indicio academy

Trusted Digital Ecosystems 基礎

分散型アイデンティティとVC

Indicio

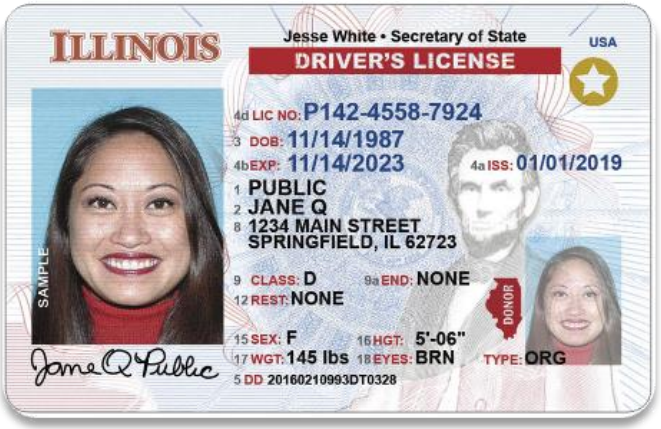
このコースの主なポイント

- 分散型アイデンティティによって、人々や組織が情報のソースと完全性（情報が改ざんされていないこと）を暗号的に検証することが可能になることを学ぶことである。
- デジタル情報は、個人や組織のプライバシーを守る方法で検証することができる。
- VC（Verifiable credentials - 検証可能な資格情報）は、シームレスなデータ共有と検証を可能にする。
- 分散型台帳には、個人データや価値の高い情報は書き込まれない。
  情報は、その所有者によってVCで保持される。
- 分散型 ID は、人、組織、およびモノに適用できる。

indicio academy

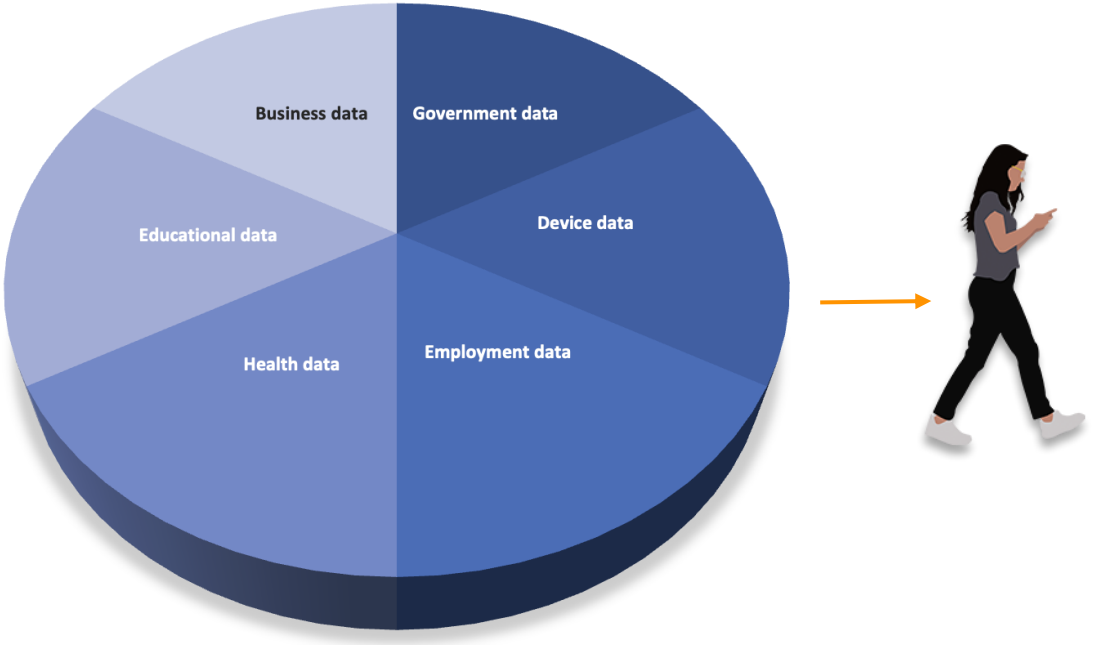
デジタルアイデンティティとは何か？

アイデンティティとは何か？



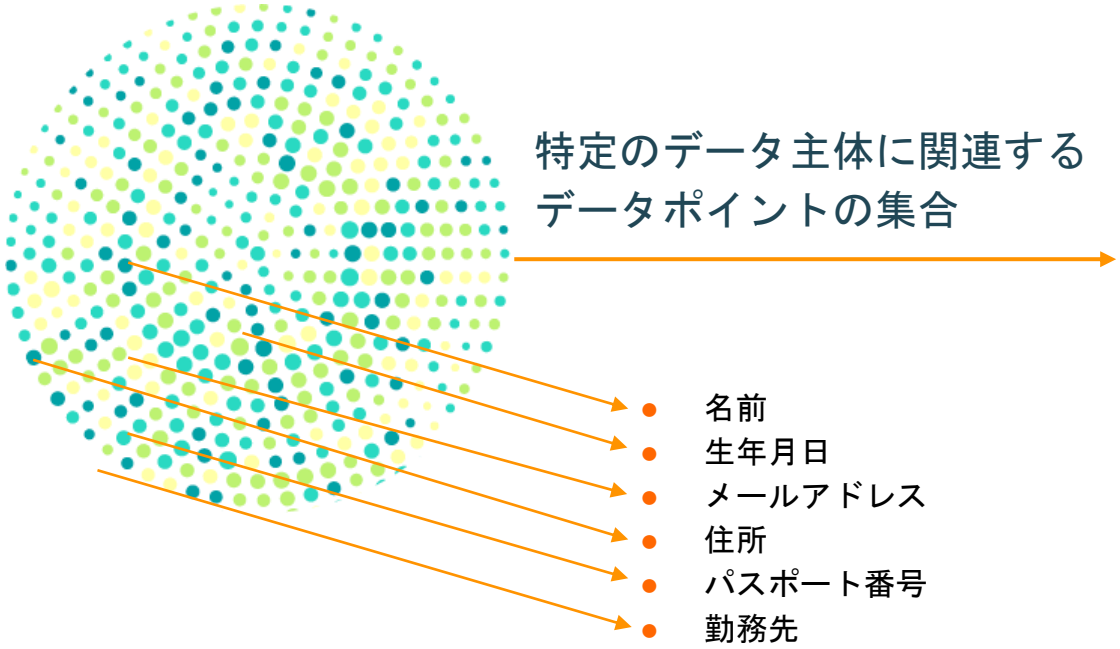
デジタルアイデンティティはデータで構成される

1つ以上のデータポイントで、
人、組織、またはモノを特定することができる。



Indicio

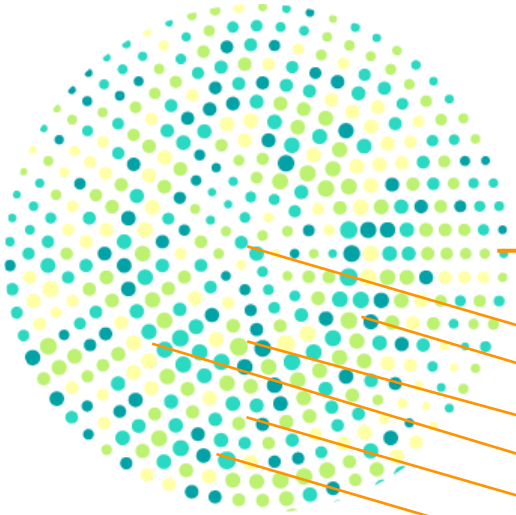
デジタルアイデンティティとは何か？



特定のデータ主体に関連する
データポイントの集合

- 名前
- 生年月日
- メールアドレス
- 住所
- パスポート番号
- 勤務先

デジタルアイデンティティとは何か？

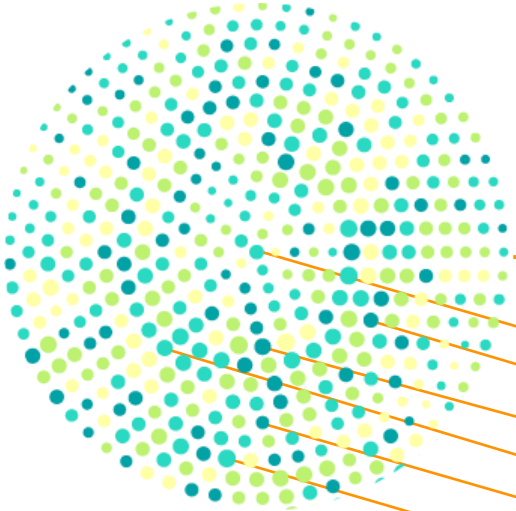


企業または団体を指す
データポイントの集合

- 営業許可
- 定款
- 財務報告
- 契約
- ベンダー
- 従業員データ

Indicio

デジタルアイデンティティとは何か？

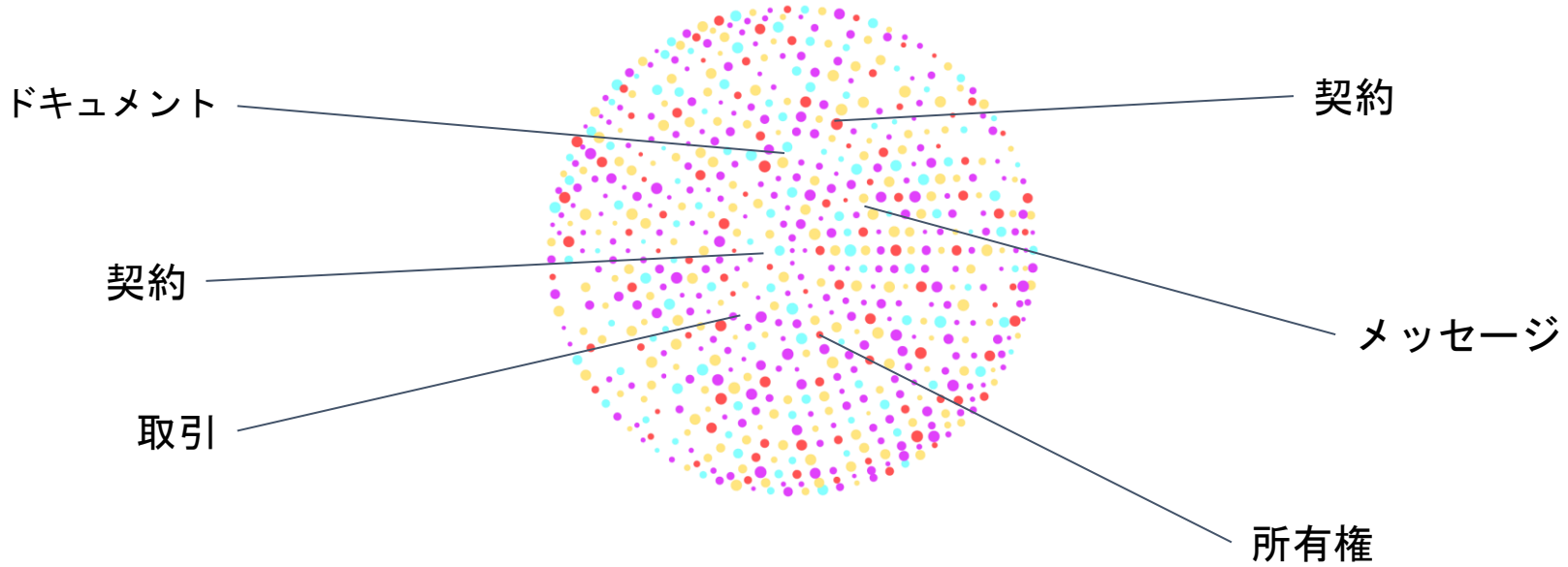


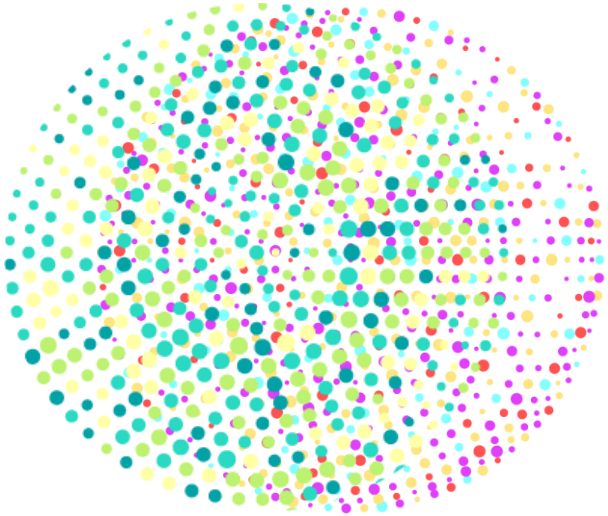
デバイスやモノを指す
データポイントの集合

- メーカー
- モデル
- 車体番号
- 販売日
- 排ガスデータ
- 修理記録

Indicio

データは関係からも生成される

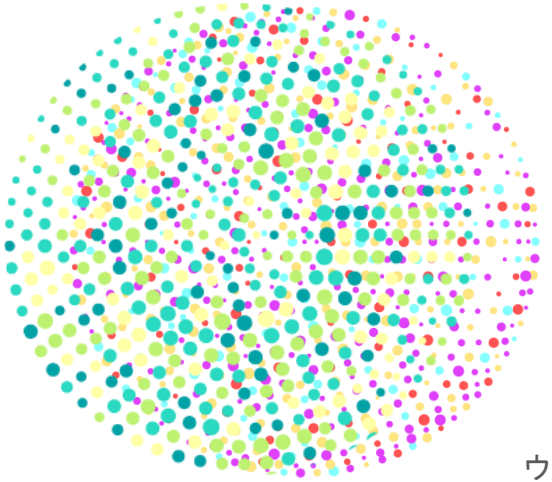




すべてのデータ・ポイントは
台帳に裏打ちされた
VC（検証可能な資格情報）
これはまた、VCを使用してあらゆる
データポイントを検証できることを
意味し、
検証可能なデータが得られる。

Indicio

分散型アイデンティティの世界



人間

組織

機械、センサー

IoTデバイス
ウェアラブル端末

検証可能なデータ＝
企業、政府、組織、機器、機械に関するデータなど、
データ主体に関連付けることができるあらゆるデータポイント。

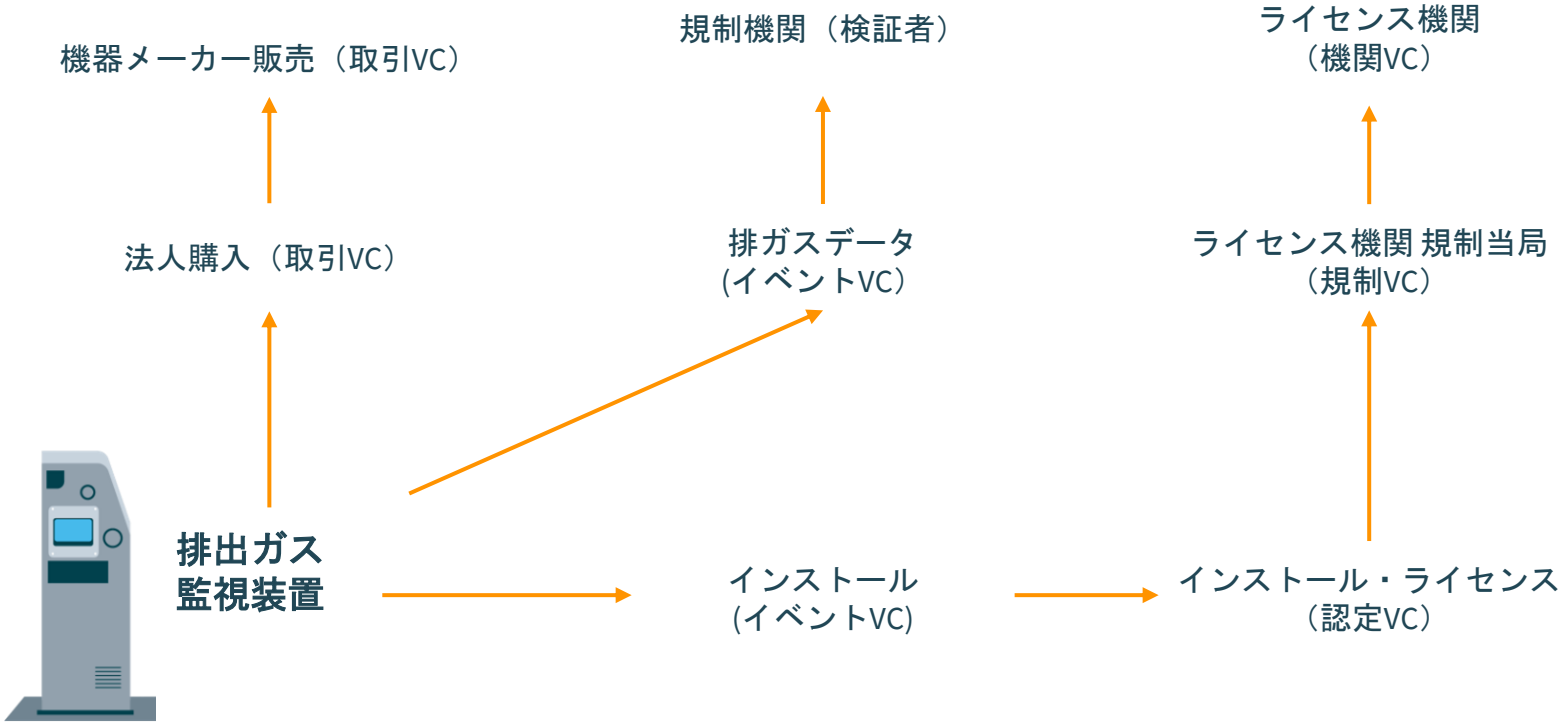
個人情報

無制限のデジタルアイデンティティ

個人データやその他のデータをオフチェーンで保持

VCを使用することで、データを共有することができる。

検証可能なデータをリンクさせることで、信頼できるエコシステムが生まれる

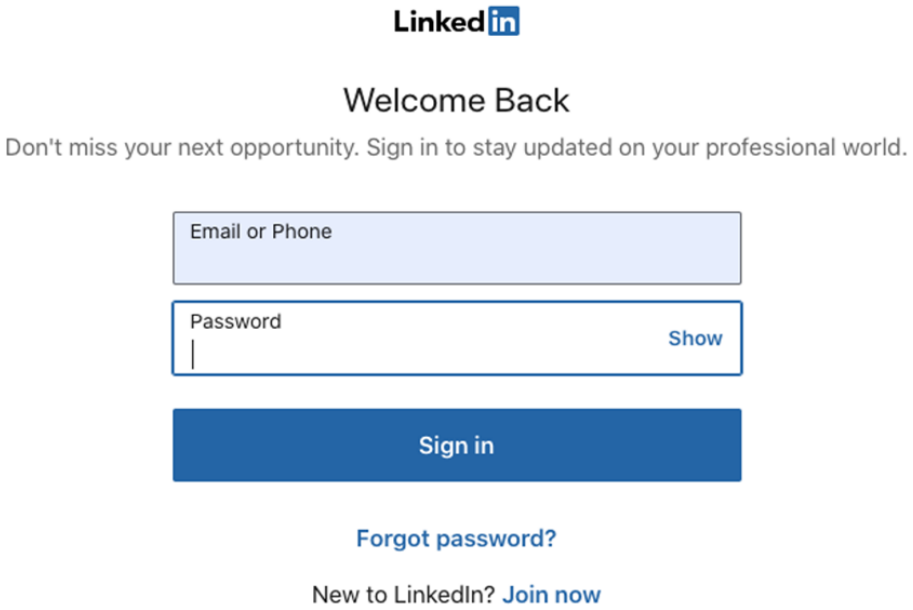


Indicio

indicio academy

デジタルアイデンティティの現在の問題点

信頼のルーツの問題



ある調査によると、平均的な人は
100のパスワードを持っており、
そのすべてを頻繁に変更し、
簡単に推測されないように十分に
複雑で、それぞれのアカウントに固有で、
再利用されないようにする必要があると
推定されている。
2022年には240億を越えるパスワードが
盗まれた。

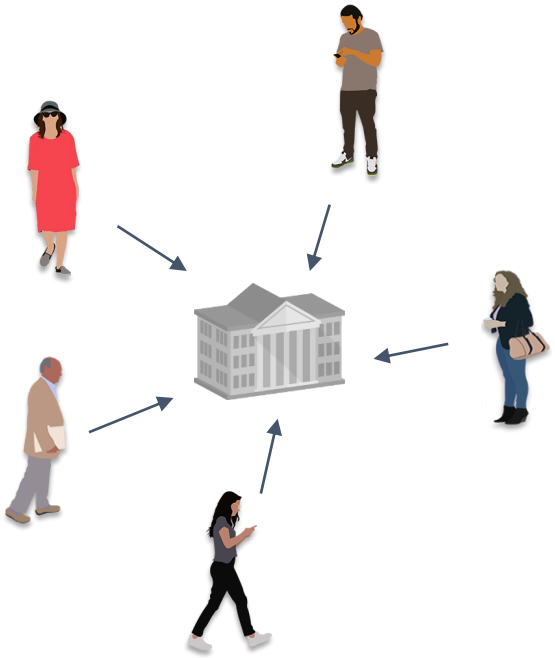
レガシーシステムの問題

- インターネットは、人や組織ではなく、コンピューターを識別するために設計された。
- World Wide Webの進化のおかげで、現在では52億人、つまり世界人口の65%がオンラインに接続し、それぞれが複数のデジタルIDを持っている。
- インターネットに接続された何十億ものデバイスやデジタル/アナログの対象物が識別子を持ち、あるいは必要としている。
- AIは、デジタル・エージェントが我々の代わりに行動することを可能にするだろう。
  エージェントとエージェントの所有者は、相互に認証可能でなければならない。

レガシー問題

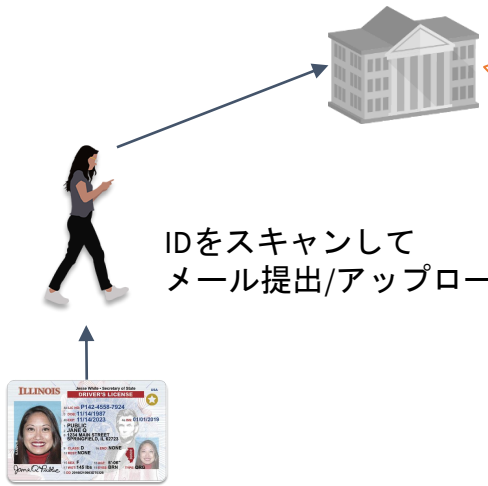
- 現在、ほとんどのデジタルアイデンティティおよびIDは「集中化」されている。
  これは、IDの管理と検証が単一のデータベースの環境内で行われることを意味する。
- デジタルアイデンティティを取得するには、自分自身に関する情報を提供し、
  その情報はIDプロバイダによってある程度検証される。
  （例：SMS認証　電話番号をプロバイダに送信し、そのプロバイダから電話番号に送信されるコードを入力して、やり取りしている人が実在することを証明する）
  その後、企業、サービス提供者は、その管理下にあるデータベース上にそのアカウント情報を保存し、責任を負う。
- つまり、デジタルアイデンティティとIDは、それが表す人々の管理下にはないということだ。

中央集権型アイデンティティのコストとリスク



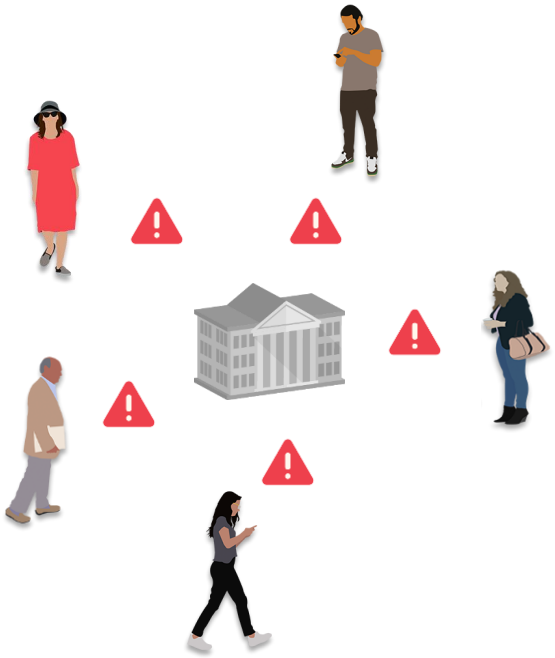
- ユーザー名、パスワード、メールアドレスといった集中型アイデンティティの構造は、デジタルアイデンティティやIDを簡単に改ざんしたり盗んだりできるものにしている。
- 個人情報や機密情報は、ユーザーのアクセスを確認するために中央に保管される必要があり、保護上の課題が生じる。
- 1つのアカウントが侵害されただけで、データベース全体の障害点となる。

中央集権型アイデンティティのコストとリスク



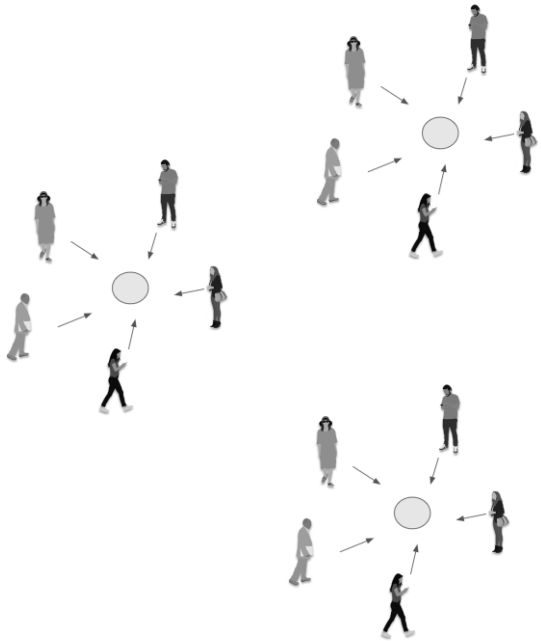
- それは本物のデータなのか？
  それともデジタル加工されたものなのか？
- 本人と名乗る人物から提出されたものなのか？
- 不正のリスクを減らすためには、どのような
  ツール・人材・時間が必要で、そのコストはどの
  くらいか？
- 不正行為を軽減する試みは、UXにどのような
  影響を与えるのか？

中央集権型アイデンティティのコストとリスク



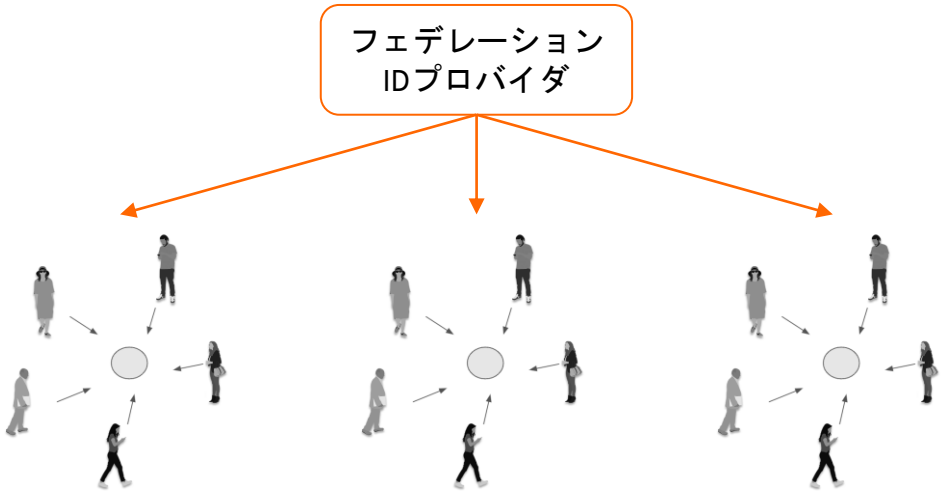
- 個人情報の保管は、ますますデータ保護規制の対象となり、法令遵守コストがかかるようになっている。
- 個人情報の保存とトラッキングは、ますます顧客の不信感の原因となっている。

中央集権型アイデンティティのコストとリスク



- それぞれのプラットフォームで
  IDアカウントを作成する必要がある。
- 個人情報は複数のユーザープロフィール／
  データベースにわたって複製されるため、
  個人情報盗難のリスクが高まる。
- データ主体（人、組織、モノ）は、自分の
  デジタルIDをコントロールできない。

フェデレーション型アイデンティティのコスト



- 1つのIDアカウントで複数のサイトやサービスにアクセスできるため、UXが簡素化される。
- しかし、ID アカウントおよびそれに関連付けられた個人情報は元の ID プロバイダが保持し管理するため、フェデレーションID は依然として中央集権的である。
- 中央集権型の根本的な欠陥がすべて残る。
- あらゆる違反や停止を規模拡大する。

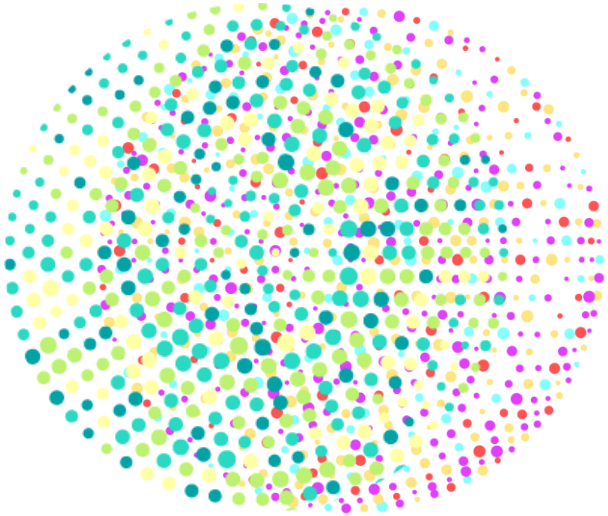
分散型アイデンティティは、
VCによってこれらの問題を解決する。

- 自分のデジタルアイデンティティ/IDは自分で管理する。ID プロバイダや認証局によって管理されることはない。
- ID プロバイダではなく、自分がデジタルアイデンティティに関連する個人情報を保有する。
- 自分のデータを自分でコントロールでき、それを誰とどのように共有するかも自分でコントロールすることができる。
- 個人情報や重要なデータが台帳に書き込まれることはない。
- 台帳に書き込まれたデータによって、あなたは自分のデジタルアイデンティティ／IDを管理していることを証明できる。
- この管理証明により、デジタルアイデンティティ所有者は相互に認証することができる。

indicio academy

デジタルアイデンティティから信頼されるデータへ

Indicio



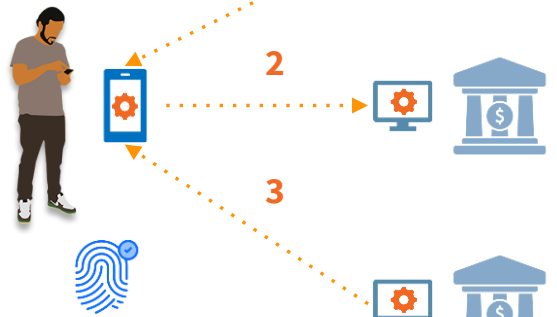
すべてのデータ・ポイントは
台帳に裏打ちされた
VC（検証可能な資格情報）
これはまた、VCを使用してあらゆる
データポイントを検証できることを
意味し、
検証可能なデータが得られる。

Indicio

どうやって検証可能なデータが信頼を生むか？
ー誰とやりとりしているかを証明できる

- DID（Decentralized Identifier - 分散型識別子）を持つ人または主体は、公開鍵暗号方式によってDIDを管理していることを証明することができる。
- DIDの通信プロトコルで銀行のDIDにメッセージを送り、銀行が応答すれば、銀行と通信していることがわかる。
- つまり、DIDの所有者は、情報を提示する前に相互に認証することができる。
- これはまた、DID所有者が、デジタル上のやり取りにおいて、誰を信頼するかについて、十分な情報に基づいた決定を下せることを意味する。
- DIDは、デジタルIDとしてのメールアドレスやユーザーアカウントにはない方法で、デジタルIDとして知ることができ、証明することができる。

例：銀行口座の相互認証



ウォレットアプリと銀行口座を確認できるVCを使って、顧客は分散型台帳上の銀行の公開DIDと鍵を読み取る。

顧客は銀行の公開鍵を使って暗号化されたメッセージを銀行に送信する。

銀行は、VC内の顧客の公開鍵を使用してメッセージを復号化し、顧客に応答する。

顧客は銀行と、銀行は顧客とコミュニケーションを取っていることを知る。

個人情報や取引データが伝達される前に、これらすべてが確認される。

生体認証でデバイスとウォレットアプリの両方へのアクセスを制限

どうやって検証可能なデータが信頼を生むか？
ー検証可能なソースによって、共有された情報が改ざんされていないことを証明できる。

- DIDは、検証可能な台帳（ブロックチェーンベースの分散型台帳ネットワーク）にVCを格納する。
  スキーマ（VCのテンプレート）およびクレデンシャル定義（スキーマを発行者に添付するための情報）は、台帳に書き込まれ、デジタル署名される。
- デジタル署名と台帳に書き込まれた資料のタイムスタンプの組み合わせは、VCまたはVC内の情報を改ざんしようとする試みが容易に発見されることを意味する。
  したがって、VC内のデータの完全性を証明することができる。

どうやって検証可能なデータが信頼を生むか？
プライバシー保護

- 個人情報は台帳に書き込まれない。VC内の情報は、VCを保有する人によって保有される。
- 一部のVCフォーマットでは、それぞれの情報に電子署名を付けることができ、これによりVC内の情報を選択的に開示できる。
- VCを保有する者がデータ要求に同意しなければ、データは提供されない。

どうやって検証可能なデータが信頼を生むか？
セキュリティ

- DIDは誰でも、いくつでも作成できる。再利用する必要はない。
- 2者間の重要なやり取りの場合、一方または両方の当事者に固有のDIDを使用することができ、これにより相関関係が第三者によって推測されることを防止できる。
- ネットワーク上の複数のノード、台帳の複数のコピーによって、冗長性が生まれる。
  中央集中型のデータベースとは異なり、情報のコピーが複数存在する。
  これにより、VCを発行し、保有し、検証することができる。

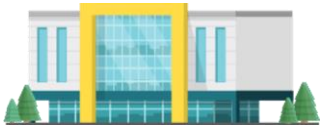
どうやって検証可能なデータが信頼を生むか？
ガバナンス

- 機械可読ガバナンスは、ガバナンスの決定を自動化することを可能にする。
- ガバナンス機関は、承認された発行者・検証者のリストを作成できる。
  その後、発行者・保有者・検証者のエージェント・ソフトウェアに保存できるファイルを公開できる。
- ガバナンスは、使用しなければならないVCのスキーマ、VCの提示方法、およびVCの失効がどのように実行されるかを確立する。
- 情報の流れは自動化され、迅速に更新される。
- ガバナンス・フレームワークにより、参加者はエコシステムにおける人間的信頼性を評価することができる。（VC発行者のID保証のルールは何か、など。）

VCを使用することで、
データとアイデンティティを検証することができ、
デジタル・エコシステム における
信頼される**デジタル・リレーションシップ**が構築される

Indicio

検証可能なデータとは、すぐに実行可能なデータを意味する



VC発行者

即効性
発行者が
信頼できる場合

リスク削減
発行者が
信頼度が低い場合

VC検証者

すぐに実行可能なデータの価値

データが信頼できる
ことを証明するため
の分析コスト

- データ統合コスト
- 人件費
- UXコスト

データが信頼できる
かどうかを検証しな
いことによる
リスクコスト

- セキュリティ・リスク
- 規制リスク
- 責任リスク
- 運用リスク
- コンプライアンス・リスク

すぐに実行可能なデータの価値

VCを使用してデータを共有し、検証することで、
データベース間の直接統合の必要性がなくなる。

検証可能なデータはすぐに実行可能であるため、
顧客体験と業務プロセスが**シームレスになる。**

シームレスなデジタル・インタラクションは、
デジタル変革の基盤である。

VCは、既存のID管理基盤に重ねることができるため、
Web3.0アプリケーションだけでなくWeb2.0アプリケーションも変革することができる。

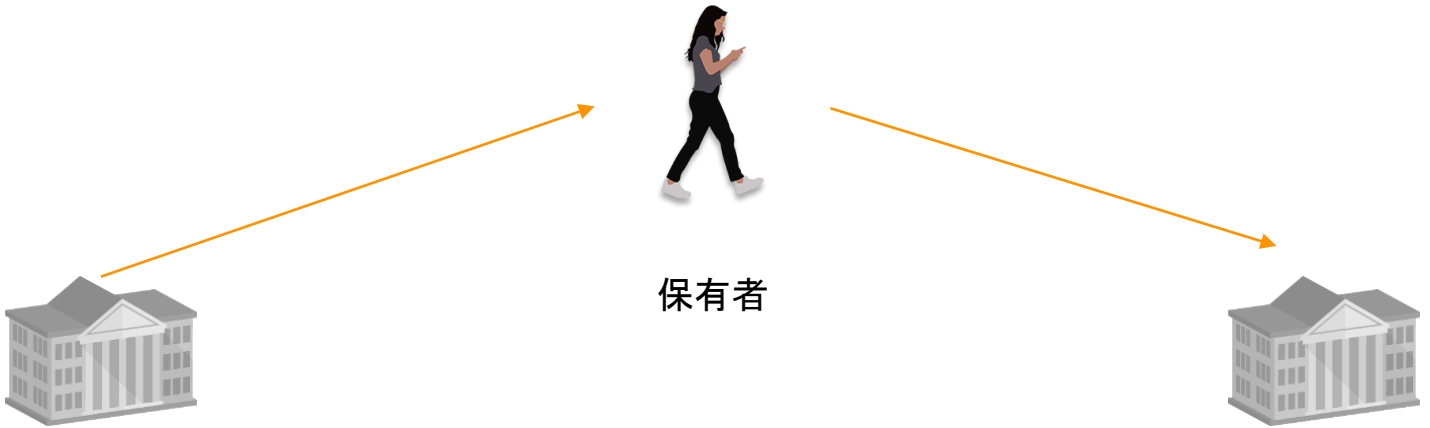
indicio academy

信頼されるデジタル・エコシステムの要素

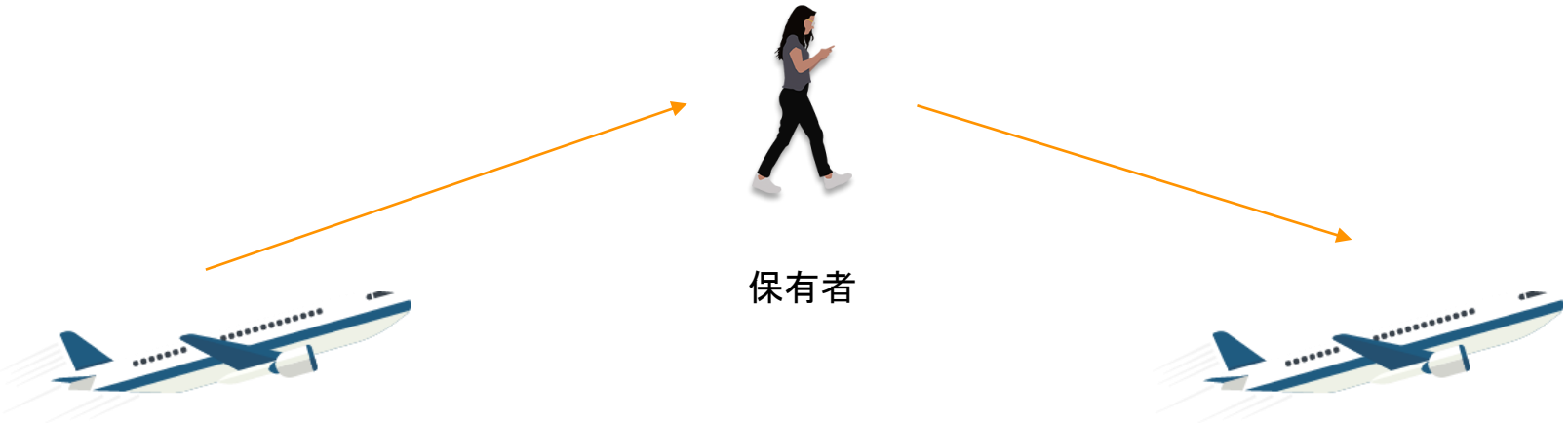
Indicio

エコシステムにおける役割

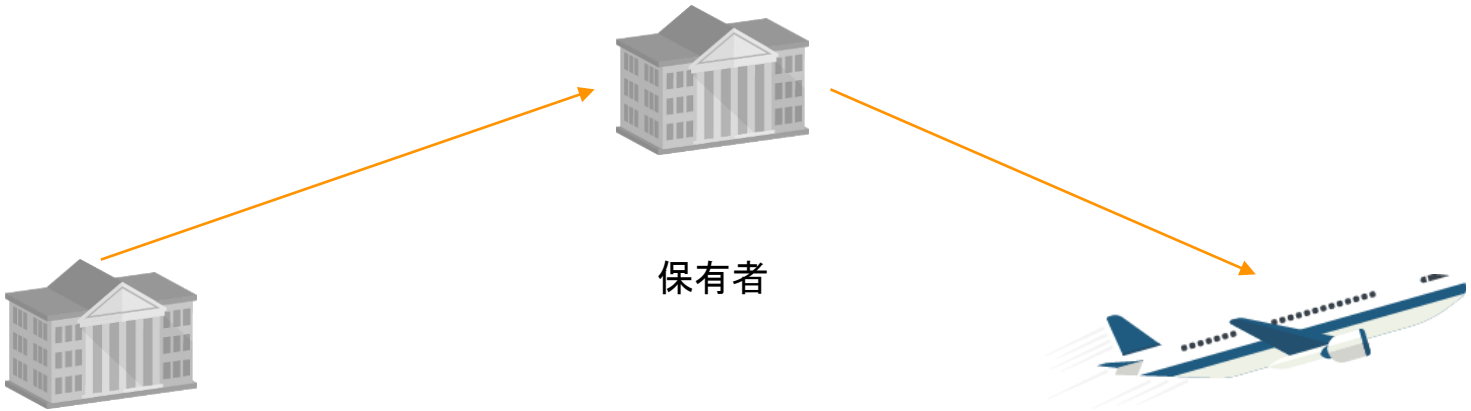
役割は互いに排他的なものではない。



役割は互いに排他的なものではない。



分散型アイデンティティ・エコシステムにおける役割



分散型アイデンティティ・エコシステムにおける役割

ノード
元帳を管理するネットワークの
サポートと構築

Indicio

分散型アイデンティティ・エコシステムにおける役割

エージェント

参加者に代わって動作し、ネットワークや台帳とのやり取りを可能にするソフトウェア・プログラム。

エンタープライズ・エージェント

モバイル・エージェント

ノード

台帳を管理するネットワークのサポートと構築

エージェントは役割を表す

エンタープライズ・
エージェント

発行者

検証者

検証者エージェント

エッジ・エージェント

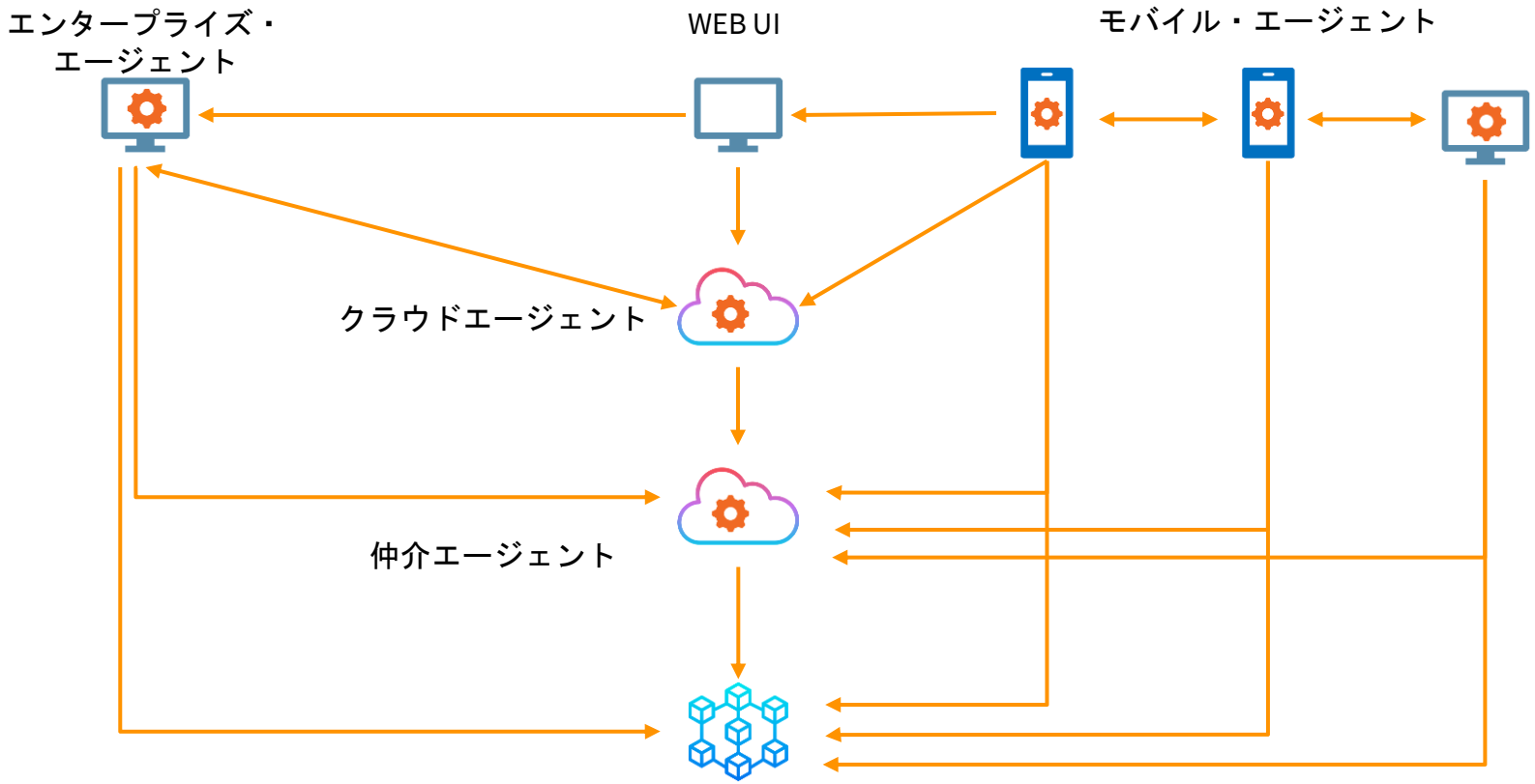
保有者

Indicio

エージェントは役割を表す

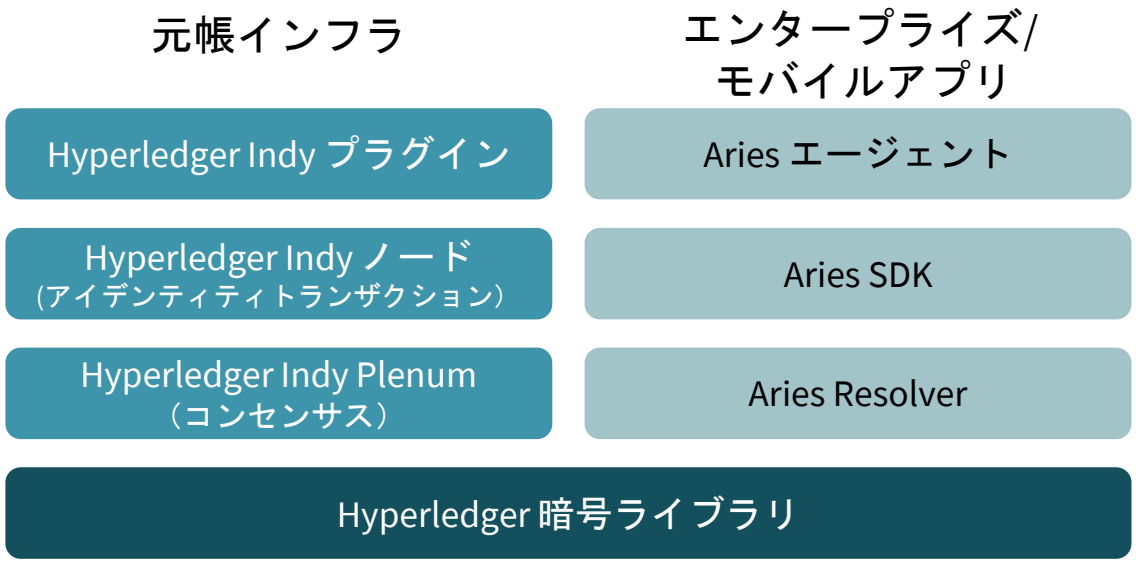
1つのエージェントが
複数の役割を管理するように
設定することができる。

アーキテクチャ概要



Indicio

Hyperledger コード プロジェクト



進化する規格

Hyperledger

- Aries - エージェント、暗号化メッセージ、プロトコル、VC交換
- Indy - 検証可能なデータ登録、豊富なセマンティクス

Decentralized Identity Foundation (DIF)

- DIDComm
- 分散型ガバナンス

World Wide Web Consortium （W3C）

- VCデータモデル
- DID仕様

Trust over IP Foundation （ToIP）

- ガバナンス（中央トラスト・レジストリ）

進化する規格

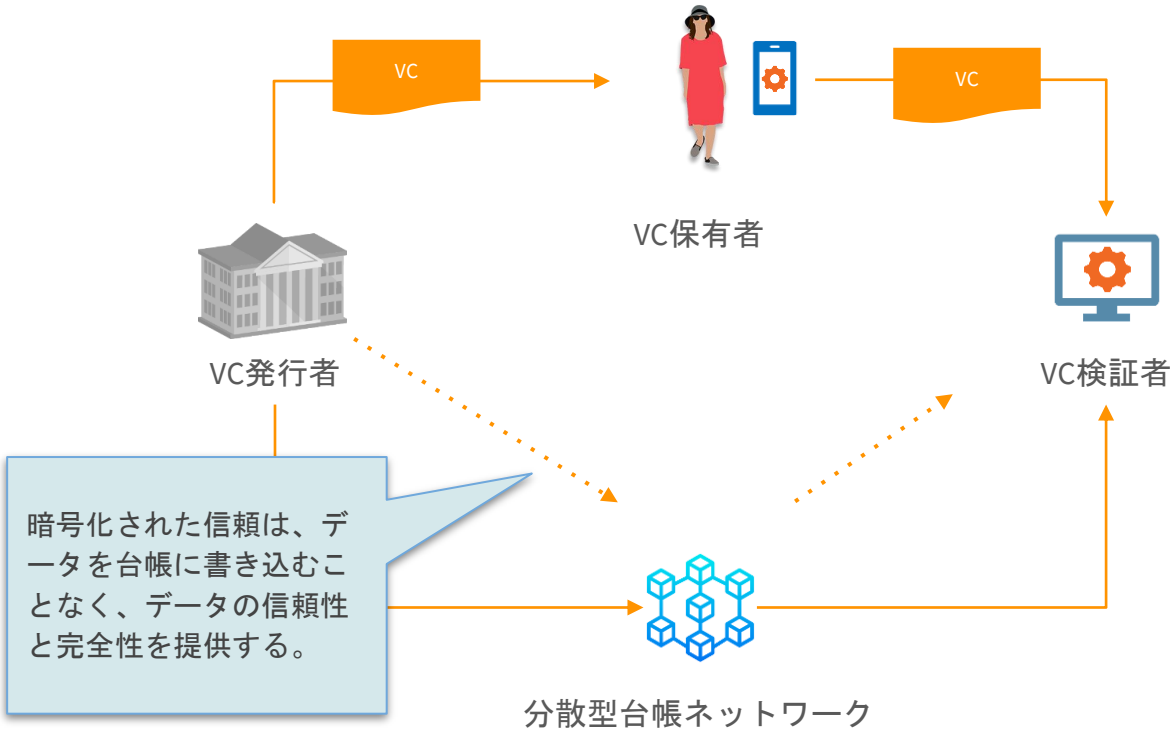
Open Badges

- JSON-LD（JavaScript Object Notation for Linked Data）クレデンシャル
  教育／実績／認定資格

OID4VC

- JWT（JSONウェブトークン）クレデンシャルタイプの発行、要求、提示のための
  プロトコル

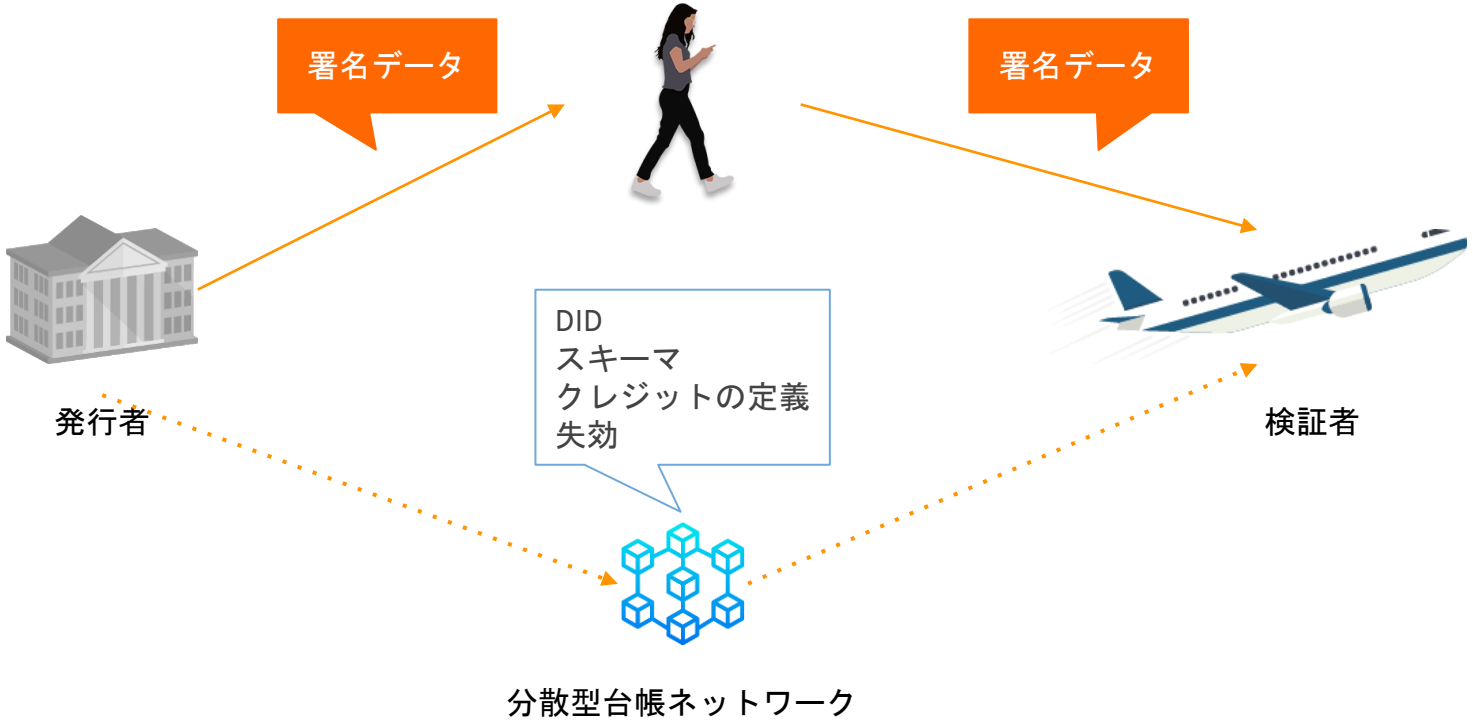
分散型アイデンティティ・エコシステムにおける役割



indicio academy

VCと台帳

台帳



個人情報が台帳に載ることはない

すべての個人情報（およびすべてのVC内の情報）は、データの所有者または承認された管理者に留まる。

プライバシー・バイ・デザインとデータコンプライアンスの確保。

台帳は、実際のデータを保存したりチェックしたりすることなく、
データの信憑性と完全性を検証することができる。

台帳のオブジェクト

- DIDs（Decentralized Identifiers - 分散型識別子）
- スキーマ
- クレデンシャルの定義
- 失効登録

これらのオブジェクトにより、**中央機関に依存することなく**
発行者は、暗号的に検証されるVCを定義・発行できる。

DIDs（Decentralized Identifiers - 分散型識別子）

どのようなものからも独立して実装できる

- 集中型レジストリ
- IDプロバイダー
- 認証局

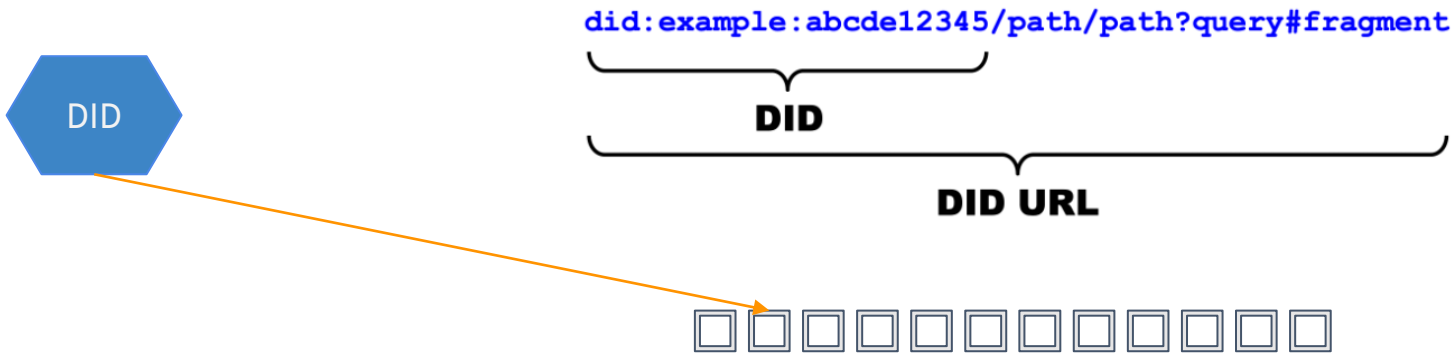
DIDsは、相関を防ぐために、すべてのやり取りに固有のIDを提供することができる。

- パブリック（帳簿上）
- プライベート（帳簿外）

DIDのコントローラは、そのDIDの制御を暗号的に証明できる。

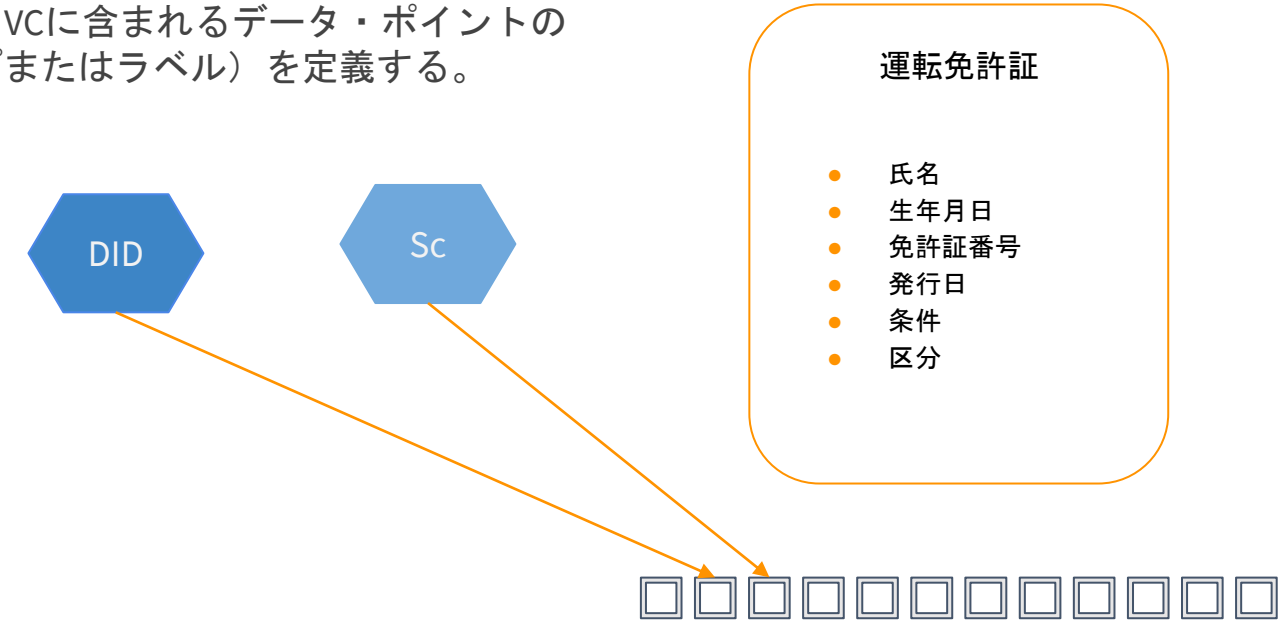
DIDs（Decentralized Identifiers - 分散型識別子）

- DIDは、DID文書を返すURLである。
- DIDの主体はエンティティ（人、組織、モノ）である。
- DIDからDID文書への変換は、以下の手段を提供する：
  - キーの認証
  - 主体（DIDを作成した人）にメッセージを送る

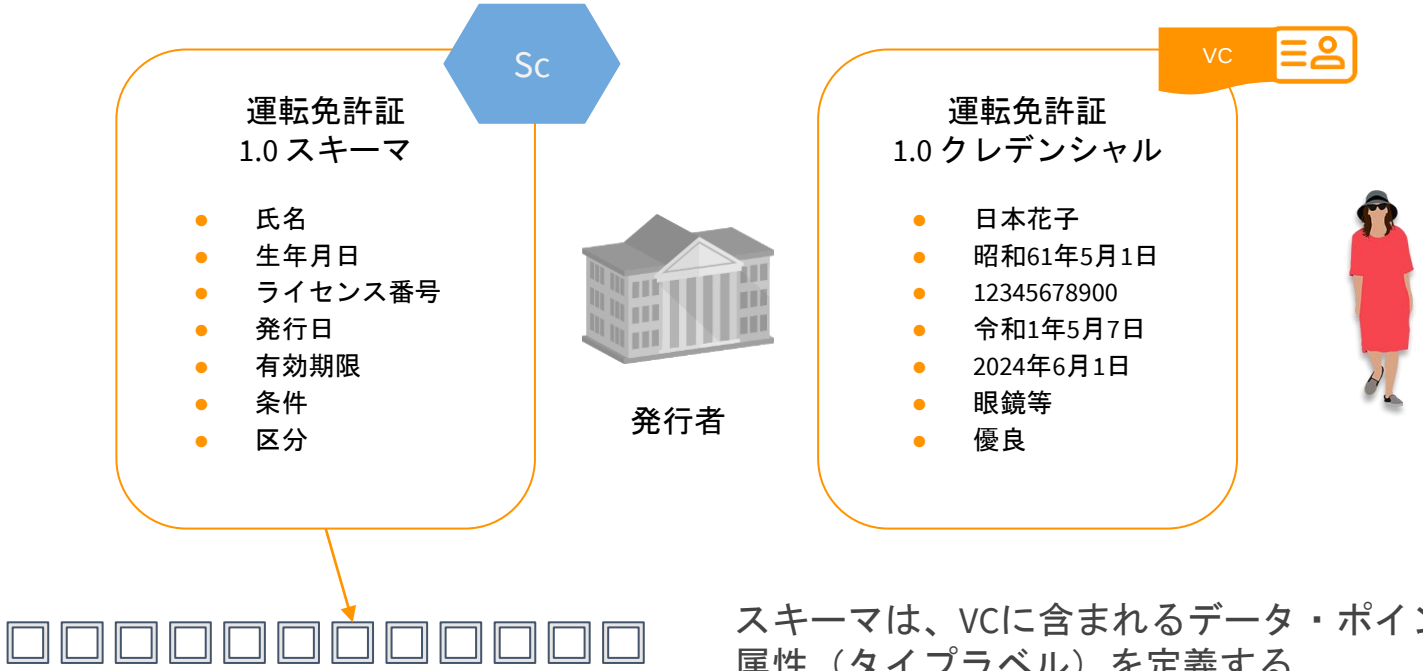


属性データのスキーマ

スキーマは、VCに含まれるデータ・ポイントの
属性（タイプまたはラベル）を定義する。

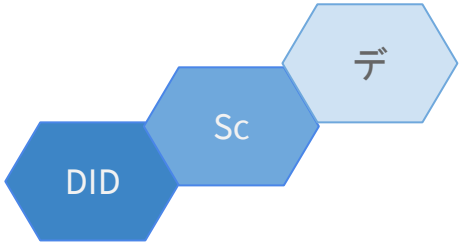


属性データのスキーマ

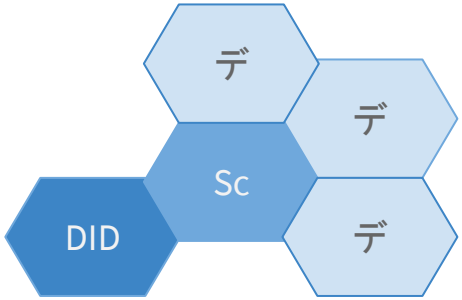


スキーマは、VCに含まれるデータ・ポイントの属性（タイプラベル）を定義する。

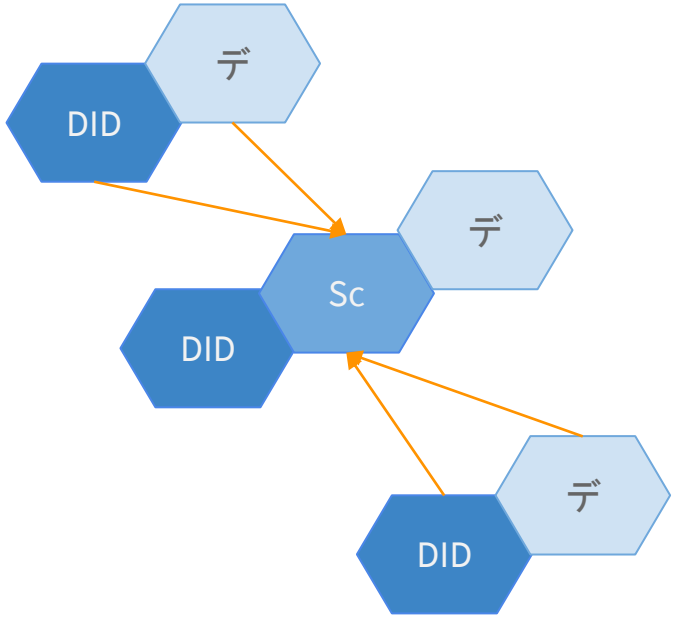
関係性



1 発行者 -> 1 スキーマ -> 1 クレデンシャル定義



1 発行者 -> 1 スキーマ -> #n クレデンシャル定義



#n 発行者 -> 1 スキーマ -> #n クレデンシャル定義

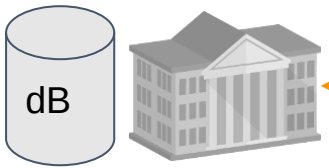
失効

- VCの不正な属性を修正する。
  - 失効／再発行
- VCが無効/盗難/その他の場合。
- 失効登録には以下のものが含まれる。
  - すべてのVCの識別子
  - 失効したVCの識別子
  - アキュムレーター
- 保有者は、提示時に登録簿にクレデンシャル ID の証明を作成する。
- VCの提示を受信した検証者は、失効レジストリを使用して、
  VCが失効 されていないことを検証する。

VCは、保有者の所有から削除されない。検証者に提示すると、失効したVCの登録簿に登録され、その有効性を取り消すことができる。

VC（Verifiable credentials - 検証可能な資格情報）

閲覧または所有の許可を得て
団体が収集したデータ

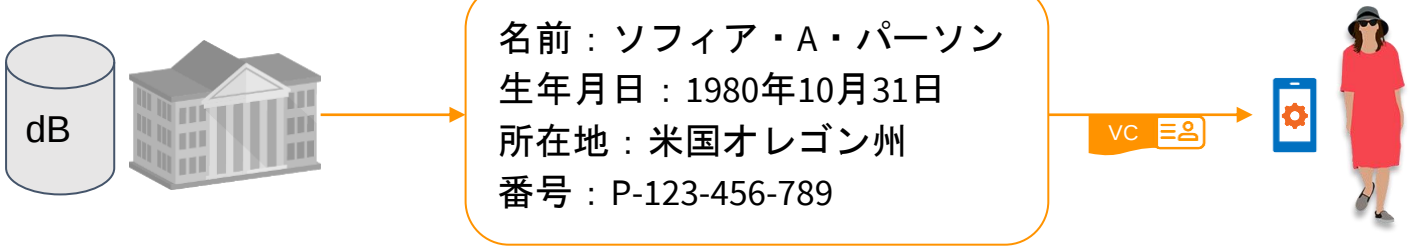


発行者

名前：ソフィア・A・パーソン
生年月日：1980年10月31日
所在地：米国オレゴン州
番号：P-123-456-789

VC（Verifiable credentials - 検証可能な資格情報）

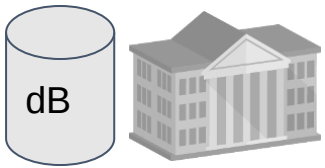
暗号的に署名され、
VC保有者に渡される。



署名タイプは、検証者に対するVC属性の開示に関して、 特定の能力を決定する場合がある。

VC（Verifiable credentials - 検証可能な資格情報）

名前：ソフィア・A・パーソン
生年月日：1980年10月31日
所在地：米国オレゴン州
番号：P-123-456-789



発行者

署名タイプは、検証者に対するVC属性の開示に関して、 特定の能力を決定する場合がある。

CL ZKP（AnonCreds）
最も強力で、選択的開示とゼロ知識証明を可能にする。

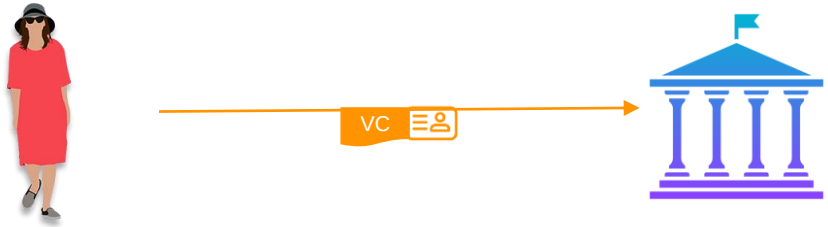
JSON-LD
リンクされたデータ署名は選択的開示を提供できるが、ゼロ知識証明は提供できない。

SD-JWT
選択的開示を可能にする。使用頻度が低い。

VC（Verifiable credentials - 検証可能な資格情報）

名前：ソフィア・A・パーソン
生年月日：1980年10月31日
所在地：米国オレゴン州
番号：P-123-456-789

保有者が検証者にVCを提示する。

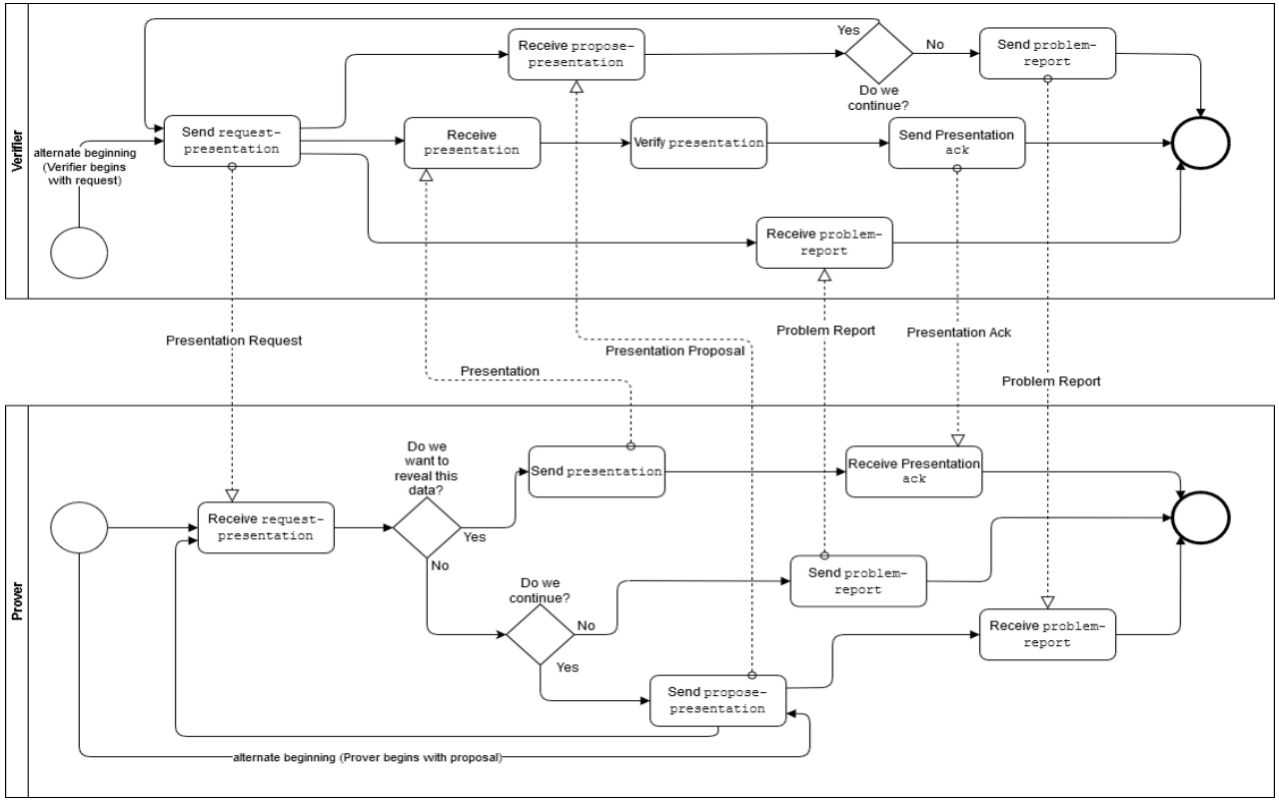


検証者

プレゼンテーションは通常、要求応答モデルによって設計され、
検証者は全体的なVCではなくVC属性を要求する。

プレゼンテーションをインタラクションにコード化し、
接続時に自動的に行うこともできる。

VC（Verifiable credentials - 検証可能な資格情報）



検証プロセス

事務手続きの承認は、
信頼とガバナンス執行の働きである。

保有者

署名データ

信頼できる発行者
＋
承認されたデータ値

検証者

ガバナンスの選択

信頼できない発行体
および/または
未承認のデータ値

DID
スキーマ
クレジットの定義
失効

分散型台帳ネットワーク

Indicio

indicio academy

ご清聴ありがとうございました