SPにまつわる仕様書と調達
～SPを独自にシボ化した場合～

金沢大学　松平 拓也（統合認証・ポータル整備WG）

金沢大学統合認証基盤構築の背景

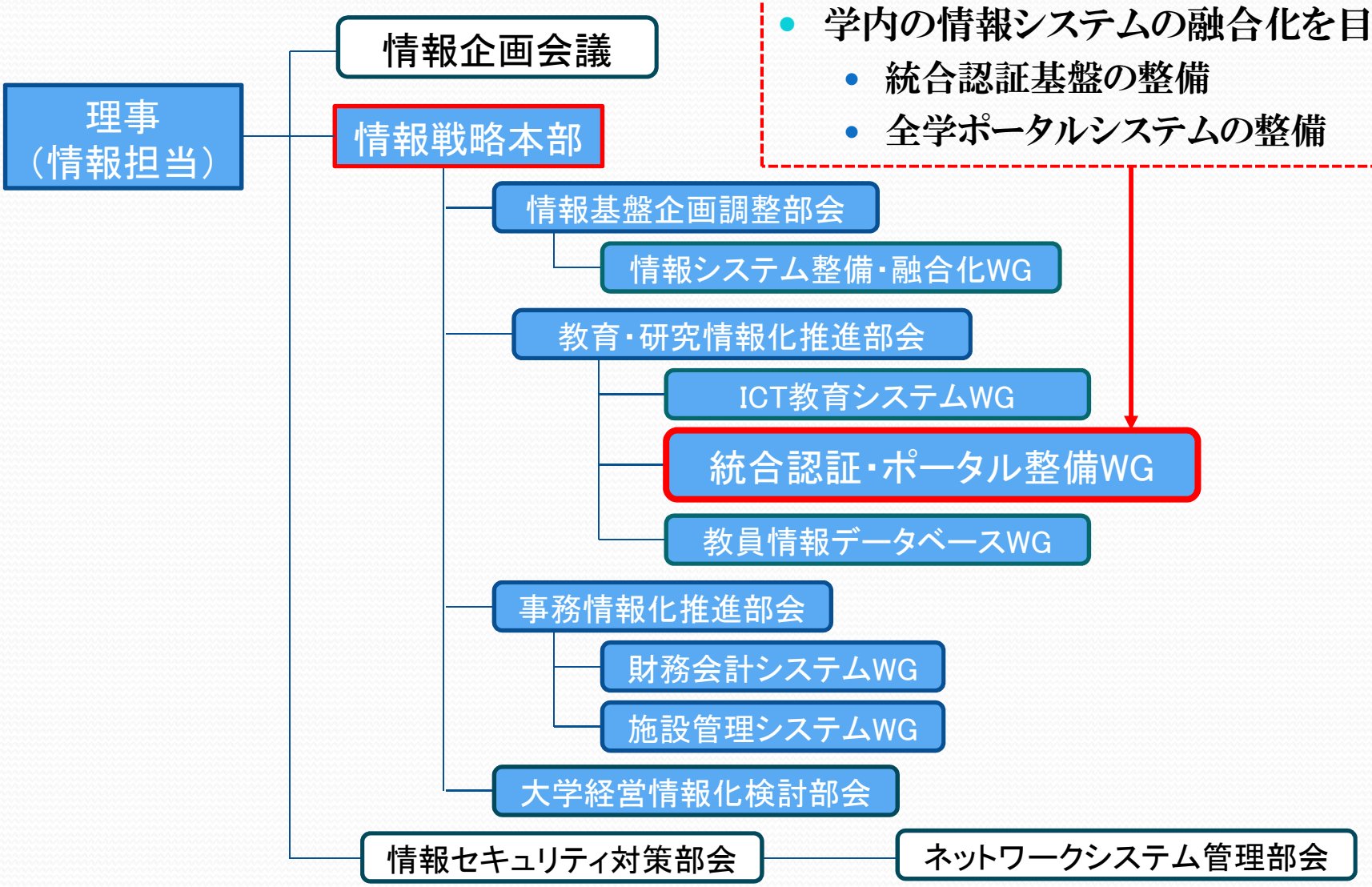
- 金沢大学情報システムにおける問題点が数々指摘
  - 各情報システム独自の認証機構
  - システム毎にID/パスワードを発行
  - 情報システム間の連携がなく、各システムが重複したデータを保持し、その鮮度も異なる

トップダウンで行う必要！

- 金沢大学 情報戦略本部の設置(H20.6～)
  - 設置目的
    - キャンパス情報ネットワーク及び情報システムに係る情報戦略について企画・立案し、実施に向けた指導・助言等を行う
    - 情報戦略本部を中心に、各部局や各関係組織と連携・協働し、全学の教育・研究活動及び事務の情報化を推進する

情報戦略本部組織体制（H24.4.1現在）

- 学内の情報システムの融合化を目的
  - 統合認証基盤の整備
  - 全学ポータルシステムの整備



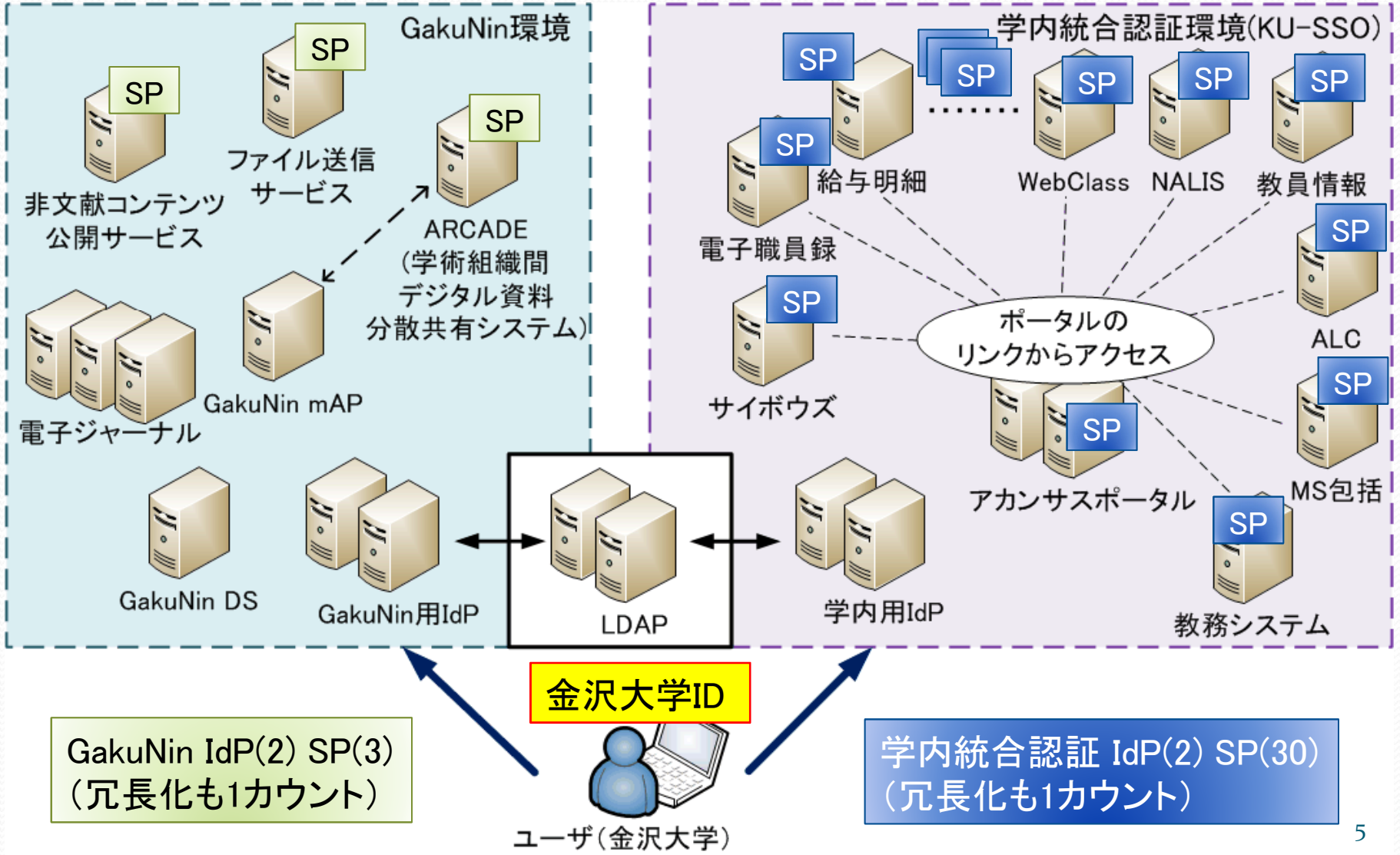
金沢大学Shibboleth化の背景

- なぜShibboleth？
  - 統合認証・ポータル整備WG
    - H21.4 発足
      （発足当時は全学ポータルWG（H22.4から現在のWG））
  - GakuNin
    - UPKI認証連携基盤によるシングルサインオン実証実験(H20)

実証実験でShibbolethに関するノウハウを蓄積し、適用可能と判断

- 統合認証・ポータル整備WG人員体制
  - WG構成員（設計・開発の指針決定）
    - 教員6、職員3　計9名
  - Shibboleth関連対応者（設計・運用に関する実務担当）
    - 教員4、職員2　計6名
      （GakuNinは教員2、職員1　計3名　（WGとは別の扱い））

GakuNinと金沢大学統合認証基盤



Shibboleth SP内訳（2012/5/31現在）

- GakuNin (3)
  - 全て独自に導入
- 学内統合認証基盤 (30 + 2(予定))
  - 独自に導入（13）
    - アカンサスポータル（2）
    - アカウント管理システム(金大ID管理・パスワード再発行)
    - Microsoft包括ライセンス（MSソフトダウンロード）
    - 電子職員録（教職員の連絡先（内線・メールアドレス）等の閲覧）
    - ソフトウェアダウンロード（ウィルス対策ソフト等のダウンロード）
    - ファイル共有アプリケーション（JavaApplet上でのファイル共有）
    - ファイル送信サービス（サイズの大きなファイルをダウンロード）（2）
    - 会議資料管理システム（会議資料をアップロード、iPadで閲覧）
    - プロジェクト管理システム（Redmine）
    - AcaNeCo（OpenPNEを利用して構築したSNS）

SP内訳(2012/5/31現在)

- 学内統合認証基盤 (30)
  - 業者に発注(17)
    - WebClass(LMS(株式会社ウェブクラス)) (3)
    - NALIS(図書業務管理(NTTデータ九州))
    - 学務情報システム(成績入力、履修者名簿の閲覧等(SCSK株式会社))
    - 学生情報システム(履修登録、連絡先入力等(SCSK株式会社))
    - 電子掲示板(学内の電子掲示板お知らせを確認(株式会社コンダクト))
    - サイボウズ ガルーン3(グループウェア(サイボウズ株式会社))
    - 給与支給明細(人材開発株式会社)
    - 源泉徴収関係届出(人材開発株式会社)
    - 施設管理システム(施設の情報入力、閲覧(株式会社サイバーブルー))
    - Webシラバス(シラバス情報をWebで入力、閲覧(ヨシダ印刷))
    - 教材データベース(教材共有(金沢電子出版株式会社))
    - ALC NetAcademy2(英語教材(株式会社日立ソリューションズ))
    - 統合アカウント管理(金大ネットワーク(WiFi)接続用ID管理(富士通))
    - 教員情報データベース(教員実績入力・閲覧、評価(田中昭文堂))
    - 留学生支援システム(留学生用交流サイト(田中昭文堂))
  - 現在導入中(2)
    - 予算執行支援システム(物品発注、(富士通))
    - 単位充足度把握システム(学生が単位取得状況を確認(SCSK))

Shibboleth SP化までの流れ

1. Shibboleth SP化の提案
   - 新規情報システム ⇒ 運用担当部署から情報戦略本部に申請し、承認を得る
     - 統合認証・ポータル整備WGから担当部署への提案/担当部署からの相談への対応
   - 既存の情報システム
     - 全部署に対して保持しているシステムをヒアリング、Shibboleth化の提案
2. 仕様書の作成
   - Shibbolethに関する項目はWGから提案
   - パッケージの開発業者や業者の問い合わせにはWGから説明
   - 予算
     - WGが負担(主に既存システムの場合)
     - 担当部署が負担(主に新規システムやリプレースの場合)
3. 開発
   - 業者開発時のShibbolethに関するエラー等の質問はWGが回答
   - テスト環境の提供
4. 納品・リリース

独自Shib化の場合はこの部分を自分たちで行う必要あり

1～4まで、数か月から1年程度

見積り金額に影響しそうな項目

- Shibboleth化に伴うシステムへの影響範囲が把握できるか
  - 業者がShibbolethを知らないと、莫大な金額を請求（調査・検証）
    - Shibbolethインストール手順書をWGで作成し、仕様書に添付
  - Shibboleth認証後、具体的にどの属性をどうやって使うかなどを提案
- 学内にテスト環境が存在するか
  - 本番環境と同等なテスト環境がない場合、テスト環境を構築するために、別途費用を要求する可能性あり
- 学内にShibboleth有識者がいるか
  - 「Shibboleth化する際にプロキシが必要」、「ログイン後のユーザ特定が困難で実現が難しい」等の問題が発生した場合、学内にShibboleth有識者がいれば、本当にそうなのか検討できる
- シングルログアウトを必要とするか
  - シングルログアウトのロジックを実現する場合、アプリケーションおよびSPのセッションを削除する必要があり、工数が増える

いかにShibboleth化が簡単であるかと業者に伝えることが重要

独自Shib化の場合、上記項目のクリアは最低条件

仕様書1 -NALIS（2009）-

1.オンラインサービスShibboleth対応

1.1 Shibboleth認証への対応

1.1.1 別紙資料「ShibbolethSPインストール手順」を参考に、Shibbolethモジュールをインストールすること。ShibbolethSP用のメタデータ、属性設定ファイルは本学から提供するものとする。

⇒Shibbolethのインストールを行うこと。ただし、必要な資料は全て提供する。

1.1.2　ログアウト処理には、本学が指定するURLを呼び出すこと。また、独自認証している場合は、本アプリケーションの認証セッションを削除すること。

⇒シングルログアウトを実装すること。

1.1.3　SSOするユーザの特定は、単一で返される利用者IDのみとしロールごとによる認証判定は必要ないものとする。

⇒複数ロール対応は必要なし。

独自にShib化した場合に想定される作業ポイントを仕様書に記載

仕様書2 予算執行支援システム（2012）

4.8　サブシステムの認証

4.8.1　本学で運用中の金沢大学統合認証システム（Shibboleth）の認証に対応して、ログインが可能なこと。

⇒Shibboleth化すること

4.8.2　認証成功後、金沢大学統合認証システムからのサーバ環境変数の個人番号（教職員番号）で，システム内に登録されているユーザの教職員番号と一致した場合に、一致したユーザとしてログインを行うこと。

⇒Shibbolethログインユーザに関するシステム内のデータを正しく呼び出すこと

4.8.3　金沢大学統合認証システムの認証とは、別の認証ページを用意して、切り替えて使用が可能なこと。その場合のパスワードは、サブシステム独自のパスワードを利用できる機能を有すること。

⇒Shibbolethに問題があった場合・特例ユーザが必要な場合に対応できること

4.8.4　シングル・ログ・アウト機能として、サブシステムの独自Sessionを削除するページと、ログアウトを行った場合に、Shibbolethの指定したログアウトURLを呼び出す機能を有すること。

⇒シングルログアウトに対応すること

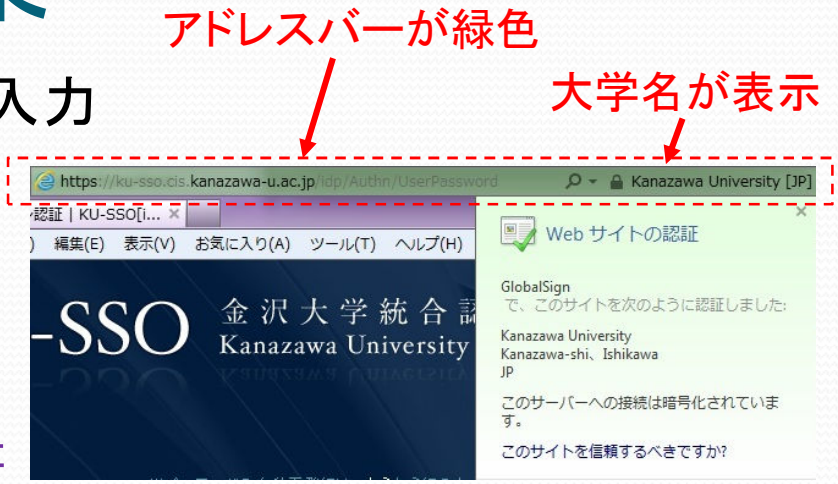
独自Shib化 vs 業者Shib化

	独自Shib化	業者Shib化
導入コスト	安い （学内人件費のみ）	高い （先行大学は特に割高）
実現性	途中で挫折の危険性あり （金沢大学では一度もない）	契約が成立すれば、必ずやり遂げる
パッケージ品の対応	ライセンス問題に抵触する可能性あり -Shib化できても、サポートが受けられなくなるケースが想定	追加モジュールとして、安定して提供される
SPバージョンアップ	担当技術者がシステム管理部署と相談し、迅速に対応可能（学内人件費のみ）	業者との打ち合わせ・日程調整が必要（バージョンアップ毎に費用）
インシデント対応	独自（学内）対応 -担当技術者の人数に依存 -担当者不在時は対応できない	業者対応 -瑕疵担保は平日 9-17時 1年が一般的 -保守費用が必要
ノウハウ	学内に蓄積	業者に蓄積
マニュアル	担当者の裁量 - 不備があるケースが多い	書類として納品

IdPのセキュリティ対策

- IdPでは、生涯IDである金沢大学IDを入力
  - フィッシング対策が必要

EV-SSL証明書の導入



- EV(Extended Validation)-SSL証明書
  - 証明書に記載される組織が法的かつ物理的に実在し、その組織が証明書に記載されるドメインの所有者であることを認証
    (必要書類:印鑑証明書、登記事項証明書等(法人のみ取得可))

- グローバルサインから購入
  - 金額　1年 ¥134,400 (1コモンネームあたり(複製してインストール可))
    - gakunin-idp.cis.kanazawa-u.ac.jp (GakuNin用IdP)　× 2
    - ku-sso.cis.kanazawa-u.ac.jp (学内用IdP) × 2
    - それぞれ冗長化しても　¥133,400×2=¥266,800(2枚以上購入でまとめ割あり)

予算に余裕があれば、是非仕様書に一行「EV-SSL証明書を使用すること」と記載

まとめ

- 学内のShibboleth化推進にむけて
  - トップダウンでShibboleth化を提案できる組織体系が必要
- 金沢大学のShibboleth SP対応状況
  - GakuNin SP (3)
  - 学内 SP (30) + (2 予定)
- 仕様書作成について
  - いかに業者に不透明な作業部分を見せないかが重要
  - 学内でShibboleth技術者を育成
- 独自Shib化と業者Shib化
  - 独自開発システムは学内、パッケージ品は業者でShib化するのがベター
- IdPのセキュリティ対策
  - EV-SSL証明書の導入によるフィッシング対策
  - ID/PW以外の他要素認証の検討

学内認証基盤をShibboleth化しておけば、GakuNinへの適用は簡単