アイデンティティラウンドロビンワークショップ

ラウンド１：サーバーレス–ホストされた静的ウェブサイト

aws | Pop-up Loft

このラウンドの予定

- AWS IAM のコンセプト
- Cognito を使用したアプリケーションユーザー管理
- WildRydes サーバーレスアプリケーション
- グループ実習
- レビューとディスカッション

https://awssecworkshops.com

プリンシパルのレイヤーの考察

アプリケーション
- アイデンティティ: アプリケーションユーザー、アプリケーション管理者

オペレーティングシステム
- アイデンティティ: 開発者またはシステムエンジニア (あるいはその両方)

AWS
- アイデンティティ: 開発者、ソリューションアーキテクト、テスター、ソフトウェア/プラットフォーム
- AWS アイデンティティの操作:
  - EC2 インスタンスおよび EBS ストレージのプロビジョニング/プロビジョニング解除
  - Elastic Load Balancer の構成
  - S3 オブジェクトまたは DynamoDB のデータへのアクセス
  - DynamoDB のデータへのアクセス
  - SQS キューの操作
  - SNS 通知の送信

プリンシパルのレイヤーの考察

アプリケーション

- アイデンティティ: アプリケーションユーザー、アプリケーション管理者

オペレーティングシステム

- アイデンティティ: 開発者またはシステムエンジニア (あるいはその両方)

AWS

- アイデンティティ: 開発者、ソリューションアーキテクト、テスター、ソフトウェア/プラットフォーム
- AWS アイデンティティの操作:
  - EC2 インスタンスおよび EBS ストレージのプロビジョニング/プロビジョニング解除
  - Elastic Load Balancer の構成
  - S3 オブジェクトまたは DynamoDB のデータへのアクセス
  - DynamoDB のデータへのアクセス
  - SQS キューの操作
  - SNS 通知の送信

AWS プリンシパル

アカウント所有者 ID (ルートアカウント)

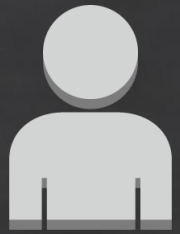
- すべての登録済みサービスへのアクセス
- 請求へのアクセス
- コンソールと API へのアクセス
- カスタマーサポートへのアクセス

AWS Identity and Access Management (IAM)

- 特定のサービスへのアクセス
- コンソールまたは API (あるいはその両方) へのアクセス
- カスタマーサポート (ビジネスおよびエンタープライズ) へのアクセス

AWS Identity and Access Management (IAM)

AWS アカウントにおいてユーザーが実行できる処理を個別に制御可能



IAM ユーザー

IAM グループ

IAM ロール

ポリシー

AWS IAM ポリシータイプ

アイデンティティベース
ポリシー

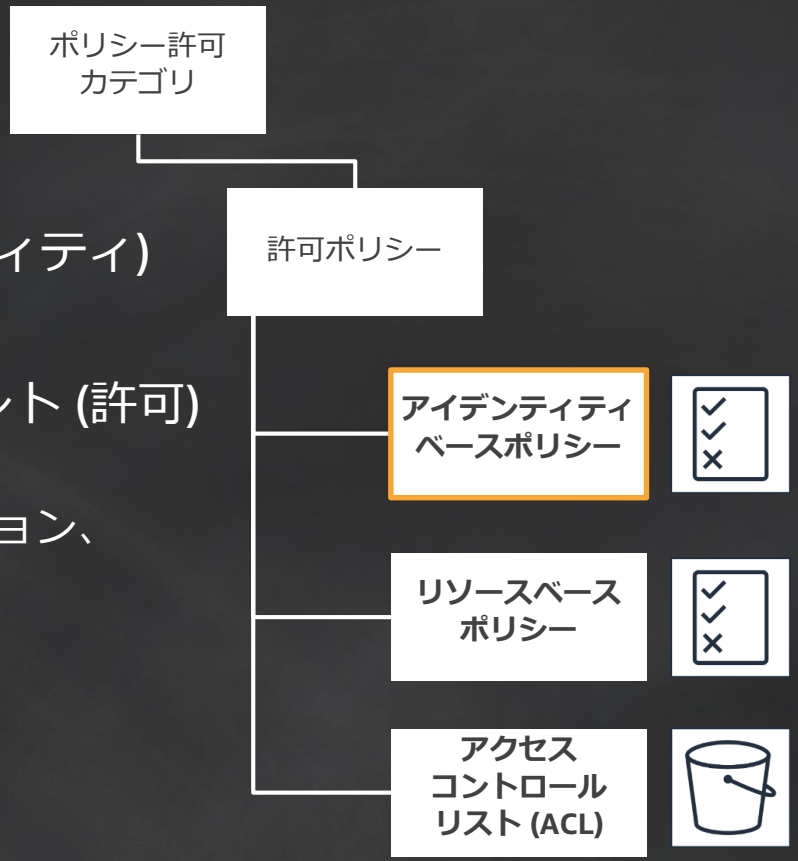
リソースベース
ポリシー

アクセスコントロール
リスト

AWS IAM ポリシータイプ

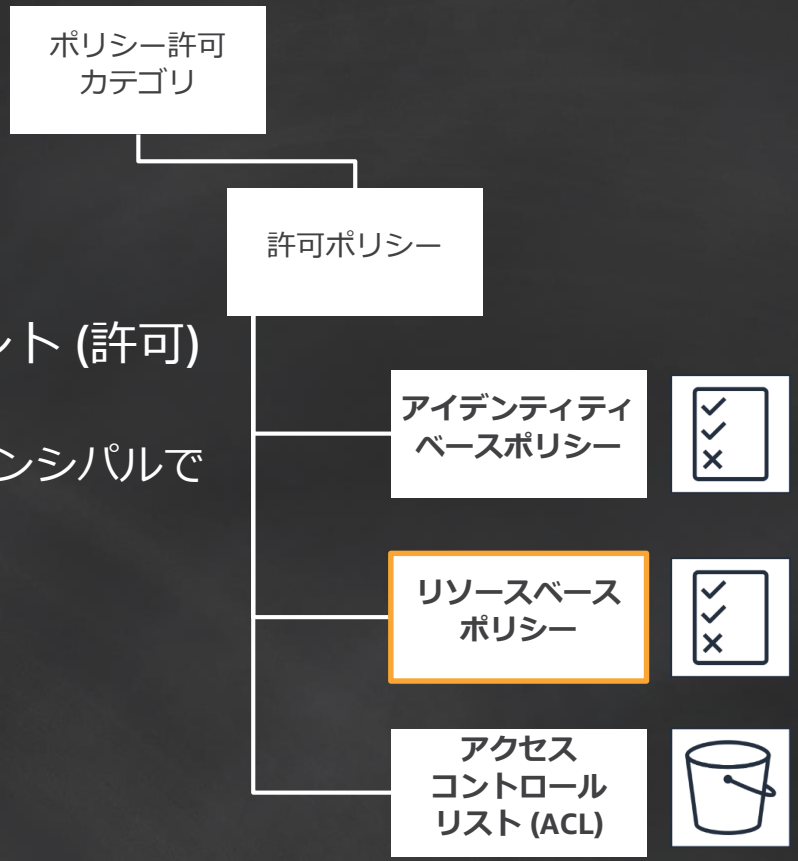
- JSON 形式のドキュメント
- **プリンシパル** (またはアイデンティティ) にアタッチ
- 次の内容を指定したステートメント (許可) を含む:
  - プリンシパルで実行可能なアクション、対象リソース、実行条件

Principal (暗黙的)
Action
Resource
Condition



AWS IAM ポリシータイプ

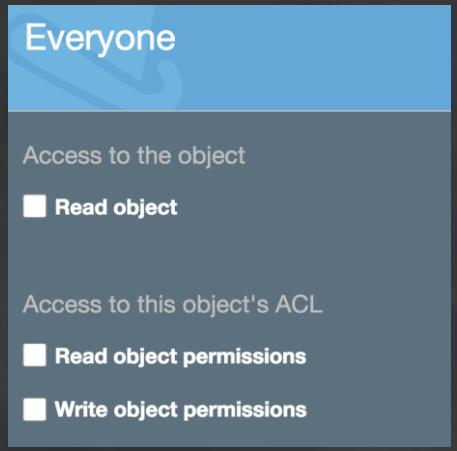
- JSON 形式のドキュメント
- リソースにアタッチ
- 次の内容を指定したステートメント (許可) を含む:
  - 該当リソースに対して特定のプリンシパルで実行可能なアクションと実行条件

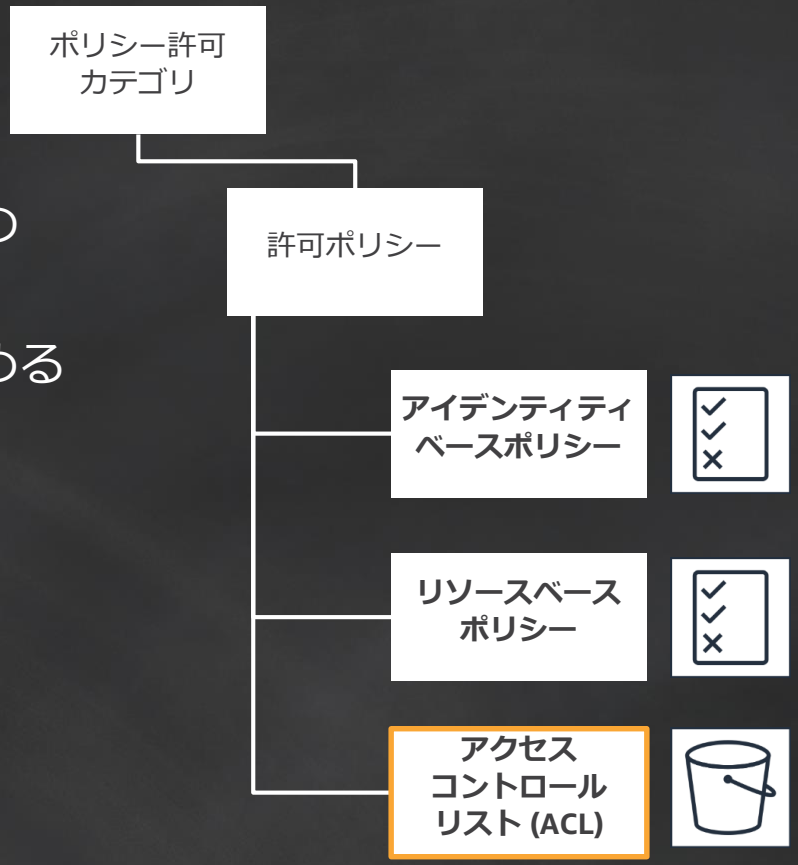


Principal
Action
Resource
Condition

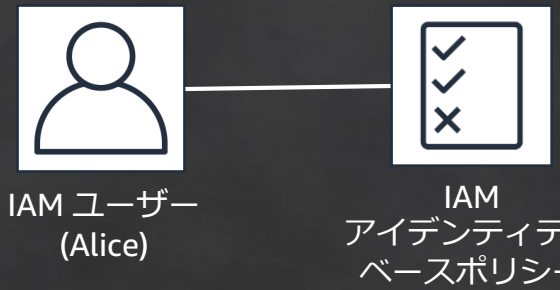
AWS IAM ポリシータイプ

- バケットおよびオブジェクトへのアクセスの管理
- 付与されるユーザーと許可を含める





IAM アイデンティティベース ポリシーの例




```
"Version": "2012-10-17"
"Statement": [
  {
    "Effect": "Allow",
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::examplebucket/*"
  }
 ]
```

IAM アイデンティティベース ポリシーの例


```
"Version": "2012-10-17"
"Statement": [
  {
    "Effect": "Allow",
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::examplebucket/*”,
    "Condition": {
      "StringEquals": {
        "s3:ExistingObjectTag/classification": ”sensitive"
      }
    }
  }
]
```

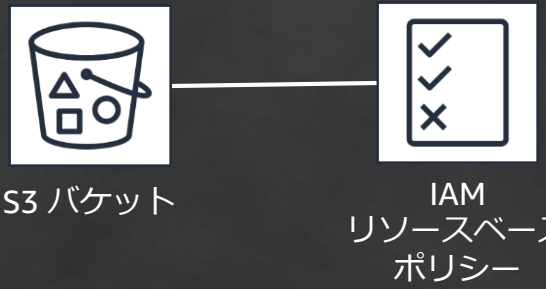
IAM リソースベース ポリシーの例

S3 バケット

IAM
リソースベース
ポリシー

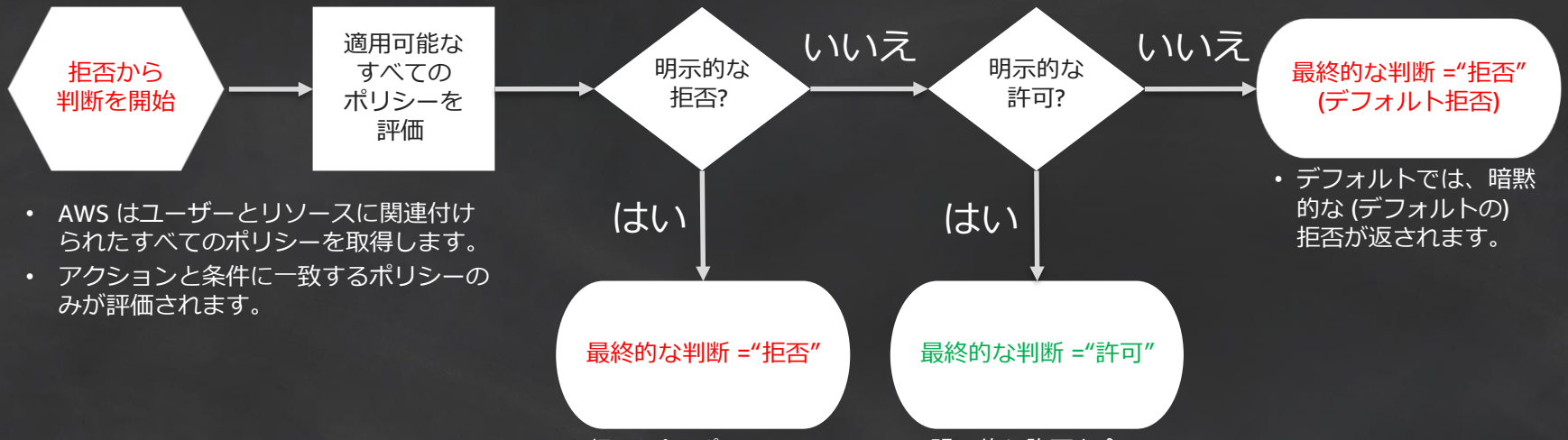
```
"Version": "2012-10-17"
"Statement": [
  {
    "Effect": "Allow",
          ”Principal": {
     "AWS" : "*"
    },
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::examplebucket/*”
  }
]
```

IAM リソースベース ポリシーの例




```
"Version": "2012-10-17"
"Statement": [
  {
    "Effect": "Allow",
          ”Principal": {
     "AWS" : "*"
    },
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::examplebucket/*”,
    "Condition" : {
     "IpAddress" : {
       "aws:SourceIp": "192.168.143.0/24"
      },
    }
   }
 ]
```

IAM ポリシーの評価ロジック



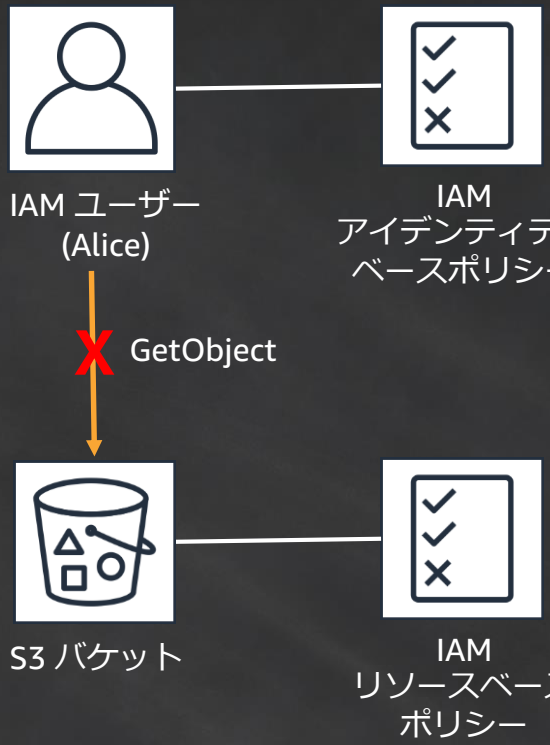
- AWS はユーザーとリソースに関連付けられたすべてのポリシーを取得します。
- アクションと条件に一致するポリシーのみが評価されます。

- デフォルトでは、暗黙的な (デフォルトの) 拒否が返されます。

- 拒否を含むポリシーステートメントが、その他すべてのポリシーステートメントより優先されます。

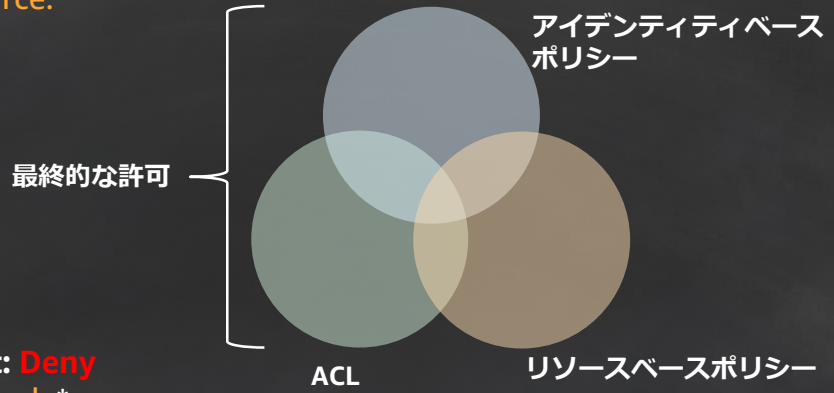
- 明示的な許可を含み、拒否が含まれていない場合、アクセス権が付与されます。

IAM ポリシーの評価ロジック – 例 1

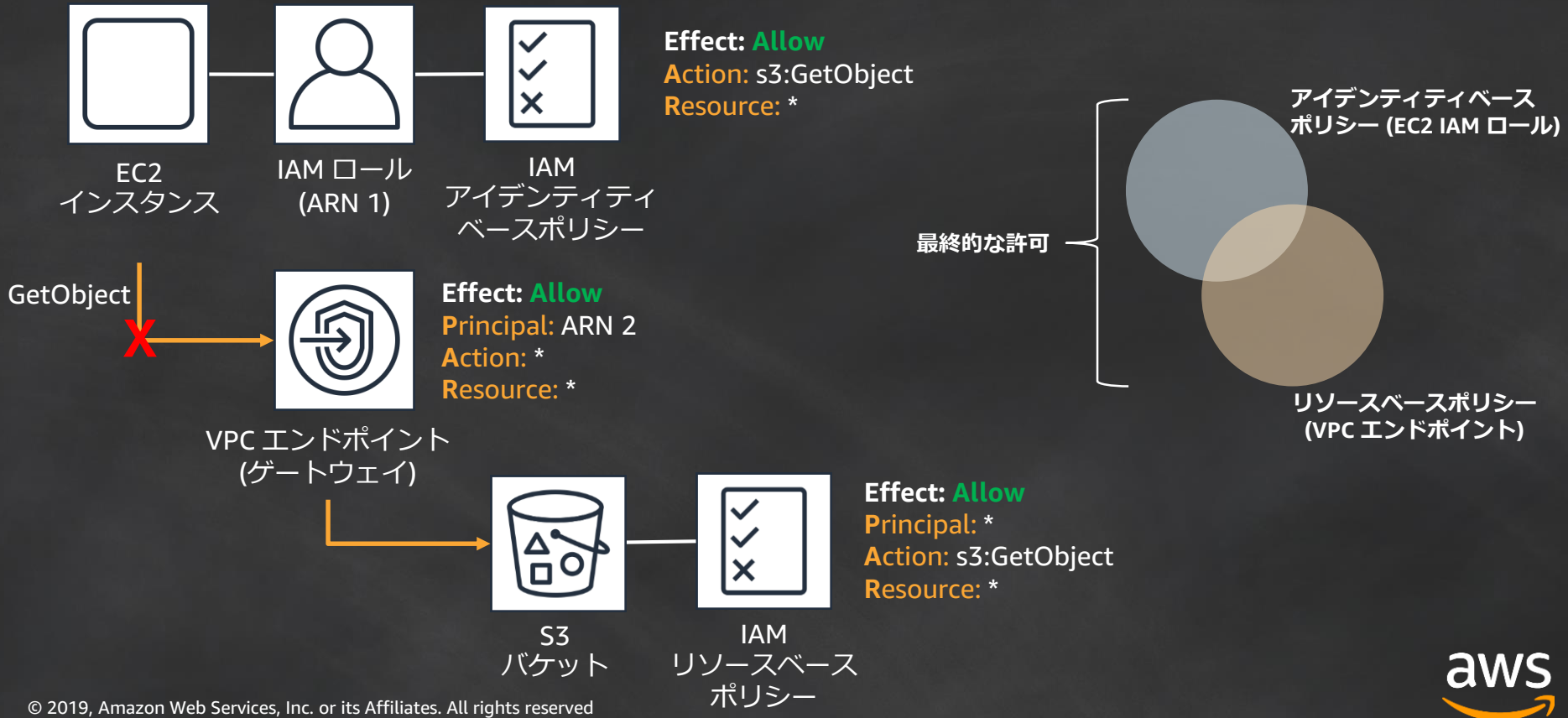


Effect: Allow
Action: s3:GetObject
Resource: *

Effect: Deny
Principal: *
Action: s3:GetObject
Resource: *



IAM ポリシーの評価ロジック – 例 2



プリンシパルのレイヤーの考察

アプリケーション
- アイデンティティ: アプリケーションユーザー、アプリケーション管理者

オペレーティングシステム
- アイデンティティ: 開発者またはシステムエンジニア (あるいはその両方)

AWS
- アイデンティティ: 開発者、ソリューションアーキテクト、テスター、ソフトウェア/プラットフォーム
- AWS アイデンティティの操作:
  - EC2 インスタンスおよび EBS ストレージのプロビジョニング/プロビジョニング解除
  - Elastic Load Balancer の構成
  - S3 オブジェクトまたは DynamoDB のデータへのアクセス
  - DynamoDB のデータへのアクセス
  - SQS キューの操作
  - SNS 通知の送信

aws

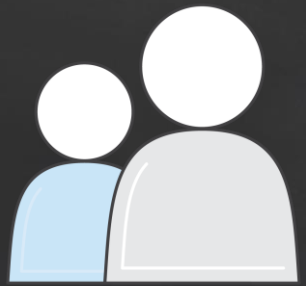
Amazon Cognito

ウェブおよびモバイルアプリのためのアイデンティティ

セキュリティと
アクセス

ユーザーの
所有権

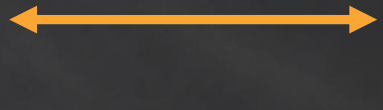
エクスペリエンス



顧客関係

Amazon Cognito

ウェブおよび
モバイルアプリ



Amazon
Cognito

Cognito ユーザープール

Cognito ID プール

マネージドユーザー
ディレクトリ

AWS 認証情報

フェデレーション

SAML

Hosted UI

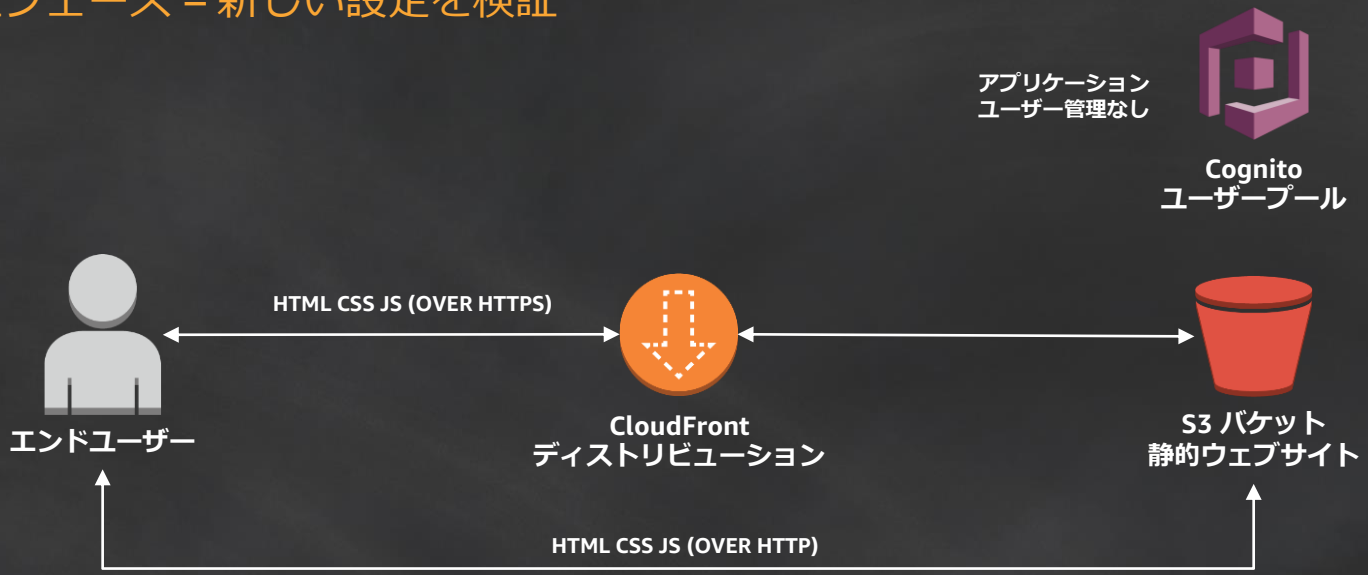
標準的なトークン

開発者はアプリの
重要な部分に集中

Cognito は認証と
アイデンティティを処理

WildRydes サーバーレスアプリケーション

- 構築フェーズ – アクセス制御を設定
- 検証フェーズ – 新しい設定を検証



WildRydes サーバーレスアプリケーション

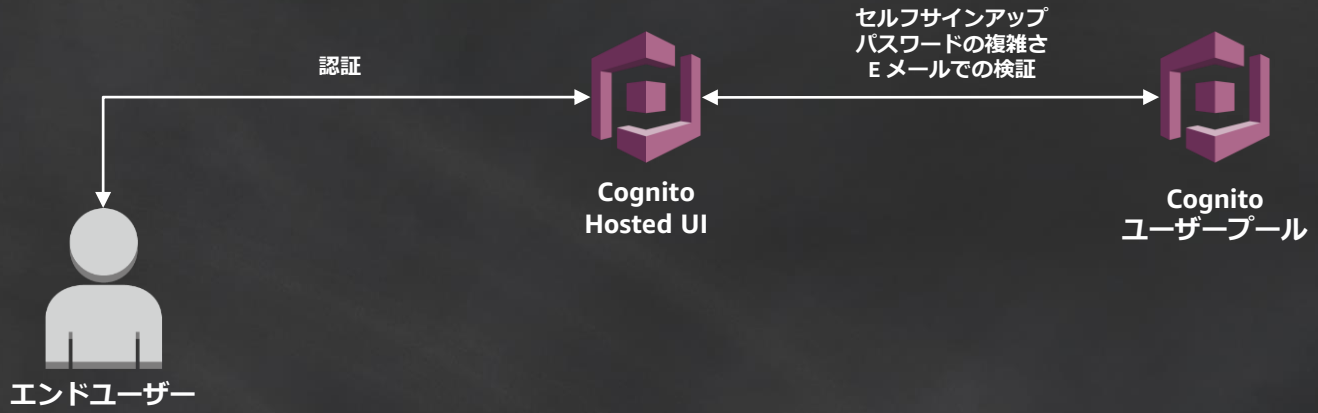
構築フェーズ - タスク 1

オリジンの攻撃対象となりうる箇所を減らす

WildRydes サーバーレスアプリケーション

構築フェーズ - タスク 2

アプリケーションユーザー管理の設定



WildRydes サーバーレスアプリケーション

構築フェーズ（１時間）

https://awssecworkshops.com/

内容:

- ワークショップ (上部ナビゲーション)
  - アイデンティティラウンドロビン
  - **サーバーレスラウンド – シナリオ (右下)**
    - ***AWS* 提供イベント**
  - **構築フェーズ (右下)**
    - **タスク 1 – S3オリジンの攻撃対象となりうる箇所を減らす**
    - **タスク 2 – アプリケーションユーザー管理の設定**

WildRydes サーバーレスアプリケーション

検証フェーズ (15 分)

https://awssecworkshops.com/

内容:

- ワークショップ
  - アイデンティティラウンドロビン
  - サーバーレスラウンド – シナリオ
  - ビルドフェーズ
  - **検証フェーズ (右下)**
    - **他のチームの AWS アカウントにログイン**
    - **タスク 1 と 2 の検証**

WildRydes サーバーレスアプリケーション

アーキテクチャ

レビューとディスカッション

S3 バケットへのアクセス制限はどのように行いましたか?

レビューとディスカッション

S3 バケットへのアクセス制限はどのように行いましたか?

許可ステートメント

```
{
  "Sid": ”AllowCF",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity <OAI ID>"
  },
  "Action": "s3:GetObject",
  "Resource": "arn:aws:s3:::<BUCKET NAME>/*"
}
```

レビューとディスカッション

S3 バケットへのアクセス制限はどのように行いましたか?

拒否ステートメント

```
{
  "Sid": “DenyMost”,
  "Effect": "Deny",
  "NotPrincipal": {
    "AWS": [
      "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity <OAI ID>"
    ]
  },
  "Action": "s3:GetObject",
  "Resource": "arn:aws:s3:::<BUCKET NAME>/*”
}
```

レビューとディスカッション

S3 バケットへのアクセス制限はどのように行いましたか?

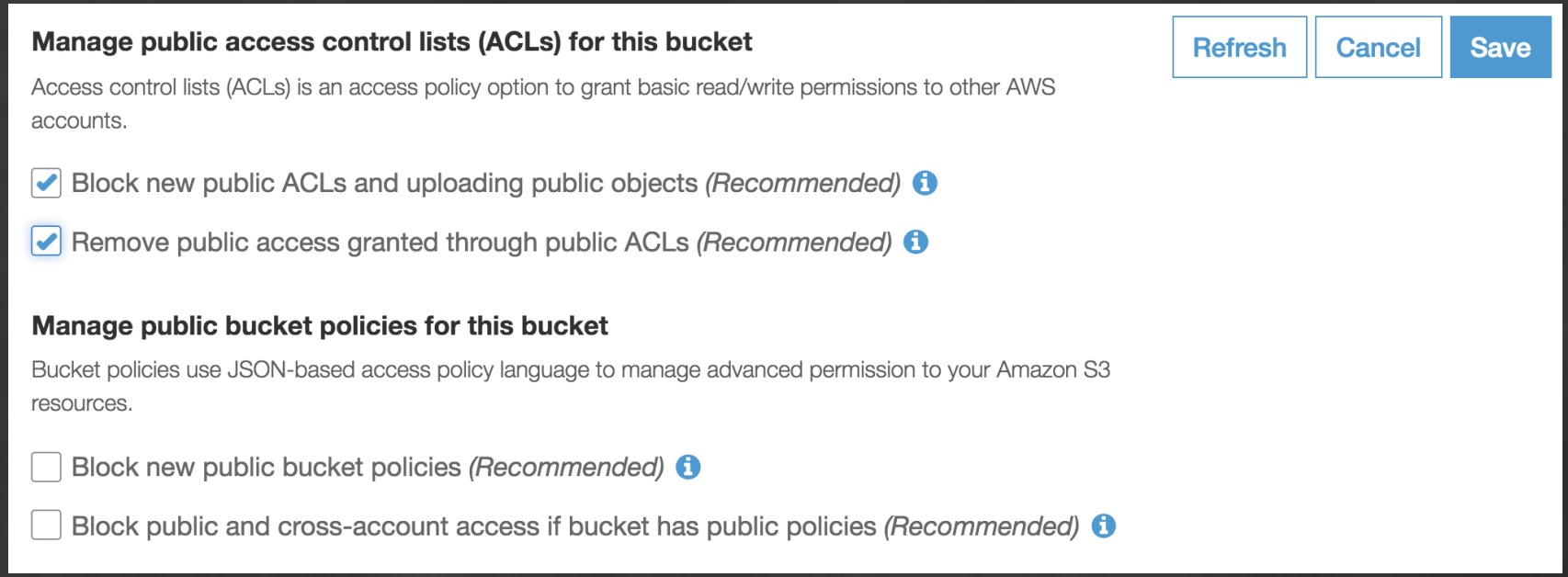
拒否ステートメント

```
{
  "Sid": ”DenyMost",
  "Effect": "Deny",
  "NotPrincipal": {
    "AWS": [
      "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity <OAI ID>"
    ]
  },
  "Action": "s3:GetObject",
  "Resource": "arn:aws:s3:::<BUCKET NAME>/*",
  "Condition": {
    "StringNotLike": {
      "aws:userId": ["<ADMINROLEID>:*"]
    }
  }
}
```

レビューとディスカッション

S3 バケットへのアクセス制限はどのように行いましたか?

公開アクセス設定



レビューとディスカッション

Hosted UI の URL に使用したレスポンスタイプは何ですか?

レビューとディスカッション

JWT トークンが格納されている場所はどこでしたか?

ありがとうございました