大学等におけるクラウドサービス利用シンポジウム2017

アカデミック IDaaS の ウラ(現実編)

エクスジェン・ネットワークス株式会社
野村 健太郎

自己紹介

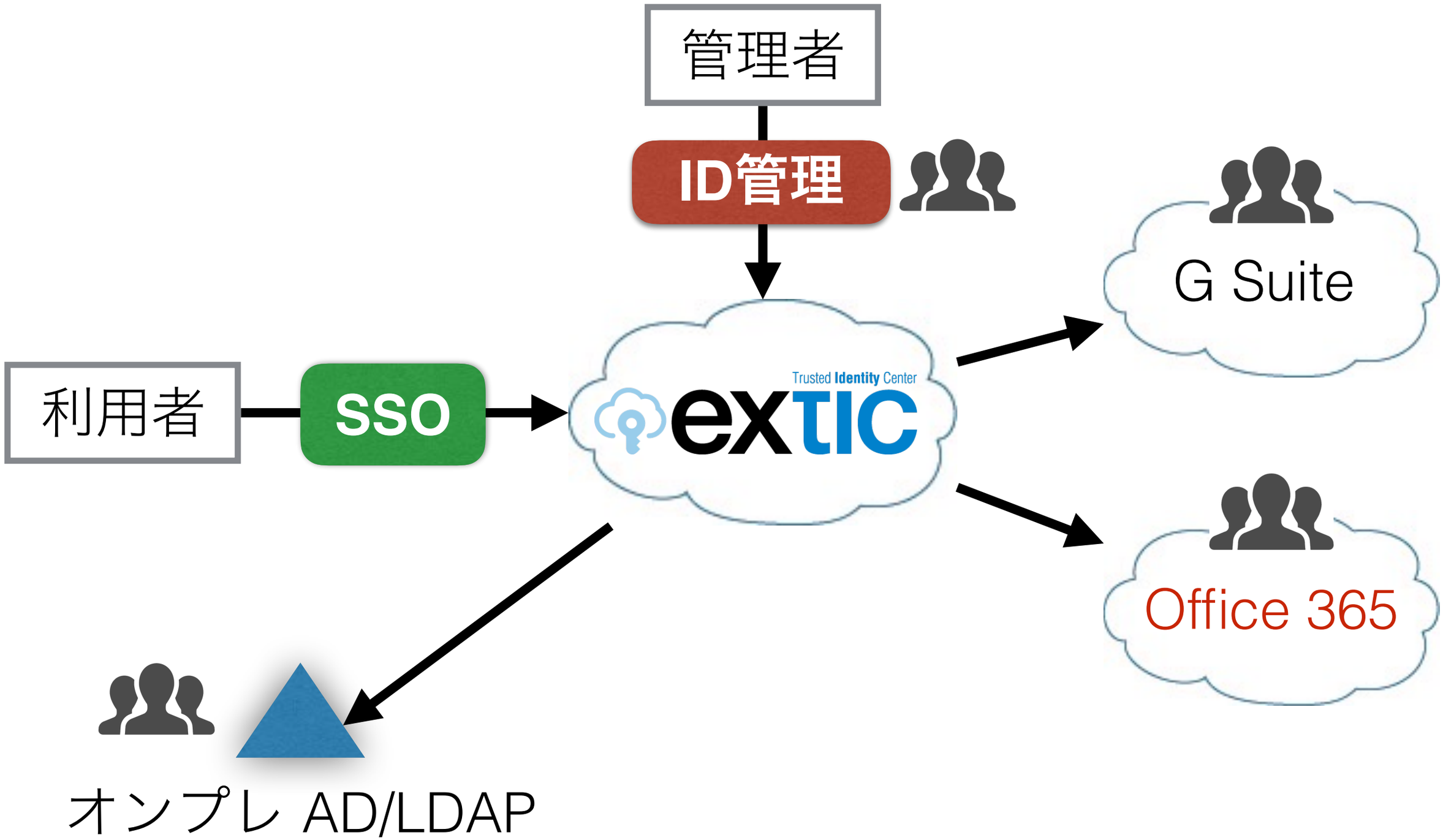
- 大分県出身
- 2000年4月 広島大学工学部第二類 入学
- 2006年3月 広島大学大学院工学研究科情報工学専攻 修了
- 広島で一番好きなお好み焼き屋：西条の「くいしん坊」(コスパ最強！)
- 就職して以来ずっと認証関連の仕事に従事
- 最近のお気に入り： Docker、Alpine Linux

今日お話しすること

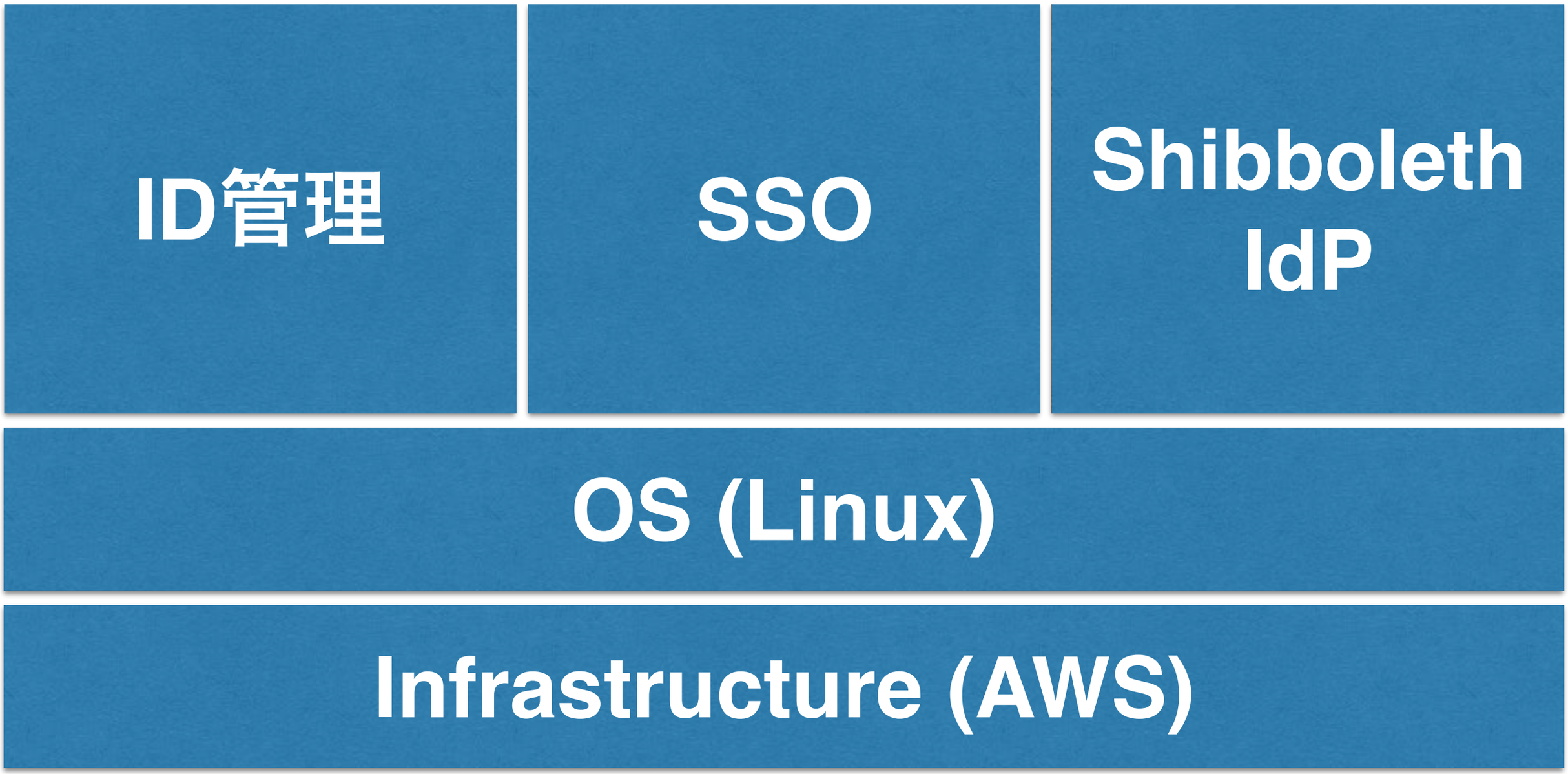
IDaaS(Identity as a Service)
を開発するにあたって

- 苦労した点
- 工夫した点
- 悩んでいること

IDaaS でできること



IDaaS 構成要素



IDaaS を開発するにあたって

- これまでのオンプレの ID 管理/SSO の経験から、機能面では文教分野において必要な機能はたいがいは実装できるだろうという見込みはあった

- サービスとしての開発・運用は初めてだったため様々な課題に直面した

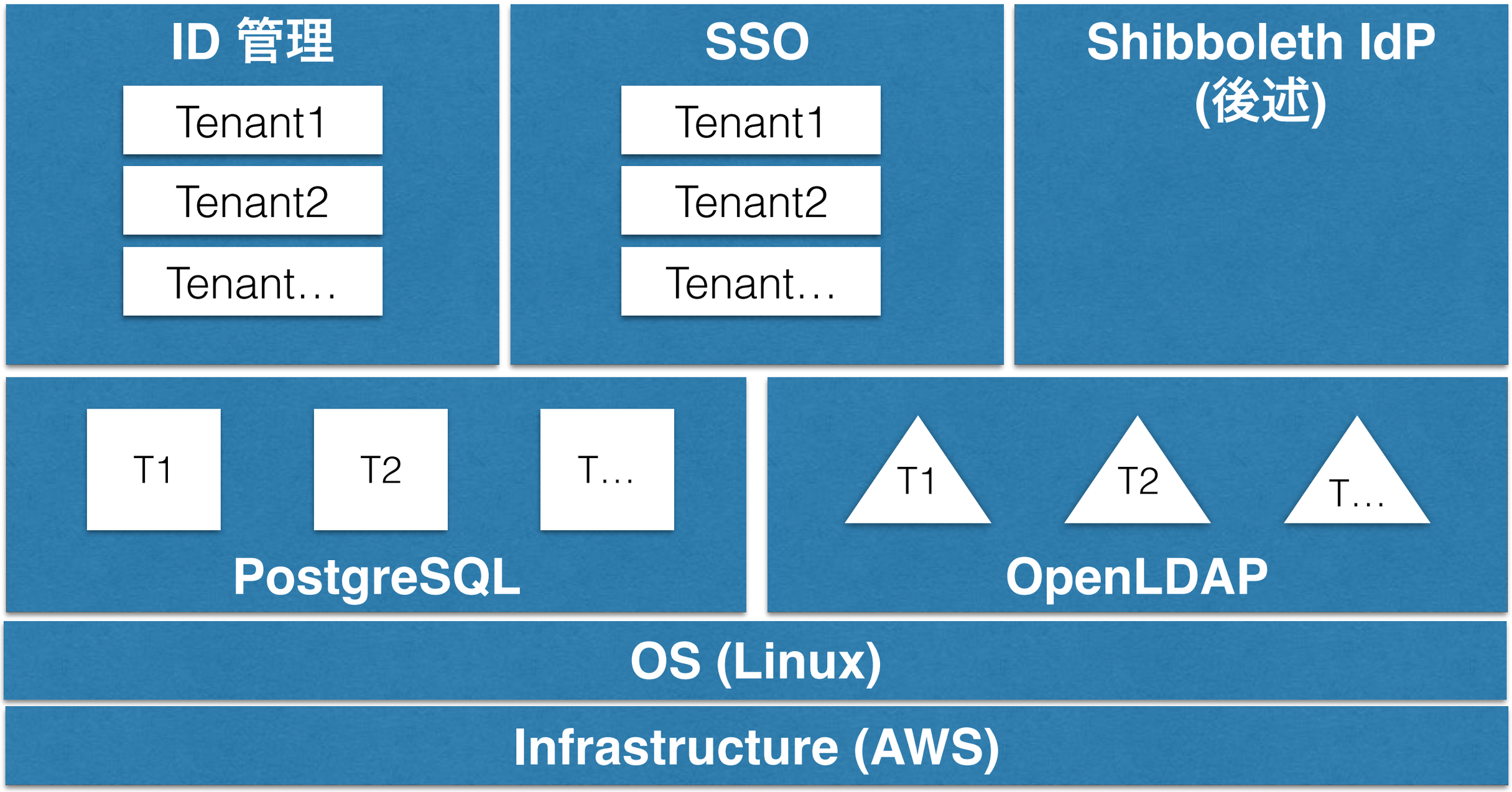
マルチテナント

マルチテナントの実現

- オンプレにはないサービスならではの要件

- 論理的にマルチテナントを実現

論理的にマルチテナントを実現



ID 管理

ID 管理

- 弊社が最も得意とするところ
- オンプレ AD/LDAP への ID 連携のノウハウは豊富
- クラウドの ID 管理も API を叩けば ID は作れる
- 機能
  - GUI 、CSV 、API

ID 管理の課題

- クラウドサービスの「ライセンス」
  - オンプレの ID 管理ではあまりなかった概念
    - ユーザー単位の課金
- 1番複雑なケースが Office 365 (弊社で調査した範囲で)

ID 管理 - ライセンスの例

Office 365

ライセンス	つかえる機能
Office 365 Education	Office アプリケーション Skype SharePoint Exchange …
別のライセンス	…

ID 管理の課題 - ライセンス

- Office 365 のライセンス管理
  - 1つのテナント(大学)で複数のライセンスが”**混在**”する場合がある
    - メインのライセンス + 付加的機能のライセンス
- ライセンスを付与しないという選択肢もある

ID 管理 - 課題解決

- 最初から完璧な機能の提供は難しい…
  - クラウドサービスは変化が速い
  - 実装しても顧客の要望にマッチしていなかったら意味がない
- Must な機能からやっていく
  - 要望がある機能
  - すぐに実装できる機能

SSO

SSO

- まずは OpenAM でチャレンジ
    - マルチテナント対応
    - 機能が豊富
        - SAML IdP
        - ワンタイムパスワード
        - クライアント証明書認証
- 構築ノウハウがあった

SSO の課題

- 運用工数が大きい
- 自動化が大変
- バグ・脆弱性が多い
    - 影響はなかったが、情報の精査に手間がかかる

SSO - 課題解決(案)

- もっと”**軽い**”ものがよい

- SAML IdP があればなんとかなる(Must)
  - 自分たちで作る
  - Shibboleth IdP を使う(後述)

- 認証機能の拡充は今後の課題

Shibboleth IdP

Shibboleth IdP の課題

- ぶっつけ本番の設定変更
- マルチテナントの実現

Shibboleth IdP の課題
ぶっつけ本番の設定変更

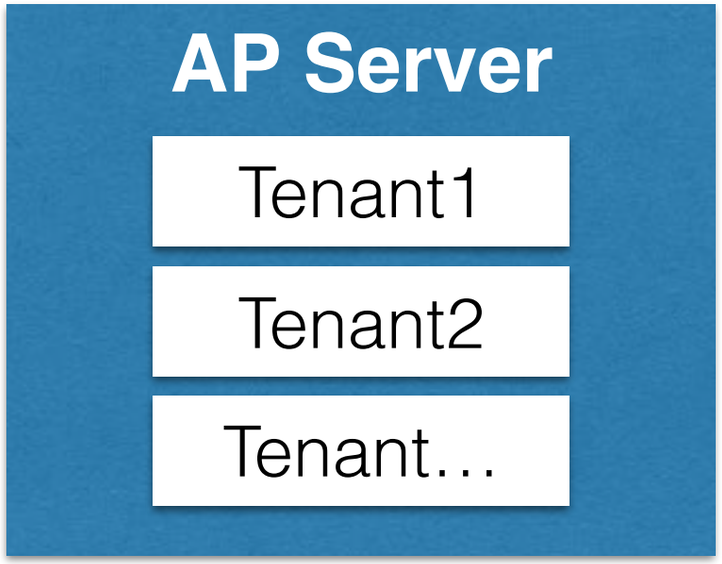
- フェデレーションの成否は”**やってみなければわからない**”

- 学認運用フェデレーションの SP は検証環境の準備が困難

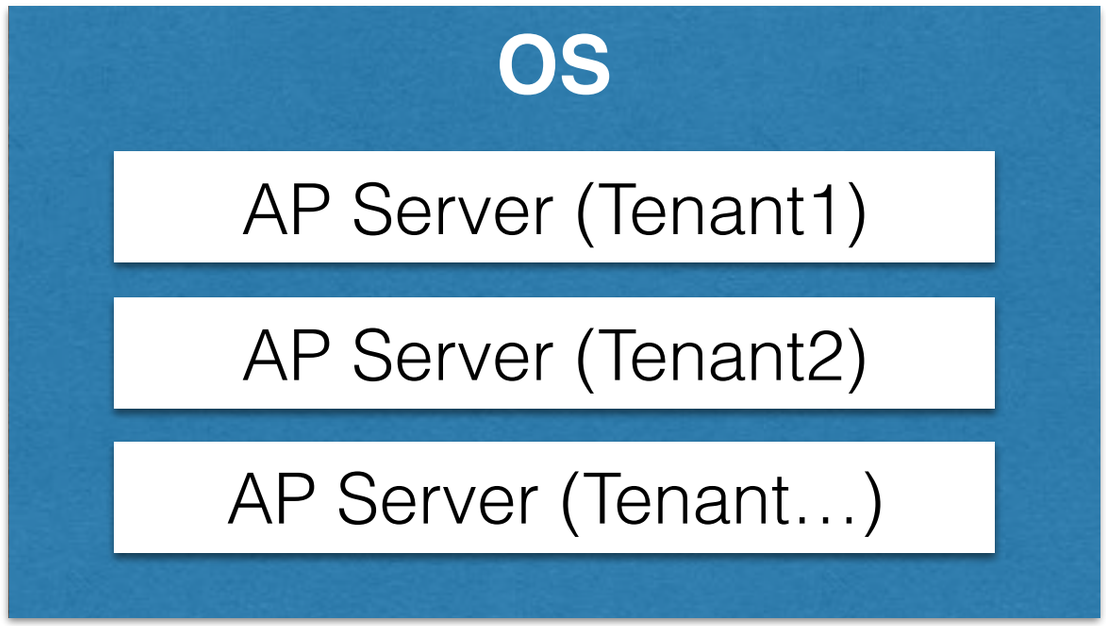
- 必然的に、運用中の本番環境に対する設定変更が必要になる

- 無停止、かつ、他のテナントに影響を与えずに設定変更できる仕組みが必要

Shibboleth IdP マルチテナント実現案

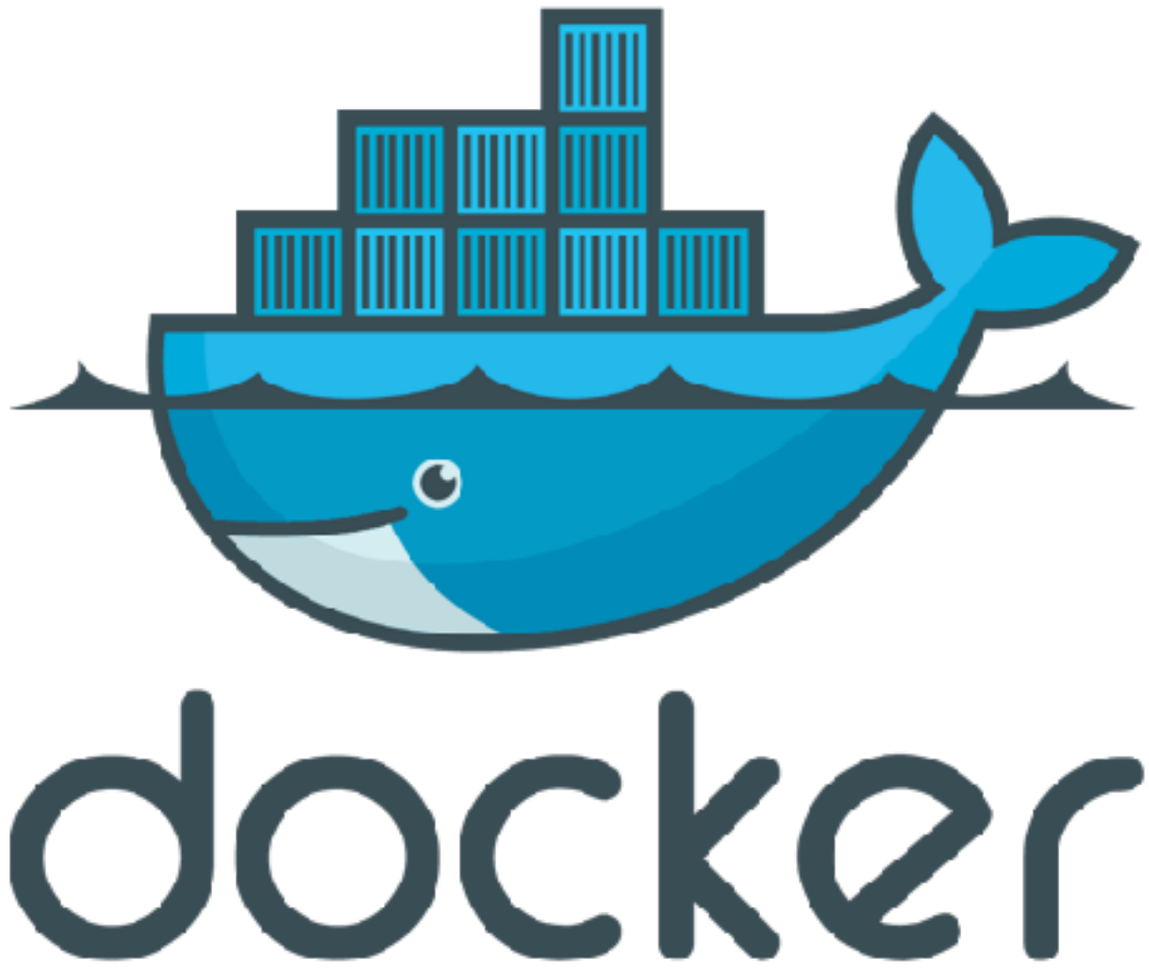


- 一つの AP サーバー(Tomcat など)の中に複数のテナントを収容
- AP サーバー/OS 再起動が全テナントに影響



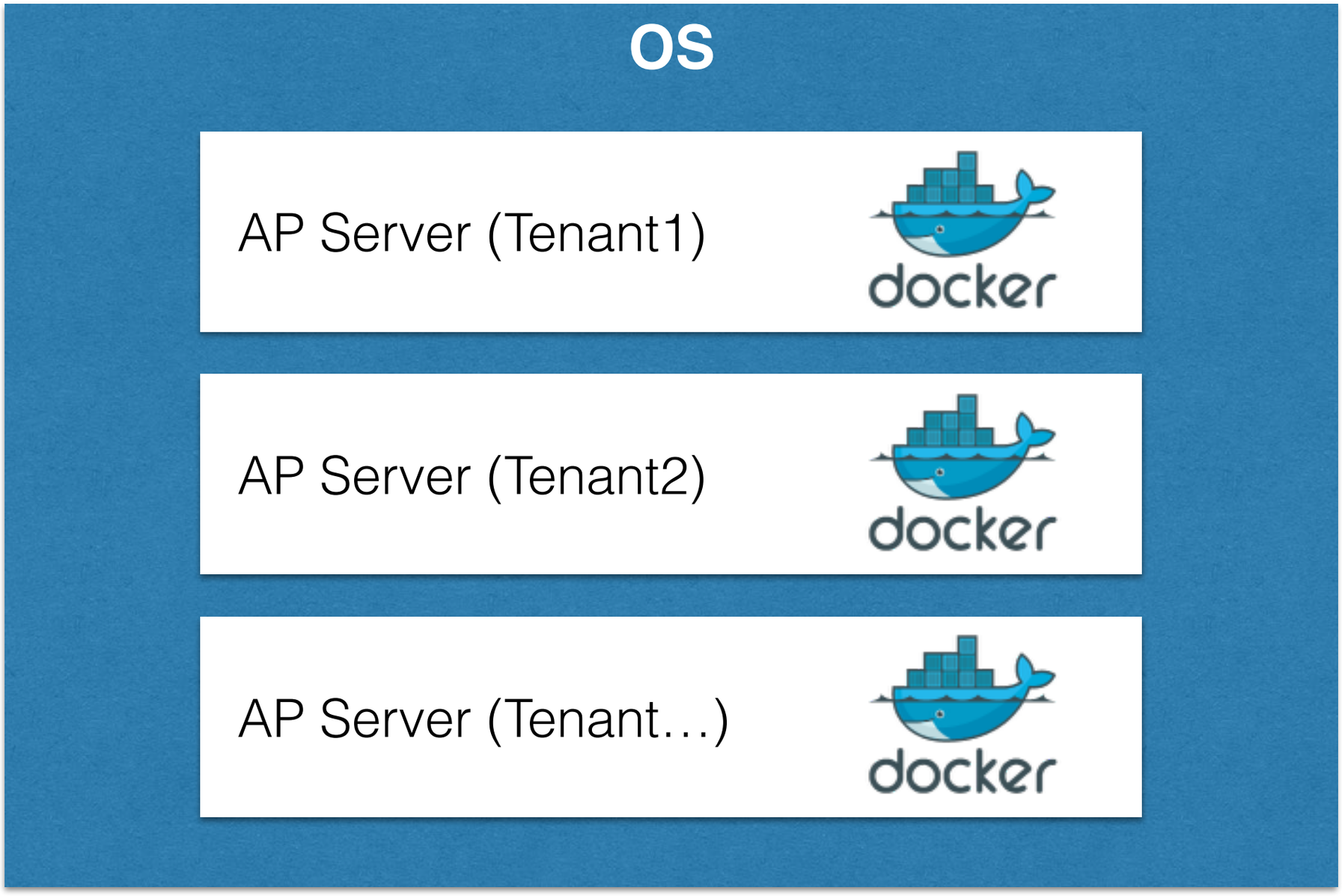
- テナントの独立性は確保できる
- 管理が面倒

Shibboleth IdP
マルチテナント実現案



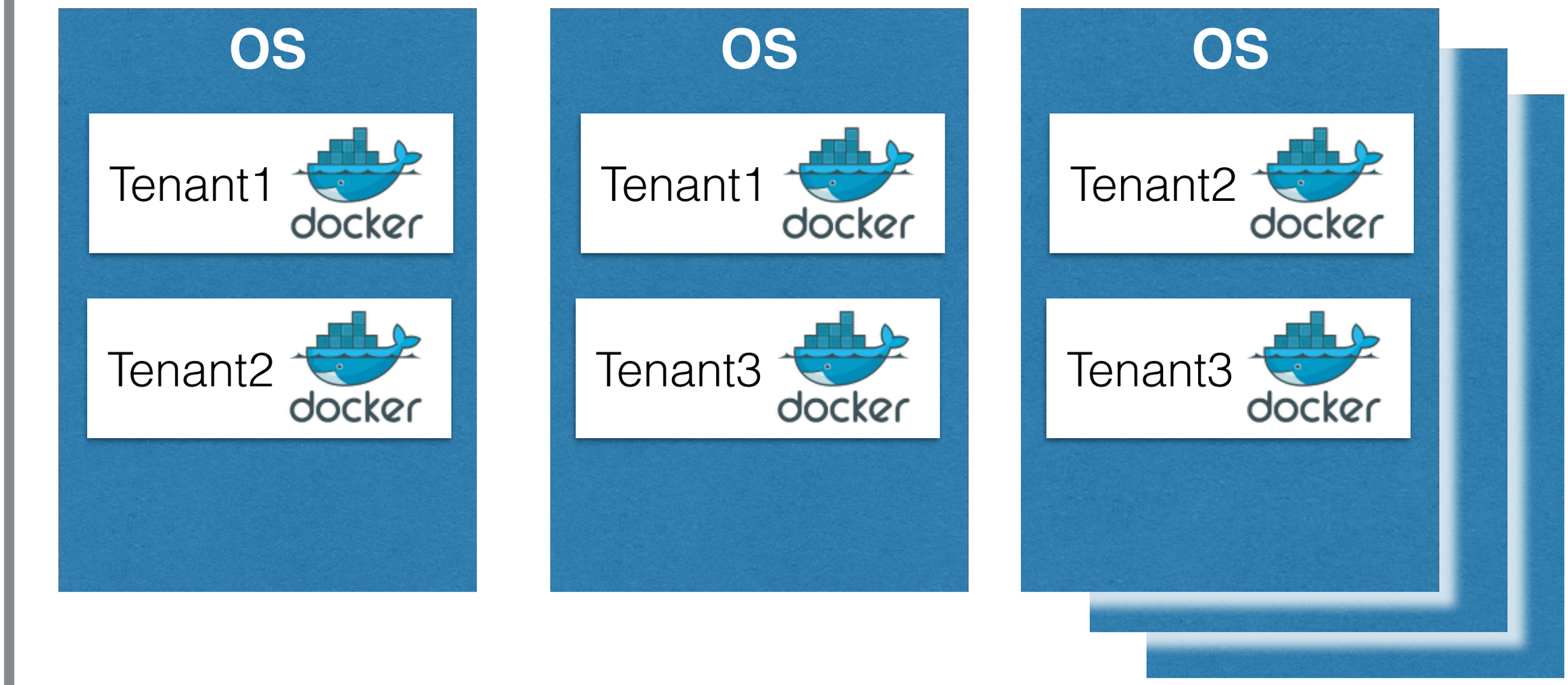
Shibboleth IdP を

Docker コンテナとして動かす



Shibboleth IdP を AWS ECS で動かす

AWS ECS(EC2 Container Service)
Cluster



Shibboleth IdP - 課題解決

- Docker (AWS ECS) により実現
- テナントの独立性
- 冗長性
- 柔軟性(設定反映作業)

その他

- セキュリティの担保
- 暗号化
- 脆弱性対応

今後について

今後の課題・悩み

- 多要素認証
  - ユーザー(学生)はどの方式なら使ってくれる？
  - スマートフォンなどの OTP アプリは利用可能？
    - 全員がスマートフォンを持っているとは限らない
  - OTP を個人のメールアドレス/ SMS に送信でもよい？
    - 全員がメール受信/ SMS 受信できるとは限らない
- SSO/Shibboleth IdP
  - クラウドサービスとの連携が増えた場合、属性情報はどこまで提供していいのか？