NII学術情報基盤オープンフォーラム2018@NII
2018/6/21(Thu)

金沢大学における多要素認証

金沢大学　松平　拓也

KANAZAWA UNIVERSITY

本日の発表内容

- 金沢大学における多要素認証導入方針
  - どのような多要素認証環境を実現したいか
- MultiFactor認証フロー
  - Shibboleth IdP 3.3から導入された機能
  - 本学の多要素認証導入方針にどれだけ対応できるか
- 本学の多要素認証準備状況
  - MultiFactor認証フローを利用して環境を構築
- まとめと今後の課題

国立大学法人 金沢大学

- 構成員
  - 学生（院生含む）
    - 約 10,300名
  - 教職員（非常勤含む）
    - 約3,800名

2015年3月14日・北陸新幹線開業

KANAZAWA UNIVERSITY

金沢大学統合認証基盤（KU-SSO）

- Shibbolethによるシングルサインオンを実現
  - Kanazawa University Single Sign On（KU-SSO）
    - 平成22年3月から本格運用を開始
    - 30以上の学内情報システムをShibboleth SP化
      - 予算執行支援、給与明細、教務システム、教員DB等、機微な情報を取り扱うシステムも多い
- KU-SSOの認証方式
  - 金沢大学ID・パスワードによる認証
    - 世の中ではID・パスワードに関わるセキュリティインシデント報告の増加
      - 総当り攻撃、辞書攻撃、パスワードリスト攻撃など

多要素認証への移行が重要

KANAZAWA UNIVERSITY

金沢大学における多要素認証導入方針

- 多要素認証導入の課題
  - 特定の所有物（スマートフォン、ICカードなど）がないと認証できない
  - ID・パスワード認証より手間がかかる

1. 複数の多要素認証方式を選択できるようにする
   - 全員に同じ多要素認証方式を指定するのではなく、複数の多要素認証方式を用意し、ユーザが選択できるようにする
     - トータルで全構成員が多要素認証を扱える環境を整備する
2. サービスの重要度に応じて認証レベルを変更できるようにする
   - 従来の認証レベルで十分なサービスはID・パスワード認証で対応
   - 高いレベルを要求するサービスにおいては、ユーザの利用環境に応じて多要素認証を要求
     - サービスの重要度に応じて多要素認証を要求することで、ユーザの利便性を維持する

KANAZAWA UNIVERSITY

MultiFactor認証フロー

- MultiFactor認証フロー
  - Shibboleth IdP バージョン3.3より導入
  - 単体、又は複数の認証フローを組み合わせ、独自の認証シーケンスを作成できる
  - MultiFactor認証フローを利用することで、Shibboleth IdPバージョン2向けにNIIと金沢大学で共同開発したGUARDプラグインと同様な認証シーケンスを実現可能

NIIが設定方法を公開
https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=26186832

- 実現したい認証シーケンス
  1. ユーザのIPアドレスに応じて要求する認証方式を変更したい（リスクベース）
  2. 複数の認証方式を選択できるようにしたい（and/or 条件）
  3. 認証方式をレベルとして抽象化したい

MultiFactor認証フローを用いてどこまで対応可能か？

実現したい認証シーケンスの対応状況

1. ユーザのIPアドレスに応じて要求する認証方式を変更可能
   - 認証方式ごとにどのIPアドレスから来たら提示するかを決定できる
     - 例　学内IP：ID・パスワード
       学外IP：tiqr
2. 複数の認証方式を選択可能（and/or 条件）
   - ユーザが複数の多要素認証から選択可能（or条件）
     - 全員が同じ所有物を持たなくてもトータルのカバー率を向上
     - 同強度の認証方式を選択肢に用意することで、セキュリティレベルは維持
       - 例：　tiqr or X509（tiqrがだめでもX509ができればOK）
   - 非常に重要な情報を扱うSPは強固に設定可能（and条件）
     - 例：　tiqr and X509（両方成功しないとNG）

実現したい認証シーケンスの対応状況

3. 認証方式をレベルとして抽象化

Level1：（どのIPからも）ID・パスワード
Level2：（学内IP）ID・パスワード　（学外IP）tiqr
Level3:（どのIPからも）tiqr

- 上記のように同一の認証方式にIPアドレス制限をかけたい場合は、別途認証フローを作成する必要がある
（Level1のID・パスワードと Level2のID・パスワードは別物）

⇒ 学内ユーザはLevel1 でID・パスワード認証を行って、Level2のSPにアクセスすると再度ID・パスワード認証が必要になる

- 対応策として学外用ID・パスワードと学内用ID・パスワードの認証フローをそれぞれ作成

  - 学外用 ID・パスワード
    - Level1
  - 学内用 ID・パスワード
    - Level1-2
  - tiqr
    - Level1-3

MultiFactor認証フローを利用すれば1.2.3いずれも実現可能

tiqr認証

- tiqr
  - SURFnetで開発（オープンソースソフトウェア）
    - スマートフォンのアプリとして実装（iPhone、Androidで利用可）
    - スマートフォン（所有物）とPIN（知識）の多要素認証
    - QRコードを用いてユーザのログイン操作を軽減

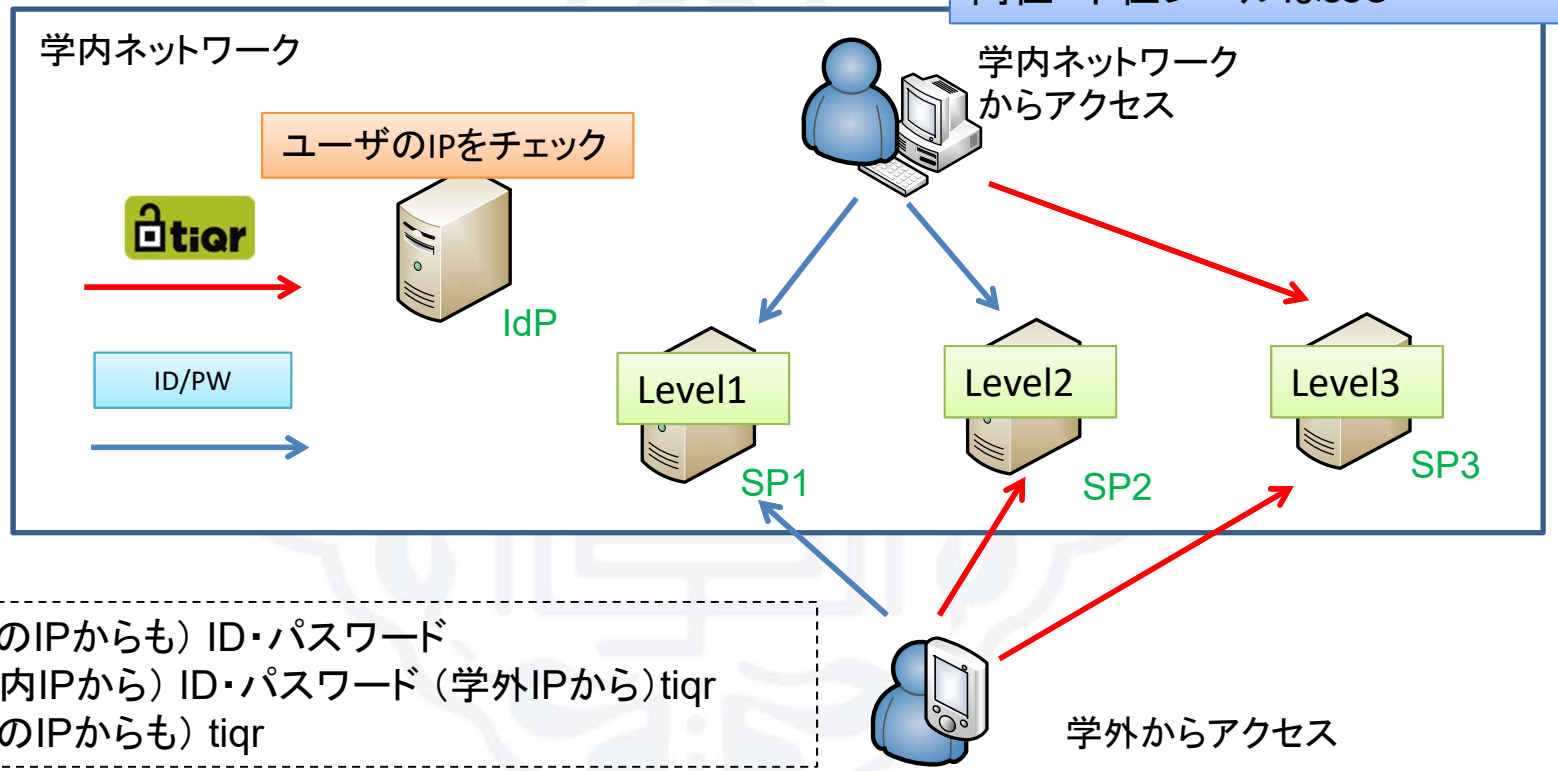
NIIがShibolethでtiqrを利用できるプラグインを提供！

https://meatwiki.nii.ac.jp/confluence/display/tiqr/Home

QRコードをスキャンしてPINを入力するだけ！

KU-SSO更新概念図
（tiqr+MultiFactor認証フロー）

上位レベルで認証に成功した場合、
同位・下位レベルはSSO



Level1：（どのIPからも）ID・パスワード
Level2：（学内IPから）ID・パスワード（学外IPから）tiqr
Level3:（どのIPからも）tiqr

tiqrとMultiFactor認証フローを利用して
本学の多要素認証環境を構築

KANAZAWA UNIVERSITY

Level1、Level2（学内）におけるIdPの挙動

- Level1、Level2（学内）ID・パスワード認証

SPへ
アクセス

サービス
開始

これまでと同様の認証

KANAZAWA UNIVERSITY

Level2（学外）、Level3におけるIdPの挙動

- Level2（学外）、Level3　tiqr認証

SPへアクセス

tiqrを選択

サービス
開始

まとめと今後の課題

- まとめ
  - MultiFactor認証フローを利用することで、本学の多要素認証導入指針を実現可能
  - 金沢大学ではtiqr認証を利用した導入を進めている
    - 重要SPから順次導入予定
- 今後の課題
  - 多要素認証方式を増やし、and/orを使ってより利便性が高くかつセキュアな環境を作っていく

KANAZAWA UNIVERSITY