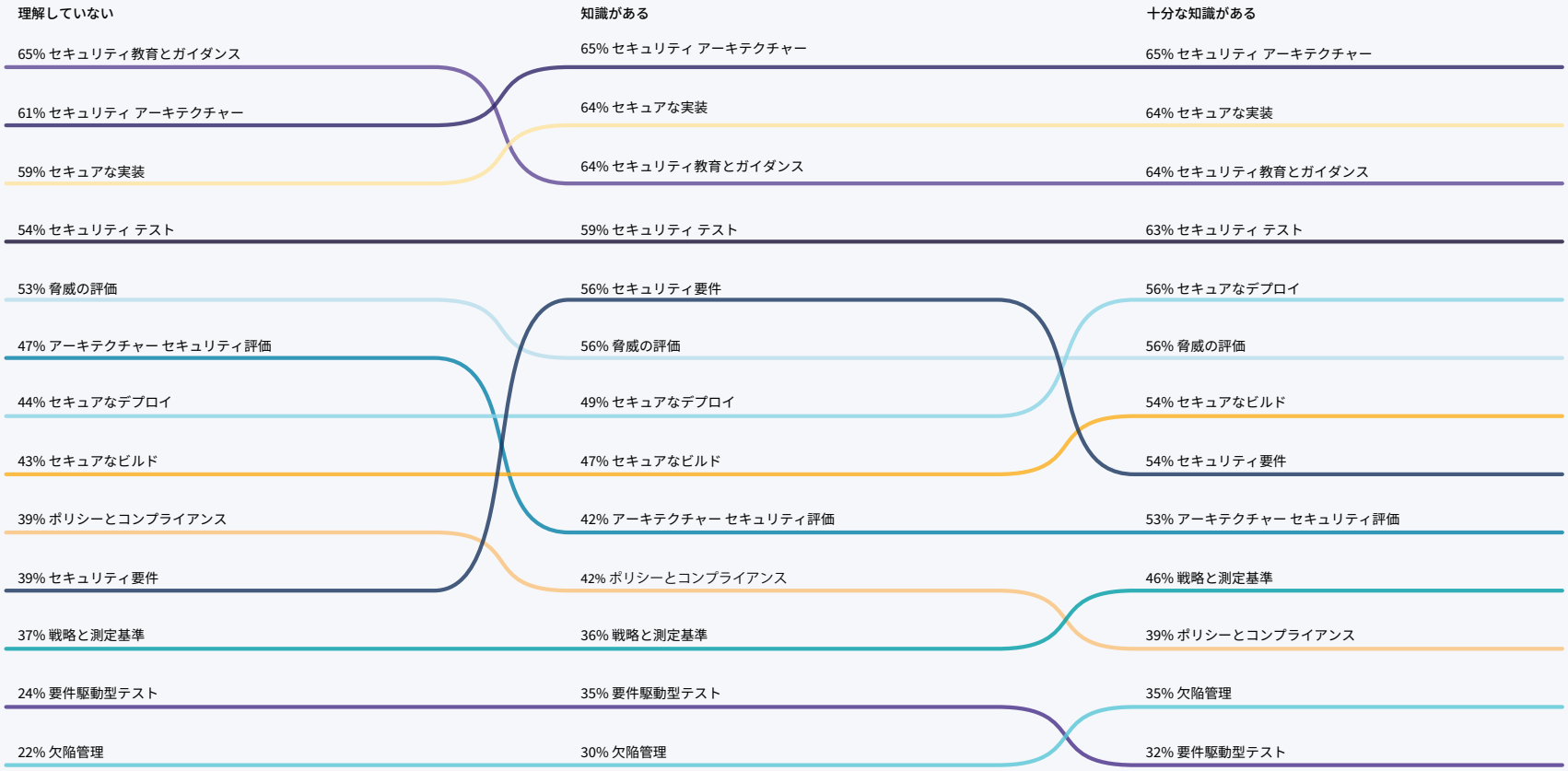


2024 年 SecEd 調査、問 25 と問 12 から構成、サンプル数＝ 307、総回答数＝ 1,983、名前の前の数字は回答者の割合を表し、各列はこの数字でソートされています。

図 32

プログラミング言語に依存しないコース（知識レベル別）

ITスタッフがセキュア ソフトウェア開発に適切に対処できるようにするために、あなたの勤務する組織の大きなギャップを埋めることができるのは、以下のコースのうちどれですか？（該当するものをすべて選択してください。）

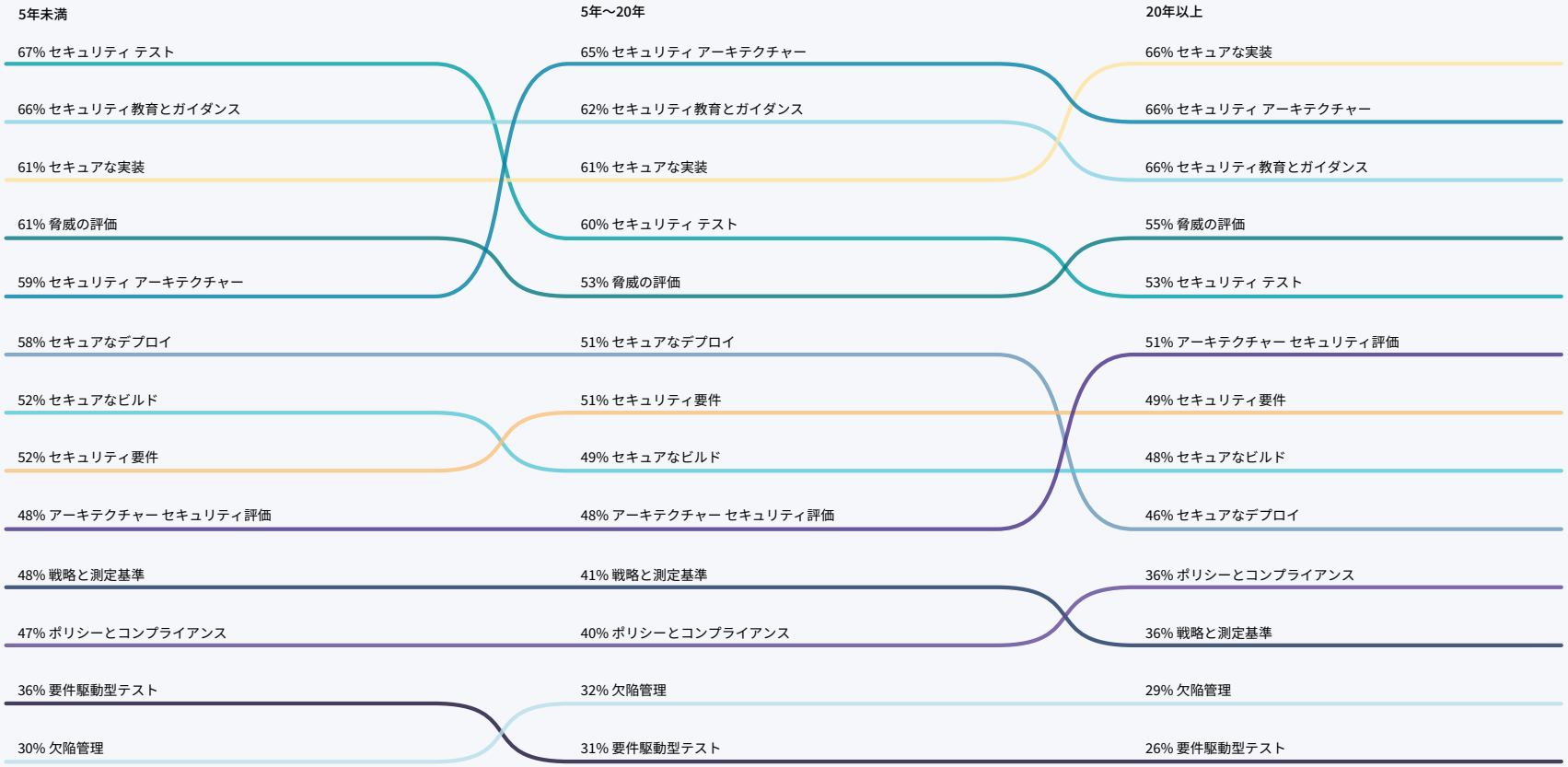


2024 年 SecEd 調査、問 25 と問 14 から構成、サンプル数＝ 340、総回答数＝ 2,223、名前の前の数字は回答者の割合を表し、各列はこの数字でソートされています。

図 33

プログラミング言語に依存しないコース（経験年数別）

ITスタッフがセキュア ソフトウェア開発に適切に対処できるようにするために、あなたの勤務する組織の大きなギャップを埋めることができるのは、以下のコースのうちどれですか？（該当するものをすべて選択してください。）



2024 年 SecEd 調査、問 25 と問 15 から構成、サンプル数＝ 340、総回答数＝ 2,227、名前の前の数字は回答者の割合を表し、各列はこの数字でソートされています。

付録 C：プログラミング言語別コースのカテゴリー別ランキング

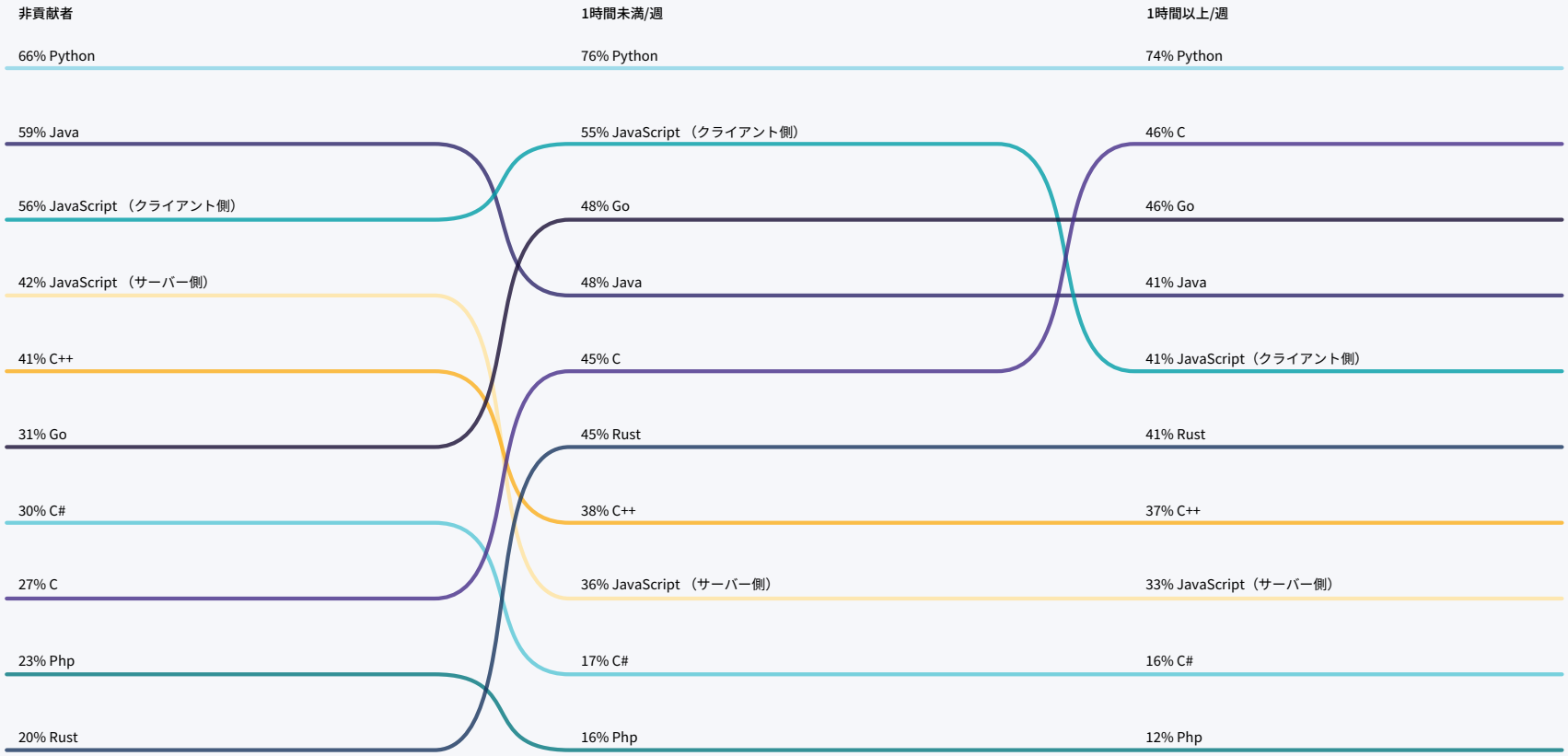
以下の図は、プログラミング言語別コースのランキングをさまざまな基準で分類したものです。

当然のことながら、プログラミング言語別コースの相対的な重要度は、さまざまな要因によって異なります。

図 34

プログラミング言語別コース（OSS への貢献度別）

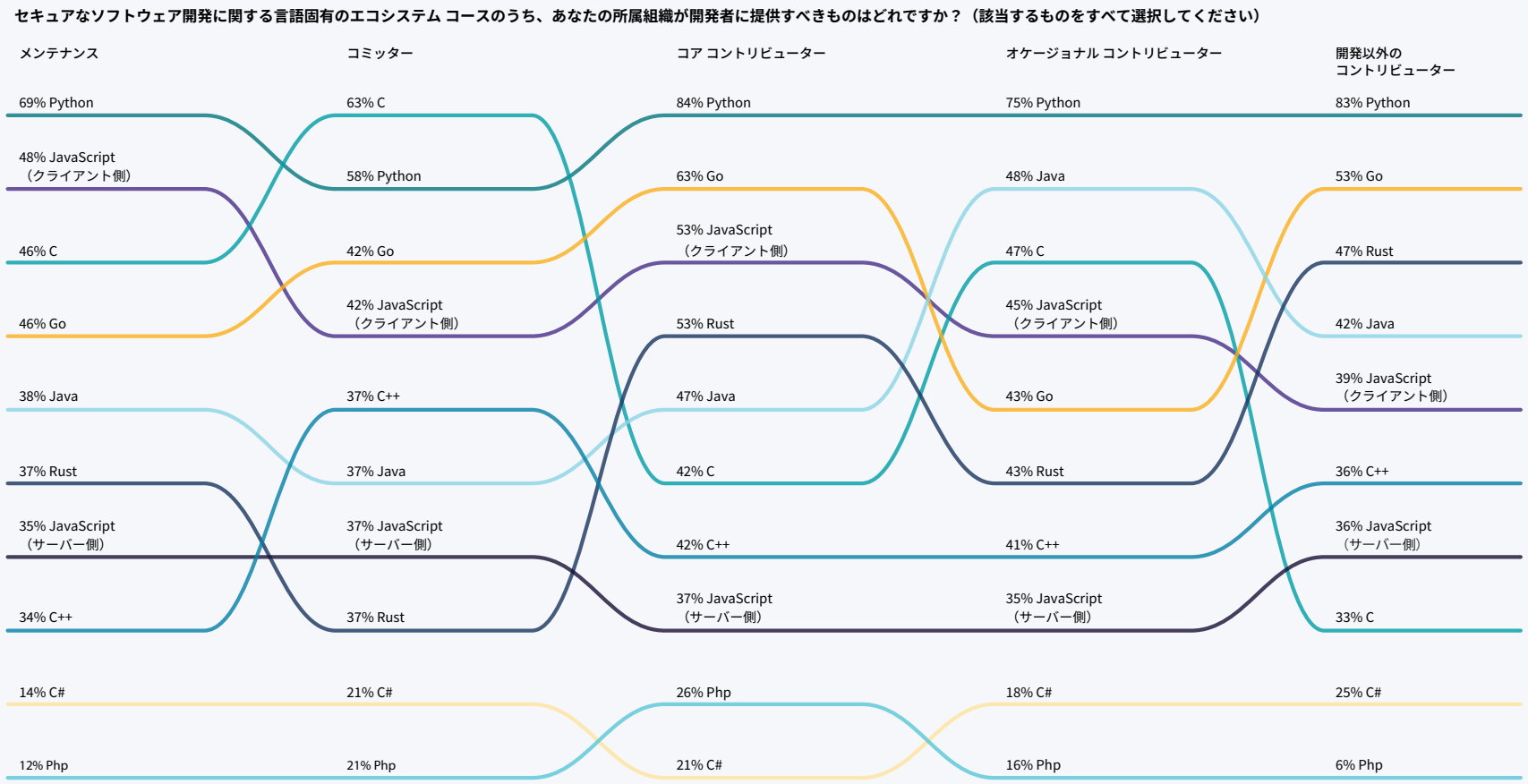
セキュアなソフトウェア開発に関する言語固有のエコシステム コースのうち、あなたの所属組織が開発者に提供すべきものはどれですか？（該当するものをすべて選択してください）



2024 年 SecEd 調査、Q23 と Q7 から構成、サンプル数＝ 329、総回答数＝ 1,342、名前の前の数字は回答者の割合を表し、各列はこの数字でソートされています。

図 35

プログラミング言語別コース（OSS での役割別）

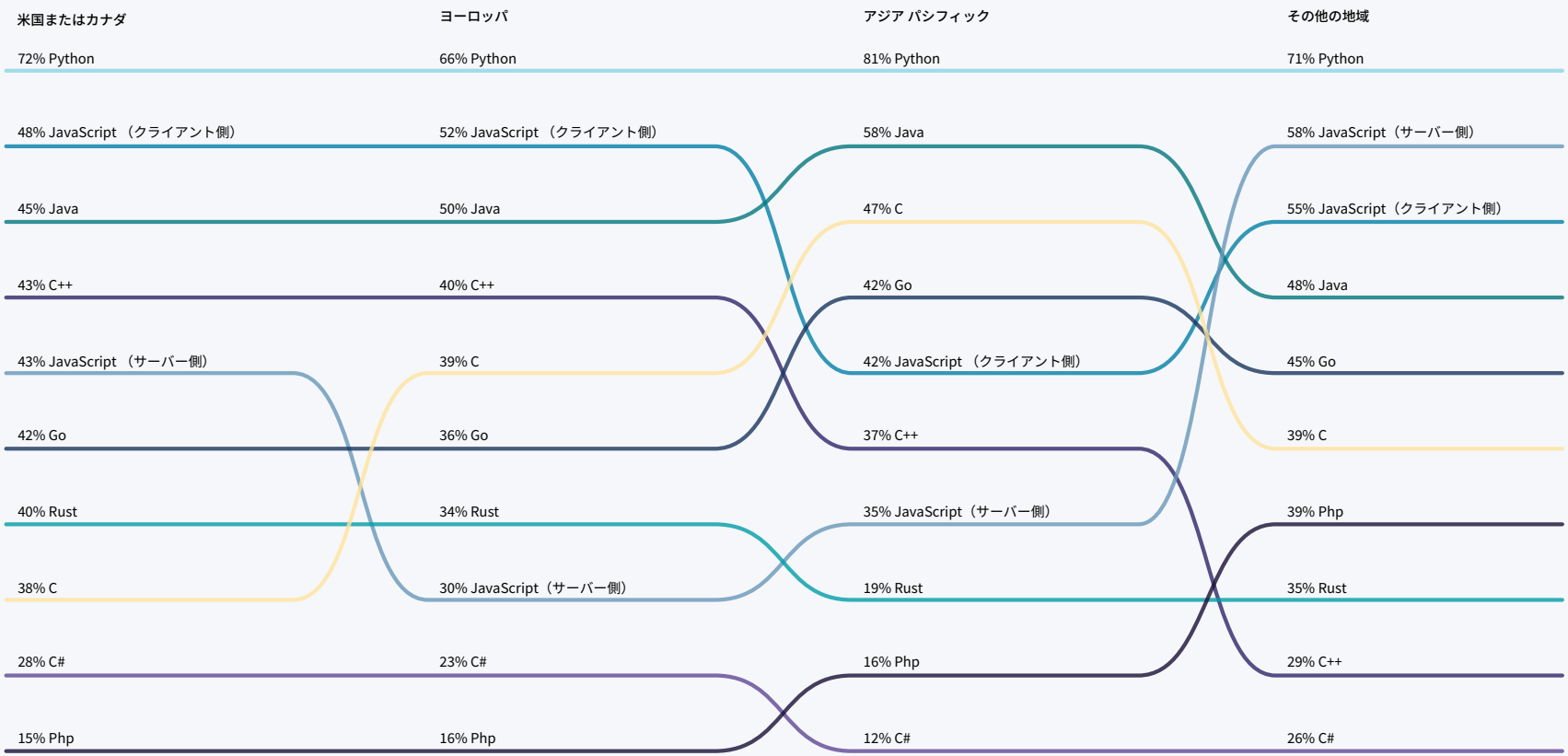


2024 年 SecEd 調査、問 8 と問 23 から構成、サンプル数＝ 239、総回答数＝ 991、名前の前の数字は回答者の割合を表し、各列はこの数字でソートされています。

図 36

プログラミング言語別コース（地域別）

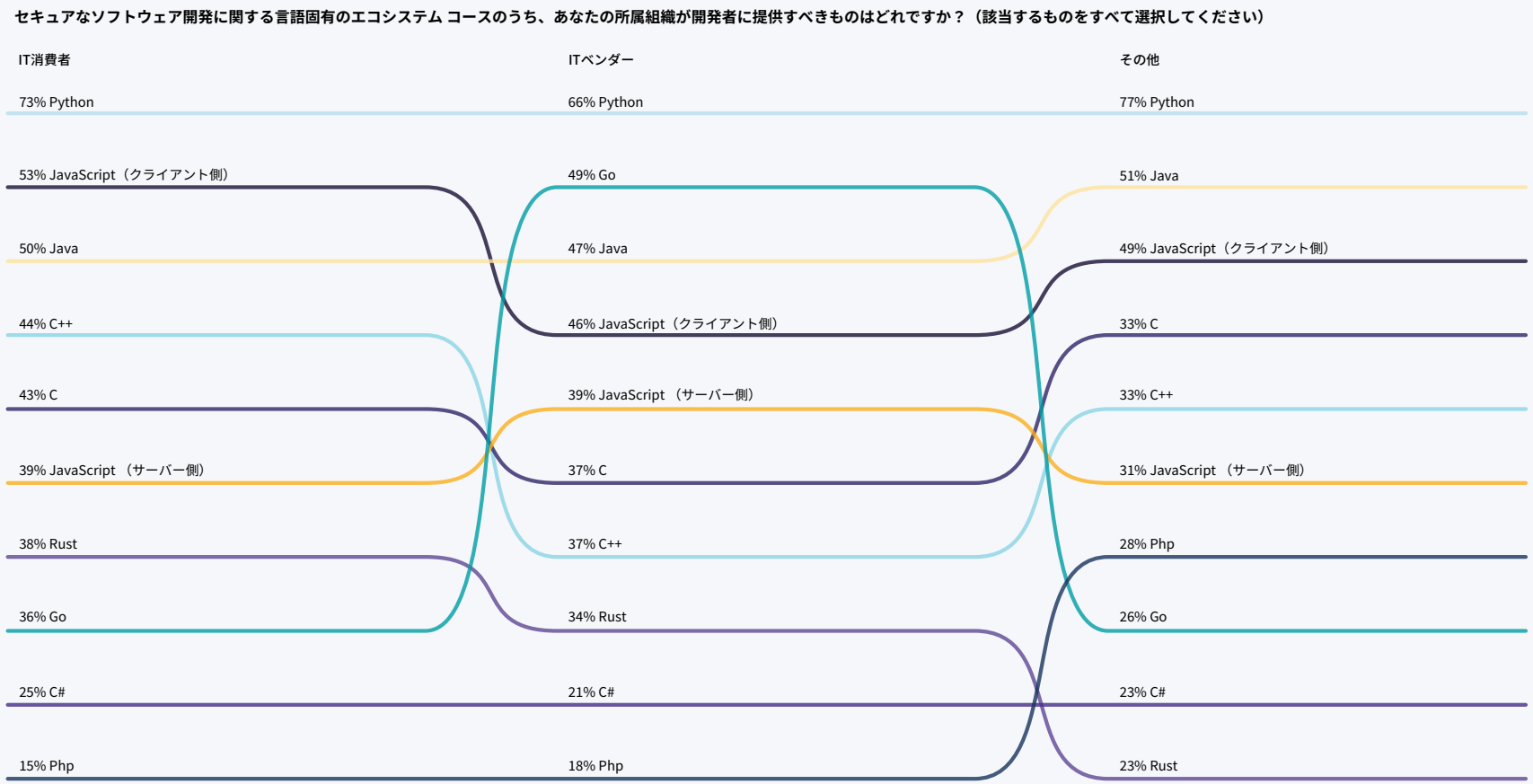
セキュアなソフトウェア開発に関する言語固有のエコシステム コースのうち、あなたの所属組織が開発者に提供すべきものはどれですか？（該当するものをすべて選択してください）



2024 年 SecEd 調査、問 23 と問 9 から構成、サンプル数＝ 321、総回答数＝ 1,330、名前の前の数字は回答者の割合を表し、各列はこの数字でソートされています。

図 37

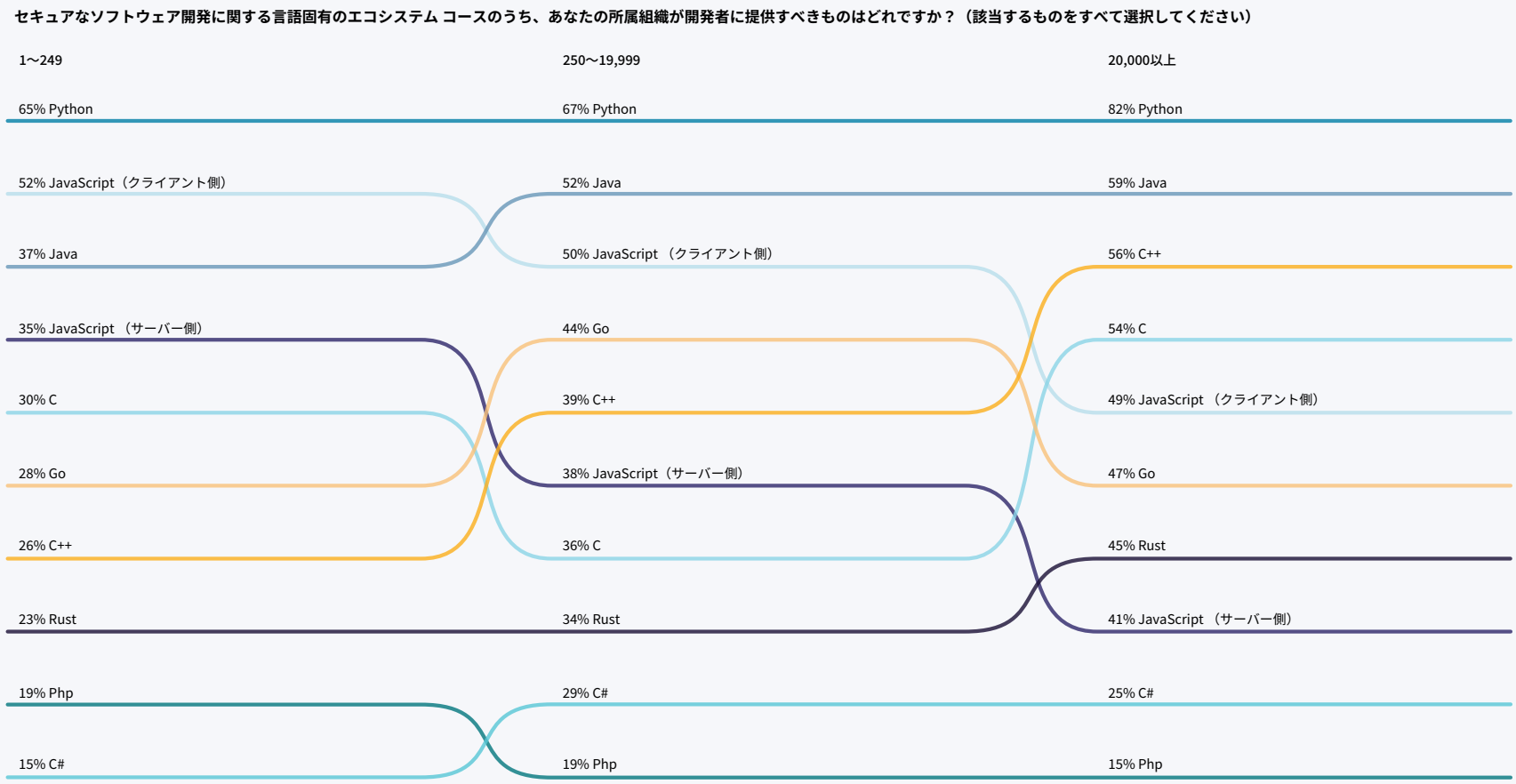
プログラミング言語別コース（組織タイプ別）



2024 年 SecEd 調査、問 23 と問 10 から構成、サンプル数＝ 321、総回答数＝ 1,330、名前の前の数字は回答者の割合を表し、各列はこの数字でソートされています。

図 38

プログラミング言語別コース（組織規模別）

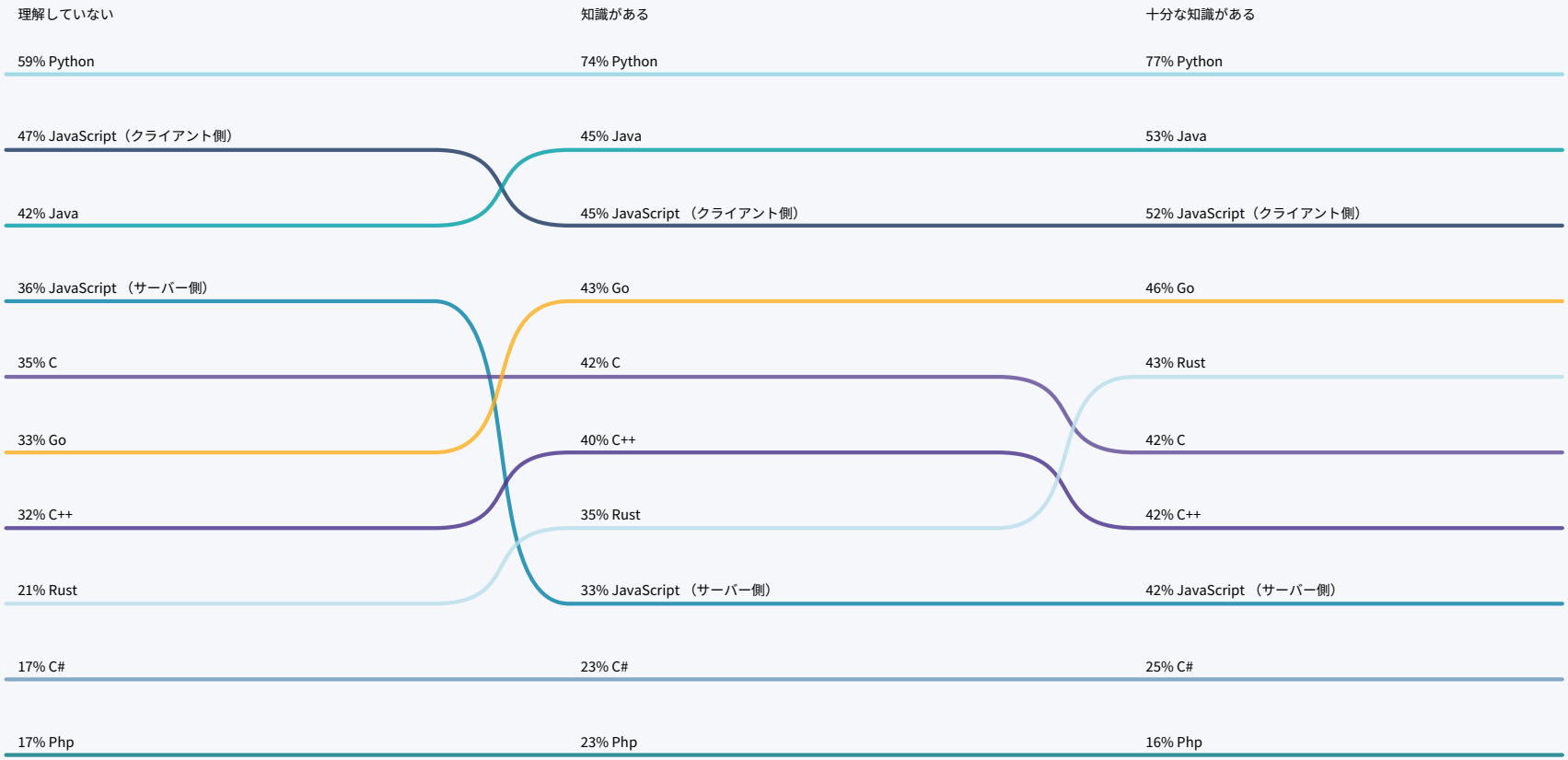


2024 年 SecEd 調査、問 23 と問 12 から構成、サンプル数＝ 315、総回答数＝ 1,315、名前の前の数字は回答者の割合を表し、各列はこの数字でソートされています。

図 39

プログラミング言語別コース（知識レベル別）

セキュアなソフトウェア開発に関する言語固有のエコシステム コースのうち、あなたの所属組織が開発者に提供すべきものはどれですか？（該当するものをすべて選択してください）

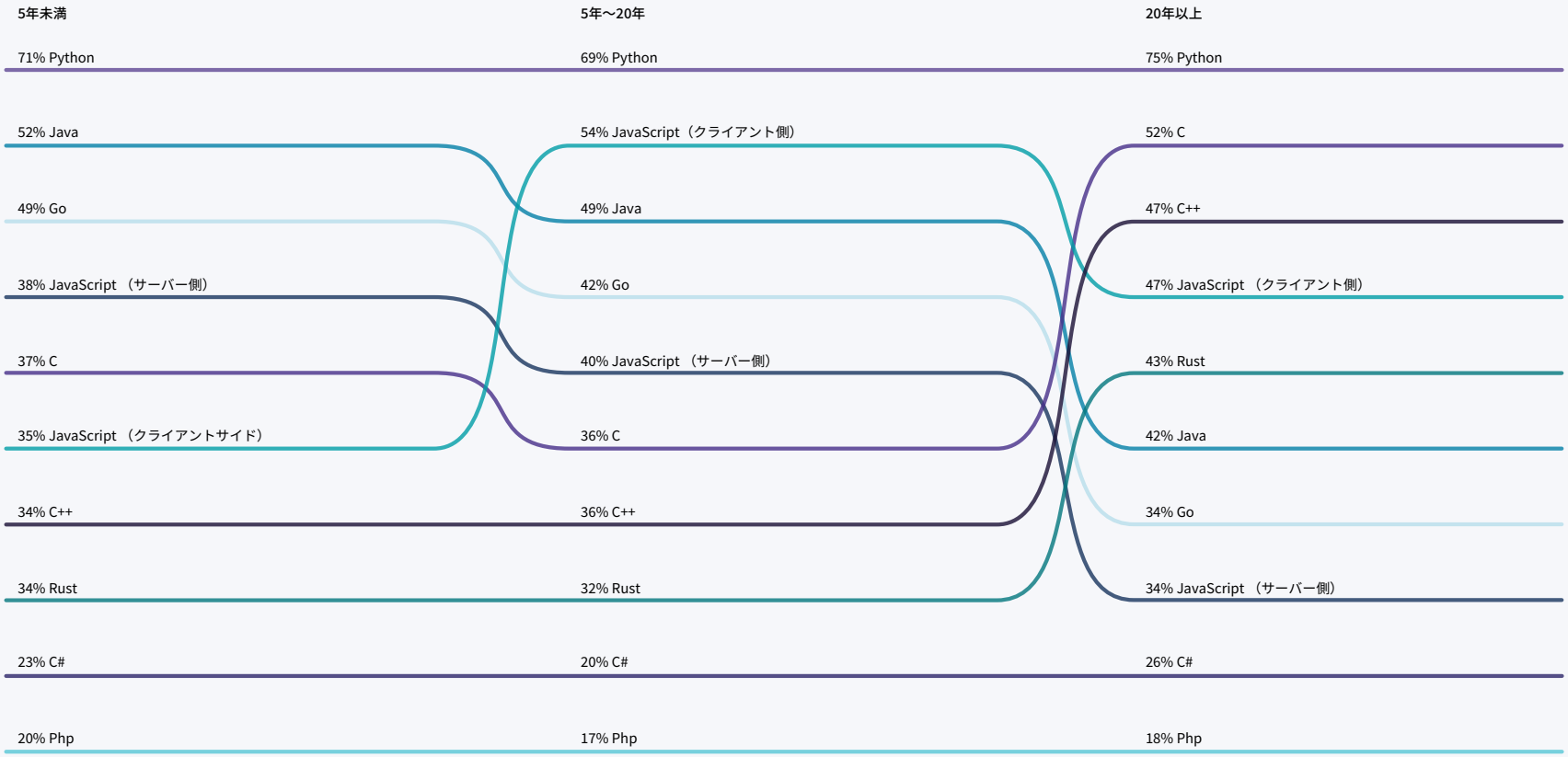


2024 年 SecEd 調査、問 23 と問 Q14 から構成、サンプル数＝ 350、総回答数＝ 1,448、名前の前の数字は回答者の割合を表し、各列はこの数字でソートされています。

図 40

プログラミング言語別コース（経験年数別）

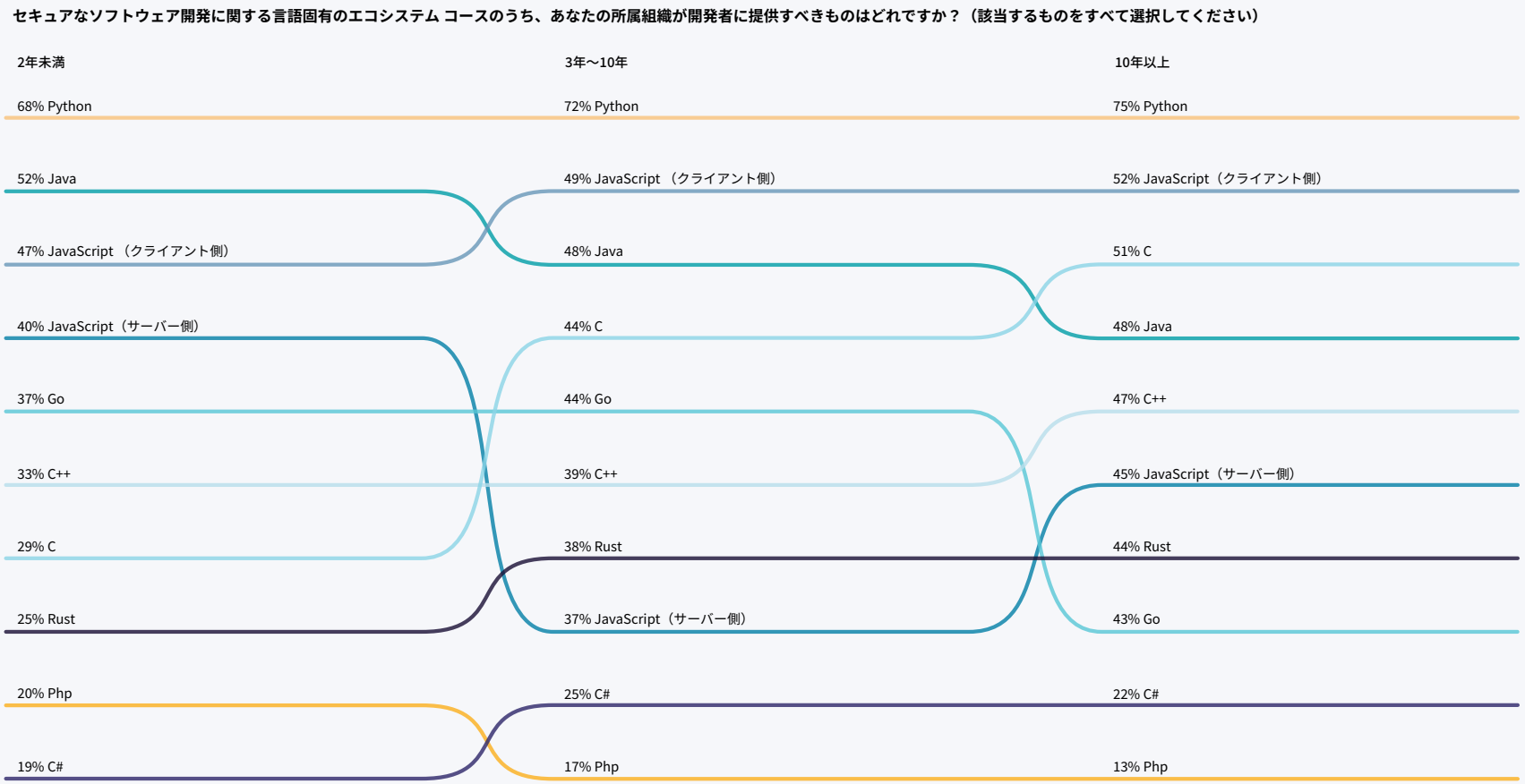
セキュアなソフトウェア開発に関する言語固有のエコシステム コースのうち、あなたの所属組織が開発者に提供すべきものはどれですか？（該当するものをすべて選択してください）



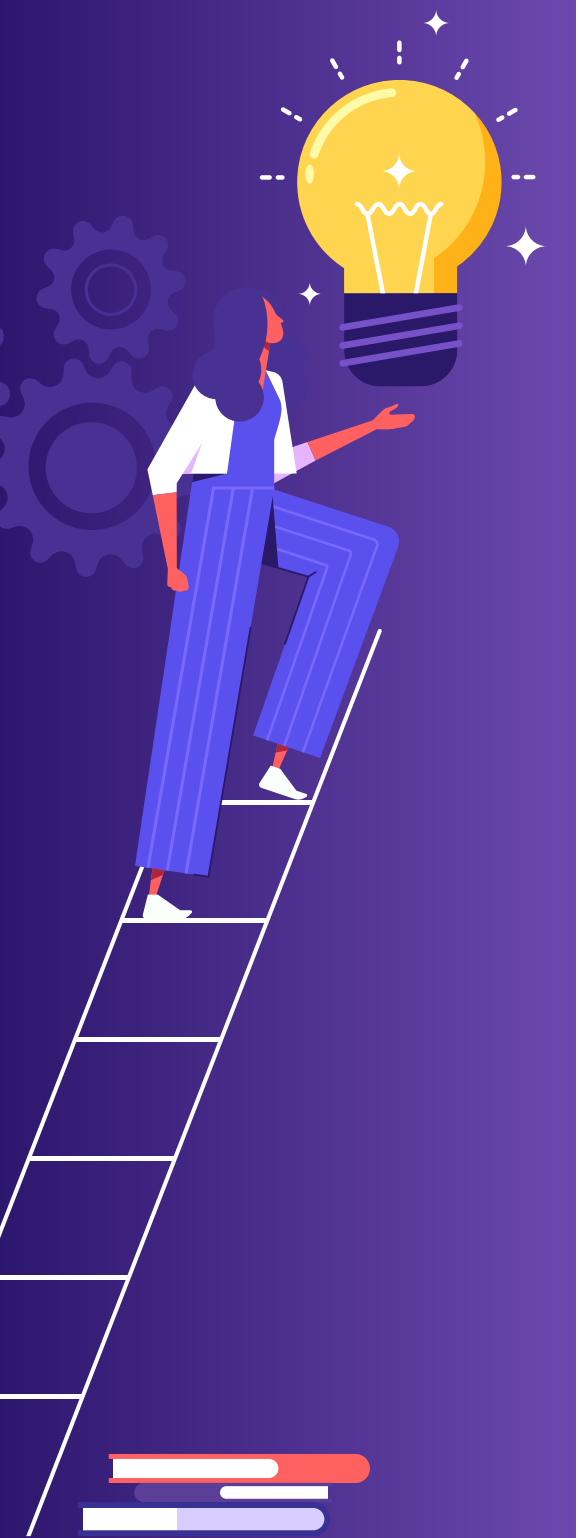
2024 年 SecEd 調査、問 23 と問 15 から構成、サンプル数＝ 350、総回答数＝ 1,445、名前の前の数字は回答者の割合を表し、各列はこの数字でソートされています。

図 41

プログラミング言語別コース（セキュアなソフトウェア開発経験年数別）



2024 年 SecEd 調査、問 23 と問 Q15 から構成、サンプル数＝ 328、総回答数＝ 1,377、名前の前の数字は回答者の割合を表し、各列はこの数字でソートされています。

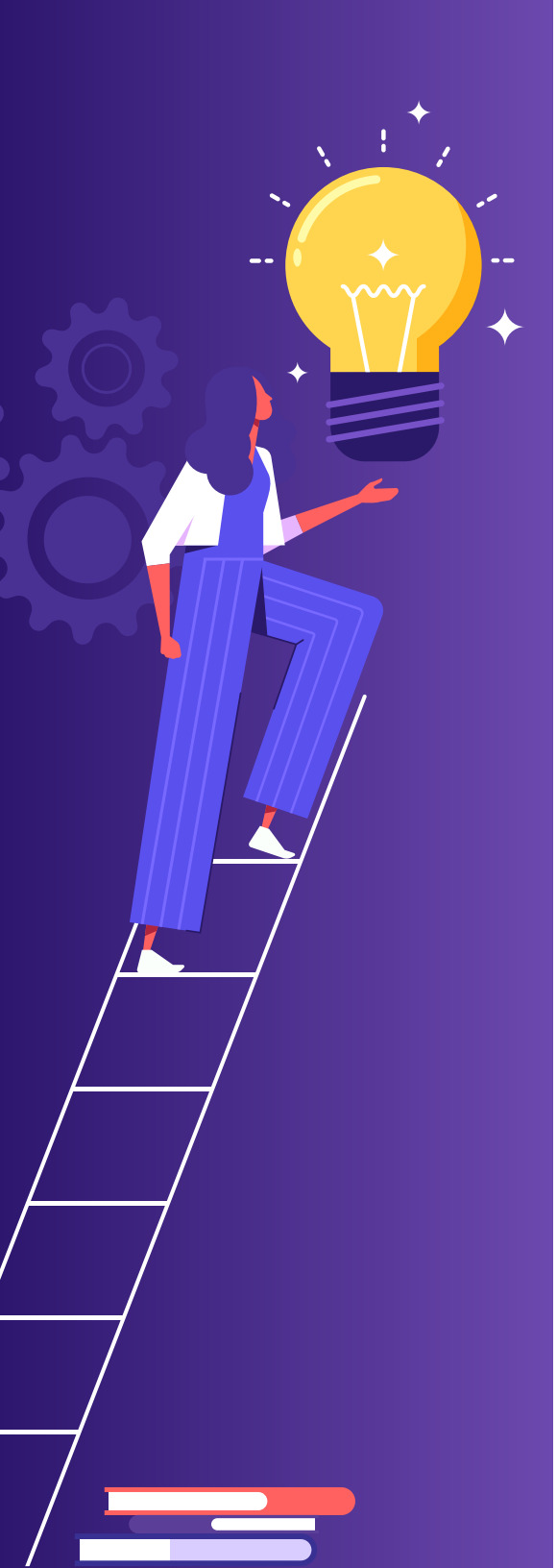


著者について

Dr. MARCO A. GEROSA は、Northern Arizona University における Computer Science の full professor であり、LF Research の research analyst でもあります。ソフトウェア工学とオープンソース ソフトウェアに関する研究により、一流誌に 200 以上の論文を発表。また、著名なカンファレンスのプログラム委員や複数の学術誌の査読者を務めています。博士、情報学修士、コンピュータ工学学士を取得。Institute of Electrical and Electronics Engineers（IEEE）および the Association for Computing Machinery（ACM）のシニア会員。現在、一流研究機関で研究者として活躍している博士課程および修士課程の学生数名を指導。また、20 年以上の教育経験もあります。詳細については、**http://www.marcoagerosa.com** を参照してください。

Dr. DAVID A. WHEELER は、OSS とセキュア ソフトウェア開発のエキスパートです。セキュア ソフトウェア開発に関する著作には、「Secure Programming HOWTO」、「the OpenSSF Secure Software Development Fundamentals Courses」、「Fully Countering Trusting Trust through Diverse Double-Compiling」などがあります。Linux Foundation のオープンソース サプライチェーン セキュリティ担当ディレクターであり、George Mason University でセキュア ソフトウェア開発の大学院コースを教えています。George Mason University で情報工学博士、コンピューター サイエンス修士、情報セキュリティ修了認定、ソフトウェア工学修了認定、電子工学学士を取得。情報セキュリティ プロフェッショナル（CISSP）であり、Institute of Electrical and Electronics Engineers（IEEE）のシニア会員。バージニア州北部在住。

STEPHEN HENDRICK は、Linux Foundation の vice president of research であり、OSS が IT の生産者と消費者にとってイノベーションの原動力となることを Linux Foundation が理解する上で中核となるさまざまな研究プロジェクトの主任研究員を務めています。ソフトウェア業界のアナリストとして 30 年以上にわたって培った一次調査技術を専門としています。また、DevOps、アプリケーション管理、意思決定分析など、アプリケーション開発とデプロイに関する専門家でもあります。市場ダイナミクスを深く洞察するさまざまな定量・定性調査手法の経験を生かし、多くのアプリケーション開発・デプロイの領域で先駆的な調査を行っています。1,000 以上の出版物を執筆し、シンジケート リサーチやカスタム コンサルティングを通じて、世界有数のソフトウェア ベンダーや著名な新興企業に市場ガイダンスを提供しています。



謝辞

調査プロセスに参加してくださったすべての方々、およびセキュアなソフトウェア開発教育の改善に時間と労力を費やしてくださった方々に感謝します。調査プロセスのさまざまな段階に関わってくれた Look Left Marketing と Linux Foundation の同僚に特に感謝します。

- Omkhar Arasaratnam
- Jennifer Bly
- Sally Cooper (Look Left Marketing)
- Anna Hermansen
- Hilary Carter
- Adrienn Lawson
- Noah Lehman
- Angelah Liu
- Geena Pickering (Look Left Marketing)
- Chris Poisson (Look Left Marketing)
- Bryan Scanlon (Look Left Marketing)
- David Sprague (Look Left Marketing)
- Jennifer Tanner (Look Left Marketing)
- Harry Toor

本訳文について

この日本語文書は、**Secure Software Development Education 2024 Survey** の参考訳として、The Linux Foundation Japan が便宜上提供するものです。英語版と翻訳版の間で齟齬または矛盾がある場合（翻訳版の提供の遅滞による場合を含むがこれに限らない）、英語版が優先されます。
この日本語文書を引用する際には、下記の一文を記載してください。
引用：Secure Software Development Education 2024 Surve 参考訳（The Linux Foundation Japan 提供）

翻訳協力：辻村幸弘

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Open Source Security Foundation (OpenSSF) は、Linux Foundation による業界横断的なイニシアチブであり、業界で最も重要なオープンソース セキュリティ イニシアチブと、それらを支援する個人や企業を結集しています。OpenSSF は、オープンソース セキュリティを推進するために、上流や既存のコミュニティとの協力・連携に取り組んでいます。詳細については、openssf.org をご覧ください。

THE LINUX FOUNDATION | Research

2021 年に設立された **Linux Foundation Research** は、拡大するオープンソース コラボレーションを調査し、新たな技術トレンド、ベストプラクティス、オープンソース プロジェクトのグローバルな影響に関する見識を提供しています。プロジェクトのデータベースやネットワークを活用し、定量的・定性的手法のベストプラクティスに取り組むことで、Linux Foundation Research は、世界中の組織にとって有益なオープンソースの見識を得るための最適なライブラリを構築しています。

x.com/linuxfoundation

youtube.com/user/TheLinuxFoundation

facebook.com/TheLinuxFoundation

github.com/LF-Engineering

linkedin.com/company/the-linux-foundation

この著作物を参照するには、以下のように引用してください。
Marco Gerosa, David A. Wheeler, Stephen Hendrick, "Secure Software Development Education Study: Understanding Current Needs," foreword by Christopher Robinson and Dave Russo, The Linux Foundation, June 2024.