GakuNin IAL/AAL の基本方針について

佐藤周行

次世代認証連携検討作業WG

この発表は

- 表紙を含めスライドにして14枚、時間にして約15分を予定しています
- 2021年度から活動を続けている「次世代認証連携検討作業部会」の成果の一部として、ポリシー策定に関係する部分を発表します
- ポリシー文書の状況は以下のようになります
  - IALに関する文書：公表の上コメント受付中
  - AALに関する文書：公表の上コメント受付中
  - KYCに関する文書：内部で検討中
    - 組織に属さない利用者を収容するためのガイドライン

次世代認証連携の目指すこと includes

- 今まで、ネットで完結しなかった（できなかった）さまざまなサービスをネットで完結させる
  - たとえば、スーパーコンピュータシステム利用のためのアカウント申請
  - たとえば、ヘルスケアデータへのアクセス
- そのためのトラストを構築する
  - 必要となるトラストレベルの特定
  - 日本での運用
  - 世界での相互運用性の保証
    - Kantara, IGTF

ポリシーに関しての実施シナリオ

- ポリシー文書の作成
  - （日本で正当だと了解される）リスク評価
  - 実運用での評価
- ポリシーの内容をIdP、SPが双方了解する
  - CrP/CrPS
- ポリシーを実施
  - ポリシーに従ったIdP運用
  - それをSPに発出（アサーションの中に記述）
  - SPがアサーションをチェックして、リクエストをアクセプト

学認、参加IdP、参加SPの共同作業です

- 参加IdPは、ポリシーを実装、実施
- 参加SPは、計算/データリソースを提供
- 学認 (NII) は、ポリシーと関係するプロトコルを整備

ポリシー策定

- 基本：標準的な文書のレベルに合わせる
  - NIST SP800-63 Digital Identity Guideline
- IAL（身元確認レベル）
  - NIST SP800-63Aのレベル2相当
- AAL（当人確認レベル）
  - NIST SP800-63Bのレベル2相当
- 日本の事情を考慮　&& 相互運用性を重視
  - 文科省等の監督内容の援用
  - Kantara, IGTFをどう説得するかは問題として意識

IdPが発行するアカウントの種類

- 大学等研究機関が教職員（学生）に対してアカウントを発行する場合
  - 日本の場合は、文科省等、国の監督が厳しいことがこの点ではアドバンテージ
  - 学認参加機関のIdP運用に対する努力に感謝

- 共同研究利用機関が、共同研究のために組織外の人にアカウントを発行する場合
  - 研究組織に直接属しているのではない利用者をサポートするIDaaSを含む

Identity Assurance Level 2

- 相互運用性に配慮することを前提として、日本の規制の強さを評価
  - 「正しく」運用されていれば、レベル2はクリアしているはず
  - 組織のTrusted DBに接続してアカウントを発行することが大前提
  - …ということを反映した学認IAL2規準を提案しました
  - コメントをお寄せください
- SPは、利用者の所属証明を結構気にすることがわかった
  - Due Diligence (資格証明)との関係上
  - O属性のレベル2の保証が必要

https://www.gakunin.jp

お知らせ

NII学術情報基盤オープンフォーラム2022のお知らせ	2022-05-12 16:42
【重要】学認申請システムメンテナンスのお知らせ(2022/4/26 15:00 - 16:00)	2022-04-15 14:16
【重要】学認申請システムメンテナンスのお知らせ(2022/3/30 13:00 - 17:00)	2022-03-23 14:06
【重要】学認 ウェブサイトメンテナンスのお知らせ（2022/3/28）	2022-03-17 13:40
次世代認証基盤構築のための基準策定と配備の観点からの文書再評価のお願いについて	2022-03-11 16:04

すべて見る

新着資料

IAL2の新学認での運用に当たって（案）Ver.2	2022-03-11 15:46
次世代認証基盤構築のための基準策定と配備の観点からの文書再評価のお願い	2022-03-11 15:41
学認参加IdP運用状況調査票(令和3年度実施版)	2021-11-09 13:10
次世代認証基盤構築のための基準策定と配備の観点からの文書評価のお願い	2021-11-08 11:26
CrPCrPSテンプレート（案）	2021-11-08 10:51

すべて見る

CrP/CrPS

- Credential Policy/Credential Practice Statement
- アカウントの運用ポリシーを公表しましょう
- SPが、IdPから送られてくる属性のどの部分が信頼できるかを判断できるように
  - 特にO属性

eKYCの利用

- 共同研究利用機関が、大学等研究機関以外の利用者を収容する際の基準を検討中
  - 「研究コミュニティ」全体をサポートすることが、そのコミュニティの発展につながる　←　共同研究利用機関が発行するアカウントの評価
  - 一般　←IDaaSが行っているアカウントの質保持に関する努力を正しく評価
- 他のアイデンティティ提供システムとの連携を模索
  - ORCHID
  - 研究者番号
  - GビズID
  - …（協力していただけるところはありませんか？）
- Due Diligenceの一部採用
  - 「信頼できる」組織（会社等）の身分証の受け入れ
  - 許可リストを学認が保守することを検討

Authentication Assurance Level 2

- 世間は、「パスワードレス」に舵を切りつつある（Securityの意味でもUsabilityの意味でも）
  - その中で多要素認証を採用←リスク評価が必要
  - 多要素認証のベンダーサポートが充実することが予想される
  - 特に「パスワード」＋「もう一つの認証」を推奨

- 一定数のIdPは、エンタープライズIdPとして、ベンダー提供の多要素認証方式を提供していることを理解
  - 学認IdPとの接続を支援（技術支援）
  - 多要素認証の運用についての基準を提示
    - 特に認証要素と利用者の結び付け（汗をかく必要）

- 利用できる認証器のレジストリを学認として運用することを予定
  - 関連するベンダーやコンソーシアムのご協力が不可欠です

学認のサポート

- 学認内で流通する属性の保証レベルを認定し、SPが安心して利用できるようにします（IAL）
  - 保証レベル2の属性値を定義
- SPが多要素認証を要求する際の要求の送出方法を定めます
- IdPが、特にAAL2を運用する場合についての技術サポートを行います
  - サービスモデルごとのconfigの仕方を含む
- 国際的な相互運用性保証のための交渉の窓口になります

終わりに

- 現在、基準実施のテストを一部のIdPとSPとで計画しています
- その後、パートナーを募り、全体で運用していく予定です（今年度中）

- 基準は、実施してリスクを不断に評価することで、堅牢なものになります。ぜひご協力ください