Deloitte.
デロイト トーマツ

パブリッククラウドのDNAにセキュリティを組み込む

パブリッククラウドへの移行において考慮すべき事項

MAKING AN IMPACT THAT MATTERS since 1845

目次

パブリッククラウドにおける資産の保護

クラウドは組織の主要なデータ保管場所となっています。大半の組織は既にアプリケーションをクラウドプラットフォームに移行しており、現在オンプレミスでデータを管理している企業の多くもクラウドへの移行を近い将来に計画しています。また、クラウドへの移行と並行して、あらゆる部門で、次世代のアプリケーションや高度なアナリティクスを活用するためのデータプラットフォームの近代化が進んでいます。

クラウドの利点の多くは、APIやネイティブサービスによる自動化によってもたらされます。これによって、コストとパフォーマンスを最適化しながら、より短期間で、より多くの機能変更や新機能のリリースを実現します。

しかし、自動化やそれに伴う頻繁な機能変更が行われる環境においては、セキュリティとコンプライアンスはさらに重要となっています。従来、セキュリティはビジネスとITの進展や目標達成の阻害要因となってしまうことがありました。自動化の活用によって、ビジネス機能とIT機能が、より早く、より頻繁に機能変更と新しいソリューションを展開できる一方で、セキュリティは相変わらず従来の方法でチェックやコントロールを実施しているケースが多く見られます。クラウドネイティブサービスやクラウドプラットフォームの導入が進む中、この従来型のセキュリティを確保する方法はますます非効率的になりつつあります。

このような望ましくないシナリオを2つ紹介します。

1つ目は、セキュリティに関する懸念を脇に置いて、テクノロジーとビジネス機能を優先し、より迅速な導入とビジネス機能の自動化の拡大を優先することです。これによってフルスピードで推進することが可能になる反面、セキュリティとコンプライアンスの効果的な管理が欠如しているため、結果としてインパクトの大きいインシデント発生につながるリスクがあります。

2つ目は、規制の強い業界ではセキュリティとコンプライアンスを遵守することを優先し、適切なセキュリティチェックを実施することを重視するアプローチを取ることによって、クラウドの提供する新しい機能の導入スピードを遅らせる可能性があります。これではセキュリティは確保できても、クラウドの利点をフル活用するというビジネス上の目標を達成できず、競争力を損なうことになりかねません。

自社の全体的なクラウド戦略と整合した、明確なクラウドリスク管理戦略を持つ組織は、ビジネス、テクノロジー、セキュリティの各機能の目標を整合させるための重要な基盤を持っています。

ビジネスプロセスやテクノロジープロセスと同様に、セキュリティを自動化することは、従来のセキュリティアプローチの弊害を取り除く方法の1つです。また、クラウドのアセットを単体で運用するのではなく、クラウドとクラウドセキュリティを統合管理するアプローチを採用することも、セキュリティをエンドツーエンドで首尾よく統合するためには不可欠です。さらに、クラウド技術に精通し、サービスプロバイダーが定期的に導入する機能変更や新サービスに対応できる人材を確保することも、パブリッククラウドにおいて組織が適切かつ安全に統合と成長するために欠かせません。

私たちは、クラウドに移行する組織は、最初の段階から統合的なアプローチを意識して活動を推進することが必要だと考えています。このようなアプローチによって、クラウドベンダーの選定時に行うベースライン分析やセキュリティ要件の評価から、クラウドベンダーとの責任共有モデルの決定、インフラ内のセキュリティガードレールの設定、DevSecOpsプロセスの管理まで、移行のあらゆる段階において、組織がクラウドのDNAにセキュリティを組み込むことが可能になります。

本レポートでは、パブリッククラウドの導入に伴うセキュリティ上の考慮事項や、クラウドへの移行において組織をリードする際に、セキュリティバイデザインを確保するためのステップに関する知見を提供します。

パブリッククラウドの導入に伴う サイバーセキュリティリスクへの対応

新型コロナウイルス感染症のパンデミックを背景にDX化のペースが加速している状況下で、パブリッククラウドプラットフォームの導入が拡大するにつれて、企業がパブリッククラウドに資産を移行する際に晒されるリスクも増加しています。

以下に、組織がパブリッククラウドプラットフォームを導入する前に考慮すべき主要なリスクとそれに対応する管理策を紹介します。

リスク 1 **クラウドに適したリスク管理戦略やガバナンスの欠如により、組織はクラウドに適していない可能性のある既存のポリシーやプロセスを利用することになる**

クラウドのリスク管理戦略の策定

パブリッククラウドプラットフォームの特性を考慮した、パブリッククラウドのリスク管理戦略を策定します。

リスク 2 **アプリケーションをクラウドに移行する際、クラウドネイティブプラットフォームのサービスを利用する場合に、セキュリティ設定や使用方法が安全ではないリスクがある**

クラウド環境における強力なコントロールの導入

ベストプラクティスのガイドラインに従い、ID およびアクセス管理（IAM）、サイバーセキュリティ、データ保護、暗号鍵管理などの主要なセキュリティ領域で、クラウドプラットフォーム自体が提供するセキュリティサービスを活用します。

リスク 3 **マルチクラウドやハイブリッドクラウドを含む、複数の多様なクラウドプラットフォームの監視を一元的に監視する統合監視ソリューションの欠如により、重要なインシデントが発見されなかったり、その影響が過小評価される等のリスクがある**

組織のサイバーセキュリティ業務のクラウドへの拡大

既存のレガシー／オンプレミス監視と組み合わせて、パブリッククラウドのワークロードのセキュリティも含めたサイバーセキュリティ運用の範囲を拡大します。

リスク 4 **従来型の手作業によるセキュリティチェックは、クラウドの自動化によるメリットを阻害する要因となるだけでなく、自動化によってもたらされる機能変更の規模やスピードに対応できず、セキュリティチームが脆弱性を見過ごすリスクがある**

クラウド技術を活用したセキュリティコントロールの自動化

IT 機能やビジネス機能の自動化に使用されているのと同じクラウド技術を活用してセキュリティコントロールを自動化し、手作業によるコントロールで生じる弊害を排除するのと同時に、セキュリティが機能変更の規模やスピードに対応できるようにします。

リスク 5 **クラウドサービスが急速に進化し、新サービスを活用する組織のテクノロジーおよびビジネス要件が変化している環境下で、クラウドに関連するセキュリティの影響を理解し対応するための十分かつ適切なスキルセットを有した人材が存在しないリスクがある**

クラウドの適切なスキルセットの確保

新規導入するクラウドサービスやケイパビリティによってもたらされるリスクを適切に理解し、管理するために、組織のスキルや知識プールが十分な深さと幅を持つようにします。

本レポートでは、5 つのリスクと関連する管理策をそれぞれ詳しく見ていただくとともに、組織がこれらのセキュリティ上の課題を設計によって克服し、パブリッククラウドプラットフォームが提供するメリットを享受しながら、付随するテクノロジーリスクとサイバーセキュリティリスクをあらかじめ軽減することを可能にする一連のステップについて詳しく説明します。

クラウドのリスク管理戦略の策定

パブリッククラウドのリスク管理戦略を策定するための最初のステップとして、責任共有モデルと自組織の責任下にあるメタストラクチャレイヤーにおける設定ミスのリスクについて明確に理解する必要があります。これによって、組織固有のニーズに合わせてカスタマイズされたクラウドリスク管理戦略の設計が可能になります。最後のステップでは、セキュリティ上のギャップを特定してそれを解消するために、組織はクラウド構成管理のベースライン評価を実施すべきです（図1参照）。

図1：パブリッククラウドのリスク管理戦略を策定するための3つのステップ

ステップ1

責任共有モデルと、自組織の責任下にあるメタストラクチャレイヤーの設定ミスのリスクについて明確に理解する

以下のパブリッククラウドプラットフォームの特性に応じて、自組織にもたらされるリスクに注意を払う必要があります。

- クラウドデプロイメントモデルの種類（シングルベンダー、マルチクラウド、ハイブリッドクラウド）
- クラウドサービスモデルの種類（Infrastructure as a Service（IaaS）、Platform as a Service（PaaS）、Software as a Service（SaaS）、またはこれらの組み合わせ）

リスクの例として、責任共有モデルの誤った解釈や、組織の責任下にあるメタストラクチャレイヤーの設定ミスなどがありますが、これらに限定されるものではありません。

どのようなリスクが自組織に該当するのかを特定する第一歩として、セキュリティに関するプロセス、ツール、テクノロジーに対して成熟度ベンチマークを実施することが有効です。

この成熟度ベンチマークの取り組みは、米国国立標準技術研究所（NIST）やクラウドセキュリティアライアンス（CSA）が提供する適切な規格に基づいたサイバークラウドに関するフレームワークを使用して実施する必要があります。この結果に基づいて、組織は特定された問題を解消するための戦略ロードマップを設計し、実装すべきクラウドセキュリティのリファレンスアーキテクチャとデザインパターンを策定することができます。

自組織の責任下のメタストラクチャレイヤーを含むすべてのインターフェースを考慮して、クラウドセキュリティの設計、実装、その後の評価をするために、組織は脅威モデリングにも取り組むべきです。脅威モデリングは、クラウドのインターフェースに存在する可能性のあるリスクと脅威の詳細な分析に加えて、セキュリティに焦点を当てたテストケースの作成も可能にします。これにより、組織はコンプライアンスに準拠しながら、ベストプラクティスに沿った運用が可能になります。

ステップ 2

組織に合わせてカスタマイズしたクラウドリスク管理戦略を策定する

カスタマイズされたクラウドリスク管理アプローチを策定するには、組織は業界標準のクラウドコンピューティングリスクフレームワークを活用して自社の現状を把握し、ヒト、プロセス、テクノロジーの観点から存在する可能性のある問題を特定すべきです（図2参照）。

このために使用するフレームワークは、テクノロジー、サイバー、エンタープライズに関する主要なリスクをすべて網羅する必要があります。これらに含まれる構成要素として、ガバナンス、リスクマネジメント、コンプライアンス、デリバリー戦略およびアーキテクチャ、インフラセキュリティ、IAM、データ管理、ビジネスレジリエンスおよび可用性、ITオペレーション、ベンダー管理、ビジネス運用などが挙げられます。

その後、業界のベストプラクティスに基づいて、組織は特定のクラウドセキュリティプロバイダー（CSP）、クラウドベースのソリューション、Software as a Service（SaaS）のデプロイメントのためにカスタマイズされたリファレンスアーキテクチャを設計することができます。

図2：業界標準のクラウドコンピューティングリスクフレームワーク

組織のクラウドリスク戦略をカスタマイズする際に、業界のベストプラクティスに基づいてリスクとギャップの現状評価を行うことが非常に有効です。私たちのクライアントの中には、NISTやクラウドセキュリティアライアンス（CSA）のフレームワークを基にした成熟度評価の結果を、ロードマップの策定やプロセスの改善の参考にしているケースが多くあります。

このことを念頭において、デロイトは業界のベストプラクティスを用いてクラウドセキュリティを対象としたサイバーセキュリティフレームワークを整備しています。クラウドに関する主要なリスクを体系化しており、ステートメント（質問項目）に基づいて組織のベンチマーキングを提供します。この結果、リスクアセスメントとベンチマーキングの取り組みでカバーすべきすべての関連分野を包括的に網羅することができます。

21のクラウドセキュリティのケイパビリティ：概要

クラウドガバナンス
- プロバイダーガバナンス
- コンプライアンスおよび監査
- リスク管理
- セキュリティガバナンス

デバイス、ID、アクセス
- デバイス
- IDおよびアクセス管理

ネットワークおよびインフラ
- プラットフォーム保護
- クラウド統合
- ネットワーク保護

データ保護
- データガバナンス
- 暗号技術
- データ損失防止

アプリケーションセキュリティ
- セキュアな設計と開発
- セキュアデプロイメント
- セキュア運用

クラウドセキュリティ監視
- ロギングおよび監視
- セキュリティ設定および検出
- セキュリティおよび使用状況の分析

クラウドレジリエンス
- 耐久性
- レスポンス
- リカバリー

ステップ3

セキュリティベンチマークに照らしてクラウド構成のベースライン評価を実施し、ギャップを特定して解消する

セキュリティ上のギャップを特定する際に、組織はセキュリティベンチマークに照らしたクラウド構成のベースライン評価を実施することが求められます。この評価では、クラウドのセキュリティ、包括的なコンテナセキュリティ、アセットの検出スキャン、役割および責任、アカウント管理のベストプラクティス、さらにポリシーおよび基準のコンプライアンスレビューなどの分野を網羅する必要があります。

通常、評価結果は、ベースラインとの差異や各リスク評価を明確にした包括的な報告書として、具体的な改善提案とともに提供されます。さらに、評価中に見つかったグッドプラクティスは、組織の強みとして継続的に活かせるよう、詳しく分析すべきです。その後、未解決のリスク項目を迅速に是正し、セキュアなベースラインを構築したうえで、クラウドセキュリティを自動化するケイパビリティを追加することで、継続的なコンプライアンスを実現します。

対象クラウドのサービスモデルがPlatform as a Service（PaaS）かSoftware as a Service（SaaS）かによって、クラウドセキュリティの自動化は実装方法が異なる可能性があります。

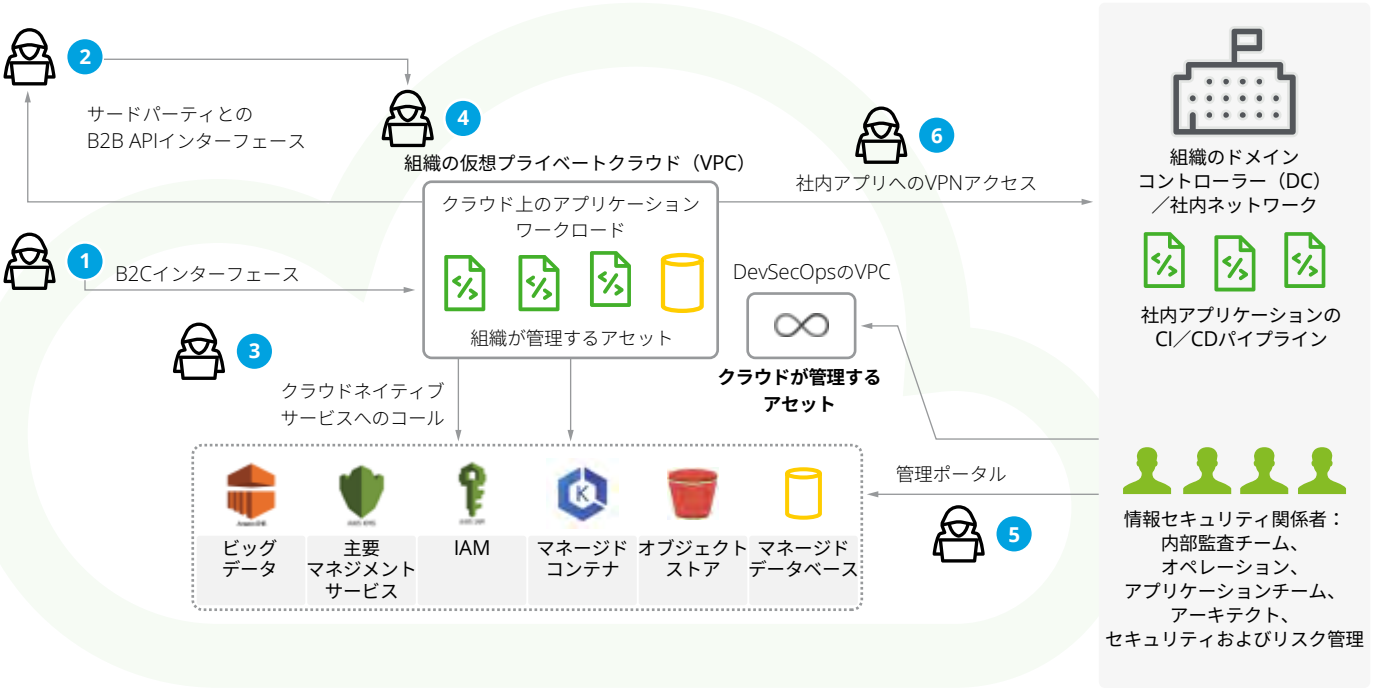
PaaSモデルを採用する際、組織はマネージドサービスプロバイダーと協力して、Cloud Security Posture Management（CSPM）とCloud Workload Protection Platform（CWPP）を実装することが可能です。

SaaSモデルを採用する際、組織はアプリケーションの構成により一層注意を払う必要があります。 今日、一部のエンタープライズ向けのSaaSソリューションは、サードパーティとの統合やその他のカスタマイズオプションはもちろんのこと、200を超えるサービス構成の設定情報を持っているため、この課題は組織にとってより複雑になっています。SaaSソリューションが、ユーザー受け入れテスト（UAT）または本番フェーズに到達した時点で、SaaSソリューションの安全でない設定を管理するためにSaaSのセキュリティポスチャマネジメントを提供する監視ツールをデプロイすることができます。また、組織は特定のイベントに対する詳細な改善提言をITサービス管理（ITSM）に統合することで、インシデント対応管理も効果的に行えます。

従来の脆弱性診断やペネトレーションテスト（VA／PT）は、エンドユーザーに公開されているインフラやWeb／APIインターフェースのみを対象にしていました。しかし、クラウドセキュリティ評価では、組織が管理するすべてのレイヤーを対象とする必要があります。これらのレイヤーがテストされること、特に組織のアプリケーションとクラウドネイティブサービス間に相互作用するセキュリティを定義したクラウドメタストラクチャ構成の設定をテストすることが重要です。

以下に例を示します。

図3：一般的なクラウドアプリケーションが晒される様々なインターフェース



インターフェース1はB2Cの従来のウェブやモバイルのインターフェース、インタフェース2はB2B／B2CのAPIインターフェースです。これらはクラウドに限定されない一般的なものであり、適切にテストされていることが多いです。

クラウドの場合、構成や設定に応じて、上記以外にもセキュリティ対策が必要となるインターフェースが追加される可能性があります。

インターフェース3では、クラウドネイティブサービスと自組織の管理するアセットとの統合を扱います。

インターフェース4では、クラウド自体のソリューションやワークロード（例：IaaS仮想マシン（VM）や顧客が管理するコンテナデプロイメントなど）を扱います。

インターフェース5は、CSPの管理ポータルまたはAPIベースのアクセスを通じて定義できる管理ルール、ポリシー、ロールなどを指します。

インターフェース6は、クラウドに移行したワークロードと社内アプリケーションの安全な統合を行います。

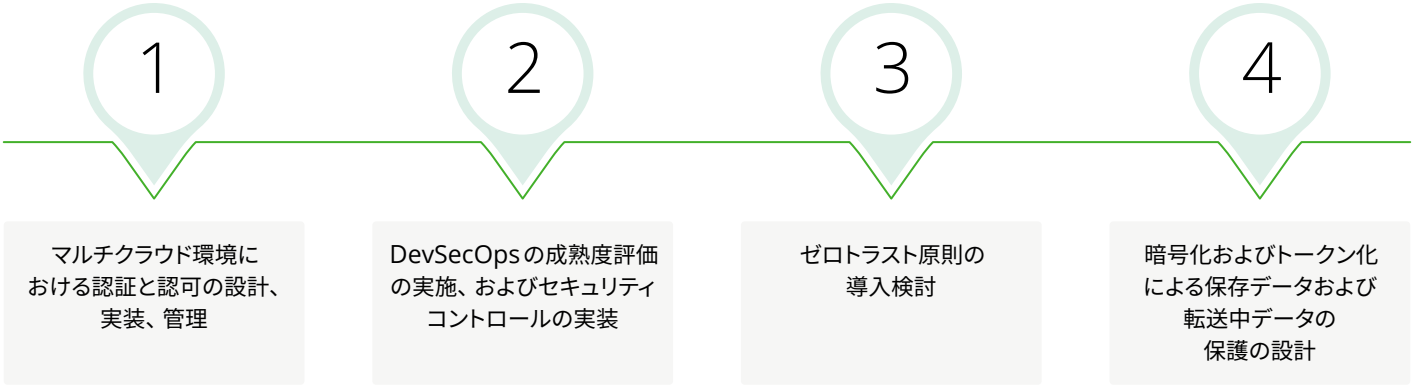
クラウドセキュリティの評価アプローチとして、クラウドの場合に追加されるインターフェース3から6を包括的にテストすること、また、適切なツールを使用することで従来の（インターフェース1と2を対象とした）VA／PTの アプローチを補完することが推奨されます。

セキュリティの設計と実装の観点から、クラウドに移行するソリューションが設定ミスやクラウドメタストラクチャに関連する脆弱性から保護されるように、インターフェース3から6により細心の注意を払うべきです。

クラウド環境における強力なコントロールの導入

組織は、特にIAM、サイバーセキュリティ、データ保護、暗号鍵などの分野で、クラウド環境に強力なコントロールを導入することが求められます。そのためには、マルチクラウド環境における認証と認可の設計、実装、管理、DevSecOpsの成熟度評価の実施とそれに見合ったセキュリティコントロールの実装、ゼロトラスト原則の導入の検討、そして暗号化およびトークン化による保存データおよび転送中データの保護の設計が必要になります（図4参照）。

図4：クラウド環境に強力なコントロールを導入するための4つのステップ



ステップ1

マルチクラウド環境における認証と認可の設計、実装、管理

クラウドにおける全社的なIDおよびアクセス管理（IAM）と特権アクセス管理（PAM）を設計、実装するために、組織はクラウドネイティブサービスの活用を模索すべきです。これには、オンプレミス環境とクラウド環境の認証プロセスを統合するためのロールベースのアクセス制御、多要素認証（MFA）などが含まれます。

主な活動には、ユーザー、ロール、権限の定義、認証仕様の設計、特権ID管理（PIM）およびPAMのプラットフォームプロセスの定義、ユーザープロファイル、ユーザーグループ、ロールの構築、ユーザーに対するMFAの実装、ユーザーマッピングの実行、ユーザー管理プロセスの開発、特権アクセス管理プロセスの実装などがあります。

ステップ2

DevSecOpsの成熟度評価の実施、およびセキュリティコントロールの実装

CI／CDパイプライン全体にセキュリティが組み込まれるために、組織はDevOpsに適切なセキュアソフトウェア開発ライフサイクル（SSDLC）を採用すべきです。DevSecOpsとして知られているこのアプローチは、クラウド環境内で運用する組織にとって特にふさわしいものです。

一般的に、組織はDevSecOpsによって、セキュリティを追加で開発するのではなく、ワークフローに組み込むことができます。これにより、開発者とセキュリティの専門家は、サイバーセキュリティのためにセキュアな構成を継続的に監視、修復、管理するという共通の目標を持ちながら、アジャイルでレジリエントなソリューションの開発を推進することが可能となります。

クラウドプラットフォームは通常、ソフトウェアパイプラインの開発とデプロイメントを加速するための包括的なツールとサービスの一式をユーザーに提供しています。しかし、このようなスピードの向上によって、対応するソフトウェアの脆弱性も高まる傾向にあります。

クラウドで安全にDevSecOpsパイプラインを設計、実装、運用するために、組織は業界標準のDevSecOpsプロセスをベンチマークとして成熟度を評価し、ギャップ分析を実施すべきです。つまり、DevSecOpsのフレームワークは、パイプラインの6つの主要なステージ（設計、開発、ビルド、テスト、デプロイ、運用／監視）をカバーし、ベストプラクティスにマッピングされた各ステージのセキュリティケイパビリティとコントロールを備えている必要があります（図5参照）。

詳細な成熟度評価とは別に、このフレームワークを活用して、オンプレミス環境とクラウド環境の両方で、組織のDevSecOpsプロセスの高度化に向けたヘルススコアカードと戦略ロードマップを作成することもできます。この段階で、組織のクラウドアプリケーションとパイプラインのセキュリティを強化するために、静的アプリケーションセキュリティテスト（SAST）、動的アプリケーションセキュリティテスト（DAST）、コンテナセキュリティ、クラウドコンプライアンスモニタリングなどのセキュリティコントロールも設計し、実装する必要があります。

図5：DevSecOpsパイプラインの主要な6つのステージ

ステップ 3

ゼロトラスト原則の導入検討

組織は、クラウドアーキテクチャ全体におけるゼロトラスト原則の導入を検討すべきです。ゼロトラスト原則の包括的な導入と実装には、ユーザー、ワークロード、データ、ネットワーク、デバイスの5つの柱にわたる強力なケイパビリティの開発が必要です。この5つの縦方向の柱は、テレメトリーおよびアナリティクス、自動化およびオーケストレーションという2つの横方向の柱によって支えられる必要があります（図6参照）。

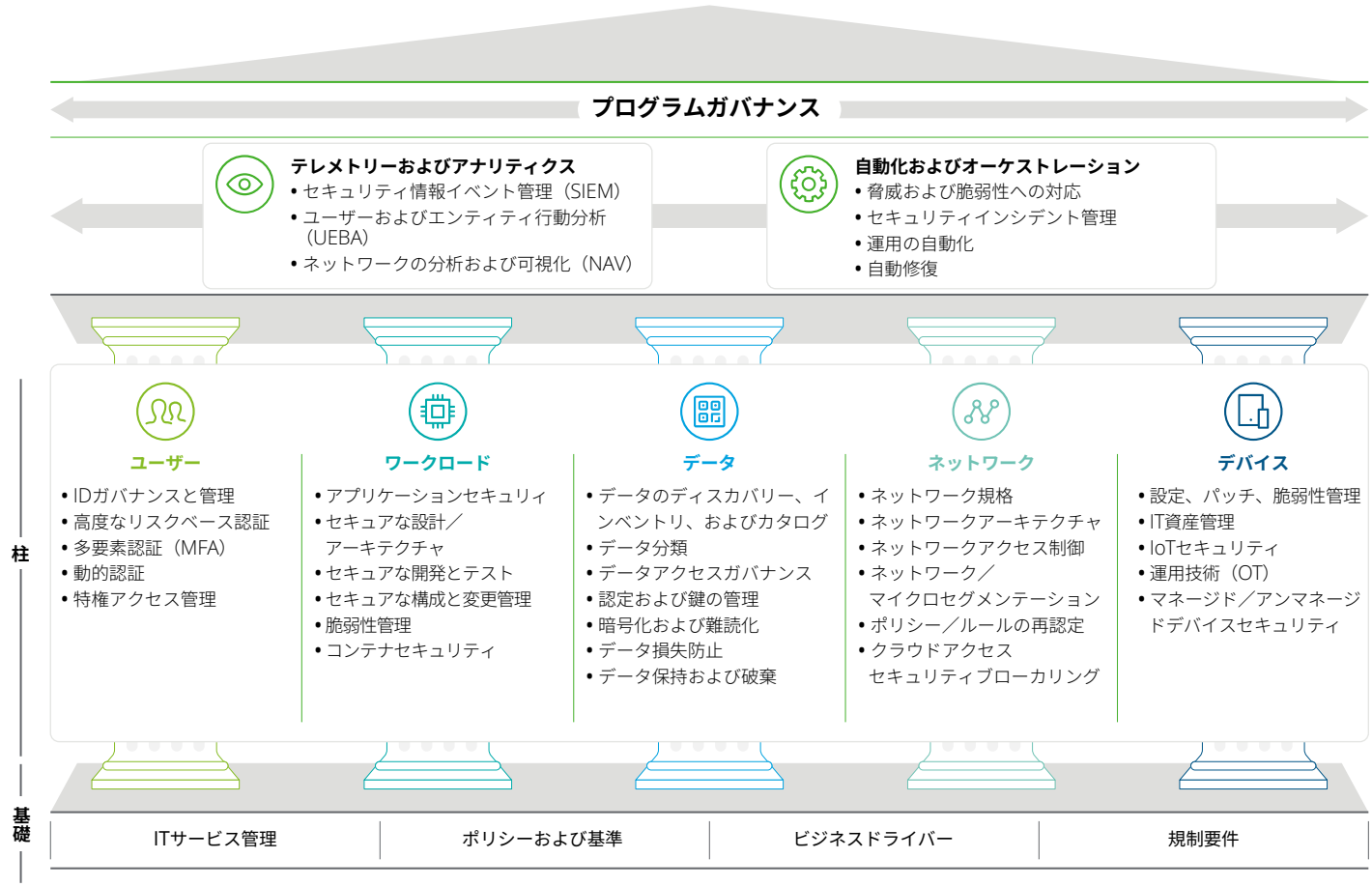
それぞれの柱の成熟度レベルは各組織で異なるため、様々なゼロトラストのマイルストーンをカバーするためにカスタマイズしたロードマップを作成する必要があります。主要な初期活動には、ゼロトラストの範囲の決定、基礎的なケイパビリティの確立、トラフィックフローやアプリケーション関係のマッピング、ユーザー管理のフェデレーションと一元化、データの検出、インベントリ、暗号化の確立などが含まれます。同時に、組織はテレメトリーおよびアナリティクス、自動化およびオーケストレーションの実装も開始し、これらのケイ

パビリティが時間をかけて成熟するための十分な道筋をつけるべきです。

その後、組織はデバイスセキュリティサービスを実装し、クラウドの導入をサポートするために、広域通信網（WAN）およびクラウドとオンプレミス環境間のネットワークセキュリティを保護し、ソフトウェア定義の境界（SDP）を使用してネットワークアクセスを制限し、ゼロトラストのクラウド環境を構築し、クラウドネイティブのセキュリティケイパビリティをオンプレミス環境に統合または拡張する必要があります。

組織が自社のアプリケーションを評価し、ゼロトラストのクラウド環境に移行させた後は、アプリケーションの戦略を定義する必要があります。これには、クラウドに適さないシステムの仮想化、マイクロセグメンテーションの実装、そして最終的に、ゼロトラストの5つの基本的な柱にわたる追加の統合と先進的なケイパビリティの導入を通じて、ゼロトラストケイパビリティをさらに進化させることが含まれます。

図6：5つの縦方向の柱にわたるゼロトラスト原則の包括的導入



ステップ 4

暗号化およびトークン化による保存データおよび転送中データの保護の設計

使用中、保存中、転送中のすべての段階でデータを十分かつ適切に保護するために、組織はデータ保護のためのマネージドサービスの設計、実装、デプロイメントにおいてクラウドネイティブの視点を取り入れるべきです。

ここで重点を置く主な分野には、以下のものを含める必要があります。すなわち、暗号化、トークン化、マスキングを使用したクラウド上のデータ保護の設計と統合、CSPが提供するマネージドキーサービスやクラウドホスティング専用のハードウェアセキュリティモジュールを含む暗号化および鍵管理、証明書管理と相互TLS認証などです。

組織のサイバーセキュリティ業務のクラウドへの拡大

サイバーセキュリティ業務をパブリッククラウドのワークロードのセキュリティ対応にまで拡大するためには、組織は情報資産の全体的なサイバー状況認識を維持し、インシデント対応、処理、調査のプロセスをパブリッククラウドに適応させる必要があります（図7参照）。

図7：組織のサイバーセキュリティ業務を拡大するための2つのステップ

ステップ 1

情報資産の全体的なサイバー状況認識を維持する

情報資産の全体的なサイバー状況認識を維持するために、組織はクラウド資産とオンプレミス資産のセキュリティ監視をサイロ化して行うことを避ける必要があります。しかしそのためには、クラウド環境で導入されるすべての新しい資産とテクノロジーを網羅する十分な監視ケイパビリティが不可欠です。また、ロギングと監視のソリューションを既存のオンプレミスソリューションとシームレスに統合し、単一で統合されたセキュリティインシデントイベント監視（SIEM）ソリューションを構築する必要もあります。

組織は、すべての監視およびロギング活動を一元化するために、ダッシュボードのような「Single Pane of Glass」のアーキテクチャに目を向けるべきです。このような単一のアクセスコントロールポイントを持つことの利点として、すべての監視およびロギング活動の一貫した視点、データの保存と保持の管理のしやすさ、アクセスコントロールと監査の一元化が挙げられます。

ただし、注意すべき点として、組織はこの中央リポジトリに転送されるデータの安全性を確保する措置を講じる必要があります。

CSPはそれぞれ、様々なサービス、コンテナ、アプリケーション、インフラを監視／管理するための独自のソリューションを持っていますが、これら全体を通していくつかのベストプラクティスが見られます。例えば、コンプライアンスを確保するためのログ保存ストレージの設定（組織の要件と適用される規制に従って）、セキュリティとアクセス分析のためのログエクスポートの設定、機密性の高い業務のデータにアクセスしたユーザーを追跡するための監査ログの有効化、関連する基準に準拠するために機密ログデータをフィルタリングするためのルールの作成などです。

ステップ 2

インシデント対応、処理、調査のプロセスをパブリッククラウドに適応させる

さらに、組織はCloud Security Posture Management（CSPM）やCloud Workload Protection Platform（CWPP）のコンプライアンス違反アラートをITSMツールに統合する必要があります。これを実現するためには、CSPM／CWPPツールのケイパビリティをクラウドコンプライアンスの監視やクラウドセキュリティポスチャ管理に利用する前に、まずクラウドセキュリティコントロールのフレームワークのベースラインを設定する必要があります。その後、継続的なクラウドコンプライアンスの指標と分析方法を確立してから、セキュリティアラートをITSMツールに統合する必要があります。

セキュリティの自動化における新たな進歩に伴い、CSPMとCWPPは、Cloud Native Application Protection Platform（CNAPP）へと進化し始めました。このプラットフォームは、CWPPとCSPMの機能を1つに統合することで、クラウドにおけるアプリケーションセキュリティのライフサイクル全体にわたるアプローチに焦点を当てたものです。

ほぼリアルタイムでコンプライアンス違反が自動修復されれば、リスクに晒される時間は数時間から数分にまで大幅に縮小されることになります。この実現に向けて、組織は、インシデント対応プロセスをDevSecOpsのスピードで運用する方法も検討する必要があるでしょう。

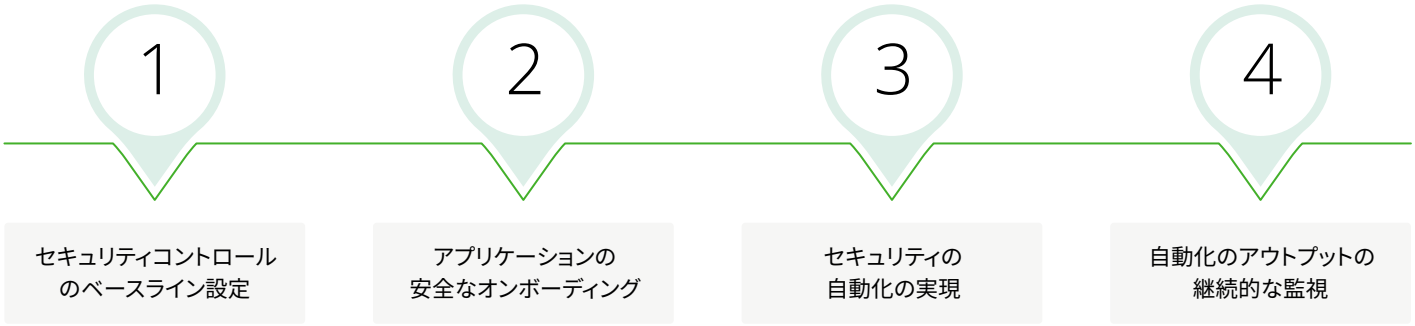
クラウド技術を活用したセキュリティコントロールの自動化

セキュリティコントロールを自動化しなければ、クラウド上のビジネス機能やIT機能に自動化がもたらす変化のスピードにセキュリティ機能が追い付くことはできません。

クラウドプラットフォームへの移行は、従来のコントロール手法とは異なるアプローチを必要とするリスクをもたらします。こうしたリスクには、アウトソーシングリスク、変更管理リスク、責任共有についての誤解によって生じるリスクなどがあります。

このようなリスクに対処するには、セキュリティコントロールの自動化が必須です（図8参照）。

図8：セキュリティコントロールの自動化を導入するための4つのステップ



ステップ 1

セキュリティコントロールのベースライン設定

セキュリティコントロールを自動化する前に、セキュリティの観点から許容基準を客観的に定義するために、ベースラインを確立しなければなりません。このベースラインに含まれる対象は、アプリケーションのセキュリティ構成や技術構成、クラウドプラットフォームサービスとの統合があります。

これは明確なポリシーおよび基準を持ち、それらとの関連付けおよび最新化されたセキュリティパターンを持つことによって達成されます。アプリケーションユーザーは、セキュリティパターンを参照することで、クラウドにアプリケーションを安全に移行しようとする際に「適切な」状態がどのようなものであるかを理解することができます。

ステップ 2

アプリケーションの安全なオンボーディング

この作業は、手動レビュー用のチェックリスト、セキュリティ評価、ポイントインタイムの自動スキャンなどを用いて実施し、セキュリティコントロールの現状を把握します。

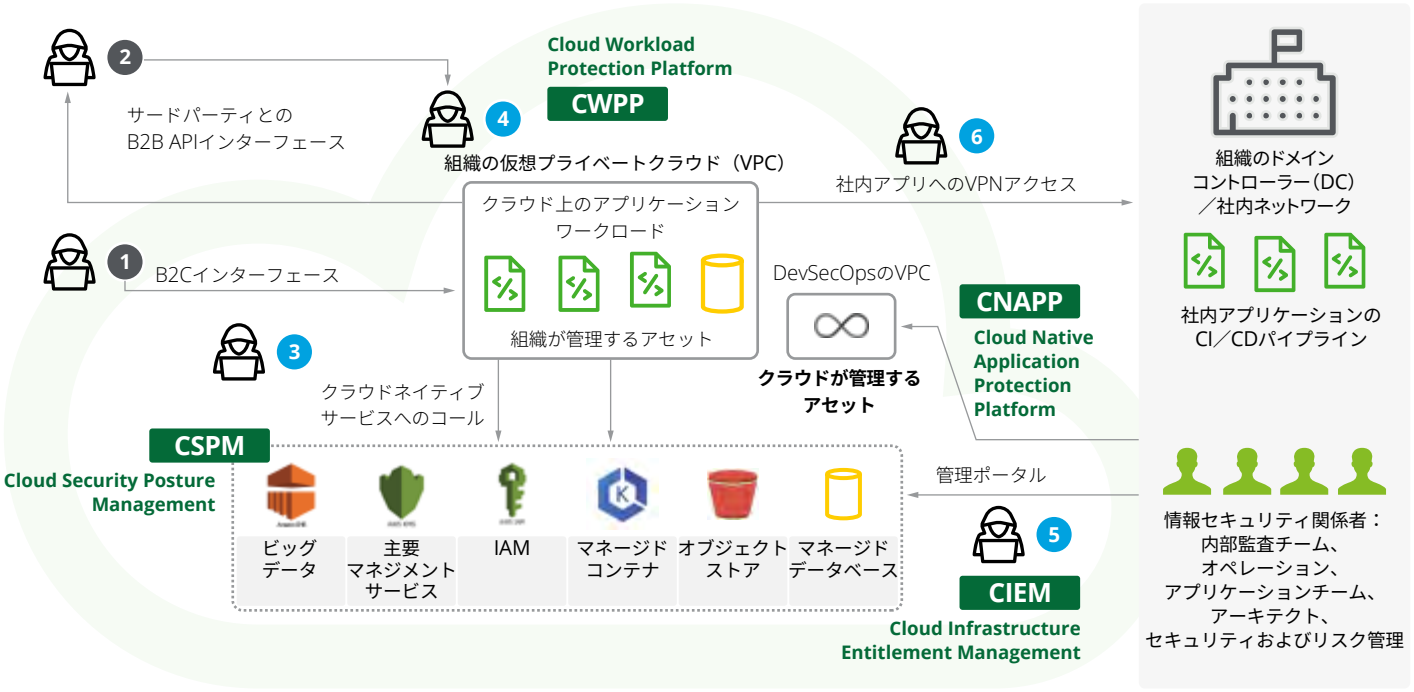
その後、アプリケーションに対するハードニングプロセスとして、検出された問題や不備の修正が行われます。これにより、セキュリティ自動化をアプリケーションがクリーンに整備された状態から開始できるようにします。

以上のようなアプリケーションのオンボーディングを正しく行わないと、適切に修正されなかったアプリケーションの問題や不備が残存することによって、セキュリティの自動化の開始後に、手作業で分析しなければ解決できないような数多くの問題が発生するリスクがあります。

ステップ 3

セキュリティの自動化の実現

図9：クラウドにおけるセキュリティの自動化



セキュリティを自動化できる個所は複数あります。以下にその例をいくつか列挙します。

- Cloud Security Posture Management（CSPM）：アプリケーションのワークロードが消費するクラウドサービスにおけるセキュリティの設定ミスの検出（場合によっては修復も）を自動化します。
- Cloud Workload Protection Platform（CWPP）：サーバーのワークロード（例：コンテナなど）を静的に（例：コンテナイメージがパイプラインで構築される際のスキャンなど）、および実行時に動的に（例：コンテナが起動されたとき、実行時のサービスとトラフィックの異常や脅威パターンをCWPPが監視するなど）保護します。
- Cloud Infrastructure Entitlement Management（CIEM）：クラウドやマルチクラウド環境における様々な主体（ユーザー、サービス、ロールなど）のIDとアクセス権限を管理します。
- Cloud Native Application Protection Platform（CNAPP）：クラウドにおける開発から構築、デプロイ／運用に至るまで、一貫したセキュリティのアプローチと備えを提供するために、上記3つのテクノロジーすべての要素を組み合わせます。
- Infrastructure as Code（IaC）のセキュリティ：DevSecOpsプロセスに沿ったセキュアスキャニング／セキュアデプロイメントによるIaCのセキュリティ確保は、クラウドにインフラをデプロイする際の設定ミスをなくすためにも重要です。

組織は、上に例示したものを実装するため、様々な戦略を採用し、適切なテクノロジーと製品を選択することができます。セキュリティの自動化を実現するものとしては、クラウドネイティブサービスのほか、様々なサードパーティ製品があり、組織は選択肢を十分に評価したうえで、ニーズに合ったソリューションを選択することができます。

ステップ 4

自動化のアウトプットの継続的な監視

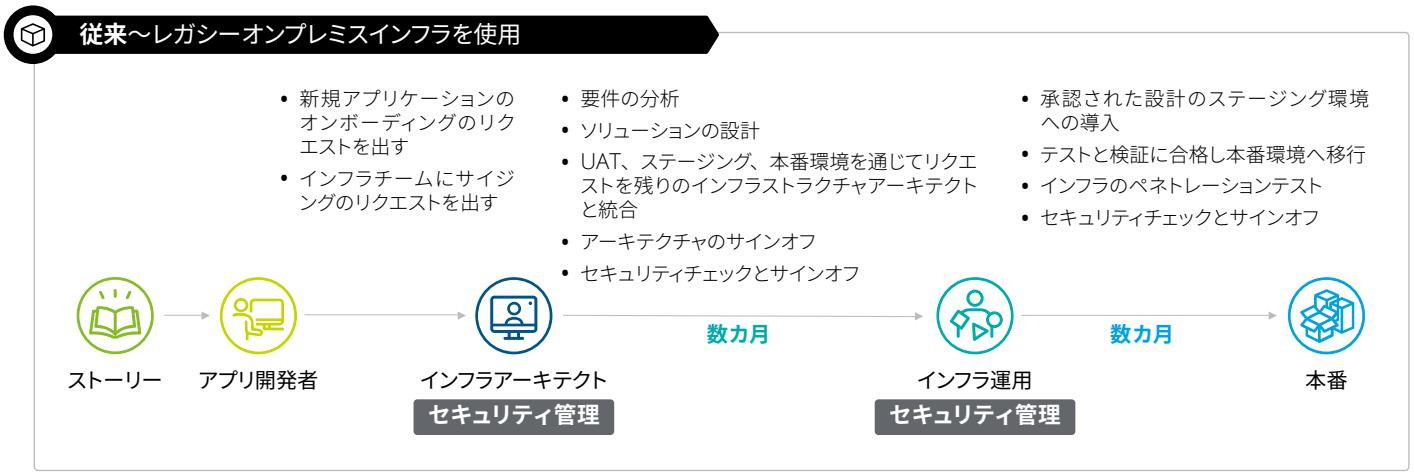
セキュリティコントロールを自動化するための重要な要素は、自動化によって生成されたアラートを監視することです。

上記のツールは、組織が使用しているSIEMソリューションに取り込まれ、自動化によってセキュリティイベントが検出されたときに、運用チームが適切な措置を講じるようアラートをあげます。

クラウド技術がセキュリティに与える影響の例

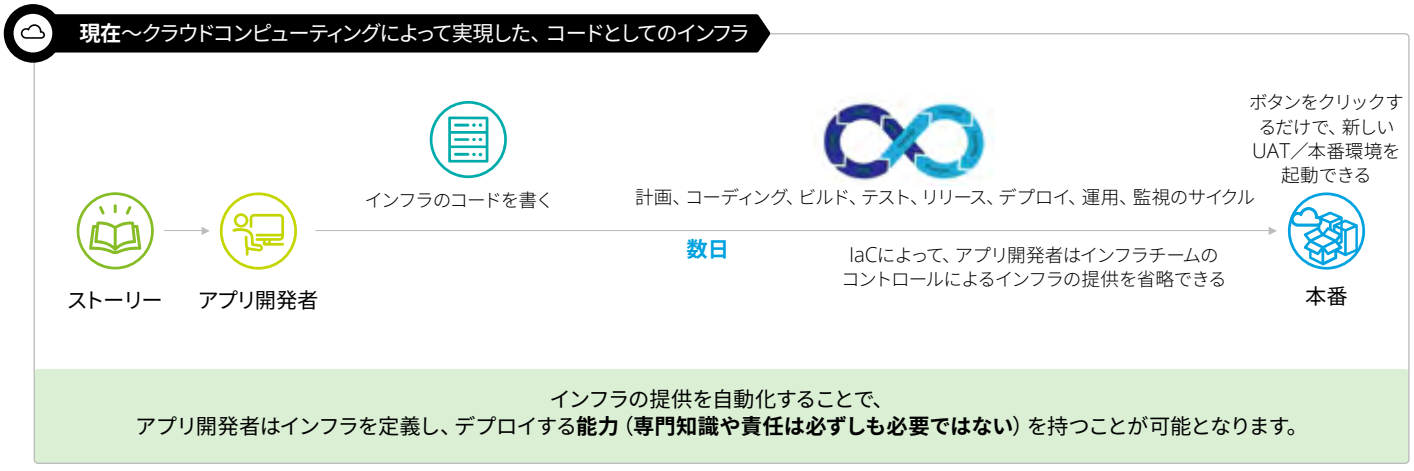
Infrastructure as Code（IaC）がセキュリティに与える影響を考えてみましょう。IaCでは、クラウドプラットフォームに内在する仮想化技術により、インフラをスクリプト言語で定義し、クラウドプラットフォームのAPIを通してオンデマンドでクラウド上のインフラを変更することができます。

図10：レガシーインフラのデプロイメント



上の図に示されている通り、従来のレガシー／オンプレミスインフラでは新しいインフラ環境の構築には時間を要することが多く、大企業では構築に数カ月を要することもありました。

図11：クラウド上でInfrastructure as Code（IaC）を使用したインフラストラクチャのデプロイメント



インフラの提供を自動化することで、
アプリ開発者はインフラを定義し、デプロイする**能力（専門知識や責任は必ずしも必要ではない）**を持つことが可能となります。

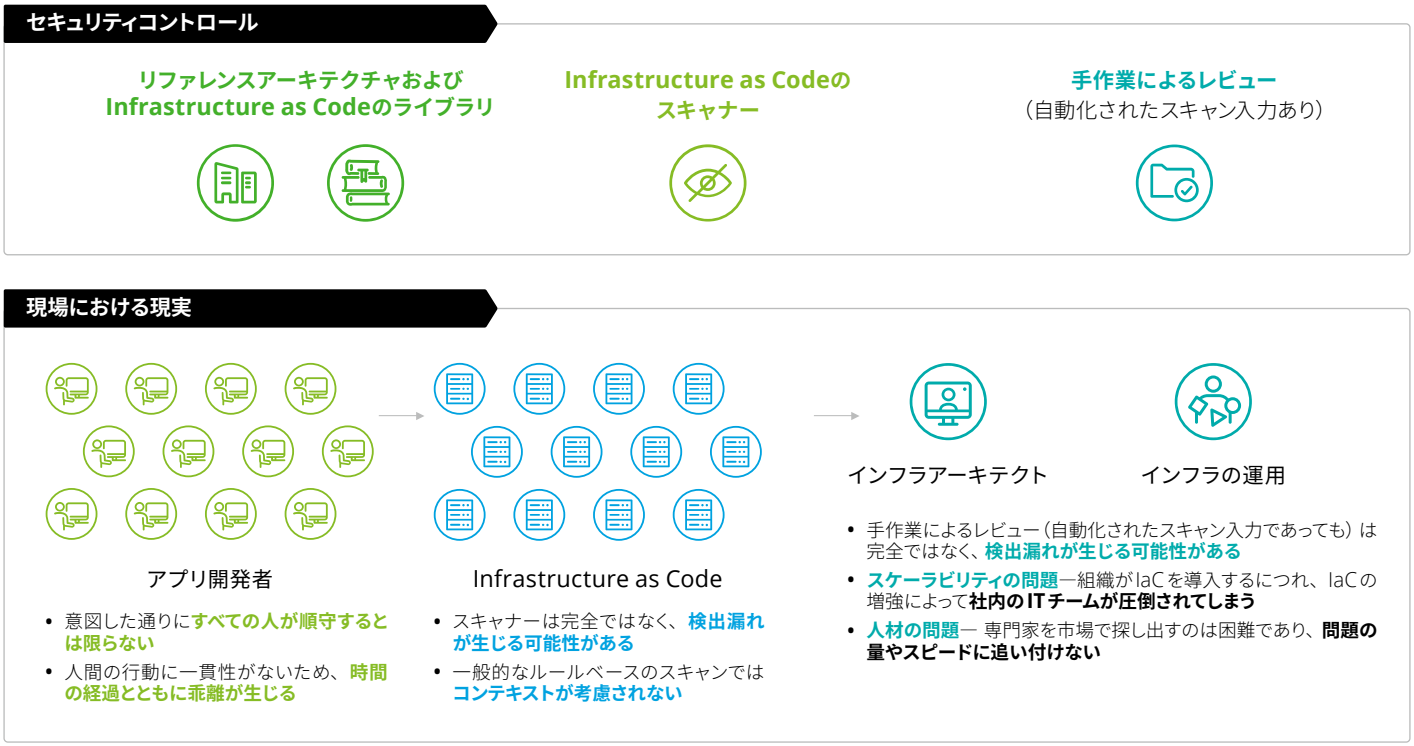
企業にとって数カ月かかっていた活動は、IaCの利用により、数週間や数日どころか、わずか数時間に短縮されます。しかし、このような自動化技術の飛躍は、セキュリティに重大な影響を及ぼす可能性があります。その主なリスクとしては、**インフラ構成が安全でなかったり、既存の企業セキュリティポリシーに準拠していなかったり、適切に設計されていなかったりする懸念が挙げられます。**

組織が、既存のセキュリティコントロールとガバナンスの方式を用いてこの問題に対処しようとした場合、以下のように対応すると考えられます。

- IaCを変更するたびに、専門家によるレビューを受けること
- IaCのリファレンスアーキテクチャとテンプレートを提供すること
- IaCのスキャンはDevSecOpsパイプラインで自動化された方法で行うこと

しかし、大規模な運用において、従来のレビュープロセスと同様の手作業によるコントロール（例えば、専門家によるレビュー）には大きな負担があり、このアプローチは長期的には十分な成果を上げることが難しい可能性があります。特に、組織がクラウドベースのソリューションに対して多数の変更と新機能を積極的に導入し、自動化の力とIaCの機能を最大限に活用しようと考えた場合、こうした運用上の課題が顕著になると考えられます。

図12：Infrastructure as Code（IaC）の一般的なセキュリティコントロール

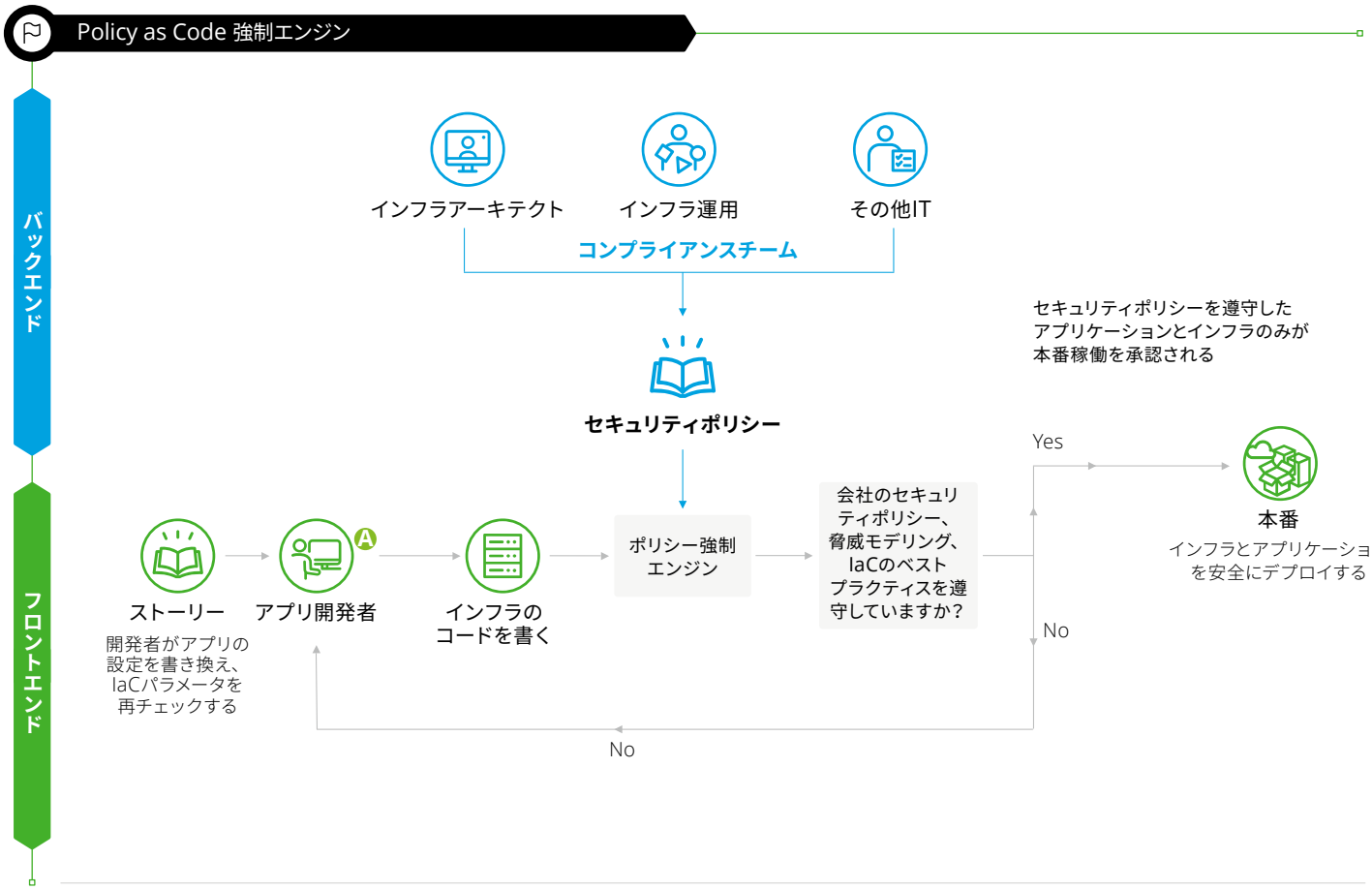


この問題を解決するためのアプローチの1つは、手作業による確認に替えてポリシー強制エンジンを導入し、セキュリティコントロールを自動化することです。

このようなサービスに開発者のコードを取り込むことで、IaCのベストプラクティスとデザインパターンを直接IaCに組み込むことができ、IaCのセキュリティ面が開発者まかせになってしまうことを防ぎます。

このPolicy as Codeアプローチを採用することで、セキュリティポリシーが自動的に強制されるため、組織のインフラがセキュリティポリシーに準拠していることを保証することにも役立ちます。
また、ポリシーの遵守を確保しながらも、IaCにおける自動化のボトルネックとなっていた、手作業による確認と承認というタスクを取り除くことができます。

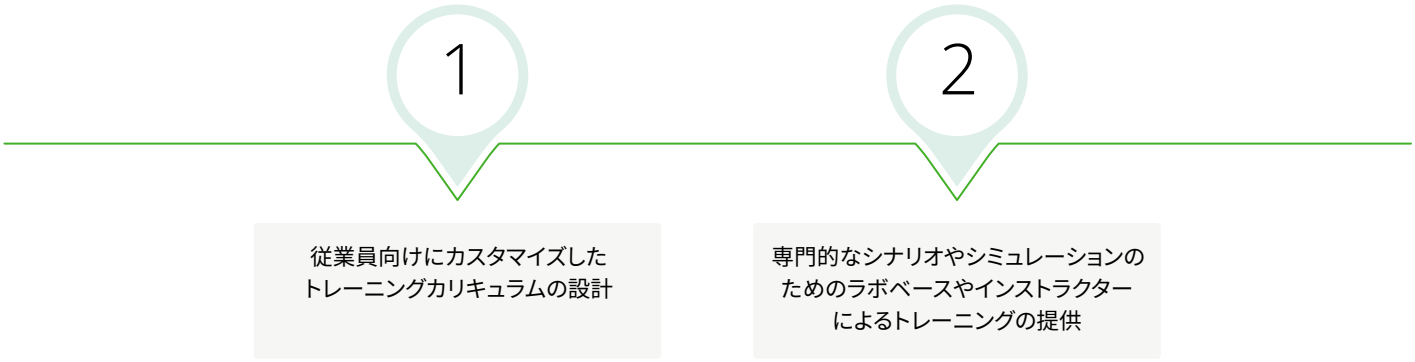
図13：コードとしてのポリシー



クラウドの適切なスキルセットの確保

組織がパブリッククラウドのワークロードとリスクを管理するための適切なスキルセットを確実に身に着けるためには、従業員向けにカスタマイズしたトレーニングカリキュラムを設計し、クラウドとテクノロジー関連のトピックを網羅する必要があります。また、特定のシナリオを管理するために必要なスキルを従業員に習得させるには、ラボベースのトレーニングやインストラクターによるトレーニングも役立ちます。

図14：適切なスキル確保のための2つのステップ



ステップ1

従業員向けにカスタマイズしたトレーニングカリキュラムの設計

組織全体のクラウドやテクノロジー関連のスキルを強化するために、組織は従業員向けにカスタマイズしたトレーニングカリキュラムを設計することでメリットを享受できます。特に最前線のITチームにとっては、サイバー攻撃のシミュレーションができるトレーニングカリキュラムは、実際のサイバー攻撃への対応を学ぶうえで有益です。

このようなカリキュラムによって、組織の実環境を忠実に模した仮想環境が提供されることで、アプリケーション開発者は、アプリケーションに対する本物そっくりの攻撃をリアルタイムで体験し、組織のインフラを効果的に保護するために必要なセキュリティに関する洞察と、組織を超えたコミュニケーションスキルを身に着けることができます。

その他のトレーニング分野には、継続的なコンプライアンス、セキュリティ監視、セキュリティ構成などのサイバークラウドに関するトピックから、成熟度計画、ロードマップ、SAST／DASTなどのDevSecOpsに関するトピック、ゼロトラストを成熟させるまでのロードマップやゼロトラストリファレンスアーキテクチャの設計などのゼロトラストに関するトピックも含まれます。

ステップ2

専門的なシナリオやシミュレーションのためのラボベースやインストラクターによるトレーニングの提供

多くの場合、組織が直面する可能性のある特定の状況では、専門的なトレーニングセッションが必要になります。例えば、組織が移行を検討している新しいプラットフォームについて、ITチームやセキュリティチームが習熟度を高める必要がある場合や、組織内に存在する特定の問題を解決する必要がある場合などです。

このようなトレーニング活動は、従業員がより実践的な経験を積むことができるように、ラボやその他のインストラクター主導のデモンストレーションを通じて実施することが理想です。場合によっては、他の組織上の目標をトレーニングのカリキュラムと組み合わせることも可能です。例えば、トレーニングセッションの一環として、実用最小限の製品（MVP）やプロトタイプの作成を行うことなどが挙げられます。

将来に向けて

サイバー攻撃の脅威は絶えず変化しており、悪意ある攻撃者によって常に新たな攻撃の手口が生み出されています。 これらの手口のいくつかには、AIやクラウドを活用した自動化など、ビジネスやテクノロジーの目標を推進するために使用されているものと全く同じテクノロジーが利用されています。組織が急速にクラウドサービスを採用しており、また、これらのクラウドサービス自体の進化するペースも速い環境下において、サイバー攻撃の脅威は加速的に増大しています。

本レポートで繰り返し述べているように、これらの脅威の一歩先を行くには、組織がクラウドを採用する最初の段階から、統合的なセキュリティバイデザインのアプローチを採用する必要があります。

とはいえ、非常に良く設計された統合戦略であっても、適切なケイパビリティを有するチームによって実施されなければ失敗に終わります。

多くの組織では、サイバーセキュリティチームは組織の他の部門からサイロ化されている傾向があり、人数が少なかったり、適切な権限が割り当てられていなかったりすることもあります。組織がクラウドへの移行を進めるにつれ、この問題はより深刻化し、移行プロセスそのものを脅かす可能性もあります。

したがって、ここで急務となるのが、クラウドチームとサイバーチームが共有オペレーティングモデルとして協力体制を構築し、人材オペレーティングモデル、DevSecOps、マイクロサービスなど、クラウドジャーニーの様々な側面を考慮した活動を共同で推進できるようにすることなのです。

このような共有オペレーティングモデルを導入することで、クラウドチームとサイバーチームのより高度なコラボレーションが可能になるだけでなく、リスク管理、コンプライアンス、その他のセキュリティ対策がITインフラレイヤーの管理に最初から組み込まれるため、組織はクラウドプラットフォームを活用してビジネスパフォーマンスを向上させたり、顧客体験を向上させるなど、より付加価値の高い取り組みに注力できるようになります。

クラウド移行のプロセスは、組織にとって自社のセキュリティモデル、ツール、ケイパビリティを再評価する良い機会であると言えます。クラウドジャーニーに乗り出す今こそ、組織が自社のコントロールフレームワークを再検討し、クラウドとサイバーに対するアプローチをより統合した形で強化し、最終的には今後長期にわたって自社のオペレーティングモデルの基盤となる安全なクラウドプラットフォームを構築するチャンスなのです。

執筆者および貢献者

執筆者

Amol Dabholkar
アジアパシフィック地域サイバークラウドリーダー

主な貢献者

Karen Grieve
ディレクター

Ho Kyoo Hahn
ディレクター

David Hawks
パートナー

石井 友貴
マネージングディレクター

Eric Leo
ディレクター

Max Y Lin
パートナー

Joanne Lu
パートナー

Rahul Mengale
ディレクター

Tonny Xue
パートナー

問い合わせ先

デロイト トーマツ サイバー合同会社
Tel: 03-6213-1900
E-mail: ra_info@tohmatsu.co.jp

Deloitte.

デロイト トーマツ

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーであるデロイト トーマツ合同会社ならびにそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイトトーマツ税理士法人、DT弁護士法人およびデロイト トーマツ グループ合同会社を含む）の総称です。デロイトトーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約30都市に約1万7千名の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト（www.deloitte.com/jp）をご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイトネットワーク”）のひとつまたは複数を指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。DTTLおよびDTTLの各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。DTTLはクライアントへのサービス提供を行いません。詳細はwww.deloitte.com/jp/aboutをご覧ください。
デロイト アジア パシフィック リミテッドはDTTLのメンバーファームであり、保証有限責任会社です。デロイトアジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市（オークランド、バンコク、北京、ベンガルール、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、ムンバイ、ニューデリー、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリー、リスクアドバイザリー、税務、法務などに関連する最先端のサービスを、Fortune Global 500®の約9割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促し、より豊かな経済、公正な社会、持続可能な世界の実現に向けて自ら率先して取り組むことを通じて、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来175年余りの歴史を有し、150を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をパーパス（存在理由）として標榜するデロイトの約415,000名の人材の活動の詳細については、(www.deloitte.com）をご覧ください。

Member of
Deloitte Touche Tohmatsu Limited

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301