Ponemon INSTITUTE

# ソフトウェア・サプライチェーンの セキュリティ・リスクの現状

## 委託元：ブラック・ダック

独立調査実施：Ponemon Institute LLC

発行日：2024 年 5 月

**ソフトウェア・サプライチェーンのセキュリティ・リスクの現状**
Ponemon Institute 作成
2024 年 5 月

## パート 1. はじめに

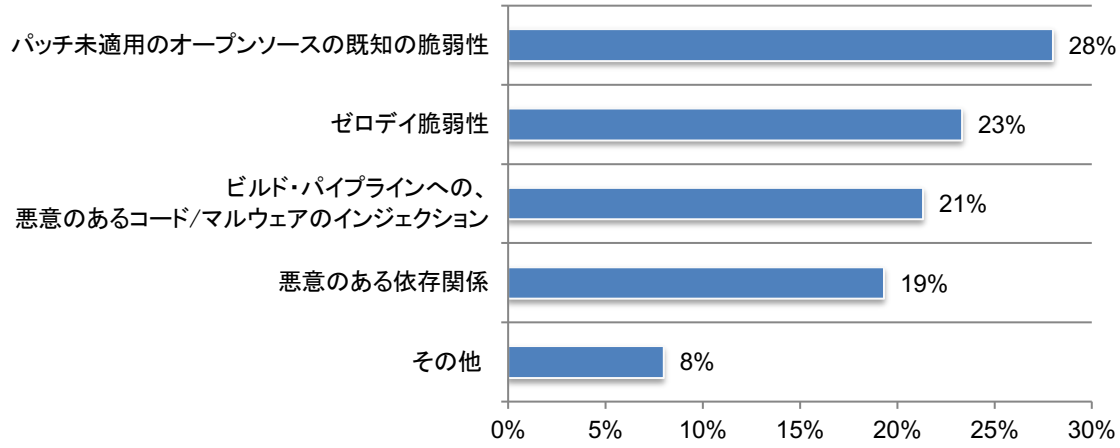
本調査の目的は、サプライチェーンにおけるソフトウエア・セキュリティ・リスクを低減するために組織の備えがどの程度進んでいるかを把握することです。Ponemon Institute は、ブラック・ダックの委託を受け、セキュアなソフトウェア・サプライチェーンの実現に取り組んでいる組織内で組織のソフトウェア・サプライチェーンのセキュリティ戦略に一定の責任を持つ立場にある IT 担当者および IT セキュリティ担当者 1,278 名を対象に調査を実施しました。対象地域/国は、北米（613 人）、ヨーロッパ/中東/アフリカ地域（362 人）、日本（303 人）です。

米国立標準技術研究所（NIST）によると、**ソフトウェア・サプライチェーン攻撃は、マルウェアを仕込むような高度なものからパッチ未適用の脆弱性を日和見的に悪用するような単純なものまでさまざまです。**悪意のあるコードが組織のシステムに入り込むと、ハッカーに機密データへのアクセスを許す、またはコードの侵害によって顧客へのアクセスを許してしまうことがあります。その結果、ランサムウェア攻撃やその他の悪意のあるインシデントが発生する可能性があります。通常、攻撃者はサプライチェーンの弱点を見つけ、その弱点を突いてサプライチェーンをさかのぼるか横断して本当の標的にたどり着き、対象のソフトウェア・サプライチェーン上のソフトウェアに悪意のあるコードを送り込むことができます。

**本調査における多くのソフトウェア・サプライチェーン攻撃の根本原因となっているのは脆弱性です。**ソフトウェア・サプライチェーンの攻撃や悪用による影響を受けたことがある組織は今回調査した組織の 59%にのぼり、これらの回答者の 54%が過去 1 年間に攻撃が発生したと答えています。

図 1 に示すように、攻撃や悪用の根本的な原因については、回答者の 28%がパッチ未適用の既知のオープンソース脆弱性、23%がゼロデイ脆弱性の結果であると答えています。これらの組織の 50%は攻撃への対応に 1 ヶ月以上を要しました。

**図 1：攻撃や悪用の根本原因は何でしたか？**



**調査結果に基づく、ソフトウェア・サプライチェーンのリスクを軽減するための推奨事項**

**アプリケーションのすべての構成要素（特にサードパーティ製）を可視化する。**その他のアクションとして、実行中のアプリケーションの脅威に対する継続的な監視、提供されたソフトウェア部品表（SBOM）と既知の悪意のあるパッケージおよびマルウェアとの比較、実行中のアプリケーションの動的解析、アプリケーションの依存関係のバイナリ解析などが挙げられます。

**ソースコード、ファイル、コンテナ、アーティファクト内のオープンソースの依存関係を検出、追跡、管理する。**ほとんどの組織はオープンソースの依存関係の範囲を把握していません。未管理の依存関係はセキュリティ上の脆弱性となり得ます。依存関係を管理することには、各コンポーネントに関連するライセンスを把握して準拠することが含まれます。オープンソース・ライブラリには、速やかに対処しなければプロジェクト全体を潜在的な脅威にさらしかねない脆弱性が含まれている可能性があります。依存関係を定期的に更新して監視することで、そのようなリスクを軽減できます。

**ソフトウェア・サプライチェーンのセキュリティを確保するには、継続的な監視によって新しい脆弱性のリスク・ステータスとそのリスクの重大度を検出することが重要であることを理解する。**セキュリティのリスクは常に変化し、進化しています。したがって、継続的な監視によって新しい脆弱性とリスクの重大度を検出することが重要です。

**AI が生成するコードには大きな利点がある一方で、評価とアセスメントを要するセキュリティ上のリスクがあることを理解する。**利点には、開発者の生産性向上や意思決定の自動化などがあります。AI の導入を成功させるには、組織は IP、セキュリティ・リスク、コードの品質を評価するプロセスを導入する必要があります。手作業による評価では不十分であり、かつ多大な労力がかかるため、評価は自動化する必要があります。

**SBOM を管理することはベストプラクティスであり、ソフトウェア・サプライチェーンのセキュリティ・プログラムを成功させる鍵である。**サードパーティの SBOM をインポートし、コンポーネントのリスクを評価します。オープンソース、独自開発、および商用ソフトウェアとの依存関係を含む SPDX あるいは CycloneDX の SBOM を生成します。業界、規制、または顧客の要件に合わせて SBOM のデータフィールドをカスタマイズします。CI/CD ツールとの統合と API により、SBOM を自動的に生成します。

## パート 2. 主な調査結果

このセクションでは、本レポートは以下のトピックに沿って構成し、調査結果を深く掘り下げていきます。なお、検証済みの全調査結果については、本レポートの付録に記載しています。

- ソフトウェア・サプライチェーンのセキュリティ対策の準備はどの程度整っているか
- ソフトウェア・サプライチェーン上のオープンソース・ソフトウェアはセキュアか
- ソフトウェア・サプライチェーン上の商用ソフトウェアのセキュリティ・リスク
- ソフトウェア・サプライチェーンのセキュリティ対策に対するセキュアなソフトウェア開発ライフサイクル（SSDLC）の役割
- SDLC における AI の活用と、それがソフトウェア・サプライチェーンのセキュリティにもたらす影響
- ソフトウェア・サプライチェーンのセキュリティ対策に対するソフトウェア部品表（SBOM）の役割

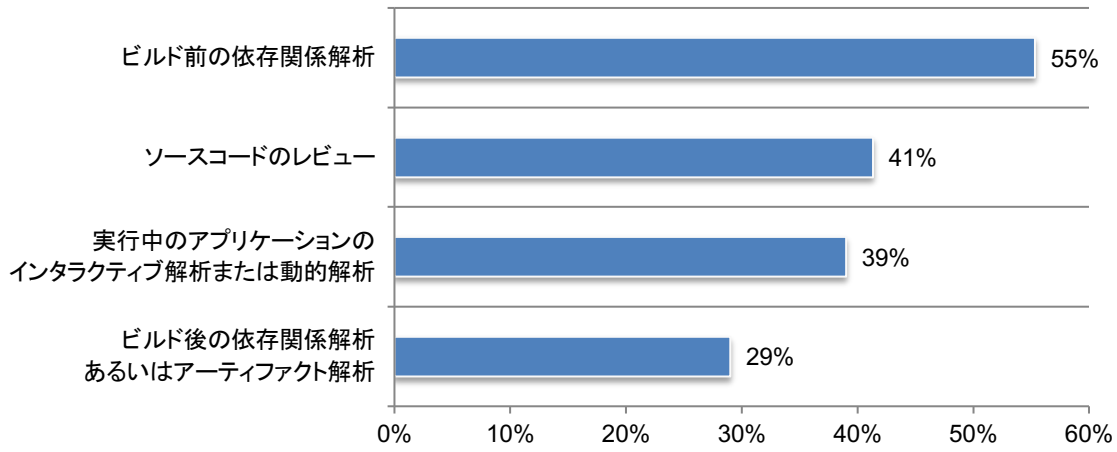
### ソフトウェア・サプライチェーンのセキュリティ対策の準備はどの程度整っているか

**悪意のあるコード/マルウェアのリスクを低減する取り組みに組織が力を入れていないことが、ソフトウェア・サプライチェーンのセキュリティを脅かしています。**経営幹部がソフトウェア・サプライチェーンにおける悪質なコードやマルウェアのリスクを軽減することに、非常に/大変熱心であると答えた人は回答者のわずか 39%しかいませんでした。悪意のあるパッケージが含まれていないか確認するために組織がソフトウェアを評価していると答えた人は回答者の 53%でした。

ビルドしたソフトウェアが悪意のあるパッケージの影響を受けないようにするために、ビルド前に依存関係を分析していると答えた人は回答者の 55%でした。図 2 に示すように、それ以外に行ったことは、ソースコードのレビュー（回答者の 41%）、実行中のアプリケーションのインタラクティブ解析または動的解析（回答者の 39%）などがあります。

組織が悪意のあるオープンソース・パッケージ（例：タイポスクワッティング、依存関係かく乱やブランド・ジャッキングなどを介して注入されたもの）から保護するためのプロセスを導入していると答えた人は回答者のわずか 45%でした。

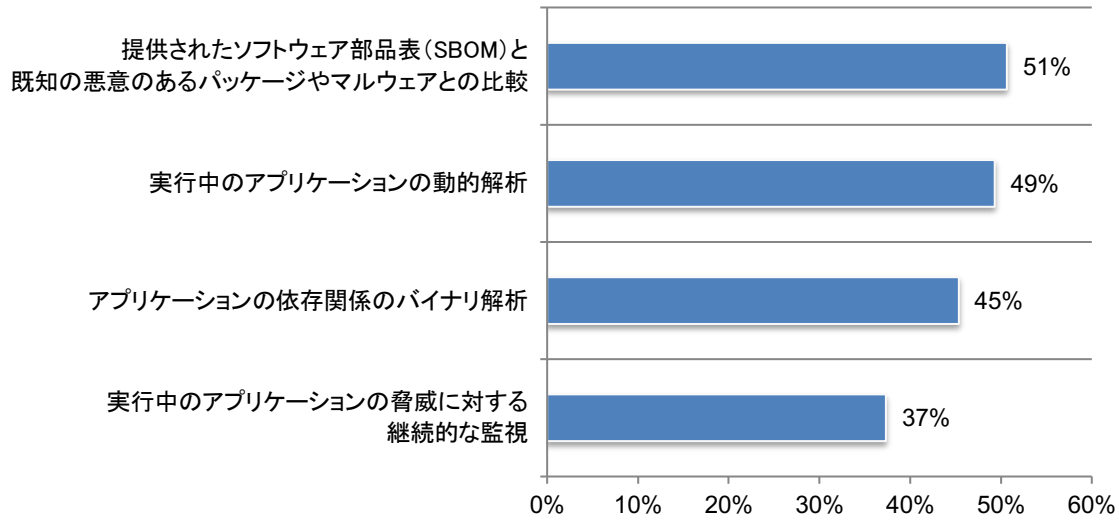
**図 2：あなたが所属する組織では、ビルドしたソフトウェアが悪意のあるパッケージの影響を受けないようにするために、ソフトウェアをどのように評価していますか？**
複数回答可



**ソフトウェア・アップデートにマルウェアを仕込むのは SolarWinds を通して行われたソフトウェア・サプライチェーン攻撃で利用された手法であり、サードパーティ製ソフトウェアを評価することの重要性を裏付けるものです。**マルウェアの有無についてサードパーティ製ソフトウェアを評価していると答えた人は回答者の 63%でした。

図 3 に示すように、マルウェアの有無についてサードパーティ製ソフトウェアを評価するために取られる手段には、提供されたソフトウェア部品表（SBOM）と既知の悪意のあるパッケージやマルウェアとの比較（回答者の 51%）、実行中のアプリケーションの動的解析（回答者の 49%）、アプリケーションの依存関係のバイナリ解析（回答者の 45%）があります。実行中のアプリケーションの脅威を継続的に監視していると答えた人は回答者のわずか 37%でした。

**図 3：あなたが所属する組織では、マルウェアの有無についてサードパーティ製のソフトウェアやアーティファクトをどのように評価していますか？**
複数回答可



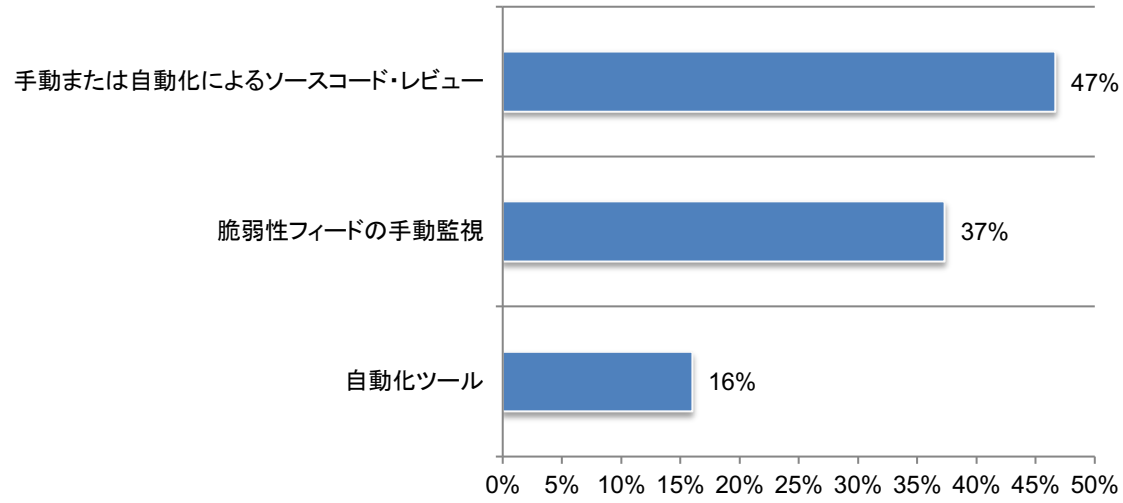

**ソフトウェア・サプライチェーンのセキュリティを確保するのに、予算またはその他のリソースが十分でないと考えられています。**SolarWinds や Kaseya のようなサプライチェーンの侵害によってソフトウェア・サプライチェーンのセキュリティへの投資が増加したと答えた人は回答者の 45%にのぼる一方で、サプライチェーンのセキュリティ対策のための予算や人員が十分である/必要以上確保されていると回答した人は 38%に過ぎません。

本調査に参加した組織の 2024 年の平均 IT 予算は 2 億 8,200 万ドルでした。平均で 25%（7,050 万ドル）が IT セキュリティに、19%（1,340 万ドル）がサプライチェーンのセキュリティ対策（技術、セキュリティ人材、サービスへの投資）に割り当てられます。

**脆弱性はソフトウェア・サプライチェーンを危険にさらします。**所属組織のソフトウェアの脆弱性を突く攻撃の検知と対応について「非常に/大変成果をあげている」と答えた人は 38%に過ぎません。回答者のほぼ半数(47%)が、重大なソフトウェアの脆弱性に対応するには少なくとも 1 ヶ月から 6 ヶ月以上かかると回答しています。

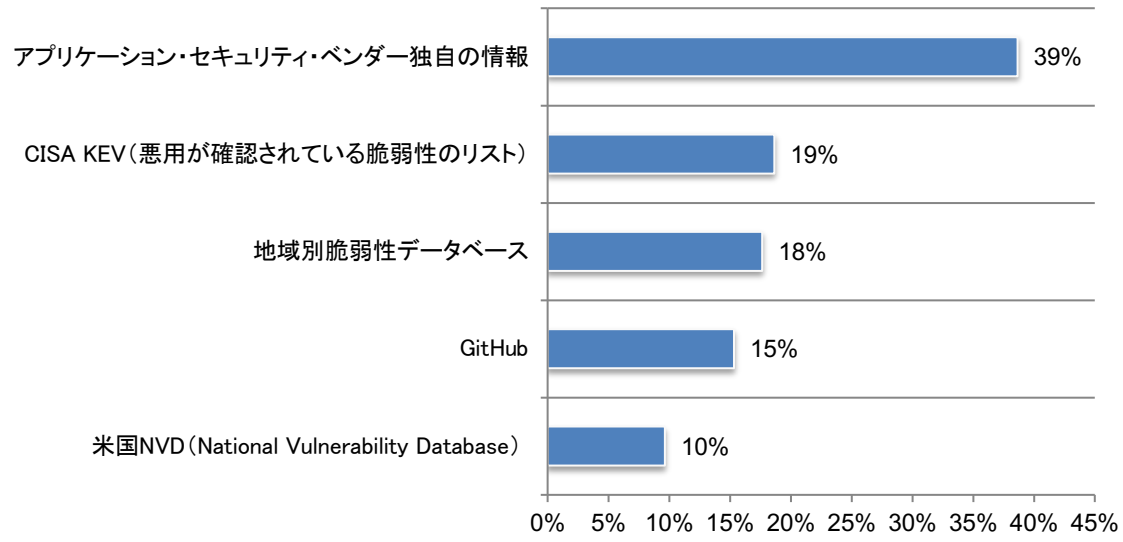
図 4 に示すように、ソフトウェアの新たな脆弱性を監視するために、所属組織で手動または自動化ソースコード・レビューを使用していると答えた人は回答者の 47%にのぼります。回答者の 37%が、脆弱性フィードを手動で監視していると答えています。よく知られている通り、手作業による追跡は不十分で手間もかかります。人員不足のため、自動化ツールの導入を検討することが重要です。

**図 4:あなたが所属する組織では、ソフトウェアに新たな脆弱性が生じていないかをどのように監視していますか?**




**多くの組織は、ソフトウェアの脆弱性を特定するための情報源としてアプリケーション・セキュリティ・ベンダー独自の情報に頼っています。**このことは、組織がリスクを軽減するためにソフトウェアの脆弱性を特定することに対してそれほど積極的でない(あまり関与していない)ことを示しているのかもしれません。図 5 に示すように、回答者の 39%が、ソフトウェアの脆弱性情報の情報源は、各アプリケーション・セキュリティ・ベンダー独自の情報であると答えています。

**図 5:あなたが所属する組織のソフトウェアの脆弱性に関する情報源は何ですか?**
複数回答不可



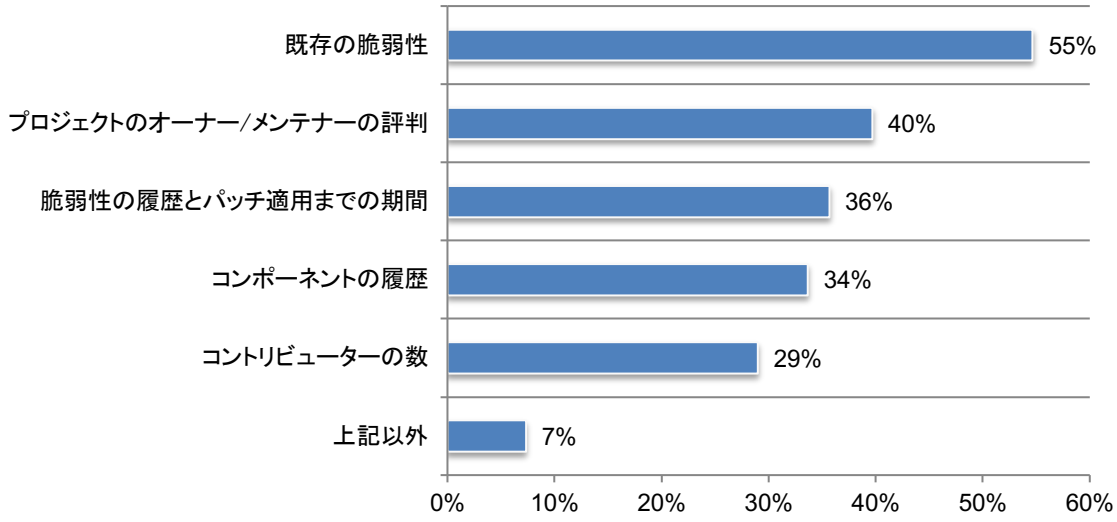
## ソフトウェア・サプライチェーン上のオープンソース・ソフトウェアはセキュアか

**オープンソース・ソフトウェアの脆弱性は、ソフトウェア・サプライチェーンのセキュリティに対するもう1つの深刻な脅威です。**所属する組織でオープンソース・ソフトウェアを使用していると答えた人は回答者の 65%にのぼります。一方で、組織のサプライチェーンにおけるオープンソース・ソフトウェアのセキュリティ対策が「非常に/大変成果をあげている」と答えた人は回答者の半数以下（47%）でした。

2024 年で 9 回目の発行を迎えた「オープンソース・セキュリティ&リスク分析（OSSRA）」年次レポートは、17 業界にわたる 1,000 以上のコードベースで見つかった脆弱性とライセンスの競合を調査しています。2024 年の OSSRA レポートによると、調査されたコードベースの 84%に少なくとも 1 つのオープンソースの脆弱性が見つかりました。

図 6 に示すように、オープンソース・コンポーネントのセキュリティの評価に使用される主な 3 つの項目は、既存の脆弱性（回答者の 55%）、プロジェクトのオーナー/メンテナーの評判（回答者の 40%）、脆弱性の履歴とパッチ適用までの期間（回答者の 36%）でした。

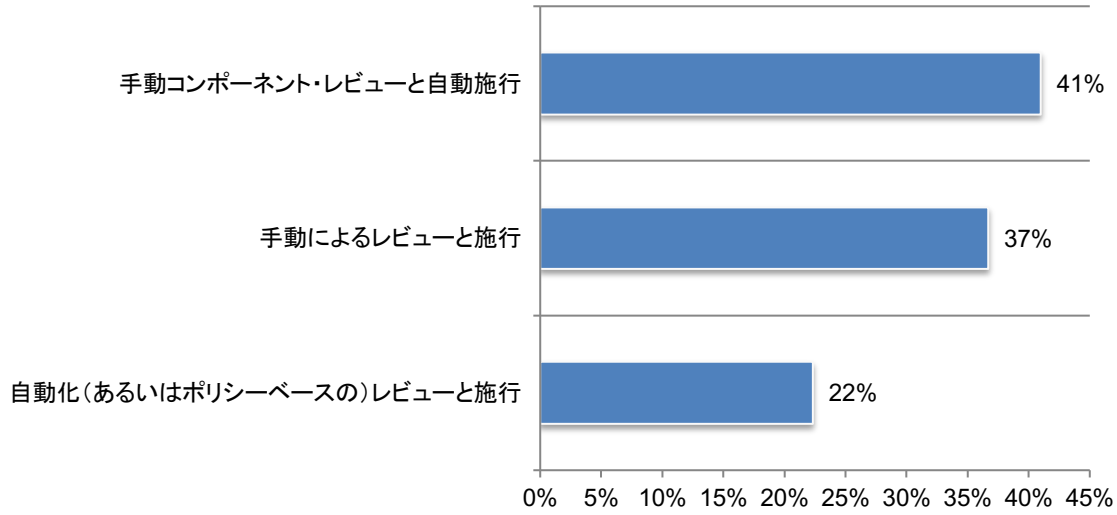
**図 6：オープンソース・コンポーネントのセキュリティの評価に使用している項目はどれですか？**
2 つ選択可



**オープンソースの依存関係を承認または禁止する方法として自動化を採用している組織は少数です。**オープンソースの依存関係とは、ソフトウェア・プロジェクトが機能するために依存している外部のライブラリ、フレームワーク、またはモジュールのことです。これらのコンポーネントは他の個人やグループによって個別に開発され、誰でも使用、変更、配布できるようになっています。オープンソースの依存関係を使用する利点は、ソフトウェア開発にかかる時間を短縮できることです。一方、その使用にはセキュリティ上のリスクもあります。特に、依存関係が追跡されていない、または未知である場合、リスクは高まります。自動化を利用すると、依存関係の追跡と特定をより効率的かつ効果的に行えるようになります。

組織でオープンソースの依存関係を承認または禁止する方法を導入していると答えたのは回答者のわずか 48%でした。オープンソースの依存関係を承認または禁止する方法としては、手動コンポーネント・レビューと自動施行を使用している組織が回答者の 41%を占め、次いで手動によるレビューと施行を使用していると答えた組織が 37%でした。図 7 に示すように、自動化による/ポリシーベースのレビューと施行を使用している組織は 22%に過ぎませんでした。

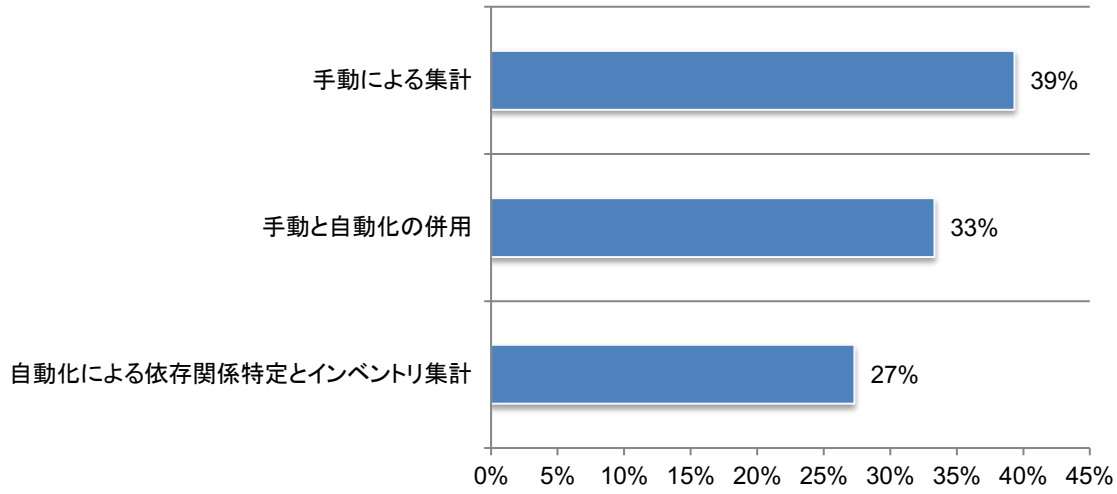
**図 7:オープンソースの依存関係を承認または禁止する方法に最も近いものはどれですか？**
複数回答不可



**ほとんどの組織は、自分の組織がどの程度オープンソースに依存しているかを把握していません。**管理されていない依存関係は、セキュリティ上のリスクをもたらす可能性があります。オープンソース・ライブラリには、速やかに対処しなければプロジェクト全体を潜在的な脅威にさらしかねない脆弱性が含まれている可能性があります。依存関係を定期的な更新や監視によって、そのようなリスクを軽減できます。

図 8 に示すように、組織がオープンソースの依存関係のインベントリを管理していると答えた回答者はわずか 39%でした。インベントリの管理方法としては、手動による集計を使用している人が回答者の 39%、次いで手動と自動化を併用している人が回答者の 33%でした。

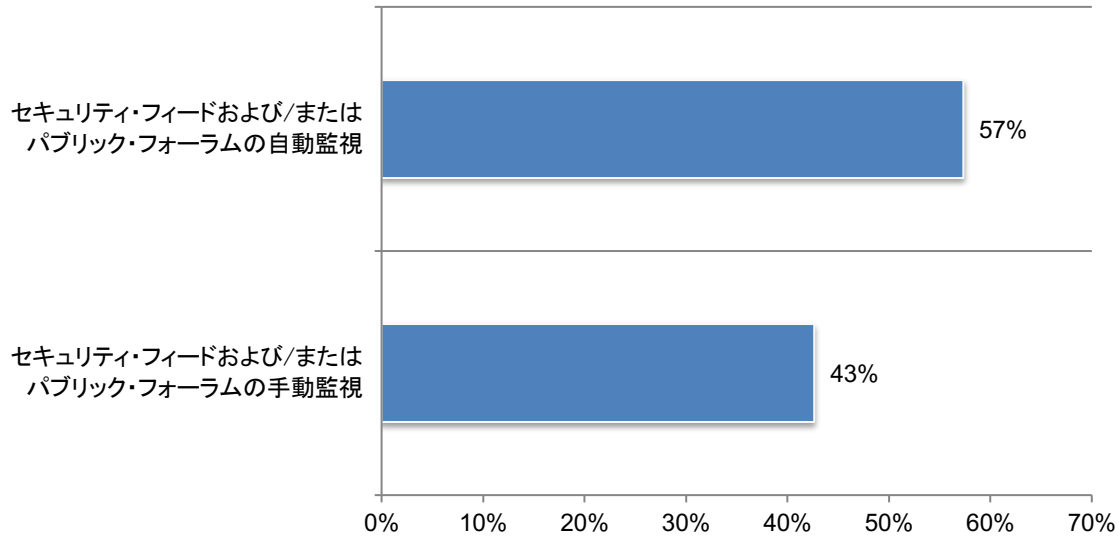
**図 8:このインベントリを管理するために使用しているプロセスについて、最も近いものはどれですか？**



**ソフトウェア・サプライチェーンのセキュリティを確保するには、継続的な監視によって新しい脆弱性のリスク・ステータスとそのリスクの重大度を検出することが重要です。**セキュリティのリスクは常に変化し、進化しています。したがって、継続的な監視によって新しい脆弱性とリスクの重大度を検出することが重要です。

オープンソースの依存関係に新たな脆弱性が生じていないかを継続的に監視している組織は少数です（回答者の 41%）。これらの回答者のうち、セキュリティ・フィードおよび/またはパブリック・フォーラムの自動監視を行っていると述べたのは 57%、セキュリティ・フィードおよび/またはパブリック・フォーラムの手動監視を行っていると述べたのは 43%でした（図 9 参照）。

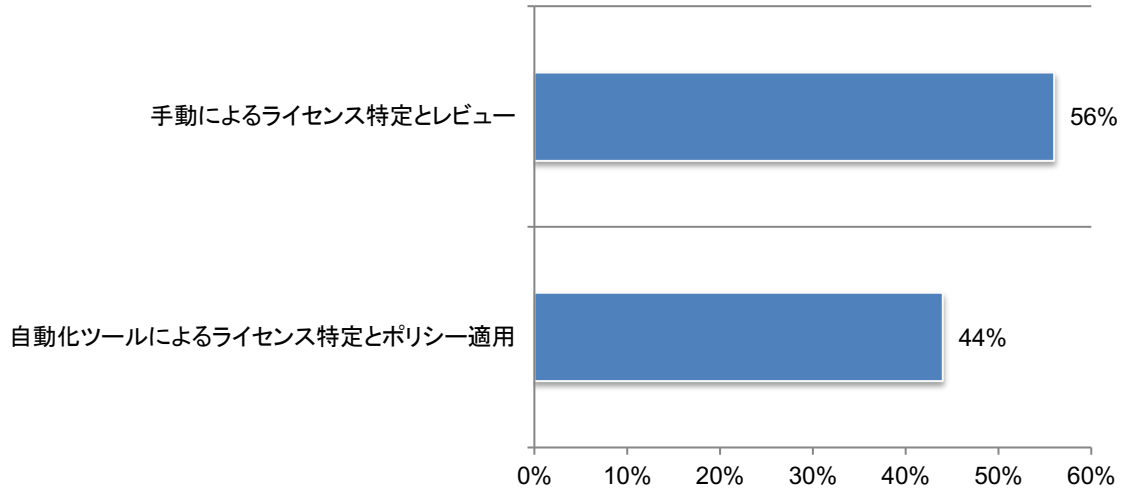
**図 9：あなたが所属する組織では、オープンソースの依存関係に新たな脆弱性が生じていないかをどのような方法で継続的に監視していますか？**
複数回答不可



**依存関係を管理することには、各コンポーネントに関連するライセンスを把握して準拠することが含まれます。**使用している依存関係に関連する IP/ライセンス義務を追跡していると答えた回答者はわずか 40%でした。2024 年の OSSRA レポートによれば、オープンソース・コードベースの 53%にライセンスの競合が含まれていました。

図 10 に、その 40%の回答者が IP/ライセンス義務を追跡するために使用したプロセスを示しています。追跡のために使用されている主な方法は、手動によるライセンス特定とレビュー（回答者の 56%）と、自動化ツールによるライセンス特定とポリシー適用（回答者の 44%）です。

**図 10：IP/ライセンス義務を追跡するために使用しているプロセスについて、最も近いのはどれですか？**
複数回答不可



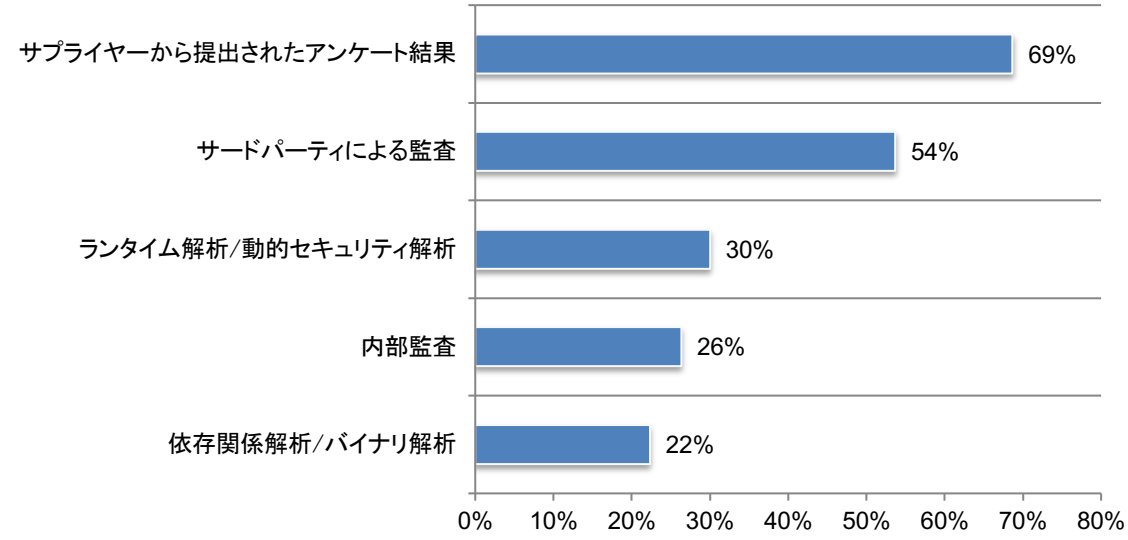
## ソフトウェア・サプライチェーン上の商用ソフトウェアのセキュリティ・リスク

**商用ソフトウェアのリスク評価に失敗すると、ソフトウェアのサプライチェーンにセキュリティ上の脅威がもたらされます。**所属組織が商用ソフトウェアを活用していると答えた人は回答者の 46%にのぼります。このうち、組織が商用ソフトウェアのセキュリティ評価に非常に/大変熱心だと答えた回答者は 41%に過ぎません。

図 11 に示すように、使用または調達した商用ソフトウェアのリスク評価を組織で実施していると答えた人は回答者のわずか 44%でした。リスク評価の方法については、回答者の 69%がサプライヤーから提出されたアンケート結果に依存しており、回答者の 54%がサードパーティによる監査を実施していると答えています。

商用ソフトウェア・サプライヤーに対するこのようなレビューは、最初の契約交渉時に 1 回だけ行うか（回答者の 29%）、契約更新時に行うか（回答者の 22%）、1 回も行われない場合もあります（回答者の 21%）。

**図 11：どのような種類の商用ソフトウェアのリスク評価を、使用または調達しましたか？**
複数回答可



**ソフトウェア・サプライチェーンのセキュリティ対策に対する SSDLC の役割**

**回答者の 54%が、コードのセキュリティと品質についてのレビューを行っていると答えています。**セキュアなソフトウェア開発ライフサイクル（SSDLC）は、ソフトウェア製品を安全かつセキュアに開発するためのプロセスです。これはセキュリティを最優先事項に置いてソフトウェア・アプリケーションを構築するための体系立った手法です。図 12 は、回答者の 54%がセキュリティと品質に問題がないか確認するために利用しているコード・レビューの方法を示しています。コード・レビューに最も多く利用されている方法は手動コード・レビュー（回答者の 56%）と静的解析（回答者の 49%）です。

**図 12：開発チームは、セキュリティや品質に問題がないか確認するために、どのような方法でコード・レビューを行っていますか？**
複数回答可

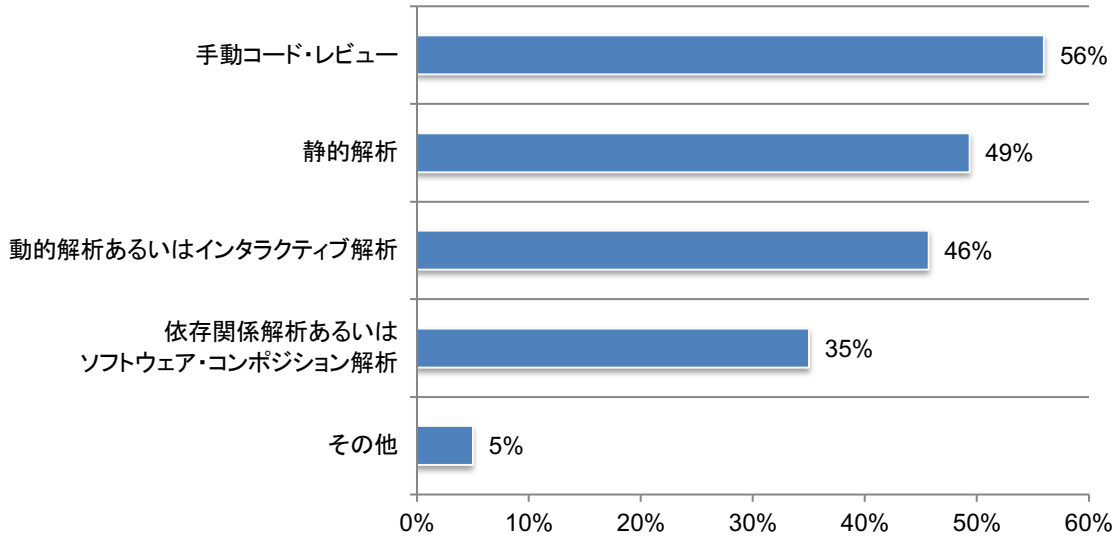



図 13 に示すように、SDLC における開発チームによるセキュリティ解析が最も行われる段階として最も多いのはコーディング（回答者の 64%）、チェックイン前（回答者の 58%）、ビルド（回答者の 56%）です。

**図 13：開発チームは、SSDLC のどの段階でセキュリティ分析を実施していますか？**
複数回答可

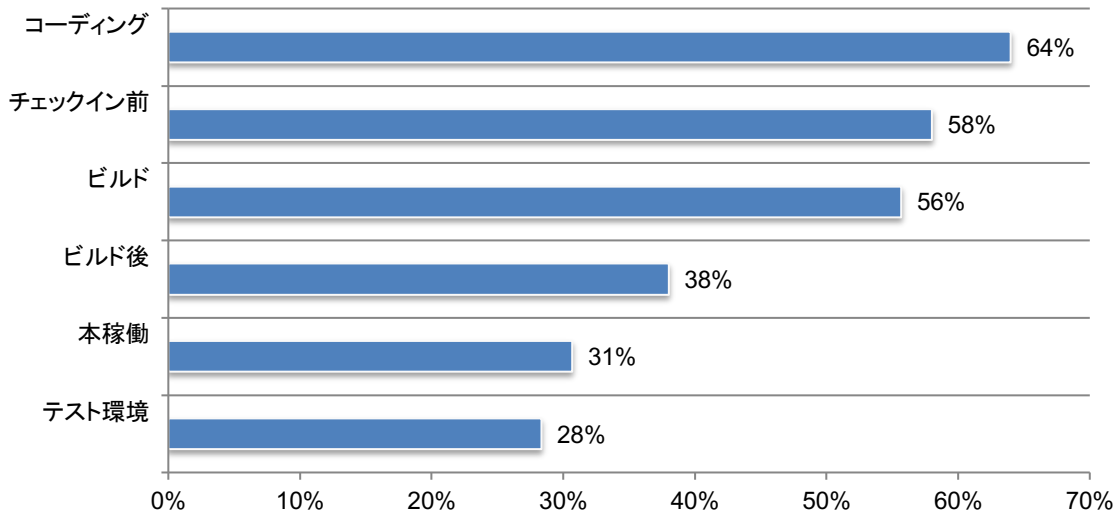


図 14 に示すように、SSDLC の完全性を保護する方法としてビルド・ツールのアクセス保護を使用している人は回答者の 58%、承認済みの依存関係の内部/プライベート・リポジトリ（オープンソース・コンポーネントを含む）を使用している人は 54%、テスト環境およびステージング環境のアクセス保護を使用している人は 48%いました。

**図 14：あなたが所属する組織では、SSDLC の完全性をどのように保護していますか？**
複数回答可

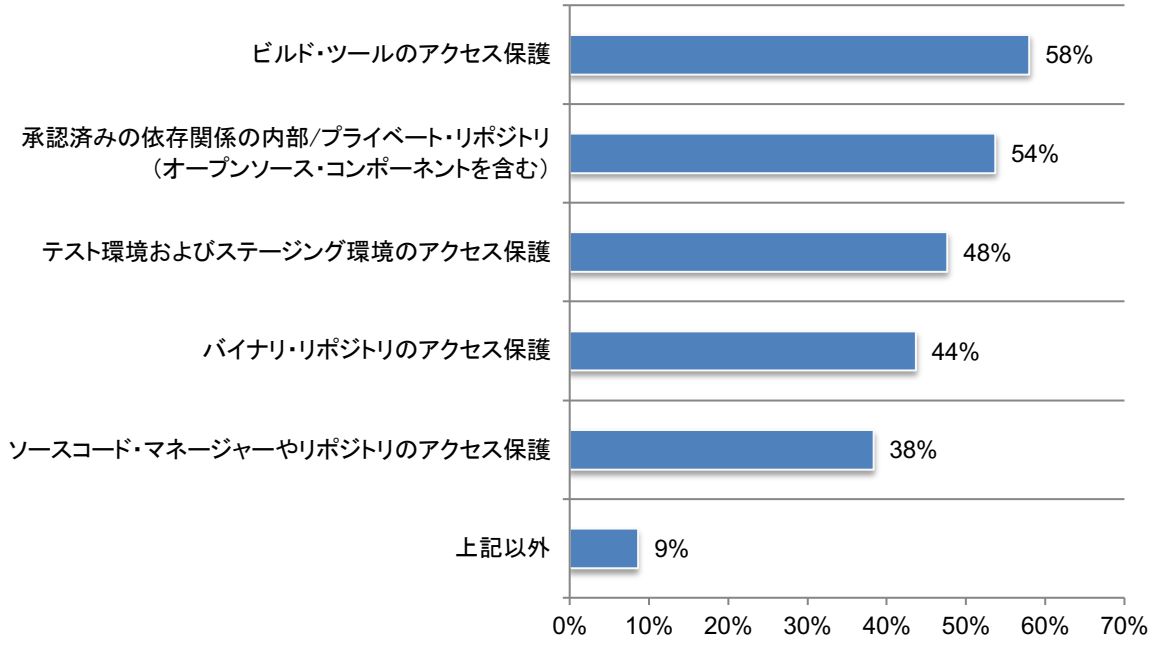


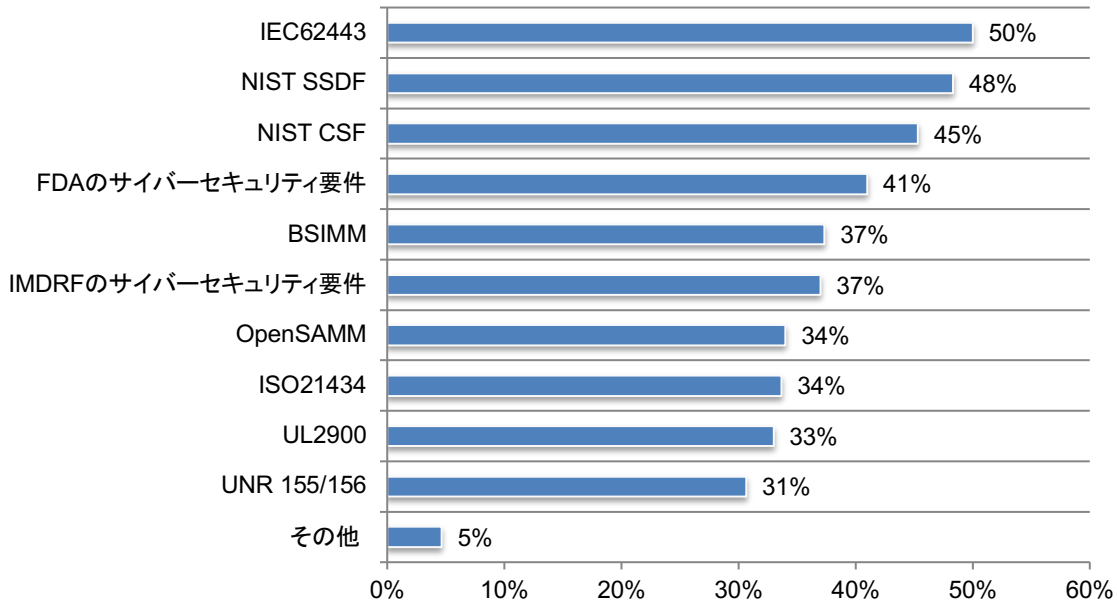
**図 15 に示すように、セキュアなソフトウェア開発について標準モデルに従っていると答えた人は回答者の 57%にのぼります。**国際規格として、IEC（国際電気標準会議）の IEC 62443 シリーズの規格は関係する 89 の国家の委員会が共通の規格に合意した規格制定プロセスの結果です。組織が IEC 62443 のモデルに従っていると答えた人は回答者の 50%にのぼります。

NIST SSDF（セキュアなソフトウェア開発フレームワーク）は、BSA、OWASP、SAFECode などの団体から提供された確立されたセキュアなソフトウェア開発プラクティスのドキュメントを元に、基本的かつ堅固かつセキュアなソフトウェア開発プラクティスを集約したものです。

ソフトウェア・メーカーは SSDF のプラクティスに従うことで、リリースするソフトウェアの脆弱性の数を減らし、未検出または未対処の脆弱性が悪用された場合の潜在的な影響を軽減し、再発を防止するために脆弱性の根本原因に対処する支援を受けられます。また、SSDF はセキュアなソフトウェア開発プラクティスを記述するための共通言語を提供するため、ソフトウェアのメーカーと利用者は SSDF を利用して調達プロセスやその他の管理活動におけるコミュニケーションを促進できます。組織が NIST SSDF に従っていると答えた人は回答者の 48%にのぼります。

NIST CSF（サイバーセキュリティ・フレームワーク）は、サイバーセキュリティ上のリスクを低減するためのガイダンスを提供します。NIST は CSF のコア・ガイドラインを拡充し、関連リソースを開発することで利用者がフレームワークを最大限に活用できるようにしました。これらのリソースはさまざまな対象者の状況に合った道筋を示すように設計されており、フレームワークを実行に移しやすくしています。組織が NIST CSF に従っていると答えた人は回答者の 45%にのぼります。

**図 15：あなたが所属する組織では、セキュアなソフトウェア開発についてどの標準モデルに従っていますか？**
複数回答可

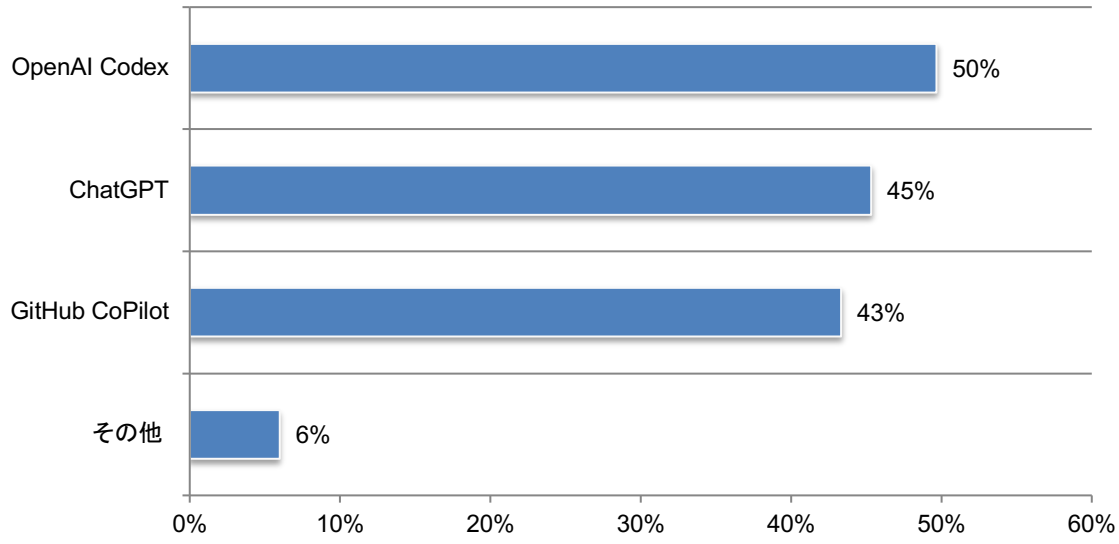


**SDLC における AI の活用と、それがソフトウェア・サプライチェーンのセキュリティにもたらす影響**

**SDLC における AI の活用は急速に広がっています。**開発チームがコードの生成に AI ツールを活用していると答えた回答者は 52%にのぼります。ブラック・ダックのソフトウェア・セキュリティ・アドボケイトを務める Charlotte Freeman によると、組織は知的財産の保護、コード品質の確保、倫理的配慮を行いながら、AI による変革の可能性を取り入れる必要があります。AI を戦略的に導入することで、組織は効率化を進め、意思決定を自動化し、進化し続けるソフトウェア開発の分野で他社の一歩先を行くことができます。[1]

図 16 は、開発チームがコード生成に使用している AI ツールの一覧を示しています。先ほどの回答者 52%のうち、OpenAI Codex を使用していると答えた人が 50%、ChatGPT を使用していると答えた人が 45%います。

**図 16：開発チームはどの AI ツールを使っていますか？**
複数回答可

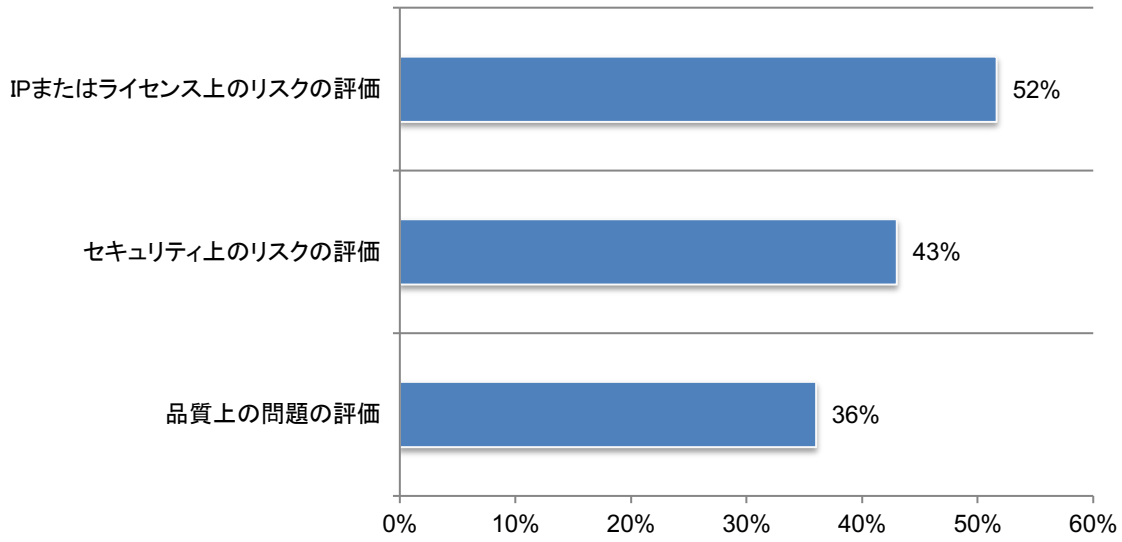



[1] 2024 年 2 月 19 日公開の Charlotte Freeman が執筆したブラック・ダックのブログ記事『How AI Is Changing Software's Role in the SDLC』。

**AI には大きな利点がある一方で、評価とアセスメントを要するセキュリティ上のリスクもあります。**
AI の導入を成功させるには、組織は IP、セキュリティ・リスク、コードの品質を評価する必要があります。しかしながら、AI によって生成されたコードを評価するプロセスを導入している組織は 32%に過ぎません。

これらの回答者に最もよく使用されているプロセスは、IP またはライセンス・リスクに対する評価（52%）とセキュリティ・リスクに対する評価（43%）です（図 17 参照）。これらの評価を自動化して行っていると述べたのは回答者の 51%で、49%は手作業で行っています。

**図 17：AI によって生成されたコードを評価するために、どのようなプロセスを導入していますか？**
複数回答可

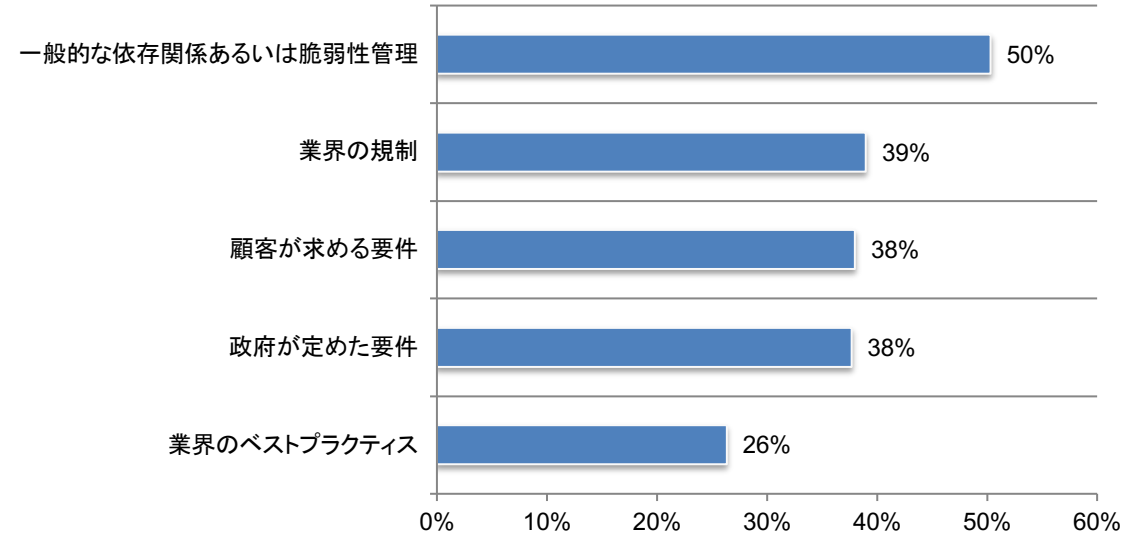


**ソフトウェア・サプライチェーンのセキュリティ対策に対するソフトウェア部品表（SBOM）の役割**

**SBOM はベストプラクティスであり、セキュアなソフトウェア・サプライチェーンを構築するために不可欠なものですが、SBOM を作成または生成していると回答した組織はわずか 35%に過ぎませんでした。**SBOM とは、ソフトウェア・コンポーネント構成要素のリストの入れ子構造のインベントリです。図 18 に示すように、SBOM を作成する主な理由は、一般的な依存関係/脆弱性管理（回答者の 50%）、業界の規制（回答者の 39%）、政府が定めた要件（回答者の 38%）です。

IP/ライセンスの競合を追跡し、回避することは極めて重要です。しかし、組織の法務/ガバナンスチームが SBOM の正確性を検証する役割を担っていると答えた回答者は 26%に過ぎず、その役割は主に配布を許可すること（回答者の 39%）と配布ルールを定めること（回答者の 37%）でした。

**図 18：あなたが所属する組織が SBOM を生成する理由は何ですか？**
複数回答可



**SBOM の作成について定期的なスケジュールが定められていないと、ソフトウェア・サプライチェーンのセキュリティに影響を与える可能性があります**。先ほどの回答者の 35%のうち、製品リリース時に SBOM を生成すると答えたのはわずか 20%でした。図 19 に示すように、「提供を求められたときはいつでも」と答えた人は回答者のわずか 21%でした。

**図 19：あなたが所属する組織では、どの程度の頻度で SBOM を生成していますか？**

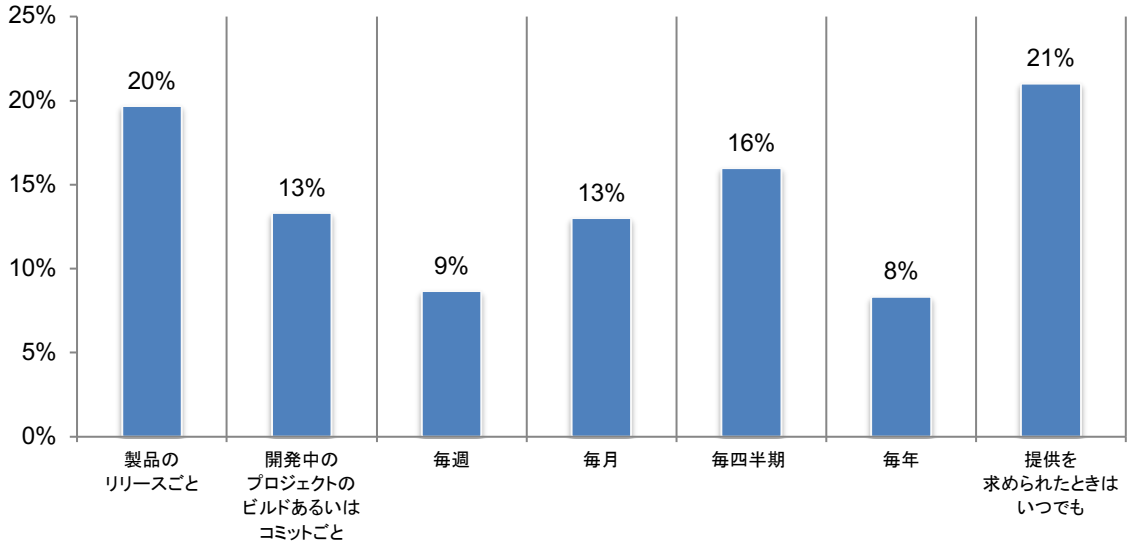
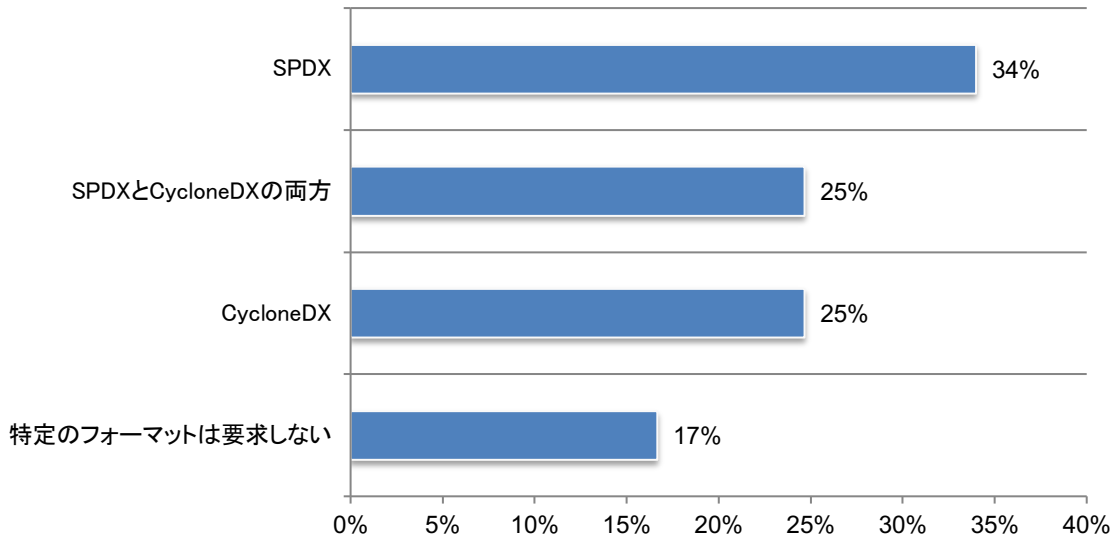



図 20 に示すように、SBOM の生成に最も多く使用されているフォーマットは、SPDX（回答者の 34%）、CycloneDX（回答者の 25%）、SPDX と Cyclone DX の両方（回答者の 25%）でした。特定のフォーマットは要求しないと答えた人は回答者の 17%です。

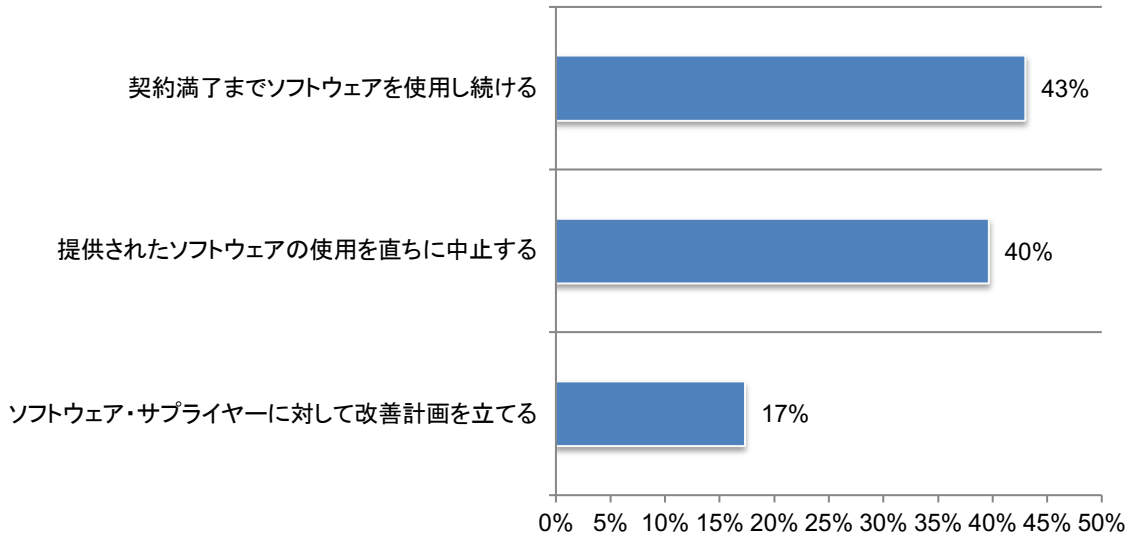
**図 20：リクエストした SBOM について、あなたが所属する組織が要求するフォーマットはどれですか？**



**リクエストした SBOM をサプライヤーが提供しない場合、提供されたソフトウェアの使用を直ちに中止すると答えたのは回答者のわずか 40%でした。**回答者の 29%がサプライヤーに SBOM をリクエストしており、最も多く要求されているフォーマットは SPDX（回答者の 34%）、CycloneDX（回答者の 25%）、SPDX と CycloneDX の両方（回答者の 25%）です。サプライヤーから提供される SBOM に脆弱性開示情報が含まれていると答えたのは回答者のわずか 34%でした。サプライヤーから提供された SBOM を組織で検証していると答えた人は回答者のわずか 40%でした。

図 21 に示すように、サプライヤーがリクエストした SBOM を提供しない場合、契約満了までソフトウェアを使用し続ける人は回答者の 43%、提供されたソフトウェアの使用を直ちに中止すると答えた人は回答者の 40%でした。ソフトウェア・サプライヤーに対する改善計画を立てると答えた回答者はわずか 17%に留まりました。

**図 21：あなたが所属する組織は、リクエストした SBOM を提供しないサプライヤーに対してどのように対処していますか？**



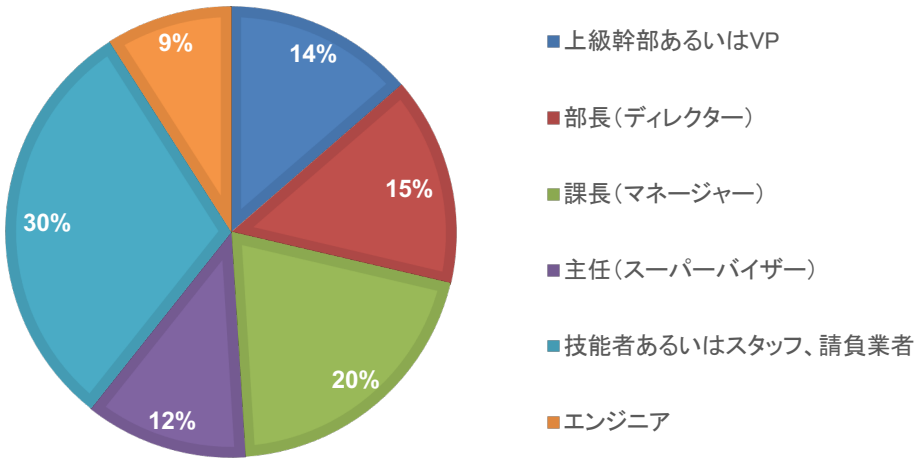
**パート 3. メソドロジー**

本調査のサンプル抽出枠として、セキュアなソフトウェア・サプライチェーンの実現に取り組んでいる組織内で、組織のソフトウェア・サプライチェーンのセキュリティ戦略に一定の責任を持つ立場にある IT 担当者および IT セキュリティ担当者 45,710 名を選択しました。表 1 から回答の総数は 1,456 件であったことが分かります。スクリーニングと信頼性チェックの結果、178 件の調査が却下されました。最終サンプルの回答数は 1,278 件（回答率は 3.4%）でした。

| **表 1：サンプル回答** | 度数 | 割合（%） |
|---|---|---|
| サンプル抽出枠 | 37,399 | 100.0% |
| 回答総数 | 1,456 | 3.8% |
| 却下/スクリーニングされた調査回答 | 178 | 0.5% |
| 最終サンプル | 1,278 | 3.4% |

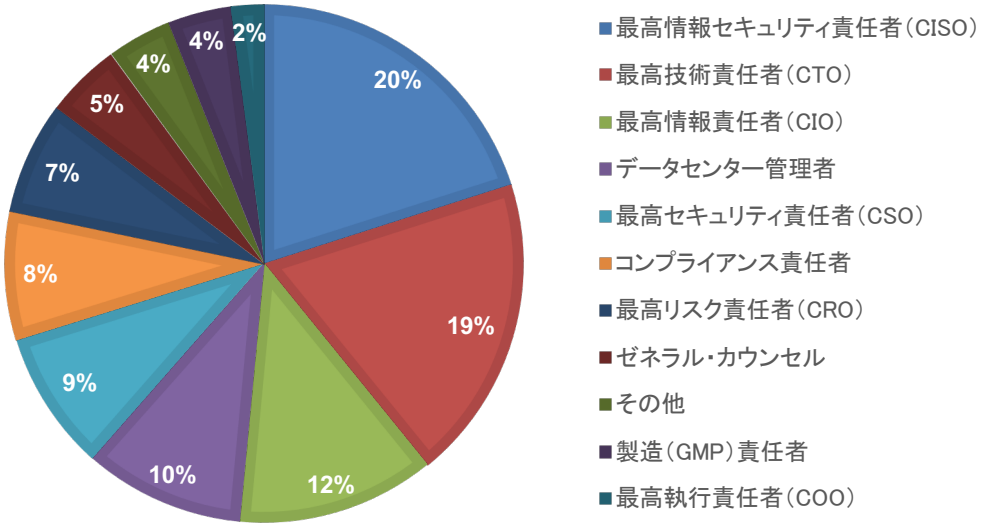
円グラフ 1 は、参加組織内の回答者の職位を示しています。意図的に、回答者の半数（51%）が管理階層以上になっています。最も多いのは「技術者/スタッフ/請負業者」で、回答者の 30%を占めています。

**円グラフ 1. 現在の職位**



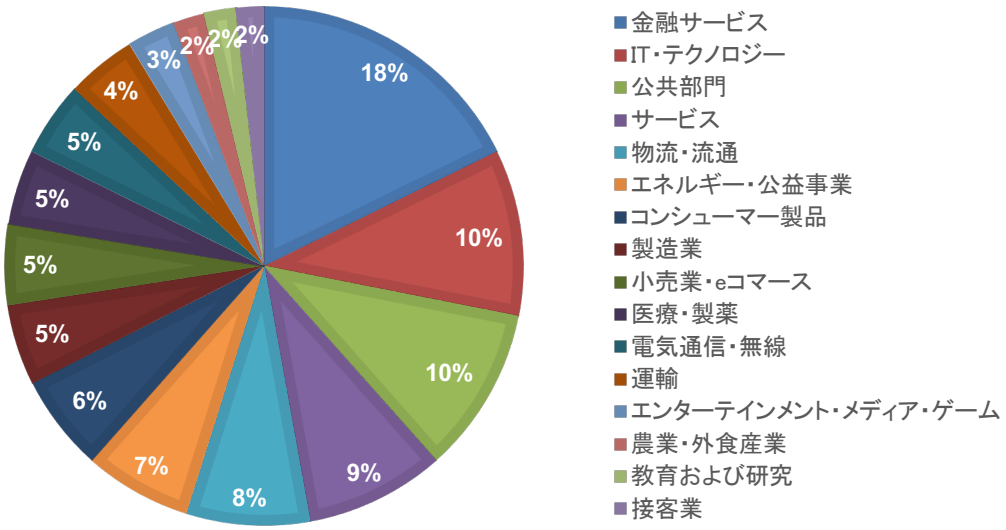
円グラフ 2 に示すように、回答者の直属の上司の役職については、最高情報セキュリティ責任者が 20%、最高技術責任者が 19%、最高情報責任者が 12%、データセンター管理者が 10%でした。

**円グラフ 2. 直属の上司**



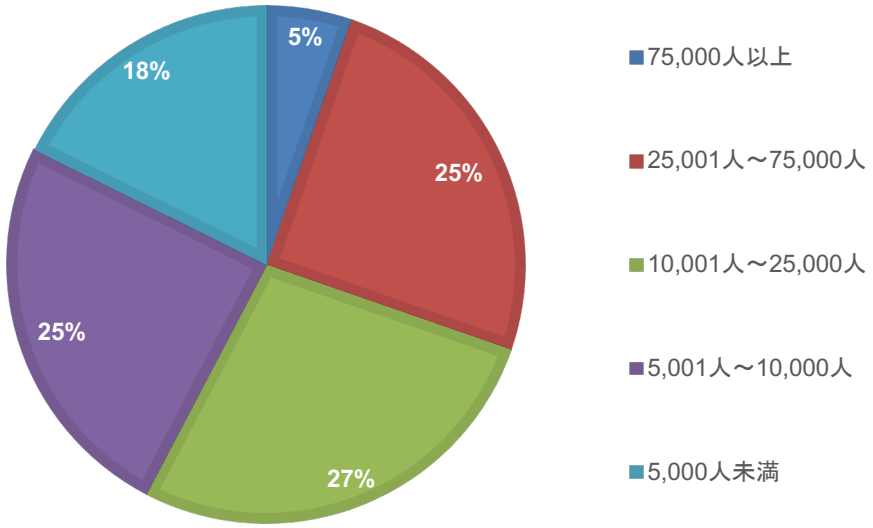

円グラフ 3 は、回答者の組織の業種を示しています。このグラフから、最も多い業種は金融サービス（18%）であることが分かります。金融サービスには、銀行、投資管理、保険、証券、決済、クレジット・カードが含まれます。次いで、IT・テクノロジー（回答者の 10%）、公共部門（同 10%）、サービス（同 9%）、物流（同 8%）、エネルギー・公益事業（同 7%）でした。

**円グラフ 3. 主な業種**



円グラフ 4 に示すように、回答者の半数以上（57%）は全世界の従業員数が 10,000 人を超える組織に所属しています。

**円グラフ 4.全世界の従業員数**




**パート 4. 本調査の注意事項**

調査結果から推論を導く際は、調査に内在する制限事項に十分留意する必要があります。ほとんどの Web ベースの調査には、以下に示す特有の制限事項があります。

- 非回答バイアス：現在の調査結果は、回答が返された調査のサンプルに基づいています。個人の代表サンプルに調査票を送付し、有効な回答を多数得ました。非回答に関するテストは実施していますが、回答をした人としなかった人との間で根本的な信念が大幅に異なっている可能性は常に存在します。

- サンプル抽出枠バイアス：精度は、連絡先情報と、連絡先リストが IT 担当者および IT セキュリティ担当者である個人をどの程度代表しているかに基づきます。また、調査結果にはマスコミ報道など外部のイベントのバイアスがかかる可能性があることも認識しています。最後に、Web ベースの回答収集方法を採用したことにより、郵送または電話による Web 以外の回答方法を採用した場合は異なるパターンの調査結果が得られた可能性もあります。

- 自己申告による結果：調査研究の品質は、対象者から得られた非公開の回答の完全性に依拠します。調査のプロセスに一定のチェック・バランスを組み込むことは可能ですが、対象者が正確な回答を提供していない可能性は常に存在します。

**付録：詳細な調査結果**

以下の表は、調査質問への回答の度数、または度数の割合（%）を示しています。すべての調査回答は2024年2月に収集されました。

| **調査回答** | 集計 |
|---|---|
| 総サンプル抽出枠 | 37,399 |
| 回答総数 | 1,456 |
| 却下された調査回答 | 178 |
| 最終サンプル | 1,278 |
| 回答率 | 3.4% |

**パート 1. スクリーニング**

| S1. 組織のソフトウエア・サプライチェーン・セキュリティ戦略の策定や実施について、どの程度の責任を負っていますか？ | 集計 |
|---|---|
| 戦略の全責任を負っている | 40% |
| 他者と責任を分担している | 60% |
| 責任はない（停止） | 0% |
| 合計 | 100% |

| S2. あなたが所属する組織は、セキュアなソフトウェア・サプライチェーンの実現にどの程度熱心ですか？ | 集計 |
|---|---|
| とても熱心である | 49% |
| 熱心である | 33% |
| 少し熱心である | 18% |
| 熱心ではない（停止） | 0% |
| 合計 | 100% |

| S3. 組織であなたが果たしている役割に最も近いものはどれですか？<br>回答を **1 つ**だけ選択してください。 | 集計 |
|---|---|
| 最高情報セキュリティ責任者（CISO） | 16% |
| 最高技術責任者（CTO） | 12% |
| 最高データ責任者（CDO） | 8% |
| 製品セキュリティ・アナリスト | 12% |
| DevSecOps チーム | 11% |
| セキュリティ・オペレーション・センター（SOC）責任者 | 12% |
| セキュリティ製品テスト | 8% |
| セキュリティ・エンジニアリング | 12% |
| リバース・エンジニア/脆弱性研究者 | 8% |
| 上記以外（中止） | 0% |
| 合計 | 100% |

**パート 2. セキュリティ態勢の背景**

| Q1. サプライチェーンのセキュリティ対策のために利用できるリソースは十分ですか？（1 =「十分でない」、10 =「必要以上」） | 集計 |
|---|---|
| 1 または 2 | 12% |
| 3 または 4 | 20% |
| 5 または 6 | 30% |
| 7 または 8 | 21% |
| 9 または 10 | 17% |
| 合計 | 100% |

| Q2. あなたが所属する組織のソフトウェア・サプライチェーンのセキュリティの**最高責任者**は誰ですか？回答を **1 つ**だけ選択してください。 | 集計 |
|---|---|
| 最高情報セキュリティ責任者（CISO） | 15% |
| 最高技術責任者（CTO） | 16% |
| 最高データ責任者（CDO） | 9% |
| 製品セキュリティ・アナリスト | 8% |
| DevSecOps チーム | 8% |
| セキュリティ・オペレーション・センター（SOC）責任者 | 7% |
| セキュリティ製品テスト | 8% |
| セキュリティ・エンジニアリング | 9% |
| リバース・エンジニア/脆弱性研究者 | 9% |
| 最高責任者にあたる 1 人の人物は存在しない | 11% |
| その他（具体的に記述してください） | 1% |
| 合計 | 100% |

| Q3. あなたが所属する組織はどのようなソフトウェアを開発していますか？最も当てはまるものを **1 つ**選択してください。 | 集計 |
|---|---|
| エンタープライズ・アプリケーション | 34% |
| Web アプリケーション | 30% |
| 商用（COTS）ソフトウェア | 28% |
| 組み込み/ファームウェア | 8% |
| 合計 | 100% |

| Q4. 2024 年のおおよその IT 予算に最も近い範囲を選択してください。 | 集計 |
|---|---|
| 100 万ドル未満 | 4% |
| 100 万ドル～500 万ドル | 6% |
| 600 万ドル～1,000 万ドル | 10% |
| 1,100 万ドル～5,000 万ドル | 13% |
| 5,100 万ドル～1 億ドル | 15% |
| 1 億 100 万ドル～2 億 5,000 万ドル | 14% |
| 2 億 5,100 万ドル～5 億ドル | 15% |
| 5 億 100 万ドル～7 億 5,000 万ドル | 13% |
| 7 億 5,100 万ドル～10 億ドル | 7% |
| 10 億ドル超 | 3% |
| 合計 | 100% |
| 外挿された値 | 2 億 8,200 万ドル |

| Q5. 2024 年の IT 予算のうち約何%が IT セキュリティに割り当てられる予定ですか？ | 集計 |
|---|---|
| 1%未満 | 1% |
| 1%～2% | 4% |
| 3%～5% | 7% |
| 6%～10% | 11% |
| 11%～15% | 14% |
| 16%～20% | 17% |
| 21%～30% | 12% |
| 31%～40% | 13% |
| 41%～50% | 12% |
| 50%超 | 10% |
| 合計 | 100% |
| 外挿された値 | 25% |

| Q6. 2024 年の IT セキュリティ予算のうち約何%がソフトウェア・サプライチェーンのセキュリティ対策（技術、セキュリティ人材、サービスへの投資など）に割り当てられる予定ですか？ | 集計 |
|---|---|
| 1%未満 | 5% |
| 1%～2% | 7% |
| 3%～5% | 9% |
| 6%～10% | 12% |
| 11%～15% | 15% |
| 16%～20% | 18% |
| 21%～30% | 11% |
| 31%～40% | 11% |
| 41%～50% | 8% |
| 50%超 | 4% |
| 合計 | 100% |
| 外挿された値 | 19% |

| Q7. SolarWinds や Kaseya などのソフトウェア・サプライチェーンの侵害を受けて、所属する組織のソフトウェア・サプライチェーンのセキュリティへの投資は増加しましたか？「1 = 増加していない」から「10 = 大幅に増加した」までの 10 段階評価で回答してください。 | 集計 |
|---|---|
| 1 または 2 | 8% |
| 3 または 4 | 16% |
| 5 または 6 | 31% |
| 7 または 8 | 26% |
| 9 または 10 | 19% |
| 合計 | 100% |

| Q8. 所属する組織は、ソフトウェア・サプライチェーンの攻撃や悪用による影響を受けたことがありますか？ | 集計 |
|---|---|
| はい | 59% |
| いいえ（Q12 に進んでください） | 24% |
| 分からない（Q12 へ進んでください） | 17% |
| 合計 | 100% |

| Q9. 攻撃や悪用が発生したのはいつですか？ | 集計 |
|---|---|
| 6 ヶ月前以内 | 25% |
| 6 ヶ月～1 年前 | 29% |
| 1～2 年前 | 30% |
| 2 年前超 | 16% |
| 合計 | 100% |

| Q10. 攻撃や悪用の根本原因は何でしたか？回答を **1 つ**だけ選択してください。 | 集計 |
|---|---|
| パッチ未適用のオープンソースの既知の脆弱性 | 28% |
| ゼロデイ脆弱性 | 23% |
| 悪意のある依存関係 | 19% |
| ビルド・パイプラインへの、悪意のあるコード/マルウェアのインジェクション | 21% |
| その他（具体的に記述してください） | 8% |
| 合計 | 100% |

| Q11. 攻撃に対応するのにどの程度の時間を要しましたか？ | 集計 |
|---|---|
| 1 日未満 | 13% |
| 1 日～1 週間 | 14% |
| 1 週間～1 ヶ月 | 19% |
| 1 ヶ月～3 ヶ月 | 25% |
| 3 ヶ月～6 ヶ月 | 15% |
| 6 ヶ月超 | 10% |
| 分からない | 5% |
| 合計 | 100% |

**パート 3. オープンソース・ソフトウェアのセキュリティ対策**

| Q12. 開発チームはオープンソース・ソフトウェアを使用していますか？ | 集計 |
|---|---|
| はい | 65% |
| いいえ（Q20 に進んでください） | 31% |
| 分からない（Q20 へ進んでください） | 4% |
| 合計 | 100% |

| Q13. 所属する組織は、オープンソース・ソフトウェアのセキュリティ対策についてどの程度成果をあげていますか？「1 = 成果をあげていない」から「10 = 大変成果をあげている」までの 10 段階評価で回答してください。 | 集計 |
|---|---|
| 1 または 2 | 9% |
| 3 または 4 | 21% |
| 5 または 6 | 23% |
| 7 または 8 | 20% |
| 9 または 10 | 27% |
| 合計 | 100% |

| Q14. オープンソース・コンポーネントのセキュリティの評価に使用している項目はどれですか？上位 2 つを選択してください。 | 集計 |
|---|---|
| 既存の脆弱性 | 55% |
| 脆弱性の履歴とパッチ適用までの期間 | 36% |
| プロジェクトのオーナー/メンテナーの評判 | 40% |
| コントリビューターの数 | 29% |
| コンポーネントの履歴 | 34% |
| 上記以外 | 7% |
| 合計 | 200% |

| Q15a. 所属する組織にオープンソースの依存関係を承認または禁止する方法はありますか？ | 集計 |
|---|---|
| はい | 48% |
| いいえ（Q16a に進んでください） | 38% |
| 分からない（Q16a へ進んでください） | 13% |
| 合計 | 100% |

| Q15b. オープンソースの依存関係を承認または禁止する方法に最も近いものはどれですか？回答を **1 つ**だけ選択してください。 | 集計 |
|---|---|
| 手動によるレビューと施行 | 37% |
| 手動コンポーネント・レビューと自動施行 | 41% |
| 自動化（あるいはポリシーベースの）レビューと施行 | 22% |
| 合計 | 100% |

| Q16a. 所属する組織では、オープンソースの依存関係のインベントリを管理していますか？ | 集計 |
|---|---|
| はい | 39% |
| いいえ（Q17a に進んでください） | 42% |
| 分からない（Q17a へ進んでください） | 19% |
| 合計 | 100% |

| Q16b. このインベントリを管理するために使用しているプロセスについて、最も近いものはどれですか？回答を **1 つ**だけ選択してください。 | 集計 |
|---|---|
| 手動による集計 | 39% |
| 自動化による依存関係特定とインベントリ集計 | 27% |
| 手動と自動化の併用 | 33% |
| 合計 | 100% |

| Q17a. 所属する組織では、オープンソースの依存関係に新たな脆弱性が生じていないかを継続的に監視していますか？ | 集計 |
|---|---|
| はい | 41% |
| いいえ（Q18a に進んでください） | 49% |
| 分からない（Q18a へ進んでください） | 9% |
| 合計 | 100% |

| Q17b. 所属する組織では、オープンソースの依存関係に新たな脆弱性が生じていないかをどのような方法で継続的に監視していますか？回答を **1 つ**だけ選択してください。 | 集計 |
|---|---|
| セキュリティ・フィードおよび/またはパブリック・フォーラムの手動監視 | 43% |
| セキュリティ・フィードおよび/またはパブリック・フォーラムの自動監視 | 57% |
| 合計 | 100% |

| Q18a. 所属する組織では、使用している依存関係に関連する IP/ライセンス義務を追跡していますか？ | 集計 |
|---|---|
| はい | 40% |
| いいえ（Q20 に進んでください） | 49% |
| 分からない（Q20 へ進んでください） | 11% |
| 合計 | 100% |

| Q18b. IP/ライセンス義務を追跡するために使用しているプロセスについて、最も近いのはどれですか？回答を **1 つ**だけ選択してください。 | 集計 |
|---|---|
| 手動によるライセンス特定とレビュー | 56% |
| 自動化ツールによるライセンス特定とポリシー適用 | 44% |
| 合計 | 100% |

| Q19. オープンソース・ライセンスの IP あるいはライセンス義務の主な責任者は誰ですか？回答を 1 つだけ選択してください。 | 集計 |
|---|---|
| 法務 | 17% |
| アプリケーション・セキュリティ | 36% |
| 開発 | 25% |
| 製品/プロジェクト管理 | 22% |
| 合計 | 100% |

**パート 4. サプライチェーンにおける商用ソフトウェアの使用とセキュリティ**

| Q20. 所属する組織は商用ソフトウェアを利用していますか？ | 集計 |
|---|---|
| はい | 46% |
| いいえ（Q25 に進んでください） | 54% |
| 合計 | 100% |

| Q21. 所属する組織では、商用ソフトウェアのセキュリティを評価することに、どの程度熱心ですか？「1 = 熱心ではない」から「10 = 大変熱心だ」までの10 段階評価で回答してください。 | 集計 |
|---|---|
| 1 または 2 | 19% |
| 3 または 4 | 22% |
| 5 または 6 | 18% |
| 7 または 8 | 21% |
| 9 または 10 | 20% |
| 合計 | 100% |

| Q22. 所属する組織では、使用または調達した商用ソフトウェアのリスク評価を行っていますか？ | 集計 |
|---|---|
| はい | 44% |
| いいえ（Q25 に進んでください） | 56% |
| 合計 | 100% |

| Q23. 行っているリスク評価の種類はどれですか？当てはまるものをすべて選択してください。 | 集計 |
|---|---|
| サプライヤーから提出されたアンケート結果 | 69% |
| サードパーティによる監査 | 54% |
| 内部監査 | 26% |
| 依存関係解析/バイナリ解析 | 22% |
| ランタイム解析/動的セキュリティ解析 | 30% |
| 合計 | 201% |

| Q24. 所属する組織では、商用ソフトウェア・サプライヤーのセキュリティをどの程度の頻度でレビューしていますか？ | 集計 |
|---|---|
| していない | 21% |
| 最初の契約交渉時に 1 回だけ | 29% |
| 毎四半期 | 16% |
| 年 1 回 | 12% |
| 契約更新時 | 22% |
| 合計 | 100% |

**パート 5. 悪意のあるコード/マルウェアによるリスクの低減**

| Q25. 所属する組織では、悪意のあるコード/マルウェアのリスク低減にどの程度熱心ですか？「1 = 熱心ではない」から「10 = 大変熱心だ」までの10 段階評価で回答してください。 | 集計 |
|---|---|
| 1 または 2 | 21% |
| 3 または 4 | 22% |
| 5 または 6 | 17% |
| 7 または 8 | 21% |
| 9 または 10 | 18% |
| 合計 | 100% |

| Q26a. 所属する組織では、悪意のあるパッケージが含まれていないかを確認するためにソフトウェアを評価していますか？ | 集計 |
|---|---|
| はい | 53% |
| いいえ（Q29a に進んでください） | 47% |
| 合計 | 100% |

| Q26b. 所属する組織では、ビルドしたソフトウェアが悪意のあるパッケージの影響を受けないようにするために、ソフトウェアをどのように評価していますか？当てはまるものをすべて選択してください。 | 集計 |
|---|---|
| ビルド前の依存関係解析 | 55% |
| ビルド後の依存関係解析あるいはアーティファクト解析 | 29% |
| ソースコードのレビュー | 41% |
| 実行中のアプリケーションのインタラクティブ解析または動的解析 | 39% |
| 合計 | 165% |

| Q27a. 所属する組織では、マルウェアの有無についてサードパーティ製のソフトウェアを評価していますか？ | 集計 |
|---|---|
| はい | 63% |
| いいえ（Q28 に進んでください） | 37% |
| 合計 | 100% |

| Q27b. 所属する組織では、マルウェアの有無についてサードパーティ製のソフトウェアやアーティファクトをどのように評価していますか？<br>当てはまるものをすべて選択してください。 | 集計 |
|---|---|
| アプリケーションの依存関係のバイナリ解析 | 45% |
| 実行中のアプリケーションの動的解析 | 49% |
| 提供されたソフトウェア部品表（SBOM）と既知の悪意のあるパッケージやマルウェアとの比較 | 51% |
| 実行中のアプリケーションの脅威に対する継続的な監視 | 37% |
| 合計 | 183% |

| Q28. 所属する組織では、悪意のあるオープンソース・パッケージ（例：タイポスクワッティング、依存関係かく乱によるブランド・ジャックなどを介して注入されたもの）から保護するためのプロセスを導入していますか？ | 集計 |
|---|---|
| はい | 45% |
| いいえ | 45% |
| 分からない | 10% |
| 合計 | 100% |

**パート 6. ソフトウェア・サプライチェーンのセキュリティ対策における SDLC と AI 活用**

| Q29a. 所属する組織では、コードのセキュリティや品質に問題がないか確認するためにコード・レビューを行っていますか？ | 集計 |
|---|---|
| はい | 54% |
| いいえ（Q30a に進んでください） | 46% |
| 合計 | 100% |

| Q29b. 開発チームは、コードのセキュリティや品質に問題がないか確認するために、どのような方法でコード・レビューを行っていますか？当てはまるものをすべて選択してください。 | 集計 |
|---|---|
| 手動コード・レビュー | 56% |
| 静的解析 | 49% |
| 依存関係解析あるいはソフトウェア・コンポジション解析 | 35% |
| 動的解析あるいはインタラクティブ解析 | 46% |
| その他（具体的に記述してください） | 5% |
| 合計 | 191% |

| Q30a. 開発チームは SDLC の一環でセキュリティ解析を行っていますか？ | 集計 |
|---|---|
| はい | 44% |
| いいえ（Q31 へ進んでください） | 56% |
| 合計 | 100% |

| Q30b. 開発チームは、SDLC のどの段階でセキュリティ分析を実施していますか？当てはまるものをすべて選択してください。 | 集計 |
|---|---|
| コーディング | 64% |
| チェックイン前 | 58% |
| ビルド | 56% |
| ビルド後 | 38% |
| テスト環境 | 28% |
| 本稼働 | 31% |
| 合計 | 275% |

| Q31. 所属する組織では、SDLC の完全性をどのように保護していますか？当てはまるものをすべて選択してください。 | 集計 |
|---|---|
| 承認済みの依存関係の内部/プライベート・リポジトリ（オープンソース・コンポーネントを含む） | 54% |
| ビルド・ツールのアクセス保護 | 58% |
| ソースコード・マネージャーやリポジトリのアクセス保護 | 38% |
| バイナリ・リポジトリのアクセス保護 | 44% |
| テスト環境およびステージング環境のアクセス保護 | 48% |
| 上記以外 | 9% |
| 合計 | 250% |

| Q32a. 所属する組織は、セキュアなソフトウェア開発の標準モデルに従っていますか？ | 集計 |
|---|---|
| はい | 57% |
| いいえ（Q33a に進んでください） | 43% |
| 合計 | 100% |

| Q32b. 所属する組織では、セキュアなソフトウェア開発についてどの標準モデルに従っていますか？当てはまるものをすべて選択してください。 | 集計 |
|---|---|
| NIST SSDF | 48% |
| IEC62443 | 50% |
| BSIMM | 37% |
| OpenSAMM | 34% |
| NIST CSF | 45% |
| UL2900 | 33% |
| FDA のサイバーセキュリティ要件 | 41% |
| IMDRF のサイバーセキュリティ要件 | 37% |
| ISO21434 | 34% |
| UNR 155/156 | 31% |
| その他（具体的に記述してください） | 5% |
| 合計 | 395% |

| Q33a. 開発チームはコードの生成に AI ツールを活用していますか？ | 集計 |
|---|---|
| はい | 52% |
| いいえ（Q37 に進んでください） | 48% |
| 合計 | 100% |

| Q33b. 開発チームはどの AI ツールを使っていますか？当てはまるものをすべて選択してください。 | 集計 |
|---|---|
| GitHub CoPilot | 43% |
| ChatGPT | 45% |
| OpenAI Codex | 50% |
| その他（具体的に記述してください） | 6% |
| 合計 | 144% |

| Q34. 所属する組織では、AI によって生成されたコードを評価するためのプロセスを導入していますか？ | 集計 |
|---|---|
| はい | 32% |
| いいえ（Q37 に進んでください） | 68% |
| 合計 | 100% |

| Q35. AI によって生成されたコードを評価するために、どのようなプロセスを導入していますか？当てはまるものをすべて選択してください。 | 集計 |
|---|---|
| IP またはライセンス上のリスクの評価 | 52% |
| セキュリティ上のリスクの評価 | 43% |
| 品質上の問題の評価 | 36% |
| 合計 | 131% |

| Q36. 所属する組織では、これらの評価をどのように行っていますか？<br>回答を **1 つ**だけ選択してください。 | 集計 |
|---|---|
| 手動 | 49% |
| 自動/ツール使用 | 51% |
| 合計 | 100% |

**パート 7. ソフトウェアの脆弱性によるリスクの低減**

| Q37. 所属する組織では、ソフトウェアに新たな脆弱性が生じていないかをどのように監視していますか？回答を **1 つ**だけ選択してください。 | 集計 |
|---|---|
| 脆弱性フィードの手動監視 | 37% |
| 手動または自動化によるソースコード・レビュー | 47% |
| 自動化ツール | 16% |
| 合計 | 100% |

| Q38. ソフトウェアの脆弱性に関する主な情報源は何ですか？<br>回答を **1 つ**だけ選択してください。 | 集計 |
|---|---|
| 米国 NVD（National Vulnerability Database） | 10% |
| 地域別脆弱性データベース | 18% |
| GitHub | 15% |
| CISA KEV（悪用が確認されている脆弱性のリスト） | 19% |
| アプリケーション・セキュリティ・ベンダー独自の情報 | 39% |
| その他（具体的に記述してください） | 0% |
| 合計 | 100% |

| Q39. 所属する組織は、ソフトウェアの脆弱性を突く攻撃の検知と対応についてどの程度成果をあげていますか？「1 = 成果をあげていない」から「10 = 大変成果をあげている」までの 10 段階評価で回答してください。 | 集計 |
|---|---|
| 1 または 2 | 20% |
| 3 または 4 | 22% |
| 5 または 6 | 19% |
| 7 または 8 | 21% |
| 9 または 10 | 17% |
| 合計 | 100% |

| Q40. 所属する組織は、クリティカルなソフトウェアの脆弱性に対応するのにどの程度の時間を要しますか？ | 集計 |
|---|---|
| 1 日未満 | 14% |
| 1 日～1 週間 | 13% |
| 1 週間～1 ヶ月 | 21% |
| 1 ヶ月～3 ヶ月 | 22% |
| 3 ヶ月～6 ヶ月 | 15% |
| 6 ヶ月超 | 10% |
| 分からない | 5% |
| 合計 | 100% |

**パート 8. ソフトウェア部品表（SBOM）の作成と生成**

| Q41. 所属する組織は SBOM を作成または生成していますか？ | 集計 |
|---|---|
| はい | 35% |
| いいえ（パート 9 へ進んでください） | 56% |
| 分からない（パート 9 へ進んでください） | 9% |
| 合計 | 100% |

| Q42a. 所属する組織の法務あるいはガバナンス・チームは SBOM の正確性を検証する役割を担っていますか？ | 集計 |
|---|---|
| はい | 26% |
| いいえ（Q43 に進んでください） | 74% |
| 合計 | 100% |

| Q42b. 法務あるいはガバナンス・チームは SBOM の正確性を検証する上でどのような役割を担っていますか？当てはまるものをすべて選択してください。 | 集計 |
|---|---|
| 配布を許可する | 39% |
| 配布のルールを定める | 37% |
| 公開のガイドラインを定める | 32% |
| 含める情報のガイドラインを定める | 28% |
| その他（具体的に記述してください） | 7% |
| 合計 | 143% |

| Q43a. 所属する組織では、サプライヤーに SBOM をリクエストしていますか？ | 集計 |
|---|---|
| はい | 29% |
| いいえ（Q48 に進んでください） | 43% |
| ソフトウェア・サプライヤーがいない（Q48 へ進んでください） | 28% |
| 合計 | 100% |

| Q43b. リクエストした SBOM について、所属する組織が要求するフォーマットはどれですか？回答を 1 つだけ選択してください。 | 集計 |
|---|---|
| SPDX | 34% |
| CycloneDX | 25% |
| SPDX と CycloneDX の両方 | 25% |
| 特定のフォーマットは要求しない | 17% |
| 合計 | 100% |

| Q44. 所属する組織は、リクエストした SBOM を提供しないサプライヤーに対してどのように対処していますか？回答を **1 つ**だけ選択してください。 | 集計 |
|---|---|
| 提供されたソフトウェアの使用を直ちに中止する | 40% |
| 契約満了までソフトウェアを使用し続ける | 43% |
| ソフトウェア・サプライヤーに対して改善計画を立てる | 17% |
| 合計 | 100% |

| Q45. 所属する組織では、サプライヤーから提供された SBOM を検証していますか？ | 集計 |
|---|---|
| はい | 40% |
| いいえ | 60% |
| 合計 | 100% |

| Q46. 所属する組織では、SBOM を何にインポートしますか？<br>当てはまるものをすべて選択してください。 | 集計 |
|---|---|
| ITSM | 49% |
| SEIM | 45% |
| SOAR | 48% |
| パッケージ・マネージャー | 26% |
| アプリケーション・セキュリティ・ツール | 27% |
| 合計 | 195% |

| Q47. サプライヤーから提供された SBOM に脆弱性の開示は含まれていますか？ | 集計 |
|---|---|
| はい | 34% |
| いいえ | 66% |
| 合計 | 100% |

| Q48. 所属する組織が SBOM を生成するのに使用しているフォーマットはどれですか？回答を **1 つ**だけ選択してください。 | 集計 |
|---|---|
| SPDX | 31% |
| CycloneDX | 42% |
| SPDX と CycloneDX の両方 | 27% |
| 合計 | 100% |

| Q49. 所属する組織が SBOM を生成する理由は何ですか？当てはまるものをすべて選択してください。 | 集計 |
|---|---|
| 一般的な依存関係あるいは脆弱性管理 | 50% |
| 政府が定めた要件 | 38% |
| 業界の規制 | 39% |
| 業界のベストプラクティス | 26% |
| 顧客が求める要件 | 38% |
| 合計 | 191% |

| Q50. 所属する組織では、SBOM をどのように生成していますか？<br>当てはまるものをすべて選択してください。 | 集計 |
|---|---|
| 手動プロセス | 47% |
| 無償/オープンソース・ツール | 44% |
| SCA ツール | 37% |
| サードパーティ | 31% |
| その他（具体的に記述してください） | 7% |
| 合計 | 166% |

| Q51. 所属する組織では、どの程度の頻度で SBOM を生成していますか？<br>1 つだけ選んでください。 | 集計 |
|---|---|
| 製品のリリースごと | 20% |
| 開発中のプロジェクトのビルドあるいはコミットごと | 13% |
| 毎週 | 9% |
| 毎月 | 13% |
| 毎四半期 | 16% |
| 毎年 | 8% |
| 提供を求められたときはいつでも | 21% |
| 合計 | 100% |

**パート 9. 組織と回答者の属性**

| D1. 現在のポジションに最も近い組織階級はどれですか？ | 集計 |
|---|---|
| 上級幹部あるいは VP | 14% |
| 部長（ディレクター） | 15% |
| 課長（マネージャー） | 20% |
| 主任（スーパーバイザー） | 12% |
| 技能者あるいはスタッフ、請負業者 | 30% |
| エンジニア | 9% |
| 合計 | 100% |

| D2. 回答者様自身または配属先 IT セキュリティ・リーダーの**直属の上司**を選択してください。 | 集計 |
|---|---|
| 最高財務責任者（CFO） | 1% |
| 最高執行責任者（COO） | 2% |
| ゼネラル・カウンシル | 5% |
| 製造（GMP）責任者 | 4% |
| 製品エンジニアリング責任者 | 1% |
| 品質保証責任者 | 1% |
| 最高情報責任者（CIO） | 12% |
| 最高技術責任者（CTO） | 19% |
| 最高情報セキュリティ責任者（CISO） | 20% |
| 最高セキュリティ責任者（CSO） | 9% |
| コンプライアンス責任者 | 8% |
| データセンター管理者 | 10% |
| 最高リスク責任者（CRO） | 7% |
| その他 | 1% |
| 合計 | 100% |

| D3. 所属する組織の主要業種に最も近いものはどれですか？ | 集計 |
|---|---|
| 航空宇宙・防衛 | 0% |
| 農業・外食産業 | 2% |
| コンシューマー製品 | 6% |
| 教育および研究 | 2% |
| エネルギー・公益事業 | 7% |
| エンターテインメント・メディア・ゲーム | 3% |
| 金融サービス | 18% |
| 医療・製薬 | 5% |
| 接客業 | 2% |
| IT・テクノロジー | 10% |
| 物流・流通 | 8% |
| 製造業 | 5% |
| 公共部門 | 10% |
| 小売業・e コマース | 5% |
| サービス | 9% |
| 電気通信・無線 | 5% |
| 運輸 | 4% |
| その他（具体的に記述してください） | 0% |
| 合計 | 100% |

| D4. 所属する組織の全世界の従業員数を教えてください。 | 集計 |
|---|---|
| 5,000 人未満 | 18% |
| 5,001 人～10,000 人 | 25% |
| 10,001 人～25,000 人 | 27% |
| 25,001 人～75,000 人 | 25% |
| 75,000 人以上 | 5% |
| 合計 | 100% |

**この調査の詳細については、Ponemon Institute までメール（research@ponemon.org）でお問い合わせください。**

**Ponemon Institute**
**責任ある情報管理を推進**

Ponemon Institute では、企業および政府機関内で責任ある情報/プライバシー管理プラクティスを推進するための独立した調査と教育に注力しています。私たちの使命は、人と組織に関する機密情報の管理とセキュリティに影響する重大な問題について高品質な実証的調査研究を実施することです。

データの機密性、プライバシー、および調査の倫理については厳格な基準を設けています。個人から個人を特定できる情報（企業調査の場合は企業を特定できる情報）を収集することは一切ありません。また、対象者に無関係または不適切な質問をすることがないよう、厳格な品質基準を定めています。