# Amazon Elastic Container Registry
# Amazon Elastic Container Registry Public

AWS Black Belt Online Seminar

Solution Architect
浅野佑貴
2021-Dec



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

過去資料
https://amzn.to/JPArchive

# Agenda

- Amazon Elastic Container Registry(Amazon ECR)の概要
  - コンテナワークロードの基本的なワークフロー
  - Amazon ECR とは
- Amazon ECR / Amazon ECR Public の使い方
- 主要な機能

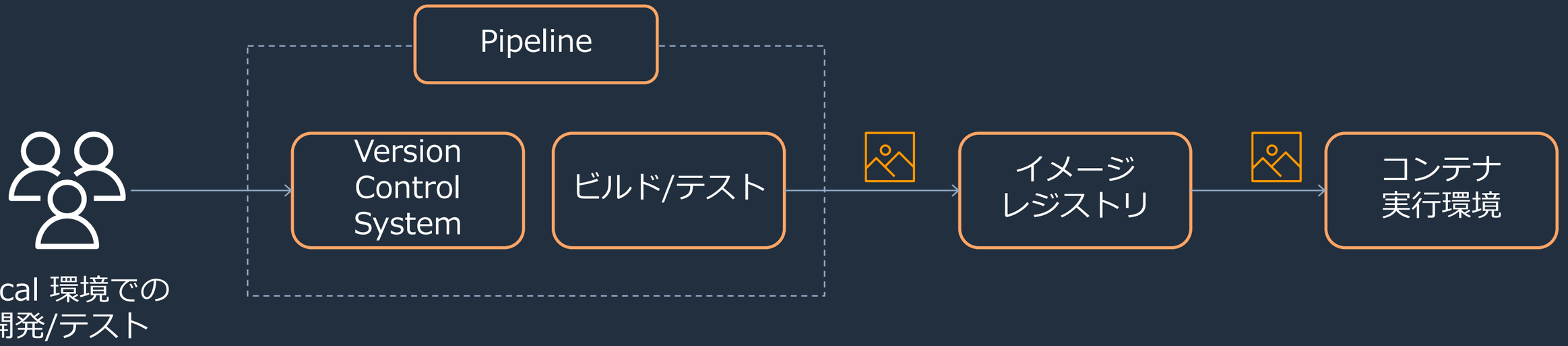


aws

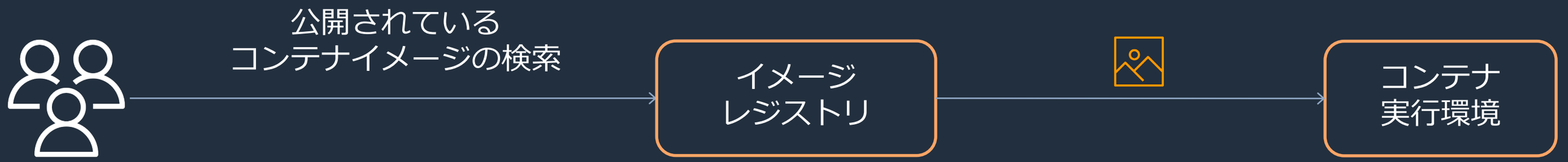
# Amazon Elastic Container Registry (Amazon ECR)の概要

# コンテナワークロードの基本的なワークフロー

プライベートレジストリ




パブリックレジストリ






aws

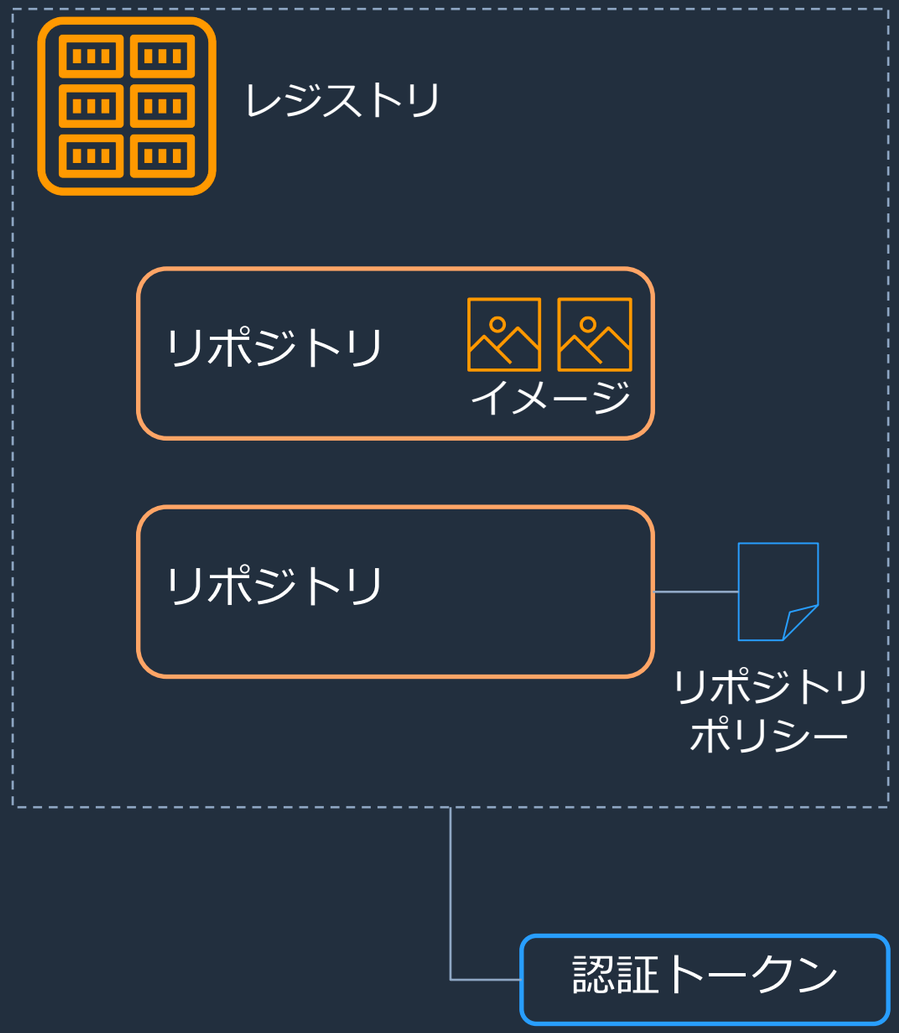
# Amazon ECRとは

- コンテナイメージレジストリのマネージドサービス
- Docker CLI コマンドを利用することが可能
- コンテナイメージ/アーティファクトはAmazon S3に保存される
- サポートする形式
  - Docker イメージ(v1,v2)
  - Open Container Initiative (OCI) イメージ
  - OCI 互換 artifacts



aws

# 基本コンセプト




- レジストリ
  - AWS アカウントごとに用意される
  - イメージを保存するためのリポジトリを複数作成可能
  - Docker クライアントを認証して利用
- リポジトリ
  - Docker イメージ、OCI イメージ、OCI 互換アーティファクトを保存
- リポジトリポリシー
  - リポジトリとリポジトリ内のイメージへのアクセス権を制御
- 認証トークン
  - IAM認証情報を利用して、レジストリに対して認証をする



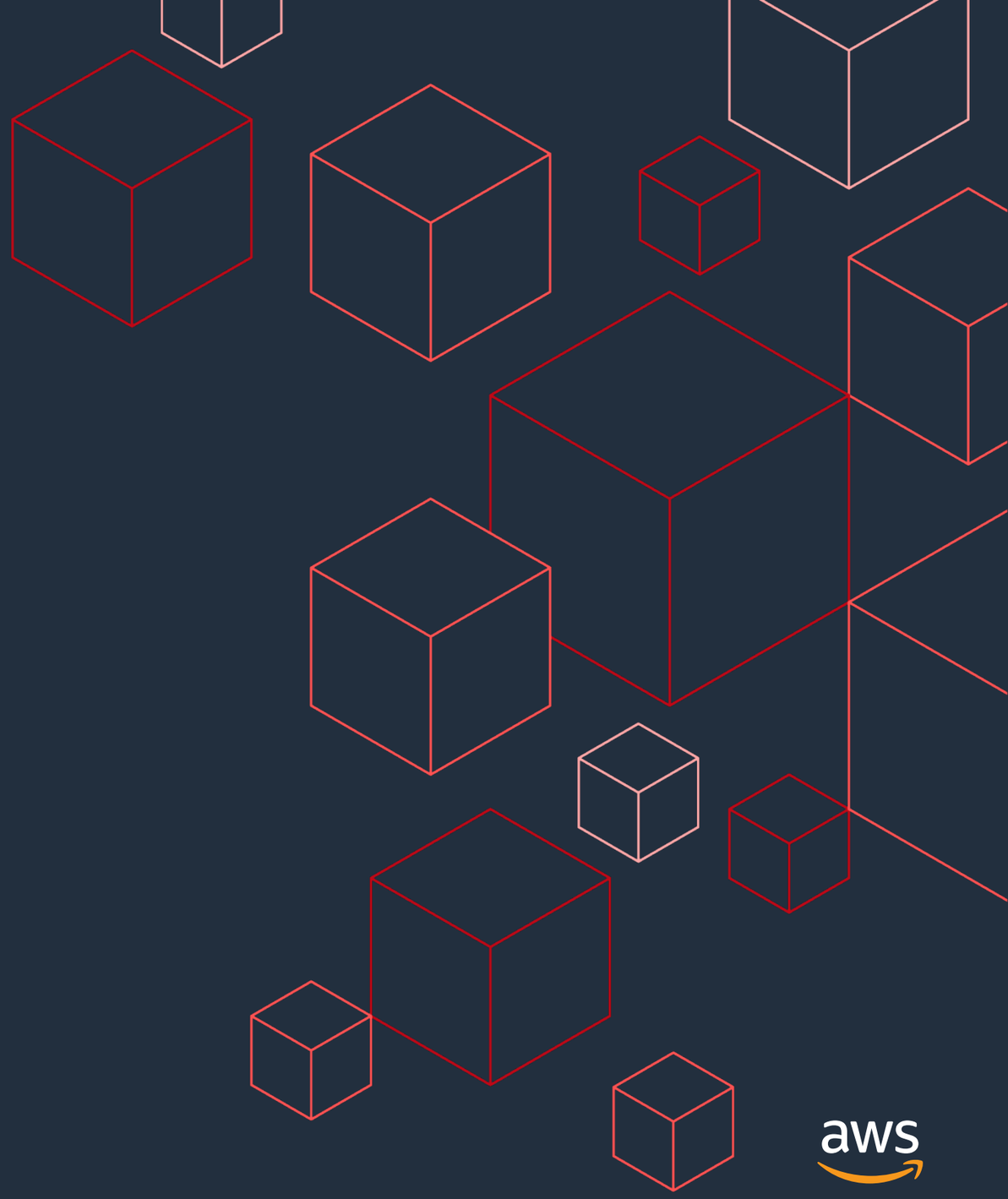
aws

# サポートする2つのアクセスタイプ

- プライベートレジストリ
  - 利用する(pull・push等)には IAM ベース認証が必須
- パブリックレジストリ
  - Amazon ECR Public
  - 認証無しでもイメージのpullが可能
  - 公開されているイメージを検索可能
- Amazon ECR / Amazon ECR Publicそれぞれでサポートされている機能が異なる


https://docs.aws.amazon.com/ja_jp/AmazonECR/latest/userguide/what-is-ecr.html
https://docs.aws.amazon.com/ja_jp/AmazonECR/latest/public/what-is-ecr.html

# Amazon ECR
# Amazon ECR Public
# の使い方



# プライベートレジストリの利用例

開発者

1. 認証トークンの取得とDocker クライアントを認証

```
$ aws ecr get-login-password | ¥
docker login --username AWS --password-stdin ¥
123456789012.dkr.ecr.<region>.amazonaws.com
```

2. イメージのビルド

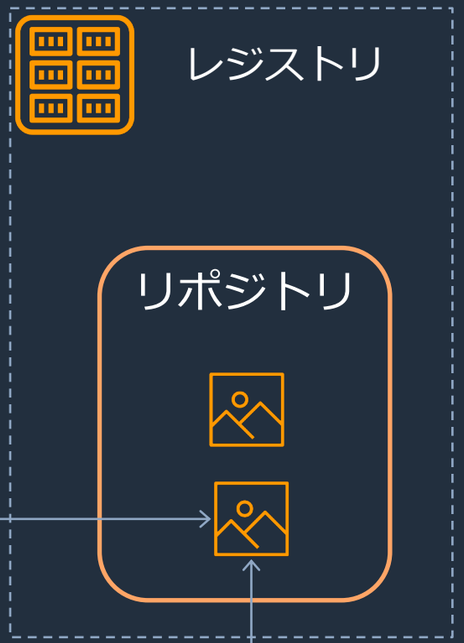
```
$ docker build ・・・・
```

3. イメージにタグ付け

```
$ docker tag <image> 123456789012.dkr.ecr.<region>.amazonaws.com/<image>:<tag>
```

4. イメージのpush

```
$ docker push 123456789012.dkr.ecr.<region>.amazonaws.com/<image>:<tag>
```




認証されていない利用者

```
$ docker pull 123456789012.dkr.ecr.<region>.amazonaws.com/<image>:<tag>
```

# パブリックレジストリの利用例

開発者

1. 認証トークンの取得とDocker クライアントを認証

$ aws ecr-public get-login-password --region us-east-1 | docker login --username AWS --password-stdin public.ecr.aws

2. イメージのビルド

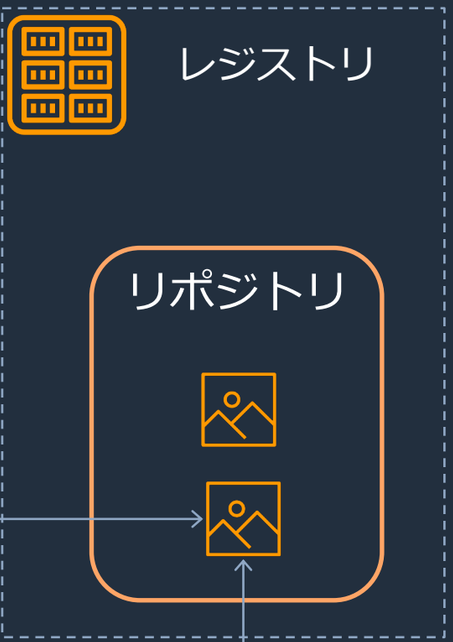
$ docker build ・・・・

3. イメージにタグ付け

$ docker tag <image> public.ecr.aws/<alias>/<image>:<tag>

4. イメージのpush

$ docker push public.ecr.aws/<alias>/<image>:<tag>




認証されていない利用者

$ docker pull public.ecr.aws/<alias>/<image>:<tag>

# Amazon ECR Docker Credential Helper

- Docker Deamon向けのcredential helper
- Dockerクライアントからより簡単にECRを利用することが可能
- プライベートレジストリ/パブリックレジストリ共に利用可能

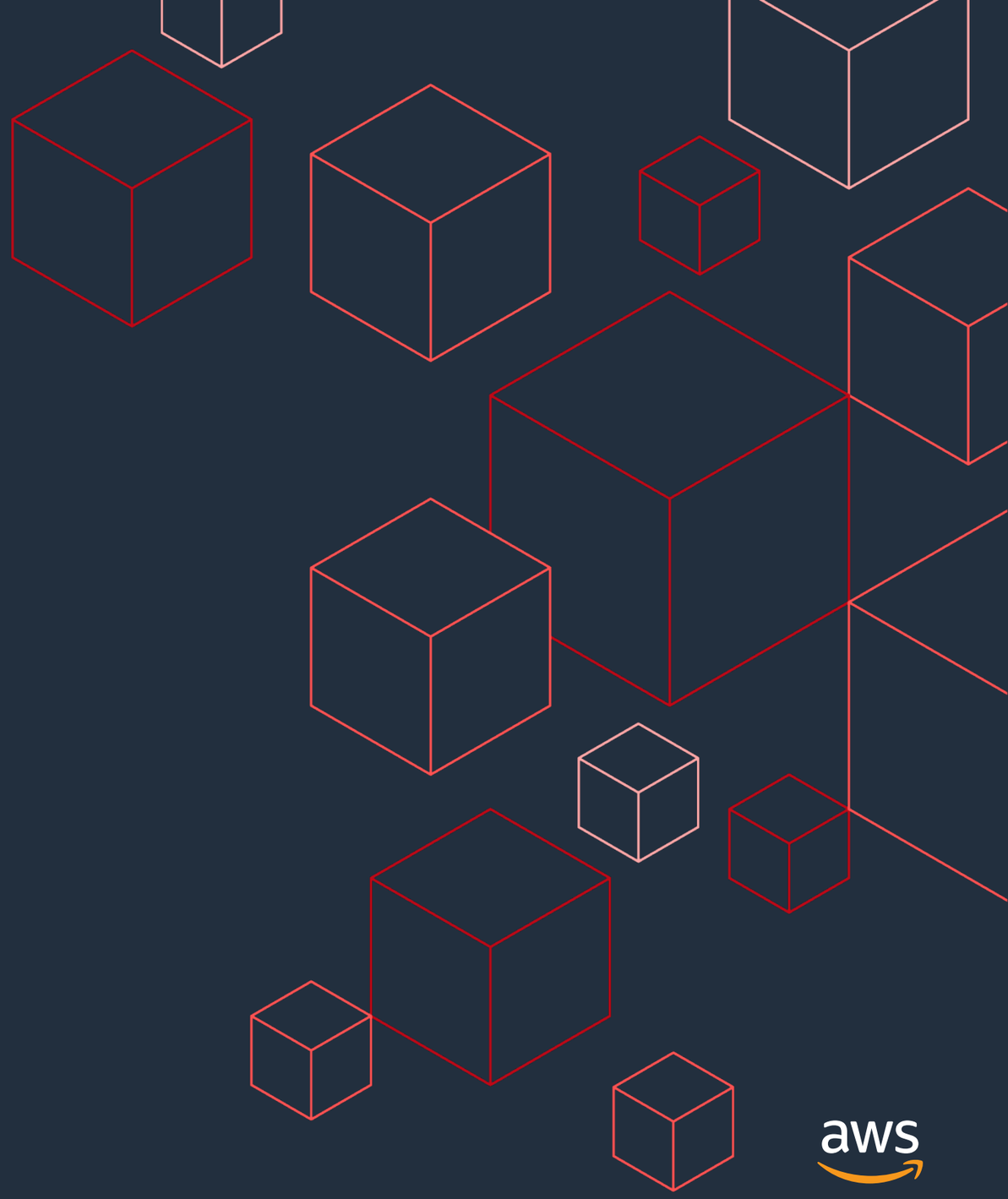
```
$ cat ./docker/config.json
{
        "credHelpers": {
                ”123456789012.dkr.ecr.ap-northeast-1.amazonaws.com": "ecr-login",
                "public.ecr.aws": "ecr-login”
         < snip >
}
$ docker pull 123456789012.dkr.ecr.<region>.amazonaws.com/<image>:<tags>
```

https://github.com/awslabs/amazon-ecr-credential-helper



aws

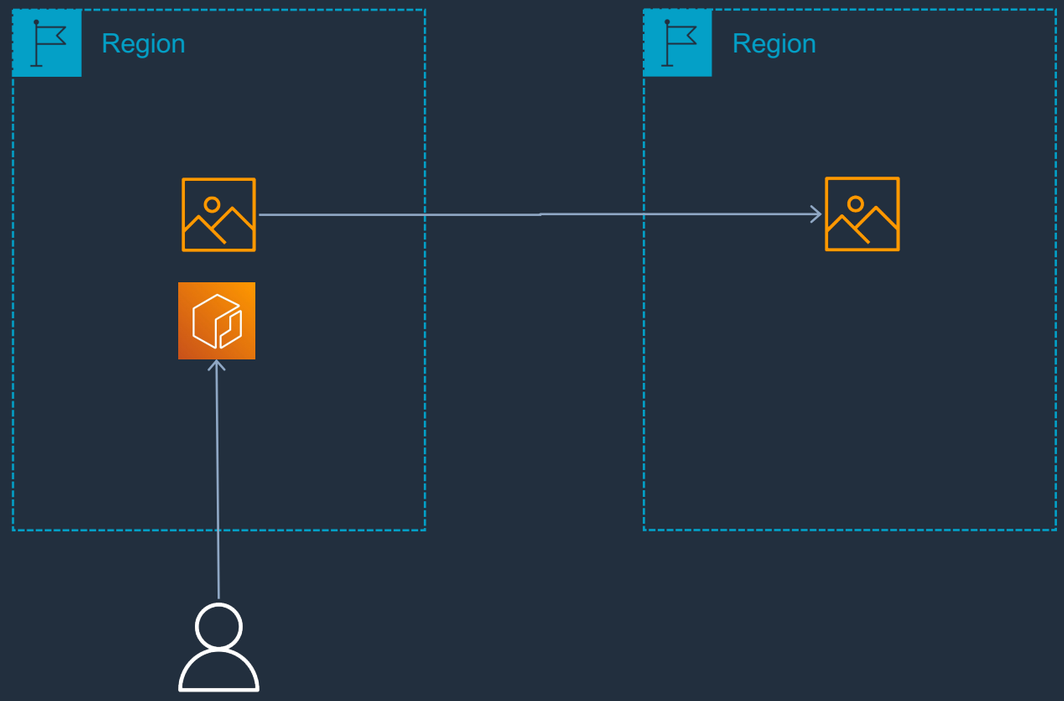
# 主要な機能



# イメージのクロスリージョンレプリケーション

プライベートレジストリ

- コンテナイメージを別リージョン・別AWSアカウントにレプリケーションすることが可能
- イメージをpushした際に自動でレプリケーションされる
- 脆弱性の検出結果はレプリケーションされない

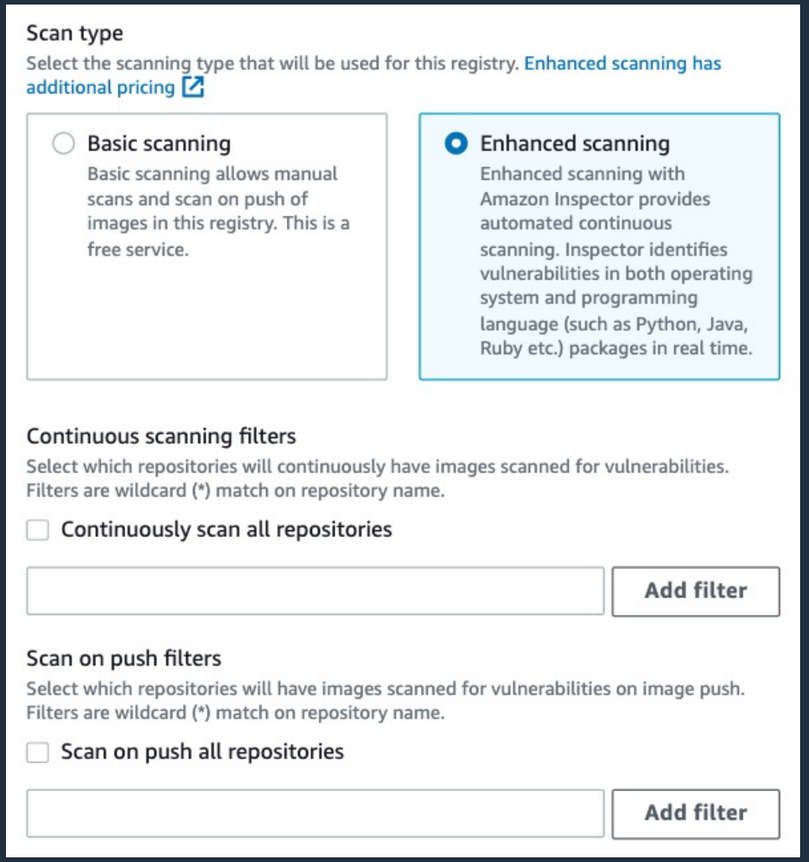



https://docs.aws.amazon.com/AmazonECR/latest/userguide/replication.html
https://aws.amazon.com/jp/blogs/news/cross-region-replication-in-amazon-ecr-has-landed-jp/

# イメージの脆弱性スキャン

プライベートレジストリ

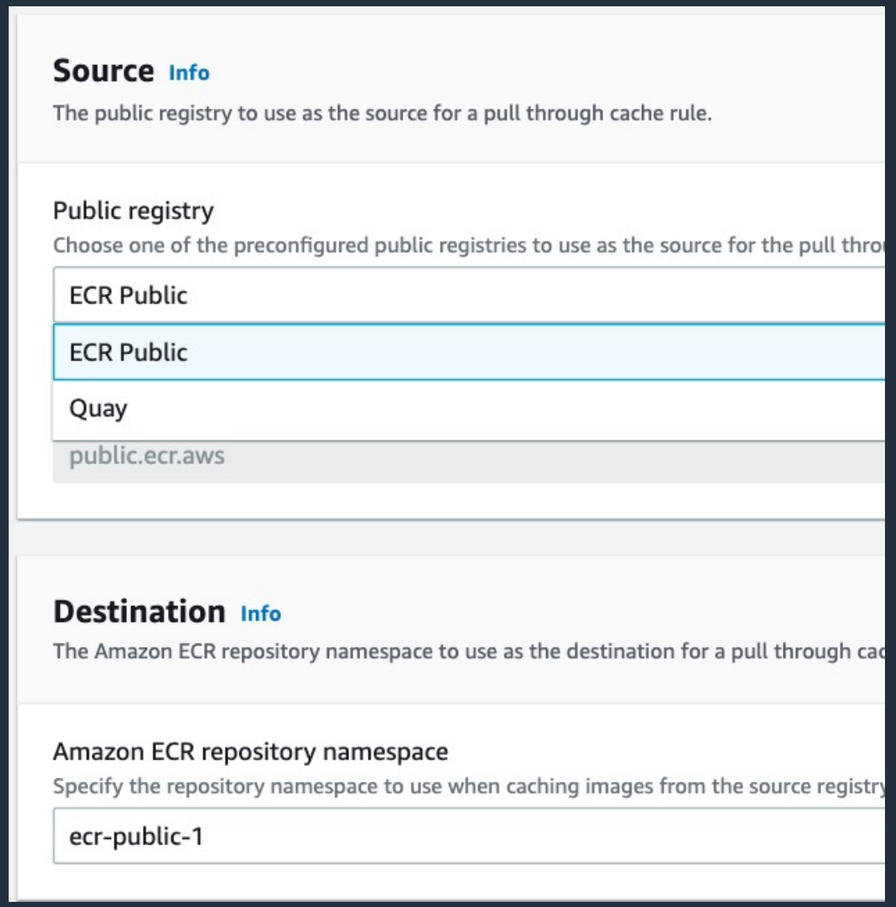
- ECR に pushされたコンテナイメージの脆弱性の検出をする
- Basic scanning
  - 検出対象：OSパッケージ
  - スキャン実行： on push / マニュアル実行
  - 追加料金なしで利用可能
- Enhanced scanning
  - 検出対象：OSパッケージ、プログラミングライブラリ
  - スキャン実行： on push / 継続的
  - Amazon Inspectorとの統合



# Pull Through Cache

プライベートレジストリ

- パブリックレジストリのイメージを ECR Private でキャッシュ
- リモートレジストリと自動同期
  - 24時間以内に同期される
- アップストリームのパブリックレジストリとして ECR Public と Quay.io をサポート




https://docs.aws.amazon.com/ja_jp/AmazonECR/latest/userguide/pull-through-cache.html

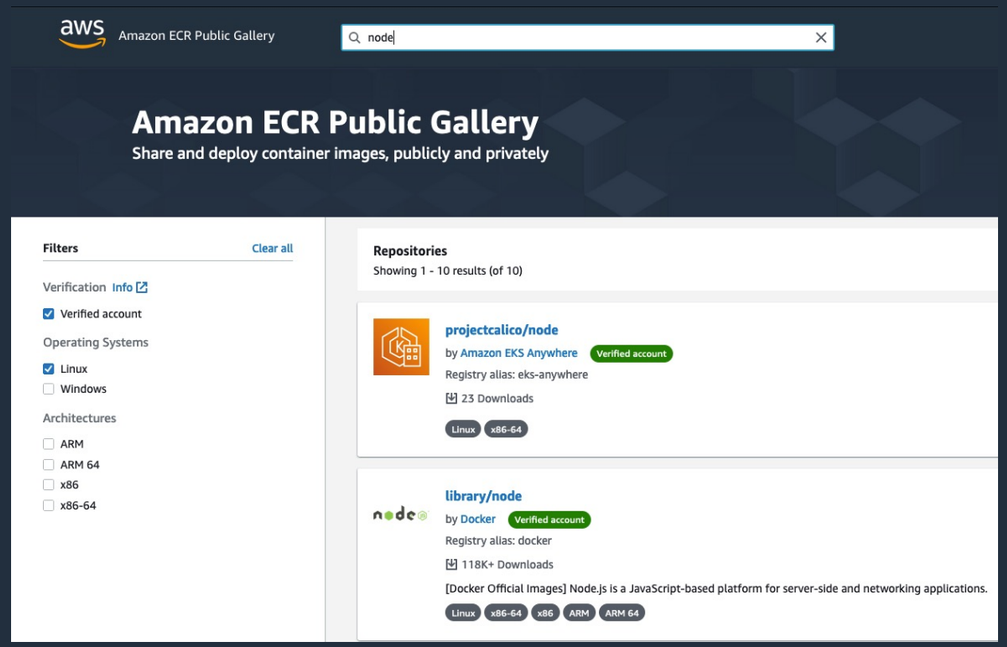


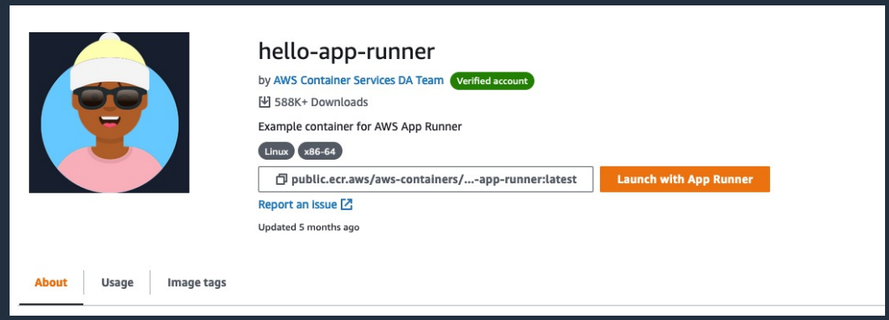
aws

# Amazon ECR Public Gallery

パブリックレジストリ

- Amazon ECR public で公開されているコンテナイメージを検索
- Docker 公式イメージも利用可能
- AWS App Runner サービスを直接起動することも可能




https://docs.aws.amazon.com/AmazonECR/latest/public/public-gallery.html
https://aws.amazon.com/jp/blogs/news/docker-official-images-now-available-on-amazon-elastic-container-registry-public/