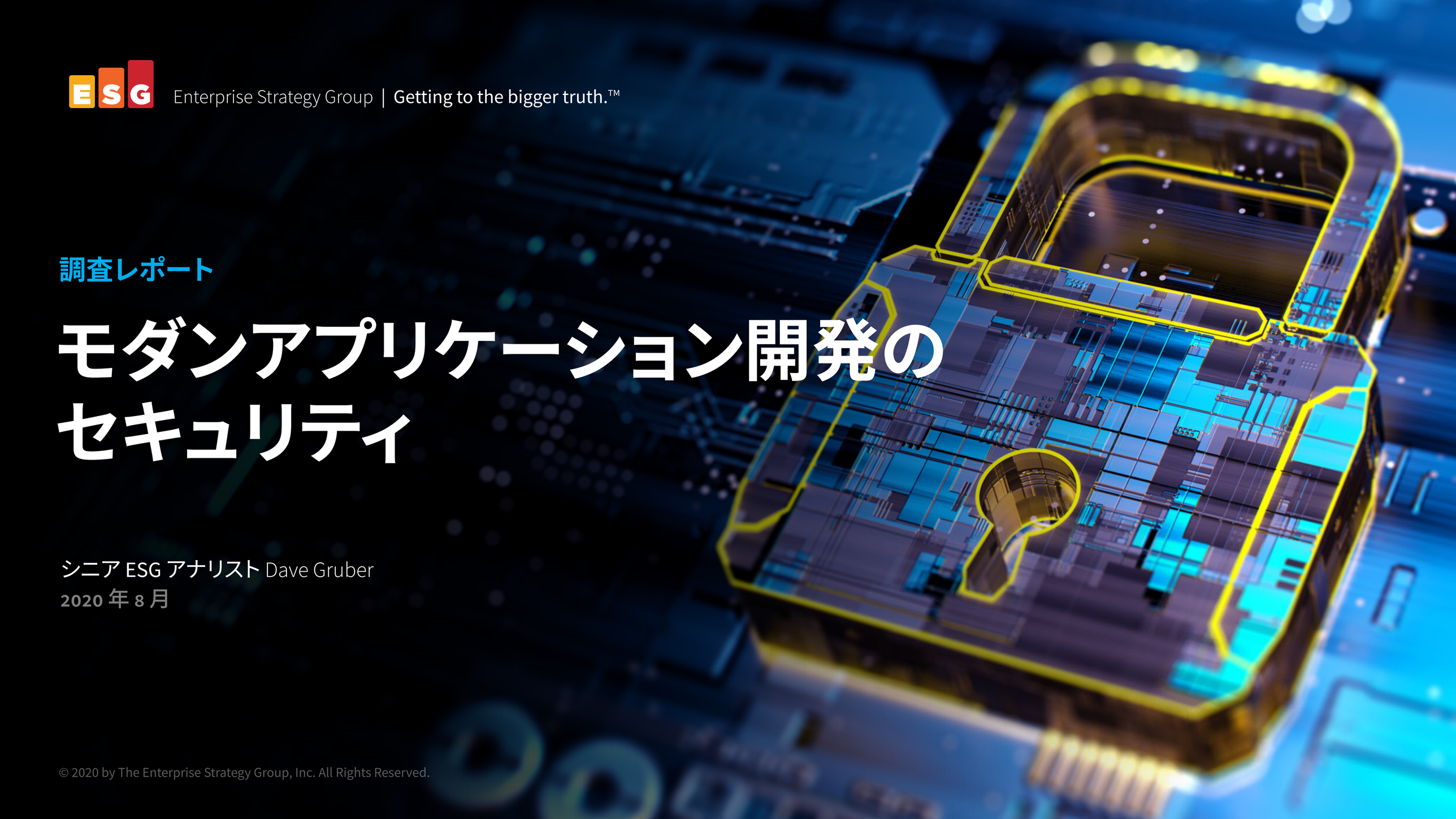
Enterprise Strategy Group | Getting to the bigger truth.™



調査レポート

モダンアプリケーション開発のセキュリティ

シニア ESG アナリスト Dave Gruber

2020 年 8 月

目次

調査の目的

モダンアプリケーションの開発現場では DevSecOps がセキュリティの前線へと躍り出て中心的な役割を果たしています。しかし、セキュリティチームと開発チームはそれぞれ独自の指標を元に動いているため、チーム間で目標を統一するのは困難です。ほとんどのセキュリティチームではモダンアプリケーションの開発手法を十分に理解できていないという事実が、この課題をさらに悪化させています。マイクロサービスを活用したアーキテクチャへの移行と、コンテナとサーバーレスの使用により、開発者のコードの構築、テスト、デプロイの方法にも大きな変化が起きています。

その結果、アプリケーションセキュリティツールを統合する動きが出始めています。複数のテスト用ツールや、複雑な優先度設定、防御策などによって生じる大量の問題や、問題の重複に組織は頭を悩ませています。必要なのは、統合型のアプリケーションセキュリティプラットフォームです。

こうしたトレンドを理解するために、ESG では北米（米国とカナダ）の組織でアプリケーション開発用のツールとプロセスに関わる IT 担当者、サイバーセキュリティ担当者、およびアプリケーション開発担当者 378 人にアンケートを実施しました。

この調査の目的

開発時のアプリケーションのセキュリティ管理策に関するアプリケーションセキュリティチームの**購入意向を調査**し、各ベンダーのさまざまなアプリケーションセキュリティソリューションに対する購買担当者の意向を評価する。

最新の開発手法とデプロイ手法をセキュリティチームが**どのレベル**まで理解し、リスクを軽減するためにどのポイントでセキュリティ管理策が必要かを特定する。

アプリケーションセキュリティへの投資に影響する**急所**、および意思決定者がどのように購入決定の優先度と時期を決めているかを理解する。

アプリケーションセキュリティソリューションの導入と管理に関する開発チームとサイバーセキュリティチームの力関係を**把握する**。

目次に戻る

調査結果の概要

大半の組織は自社のアプリケーションセキュリティプログラムが強固だと考えているが、多くの組織で依然として脆弱なコードをリリースしている。

適切なアプリケーションセキュリティプログラムを用意したからといって、脆弱性のあるコードのリリースが防止できるとは限りません。異なる点は、脆弱性のあるコードをリリースしている人物はその脆弱性を認識しており、それがもたらすリスクも完全に理解しているということです。アプリケーションを保護するには、潜在的なリスクを定期的に選別して優先度を設定することで、開発者が重要な納期を守りながらリスクを軽減できるようにする必要があります。

現在使われているさまざまなアプリケーション開発モデルやデプロイモデルを保護するには複数のセキュリティテストツールが必要である。

アプリケーションセキュリティが成熟するなか、1 つのテスト手法だけで開発チームがすべてのセキュリティリスクを軽減することはできなくなっています。そのため、多くの場合、複数のベンダーから複数のツールを導入してソフトウェア開発ライフサイクルを保護する必要があります。ツールの使い方やどのツールを重視するかは組織によって異なりますが、大半の組織ではさまざまなツールを組みわせてセキュリティの要件を満たしています。

開発者向けのセキュリティトレーニングは定期的には実施されておらず、開発者のセキュリティスキルを向上するプログラムが不足している。

大半の組織では、一定のセキュリティトレーニングを開発者向けに実施していますが、50% 以上の組織はトレーニングの実施頻度が年に一度以下となっています。ほとんどの場合、開発マネージャーがこのトレーニングを担当することになります。一方で、多くの組織ではセキュリティ問題を多数引き起こした経歴がある開発チームや開発者向けの是正トレーニングの多くをアプリケーションセキュリティアナリストが担っています。

多くの組織にとって AppSec テストツールの増加が課題となっており、1/3 以上の組織がツールの統合への投資に力を入れている。

セキュリティ制御の他のカテゴリー同様、多くの組織では統合と管理が難しいツールを多数導入しています。これにより、プログラムの効果が低下し、大量の人員をツールの管理に割くことになります。約 1/3 の組織がこの問題に直面しており、増加したツールの統合と簡素化に向けた将来の投資を検討しています。

半数以上の組織がアプリケーションセキュリティへの支出を大幅に増やすことを計画している。

44% の組織がクラウドのアプリケーションセキュリティへの投資を検討する一方で、1/3 の組織はプロセスを簡略化するためのツールの統合に力を入れています。また、開発チームやアプリケーションでテスト用ツールの利用率を高めるための投資を計画している組織もあります。

目次に戻る

大半の組織は自社のアプリケーション
セキュリティプログラムが強固だと
考えているが、多くの組織で依然として
脆弱なコードがリリースされている

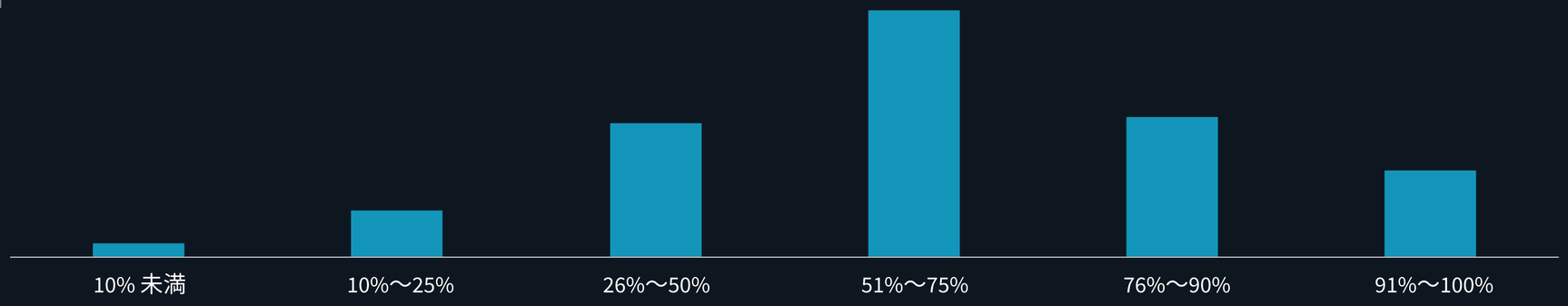
大半の組織は自社のアプリケーションセキュリティプログラムが非常に優れていると考えている

大半の組織は自社のアプリケーションセキュリティプログラムが非常に優れていると考えています。1/3 以上の組織が自社のプログラムを 9 点または 10 点と評価しており、全体の平均は 7.92 点となっています。このような高い点数がついているのは、過去数年にわたってアプリケーションセキュリティプログラムに継続的に投資してコードカバレッジのレベルを高めてきたためです。しかし、依然としてコードカバレッジは完全には程遠く、コードベースの 3/4 以上で AppSec ツールを使っている組織はわずか 34% です。

36%

の組織が自社のアプリケーションセキュリティプログラムを 9 点または 10 点と評価

AppSec ツールで保護されているコードベース

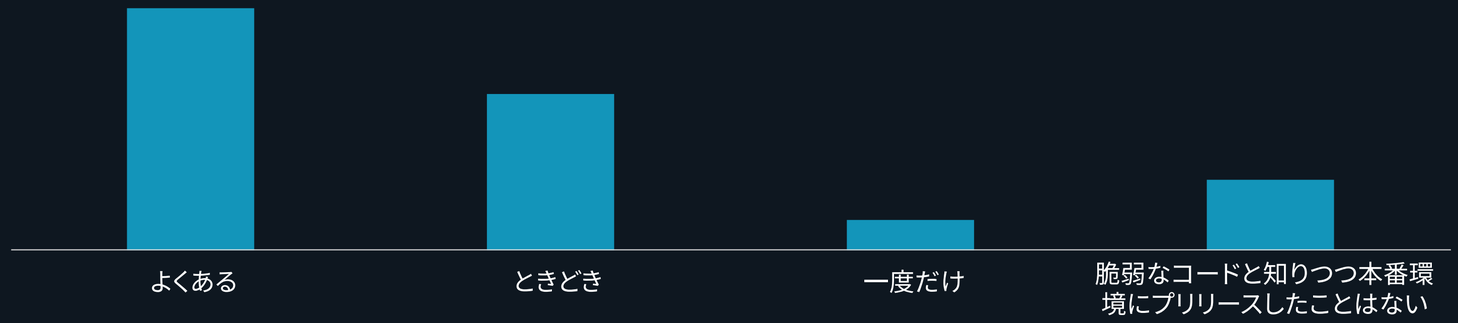


目次に戻る

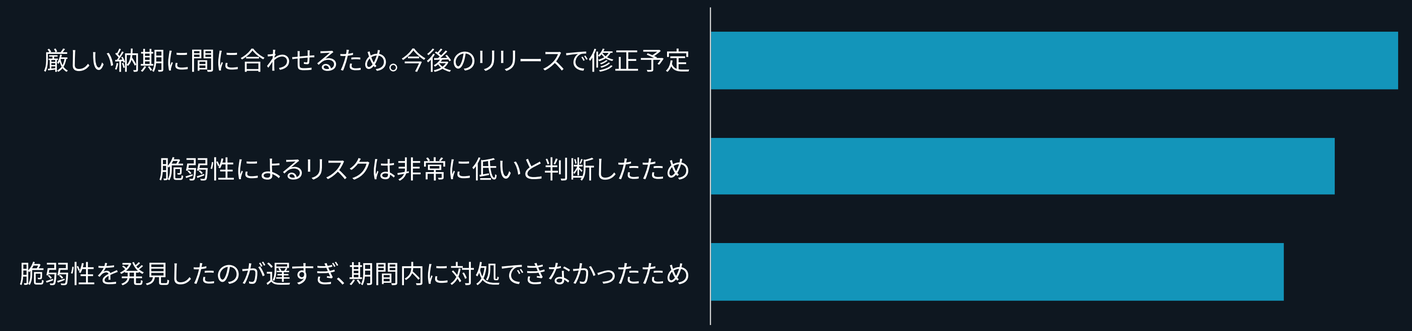
適切なプログラムの実施にもかかわらず、多くの組織で脆弱性のあるコードが定期的にリリースされている

適切なアプリケーションセキュリティプログラムを用意したからといって、脆弱性のあるコードのリリースが防止できるとは限りません。異なる点は、脆弱性のあるコードをリリースしている人物はその脆弱性を認識しており、それがもたらすリスクも完全に理解しているということです。アプリケーションを保護するには、潜在的なリスクを定期的に選別して優先度を設定することで、開発者が重要な納期を守りながらリスクを軽減できるようにする必要があります。開発サイクルの終了間際に発見された脆弱性はほとんどの場合解決できないため、納期までに重大な問題を解決するのに十分な時間が取れるよう、スケジュールのなるべく早い段階でアプリケーションのセキュリティを確認することが重要です。

脆弱性のあるコードがリリースされていますか？



組織が脆弱性のあるコードをリリースする理由



目次に戻る

多くの組織が依然として攻撃の被害を受けている

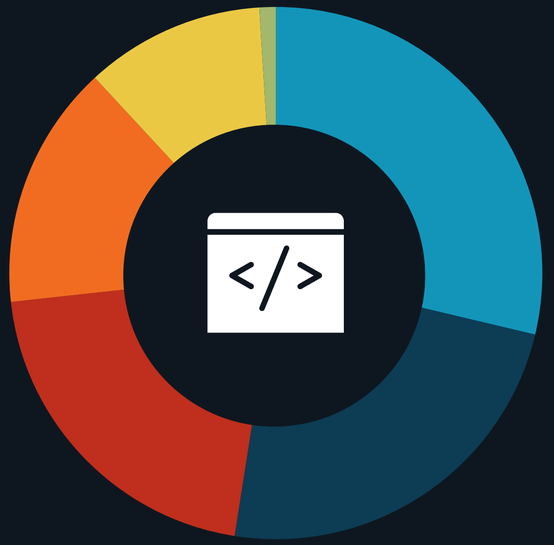
AppSec プログラムへの投資を増やすことでリスクが軽減されている一方で、依然として 60% の組織が OWASP トップ 10 の脆弱性の被害を受けています。こうした被害は必ずしも脆弱性が発見された既知のコードによるものではありませんが、コードカバレッジやソフトウェア開発ライフサイクル全体でのテストの頻度、特定した脆弱性の優先度設定などの取り組みが必要であることを示しています。

では、既知の脆弱性が含まれるコードをリリースする決定を下すのは誰なのでしょうか。開発マネージャーとセキュリティアナリストが共同でこの決定を下していることもよくありますが、多くのチームでは 1 人の担当者が最終決定を行っています。つまり、アプリケーションセキュリティプロセス全体を管理する方法は開発組織によって異なり、セキュリティチームがそれを担当する組織がある一方で、開発マネージャーが担当する組織もあります。

60%

の組織が、過去 12 ヵ月で本番アプリケーションについて OWASP トップ 10 の脆弱性の被害を受けている

コードをリリースする決定を下すのは誰ですか？

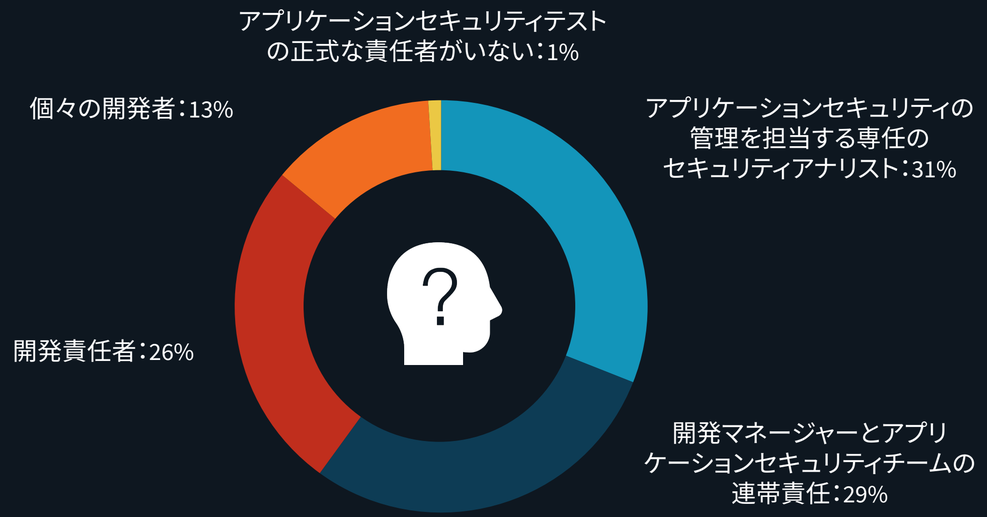


目次に戻る

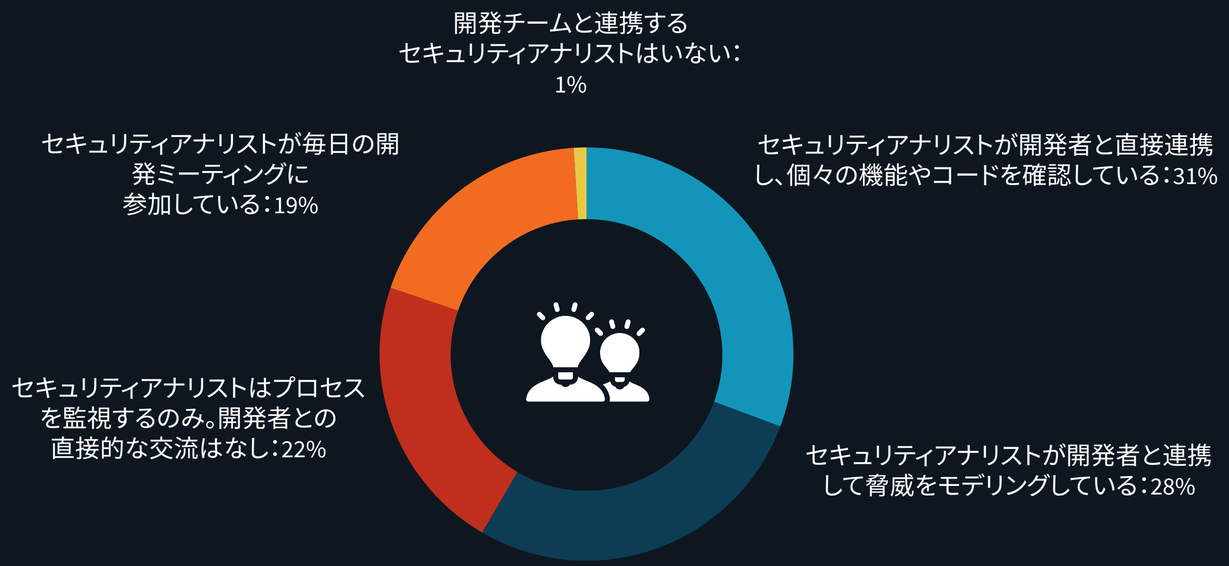
AppSec のテストへのセキュリティアナリストの関与が増えている

多くの組織では開発マネージャーやアプリケーションセキュリティアナリストがプログラムのテストの責任者となっていますが、プログラムの責任を共同で負っている組織は 29% に過ぎません。セキュリティアナリストは、開発者が安全なアプリケーションを構築するうえで重要な役割を担っています。セキュリティアナリストが開発者と直接やりとりしていると回答した組織の割合は 78% にのぼります。個別の機能やコードを確認するために開発者と直接やりとりしているアナリストは 31%、脅威のモデリングを開発者と一緒に行っているアナリストは 28%、デイリースクラムに参加しているアナリストは 19% です。このようにアナリストが開発者と深く関わることで、学習と管理が促進され、安全なアプリケーションを構築できるようになります。

アプリケーションセキュリティテストのオーナーシップ



セキュリティアナリストがプログラムの改善で果たす役割



目次に戻る

AppDev セキュリティプログラムで 最も効果的な 10 個の要素

1. アプリケーションセキュリティの制御が CI/CD ツールチェーンと密接に統合されている。

2.アプリケーションセキュリティのベストプラクティスが正式に文書化されている。

3.アプリケーションセキュリティトレーニングが進行中の開発セキュリティトレーニングプログラムの一環として含まれている。

4.開発マネージャーが開発者にベストプラクティスを提供している。

5.正式なアプリケーションセキュリティトレーニングプログラムへの開発者の参加率が高い。

6.発生したセキュリティ問題を開発チームごとに記録している。

7.正式なプロセスと指標によってアプリケーションセキュリティの継続的な改善を記録している。

8.各開発チームの改善が分かる指標が継続的に記録されている。

9.コード開発プロセス中のセキュリティ問題が記録されている。

10.自動化されたリスク集約ツールでリスクをまとめて上級開発リーダーにその情報を提供している。

目次に戻る

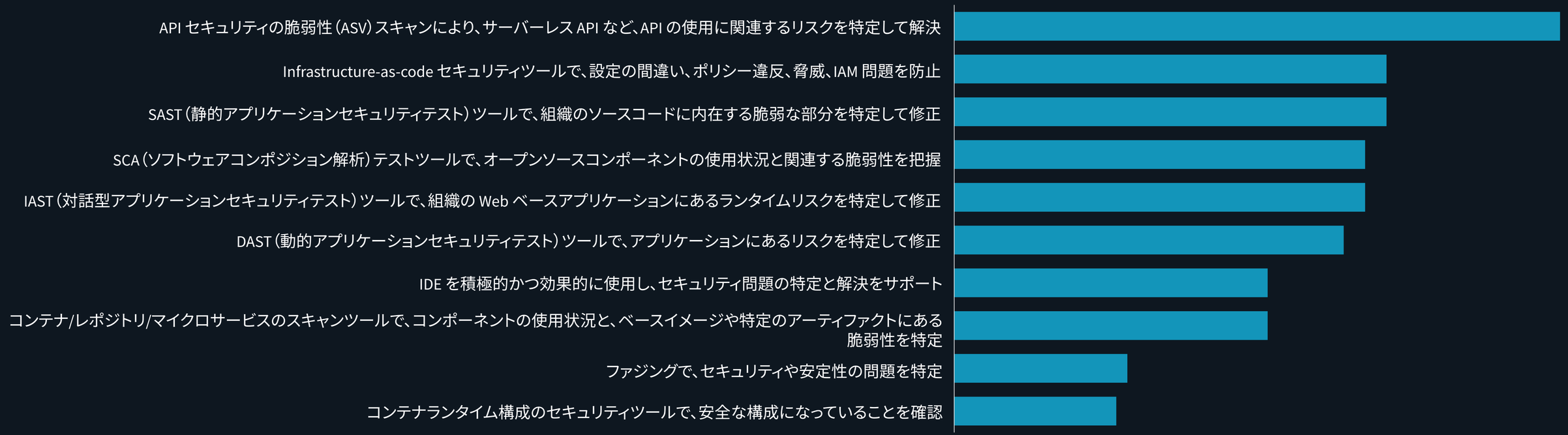
現在使われているさまざまなアプリケーション
開発モデルやデプロイモデルを保護するには
複数のセキュリティテストツールが必要である。

さまざまな AppSec テストツールの使用

アプリケーションセキュリティが成熟するなか、1 つのテスト手法だけで開発チームがすべてのセキュリティリスクを軽減することはできなくなっています。そのため、多くの場合、複数のベンダーから複数のツールを導入してソフトウェア開発ライフサイクルを保護する必要があります。ツールの使い方やどのツールを重視するかは組織によって異なりますが、大半の組織ではさまざまなツールを組みわせてセキュリティの要件を満たしています。

新たな開発モデルやデプロイモデルが登場しているため、それらを保護する新たなテストツールが作られています。テストプラットフォームを拡大する組織がある一方で、長期にわたって 1 つのツールを利用する組織もあります。

アプリケーションセキュリティテストのオーナーシップ

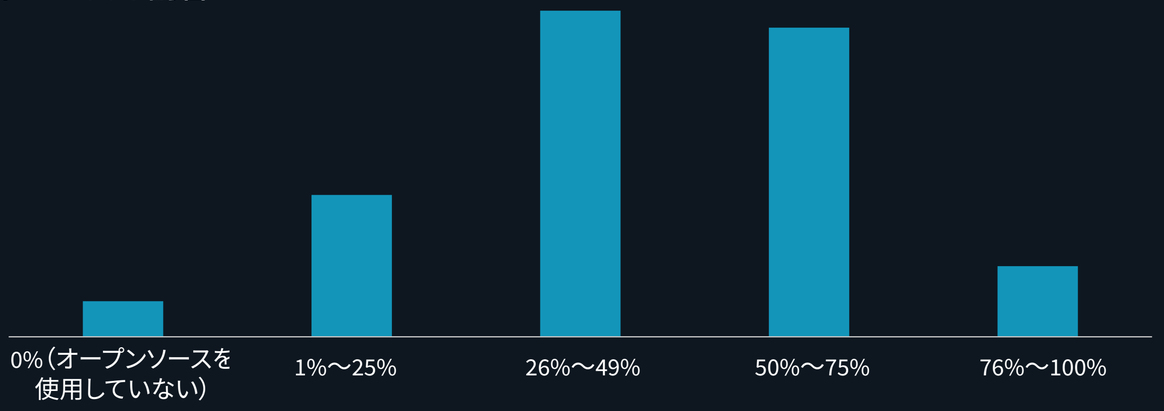


目次に戻る

最新のコードベースはオープンソースに大きく依存しているが、現在オープンソースのセキュリティ管理を使用している組織は半数にも満たない

長年にわたってさまざまなタイプのテストツールが利用されてきましたが、その利用状況は適正なレベルには達していません。たとえば、モダンアプリケーション開発でオープンソースソフトウェアが多く使用されている一方で、オープンソースセキュリティテストツールを現在利用していると回答した開発チームは半数に届きません。多くの組織は計画はしているものの、多くの企業における現在のアプリケーションセキュリティテストの導入状況を示した以下のグラフからもそのトレンドは不安定であることがわかります。

オープンソースを含むコードベースの割合



48%

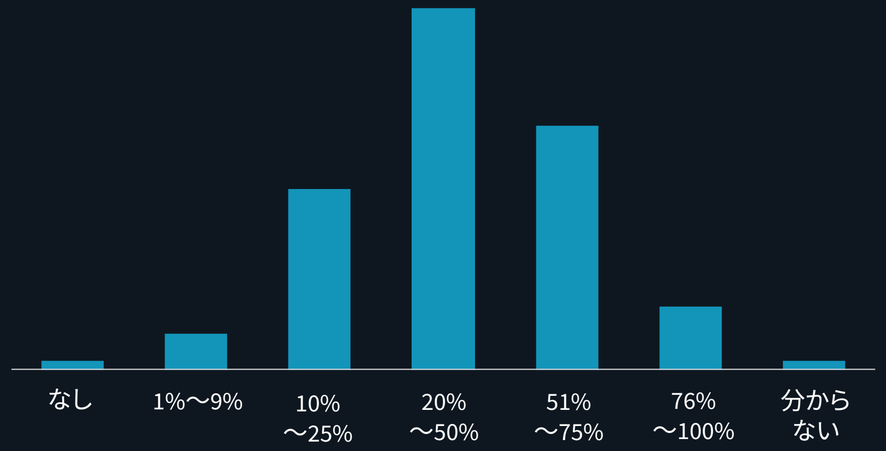
の組織は、すでにオープンソースの脆弱性をスキャンするために特定のセキュリティ管理に投資している。

目次に戻る

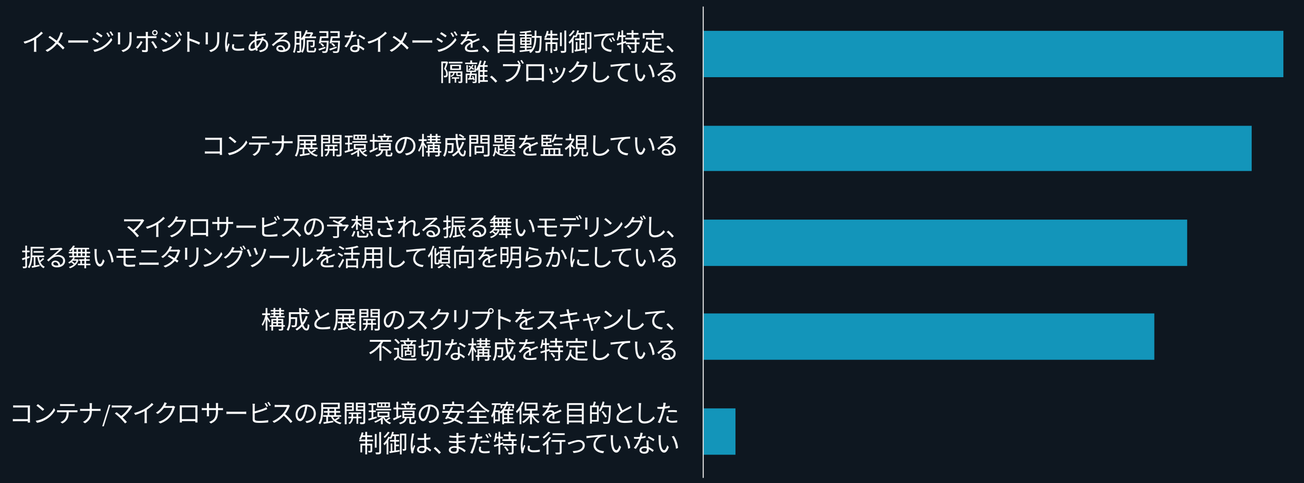
マイクロサービスコンテナ開発への移行

より新しい開発モデルやデプロイモデルでは、早い段階からセキュリティに注目している場合があります。このページのグラフからもわかるとおり、比較的短い期間でマイクロサービスコンテナ開発の導入が進んでおり、特定のセキュリティ管理の利用が進んでいます。他のクラウド開発モデルやデプロイモデルでも、利用状況のパターンは類似しています。

コンテナを使用している開発チームの割合



コンテナを保護するための対策



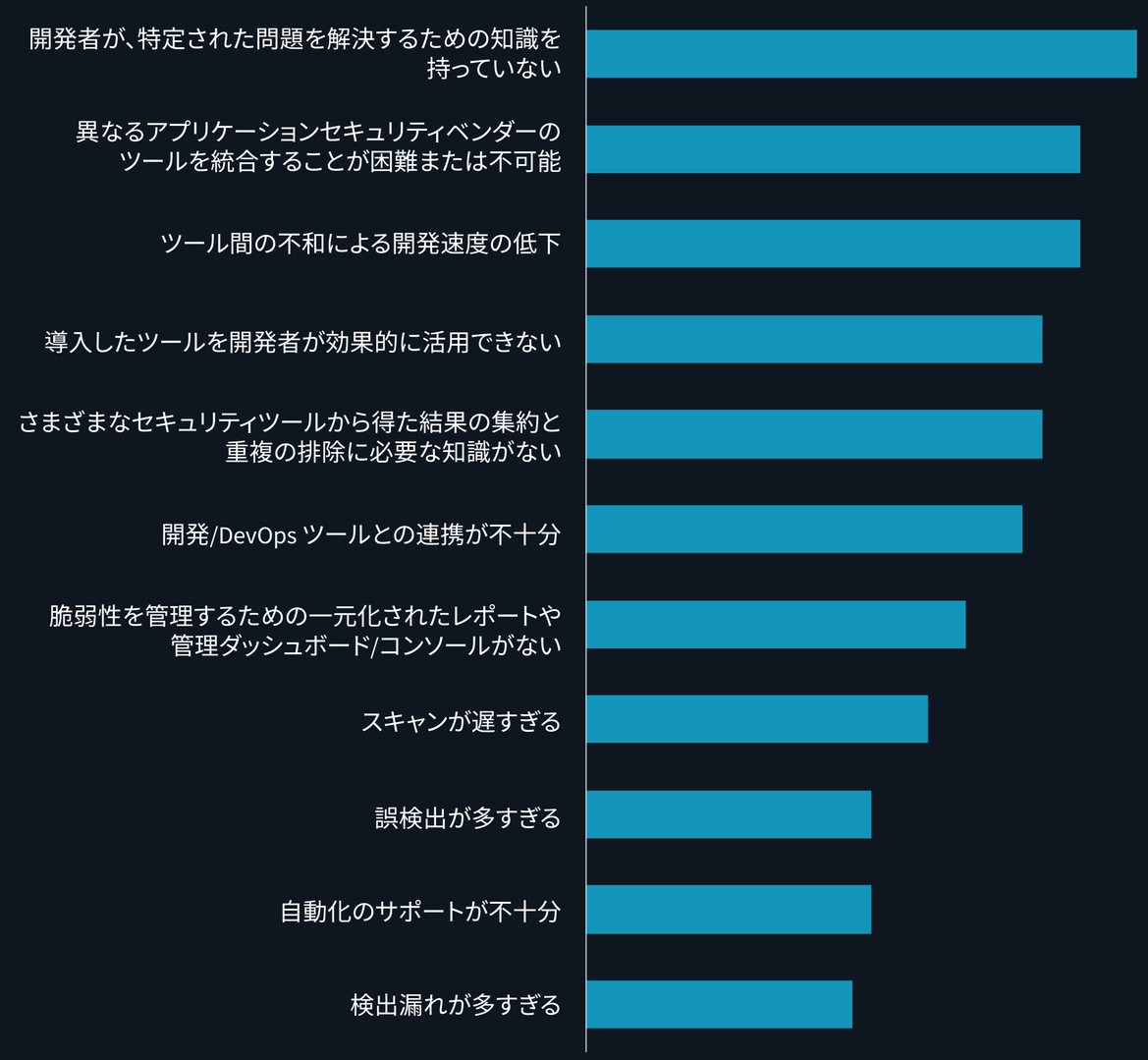
目次に戻る

現在のテストツールにおける課題

最終的には、特定したセキュリティ問題を解決するかどうかは開発者次第です。しかし、開発者にそのための知識が不足していることが現在のツールにおいてよくある課題だと多くの組織が回答しています。セキュリティツールベンダーはジャストインタイムのトレーニングや推奨される修正を通じてガイダンスを提供していますが、開発者は業務に追われています。問題を解決するには特定のコードによってどのように問題が引き起こされるかを深く理解する必要があります。開発者向けのセキュリティトレーニングは、問題解決を促進するものでなければなりません。

AppSec ツールとの統合に苦労する組織がある一方で、多くの組織は、ツールの追加に伴う作業の増加による開発プロセス全体の遅延を懸念しています。

現在のテストツールにおける主な課題

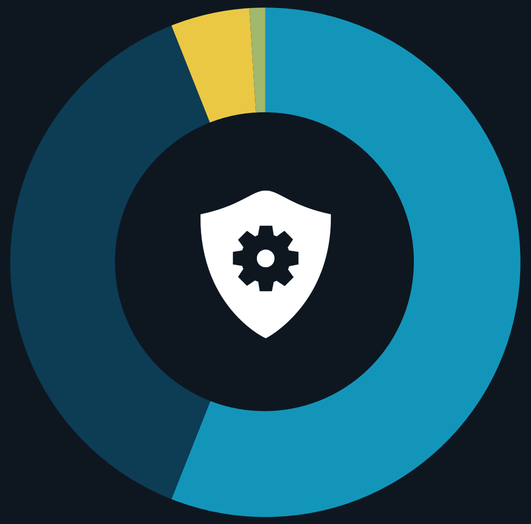


目次に戻る

アプリケーションセキュリティプログラムの改善には DevOps の統合が重要

システム開発ライフサイクル全体でアプリケーションセキュリティテストを自動化することで、プログラムの成功を促進できると多くの組織が考えています。DevOps の統合によって摩擦を軽減しながら開発の初期段階でセキュリティを確認することにより、セキュリティ問題を早期に特定することができます。開発者の教育やツールとプロセスの改善は間違いなくプログラムを良い方向に導きますが、モダンアプリケーション開発手法においては自動化が主役になります。

DevOps と AppSec の統合のレベル

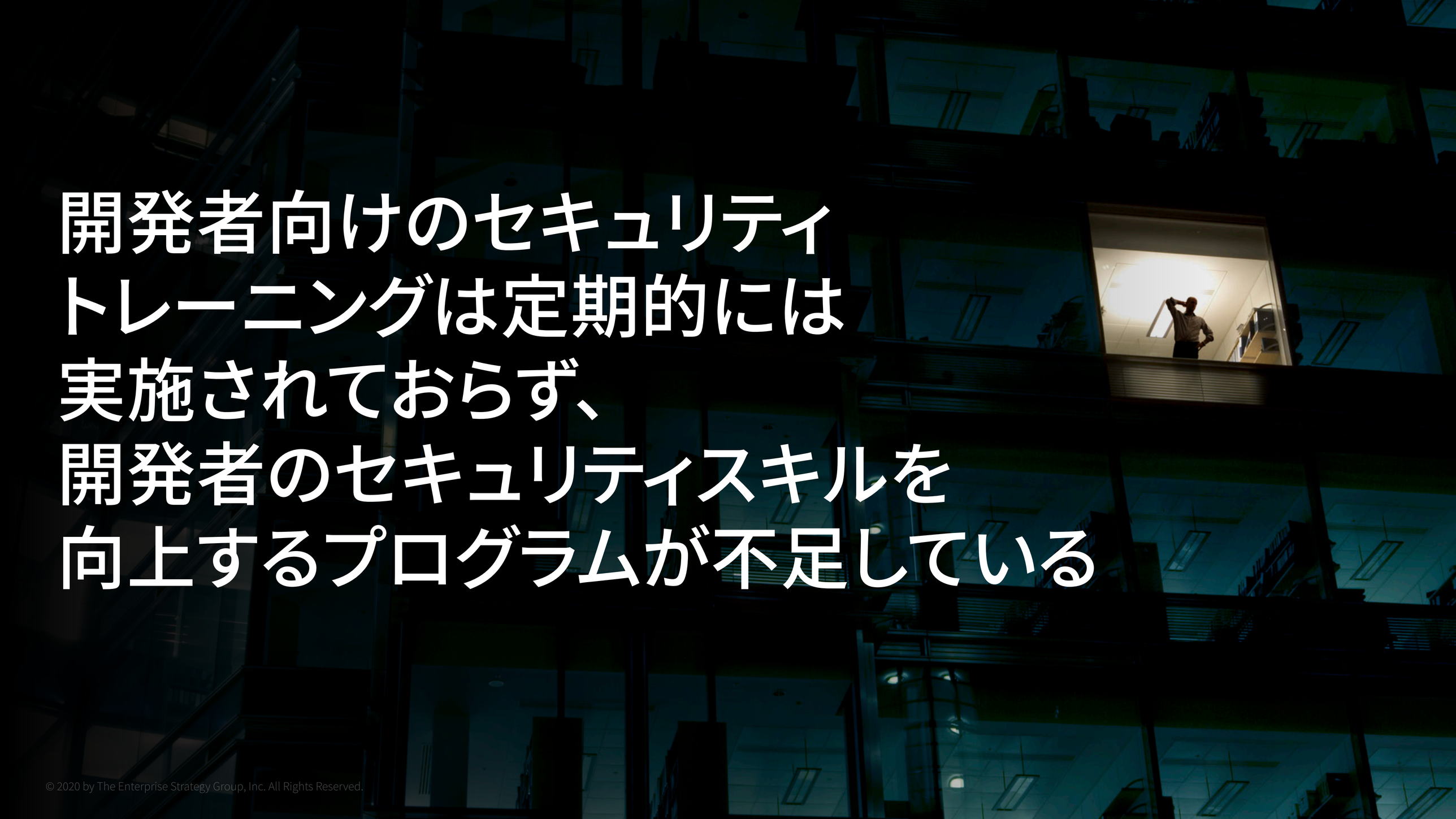


- DevOps プロセス全体で、高度に統合されたセキュリティ管理システムを活用している
- 管理機能を厳選して使用しているが、他の管理機能との統合にも継続的に投資している
- アプリケーションセキュリティツールがプロセスに適切に統合されていない
- セキュリティには、可能な限りプロセスの初期段階で取り組んでいる

43%

の組織が、AppSec プログラムを改善するうえで DevOps の統合が最も重要だと考えている。

目次に戻る

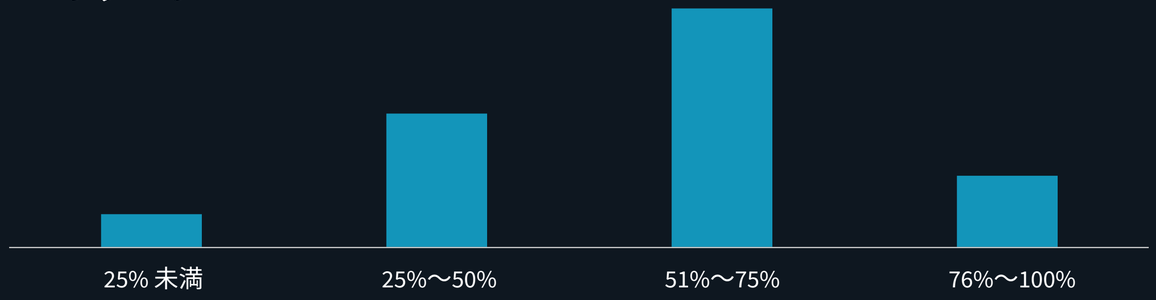


開発者向けのセキュリティ
トレーニングは定期的には
実施されておらず、
開発者のセキュリティスキルを
向上するプログラムが不足している

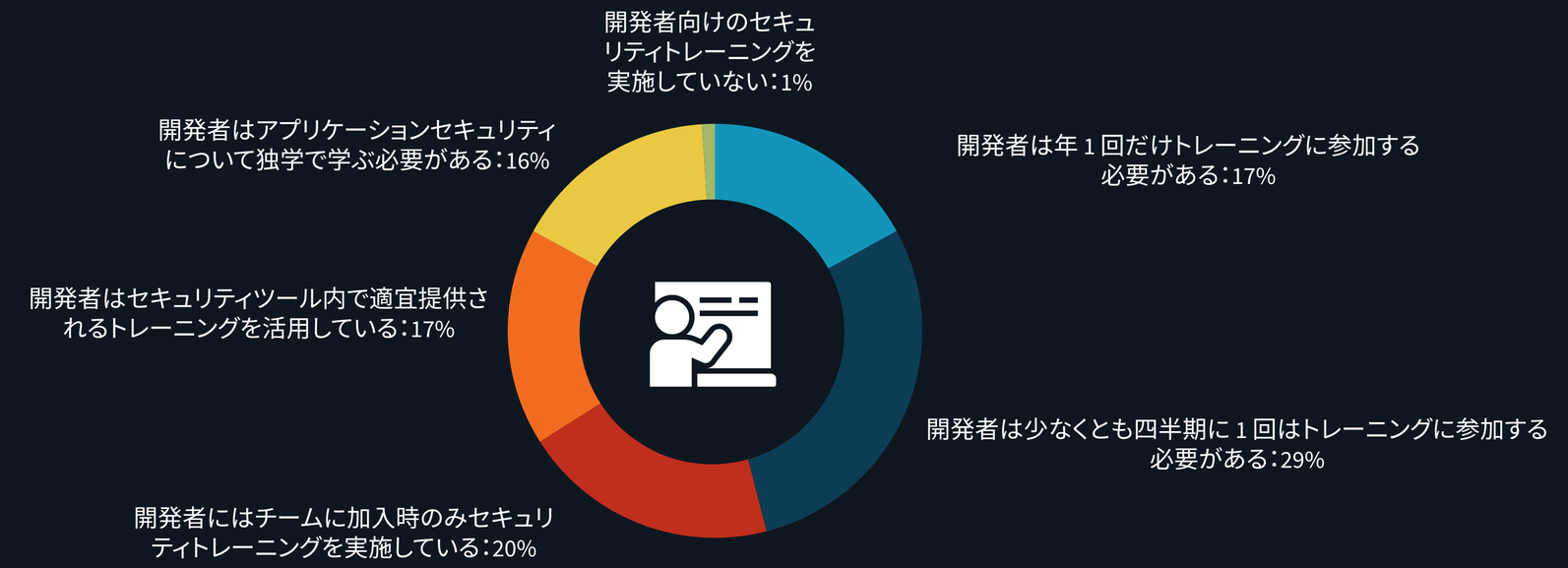
大半の組織が AppSec トレーニングの受講を開発者に義務付けている

ほとんどの組織はアプリケーションセキュリティトレーニングに参加することを開発者に義務付けていますが、35% の組織が、正式なトレーニングに参加する開発チームは全体の半数に満たないと回答しています。開発者全員がトレーニングに参加していると回答した組織の割合はわずか 15% です。頻度については、1 年に一度以上正式なトレーニングに参加するよう開発者に義務付けている組織は半数未満です。

正式なセキュリティトレーニングへの開発者の参加率



アプリケーション開発者向けセキュリティトレーニングの要件

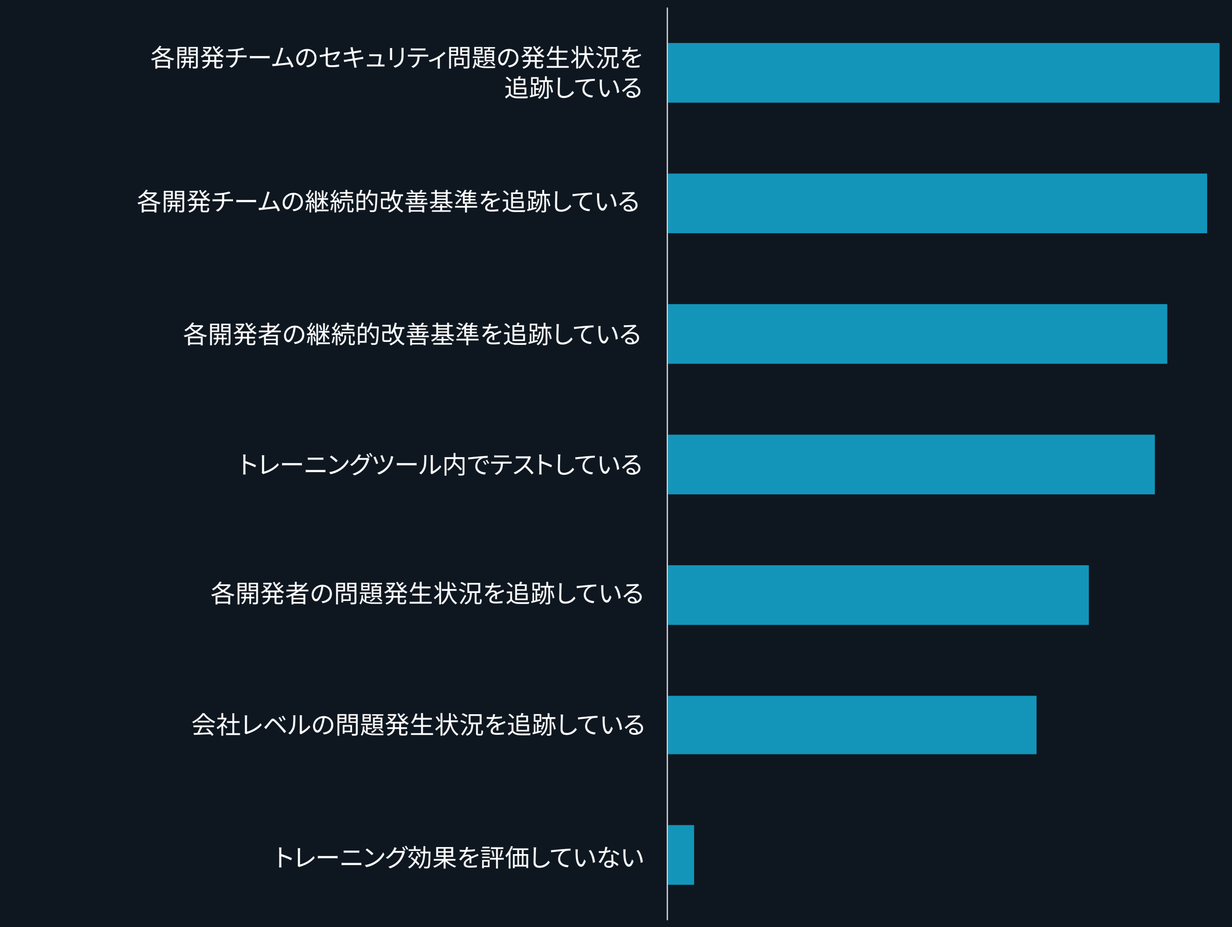


目次に戻る

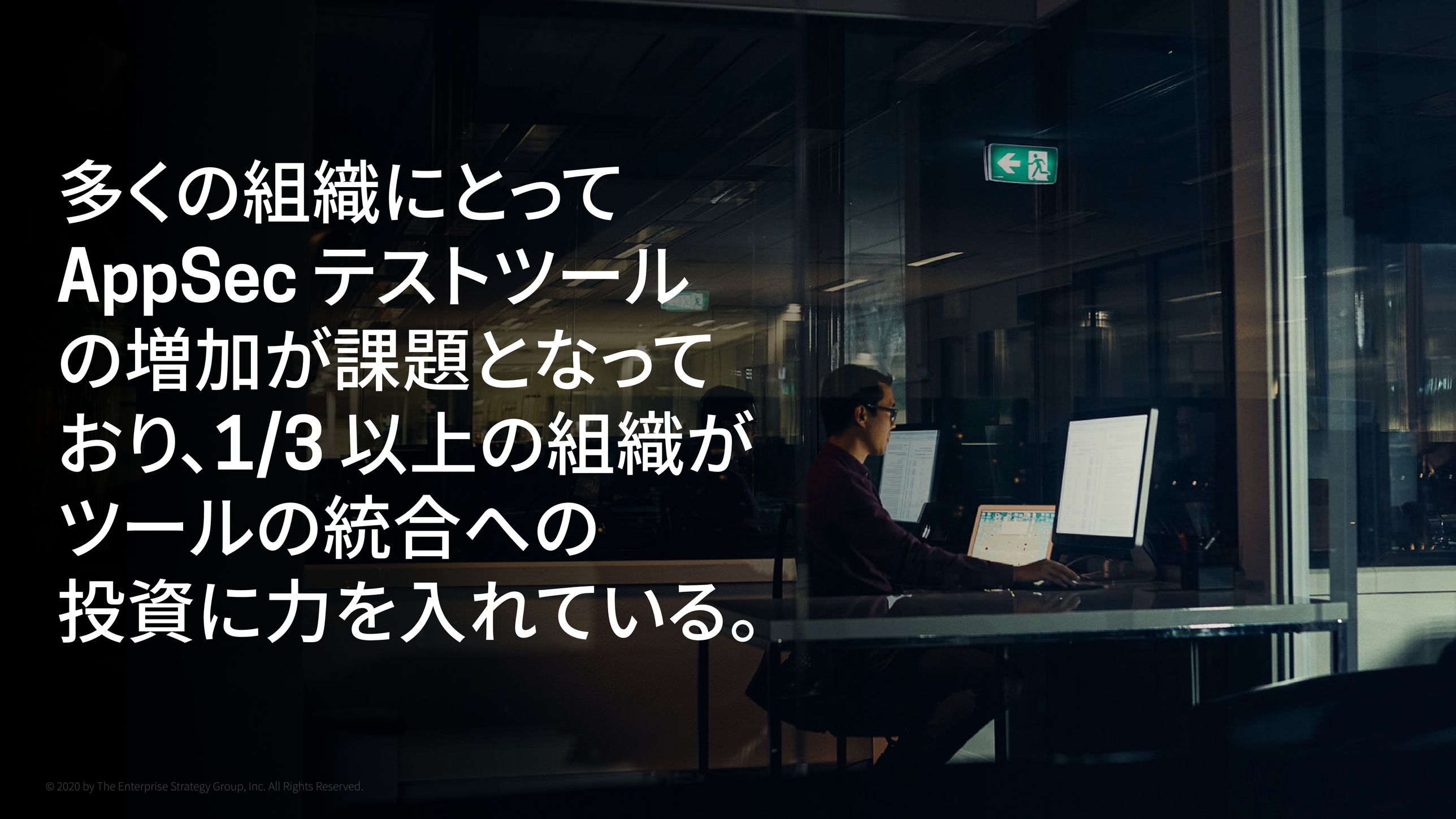
大半の組織で開発者向けセキュリティトレーニングの効果を測定するプログラムが不足している

セキュリティプログラムを継続的に改善するには、開発チームと開発者によって引き起こされた問題を測定する必要があります。発生した問題と継続的な改善の指標を記録することで、最も多くの問題を引き起こしているチームや個人を改善するための取り組みを絞り込むことができます。しかし、これを実施している組織は 40% 強です。

アプリケーション開発チーム向けセキュリティトレーニングの効果の測定方法



目次に戻る

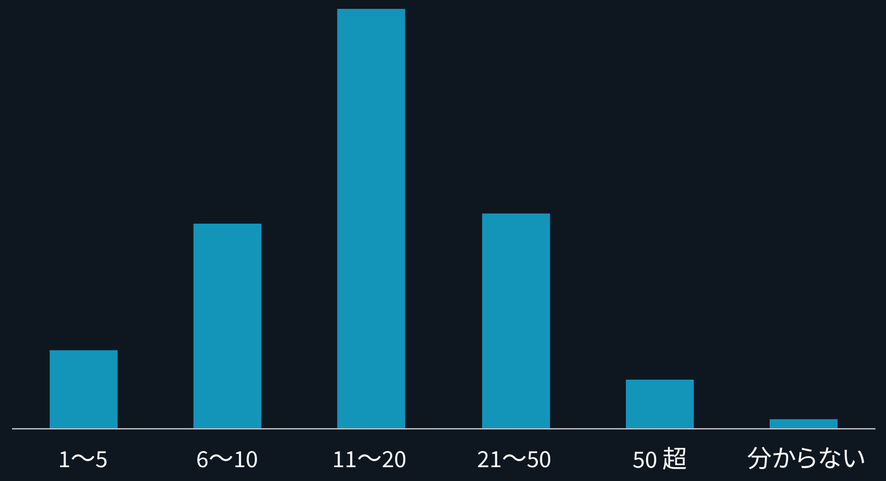


多くの組織にとって
AppSec テストツール
の増加が課題となって
おり、1/3 以上の組織が
ツールの統合への
投資に力を入れている。

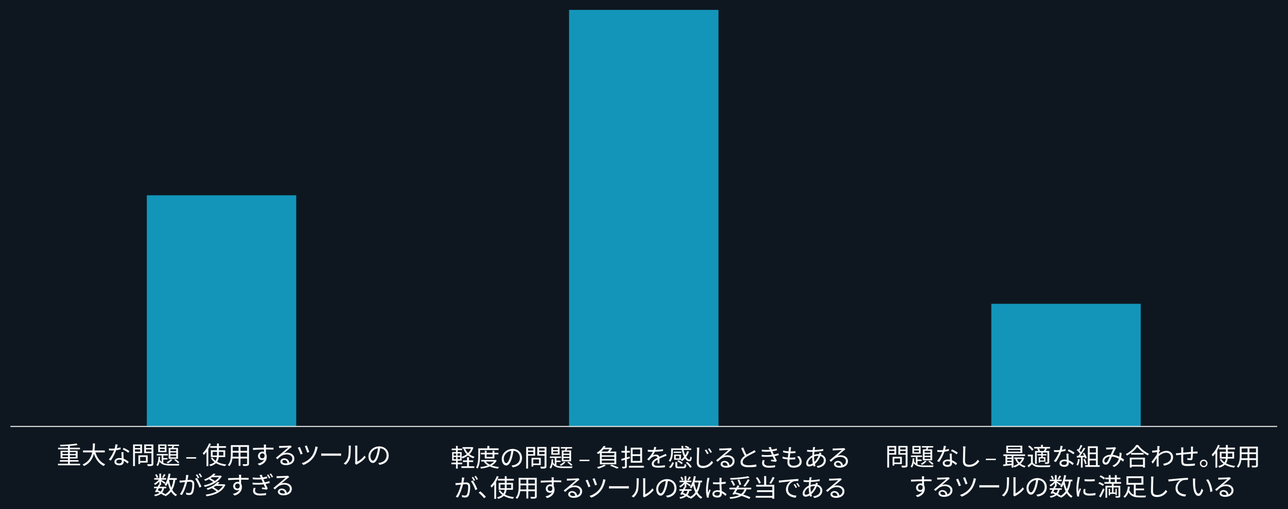
AppSec ツールの増加が統合に向けた投資の動機となっている

セキュリティ管理策の他のカテゴリー同様、多くの組織では統合と管理が難しいツールを多数導入しています。ほとんどの場合、これによってプログラムの効果が低下し、大量の人員をツールの管理に割くことになります。72% の組織は 10 個以上のツールを利用しています。この複雑さは重大な課題となっています。

使用している AppSec ツールの数



多くの組織にとってツールの増加が問題になっている



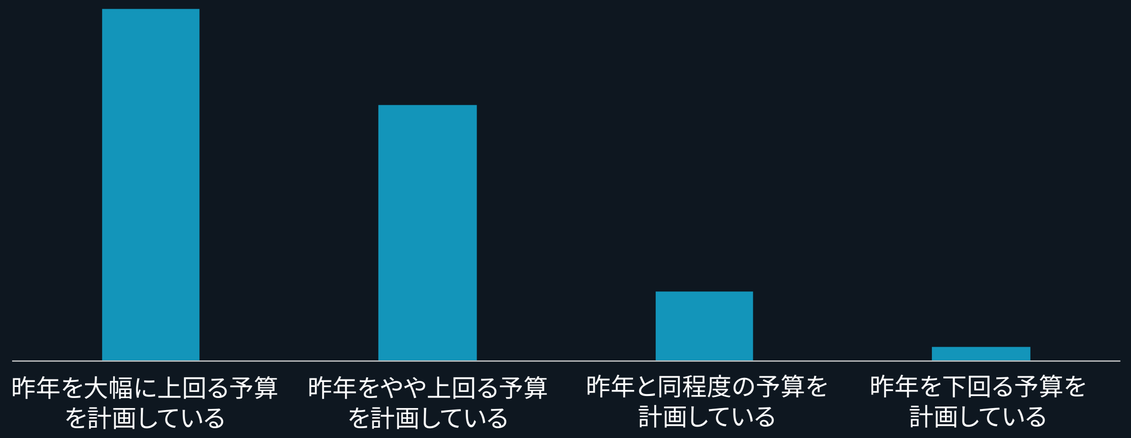
目次に戻る

半数以上の組織がアプリケーション セキュリティへの予算を大幅に 増やすことを計画している

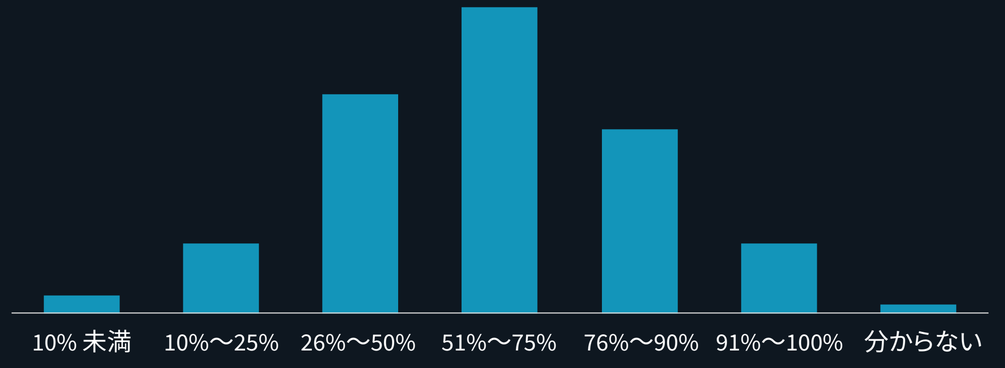
AppSec への支出は増加しているが、コードカバレッジは依然として不足

大半の組織で昨年よりもアプリケーションセキュリティへの支出を大幅に増やすことを検討している一方で、今後 12 ヵ月でコードベースの 3/4 以上を保護する予定だと回答した組織はわずか 30 %です。

今後 12 ヶ月で見込まれる AppSec ツールの予算変更



12 ヵ月以内に AppSec ツールによって保護される予定のコードベースの割合

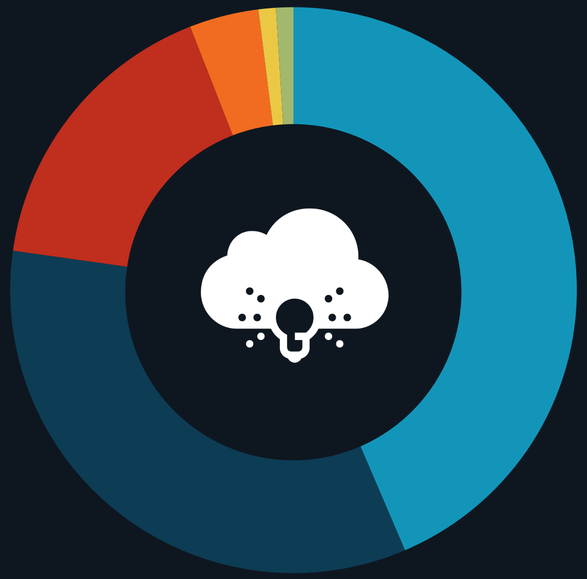


目次に戻る

AppSec ツールへの投資方法は組織によって異なるが、クラウドアプリケーション開発の保護が多数

43% の組織がクラウドのアプリケーションセキュリティへの投資を検討する一方で、1/3 の組織はプロセスを簡略化するためのツールの統合に力を入れています。また、開発チームやアプリケーションでテスト用ツールの利用率を高めるための投資を計画している組織もあります。

今後 12 ヵ月でのアプリケーションセキュリティへの投資における優先度



- クラウドアプリケーション開発プロセスのセキュリティに対する投資に大きな重点を置いている
- プロセス全体の簡素化のため、ツールの統合に対する投資に重点を置いている
- より多くの開発チームとアプリケーションにアプリケーションセキュリティを展開するための投資に重点を置いている
- アプリケーションセキュリティプログラムの効果を高めるための投資に重点を置いている
- 上記のどれでもない
- 分からない

目次に戻る

SYNOPSYS®

シノプシスのソフトウェア インテグリティ グループは、企業が安全で高品質のソフトウェアを構築し、リスクを最小限に抑えながらスピードと生産性の最大化に貢献します。シノプシスは、アプリケーション・セキュリティのリーダーであり、静的解析、ソフトウェア・コンポジション解析、動的解析ソリューションを提供しており、独自のコード、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の動作における脆弱性や欠陥を迅速に見つけて修正します。業界をリードするツール、サービス、専門知識を組み合わせることで、シノプシスはDevSecOps におけるセキュリティと品質を最大化し、ソフトウェア開発のライフサイクル全体にわたって組織を支援します。

詳しくはこちら

ESG について

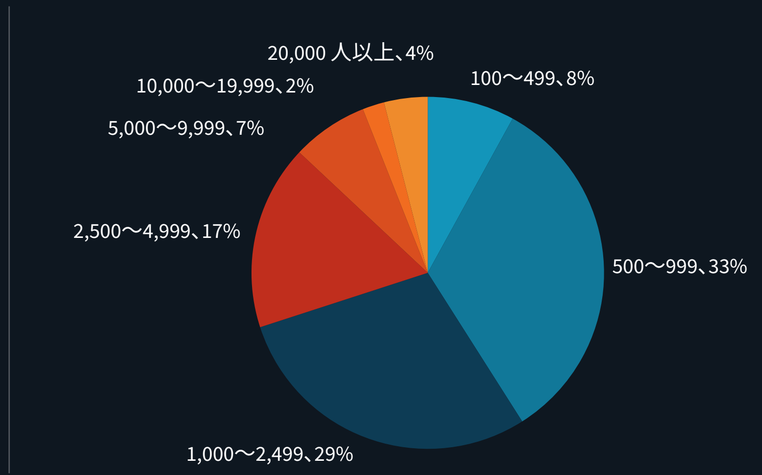
Enterprise Strategy Group は、IT アナリスト、調査、検証、戦略企業として、市場インテリジェンスと実践的な知見を世界中の IT コミュニティに提供しています。

調査手法

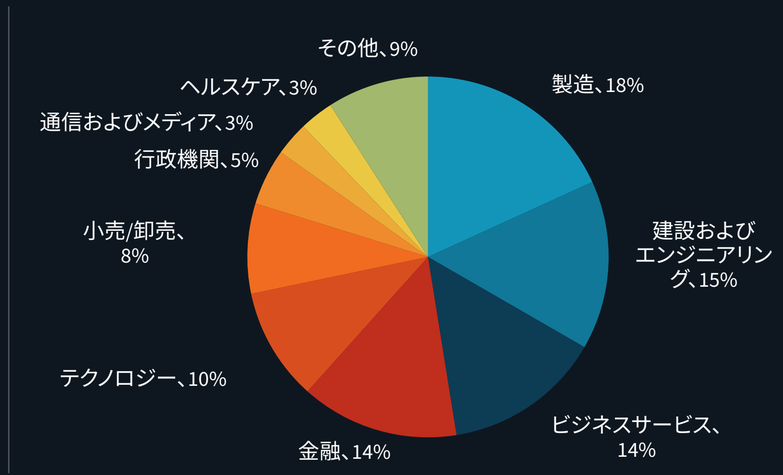
このレポートのデータを収集するために、ESG では 2020 年 6 月 12 日から 2020 年 6 月 20 日にかけて、北米（米国とカナダ）の民間部門および公共部門の組織の IT 担当者およびサイバーセキュリティ担当者に包括的なオンラインアンケートを実施しました。アプリケーション開発 関連のテクノロジーとプロセスの保護に精通しており、これらの業務を担当しているIT 担当者とサイバーセキュリティ担当者、またはアプリケーション開発用のツールとプロセスの保護に関与しているアプリケーション開発担当者をアンケート対象者としました。アンケートを完了したすべての回答者に現金、または現金に相当する報酬が提供されました。

参加資格のない回答者の除外、重複する回答の削除、および残りの入力済みの回答の（複数の基準に基づく）選別を行ってデータの整合性を取った結果、最終的に合計 378 人の IT 担当者、サイバーセキュリティ担当者、およびアプリケーション開発担当者から回答を得ました。

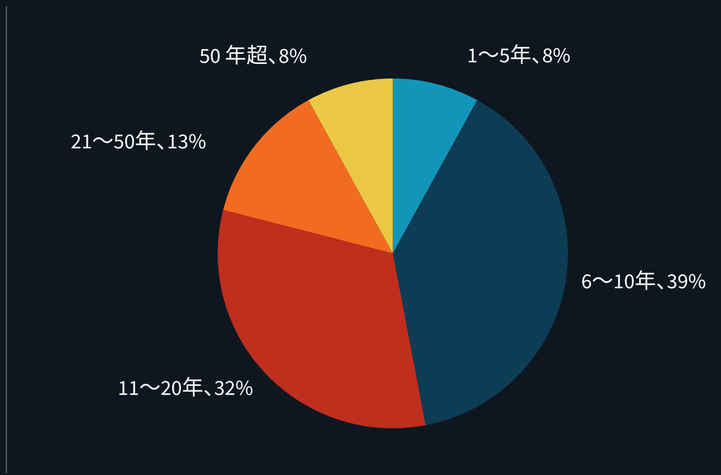
回答者が所属する企業の従業員数



回答者が所属する業界



回答者が所属する組織の設立以来の年数



目次に戻る

Enterprise Strategy Group は、IT アナリスト、調査、検証、戦略企業として、実用的な知見とインテリジェンスを世界中の IT コミュニティに提供しています。