AWS Summits 2014

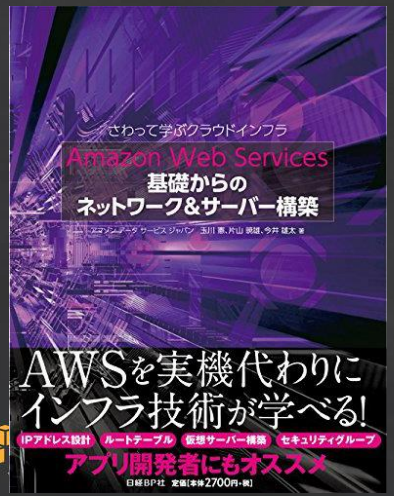
エンタープライズ向けAWSクラウドデザインパターンのご紹介（BCP-DR編）

片山 暁雄, アマゾンデータサービスジャパン株式会社

2014/7/18

Session TE-09

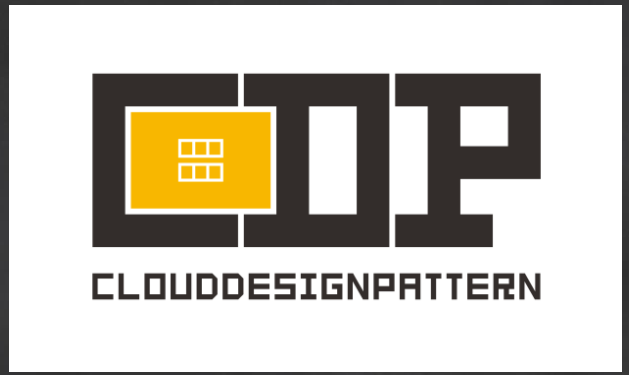
amazon web services



- 名前：片山 暁雄
- 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　エンタープライズソリューション部
  - 部長/ソリューションアーキテクト
- ソーシャル：@c9katayama
- 好きなAWSサービス：AmazonSWF

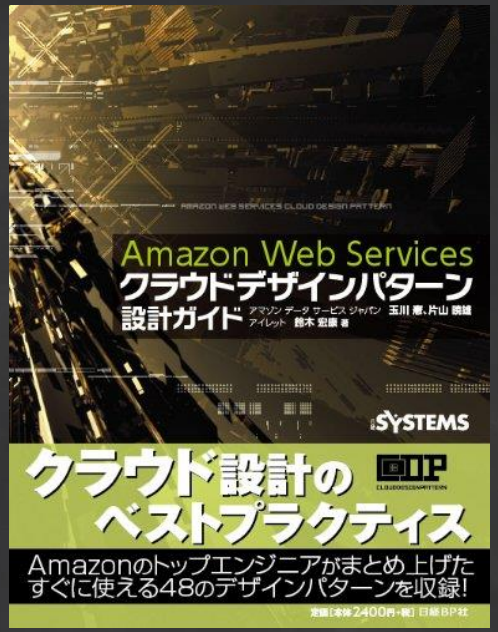
AWSクラウドデザインパターンとは

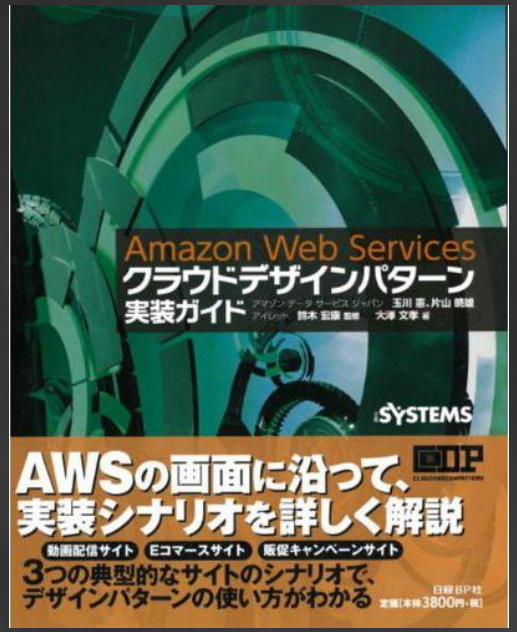
- “AWSクラウドを利用する際に発生する、**典型的な問題**とそれに対する**解決策・設計方法**について、**先人たちの知恵**を分かりやすく分類して、**ノウハウ**として利用できるように整理したもの”



– Ninja of Three –

AWSクラウドデザインパターン書籍





AWSクラウドデザインパターン設計ガイド -Kindle版-

※写真はハメコミ合成です

amazon web services

本日のテーマ

エンタープライズでよく使われる
AWSクラウドデザインパターン
↓
エンタープライズCDP

特にBCP/DRに使われるものにフォーカス

BCP/DRといえば・・

- 東日本大震災後から注目を集める
- BCP/DRが企業価値の１つに
- しかしながら上場企業でも未対策の企業が多い

話を聞きに行くと・・

クラウドを利用したDRサイト（案）

・メインデータセンターの被災に備え、
　クラウドを活用する

・2017年をメドに構築を実施
　Amazon殿に見積もりを依頼

妙な

後任者よろしくパターン

今やろう

対策済み企業でも・・・

DRサイトは、通常時は開発環境に使っています

切り替え試験？したことないですね

BCP/DRを阻む壁

- コスト
- リスク分類が出来ていない
- モチベーション

BCP –事業継続計画-

BCPとは？

- 事業継続計画（Business continuity planning、BCP）は「競争的優位性と価値体系の完全性を維持しながら、組織が内外の脅威にさらされる事態を識別し、効果的防止策と組織の回復策を提供するためハードウェア資産とソフトウェア資産を総合する計画」のこと

※http://ja.wikipedia.org/wiki/%E4%BA%8B%E6%A5%AD%E7%B6%99%E7%B6%9A%E8%A8%88%E7%94%BB

内外の脅威

ディザスタリカバリ

- 自然災害
  - 震災、津波、台風、火災
- 不正アクセス
- サイバー攻撃

etc…

- IT資産の故障、劣化
- オペレーションミス
- 情報漏えい
- 情報改ざん
- データロスト

etc…

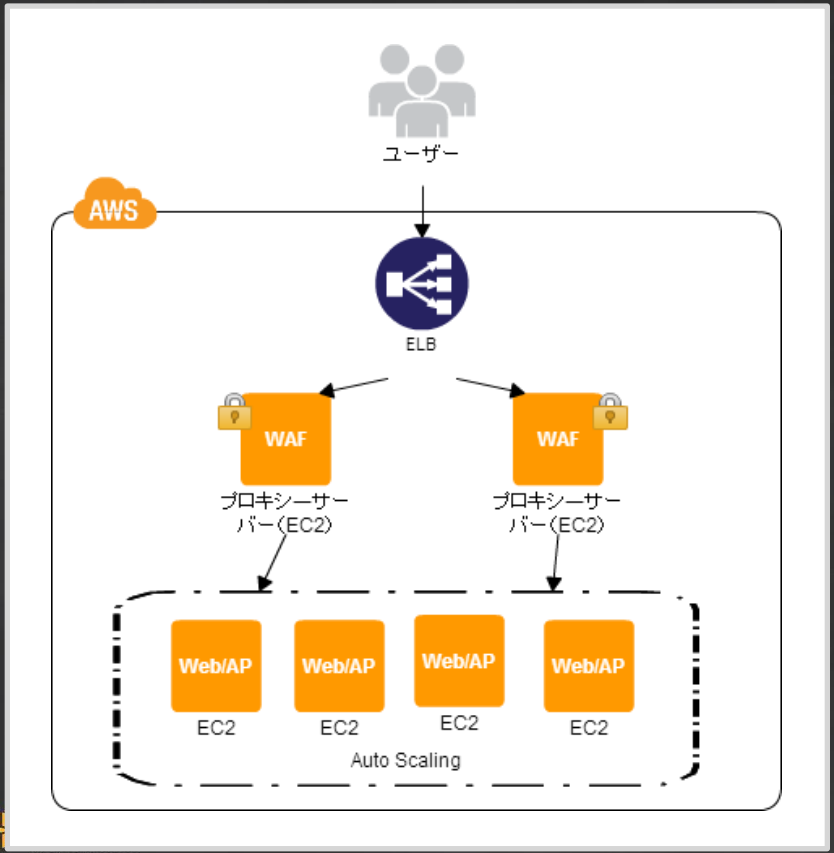
効果的な防止策/回復策

- 不正アクセス
- IT資産の故障、劣化
- オペレーションミス
- 情報漏えい
- 情報改ざん
- データロスト

- WAF/IPS/IDS
- 権限分掌
- システム冗長化
- システム隔離
- バックアップ
- ロギング

不正アクセス

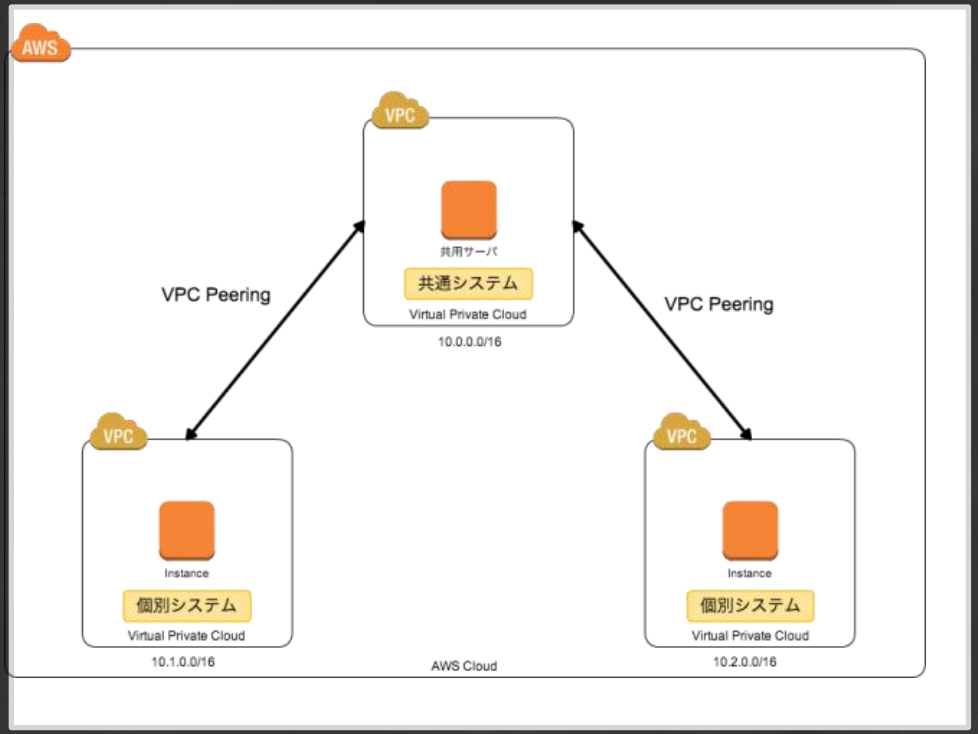
WAF Proxy パターン



- 各サーバにではなく、その上流にWAFやIPS/IDS機能を持ったサーバを配置する
- 仮想アプライアンスを効率よく使う

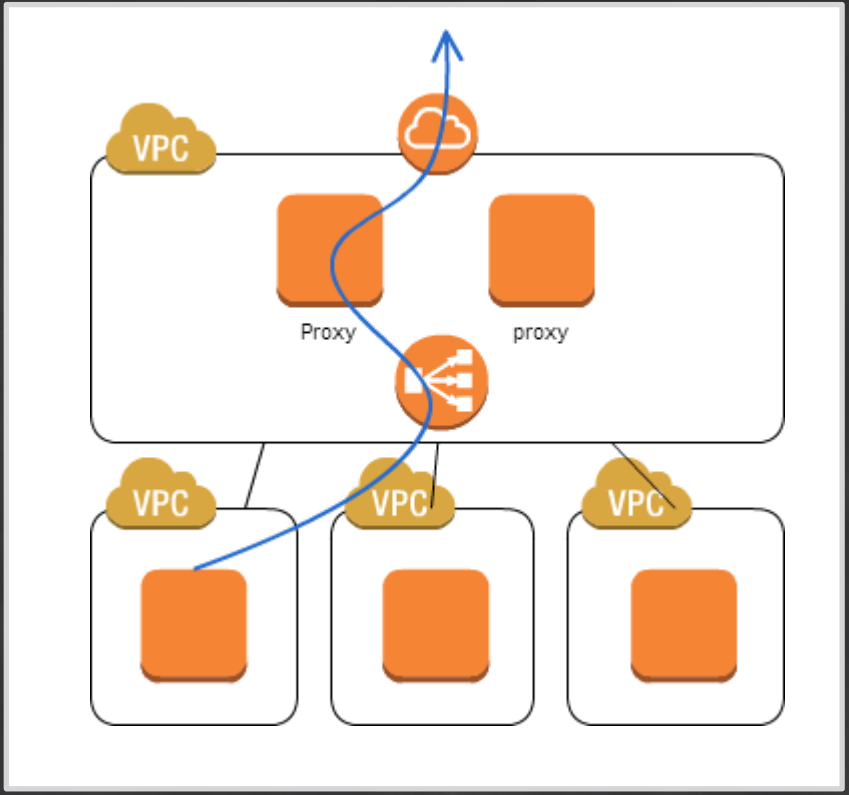
不正アクセス
情報漏えい

Shared Serverパターン(仮)



- 各システム共通で利用するサーバを、共通VPCに分けて管理する
- 監視システム、NAT、踏み台サーバ etc..

http://dev.classmethod.jp/cloud/aws/cdp-server-sharing/

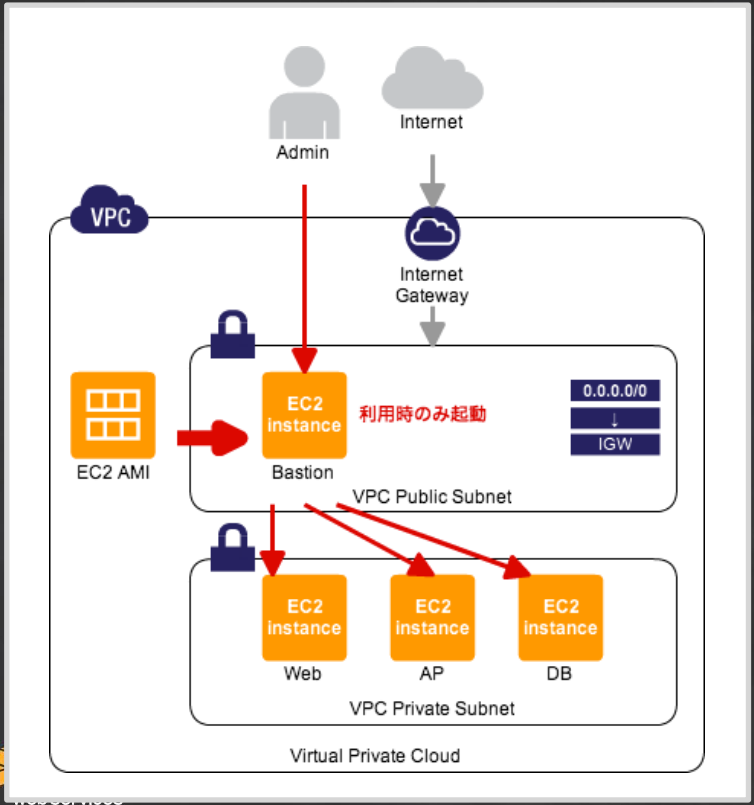


- 外部通信用の共有Proxy用のVPCを作成
- Proxyでロギングやフィルターが可能
- コスト削減効果も

オペミス

情報漏えい

On-demand Bastion / On-demand Firewall パターン

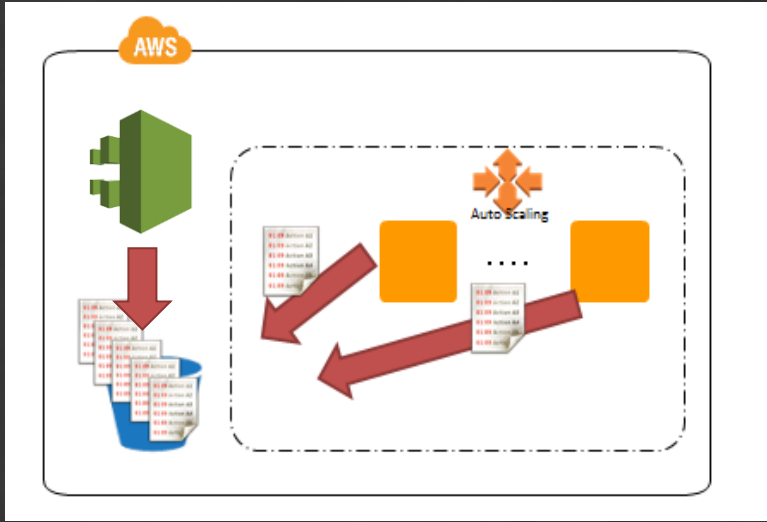


- 内部からのアクセスを制御
- サーバに接続する時だけ認可して、Bastion（踏み台）サーバを立てる
- アクセスログ、操作ログを記録

情報漏えい

情報改ざん

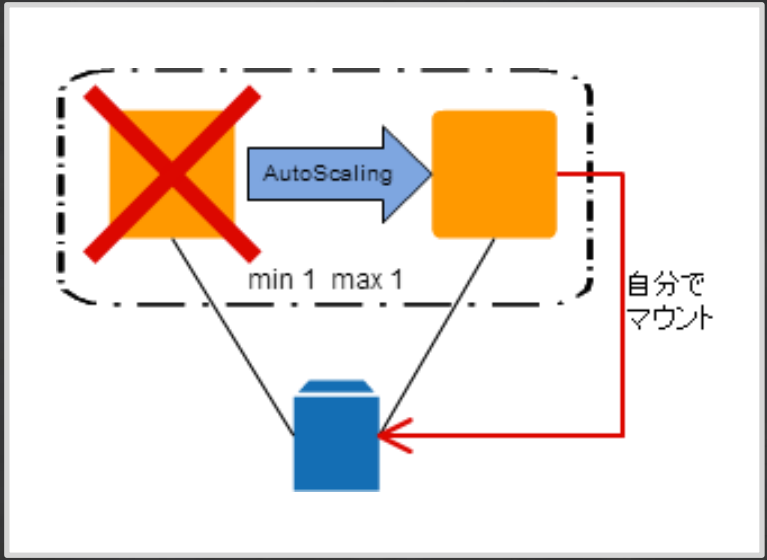
Log Aggregationパターン



- アクセスログ、操作ログなどの各種ログをS3/CloudWatch Logsに集約
- CloudTrailでAWS操作もロギング
- CloudWatch Logsへの集約で、特定イベントに合わせた通知が可能
  - “ERROR”や”create*”などの文字列で通知
- インシデント発生時のトレースが可能

機器故障

Self Healing パターン

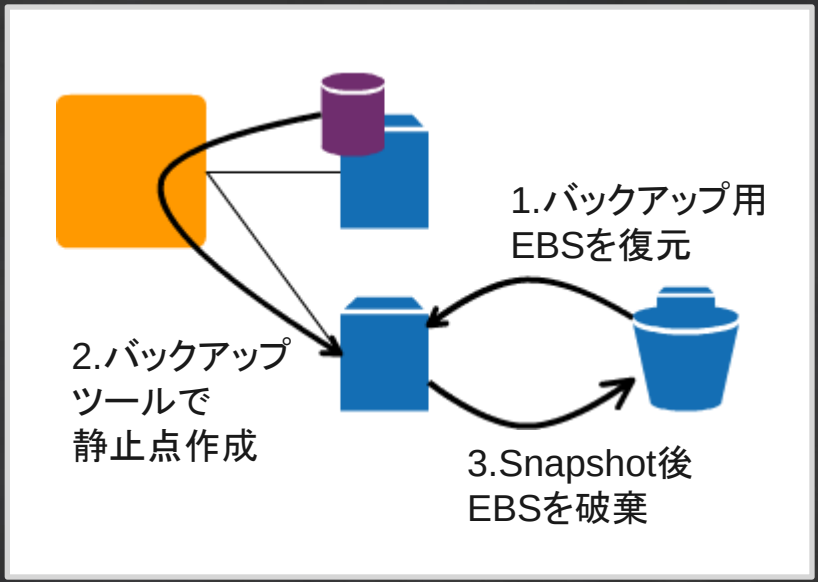


- AutoScalingを利用した、自動回復のためのパターン
- インスタンスを起動後、インスタンス自身でデータ領域のマウントを実施
  - Cloud DIパターンを併用

情報改ざん

データロスト

On-demand Backup Diskパターン

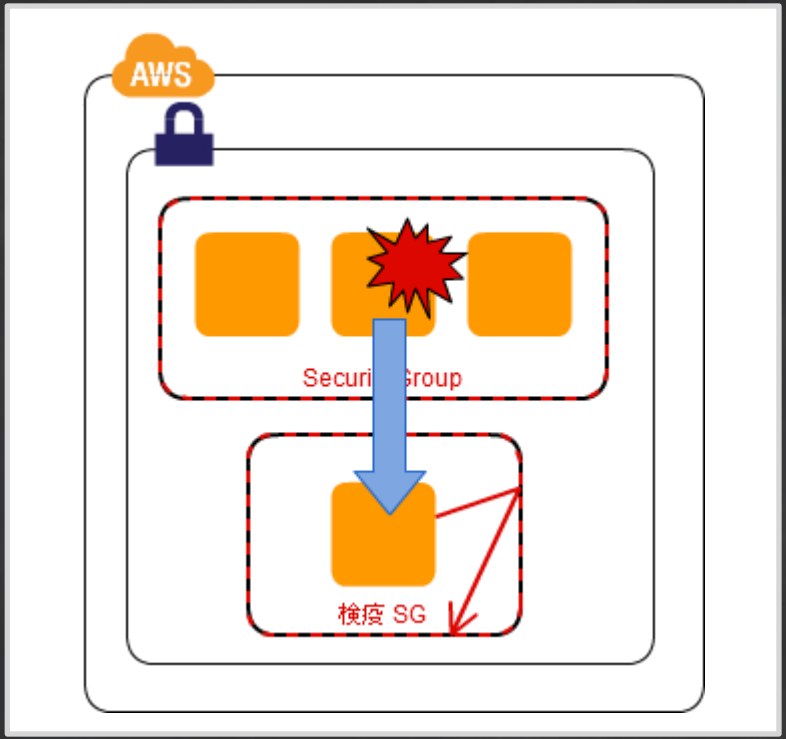


- バックアップ用のEBSをオンデマンドで作成
- バックアップツールで、バックアップ用EBSにバックアップを作成
- S3などAWSサービス非対応のツールでも、バックアップの取得が可能に
  - ツール利用でオンラインバックアップも可能

不正アクセス

情報漏えい

Quarantine(検疫) Firewallパターン



- マルウェア感染や情報流出など、疑わしいインスタンスを検疫ネットワークに隔離
- Outbound出来ないセキュリティグループを作成し、対象インスタンスをそのセキュリティグループに隔離
- 隔離後に影響を調査

DR –ディザスタリカバリ-

内外の脅威

ディザスタリカバリ

- 自然災害
  - 震災、津波、台風、火災
- 不正アクセス
- サイバー攻撃

etc…

- IT資産の故障、劣化
- オペレーションミス
- 情報漏えい
- 情報改ざん
- データロスト

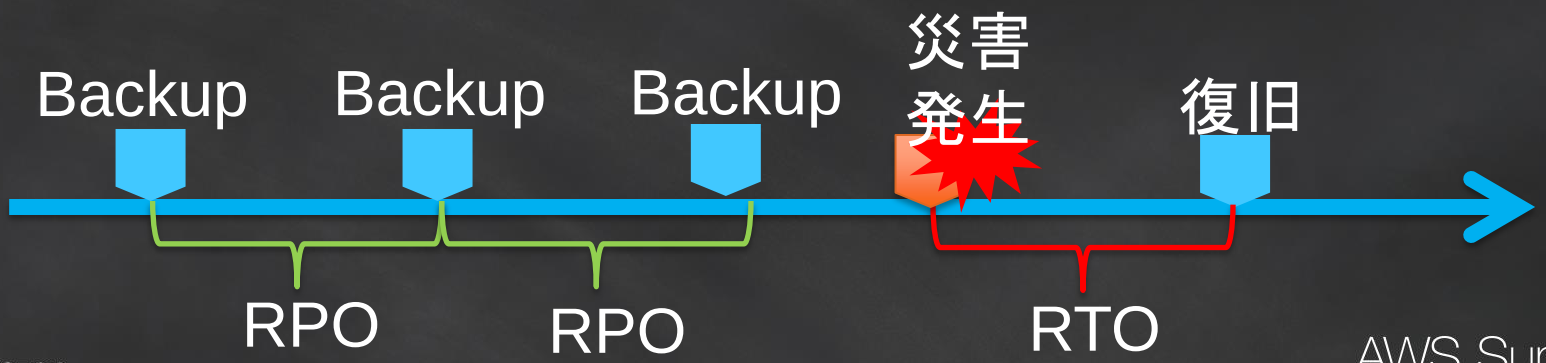
etc…

ディザスタリカバリ

- **ディザスタリカバリー (DR)** とは自然災害・人的災害発生時に企業が技術的なインフラストラクチャを復旧もしくは継続させるために準備する**一連のプロセス・ポリシー・および手順のこと**

DRで重要なポイント

- 目標復旧時点 (RPO)
  - どの時点の状況まで復旧できるのか
- 目標復旧時間 (RTO)
  - いつまでに復旧するのか

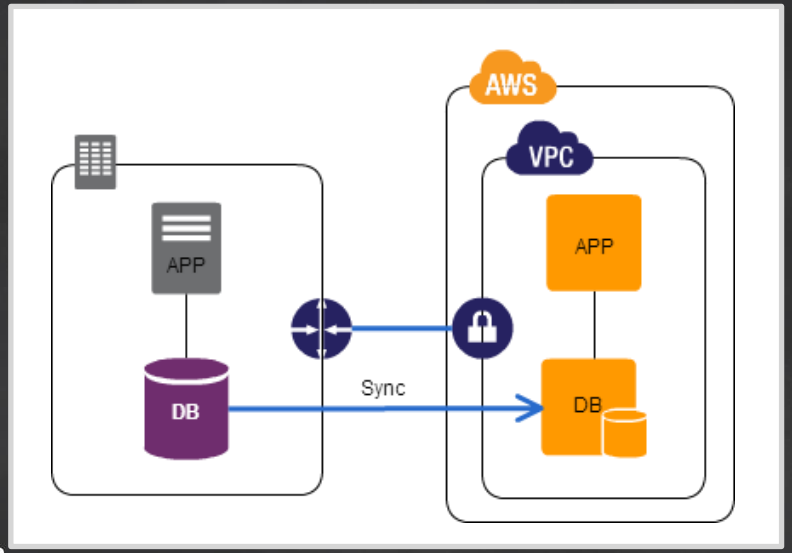


可用性とディザスタリカバリーレベルの選択例

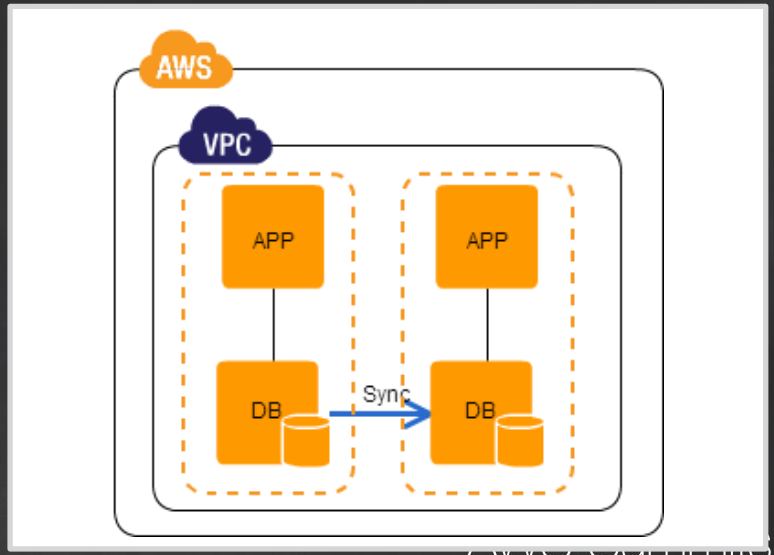
Hot Standby DC

継続的
可用性

- アプリケーションは、オンプレ/AWSにデプロイ
- DBは同期書き込みを実施（DB Replication Pattern)
- すべてのシステムを起動しておく



オンプレミス - AWS

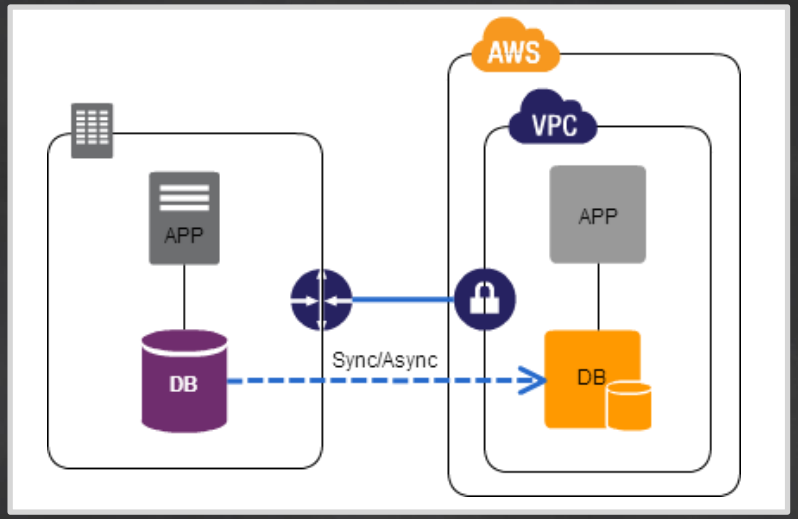


AWS - AWS

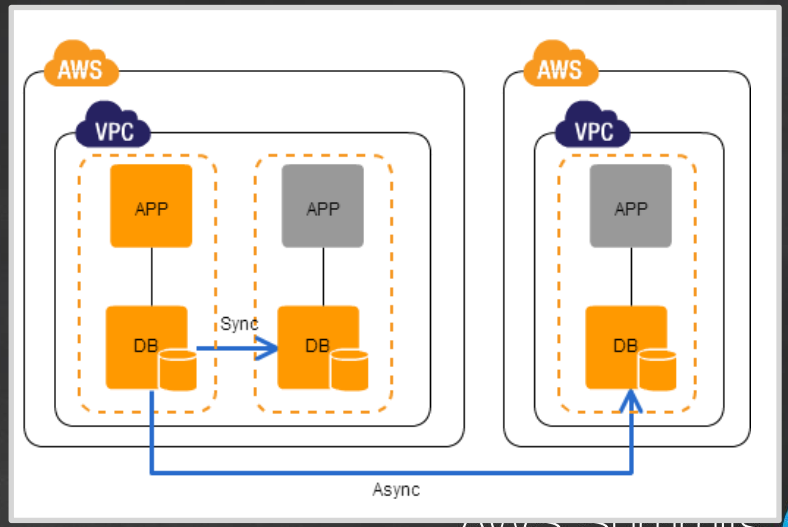
Warm Standby DC

高い可用性

- アプリケーションは、オンプレ/AWSにデプロイ
- デプロイ後、DRサイト側のアプリサーバは停止
- DBは同期もしくは非同期で書き込み



オンプレミス - AWS

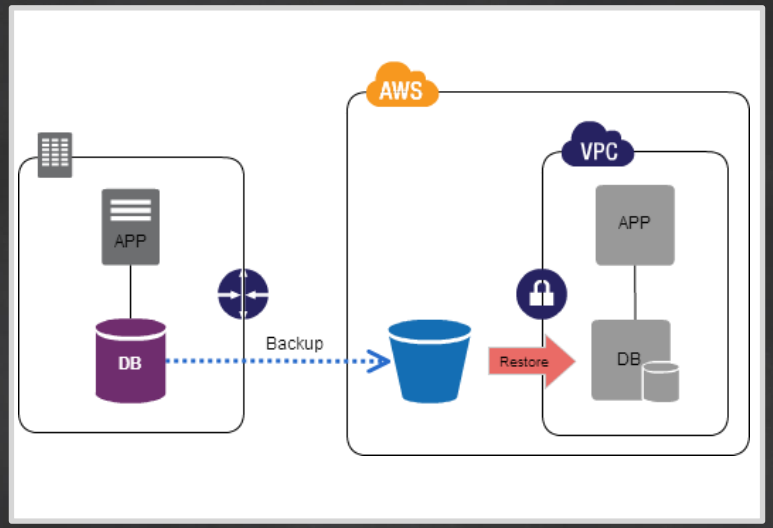


AWS - AWS

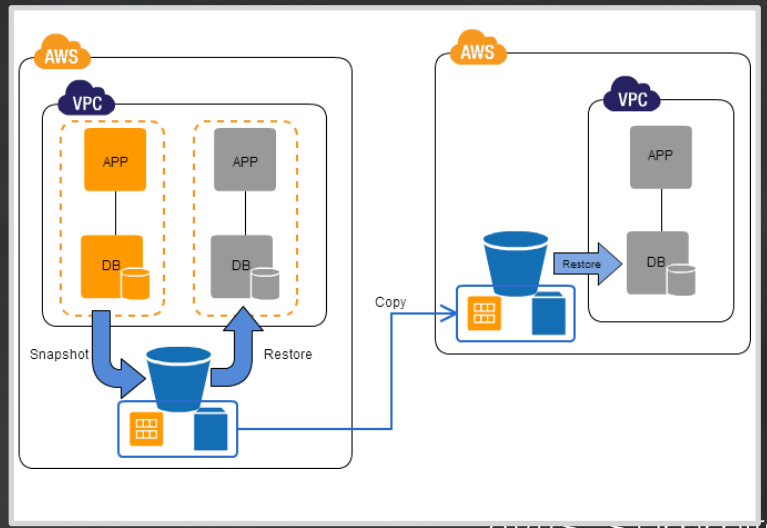
Cold Standby DC

スタンバイ
システム

- アプリケーションはDRにデプロイ後停止
- DBはデータをS3に定期バックアップ or Snapshot
- 災害発生時はS3からリストア

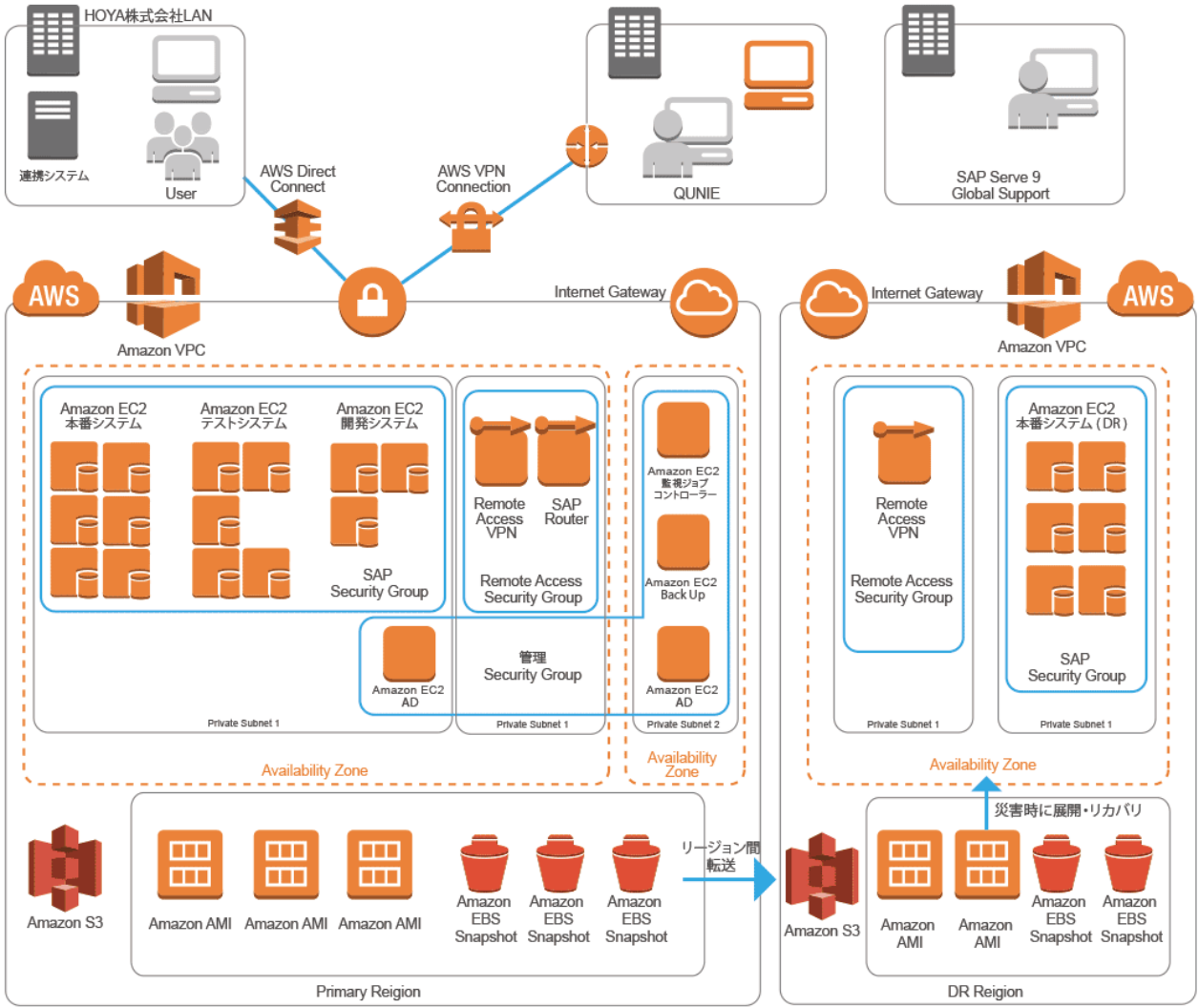


オンプレミス - AWS

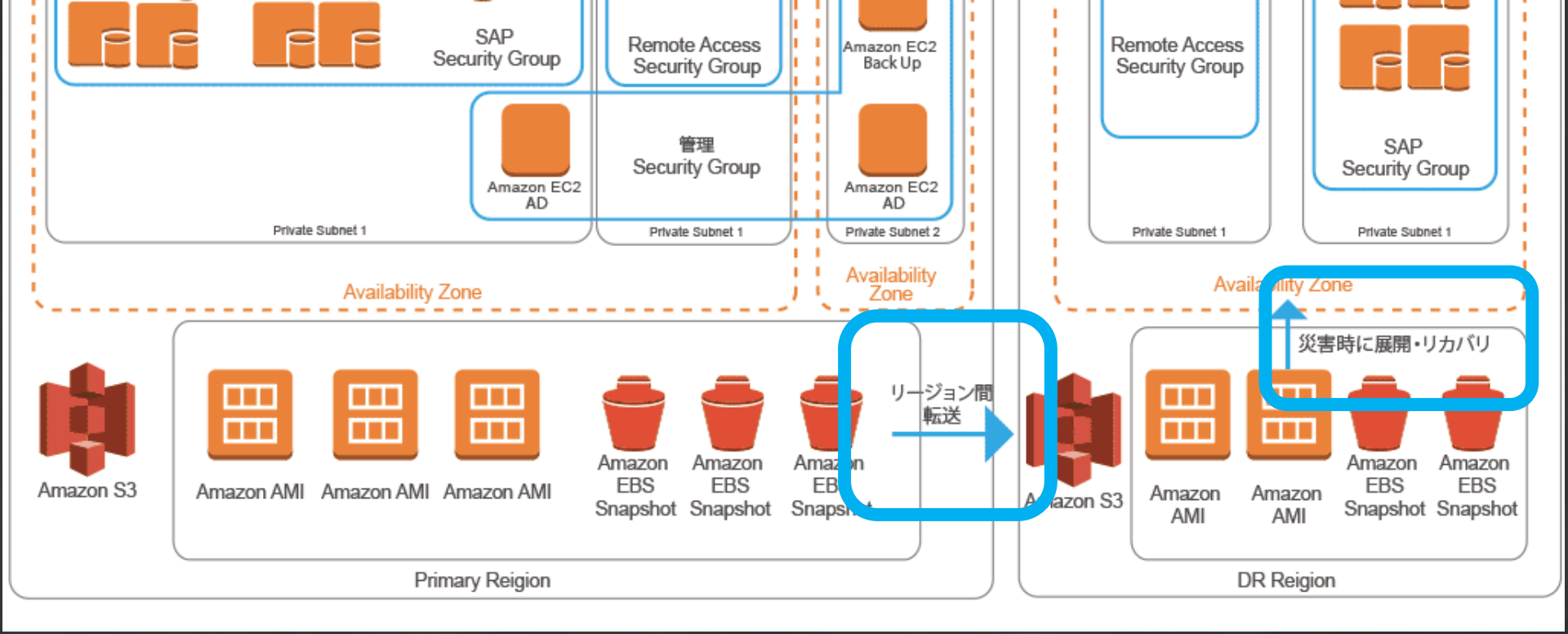


AWS - AWS

HOYA様のアーキテクチャ



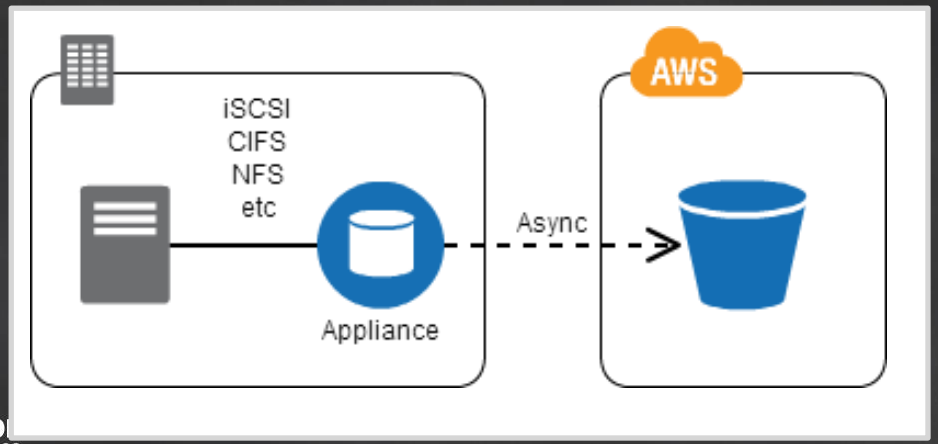
amazon web services


SAP
Security Group
Remote Access
Security Group
Amazon EC2
Back Up
Amazon EC2
AD
管理
Security Group
Amazon EC2
AD
Private Subnet 1
Private Subnet 1
Private Subnet 2
Availability Zone
Availability Zone
Remote Access
Security Group
SAP
Security Group
Private Subnet 1
Private Subnet 1
災害時に展開・リカバリ
Amazon S3
Amazon AMI
Amazon AMI
Amazon AMI
Amazon
EBS
Snapshot
Amazon
EBS
Snapshot
リージョン間
転送
Amazon S3
Amazon
AMI
Amazon
AMI
Amazon
EBS
Snapshot
Amazon
EBS
Snapshot
Primary Reigion
DR Reigion

Virtual Cloud Storage

データ
リカバリのみ

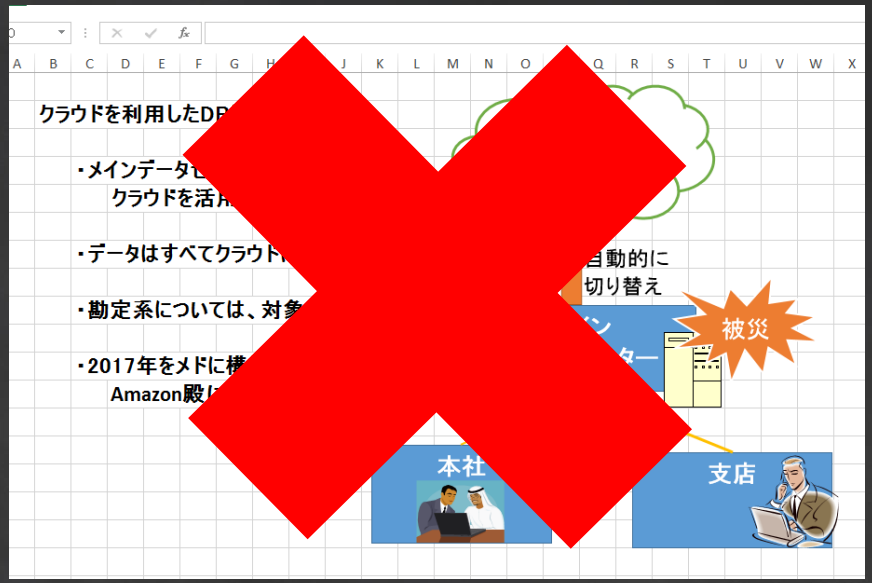
- 既存のバックアップ方式の変更にはコストがかかる
- オンプレミスに、自動的にクラウドにデータをアップロードするストレージアプライアンスを配置し、既存バックアップに組み込む



- アプライアンス
  - AWS Storage Gateway
  - Riverbed SteelStore
  - S3対応NAS(QNAP,Buffaloなど)

AWSを使ったBCP/DR

- AWSクラウドの特性を生かして、従来よりも早く、安価にBCP/DRが可能



BCP/DRは発動時の手順が重要

BCP

組織の回復策

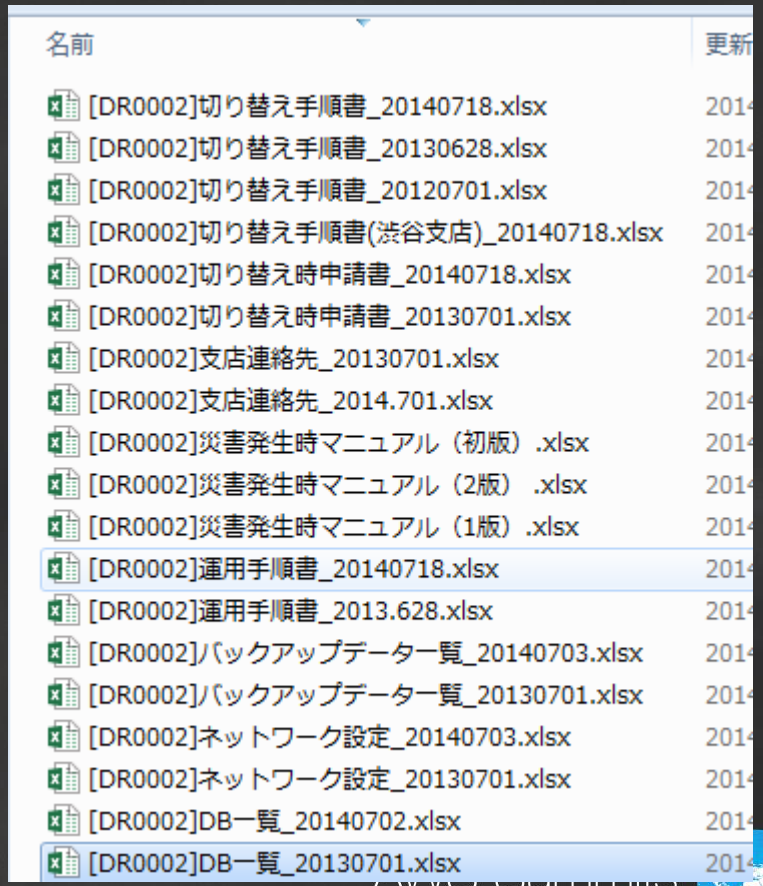
DR

一連のプロセス・ポリシー・および手順

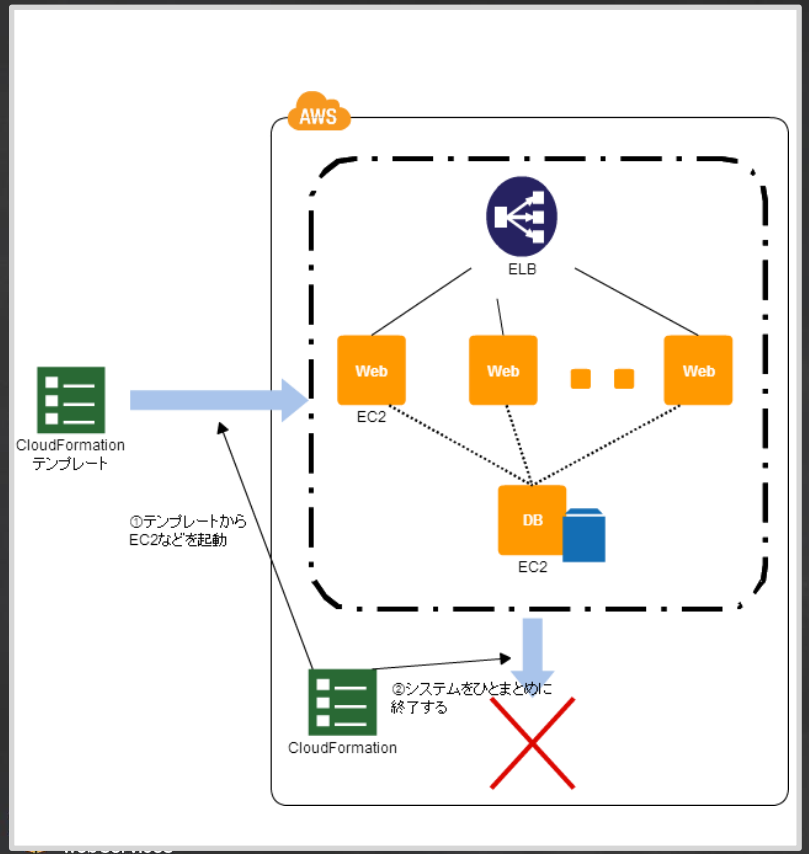
どのように対応/回復するかを決めておく
手順を訓練しておく

回復手順・・

- BCP/DR発動時の手順は複雑になりがち
- 特に混乱の中作業するため、極力手順は少なくすべき



Stack Deploymentパターン



- CloudFormationテンプレートを元に、システムを復元
- DR先へのシステム構築を自動化

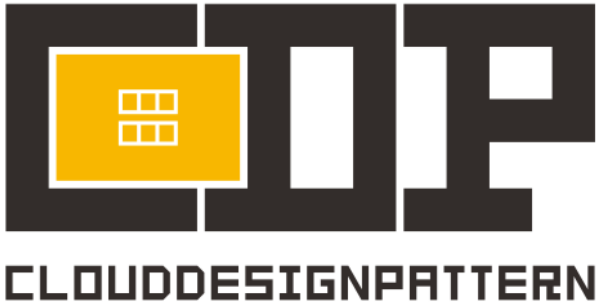
まとめ

BCP/DRに生かせるCDP

- WAF-Proxyパターン
- Shared-Serverパターン
- On-demand Bastion /On-demand Firewall パターン
- Log Aggregationパターン
- Self Healingパターン
- On-demand
- Backup Diskパターン
- Quarantine(検疫) Firewallパターン
- Hot/Warm/Cold Standby DC
- Virtual Cloud Storage


で


amazon
web services


CLOUDDESIGNPATTERN