# ゼットスケーラーのCSPM

## ――クラウドセキュリティポスチャ管理（Cloud Security Posture Management）

zscaler™

# 目次

## はじめに

我々は今、急速に変化する世界に生きています。あらゆる業界でデジタルトランスフォーメーションが進んでいることから、ソフトウェアがあらゆるビジネスに不可欠な要素になっています。競争力を維持するには、新しいアプリケーションを迅速に開発する必要があり、そのような急速な変化に対応できる唯一の環境が、パブリッククラウドなのです。

しかし、セキュリティ、リスク、ビジネスのリーダーは、次のような多くの問題に直面することになります。

1. クラウドインフラストラクチャの構成ミスに起因するデータ侵害によって、膨大な数の機密度の/高い顧客データが流出すると、法的責任や金銭的損失を被ることになります。
2. クラウドベースのワークロードに対する継続的コンプライアンスを従来のオンプレミスのツールとプロセスで達成することはできません。
3. 組織においてクラウドの採用の拡大すると、クラウドガバナンスの実装に関する課題（可視性、事業部全体へのポリシーの適用、クラウドセキュリティコントロールに関する知識の欠如）もまた増加し続けます。

本資料では、クラウドプロバイダの基本機能だけを提供するネイティブセキュリティソリューションを始めとする、クラウドアプリケーション開発の速さとセキュリティ適用の遅さのギャップの拡大について紹介し、セキュリティポスチャの動的な可視化とセキュリティ標準の適用にあたってのセキュリティチームと開発チームによるシームレスなコラボレーションの必要性について解説します。

「クラウドが安全かどうかを議論するのではなく、重要なのは、クラウドを安全に使用することです。」

- ガートナー

## クラウドには異なるセキュリティアプローチが必要である

### データ侵害はビジネスに重大な影響を及ぼす

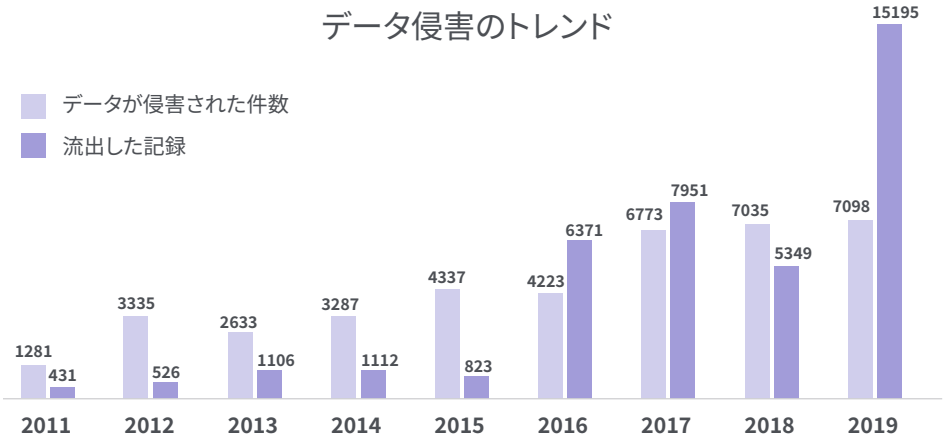
IBMの2019年版「Cost of a Data Breach」レポート[1]は、データ侵害の平均コストを全世界で390万ドル、米国で820万ドルと推定しています。顧客の信頼の損失と後のビジネスの損失が、この平均コスト推定額の最大の要素です。

## データ侵害の平均コスト

| 全世界 | アメリカ |
| --- | --- |
| 390 万ドル | 820 万ドル |

[1]「Cost of a Data Breach Report」、IBM、2019年

Risk Based Securityの最近のデータ侵害レポート[2]によると、2019年に150億件のレコードが外部に流出したと報告しており、前年までより大幅な増加を示しています。データベースの構成ミスに起因する4件のデータ侵害によって、2019年第4四半期に67億件のレコードが外部に流出しました。




IBM X-Force Threat Intelligence Indexの2020年版レポート[3]によると、構成ミスが原因で流出したレコードが前年比で10倍近く増加しており、2019年に侵害されたレコード全体の86%を占めています。

## クラウドにおける責任共有型セキュリティ

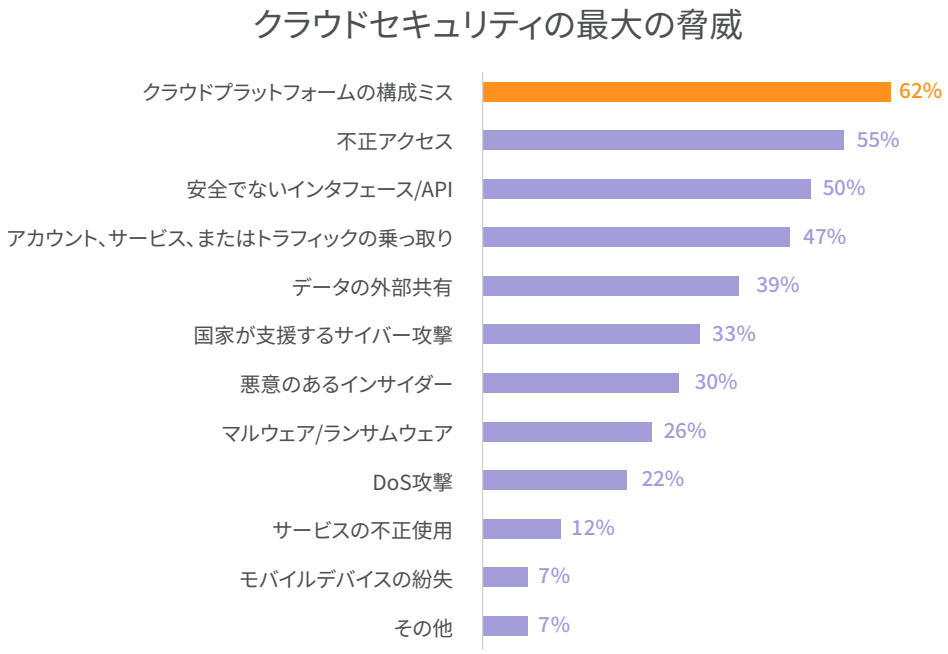
クラウドサービスプロバイダ（CSP）は、ハードウェアやソフトウェアのさまざまなコンポーネント（コンピューティング、ストレージ、データベース、ネットワーキング）を使用してインフラストラクチャを構築しています。CSPは、クラウドのセキュリティに責任を負います。クラウドインフラストラクチャのセキュリティに多大な投資を行い、複数のコンプライアンス認定を提供しています。


CSPは基盤であるインフラストラクチャの安全を保証しますが、お客様の責任で、アプリケーションを正しく構築し、データが外部に流出しないようにし、構成を安全に設定することを保証する必要があります。これは、ホストとコンテナのクラスタ、IaaS、PaaS、SaaS、セキュリティサービスなどのお客様が利用するすべてのクラウドサービスに該当します。

[2]「2019 Year End Data Breach QuickView Report」、Risk Based Security、2020年
[3]「IBM X-Force Threat Intelligence Index」、2020年

## 構成ミスはセキュリティの最大の脅威である

多くのセキュリティ担当者が、構成ミスはクラウドセキュリティの最大の脅威であると指摘しています[4]。しかし、それ以外の脅威と考えられる事象（不正アクセス、安全でないインタフェース、アカウントの乗っ取りなど）の多くにも、構成ミスが関係しています。




構成ミスに起因する脅威を、研究アナリストも十分に認識しています。ガートナーの「Innovation Insight for Cloud Security Posture Management」レポートでは、次のように説明しています。「クラウドサービスに対する攻撃の成功のほとんどは、顧客の構成ミス、管理ミス、操作ミスが原因だ。セキュリティやリスク管理のリーダーは、クラウドセキュリティのポスチャ管理プロセスやツールに投資することで、これらのリスクをプロアクティブとリアクティブの両方で特定し、修正する必要がある[5]」。

## 従来型セキュリティアプローチでは対応できない

ネットワークはかつては、データベースやファイル共有に保存された価値の高い情報を保護する、信頼できる安全な境界に囲まれた環境でしたが、クラウドでは、いくつかの簡単な構成変更だけで、データベースがインターネットに公開されてしまう可能性があります。データストアを外部から遮断せずに開発を進め、その構成が開発の終了後も残され、意図しない形で本番環境へと移行してしまう可能性があります。

## 従来型セキュリティ評価では遅すぎる

従来型のセキュリティやコンプライアンスの監査は、面倒で時間がかかる手動プロセスです。監査担当者は、ITチームに面談し、コンプライアンスの証明として製品構成のスクリーンショットを取得します。クラウドでは、クラウドインフラストラクチャが目まぐるしく変更されるため、監査の完了までにインフラストラクチャが何度も再構築される可能性があります。セキュリティとコンプライアンス保証の自動化こそが、クラウドでの開発の速度とリリースの頻度に追いつける唯一の方法です。

[4]「Cloud Security Report」、Cybersecurity Insiders、2018年
[5]「Innovation Insight for Cloud Security Posture Management」、2019年

### コンプライアンスの証明にあたっての課題

法規制の対象となる分野では、小売分野のPCI DSS、医療分野のHIPAA、金融サービス分野のFFIEC、NISTなどの分野ごとのベンチマークを遵守する必要があります。企業は今もなお、担当者との面談によるコンプライアンス評価を主な手段として実施しています。証拠を収集し、それをコントロールフレームワークにマッピングするのは、大掛かりな作業です。これらのコンプライアンスフレームワークによって、継続的に遵守が求められる高レベルのコントロールが提供されます。多くのコンプライアンスフレームワーク（PCI DSS など）は、継続的コンプライアンスの概念を要件として取り入れていますが、これらのいずれも問題も、急速に変化するクラウドワークロードによってさらに複雑になります。

### クラウドサービスプロバイダは基本機能を提供する

CSPはセキュリティとコンプライアンスポスチャを可視化するためのツールを顧客に提供しています。これらの製品は、基本的なセキュリティポリシーに対応し、限定的なコンプライアンスフレームワークをサポートしますが、組織全体のセキュリティとコンプライアンス保証を可能にするには、大掛かりな統合とカスタム開発が必要です。その結果、パブリッククラウドにアプリケーションを展開する組織は、開発の速度とセキュリティリスクのトレードオフを強いられることになります。数百人の開発者が継続的に新しいコードを本番環境にリリースする大規模の組織は、クラウドセキュリティとコンプライアンス保証の完全に自動化されたソリューションを実装する必要があります。

## クラウドセキュリティポスチャ管理（CSPM）を採用する

ガートナーによって定義された、従来型のセキュリティに存在する複数のコンプライアンスの問題を解決する新しい製品カテゴリは、セキュリティとコンプライアンス保証を自動化し、クラウドインフラストラクチャ構成に対する適切なコントロールのニーズを解決する、クラウドセキュリティポスチャ管理（CSPM）と呼ばれるものです。2020年にはCSPMソリューションの採用が確実に増加しており、今後数年で25%に達すると予測されています。これこそが「必須」のクラウドセキュリティツールであることを多くの組織が認識するようになっています。

## ゼットスケーラーのCSPMに対するアプローチ

多くのCSPMソリューションに共通する課題として、ポイント製品であるために大規模組織のセキュリティやデータ保護のツールとの統合できず、サイロ化された可視性しか提供できず、企業の既存のプロセスにCSPMを採用するのが困難である点が挙げられます。

ゼットスケーラーのCSPMは、ゼットスケーラーのクラウドセキュリティプラットフォームの包括的な100%クラウド提供型データ保護機能の一部であり、アプリケーションの構成ミスを自動的に特定して修復することで、統合の問題を解決します。

ゼットスケーラーのCSPMは、クラウドのセキュリティとコンプライアンスを自動化する広範なイノベーションと製品機能を提供することで、継続的な可視性を実現し、セキュリティポリシーとコンプライアンスフレームワークの遵守を保証します。

### 実際の構成の収集

ゼットスケーラーのCSPM アプリケーションに、お客様のクラウド環境（AWS、Azure、Office 365、Googleクラウド、その他の任意のCSP）へのアクセスが許可されます。次に、APIを利用して、クラウドインフラストラクチャの実際の構成が収集されます。少数ではありますが、ポリシーによっては、エージェントのインストールが必要になる場合があります。

### 構成ミスの特定

ゼットスケーラーのCSPMは、見つかった構成を内蔵のセキュリティポリシーと比較し、セキュリティポリシーとリソースレベルで構成ミスを特定します。また、さまざまなコンプライアンスフレームワーク内のセキュリティポリシーの完全マッピングも提供します。直感的なダッシュボードとレポートによって、これらの情報を確認できます。

### セキュリティとコンプライアンスの管理

ゼットスケーラーのCSPMは、複数のコンプライアンス標準や情報セキュリティが存在する組織や特定のアーキテクチャに合わせてポリシーセットをカスタマイズする必要がある情報セキュリティチームに対し、セキュリティポスチャのリスクベースの優先順位付け、ポリシー管理（オーバーライド、例外、サードパーティによる補償など）、構成などのさまざまなクラウドガバナンス機能を提供します。

### 構成ミスの修正

すべてのセキュリティポリシーに対する修復手順と、最も重要なセキュリティポリシーのサブセットに対する自動修復を適用できます。

## 実際の構成の収集

### オンボーディング

お客様のクラウド環境へのアクセスの提供（オンボーディング）は、迅速かつ簡単です。クラウドアカウントのオンボーディングでは、AzureとOffice 365にアプリ登録ロールを作成し、AWSにSecurityAuditロールを作成し、関連する（ほとんどの場合は読み取り専用）アクセス権限を付与します。

CSPによって必要なAPIが提供されないポリシーもあるため、ゼットスケーラーのCSPMは、メタデータ収集を自動化し、最も包括的なセキュリティポリシーカバレッジを達成するためのエージェントを開発しました。

### マルチクラウド

多くの組織は、コスト、機能、セキュリティ、スケーラビリティを比較し、クラス最高のクラウドサービスを自社のビジネスアプリケーションで活用できる、マルチクラウドイニシアチブを推進しています。ゼットスケーラーのCSPMも同様にマルチクラウド環境をサポートし、製品ロードマップにおいて、さらなる拡張を計画しています。

マルチクラウド

| CSP | 2018 | 2019 | 2020 |
|---|---|---|---|
| Microsoft Azure | ■ | ■ | ■ |
| Office 365 | ■ | ■ | ■ |
| aws | | ■ | ■ |
| Google Cloud Platform | | | ■ |

### 複数の地域

ゼットスケーラーのCSPMは、データのきめ細かいコントロールを必要とする企業向けに、パブリック SaaS（デフォルト）とプライベート SaaSを含む複数の導入オプションをサポートしています。データが置かれる地域によって要件が異なるため、これらの導入環境は、お客様のデータが置かれるそれぞれの地域でホスティングされます。

### スケーラビリティ

クラウドリソースが10,000以上の大規模環境では、次のような要件がさらに追加されます。

- 幅広いクラウドリソースの構成メタデータの収集を可能にする高いスケーラビリティ
- 収集される膨大なメタデータをデータベースに保存する機能
- 可能な限り短いスキャン時間の維持
- セキュリティポスチャデータを迅速に表示できる直感的なダッシュボードとレポート

ゼットスケーラーのCSPMは、サーバレス機能によるメタデータ収集やNoSQLデータベース（Cosmos DB）による情報の保存を始めとする、クラウドコンピューティングの最新テクノロジを活用しています。クラウドインフラストラクチャをスキャンするたびに、メタデータを並列で収集してデータベースに保存するために、何千ものサーバレス関数が同時に作成されます。NoSQLデータベースは、クラウドにデータを保存し、取得する、最もスケーラブルかつ最速の方法です。ゼットスケーラーのCSPMでは、わずか数分でスキャンが完了し、詳細分析に必要なレポートが生成されます。

### データセキュリティ

メタデータ収集プロセスの一部として保存される情報は、クラウドインフラストラクチャの実際の構成に関するものであるため、そのような情報がアクセス可能な状態になることで、より多くの情報が犯罪者に公開されてしまう可能性があります。そのため、CSPM製品には、移動データと保存データの両方の完全なデータ暗号化によって、最も厳格なルールベースアクセスコントロール（RBAC）と明確に定義されたデータ保存ポリシーを遵守する必要があります。

CSPMをSaaSサービスとして提供する企業は、SOC 2認定を取得することで、規定されたプロセスに従い、セキュリティのベストプラクティスを遵守する成熟した組織であることを証明します。

## 構成ミスの特定

### セキュリティポリシーの範囲

サポートするクラウドサービスの豊富さという観点でのセキュリティポリシーの範囲の包括性は、顧客が利用するすべてのクラウドサービスをCSPMソリューションが正しく評価できるかどうか、また、それぞれのクラウドサービスの範囲が包括的なものであるかどうかによって決まります。

ゼットスケーラーのCSPMは、1,500以上のセキュリティポリシー（クラウドセキュリティのベストプラクティス）の包括的セットを提供しており、ポリシーの範囲は今後もさらに拡大されます。

## セキュリティポリシーの範囲

| クラウドインフラストラクチャ | SaaS |
|---|---|
| **IaaSコンピュート** AWS EC2、Azure VM、VMスケールセット、Azure Service Fabric Cluster | **アイデンティティと認証** 基本/最新の認証、セルフサービスパスワードのリセット、グローバルadmin |
| **PaaSおよびサーバレス** 関数、Lambdas、Webアプリ、APIアプリ、モバイルアプリ | **アプリケーション権限** SafeLinks、外部ユーザ、ATP |
| **ネットワーキング** Azure Vnet AWS VPC、クラウドファイアウォール、NSG、セキュリティグループ、DDoS、WAF、ポート、プロトコル | **アプリケーションの利用** リスクのあるアプリ、インサイダーの脅威、侵害されたアカウントの接続 |
| **データ分析** HDInsight、データレイク | **監査** ログ、アクティビティレポート |
| **ストレージ** Azure ストレージ、AWS S3 | **データとデータ管理** |
| **PaaSデータベース** Azure SQL DB、SQLサーバ、SQL DW、NoSQL DB、AWS RDS、AWS RedShift、AWS Aurora DB、AWS Dynamo DB、Postgres SQL、MySQL | **デバイス管理** モバイルデバイス管理、Intune構成、デバイスパスワードポリシー |
| **バックアップ** バックアップボールト、保持、暗号化、アクセス | **Eメールセキュリティ/Exchange** |
| **ログ、監査、および監視** Azure Monitor、Application Insights、CloudWatch、CloudTrail | **文書の共有** 外部ドメインのホワイトリスト |
| **クラウドアカウントセキュリティ** ルートアカウント設定、アカウントIAM設定、プロファイルの監視、セキュリティセンタ/ハブ構成 | |
| **IAMアクセスコントロール** MFA、組み込みロールの使用、ゲストユーザ | |
| **仮想マシンOSベースライン** Windows 2012 R2、Windows 2016 | |
| **Kubernetesコントロールプレーン** AKSパッチ適用、ASC統合、AD統合 | |
| **キー管理** Azure Key Vault、AWS KMS | |
| **移動中データ** TLS/SSL、証明書認証, アプリケーションゲートウェイ、OWASP WAF構成 | |

ゼットスケーラーのCSPMは、最も使用されることが多いクラウドサービスはもちろん、お客様の追加要件にも対応することを目標として掲げています。CSPには、それぞれに固有の必須である一連のポリシーが存在します。ゼットスケーラーのCSPMは常に、他社に先駆けてMicrosoft AzureとOffice 365のポリシーに対応してきましたが、最近の追加により、AWSのポリシーについても業界最高レベルのサポートを提供しています。

### コンプライアンスフレームワーク

ゼットスケーラーのCSPMは、サイバーセキュリティ、業界のベンチマーク、法規制を始めとする、13のコンプライアンスフレームワークを提供しています。さらには、ヨーロッパ、オーストラリア、およびその他の国の地域コンプライアンスにも対応するため、これらのフレームワークのさらなる拡大を進めています。

## コンプライアンスフレームワーク

サイバーセキュリティベンチマーク


法律や規制


業界ベンチマーク

## セキュリティとコンプライアンスの管理

ゼットスケーラーのCSPMは、セキュリティポスチャのリスクベースの優先順位設定、ポリシー管理、プライベートベンチマークの構成などの多数のクラウドガバナンス機能を提供します。

### ポリシー管理

ゼットスケーラーのCSPMは、検出された資産にセキュリティポリシーを適用・管理する機能を提供します。

- ポリシー除外の機能によって、クラウドアカウントに対するポリシーの一時的または永続的な除外を定義できます
- ポリシーの上書きによって、特定のポリシーを「合格」（コンプライアンス）と指定し、CSPM製品で判断できないコントロールについては、サードパーティのそれに代わるコントロールを利用することもできます
- 手動ポリシーにより、自動化できない可能性のあるベストプラクティスも追跡できます（CSPがAPIを提供していない場合や、機密データをスキャンするためのアクセスがゼットスケーラーのCSPMに許可されない場合など）

### プライベートベンチマーク

セキュリティ要件は、業界や規模などの要素によって、組織ごとに大きく異なります。お客様は、（すべてのコンプライアンスとベストプラクティスの）すべてのコントロールをプライベートベンチマークに組み込みたいと考える場合もあるでしょう。組織の複数のユーザがベンチマークを作成し、特定のクラウドアカウントに適用することができます。

ゼットスケーラーのCSPMの使いやすい構成インタフェースを利用することで、既存の標準はもちろん、個々の会社の要件に基づき、ゼロからプライベートベンチマークを作成することもできます。これらのプライベートベンチマークはバージョン管理されるため、上位の標準への移行を進め、継続的に必要なバージョンのベンチマークを適用することができます。たとえば、バージョン1のプライベートベンチマークを最初に適用した後に、バージョン2のプライベートベンチマークを作成し、後続のリリースではそのバージョンを適用してセキュリティポスチャを強化することができます。

### リスクマトリックス

ゼットスケーラーのCSPMのリスクベース優先順位設定マトリックスは、ISO 27005規格に準拠しています。このリスクマトリックスによって、それぞれのセキュリティポリシーがリスクの影響と可能性によって自動的に分類されます。リスクの影響では、「Not Likely（可能性は低い）」、「Low（低い）」、「Moderate（中程度）」、「High（高い）」、「Certain（確定）」のいずれかに分類され、リスクの可能性では、「Very Low（非常に低い）」、「Low（低）」、「Moderate（中程度）」、「High（高）」、「Critical（重大）」のいずれかに分類されます。リスクの影響はセキュリティポリシーごとに事前に設定され、リスクの可能性は複数の測定基準と機械学習アルゴリズムに基づいて動的に算出されます。

リスクマトリックス（ISO 27005に基づく）

リスクレベル

高 109

中 150

低 201

| リスクの可能性 | リスクの影響 | | | | |
|---|---|---|---|---|---|
| | 非常に低い | 低い | 中程度 | 高い | 重大 |
| 確定 | 10 | 50 | 61 | 27 | 15 |
| 高い | 0 | 0 | 0 | 1 | 0 |
| 中程度 | 0 | 0 | 0 | 2 | 5 |
| 低い | 0 | 0 | 0 | 0 | 0 |
| 可能性は低い | 0 | 75 | 126 | 72 | |

色はリスクレベルを、数字はセキュリティポリシーの数を表します。

リスクマトリックスにはX軸とY軸があり、X / Yセグメントごとのセキュリティポリシーの数を表します。したがって、リスクの影響もリスクの可能性も高いセキュリティポリシーは「High（高い）」リスクレベルに分類されます。

## 構成ミスの修正

### 修復のガイダンス

クラウドインフラストラクチャを手動で展開する場合、構成ガイドを更新してリソースを修復し、プライベートベンチマークのすべてのセキュリティポリシーに準拠させる必要があります。ゼットスケーラーのCSPMは、CSPコンソールとコマンドラインまたはスクリプトを使用した、わかりやすい手順で、セキュリティポリシー修復ガイダンスを提供します。

### 自動修復

本番環境で特定の種類の構成ミスが発生した場合、チケットを正しい担当者に割り当てたり、その時間帯にいる担当者が修正したりするのを待つのでは遅すぎる場合があります。そのようなセキュリティの重大な問題は、直ちに解決する必要があります。

ゼットスケーラーのCSPMは、導入環境の変更（新規の導入やクラウドプロバイダのコンソールを使用した手動による構成の変更など）をお客様が開始した直後にトリガーされる自動修復ポリシーを提供します。ゼットスケーラーのCSPMが提供するガバナンスプレーンにより、利用可能な数百の選択肢から自動修復ポリシーを選択し、本番運用前の環境で試験運用し、本番運用前の環境でテストした後に、本番環境に適用することができます。

### 導入の自動化

構成ミスの可視性は重要ではありますが、何よりもまず、本番環境に構成ミスが持ち込まれないようにすることが重要です。クラウドインフラストラクチャを手動で展開している組織は、すべての重要なリソースの展開の自動化を検討する必要があります。

ゼットスケーラーのCSPMには、Quick Win自動化スクリプトと推奨構成を提供します。企業にとって重要なのは、展開を自動化する中央リポジトリを確立することです。重要なリソースの展開が自動化されれば、DevSecOpsの完全な自動化への移行を開始できます。

### チケット処理の統合

ゼットスケーラーのCSPMは、お客様のチケットシステムとの統合によって、チケットを自動的に生成し、クラウドオペレーション（CloudOps）チームの適切なメンバーにチケットを割り当てます。これらのチケットには、コンプライアンス違反のリソースや修復ガイダンスに関する重要な情報が含まれています。ゼットスケーラーのCSPMは、CloudOpsチームが効率的にチケットを処理できるようにするため、自動的に優先順位をチケットに割り当てます。ゼットスケーラーのCSPMの管理者は、チケットを作成する頻度（自動作成しない、毎日、毎週、毎月など）を構成し、調整できます。

### DevOpsの統合

クラウドのセキュリティとコンプライアンス保証のプロセスを実装しようとする企業は、手動または半自動のクラウドインフラストラクチャを導入しても人的ミスが発生しやすいことをすぐに理解するようになります。

ほとんどの組織が、ソフトウェアをできるだけ早くリリースする目的で自動化を実装します。導入環境の変更が頻繁であると、セキュリティポスチャが意図しない方向へと変わってしまう可能性が非常に高くなります。セキュリティポスチャを継続的に改善するため、これらのセキュリティ検証が、継続的コンプライアンス /継続的開発（CI/CD）パイプラインに統合されるようになっています。

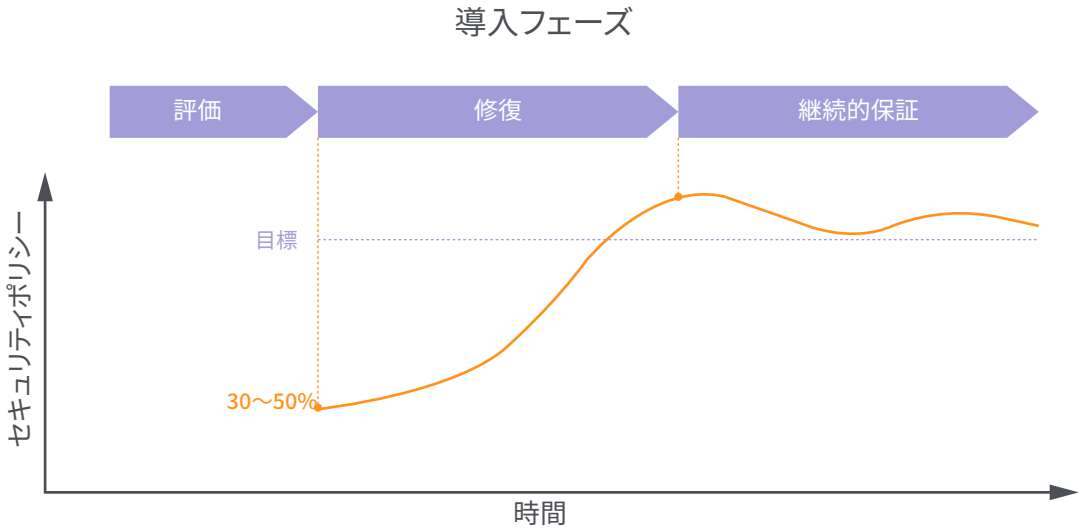
ゼットスケーラーのCSPMは、必要とされるすべてのCI/CD統合をサポートします。新しく作成したクラウドアカウントをゼットスケーラーのCSPMに自動的にオンボードできます。1つの要求を送信してインフラストラクチャセキュリティスキャンを開始し、もう1つの要求を送信してセキュリティとコンプライアンスポスチャを取得できます。自動分析を実行し、展開をそのまま本番運用するか、ロールバックするかを決定できます。これらのDevSecOps機能を、必要とされるセキュリティに沿って進めることができます。

# CSPMは複数チームのコラボレーションである

## 導入の手順

### セキュリティポスチャの評価

企業はCSPMソリューションを採用し、CISやNISTなどの共通のサイバーセキュリティフレームワークに基づいてコンプライアンスの証拠を提示します。医療機関であればHIPAA、ISVであればSOC 2、Eコマースであれば PCI DSS、国際取引がある企業であればISO 27001、金融サービスであればFFIECというように、業種に固有のコンプライアンスフレームワークもサポートする必要があります。




CSPMソリューションを使用することで、既存のクラウドインフラストラクチャを評価し、現在のセキュリティポスチャを判断できます。一般的には、その判断に基づいて、情報セキュリティ（InfoSec）チームと共同で「必須の」セキュリティポリシーを特定し、修復活動を開始するためのプロジェクトが開始します。

### 目標達成に向けての修復

修復には、クラウドセキュリティのベストプラクティスとCloudOpsチームに対する新しい構成要件に関する専門的なトレーニングが必要です。最初に本番運用前の環境で修復を検証することで、新しいクラウドインフラストラクチャ構成によってアプリケーションが動作しなくなったり、パフォーマンスに影響したりしないことを確認します。開発 /テストと本番運用前の環境は、目標とするセキュリティポスチャに合わせた新しい構成ごとに再構築されます。結果として、セキュリティポスチャが改善され、目標以上の成果を達成できます。

### 継続的保証

修正後は、CloudOpsチームが継続的なセキュリティとコンプライアンスの保証を担うことになります。本番環境のセキュリティポスチャを毎日監視し、直前の修正や更新が構成ミスにつながらないことを確認します。

セキュリティ保証ツールは、構成が正しいことを本番環境に新しいアプリケーションリリースを展開する前に検証するために、開発 /テストや本番運用前の環境でも継続的に使用されます。

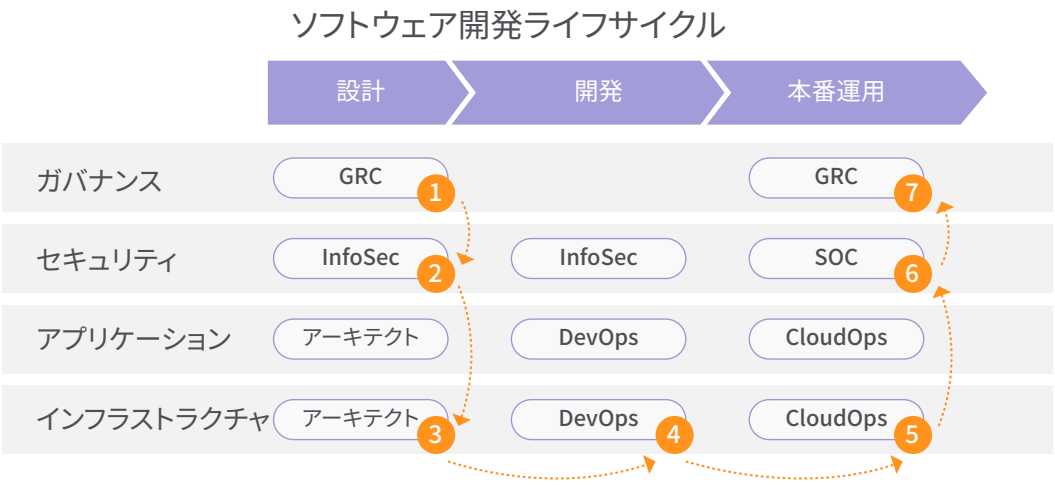
セキュリティ運用（SOC）チームは、セキュリティポスチャ監視をダッシュボードに追加し、本番環境で見つかった重大な構成ミスを迅速にエスカレーションする必要があります。

## 部門間のコラボレーション

CSPMの導入によって、InfoSec、SOC、アプリケーション開発（AppDev）のチームによるコラボレーションが容易になります。InfoSecチームは全社標準（目標）の設定に責任を負いますが、セキュリティやコンプライアンスを最終的に実装するのは、アプリケーション開発やインフラストラクチャ管理のチームです。

CSPMプロセスでは、以下の手順が実行されます。

1. GRCが、必要なコンプライアンスフレームワークを規定する
2. InfoSecが、全社的な情報セキュリティ標準を定義する
3. クラウドアーキテクトが、安全なアプリケーションアーキテクチャ構成を作成する
4. DevOps が、クラウドインフラストラクチャを展開する
5. CloudOpsが、見つかった構成ミスを修正する
6. SOCが、セキュリティポスチャを監視する
7. GRCが、継続的なコンプライアンスの証拠を提示する




### GRC：コンプライアンスフレームワーク

GRCチームは、必要な業界コンプライアンスフレームワーク（業界のベンチマーク、法律、規制）を規定します。ゼットスケーラーのCSPMは、さまざまなコンプライアンスフレームワークをサポートしており、お客様の要件に基づき、新しいフレームワークを継続的に追加しています。

### InfoSec：全社的な標準

InfoSecチームは、サイバーセキュリティのベンチマークや会社に固有の追加のポリシーなどの、組織にとって「必須の」セキュリティポリシーを定義します。ゼットスケーラーのCSPMはさらに、プライベートベンチマークを追加、追跡、適用する機能を提供しています。

### クラウドアーキテクト：構成ガイド

アーキテクトは、クラウドアーキテクチャのベストプラクティスを考慮してクラウドインフラストラクチャを設計し、CloudOpsチーム向けにセキュア構成ガイドを作成します。ゼットスケーラーのCSPMは、すべてのセキュリティポリシーの詳細定義に加えて、修復手順という形で構成ガイダンスを提供します。

### DevOps：インフラストラクチャの展開

インフラストラクチャ管理チームがクラウドインフラストラクチャを手動で展開する組織が多いものの、DevOpsチームによってクラウドインフラストラクチャの展開が自動化されている組織もあります。インフラストラクチャ管理やDevOpsのチームは、本番運用前の環境でゼットスケーラーのCSPMを使用して、クラウドインフラストラクチャをスキャンします。構成ミスが見つかった場合、本番環境へと移行する修正する必要があります。完全に自動化する方法については、本書の「DevSecOps」セクションで後述します。

### CloudOps：構成ミスの修正

CloudOpsチームは、本番環境に展開された直後にスキャンを開始します。展開されたクラウドインフラストラクチャが必要な基準を満たしていれば、本番環境をそのまま運用できます。CloudOpsは、クラウドインフラストラクチャの日次のスキャンをスケジュールします。構成ミスが見つかった場合は、優先順位に基づき、リスクレベルに応じて迅速に修正する必要があります。

### SOC：継続的な監視

本番環境を日次でスキャンして、手動での構成変更を検証する必要があります。SOCチームは、変更を監視し、迅速な修正が必要な重大な構成ミスがあればエスカレーションします。

### GRC：コンプライアンスの証拠

コンプライアンスチームは、監視結果に毎日アクセスし、継続的なコンプライアンスの証拠として、これらのレポートを規制当局や監査担当者に提示できます。

## DevSecOpsの実現

### DevSecOpsのプラクティス

**アプリケーションセキュリティ：** DevSecOpsは通常、アプリケーションセキュリティプラクティスのアプリケーション開発ライフサイクルへの統合を説明する用語として使用されます。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）、およびその他のツールは、コーディングのベストプラクティスに対するレビュー、セキュリティの問題の発見、および不備の記録に使用されます。侵入テストは、アプリケーションコードの堅牢性を本番環境にリリースする前に検証するために使用されます。ランタイムアプリケーションのセルフ保護機能も実装できます。

**データセキュリティ：** GDPR規制の導入により、データセキュリティがこれまで以上に重要になっています。DevSecOpsの一部として、本番運用前の環境で、データプライバシー、データ分類、データセキュリティプラクティスを検証する必要があります。


**クラウドインフラストラクチャ：**CSPの環境で利用されるクラウドインフラストラクチャは、IoC（Infrastructure as Code）を使用して展開し、構成できるものですが、一般的に理解されていないのは、クラウドインフラストラクチャの構成もDevSecOps運用モデル全体において不可欠な部分であるということです。

組織は最終的に、アプリケーション、データ、インフラストラクチャのセキュリティのベストプラクティスが組み込まれた、統合 DevSecOpsプロセスへと移行する必要があります。構成ミスを特定し、本番環境に持ち込まれないようにするには、本番運用前からセキュリティを考慮し、検証する必要があります。

展開の自動化がCI/CDパイプラインの一部になるため、クラウドインフラストラクチャ構成もクラウドセキュリティのベストプラクティスと照合して検証しなければなりません。CSPM製品は、CI/CDパイプラインからコールできるAPIを提供する必要があります。

### 必要なCI/CD API

CSPM製品は、次のようなエンドツーエンドのプロセスをサポートする必要があります。

1. 新しいクラウドアカウントのオンボード
2. セキュリティトークンの提供
3. 環境のスキャンの開始（開発、テスト、その他）
4. セキュリティポリシーの「合格」または「失敗」の情報の全社の標準との比較


DevOpsチームはゼットスケーラーのCSPM CI/CD APIを使用し、環境の構築後に自動的に再スキャンを開始し、すべてのセキュリティポリシーのコンプライアンスステータスを受け取ることができます。さらには、スキャン結果を分析し、設定標準に従ってIoC自動化リポジトリを更新できます。Zscaler CSPM修復ガイダンスをこれらの作業に利用することもできます。

## ゼットスケーラーのCSPM

ゼットスケーラーのCSPMは、クラウドにおけるセキュリティとコンプライアンスを自動化することで、継続的な可視性を提供し、最も包括的なセキュリティポリシーとコンプライアンスフレームワークへの遵守を保証します。マルチテナント SaaSとして提供されるこの製品は、お客様のクラウドインフラストラクチャとのシームレスな統合によって、迅速なデータ収集と包括的なダッシュボードやレポートの利用を可能にします。ゼットスケーラーのCSPMは、CI/CDパイプラインやチケットシステムとの統合をサポートし、自動修復を可能にし、プライベートベンチマークをサポートします。お客様は、自社の情報セキュリティ標準をAWS、Azure、Office365の環境に簡単に適用できるため、構成ミスに起因するデータ漏洩を防ぐことができます。

### マーケットリーダー

ゼットスケーラーのCSPMは、AWS、Azure、Office365の1,500以上のセキュリティポリシー、13のコンプライアンスフレームワークのステータスを自動的に可視化します。また、組織による独自のプライベートベンチマークの作成に加えて、大規模アプリケーション環境への迅速なDevSecOpsの導入を可能にします。

### 構成ミスの防止

クラウドインフラストラクチャの構成ミスは、クラウドセキュリティの最大のリスクです。クラウドセキュリティとコンプライアンスの保証を自動化することで、サイバーセキュリティリスクを大幅に軽減し、法規制への継続的コンプライアンスを証明できます。

### DevSecOpsの実装

クラウド環境の動的な特性を考えると、セキュリティやコンプライアンスの手動のプロセスは懸命な選択ではありません。Zscaler CSPMは、業界をリードする豊富なセキュリティポリシーを提供し、DevSecOpsツールとの迅速かつ容易なAPIベースの統合を可能にします。

### クラウドの迅速な導入

セキュリティとコンプライアンスが適切に管理されていれば、エグゼクティブは、クラウド導入を迅速に進める決断を下すことができ、デジタルトランスフォーメーションイニシアチブが加速して、ゼットスケーラーのCSPMのお客様の競争力が向上します。

### デジタルガバナンスの採用

CSPMは、セキュリティ、コンプライアンス、リスク管理、データプライバシー機能をクラウドのスピードに合わせて変革させる、重要な第一歩となります。自動化されたガバナンスプロセスは、デジタルビジネスに多くのメリットをもたらします。

詳細については、zscaler.jp/CSPMを参照してください

### ゼットスケーラーについて

ゼットスケーラーは、世界をリードする多くの組織を支援し、ネットワークとアプリケーションのトランスフォーメーションによるモバイルとクラウドファーストの環境の実現に貢献しています。代表的なサービスである、Zscaler Internet Access™とZscaler Private Access™は、デバイス、場所、あるいはネットワークに関係なく、ユーザとアプリケーションの高速かつ安全な接続を可能にします。ゼットスケーラーのサービスは100%クラウドで提供されるため、従来型のアプライアンスやハイブリッドソリューションでは実現できないシンプルさと強力なセキュリティを提供し、ユーザエクスペリエンスの向上を可能にします。185か国以上で使用されているゼットスケーラーは、マルチテナントの分散型クラウドセキュリティプラットフォームを運用することで、サイバー攻撃やデータ損失から数千の顧客を保護しています。zscaler.jpで詳細をご確認ください。



**ゼットスケーラー株式会社**
東京都千代田区大手町1-9-2
大手町フィナンシャルシティ
グランキューブ3階
**www.zscaler.jp**