AWS
Black Belt
Online Seminar

【AWS Black Belt Online Seminar】
失敗例を成功に変えるAWSアンチパターン

アマゾン ウェブ サービス ジャパン株式会社
荒木靖宏

2018/05/22

内容についての注意点

- 本資料では2018年05月22日時点のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(http://aws.amazon.com)にてご確認ください

- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます

- 価格は税抜表記となっています。日本居住者のお客様が東京リージョンを使用する場合、別途消費税をご請求させていただきます

AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at http://aws.amazon.com/agreement/. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

自己紹介

名前

- 荒木 靖宏

所属

- アマゾンウェブサービスジャパン株式会社
- 技術統括本部 シニアマネージャー
  プリンシパルソリューションアーキテクト

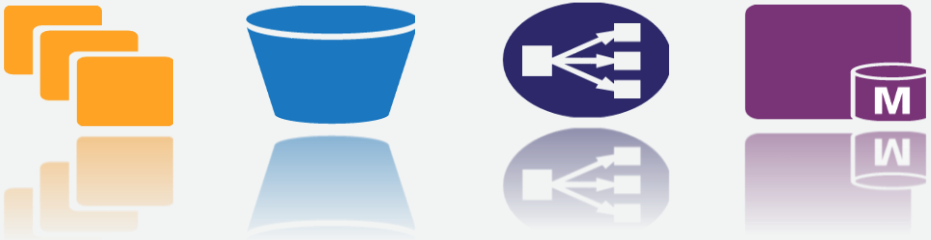
好きなAWSサービス

- Amazon Virtual Private Cloud
- AWS Direct Connect

アンチパターンの前に

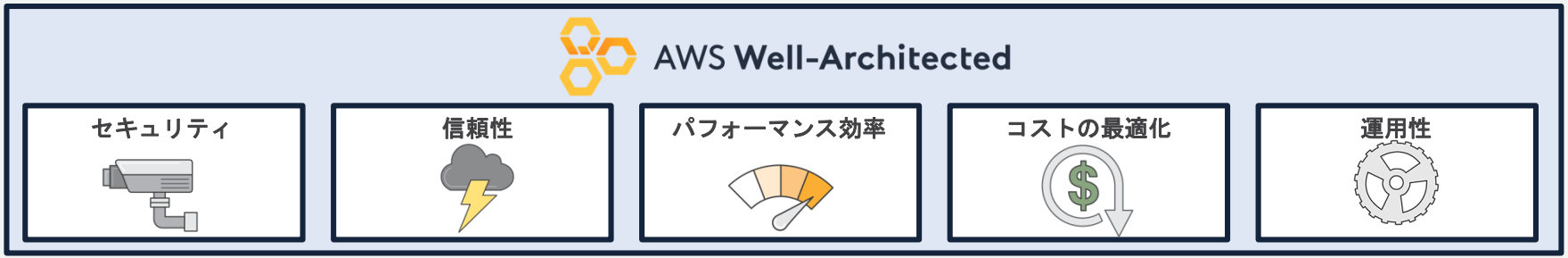
AWSクラウドデザインパターンとは…

AWSクラウドを使ったシステムアーキテクチャ設計を行う際に発生する、典型的な問題とそれに対する解決策・設計方法を、分かりやすく分類して、ノウハウとして利用できるように整理したもの。



AWS Well-Architected Frameworkとは？

- AWSが、 10年以上に渡って、様々な業種業界、数多くのお客様のアーキテクチャ設計および検証をお手伝いしてきた経験から作成した、**クラウド設計、構築、運用のベストプラクティス集**
- クラウドでの設計原則と**セキュリティ、信頼性、パフォーマンス効率、コストの最適化、運用性**についてのベストプラクティスが質問形式で記載されています



アンチパターンの紹介

これまで、数多くのAWS成功例がうまれていった。。

その成功例は「パターン」として受け継がれ。。

そして、それらは時に「秘伝のたれ」「さわってはいけないもの」とされてきた。。

アンチパターン

失敗に陥るパターンを類型化し、事例の早期発見と対応策に関しての提案を目的とする

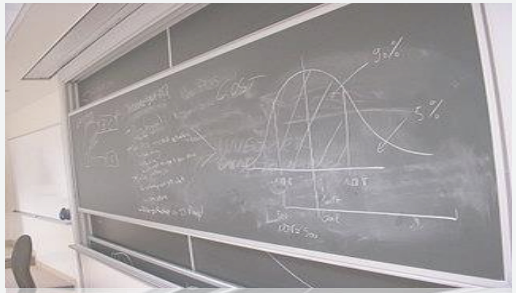
動作やプロセス、構造について、**当初は妥当であったのに**、最終的に悪い結果が繰り返されるパターン

リファクタリングするための方法が存在するパターン

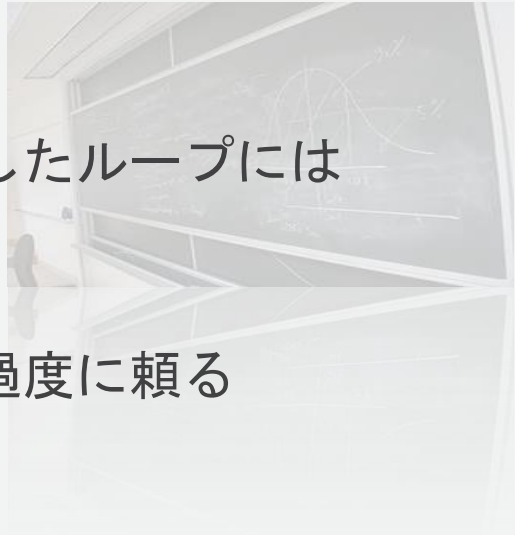
おぼえていただきたい、
タイミング別の「メタ」アンチパターン

机上の空論アンチパターン
塩漬けアンチパターン
ノーコスト最適化アンチパターン

机上の空論アンチパターン



机上の空論アンチパターン



原因

- サーバ発注、システムデプロイ、納品の硬直したループにはまっている
- （最初から）完璧を求めすぎる
- カタログスペックやマイクロベンチマークに過度に頼る

症状：利用前に発生する

- 動作確認をしない
- 事前のキャパシティプランニングに時間をかけすぎる

机上の空論アンチパターン

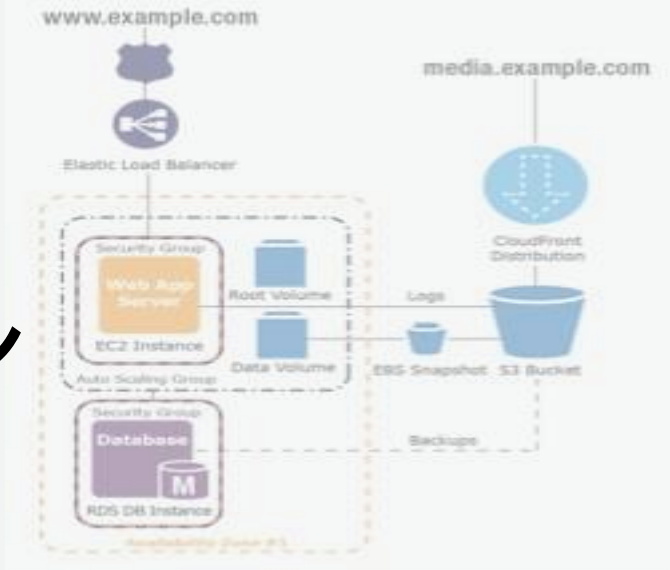
解決法

- まずは小さくても試してみること

備考

- 塩漬け＆ノーコスト最適化と結びつくと最悪の結果に

塩漬けアンチパターン



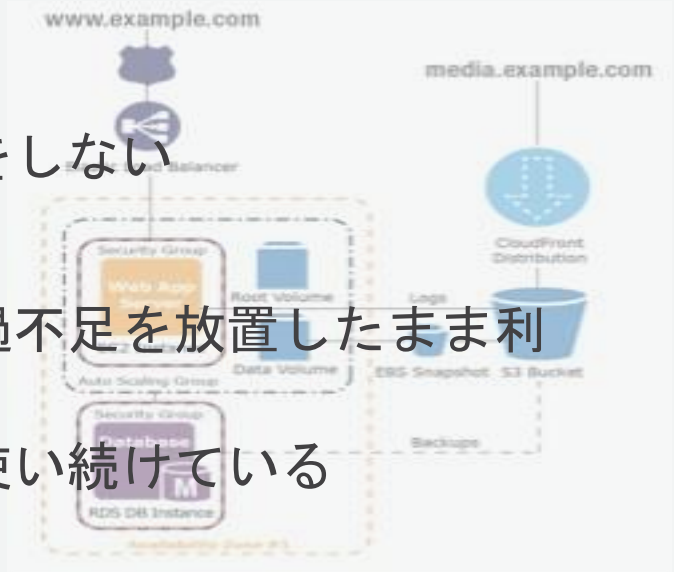
塩漬けアンチパターン

原因

- 構築した当初のままインフラの見直しをしない

症状

- 実際の利用にくらべてキャパシティの過不足を放置したまま利用している
- 一時凌ぎで選んだサービスをそのまま使い続けている



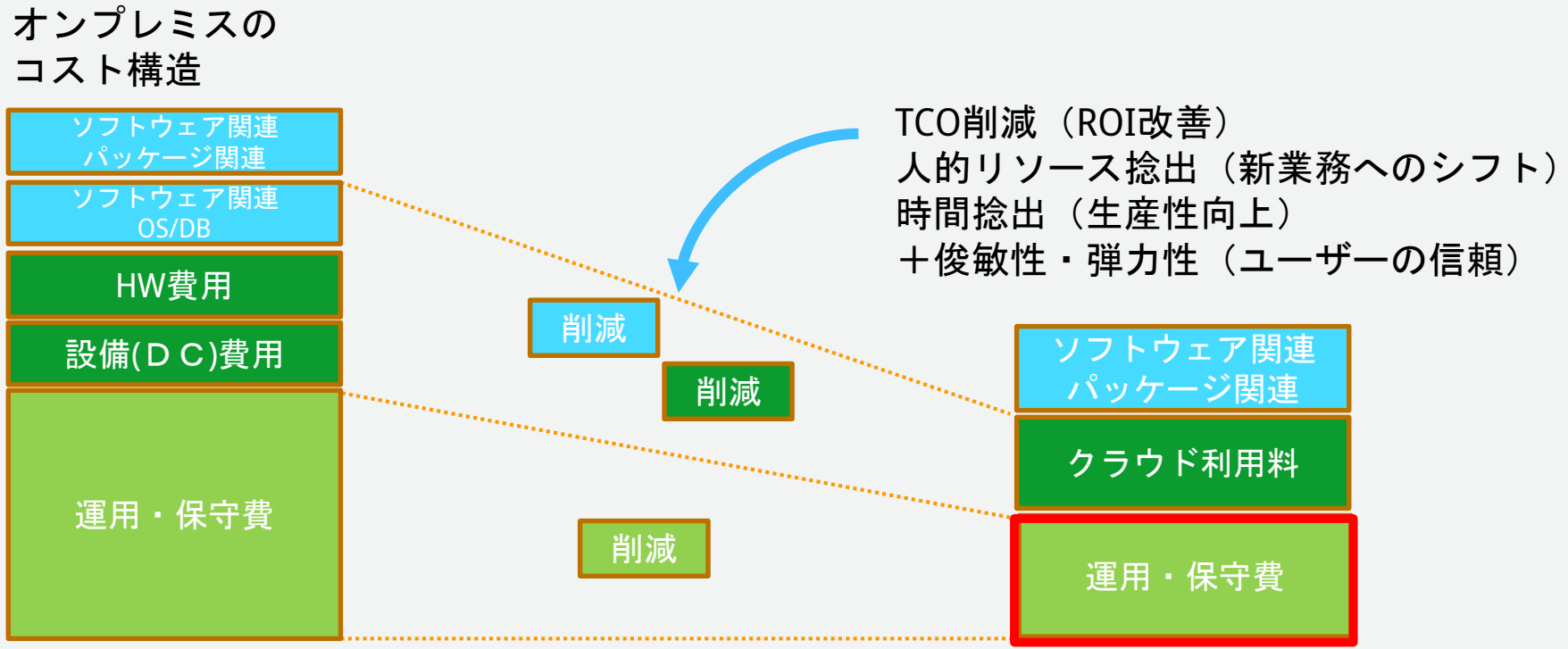
オンプレミス vs EC2+ミドルウェア vs マネージドサービス

お客様がご担当する作業

AWSが提供するマネージド機能

aws

クラウド化に伴うコスト低減イメージ



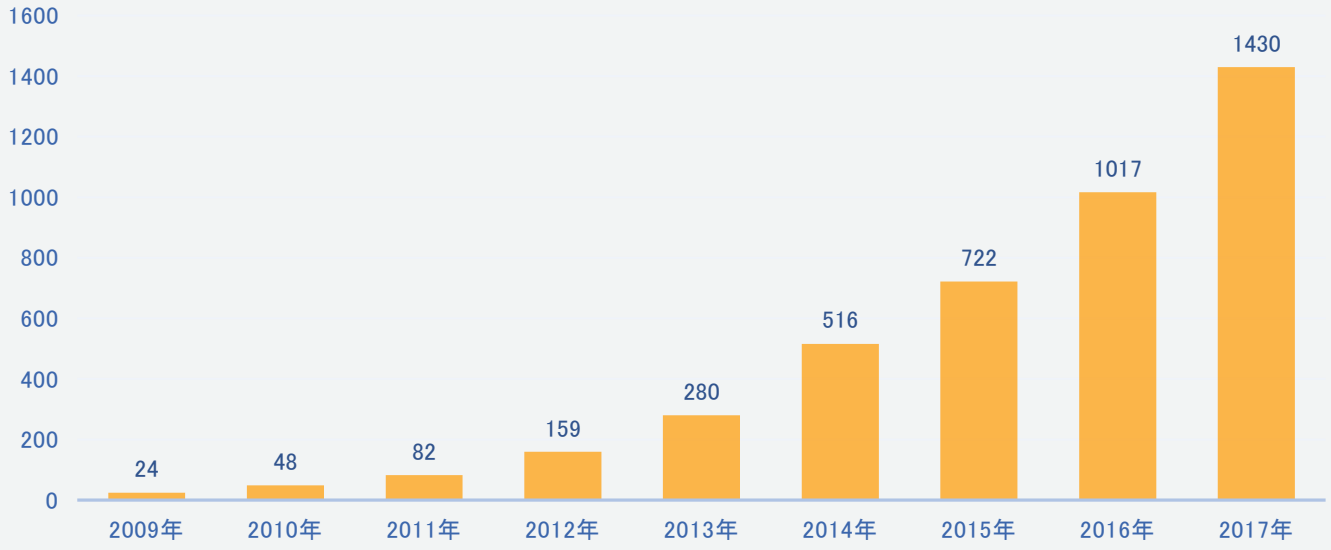
IT関連コストに占める運用管理コストは40%～50%

運用・保守費用の大きな低減が期待できる

機能追加/改善

継続的に新サービス、新機能をリリース

- 機能追加はAWSが実施
- 基盤への適用、バージョンアップ費用が不要

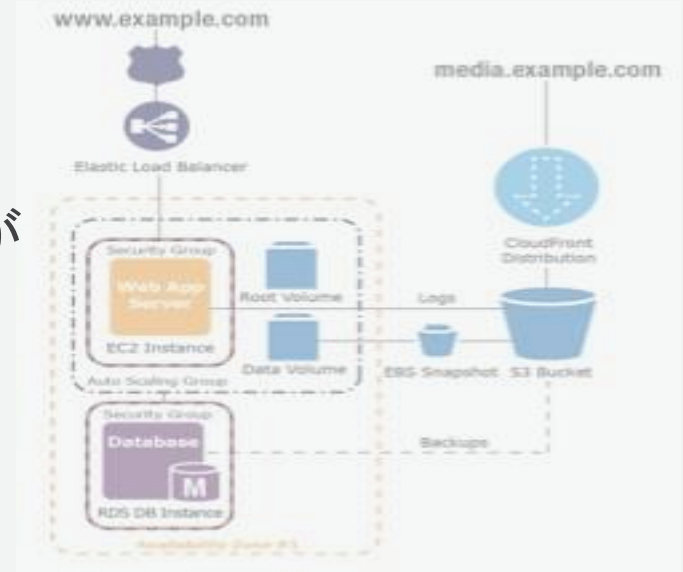


その年にリリースされた機能改善、新機能、サービスの数

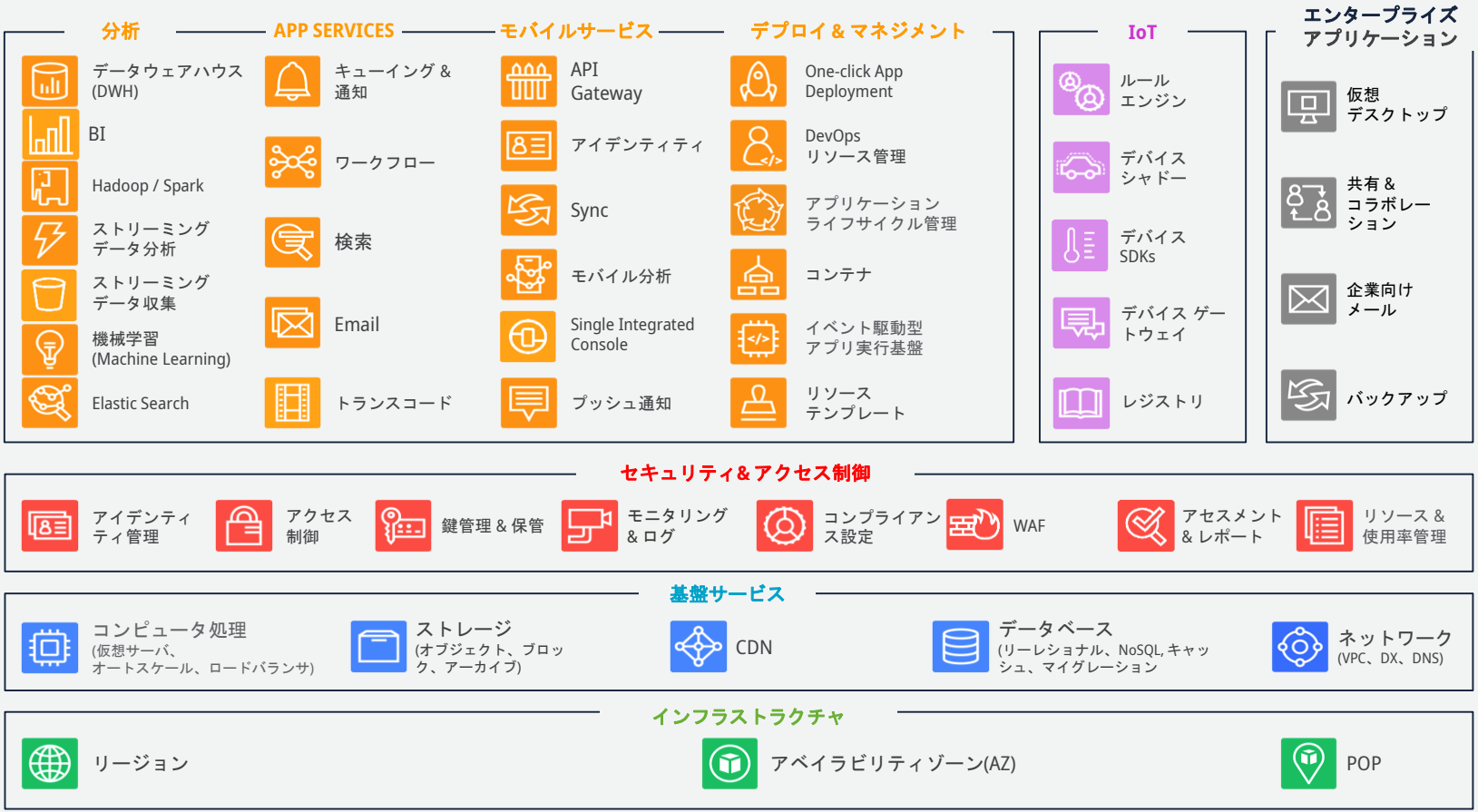
塩漬けアンチパターン

解決法

- サービスは定期的に見直す
- 新サービスや新機能が助けになることが



AWSの豊富なサービス群(100を超えるサービス)



セキュリティ向上を手助けするサービス その1

Service	Type	Use cases
Cloud Trail	APIログの取得	AWS環境の操作に関するログの取得
Cloud Watch	リソース・ログ監視	AWSサービスのリソース監視と各種ログの収集・モニタリング
AWS Config	変更管理	AWSサービスの変更記録とトラッキング
Amazon Inspector	オンデマンドの評価	EC2インスタンス内の導入されるOS・アプリケーションのセキュリティ分析
Config Rules	継続的な評価	変更による誤設定検知、ベストプラクティスの維持、脆弱性の検知
Trusted Advisor	定期的な評価	コスト、パフォーマンス、信頼性、セキュリティの観点からの広範な調査

AWS Security and Compliance

お客様のセキュリティ向上をサポートするサービス群

AWSの責任で統制

セキュリティ向上を手助けするサービス その2

Service	Type	Use cases
AWS IAM	認証・認可	AWS環境への認証・認可、アクセス権限管理
Amazon Guard Duty	脅威検知	機械学習による脅威リスク、異常検知
AWS Shield	ネットワーク防御	L3、L4を標的としたDDoS防御
AWS WAF	アプリケーション防御	SQL Injection、XSS等の悪意ある攻撃の防御
Amazon Macie	データ保護	機械学習による機密情報の検出、分類、データ漏えいの監視
AWS KMS	データ保護	データ暗号化に必要な暗号鍵の作成、管理、運用

AWS Security and Compliance

お客様のセキュリティ向上をサポートするサービス群

AWSの責任で統制

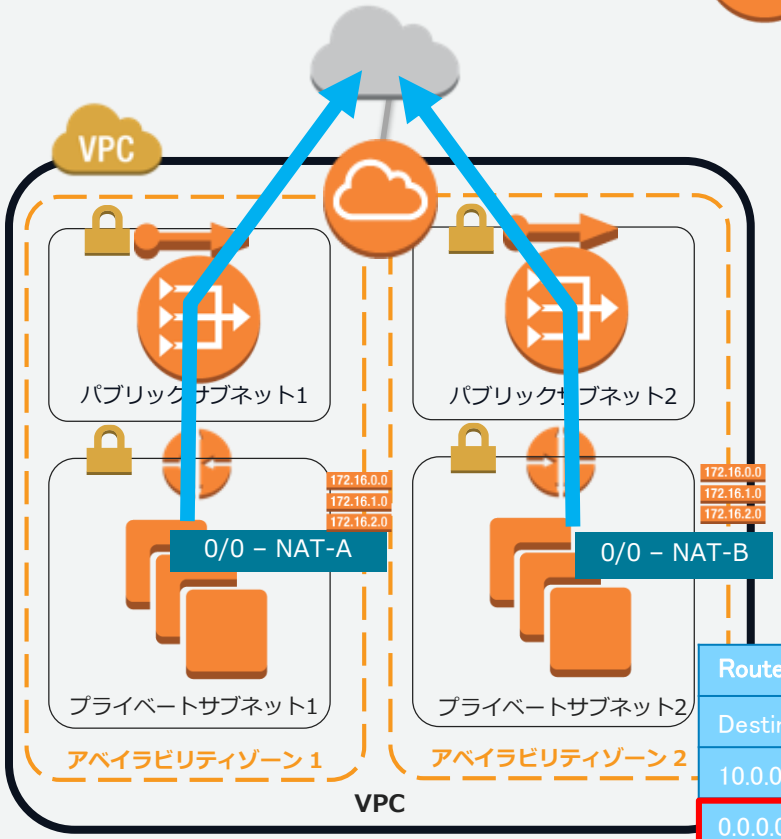
サービスアップデートにより アンチパターンとなったパターンの紹介

aws

塗り替えたパターンの例

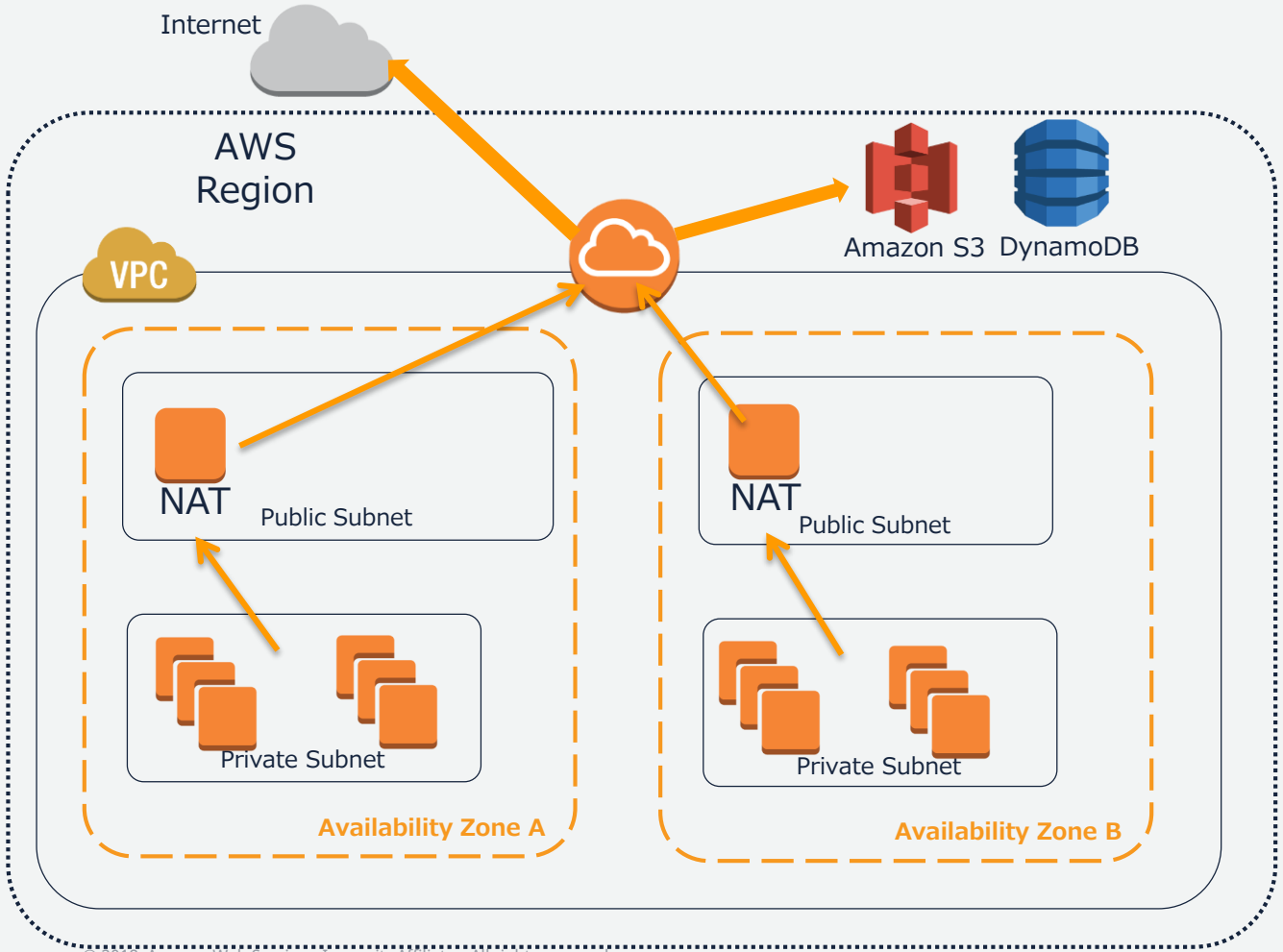
これまでのパターン	これからのサービス
NATインスタンスの高可用化	NAT Gateway
NATインスタンスのオートスケール	
VPC Peeringを使ったSaaS提供	PrivateLink for Customer and Partners
NTPサーバの参照	Amazon NTP
WAFアプライアンス on EC2 w/ ELB	AWS WAF

NATゲートウェイ



Route Table	
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	NATゲートウェイ

- AWSによるマネージドNATサービス
- プライベートサブネットのリソースがインターネットまたはAWSクラウドへ通信するために必要
- EIPの割当て可能
- 高パフォーマンス(最大10Gbpsバースト)
- 高可用性(ビルトインで冗長化)
- アベイラビリティゾーン毎に設置するのがベストプラクティス

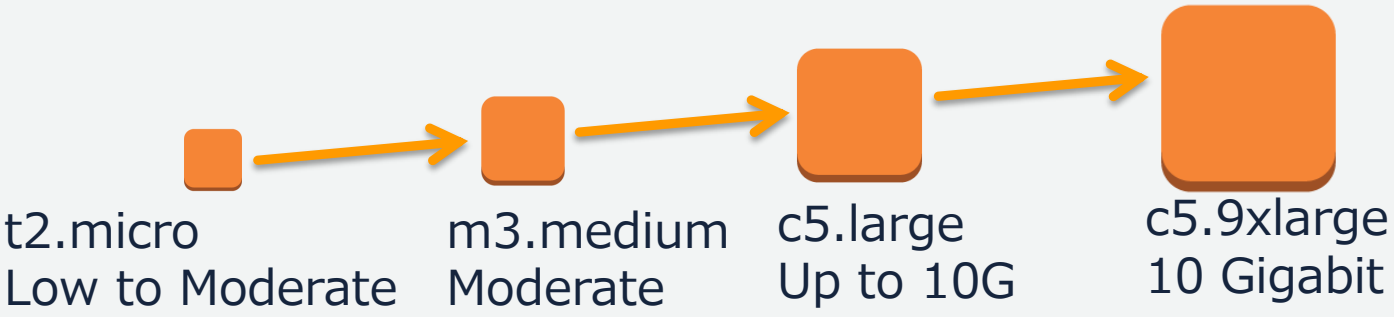


HA NAT

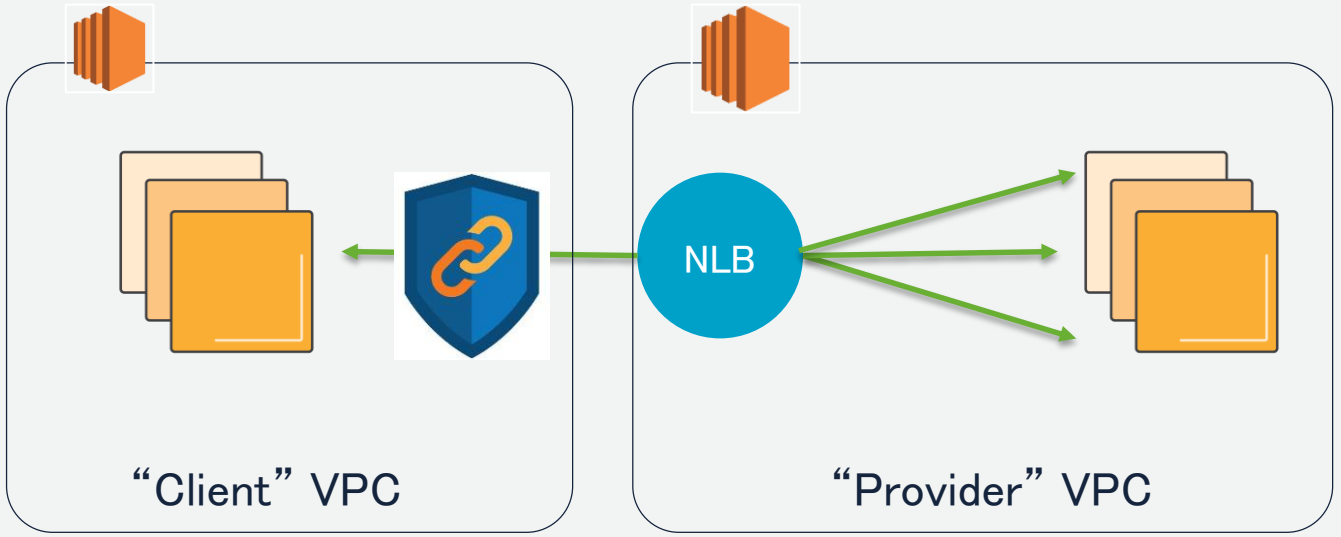
- NATインスタンスにオートスケールを設定（min=1,max=1）し、AZ毎に1NAT
- プライベートサブネットのルートテーブルは同じAZのNATにむける

Auto Scale NAT

AZ毎にHA NATを配置する
スケールアップ！
ネットワーク関連メトリクスを見る
プロトコル別アプリケーションプロキシも有効



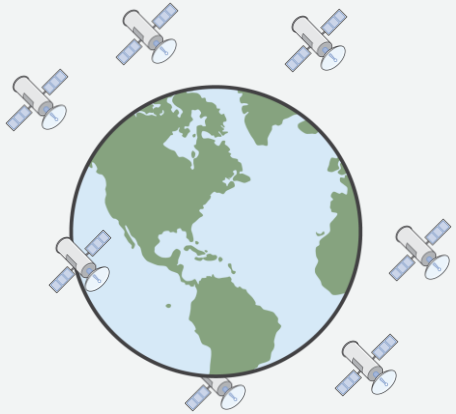
PrivateLink for Customers and Partners



VPC peeringよりもシンプルなサービス接続

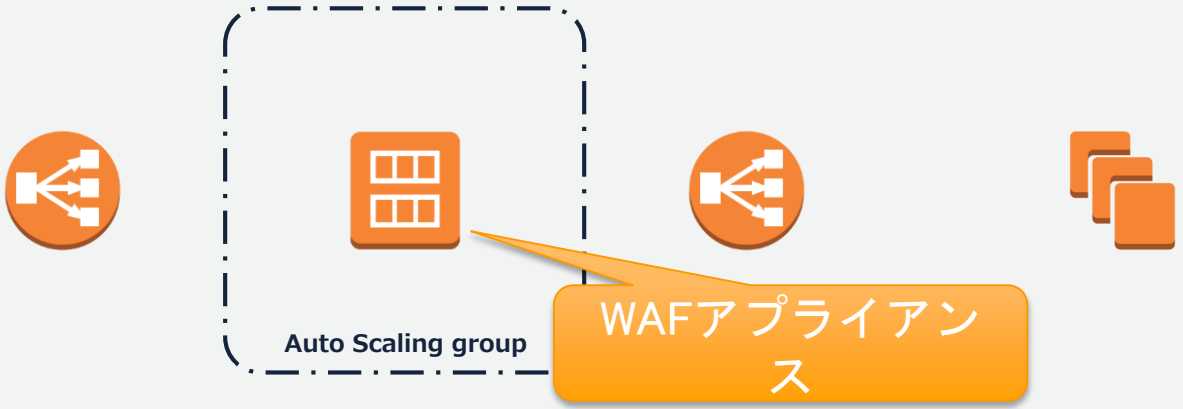
Amazon Time Sync Service

- VPC内で稼働する全てのインスタンスからNTPで利用できる高精度な時刻同期サービス
- EC2インスタンス内でNTPサーバのIPアドレスとしてとして169.254.169.123を設定するだけで利用できる
  - このアドレスはリンクローカルアドレスなので、外部インターネットへのアクセスは不要。プライベートサブネット内でも利用できる
- Leap Smearingによる「うるう秒」への対策が実装済み
- 無料で全リージョンで利用可能



ELB sandwich for WAF appliance

Auto scaleに対応していないWAFアプライアンスをELBで挟んで機能を補う



ノーコスト最適化アンチパターン

ノーコスト最適化アンチパターン

原因

- 既存構成を変更できないので何もしない

症状

- 利用額の高止まり
- 不必要なリソースの放置、不正利用
- クレジットカード与信額のつかいきり

AWSのコスト最適化

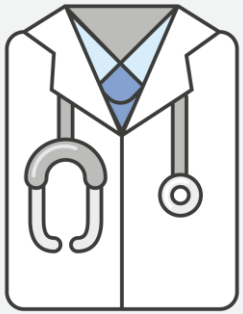
		効果	構成
クラウドネイティブアーキテクチャ	マネージドサービスの活用 インスタンス台数/タイプの最適化 スポットインスタンスの活用 運用自動化 ストレージタイプの最適化	**非常に大きい**	**変更必要**
割引オプションの活用	リザーブドインスタンス CloudFrontリザーブドキャパシティ DynamoDBリザーブドキャパシティ	**大きい**	**変更不要**
細かいリソースの無駄チェック	EBS, Snapshot, EIP等々…	**小さい**	**変更不要**

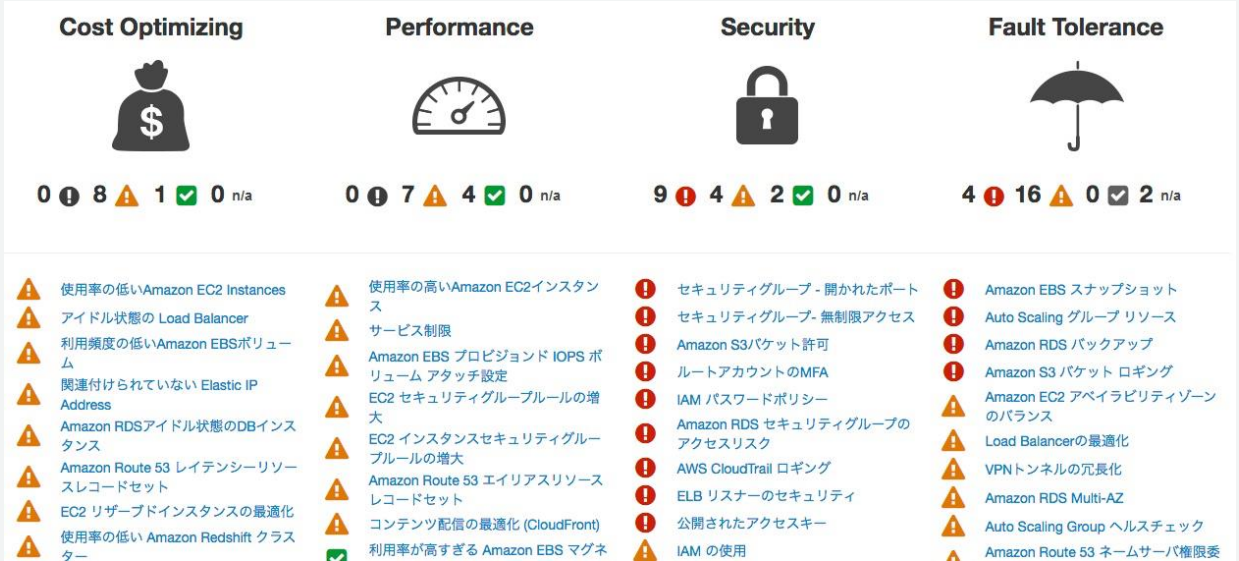
aws

Trusted Advisor(TA)の活用

ご利用実績を元に、自動的にコスト最適化提案をするツール

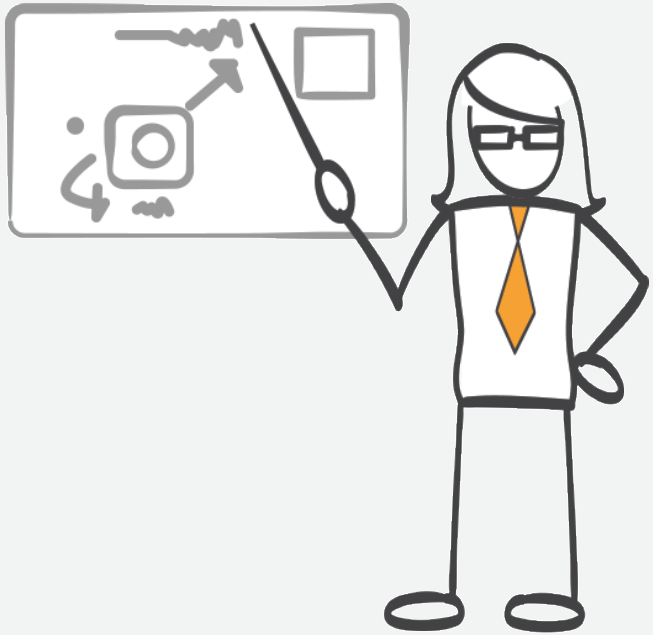
- ご利用にはAWSサポート(ビジネス)が必要
- 使用率の低いEC2, 利用頻度の低いEBS, 関連付けれれていないEIPなどを指摘





詳細は
「AWS Black Belt Online Seminar 2017 AWS のコスト最適化 リザーブドインスタンス」

観測例



観測例：DBの使い分け

状況

- RedShiftを採用したDWHがいつのまにか、パフォーマンスが高いDBと聞いて、並列度の高いSQLアクセス用途（OLTP）に使われるようになる

症状

- 「パフォーマンスが悪い」

解決法

- DBの特性を理解する
- 使ってみて気がついたら構成を見直す

Redshiftが向く用途

特化型のデータベースのため、適した用途に使うことでパフォーマンスを発揮

Redshiftに向くワークロード

- 巨大なデータ・セット（数百GB～ペタバイト）
- １つ１つのSQLが複雑だが、同時実行SQLは少ない
- データの更新は一括導入

ユースケース

- データウェアハウス（DWH）
- ユーザがクエリーを作成する（自由クエリー）（BI等）

Redshiftの特徴を生かせないユースケース

SQLの並列実行数が多い（※同時接続数ではなく同時実行数）
- RDS（MySQL ,PostgreSQL, Oracle, SQL Server)を検討

極めて短いレーテンシが必要なケース
- ElastiCache (インメモリDB)やRDSを検討

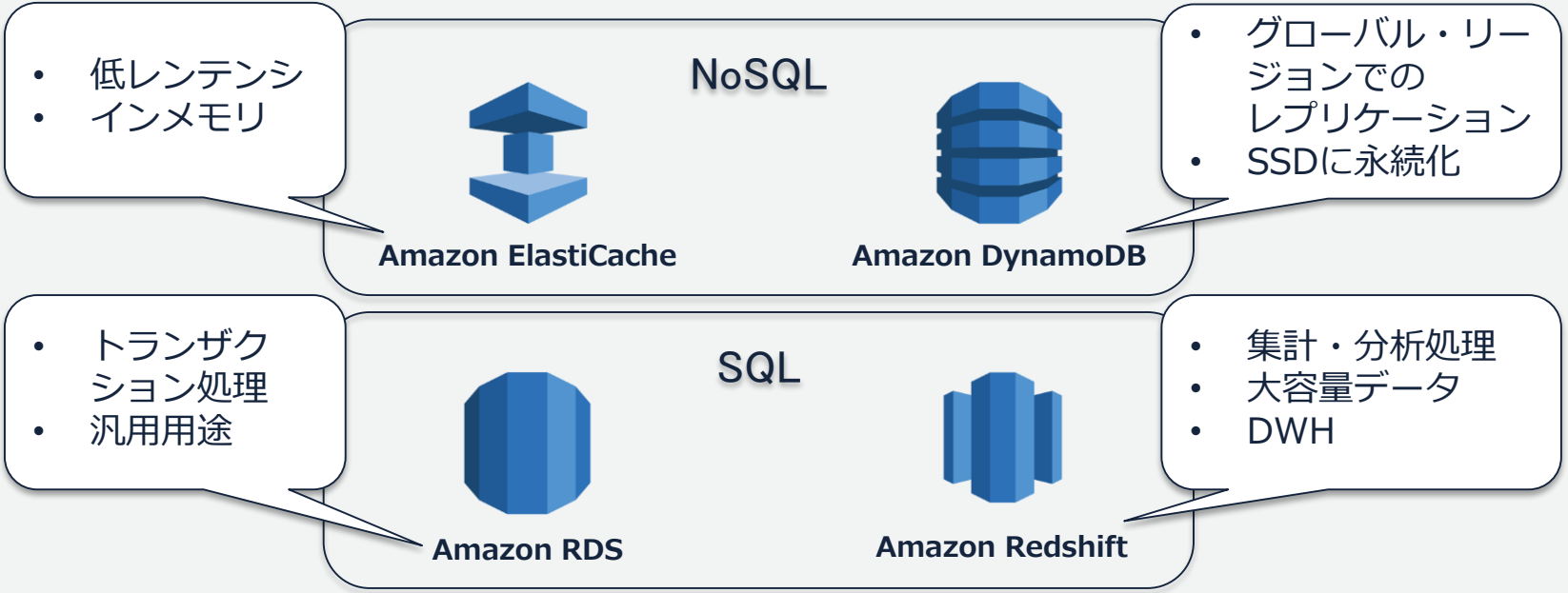
ランダム、かつパラレルな更新アクセス
- RDSもしくはDynamoDB (NoSQL)を検討

巨大なデータを格納するが集計等はしない
- DynamoDBや大きいインスタンスのRDSを検討

3つのRDBMSの特性概要

	Aurora MySQL	Aurora PostgreSQL	Redshift
OLTP性能	★★★	★★★	-
OLAP性能	-	★★	★★★
目標レスポンス時間	数ミリ秒から数十秒	数ミリ秒から数十分	数秒から数時間
結合方法	ネステッドループ、ハッシュ	ネステッドループ、ハッシュ、ソートマージ	ハッシュ、ソートマージ
インデックス	Bツリー、空間、全文	Bツリー、関数、空間、全文、ゾーンマップ	ゾーンマップ

データ・ストアの特性に応じた使い分け



観測例：ストレージの使い分け

状況

- 「ストレージ代込」でEC2が使えると聞いて、インスタンスストアにシステム構築

症状

- データの消失、容量不足

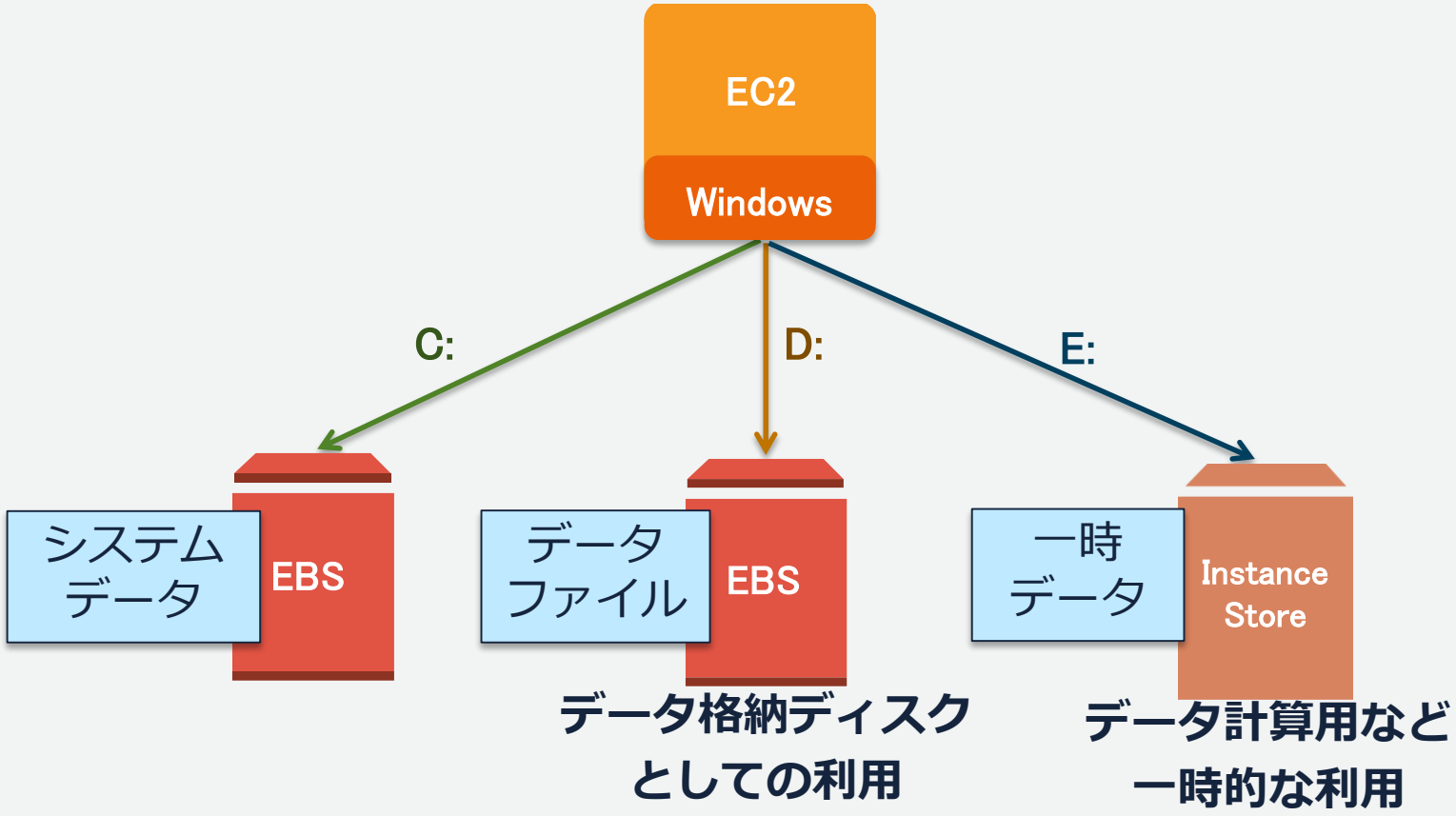
解決法

- ストレージの特性を理解する

インスタンスストアとEBS

- インスタンスタイプに応じて、追加コスト無しで揮発性のインスタンスストアが利用できる
- 実体はEC2の物理ホストのローカルディスク。Stop/Startにより仮想マシンが別ホストに移動するとデータが消去される
- アプリケーションが利用する一時的なデータの置き場所や、分散ファイルシステムのストレージとして活用する
- EBSは永続化ストレージなので、OSの領域やDBのデータなど永続化が必要なデータの置き場所としてはEBSを利用する

EBSとインスタンスストアの利用ケース



観測例：EBSの使い分け

状況

- 汎用SSDのEBS(gp2)にシステム構築

症状

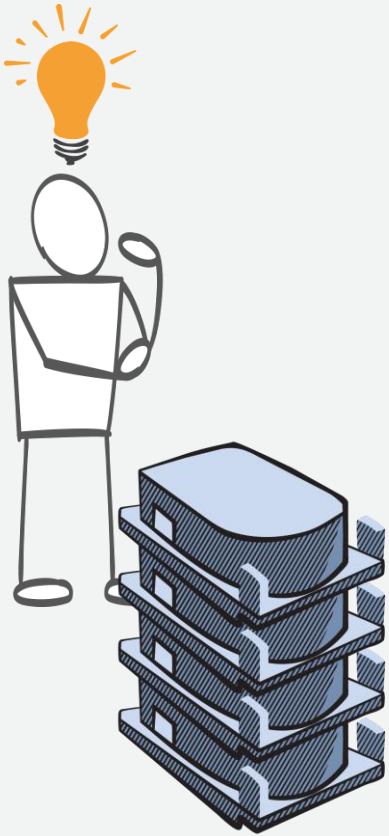
- 速度（IOPS, スループット）に不満

解決策

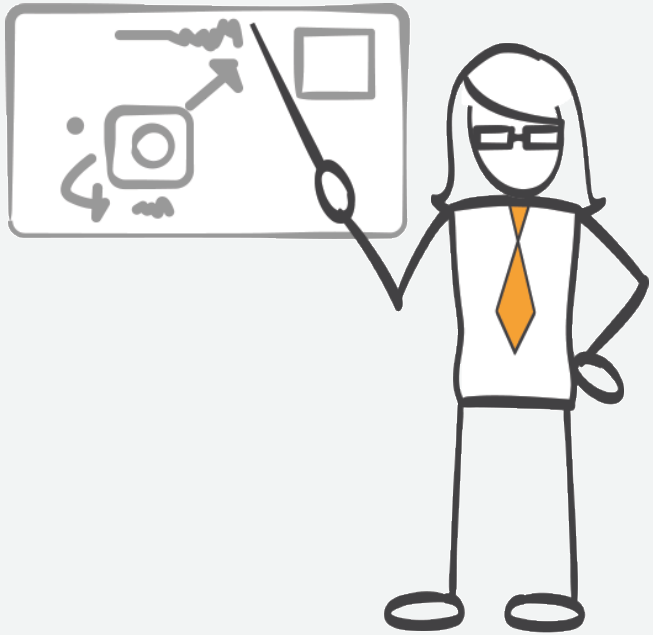
- EBSそれぞれの特性を理解する

EBSのボリュームタイプ

- ユースケースに応じて性能やコストが異なる4種類（現行世代）のボリュームタイプから選択できる
- Snapshotを経由することでボリュームタイプや容量を変更可能
- ブートボリュームになれるのはSSDのみ
- 性能重視ではプロビジョンドIOPS SSD(io1)になりがちだが、スループット最適化HDD(st1)も忘れずに



まとめ



アンチパターンまとめ

アンチパターンはリファクタリング方法が存在する

3つの避けるべきタイミング別のメタアンチパターン

- 机上の空論アンチパターン
- 塩漬けアンチパターン
- ノーコスト最適化アンチパターン

AWS Well-Architected Frameworkが手助けします

オンラインセミナー資料の配置場所

AWS クラウドサービス活用資料集

- https://aws.amazon.com/jp/aws-jp-introduction/

Amazon Web Servicesブログ

- 最新の情報、セミナー中のQ&A等が掲載されています。
- https://aws.amazon.com/jp/blogs/news/

公式Twitter/Facebook
AWSの最新情報をお届けします

@awscloud_jp

もしくは
http://on.fb.me/1vR8yWm

最新技術情報、イベント情報、お役立ち情報、
お得なキャンペーン情報などを日々更新しています！

お問い合わせ先

AWS導入に関しての問い合わせ
http://aws.amazon.com/jp/contact-us/aws-sales

(ご利用者様向け)課金・請求内容、アカウントに関するお問い合わせ
https://aws.amazon.com/jp/contact-us/

AWS技術サポート
https://aws.amazon.com/jp/premiumsupport/