ゼロトラストにおけるID管理の役割 －トラストアンカーの一つとして－

株式会社アイピーキューブ
貞弘　崇行

自己紹介

貞弘　崇行（さだひろ　たかゆき）

株式会社アイピーキューブ　IAMコンサルティング部　IDコンサルタント

SIerとして主にB2E向けのMicrosoft系プラットフォーム及びアプリケーションのアカウント管理システム、オンプレミス及びクラウドへのIDフェデレーションシステム、IDaaS導入の企画、要件定義、設計、導入を担当。

最近では、B2BやB2C向けのアカウント管理、認証基盤導入の企画、要件定義等も担当。
eKYCにも関連する要求/要件も見るようになってきました。

【主な所属団体】
・日本ネットワークセキュリティ協会（JNSA）
標準化部会　デジタルアイデンティティWG

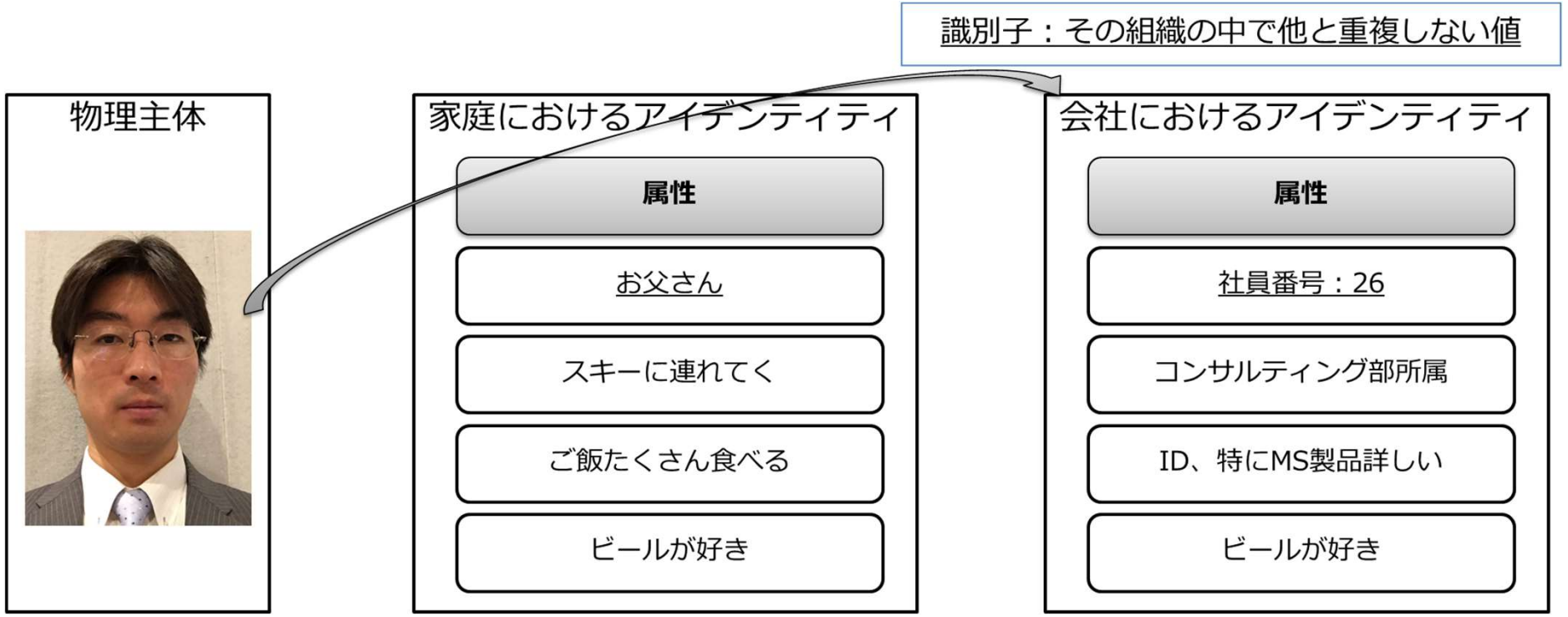
【主な活動】
・エンタープライズロール管理解説書（第3版）　主要執筆者

本資料の目的

- Identity及びID管理について概念を確認すること
- Identityに関連したトラストを構成する要素を、物理世界、デジタル世界での実例を元に洗い出すこと
- トラストを構成する要素とID管理の関係性を整理すること
- 上記を踏まえ、ゼロトラストの考え方とID管理の関係性を整理すること
- 組織をまたぐ場合、Identityはどのような保持の仕方になっていく可能性があるか、提示すること

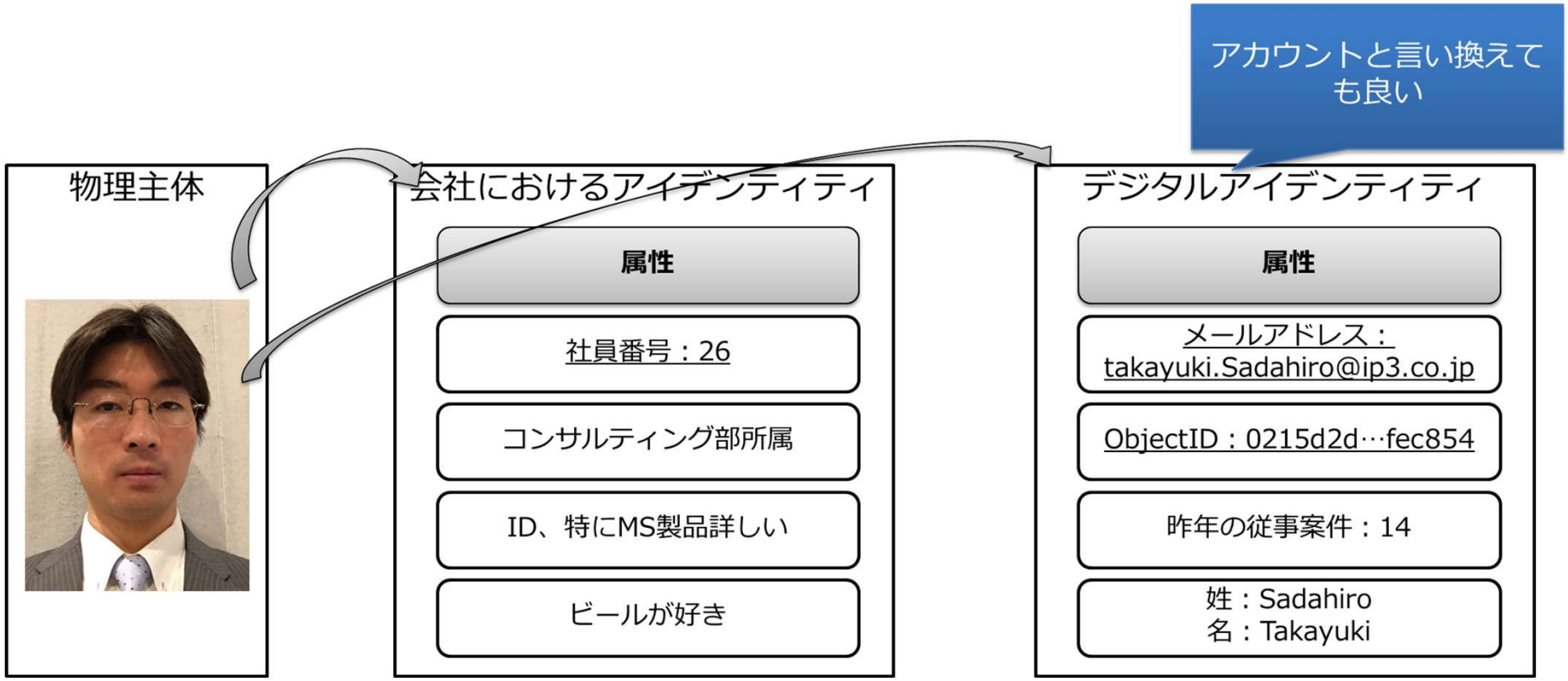
Identityとは

- 主体（人、モノなど）を特定コンテキストへ投射時の属性の集合
  - 本講演では、主体としては自然人を想定する



Identityとは

- 物理、デジタル、どちらのコンテキストでも成り立つ



ID管理（Identity Management）とは

- 前述のIdentityのライフサイクル及び属性管理のプロセスとポリシー
  - 本講演では、クレデンシャル管理もID管理の一部として議論する

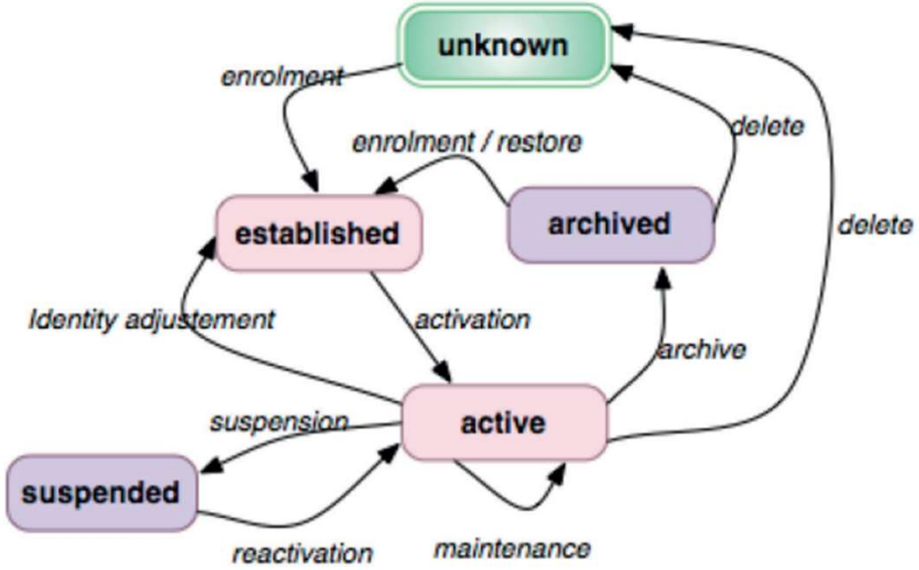


Figure 1 — Identity lifecycle

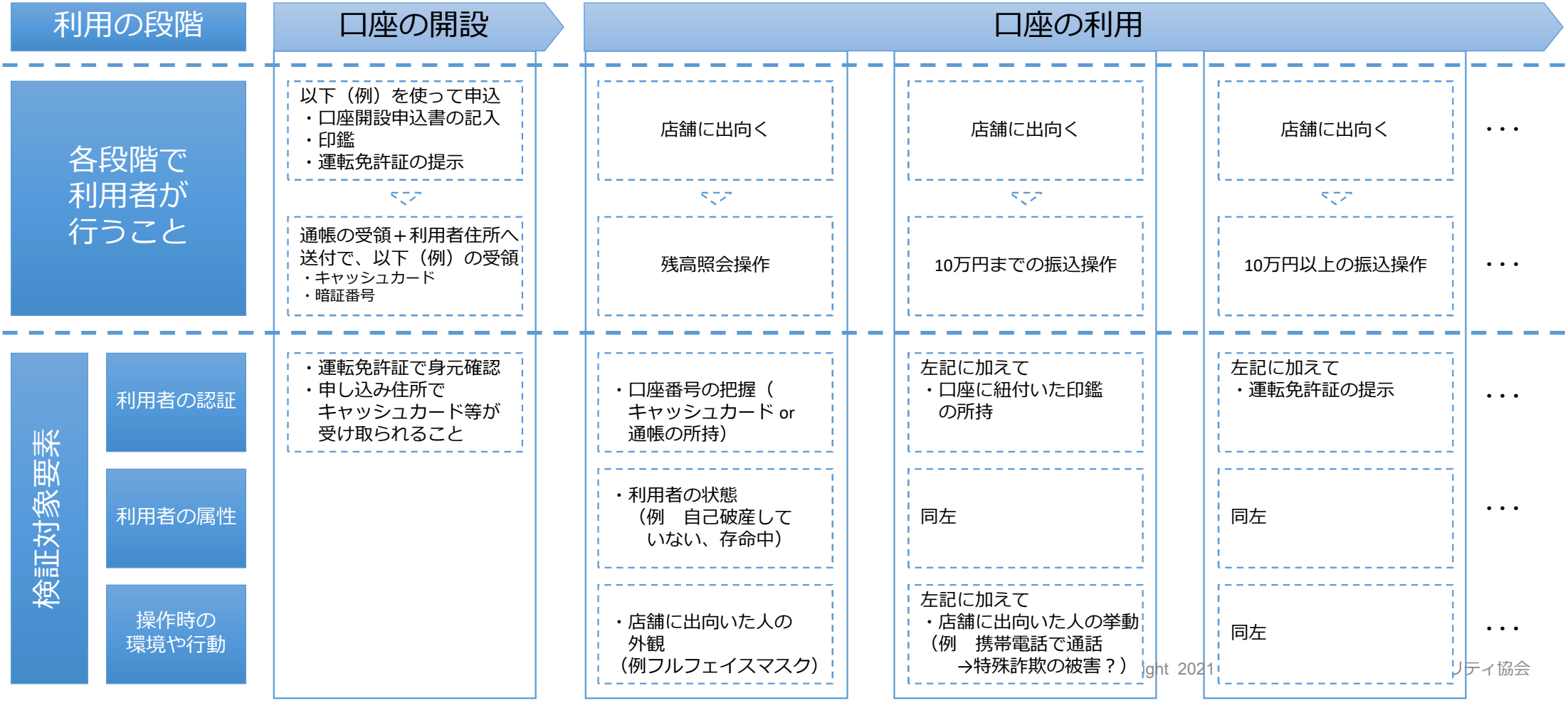
出典：ISO 24760-1 IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts

トラストを構成する要素

以下の例からIdentityに関してトラストを構成する要素（＝検証対象となる要素）をある程度単純化して考えてみる

- 銀行口座というリソース
- 銀行口座利用者というIdentityによるアクセス

物理世界での検証対象要素
：銀行店舗で個人口座開設～振込操作



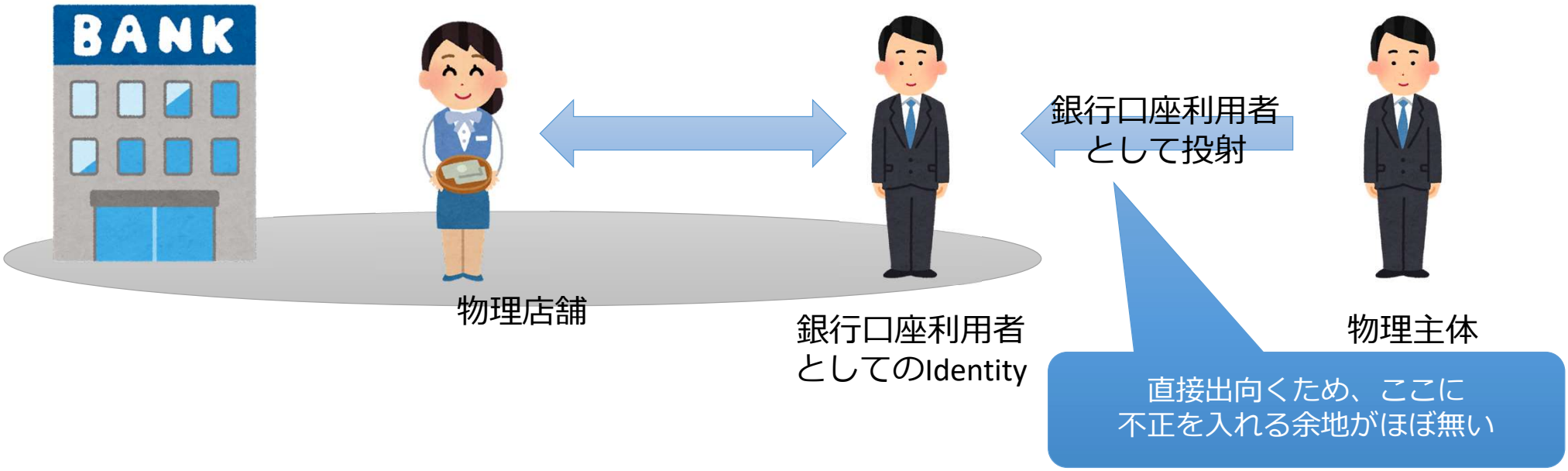
デジタル世界での検証対象要素
：インターネットバンキングで個人口座開設～振込操作

*：パスワードとは別の認証要素として利用

JNSA

利用の段階		口座の開設	口座の利用			
各段階で利用者が行うこと		以下（例）を使って申込 ・運転免許証の撮影 ・顔写真の撮影 ・ライブネスの確認	オンラインバンキングサービスにアクセス	オンラインバンキングサービスにアクセス	オンラインバンキングサービスにアクセス	・・・
		利用者住所への送付で、以下（例）の受領 ・キャッシュカード ・暗証番号、パスワード、乱数表*	残高照会操作	10万円までの振込操作	10万円以上の振込操作	・・・
検証対象要素	利用者の認証	・運転免許証で身元確認 ・申し込み住所でキャッシュカード等が受け取られること	・パスワードの把握	左記に加えて ・乱数表に記載された値の把握	同左	・・・
	利用者の属性		・利用者の状態 （例　自己破産していない、存命中）	同左	同左	・・・
	操作時の環境や行動		・アクセス時の情報（例 グローバルIPアドレス） ・認証完了からの経過時間	左記に加えて ・店舗に出向いた人の挙動 （例　携帯電話で通話 →特殊詐欺の被害？）	同左	・・・

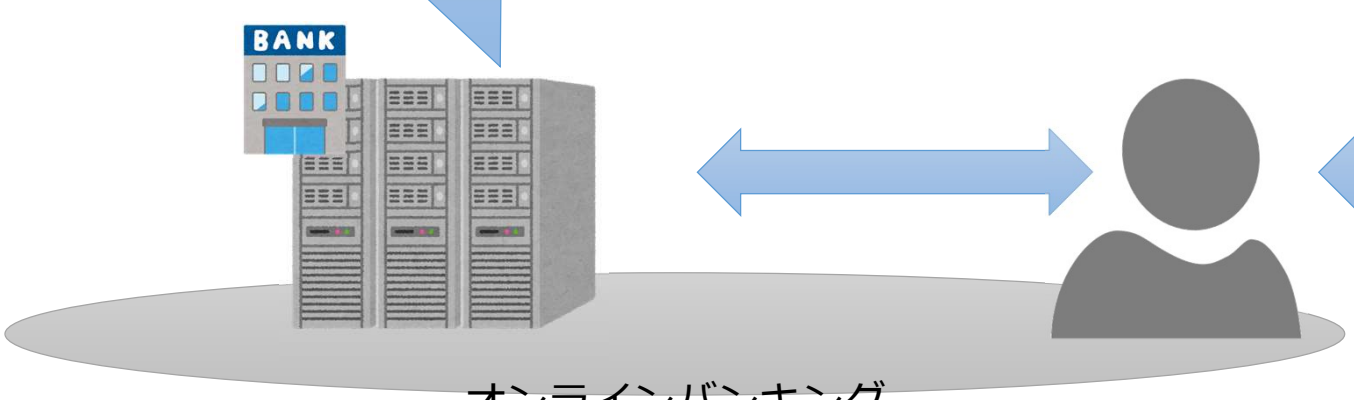
物理世界での検証対象要素
：銀行店舗で個人口座開設～振込操作



デジタル世界での検証対象要素
：インターネットバンキングで個人口座開設～振込操作

オンラインバンキングサービスが、
トラストできるプラットフォームで
稼働していることが前提

投射時に利用する
PCやスマートフォンが
トラストできることが前提



銀行口座利用者
として投射

オンラインバンキング

銀行口座利用者
としてのIdentity

直接出向くわけではないため、
主体が適切に投射されていることが
重要。それ故に一丁目一番地
＝Identityの適切な認証とアクセス制御
に使うライフサイクル/属性管理が必要

コレを避けたい

"On the Internet, nobody knows you're a dog."

引用：On the Internet, nobody knows you're a dog
https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog

利用段階とライフサイクル管理の対照

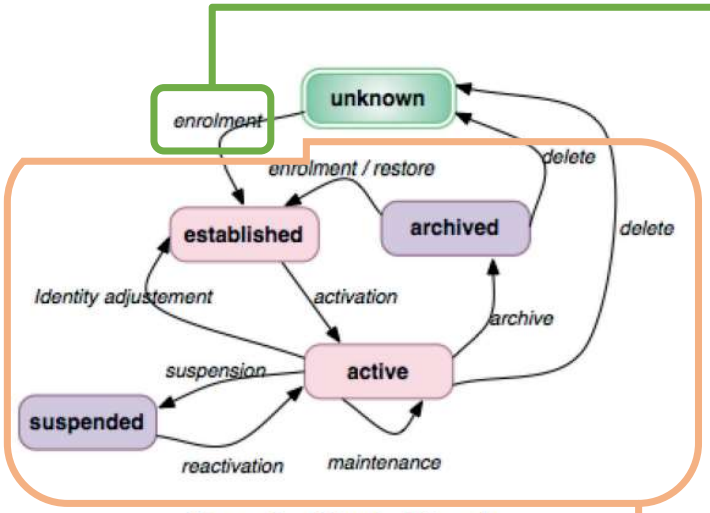
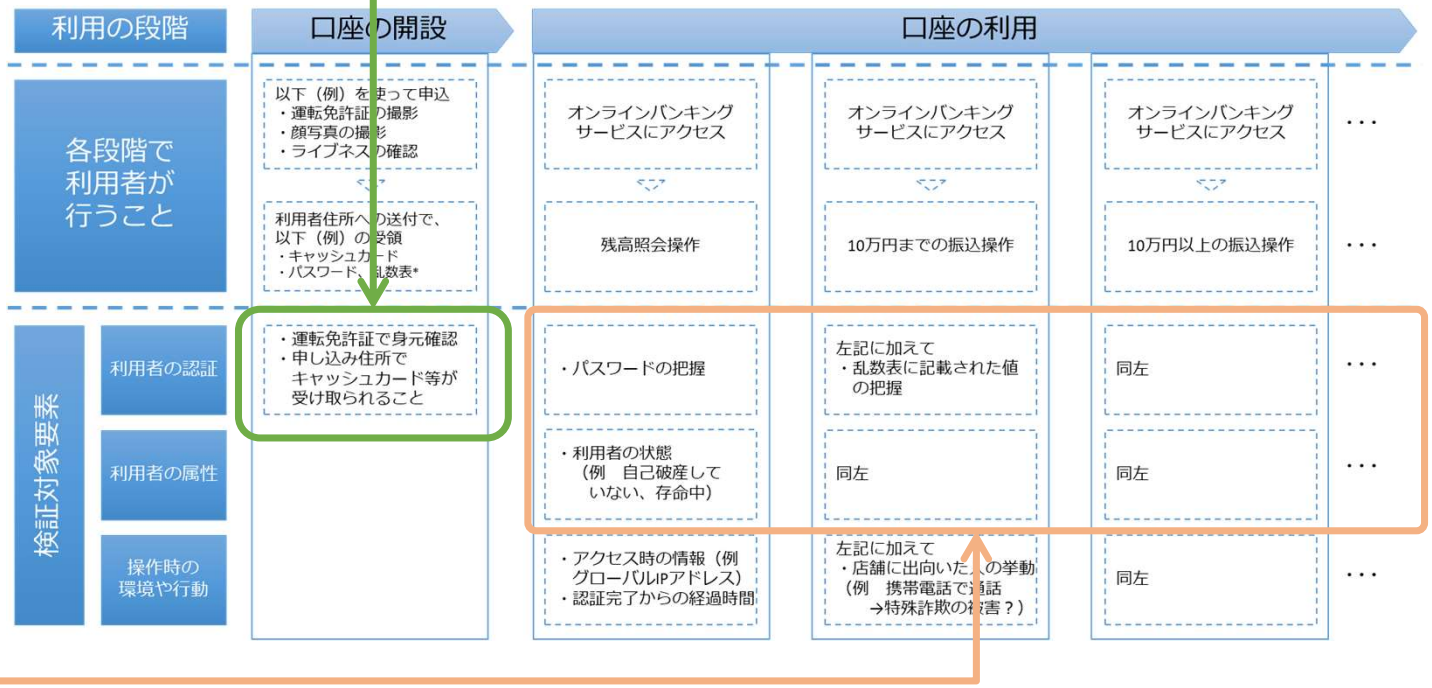


Figure 1 — Identity lifecycle



利用段階とライフサイクル管理の対照

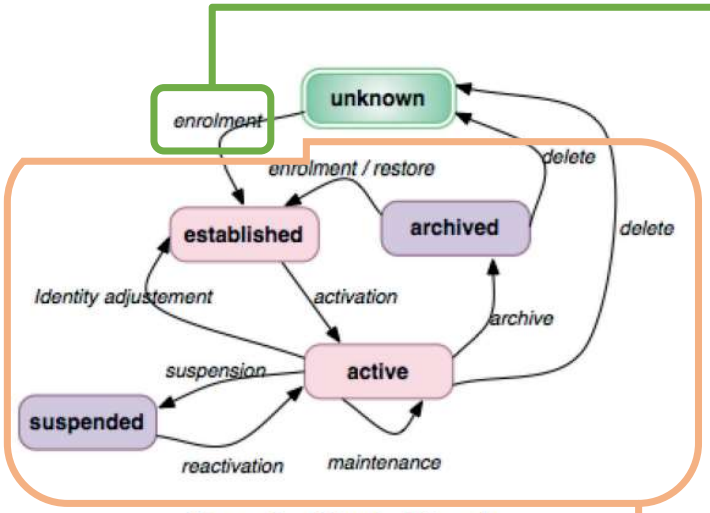
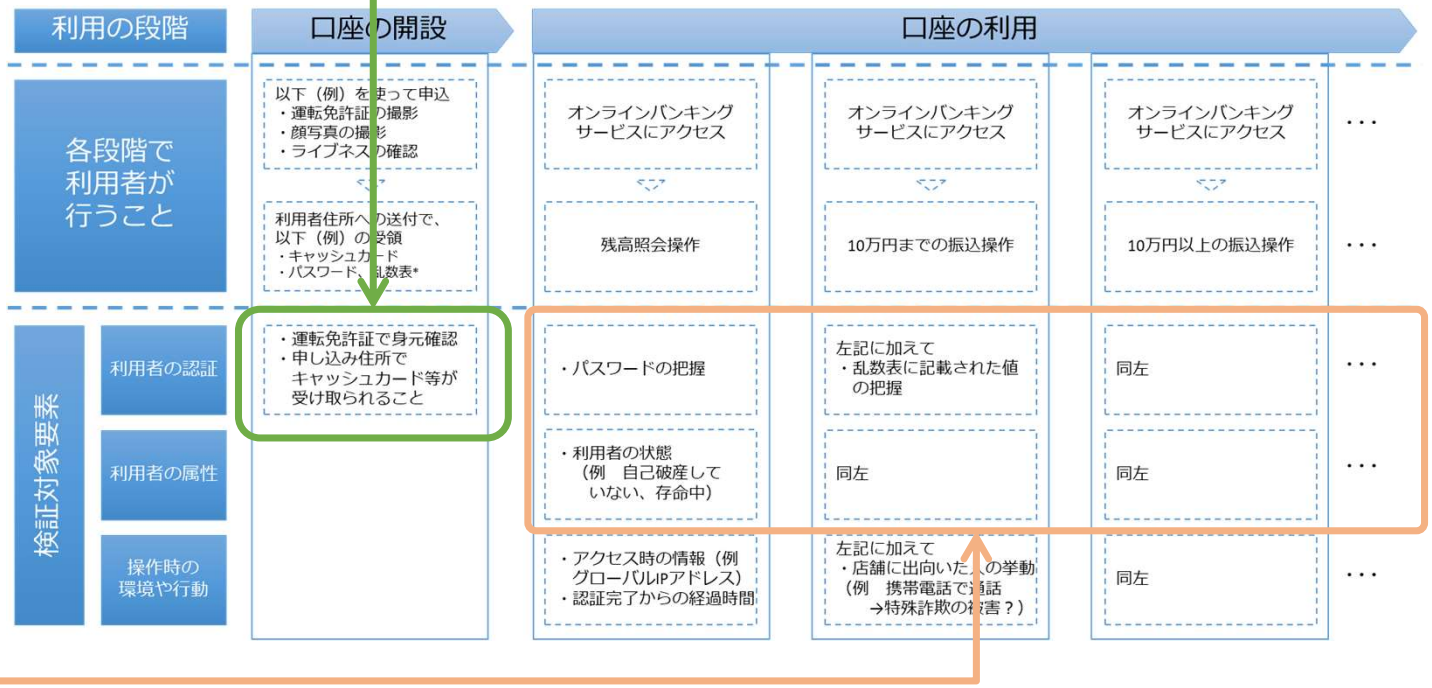


Figure 1 — Identity lifecycle



ID管理をキチンと行うことで、検証対象となる要素を
適切な状態に保つことが出来る

（参考）デジタル世界でのトラストの実現/強化

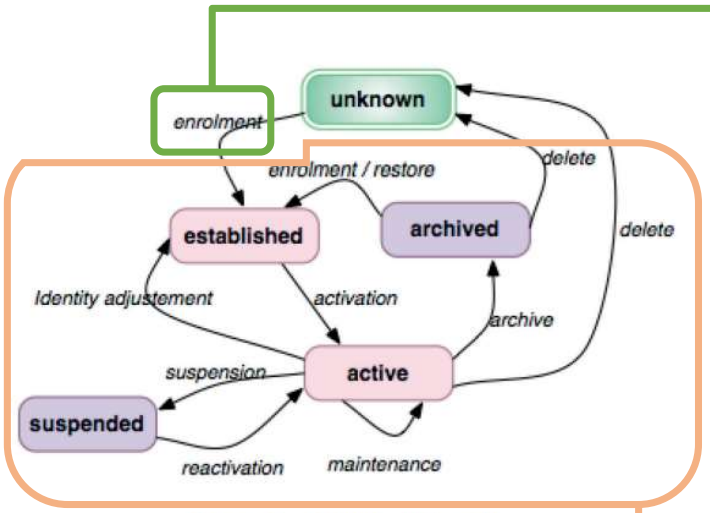


Figure 1 — Identity lifecycle

銀行口座のように
身元確認を厳密に行う
場合だとeKYC利用

認証に利用された認証器の認証方式や
生体認証精度、耐タンパー性を確認できる
FIDOデバイスの利用

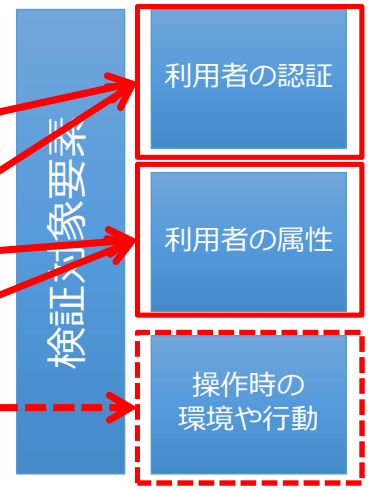
利用の段階		口座の開設	口座の利用			
各段階で利用者が行うこと		以下（例）を使って申込 ・運転免許証の撮影 ・顔写真の撮影 ・ライブネスの確認 ↓ 利用者住所への送付で、以下（例）の受領 ・キャッシュカード ・パスワード、乱数表*	オン… サー…			
検証対象要素	利用者の認証	・運転免許証で身元確認 ・申し込み住所で キャッシュカード等が 受け取られること	・パスワードの把握	左記に加えて ・乱数表に記載された値の把握	同左	…
	利用者の属性		・利用者の状態 （例　自己破産していない、存命中）	同左	同左	…
	操作時の環境や行動		・アクセス時の情報（例　グローバルIPアドレス） ・認証完了からの経過時間	左記に加えて ・店舗に出向いた人の挙動 （例　携帯電話で通話 →特殊詐欺の被害？）	同左	…

ゼロトラストにおけるID管理の位置付け

ゼロトラストの考え方とIdentityに関してトラストを構成する要素

図表2:NISTによるゼロトラストの考え方

1. すべてのデータソースとコンピューティングサービスは**リソースと見なす**
2. **ネットワークの場所に関係なく**、全ての通信を保護する
3. 企業リソースへのアクセスは、**セッション単位で付与する**
4. リソースへのアクセスは、クライアントID、アプリケーション、要求する資産の状態、その他の行動属性や環境属性を含めた**動的ポリシーによって決定する**
5. 企業は、全ての資産の整合性とセキュリティ動作を**監視し、測定する**
6. 全てのリソースの認証と認可は動的に行われ、**アクセスが許可される前に厳格に実施する**
7. 企業は、資産やネットワークインフラストラクチャ、通信の現状について可能な限り多くの情報を収集し、それを**セキュリティ対策の改善に利用する**



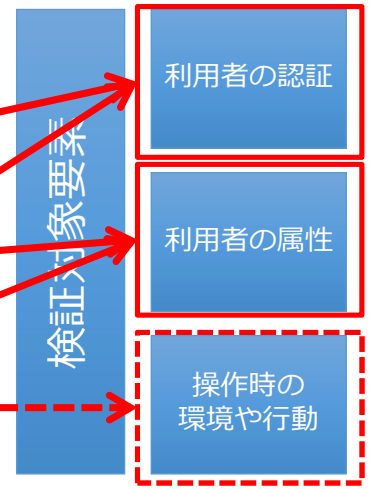
引用：NIST SP800-207 「ゼロトラスト・アーキテクチャ」の解説と日本語訳
https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/zero-trust-architecture-jp.html

ゼロトラストにおけるID管理の位置付け

ゼロトラストの考え方とIdentityに関してトラストを構成する要素

図表2：NISTによるゼロトラストの考え方

1. すべてのデータソースとコンピューティングサービスは**リソースと見なす**
2. **ネットワークの場所に関係なく**、全ての通信を保護する
3. 企業リソースへのアクセスは、**セッション単位で付与する**
4. リソースへのアクセスは、クライアントID、アプリケーション、要求する資産の状態、その他の行動属性や環境属性を含めた**動的ポリシーによって決定する**
5. 企業は、全ての資産の整合性とセキュリティ動作を**監視し、測定する**
6. 全てのリソースの認証と認可は動的に行われ、**アクセスが許可される前に厳格に実施する**
7. 企業は、資産やネットワークインフラストラクチャ、通信の現状について可能な限り多くの情報を収集し、それを**セキュリティ対策の改善に利用する**

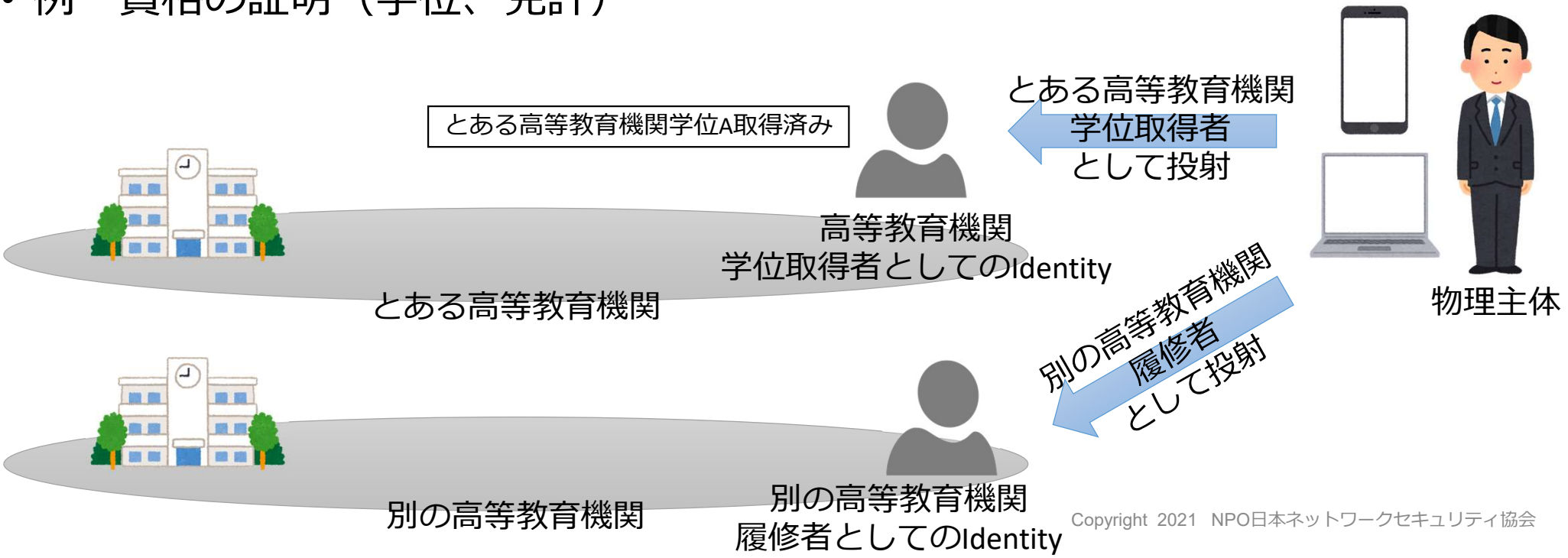


ゼロトラストの考え方は、利用者の認証や利用者の属性を使った認可が
適切に行えること＝ID管理が適切に行われていることを前提としている

引用：NIST SP800-207 「ゼロトラスト・アーキテクチャ」の解説と日本語訳
https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/zero-trust-architecture-jp.html

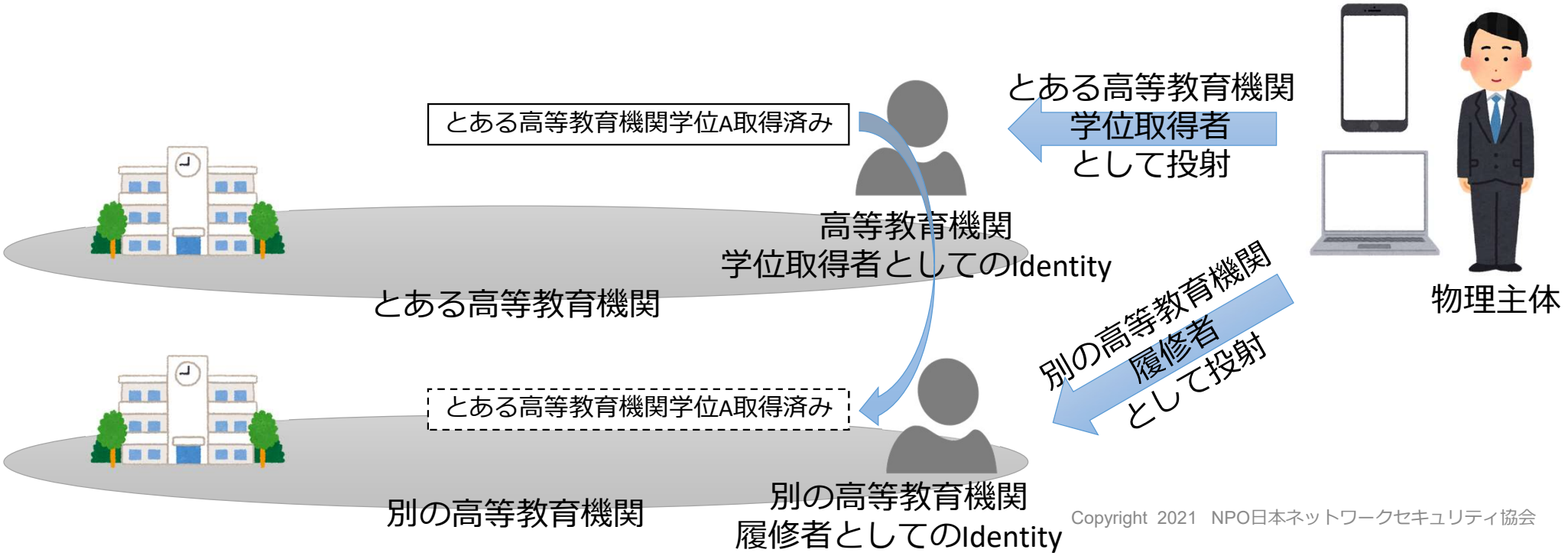
組織をまたいだIdentityの利用の拡大

- デジタル世界の拡大とともに、ある組織におけるIdentityを別の組織に対して使うケースが今後増えていくと考えられる。
  - 特にB2C、B2Bの領域で増えていくと考えられる。
  - 例　資格の証明（学位、免許）



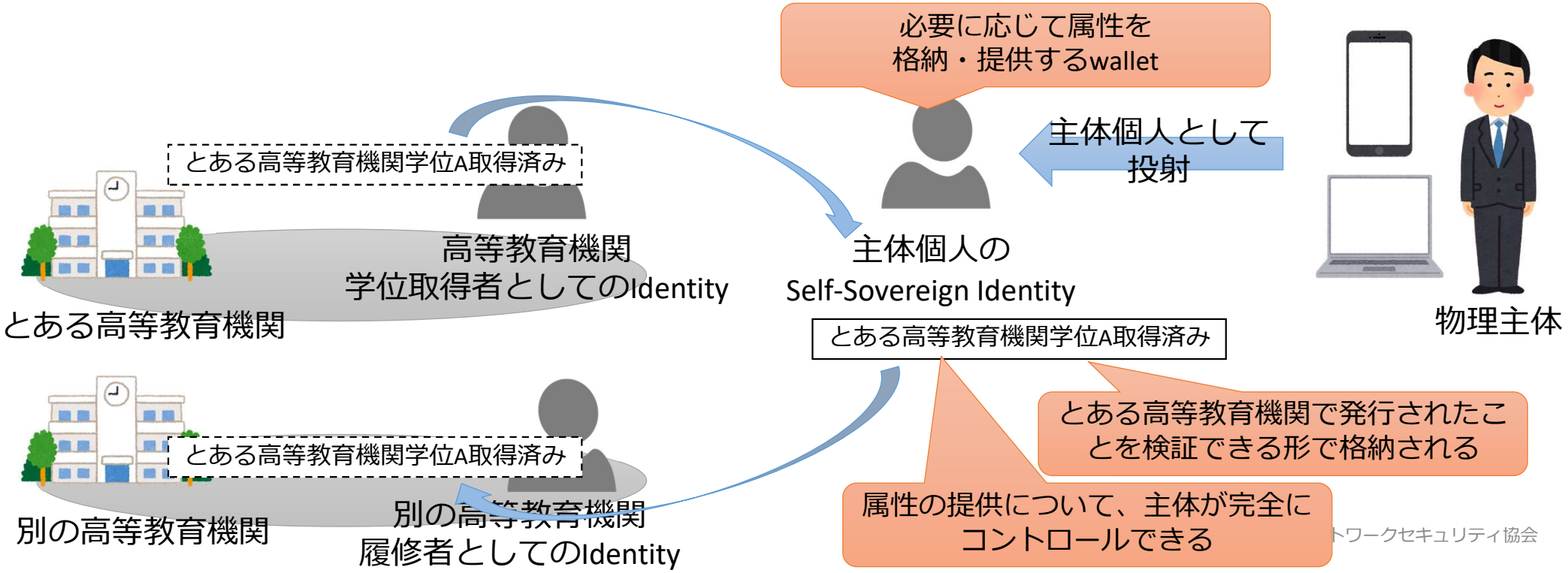
組織をまたいだIdentityの利用の拡大

- 一方での属性を他方でも使うケースがあり得る。
  1. それぞれの教育機関で属性を保持し、必要な場合は他方に提供する
  2. 属性は主体側で保持し、必要に応じて必要な方に提供する



組織をまたいだIdentityの利用の拡大

- 一方での属性を他方でも使うケースがあり得る。
  1. それぞれの教育機関で属性を保持し、必要な場合は他方に提供する
  2. 属性は主体側で保持し、必要に応じて必要な方に提供する



まとめ

- Identityに関連してトラストを確立するために検証すべき要素は、以下
  - 利用者の認証
  - 利用者の属性
  - 操作時の環境や行動
- ID管理をきちんと行うことで、これらの要素を適切な状態に保つことが出来る
- ゼロトラストの考え方は、ID管理が適切に行われていることを前提としている
- 組織をまたいだIdentity利用が拡大するにつれて、Self-Sovereign Identityの利用が増加する可能性がある