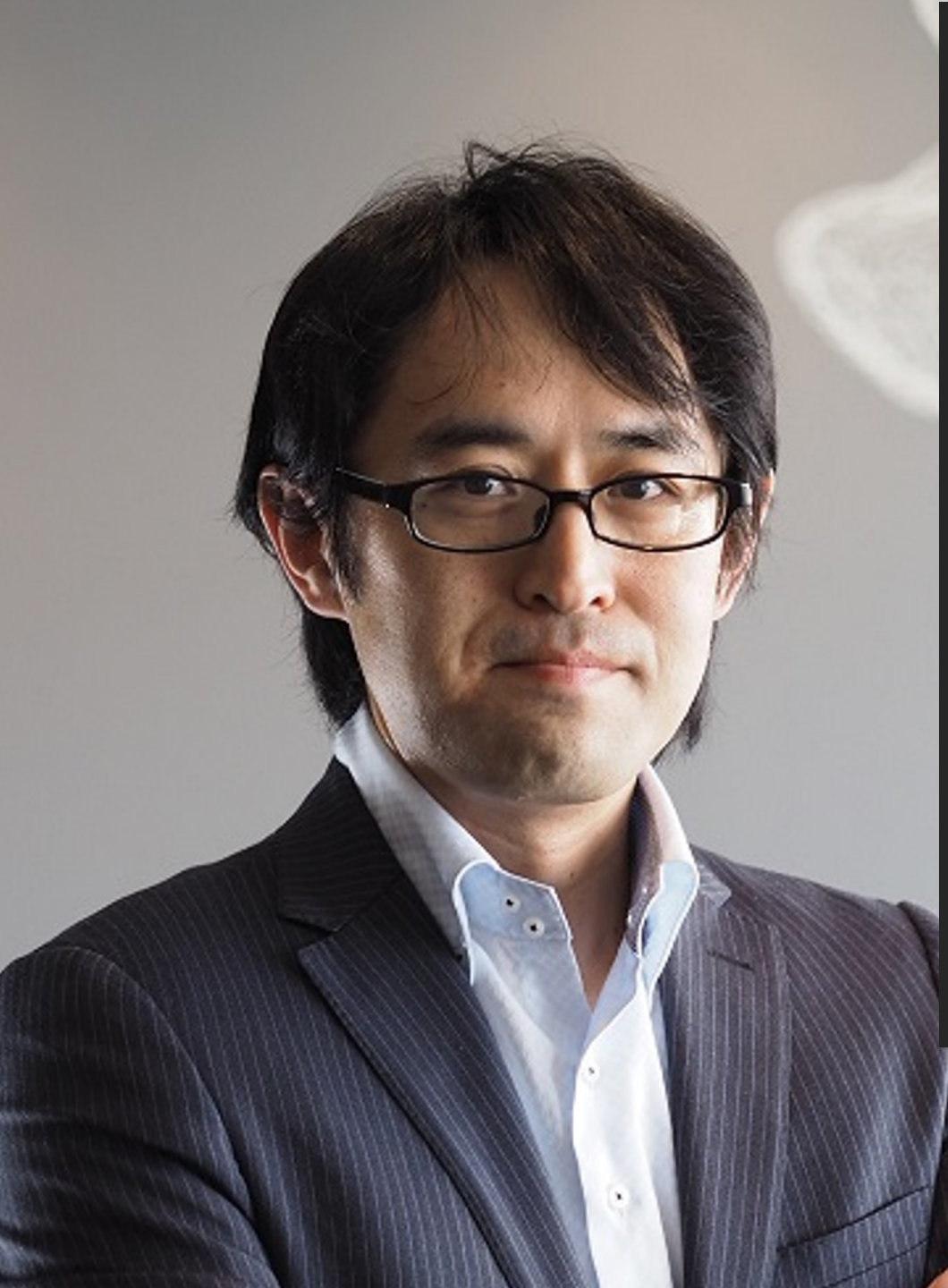
CSA JAPAN SUMMIT 2023

AWS活用の最新動向

アマゾン ウェブ サービス ジャパン 合同会社

パブリックセクター技術統括本部
統括本部長 / プリンシパルソリューションアーキテクト
瀧澤 与一



瀧澤 与一

アマゾンウェブサービスジャパン合同会社
パブリックセクター技術統括本部
統括本部長 / プリンシパルソリューションアーキテクト

2014年 最初の金融専任SAとして、AWSにジョイン。
2015年 エンタープライズソリューションアーキテクトチームの本部長。
2019年 スペシャリストソリューションアーキテクトチーム本部長。
2021年 パブリックセクター技術統括本部 統括本部長

- 経済産業省 クラウド安全性評価 管理基準WG 専門委員
- 独立行政法人情報処理推進機構（IPA）
  クラウドサービスのセキュリティ対策に係る管理基準WG 委員
- 著書：Amazon Web Services企業導入ガイドブック

Agenda

1. AWSとは？
2. AWSのセキュリティ
    1. 可視性と自動化
    2. デジタル統制の考え方
    3. 環境変化に適合したセキュリティの包括的な取り組み

Agenda

1. AWSとは？
2. AWSのセキュリティ
    1. 可視性と自動化
    2. デジタル統制の考え方
    3. 環境変化に適合したセキュリティの包括的な取り組み

Our Mission

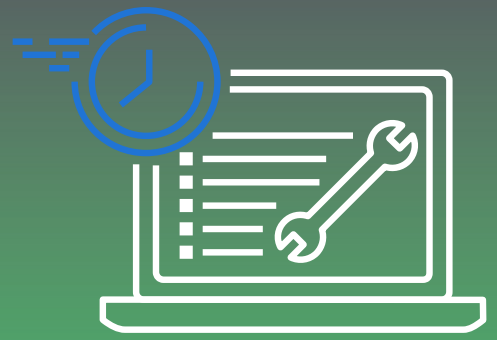
Amazonは、地球上で最もお客様を大切にする企業、そして地球上で最高の雇用主となり、地球上で最も安全な職場を提供することを目指しています。

AWS とは

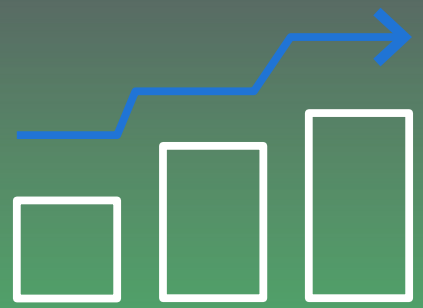
- 2006 年より、他社にさきがけてクラウドサービスを提供
- 世界数百万、日本では数十万以上のお客様
- 世界 31地域 99のデータセンター群から、200以上のクラウドサービスを提供
- 全国をカバーするパートナーコミュニティ：AWSパートナーネットワーク
- 累計で129 回値下げをして利益をお客様へ還元 (2022年9月14日時点)
- 世界中の143 のセキュリティ基準とコンプライアンス認証をサポート。

※ お客様とはアクティブカスタマー数を指します。アクティブカスタマーとは、AWS クラウド無料利用枠を含むAWS アカウントの先月の使用状況のあるアマゾン会員でない対象アカウントです。

クラウドの真価とは 価値創造に集中できること



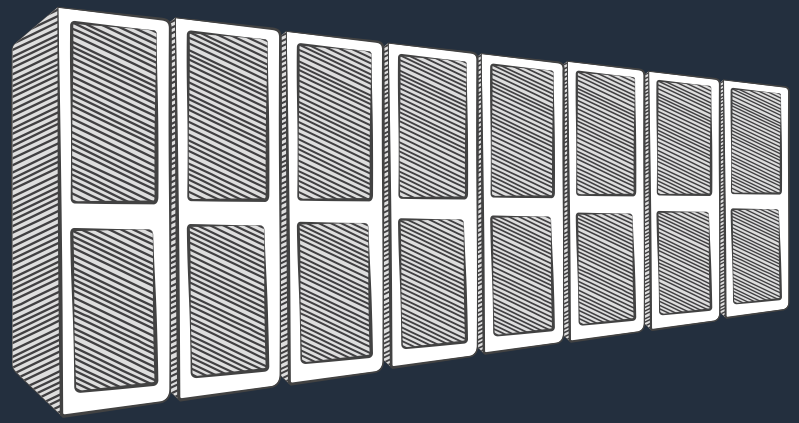
すぐに使い始められる

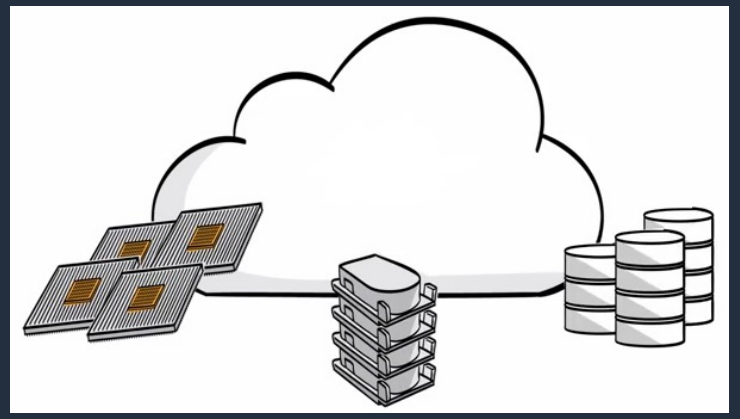


必要なときに必要なだけ使うことが可能

アイデアから実装までの時間を短縮

コストを削減しながら
迅速にアイデアを試し、**イノベーション**を加速





初期投資が発生
余剰・不足のリスク
固定費発生　→　リスクをとりづらい

初期投資が不要
必要な分だけ利用可能
変動費　→　リスクを管理しながら
新しい事業アイデアを試せる

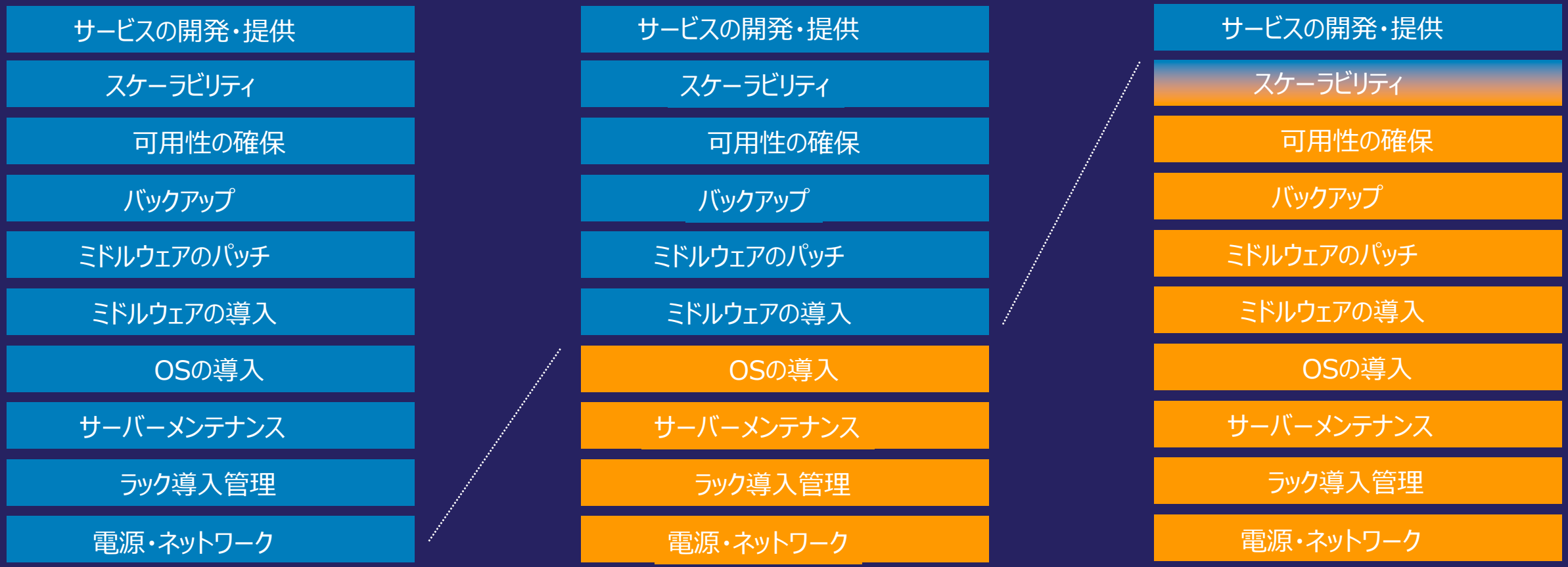
200 を超える幅広いサービスであらゆるワークロードをサポート

- コンピューティング
- モバイル
- ARとVR
- エンドユーザーコンピューティング
- ストレージ
- データベース
- ネットワークとコンテンツ配信
- AWS コスト管理
- 機械学習
- IoT
- ロボット工学
- ビジネスアプリケーション
- メディアサービス
- 分析
- マネジメントとガバナンス
- 開発者用ツール
- アプリケーション統合
- Game Tech
- 量子テクノロジー
- カスタマーエンゲージメント
- 移行と転送
- ブロックチェーン
- セキュリティ、ID、コンプライアンス
- 人工衛星

*2021年4月時点の情報

マネージド型サービスの利用で価値創造に集中

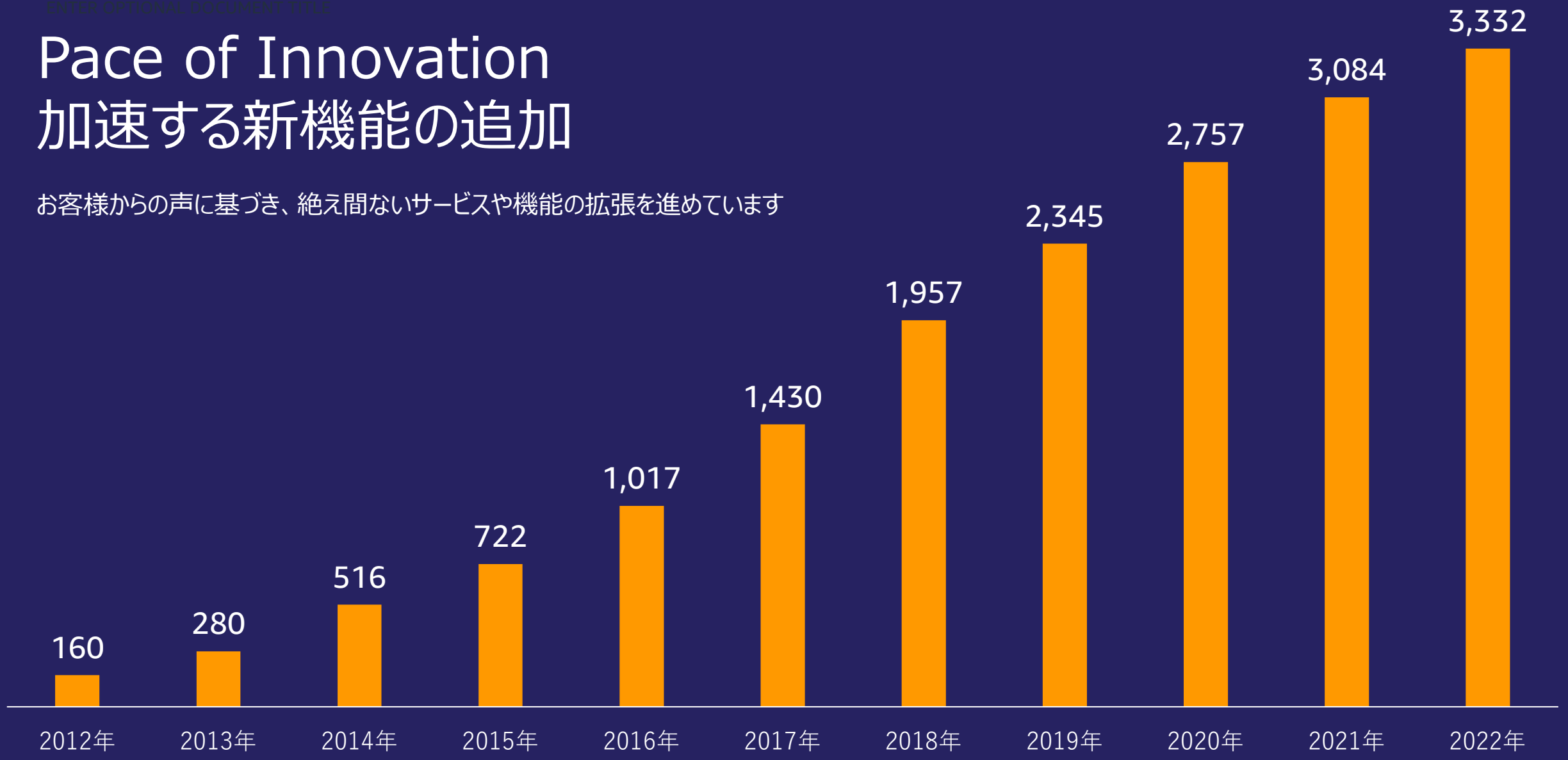
AWSにはサーバーレス アプリケーションの構築と実行に利用可能な一連のマネージド型サービスが用意されています
マネージド型サービスの活用により市場投入までの時間を短縮すると同時に、イノベーションに注力できます



AWSが提供するレイヤー　お客様に管理いただくレイヤー

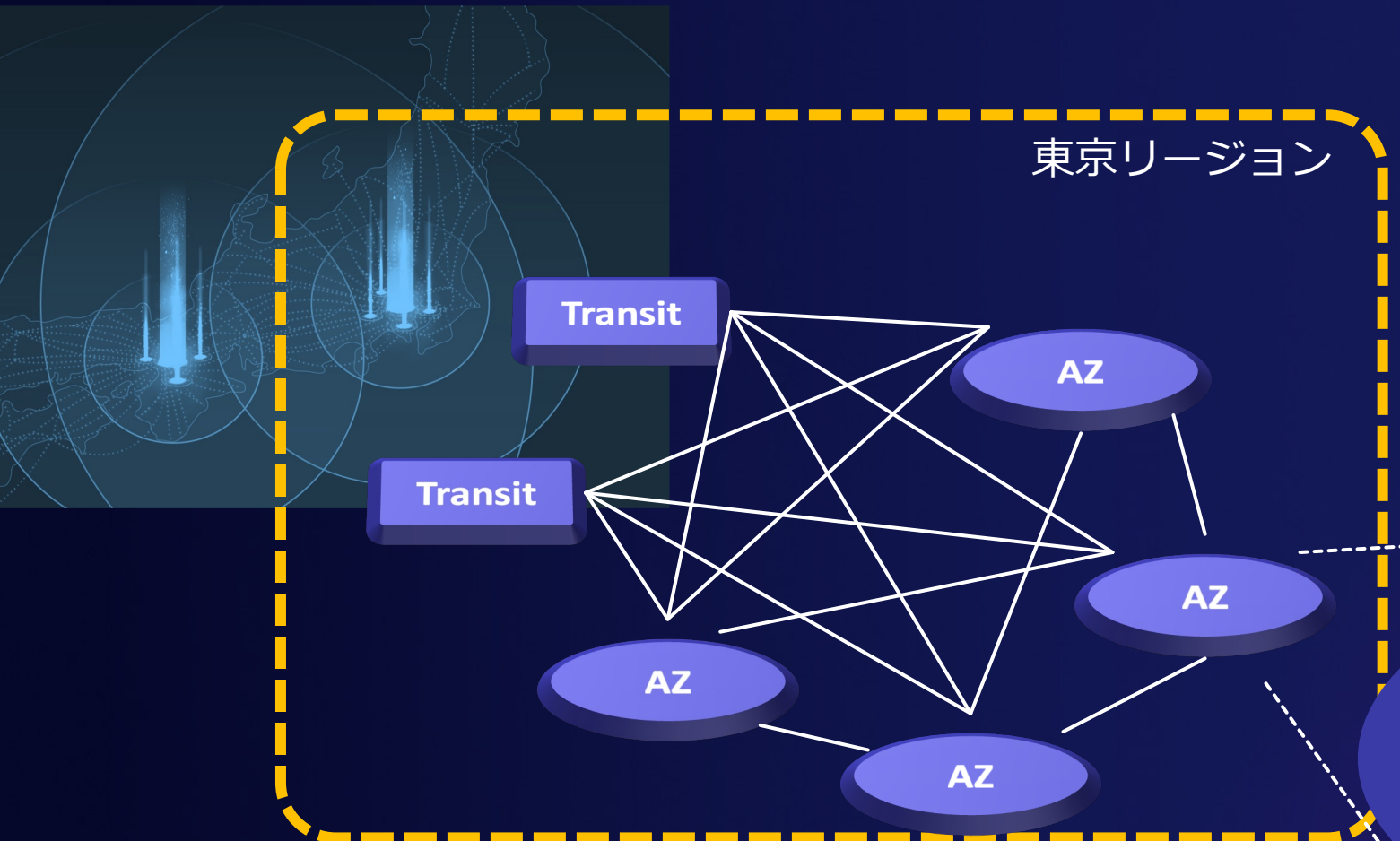
Pace of Innovation
加速する新機能の追加

お客様からの声に基づき、絶え間ないサービスや機能の拡張を進めています

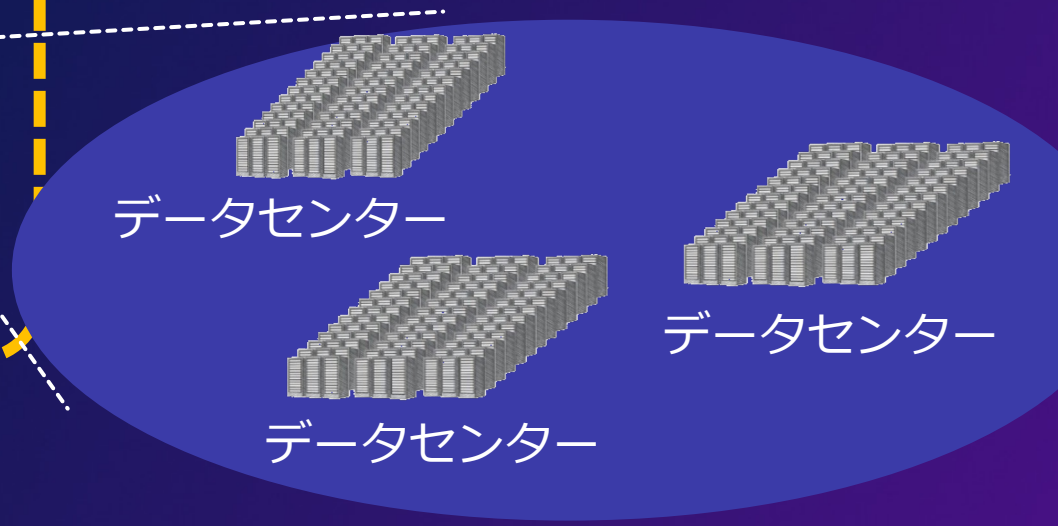


東京と大阪　2 つのリージョンで、ミッションクリティカルなニーズに対応

高可用性・耐障害性を実現するための インフラストラクチャー



AWS のリージョンは複数の
Availability Zone (AZ) で構成
AZ 間は高速ネットワークで接続され、
遅延は数ミリ秒



AWS の日本における投資

AWSの日本のインフラストラクチャは、製造業、自動車産業、金融機関、ヘルスケアから市民サービスまで、日本の様々な業種の大企業、スタートアップ、公共機関のお客様のイノベーションを実現しています。AWSの日本のインフラストラクチャへの投資は、AWSの日本への長期に渡るコミットメントと、お客様のニーズへの強い理解を示しています。

AWSの日本における投資と経済効果（2011年～2022年）

1兆3510億円

東京と大阪の AWS リージョンに関する総設備・運用投資 (2011年～2022 年)

1兆3060億円

東京・大阪の AWS リージョンによる国内総生産 (GDP)への寄与(2011年～2022 年)

20,300+人

2022年のサードパーティにおけるフルタイムの雇用創出（建設、エンジニアリング、コンピュータープログラミング、情報通信などを含む）




AWS は、テクノロジーとデータを民主化し、
一人ひとりがデジタルの恩恵を享受できる社会の実現に貢献します




THE Paris...
CLIMATE 10 years
PLEDGE Early

2025 年までに再生可能エネルギーの
電力比率を **100%** に

2030 年までに
50% の配送で炭素ゼロ化

2040 年までに
炭素ゼロ化を **100%** 達成

78% 削減

自社所有のデータセンターと比較した場合の
カーボンフットプリント削減量

Source: 451 Research, 2021, all rights reserved

- クラウドに移行するとコストが下がる、効率性が上がる

27.4%
Reduction in overall spend per user

57.9%
Increase in VM managed per admin

56.7%
Decrease in downtime

37.1%
Decrease in time to market for new features/ applications

AWS Well-Architected Frameworkに
AWS Well-Architected Sustainability Pillarを追加

新たなPillar(柱)「Sustainability」
の追加をre:Invent 2021にて発表

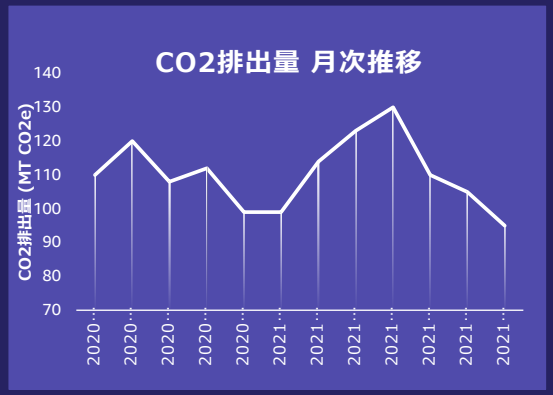
- 持続可能性を目標設定する組織の増加から、その**実現に向けたベストプラクティスを集積**
- **クラウドのワークロードによる環境へのインパクトを最小化**するため、リソース利用率の向上、必要リソース量を削減する概念を含める

AWS Well-Architected Framework
アーキテクトが優れたクラウドインフラストラクチャを設計するための
ベストプラクティス集

AWS Customer Carbon Footprint Toolを提供

- お客様のAWS利用実績による CO2 排出量のモニタリング、分析、将来予測を提供（2022年初頭に提供開始予定）

利用実績に基づき、月ごとのCO2排出量をモニタリング



オンプレミスからクラウド移行による
CO2排出削減効果を推定

貴社の炭素排出量の概要
オンプレミス施設との比較

1843 MTCO2e
AWS利用の炭素排出量

1401 MTCO2e
オンプレ比較での削減量

削減排出量の内訳

13 MTCO2e
AWSの再生可能エネルギー購入効果

1388 MTCO2e
AWSクラウドサービス使用による削減効果

Agenda

1. AWSとは？
2. AWSのセキュリティ
    1. 可視性と自動化
    2. デジタル統制の考え方
    3. 環境変化に適合したセキュリティの包括的な取り組み

クラウドセキュリティはAWSの最優先事項

AWSを活用する利点

- 優れた可視性と制御による安全な拡張
- 統合されたサービスでリスク対策を自動化し、リスクを低減
- 最高水準のプライバシーとデータセキュリティ
- セキュリティパートナーとのエコシステム
- 包括的なセキュリティとコンプライアンス管理

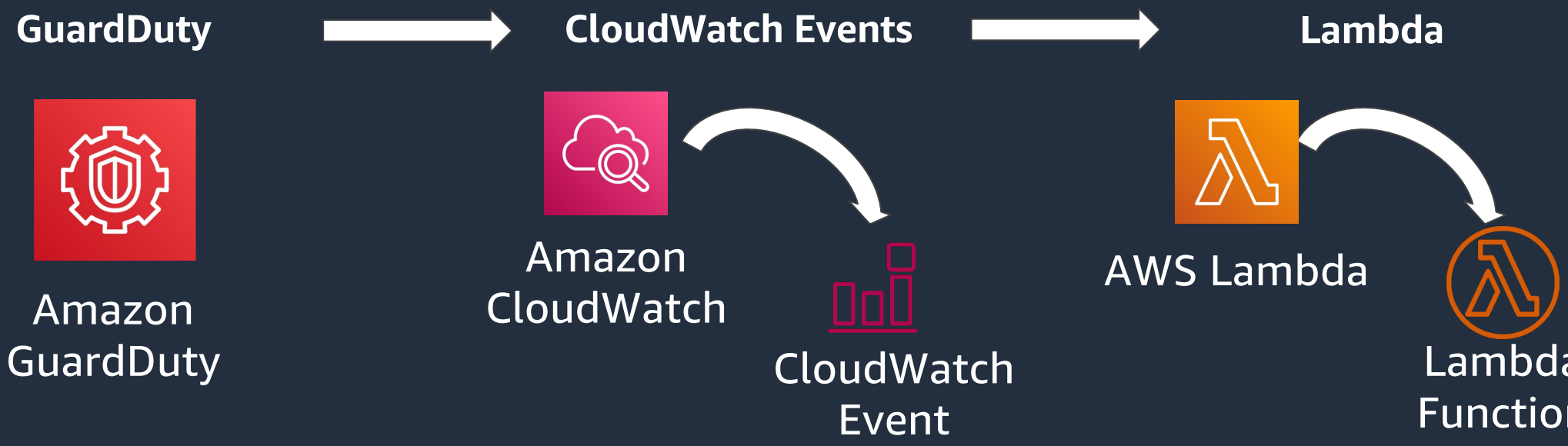
クラウドセキュリティはAWSの最優先事項

可視性

自動化

Amazon GuardDuty
インテリジェントな脅威検出で
AWS アカウントを保護

セキュリティインシデントの検知から自動化



自動化の利点：

検知から対処までの時間を短縮することができ、**リスクを回避または軽減**することが可能

AWSが提供するセキュリティ、アイデンティティ、コンプライアンスサービス

カテゴリ	概要	AWS のサービス
ID及びアクセス管理	ID と AWS のサービスおよびリソースへのアクセスを安全に管理する	AWS Identity and Access Management (IAM)
	複数の AWS アカウントやアプリケーションへのワークフォースのアクセスを一元管理	AWS IAM アイデンティティセンター (SSO の後継)
	安全でフリクションレスなカスタマー ID およびアクセス管理の実装と拡張	Amazon Cognito
	カスタムアプリケーション内できめ細かい権限と承認を管理する	Amazon Verified Permissions (プレビュー)
	フルマネージドのマイクロソフトアクティブディレクトリサービスで効率を高める	AWS Directory Service
	複数のアカウント間でAWSリソースを簡単かつ安全に共有	AWS Resource Access Manager
	AWS リソースをスケーリングする際に、環境を一元管理する	AWS Organizations
検出	AWS のセキュリティチェックの自動化とセキュリティアラートの一元化	AWS Security Hub
	インテリジェントな脅威検出で AWS アカウントを保護	Amazon GuardDuty
	大規模な自動化された継続的な脆弱性管理	Amazon Inspector
	数巣s轍鮒でセキュリティデータを自動的に一元化	Amazon Security Lake (プレビュー)
	リソースの構成を評価、監査、評価する	AWS Config
	AWS、オンプレミス、および他のクラウド上のリソースとアプリケーションを観察および監視する	Amazon CloudWatch
	ユーザーアクティビティと API 使用状況の追跡	AWS CloudTrail
	IoT デバイスとフリート全体のセキュリティ管理	AWS IoT Device Defender
ネットワークとアプリケーションの保護	アカウント全体のファイアウォールルールを一元的に構成および管理する	AWS Firewall Manager
	VPC 全体に Network Firewall セキュリティをデプロイする	AWS Network Firewall
	マネージド DDoS 保護でアプリケーションの可用性と応答性を最大化する	AWS Shield
	VPN なしで企業アプリケーションに安全にアクセス	AWS Verified Access (プレビュー)
	一般的な攻撃からウェブアプリケーションを保護	AWS Web Application Firewall (WAF)
	VPC のアウトバウンド DNS トラフィックのフィルターと制御	Amazon Route 53 Resolver DNS Firewall
データ保護	大規模な機密データを検出して保護する	Amazon Macie
	データを暗号化またはデジタル署名するためのキーを作成および管理する	AWS Key Management Service (AWS KMS)
	AWS 上のシングルテナントのハードウェアセキュリティモジュール (HSM) の管理	AWS CloudHSM
	AWS のサービスと接続されたリソースを使用した SSL/TLS 証明書のプロビジョニングと管理	AWS Certificate Manager
	リソースを識別してデータを保護するためのプライベート証明書を作成する	AWS Private Certificate Authority
	シークレットのライフサイクルを一元的に管理する	AWS Secrets Manager
インシデントへの対応	セキュリティデータを分析および視覚化して、潜在的なセキュリティ問題を調査する	Amazon Detective
	スケーラブルでコスト効率性に優れた AWS へのアプリケーションの復旧	AWS Elastic Disaster Recovery
コンプライアンス	AWS のコンプライアンスレポートにオンデマンドでアクセスできる、無料のセルフサービスポータル	AWS Artifact
	AWS の使用状況を継続的に監査して、リスクとコンプライアンスの評価を簡素化する	AWS Audit Manager

https://aws.amazon.com/jp/products/security/

Amazon Security Lake (Preview)

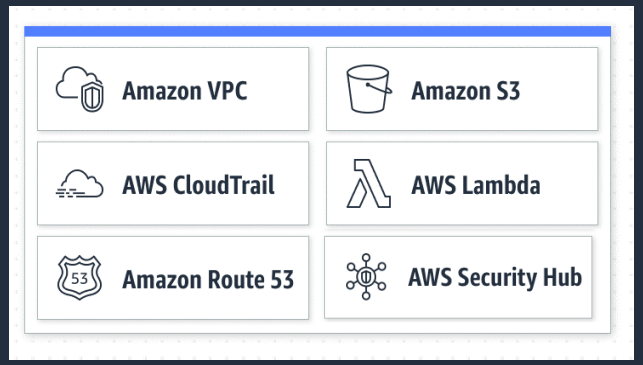
クラウド、オンプレミス、カスタムソースからのデータをリージョン全体で一元化

セキュリティデータを最適化して、より効率的なストレージとクエリのパフォーマンスを実現

データを業界標準に標準化して、複数の分析ツールと簡単に共有

セキュリティデータの管理と所有権を維持しながら、好みの分析ツールを使用して分析が可能

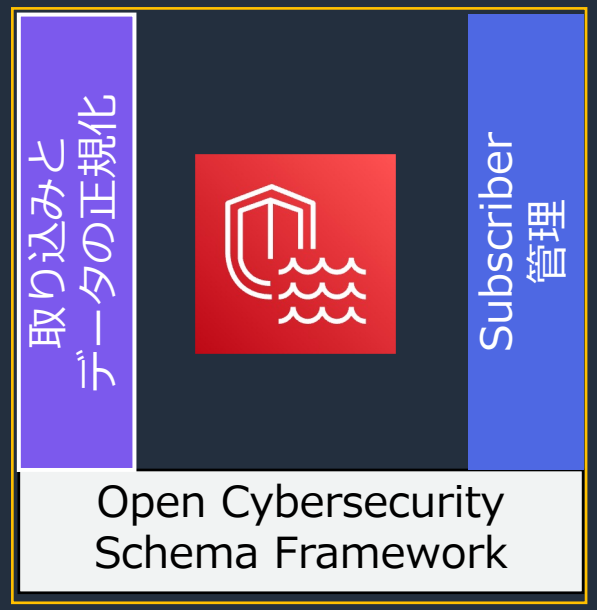
Amazon Security Lake の動作



AWS サービス

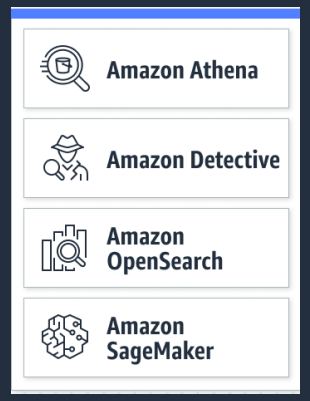
ログデータ

Amazon Security Lake



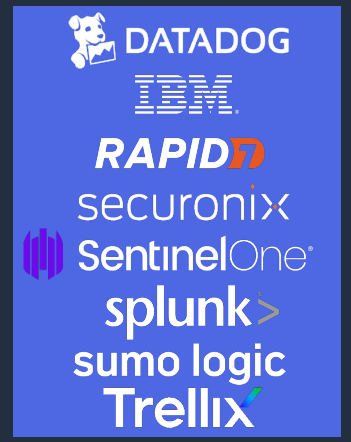
顧客管理のデータレイク

ツールによる分析



AWS 分析サービス

パートナー
セキュリティソリューション



分析プラットフォーム

aws

Amazon Security Lake パートナー

お客様ワークロードに対して幅広い観点での可視性を導入

大規模運用に対応可能な「セキュリティモニタリング基盤」の実現

クラウドセキュリティはAWSの最優先事項

AWSを活用する利点

- 優れた可視性と制御による安全な拡張
- 統合されたサービスでリスク対策を自動化し、リスクを低減
- 最高水準のプライバシーとデータセキュリティ
- セキュリティパートナーとのエコシステム
- 包括的なセキュリティとコンプライアンス管理

AWS のインフラストラクチャ – データセンター

環境レイヤー

地震や洪水などの環境的なリスクを踏まえた立地

境界防御レイヤー

防御壁、保安要員、入退館、監視カメラなど

インフラストラクチャレイヤー

建屋、各種機器、空調、消火設備、運用機能など

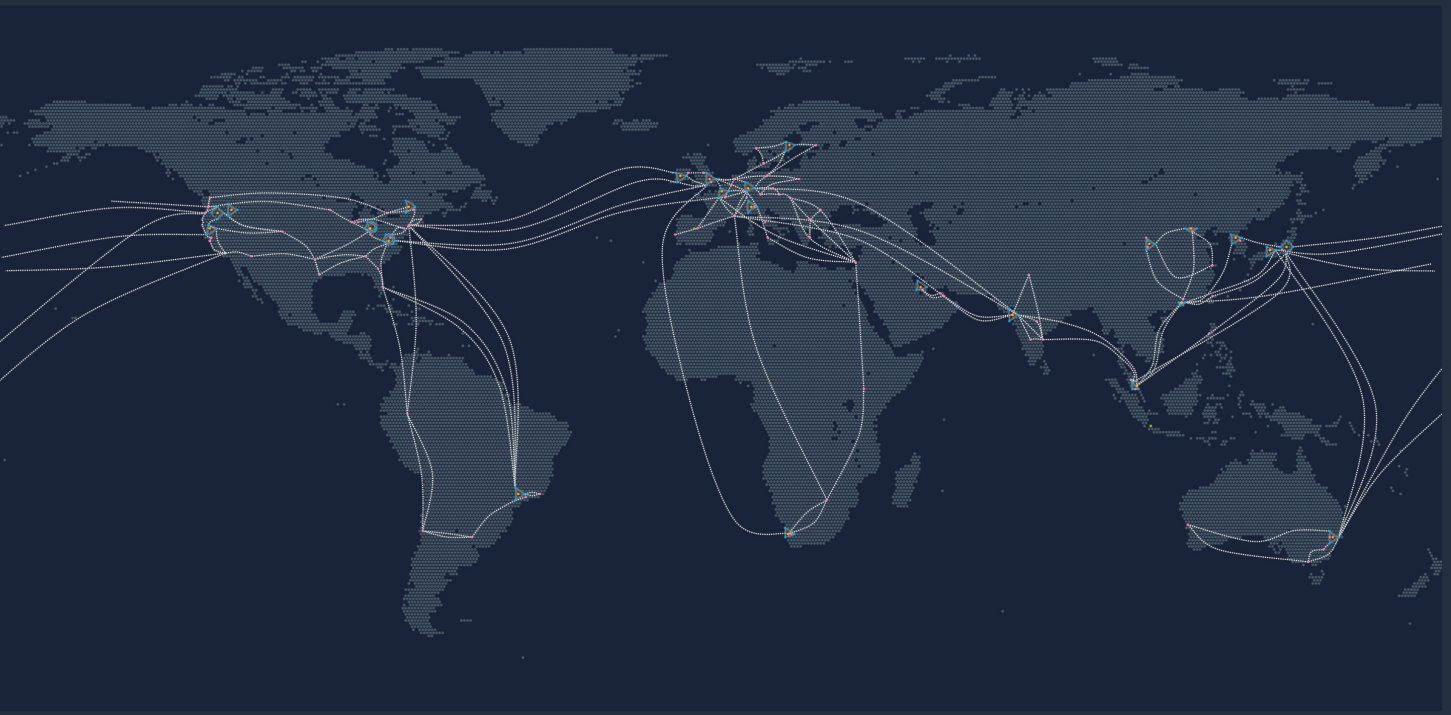
データレイヤー

特権の分離、お客様の分離、データの廃棄など

グローバルなセキュリティおよびコンプライアンスの考慮と独立した監査人による継続的な確認・審査

データは海外に移転されない

⇒所在地の選択やデータの移転は、お客様がコントロール
　お客様は、お客様自身のデータを国内に保持可能



お客様は、複数のリージョンでコンテンツを複製およびバックアップすることができます。

お客様のコンテンツがお客様が選択したリージョン外に AWS によって移動されることはありません。

https://aws.amazon.com/jp/compliance/data-privacy-faq/

データの取り扱い

データの管理権、所有権
については、
お客様にあります。

様式 3 別添 2

ISMAP クラウドサービス登録規則 3.4(2)に定める情報の提供について

2022 年 3 月 8 日

当社 Amazon Web Services, Inc. が申請したクラウドサービスについて、ISMAP クラウドサービス登録規則 3.4(2)に基づき、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用され、調達府省庁等が意図しないまま当該調達府省庁等の管理する情報にアクセスされ又は処理されるリスクについて、ISMAP 運営委員会及び当該省庁等がリスク評価を行うために必要な情報を下記の通り提供します。

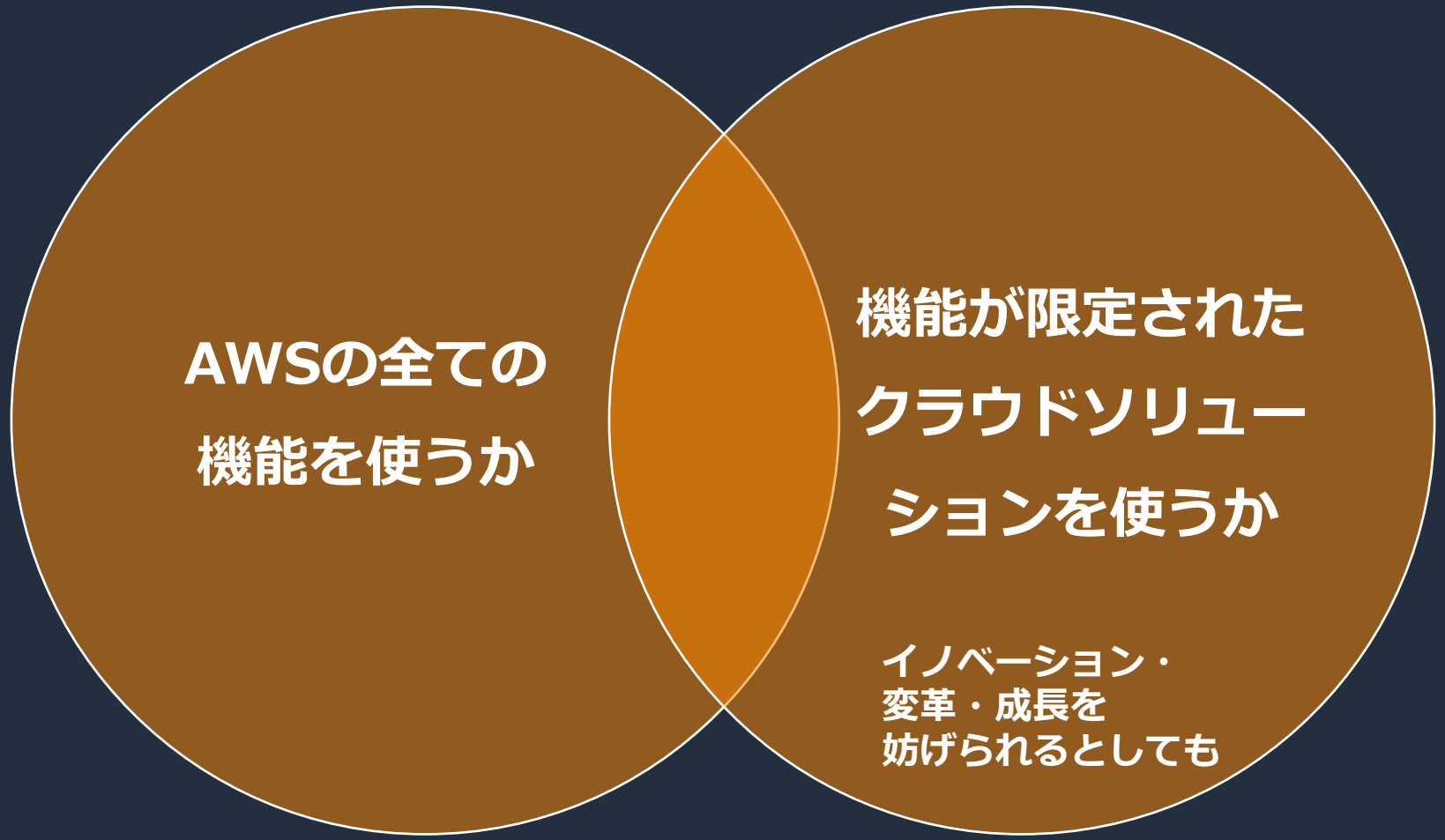
記

1　ISMAP クラウドサービス登録規則 3.4(2)に定める情報：
AWS のお客様は、適用されるコンプライアンスに関する法律および規制に準拠する責任があります。場合によっては、お客様のコンプライアンスをサポートするために、AWS から機能（セキュリティ機能など）、支援ドキュメント、法的な契約書（AWS データ処理契約や事業提携契約など）が提供されます。

お客様がプライバシーとデータセキュリティについて懸念されるのは当然のことです。このため、AWS ではコンテンツの所有権と管理権をお客様にお渡ししています。シンプルかつパワフルなツールによって、自分のコンテンツをどこに保存するかをお客様に決定していただき、転送中のコンテンツと保管中のコンテンツを保護し、お客様のユーザーの AWS のサービスとリソースに対するアクセスを管理できるようにしています。また、お客様のコンテンツに対する不正アクセスや開示を防止するよう設計された、洗練された信頼性の高い技術的および物理的な管理を実践しています。

以上

デジタル統制に関するお客様の声



AWSのデジタル統制に関するお客様との約束

クラウドの可能性を最大限に引き出すためには、お客様が自らデータを管理することが不可欠

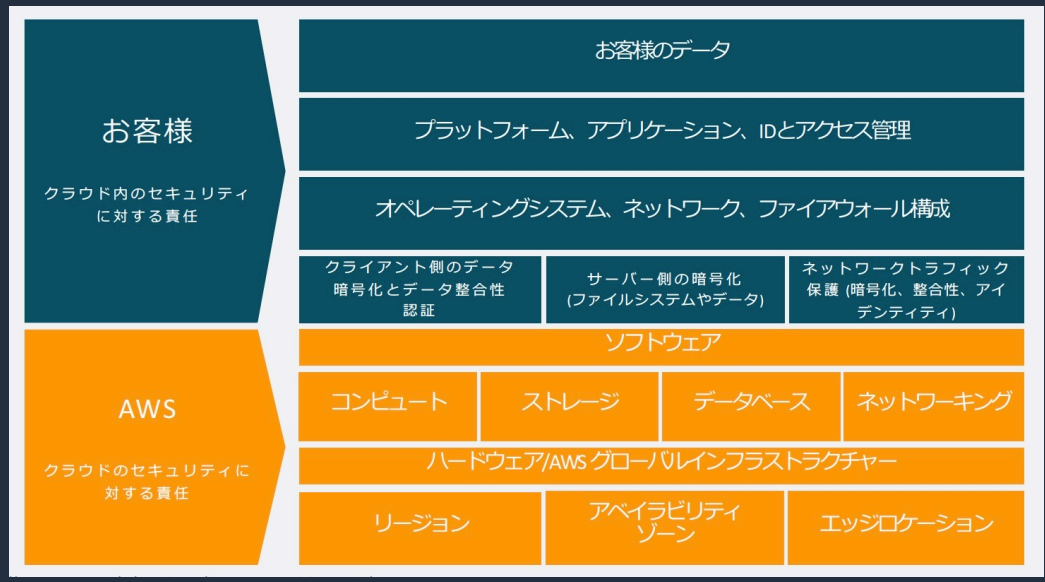
1.企画・設計段階からの統制（sovereign-by-design）

1.データの保管場所の管理
2.検証可能なデータアクセスの管理
3.あらゆる場所ですべてを暗号化する機能
4.クラウドの耐障害性

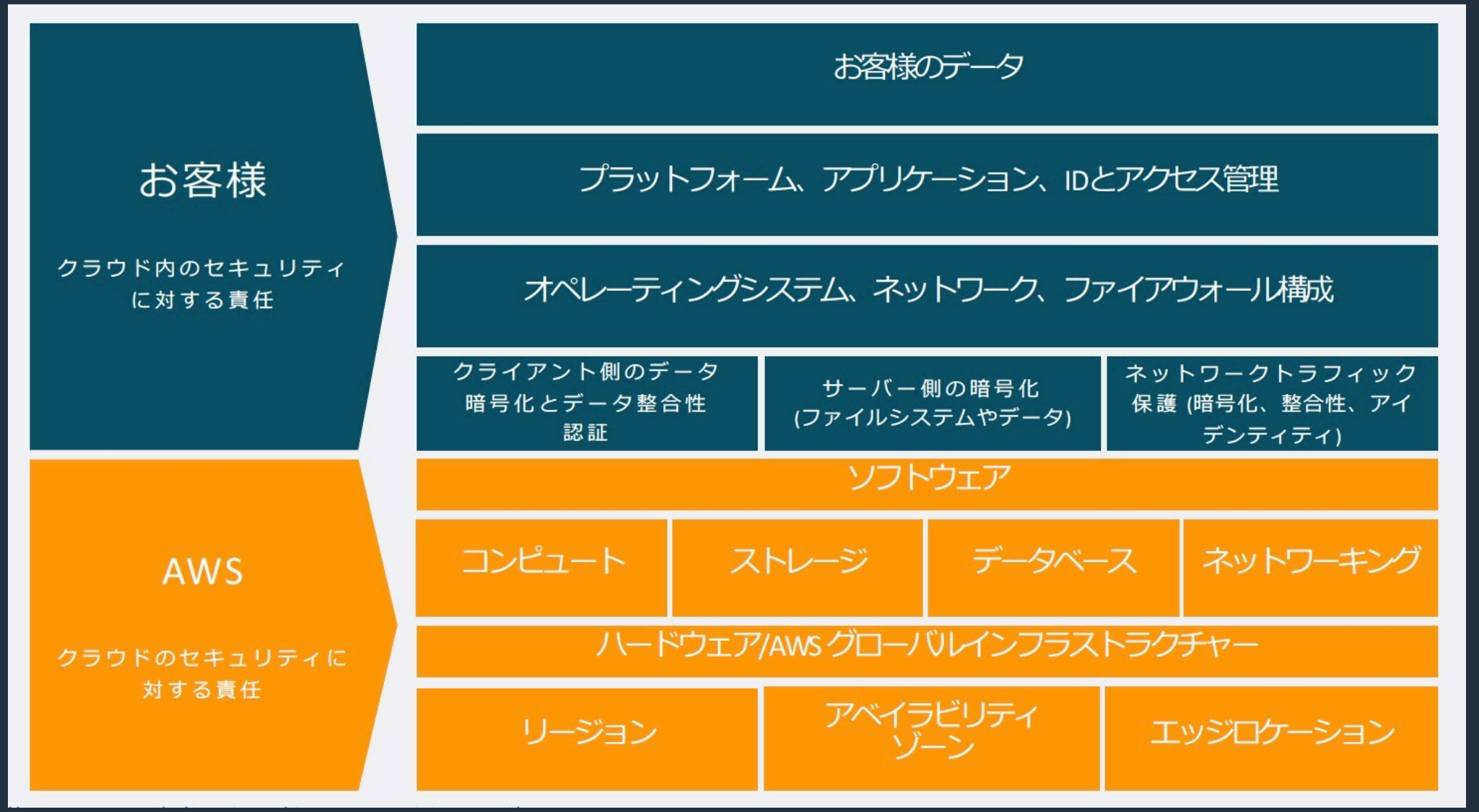
2.透明性と保証による信頼の獲得

3.チームとしての変化への対応

https://aws.amazon.com/jp/blogs/security/aws-digital-sovereignty-pledge-control-without-compromise/



AWS 責任共有モデル



1.企画・設計段階からの統制 (sovereign-by-design)

技術による
対応

データ暗号化

AWS CloudHSMやAWS Key Management Serviceなどのサービスにより、暗号鍵を安全に生成。お客様にて暗号鍵を管理することができます。

AWS Identity and Access Management (IAM) と AWS Control Tower

IAMにより、お客様はAWSのサービスやリソースへのアクセスを安全に管理することができ、特定のリージョンのサービスへのアクセスを制限することもできます。Control Towerのデータレジデンシーガードレールは、お客様のデータが特定のAWSリージョンまたはリージョン外で保存または処理されないようにします。

モニタリングとログ記録

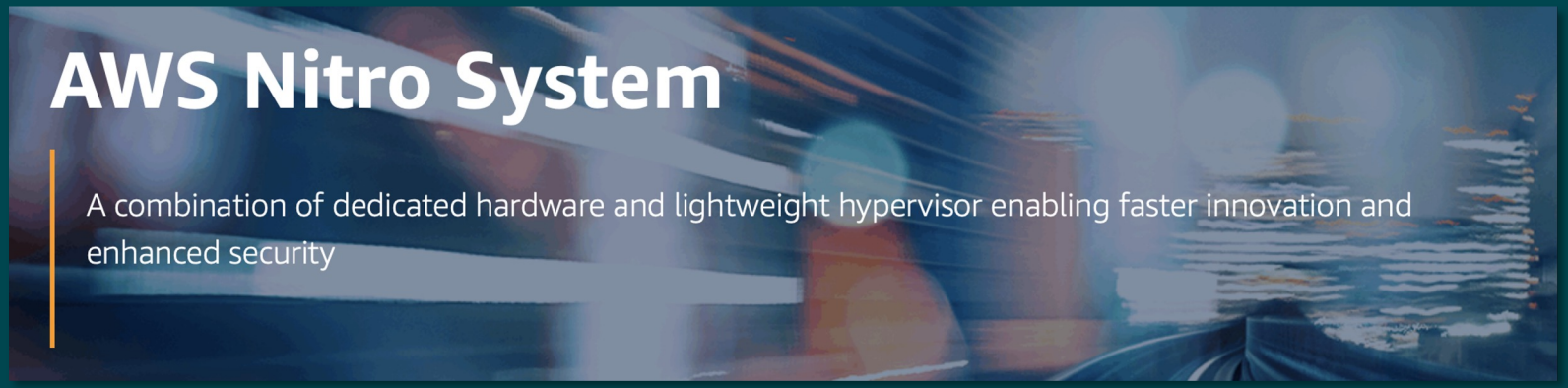
AWS CloudTrailやAmazon CloudWatchなどのサービスは、アクセスコントロールのためのモニタリングとログ記録の機能を提供します。

Amazon Macie

Amazon Macieは、パターンマッチングと機械学習により、暗号化されていない情報を含む個人を識別可能な情報を検出し、S3バケット内の機密データを検知して保護します。

1.企画・設計段階からの統制 (sovereign-by-design)

コンフィデンシャル・
コンピューティング



AWS Nitro Systemは、最新のAmazon Elastic Compute Cloud（Amazon EC2）インスタンスすべての基盤プラットフォームであり、お客様のアプリケーションにさらなるコントロールを提供します。

AWS Nitro Systemは、主に3つの保護を提供します。

1. クラウドサービス提供事業者 (AWS) からの保護
2. AWSのシステムソフトウェアからの保護
3. お客様自身のオペレータやソフトウェアからの保護

1.企画・設計段階からの統制（sovereign-by-design）

データの統制の実現

- 暗号技術の採用と、暗号化鍵をお客様で管理することで、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討済みの方法を実装可能。
  - CRYPTREC; Cryptography Research and Evaluation Committees 参照：https://www.cryptrec.go.jp/about.html
- お客様はOSを含むソフトウェアの領域において、お客様が統制可能。ベアメタルインスタンスを活用すると、Intel VT-x などのハードウェアの機能セットへのアクセスが必要なワークロード（Hypervisorのソフトウェア）をお客様のみが統制可能。
- データの統制に関しては、上記の施策と、アクセス管理、ログ記録/確認をお客様による実施、第三者による監査レポートの確認で、対応可能。データの統制はお客様にて実施可能。

https://aws.amazon.com/jp/compliance/programs/

2. 透明性と保証による信頼の獲得

第三者機関による認証と認定

ISO 27001
セキュリティ管理統制

ISO 27017
クラウド固有の統制

ISO 27701
プライバシー情報管理

ISO 27018
個人データ保護

PCI DSS レベル 1
ペイメントカード基準

SOC 1
監査統制報告書

SOC 2
セキュリティ、可用性、機密性レポート

SOC 3
全般統制報告書

アジアパシフィック

FinTech
リファレンスアーキテクチャ日本版

FISC
日本の金融業界情報システムセンター

IRAP
オーストラリアのセキュリティ基準

K-ISMS
韓国の情報セキュリティ

ISMAP
日本のパブリッククラウドサービスのセキュリティを評価する政府プログラム

医療情報ガイドライン
日本のガイドライン

MTCS ティア 3
シンガポールの多層クラウドセキュリティ基準

NISC
日本の内閣サイバーセキュリティセンター

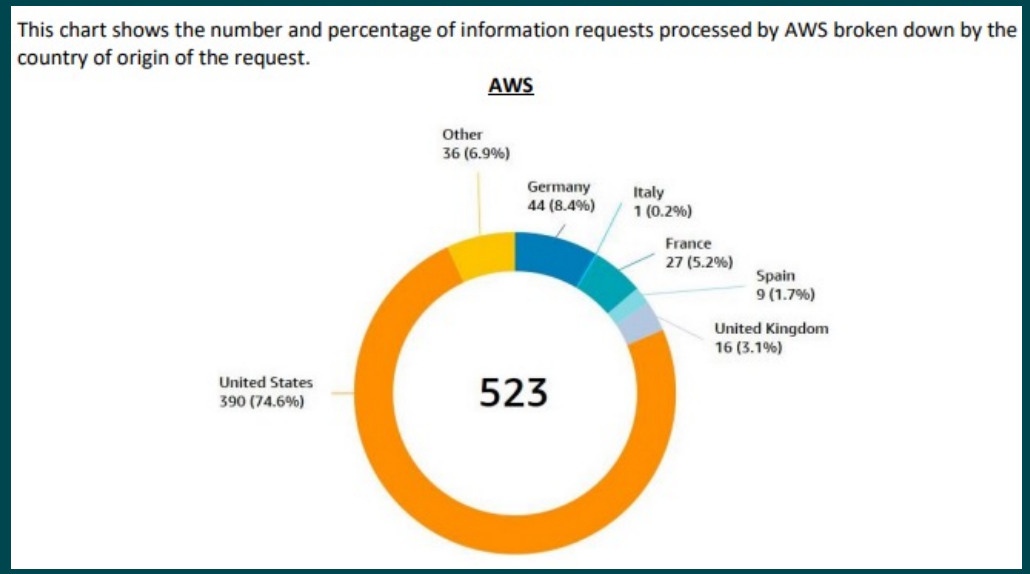
OSPAR
シンガポールのアウトソーシングに関するガイドライン

https://aws.amazon.com/jp/compliance/programs/

2. 透明性と保証による信頼の獲得

手続による対応

AmazonとAWSは、アマゾンに要求された情報の種類と数についての情報を提供します。
法的に有効で拘束力のある命令を遵守するために必要な場合を除き、アマゾンは当然のことながら、過度に広範な、またはその他の不適切な要求には反対します。



https://d1.awsstatic.com/certifications/Information_Request_Report_December_2020.pdf

3.チームとしての変化への対応

パートナーとの連携

- 規制、テクノロジー、リスクが変化する世界において、お客様によるデータの保護を支援するためには、チームワークが必要です。私たちは、お客様だけで対応することを期待するようなことは決してありません。
- AWS の信頼できるパートナーが、お客様にソリューションを提供するうえで顕著な役割を果たします。
- 例えば、ドイツでは、T-Systems (ドイツテレコムグループ) が AWS のマネージドサービスとしてデータ保護を提供しています。同社は、データ保護・管理が適切に設定されていることを確認するためのガイダンスを提供し、暗号化キーの設定と管理に関するサービスと専門知識を提供して、顧客が AWS クラウドでデジタル統制要件に対応できるよう支援しています。
- 私たちは、デジタル統制要件への対応を支援するために、お客様が信頼するローカルパートナーとの連携を強化しています。

クラウドセキュリティはAWSの最優先事項

AWSを活用する利点

- 優れた可視性と制御による安全な拡張
- 統合されたサービスでリスク対策を自動化し、リスクを低減
- 最高水準のプライバシーとデータセキュリティ
- セキュリティパートナーとのエコシステム
- 包括的なセキュリティとコンプライアンス管理

セキュリティ、アイデンティティ、コンプライアンスのための包括的なサービスと機能を提供

アイデンティティ
&アクセス管理

発見的統制

インフラストラクチャ
防御

データ保護

インシデント
レスポンス

コンプライアンス

セキュリティ状態の一元化と逸脱チェック、可視性を高め継続的に改善していく - AWS Security Hub

セキュリティ状態の可視化

Amazon GuardDuty

Amazon Inspector

Amazon Macie

Compliance Check

aws partner network

・・・

データ集約

セキュリティ状態の一元化で継続的な改善サイクルの運用基盤となる

AWS Security Hub 管理コンソール画面

対応実施（改善）

運用手順に則って対応

自動的に修復

予防的統制に取り込み

・・・

AWS Generative AI(生成系AI)の最新情報については、下記のサイトを参照願います。

https://aws.amazon.com/jp/generative-ai/

AWS のセキュリティ、ID、コンプライアンスソリューション

IDとアクセス管理

AWS Identity and Access Management (IAM)

AWS IAM Identity Center (successor to AWS SSO)

AWS Organizations

AWS Directory Service

Amazon Cognito

AWS Resource Access Manager

発見的統制

AWS Security Hub

Amazon GuardDuty

Amazon Inspector

Amazon CloudWatch

AWS Config

AWS CloudTrail

VPC Flow Logs

AWS IoT Device Defender

インフラストラクチャ保護

AWS Firewall Manager

AWS Network Firewall

AWS Shield

AWS WAF

Amazon VPC

AWS PrivateLink

AWS Systems Manager

データ保護

Amazon Macie

AWS Key Management Service (KMS)

AWS CloudHSM

AWS Certificate Manager

AWS Secrets Manager

AWS VPN

Server-Side Encryption

インシデント対応

Amazon Detective

Amazon EventBridge

AWS Backup

AWS Security Hub

AWS Elastic Disaster Recovery

コンプライアンス

AWS Artifact

AWS Audit Manager

まとめ

今日お話ししたこと
クラウドセキュリティはAWSの最優先事項

AWSを活用する利点

- 優れた可視性と制御による安全な拡張
- 統合されたサービスでリスク対策を自動化し、リスクを低減
- 最高水準のプライバシーとデータセキュリティ
- セキュリティパートナーとのエコシステム
- 包括的なセキュリティとコンプライアンス管理

AWS 環境でセキュリティに取り組むための道標

AWS Well-Architected Framework

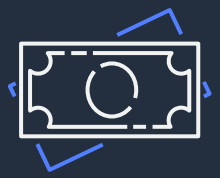
AWS のソリューションアーキテクト (SA)、パートナー様、
お客様の **10 年以上にわたる経験** から作り上げた
ベストプラクティス

運用上の
優秀性

セキュリティ

信頼性

パフォーマンス
効率

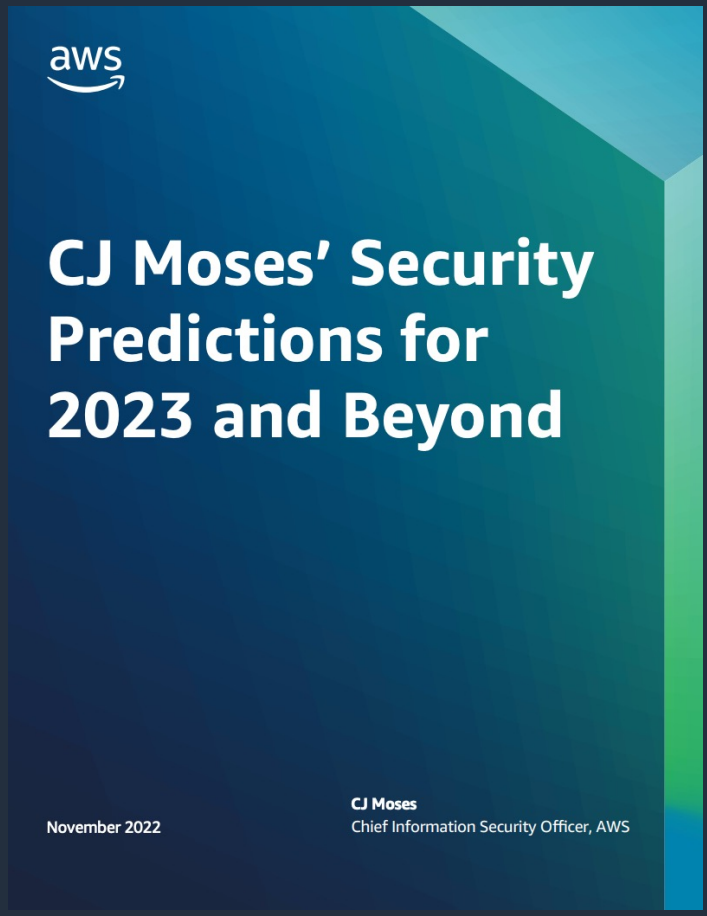


コスト
最適化

持続可能性

AWS, Security Predictions 2023, CJ Moses

1. セキュリティは、組織が行うすべてのことにおいて「**不可欠**」になる
2. **ダイバーシティの考慮**は、セキュリティ人材のギャップに継続的に対処できる
3. **AI/ML による自動化**で、より強力なセキュリティが実現
4. **データ保護への投資**が促進される
5. **多要素認証のより高度な形式**が普及する
6. **量子コンピューティング**がセキュリティに効果を発揮する



https://aws.amazon.com/jp/blogs/security/new-ebook-cj-moses-security-predictions-in-2023-and-beyond/

Thank you!