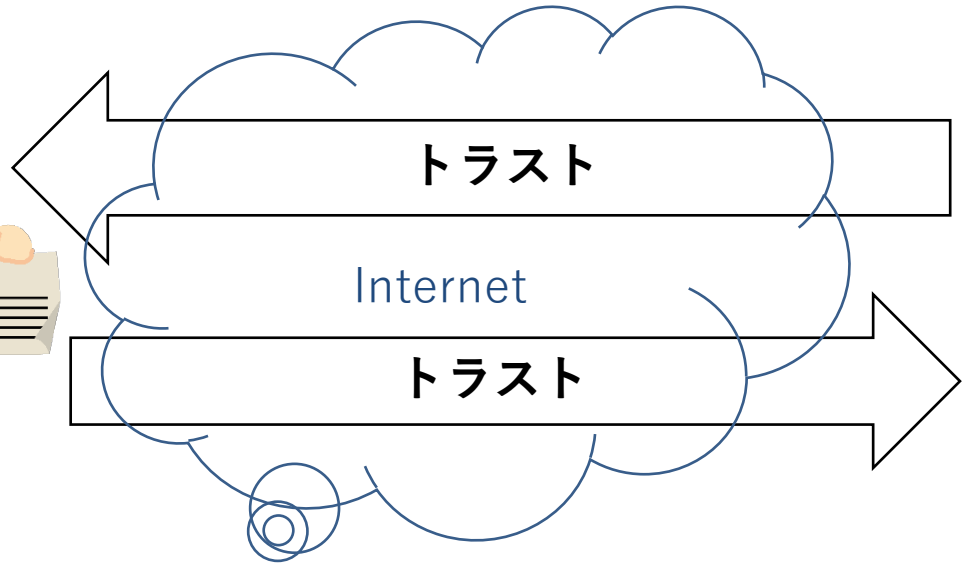
CAのなりすまし

◆石井先生は法的論点から分析
◇中川は技術とトラストから考察

中川裕志
理化学研究所・革新知能統合研究センター

従来のトラスト

事業者



本人

- 本人の認証があれば、化粧しているだけと思ってはマズいのか？
- でも警察官などを装ったらどうなのか？

平安時代からの問題
末摘花

自己イメージコントロール権　１００％保護してよいか？

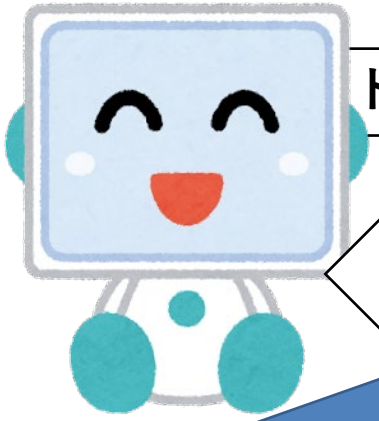
他者

トラスト

インター
ネット

トラスト

CA



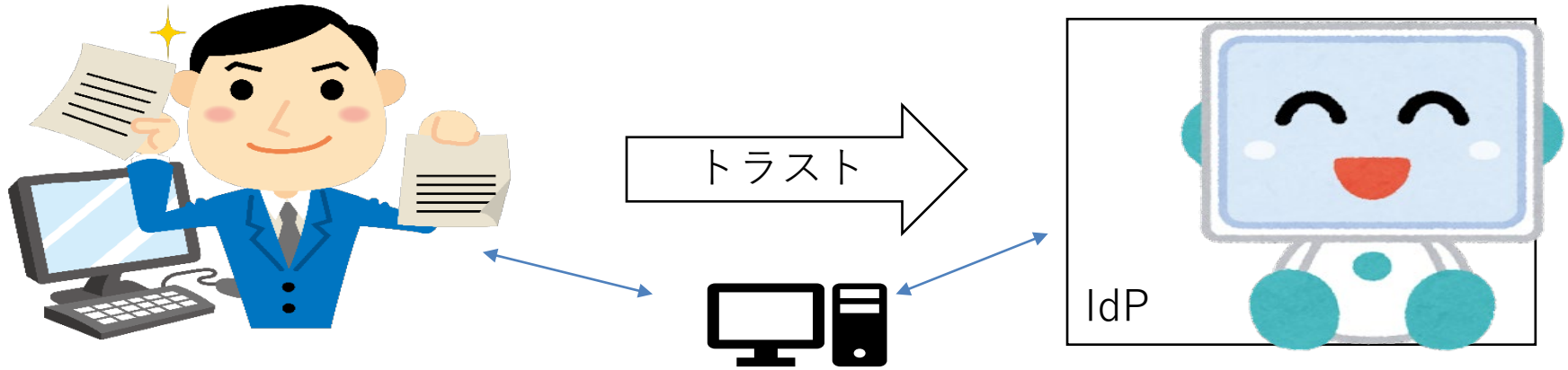
トラスト

トラスト

本人

本人とCAの人格的結びつきは、この双方向
トラストがないと成立しない

(1)論点③　匿名、仮名CAだと、そのCAの背後の操作者が分からない。CA自体をアイデンティティ認証する必要

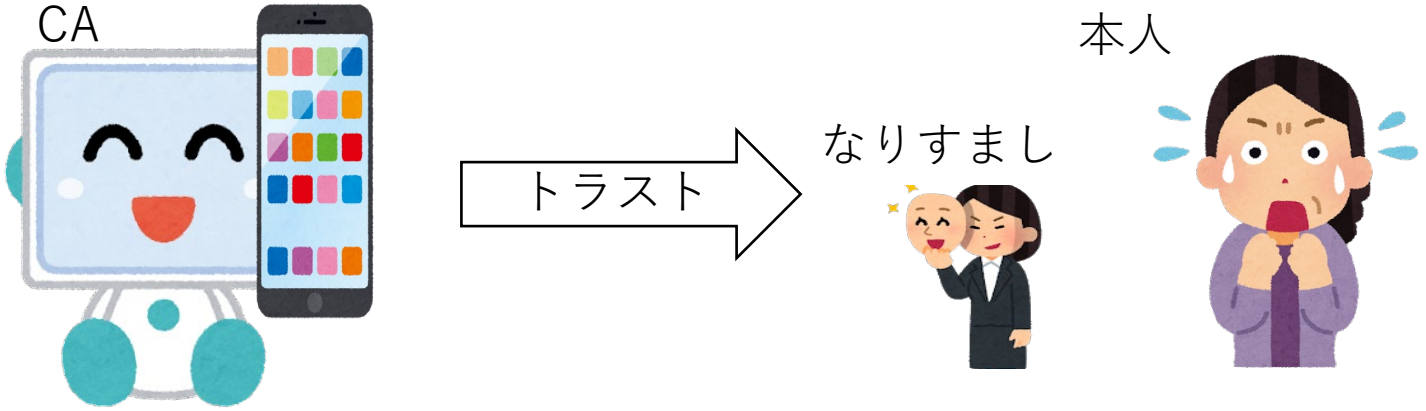


認証サーバ：IdP(Identity Provider)

- ディジタル　アイデンティティー
  - エンティティ認証：FIDO 2.0
  - ID連携認証：OpenID Connect 1.0
  - アクセス認証：OAuth 2.0

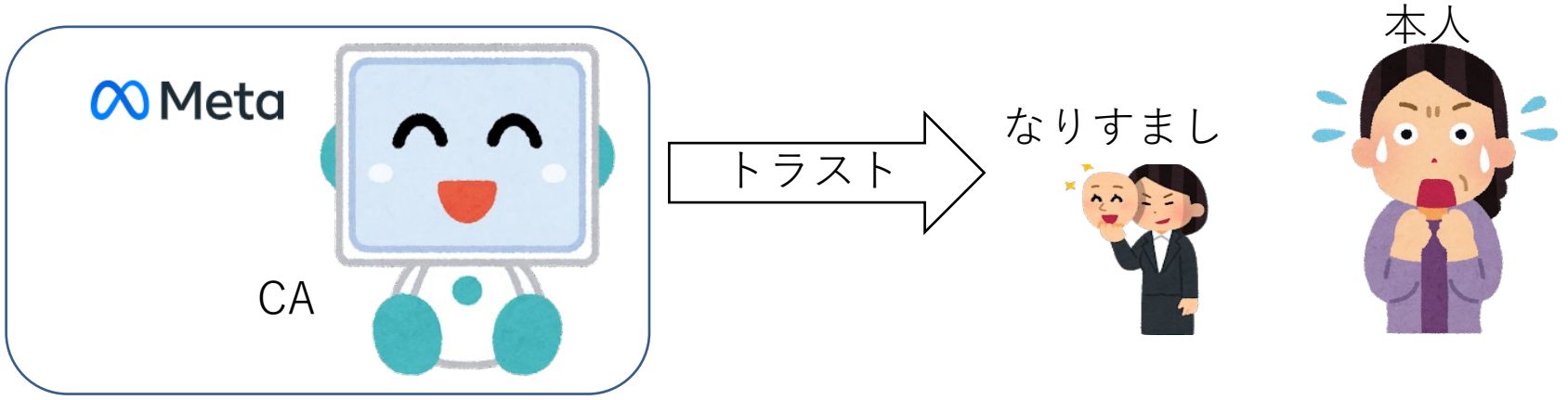
崎村夏彦著：デジタルアイデンティー　参照

- SSI
  - 個人（この場合はCA）がIdPとして個人認証を行う
  - できるだけ少ない情報で個人認証させる思想.

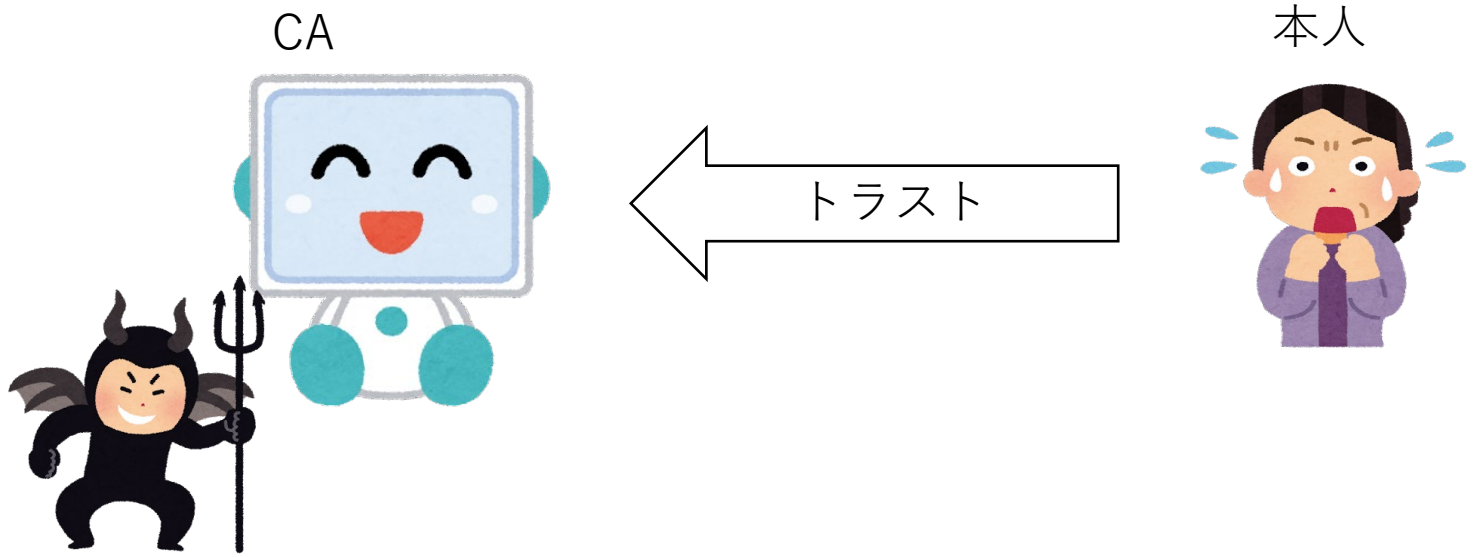


- 個人がCAを使うとき、CAが行う本人認証の問題
  - （パスワードや生体認証）による　　i.e. FIDO2.0
  - スマホなどがなりすまし人に乗っ取られることは常に起きうる問題
    - CAが乗っ取られたことを他者が認識できればよいのだが，実はこの部分は困難．AI技術の応用が待たれる。

- ログインするときには正しい利用者しか知らない鍵を用いる2段階認証が効果的だが．．．

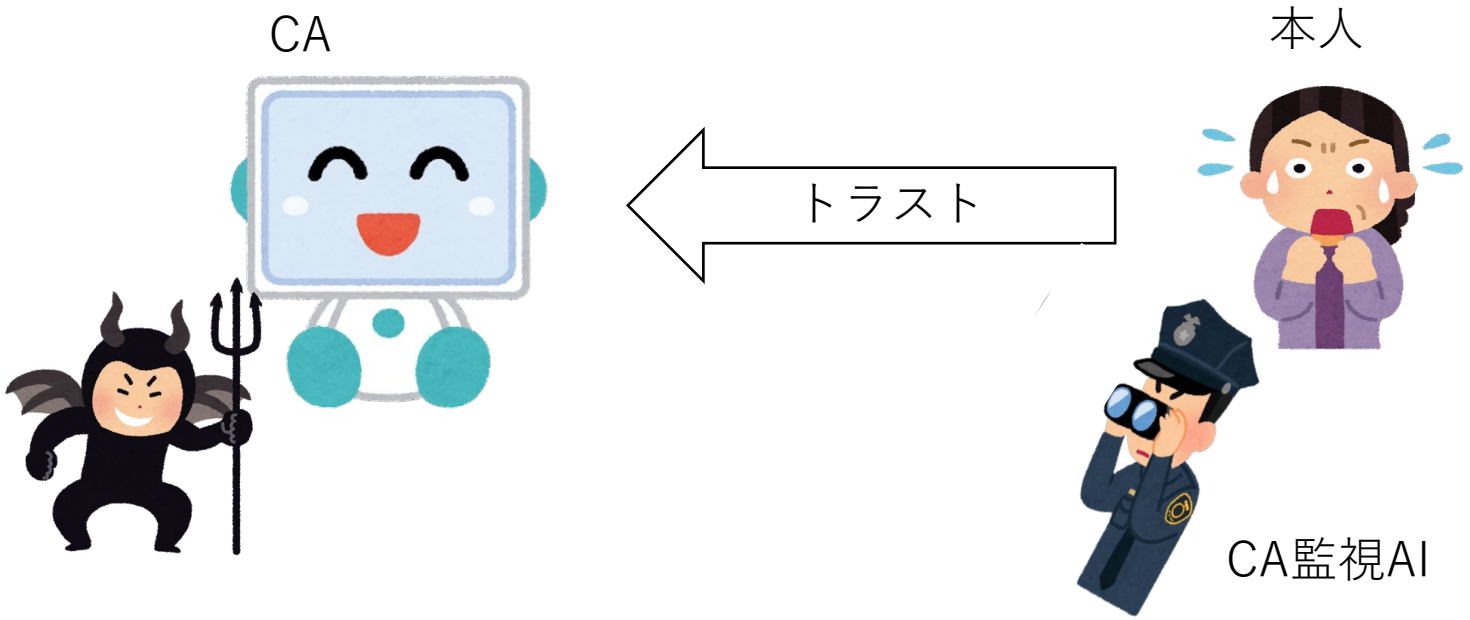


- CAがPF（Meta)の個別ユーザインタフェースの場合.
  - 悪意のある人が本人になりすましてCAを操る場合
    - 通常の正しい本人と違う行動をしているかどうかをPFが監視する（AI技術の応用）
    - 複数のCAが相互監視（CAの村社会）
  - 正しい利用者でも，いつもと違う行動をするかもしれないし，考え方を変えることもありえる.
- ログインするときには正しい利用者しか知らない鍵を用いる2段階認証が効果的だが．．．



- CAの開発，販売会社との利用契約
- CAがPFの個別ユーザーインタフェースである場合は利用契約がさらに重要

- CAがマルウェアに乗っ取られる問題
  - 本人が気が付けるか？
  - 本人の意思と離れた行動をしてしまうかもしれない
  - ◆ 自己イメージがコントロールできない状態



- CAが本人になりすまして、本人の思惑と違う行動をした場合
  - このような行動を本人が遅滞なく認識できるか？
    - **CAを監視するAI**が必要かもしれない．技術課題は何か？
  - 動作停止させることはできるが，既に行った行動（例えば，第3者との契約）を廃棄できるかという法的問題を解決しておく必要がある．
  - CAの行為に対するの免責事項を予め決めておくこと→法的問題点は石井先生が指摘している

最後に

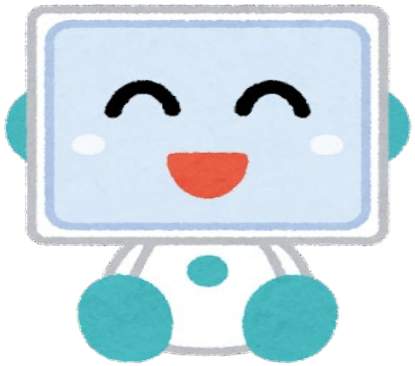
- CAは本人の死後も生き続けることができる。
- Facebookは死者のレガシーアカウントを作り、死後も死者から儲けるビジネスモデルを考えている

- Meta社が提供するメタバースになったとき、死後に残されたCAは本人のディジタル遺骸として生き続けることが現実化。
  - ディジタル遺骸のビジネス化と法的問題
    - 著作権か？人権か？プライバシー権か？
  - Digital Immortality の研究
    - Maggi Savin-Baden and David Burden: Digital Immortality and
    - Virtual Humans. Postdigital Science and Education (2019) 1:87–103
    - https://doi.org/10.1007/s42438-018-0007-6

事業者

トラスト

CA



- サービス利用契約：法的かつ形式的なトラスト
  - 個人データの利用法：目的の定義（広すぎるとトラストしにくい），第3者移転の有無
  - これらをチェックできる能力がPAI Agentに欲しいが．．．

- 認証
  - 組織としてのディジタル認証がインターネット経由で行える
  - 認証機関（政府，etc）