



# Zscaler Zero Trust Cloud: マルチクラウド ワークロードのための 最新セキュリティ

あらゆる場所のすべてのワークロードを  
保護する最もシンプルな方法



# マルチクラウド セキュリティへの対応

複数のクラウド、リージョン、アベイラビリティゾーンにわたるワークロードの保護は、組織にとって重大な課題です。ワークロードは、インターネット、SaaSアプリケーション、プライベートアプリケーションとシームレスに接続するために、多様なトラフィック経路を必要とします。同時に、これらの環境で実行されるミッションクリティカルなワークロードは、進化する脅威から隔離された状態を維持しなければなりません。従来のセキュリティとネットワークモデルはこのような複雑さに適しておらず、スケーラブルかつコスト効率の高い方法でクラウド環境を保護できません。

- **攻撃対象領域の拡大:** 公開されているファイアウォールはすべて、攻撃者にとって潜在的な侵入口となります。
- **脅威のラテラルムーブメント:** VPNではセグメント化が行われないため、ひとたびアクセスが可能になると脅威は内部で拡散します。
- **運用の複雑さ:** 複数のクラウド サービス プロバイダーにわたるセキュリティ管理は一貫性に欠け、非効率的でコストがかかります。

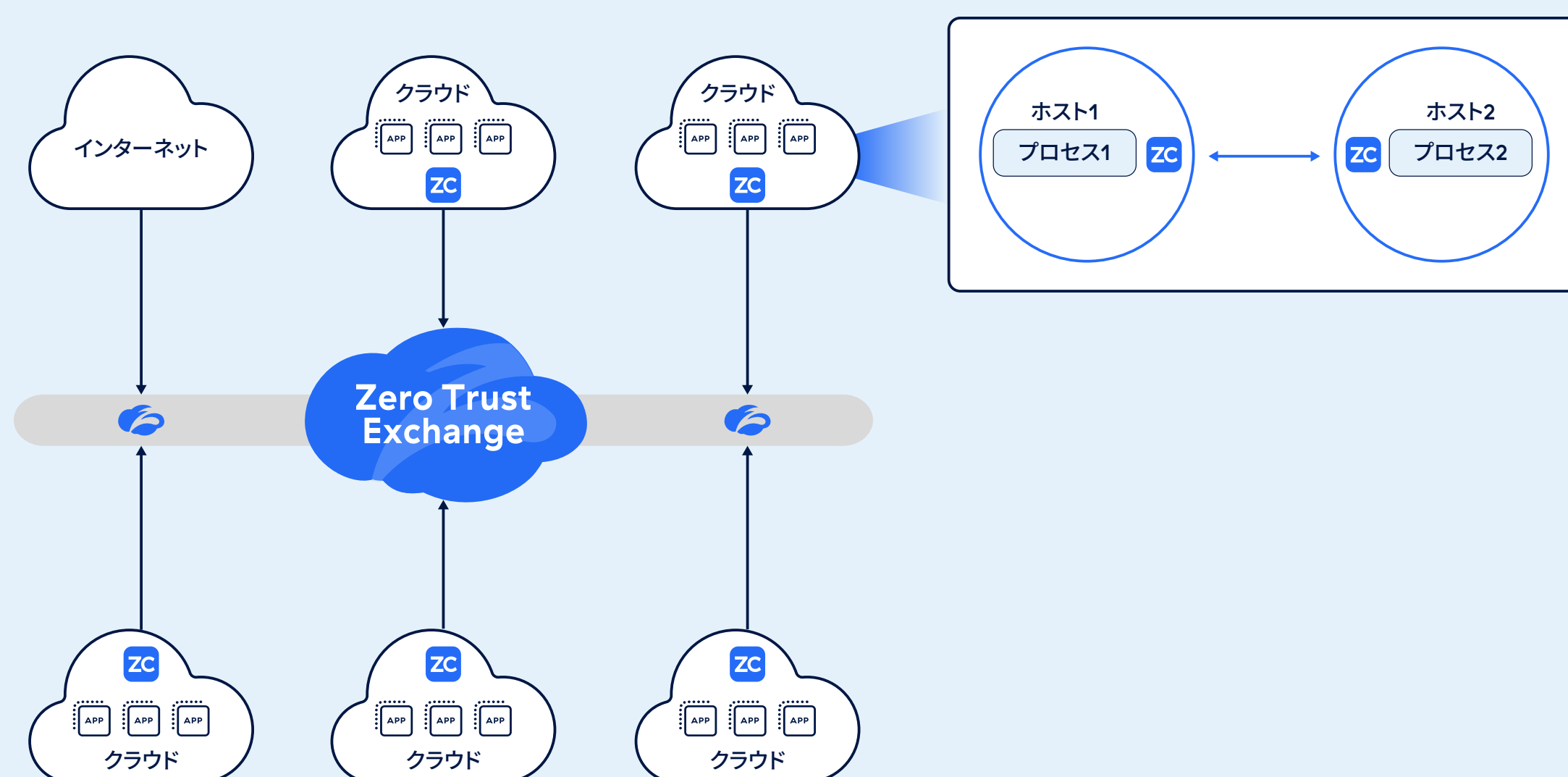
その結果、組織のマルチクラウド環境における脅威対策とデータ保護は、全体として一貫性のないものになります。

## Zscaler Zero Trust Cloud

### 従来のセキュリティの課題

ファイアウォール、VPN、プライベート ネットワークで構成される従来のセキュリティフレームワークは、クラウド主導のアーキテクチャーの要件を満たすことができません。これらのツールには、次のようなリスクと非効率性があります。

Zscaler Zero Trust Cloudは、従来のファイアウォール、VPN、プライベート ネットワークへの依存を排除することで、ワークロード セキュリティを刷新します。これにより、マルチクラウド環境全体に拡張され、標準化されたクラウドネイティブのゼロトラスト制御が可能になります。



# 重要機能

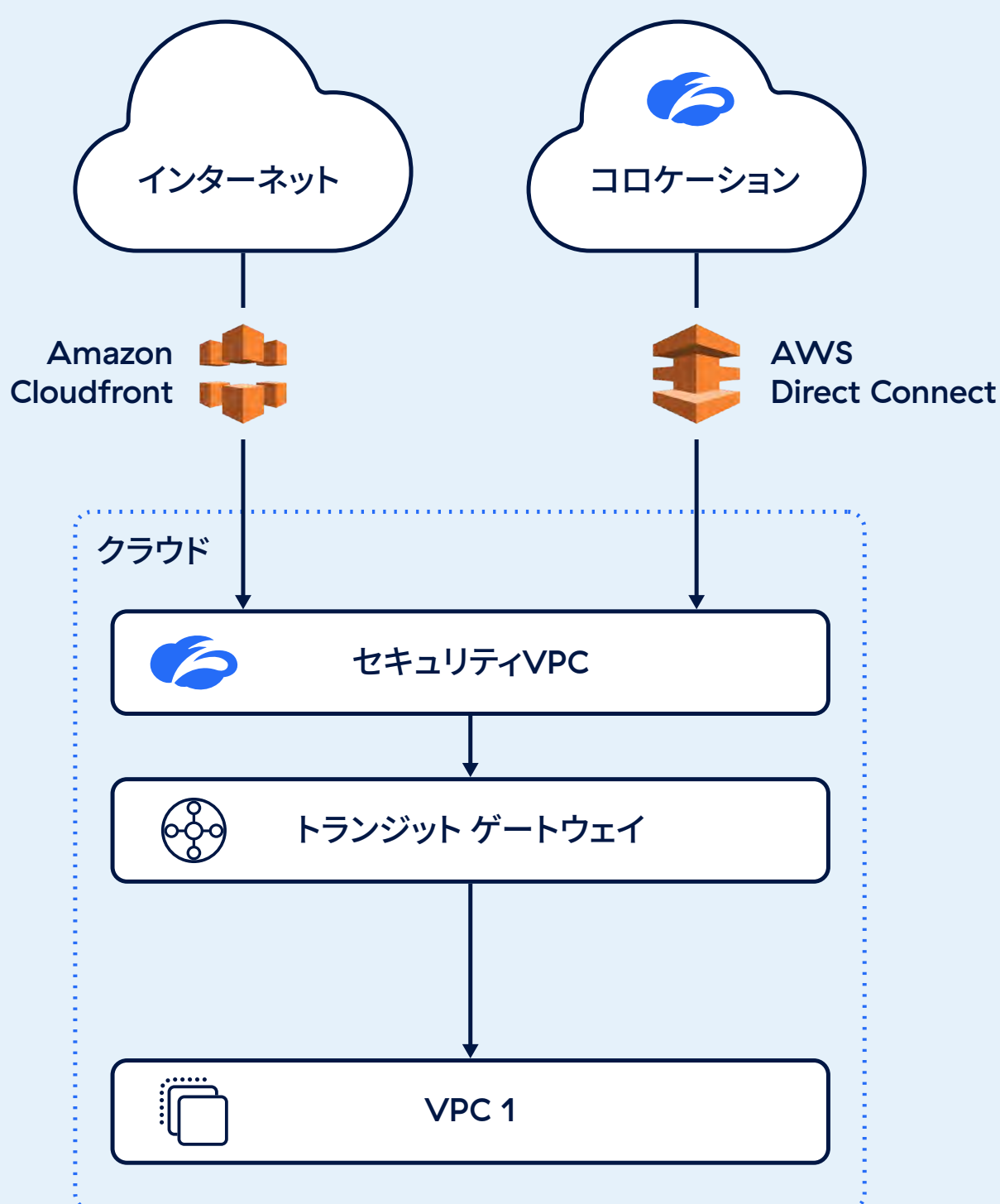
Zero Trust Cloudは、ワークロードに対して一貫した脅威対策とデータ保護を提供します。攻撃対象領域を削減し、脅威のラテラルムーブメントを排除するとともに、運用の複雑さとコストも削減します。Zero Trust Gatewayを使用すると10分以内に展開でき、Zscalerが完全に管理するクラウドネイティブサービスとしてZero Trust Cloudの機能を利用できます。ここからは、Zero Trust Cloudの主な機能について紹介します。

## 送受信トラフィックの保護

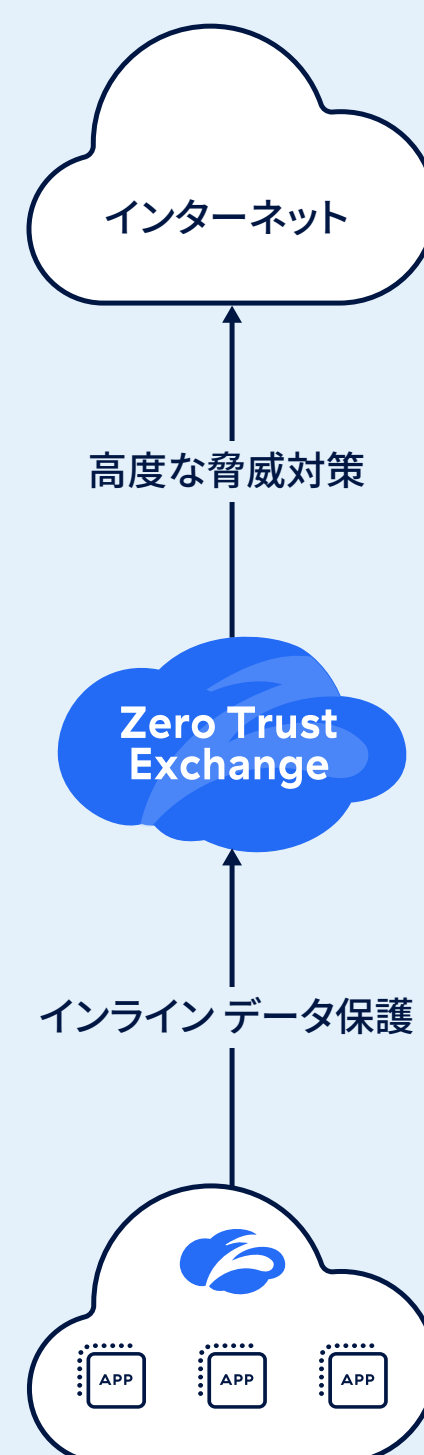
ワークロードとインターネット間またはSaaSアプリ間の安全な接続を実現します。

- クラウド規模のTLSインスペクションを通じて高度な脅威対策を提供します。
- インラインの情報漏洩防止によってデータ漏洩を阻止します。
- インバウンドとアウトバウンドの接続に対し、厳格な制御を施行します。

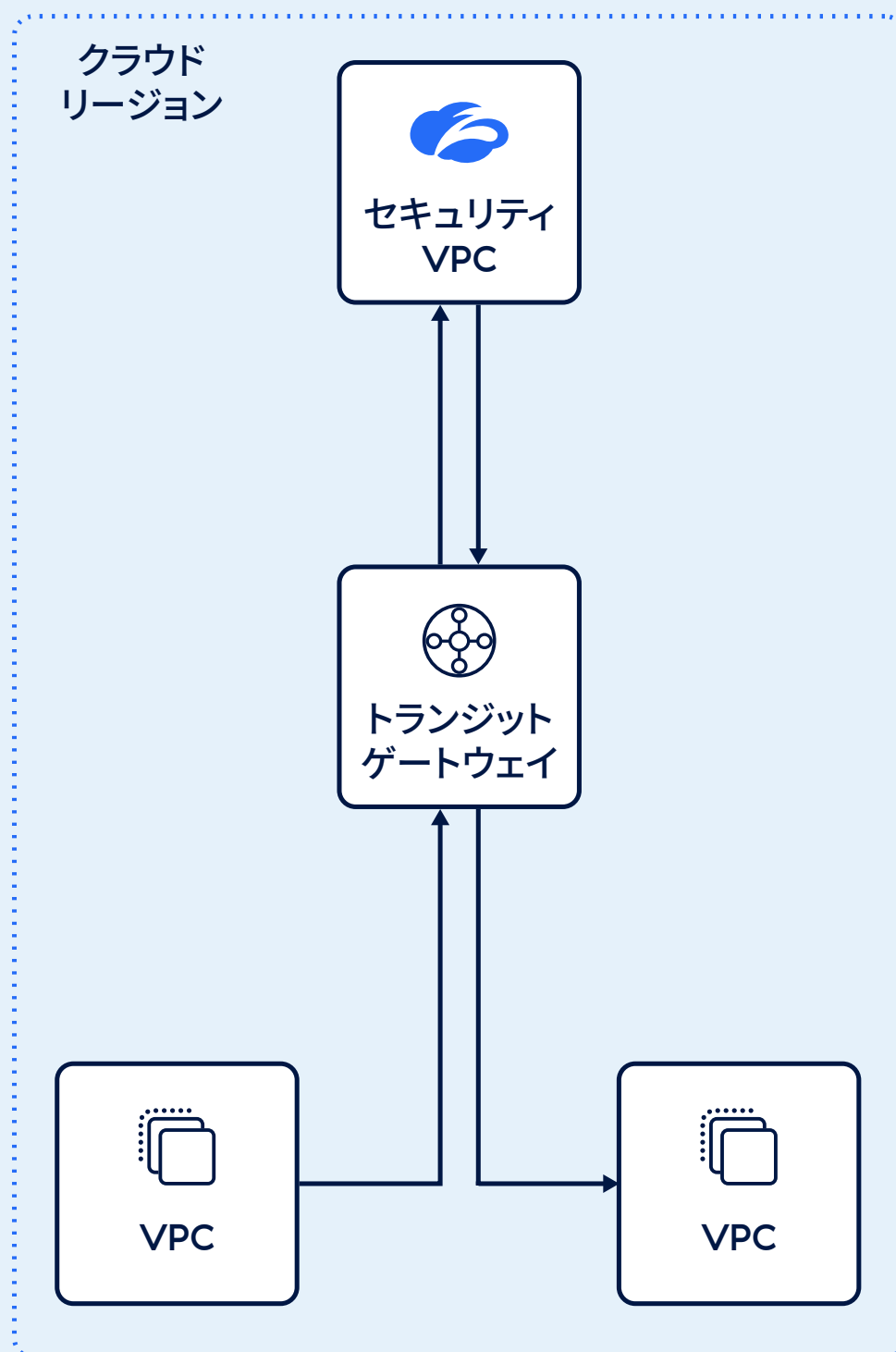
### 受信トラフィックの保護



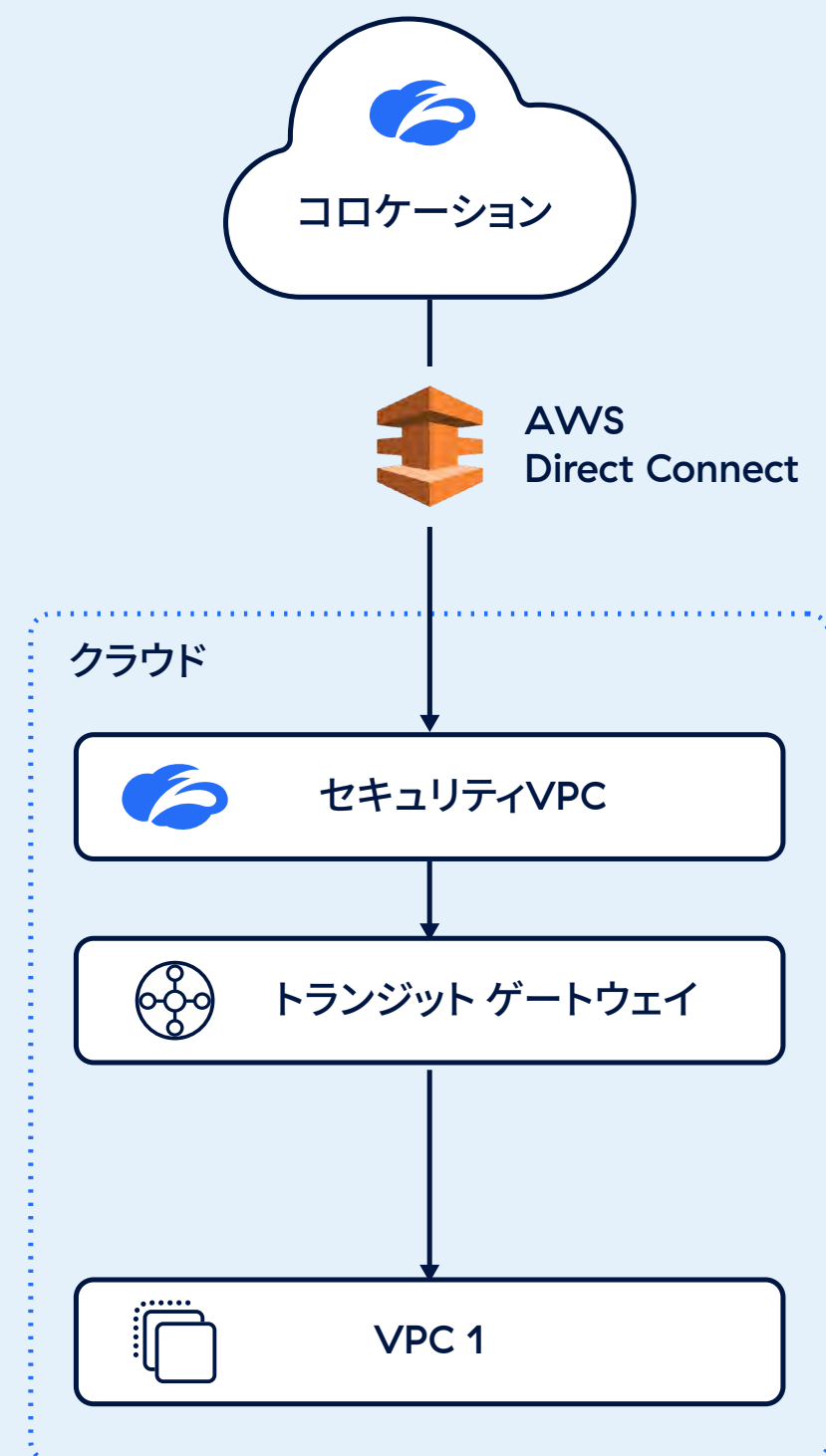
### 送信トラフィックの保護



## 同一クラウド リージョン内の VPC間/VNet間のトラフィック保護



## コロケーションとクラウド間での トラフィック保護



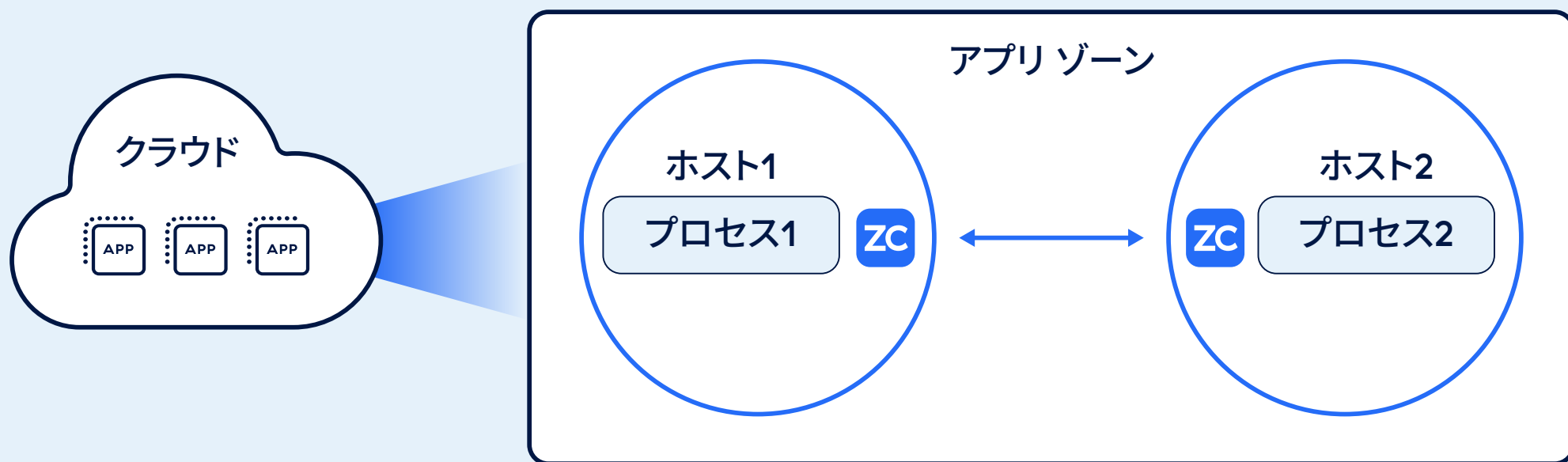
## 東西トラフィックの保護

相互に通信するワークロードを保護します。

- ローカル検査により、コロケーションとクラウド間の双方向トラフィックを保護します。
- 同一リージョン内でのVPC間およびVNet間の接続を保護します。







## ワークロード マイクロセグメンテーション

高リスクのアプリケーションを分離、保護します。

- リソースをリアルタイムで可視化します。
- AIが提案するリアルタイムのルールによるポリシー管理の合理化
- アプリケーション レベルのきめ細かなセグメンテーション ポリシーにより、攻撃対象領域を削減します。

これらの機能により、5つの重要ユース ケースに効果的に対応できます。

- DevinやCursorなどのAI活用型ツールによるソフトウェア開発を、イノベーションの停滞を招くことなく保護します。
- 単一のポリシー フレームワークにより、AWS、Azure、GCP間でのセキュリティのサイロ化を解消します。
- クラウド/仮想ファイアウォールの拡散を軽減し、コストと複雑さを最小化します。
- アイデンティティベースのマイクロセグメンテーションにより、重要なアプリケーション(Oracleなど)を分離し、侵害を瞬時に封じ込めます。
- セキュリティをネットワークから切り離すことで、「リフト&シフト」プロジェクト(SAPのクラウド移行など)のリスクを回避します。

## 次のステップ

Zero Trust Cloudは、マルチクラウド全体でワークロード セキュリティを標準化します。あらゆる環境にわたってワークロードを統合的に保護し、脅威のラテラルムーブメントを排除し、運用の複雑さを軽減します。詳細は、[Zero Trust CloudのWebページ](#)をご覧ください。

### Zscalerについて

Zscaler (NASDAQ: ZS)は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchange™プラットフォームは、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界150拠点以上のデータ センターに分散されたSSEベースのZero Trust Exchange™は、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細は、[zscaler.com/jp](https://zscaler.com/jp)をご覧ください。Twitterで@zscalerをフォローしてください。

© 2025 Zscaler, Inc. All rights reserved. Zscaler™および[zscaler.com/jp/legal/trademarks](https://zscaler.com/jp/legal/trademarks)に記載されたその他の商標は、米国および/または各国のZscaler, Inc.における(i)登録商標またはサービス マーク、または(ii)商標またはサービス マークです。その他の商標はすべて、それぞれの所有者に帰属します。



Zero Trust  
Everywhere