Akamai

ホワイトペーパー

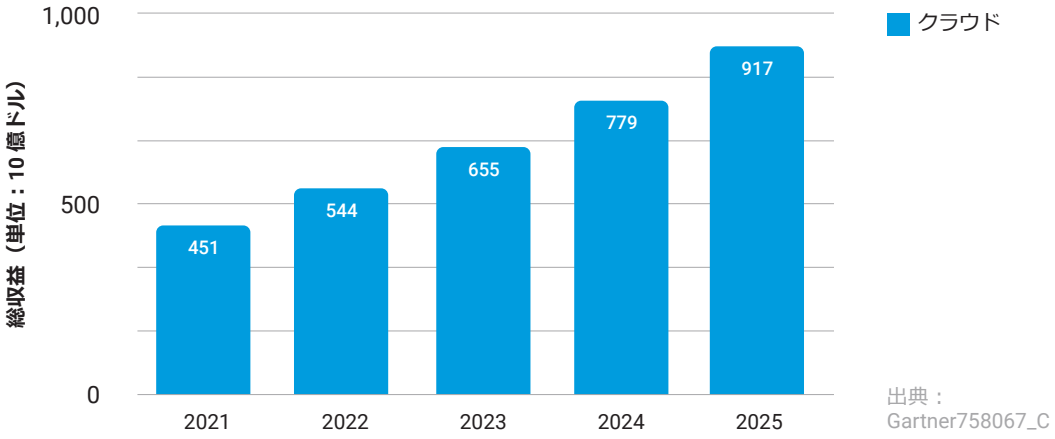
マイクロセグメンテーションへの道を切り拓く

ハイブリッドクラウドにマイクロセグメンテーションを実装するための戦略ガイド

クラウドはさらに増えると予測

膨大な量のデータやデータ処理をクラウド（正確には複数のクラウド）に移行することは、エンタープライズコンピューティングにおける過去 10 年間で最大の変化と言えます。パブリッククラウドに移行する組織が増えています。一般的には、パブリックプライベートハイブリッドのデータセンターアーキテクチャに移行しています。同時に、Infrastructure-as-a-Service（IaaS）を活用して、アジリティがますます求められています。テクノロジーアナリストの Gartner は、2025 年までに、獲得可能な市場セグメントにおける IT 支出の半分余りが従来のソリューションからパブリッククラウドにシフトすると予測し、2022 年の 41% よりも増加するとしています。また、パブリッククラウドの収益的支出は、総額が 2025 年までに 9,000 億ドルを上回ることが見込まれています。[1]

「クラウド」と「複数のクラウド」では大きな違いがあります。エンタープライズは、マルチクラウドのプラットフォームやサービスプロバイダーを採用する傾向が高まっています。確かなことが 1 つあります。エンタープライズデータセンターを単一の安全な物理スペースとして考えるのは時代遅れだということです。最新のデータセンターは、環境やテクノロジーがますます異種混合となり、物理サーバー、仮想マシン、コンテナがオンプレミスの施設、プライベートクラウド、パブリッククラウド IaaS プロバイダーに統合されています。こうした異種混在の状況は静的なものではありません。組織では、トラフィックレベルや処理要求の指示に応じて、さまざまなオンプレミス環境やクラウド環境でデータやワークロードの移行が絶えず行われています。



世界のパブリッククラウドサービスの収益予測（単位：10 億）

複雑さが増すと、新たな脆弱性がもたらされ、アタックサーフェスが広がる

クラウドの顧客は、IaaS によりアジリティ、適応性、スケーラビリティが向上するというメリットが得られるのは確かです。こうした恩恵が、クラウドの魅力の大部分を占めています。しかし、その二律背反として、管理が大幅に複雑化し、環境全体でワークロードの可視性が失われ、その結果、サイバーセキュリティの状況を把握できなくなります。複数のクラウドプロバイダーと連携すると、セキュリティチームは、さまざまなセキュリティ標準や機能に幅広く対応していかなければならなくなります。オンプレミスのサーバーやエンドポイント向けに設計された従来のセキュリティツールでは、クラウドの規模や複雑さにとても対応できません。IaaS ベンダーが提供する最新ツールは、プロバイダーの環境では効果的でしょう。しかし、複数プロバイダーのインフラではほとんど価値がありません。

さらに、仮想化や「すべてソフトウェア定義される」時代においても、セキュリティに対する考え方（これに伴う投資の大部分）は、特にエントリー時点での攻撃をブロックする必要があるという認識に基づいています。これは、境界防御での攻撃ではありません。それでも、境界防御は IT セキュリティスタックと非常に関係しています。しかし、境界が絶えず変化すると、境界防御は機能しません。データやワークロードは、パブリックおよびプライベートクラウド間や、オンプレミスのデータセンター間でやり取りが行われています。これらにアクセスするユーザーは、適切なセキュリティ制御の有無を問わず、リモートで作業するようになってきています。

毎年報告されているデータ侵害は膨大な数に上ります。これは、鋭敏な攻撃者が境界防御を自在に通り抜けていることを十分に物語っています。内部に侵入すると、攻撃者は比較的フラットなネットワークを見つけます。この境界内にある資産は保護されていないも同然の状態です。組織が柔軟性を備えていても、マルチクラウドのインフラの管理やセキュリティが複雑化すると、アタックサーフェスが急激に拡大することになります。通信制御はほぼ行われないため、個々のサーバー自体がアタックサーフェスになってしまいます。その結果、攻撃者は、水平方向のトラフィックのワークロード間で検知されることなく、時間をかけてラテラルムーブメントを行い、最も重要な資産を見つけることができます。

ネットワークセグメンテーションは、セキュリティ慣行として十分に認識および確立されているものです。しかし、現在では、ワークロードが通信を行っている場合や、セグメント間でワークロードの移行が頻繁に行われている場合があり、動的な IT インフラやクラウド規模で実行するのが困難になっています。エンタープライズクラウドの顧客の間では、アプリケーションやワークロードをさらにセグメント化して、通信フローをリアルタイムで厳重に制御し、データセンター内の脅威を検知および阻止して、被害を未然に防ぐ必要があるという認識が高まっています。必要なのは、インフラの境界を越えた一貫性のある機能でアタックサーフェスを縮小して、セキュリティの複雑さを軽減するソリューションです。これにより、セキュリティチームは多くの脅威をすばやく検知して、脅威の拡散を阻止することができるようになります。

ここで一役買うのが、マイクロセグメンテーションです。

マイクロセグメンテーションの定義

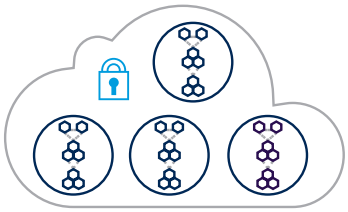
Gartner は、マイクロセグメンテーションを「仮想データセンター内におけるセキュリティを目的とした分離やセグメンテーションの実装プロセス」と定義しています。さらに、マイクロセグメンテーションにより、「エンタープライズデータセンターで高度な攻撃が水平方向に拡散されるリスクが軽減され、エンタープライズはオンプレミスやクラウドベースのワークロード全体で一貫したセグメンテーションポリシーを適用できるようになる」と、付け加えています。[2]

マイクロセグメンテーションは一般的に、ハイブリッドデータセンター内の配置場所に関係なく、個別またはグループのアプリケーションに関するセキュリティポリシーを確立することで機能します。これらのポリシーにより、どのアプリケーションやコンポーネントが相互通信できるか、またはできないかが定められます。不正な通信が試行された場合、脅威の存在が即座に示されます。最も理想的なのは、マイクロセグメンテーションテクノロジーがインフラに依存しないことです。これにより、セキュリティポリシーは、クラウド環境間での移行が行われても、各アプリケーションを保護し続けることができるようになります。

セグメンテーションのソリューション領域

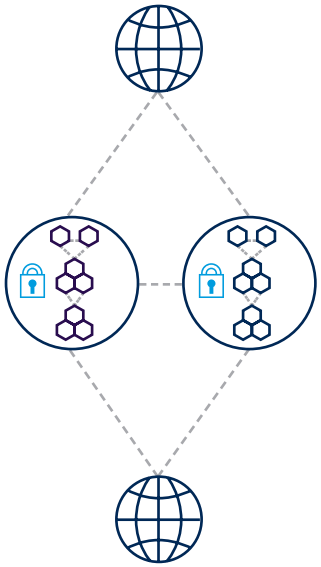
インフラのセグメンテーション

特定のインフラ内のアプリケーションのトラフィックを保護します。



アプリケーションのセグメンテーション

アプリケーションと外部ネットワーク間のトラフィックを保護します。



マイクロセグメンテーション

プロセスレベルの属性など、コンテキストが追加されたアプリケーションでのトラフィックを保護するルール。

2 Gartner、「Technology Insight for Microsegmentation（マイクロセグメンテーションのテクノロジーに関する知見）」、2017 年 3 月
「Hype Cycle for Cloud Security 2017（2017 年クラウドセキュリティに関するハイプサイクル）」、2017 年 7 月

マイクロセグメンテーションの事例

今日の動的なデータセンターにおいてエンタープライズは、侵入防止やアクセス管理からワークロードやアプリケーション自体に注意を向けていくことが求められています。これは加速的に起こっているようです。2017 年の時点で Gartner は、「従来の境界やシグニチャベースの保護をバイパスする高度な標的型脅威からサーバーワークロードを保護することに重点を置く」傾向が高まっていることに気付き始めていました。こうした攻撃は金銭目的で、機密データやトランザクションにアクセスする手段としてサーバーやアプリケーションのワークロードを標的にするのが一般的です。[3]

マイクロセグメンテーションの主な原動力は、ミッションクリティカルなアプリケーションやワークロードを保護するニーズです。単に自己利益やビジネス向上の問題のように思われるかもしれませんが、多くの場合、セキュリティポリシーや規制要件によって義務付けられてもいます。

セキュリティチームは、データセンター内でアタックサーフェスを削減する方法を見つける必要があります。つまり、アプリケーションを実行しているサーバーの脆弱性を削減する方法です。シグネチャーブロックやアプリケーションの許可リストなどの従来の認証手法では、高度な攻撃者に簡単に打ち破られてしまいます。マイクロセグメンテーションを使用すると、チームは厳重かつきめ細かなアクセスポリシーや通信ポリシーを設定し、適用することができます。また、アプリケーションフローの可視性を高め、セキュリティ体制をチームで適切に評価できるようにする必要もあります。

マイクロセグメンテーションが必要ですか？

いくつかの簡単な質問に回答することで、マイクロセグメンテーションの必要性を確認できます。

- □ 制のある業界で従事していますか？または、データやトランザクションのセキュリティを管理する規制を遵守する必要がありますか？
- 複数のクラウドにまたがるワークロードを有するハイブリッドインフラはありますか？
- 仮想マシンやコンテナでアプリケーションを実行していますか？
- ワークロードの可視性や制御が失われていると感じていますか？
- 脅威が存在していることや、データセンターで攻撃が進行中であることをいつでも確認することができますか？
- 「1 つの画面」でインフラ全体のセキュリティを制御できますか？

道のりを阻む 4 大障害

今日の動的なデータセンターにおけるマイクロセグメンテーションのニーズをセキュリティ専門家が概ね認めていても、効率的かつ効果的に実装することが非常に困難だと判断されてしまうのはなぜでしょうか。従来のツールを使用してマイクロセグメンテーションを実装しようとする組織は、一般的に次の 4 つの大きな障害に直面します。

1. **プロセスレベルの可視性の欠如**
   これは多くの場合、最初に直面する障害となります。目に見えないものを保護することはできません。マイクロセグメンテーションは、個々またはグループのアプリケーションやワークフロープロセスを保護するものです。セキュリティチームは、コンテキスト内で水平方向のトラフィックフローを実際に可視化して、把握する必要があります。ほとんどのツールでは、そこまで深く把握することはできません。

2. **ハイブリッドマルチクラウドのサポートの不足**
   マイクロセグメンテーションのセキュリティポリシーは、オンプレミス環境やパブリッククラウド環境で簡単にスケーリングができ、ワークロードが移行してもこれらを追跡できなければなりません。特定の環境で機能するように設計されたツールは、ハイブリッド環境では役に立ちません。

3. **柔軟性のないポリシーエンジン**
   前述のように、今日のデータセンターは静的ではありません。セキュリティ対策も同様です。「設定すればあとは何もしなくてよい」という考え方は、もう通用しません。残念ながら、クラウドプロバイダーの既存のツールでは、ルールの調査、テスト、調整を常に行えるだけの柔軟性が許容されていません。この問題により、ハイブリッドインフラにおいて複数のポリシーツールが必要になってしまいます。

4. **補完的な制御と統合されていない**
   正しく行えば、マイクロセグメンテーションはプロセスを保護するだけでなく、攻撃を捉えることもできます。ただし、単機能のマイクロセグメンテーションツールには、一般的に侵害検知機能が含まれていません。ユーザーがツールを統合することで、効果的に連携させることができます。このパッチワークのアプローチは、故障のリスクが高まります。

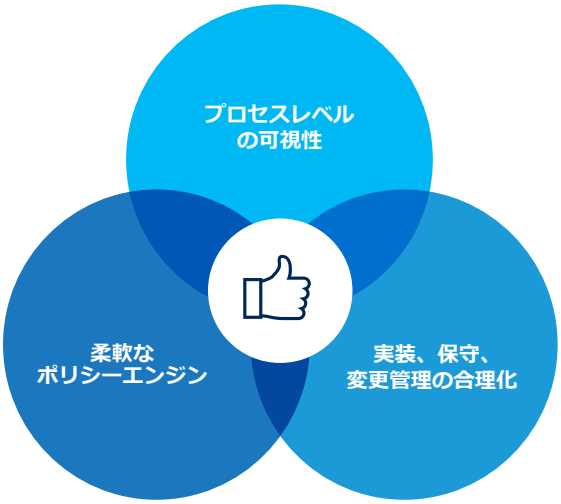
プロジェクトの失敗は普通のことで、 例外的なことではない

このような障害を考えると、ほとんどのマイクロセグメンテーションプロジェクトは、実装サイクルが遅々として進まず、コストや税務リソースがかさみ、結局、目標を達成できずに終わる傾向にあるというのも不思議ではありません。可視性の欠如によりセグメント化に必要なものが見い出せなかったり、セグメンテーションの必要性を判断できなかったりするなど、つまずくことは多々あります。プロセスレベルの通信の複雑なルールを数か月もかけてスプレッドシートで作成して、アプリケーションのグループ化やポリシーの合理化のチャンスを見逃してしまうこともあります。多くの場合は、「オーバーセグメンテーション」での失敗です。個別のポリシーを設定しすぎて、セキュリティが複雑になりすぎてしまうのです。これが、まさに解決しようとしていることです。Gartner は、「セグメンテーションプロジェクトの 70% 以上が、オーバーセグメンテーションのために、当初の設計を再設計することになる」と、指摘しています。[4]

オーバーセグメンテーションは、アプリケーションや、最終的にはビジネスを減速させるリスクをもたらします。しかし、時計の振り子が正反対の方向に振られるように、セグメンテーションが不十分なまま進めると、セキュリティ体制を損ねる結果になる恐れがあります。

マイクロセグメンテーションの成功戦略

マイクロセグメンテーションを実装する道のりは、直線的なものではありません。環境内の通信フローの検知、把握、制御など、紆余曲折の道のりと言えます。セキュリティチームには、アプリケーションを中断することなく、セキュリティポリシーを開発して、常に新たな変更や追加を組み込むことができる柔軟性が必要です。多くのソリューションが提供するポリシー作成エンジンには柔軟性がありません。そのためセキュリティチームは、準備が不十分なまま不完全なルールや効果のないルールの実装を余儀なくされることも少なくありません。



簡単に言えば、実装を成功させるには、4 大障害を克服または回避できるソリューションが必要だということです。段階的なアプローチを実現することで、過度の複雑さを回避し、セグメンテーション不足やオーバーセグメンテーションのリスクを軽減することができるようになります。つまり、ソリューションは次の要件を満たすものである必要があります。

- **プロセスレベルの可視性 ：** チームは、水平方法および縦方向すべてのフローを表示、収集、標準化できる必要があります。たとえば、アプリケーションを自動的に検出し、通信要件を把握することができるようになるツールが必要です。また、複数のアプリケーション属性をフィルタリングして、資産のラベリングやグループ化を促進し、ポリシーを共有する機能も必要です。
- **柔軟なポリシーエンジン ：** 大規模なセグメントにおいては高度なベストプラクティスやコンプライアンスルールを、マイクロセグメントにおいてはきめ細やかなルールを同時に設計できる必要があります。このソリューションにより、アラートから施行へと徐々に移行できるようになります。また、すべてのプラットフォーム、デバイス、クラウドで機能するポリシーを確立できる必要があります。
- **実装、 保守、 変更管理の合理化 ：** システムでは、必要に応じて実装、保守、変更を簡単に行えるようにする必要があります。内蔵型の侵害検知機能やインシデント対応機能を組み込む必要があります。最終的には、ポリシーが十分に定義されるようにする必要があります。これにより、新しいアプリケーションを起動するたびに、ポリシーを自動実装（CI ／ CD）ツールに統合できるようになります。

理想的なソリューション機能

市場には数多くのマイクロセグメンテーションツールがありますが、当然のことながら、すべてのツールがこの道のりを簡単にたどれるわけではありません。スムーズかつ効果的な実装を実現するためには、次の機能を備えたソリューションを選択する必要があります。

- ベアメタルサーバー、仮想マシン、コンテナをプロセスレベルで完全に可視化できる**自動アプリケーション検知**
- **堅牢かつ広範なクエリ**を定義して、コンテキストラベルやオブジェクトのグループを作成することができる機能
- ポリシーの調整、強化、維持ができるインテリジェントなルールを備えた**柔軟なポリシーエンジン**
- より多くの脅威をすばやく検知して拡散を阻止できる、さまざまな手法が統合された**侵害検知機能**
- 単一のプラットフォームで、データセンター、パブリッククラウド、プライベートクラウドなど、あらゆるインフラに対応する、**ハイブリッドインフラのサポート**

マイクロセグメンテーションの実装については、これらのコア機能を備えたソリューションが成功への一番の近道となります。さらに、既知の障害や複雑さを克服し、セキュリティを損ねることなく、柔軟なハイブリッドクラウドインフラのビジネスメリットをすべて享受できるようになります。

組織では、ハイブリッドデータセンター、マルチクラウドプラットフォーム、IaaS により、「クローズド」なオンプレミスデータセンターの場合よりも柔軟性、スケーラビリティ、アジリティを向上させることができます。しかし、アプリケーションやワークロード（サイバー攻撃者が標的にしている実際の資産）はそのままの状態となり、露出や脆弱性が高まります。マイクロセグメンテーションは、クラウドのワークロードを保護するベストプラクティスとして広く認められていますが、エンタープライズではそれがなかなかうまくいきません。それでも、一度にすべてを行う必要はありません。今日の高度なソリューションでは、段階的なアプローチと組み合わせることで、マイクロセグメンテーションの実装が非常に簡単になります。これにより、組織の最も重要な資産に対するセキュリティが向上します。

成功するマイクロセグメンテーションの実装の詳細については、akamai.com/guardicore をご覧ください。

1 「Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025（Gartner、主要市場セグメントにおけるエンタープライズの IT 支出の半分以上がクラウドにシフトすると予測）」、Gartner、2022 年 2 月 9 日。

2 Jay Heiser、「Hype Cycle for Cloud Security, 2017（2017 年クラウドセキュリティに関するハイプサイクル）」、Gartner、2017 年 7 月 17 日。

3 Neil MacDonald、「Market Guide for Cloud Workload Protection Platforms（クラウドワークロード保護プラットフォームに関するマーケットガイド）」、Gartner、2017 年 3 月 22 日。

4 Greg Young、「Best Practices in Network Segmentation for Security（セキュリティを実現するネットワークセグメンテーションのベストプラクティス）」、Gartner、2016 年 7 月 28 日。

Akamai は、お客様が生み出すもの全てにセキュリティを組み込む取り組みを支援することで、どこで構築しどこへ提供しようとも、顧客体験、従業員、システム、データを守ります。グローバルな脅威に対する可視性を備えた Akamai のプラットフォームは、セキュリティポスチャの適応と進化を後押しして、ゼロトラストの実現、ランサムウェアの阻止、アプリケーションと API のセキュリティの確保、DDoS 攻撃の撃退を支援します。これにより、お客様は自信を持って、継続して、イノベーションを起こし、可能性を広げ、新たな可能性を生み出すことができます。Akamai のセキュリティ、コンピューティング、デリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、Twitter と LinkedIn で Akamai Technologies をフォローしてください。公開日：2023 年 5 月。