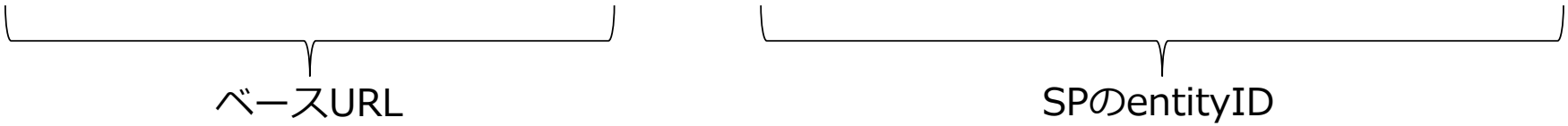
学認・Shibbolethの動向

2024.9.17 大学ICT推進協議会認証基盤部会勉強会
国立情報学研究所　西村健

Metadata Query Protocol(MDQ)について

- フェデレーションメタデータを丸ごと取得するのではなく、個々のentityID単位等オンデマンドで取得するためのプロトコル
  - https://datatracker.ietf.org/doc/draft-young-md-query/
  - https://datatracker.ietf.org/doc/draft-young-md-query-saml/
  - アクセス例：
    https://mdq.example.org/global/entities/https%3A%2F%2Fsso.example.org%2Fsp



- Shibbolethが対応している
  - https://shibboleth.atlassian.net/wiki/spaces/IDP5/pages/3199507683/MetadataQueryProtocolExample
  - https://shibboleth.atlassian.net/wiki/spaces/SP3/pages/2060616133/MDQMetadataProvider

MDQサーバに対する考慮事項

- 仕様自体は検索やフィルタリングの機能を有する。極端な話全体を取得することも可能。
- 各レスポンスに署名が必要

- 学認においては、
  - 検索やフィルタリングは対応せず、entityID指定でのIdP/SP単体のメタデータ取得のみ対応としたい
  - リアルタイムでの署名は時間がかかりすぎる→キャッシュしておく

NII情報処理技術セミナー認証活用編について

- NIIの教育研修事業として例年2日間コースでShibboleth等の実習を行っております
  - 教育・研究機関等のシステム運用担当の教職員を対象としています

- 活用編（隔年で開催）
  - 9月26~27日
  - テーマ：構築されたShibboleth環境の活用

- 詳細は下記にて：
  https://contents.nii.ac.jp/hrd/joho-karuizawa/2024

今年度のセミナー活用編の内容（予定）

- 1. 学認申請システムを使ってテストフェデレーションに参加する
- 4. attribute-filterの自動生成演習
- 5. mAP Coreを使ったグループの活用
- 7. Webアプリケーションのシボレス化実習
- 9. Embedded DSの導入
- 10. 学認DSの機能について
- 11. クライアント証明書認証を使った認証
- 12. セキュリティレベルを設定したSPに対する認証（MFAフロー関連）
- 13. ユーザによる認証方式が選択できる設定（MFAフロー関連）
- 14. TOTPを用いた多要素認証方式の導入（TOTPプラグイン関連）
- 15. TiqrShibプラグイン
- 16. FIDO2プラグイン（WebAuthn）
- 17. SAMLAuthnConfiguration機能を利用したSAML Proxy

WebAuthn(FIDO2)サポート

- Shibboleth IdPバージョン5でWebAuthnを用いた認証がサポートされた
  - https://shibboleth.atlassian.net/wiki/spaces/IDPPLUGINS/pages/3395321933/WebAuthnAuthnConfiguration
- 例によって登録が課題であるが、簡易的なものを実装して体験してもらう

SAMLプロキシ

- 最近のShibbolethではバックエンドにある別のSAML IdPへ認証をプロキシすることが可能
  - https://shibboleth.atlassian.net/wiki/spaces/IDP5/pages/3199505973/SAMLAuthnConfiguration

MFAフロー

- 以上のような認証フローをいかに組み合わせるかを定義する
  - セキュリティレベルを設定したSPに対する認証（MFAフロー関連）
  - ユーザによる認証方式が選択できる設定（MFAフロー関連）

- 参考：MultiFactor認証フロー(MFA)を用いた認証設定
  - https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=26186832

学認における自己署名証明書対応

- パブリックなサーバ証明書の有効期間短縮の影響で、学認において自己署名証明書を使いたいという要求が増加
  - いずれの場合も3年ごとに更新すべき（SHOULD）
- パブリックな証明書との紐付けを確認することで自己署名証明書の利用も可能

- IdP/SPで「パブリックでない証明書」（自己署名証明書）を利用する場合
  - https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=159744061