THE LINUX FOUNDATION | Research

SBOM（ソフトウェア部品表）とサイバーセキュリティへの対応状況

2022年1月

Stephen Hendrick, VP Research, The Linux Foundation

序文：Jim Zemlin（Executive Director, The Linux Foundation）

協力：

OpenSSF OPEN SOURCE SECURITY FOUNDATION

OPENCHAIN

SPDX

目次

目次

序文

オープンソース コミュニティはソフトウェア、ハードウェア、標準のイノベーションを加速させ続けていますが、ソフトウェアのサイバーセキュリティに関する懸念は絶えず我々の関心を集めています。SolarWinds Orionに対する攻撃が明らかになってからほぼ1年が経過した2021年は、Apache Log4j関連のセキュリティ危機が注目を集めて幕を閉じました。SolarWindsなど過去の多くのクローズドソースの問題は、ソフトウェア セキュリティがオープンソースだけの問題ではないことを示しています。しかし、オープンソースが大きな攻撃対象になっていることは否定できず、私たちのコミュニティとエコシステムは、グローバルなサプライチェーンに対するリスクを軽減するために、標準、プロセス、教育、ツールの整備に共同で取り組む必要があります。今年はサイバーセキュリティへの投資とコンプライアンス要件が大幅に改善されましたが、ソフトウェア サプライチェーンを強化するためには、予防と対応の両面で多くの課題が残されています。これはオープンソースに限った問題ではありませんが、オープンソースのイノベーションは、しばしば集団的な問題を解決へと導いてきました。これは、1つの組織が単独で解決できる問題ではありません。

はっきりさせておきたいのは、私たちは1年前とは違うということです。バイデン政権の「国家のサイバーセキュリティの向上」に関する大統領令は、米国の最も重要な動きとして世界のテクノロジー業界全体に影響を与えました。これを契機に、SBOM（Software Bill of Materials、ソフトウェア部品表）がソフトウェア調達の最前線に位置づけられるようになりました。米国だけでなく他の国々でも、同様の要件を導入すべく議論や計画が進められています。ソフトウェアの脆弱性によって引き起こされる被害を軽減するためには、ソフトウェア部品を特定することが重要です。こうした認識は、グローバルなソフトウェア セキュリティにおける重要なマイルストーンです。

幸いなことに、SBOMを使用してサプライチェーン全体でより強力なソフトウェア セキュリティ対策を実施するための標準とツールがすでにあります。SBOMは、すべてのソフトウェアがサプライチェーン全体でどのように作成され、配布され、使用されるかについて、より信頼と透明性を構築する上で不可欠な役割を果たします。昨年、SPDX仕様はISO/IEC JTC1 5962:2021として国際標準になりました。SPDXや、SBOMコミュニティによって開発されたSBOMツールセットは、SBOMの採用と推進に不可欠です。SPDXはすでに、世界最大の商用サプライチェーンのいくつかで、ソフトウェアのセキュリティと整合性に重要な役割を果たしています。HITACHI、Samsung、Microsoft、Intel、Cisco、Siemens、Googleなどの企業は、すでに何年も前からSPDX SBOMを作成し、使用しています。私たちはこれが今後数年間で大きく拡大することを期待しています。そして、SBOMエコシステムに新しく入ってくる人たちが、そのベストプラクティスを難なく採用できるよう、彼らが直面する課題を理解したいと考えています。

私たちは、SBOMだけでなく、セキュリティにフォーカスした活動を行っているコミュニティにも投資してきました。大手企業のサポートを得て、Open Source Security Foundation（openSSF）を拡大し、サイバーセキュリティの脆弱性に対処するためのツール、サービス、トレーニング、インフラストラクチャ、リソースの提供を充実させてきました。

また重要なこととして、私たちは、サイバーセキュリティの課題の範囲についての全体的な理解を助けるために、積極的に調査を行っています。The Linux Foundationは、サイバーセキュリティのベストプラクティスの実装と標準の採用に関連する重要な問題を調査する一連の中核的な研究プロジェクトの第1弾として、SBOMへの対応状況の調査から始めました。本報告書は、将来のSBOMコラボレーションの取り組みと実装に情報を提供し、影響を与える手段として、SBOMの認知度、採用、および課題の現状を明確に示しています。

私たちは、世界中のサイバーセキュリティとITの専門家に、この、2021年におけるSBOMへの対応状況を参考にしていただけたらと考えています。本書をお読みになり、関係者の方々と共有して、SBOMやその他のプラクティスをそれぞれの組織で実践していただけたらと思います。

Jim Zemlin Executive Director, The Linux Foundation

Of organizations surveyed,
98% use open source software.

FIGURE 6 | PAGE 15

Of organizations surveyed,
95% are concerned about software security.

FIGURE 9 | PAGE 18

Of organizations surveyed,
76% currently have a level of SBOM readiness.

FIGURE 20 | PAGE 29

Of organizations surveyed,
47% are using SBOMs today.

FIGURES 21 & 24 | PAGE 30

SBOM use will increase by 66%
for organizations in 2022.

FIGURE 29 | PAGE 43

Based on organizations surveyed, it's forecasted
78% will use SBOMs in 2022.

FIGURE 29 | PAGE 43

Based on organizations surveyed, it's forecasted
88% will use SBOMs in 2023.

FIGURE 29 | PAGE 43

Of organizations using SBOMs today,
74% produce AND consume SBOMs.

FIGURES 21 & 24 | PAGE 30

#1 ACTION:
Get a vulnerability reporting system
in order to better secure your software supply chain.

FIGURE 13 | PAGE 23

#2 ACTION:
Use SBOMS to better secure your software supply chain.

FIGURE 13 | PAGE 23

When *producing* SBOMs...
#1 BENEFIT:
developers better understand dependencies.

FIGURE 22 | PAGE 31

When *consuming* SBOMs...
#1 BENEFIT:
better support for compliance and reporting.

FIGURE 25 | PAGE 37

要旨

SBOM（ソフトウェア部品表、Software Bill of Materials）は、ソフトウェアのコンポーネントとその依存関係、およびライセンス データを一意に識別する形式的で機械可読なメタデータです。SBOMデータ フォーマットは進化しており、近い将来コンポーネントの信頼性を検証するための情報を提供し、既知の脆弱性へのリンクを提供するようになるでしょう。SBOMは組織全体で共有されるように設計されており、ソフトウェア サプライチェーンの参加者によって提供されるコンポーネントの透明性を提供するのに特に役立ちます。ソフトウェア セキュリティに関心のある組織は、SBOMをサイバーセキュリティ戦略の要としています。

Linux Foundation Researchは、2021年の第3四半期に組織のSBOMの準備と採用に関する世界的な実証研究を実施しました。調査には世界から412の団体が参加しました。本報告書では、この調査の結果を詳しくレポートしていますが、、特に重要なポイントは以下のとおりです。

1. 98%の組織が導入しているソフトウェアのセキュリティを憂慮していて、72%がソフトウェア セキュリティに強い懸念を抱いています。ソフトウェア セキュリティに対する懸念は、アジア太平洋地域で最も高く、35%の組織が非常に懸念しています。これに対してアメリカ大陸では21%、EMEA（ヨーロッパ、中東、アフリカ）では18%です。**図:1**、**A15**。

2. 組織が使用するソフトウェアを選定する際に最も優先する事項は、第1位が「セキュリティ」で、第2位はライセンス コンプライアンスでした。これらは、2番目に優先する事項、3番目に優先する事項でも、同じでした。**図5**。

3. 組織がソフトウェア セキュリティに関心を持つ主な理由は、財務リスク(66%)、風評リスク(61%)、法的リスク(53%)です。これらは潜在的なリスクなので、ソフトウェア セキュリティに対処するためには、一貫した戦略が必要だということを表しています。**図10**。

4. 米国の「国家のサイバーセキュリティ向上に関する大統領令」は、世界中に影響を及ぼしています。全体として、80%の組織がこの大統領令を認識しており、76%の組織がこの大統領令を受けて変更を検討しています。**図A16**および**A17**。

5. ソフトウェア サプライチェーンを保護するための主な活動はSBOMを重視しています。全体として、47%の組織が拡張性のある脆弱性レポートを望んでおり、45%がSBOMをソフトウェア サプライチェーンを保護するための重要な方法と考えています。さらに、39%の組織がグローバルに一意な識別子の対応を希望しており、34%が再現可能なビルドを使用したコンポーネント検証を希望しています。現在、一部のSBOMデータ フォーマットでは、コンポーネント検証と脆弱性報告がサポートされています。グローバルに一意な識別子は、パッケージURL(PURL)の主要なデータ形式でサポートされつつあります。今日、SBOMはソフトウェア サプライチェーンを確保するための様々な活動をサポートしています。**図13**。

6. サンプルの組織全体では、90%の組織がSBOMへの移行を開始しています。10%の組織がSBOMの計画を開始しておらず、14%が計画または開発段階にあり、52%がビジネスのいくつか、または多くの領域でSBOMに取り組んでいて、23%が事業のほぼすべての分野でSBOMに取り組んでいるか、SBOMの使用を含む標準的な慣行を有しています。これは、全体として76%の組織がSBOMに対応していることを意味します。**図20**。

7. SBOMの作成は、商用ソフトウェアを開発する組織で行われることが最も多いですが、私たちの調査では、SBOMがはるかに広く採用されていることが示唆されています。私たちのサンプルのすべての組織で、SBOMを作成する計画がないのは7%だけです。40%は6-24ヶ月でSBOMを作成する計画があり、27%はいくつか、いくつか、または多くの事業分野でSBOMを作成しており、21%はほぼすべての事業分野でSBOMを作成しているか、SBOMの使用を含む標準的な習慣を持っていますが、4%はそれを知りません。全体として、48%の組織が今日ある程度のSBOMを作成しています。**図21**。

ITベンダー、サービスプロバイダ、およびエンドユーザーを調査したこの画期的な調査では、SBOM（ソフトウェア部品表）の準備と採用に関する経験的な見解が示されています。この調査では、オープンソースソフトウェアの使用が広く普及しており、ソフトウェアセキュリティが組織の最優先事項であることが示されています。ソフトウェアセキュリティへの世界的な取り組みを受けて、SBOMは重要な実現手段として注目されるようになってきました。

SBOMに精通していること、準備ができていること、採用されていることは、予想以上に広範囲にわたっています。SBOM用語に精通している割合は82%でした。SBOMの準備状況（SBOMのニーズへの対応に積極的に取り組んでいる）は76%でした。少なくともいくつかの事業部門におけるSBOMの作成または使用は、それぞれ48%と46%でした。

SBOMを作成または使用する組織計画に基づくと、2021年には47%の組織がSBOMを作成または使用しています。SBOMの作成または使用の増加は、2022年の間に約66%加速すると予想され、78%または組織によるSBOMの作成または使用につながります。2023年のSBOMの増加率は13%に減少し、組織全体でSBOMの作成または使用をしている率は88%に達すると予想されています。

8. 私たちの調査参加者が明らかにしたメリットの上位3つは、開発者がアプリケーション内のコンポーネント間の依存関係を理解しやすいこと(51%)、コンポーネントの脆弱性を監視しやすいこと(49%)、ライセンスコンプライアンスを管理しやすいこと(44%)です。SBOM**図22**。

9. 組織は、SBOMの採用と利用がどのように進化するかについて、引き続き懸念を抱いています。40%はSBOMに対する業界のコミットメントが不明確であることに、39%はSBOMに何を含めるべきかについて業界のコンセンサスがあるかどうか疑問であることに、37%はSBOMが顧客に提供する価値が明確でないことに、それぞれ懸念しています。ここに、SBOM市場の二面性があります。運用面でSBOMに大きく関与しているのに、コミットメントは低くなっているのです。**図23**。

10. SBOMをどう活用するかは、SBOMをどのように構築するかによります。SBOMを活用する計画がない組織は全体のわずか6%で、42%は今後6～24か月以内にSBOMを活用する計画をもっています。28%は事業のいくつか、または多くのセグメントでSBOMを活用していて、18%は事業のほぼすべてのセグメントでSBOMを活用しているか、またはSBOMの利用を含む標準的な習慣を持っています。全体として、現在は、組織の46%がある程度SBOMを活用しています。**図24**。

11. SBOMの活用メリットは説得力があります。組織の53%が、SBOMは報告とコンプライアンス要件に対処するためのより良いアプローチを提供していると語っています。53%はまた、SBOM情報によってリスクに基づく意思決定が改善されると答えており、49%はSBOM脆弱性レポートによって組織がセキュリティ リスクをより迅速に理解できると答えています。これらの活用メリットは、作成メリットと整合性がとれています。コンプライアンス要件への対応は、ライセンス コンプライアンスの管理に結び付きます。リスクに基づく意思決定とセキュリティ リスクにさらされる機会を減らすことは、依存関係の明確化とコンポーネントの脆弱性の監視によってもたらされます。**図25**。

12. 業界のコンセンサスがさらに得られれば、SBOMの導入と活用がいっそう進むでしょう。62%の組織は、SBOMの構築と利用をDevOpsに統合する方法について、業界のコンセンサスが広がることを期待しています。また、58%はSBOMをリスクとコンプライアンスのプロセスに統合することについて、53%はSBOMがどのように進化し改善するかについて、業界での理解が広がることを望んでいます。**図27**。

業界や組織を超えたSBOMの準備、作成および利用は、運用化の過程にある。ソリューションは出現しつつありますが、業界全体の実践者のコンセンサスはまだ特定の方法論、フォーマット、ツール ワークフローに統合されていません。ソフトウェア ベンダーおよびサービス ベンダー コミュニティによる目に見えるサポートは、成長を加速させるために重要で、ソフトウェア サプライチェーンを保護するというSBOMの役割を明確にします。

はじめに

現在行われているデジタル トランスフォーメーションの多くは、ビジネス プロセスの改善、自動化、リソース会計への対応を改善し、生産性を向上させるために自らを位置づけている企業に焦点を当てています。デジタル経済によってもたらされる機会には、新しいビジネスモデルを追求し、新しい顧客セグメントと収入源にアクセスする能力も含まれます。多くの場合、業界のリーダーは、クラウド コンピューティング、エッジ コンピューティング、人工知能ソフトウェア、組み込みシステムによって実現される「ソフトウェア定義」（Software Defined）モデルに移行してきました。このようなデジタル変革の時代には、ソフトウェア資産が適切に調達および管理されていなければ、サイバーセキュリティのリスクが増大することになります。

サイバーセキュリティ：世界的な懸念

サイバーセキュリティは世界的な関心事です。SolarWindsへの攻撃は米企業に対するものでしたが、当時の同社の顧客は190カ国、30万人を超え、売上の38%は米国外からのものでした。このことは、SolarWindsへの攻撃は全世界が対象となっていて、国家や非政府によるサイバー攻撃がますます巧妙化していることを示しています。サイバーセキュリティ攻撃には、さまざまな目的があります。ほとんどの攻撃は金融犯罪に分類されますが、より洗練された攻撃は政治的、産業的、経済的、影響力指向の目的を持つことがあります。

米国は、世界のGDPの24%を占めていますが、地域別のGDPの割合はもっと均等に分布しています。GDPに占めるアメリカ大陸の割合は32%であるのに対し、欧州、中東、アフリカ（EMEA）では30%、アジア太平洋地域では38%です。世界のGDPの地域別分布は、ソフトウェア セキュリティに対する地域ごとの懸念レベルとよく相関しています。図1は、組織が使用するソフトウェアのセキュリティに対する懸念レベルを示しています。ここで「非常に懸念している」と回答した割合は、アメリカ大陸が49%、欧州・中東・アフリカ（EMEA）地域が55%で、共にこれがピークとなっています。これらはおおむね正規分布であり、アメリカ大陸とEMEAでは約20%が「懸念している」または「極めて懸念している」と回答しています。[1]

欧州連合（EU）は過去10年間、サイバーセキュリティ分野での影響力を拡大してきました。一般データ保護規則（GDPR）は2014年にEUで採択され、2016年に強制力のある規則となりました。GDPRは、個人情報（PI）を高度に管理し、PIを処理するための要件を確立することを目的としています。これに基づいて、ネットワークと情報システムのセキュリティに関する指令（NIS指令）と2019年のEUサイバーセキュリティ法が制定されました。NIS指令は、デジタル サービス プロバイダーに対し、リスクを積極的に管理し、サイバーセキュリティ インシデントに対処するための国家の能力を高めることを求めています。EUサイバーセキュリティ法は、デジタル製品、プロセス、サービスを認証するための規制を定めています。

図1のアジア太平洋地域の分布は、米国やEMEA地域の分布とは大きく異なっています。アジア太平洋地域のセキュリティ上の懸念は徐々に高まっており、15%が「やや懸念している」と回答しています。18%が「懸念している」31%「非常に懸念している」、35%が「非常に懸念している」と回答しました。アジア太平洋地域で「非常に懸念している」組織の数は、EMEAの約2倍で、アメリカ大陸と比較しても約67%多くなっています。アジア太平洋地域でソフトウェア セキュリティの懸念が高い理由は、本報告書全体を通して説明されることになりますが、これはアジア太平洋地域がこれまでセキュリティ関連の役割、機能、活動に投資してこなかったためと思われます。[2]

中国も同様に、サイバーセキュリティに関する態勢を改善してきていて、2017年のサイバーセキュリティ法では、ITサービス提供者とそのPIの処理方法が規制されました。この規制に続いて、2021年に制定された「データセキュリティ法」では、「国家基幹データ」に関して、政府を中心とした規制が強化されました。2021年11月現在、中国は新しい個人情報

保護法（PIPL）を制定しました。これは、政府がテクノロジー企業に対してより大きな影響力を持つと同時に、PI要件を徐々に改善してきています。

2021年5月の米国大統領令と合わせて考えると、ソフトウェア セキュリティとサイバーセキュリティに世界的な大変化が起きていることは明白でしょう。PIの保護は明らかに1つの側面ですが、ソフトウェア製品、プロセス、サービスの形でのデジタル資産の保護も極めて重要です。

米国のサイバーセキュリティ

サイバーセキュリティの問題は非常に深刻になっており、米国では、2021年5月にホワイトハウスが国家のサイバーセキュリティの改善に関する大統領令（EO）を発令しました。このEOの理論的根拠は、「公的部門、民間部門、そして究極的には米国民の安全とプライバシーを脅かすサイバーキャンペーンが、ますます巧妙化している」ことでした。EOは以下の7つの分野に焦点を当てています。[3] [4]

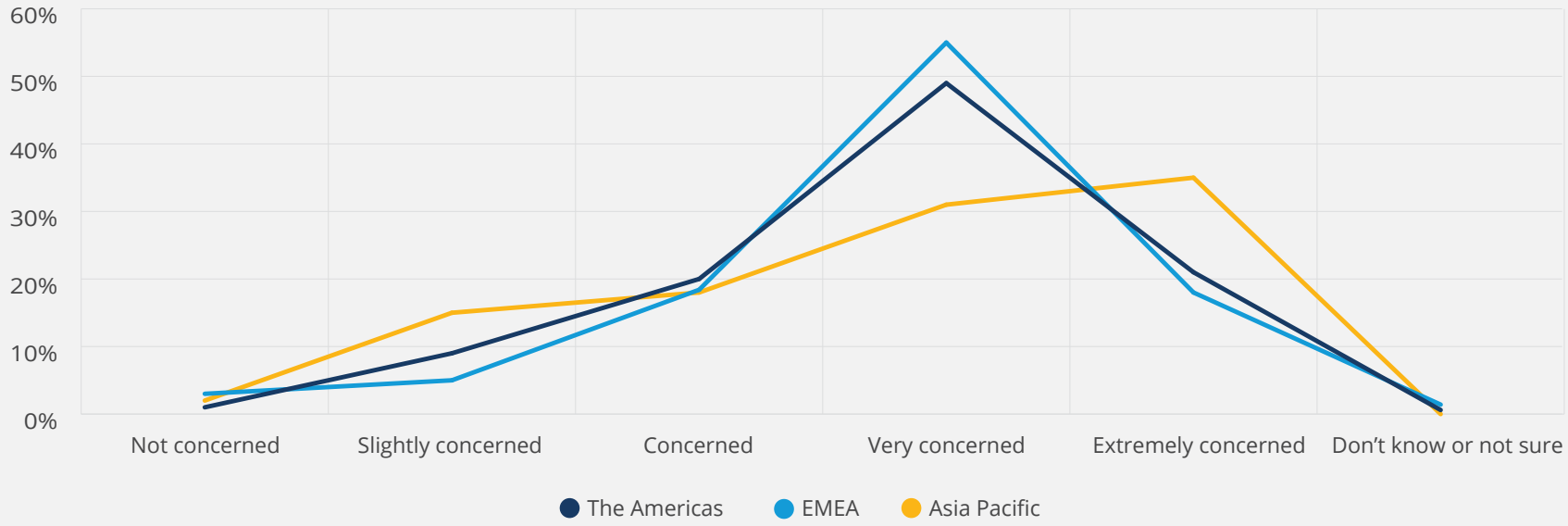
1. 脅威に関する情報共有の障壁を取り除く

2. 連邦政府のサイバーセキュリティの近代化

図1

How concerned is your organization about the security of the software that it uses?

Single Response | N = 341



3. ソフトウェア サプライチェーンの透明性と安全性の強化

4. サイバー安全審査委員会の設置

5. 脆弱性とインシデントに対する連邦政府の対応の標準化

6. 連邦政府ネットワークにおける脆弱性およびインシデントの検出の改善

7. 連邦政府の調査・修復能力の向上

この問題は米国に限った話ではなく、サイバーセキュリティを改善するために力を注いでいる国は米国だけではありません。ソフトウェア サプライチェーンの透明性とセキュリティを強化することは非常に重要です。これは、米国連邦政府だけでなく、世界中のほぼすべての公共部門および民間企業が、ビジネスおよびミッションクリティカルな活動をサポートするためにクリティカルなソフトウェアに依存しているからです。EOで定義されているように、クリティカル ソフトウェアとは、高度なシステム特権を与えたり要求したり、ネットワークやコンピューティング リソースに直接アクセスしたりするなど、信頼に不可欠な機能を実行するソフトウェアです。ソフトウェア サプライチェーン セキュリティへの対応には、次のような多くのアクティビティが含まれます。

- 開発環境の確保
- 含まれているソフトウェア コンポーネントの既知の脆弱性と潜在的な脆弱性をチェックし、修正するツールを使用する
- ソフトウェア製品に組み込まれるコードの正確で最新のデータと出所を維持する
- 購入者に各ソフトウェア製品のSBOM（ソフトウェア部品表）を提供する

SBOM（ソフトウェア部品表）は、これらのニーズのいくつか、特にソフトウェア ベースの製品の脆弱性、ライセンス義務、および出所の理解に焦点を当てたニーズに対処するための効果的な方法です。したがって、SBOMの作成と使用は、オープンソース コンポーネントとクローズドソース コンポーネントの両方を含むすべてのタイプのソフトウェア製品にわたって、さまざまな信頼の問題に対処する効果的な方法であると考えられています。国家電気通信情報管理局（NTIA）が特定したSBOMのメリットは、次のとおりです。

- コストの削減
- セキュリティリスクの軽減
- ライセンスリスクの軽減
- コンプライアンス・リスクの軽減

SBOMの使用事例には、ソフトウェア開発、サプライチェーン管理、脆弱性管理、資産管理、調達、および高保証プロセスの改善が含まれます。[5]

テクノロジー ベンダー、ソリューション／サービス プロバイダー、業界組織は、このEOを真剣に受け止めています。ソフトウェア サプライチェーン セキュリティに対処する上でSBOMが中心的な役割を果たすということが、本調査研究の重要なきっかけとなりました。この調査では、「組織はSBOM要件とそれを実施するために必要なサイバーセキュリティ プラクティスに対して、どの程度の準備ができているか」という疑問に答えることを試みました。

SBOM成熟度

本報告書では、SBOMの作成と使用のレベルだけでなく、SBOMの準備状況についてもレポートします。調査で用いた質問項目は、組織がSBOM活用のどの段階にいるかを明らかにするよう設計されました。それは、無関心から計画中、あるいはさまざまな採用段階に至るまで多岐に渡っています。SBOM採用課程の全体的な識別に適していたので、私たちは、この質問に対する回答を、「SBOM慎重派」「SBOMアーリー アダプター」「SBOMイノベーター」の3つのカテゴリーに集約しました。回答者は、報告されたカテゴリーを自己選択しました。これらのカテゴリーがSBOM準備対応にどのようにマップされたかについての詳細は、本報告書の「方法論」のセクションをご参照ください。

調査対象

このセクションでは、調査対象者の統計データを抜粋して示します。残りの属性は付録Aにまとめました。このセクションで説明する属性は、調査対象者、組織の規模と収益、役割、業界――といった点を理解するのに役立ちます。**図2**は、この情報をまとめたものです。

図2は、SBOM準備状況の調査が世界中で実施されたことを示しています。この調査には、あらゆる規模および収益の企業が参加し、主に情報技術（IT）の役割に焦点を当て、多くの垂直的な業界にまたがっています。情報技術、自動車、医療およびライフサイエンス、製造業、金融サービスおよびエネルギーの各業界で、多くの企業が参加しています。

地域別SBOM成熟度

SBOMの成熟度については、各地域で独自のプロファイリングが行われています。**図3**は、3つの主要地域ごとに、SBOMの成熟度分布を示したものです。SBOMイノベーターは、アメリカ大陸とアジア太平洋地域で高い存在感を示しています。回答の90%が北米からのものであったアメリカ大陸

図2

Summary level demographics

N = 412

- **44%** IT & Engineering
- **39%** Prod/Pgm Management
- **17%** Business Operations

- **24%** $1m–$50m
- **12%** $50m–$100m
- **15%** $100m–$500m
- **11%** $500m–$1b
- **12%** $1b–$5b
- **4%** $5b–$10b
- **7%** $10b+
- **14%** No answer or DKNS

- **13%** 1–100 Employees
- **21%** 100-500 Employees
- **29%** 500–2K Employees
- **15%** 2K–5K Employees
- **8%** 5K–15K Employees
- **15%** 15K+ Employees

- **45%** Development
- **31%** C-level
- **13%** Operations
- **11%** OSPO & Other

- **25%** IT
- **12%** Automotive
- **11%** Healthcare
- **7%** Manufacturing
- **6%** Fin Services
- **5%** Energy
- **4%** Telco
- **4%** Retail/Wholesale
- **26%** Other Industries

では、北米におけるSBOMイノベーターの相対的割合は、他のアメリカ大陸（メキシコ、中南米）と同じでした。

アジア太平洋地域でSBOMイノベーターの相対的な割合が多いのは、オーストラリアやシンガポールなどのアジア太平洋諸国とインドの状況が反映されたからです。一方で、アジア太平洋地域では、SBOMイノベーターとSBOM慎重派との二極化が特徴となっています。この特徴は特に中国、ロシア、その他のアジア太平洋地域で顕著でした。EMEAは、SBOMイノベーターの相対的な割合は少ないのですが、SBOMアーリー アダプターのそれは、アメリカ大陸に匹敵します。

企業収益別のSBOM成熟度

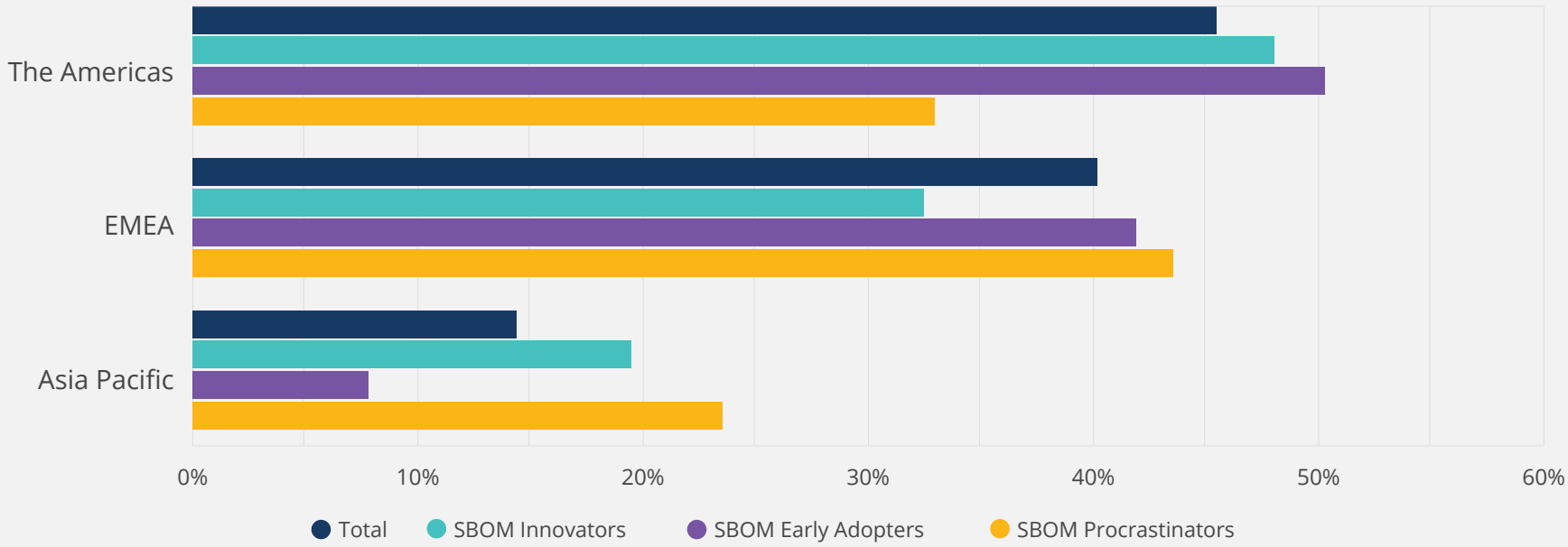
調査対象には、多くの中小企業と、驚くべき数の超大企業が含まれています。全体として、調査対象の51%は年間収益が5億ドル未満で、11%は50億ドル以上でした（調査対象の14%は、企業収益が分からない、または未回答）。さらに、調査対象の63%は従業員2000人未満の企業で、15%は従業員1万5000人以上でした。

調査対象企業が多岐にわたることを考慮して、企業規模と収益がSBOMの成熟度に影響するかどうかを把握したいと考えました。私たちの仮説は、企業の規模と企業の収益が増加するにつれて、SBOMの成熟度も増

図3

What geographic region do you live in?

Single Response | Segmented by SBOM maturity | N = 341



加するというものでした。大企業ほど製品ポートフォリオが複雑になり、ITへの投資が増え、ソフトウェアサプライチェーンの問題を改善する必要性が高まる可能性があります。**図4**は、SBOM成熟度別の平均年間収益を示しています。

この結果は、私たちの仮説を裏付けるものでしたが、期待したほど顕著ではありませんでした。その理由は、収益分類の数値幅が大きく、数十億の収益がある回答者は割合が少なくても影響が大きく、逆に収益が数百万の回答者では影響が小さくなってしまうからです。SBOMの成熟度が進むほど収益が大きい傾向がありますが、それは収益が2億5000万ドル以上になったところで最も顕著でした。

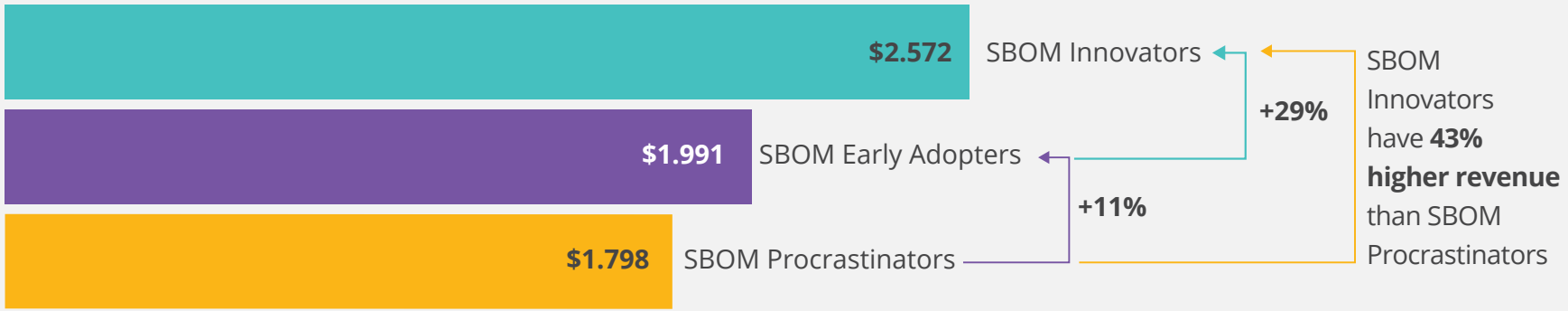
このことからわかるのは、大企業と超大企業が主にSBOMを推進しているということです。これは理にかなっています。なぜなら、大企業は中小企業よりも得るものが多く、失うものも大きいからです。また、中小企業の規模とIT優先順位では、SBOMはあれば良いものの、後でも構わないものとなっているからです。

大企業は中小企業よりも得るものが多く、失うものも大きい。中小企業では、規模が小さく、他にも優先すべき課題があるため、SBOMはあれば良いもの、後でも構わないものとなっている。

図4

Average Annual Revenue ($B)

Segmented by SBOM maturity | N = 341



ソフトウェア セキュリティの重要性

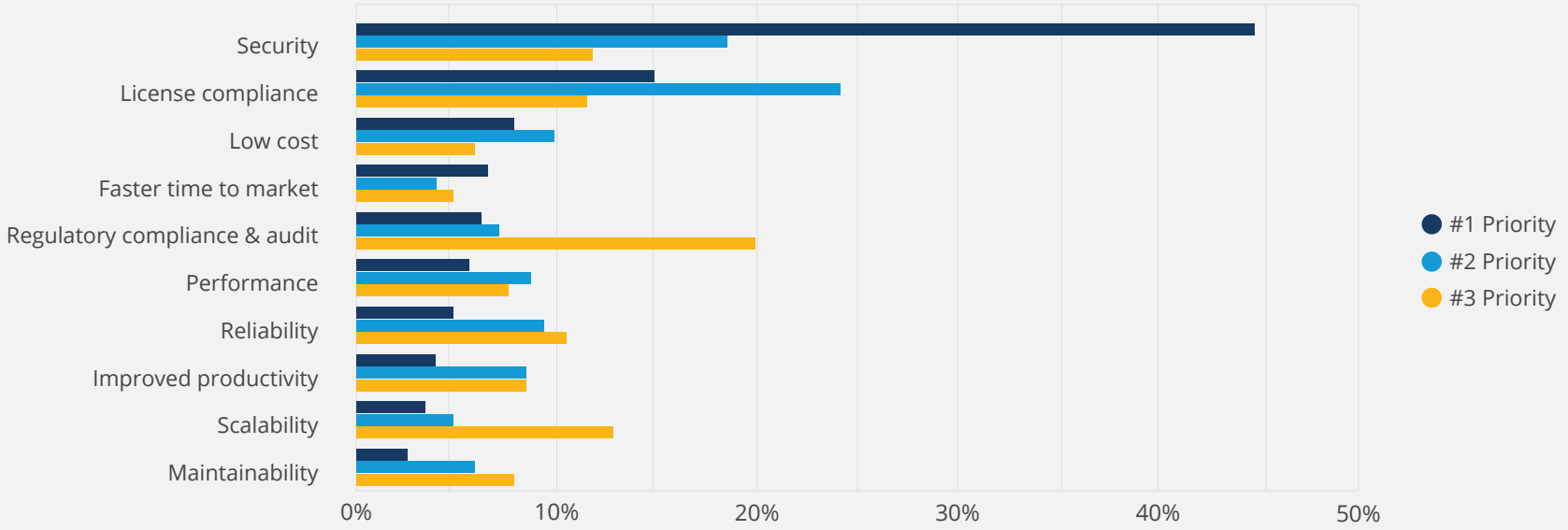
企業のさまざまな優先事項の中で、セキュリティがどのように位置づけられているかを明確にするために、私たちは回答者に、10のIT目標をランク付けするよう求めました。**図5**は、この質問の上位3つ（#1プライオリティ、#2プライオリティ、#3プライオリティ）にランク付けされた割合を、#1プライオリティに選ばれた割合が多い順にソートしたものです。「セキュリティ」は最優先事項（#1プライオリティ）の45%であっただけでなく、ライセンス コンプライアンス（15%）よりも3倍も重要でした。

セキュリティが重要であることは、#1～#3に選ばれた割合の合計が最大となっていることからも、明らかです。ライセンス コンプライアンスは、#1プライオリティおよび#2プライオリティの合計で2番目に重視されているIT目標です。#2プライオリティに選ばれた割合では、ライセンス コンプライアンスは、セキュリティと肩を並べています。また、#1プライオリティで5位にランクされている法規制コンプライアンスは、#3プライオリティに挙げられた割合が多かったことにより、トータルでは第3位となりました。

こうした分析により、セキュリティとコンプライアンス（ライセンス、規制、監査）が、従来からあるさまざまなIT目標と比較しても、特に重要視されていることが分かります。現在は、GRC（ガバナンス、リスク、コンプライアンス）に伴うセキュリティと財務リスクが大きくなり、これらが優先度の高い課題になっていることを意味しています。

図5

Rank order the priorities below that most often influence what software your organization chooses to use.



オープンソースの成熟度とSBOM準備の関係

オープンソースがアプリケーションの開発と運用に広く浸透している今、オープンソース ソフトウェアの使用におけるSBOM成熟度の関係を調べることは重要です。次の4つの質問と図は、企業がオープンソース ソフトウェアの使用に基づいてSBOMの成熟度にアプローチする方法の類似点と相違点を示しています。

SBOMイノベーターはオープンソース ソフトウェアを利用することでリスクが高まるか?

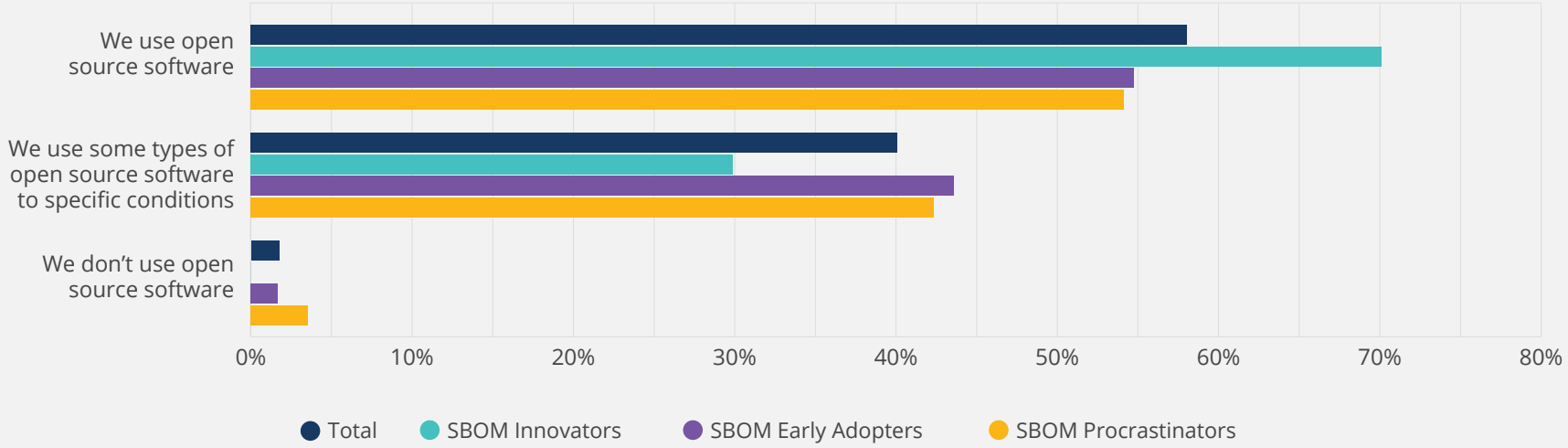
図6を見ると、オープンソース ソフトウェアの使用が普及していることが分かります。全体として、サンプルの98%がオープンソース ソフトウェアを使用しています。企業がオープンソース ソフトウェアを使用する方法の違いは、その使用に付随する条件に基づいています。サンプル全体の58%がオープンソース ソフトウェアを使用しており、ニーズ、機能、コストに基づいて、クローズドソース ソフトウェアを使用するのと同じ方法で使用しています。しかし、サンプル全体の40%は特定の条件に従ってオープンソース ソフトウェアを使用しています。おそらく、これらの条件は、ソフトウェアがリスクを軽減するように設計された内部要件を満たしているか、または、それを超えていることを確認するために設定されていると思われます。

SBOMイノベーターを除き、SBOM成熟度による区分けは、SBOMイノベーターが条件なしにオープンソース ソフトウェアを使用する傾向が高いことを除いて、サンプル全体の特性とほぼ完全に一致しています。SBOMのイノベーターは、主にSBOMを標準的なプラクティスの一部として利用しているため、SBOMの自動利用によって、ライセンスとセキュリティに関する

図6

What is your organization's perspective on using open source software?

Single Response | Segmented by SBOM maturity | N = 341



多くの重要な懸念事項が確実に解決されると考えられます。SBOMイノベーターはリスクにさらされることはありません。オープンソース ソフトウェアの使用に関して、より包括的で洗練された文化を持っているだけです。

オープンソース ソフトウェアの条件付き使用

特定の条件に従ってオープンソース ソフトウェアを使用すると答えた回答者に対しては、組織がオープンソース ソフトウェアを使用する条件を理解するために、複数回答のフォローアップ質問が行われました。図7に示すように、全体的な調査結果には、コード パフォーマンスの検証（54%）、コード セキュリティの検証（51%）、適切なコード サポートの検証（51%）、コードの出所の検証（48%）、コード ライセンスの検証（41%）が含まれています。

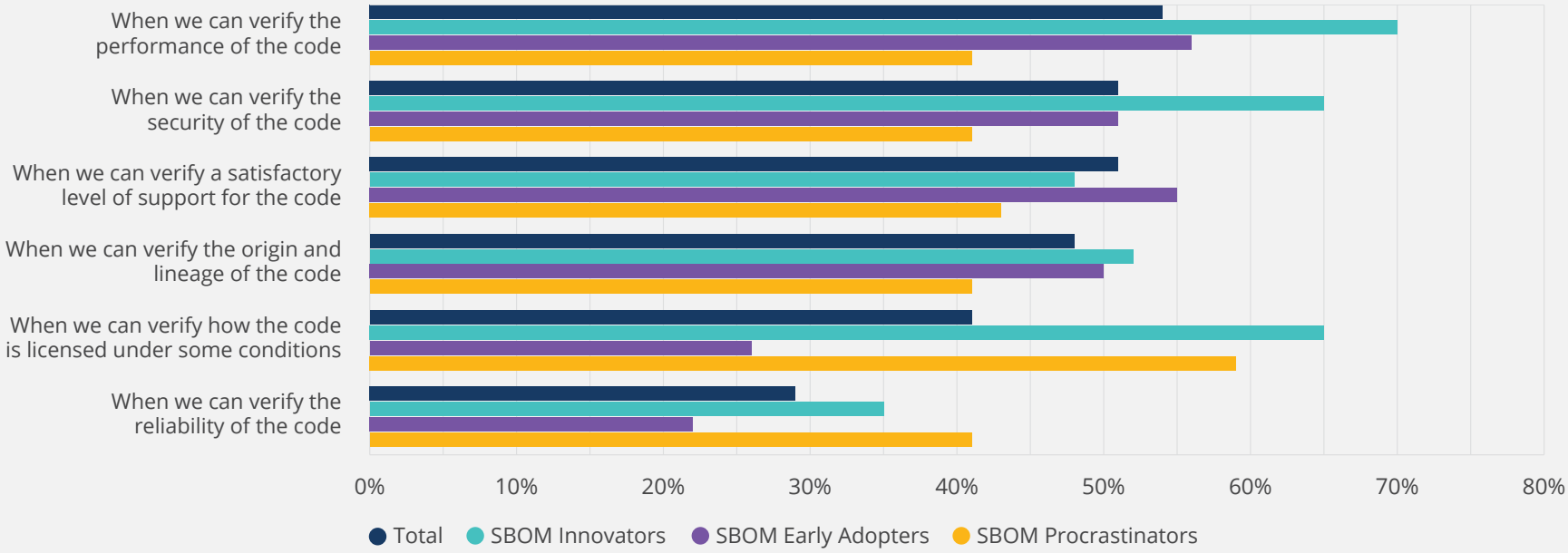
図7を全体的に見ると、特定の基準に従ってオープンソース ソフトウェアを使用している組織は、説明されているすべての方法でこのソフトウェアを検証することに関心があることが分かります。SBOMは、これらの基準のうち、セキュリティ（脆弱性）、出所（起源と系譜）、およびライセンスの3つに対処する上で効果的です。オープンソース コードのパフォーマンス、テクニカル サポート、信頼性を検証することも重要ですが、そのためには利用側の組織がコンポーネントを慎重にテストする必要があります。

SBOM成熟度によりデータをセグメント化すると、全体の結果とわずかな違いが見られました。SBOMイノベーターは、コード パフォーマンスの検証（70%）、コード セキュリティの検証（65%）、およびコード ライセンスの検証（65%）に強い関心を示しています。これら3つの課題は、SBOMイノベーターにとって明らかな優先事項です。

図7

Under what conditions will your organization use open source software?

Select all that apply | Segmented by SBOM maturity | N = 138, Valid Cases = 138, Total Mentions = 381



SBOMのアーリー アダプターは、パフォーマンス、セキュリティ、サポート、およびソースに関連する問題の全体的な合計とほぼ一致しています。唯一の違いはコード ライセンスであり、サンプル全体の41%に対して、SBOM アーリー アダプターは26%にとどまっています。

SBOM慎重派は、すべてのことが気になるという点が特徴的です。59%のライセンスが際立っていますが、SBOMの慎重派はオープンソースの使用に関してより高いレベルの不安を持っているようであり、これはオープンソース ポリシーの策定に対して彼らが行った投資のレベルが低いことと相関しています。

SBOM成熟度によるオープンソース ソフトウェアの使用状況の変化

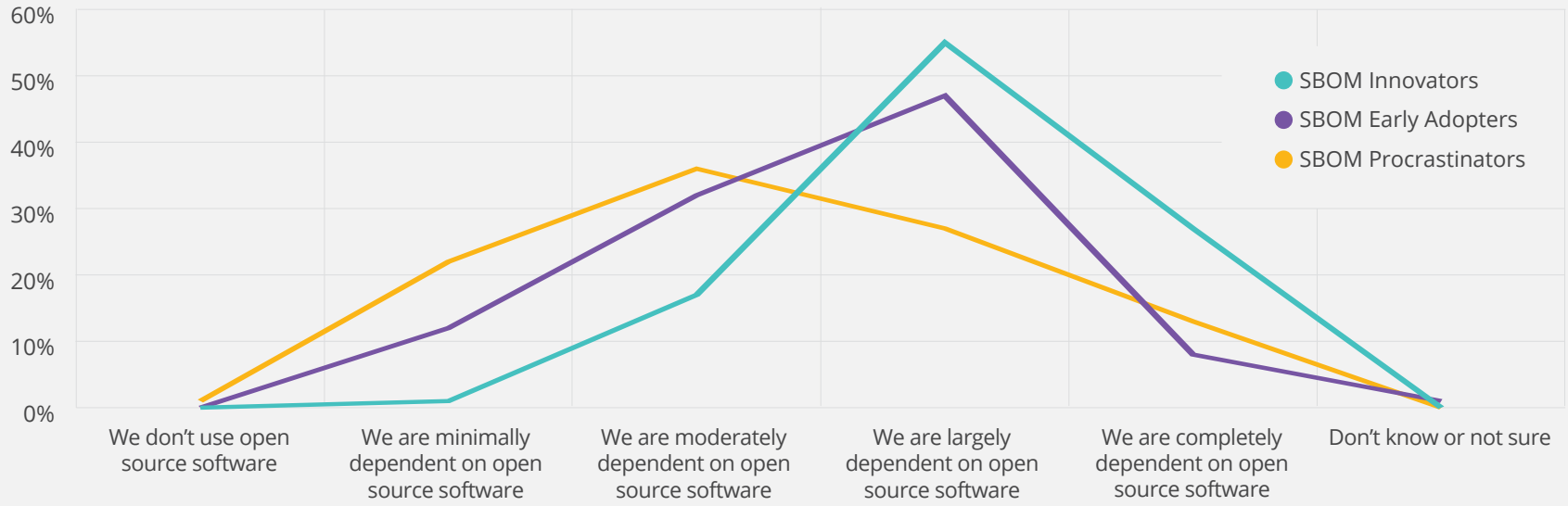
図8は、オープンソース ソフトウェアが広く使用されていることを示しています。しかし、企業がオープンソース ソフトウェアにどれだけ依存しているのか、また、SBOMの成熟度に基づいて、この依存関係はどのように変化するのでしょうか。**図8**は、企業がオープンソース ソフトウェアにどの程度依存しているかをSBOM成熟度別に示したものです。**図8**の分布は、SBOM成熟度別の分布をより連続的に示すもので、これらの分布の形状に対する視覚的な洞察を提供するだけです。

SBOM慎重派の分布は36%にピークがあり、オープンソース ソフトウェアへの依存度は中程度です。SBOMのアーリー アダプター47%) とイノベーター (55%) の分布にはピークがあり、オープンソース ソフトウェアに大きく依存していることが示されています。SBOMイノベーターは、オープン

図8

How dependent is your organization on open source software?

Single Response | Segmented by SBOM maturity | N = 341



ソース ソフトウェアに完全に依存していると主張する回答者の割合が27%である唯一のセグメントです。

ソフトウェア セキュリティに関する主な懸念事項

使用されているソフトウェアのセキュリティに関する懸念は、サンプル全体でほぼ一致していました。図9は、サンプル全体の91%が、組織が使用するソフトウェアのセキュリティに関心を持っているか、非常に関心があるか、または非常に関心があることを示しています。わずかに懸念していた企業の8%を加えると、全体の99%になります。

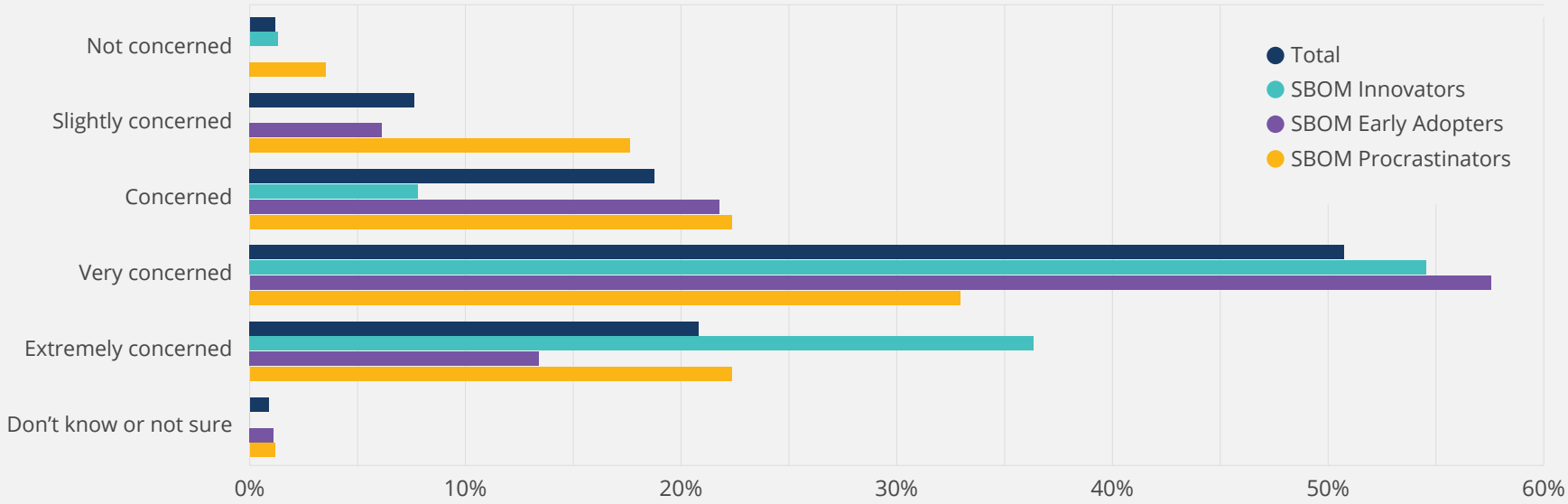
図9もSBOMの成熟度によっても区分されていますが、分布の比較にはいくつかの違いがありますが、驚いたことに、SBOMの管理者の18%はソフトウェアのセキュリティにわずかに関心があり、4%は関心がありませんでした。ソフトウェア セキュリティに若干の懸念を抱いているSBOMプロセスの18%は、1～99人の従業員と100万ドル100万ドル未満の企業によって特徴づけられます。これらの企業は生き残りと成長に重点を置いており、まだソフトウェア セキュリティを優先する立場にはありません。

SBOMの成熟度は、ソフトウェア セキュリティに関する懸念とよく相関しています。セグメント全体を比較すると、SBOMイノベーターの99%が、ソフトウェア セキュリティに対して非常に懸念しているか、非常に懸念しているか、あるいは懸念していたのに対して、SBOMアーリー アダプターは93%、SBOM慎重派は77%にすぎません。結局のところ、ソフトウェア セキュリティが依然として重要な問題であるという点では共通しています。

図9

How concerned is your organization about the security of the software that it uses?

Single Response | **Segmented by SBOM maturity** | **N = 341**



企業がソフトウェア セキュリティに関心を持つ理由

では、なぜ組織はソフトウェア セキュリティに関心を持つのでしょうか？**図10**は全体として、サンプルの66%が財務リスク、61%が風評リスク、53%が法的リスク、40%がお客様のシステムへの不正アクセス、31%がシステムへの不正アクセスを懸念していることを示しています。

この結果に、SBOM成熟度別セグメンテーションを加えて、分かりやすいように色分けしました。ほとんどのセグメントの回答は、サンプル全体とほぼ同じでしたが、2つの顕著な例外があります。

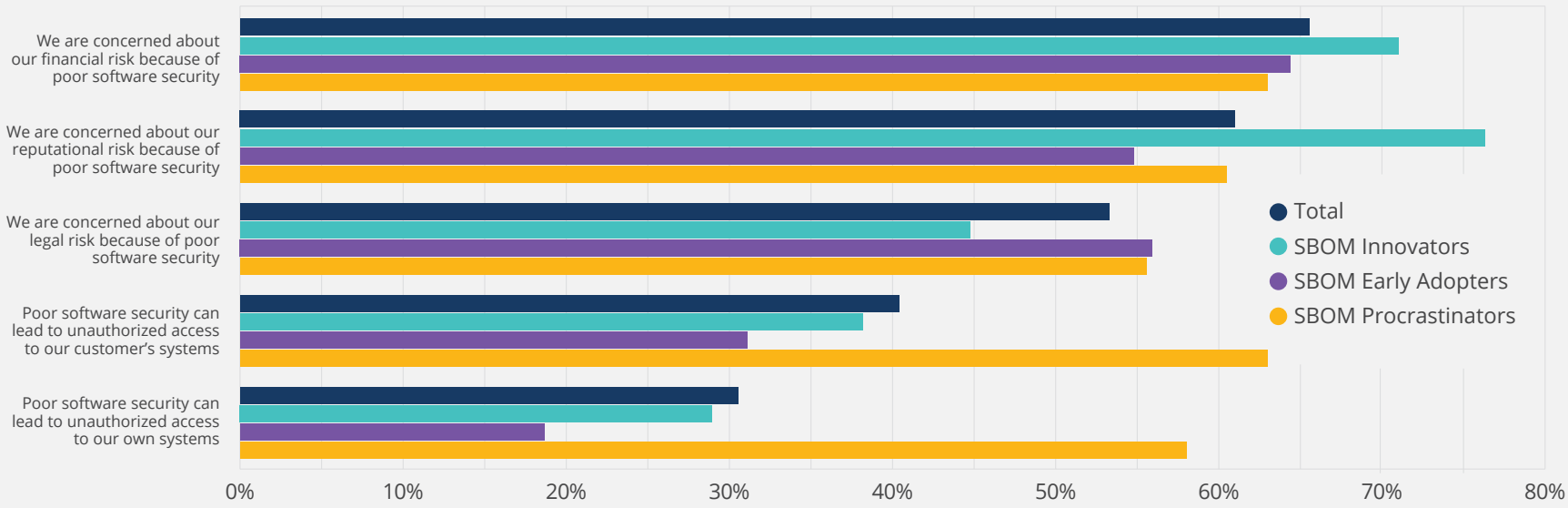
1つは、SBOMイノベーターは、財務リスク（71%）、特に評判リスク（76%）について、全体のサンプルよりも高い懸念を持ち、その他の問題についての懸念はわずかに低いということです。SBOMのイノベーターは、ソフトウェア セキュリティの経験が長いため、不正アクセスや法的リスクなどの一次的な問題にはほぼ対処してきたと思われます。しかし、財務リスクと風評リスクは、より複雑なソリューションを必要とする二次的なセキュリティ上の懸念です。

もう1つの例外は、SBOM慎重派は、お客様のシステム（63%）またはお客様自身のシステム（58%）への不正アクセスを非常に懸念していることです。これらの一次的なセキュリティ上の懸念は、SBOMイノベーターやアーリー アダプターに対しては、それほど大きな不安を引き起こしません。おそらく、これらの問題はすでに大部分が対処されているためでしょう。

図10

Why is your organization concerned about software security?

Select all that apply | Segmented by SBOM maturity | N = 334, Valid Cases = 334, Total Mentions = 840



サイバーセキュリティとSBOMの推進力

2021年5月12日、バイデン大統領による「国家のサイバーセキュリティの改善に関する大統領令」は、サイバーセキュリティ要件に関する規則とガイダンスを策定するための厳しい時間枠を定めました。大統領令の要件は、国家電気通信情報局（NTIA）がSBOMの最低要件を公表することでした。商務省はNTIAと協力して、2021年7月にSBOMの最低要件を発表しました。「Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations」と題する本報告書の第2次草案は、2021年10月にNISTによって公表されました。これらの文書は、米国政府がソフトウェア サプライチェーンのセキュリティをどのように改善しようとしているのかを示すものです。[6] [7]

NTIAの出版物では、SBOMを「ソフトウェアの構築に使用される様々なコンポーネントの詳細とサプライチェーンの関係を含む正式な記録」と定義しています。本文書はさらに、SBOMの価値提案を次のように説明しています。「SBOMは、ソフトウェアを開発、購入、運用する人々に、サプライチェーンの理解を深めるための情報を提供します。これにより、複数のメリット、特に、新たに発生した脆弱性やリスクを追跡できるようになります。SBOMはすべてのソフトウェア セキュリティ問題を解決するわけではありませんが、セキュリティ ツール、プラクティス、保証を構築するための基盤となるデータ層を形成します」。NTIA文書およびNIST文書の付録Fは、SBOMに関与している、または関与する予定のベンダーおよびエンドユーザー企業にとって必読と言えるでしょう。

サイバーセキュリティに関する大統領令は、SBOM市場の行動をうながすきっかけとなるでしょう。マーケットという言葉は少し時期尚早かもしれませんが、SBOMに精通していることと、SBOMをフォーマットするためのISO標準と相まって、SBOMツールの需要を生み出しています。

大企業は中小企業よりも得るものが多く、失うものも大きい。また、中小企業の規模とIT優先順位では、SBOMはあれば良いもの、後でも構わないものとなっている。

米国サイバーセキュリティ行政命令の認識と行動

米国の行政命令は、サイバーセキュリティに対する意識を高め、ソフトウェア セキュリティを向上させるための製品、プロセス、ベストプラクティスの開発と使用を加速することを目的としています。この行政命令の影響を理解するために、組織の認知度について質問し、さらにこの大統領令の結果としての変化についても質問しました。図11に示すように、全体として、大統領令を認識していたのは84%、認識していないのが11%、そして5%が分からないと回答しています。図示はしませんが、大統領令に対する認知度は地域によって異なっていました。アメリカ大陸での認知度は86%、EMEAが79%、そしてアジア太平洋地域が64%でした。

図11は、SBOM成熟度別の大統領令の認知度も示しています。当然ながら、SBOMイノベーターが97%と最も高く、次いでSBOMアーリー アダプターが91%、SBOM慎重派が56%でした。

意識改革は大前提です。図12に示すように、77%の企業が大統領令に対応した変更を検討していますが、13%は検討しておらず、6%が未回答、4%が分からないと回答しました。**図12**のSBOM成熟度によるセグメンテーションでは、大統領令に対応した変更を検討しているグループ間で有意な差は確認されませんでした。

しかし、**図11**に示された高い認識度と、**図12**に示された変更を検討している77%を考え合わせると、大統領令が、官民を問わず、サイバーセキュリティの改善を促すという意図された結果に結びついていることがうかがえます。

サイバーセキュリティとソフトウェア サプライチェーンの優先事項としてSBOMを重要視

ソフトウェア サプライチェーンを保護するための主要な活動として、SBOMは幅広いニーズに対応します。**図13**は、全体の47%が、サプライチェーンを保護するための主要な活動として、脆弱性報告システムを位置づけていることを示しています。現在、オープンソース ソフトウェアの脆弱性とライセンス コンプライアンスを特定するには、SCAツールが推奨されています。SBOMには依存関係を特定する能力があり、最終的には既知の脆弱性に関する情報を含めることができます。しかし、脆弱性に関する課題は、どの脆弱性が利用可能であるかを理解し、この情報を最新の状態に保つ方法を理解することです。SBOMはまだ脆弱性の識別をサポートしていませんが、いずれそうなることになるでしょう。

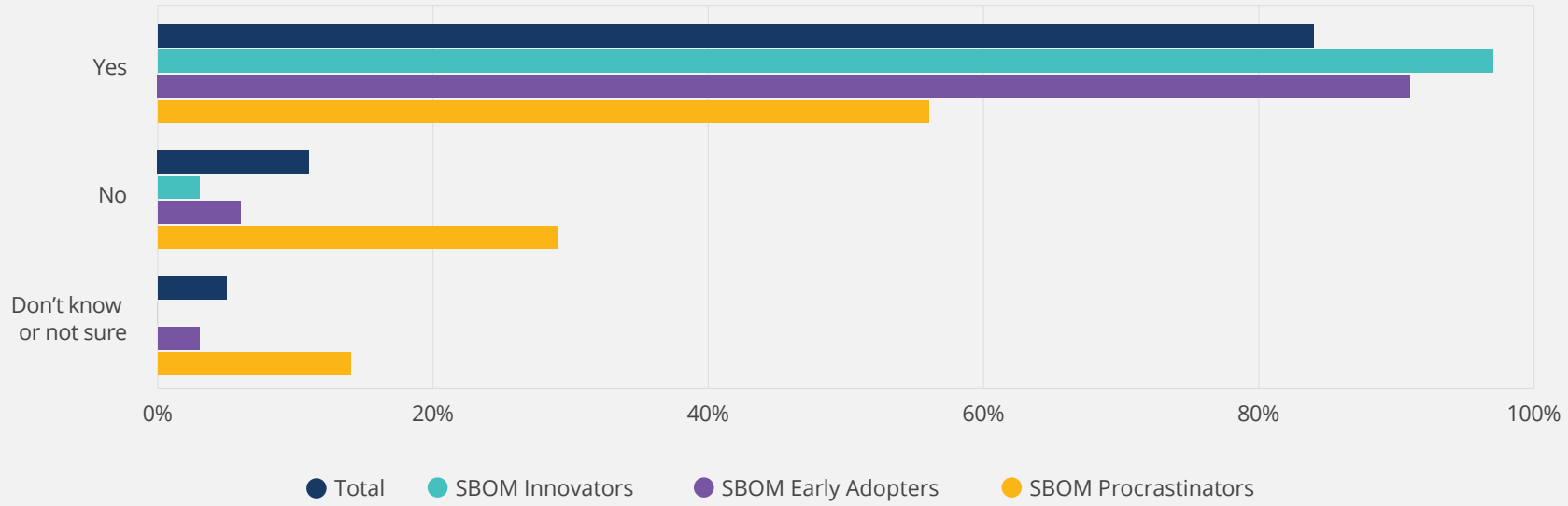
図13の全体的な所見は、SBOMがソフトウェア サプライチェーンのセキュリティを可能にするための不可欠な方法であると認識されているということです。SBOMイノベーターは、SBOMの重要性を納得のいく形で伝え、SBOMを使用した経験によって、SBOMの価値を信頼できる形で確認することができました。

ソフトウェア サプライチェーンを保護するための活動として、「SBOMの利用」が第2位となっています。全体的に見ると、回答者の45%がSBOMを

図11

Is your organization aware of the recent US Executive Order on Cybersecurity that mentions a software bill of materials?

Single Response | Segmented by SBOM maturity | N = 341



特定しており、その中にはSBOMイノベーターの65%、SBOMアーリー アダプターの39%、SBOM慎重派の37%が含まれています。これはSBOMを強く支持するものであり、コンポーネントの出所、ライセンス、依存関係を定義し、暗号化情報を提供するSBOMの能力によって推進されています。

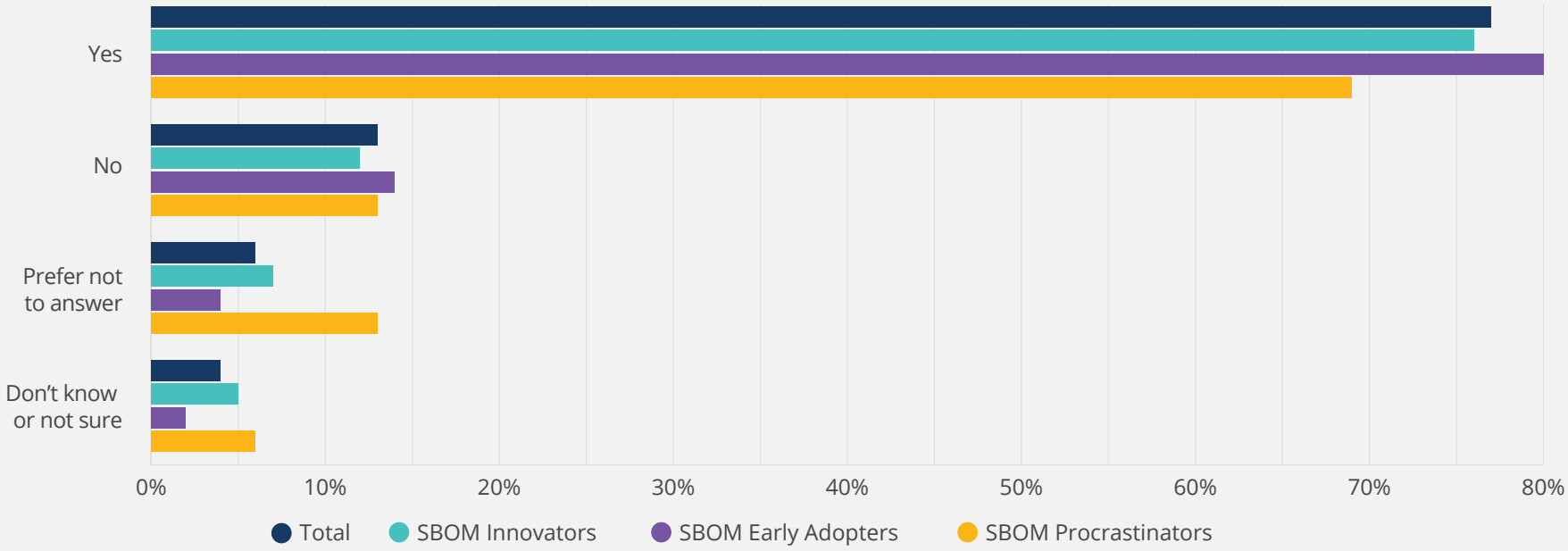
2要素認証（2 FA）は、**図13**で第3位にランクされ、サンプルの42%が認知しています。2 FAはセキュリティを改善するための十分に確立された技術ですが、頻繁に目にするセキュリティ侵害が続いていることは、2 FAが常に遵守されているわけではないことを意味します。2 FAはベストプラクティスであり、簡単に実装できるのに、それほど生かされていないのは残念なことです。

メモリ安全なプログラミング言語の使用は、サンプルの40%で確認されているように、ソフトウェア サプライチェーンを保護するための非常に重要な方法です。Rust、Go、Java、C#、Swift、JavaScript、Pythonなどの新しい言語のほとんどは、メモリ安全です。このリストに含まれていないのは、CとC++です。MicrosoftやGoogleを含むベンダーは、見つかった脆弱性の大半がメモリの安全性の問題であると報告しています。これらの脆弱性は、攻撃者がアプリケーションやオペレーティング システムを不正利用するための簡単な経路となります。

図12

Is your organization considering any changes in response to the US Executive Order on cybersecurity?

Single Response | Segmented by SBOM maturity | N = 285



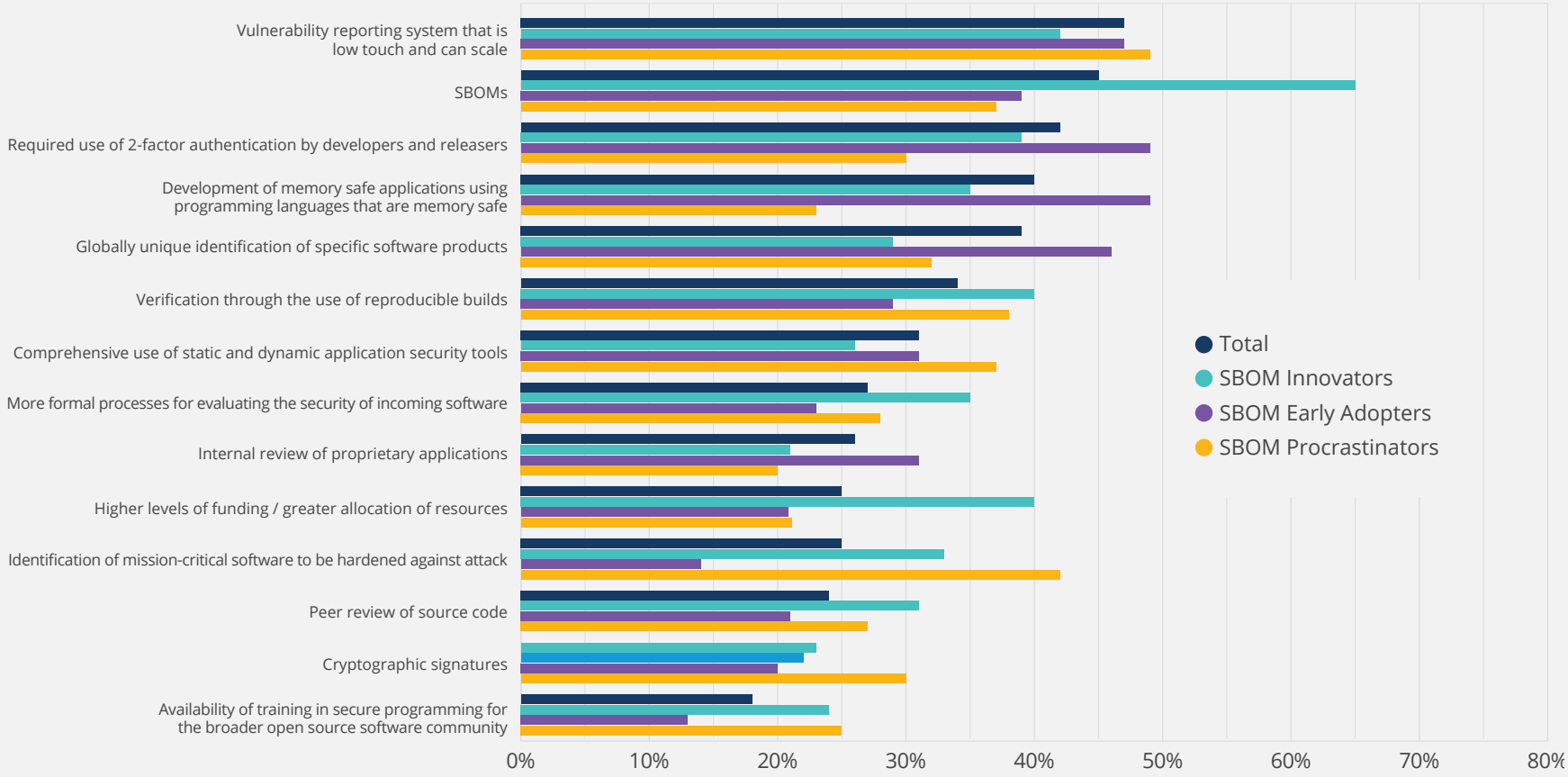
また、グローバルに一意な識別子（39%）、再現可能なビルドの使用による検証（34%）、および暗号署名（23%）は、今日SBOMを使用するときにすべて達成可能な機能であることにも言及する必要があります。

このように多様な機能があるため、SBOMは非常に魅力的なのです。

図13

What do you think are the key activities for securing the software supply chain?

Select all that apply | Segmented by SBOM maturity | N = 316, Valid Cases = 316, Total Mentions = 1,416



SBOMのニーズ

以下の6つの数値（14〜19）の枠組みは、NTIAから提供されたものです。これらの図は、SBOMのためのNTIAマルチステークホルダー プロセスから生まれた6つの主要な側面と決定点を強調しています。

各図の凡例には3つの側面が含まれています: [8]

- 業界の採用時期と従来のプロセス/テクノロジーに対応する**代替手段**
- 現代の開発プロセスで今日可能なことについての**最初のコンセンサス**
- 新たに発生した高保証のユースケースの**拡張**

NTIAは、ベースライン コンポーネント情報を以下のように定義しています。

「SBOMの主な目的は、コンポーネントとその相互関係を一意的かつ明確に識別することです。そのためには、ベースラインコンポーネント情報のいくつかの組み合わせが必要です。特定の属性は、SBOMエントリでより多くのベースライン属性を持つのと同様に、より大きな一意性または非曖昧性を提供します。[9]」

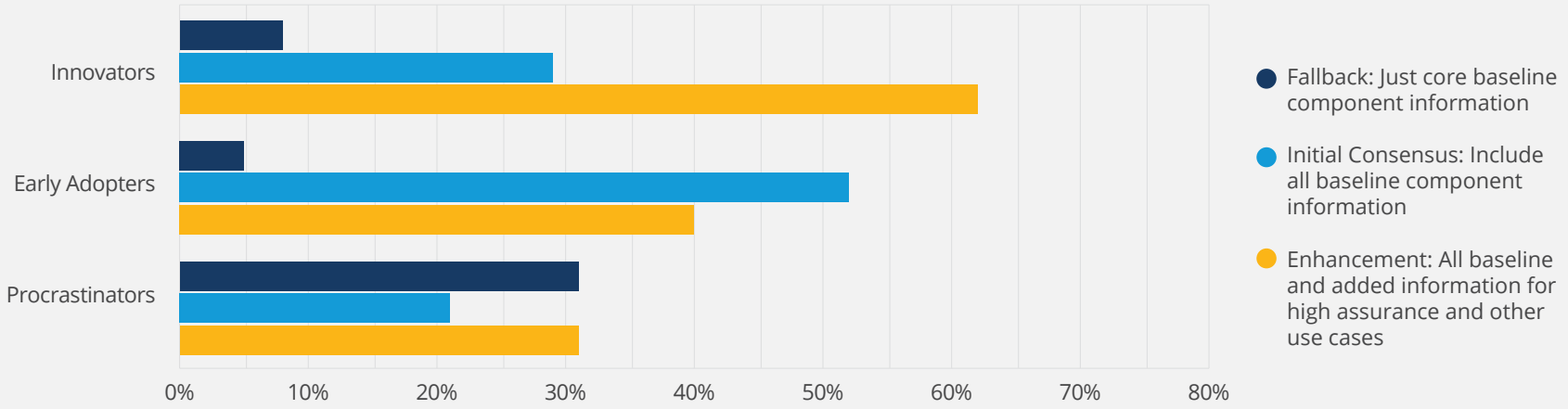
SBOMにメタデータの豊富さを求める組織

図14とそれに続く5つの図は、SBOMの重要な側面を説明しており、どのレベルの機能が必要か（フォールバック、初期コンセンサス、または拡張）についてユーザーからのフィードバックを提供しています。図14は、SBOM成熟度別に区分されたベースラインコンポーネント情報の好ましいレベルを示している。図14のSBOMプロセスは、代替計画、コンセンサス計画、拡張計画にわたって比較的均等に分布していることを考慮すると、最も意見の少ないセグメントです。SBOMアーリー アダプターは52%で当初の

図14

What level of SBOM baseline component information do you currently need?

N = 356



コンセンサス計画を中心に融合しているが、40%は強化計画に関心を持っています。SBOMのイノベーターは62%で強化計画に引き寄せられており、他の計画に対するセグメントの残りの反応を矮小化しています。強化されたベースライン情報への、この強い関心は、暗号ハッシュ情報（オプション）と脆弱性情報（開発中）が提供できる大きな価値によるものであると期待しています。

機械可読性はSBOMの重要な要件

図15は、SBOMのフォーマットとマージ マシンの可読性が、どのレベルまで必要かを定義しています。SBOM慎重派は、ここでも比較的均等に分布していますが、最初の合意計画が33%というのは、SBOMアーリー アダプター（60%）とSBOMイノベーター（60%）の主要な選択と一致しているので際立っています。ベースライン情報が主要なSBOMフォーマットのそれぞれで機械読み取り可能であることを要求する初期の合意計画は、明らかに計画の中で最も実用的です。代替計画は、CSVが過度に単純であることを意味し、拡張計画は、SBOM空間の標準が急速かつ大幅に変化しているため、必要とされない、または容易にサポートされない可能性のある高いレベルの複雑さを生み出します。

SBOMは関連する依存関係をすべて明確にすべき（「未知」であることを含め）

図16は、ユーザーが必要とするコンポーネントの依存関係の深さを評価しています。SBOM慎重派の65%、SBOMアーリー アダプターの40%、SBOMイノベーターの49%が強く望んでいることから、最初のコンセンサス計画が有力な候補であると思われます。最初の合意計画の魅力は、依存関係がどのように識別されるかにインテリジェンスの層を組み込む、推移的な依存関係をサポートしていることです。強化計画はSBOMイノベーターたちにやや好まれているが、未知のものをどのように宣言できないかを決定するには課題があります。

図15

What level of SBOM format and machine readability do you currently need?

N = 355

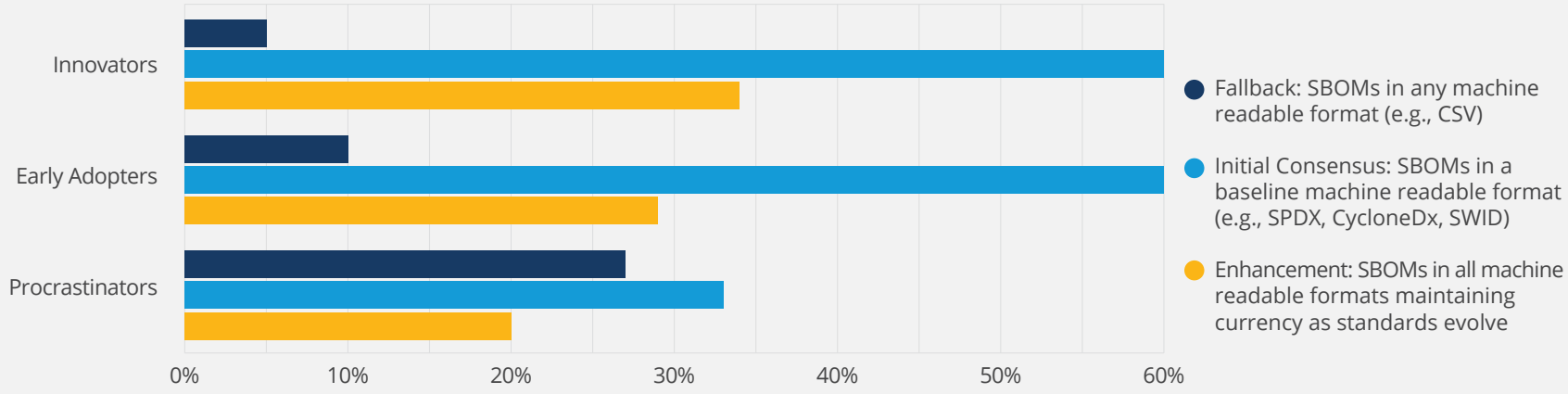


図16

What level of SBOM depth of dependencies do you currently need?

N = 355

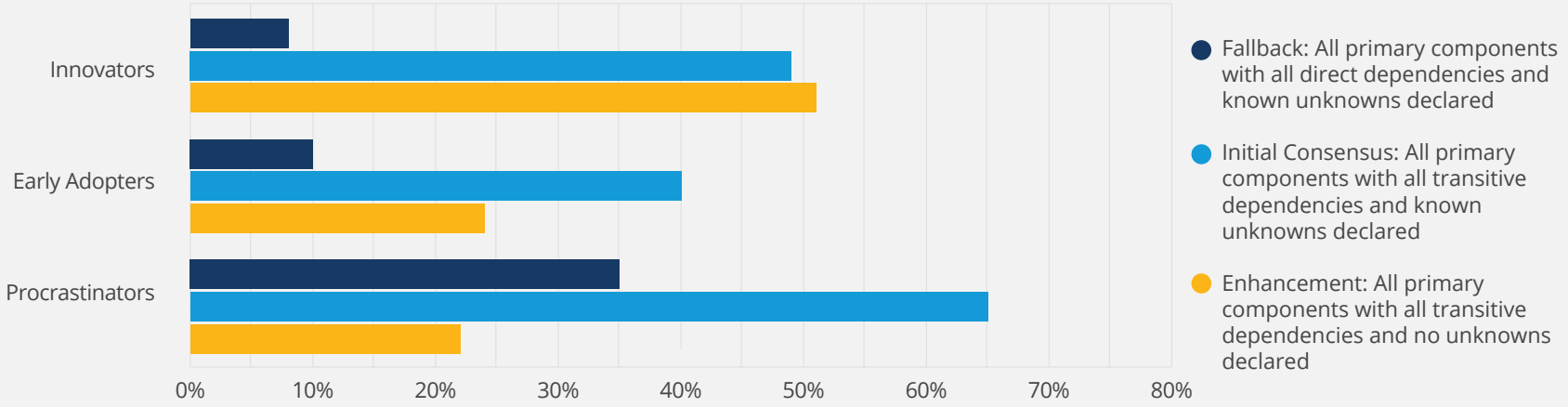
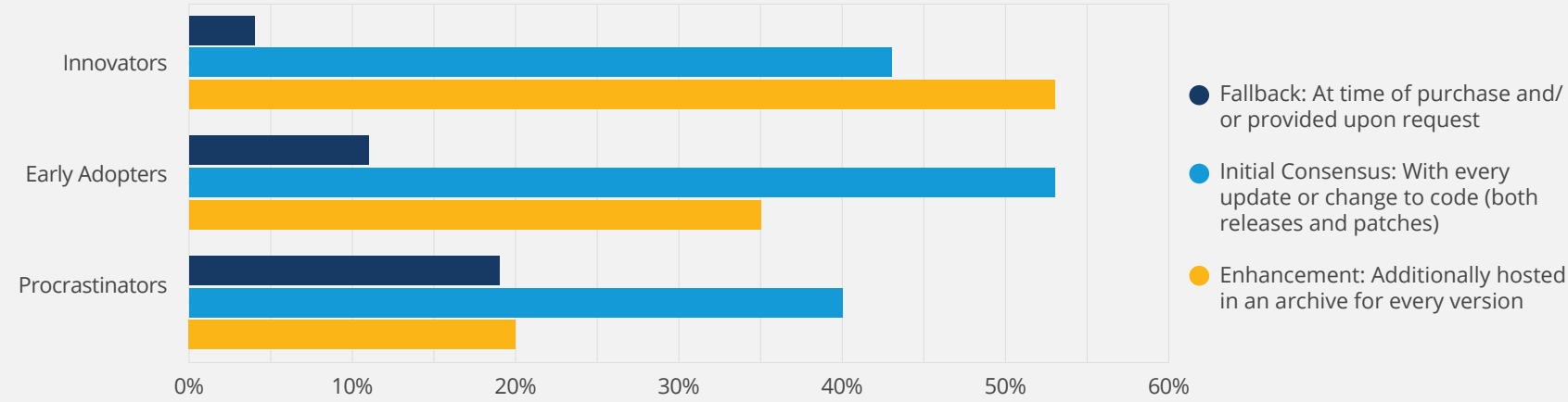


図17

What level of SBOM generation frequency do you currently need?

N = 353



コード変更ごとにSBOMを更新する必要がある

図17は、必要なSBOM生成頻度のレベルを示しています。SBOM慎重派（40%）とアーリー アダプター（53%）は、いずれも当初のコンセンサス計画を強く支持しています。SBOMイノベーターは計画の選択に関して意見が分かれており、43%が最初のコンセンサス計画を、53%が強化計画を支持しています。初期コンセンサス計画は、コンポーネントの更新または変更ごとにSBOMを生成するため、フォールバック計画よりもはるかに有用です。ただし、拡張計画では、すべてのバージョンのアーカイブのサポートを追加で提供することにより、アクセスが向上し、異常を調査する際に貴重な履歴コンテキストが提供されます。

SBOMメタデータはコンポーネントにバンドルする必要がある

図18は、ユーザーが必要とするSBOM配布能力と相互運用性のレベルを示しています。初期の合意計画は、SBOM慎重派の45%、SBOMアーリーアダプターの51%、SBOMイノベーターの42%を含む大多数のユーザーによって相対的に好まれています。しかし、この強化計画は、SBOMのアーリー アダプターの43%とSBOMイノベーターの42%から大きな支持を受けています。コンセンサス計画と拡張計画の違いは、自動化、拡張性、相互運用性のために提供されるサポートです。M2M通信によって促進されたAPIアクセスと相互運用性のための拡張計画の提供は、SBOMの使用を大幅に加速し、簡素化します。しかし、コンセンサス計画はある程度の自動化をサポートしているので、それは強化計画への道のりの有用な一時的な足がかりと見なすことができます。

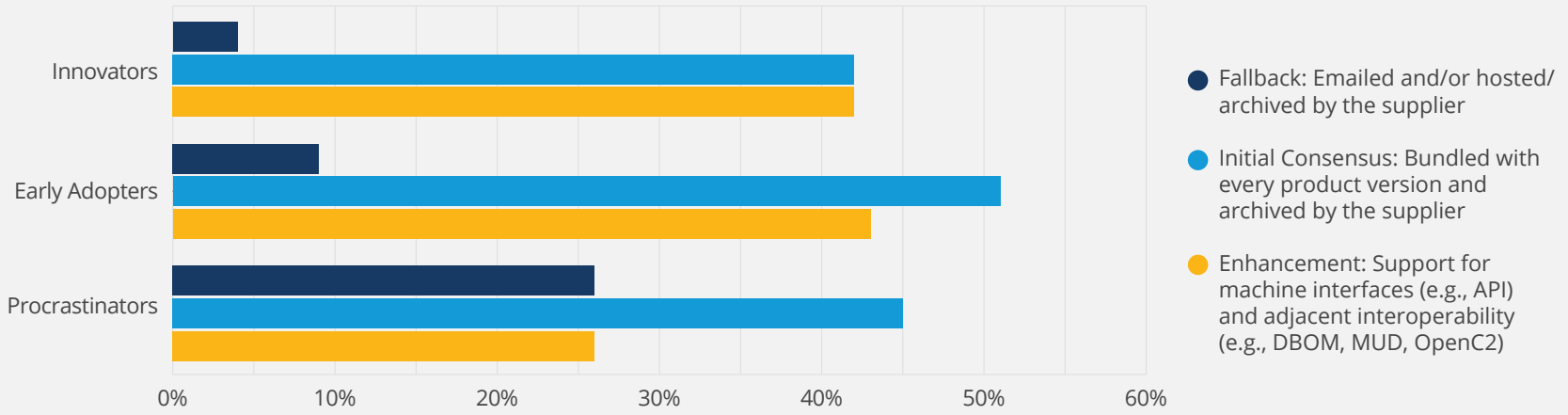
脆弱性が発見された場合、脆弱性を反映する必要がある

脆弱性情報を活用するために必要なアクセスと統合のレベルを図19に示します。最初の合意計画と強化計画は、どちらもSBOMユーザーにとって同じように魅力的です。これらのプランのサプライヤーは、脆弱性データをリアルタイムで消費者にプッシュしているため、これは心強いことです。フォールバック計画にはそのような規定はなく、脆弱性を理解するには非常に非効率的なプロセスで、消費者をリスクにさらすことになります。

図18

What level of SBOM deliverability and interoperability do you currently need?

N = 353



SBOM準備とSBOM成熟度によるセグメンテーション

調査データの重要なセグメント化はSBOM即応性によるものでした。質問は「あなたのグループの現在のSBOM準備状況はどうなっていますか?」でした。この質問は、SBOMとは何かの定義を提供した後に行われたもので、調査の最初の質問であり、回答者に対して、彼らが作業するグループまたはビジネスユニットで発生しているSBOMアクションについて直接質問しました。SBOMの作成と使用の状況に特化した質問とは異なり、この質問はより広い範囲を対象とし、サンプルをセグメント化するための基礎資料として価値があります。

質問は、「知らない」(Don't know)と「よく分からない」(not sure)を除く、8つの回答がありました。図20は、サンプルの組織全体で、90%の組織がSBOMへの移行を開始していることを示しています。10%の組織がSBOMの計画を開始しておらず、14%が計画または開発フェーズにあり、52%がビジネスのいくつか、または多くの領域でSBOMに対応しており、23%がビジネスのほぼすべての領域でSBOMに対応しているか、SBOMの使用を含む標準的なプラクティスを持っています。これは、全体として76%の組織がSBOMの準備状況を把握していることを意味します。

図20は、全体的な回答(合計)と、これらの回答をSBOMイノベーター、SBOMアーリー アダプター、SBOMプログレッサの3つのカテゴリーにマッピングした方法を示しています。

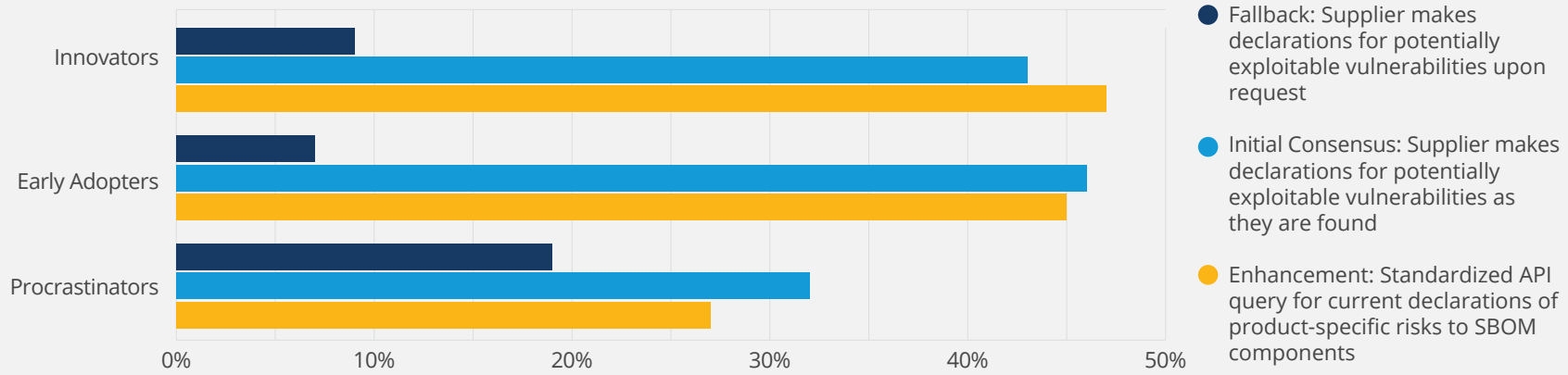
カテゴリSBOM慎重派には、SBOMへの対応を開始していない回答者、SBOMへの対応を計画している回答者、またはSBOMへの対応を開始している回答者が含まれます。SBOM慎重派は回答者全体の24%を占め、SBOM慎重派の58%がSBOMサポートへの対応を計画しているか、または対応を開始しています。SBOMプロセスの41%(サンプル全体の10%)がSBOMへの移行を開始していません。

カテゴリーSBOMアーリー アダプターには、事業の一部にわたってSBOMの作成または使用に取り組んできた組織と回答者が含まれます。全サンプルの53%がこのカテゴリーに分類される。SBOMのアーリー アダプターのうち、29%がビジネスのいくつかのセグメントでSBOMに取り組んでおり、42%がいくつかのセグメントで、28%が多くのセグメントでSBOMに取り組んでいます。

図19

What level of SBOM-adjacent enhancement for vulnerability claims do you currently need?

N = 353



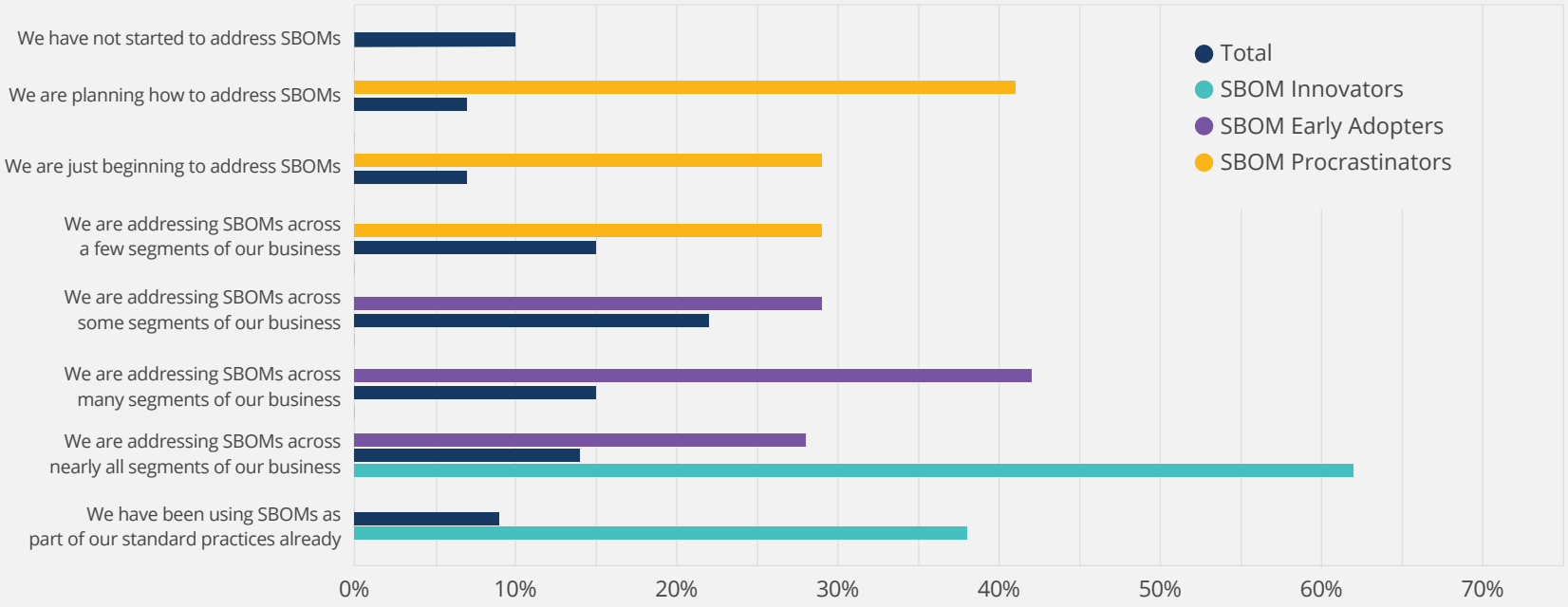
SBOMイノベーターは、SBOMの使用に深く関与し、経験を積んでいる組織に限定されたカテゴリーです。SBOMイノベーターは全サンプルの23%を占めており、SBOMイノベーターのうち、62%がほぼすべての事業分野でSBOMに取り組んでおり、38%がSBOMを使用するための標準的なプラクティスを有しています。

SBOMの準備状況に基づいてこのビューを構成することの利点は、調査で他の変数と相互に関連付けられた場合、これらの3つのセグメント（SBOM慎重派、SBOMアーリー アダプター、SBOMイノベーター）のそれぞれに関連する優先順位とアクションについての洞察を得ることができることです。SBOMの成熟度レベルに基づいて、これらの優先順位とアクションがどのように変化するかを調べることによって、組織がSBOMをどのように採用しているかについても洞察することができます。

図20

What is your group's current SBOM readiness?

Single Response | **Segmented by SBOM maturity** | **N = 341**



SBOM作成の視点

以前の調査では、SBOMの認知度とSBOMへの対応について質問しました。これは主に、回答者に彼らの組織がSBOMを使用していることについて考えてもらうために行われました。SBOM調査の後半では、SBOMの作成と使用における組織の関与についてさまざまな質問をしました。これらの質問には、現在または計画中のSBOM契約に対するより正確なコミットメントが必要でした。

SBOMの作成は、商用ソフトウェアを作成する組織に最も関連性があります。これは、規制当局と顧客がこの情報を要求するためです。しかし、内部使用を目的としたソフトウェアも、セキュリティと保守性を向上させるために、SBOMの恩恵を受けることになります。

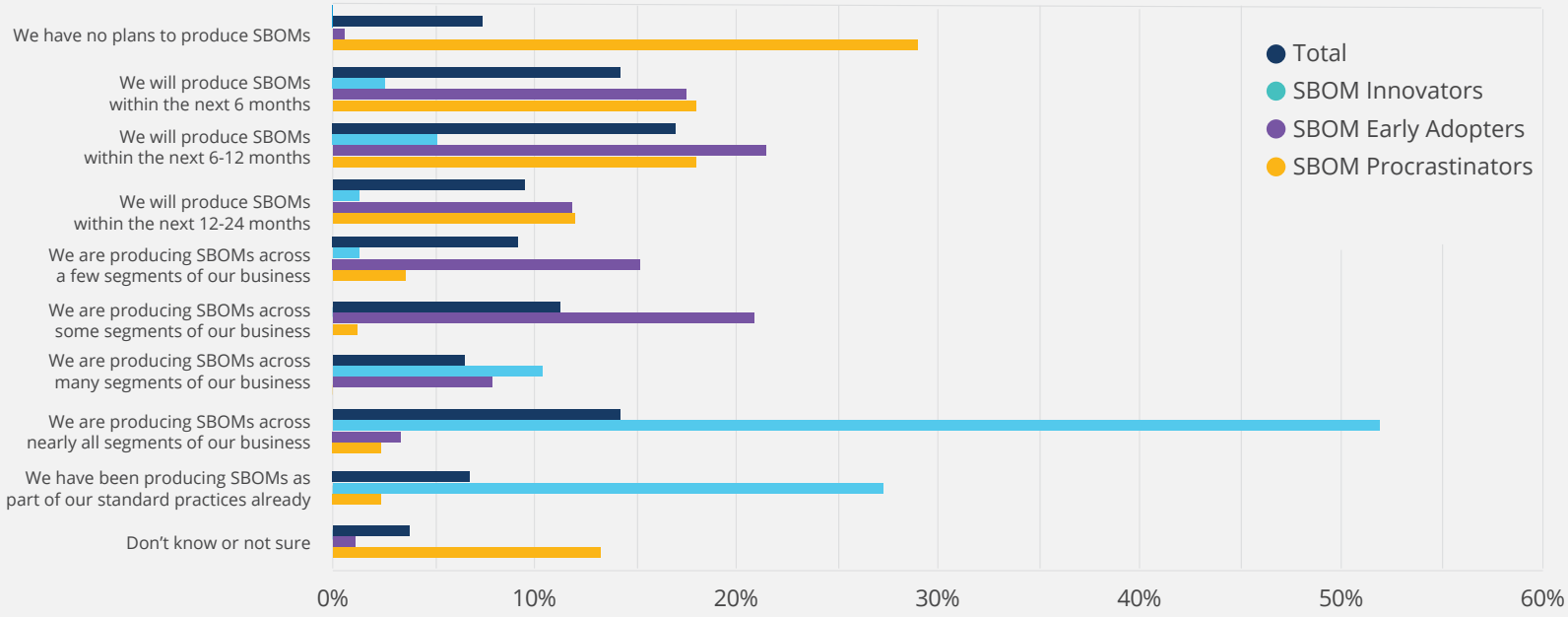
SBOM作成

SBOM即応性分布の全体的な結果（**図20**）をSBOMを作成するための組織計画（**図21**）と比較すると、組織はSBOM即応性が示すほどには進んでいないことがわかります。図21は、サンプル全体の40%がSBOM計画フェーズにあることを示しています（今後6〜24カ月でSBOMを作成する予定)。 これは、SBOM準備計画/開始フェーズの14%を大幅に上回っています。

図21

What are your organization's plans for producing SBOMs?

Single Response | **Segmented by SBOM maturity** | **N = 337**



同様に、全体のサンプルの20%は、彼らのビジネスのいくつかのセグメントでSBOMを作成していると言っており、これは、彼らがいくつかのセグメントでSBOMに取り組んでいると主張した38%よりはるかに少ないです。彼らのビジネスの多くまたはほとんどすべてのセグメントでSBOMを作成しているのは21%ですが、SBOM準備の質問での29%と比べると、その差は少し縮まっています。

SBOM準備とSBOM作成の間の全体的な差異は、現在SBOMを作成している組織では27%の削減（67%から49%へ）、SBOMの提供を計画している組織では66%の増加（24%から40%へ）になります。SBOMの移動を開始していない組織、不明な組織、または質問への回答方法を知らない組織には、重要な変更はありません。

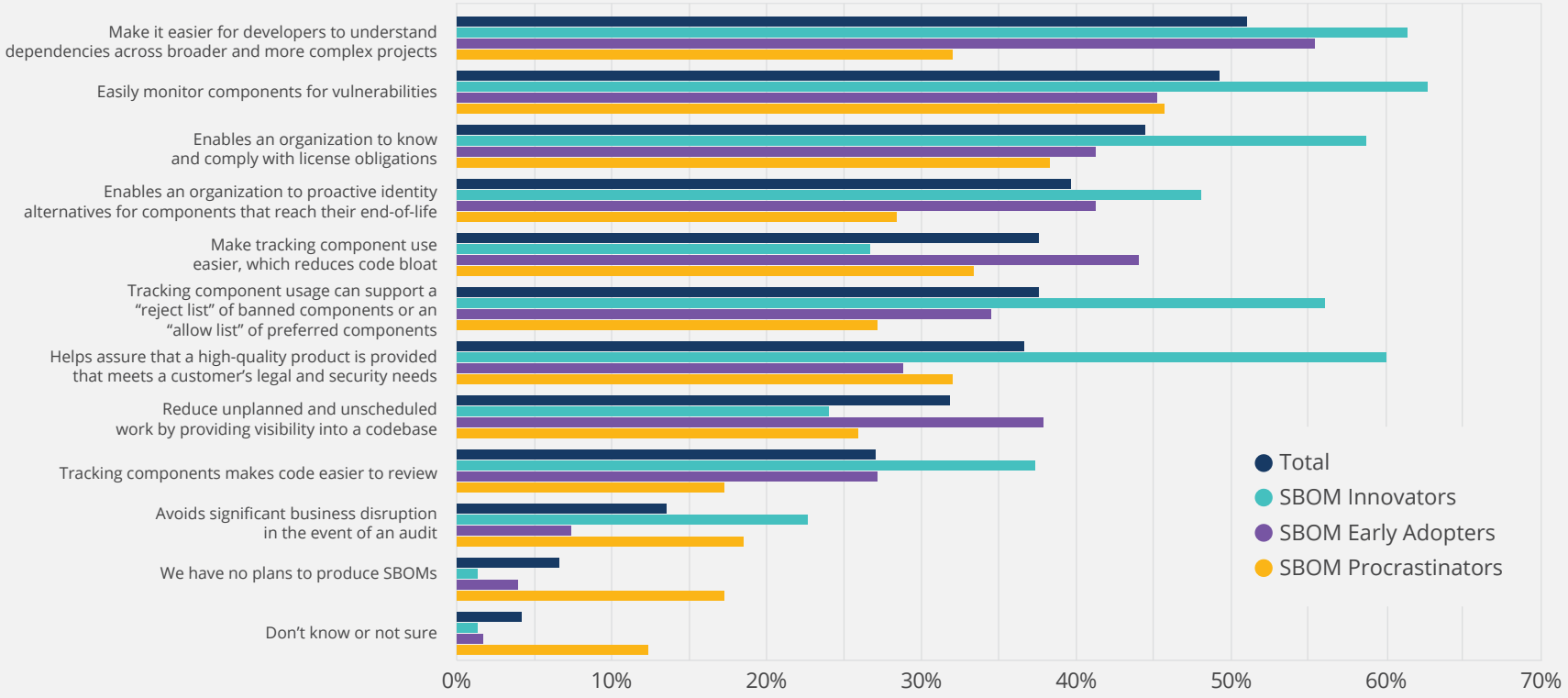
SBOM作成特典

サンプルの49%の組織がすでにSBOMを作成しており、40%が計画段階にあることを考えると、これらの組織はSBOMの関与からメリットを得ています。図22は、ユーザーがSBOMを作成することによって実現すると期待している利点を示しています。全体として、51%の組織が、SBOMによって開発者がより広範で複雑なプロジェクト間の依存関係を理解しやすくなると報告しています。マイクロサービス アプリケーションが多くのコン

図22

What benefits do you expect to realize by producing SBOMs?

Select all that apply | Segmented by SBOM maturity | N = 333, Valid Cases = 333, Total Mentions = 1,263



ポーネントを持つ時代には、通常、各コンポーネントにはいくつかの依存関係があります。SBOMは依存関係の明示的な識別を提供します。これは、アプリケーション内のコンポーネントの複雑さと数が増加するにつれて、ますます有用になります。依存関係の特定は、SBOMイノベーター（61%）とSBOMアーリー アダプター（55%）にとって特に重要でした。依存関係の特定は、強調された2つの最も重要な利点の1つです。

図22は、脆弱性に対するコンポーネントのモニタリングの全体的な重要性も示しています。全体として、組織の49%がこれはメリットであると認識しており、SBOMイノベーターの63%も同様です。脆弱性の監視は、図28の分析で議論したように、非常に進行中の作業です。課題は、新しい脆弱性が発見され、既存の脆弱性が軽減されるにつれて、各コンポーネントの脆弱性のリストが常に変化することです。この情報をコンポーネントのコンシューマーにタイムリーに伝達する方法は、現在進行中の作業です。これはSBOMイノベーターによって特定された主要なメリットであるため、脆弱性モニタリングへの効果的なアプローチは、SBOMに期待される機能です。

オープンソース ソフトウェアの使用が普及している現在、ライセンス コンプライアンスは重要な要件です。図22は、44%の組織がSBOMをライセンス義務を特定し、遵守するための効果的な方法と見なしていることを示しています。SBOMのイノベーターの59%は、ライセンス コンプライアンスの重要性を即座に強調しました。

これらを総合すると、依存関係、脆弱性、およびライセンス コンプライアンスの理解は、SBOMが提供する最も重要な利点となります。

図22はまた、SBOMがどこに向かっているのかを示しています。56%のSBOMイノベーターが、アクセス制御を支援するためのコンポーネント「REJECT AND ALLOW LIST」の概念に関心があります。60%のSBOMイノベーターは、顧客の法的およびセキュリティ上のニーズを満たす高品質な製品の提供を保証する方法として、SBOMの使用にも関心を持っています。

エネルギー製品の世界的な大手サプライヤーが、SBOMへの道のりについて当社と話し合いました。

「SBOMの必要性は、何千もの製品とそれらの製品の何千ものバージョンがあるという事実から始まりました。サードパーティの脆弱性が特定されると、私たちは毎年何千時間もの時間をかけて影響評価を行い、製品の脆弱性を探します。 ... SBOMがあれば、プロジェクト チームの手間が省け、調査にかかる時間も短縮されることがわかりました」

「SBOMの必要性は、何千もの製品とそれらの製品の何千ものバージョンがあるという事実から始まりました。サードパーティの脆弱性が特定されると、私たちは毎年何千時間もの時間をかけて影響評価を行い、製品の脆弱性を探します。それを実行する唯一の方法は、これらの影響評価を製品チームに送ることです。何千もの製品があって、これらの製品チームの中にはもはや存在しないものもあるので、それはかなりの苦闘です。構築したものを調査できる既存のプロジェクト チームがある場合でも、調査には多くの時間がかかります。SBOMがあれば、プロジェクト チームの手間が省け、調査にかかる時間も短縮されることがわかりました」

SBOM作成に関する懸念事項

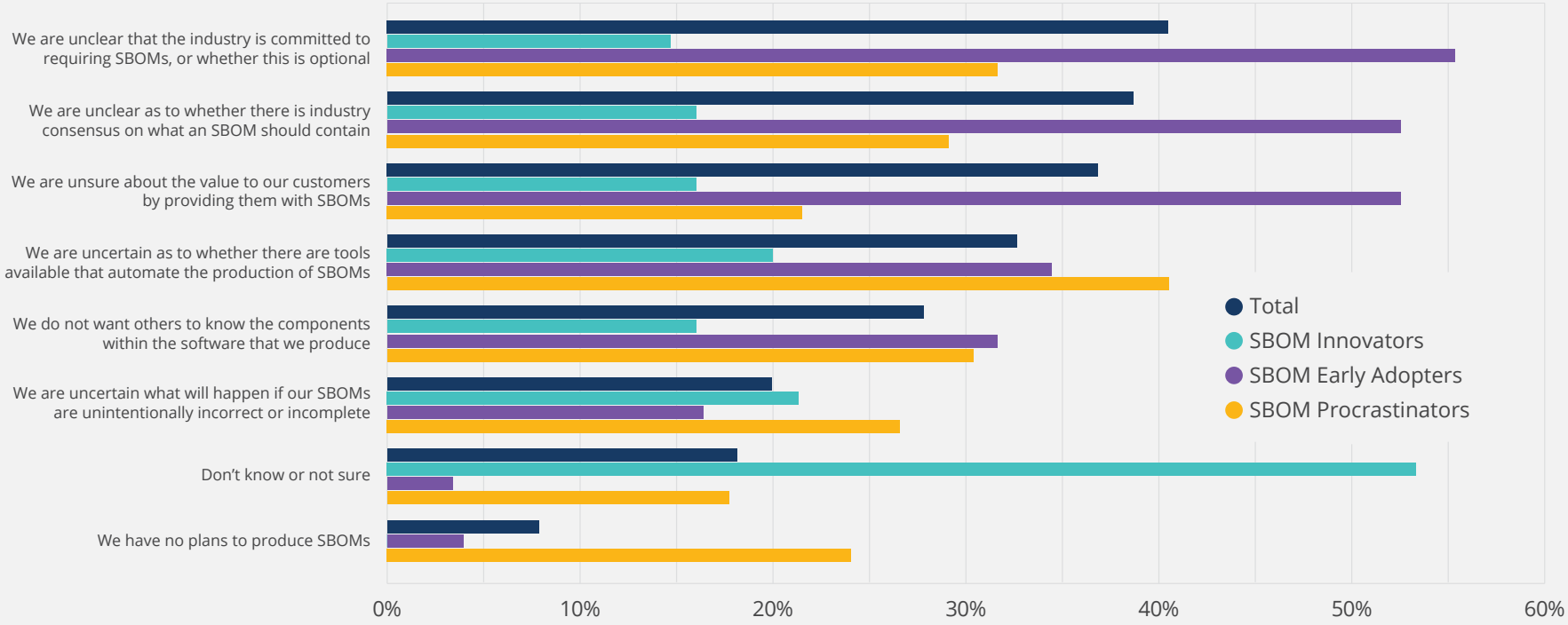
SBOM市場の初期の状況は、SBOMの使用に関する組織の懸念に明確に反映されています。**図23**は、これらの懸念を重要度の高い順に示し、SBOMの成熟度別にデータをセグメント化したものです。上位4つの懸念は、サンプル全体の40%から33%の間で表明されました。

サンプルの40%によって特定された主な懸念事項は、業界がSBOMを要求することにコミットしているかどうかでした。米国食品医薬品局（FDA）は2018年から最初のSBOM市場ガイダンスを提供し、2021年にはFDAは最終的なSBOM市場ガイダンスの提供を優先しました。このガイダンスは、医療機器製造業者に対して、SBOM情報を製品に含めるよう要求することが期待されます。そのため、医療市場ではSBOMが急速に追跡されています。自動車、製造業、エネルギーを含むその他の市場は、それぞれドメイン固有のニーズを持っていますが、医療におけるSBOMコンプライアンスの進化からベストプラクティスを特定し、採用しようとしています。これは、SBOM市場が勢いを増していることを示していますが、主要なソフトウェア ベンダーの関与は限定的であり、主要なベンダーやエンドユーザーがSBOMイニシアティブの実際性に疑問を抱く原因となっています。

図23

What concerns do you have in producing SBOMs?

Select all that apply | **Segmented by SBOM maturity** | **N = 331, Valid Cases = 331, Total Mentions = 736**



第2の重要な懸念事項は、サンプル全体の39%が述べているように、SBOMに何を含めるべきかについて業界のコンセンサスがあるかどうかということです。NTIAは、2021年7月の文書「ソフトウェア部品表の最小構成要素」でこの点に関するガイダンスを提供しています。この文書は、SBOMに何を含めるべきかを定義するのに有用ですが、データフォーマット、実装、プロセスに関する議論は、ベンダーや業界団体の手に委ねられています。SBOMドメイン全体での進展は加速していますが、主要なITベンダーや組織による明確な可視性とメッセージングの欠如が、これらすべての懸念事項の根底にあります。

ベンダーやエンドユーザーは、SBOMを顧客に提供することの価値についても確信が持てませんでした。これはサンプル全体の37%によって表明されました。SBSMが提供する依存関係、脆弱性、およびライセンスの特定という点で明らかな利点があることを考えると、この懸念は長続きしない傾向があります。

最後に、全体のサンプルの33%は、SBOMの作成を自動化するツールの利用可能性については不確実でした。これは妥当な懸念ではありますが、組織のポリシーやDevOpsプロセスの中で対処する必要があります。

これらの懸念を緩和するための効果的なアプローチは、製品開発と製品マーケティング能力の有効性と規模を考慮すると、ITベンダーとサービスプロバイダー コミュニティのサポート レベルを大幅に高めることです。

第2の重要な懸念事項は、サンプル全体の39%が述べているように、SBOMに何を含めるべきかについて業界のコンセンサスがあるかどうかということです。NTIAは、2021年7月の文書「ソフトウェア部品表の最小構成要素」でこの点に関するガイダンスを提供しています。この文書は、SBOMに何を含めるべきかを定義するのに有用ですが、データフォーマット、実装、プロセスに関する議論は、ベンダーや業界団体の手に委ねられています。SBOMドメイン全体での進展は加速していますが、主要なITベンダーや組織による明確な可視性とメッセージングの欠如が、これらすべての懸念事項の根底にあります。

図23はまた、SBOMイノベーターがSBOM作成の問題（15%から21%）に対して、SBOMアーリー アダプター（16%から55%）やSBOM慎重派（22%から41%）よりもはるかに関心が低いというユニークな特徴を示しています。さらに、SBOMイノベーターの「知らない」または「よく分からない」という回答は53%であり、イノベーターは主にSBOMにコミットしており、ほとんどが未知の未知のものに関与していることを示しています。

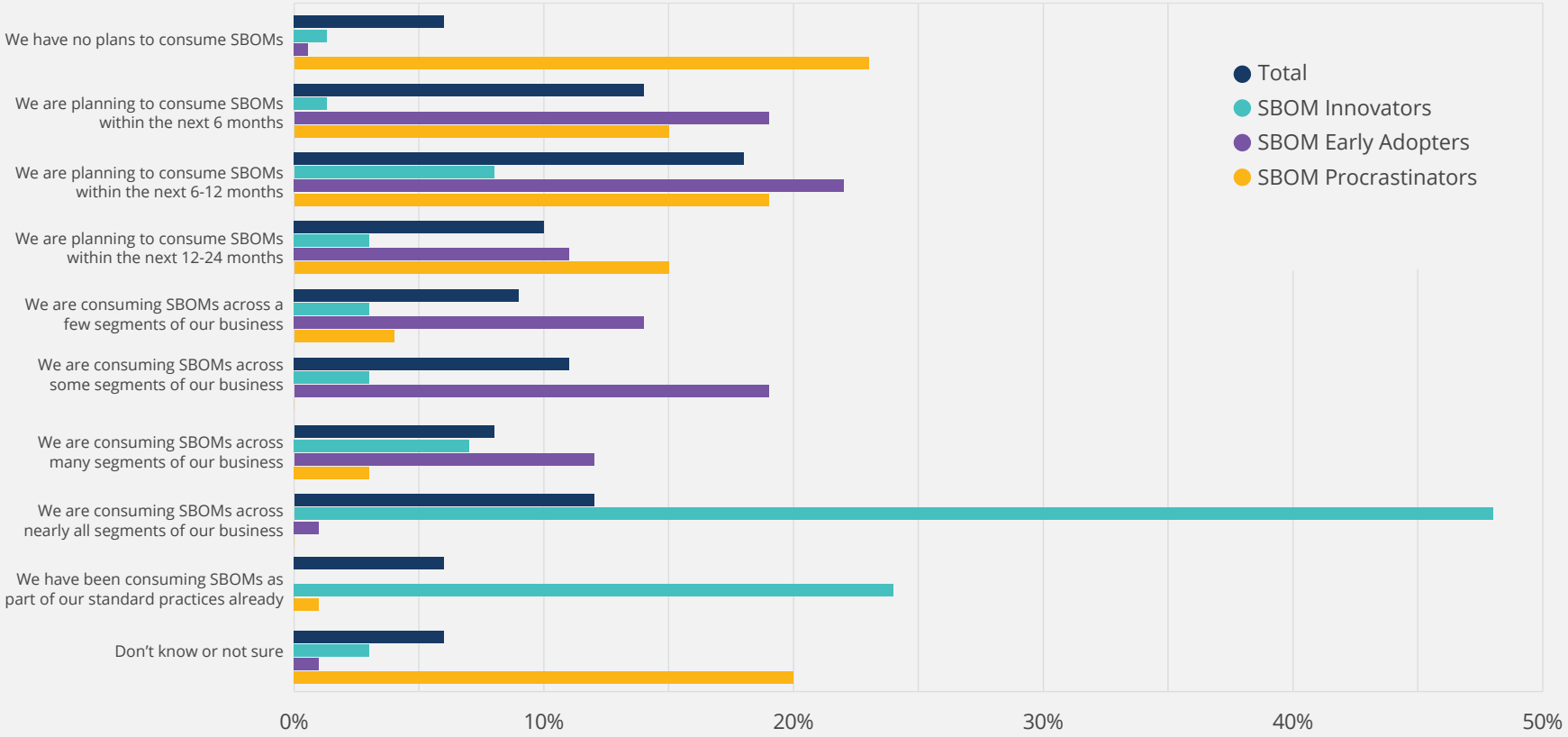
SBOM使用の視点

SBOM使用パターンはSBOM作成パターンとよく一致しています。**図21**（SBOM作成）と**図24**（SBOM使用）のデータの相関は「0.70」となり、強い相関にあることがわかります。これは、回答者がこれらの質問に概ね同じように答えているということを意味しています。これは直感的に理にかなっています。なぜなら、SBOMの作成に関心のあるベンダーやエンドユーザーは、SBOMの上流での使用にも関心があるからです。エンドユーザーはSBOMの使用により関心を持っているかもしれませんが、彼らが作成するソフトウェアのセキュリティと保守性をサポートするために、SBOMの作成にも関心があります。

図24

What plans does your company have for consuming SBOMs?

Single Response | Segmented by SBOM maturity | N = 330



今回お話を伺ったエネルギー製品のグローバル サプライヤーは、SBOMの価値を以下のように要約しました。

「資産所有者の役割を果たす場合、SBOMだけでなく、脆弱性情報、コンポーネントの完全性と整合性を検証する方法も必要になります。そのため、証明書情報を入手し、証明書に付随するハッシュを知る必要があります。」

米国食品医薬品局（FDA）の上級政策アドバイザーは、医療業界におけるSBOMの有用性と重要性について以下のように述べています。

「SBOMは多目的に使えます。私たちはソフトウェアの透明性の観点から始める傾向があります。なぜなら、医療およびヘルスケア部門がある場所には、この情報さえないからです。ごくまれに、必要に応じて自分で情報を探し出すことができるスキルを備えたスタッフが病院にいる場合もあります。しかし、病院の調達担当者は、SBOMやパッケージ マネージャーのリスト、オープンソース ライセンス配布リストなどを調べて、自分たちの環境に持ち込むべきでない危険なソフトウェアがあるかどうかを確認する方法を知りません。彼らにはそのような決定を下すための情報も専門知識もありません。また、誰もこの情報を公開したくないという問題もあります。医療機器メーカーは、状況によっては時代遅れのソフトウェアを使用していることを認めたがりません。だから、彼らは自分たちの製品に何が含まれているかを、必ずしも誰にも話したがらないのです。私たちにとっては透明性から始まります。これらの情報がなければ、簡単に決定を下すことはできず、評価や評価も簡単に行うことはできません。しかし、一度それを手に入れたら、誰もが見ることのできる情報がそこにあり、リスクをはるかに効果的に管理するために、正式な方法でSBOMを使い始めることができます。

また、サイバーセキュリティの脆弱性が他の場所で発生した場合、それは迷惑であるという認識もあります。情報が失われたり、大きな経済的影響が出たりするかもしれないが、人が傷つく可能性は低いでしょう。医療では、サイバーセキュリティの脆弱性が悪用された場合、誰かや多くの人が被害を受ける可能性が非常に高くなります。

現在、病院はより大きな購買力を有しており、基本的にはSBOM要件を契約に盛り込んでいます。病院が装置を購入しようとするとき、彼らは基本的に、SBOMが提供されなければ製品を購入しないと言っています。市場原理がより優先されるようになったのです」と述べた。

SBOM使用

図24は、サンプルの組織のうち、SBOMを使用する計画がない組織は6%のみであることを示しています。次の6カ月から24カ月の間に、サンプルの組織の42%がSBOMの使用を計画しています。これにより、サンプルの40%が本番でSBOMを使用し、6%がSBOMの使用を標準的なプラクティスの一部としました。SBOM成熟度によるセグメンテーションは、SBOMイノベーターがSBOMの大量生産使用を示していることを確認しており、SBOM慎重派はSBOMを使用する計画がないか、SBOM計画フェーズに深く関与しています。

SBOM使用メリット

ベンダーとエンドユーザーは一貫して、SBOMの使用から期待される利益について声をあげていました。図25は、上位5つの利益がサンプル全体の48%から53%の間で確認されたことを示しています。上位2つの利点には、コンプライアンスおよび報告要件をよりよくサポートするコンポーネントに関する情報の提供（53%）と、より多くの情報に基づいたリスクに基づく意思決定を可能にする情報の提供（53%）が含まれます。コンプライアンス、財務、レピュテーション リスクへの対応は、組織がサードパーティ製ソフトウェアを活用する際に考慮する必要がある重要な目標です。

脆弱性のタイムリーな認識（49%）、寿命に達するコンポーネントの積極的な識別（49%）、危険なコンポーネントの認識（48%）の3つの利点はすべて、SBOMによる透明性によって可能になったものです。

これらのメリットは、組織がセキュリティを向上させ、リスクを軽減し、お客様やビジネス・パートナーに対して信頼性の高いサービスを提供するのに役立ちます。

SBOM使用に関する懸念事項

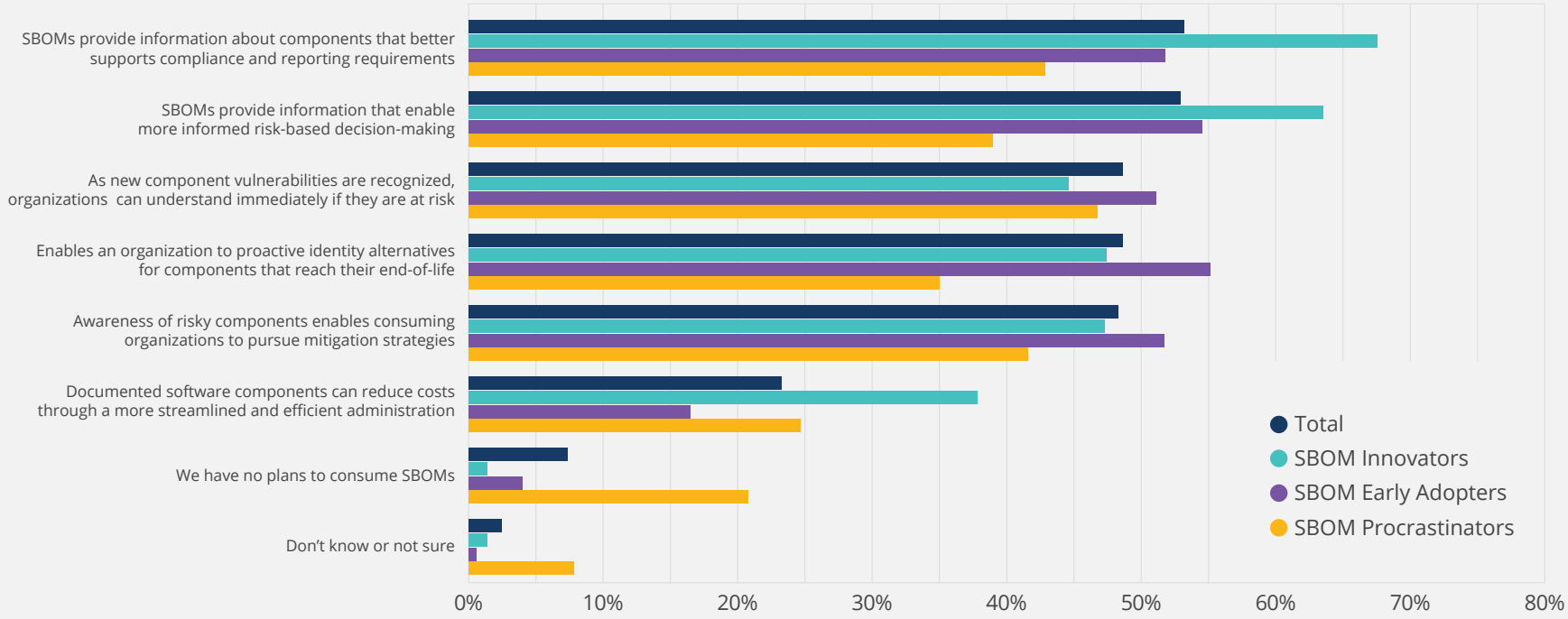
SBOMの作成に関する懸念の調査結果と同様に、SBOMの使用に関する懸念は、主にSBOMのアーリー アダプターとSBOMの慎重派によって表明されています。SBOM sBOMの使用に関する主な懸念事項には、SBOMの業界要件に関する不確実性（49%）、SBOMの使用を自動化するためのツールの利用可能性（48%）、SBOMに含めるべきものに関する業界のコンセンサス（44%）などがあります（**図26**）。

これらは深刻な懸念事項です。SBOMのイノベーターがこれらの問題にあまり関心を持っていなかったことは勇気づけられるものであるが、これは肯定的な兆候であり、サンプルの75%を占めるSBOMのアーリー アダプターや慎重派にSBOMの価値提案を伝えることはほとんどありません。SBOMに対する業界固有の要件についての不確実性を取り除くためには、政府機関、業界団体（業界固有の情報共有分析センターを含む）ITベンダやサービス プロバイダーなどがSBOMの価値提案、ツールの可用性、統合機能、DevOpsプロセス、ベストプラクティスに関するメッセージを増やすために協調して努力する必要があります。

図25

What benefits do you expect to realize by consuming SBOMs?

Select all that apply | Segmented by SBOM maturity | N = 327, Valid Cases = 327, Total Mentions = 931



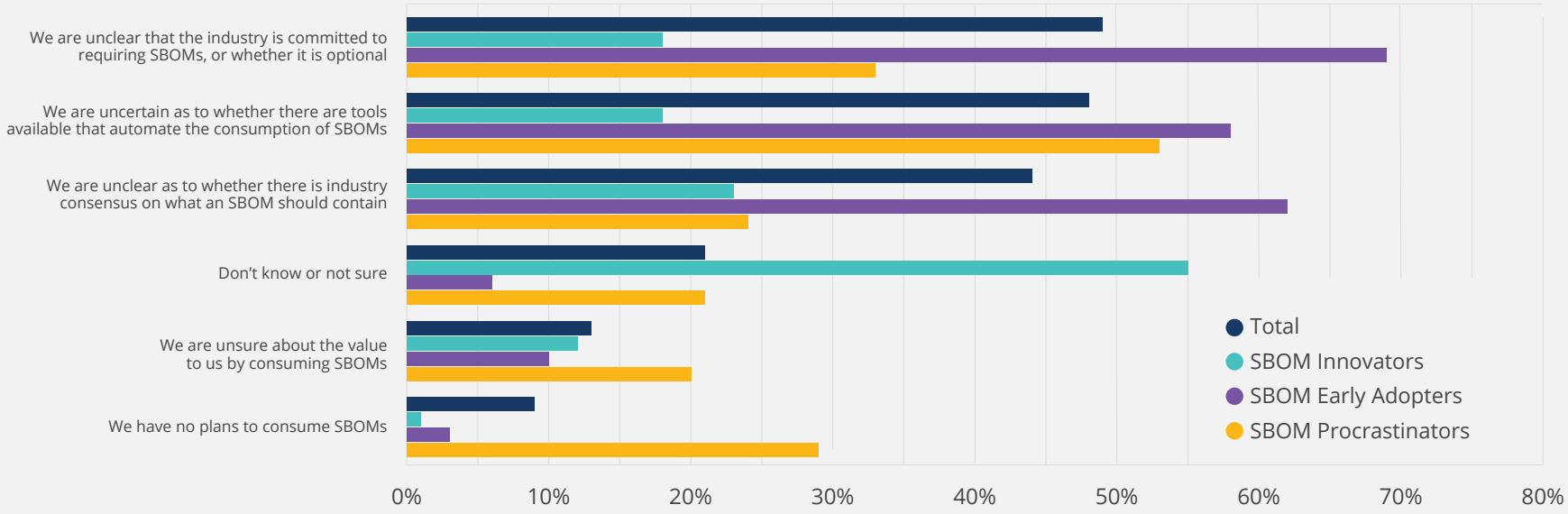
SBOMツールの可用性に関して存在する不確実性は、供給サイドの問題です。業界組織とベンダーは、SBOMツールのポートフォリオへの投資とそれに関連するメッセージングを強化する必要があります。後述するように、SBOMツールの市場は2022年と2023年に爆発的に拡大する可能性が高まっています。ベンダーやサービス プロバイダーは、エンドユーザーの需要を活用するために、製品やサービスを迅速に追跡することが推奨されます。

最後の懸念事項である、SBOMに何を含めるべきかに関する業界のコンセンサスの欠如は、知的財産の問題ではなく、セキュリティの問題です。脆弱性の特定と報告における進歩は、現在進行中です。セキュリティはSBOMの重要な側面となっているため、この問題は2022年に終結すると予想しています。

図26

What concerns do you have in consuming SBOMs?

Select all that apply | Segmented by SBOM maturity | N = 324, Valid Cases = 324, Total Mentions = 593



結論

この2021年のSBOM準備状況調査では、SBOM認知、SBOM準備、およびSBOMの作成と使用が予想以上に進んでいることが示されました。SBOMへのこれまでの投資の多くは、Intel、Siemens、Sony、Toyota、Wind Riverなどの企業や公共組織によって行われました。米国連邦政府機関（NTIA、FDA、NISTおよび商務省）は現在、SBOMの提唱と法制化（一部の業界で）に関与しています。IT業界の組織とベンダーは、SBOMの重要性についてメッセージを発信するようになり、データ フォーマットの進化、ベストプラクティスやテクノロジー ロードマップの定義をサポートするようになっています。これは素晴らしいスタートですが、キャズムを超えるためには、SBOM市場は大幅に進化する必要があります。

米国食品医薬品局（FDA）の政策アドバイザーは、SBOMの進化についてこう語っています。

「ヘルスケアで起きていることは、草の根のベストプラクティスが時間をかけて採用され、最終的に規制当局がこれをベストプラクティスとして正式に採用するというような他の産業とは異なります。ヘルスケアでは、その逆でした。規制当局がSBOMを追求することを発表し、最終的には米国で医薬品を販売するためにはSBOMが必要であると期待されるようになりました（この業界は数十億ドル規模の産業です）。今回の大統領令は、その数年後に出されたものですが、それは、医療に対する規制当局圧力がさらに強まったことを示しています。さまざまな関係者が口にしているのは、私たちには基本的に選択の余地はない、ということだと思います。サプライチェーンのすべてに影響が及ぶため、私たちはこれを解決しなければなりません。ヘルスケア メーカーがサプライヤーに対して「SBOMを提供しないなら、お金を払うつもりはない」と言えば、そこから連鎖が広がっていくことになります。」

SBOMを改善する方法

図27は、SBOM活動を改善する方法についてのフィードバックを示しています。全体の62%が指摘した最も差し迫った課題は、SBOMの作成と使用をソフトウェア開発に統合するためのベストプラクティスに関する業界のコンセンサスの必要性でした。SBOMの作成と使用はDevOpsで行われます。課題は、すべての組織が独自のDevOpsツールチェーン、プロセス、アクティビティを持っていることです。また、SBOMの作成や使用がDevOpsのどこで行われるべきなのかについても、まだコンセンサスが得られていません。SBOMの作成は明らかに開発指向のアクティビティですが、SBOMの使用はDevまたはOpsのいずれかで発生します。SBOMをどこで作成または使用すべきかというこの混乱に加えて、SBOMをいつ作成または使用すべきかという問題もあります。SBOMの作成と使用のもう1つの側面は、既知の依存関係と脆弱性が常に変化しており、SBOMが作成され使用された場所と時期に影響を与えるということです。

家電製品の大手メーカーは、SBOMを採用する際の課題について、次のように述べました。重要な課題は、データ フォーマットの複雑さゆえに、どこからどのように始めるべきかを判断するのが難しいということです。もう1つの関連する問題は、さまざまなSBOMデータ フォーマット間の相互運用性の欠如でした。これらの問題は、SBOMの作成、使用、統合、および相互運用性を容易にするSBOMツールの利用可能性が限られていることを示しています。

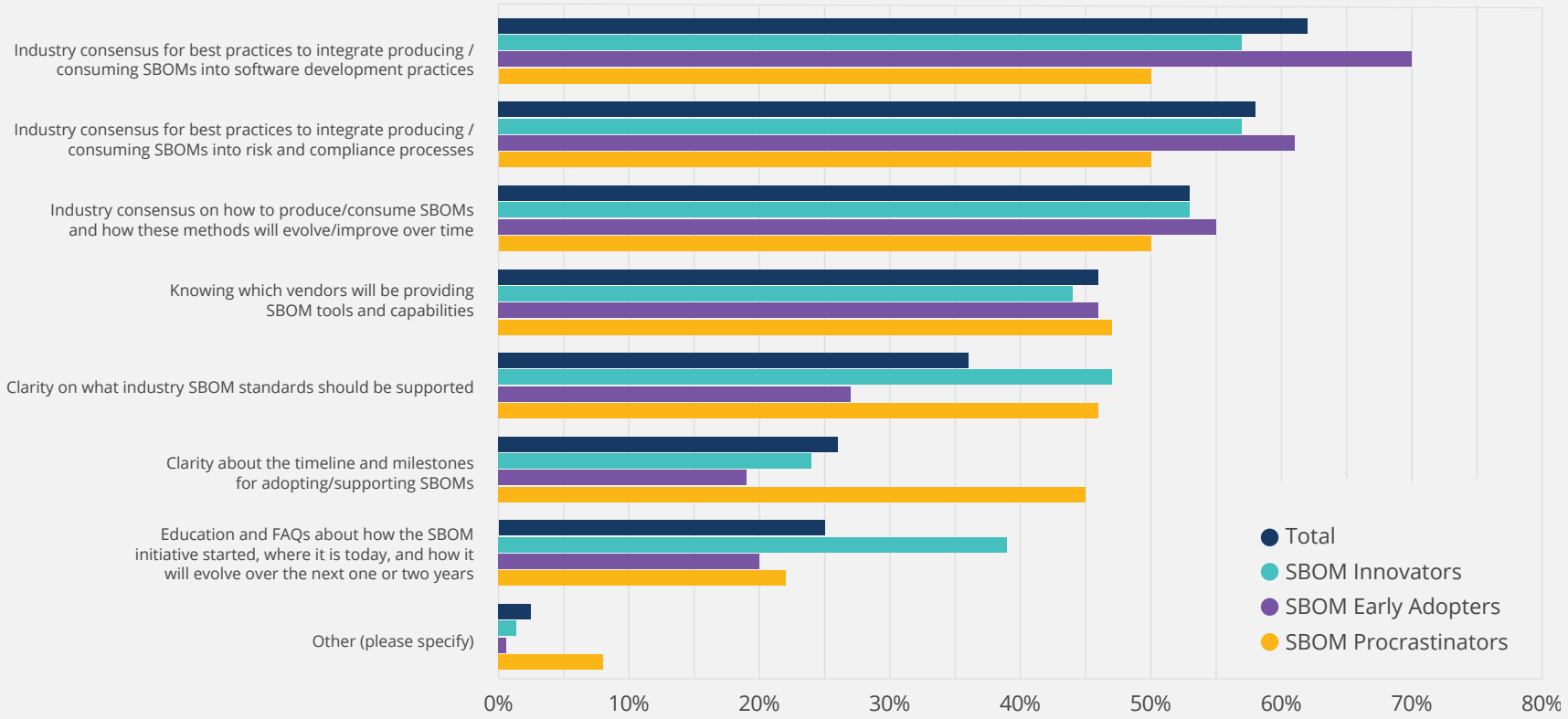
全体の58%が指摘している第2位の業界ニーズは、SBOMの作成と使用をGRC（ガバナンス、リスク、コンプライアンス）プロセスに統合するためのベストプラクティスに関するコンセンサスです。OSPO（オープンソース プログラム オフィス）および/またはCISO（最高情報セキュリティ責任者）を持つ組織は、このニーズに対処するのに十分な立場にあります。しかし、この2021年のSBOM準備調査では、全体として約20%の組織がOSPOまたはCISOを持っていないことが示されました。これらの数字は、SBOMイノベーターとアーリー アダプターでは約10%にまで減少しましたが、SBOM慎重派では35%から40%に増加します。

図27はまた、全体の53%が、SBOMを作成または使用する方法が時間とともにどのように進化するかについて、業界のコンセンサスを求めていることも示しています。NTIAはSBOM（ソフトウェア部品表）の最小要素を最近発表したばかりですが、SBOMのデータフォーマットも急速に発展し

図27

What would be useful to your organization to improve its ability to produce and/or consume SBOMs?

Select all that apply | Segmented by SBOM maturity | N = 319, Valid Cases = 319, Total Mentions = 983



ています。この変化は初期の市場の特徴ではありますが、それは明らかにSBOMの作成と使用を困難にしています。同時に、ITベンダー コミュニティがSBOM市場の形成と拡大に貢献できる大きなチャンスがあることは明らかです。**図27**は、全体の46%が、SBOMツールと機能を提供するベンダーがどこなのか理解するのに苦労していることを示しています。

SBOMの重要性

このレポートの前半に示した**図6**で、98%の組織がオープンソース ソフトウェアを使用していることを示しました。また、市場で入手可能なプロプライエタリ ソフトウェアの多くが、何らかの形でオープンソース ソフトウェアを利用していることが分かります。この状況から、**図28**は、プロプライエタリ ソフトウェアと比較して、オープンソース ソフトウェアにとってSBOMがいかに重要であるかを示しています。

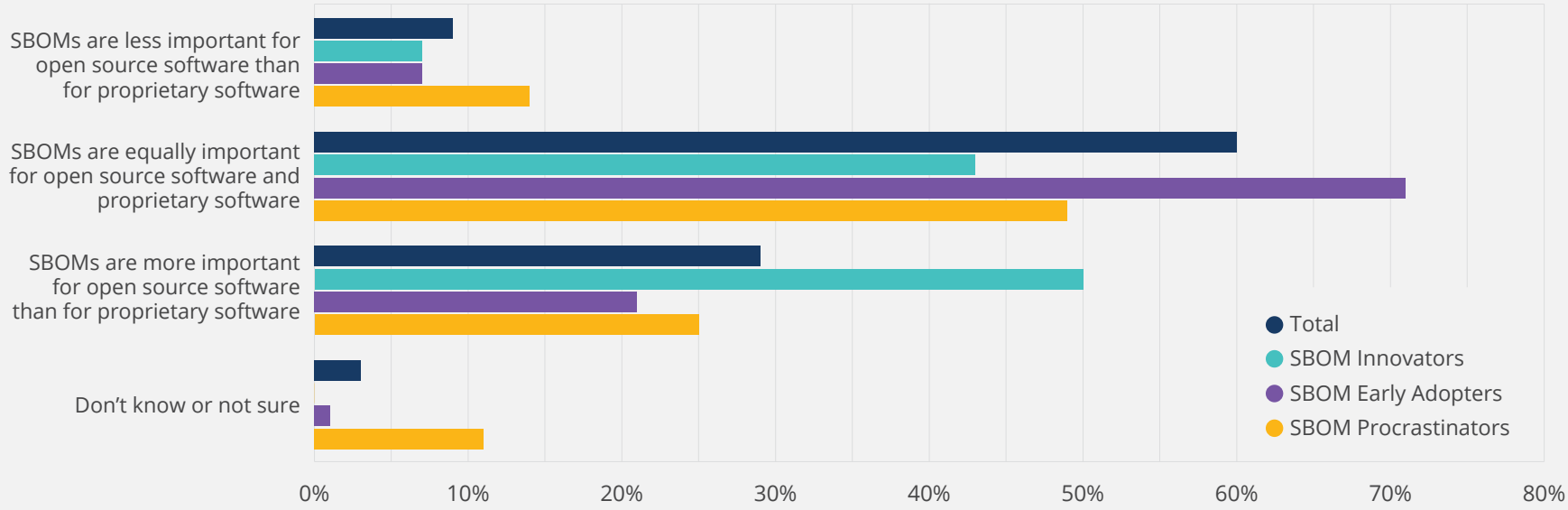
図28によると、60%の組織が、SBOMは、オープンソース ソフトウェアとプロプライエタリ ソフトウェアのどちらにとっても等しく重要であると考えています。残りの組織のうち、29%はSBOMがオープンソース ソフトウェアとプロプライエタリ ソフトウェアにとってより重要であると考えており、9%はSBOMがオープンソース ソフトウェアにとってそれほど重要ではないと考えています。このデータが示すことは、いくつかの解釈が可能です。

サンプルの60%が、SBOMはオープンソース ソフトウェアとプロプライエタリ ソフトウェアの両方にとって等しく重要であると考えているという事実は、大多数の組織がすべてのソフトウェア コンポーネントについてSBOMを見ることに関心があることを意味します。しかし、SBOMがオープンソース ソフトウェアにとってより重要であると考えている29%の人々は、自社

図28

How important are SBOMs for open source software compared to proprietary software?

Single Response | Segmented by SBOM maturity | N = 316



製品にオープンソースを活用している可能性があるにもかかわらず、プロプライエタリ ソフトウェアのベンダーの方が、製品の審査とテストにおいてより良い仕事をしている、と捉えていると解釈できます。問題を複雑にしているのは、SBOMイノベーターがこのトピックに関して、43%がSBOMは同じくらい重要だと考えており、50%がSBOMの方がオープンソース ソフトウェアにとって重要だと述べていることです。おそらく、SBOMイノベーターは、SBOMの作業経験が豊富であり、オープンソースのSBOMの必要性が高いと考えているのでしょう。

このジレンマに対する答えは、すべてのソフトウェア製品が何らかのオープンソース コードを含む可能性が高いという前提のもとで、すべてのソフトウェアに対してSBOMを法制化することです。このアプローチはヘルスケアで成功し、ベンダーに受け入れられ、エンドユーザーから称賛されています。自動車、エネルギー、製造業など他の市場では、ヘルスケアにおけるSBOMへの移行を評価しています。

オープンソース ソフトウェアのSBOMニーズと、プロプライエタリ ソフトウェアのSBOMニーズを比較することは、不自然さを孕んでいますが、サイバーセキュリティの問題を解決することの重要性は、ソフトウェア サプライチェーン全体で最も重要なことです。大統領命令は警鐘ではなく、サイバーセキュリティが深刻な問題であり、サイバーセキュリティへの取り組みを加速させる必要があることを確認したに過ぎないのです。幸いなことに、SBOMポリシー、データ フォーマット、およびツールは過去4、5年に渡って、米国連邦政府、ITベンダー、およびIT業界団体によって開発されてきました。初期のSBOM生成の問題は過去のものとなり、近い将来に迫り来る最大の課題は、SBOMが早期に大多数に採用されるように、いかにキャズムを超えるかにあります。課題は、規制の監視、SBOMの成熟度、ベンダーの参加、製品開発、効果的に付加価値を伝えるメッセージ発信を、いかに首尾一貫した方法で推進するかです。

SBOMの将来

SBOMを作成（**図21**）または使用（**図24**）するという組織の意図に基づいて、SBOMの使用（普及）と成長の予測を推定することができます。SBOMの作成と使用の全体的なプロファイルは類似しており、図29に示すように、これら2つの指標を集約することができます。図29の予測は、すでにSBOMを作成または使用している組織に、SBOMの作成または使用を計画している組織の増分を加えたものです。2021年の48%の普及率は、

オープンソース ソフトウェアのSBOMニーズと、プロプライエタリ ソフトウェアのSBOMニーズを比較することは、不自然さを孕んでいますが、サイバーセキュリティの問題を解決することの重要性は、ソフトウェア サプライチェーン全体で最も重要なことです。大統領命令は警鐘ではなく、サイバーセキュリティが深刻な問題であり、サイバーセキュリティへの取り組みを加速させる必要があることを確認したに過ぎないのです。

（図21および図24から）ビジネスのセグメント（少数／一部／多数／ほぼすべて／標準的なプラクティスとして）にわたってSBOMを作成または使用している組織の割合です。2022年の普及率は、今後6カ月または1年以内にSBOMを作成または使用することを計画している組織を追加したものです。同様に、2023年には、今後12～24カ月にSBOMの作成または使用を計画している組織が追加されます。

図29によれば、2022年のSBOMの作成/使用の伸びが66%と高く、SBOMの普及率が78%に達すると予想されます。SBOMの年間成長率は、2023年には13%まで低下していますが、それでもSBOMの普及率を88%にまで押し上げています。これは非常に積極的な成長シナリオであり、SBOM作成と使用のためのツール市場が急速に発展、成長することが条件となりそうです。

米国政府は、ソフトウェアを購入する際にSBOMを義務付けることについて、毅然とした態度をとっています。これは、SunBurstを初めとするサイバー攻撃の経験によるものです。しかしそれ以上に、デジタル経済への移行とソフトウェアへの依存により、デジタル資産は事実上すべての組織にとってミッションクリティカルであり、場合によっては医療機器業界のようにライフクリティカルであるという認識のほうが重要です。この調査は、SBOMの作成と使用によってもたらされる様々な利点を明らかにして

きました。SBOMは当初、知的財産を特定し保護する方法として始まりました。しかし現在では、セキュリティもSBOMの課題の一部となっています。最近行った、米国国土安全保障省の上級政策アドバイザーとの議論により、SBOMの役割が拡大されました。

「SBOMはいくつかの重要な問題を解決するのに役立ちます。その1つは、新しい脆弱性が発見されたときに、自分が影響を受けるのか、という問題です。SBOMがある場合は、影響を受ける可能性がある場所を特定できます。SBOMが完全であるほど、影響を受けていないことを証明できる可能性が高くなります。しかし、より大きな視点は、ソフトウェアのサプライチェーンを把握することです。可視性とインセンティブ、柔軟性が必要です。SBOMはそれらを提供しませんが、それらすべてを可能にします。言い換えれば、SBOMなしでは前進できないということです。SBOMが広く使用されるようになれば、より多くの組織が、使用しているオープンソース製品やサプライチェーンで使用している商用製品に注意を払うことができる

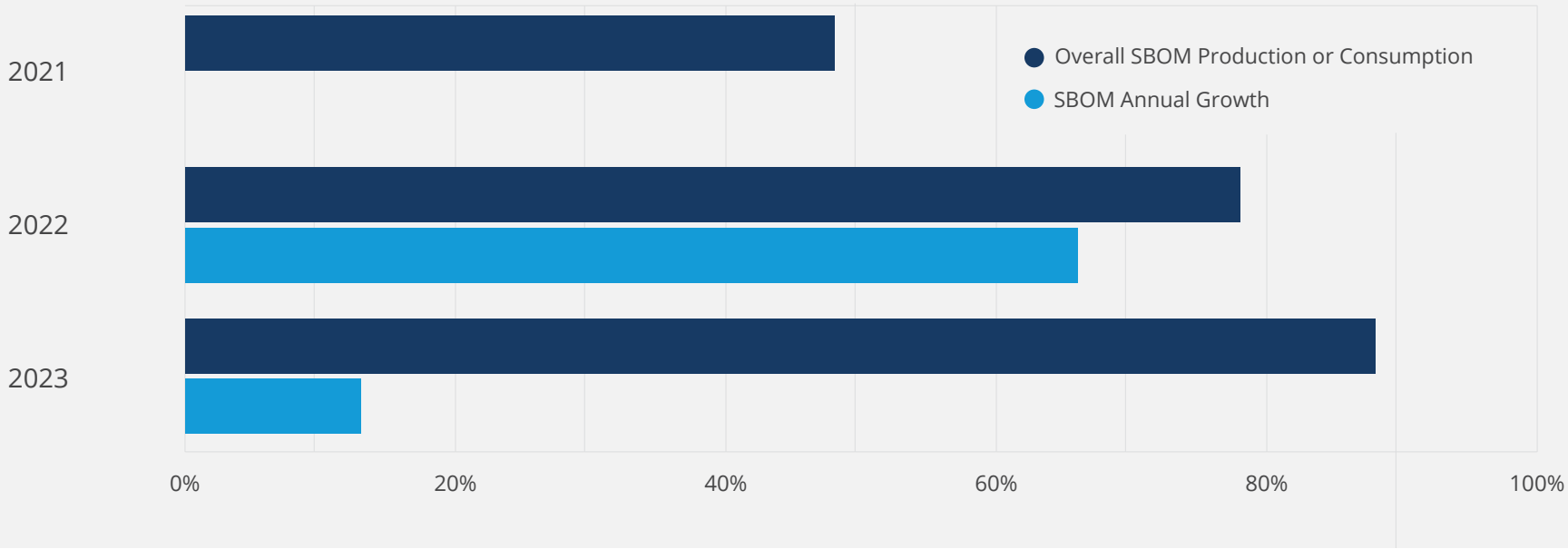
「可視性とインセンティブ、柔軟性が必要です。SBOMはそれらを提供しませんが、それらすべてを可能にします。言い換えれば、SBOMなしでは前進できないということです。」

ようになります。伝統的なサプライチェーンや物理的な商品で見てきたように、意識することで品質の向上が促されるのです。今のところ、基本的なSBOMでは、誰かが人気のある製品にバックドアを注入したかどうかを知ることはできません。SBOMができることは、バックドアが注入されたことがわかれば、誰もが影響を受けているかどうかを判断できるということです。しかし、その可視性が得られたら、次のステップでは、系統と起源のメタデータを重ね合わせて、私たちのツールに統合し、悪意のある攻撃

図29

Forecast organizational production or consumption and growth of SBOMs 2021-2023

N = 330-337



者を実際に検出できるようになります。このようにSBOMは、より良いソフトウェア保証とより良いソフトウェアサプライチェーンを実現するために必要なものですが、これだけでは十分ではありません。

本報告書のSBOMに関する作成（**図21**）と使用（図24）のデータは、49%の組織がいくつかのSBOMを作成しており、同様に56%がいくつかのSBOMを使用していることを示しています。SBOMの対象とツールのSBOM市場はあまり注目されておらず、可視性を生み出していませんが、多くの業界がSBOMポリシーとベストプラクティスの構築に取り組んでいます。SBOMが現在、今ひとつ注目されていないのは、業界の活動がドメインに特化しているからです。IACS（Information Sharing and Analysis Centers）は多くの主要産業で設立されています。

SBOMツールの市場には、すでに約20社のベンダーが参入しています。これらのベンダーの中には、Software Composition Analysis（SCA）Artifact Registry and Repository Managers（ARRM）、ソフトウェア セキュリティなど、隣接する市場から参入しているベンダーもあります。SBOM生成に焦点を当てたさまざまなオープンソース プロジェクトも存在します。業界ごとにポリシー、データ、メタデータを調整するためのドメイン固有のプラグインを備えた水平的なSBOMツール市場があると想定されています。

現時点で、米国連邦政府は、SBOMの需要を刺激するために地歩を固めています。彼らのアプローチは、政府が購入したソフトウェアに対してSBOMを要求することです。これは、連邦政府がデバイス製造業者にSBOMの提供を義務付ける規制を導入したヘルスケアとは少し異なります。しかし、結果は同様で、真のエンドユーザーの要求、または代理人による要求です。SBOMのデータ フォーマットは、様々なアプローチによってサポートされており、そのいくつかはISO標準として認められています。すでに述べたように、急速に増大する需要に対処するために、SBOM供給側ツールの活動がすでに進行中です。SBOMの市場は急速に発展する可能性が高く、世界の主要なソフトウェア ベンダーによるサポートを通じて、さらに急速に発展する可能性があります。

調査方法

このセクションでは、サンプリング、データ分割、およびSBOM準備への応答をSBOM成熟度の尺度に集約する方法について説明します。

調査対象者と分析方法

本研究の目的は、SBOMの作成と使用における組織の即応性を理解することです。採用された技術には、定量的調査に基づく研究と定性的面接に基づく研究が含まれます。このプロジェクトの定量的な側面には、2021年6月から2021年8月にかけて実施された技術専門家の世界的な調査が含まれています。調査は英語以外の6つの言語（中国語（簡体字）、日本語、韓国語、フランス語、ドイツ語、ロシア語）で行われました。回答者は、Linux Foundationコミュニティ メンバーとサードパーティ パネルの技術専門家の2つの関係者から選ばれました。対象となった回答者は、エンドユーザー企業、テクノロジー ベンダー、ソリューションおよびサービス プロバイダ、公的機関のIT意思決定者と基幹業務のリーダーです。

調査を開始した回答者は519人で、そのうち291人（56%）がLinux Foundationから、228人（44%）がサードパーティの市場調査サービスITパネルからの回答でした。調査期間中、回答者が確実に回答できるよう、スクリーニング基準を設けました。スクリーニング後のサンプルには、市場調査委員会の222組織（54%）とLinux Foundationが無作為に抽出した190組織（46%）のうち412組織が含まれていました。

データのセグメンテーションとスクリーニング

調査データは複数の方法でセグメント化され、データを調査するための様々な方法を提供しています。主なセグメント変数と定義は次のとおりです。

- **データ コレクター、N=412。** Linux Foundationが提供する回答者の数(N)(46%)とサードパーティのパネル プロバイダーが提供する回答者の数(54%)を比較します。誤差の範囲(MoE)=±4.1%@90%信頼水準(CL)。

- **業種、N=405。** 回答者のうち、テクノロジー ベンダーまたはサービス プロバイダーに勤務する人(21%)とエンドユーザー企業に勤務する人(79%)を識別します。MoE=±4.1%@90%CL。

- **主要産業グループ、N=405。** 世界中の22の業界の回答者を、テクノロジー ベンダー、ソリューション、サービス プロバイダー(25%)、自動車(12%)、医療およびライフサイエンス(11%)、製造業(7%)、金融サービス(6%)、エネルギー(5%)、その他(34%)の6つの主要業界(および「その他」)に分類します。MoE=±4.1%@90%CL(34%)。

- **地域、N=402。** 10カ国からの世界中の回答者を、3つの主要な地理的地域(アメリカ(44%)、西欧(39%)、アジア太平洋(17%))に集計した。MoE=±4.1%@90%CL。

- **SBOM準備状況、N=357。** 回答者の組織のSBOM即応性に関する回答者の信念に基づいて自己選択した回答の集合:イノベーター(21%)、アーリー アダプター(51%)、プロクラスティネーター(24%)、知らないまたは確信がない(4%)。MoE=±4.3%@90%。

- **SBOM適格、N=341。** 回答者がソフトウェア部品表に関する質問に回答する資格があると感じたかどうかを尋ねる自己評価の質問に基づく:SBOM質問に回答する資格があると感じた回答者(83%)、SBOM質問に回答する資格がないと感じた回答者(11%)、知らないまたは確信がないと感じた回答者(5%)。MoE=±4.5%@90%。

この調査のすべての数値は、すべて小数点以下第2位を四捨五入した結果を含んでいます。したがって、セグメント データの合計が100%にならない場合があります。

この調査は、完了までの平均時間が20分以上と長く、調査の完了率は64%でした。このことから、上記のセグメント変数のサンプル サイズにある程度のばらつきがあることがわかります。

回答者がすべての調査質問に回答できる可能性が高いことを保証するために、包括的なスクリーニング基準が用いられました。スクリーニング基準には、特定のIT問題への精通度、ITドメインの経験、ITまたは同様の事業分野におけるシニア ロール、および確立された業界における雇用が含まれています。

このプロジェクトの定性的側面としては、業界や連邦政府のサイバーセキュリティ政策開発に携わる人物への綿密なインタビューを行いました。

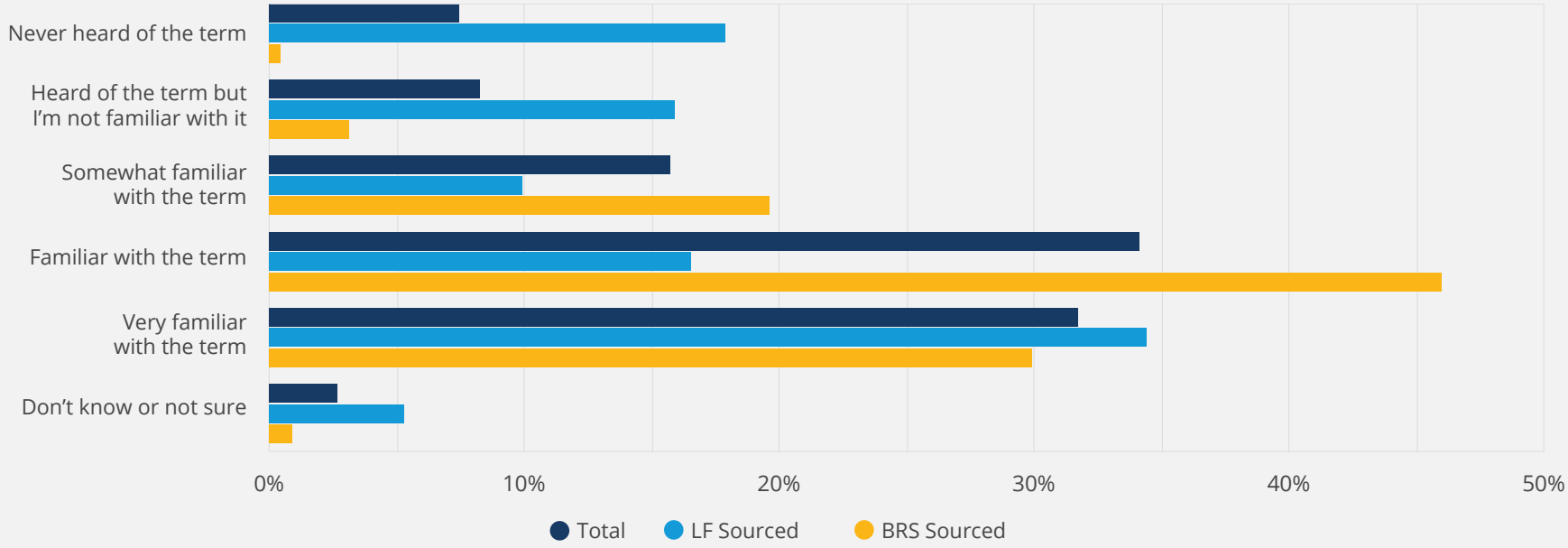
サンプル の偏りについて

調査の回答者は、最初はLinux Foundation（LF）コミュニティのメンバーから得ていました。研究の観点から見ると、これはサンプルに偏りをもたらす可能性がありました。このため、回答者は第三者の市場調査パネル提供者からも選びました。2つのサンプルの間に関係があるかどうかを決定するために、有意性検定を用いました。データ セットのほとんどの変数に対して2つのサンプル間に有意差が認められました。**図30**は、SBOMの認知について、データ収集者別に区分したもので検出された違いを示しています。

図30

What is your organization's familiarity with a software bill of materials (SBOM)?

Single Response | **Segmented by data collector** | **N = 375**



LFのデータは、SBOMを知らない、またはよく知らないグループが34%と多く、SBOMをよく知っている、または非常によく知っているグループが51%と、二峰性の分布を示しています。これは、LFコミュニティの参加者と一致しています。LFコミュニティには、キャリアの早い段階から、スキルセットを向上させ、雇用機会を増やす方法としてトレーニングや認定を受けるためにLFに来る若いITプロフェッショナルのグループが含まれています。このセグメントがSBOMに不慣れであることは驚くべきことではありません。また、LFには、ITの意思決定とポリシーにおいて重要な役割を担う、経験豊富なITプロフェッショナルを含む別のグループも存在します。このグループは、SBOMに精通している可能性が高いと考えられます。

調査委員会が入手したデータは、回答全体がある程度、正規分布しており、非常に異なった特徴を示しています。調査委員会のサンプルのうち、SBOM用語を聞いたことがないか、その用語に精通していなかったのはわずか4%であり、これに対して調査委員会のサンプルの大多数（76%）はSBOM用語に精通しているか、非常に精通していました。

この比較は、LFと研究パネルのサンプルが有意に異なることを示す多くのものの1つにすぎません。これら2つのサンプルは異なっており、研究パネルのサンプルはSBOMに精通しており、LFサンプルははるかに精通していないという事実は、SBOM準備の保守的な見解を提供することを可能にします。

回答者のSBOM質問への回答能力

回答者にSBOM定義を提供した後、調査は、回答者の組織がどのようにSBOMを使用しているか、または使用する予定があるかについて、質問に回答する資格があるかどうかを尋ねました。この質問の目的は、SBOMの知識のない回答者をセグメント化すると同時に、SBOMに関する知識を理解するための別の方法でした。**図31**は、回答者がSBOMに関する質問に回答する資格があると感じているかどうかを、SBOM成熟度別に区分して示したものです。

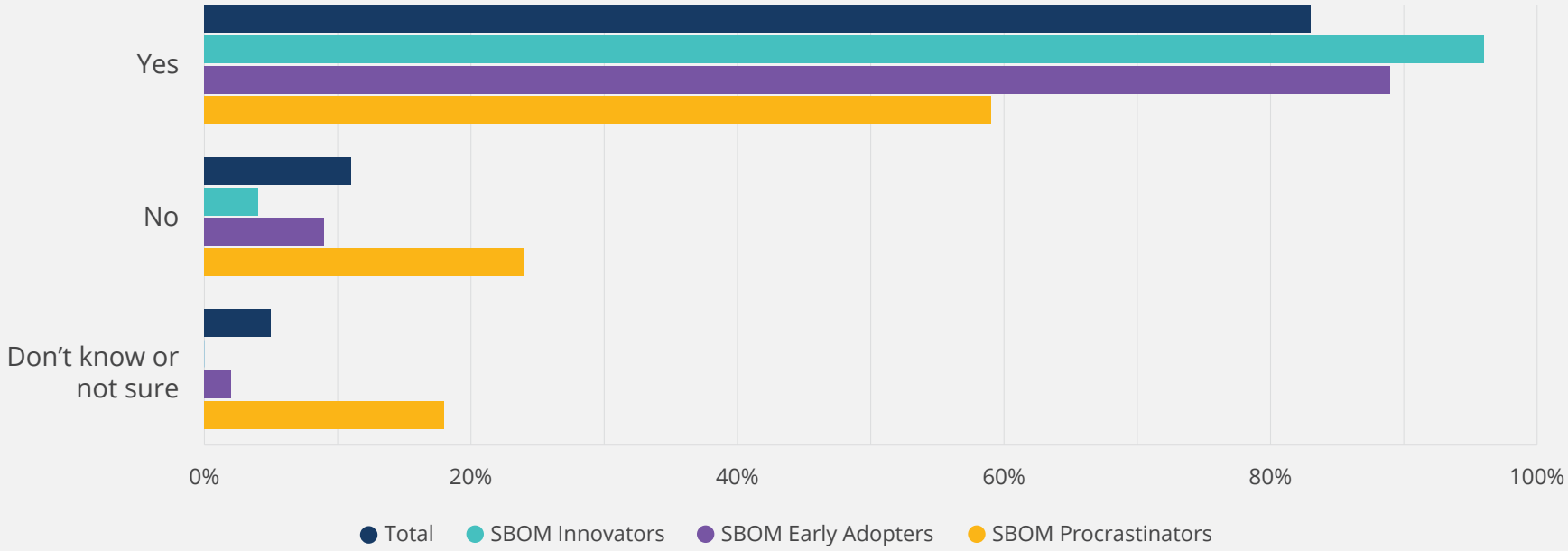
全体として、ほとんどの回答者（83%）はSBOMの使用に関する質問に答える資格があると感じており、11%はSBOMの使用について話す資格がないと感じており、5%はSBOMの使用について知らなかったか、確信がありませんでした。SBOM適格回答は、SBOM成熟度と高い相関を示しました。SBOM成熟度の高さは、SBOM適格回答者の高さと非適格回答者の低さと相関していました。図31は、SBOMイノベーターの96%がSBOMの質問に答える資格があると感じているのに対して、SBOMアーリー アダプターでは89%、SBOM慎重派では59%であることを示しています。SBOMの質問に回答する資格がないと感じた回答者（24%）またはDKNS（Don't know/Not sure）と回答した回答者（18%）のうち、最も高い割合を占めたのはSBOM慎重派でした。

調査では、回答者がどの程度資格があると感じているかにかかわらず、SBOMに関するすべての質問に回答し続けるよう、回答者に求めました。本報告書のSBOM分析では、調査を完了したすべての回答者からのデータを使用することにしました。というのも、資格のない回答者はSBOMの質問に対して、ほとんど常にDKNSと回答しているので、これは実際に問題を引き起こすことはありません。

図31

Do you feel qualified to answer a questions about how your company uses/intends to use SBOMs?

Single Response | **Segmented by SBOM maturity** | **N = 341**



脚注

1 国際通貨基金、世界経済見通しデータベース、2019年データ。

2 国際通貨基金、世界経済見通しデータベース、2019年データ。

3 地理的領域の区分については、このレポートの次の図を参照してください：図3、A9、A10、A11、A14-A17

4 国家のサイバーセキュリティの改善に関する大統領令」2021年5月、https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cyber_securityで利用可能

5 ID。第1節において

6 「SBOMの概要」『National Telecommunications and Information Administration』2021年4月27日、https://www.ntia.gov/files/ntia/publications/sbom_at_a_glance_apr2021.pdfから入手可能。

7 The Minimum Elements for a Software Bill of Materials(SBOM)、米国商務省、2021年7月12日

8 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations,アメリカ国立標準技術研究所,SP.800-161r1-draft2,October 2021

9 SBOM Options and Decision Points,National Telecommunications and Information Administration,2021年4月27日

9 SBOM at a Glance、National Telecommunications and Information Administration、2021年4月27日

付録A:人口統計とSBOM準備状況に関する追加情報

付録には、サンプルの人口統計、現在のIT環境、およびSBOMの準備状況を詳細に説明するための図が含まれています。次の図が含まれます。

A1 全社員数

A2 主な役割

A3 主な責任分野

A4 組織の業種

A5 IT産業組織の場合、IT組織の種類

A6 Linux Foundationのメンバー企業ですか?

A7 地域別の回答者

A8 組織の年間収益

A9 地理的地域別のSBOMに関する組織的な知識

A10 地理的地域別組織におけるOSPOの存在

A11 OSPOはプロジェクトのインベントリーを
セキュリティ チームと共有しているか? (地域別)

A12 地域別組織における最高セキュリティ
責任者/セキュリティ チームの存在

A13 i組織は、ソフトウェア ライフサイクルのどこで
SBOMを作成しているか? (SBOM成熟度別)

A14 組織は、ソフトウェア ライフサイクルのどこで
SBOMを使用しているか (SBOM成熟度別)

A15 地域別のSBOM準備状況

A16 地域別のソフトウェア セキュリティに関する組織の懸念事項

A17 米国サイバーセキュリティ行政命令に対する地域別組織の認識

A18 米国サイバーセキュリティ行政命令に対応した地域別の変化

A19 組織のSBOM作成に関する計画 (業種別)

A20 組織のSBOM使用に関する計画 (業種別)

図 A1

あなたの会社の従業員数（世界全体）を教えてください。

（1つ選択） | 回答数 (N) = 412

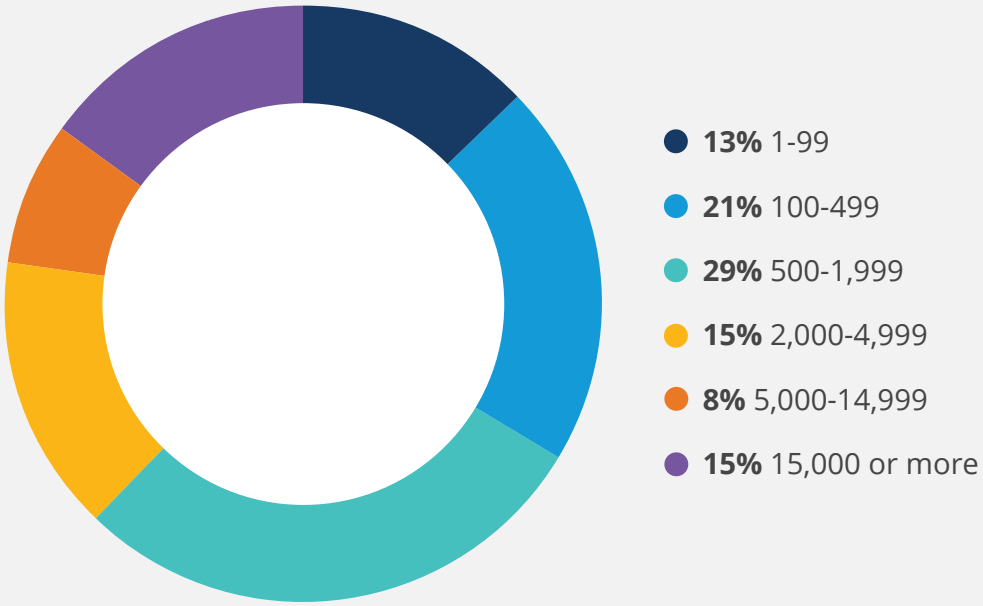


図 A2

あなたの職務や役職を最も適切に表しているものはどれですか？

（1つ選択）| 回答数 = 412

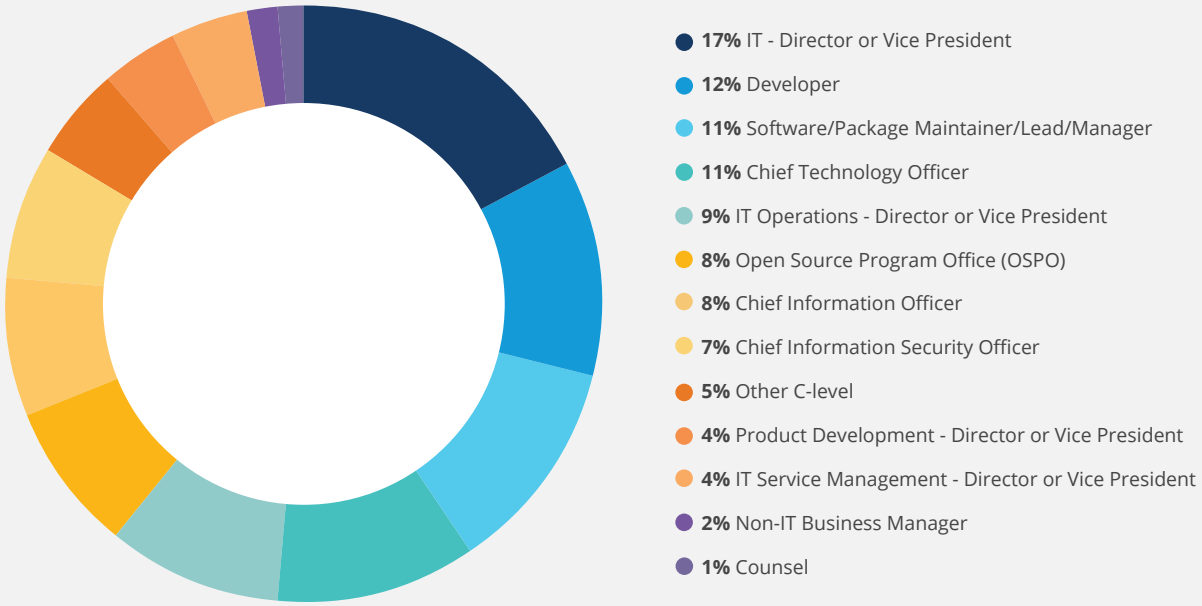
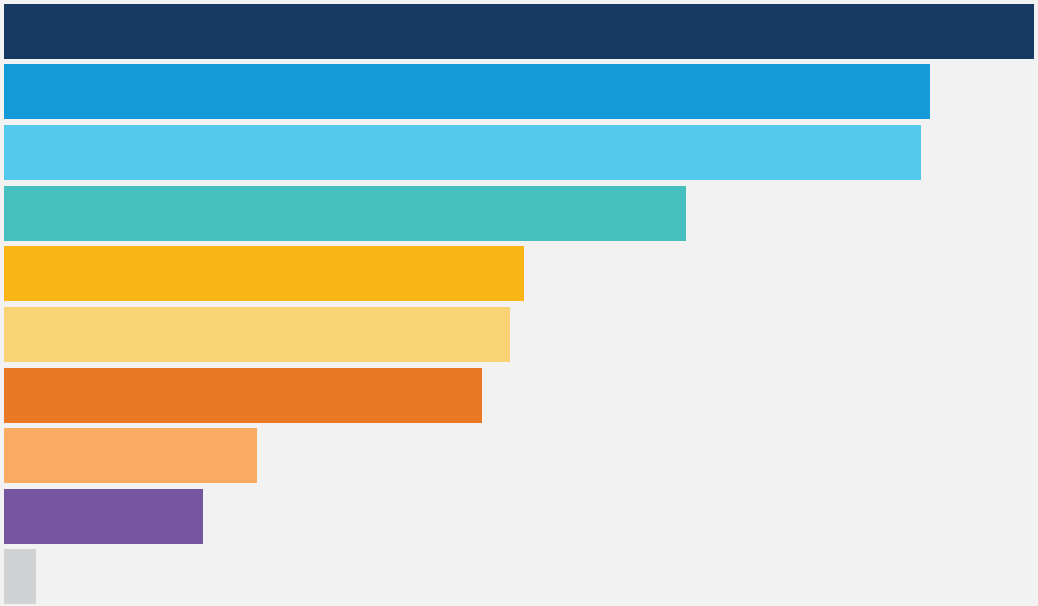


図 A3

あなたの主な責任分野は何ですか？

（当てはまるものをすべて選択） | 回答数 = 407、有効回答数 (Valid Cases) = 407、回答結果総数 (Total Mentions) = 1,227



56% Software development

50% IT Services management

50% Security

37% Software delivery or deployment

28% Legal, Governance, Risk, or Compliance

28% Strategy

26% Operations

14% Procurement

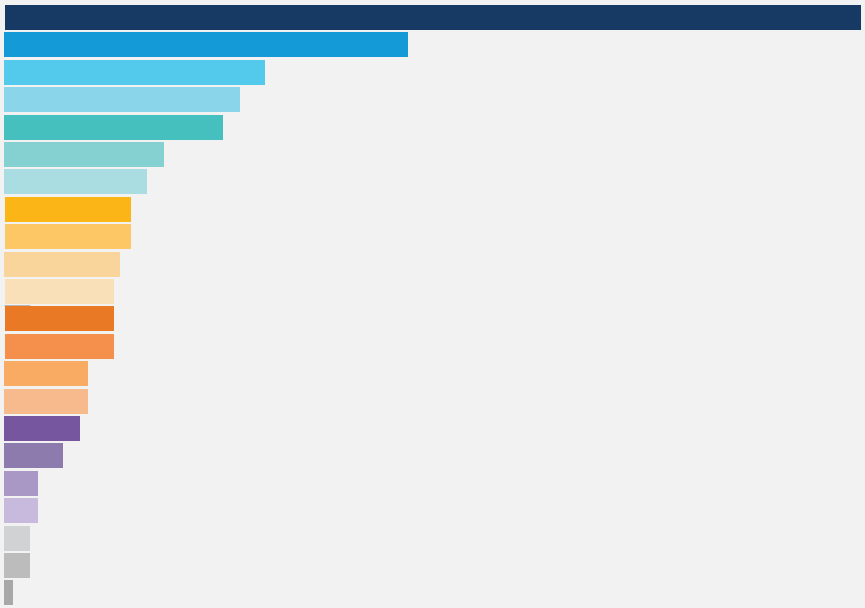
11% Senior Management

2% Other (please specify)

図 A4

あなたの組織の業種は何ですか？

（1つ選択）|回答数 = 405

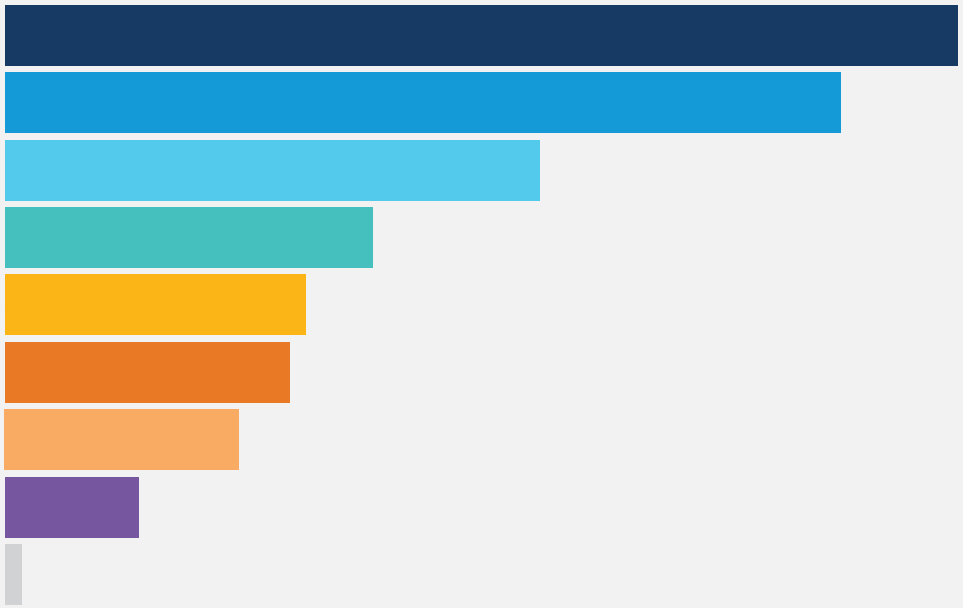


25% Information Technology
12% Automotive
8% Healthcare
7% Manufacturing (discrete or process)
6% Financial Services (Banking/Insurance/Securities)
5% Energy
4% Telecommunications / Internet Service Provider (ISP) / Web Hosting
4% Retail & Wholesale
4% Professional Services
3% Education (K-12/Primary/Secondary)
3% Other (please specify)
3% Life Sciences (biotech, pharmaceuticals, etc.)
3% Utilities (other than energy)
2% Construction/Engineering
2% Business Services (accounting, consulting, legal, etc.)
2% Consumer Packaged Goods
2% Government (Federal/National)
1% Education (College/University)
1% Oil & Gas
1% Transportation & Logistics (other than automotive)
1% Government (State/Province/County/Municipal/other local government)
0.25% Media (broadcast communications, entertainment, publishing, website, social networking …)

図 A5

IT組織で働いている方への質問です。どのようなIT組織で働いていますか？

（当てはまるものをすべて選択） | 回答数 = 101、有効回答数 = 101、回答結果総数 = 220



57% A software vendor or supplier

50% A system integrator or IT consulting firm

32% A cloud service provider or managed service provider

22% A software reseller or distributor

18% An embedded systems vendor

17% A hardware vendor or supplier

14% A nonprofit association or foundation

8% An academic or research institution

1% Other (please specify)

図 A6

あなたが働いている組織は Linux Foundation メンバー企業ですか?

（1つ選択）| 回答数 = 404

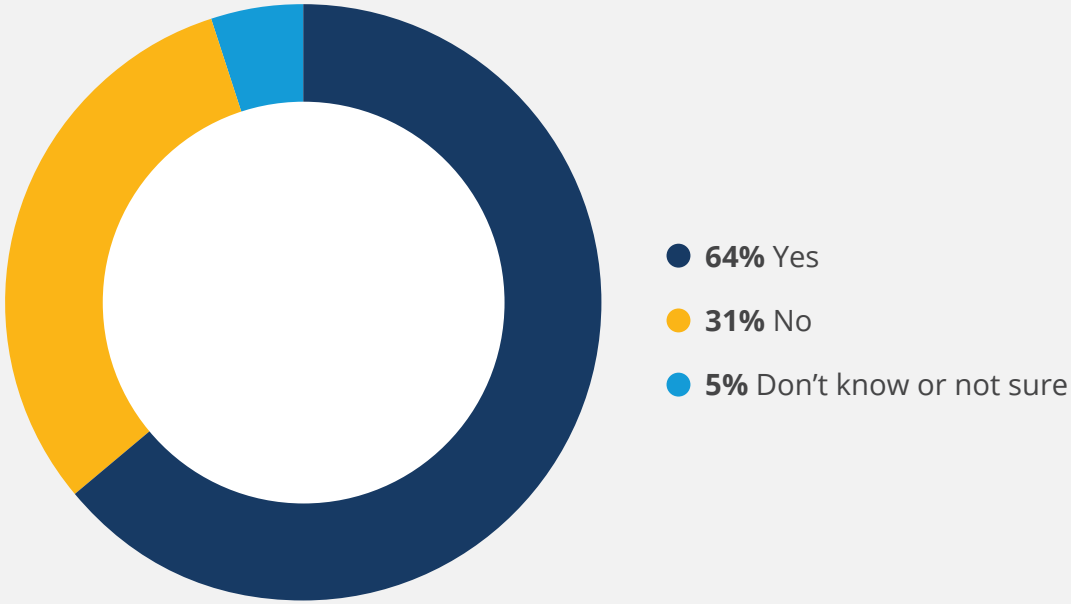


図 A7

あなたの居住地域を教えてください。

（1つ選択） | 回答数 = 402

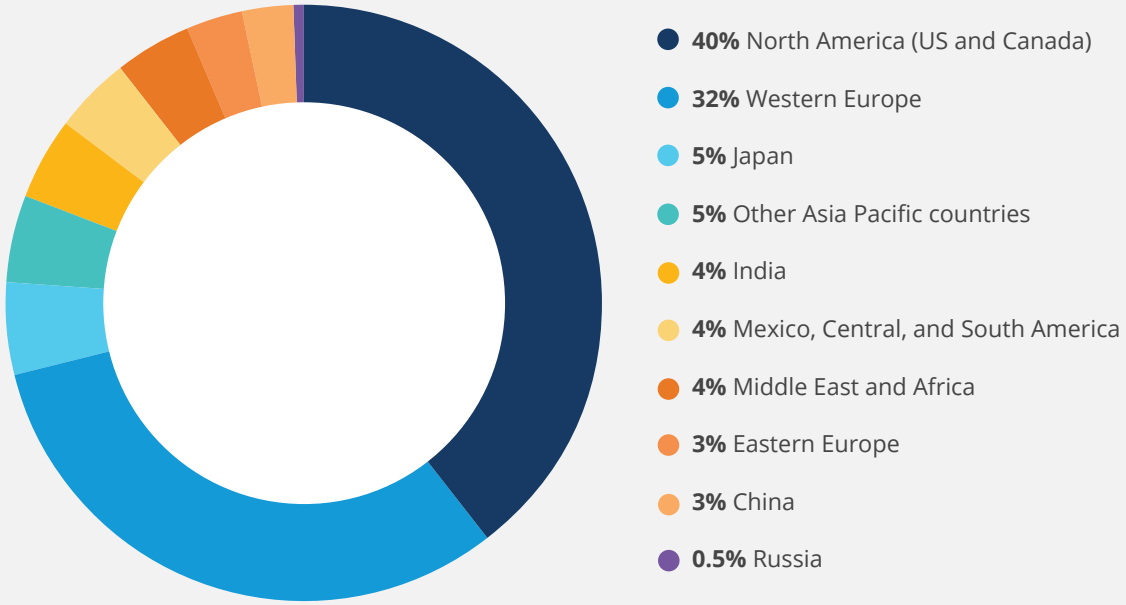


図 A8

あなたの組織の2020年の年間収益を教えてください。

（1つ選択）| 回答数 = 402

- **5%** Less than $1 million
- **5%** $1 million to less than $5 million
- **4%** $5 million to less than $10 million
- **4%** $10 million to less than $25 million
- **5%** $25 million to less than $50 million
- **12%** $50 million to less than $100 million
- **4%** $100 million to less than $250 million
- **11%** $250 million to less than $500 million
- **11%** $500 million to less than $1 billion
- **6%** $1 billion to less than $2 billion
- **6%** $2 billion to less than $5 billion
- **4%** $5 billion to less than $10 billion
- **7%** $10 billion or more
- **5%** Prefer not to answer
- **9%** Don’t know or not sure

図 A9

あなたの組織のSBOMに関する認知度を教えてください。

（1つ選択）| 地域別に集計 | 回答数 = 361

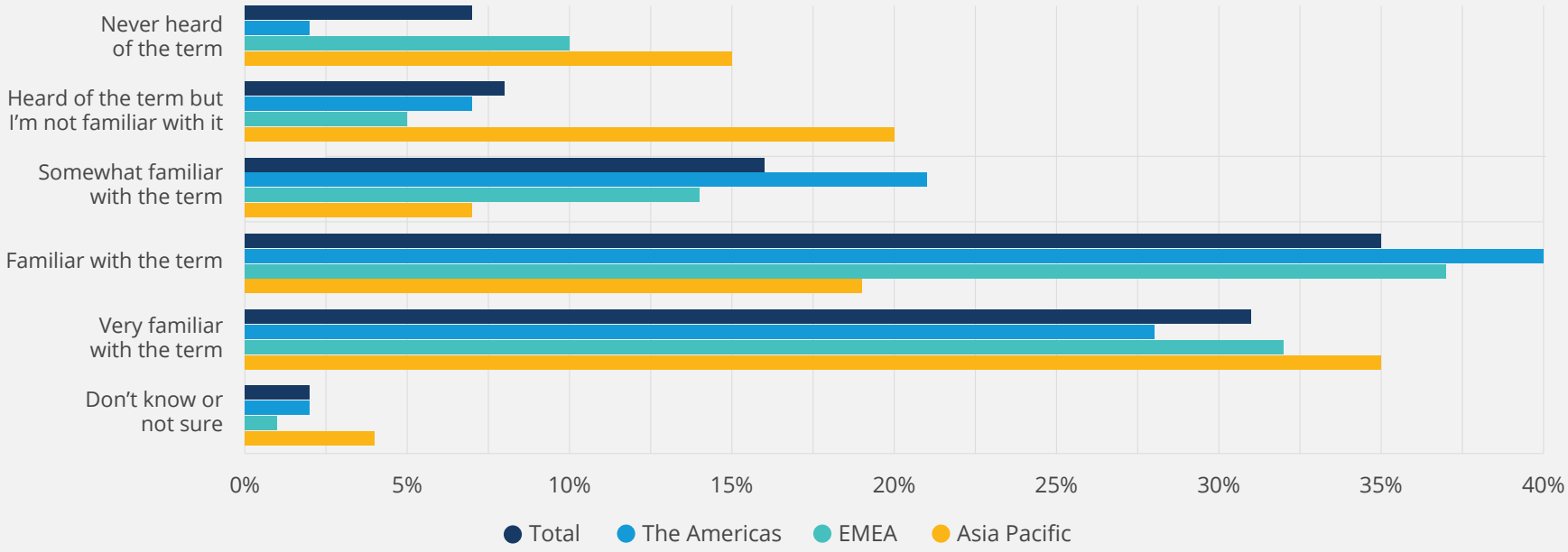


図 A10

あなたの組織は、オープンソース プログラム オフィス（OSPO）を設置してオープンソースの使用について管理していますか？

（1つ選択） | 地域別に集計 | 回答数 = 390

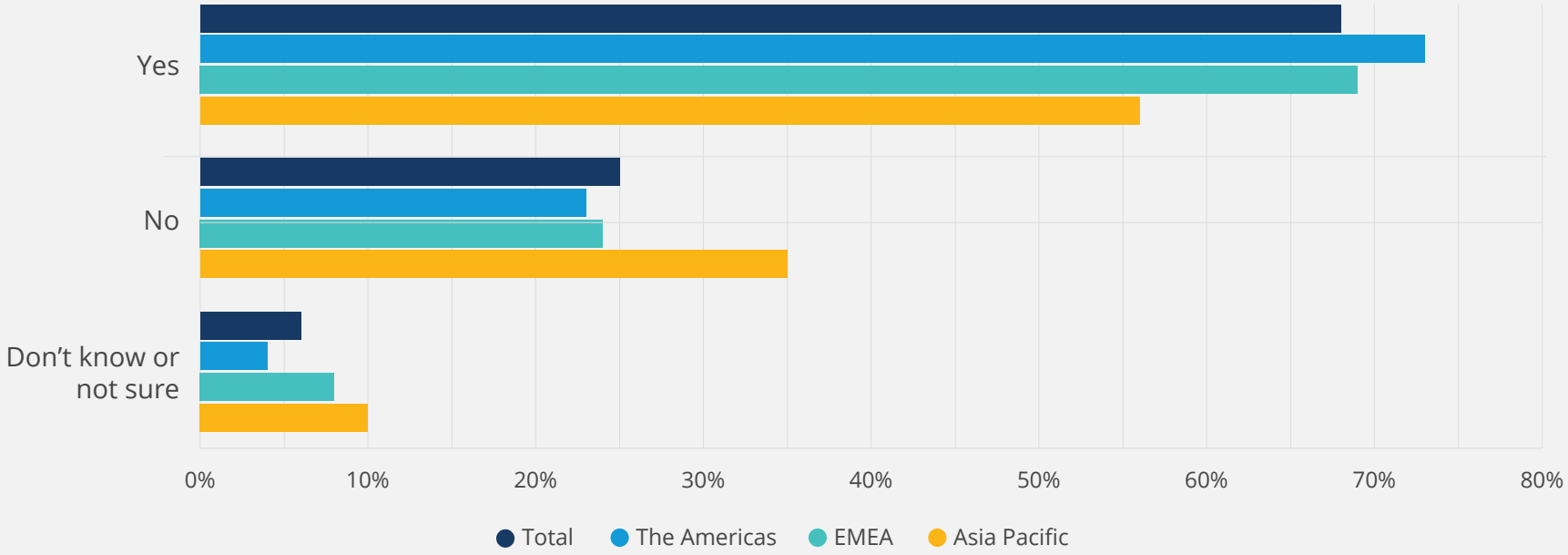


図 A11

あなたのオープンソース プログラム オフィスは、オープンソース プロジェクトの共通インベントリーをセキュリティ チームと共有して追跡していますか?

（1つ選択）| 地域別に集計 | 回答数 = 384

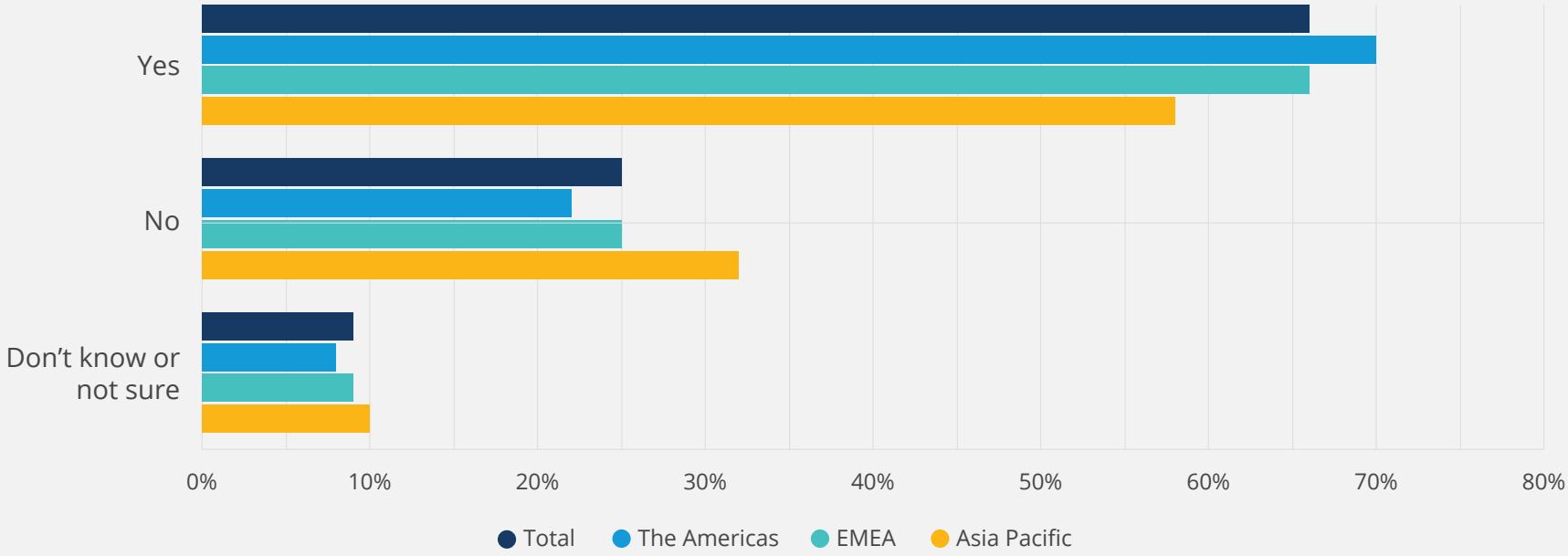


図 A12

あなたの組織には、最高情報セキュリティ責任者（CISO）やセキュリティチームを配置して、上流のオープンソース プロジェクトの脆弱性を監視していますか?

（1つ選択） | 地域別に集計 | 回答数 = 388

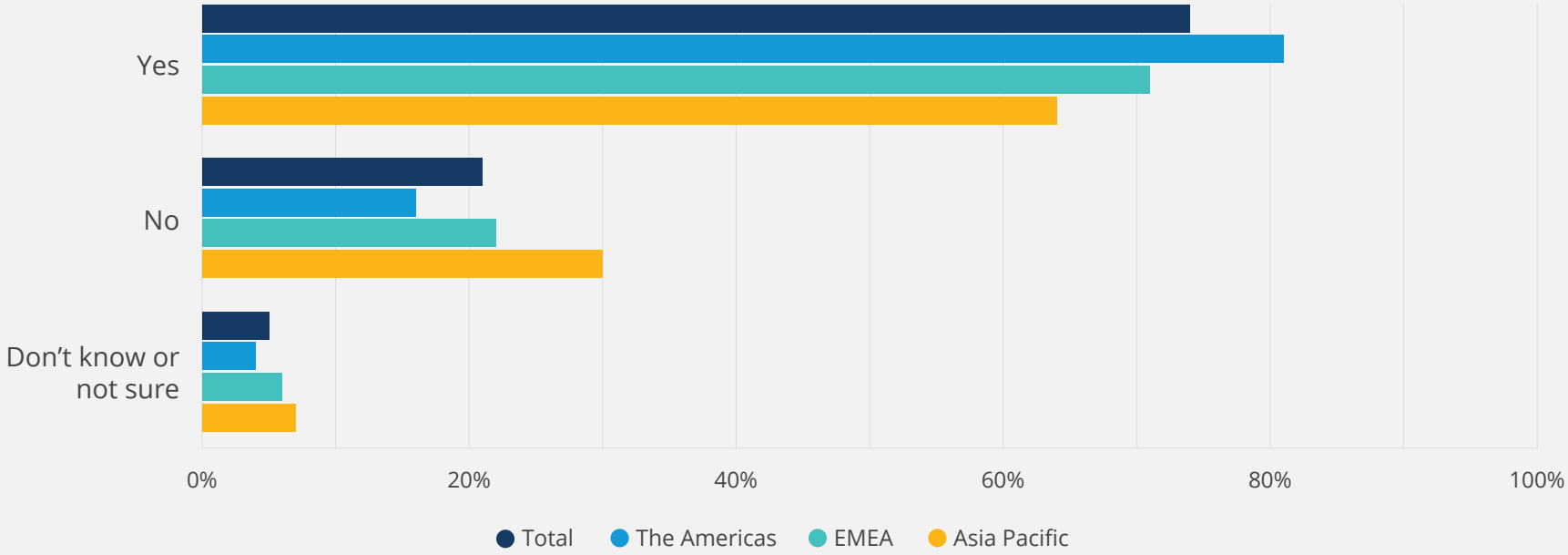


図 A13

あなたの組織は、ソフトウェア開発ライフサイクルのどこでSBOMを作成していますか／または作成する予定ですか？

（当てはまるものをすべて選択） | SBOMの成熟度別に集計 | 回答数 = 335、有効回答数 = 335、回答結果総数 = 849

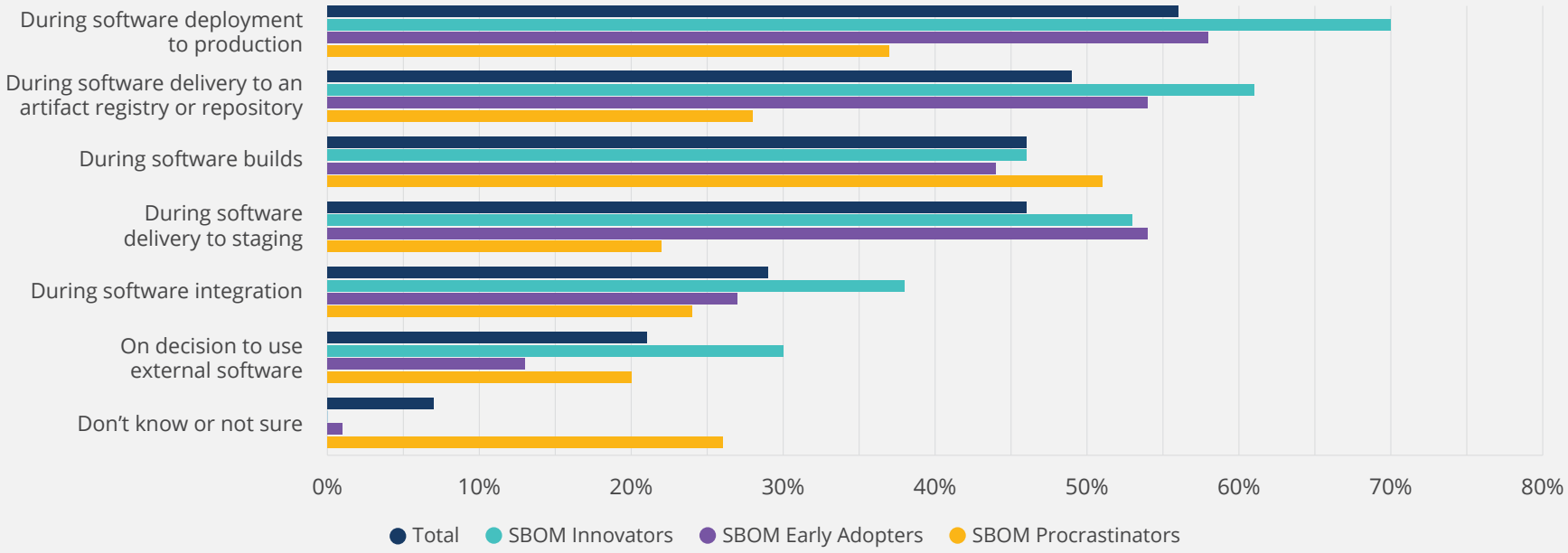


図 A14

あなたの組織は、ソフトウェア開発ライフサイクルのどこでSBOMを使用していますか／または使用する予定ですか？

（当てはまるものをすべて選択） | SBOMの成熟度別に集計 | 回答数 = 325、有効回答数 = 325、回答結果総数 = 896

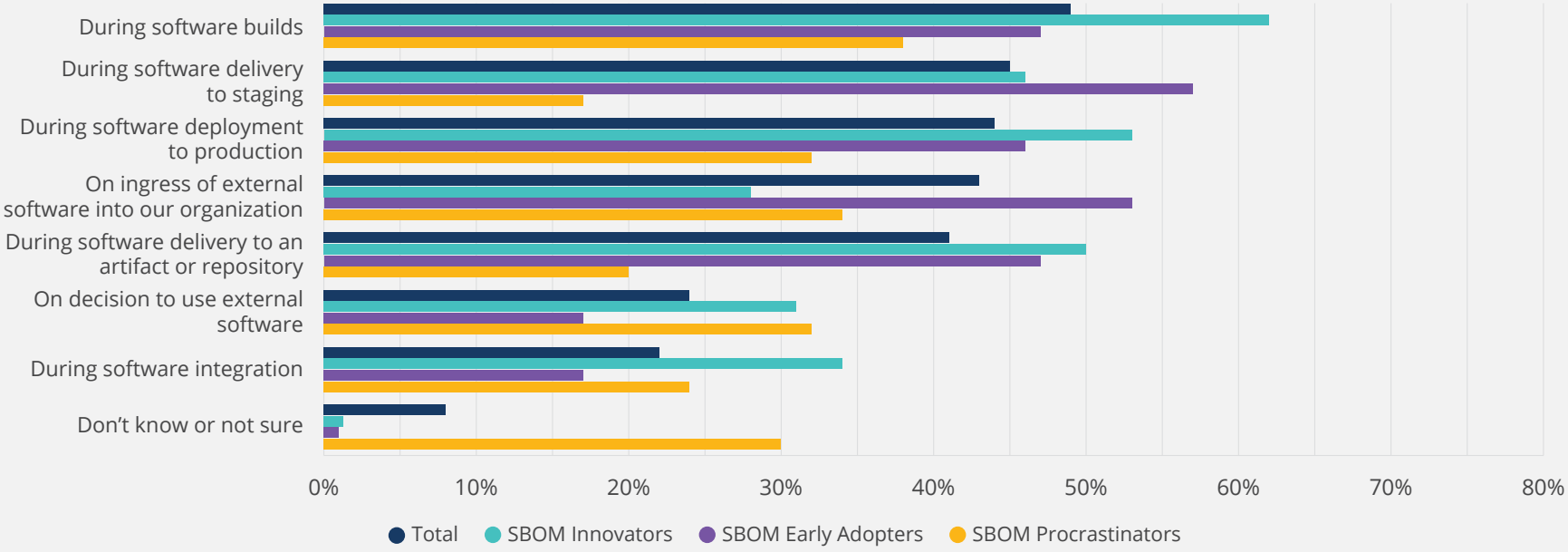


図 A15

あなたのグループの現在のSBOM対応状況を教えてください。

（1つ選択） | 地域別に集計 | 回答数 = 357

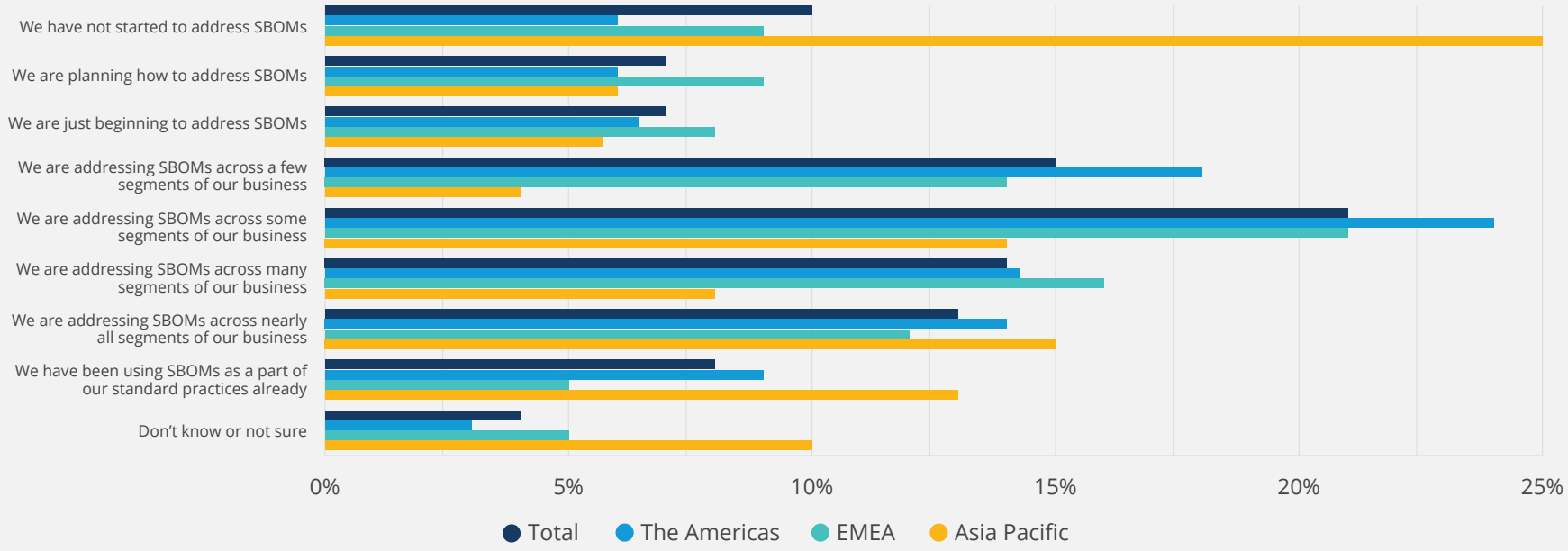


図 A16

あなたの組織は、使用しているソフトウェアのセキュリティについてどの程度懸念していますか？

（1つ選択） | 地域別に集計 | 回答数 = 363

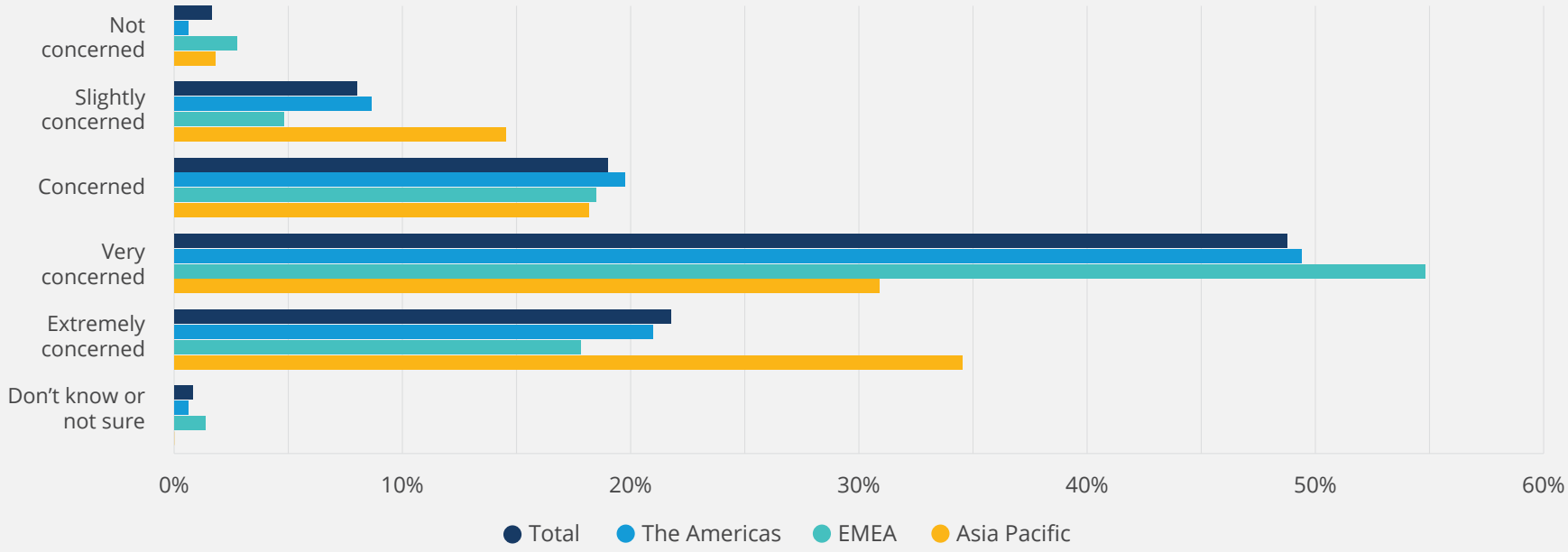


図 A17

あなたの組織は、サイバーセキュリティに関する米国の最近の大統領令で、ソフトウェアの部品表について言及があったことを認識していますか?

（1つ選択） | 地域別に集計 | 回答数 = 362

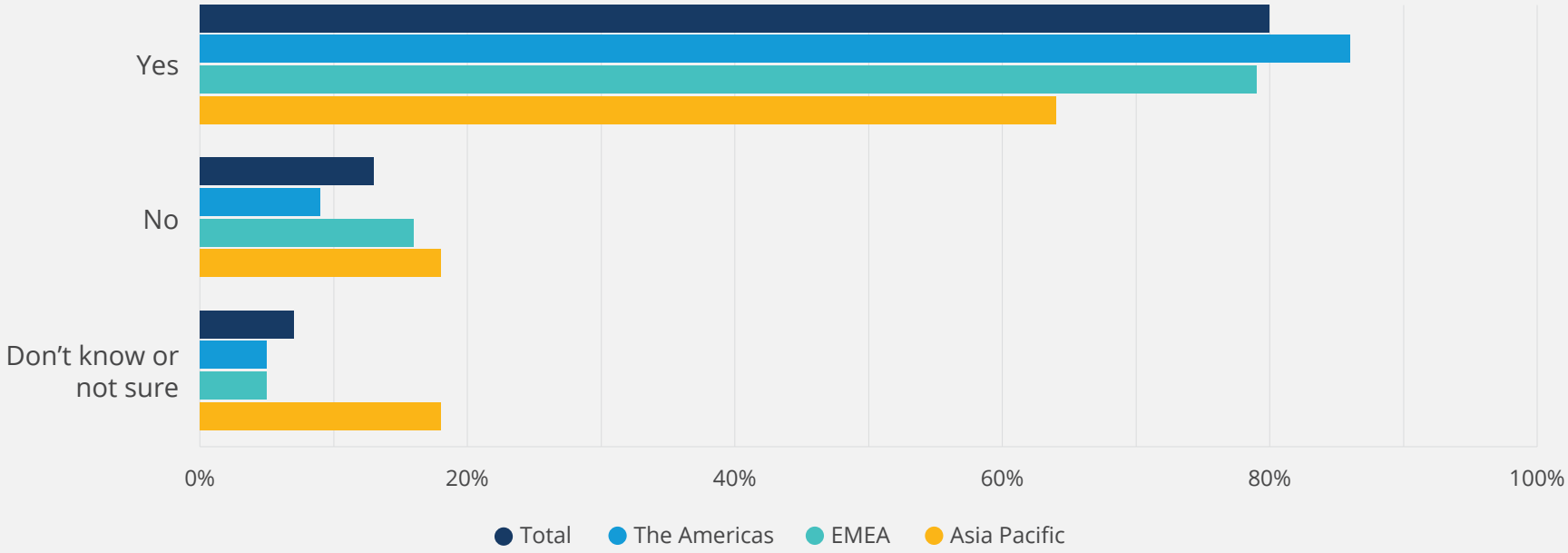
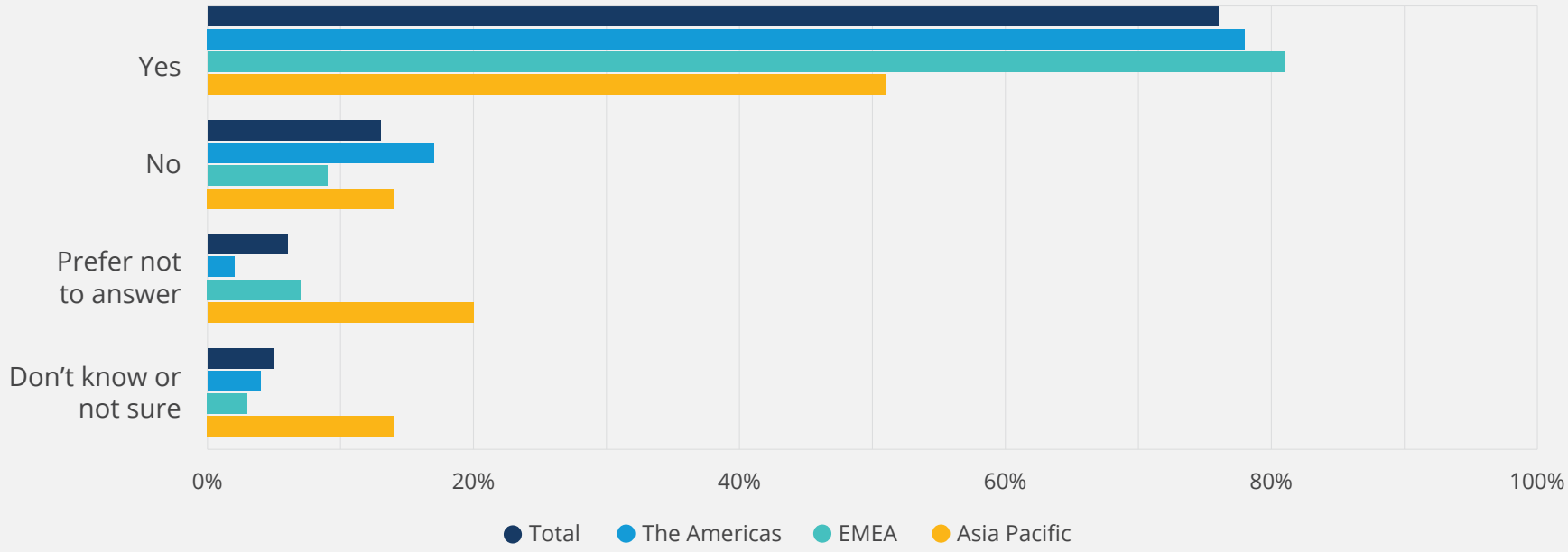


図 A18

あなたの組織は、サイバーセキュリティに関する米国の大統領令に対応して何らかの変更を検討していますか？

（1つ選択） | 地域別に集計 | 回答数 = 290



図A19

SBOMの作成に関するあなたの組織の計画について教えてください。

（1つ選択） | 業種別に集計 | 回答数 = 352

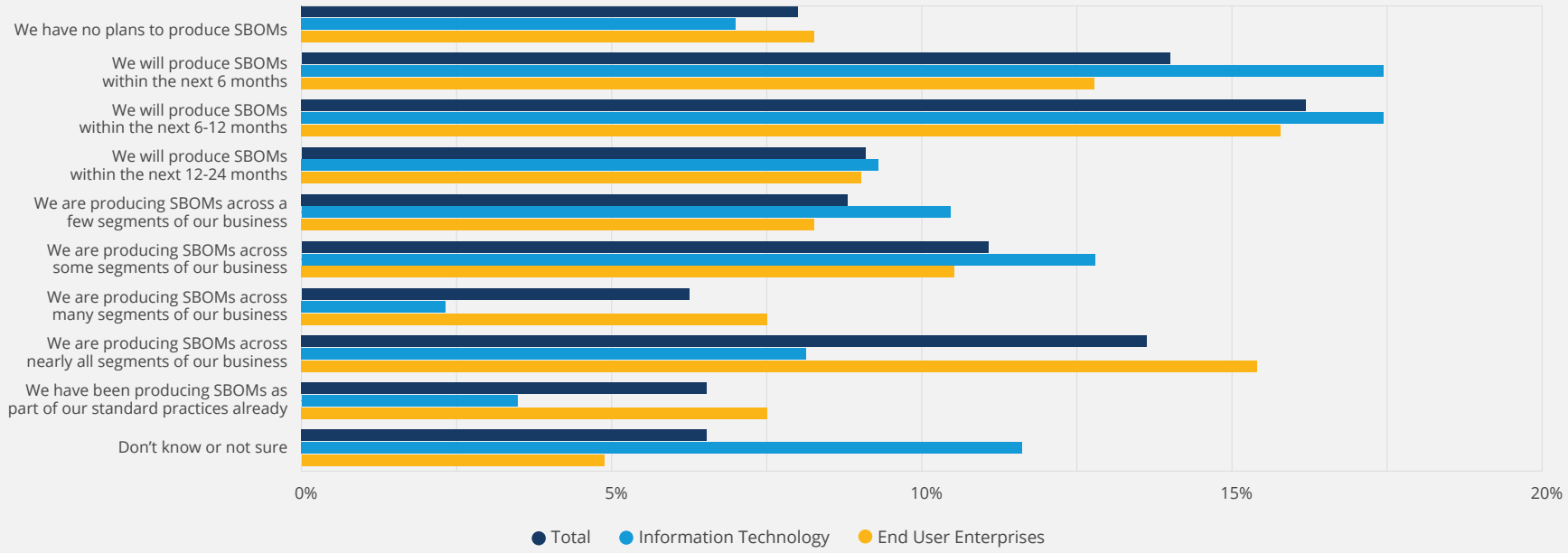
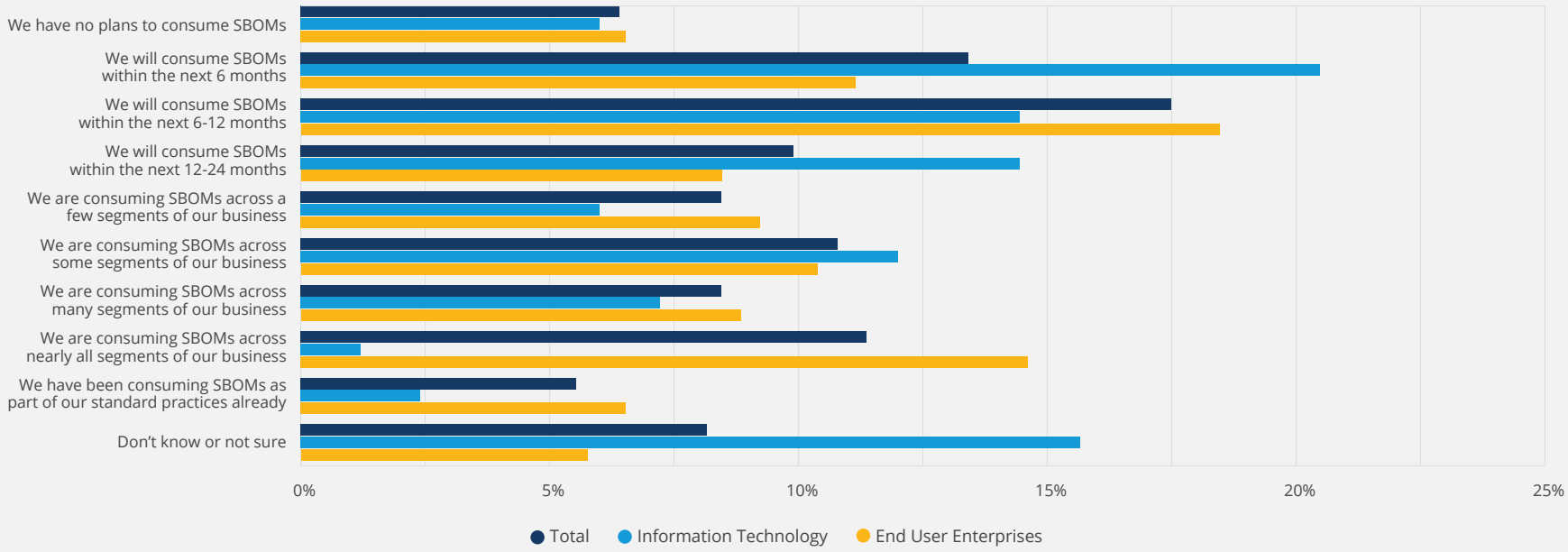


図 A20

SBOMの使用に関するあなたの会社の計画について教えてください。

（1つ選択） | 業種別に集計 | 回答数 =343



免責事項（原文および参考訳）

This report is provided “as is.” The Linux Foundation and its authors, contributors, and sponsors expressly disclaim any warranties (express, implied, or otherwise), including implied warranties of merchantability, non-infringement, fitness for a particular purpose, or title, related to this report. In no event will the Linux Foundation and its authors, contributors, and sponsors be liable to any other party for lost profits or any form of indirect, special, incidental, or consequential damages of any character from any causes of action of any kind with respect to this report, whether based on breach of contract, tort (including negligence), or otherwise, and whether or not they have been advised of the possibility of such damages. Sponsorship of the creation of this report does not constitute an endorsement of its findings by any of its sponsors.

本報告書は、「現状有姿(as is)」で提供されます。The Linux Foundation (LF)、その著者、コントリビューター、およびスポンサーは、本報告書に関連した、商品適格性、非侵害、特定の目的への適合性、または権原に関する暗黙の保証を含む一切の保証（明示的なもの、黙示的なもの、その他）を明示的に否認します。また、いかなる場合も、The Linux Foundation、その著者、コントリビューター、スポンサーは、本報告書に関連したいかなる種類の訴訟原因による利益の滅失、またはあらゆる形態の間接的、特定的、不随的、あるいは結果的な損害について、他者に対して一切の責任を負いません。契約違反、不法行為（過失を含む）、またはその他に基づくかどうか、およびそのような損害の可能性について知らされていたかどうかに関わりません。本報告書のスポンサーであることは、スポンサー企業による調査結果の承認を意味するものではありません。

twitter.com/linuxfoundation

facebook.com/TheLinuxFoundation

linkedin.com/company/the-linux-foundation

youtube.com/user/TheLinuxFoundation

提携先:

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

OPENCHAIN

SPDX

THE LINUX FOUNDATION | Research

Linux Foundation Researchは、拡大するオープンソースコラボレーションの規模を調査し、オープンソースプロジェクトの新たな技術トレンド、ベストプラクティス、およびグローバルな影響に関する洞察を提供します。

Stephen Hendrick,"2021 State of Software Bill of Materials(SBOM)Readiness","Jim Zemlinによる序文、The Linux Foundation、2022年1月