

# AWS Black Belt Online Seminar

## AWS Backup で考える DR 戦略 #1 基本編

小島 七海

Cloud Support Engineer

2025/03



# 自己紹介

## 小島 七海

アマゾン ウェブ サービス ジャパン合同会社  
技術支援本部 クラウドサポートエンジニア



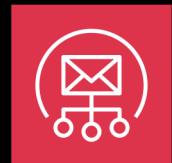
### 好きな AWS サービス



AWS Backup



Amazon Simple Storage  
Service (Amazon S3)



Amazon Simple Email  
Service (Amazon SES)

# AWS Black Belt Online Seminar とは

- ・ 「サービス別」「ソリューション別」「業種別」などのテーマに分け、  
アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- ・ AWS の技術担当者が、 AWS の各サービスやソリューションについてテーマごとに動画を公開します
- ・ 以下の URL より、過去のセミナー含めた資料などをダウンロードすることができます
  - > <https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/>
  - > <https://www.youtube.com/playlist?list=PLzWGOASvSx6FlwIC2X1nObr1KcMCBBlqY>



ご感想は X (Twitter) へ！ハッシュタグは以下をご利用ください  
#awsblackbelt

# 内容についての注意点

- ・ 本資料では資料作成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。AWS のサービスは常にアップデートを続けているため、最新の情報は AWS 公式ウェブサイト (<https://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には別途消費税をご請求させていただきます
- ・ 技術的な内容に関しては、有料の [AWS サポート窓口](#)へお問い合わせください
- ・ 料金面でのお問い合わせに関しては、[カスタマーサポート窓口](#)へお問い合わせください (マネジメントコンソールへのログインが必要です)

# 本セミナーの対象者

## 対象者

- DR 戦略において AWS Backup がどのように活用できるか知りたい方
- AWS Backup を用いたバックアップ方法を学びたい方

# アジェンダ

1. AWS における DR 戦略
2. AWS Backup の概要
3. AWS Backup の DR への応用
4. まとめ

# AWS における DR 戦略

# 災害対策 (Disaster Recovery: DR) の重要性

## 災害による被害シナリオとは？

- 広範囲での障害やシステムの停止が発生し、ワークフローがビジネス目標を達成することが困難となるイベント

## 想定する災害の例

- 地震や洪水などの自然災害
- 大規模停電や広域ネットワークなど、社会のインフラ設備障害
- 不注意による設定ミス、不正アクセス/外部からのアクセス、改ざんなどの人的行為

災害が発生してもサービスの中斷を最小限に抑えられるようあらかじめ **DR** 戦略を準備しておくことが重要

# DR と High Availability の違い

	DR	High Availability
対象	発生確率は小さいがビジネス影響が甚大となる災害への対策	コンポーネントの障害、ネットワーク障害、負荷のスパイクなど災害と比較し頻度は高い障害への対策
このセミナーでの具体例	リージョン単位に着目したソリューション	AZ 単位以下に着目したソリューション
目標	個々の災害イベントに対する目標で、RTO/RPO といった時間が基準	可用性 99.99 といった一定期間のメトリクスが基準

本セミナーでは DR におけるバックアップ & リストアで  
賄うことのできるビジネス継続にフォーカス

# DR における AWS の強み

## オンプレミス

1. 初期投資が必要
  - データセンターやサーバーの確保などが必要
2. 設備維持コストがかかる
  - インフラ維持費が必要
3. 運用手順が煩雑
  - インフラ運用に手間がかかる



## AWS

1. 初期投資が不要
  - 必要なリソースをオンデマンドで提供
2. 設備維持コストを最小化
  - 必要時のみ立ち上げることで、平常時のコストを最小化
  - 使用した分だけの料金
3. 豊富なマネージドサービス
  - 手間のかかるインフラ運用を削減
  - AWS CloudFormation や AWS CDKなどを活用することで手順の自動化も可能

# DR の検討事項

RPO

(Recovery Point Objective: 目標復旧時点)

最後の復旧可能時点からサービス中断までの間に  
どの程度のデータ損失を許容するか

RTO

(Recovery Time Objective: 目標復旧時間)

サービスの中断から復旧までに  
どの程度の時間を許容するか



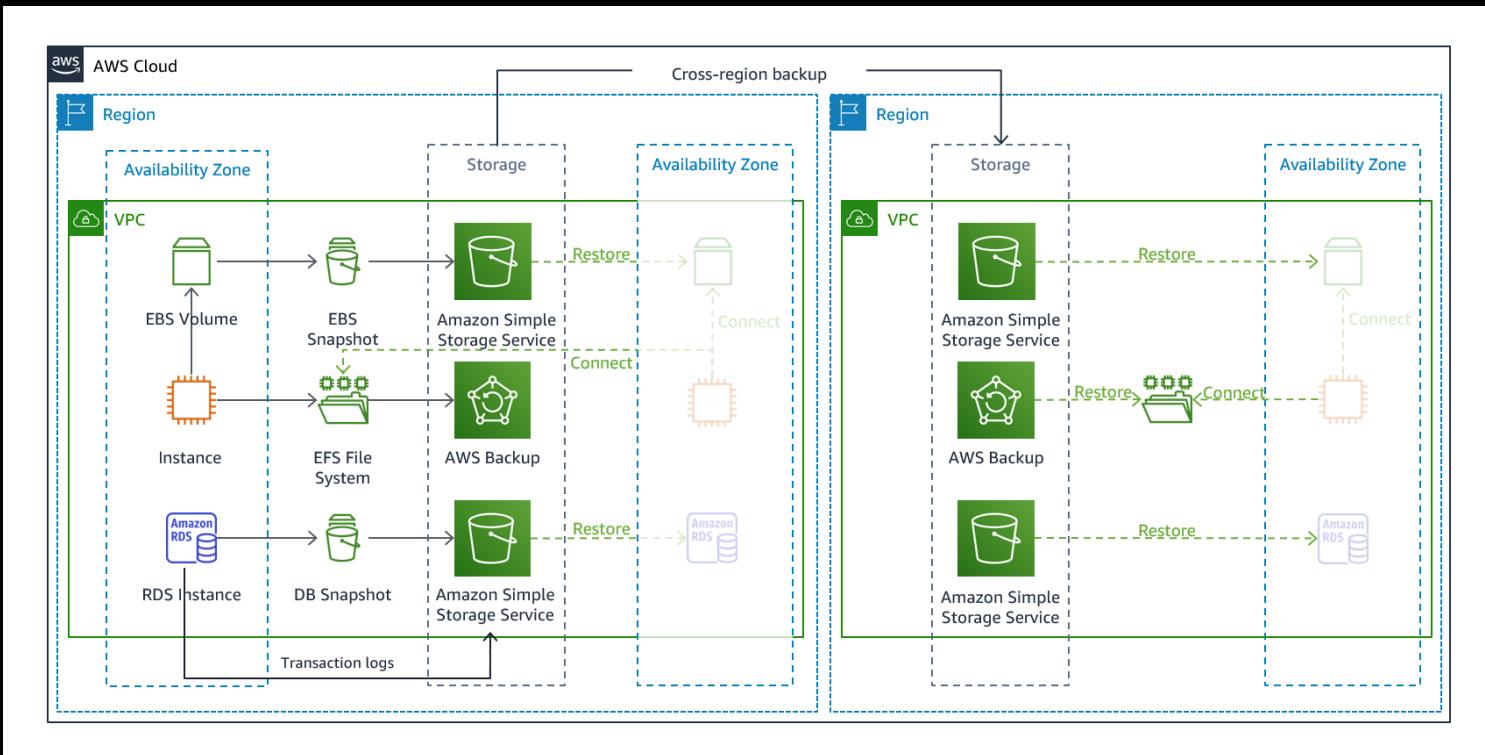
# AWS 上での DR における 4 つのシナリオ

バックアップ&リストア	パイロットライト	ウォームスタンバイ	マルチサイトアクティブ/アクティブ
RPO / RTO: Hours	RPO / RTO: 10s of minutes	RPO / RTO: Minutes	RPO / RTO: Real-time
<ul style="list-style-type: none"><li>データ/アプリケーションのバックアップ</li><li>イベント発生後リソースをプロビジョニング</li><li>費用 \$</li></ul>	<ul style="list-style-type: none"><li>データのレプリケーション</li><li>コア要素の実行環境のみプロビジョニング</li><li>費用 \$\$</li></ul>	<ul style="list-style-type: none"><li>本番環境のスケールダウンしたコピーを別リージョンで稼働</li><li>費用 \$\$\$</li></ul>	<ul style="list-style-type: none"><li>ワークロードを複数のリージョンで同時に実行</li><li>費用 \$\$\$\$\$</li></ul>

本セミナーでは  
こちらにフォーカス

# バックアップ & リストアとは

- ・データの損失や破損を軽減するために適したアプローチ
- ・他の AWS リージョンにデータをレプリケートすることによる別リージョンでの復旧や、操作ミス・設定ミスからの回復に備えるために使用
- ・データに加え、インフラストラクチャ、設定、アプリケーションコードを復旧先リージョンにデプロイする
- ・インフラストラクチャについては AWS CloudFormation や AWS CDK などを使用してデプロイ



[https://docs.aws.amazon.com/ja\\_jp/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html#backup-and-restore](https://docs.aws.amazon.com/ja_jp/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html#backup-and-restore)

# データのバックアップ & リストアのプロセス

## バックアップの設計

- ・ワークフローにおける全てのデータソースを特定
- ・データソースを重要性に基づいて分類
- ・バックアップの必要性を評価
- ・バックアップの頻度、保持期間を決定
- ・バックアップ取得方法の決定

## バックアップの保護

- ・バックアップに対するアクセス制御を設定
- ・バックアップを暗号化

## バックアップの自動化

- ・RPO をもとにバックアップが自動で行われるよう設定

## バックアップの復旧

- ・復元手順の確認
- ・復元可能であるかの確認
- ・定期的に復旧し、RPO/RTO を満たすか検証
- ・復旧プロセスの自動化

詳細なプロセスは AWS Well-Architected フレームワークを参照ください:  
[https://docs.aws.amazon.com/ja\\_jp/wellarchitected/latest/reliability-pillar/back-up-data.html](https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/back-up-data.html)

# AWS Backup の概要

# AWS Backup とは

AWS サービス全体のデータのバックアップを一元的にオーケストレーションし、自動化できるフルマネージドバックアップサービス



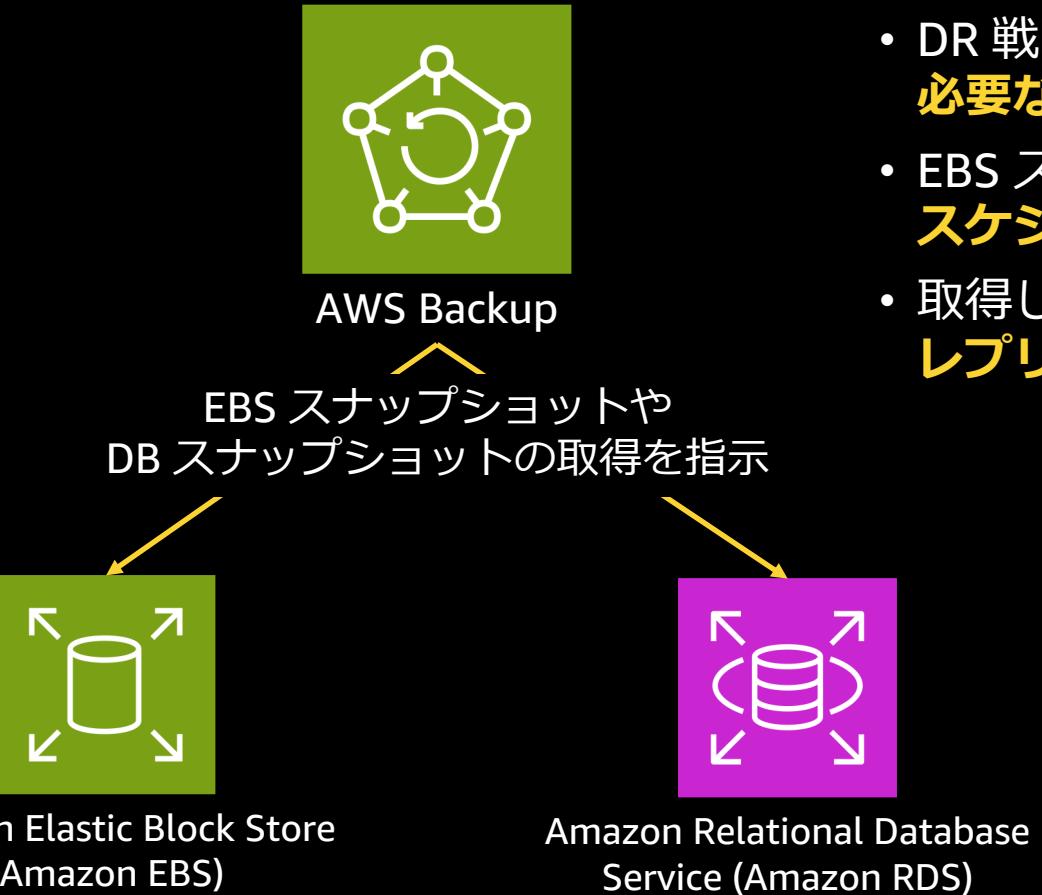
AWS Backup

AWS とハイブリッドサービス上のアプリケーションリソース  
データ保護を簡素化

DR と事業継続の基盤を構築

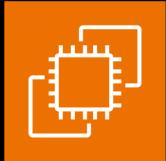
ランサムウェアやアカウントの侵害から保護およびリカバリする  
データ保護コンプライアンスを管理する

# DR 戦略における AWS Backup の位置付け



- DR 戰略におけるデータのバックアップ & リストアに必要なプロセスをマネージドに実現
- EBS スナップショットや DB スナップショット等の取得をスケジュールに従って AWS Backup が指示
- 取得したスナップショットを AWS Backup が管理し、レプリケーションや復元までサポート

# 対応 AWS サービス



Amazon Elastic Compute  
Cloud (Amazon EC2)



VMware Cloud on AWS



Amazon Elastic Block Store  
(Amazon EBS)



Amazon Simple Storage  
Service (Amazon S3)



Amazon Elastic File System  
(Amazon EFS)



AWS Storage  
Gateway



Amazon FSx  
for Lustre



Amazon FSx for  
Windows File Server



Amazon FSx for NetApp  
ONTAP



Amazon FSx for OpenZFS



Amazon Redshift



AWS CloudFormation



Amazon Aurora



Amazon DocumentDB  
(with MongoDB compatibility)



Amazon DynamoDB



Amazon Neptune

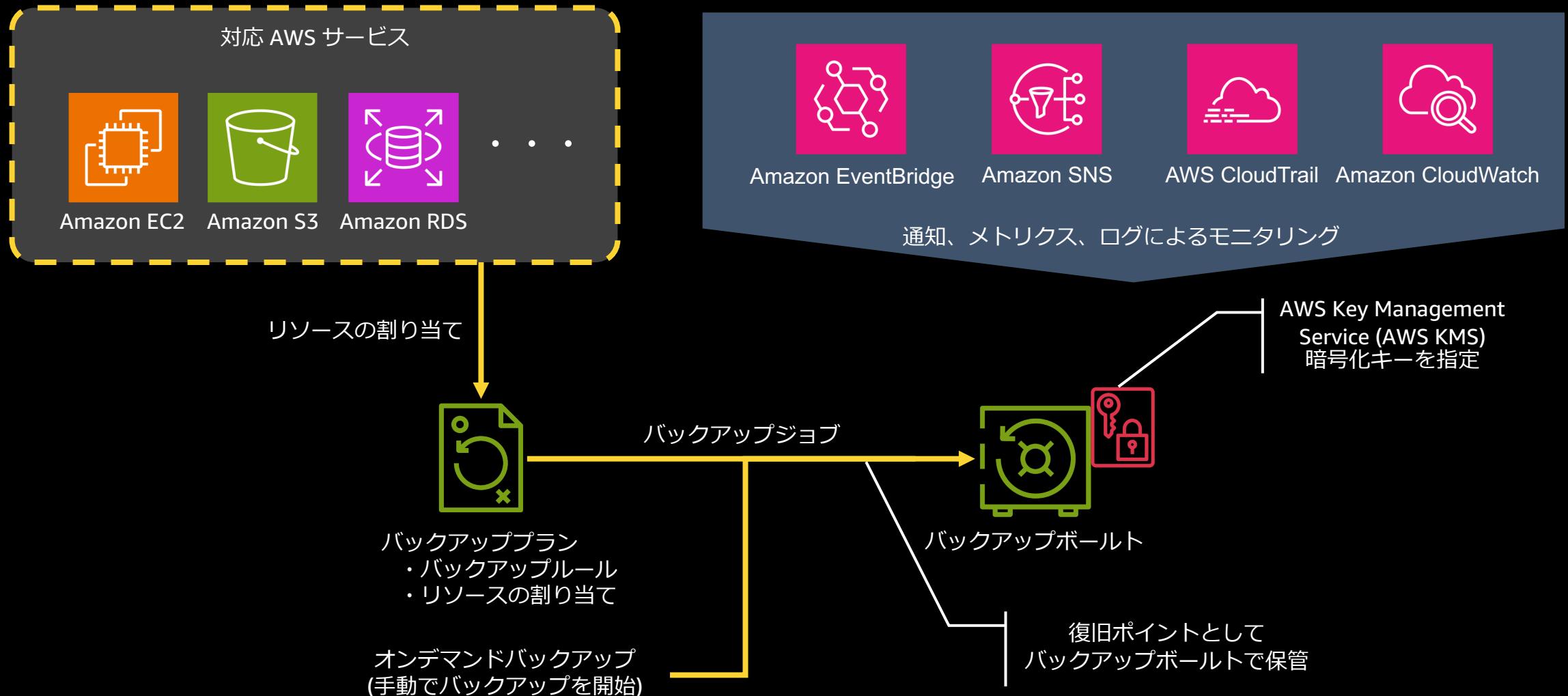


Amazon Timestream



Amazon Relational Database  
Service (Amazon RDS)

# AWS Backup の基本アーキテクチャ



# AWS Backup で使用される用語

バックアップボルト	バックアップを保存および整理するためのコンテナ（入れ物）
バックアッププラン	AWS リソースをいつどのようにバックアップするかを定めるポリシー「バックアップルール」と「リソースの割り当て」を設定
バックアップルール	バックアップスケジュールやバックアップウィンドウ、バックアップの保持期間を定義するルール
リソースの割り当て	バックアップ対象リソースの定義
復旧ポイント	取得された個々のバックアップを指し、バックアップボルトで管理される
保持期間	バックアップルールごとに、復旧ポイントを保存する期間である保持期間を設定 この期間を過ぎた復旧ポイントは自動的に AWS Backup が削除する

※ 2025 年 3 月現在、バックアップルール作成において、保持期間を世代数ベースで行うことはできません。  
取得頻度と保持期間から逆算する必要があります。

# AWS Backup の料金

AWS Backup では以下に対して支払いが発生し、最低利用料金および初期費用は不要

- 使用するバックアップストレージ
- AWS リージョン間で転送されるバックアップデータのデータ転送料金
- 復元するバックアップデータ
- 復元テストの評価
- Backup search, Backup Audit Manager (本セミナーでは扱っておりません)

リソースタイプに応じて料金は異なりますので、詳細は AWS 公式ウェブサイトをご参照ください。

<https://aws.amazon.com/jp/backup/pricing/>

# AWS Backup の DR への応用

# データのバックアップ & リストアのプロセス

再掲

## バックアップの設計

- ・ワークフローにおける全てのデータソースを特定
- ・データソースを重要性に基づいて分類
- ・バックアップの必要性を評価
- ・バックアップの頻度、保持期間を決定
- ・バックアップ取得方法の決定

## バックアップの保護

- ・バックアップに対するアクセス制御を設定
- ・バックアップを暗号化

## バックアップの自動化

- ・RPO をもとにバックアップが自動で行われるよう設定

## バックアップの復旧

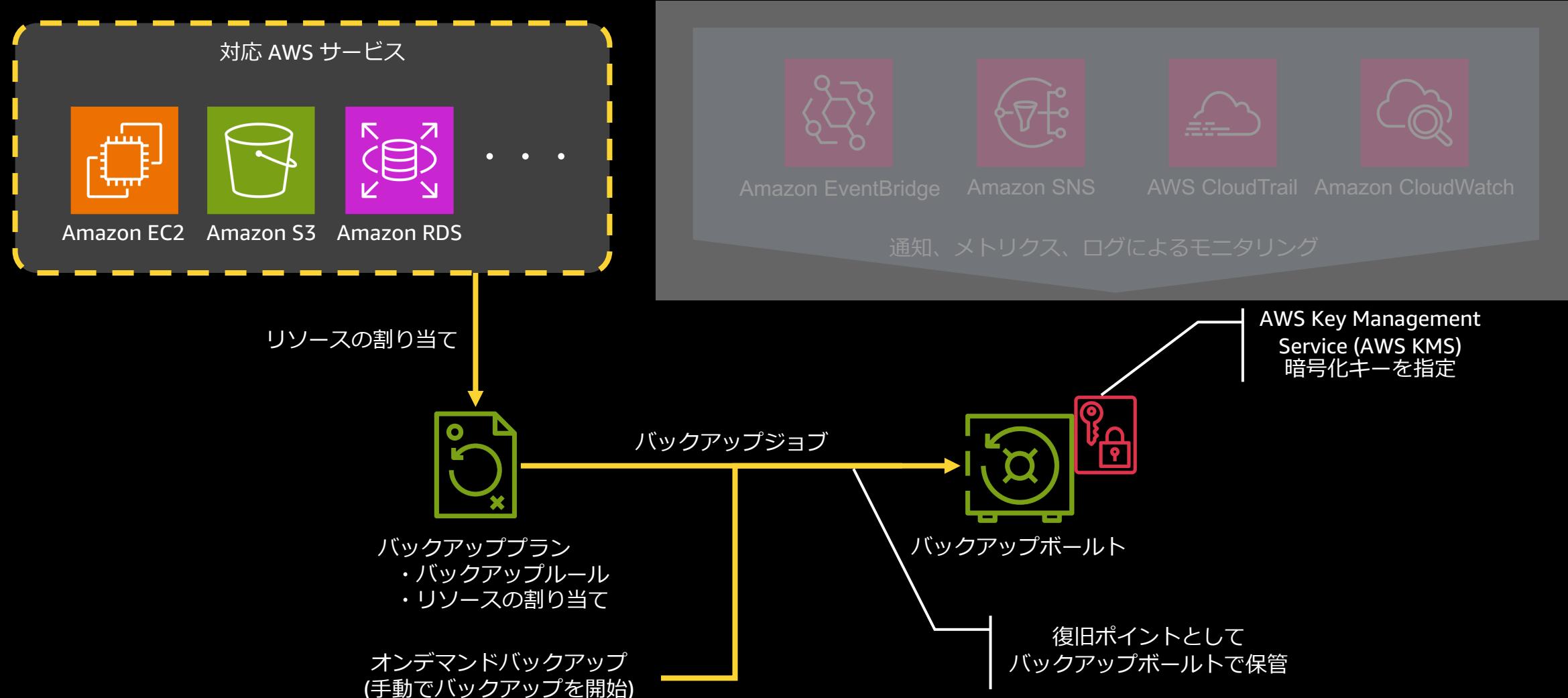
- ・復元手順の確認
- ・復元可能であるかの確認
- ・定期的に復旧し、RPO/RTO を満たすか検証
- ・復旧プロセスの自動化

詳細なプロセスは AWS Well-Architected フレームワークを参照ください:  
[https://docs.aws.amazon.com/ja\\_jp/wellarchitected/latest/reliability-pillar/back-up-data.html](https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/reliability-pillar/back-up-data.html)



# AWS Backup の基本アーキテクチャ

再掲



# バックアップボルト

バックアップの設計

バックアップの保護

バックアップの自動化

バックアップの復旧

ボルトを作成 情報

全般

ボルト名  
BackupVault\_Tokyo

ボルト名では大文字と小文字が区別されます。2~50 文字の英数字または「\_」を含める必要があります。

ボルトタイプ

バックアップボルト  
バックアップボルトには、リースインスタンスとは別のイミュータブルなバックアップが保存されます。

- 暗号化キーはお客様が管理するか、AWS が管理します
- ボルトロックはオプションです

論理的にエアギャップのあるボルト  
論理的にエアギャップのあるボルトには、バックアップのコピーが保存されます。

- 暗号化キーは AWS が所有しており、削除できません
- 直接復元をサポートするアカウント間および組織間の共有
- ボルトロックは必須です

暗号化キー | 情報

(デフォルト) aws/backup

説明	アカウント	キー ID	ステータス
Default key that protects my Backup data when no other key is defined	このアカウント	[REDACTED]	有効

ボルトタグ - オプション

ここで指定するタグは、ボルトの整理と追跡に役立ちます。

このボルトにはタグが関連付けられていません。

新しいタグを追加

最大 50 個のタグをさらに追加できます。

キャンセル ボルトを作成

- 復旧ポイント（バックアップ）を保存および整理するコンテナ
- 作成時にはボルト名と AWS KMS 暗号化キーを指定
  - デフォルトでは aws/backup の KMS キーを使用
  - カスタマーマネージドキーも使用可能

(注) バックアップボルトで指定した暗号化キーは特定のリソースタイプのバックアップのみに適用されます。  
対象外となるリソースタイプの場合は、元となるリソースの暗号化に使用されたキーを使用してバックアップを暗号化します。

[https://docs.aws.amazon.com/ja\\_jp/aws-backup/latest/devguide/encryption.html](https://docs.aws.amazon.com/ja_jp/aws-backup/latest/devguide/encryption.html)



# バックアップポールト

バックアップの設計

バックアップの保護

バックアップの自動化

バックアップの復旧

BackupVault\_Tokyo 情報

概要

ポート名 BackupVault_Tokyo	KMS 暗号化キー ID [REDACTED]	ポートロック -
ポートタイプ バックアップポート	作成日 2025年2月18日, 17:00 (UTC+09:00)	ポートロックの保持期間 最小保持期間: - 最大保持期間: -
ポート ARN <a href="#">arn:aws:backup:ap-northeast-1:[REDACTED]backup-vault:BackupVault_Tokyo</a>		

復旧ポイント | 保護されたリソース

復旧ポイント (1) 情報

復旧ポイント ID	ステータス	リソース名	リソース ID	リソースタイプ	バックアップタイプ
image/ami-[REDACTED]	完了	Test_EC2_Instance	instance/i-[REDACTED]	EC2	イメージ

復旧ポイントを選択して復元操作を行うことで、取得時点の状態にデータを復元

# アクセスポリシー

- ・バックアップポートに割り当てる
- ・バックアップポートや復旧ポイントに対するアクセスを制限することが可能

例) 特定のプリンシパル以外へ復旧ポイントの削除を禁止するポリシー

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Deny",  
      "Principal": "*",  
      "Action": "backup:DeleteRecoveryPoint",  
      "Resource": "*",  
      "Condition": {  
        "ArnNotEquals": {  
          "aws:PrincipalArn": [  
            "arn:aws:iam::112233445566:user/Alice",  
            "arn:aws:iam::112233445566:role/Backup_Admin"  
          ]  
        }  
      }  
    }  
  ]  
}
```



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

バックアップの設計

バックアップの保護

バックアップの自動化

バックアップの復旧

## アクセスポリシーを編集

アクセスポリシーを編集するときは、バックアップポートとそれに含まれるリソースにポリシーを割り当てる事ができます。ポリシーを割り当てる、バックアッププランやオンデマンドバックアップを作成するためのアクセス権をユーザーに付与するなどの操作を実行できますが、作成後に復旧ポイントを削除する権限は制限されます。

### アクセスポリシーの詳細 情報

① ポリシー JSON は、すぐ下で編集できます。 [詳細ははこちら](#)

```
1  [ {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Deny",  
6       "Principal": "*",  
7       "Action": "backup:DeleteRecoveryPoint",  
8       "Resource": "*",  
9       "Condition": {  
10         "ArnNotEquals": {  
11           "aws:PrincipalArn": [  
12             "arn:aws:iam::112233445566:user/Alice",  
13             "arn:aws:iam::112233445566:role/Backup_Admin"  
14           ]  
15         }  
16       }  
17     }  
18   ]  
19 }
```

ポリシージェネレータ [\[ \]](#) を使用して、ポリシーの許可を構築できます。

キャンセル

ポリシーを保存

# バックアッププラン ～バックアップルール～

バックアップの設計

バックアップの保護

バックアップの自動化

バックアップの復旧

バックアップルールの設定 [情報](#)

スケジュール

バックアップルール名

バックアップルール名では大文字と小文字が区別されます。1~50 文字の英数字または「\_」を含める必要があります。

バックアップボートルト [情報](#)   [新しいボートルトを作成](#) 

バックアップボートルト

バックアップ頻度 [情報](#)

バックアップ期間 [情報](#)

開始時間

バックアップを開始する時刻を指定します。時間単位の頻度では、開始時刻は 1 日のうちで初めてバックアップが作成される時刻です。該当する場合、時刻はサマータイムに合わせて調整され、1 年を通して同じ現地時間が維持されます。

:

次の時間以内に開始 [情報](#)

指定した時間にバックアッププランが開始されない場合は、バックアッププランが開始される期間を指定します。

次の時間以内に完了 [情報](#)

合計保持期間 [情報](#)  
バックアップを保存する期間を AWS Backup に指示します。



合計保持 (日)

  
0 10 20 30 40 50 60 70 80 90 100

■ ウォームストレージ

コピー先にコピー - オプション [情報](#)

別のバックアップボートルトまたは論理的にエアギャップのあるボートルトにバックアップのコピーを作成します。

リージョン   

別のアカウントのボートルトにコピー

送信先ボートルト

バックアップコピーが作成されるボートルト。  
  [新しいボートルトを作成](#) 

バックアップボートルト

ライフサイクル

追加のバックアップコピーの合計保持期間とコールドストレージ設定を指定します。

バックアップルールと同じ設定を使用する  
コールドストレージ: 有効になっていません; 合計保持期間: 5 週

ライフサイクルをカスタマイズ

[コピーを追加](#)



# バックアッププラン ~リソースの割り当て~

バックアップの設計

バックアップの保護

バックアップの自動化

バックアップの復旧

**リソースの選択** 情報  
タグとリソース ID を使用して、このバックアッププランにリソースを割り当てます。

**1. リソース選択を定義** 情報  
すべてのリソースを保護するか、タイプまたは ID でリソースを指定します。

すべてのリソースタイプを含める  
アカウントで有効になっているすべてのリソースタイプを保護します。

特定のリソースタイプを含める  
タイプ別にリソースを選択するか、ID で個別のリソースを指定します。

**2. 特定のリソースタイプを選択** 情報  
このバックアップ計画で保護する特定のリソースタイプを選択します。特定のリソース ID を選択から除外することもできます。

リソースタイプを選択 ▾

**3. 選択したリソースタイプから特定のリソース ID を除外する - オプション** 情報  
この割り当てから除外する特定のリソース ID を選択します。

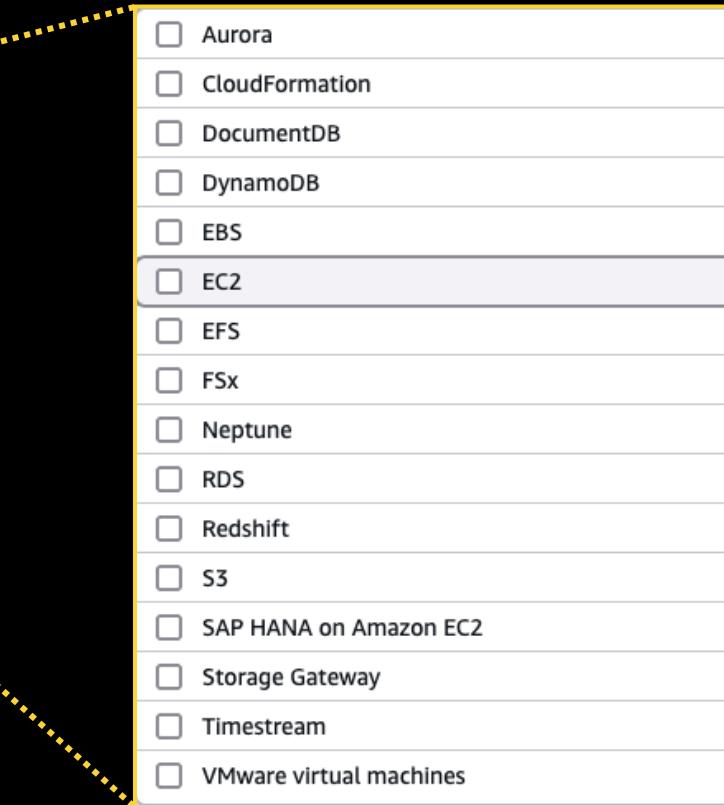
リソースタイプを選択 ▾

**4. タグを使用して選択を絞り込む - オプション** 情報  
タグでリソースをフィルタリングします。タグが複数ある場合、リソースはすべてのタグ条件を満たす場合にのみバックアッププランに割り当てられます。

リソースの選択を絞り込むためのタグが選択されていません。

タグを追加

最大 30 個のタグを追加できます。



特定のリソースタイプ・リソース ID での割り当てや  
特定のタグを持つリソースを割り当てることが可能

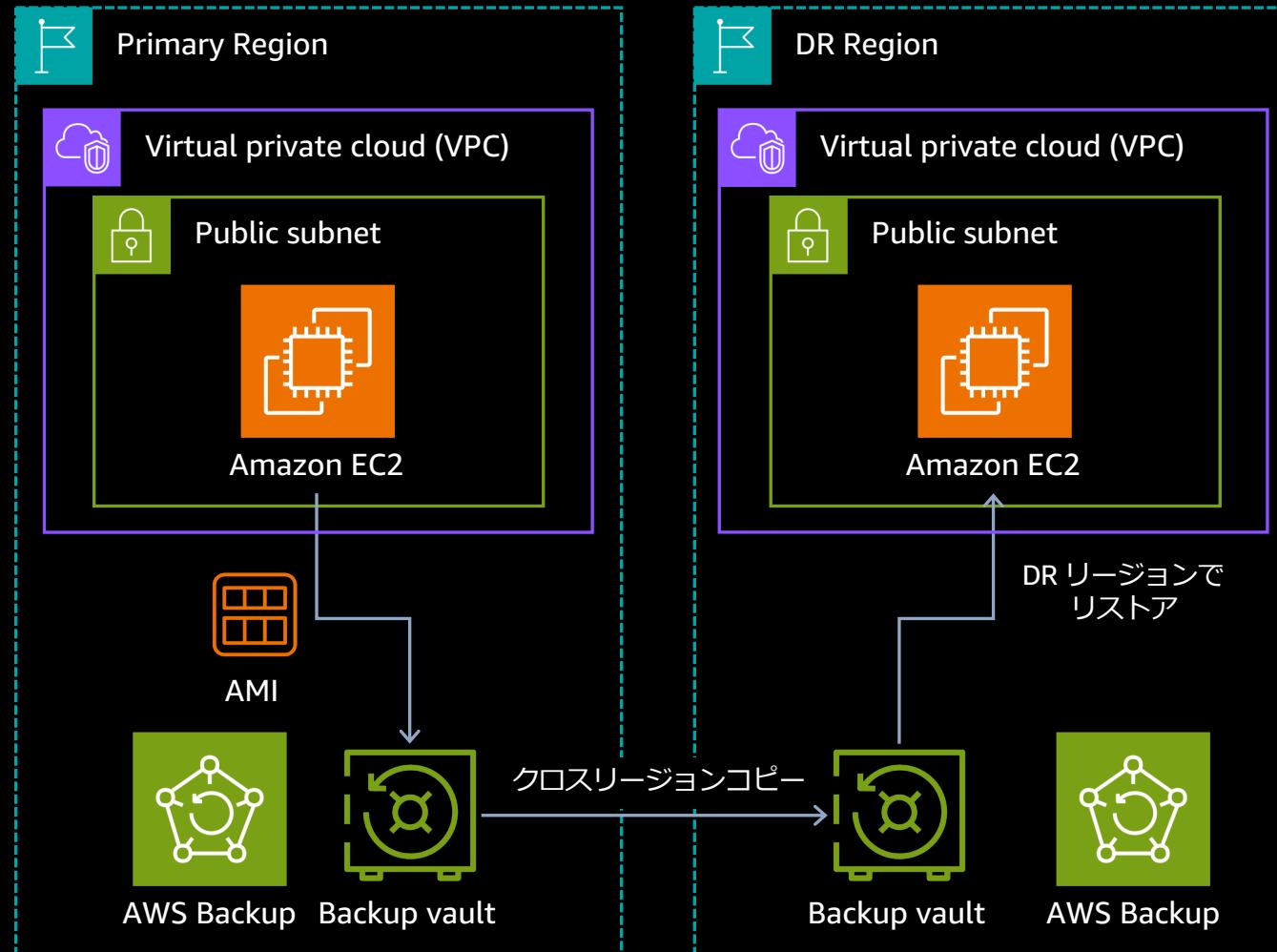
# クロスリージョンコピー

バックアップの設計

バックアップの保護

バックアップの自動化

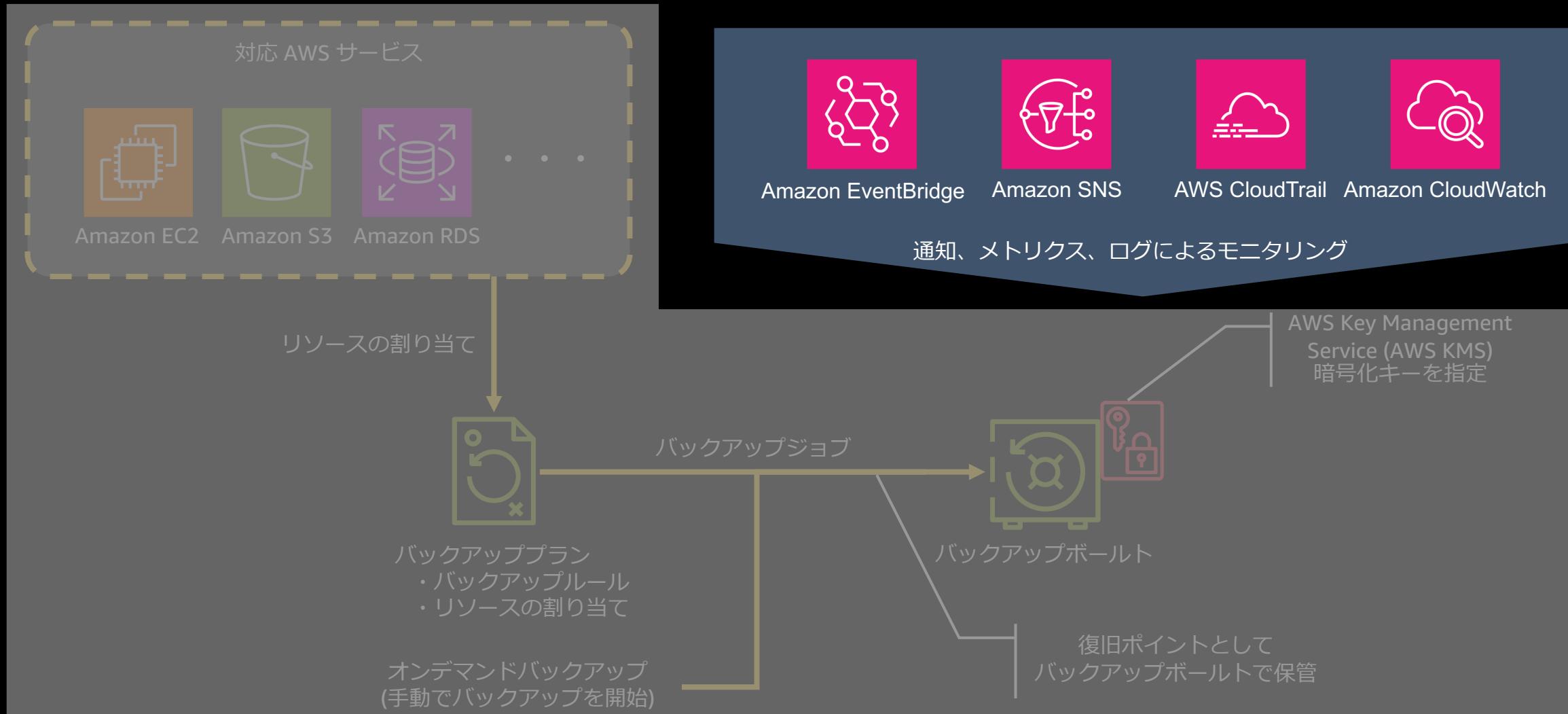
バックアップの復旧



- ・バックアップルールでクロスリージョンコピーの設定が可能
- ・Primary Region でバックアップ取得後、指定した DR リージョンのバックアップポールトへ復旧ポイントをコピー
- ・Primary Region 被災時は DR リージョンにコピーした復旧ポイントからリストアし、ワークロードを復旧
- ・あくまでデータの復旧がメインであるため、インフラストラクチャなどについては別途検討が必要

# AWS Backup の基本アーキテクチャ

再掲



# モニタリング

バックアップの設計

バックアップの保護

バックアップの自動化

バックアップの復旧



Amazon EventBridge

AWS Backup のバックアップジョブなどの状態が変更された時に発生するイベントをモニタリング



AWS CloudTrail

AWS Backup API コールをイベントとしてキャプチャ



Amazon SNS

バックアップジョブやコピージョブなどのイベントを通知



Amazon CloudWatch

AWS Backup メトリクスのモニタリング



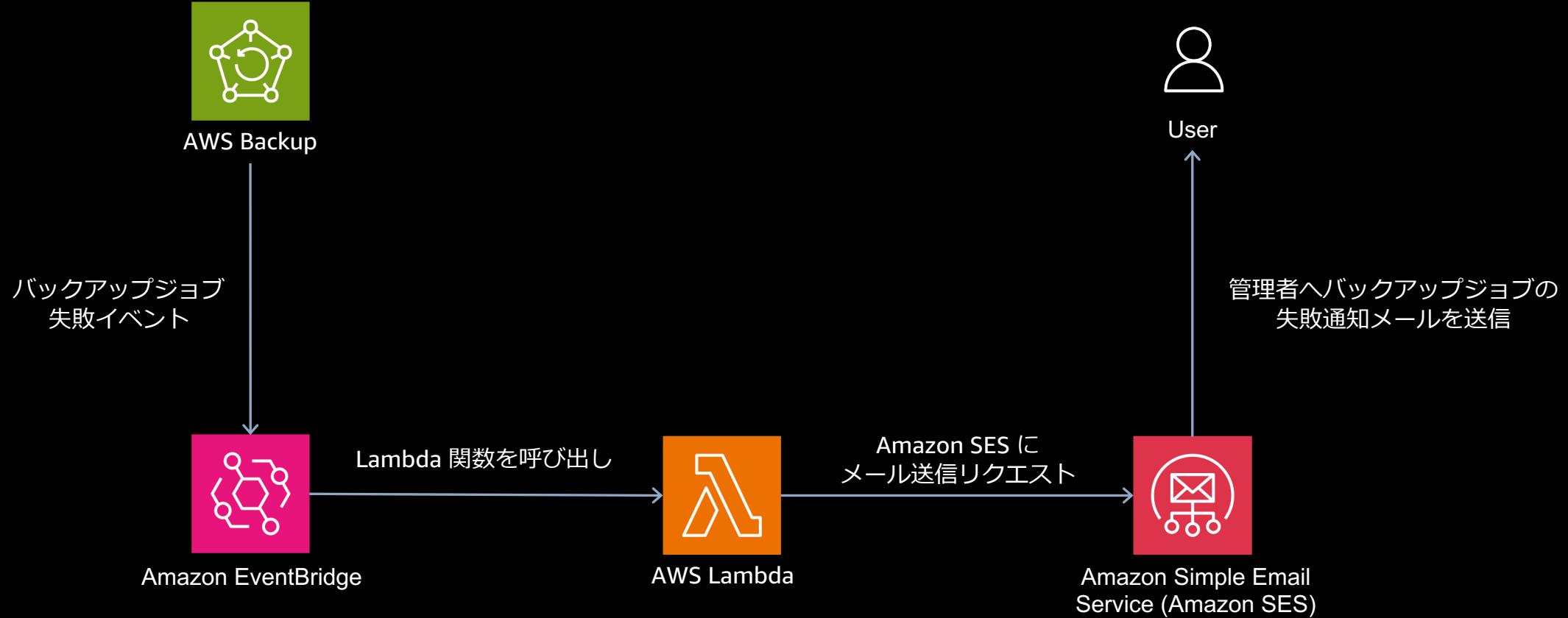
# モニタリング

バックアップの設計

バックアップの保護

バックアップの自動化

バックアップの復旧



# 復元

バックアップの設計

バックアップの保護

バックアップの自動化

バックアップの復旧

## バックアップを復元

EC2 インスタンスを復元して、スケジュール済みバックアップ、ライフサイクル管理、迅速な復元などの主要な機能を使用しながら、他のリソースでバックアップを一元管理できるようにします。インスタンス全体の復元機能にアクセスするには、次に移動してください。[インスタンス起動ウィザード](#)

### ネットワーク設定

#### インスタンスタイプ 情報

インスタンスの計算容量とメモリ容量を定義します。

t2.micro - 1 vCPU, 1 GiB RAM

#### 仮想プライベートクラウド (VPC)

VPC を選択して、仮想ネットワーキング環境を定義します。

デフォルトの VPC [REDACTED]



#### サブネット 情報

異なる EC2 リソースを相互またはインターネットから分離するために使用できる VPC の IP アドレスの範囲を指定します。各サブネットは 1 つのアベイラビリティーゾーンに存在します。

指定なし (任意のアベイラビリティーゾーンのデフォルトサブネット)



#### セキュリティグループ 情報

セキュリティグループを指定して、インスタンスのトラフィックを制御するファイアウォールルールのセットを決定します。

セキュリティグループを追加



default X

#### インスタンス IAM ロール 情報

EC2 インスタンスに AWS 認証情報を自動的にデプロイする IAM ロールを指定します。

- IAM ロールなしで続行
- 元の IAM ロールで復元

### ▼ 詳細設定

シャットダウンと休止動作、終了保護、プレイスメントグループ、テナンシー、およびその他の詳細設定をカスタマイズします。

#### シャットダウンの動作 情報

OS レベルのシャットダウンを実行したときのインスタンスの動作を指定します。

停止

#### 停止 - 休止動作 情報

- 追加の停止動作として休止を有効化

#### 終了保護を有効化

インスタンスが誤って終了しないように保護します。有効にすると、終了保護が無効になるまで、API または AWS マネジメントコンソールからこのインスタンスを終了することはできません。

#### プレイスメントグループ 情報

1 つのアベイラビリティーゾーン内のインスタンスの論理グループの名前を指定します。この名前は、ネットワークレイテンシーが低く、全体のネットワークが高いという利点があります。

- プレイスマントグループにインスタンスを追加

#### T2/T3 無制限

T2/T3 無制限を有効にすると、アプリケーションはいつでも必要なだけベースラインを超えてペーストできます。インスタンスの平均 CPU 使用率がベースライン以下である場合、すべての使用量に対して時間単位のインスタンス料金が自動的に適用されます。それ以外の場合、ベ

- 復元時には復元先の VPC やインスタンスタイプなどリソースタイプに応じたパラメータを指定して復元
- AWS Backup を使用した復元では、既存リソースを上書きすることではなく、新規リソースが作成される



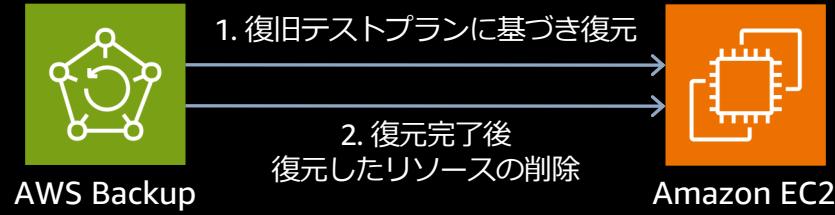
# 復元テスト

バックアップの設計

バックアップの保護

バックアップの自動化

バックアップの復旧



- ・復元テストプランを作成し、プランに含めるリソースを割り当てる
- ・プランで指定されたスケジュールに基づき復元ジョブが作成され、復元の完了にかかる時間をモニタリング
- ・復元テストが終了すると、復元したリソースは自動的に削除される
- ・オプションとして Amazon EventBridge を使用し、AWS Lambda などを呼び出すことで復元したリソースの検証プロセスを自動化可能

(注) 検証プロセスの実現においては、復元した EC2 インスタンスに対してヘルスチェックを行う等の処理を AWS Lambda などで実装いただく必要があります。

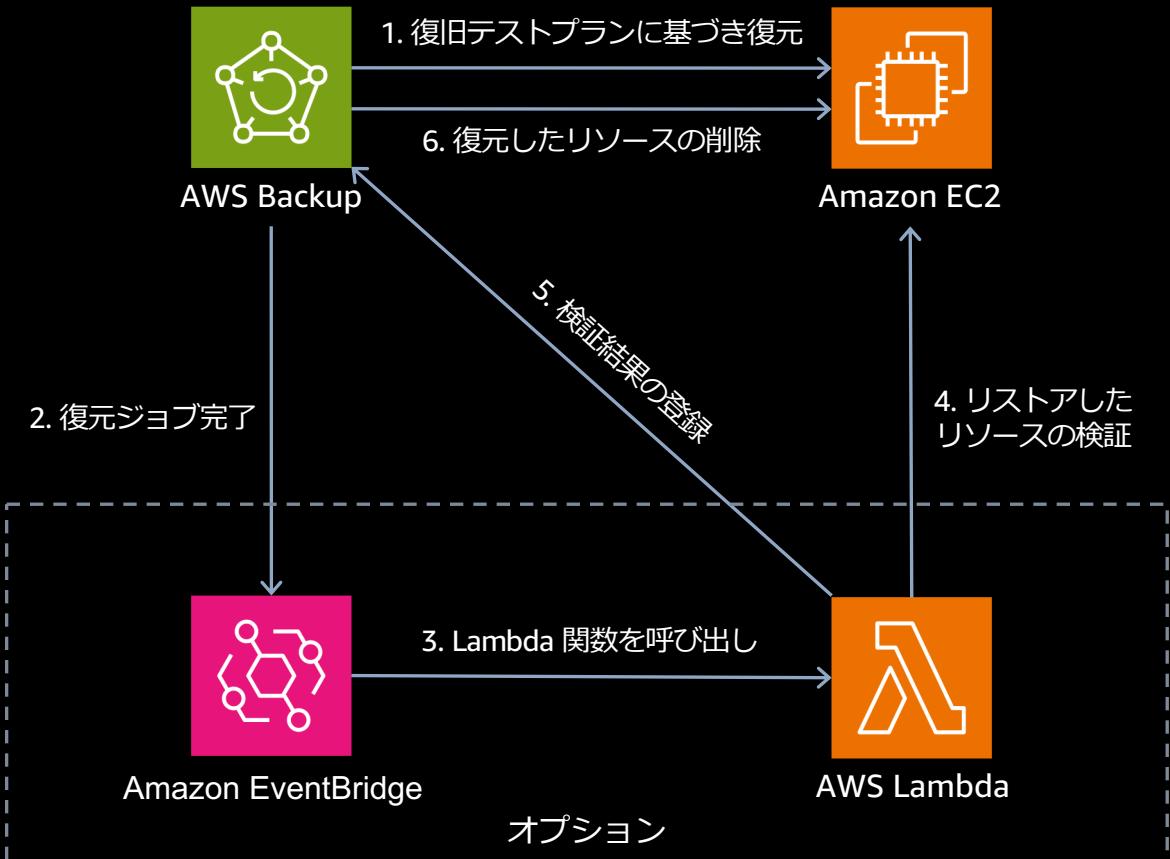
# 復元テスト

バックアップの設計

バックアップの保護

バックアップの自動化

バックアップの復旧



- 復元テストプランを作成し、プランに含めるリソースを割り当てる
- プランで指定されたスケジュールに基づき復元ジョブが作成され、復元の完了にかかる時間をモニタリング
- 復元テストが終了すると、復元したリソースは自動的に削除される
- オプションとして Amazon EventBridge を使用し、AWS Lambda などを呼び出すことで復元したリソースの検証プロセスを自動化可能

(注) 検証プロセスの実現においては、復元した EC2 インスタンスに対してヘルスチェックを行う等の処理を AWS Lambda などで実装いただく必要があります。

# 復元テスト

バックアップの設計

バックアップの保護

バックアップの自動化

バックアップの復旧

## 復元テストプランを作成 情報

頻度、回復ポイント選択ルール、およびその他の項目を指定して、定期的な復元テストを容易に行えるようにします。

### 全般

#### 復元テストプラン名

RestoreTest\_Tokyo

復元テストプラン名では大文字と小文字が区別されます。1~50 文字の英数字またはアンダースコアを含める必要があります。プランの作成後は編集できません。

#### テスト頻度

復元テストプランを実行する頻度を指定します。

毎日

#### 開始時間

復元テストを開始する時刻を指定します。

00 : 30 Asia/Tokyo (UTC+09:00)

#### 次の時間以内に開始

復元ジョブは、指定された時間枠内に開始されます。例えば、8 時間を選択した場合、復元ジョブはプランの開始予定時刻から 8 時間に内にランダムに開始されます。

8 時間

## 回復ポイントの選択 情報

この復元テストプランを実行するときにどの復旧ポイントを復元するかを指定します。

#### ソースポールト

どのポールトから回復ポイントを取得するかを選択します。

- 利用可能なすべてのポールト
- 特定のポールト

#### 特定のポールト

ポールトを選択

BackupVault\_Tokyo

## リソースを割り当てる 情報

この復元テストプランに含める保護されたリソースを、一度に 1 種類ずつ選択してください。

### 全般

#### リソース割り当て名

RestoreTestSelection\_Tokyo

リソースの割り当て名では大文字と小文字が区別されます。1~50 文字の英数字またはアンダースコアを含める必要があります。リソースの割り当てが作成された後は編集できません。

#### IAM ロールを復元

復元テストの実行時に AWS Backup が引き受ける IAM ロールを指定します。

- デフォルトのロール  
AWS Backup のデフォルトのロールが存在しない場合は、正しい許可を持つロールが作成されます。
- IAM ロールを選択してください

#### クリーンアップ前の保持期間 | 情報

復元されたデータが保存される期間（削除されるまでの期間）を指定して、コストを最適化します。クリーンアップ前に検証が必要な場合は、検証の実行に必要な時間を反映するようにこの時間を変更してください。検証が成功すると、データは保持期間にかかわらず削除されます。

- [すぐに削除] を開始
- 特定の時間数について保持

## 保護されたリソース 情報

リソース ID またはタグを使用して、この復元テストプランにリソースを割り当てます。

### リソースタイプ

#### リソースタイプを選択

復元テストプランの一環として復元するリソースタイプを選択します。

EC2

#### リソースの選択の範囲

- このリソースタイプのすべての保護されたリソースを含める
- このリソースタイプの特定の保護されたリソースを含める



# データのバックアップ & リストアのプロセス

バックアップの設計

バックアップの保護

バックアップの自動化

バックアップの復旧

バックアップボルト

アクセスポリシー

バックアッププラン

バックアッププラン

クロスリージョンコピー

復元

復元テスト

データのバックアップ & リストアのプロセスを網羅的に実現

# まとめ

# まとめ

- AWS 上の DR 戦略では、バックアップ&リストア・パイロットライト・ウォームスタンバイ・マルチサイトアクティブ/アクティブの 4 つのシナリオがある
- 目標とする RPO/RTO とコストとのトレードオフで、適用するシナリオを決定する
- バックアップ&リストアは短い RPO/RTO が求められないワークフローに適している
- AWS Backup を使用することでバックアップ&リストアに必要なプロセスをマネージドで実現
- バックアップの取得から復旧プロセスまで一元的に管理・自動化

# まとめ

- 本セミナーでご紹介していない機能については、別の Black Belt Online Seminar で紹介予定です
  - AWS Backup における継続的バックアップ
  - AWS Organizations と統合した組織内アカウントにおけるバックアップの一元管理
  - バックアップポルトロックによるセキュリティの強化
  - Backup Audit Manager によるコンプライアンス要件の監査
  - ...etc

# Thank you!

