学認を利用したパブリッククラウドへのシングル・サインオン

坂根 栄作
クラウド基盤研究開発センター(CCRD)
国立情報学研究所

GakuNin Cloud

背景と目的

- パブリッククラウドの利活用が広がるにつれて、そのままではユーザ自身のアカウントが増えていき、管理が煩雑になるかも…
  - 自組織の資源とパブリッククラウドの資源のユーザ管理は独立
    - いろんなパターンがあり得ますが…
  - 複数のクラウドサービスを使い分けるハイブリッドな形態
    - 「どこのクラウド」を使っている、ということを特に意識する必要のない世界では、それぞれのクラウドを使うためのアカウントがユーザに剥き出しになる状況は好ましくない

- パブリッククラウドでも シングル・サインオン したい
  - 実際にシングル・サインオン サービスが提供されつつある
  - 自組織のアカウントから生成されるクレデンシャルを利用
- パブリッククラウドへの SSO の敷居は高い？参照できる導入事例はある？

- CCRD では、まずは著名なクラウドに対し SSO 実証実験を行なう
- 実証実験で得られたノウハウを共有

勘どころ：管理者視点から

- そのサービスはどんなもの？
  - 誰が使う？
  - その誰を、どのようにして認可できるか？
- 認可の方法：SP は何を照合して判断するか？
  - 人物（エンティティ）
  - 属性／ロール

- 認可判断のための属性を、現実的に SP に送出できるか？
  - 自組織 IdP が自然に付与できる属性
    - 教員、職員、学生、…
  - それ以外の属性

- サービスの分類（この資料でのみ）
  - *Common* service：自組織 IdP が自然に持つ属性で認可
  - *Private* service：それ以外で認可

デモ動画を紹介します

AWS へのシングル・サインオン

デモ 内容／環境

- シナリオ
  - AWS マネジメントコンソールへのアクセス
  - 認可は、AWS のロールに基づく
  - 自組織 SAML IdP から発行される SAML アサーションを利用
    - アサーションに含める必須属性は AWS により規定

- 環境
  - AWS アカウント（ホンモノ）
    - 自組織 IdP からの認証情報を受け入れる SP
    - SAML ID provider を作成
    - シナリオに適したロールを作成
  - 学認クラウドゲートウェイ（本運用）
    - サービスの起点
    - プライベートサービスとして登録：https://idp.local/SAML2/Unsolicited/SSO?providerId=urn:amazon:webservices
  - 自組織 Shibboleth IdP（実験用）
    - AWS endpoint に送る認証レスポンスを生成

今後の展開

- パブリッククラウドへの SSO 実験の実施
  - クラウド：AWS, Azure, …
  - 認証技術：SAML 2.0
- 実験で得られた知見を共有し、学術機関でのクラウド利活用の促進に貢献できれば ☺

- 学認クラウドゲートウェイでできることは…
  - クラウドのサービスが *private* の場合
    - サービスは、あるグループが利用
    - クラウドの要求する認証レスポンスを、グループメンバの認証情報をもとに生成し送出するような機能？
  - その他