AWS Summitミニセッション
「あなたのIaC、今でも動きますか？」

2024/6/20

株式会社NTTデータ

自己紹介

奥村 康晃（Okumura Yasuaki）

NTTデータ データセンタ&クラウドサービス事業部 エグゼクティブITスペシャリスト

ミッション：

クラウド領域における技術リード

先進技術を用いた新規サービスの創出

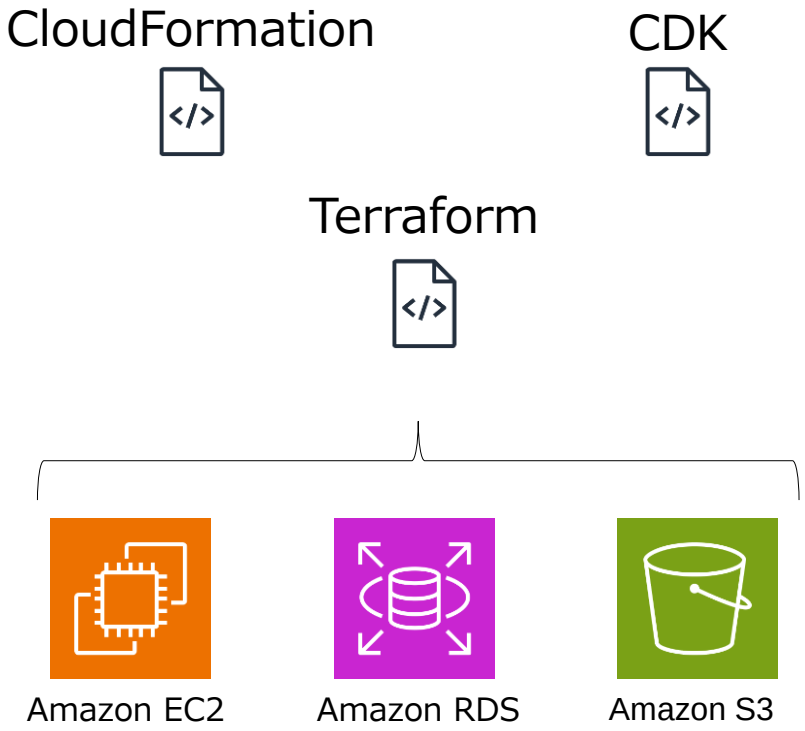
社外活動：

- 2022 APN AWS Top Engineers / 2023 AWS Ambassadors
- AWS Summit Tokyo 2023登壇など
- CodeZine:これだけは押さえておきたい！ AWSサービス最新アップデート[連載中]
- マイナビ Tech+:AWS Organizations連携サービス最新情報＆セットアップのコツ[連載中]

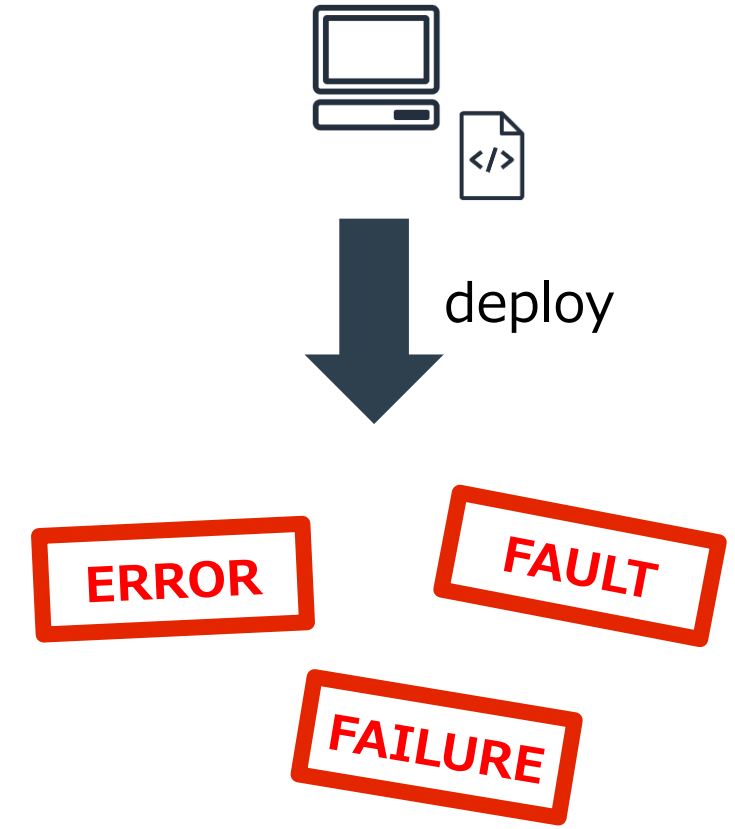
保有資格：

こんなことありませんか？

IaCはやっているから、必要な時に
すぐに作ることができる！



(久しぶりに)デプロイしてみたら、
動かない・・・！



アマゾン ウェブ サービス (AWS)側の仕様変更により、今までのIaCが動作しないことが・・・ 1/2

S3 Block Public Accessがデフォルト有効化

パブリックバケット作成時にコード修正が必要

Amazon Web Services ブログ

お知らせ: Amazon S3 のセキュリティに関する変更が 2023 年 4 月に予定されています

by Jeff Barr | on 22 12月 2022 | in Amazon Simple Storage Service (S3), Announcements, Launch, News, Security, Identity, & Compliance | Permalink | Share

2023 年 4 月より、バケットセキュリティに関する最新のベストプラクティスを自動的に適用するために、Amazon Simple Storage Service (Amazon S3) に 2 つの変更を加えます。この変更は 4 月に有効になり、数週間以内にすべての AWS リージョンに展開される予定です。

(・・・中略・・・)

この変更の観点からは、パブリックバケットや ACL に依存する新しいバケットの作成には、慎重で思慮深いアプローチが推奨されます。また、当社は、ほとんどのアプリケーションではいずれも必要ないと考えています。お客様のアプリケーションがパブリックバケットや ACL を必要とする場合には、以下で説明する変更を加える必要があります (コード、スクリプト、AWS CloudFormation テンプレート、および他のオートメーションを必ず確認してください)。

アマゾン ウェブ サービス (AWS)側の仕様変更により、今までのIaCが動作しないことが・・・ 2/2

IAMの変更

サービスプレフィクスやアクションの廃止

Amazon Web Services ブログ

AWS 請求、コスト管理、アカウントコンソール権限の変更

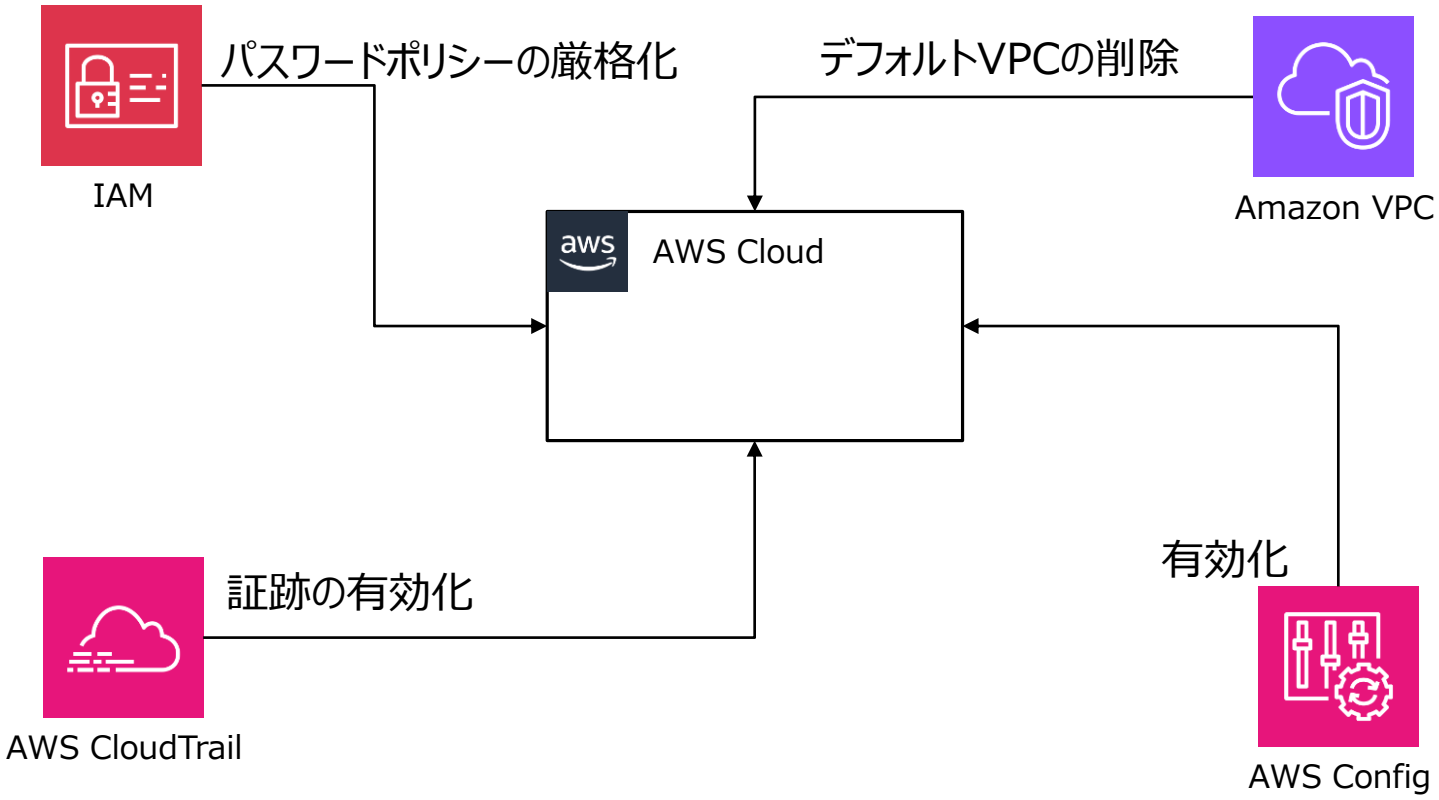
by 前田 賢介(Maeda Kensuke) | on 16 1月 2023 | in Announcements, AWS Cloud Financial Management, AWS Identity and Access Management (IAM), AWS Organizations, Billing & Account Management, Identity, Security, Identity, & Compliance | Permalink | Share

(・・・中略・・・)

AWS はサービスプレフィックス `aws-portal` と、発注書ネームスペースにある 2 つのアクション(`purchase-orders:ViewPurchaseOrders` , `purchase-orders:ModifyPurchaseOrders`)を、請求、コスト管理、およびアカウントコンソールの AWS Identity and Access Management (IAM) アクションから廃止し、請求、コスト管理、およびアカウントサービスへのアクセスをより詳細に制御できる、きめ細かなサービス固有の権限に置き換えました。これらの新しい権限により、コンソールインターフェイスとプログラムインターフェイスの両方へのアクセスを管理する単一の AWS Identity and Access Management (IAM) アクションセットが提供されます。

当社のIaCの例

当社は**最低限必要なセキュリティ設定を実施済みのAWSアカウント**を払い出す
「セキュリティアカウント発行サービス」を提供中
※裏側の設定は実施内容の関係でPython(boto3)で実装



当社のIaCにおける課題

課題１：

多岐にわたるAWSサービスへの設定が必要であり、対象の全AWSサービスの全アップデートを追うことが難しい。**気づかないうちに設定対象のサービス仕様が変わっており、IaCが動作しなくなる**可能性があるのではないか？

課題２：

ベースとしているSecurity HubのAWS 基礎セキュリティ・ベスト・プラクティス (FSBP) 標準に頻繁に更新が入り、**IaCの変更が頻発**するため、動作しなくなる可能性があるのではないか？

(FY2023は72件の更新)

IaCの継続的なテスト

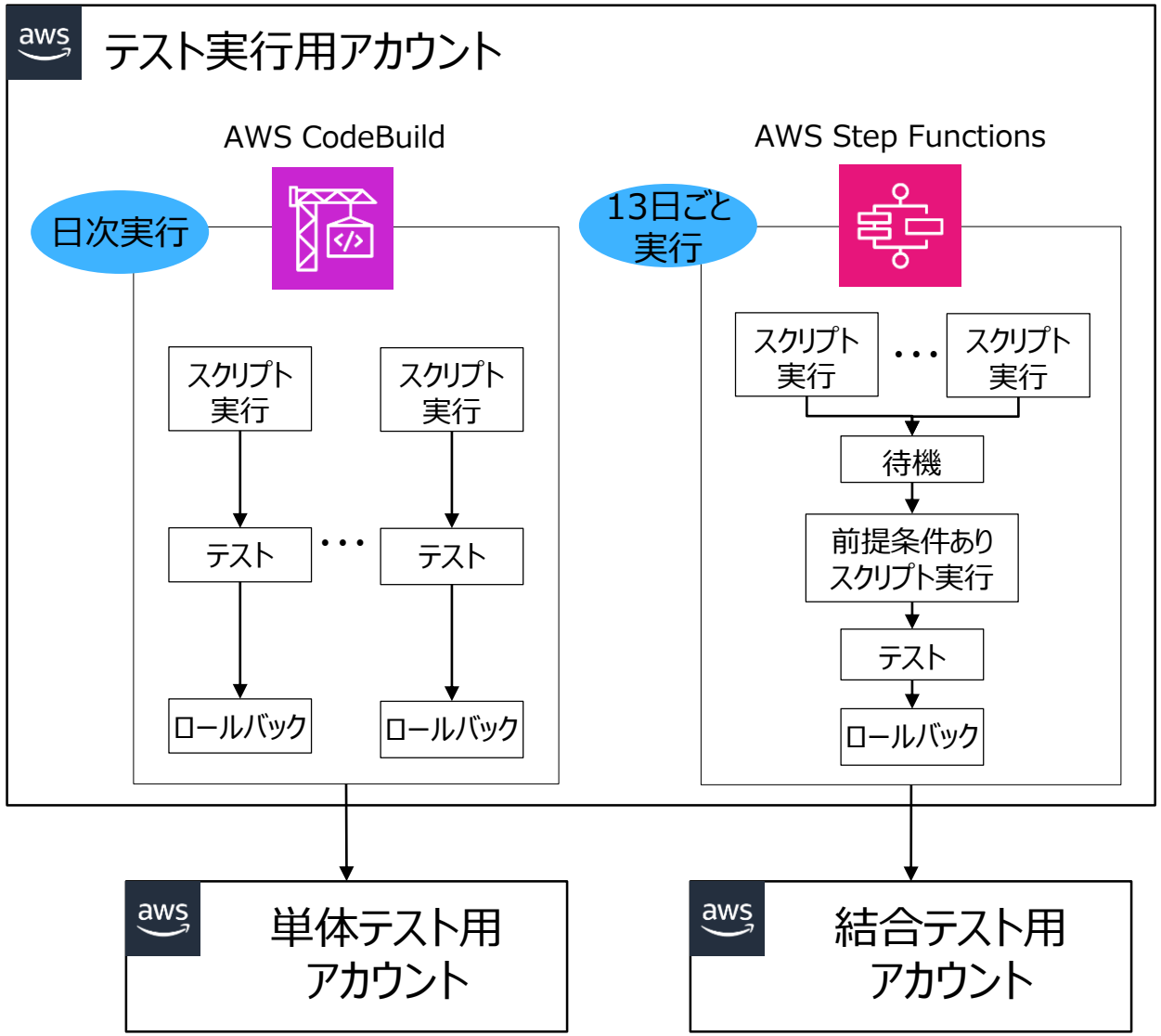
継続的なテストの実現方法

3つのAWSアカウントによるテスト環境

1. テストの実行基盤のあるアカウント
2. 単体テストの対象となるアカウント
3. 結合テストの対象となるアカウント

継続的なテストの実装

- AWS CodeBuild：AWSサービスごとの設定変更スクリプトの単体テスト
- AWS Step Functions：依存関係を考慮した全スクリプトを通した結合テスト



継続的なテストの実現方法 | ポイント①ロールバック

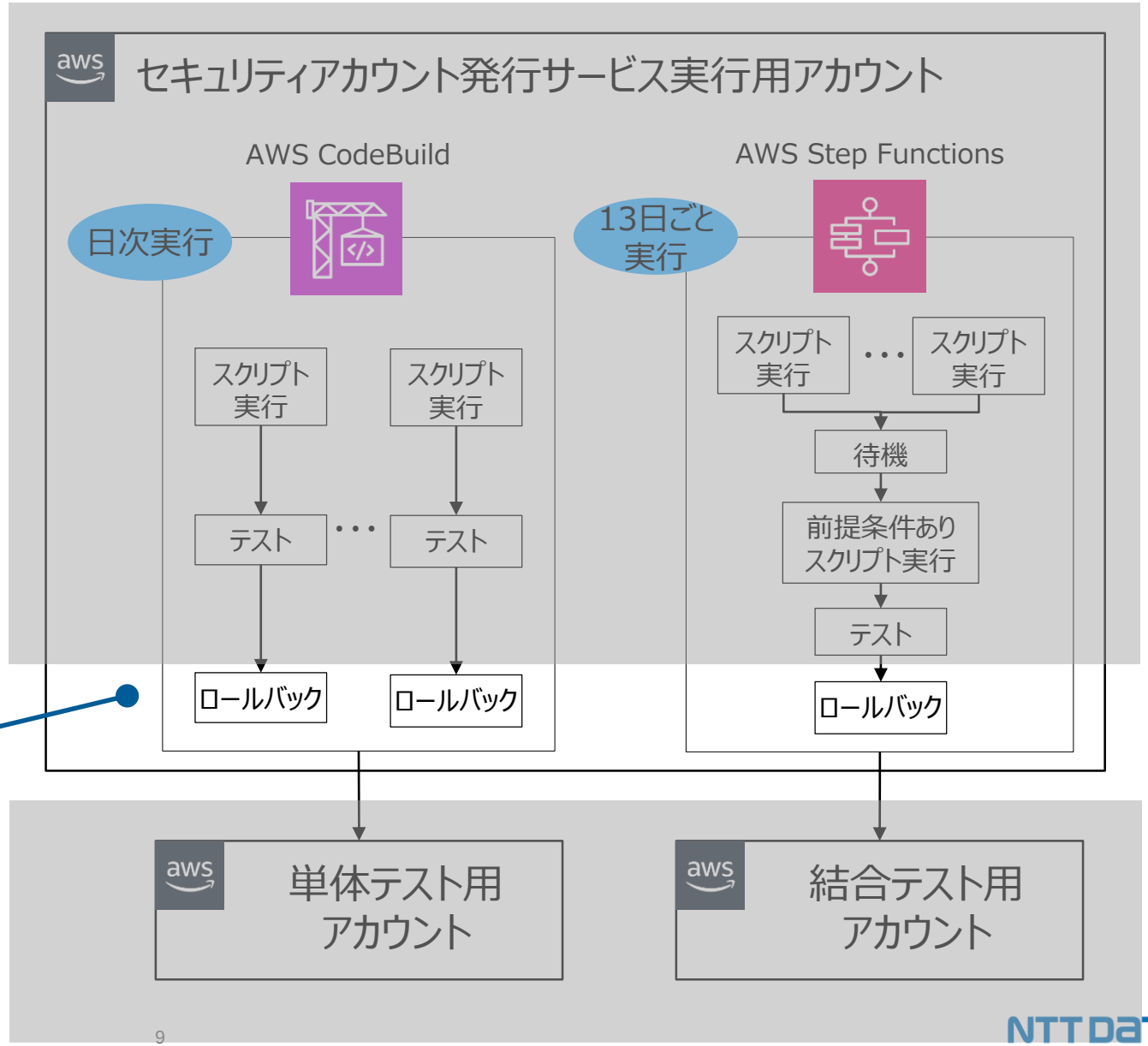
3つのAWSアカウントによるテスト環境

1. テストの実行基盤のあるアカウント
2. 単体テストの対象となるアカウント
3. 結合テストの対象となるアカウント

継続的なテストの実装

- AWS CodeBuild：AWSサービスごとの設定変更スクリプトの単体テスト
- AWS Step Functions：依存関係を考慮した全スクリプトを通した結合テスト

クリーンな状態のAWSアカウントを
多数用意するのは難しいため、
ロールバックを行い、**毎回クリーンな状態**とする



継続的なテストの実現方法 | ポイント②単体テスト

3つのAWSアカウントによるテスト環境

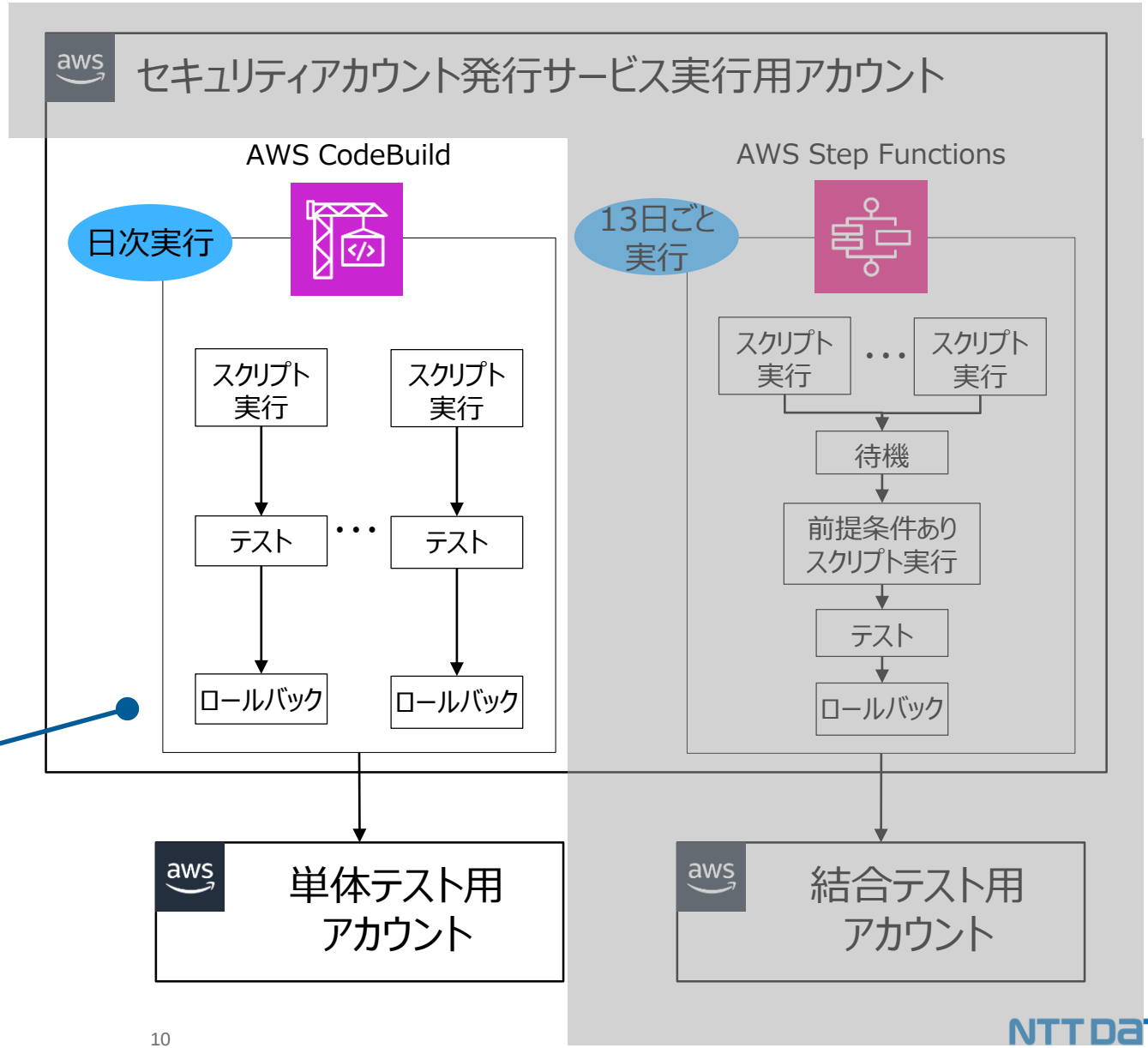
1. テストの実行基盤のあるアカウント
2. 単体テストの対象となるアカウント
3. 結合テストの対象となるアカウント

継続的なテストの実装

- AWS CodeBuild：AWSサービスごとの設定変更スクリプトの単体テスト
- AWS Step Functions：依存関係を考慮した全スクリプトを通した結合テスト

待機が必要な設定やロールバックに時間がかかる設定以外のスクリプトの単体テストを実行
処理単体での品質を確保

(例)
DetectiveはGuardDuty有効後2日待機が必要
CMKの削除は7日必要



継続的なテストの実現方法 | ポイント③結合テスト

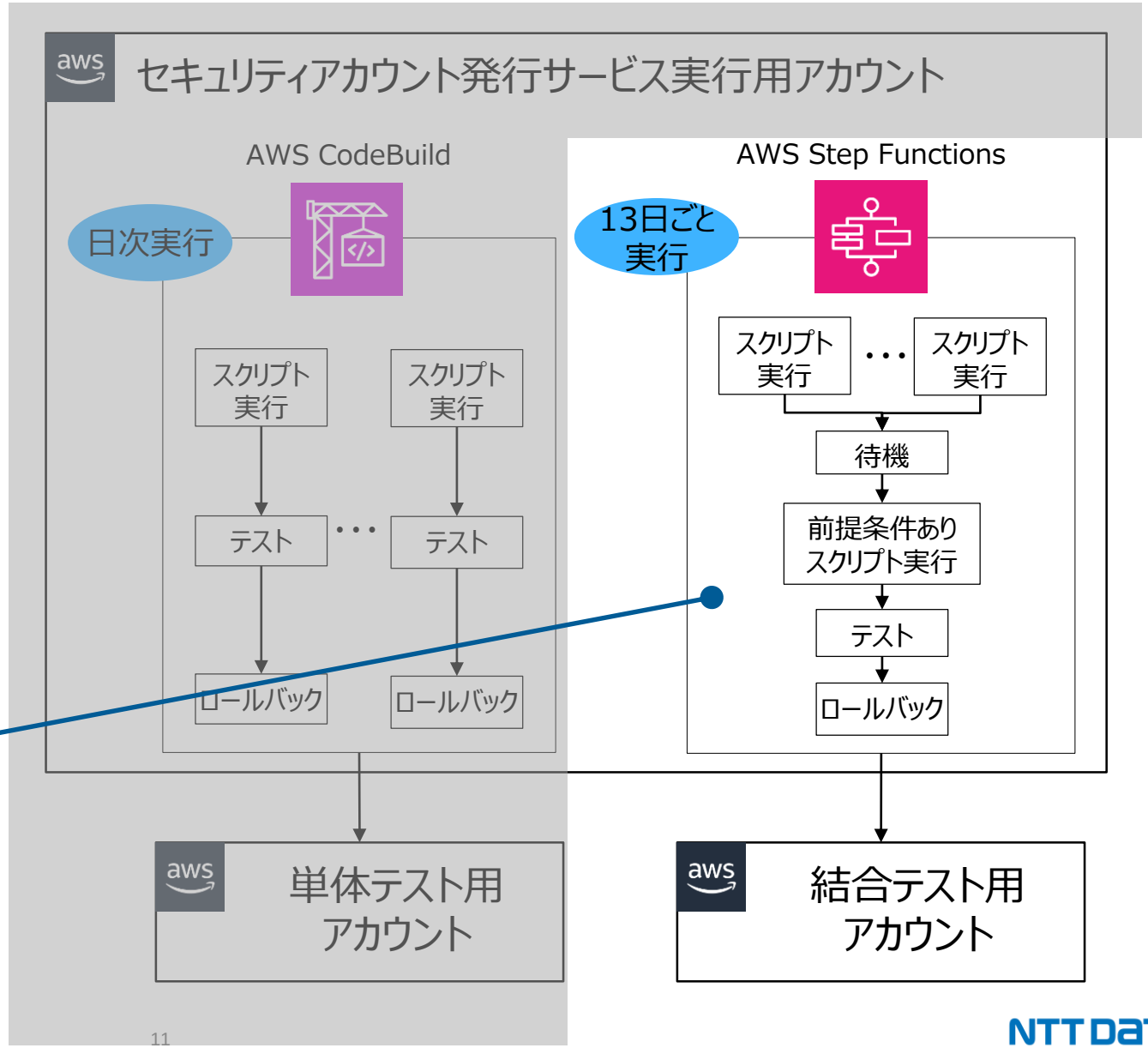
3つのAWSアカウントによるテスト環境

1. テストの実行基盤のあるアカウント
2. 単体テストの対象となるアカウント
3. 結合テストの対象となるアカウント

継続的なテストの実装

- AWS CodeBuild：AWSサービスごとの設定変更スクリプトの単体テスト
- AWS Step Functions：依存関係を考慮した全スクリプトを通した結合テスト

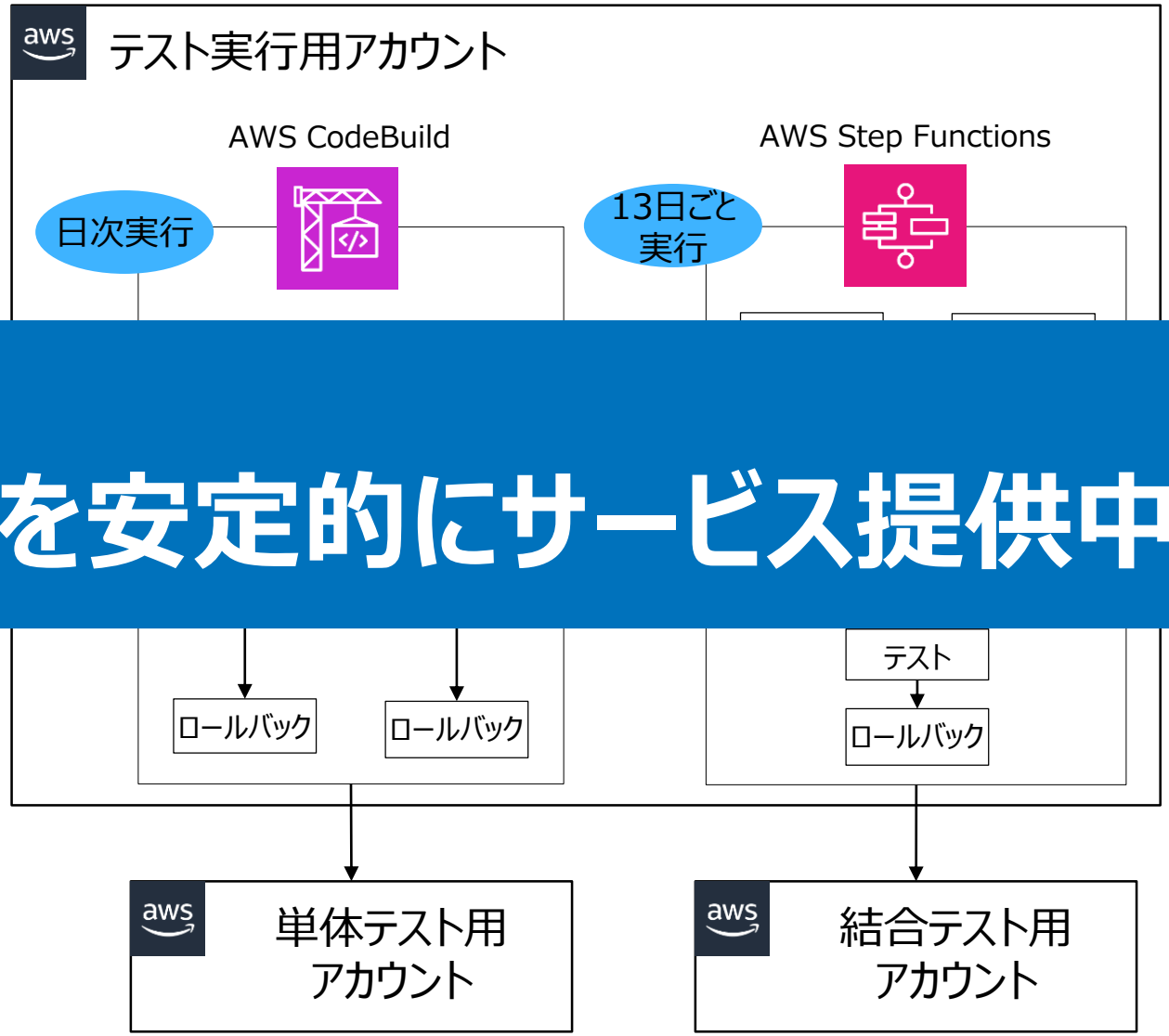
全体としての整合性をとれているかの
結合試験を別途用意



継続的なテストの実現方法

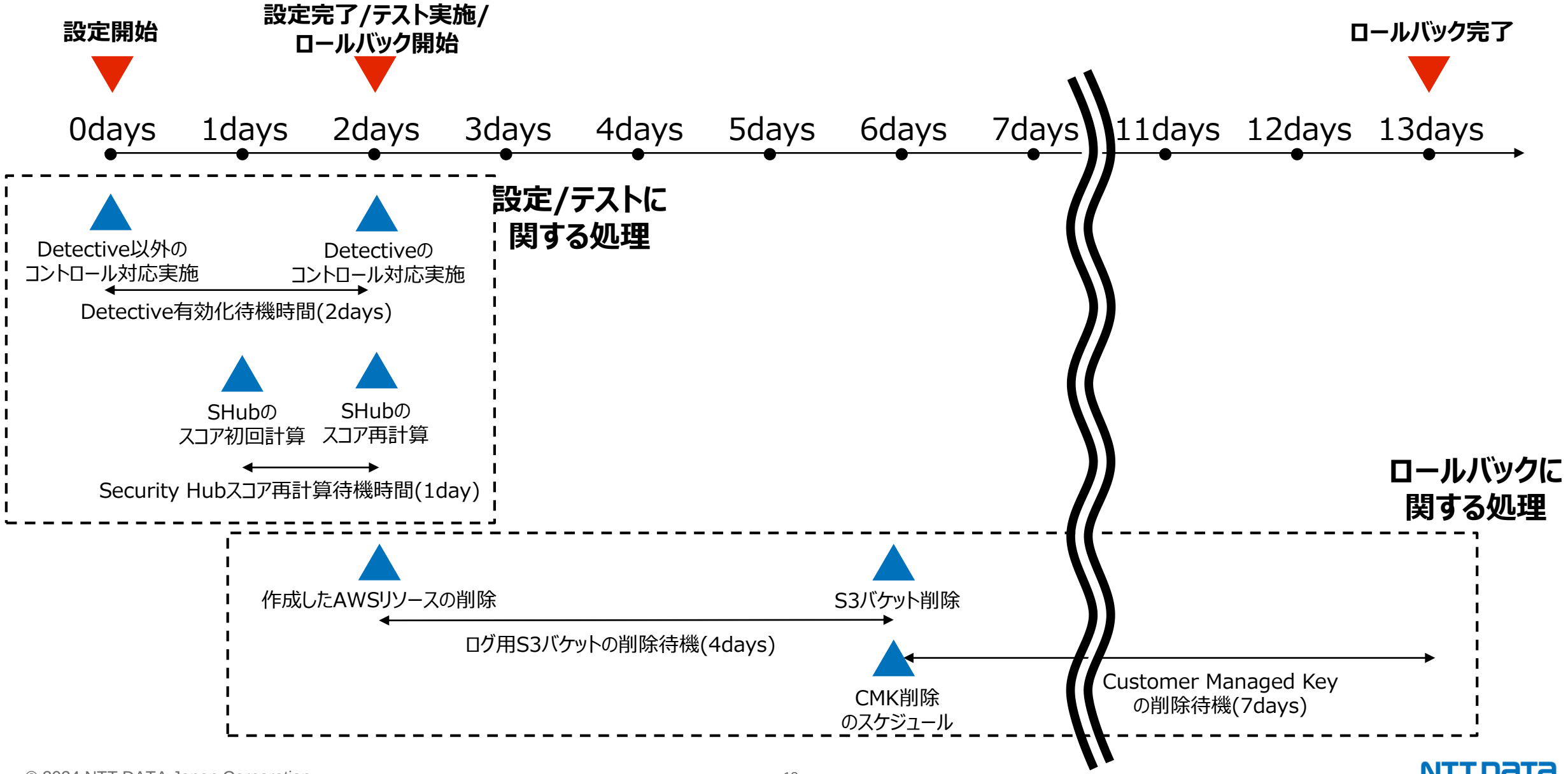
3つのAWSアカウントによるテスト環境

1. テストの実行基盤のあるアカウント
2. 単体テストの対象となるアカウント
3. 結合テストの対象となるアカウント



提供後の約2年間を安定的にサービス提供中

13日間を1サイクルにしている理由



まとめ

- クラウドを操作するIaCは様々な理由により、動作しなくなるリスクがあり、安定的に利用するためには、**継続的なテストが必要**になる
  場合によってはlocalstackなどでもOK

- 当社独自のセキュリティルール(ガードレール)を設定する「セキュリティアカウント発行サービス」の裏側では、単体試験と結合試験を組み合わせて品質を担保

- お客様独自セキュリティルール構築を支援するサービス(**SRE as a Service**)もありますので、興味がある方はぜひともお声がけください！

NTTデータのSRE as a Service

以下サービスメニューをお客様の状況に応じて時間単位でご利用可能です

クラウドネイティブ開発支援サービス

#	サービスメニュー例	内容
1	**システム アーキテクチャ検討**	マネージドサービスを活用したシステムアーキテクチャ検討支援
2	**PoC**	お客様にとって未経験のサービスのPoC
3	**開発ガイドライン作成支援**	お客様特性を踏まえたクラウドでの開発ガイドラインの作成支援
4	**PMO/QA支援**	クラウド開発での品質保証のためのコーチングやレビューなどを支援

※システムの要件定義はお客様自身で実施
※お客様環境での実作業（AWSリソースの構築など）はお客様自身で実施
※新規契約の場合、1契約最大3か月間までのご支援(最低稼働時間10H/契約)

クラウドネイティブ運用支援サービス

#	サービスメニュー例	内容
1	**アップデート対応支援**	クラウドサービスアップデート情報を踏まえた改善やEOL対応支援
2	**コスト可視化／最適化支援**	お客様の全社視点でのコスト可視化／最適化支援
3	**セキュリティガードレール実装／運用支援**	お客様全社でクラウドをセキュアに利用するためのセキュリティガードレール実装やその運用を支援

※お客様環境での実作業（AWSリソースの設定変更など）はお客様自身で実施
※新規契約の場合、1契約最大3か月間までのご支援(最低稼働時間10H/契約)


NTT DATA