AWSが考えるハイブリッドクラウド

～オンプレからのスムーズな移行の選択肢～

アマゾンウェブサービスジャパン
パブリックセクター　豊原啓治

2018/3/9

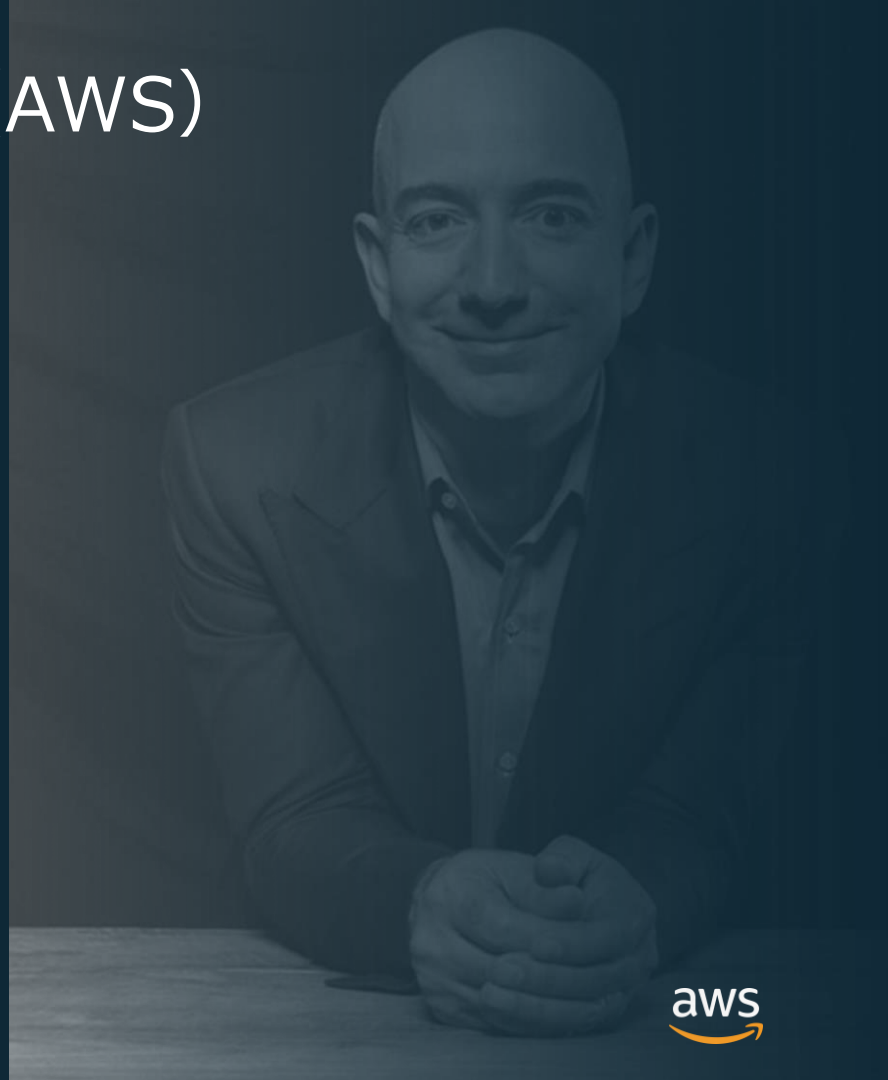
アジェンダ

- スムーズな移行への準備
  - AWS基本
  - SINETネットワークを活用したクラウド基盤構築
- 移行の選択肢
  - VMware Cloud on AWSへ移行

アマゾン ウェブ サービス（AWS）

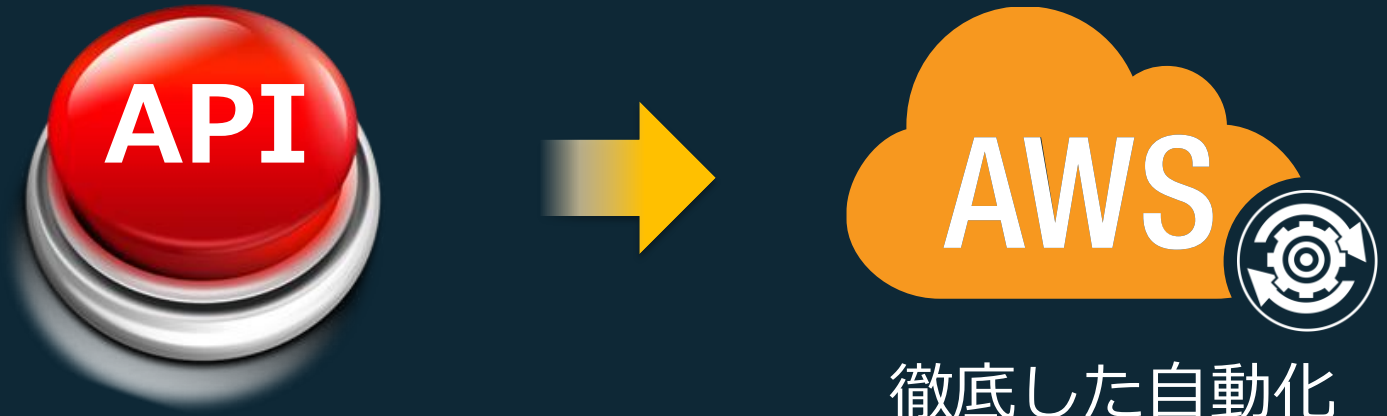
アマゾン の DNA
を持ったクラウドサービス

amazon



aws

Amazon のビジネス課題を克服するために生まれた API ベースのクラウド



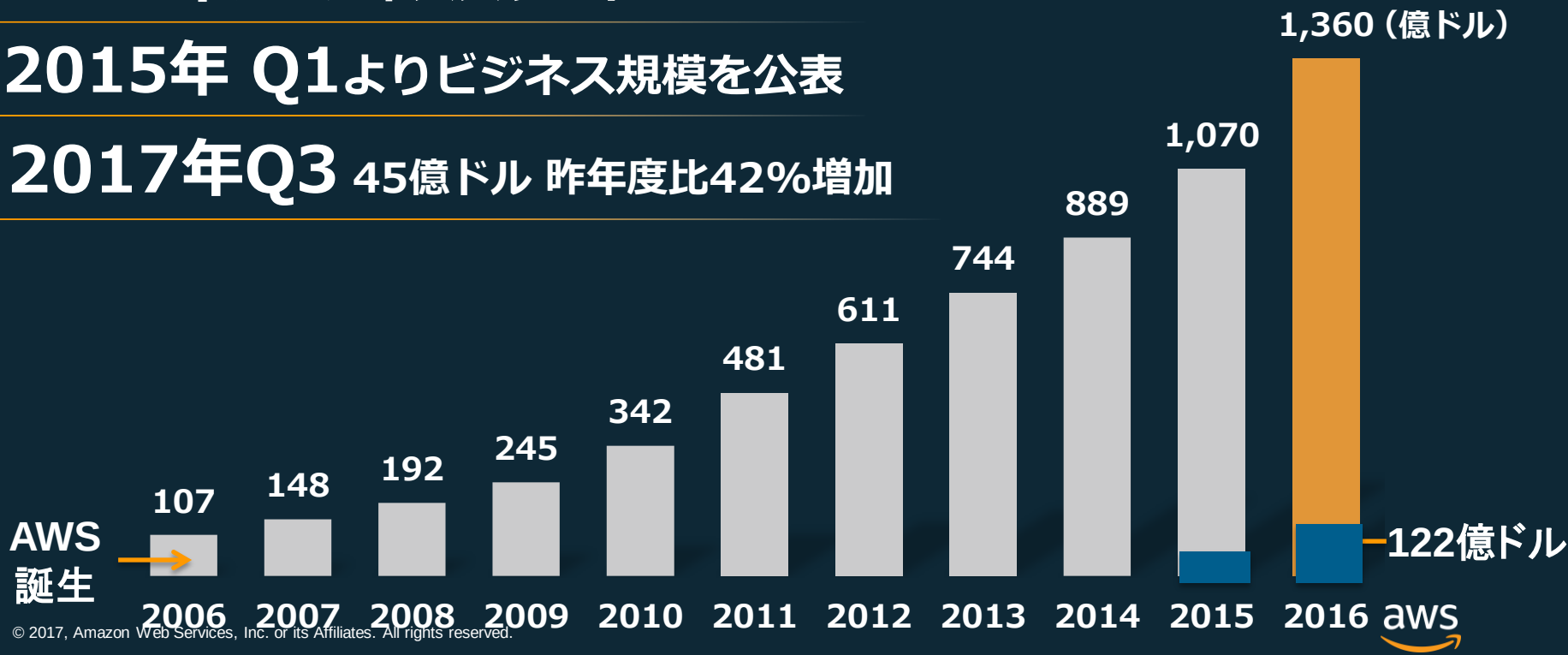
徹底した自動化

AmazonとAWSのビジネス

2006年にビジネススタート

2015年 Q1よりビジネス規模を公表

2017年Q3 45億ドル 昨年度比42%増加



運用コストを下げてお客様に還元

継続的なコストダウンを達成

Apr 22, 2008: AWS Lowers Data Transfer Costs
Oct 09, 2008: New Tiered Pricing for Amazon S3 Storage
Jan 28, 2009: New Lower Pricing Tiers for Amazon CloudFront
Aug 20, 2009: New Lower Prices for Amazon EC2 Reserved Instances
Sep 30, 2009:New Lower Price for Windows Instances with Auth Services
Oct 27, 2009: Announcing Lower Amazon EC2 Instance Pricing
Dec 08, 2009: New Lower S3 and EC2 Pricing, Free Inbound Data Transfer
Feb 01, 2010: New Lower Pricing for Outbound Data Transfer
Jun 07, 2010: Amazon CloudFront Lowers Prices with HTTPS Support
Sep 01, 2010:New Lower Prices for High Memory 2x and 4x XL Instances
Oct 05, 2010: Lower High Memory DB Instance Prices for Amazon RDS
Nov 01, 2010: Amazon S3 Reduces Storage Pricing
Jan 06, 2011: New Plans, Lower Pricing in AWS Premium Support
May 18, 2011: New Lower Prices for Amazon CloudWatch Monitoring
June 1, 2011: Free Inbound Data Transfer and Lower Outbound Tiers

規模の拡大とイノベーション

90%がお客様のフィードバックに基づき2017年は1,430の機能拡張・改善を実施

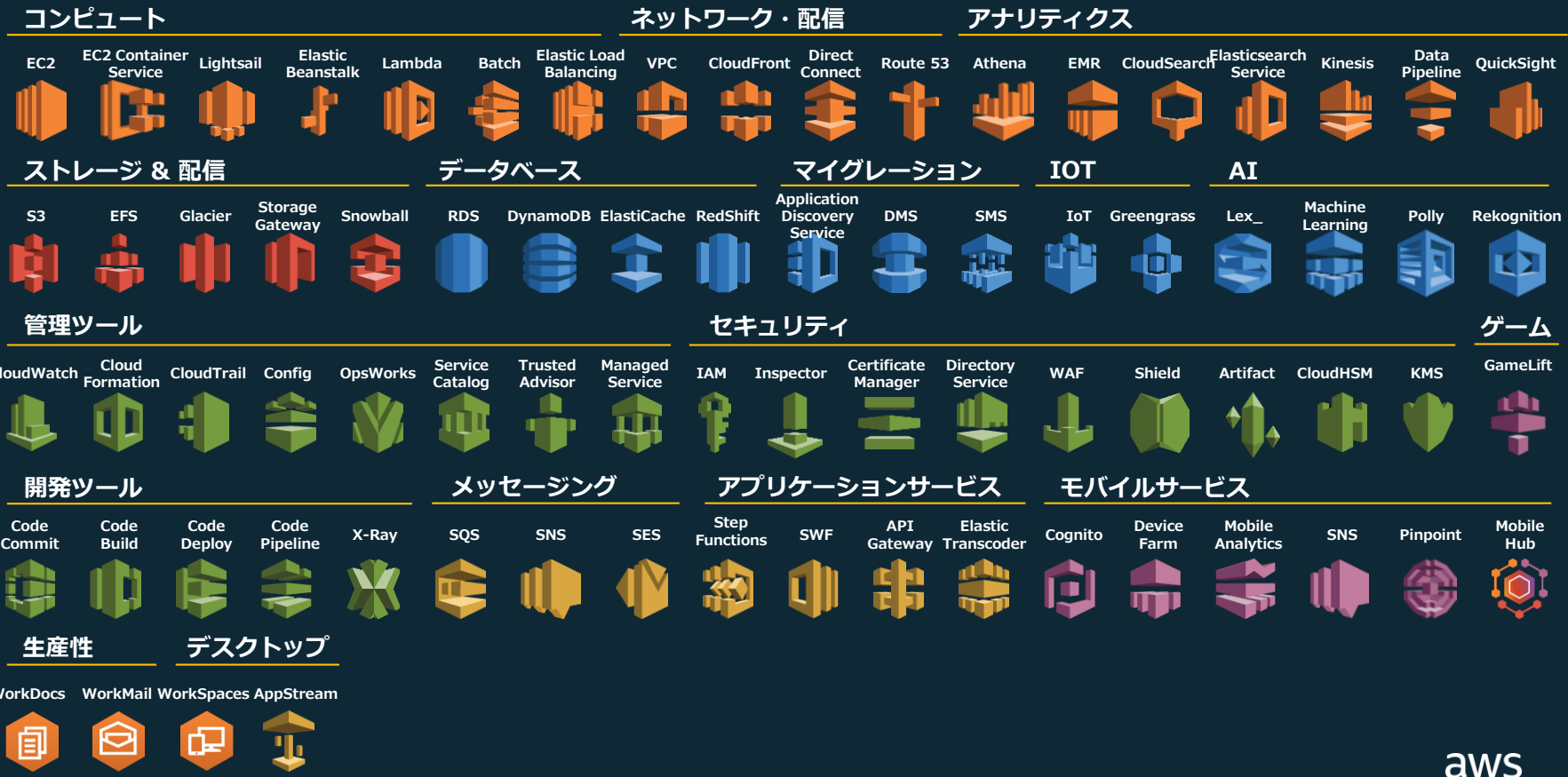
過去11年間で**63**回以上の値下げを実施

AWS 上に展開される Amazon のイノベーション

AWSを
理解する

オンプレのシステムを移行するのに
知っておくべきAWSの基本サービス

100を超えるサービス



米国ワシントン州警察
犯罪者の顔認識と徘徊中の方々の探索

TIGARD POLICE DEPARTMENT

ATTEMPT TO ID

Prepared by Crime Analyst Gayla Shillitto 503-718-2746 gayla.shillitto@tigard-or.gov
13125 SW Hall Blvd, Tigard OR 97223

THE INFORMATION CONTAINED IN THIS BULLETIN DOES *NOT* ESTABLISH OR CONVEY AUTHORITY TO ARREST, DETAIN, OR TOW, UNLESS SPECIFICALLY STATED. THIS INFORMATION IS LAW ENFORCEMENT SENSITIVE, UNLESS OTHERWISE INDICATED, AND IS RESTRICTED TO LAW ENFORCEMENT AND LP PERSONNEL ONLY. THIS INFORMATION MAY ONLY BE DISSEMINATED WITH PROPER AUTHORITY.

(U/FOUO)

The above subject entered Lowes alone, selected $953 in Dewalt tools, scanned them in at the self-checkout, then left without paying. He left as the passenger in the above vehicle. If you recognize this person, please contact Officer Tillotson.

- 指名手配犯の顔を効率的に探索
- 従来，PDF を各機関に配布し，みたことがある警官がメールで返信
- 手間がかかり，捜索精度が低かった
- Rekognition を使って他機関と連携し，効率的に探す仕組みを構築

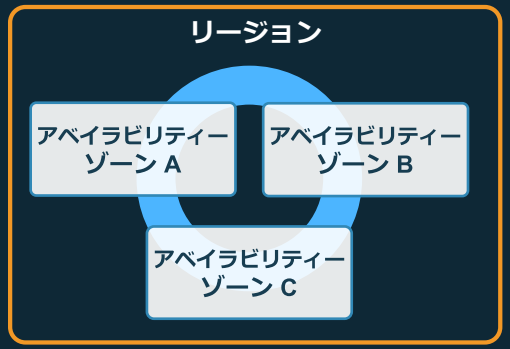
https://www.slideshare.net/AmazonWebServices/the-unusual-suspect-how-washington-county-sheriffs-office-is-using-amazon-ai-to-identify-persons-of-interest-for-law-enforcement-mcl204-reinvent-2017

AWSのグローバル インフラストラクチャ

リージョン

- **サービスを提供するデータセンタの地域や国**
  - 各リージョンは完全に独立
  - 日本では東京に加えて大阪リージョンを開始
  - リージョン間の通信はインターネット経由（大阪ローカルリージョンへはAmazonバックボーン）

アベイラビリティゾーン（AZ）



- **リージョンは２つ以上のAZから構成**
  - 災害などの影響を受けないように地理的に独立
  - AZは最低１ヶ所以上のデータセンタで構成
  - データセンタの電源やネットワークは独立
  - AZ間は低遅延の高速専用線で接続

キホンのおさらい：EC2とRDS

コンピュートとデータベース

EC2（Elastic Computing Cloud）

EC2

- **AWSの世界の「仮想マシン」**
  - 安価に使えるモデルから、GPU搭載、基幹システムまで構成できる多様なインスタンス
  - スケールアウト, スケールアップが可能
  - Widows 2003～2016、各種Linux、ML
  - インスタンス切り替え（HW移行完了）

RDS（Relational Database Services）

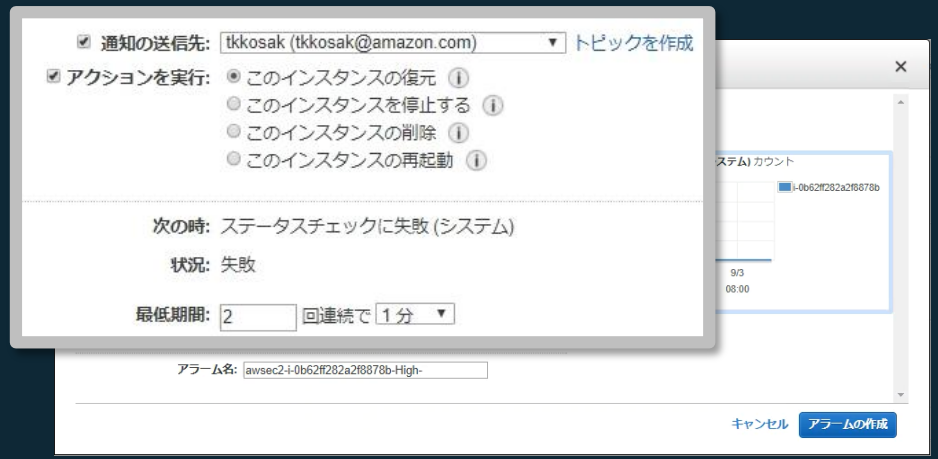
RDS

- **データベースのマネージドサービス**
  - MySQL、Postgres、MariaDB、SQL ServerやOracleをDBをAWSでホスティング
  - 人気のAurora 、DynamoDB（NoSQL)
  - データベースインフラ運用からお客様を開放
  - DMSを利用し既存VMからRDSへの移行も可能

aws

ご存知ですか？：意外と知られていないAuto Recovery

インスタンスを動かすハードウェアが故障したときは、AZの切り替えが必要なんでしょうか？



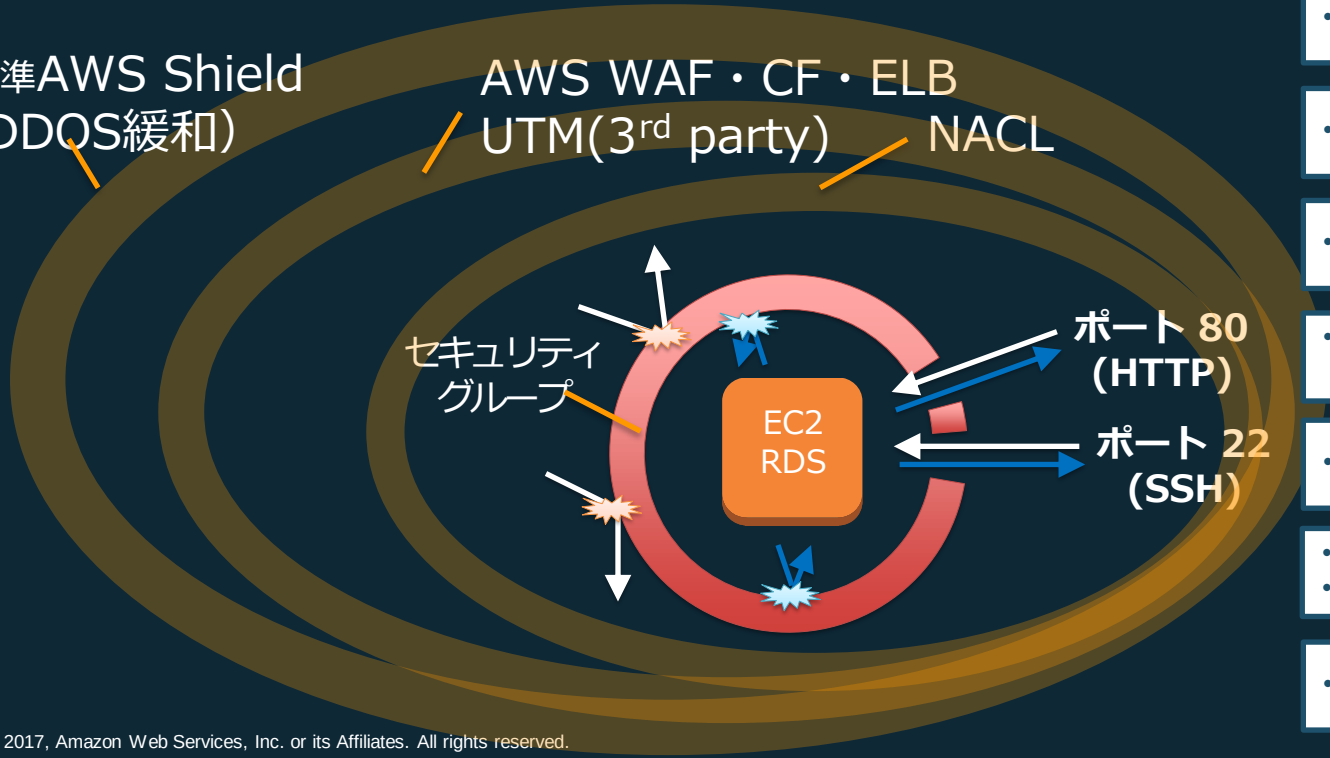
AWSにはAuto Recoveryがあります！

- vmware HAやHyper-V WSFCに相当する機能
- 障害インスタンスはAZ内の他のホストで再開（復元）
- 無償で利用可能
- AWSインフラのステータスチェック※に失敗したものが対象。**OSやアプリの障害は対象外**

※ インスタンス（仮想マシン）の健全性チェック

ご存知ですか？：意外と知られていないSecurity Group

インスタンス単位で制御できる組込みファイアウォール機能です。



- APIログの記録(Cloud Trail)
- 脆弱性診断(Inspector)
- パッチ管理(Patch Manager)
- 健全性診断(Trusted Advisor)
- 機械学習（GuardDuty）
- DDOSレスポンスチーム
- 脅威ダッシュボード
- ISO等世界中の外部認証

キホンのおさらい：EBSとAmazon S3

ストレージ

EBS（Elastic Block Storage）

EBS

- **仮想マシンに接続できるブロックストレージ**
  - 通常SSDおよびIOPS保証型SSDも提供
    システム要件に沿った設計が可能
  - オンラインでサイズ拡張や種類の変更が可能
  - スナップショットの取得も可能（S3に保存）

S3（Simple Storage Service）

S3

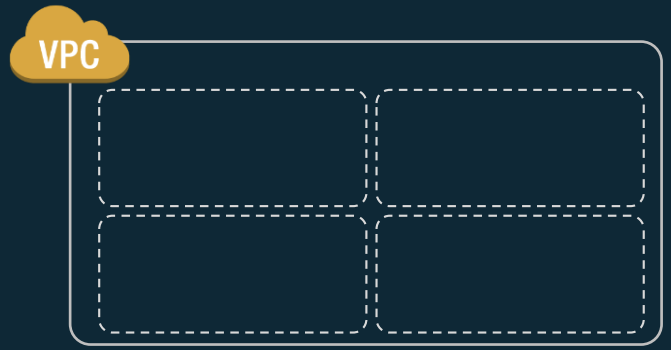
- **汎用的に使えるオブジェクトストレージ**
  - 多彩な目的（非構造データ、バックアップ，
    アーカイブ）さらに災害対策）に利用できる
  - 安価＋99.999999999%の耐性を持つ
  - 容量無制限、スケールアウト

aws

キホンのおさらい：VPCとオンプレ接続

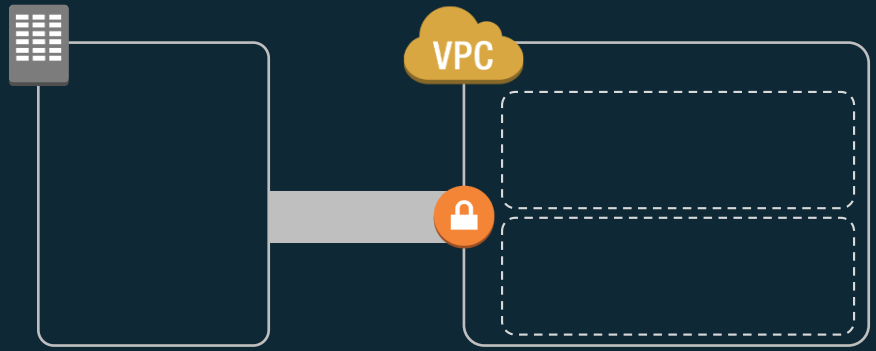
ネットワーク

VPC（Virtual Private Cloud）



- **AWSに構成する仮想ネットワーク**
  - 他のお客様との境界, 用途別の境界として
  - インスタンス（仮想マシン）は VPC 内にサブネットを構成して展開
  - DHCPも固定IPにも対応

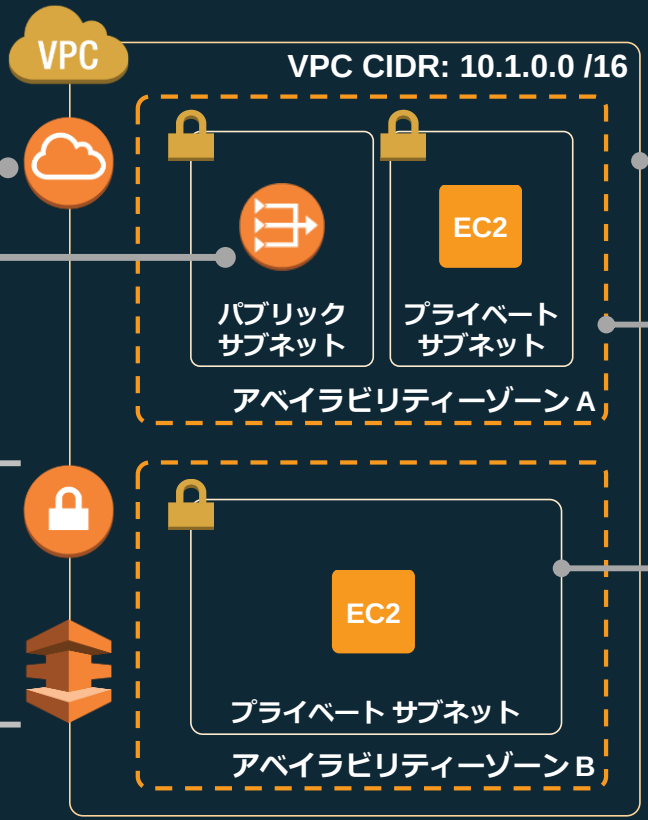
オンプレとの接続（DirectConnect / VPN）



- **オンプレミスとAWSを安全に接続**
  - お客様データセンタと AWS を安全に接続するためのネットワーク
  - 最初は VPN で初めて, 台数が増えたら専用線などのステップアップも可能

AWS でもオンプレと同じように構成できる

ネットワーク



インターネット ゲートウェイ

VPC からインターネットに接続する場合に設定するゲートウェイ

NATゲートウェイ

プライベートサブネットにある EC2 インスタンスがインターネットにアクセスするためのゲートウェイ。

DirectConnect / VPN ゲートウェイ

VPC 単位でオンプレ環境との接続に利用。DirectConnectは閉域網などによる低遅延のネットワークを構成することができます。

VPC

仮想ネットワークとして最初に定義する「箱」。 VPC の中で作成するネットワーク CIDR を定義する。

アベイラビリティゾーン（AZ）

リージョン内の異なるデータセンタでのシステムの冗長化や障害に対応。AZ間は高速ネットワークで接続。

サブネット

各アベイラビリティゾーンの中に構成するネットワーク。

インターネットに接続できる「**パブリック**」と「**プライベート**」などで使い分けたり、用途毎に作成が可能。

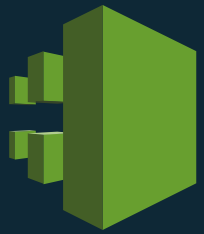
aws

AWS でオンプレ同等の運用サービス, 機能を提供

運用管理

Cloudwatch / Cloudwatch Logs / Cloudtrail

Cloudwatch



CloudTrail

- 性能監視や証跡を一元管理
  - ほぼすべてのAWSサービスの監視が可能
  - EC2やRDSでは性能監視、性能のログ蓄積
  - オンプレの運用監視製品との連携可能
  - 操作履歴をS3に保存することもできる

EC2 Systems Manager

Systems Manager

- パッチ管理やイメージへのパッチ適用を自動化
  - 展開しているWindowsサーバーへの定期的なパッチ適用のベースライン設定
  - テンプレートOS（AMI）にも適用できる
  - パッチ運用の自動化も可能
  - 他、複数の機能を提供

aws

オンプレから AWS に移行するサービスも充実

移行ツール

VM Import / Export	Server Migration Service	Database Migration Service

VM Import / Export

- **手軽にできるコマンド型移行**
  - 既存の仮想マシンイメージをAWSで利用できるようにする
  - 開発・検証機など一定時間停止が許容されるものに利用
  - 差分移行はできない

Server Migration Service

- **仮想基盤と連携する移行ツール**
  - VMware vCenterと連携
  - 本番機含めて段階移行する場合に利用
  - 差分移行も可能

Database Migration Service

- **DBだって移行できる！**
  - 仮想・物理、他社クラウド
  - エージェント導入による常時同期型のサービス
  - ダウンタイムも最小化

aws

ここまでのまとめ

オンプレと同じように使える

- **AWSもオンプレと同じように使える！**
  - コスト重視～性能重視まで豊富なインスタンス選択肢を提供
  - 自動バックアップ（EC2 Snapshot Scheduler）
  - 性能監視（Cloudwatch）
  - パッチ管理（Systems Manager）
  - 固定IP（VPC）

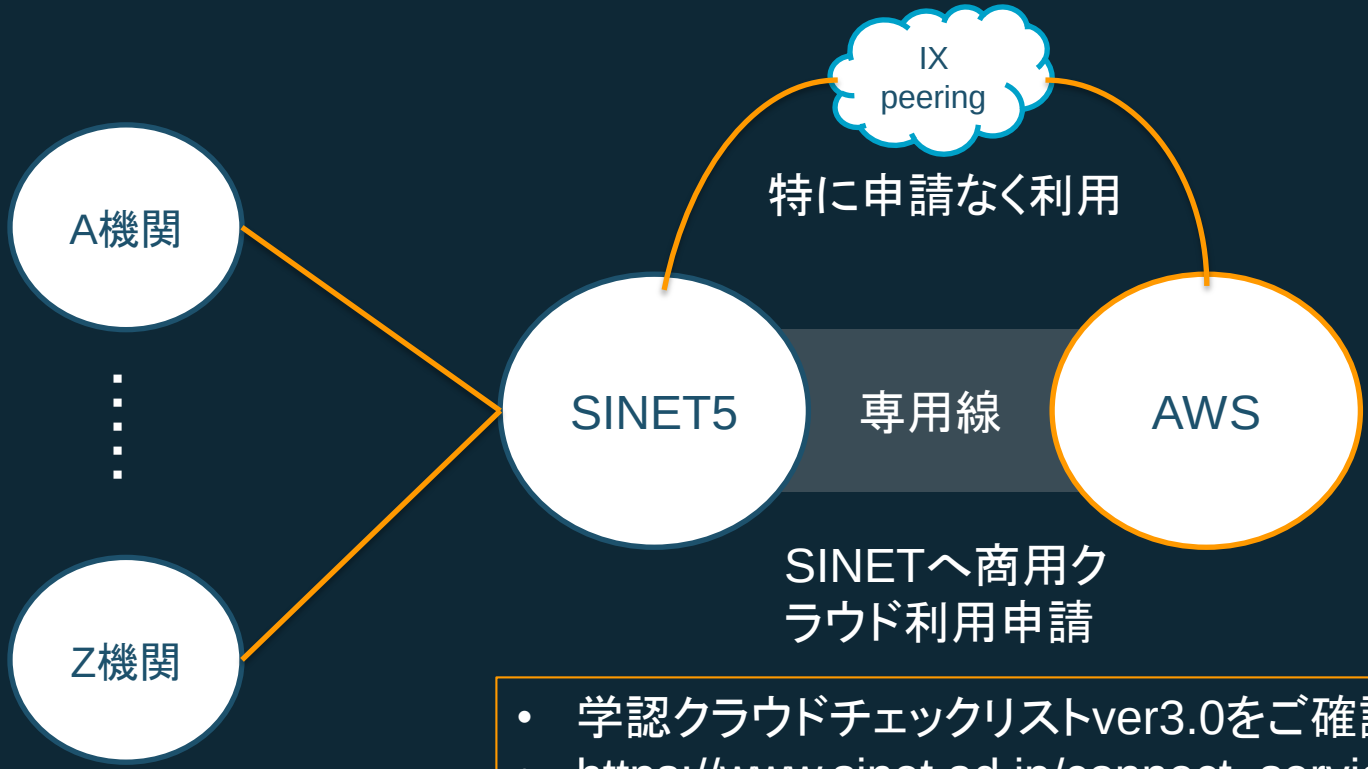
移行もカンタン！

- **SMSを使えば, ほぼあとはお任せ**
  - 一回作ればあとは移行するだけ
  - リハーサルもできる
  - SMSは「**超**」低コスト移行できる
- **P2Vのような苦労はほとんどなし**
  - ドライバなどは自動インストール
  - デバイスドライバの違いもなし

学術機関向け

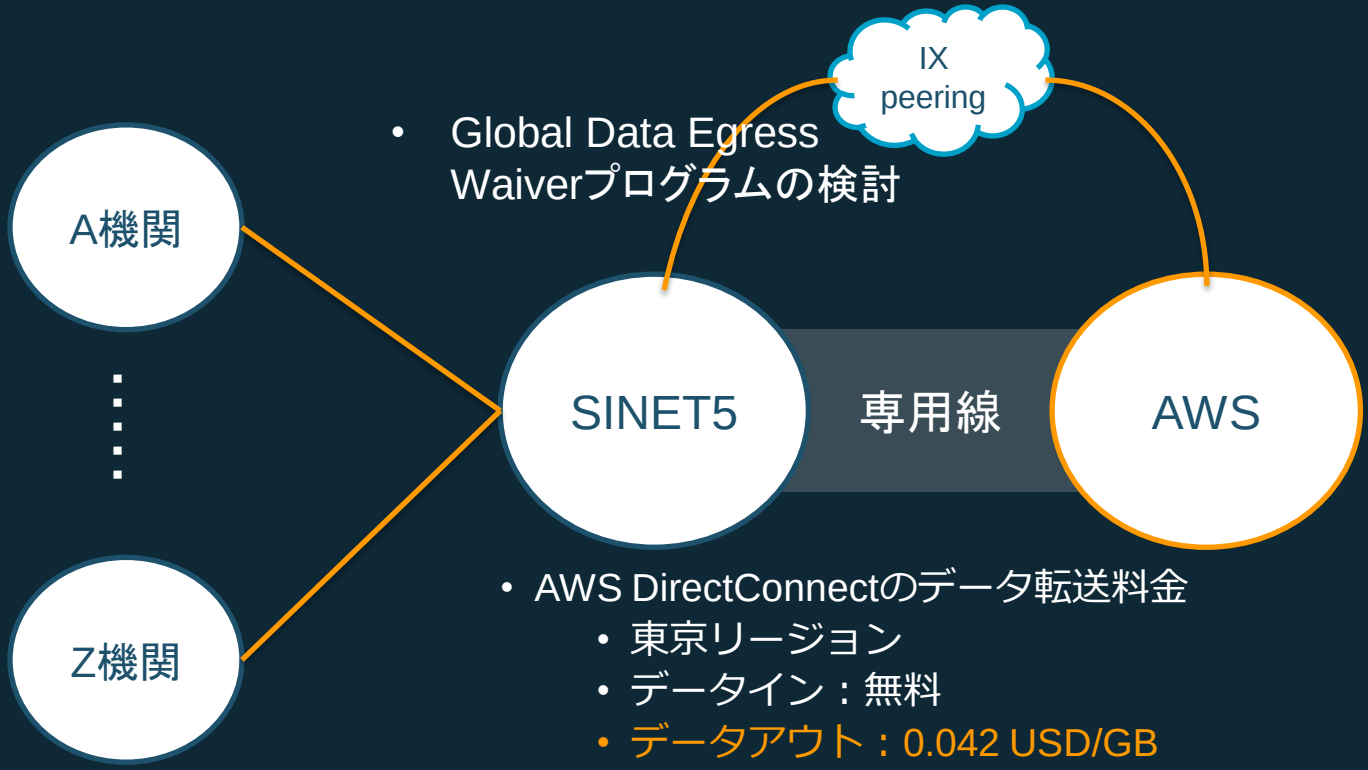
スムーズな移行への準備

AWSはSINET5と接続しています



- 学認クラウドチェックリストver3.0をご確認
- https://www.sinet.ad.jp/connect_service/service/cloud_connection

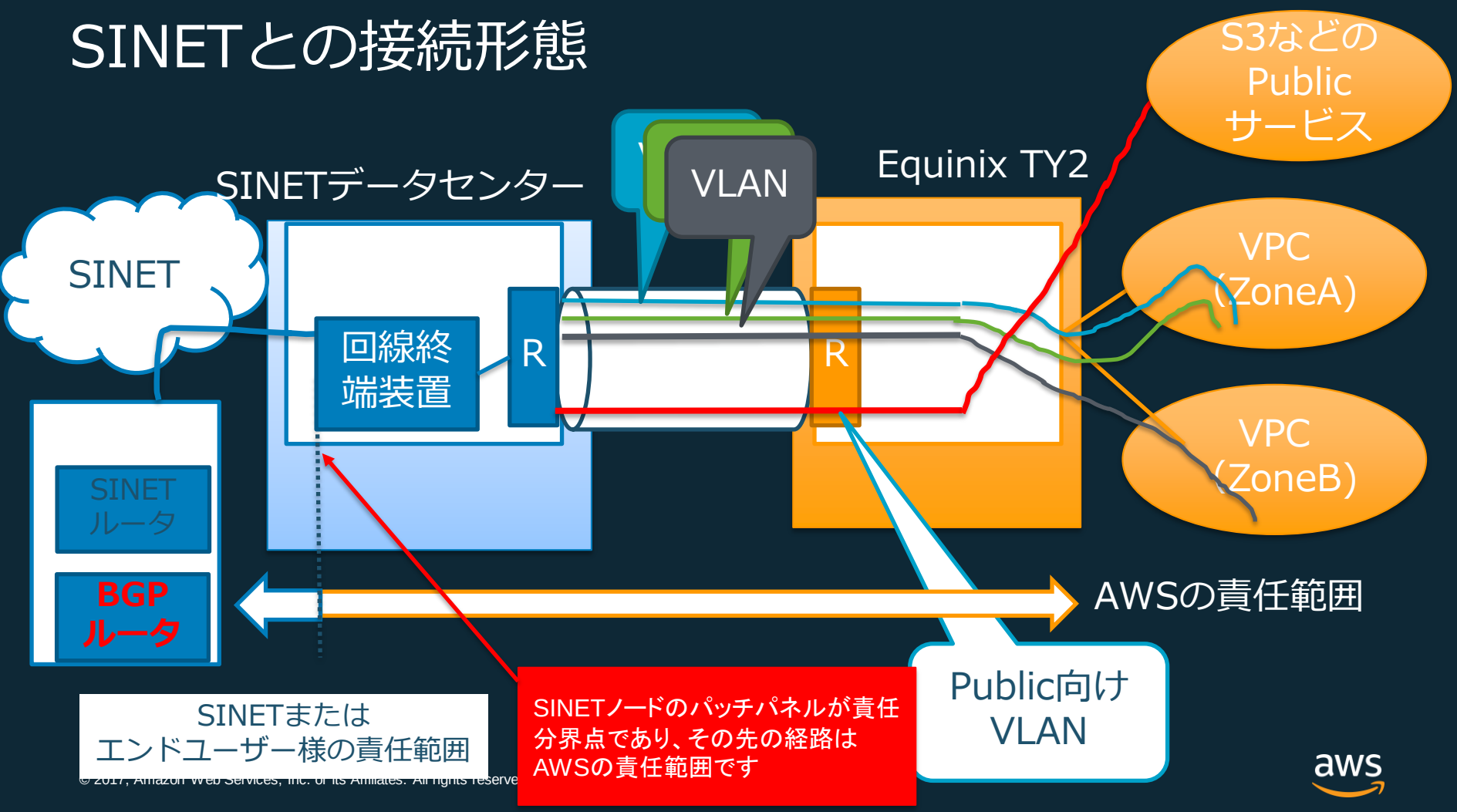
AWSなら、安価にクラウドとの閉域接続が完了



- Global Data Egress Waiverプログラムの検討

- AWS DirectConnectのデータ転送料金
  - 東京リージョン
  - データイン：無料
  - データアウト：0.042 USD/GB
  - 専用線＋ポート料金（2.142 USD/時間）は弊社負担
  - VPN費用より安価です

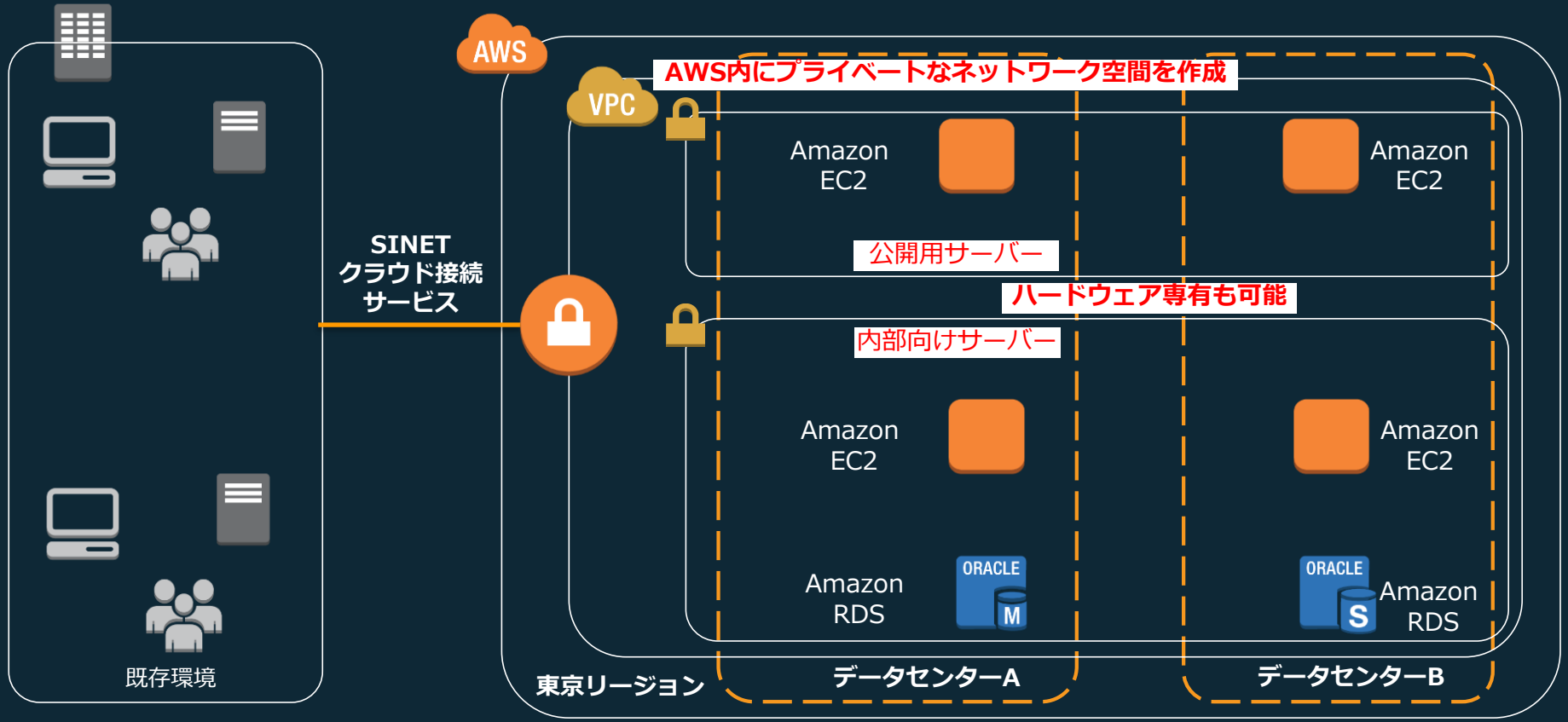
SINETとの接続形態



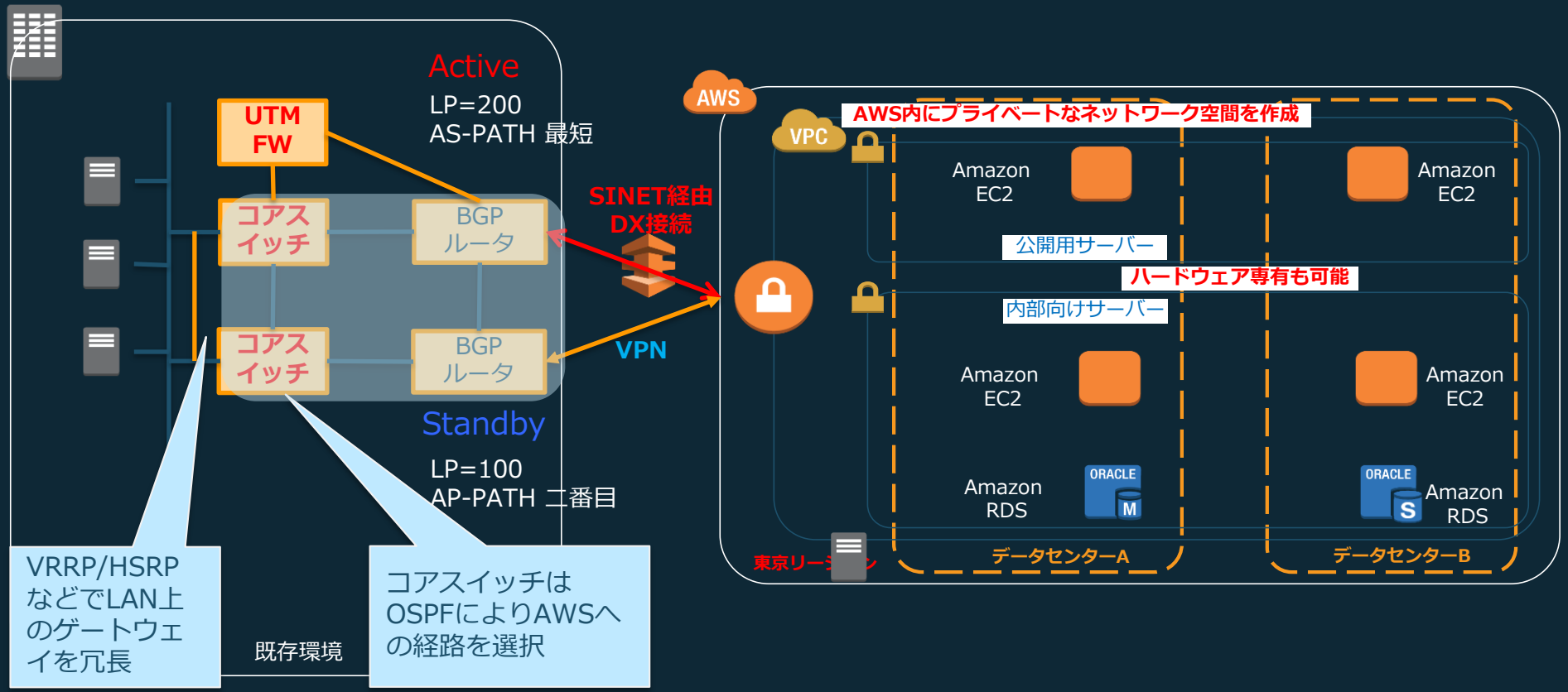
学術機関向けシェアードエコノミー

Connectionを保持している弊社アカウントより、SINETクラウド接続サービスのユーザー様にVirtual Interfaceを提供します。

SINETクラウド接続サービスによるセキュアな構成

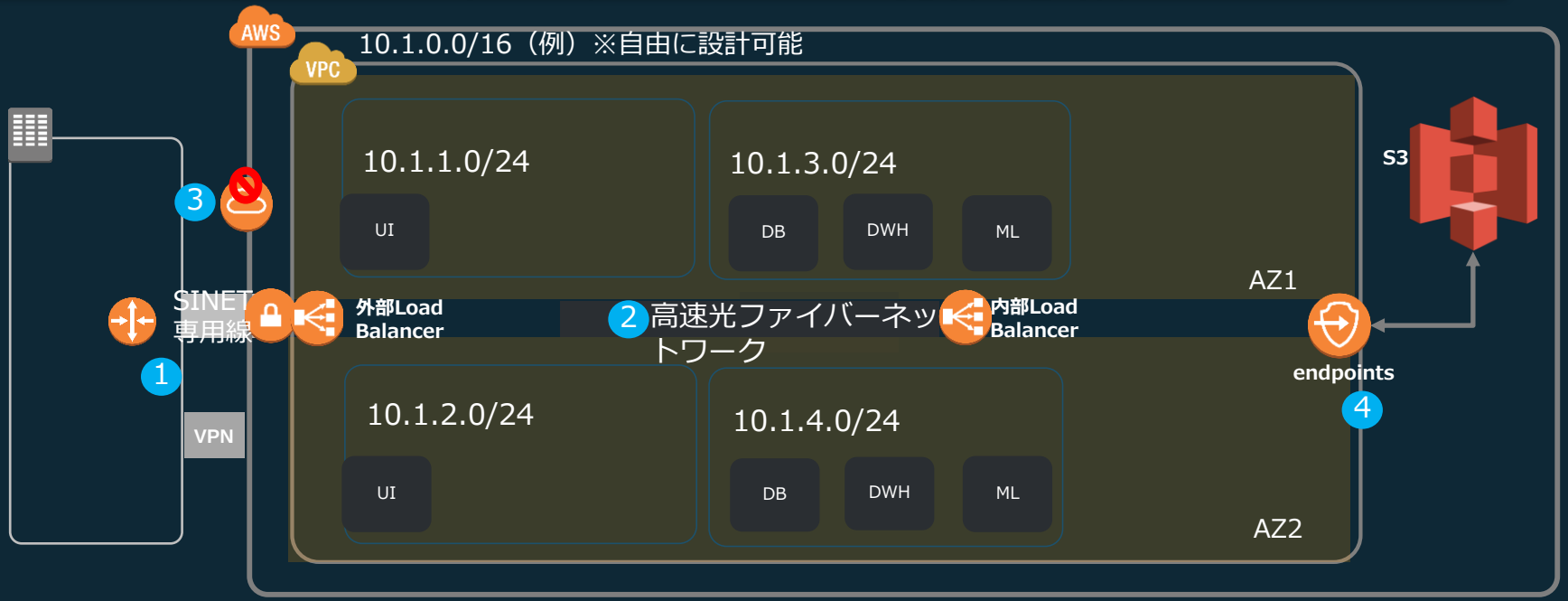


冗長化のご検討をお願いします

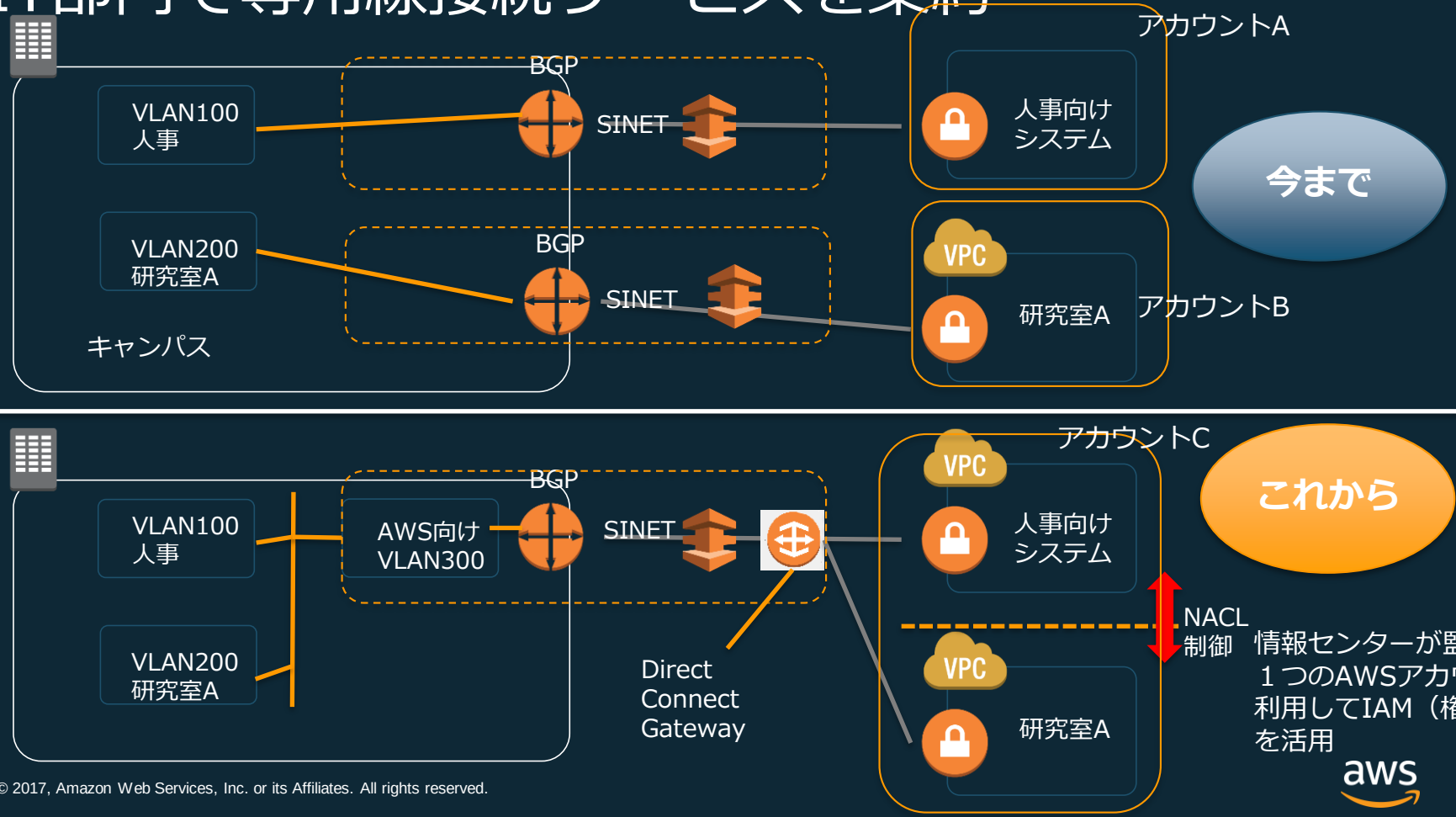


学内～VPC～S3へプライベートネットワーク

1）VPC(バーチャルプライベートクラウド）とオンプレミスネットワークを専用線(Direct Connect)あるいはIP-VPNで接続します。
2）アベイラビリティゾーン(AZ)にシステムを分散できるよう２つのAZにサブネットを作成しシステムを配置します。
3）サブネットにインターネットゲートウェイをアタッチしなければインターネットにはルーティングされません。
4）マネージドサービス（S3ストレージ等）へはプライベートエンドポイントを活用し閉域接続します。

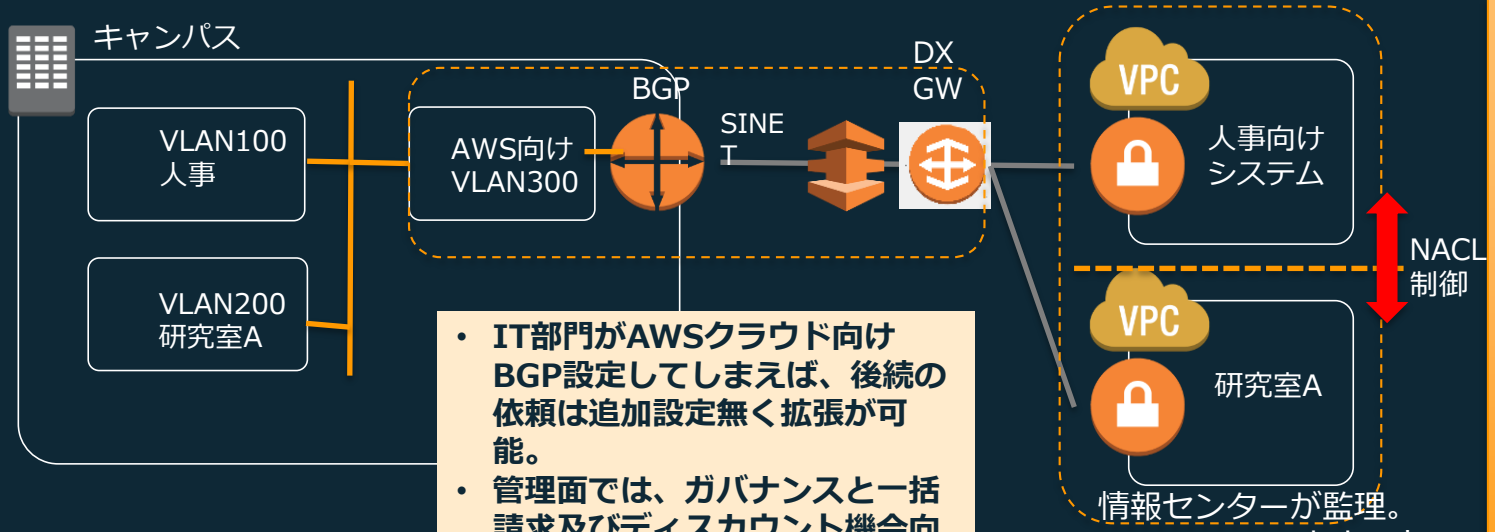


IT部門で専用線接続サービスを集約



共通基盤で専用線接続サービスを集約

Direct Connect Gateway を活用しAWSクラウド向けネットワーク集約を
（従来は1システムや研究室単位でDirect Connectの設定が必要でしたがDXGWリリースにより改善）



- **IT部門がAWSクラウド向けBGP設定してしまえば、後続の依頼は追加設定無く拡張が可能。**
- **管理面では、ガバナンスと一括請求及びディスカウント機会向上のメリットがある**
- **ユーザとしては請求処理やBGP設定の学内交渉が楽になる**

ポイント：

・IT部門による見える化の実現（各部門、研究室の把握）

・Billingの集約

・マルチVPCへの接続（柔軟対応、AWSへ追加設定依頼不要、BGP追加変更不要）

AWSクラウド共通基盤利用化の検討ポイント

ステップ 1

AWSアカウント
VPC設計(SINET)
FW設計

- 組織形態にあったアカウント利用
- 開発と本番
- 情シス部門主導でSINETとAWS接続の設計

ステップ 2

IAM管理

- 認証認可
- サービス単位、リソース単位
- 開発と運用の分離

ステップ 3

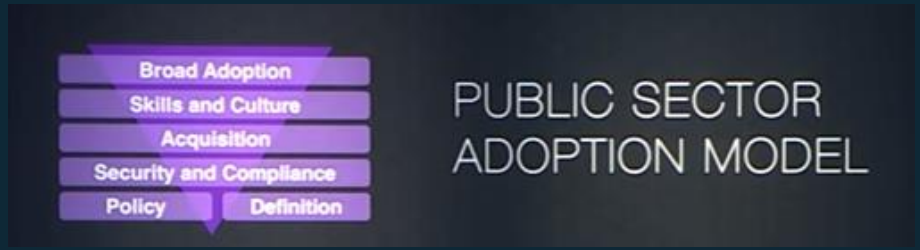
監視
ログ分析

- AWSのサービスを検討
- 従来を踏襲
- 一元化（将来）

問い合わせ窓口

SINET@amazon.com

AWSが考える公共機関のクラウド適用モデル



幅広い利用に向けた展開

スキルと習慣

調達

セキュリティとコンプライアンス

政策

定義

- 学認クラウド導入支援（チェックリスト）
- 広大ガイドライン
- 先行事例

クラウドの理解、技術的な学習のご支援

1

・セキュリティ回答
・仕様書支援
・技術支援
・ベストプラクティスを元にした診断

2

次回
4/20@
目黒

3

aws educate
～明日のクラウドワーカーを今日作る～

アジェンダ

- スムーズな移行への準備
  - AWS基本
  - SINETネットワークを活用したクラウド基盤構築
- 移行の選択肢
  - VMware Cloud on AWSへ移行

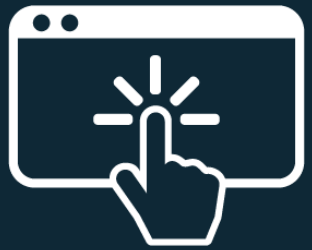
改めて、クラウド利用が進む理由

初期投資が不要

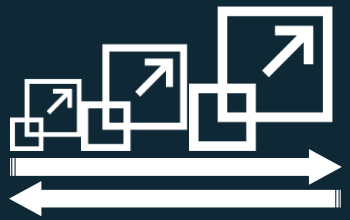
実際の使用分のみ支払い

継続的な値下げ

セルフサービスなインフラ



スケールアウト/イン・アップ/ダウンが容易



お客様のビジネススピードを改善

クラウド化で生ずるハイブリッドアーキテクチャ

オンプレミスで
ワークロードを
稼働

クラウド上で
ワークロードを
稼働

クラウド間の
緊密な連携

ハードウェアの
リプレースを回
避（基盤アップ
デートの費用と
工数）

ハイブリッド運用への移行上の課題

仮想マシンの
フォーマット

ネットワーク

運用手順

スキルとツール

監視と制御

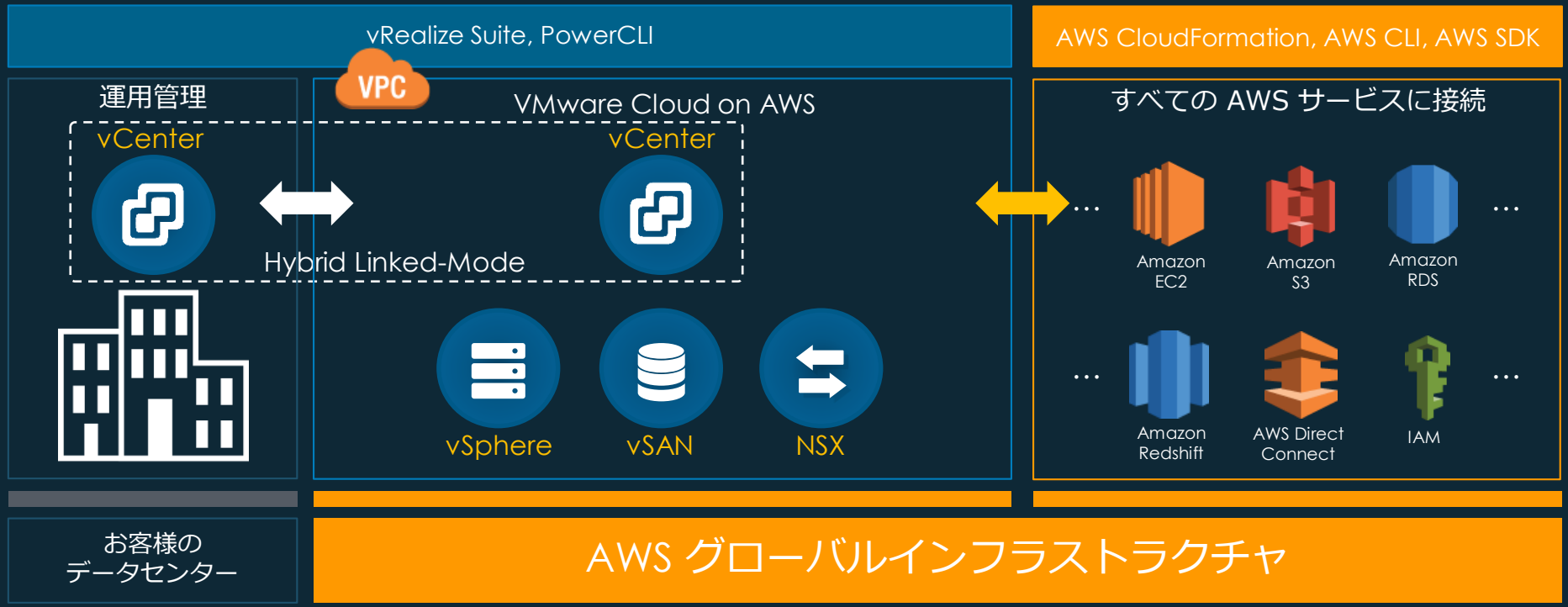
重複する作業

新たな選択肢

aws

VMware Cloud on AWS: 概要

VMware SDDC をベアメタル の AWS 基盤上で直接実行するマネージドサービス



VMware Cloud on AWS: アクセスモデル

- 物理リソースとして EC2 をベアメタルとして提供

- ハイパーバイザ（vSphere）や仮想化技術の管理コンポーネントの提供
- 仮想化基盤の管理
（監視、パッチ管理、アップデート等）

- VMCポータル及び vCenter からお客様テナントへのアクセス
- テナント上の仮想マシン及びネットワークの管理

※ ESXi root権限、VDS設定、管理VM/NSX Edge への直接アクセスはありません

利用シナリオとユースケース

VMware または AWS のお客様が VMware Cloud on AWS に感心を示す理由は幾つかのシナリオに集約されます。

シナリオ 1: メンテナンスと拡張

- 地域拡散 グロバリゼーション
- 災害対策、バックアップ、運用継続性

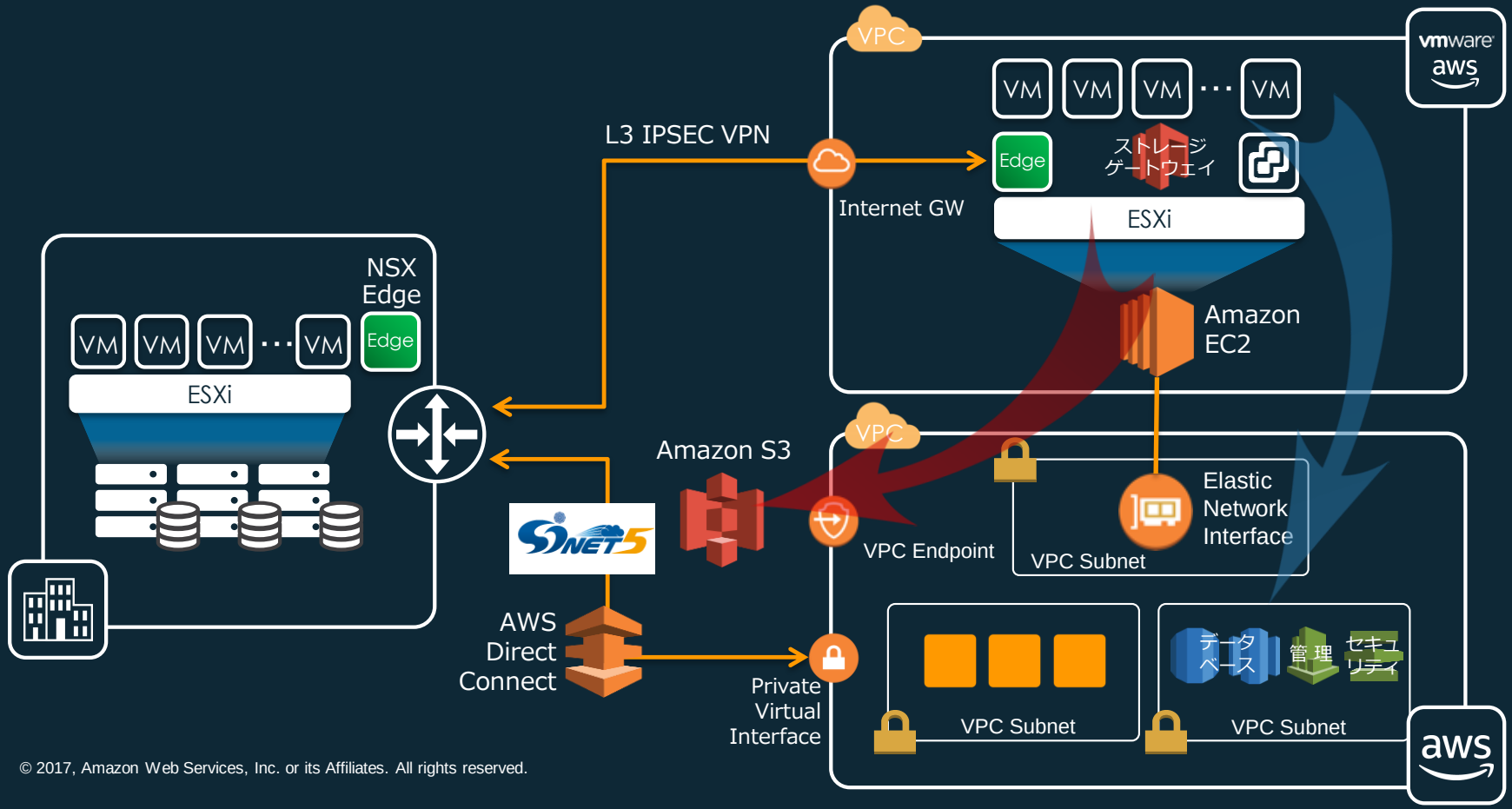
シナリオ 2: DC統合と移行

- データセンタ統合
- アプリケーション移行

シナリオ 3: ﾜｰｸﾛｰﾄﾞの柔軟性

- 本番/開発/テスト/教育 用途別に稼働領域を選択
- バースト対応

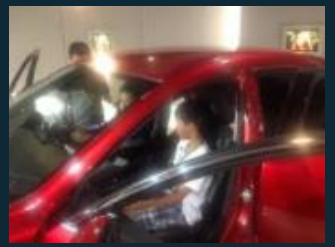
AWS のネイティブサービスとの連携



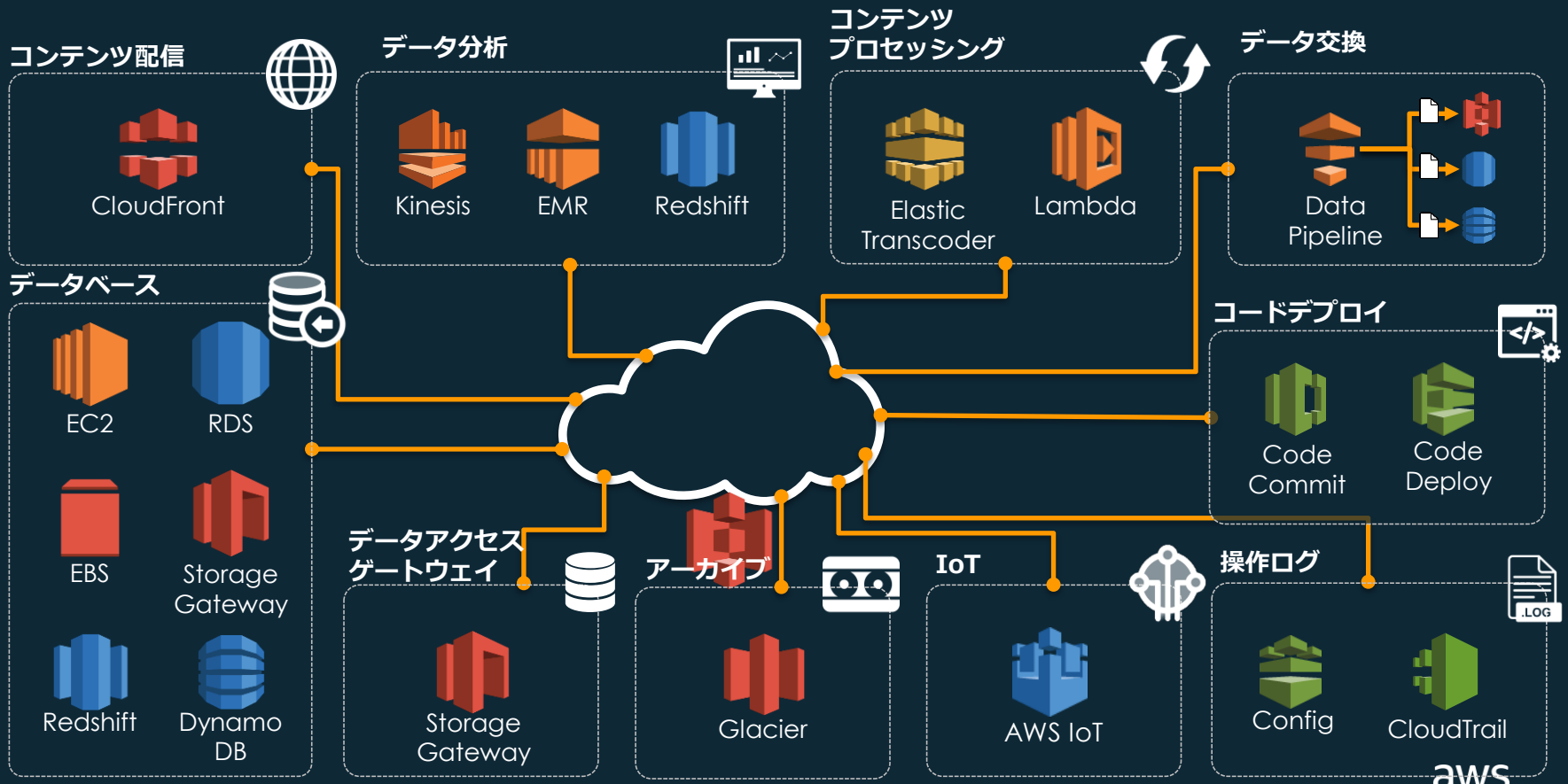
お客様が得られる価値(AWSクラウドで得られる価値に加えて)

- 基盤アップデートから解放（塩漬けからも解放）
- 既存アプリの対応
- L2延伸
- 大量VMの容易なLift＆Shift
- vMotion移行?(SINET-DX)
- VMC内のvMotion
- VSANストレージ

- Amazon S3のプライベート接続
- AWSのネイティブサービスとの連携



S3 によるデータハブで付加価値



- ✓ VMware Cloud on AWS で、既存の運用を変更せずにクラウドへ移行
- ✓ クラウドならではの価値を享受
- ✓ VMware vSphere で培ったスキルをそのままに、AWS のサービスで提供される価値との融合
- ✓ 運用管理からの解放で、守りから攻めの IT へシフト
- ✓ まずはSINET専用線でAWSクラウドへ接続しておく

aws

Still Day One.