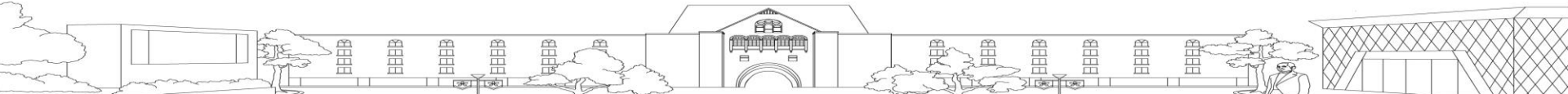
〈学術情報基盤オープンフォーラム2019〉

学認クラウドゲートウェイサービスへの期待

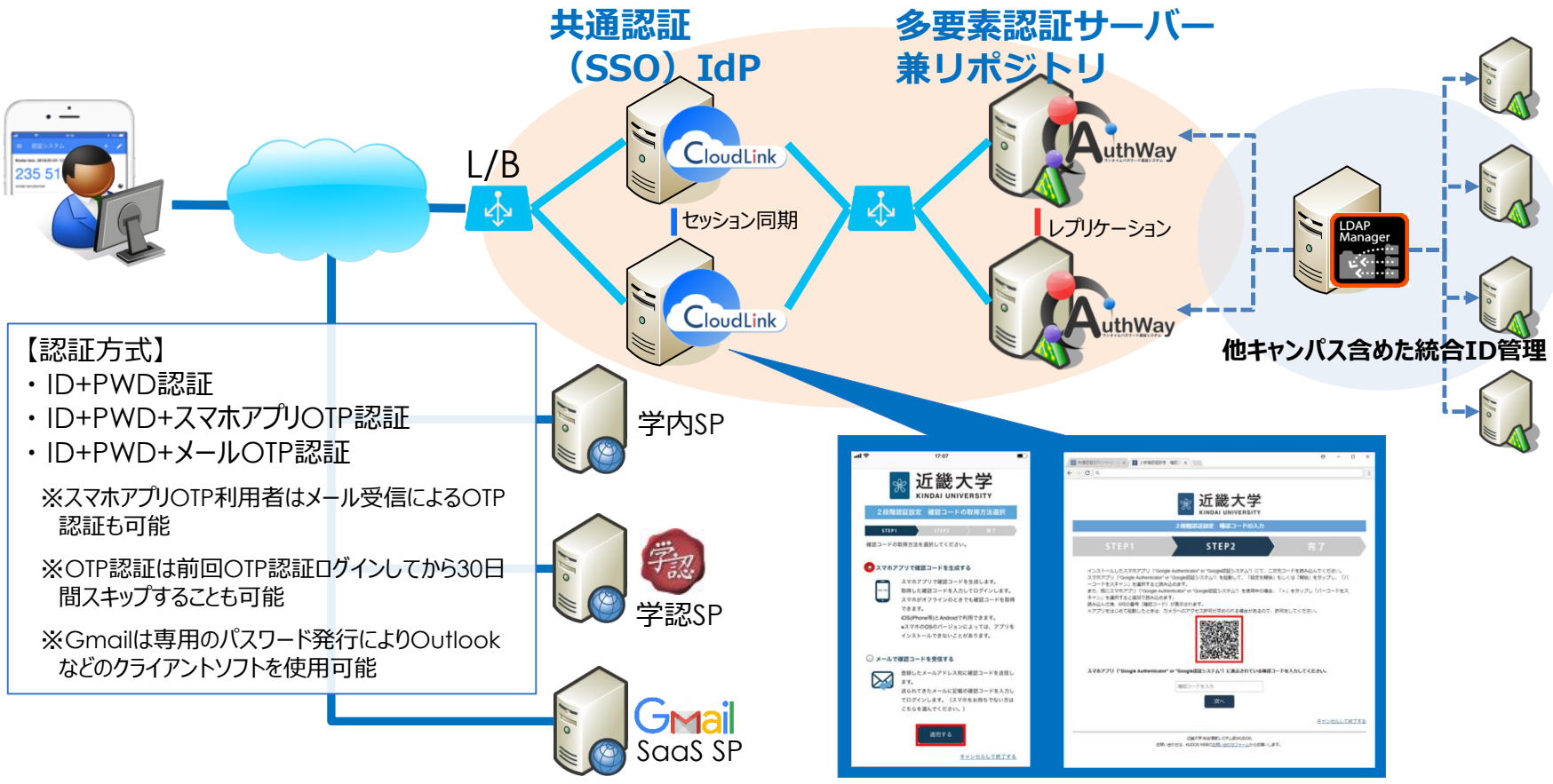
学校法人 近畿大学
総合情報システム部

2019-05-30



アジェンダ

- 自己紹介
- 近大IdP/SP
- クラウドゲートウェイサービスに期待すること
- さいごに


共通認証
（SSO）IdP
多要素認証サーバー
兼リポジトリ
L/B
CloudLink
CloudLink
セッション同期
AuthWay
AuthWay
レプリケーション
LDAP Manager
他キャンパス含めた統合ID管理
【認証方式】
・ID+PWD認証
・ID+PWD+スマホアプリOTP認証
・ID+PWD+メールOTP認証
※スマホアプリOTP利用者はメール受信によるOTP認証も可能
※OTP認証は前回OTP認証ログインしてから30日間スキップすることも可能
※Gmailは専用のパスワード発行によりOutlookなどのクライアントソフトを使用可能
学内SP
学認SP
Gmail
SaaS SP
近畿大学
KINDAI UNIVERSITY
利用者自身が使用する認証方式を設定
近大IdP

LDAP Manager（EXGEN）

アカウント管理システム。源泉からデータを受け取り、AD/LDAPにアカウント情報を同期

CloudLink（IP3）

SAML IdP（Shibboleth同等の機能）、SSOログイン画面のUI、MFA設定画面UI、MFAスキップ用のcookie発行

AuthWay（IP3）

パスワード認証、MFA認証（スマホOTP、メールOTP）、MFA設定情報（メルアド等）、アカウントロック

近大IdP

対象者　　：　約47,000人

開始時期　：　2018年3月

対象SP　　：　学認SP5、独自SP30

近大IdP

学認SP

りんりん姫、eduroamJP認証連携ID、OverDrive、丸善、日経BP

独自SP（プライベートサービス）

ERP、教職員ポータル、LMS、G suite、コンビニ証明書、

ゲストWi-Fi、オンラインストレージ、VPN、etc

近大IdP

・学生、常勤/非常勤教員、職員で、使えるSPがバラバラ
　使えるポータルもバラバラ

・→のようにWebにリンクを並べて対処
　但し学生向けのみで、大切な情報が
　格納されていて、かつ学外公開のSPは
　セキュリティの観点でどこからも
　リンクしていない。

課題・期待

・クラウドゲートウェイサービスにログインしたユーザが

利用可能なSPのみ表示されると良い

→現状、グループ管理者の機能で手作業でグループを作成したら実現できなくないが、メール送ったりユーザ側でアクションが必要だったりするので運用的に実質実現不可

以下提言（テキトーに言ってるんで話半分で聞いてください）

1. REST APIをIdP側から操作できるような機能改修を実施いただき、グループ機能を使ってグループを手動で作成し、そこにREST APIを使ってユーザを自動追加する。ただ、「学生」といったグループだと、本学の場合メンバーシップが数万に及び、REST APIだと、1メンバーの登録につき1リクエストが必要なので、初期登録処理はかなり大がかりになりそう。

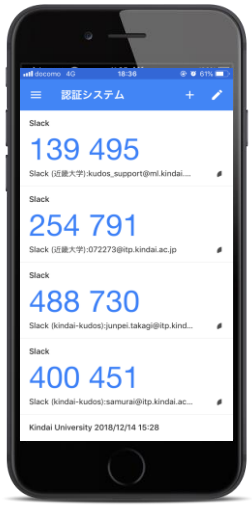
課題・期待

2. REST APIを用いるのではなく、LDAPの動的グループを用い、ユーザを個別に列挙することによるのではなく、LDAPの条件式（◎◎属性の値が●●である 等）によってグループメンバーシップを定義する、といったことはできないか。

3. グループメンバーを定義することはせず、ユーザの属性値（isMemberOf、もしくはjaOrganizationalUnitName、eduPersonPrincipalName、eduPersonAffiliation等の属性を活用）を条件として判定し、各SPごとの表示有無を条件指定できるようにする、という方向性は取れないものか。

課題・期待

・現状はレスポンシブ？な感じでスマホ対応しているが、ネイティブアプリがあると利便性が向上（OneLoginアプリみたいに）
さらにいうと、コードジェネレータも付いてるとなお良い。



課題・期待

近畿大学

KINDAI UNIVERSITY