TechHarmony 勉強会 LT 仕様

AWS Amplify を 別のサービスで再現してみた

ソリューション事業グループ
クラウドサービス事業本部
サービス開発推進部
広野　祐司

2022年6月23日

って言うけど、何をしたの？

やったこと

AWS Amplify の機能を、AWS の別サービスを組み合わせて作ってみました。

AWS Amplify
サーバーレスアプリの
ビルド・デプロイ

- Amazon Route 53
  DNS管理
- AWS Certificate Manager
  SSL証明書管理
- Amazon EventBridge
  イベント管理
- AWS CodePipeline
  CI/CDパイプライン管理
- AWS CodeBuild
  アプリケーションコードのビルド
- AWS Lambda
  AWS リソースをコードで実行
- Amazon S3
  アプリケーションホスティング・CI/CDアーティファクト用一時ストレージ
- Amazon CloudFront
  コンテンツ配信・キャッシング（CDN）
- AWS CloudFormation
  リソースプロビジョニング

全9種類

なんでわざわざそんなことを？

当社ワクチン予約システム開発時の課題がずっと気になっていたからです。

樋口さんのプレゼンを拝借

技術面で難しかった部分②

技術面で苦労した部分

プロジェクト的な反省点

IPアクセス制限

- 管理者画面へのアクセスは、会社のIPアドレスからのみに制限するという要件。
- 調べたものの、現実的な解決策が無く、実装できず。
  - Amplify は、全世界にオープン or ベーシック認証 しかない模様
  - 業務アプリに Amplify は厳しい？
- 【補足】hosting + Cloudfront でIP制限自体はできる
  - 今回は、「管理者画面へのアクセスのみIP制限（≒一般画面には制限無し）」という要件だったので、この方法は使えなかった。

ワクチン予約システム開発当時、樋口さん、広野、AWSさんですぐに解決できませんでした。

aws

いい方法が見つからない！

これを解決しておきたかったのが理由です。

そもそも AWS Amplify って

なので、AWS Amplify でできないことをしようと思ったら
独自に機能を作りこむ必要がありました。

実際にやってみたこと

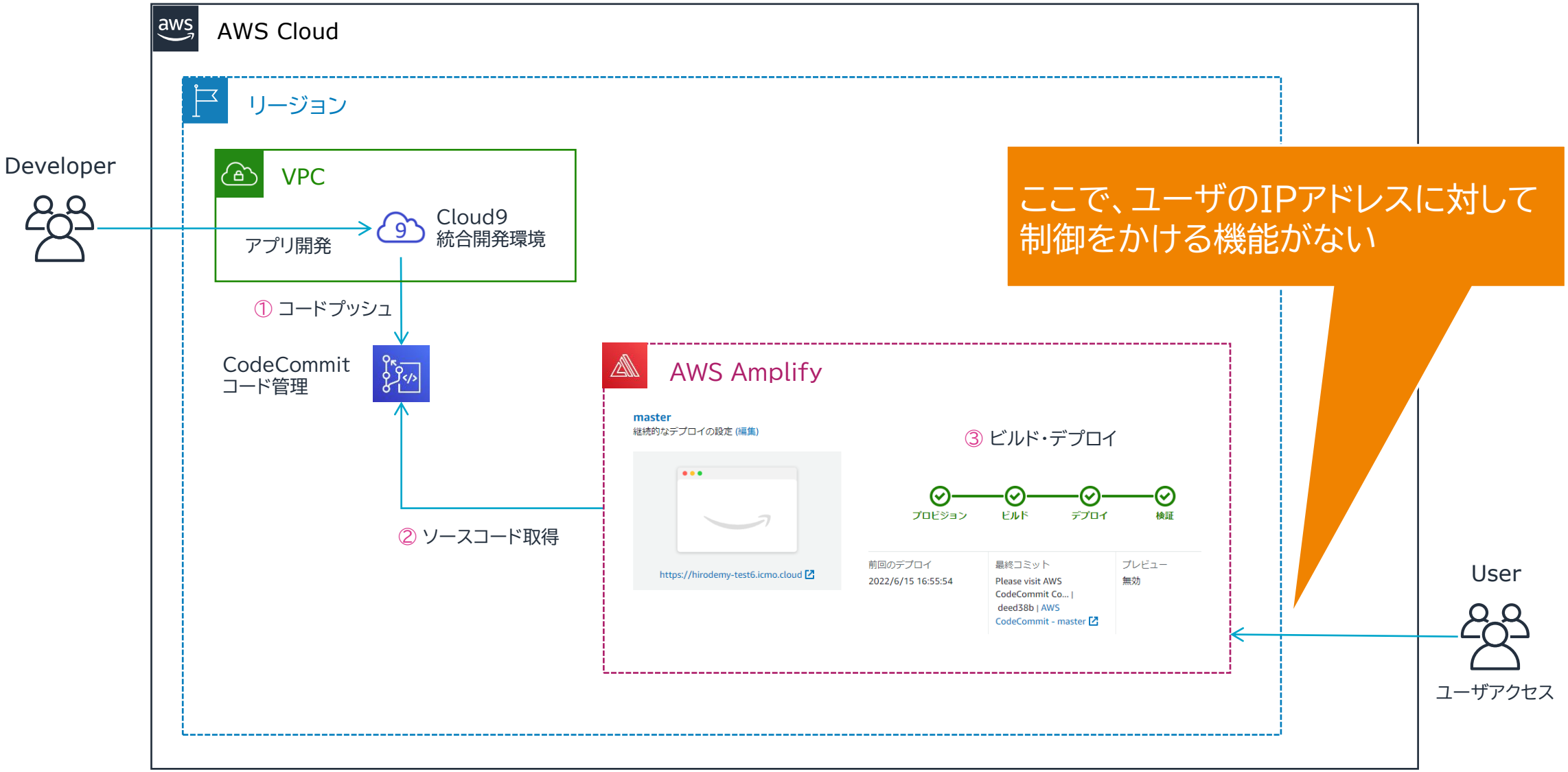
IPアドレス制限の実装方法を2パターン考えました

1. アプリ全体にIPアドレス制限をかける

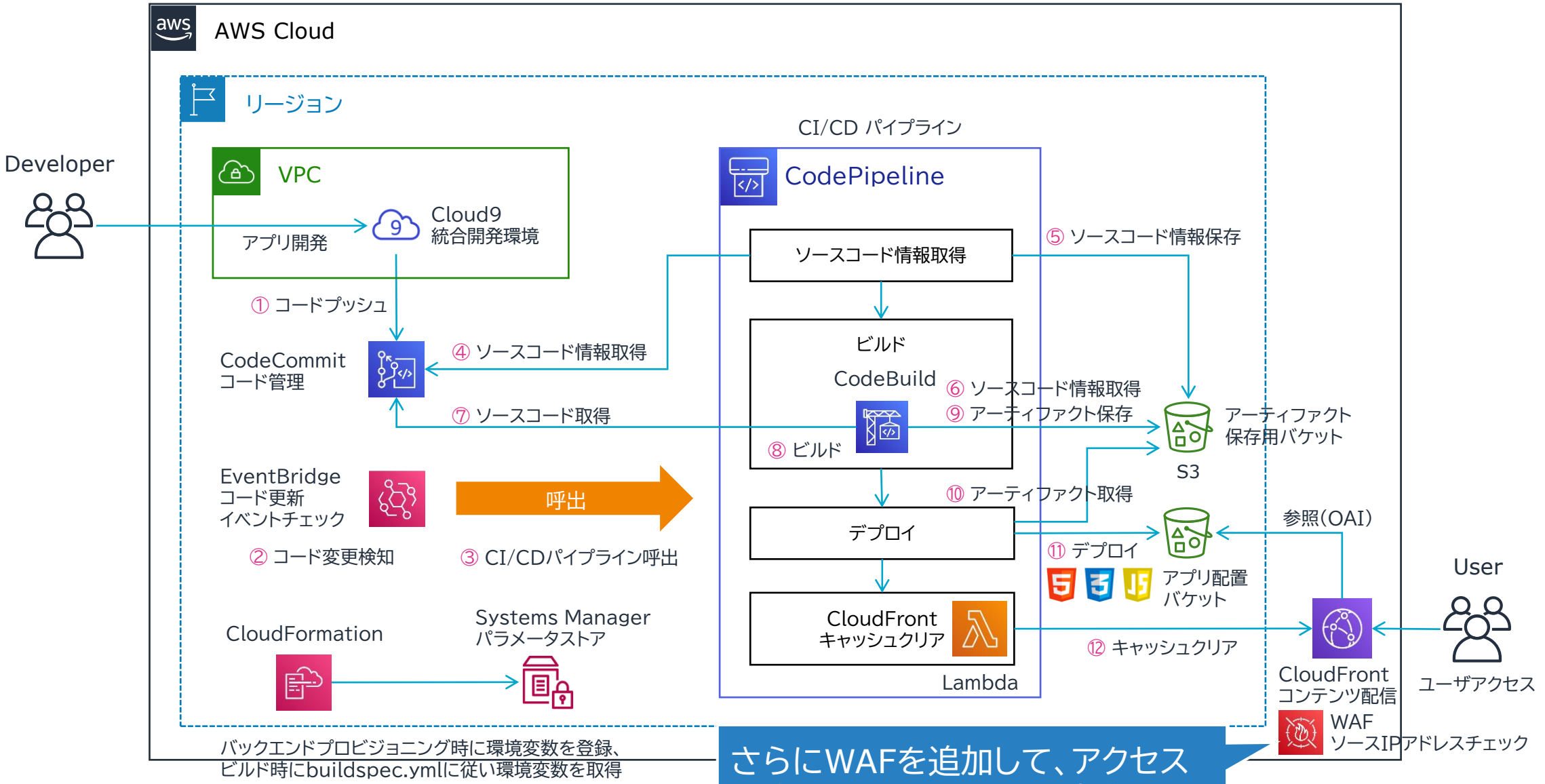
2. アプリ内、特定のページだけIPアドレス制限をかける

1. アプリ全体にIPアドレス制限をかける

AWS Amplify だと

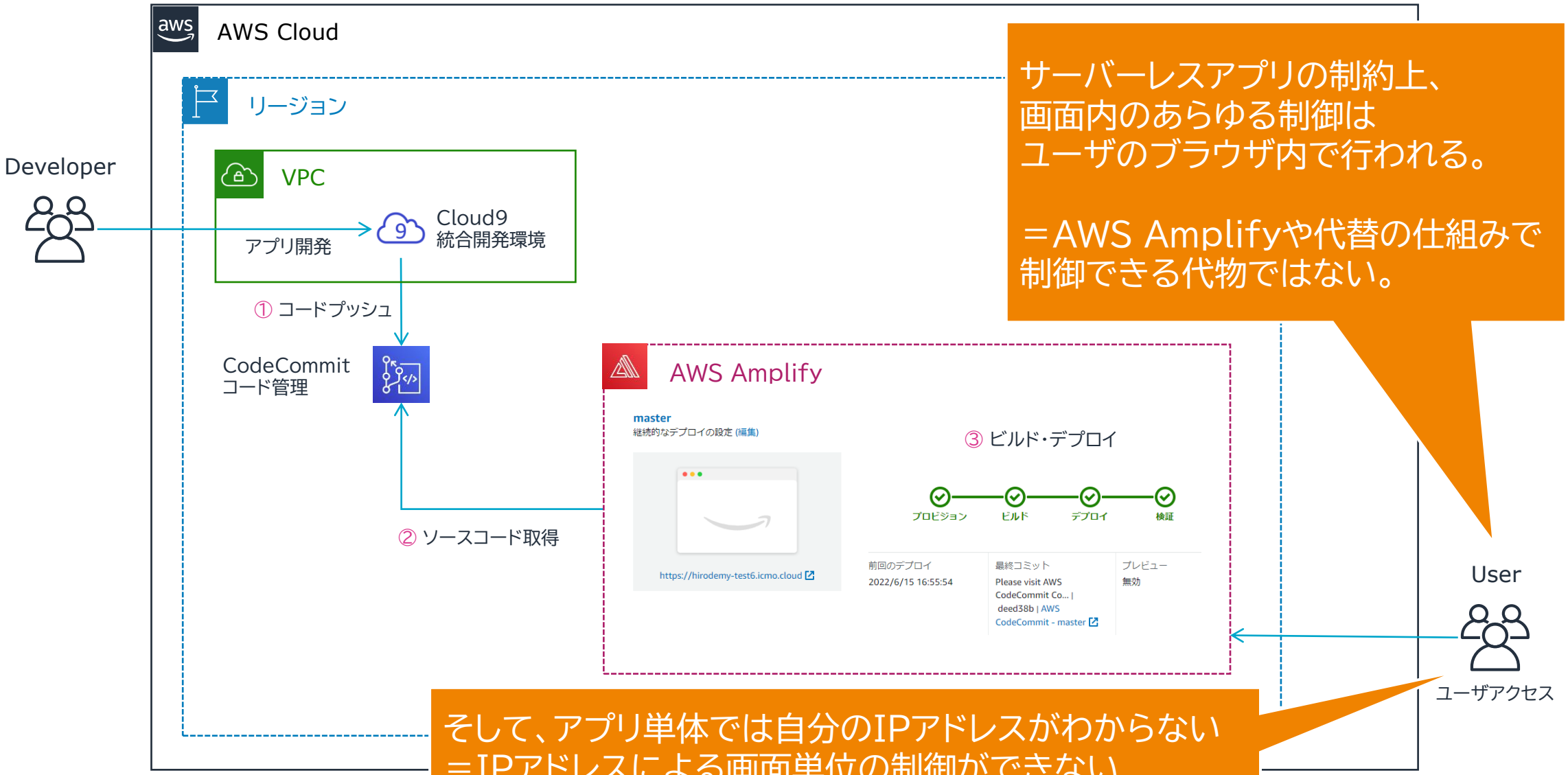


AWS Amplify を使わずに同等の仕組みを作ってみた



2. アプリ内、特定のページだけ IPアドレス制限をかける

AWS Amplify だと



サーバーレスアプリの制約上、
画面内のあらゆる制御は
ユーザのブラウザ内で行われる。

＝AWS Amplifyや代替の仕組みで
制御できる代物ではない。

そして、アプリ単体では自分のIPアドレスがわからない
＝IPアドレスによる画面単位の制御ができない
という課題がある

自分のIPアドレスさえわかればアプリ内で制御を入れられる

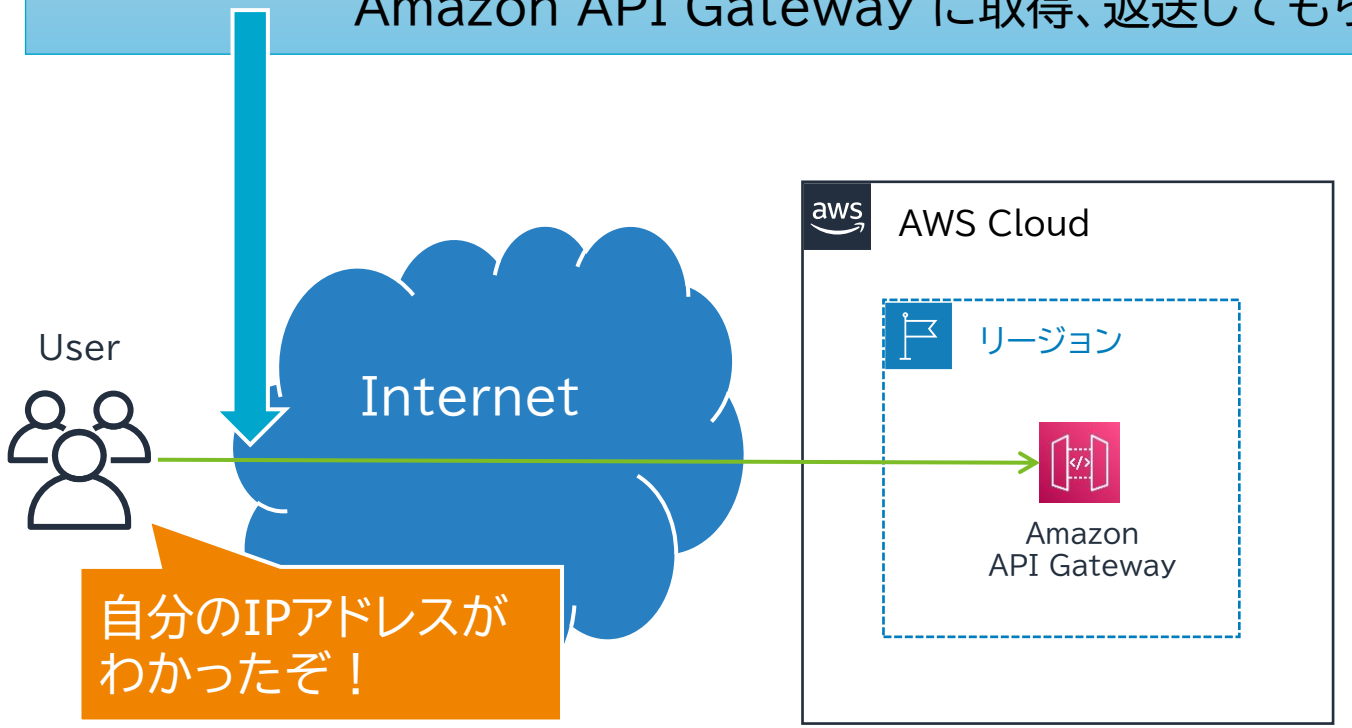
例えば、管理者画面 (Admin) のボタンを表示させる／させない を制御する

例えば、ソースコード内で 管理者画面を構成するパスを 有効にする／しない を制御する

```
{/* 設定 */}
<Route path="/config" element={<C                ername={user.attributes.email} groups={user.
{/* お知らせ */}
<Route path="/news" element={<N                  sername={user.attributes.email} groups={user.sign
{/* Hirodemyについて */}
<Route path="/hirodemy" elem                     {<Hirodemy username={user.attributes.email} groups={u
{/* 秘伝の書 */}
<Route path="/secrets" ele                       ent={<Secrets username={user.attributes.email} groups={use
{/* Adminメニュー */}
<Route path="/admin" element={<Admin username={user.attributes.email} groups={user.si
{/* Admin ユーザ作成 */}
<Route path="/usercreate" element={<UserCreate username={user.attributes.email} group
{/* Admin ユーザインポート */}
<Route path="/userimport" element={<UserImport username={user.attributes.email} group
{/* Admin ユーザ一括削除 */}
<Route path="/userdelete" element={<UserDelete username={user.attributes.email} group
{/* Admin ユーザリスト */}
<Route path="/userlist" element={<UserList username={user.attributes.email} groups={u
{/* 開発中 - ランキングテスト */}
```


ということで、自分のIPアドレスを取得する仕組みを作ってみた

ここに存在する、ユーザのソースIPアドレス（グローバルIPアドレス・IPv4）を
Amazon API Gateway に取得、返送してもらう



Amazon API Gateway には MOCK モードがあり、API Gateway 内で処理を折り返すことができる。
アクセスログ取得用途でユーザのIPアドレスを取得する機能があるので、それを利用する。

めでたし、めでたし。

樋口さーん、あのときできなかったこと、できるようになったよ～！

紹介した機能の実装方法は TechHarmony ブログで紹介しています

1.アプリ全体にIPアドレス制限をかける

https://blog.usize-tech.com/build-cicd-env-as-amplify-console/

2.アプリ内、特定のページだけIPアドレス制限をかける

https://blog.usize-tech.com/get-ipaddress-by-api-gateway/

駆け足でしたが、
ご清聴ありがとうございました。

Appendix

広野　祐司（ひろの　ゆうじ）

ソリューション事業グループ　クラウドサービス事業本部
サービス開発推進部　サービス開発課

略歴

- netXDC 監視･運用サービス運営
- 海外グローバル運用サービスの国内展開
- 2019年度より社内クラウド人材育成を推進
  教育進捗管理ツール や e-Learningツール を開発･提供中
  2020, 2021 APN AWS Top Engineers 受賞
  2022 AWS Partner Ambassador 受賞

aws partner network ambassador

ひろのくん　Hirodemy

