次世代クラウドセキュリティー：リスク管理、コンプライアンス、ゼロトラストの統合

ハイブリッドクラウド環境において断片化を排除し、
リスクを減らし、コンプライアンスを徹底する方法

HashiCorp
an IBM Company

内容

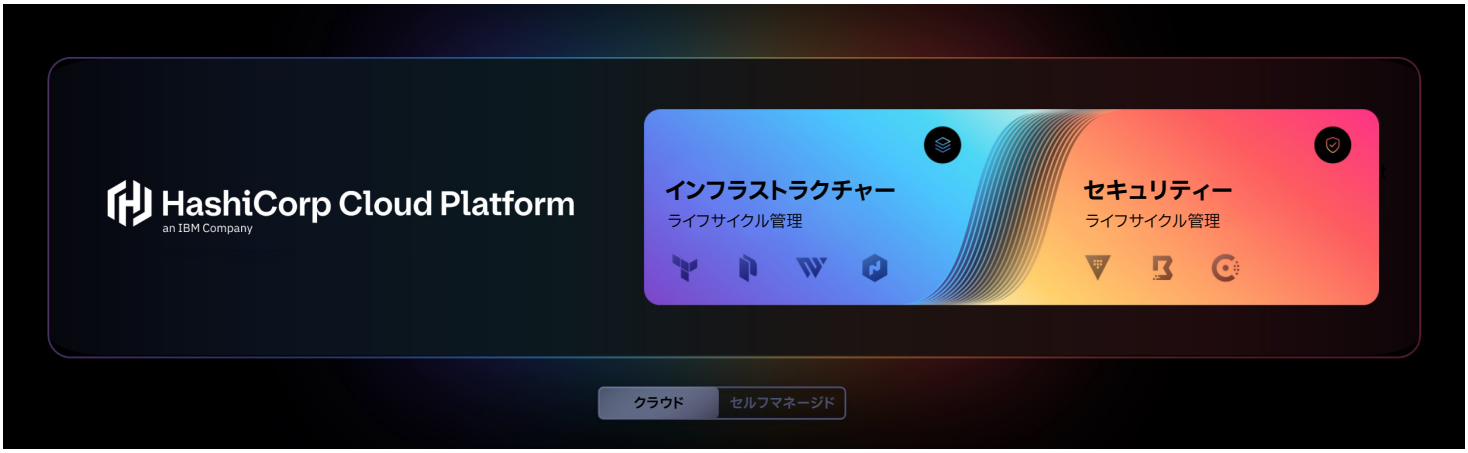
概要

組織はデジタル・トランスフォーメーションの迅速性、拡張性、効率性を向上させるため、クラウドの導入を加速しています。しかし、特にハイブリッドやマルチクラウド環境間におけるクラウド化は、単に迅速に進めればいいというものではありません。リスクを高めることなく、セキュリティーとガバナンスをしっかり強化することが重要になります。

従来型のITに比べて、クラウド・インフラストラクチャーは動的で、分散化しており、絶えず進化しています。静的で境界に縛られたネットワークのために構築されたセキュリティー・モデルでは、こうした変化に追いつけません。実のところ、こうしたモデルはしばしば妨げとなり、ツールの断片化、ポリシーの不整合、そして攻撃者が素早くつけ込める隙をもたらしてしまいます。

こうした時こそ、技術リーダーの出番です。迅速に提供する圧力が高まる中で、技術リーダーは組織をリスクから守り規制要件への準拠も確保する必要があります。リスクは高いですが、チャンスも大きい状況です。

HashiCorpのThe Infrastructure Cloudは、Infrastructure Lifecycle ManagementとSecurity Lifecycle Managementを統合する一元化されたコントロールプレーンを通じて、プロアクティブなリスク管理、コンプライアンス体制の強化、高度なゼロトラスト・クラウドの実践を可能にするという新たなアプローチを提供しています。



クラウド・セキュリティーの課題：攻撃対象領域の拡大とコンプライアンスの複雑さ

ハイブリッドクラウドの導入とAIが拡大するにつれて、課題もまた増加します。攻撃対象領域は広がり、手動プロセスはうまく機能せず、コンプライアンスはイタチごっことなります。ハイブリッドクラウドにおける実験から本番運用への過程においては、サイロ化、再現性に乏しいデプロイメント、そしてレガシー・ツールでは抑えられないような攻撃対象領域の拡大が起こりがちです。

断片化したセキュリティー・ツール、分断されたワークフロー、そして変化に追いつけない手動のチケット発行システムのせいで、多くの組織が行き詰まっています。可視性は限られ、構成ミスは気付かれません。そして認証情報は、あまりに多くの場所に長時間残っています。これは理論上のリスクではありません。攻撃者が悪用できる隙をもたらす、日常的な運用上の失敗なのです。

参考データ：

83%

の侵害がIDとアクセスの失敗に起因する。[1]

57%

が盲点のせいで
セキュリティー・インシデントを経験。[3]

80%

の会社がクラウド攻撃の増加を報告。[2]

1. 2024 Verizon Data Breach Investigations Report
2. 2024 Crowdstrike Global Threat Report

この問題を解決するには、単なる監視の強化以上の取り組みが組織に求められます。インフラストラクチャーの構築・デプロイ・管理のあり方そのものを見直し、機密情報、ユーザー、サービスを保護・検査・管理できるセキュリティー・ソリューションを組み込む必要があります。

この変革は、環境全体で厳格な制御を維持しつつ、より迅速に行動することが求められている今日の技術リーダーにとって不可欠です。セキュリティーとガバナンスの強化は、モダナイゼーションの単なる一要素ではなく、現代のクラウド運用を持続可能にするためのフレームワークなのです。

以下のセクションでは、この変革を実現するための3つの基本的機能について探ります。

1

先回り型のリスク管理

環境全体にわたる脅威への露出を低減するために

2

強化されたコンプライアンス体制

継続的なポリシーの適用を通じて実現します。

3

Advancedゼロトラストの実践

アイデンティティーを新たな境界とするものです。

プロアクティブなリスク管理：ハイブリッドクラウド環境における脅威エクスポージャーの軽減

プロアクティブなリスク対処の価値は明確です。セキュリティー上の問題は、発生する前に回避できるに越したことはありません。しかし、それを常に、あらゆるクラウドと環境にわたって一環して行うという点において、多くのチームは苦慮しています。これは、さまざまな環境にわたって一元管理するような環境がないためです。

一元管理とポリシーの施行がなければ、セキュリティーのプロセスに亀裂が生じ始めます。構成ミスが忍び込み、パッチの適用されない脆弱性が残り、アクセス制御が停滞するようになります。時が経つにつれ、その裂け目はデジタル資産の全体に広がっていき、攻撃対象領域が大幅に拡大することになります。

HashiCorpのThe Infrastructure Cloudにより、技術リーダーは1回限りの修復から、反復可能な自動化モデルに移行でき、以下のことが可能になります。

Terraformによる一元化コントロール・プレーンを活用することで、組織の健全性を確認し、セキュリティー・リスクを検知し、ハイブリッドクラウド環境全体にわたってポリシー施行を徹底し、デジタル資産全体にわたるセキュリティー上のインサイトを獲得できます。

Terraform、Vault、Boundaryを使用して、機密性の高いシステムに時間制限付きの最小権限アクセスを与えることにより、認証情報の共有や過度に広範囲な権限のリスクを排除するため、**機密とIDの管理を自動化します。**

VaultとBoundaryによるアクティブ・セッション監視、ポリシーの施行、自動監査ロギングにより、**人間と機械によるアクセスを管理、監視します。**

Terraform、Packer、Vaultにより、合理化された修復ワークフローと自動化されたCI/CDパイプラインを通じて、**脆弱性を特定し、優先順位を付けて修復します。**

例えばManTechでは、長時間残る認証情報や一貫性のないアクセス制御が深刻なリスクとなっていることを把握していたセキュリティー・チームが、**シークレット管理のために Vault を、ユーザー・アクセスを標準化するために Boundary を導入することで、認証情報のローテーションを自動化し、認証情報のローカル保存を不要にしました。**同社の開発者は、Terraformワークフロー上に構築された安全でポリシー主導のインフラストラクチャー内で作業できるようになりました。

リスクを管理できるようになったら、セキュリティーとガバナンスを強化するための次のステップは、内部の利害関係者と外部の規制の両方により定められた厳格な基準に、インフラストラクチャーが準拠するよう徹底することです。

セキュリティー体制の強化：大規模なガバナンス

コンプライアンスは単なるチェックリストではなく、ビジネスを成功させる力です。そもそもコンプライアンス規制の本旨は、事業と顧客へのリスクを減らすことにあります。正しく実施するなら、ビジネス上の優先事項に沿うものとなるはずです。しかし61%の企業は、コンプライアンスがクラウド導入における主な障壁となっていると述べています。[4]

多くのチームにとって、監査はいまだに大きな負担です。ポリシーの適用が一貫性を欠き、SOC 2、PCI-DSS、HIPAA、DORAといった規制にすべて対処しなくてはならないため、複雑さは身に迫る課題となっています。リスクおよびコンプライアンスのチームは、地域、業種、部門にまたがる規制を解釈し、把握することに追われてしまうことがよくあります。

チームに必要なのは明確さです。監査や違反が起こる前に、デプロイするインフラストラクチャーが社内ポリシーおよび社外規制に沿っていることを、自信を持って確認したいのです。

だからこそ、コードとしてのポリシーと単一の記録システムによる継続的な監視は非常に強力です。コードとしてのポリシーがあれば、全環境にわたりポリシー遵守を一貫して定義、展開、施行できます。監査の負担を減らすだけでなく、チーム間の信頼も築けるのです。**The Infrastructure Cloudは、セキュリティーおよびコンプライアンス・チームに、コンプライアンスを示す共通の自動化された基盤をもたらし、しかも革新を遅らせることがありません。**

> 「成功するためには、ポリシーをコードとして扱う必要があることを私たちは理解していました。そして、完全な自律性を可能にするパラダイム・シフトが求められたのです。」
> 多国籍銀行のクラウド製品責任者

ある多国籍銀行のプラットフォーム・チームは、オペレーションを加速するにあたって、共通のコードとしてのポリシーのプラットフォームが必要であることを認識しました。**同チームはTerraformを使用することで、コンプライアンスに準拠したTerraformインフラストラクチャー・モジュールのライブラリーを構築して、組織全体に共有することができました。**これらの事前承認済みモジュールは、標準化された金融関係ポリシーに裏付けられたものであるため、クラウド・プラットフォーム・チームのワークフロー内で行われるすべてのデプロイがコンプライアンスに準拠したものとなります。また、Terraformはポリシーとしてのコードのプラットフォームであるsentinelも提供しました。これにより、クラウド・プラットフォーム・チームの一元化したポリシー・フレームワークに沿って、Terraform上の各デプロイに対するポリシーの確認を自動化できるようになりました。

3. 2024 IDC Cloud Security Survey

The Infrastructure Cloudは、以下の機能により、コンプライアンスおよびリスク・チームが、デプロイメントの前後にわたって一貫したガバナンスを実現できるようにします。

TerraformとVaultによる**単一のデータ管理システム**と一元的なコントロール・プレーンにより、デプロイメントの前、最中、後にわたってコンプライアンスを徹底できます。

ゴールデン・イメージとモジュールにより、安全なインフラストラクチャーを標準化し、コードとしてのポリシーにより、CI/CDパイプラインにガードレールを直接組み込めます。

アクティブなユーザーおよびセッションの監視により、ポリシー違反をリアルタイムで特定し、事前承認済み構成からの逸脱を通知します。

ロギングの自動化、シークレットのアクティビティー追跡、セッション記録を通じて、**コンプライアンス監査の効率化を実現します。**

ガバナンスとコンプライアンスを日常のオペレーションに組み込んだ後で、変革の最後に必要となる要素は、最も重要なもの、すなわちアクセスを守ることです。ここで威力を発揮するのがゼロトラストです。理論上のフレームワークではなく、アイデンティティーに根ざした運用上の現実として具現化します。

高度なゼロトラストの実践：アイデンティティー・ベースクラウド・セキュリティー

今日、多くの組織はコントロールについて幻想を抱いています。アクセスはコントロールされ、認証情報は安全で、適切な人が適切な権限を持っていると思い込んでいるのです。しかしハイブリッドおよびマルチクラウド環境においては、その幻想はあっという間に崩れるかもしれません。そこではGitHubのリポジトリに埋め込まれた平文の認証情報、無差別なアクセス権が与えられたVPN、一様に適用されないポリシーなどによって、セキュリティーが脅威にさらされています。

進むべき道は、ゼロトラストしかありません。データ侵害の80%は権限の誤用から生じているため、アイデンティティー・ベースのセキュリティーが必要であることは議論の余地がありません。[5]ただし、自動化、可視性、アイデンティティーを基盤としなければ、それを大規模に実装するのは困難です。

HashiCorpは、組織が思い込みから確信へと進めるよう後押しすることで、こうした課題に応えます。The Infrastructure Cloudにより、チームは脆弱な境界ベースのモデルに頼ることなく、アクセスを動的に保護できます。

> 「Vaultは私たちにとって、機密データのセキュリティーと保護を徹底しつつ、そのためにかかる時間や労力を最小化するというバランスを取るという難題に答えるための切り札となりました」
>
> ヘルスケア・テクノロジー企業のプラットフォーム・サービス担当シニア・エンジニアリング・マネージャー

athenahealthでは、この変換が大きな変革をもたらしました。Vaultは現在、1日あたり300万件以上の機密情報リクエストを処理しており、手動のチケット発行システムをなくすことで、解決時間を4時間から30分未満に短縮しました。**Zeroゼロトラストはもはやプロジェクトではなく、業務の進め方そのものなのです。**

4. 2025 State of Cloud Security Report, Cybersecurity Insiders
5. 2020 Verizon Data Breach Investigations Report

成功の鍵は、信頼できるIDを用いて機械、人、ネットワークを接続できる、IDベースのアクセス制御を活用することにあります。IDベースのアクセス制御を高度なデータ保護と組み合わせることで、組織がプロアクティブ（事前対応型）およびリアクティブ（事後対応型）な観点から保護されるようになります。包括的なゼロトラスト・セキュリティー・アーキテクチャーには、次のものが含まれる必要があります。

最小権限とMFAによる制御によるユーザーのアクセスを確保し、共有の認証情報や過度に広範囲な権限に頼ることなく、スコープを限定した、期限付きのアクセスを開発者と運用担当者に付与します。

機械間のアクセス要求の認証により、リスクを低減し、機械IDのシークレットに関するライフサイクル管理を標準化します。

シークレットのオンデマンドによる生成、ローテーション、取り消しにより、シークレットに関するポリシーを強制し、シークレットの漏洩リスクを減らして、長時間残るシークレットをなくします。

人間のユーザーと機械間の接続との両方において、IDベースの制御に基づき、**自動的かつ動的に鍵と証明書の作成を行います。**

これら3つの機能が一体となって、組織に合わせて進化し、環境全体に拡張し、今日のチームが実際に構築および導入を行う方法に合わせた、一貫性のあるセキュリティー・アーキテクチャーが形成されます。

結論：HashiCorpのThe Infrastructure Cloudによりセキュリティーとガバナンスを強化する

クラウドを適切に運用するというのは、セキュリティーを適切に運用するということであり、その出発点は統一的な戦略にあります。HashiCorpのThe Infrastructure Cloudは、Infrastructure Lifecycle Management（ILM）とSecurity Lifecycle Management（SLM）を統合して、あらゆる環境にわたって制御、一貫性、拡張性を実現するための青写真を提供します。

The Infrastructure Cloudは、修復までの時間を短縮する、コンプライアンスをリアルタイムで実証する、開発者のワークフローを加速するといった、現在求められるあらゆる局面に対応できるよう構築されています。

これから進むべき道は分断化ではなく、統合化です。HashiCorpのThe Infrastructure Cloudは、リスクをなくし、手作業を減らし、コンプライアンスに準拠したインフラストラクチャーを導入初日から実現するために役立ちます。技術リーダーにとって、これこそ待ち望んでいた変革であり、理想の場所へと導くパートナーなのです。

40%

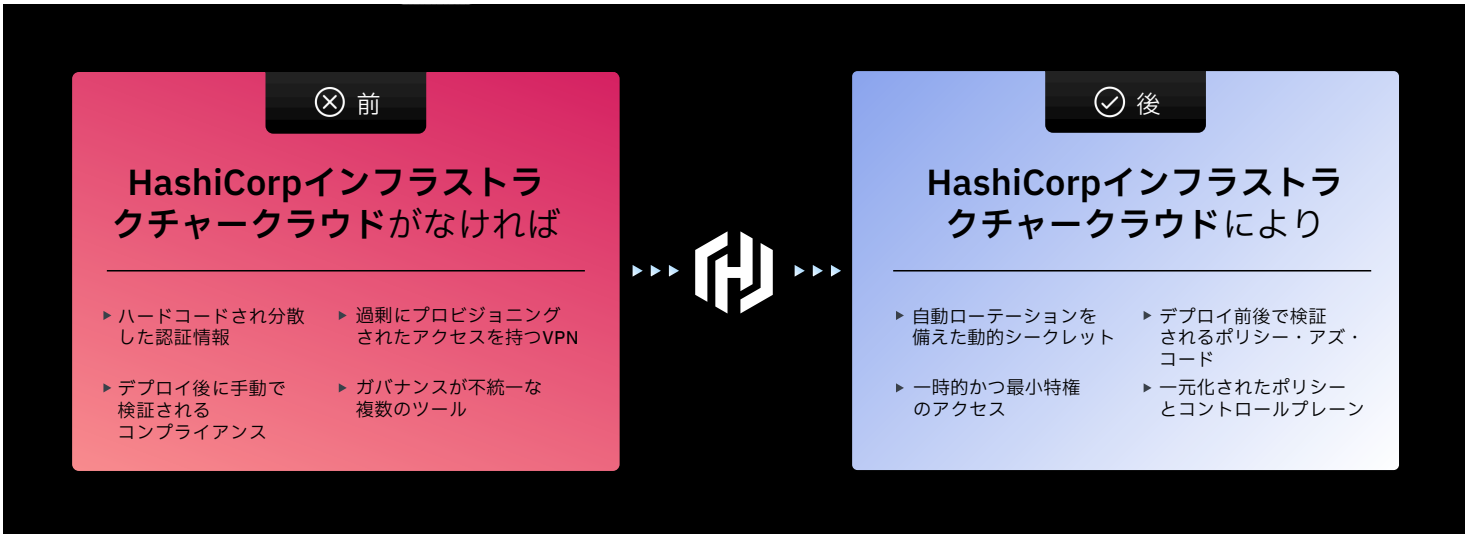
データ侵害が減少

50%

コンプライアンス対応を強化

25%

セキュア・アクセスの効率が向上



2025年8月