平成26年度第2回学術情報基盤オープンフォーラム@NII
2015/2/3(Tue)

大学統合認証基盤における多要素認証について

金沢大学　松平　拓也

KANAZAWA UNIVERSITY

金沢大学統合認証基盤

- 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
- KU-SSOの認証方式
  - 金沢大学ID・パスワード認証のみ提供中（2015/2現在）
    - パスワード認証の強度はパスワードの強度に依存
    - そのため、パスワードポリシーは徹底
      - 文字が8文字以上
      - 大文字、小文字、数字、記号のいずれかの2種類以上が含まれること
        などなど
    - 予算執行、給与明細などの重要なSPは学外からの利用不可（VPN）

KANAZAWA UNIVERSITY

ID・パスワード認証の今

- ID・パスワード認証はもう限界？
  - 最近よく聞く言葉 「Password is Dead」
    - 背景には、ID・パスワードに関わるセキュリティインシデントの増加
- IPAによる「オンライン本人認証方式の実態調査報告書」（2014年8月）

  (http://www.ipa.go.jp/security/fy26/reports/ninsho/index.html)
  - オンライン認証における認証方式、インシデント事例、ユーザアンケート等が記載
    - パスワードに対する主な攻撃

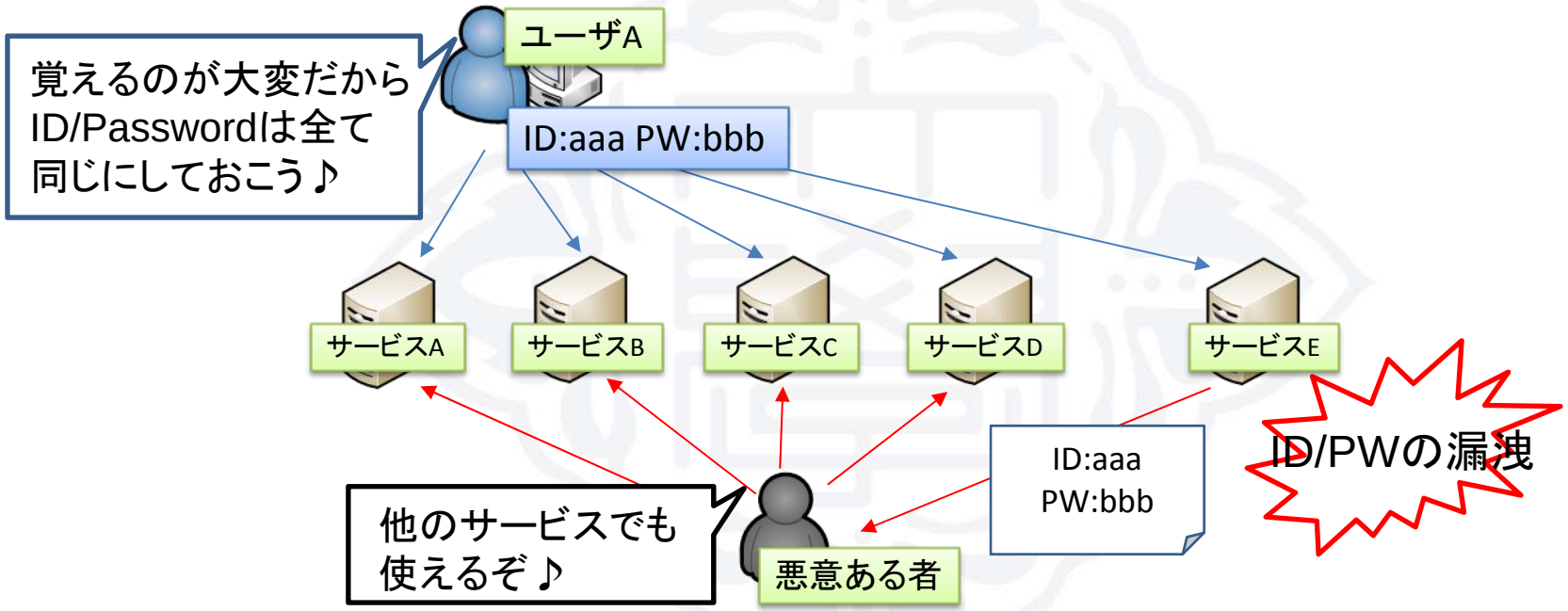
主な脅威	説明
総当り攻撃（ブルートフォース攻撃）	全てのパスワードの組み合わせを試行する攻撃
逆総当り攻撃（リバースブルートフォース攻撃）	パスワードを固定し、IDを変えて攻撃を試みる手口
類推攻撃	利用者の個人情報からパスワードを類推
辞書攻撃	パスワードとして使われていそうな文字列を収録した辞書を用意し、それらを試行

      - 最近はパスワードリスト攻撃が増加！
        - 平成25年 約800,000件（平成24年 114,013件）

パスワードリスト攻撃とは？

- 不正取得したID・パスワードのリストを流用し、連続自動入力プログラムなどを用いてID・パスワードを入力しログインを試行する手口

出典：http://www.ipa.go.jp/security/txt/2013/08outline.html



利用者側で強固なパスワードを設定し、かつパソコン上でセキュリティソフトを利用していても同一のパスワードを使い回している限り、パスワードリスト攻撃の被害を防げない！

多要素認証の定義

- 運用担当者としては早く「多要素認証」に移行したい！
- 認証の定義
  - 認証
    - 利用者が本人であるかどうかを確認する作業
  - 確認するための認証要素（認証の3要素）
    - 本人しか知らない知識（Something You Know）
      - Password、PIN、秘密の質問など
    - 本人しか持っていない所有物（Something You Have）
      - ICカード、スマートフォンなど
    - 本人の生体的特徴（Something You Are）
      - 指紋、静脈、虹彩など（バイオメトリクス）
- 多要素認証
  - 前述の3種類の要素のうち、2要素以上を必要とする認証方式
    - 例：スマートフォンとPIN（所有物＋知識）

KANAZAWA UNIVERSITY

他大学での多要素認証導入状況 -1-

- 複数の大学に対して統合認証関連のヒアリングを実施（H26年度NII共同研究（研究企画会合公募型）の一環）
  - その中の一つとして「多要素認証の導入状況」を調査

1. 佐賀大学
   - ワンタイムパスワード（タイムベース（30分）、8文字の英数字）（LiveSignOn（NTTデータ九州））
     - 携帯電話、スマートフォンなどのメールアドレスへ送付
   - 対象：特定のWebサービスに対しての認証
2. 九州大学
   - マトリクスコード認証（WisePoint（ファルコンシステムコンサルティング））
     - 職員証（ICカード）の裏にマトリクスコードを印刷
   - 対象：特定のWebサービスに対する認証

他大学での多要素認証導入状況 -2-

3. 秋田大学
   - 手のひら静脈認証（PalmSecure（富士通））
     - 新規採用オリエンテーション時に採取
   - 対象：事務用クライアント端末へのログオン
     特定のWebサービスに対する認証
4. 岡山大学
   - ICカード認証（EVE MA（DDS））
     - 職員証（ICカード）＋PINコードによる認証
   - 対象：事務用クライアント端末へのログオン
     特定のWebサービス（一部クラサバ）に対する認証
5. 京都大学
   - ICカード認証
     - 職員証（ICカード）＋クライアント証明書＋PINコードによる認証
   - 対象：特定のWebサービスに対する認証

多くの大学で多要素認証の導入が進んでいる

KANAZAWA UNIVERSITY

金沢大学で導入予定の多要素認証方式

- 2015年中
  - tiqr認証
    - スマートフォン（所有物）+ PIN（知識）
  - YubiKey認証
    - YubiKeyデバイス（所有物）+ ID/パスワード（知識）
- 検討中
  - クライアント証明書認証
    - ICカード（所有物）+ クライアント証明書（所有物）+ PIN（知識）

KANAZAWA UNIVERSITY

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

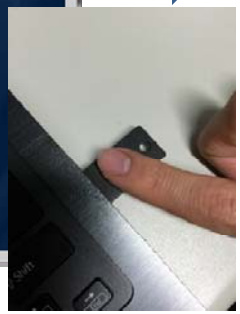
ある学内アンケートでは、新入生の9割以上がスマホを所持
⇒ 大多数のユーザはtiqr認証でカバー可能

KANAZAWA UNIVERSITY

YubiKey認証

- YubiKeyとは？
  - Yubico社が開発したワンタイムパスワード生成デバイス
  - USBキーボードとして動作（OS、ブラウザに依存しない）
  - YubiKeyをタッチするだけ（動作が簡単）
    - タッチすると　ccccccbgjfkivkjtcvujikfbhcrrvgefrhkfrutfndje のようなランダム文字列が入力

SPに
アクセス



サービス
開始

タッチするだけ

tiqrを利用できないユーザ向けの認証方式として提供

KANAZAWA UNIVERSITY

ユーザに対する利便性の問題

- 多要素認証（一般的）
  - ID・パスワード認証より手間がかかる
  - 特定の所有物（tiqrならスマートフォン）がないと認証できない

  ⇒ いきなり全てのSPに対応するのはユーザに対するインパクトが大きい
  （多要素認証を導入したことでユーザに不便になったと思われたくない）

- GUARDプラグインを開発中

  (Gakunin mUlti Authentication mechanism with Risk-based Decision plug-in)
  - NIIと金大で共同研究中のShibbolethにおける認証方式選択プラグイン

KANAZAWA UNIVERSITY

GUARDプラグインの特徴

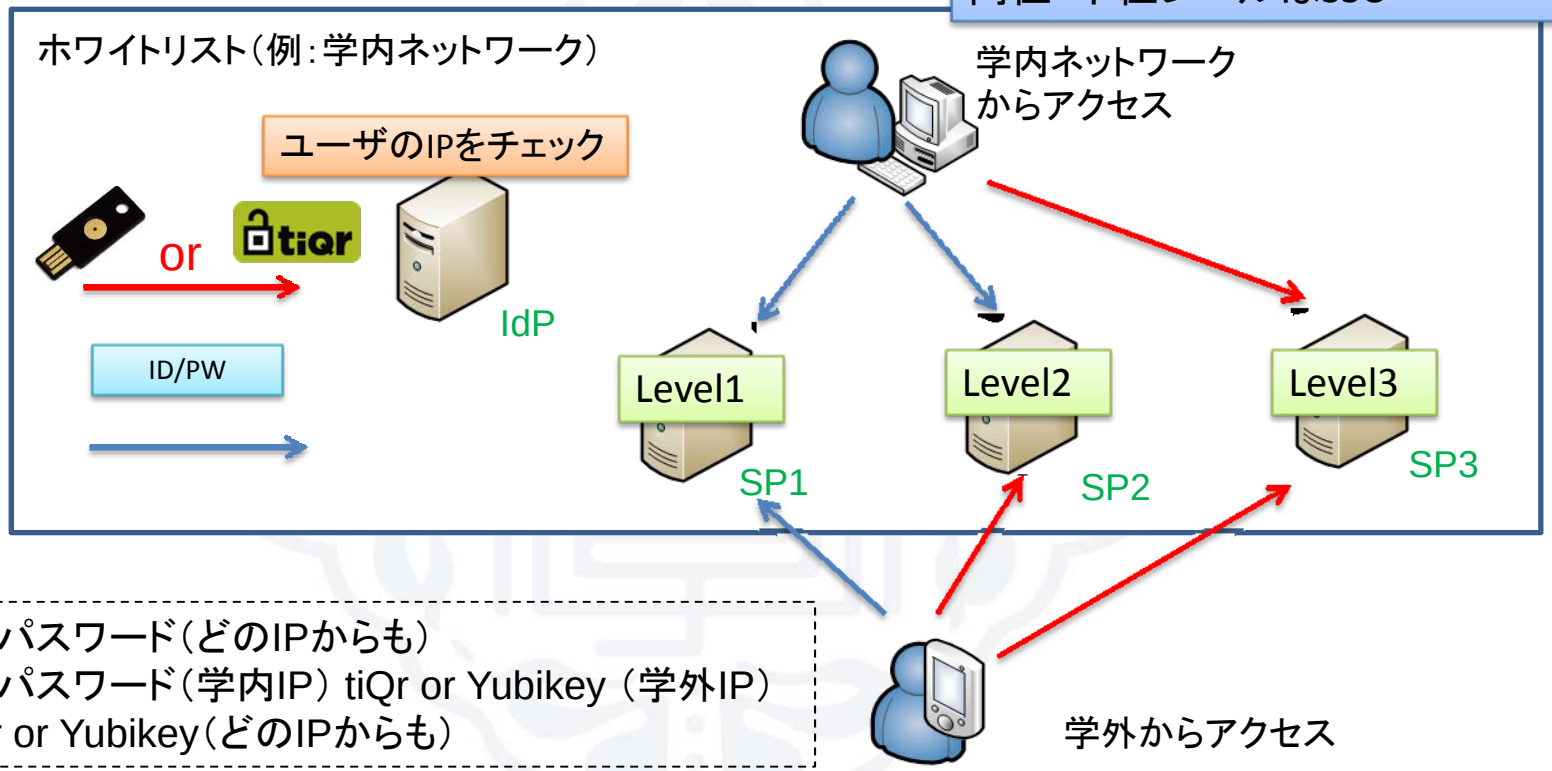
1. ユーザのIPアドレスに応じて要求する認証方式を変更可能
   - 例　学内IP：ID・パスワード認証　学外IP：tiqr認証（リスクベース認証）
2. 複数の認証方式を選択可能（and/or 条件）
   - ユーザが複数の多要素認証から選択可能（or条件）
     - 全員が同じ所有物を持たなくてもトータルのカバー率を向上
     - 同強度の認証方式を選択肢に用意することで、セキュリティレベルは維持
       - 例：　tiqr or YubiKey（tiqrがだめでもYubiKeyができればOK）
   - 非常に重要な情報を扱うSPは強固に設定可能（and条件）
     - 例：　tiqr and YubiKey認証（両方成功しないとNG）
3. 認証方式をレベルとして抽象化（大学の環境に応じて設定変更可能）
   - Level1：ID・パスワード(どのIPからも)
   - Level2：ID・パスワード (学内IPから)　tiqr or YubiKey(学外IPから)
   - Level3：tiqr and YubiKey（どのIPからも）

   ⇒ 重要度に応じてSP群をレベル分けしておけば、あるレベルの認証方式に追加・変更があっても、そのレベルのSPだけに直ちに適用できる（LoAとのすり合わせは検討中）

KU-SSO更新概念図（2015年予定）

（tiqr+YubiKey+GUARDプラグイン）

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：ID・パスワード（どのIPからも）
Level2：ID・パスワード（学内IP）tiQr or Yubikey（学外IP）
Level3：tiQr or Yubikey（どのIPからも）

tiQr+Yubikey+GUARDプラグインの利用により、導入コストをおさえながらも
利用者の利便性を確保できる多要素認証環境を実現

KANAZAWA UNIVERSITY

クライアント証明書による認証

- クライアント証明書とは？
  - 個人（クライアント）に対して発行される電子的な身分証明書
    - 公開鍵暗号方式を利用しており、証明書の偽造は非常に困難
    - 第三者（認証局（CA））が証明書を発行し、証明書の正当性を保証

      ⇒ なりすまし、不正アクセスに対して非常に有効
- 発行形態
  - プライベート認証局（Private CA）
    - 個人や大学（組織）が独自にCAを構築して発行
      - 発行した組織（個人）の限られた環境で有効
  - パブリック認証局(Public CA)
    - ベリサインやグローバルサインなどの企業が運用するCAが発行
      - 発行元を信頼している多くの環境で有効

KANAZAWA UNIVERSITY

クライアント証明書の配布・利用方法

- クライアント証明書のユーザへの配布方法
  - デバイスへ格納
    - 格納するデバイスは本人が既に所持している（かつ本人を特定できる）もの
  - 金大ICカード（職員証・学生証）の利用
    - 入退館、出席管理、生協マネー、証明書発行、図書貸し出しなど、大学での活動に必要不可欠なため、ほとんどの構成員が常に携帯している（もちろん、身分証として携帯は義務）
    - 身分証を簡単に貸したり、紛失したりすることはない
    - 金沢大学のICカードはFelica
      - Felicaでクライアント証明書による認証を行うためのよい方法はないか？

UPKIパス（JCANパス）方式の利用

KANAZAWA UNIVERSITY

UPKIパス（JCANパス）

- JCANパス方式とは？
  - 証明書をサーバに格納させておき、ICカードをリーダにかざした際にクライアントPC上の証明書ストアにインストールする方式
  - JCANパスをNIIが監修して強化　⇒　UPKIパス
- UPKIパス方式のメリット
  - Felicaで利用可能（FCFフォーマットVer.3が必要）
  - 証明書の更新における作業がサーバ側のみ
    - ICカードに格納しておく場合、一度ICカードを回収する必要があるが、UPKIパス方式ではサーバ側の証明書を更新するだけでICカード側は変更する必要なし
    - ICカードを紛失しても、証明書をサーバから削除すればよい
  - ICカードをかざした時だけ証明書がストアされる
    - 共有PCでもクライアント証明書が利用可能

詳細は次の発表で！

KANAZAWA UNIVERSITY

まとめと課題

- まとめ
  - ID・パスワード認証は危険
    - 多要素認証への移行が必須
  - 多くの大学で多要素認証の導入が進んでいる
  - 金沢大学ではtiqr認証、YubiKey認証、UPKIパス（JCANパス）を利用したクライアント証明書認証を導入予定
  - GUARDプラグインを利用し、重要SPから順次多要素認証を導入
- 課題
  - タブレット端末（スマートフォン含む）の対応
    - クライアント証明書が解決のキーになるかも？