デジタル証明書の技術

京都産業大学
秋山　豊和

自己紹介：秋山 豊和

- 職歴
  - 2000年 大阪大学 サイバーメディアセンター
    - キャンパスネットワークの構築・運用
    - 認証基盤システムの構築・運用
  - 2008年 京都産業大学 コンピュータ理工学部
  - 2018年 京都産業大学 情報理工学部
    - 情報セキュリティコース

- 関連団体等
  - 電子情報通信学会インターネットアーキテクチャ研究会（IA）
  - サイバー関西プロジェクト（CKP）
  - 産学協力研究コンソーシアムインターネット技術研究会（ITRC）
  - 国立情報学研究所（NII）学術認証運営委員会

本日の内容

- デジタル証明書とは？
  - 公開鍵暗号・デジタル署名
- デジタル証明書の基盤とその応用
  - Public Key Infrastructure (PKI: 公開鍵基盤)
  - サーバ証明書
  - Single Sign On (SSO)
- 新しいデジタル証明書の基盤
  - Verifiable Credentials (VC)

注）本資料での説明は時間の都合上，概要のみで詳細は省略しています．正確なプロトコルの動作については参考文献に示した資料等，別途資料をご確認ください

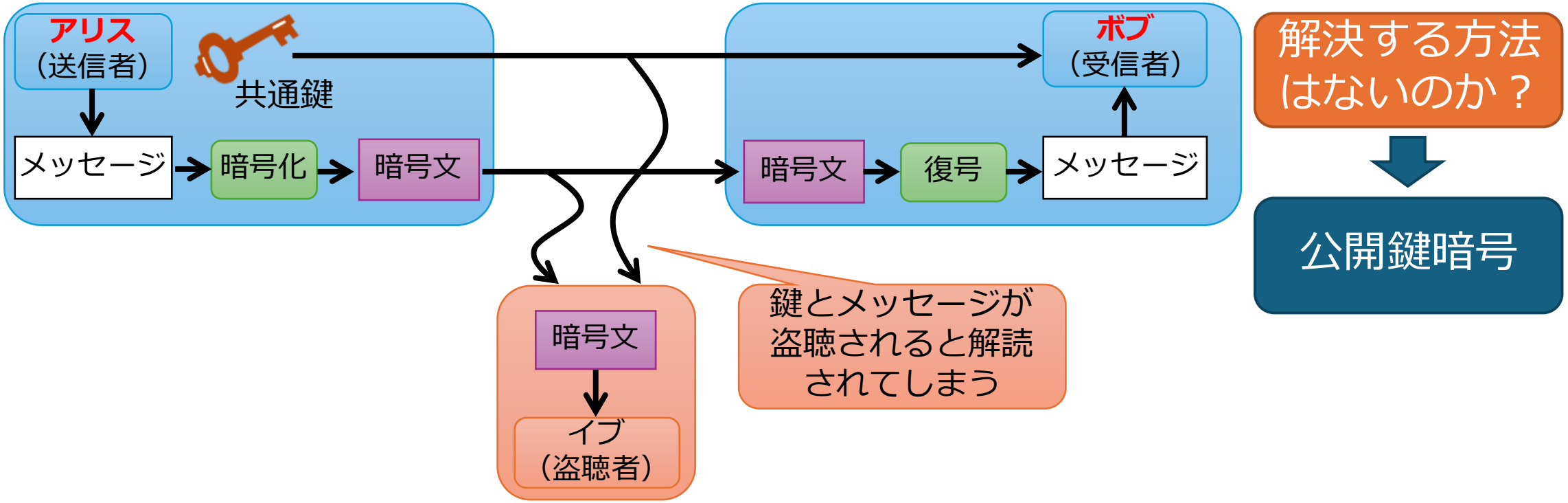
デジタル（電子）証明書とは？

- 公開鍵暗号・デジタル（電子）署名技術
  - これらの技術を活用するために登場

- 以降の説明
  - 公開鍵暗号とは？（秘密鍵と公開鍵）
  - デジタル署名とは？
  - デジタル証明書とは？
  - PKI（公開鍵基盤）とは？

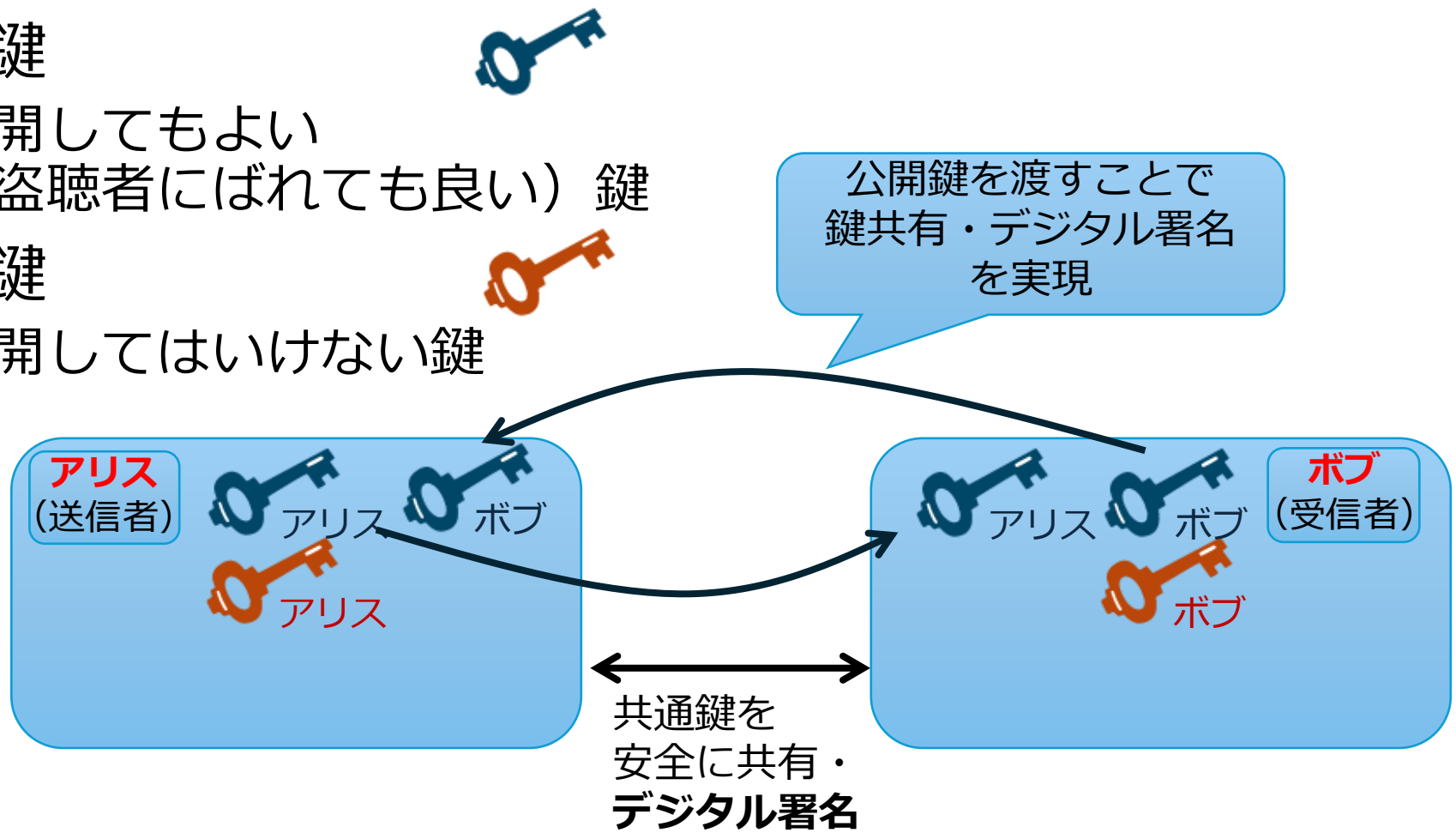
対称（共通鍵）暗号の課題

- 対称（共通鍵）暗号を使った暗号アルゴリズムの課題（鍵配送）
  - 鍵を受信者に送る必要があるが安全に送れない



公開鍵暗号[1]

- 公開鍵
  - 公開してもよい（盗聴者にばれても良い）鍵
- 秘密鍵
  - 公開してはいけない鍵

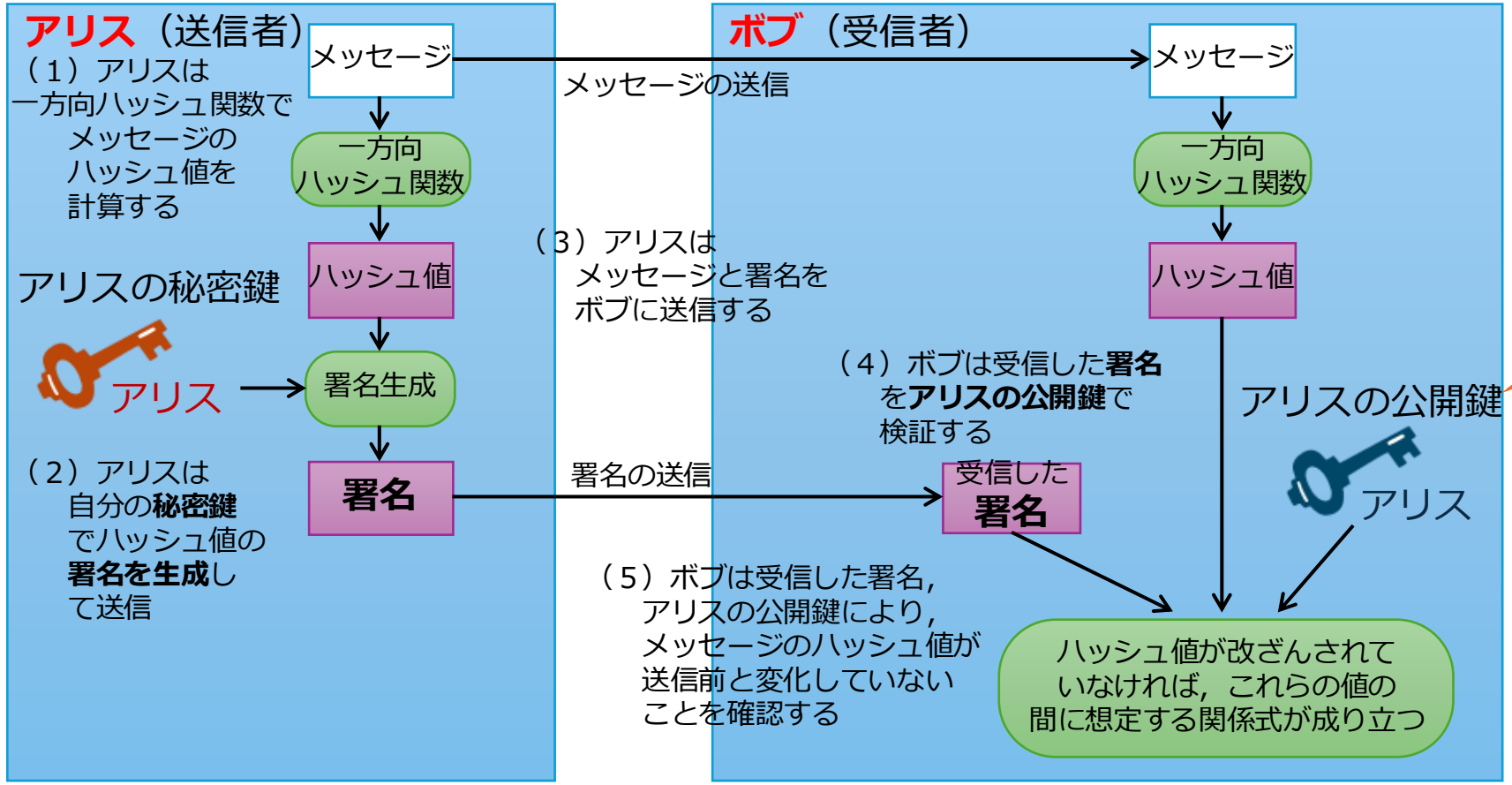


[1] W. Diffie and M. Hellman, "New directions in cryptography," in IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, November 1976, https://ieeexplore.ieee.org/document/1055638.

デジタル署名技術 [2]

以降わかりやすさのために
「秘密鍵で署名・公開鍵で検証」
という形で説明

- 公開鍵暗号を活用して署名後のメッセージの改ざんを防止



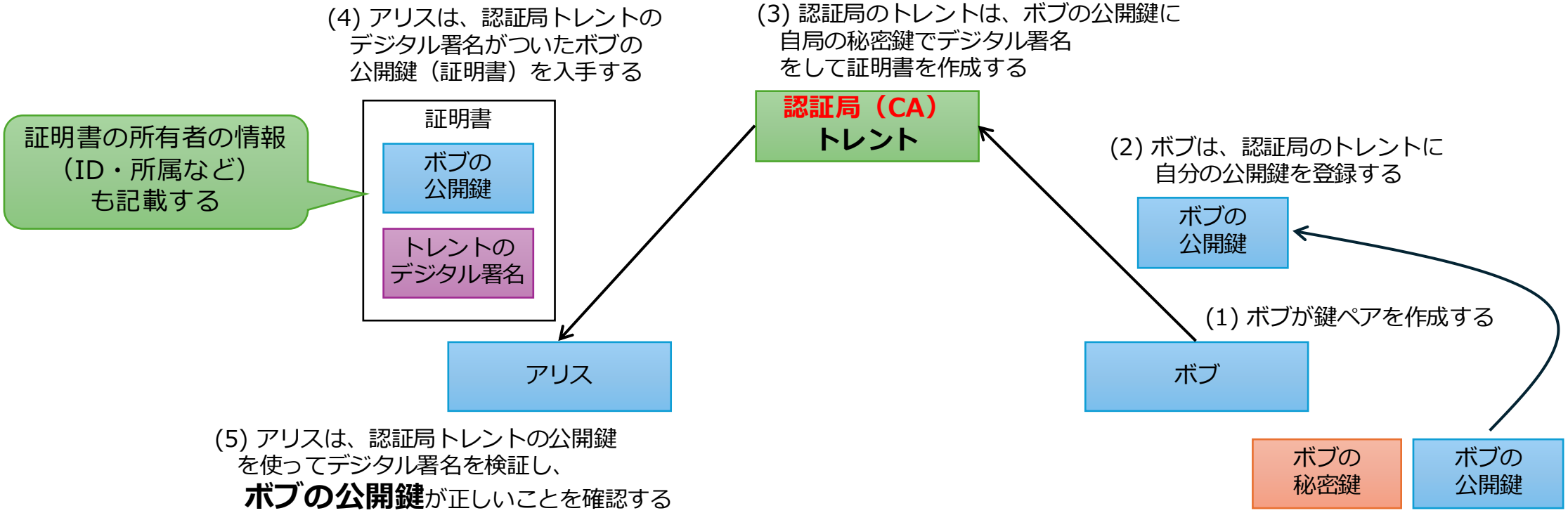
本当にアリスから
受け取った公開鍵
なのか？

[2] R. L. Rivest, A. Shamir, and L. Adleman. 1978. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 21, 2 (Feb. 1978), pp.120–126. https://dl.acm.org/doi/10.1145/359340.359342.

※これは一例でありアルゴリズムによってハッシュ値や署名の計算方法が異なるので注意

デジタル証明書[3]

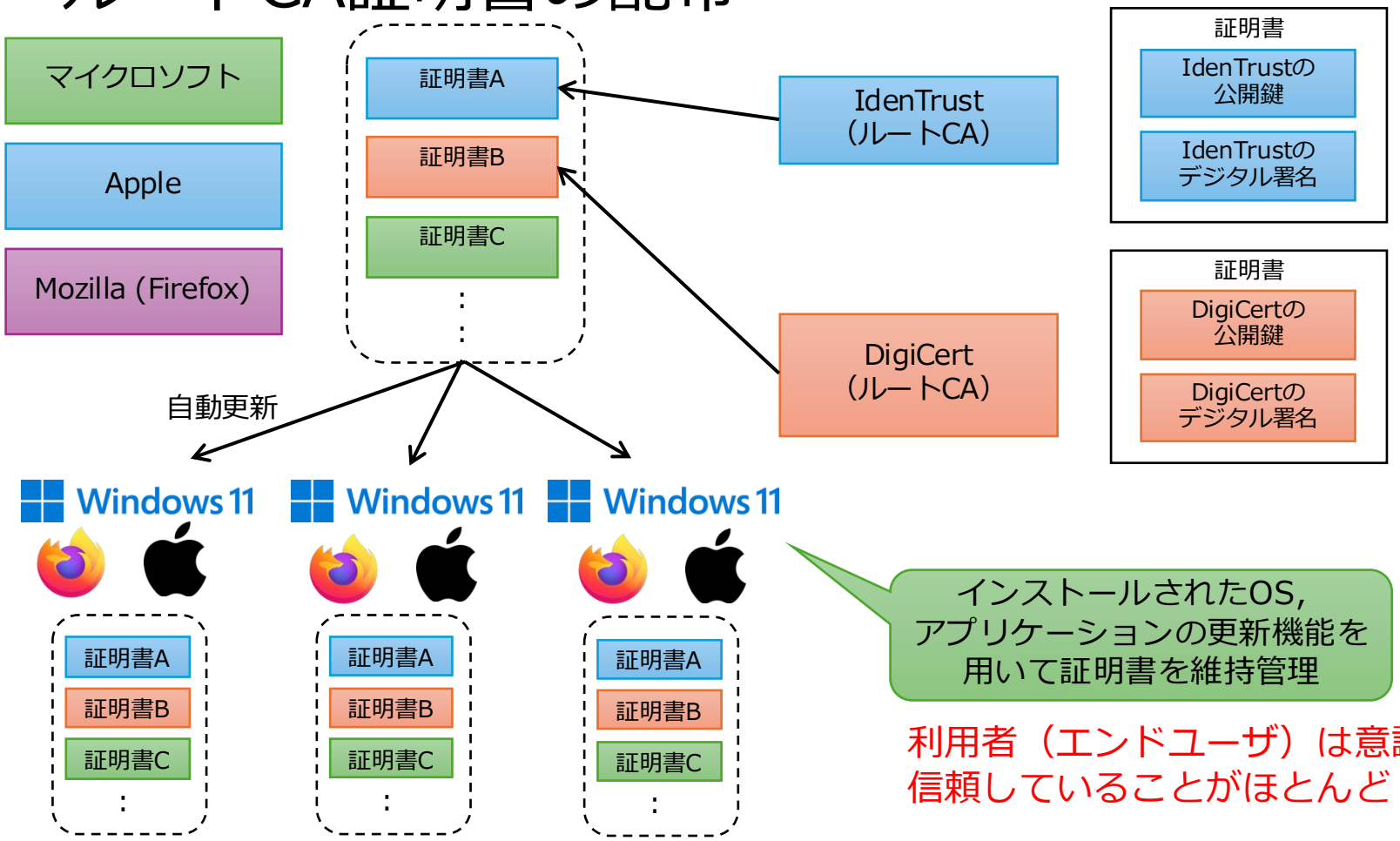
- 認証局（CA）トレントを利用して、アリスにボブの公開鍵を渡す例
  - 認証局（CA）はすべてのユーザから信頼されている（Trust AnchorであるルートCAのトレントの公開鍵（証明書）はすべてのユーザがもっている）



[3] IETF PKIX WG, Public-Key Infrastructure (X.509) (pkix), https://datatracker.ietf.org/wg/pkix/about/

Public Key Infrastructure (PKI: 公開鍵基盤)

- ルートCA証明書の配布



インストールされたOS,
アプリケーションの更新機能を
用いて証明書を維持管理

利用者（エンドユーザ）は意識せずに
信頼していることがほとんど

デジタル証明書技術の応用例

- サーバ証明書（DV証明書）
  - アクセスしているWebサーバが正しくそのドメインの所有者によって運用されていることを示す

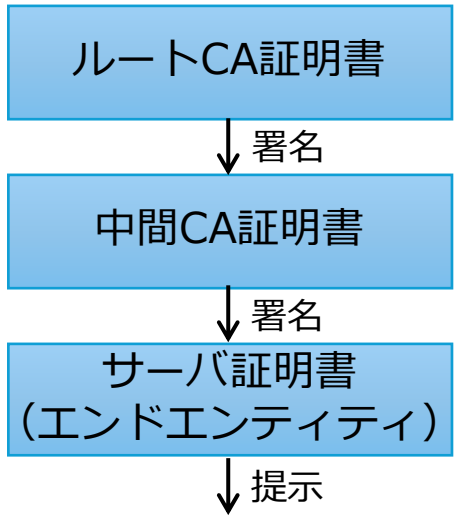
例）https://www.kyoto-su.ac.jp/ が本物のwww.kyoto-su.ac.jpであることを確認したい

証明書に記載されている内容

フィールド	内容
Subject	サーバのドメイン名（CN / SAN）
Public Key	サーバの公開鍵
Issuer	発行したCA名
Validity Period	有効期間（開始～終了）
Signature	CAの秘密鍵による署名
Serial Number	証明書の一意識別子

※さらに組織の存在確認，より厳密な
組織の審査を含むOV, EV証明書などもある

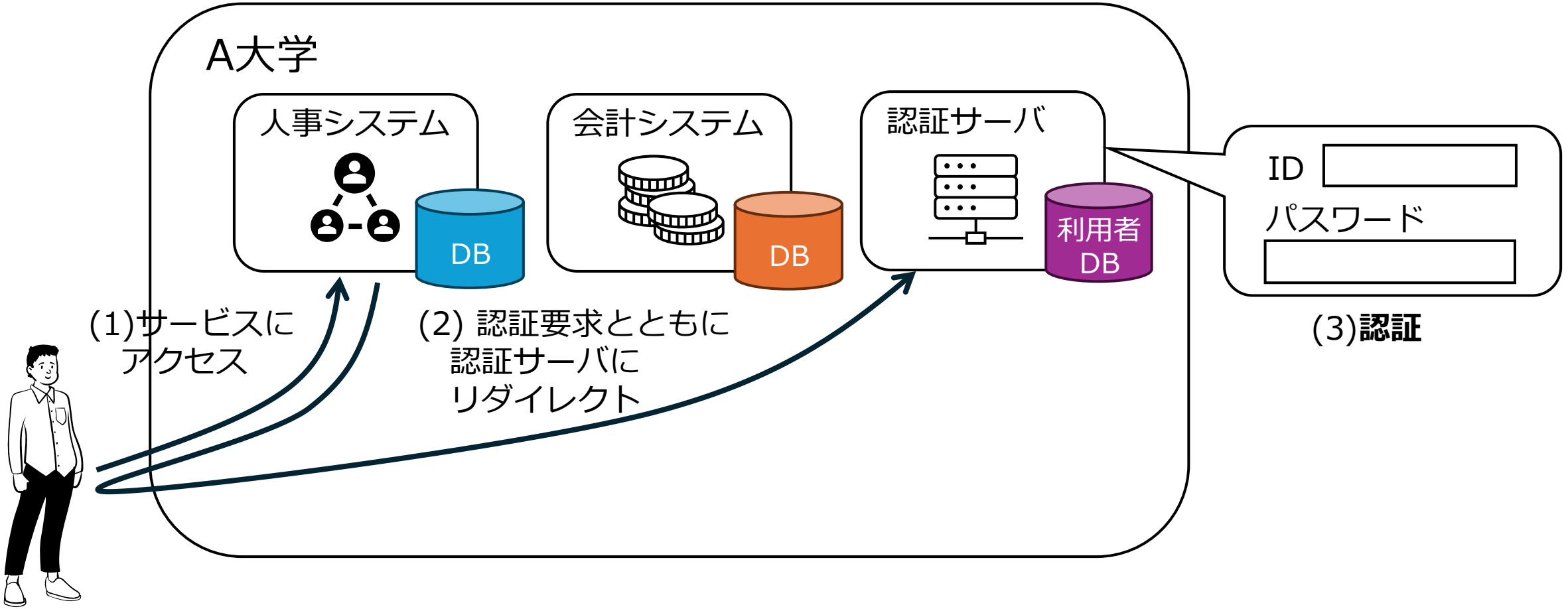
信頼チェーン（Trust Chain）



ブラウザがチェーンを検証 → 🔒 HTTPS 接続成立

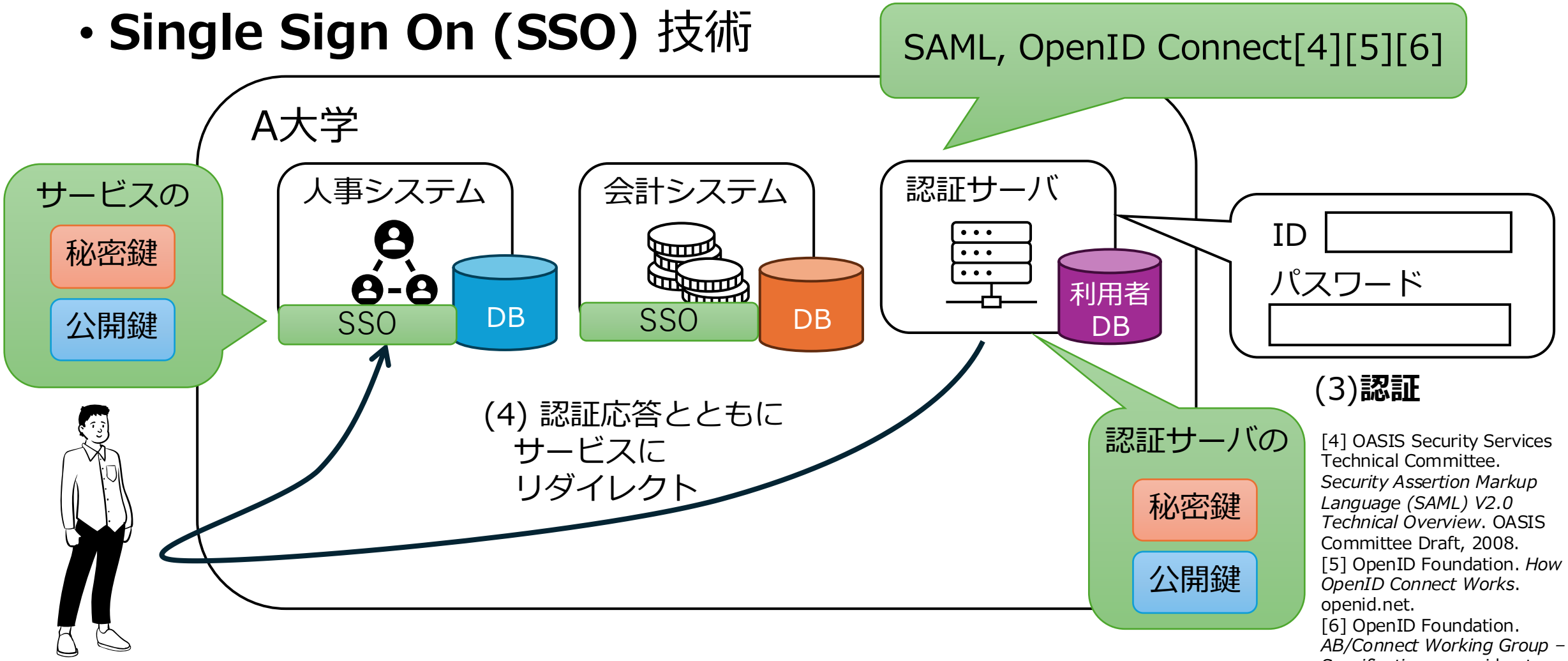
デジタル証明書技術の応用例

- **Single Sign On (SSO)** 技術



デジタル証明書技術の応用例

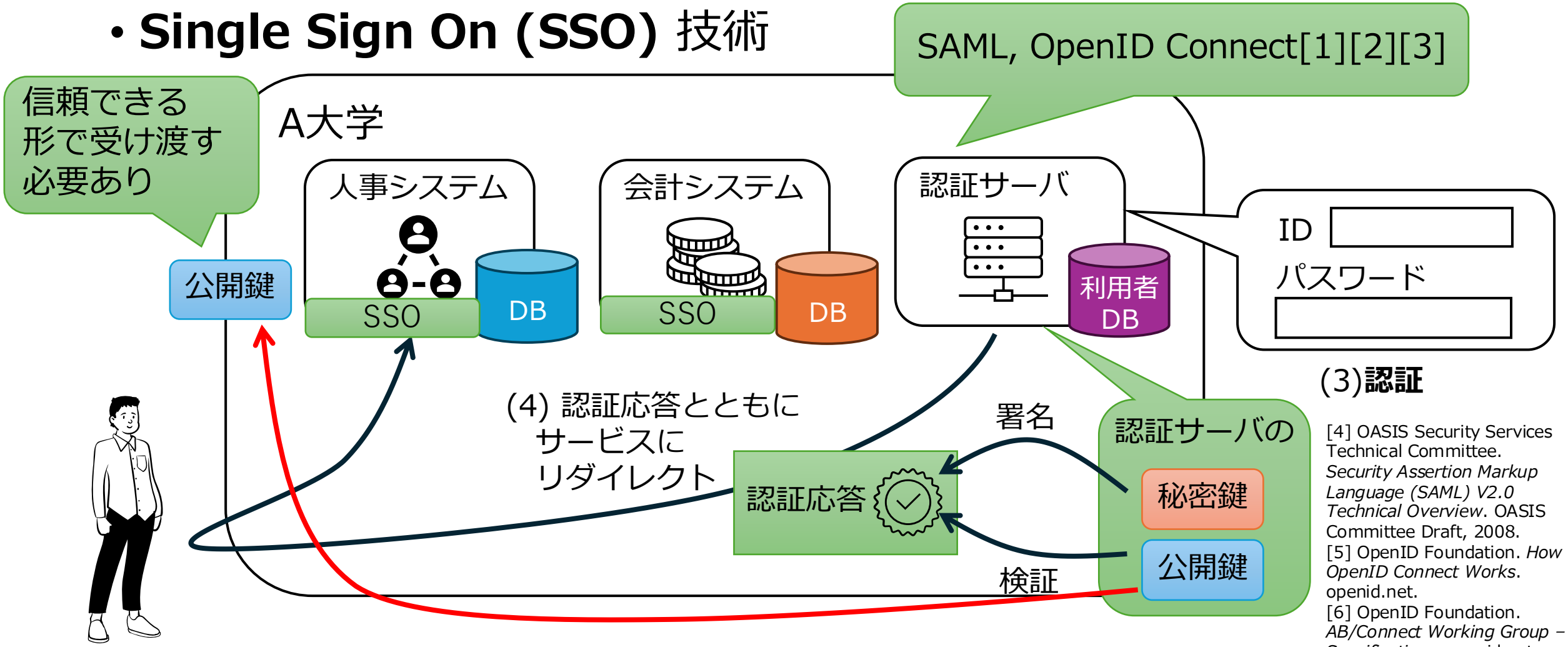
- **Single Sign On (SSO)** 技術



[4] OASIS Security Services Technical Committee. *Security Assertion Markup Language (SAML) V2.0 Technical Overview*. OASIS Committee Draft, 2008.
[5] OpenID Foundation. *How OpenID Connect Works*. openid.net.
[6] OpenID Foundation. *AB/Connect Working Group – Specifications*. openid.net.

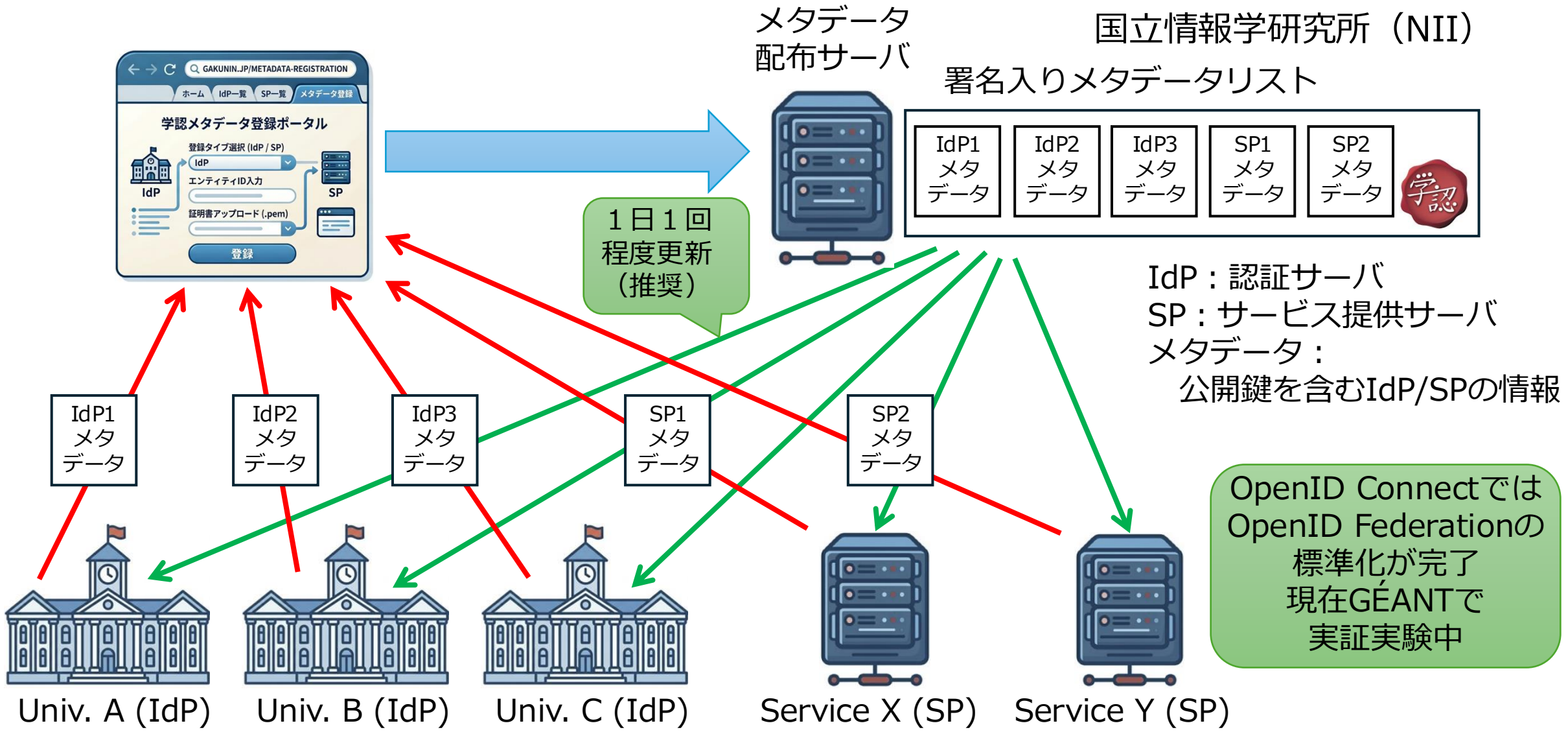
デジタル証明書技術の応用例

- **Single Sign On (SSO) 技術**



[4] OASIS Security Services Technical Committee. *Security Assertion Markup Language (SAML) V2.0 Technical Overview*. OASIS Committee Draft, 2008.
[5] OpenID Foundation. *How OpenID Connect Works*. openid.net.
[6] OpenID Foundation. *AB/Connect Working Group – Specifications*. openid.net.

フェデレーション
～学認フェデレーション（SAML）でのメタデータ配布～



フェデレーションでの信頼性

- トラストフレームワーク[7]
  - フェデレーションの参加機関の運用するIdPやSPは信頼できるのか？
  - 信頼性を担保する仕組みが必要
    - 運用規定の策定・遵守
    - アンケート評価

- 学認が目指す次世代認証連携[8][9]
  - 身元確認や当人認証をどのくらい厳密におこなっているかで信頼性を判断
    - IAL：Identity Assurance Level（身元確認のレベル）
    - AAL：Authenticator Assurance Level（当人認証のレベル）

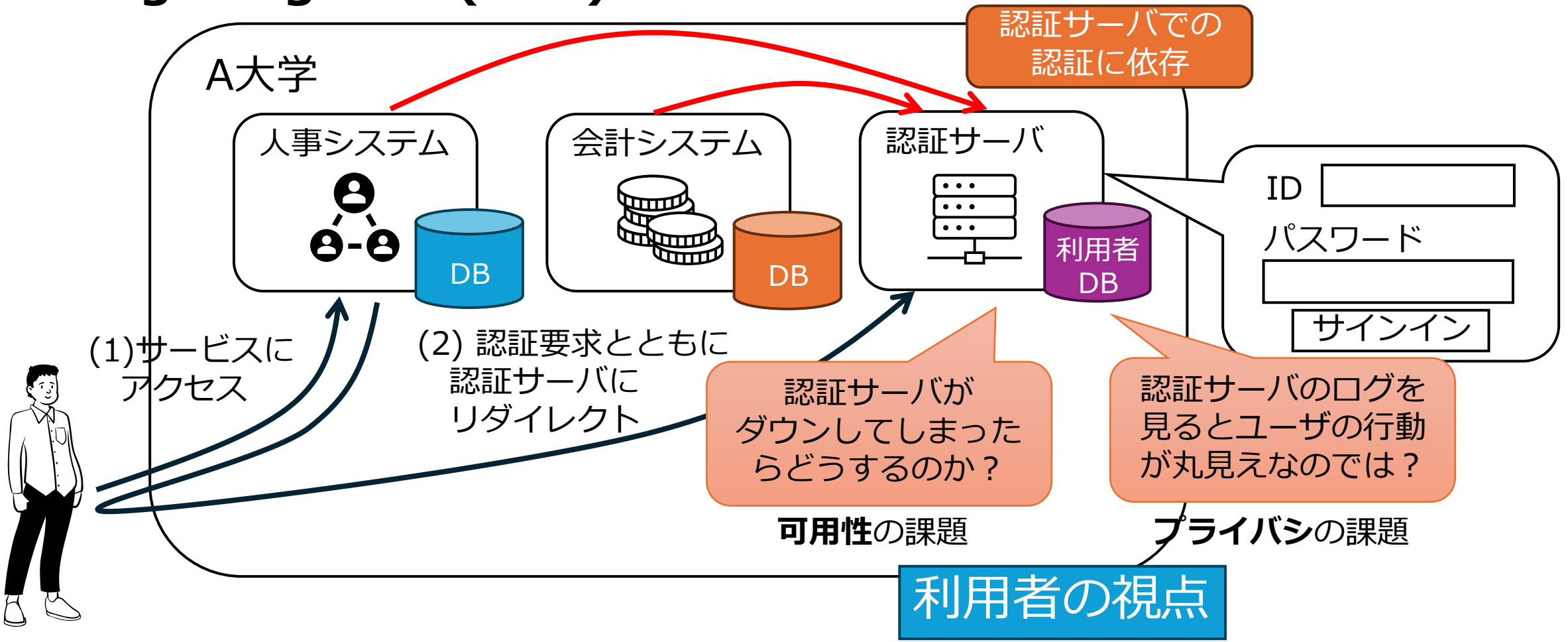
[7] 佐藤 周行，学認トラストフレームワーク，https://gakunin.jp/sites/default/files/2019-10/sato%20%281%29.pdf，（2026/6/12確認）．
[8] 坂根 栄作，学認が目指す次世代認証連携，NII 学術情報基盤オープンフォーラム 2023.
[9] 古川 英明，【解説】デジタルアイデンティティガイドライン「NIST SP 800-63」第4版ドラフトはどう変わる？＜全体編＞，https://www.nri-secure.co.jp/blog/nist-sp-800-63-4-draft01，（2026/6/12参照）．

フェデレーションの特徴

- 組織単位での信頼関係の構築・維持
  - エンドユーザはIdPの配下で管理されているという関係
- 組織ごとにポリシーを策定して信頼する組織を決定可能
  - ただし，ユーザの混乱を避けるため運用上の合意（アクセスできるサービスはどれかが分かりやすくなるように）を調整する必要あり

新しいデジタル証明書基盤について

- **Single Sign On (SSO)** 技術（振り返り）



Verifiable Credentials (VC) [10] への注目

技術的には
公開鍵による
VCへの署名の検証

発行時に署名
Issuerの
秘密鍵

Issuer
（発行者）

Issue
（発行）

Verifiable
Credential

Holder
（保持者）

Present
（提示）

Verifiable
Presentation

Verifier
（検証者）

検証に必要
Issuerの
公開鍵

認証サーバ

既存の認証基盤で認証し
資格をもつユーザに
オンラインでVCを発行
（容易な再発行）

スマートフォンアプリ
（Walletアプリ）

オフライン
での利用も可能

選択的開示により
必要な属性のみ提示
（プライバシの確保）

公開鍵基盤
（トラストフレーム
ワーク）の整備

フェデレーションに
よる整備

OID4VCI/OID4VP
トランスポートを想定した例

※注）本例はVCの一側面を示すものであり，
仕様全体を代表するものではない

[10] 富士榮尚寛, 阿部涼介, 鈴木茂哉, “学修歴デジタルクレデンシャルの現状と課題”, 会誌「情報処理」Vol.67 No.5（May 2026）「デジタルプラクティスコーナー」

VCへの期待

- VCが有効なユースケース
  - 「サービスにおいて認証サーバへの依存を回避したい」
    - オフラインでの提示・検証機能の活用
    - オンラインでVerifierにVCを提示し，検証する場合でも認証サーバに依存しない形での検証も可能
  - 「認証サーバの管理組織に、自分の行動履歴をトラッキングされたくない」
    - Issuerでの発行後の証明書提示はトラッキングされない形で実装可能（ただし，証明書検証の実装に注意が必要）
  - 「不必要な属性情報をサービス側に収集されたくない」
    - 選択的開示の機能を活用すれば本当に必要な属性の提示のみに限定可能
  - 「有効期間内に繰り返し利用する情報」（例：学生証，免許，ワクチン接種証明）
    - １度しか利用しないものではコストメリットが得られない

サービス提供者の視点
利用者の視点

利用者の視点

利用者の視点

サービス提供者の視点
利用者の視点

VCへの期待（実証実験事例）

- 「Verifiable Credentialsを活用した学生向けサービスの実証事業」（2025年3月）
  - デジタル庁・西日本旅客鉄道株式会社・国立情報学研究所（NII）・OpenIDファウンデーション・ジャパン
  - 大学が発行する**在学証明**をVCとして学生のウォレットに発行し、JR西日本が提供するチケット販売サイト等において提示することで、学割チケット購入時の学生向けサービスの社会実装を目指した実証実験。
  - 関連URL: https://www.openid.or.jp/news/2025/03/verifiable-credentials.html
- 「デジタルアイデンティティウォレットを活用した年齢確認の実証実験」. SYNCHRONICITY'25 MIDNIGHT, 東京・渋谷（2025年4月）
  - NTT Digital・NTTドコモ・NTTコミュニケーションズ・株式会社Kulture・株式会社Spincoaster
  - マイナンバーカードをトラストアンカーとし、VCとして**成人証明書**を発行・提示することで音楽イベント入場時の年齢確認を行った実証実験。イベントでの身分証明やチケット不正転売対策へのVC活用を視野に入れた取り組みとして実施された。
  - 関連URL: https://prtimes.jp/main/html/rd/p/000000024.000136141.html
- 「入退館システムでのVC化に関する実証実験」 （2025年11月）
  - 株式会社電通総研・京都産業大学
  - EUDI Walletベースの Wallet実装を用いて大学における**入退館管理**システムをオンライン、オフライン両方のプロトコルでプロトタイプを構築し、その課題について検証が行われた。
  - 関連URL: ITRC meet58 https://www.itrc.net/meet/meet58%e3%83%97%e3%83%ad%e3%82%b0%e3%83%a9%e3%83%a0%ef%bc%88%e9%9a%8f%e6%99%82%e6%9b%b4%e6%96%b0%ef%bc%89/

VCエコシステムの仕様の複雑性と今後の課題

■ 仕様スタック比較表

構成要素	スタックA Open Badges / CLR (1EdTech)	スタックB DID / VC (W3C)	スタックC（学修歴） EDC / ELM / EUDI Wallet (欧州委員会)	スタックC（ID領域） EUDI Wallet (欧州委員会)	スタックD プラットフォーム独自
識別子	IRI / DID / URL	IRI / DID / URL	IRI / DID / URL	IRI / DID / URL	独自（非標準）
トランスポート プロトコル	Open Badges独自プロトコル	定義なし	OID4VCI / OID4VP	OID4VCI / OID4VP	独自（非標準）
データモデル	W3C VCDM 2.0 利用	W3C VCDM 2.0	W3C VCDM 2.0 準拠	W3C VCDM 2.0非依存を含む	独自（非標準）
クレデンシャル フォーマット	W3C Data Integrity VC	W3C Data Integrity VC	W3C Data Integrity VC 優先	SD-JWT VC 優先 ISO/IEC 18013-5（mdoc）	独自（非標準）
セマンティクス （語彙）（学修歴）	1EdTech標準語彙	スコープ外	ELM Vocabulary	ARFによる事前合意	独自（非標準）
質保証 フレームワーク（学修歴）	スコープ外	スコープ外	EQF / QF-EHEA / ENIC-NARIC	スコープ外	独自（なし）
トラスト フレームワーク	スコープ外	スコープ外	eIDAS 2.0 / EDC / EUDIW TF	eIDAS 2.0 / EUDIW TF	独自（なし）

○ 定義あり・標準準拠　△ 部分的・独自拡張　× 未定義・スコープ外・独自仕様

■ VCエコシステムの今後の課題

① ユースケースに適した技術選定

- スタックA〜Dは技術基盤・ガバナンス・ビジネスモデルが異なる
- 識別子・プロトコル・クレデンシャルフォーマット・署名アルゴリズムなど多数の選択肢が乱立
- ユースケース（学修歴・身分証・資格）ごとに最適な技術スタックを慎重に選定する必要がある

② インターオペラビリティの確保

- スタック間・エコシステム間で実質的なサイロ化が進行
- 技術面（データモデル・語彙・プロトコル）と非技術面（質保証・トラストフレームワーク）の両軸での合意が必要
- 国境を跨いだ越境シナリオでは各国トラストフレームワーク同士の連携も不可欠

③ 統一されたユーザ体験（UX）の提供

- 技術スタックが異なっても、利用者・検証者が混乱しない一貫したUXの設計が理想
- ウォレット・プロトコル・提示フローの差異をユーザから隠蔽する抽象化レイヤが求められる
- 発行者中心の議論から脱し、検証者・保持者視点のエコシステム設計へのシフトが急務

参考：[10] 富士榮尚寛, 阿部涼介, 鈴木茂哉, “学修歴デジタルクレデンシャルの現状と課題”, 情報処理 Vol.67 No.5 (May 2026)　※ID領域関連の部分を追記

まとめ

- デジタル証明書とは？
  - 公開鍵暗号・デジタル署名
- デジタル証明書の基盤とその応用
  - Public Key Infrastructure (PKI: 公開鍵基盤)
  - サーバ証明書
  - Single Sign On (SSO)
- 新しいデジタル証明書の基盤
  - Verifiable Credentials (VC)

参考文献

- 公開鍵暗号

  [1] W. Diffie and M. Hellman, "New directions in cryptography," in IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, November 1976, https://ieeexplore.ieee.org/document/1055638.

- デジタル署名

  [2] R. L. Rivest, A. Shamir, and L. Adleman. 1978. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 21, 2 (Feb. 1978), pp.120–126. https://dl.acm.org/doi/10.1145/359340.359342.

- デジタル証明書

  [3] IETF PKIX WG, Public-Key Infrastructure (X.509) (pkix), https://datatracker.ietf.org/wg/pkix/about/

- SAML・SAMLフェデレーション

  [4] OASIS Security Services Technical Committee. *Security Assertion Markup Language (SAML) V2.0 Technical Overview*. OASIS Committee Draft, 2008. https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html, (2026/06/12確認).

参考文献

- OpenID Connect・OpenID Federation
  [5] OpenID Foundation. *How OpenID Connect Works*. openid.net. https://openid.net/developers/how-connect-works/, (2026/06/12確認).
  [6] OpenID Foundation. *AB/Connect Working Group – Specifications*. openid.net. https://openid.net/wg/connect/specifications/, (2026/06/12確認).
- フェデレーション
  [7] 佐藤 周行，学認トラストフレームワーク, https://gakunin.jp/sites/default/files/2019-10/sato%20%281%29.pdf, （2026/6/12確認）.
  [8] 坂根 栄作，学認が目指す次世代認証連携，NII 学術情報基盤オープンフォーラム 2023.
  [9] 古川 英明，【解説】デジタルアイデンティティガイドライン「NIST SP 800-63」第4版ドラフトはどう変わる？<全体編>，https://www.nri-secure.co.jp/blog/nist-sp-800-63-4-draft01,（2026/6/12参照）.
- Verifiable Credentials (VC)
  [10] 富士榮尚寛, 阿部涼介, 鈴木茂哉, “学修歴デジタルクレデンシャルの現状と課題”, 会誌「情報処理」Vol.67 No.5（May 2026）「デジタルプラクティスコーナー」