Enterprise Strategy Group by TechTarget

ホワイトペーパー

ハイブリッド環境とマルチクラウド環境にまたがるセキュリティでビジネスの成長を加速

セキュリティの効率的な管理によりデジタル トランスフォーメーションを促進

Enterprise Strategy Group サイバーセキュリティ担当ディレクタ
Melinda Marks

2023 年 10 月

目次

はじめに

今日の組織は、デジタル トランスフォーメーションによって生産性を最適化し競争優位を獲得するよう迫られています。その手段としてアプリケーションをクラウドサービスに移行する動きが拡大しています。サーバーやハードウェアのプロビジョニングに煩わされることなくソフトウェア開発を迅速化できるからです。また、従業員と成長するチームが柔軟に働けるよう、テレワークをサポートする必要もあります。デジタル トランスフォーメーションの過程で、アプリケーションがハイブリッド環境とマルチクラウド環境にまたがって分散化されるだけでなく、分散して働くワークフォースをサポートする必要性も生じます。その結果、組織はますます複雑化する IT に直面することになります。

今新たに求められているのは、さまざまな環境にまたがってアプリケーションをサポートし、ビジネスの成長を全面的に後押しする拡張性のあるセキュリティです。セキュリティは、それぞれが独自のプラットフォーム アーキテクチャ、特徴、機能を持つ多様化した環境にまたがって、アプリケーションとユーザーをサポートする必要があります。さらに、セキュリティチームは、本業の成長や企業買収など変化を続けるビジネスニーズに応えて柔軟に役割を拡大できる必要があります。

セキュリティチームは、拡大を続けるクラウドサービスの利用やクラウドネイティブ開発に歩調を合わせてセキュリティ戦略を見直していくなかで、数多くの課題に直面しています。短期間のうちに拡大と縮小を繰り返すクラウドのリソースやインフラストラクチャを可視化することが困難なためです。また、開発者の生産性の向上に追従していくことも、アクセス件数や権限設定が急増するなかで脅威にさらされるのを防ぐことも困難です。

多くの組織が複数のセキュリティソリューションやプラットフォームを使用してこれらの課題に対処しようとしていますが、頻繁にセキュリティインシデントに直面しています。その原因は設定不備やアクセスに対するオーバープロビジョニングといったありふれたものです。複数のツールを使用すると死角やギャップができ、可視性の問題を引き起こします。さらに、ツールがセキュリティの脆弱性を警告したとしても、重要な問題を優先できないためにセキュリティチームによる修復が間に合わず、アプリケーションを攻撃から防御できないことも少なくありません。資産とアプリケーションが複数のクラウド環境にまたがって急増しているため、このような課題は増える一方です。

セキュリティチームには、ワークロードのモビリティをサポートする広範な可視性とアクセス保護を提供し、環境全体にわたってアプリケーションを保護する効果的な戦略が必要です。ビジネスの急速な成長とそれによって生じたハイブリッド環境やマルチクラウド環境に対するニーズに柔軟に応えられる効果的なアプリケーション セキュリティが必要です。このホワイトペーパーではこれを実現するためのアプローチに欠かせない要素を説明します。

セキュリティチームは、そのスキルセットに関係なく、資産を完全に可視化して脆弱性を効果的に修復し、ゼロトラストアプローチによって環境のいたるところで発生する攻撃からアプリケーションを保護する必要があります。組織はこれをサポートする柔軟なアプローチを見出さなければなりません。このようなアプローチの要素としては、セキュリティ問題の迅速な検出に加え、リスクの軽減に最も効果のあるアクションを優先するためのコンテキストに基づくインサイトと脅威インテリジェンスが挙げられます。また、資産を保護するためのポリシーを設定する集中化されたシンプルな手段も要素の 1 つです。

セキュリティチームは、相互接続された動的なマルチクラウド環境とハイブリッド環境にまたがってアプリケーションとアクセスに対処するアプローチを採用することで、リソースと運用を最適化できます。その結果、リスクの効果的な管理と、脅威への迅速な対応が可能になります。これにより、効率的に役割を拡大し、迅速化した開発とビジネスの成長をサポートできるようになります。

デジタル トランスフォーメーションに関連するセキュリティの課題

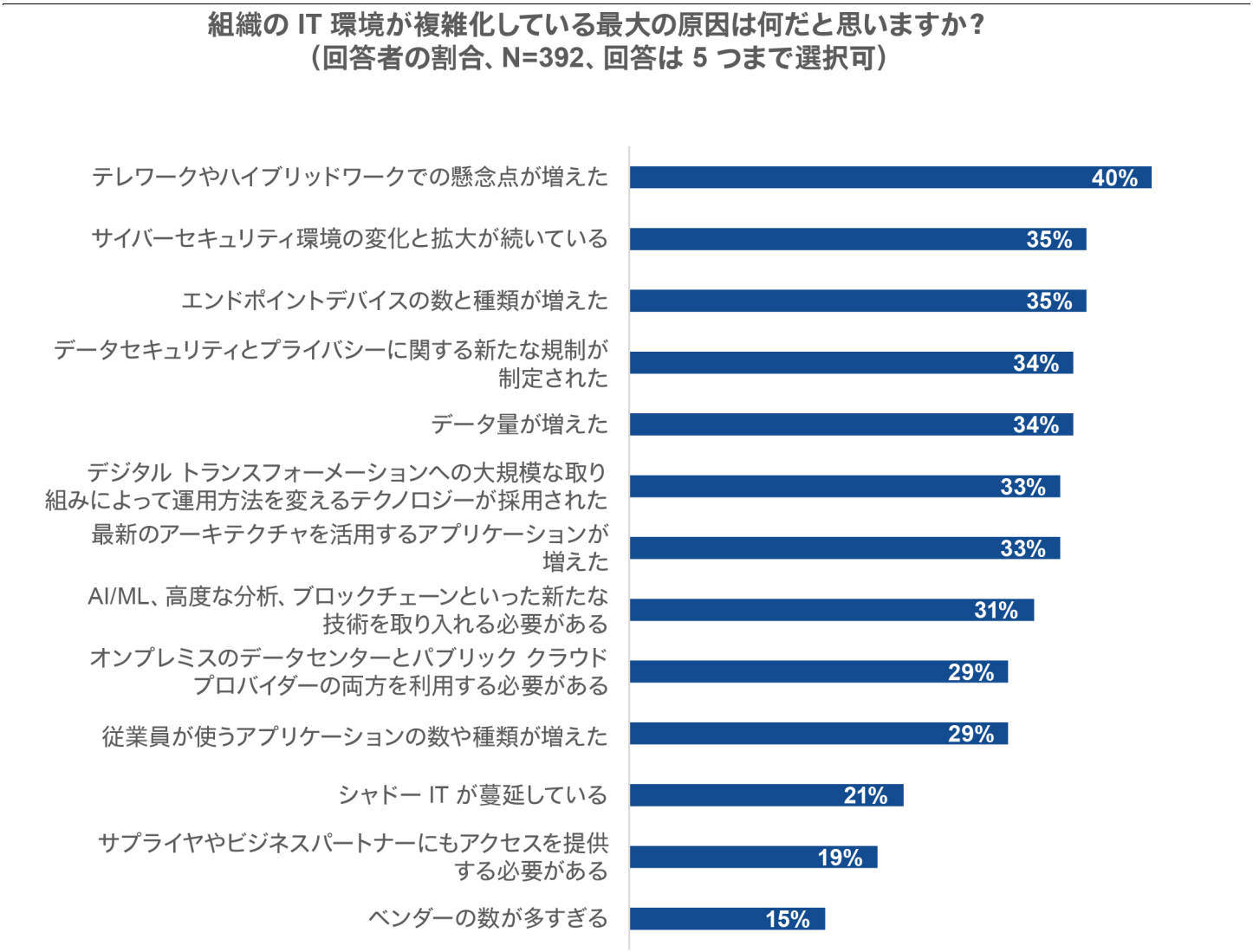
TechTarget の Enterprise Strategy Group が実施した調査によると、最近の絶え間なく続く開発がセキュリティチームに課題をもたらしています。IT 環境の複雑化、開発者の生産性向上に伴うクラウドネイティブ アプリケーションの急増、複数のパブリッククラウドがあるために生じた可視性のギャップがその例です。これらによってさまざまなセキュリティインシデントが発生しています。セキュリティチームには、これらの課題に対処してビジネスを成長させながらさまざまな環境でアプリケーションを安全に保護できる、特別なスキルに依存しない効果的な戦略が必要です。

IT が複雑化した

デジタル トランスフォーメーションによって生産性を高め、競争上の優位性を獲得するにつれて、IT とセキュリティは複雑さを増し、新たな要求を受けるようになっています。Enterprise Strategy Group が実施した調査によると、半数を超える組織（53%）が、自組織の IT 環境が 2 年前と比べて複雑になっている、または大幅に複雑になっていると回答しています。[1] 複雑さが増した最大の原因としてテレワークやハイブリッドワークの増加を挙げた組織が最も多くなっています（40%）。サイバーセキュリティ環境の変化（35%）、エンドポイントデバイスの数と種類の増加（35%）、データセキュリティとプライバシーに関する新たな規制（34%）、データ量の増加（34%）がこれに続きます。さらに組織の 29% がオンプレミスのデータセンターとパブリック クラウド プロバイダーの両方の使用が必要になったことを挙げています（図 1 を参照）。

[1] 『Research Report: *2023 Technology Spending Intentions Survey*』、Enterprise Strategy Group、2022 年 11 月

図 1. IT が複雑化している原因



出典：Enterprise Strategy Group（TechTarget の一部門）

このようにさまざまな領域で増加した複雑さに直面しながらも成長と拡大を支える効果的な方法があります。

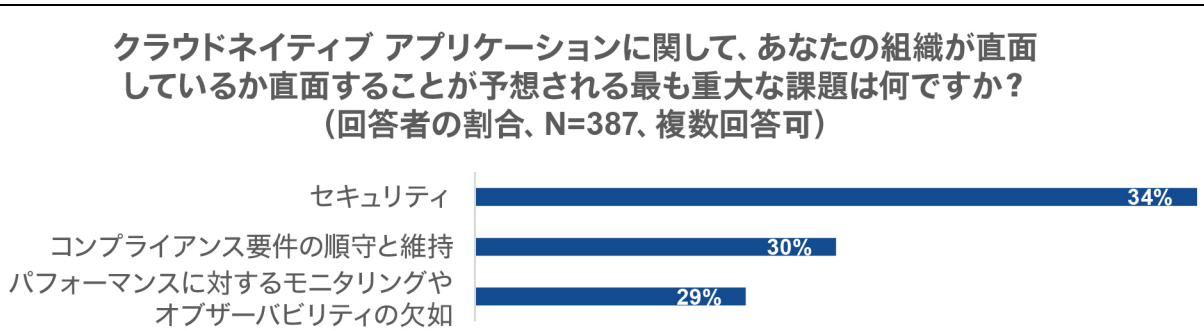
アプリケーションのクラウド環境への移行が増加している

組織は今、パブリック クラウド インフラストラクチャの活用を拡大することで、クラウドネイティブ開発による生産性の向上とイノベーションの加速を目指しています。基盤となるインフラストラクチャやメンテナンスについて心配することなく、クラウド サービス プロバイダー（CSP）の従量制課金モデルを利用することで規模の経済のメリットを享受できます。

Enterprise Strategy Group が実施したアプリケーション インフラストラクチャの刷新に関するトレンド調査によると、調査対象組織の 88% がパブリック クラウド インフラストラクチャやそのプラットフォームで実稼働ワークロードを実行しています。また組織は、実稼働ワークロードのクラウド移行を拡大させています。[2] さらに、この調査によると、アプリケーションをクラウドに移行した組織は、俊敏性の向上、インフラストラクチャコストの削減、展開の迅速化など、多くのメリットを実現しています。

クラウドの活用によって DevOps も可能になります。つまり、運用を「シフトレフト」することで、IT チームや運用チームによるサーバーのプロビジョニングを待つことなく、開発者が自分自身のインフラストラクチャをプロビジョニングできるようになります。開発者が効率的に業務を進めることで、従来のアプリケーション開発手法に比べて短期間で価値を実現できるようになります。ただし、クラウド活用によってソフトウェア開発の生産性が向上する一方で、クラウドネイティブ アプリケーションに関するセキュリティとコンプライアンスの課題が発生します。

図 2. クラウドネイティブ アプリケーションに関して組織が直面している課題の上位 3 つ



出典：Enterprise Strategy Group（TechTarget の一部門）

組織には、セキュリティリスクを管理する効果的な方法が必要です。これがなければ、クラウドネイティブ開発に移行することでリリースの規模を拡大し提供を迅速化するというビジネスニーズに応えることができません。効率を最適化してこの拡大と成長を支えられるセキュリティチームは、ビジネス成果の向上に向けて強力な役割を果たすことができます。開発者の生産性を向上させイノベーションを加速させる新しいテクノロジーの導入を妨げることはありません。

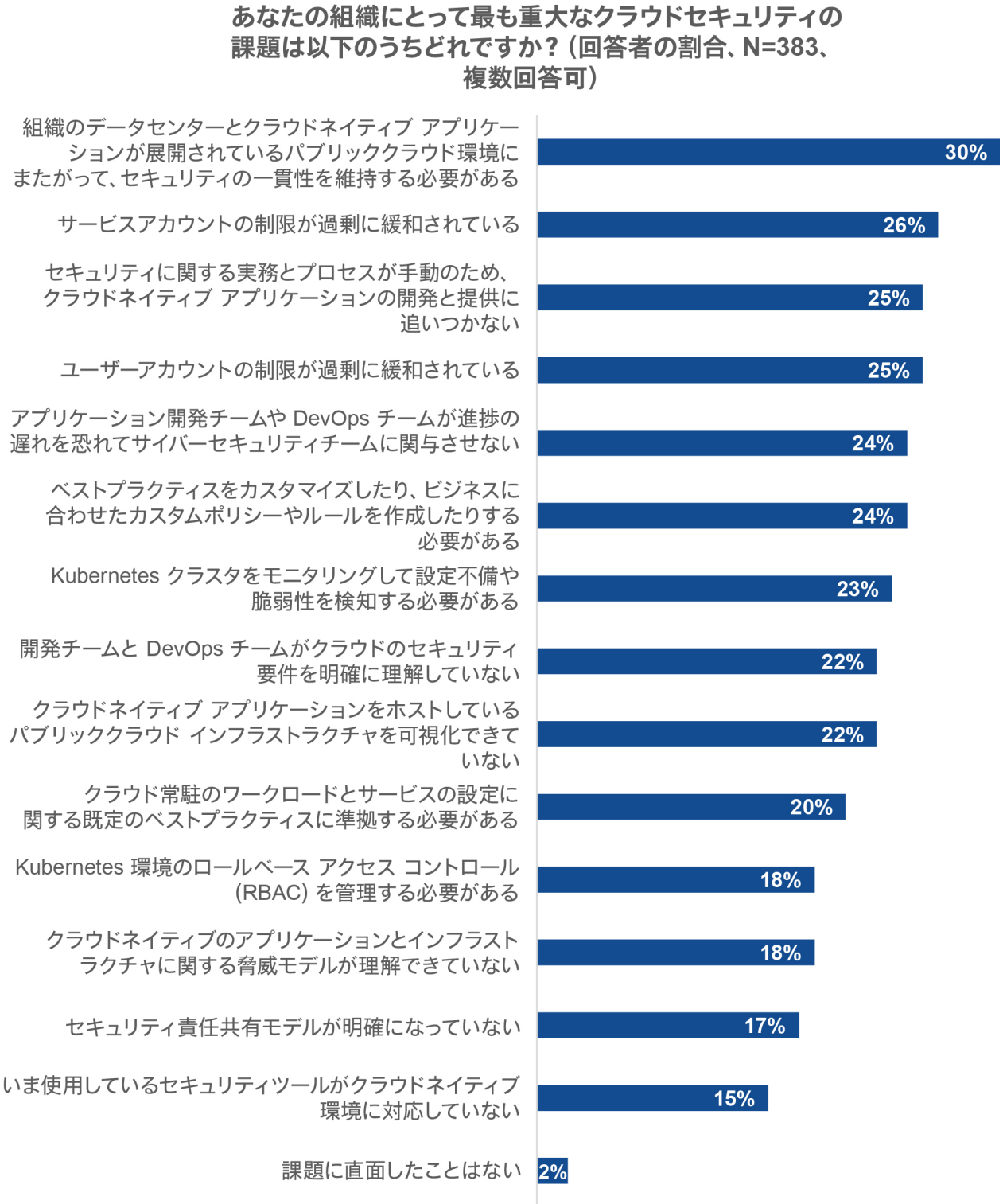
[2] 出典：『ESG Research Report: *Cloud-native Applications*』、Enterprise Strategy Group、2022 年 5 月

マルチクラウド環境全体のセキュリティ態勢を管理する

これに加えて、クラウド環境を用いて成長を支えるためには、セキュリティチームがマルチクラウド環境をサポートする必要があります。クラウド環境におけるセキュリティ態勢の管理に関する Enterprise Strategy Group の調査によると、ほとんどの組織（94%）が複数のクラウド インフラストラクチャのサービスプロバイダーを使用していて、そのうち大多数（69%）が 3 つ以上のサービスプロバイダーを使用しています。[3] 大多数の組織（68%）が、クラウド環境のセキュリティ態勢を管理する堅牢なソリューションを導入していると回答する一方で、さまざまな課題に言及しています。主に、環境とチームの全体的なリスクを効果的に管理するために必要な可視性と管理の確保に関するもので、データセンターとクラウド環境にまたがる一貫したセキュリティの実現がその一例です（30% が回答）。その他の課題としては、サービスアカウントとユーザーアカウントの制限が過剰に緩和されている（それぞれ 25% と 26%）、セキュリティに関する実務とプロセスが手動のためクラウドネイティブ アプリケーションの提供に追いつかない（25%）、開発プロセスへの参画とその管理ができていない（24%）、パブリック クラウド インフラストラクチャが可視化できていない（22%）、クラウドネイティブの脅威に対する理解が不十分（18%）などがあります（図 3 を参照）。[4]

[3] 出典：『Research Report: *Cloud Entitlements and Posture Management Trends*』、Enterprise Strategy Group、2023 年 4 月
[4] 同上

図 3. 組織にとって最も重大なクラウドセキュリティの課題



出典：Enterprise Strategy Group（TechTarget の一部門）

組織が求めているのは、これらの課題に対処しさまざまな環境にまたがってアプリケーションを保護する効果的なアプローチです。これを実現するには、アプリケーションが別々の環境ではなく相互接続された動的な環境にあるかのように包括的に見る手段を確立し、アプリケーションを稼働環境に関係なく可視化して管理できるようにする必要があります。マルチクラウド環境とハイブリッド環境から情報を集約することでセキュリティ運用の効率が向上し、リスクの軽減と脅威への迅速な対応が可能になります。これがクラウドの利用を拡大しながらセキュリティを拡張して成長するビジネスを支える唯一の方法です。

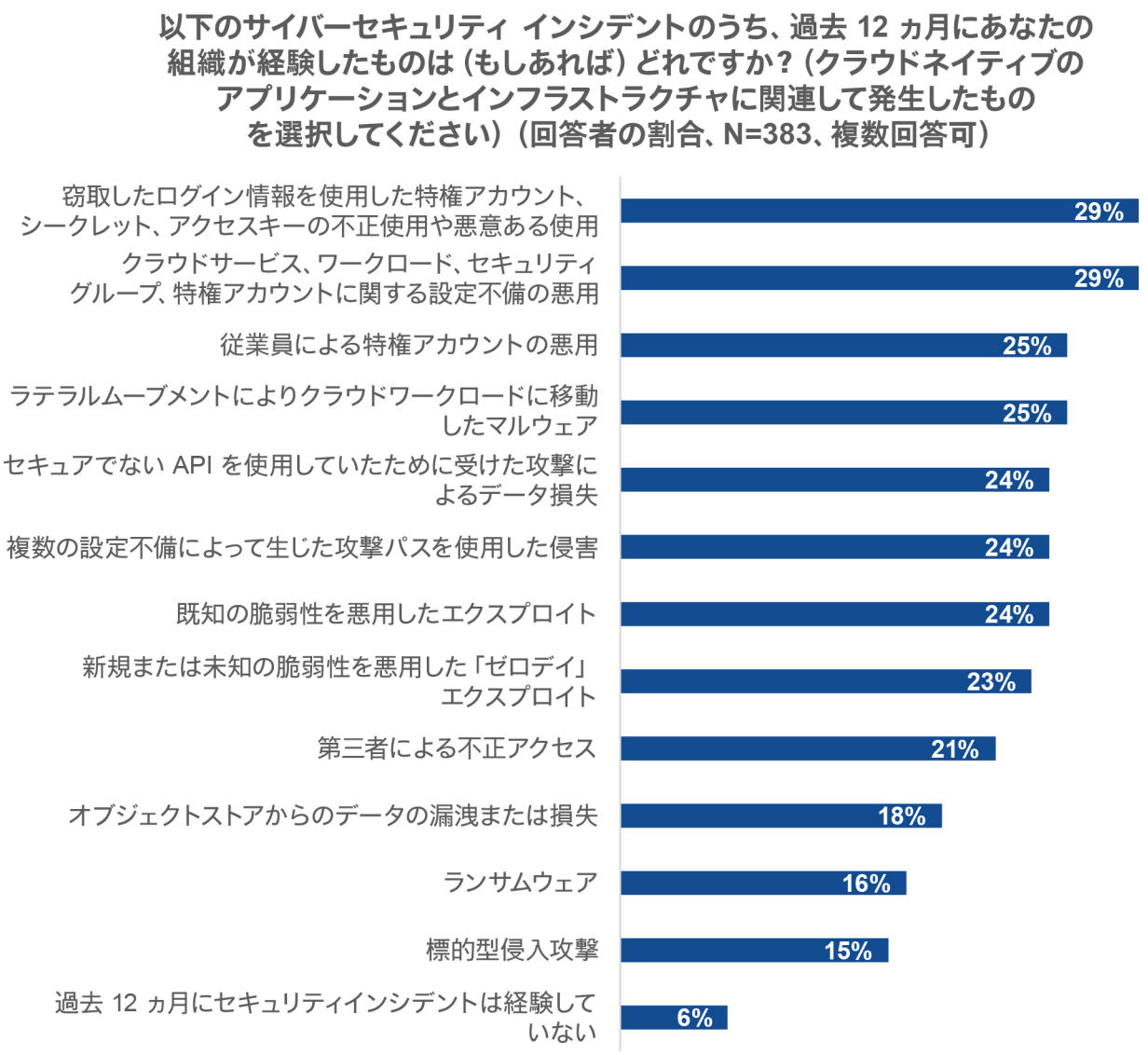
セキュリティインシデントは広範囲に及んでいる

一般的に組織は複数のセキュリティソリューションを導入しています。それにも関わらず、そのほとんどがクラウドネイティブのアプリケーションとインフラストラクチャに関連したセキュリティインシデントを経験しています。具体的には、組織の 94% が過去 12 ヵ月間に攻撃やラテラルムーブメントによるセキュリティインシデントに直面したと報告しています。その内訳は、ログイン情報の窃取（29%）、設定不備の悪用（29%）、セキュアでない API の使用によるデータ損失（24%）、ランサムウェア（16%）です（図 4 を参照）。[5]

この原因は、組織がリスクにさらされていることを認識していなかったか、セキュリティ問題の解決が間に合わず、インシデントの防止や封じ込めに失敗したかのいずれかです。これを見れば、環境全体の可視化が必要なだけでなく、リスク軽減に最も効果のあるアクションを優先的に実行することでセキュリティ運用を効率化するプラットフォームアプローチが欠かせないことは明らかです。

[5] 同上

図 4. 過去 1 年間に経験したクラウドネイティブのアプリケーションとインフラストラクチャに関連するセキュリティインシデントの種類



出典：Enterprise Strategy Group（TechTarget の一部門）

サイロ化したツールとデータが多すぎる

IT、ネットワーク、セキュリティの各チームがサイロ化した複数のツールを多用しているため、セキュリティ運用が非効率になっていることも組織の課題となっています。従来のアプリケーション セキュリティでは、複数のセキュリティ製品を使用してテストとモニタリングを行い、セキュリティ問題を検出することでカバレッジを確保していました。しかし、必要なアクションに優先順位を付けるためのコンテキストがないアラートを生成する個別のツールを追加し続けても、クラウドネイティブ アプリケーションや加速する開発サイクルに対応することはできません。

33% が、複数のセキュリティ製品からの結果を集約することが大きな課題であると回答

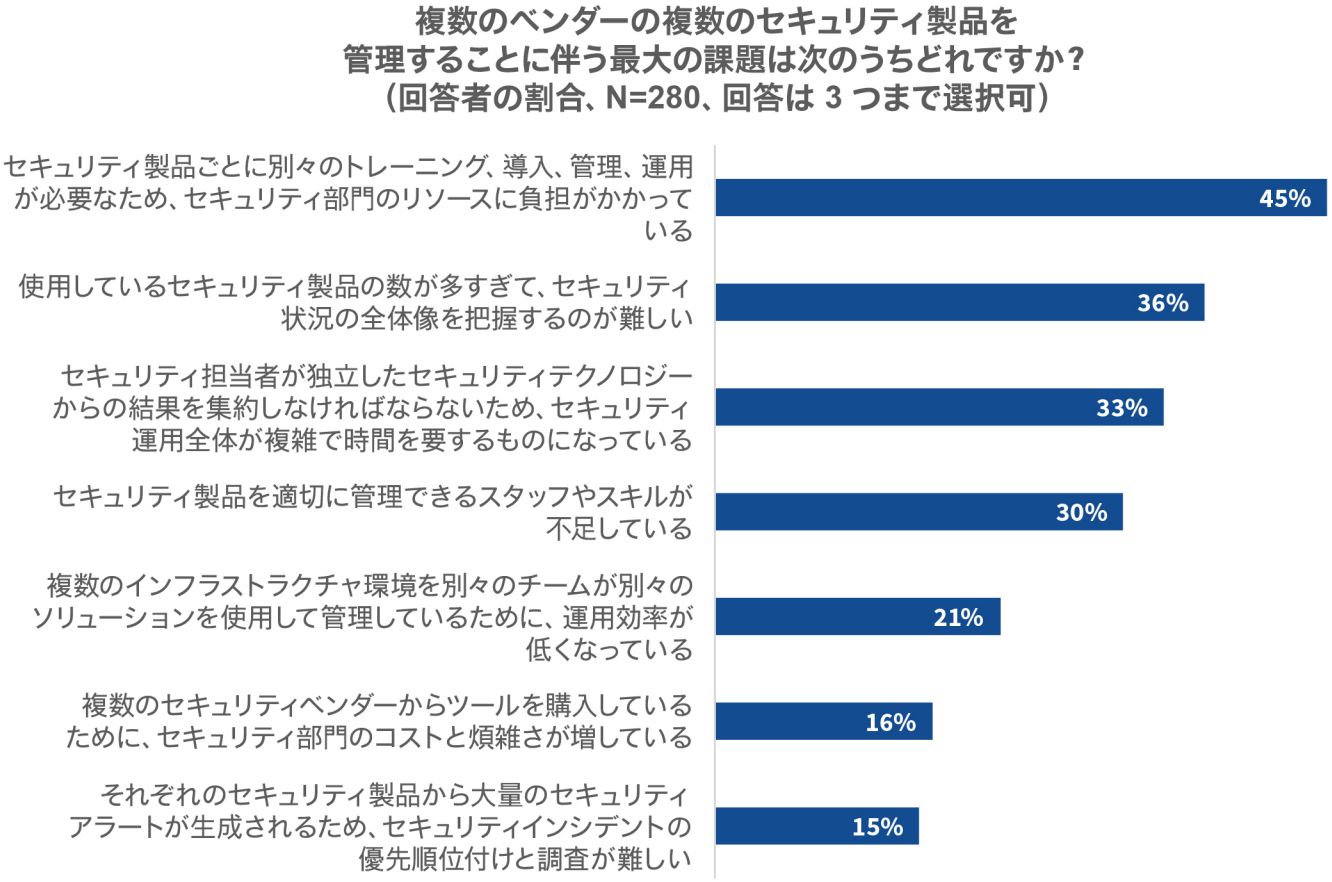
セキュリティ担当者が複数の独立したセキュリティテクノロジーからのデータを照合しなければならない場合、セキュリティ運用全体が過度に複雑で時間を要するものになります。

複数の製品から大量のアラートが出されると、開発者とセキュリティチームが対応できません。また、それぞれのツールが異なる用語を用いていることが多いため、ツールからの結果を分析してコンテキストを得ることが困難です。コンテキストは注意が必要な事象を優先するために欠かせません。さらに、いずれのツールにも、時間の浪費につながりかねないアラートの生成や誤検出を行う可能性があります。

Enterprise Strategy Group が実施した調査によると、複数のツールの管理がサイバーセキュリティ担当者の課題となっています。回答者の 45% がツールごとの展開と管理にトレーニングと時間が必要であると指摘しています。また、個別のツールではセキュリティ状況の全体像を把握するのが困難である（36%）、各ツールからの結果を集約するためセキュリティ担当者の負担が増えている（33%）と回答しています（図 5 を参照）。[6]

[6] 出典：『ESG Complete Survey Results: *ESG/ISSA Cybersecurity Process and Technology Survey*』、Enterprise Strategy Group、2022 年 6 月

図 5. 複数のセキュリティ製品を管理することに伴う課題



出典：Enterprise Strategy Group（TechTarget の一部門）

組織は、この状況を踏まえ、複数のクラウド サービス プロバイダー（CSP）にまたがって必要な情報を収集しその全体像を明らかにする製品やサービスに移行しつつあります。これが実現すると、セキュリティリスクをより効果的に管理できるようになります。たとえば、脆弱性の管理、攻撃対象領域の管理、攻撃パスの分析が効率化されるため、セキュリティリスクをより詳細に把握できるようになります。

ハイブリッド環境とマルチクラウド環境にまたがる統合プラットフォームのメリット：

- 特権アクセスの最小化と集中管理によるラテラルムーブメントの阻止
- 資産検出の広範な可視化とすべてのアプリケーション、ワークロード、リソースを対象とした攻撃パス管理
- SecOps チームへの信頼性の高いインサイト、アクション、優先順位の提供とセキュリティ態勢に関する情報の一元化

ネットワークアクセスがオーバープロビジョニングされている

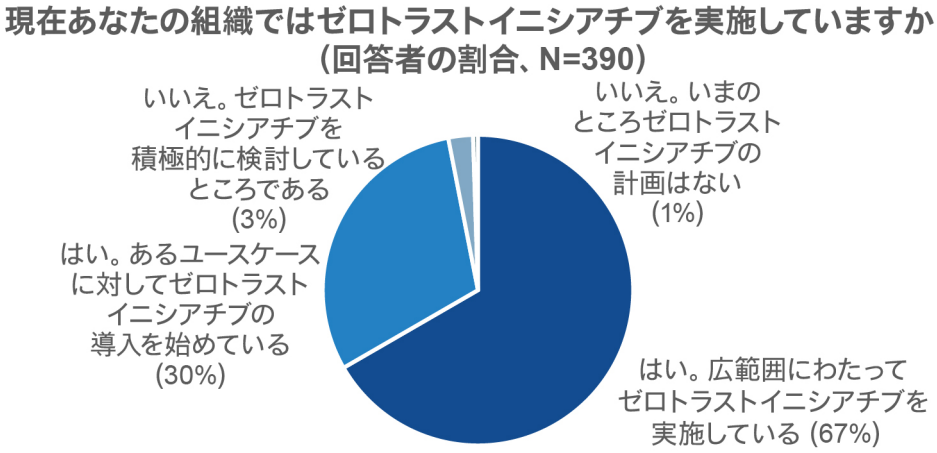
アイデンティティとセキュアなアクセスを管理することもセキュリティプログラムを効果的なものにするうえで重要な役割を果たします。クラウドネイティブ開発によって、組織とその開発者によるアプリケーションのクラウドへの展開と顧客、従業員、パートナーへの提供が簡単になるからです。アプリケーションをクラウドに展開するだけで対象のユーザーが利用できるようになりますが、アクセスを適切に管理して企業や顧客のデータを危険にさらす可能性のあるリスクを軽減する必要があります。つまり、クラウドにはワークロードを保護するための境界が存在しません。アイデンティティとアクセスが境界の役割を果たします。

前述のクラウドネイティブ セキュリティの課題とインシデントを見ると、その多くはアイデンティティとアクセスの問題に関連しています。これは、迅速な開発を促すためにアクセスをオーバープロビジョニングすることが簡単にできるからです。しかし、適切に管理されていない場合、アクセスを拡大したことで攻撃対象領域も拡大します。さらにアプリケーションが攻撃を受けやすくなったり、攻撃者がシステムに侵入したあとラテラルムーブメントを簡単に実行できたりするため、組織がリスクにさらされるようになります。

ゼロトラスト ネットワーク アクセス（ZTNA）アプローチの導入はアプリケーションの保護に効果的です。アクセス要求があるたびに検証を行い、それから接続を確立するため、インシデントが発生する可能性とその影響を最小限に抑えることができます。そのため、ゼロトラスト環境では、ワークロードやアプリケーションが侵害されてもデータアクセスやデータ漏洩を防ぐことができます。Enterprise Strategy Group の調査によると、ほとんどの組織（97%）が、ワークロードの保護を環境全体で強化するために、ゼロトラストイニシアチブをすでに実施しているかその導入を進めています。[7]

[7] 出典：『Complete Survey Results: *2023 SASE Series: SSE Leads the Way Toward SASE*』、Enterprise Strategy Group、2023 年 8 月

図 6. ゼロトラストイニシアチブを実施している組織の割合



出典：Enterprise Strategy Group（TechTarget の一部門）

しかし、組織が直面する課題としては、マルチクラウド環境とハイブリッド環境にまたがったアプリケーションへの最小権限アクセスの導入に加え、IT、運用、セキュリティの各チームによるコラボレーションの円滑化、さまざまなデバイスからのセキュアなアクセスの実現、コストの管理、データセキュリティの確保、パフォーマンスの維持、包括的な可視化とレポートの提供などがあります。

そのため、ハイブリッド環境とマルチクラウド環境の両方に対応し、ゼロトラストアプローチを統合したソリューションを見つける必要があります。このようなソリューションがあれば、運用効率を最適化しながらリスクを軽減できます。それによって、IT、ネットワーク、セキュリティの各チームは環境全体でアプリケーションを保護できるようになります。

Cisco Cloud Protection Suite について

Cisco Cloud Protection Suite は、ハイブリッドおよびマルチクラウドのアプリケーション環境にエンドツーエンドのセキュリティを提供することで、最新のアプリケーション セキュリティ アプローチを実現します。Cloud Protection Suite は、ベアメタルからクラウドネイティブまで、お客様に包括的なアプリケーション セキュリティを提供し、オンプレミスとクラウドの環境全体でワークロードを保護します。

Cisco Cloud Protection には以下の機能があります。

- **ハイブリッドとマルチクラウドの包括的なセキュリティ。**シスコの Cloud Protection Suite を使用すると、複数の環境にまたがるセキュリティリスクを効率的かつ効果的に管理できます。
- **すべての資産に対する広範な可視性。**ネットワーク、アプリケーション、クラウドの各資産を明確に把握することで、セキュリティ態勢を検証し、ビジネスに対するリスクに優先順位を付けることができます。

- **環境全体での一貫性。**シスコのスイートによってセキュリティフレームワーク、管理、コンプライアンスポリシーの適用が円滑化され、リスクの軽減と業界のベストプラクティスへの準拠が容易になります。
- **修復効率の最適化。**シスコのスイートは、データサイエンスに基づくリスクスコアリングを利用して、実際のリスクをもたらす脆弱性にハイブリッド環境全体にわたって優先順位を付けます。
- **アプリケーション保護。**ネットワーク、クラウド、VPC にまたがるトラフィックを保護することで、環境全体で一貫性のある正確なマクロセグメンテーションとマイクロセグメンテーションを実現します。
- **ゼロトラストアプローチに基づく最小権限アクセス。**Cisco Cloud Protection は、ZTNA を活用してオンプレミスとクラウドのワークロードを保護することで、攻撃対象領域を縮小し、ラテラルムーブメントを防止します。

Cisco Cloud Protection Suite を使用して複数のクラウド環境にまたがってアプリケーション セキュリティを管理することで、

- 運用のオーバーヘッドを削減し、リソースを最適化できます。
- リスクに応じて脆弱性に優先順位を付けることでセキュリティリスクを軽減できます。
- コンプライアンス規制への準拠を促進できます。
- 包括的な可視性により脅威への対応を迅速化できます。
- ビジネスの成長を後押しするデジタル トランスフォーメーションを実現できます。

まとめ

生産性の最適化を目的にワークロードのクラウド移行を拡大させるなかで、セキュリティチームは、環境全体でアプリケーションを保護しながらビジネスの成長に足並みをそろえなければならないという課題に直面しています。ハイブリッド環境とマルチクラウド環境にまたがってアプリケーションをサポートしながら、クラウドへの移行やクラウドからの移行を行うという複雑な状況が生じています。これに対応するには、統合された柔軟なアプローチが必要です。

Cisco Cloud Protection Suite は、複数のクラウドやデータセンターにまたがってアプリケーション セキュリティを管理するための効果的な手段をセキュリティチームに提供します。包括的な可視性と最小権限アクセス制御を実現することで、環境全体で資産とアプリケーションを保護する総合的で効果的な手段を提供します。自動化、環境全体での一貫性、統合化セキュリティツールによってセキュリティを管理する一元的な手段を提供します。これを利用することで手作業が削減され、IT、ネットワーク、セキュリティの各チーム全体の効率が最適化されます。

Cisco Cloud Protection Suite は、セキュリティチームがビジネスの成長とデジタル トランスフォーメーションを後押しするための効果的な手段になります。これを利用することで、開発チームの強化、新しいテクノロジーの導入、企業の競争力を維持するための合併や買収などをサポートできます。

Enterprise Strategy Group について

TechTarget の Enterprise Strategy Group は、焦点を絞った実用的な市場インテリジェンス、需要サイドの調査、アナリストによるアドバイザリサービス、GTM 戦略に関するガイダンス、ソリューションの検証、カスタムコンテンツを提供し、企業によるテクノロジーの売買を支援しています。

contact@esg-global.com

www.esg-global.com