uApprove.jpをインストールする（にいたるまで）

豊橋技術科学大学における認証統合の事例紹介

豊橋技術科学大学情報メディア基盤センター　土屋雅稔

豊橋技術科学大学

- 愛知県豊橋市
- 1976年開学
- 工学部のみの単科大学
- 教職員333人，学生2166人
- 高等専門学校（5年制）卒業生を，学部3年次に編入し，大学院卒業まで4年間の教育を行う，という方針でカリキュラム設定されている

認証統合への道程

- 2005年度まで認証統合はまったく行われていなかった.
  - 教務システム，情報処理センター端末室，マルチメディアセンター端末室，語学センター端末室，どれもユーザ名とパスワードが違っていた.
  - そもそも全学生と全教職員を対象としてアカウントを発行する体制になっていなかった.
- 認証統合を実現するには，メリットをうまく伝える必要がある.
  - アカウントが別々だと不便でしょ？ →それが当たり前だと思っている人には伝わらない.
  - 情報メディア基盤センターのアカウントってそれ何？ →新たに覚えないといけないなんて面倒だよ.
  - 認証統合のためにお金がかかる？ →それは困るよ.

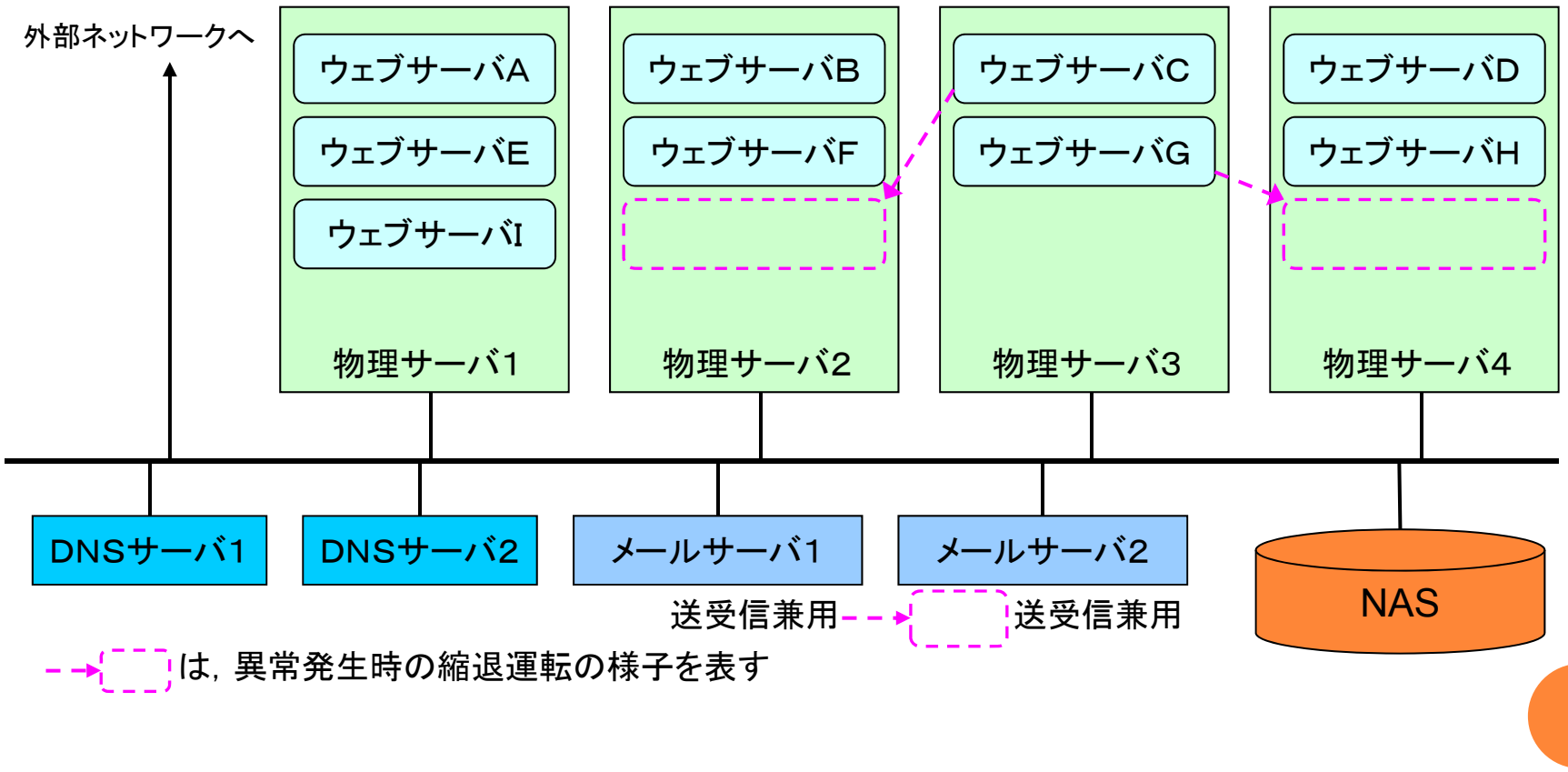
認証統合の経過（1）

- 情報処理センター演習用システムとマルチメディアセンターマルチメディア教室の認証統合：2006年4月
  - SambaとLDAPサーバを組み合わせたシステムを構築．このLDAPサーバを足掛かりに小規模スタート
- 全学生にアカウントを配布：2006年9月
- ホスティングサービス開始：2007年10月
- 講義棟無線LAN用パスワードの統合：2008年5月
- WebCT用パスワードの統合: 2009年4月
- 語学センターの認証統合: 2009年4月
- メール転送サービス（xxx@tut.jp）の提供：2009年9月
- 教務システムの認証統合: 2010年4月
- 情報知能工学系実験室の認証統合: 2010年4月

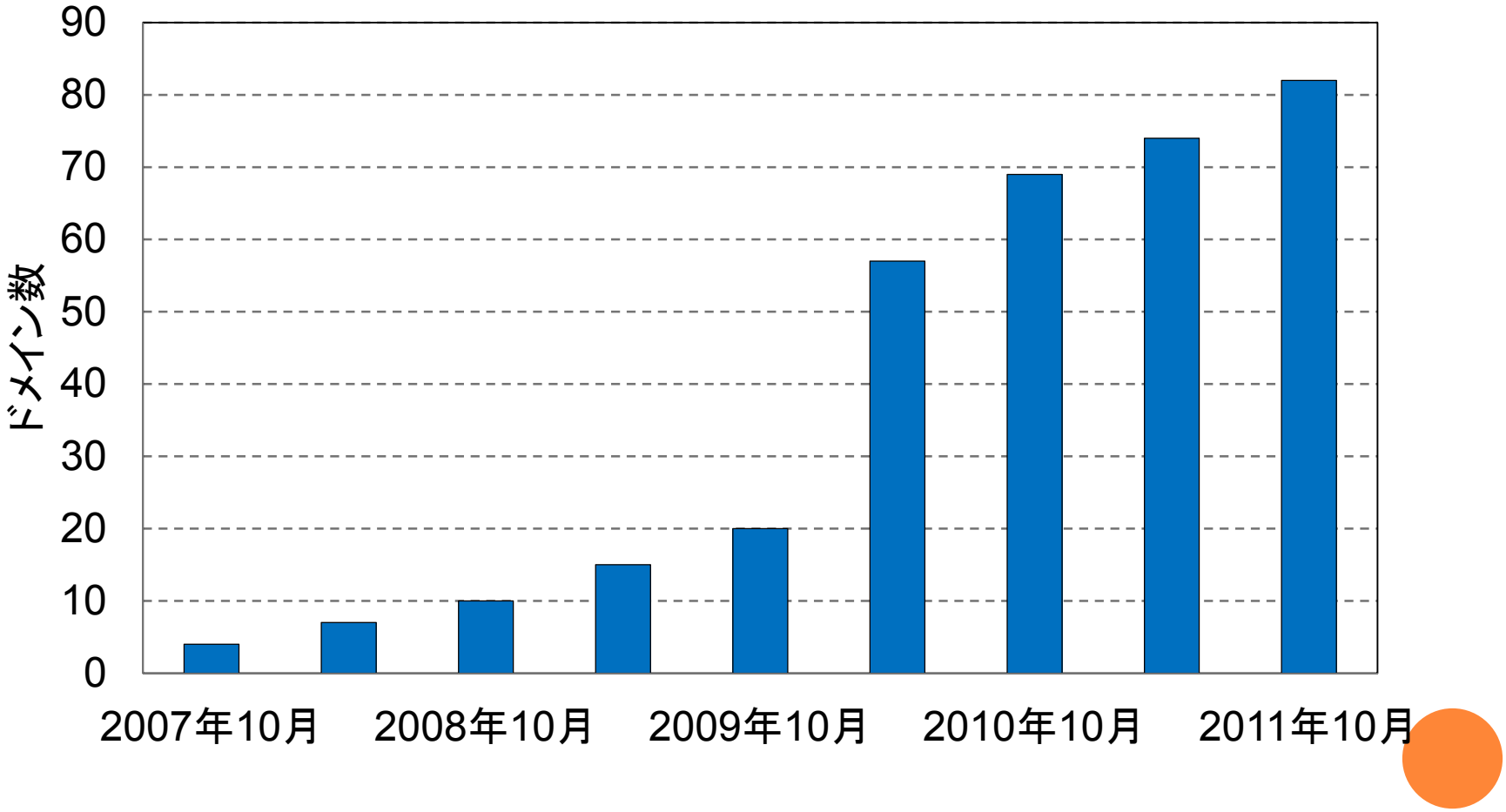
ホスティングサービス

- 研究室や部局のサーバは，専門外の職員や学生によってメンテナンスされている場合が多い．
  →技術的に未熟でセキュリティリスクが高い．
- ホスティングサービスの提供が必要
- 豊橋技術科学大学のサービス状況
  - ウェブサーバホスティング
    - ドメイン毎に仮想マシン（コンテナ）を割り当て．
    - 仮想マシンのコンテンツ領域のメンテナンスは，利用組織側が対応．WebDAVで編集．
  - メールサーバホスティング
    - Postfix の仮想ドメイン機能を使って実現．
  - DNSサーバホスティング
    - rndcコマンドを呼び出すCGIを用意．
    - 利用組織の管理者は，WebDAVでゾーンファイルを書き換え
      →CGIを使って再読み込みを依頼．

ホスティングサービスのサーバ構成



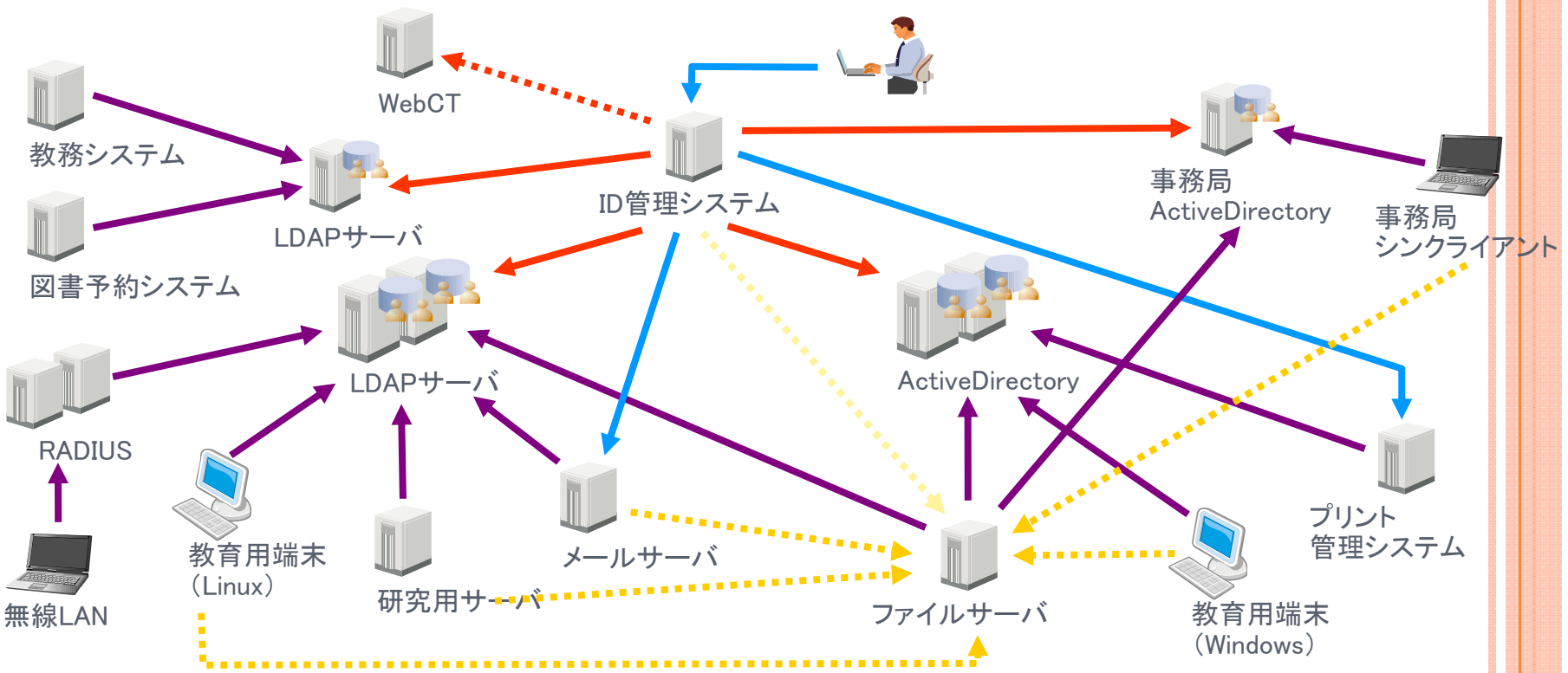
ホスティングサービスの利用ドメイン数推移



認証統合の経過(2)

- 学科再編:2010年4月
  - 各学科毎に独立していたメールサーバ・ウェブサーバを情報メディア基盤センターのホスティングサービスで巻き取ることに成功.
  - この時点で，全教職員が情報メディア基盤センターのアカウントを日常的に利用するようになった.
- 新教育研究用システムの稼働:2010年10月
  - SambaとLDAPサーバを，Sun Java Identity Manager, Sun Java Directory Server, Microsoft Active Directory を組み合わせたシステムでリプレース.
- Shibboleth IdP 設置と学認テストフェデレーション参加:2011年6月

認証統合の状況(2010年10月)



- 全ての教育用端末・メールサーバ・無線LANが，同一ユーザ名・パスワードで利用できる.
- 全ての教育用端末で，同じホームディレクトリが使える.
- 教育用システムと事務局システムの認証基盤を統合.

アカウント発行時に考慮が必要になること

- 名寄せをどうする？
  - 学生：教務システムによる登録．一意の学籍番号．
  - 教職員：人事システムによる登録．一意の職員番号．
  - 大学には，番号が付番されない利用者が多数存在する．
    - 産学連携研究員，派遣職員，アルバイトなどなど．
    - 教職員が身元引受人として申請．使い捨ての番号を付与．
- 複数の役割を持つ利用者はどうする？
  - 例えば，博士後期課程在籍中の助手はどうするか．
  - アカウントを2つ出す．
- 組織単位のアカウントはどうする？
  - 例えば，教務委員が共用している教務システムのアカウント（シラバス・成績書き換えに使っており，ユーザのロールとも関連付けられている）をどうするか．
  - 人間に紐付けられているアカウントのみ受け付ける．組織単位のアカウントがどうしても必要な場合は，システム側でローカルにアカウントを作成してもらう．

認証統合からSSOへ

- LDAPを核とする認証統合は，順調に進展.
- このままではアカウント情報を入力する回数は減らせない.
  単純な認証統合から Single Sign On に目標を展開.
- SSO を実現するミドルウェアとして何を使う？
  - IceWall
  - CAS
  - Shibboleth ←学認で使っていることが選定の決め手.
- 2011年6月作業開始
- 学内SPの例
  - 情報メディア基盤センターwiki
  - セキュリティポリシー遵守状況調査システム
  - 公文書公開システム
  - 高圧ボンベ庫管理システム
  - 学内限定ウェブページの学外からのアクセス制御

SHIBBOLETH IDP 設置にあたって考えたこと

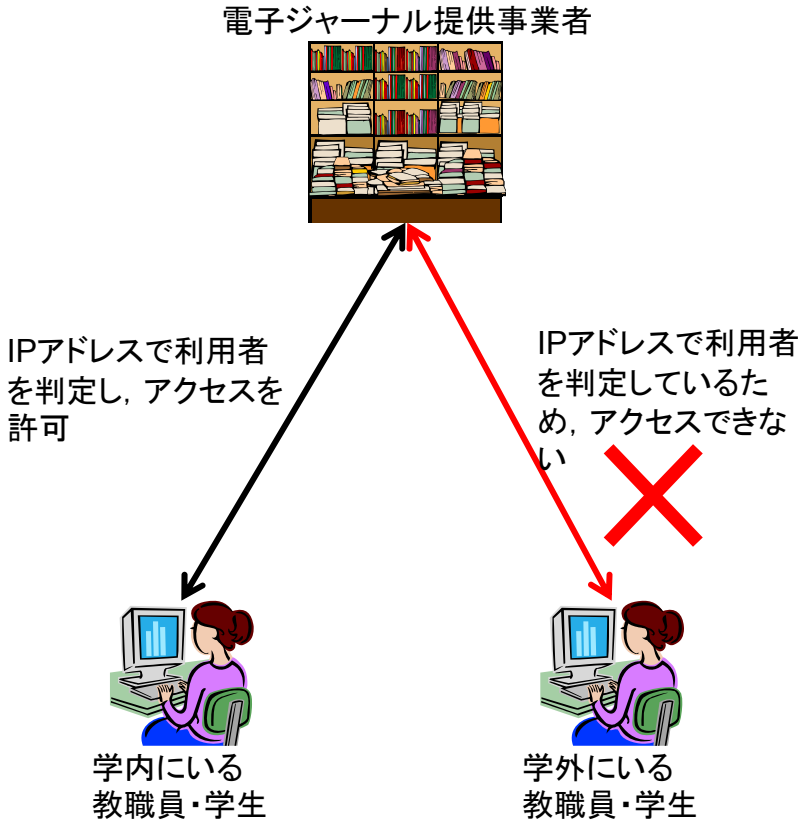
- 長期運用をどうやって乗り切るか?
  - セキュリティフィックスを継続的に適用する必要がある. IdPの更新が必要になる場合も.
  - 対応方法
    - Debian GNU/Linux の安定版を採用.
    - IdP を Debian パッケージ化. 更新手順を明文化.
- 可用性をどうやって確保するか?
  - 本来なら, IdPの冗長化で対応するべき. https://meatwiki.nii.ac.jp/confluence/display/GakuNinShare/IdPClustering
  - 実装の容易さを優先. 単純に物理サーバを2台用意し, Heartbeat でサービス用IPを取り合うように設定.

学内フェデレーションの運用の注意点

- IdPのログイン画面のローカライズ
  - 留学生が増加しており，各種情報サービス（含むIdP）のローカライズは重要な課題．
  - Java Servlet の国際化は，技術的には2通りの方法がある．
    - java.util.ResourceBundle というプリミティブな関数を使う
    - Java Standard Tag Library (JSTL) を使う
      - https://www.gakunin.jp/ml-archives/upki-fed/msg00477.html
- メタデータの配布方法
  - IdPの証明書を更新する場合，更新したメタデータを全ての学内SPにインストールする必要がある．
  - 学内SPが少ない間はともかく，学内SPが増えてくると，配布方法の自動化が必要．
  - 署名したメタデータを HTTP でダウンロードできるようにすればよい．意外と簡単．
    - https://www.gakunin.jp/ml-archives/upki-fed/msg00463.html

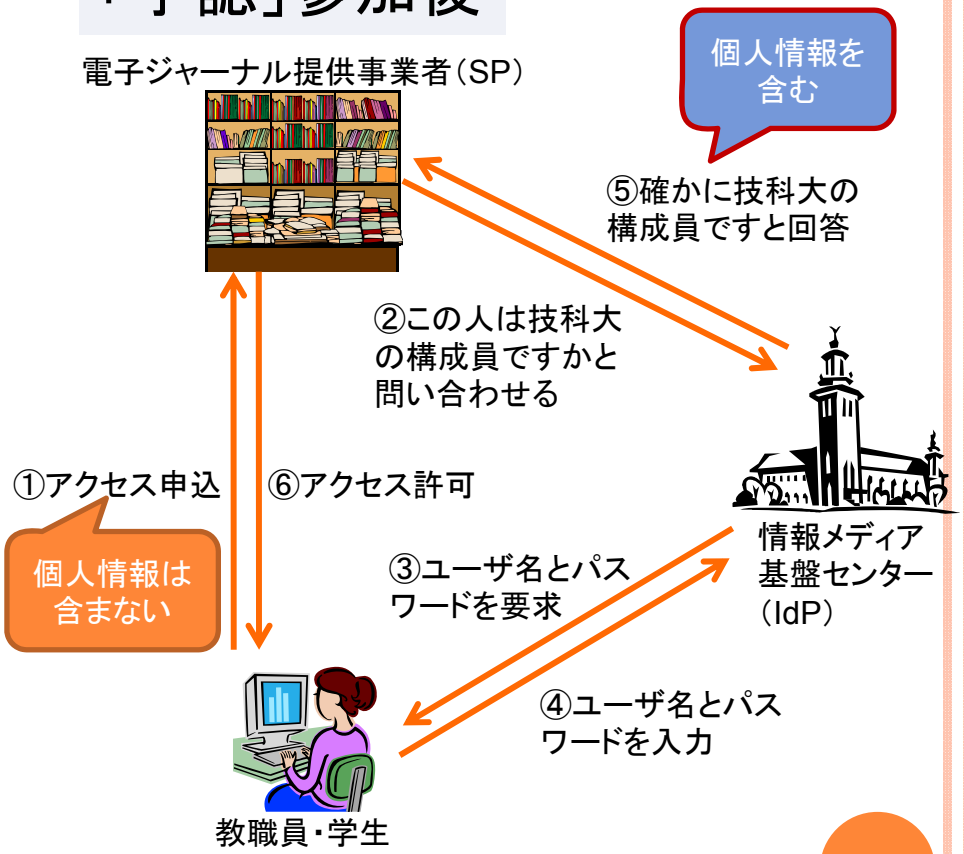
学認参加による個人情報の第3者への送信

「学認」参加前



出張中や在宅時にはアクセスできず，大変不便！

「学認」参加後



出張中や在宅時でも，学内と同様にアクセス可能

eduPersonTargetedID が問題

- サービス提供者（前ページの例では，電子ジャーナル提供事業者）は，「技科大の構成員である」という情報だけでなく，構成員を区別する情報が必要．
  - 例えば，過去に閲覧した論文のリストを保存しておいて，関連文献を推薦するなどのサービスを提供するためには，構成員を区別しておく必要がある．
- 学内のサービスでは，学籍番号や職員番号を使うことができるが，学外のサービス提供者に対しては提供できない．
- そこで，学籍番号や職員番号を，1方向ハッシュ関数により暗号化してから送信する．
  - 学外のサービス提供者は，学籍番号や職員番号を取り出すことはできない．同じユーザがアクセスしてきたということが分かるだけ．
  - サービス提供者毎に異なる暗号化を行う．そのため，複数のサービス提供者が結託しても，サービス間で利用者を特定することはできない．
- 上記のように暗号化された番号であっても，「独立行政法人等の保有する個人情報保護に関する法律」が定める個人情報に該当する可能性がある．
- eduPersenTargetedId が送信できないと，学認参加の SP はほぼ全滅．

独立行政法人等の保有する個人情報の保護に関する法律

- 第4条（利用目的の明示）
  - （略）当該本人の個人情報を取得するときは、次に掲げる場合を除き、あらかじめ、**本人に対し、その利用目的を明示しなければならない**。
- 第9条（利用及び提供の制限）
  - 独立行政法人等は、法令に基づく場合を除き、利用目的以外の目的のために保有個人情報を自ら利用し、又は提供してはならない。
  - 二　前項の規定にかかわらず、独立行政法人等は、次の各号のいずれかに該当すると認めるときは、利用目的以外の目的のために保有個人情報を自ら利用し、又は提供することができる。
    - 一　**本人の同意があるとき**、又は本人に提供するとき。
    - 二　独立行政法人等が法令の定める業務の遂行に必要な限度で保有個人情報を内部で利用する場合であって、当該保有個人情報を利用することについて相当な理由のあるとき。
    - 三　行政機関（行政機関の保有する個人情報の保護に関する法律（平成十五年法律第五十八号。以下「行政機関個人情報保護法」という。）第二条第一項に規定する行政機関をいう。以下同じ。）、他の独立行政法人等、地方公共団体又は地方独立行政法人に保有個人情報を提供する場合において、保有個人情報の提供を受ける者が、法令の定める事務又は業務の遂行に必要な限度で提供に係る個人情報を利用し、かつ、当該個人情報を利用することについて相当な理由のあるとき。
    - 四　前三号に掲げる場合のほか、専ら統計の作成又は学術研究の目的のために保有個人情報を提供するとき、本人以外の者に提供することが明らかに本人の利益になるとき、その他保有個人情報を提供することについて特別の理由のあるとき。

UAPPROVE.JP がなぜ必要か?

- 法第9条第2項第1号の規定「本人の同意があるとき」を満たすため.
- IdPのログインページに「第3者送信をすることがあります」「ログインした場合は承諾と見なします」と書くことで対応できるか?
  - 実際に裁判をしてみるまで分からない.
  - 特に, 学内システム向けの IdP が同居している場合には, 以下のようなフローが有り得るから, 明示的な同意と見なされない可能性がある.
    1. 学内SPにログイン
    2. 学外SPにログイン
       - この時, IdPのログインページが表示されない.

個人情報の保護に関する法律

- 第二十三条（利用及び提供の制限）
  - 個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。（略）
  - ２　個人情報取扱事業者は、第三者に提供される個人データについて、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。
    - 一　第三者への提供を利用目的とすること。
    - 二　第三者に提供される個人データの項目
    - 三　第三者への提供の手段又は方法
    - 四　本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。
  - ３　個人情報取扱事業者は、前項第二号又は第三号に掲げる事項を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置かなければならない。
  - （略）
- 私立大学は法第２３条２項の規定（オプトアウト）で対応できる？

学内規則との関係

- 国立大学法人豊橋技術科学大学個人情報管理規定
  - 第37条（保有個人情報の提供）
    - 保護管理者は，法第9条第2項第3号又は第4号の規定に基づき行政機関及び独立行政法人等以外の者に保有個人情報を提供する場合には，原則として，提供先における利用目的，利用する業務の根拠法令，利用する記録範囲及び記録項目，利用形態等について書面を取り交わすものとする。
- 法第9条第2項第1号に関する学内規則は存在しなかった
  - とりあえず学認には参加できそう.
  - 個人情報保護委員会で承認済み

uApprove.jp をインストールする

- （ほぼ）ドキュメントの通り
  - https://www.gakunin.jp/docs/files/uApprove.jp-installation_ja.html
  - IdP の Debian パッケージに同梱した.
- はまったポイント
  - uApprove.jp から MySQLにアクセスできない.

```
CREATE USER 'uApprove'@'localhost' IDENTIFIED BY 'uApprove';
GRANT USAGE ON *.* TO 'uApprove'@'localhost';
GRANT SELECT , INSERT , UPDATE , DELETE ON `uApprove`.* TO
'uApprove'@'localhost';
```

    - 冗長化のため，DRBD上にMySQLデータベースを置き，MySQLを heartbeat で管理，接続には 133.15.xxx.yyy と IP アドレスを使う指定にしてあったため.
  - 本人による同意の取り消しの設定
  - Apacheをフロントエンドに使っている場合，Tomcatに認証情報を渡す必要がある

本人による同意の取り消し

- In-flow モードと Standalone モードという2つのモードがある
- 学内システム向けと学認向けIdPが同居している場合，In-flow モードは使いにくい
  - In-flowモードでは，IdP のログイン画面にリンクを用意して，ログイン時に同意の取り消しを選べるようにしておく.
  - 学内システム向けと学認向けIdPが同居している場合，以下のようなフローが有り得るから，利用者側から見ると，どのようにすれば同意が取り消せるのか良く分からない
    1. 学内SPにログイン
       - ここで同意を取り消すボタンをクリックしておいても，同意を取り消すページに遷移しない.
    2. 学外SPにログイン
       - IdPログインページに遷移しないし，同意を取り消すページにも遷移しない.
- Standaloneモードを用意.
  - インストールマニュアルでは，standalone_next_url とアンダースコアになっているが，正しくは standalone-next-url とハイフンである. UTSL.

APACHEからTOMCATに認証情報を渡す

- Apache をフロントエンドに使っている場合に限定.
- Tomcat はデフォルトでは，Apache 上の認証情報を受け取らない．そのため，uApprove.jp は以下のエラーを表示する.

  Username is not set, can't reset attribute release approval

- 以下の設定が必要になる.

  <Connector port=“8009” protocol=“AJP/1.3” redirectPort=“8443”
  tomcatAuthentication="false" />

今後の予定

- 学認フェデレーション本参加
  - uApprove.jp もインストールできたので，これで進められるはず．
  - 2012年12月に参加が認められた．設定変更作業中．
- 多要素認証の導入
- OpenID の対応
  - Shibboleth は，SP の情報を IdP に登録する必要がある．
  - そのため，研究室単位のカジュアルなアプリケーションには敷居が高い．また，Shibboleth に対応していないアプリケーションも多い．
  - OpenID に対応して，センターへの申し込みなしに認証連携できるようにできないか？