デジタル証明書の意義と課題

阿部涼介

慶應義塾大学大学院 政策・メディア研究科 特任助教
Trusted Web 推進協議会 タスクフォース 構成員
WIDEプロジェクト ボードメンバ

2024/12/11 @ AXIES2024『デジタルキャンパスを支える認証インフラの展望』

自己紹介

阿部涼介 (あべ りょうすけ, chike)

- 修士（政策・メディア）
- 慶應義塾大学大学院 政策・メディア研究科 特任助教 (2022.4 ~)
- WIDE Project Board Member (2022.3 ~)
- Trusted Web推進協議会 タスクフォースメンバ (2023.04 ~)

- 2016年よりブロックチェーン関連技術の研究に従事

➡ **情報の検証可能性を担保するシステムアーキテクチャ、及びその応用**

- キーワード: 検証可能性, トラスト, デジタル証明書, DID/VC, ブロックチェーン

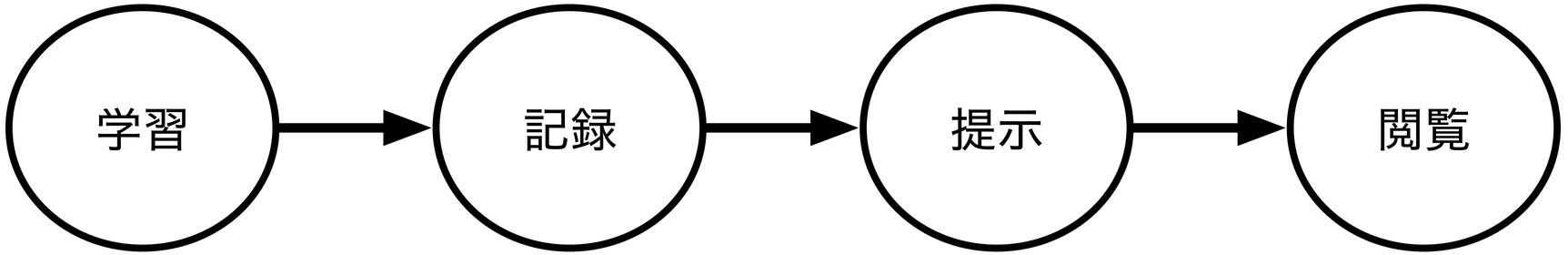
学修歴証明書のデジタル化で
何が変わるのか

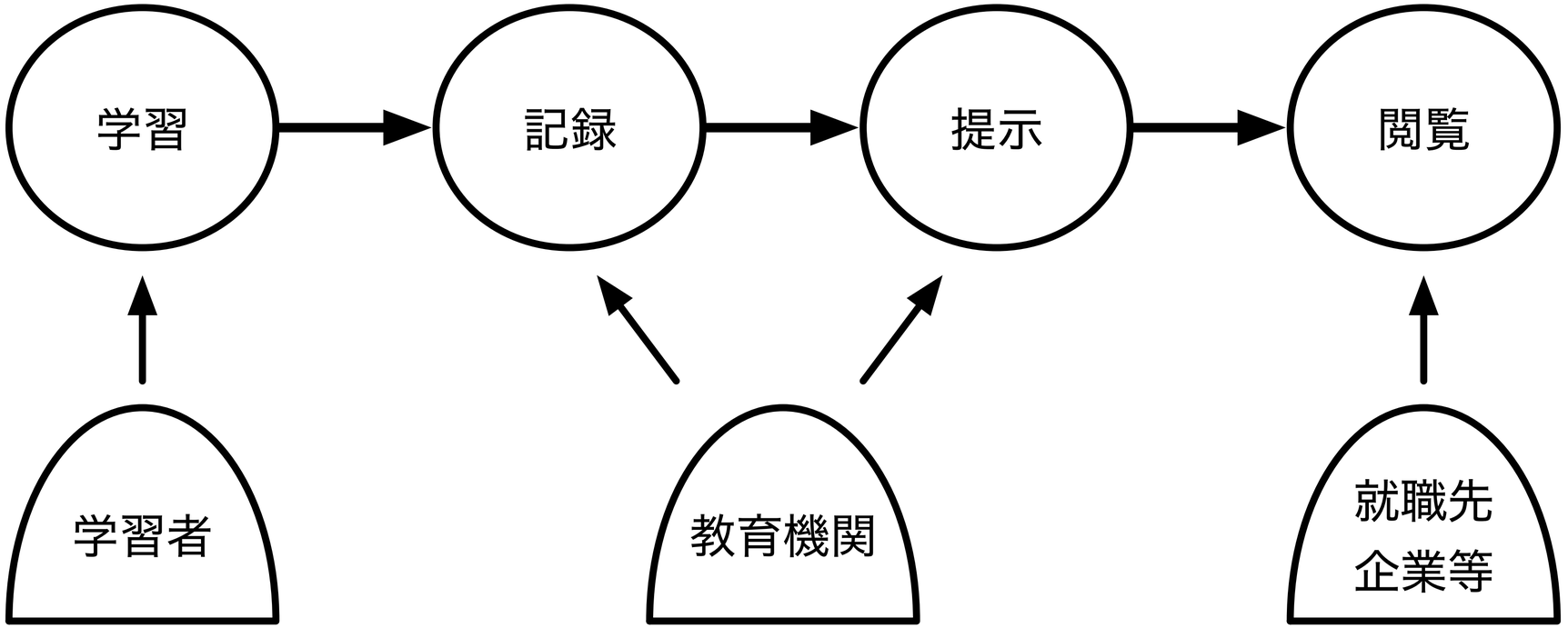
学修歴におけるステークホルダー

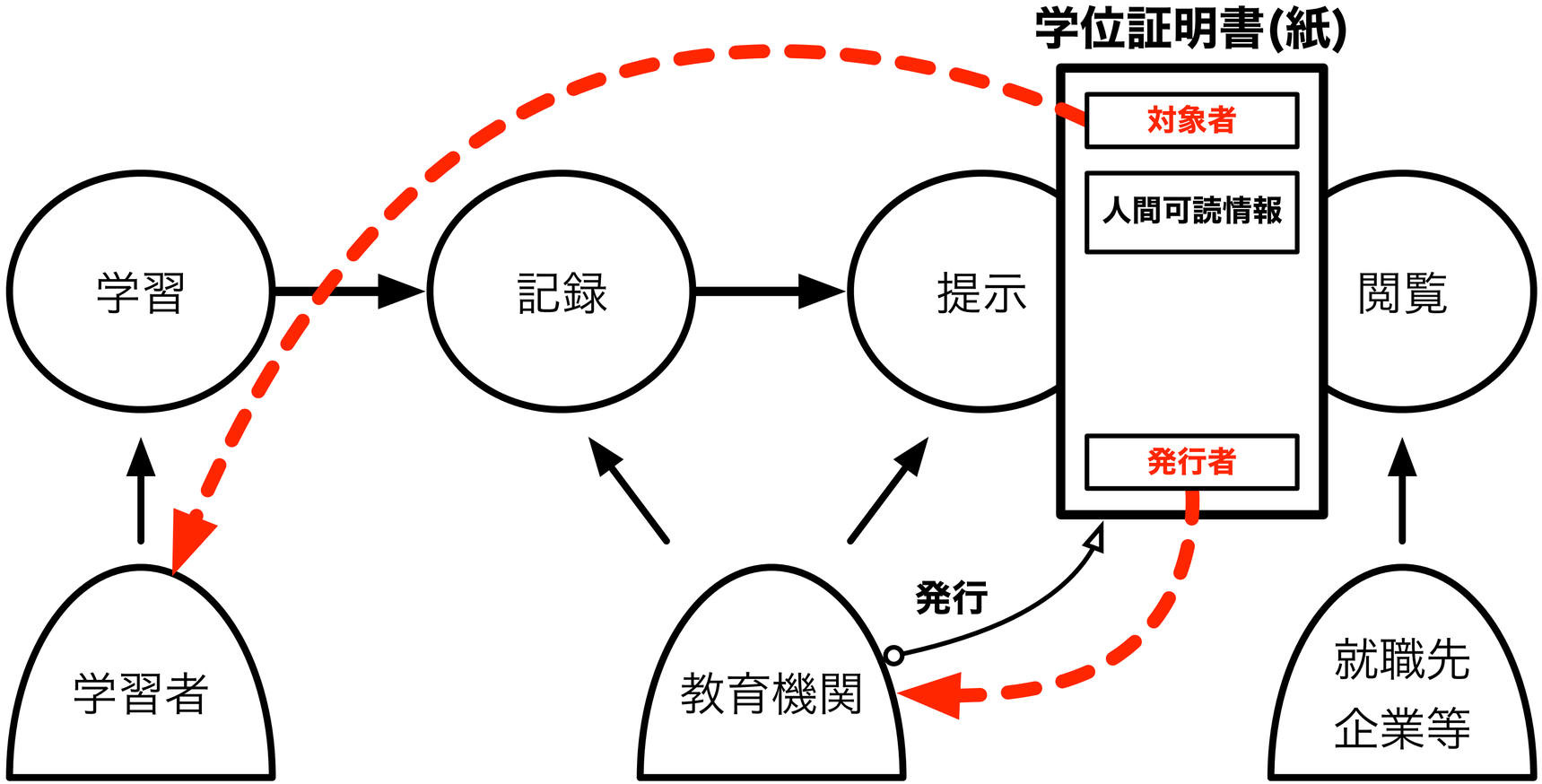
- 学習者
- 教育機関
- 学修歴を参照する者
  - 教育機関
  - 就職先企業等

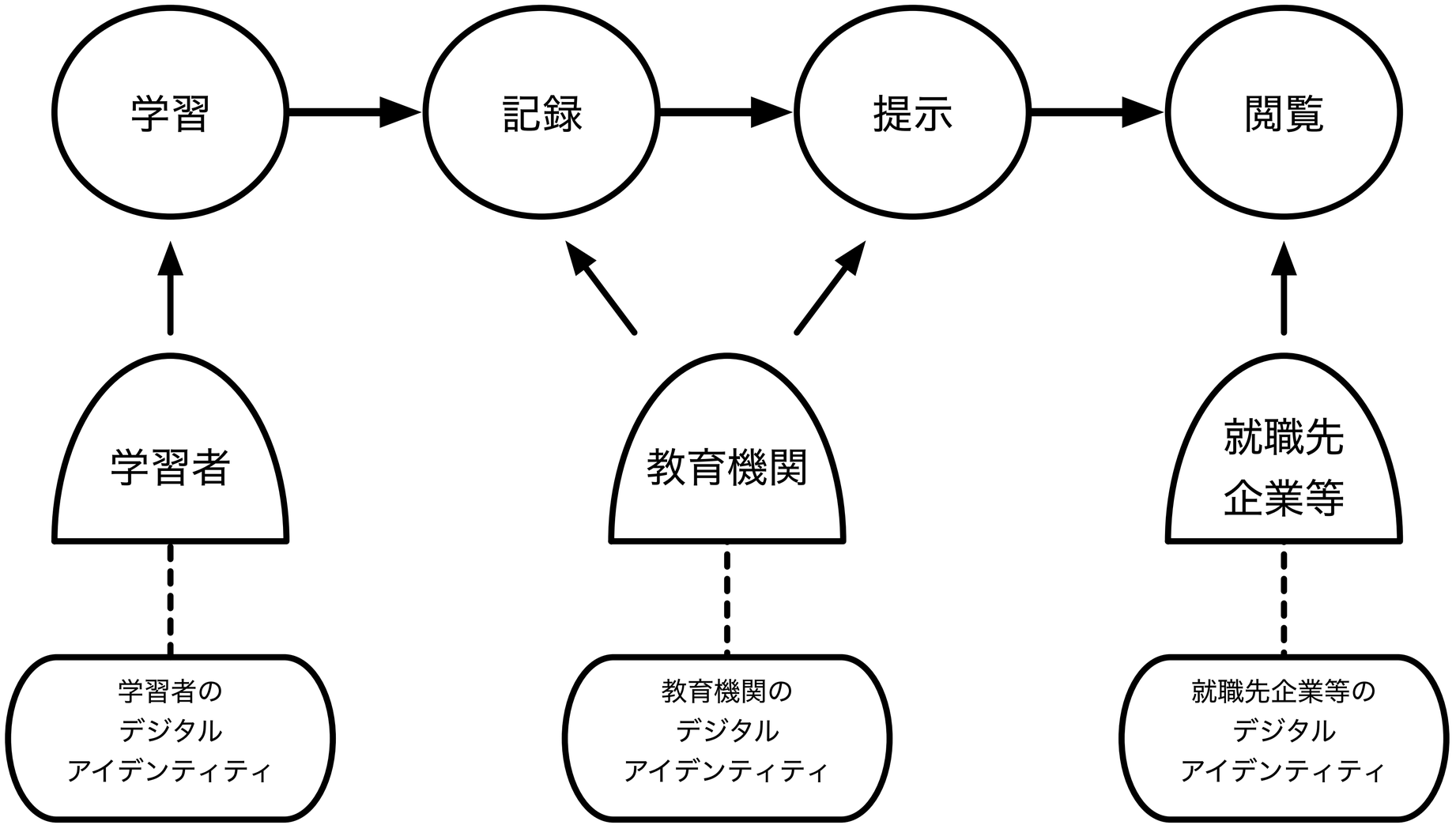
- デジタル署名された証明書の活用により、各ステークホルダが示した情報であること示せる

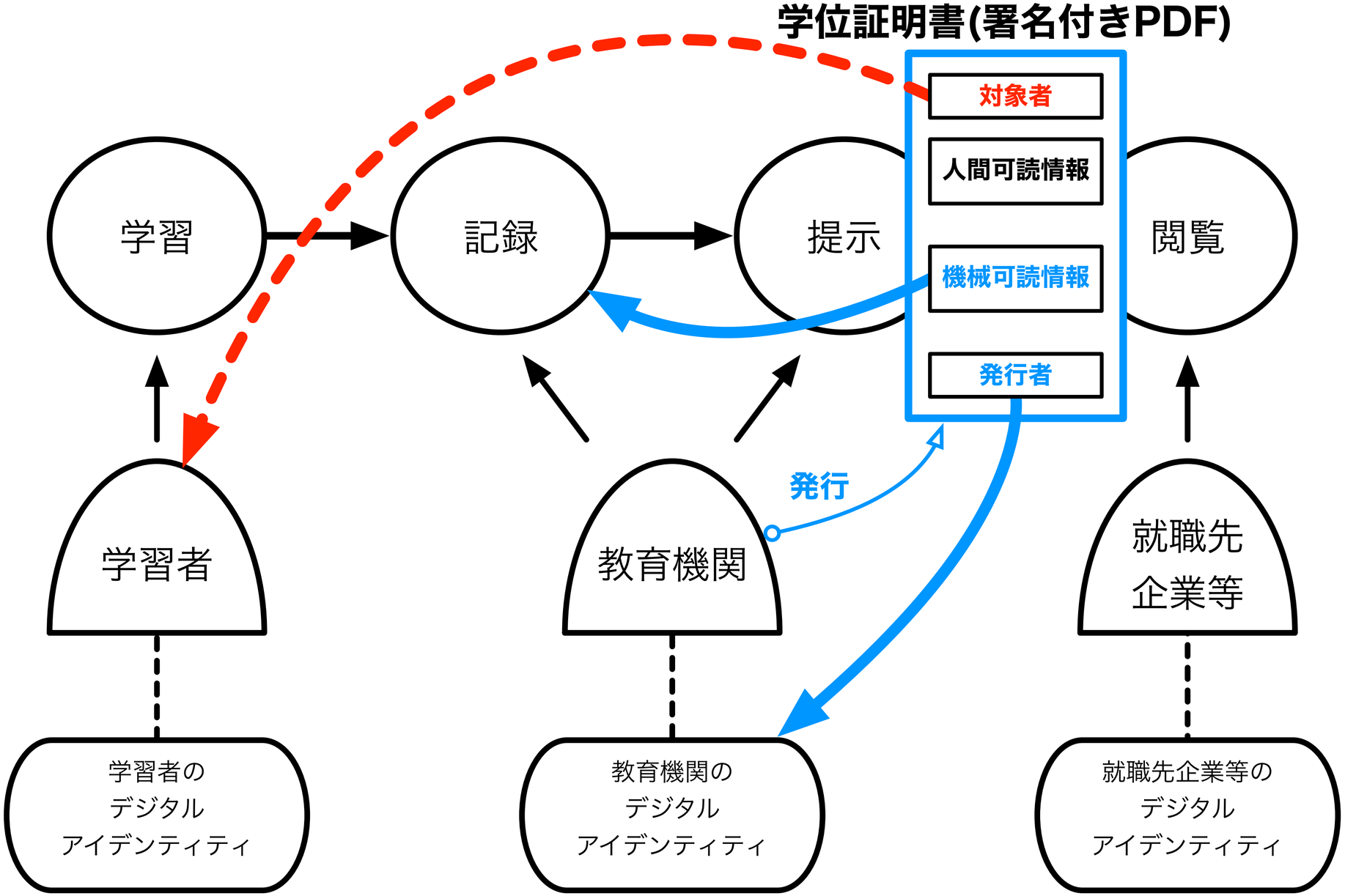
学習歴のやり取りをデジタルアイデンティティ間のやりとりとして捉える

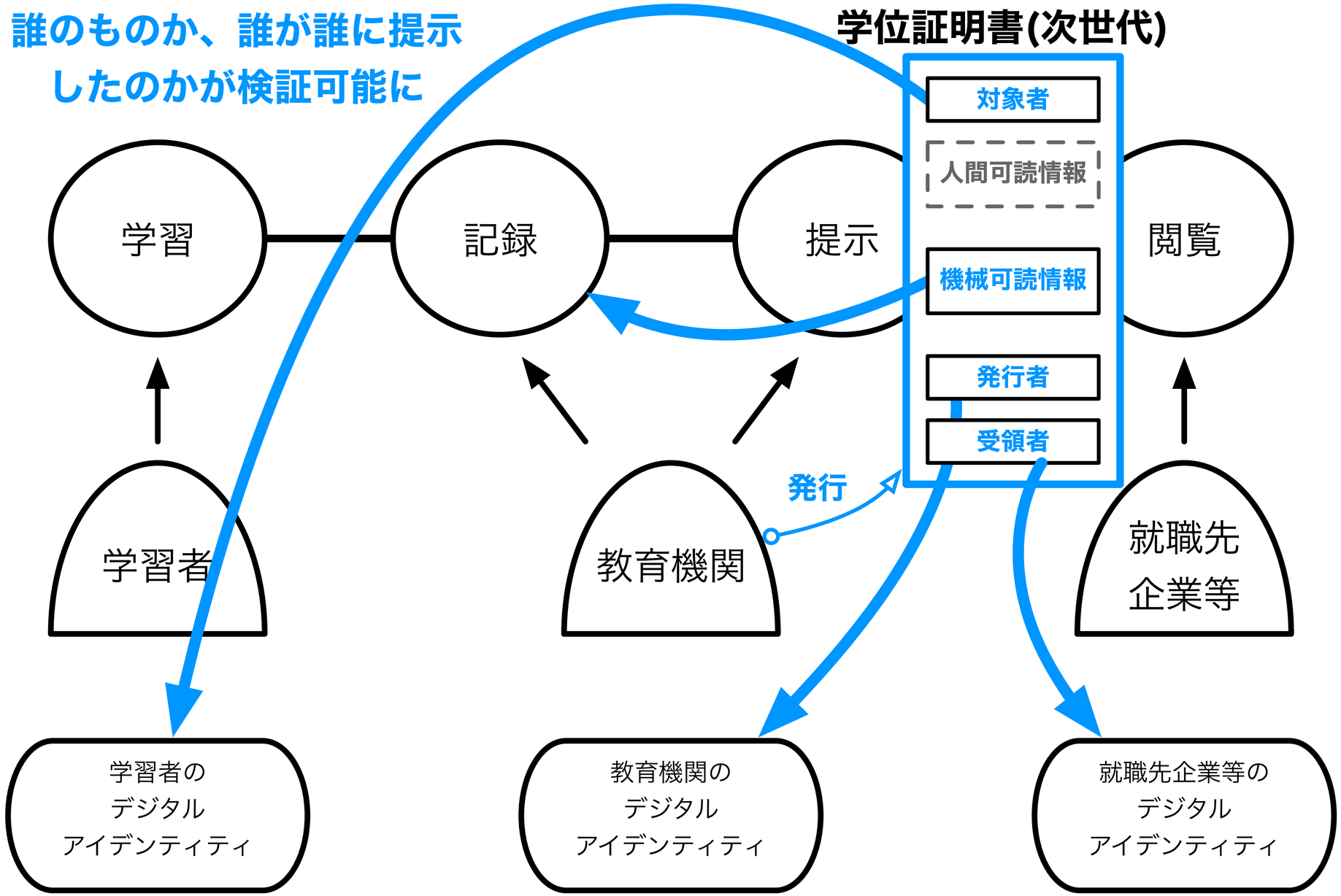


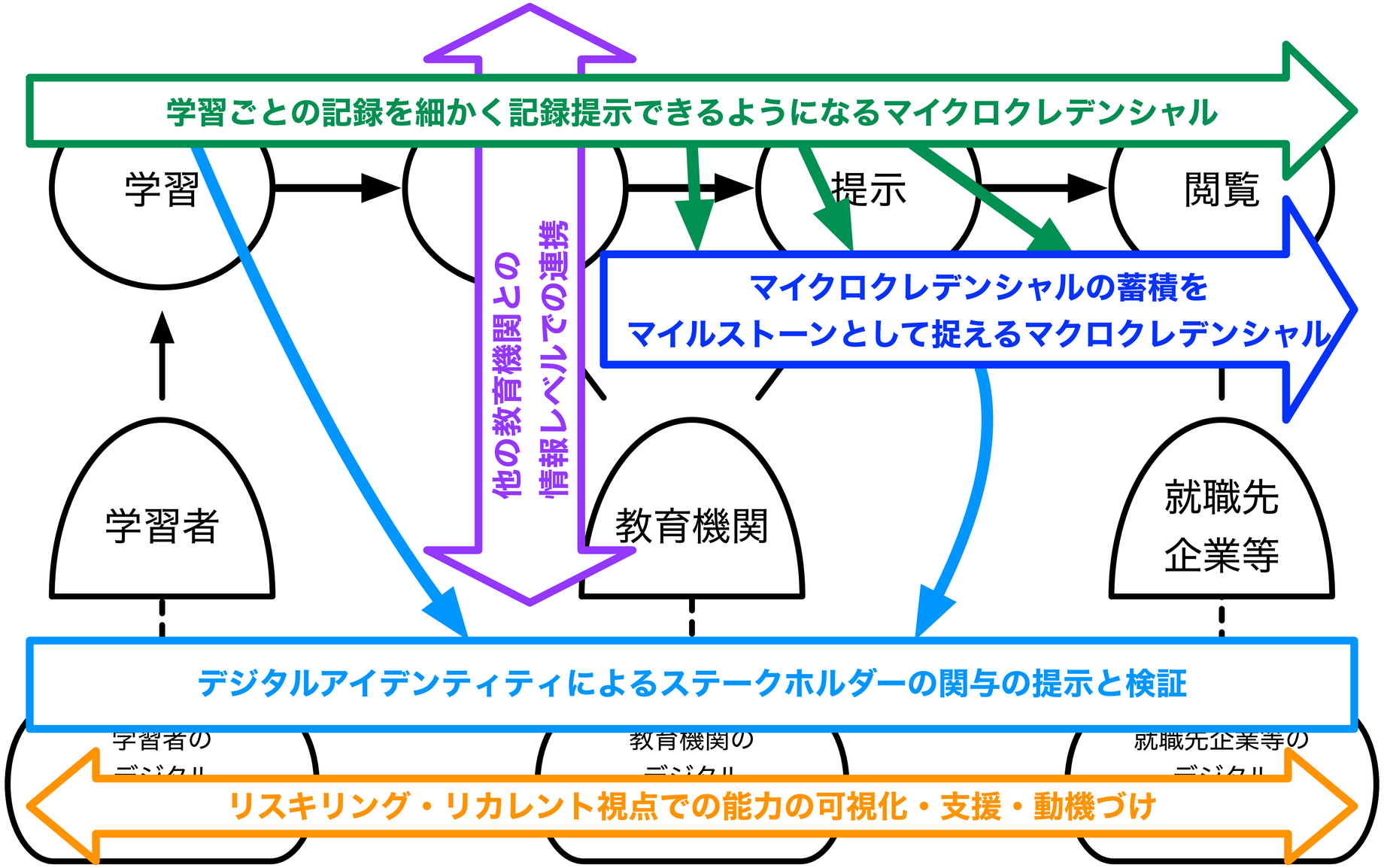












デジタル証明書の意義

- **証明書自体の《検証可能性》の段階的な高度化**

  (1) 機械可読化

  (2) 改竄検知

  (3) 発行者検証

  (4) 無効化確認

  (5) 複数の証明書の組合せによる総合的な検証 (本人確認の高度化)

  (6) 証明書提示の高度化 (選択的開示、ゼロ知識証明等)

- **エコシステムにおける活用の段階的拡大**

  (7) 証明書をやりとりできる（示せる、受け取れる）

  (8) 証明書の情報を人の関与によらずに適切に解釈し利用できる

  (9) 証明書を解釈した結果を人に頼らずに評価・比較できる

デジタル証明書の課題

- **オープンな標準と相互運用性**
  - 各種【独自】方式の乱立の結果、受取り側からすると各方式に対応する必要
    - 「証明書」というデータとして分離し、扱えることによるメリットが損なわれる

  ➡データモデルおよびトランスポートプロトコルのオープンな標準に基づく相互運用性

- **デジタルアイデンティティの確認方法**
  - デジタル化されていない本人確認も含め、どう実現できるか？
  - 確認されたアイデンティティをどう評価するか？

- **デジタル視点での最適なエコシステムデザイン**
  - 証明書ので示される情報の「解釈」をステイクホルダ間で共有できるか？
  - 実空間（リアル）とデジタル（サイバー）では、最適な方法にズレがある
    - 【ウォレット】という言葉が聞かれるが、本当に適切なのか？

「受け取り側」にとって、「なにを」「なぜ」証明書で検証できるのか
また、「相互運用」ができるのか、という視点が極めて重要