

よりよいeリソース 利用環境整備のために

北海道大学附属図書館

野中雄司

平成21年度 国立情報学研究所情報処理軽井沢セミナー

内容

- **北海道大学認証基盤現況**
 - 認証基盤
 - シングルサインオン（縦横）
 - 望むこと
 - ユーザ管理
 - 認証
- **北海道大学eリソースアクセス環境の現状と今後の希望**
 - 現況
 - やりたいこと
 - 個人認証シングルサインオン
 - リモートアクセス
- **実現のために**

- **北海道大学認証基盤現況**

- 認証基盤
- シングルサインオン（縦横）
- 望むこと
 - ユーザ管理
 - 認証

- 北海道大学eリソースアクセス環境の現状と今後の希望

- 現況
- やりたいこと
 - 個人認証シングルサインオン
 - リモートアクセス

- 実現のために

認証基盤現況

- 全構成員（学生教職員）を統合したデータベースなし。
- **=全学統合認証基盤なし（全学生教職員のユニークIDはなし）**
 - 全学統合認証基盤については未定

シングルサインオン現況

- SSOシステムあり（**教職員のみ**） H20-
 - 基本**各業務系システム**のSSO（ログインしたら各システムへのメニューが表示される。ポータルの）→横のシングルサインオン
 - リバースプロキシタイプ
 - 学生は投入予定なし。
 - 教育情報システムが既に学生にとってのポータル（こちらは基本学部生のみ）
 - 原則学外からアクセスできない。
 - ユーザ情報はSSOシステム用のIDとパスワードを持っているだけ。
 - **属性情報は持っていない**

認証基盤に対して望むこと

<ユーザ管理>

- 現在図書館システムでユーザ情報保持
- 図書館で提供しているサービス（本の貸出からパスワード認証が必要なオンラインサービスまで）は、すべてこの独自ユーザ情報でサービスを行っている。

・大学内で多重ユーザ管理になっており無駄
・やっぱりユーザ情報の維持管理は大変

- 利用者（個人）情報は保持したくない
 - パスワード認証しない例えば貸出時の照合とかも。特に在籍管理はしたくない。
- 大学で図書館から参照可能な全構成員のデータベースを保持してくれているとうれしい

認証基盤に対して望むこと

<認証>

- **全構成員のデータベースだけではなく、当然そのデータベースを基にした認証基盤もほしい**
 - 各種図書館サービスで使いたい
 - 従来のサービス（貸出状況照会とか文献複写取り寄せ依頼とか）
 - **eリソースへのアクセスで使いたい**
 - リモートアクセス
 - 個人認証
 - その他もろもろのシステムで使いたい
 - （機関リポジトリ）etc...

図書館以外で学内で全構成員に対して認証を伴ったサービスが必要なものは少ないが。

- 北海道大学認証基盤現況

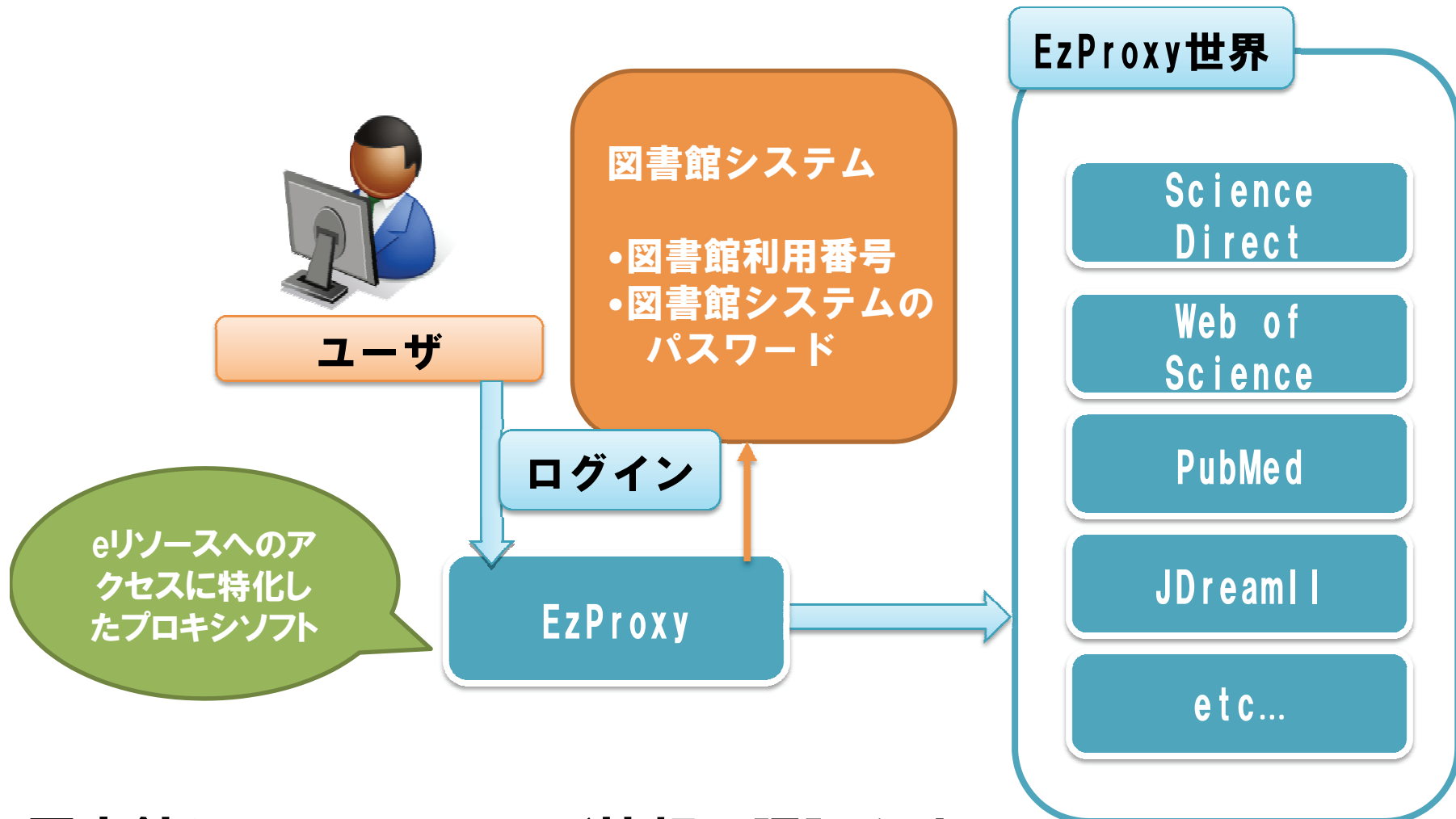
- 認証基盤
- シングルサインオン（縦横）
- 望むこと
 - ユーザ管理
 - 認証

- 北海道大学eリソースアクセス環境の現状と今後の希望

- 現況
- やりたいこと
 - 個人認証シングルサインオン
 - リモートアクセス

- 実現のために

リモートアクセス現況



**図書館システムのユーザ情報で認証させている
(図書館の利用者ID/PWDなんて誰も覚えてない) ←できればはやくやめたい。**

EZproxyの弱点

- **リバースプロキシなため、設定されているURLの範囲内をたどることが必要。**
- **一度範囲外に出てしまうと、機関で用意したメニュー画面等に戻って再びたどらなければならない。**
- **ベンダーによっては個人認証サービスがある。これらには当然、それぞれのサービス毎にそれぞれのID/PWDでログインしなければならない。**

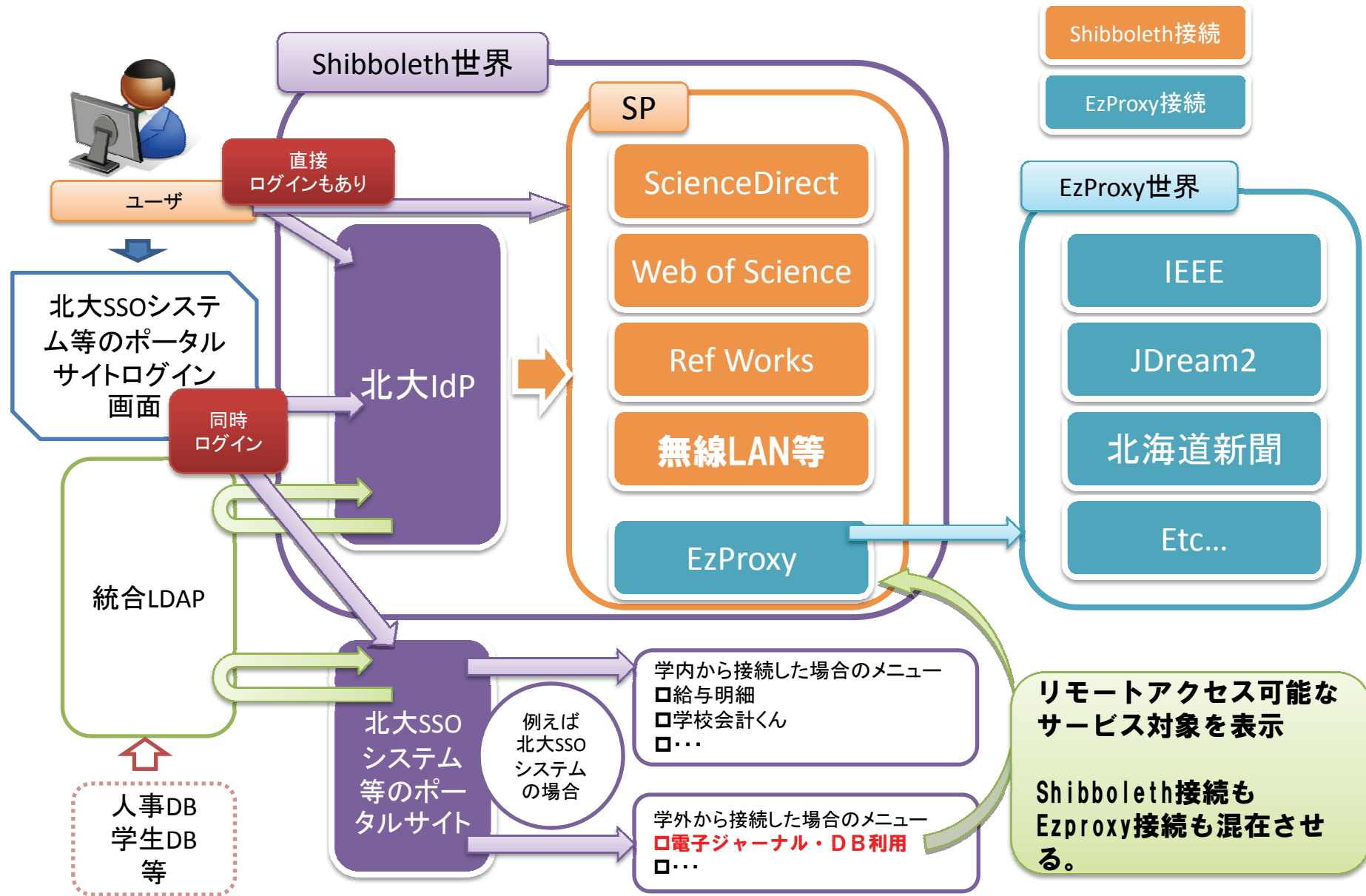
Eリソースサービスの今後

- よりきめ細かな情報利用行動に対応するため、**個人向けサービス**が強化されるのではないか。
- 個人向けサービスが強化された文献探索ツール(電子ジャーナルプラットフォーム, 文献データベース), 文献管理ツール(RefWorks等)が増える場合, これらのサービスへの横断的なアクセス(**シングルサインオン**)が求められてくるだろう。
- もちろんこれらはいつでもどこでも同じ環境(**リモートアクセスでも**)で利用できること。

そのための環境構築

- 各電子ジャーナルプラットフォーム，データベースが提供する**個人向けサービス**（**要個人認証**）に対して，**シングルサインオン**で使用可能なように。
 - 縦のシングルサインオンが可能な仕組みで。
→ Shibbolethなら実現可能
- どこからでも同じ環境（リモートアクセス）で
 - Shibbolethはリモートアクセスも実現する
 - VPN，プロキシではリモートアクセスは実現できても上記個人向けサービスのシングルサインオンは実現できない。
- ID・パスワードは大学一元管理のもので
 - 統合認証基盤で
 - 覚えていられるもので

今後の希望 (イメージ)



今後の希望

既存ポータルサイトとの連携-例えばSSOログインについて-

SSOシステムログイン画面（現）

学外から

学内から

- ICカード（PKI）認証のみ可能（試行：全学で70枚）
- VPN接続

クリックするとID,PWDの
入力画面表示

SSOシステムログイン画面（将来）

ICカード認証

パスワード認証

- 接続元（学内 or 学外）はIPから判断
- 学内からのアクセスはフルメニュー表示
- 学外からのアクセスは、セキュリティポリシーでメニューを分ける。（eリソースへのアクセスはパスワード認証でもOK）
- 認証はShibboleth認証も兼ねる

同時ログインは可能らしい

東工大SSOとShibbolethの連携

連携の基本方針

東工大SSOにログインできれば簡単に東工大IdPへもログイン可能であること

東工大SSOからログアウトすれば東工大IdPからもログアウトされること

東工大SSOにログインすればShibbolethのDSによるIdP選択を省略できること

実装概要

東工大IdPのコンテンツを東工大SSOの保護下に設定

東工大SSOは認証済みユーザIDをHTTP Headerに埋め込むように設定

東工大IdPはHTTP Headerに埋め込まれたユーザIDで自動的にログインするように設定 (RemoteUserAuthServletを利用)

東工大SPにおいて東工大IdPを常に参照するように設定したリンク集を作成

東工大SSOとShibboleth連携(東京工業大学)「平成20年シングルサインオン実証実験報告書」より

- **北海道大学認証基盤現況**

- 認証基盤
- シングルサインオン（縦横）
- 望むこと
 - ユーザ管理
 - 認証

- **北海道大学eリソースアクセス環境の現状と今後の希望**

- 現況
- やりたいこと
 - 個人認証シングルサインオン
 - リモートアクセス

- **実現のために**

学内合意形成

- **図書館単独で動くつもりはなし。**（ただし自前（図書館）でテストIdPを構築しいろいろ試すことは必要か）
- **学内担当部署（特に情報基盤センター）と歩調をあわせつつ。**
- **まずは、安くない金額で購入しているeリソースを最大限使いこなすためには学内認証環境の整備が必要であることを訴えていきたい。**

業界の発展のためにも？

- **個人認証に移行することにより、ベンダー側・図書館側でより付加価値の高いサービスを展開できる下地ができるのでは？**
- **また他ベンダーのサービスとシングルサインオンできるのであればまた新たなアイデアも出てくるのでは？**

ERソースについてはまだまだ環境改善できることはある。

よりよい環境を作っていきたい！