Trusted Web とリスキリング

鈴木茂哉

慶應義塾大学大学院政策・メディア研究科 特任教授
慶応義塾大学SFC研究所データアーキテクチャラボ 副所長（技術統括)
Trusted Web 推進協議会 タスクフォース 構成員
Originator Profile 技術研究組合 技術開発WG 部会長

2024/10/19 @ TIESシンポジウム2024『学び続ける未来のために―リスキリングの危機を越えて』

鈴木 茂哉

慶應義塾大学大学院 政策・メディア研究科 特任教授 / 博士 (政策・メディア)

Shigeya Suzuki, Ph.D

Project Professor,
Graduate School of Media and Governance, Keio University

shigeya@wide.ad.jp
shigeya@keio.jp

主たる研究領域

ネットワーク化されたセキュアな情報システムの設計 / 開発 / 構築

情報システムアーキテクチャ / コンピューターネットワーク / 分散システム / デジタルアイデンティティ / ネットワークシステムセキュリティ / 量子インターネット

現在の主たる肩書き・活動等

慶應義塾大学SFC研究所 データーアーキテクチャラボ 副所長(技術統括)

慶應義塾大学SFC研究所 トラステッド・インターネット・アーキテクチャ・ラボ 副所長

慶應義塾大学SFC研究所 Auto-ID Labs Japan副所長

WIDEプロジェクト ボードメンバ/研究者

Trusted Web推進協議会タスクフォースメンバ
(内閣官房デジタル市場競争会議)

W3C DID WG / VC WG / Credentials CCG メンバ

Rebooting the Web of Trust, Board Member

Originator Profile技術研究組合 技術開発WG部会長

Recent Papers and Other works 最近の主な研究業績

Mitigation of Seller and Buyer's Dilemma with Transaction History and Escrow *(2023)*
Ryosuke Abe, Seiyo Kurita, Mariko Kobayashi, Shigeya Suzuki
AINTEC'22: The 17th Asian Internet Engineering Conference, Hanoi, Vietnam
BEST PAPER AWARD Blockchain

Trusted Web ホワイトペーパ Ver.3.0 *(2023)*
Trusted Web推進協議会 (内閣官房デジタル市場競争会議)
Identity Privacy Blockchain Member/Architect

A System for Selective Disclosure of Information about a Patient with Intractable Disease *(2023)*
Erika Sugita, Ryosuke Abe, Shigeya Suzuki, Keisuke Uehara, Osamu Nakamura
ESAS 2023: The 18th IEEE International Workshop on e-Health Systems and Web Technologies, Trino, Italy
Verfiable Credentals

Verifiable Issuers & Verifiers *(2022)*
Manu Sporny, Oskar van Deventer, Isaac Henderson Johnson Jeyakumar, Shigeya Suzuki, Konstantin Tsabolov, Line Kofoed, Rieks Joosten
A WHITE PAPER FROM RWOT XI: THE HAGUE, 22 Dec 2022
Verfiable Credentals

QuISP: a Quantum Internet Simulation Package *(2022)*
Ryosuke Satoh, Michal Hajdušek, Naphan Benchasattabuse, Shota Nagayama, Kentaro Teramoto, Takaaki Matsuo, Sara Ayman Metwalli, Poramet Pathumsoot, Takahiko Satoh, Shigeya Suzuki, Rodney Van Meter, 2022 IEEE International Conference on Quantum Computing and Engineering (QCE22), Broomfield, CO, USA
BEST PAPER AWARD Quantum Internet

A Quantum Internet Architecture *(2022)*
Rodney Van Meter, Ryosuke Satoh, Naphan Benchasattabuse, Kentaro Teramoto, Takaaki Matsuo, Michal Hajdusek, Takahiko Satoh, Shota Nagayama, Shigeya Suzuki, 2022 IEEE International Conference on Quantum Computing and Engineering (QCE22), Broomfield, CO, USA
Quantum Internet

Decentralized Identifiers (DIDs) v1.0 *(2021)*
Manu Sporny, Amy Guy, Markus Sabadello, Drummond Reed (Editors)
World Wide Web Consortium, 26 July 2021
Identity Contributor

DID Core Specification Test Suite and Implementaiton Report *(2021)*
Orie Steele, Shigeya Suzuki, Manu Sporny, Markus Sabadello (Editors)
World Wide Web Consoritium, 26 July 2021
Editor Identity

Attacking the Quantum Internet *(2021)*
Takahiko Satoh, Shota Nagayama, Shigeya Suzuki, Takaaki Matsuo, Michal Hajdušek, Rodney Van Meter.
IEEE Transactions on Quantum Engineering
Security Quantum Internet

ニューノーマル時代における人間の社会活動を支える情報基盤の在り方とデジタルアイデンティティの位置づけ (ディスカッションペーパ 2020)
村井 純、鈴木 茂哉、松尾 真一郎、クロサカタツヤ, 慶應義塾大学SFC研究所 ブロックチェーン・ラボ
Privacy Identity Blockchain

令和元年度:ブロックチェーン技術等を用いた金融システムのガバナンスに関する研究
[慶應義塾大学SFC研究所との合同研究]
金融庁 総合政策局 総合政策課 フィンテック室
Blockchain DeFi Multistakeholder Governance

Mitigating Bitcoin Node Storage Size By DHT *(2018)*
Ryosuke Abe, Shigeya Suzuki, Jun Murai, AINTEC 2018, Bangkok, Thailand
Blockchain Scalability

Blockchain as an Audit-able Communication Channel *(2017)*
Shigeya Suzuki, Jun Murai
STFSA 2017: The 12th IEEE International COMPSAC Workshop on Security, Trust and Privacy for Software Applications, Trino, Italy
Blockchain Traceability

https://member.wide.ad.jp/~shigeya

鈴木 茂哉

慶應義塾大学大学院 政策・メディア研究科 特任教授 / 博士 (政策・メディア)

Shigeya Suzuki, Ph.D

Project Professor,
Graduate School of Media and Governance, Keio University

shigeya@wide.ad.jp
shigeya@keio.jp

主たる研究領域

ネットワーク化されたセキュアな情報システムの設計 / 開発 / 構築

情報システムアーキテクチャ / コンピューターネットワーク / 分散システム / デジタルアイデンティティ / ネットワークシステムセキュリティ / 量子インターネット

現在の主たる肩書き・活動等

慶應義塾大学SFC研究所 データーアーキテクチャラボ 副所長(技術統括)

慶應義塾大学SFC研究所 トラステッド・インターネット・アーキテクチャ・ラボ 副所長

慶應義塾大学SFC研究所 Auto-ID Labs Japan副所長

WIDEプロジェクト ボードメンバ/研究者

Trusted Web推進協議会タスクフォースメンバ
(内閣官房デジタル市場競争会議)

W3C DID WG / VC WG / Credentials CCG メンバ

Rebooting the Web of Trust, Board Member

Originator Profile技術研究組合 技術開発WG部会長

Recent Papers and Other works 最近の主な研究業績

Mitigation of Seller and Buyer's Dilemma with Transaction History and Escrow *(2023)*
Ryosuke Abe, Seiyo Kurita, Mariko Kobayashi, Shigeya Suzuki
AINTEC'22: The 17th Asian Internet Engineering Conference, Hachi, Vietnam
BEST PAPER AWARD Blockchain

Trusted Web ホワイトペーパ Ver.3.0 *(2023)*
Trusted Web推進協議会 (内閣官房デジタル市場競争会議)
Identity Privacy Blockchain Member/Architect

A System for Selective Disclosure of Information about a Patient with Intractable Disease *(2023)*
Erika Sugita, Ryosuke Abe, Shigeya Suzuki, Keisuke Uehara, Osamu Nakamura
ESAS 2023: The 18th IEEE International Workshop on e-Health Systems and Web Technologies, Trino, Italy
Verfiable Credentals

Verifiable Issuers & Verifiers *(2022)*
Manu Sporny, Oskar van Deventer, Isaac Henderson Johnson Jeyakumar, Shigeya Suzuki, Konstantin Tsabolov, Line Kofoed, Rieks Joosten
A WHITE PAPER FROM RWOT XI: THE HAGUE, 22 Dec 2022
Verfiable Credentals

QuISP: a Quantum Internet Simulation Package *(2022)*
Ryosuke Satoh, Michal Hajdušek, Naphan Benchasattabuse, Shota Nagayama, Kentaro Teramoto, Takaaki Matsuo, Sara Ayman Metwalli, Poramet Pathumsoot, Takahiko Satoh, Shigeya Suzuki, Rodney Van Meter, 2022 IEEE International Conference on Quantum Computing and Engineering (QCE22), Broomfield, CO, USA
BEST PAPER AWARD Quantum Internet

A Quantum Internet Architecture *(2022)*
Rodney Van Meter, Ryosuke Satoh, Naphan Benchasattabuse, Kentaro Teramoto, Takaaki Matsuo, Michal Hajdusek, Takahiko Satoh, Shota Nagayama, Shigeya Suzuki, 2022 IEEE International Conference on Quantum Computing and Engineering (QCE22), Broomfield, CO, USA
Quantum Internet

Decentralized Identifiers (DIDs) v1.0 *(2021)*
Manu Sporny, Amy Guy, Markus Sabadello, Drummond Reed (Editors)
World Wide Web Consortium, 26 July 2021
Identity Contributor

DID Core Specification Test Suite and Implementaiton Report *(2021)*
Orie Steele, Shigeya Suzuki, Manu Sporny, Markus Sabadello (Editors)
World Wide Web Consoritium, 26 July 2021
Editor Identity

Attacking the Quantum Internet *(2021)*
Takahiko Satoh, Shota Nagayama, Shigeya Suzuki, Takaaki Matsuo, Michal Hajdušek, Rodney Van Meter.
IEEE Transactions on Quantum Engineering
Security Quantum Internet

ニューノーマル時代における人間の社会活動を支える情報基盤の在り方とデジタルアイデンティティの位置づけ (ディスカッションペーパ 2020)
村井 純、鈴木 茂哉、松尾 真一郎、クロサカタツヤ, 慶應義塾大学SFC研究所 ブロックチェーン・ラボ
Privacy Identity Blockchain

令和元年度:ブロックチェーン技術等を用いた金融システムのガバナンスに関する研究
[慶應義塾大学SFC研究所との合同研究]
金融庁 総合政策局 総合政策課 フィンテック室
Blockchain DeFi Multistakeholder Governance

Mitigating Bitcoin Node Storage Size By DHT *(2018)*
Ryosuke Abe, Shigeya Suzuki, Jun Murai, AINTEC 2018, Bangkok, Thailand
Blockchain Scalability

Blockchain as an Audit-able Communication Channel *(2017)*
Shigeya Suzuki, Jun Murai
STFSA 2017: The 12th IEEE International COMPSAC Workshop on Security, Trust and Privacy for Software Applications, Trino, Italy
Blockchain Traceability

Trust / Identity

Quantum Internet

Blockchain

https://member.wide.ad.jp/~shigeya

今日お話したいこと

- デジタル証明書とデジタルアイデンティティ
  - 公開鍵暗号とデジタル署名
  - デジタルアイデンティティと署名者
- 学修歴証明書のデジタル化で何が変わるのか
- Trusted Web — デジタルアイデンティティ活用による検証可能性の向上
- デジタルアイデンティティとDID/VC
- 学修歴証明書デジタル化における課題

デジタル証明書とデジタルアイデンティティ

デジタル証明書を構成する要素

前提知識: 公開鍵暗号とデジタル署名

二種類の暗号アルゴリズム

- **共通鍵暗号（対称鍵暗号）**：暗号化するのも、平文に戻すのも同じ鍵を使う
  → この鍵があると解けてしまうので、鍵の受け渡し（伝える）のが難しい
  - 事前の安全な鍵の共有が必要
  - Shared Key Cryptography (Symmetric Key Cryptography)

- **公開鍵暗号（非対称鍵暗号）**： 暗号化するのと、平文に戻すのに違う鍵を使う
  → 平文に戻す鍵は公開しても弊害がないので、鍵の受け渡しがしやすい
  - 公開してしまって良い鍵を**公開鍵**、一方の秘匿すべき鍵を**秘密鍵**という
  - 事前の鍵の共有なしに、情報を暗号化して伝えることができる
  - Public Key Cryptography (Asymmetric Key Cryptography)

公開鍵暗号のイメージ

- 公開鍵暗号でできることのイメージを雑に説明すると:

  - E(x) という関数に対する逆関数 E’(x) を考える
    - 例えば E(x) を x を 10で割る関数、とし、
      E’(x) を x に 10 をかける関数とするなら、
      E’(x)はE(x)の逆関数である

  - 秘密鍵と公開鍵は、組で用意される数で、上記のような「関数」と「逆関数」を鍵(大きな数)の組によって構成できる

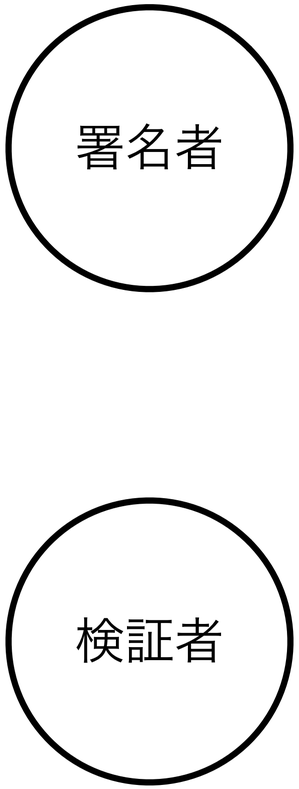
- 公開鍵や秘密鍵の【形】や、関数の形状は、用いる方式（アルゴリズム）で異なる

公開鍵暗号の特性

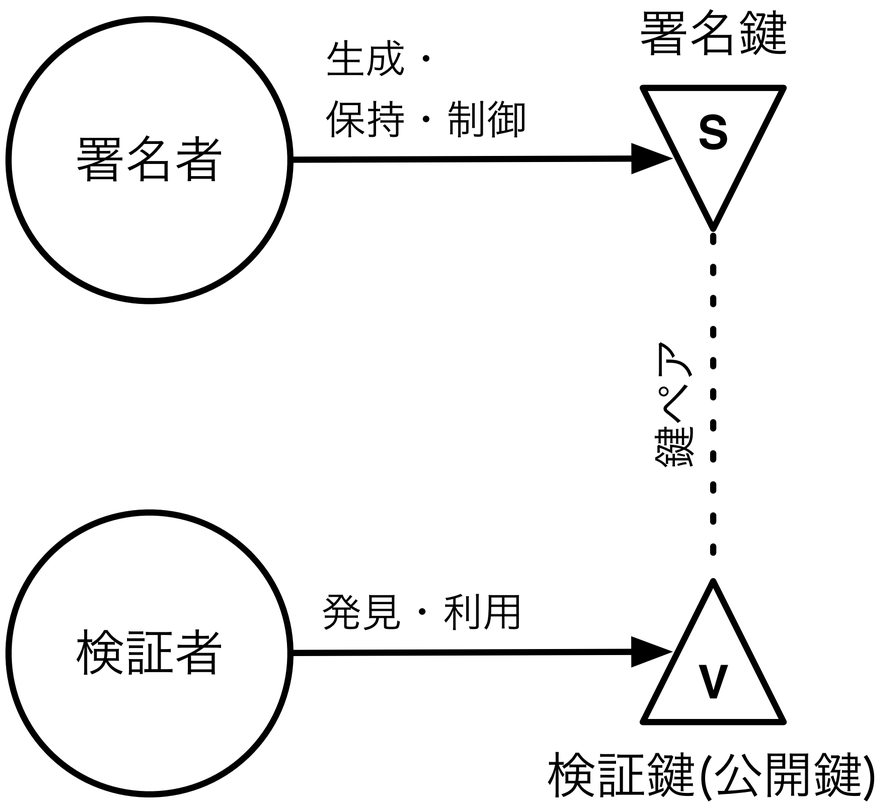
- 公開鍵は、誰の目に触れても構わない
- 秘密鍵は、鍵の所有者が確実に秘匿する必要がある

- 「秘密鍵」と「公開鍵」の組み合わせで以下を実現できる:
  - **メッセージの暗号化**: 公開鍵を用いて暗号化されたデータは、その公開鍵に対応する秘密鍵を用いてのみ、暗号を解ける（平文に戻せる）
  - **デジタル署名**: 秘密鍵で作られた署名を、その秘密鍵に対応する公開鍵を用いて確認することができる
    - 秘密鍵の保持者のみが署名できる
    - デジタル署名は、必要な情報が揃っていれば誰でも検証できる

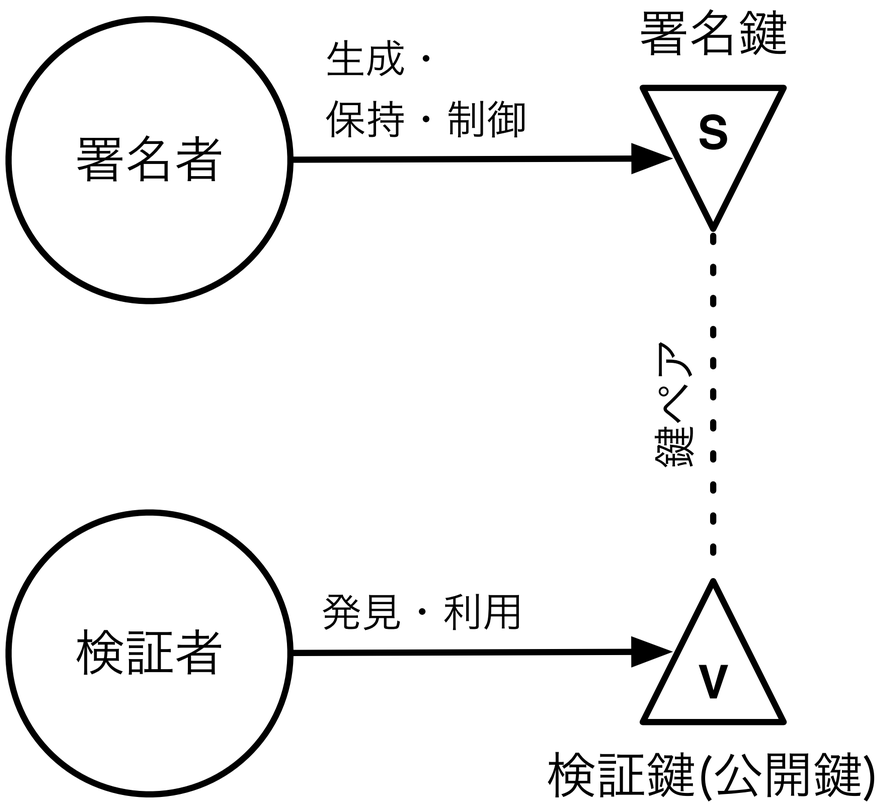
公開鍵暗号方式によるデジタル署名の構成要素



公開鍵暗号方式によるデジタル署名の構成要素

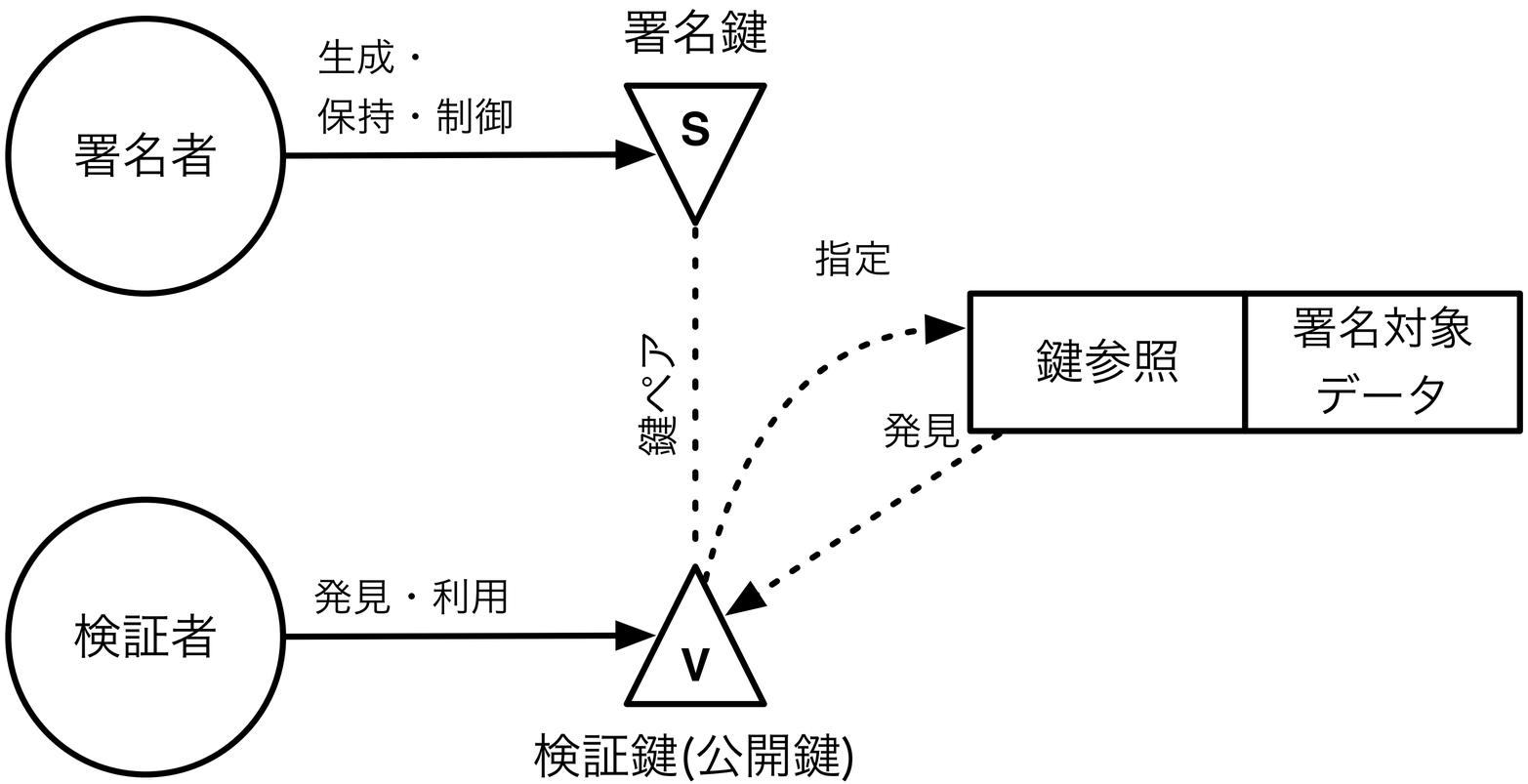


公開鍵暗号方式によるデジタル署名の構成要素

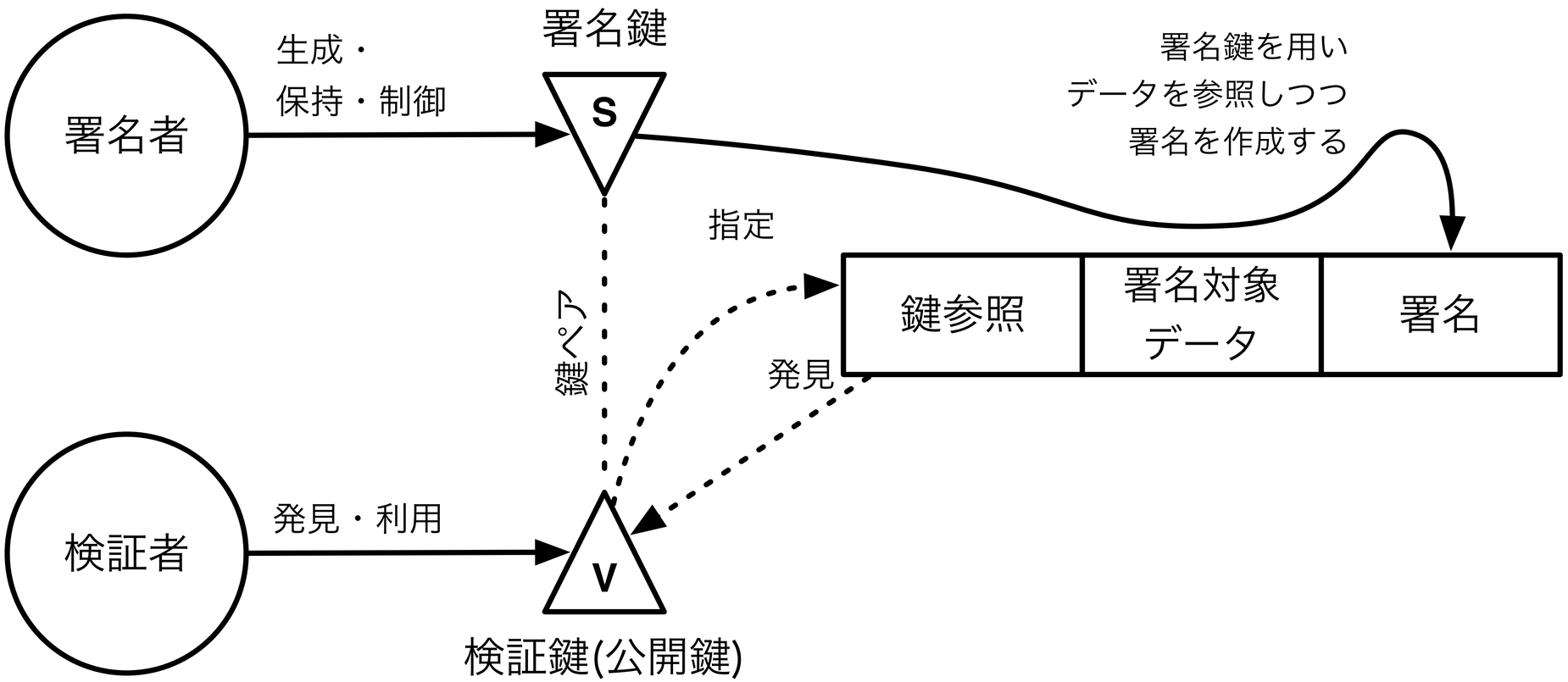


署名対象
データ

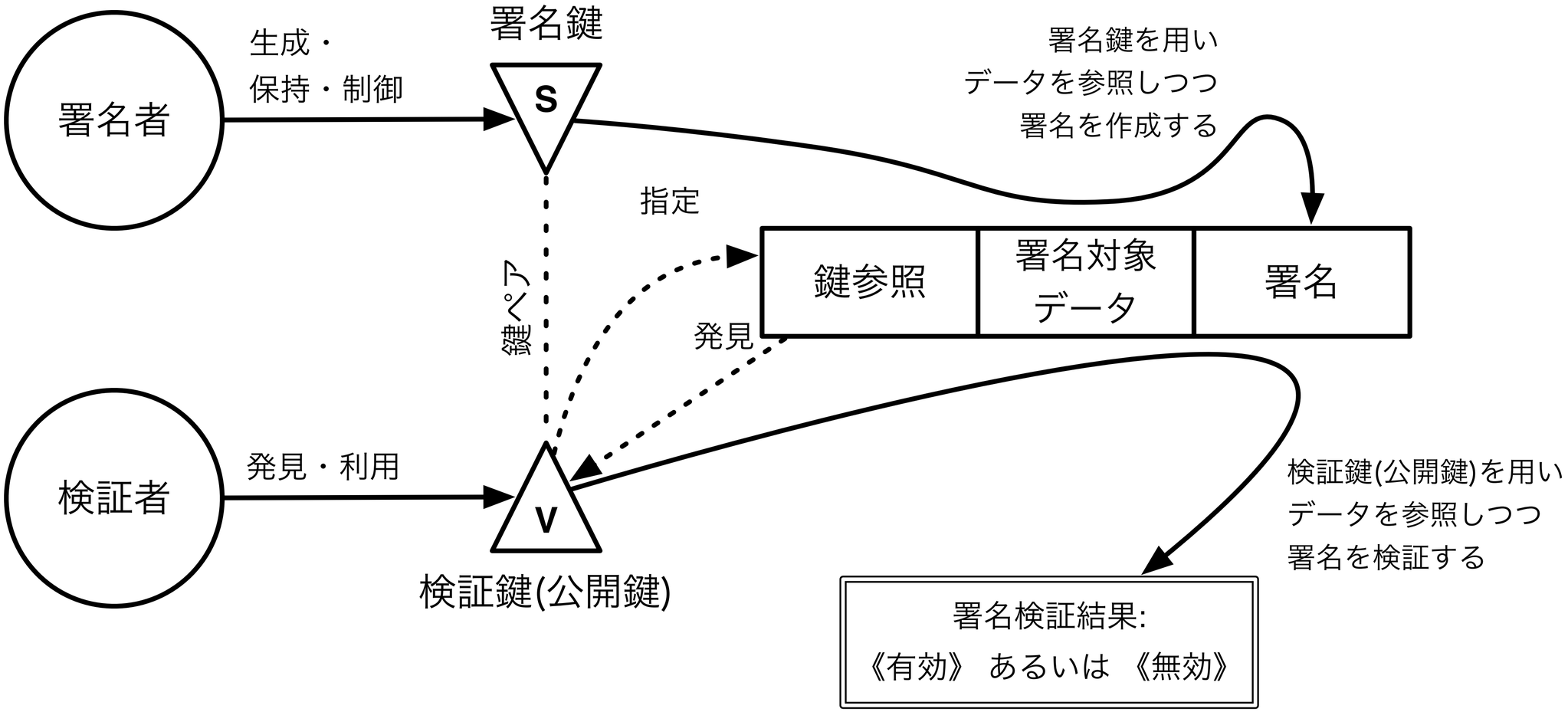
公開鍵暗号方式によるデジタル署名の構成要素



公開鍵暗号方式によるデジタル署名の構成要素



公開鍵暗号方式によるデジタル署名の構成要素



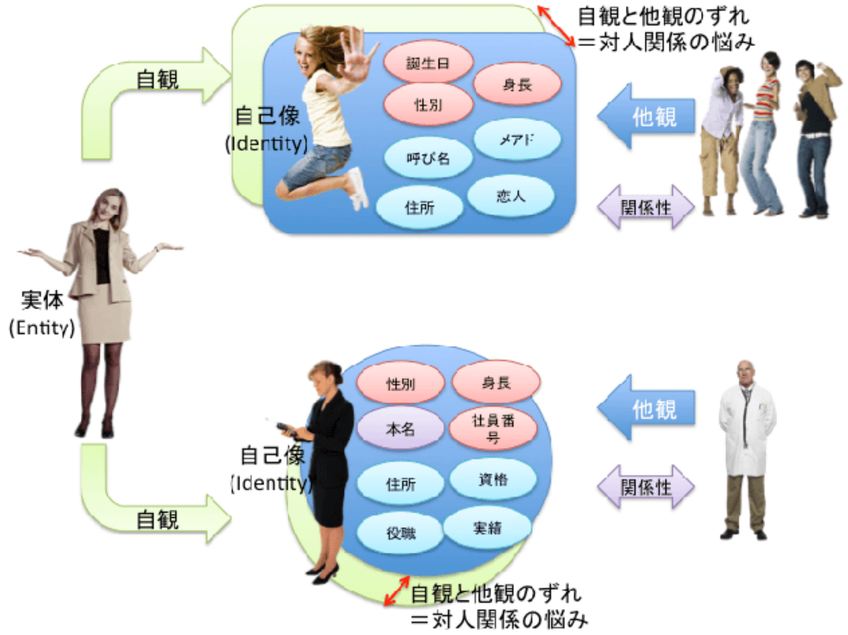
デジタルアイデンティティと署名者

デジタルアイデンティティ

- ものすごく「丸めて」表現すると:
  「**ある人**(= 実体: 一つ)**に対応するサイバー空間中で識別可能な自己像**(複数可)」

- 実体と自己像、自己像に対する自観、
  他人からみた他観や関係性など、
  厳密に説明するのは難しい。
  [1]参照のこと（右図も同文書から)

- ISOの定義では
  「実体を構成する属性の集合」
  (ISO/IEC 24760-1)



[1] 非技術者のためのデジタル・アイデンティティ入門, @_Nat Zone, 2011/6/21
https://www.sakimura.org/2011/06/1124/

デジタルアイデンティティにおける公開鍵暗号活用とデジタル証明書

- デジタルアイデンティティの《実体》が、その実体を示す公開鍵暗号の鍵ペアを作成・保持・制御することにする
  - この公開鍵暗号の鍵ペアはデジタルアイデンティティの属性

- 実体は、デジタル署名を適宜用いることにより、発信者を明らかにしながら、改竄検知が可能な形で、何らかの意図を込めつつ、情報を伝達できる

- たとえば、
  - デジタルアイデンティティに紐付けられた**本人であることを示せる**
  - 本人が確認した上で提示した情報であることを示せる → **デジタル証明書**

証明書に関係するデジタルアイデンティティ

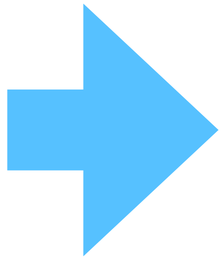
- 証明書に直接関与するもの
  - 証明書の**発行者**のデジタルアイデンティティ
  - 証明書の**対象者**のデジタルアイデンティティ
  - 証明書の**検証者**のデジタルアイデンティティ

- 証明書に間接的に関与するもの
  - 証明書の発行者、対象者、検証者が誰であるかを信頼できる形で示してくれるデジタルアイデンティティ

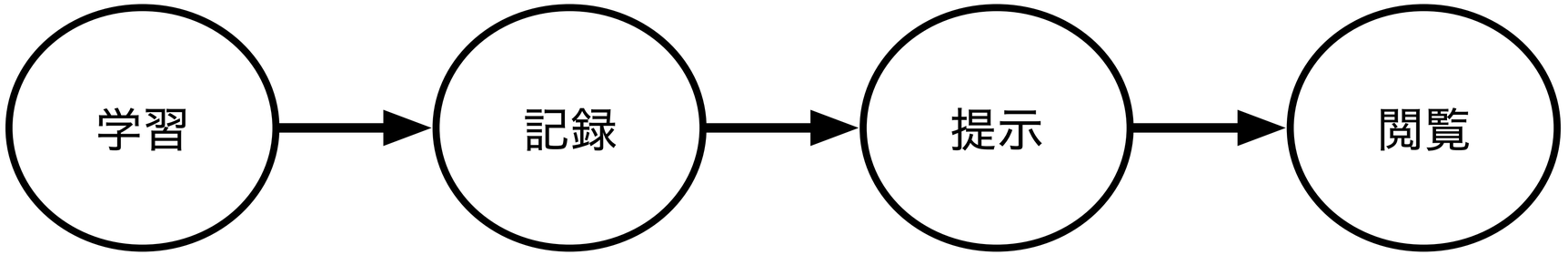
学修歴証明書のデジタル化で
何が変わるのか

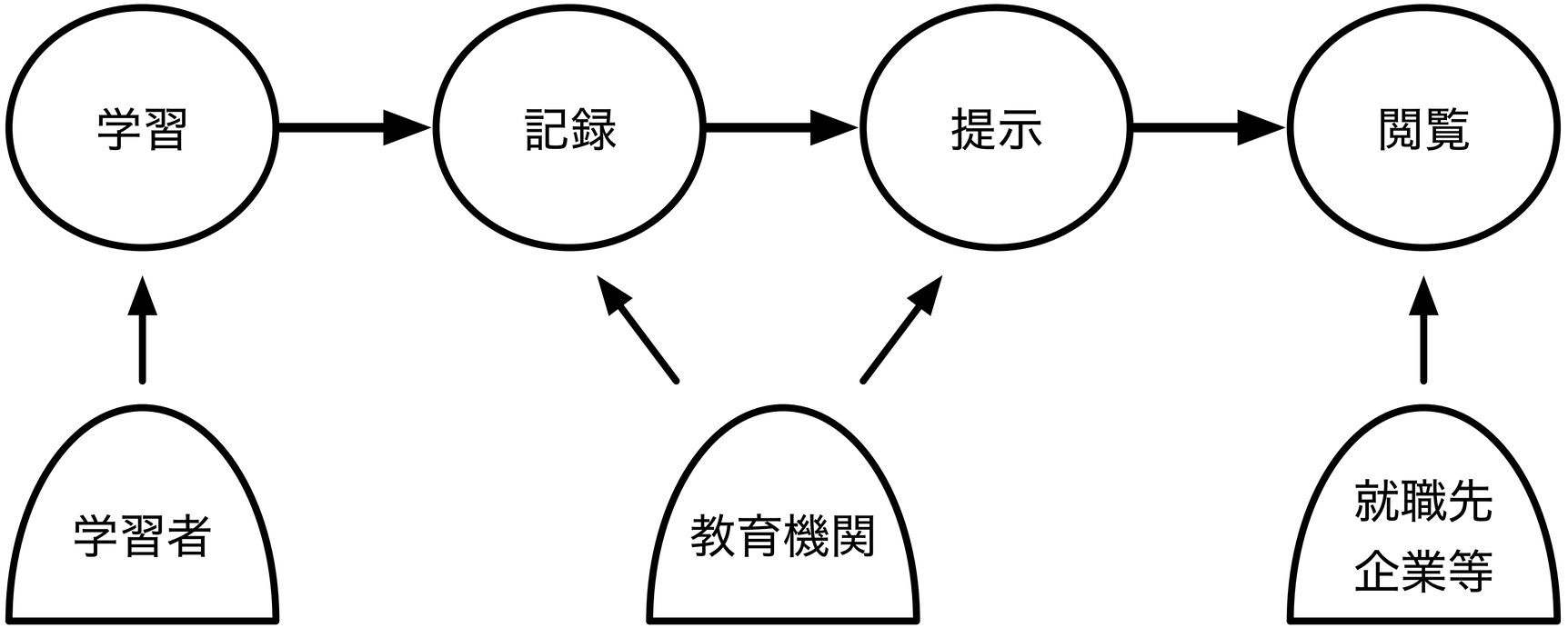
学修歴におけるステークホルダー

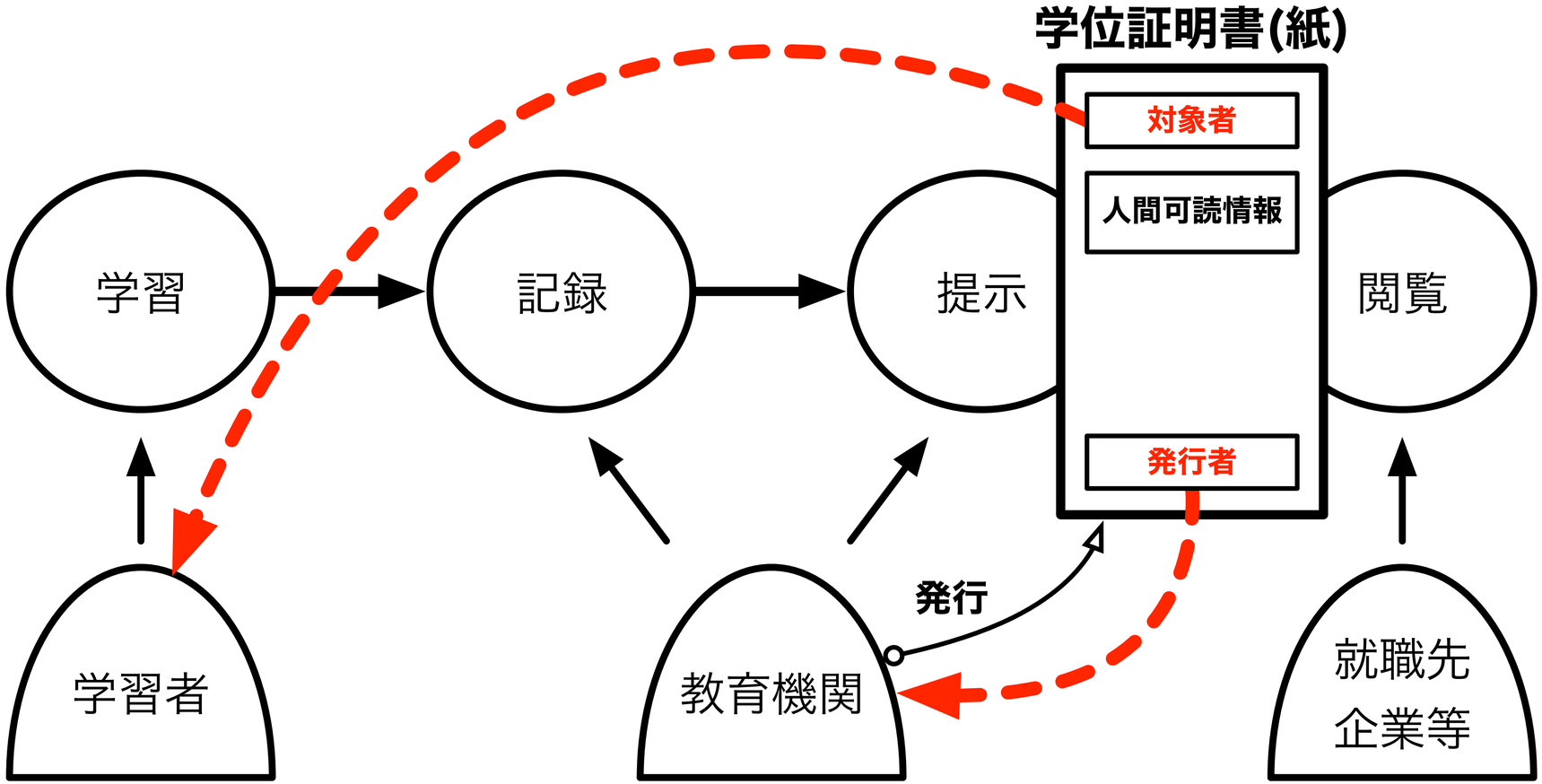
- 学習者
- 教育機関
- 学修歴を参照する者
  - 教育機関
  - 就職先企業等

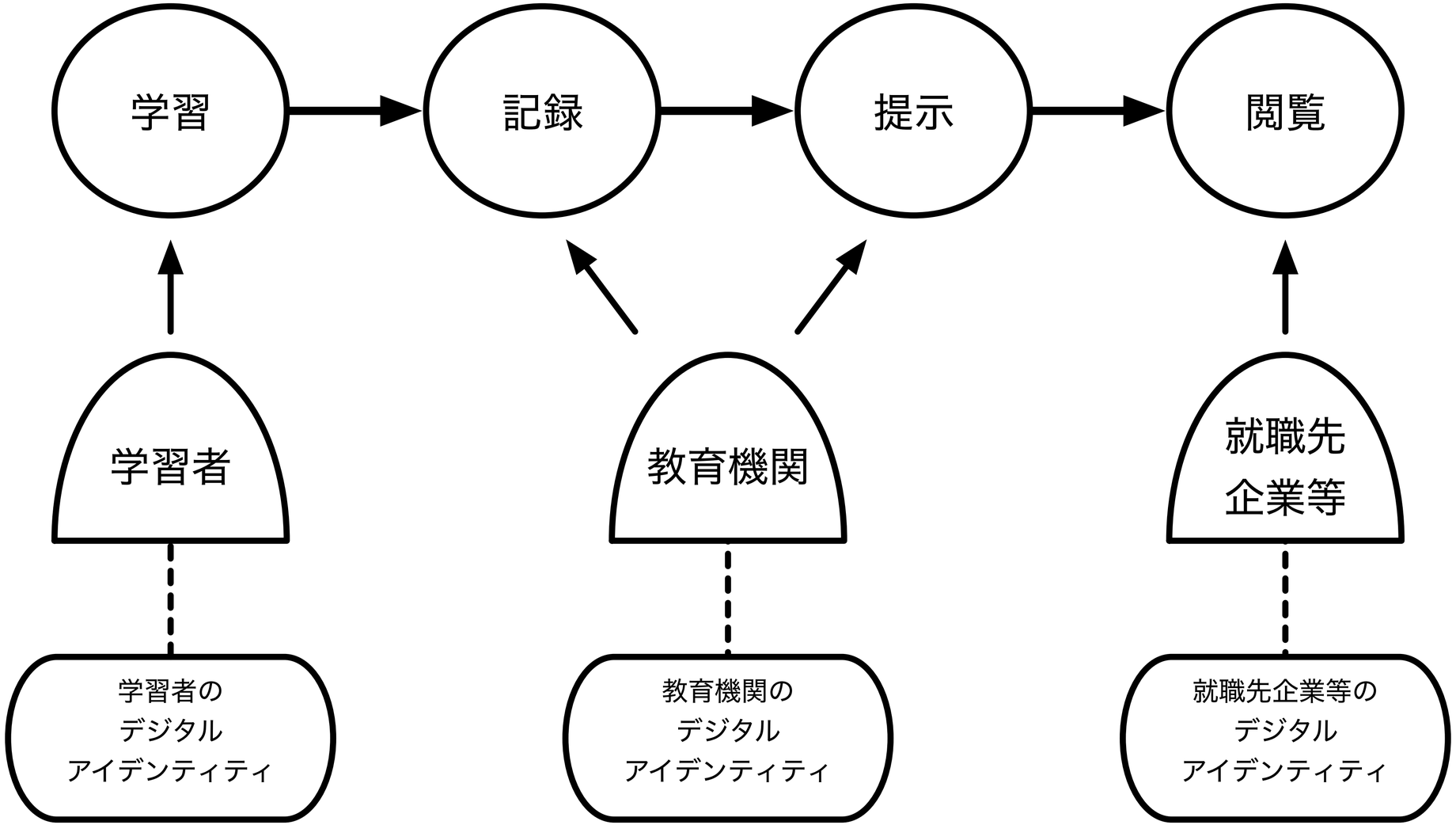


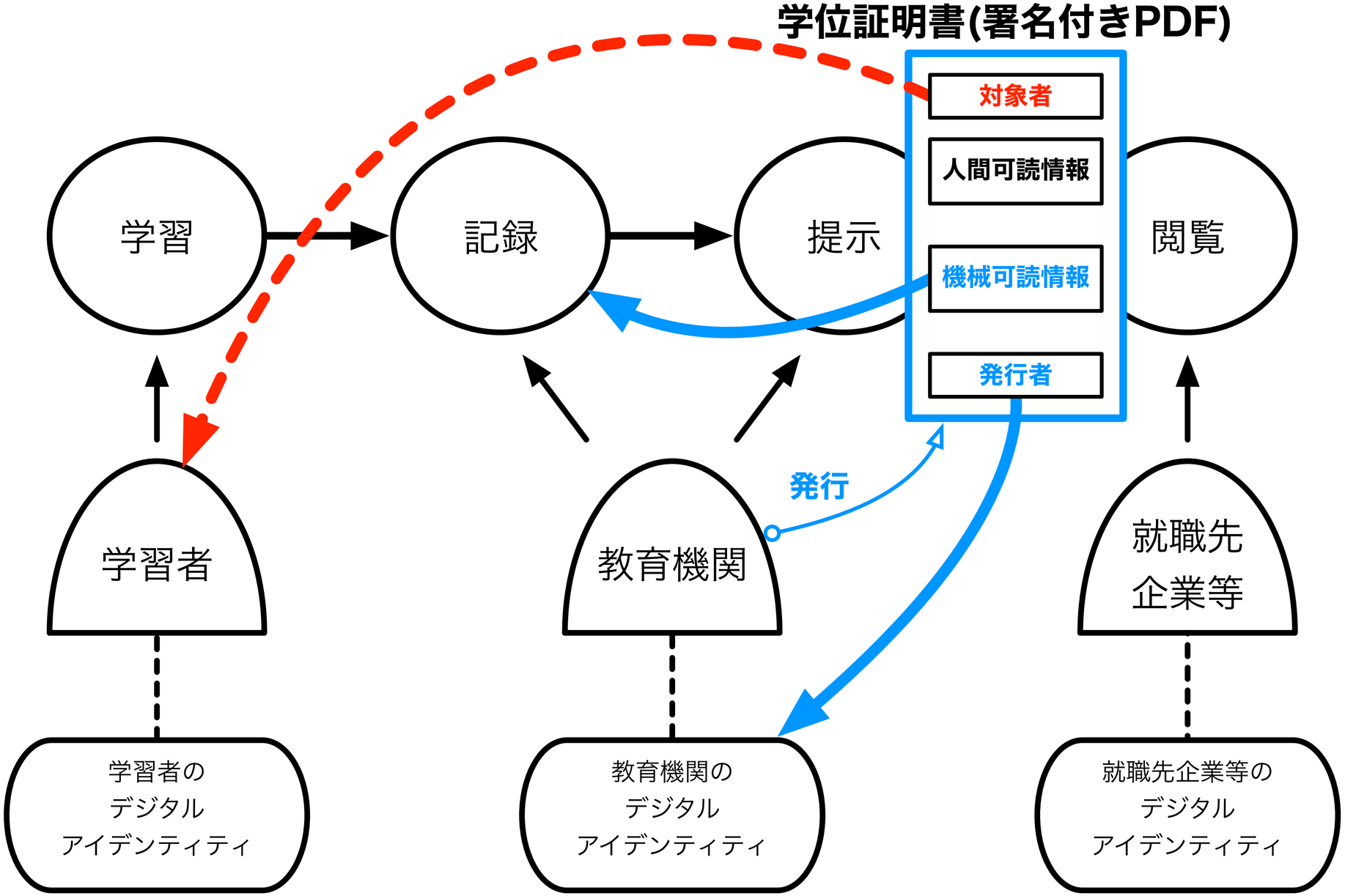
デジタルアイデンティティ間の
やりとりとして捉える

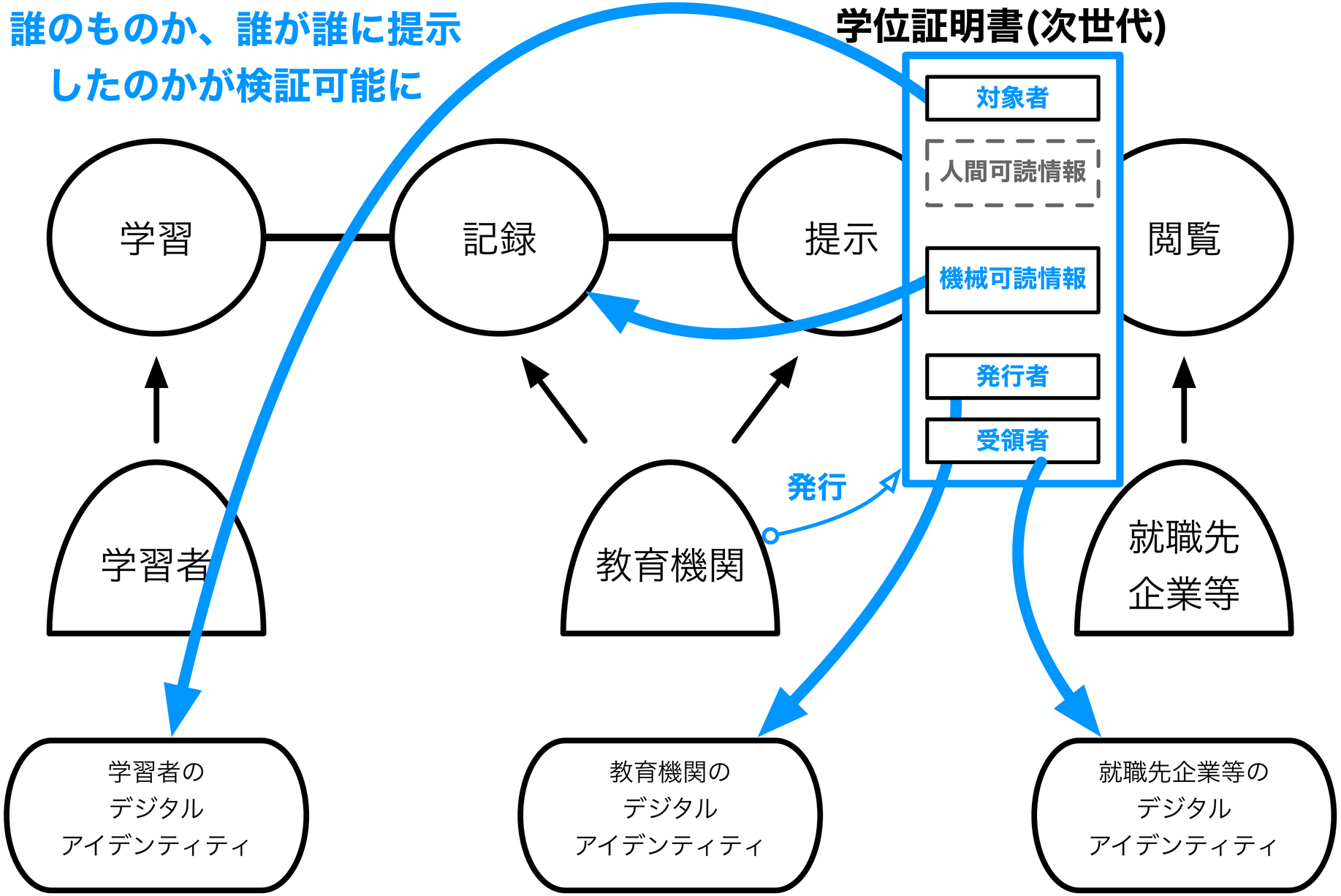


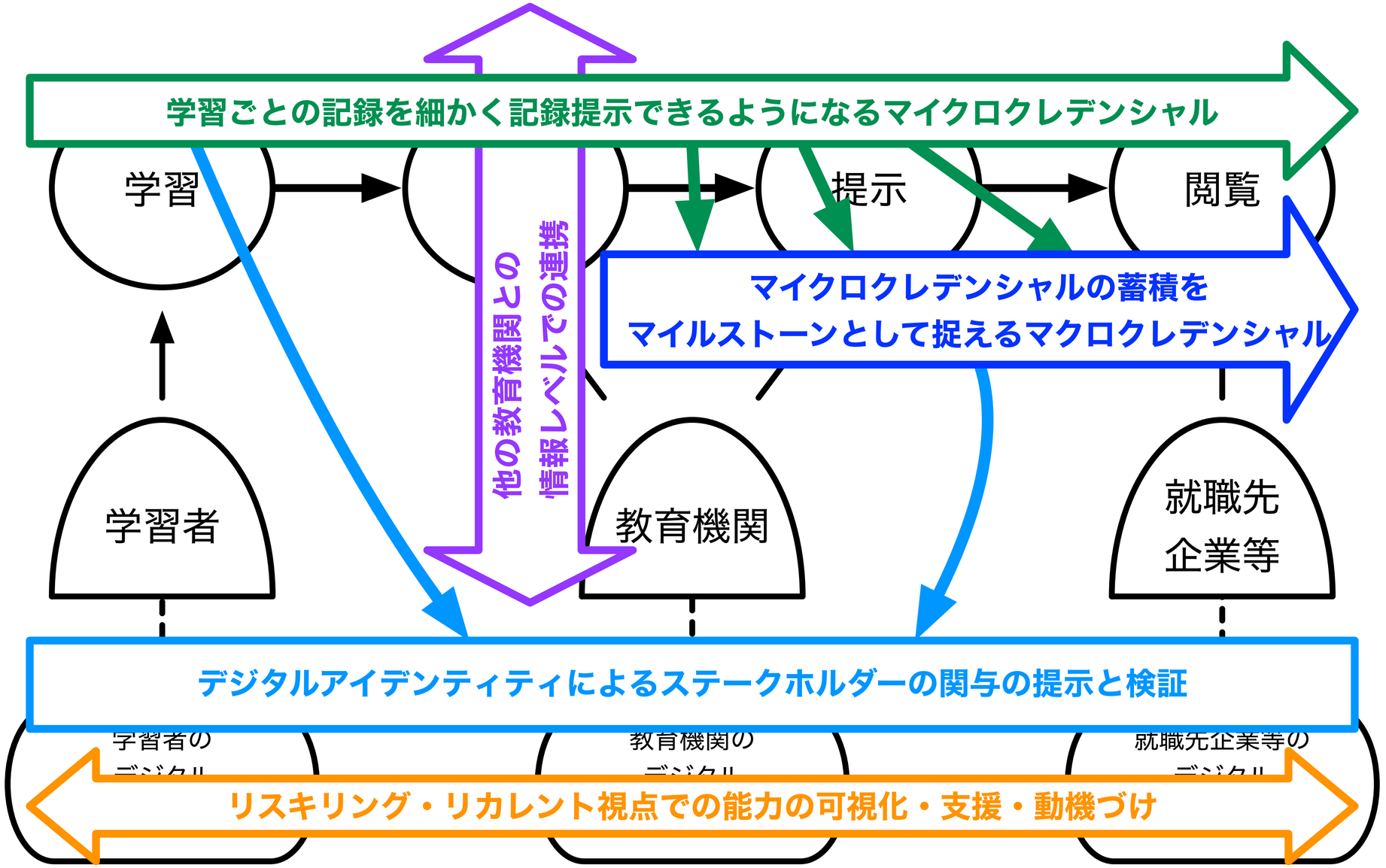












証明書の高度化と活用の段階的高度化

- 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

Trusted Web

― デジタルアイデンティティ活用による検証可能性の向上

Trusted Web 推進協議会

- **内閣官房デジタル市場競争本部内でデジタル市場競争会議**が令和２年６月に取りまとめた「中期展望レポート」に基づき**令和２年10月**に設立された協議会

- 趣旨[1]:
  - 「デジタル市場競争に係る中期展望レポート」（令和 2 年 6 月 16 日デジタル市場競 争会議）に基づき、将来の競争構造の変化を睨み、**データ・ガバナンスのあり方をテクノロジーで変える分散型の“Trusted Web”の構築を進める。**推進にあたっては、官民の連携体制の下で、データ・ガバナンスの構造設計、その際に必要となる要素やそれを実現する技術の抽出・課題検証、移行のためのロードマップの策定、具体的なユースケースに即した検証、必要な政策面での対応、国際的な発信等の具体化を進めていく必要がある。
  - このため、これらを実行する官民の連携体制として、専門家・関係者から成る「Trusted Web 推進協議会」（以下「協議会」という。）を設立し、上記の事項について検討を行う。
  - 協議会での検討の成果は、デジタル市場競争会議等に適宜報告し、必要に応じてルール整備、技術開発支援や国際的な発信等に反映させる。

[1] https://github.com/TrustedWebPromotionCouncil/Documents/blob/master/20201015_第1回_TrustedWeb推進協議会/01_当日資料/03_参考資料１_Trusted%20Web推進協議会について.pdf

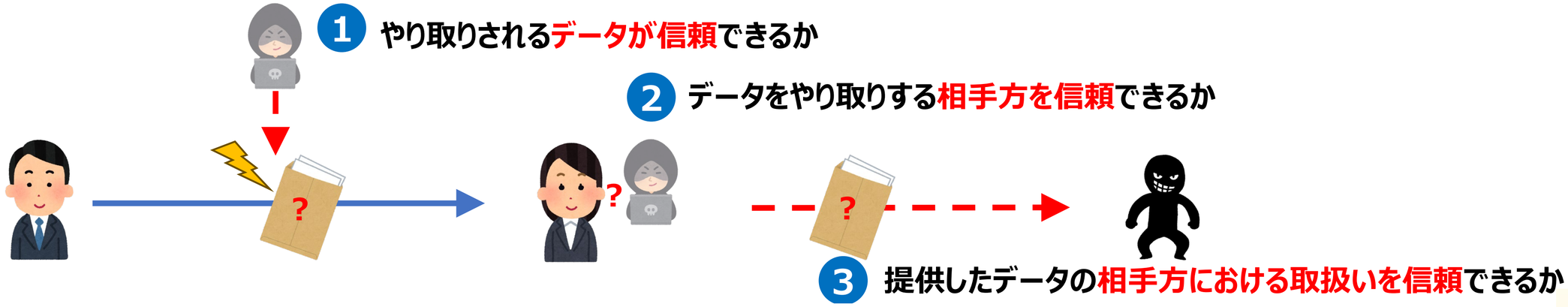
Trusted Webにおける着眼点

ペインポイントの例

〇フェイクニュースや虚偽の機器制御データなど、**流れるデータへの懸念**
〇生体情報も含めたデータの集約・統合による**プライバシーリスク**
〇**プライバシーと公益のバランス**
〇**サイロ化された産業データ**の未活用
〇**勝者総取り**等によるエコシステムのサステナビリティへの懸念
〇社会活動を行う上での社会規範による**ガバナンスの機能不全**

○ **ペインポイントの原因**としては、「**①やり取りされるデータが信頼できるか**」、「**②データをやり取りする相手方を信頼できるか**」、「**③提供したデータの相手方における取扱いを信頼できるか**」についてそれぞれ**懸念がある状況**

○ また、これらの原因に対応する**標準的かつグローバルで合意された技術や仕組みはない状況**



https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/pdf/trustedweb_gaiyou.pdf

解決に向けての手段: デジタルアイデンティティの活用

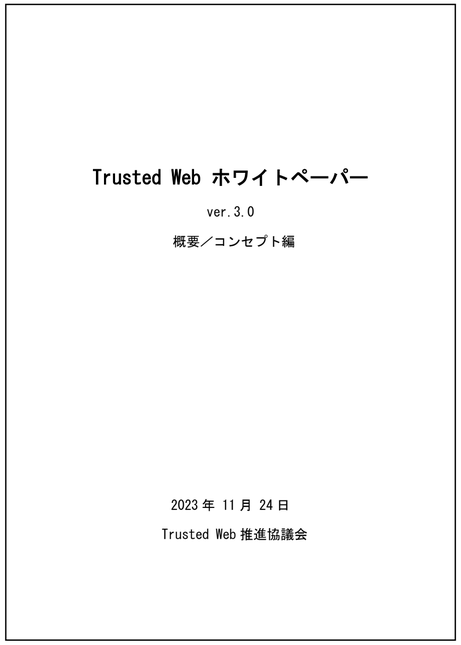
- **データや、データのやりとりの検証可能性を高められないか？**
  A. データの保持される場所に依存せず、**データ自身を検証できるようにする**
  B. データが保持されうる場所の間でのデータに関する**やりとりを検証できるようにする**

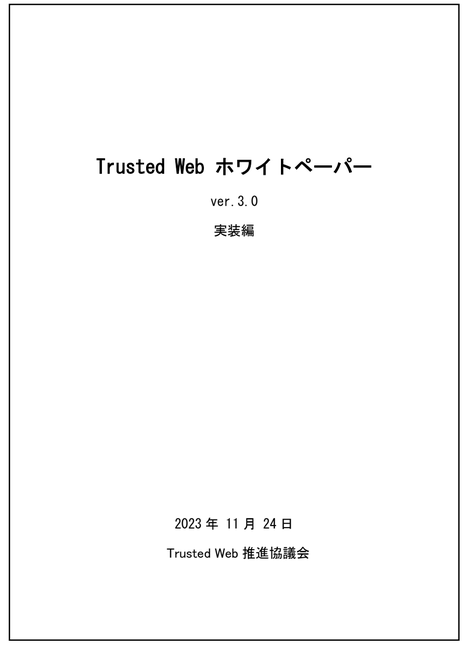
- すなわち、
  - **データの保持者とデータの検証可能性を分離する (アンバンドル)**
  - **ステークホルダー（エンティティ）の間のやりとりを検証可能とすることで、責任分解点を明確にする**

デジタル署名（公開鍵暗号）技術の活用により、
ステークホルダー間のデジタルアイデンティティによる連携を確立し
やりとりとデータを《検証可能》に

Trusted Web ホワイトペーパ Ver3.0

- 本編 3部構成 + 概要スライド
  - 概要/コンセプト編
  - ユースケース編
  - 実装編





https://trustedweb.go.jp/documents/

Trusted Web ホワイトペーパーVer3.0 - 章立て

概要/コンセプト編

- エグゼクティブサマリ
1. 検討の背景とこれまでの検討経緯
2. 用語定義
3. 直面している課題とその原因
4. Trusted Webの目指す方向性
5. Trusted Webのもたらすベネフィット
6. Trusted Webのコンセプトの具現化
7. 国際的な取り組みについて
8. 今後の取り組みについて

ユースケース編

1. 用語定義
2. Trusted Web実現に向けたユースケース
   (1) Trusted Webにおける4つの構成要素
   (2) 「個人」の属性情報のユースケース
   (3) 「メディア」の属性情報のやりとり
   (4) 「ヘルスケア」の属性情報のやりとり
   (5) 法人の行政庁との情報のやりとり
   (6) 「サプライチェーン」における情報のやりとり
   (7) 「IoT」の属性情報のやりとり
   (8) ユースケースの課題と示唆

実装編

1. 用語定義
2. Trusted Webが目指すべき方向性
3. Trusted Webのアーキテクチャデザイン
   (1) 概要
   (2) Trusted Webアーキテクチャ概観
   (3) Verifiable Data
   (4) Verifiable Messaging
   (5) Verifiable Identity
4. Trusted Webにおけるガバナンス
   1. Trusted Web実現におけるガバナンスの必要性
   2. ガバナンスの検討に関する課題と考え方
   3. Trusted Webにおけるガバナンス
5. Trusted Webにおけるセキュリティの考え方
6. 今後の取組について

ニューノーマル時代における人間の社会活動を支える情報基盤の在り方とデジタルアイデンティティの位置づけ

Version 0.1 (2020/8/3)

慶應義塾大学SFC研究所 ブロックチェーン・ラボ

村井 純
慶應義塾大学 教授

鈴木 茂哉
慶應義塾大学大学院政策・メディア研究科 特任教授

松尾 真一郎
慶應義塾大学大学院政策・メディア研究科 特任教授(非常勤)
ジョージタウン大学研究教授

クロサカタツヤ
慶應義塾大学大学院政策・メディア研究科 特任准教授(非常勤)

ニューノーマルと新たなインターネット文明の調和

新型コロナウイルス感染症（COVID-19）の感染拡大は、人間社会に新しい生活様式を要求しはじめている。我が国をはじめ、世界中の多くで、人間との接触（フィジカル・コンタクト）への制限が求められる中、デジタル・テクノロジーの活用は、従来のような付加価値向上という水準を超えて、すでに生命や健康の安全にとって重要な手段として位置づけられはじめている。こうした現状を、マイクロソフトのサティア・ナデラCEOは、同社の決算発表において「この２ヶ月で２年分に匹敵するほどのデジ

https://kbcl.sfc.keio.ac.jp/TR/global-digital-identity-for-new-normal/

デジタルアイデンティティと DID/VC

デジタルアイデンティティの活用

- 適用可能な道具
  - 既存のPKI (X.509)、法制度、トラストフレームワーク、PGP的Web of Trust
  - クレデンシャルフォーマット関連標準
    - **Verifiable Credentials (W3C)**
    - **Decentralized Identifiers (W3C)**
    - ISO 18013-5 (mobile driver license (mDL) + mobile doc (mdoc))
  - 様々な通信プロトコル
    - OpenID Connect for Verifiable Credential Issuance/Presentation他多数
  - 上記を組み合わせた、Digital Identityフレームワーク
    - 例: EU eIDAS

これらの技術を相互運用性のある形で実装・運用するためには、きめるべきこと・やるべきことが非常に多い

また既存技術だけでは不十分な点が多い。特にPKIについては繊細な表現力が無いので補う必要がある

自己主権型で実装可能な分散型ID (Decentralized Identifiers) とデジタル証明書 (Verifiable Credentials)

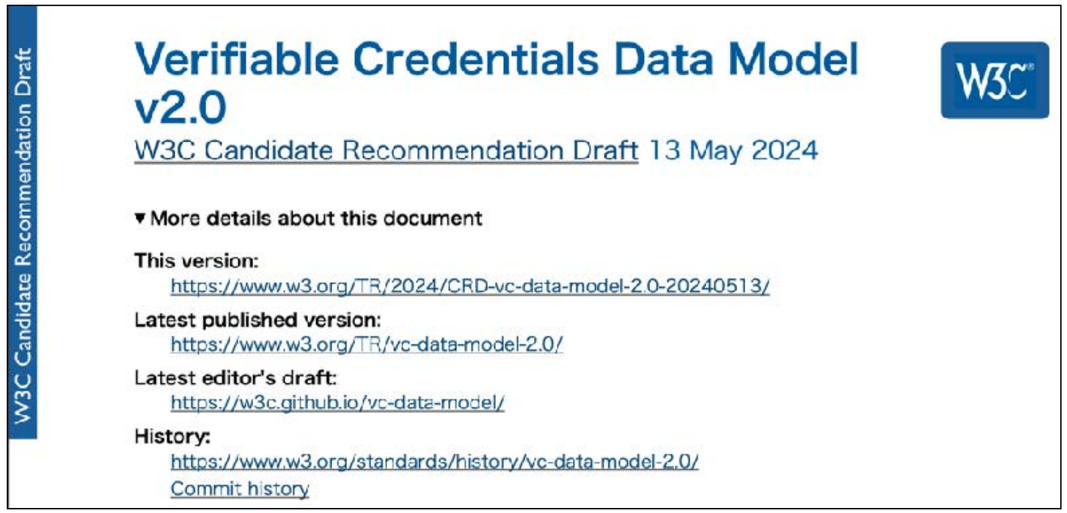
- **Decentralized Identifiers (DID) / W3C Candidate Recommendation (v1.0)**
  - 属性情報と紐付けられていない「限り無く無色の」アイデンティティ
  - 分散システム指向であり、自己主権型で実装可能
  - **自己主権型デジタルアイデンティティ**
    - 一つの定義: 誰にも依存せずに自身で制御可能なデジタルアイデンティティ

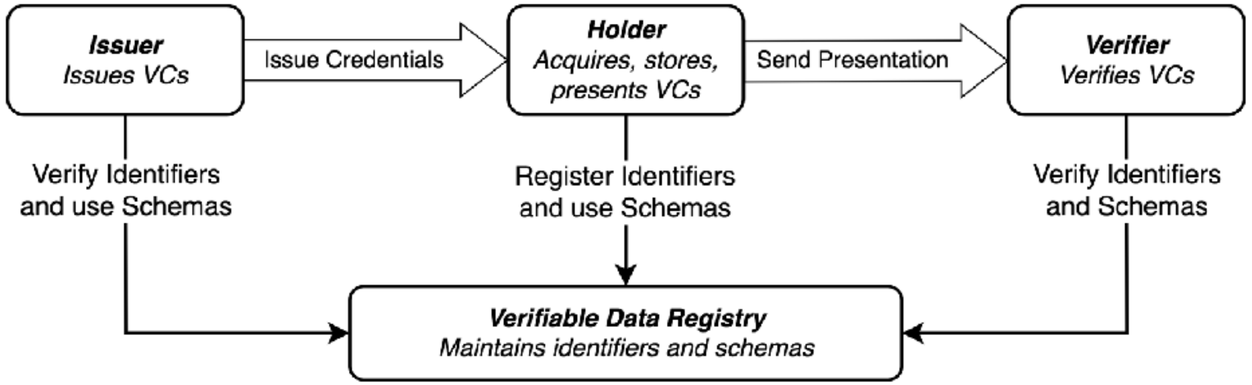
- **Verifiable Credentials / W3C Recommendation (v1.1 - v2.0作業中)**
  - 属性情報を第三者に証明してもらうための【デジタル証明書】仕様
  - ゼロ知識証明などの技術の組み合わせにより個人情報の「選択的最小開示」を実現できる

- **よくある勘違い:** VCはDIDと共に用いることでプラバシーリークを抑えることができるが、必ずしも組み合わせて使う必要はない。またDIDはブロックチェーンだけのものではない

Verifiable Credentials Data Model v2.0 (W3C Candidate Recommendation Draft)

- 検証可能なデジタル証明書の**データモデル標準**
- さまざまな「証明書」のデジタル化手段
- デジタル署名技術を用いた【発行者】(Issuer)により【対象者】(Subject)が特定の条件を満たしている事を【保持者】(Holder) が示すことができる





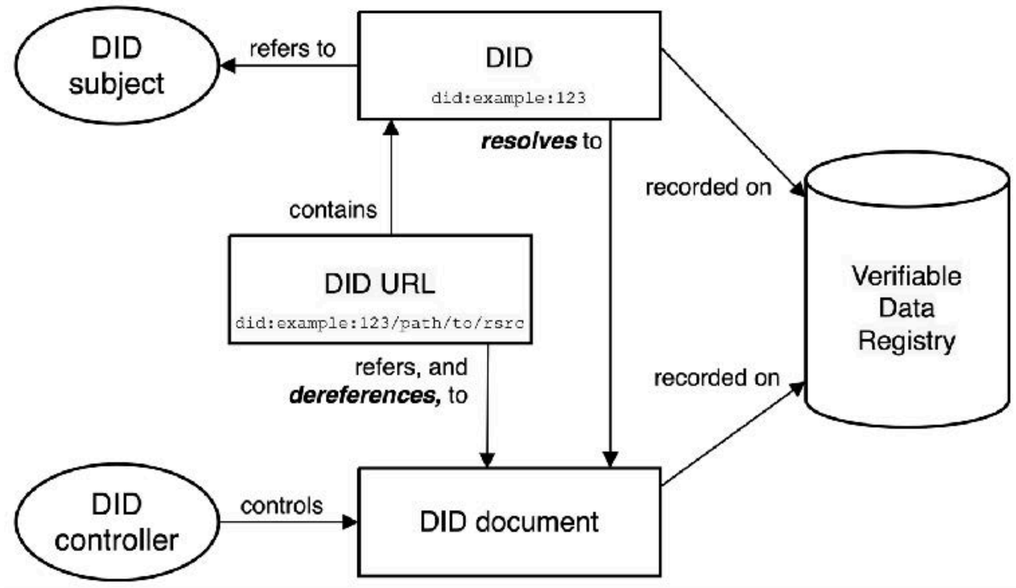
Latest Candidate Recommendation Draft:
Verifiable Credentials Data Model v2.0, W3C Candidate Recommendation Draft 15 October 2024
https://www.w3.org/TR/2024/CRD-vc-data-model-2.0-20241015/

Latest Recommendation:
Verifiable Credentials Data Model v1.1, W3C Recommendation 03 March 2022
https://www.w3.org/TR/2022/REC-vc-data-model-20220303/

備考: 2024年6月までにRecommendationとする予定だったが、作業が遅れていることもあり、VC WGの活動期間が期間延長になり、2025年1月までにはRecommendationとなる見込み →　https://www.w3.org/2022/06/verifiable-credentials-wg-charter.html

Decentralized Identifier (DIDs) v1.0 (W3C Recommendation)

- 自己主権型の識別子にまつわる**<u>データモデル標準</u>**
  - 周辺技術との組み合わせで自己主権型のアイデンティティを実現できる
  - 複数の方式(メソッド)で実装され、メソッドにより、ブロックチェーン技術を下支えにするものも、しないものもある



Decentralized Identifier (DIDs) v1.0 (W3C Recommendation)
https://www.w3.org/TR/2022/REC-did-core-20220719/

備考: 2024年4月から、改訂作業が始まっている
https://www.w3.org/2024/04/did-wg-charter.html

DID/VC 解説論文

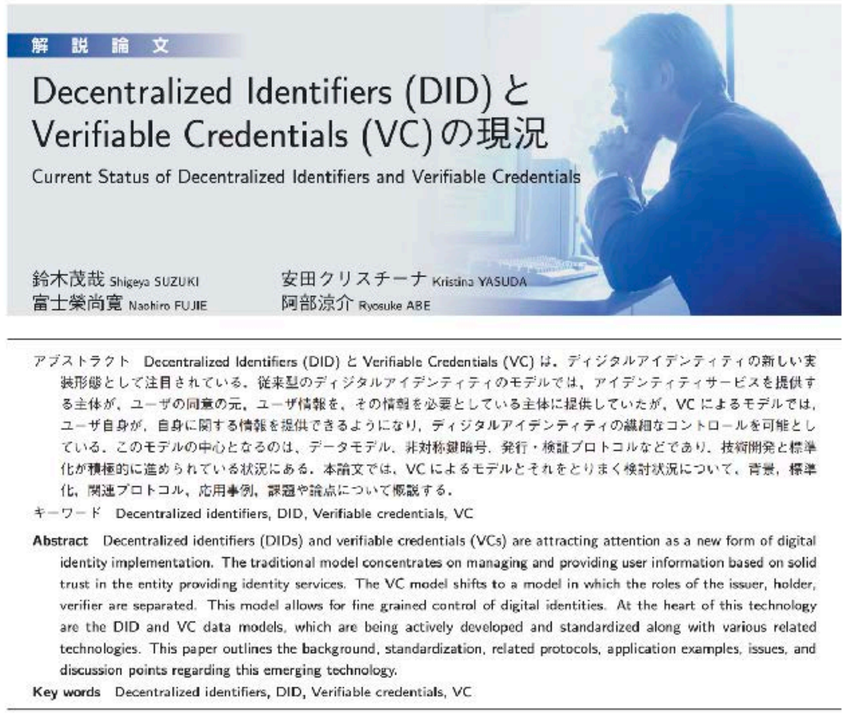
Decentralized Identifiers (DID) と Verifiable Credentials (VC) の現況

鈴木茂哉、富士榮尚寛、安田クリスチーナ、阿部涼介

電子情報通信学会 基礎・境界ソサイエティ
Fundamentals Review Vol.18 No.1
2024年7月

https://doi.org/10.1587/essfr.18.1_42

(Open Access なので無料で読めます)



解 説 論 文

Decentralized Identifiers (DID) と Verifiable Credentials (VC) の現況

Current Status of Decentralized Identifiers and Verifiable Credentials

鈴木茂哉 Shigeya SUZUKI　安田クリスチーナ Kristina YASUDA
富士榮尚寛 Naohiro FUJIE　阿部涼介 Ryosuke ABE

アブストラクト　Decentralized Identifiers (DID) と Verifiable Credentials (VC) は，ディジタルアイデンティティの新しい実装形態として注目されている．従来型のディジタルアイデンティティのモデルでは，アイデンティティサービスを提供する主体が，ユーザの同意の元，ユーザ情報を，その情報を必要としている主体に提供していたが，VC によるモデルでは，ユーザ自身が，自身に関する情報を提供できるようになり，ディジタルアイデンティティの繊細なコントロールを可能としている．このモデルの中心となるのは，データモデル，非対称鍵暗号，発行・検証プロトコルなどであり，技術開発と標準化が積極的に進められている状況にある．本論文では，VC によるモデルとそれをとりまく検討状況について，背景，標準化，関連プロトコル，応用事例，課題や論点について概説する．

キーワード　Decentralized identifiers, DID, Verifiable credentials, VC

Abstract　Decentralized identifiers (DIDs) and verifiable credentials (VCs) are attracting attention as a new form of digital identity implementation. The traditional model concentrates on managing and providing user information based on solid trust in the entity providing identity services. The VC model shifts to a model in which the roles of the issuer, holder, verifier are separated. This model allows for fine grained control of digital identities. At the heart of this technology are the DID and VC data models, which are being actively developed and standardized along with various related technologies. This paper outlines the background, standardization, related protocols, application examples, issues, and discussion points regarding this emerging technology.

Key words　Decentralized identifiers, DID, Verifiable credentials, VC

学修歴証明書デジタル化における課題

証明書の高度化と活用の段階的高度化

再掲

- 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

学修歴デジタル化における課題 (1)

- どのようにデータが記載されているか（データモデルの標準化）
  - Verifiable Credentials 2.0 標準化における単一方式への統合の失敗
    - どうやって使うのが適切なのか、関係者も分からなくなっている状況
    - 影響 → **OpenBadge 3.0 “FINAL” は全く最終版ではない**
  - 各種【独自】方式の乱立
    - 発行する側の技術選択に自由はあるが、受け取る側からすると悪夢
    - 受け取り人にとって、**なにを検証できるのか**という視点が極めて重要

→ 関係者としては、大変残念な状況に陥っていると認識。忸怩たる思い

→ 実験、実証など、様々なチャレンジに感謝！チャレンジ無しには進まない

→ 一方、現時点での極端に先行した取り組みは、結果的にやり直しになる恐れ

学修歴デジタル化における課題 (2)

- どのようにデジタルアイデンティティが確認されるのか
  - デジタル化されていない本人確認 (免許証、マイナンバーカードの目視確認)
  - デジタル化における課題　(→ ご参考: デジタル本人確認ガイドライン[1])
  - デジタルアイデンティティの検証 (→ Trusted Web のVerifiable Identity[2])

→ 業界内でも様々な取り組みが進行中かつ流動的であり、
【デジタル学生証】との関連もあり慎重な検討が必要

[1] 民間事業者向けデジタル本人確認ガイドラインについて, https://www.openid.or.jp/news/2023/03/kycwg.html
[2] Trusted Web ホワイトペーパ ver.3.0 の 【実装編】参照. https://trustedweb.go.jp/documents/

デジタル化における課題 (3)

- 証明書における《検証可能性》の段階的拡大 (DID/VC解説論文での整理)
  - (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, (6) 証明書提示の高度化

- 《インターオペラビリティ達成》での整理
  - 証明書を検証できる （上記）
  - 証明書をやりとりできる（示せる、受け取れる）
  - **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**
    (Machine Understandable ?)
  - **証明書を解釈した結果を評価・比較できる**

- **現在のOpenBadge仕様は記述方法に自由度が高すぎるため、一定の制約を設けるなどしない限り、機械可読ではあるが、機械解釈可能であるとは言えず、インターオペラビリティが存在しない。これをどう打破するのか**

宣伝: Originator Profile

Originator Profile 技術について

Originator Profile (OP) 技術とは、Web に流通する情報の作成者や発信者の真正性と信頼性を確認できるデジタル社会を実現するための技術です。情報の発信者を識別可能とし、第三者認証済みの情報発信者によるコンテンツを読者が容易に見分けられる仕組みを確立し、偽・誤情報やアドフラウドなどの氾濫を抑止する技術です。

OP 技術では、Web コンテンツの作成者やサイトの運営者といった情報発信者に誤りがなく、内容の改竄もされていないことをデジタル署名技術を用いて確認可能とします (情報発信者の真正性)。コンテンツに対しても一定の信頼を合理的に推測・判断する指標となるよう、責任ある発信主体として振る舞うため情報発信ポリシーを持ち、それを業種・業態の実情に応じて実効性あるものとするガバナンスの整備に努めている情報発信者であることも確認可能とします (情報発信者の信頼性)。

このような技術が求められている、現在のデジタル空間の課題や OP 技術が目指す方向性については、次の動画にて解説しています。OP 技術が目指すデジタル社会の方向性や、情報発信者に求める基本姿勢などについては「Originator Profile 憲章」をご覧ください。

https://originator-profile.org/ja-JP/overview/

ORIGINATOR PROFILE

その情報、本当に信頼できますか？

終わりに: 広く役立つように使われるようにするには

- 証明書のユーザは、究極的には受取人

- 何を検証できているのか、検証出来ていないのかを、丹念に検討すべき時代になっている
  - 偽の証明書類などフェイクへの対応 (生成AIによって真偽判定の困難さが増している)
  - 対面でない世界では、検証可能性の追求が重要であることへの意識が必要
  - ステークホルダーを見いだし、それぞれの視点で検討することが重要

- 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ことへの意識が必要
  - デジタル化しただけでは、かえって負担になりうる
  - デジタルにおいて、リアルの模倣をすることが必ずしも適切とは言えないのではないか
  - 【ウォレット】という言葉が聞かれるが、本当に適切なのか？

- 同じ標準を長期間使うことを考えたい
  - 「いま動けば良い」ではなく、長期運用への考慮 → 総合的なコストダウン

ラップアップ

- デジタル証明書とデジタルアイデンティティ
  - 公開鍵暗号とデジタル署名
  - デジタルアイデンティティと署名者
- 学修歴証明書のデジタル化で何が変わるのか
- Trusted Web — デジタルアイデンティティ活用による検証可能性の向上
- デジタルアイデンティティとDID/VC
- 学修歴証明書デジタル化における課題