平成27年度第1回学術情報基盤オープンフォーラム@NII
2015/6/12(Fri)

大学におけるクライアント証明書利用イメージ

金沢大学　松平　拓也

KANAZAWA UNIVERSITY

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
    - 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

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

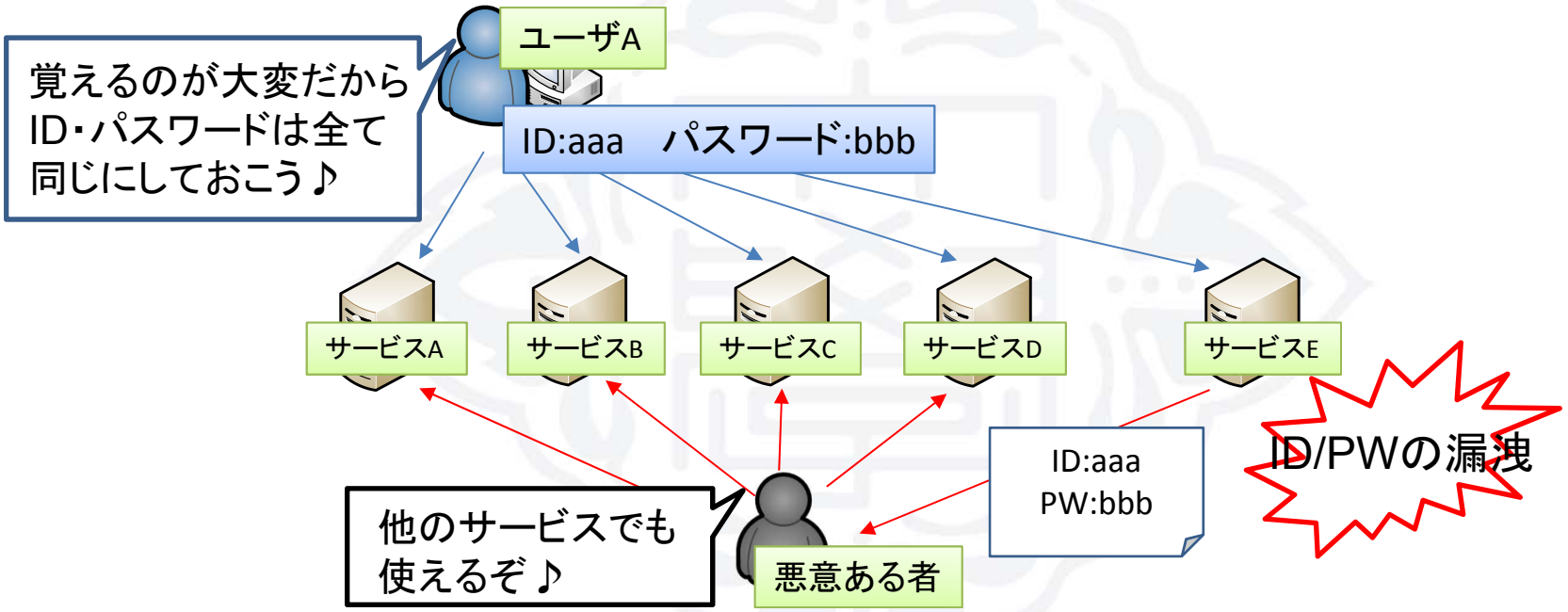
主な脅威	説明
総当り攻撃（ブルートフォース攻撃）	全てのパスワードの組み合わせを試行する攻撃
逆総当り攻撃（リバースブルートフォース攻撃）	パスワードを固定し、IDを変えて攻撃を試みる手口
類推攻撃	利用者の個人情報からパスワードを類推
辞書攻撃	パスワードとして使われていそうな文字列を収録した辞書を用意し、それらを試行

    - 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ID・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！

KU-SSOの多要素認証への移行

- ユーザが金大ID・パスワードをKU-SSO以外のサービスに登録し、そのサービスからID・パスワードが流出した場合
  - KU-SSOがパスワードリスト攻撃の対象となった場合に突破されてしまう

もはやKU-SSOをID・パスワード認証だけで守ることはできない！

多要素認証への移行が必須！

KANAZAWA UNIVERSITY

多要素認証とは？

- 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

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
  - ICカードを用いたクライアント証明書による認証
    - ICカード/クライアント証明書（所有物）+ PIN（知識）

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
      - 発行コストはかからないが、発行した組織（個人）の限られた環境でのみ有効
  - 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
      - 発行コストは高いが、発行元を信頼している多くの環境で有効
      - UPKIを使えば3年は発行コストが無料（その後は？）

KANAZAWA UNIVERSITY

Shibbolethのクライアント証明書認証

- Shibbolethにおけるクライアント証明書認証対応
  - 認証拡張方式
    - Remote User Login Handler
      （REMOTE_USER環境変数にIDを入れる認証実装の場合に利用）
    - 実際の認証処理はApacheが行う
  - 参考URL
    https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=12158431
  - 実装例
    - クライアント証明書を発行する認証局のCA証明書＝Kanazawa-CA.crt
    - クライアント証明書のサブジェクト”O”の値＝”Kanazawa University”
    - クライアント証明書のサブジェクト”CN”の値をuidとして使用

UPKIのクライアント証明書でも動作確認済！

IdPの設定（1）

1. handler.xmlにクライアント証明書認証を用いた認証メソッドの追加

```
<!-- Login Handlers -->
  <ph:LoginHandler xsi:type="ph:RemoteUser">
      <ph:AuthenticationMethod>
        urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient    ← 認証メソッドの追加
    </ph:AuthenticationMethod>
  </ph:LoginHandler>
```

2. Apacheのssl.confにクライアント証明書認証の処理を記載

```
<Location /idp/Authn/RemoteUser>
   SSLCACertificateFile /opt/shibboleth-idp/credentials/Kanazawa-CA.crt ← 認証局のCA証明書
   SSLVerifyClient require  ← クライアント証明書を検証
   SSLVerifyDepth 3
   SSLRequireSSL SSLOptions +ExportCertData +StdEnvVars
   SSLUserName SSL_CLIENT_S_DN_CN  ← “CN”の値を”REMOTE_USER”環境変数にセット
   SSLRequire %{SSL_CLIENT_S_DN_O} eq “Kanazawa University“← “O”の値が”Kanazawa University ”かどうかをチェック
</Location>
```

IdPの設定（2）

3. /TOMCAT_HOME/webapps/idp/WEB-INF/web.xmlにパラメータを追加

```
<!-- Servlet protected by container user for RemoteUser authentication -->
  <servlet>
     <servlet-name>RemoteUserAuthHandler</servlet-name>
     <servlet-class>edu.internet2.middleware.shibboleth.idp.authn.provider.RemoteUserAuthServlet</servlet-class>
     <load-on-startup>3</load-on-startup>
     <init-param>
        <param-name>authnMethod</param-name>
        <param-value>urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient</param-value>
     </init-param>
  </servlet>
  <servlet-mapping>
     <servlet-name>RemoteUserAuthHandler</servlet-name>
     <url-pattern>/Authn/RemoteUser</url-pattern>
  </servlet-mapping>
```

4. relying-party.xmlにデフォルトの認証手段を指定（パスワード認証）

```
<rp:DefaultRelyingParty provider=https://IDP_SERVER/idp/shibboleth
        defaultSigningCredentialRef="IdPCredential"
        defaultAuthenticationMethod="urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport">
```

SPの設定

1. IdPに対して認証方式の指定

shibboleth2.xml

```
<SessionInitiator type="Chaining" Location="/Login" isDefault="true" id="Intranet“
        authnContextClassRef="urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient"
          relayState="cookie" entityID="https://IdPserver/idp/shibboleth">
          <SessionInitiator type="SAML2" acsIndex="1" template="bindingTemplate.html"/>
          <SessionInitiator type="Shib1" acsIndex="5"/>
</SessionInitiator>
```

または、shib.conf

```
<Location /secure>
  AuthType shibboleth
  ShibCompatWith24 On
  ShibRequestSetting requireSession 1
  ShibRequestSetting authnContextClassRef urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient
  require shib-session
</Location>
```

Shibbolethでは特に複雑な設定を行う必要なし！

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・利用方法
  1. ユーザがWebから取得
     - ID/PW認証（学内限定）を行い、自分のクライアント証明書を取得
       - 利用者がクライアント証明書を雑に扱う危険性
       - NIIのクライアント証明書発行システムがそのような運用に対応していない（管理者が申請する必要）
  2. デバイスへ格納して配布
     - 利用者がクライアント証明書を雑に扱う危険性の排除
     - 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

       ⇒ ICカード（職員証・学生証）の利用が最適！
       - 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
       - 身分証を簡単に貸したり、紛失したりすることはない

ICカードでのクライアント証明書運用事例（1）

- 京都大学
  - 非接触（Felica）+接触のハイブリッドICカード
    - 接触部分にクライアント証明書を格納
  - 2010年度から導入
    - 導入時
      - 常勤教職員（約6,500名）にIC職員証
      - 非常勤教職員等（約5,500名）に認証IC カード

        ※2012年度からIC職員証は認証ICカードとして発行（IC職員証廃止）
  - Private CAで発行（更新作業が発生しないよう長い有効期間が必要なため）

    ※有効期間10年(2020年)、今年度から毎年5年設定とし、一斉変更問題を回避

ICカードでのクライアント証明書運用事例(2)

- 北陸先端科学技術大学院大学(JAIST)
  - 非接触(Felica)+接触のデュアルインターフェースICカード
    - クロスアクセス(非接触インターフェースから接触の領域を参照)可能
    - 接触部分にクライアント証明書を格納
  - 2008年から教職員・学生(約2,000人)に配布
  - Private CAで発行(身分に応じて柔軟に有効期限を変更するため)

- 名古屋工業大学
  - 非接触(Felica)+接触のハイブリッドICカード
    - 接触部分にクライアント証明書を格納
  - 2007年度末から教職員・学生(10,000人程度)に配布
  - Private CAで発行(長い有効期間が必要なため、発行コストが無料)
    ※職員は約15年

ICカードでの運用における課題

- ハイブリッドICカード自体のコストが高い
  - デュアルインターフェースICカードはさらに割高
- 接触型のICカードリーダライタが必要
  - 非接触側からクライアント証明書を読むと通信に時間がかかる
  - 入退館や出席管理は接触型では不便（用途に応じて使い分ける必要）
- ICカード内情報に変更があった際はカードを回収・再配布する必要
  - クライアント証明書の期限切れ、S/MIMEでメールアドレスが変更になった場合などはカード情報の書き換え作業が必要
- Private CAは厳格に運用するとコストが高い
  - 有効期限の長い証明書を発行したり、証明書の発行コストをなくすためにPrivate CAでの運用になるが、厳格に運用するとコストが高い

最近の大学におけるICカード導入状況

- 金沢大学も職員証・学生証はICカード
  - 入退館、出席管理、生協マネー、証明書発行など、大学での活動に必要不可欠
  - 金沢大学のICカードはFelica（FCFフォーマット）
  - FCFフォーマット
    - 一般社団法人FCF推進フォーラムで提唱
      - 大学等教育機関181機関で導入（2014/11）
        （教育機関におけるICカードのデファクトスタンダード）
  - Felica（FCFフォーマット）の特徴
    - カード自体は安価、カードリーダも一般的なものでOK
    - 多くのアプリケーションが対応
    - クライアント証明書のような大きなデータは格納できない

金沢大学を含む多くの大学でICカードによるクライアント証明書認証を行うには？

UPKIパス（JCANパス）方式の利用

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に一時的にダウンロード/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
  1. Felicaで利用可能（FCFフォーマットVer.3が必要）
  2. 証明書の更新における作業がサーバ側のみ
     - 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

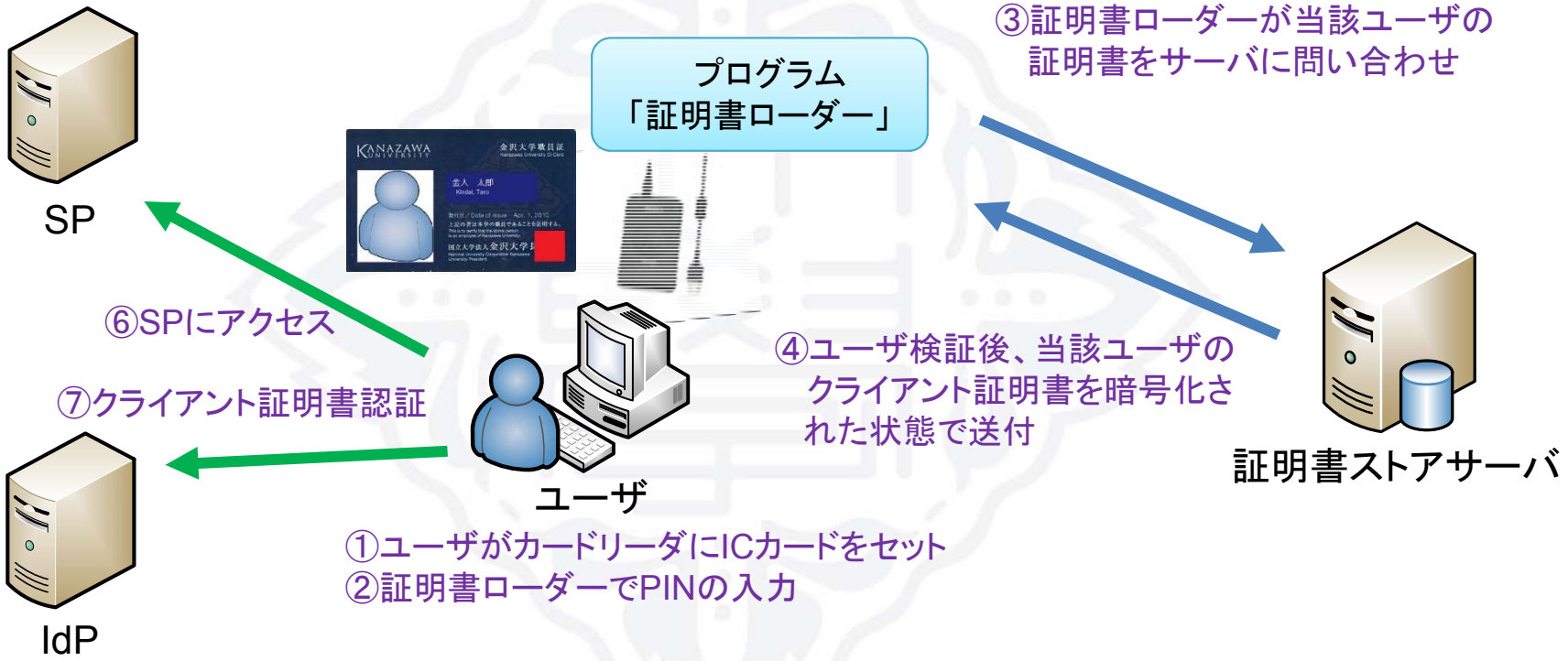
       ⇒　カードを回収して再配布する必要がない
  3. Public CAによる運用が容易になる
     - 証明書が書き換えになってもカードの回収が必要なくなる

       ⇒ Public CAで発行される（ある程度期限の短い）証明書での運用でもよくなる（UPKI証明書なら発行コスト問題も解決）

UPKIパスの利用イメージ

詳細は次の発表で！

⑤ICカード内に格納されている解凍パスフレーズにより復号化し、クライアント証明書をOS標準の証明書ストアに格納



ユーザはICカードをかざして、PINを入力するだけ！

KANAZAWA UNIVERSITY

各認証方式のターゲット

tiqr認証

・学生（主）・教職員
　※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
・ノートPC

YubiKey認証

・スマホ、ICカードを持っていないユーザ
・出張先でKU-SSOを（頻繁に）利用するユーザ
　⇒ tiqr認証とICカード認証を補う役割

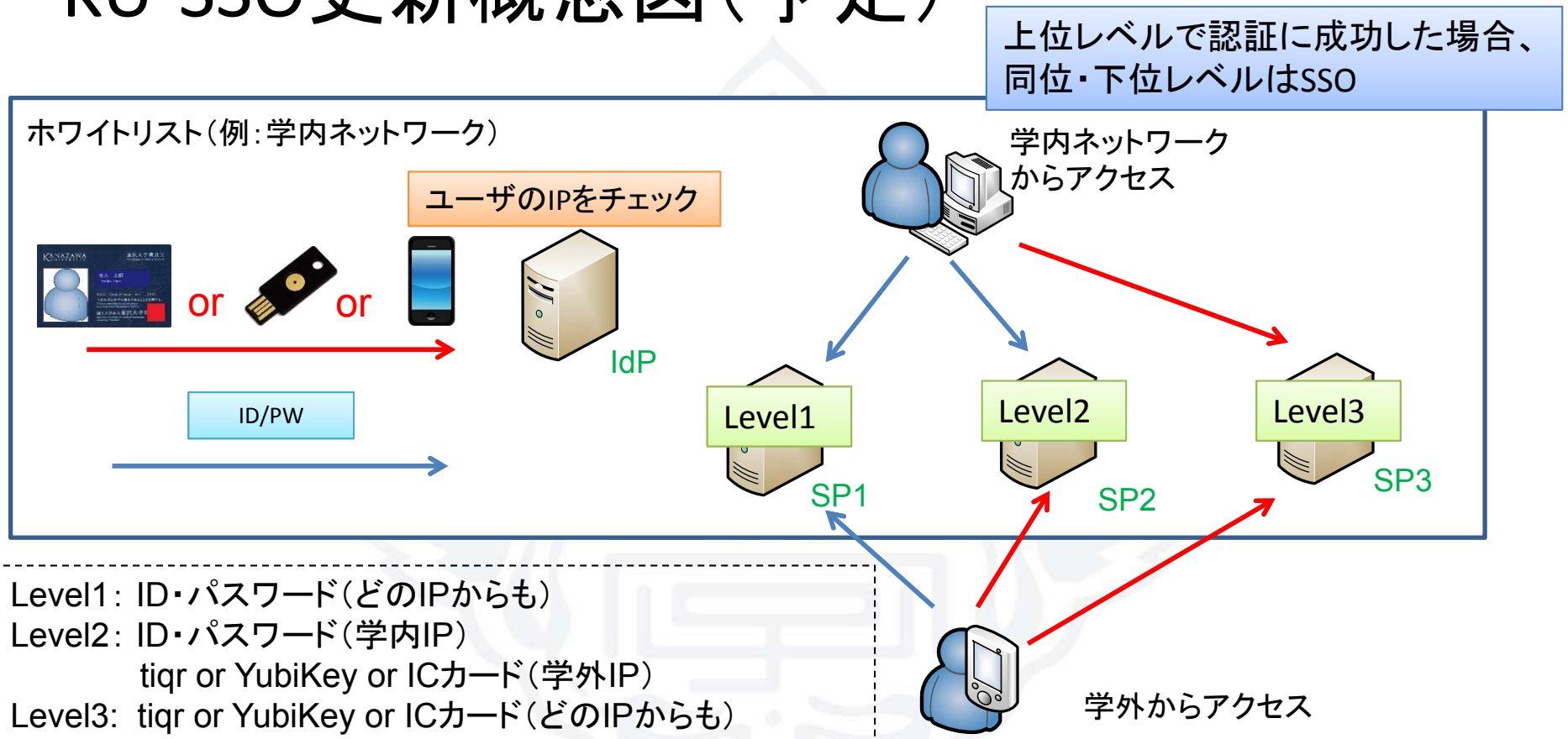
ICカード認証

・教職員（主）・学生
・デスクトップPC

KU-SSOを利用する全てのユーザが多要素認証できる環境を構築

KANAZAWA UNIVERSITY

KU-SSO更新概念図（予定）



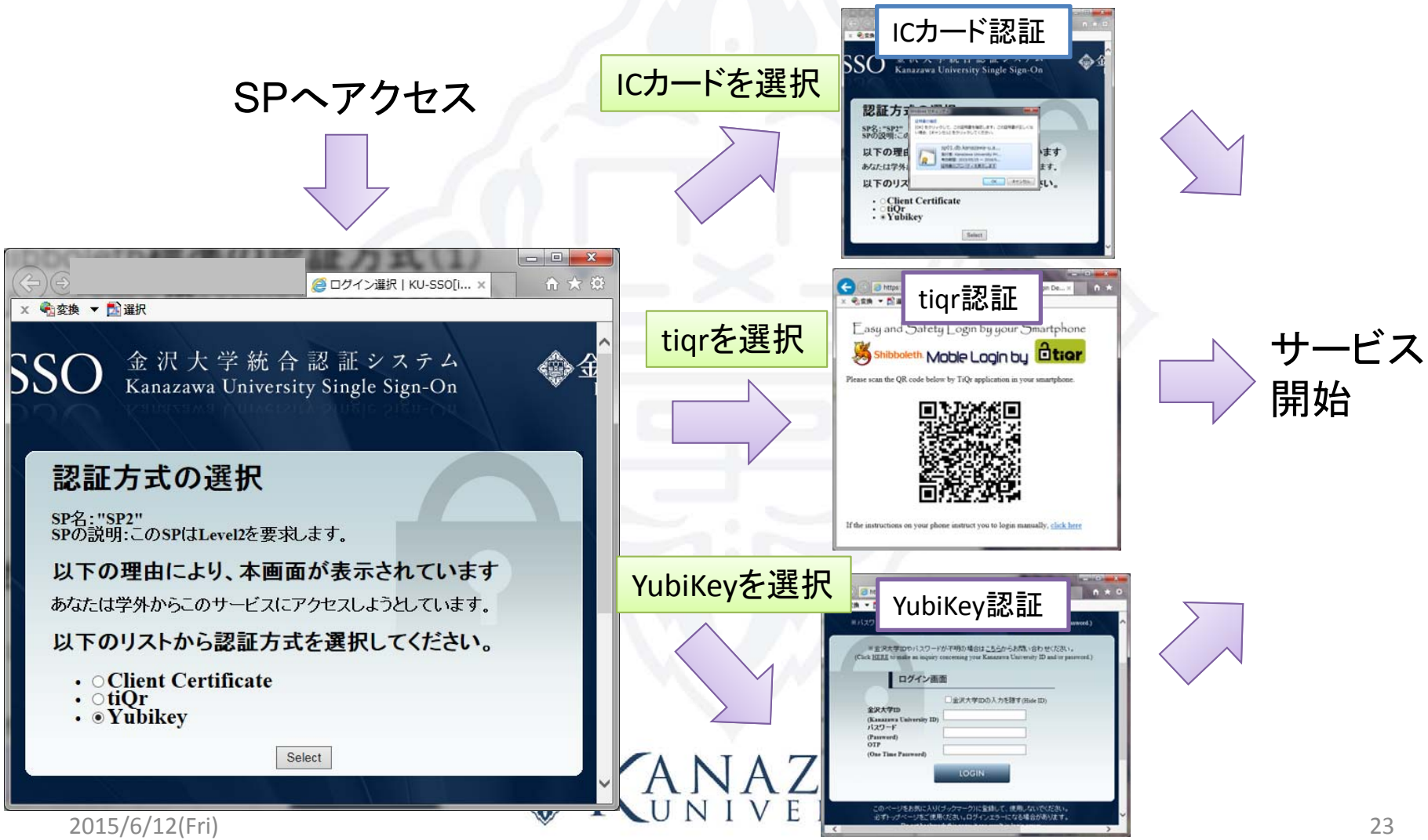
Level1：ID・パスワード（どのIPからも）
Level2：ID・パスワード（学内IP）
　　tiqr or YubiKey or ICカード（学外IP）
Level3：tiqr or YubiKey or ICカード（どのIPからも）

- GUARDプラグインの利用
  - ユーザは自分に合った認証方式を選択可能
  - サービスの重要度に応じて認証レベルを変更可能

KANAZAWA UNIVERSITY

Level2（学外）、Level3におけるIdPの挙動

- Level2（学外）、Level3　ICカード認証 or tiqr認証 or YubiKey認証



まとめと要望

- 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
  - Shibbolethではクライアント証明書認証が実装可能
  - UPKIパスにより、Felicaでのクライアント証明書認証が実現可能
  - 金大では多要素認証方式としてtiqr認証、YubiKey認証、UPKIパスを利用したクライアント証明書認証を導入予定
- 要望
  - クライアント証明書は3年後も安く提供してほしい
  - もっと証明書の有効期間を長く設定できるようにしてほしい