

アフターコロナの トラスト形成

崎村夏彦

サイバー大陸への強制移住



不足していた準備

- 自宅に固定回線インターネットがなくてパケ死
- VPN飽和
- F/Wがビデオ電話のトラフィックに耐えられない
- セキュリティ上の理由でオフィスからしか仕事ができない
- Zoom Bombing
- 給付金問題
- etc.



サイバー空間で 互いの識別ができない問題

同じ物理的空間を共有すること
に基づく「信頼」の形成が使えな
くなった。

Physical



The background is a dark blue gradient with a complex network of glowing white and light blue nodes connected by thin lines, resembling a digital or neural network. Two wireframe spheres, one on the left and one on the right, are also composed of these nodes. A semi-transparent image of a smartphone is visible in the upper right quadrant. A horizontal dark blue band across the center contains the title text.

Digital Identity

The background is a dark blue gradient with a complex network of glowing white and light blue nodes connected by thin lines, resembling a digital or neural network. Two wireframe spheres, one on the left and one on the right, are also composed of these nodes. A semi-transparent image of a smartphone is positioned diagonally across the center, with its screen area appearing as a bright light source. A horizontal semi-transparent bar is located behind the text.

OpenID

The background is a dark blue gradient with a complex network of glowing white and light blue nodes connected by thin lines, resembling a digital or neural network. Two spherical clusters of these nodes are visible on the left and right sides. A semi-transparent image of a smartphone is positioned diagonally across the center, with its screen area appearing as a bright light source.

OpenID

Identity

The background of the slide features a hand holding a smartphone, which is slightly out of focus. Overlaid on this is a complex digital network of glowing blue and white nodes connected by thin lines, creating a sense of connectivity and data flow. Two wireframe spheres, one on the left and one on the right, also feature this network pattern. A semi-transparent dark blue horizontal band serves as a backdrop for the main text.

Identity = 属性の集合

識別子

Identifier



Prepare your I.D.

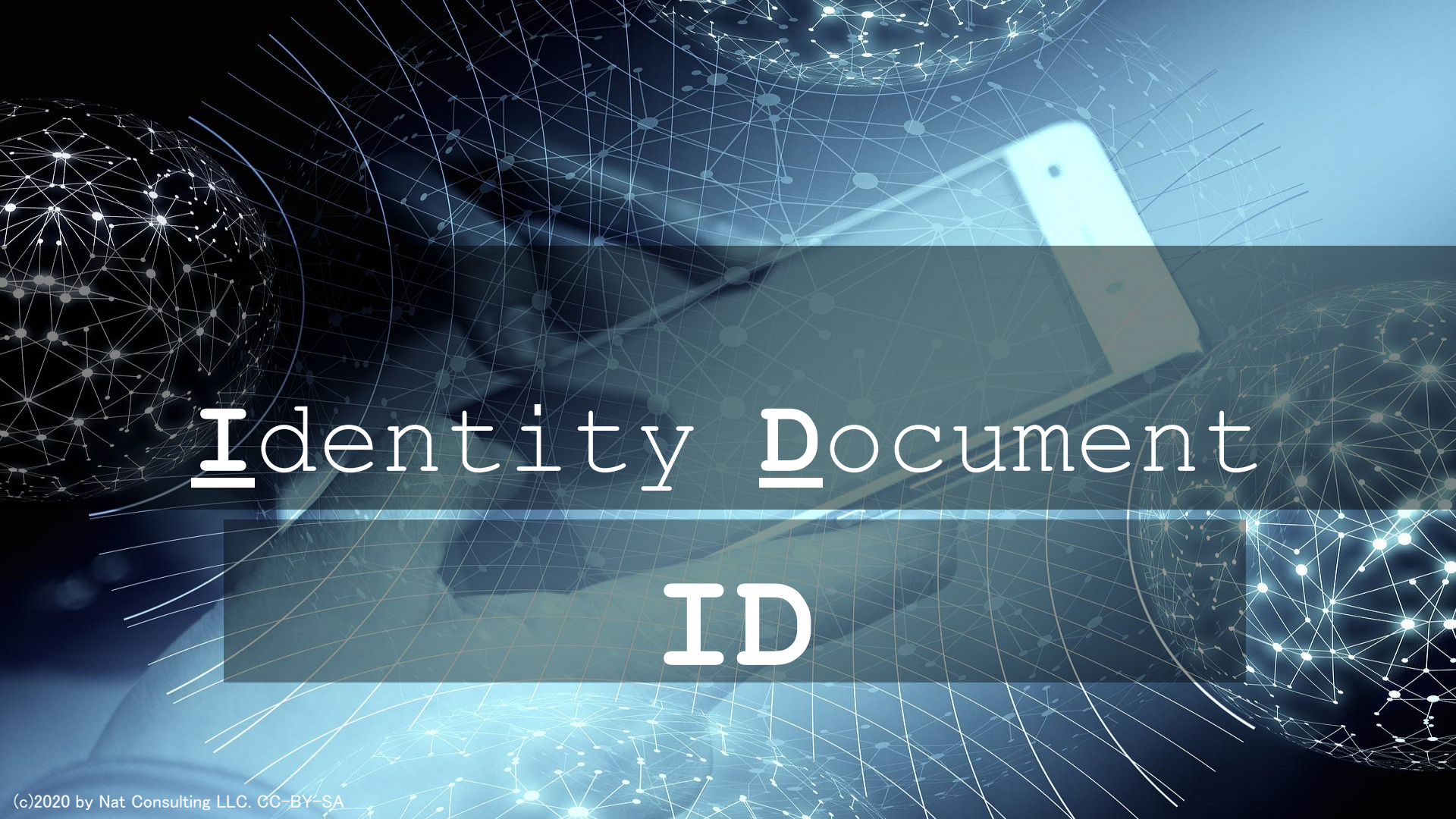
Identity Document

機械読み取り式旅券の例



出所:外務省

機械読取り式



Identity Document ID

機械読み取り式旅券の例



出所:外務省

機械読取り式

メタデータ+データ+改ざん検知機構

メタデータ
(付随情報)

データ

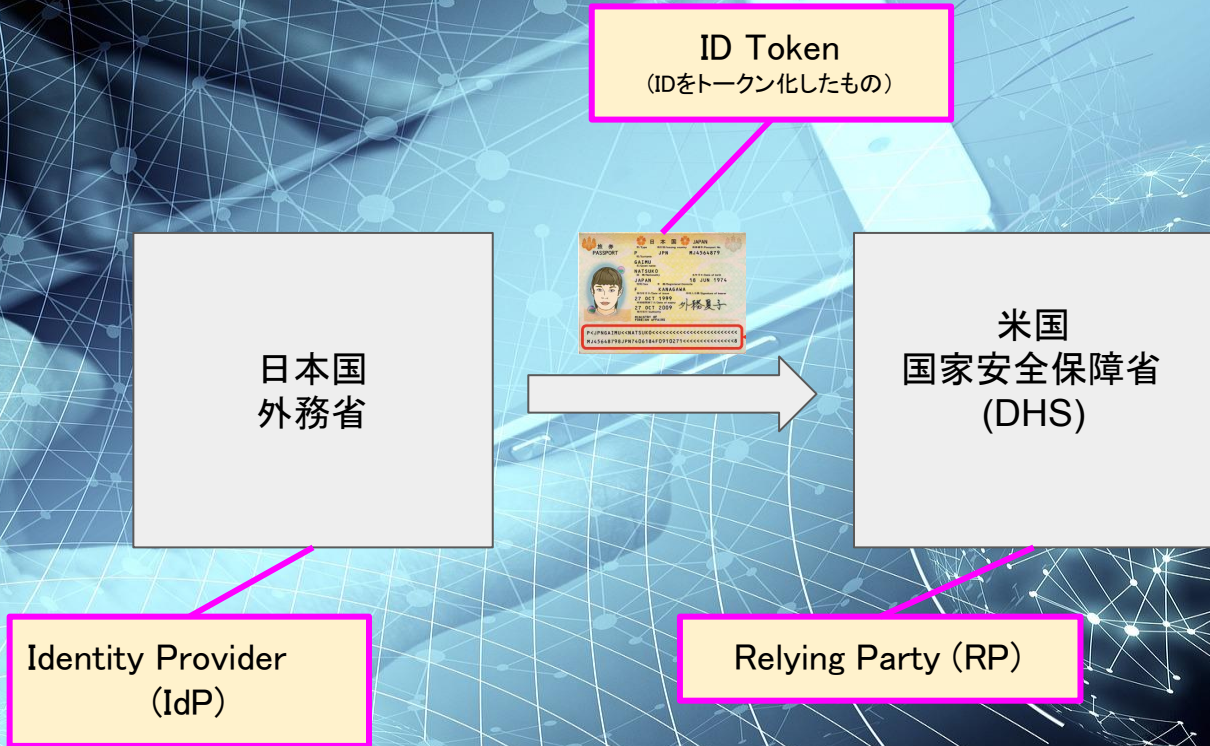
改ざん検知機構

```
{
  "verified_claims": {
    "verification": {
      "trust_framework": "de_aml",
      "time": "2012-04-23T18:25Z",
      "verification_process": "f24c6f",
      ...
    },
    "claims": {
      "given_name": "Max",
      "family_name": "Meier",
      ...
    }
  }
}
```

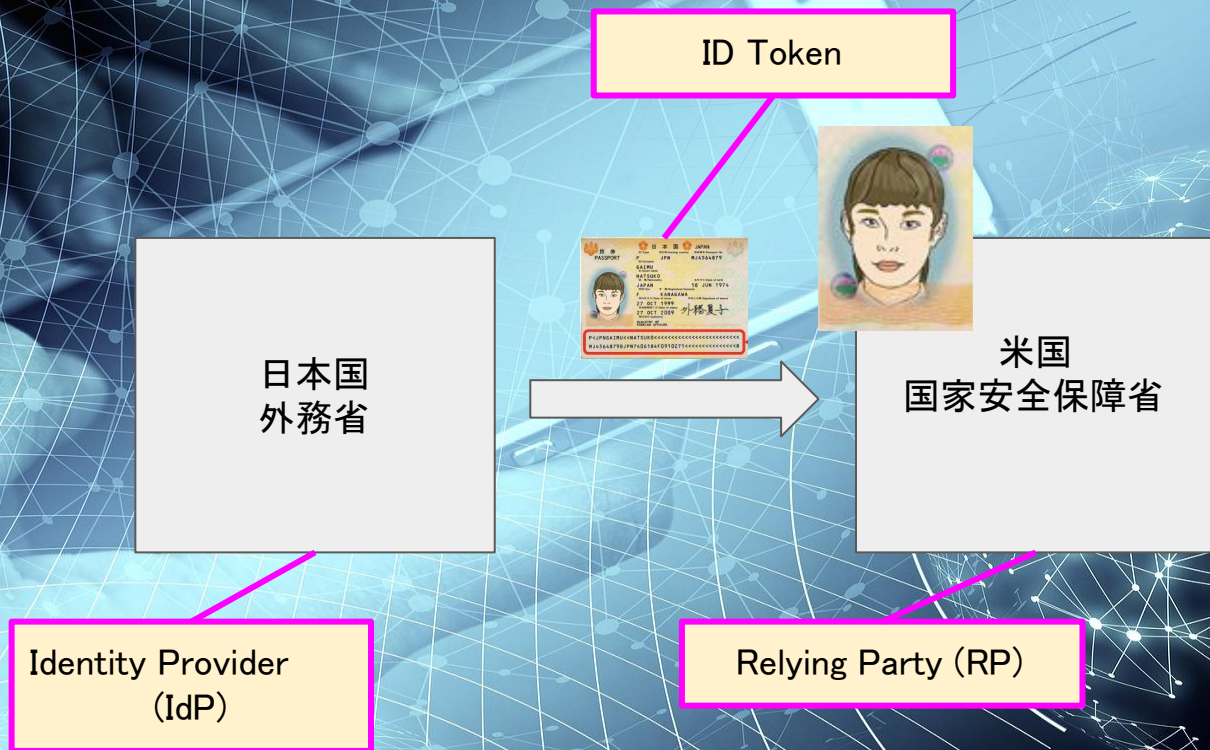
JWS (RFC7515) 署名

OIDC for Identity AssuranceのID Token
抜粋

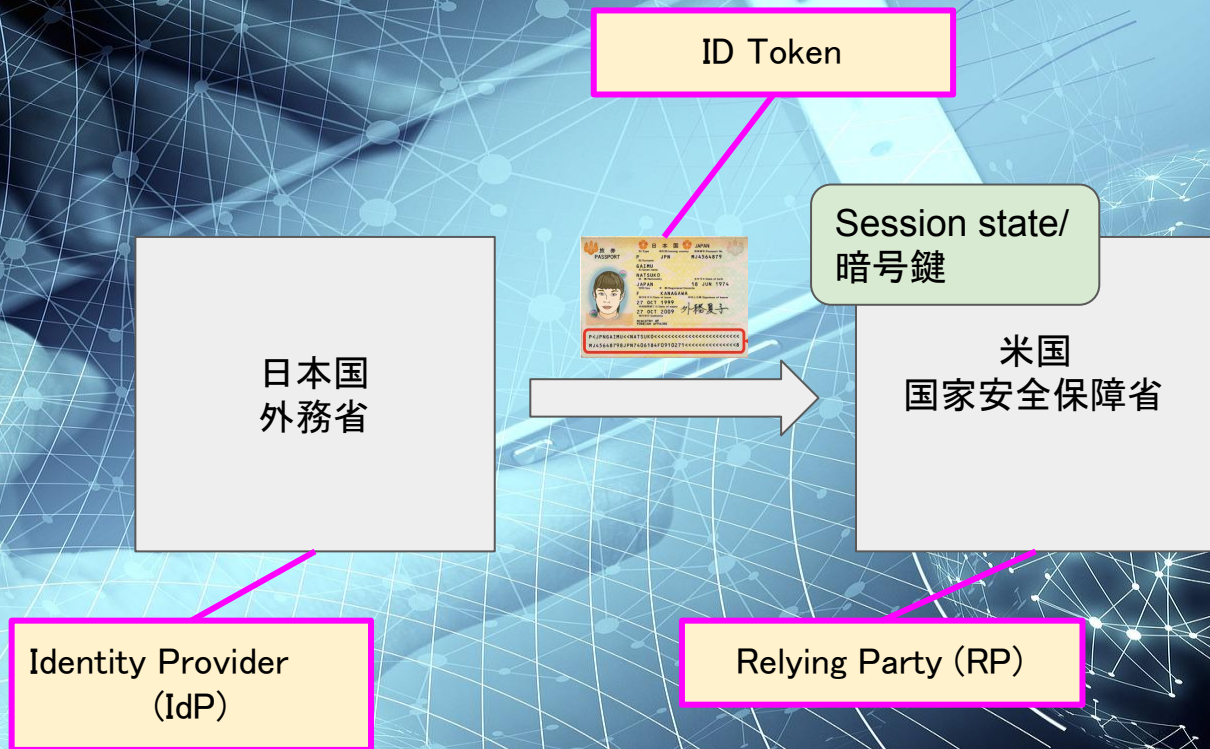
ID連携 (Identity Federation)



パスポートの場合は物理的実体がID Tokenを提示

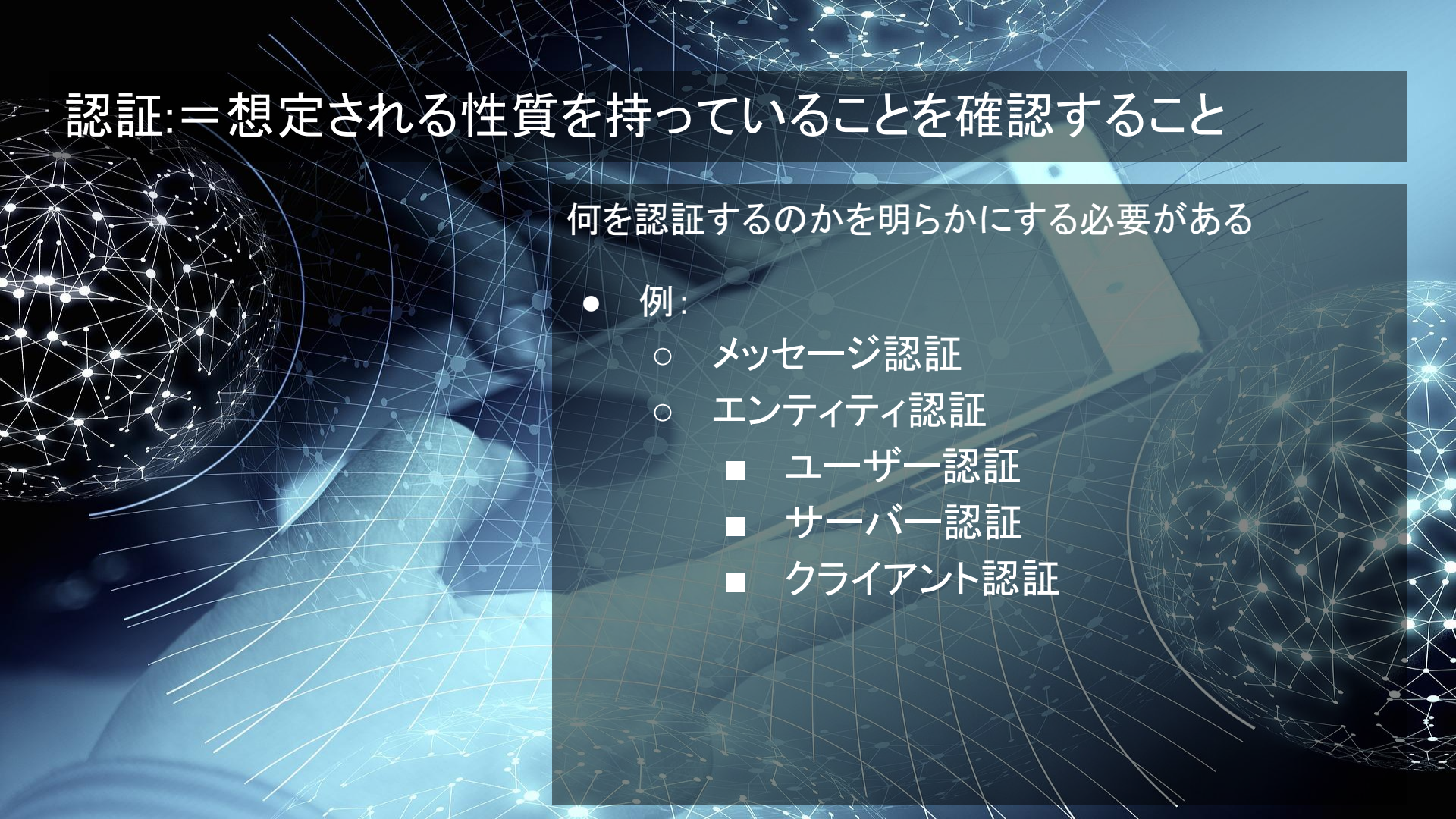


OpenIDでは、Session State や暗号鍵で代理



IDトークンの発行には「認証 (authentication)」とセッションの紐付けが必要

1. ユーザがRPに到着
2. RPはセッションを作成
3. RPはユーザをIdPにSession情報とともに転送
4. IdPはユーザの「認証」を行いIDトークンを発行
5. IdPはユーザをRPに転送
6. RPはIDトークンとセッションの結びつきを確認
7. RPはIDトークンの内容を確認



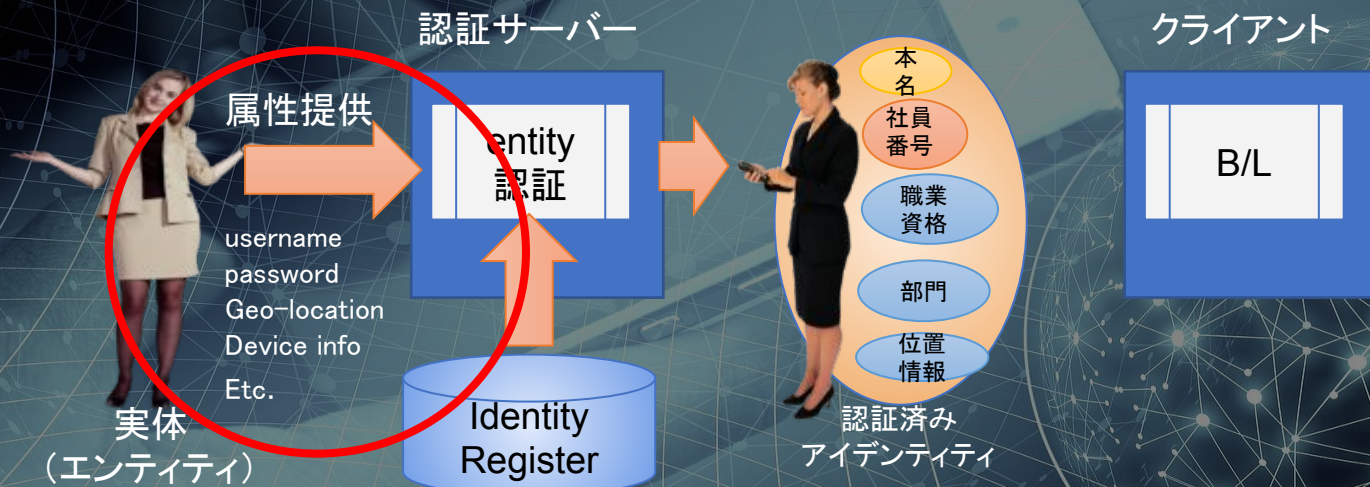
認証:＝想定される性質を持っていることを確認すること

何を認証するのかを明らかにする必要がある

- 例:
 - メッセージ認証
 - エンティティ認証
 - ユーザー認証
 - サーバー認証
 - クライアント認証

エンティティ認証

そこに来たエンティティの性質を、事前にわかっている性質と比べて検証すること



エンティティ認証
(Entity Authentication)
e.g. ID/パスワード, FIDO

ID Token

Digital Identity Guidelines

Authentication and Lifecycle Management

Paul A. Grassi

James L. Fenton

Elaine M. Newton

Ray A. Perlner

Andrew R. Regenscheid

William E. Burr

Justin P. Richer

Privacy Authors:

Naomi B. Lefkowitz

Jamie M. Danker

Usability Authors:

Yee-Yin Choong

Kristen K. Greene

Mary F. Theofanos

This publication is available free of charge from:

<https://doi.org/10.6028/NIST.SP.800-63b>

COMPUTER SECURITY

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Clip slide



NIST Special Publication 800-63B

Digital Identity Guidelines (翻訳版)

Authentication and Lifecycle Management

2017/10/27 @ LODGE

Tatsuya Katsuhara

(出所) NIST SP800-63-3翻訳版63-Bパートの紹介

<http://bit.ly/sp800-63-3b-intro>

取扱が厳しくなった秘密の質問

- SP800-63-2では“Pre-registered Knowledge Token”と呼称。
- SP800-63-3では記憶シークレットの一部に再編され「やってはいけない」記憶シークレットの例として記載されることになった。

5.1.1.2 記憶シークレットVerifier

記憶シークレットを選択する際、VerifierはSubscriberに対して**特定のタイプの情報（例えば、「あなたが飼った最初のペットの名前はなんですか？」といったもの）の入力を求めないものとする(SHALL NOT).**

- サービス事業者の立場では「厳しい」かもしれない。
 - 秘密の質問に頼らない、より安全なパスワードリマインダの再設計

パスワードの定期変更は条件付”SHOULD NOT”

強制されるとユーザは結果として「弱いパスワード」を使うようになってしまう研究結果（CMU教授兼FTC主任技術者が言及）

例)

password Passw0rd P@ssw0rd P@ssw0rd! P@ssw0rd!1 P@ssw0rd!2

└──┬──┘ └──┬──┘ └──┬──┘ └──┬──┘ └──┬──┘

大文字/数字 記号 桁数 定期的変更!! 定期的変更!!

5.1.1.2 記憶シークレットVerifier

記憶シークレットを任意で(例えば、**定期的に**)変更するよう要求すべきではない(**SHOULD NOT**)。しかしながらAuthenticatorが**危殆化している証拠**がある場合は、**変更を強制するものとする**(SHALL)。

経路外認証は引き続き使えるが“RESTRICTED”

- ドラフト改訂の当初は、公衆交換電話網(PSTN)を使っている場合、SMSの経路外認証は非推奨に。
 - PasswordCon 2016 での議論で大盛り上がり
 - CMU教授兼FTCの主任技術者 Lorrie Cranor
 - <http://arstechnica.com/security/2016/08/frequent-password-changes-are-the-enemy-of-security-ftc-technologist-says/>
- 最終的には“**RESTRICTED**”という記載で許容された。
 - VoIPやEメールはNG（特定デバイスの所有証明とならない方式のため）
 - 事前登録済みの電話番号は物理デバイスと結びついていることを確認
 - スマホのPush通知インフラはセカンダリチャネルとして利用可能
 - 電話番号の変更は、新しいAuthenticatorのバインディングとみなされ、特別な要件を追加（6章）
 - 状況が変われば制約追加がありうる旨明言



AAL: Authentication Assurance Level

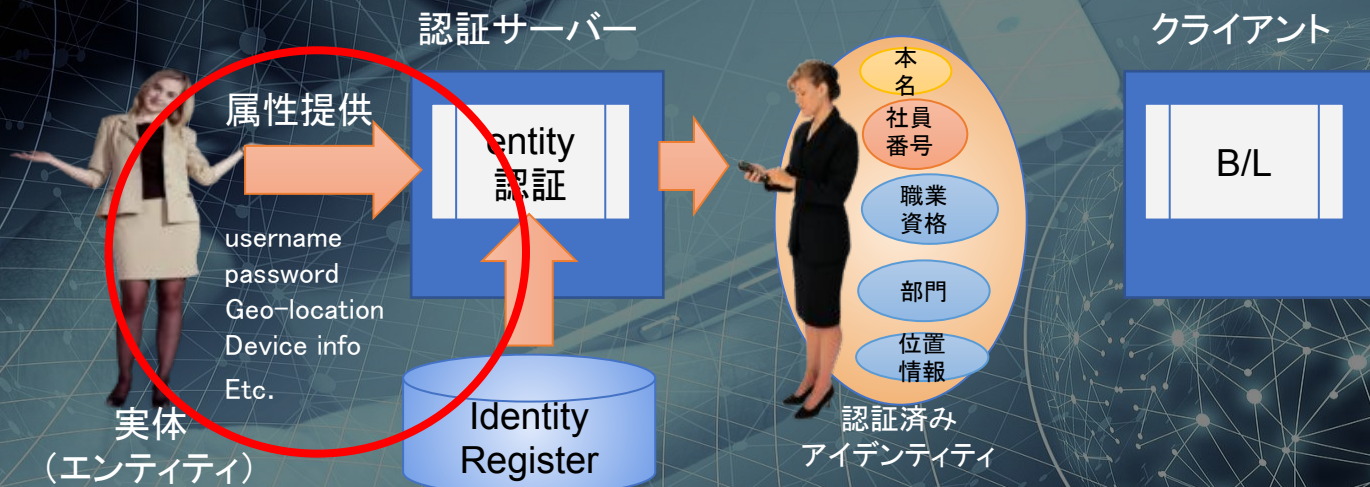
要求事項	AAL 1	AAL 2	AAL 3
許容される Authenticatorタイプ	9タイプ全部OK (何でも良い)	- Authenticator単独で2要素以上 - またはPW(知識)+2要素目(所有,生体)	2要素以上 - 暗号鍵の所持証明要素 - ハードウェア関与
FIPS 140適合	Level 1 (政府機関のVerifier)	Level 1 (政府機関のAuthenticator及びVerifier)	Level 1 総合 (Verifier及び単一要素暗号デバイス) Level 2 総合 (多要素Authenticator) Level 3 物理セキュリティ (全てのAuthenticator)
再認証	30 日	12 時間または30分間活動なしの場合に、1つの認証要素を利用して再認証(任意)	12 時間または15分間活動なしの場合に、両方の認証要素を利用して再認証(必須)
セキュリティ統制	[SP 800-53] 低い基準 (または等価なもの)	[SP 800-53] 中度の基準 (または等価なもの)	[SP 800-53] 高い基準 (または等価なもの)
中間者攻撃耐性	必須	必須	必須
Verifierなりすまし耐性(Phishing耐性)	不要 →必要 or 推奨	不要 →必要	必須
Verifier改竄耐性	不要 →必要 or 推奨	不要 →必要	必須
リプレイ耐性	不要	必須	必須
認証意図 (AuthN Intent)	不要	推奨	必須
レコード保持ポリシー	必須	必須	必須
プライバシー統制	必須	必須	必須

Take Away

- 目的ベース: 形式を追うのではなく、総合的に見て強い認証手段を使う。
 - 二段階だろうと二要素だろうと弱いものは弱い。
- 運用を考えて: 認証器を複数 Identity Proofingの前あるいは最中に登録してスタートすると楽になる。

エンティティ認証

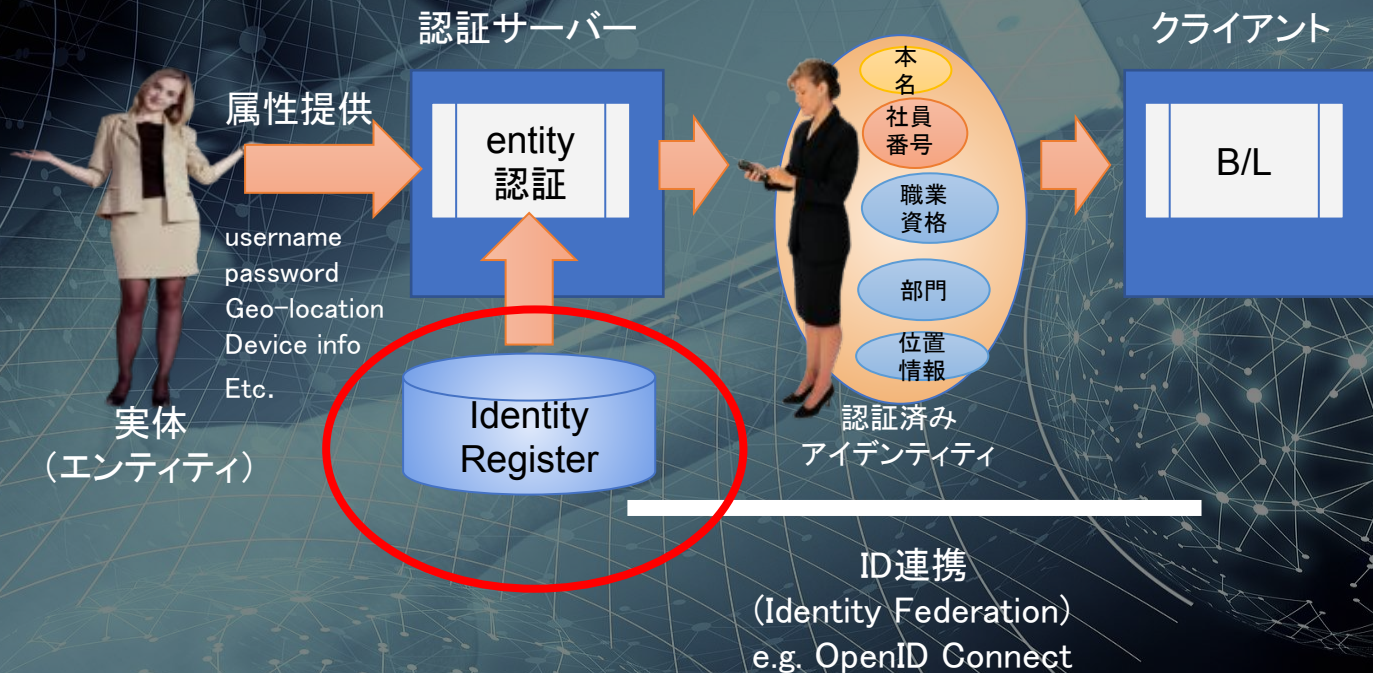
そこに来たエンティティの性質を、事前にわかっている性質と比べて検証すること



エンティティ認証
(Entity Authentication)
e.g. ID/パスワード, FIDO

ID Token

Identity Registerの重要性





そもそも
「本人確認」に対応す
る英語は無い



Identity Proofing

属性の集合の確認



NIST Special Publication 800-63A

Digital Identity Guidelines

Enrollment and Identity Proofing Requirements

Paul A. Grassi

James L. Fenton

Privacy Authors:

Naomi B. Lefkowitz

Jamie M. Danker

Usability Authors:

Yee-Yin Choong

Kristen K. Greene

Mary F. Theofanos

This publication is available free of charge from:

<https://doi.org/10.6028/NIST.SP.800-63a>

Te Tari Taiwhenua | Department of Internal Affairs

Building a safe, prosperous and respected nation



Te Tari Taiwhenua
Internal Affairs

FOR PEOPLE, COMMUNITIES
AND BUSINESSES

FOR CENTRAL AND
LOCAL GOVERNMENT

WHAT'S NEW
ON THIS SITE

FORMS TO
DOWNLOAD

PUBLICATIONS
AND REPORTS

DATA AND
STATISTICS

ABOUT US

CONTACT US

EVIDENCE OF IDENTITY
STANDARD

DOCUMENTS USED FOR
EOI

QUESTIONS AND
ANSWERS

Resource material ›

Evidence of Identity Standard

The Evidence of Identity (EOI) Standard (Version 2.0) is part of a suite of [Authentication Standards](#), developed to provide a framework for consistent authentication of online identity by agencies. However, the EOI Standard applies to both online and offline settings.

The purpose of the EOI Standard is to provide good practice guidance for government agencies about the required process for initial establishment and subsequent confirmation of an individual's identity.

The EOI Standard was first developed and released in June 2006 (Version 1.0), and has been redeveloped and released in December 2009 as Version 2.0. The new version includes some revision of original content and additional areas of guidance.

- › [Evidence of Identity Standard \(Version 2.0\)](#) - Searchable (html) version
- › [Evidence of Identity Standard \(Version 2.0\)](#) - Printable (pdf) version (2mb)*
- › [Fact Sheets - documents referenced in the EOI Standard](#) (v2.0)

(サービス利用者の)Identity Proofing とは、

1. 目的のためにどの属性が必要かを明らかにし、
2. その属性の値を確認するための証拠を集め検証し、
3. そのアイデンティティが使われ続けていること、
4. 他にそのアイデンティティを使っている人がいないこと、
5. そのアイデンティティと、その人の肉体が結びついていること

を確認すること。

Identity Proofing とは、

1. 目的のためにどの属性が必要かを明らかにし、
2. その属性の値を確認するための証拠を集め検証し、
3. そのアイデンティティが使われ続けていること、
4. 他にそのアイデンティティを使っている人がいないこと、
5. そのアイデンティティと、その人の肉体が結びついていること

を確認すること。

必要な属性の組み合わせとは、最低限、

- 1-1 それらを組み合わせることによって、当該コンテキスト内で継続的に唯一性を担保でき、
- 1-2 それらの組み合わせによって、効果的にクリアランスができるような組み合わせ。

その他にも、認証クレデンシャルの配布やリセットに必要な情報、あるいはすでに当該ユーザが持っている認証クレデンシャルを確認するための情報などにも必要に応じて。

例) 犯罪収益移転防止法

目的:

マネー・ローンダリング／テロ資金供与防止

- 収集する属性

- 本人特定事項
- 取引を行う目的
- 職業(自然人)又は
- 事業の内容(法人・人格のない社団又は財団)
- 実質的支配者(法人)
- 資産及び収入の状況
- 外国PEP該当性

例) 犯罪収益移転防止法

1-1 それらを組み合わせることによって、当該コンテキスト内で継続的に唯一性を担保でき、



- 本人特定事項
 - 自然人: 氏名、住居及び生年月日
 - 法人: 名称及び本店又は主たる事務所の所在地

1-2 それらの組み合わせによって、効果的にクリアランスができるような組み合わせ。



- 取引を行う目的
- 職業(自然人)又は事業の内容(法人・人格のない社団又は財団)
- 実質的支配者(法人)
- 資産及び収入の状況
- 外国PEP該当性

1-1 コンテキスト内の継続的唯一性

Identity proofing 要件

1. それらを組み合わせることによって、当該コンテキスト内で継続的に唯一性を担保でき、

犯収法の本人特定事項

- 自然人にあつては氏名、住居及び生年月日をいい、法人にあつては名称及び本店又は主たる事務所の所在地をいう。
 - （犯罪収益移転防止法第四条第一項第一号）

クリアランス用属性

Identity proofing 要件

1-2 それらの組み合わせによって、効果的にクリアランスができるような組み合わせ。

犯収法の要件

- 取引を行う目的
- 職業(自然人)又は事業の内容(法人・人格のない社団又は財団)
- 実質的支配者(法人)
- 資産及び収入の状況
- 外国PEP該当性

Identity Proofing とは、

1. 目的のためにどの属性が必要かを明らかにし、
2. その属性の値を確認するための証拠を集め検証し、
3. そのアイデンティティが使われ続けていること、
4. 他にそのアイデンティティを使っている人がいないこと、
5. そのアイデンティティと、その人の肉体が結びついていること

を確認すること。

属性確認のための証拠(Evidence of Identity)の収集

- 継続的唯一性のための証拠

- マイナンバーカード、運転免許証、住民票、保険証 など

- クリアランス属性確認のための証拠

- 職業

- 基本的に日本では自己申告？

- 事業の内容

- 法人の登記簿と、いくつかの契約書。

- 実質的支配者

- 大株主の大株主の大株主の大株主の...大株主を株主名簿からおいかけるなど...

- 資産及び収入の状況

- 預金残高証明書、納税証明書など？

- 外国PEP該当性

- 親族に外国籍のものがいないか？そのものはPEPではないか？

属性確認のための証拠(Evidence of Identity)の確認

- その証拠が偽造でないか
 - 券面: 特殊印刷、ホログラムの確認
 - より高いレベル(IAL3)の確認のためには、専用の教育を受けた資格を持つ人材による確認が必要。
 - ICチップ: 署名の確認
 - 両方: それらが失効していないかの確認
- それが確認できない場合には、内容の権威的源泉への確認
 - APIなどを使って、値を確認
- それらができない場合は、補足的源泉としてしか扱えないので、十分な数の独立した補足的源泉を集めて確度を上げる。
 - 公的な立場に有る、その人物をよく知る人間複数人の署名付き証言など
 - ↑ トラストアンカー

Identity Proofing とは、

1. 目的のためにどの属性が必要かを明らかにし、
2. その属性の値を確認するための証拠を集め検証し、
3. そのアイデンティティが使われ続けていること、
4. 他にそのアイデンティティを使っている人がいないこと、
5. そのアイデンティティと、その人の肉体が結びついていること

を確認すること。

3. そのアイデンティティが使われ続けていること、

- あまり使われたことがないアイデンティティは危ない。
 - 本人が使っていないことを良いことに、そのアイデンティティを盗んで(Identity Theft)または買収して(takeover) 使おうとしているかもしれない。
 - 社会的困窮者からの買収
 - 死亡確認されていない死者や行方不明者のアイデンティティの乗っ取り
 - 合成アイデンティティ(Synthetic Identity)

4. 他にそのアイデンティティを使っている人がいないこと、

- 一人の人が、複数の人として登録して
くることが有る。
 - 例：NZの年金不正受給
- 顔写真などの生体情報で検索して、重
複登録していないかを調べる。

Identity Proofing とは、

1. 目的のためにどの属性が必要かを明らかにし、
2. その属性の値を確認するための証拠を集め検証し、
3. そのアイデンティティが使われ続けていること、
4. 他にそのアイデンティティを使っている人がいないこと、
5. そのアイデンティティと、その人の肉体が結びついて
いること

を確認すること。

5. そのアイデンティティと、その人の肉体が結びついていること

- 別名「バインディング」
 - Entity – Identity Binding
 - Carbon Form – Digital Binding
- 顔写真付き証明書をもとめられるのはこのため。
 - しかし、その証明書自体が信用できるかは、それがどのように作られたのかを吟味する必要あり
 - 一番当初は、そのようなバインディングがしてある証明書は存在しないので、要ブートストラップ。

バイディングのブートストラップ

- Identity Referee が写真に裏書き。
- Identity referee は証明済みの、「公的」立場の人である必要。
 - カナダ、NZなど：パスポートを取るのには、写真に裏書きと署名が必要。
 - ドイツ：16歳のときに学校の先生が証明 etc.
 - 昔の日本：村役場の担当は、その人を子供の時から知っていたはず。だが今は？
- 実は日本はここが決定的に弱い。
- 首相からつらなるトラストチェーンを可及的速やかに作るべきなのではないか？
 - パキстанは3年で1.3億人やったんだからできる！

The background features a dark blue gradient with a network of glowing white and yellow nodes connected by thin lines, resembling a digital or molecular structure. A semi-transparent smartphone is positioned diagonally across the center. The text is overlaid on the left side of the phone.

身元確認 エンティティ認証 ID連携



ヒト・モノ・コト



IAL(身元確認レベル)

(Identity Assurance Level)

AAL(エンティティ認証レベル)

(Authentication Assurance Level)

FAL(ID連携レベル)

(Federation Assurance Level)

Cyber



Fake?



Physical





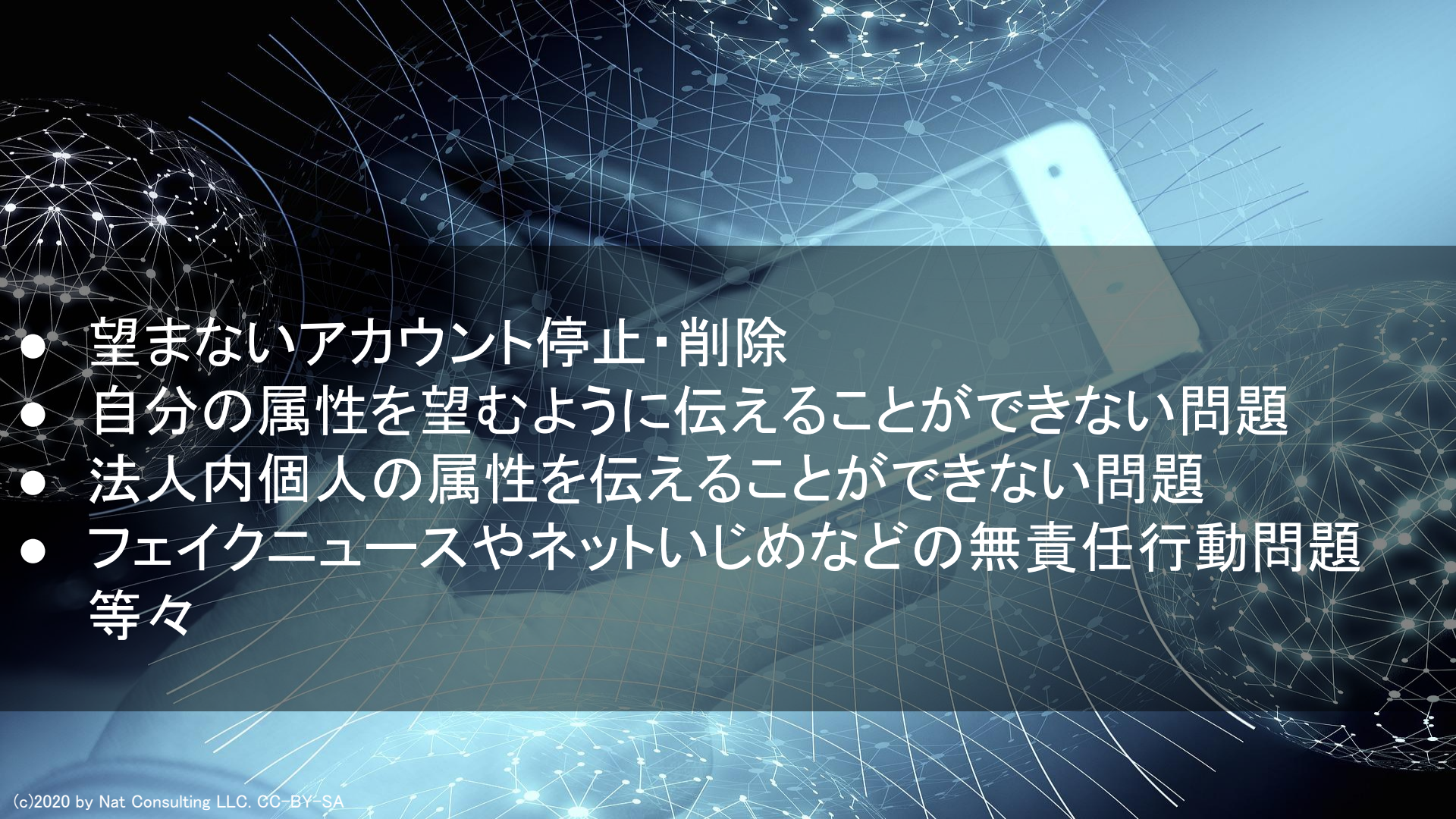
インターネット上のセキュリティ問題の9割方は、よろしくないIAMに起因している

ホワイトは素手のO5会合にて
アンチウイルスソフトの父
ピーター・ティペット博士

これらの事例もIAMがきちんとしていればきっと防げた

- NTT Comで「水平移動」型の不正アクセス、621社の情報流出の恐れ (ZDNet, 2020-05-28)
- JAXAサイバー攻撃に関与 中国共産党員、不正契約容疑で書類送検 (朝日新聞, 2021-04-21)
- ドコモ口座の開設や銀行との連携、銀行側の本人確認の仕組みなどでセキュリティ面で穴があった可能性がある。(日本経済新聞 2020-09-09)
- 本人確認の手続き突破 SBI証券で顧客資金流出 (日本経済新聞 2020-09-17)
- 「SMS認証代行」対策強化 「犯罪の温床」指摘—本人確認すり抜け・警察庁

これだけでトラストは
確保できるのか？

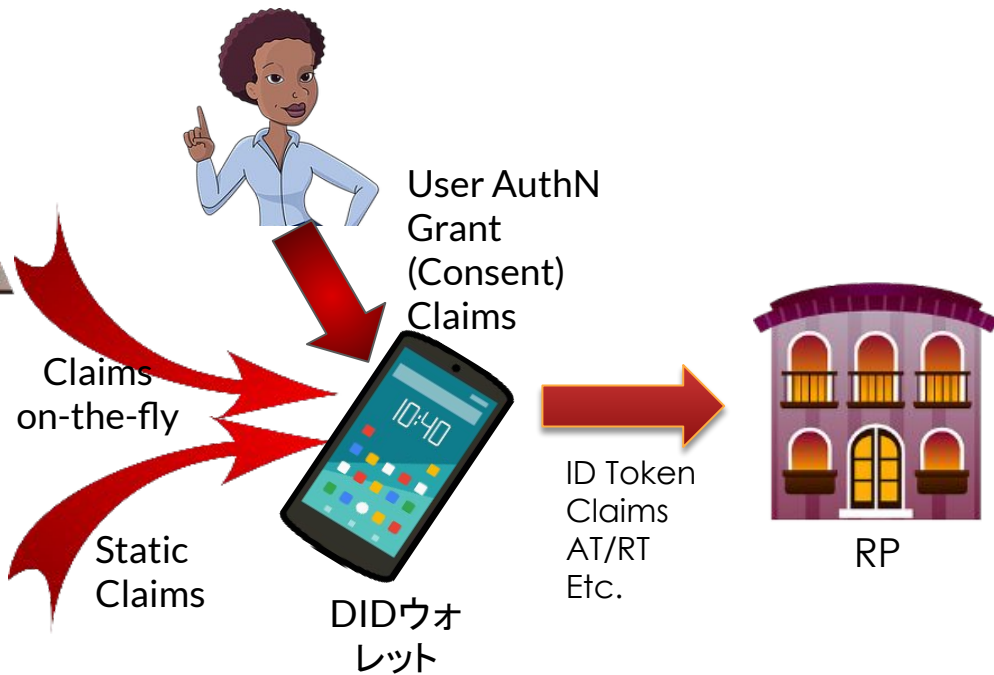
- 
- 望まないアカウント停止・削除
 - 自分の属性を望むように伝えることができない問題
 - 法人内個人の属性を伝えることができない問題
 - フェイクニュースやネットいじめなどの無責任行動問題等々

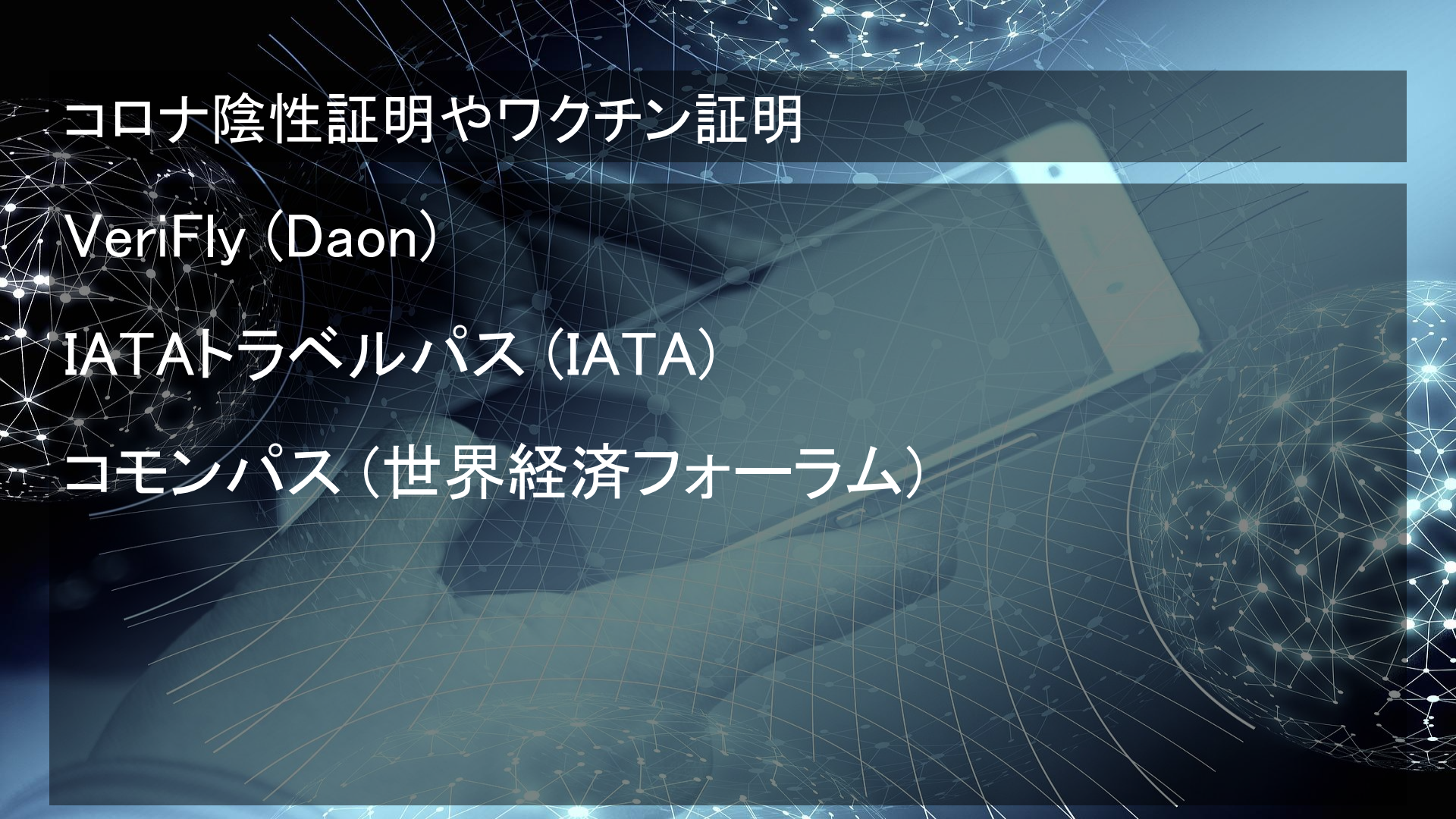
自己主権型アイデンティティ 非集中型識別子(DID) 検証可能クレデンシャル(VC)

SSI/DID、DID/VC

発行されたVCを DIDウォレットに 保存しておいて 使う

選択的属性提供も



The background of the slide features a hand holding a smartphone, with a complex network of glowing lines and nodes overlaid on the image, suggesting a digital or technological theme.

コロナ陰性証明やワクチン証明

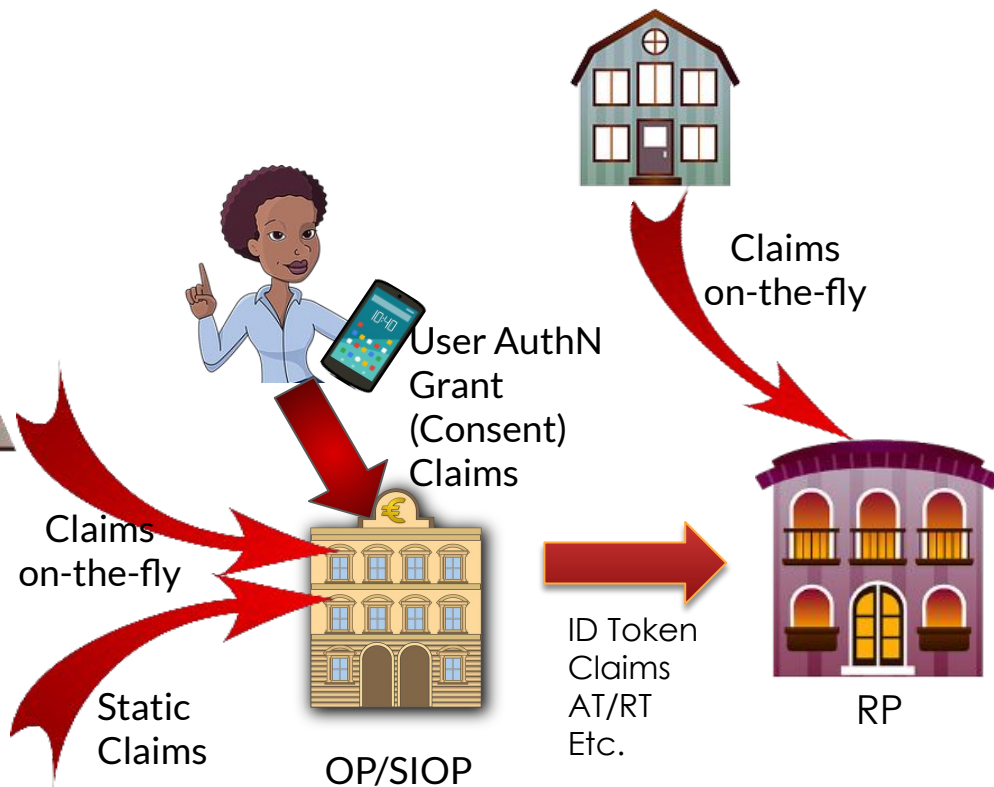
VeriFly (Daon)

IATAトラベルパス (IATA)

コモンパス (世界経済フォーラム)

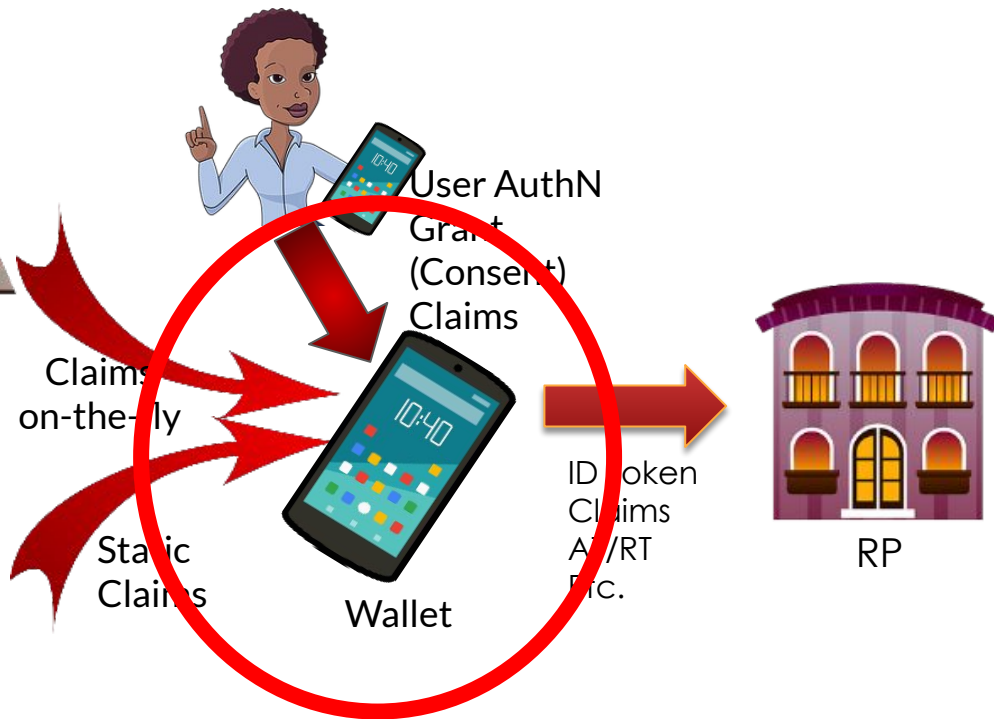
属性の権威的 源泉は必然的 に分散している

Which also forms
Basis for ABAC.



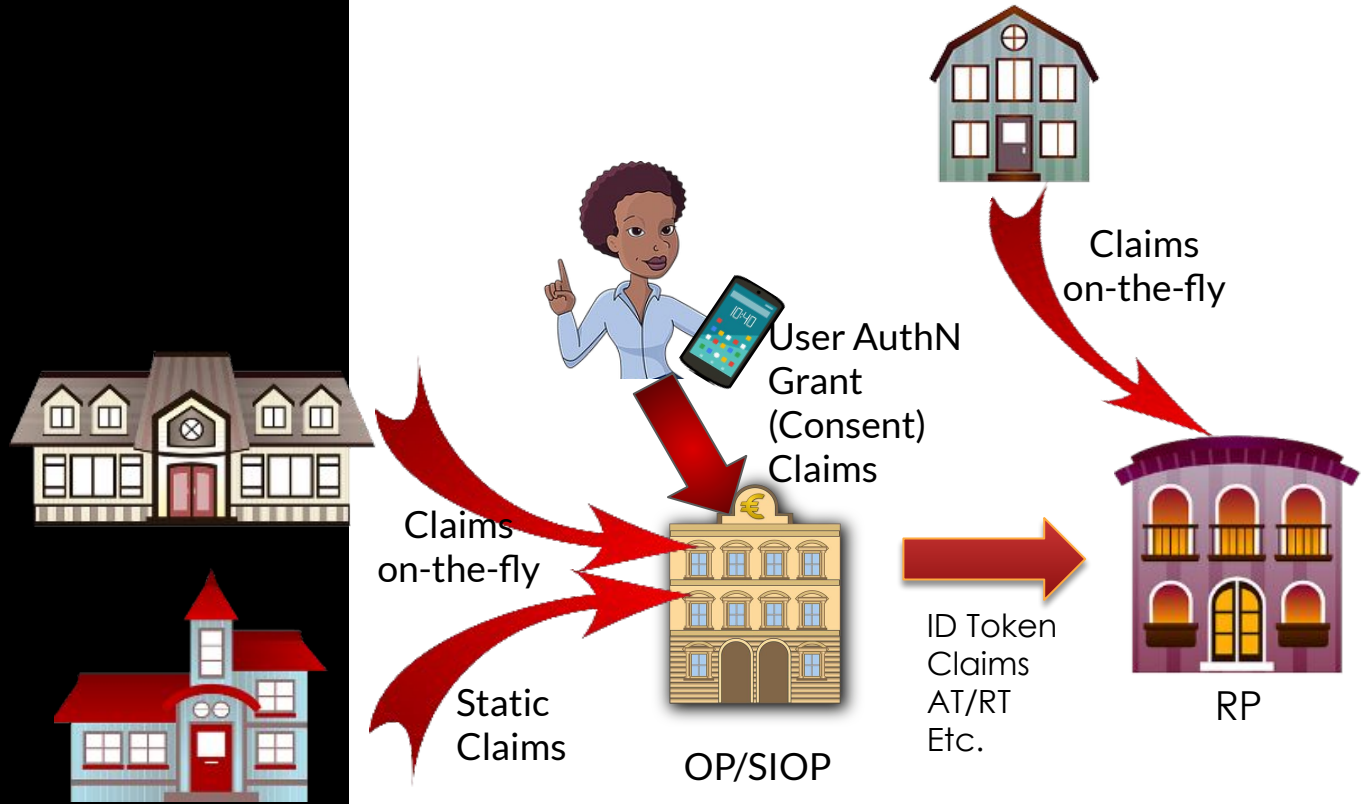
広がるか？！

DID/VC Framework



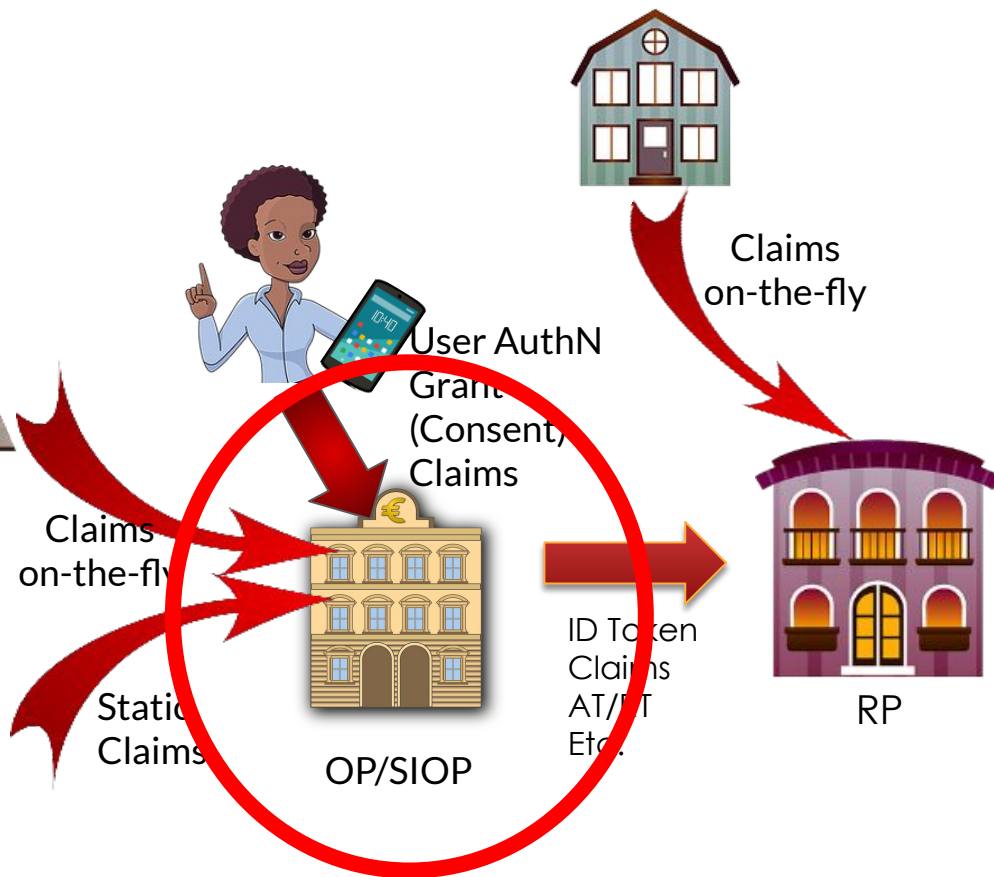
OpenID Connect

Which also forms
Basis for ABAC.



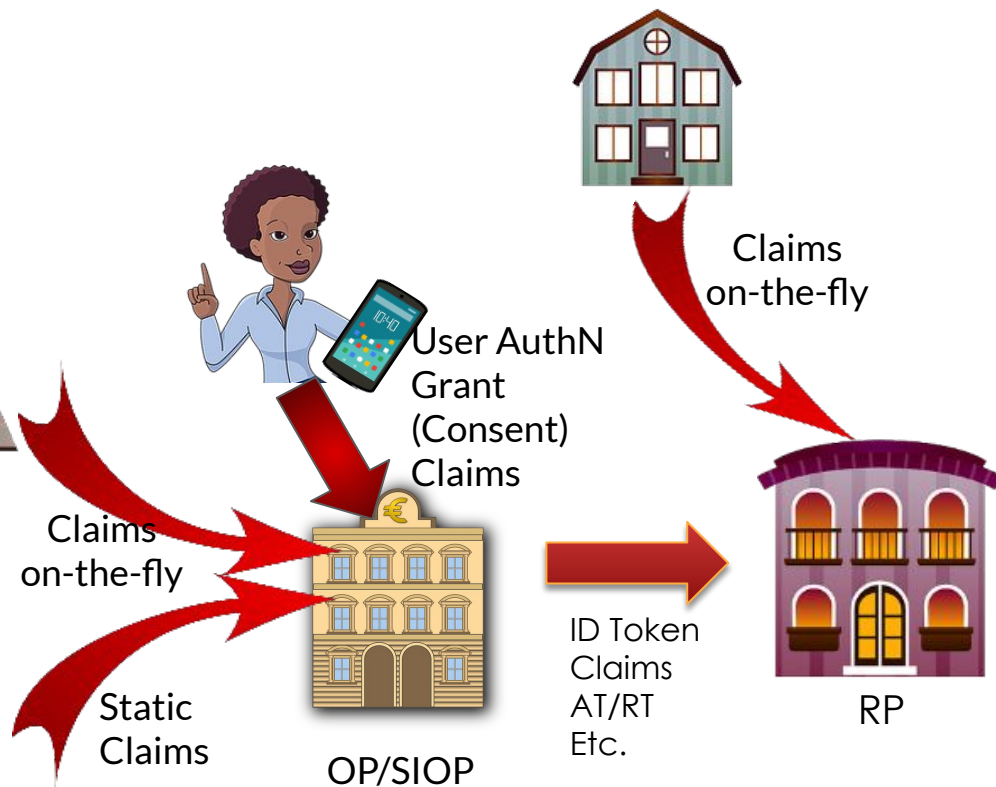
巨大Tech 携帯電話会社 etc.

Which also forms
Basis for ABAC.



2011年からある のにほぼ全く使 われていない

Which also forms
Basis for ABAC.



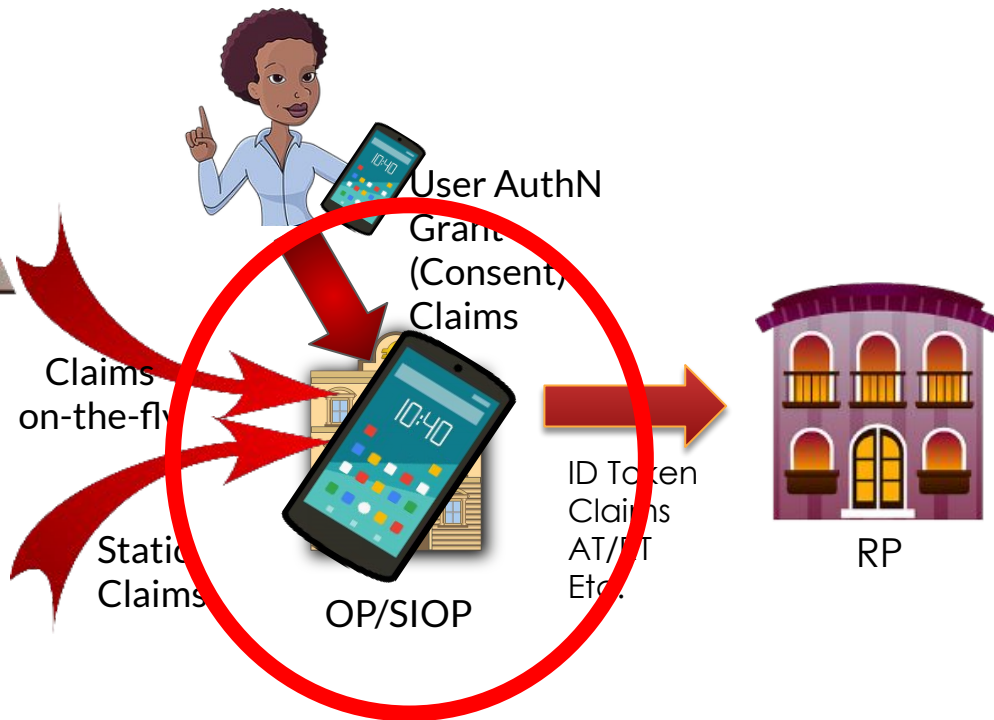


トラスト形成の問題

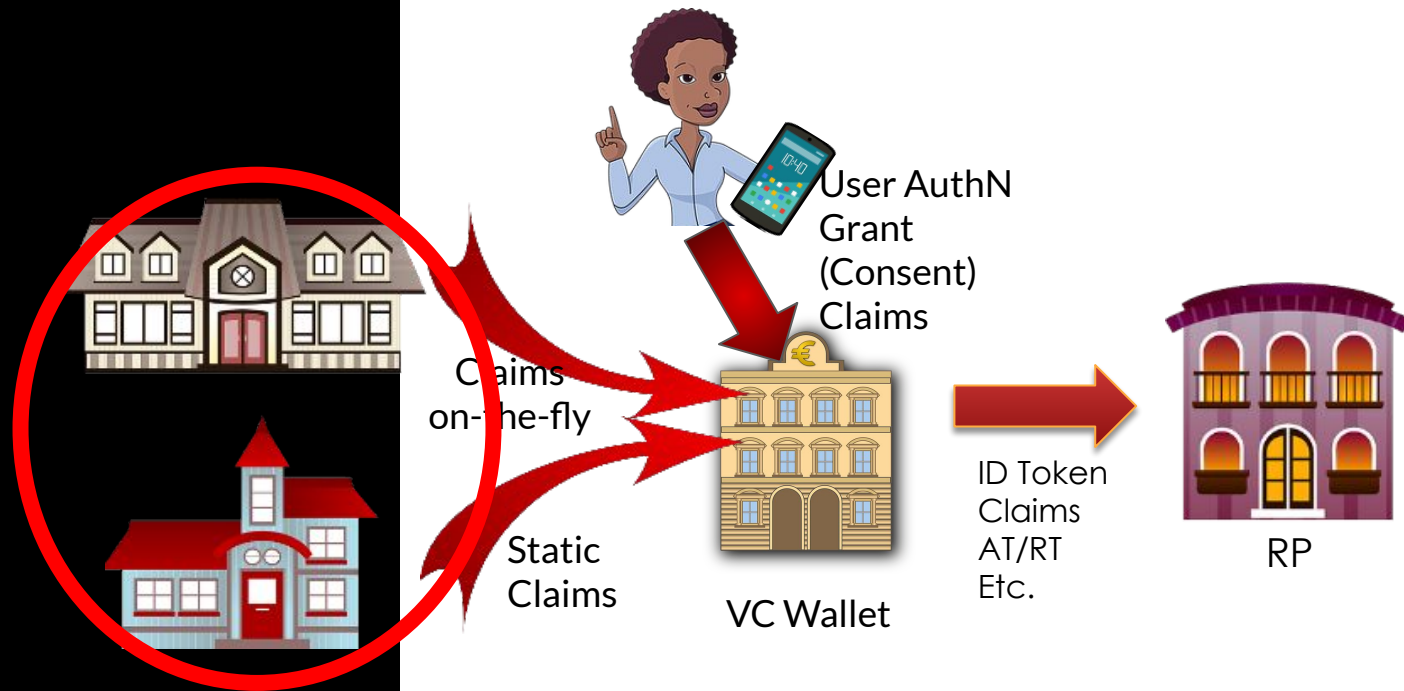
鍵を握る2つの ステークホルダー



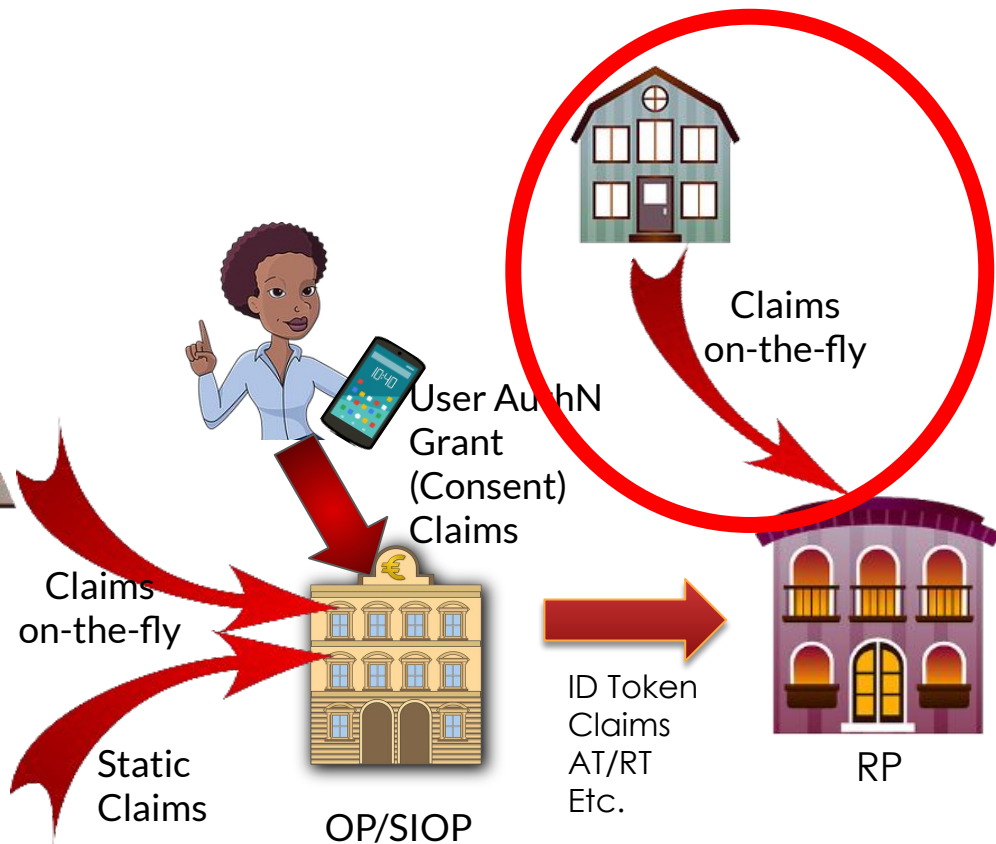
Hubの運用レベルに信頼度が依存



ビジネス上の問題



OpenIDのBy Referenceモデルは、この問題 に 対処する 意味もある





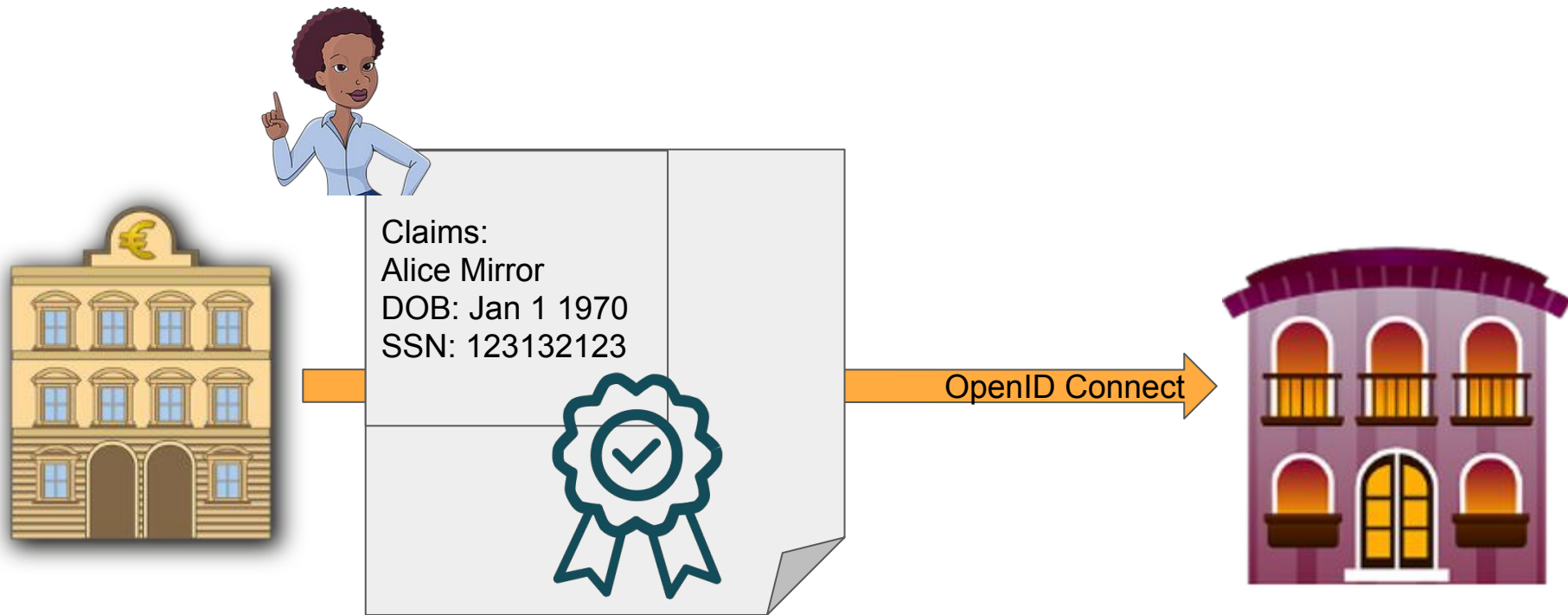
様々な権威的源泉が、Identity Document を発行することに対してインセンティブをもつようにならないければ、自分の属性を望むように伝えるようにはならない



法人内個人の属性を
伝えることができない問題

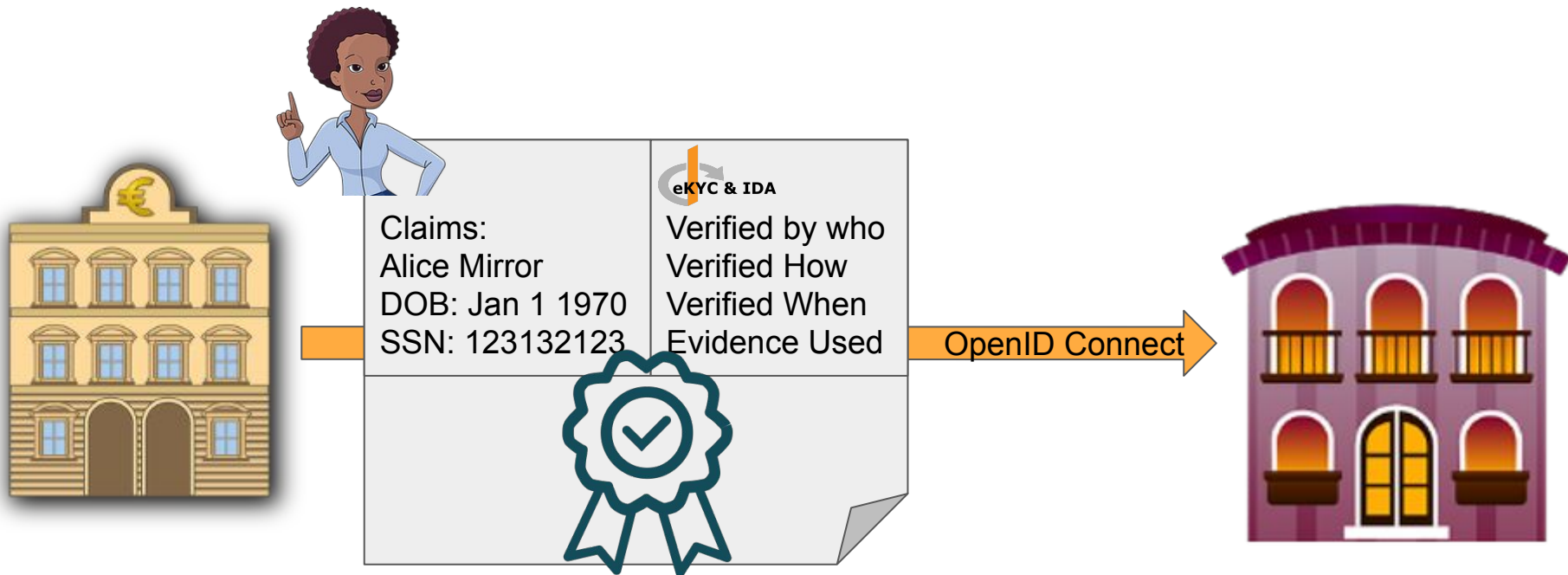


Signed Claims Passing Protocol



Signed Claims Passing Protocol

With added verification metadata





Signed Claims Passing Protocol

With added verification metadata
And draft (legal) entity authority claims



Claims: Alice Mirror DOB: Jan 1 1970 SSN: 123132123	eKYC & IDA Verified by Verified How Verified When Evidence Used
Authority to act... For: ACME Co Role: Director Granted by: Board of directors	

OpenID Connect





フェイクニュースやネットいじめなどの
無責任行動問題 etc.



トラスト形成に銀の弾丸は無い

デジタル存在の7つの原則

原則1. 責任あるデジタル存在 (Accountable Digital Being)

原則2. 表現力のあるデジタル存在 (Expressive Digital Being)

原則3. データの正当な取り扱い (Fair Data Handling)

原則4. 忘れられない権利の尊重 (Right NOT to be forgotten)

原則5. 人間に優しい (Human Friendly)

原則6. 普及しやすい (Adoption Friendly)

原則7. 誰もが利益を得られる (Everyone benefit)