IDPの信頼を高めるために –学認アンケートの傾向と対策–

東京大学 / 学認
佐藤周行

学認アンケート

- 2011年10月12日付け、本運用を行なっているIdPに発送（10月31日締め切り）

- 26大学から回答
- ご協力ありがとうございました。

- アンケートをなぜするのか？
- どこに気をつけて運用すればよいのか？

アンケートの意義について

http://www.gakunin.jp/docs/fed/loa

概要

学認では、定められた規定（ポリシー）を信頼し合うことで、IdPとSPの間で相互に接続することを可能としています。この信頼関係（トラストサークル）を保つことは、参加機関に対し学認が果たすべき重要な役割の１つです。学認に参加する際に、各機関には、

- 学術認証フェデレーション実施要領
- 学術認証フェデレーション システム運用基準

を遵守することに同意して頂きました。実施するアンケートは、**これらのポリシーに適合して、IdPが適切に運用されているかを定期的に確認**するためのものです。

プラスアルファの価値

- 世界標準に適合したトラストサークルの確立
- 学認における認証の保証レベル導入の必要性
- 保証レベルの導入から展開する学認のサービス革新

- この議論は午後にできるのではないか、と

アンケートの詳細

- ポリシーへの準拠性を求めるための質問
  - 利用者Idと属性の管理・運用について
  - 共有Idの禁止について
    - ユーザ登録とID Proofing（より一般にアイデンティティ管理）、パスワード（Token）管理
  - 個人情報保護について
  - 一般的なセキュリティについて

個々にみていく

- 利用者Idと属性の管理・運用について
  - 利用者IDは信頼できるデータベースから作成されるように定められていますか？
  - 組織のメンバーを定めるDB以外からIDを作成する場合のルールと管理体制は？
  - 利用者IDの属性でIdPが保証するものは自組織のものに限ることが保証されるか？
  - 属性の信頼性の根拠？
  - 流通する属性情報は運用基準で定められているものか？
  - IDのライフサイクル管理についての規定は？（特に廃棄）
- 共有Idの禁止について
  - 共有IDの運用のされ方、同一IDでのアクセスが同一人物からであることの保証のための対策

得られた回答の観察

- 回答の観察
  - 全学、または部局の「信頼のおける」DBからIDを作成しているものが大部分
  - 失効についても一定の努力（ライフサイクル）
  - ゲストIDの管理
    - 禁止
    - 可能だが、「適切に」管理している
  - 共有IDの禁止等（より高い信頼性を得るための第一歩）

利用者IDと属性の管理・運用

- 信頼できるDBに（半）直結すると信頼性は向上します
  - 技術のサポートがあると強い
- IDライフサイクルをきちんと回すことが必要です
  - 廃棄、停止のプロセスが大切
- これらを「慎重な」「適切な」運用で実現することはもちろん可能です。

属性の運用について

- IdPは属性を保証
- 「変な」属性は流通していない

- 属性の値に与えられる意味に若干の不整合
  - 特にeduPersonAffiliation
    - student, staff, facultyの意味
    - 各大学の個性はあってもよいし、微妙なところもある
    - SP次第 or SPとの交渉ごと

- 個人情報保護
  - 規程はありますか？
  - SPの定める属性以外が送られることを拒否する場合、それへの対処は可能ですか？
- 一般的なセキュリティ
  - ログの保存期間は定められているか？
  - 以上のほかに規定されていれば書いてください

個人情報保護

- IdPは個人情報を本質的に取り扱う
  - 特に問題になるのが
    - 適切な通知
    - OptIn（属性リリースにあたっての利用者同意）
    - 最低限の情報リリース
    - 活動情報を他に開示しない
    - 個人情報が不要になったときに適切に処分（廃棄、保管を含む）
  - これらを「守っていること」がわかることが必要

回答の観察

- 個人情報保護についての規則の整備が必要かも
  - 上部の規則が準用されればそれでもOK
    - 法律までさかのぼるのはNG
    - 大学内のどこかの階層で規則があることを確認
  - 特に「世界」で求めるOptInは、「リリースする情報をすべてあげた上で、それに対して同意をもらう」
    - IdPの運用で対応が可能です。慎重な運用＋利用者同意を得る何らかの手段があれば問題ありません
    - 技術のサポートがあります。uApproveの採用をお勧めします（shib固定になってしまいますが…）

一般的なセキュリティ

- IdPが、学内のどこかの階層で定められた「セキュリティポリシー」および、各種規則、手続きに則って運用されていることが本質的に重要です
  - 学内のサービスとして

学認アンケートと学認の信頼

- 学認の体制
  1. ポリシーの策定（実施要領、システム運用基準とプライバシーについて）
  2. IdPがポリシーを遵守した上で学認に参加
  3. 学認が、「遵守」の度合いを監査・評価して公表

＝　トラストフレームワーク

特にアメリカで整備が急。

アメリカの（連邦）サービスを利用しようとすると上の意味での信頼性を求められる

学認アンケートの設計

- 学認は、以下の方針で学認アンケートを設計しました
  - 「学認アンケート」にポジティブな回答ができればおおよそFICAM LoA 1（実質的な世界標準）相当の信頼度が認められる（今後アンケートを微調整する必要はありますが…）
  - 上を処理するためのチームを学認内に作ります
- **学認アンケート対応以外の特段の努力は必要ありません**

一般論

- レベル認定のために必要なものは一般に次のようなものとされています。
  - 組織が「きちんと」していること
    - 財務関係書類、セキュリティの全学規程、IdPがその規程に則って運用されていることの証明
  - 個人情報保護が「きちんと」していること
    - 日本の法令にしたがって各大学で対応されていること
  - 技術的要件がみたされていること
    - 今回の学認アンケートは主としてこちらを調査しました
  - これらを正しく評価・監査できること

みなさまへのお願い

- 学認アンケートへご協力ください
- もし、学内のセキュリティ上の体制上のポリシーなどが非公開になっていれば、公開に向けて努力してください（でないと、追加アンケートが必要になる）
- ID管理をTrusted DB直結にする、uApproveを採用する等、信頼性を高める努力をしているところは、より高いLoAを付与できる可能性があります。「努力は報われる」
  - 制度設計を含めて今後2年程度で結論