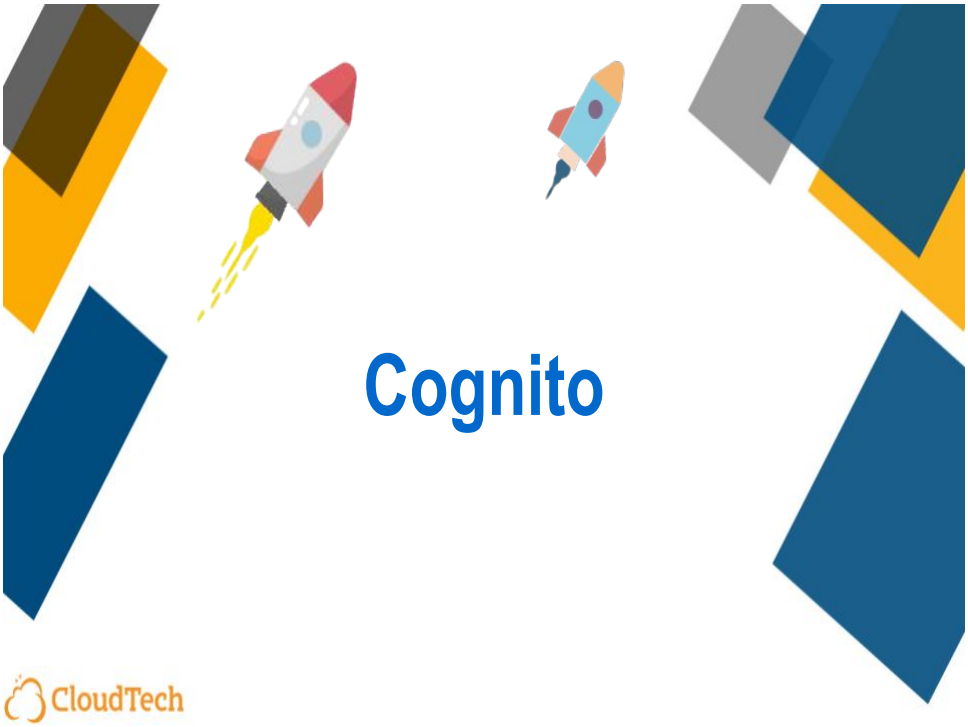
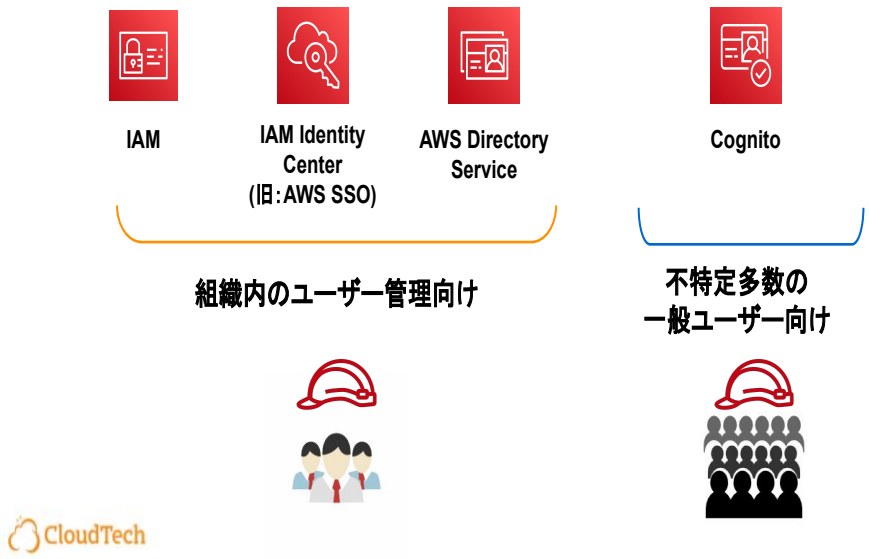


- Cognitoとは、Webアプリケーションやモバイルアプリケーションに対して、ユーザーの登録やログインのための認証機能を提供するマネージドサービスです

AWSの認証・認可系サービス

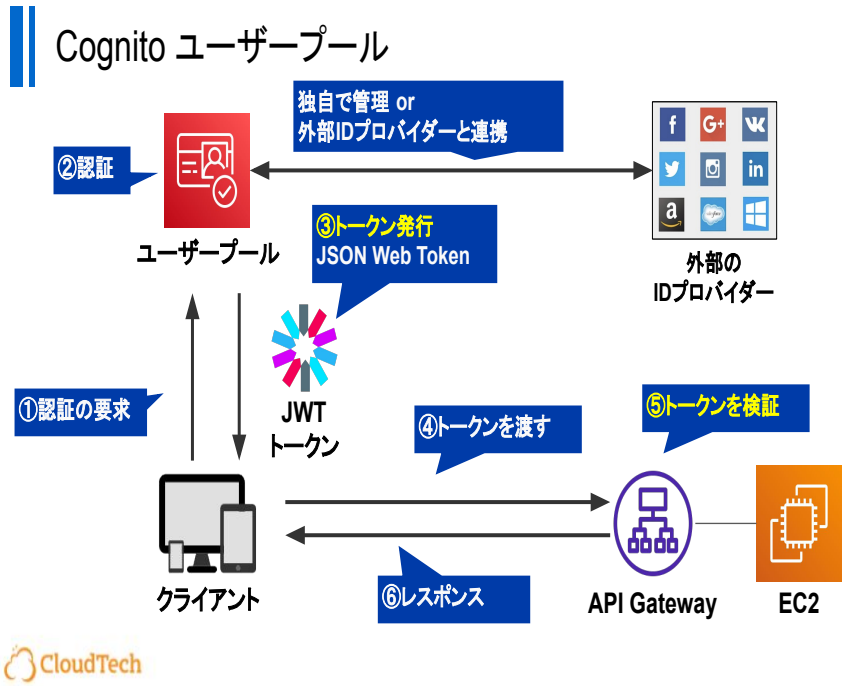


- おさらいですが、認証・認可を行うサービスはいくつかあります。
  - IAM
  - IAM IC
  - DS
    - これらは組織内の、いわば既に知っている人に対して権限を付与するものでした
    - 目的は、組織のユーザーにAWSサービスへアクセスする権限を付与することです。
  - 一方のCognitoは
    - 不特定多数のユーザーに向けて権限を付与するものです。
      - 権限を付与する、つまり
        - 操作権限を与える、AWSで言うと、これはIAMロールを適切に付与するのと同じ意味ですよね。
    - CognitoはユーザーにIAMアクセスキーとシー

- クレットを発行し、特定の AWSリソースにアクセス権限を持つロール/ポリシーを割り当てることができます。
- 作成できるユーザーの上限数についてもデフォルトで「20,000,000」(二千万) と、不特定多数のユーザーを意識した仕様となっています。
    - ユーザープールとIDプールの違いについての理解が重要です。

Cognito
ユーザープール

CloudTech



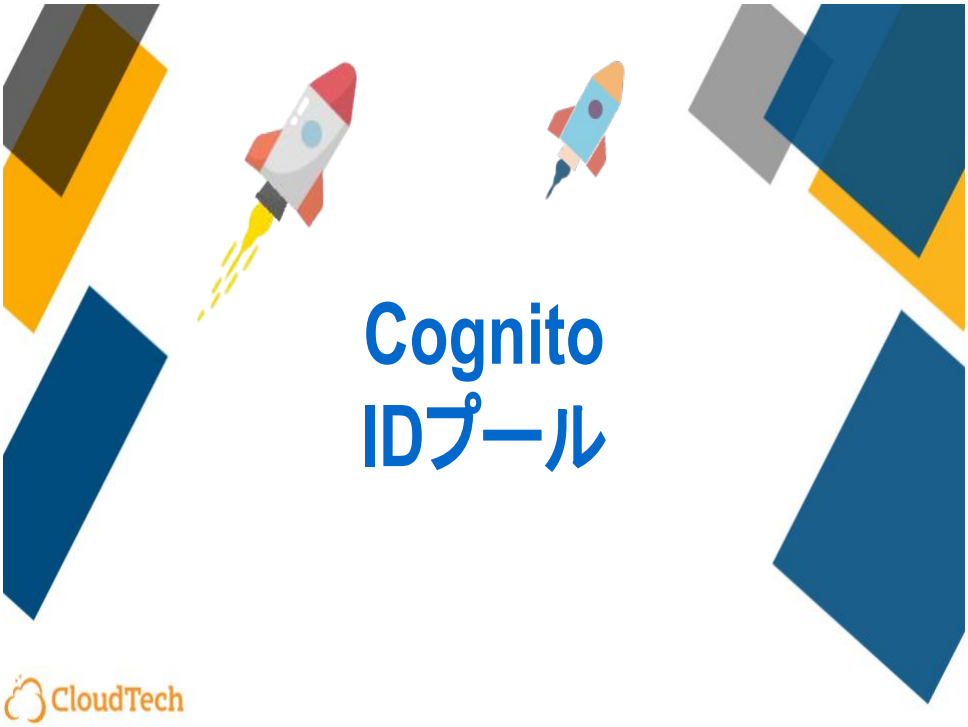
- ユーザープールは ユーザー認証 と ユーザー管理 を行うコンポーネントです。
    - なお、プールとは、貯めておく場所、のようなニュアンスがあり、ユーザー情報を一元管理するようなイメージですね。
  - クライアントがあります。（これは、利用者のブラウザ、Webアプリケーションやモバイルのアプリケーションが想定されます）
  - そして、接続するAWSサービス、例えばALBの配下に限定コンテンツがあるとします。
    - 認証を通過したユーザーのみ、ALB配下のEC2上のコンテンツにアクセスできるようになります。
      - 他にもAPI GatewayやAppSyncとも連携できますが、
        - 大切なのは、不特定多数のクライアントへ、AWSサービスの認証を

        - どうやって実現するかです。
- ここで、Cognitoのユーザープールを使用できます。
    - ユーザープールがユーザーを認証する方式としては、2通りあります。
        - Cognitoユーザープールが提供するスタンドアローンの認証機能
            - マネージド型のユーザーディレクトリを作成し、管理者が独自でユーザーを管理する方法
        - 外部IDプロバイダーと連係した認証
            - OpenIDConnect、OAuth2.0、SAML 2.0などの一般的なID管理規格をサポートしているので、これらに対応した認証サービスとの連係が可能です。
            - Cognitoは3rdPartyのソーシャルなIDプロバイダー、google, facebook, twitter, amazon

- などのアカウントと連携できる認証・認可の機能を持っており、
  - これらで連携したIDプロバイダーを介して、利用者自身でユーザー登録、ユーザー認証を行うことが可能になります。
  - 外部IDプロバイダーと連係した認証では、ユーザープールに対する明示的なユーザー登録は行わず、初めて認証

        - が行われた時にユーザーが登録されます。
    - クライアントはユーザープールに対して認証を要求し、
    - 認証に成功すると、Amazon Cognitoのユーザープールはクライアントに認証トークンを返します
        - トークンはJWT JSON Web Tokenと呼ばれる形式が使用可能です。
            - 名前やメールなど、認証されたユーザーのIDに関する情報が含まれています。
            - トークンはその後、認証するAWSサービスに渡されて、適切であればしかるべきレスポンスなどを受け取れます（要はアクセスできます）。
    - ちょうど、Cognitoが認証情報を

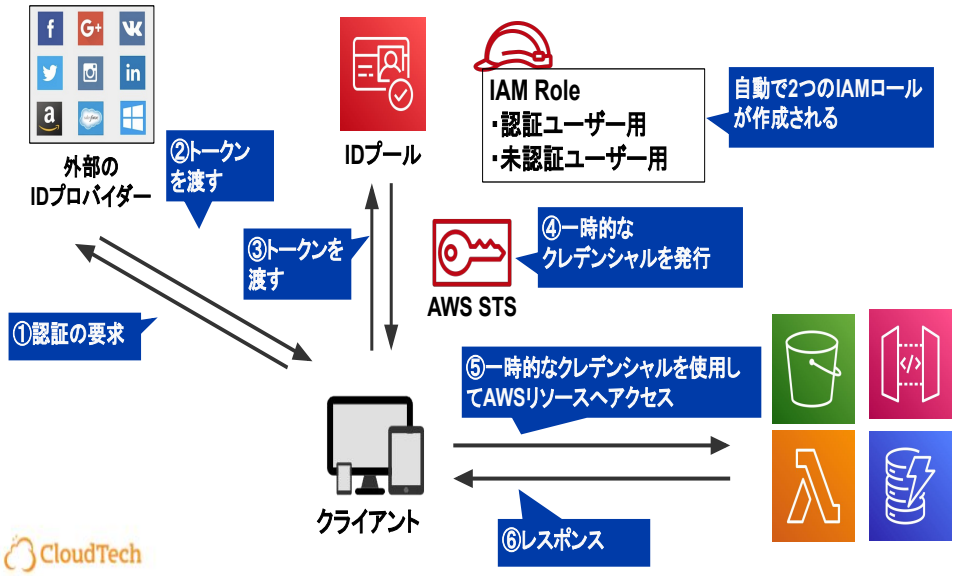
- IdPからAWSにわたす仲介役のような形ですね。



Cognito
IDプール

CloudTech

Cognito ID（アイデンティティ）プール

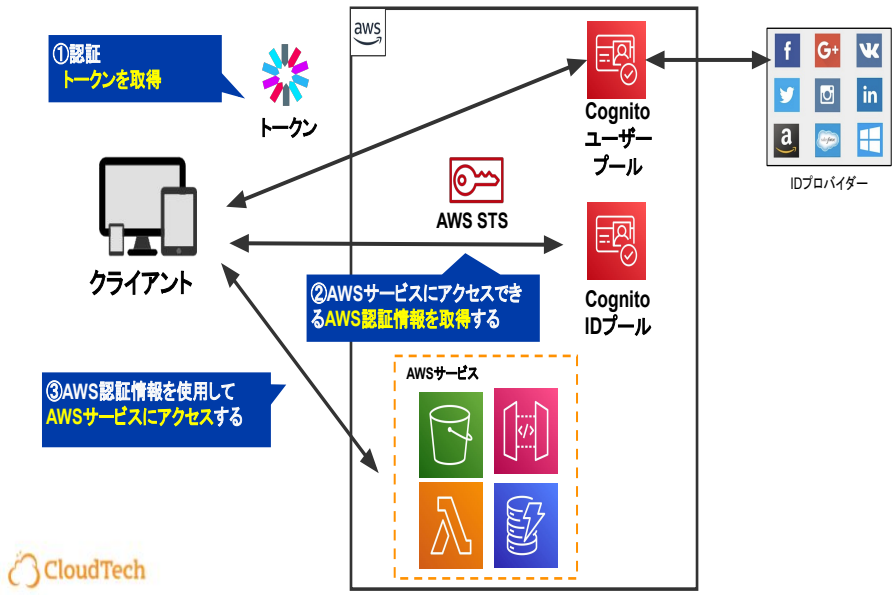


- Cognito IDプールとは、クライアントに対し、IAMロールによるAWSへの一時的なアクセス権限を付与するために使用されます。
  - クライアントはAWSサービス（例えばAmazon S3やDynamoDBなど）のアクセス件を取得するために、先ほどと同様に認証が必要です。
    - ここで、外部のIDプロバイダーに対して認証を認証したとしましょう。
      - ここに、Cognitoユーザープールを使用できますが、これは後ほど解説します。
      - クライアントはIDプロバイダーに認証を要求し、認証が通ったのでトークンを受け取ります。
        - このトークンをCognitoのIDプールに私ます。
        - IDプールにて、ユーザーの

- 認証が成功すると、ID poolは STS assume roleの仕組みを利用してクレデンシャルを発行します。
    - あらかじめユーザープールのグループにマッピングされた設定をもとに、ロールが決定されます。
        - ID Poolを作成すると、自動的に2つのIAMロール（認証ユーザー用と未認証ユーザー用）が作成されます。
        - このように、「認証されていないゲストユーザーに対して、一定のアクセス権限を与える用のIAMロール」を定義することもできます。
- IAMロールには、IAMポリシーを紐づけて使用するものでしたね。
    - なので、それぞれのロールに対して、適切なポリシーをアタッチ

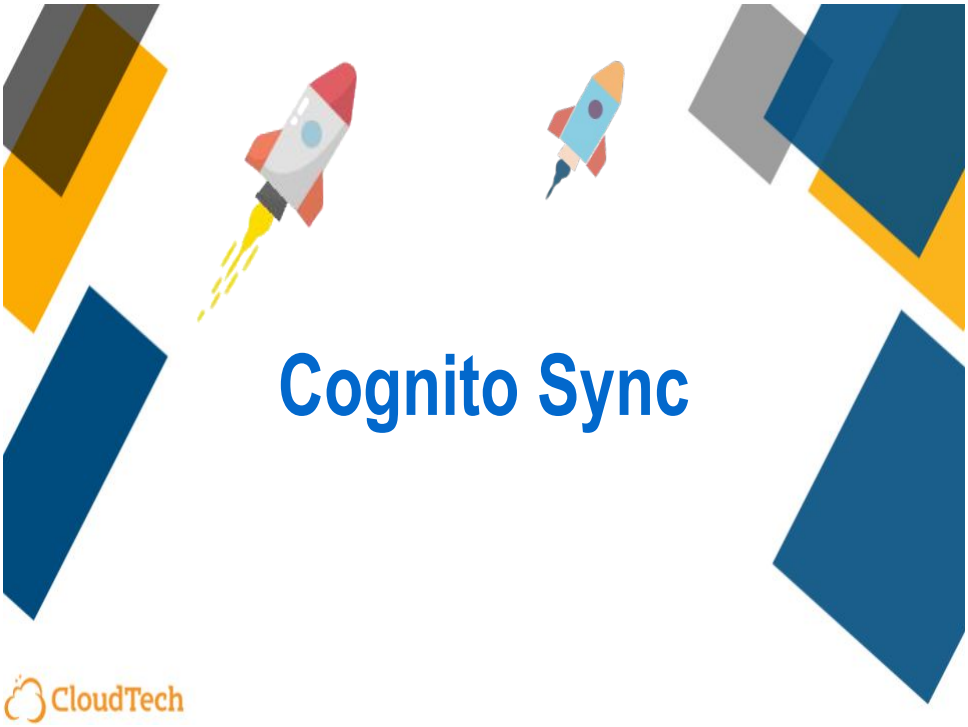
        - します。
        - 例えば、DynamoDBのテーブルの読み込みは未認証ユーザーを含む全てのユーザーに許可、
        - 書き込みは認証ユーザーのみに許可するといったような形です。
    - このように、認証されたクライアントはAWSの一時的なクレデンシャルを取得するので、
    - これを使ってAWSリソースへアクセスすることができるようになります。
- では、認証の要求を、Cognitoユーザープールを使用した組み合わせをみていきましょう。

Cognito（ユーザープールとIDプールの組み合わせ）



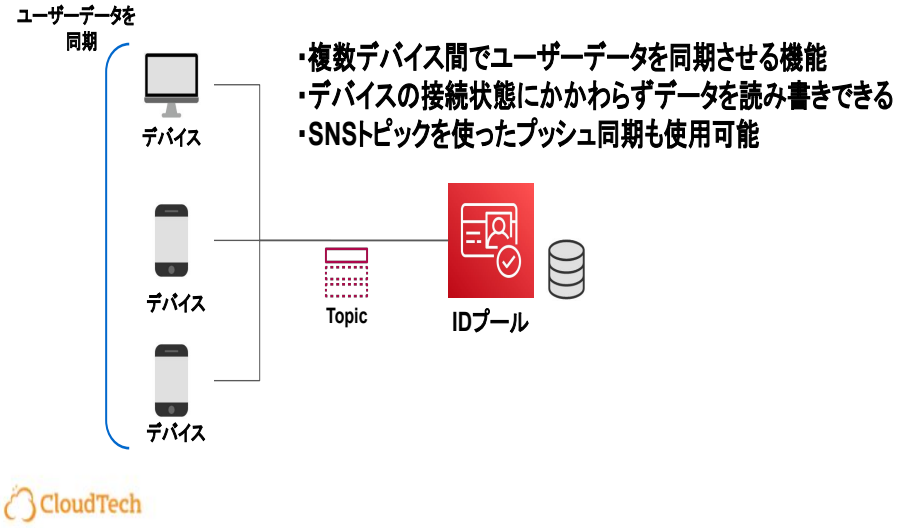
- ユーザープールとIDプールを使用した組み合わせです。
  - ユーザープールとIDプールをそれぞれ作成して、
    - クライアントの認証は、「Cognitoユーザープールが提供する認証機能（ユーザー名/パスワードによる認証）」でも構いませんし、
      - 「外部IDプロバイダーと連係した認証」でも構いません。
      - 両方を有効にすることもできます。
  - IDプールのIDプロバイダーとしてユーザープールを指定します。
    - 取得したIDトークンをIDプールに渡して、IDトークンの正当性が確認されると、定義されたIAMロールに割り当てられたAWS一時クレデンシャルが発行されます。
  - クライアントは一時的なクレデンシャルを使うことにより、IAMロールの設定に応じたAWSリソースに対してアクセスすることができます。

- まとめると、ユーザープールで認証、IDプールで認可を行い、不特定多数のクライアントに対して AWSサービスのアクセスを管理する、Cognitoはこのような一連の動きをまとめるサービスです。


Cognito Sync
CloudTech

•

Cognito Sync *現在はAppSyncの使用が推奨される



Amazon Cognito Syncは、ユーザーデータを複数デバイス間で同期させる機能です。
※現在はデバイス間のアプリケーションデータを同期するためのサービスとしてAWS AppSyncの利用が推奨されています。

独自のバックエンドを必要とせず、クライアントはデータをローカルにキャッシュするため、アプリケーションはデバイスの接続状態に関わらずにデータを読み書きすることが可能です。
そして、デバイスがオンラインになったときにデータの同期を行います。
SNSトピックを使ったプッシュ同期を設定している場合は、他のデバイスにアップデートがあることを通知することも可能です。