Enterprise Strategy Group | Getting to the bigger truth.™

社会的な規範を守る：
GitOps とシフト・レフト・セキュリティ

開発者中心のスケーラブルな
サプライチェーン・セキュリティ・ソリューション

Melinda Marks ESG シニア・アナリスト

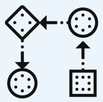
2022 年 8 月

調査の目的

組織がモダン・ソフトウェア開発プロセスの採用を進める中、開発者はアプリケーションをクラウドへデプロイすることによって開発とリリースを迅速化できるようになっています。一方、セキュリティ・チームは継続的インテグレーション / 継続的デプロイ（CI/CD）サイクルとその動的コンポーネントの成長とスピードにいかに対応するかが課題となっています。

業界では、開発ペースの加速に対応できるスケーラブルなセキュリティを実現するためにセキュリティのシフト・レフトが以前から提唱されています。しかしいざ実践に移そうとすると、組織は多くの課題に直面しているのが現状です。クラウドネイティブ環境におけるセキュリティ・インシデントのほとんどは設定ミスによって生じているため、コーディングの問題をデプロイ前に見つけて修正できるよう、セキュリティを開発に組み込む方法を見つけることがセキュリティ・チームにとって急務となっています。また、検出されたセキュリティ問題を迅速に修正できるようにするため、開発者との連携を改善する方法についても重点的に取り組むことが必要となっています。こうしたトレンドについての知見を得るため、ESG は北米地域（米国、カナダ）の中堅企業（従業員数 100 ～ 999 人）および大企業（従業員数 1,000 人以上）で開発者中心のセキュリティ製品の、評価、購入、および利用に責任を負う 350 人の IT（30%）およびサイバーセキュリティ（40%）意思決定担当者、アプリケーション開発者（30%）を対象に調査を実施しました。

今回の調査の目的



組織が**どの程度**セキュリティを開発ワークフローに組み込んでいるかを**調査する。**

クラウドネイティブ開発サイクルの加速に伴い組織が直面している**課題を理解する。**

開発プロセスの速度を低下させることなくソフトウェアのセキュリティを確保するにはどのような種類のソリューションが最も効果的かについて**知見を得る。**

ベンダー・ソリューションの種類、そのソリューションの導入方法、そしてチーム間の作業を軽減する方法についての**バイヤーの好みを見定める。**

目次へ

目次

クリックすると
該当ページへジャンプします

モダン開発により
スピードが加速すると同時に
セキュリティ・リスクも増大

オープンソース・ソフトウェア（OSS）の普及

回答者は、アプリケーション開発において OSS コンポーネントの利用が拡大していることを認識しています。事実、80% の組織がクラウドネイティブ・アプリケーションのプログラミングにオープンソース・ソフトウェアを使用していると回答しています。既存のオープンソース・コードを使用してアプリケーションを開発すれば時間を短縮でき、ソフトウェアの独自機能を担うカスタム・コードの作成により多くの時間を費やすことができます。しかしそれによってセキュリティ・リスクが混入することがあってはなりません。クラウドネイティブ開発には強力なコミュニティが存在し、開発者がコードを共有・貢献してくれているため、多くのオープンソース・ソフトウェアを利用できます。このため、ソフトウェアのコード全体に占める OSS の割合が高いのは驚くべきことではありません。

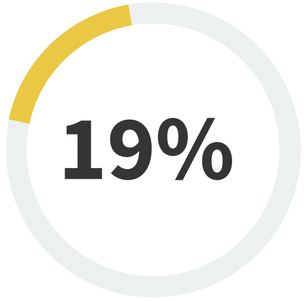
80%

の組織が**クラウドネイティブ・アプリケーションのプログラミングにオープンソース・ソフトウェアを使用している**と回答。

» クラウドネイティブ・アプリケーションにおけるオープンソース・ソフトウェアの使用状況

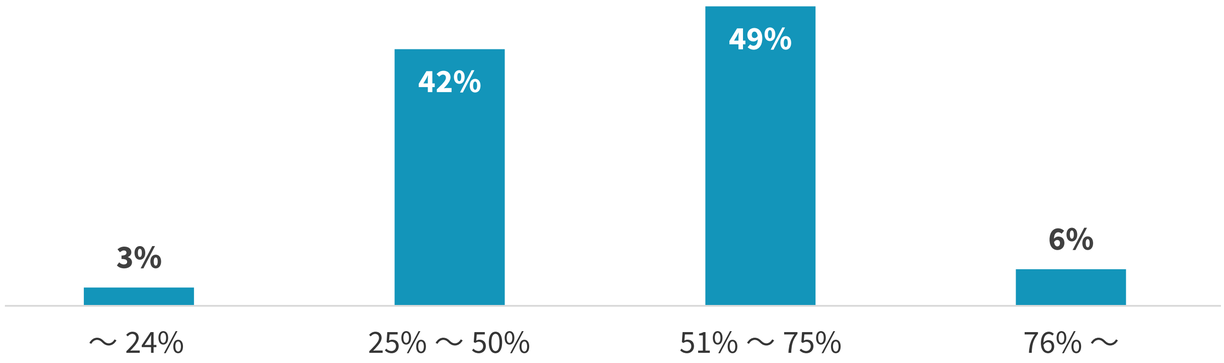
オープンソース・ソフトウェアを
既に使用している

オープンソース・ソフトウェアを
今後 12 カ月以内に**使用する計画がある**



その他の 1% はオープンソース・ソフトウェアの使用に関心があると回答。

» コード全体に占める OSS の割合



目次に戻る

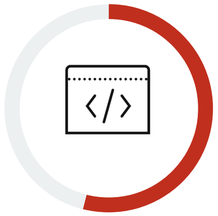
オープンソースのセキュリティに関する主な懸念材料

OSS を利用すると開発期間は短縮されますが、組織はセキュリティへの影響を懸念しています。人気のある OSS に弱点があれば、その OSS を使用しているすべての企業が攻撃の標的になりうるため、ハッカーは OSS の脆弱性を探すことに大きな魅力を感じています。

そこで、組織は使用している OSS コンポーネントを完全に把握し、何らかの脆弱性が見つかったらすぐに対処できるようにする方法を模索しています。

> 組織は使用している OSS コンポーネントを完全に把握し、**何らかの脆弱性が見つかったらすぐに対処できるようにする方法を模索しています。”**
>
> Melinda Marks ESG シニア・アナリスト

» オープンソース・ソフトウェアの課題と懸念



54%
アプリケーション・コードに占めるオープンソースの割合が大きいこと

41%
広く使用されているオープンソース・ソフトウェアを標的としたハッカーの攻撃を受けること

40%
コードの出所を信頼すること

39%
コードに潜む脆弱性を特定すること

39%
コードのコンポジション（構成）を把握し、SBOM（ソフトウェア部品表）を生成すること

39%
リリースされたパッチを直ちに適用すること

38%
脆弱性を迅速に修正すること

目次に戻る

IaC（Infrastructure as Code）の利用拡大

IaC（Infrastructure as Code）を使用すると、IT チームや運用チームによるプロビジョニングを待たずして、開発者自身がインフラストラクチャをプロビジョニングできます。通常、開発者はテンプレートのコードを使用して必要なクラウド・インフラストラクチャを宣言によってスクリプト化し、ネットワーキング、コンピューティング・サービス、ストレージなどのリソースを管理します。現在、2/3 以上（69%）の組織が IaC テンプレートを使用してクラウド・インフラストラクチャをプロビジョニングしており、今後 12 カ月以内にその計画があると回答した組織も 27% にのぼっています。現在、IaC テンプレートの利用範囲はまだ限定的ですが、61% の組織が今後 2 年間でクラウドネイティブ・アプリケーションの半数以上に IaC テンプレートを使用する予定と回答しています。

今後 2 年間で

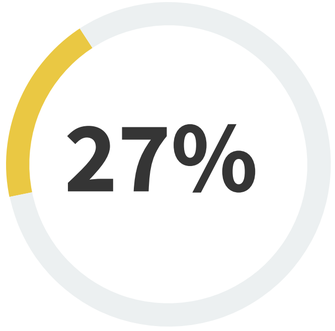
61%

の組織が**クラウドネイティブ・アプリケーションの半数以上**に IaC テンプレートを使用する予定。

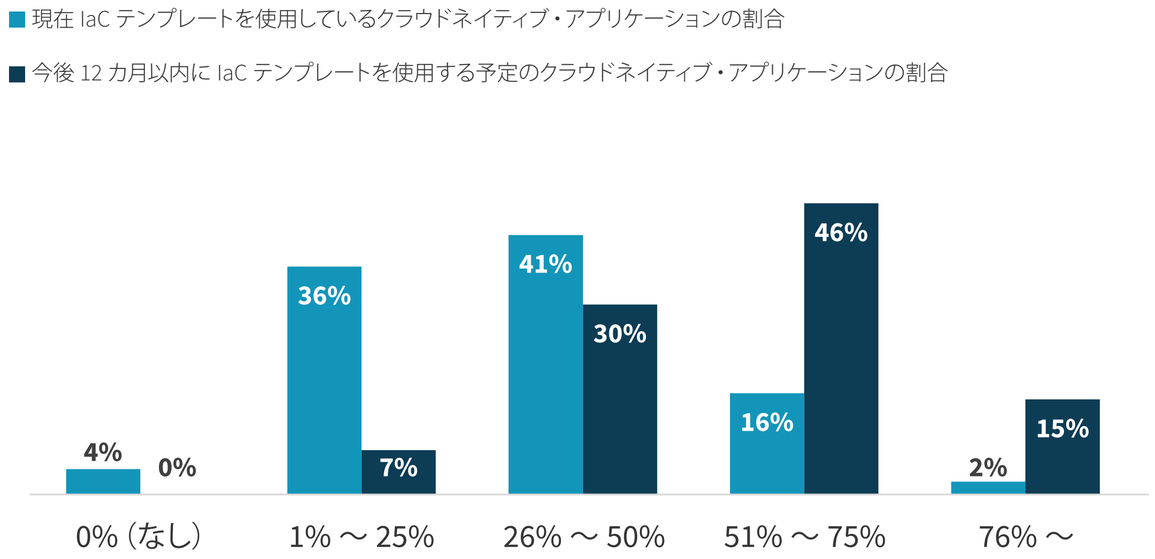
» IaC テンプレートの使用状況

IaC テンプレートを**既に使用して**クラウド・インフラストラクチャをプロビジョニングしている

IaC テンプレートを今後 12 カ月以内に**使用する計画がある**



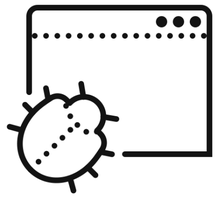
その他の 4% は IaC テンプレートの使用に関心があると回答。



目次に戻る

IaC の利用に関する設定ミスとインシデント

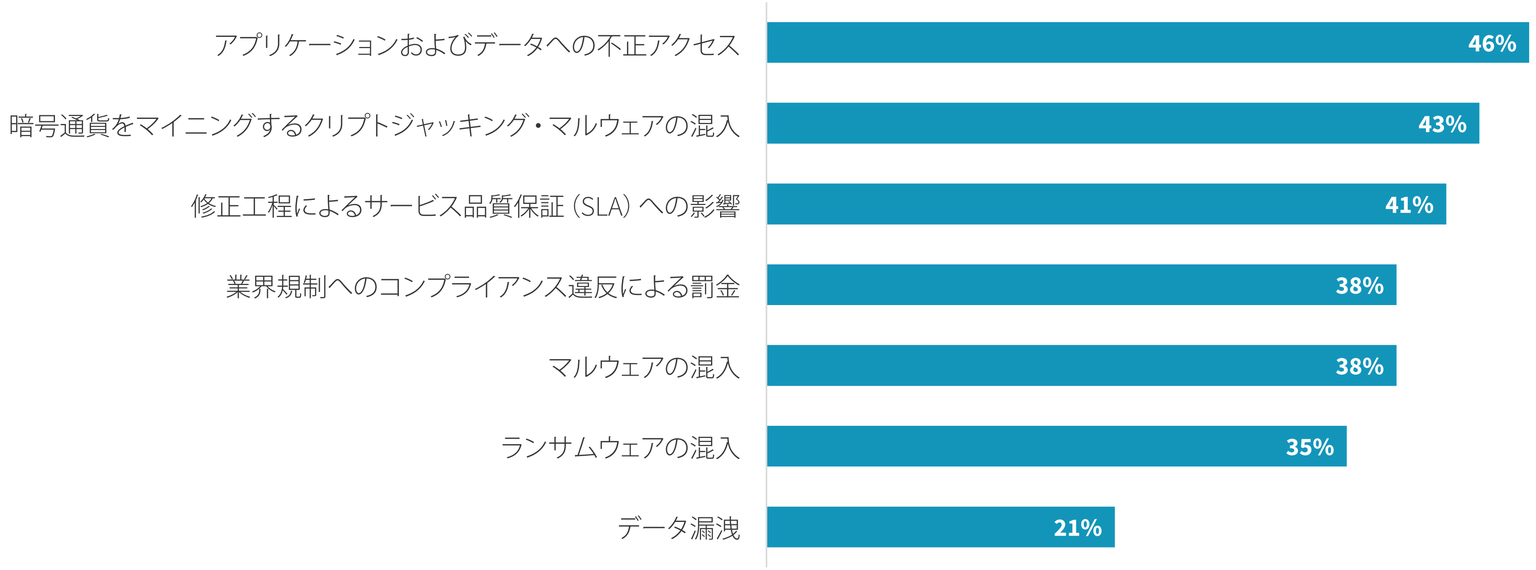
開発者による IaC の利用が増えていくと、ミスが起こる可能性も高くなります。コーディングの問題は検出が難しいことがありますが、これらはリソースへのアクセスを制御するものであるため、設定ミスは非常に深刻な結果を招く可能性があります。回答者の大半（83%）が、IaC の利用に関する設定ミスが増えていることを認識しています。この結果、アプリケーションおよびデータへの不正アクセス、マルウェアの混入、サービス品質への影響、データ漏洩など、さまざまな被害が生じています。



83%

の回答者が、**IaC テンプレートの設定ミス**が増えていることを認識している。

» IaC テンプレートの設定ミスの増加がもたらす影響



目次に戻る

セキュリティを
開発プロセスに
組み込むことが必要

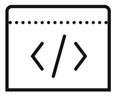
セキュリティを開発に組み込む

リリース・サイクルの加速によって管理できないほどのセキュリティ・リスクにさらされることのないよう、組織はセキュリティ・プロセスを開発に組み込もうと努めています。これには、アジャイル・ソフトウェア開発プロセスにおけるサイバーセキュリティ・ユーザー・ストーリー、SaC（Security-as-Code）、GitOps などが含まれます。回答者の 59% が既に SaC を導入済みと答えていますが、多くの回答者が今後 2 年間で SaC が非常に重要なアプローチになると考えています。SaC を導入することの有用性はほとんどの回答者が認めていますが、SaC の成熟度やサイバーセキュリティ・スキルの慢性的な不足などを理由に、SaC をどのように実装するか、あるいは複数のプロジェクトやチーム間でどのように実装するか、その方法を組織はまだ決めかねています。

» クラウドネイティブ・アプリケーションのセキュリティ対策に現在使用しているセキュリティ・プロセス

アジャイル・ソフトウェア開発プロセスにおける
サイバーセキュリティ・ユーザー・ストーリーの定義

63%



SaC（Security-as-Code）

59%

GitOps による以前の構成へのロールバック

55%

» SaC（Security-as-Code）に対する認識

SaC は今後 24 カ月以内に非常に重要な
サイバーセキュリティ・アプローチになる

72%

自社のサイバーセキュリティ・チームには、SaC を実装できる
スキルを持ったセキュリティ・アナリストが不足している

56%

現在の SaC はサイバーセキュリティ・プログラムに
組み込めるほどには成熟していない

51%

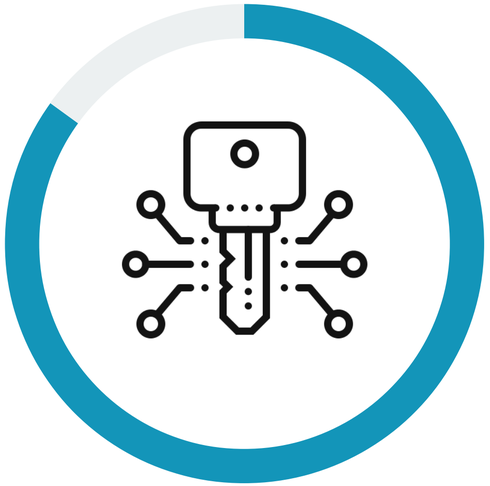
目次に戻る

Git リポジトリに保存されたシークレットのスキャン

開発者がシークレット（パスワード、API キー、トークンなどの資格情報）を安易にハードコーディングすることがよくあります。この結果、85% の組織が Git リポジトリに対してシークレットのスキャンを実施しており、実際に数多く検出されています。もちろんスキャンを実施するのは良いことですが、それで保護が保証されるわけではありません。リスクを軽減できるかどうかは、セキュリティ・チームが修正アクションを徹底できるかどうかにかかっています。事実、組織の大半が Git リポジトリに対してスキャンを実施しているにもかかわらず、ほぼ 1/3（31%）がソース・コード・リポジトリからシークレットを盗まれたことがあると答えています。

31%

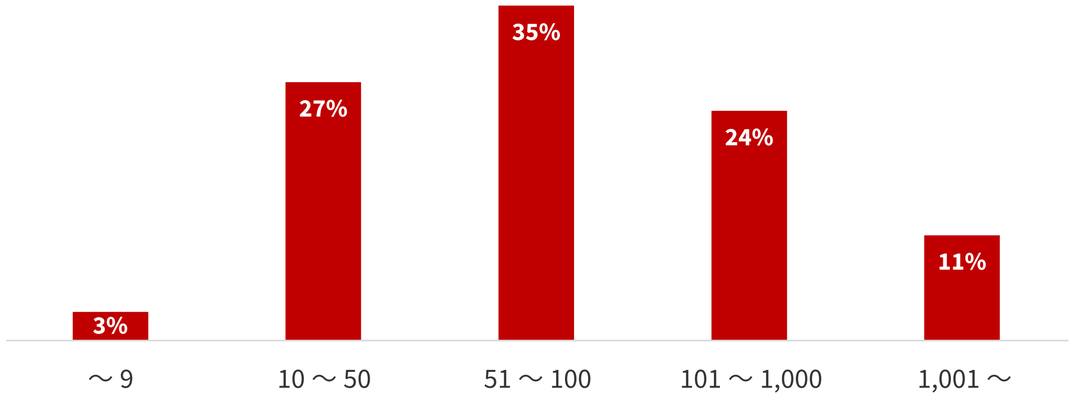
の組織が過去 12 カ月以内にソース・コード・リポジトリから**シークレットを盗まれたことがある。**



リスクのあるシークレットを検出するために Git リポジトリのスキャンを**既に実行している**

85%

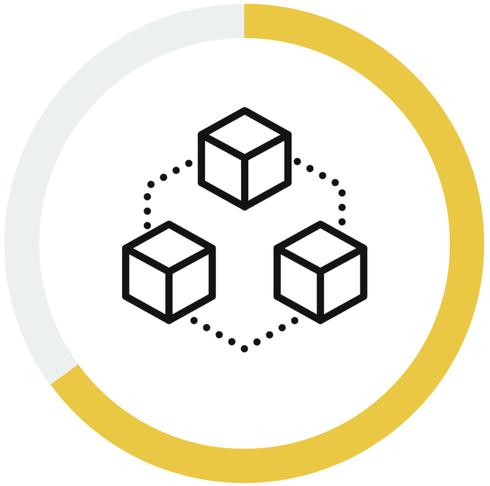
» Git リポジトリのスキャンで見つかったシークレットの推定件数



目次に戻る

加速する開発サイクルを考慮しながらセキュリティ・プラクティスを適用する上での課題

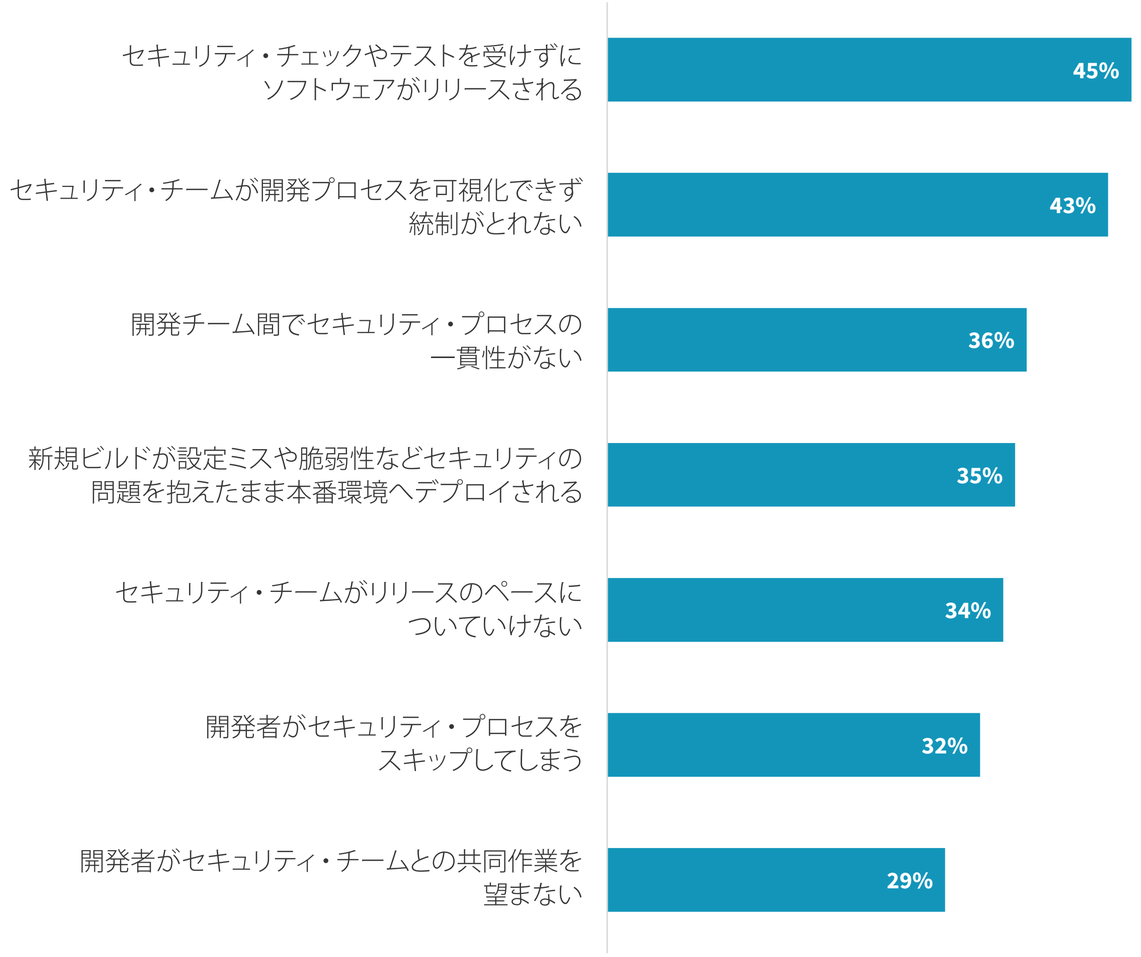
セキュリティ・チームがセキュリティを開発に組み込もうとすると、CI/CD によるリリースのスピードと量への対応という点でいくつもの課題に直面します。回答者が特に多く挙げたのが、セキュリティ・チェックやテストを受けずにソフトウェアがリリースされる（45%）、セキュリティ・チームが開発プロセスを可視化できず統制がとれない（43%）という課題でした。また、ほぼ 2/3 の組織が 50 を超える Git リポジトリを所有していることも、この問題をさらに悪化させる要因となっています。



65%

の組織が **50 を超える Git リポジトリを所有**しています。

» CI/CD 開発サイクルの加速によって生じるセキュリティの課題



目次に戻る


クラウドネイティブを取り巻く
サイバーセキュリティ上の
脅威が激化

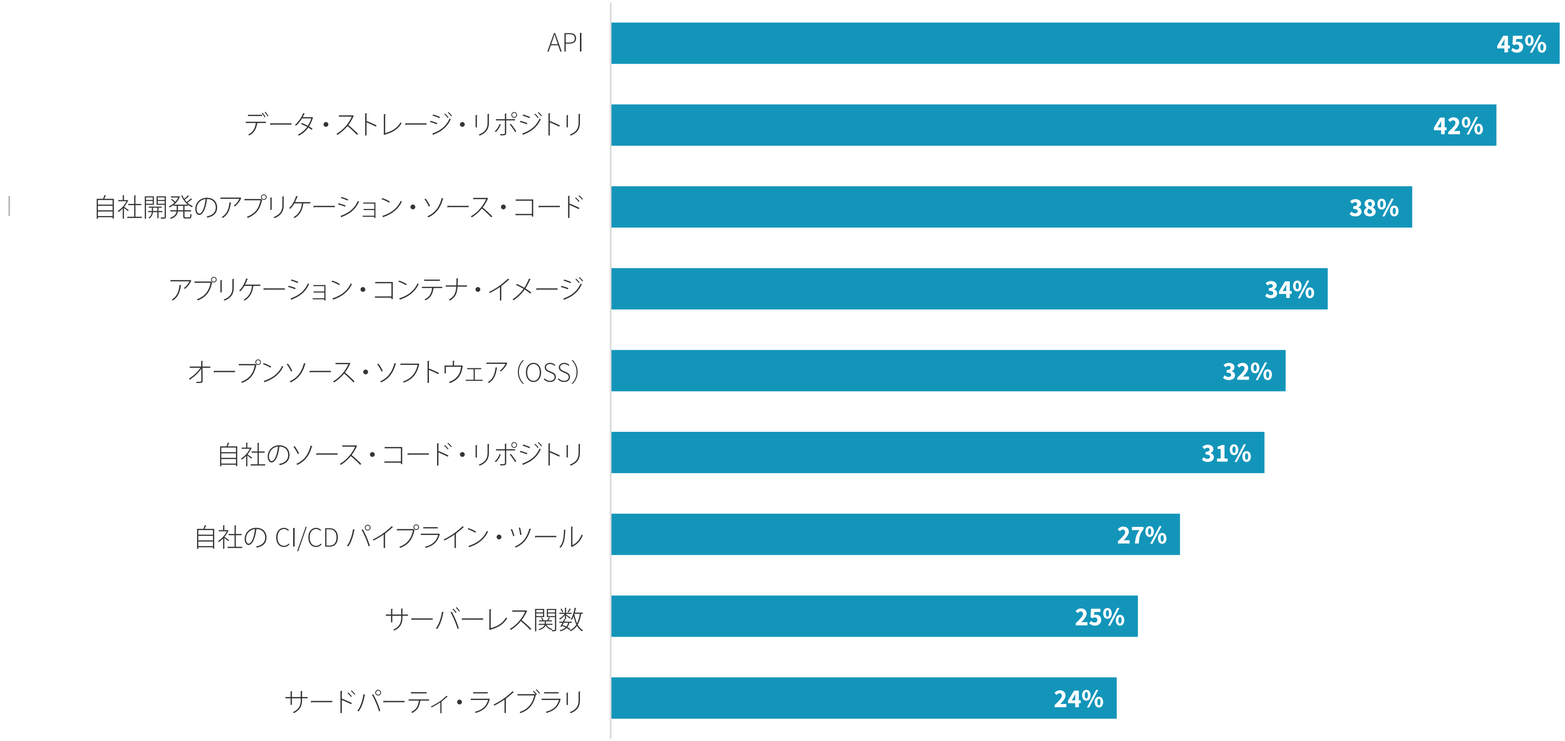
最も攻撃を受けやすいクラウドネイティブの要素が実際に最近のインシデントで攻撃の標的に

ソフトウェア・スタックとツールチェーン全体で、どの要素が最も攻撃を受けやすいかを組織に評価してもらったところ、最も多く挙げられたのが API で、次に多かったのがデータ・ストレージ・リポジトリ、そして組織内部で開発したアプリケーション・ソース・コードでした。

回答者の大多数がさまざまなセキュリティ・インシデントとそれに関連する被害を受けており、それらは組織内部で開発したクラウドネイティブ・アプリケーションに起因するものであったと答えています。回答者が挙げたインシデントの種類として最も多かったのは、API の安全でない使用、コードの脆弱性、アカウント資格情報の流出の 3 つで、これらは最も攻撃を受けやすいと考えられるソフトウェア・スタック要素のうち 2 つと符合しています。

> **最も多く挙げられたのが API で、**
> 次に多かったのがデータ・ストレージ・リポジトリ、
> そして組織内部で開発したアプリケーション・ソース・コードでした。”

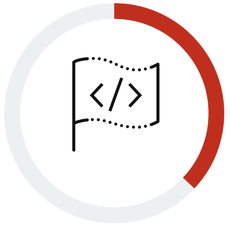
» クラウドネイティブ・アプリケーション・スタックのうち、最も攻撃を受けやすいと考えられる要素



目次に戻る

» クラウドネイティブ・アプリケーションに起因して経験したサイバーセキュリティ・インシデント

API の安全でない使用が原因で
攻撃を受け、データ漏洩を招いた
38%

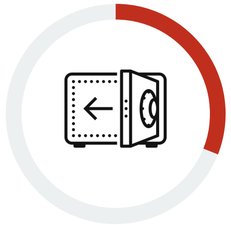


組織内部で開発したコードに
存在する既知の脆弱性を
悪用された
37%

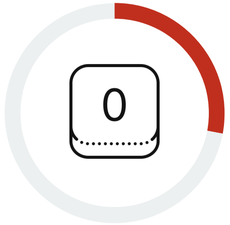
サービス・アカウントの
資格情報が流出した
35%

オープンソース・ソフトウェアに
存在する既知の脆弱性を
悪用された
34%

クラウド・サービスの
設定ミスを悪用された
33%



ソース・コード・リポジトリから
シークレットを盗まれた
31%



オープンソース・ソフトウェアに
存在する未知の新しい脆弱性を
悪用した「ゼロデイ」攻撃を受けた
28%

組織内部で開発したコードに
存在する未知の新しい脆弱性を
悪用した「ゼロデイ」攻撃を受けた
27%

特権ユーザーの資格情報が
流出した
26%

目次に戻る

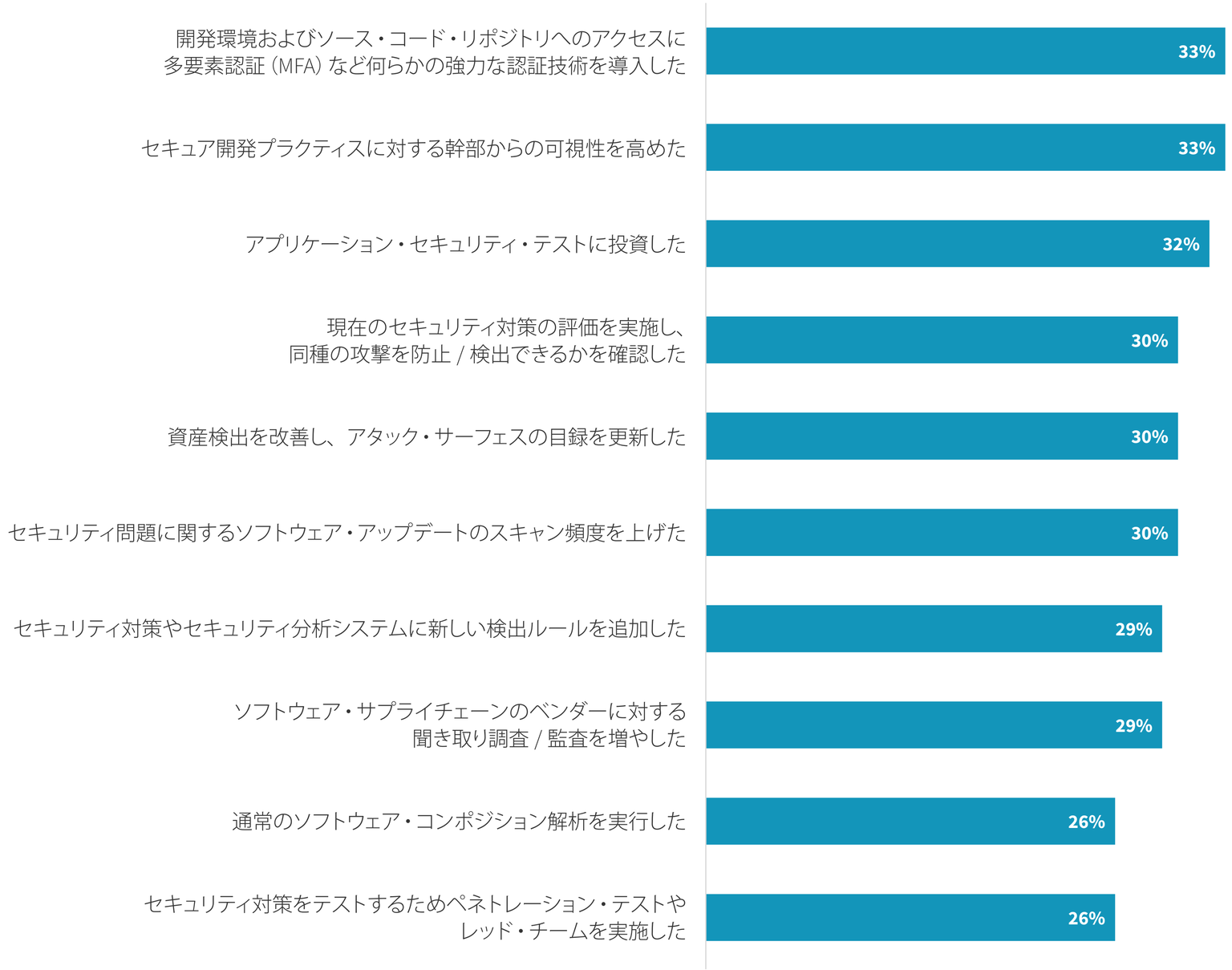
相次ぐ攻撃の報道を受けて強化へ向かうソフトウェア・サプライチェーンのセキュリティ対策

クラウドネイティブ・アプリケーションに関する懸念が現実のインシデントになる前に、組織は予防的手段を講じてこれらの問題を軽減することが望まれます。事実、最近発生したソフトウェア・サプライチェーン攻撃をふまえ、約 3/4（73%）の組織がオープンソース・ソフトウェア、コンテナ・イメージ、およびサードパーティ・ソフトウェア・コンポーネントのセキュリティ対策を大幅に強化しています。これらの攻撃から想定されるリスクを軽減するために、組織はさまざまな対策を講じています。

73%

の組織が、最近発生したソフトウェア・サプライチェーン攻撃をふまえ、オープンソース・ソフトウェア、コンテナ・イメージ、およびサードパーティ・ソフトウェア・コンポーネントのセキュリティ対策を大幅に強化していると答えています。

» 最近のソフトウェア・サプライチェーン攻撃をふまえて実施した対策トップ 10



目次に戻る

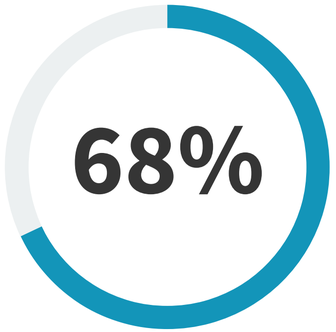
セキュリティと開発プロセスは、混乱を招かないように統合することが必要

シフト・レフトによりスケーラブルなセキュリティを実現

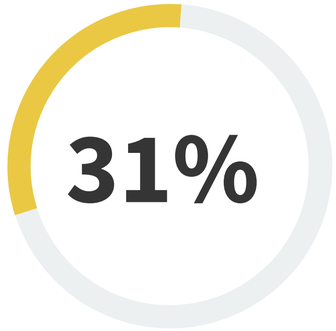
ほとんどの組織は開発者中心型セキュリティ・ソリューションに高い優先度を置き、セキュリティ責任の一部を開発者へシフトするようにもなっています。その理由は、スケーラブルなセキュリティを実現する方法がこれ以外に存在しないことにあります。事実、ほとんどすべての回答者がこの取り組みを重要視しており、その優先度が高いと答えた回答者も 2/3 以上（68%）にのぼっています。36% がセキュリティ責任を開発チームへシフトすることに**完全に**満足していると答えている一方、ほぼ満足（49%）とやや満足（15%）を合わせた回答が過半数に達しています。

» 開発者中心のセキュリティ戦略導入の優先度

優先度が高い
（すなわち、現在のセキュリティ・プログラムに大きな影響がある）

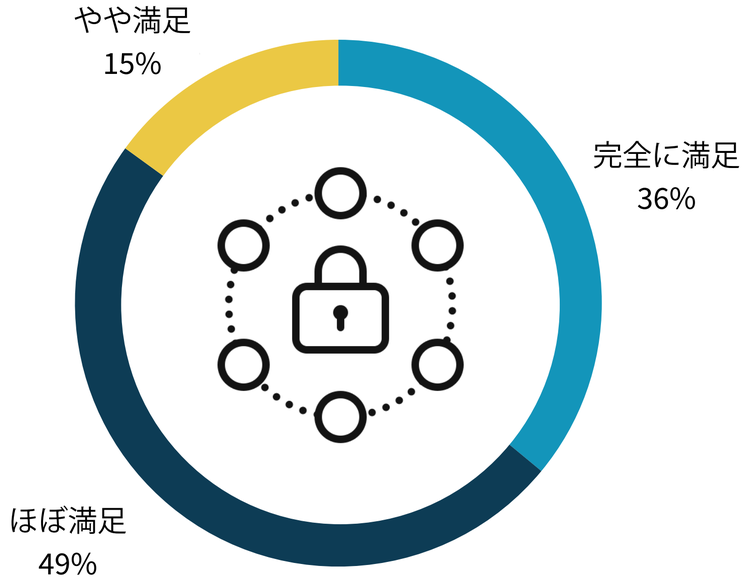


重要ではあるが、優先度は高くない
（すなわち、セキュリティやアプリケーション開発に関して他に優先度の高いものがある）



その他の 1% は、**まったく優先事項ではない**（すなわち、セキュリティ責任を開発者にシフトしなくても現状のセキュリティ対策で十分）と回答。

» 開発者中心のセキュリティ戦略の導入に関するセキュリティ・チームの満足度



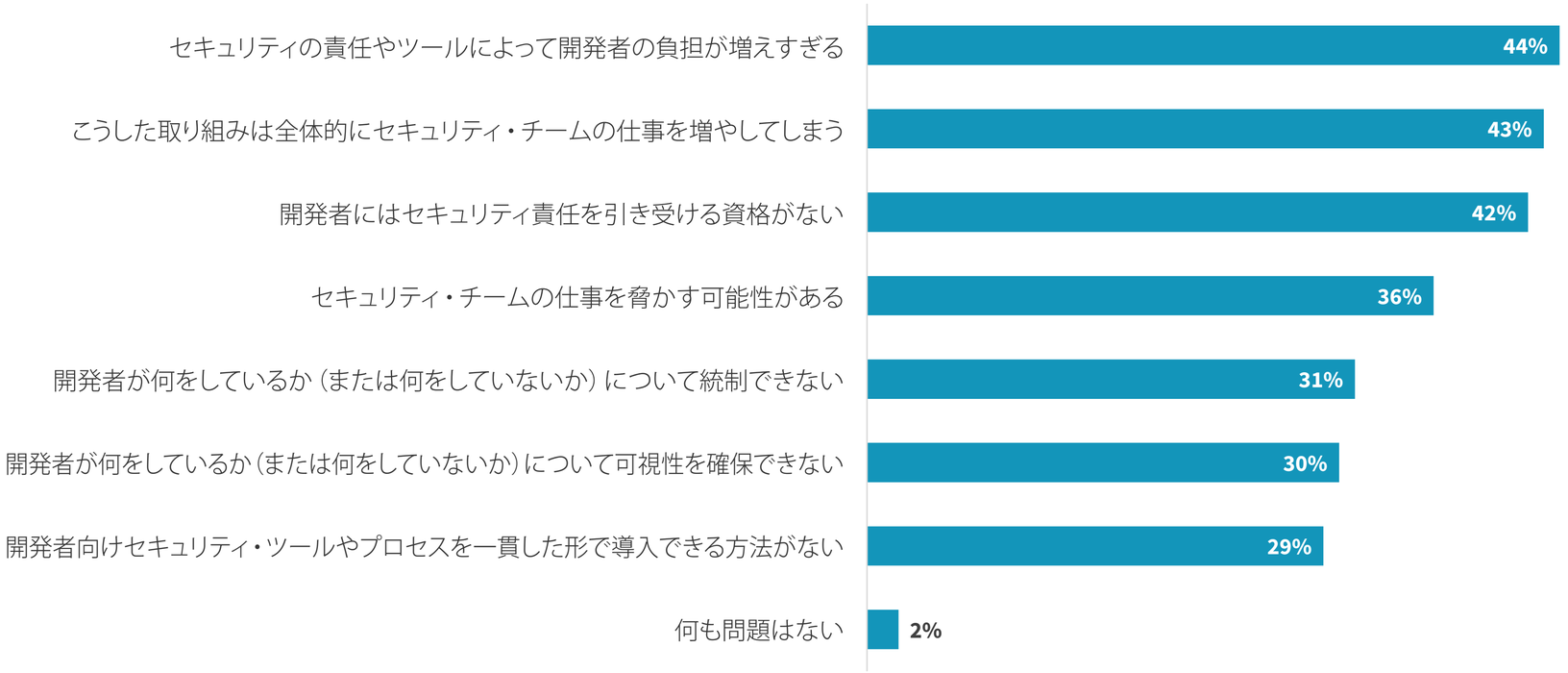
目次に戻る

セキュリティを開発チームにシフトする上での課題

セキュリティ・アクティビティおよびプロセスに対する開発者の関与を増やすことには明らかな利点があるものの、克服すべき課題もいくつか存在します。開発者がセキュリティ・タスクを引き受けることについての課題としては、セキュリティ責任を負うことで開発者の負担が増えすぎる（44%）、開発者にはセキュリティ責任を引き受ける資格がない（42%）とする意見や、それに関連し、こうした取り組みはサイバーセキュリティ・チームの仕事を増やしてしまう（43%）という意見が多く見られました。

“... 明らかな利点があるものの、
克服すべき課題もいくつか存在します。”

» 開発者がより多くのセキュリティ責任を負うことについての課題

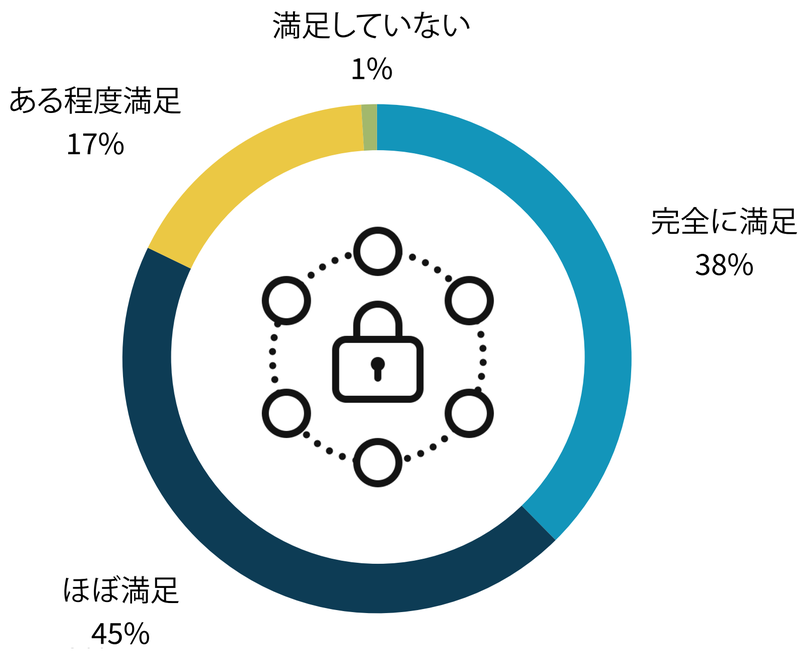


目次に戻る

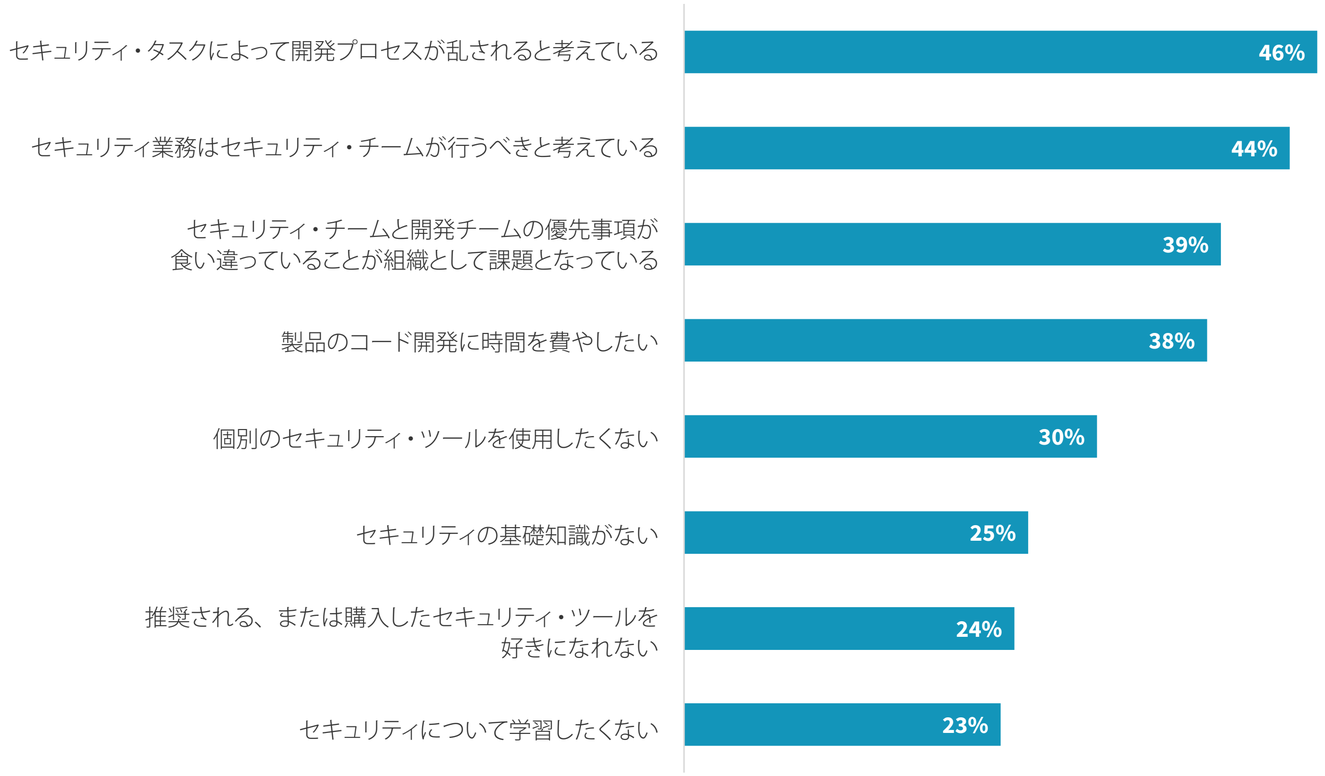
開発者にとっての課題

開発者の立場からは、これまで以上にセキュリティ責任を負うことについて完全に満足 (38%) またはほぼ満足 (45%) とする意見が大半を占めています。このシフト・レフト・ストラテジーについて「完全に満足」以外の回答をした開発者が不満を感じている理由としては、セキュリティ・タスクによって開発プロセスが乱される、セキュリティ・エコシステムに対してはセキュリティ・チームが全責任を負うべき、などが挙げられました。

» セキュリティへの関与が増えたことに対する開発者の満足度



» セキュリティ責任を負うことに開発者が不満を感じている理由



目次に戻る

組織はリスクを軽減するために監視やセキュリティ・テストを開発に組み込んでいる

開発ワークフロー外部のセキュリティ・ツール

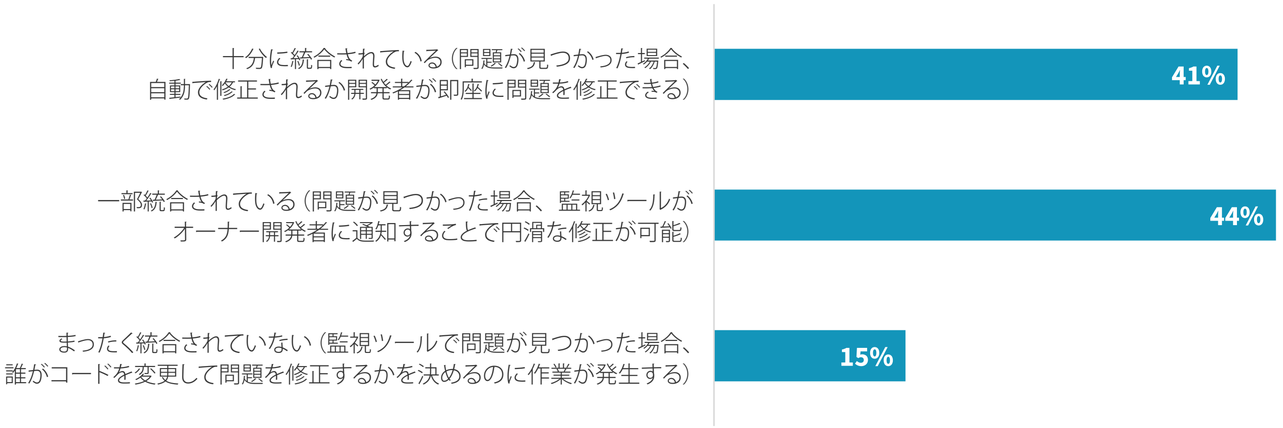
半数を超える（56%）組織が開発ツール内で動作するセキュリティ・ツールを使用していますが、44% は依然として個別のセキュリティ・ツールを使用してテストを実施しています。より多くの開発者に受け入れてもらうには、開発ワークフロー内で動作するセキュリティ・ツールを選び、コンテキストの切り替えなしにコーディングの問題を修正できるようにする必要があります。

» セキュリティ・ツールが開発ツールおよびワークフローに統合されているか

セキュリティ監視ツールと開発プロセスの統合

修正を迅速化するため、組織は監視ソリューションを開発者中心型のセキュリティ・ツールに統合しつつあります。このアプローチは、実行時にセキュリティの問題が見つかった場合に、セキュリティ・チームと開発チーム双方がそれほど時間をかけずに問題を効率的に修正できる方法として推奨されます。統合に成功すれば、開発者はセキュリティ・チームの助けを借りず問題を効率的に修正できるようになります。

» クラウド・セキュリティ監視ソリューションと開発プロセスの統合度



目次に戻る

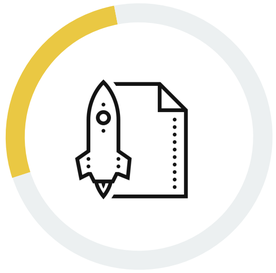
開発チーム内でのセキュリティ・テスト実施に関する主な課題

最近急速に増えている開発者中心型セキュリティ・ストラテジーの一環として、組織はサードパーティのペネトレーション・テスト・ツールやコンサルティング・サービスを利用するなど、さまざまなツールを導入してアプリケーションのセキュリティ確保に努めています。セキュリティ・チームは、セキュリティ・テストを開発者にシフト・レフトしようとしていますが、それには多くの課題が存在します。特に、テストが実施されたかどうかや、プロセスを乱すことなく開発者が必要な変更を実施できたかどうかについて、セキュリティ・チームが可視性と統制を確保することが大きな課題として挙げられています。

» クラウドネイティブ・アプリケーションのセキュリティ対策としてのサードパーティのペネトレーション・テスト・ソリューションまたはコンサルティング・サービスの利用

すべてのアプリケーションで利用

71%

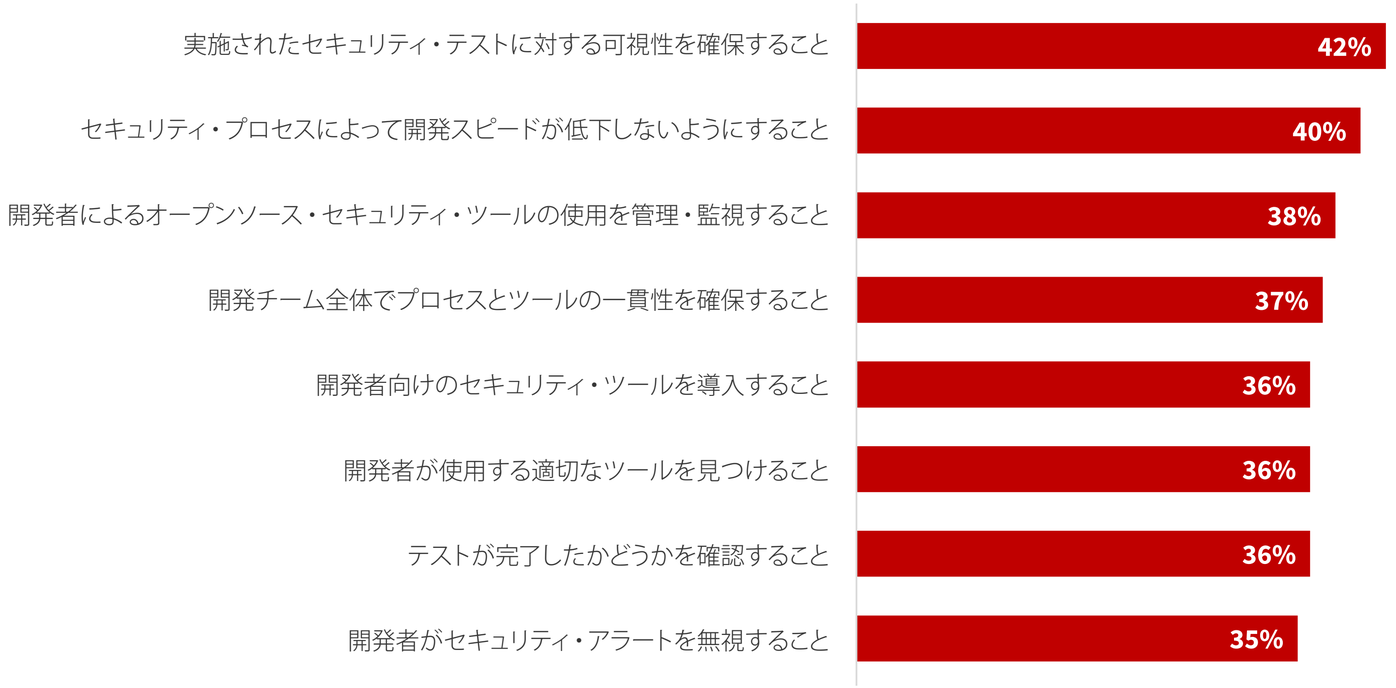


基幹業務系アプリケーションにのみ利用

27%

その他、1% はこれらのサービスを利用していないと回答。

» 開発チーム内でのセキュリティ・テスト実施に関する課題



目次に戻る

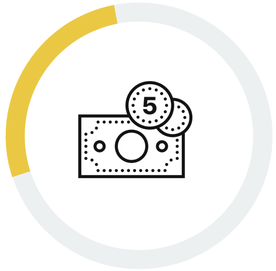
組織は開発プロセスの
セキュリティ対策に
投資をしている

組織は開発プロセスのセキュリティ対策に投資をしている

今後、クラウドネイティブ・ソフトウェアの開発プロセスに統合可能なセキュリティ・ソリューションへの大規模な投資を計画している組織は全体の 2/3 を超えています（69%）。具体的な投資対象としては、1/3 以上（34%）がアプリケーション・セキュリティ・テストの改善を挙げており、ソース・コード・リポジトリに保存されたシークレットの検出、実行時の API セキュリティ対策の適用を挙げた回答者もそれぞれ 31% ありました。

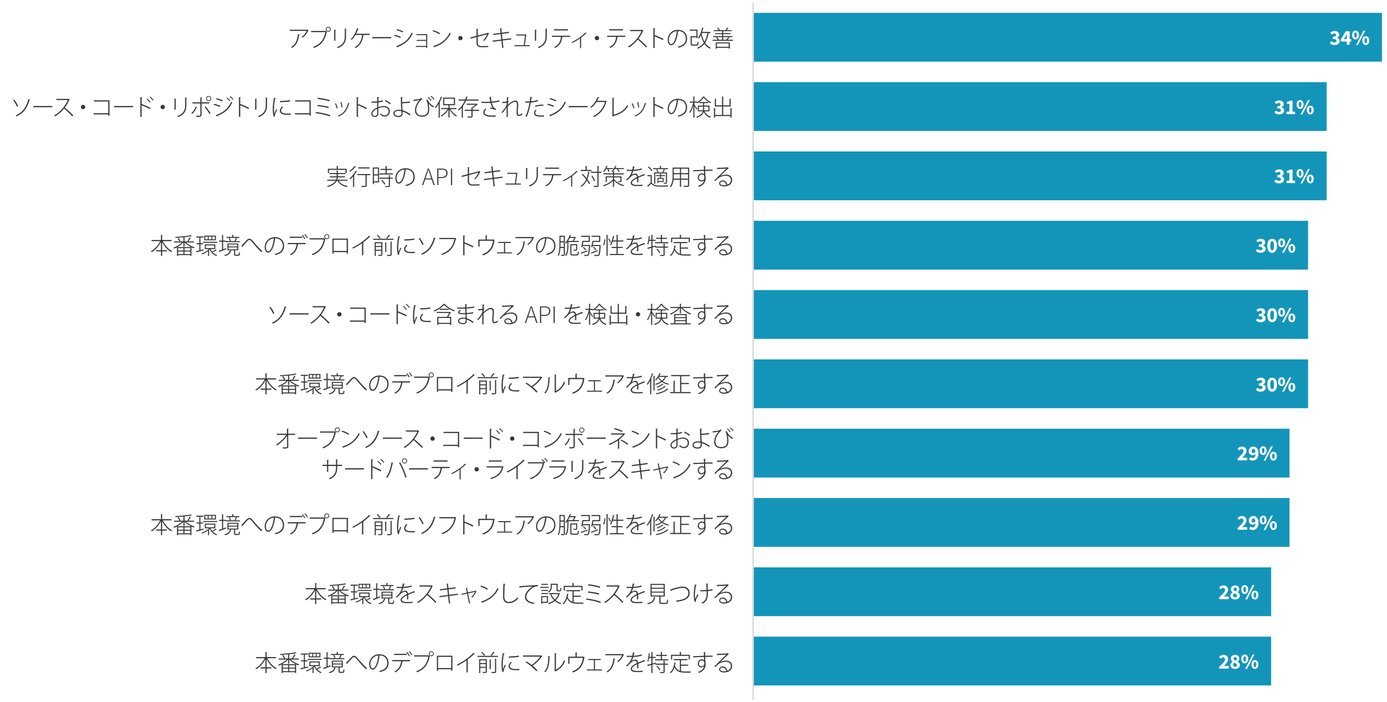
» クラウドネイティブ・ソフトウェアの開発プロセスに統合可能なセキュリティ・ソリューションへの投資計画

大規模な投資を計画している
69%



ある程度の投資を計画している
31%

» クラウドネイティブ・ソフトウェア開発プロセスのセキュリティ対策における優先事項トップ 10



目次に戻る

SYNOPSYS®

シノプシスは、開発チームがリスクを最小化しながらスピードと生産性を最大化しつつ、セキュアで高品質なソフトウェアを開発できるよう支援しています。アプリケーション・セキュリティ分野のリーダーとして定評のあるシノプシスが提供する静的解析、ソフトウェア・コンポジション解析、および動的解析ソリューションにより、自社開発コード、オープンソース・コンポーネント、およびアプリケーション動作に潜む脆弱性や不具合を迅速に見つけて修正することができます。

詳細はこちら

ESG について

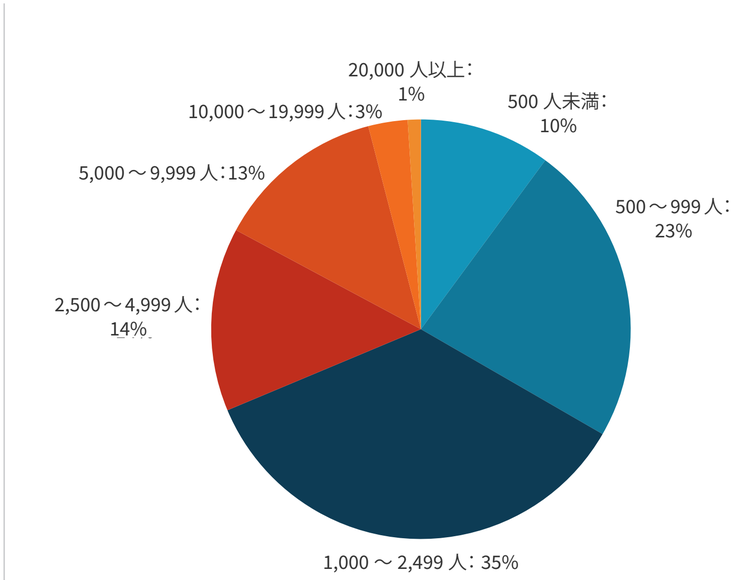
Enterprise Strategy Group はテクノロジーの分析、調査、戦略立案を総合的に手がけ、グローバルなテクノロジー・コミュニティに対してマーケット・インテリジェンス、実践的な知見、GTM（Go-to-Market）コンテンツ・サービスを提供しています。

調査の手法

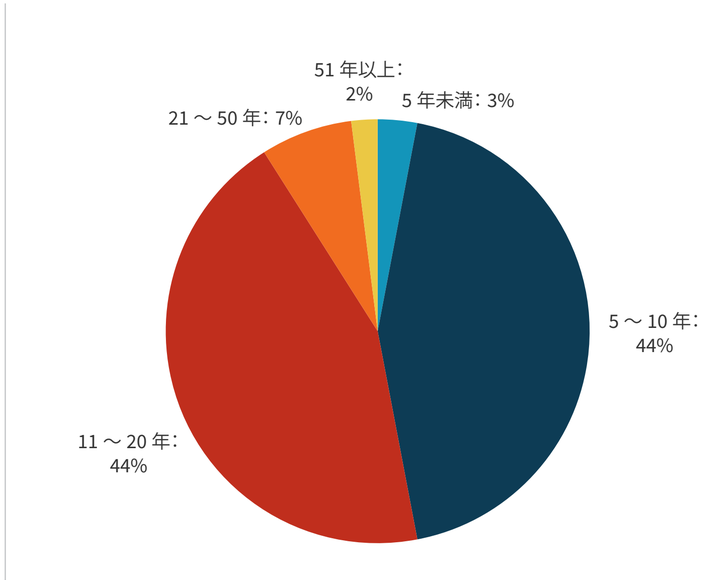
今回のレポート作成にあたり、ESG は 2022 年 5 月 18 日～ 2022 年 6 月 10 日にかけて、北米地域の民間企業および公的機関に所属する IT およびサイバーセキュリティの専門家とアプリケーション開発者を対象に包括的なオンライン調査を実施しました。今回の調査の有効性を担保するため、回答者は開発者中心型セキュリティ製品の評価、購入、および利用に関する責任者であることを資格としました。調査への協力を促すため、回答者全員に現金または現金相当の謝礼を提供しました。

資格を満たさない回答者、および重複回答を削除し、残った回答をさまざまな条件でスクリーニングしてデータの整合性を取った結果、最終的に合計 350 人の IT およびサイバーセキュリティ専門家とアプリケーション開発者がサンプルとして残りました。

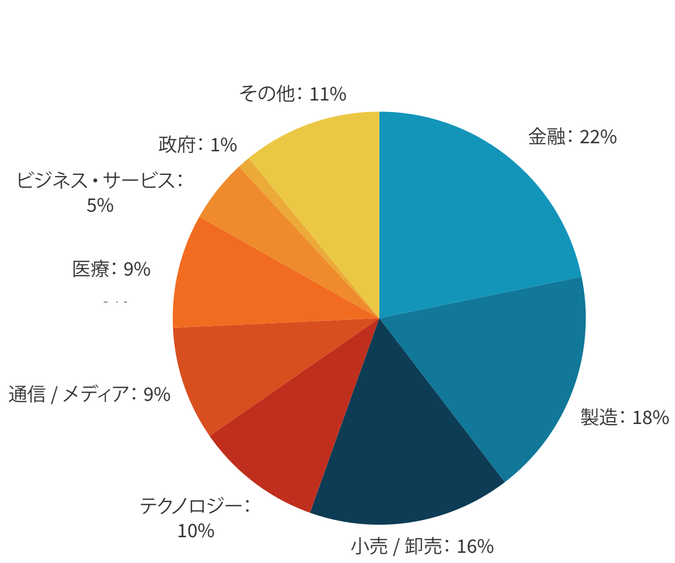
回答者の所属組織の従業員数



回答者の所属組織の設立年数



回答者の業種



目次に戻る

Enterprise Strategy Group はテクノロジーの分析、調査、戦略立案を総合的に手がけ、グローバルなテクノロジー・コミュニティに対して
マーケット・インテリジェンス、実践的な知見、GTM（Go-to-Market）コンテンツ・サービスを提供しています。