Principle of SSI

- 自己主権型アイデンティティの原理原則 -

by **@kota_yata**

八谷航太（やたがいこうた）

- 高2
- JS/TS書いてます
- 最近Markdownパーサーを作っている
- Marp初めて使った。これは良いぞ

by **@kota_yata**

今日のはなし

Self-Sovereign Identity（SSI: 自己主権型アイデンティティ）が個人的に盛り上がってて卒業論文これで書くことも確定したのでSSI単体についてここ2ヶ月くらいで調べたことを少し紹介します。

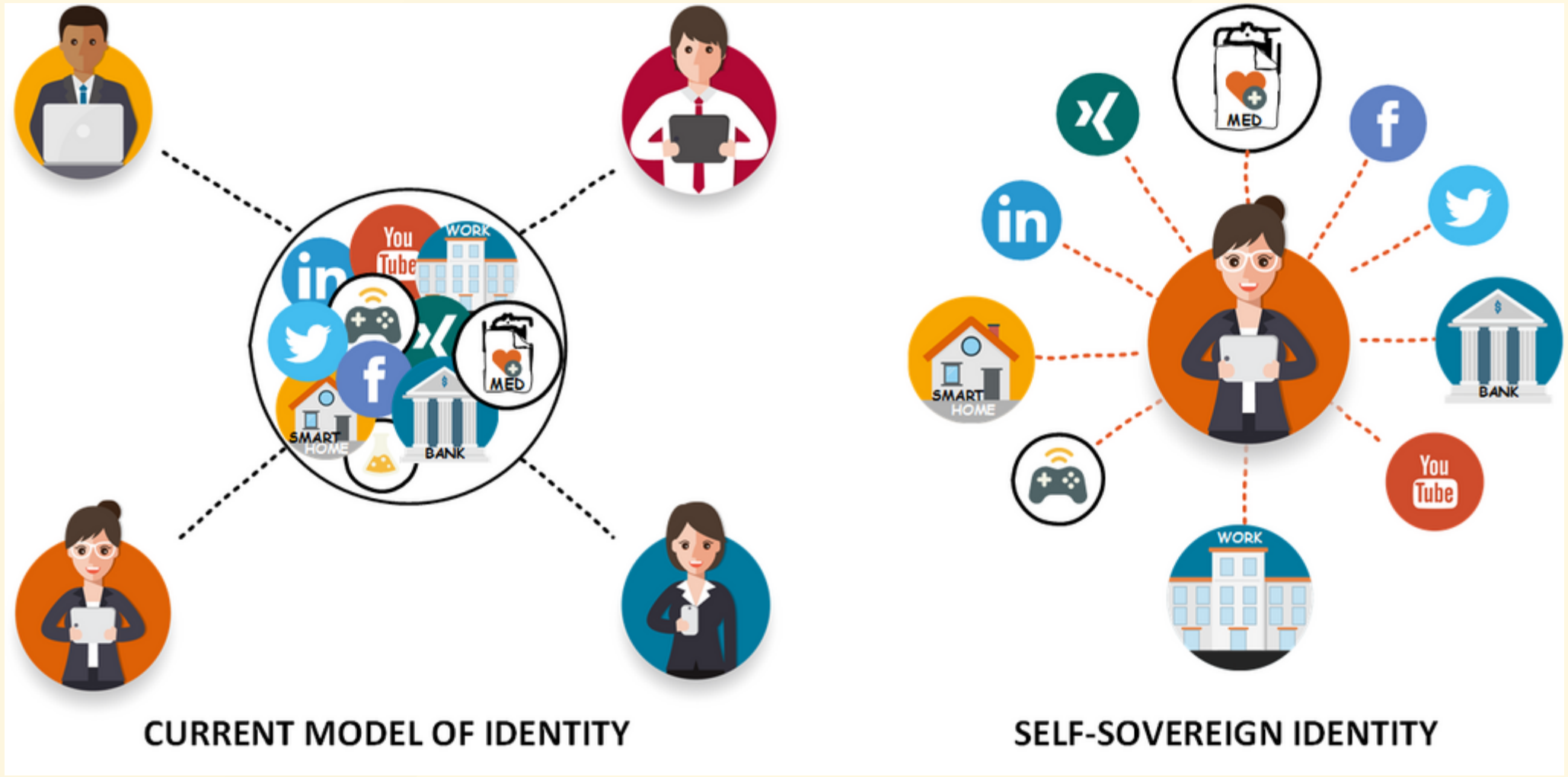
なので今日はより技術的なDID(Decentralized Identifier)やVC(Verifiable Credential)の話はメインじゃないです。

もくじ

by **@kota_yata**

SSIってなに

- 自分のアイデンティティは自分で守ろうという**ポリシー**
- 自分を中心としたアイデンティティ管理を行うことが目的
- Christopher Allen氏による提唱
- SSIを実現する技術がVCとDID


You Tube
WORK
MED
SMART HOME
BANK
CURRENT MODEL OF IDENTITY
MED
SMART HOME
BANK
You Tube
WORK
SELF-SOVEREIGN IDENTITY

by **@kota_yata**

従来のアイデンティティ管理の問題点

- SPOF（単一障害点）になる
- プロバイダ側がアイデンティティを消失させる権利を持っている
- データ流出の危険性がある

SSI 10の原則

1. Existence
2. Control
3. Access
4. Transparency
5. Persistence
6. Portability
7. Interoperability
8. Consent
9. Minimalization
10. Protection

by **@kota_yata**

Existence（存在）

- ユーザーが実世界に存在している必要がある
- ユーザーが人である必要はない（車とか犬とかでも良い）

SSIはすでに存在するユーザーのアイデンティティの一部をアクセス可能にするものである

Control

- 自らのアイデンティティに最もアクセスできるのは自分である
- ユーザーは自分のアイデンティティを参照、変更できる
- 誰にどこまで公開するのか、完全に秘匿するのかもユーザー自身が決められる

※自分で自分のアイデンティティを全て証明するという意味ではない

Access

- 自らのアイデンティティに関する情報・証明書全てにアクセス権を持っていなければいけない
- これらの情報・証明書の変更を全て検知できる

※ これらの情報・証明書を自由に変更できるという意味ではない

Transparency（透明性）

- SSIを実現するシステムとアルゴリズムは公開されていなければならない
- 無料かつオープンソースで、他のアーキテクチャから独立しているものでないといけない

Persistence（永続性）

- アイデンティティはできる限り長く存在するべきである
- 理想は永遠に存在すること。最低でもそのアイデンティティシステムが時代遅れになるまでは存続するべき

証明書が変わってもデータが変わってもアイデンティティは永続すべきだよ

Portability

- アイデンティティに関する情報とサービスはWeb上において持ち運び可能でなければならない
- どんだけ信頼できる企業でも、いずれ消滅することは確実

単一の第三者企業にアイデンティティ管理を任せてはいけないという意味

Interoperability（相互接続性）

- アイデンティティは分野、地理的に分断されるべきではない
- ある一つの分野でしか使えないアイデンティティでは意味がない
- 国境またいだら使い物にならない電子機器は困るじゃん？

Consent（同意）

- ユーザーの同意なしにそのアイデンティティを利用することはできない
- アイデンティティの証明書も同意なしに有効化することはあってはならない

Minimalization（最小化）

- 証明書の開示は最小化されている必要がある

例えば一定年齢以上であるかを証明する際に、誕生年月日や年齢を開示する必要はない。ただ一定年齢以上であるという証明ができれば良い

- ここはZKP（ゼロ知識証明）と密接に関わる

Protection（権利の保護）

- ユーザーの権利・人権は保護されている必要がある
- サービスなどネットワーク側のニーズとユーザーの権利が衝突した場合、必ずユーザーの権利が優先されるべきである

SSIの課題

SSI元年から5年...

- SSIの概念がChristopher氏によって提唱されたのが2016年
  - https://www.coindesk.com/path-self-sovereign-identity
- 提唱からすでに5年たち、VC/DID関係も含めるとかなりの数の論文が出ている（もち英語）
- ところが未だにアイデンティティ管理は大企業のプロバイダが寡占している

なぜなのか

理由1: 実装例が少なすぎる

- SSIを取り巻く技術（VC/DID）の仕様は策定されている
- 一方で技術的な実装の例が少なすぎる
- W3CやDIF以外、非公式の実装文献が少ない

開発者「SSIやりたいけど文献少ないからまだいっか」

理由2: アイデンティティ管理の責任

- 第三者企業にアイデンティティ管理を任せない => **自己責任**
- ユーザー自身が責任を持ってアイデンティティの共有・秘匿を行う

つまりユーザー側にそれなりのリテラシーが求められる

残念ながら普通のユーザーはそこまで個人のアイデンティティ管理に興味はない

理由3: 快適さが足りない

- 第三者企業にアイデンティティ管理を任せるのは**快適だから**
- 開発者・ユーザー双方にとって、快適でないと普及には至らない

アイデンティティ管理の責任 < 実装・利用の快適さ（UI・UXが神）

これを満たせば普及する（かも）

まとめ

- SSIとは、アイデンティティを自分で管理するというポリシー
- 10の原則を満たしたアイデンティティ管理システムはまだない
- 従来のプロバイダに頼る管理方法より快適なエコシステムを構築しなければ普及の道は開けない

さいごに

SGGのSlackのチャンネルでSSIを語ってます
興味のある方は#ssiで一緒に仕様書読みましょう！

by **@kota_yata**