DR対策としての
マルチリージョン対応について

株式会社 Works Human Intelligence
Product Div. Advanced Technology Dept.

兒玉 拓也

スピーカー

兒玉 拓也

株式会社 Works Human Intelligence

Product Div.Advanced Technology Dept.Chatbot & MKS Ops Grp.Chatbot & MKS Ops

略歴

- 2011年 ワークスアプリケーションズに入社
- 2019年 社会人大学院 入学
- 同年 ワークスアプリケーションズ分社に伴い Works Human Intelligence へ転籍
- 2021年 社会人大学院 卒業

業務領域

- インフラ、CI/CD周りの構築、モニタリング等の SRE領域を担当

その他

- Qita「アジャイルを使ってクリスマスまでに彼女を作る方法を考えてみる」

アジェンダ

Works Human Intelligence

01 はじめに
会社紹介 / サービス紹介 / 想定対象者 / 用語解説

02 事前検討
DRが必要な状況 / 過去のAWS障害 / 現在の災害対策の状態を把握する

03 アーキテクチャ設計
復旧時のアーキテクチャ選択/ アプリケーション層と永続層/ 永続層の設計

04 運用設計
FailOver・FailBackの移行条件 / 緊急時対応計画ガイド

05 災害訓練
BCPテスト

アジェンダ

01 **はじめに**
会社紹介 / サービス紹介 / 想定対象者 / 用語解説

02 **事前検討**
DRが必要な状況 / 過去のAWS障害 / 現在の災害対策の状態を把握する

03 **アーキテクチャ設計**
復旧時のアーキテクチャ選択/ アプリケーション層と永続層/ 永続層の設計

04 **運用設計**
FailOver・FailBackの移行条件 / 緊急時対応計画ガイド

05 **災害訓練**
BCPテスト

Works Human Intelligence

業種・業態を問わず、数千名～数万名規模の大手法人にご利用いただいています

※2021年度　ERP市場 - 人事・給与業務分野：ベンダー別売上金額シェア
出典：ITR「ITR Market View：ERP市場2023」

ERP市場人事・給与業務分野
シェアNo.1※
※2021年度　ERP市場 – 人事・給与業務分野：ベンダー別売上金額シェア
出典：ITR「ITR Market View：ERP市場2023」

国内大手法人※の（※従業員数3,000人以上）
3社に1社が
WHIのHR製品を利用（当社調べ）

年間継続利用率 **98%※**
※2022年度　金額ベース

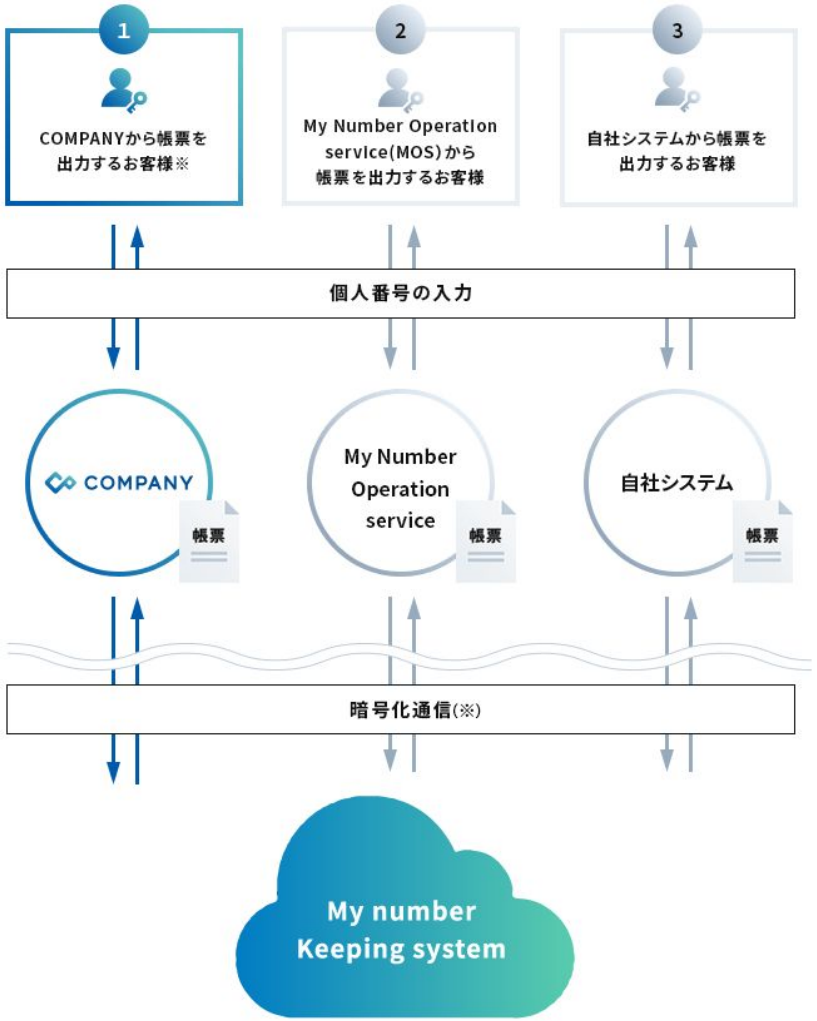
平均継続利用年数 **11年※**
※2022年末時点

日本の大手約1,200法人
グループが導入

「COMPANY」が管理する
人事データ数は**490万**※
※2022年12月末時点の
「COMPANY 人事」の契約ライセンス数合計

はじめに - サービス紹介 -

サービス概要



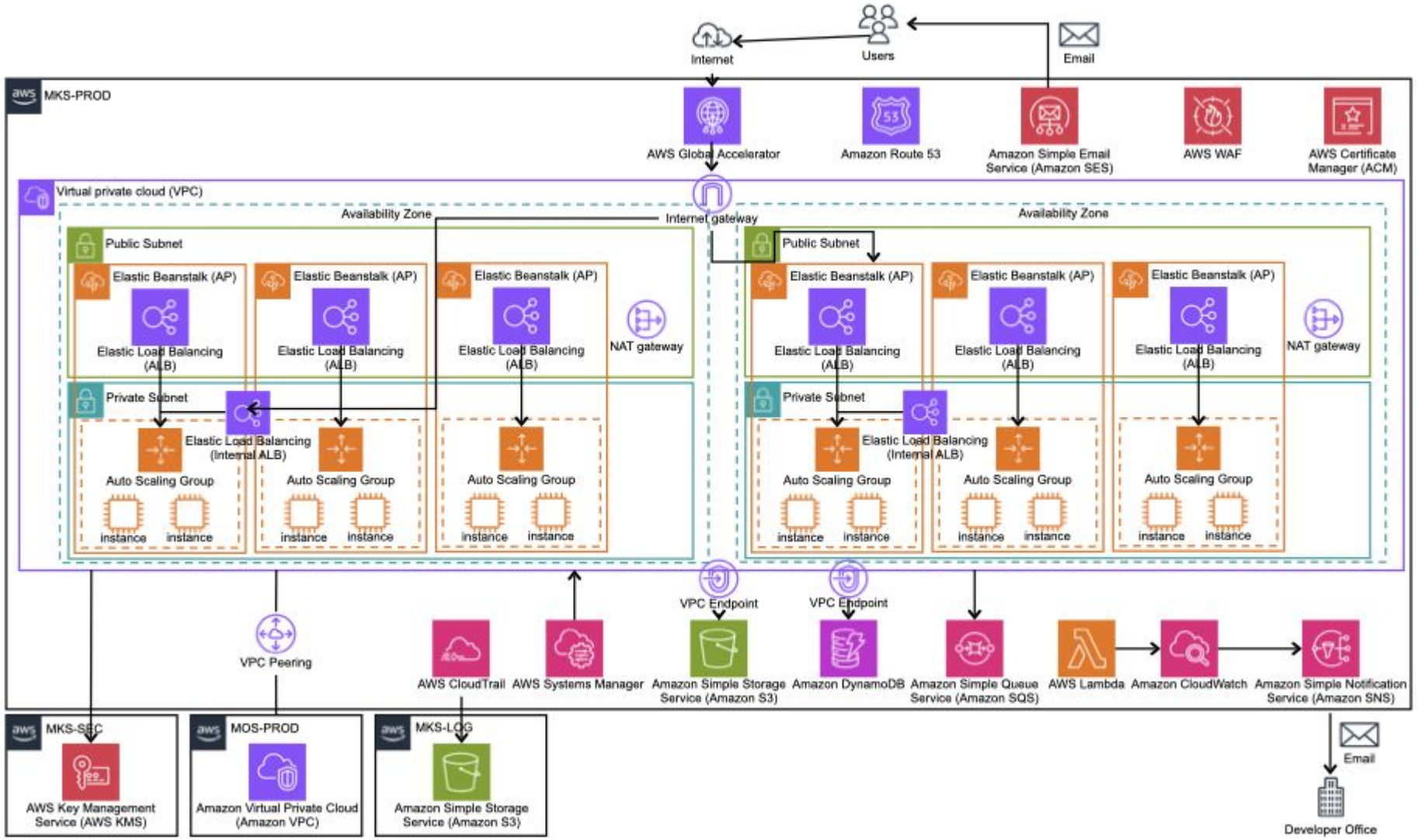
マイナンバー管理プラットフォーム

My Number Keeping System（MKS）は、
クラウドサービス上で各企業の従業員、
およびその家族のマイナンバーを一括で管理する
マイナンバー管理プラットフォームです。

MKSの利用により、
お客様は自社でマイナンバーを
保持・管理する必要がなくなります。

はじめに

MKSのサービス構成図



はじめに

本講演の想定対象者

DR対策が必要か考えている方

・事前の検討の中で、DRの目的や検討事項をご説明します

これからDR対策を始めようとしている方

・対策を実施した際の検討すべき内容、構成例や災害時への備えについてご説明します

この資料の用語集

DRリージョン

・データやアプリケーションをバックアップおよび復元するための地理的なリージョンまたは場所を指す
　本資料では大阪リージョンを想定している

プライマリリージョン

・サービスの主要な運用リージョンや本番運用リージョンを指す
　本資料では東京リージョンを想定している

アジェンダ

01 はじめに
会社紹介 / サービス紹介 / 想定対象者 / 用語解説

02 **事前検討**
DRが必要な状況 / 過去のAWS障害 / 現在の災害対策の状態を把握する

03 アーキテクチャ設計
復旧時のアーキテクチャ選択/ アプリケーション層と永続層/ 永続層の設計

04 運用設計
FailOver・FailBackの移行条件 / 緊急時対応計画ガイド

05 災害訓練
BCPテスト

事前検討 - マルチリージョン対応が必要な状況

状況例

関東への直下型大地震

・AWSのデータセンターが全てのAZで一斉に壊滅的なダメージを受ける
・復旧までの時間が長期間である

AWSのリージョン障害

・リージョンサービス(※)などが使用出来なくなる
　ex. Amazon DynamoDB、AWS Lambda、Amazon S3、Amazon API Gateway、Amazon SQS etc...

マルチリージョン対応が必要となる場面は、いずれも関東での障害発生時である

※ 参考：https://docs.aws.amazon.com/ja_jp/whitepapers/latest/aws-fault-isolation-boundaries/regional-services.html

事前検討 - 現在の災害対策の状態を把握する

基本のマルチAZとマルチリージョン対応の目的

実はマルチAZでも結構障害対策してくれてる

・AWS障害の半数はマルチAZで回避出来る場合が多い
・仮に単一AZの障害が発生しても半日程で復旧されている事が多い
・Well-Architected フレームワークの基本としてマルチAZが記載されている
https://aws.amazon.com/jp/blogs/startup/techblog-well-architected-reliability-1/#02

それでもマルチリージョン対応する目的は？

・サービス稼働率の維持
・リージョン単位の障害への対策
・マルチリージョンを求めるお客様へ応える

マルチリージョン対応には工数やコストがかかる
その上でマルチリージョン対応をする目的は何か、本当に必要かを考える

事前検討 - 現在の災害対策の状態を把握する

MKSの事例

マルチリージョン対応の目的

ユーザーのニーズ

・障害発生時でも事業継続を求めるお客様の強いニーズ
・ユーザー規模の多い法人が多く、日本各地に支店があり業務を回し続ける必要がある

リージョン災害に備える

・リージョン災害が長期化した場合に備える

事前検討 - 現在の災害対策の状態を把握する

災害対策の状況を確認し検討する必要があるものを洗い出す

災害発生時の対応体制

・対応要員が一局集中していないか
・災害発生時の安否確認と連絡手段は確立しているか

復旧目標

・復旧までの最低ライン
  - SLA/SLOでDR対策の設計方針が変わってくる

監視体制

・障害が発生してもアラートの通知などが適切に行えるか
  - AWSリソースのリージョンサービスに依存していた場合、災害発生時に通知が飛ばない場合がある

事前検討 - 現在の災害対策の状態を把握する

Works Human Intelligence

MKSの事例

検討項目	詳細項目	現在の状態
災害時の対応体制	対応要員	関東と福岡に要員が存在
		安否確認システムによるメンバーの安否確認
復旧目標	復旧の最低ライン	SLO 99% (直近1年稼働実績 100%)
		目標復旧時点　1日 (RPO)
		大規模災害時でもSLOの数値は計算される
監視体制	災害時のアラート通知	リージョンサービスに依存していないアラート通知

アジェンダ

01 はじめに
会社紹介 / サービス紹介 / 想定対象者 / 用語解説

02 事前検討
DRが必要な状況 / 過去のAWS障害 / 現在の災害対策の状態を把握する

03 アーキテクチャ設計
復旧時のアーキテクチャ選択/ アプリケーション層と永続層/ 永続層の設計

04 運用設計
FailOver・FailBackの移行条件 / 緊急時対応計画ガイド

05 災害訓練
BCPテスト

アーキテクチャ設計 – 復旧時のアーキテクチャ選択

Backup&Restore

データリソースのみDRリージョンにバックアップし、
それ以外のリソースは障害発生時に構築。

Pilot Light

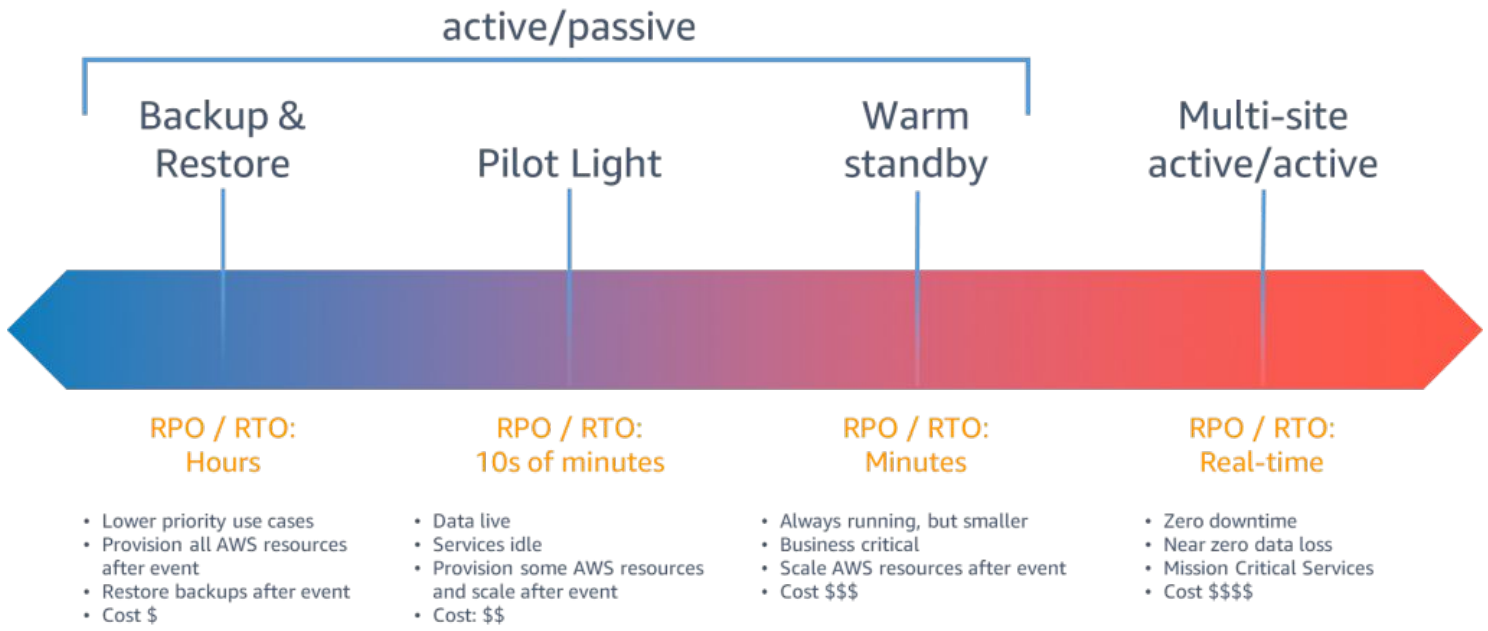
データリソースと一部リソースのみ DRリージョンに構築し、サービス自体はアイドル状態。

Warm standby

プライマリリージョンと同様に DRリージョンに
リソースを構築するが、
アプリケーションリソースは最小限にとどめる。

Multi-site-active/active

プライマリリージョンと同様のリソースを
DRリージョンに構築。



参照：https://aws.amazon.com/jp/blogs/news/disaster-recovery-dr-architecture-on-aws-part-1-strategies-for-recovery-in-the-cloud/

アーキテクチャ設計 – 復旧時のアーキテクチャ選択

MKSの事例 Pilot Lightを参考にした

コスト

サービスの構成上インスタンス、Application Load Balancer、Nat Gatewayなど常時待機の場合コストのかかる構成であった。

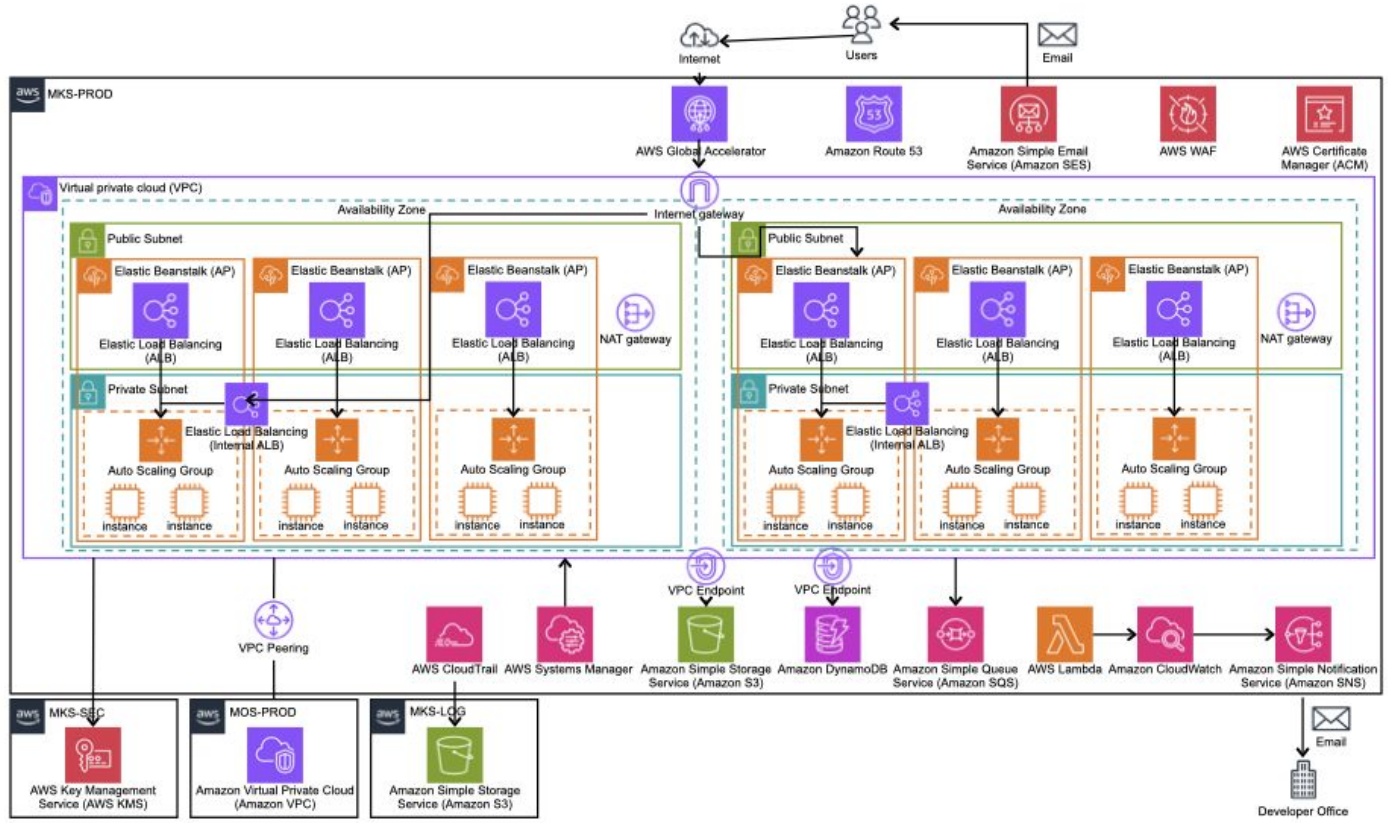
発生頻度と対応時間

AWSのリージョン障害の発生頻度、
障害発生から復旧までの時間と、移行コストを検討。
移行の判断を考慮した場合、
ある程度の時間がかかる可能性があった。

通常デプロイ時のメンテナンス性

構成上Warm Standby, active/active構成が不可。

また、Pilot Light構成の場合でもマルチリージョン間で差分を意識して変更やデプロイをしなければならない構成は避けるようにした。



アーキテクチャ設計 – アプリケーション層と永続層

MKSの事例　Pilot Lightで対応をする為に

IaC化

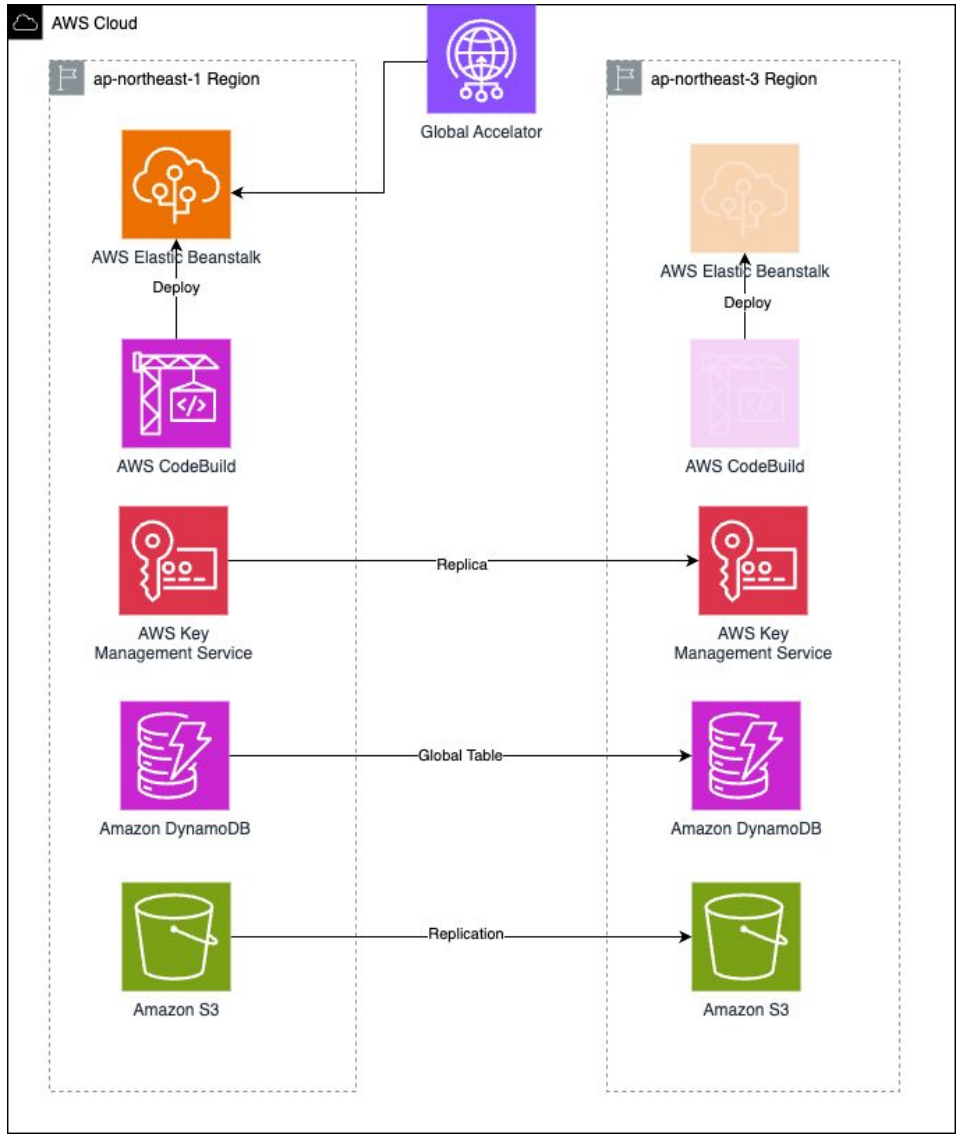
サービス構築時作業の 8割程度が元々 IaC化されており、
今回のDR化で必要な永続層のレプリケート対応や、
DRリージョン構築時のパラメータ化の IaC対応が
別途必要になった。

切り替え時にアプリケーション層を構築

DRリージョン移行時には毎回0からデプロイ機構を構築し、
ネットワークとアプリケーション層の構築を
実施する構成とした。

永続層のレプリケート

サービスで利用している永続層を洗い出し、
DRリージョンへのデータレプリケートやバックアップの実施。

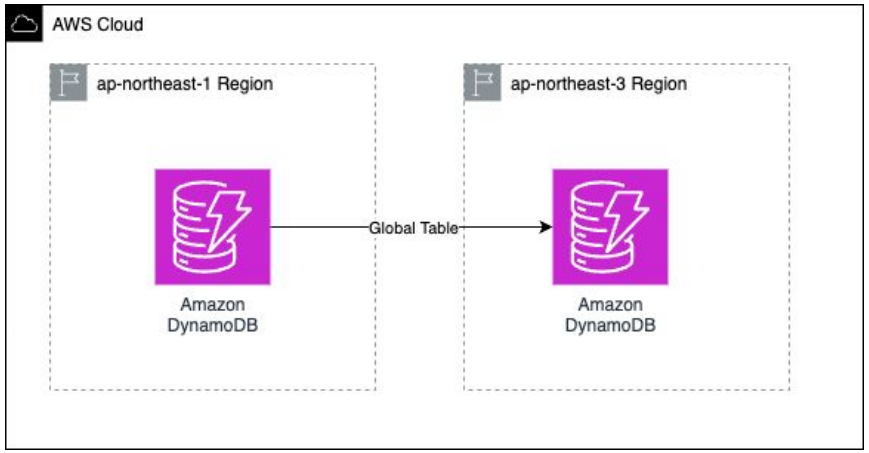


アーキテクチャ設計 – 永続層設計

MKSの事例

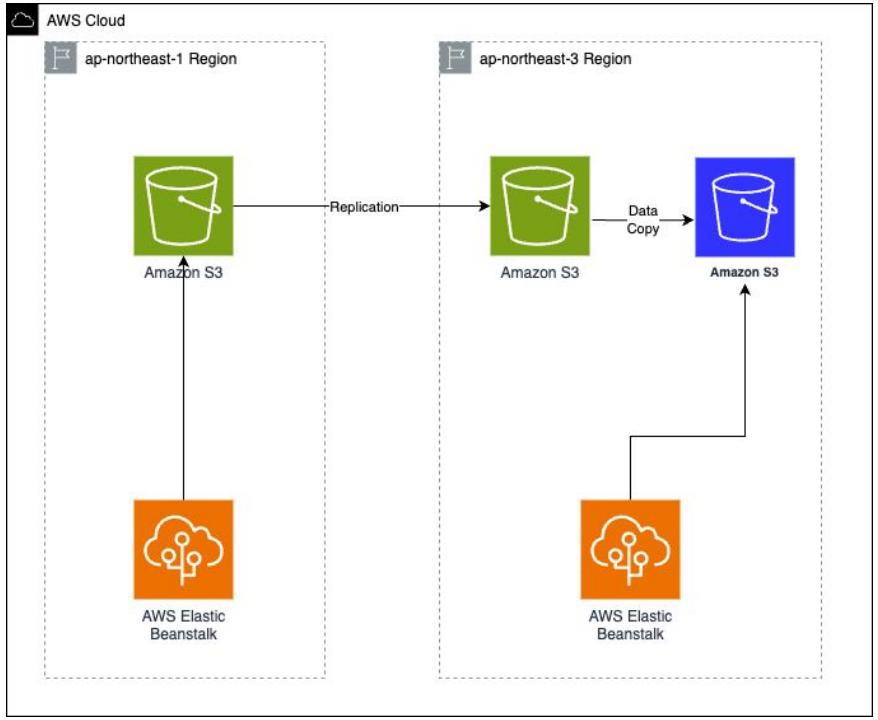
Amazon DynamoDB

グローバルテーブルを設定し DRリージョンに
プライマリリージョンのデータを同期させる。



Amazon S3

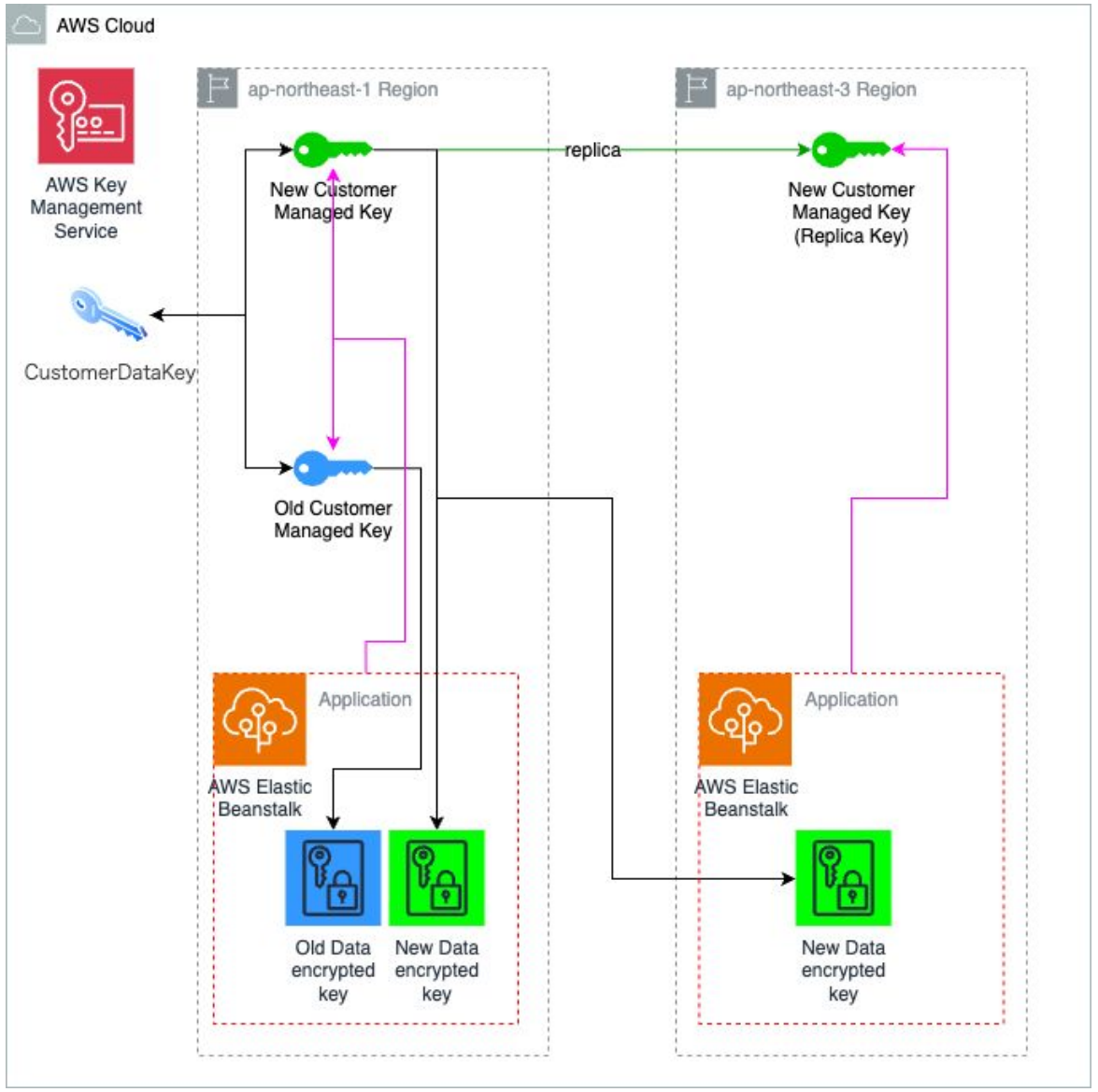
S3もDRリージョンにデータをレプリケーションさせる。
該当箇所は既存の S3バケットの作り直しを避ける為、
レプリケーションバケットを経由する方式にした。



MKSの事例

AWS Key Management Service (AWS KMS)

マルチリージョン対応前に使用していた AWS KMSのキーは
2015年に作成されたキーの為、
マルチリージョンキーに対応していなかった。
その為一度キーを作成し直し、データキーを移行した。



アジェンダ

01 はじめに
会社紹介 / サービス紹介 / 想定対象者 / 用語解説

02 事前検討
DRが必要な状況 / 過去のAWS障害 / 現在の災害対策の状態を把握する

03 アーキテクチャ設計
復旧時のアーキテクチャ選択/ アプリケーション層と永続層/ 永続層の設計

04 運用設計
FailOver・FailBackの移行条件 / 緊急時対応計画ガイド

05 災害訓練
BCPテスト

運用設計 – 移行条件

運用として何を決めたか

いつDRリージョンに移すか（FailOver）

・条件：どのような状態だった場合にDRリージョンへの移行を実施するかの条件を決めておく

いつプライマリリージョンに戻すか（FailBack）

・条件：災害復旧時のプライマリリージョンへの復帰条件を決めておく

運用設計 – 移行条件

MKSの事例　FailOver・FailBackの条件

FailOver条件

・**構築開始条件**:障害発生から**6時間以上**プライマリリージョンでサービスが利用出来ない障害（※）が継続しており、復旧の目処が立っていない場合

・**移行条件**　:障害発生から**12時間以上**プライマリリージョンでサービスが利用出来ない障害（※）が継続しており、復旧の目処が立っていない場合

（※ ）ユーザーが障害によってMKSを利用した業務が実施出来ないこと ex. APIの接続や、管理画面へのアクセスが出来ない等

（構築・移行時共に）AWSサポートに連絡し、AWS側で復旧の目処が立っていないことを確認する

FailBack条件

・**移行条件**　:DRリージョン移行後、プライマリリージョンが完全復旧した翌営業日以降にプライマリリージョンへの移行作業を実施

AWSサポートに連絡し、AWS側で復旧が確認できていることを確認する

運用設計

緊急時対応計画ガイド

緊急時の対応計画を規定する

・災害発生時にはDRリージョンへの移行、インシデント連絡など、都度判断をして行動をしなければならない

・災害時に判断基準となるガイドブックを用意しておく事で、災害の混乱時に誤った判断のリスクの軽減や、知識の俗人化などを防ぐ事が出来る

MKSの事例

緊急時対応計画ガイド

手順緊急時対応ガイドでの手順

#	ステップ	概要
1	安全確保	自身含めた安全確保を行い定められた安否報告を行う
2	インフラ状況把握	作業端末とインターネットが利用できるか確認する ※利用できない場合は、災害対策本部に指示を仰ぐ
3	チーム担当者状況確認	チームとしての業務が可能か確認及び報告をする
4	本番環境状況把握	作業可能な人員を把握した上で、各種監視ツール等を用い 本番環境の状況を把握する アベイラビリティゾーンの利用可否を確認する 東京リージョン自体が利用不可の場合は、RedBookを参照
5	状況共有	把握した状況を、MKS 関係者へ報告する その後、Newsサイトを通じ状況を周知する
6	本番環境の復旧	FailOver条件に該当する場合、手順書に従いDRリージョンへの構築作業を実施し、移行する。 FailBack条件を満たした場合、手順書に従いプライマリリージョンへの移行作業を実施する
7	運用基盤の復旧	監視の復旧、運用基盤の復旧 復旧後環境に対する下記作業可否の確認 オートリカバリー、適用（migration、war）、DBバックアップ、CloudWatchでのログモニタリング

アジェンダ

01 はじめに
会社紹介 / サービス紹介 / 想定対象者 / 用語解説

02 事前検討
DRが必要な状況 / 過去のAWS障害 / 現在の災害対策の状態を把握する

03 アーキテクチャ設計
復旧時のアーキテクチャ選択/ アプリケーション層と永続層/ 永続層の設計

04 運用設計
FailOver・FailBackの移行条件 / 緊急時対応計画ガイド

05 災害訓練
BCPテスト

災害訓練

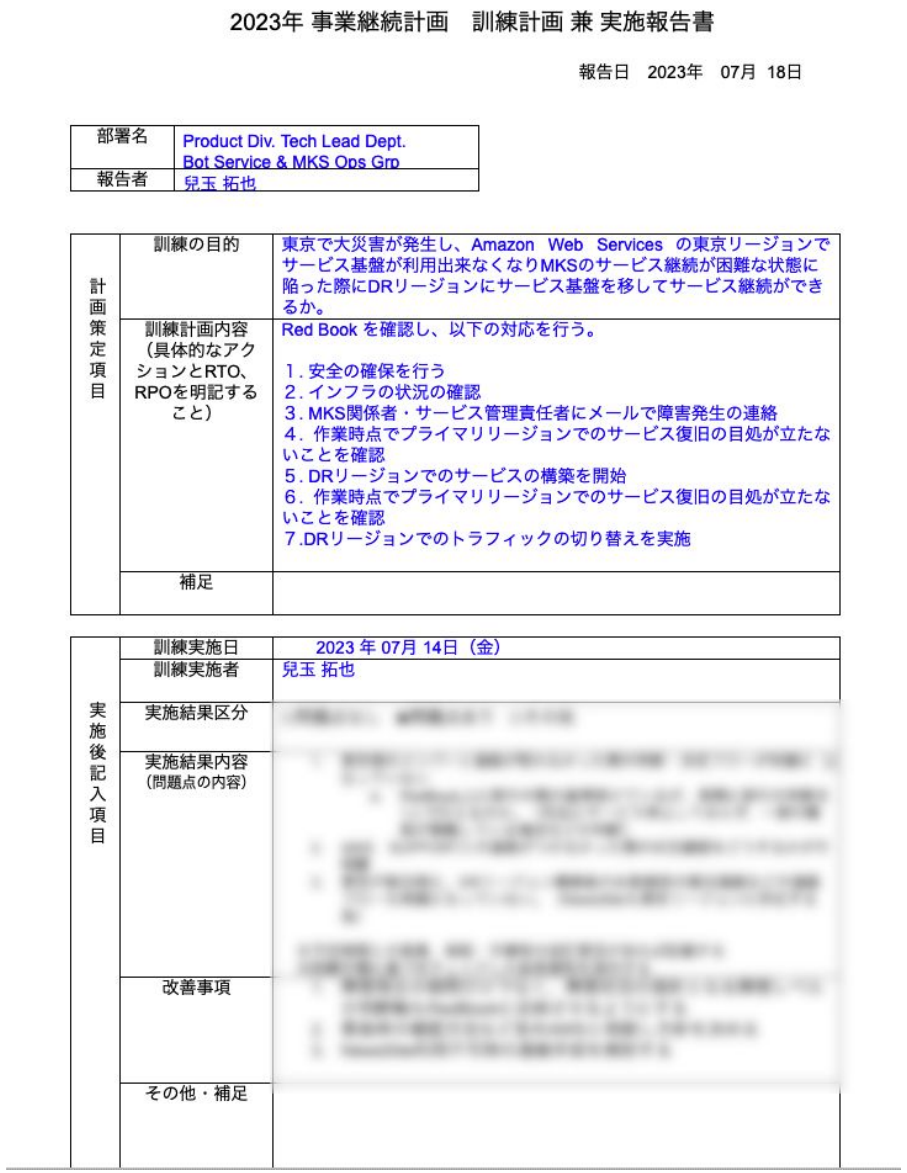
BCPテストの実施

大規模災害想定のBCPテスト

・大規模災害を想定した年1回のBCPテストを実施

・DR対応や、移行時の規定を決めていても災害時に
どのように動くべきかを訓練しておく必要がある

・BCPテストを実施することで課題点も見えてくる



2023年 事業継続計画　訓練計画 兼 実施報告書

報告日　2023年　07月 18日

部署名		Product Div. Tech Lead Dept. Bot Service & MKS Ops Grp
報告者		兒玉 拓也

計画策定項目	訓練の目的	東京で大災害が発生し、Amazon Web Services の東京リージョンでサービス基盤が利用出来なくなりMKSのサービス継続が困難な状態に陥った際にDRリージョンにサービス基盤を移してサービス継続ができるか。
	訓練計画内容（具体的なアクションとRTO、RPOを明記すること）	Red Book を確認し、以下の対応を行う。 1. 安全の確保を行う 2. インフラの状況の確認 3. MKS関係者・サービス管理責任者にメールで障害発生の連絡 4. 作業時点でプライマリリージョンでのサービス復旧の目処が立たないことを確認 5. DRリージョンでのサービスの構築を開始 6. 作業時点でプライマリリージョンでのサービス復旧の目処が立たないことを確認 7.DRリージョンでのトラフィックの切り替えを実施
	補足	

実施後記入項目	訓練実施日	2023 年 07月 14日（金）
	訓練実施者	兒玉 拓也
	実施結果区分	
	実施結果内容（問題点の内容）	
	改善事項	
	その他・補足	

人に真価を。

企業と従業員の間にある様々な障害・不整合を解消し、
すべての人が真価を発揮する社会を実現する