技術推進本部　テクノロジーイノベーション部

AWS + G Suite を使ったマルチクラウドなサーバレスアプリケーション開発

社内サービスを外部クラウド(AWS)上でサーバレスアプリケーションとして構築すると、新規サーバの調達・サーバ保守の負荷が軽減される反面、セキュリティ・運用コスト面においては課題が生じやすい。弊社では社内サービスの1つをAWSにリプレースするにあたり、社内グループウェアとして利用しているG Suiteを併用する事によりこれらの課題を解決した。

背景

社員の研修実績を登録・管理する「研修実績システム」(以下、本システム)が運用サーバ老朽化等の理由でリプレースする必要性が生じた。この際、新規サーバの調達・サーバ保守の負荷軽減のため、AWS上にサーバレスアプリケーションとしてリプレースした。

課題

本システムをAWS上にリプレースするにあたり、以下の点が課題となった。

- 社員以外がシステムを利用できてはならない
- 社員情報を社外の第三者に閲覧される危険性がある場所に置いてはならない
- 運用コストは最小限に抑える

本稿では、これらの課題に対する解決手法について述べる。

アプローチ方針

本システムでは、弊社でグループウェアとして利用しているG Suiteを併用し、マルチクラウドな構成にする事で先述の課題を解決する。

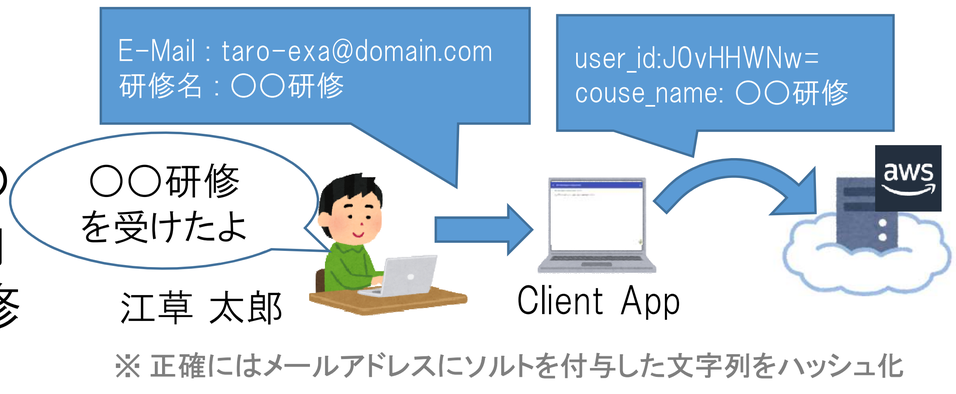
社員以外が本システムを利用できない様に、G SuiteへのOAuth2.0による認証を実装する。これにより、社内の認証基盤を外に持ち出すことなく認証機能が実現できる。また、システムで使用する社員の情報はAWSには置かず、G Suite上で管理する実装とした。G Suiteには社員しかアクセスできないようにセキュリティポリシーが設定されているため、新たにコストを発生させる事なくセキュリティを担保する事が可能となる。

G SuiteへのOAuth2.0による認証

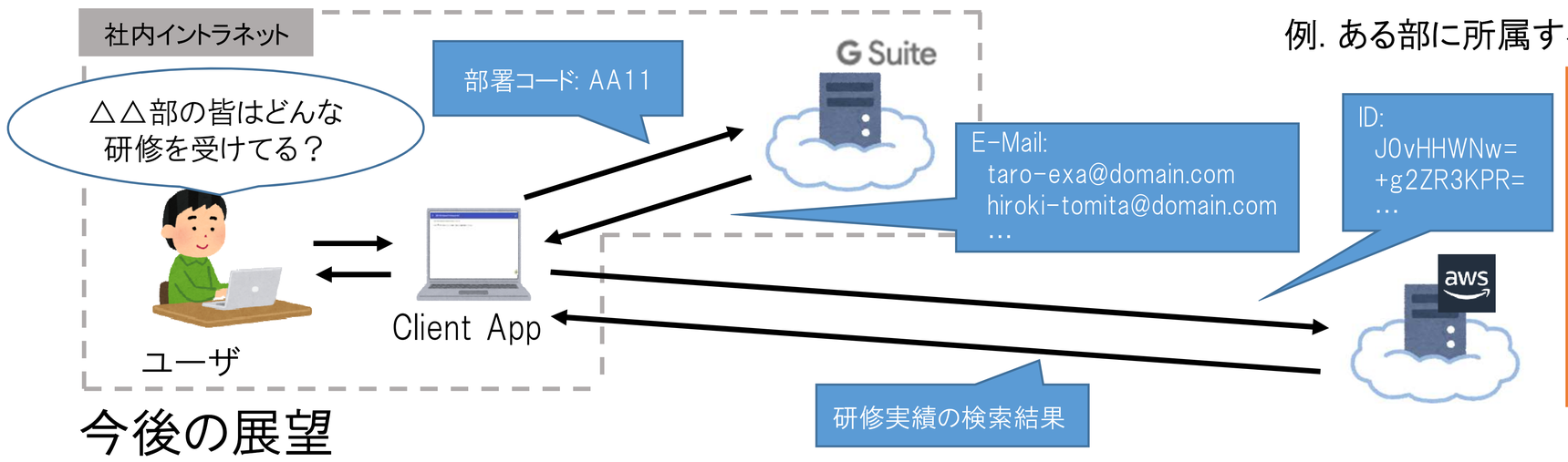
本システムの認証にはGoogleのOAuth2.0による認証を採用している。弊社G Suiteアカウント以外のGoogleアカウントは認証が通らないため、社員以外はシステムを利用する事はできない。これで、社内認証基盤には手を入れる事なくセキュアな認証機能を実現できた。Googleが無償で提供しているライブラリを利用しているため、費用はかかっておらず実装も容易である。

社員情報をAWS上に置かないための工夫

社員情報をAWS上には置かないようにするため、本システムのDB上では社員を識別するIDとして社員のメールアドレスを一方向ハッシュ関数でハッシュ化した値(※)を使用し、どのIDがどんな研修を受けたかのみを保存している。IDはクライアント側で計算した後AWSに送信しており、第三者から見て社員を特定できる情報がAWS上に保存されることはない。



しかしこのIDだけでは、各社員の氏名や所属組織等の社員情報を利用することはできない。そこで、G SuiteのGoogle Drive上に社員情報を列挙したスプレッドシートと、これを検索できるGoogle Apps Script(GAS)を作成し、API経由でGASを実行する事で社員情報を取得できるようにした。



例. ある部に所属する社員全員の研修実績を閲覧する場合

① G Suiteでその部署に所属する社員を全て検索する
② Client Appでメールアドレスから IDを計算する
③ AWSでは渡ってきたIDを元にデータを検索して返す

今後の展望

今回の取り組みは、ルール上社外に持ち出すことができない情報を利用したい様なケースで活用できると考えている。なお、AWS上でサーバレスアプリを開発する上での知見や勘所に関してはEVF2018にて発表したので、興味があれば資料をご覧いただきたい。