このコンテンツは公開から3年以上経過しており内容が古い可能性があります
最新情報についてはサービス別資料もしくはサービスのドキュメントをご確認ください

[AWS Black Belt Online Seminar]

AWS CodeCommit & AWS CodeArtifact

サービスカットシリーズ

Solutions Architect 松本 雅博
2020/10/20

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive

自己紹介

松本 雅博（まつもと まさひろ）
技術統括本部 西日本ソリューション部
ソリューションアーキテクト

関西を中心に、西日本のお客様をご支援
好きなサービス

- Code シリーズ
- AWS CloudFormation, AWS Cloud Development Kit

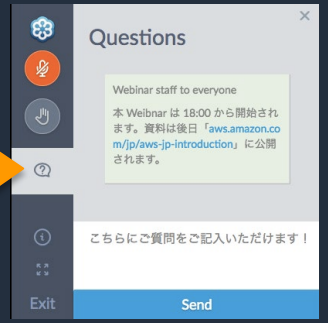
AWS Black Belt Online Seminar とは

「サービス別」「ソリューション別」「業種別」のそれぞれのテーマに分かれて、アマゾン ウェブ サービス ジャパン株式会社が主催するオンラインセミナーシリーズです。

質問を投げることができます！

- 書き込んだ質問は、主催者にしか見えません
- 今後のロードマップに関するご質問は
  お答えできませんのでご了承下さい

① 吹き出しをクリック
② 質問を入力
③ Sendをクリック



Twitter 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2020年10月20日現在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には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.

本セミナーの概要

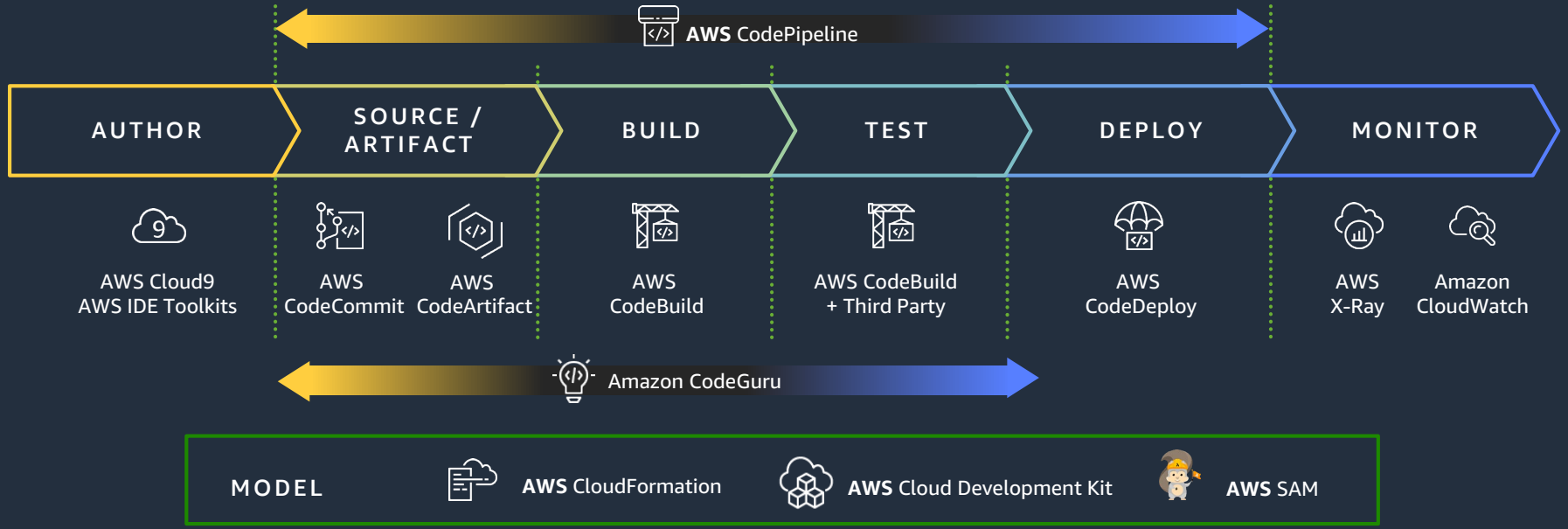
- 本セミナーで学習できること
    - AWS CodeCommit
    - AWS CodeArtifact

- 対象者
    - アーキテクトの方
    - 技術者の方

本日のアジェンダ

- ソフトウェア開発に関連する AWS サービス
- AWS CodeCommit
- AWS CodeArtifact
- まとめ

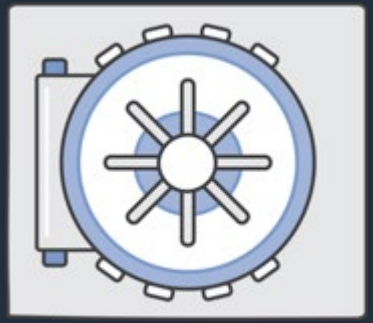
ソフトウェア開発に関連する AWS サービス



自社でホストするツールの課題

- 開発者ごとの高価なライセンス費用
- ハードウェア保守コスト
- サポートスタッフのコスト
- 保存や管理できるデータ量やファイルタイプの制限
- 管理できるブランチの数やバージョン履歴の数の制限

クラウドにおけるソース管理に求められるもの



Secure

Fully managed

High availability

Store anything

aws

AWS CodeCommit

AWS CodeCommit

- ✓ **セキュア**で**スケーラブル**な**マネージドGit互換ソース管理**
- ✓ 標準的な Git ツールが利用可能
- ✓ Amazon S3 のスケーラビリティ、可用性、堅牢なストレージを利用
- ✓ 利用者固有のキーを使用した暗号化
- ✓ **レポジトリサイズの上限なし**
- ✓ コンテンツの直接編集をサポート
- ✓ プルリクエスト機能に対応
- ✓ VPC エンドポイントをサポート

AWS CodeCommit 概要

SSH or HTTPS

`git pull/push`

Git オブジェクトは
Amazon S3で管理

Git インデックスは
Amazon DynamoDB
で管理

暗号化キーは
AWS KMSで管理

リポジトリの作成

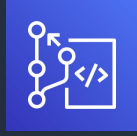
- リポジトリ名を指定するだけ
- 説明とタグはオプション
- Amazon CodeGuru Reviewer for Java との連携設定も可能

CLIから

```
aws codecommit create-repository --repository-name myfirstrepo ¥

--repository-description "My first repository"
```

CodeCommit を利用するには



最も簡単な方法： CodeCommit の HTTPS 接続で Git 認証情報を設定する

- IAM で Git ユーザー名とパスワードを生成して使用する
- 様々な IDE と互換性がある

その他の接続方法：

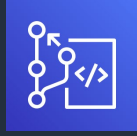
- SSH 接続 (IAM と SSH キーを紐付ける)
- git-remote-codecommit (IAM のクレデンシャルを利用する)
- 開発ツールからの接続 (AWS Toolkit を利用する)

詳細は以下の URL を参照

https://docs.aws.amazon.com/codecommit/latest/userguide/setting-up.html

aws

HTTPS 接続と Git 認証の手順



1. AWS CodeCommit にアクセスするユーザを作成
2. IAM に静的なユーザー名とパスワードを生成
3. 生成した認証情報を Git のユーザー名、パスワード認証で利用

- AWS CodeCommit は Git 1.7.9 以上をサポート
- AWS CodeCommit は Curl 7.33 以上が必要
    - curl update 7.41.0 をHTTPSで利用する場合は既知の障害あり

以下を参照：
https://docs.aws.amazon.com/codecommit/latest/userguide/troubleshooting.html

aws

HTTPS 接続 – IAM からの Git 認証情報の作成

- 認証情報 タブを選択

HTTPS 接続 – IAM からの Git 認証情報の作成

- 認証情報を生成をクリック

HTTPS 接続 – IAM からの Git 認証情報の作成

- 認証情報が作成される
- パスワードはこのタイミングでしか確認できない
- 認証情報のダウンロードを忘れずに

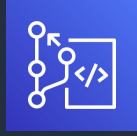
HTTPS 接続 – IAM からの Git 認証情報の作成

- パスワードを忘れてしまった場合、この画面よりリセット可能

Local Git から CodeCommit への接続

- リポジトリの URL を取得する

Local Git から CodeCommit への接続

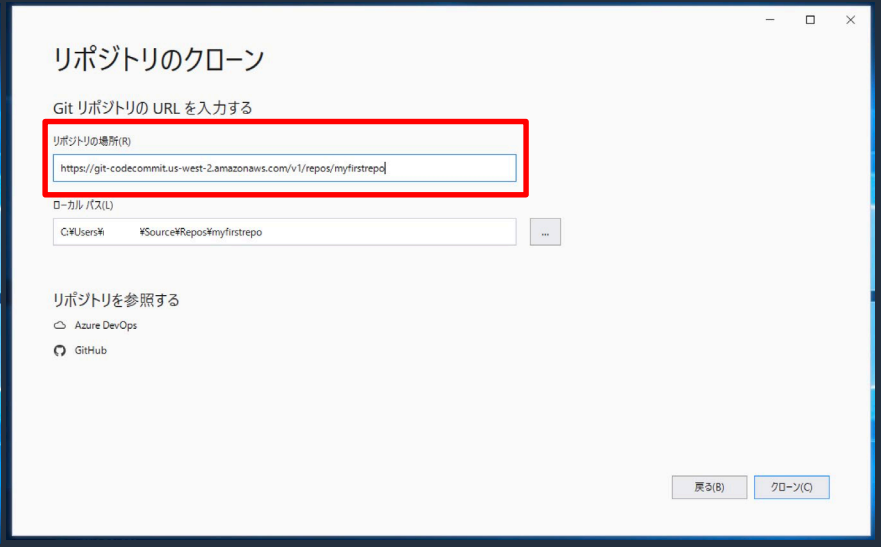


- 作成した認証情報を利用して接続

```
$ git clone https://git-codecommit.us-west-2.amazonaws.com/v1/repos/myfirstrepo
Cloning into 'myfirstrepo'...
Username for 'https://git-codecommit.us-west-2.amazonaws.com': developer01-at-
Password for 'https://developer01-at-           @git-codecommit.us-west-2.amazonaws.com':
warning: You appear to have cloned an empty repository.
```

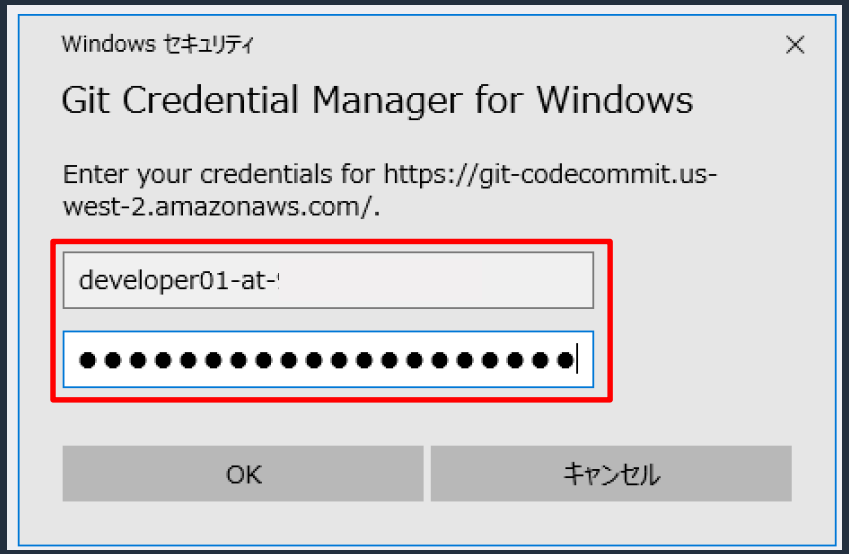
Visual Studio からの接続

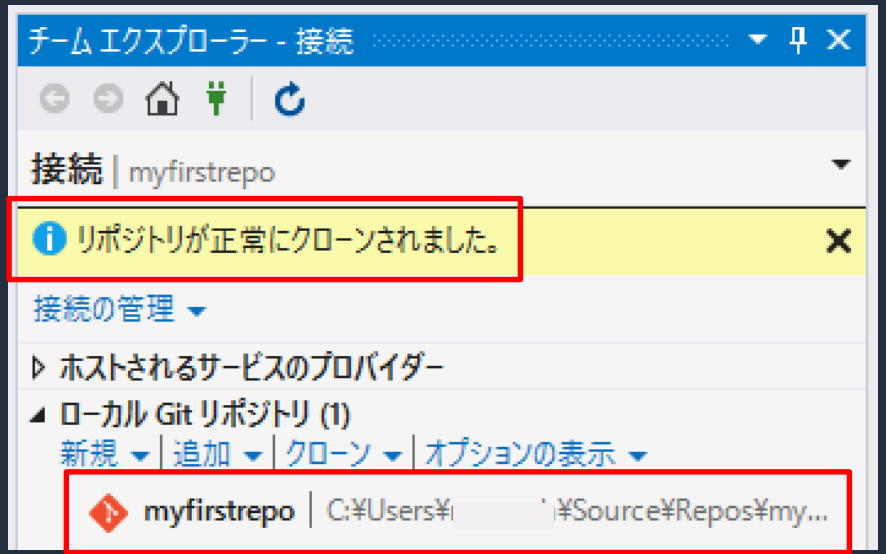
- リポジトリのクローンをクリックし、 URL を入力する



Visual Studio からの接続

- 認証情報を入力する

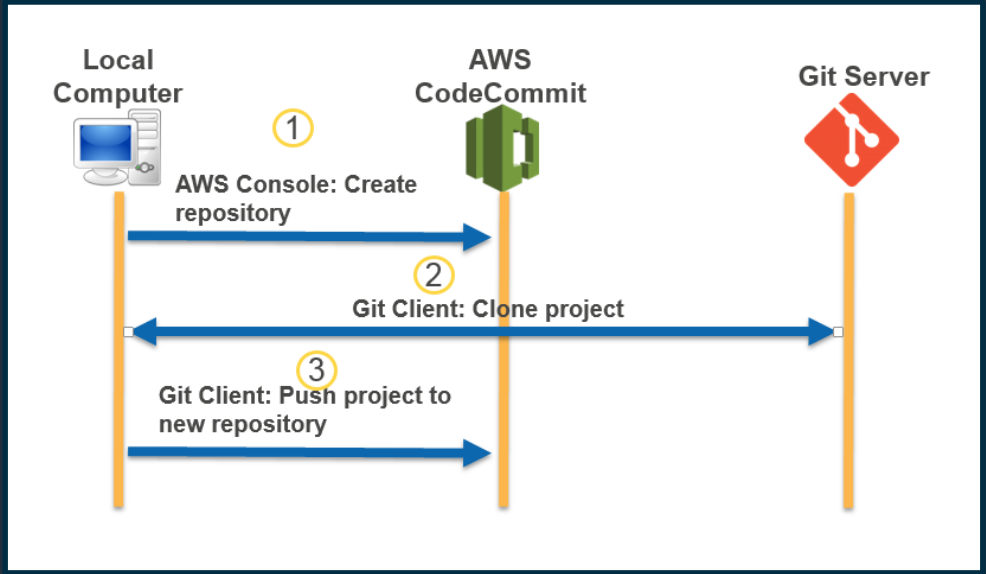




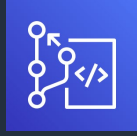
他の Git リポジトリからのマイグレーション

他の Git リポジトリからのマイグレーションは非常にシンプル

1. CodeCommit にリポジトリ を作成
2. 他の Git リポジトリからローカルにクローン
3. CodeCommit へ Push



参考資料：git を学ぶ



Pro Git
https://git-scm.com/book/ja/v2 （日本語）

Git Cheat sheet
https://training.github.com/downloads/ja/github-git-cheat-sheet.pdf （日本語）

Git Immersion
http://gitimmersion.com/

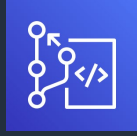
Git Reference
https://git-scm.com/docs

git はHTTPプロトコルを利用する場合、デフォルトでは毎回ユーザー名、パスワードの入力を求めるが、git config --global credential.helper を利用することでクレデンシャル情報をキャッシュまたは保存することが可能

https://git-scm.com/book/en/v2/Git-Tools-Credential-Storage

aws

コンテンツの参照・編集・追加



- AWS CodeCommit コンソールでリポジトリのコンテンツを閲覧
    - ブランチやタグを切り替えて表示可能
- ファイルの編集、追加も可能
    - リポジトリ内のファイルを直接編集
    - ファイルの作成や、ローカルからのアップロードも可能

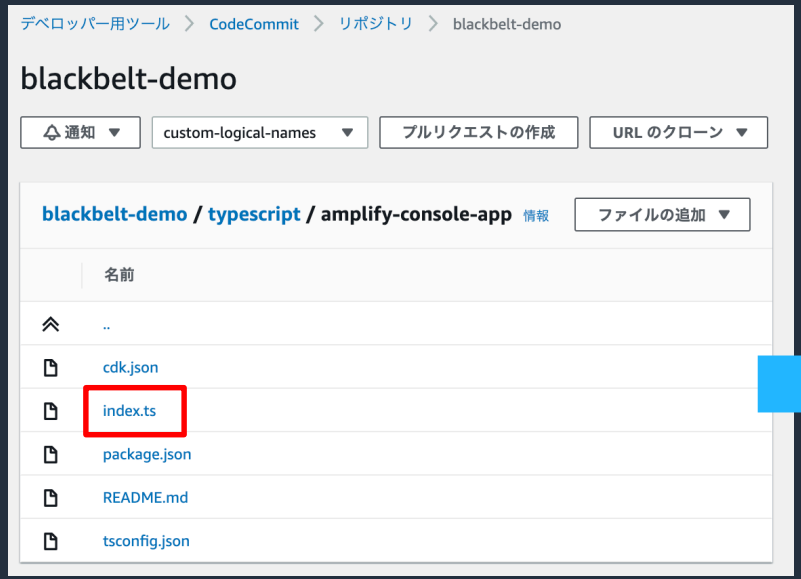
aws

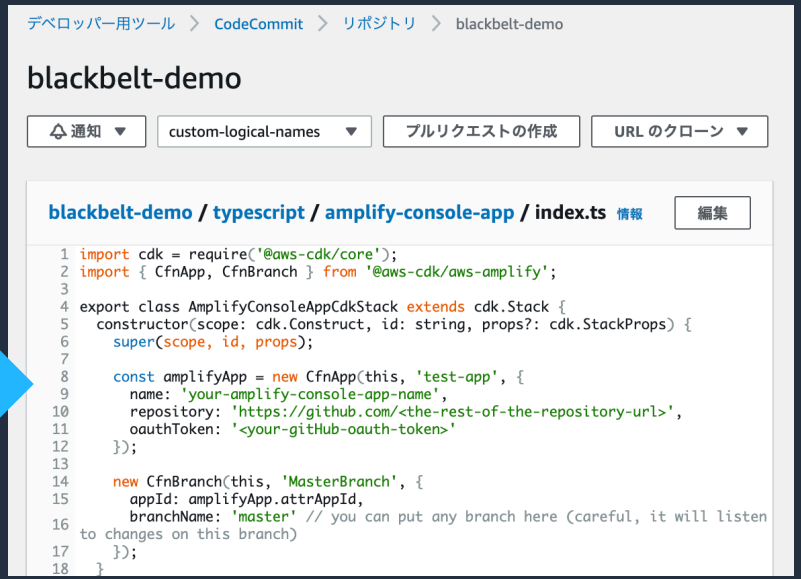
リポジトリのコンテンツ参照

- マネジメントコンソールから、リポジトリを選択

リポジトリのコンテンツ参照

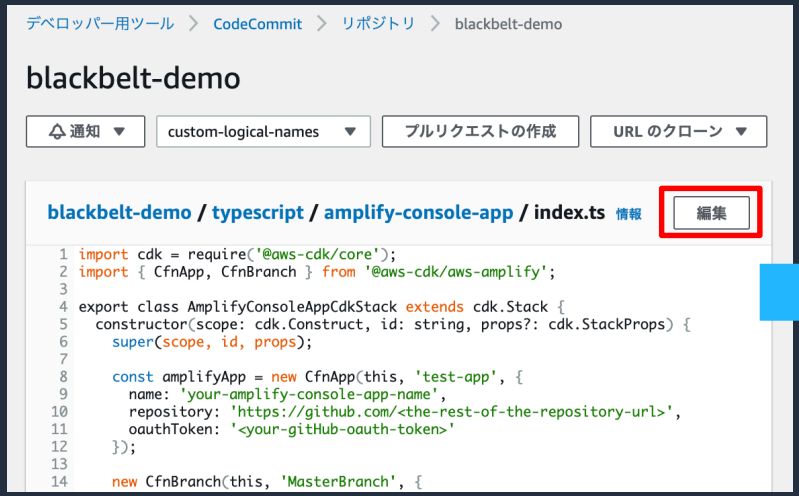
- リポジトリ内を参照することが可能
- これ以降の表示内容は aws-samples/aws-cdk-examples





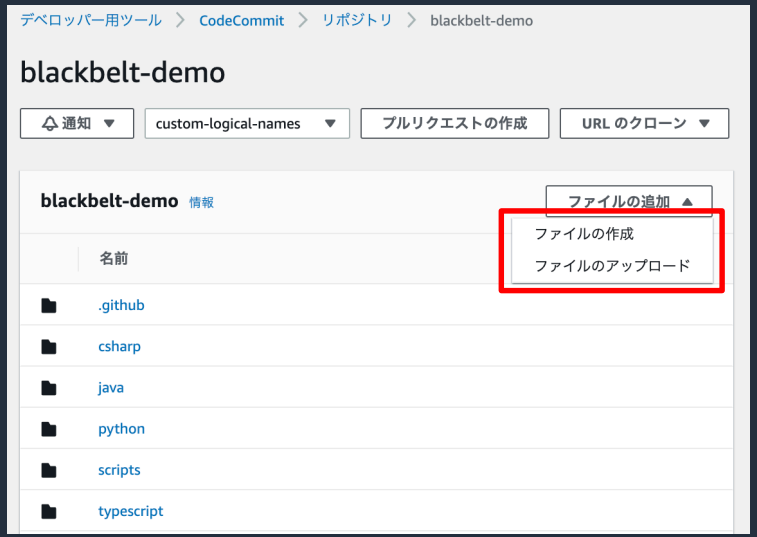
リポジトリのコンテンツ編集

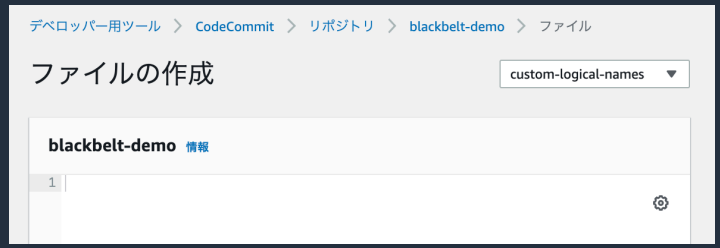
- 参照だけでなく、ファイルの編集も可能

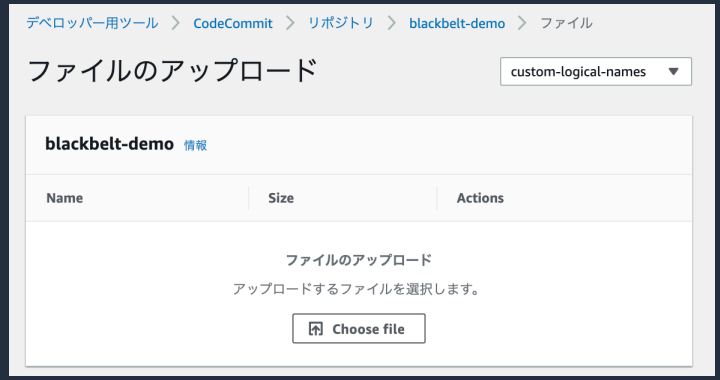


リポジトリのコンテンツ追加

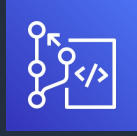
- 参照だけでなく、ファイルの追加も可能







コミット履歴の表示

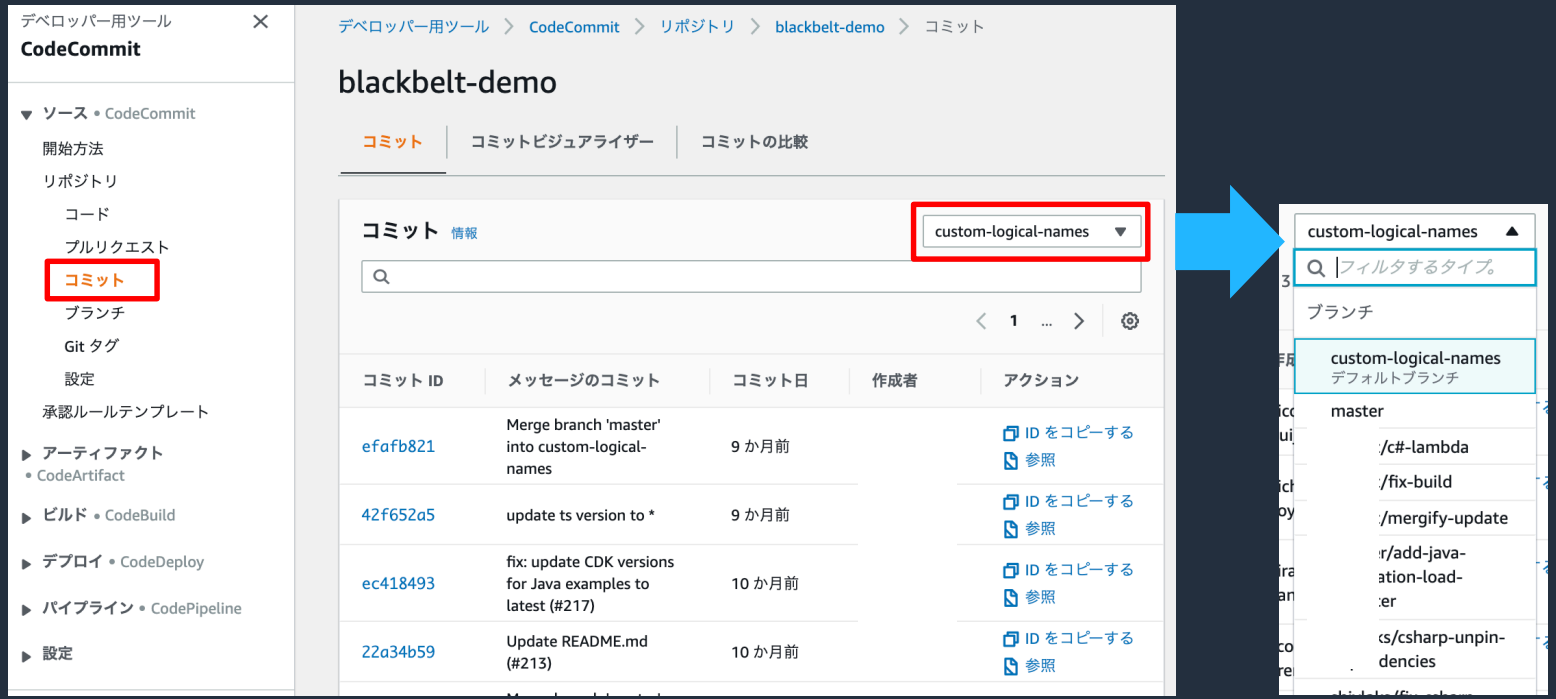


- AWS CodeCommit コンソールでリポジトリのコミット履歴を表示
  - git rebase コマンドでリベースを行った場合は、リポジトリの履歴が変更されるので注意
  - ブランチやタグを切り替えて表示可能
  - 直前のコミットとの差分比較（分割表示または結合表示が可能）
  - Commit IDをコピー可能。コマンドラインのコミットの比較で利用可能
  - </>マークをクリックすると対象のソースコードを表示

aws

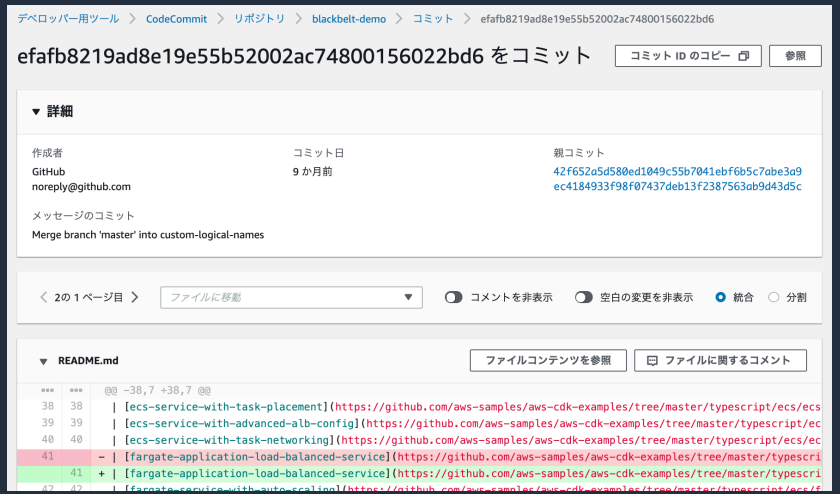
コミット履歴の表示

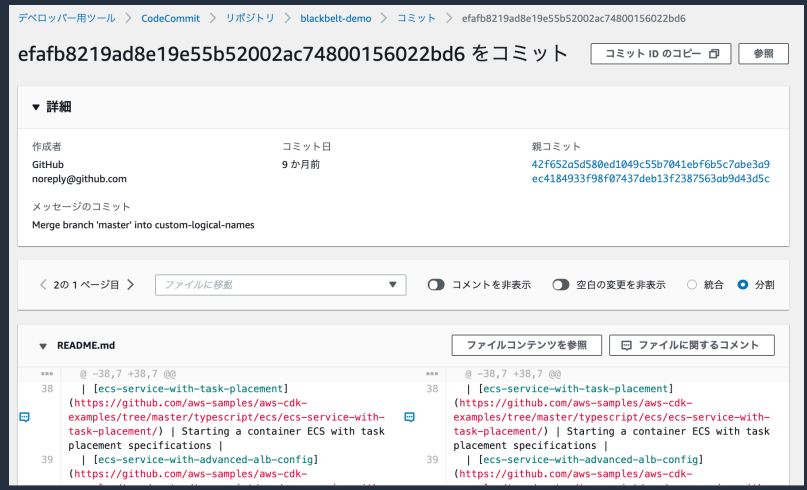
- ブランチやタグを切り替えて表示することが可能



コミット履歴の表示

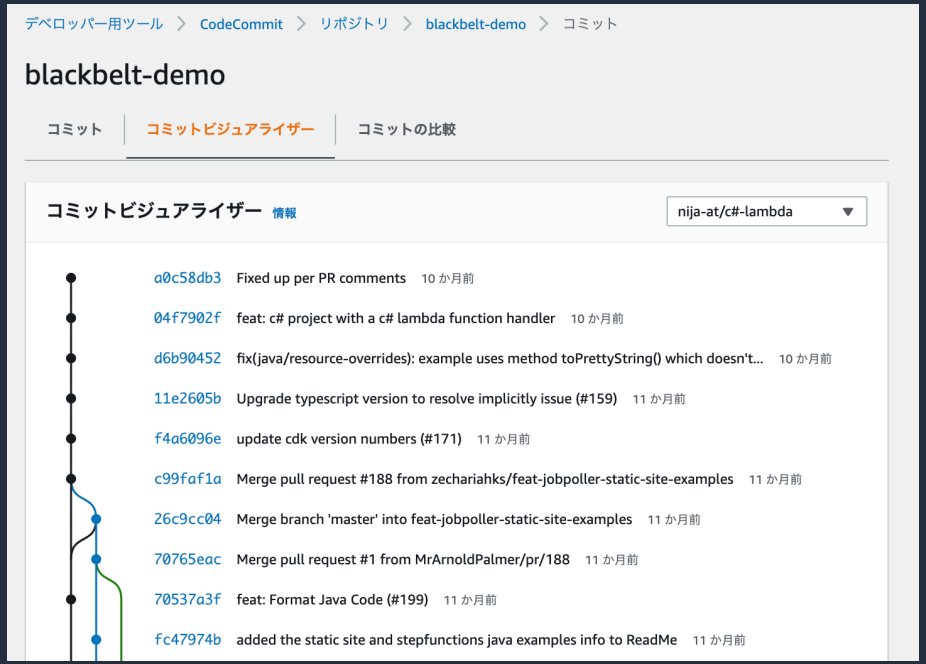
- 直前のコミットとの差分比較



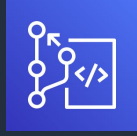


コミット履歴の表示

- コミットビジュアライザーを選択



プルリクエストの作成



プルリクエストとは？

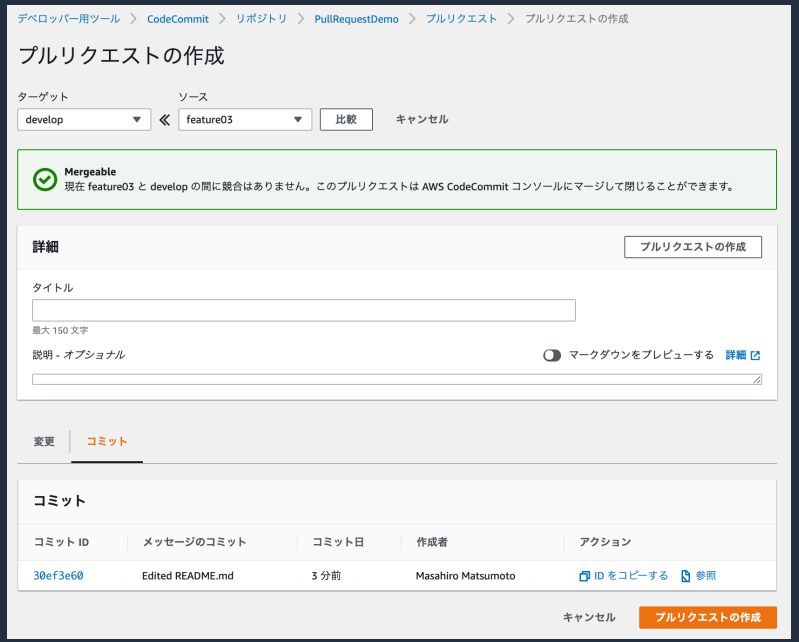
- リポジトリのユーザに対する作業内容の通知
- プルリクエストを起点として、議論やコミュニケーションを機会を提供
- コードレビューや変更箇所の精査ができ、品質改善につなげる

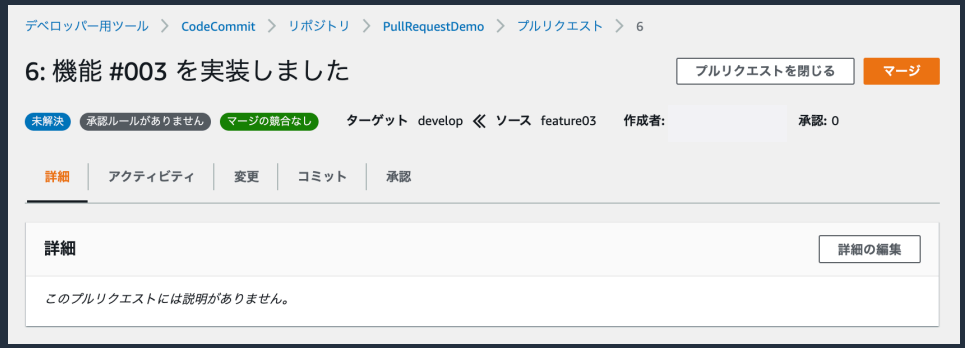
aws

プルリクエストの作成

ターゲットブランチとソースブランチを選択して作成

- タイトルと説明を入力





プルリクエストへのコメント

以下に対してコメントを追加可能
- プルリクエスト
- ファイル
- コードの行

絵文字によるリアクションも可能に

プルリクエストのマージ

3 つのマージ戦略をサポート

- fast-forward
- 3-way merge
- Squash merge

プルリクエストの承認ルールワークフロー

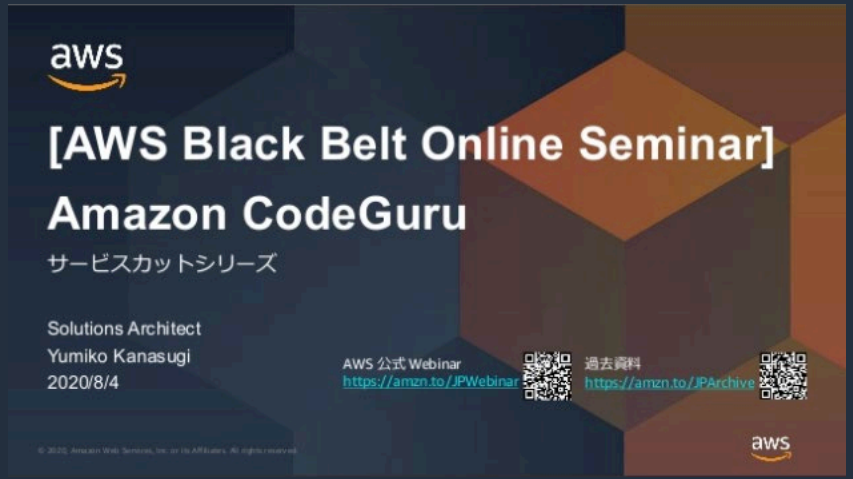
コードをマージする前に満たなさければならないルール要件を定義し、
高品質のコード変更のみがマージされるようにすることに役立つ

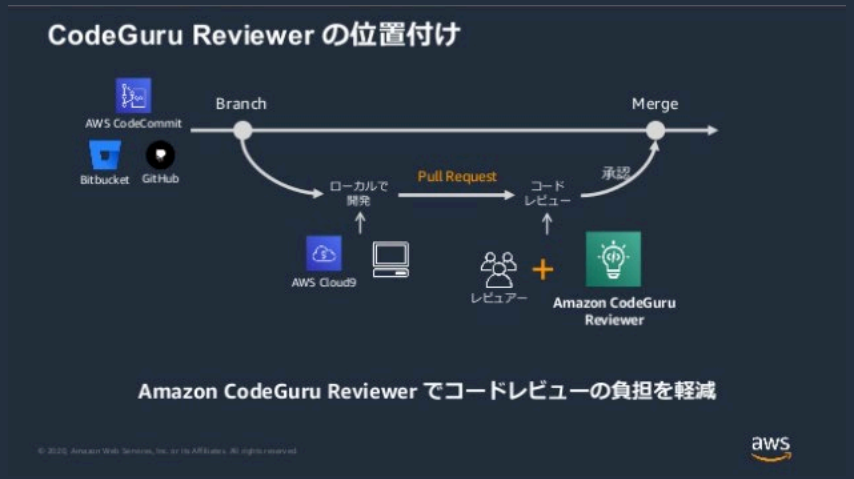
- 承認の総数
- 特定ユーザーからの承認

任意のリポジトリ、ブランチへ適用可能

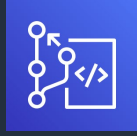
Amazon CodeGuru Reviewer との連携

- CodeGuru Reviewer と連携したレビューの実施も可能
- 詳細は 2020/8/4 の Amazon CodeGuru を参照





AWS CloudTrail を利用した API コールログ取得



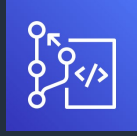
AWS CodeCommit は、AWS CloudTrailと連携可能

- コンソール、git クライアント、AWS CLI から発行される CodeCommit API をキャプチャーしてS3 バケットに保存可能

```
{
      "eventVersion":"1.05",
     "userIdentity": {
           "type":"IAMUser",    "principalId":"AIDACKCEVSQ6C2EXAMPLE",
          "arn":"arn:aws:iam::444455556666:user/Mary_Major",    "accountId":"444455556666",
           "accessKeyId":"AKIAIOSFODNN7EXAMPLE",    "userName":"Mary_Major"
        },
        "eventTime":"2016-12-14T17:57:36Z",
     "eventSource":"codecommit.amazonaws.com",
     ....
}
```


aws

ブランチレベルのアクセス許可

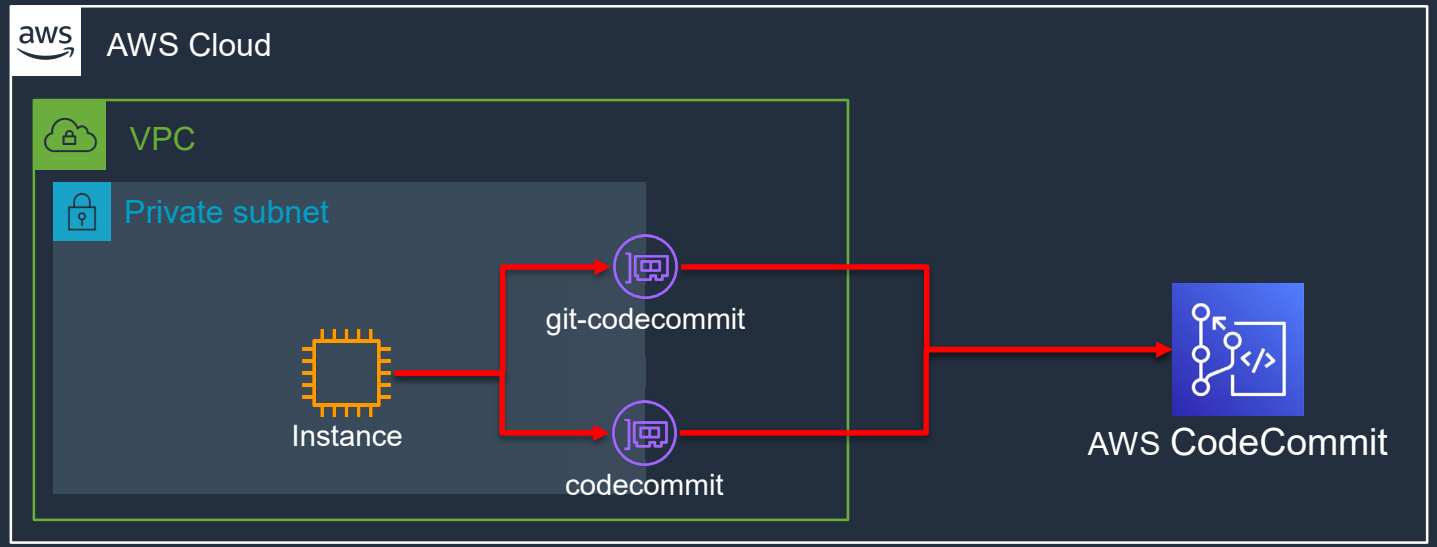


- リポジトリを変更できるユーザーの制御だけでなく、リポジトリ内のブランチを変更できるユーザを制御可能
- IAM ポリシーの Condition で操作の行えるブランチを制限
- 開発チーム以外にはプルリクを master ブランチへ マージさせないなど、ブランチへのアクセスを柔軟に制御できる

aws

VPC エンドポイントをサポート

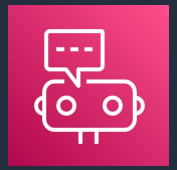
- Git 操作用と CodeCommit API 操作用の2種類のエンドポイント
- 連邦情報処理標準(FIPS) 準拠オプションもあり



リポジトリイベントの通知

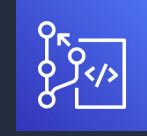
- 従来のトリガーよりも細かな条件設定が可能
    - プルリクエスト、承認、ブランチ・タグ操作
- Amazon SNS によるトピックの通知
- AWS Chatbot と連携した Slack への通知
- 詳細は以下を参照
    - https://aws.amazon.com/jp/blogs/news/receive-aws-developer-tools-notifications-over-slack-using-aws-chatbot/

Amazon Simple Notification Service



AWS Chatbot

AWS サービスとの連携



AWS Cloud9

AWS CodeBuild

AWS CodePipeline

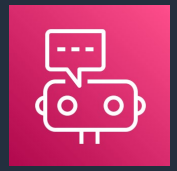
AWS CodeStar

AWS CloudFormation

AWS CloudTrail

Amazon CloudWatch

Amazon Simple Notification Service



AWS Chatbot

AWS Amplify

AWS Key Management Service

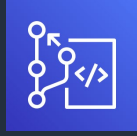
AWS Elastic Beanstalk

AWS Lambda

Amazon CodeGuru

aws

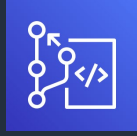
AWS CodeCommit 制限事項



リポジトリの数	アカウントごとに1,000まで
単一のPushの参照数	最大4,000 （create, delete, update を含む）。リポジトリ内の全体の参照数は無制限。
リポジトリ名	1～100文字まで。.gitで終わる名前をつけることは出来ない。以下の文字は含むことができない。 ! ? @ # $ % ^ & * ( ) + = { } [ ] | ¥ / > < ~ ` ‘ “ ; :
Git blob サイズ	ファイルの数や単一のコミットでのファイルの合計サイズは無制限。メタデータは6MB以下、単一のblobファイルのサイズは2GBまで。
Commit　Visualizer のブランチ数	35 ブランチ/ページ。

aws

料金



アクティブユーザー：コンソールや CLI、SDK を使ってアクセスする AWS Identity (例：IAM ユーザーや IAM ロールなど) のこと。

最初の 5 アクティブ ユーザーまで	最初の 5 を超えるアクティブ ユーザー（1 人当たり）
無料	1ドル/月
• 無制限のリポジトリ数 • 月に 50GB のストレージ • 10,000 Git リクエスト/月	• 無制限のリポジトリ数 • 月に 10GB のストレージ/ユーザー • 2,000 Git リクエスト/月/ユーザー

上記の制限を超えた場合
- ストレージ：$0.06 / GB / 月
- Git リクエスト：$0.001 / リクエスト / 月

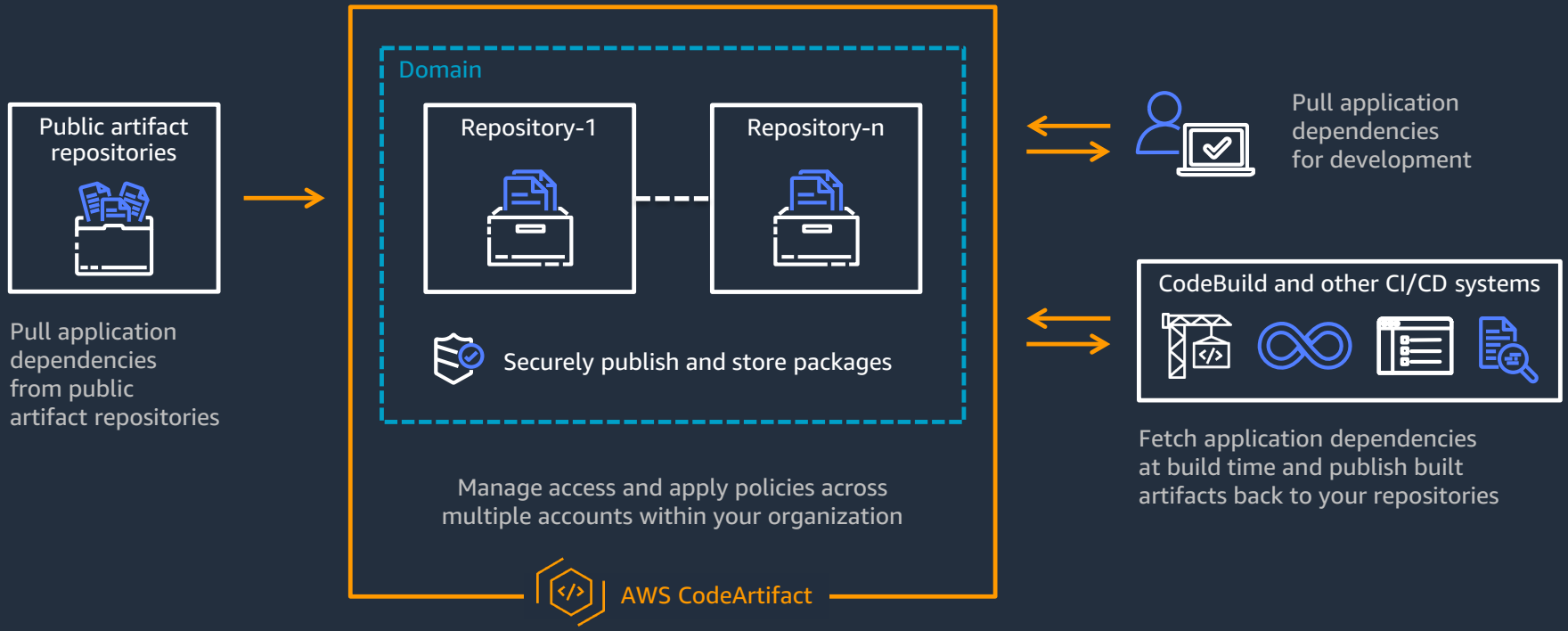
が費用としてかかる。

AWS CodeArtifact

AWS CodeArtifact

- ✓ **セキュア**で**スケーラブル**な**マネージドアーティファクト管理**
- ✓ Maven, Gradle, npm, yarn, twine, pip などの一般的なビルドツール、パッケージマネージャーから利用可能
- ✓ npm パブリックリポジトリ、Maven Central, Python Pacage Index (PyPi) などからパッケージ取得可能
- ✓ AWS Key Management Service (KMS) による暗号化をサポート
- ✓ リポジトリはポリグロットでサポートされている任意のパケージを含めることができる
- ✓ VPC エンドポイントをサポート

AWS CodeArtifact 概要



ドメイン

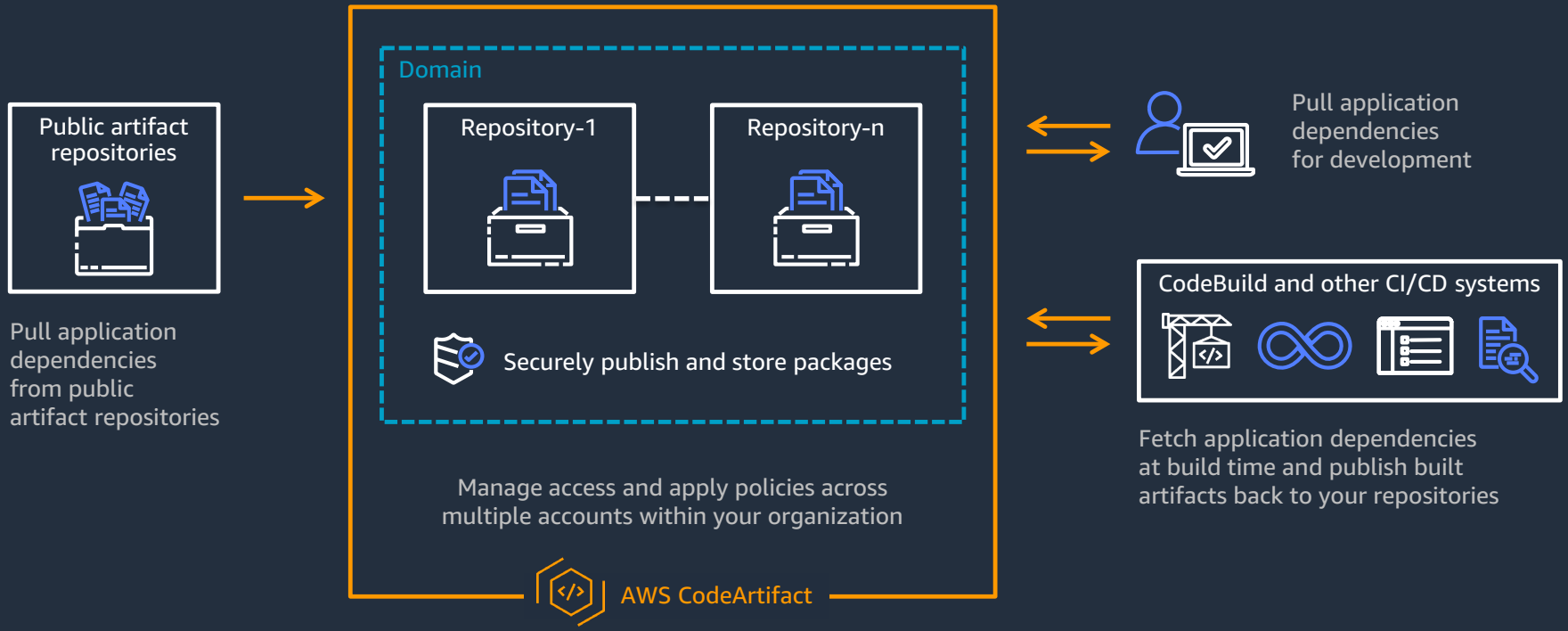
- パッケージとメタデータを格納する単位
    - パッケージが複数のリポジトリに存在していても、**保存はドメインごとに一度だけ**
    - ドメイン内の全てのアセット、メタデータは単一の キーで暗号化
- リポジトリを集約する
    - クロスアカウントに対応、別アカウントのリポジトリも格納可能
- 複数作成できるが、単一の本番用とテスト用を作成することを推奨
- アカウント内で一意であること

aws

リポジトリ

- ドメインのメンバー
    - 必ず1つのドメインに所属する
    - 作成後に他のドメインへ移動できない
- **ドメインに格納されたパッケージにアクセスするためのエンドポイント**
- パッケージバージョンのセットが含まれる
- ポリグロット （多言語対応）
- リポジトリは他のリポジトリのアップストリームになることができる

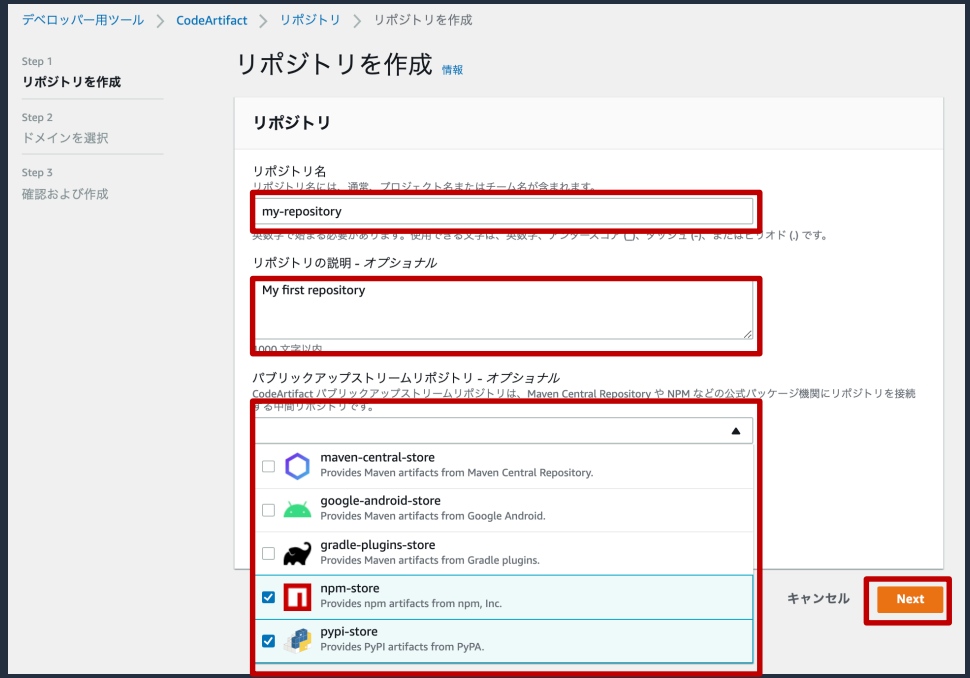
AWS CodeArtifact 概要（再掲）



リポジトリの作成

以下を入力

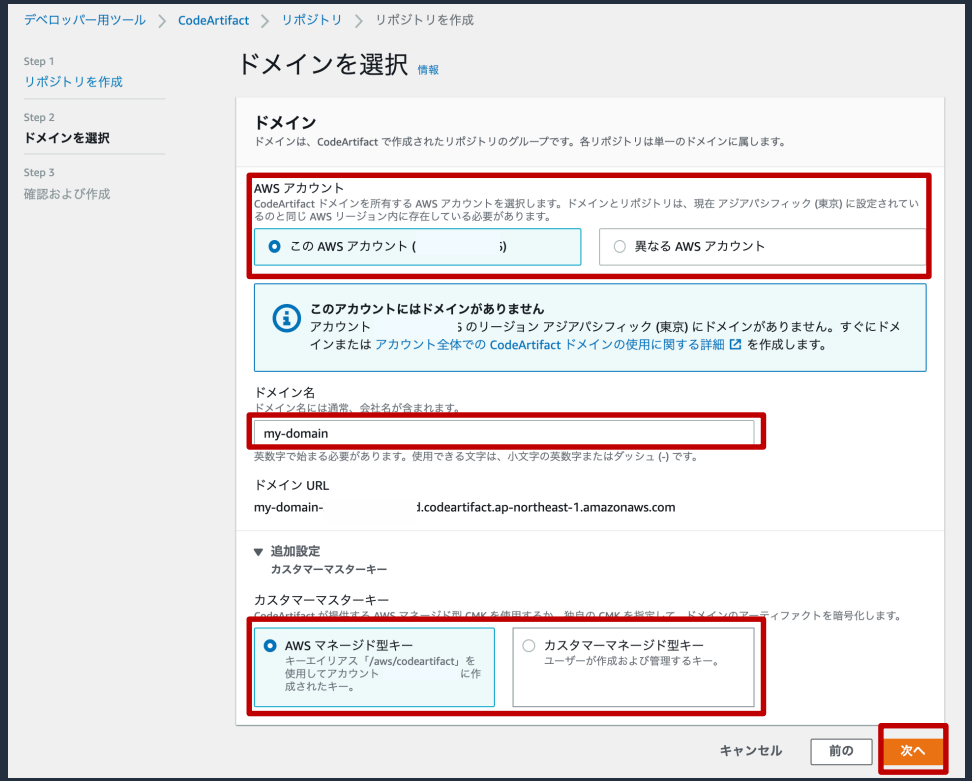
- リポジトリ名
- リポジトリの説明
- パブリックアップストリーム



リポジトリの作成

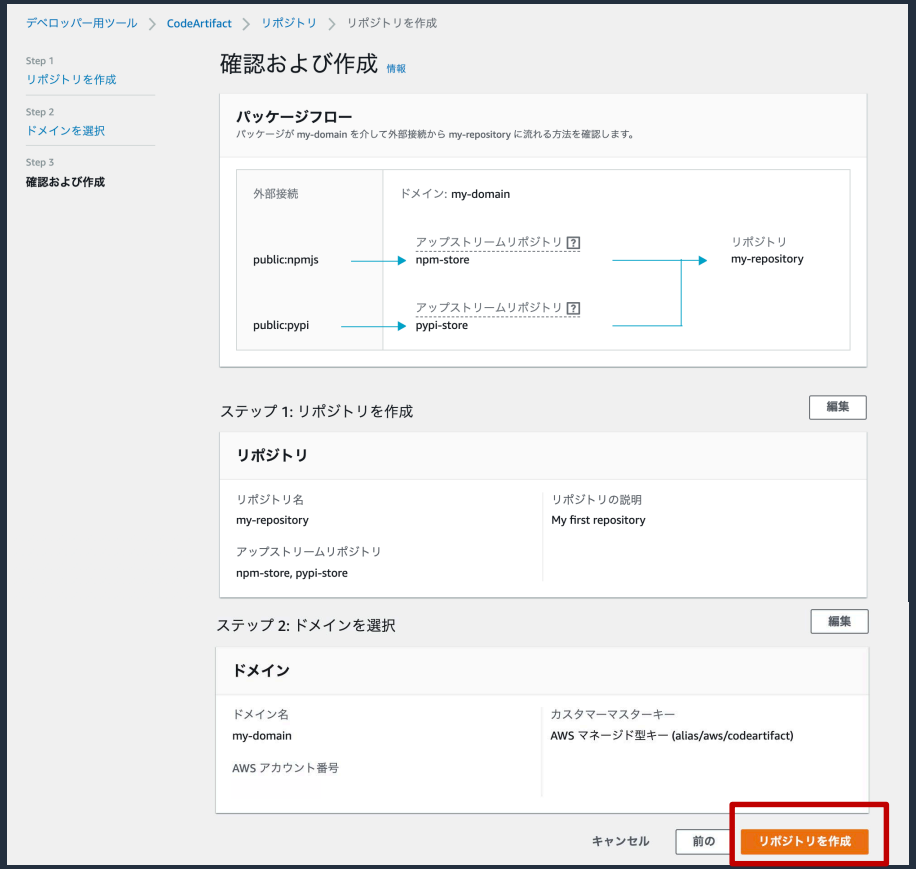
以下を入力

- ドメインのアカウント
- ドメイン名
- 暗号化に利用するキー



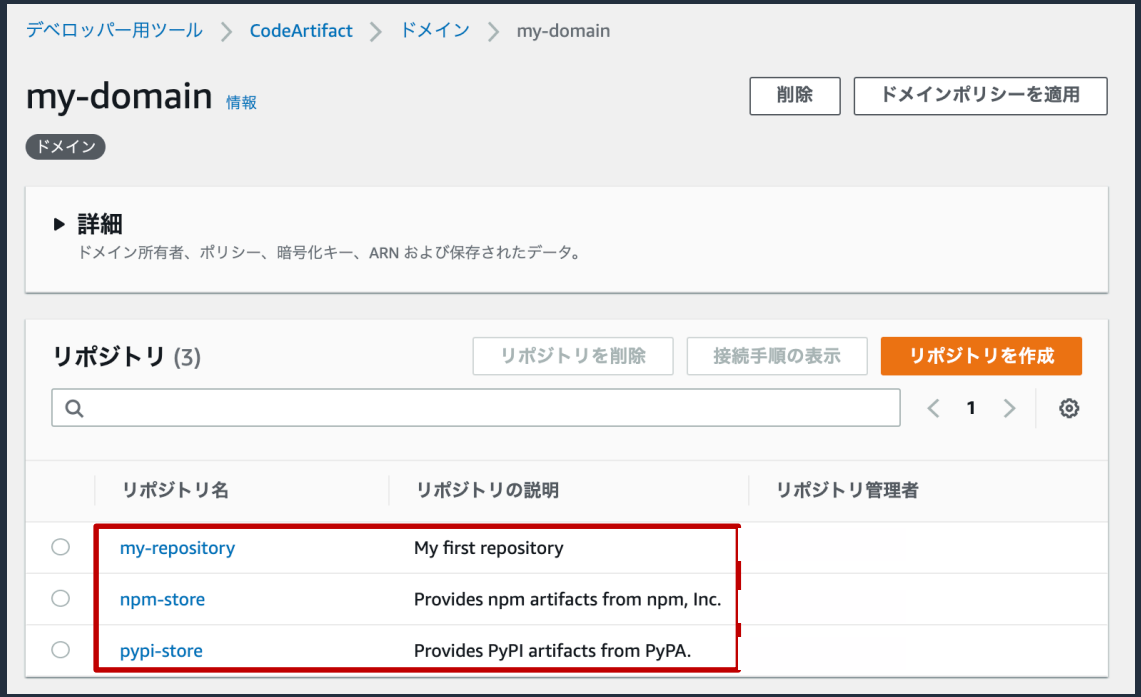
リポジトリの作成

入力内容の確認



リポジトリの作成

作成したリポジトリと、アップストリームを表す追加リポジトリがドメイン内に作成される



パッケージマネージャの設定

パッケージマネージャ毎の設定方法をマネジメントコンソールで確認可能

- AWS CLI を使用した設定を**推奨**
- トークンの**有効期間は 12 時間**

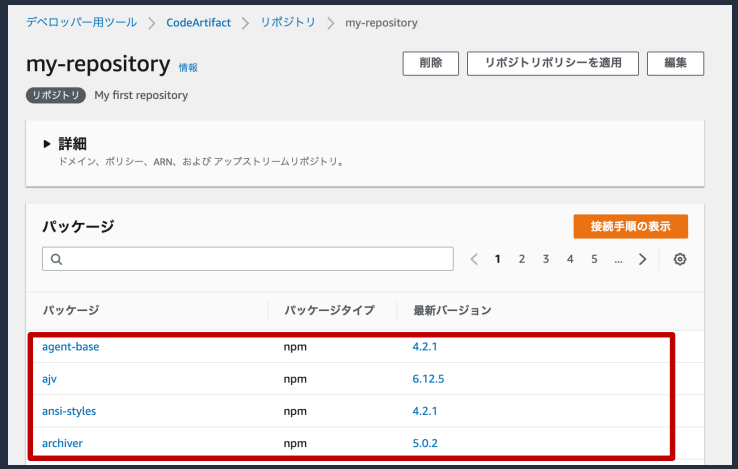

```
aws codeartifact login --tool npm ¥
--repository ${リポジトリ名} ¥
--domain ${ドメイン名} ¥
--domain-owner ${ドメインのアカウントID}
```

パッケージの取得

例：AWS Cloud Development Kit(AWS CDK) のインストール

```
npm install -g aws-cdk
```

AWS CDK と依存するパッケージが npm パブリックリポジトリから
ダウンロードされ、リポジトリに追加される

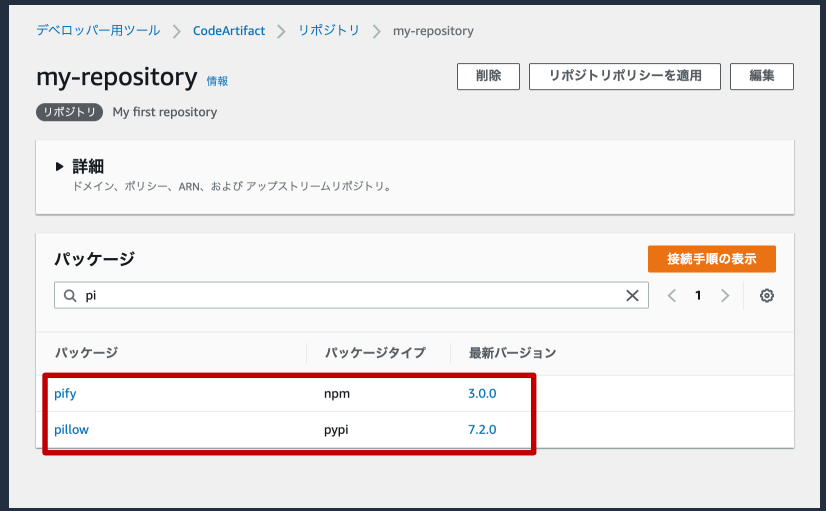


パッケージの取得

例：Pillow のインストール

```
pip3 install Pillow
```

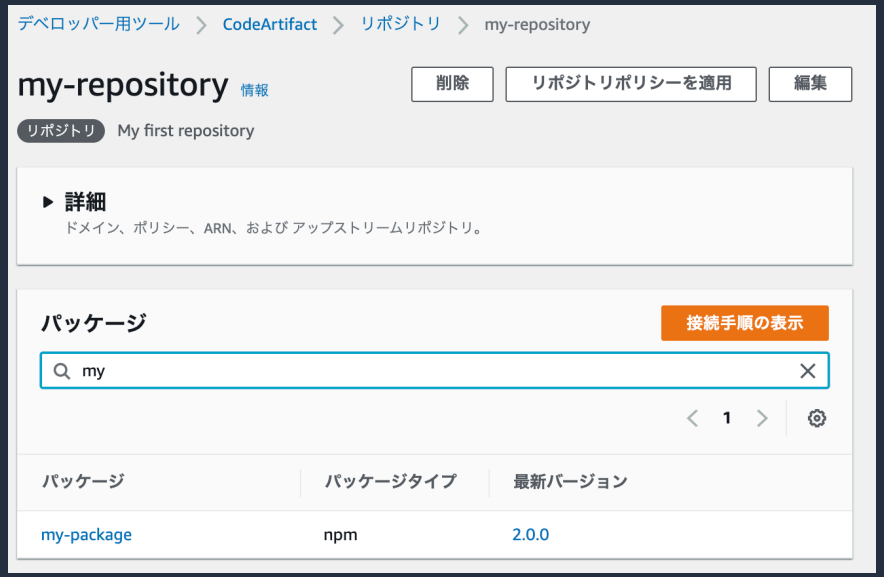
CodeArtifact は **ポリグロット(多言語対応)**
サポートされる任意のタイプのパッケージを格納できる



パッケージの登録

例：独自のパッケージ

```
npm publish
```



AWS CodeBuild からの利用例

CodeBuild でのビルド時にも利用可能

CodeBuild のサービスロールに以下の権限が必要

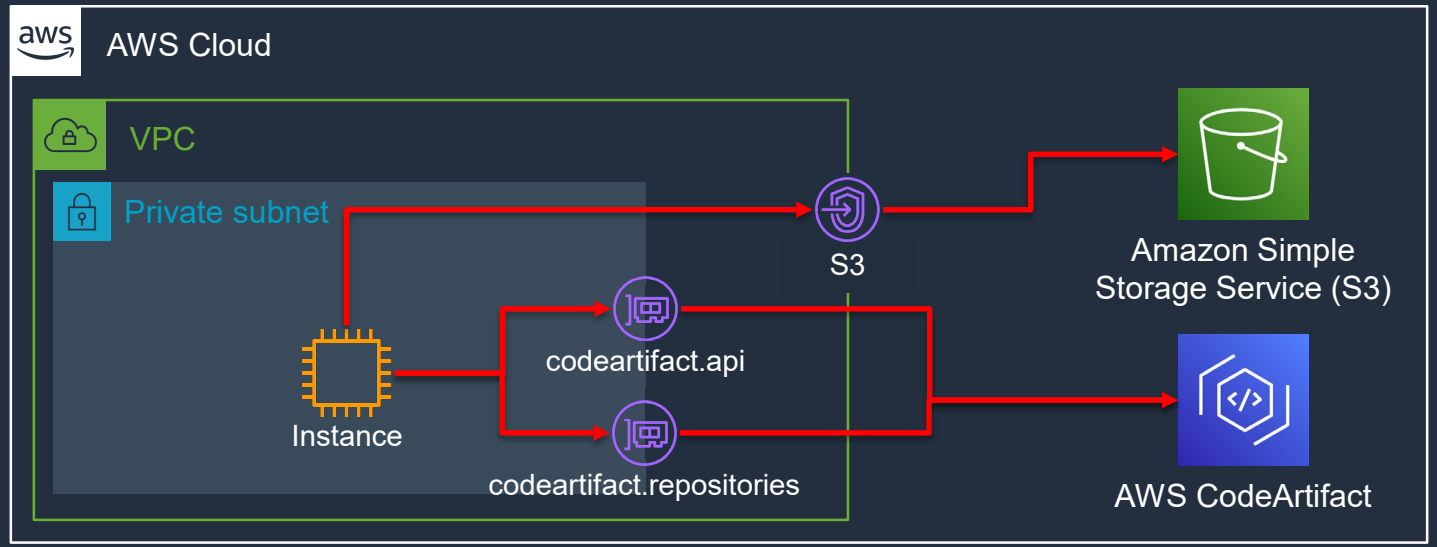
```
pre_build:
  commands:
    - aws codeartifact login --tool npm …
build:
  commands:
    - npm install
```

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [ "codeartifact:GetAuthorizationToken",
                      "codeartifact:GetRepositoryEndpoint",
                      "codeartifact:ReadFromRepository"
                      ],
          "Resource": "*"
      },
      {
          "Effect": "Allow",
          "Action": "sts:GetServiceBearerToken",
          "Resource": "*",
          "Condition": {
              "StringEquals": {
                  "sts:AWSServiceName": "codeartifact.amazonaws.com"
              }
          }
      }
  ]
}
```

詳細は以下を参照：
https://docs.aws.amazon.com/ja_jp/codeartifact/latest/ug/using-npm-packages-in-codebuild.html

VPC エンドポイントをサポート

VPC エンドポイント経由での利用には CodeArtifact だけでなく、**S3 の VPC エンドポイントも必要**



VPC エンドポイントをサポート

VPC エンドポイント経由で CodeArtifact を利用する際は、パッケージマネージャの設定時に**エンドポイント URL の指定が必要**

```
aws codeartifact login --tool npm ¥

--repository ${リポジトリ名} ¥

--domain ${ドメイン名} ¥

--domain-owner ${ドメインのアカウントID} ¥

--endpoint-url ${VPC エンドポイント}
```


aws

AWS CloudTrail を利用した APIコールログ取得

GetAuthorizationToken API の例

```
GetAuthorizationToken API
{
  "eventVersion": "1.05",
  "userIdentity": { "type": "AssumedRole", "principalId": "AIDACKCEVSQ6C2EXAMPLE", ...,
      "sessionContext": {
          "attributes": {...}, "sessionIssuer": {...}
      }
  },
  "eventSource": "codeartifact.amazonaws.com",
  "eventName": "GetAuthorizationToken",
  ...
}
```

詳細は以下を参照：
https://docs.aws.amazon.com/ja_jp/codeartifact/latest/ug/codeartifact-information-in-cloudtrail.html

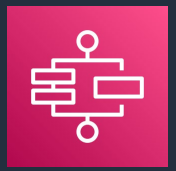
Amazon EventBridge との連携

リポジトリ内のイベント（新しいパッケージバージョンの作成など）をトリガーに処理を自動化できる

- Amazon SNS による通知
- AWS Lambda や AWS Step Functions の起動
- AWS CodePipeline の起動

Amazon Simple Notification Service

AWS Lambda



AWS Step Functions

AWS CodePipeline

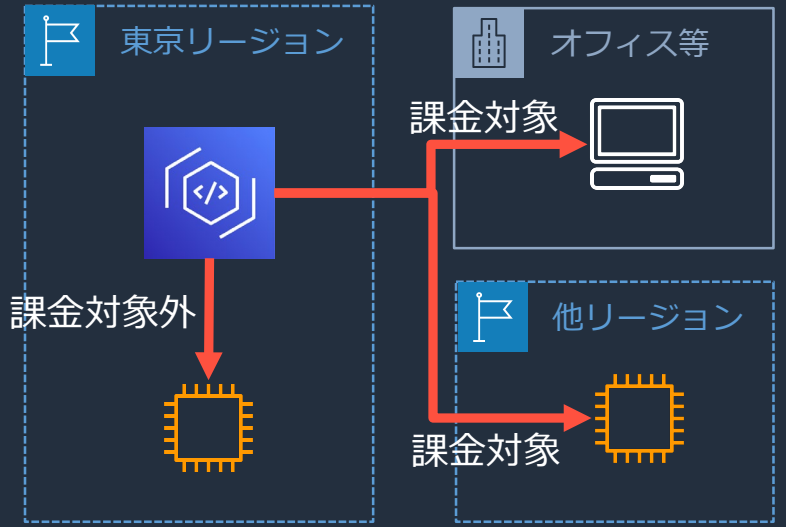
AWS CodeArtifact の制限事項

ドメインの数	アカウントごとに 10 個まで
リポジトリの数	ドメインごとに 1,000 個まで
アセットの数	パッケージバージョンごとに 100 個まで
アセットのサイズ	最大 1 GB
パッケージメタデータファイルのサイズ	最大 100 KB
設定できるアップストリームリポジトリの数	リポジトリ毎に 10 個まで

aws

利用料金

- 料金（東京リージョン）
  - ストレージサイズ
    - $0.055/GB
  - リクエスト数
    - $0.06/10,000 リクエスト
  - データ転送量（アウトバウンド）
    - インターネットへ $0.144/GB
    - 別リージョンへ $0.09/GB
- 無料枠
  - 2GB のストレージ（月）
  - 100,000 回分のリクエスト（月）



まとめ

まとめ

AWS CodeCommit は、
- セキュア
- スケーラブル
- フルマネージドネージド
- Git 互換ソース管理

AWS CodeArtifact は、
- セキュア
- スケーラブル
- フルマネージドネージド
- アーティファクト管理

初期費用無料、従量課金で簡単に使い始めることができる

Q&A

お答えできなかったご質問については
AWS Japan Blog 「https://aws.amazon.com/jp/blogs/news/」にて
後日掲載します。

AWS の日本語資料の場所「AWS 資料」で検索

https://amzn.to/JPArchive

AWS Well-Architected 個別技術相談会

毎週”W-A個別技術相談会”を実施中

- AWSのソリューションアーキテクト(SA)に対策などを相談することも可能
- 申込みはイベント告知サイトから

(https://aws.amazon.com/jp/about-aws/events/)

AWS イベント で[検索]

ご視聴ありがとうございました

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive