Shibbolethでの属性変換を用いた認可の制御について

徳島大学　高度情報化基盤センター
金西　計英

認証基盤の連携構築

- Webアプリケーションの利用需要の拡大
  - 学外のサービスを利用したい
  - ID・パスワードの管理は，なるべく簡単に
- 連携（Federation）の構築
  - 学内の認証基盤
  - 認証と認可
  - 認証基盤の連携
- 連携　→　SSO(Single Signe On)の実現
- 連携方式
  - ライブラリ方式
  - エージェント方式
  - リバースプロキシ方式

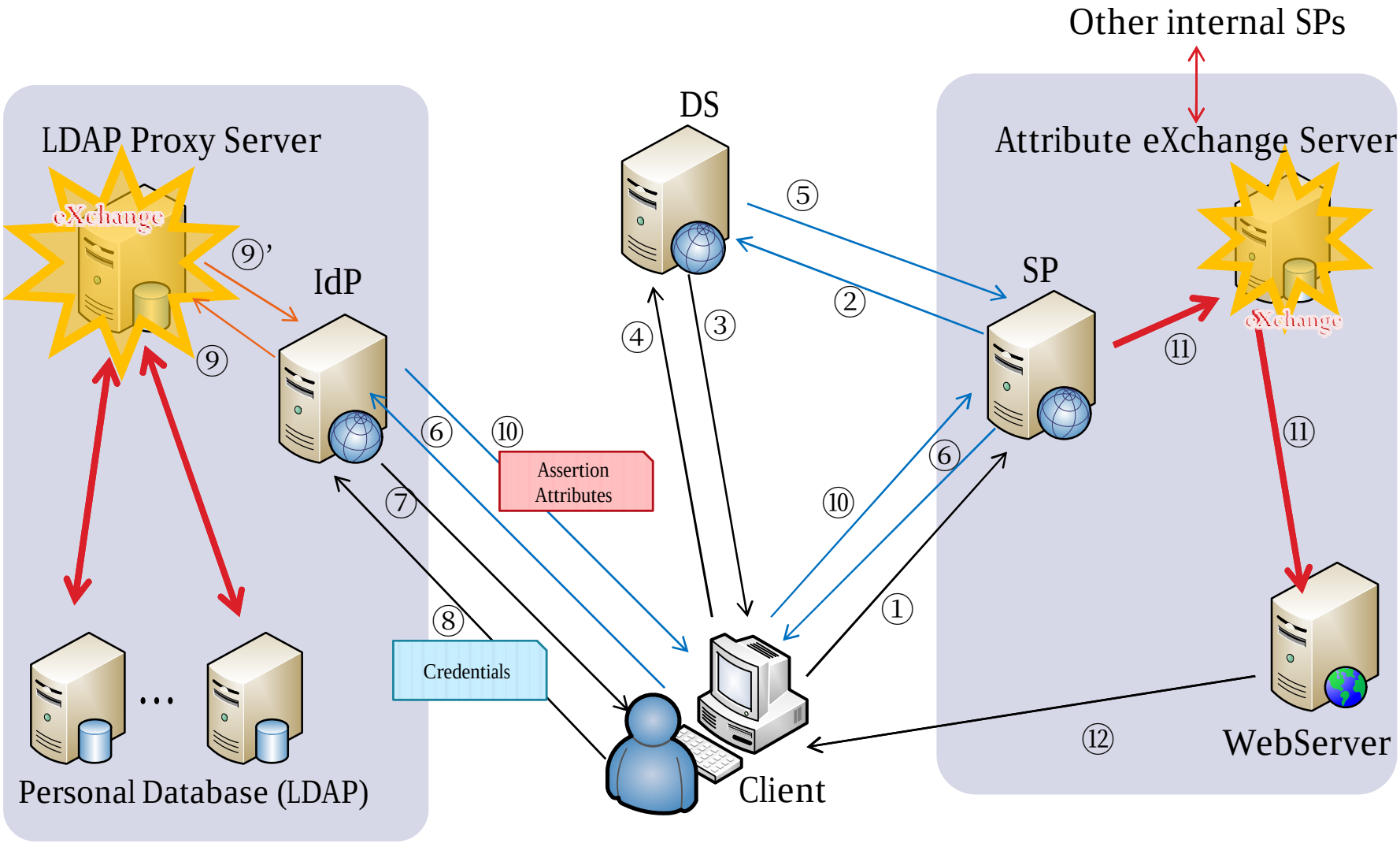
連携の運用における問題点

- 認証(Authentication)と認可(Authorization)
  - 認証にのみ注目が集まる傾向
- 高等教育における認可
  - 構成員の属性は，比較的に，明確に分かれる
    - 学生，職員，教員
  - 各Webアプリは，属性によって振る舞いが変化
- 既存の情報系システムと連携のスムーズな接続
    - 個人属性データベースとしてLDAP等が既設
    - 既設Webアプリは，独自の属性フォーマットで可動
  - 連携の属性と既設属性は，一致しない
  - どこかでフォーマットの調整が必要
- 個人属性変換による認可の間接的制御
  - 送信側（LADPの多段接続）
  - 受信側（ID Mapping　＆　属性変換）
- 柔軟な認可環境の実現
  - ポリシの適切な運用
    - メタデータの交換
    - ポリシの編集・交換の枠組み

連携における属性変換の可能性

- 連携の枠組みに対する変更は小さくしたい
  - IdP，SPへ手を入れない
  - 連携内では，相手を信用が原則
    - 原則を崩さない
- 既存の情報系システムとの協調
  - 送信側と受信側の２箇所での属性変換
- 属性変換の可能性
  - 認証に用いるIDと，Ｗｅｂアプリの IDは一致している必要はない
  - 属性の組み合わせによって，新たな属性を生成することで，Webアプリ側の負担を軽減
  - 柔軟な運用の枠組みを提供

Shibbolethと属性変換

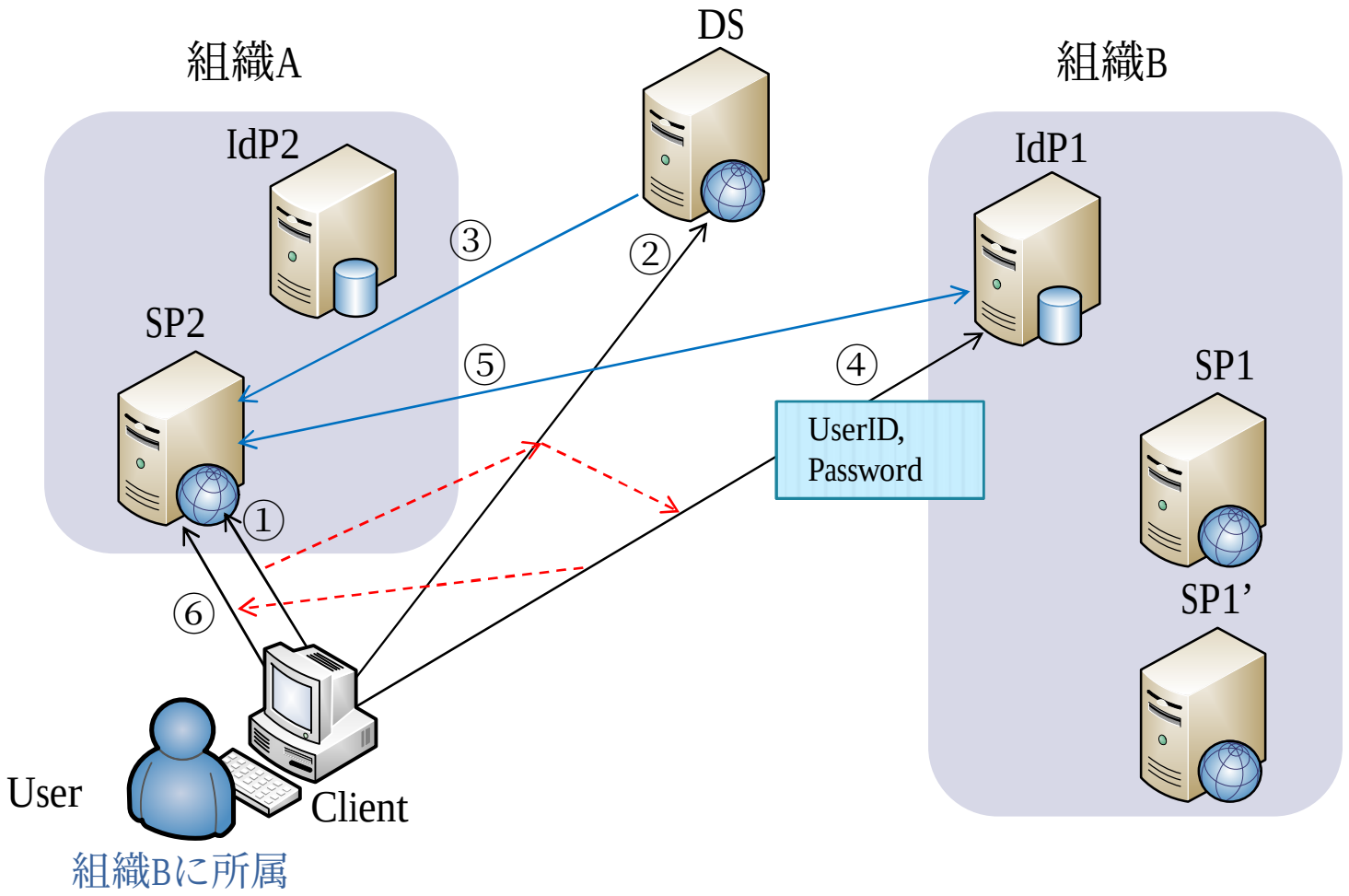


実験環境

- Shibbolethを使った属性変換機能の実証
- 大学内に実験環境を構築
- 内容
  - ２つの組織をシミュレーション
  - 属性変換の検証
  - SP間でのSSO（その際，属性を変換）
- 環境
  - Shibboleth2.0（← Shibboleth1.3）
  - IdP ２台
  - DS １台
  - SP+Web　　３台（内1台は予備）
    - ターゲットアプリとしてSNS（OpenPNE）
  - 被験者　約40名
  - 期　間　9月中旬より試行開始

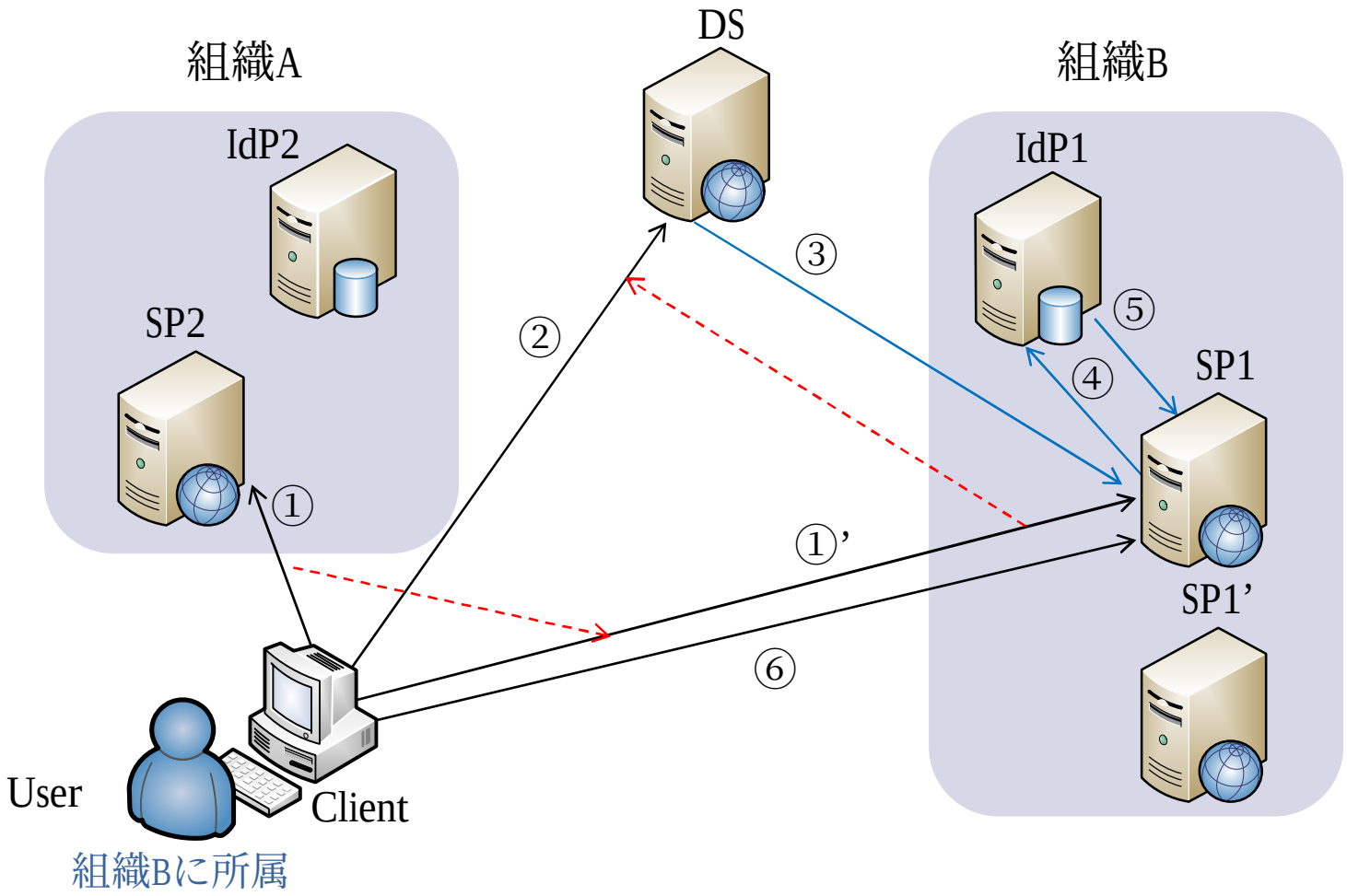
実験環境の概要

- ログインの例

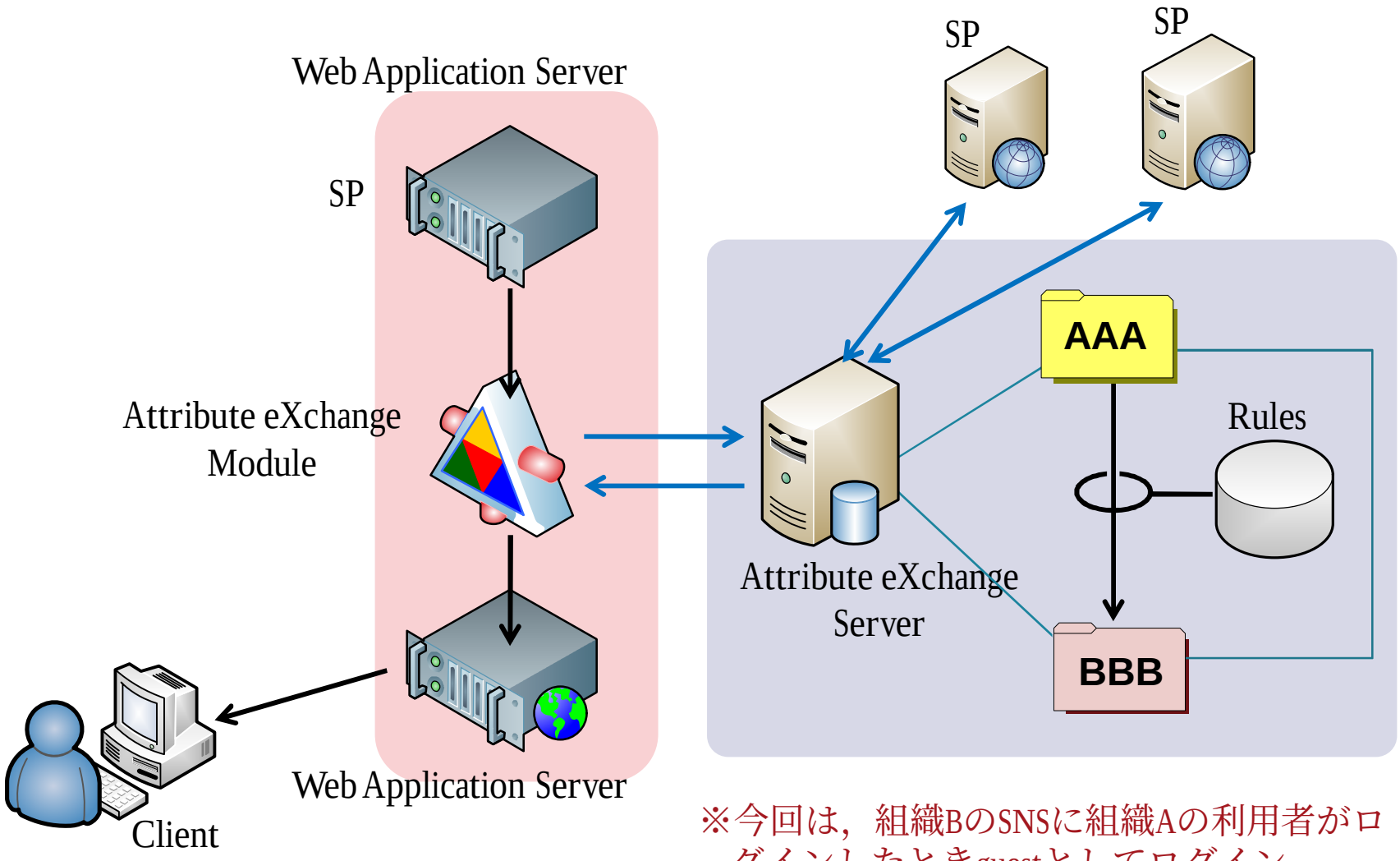


実験環境の概要

- SSOの例



属性情報の変換

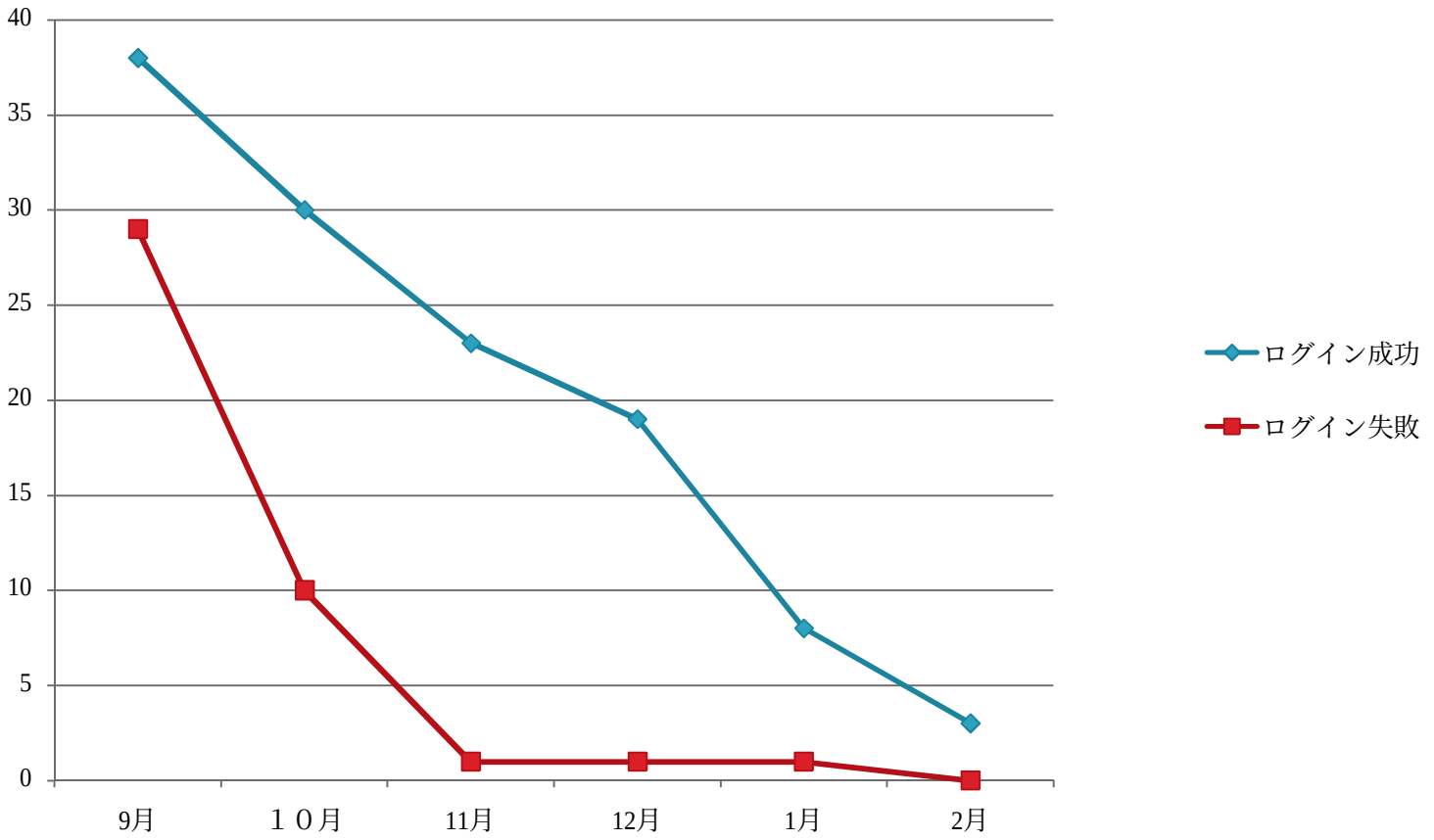


※今回は，組織BのSNSに組織Aの利用者がログインしたときguestとしてログイン

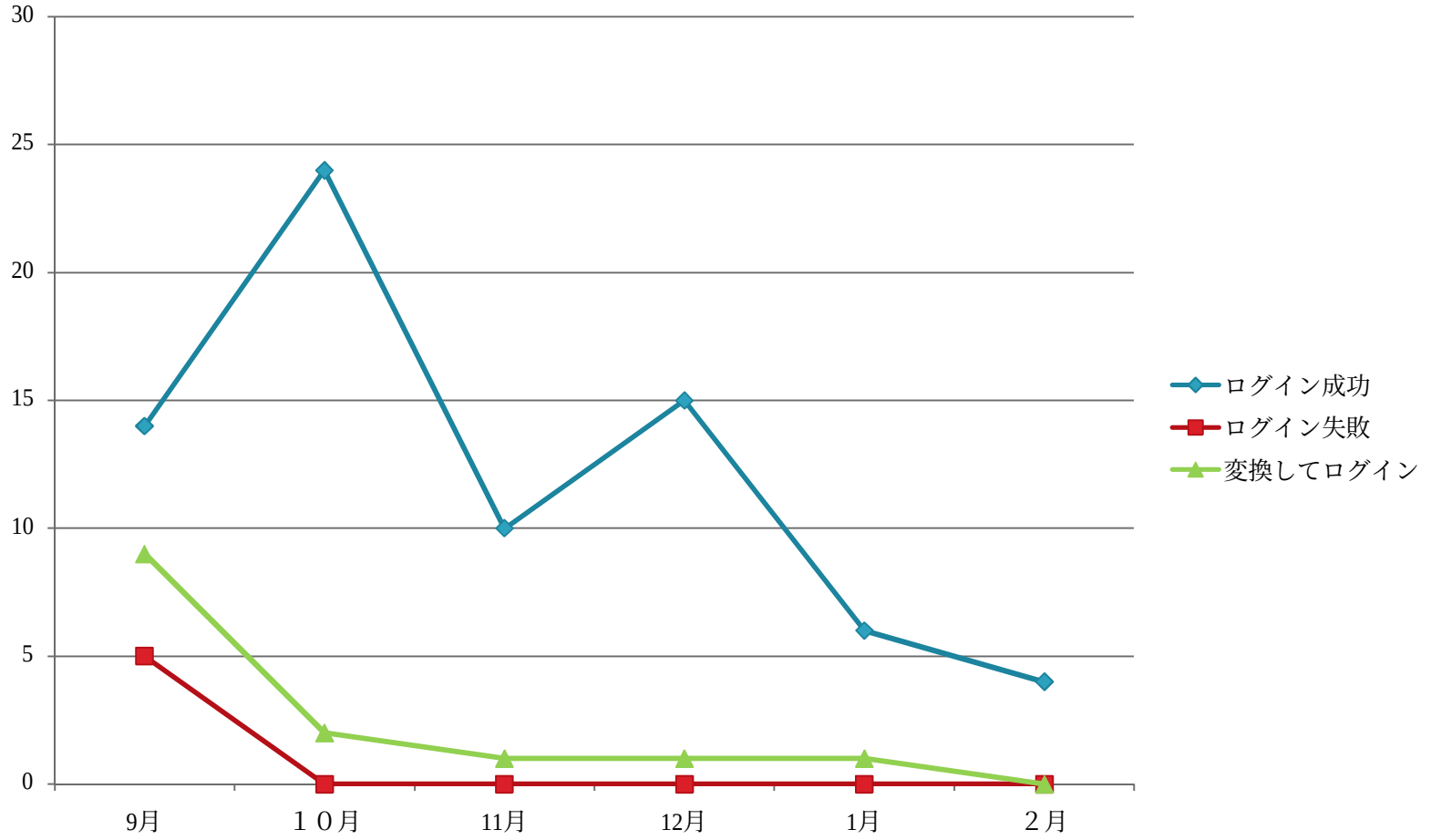
今回の属性変換方法について

- SPとWebサーバの間に属性変換機能を実現
  - SPとWebサーバの間をフック
  - 属性変換機能をサーバとして外部に設置
- 属性変換サーバ
  - 変換機能を外部に設置することで，情報処理センター等で，一元管理
  - 各Webアプリの管理者が属性変換ルールを管理するのか？センター等で属性変換のルールを管理するのか？
    - 属性変換を完全に末端側に任せてしまうと，運用上，混乱する可能性があり
  - Shibbolethでの属性変換
    - Shibboleth2.0から機能が充実
      - IDのマッピング
      - 属性のマッピング（置き換え）
      - 属性名や属性値の書き換えは簡単ではない（かなり大変）
- ルールベースによる変換を実現
  - 変換サーバ上に，変換ルールを記述
  - 正規表現による変換規則
  - 柔軟な変換ルールの記述
  - 変換機能の独立

シングルサインオン実証実験結果（SP1）



シングルサインオン実証実験結果（SP2）



結果と考察

- SSOの実験結果
  - ログイン，SSOは問題無し
  - SP2において，属性変換を実施
    - SP1では，認証は通るものの，アプリケーション側にユーザ登録がされていないため，アプリケーション内でエラーが発生している（ログイン失敗）
    - SP2では，アプリケーション内に登録されていないユーザは，ゲストに属性を変換し，ゲストとしてログイン
  - 変換機能も問題無く可動
  - 利用率そのものは，やや低調
    - 利用者に，SNS利用の特別なモチベーションを設定しなかった
    - 普通にSNSの利用を依頼（盛り上がらないと，SNSの利用は低下）
    - SNSシステムの実験ではないため，やむを得ず
- SSOの実験から
  - 属性変換には，運用の状況によって，一定の可能性有り
    - 複数の手法が存在するため，運用側が適切に選択する必要有り
  - 変換サーバの運用方法の設定
    - 変換ルールの記述方法の簡便な方法を確立
    - ルールの管理体制を確立

まとめ

- 連携の実用的な運用確立
- 属性変換は必要
  - 連携が普及するほど認可の問題がクローズアップ
    - 各組織の個別事情と連携との対立
  - 現実的な運用方法の開発
  - 属性の変換による認可の制御が可能
- 属性変換機能
  - 結局，送信側と受信側の双方に必要
  - 変換サーバの提供
    - Shibboleth2.0のマッピング機能だけでは，実現が大変
- 属性変換の実験
  - 実験環境で連携は，問題無く動作
  - 今回実装した属性変換は，正常に機能
- 今後の予定
  - テスト環境ではなく，実際の環境での実証実験