SPからみたトラスト
@NIIオープンフォーラム

佐藤周行
トラスト作業部会

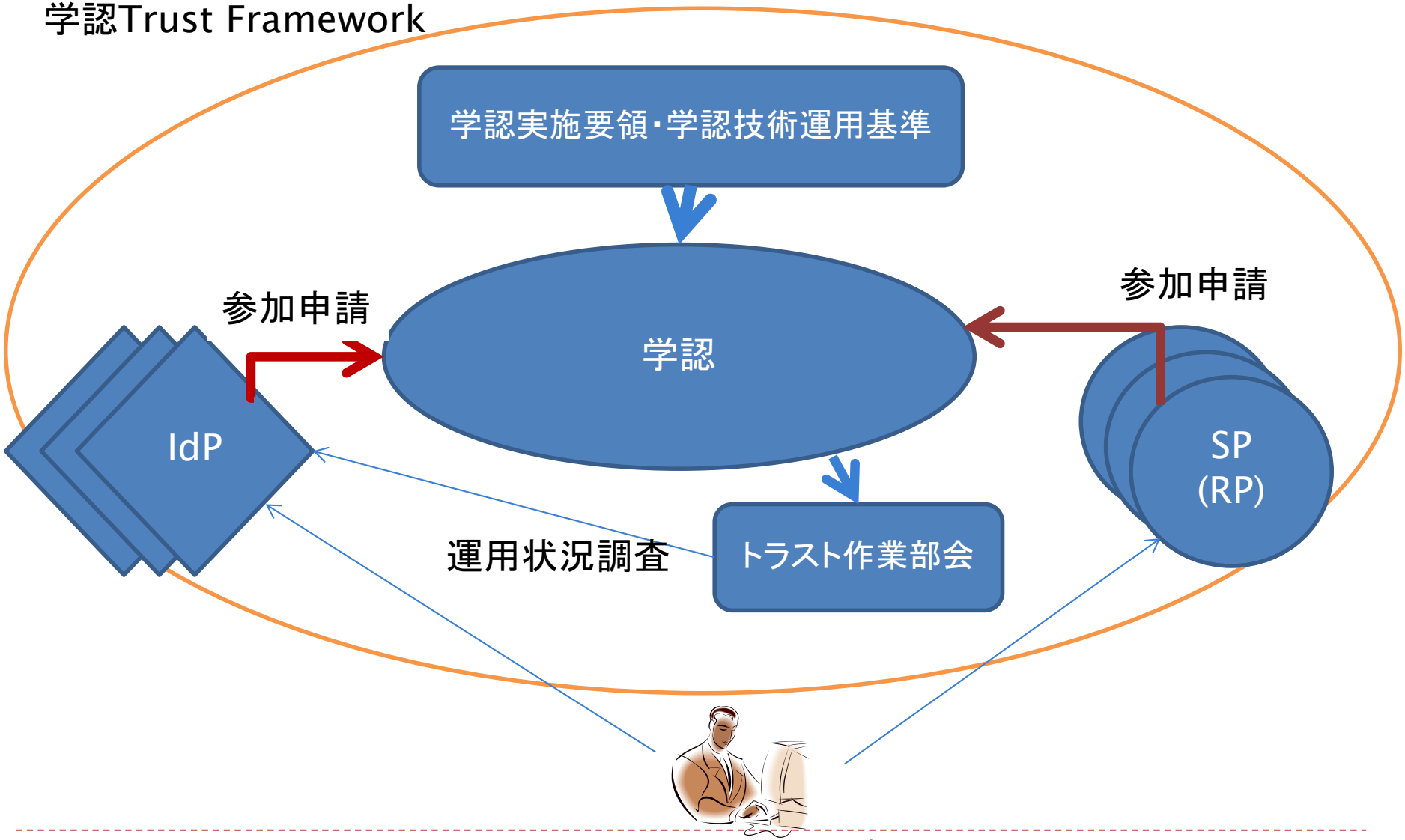
はじめに

- 「正しい認証基盤構築ガイド」の対象は機関IdPです
- では、なぜ「正しく構築する」必要があるのか？

- eduGain
  - Federation of Federations
    - 43 Full members, 5 voting members, 11 candidates (May, 2017)
    - Platform of Int'l Collaboration (LIGO etc.)
- では、もう一度、「トラストフレームワーク」のモデルをみてみましょう

学認のトラストモデル

学認Trust Framework



トラストの実際

- IdPを「正しく構築する」理由、意義はいろいろあります
  - 機関の「評判」形成
  - 「技術力を持っている」ことへのプライド
- SPからみてはどうでしょうか
  - IdPから送られてくる情報の信頼性によって、提供できるサービスが変わってくる
    - 「ノーベル賞級」の研究をするためのデータソースへアクセスするための認証の確からしさ
    - 「学割」を提供するための、「学生」情報の確からしさ
- SPからみたら経済の問題
  - 若干の不正確さを許容することも可能
    - 例： .u-tokyo.ac.jp で終わるメールアドレスを持っていれば学生とみなして、学生用のお得なサービスを提供しますよ
  - 一方、正確さをあくまでも追求しないとダメなケースもある

トラストでの解

- トラストフレームワークはこの問題に「相互信頼の枠組みの提供」で解を提供します
  - 学認に参加して、学認のポリシーを守っているIdPから出てくる情報は信用できる
  - SPは「学認の運用を信用するならば」IdPと個々に情報の精度についての確認をしない

- では、SPがほしい「情報」、「情報の精度」とはなんでしょうか
  - CASE 1:
    - SPは、利用者にidentifierを与えて管理する（OpenID Connectかもしれないし、SAMLかもしれない）
    - 学校に関係する情報は学認IdPからほしい （ネットでは、所属情報は、所属の保証がないのであれば自己申告以上の意味をもたない）
    - 学生だと分かれば、大幅にディスカウントしてもいいな…
  - CASE 2:
    - 補助金の申請において…

SPが必要とする情報

- SPがサービスを提供するためには認証情報の他に「属性情報」を必要とします
- IdPがそれを提供すると属性を含めた信頼の枠組みが構築されます

- 機関においてたとえば
  - もし、外部SPと連携して「学割」「職員割」が提供されれば、教育、福利厚生上、メリットになるでしょう
    - 米におけるNET+
  - 外部SPは、商用とは限りません
    - (国際)研究協力の模索
      - 米におけるCoManage
      - NIIでのmAP

「属性」の信頼度

- 属性の信頼度にはいくつかの評価軸があります
  - 「時間的な信頼度」
  - 属性にもライフサイクル管理が必要です（一般に失効管理が一番大変）

- 学認における属性保証について
  - 技術運用基準に記述があります
  - これを満たして運用されていることを「運用状況調査」で確認しています

技術運用基準中の記述

3. 属性情報

- 属性情報は、各エンティティが利用者への認可の判断を行うために使用する情報である。
- 学認で利用可能な属性情報については、本定義に添付する「属性情報仕様一覧」を参照するものとする。

3.1) 属性情報の利用

- 学認で定義されている全ての属性はユニークなURI名を持っている。各エンティティは利用したい属性について、可能な限り本定義に添付する「属性情報仕様一覧」から選択して利用すべきである。
- もし、利用したい属性が「属性情報仕様一覧」に存在しない場合は、各エンティティは委員会に新規属性の追加を申請することができるものとする。申請された新規属性の追加については、委員会において検討し、委員会が決定するものとする。
- なお、学認を介することのない、あるいは、学内のプライベートなフェデレーションのみで利用する場合にはこれ以外の属性を利用してもよい。

3.2) 属性情報の信頼性

- IdPは、自機関に所属する利用者の属性を保証すべきである。また、自機関に所属しない利用者の属性を保証すべきではない。例えば、A大学のIdPがB大学の学生の属性を保証すべきではない。ただし、自機関に所属しない利用者を自機関が管理する場合、SPに対する不正なアクセスが発生しないよう特に属性管理に注意することで、そのような利用者の属性を保証してもよい。

3.3) 属性情報の検証

- SPは、受信する全ての属性情報が、信頼するオーソリティから発行されたものであること
- を検証すべきである。

技術運用基準中の記述(続)

3.4) 属性情報の種別

- SPは、各サービスを提供する際に、必要となる属性情報及び当該属性情報の種別について利用者に明示すべきである。種別については“必須(required)”、“推奨(recommended)”、“任意(optional)”とし、属性情報の利用目的とともに明確に記載することが推奨される。
- SPは提供するサービスで必要な属性情報について、別途定める申請書によりフェデレーション事務局まで申請するものとする。
- なお、委員会は各SPがどの属性情報を利用するか、各エンティティに対して通知を行うものとする。

3.5) スコープ

- スコープは、原則としてentityIDに記載しているドメインがサブドメインであるようなドメイン名、もしくはentityIDに記載しているドメイン名と一致するものでなければならない。また、このドメイン名は原則として自機関が所有するものでなければならない。各IdPではメタデータにこのスコープを明示するとともに、スコープ付きの属性に対しては、同じスコープを利用しなければならない。また、SPではアサーションによって受信した属性のスコープを、IdPのメタデータに記載されているスコープと比較して判断するものとする。

具体的には

- O （機関名）が正しいことを保証します
- eduPersonAffiliation （教員/職員/学生）については、マスターDBと直結することで、ライフサイクル管理が正しくできるようになっています
  - 「運用状況調査」の精査で、ここはだいたいうまく行っていることがわかっています
- 認証は、現状ではパスワード認証がほとんどですが、各機関で気を配って行っていることがわかります
  - LoA1の認定が必要でしょうか？＞SPの方々

最後に：会場にいらっしゃっているSPの方々へ

- 学認では、このように属性情報についての運用基準を定めています
- 運用は安定しています
- 学認、または学認の一部を利用することで、経済的にサービスが展開できます

- …という感じで「トラストフレームワーク」は拡大していきます