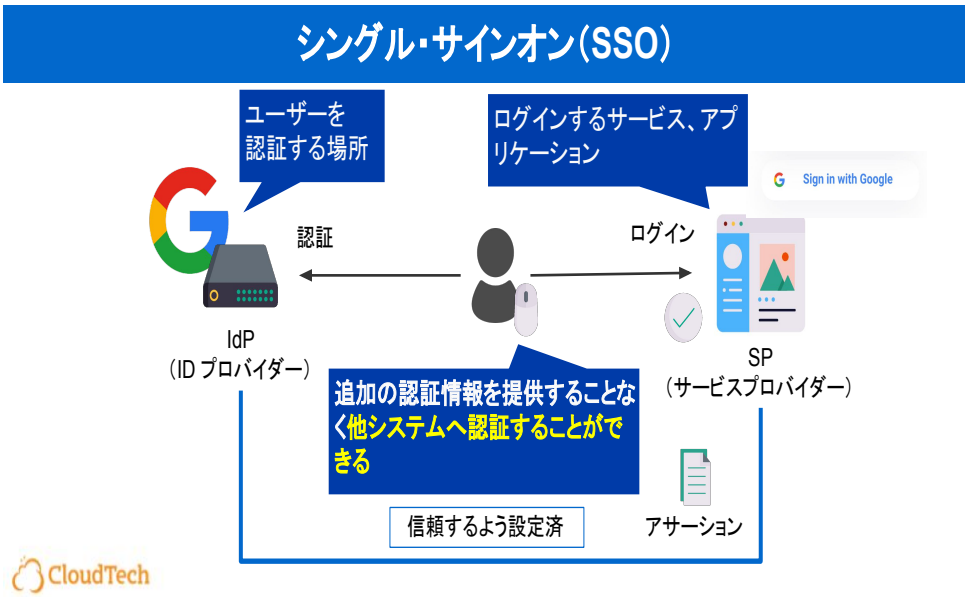
- IAM Identity Centerは、旧AWS SSOと呼ばれていた、シングルサインオンサービスです。

IDフェデレーションとは？



- まず前提知識、IDフェデレーションについて説明します。
- IDフェデレーションとは、アクセス制御の一般的なアプローチです。
    - IdPでユーザーを一元管理し、SPとしてアプリケーションやサービスへのアクセスを制御します。
        - 2つ用語が出てきました。
    - まず、IDP(IDプロバイダー)ですが、
        - これはユーザーを認証する、中心となる場所のことです。
    - そして、SP(サービスプロバイダー)
        - これは、ログインするサービスやアプリケーションなどのことを指します。
            - SPはIdPをあらかじめ信頼するよう設定しておきます。
            - IdPが提供するユーザーの認証情報(アサーション)に基づいてサービスへのア

- クセスを制御します。

- 例えば、あるWebサイトが、Googleアカウントでのログインと、独自のユーザー登録でのログインが実装されている場合
  - IDPはGoogle、SPはサイト
    - このサイトでユーザー登録することも可能ですが、
    - このサイトは、あらかじめ Google IdPを信頼しておくことで、ユーザーがサイト上で Googleを選択した登録やログインを選択したら、
    - Google側で認証情報を使ってユーザーを認証し、ユーザーはその認証に基づいて Webサイトのアカウント作成やログインをすることができます。
- ID情報を連携（フェデレーション）する仕組みとなりますが、一回認証すれば、さまざまなサービスにログインできることから、シングル・サインオンとも呼ばれます。
  - あるシステムにサインインすると、追加の認証情報を提供することなく、他のシステムへ認証することができる方法です。

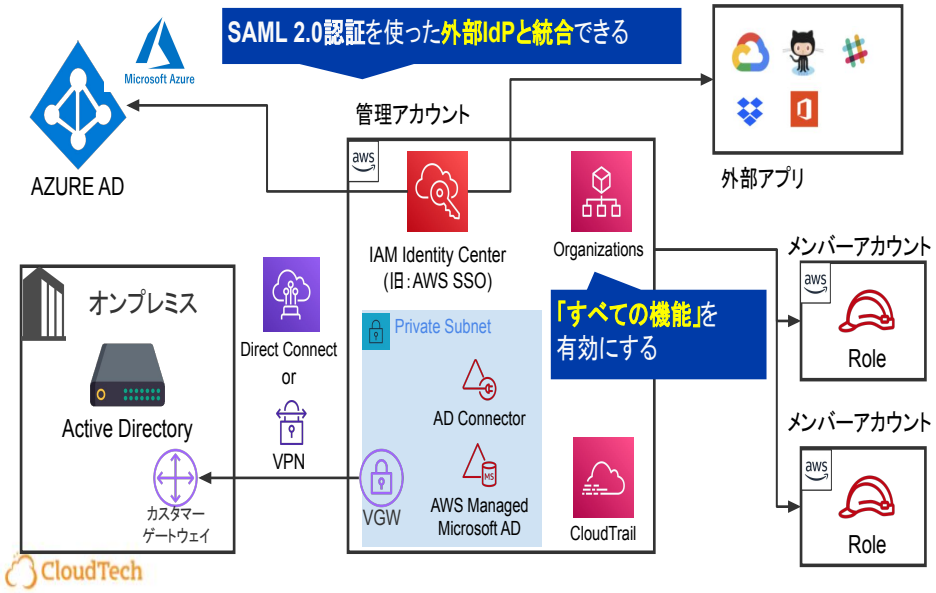
IAM Identity Center（管理ポータル）

IAM Identity Centerは、無料で使うことができます。

- 使い方の一例です。
  - IAM Identity Centerが有効化されるとユーザーポータルのURL が自動生成されます。
    - 生成したURLを開き、一元管理されたユーザー名/パスワードでログインすると、、
      - そのユーザーの持っている権限に応じて
        - アクセスできるすべてのAWSアカウント、
        - 引き受けることのできるIAMロール
        - 管理コンソールへのリンク
        - または、AWS CLIアクセス用に一時的な認証情報など、

        - が一覧で表示されます。
            - この例では、アカウントのAdministorator権限のロールでそれぞれログインできる設定となっています。
    - このように、ユーザーポータルにログインしさえすれば、自分が使用可能な権限が分かります。
        - 他、多要素認証（MFA）の入力を必須とすることもできます。
- さて、その一元管理されたユーザーについて、詳しくみていきましょう。

IAM Identity Center（基本概念）



- AWS SSOでは、ユーザー情報などを登録・参照するデータベースとして、
  - ネイティブに搭載されているデフォルトの IAM Identity Center内のユーザーストアで、手動で登録していくこともできますが、
    - SAML2.0認証を使ったさまざまなAWS外部のIdPと統合して連携できます。
      - 会社などでは既に、オンプレで構築したMicrosoftのActive Directory を使っているケースが多いかと思います。この AD との連携もできます。
        - プライベート接続を設定して連携しますが、これにはAWS Directory Serviceの機能である、AD Connectorや、Managed Microsoft ADを間にはさむ必要があります。

        - 他、AZUREのAZURE ADやOkta Universal Directoryなど外部サービスがサポートされています。

ADなどでIdPの認証を通過した後の動きです。

- AWS Organizations との統合機能について説明します。
    - AWS Organizations は複数のAWSアカウントを管理できるものとなります。
        - 詳細は別講座をご覧ください。
    - AWS ICとOrganizationsを連携して、先ほど見たように、他AWSアカウントへのログインができます。
        - なお、準備としては、Organizationsで「すべての機能」オプションを有効にする必要があります。
            - これにはOrganizationsの管理AWSアカウントを使用する必要があります。

- CloudTrailとも統合されているので、ユーザーのアクティビティを監査することができます。
- AWS Well-Architected フレームワークのセキュリティの柱、「アイデンティティ管理とアクセス管理」にもあるとおり、「一元化された ID プロバイダーを利用する」ベストプラクティスに準拠できます。
    - もちろん、ベストプラクティスは必ず守らなければならないものではありませんが、
    - ユーザー/パスワードの情報を1箇所で管理できるので、大規模な組織ほどシングルサインオンの仕組み導入は管理面で恩恵を受けることでしょう。

また、SAML が利用できるビジネスアプリケーションへの SSO アクセスを設定できます。

- 権限管理については色々と制御ができますが、試験レベ

- ルとしてはこのような概念の理解で十分です。

Amazon Web Services ブログ
AWS Single Sign-On 紹介
https://aws.amazon.com/jp/blogs/news/introducing-aws-single-sign-on/

G Suiteなど外部サービスをIdPにすることもできます。
G Suite アカウントを用いた AWS へのシングルサインオン
https://aws.amazon.com/jp/blogs/startup/techblog-saml-gsuite/