



# INNOVATE

ONLINE CONFERENCE

# 金融機関における AWS 活用事例 とアーキテクチャ解説

有岡 紘佑

技術本部 金融ソリューション部 ソリューション アーキテクト

TWITTERハッシュタグ #AWSInnovate

# Agenda

金融機関における AWS 活用

AWS におけるセキュリティとシステム構築手法

主要な活用例とアーキテクチャ



# AWS Summit Tokyo 2019 金融セッションレポート

The graphic features a dark background with a grid pattern and orange line charts. At the top, there are logos for '日経 XTECH Special' and '日経 XTECH Special 一覧'. Below these, a purple banner contains the text 'AWS SUMMIT TOKYO/OSAKA 金融トラックセッションレポート'. The main title is '金融業界が乗り越えるべき“デジタルの壁”' (The 'Digital Wall' the Financial Industry Must Overcome). Below this, the subtitle is '進む金融業界での AWS 活用' (AWS Utilization in the Advancing Financial Industry). The main headline is '7つの先進事例' (7 Advanced Cases). At the bottom, a paragraph of text discusses the challenges of cloud adoption in the financial industry and mentions that the report explores 7 advanced cases.

日経 XTECH Special

日経 XTECH Special 一覧

AWS SUMMIT TOKYO/OSAKA 金融トラックセッションレポート

金融業界が乗り越えるべき“デジタルの壁”

進む金融業界での AWS 活用

**7つの先進事例**

変化の激しい金融業界では、いまや大手金融機関までもがクラウド化へ舵を切っている。しかし、その宿命として安全性には厳しい評価も必要になる。例えば、金融業界で基幹系にクラウドを活用するには、どのような乗り越えるべき課題があるのだろうか？ セキュリティ評価の方法論や事業創出のコツとは？ 先進企業の7事例からクラウド活用のポイントを探る。

<https://special.nikkeibp.co.jp/atcl/NXT/19/aws0828/>

# 金融機関における AWS 活用

# 国内外の金融機関における AWS の活用

2018年の「**Forbes FinTech 50**」  
の全ての企業がAWSを利用

Fin-Tech 企業

IT トランス  
フォーメーション

既存金融機関様

デジタルトランス  
フォーメーション

既存のアプリケーションを  
変更せず移行でコストを削減

Fin-Tech 企業のようなスピードで  
サービスを開発し世の中へ送り出す

1. 周辺系(ノン・コア)
2. ダイレクト・チャネル
3. 情報系・データ分析
4. 基幹系

- マネージドサービス活用
- コンテナ
- マイクロサービス

# 国内外の金融機関で AWS が利用される理由



## Time

必要な時に必要なコンピュート  
やストレージを調達



## Low Cost

使った分だけの課金  
オンプレミスに対してTCO削減が可能



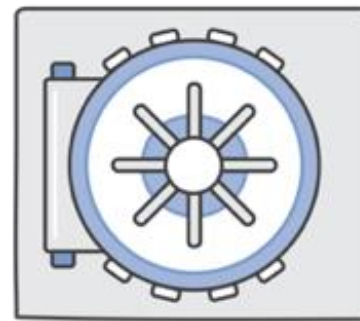
## Elastic

処理量に合わせて  
柔軟にリソースを調達



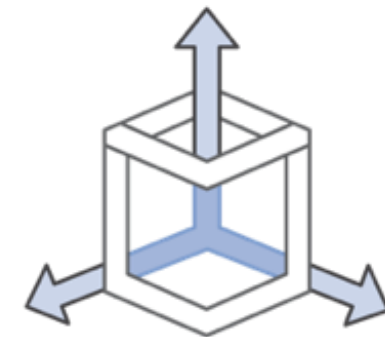
## Globally Accessible

日本で開発したシステムをNY、ロンドン、シンガポールなどで利用



## Secure

データ暗号化などセキュリティ対策の機能とコンプライアンス



## Scalable

大規模なリソースを利用可能

# AWS におけるセキュリティ とシステム構築手法



# 責任共有モデル



# マネージドサービスの活用

付加価値につながらない作業やプロセスを AWS に任せることでビジネスに集中できる

アプリケーション作成	アプリケーション作成	アプリケーション作成	アプリケーション作成
スケールアウト設計	スケールアウト設計	スケールアウト設計	スケールアウト設計
定形運用設計	定形運用設計	定形運用設計	定形運用設計
ミドルウェアパッチ	ミドルウェアパッチ	ミドルウェアパッチ	ミドルウェアパッチ
ミドルウェア導入	ミドルウェア導入	ミドルウェア導入	ミドルウェア導入
OSパッチ	OSパッチ	OSパッチ	OSパッチ
OS導入	OS導入	OS導入	OS導入
HWメンテナンス	HWメンテナンス	HWメンテナンス	HWメンテナンス
ラッキング	ラッキング	ラッキング	ラッキング
電源・ネットワーク	電源・ネットワーク	電源・ネットワーク	電源・ネットワーク
オンプレミス	独自構築 on EC2	マネージドサービス	サーバーレス

お客様が担当

AWSが担当

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.



# コンプライアンス

Compliance Center – <https://atlas.aws>

## Global

 **CSA**  
cloud security alliance®  
CSA  
Cloud Security Alliance Controls

 **ISO 9001**  
Global Quality Standard

 **ISO 27001**  
Security Management Controls

 **ISO 27017**  
Cloud Specific Controls

 **ISO 27018**  
Personal Data Protection

 **PCI DSS Level 1**  
Payment Card Standards

 **SOC 1**  
Audit Controls Report

 **SOC 2**  
Security, Availability, & Confidentiality Report

 **SOC 3**  
General Controls Report

## United States

 **CJIS**  
Criminal Justice Information Services

 **DoD SRG**  
DoD Data Processing

 **FedRAMP**  
Government Data Standards

 **FERPA**  
Educational Privacy Act

 **FFIEC**  
Financial Institutions Regulation

 **FIPS**  
Government Security Standards

 **FISMA**  
Federal Information Security Management

 **GxP**  
Quality Guidelines and Regulations

 **HIPAA**  
Protected Health Information

 **ITAR**  
International Arms Regulations

 **MPAA**  
Protected Media Content

 **NIST**  
National Institute of Standards and Technology

 **SEC Rule 17a-4(f)**  
Financial Data Standards

 **VPAT/Section 508**  
Accountability Standards


## Asia Pacific

**FISC [Japan]**  
Financial Industry Information Systems

 **IRAP [Australia]**  
Australian Security Standards

 **K-ISMS [Korea]**  
Korean Information Security

 **iDA**  
SINGAPORE  
MTCS Tier 3 [Singapore]  
Multi-Tier Cloud Security Standard

 **My Number Act [Japan]**  
Personal Information Protection

## Europe

 **C5 [Germany]**  
Operational Security Attestation

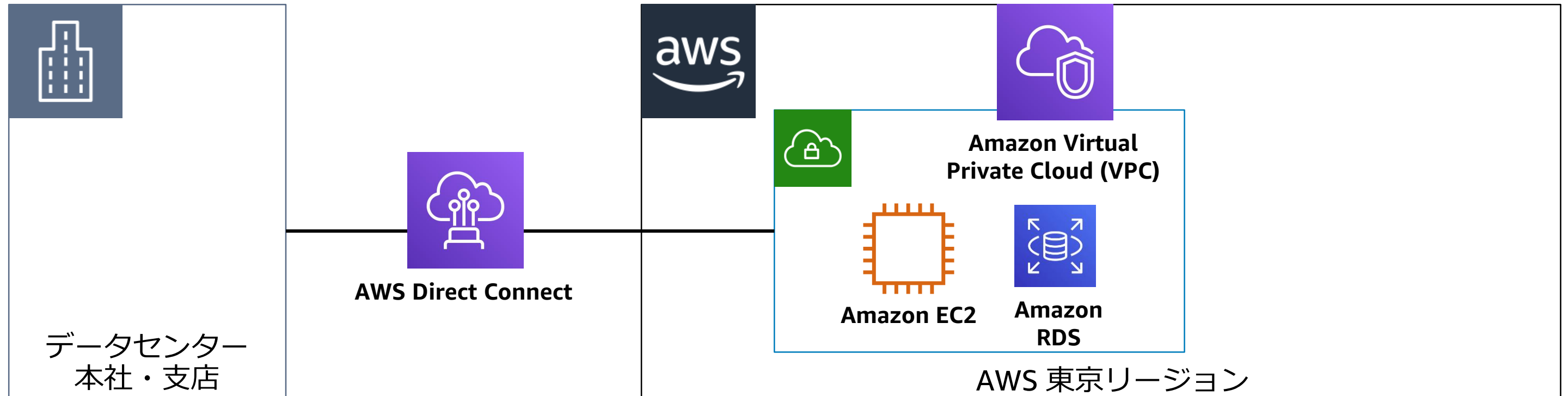
 **Cyber Essentials Plus [UK]**  
Cyber Threat Protection

 **G-Cloud [UK]**  
UK Government Standards

 **TUV AUSTRIA**  
IT-Grundschutz [Germany]  
Baseline Protection Methodology

# 1.VPC 内のサービス利用

専用線接続サービスを利用して閉域網で、お客様の専用ネットワーク区画であるVPCへアクセス

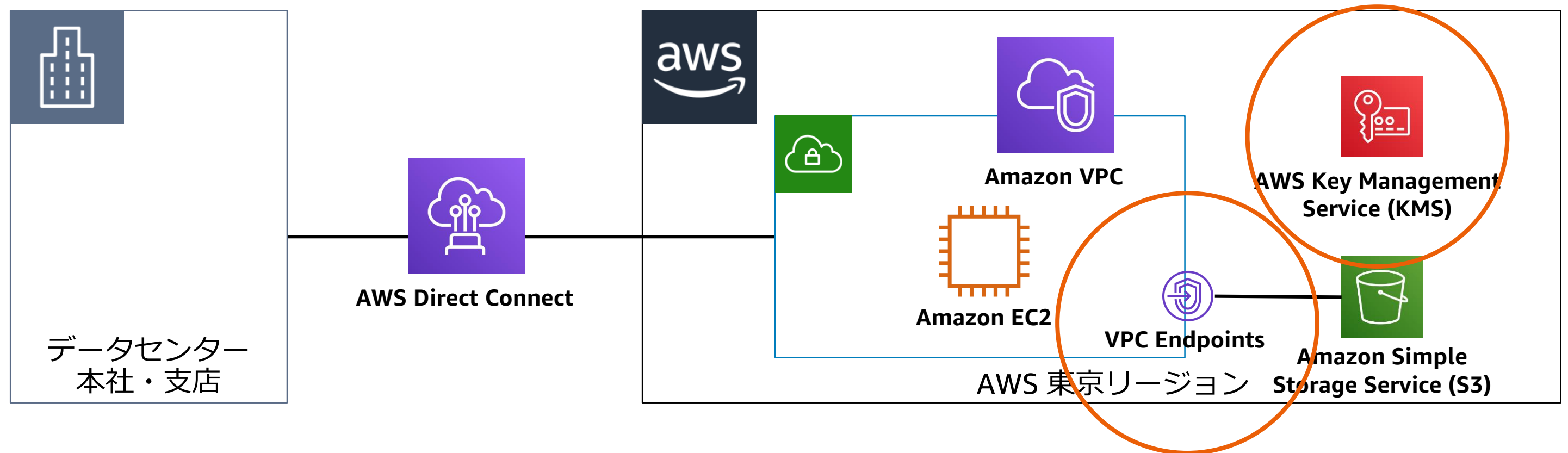


- AWS の環境をオンプレミスの延長として利用する
- VPC内で稼働するサービス（EC2, RDSなど）が選択の基本となる



## 2.VPC 外のサービス利用

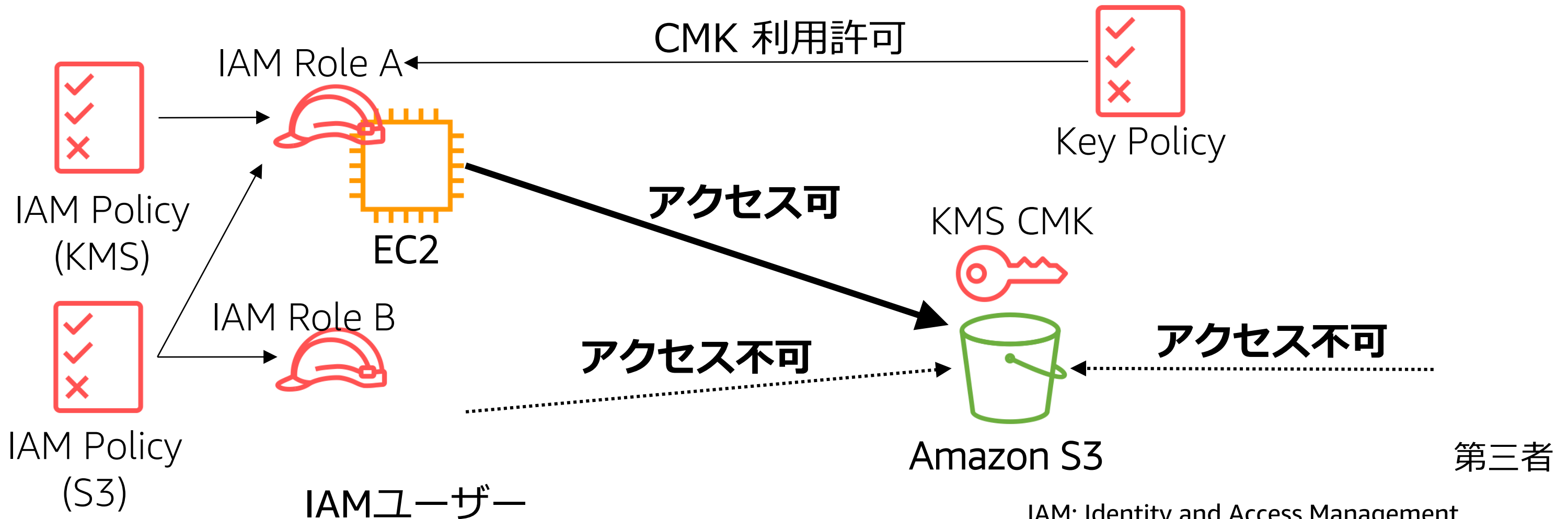
インターネットを経由せずにVPC外のサービスを利用、暗号化の鍵はお客様が管理



- AWS の環境をオンプレミスの延長として利用する
- VPC外で稼働するサービスを安全に組み合わせる

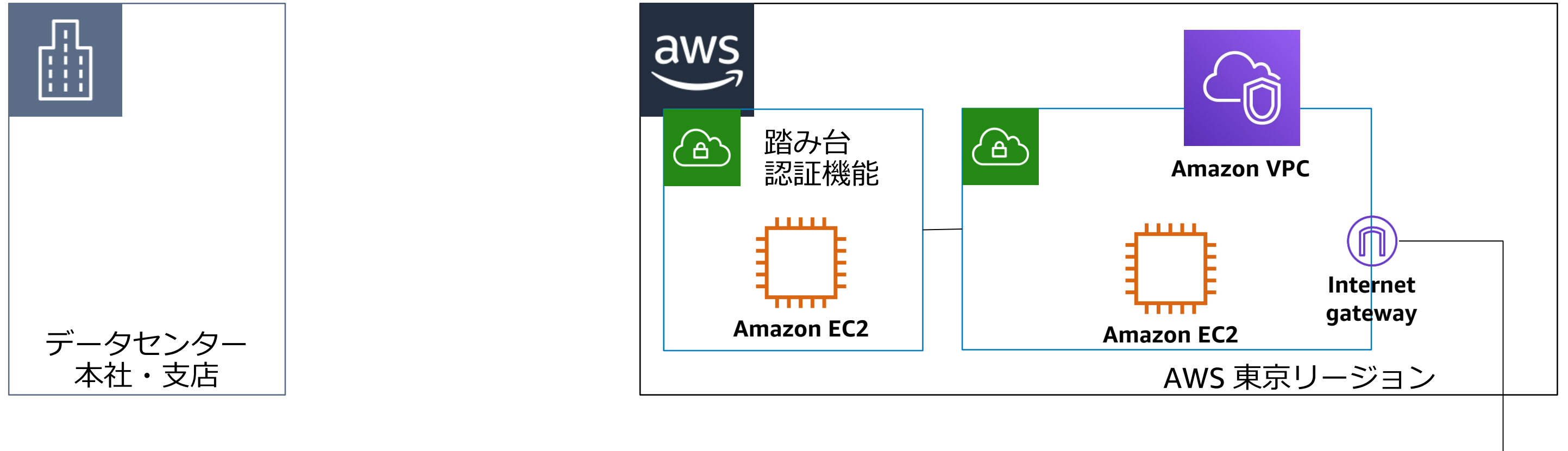
# KMS によるデータ保護

- S3 バケットがパブリック公開されてもアクセス不可
- S3 だけのアクセス権があってもアクセス不可



# 3. デジタル・サンドボックス

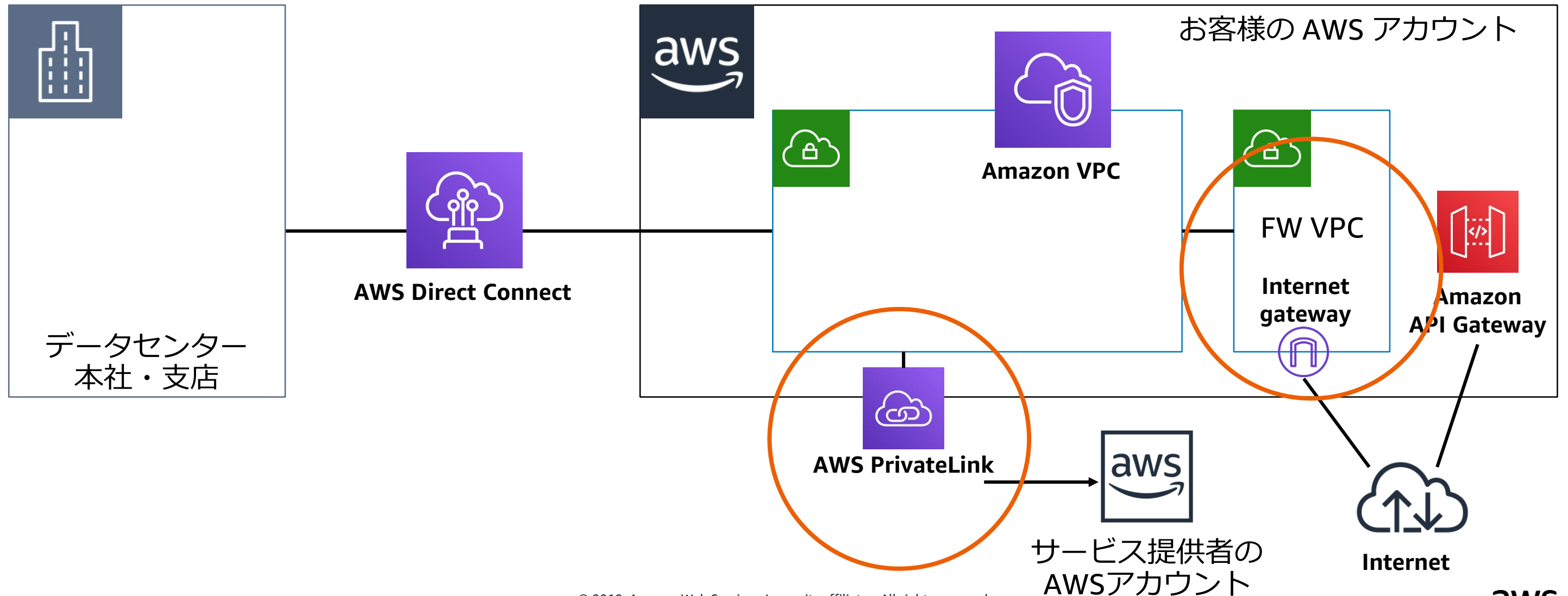
開発やプロトタイピング、外部組織との共同作業環境などに利用



- AWS の環境をオンプレミスと接続せずに利用する
- インターネット接続、PrivateLink経由での外部サービスとの接続など

# 4.インターネット接続

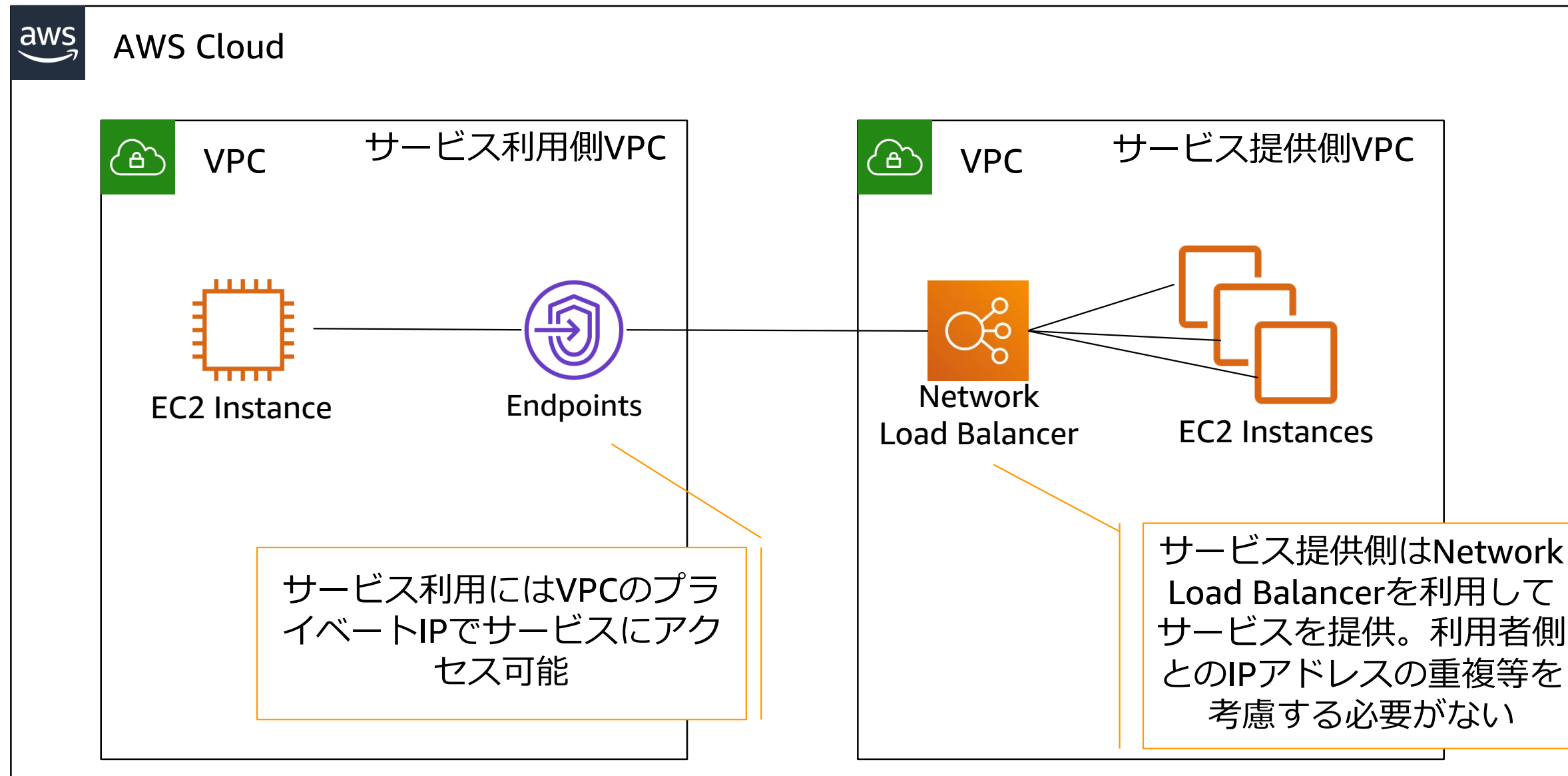
AWS上で他の金融機関やユーザー企業と安全に閉域網で接続可能。ファイアウォールサービスVPCを構築、またはAPI Gatewayなどのサービスでインターネットと接続





# 参考) AWS PrivateLink

他のアカウントを含むVPC間で、プライベートIPでサービスを公開可能



# マルチアカウント戦略と Landing Zone

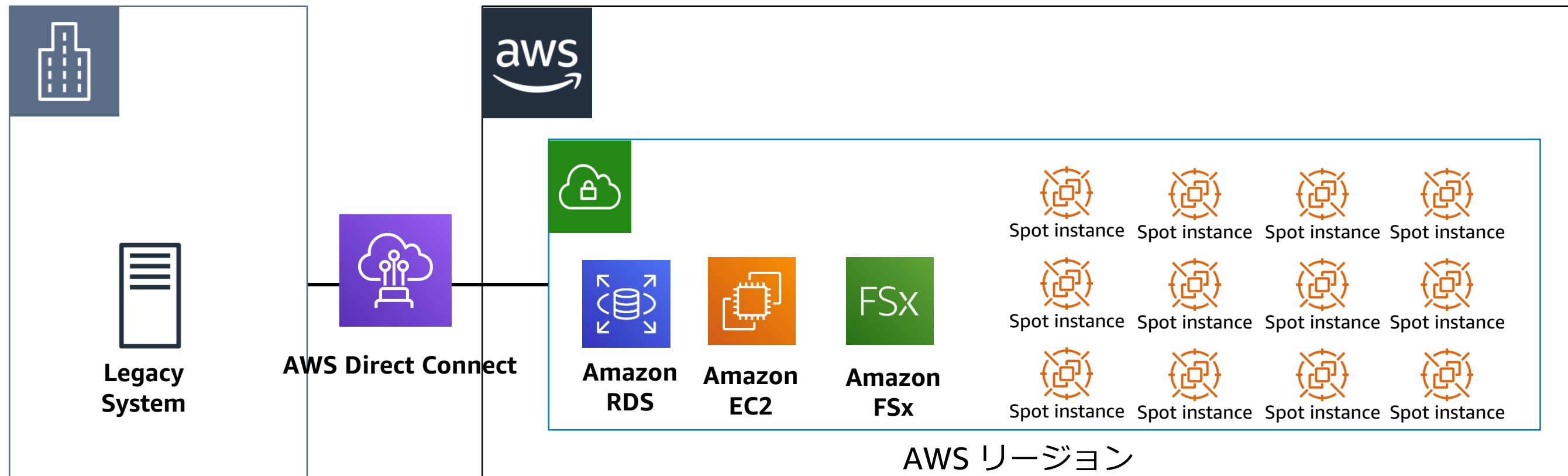
- システム毎にAWSアカウントを構成（**マルチアカウント**）し、新規システム構築や既存システムの移行を行うことが増えています。
- 各アカウントのシステムは個別に構築するのではなく、共通基盤上に構築されます。共通基盤は、通信経路をクローズドにしたり、サービスに対するアクセス権限の制御やデータ保護、監査機能などを共通的に、企業のベースラインポリシーとして実装します。
- 共通基盤は**セキュリティのガードレール**になり、この範囲であれば業務アプリケーションを安全に使えます。
- マルチアカウント戦略を支援する各種サービスとソリューション群：**AWS Organizations, AWS Control Tower, AWS Landing Zone Solution**

# 主要な活用例とアーキテクチャ

# リスク計算

- FRTB
- CVA

- ソルベンシーII

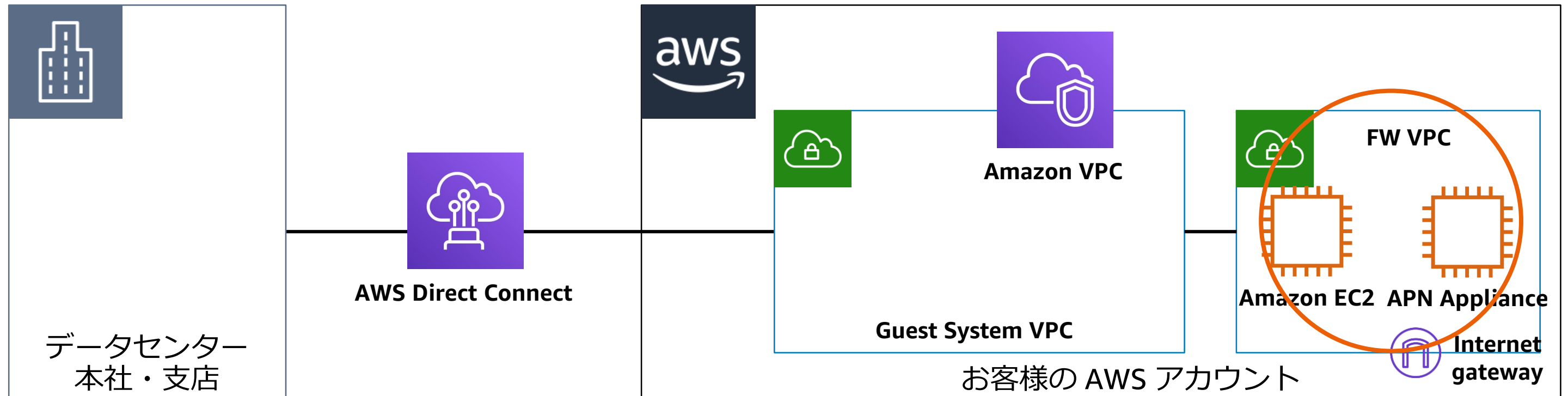


- 一時的に大量の計算リソースを必要とするワークロードはクラウドに最適
- 稼働コストとリソース調達のしやすさから海外リージョンのスポットインスタンスを活用する場合も

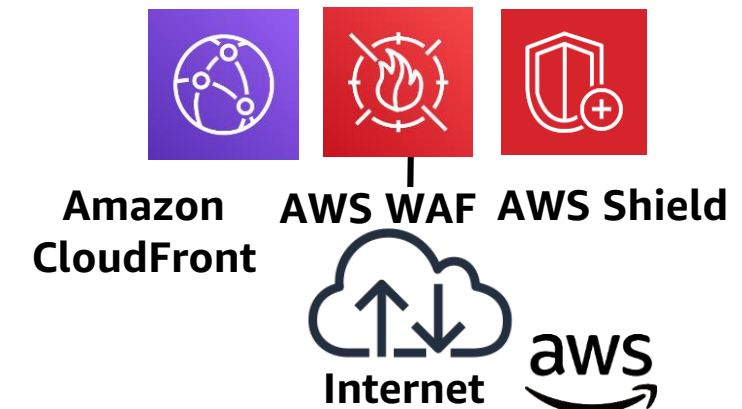


# 外部ネットワーク接続

- ・ オンプレミスDMZ機能のリプレイ + アルファ
- ・ インターネットに面するフロントシステムを AWS 上に移行

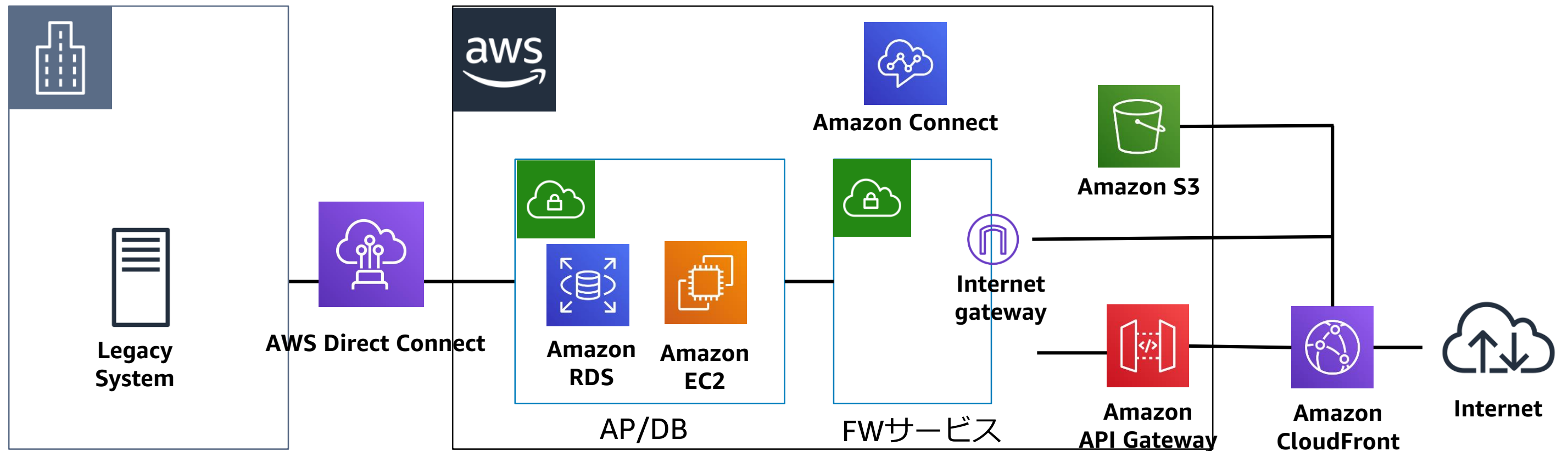


- ・ インバウンド/アウトバウンド プロキシサービス
- ・ APN パートナーソリューション (次世代FW, IDS)
- ・ CDNとDDoS防御 (Amazon CloudFront, AWS Shield, AWS WAF)



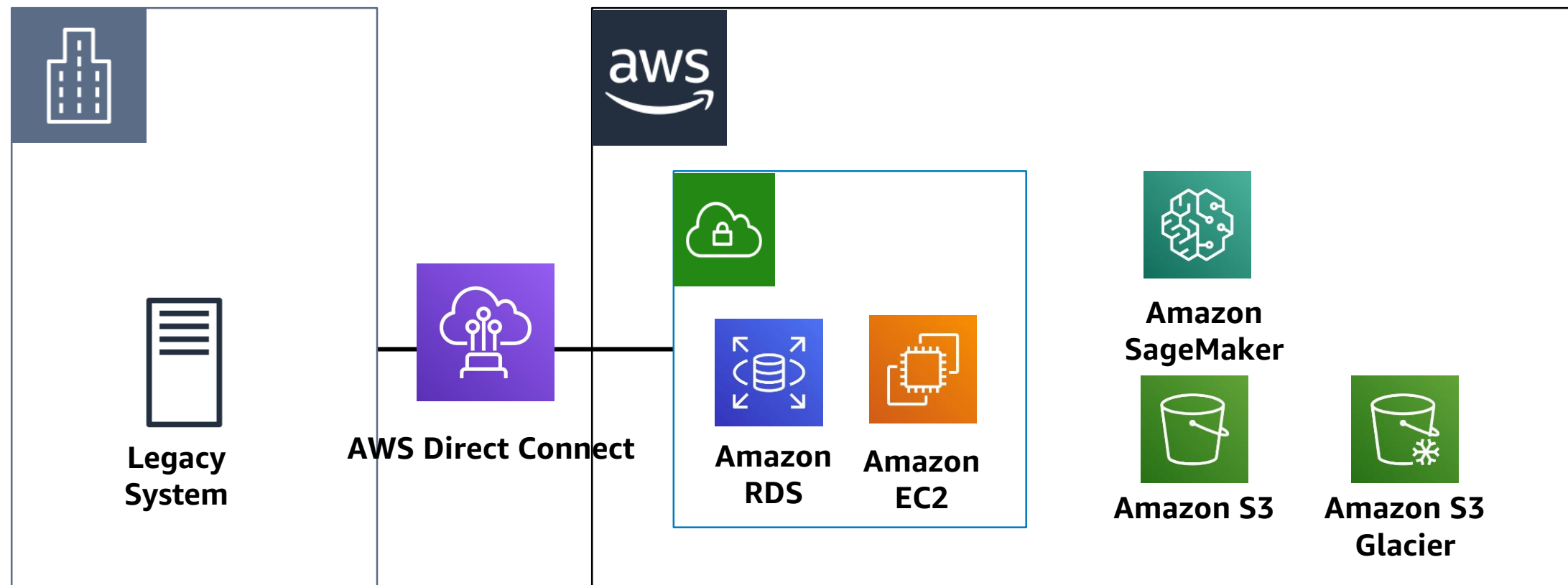
# ダイレクト・チャネル

- インターネットバンキングやインターネットトレーディングなど
- API
- コンタクトセンター
- 外部向けWebサイト



# 事務集中・後方業務の効率化

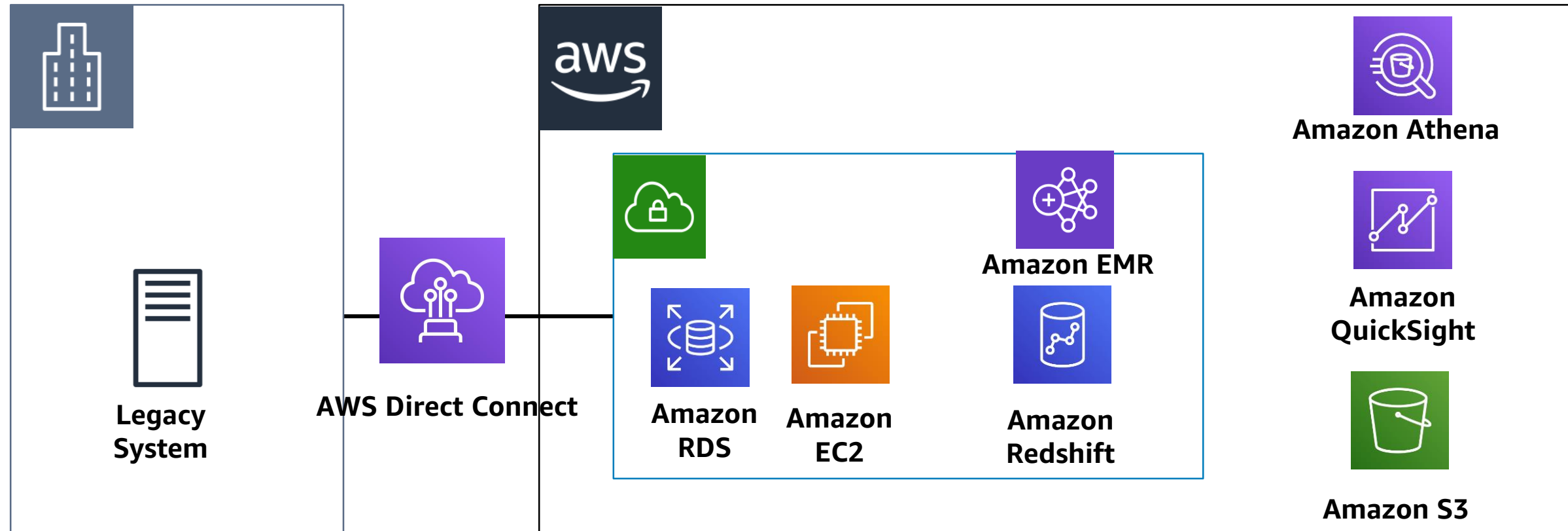
- RPA
- 機械学習を活用した省力化
- OCRデータの処理
- データの長期保管



# 情報系・データ分析

- DWH
- データレイク

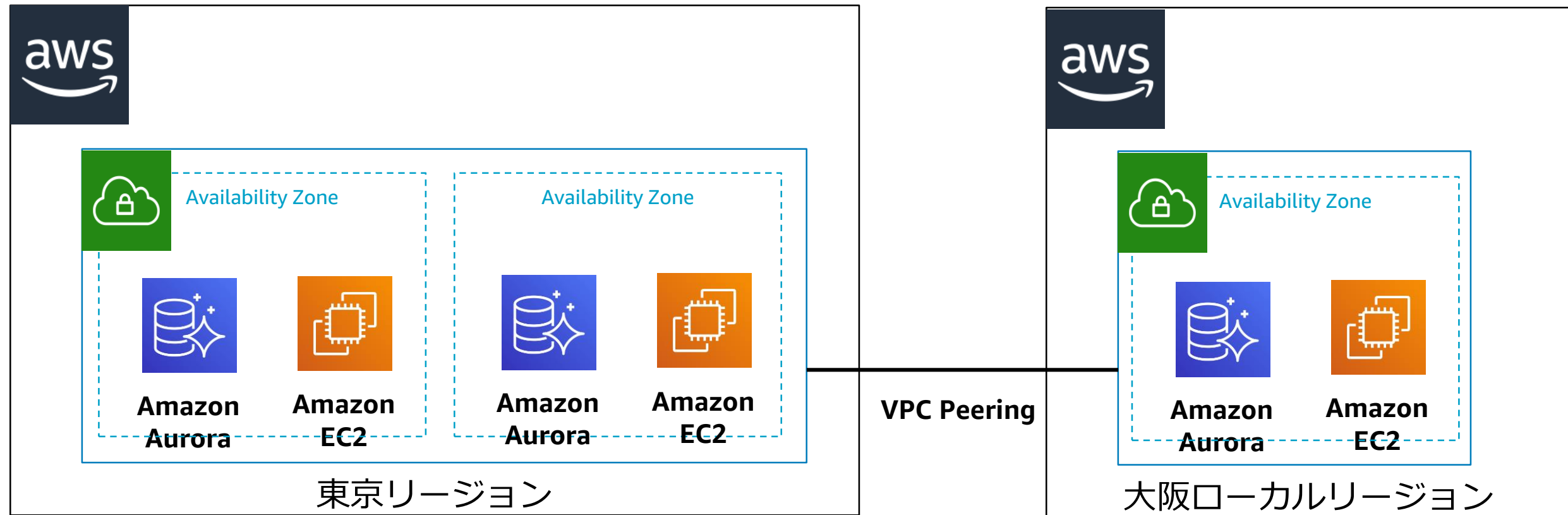
- CRM
- BI





# ミッションクリティカルなシステム

- 勘定系
- 契約管理



まとめ

# 金融機関における AWS の活用例

- 日本及び世界の金融機関でAWSの利用が広がっています。銀行、証券、生損保、カード、リース、Fintech企業などすべてのサブインダストリーでAWSは利用されています。
- 金融機関のお客様におけるAWS活用領域として、既存ITのトランスフォーメーションと、新しいサービスを展開するためのデジタルトランスフォーメーションがあり、AWS上での企業間連携も始まっています。
- 利用の前提となるセキュリティの考え方があり、VPCを基本に、システムへのアクセスやデータを保護するための仕組みを適切に利用することで、システムを強固に保護することが可能です。

# Thank you!

有岡 紘佑



Event info - <https://amzn.to/JPEvents>

Webinar - <https://amzn.to/JPWebinar>

Archive - <https://amzn.to/JPArchive>