次世代認証連携の枠組

佐藤周行
東京大学情報基盤センター/
NII学術認証運営委員会次世代認証連携検討作業部会主査

今回の話の趣旨

- このスライドは表紙を入れて17枚、時間にして約15分あります
- 学認のトラストを強化して、研究協力のための情報・計算リソースの共同利用の促進を認証面からサポートするための取り組みについて紹介します

- 大学等、IdPを運用しているところについては「自機関の発行するアカウントの価値を高める」
- 共同利用機関等、サービスを提供しているところについては「学認が、大学等のアカウントの信頼性を保証する」

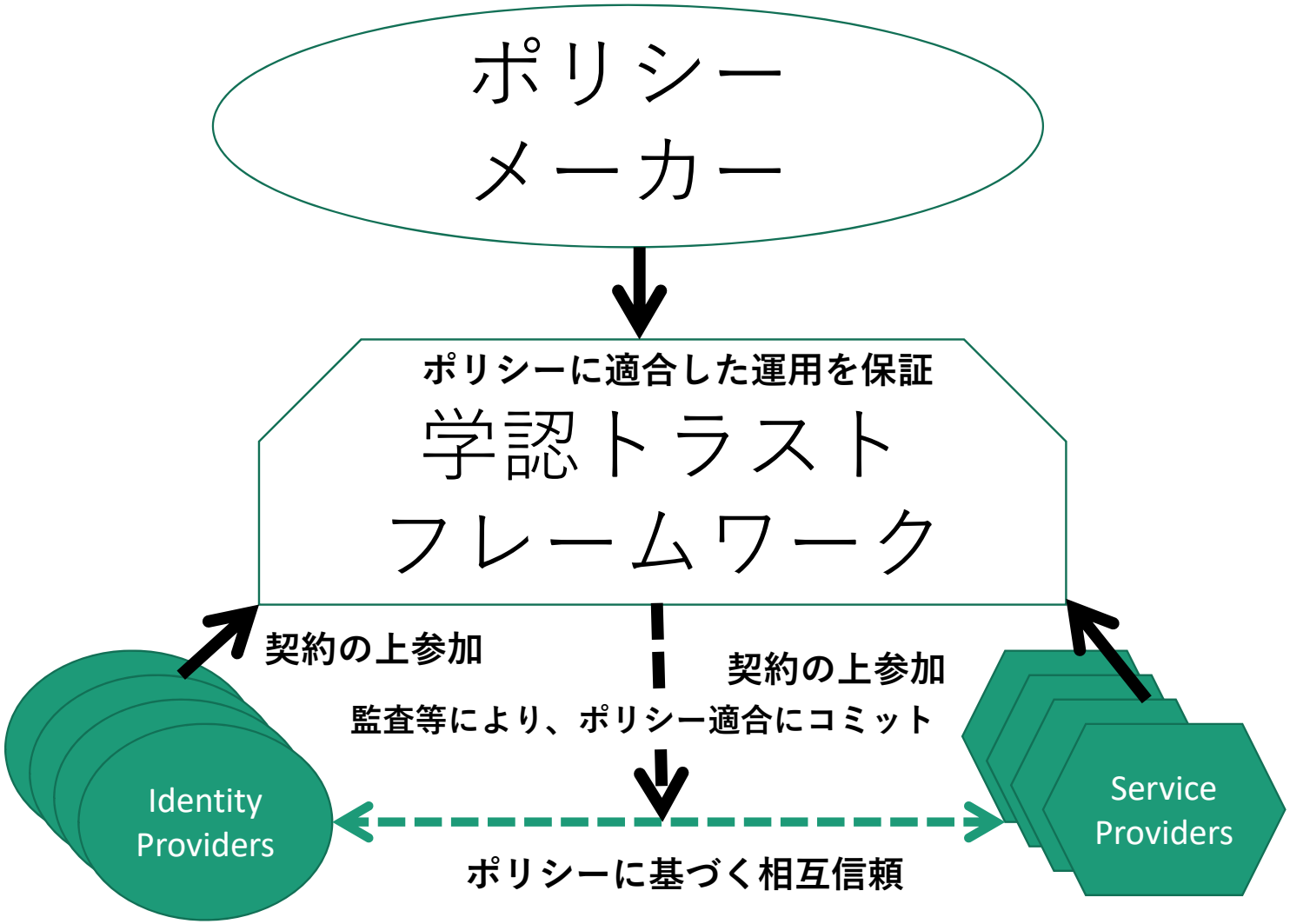
認証連携

- 認証連携（Identity Federation）という言葉は、すでに一般的なものになりました
- 大学等では、教職員、学生にアカウントを一つ与えて、SSO (Single Sign-On)で学内のリソースを利用することが一般的になっています

- 世界的にこの種の枠組の構築が進んでいます
  - eduGAIN
- 学認は、世界の動向に常に気を配っています
  - Kantaraへの参加
  - eduGAINへの参加

学認

- 学認は、大学の発行するアカウントを用いて、学外の情報リソースにアクセスするための認証連携のフレームワークとして構築されました
  - 電子ジャーナル等各種図書館サービスが初期の代表例です
- 学認に参加している機関のIdPは「正しく」運用されているだろうとサービス提供側が信頼してくれることが大前提となっています
- ⇒トラストフレームワーク
- 学認は、教育研究機関に構築された認証連携のトラストフレームワークとして機能しています

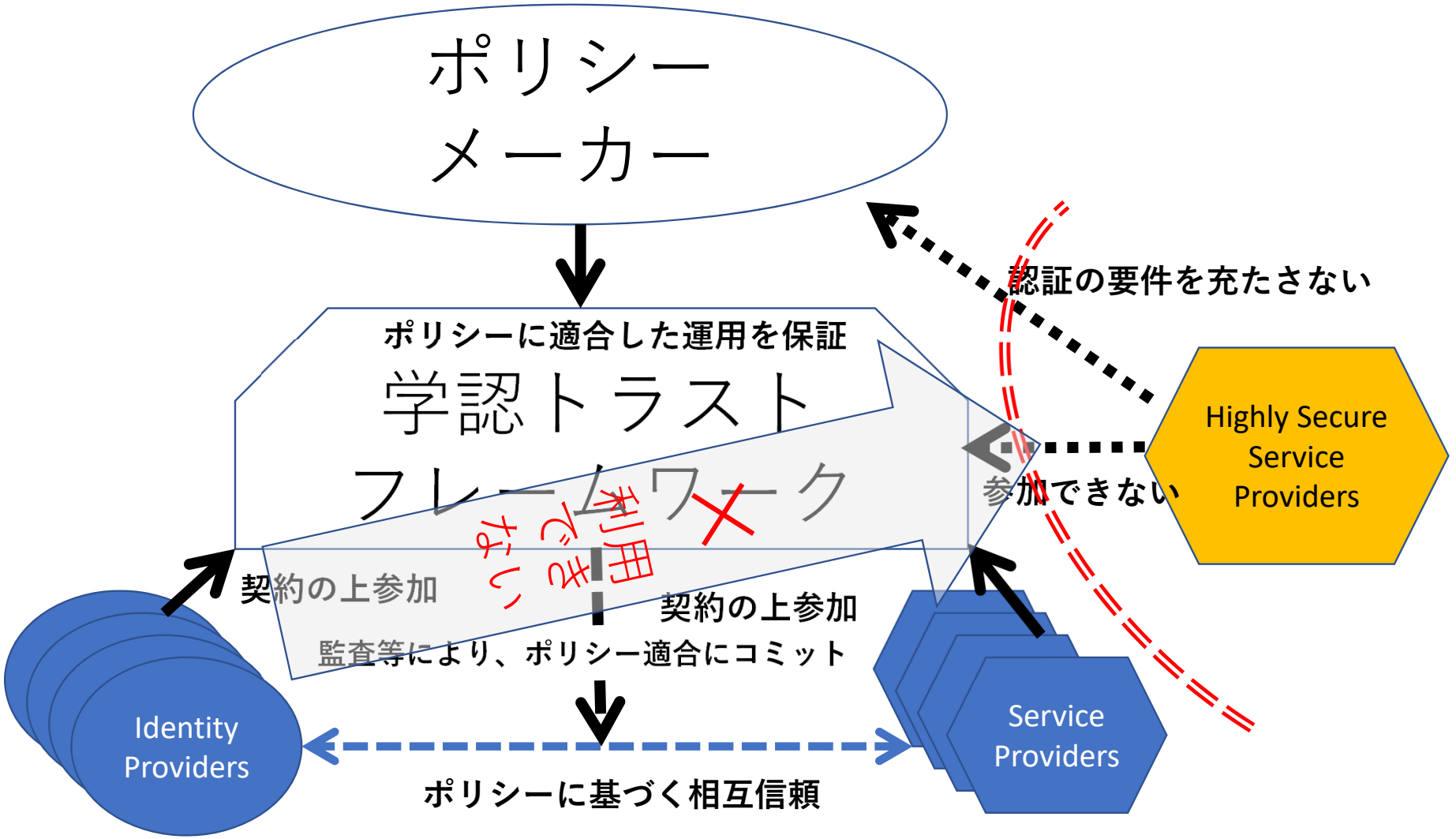

ポリシー
メーカー
ポリシーに適合した運用を保証
学認トラスト
フレームワーク
契約の上参加
契約の上参加
監査等により、ポリシー適合にコミット
Identity
Providers
Service
Providers
ポリシーに基づく相互信頼

現状トラストフレームワークの外にあるもの

- 一方、セキュリティ的に強い措置を必要とするような情報・計算リソースがサービスされるようになっています

- スーパーコンピュータのリソース
- 研究管理基盤等

- セキュリティの担保のために、運用側はコストをかけて身元確認と高度な認証手段（e.g. 生体認証、公開鍵認証）を運用せざるを得なくなっています


ポリシー
メーカー
ポリシーに適合した運用を保証
学認トラスト
フレームワーク
認証の要件を充たさない
Highly Secure
Service
Providers
参加できない
契約の上参加
契約の上参加
監査等により、ポリシー適合にコミット
Identity
Providers
Service
Providers
ポリシーに基づく相互信頼

- さらに、研究分野ごとに情報・計算リソースを運用して、分野のコミュニティのメンバーにサービスするようになりました

- ここでは、大学等機関に属しない人もメンバーとして重要な役割を持っています
  - この身元確認をどのようにするかについて、推薦制をはじめとする様々なノウハウの蓄積が行われてきました

- ここでも、セキュリティの担保のためにコストをかけて高度な認証を運用しています


HPCI High Performance Computing Infrastructure
English
サイト内検索
詳細検索
HPCIについて
利用案内・申請
利用支援
HPCI研究成果
イベント・講習会
広報
2020年
10月31日
OPEN!
HPCI広報サイト
https://mits.nims.go.jp
https://rdm.nii.ac.jp
GakuNin RDM
検索
所属している機関
GakuNin RDM
データ管理による研究推進と研究公正
DICE
MatNavi
データサービス
DICEとは
利用方法
お知らせ
目的別ショートカット
計算機利用の流れを知りたい
使える計算機について知りたい
NIMS 物質・材料データベース (MatNavi)
NIMS 物質・材料データベース(MatNavi)は、新材料の開発、材料の選択に貢献することを目的としています。MatNaviは、高分子デー
性、NMRスペクトル・・・)、無機材料データベース(結晶構造、状態図、物性・・・) 、金属材料データベース(密度、弾性係数、クリ
造計算データベース(第一原理計算によるバンド構造・・・)など、十数種類の材料データベースで構成された統合データベースシステム
ステムのようなアプリケーションも提供しています。これらのデータベースはユーザ登録を行えば、無料で各種データベースを検索・閲
報学研究所（NII）がサービスを提供しているものであり、利用にあた
、利用機関が定めた規程が適用されます。また、GakuNin RDMでは
キーを利用しております。GakuNin RDMをご利用されるお客様は、
「同意する」をクリックまたは当サイトの利用を継続されることで、
MatNaviユーザ登録・認証システム移行に関するお知らせ
NIMS物質・材料データベース(MatNavi)は更なるセキュリティ強化のため、2020年12月1日にMatNaviユーザ登録・認証システムを含
11/30以前にユーザ登録された方は、再度ユーザ登録が必要になります。
旧システムにご登録いただいたユーザ情報につきましては、全て破棄され、ユーザ登録は無効となります。
皆様には大変ご不便とお手数をおかけ致しますが、ご対応のほどお願い申し上げます。

学認参加のIdP

- 学認は、参加機関のIdPが運用するアカウントが、これらの高度なサービスへの認証として、十分利用可能なものであると信じています
- 大学や参加機関は「信頼の起点」（オーソリティ）になることができます
  - アカウント管理の信頼をそこに求めることで、そのアカウントでの認証を「高度なサービス」側に信頼してもらうことができるでしょう
  - もちろん、IdPの側でも、高度な認証器の運用等、信頼を高める証拠を固めることが必要になります

学認 Has a Dream…

- 一定の保証があれば（全員はカバーしないにしても）大学のアカウントから、スーパーコンピュータへの利用申請やクレデンシャルの配布がオンラインで行える
- **大学のアカウントの価値を高める**

- サービス提供側が、従来スケールしない形で運用してきたアカウント管理を、IdP側に委託できる
- **サービス側の運用コストを最適化する**

次世代学認の責任

- 次世代学認は、「強い」IdPと「強い」SPの間で交換される「認証の強い保証度」を決めるためのトラストフレームワークのサービスを行います
  - これこそが次世代認証基盤です

- 「大学アカウントの価値を高めます」「研究者にとって、高度なサービスがより便利に利用可能になります」
- **国内外の研究コミュニティの信頼に足る認証基盤を提供する**

基本技術

- このような次世代認証基盤の実現にむけて

- 多要素認証をはじめとする、高度な認証器での認証が求められるでしょう
- （オーソリティの起点としての大学の）「信頼されるDB」の運用も求められるでしょう
- これらを評価するための技術の開発も必須です
- もちろん国際的な連携も求められます
- ⇒これらについては、ロードマップを用意します

- 身元確認の方法の基準
- 本人確認の方法の基準（認証器の運用の強度とそれにともなう認証の保証度）

⇒　基準文書（ポリシー）の策定と運用（IAL2とAAL2について作業が進んでいます）

- ⇒これらについては、世界的な基準が作られ、定期的に改訂されています（NIST等）
- 学認では、これらを教育研究機関で現実的に運用するために、世界基準と相互運用可能な「**学認基準**」を運用します

技術開発

- 一方、既存の基準や技術では高度な認証の普及にいまいち結びついていないことも事実でした
- ⇒運用の難しさ（コスト、スケーラビリティ）、標準的な技法の不存在（ノウハウ頼み）

- 次世代学認は、これらの問題を解決するために、技術の研究と開発とそれに基づくサービスの提供を精力的に行います

  - オーソリティのための標準モデル
  - 低コスト運用モデルとパッケージの提供

技術開発（続き）

- 申請文書と証拠の電子化とそのためのPKIの提供
- 高度な認証器運用のためのスケーラブルなフレームワーク

- （身元確認の拡張としての）研究者異動にもとづく引っ越しサービス

- 評価技術、リスク管理の方法論の開発
- **高保証度（High Assurance）の世界的に相互運用性を持った認定制度とコンサルティング**

終わりに

- 次世代学認の提供する認証基盤の目的は以下の通りです

- 大学のアカウントの価値を高める
- 研究者にとって、高度なサービスが次世代学認のもと、より便利に利用可能になる
- サービス提供者の認証に関する運用を最適化する

- そのためのサービスをできるだけ早期に投入したいと考えています