AWS へ全面 Migration するために

アマゾン データ サービス ジャパン株式会社
ソリューションアーキテクト シニアマネージャ
荒木靖宏

amazon web services

ハッシュタグは　#AWSRoadshow
皆さんのご意見聞かせてください！

公式Twitterアカウント@awscloud_jp
を**フォローすると**、ロゴ入り
コースターを**プレゼント**

【コースター配布場所】　会場受付

amazon
web services

自己紹介

- 名前
  - 荒木 靖宏
- 所属
  - アマゾンデータサービスジャパン株式会社
  - 技術本部レディネスソリューション部
    シニアマネージャ
- 好きなAWSサービス
  - Amazon Virtual Private Cloud
  - AWS Direct Connect
- 博士（科学）

AWSへの移行メリット

コスト
高額な先行投資から実需に合わせた
オンデマンドな利用へ

ハイブリッド
自社DCの拡張としてクラウドを活用
段階的移行、用途に合わせた環境選択

ビッグデータ,BCP-DR
オンプレミスでは難しい新領域への投資

セキュリティ
AWSの優れたセキュリティ環境の利用と
自社セキュリティポリシーの適用

クラウドネイティブな “マネージドサービス” も数多く提供

AWS マーケットプレイス

エンタープライズ
アプリケーション

プラットフォーム
サービス

セキュリティ&管理・運用

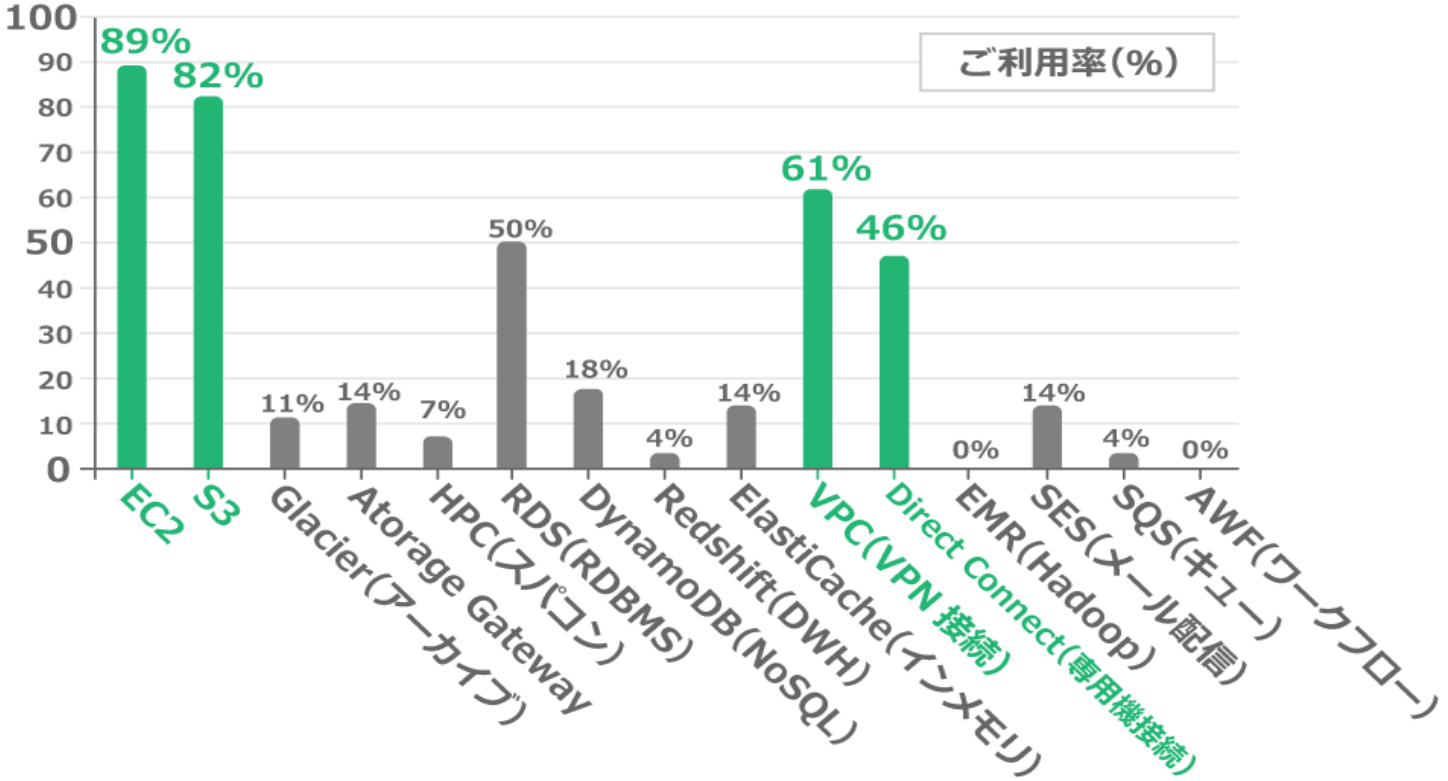
コア　サービス

インフラストラクチャー

amazon web services

E-JAWS調べ

どのサービスを使っていますか？（2013年11月）



amazon web services

企業ITのAWS移行を促進した“３つの特長”

仮想**プライベートクラウド**

Amazon VPC

専用線接続サービス

Amazon Direct Connect

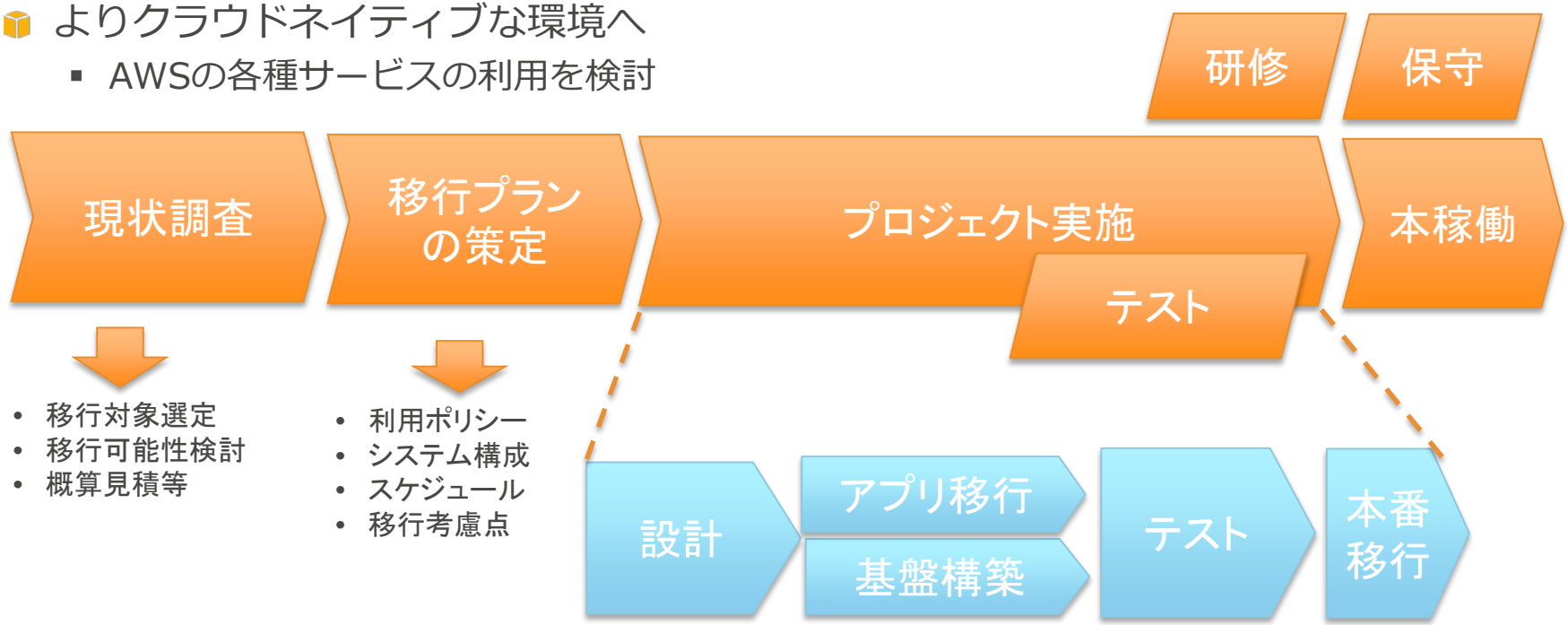
商用**ライセンスのAWSへの持込**
BYOL(Bring Your Own License)

Microsoft SAP IBM TREND MICRO WORKS APPLICATIONS
redhat ORACLE FUJITSU infoteria SOFTBRAIN Co.,Ltd.
HITACHI Inspire the Next CITRIX 1ST WingArc SuperStream SAISON INFORMATION SYSTEMS CO.,LTD 株式会社セゾン情報システムズ

amazon web services

マイグレーションの流れ

- 基本はストレート移行
  - 移行のインパクトを下げ、移行コストを低減
- よりクラウドネイティブな環境へ
  - AWSの各種サービスの利用を検討

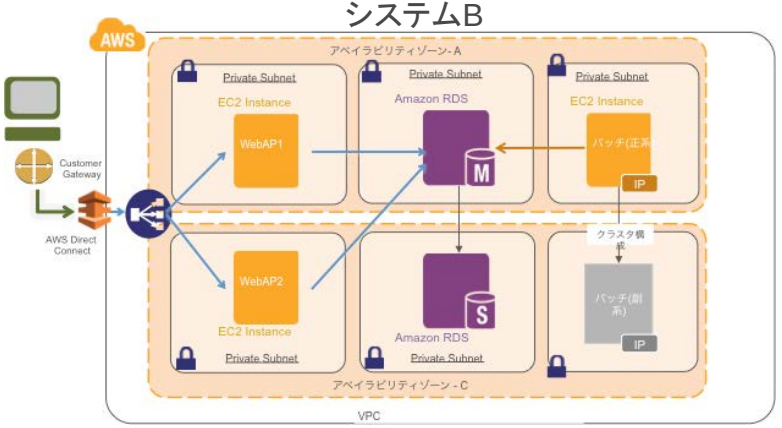


移行プランの策定

- 現状調査
  - 移行対象の選定
    重要度、移行難易度、コスト効果に応じて移行対象を優先度付け
    - アプリ改修の要否
    - ミドルウェアの対応
    - システム間連携
- 移行プランの策定
  - 移行考慮点の洗い出し
  - システム構成の検討
    - クラウドデザインパターンの適用検討
    - マネージド・サービスの活用検討
  - データ移行、アプリケーション移行方式の検討
  - セキュリティポリシー/利用ポリシーの作成
  - 移行スケジュールの策定

システム	重要度	移行難易度	コスト効果	移行優先度
システムA	◎	△	○	○
システムB	△	◎	◎	◎
システムC	○	×	×	×
…	…	…	…	…

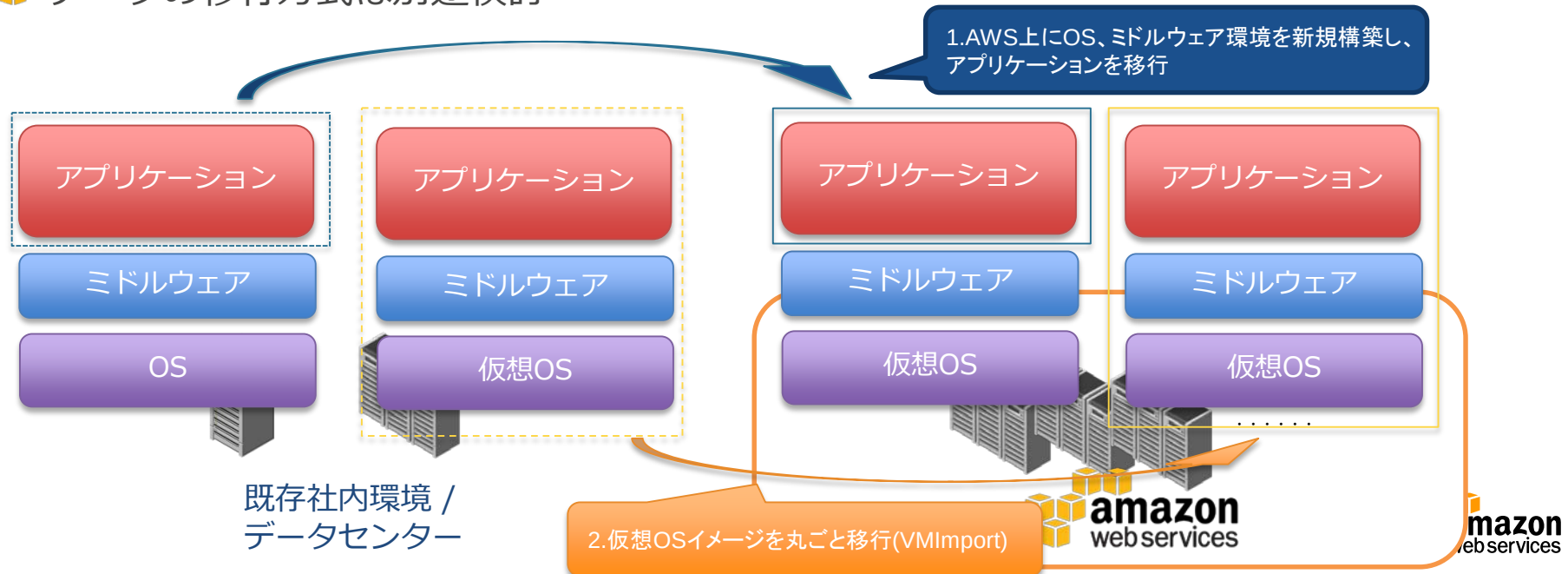
システムB



AWSへの移行イメージ

- 典型的な移行パターン
  1. AWS上に既存環境と同等のOS/ミドルウェア環境を構築し、アプリケーションを移行
  2. 仮想OSイメージをVMImportにより移行※
- データの移行方式は別途検討

※Import元はx86プラットフォームの一部の仮想化環境(Windows,Linux)のみとなります。



移行プラン策定のポイント(1/3)

- OS、ミドルウェア、業務パッケージソフト、アプリケーション、運用管理の変更点を踏まえた移行方針・方式を検討
  - ミドルウェアのバージョンアップ等
  - 基本的にはなるべく変更が少ない移行方式が望ましい
- UNIXシステムから移行の場合にはアーキテクチャーの変更にも注意
  - マイグレーションサービスの利用検討

※アプリケーションの言語、プラットフォームやOS変更の有無によっては再コンパイルが必要なケースがあります。

移行プラン策定のポイント(2/3)

- AWSの各種サービスの活用を検討する
  - デプロイメント
  - オートスケーリング
  - RDBMS
  - KVS
  - キャッシング
  - イベント・ドリブン処理
  - 非同期処理
  - etc,…


Elastic Beanstalk


DynamoDB


AWS OpsWorks


Amazon RDS


ElastiCache


Auto Scaling


Amazon SNS


Amazon SQS


Amazon SWF

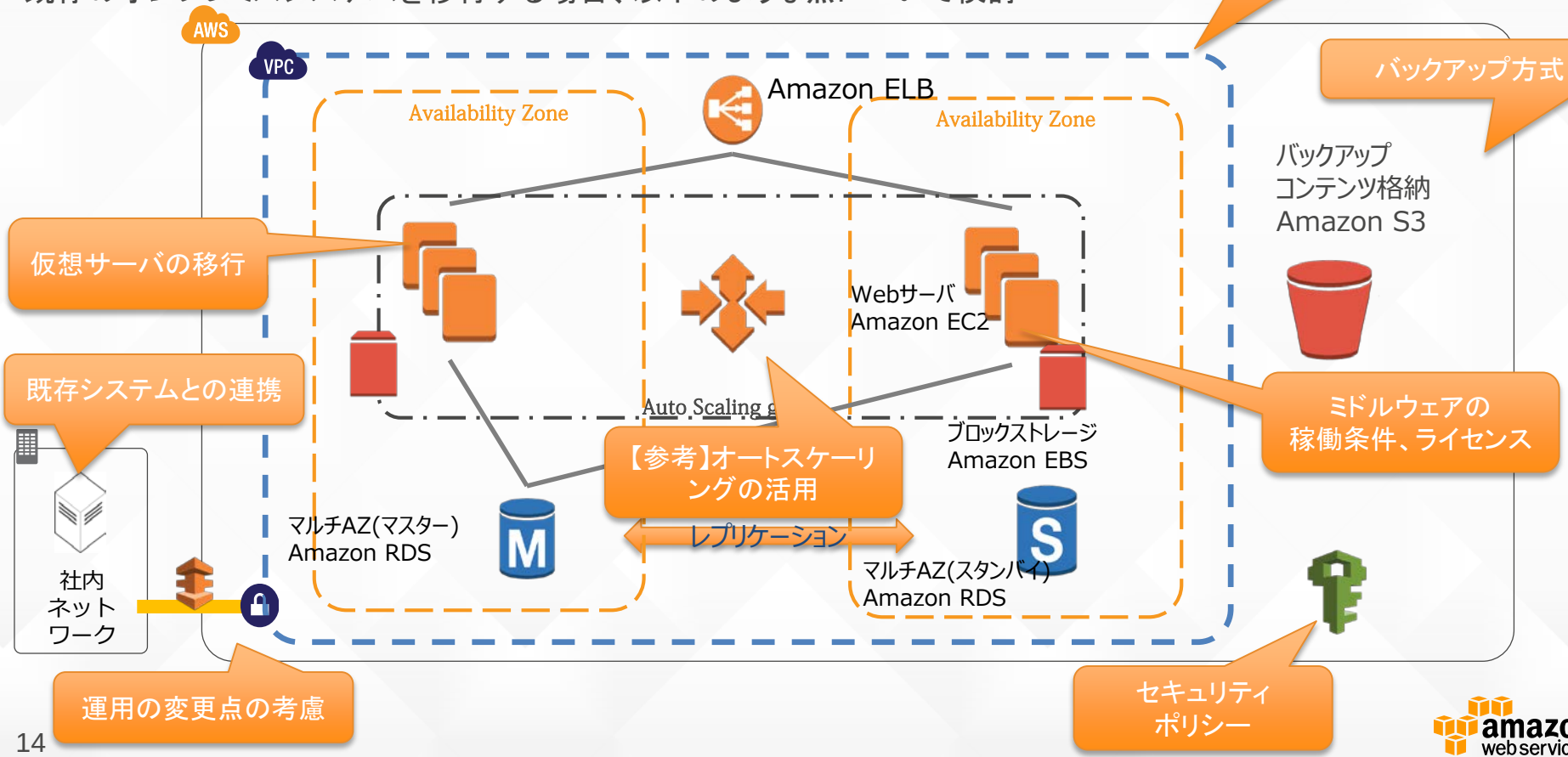
amazon web services

移行プラン策定のポイント(3/3)

- AWS利用に関するガイドラインの作成
  - 社内IT標準に則した形でクラウド環境に適合した新たなガイドラインを策定
    - AWS利用ポリシー
      - AWS採用システムの範囲の策定
      - システム重要度の定義と適用技術のマッピング
    - セキュリティポリシー
      - 自社標準ポリシーに合わせた採用技術の選択
      - AWSアカウント管理のガイドライン策定
      - etc…

既存システムからの移行における検討ポイント

既存のオンプレミスシステムを移行する場合、以下のような点について検討



amazon web services

仮想サーバの移行

- **VM Import/Export**
  (仮想サーバイメージのインポート／エクスポートツール)
  - VMware/Hyper-V/Citrix Xenの仮想イメージファイルを、AWS上へ移行する為のツール

    <対応OS一覧>

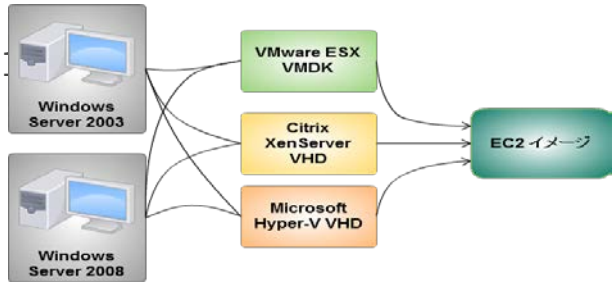
    Windows Server2003/2003R2/2008/2008R2/2012/201

    RHEL5.1～6.5 (Redhat Cloud Accessを利用)

    Centos 5.1～6.5

    Ubuntu12.04, 12.10, 13.04, 13.10

    Debian 6.0.0～6.0.8, 7.0.0～7.2.0

    http://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/VMImportPrerequisites.html
  - インポート後のインスタンスは、他のEC2と同じ様にS3やELB, Autoscalingなどを利用したAWSクラウドの可用性、堅牢性、リソースの柔軟性を享受可能

amazon web services

AWSへのデータ移行

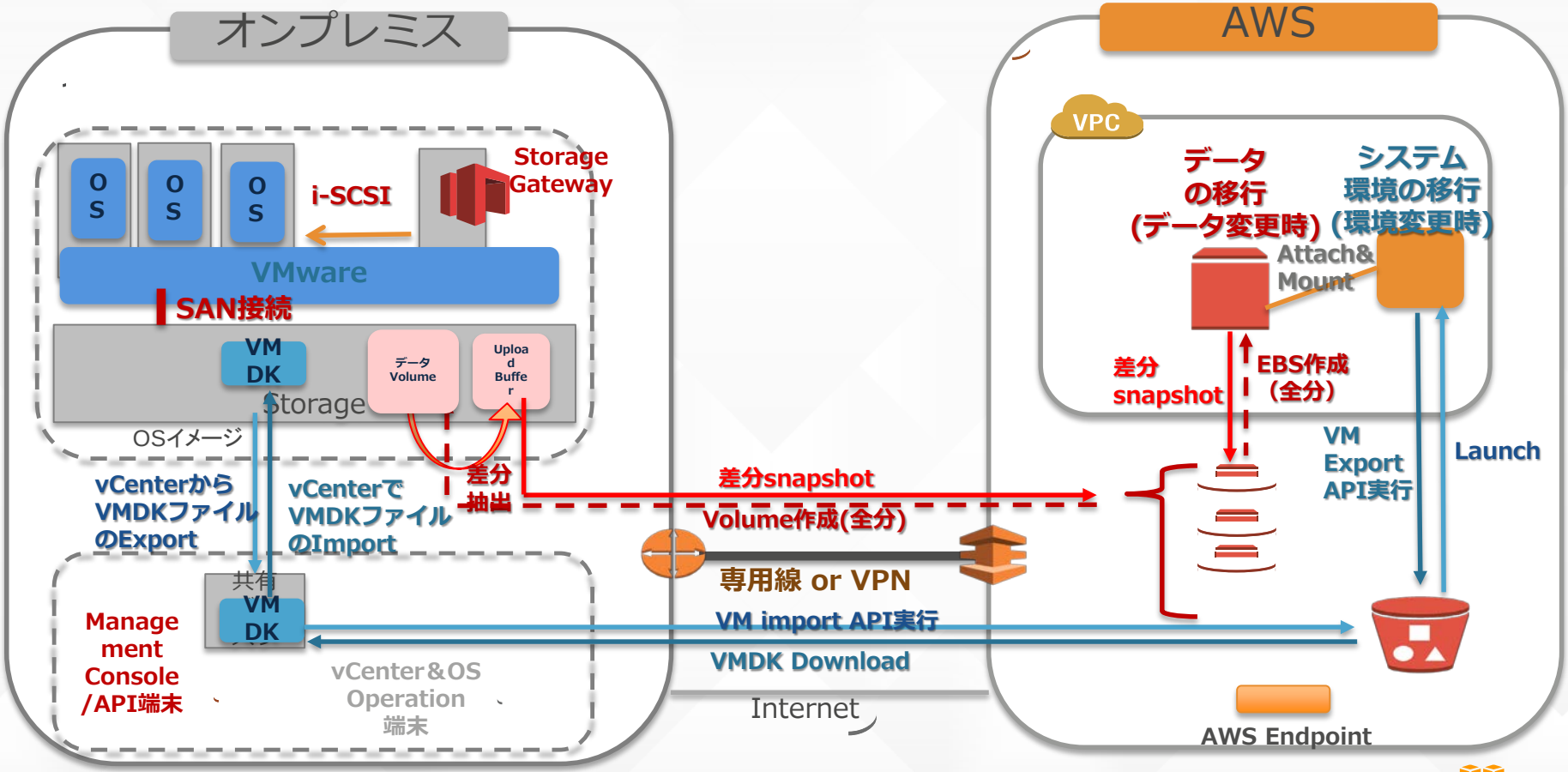
データの形式、切り替え時間を考慮し、最適な方式を選択

- AWS Database Migration Serviceの使用
- フラットファイル
  - データをフラットファイルにダンプアウトし、S3等を活用してデータ移行
- DBのレプリケーション
  - オンプレ-AWS間でデータを同期し、切替時に切断
- StorageGatewayの活用
  - オンプレミスのデータをボリューム単位で移行
- ミドルウェア固有の移行方式
  - ミドルウェア毎に固有のデータ移行方式を持つものが有る

基本はネットワーク経由

- 移行時間はネットワーク帯域に大きく依存
  - インターネット(VPN)経由 or Direct Connectの選択
- パートナーソリューションの活用
  - DX環境を利用したデータインポートサービス
    (参考)http://cloudpack.jp/service/spin-off/directimport.html

VM移行/データ移行例(VMImport/StorageGateway)



amazon web services

ミドルウェアの稼働条件、ライセンスの考慮

利用ミドルウェアの稼働条件を確認

- ミドルウェアによっては、クラウド対応(時間課金)のライセンスが適用可能なものもある
- 個別のミドルウェアについてBYOL対応、時間課金対応、移管方法などの調査が必要
- ミドルウェアによってはインスタンスタイプが決まっているものもある(SAP等)

マーケットプレイスの活用

- 一部ミドルウェアではミドルウェア導入済みのAMIが提供されている
- 利用料金はAWSから一括請求

https://aws.amazon.com/marketplace

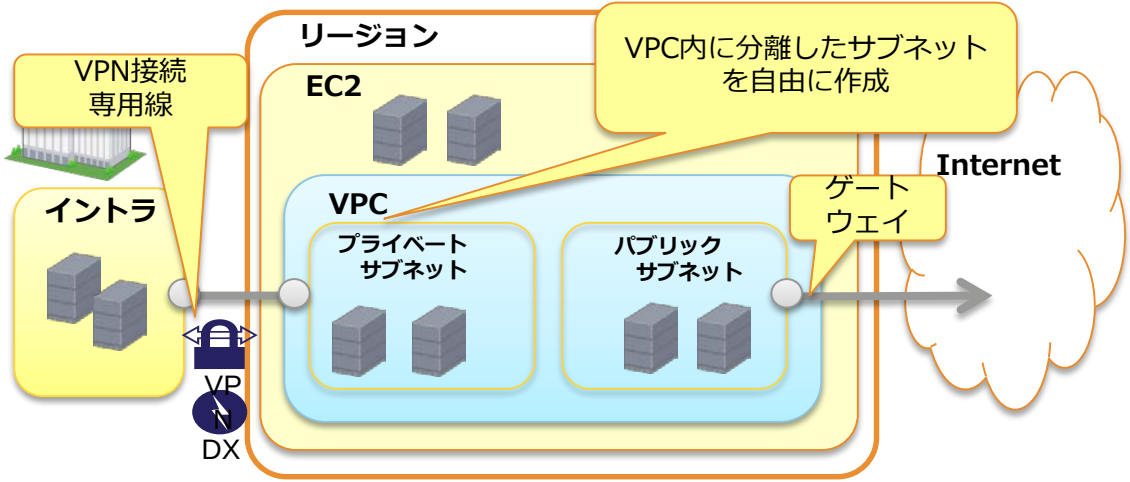
	主要なアプリケーション	ライセンスの持込み	1時間単位での従量課金
Microsoft	Microsoft SharePoint Server Microsoft Server and Tools Microsoft Windows Server Apps	○	○
SAP	SAP Business Suite / A1 SAP Business Objects SAP HANA One	○	△
IBM	IBM DB2 and Informix IBM WebSphere IBM Domino,Lotus, Tivoli, etc.	○	○
ORACLE	Oracle Applications Oracle Fusion Middleware Oracle DB 11g	○	△
RedHat	RedHat Enterprise Linux JBOSS Gluster	○	○

amazon web services

ネットワーク構成の検討(1/2)

AWS-既存DC間のネットワーク構成

- Direct Connect or VPN
  - 必要帯域や予算、社内ポリシーに応じて選択
  - DX複数回線、DXとVPNの併用による冗長構成も可能
- インターネット接続経路の設計
  - セキュリティポリシーに応じて設計



ネットワーク構成の検討(2/2)

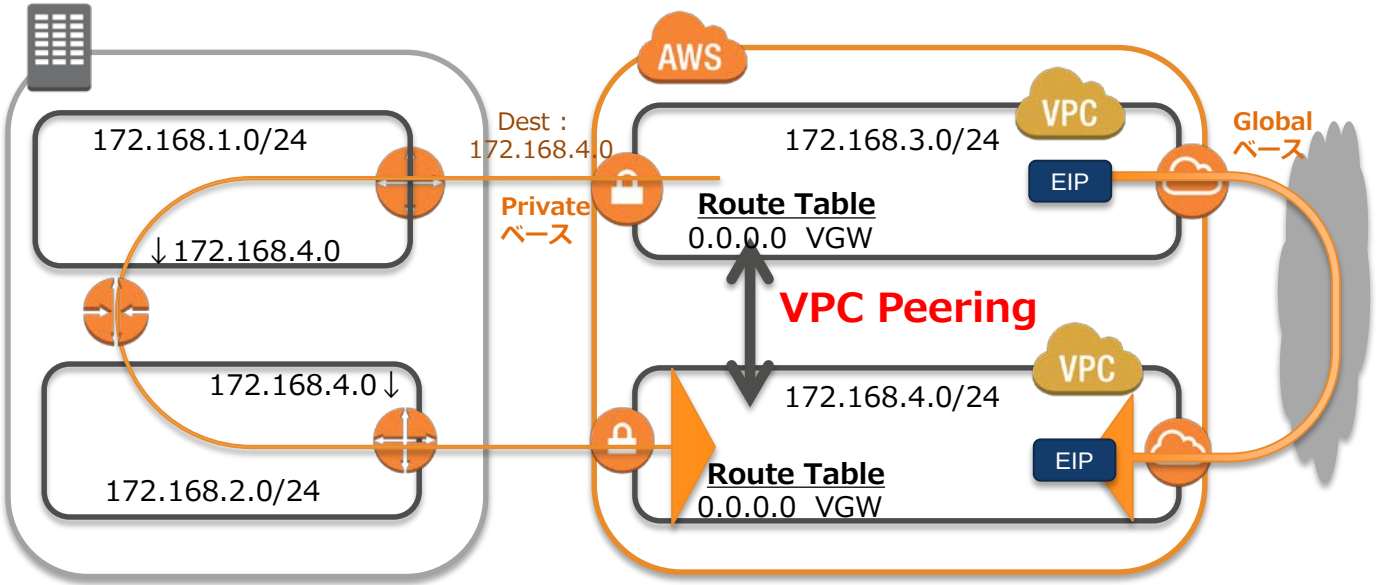
AWS内のネットワーク構成の決定要素

- VPC CIDR / Subnetの設計
- Route Tableの設計
- Internet Gateway(IGW)の配置検討
- Security Groupの設定
- Network Access Control List (NACL)の設定
- Elastic Network Interfaceの設定

VPCを使用することで、AWS上にオンプレミス同様の
ネットワーク環境を作り出すことが可能

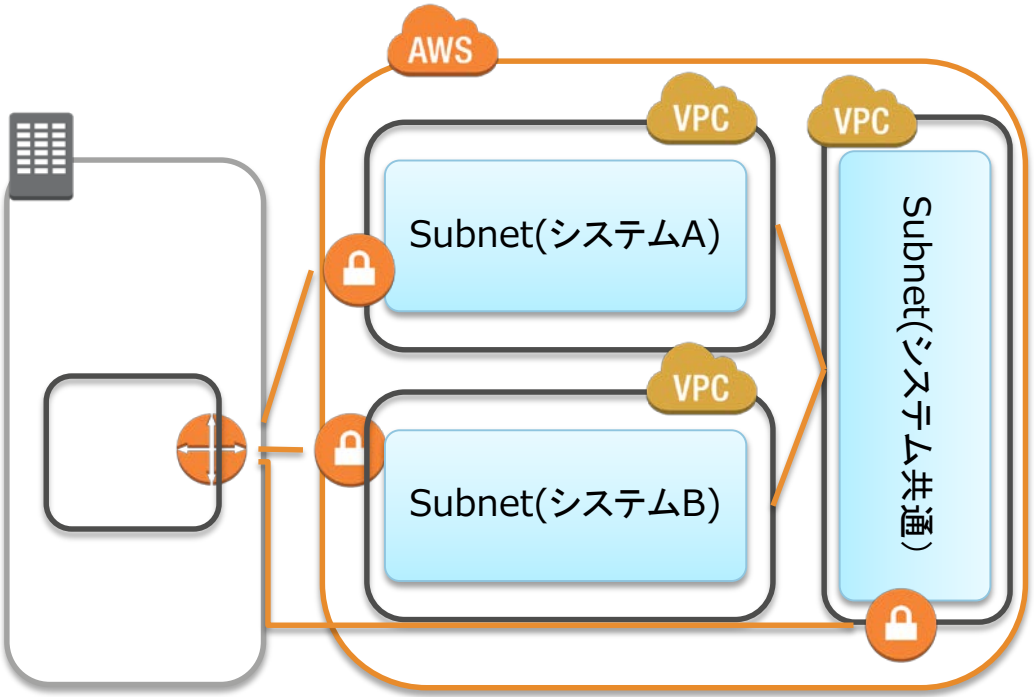
VPCの基本制約

- CIDRは大きめに（サイズ拡張できないため）
- L2延伸は出来ないため、拠点側とVPCはCIDRは重複しないことを推奨
- VPC間は接続可能。ただしCIDRの重複はNG
- 各VPCのCIDRは間接的に通信しない場合、CIDR重複可



amazon web services

VPC設計例: システムごとにVPCを構築



- 利点
  - システムごとに独立してリソースが管理可能
  - AWSアカウントをVPCごとに作成すれば、課金の把握が容易
- 欠点
  - CIDRブロックを多く消費するため、事前設計が必要
  - オンプレミスとVPCを直接つなぎたい場合、VPCの数だけ接続をする必要がある

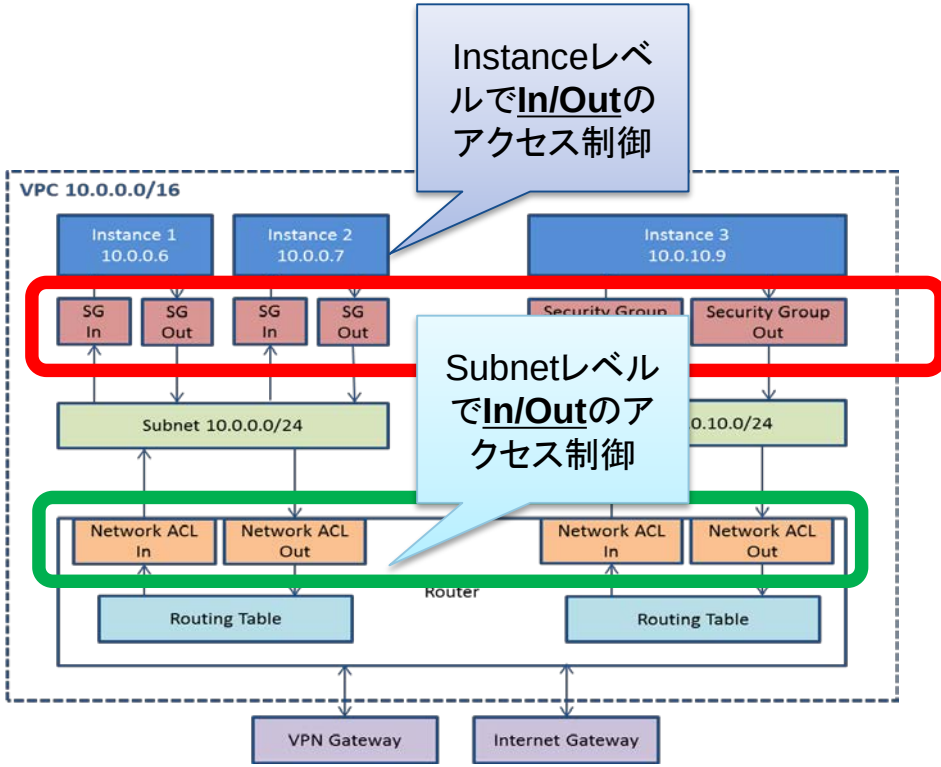
現在はVPC Peeringがサポートされているため、本構成が推奨

Security GroupとNACL(Network Access Control List)

AWSでは以下のファイヤーウォール機能が提供されている

- Security Group
  - インスタンスベースのステートフルなファイヤーウォール
- NACL
  - ネットワークセグメントベースのステートレスなファイヤーウォール

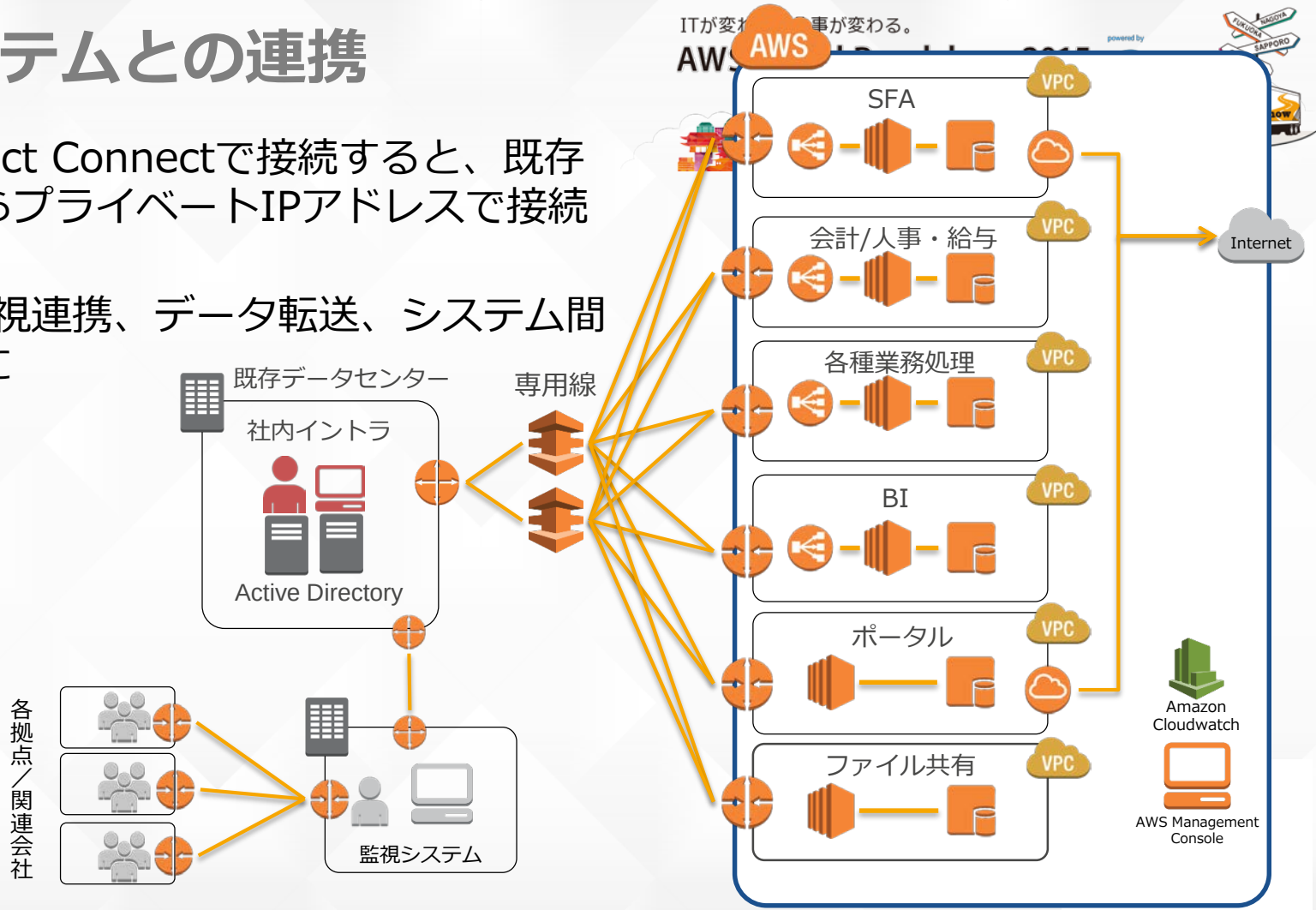
各システムにおける通信要件、セキュリティポリシーに応じてそれぞれを適切に設計、設定する



amazon web services

既存システムとの連携

- VPN or Direct Connectで接続すると、既存システムからプライベートIPアドレスで接続可能
- AD連携、監視連携、データ転送、システム間連携が容易に



システム連携の留意点

- 既存システム/AWS間のネットワークレイテンシー
  - VPNの場合数十ms～　Direct Connectの場合数ms～
  - 例えばオンプレミスのDBにAWS上のEC2から頻繁にアクセスするような場合に注意が必要
- アクセス先IPアドレス
  - オンプレミスのCIDRブロック以外でシステム構築するため、オンプレミスからの通信先が変わる
  - IPアドレスではなく、DNSサーバを使ってホスト名でアクセスする

AWSの運用管理のポイント

- AWSでの運用、監視の変更点

監視

- AWS以外(OS以上)のレイヤー
  - 従来通りの監視
- AWSが提供するレイヤー
  - Cloudwatch、AWS Event等、AWSが提供する機能を活用

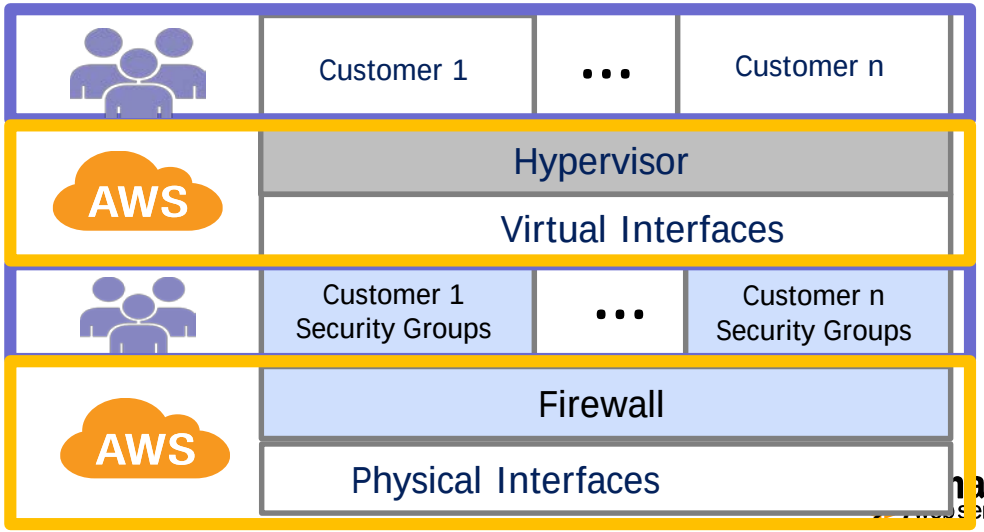
運用

- 基本はセルフサービス
  - AWS提供機能を活用(バックアップ等)
- 自動化にはAWSのAPIを利用
- 既存の運用管理ツールとの連携

AWS環境での運用

- **必要な作業(お客様の管理範囲)**
  - **システム設計・構築**
  - **ネットワークの割り当て**
  - **ネットワーク構築**
  - **システム監視**
  - **障害発生時の復旧作業**
  - **OSより上の作業**
    - **パッチ適用**
    - **セキュリティ設定**
    - **アプリケーション管理**
    - **バックアップ**

- 必要でない作業(AWSの管理範囲)
  - ハードウェア調達
  - ハードウェアのセットアップ
  - ハード故障時の交換
  - ハイパーバイザーのメンテナンス



運用範囲の変更点

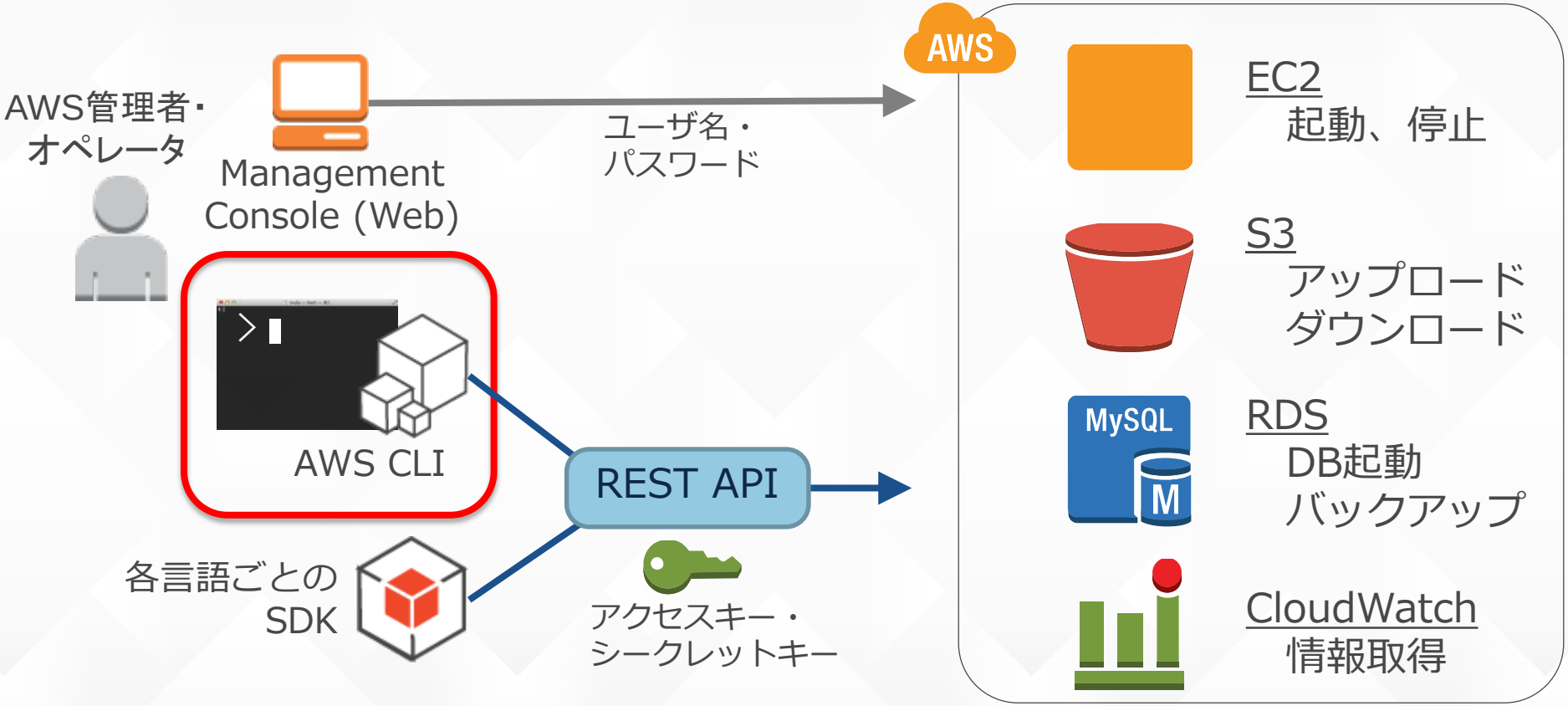
・OSより上位レイヤーは既存から変更なし
・既存の運用管理の仕組みを流用可能

	レイヤー	オンプレ/仮想化	AWS
ソフトウェア	アプリケーション	変わらない サーバ管理はRDP/SSH等でOSへログイン （＝オンプレDCとAWSでOS以上の運用は同じ）	
	ミドルウェア		
	OS		
	仮想化（サーバ）	サーバ＋仮想化ソフト	EC2
	仮想化（ストレージ）	Storage+仮想化ソフト	EBS
	仮想化（ネットワーク）	N/W機器＋仮想化ソフト	VPC
ハードウェア	バックアップストレージ	機種ごとの管理が必要	S3
	負荷分散装置	機種ごとの管理が必要	ELB
	ネットワーク（WAN）	不要	Direct Connect業者に委託 (AWS側回線の管理は不要
	物理ネットワーク（LAN）	機種ごとの管理が必要	不要 ネットワーク設計のみ
	物理ストレージ	機種ごとの管理が必要	
	物理サーバ	機種ごとの管理が必要	
	データセンター	貴社委託先DC	

採用技術毎に異なる管理

AWSにより標準化された管理

AWSの管理方法



AWS環境の監視方法(EC2/EBS/etc...)

- アプリ性能/死活監視
- リソース監視
- 死活監視
  (ログ,プロセス,OS)

- Service Status監視
- リソース監視
- Event監視

アプリチェック

Agent経由等の
情報収集

**CloudWatch/
API/SDK**

Alarm

amazon
web services

AWS環境の監視方法(マネージドサービス)

- アプリ性能/死活監視

アプリチェック

Application

CloudWatch/
API/SDK

Alarm

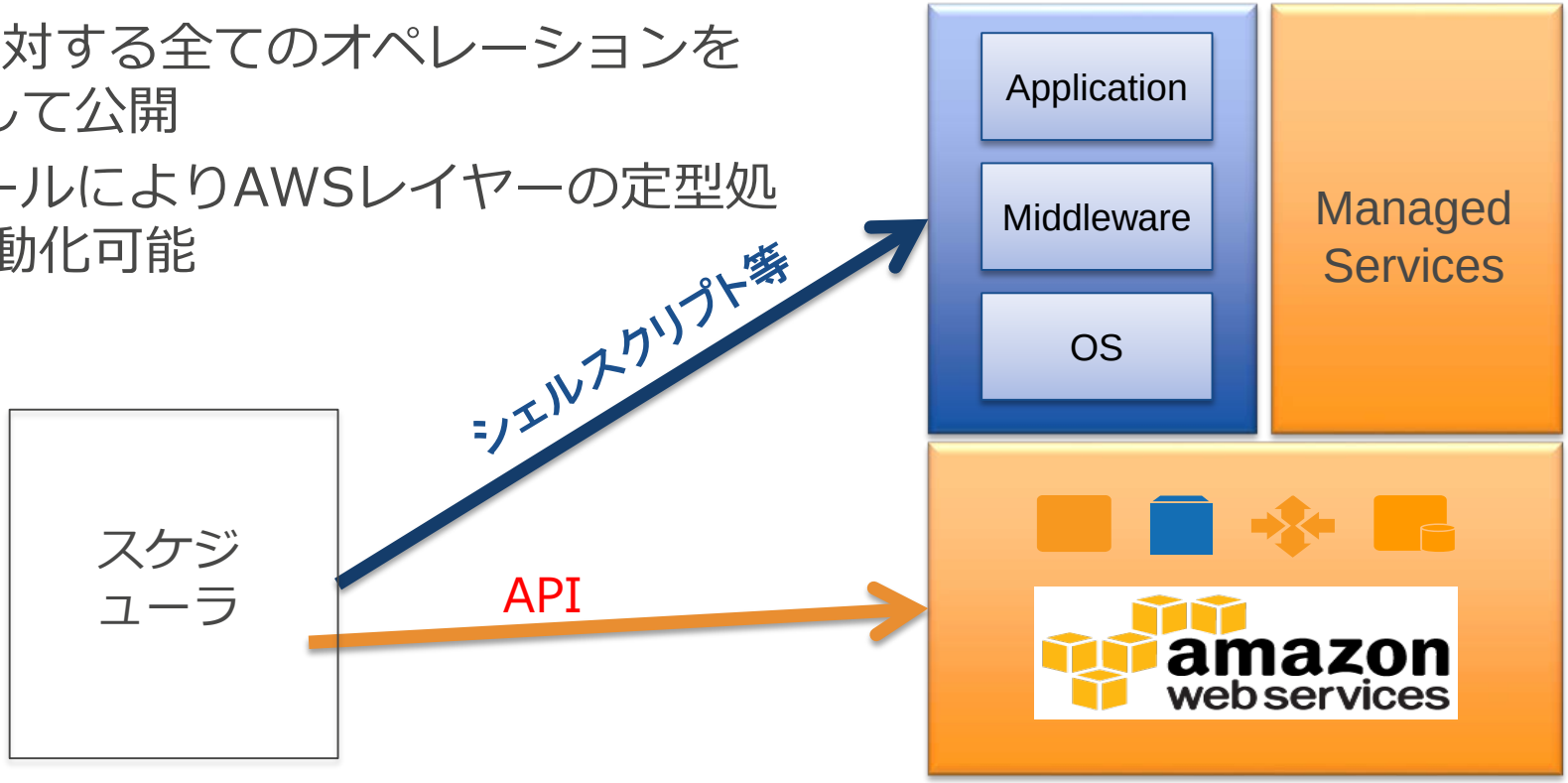
- Service Status監視
- リソース監視
- Event監視

AWSの監視項目一覧

- Service Status監視 (API/SDK/CloudWatch)
  - サービスのステータスを確認
  - ステータスが正常でない場合は再起動などの対策を実施
- Event監視 (API/SDK)
  - 不定期に発生するメンテナンスに関する情報を取得
  - 関連するサービスに関しては事前に再起動などの対策を実施
- リソース監視 (CloudWatch/API/SDK)
  - ハイパーバイザーからのリソース情報を取得
  - 使用状況を確認し、必要に応じてリソース量を増減する
- AWS Service Health Dashboard確認
  - Service Health Dashboardでサービスステータスを確認
  - http://status.aws.amazon.com/

AWS環境の自動化

- AWSに対する全てのオペレーションをAPIとして公開
- APIコールによりAWSレイヤーの定型処理を自動化可能



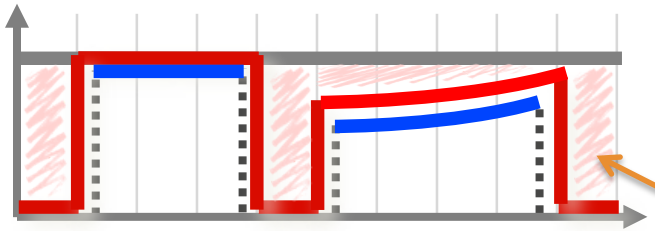
まとめ

amazon web services

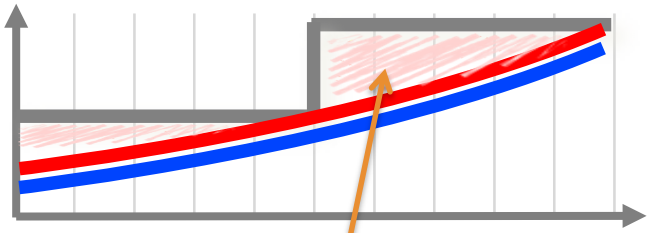
実需に合わせた柔軟なキャパシティ対応

コスト

- AWSでは実際の需要に合わせた柔軟なシステム構成を取る事により投資を最適化



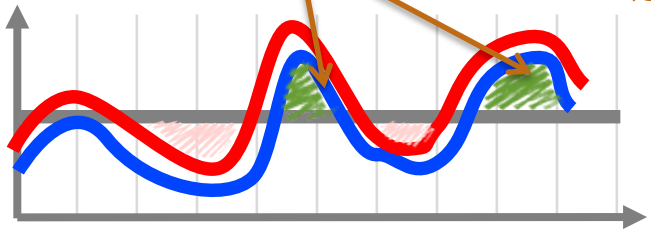
オンとオフ



ニーズの増加への対応

キャパシティ不足

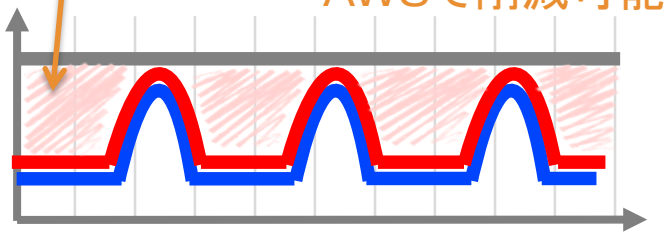
=AWSで適正化



予測できないピーク

過剰なキャパシティ

=AWSで削減可能なコスト



予測可能なピーク

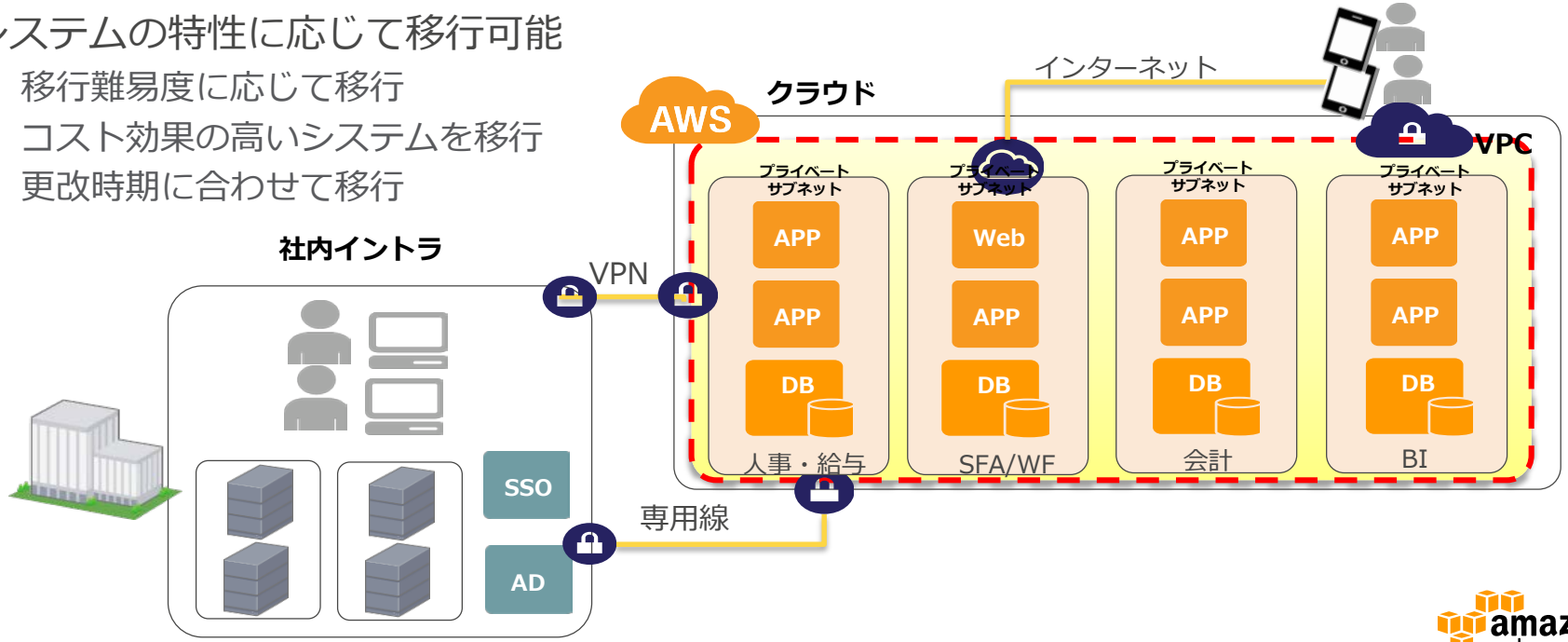
キャパシティの需要　オンプレミス環境　AWS環境

AWSへ移行するメリット

ハイブリッド

- オンプレミスとAWSのハイブリッド構成が可能
  - 既存DCの延長としてAWSを利用
    - 既存資産を有効活用
  - システムの特性に応じて移行可能
    - 移行難易度に応じて移行
    - コスト効果の高いシステムを移行
    - 更改時期に合わせて移行

✓周辺システムから基幹システムへ
✓既存資産とクラウドを最大活用



amazon web services

ビッグデータ・プラットフォームとしてのAWS

ビッグデータ/BCP

- DWH、ストリーミング等、様々なビッグデータ関連サービスを提供
  - 初期投資不要、低額な従量課金で利用可能
  - スケーラブル

Small Start/Try&Errorが可能
ビジネス要件に合わせて必要なだけスケール

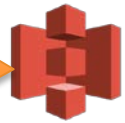
収集

Amazon Kinesis

大量データのストリーミング処理

保存

容量無制限のインターネットストレージ



Amazon S3

Amazon DynamoDB

高信頼かつスケーラブルなNoSQL

Amazon RDS

フルマネージドRDBMS

解析

Amazon EMR

フルマネージドHadoopクラスタ

Amazon Redshift

ペタバイト級のデータウェアハウス

可視化

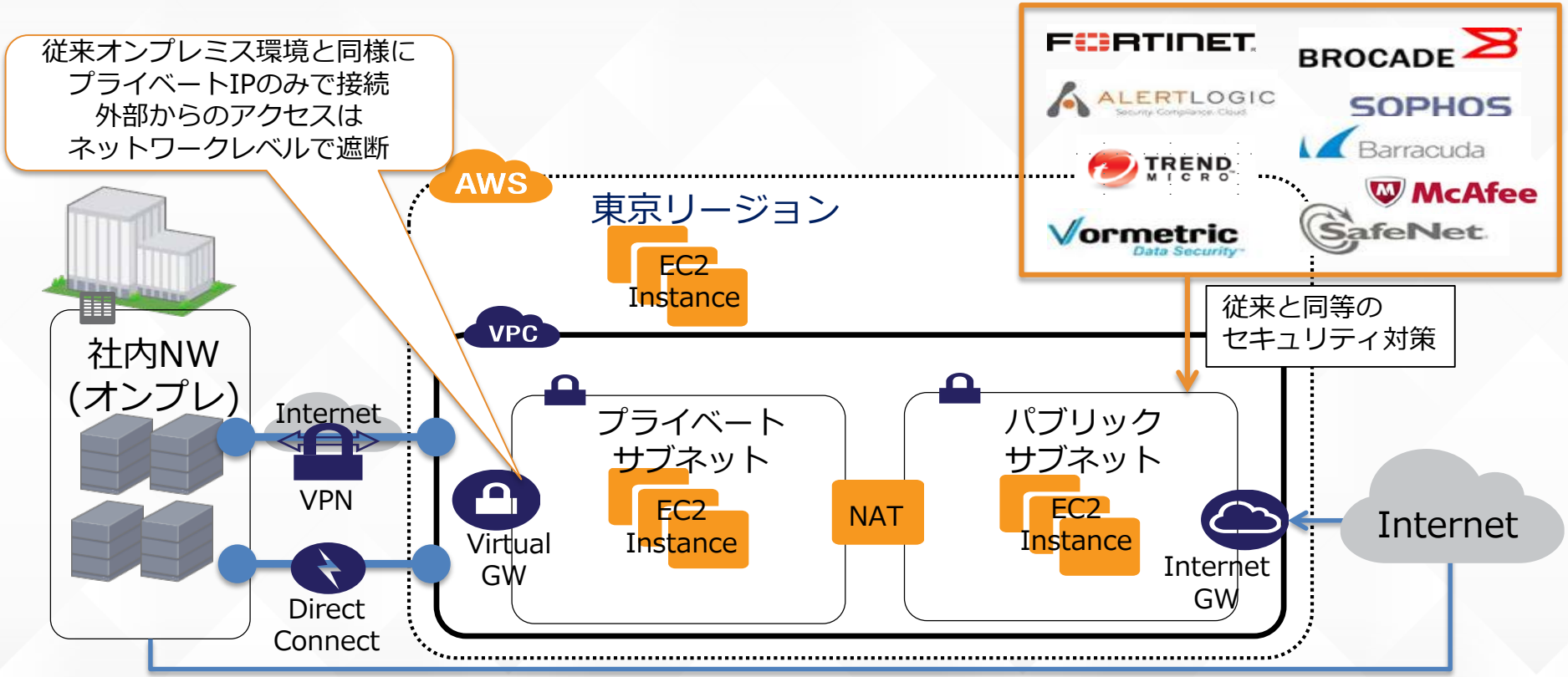
BI Tools
or
Custom App

Amazon EC2

オンデマンドなコンピュートリソース

オンプレミスと同等以上の環境を構築可能

セキュリティ



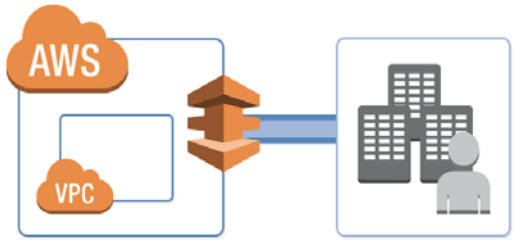
amazon web services

AWS専用線アクセス体験ラボ sponsored by Intel

■オンプレミスとAWSとの接続を検証してみたい
■フェイルオーバー時の動作を確認したい
■スループットがどれだけなのか実際に試してみたい
■自前のルータがDirect Connectに接続できるか確認したい

・・・などなど

AWS専用線アクセス体験ラボ
sponsored by Intel®



http://aws.amazon.com/jp/dx_labo/

amazon web services

AWSプロフェッショナルサービスによるご支援

- AWSを利用したシステムのアーキテクチャ設計と実装のご支援、スキルトランスファを行います

お客様の計画の様々なフェーズにおいてご支援を提案させていただきます。

amazon web services

サポートについて

- AWSでは日本語でのサポートを提供
  - エンタープライズ環境ではビジネス以上を推奨
    http://aws.amazon.com/jp/premiumsupport/

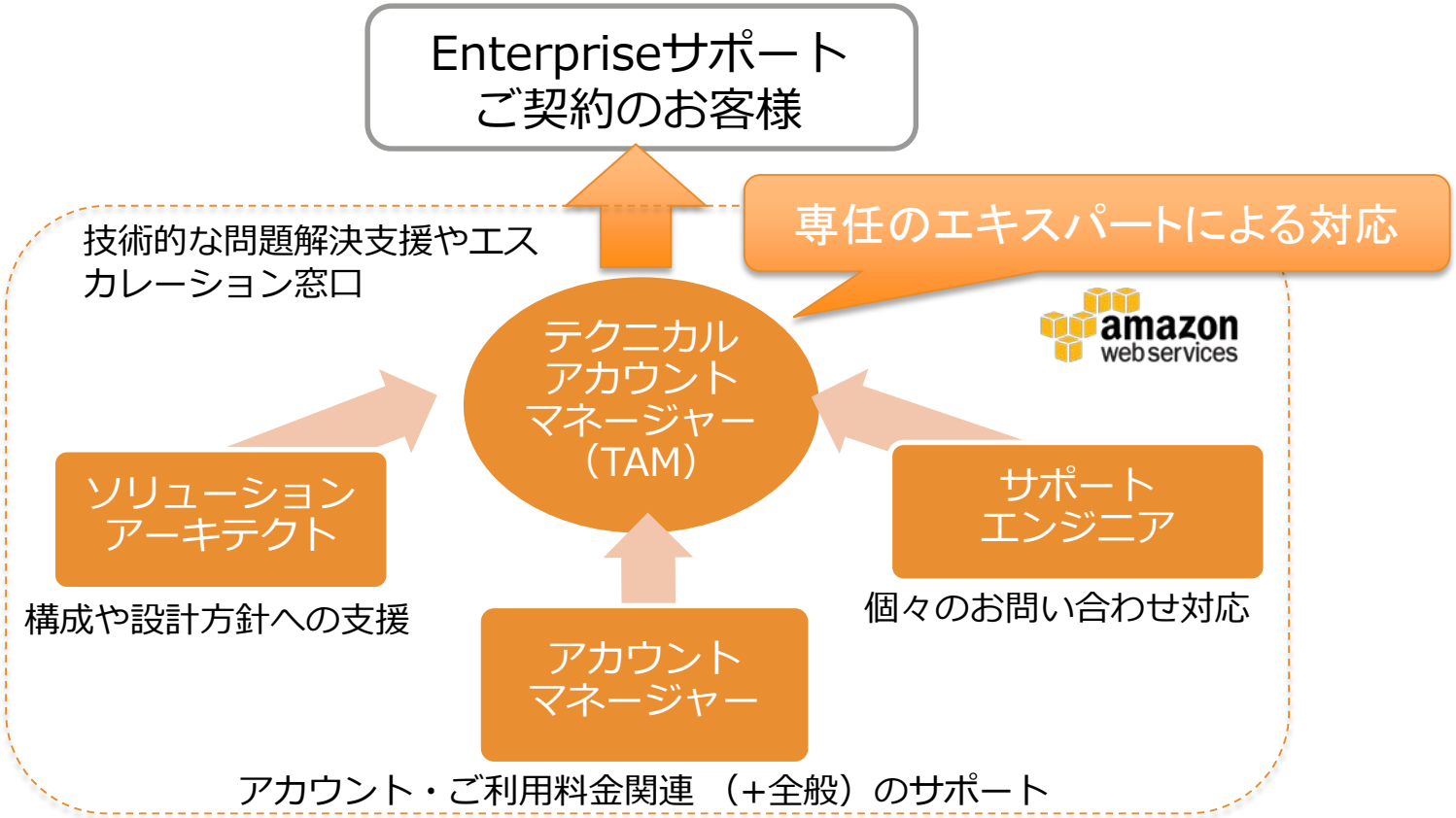
AWS サポート は、AWS の製品やサービスの開発時および実運用時の問題をカバーするのに加えて、他の主要スタックコンポーネントについても対応します。

- AWS サービスや機能に関する「操作手順」の質問
- クラウドでアプリケーションをうまく統合、デプロイ、そして管理するためのベストプラクティス
- API と AWS SDK の問題のトラブルシューティング
- AWS のリソースに関する操作または体系の問題のトラブルシューティング
- 当社の Management Console や他の AWS ツールの問題
- 健全性チェックで検出された問題
- 多数のサードパーティ製アプリケーション（例: OS、ウェブサーバー、E メール、データベース、ストレージ構成）

	ベーシック	デベロッパー	ビジネス	エンタープライズ
サポートフォーラム	利用可能	利用可能	利用可能	利用可能
サポートへのコンタクト	EC2の健全性エラーが発生した場合	コンタクトフォーム	電話、チャット、コンタクトフォーム	電話、チャット、コンタクトフォーム
最速初回応答時間	不可	12時間以内（営業時間内）	1時間以内	１５分以内
連絡先登録		1	5	無制限
24/365対応	なし	なし	あり	あり
上級サポートエンジニアへの直接ルーティング	なし	なし	あり	あり
専任スタッフ	なし	なし	なし	あり
特別サポート	なし	なし	なし	あり
料金（月額）	無料	4,900円	AWS利用総額の 0円~120万円: 10% 120万円~840万円: 7% 840万円~3,000万円: 5% 3,000万円~ 3% （最低12,000円）	AWS利用総額の 0円~1,800万: 10% 1,800万~6,000万: 7% 6,000万~12,000万: 5% 12,000万~ 3% （最低150万円）

※1ドル120円換算

エンタープライズサポートご支援体制



amazon
web services

amazon web services

amazon web services

Thank You