re:Invent Re;Cap AWS Verified Accessにちょっぴりdd

Yuki Yoshida

Solutions Architect ISV/SaaS

自己紹介

- 名前　吉田 裕貴 (Yuki Yoshida)
- 役割　ISV/SaaS ソリューションアーキテクト
- 好きなAWSサービス Amazon GuardDuty
- 趣味　筋トレ・バイク

本日話す内容と注意事項

- 時間が限られた中で最大限デモをお見せしたいので、サービスの細かい話については割愛します。
- 概要と何ができるかに焦点を当ててお話します。
- 東京リージョンではまだ使えません（2022/12/22 現在）
- プレビューなのでまだ本番環境で使わないようにしましょう

Q:皆さんに質問です

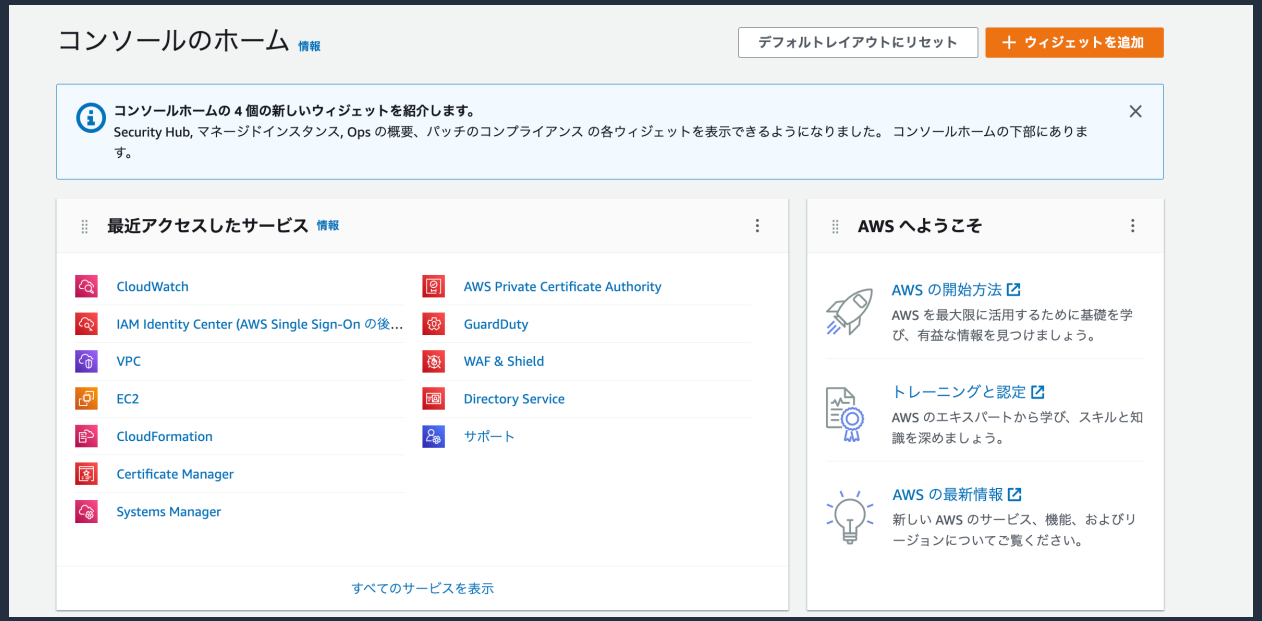
VPNはお好きですか？

なんのためにVPNを使うか（一例）

- 拠点間で安全に社内システムにアクセスするために使用します
- インターネット回線は危険だからVPNを使うように言われた
- VPN使わないとつながらないから
- お仕事をするために
- 社内のみの情報だから

通信の安全性の確保
アクセス制御

マネジメントコンソール



- インターネット越しにアクセス
- 通信は暗号化されている
- IAMによってすべての通信が確認される

AWS Verified Access

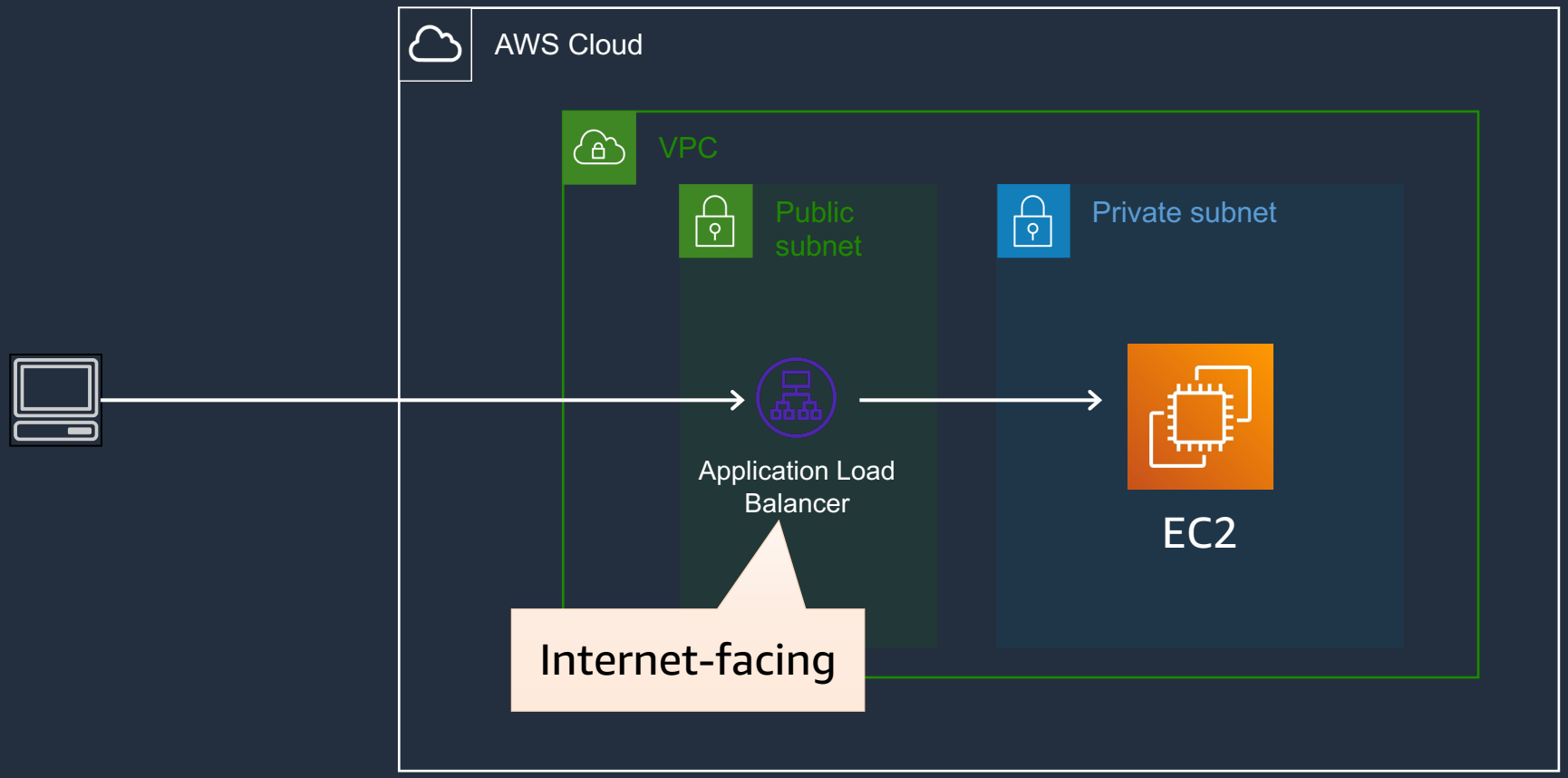
仕組み

AWS ゼロトラストの基本原則に基づいて構築された AWS Verified Access は、アクセス権を付与する前に、すべてのアプリケーションリクエストを検証します。Verified Access により VPN が不要になるため、エンドユーザーのためのリモート接続エクスペリエンスが簡素化され、IT 管理者のために管理の複雑さが軽減されます。

社内・社外のネットワークと言う単位でアクセスががあれば信頼する・しないとするのではなく、
（社内であっても）あらゆる入力は潜在的に悪意あるものとして信頼しない（検証する）。

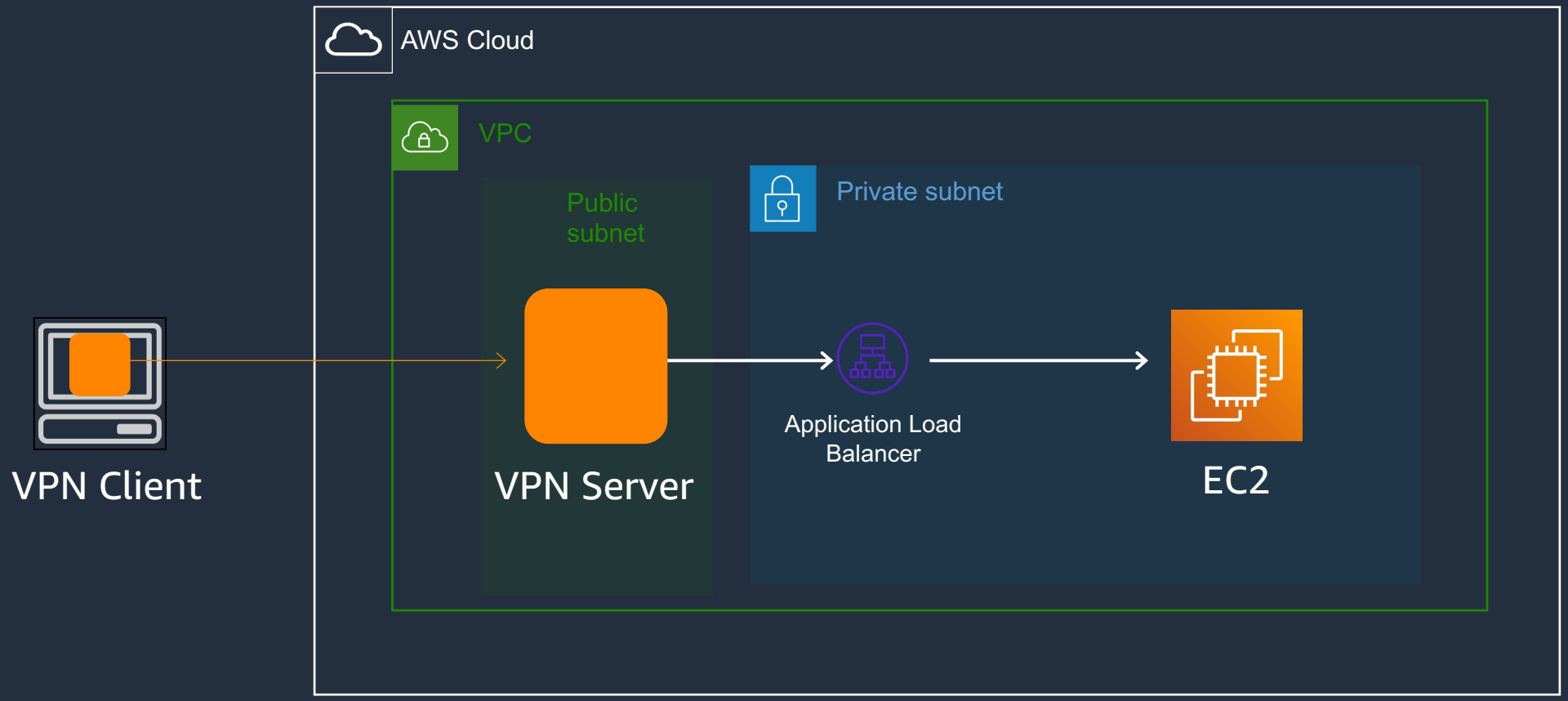
VPNを使わないアクセス

公開サーバー



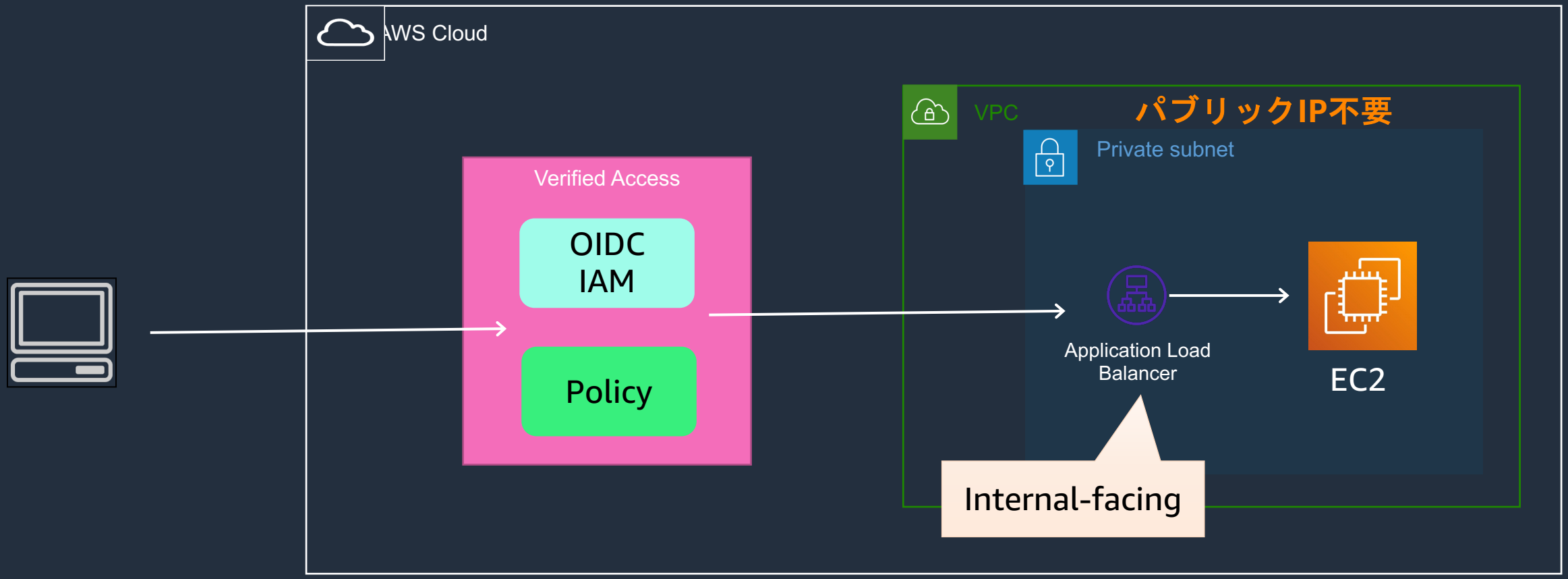
EC2にアクセスはできるがアクセス元の検証などはしていない

VPNの利用



VPNを張る際に認証されたユーザーのみに公開ができる

AWS Verified Access



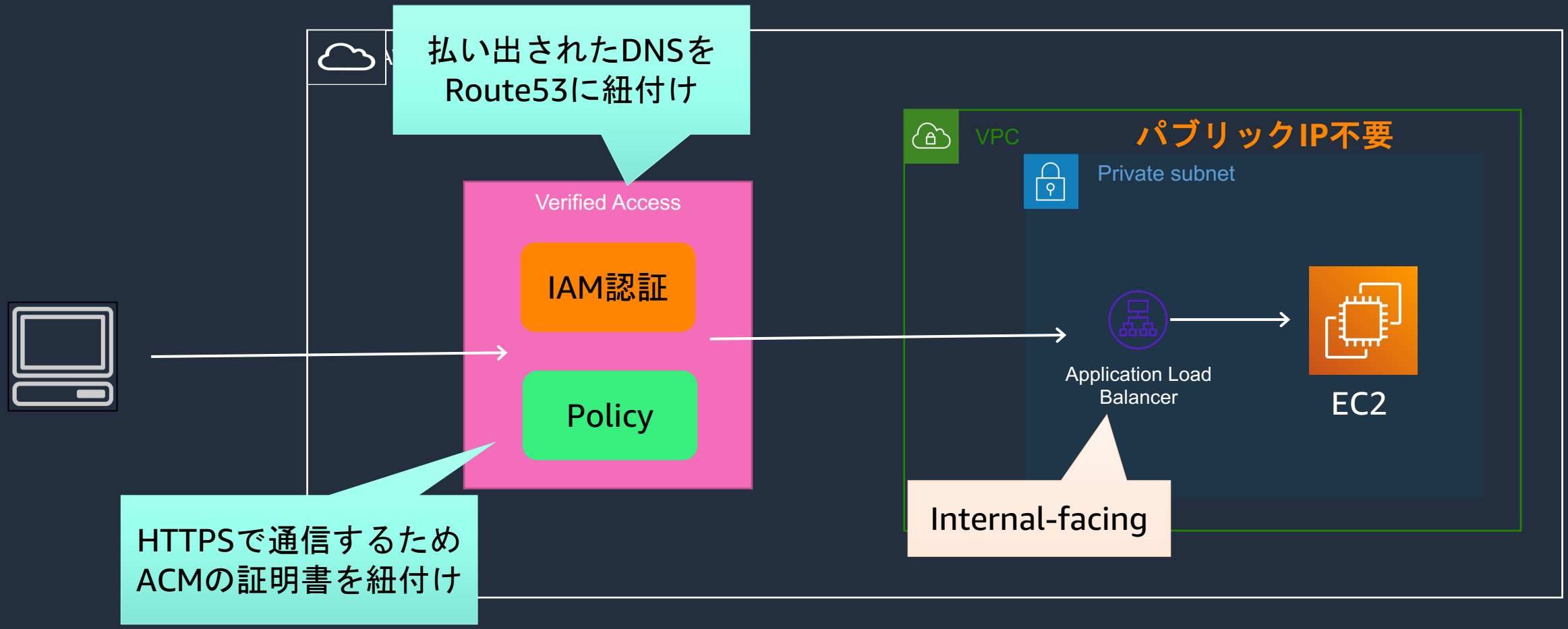
Verified Access にアクセスすればInternal-facingのALBなどにつないでくれる

構築のデモ

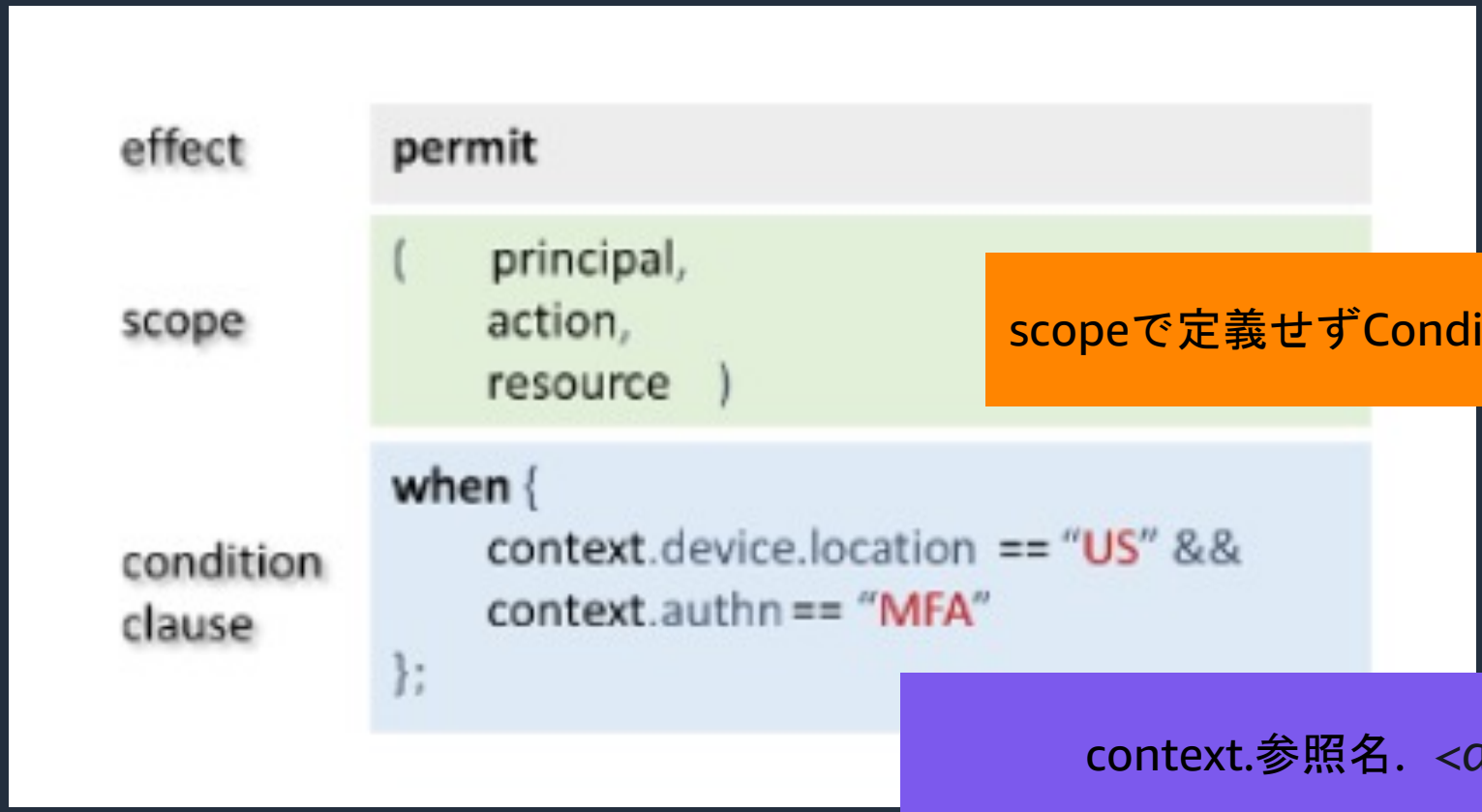
今回のデモ環境の前提条件

- us-east-1：バージニアで実施
- IAM Identity Center (AWS Single Sign-On)をバージニアで構築
- AWS Verified Access プレビュー – 企業アプリケーションへの VPN レスの安全なネットワークアクセス の設定をなぞります。参考にしてやってみましょう！

AWS Verified Access：デモ環境



ポリシー（cedar）



scopeで定義せずCondition clauseを使用する

context.参照名.<attribute>

JSONフォーマット

```
{
  "title": "AWS IAM Identity Center context specification",
  "type": "object",
  "properties": {
    "user": {
      "type": "object",
      "properties": {
        "user_id": {
          "type": "string",
          "description": "a unique user id generated by AWS IdC"
        },
        "user_name": {
          "type": "string",
          "description": "username provided in the directory"
        },
        "email": {
          "type": "object",
          "properties": {
            "address": {
              "type": "email",
              "description": "email address associated with the user"
            },
            "verified": {
              "type": "boolean",
              "description": "whether the email address has been verified by AWS IdC"
            }
          }
        }
      }
    },
    "groups": {
      "type": "object",
      "description": "A list of groups the user is a member of",
      "patternProperties": {
        "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{12}$": {
          "type": "object",
          "description": "The Group ID of the group",
          "properties": {
            "group_id": {
              "type": "string",
              "pattern": "^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}$",
              "description": "The Group ID of the group"
            },
            "group_name": {
              "type": "string",
              "description": "The customer-provided name of the group"
            }
          }
        }
      }
    }
  }
}
```

ドキュメントにJSONフォーマットが記載されているのでこれを元に<attribute>の部分を書いていく。

■AWS IAM Identity Center
https://docs.aws.amazon.com/verified-access/latest/ug/trust-data-iam.html

Thank you!