Red Hat

2026

クラウドネイティブ・セキュリティの現状

クラウドネイティブ・エコシステム全体を保護する

目次

はじめに

2026 年版クラウドネイティブ・セキュリティの現状に関するレポートは、昨年のエディションを基にしながら、Kubernetes 以外にも焦点を広げ、より広範なエンタープライズ・セキュリティ・ランドスケープを反映しています。組織がハイブリッドおよびマルチクラウド環境においてコード、インフラストラクチャ、ワークロードのセキュリティをどのように重視しているかについて調査するとともに、ガバナンス、自動化、AI の影響にも重点を置いています。

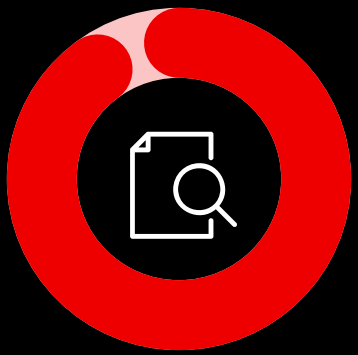
今年のレポートは、2025 年 8 月 25 日から 9 月 23 日の間にオンラインで実施された 600 件のアンケート結果をまとめたものです。各アンケートの所要時間は約 20 分でした。回答者は、従業員 100 名以上の企業でアプリケーション、セキュリティ、プラットフォーム、開発を担当する IT プロフェッショナルで、エキスパートのネットワークやオンラインパネルを通じて集められました。

主な調査結果

インシデントは組織の規模や地域を問わず、ほぼすべての組織に影響を与える

97%

少なくとも 1 件の問題が発生した組織の割合



報告されたインシデント

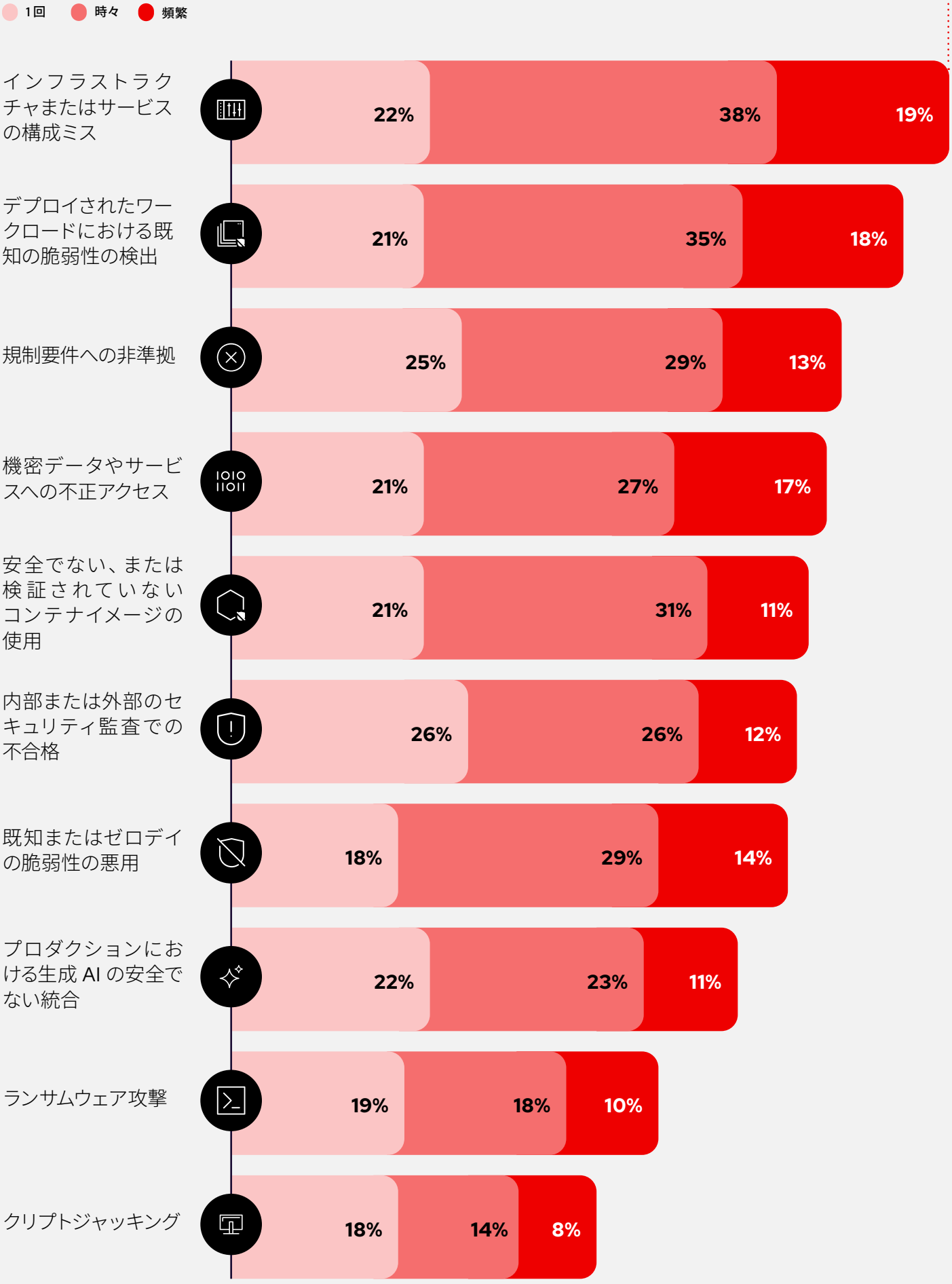


図 1. インシデントを引き起こす主な要因は構成ミスと脆弱性。

セキュリティインシデントは頻繁に発生し、コストがかかる

セキュリティの問題は、ほぼすべてのクラウドネイティブ・チームにとって悩みの種です。昨年では **97%** の企業でクラウドネイティブ・セキュリティのインシデントが少なくとも 1 件発生しています。これらのインシデントにより、ビジネスに実質的なコストがもたらされます。**74%** の組織に、セキュリティ上の懸念から過去 12 カ月間にアプリケーションのデプロイメントの遅延や延期が発生しています。

つまり、セキュリティ問題による遅延、その場しのぎの一時的な対応、中断は、例外ではなく一般的なものであり、不適切なセキュリティ対策ではコストがかさんでしまうということが明確に示されています。

97%

過去 1 年間にクラウドネイティブ・セキュリティのインシデントが 1 件以上発生した組織の割合

74%

セキュリティ上の懸念により、過去 12 カ月間にアプリケーションのデプロイメントの遅延や延期が発生した組織の割合

39%

明確に定義されたクラウドネイティブ・セキュリティ戦略を実施している組織の割合。半数以上がまだ計画を策定中または開発中。

クラウドネイティブ・セキュリティは基礎的だが不均一

クラウドネイティブ・セキュリティは重要なものとして広く認識されていますが、その成熟度は組織によって大きく異なります。明確に定義されたクラウドネイティブ・セキュリティ戦略を実施していると回答した企業はわずか **39%** で、半数以上がまだ計画を策定中または開発中であるとしています。それと同時に、大半の回答者 **(56%)** が、日常的なセキュリティポスチャは極めてプロアクティブであると回答しています。

これは、実際の戦略や実行よりも、自信のほうが上回っていることが多いということを示唆しています。

このギャップから、クラウドセキュリティのガバナンスと成熟度に対する、より構造化されたアプローチの必要性が浮き彫りになります。

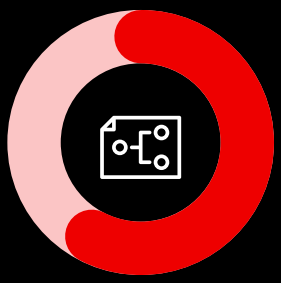
防護機能は成熟度を定義するものだが、導入には一貫性がない

セキュリティ防護機能 (組み込みのセキュリティ制御やベストプラクティス) の使用は成熟度の重要な指標となりますが、その実装はつぎはぎの状態のままです。たとえば、基本的な ID 制御はほぼ普遍的に使用されており、約 4 分の 3 の組織が ID およびアクセス管理 (IAM) ツールを使用しています。しかし、ソフトウェアの整合性のためにコンテナイメージの署名と検証を導入しているのは、およそ半数でしかありません。

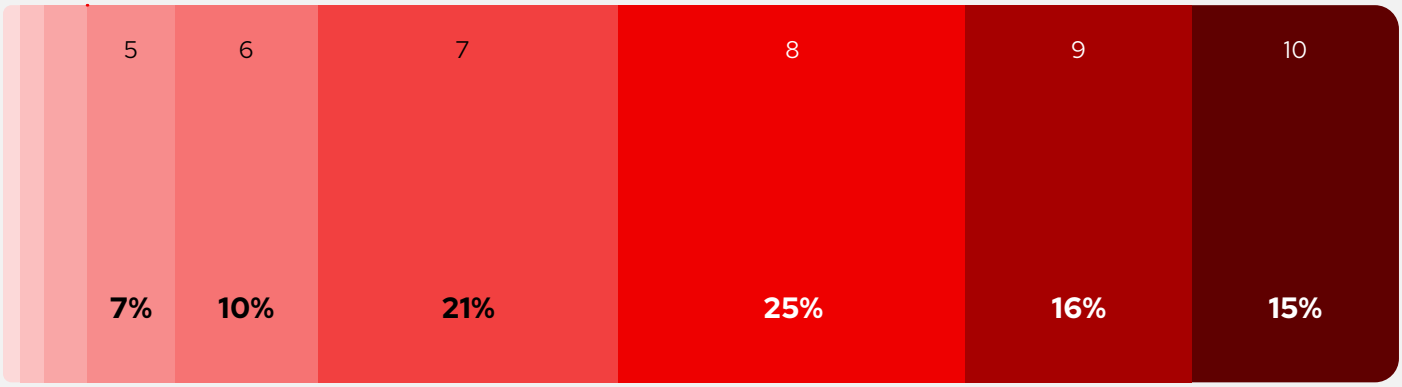
これらにはイメージ署名、ランタイム保護、自動ポリシー適用などの対策が該当し、業界全体でセキュリティのベースラインが不均一になっています。あるセキュリティ担当者は、「クラウドネイティブ・セキュリティは一度設定したらそれで終わり、と考えるのは大きな誤解です。継続的な監視や適応の必要性が完全に忘れ去られています」と警告しています。

つまり、多くのチームが重要な防護機能をいまだに見落としているのです。

セキュリティポスチャがほとんどリアクティブであると回答した組織は 7% 未満 (評価 0 - 4)



56%
プロアクティブであると回答した組織の割合 (評価 8 - 10)



完全にリアクティブ
(問題が発生したら対応)

極めてプロアクティブ
(戦略的、予防的、予測的)

日常のアプローチ

図 2. クラウドネイティブのセキュリティ重視における機能よりも自信が上回っている。

自動化およびサプライチェーンのセキュリティへとシフトする投資

先を見据えて、組織はこれらの成熟度のギャップに対処するために、セキュリティに対する投資のバランスを再調整しています。今後 1 - 2 年間の最優先事項は、DevSecOps の自動化とソフトウェア・サプライチェーンのセキュリティです。調査対象の組織の **60%** 以上が、継続的インテグレーション/継続的デリバリー (CI/CD) パイプラインのセキュリティ自動化 (ポリシーの自動化、統合など) に投資することを計画しており、**56%** はソフトウェア・サプライチェーンのセキュリティ保護 (コードからランタイムに至る整合性の管理) に投資することを計画しています。それに次いで多くの組織が挙げたのが、ランタイム保護の拡張 (**54%** が投資を計画) で、デプロイ時に継続的な防御を組み込むことを重視しています。これは、自動化と組み込みセキュリティに関する取り組みの統合を示しており、成熟した回復力のあるクラウドネイティブ・プログラムを形成する分野に投資が向けられています。

超

60%

調査対象の組織のうち、CI/CD パイプラインのセキュリティ自動化に投資する予定の組織の割合

56%

ソフトウェア・サプライチェーンの保護 (コードからランタイムまでの整合性の管理) に投資する予定の組織の割合

79%

生成 AI によってセキュリティに関する新たな課題がクラウド環境に発生していると回答した組織の割合

59%

文書化された社内 AI 使用ポリシーやガバナンス・フレームワークが欠如している組織の割合

ガバナンスの課題は AI リスクへの対応

開発および DevOps への AI の急速な導入によって新たなリスクがもたらされ、ガバナンスがそれに追いつかない状況が生じています。回答者の **79%** が、生成 AI によってセキュリティに関する新たな課題がクラウド環境に発生していると述べています。しかし、正式なポリシー策定は遅れており、**59%** の企業では文書化された社内 AI 使用ポリシーやガバナンス・フレームワークが欠如しています。

このような隔たりは、AI 関連のリスク (データの漏洩や安全でない AI ツールなど) が監視されずに増大し、組織が危険にさらされるようになることを示唆しています。

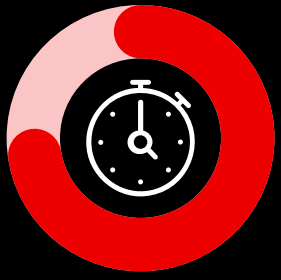
第1章

セキュリティインシデントとそのコスト

クラウドネイティブ環境では依然として、セキュリティインシデントが実際に発生しています。データによると、セキュリティインシデントは比較的一般的であり、運用に支障をきたす可能性があります。

過去1年間において、調査対象となったほぼすべての組織 (**97%**) で、クラウドネイティブ・セキュリティに関する問題が1件以上発生しています。構成ミスや既知の脆弱性などのインシデントは、稀に起きる異常と言うにはほど遠く、ほぼ日常的なものとなっています。実際、最も多いインシデントタイプはクラウド・インフラストラクチャの構成ミスと既知の脆弱性の検出です。これは、日常的な不備 (S3 バケットを開いたままにしたり、パッチを適用していないコンテナをデプロイしたりするなど) が、高度な攻撃よりも多くの問題を引き起こしていることを意味します。

これらのインシデントがビジネスに与える影響は甚大です。



74%

過去 12 カ月間において、セキュリティ上の懸念により**クラウドネイティブ・アプリケーションのデプロイメントの遅延や延期**が発生したことがある組織の割合

クラウドネイティブ・セキュリティ・インシデントによる影響

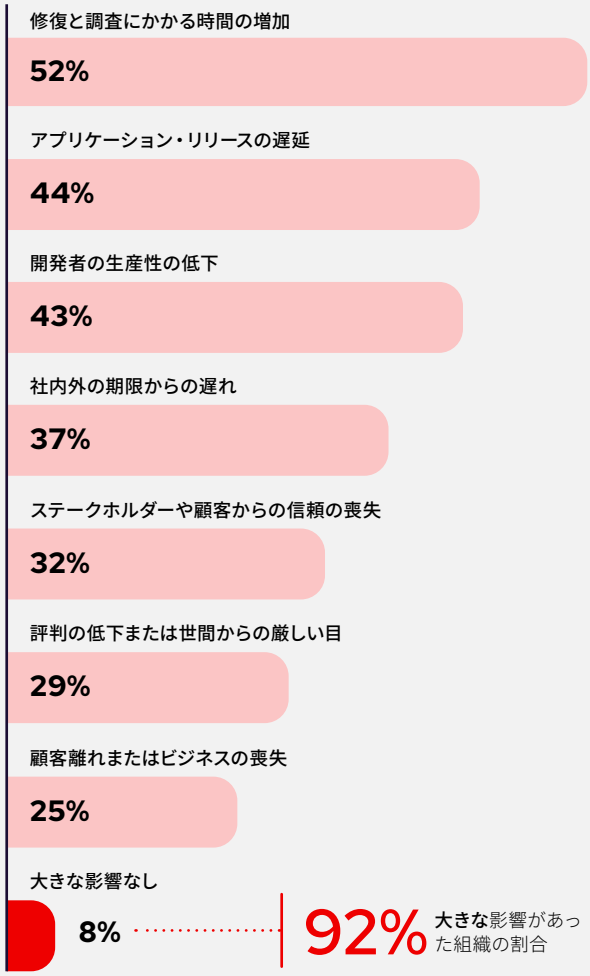


図 3. セキュリティの遅延は珍しいものではなく、それによってコストがかかっている。

調査対象の組織のうち、セキュリティ上の懸念から過去 12 カ月間にアプリケーションのリリースの遅延や延期が発生したと回答した組織は、**74%** にも上ります。つまり、4 分の 3 のチームはセキュリティの問題が発生したためにデプロイメントが遅れ、アジリティや市場投入時間に直接影響が生じています。この種の遅延はただ不便というだけでなく、収益機会の逸失、納期の遅れ、チームの不満を招くことになります。

クラウドネイティブ・セキュリティのインシデントがもたらす一般的な影響には他にも、予定外の作業の増加や顧客からの信頼の失墜などがあります。調査によると、**92%** の企業はセキュリティインシデントにより、ソフトウェア提供能力やビジネス目標の達成能力について、少なくとも 1 つの大きな影響が及んでいます。報告された影響の種類は多岐にわたり、たとえば次のようなものがあります。

アプリケーション・リリースの遅延
チームはセキュリティの問題を修正している間、デプロイや機能のリリースを延期しなければなりません。

開発者の生産性の低下
開発者は、脆弱性の修復や構成エラーへの対処のために、サイクルから逸脱することになります。

社内または顧客の期限からの遅れ
セキュリティの問題により、納品の期日を守れなくなります。

ステークホルダーや顧客からの信頼の喪失
重要なセキュリティ問題により、経営陣や顧客からの信頼が損なわれます。

評判の失墜やビジネスの損失
最悪の場合は、セキュリティ障害が人々からの注目を浴びたり、顧客離れが発生したりすることになります。

脆弱なクラウドセキュリティが組織の時間とコストを直接損なうことは明らかです。遅延によってエンジニアリングの生産性が低下し、ビジネスに連鎖反応が起き、市場機会の逸失や収益の損失が発生します。このような不利益は珍しくなく、4 分の 3 のチームでデプロイメントが遅延しているという事態は、クラウドセキュリティが単なる技術的な懸念事項ではなく、重大なビジネスリスクであることを示しています。

このようなインシデントコストに対処するには、よりプロアクティブな対策が必要になります。

構成ミスの割合が高い (過去 12 カ月以内に **78%** があったと報告) ことは、構成管理や脆弱性に対するパッチの適用などの基本的な部分に改善の必要があることを示唆しています。どの組織も、より強固な防護機能とプロセスがなければ、頻繁なインシデントやそれに関連する遅延に直面し続けることになると考えるべきです。このデータは、繰り返し発生する問題に対応するための多額のコストを回避するには、予防的なセキュリティに投資するべきであるという説得力のある根拠となります。

第2章

クラウドネイティブ・セキュリティのガバナンスと成熟度

強力なクラウドネイティブ・セキュリティポスチャを実現するには、ツールと同程度にガバナンスとプロセスの成熟度が重要となります。この調査ではある矛盾が明らかとなりました。それは、多くの組織は適切に運営していると信じているにもかかわらず、成熟したセキュリティプログラムを形成する正式な戦略と制御を実際に導入している組織は比較的少数である、ということです。

プロアクティブな態勢

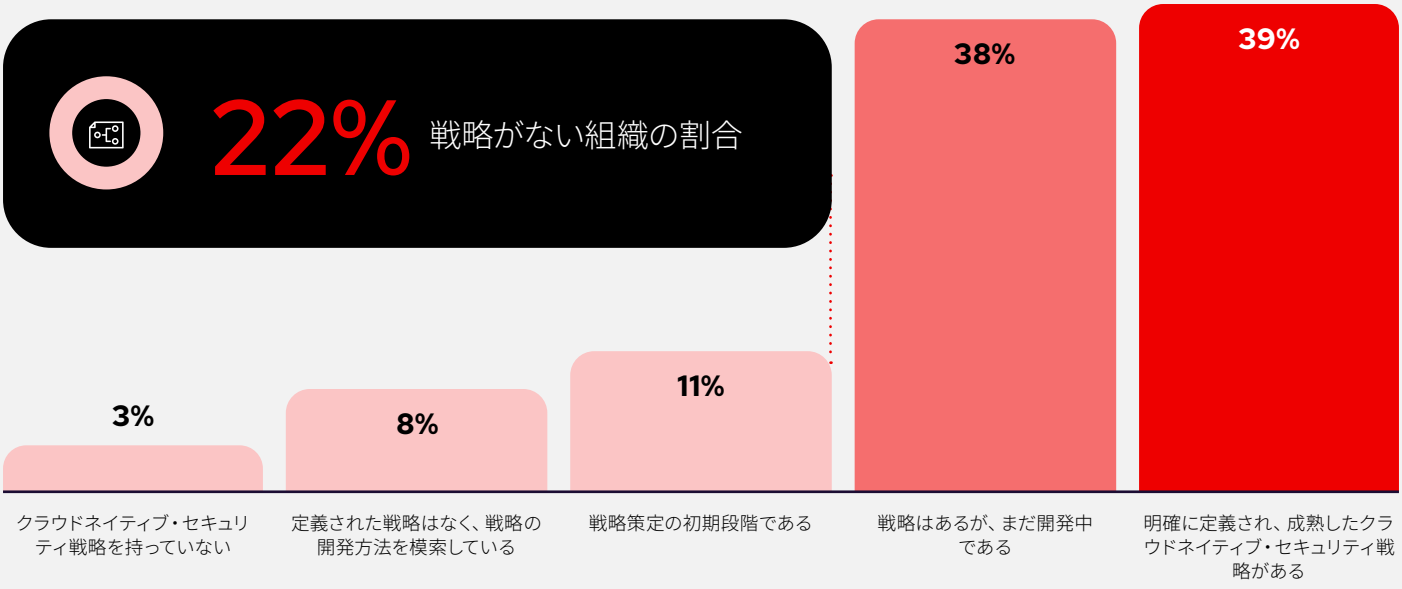


図 4. 定義された戦略がなければ、セキュリティはリアクティブかつ断片化されたままとなり、チームは危険にさらされる。

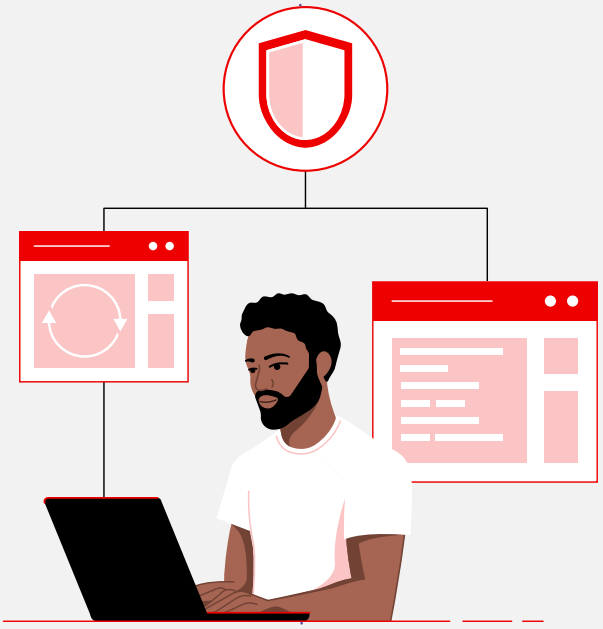
調査対象のチームの大多数がプロアクティブな態勢であると主張しており、**56%** が日常的なセキュリティアプローチは「極めてプロアクティブ」であると評価しています。さらに、ほとんどリアクティブであると回答したのは 7% 未満でした。これは、大半の組織が将来を見据えたいと考えていることを示しています。

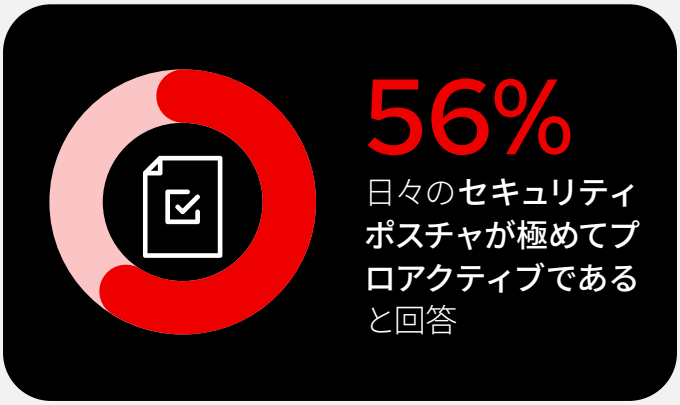
チームがセキュリティを確保したいと考えていることは明らかです。その一方で、それを支える基盤となるガバナンスを策定している組織ははるかに少数です。

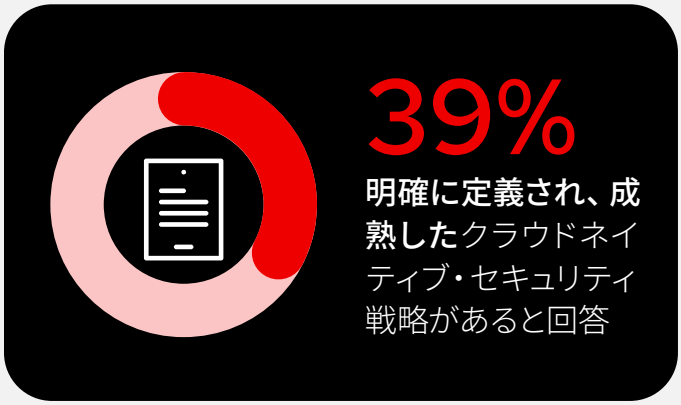
明確に定義されたクラウドネイティブ・セキュリティ戦略を実施している企業はわずか **39%** でした。それ以外の企業はその場しのぎであり、半数以上がセキュリティ戦略をまだ開発中または改良中、あるいは戦略の作成方法を検討中の段階にあります。クラウドセキュリティ戦略がまったくない場合 (約 22% の組織) もあり、成熟度には明らかにギャップがあります。

実際には、多くの組織は自分たちの準備状況を過大評価していると考えられます。

プロアクティブな態勢であると宣言しても、組織がポリシーを持っておらず、それを施行するための構造がないなら、準備が整っていることにはなりません。クラウドネイティブ・セキュリティを真に成熟させるには、定義された目的、チーム間の連携、組み込みの制御機能が必要になります。多くのプログラムはこの点が不十分です。







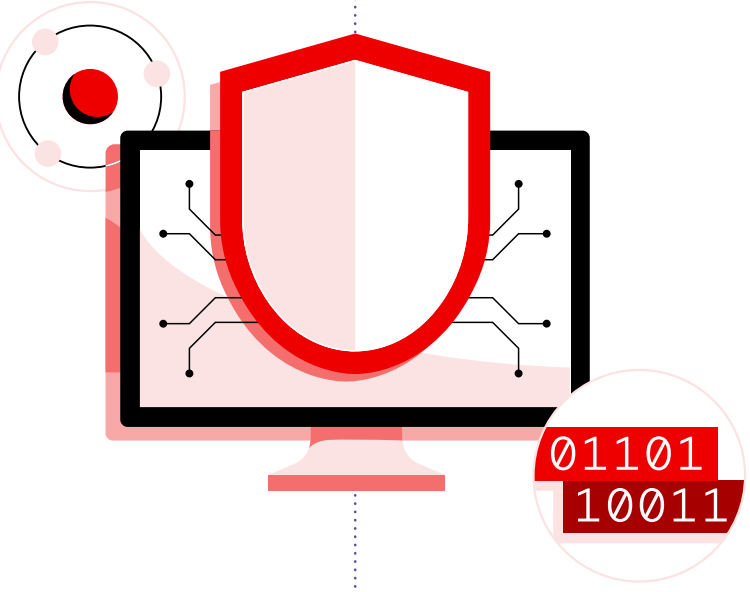
セキュリティ防護機能

成熟度の主な指標はセキュリティ防護機能、つまりクラウド環境を安全に保つために設計された組み込みの制御とプラクティス (アクセス管理から継続的な監視まで) の導入です。この調査では、防護機能の導入状況が組織によって非常に不均一であることが示されています。

特定の基本的な対策は広く実装されています。たとえば、回答者の約 4 人に 3 人が IAM ソリューションを導入しています。これは、大半の人々が強力な ID および認可制御の必要性を理解していることを示しています。しかし、より高度な、または新しいベストプラクティスの場合、理解度ははるかに低くなります。

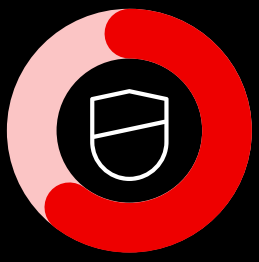
コードの整合性を管理するためにコンテナイメージの署名と検証を実装しているのはわずか**半数**であり、同様に、多くの組織はランタイム保護やポリシー施行の自動化などをまだデプロイしていません。

言い換えれば、防護機能の幅広さと一貫性が、あるべき状態ではないのです。



61%

ソフトウェア・サプライチェーンの保護に非常に自信を持っている成熟した組織の割合。成熟度の低い組織では、自信ははるかに低い。



多くのチームが一部のギャップを埋めているものの、残りのギャップはそのままにしています。包括的で意図的なガバナンスがなければ、チームはデフォルトの設定やアドホックな作業でセキュリティが守られているという誤った認識に陥りかねません。

この調査で判明した中でも注目すべき点は、明確に定義されたセキュリティ戦略を持つ組織では、このような防護機能の導入率が高く、セキュリティに対する自信がより高いことが一貫して示されていることです。成熟したプログラムでは、セキュリティを後付けではなく、プラットフォームやパイプラインの一部として扱います。

たとえば、明確な戦略があるチームでは、ソフトウェア・サプライチェーンのセキュリティツールや自動ポリシー適用などの制御を使用している割合が、まだ戦略を策定中のチームに比べてはるかに高くなります。

また、サプライチェーンの保護などの分野における自信もかなり高くなっており、成熟した組織の **61%** がソフトウェア・サプライチェーンの保護に非常に自信を持っているのに対し、成熟度の低い企業ではるかに低くなっています。

つまり、成熟度はセキュリティに具体的なメリットをもたらします。それは、一貫性の高い防護機能、可視性の向上、全体的なセキュリティポスチャの強化です。

規制への準拠

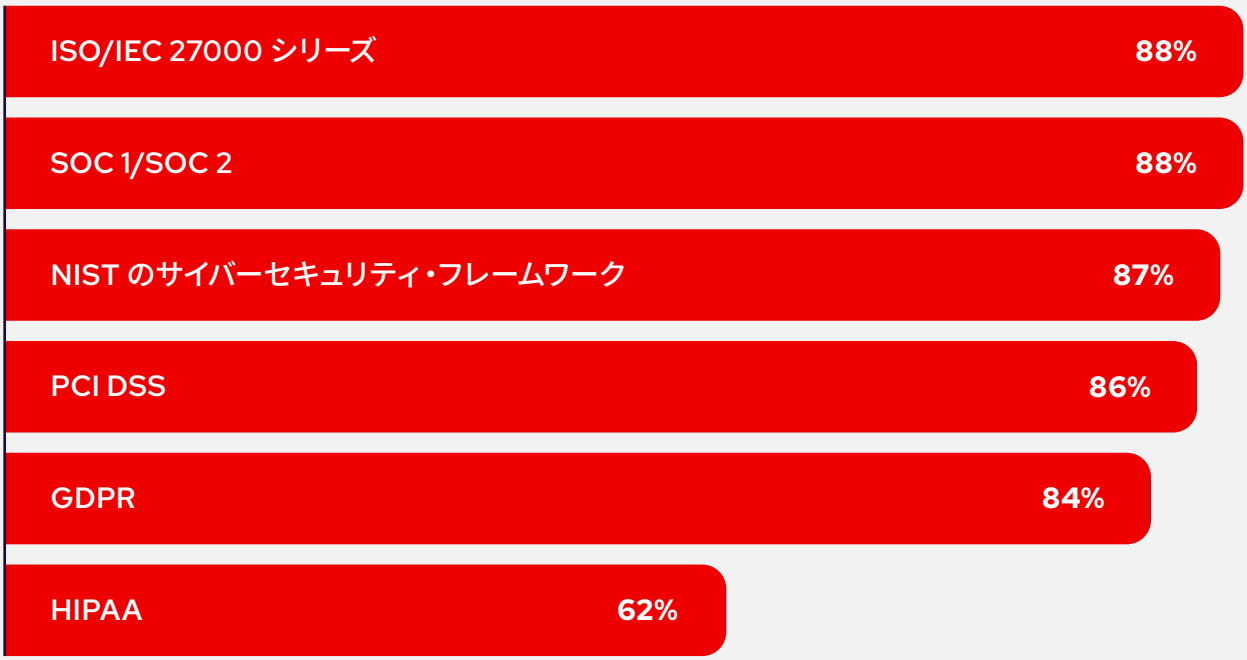


図 5.「次の各事項は、今後 12 カ月間に組織のクラウドネイティブ・セキュリティ戦略にどの程度の影響を与えると思いますか?」との質問に対する回答 (何らかの影響がある、または強い影響力を持つと回答した割合)

現在のクラウドガバナンスにおけるもう 1 つの重要な側面は、コンプライアンスと規制への準拠です。企業は、社内だけでなく外部の要件により、セキュリティを正式化しなければならないというプレッシャーを感じています。このレポートでは、新しい規制によって「ガバナンスが要件になる」ことを示しています。たとえば、回答者の **64%** は、新しい EU サイバーレジリエンス法 (CRA) が来年、クラウドネイティブ・セキュリティへの投資に影響を与えると予想しています。同様に、業界のフレームワークや標準も幅広い影響を与えています。ISO/IEC 27000 シリーズ、SOC 2、米国国立標準技術研究所 (NIST) のサイバーセキュリティ・フレームワーク、Payment Card Industry Data Security Standard (PCI-DSS)、一般データ保護規則 (GDPR) など、これらの標準がセキュリティ戦略とツールの決定に大きな影響を与えていると、あらゆる地域の多数の組織が報告しています。

それらが意味することは明らかです。共通のセキュリティ・フレームワークを早期に導入すれば、成果が得られます。

このレポートで触れられているように、共有される標準を早期に取り入れた組織は、コンプライアンスに関する「将来のコストと複雑さを軽減」できる可能性が高くなります。実際に、ガバナンスはもはや任意ではなく、無視できる項目でもありません。クラウドでビジネスを行う際の基本的な期待事項になりつつあります。

多くのチームが正しい考え方を持ち、セキュリティの重要性を認識していますが、それを構造化された戦略や全領域にわたる制御に反映しているチームは多くありません。このデータからは、より多くの組織がクラウド・セキュリティ・プログラムを正式化する必要性が読み取れます。明確な戦略を定義し、一定の防護機能を実装し、フレームワークを採用することで、プロアクティブな意図を準備が整った態勢でサポートできます。正しく実行すれば、このようなガバナンスによってレジリエンスを得ることができます。

第3章

新たな投資トレンド：自動化とサプライチェーンの重視

最初の 2 つの章で概説した課題を踏まえると、これらのギャップに対処するために組織がセキュリティへの投資を調整していることは驚くものではありません。この調査結果は、クラウドネイティブ分野におけるセキュリティ対策が統合と自動化の段階に入っているという明確な傾向を示しています。組織は、あまりにも多くの異種ツールや個別の修正にリソースをまばらに分散させるのではなく、クラウドネイティブ環境を最も効果的に強化する、数少ない優先度の高い重要な領域にリソースを集中させています。

2024 年から 2025 年にかけての投資分野の上位はすべて、ソフトウェアのライフサイクルおよびインフラストラクチャへのセキュリティの組み込みを中心としています。

特に、次の 3 つのテーマが際立っています (それぞれ、半数以上の組織が投資予定として挙げています)。

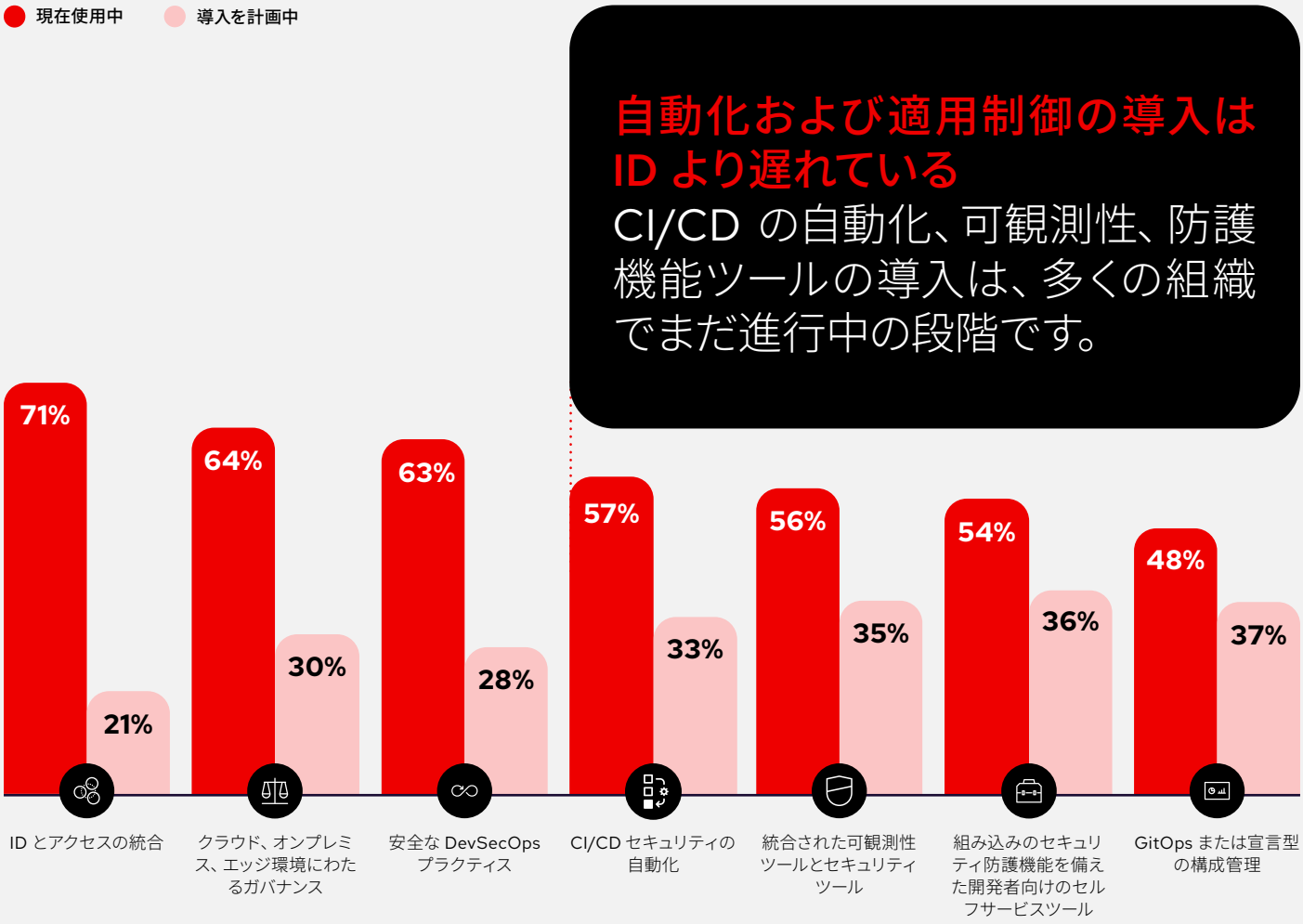


図 6. 自動化とポリシーの適用は、コア制御に遅れを取っている。このギャップにより可視性が制限され、組織は DevSecOps の成熟度のメリットを完全に実現することができない。

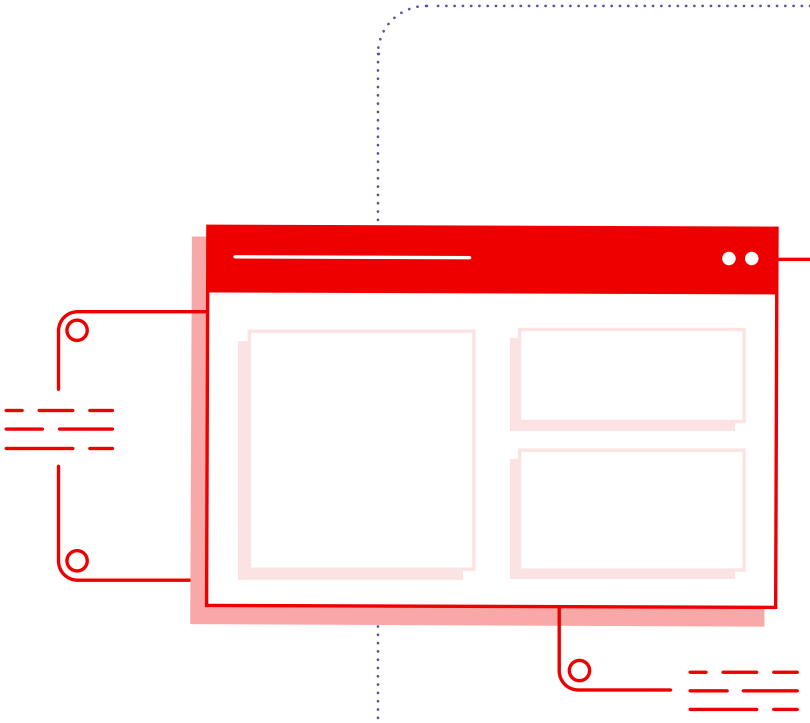
DevSecOps パイプラインの自動化

調査対象の組織の **10 社のうち 6 社**が CI/CD パイプラインと開発ワークフローへのセキュリティの統合を検討していることから、自動化は大きな焦点となるでしょう。これにはポリシー適用と環境全体でのセキュリティチェックの自動化が含まれます。これにより、セキュリティは最終段階にある手動のゲートではなく、デプロイプロセスに組み込まれた部分となります。その目標は、問題を早期に、一貫して検出することです (自動コードスキャン、構成チェック、すべてのビルドおよびデプロイにおける防護機能など)。

チームは「Security as code (コードとしてのセキュリティ)」および自動制御に移行することにより、人的ミスを削減し、安全なソフトウェア提供を迅速化することを目指しています。

ソフトウェア・サプライチェーンの保護

組織の半数以上がソフトウェア・サプライチェーンのセキュリティに多額の投資を行う予定です。これは、アプリケーションに流れ込むコードとコンポーネント (オープンソース・ライブラリ、コンテナイメージ、ビルドアーティファクトなど) は検証され、保護されなければならないという認識の高まりを表しています。依存関係の改ざんやアップストリーム・コンポーネントへの悪意のあるコードの挿入など、サプライチェーン攻撃の脅威は増大しています。ここでの目的は、コードからランタイムまでの整合性の管理です。イニシアチブには、ソフトウェア構成分析におけるツールの使用、依存関係スキャン、出所を検証するためのアーティファクト署名、セキュリティ重視のシステムなどが含まれます。



「誰もがオープンソースを使っているのでサプライチェーン攻撃が急増していますが、依存関係をスキャンしたり署名したりする人はほとんどいません」

ソフトウェアエンジニア (英国)

ランタイム保護の拡張

回答者の**半数強**が、プロダクション環境におけるランタイムセキュリティの強化も優先事項として挙げています。これは、クラスタやクラウドワークロードに、コンテナランタイムの保護、リアルタイムの脅威検出、自動応答機能などのソリューションをデプロイすることを意味します。多くのチームはすでに検出 (問題の発見) に投資しており、現在はワークロードの継続的な監視、異常検出、ランタイム時の攻撃の自己修復やブロックなど、より統合された積極的な防御へと移行しています。

プラットフォーム内に継続的な防御を組み込むことで、組織は早期段階のセキュリティゲートをすり抜けたインシデントを検出し、損害を抑制することを目指しています。

たとえば、不正なコンテナ動作やクリプトマイニング・プロセスを検出したら、即座にシャットダウンします。

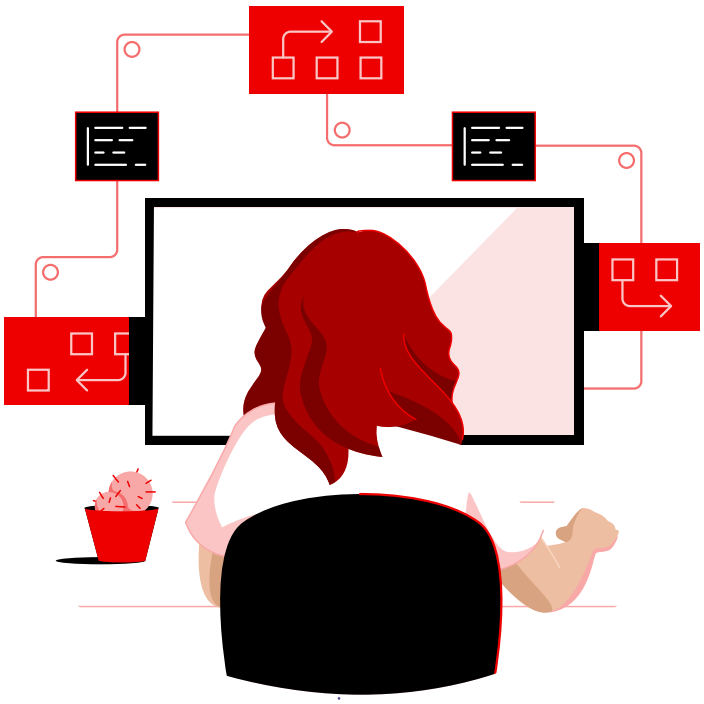
自動化と防護機能

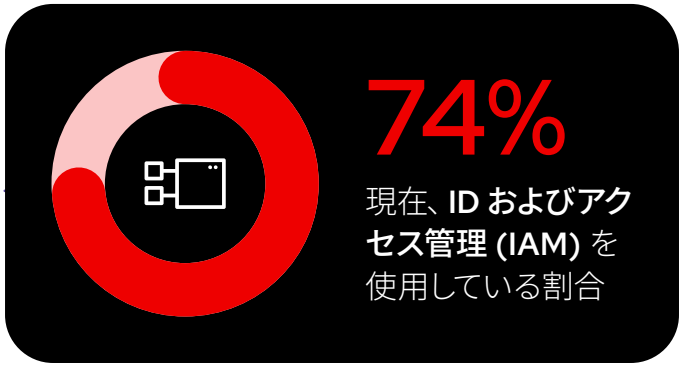
これらの特定の領域を支えるのは、より幅広い戦略です。それは、自動化と防護機能に投資して、セキュリティを継続的でスケーラブルにするというものです。

投資の選択は、成熟度評価で特定されたギャップを反映しています。

チームは、成熟したセキュリティプログラムを特徴づける機能そのものにリソースを投入しています。つまり、組織はデータから学んでいるのです。自動化の欠如と一貫性のない防護機能がセキュリティを妨げているため (第 2 章で説明)、今ではこれらの問題を解決するように予算の投入先が変化しています。個別のセキュリティツールを追加するのではなく、セキュリティを開発と運用に深く組み込むことが求められています。

このような投資の変化は、前述の外部要因 (コンプライアンスおよび侵害の恐れ) にも影響されています。CRA などの規制の導入が迫っているため、企業は後で慌てることのないよう、今、コンプライアンスを自動化してサプライチェーンを保護し、時代の先を行くことを目指しています。また、注目度の高いサプライチェーン攻撃 (依存関係のハッキングなど) がきっかけとなり、この分野への注力が急激に高まっています。企業はこの機会を利用して、単にコンプライアンスをチェックリストとして見るだけでなく、ソフトウェア部品表 (SBOM) を導入して規制要件を満たすとともに、改ざんの防止、透明性の提供、インシデント対応の効率化を実現できます。





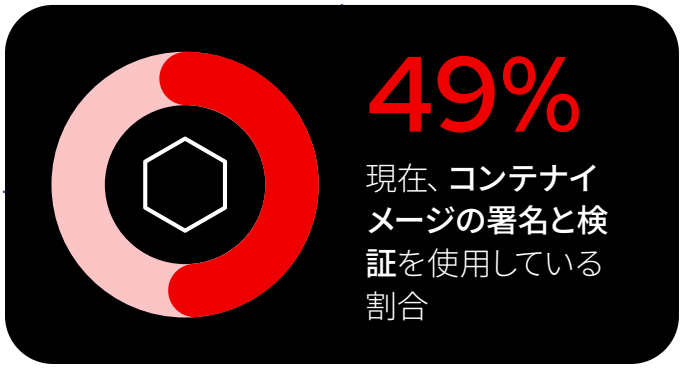


図 7. 防護機能は成熟度を定義するものだが、導入には一貫性がない。

プラットフォームの統合

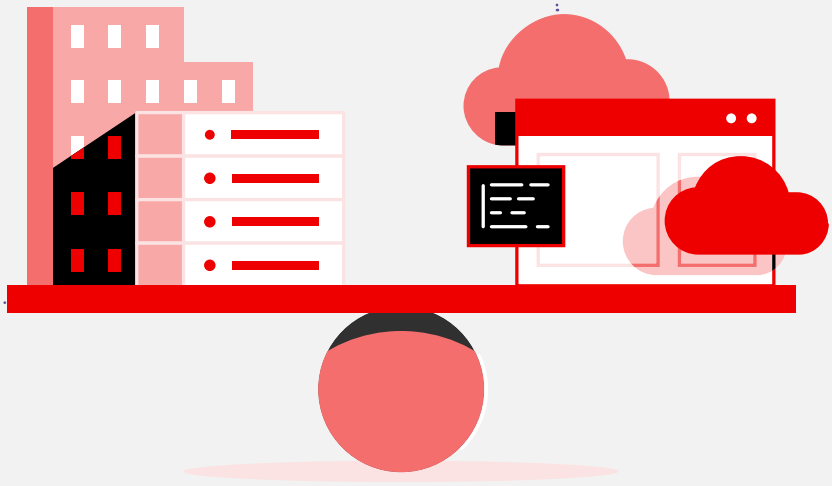
もう 1 つのトレンドはプラットフォームの統合です。多くの組織は、問題ごとに個別のツールを用意するのではなく、複数のセキュリティニーズに対応するプラットフォームや統合ソリューションを求めています。統合することにより、エンドツーエンドの可視性と制御 (コードのコミットからランタイムまで) をより最適化された方法で手に入れたいと考えています。しかし、クラウドネイティブ・アプリケーション保護プラットフォーム (CNAPP) の導入に投資していると回答した組織は、調査対象のわずか **42%** でした。

2026 年のクラウドネイティブ・セキュリティにおける投資パターンは、市場が成熟していることを示しています。

企業は基本的な事項に予算を投入しています。具体的には、構築するものにセキュリティ重点を置く取り組み (サプライチェーン)、セキュリティ重視を自動化する取り組み (DevSecOps パイプライン)、動作する場所を保護する取り組み (ランタイム防御) です。これらはアーキテクチャレベルのプロアクティブな改善であり、単なるリアクティブなアドオンではありません。今後 1 - 2 年で、平均的な組織のセキュリティツールキットの自動化が進み、さらに統合されると予測されます。こうした投資が適切に実行されれば、その結果、最終段階での予想外の事態が減少し (セキュリティチェックが組立ラインの一部になるため)、侵害の機会が少なくなります (コードの整合性とランタイム監視が向上するため)。

42%

調査対象の組織のうち、クラウドネイティブ・アプリケーション保護プラットフォーム (CNAPP) の導入に投資していると回答した割合

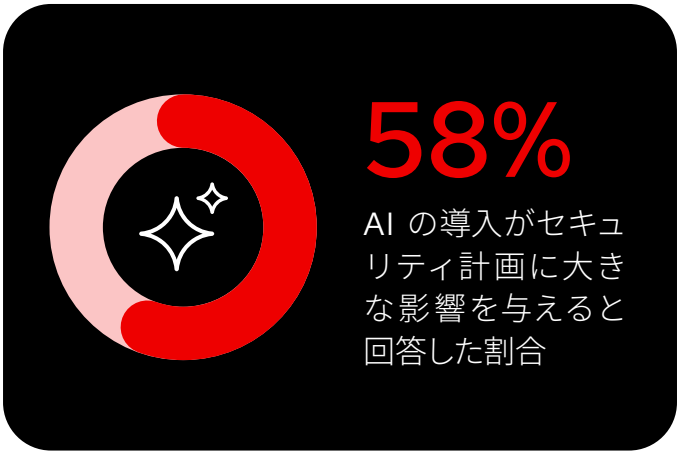


第 4 章

新たなリスクフロンティア：AI とクラウドのセキュリティ

2026 年のテクノロジーに関するレポートで、AI を取り上げないわけにはいきません。実際、AI はクラウドネイティブ環境における両刃の剣として急速に台頭してきました。AI と機械学習 (ML) は強力な機能と効率性を提供します。その一方で、セキュリティ上の新たな懸念も生じ、多くの組織は依然としてその問題に取り組んでいます。

この調査結果からは、AI に対する熱意が高い一方で、AI に関するセキュリティガバナンスは危険なほど遅れを取っていることがわかります。



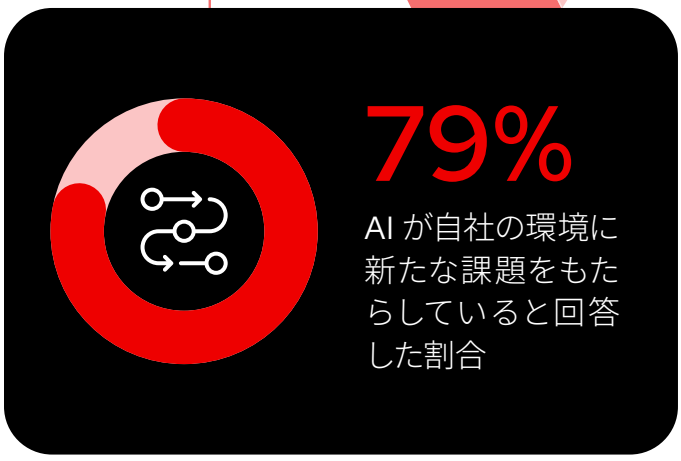


図 8. AI によってイノベーションも攻撃対象領域も同様に拡大する。

あらゆる人にとっての懸念事項

まず、ほぼ誰もが AI 関連のリスクを懸念しています。**96%** と圧倒的多数の回答者が、自社のクラウド環境での生成 AI の使用に懸念があると回答しています。これらの懸念は抽象的なものではありません。実際に観察された問題や不確実性から発生しています。AI 関連のセキュリティ上の懸念として最も多かったのは、機密データの漏洩、シャドー AI ツールの存在 (従業員またはチームが AI SaaS ツールまたは API を承認を得ずに使用する)、サードパーティの AI サービスとの統合による攻撃対象領域の拡大などです。

つまり、組織は AI の統合がもたらす未知のリスクを恐れているのです。

たとえば、エンジニアが誤ってプロプライエタリーなコードやデータを生成 AI サービスに入力してしまうと、データ漏洩のリスクが生じます。あるいは、デプロイした AI ベースのアプリケーションに隠れた脆弱性がある、または適切な監視がなければセキュリティに影響を与える決定を下してしまうこともあります。また、AI システムが悪用され、もっともらしいフィッシングコンテンツが生成されたり、従来のセキュリティツールでは検知できないロジックが導入されたりすることについての懸念もあります。

96%

自社のクラウド環境での生成 AI の使用に懸念があると回答した割合

「AI は見過ごされているリスクです。自信を持って導入できるように、規制を適用し、安全性を確保する必要があります」

IT 運用責任者 (英国)

強力なガバナンスはいまだに実現が困難

このような懸念は広く共有されていますが、ほとんどの企業は AI の使用に対する強力なガバナンスをまだ実装していません。データによると、調査対象の企業の 59% は、AI 関連の文書化されたセキュリティポリシーやガイドラインを持っていませんでした。

言い換えれば、開発者や従業員がどのようにして AI ツールを安全に使用すべきか、AI モデルをどのように精査すべきか、データをどのように処理すべきかについて、ルールを規定している組織は半数に満たないということです。

ガイドライン作成の初期段階にある企業や、チーム固有のアドホックなルールに依存している企業もありますが、全体的に見ると、AI ガバナンスは現時点では、これから開拓していく分野であることがわかります。この正式なポリシーの欠如は、特に AI 導入のスピードを考慮すると、ガバナンスに関する重大なギャップです。

AI の導入と AI の管理の不一致は深刻な問題につながる可能性があります。企業は AI の利点を認識していますが、AI の使用に防護機能を設けていなければ、意図せず新たな脆弱性やコンプライアンス上の課題が生じてしまう可能性があります。たとえば、AI サービスによってセキュリティバグをもたらされた場合、誰が説明責任を負うのでしょうか？AI が生成した意思決定や出力がセキュリティに与える影響をどのように監視しますか？これらの質問は、AI ポリシーを持たない組織では解決されないままになります。

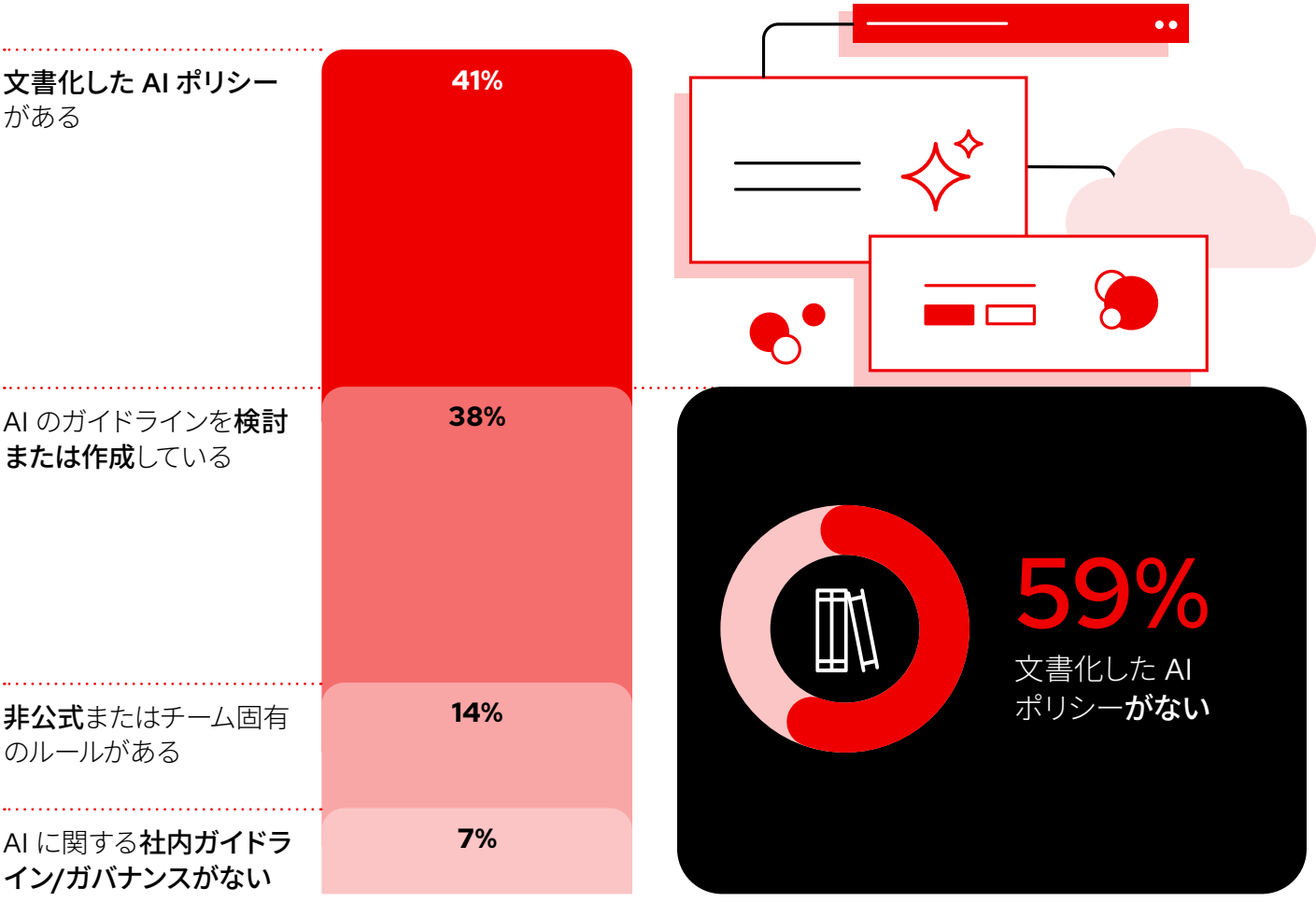


図 9. AI ポリシーの導入は遅れており、標準化された AI ガイドラインを施行している組織は半数未満。

AI がリスクを倍増させる

もう 1 つの側面は、AI によって既存のセキュリティ問題が増幅される可能性があることです。適切な制御がなければ、AI ツールによって ID およびアクセスのリスク、CI/CD パイプラインのリスク、サプライチェーンの問題がさらに悪化します。これらはまさに前述した領域です。たとえば、制御されていない AI スクリプトがクラウドリソースをスピンアップしたり、通常のプロセス外で構成を変更したりする可能性があります (シャドー IT のシナリオ)。

AI に関する懸念のトップ (データ漏洩、シャドーツール、サードパーティの AI) は、不十分な可視性と制御の断片化から生じています。

共有される所有権や、アプリケーションに伴うポリシーがなければ、これらのリスクは導入とともに拡大します。簡単に言うと、AI を含めるようにガバナンスのフレームワークを拡張しなければ、AI の使用が増えるほど混乱や危険にさらされる可能性が高まります。

明るい兆しもある

すべてが悲観的というわけではなく、対策を講じている組織もあります。多くの回答者が現在 AI ガイドラインを検討中または作成中であると回答しており、一部の回答者は AI に関する社内委員会があったり、監視を行ったりしていると報告しています。認識することがその最初のステップであり、ほぼ普遍的な懸念事項は、AI の不正な使用への対処方法についてリーダー陣との話し合いを余儀なくされることです。外部からの指導の要求もあります。政府や業界団体は AI 規制 (EU が提案した AI 法など) の議論を開始しており、最終的にはデータ保護法と同様の要件を課す可能性があります。しかし企業はそれを待ってはいられません。プロアクティブに対応する必要があります。

AI はクラウドネイティブ・セキュリティにおけるリスクの新たな最前線であり、ほとんどの組織はその対処を始めたばかりです。 2026 年は、この分野での急速な進化が見られることでしょう。DevOps には AI を活用したツールや機能が増えていき、その一方で、それらに対するガバナンスの確立に奮闘することになります。

重要なポイントは、ガバナンスの速度がイノベーションの速度に追いつく必要があるということです。

組織は、クラウドにおける AI を、他の強力なテクノロジーを扱うのと同じ厳密さで、明確なポリシー、監視、制御をもって扱う必要があります。そうしないと、ビジネスを加速するはずの AI が、次の大きなセキュリティインシデントの原因になる可能性があります。

> 「AI ガバナンスは重要であると考えており、当社では明確なルールの導入に取り組んでいます」
>
> ソフトウェア・エンジニアリング責任者
> (ニュージーランド)

まとめ

データに基づく 2026 年の推奨事項

この調査結果から、組織がすぐに行動を起こす必要があるいくつかの領域が明らかになります。このレポートの知見に基づき、クラウドネイティブ・セキュリティの成果を向上させるための主な推奨事項は以下のとおりです。

61%

定義されたクラウドネイティブ・セキュリティ戦略を持っていない企業の割合

正式なクラウドセキュリティ戦略と成熟度ロードマップを策定する

組織に定義済みのクラウドネイティブ・セキュリティ戦略がない場合 (調査対象の企業の **61%** が該当)、戦略の構築を優先しましょう。

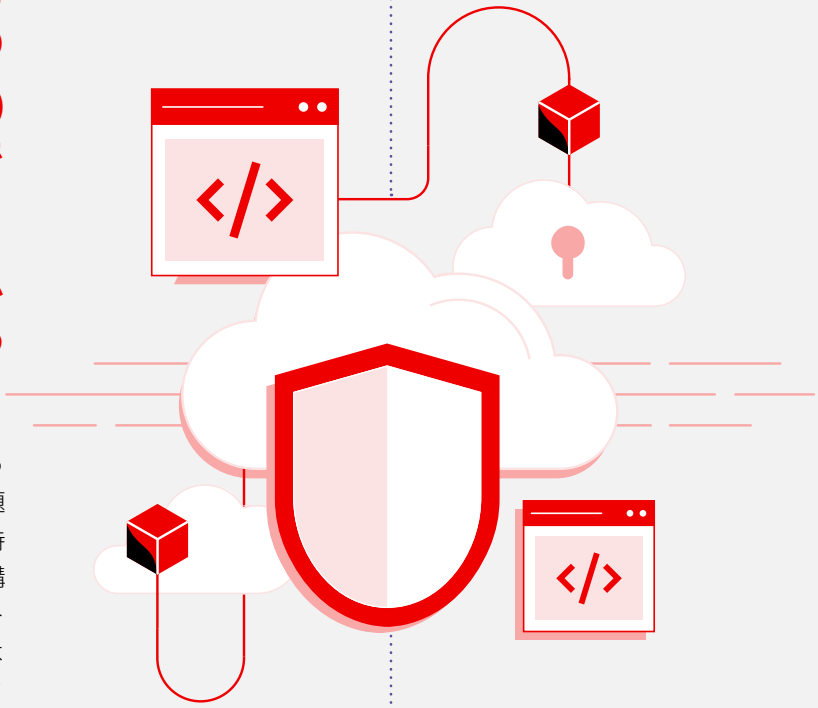
クラウドセキュリティ成熟度モデルを使用した明確な戦略が、セキュリティポスチャをリアクティブからプロアクティブへと変える構造化された道筋となります。

これにより、セキュリティの取り組みがビジネス目標に沿ったものとなり、すべてのチームがその計画について常に把握することができます。データによると、明確に定義された戦略を持つ企業は、セキュリティプログラムに対する自信と一貫性が大幅に高くなっています。今、戦略とアーキテクチャに時間を費やしておけば、後になってその場しのぎの一時的な処置で対応する事態を防ぐことができます。

開発ライフサイクルにセキュリティ防護機能と自動化を組み込む

クラウドセキュリティで成功を収めている組織は、クラウドセキュリティを追加のものとしてではなく、プラットフォームとパイプラインの不可欠な要素として扱っています。

チームは、セキュリティ重視のコーディング標準やコミット前のチェック、コマンドラインでのIaC (Infrastructure as Code) スキャン、プロダクション環境での継続的なランタイム監視など、あらゆる段階でプラットフォームの防護機能を実装する必要があります。



可能な限り、これらの制御を自動化することを目指しましょう (Policy as Code、自動脆弱性スキャンなど)。自動化により、問題を早期に発見できるだけでなく、広範囲にわたって一貫性を維持できます。これにより、多くのインシデントの原因となる頻繁な構成ミスや人的ミスに直接対処できます。基本的には、「デフォルトでセキュリティ保護する」を標準にすることです。データが示すように、組織は制御をワークフローに組み込むことで、セキュリティを希望する状態からセキュリティを実行する状態へと移行する必要があります。CNAPP の導入 (組織の **42%** が優先事項としている) など、自動化された統合セキュリティ・プラットフォームを使用すると、物事が見落とされる可能性が低くなります。この転換には、多くの場合 DevOps またはプラットフォーム・エンジニアリング・チームが遂行する組織的な権限を定義し、開発者に摩擦をもたらすことなくセキュリティを拡張することが必要です。

ソフトウェア・サプライチェーンの整合性を優先する

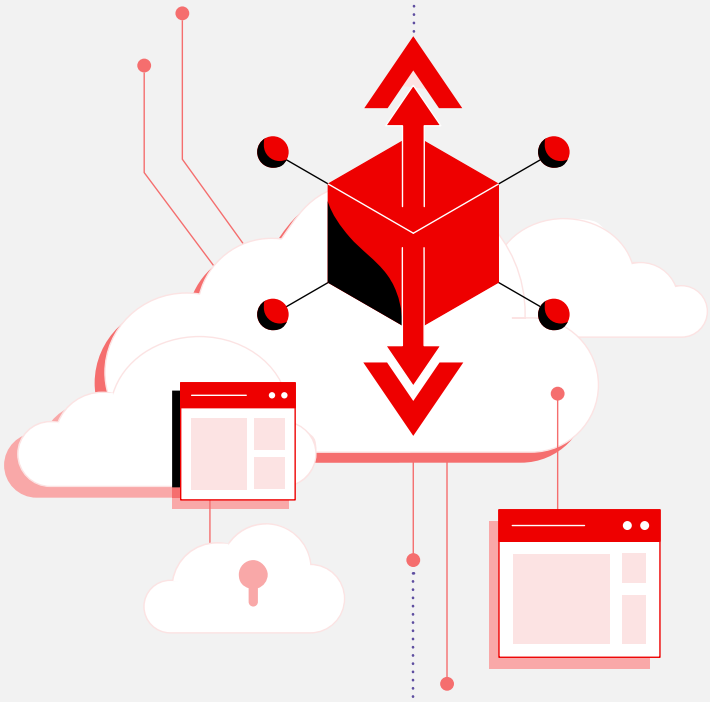
サプライチェーンを保護するには、すべてのコンテナイメージとパッケージに対して、依存関係スキャン、SBOM、追跡、イメージ署名などの対策を実施します。

現在、イメージ署名などのサプライチェーンのセキュリティ手法を実施している組織は約半数に過ぎません。これは、多くの組織がリスクにさらされていることを意味します。どのチームもオープンソース・コンポーネントを使用しているため、それらが信頼できるものかを検証してください。出所の確認 (署名済みアーティファクトの要求など) を実施し、ツールを使用して、脆弱なコンポーネントや悪意のあるコンポーネントがプロダクション環境に到達する前に検出します。ある回答者は、オープンソースを使用するのは一般的であるものの「依存関係をスキャンしたり署名したりする人はほとんどいない」と述べています。貴社がこれに当てはまらないようにしてください。ソフトウェア・サプライチェーンを強化することで、拡大し続ける攻撃経路を遮断し、構築してデプロイするものがアップストリームで改ざんされていないことを確認します。

統一された可視性とライフサイクル全体のフィードバックループによって成熟度のギャップを埋める

孤立したチーム構造で運用するのではなく、チーム間で可観測性とセキュリティデータを統一します。

この統一は、ライフサイクル全体にわたるセキュリティのフィードバックループを確立するために不可欠です。企業は DevSecOps の自動化 (**60%**) とランタイム保護の拡張 (**54%**) の両方に多額の投資を行っていますが、これらの取り組みはつながっていなければなりません。成熟したセキュリティでは、ランタイムの脅威検出から得られた知見を使用して、開発およびビルドプロセスの早い段階で最も重大な脆弱性に優先順位を付けて修正する必要があります。ビルド/デプロイからランタイム、インテリジェンスのフィードバックまで、ライフサイクル全体にわたってセキュリティを拡張することで、一貫した防護機能を確保し、安全なソフトウェア提供を加速させ、DevOps ユーザーをセキュリティユーザーに変えることができます。



ソブリンクラウドとエッジデプロイメントによるハイブリッドクラウドのセキュリティポスチャ

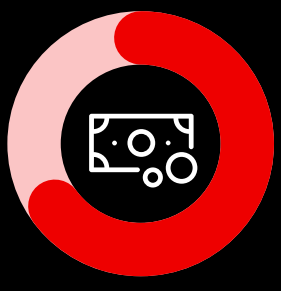
クラウド、オンプレミスのデータセンター、エッジ全体で機能するセキュリティ制御を導入します。

クラウドネイティブ・セキュリティ・ツールは、オフライン、ソブリン、またはデータレジデンシー環境でも一貫して動作できる必要があります。ワークロードがパブリッククラウド、プライベートクラウド、オンプレミスのどこにあっても、ポリシーを一律に適用するツールを導入します。分散ワークロードのためのエッジセキュリティは、**38%** の組織にとって優先的な投資対象となっています。セキュリティツールは、中央のセキュリティチームへの継続的な高帯域幅の接続がなくてもこれらの遠隔環境を保護できる、軽量で自律的なものでなければなりません。

早期にセキュリティ・フレームワークおよびコンプライアンスに適合する

監査や規制によって強制されるのを待つのではなく、自社のビジネスに関連する業界セキュリティ・フレームワークをプロアクティブに導入しましょう。

調査によると、共通の標準に準拠する企業は長期的な複雑さを軽減できることがわかっています。ベストプラクティスのフレームワークを採用することで、ID、アクセス、監視、インシデント対応などの領域をカバーし、クラウド環境を強化するための構造化されたチェックリストが作成されます。また、先進的な規制への備えにもなります。たとえば、EU サイバーレジリエンス法の影響を受ける可能性がある場合は、今すぐその要件の評価を始めましょう。今回の調査によると、このことが 2026 年の投資に影響を与えたと回答している組織は **64%** でした。コンプライアンスを戦略の一部に組み込むことで、最終段階で慌てるような事態を回避し、セキュリティとガバナンスを統一した状態に保つことができます。まとめると、コンプライアンスを上限ではなく下限として扱い、セキュリティの基礎を強化するために使用しましょう。



64%

このことが 2026 年の投資に影響を与えたと回答した組織の割合

堅牢な AI ガバナンスとポリシーを実装

クラウドアプリケーションおよび DevOps への AI の急速な導入とそれに伴うリスクを考慮すると、組織はできるだけ早く明確な AI 使用ポリシーを導入し、監視を行う必要があります。

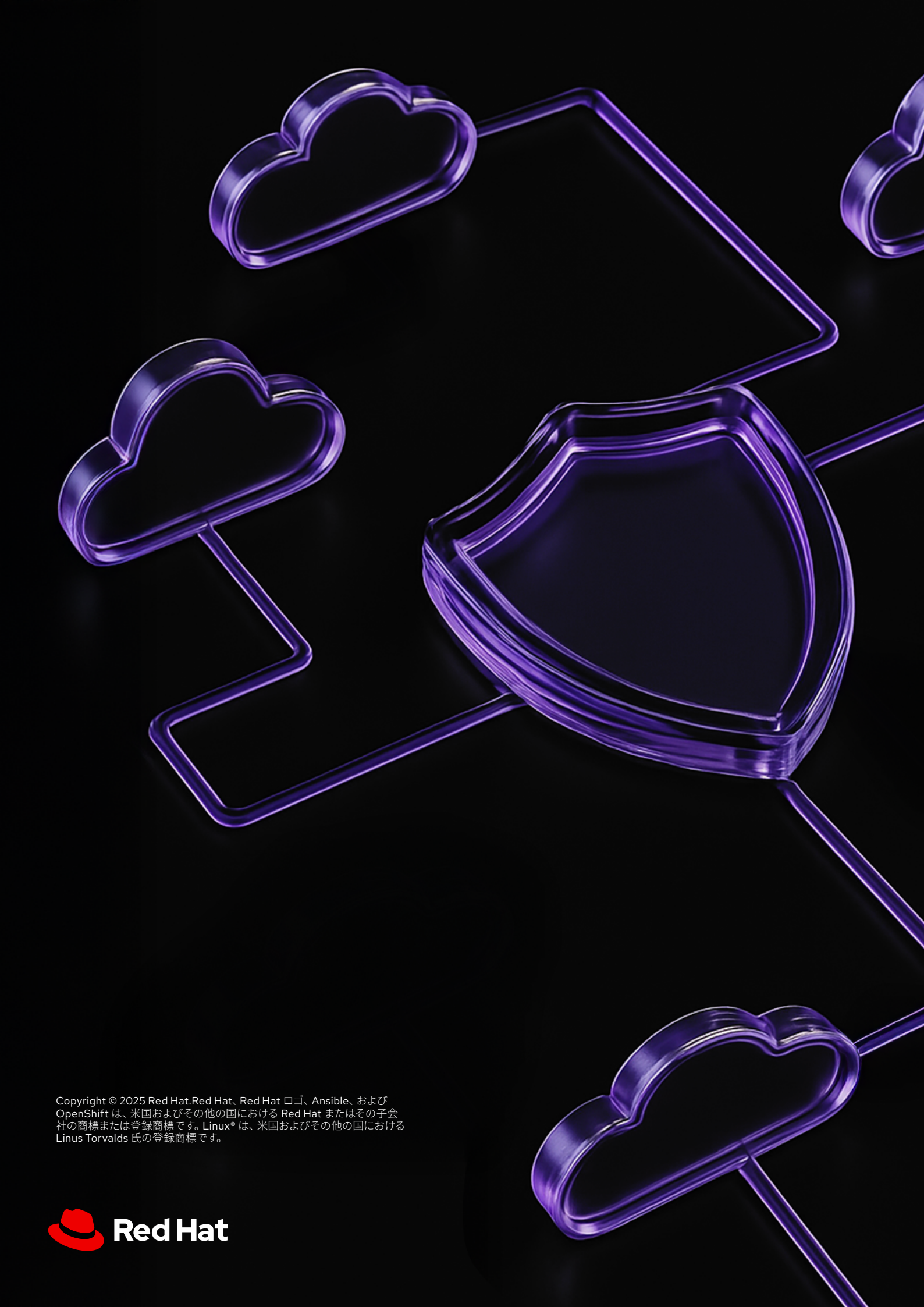
現在、調査対象の企業のほぼ **60%** に AI ガバナンスがないという事実があり、この大きなギャップを解消する必要があります。部門横断的なチーム (セキュリティ、IT、データサイエンス、法務) を招集して、許容される AI の使用に関するガイドラインを作成します。これには、機密データを AI サービスでどのように使用できるか、または使用できないか、AI ベースのソリューションをデプロイするために必要な承認、AI の出力にセキュリティや倫理上の問題がないかどうかを監視する方法などが含まれます。これらのポリシーについて開発者やエンジニアを教育します。さらに、機密データが外部の AI アプリケーション・プログラミング・インタフェース (API) にエクスポートされないようにするためのデータのタグ付けや、AI 使用時の異常な動作の監視など、AI に関する技術的制御を検討してください。

これらの推奨事項 (戦略の策定、防護機能/自動化の組み込み、サプライチェーンのセキュリティ保護、標準への準拠、AI のガバナンス) を実行することで、組織はクラウドネイティブのセキュリティポスチャを劇的に改善できる態勢が整います。

2026 年の見通しでは、脅威が進化し続けることだけでなく、防御に役立つデータがこれまで以上に増えていることも示されています。

60%

AI に関するガバナンスがないと回答した企業の割合



Red Hat