Akamai

ホワイトペーパー

コンテナを最大限活用する

重要な資産やアプリケーションに対するセグメンテーションのシンプル化と促進

はじめに

コンテナ化は、クラウドおよびハイブリッド環境でのアプリケーション実装に最適なソリューションとして急浮上しており、コンテナの増加は加速し続けています。Gartner によると、2026 年までにグローバル企業の 90% がコンテナ化されたアプリケーションを運用するようになると予測され、2021 年の 40% よりも増加しています。[1]また、Capital One の Forrester 調査によると、**調査を行った IT リーダーの 86%** が、より多くのアプリケーションでコンテナの使用を拡大していくことに優先順位を置くと回答しています。[2]

> Gartner によると、2026 年までに**グローバル企業の 90%** がコンテナ化されたアプリケーションを運用するようになると予測されています。これは 2021 年の 40% から増加しています。

当然ながら、これらはすべて、IT 環境のセキュリティ責任者への負担を増やすことになります。特に、迅速な導入や拡張を重視する DevOps モデルではなおさらです。特化型のコンテナ・セキュリティ・ソリューションが次々と生まれる中、プラットフォーム固有のコンテナに特化したエンティティは、エンタープライズデータセンター全体に対応することなく、複雑さや管理オーバーヘッドを増大させ、セキュリティチームの仕事をより複雑化してしまうことになります。必要なのは、コンテナを含むオンプレミス、クラウド、ハイブリッド環境で実行されるあらゆるアプリケーションやテクノロジーで一貫性を持って機能する、単一の包括的なセキュリティソリューションです。

ここで、ソリューションの話に入る前に、コンテナの事象、事象の要因、セキュリティの観点から推測されることについて簡単に解説します。

高まるプレッシャー：導入を促進するビジネスニーズ

コンテナへの移行と導入増加の予測は、エンタープライズの IT 部門に求められるビジネスニーズが背景にあると言えます。現代のエンタープライズでは、スピードとアジリティを持って展開して、競合他社の脅威や市場機会に対応できるようになることと見込まれています。イノベーションをサポートし、市場投入までの時間を短縮できるソリューションが必要です。さらにエンタープライズでは、継続的な効率改善を常に求めています。相互のつながりがますます増えていく中、サプライヤーやベンダー、ビジネスパートナー、特に顧客とのビジネスをもっと簡単にデジタル化したいと考えています。

エンタープライズの IT 部門がクラウド（正確にはオンプレミス／クラウド・ハイブリッド・モデル）に移行しているのは、これらが主な理由です。また、DevOps の傾向を推進する大きな要因でもあります。着想から実装まで、障壁となるものを排除し、自動化や自動スケーリングでアプリケーションをより迅速に実稼働環境に導入することで、重要なアプリケーションの実装を迅速化しようとしています。

> 「実稼働環境でコンテナを運用するうえで必要な取り組みが組織で過小評価されることも少なくない」
>
> **– Gartner**

こうしたあらゆることが、IT 部門でコンテナ化が採用されている理由と言えます。仮想マシンに比べ、コンテナは起動がはるかに簡単かつ高速で、実質的にレイテンシーのないジャストインタイムの配信が実現し、チームは「サーバーではなくサービスのスピンアップ」に注力できるようになります。コンテナの主なメリットは、最新の動的なデータセンター環境における移植性です。これにより、オンプレミスの施設において、アプリケーションをマルチクラウドインスタンスに簡単に移行できるようになります。これは、Kubernetes（K8s）を介したコンテナオーケストレーションでさらに強化されます。これにより、チームはさまざまな環境で大規模にコンテナ化された大容量のアプリケーションを実装し、管理できるようになります。オーケストレーションは次第に、コンテナの実装と管理のベストプラクティスと考えられるようになってきています。

つまり、IT 部門では、コンテナを使用することで、スピード、自動化、耐障害性、可用性に関するビジネスニーズに適切に対応し、他のテクノロジーに比べ総所有コストを削減できるようになります。ただし、実装の試みに欠点がないわけではありません。2019 年 Gartner レポートでは、コンテナ化のベストプラクティスについて「実稼働環境でコンテナを運用するうえで必要な取り組みが組織で過小評価されることも少なくない」と述べています。[3] コンテナ化は普及性がある一方で、テクノロジーは初期段階的で、安全な実装に関するベストプラクティスは十分にまとまっていません。Red Hat の 2022 State of Kubernetes Security レポートによると、「コンテナの導入における最大の懸念事項の 1 つが［依然として］セキュリティであり、セキュリティの問題により、実稼働環境でのアプリケーション実装に遅れが継続的に生じている」とされています。[4] エンタープライズでは、実装戦略においてサイバーセキュリティが盛り込まれていなければ、コンテナの潜在的なメリットをすべて享受することができないのは確かです。

Red Hat の 2022 State of Kubernetes Security レポートによると、「**コンテナの導入における最大の懸念事項の 1 つが［依然として］セキュリティ**であり、セキュリティの問題により、実稼働環境でのアプリケーション実装に遅れが継続的に生じている」とされています。

セキュリティチームに対する影響

Gartner は、「セキュリティは後付け的なものであってはならない」と、ベストプラクティスレポートで断言しています。さらに、「DevOps のプロセスに組み込む必要がある」と、コメントしています。しかし、多くの場合において、そのようになっていません。コンテナ化の実装を急ぐあまり、セキュリティチームは自分たちが「不可能な三角形」の頂に置かれているような感覚になることがあります。これは目の錯覚を起こす画像「ペンローズの不可能な三角形」で、Akamai ではクライン＆ハワードの不可能な三角形とも呼ばれています。

> 従来のセキュリティソリューションでは、現代のエンタープライズに適応できません。セキュリティソリューションは、迅速で適応性が高く、動的で、「DevSecOps」アプローチにシームレスに適合できなければなりません。

三角形の頂は他の 2 つの頂点よりも遠くにあるように錯覚して見えるのと同様に、セキュリティは、ビジネスニーズや、ニーズに対応する IT イニシアチブに比べ距離があるように見えます。しかし、三角形が目の錯覚であるように、セキュリティソリューションも見かけよりも実際には近いものなのです。チームはとにかく、これまで使用してきた煩雑で従来的なソリューションとはまったく違った観点で考えていかなくてはなりません。現在のエンタープライズの IT 部門が実現できる方法を策定し、「DevSecOps」アプローチにシームレスに適合するソリューションを検討していく必要があります。つまり、迅速かつ適応性が高い動的なソリューションであり、それ自体に DevOps プレイブックのアプローチを採用するソリューションです。最も重要なのは、基盤となるオペレーティングシステムやプラットフォームから切り離され、実装や管理が簡素化されているソリューションです。

クライン＆ハワードの不可能な三角形

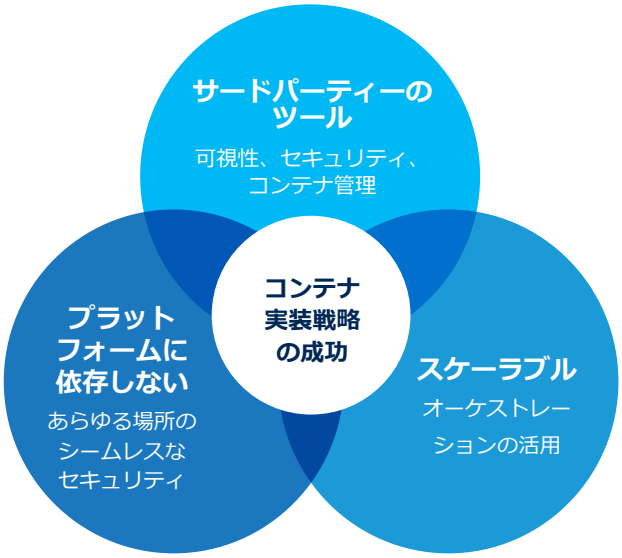
「ネイティブな」だけでは不十分な理由

仮想化やクラウド移行の当初、エンタープライズでは、クラウドネイティブの制御であればワークロードを十分に可視化、管理、保護できると考えられ、安心していた傾向がありました。IT 部門のマネージャーは、多くの試行錯誤を経て初めて、ネイティブ制御を上回るセキュリティを実現するサードパーティーソリューションを組み込んだオーバーレイ管理モデルが必要であることに気づきました。

Gartner と Forrester Research が述べているように、コンテナ実装戦略の成功は、次の「コンテナの 3 要素」が基礎となります。

- 複数のクラウドアーキテクチャやオンプレミスアーキテクチャのどこにでもシームレスに実装できる、プラットフォームに依存しない移植可能な方法でコンテナを実行する
- オーケストレーションを活用して、コンテナを大規模に実行および管理する
- コンテナの管理、可視化、セキュリティにサードパーティーのツールを使用する

これまでの仮想化やクラウドの取り組みとは異なり、特にセキュリティ制御をはじめ、クラウドネイティブの管理システムでは効果的なコンテナ戦略に不十分であるということが、当初からコンテナ業界の間で認識されていました。Gartner のコンテナ管理ソリューションの調査では、**65% が、コンテナ化されたワークロードを可視化、管理、保護する目的でサードパーティーの管理ツールを活用していると回答しました。**[5] しかし、これらのサードパーティーのツールは、オンプレミスとクラウドの両方のインスタンスでシームレスに機能し、きめ細かいアプローチを使用して、これまで使用されていた複雑に混合された手法の思わぬ危険も回避していかなければなりません。たとえばセキュリティグループ、VLAN、ファイアウォールなどの手法では、可視性がなく、きめ細かさはないに等しいものでした。



Akamai Guardicore Segmentation でコンテナの採用を実現

Akamai Guardicore Segmentation は、今日の動的なハイブリッドデータセンターのインフラ問題に対応できるように設計されています。Akamai では、さまざまな環境で実行されているアプリケーションやワークロードをすべて包括的に可視化します。また、個々のアプリケーションや論理的にグループ化されたアプリケーションにおいてセキュリティポリシーの作成、実装、適用を迅速化することで、実装が簡単な、きめ細かいソフトウェア定義のセグメンテーションを実現します。

はっきり言うと、Akamai Guardicore Segmentation はコンテナに特化したポイント製品ではありません。むしろ、コンテナセキュリティはプラットフォームの重要機能です。ベアメタルサーバー、仮想マシン、サーバーレスワークロード、リモートデバイスなどの混合環境でも一貫して機能することができます。したがって、単一の包括的なソリューションが提供されるので、場所や実装方法に関係なく、データセンターやクラウドにある資産のセキュリティ確保を実現できます。これにより、ポイントソリューションを複数管理する必要がなくなります。また、ソリューションは基盤となるプラットフォームやオペレーティングシステムから切り離されているため、アプリケーションやワークロードがオンプレミス環境間やクラウド環境間で移行しても、セキュリティポリシーが適用されます。これにより、移植性の要因が強化され、ハイブリッドクラウドのインフラでのアプリケーション実装においてコンテナが最適化されます。

コンテナのセキュリティは、Akamai Guardicore Segmentation プラットフォームの重要機能で、動的で異種混在のデータセンター環境上で一貫した機能を実現します

コンテナに関しては、コンテナのホストノードにエージェントを配置することで Akamai Guardicore Segmentation が機能し、ポッド間やポッドと仮想マシン間の通信フローなど、コンテナクラスター全体の可視化が実現します。これにより、プロセス、ユーザー、完全修飾ドメイン名（FQDN）ごとに、非常にきめ細かいセキュリティポリシーの実装と適用が可能になります。オーケストレーションシナリオにおいては、K8s オーケストレーションをサポートし、Kubernetes や OpenShift メタデータの可視化が可能になり、優れたコンテキストを実現します。柔軟なラベリングモデルにより、オペレーターはネイティブの K8s 用語でポリシーを表現できるようになります。K8s の実行では、ネイティブの Container Network Interface（CNI）を活用します。K8s にポリシーを適用するための非侵入型の手法となり、スケーリングの制限はありません。専用テンプレートを使用すると、名前空間、アプリケーション、その他のオブジェクトなど、Kubernetes のビジネス上重要なアプリケーションをリングフェンスできます。また、K8s のワークロード量や変化率に合わせてスケーリングすることもできます。Akamai のソリューションは、他のあらゆるエンタープライズのワークロードでも同様に機能するため、単一のソリューションとしての利用で、エンタープライズ全体の資産を可視化、管理、保護できるようになります。

DevOps 環境で特に重要なのは、作成するセキュリティポリシーが継続的インテグレーション／継続的デリバリー（CI ／ CD）のプロセスに効果的に統合されることです。これにより、セキュリティが後付け的なものになることはなく、デリバリーモデルに完全に組み込まれるようになります。

結論

コンテナは、多くのビジネス環境においてますます重要になっています。リソースの使用効率を高め、プロセスを合理化し、移植性やスケーラビリティを向上させることができます。同時に、提供される内蔵セキュリティは十分ではありません。特に、ハイブリッド環境を利用する企業にとっては不十分です。

企業の成長とともに拡張できるセキュリティソリューションをお探しなら、プラットフォームに依存しないツールを選んでください。そのようなツールであれば、発生場所に関係なく、エンドツーエンドのプロセスを詳細に把握できるようになります。Akamai Guardicore Segmentation ならそれが可能です。それだけでなく、現在と将来に備えるために、現代のエンタープライズが求めるさまざまな機能を提供します。

Akamai Guardicore Segmentation を使用すると、セキュリティチームは、動的で異種混在のデータセンター環境で一貫性のあるセキュリティを実現できるようになります。これにより、IT チームがコンテナ化を最大限活用できるようサポートし、エンタープライズのビジネスニーズに不可欠な重要アプリケーションの開発や実装を、迅速かつ優れたコスト効率で、安全に行うことができるようになります。

環境全体でセキュリティをシンプル化します。コンテナ向けの強力かつ統合型のセキュリティソリューションなどの詳細については、akamai.com/guardicore をご覧ください。

1 Arun Chandrasekaran、Wataru Katsurashima、「The Innovation Leader's Guide to Navigating the Cloud-Native Container Ecosystem（イノベーションリーダーたちのクラウドネイティブ・コンテナ・エコシステム・ガイド）」、Gartner、2021 年 8 月 18 日。

2 「Cloud Container Adoption In The Enterprise（エンタープライズでのクラウドコンテナ採用）」、Forrester、2020 年 6 月。

3 「Best Practices for Running Containers and Kubernetes in Production（実稼働環境でのコンテナおよび Kubernetes の実行に関するベストプラクティス）」、Gartner、2019 年 2 月 25 日。

4 「State of Kubernetes Security Report（Kubernetes（セキュリティの状況に関するレポート）」、Red Hat、2022 年 5 月。

5 「Gartner Forecasts Strong Revenue Growth for Global Container Management Software and Services Through 2024（Gartner、2024 年にグローバルコンテナ管理ソフトウェアおよびサービスの大幅な増収を予測）」、2020 年 6 月 25 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。