

The Continuous Intelligence Report

第4回「継続的インテリジェンスレポート」

The state of modern applications & DevSecOps in the cloud

クラウドのモダンアプリケーションと
DevSecOpsに関するアニュアルレポート (2019年版)



Fourth annual report, 2019 edition

sumo logic

モダンアプリケーション、DevSecOps、そしてインテリジェンスエコノミーの台頭

Sumo Logicの継続的インテリジェンスプラットフォーム

デジタルビジネスが加速する今日、Sumo Logicはモダンアプリケーションとクラウドインフラストラクチャが生み出す膨大なデータを管理するためのクラウドネイティブなインテリジェンスプラットフォームを提供しています。Sumo Logicのソリューションは、開発とセキュリティ、そしてオペレーション (DevSecOps) というあらゆるビジネスシーンでの活用が想定されています。

世界で2,000社以上がモダンアプリケーションとクラウドインフラストラクチャの構築、そしてセキュリティの確保においてSumo Logicを採用しています。

アプリケーションのアーキテクチャ、プロセス、ツール、およびユースケースの新たなトレンド

第4回目となる2019年のレポートは、業界レポートとしては初めて、そして唯一、モダンアプリケーションの市場浸透状況やユーザーのDevSecOpsの導入状況を定量的に調査し、様々な企業やユーザーの取り組みを通じて、モダンアプリケーションのアーキテクチャに関する主要なトレンドの特定に至っています。



モダンアプリケーションの台頭

市場を牽引する企業は、高いパフォーマンス、拡張性、そして停止することのないデジタルサービスの提供に日々邁進しています。これらのサービスは、カスタマイズされた「モダンアプリケーション」の上に構築されており、新しい階層やテクノロジー、そしてマイクロサービスから構成されるアプリケーションスタックで、通常はAmazon Web Services(AWS)やMicrosoft Azure(Azure)、Google Cloud Platform (GCP)などのクラウドプラットフォーム上で運用されています。

DevSecOpsの導入による迅速性の確保

クラウドアプリケーションを構築する際、多くのエンタープライズ企業はDevOpsやDevSecOpsのツールやプロセスを導入し、信頼のおけるソフトウェアを迅速に開発しています。しかしこれらモダンアプリケーションは置き換えと開発のスピードが早いため、従来のモニタリングやトラブルシューティング、そしてセキュリティ管理ソリューションでは十分に対応できません。この早いライフサイクルを管理する唯一の方法が、クラウドネイティブの継続的インテリジェンスプラットフォームなのです。継続的インテリジェンスプラットフォームを利用することにより、企業はエンドツーエンドのアプリケーションライフサイクルプロセス (開発=>運用=>セキュリティ確保) を自動化し、監視できるようになります。

インテリジェンスエコノミーの台頭

クラウドアーキテクチャとモダンアプリケーションからは莫大な量のデータが生成され、企業はそれを分析して継続的、かつ優れたカスタマーエクスペリエンスへとつなげる必要があります。弊社ではこれをインテリジェンスエコノミーと呼んでいます。リアルタイムに対応できない企業は、インテリジェンスの波に飲み込まれてしまうでしょう。

インテリジェンスの波に乗るためには、継続的インテリジェンスプラットフォームを活用してオペレーションを管理し、セキュリティとコンプライアンスを実現すると同時に、エンドユーザーの振る舞いを理解してビジネスの洞察を得る必要があります。Sumo Logicは唯一、SaaSアーキテクチャをベースにした真のマルチテナントプラットフォームを提供し、インテリジェンスエコノミーの実現を可能にします。

モダンアプリケーション、DevSecOps、そして インテリジェンスエコノミーの台頭

Sumo Logicのユニークなポジションが 本調査を可能にしています

Sumo Logicは2010年の設立以来、業界をリードするクラウドネイティブな継続的インテリジェンスプラットフォームの提供を通して、多岐にわたるモダンアプリケーションやインフラストラクチャに加え、様々な開発、セキュリティ、運用ツールから生成される100ペタバイト以上のデータを日々分析しています。この膨大なデータを分析することにより、エンタープライズから中小まで、あらゆる規模の企業に画期的な洞察を提供し、次世代のモダンアプリケーションとクラウドインフラストラクチャの構築、実行、そしてセキュリティの確保に貢献しています。

本レポートの目的

本レポートの主な目的は、AWS、Azure、そしてGCPなどのクラウドプラットフォーム、そしてハイブリッドクラウドインフラストラクチャの上で実行される大規模かつミッションクリティカルなアプリケーションやテクノロジー

の導入状況を分析し、ベストプラクティスや洞察、そしてトレンドを提供することです。本レポートは、クラウドファースト型の組織が「リフトアンドシフト」する、または既存アプリケーションを刷新して移行する際に使うDevSecOpsのツールやソリューションに関するトレンドについても掲載しています。

本レポートの対象者

本レポートの対象者は、クラウドアーキテクト、サイトリライアビリティエンジニア (SRE)、データエンジニア、オペレーションチーム、DevOps および最高情報セキュリティ責任者 (CISO)、そしてセキュリティオペレーションチームや実務担当者の方々等、多岐に渡ります。本レポートを読んで学んでいただいた内容を、効果的かつ安全なモダンアプリケーションとクラウドインフラストラクチャの構築、実行、およびセキュリティの確保に活かしていただければと考えます。



データ手法と前提条件

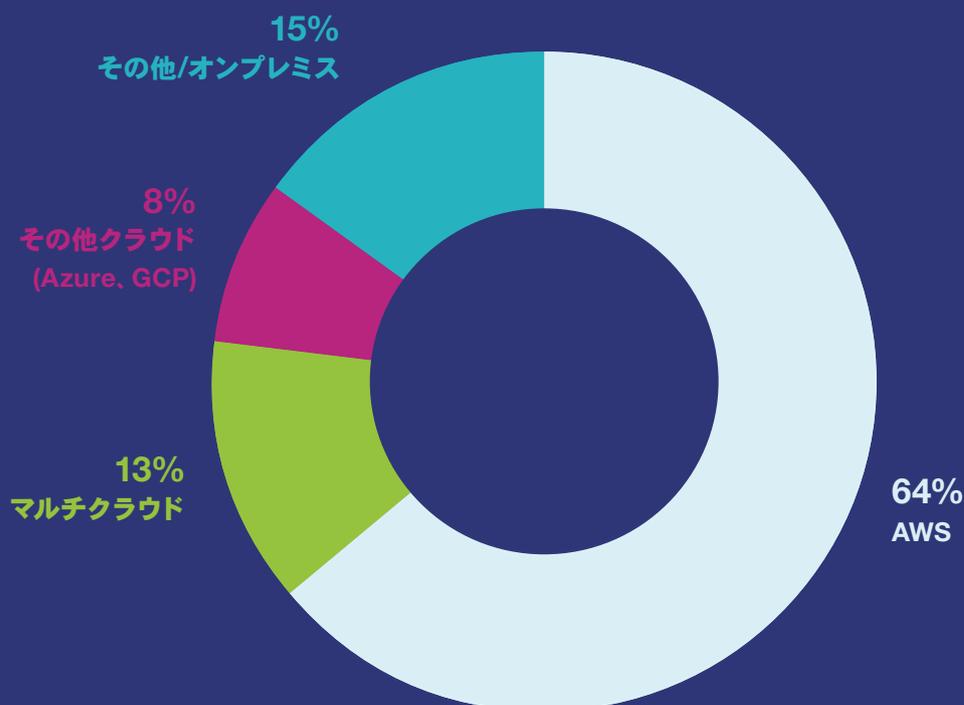
本レポートで使用しているデータは、大手クラウドプラットフォームとオンプレミス環境でアプリケーションを実行している Sumo Logicのユーザー、2,000社以上から取得したものです。個別の顧客データは匿名化されています。

ユーザーは、本番アプリケーションや基盤インフラの管理にSumo Logicを採用しているため、本レポートでは、本番アプリケーションの稼働状況が基礎となっています。

Sumo Logicの継続的インテリジェンスプラットフォームは、100%クラウド上で実行されています。ここから弊社が得たミッションクリティカルかつ大規模な分析やエクスペリエンスも、本レポートでは触れています。

本レポートの作成にあたり、分析対象となるアプリケーションやインフラストラクチャ、そしてそこから発生するソースデータやクエリは、全て本番環境であると想定しています。

Sumo Logicのユーザーの内訳



* データインジェスト量は、ユーザーの内訳とは異なります。

重要なポイント



1

マルチクラウドの導入は昨年から50%上昇。AWSが依然として市場を支配。



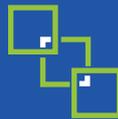
2

Kubernetes (K8s) の導入も引き続き拡大。マルチクラウドユーザーのK8s導入も大幅に増加。



3

コンテナ、オーケストレーション、インフラストラクチャ、およびアプリケーションサービス向けのオープンソースソリューションがトランスフォーメーションを牽引し、オープンソースがモダンアプリケーションスタックの混乱を招いている。6つのインフラストラクチャプラットフォームのうち4つがオープンソーステクノロジーを活用。



4

典型的な企業は、AWSが提供する150以上のサービスの中から、15前後のサービスを利用。導入されている主なサービスは、コンピューティング、ストレージ、データベース、そしてネットワーク。管理ツールなどの付随的なサービスの導入は少ない。



5

サーバーレスが転機を迎えている。3分の1の企業が、AWS Lambdaを本番環境で使用。AWS Lambdaは本番環境以外でも多く使われており、導入件数ではAWSサービスのトップ10に入る。



6

AWSネイティブのセキュリティと脅威インテリジェンスサービスが大規模採用されていることから、企業が次世代のクラウドホスティング型セキュリティテクノロジーの導入を進めていることがわかる。

モダンアプリケーションスタック

本レポートでは、以下のようなクラウド上の新しいモダンアプリケーションに焦点を当てています。

- ・ 新たな階層がモダンアプリケーションスタックを構成。
- ・ これらの新たな階層で新たなテクノロジーが台頭。
- ・ 新たなサービスがアプリケーションオペレーションとセキュリティマネジメントを実現。

DevSecOpsのマネジメントとサービス

アプリケーションサービス

AWS Cloudfront、Akamai、Fastly、他

カスタムアプリケーションコード

Java、Scala、.Net、Rails、Serverless/Lambda、他

アプリケーションランタイムインフラストラクチャ

ウェブサーバー、アプリケーションサーバー、他

データベースおよびストレージサービス

RDS、SQL、NoSQL、S3、他

インフラストラクチャ、コンテナおよびオーケストレーション

Docker、Kubernetes、他



パブリックまたはハイブリッド

IaaSサービスの導入は、 企業のベンダーロックイン回避を示唆

背景

- 市場で公開されているAWS向けサービスは150種類以上あり、コンピューティング、ネットワーク、ストレージ、データベース、ツール、マネジメント、セキュリティ、デベロッパツール、分析等、多岐にわたる。

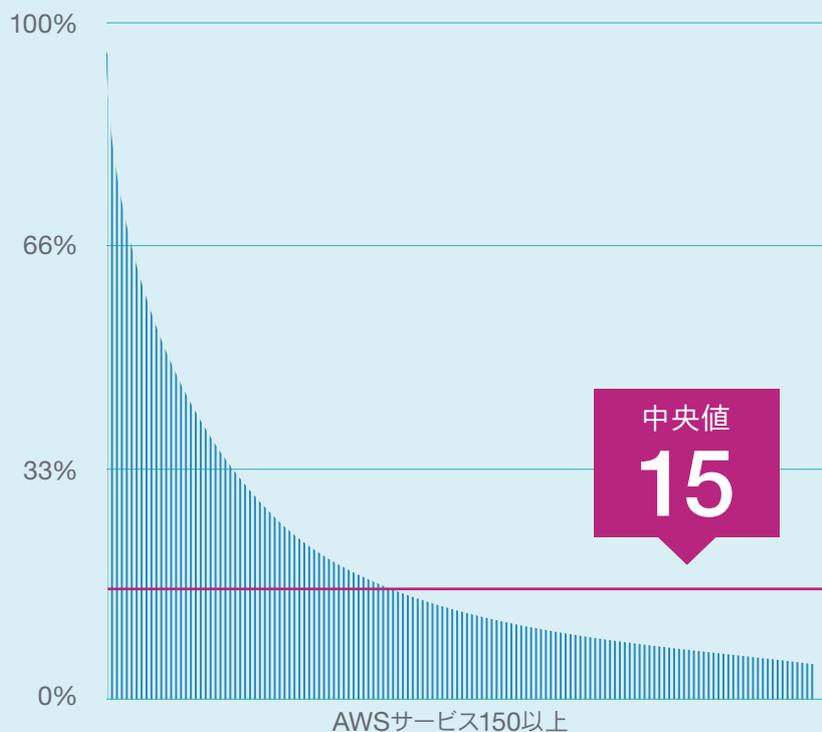
発見事項*

- AWSサービスの中で多くのユーザーに幅広く採用されているサービスは10%未満。ロングテールのサービスはまばらに採用されている。
- 基本的なコンピューティングやストレージ、データベース、ネットワーク、およびアイデンティティサービスが、導入されているAWSサービスのトップ10を構成。
- マネジメントツールや高度なセキュリティサービスの導入は、主要なインフラストラクチャサービスよりも導入スピードがはるかに遅い。

企業はクラウドサービスの導入により、柔軟性とベンダー選択の自由を保持できます。

マルチクラウド戦略を実現する際には、単一ベンダーにロックインされる可能性のあるサービスの導入には注意が必要です。

特に、異なるクラウド間で移植や管理が容易なベンダーが提供するマネジメントツールやセキュリティツールを選択する必要があります。



* AWS CloudTrailサービスの利用状況から特定したデータ

利用されている AWSサービストップ5



EC2



RDS



IAM



STS



CloudFormation

AWSでのDocker導入も引き続き拡大



背景

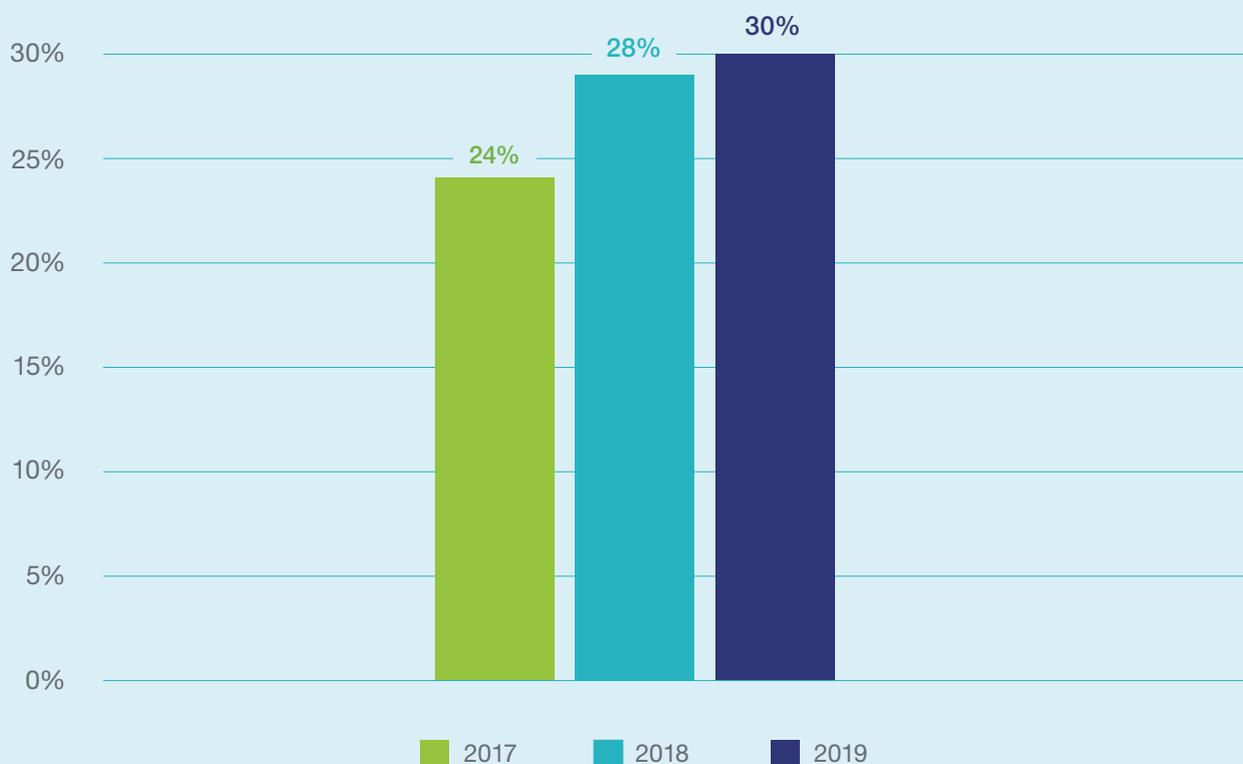
- Dockerをはじめとするコンテナテクノロジーにより、DevOpsチームは分散アプリケーションをより効率的に構築、リリース、そして実行できるように。
- Dockerは、マイクロサービスの構築におけるインフラストラクチャとしても優れた選択肢。

企業の30%がDockerを使用していることから、Dockerがモダンアプリケーションで重要な基盤レイヤーになっていることは明らかです。企業は、マイクロサービスまたはコンテナをベースとしたアーキテクチャを次世代アプリケーションとして検討すべきでしょう。

発見事項

- 企業の3分の1がAWSでDockerを使用。
- Dockerの大規模な導入状況から、マイクロサービスをベースとしたアプリケーションの使用拡大が見て取れる。

AWSでのDocker導入



Kubernetesがオーケストレーション戦争で勝利を収めつつある



背景

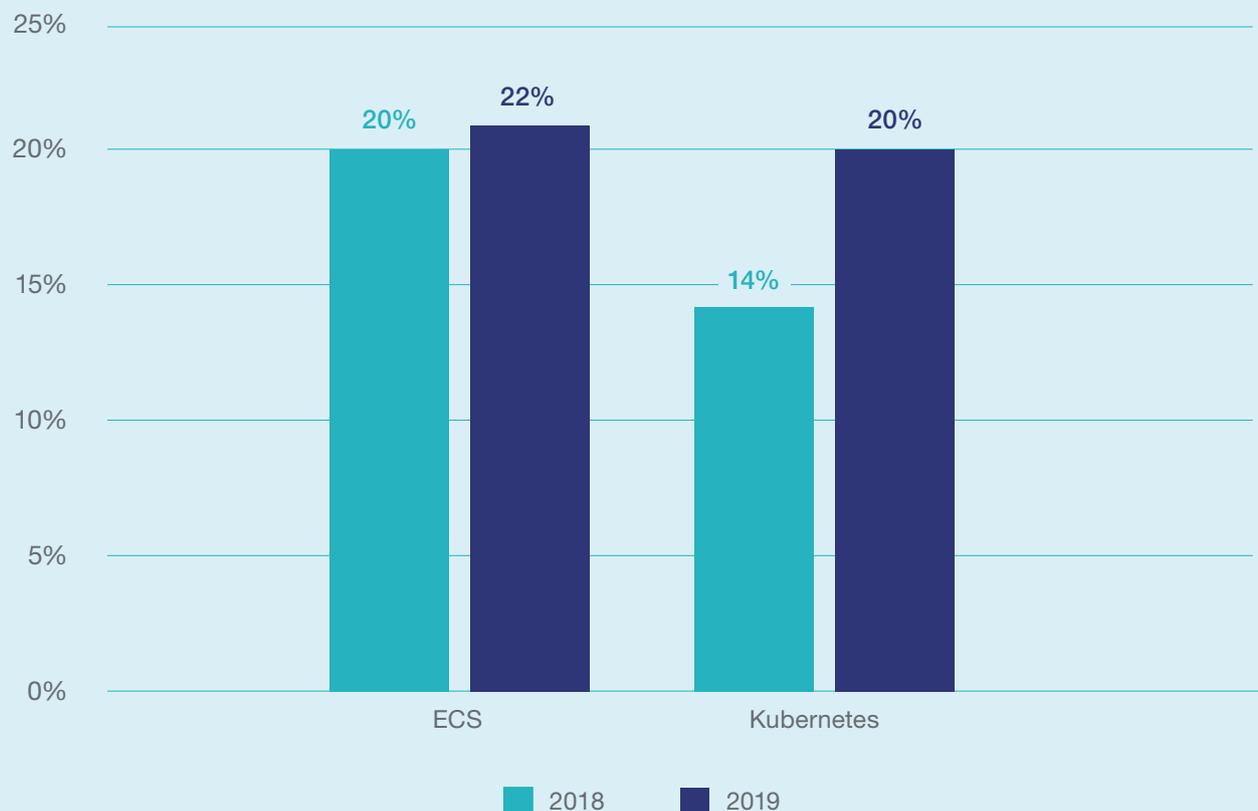
- オーケストレーションテクノロジーがコンテナの展開とスケーリングを自動化。
- コンテナ上で実行されるアプリケーションとワークロードの信頼性も確保。

今後数年で、KubernetesとEKS(Elastic Kubernetes Service)の導入がAWSで加速すると予想されます。またGoogle とAzureのKubernetesサービスの導入も同様に予測されます。

発見事項

- エンタープライズの3分の1がAWSでオーケストレーションテクノロジーを使用。
- 過去12ヶ月、AWSの他のオーケストレーションテクノロジーを大幅に上回るスピードでKubernetesが拡大。

オーケストレーションを使用しているAWSユーザー



Kubernetesがマルチクラウド環境を支配



背景

- Kubernetesはマルチクラウドに対応しており、オンプレミスとクラウド環境を横断したアプリケーションの実行環境でも多くの企業の選択肢となる。

発見事項

- マルチクラウドの利用は、Kubernetes導入の加速と強い相関関係がある。
- GCPユーザーは、他のクラウドユーザーよりも早いスピードでKubernetesを採用している。

企業のマルチクラウド戦略の推進には、Kubernetesが大きな影響を及ぼしています。企業はアプリケーションをKubernetesで展開し、アプリケーションを容易にオーケストレーション、管理、スケールさせて、かつ複数クラウドのアプリケーションに確実かつ柔軟に移植できる状態を確保することが重要です。

Kubernetes - マルチクラウド導入トレンド



* 初期のユーザーデータに基づく

NoSQLがクラウドにおけるRDBMSデータベースの導入を牽引



背景

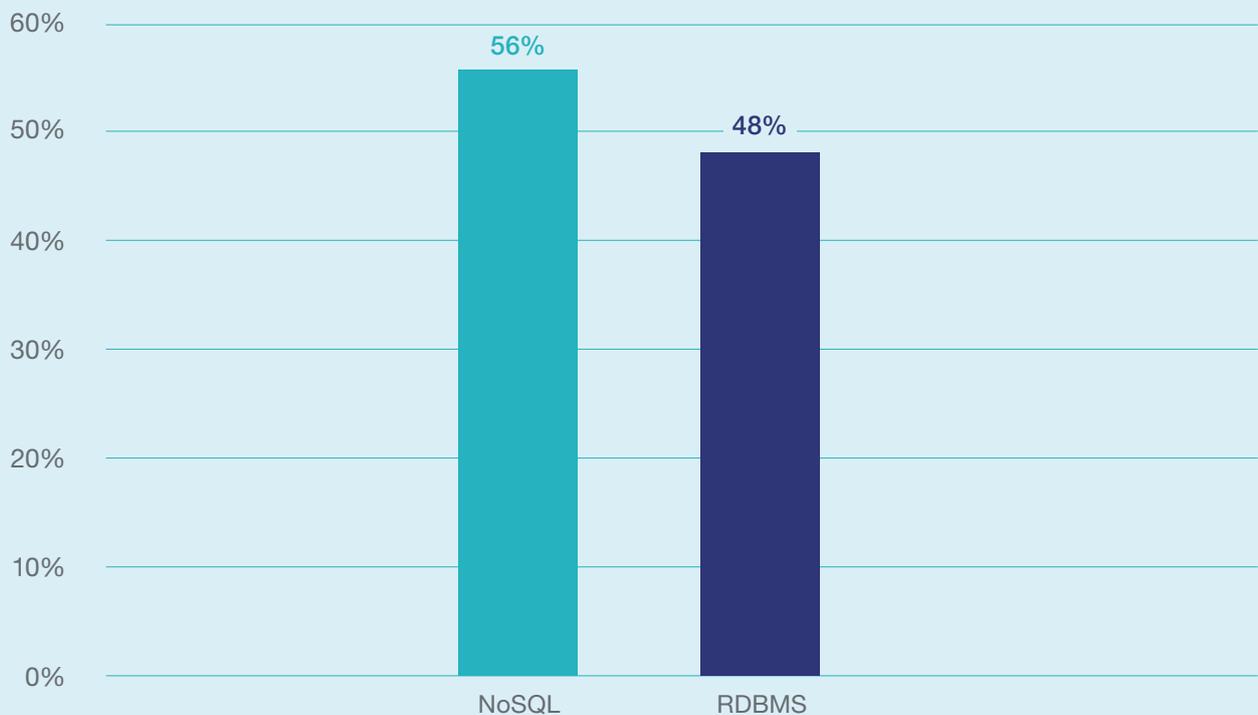
- データベースは多くのアプリケーションにとって中核となる。
- アプリケーションアーキテクチャのデータベースはクラウドへの以降において多数の選択肢がある - Relational DB、NoSQL DB (インメモリーDBを含む)、他。

クラウド移行とマイクロサービスベースのアーキテクチャは、最適なバックエンドのデータストアを選択し、適切なアプリケーションのユースケースを発見する良い機会です。

発見事項

- AWS環境では、NoSQLデータベースの採用がRDBMSデータベースを上回っている。

AWSでのデータベース導入状況



AWS上のデータベーストップ5のうち、NoSQLが3つを占める



背景

- エンタープライズのデータベーステクノロジーの選択肢は広いーオープンソース、商用、NoSQL、インメモリー、ディスクベースなど。

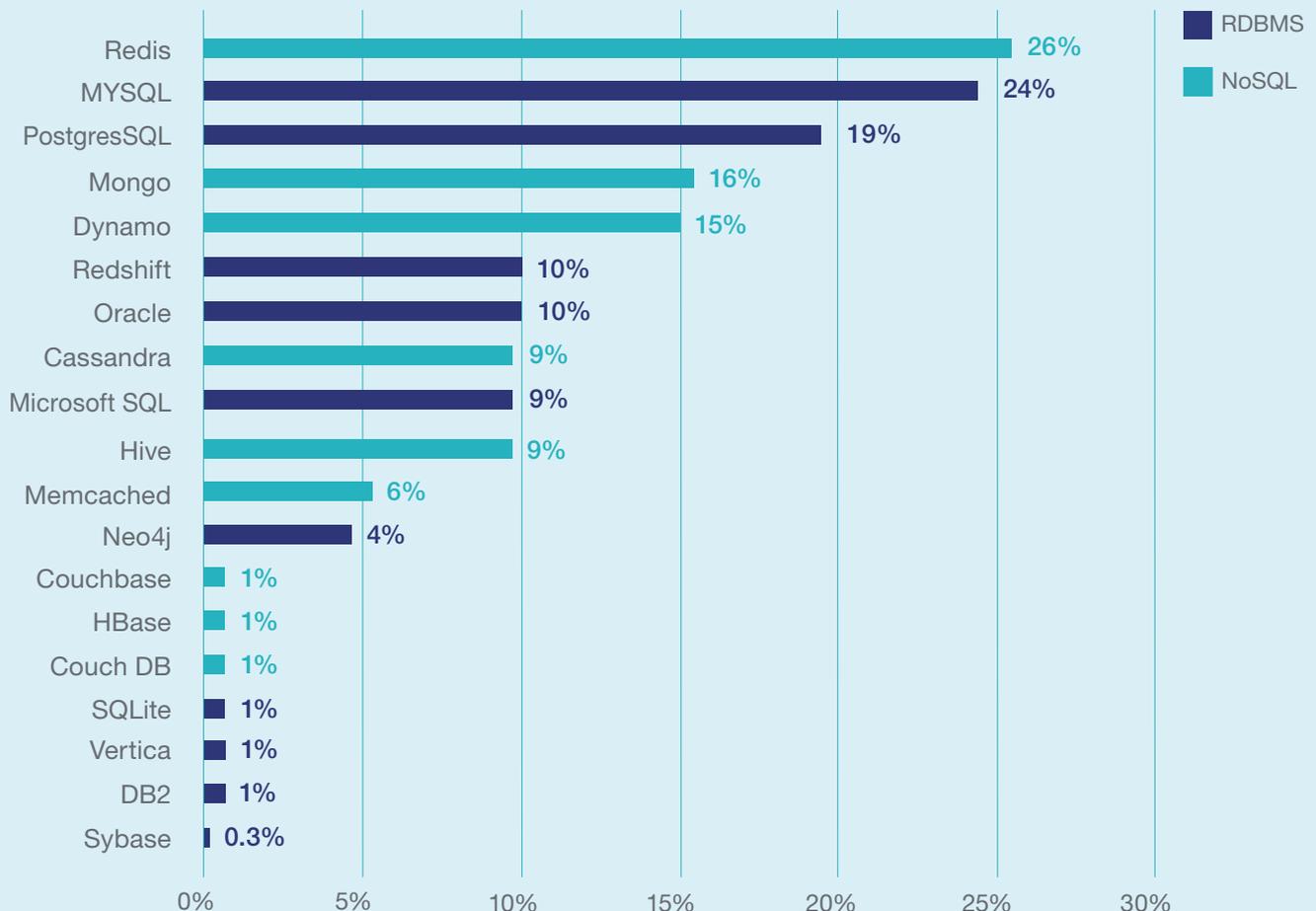
データベースの選択肢としては、トップ5のデータベースーRedis、MySQL、PostgreSQL、MongoDB、Dynamoーを優先して検討すべきでしょう。

発見事項

- RedisがAWSで最も採用されている。
- AWSでの利用においては、Microsoft SQLとOracleDBは大幅に遅れている。

* AWSではMySQLが複数の形態で提供されている（ネイティブまたはRDSソース）。

AWSでのデータベースの利用状況



*一部のユーザーはデータベースを複数使用

NGINXとApacheはAWSで最も選ばれているウェブサーバー



背景

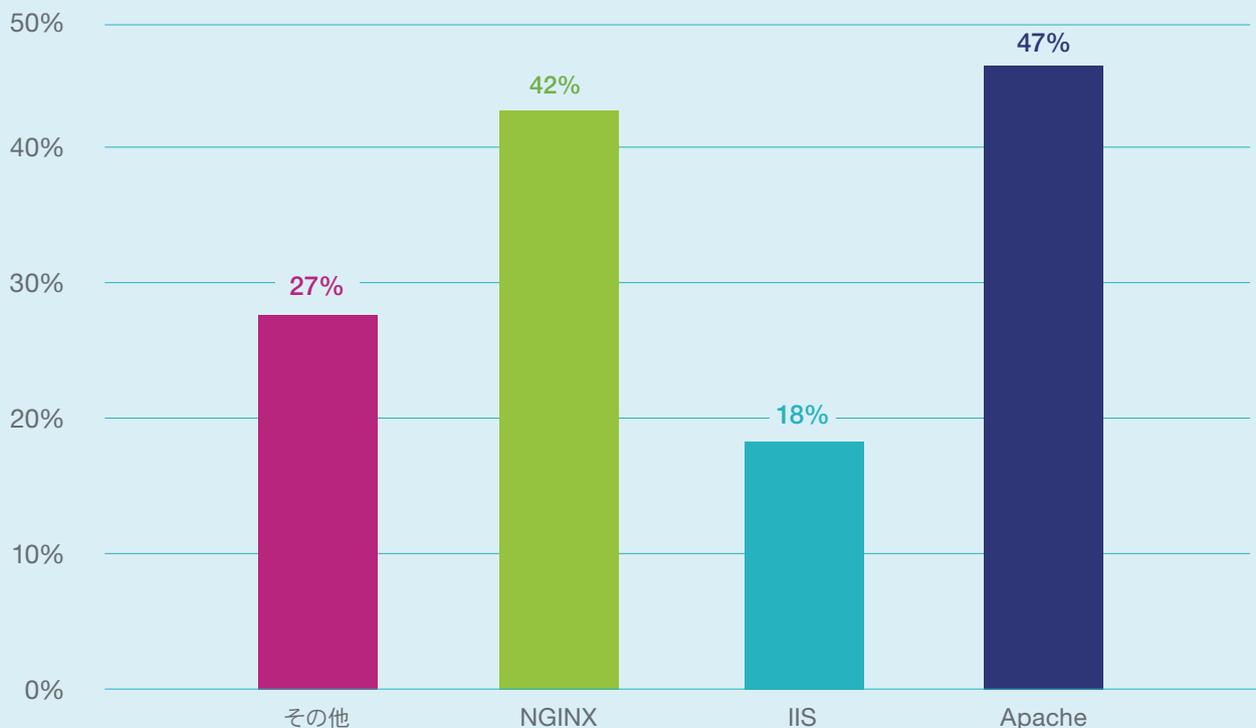
- ウェブサーバーは、モダンアプリケーションの基本構成要素。

AWS環境でアプリケーションを構築する際は、NGINXとApacheをウェブサーバープラットフォームとして検討すべきでしょう。

発見事項

- AWSのウェブサーバーではApacheがリード。
- ApacheとNGINX は、AWSベースのアプリケーションの4分の3で利用されている。

AWSでのウェブサーバーの利用状況*



*一部のユーザーはウェブサーバーを複数使用

IISとApacheはAzureで最も選ばれているウェブサーバー



背景

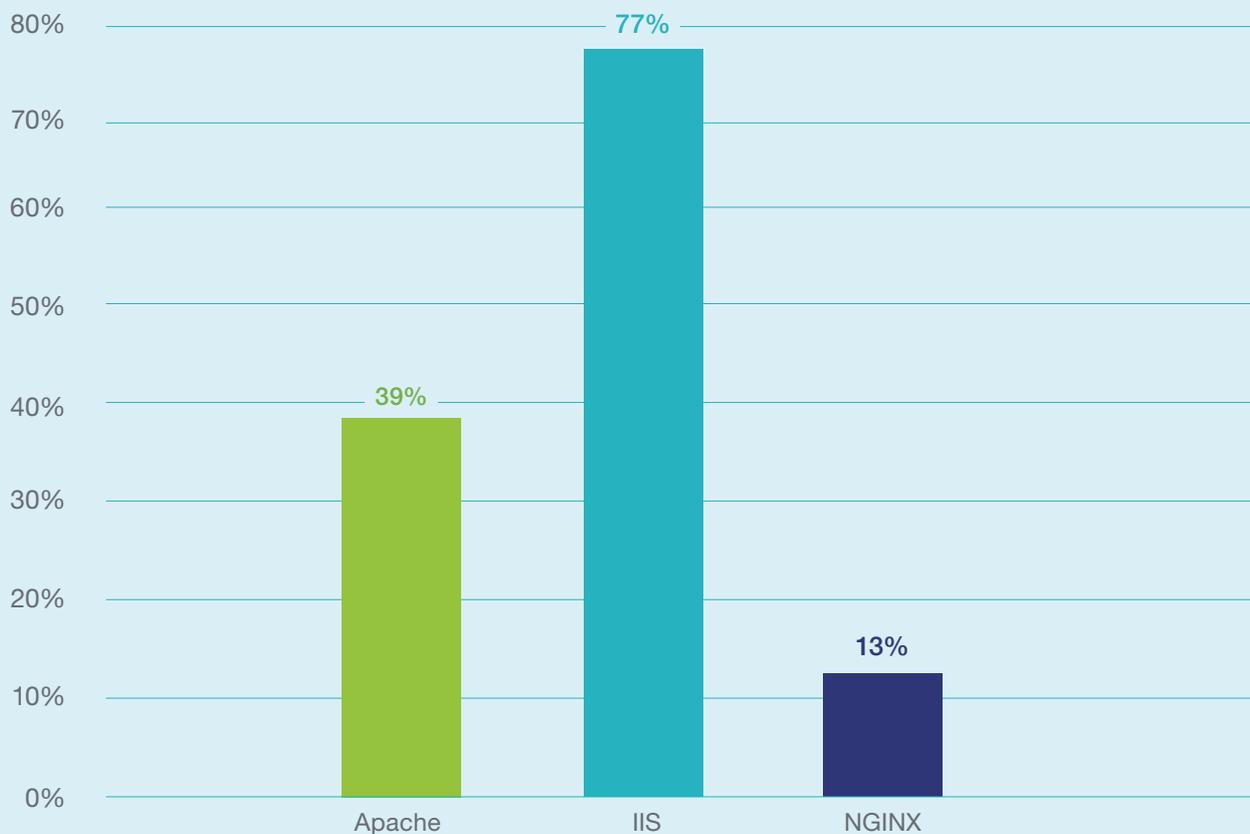
- ウェブサーバーは、モダンアプリケーションの基本構成要素。

Azure環境でアプリケーションを構築する際は、IISとApacheをウェブサーバープラットフォームとして検討すべきでしょう。

発見事項

- AzureのウェブサーバーではIISがリード。
- 多くのAzureユーザーはApacheも使用。

Azureでのウェブサーバーの利用状況*



*一部のユーザーはウェブサーバーを複数使用

サーバーレステクノロジーの導入が引き続き拡大



背景

- AWS Lambdaにより、ITチームはサーバーインフラストラクチャをプロビジョニングしたり管理したりすることなくコードを実行可能。

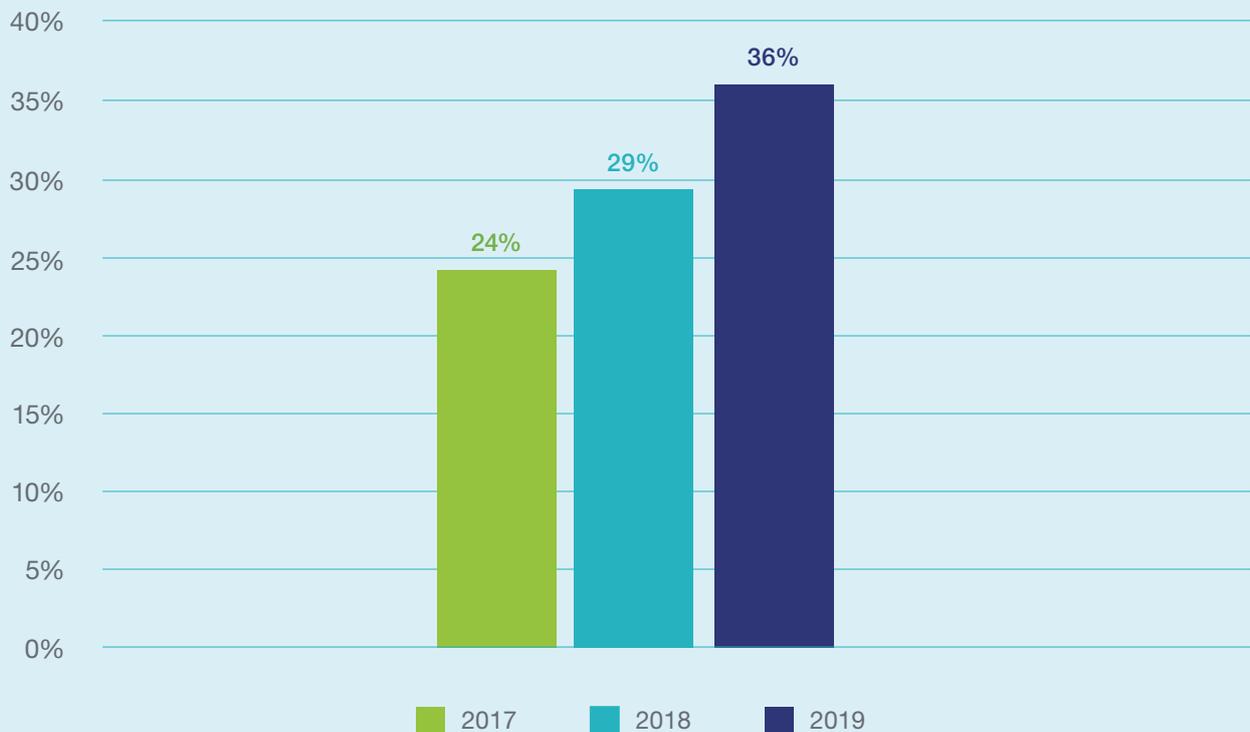
発見事項

- AWS Lambdaの導入は、29% (2018年) から36% (2019年) に大幅に増加。
- AWS Lambdaの初期のユースケースは、クラウド/DevOps展開と自動化が中心。

全ての本番環境で、アプリケーションや自動化テクノロジーとしてLambdaの採用を検討すべきでしょう。

本番かそれ以外の環境かに関わらず、一時的なタスクでもサーバーレスの使用を検討すべきでしょう。

AWSでのLambda導入状況



Amazon CloudFrontがAWSの主要なCDNサービス



背景

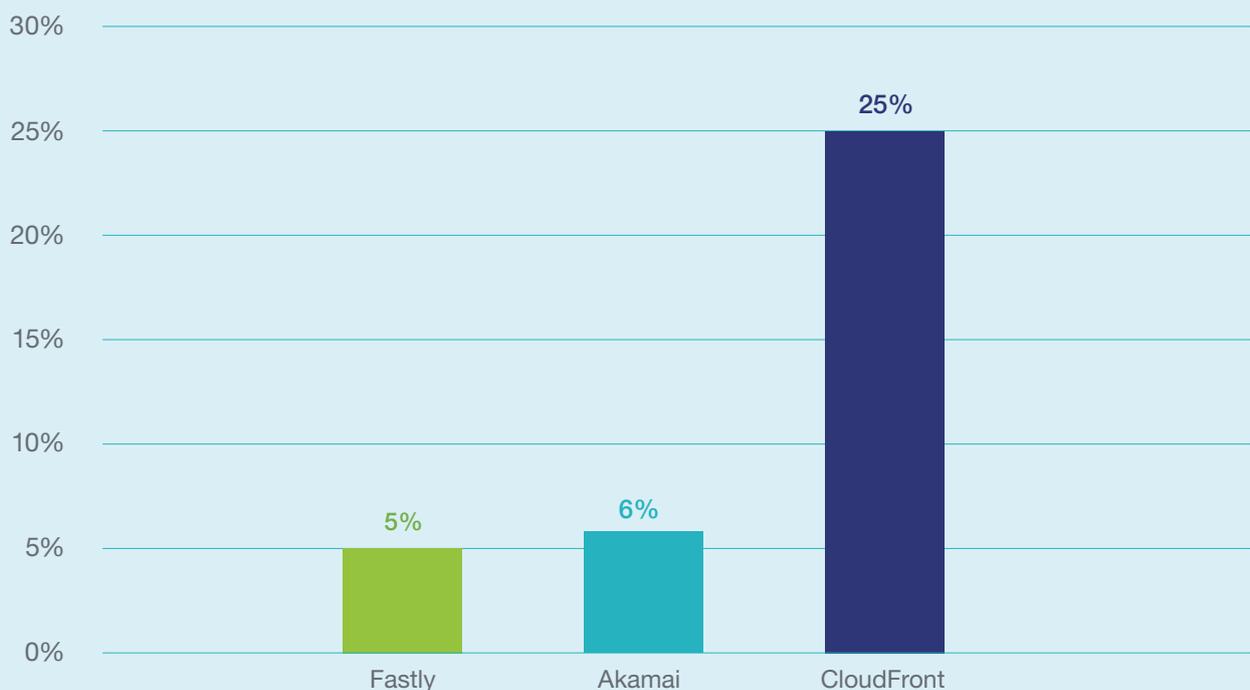
- コンテンツデリバリネットワーク (CDN) は、優れたアプリケーション性能の実現に必要不可欠。
- Amazon CloudFrontは、AWSネイティブのCDNサービス。
- AkamaiとFastlyは、AWSユーザーにサードパーティとしてCDNサービスを提供。

モダンアプリケーションのデリバリ改善策としてCDNを採用する際には、コストと機能、そしてグローバル対応を検討すべきでしょう。

発見事項

- 顧客体験の重要性が増す中、多くのエンタープライズがCDNを導入し、アプリケーションとコンテンツの性能改善を図っている。
- AWSネイティブのCloudFrontは、AWSで最も利用されているCDN。
- 比較的新しいCDNベンダーであるFastlyも、グローバルリーダーのAkamaiと同様に市場で受け入れられている。

AWSでのCDN導入状況



企業は本番環境のCI/CDパイプラインの監視と トラブルシューティングに商用テクノロジーを活用



背景

- DevOpsの導入企業は、継続的な統合・デリバリ (CI/CD) プロセスとツールの監視に取り組んでおり、アプリケーションの俊敏性と信頼性を向上させている。
- DevSecOpsは、セキュリティワークフローを開発プロセス上にシフト (SecからDevへ) するため、DevOpsチームとSOCチームの両方が利用できる高品質かつセキュアな統合プラットフォームが必要となる。

発見事項

- リアルタイムのマシンデータ分析を使った開発/リリースプロセスの監視と可視化は、全ての開発従事者 (開発者、テスト担当者、リリースエンジニア、そしてエクゼクティブ) にとって重要。

- Sumo Logicのユーザーは、ソースコードレポジトリ、ビルド/CI、アーティファクトレポジトリの監視とトラブルシューティング、テスト (静的コード分析、単体/機能テスト)、CD/パイプラインの自動化等を、リリース自動化ツールとSumo Logicのリアルタイムかつ継続的なインテリジェンスプラットフォームを使い実現。

ソフトウェア開発プロセスは、エンタープライズの俊敏性を追跡、改善するために重要です。

開発パイプライン全体 (コードからリリースまで) を監視し、開発プロセスを測定し、常に改善することが重要です。

Sumo Logicが監視に用いられている主なDevOpsツール



AWSユーザーは、アプリケーションセキュリティの改善のため、多くのサービスやテクノロジーを活用



背景

- パブリッククラウドに移行する企業にとって、セキュリティは最重要事項。AWSは複数の「ネイティブ」なアプリケーションセキュリティサービスを提供。
- AWS CloudTrailは、監査とレポートに関するAWSコールの追跡記録を提供。
- AWS VPCおよびVPC Flow Logsにより、企業はセキュアな仮想プライベートネットワークを構築し、そのネットワークに向けたトラフィックを監視することが可能。
- Amazon GuardDutyは、悪意ある、または不正な振る舞いを継続的に監視し、AWSアカウントやワークロードを保護する脅威検知サービス。

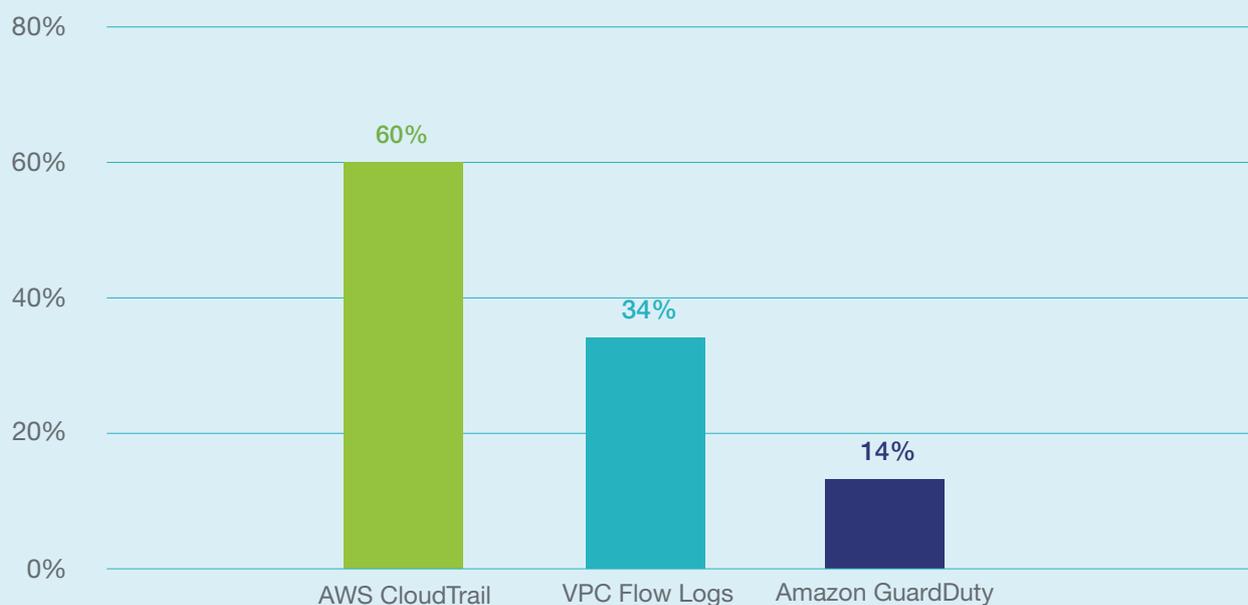
発見事項

- AWSアプリケーションの50%以上が、AWSの成熟した監査サービスであるCloudTrailを利用。
- セキュリティ強化のため、AWSユーザーは仮想プライベートネットワークを実装し、VPC Flow Logsも分析すべき。

クラウド移行時、企業はセキュリティの状況と管理・コントロールについて時間をかけて見直すべきです。

まずはAWS CloudTrailやVPC Flow Logsなどの最低限必要なサービスを活用し、AWS環境のセキュリティを確保することが大切です。

AWSでのセキュリティサービス導入状況



脅威インテリジェンスサービスの導入が進む



背景

- 脅威インテリジェンスとは、コンテキストや仕組み、既存または新たなセキュリティ攻撃やハザードのインジケータを含む、証拠をベースとした知識。
- Amazon GuardDutyは、悪意のある、または不正な振る舞いを継続的に監視し、AWSアカウントとワークロードの保護を支援する脅威検知サービス。
- 多くのサードベンダーの脅威インテリジェンスサービス (CrowdStrike等) は、クラウドからソーシングされた情報を元に、セキュリティの脅威を独自に可視化。

発見事項

- 企業の約半分は、なんらかの脅威インテリジェンスサービスを利用している。

セキュリティの脆弱性に対する企業のプレッシャーは高まっている一方、脅威の環境は常に進化しています。

企業は、既存または新たなセキュリティの脅威についての最新情報を取得するため、脅威インテリジェンスサービスを検討すべきです。

AWSユーザーの脅威インテリジェンスサービスの導入状況



セキュリティベンダーは需要が増すクラウドセキュリティに対応しているが対応方法は様々



背景

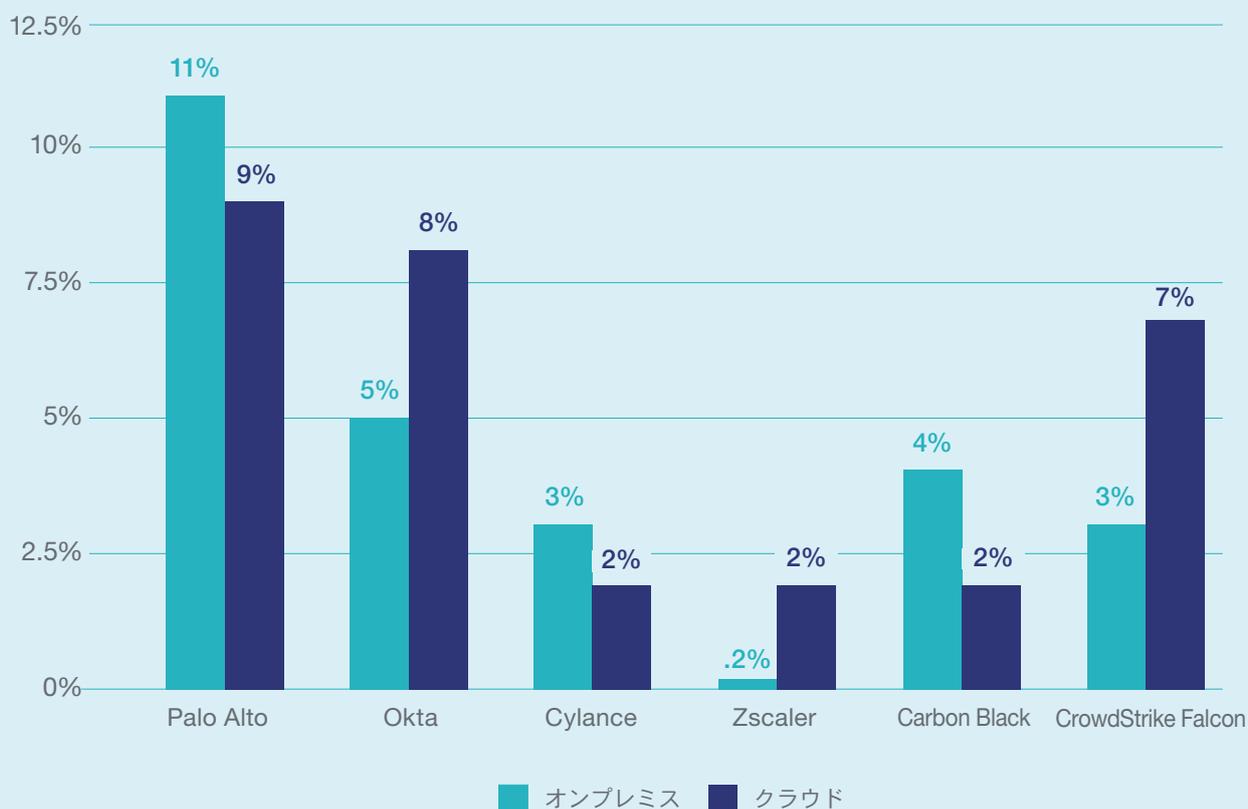
- クラウドセキュリティはオンプレミスセキュリティとは異なる。
- 検討すべき点は、対応するテクノロジー、脅威の対象領域、そしてデリバリーモデル。

サードパーティのクラウドセキュリティソリューションを評価する際には、クラウドファーストセキュリティベンダーを検討すべきでしょう。

発見事項

- クラウドネイティブのベンダーのテクノロジーは、オンプレミスよりもクラウドを活用する企業に浸透している。
- 一部の従来型オンプレミスベンダーがクラウド対応を強気に推し進めている一方、他の従来型のオンプレミスベンダーはクラウドへの対応が遅れている。

Sumo Logicに統合されたセキュリティツールの導入状況



Sumo Logicについて

Sumo Logicを使い、エンタープライズ企業はモダンアプリケーションの構築と展開、そして強固なセキュリティを実現しています。

2,000社以上の顧客

膨大な量のAWSデータを分析

1日あたりのデータ分析量

**100
PB超**

1日あたりの検索数

**3,000
万件以上**

1日あたりのクエリ数

**5,000
兆件以上**

Sumo Logicは、DevSecOpsライフサイクルとスタック全体にわたって可視化を提供する、セキュアでクラウドネイティブな継続的インテリジェンスプラットフォームです。世界で2,000社以上がSumo Logicを使い、モダンアプリケーションとクラウドインフラストラクチャを構築・実行し、セキュリティを確保しています。

詳しくはこちら www.sumologic.jp

s

u

See business differently

m

o



sumo logic

Sumo Logic ジャパン株式会社

〒101-0051 東京都千代田区神田神保町2-11-15 住友商事神保町ビル 2F
www.sumologic.jp

© Copyright 2019 Sumo Logic, Inc. All rights reserved. Sumo Logic, Elastic Log Processing, LogReduce, Push Analytics and Big Data for Real-Time IT are trademarks of Sumo Logic, Inc. All other company and product names mentioned herein may be trademarks of their respective owners. Updated 09/19