THE LINUX FOUNDATION | Research

CLOUD NATIVE COMPUTING FOUNDATION

2024 クラウドネイティブ セキュリティ レポート

クラウドネイティブ アプリケーション開発のセキュリティに組織はどのように取り組んでいるか

Stephen Hendrick, *The Linux Foundation*
Adrienn Lawson, *The Linux Foundation*
Jeffrey Sica, *The Linux Foundation*

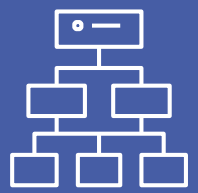
序文
Eddie Knight, *Sonatype*

2024年10月

2024 クラウドネイティブ セキュリティ レポート

84%の組織が、クラウドネイティブ アプリケーションが2年前**より安全**になったと報告。

76%の組織が、ほとんどまたはほぼすべての**アプリケーション開発がクラウドネイティブ**であると報告。



クラウドネイティブ アプリケーションのセキュリティ確保における最大の課題：**ソフトウェアとインフラストラクチャーの複雑さ**。

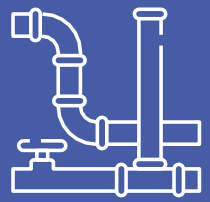
クラウドネイティブ アプリケーションのセキュリティ確保におけるベンダー最大の課題：**新たな脅威に対応しつづけること。**

40%の組織が、クラウド インフラストラクチャーとサービスの**セキュリティ インシデント**を経験。

63%の組織が、静的アプリケーション セキュリティ テスト（**SAST：Static Application Security Testing）ツール**を使用。

51%の組織が、更新のたび、セキュリティを評価するために、**手動のコード レビュー**を使用。

49%の組織が、更新のたびに**CI/CDセキュリティ テスト**を使用。

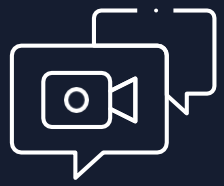


セキュリティ評価の成長分野第1位：**脆弱性のスキャンと修復。**

84%

の回答者が、**手動コード レビュー**は非常に重要であると回答。

67%の回答者が、クラウドネイティブ セキュリティ ツールと更新に関する最新情報を入手するために、**CNCFウェビナー、ワークショップ、カンファレンス**を利用。



65%の回答者が、クラウドネイティブ アプリケーションのセキュリティ強化を進めるために**CNCFのベストプラクティス**を利用。

目次

序文 4

はじめに 5

クラウドネイティブ セキュリティ調査結果 6

クラウドネイティブ アプリのセキュリティと
クラウドネイティブ技術の採用との関係 6

クラウドネイティブ開発視点から見た クラウドネイティブ
アプリケーションの セキュリティ確保における主な課題 7

組織タイプ別に見た クラウドネイティブ
アプリケーションの セキュリティ確保における主な課題 7

セキュリティ インシデントが発生する場所は
クラウド インフラストラクチャーとサービスが中心 10

セキュリティインシデントは、クラウドネイティブの道程に内在する
サイバーセキュリティリスクを浮き彫りに 11

生存者バイアスがクラウドネイティブ アプリケーションの
セキュリティ認識を歪める可能性がある理由 12

セキュリティ評価とテスト ツールはクラウド ネイティブ
コンピューティングの重要な側面 14

セキュリティツールの使用の増加はクラウドネイティブ
アプリケーションのセキュリティに良い影響を与える 16

コード レビューとCI/CDセキュリティを含むことが
セキュリティ戦略の鍵 17

脆弱性スキャン、自動セキュリティ テスト、CI/CDセキュリティは、
セキュリティ向上への近道 18

主要なクラウドネイティブ セキュリティ戦略の検証 20

ウェビナーとカンファレンスは、CNCFの セキュリティ ツールと
アップデートに関する情報を得るための主な情報源 21

ベストプラクティスとトレーニング資料は、クラウドネイティブ
アプリケーションのセキュリティを向上させるために最も望まれるコンテンツ 22

調査方法 23

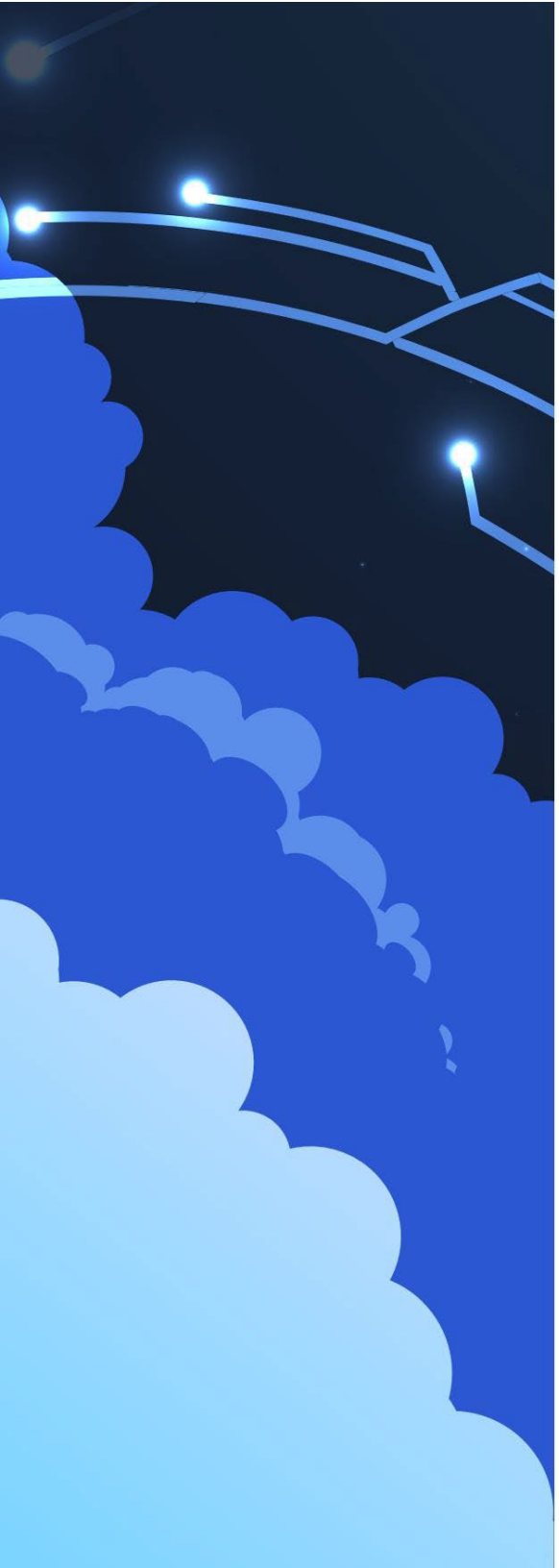
調査について 23

Data.World へのアクセス 24

回答者の人口構成 25

著者について 26

謝辞 27



序文

利用者にとっても、保守管理者にとっても、LF Researchによって生み出された成果は、オープンソース コミュニティ全体のイノベーションの柱となっています。CNCF（Cloud Native Computing Foundation）とLF Researchのコラボレーションは、ソフトウェアのセキュリティを世界的に向上させる上で、大きな進歩が遂げられていることを実証し、コミュニティがサイバーセキュリティにとって最も価値があると考える要素を明らかにしています。

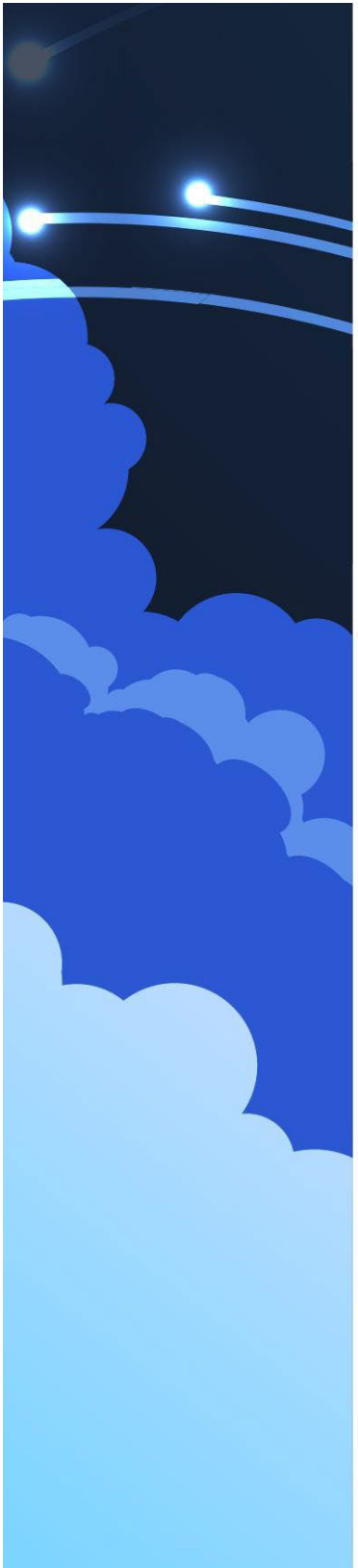
近年、サイバー攻撃の件数が大幅に増加しており、2024年には他のすべての年を合わせたよりも多くの悪意のあるオープンソース パッケージが作成されています。そしてこのレポートでは、現在、組織の76%がクラウドネイティブ開発に大きく依存していることを示しています。最も重要なインフラストラクチャーの攻撃対象領域は、多くの人が考えていたよりも大きく複雑になっていますが、このレポートには希望の光も示されています。組織の84%が、クラウドネイティブ アプリケーションは2年前よりも安全になったと報告していることです。

この希望の多くは、ソフトウェア構成分析（SCA：Software Composition Analysis）ツールなどの自動化の使用が増えていることに起因しています。これらのツールは、最新のアプリケーションを動かすオープンソース コンポーネントに関連する脆弱性を特定し、リスクを軽減するのに役立ちます。しかし、多くの組織が理解しているように、自動化ツールを導入するだけでは十分ではありません。残りの半分は、手動テスト、ポリシー、およびレビューが不可欠であることをお伝えしておきます。SCAポリシー違反の適切な人間によるレビュー、適切なテスト範囲の評価、および手動による行ごとのセキュリティ レビューがなければ、攻撃対象領域は適切に防御されません。

このレポートでは、ツールやテクノロジーだけでなく、セキュリティのもう1つの重要な側面である「情報を入手し続ける」ことに焦点を当てています。脅威の状況は常に進化しており、最新のリスクとベストプラクティスを把握し続けることは困難です。そのため、回答者の67%がCNCFのウェビナー、ワークショップ、カンファレンスに注目しているのです。Sonatypeが過去数年間、KubeConやCloudNativeConなどのイベントをサポートしてきた理由は、これらのイベントの空間が、参加者が知識を共有し、ベストプラクティスを自分の環境に適用する方法を学ぶための最も効果的なツールを提供することを知っているからです。

このレポートは、クラウドネイティブ セキュリティの現状を明確に示し、継続的な学習と適応が不可欠であり、多面的であることを思い出させてくれます。適切なツールを活用するか、コミュニティ イベントに積極的に参加するかにかかわらず、絶えず変化する環境においてシステムを安全に保つために、常に関与し、情報を得ることが鍵となります。

Eddie Knight, *CNCF TAG* Security Co-Chair, FINOS Technical Oversight Committee, Sonatype OSPO Lead



はじめに

クラウドネイティブ コンピューティングの構成要素であるコンテナー化とマイクロサービス アーキテクチャは、約15年前にITに台頭し始めました。5年後、オーケストレーション（Kubernetes）とDevOps（CI/CD）によって、業界全体でのクラウドネイティブ コンピューティングの採用を促進する重要なインフラストラクチャー要素と手順要素が追加されました。過去の世代の経験とベストプラクティスを基に、クラウドネイティブ コンピューティングでは、自動プロビジョニング、バージョン管理、オンデマンド スケーラビリティ、分散型管理機能、API駆動型インタラクション、可観測性、トラフィック管理、ポリグラフ プログラミングなどの主要な機能を有効にするツール（多くの場合、オープンソース）が追加されました。その結果、クラウドネイティブ コンピューティングは、アプリケーションの開発、展開、および運用に対する完全に現代的なアプローチとなりました。

しかし、クラウドネイティブ コンピューティングを強力で効果的かつ生産的にするには、サイバーセキュリティに対する高度なアプローチが必要です。クラウドネイティブ コンピューティングの分散アーキテクチャでは、各マイクロサービスに独自の脆弱性が存在する可能性があり、 データ侵害や不正アクセスを防ぐために、サービス間の通信を安全に保つ必要があります。クラウドネイティブ環境の動的な性質（頻繁な展開、双方向のスケーリング、インフラストラクチャーの変更）により、従来のセキュリティ対策の効果が低下する可能性があり、自動化され、スケーラブルで、新しい脅威に適応できるセキュリティ プラクティスが必要になります。コンテナー、サーバーレス機能、オーケストレーション ツールなど、クラウドネイティブ アーキテクチャの複雑さにより、各コンポーネントは継続的な監視とセキュリティを必要とする潜在的な脆弱性を持ち、攻撃可能な攻撃対象領域が増加します。

脅威の状況も絶えず進化しており、攻撃者はクラウド環境を悪用する新しい方法を開発しています。継続的な監視、脅威インテリジェンス、適応型セキュリティ対策が、潜在的な脅威に先手を打つためにはすべて必要です。

Cloud Native Computing Foundation（CNCF）は、組織がクラウドネイティブ セキュリティにどのように取り組んでいるかを理解するための実証的調査研究を開発および実施するため、2024年3月にLinux Foundation Researchと契約しました。対象読者には、次の基準を満たす回答者が含まれました。

- クラウドネイティブ アプリケーションの開発に携わっている必要があります
- 勤務先の組織がクラウドネイティブ アプリケーションのセキュリティをどのように対処しているか、に精通している必要があります
- 勤務先の組織がクラウドネイティブのテクノロジーと手法を使用している必要があります
- 雇用されている必要があります

Linux Foundation Researchによる調査は2024年3月に作成、2024年4月に実施され、200の調査を完了しました。調査方法と調査対象者に関する詳細については、このレポートの最後の「About the survey（調査について）」セクションを参照してください。

クラウドネイティブ セキュリティ調査結果

クラウドネイティブ アプリのセキュリティと クラウドネイティブ技術の採用との関係

過去2年間、ほとんどの組織がサイバーセキュリティに注力してきたことが成果を上げてきました。この調査で、2年前と比較してクラウドネイティブ アプリのセキュリティがどの程度向上したかを組織に尋ねたところ（Q21）、図1に示すように、わずか1%（3人の回答者）がセキュリティが低下したと回答、14%がほぼ同じと回答、85%がセキュリティが向上したと回答しました。

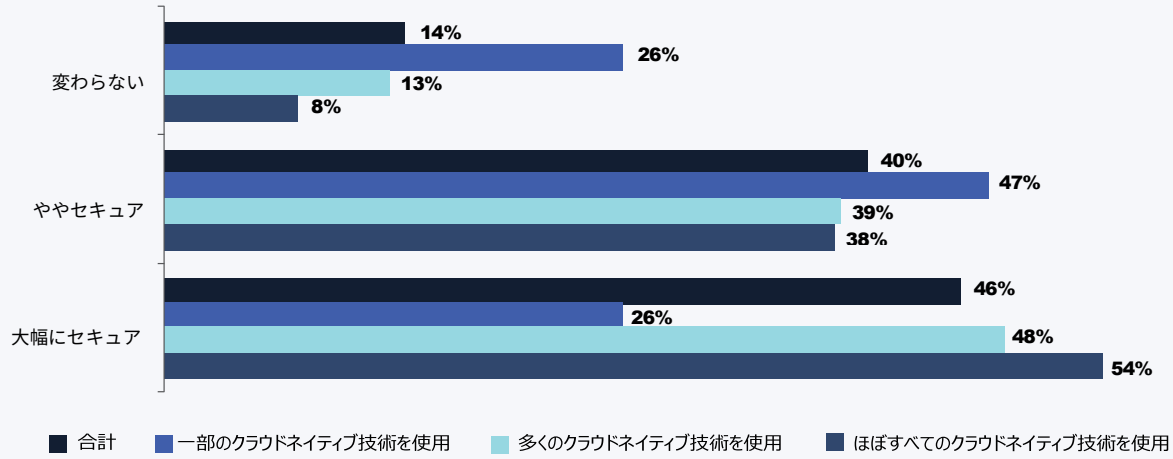
セキュリティが向上したと答えた85%は、「ややセキュア」になったと答えた40%と、「大幅にセキュア」になったと答えた45%で構成されています。これは、組織が意識的にサイバーセキュリティに投資してきたことを示しています。

クラウドネイティブ技術の採用状況（Q7、図には示されていません）を見ると、クラウドネイティブ技術を使用し始めているのはわずか5%で、19%が一部の開発がクラウドネイティブ、44%が多くの開発がクラウドネイティブ、33%がほぼすべての開発がクラウドネイティブと回答しています。

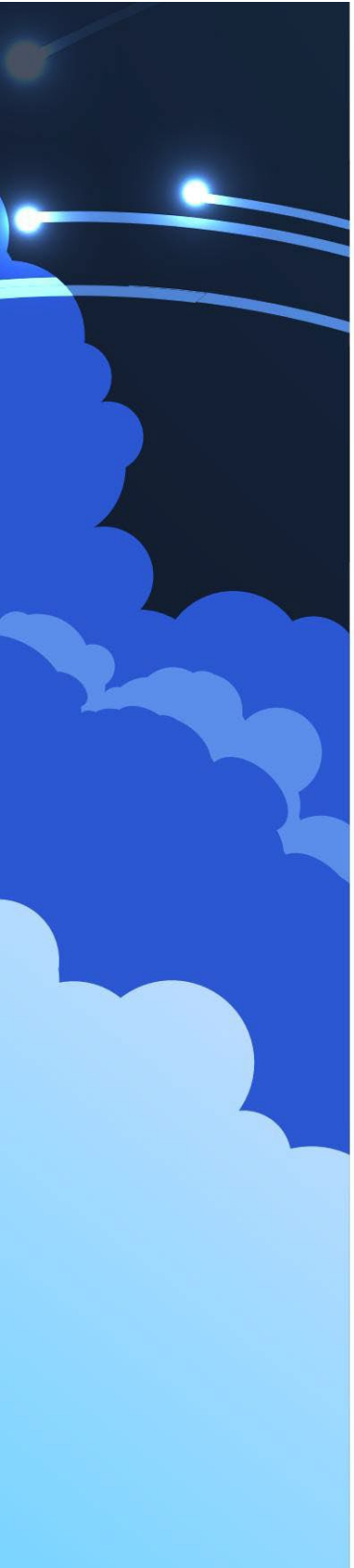
図 1

クラウドネイティブ採用の進化により クラウドネイティブ アプリケーションのセキュリティに対する認識が向上

2 年前と比べて、クラウドネイティブ アプリはどの程度安全ですか？（1つ選択してください）
（「組織はクラウドネイティブ技術をどの程度導入していますか？（1つ選択してください）」の回答別データ）



2024 Cloud Native Security Survey, Q21a x Q7a, サンプル数 = 188



しかし、アプリケーション セキュリティのこれらの改善と、組織がクラウドネイティブ技術を採用している程度を比較すると、より微妙な状況が浮かび上がってきます。アプリケーション セキュリティに大きな変化はないと回答した14%の組織のうち、アプリケーション開発に一部のクラウドネイティブ技術を使用していると回答した組織は26%、アプリケーション開発に多くのクラウドネイティブ技術を使用していると回答した組織は13%、アプリケーション開発にほぼすべてのクラウドネイティブ技術を使用していると回答した組織はわずか8%でした。一方、アプリケーションのセキュリティが大幅に向上したと回答した45%の組織のうち、アプリケーション開発の一部にクラウドネイティブ技術を使用していると回答した組織は26%、アプリケーション開発の多くにクラウドネイティブ技術を使用していると回答した組織は47%、アプリケーション開発のほぼすべてにクラウドネイティブ技術を使用していると回答した組織は54%でした。このことはから、クラウドネイティブ技術の採用が増えるとセキュリティが向上する、もしくは、セキュリティの強化によってクラウドネイティブ技術を採用する組織が増えると推察することができます。組織がクラウドネイティブ技術を採用している程度が、セキュリティの向上に対する認識に影響を与える可能性があります。クラウドネイティブ テクノロジーに深く投資している企業は、セキュリティ プラクティスがより優れ、統合されているため、より安全だと感じています。いずれにしても、これは勝利です。

クラウドネイティブ開発視点から見たクラウドネイティブ アプリケーションのセキュリティ確保における主な課題

クラウドネイティブ アプリケーションのセキュリティ保護に関して組織が直面する主な課題は、クラウドネイティブの取り組みがどの段階にいるかによって異なります。図2は、いくつかの重要な発見から、上位8つの主要課題を示しています。

複雑さは変わらないまま：導入レベルを問わず、複雑さは依然として最大の課題であり、クラウドネイティブ技術が運用に不可欠なものになるにつれて、システムの複雑さと高度な管理の必要性が増すことを示しています。

新たな脅威と高度な導入：クラウドネイティブの導入レベルが高まると、新たな脅威に関連するセキュリティ上の課題への重点が高まり、セキュリティ能力に、絶え間ない警戒と継続的な改善が必要とされます。

規制の遵守：組織がクラウド テクノロジーへの依存を深めるにつれて、規制の遵守がより困難になり、堅牢なガバナンス フレームワークの必要性が強調されます。

クラウドネイティブに取り組み始める際の課題：図2は、一般的に、クラウドネイティブへの取り組みの初期段階にある組織と、開発の大部分またはほぼすべてがクラウドネイティブである組織とに二分されています。開発に一部のクラウドネイティブ技術を使用している組織では、資金（37%）とセキュリティ意識の欠如（32%）が主な課題ですが、他のより成熟したクラウドネイティブ組織ではそれほど大きな課題ではありません。一方、開発に一部のクラウドネイティブ技術を使用している組織では、脅威への対応（29%）、安全な展開（24%）、規制遵守（21%）の懸念ははるかに小さく、他のより成熟したクラウドネイティブ組織では、はるかに大きな懸念になっています。

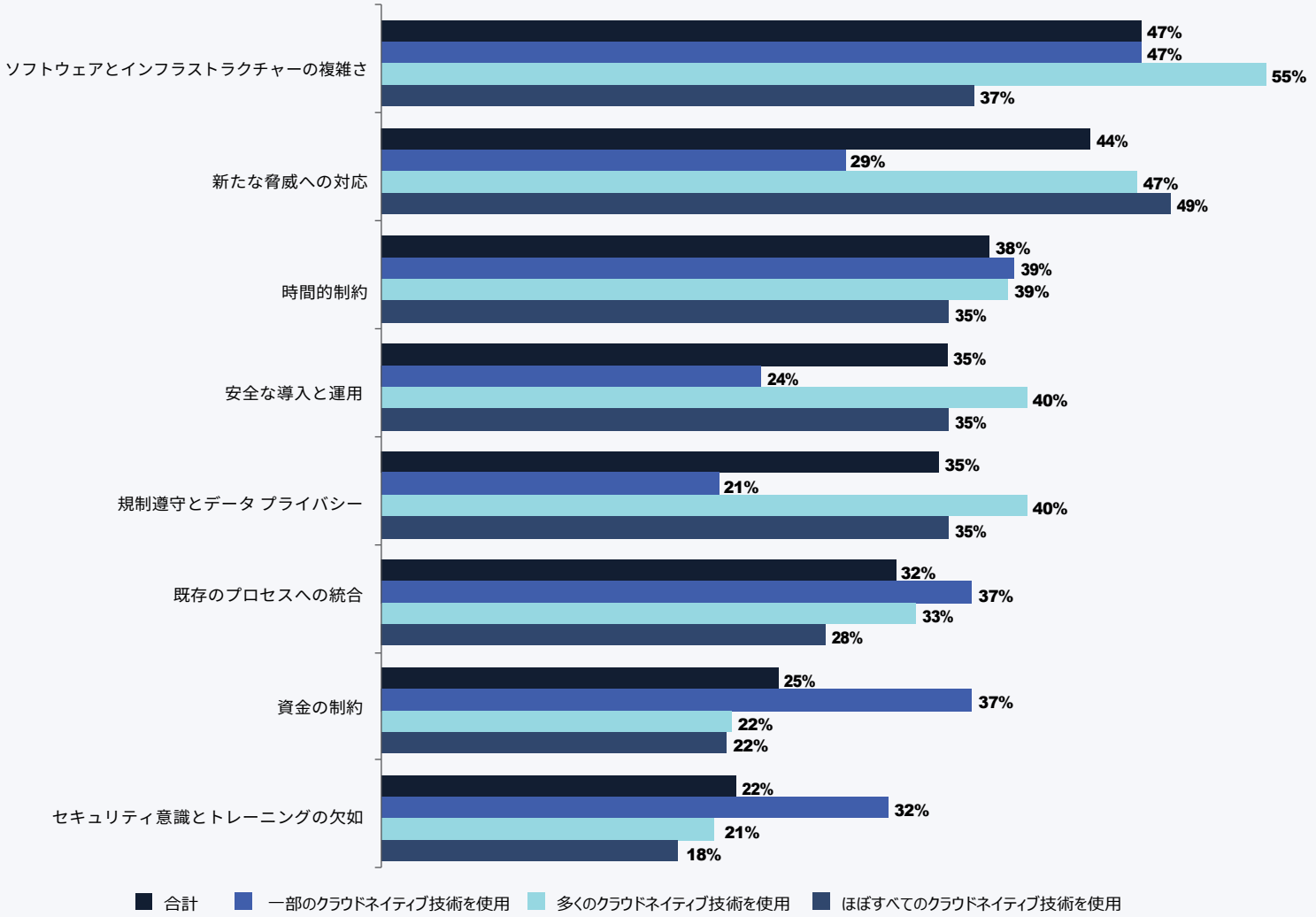
組織タイプ別に見たクラウドネイティブ アプリケーションのセキュリティ確保における主な課題

クラウドネイティブ アプリケーションのセキュリティ保護には常に課題が伴いますが、これらの課題は、組織がベンダー/サービス プロバイダーであるか、エンドユーザー組織（業界に特化した製品を持ち、IT製品やサービスの「エンドユーザー」である組織）であるかによって大きく異なります。図3は、クラウドネイティブ アプリケーションのセキュリティ保護に関する主な課題を、組織のタイプ別に示したものです。

図 2

クラウドネイティブ開発視点から見た クラウドネイティブ アプリケーションのセキュリティ確保における主な課題

クラウドネイティブ アプリケーションのセキュリティ保護で直面している最大の課題は何ですか？（該当するものをすべて選択してください）
（「組織はクラウドネイティブ技術をどの程度導入していますか？（1つ選択してください）」の回答別データ）

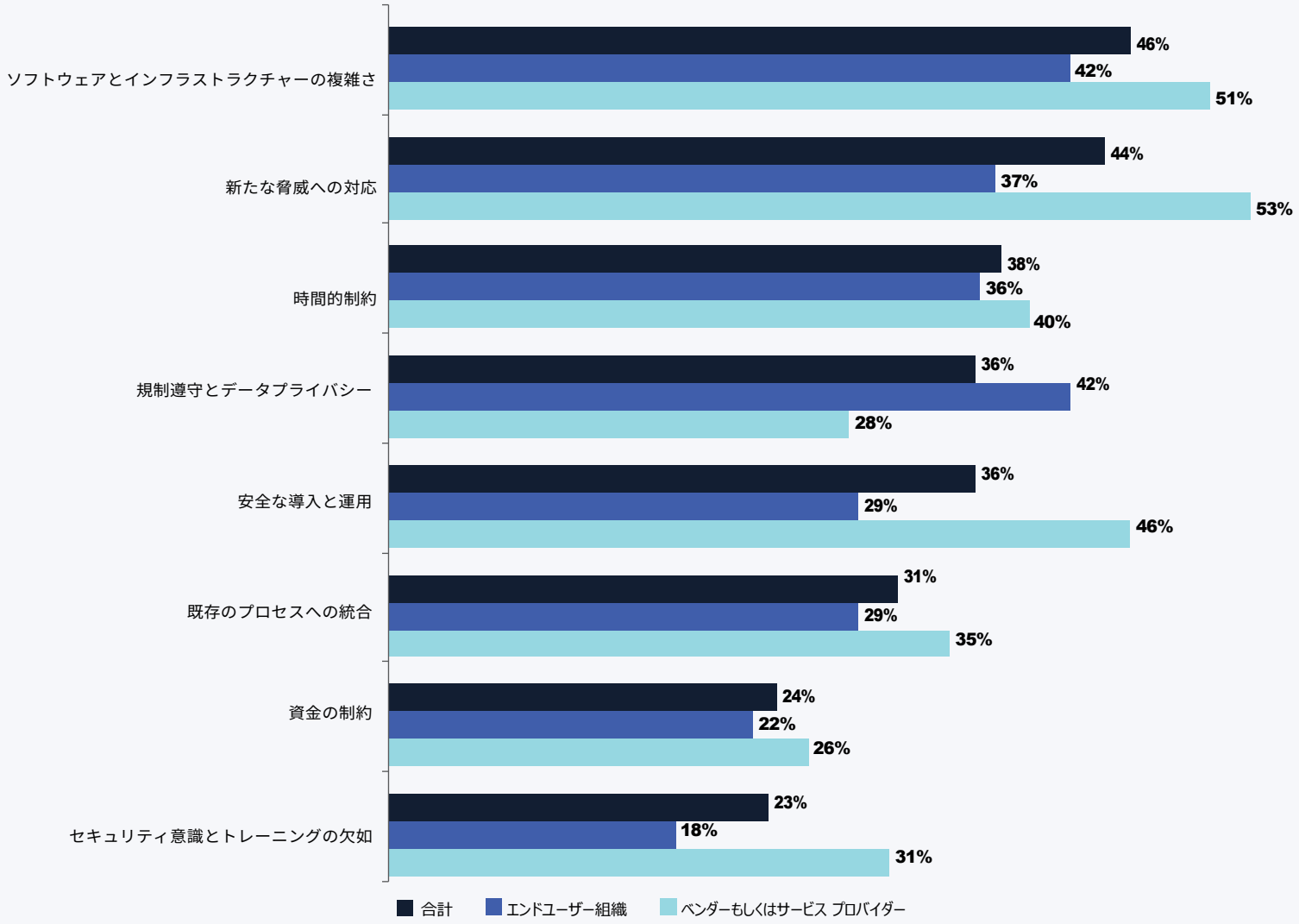


2024 Cloud Native Security Survey, Q20 x Q7a, サンプル数 = 190, 有効数 = 190, 総言及数 = 601

図3

組織タイプ別に見た クラウドネイティブ アプリケーションのセキュリティ確保における主な課題

クラウドネイティブ アプリケーションのセキュリティ保護で直面している最大の課題は何ですか？（該当するものをすべて選択してください）
（「どのような種類の組織または団体で働いていますか？（1つを選択してください）」の回答別データ）



2024 Cloud Native Security Survey, Q20 x Q13a, サンプル数 = 188, 有効数 = 188, 総言及数 = 597

図3は、新たな脅威への対応（53%）、ソフトウェアとインフラストラクチャーの複雑さ（51%）、安全な導入（46%）が、ベンダーとサービス プロバイダーにとっての3大懸念事項であることを示しています。エンドユーザーは、ソフトウェアとインフラストラクチャーの複雑さ（42%）、新たな脅威への対応（37%）、時間的制約（36%）を主な課題と見なしています。ベンダーとサービス プロバイダーは、規制遵守を除くこれらすべての課題について、エンドユーザーよりもはるかに大きな懸念を抱いています。その理由は、ソフトウェア ベンダーとサービス プロバイダーは、複数のクライアント、環境、インフラストラクチャーにわたってセキュリティを管理する必要があるため、クラウドネイティブ アプリケーションのセキュリティ保護において、より深刻な課題に直面していることが考えられます。同時に、多様な規制への準拠を維持し、高度な攻撃を防御し、厳格なSLAを維持する必要があるためです。運用に伴う複雑さ、規模、およびリスクの高さにより、クラウドネイティブ環境のセキュリティ保護は、これらの組織にとって特に困難になっています。

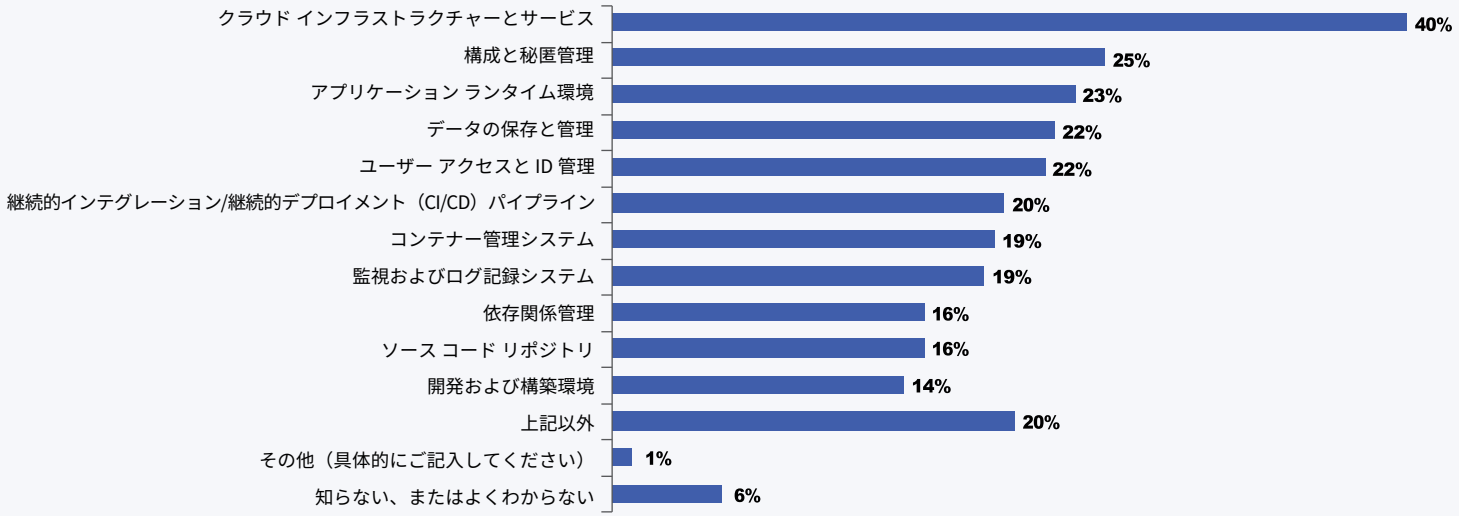
セキュリティ インシデントが発生する場所はクラウド インフラストラクチャーとサービスが中心

図4は、クラウド インフラストラクチャーとサービスで発生したセキュリティ インシデントが他と大きく解離していることを示しています。その主な理由は、クラウド環境が非常に動的かつ短命であることです。継続的な変化により、一貫したセキュリティ ポリシーを維持することが困難になり、攻撃者が悪用できる潜在的な

図4

組織がセキュリティ インシデントを経験している場所

過去2年間に、クラウドネイティブ ソフトウェア開発のどの分野でセキュリティ インシデントを経験しましたか？（該当するものをすべて選択してください）



2024 Cloud Native Security Survey. Q22. サンプル数 = 200. 有効数 = 200. 総言及数 = 519

ギャップが生じる可能性があります。クラウド インフラストラクチャーには、仮想化、ネットワーク、ストレージ、アプリケーション レイヤーなど複数のレイヤーが含まれ、それぞれのレイヤーに潜在的な脆弱性が存在します。これらのレイヤーの管理とセキュリティ保護の複雑さが、構成ミスやセキュリティの見落としの可能性を高めます。

図4のデータは、クラウドネイティブ環境（開発、および/または展開）内のセキュリティの多様な性質を強調しており、インフラストラクチャー、構成管理、およびアプリケーション ランタイムを主な懸念事項として強調しています。組織は、リスクを効果的に軽減するために、これらの領域を網羅する包括的なセキュリティ戦略を採用する必要があります。データは、クラウドネイティブ システムのさまざまなコンポーネントにまたがって脆弱性が広がることを示唆しており、クラウド セキュリティに対する統合されたプロアクティブなアプローチによる補強の必要性を裏付けています。

セキュリティ インシデントは、クラウドネイティブの道程に内在するサイバーセキュリティ リスクを浮き彫りに

過去2年間にセキュリティ インシデントが報告されたクラウドネイティブ ソフトウェア開発の領域を、クラウドネイティブ技術の採用状況別に分類すると、いくつかの気になるパターンが見られます。図5は、各セグメントの組織がセキュリティ インシデントを経験した主な領域を示しています。

クラウドネイティブ アプリケーションの開発を始めたばかりの組織でセキュリティ インシデントのレベルが大幅に低く見受けられるのは、主に、環境が小規模で複雑ではなく、より慎重で集中的にセキュリティにアプローチでき、そして、クラウドネイティブ プラクティスを徐々に採用しながらセキュリティの専門知識を身に付ける機会があるためです。

図5

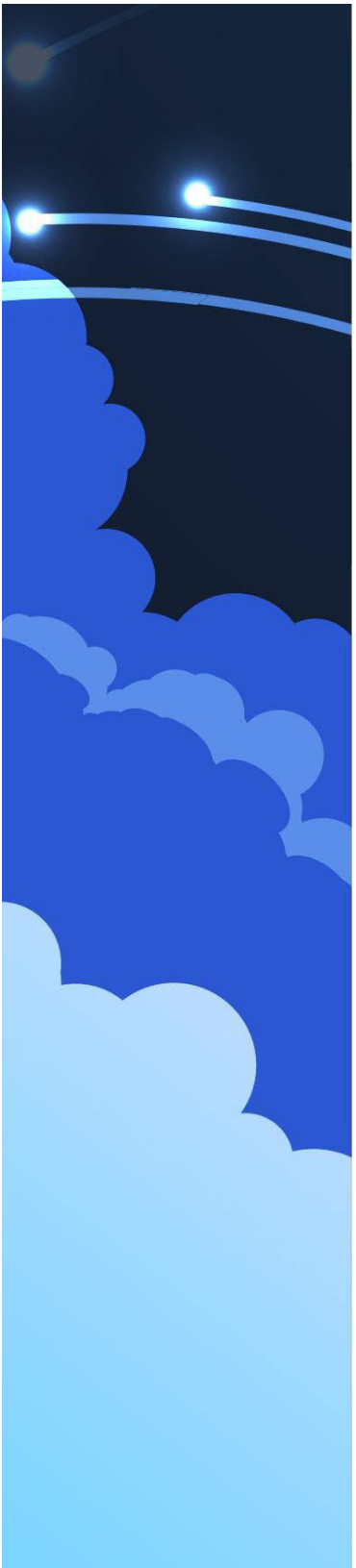
クラウドネイティブ利用レベル別に見たセキュリティ インシデントの発生場所

過去 2 年間に、クラウドネイティブ ソフトウェア開発のどの分野でセキュリティ インシデントを経験しましたか？（該当するものをすべて選択してください）

（「組織はクラウドネイティブ技術をどの程度採用していますか（1つ選択してください）」の回答別データ）

インシデントが発生した主要領域	一部のクラウドネイティブ技術を使用	多くのクラウドネイティブの技術を使用	ほぼすべてのクラウドネイティブ技術を使用
1	アプリケーション ランタイム環境（18%）	クラウド インフラストラクチャーとサービス（49%）	クラウド インフラストラクチャーとサービス（42%）
2	クラウド インフラストラクチャーとサービス（18%）	データの保存と管理（29%）	構成と秘匿管理（29%）
3	依存関係管理（18%）	監視およびログ記録システム（28%）	ユーザー アクセスとID管理（28%）
「上記のいずれでもない」を選択した回答者の割合	37%	13%	22%

2024 Cloud Native Security Survey, Q22 x Q7, サンプル数 = 190, 有効数 = 190, 総言及数 = 500



組織が成熟し、クラウド ベースの展開を拡大するにつれて、複雑さの増加、攻撃対象領域の広がり、他のシステムとの統合の進化が、セキュリティ管理をより困難にし、インシデントの発生可能性を高めます。

クラウドネイティブの開発を大規模に展開している組織では、主にクラウドネイティブ環境の複雑さ、規模、動的性質が増すため、セキュリティ インシデントを多く経験しています。頻繁な変更、サードパーティ コンポーネントへの依存、監視とインシデント対応、成熟したセキュリティ文化の必要性など、これらの課題すべてが、組織でセキュリティ インシデントが発生する可能性を高めています。クラウドネイティブの実践を拡大するにつれて、複雑さと潜在的な攻撃対象領域が拡大し、セキュリティ管理をより困難にします。

データによると、組織がクラウドネイティブ テクノロジーの使用を増やすにつれて、経験するセキュリティ インシデントの種類が進化し、特定の領域では増加する傾向にあります。これは、環境の複雑化と検出能力の向上の両方を反映しています。課題が、導入レベルが低い基本的なインフラストラクチャーから、導入段階が高い構成や秘匿管理などのより高度な領域に移行していることは、クラウドネイティブ導入の成熟度レベルに合わせた高度なセキュリティ戦略の必要性を裏付けています。

生存者バイアスがクラウドネイティブ アプリケーションのセキュリティ認識を歪める可能性がある理由

図6は生存者バイアスを視覚的に表したものです。この図は帰還中の第二次世界大戦時代の飛行機が撃たれた場所を示しています。分析した飛行機には墜落して帰還できないほどの深刻な損傷を受けた飛行機は含まれていなかったことから、青いドットの部分を補強すべきだという提案は選択バイアスの例となります。サンプルには帰還できる程度の軽度の損傷を受けた飛行機のみが含まれていました。したがって、適切な処置は、見えている損傷の少ない部分を補強することです。

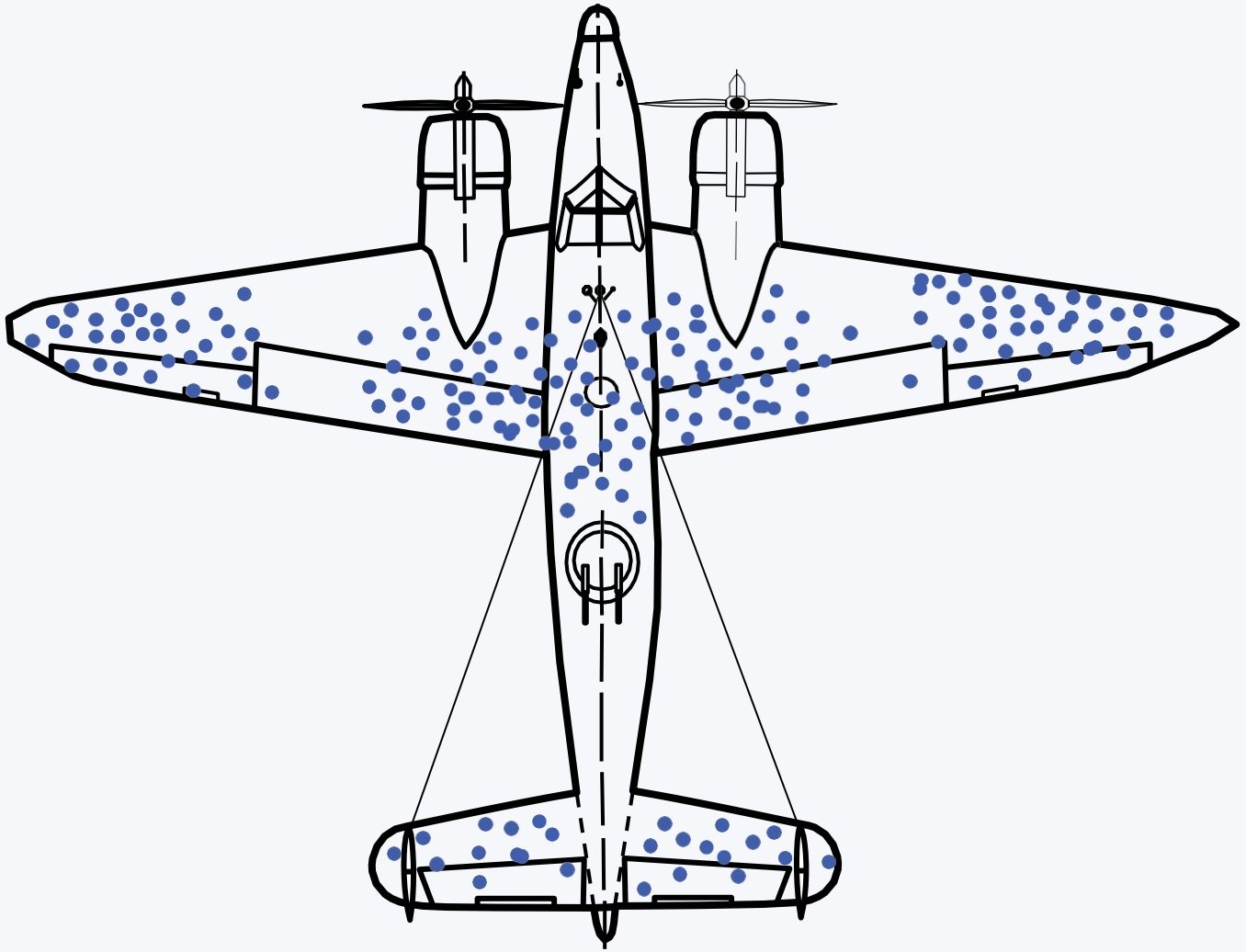
生存者バイアスまたは生存バイアスとは、選択プロセスを通過したエンティティに集中し、通過しなかったエンティティを無視するという論理的誤りです。これは、不完全なデータのために誤った結論につながる可能性があります。

クラウドネイティブ テクノロジーに関連するセキュリティ インシデントに関するデータを解釈する際には、生存者バイアスを考慮することが重要です。成熟したクラウドネイティブ組織でインシデント報告数が多いことは、本質的にセキュリティが低いことを意味するのではなく、セキュリティ問題に対する認識が高く、検出能力が向上していることを示している可能性があります。これを、採用率の高さが直接リスクの高さに相関していると認識をゆがめて見ることもできますが、一方、セキュリティ プラクティスと検出能力がより堅牢であることを示している可能性もあります。

図5は、クラウドネイティブの取り組みの初期段階にある組織（一部のクラウドネイティブ技術を使用）と、取り組みがかなり進んでいる組織（ほぼすべてのクラウドネイティブ技術を使用）とで、経験が大きく異なることを示しています。サイバーセキュリティにおける生存者バイアスの可能性は、クラウドネイティブの取り組みの初期段階にある組織にとって懸念事項です。これらの組織ではクラウドネイティブ運用の規模が小規模であるため、一般的にセキュリティに対するアプローチが単純化され、識別可能なインシデントが少なくなり、図5に示されている領域でインシデントを経験していない組織の割合が増加します。これらの組織は、クラウドネイティブ活動を拡大するにつれて、より包括的なセキュリティ対策を実装することの重要性を過小評価する可能性があります。次のセクションの図7で説明されている厄介な結果は、クラウドネイティブの取り組みの初期段階にある組織が、自社の経験から学ぶだけでなく、成熟したクラウドネイティブ ステータスを達成した組織の経験からも学ぶ必要があることを示すもう1つの指標です。

図6

数字の向こう側：生存者バイアスがクラウドネイティブ アプリケーションのセキュリティ認識を歪める可能性



Martin Grandjean（ベクター）, McGeddon（画像）, 米国空軍（ヒット プロット）,
CC BY-SA 4.0 <https://creativecommons.org/licenses/by-sa/4.0>, 経由 Wikimedia Commons

セキュリティ評価とテスト ツールはクラウド ネイティブ コンピューティングの重要な側面

クラウドネイティブ開発の粒度と複雑さにより、より大規模な特注のテスト ツール ポートフォリオが必要になります。図7の肯定的な結果は、テスト ツールの使用の濃度と度合いが、過去の調査よりも大幅に増加していることです。使用されているセキュリティ評価手法の平均数は、2022年と2023年の過去の調査では2〜3でしたが、現在は4.5になっています。

静的アプリケーション セキュリティ テスト（SAST：Static Application Security Testing）およびソフトウェア コンポジション分析（SCA：Software Composition Analysis）ツールはセキュリティ テストの基礎であり、アプリケーション開発の大部分またはほぼすべてがクラウドネイティブである組織では、これらのツールの浸透率は60%を超えています。しかしながら、アプリケーション開発の一部のみがクラウドネイティブである組織では、これらのツールの普及率ははるかに低くなります。

もう1つの興味深い進展は、セキュリティ テストのゴールド スタンダードである手動コード検査を使用している組織が49%〜57%に上ることです。手動コード検査は、コンテキストの理解、微妙で複雑な問題の検出、コード品質とセキュリティ文化全体の改善に役立つという点で価値がありますが、リソースを大量に消費し、大規模なプロジェクトでは拡張性が低い可能性があります。SAST、SCA、WAS/DASTなどの自動化ツールは、既知の脆弱性を迅速に特定し、確立されたセキュリティ プラクティスへの準拠を確認する点で優れていますが、経験豊富な人間のレビュー担当者がもたらす微妙な分析と判断に取って代わることはできません。実際、最適なアプローチは、自動化ツールの速度とカバレッジ、それに手動コード検査の深さと洞察力の両方を組み合わせることです。このハイブリッド アプローチにより、組織は両方の方法の制約を管理しながらセキュリティを最大限に高めることができます。

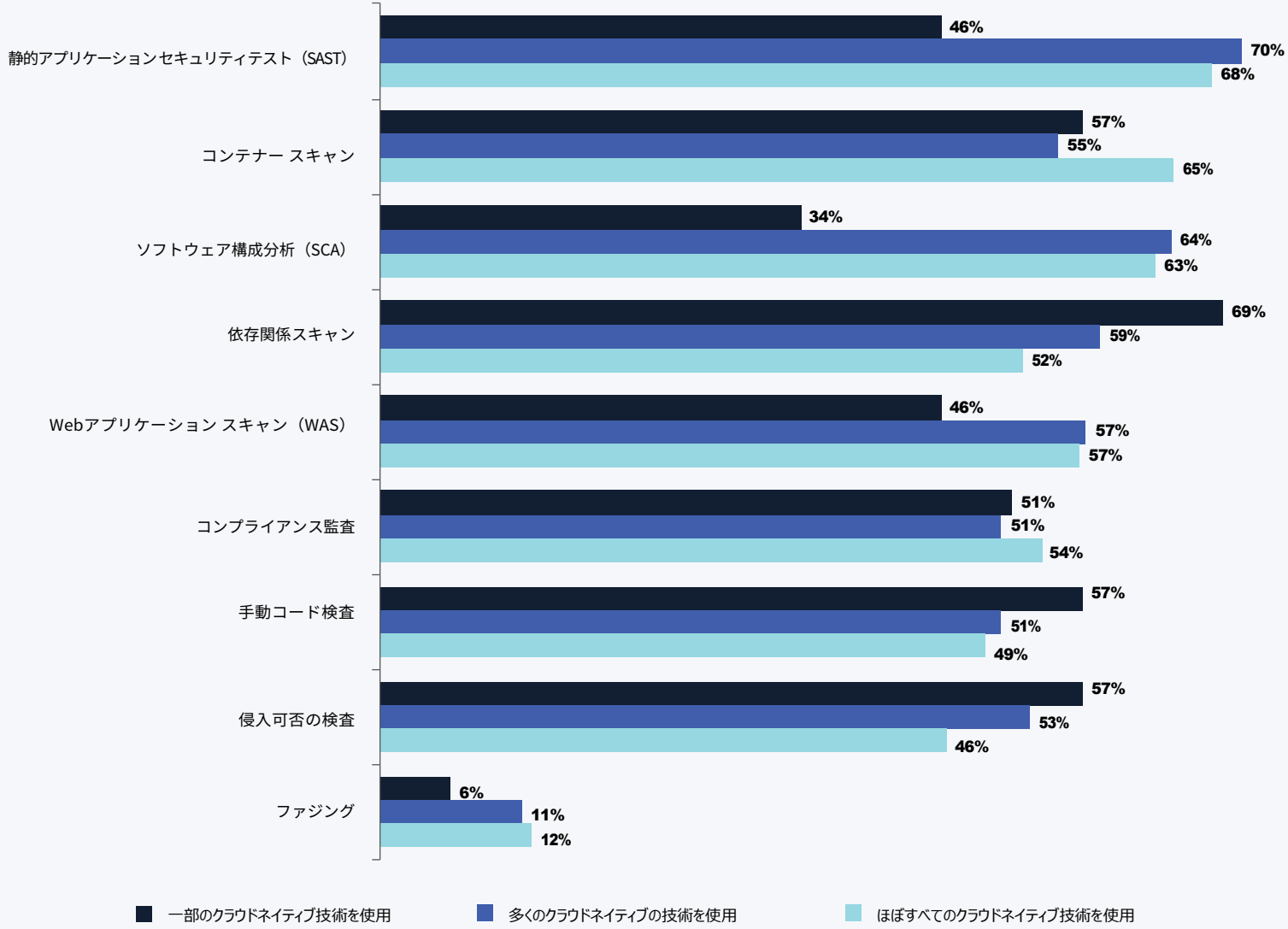
*静的アプリケーション セキュリティ テスト（**SAST**）とソフトウェア構成分析（**SCA**）ツールはセキュリティ テストの基礎であり、アプリケーション開発の大部分またはほぼすべてがクラウドネイティブである組織では、その浸透率は**60**％を超えています*

これにより、図7の厄介な結果が導き出されます。すなわち、一部のクラウドネイティブ技術を使用している組織は、SAST、SCA、WAS/DASTの導入が遅れているということです。アプリケーション開発の多くまたはほぼすべてがクラウドネイティブ技術である組織では、これら3つのツール カテゴリの使用率が最も高いことを考えると、この普及率の二分性は驚くべきものです。

図 7

クラウドネイティブ開発のレベル別に使用されるセキュリティ評価

どのような種類のセキュリティ評価を実施していますか？（該当するものをすべて選択してください）
（「組織はクラウドネイティブ技術をどの程度導入していますか？（1つ選択してください）」の回答別データ）



2024 Cloud Native Security Survey, Q19 x Q7, サンプル数 = 190, 有効数 = 190, 総言及数 = 865, DKNS回答は除く（DKNS：知らない、またはよくわからない）

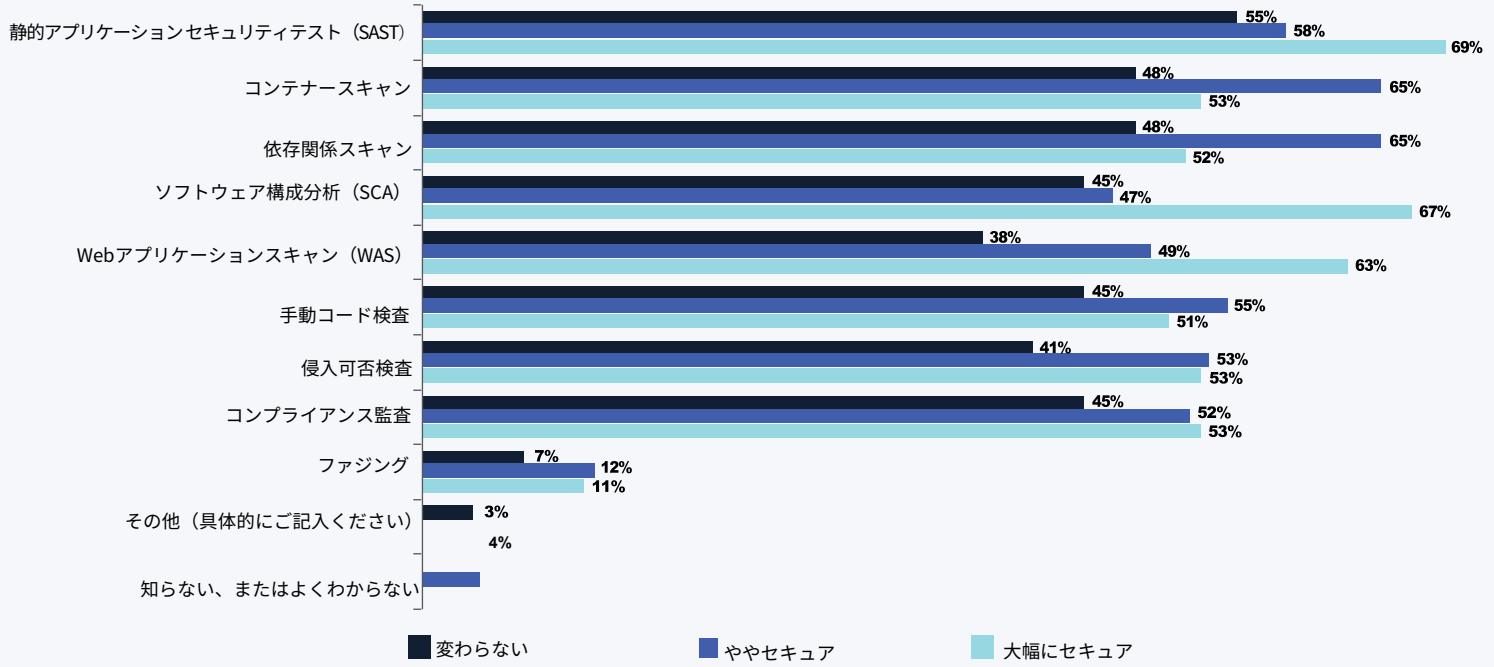
セキュリティ ツールの使用の増加はクラウドネイティブ アプリケーションのセキュリティに良い影響を与える

図7に示されているように、セキュリティ ツールの使用が増え、意図した結果が生まれています。図1で述べたように、回答者の84%が、クラウドネイティブ アプリケーションは2年前よりも安全だと考えています。図8は、セキュリティ ツールの使用と評価を、セキュリティがどのように改善されたかという認識で区分したものです。「ほぼ同じ」という回答を基準にすると、SAST、SCA、WAS（DAST）ツールを使用するとセキュリティが大幅に向上します。コンテナー スキャンと依存関係スキャンでも実質的な向上が見られます。

図8

クラウドネイティブ アプリケーションのセキュリティがどのように変化してきたかによって分類された利用中のセキュリティ評価

どのような種類のセキュリティ評価を実行していますか？（該当するものをすべて選択してください）
（「2年前と比較して、クラウドネイティブ アプリはどの程度安全ですか？（1つ選択してください）」の回答別データ）



2024 Cloud Native Security Survey, Q19 by Q21a, サンプル数 = 197,有効数 = 197, 総言及数 = 891

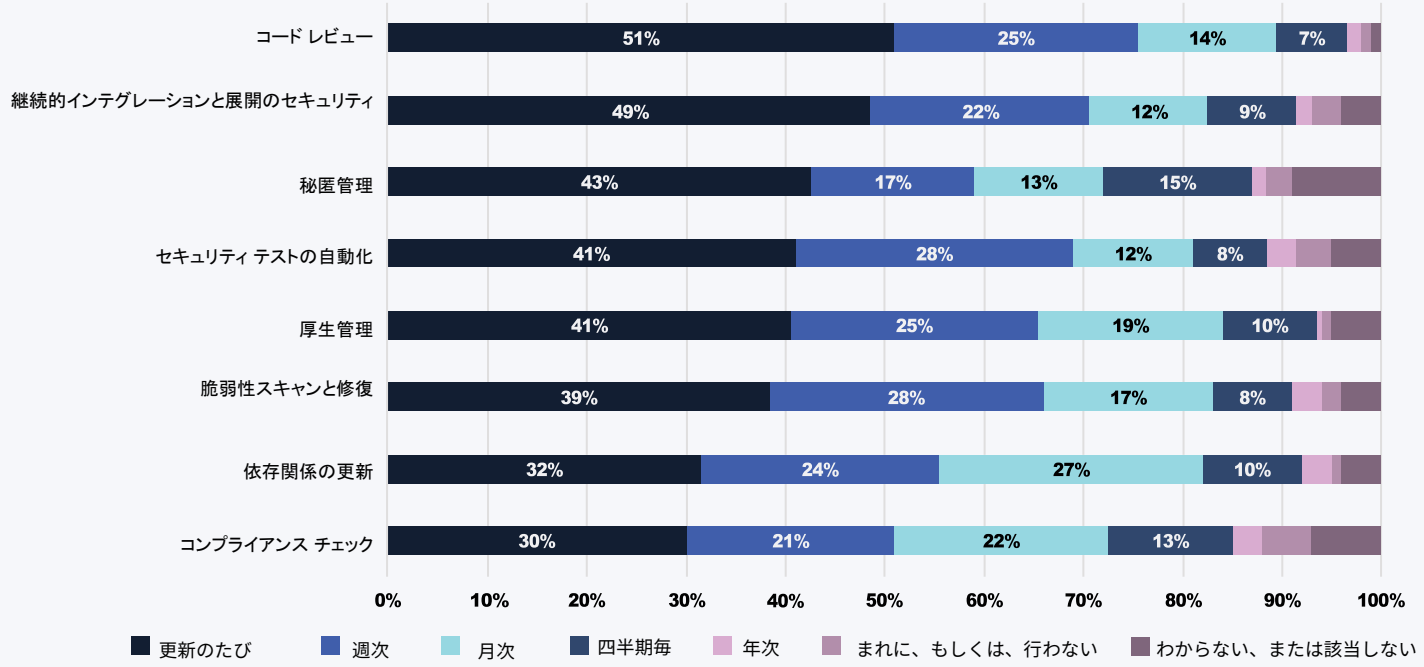
コード レビューとCI/CDセキュリティを含むことがセキュリティ戦略の鍵

図9は、手動コード レビューがクラウドネイティブ セキュリティを向上させる効果的なツールであり、自動化ツールでは見逃される可能性のあるビジネス ロジック、アーキテクチャ パターン、複雑なセキュリティ問題に関する深い洞察を提供します。手動レビューをSASTやSCAなどの自動化されたセキュリティ テスト ツールと組み合わせ、技術的な脆弱性とコンテキスト固有の脅威の両方に対処することにより、クラウドネイティブ アプリケーションのセキュリティ態勢を大幅に強化できます。

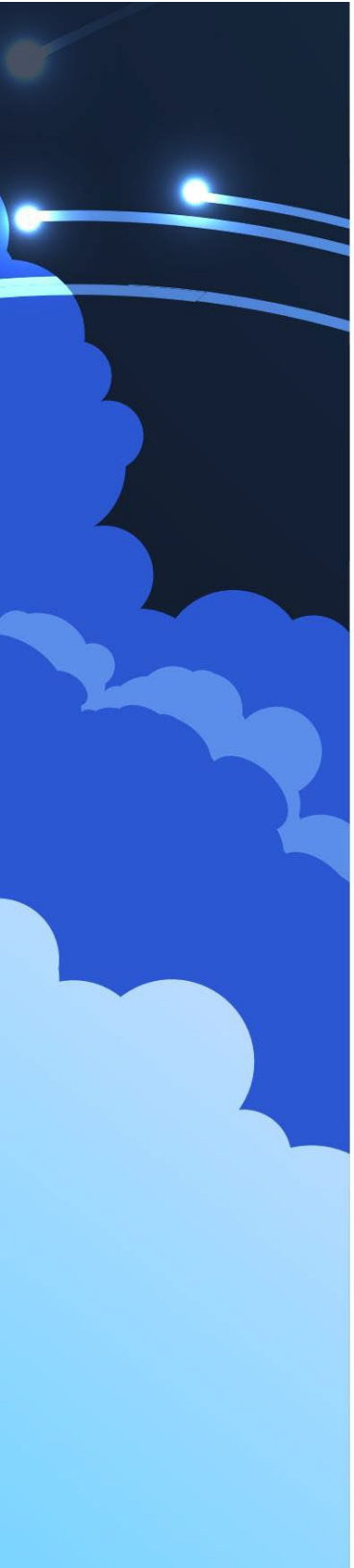
図9

クラウドネイティブ アプリケーション開発における一般的なセキュリティ戦略の使用特性

あなたの組織は、クラウドネイティブ エコシステム内で以下のセキュリティ戦略をどのくらいの頻度で実践していますか？（1行につき1つ回答してください）



2024 Cloud Native Security Survey, Q17, サンプル数 = 200



ただし、手動レビューの有効性は、レビュー担当者の専門知識、レビュー プロセスの徹底性、および検査結果をより広範な開発とセキュリティ ワークフローに統合する能力に依存します。実際に、包括的なセキュリティ戦略を作成するために、手動コード レビューと自動化ツールを組み合わせて使用することで、最良の結果が得られます。

CI/CDセキュリティは、CI/CDパイプラインの自動化と効率化の利点がセキュリティを犠牲にしないようにするために不可欠です。コード開発、依存関係管理、展開、監視に至るまで、パイプライン全体にセキュリティ プラクティスを組み込むことで、組織は強力なセキュリティ体制を維持しながら、ソフトウェアを迅速かつ確実に提供できます。

図9に示されている改善の余地がある戦略の1つは、自動化されたセキュリティ テストです。多くのセキュリティ ツールに自動化されたテスト機能があり、更新のたびにこれらのツールを使用している組織は41%に過ぎないという現実を考えると、改善の余地があることは明らかです。

脆弱性スキャン、自動セキュリティ テスト、CI/CDセキュリティは、セキュリティ向上への近道

クラウドネイティブ エコシステムで使用されているセキュリティ戦略（図9）と、過去2年間にクラウドネイティブ セキュリティがどの程度改善されたかに関する組織の認識を組み合わせて考えることにより、最高のパフォーマンスを発揮する戦略についての洞察が得られます。図10では、再び「ほぼ同じ」をベースラインとして使用すると、ベースラインから最も著しい改善は、脆弱性スキャンと修復ツール、自動化されたセキュリティ テスト、およびCI/CDセキュリティの使用に関係しています。

コード開発、依存関係管理から展開、監視まで、パイプライン全体にセキュリティ プラクティスを組み込むことにより、組織は強力なセキュリティ態勢を維持しながら、ソフトウェアを迅速かつ確実に提供できます

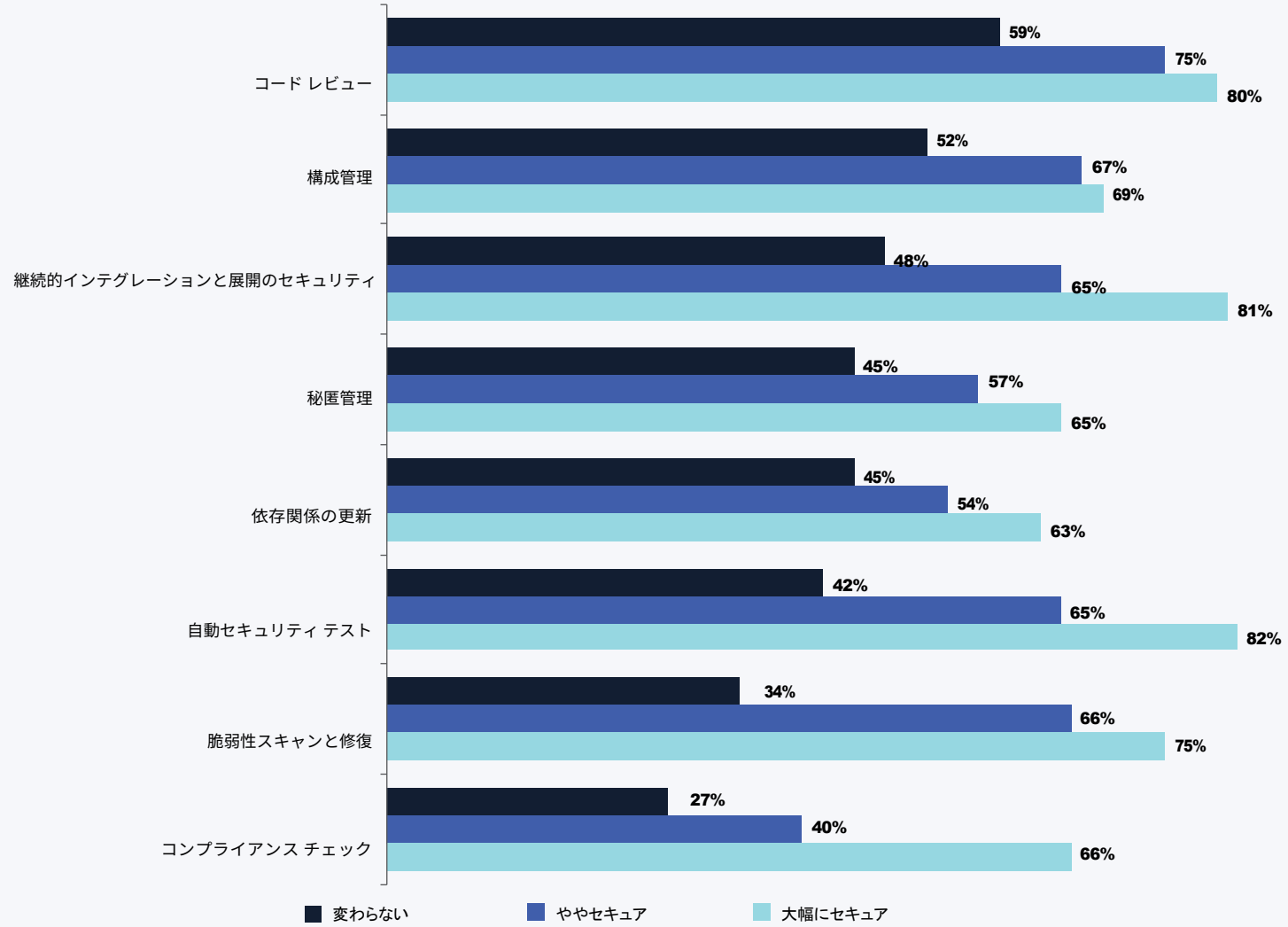
クラウドネイティブ アプリケーションが「大幅にセキュア」であると認識している組織は、セキュリティ戦略をより頻繁に実践するという明確な傾向があります。これは、頻繁でプロアクティブなセキュリティ対策とセキュリティ認識の向上との間に相関関係があることを示しています。組織が自動テスト、継続的インテグレーション、脆弱性スキャンなどのセキュリティ対策を頻繁に実施する取り組みを強化すると、環境がより安全であると認識する傾向があります。それでもなお、コード レビューは、セキュリティ上の懸念に対処するためのゴールド スタンダードです。

図10

クラウドネイティブ アプリケーションのセキュリティを著しく向上させるセキュリティ戦略

どのような種類のセキュリティ評価を実行していますか？（該当するものをすべて選択してください）

（「2年前と比較して、クラウドネイティブ アプリはどの程度安全ですか？（1つ選択してください）」の回答別データ）



2024 Cloud Native Security Survey Q17 x Q21a, サンプル数 = 197,「更新のたび」または「毎週」と回答した回答者。

主要なクラウドネイティブ セキュリティ戦略の検証

図9では、組織がさまざまなセキュリティ戦略を採用する頻度を尋ねました。図11では、同じ戦略リストを使用していますが、代わりに、これらの各戦略が組織にとってどの程度重要かを尋ねています。コード レビューは、ここでもリストのトップに位置し、84%がこの戦略を極めて重要またはとても重要と認識しています。手動レビューは、セキュリティ上の懸念を評価する際のゴールド スタンダードであり、ビジネス ロジックの欠陥、アーキテクチャの欠陥、コードの臭い（コード内の問題の兆候）、アンチパターン、ロジック エラー、エッジ ケース（極端なパラメータによる動作不良）の特定やセキュリティ ツールの検出結果の検証に優れています。

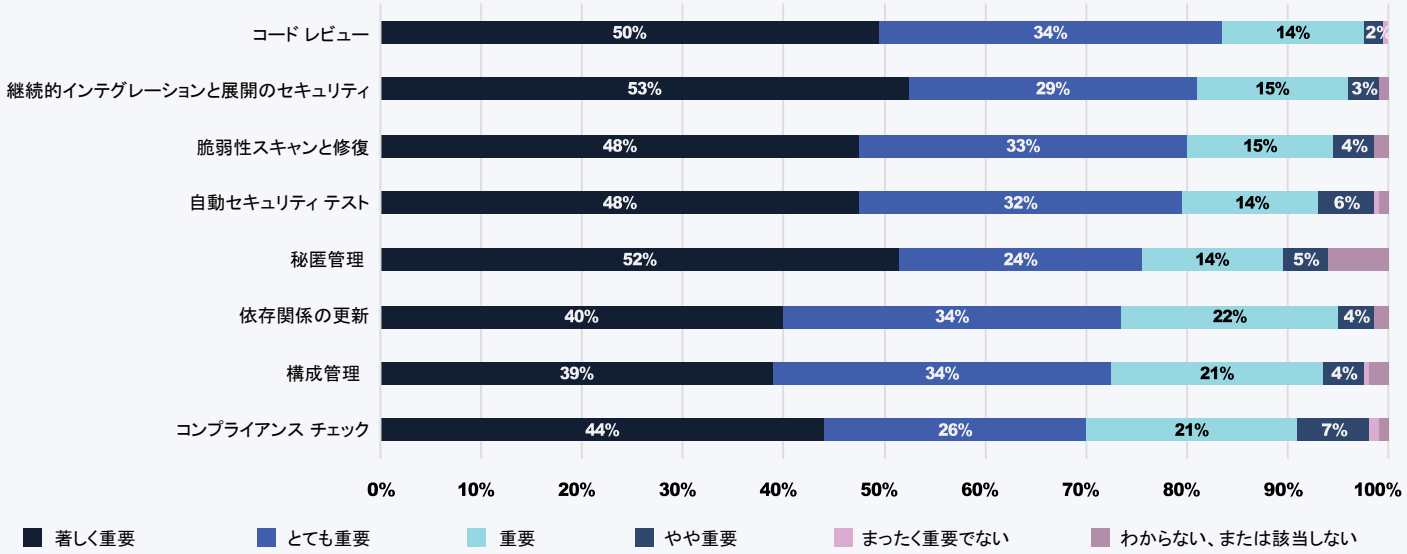
知識豊富なレビュー担当者が体系的に実施すれば、手動コード レビューはクラウドネイティブのセキュリティの向上に非常に効果的です。SASTやSCAなどの自動化ツールは脆弱性の検出に重要な役割を果たしますが、手動コード レビューには、特にクラウドネイティブ環境のコンテキストにおいて、これらのツールを補完する独自の利点があります。

CI/CDセキュリティ（82%）、脆弱性スキャンと修復（81%）、自動セキュリティ テスト（80%）の重要性は、図9に見られる相違と一致しており、組織のセキュリティ ツール ポートフォリオとツール チェーンの一部としてこれらのツール カテゴリを採用することの重要性を裏付けています。

図11

選択されたクラウドネイティブ セキュリティ戦略の重要性

これらのセキュリティ戦略はそれぞれどの程度重要ですか？（1行につき1つ回答してください）



2024 Cloud Native Security Survey. Q18. サンプル数 = 200.「著しく重要」または「とても重要」を選択した回答者の割合で並び替え

ウェビナーとカンファレンスは、CNCFのセキュリティ ツールとアップデートに関する情報を得るための主な情報源

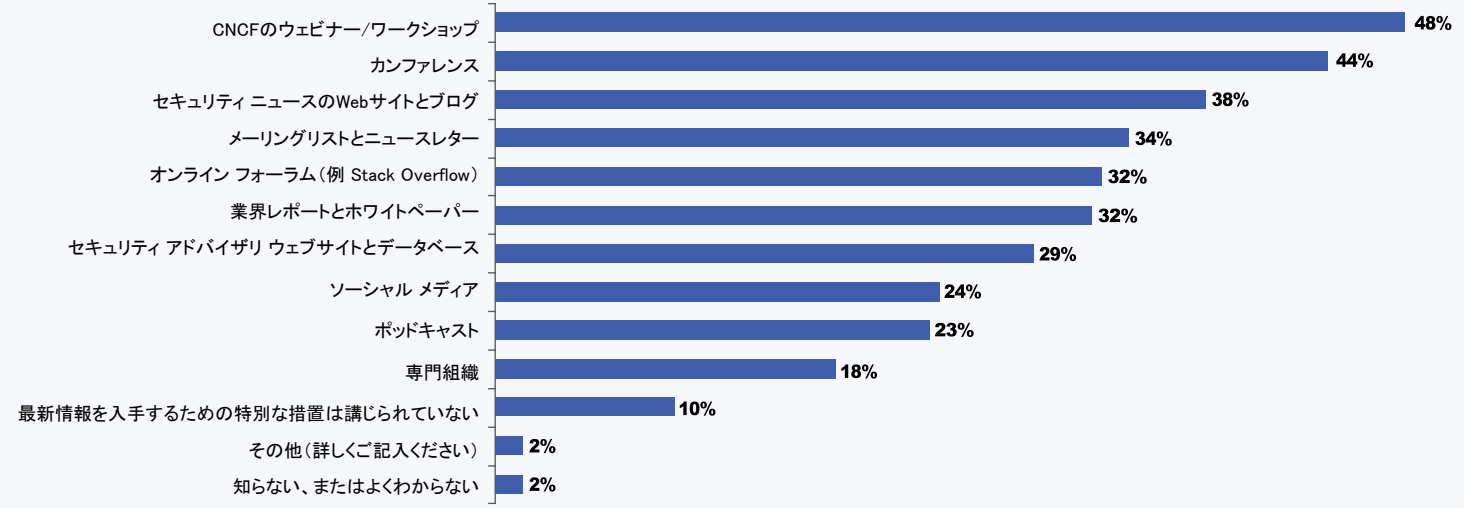
サイバーセキュリティ分野は絶えず変化しています。新しい脆弱性、脅威、エクスプロイト（脆弱性を狙う攻撃）、パッチ、ツール、コンポーネント、ベストプラクティスが常に出現しています。コンポーネントが変更されなくても、新しい脆弱性が発見されれば、脆弱性を悪用しようとする者と脆弱性を修正しようとする者の間で競争が生じ得ます。

図12は、回答者の48%がCNCFのセキュリティ ツールと更新の最新情報を入手する主なアプローチが、CNCFのウェビナーとワークショップであることを示しています。最新情報を入手するための他の主なアプローチには、カンファレンス（44%）、セキュリティ ニュースWeb サイトとブログ（38%）、メーリング リストとニュースレター（34%）などがあります。回答者の大多数が単一のアプローチを使用していないことから、回答者の大多数が好むアプローチの組み合わせがあるのではないでしょうか。サンプルの67%がCNCFウェビナーとカンファレンスを組み合わせて使用しています。メーリング リストとニュースレターを追加すると、サンプルの合計は76%に増加し、セキュリティ ニュースWebサイトとブログを追加すると、サンプルの合計は82%に増加し、セキュリティ アドバイザリWebサイトとデータベースを追加すると、サンプルの合計は84%に増加します。重要なイベントとコーナー ケース（複数の極端なパラメータによる動作不良）を識別するには、アプローチのポートフォリオを採用することが最善であると推奨します。

図12

回答者はクラウドネイティブ セキュリティのプロジェクト、ツール、問題についてどのように最新情報を入手しているか

CNCF のセキュリティ ツールと更新についてどのように最新情報を入手していますか？（該当するものをすべて選択してください）



2024 Cloud Native Security Survey. Q44. サンプル数 = 200. 有効数 = 200. 総言及数 = 664

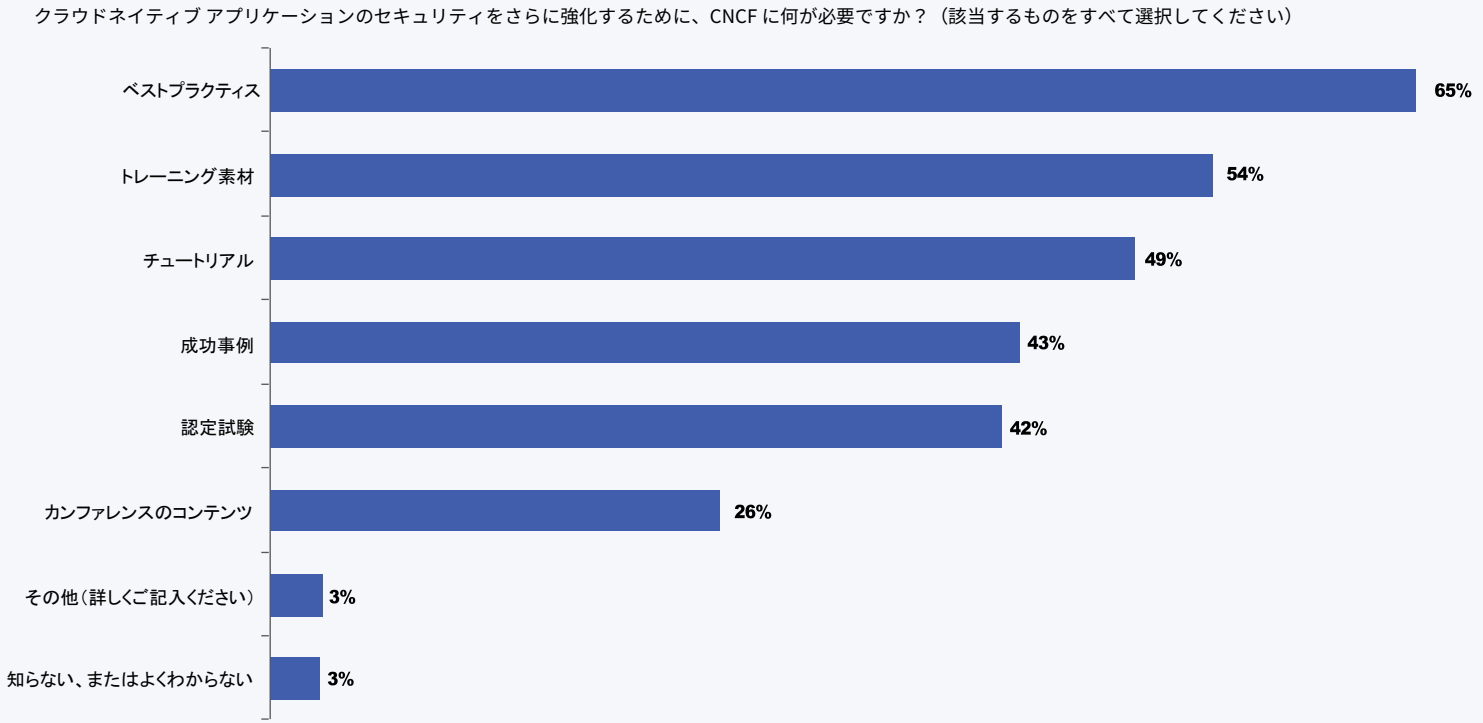
ベストプラクティスとトレーニング資料は、クラウドネイティブ アプリケーションのセキュリティを向上させるために最も望まれるコンテンツ

図13は、クラウドネイティブ セキュリティのベストプラクティスとそれに続くトレーニング マテリアルが、CNCFに回答者が求める最も望ましいコンテンツであることを示しています。これは、以前のCNCFおよびOpenSSFの調査結果を再び裏付けています。

Linux Foundationは、安全なソフトウェア開発、Kubernetes、サービス メッシュ、APIに重点を置いた、さまざまなトレーニングおよび認定コース、チュートリアル、試験を提供しています。これらのコースの一部は無料ですが、その他は有料です。これらのコースのほとんどには、コンテンツ全体にベストプラクティスが分散して含まれています。サイバーセキュリティは、CNCFやOpenSSFなどの確立された大規模プロジェクトの重要な焦点です。詳細については、以下を参照ください。
training.linuxfoundation.org/resources

図13

クラウドネイティブ アプリケーションのセキュリティをサポートするためのCNCF推奨コンテンツ



2024 Cloud Native Security Survey. Q42. サンプル数 = 200. 有効数 = 200. 総言及数 = 565

調査方法

調査について

この調査は、Linux Foundation ResearchとCNCFが2024年3月から2024年5月にかけて実施したWeb調査に基づいています。調査の目的は、組織がクラウドネイティブ セキュリティにどのように取り組んでいるかを把握することでした。このセクションでは、調査方法と、データの分析方法に関する背景、および回答者の人口構成について説明します。

研究の観点からは、サンプルの偏りを排除し、高いデータ品質を確保することが重要でした。サンプルの偏りを排除するために、Linux Foundationの加入者、メンバー、パートナー コミュニティ、ソーシャル メディアから使用可能なサンプルを調達しました。広範な事前スクリーニング、調査のスクリーニング質問を通じてデータ品質に対処し、回答者が所属組織を代表して質問に正確に回答できるだけの十分な専門的経験を持っていることを確認することで、データ品質をチェックしています。

調査データは、特定業界の企業、ITベンダーやサービス プロバイダー、非営利団体、学術機関、政府機関から収集しました。回答者はさまざまな垂直産業やあらゆる規模の企業にまたがり、主に北米（76%）からではありますが、複数の地域からデータを収集しました。

2024年クラウドネイティブ セキュリティ調査は、スクリーニング、回答者の人口構成、クラウドネイティブ アプリケーションのサプライ チェーン セキュリティ、オープンソース セキュリティ ツールの使用、CNCFがどのようにニーズをより良くサポートしているかなど、45の質問で構成されています。このレポートではオープンソース セキュリティ ツールの使用状況は公開していませんが、Data.Worldでデータセットと調査の度数を確認できます。2024年クラウドネイティブ セキュリティ調査、データセット、調査の度数へのアクセスについては、「Data.World access（Data.Worldへのアクセス）」を参照してください。

調査のハイレベルの設計概要を図14に示します。

対象読者には、以下の基準を満たす回答者が含まれていました。

- クラウドネイティブ アプリケーションの開発に携わっていること
- 勤務先の組織がクラウドネイティブ アプリケーションのセキュリティをどのように扱っているかに精通していること
- 組織がクラウドネイティブのテクノロジーと手法を使用していること
- 雇用されていること

Linux Foundation Researchによる調査は2024年3月に作成され、2024年4月に実施されました。合計200人の回答者が調査に回答しました。サンプル サイズに対する誤差の範囲は、信頼水準で90%±5.8%、信頼水準で95%±6.9%でした。

データ収集は、企業規模、地理的地域、組織の種類ごとに階層化しました。データは主に、地理的地域、企業規模、組織の種類ごとにセグメント化されました。

図14

調査設計

ページ	質問	質問のカテゴリ	質問に答えるのは誰か
P1		はじめに	回答者全員
P2	Q1 – Q7	導入の質問	回答者全員（N=200）
P3	Q8 – Q9	あなたご自身について教えてください	回答者全員（N=200）
P4	Q10 – Q11	オープンソースへの関わりについて教えてください	オープンソース貢献者（N=153）
P5	Q12 – Q16	あなたの勤務先組織について教えてください	回答者全員（N=200）
P6	Q17 – Q23	クラウドネイティブ アプリケーションのサプライチェーン セキュリティ	回答者全員（N=200）
P7 – 15	Q24 – Q41	オープンソース セキュリティ ツールの使用（9つのカテゴリ）	ツール使用経験のある回答者（N=54 to 87）
P16	Q42 – Q45	最後の質問	回答者全員（N=200）

2024 Cloud Native Security Survey

回答者は調査のほぼすべての質問に回答する必要がありましたが、回答者が質問に答えられない場合に備えて、すべての質問の回答リストに「知らない、またはよくわからない」（DKNS：Don't know or not sure）という回答を追加するという規定を設けました。しかし、これによりさまざまな分析上の課題が生じました。

1つのアプローチは、DKNSを他の回答と同様に扱い、DKNSに回答した回答者の割合を決定することでした。このアプローチの利点は、収集したデータの正確な分布を示すことです。このアプローチの課題は、有効な回答分布がゆがむことです。つまり、回答者が質問に答えられる回答の分布が歪む可能性があることです。

このレポートの分析の一部では、DKNS回答を除外しています。これは、欠落データをランダムに欠落しているか、完全にランダムに欠落しているかに分類できるからです。質問からDKNSデータを除外しても、他の回答のデータ（カウント）の分布は変わりませんが、残りの回答全体の回答率を計算するために使用される分母のサイズは変わります。これにより、残りの回答のパーセンテージ値が比例して増加します。DKNSデータを除外することを選択した場合、図の脚注に「DKNS回答は除く」というフレーズを記載されます。

このレポートのパーセンテージ値は、四捨五入により合計が正確に100%にならない場合があります。

Data.World へのアクセス

LF Researchは、それぞれの実証的プロジェクトのデータセットをData.World公開しています。このデータセットには、調査ツール、生の調査データ、スクリーニングおよびフィルタリング基準、調査の各質問の度数分布表が含まれています。このプロジェクトを含むLF Researchデータセットは、data.world/thelinuxfoundationで見つかります。Linux Foundationデータセットへのアクセスは無料ですが、data.worldアカウントを作成する必要があります。

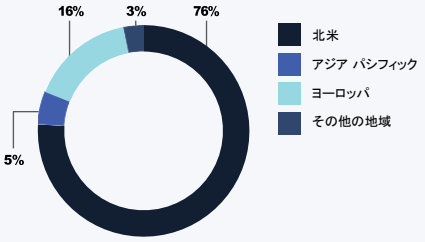
回答者の人口構成

これらの人口構成は、2024年のクラウドネイティブ セキュリティ調査の回答者像を提供します。図15では、より洞察に富んだ分析を容易にするために、すべての人口統計を再グループ化しています。元のソース データと調査度数については、上記のData.Worldアクセスを参照してください。

図15

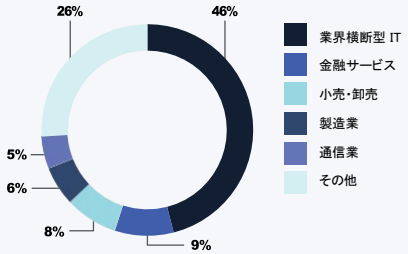
回答者の人口構造

組織本部所在地



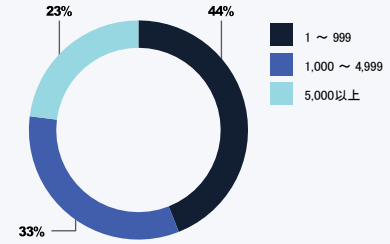
2024 Cloud Native Security Survey, Q12, サンプル数 = 200

組織の業種



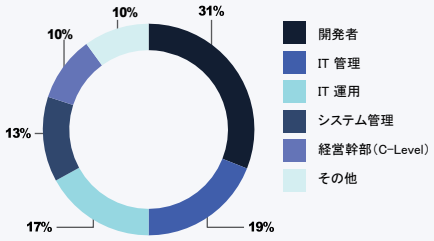
2024 Cloud Native Security Survey, Q14, サンプル数 = 200

企業規模（従業員数）



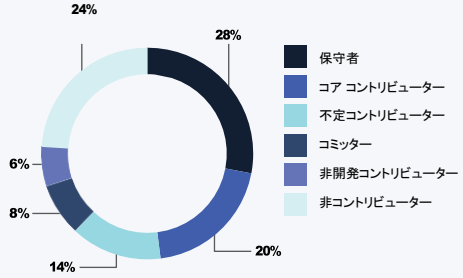
2024 Cloud Native Security Survey, Q15, サンプル数 = 200

回答者の役割



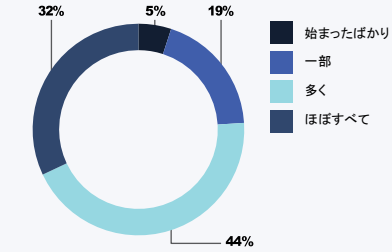
2024 Cloud Native Security Survey, Q8, サンプル数 = 200

OSSの役割

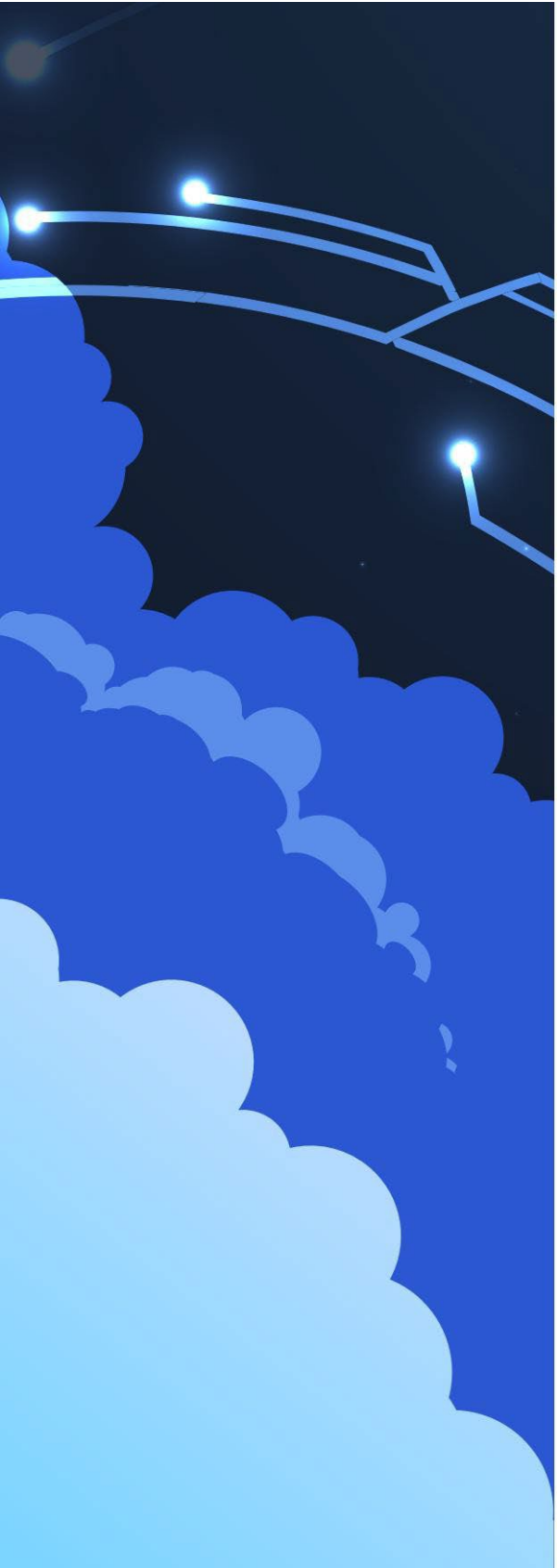


2024 Cloud Native Security Survey, Q11, サンプル数 = 200

クラウドネイティブの導入



2024 Cloud Native Security Survey, Q7, サンプル数 = 200

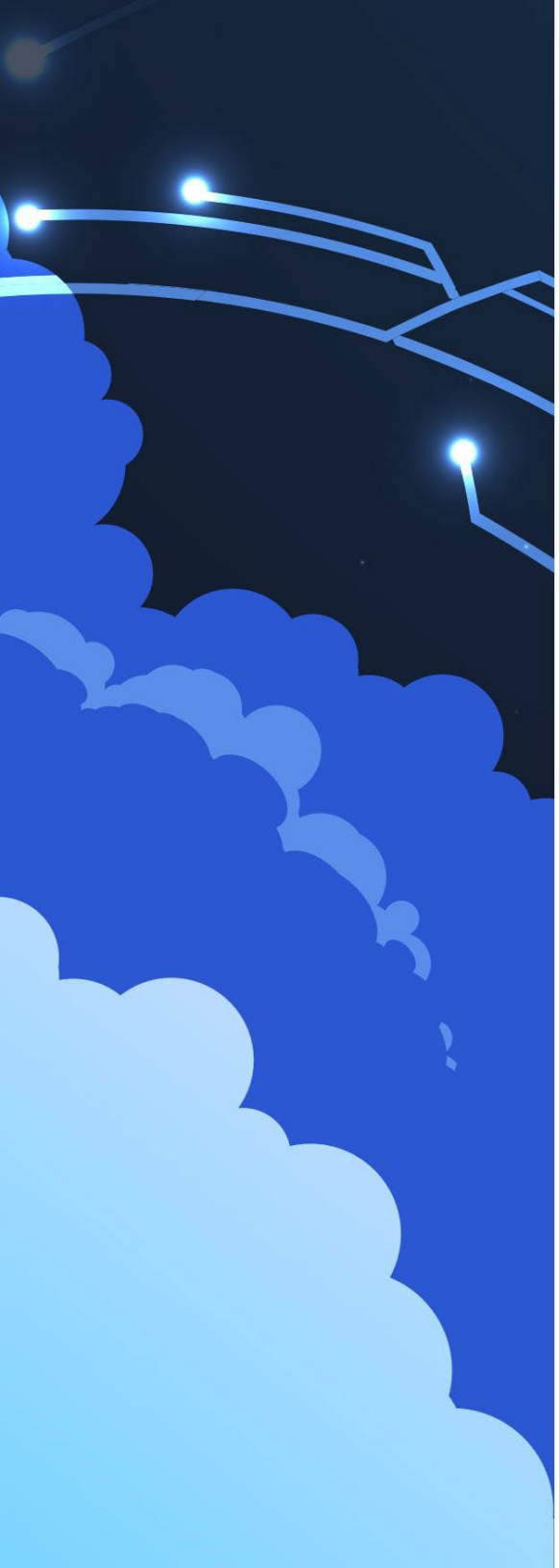


著者について

STEPHEN HENDRICKは、Linux Foundationの研究担当副社長で、オープンソース ソフトウェアがITの生産者と消費者にとって、どのようにイノベーションの原動力となるかについてLinux Foundationが理解するための中核となるさまざまな研究プロジェクトの主任研究員を務めています。Steve（Stephen）は、ソフトウェア業界アナリストとして30年以上にわたって培った主要な研究手法を専門としています。Steveは、DevOps、アプリケーション管理、意思決定分析など、アプリケーション開発と展開のトピックに関する特定分野の専門家です。Steveは、市場の動向を深く理解できるさまざまな定量的および定性的研究手法の経験を持ち、多くのアプリケーション開発と展開の分野で研究の先駆者となっています。Steveは1,000を超える出版物を執筆し、シンジケート リサーチやカスタム コンサルティングを通じて、世界有数のソフトウェア ベンダーや注目度の高い新興企業に市場ガイダンスを提供しています。

ADRIENN LAWSONは、Linux Foundationのデータ アナリストです。AdriennはOxford大学で社会データ サイエンスの修士号を取得しました。彼女は調査の開発、分析、レポート作成を担当しています。Adriennはこれまで、Oxford大学、Budapest Institute for Policy Analysis（ブダペスト政策分析研究所）、U.K.’s Office for National Statistics（英国国家統計局）で研究を行ってきました。彼女は、地理的に分散したコミュニティ内でのオープンソース コラボレーションの集団的な力に最も興味を持っています。加えて、OSSの資金調達、持続可能性に関わる課題、そして、責任ある技術進歩を追求する開発者の支援に関連する傾向とソリューションを研究することに最も興味を持っています。

JEFFREY SICAは、CNCFのプロジェクト責任者で、保守者のエクスペリエンスの向上、コミュニティの構築、プロジェクトの自動化に重点を置いています。それ以前は、Red HatとMichigan大学でクラウドネイティブ テクノロジーとCICDパターンに注力していました。JeffreyはKubernetesの上流の貢献者であり、SIG-Contribex、SIG-Release、SIG-UIを支援しています。彼はオープンソース開発と燃え尽き症候群の認識と緩和を熱心に提唱しています。



謝辞

検索と分析に関する洞察と経験を親切に共有してくださった調査参加者全員に感謝します。
特に、研究プロセスのさまざまな段階に関与してくださった査読者とLFの同僚に感謝します。

- Chris Aniszczyk
- Elizabeth Bushard
- Hilary Carter
- Jorge Castro
- Mia Chaszeyka
- Anna Hermansen
- Christina Oliviero
- David Wheeler
- Katie Greenley

本訳文について

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

翻訳協力：天満尚二

CLOUD NATIVE COMPUTING FOUNDATION

クラウドネイティブ コンピューティングは、オープンソース ソフトウェア スタックを活用してアプリケーションをマイクロサービスとして展開します。マイクロサービスでは、各コンポーネントが独自のコンテナーにパッケージ化され、リソースの使用率を最適化するために動的にオーケストレーションされます。The Cloud Native Computing Foundation（CNCF）は、Kubernetes、Envoy、Prometheus、その他数多く、クラウドネイティブ エコシステム内のキー プロジェクトをホストしています。CNCFは、世界最大のパブリック クラウド プロバイダーやエンタープライズ ソフトウェア企業から革新的なスタートアップ企業まで、主要な開発者、エンドユーザー、ベンダーを結集する中立的なコラボレーション ハブとして機能します。CNCFは、非営利団体であるLinux Foundationの一員として、業界全体にわたるクラウドネイティブ テクノロジーの成長と採用を促進しています。
詳細については、www.cncf.ioをご覧ください。

x.com/cloudnativefdn

facebook.com/CloudNativeComputingFoundation

www.linkedin.com/cloud-native-computing

youtube.com/c/cloudnativefdn

github.com/cncf

THE LINUX FOUNDATION | Research

2021年に創設された Linux Foundation Research は、オープンソース コラボレーションの規模の成長を調査し、新興技術のトレンド、ベストプラクティス、オープンソース プロジェクトの世界的な影響に関する洞察を提供しています。プロジェクト データベースとネットワークを活用し、定量的および定性的な方法論におけるベストプラクティスに取り組むことで、Linux Foundation Research は世界中の組織に役立つオープンソースの洞察を提供する頼りになるライブラリを作成しています。

x.com/linuxfoundation

facebook.com/TheLinuxFoundation

linkedin.com/company/the-linux-foundation

youtube.com/user/TheLinuxFoundation

github.com/LF-Engineering

この作業を参照するには、次のように引用してください。
Stephen Hendrick, Adrienn Lawson, and Jeffrey Sica, “2024 Cloud Native Security Report: How Organizations Are Addressing Security for Cloud Native Application Development, foreword by Eddie Knight,” The Linux Foundation, October 2024.