JNSA アイデンティティ管理WG主催
「クロスボーダー時代のアイデンティティ管理セミナー」

ブロックチェーンが実現する（かもしれない）未来のIDとID管理基盤の姿

株式会社アイピーキューブ
貞弘　崇行

お持ち帰りいただきたいモノ

- Internet Identityの進化
- Self-Sovereign IDentityとその位置付け
- SSIDを支える技術としてのブロックチェーン
- 応用例としてのSovrin
- ユースケース

お約束

- 個人の見解であって、会社などを代弁しているわけではないです。
  - 想像や妄想も入ってます。
- SSIDもブロックチェーンもSovrinもまだまだ勉強中です。間違ってたらごめんなさい。

Internet Identityの進化

背景

- インターネットのアドレスシステム:
  →ネットワーク上のエンドポイント特定が目的
  →インターネット上に人を識別する術はない

結果

- エンドポイント側で人の識別
  →各エンドポイント(＝サービス)側で人の情報を持つ

Internet Identityの進化

結果

- エンドポイント側で人の識別
  →各エンドポイント（＝サービス）側で人の情報を持つ

出典：Tobin, A., & Reed, D. (2016). The Inevitable Rise of Self-Sovereign Identity. Retrieved 2017/09/25, from https://sovrin.org/library/rise-of-self-sovereign-identity/

Internet Identityの進化

何があるべき姿なのか？

物理世界でのIdentityの特性は？

健康診断5年連続総合評価A

東京都に住んでる

小学生からスキーやってた

（株）アイピーキューブの社員

JNSA IDWGのメンバー

SSIDに興味あります

Internet Identityの進化

物理世界でのIdentityの特性は？

- セキュリティ
  :属性を意図しない開示から保護
- コントロール
  :属性を誰に何の目的で開示するか制御
- ポータビリティ
  :属性は本人に付随し、どこでも利用可

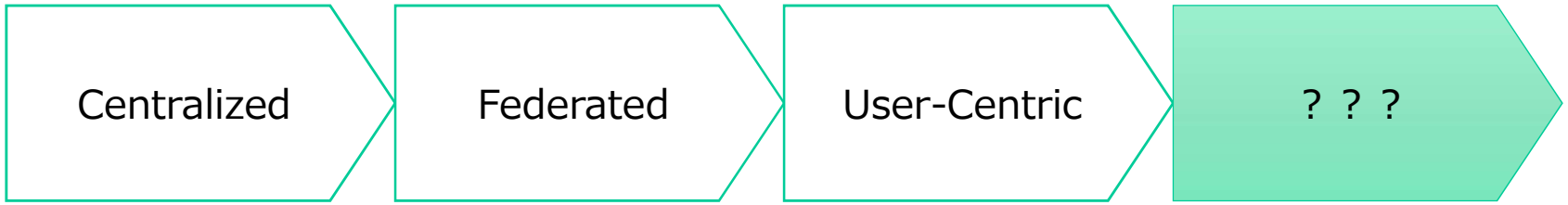
Internet Identityの進化

Internet Identityの現実

- セキュリティ
  :頻発するデータ漏えい
- コントロール
  :利用規約で、属性の利用はサービス側に牛耳られている（cf. カウンターとしてのGDPR）
- ポータビリティ
  :属性はサービス側が保持するため、ポータビリティはない

Internet Identityの進化

あるべき姿へ近づく進化



出典：Tobin, A., & Reed, D. (2016). The Inevitable Rise of Self-Sovereign Identity. Retrieved 2017/09/25, from https://sovrin.org/library/rise-of-self-sovereign-identity/

Internet Identityの進化

あるべき姿へ近づく進化

- Centralized
  :サービス内部での共通化（企業内でのID統合、SSOもその一環）
- Federated
  :サービス間でのID連携
- User-Centric
  :属性を単一のサービスに集め、利用者が属性へのアクセスを制御（例　パーソナルデータストア、ベンダーリレーションシップマネージメント）

Internet Identityの進化

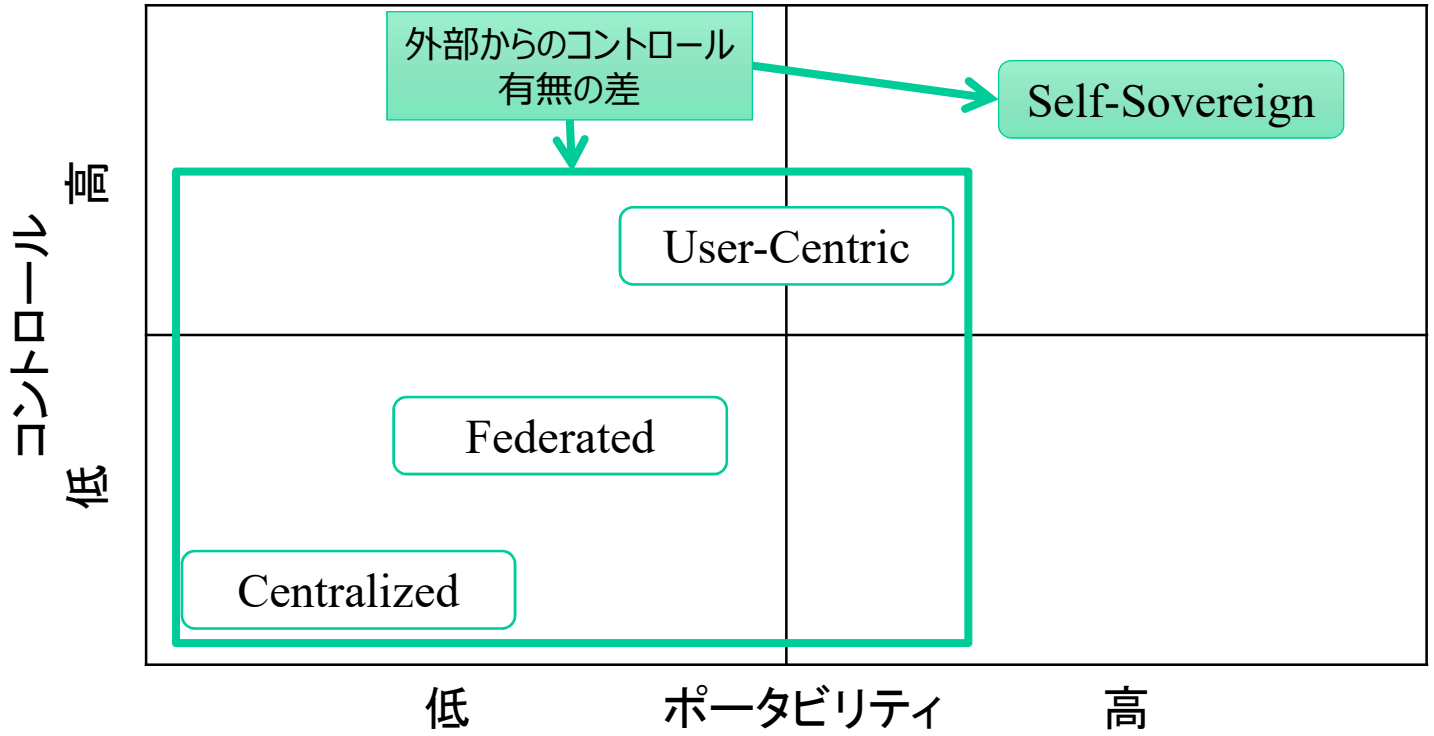
あるべき姿へ近づく進化

（次ページの軸のリマインド）

- コントロール：IDの所有者が自身のデータに対してどんな目的でアクセス出来るかを制御できるか
- ポータビリティ：IDデータの所有者がどこでも好きなところでIDデータを利用でき、かつ、単一のID Providerに縛られないか

SSIDとその位置付け

Internet Identity進化でのSSIDの位置付け

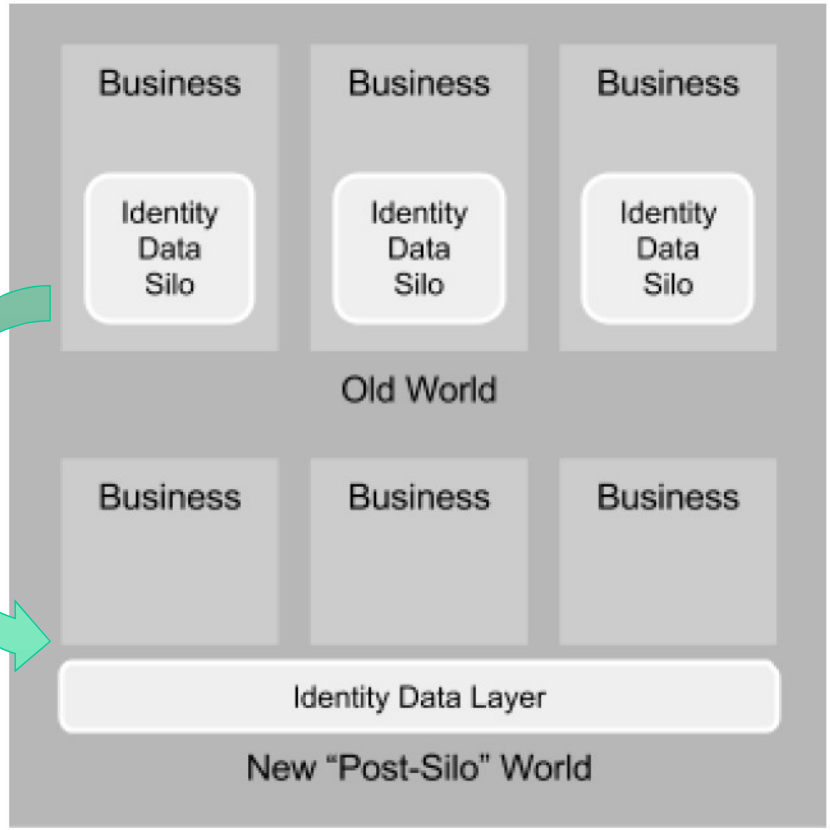


出典：Tobin, A., & Reed, D. (2016). The Inevitable Rise of Self-Sovereign Identity. Retrieved 2017/09/25, from https://sovrin.org/library/rise-of-self-sovereign-identity/

SSIDとその位置付け

IDレイヤーとSSID

- Identityのポータビリティを維持し、エンドポイントから外すこと
  ＝Identityをエンドポイントを支えるレイヤーとして捉えること



出典：Tobin, A., & Reed, D. (2016). The Inevitable Rise of Self-Sovereign Identity. Retrieved 2017/09/25, from https://sovrin.org/library/rise-of-self-sovereign-identity/

SSIDとその位置付け

IDレイヤーとSSID

- インターネットと同様の耐性を持ち、単一もしくはごく少数の組織による支配を受けない、複数組織をまたがるID層
- インターネットのID層へアクセスさえすれば、既にそこに存在する既存組織や個人、政府などの情報を活用できるようになる

SSIDを支えるブロックチェーン

ブロックチェーンの特徴

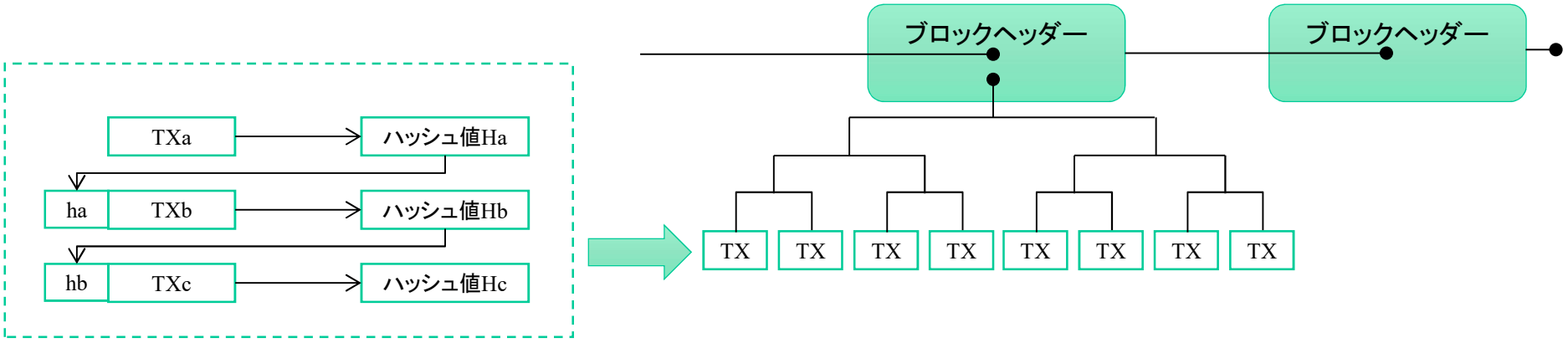
- トランザクションの改ざんの困難さ
- 非中央集権的な管理

SSIDを支えるブロックチェーン

ブロックチェーンの特徴

- トランザクションの改ざんの困難さ

  :トランザクションをその生じた順に前のトランザクションのハッシュ値とデジタル署名を付加し、ブロック化。
  →改ざんしようとすると、過去のトランザクションを全て作り直し・・・



出典:松尾, et.al (2018). ブロックチェーン技術の未解決問題. 東京. 日経BP

SSIDを支えるブロックチェーン

ブロックチェーンの特徴

- 非中央集権的

  :トランザクションやブロックの管理（生成や保持）を、中央集権的な誰かが行うわけでは無く、参加するノード*で分散して実施する。

  *：ブロックチェーンの種類によって変わる。全ノードができる場合も有るし、特定の役割を担うノードがやる場合も有る

SSIDを支えるブロックチェーン

JNSA

例としてBitcoin
→ブロックチェーンの通貨応用例

トランザクション		通貨の取引（送金、受領、etc.）
非中央集権的な管理		↓
	ブロックを生成するノード	Proof of Workという暗号処理を最も早く正しく完了したノード。計算能力依存。
	ブロック生成の理由	採掘手数料がもらえる
	ブロックを保持するノード	参加する全ノード

- 参加するノードを限定しない（不正が入り込む余地）
- 計算能力が高いと、改ざんが可能。

SSIDを支えるブロックチェーン

ブロックチェーンの特徴のIdentityへの応用

- トランザクションの改ざんの困難さ
  :属性の付与、剥奪、etc.をトランザクションと捉える
- 非中央集権的な管理
  :属性のトランザクションを分散したノードで共有する

- 参加するノードを限定する（不正を入れにくくする）
- 計算能力依存にさせない

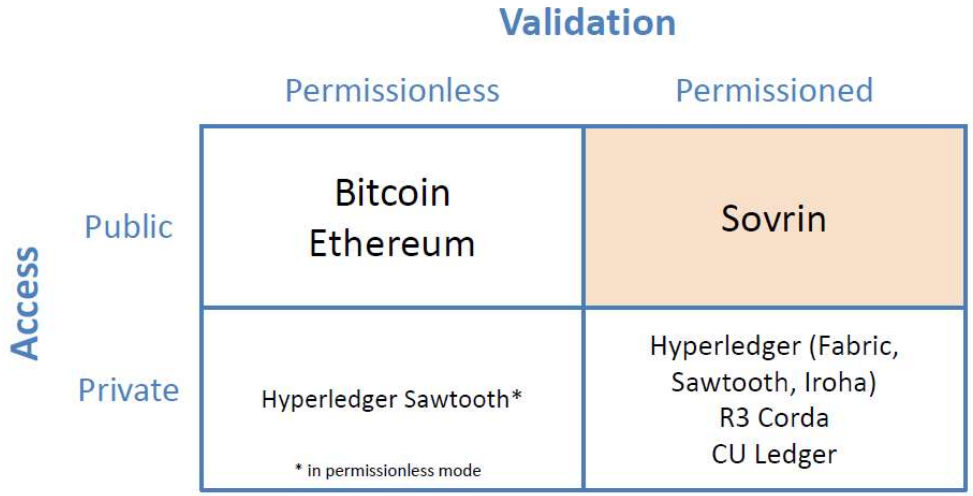
応用例としてのSovrin

ブロックチェーンの分類

- Public:
  誰でもアクセス出来る
- Permissioned:
  ブロック管理は許可されたノードのみ

利点

- マイニング無関係
  →コンピューティング
  リソース多寡無関係
- 目的の強制
  →野良アプリケーション
  の排除



出典:Tobin, A., & Reed, D. (2016). The Inevitable Rise of Self-Sovereign Identity. Retrieved 2017/09/25, from https://sovrin.org/library/rise-of-self-sovereign-identity/

応用例としてのSovrin

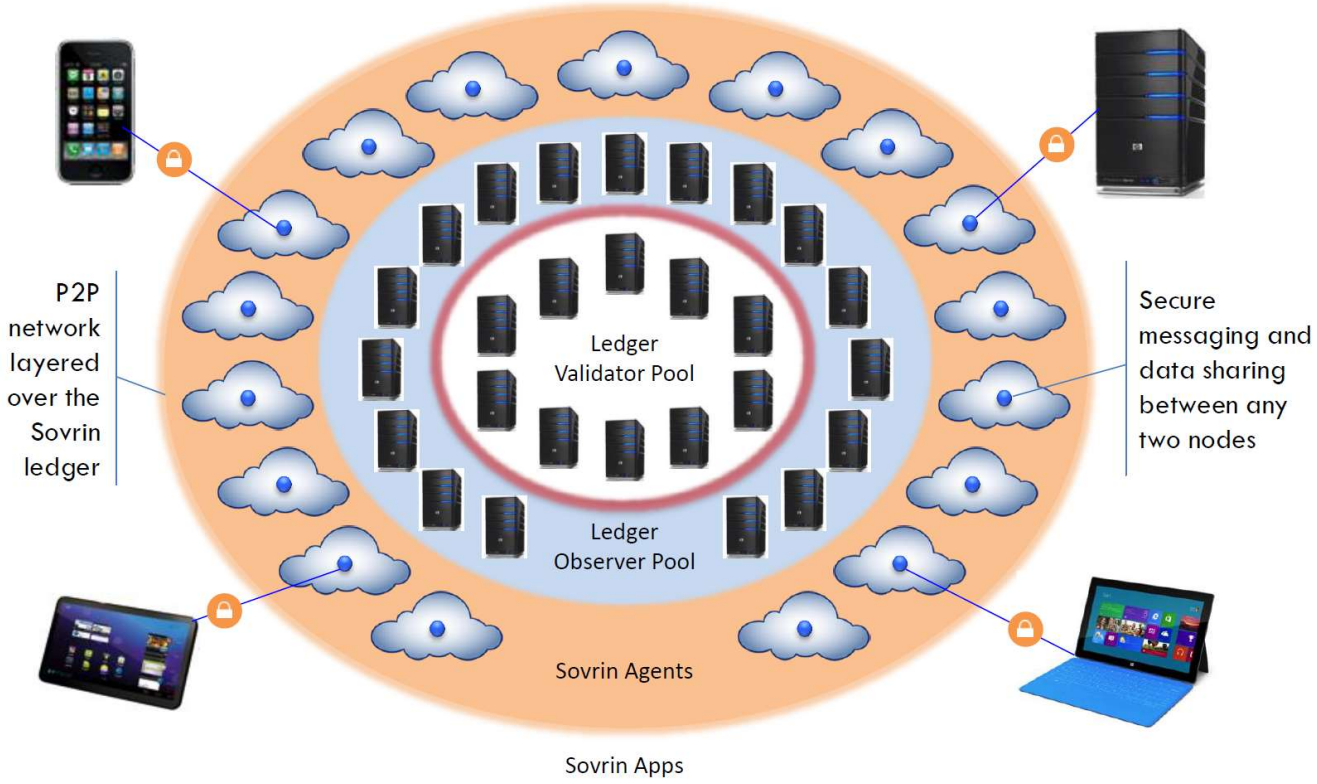
Sovrin

→ブロックチェーンに基づいたSSID実現例

トランザクション		Identityの属性操作（発行、剥奪、etc.）
非中央集権的な管理		↓
	ブロックを生成するノード	Sovrin Foundation（NPO）が認めたLedger Validationノード
	ブロック生成の理由	Sovrinフレームワークへの参加手数料の徴収
	ブロックを保持するノード	Sovrin Foundationが認めたObserverノード、Ledger Validationノード

応用例としてのSovrin

構成



出典：Tobin, A., & Reed, D. (2016). The Inevitable Rise of Self-Sovereign Identity. Retrieved 2017/09/25, from https://sovrin.org/library/rise-of-self-sovereign-identity/

応用例としてのSovrin

Sovrin Foundationの位置付け

- Permissioned：Sovrin FondationがPermissionを与える
- InternetにおけるICANNと同様の考え方
- Self-Sovereign Identityを支えるには以下が必須
  ー　ノードが単一の会社や組織、政府に依存しないこと
  ー　逆にノードが複数の会社、組織、政府をまたがっていること
  ー　非営利組織により運営されること

応用例としてのSovrin

Sovrin Foundationの位置付け

Sovrin Foundationの義務

- Sovrin Trust Framework（法的、商業的、技術的なルール）の開発と維持
- 検証ノードを維持するSteward間の調整及び監視
- Sovrinプロジェクト（＝オープンソースのDLT）のガバナンス
- SSID実現のためのSovrin Identity Networkの展開

Sovrinが機能する仕組み 1/5

Sovrinが機能する仕組みの説明

- Sovrinの論理構造
- Subjectが他のEntityと関係性を持つ場合の動作
- Subjectが複数のEntityと関係性を持つ場合の動作
- Subjectが他のEntityに情報開示を行う場合の動作

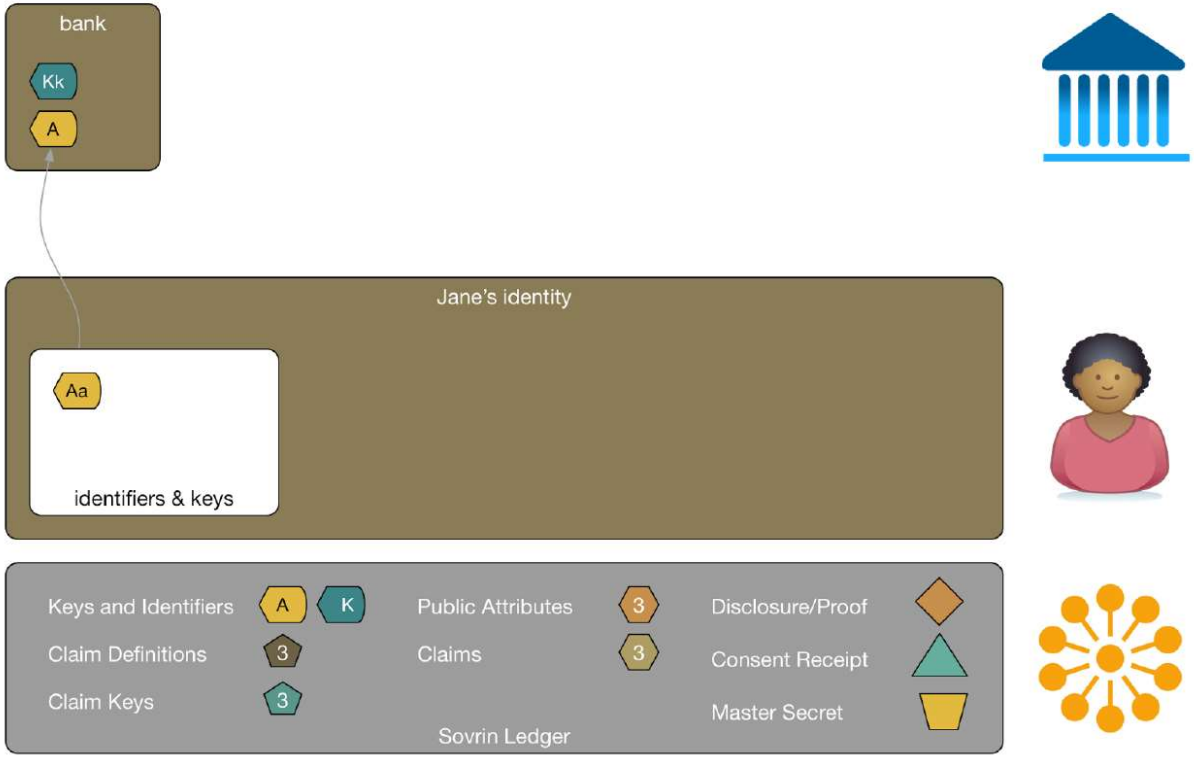
Sovrinが機能する仕組み 2/5

Sovrinの論理構造：Janeさんのケース（空っぽの状態）

出典：Windley, P. (2016). How Sovrin Works, A Technical Guide from Sovrin Foundation. Retrieved 2017/09/25, from https://sovrin.org/library/how-sovrin-works/

Sovrinが機能する仕組み 3/5

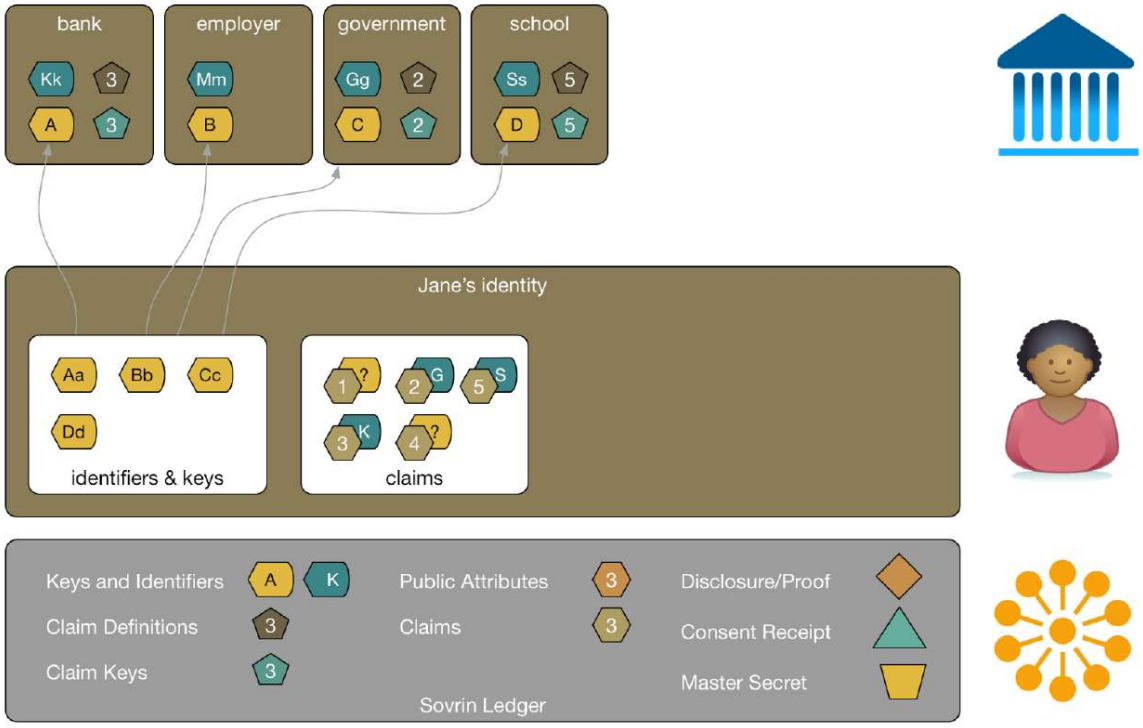
銀行との関係性が生じた（例　口座を持つ）場合に、銀行側でJaneさんを表すIdentifierとして公開鍵Aを持ち、Janeさん側ではそのAとそれに相当する秘密鍵であるaを持つ



出典：Windley, P. (2016). How Sovrin Works, A Technical Guide from Sovrin Foundation. Retrieved 2017/09/25, from https://sovrin.org/library/how-sovrin-works/

Sovrinが機能する仕組み 4/5

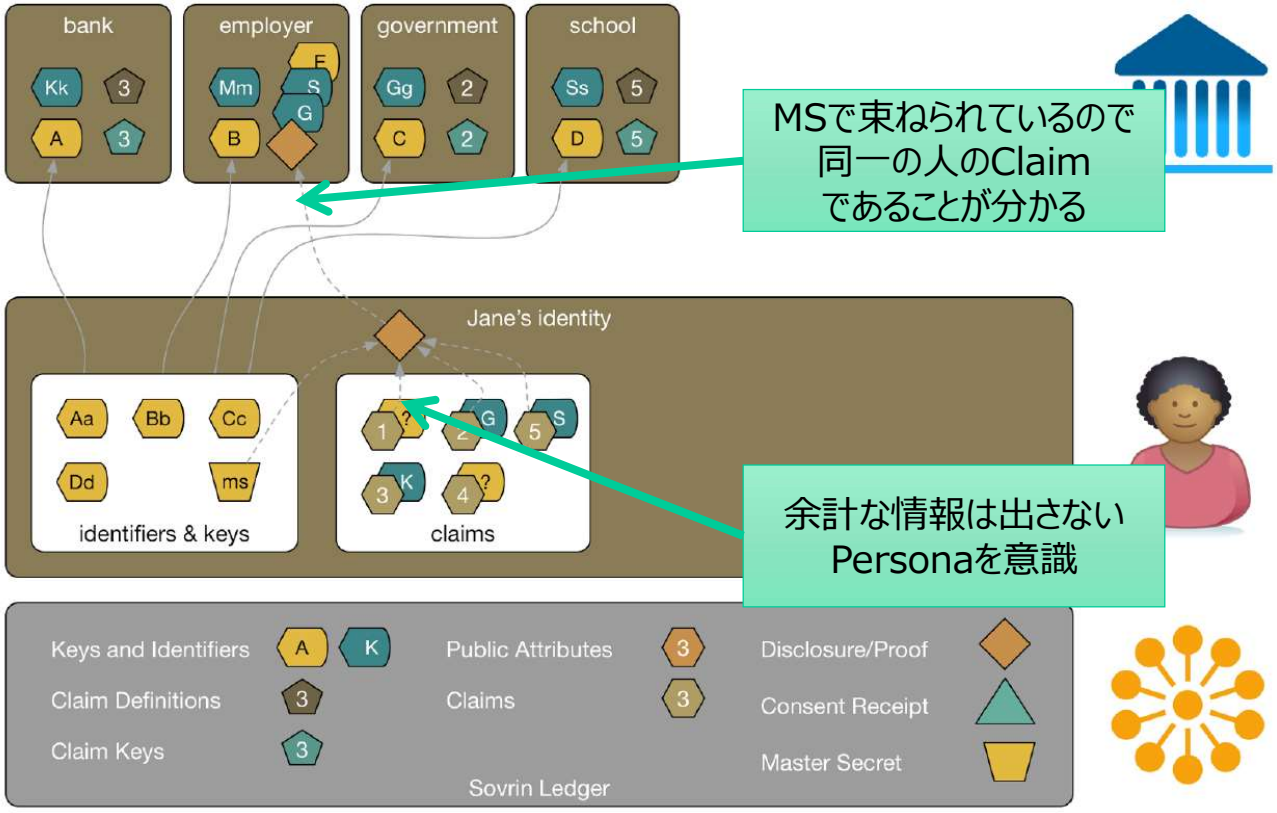
関係性のある組織毎に異なるIdentifierを持ち、それらの組織が発行したverifiable claimとself-asserted claimを持つ（以下の図ではclaim 1と4はself-asserted）



出典：Windley, P. (2016). How Sovrin Works, A Technical Guide from Sovrin Foundation. Retrieved 2017/09/25, from https://sovrin.org/library/how-sovrin-works/

Sovrinが機能する仕組み 5/5

求職に応募するために情報開示するケースでは、必要なClaim（verifiable：18歳以上、住所, self-asserted：性別）を組み合わせてMaster Secretで束ねて、Employerに開示する。



出典：Windley, P. (2016). How Sovrin Works, A Technical Guide from Sovrin Foundation. Retrieved 2017/09/25, from https://sovrin.org/library/how-sovrin-works/

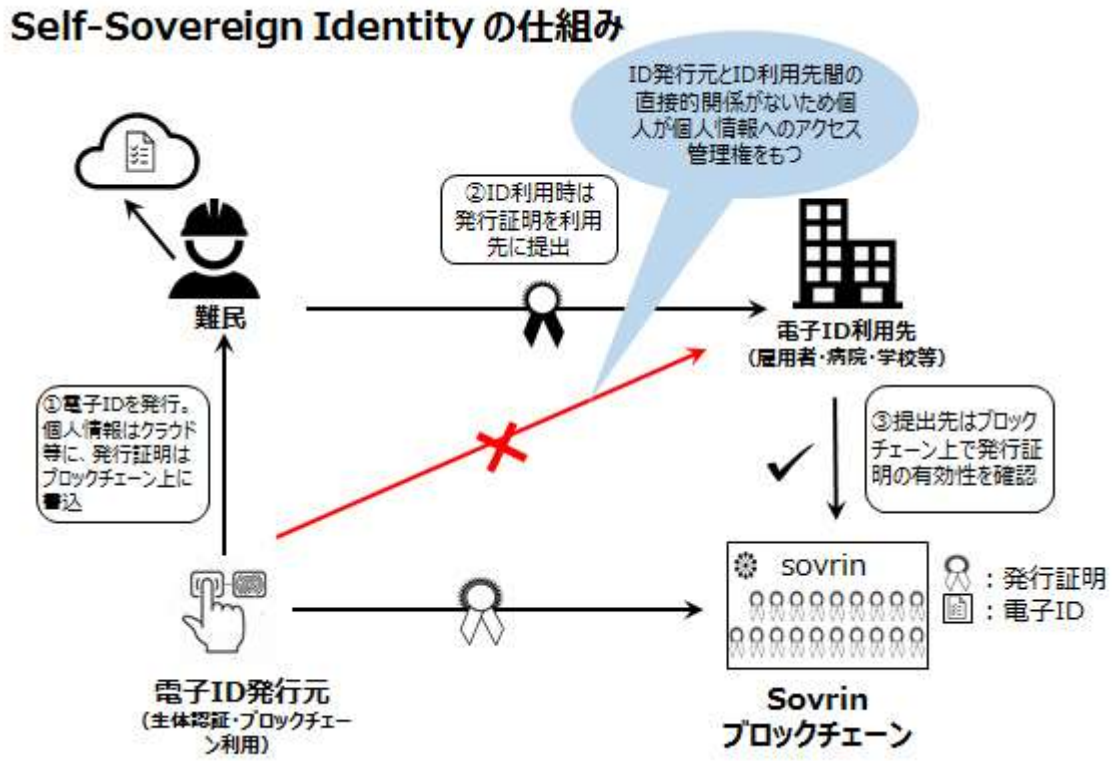
SSIDユースケース

Sovrinのユースケース

- 社会的弱者への自己証明型電子身分証明発行プロジェクト(The Invisibles)
  :戦災避難民や戸籍が未発達な国の住人などの公的機関による身分証明が不可能な人たちのInternet Identityを支える基盤
  - http://www.dhbr.net/articles/-/5146
  - 公的機関の身分証明が無くとも、Sovrinフレームワークに参加するEntityからの属性発行を証明できる

SSIDユースケース

The Invisibles

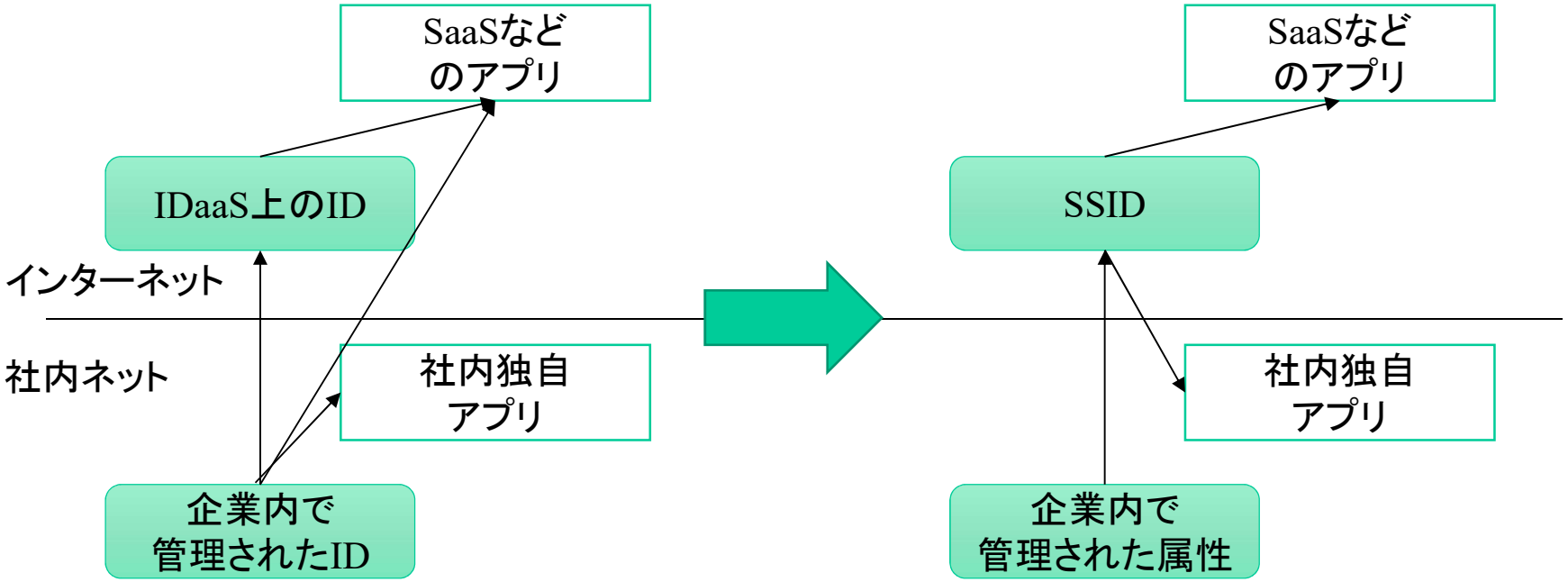


出典：安田, C., & 牧岡, (2017).テクノロジーを社会のためにブロックチェーンの技術で、個人情報を企業から個人の元へ取り戻す. Retrieved 2018/01/25, from http://www.dhbr.net/articles/-/5146

SSIDユースケース

将来的なユースケース

- 企業での利用？



お持ち帰りいただきたいモノ

- Internet Identityの進化
- Self-Sovereign IDentityとその位置付け
- SSIDを支える技術としてのブロックチェーン
- 応用例としてのSovrin
- ユースケース

参考文献

- Tobin, A., & Reed, D. (2016). The Inevitable Rise of Self-Sovereign Identity. Retrieved 2017/09/25, from https://sovrin.org/library/rise-of-self-sovereign-identity/
- 松尾, et.al (2018). ブロックチェーン技術の未解決問題. 東京. 日経BP
- Windley, P. (2016). How Sovrin Works, A Technical Guide from Sovrin Foundation. Retrieved 2017/09/25, from https://sovrin.org/library/how-sovrin-works/