デジタルアイデンティティの時代：その意味とセキュリティとの複雑な関係

株式会社パロンゴ 取締役 兼 最高技術責任者
林 達也(@lef)

2025/5/22
『第29回サイバー犯罪に関する白浜シンポジウム』

PARONGO
— internet security company —

Disclaimer

本講演・スライドはあくまで発表者個人としての発言・意見や感想にすぎず、所属組織や主催組織等の見解・表明ではありません。

発表者は弁護士等の資格を有するものではなく、法律の解釈などについては私見にすぎません。本講演の内容に基づいた結果、問題などが生じた場合にも責任を負いかねます。

基本的に発表は公開情報に基づき作成されていますが、誤りを含む可能性がございます。

また、一部質問などには業務上や法的にお返事できない場合がございます。

予めご了承ください。

About me

林 達也 (@lef)

所属(Profile)

- 株式会社パロンゴ 共同創業者 / 取締役 / 最高技術責任者
- デジタル庁 アイデンティティアーキテクト / アイデンティティユニット ユニット長
- LocationMind株式会社 シニアカウンシル
- 株式会社レピダム 創業者
- 経済産業省 商務情報政策局 情報プロジェクト室 (2020-2022)
- 慶應義塾大学大学院メディアデザイン研究科 後期博士課程
- 慶應義塾大学KMD研究所 所員
- etc...

林 達也 (@lef)

今日はここの人
として話します

所属(Profile)

- 株式会社パロンゴ 共同創業者 / 取締役 / 最高技術責任者
- デジタル庁 アイデンティティアーキテクト / アイデンティティユニット ユニット長
- LocationMind株式会社 シニアカウンシル
- 株式会社レピダム 創業者
- 経済産業省 商務情報政策局 情報プロジェクト室 (2020-2022)
- 慶應義塾大学大学院メディアデザイン研究科 後期博士課程
- 慶應義塾大学KMD研究所 所員
- etc...

PARONGO
— internet security company —

林 達也（@lef）

今日はここの人
として話します

所属(Profile)

- 株式会社パロンゴ 共同創業者 / 取締役 / 最高技術責任者
- デジタル庁 アイデンティ
  アイデンティティユニット
- LocationMind株式会
- 株式会社レピダム 創業
- 経済産業省 商務情報政
- 慶應義塾大学大学院メ
- 慶應義塾大学KMD研究所 所員
- etc...

いわゆる
『産学官』の
全部の中に

PARONGO
— internet security company —

少し前は…

- 週2日経済産業省の公務員として…
- コロナと戦ったり、
- DX(笑)をしたり、
- 省内の室をゼロトラストにしたり、
- 法人認証基盤(gBizID)や、その他gBizスタックと呼ばれるサービス基盤のお手伝いをしたりしていました(過去形?)

ちょっとゼロトラストっぽい、でも本当はゼロトラスト無理という記事

メニュー　キーワードで検索　日経XTECH

IT | 電機 | 自動車

そんな中、経済産業省は2021年5月12日に「DXオフィス関連プロジェクト管理業務等の効率化に関するデジタルツールの導入実証・調査事業」の報告書をソフトウエア開発プラットフォーム「GitHub」上で公開した。同事業ではゼロトラストの概念を取り入れた業務環境を構築し、実証と調査をしたのだという。「なぜ経産省がゼロトラストを」という興味から報告書を確認すると、民間企業でもなかなか見られない、「イケてる」アーキテクチャーを作り上げていたことに驚いた。2つ挙げたい。

経済産業省の「DXオフィス関連プロジェクト管理業務等の効率化に関するデジタルツールの導入実証・調査事業」報告書。GitHub上で公開している

［画像のクリックで拡大表示］

日経クロステックより引用
(https://xtech.nikkei.com/atcl/nxt/column/18/00138/061400820/)

最近は…(1)

BitSight	Cybersixgill	PICUS	Corelight
• Attack Surface Management (ASM)	• Threat Intelligence (TI)	• Breach & Attack Simulation (BAS)	• Network Detection and Response (NDR)

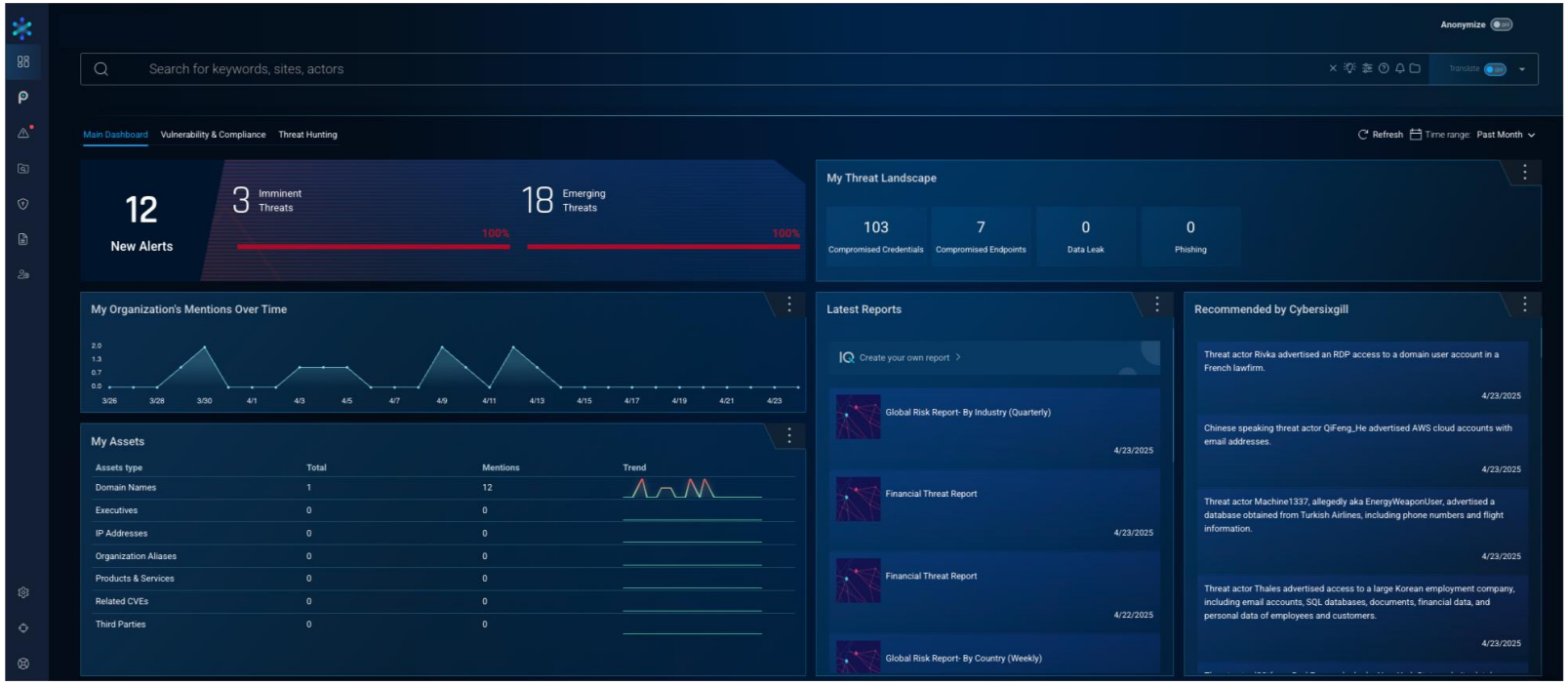
“Security Automation”をミッションとしているInternet Securityの企業

少数精鋭による効率的で効果的なManaged SOC等、多くの企業様の実用的なセキュリティ自動化を実現

近代的なセキュリティプロダクトのポートフォリオ構成が"売り"

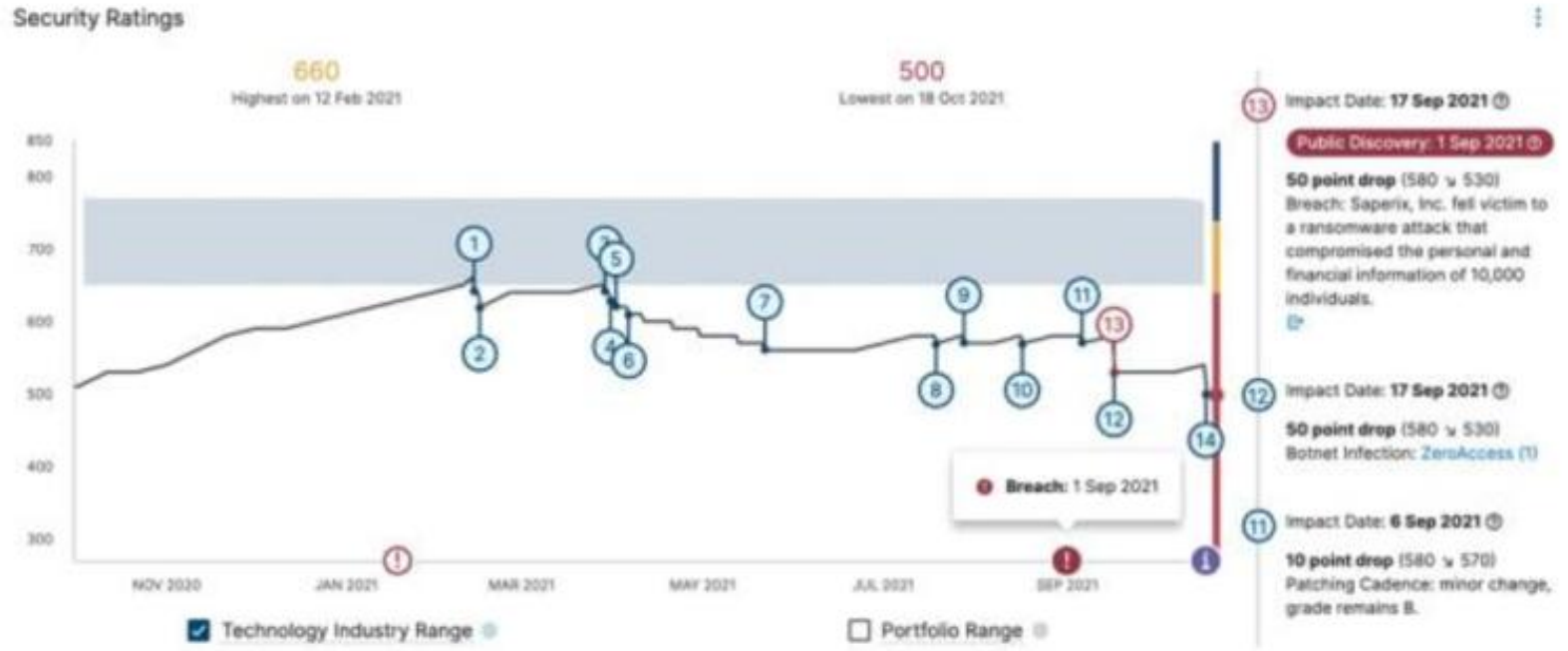
BITSIGHT

ASM:
Attack Surface Management



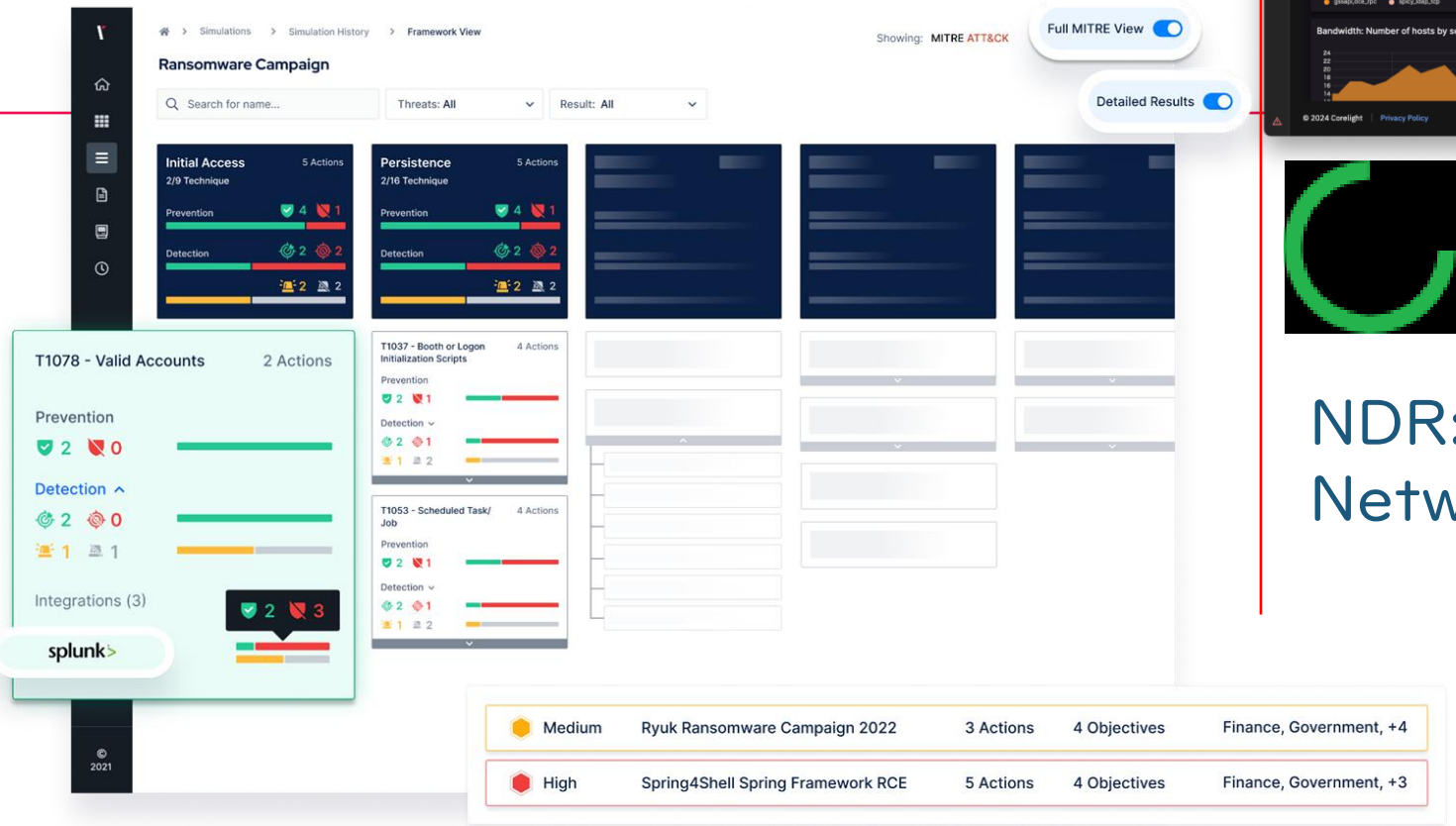
cybersixgill
A BITSIGHT Company

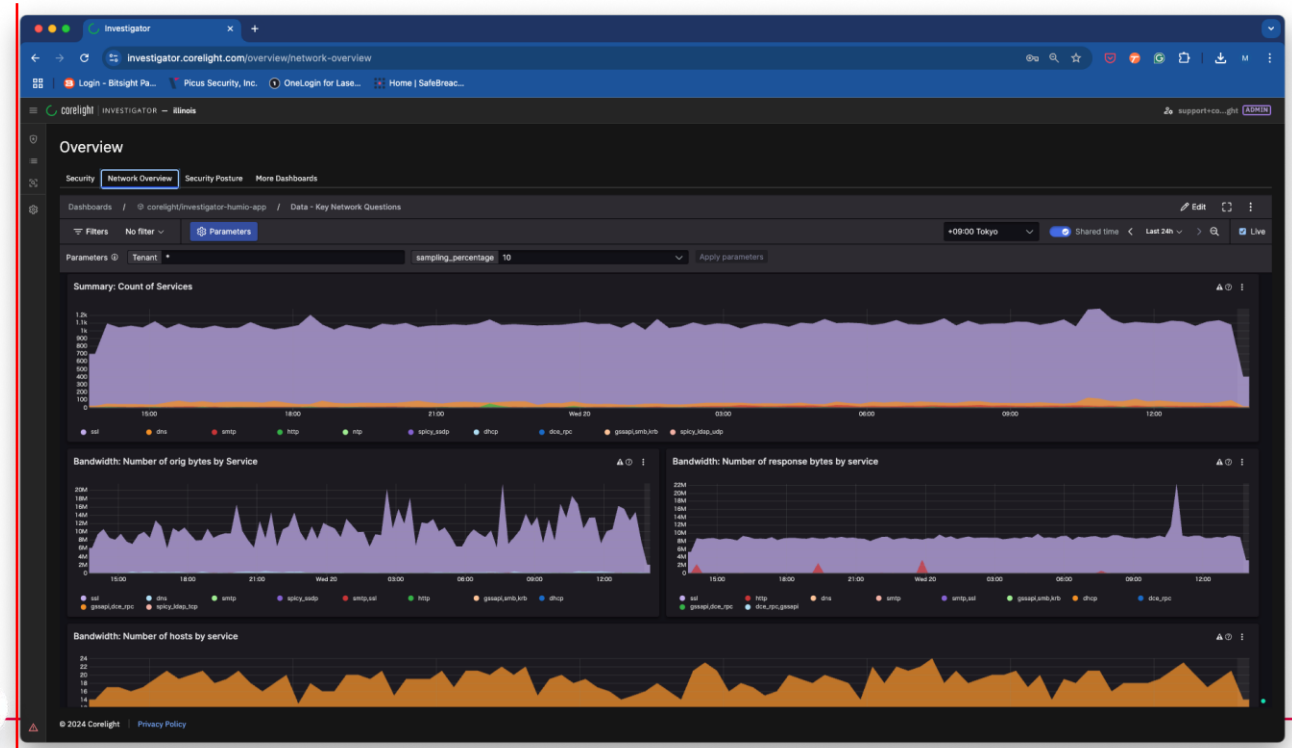
Threat Intelligence
(Coming soon / Pre-Sales)



PICUS

BAS: Breach & Attack Simulation





corelight

NDR:
Network Detection and Response

BITSIGHT

ASM: Attack Surface Management

ASMやべえ、という話は
BoFでやるので
是非ご参加ください
(イベント内イベント宣伝)

cybersixgill
A BITSIGHT Company

Threat Intelligence

(Coming soon / Pre-Sales)

BOF（1日目 20:00-21:40）

ASM

費用対効果の高いとされるASM製品の光と闇

林 達也 氏

Attack Surface Management(ASM)製品は、費用対効果の高いセキュリティソリューションとして普及が進みつつありますが、当然のように他のセキュリティと同様、奥の深い領域を持ちます。
導入や価格がライトウェイトな製品も目に付く中で、冷静にASM界隈のライトサイドと、強力さ故一歩間違うとある意味でのダークサイドに落ちるだけの側面があり、ASMのもたらしたセキュリティ観点の社会変容についてその専門性と倫理感等を踏まえた議論できればと思います。

・組織をスコアリングするというのはどういうことなのか？
・「外形的にわかる」ということの意味
・何を見るのか
・「他者」をも数値化できるということはどういうことか
・SCMと数値化の先にあるもの

実は微妙に
「アイデンティティ」
の話でもあります

最近は…(2)

アイデンティティ

プライバシー

認証・認可

国際標準

デジタル・ガバメント

各種ナショナルID
(マイナンバー/MNC、
法人番号/gBizID, etc...)

最近は…(2)

アイデンティティ

プライバシー

認証・認可

国際標準

ガバメント

種ナショナルID
(マイナンバー/MNC、
法人番号/gBizID, etc...)

世はまさに
大デジタル化時代！

最近は…(2)

アイデンティティ

プライバシー

認証・認可

国際標準

ガバメント

種ナショナルID

マイナンバー/MNC、
法人番号/gBizID, etc...)

そこらの大学院生を
国家公務員に
してしまうぐらい
人材不足！

エンジニアリング

アイデンティティアーキテクト

採用内容

採用予定官職

内閣官房情報通信技術（ＩＴ）総合戦略室室員
※身分は非常勤の一般職国家公務員となります。

採用予定人数

2名程度

採用予定日

令和3年7月1日以降（詳細は相談の上決定）

募集背景・業務内容

デジタル庁においては、行政サービスのデジタル化・ワンストップ化を推進するにあたって、利便性が高く安全な識別・認証の仕組みを構築することにより、多種多様なシステムにまたがった円滑なデータ連携を実現していくことが求められます。

アイデンティティアーキテクトは、各省庁の担当者や専門家と連携して、デジタルガバメントのサービス高度化に必要な、アイデンティティ管理、データ連携の枠組みを構想し、その整備を推進する役割を担っていただきます。

具体的な業務内容は、以下のとおりです。

- 政府情報システムに関わるアイデンティティ管理の計画策定全般
- 住民制度、公的個人認証、マイナンバー制度に関わる個人のアイデンティティ管理もしくはGビズID、商業登記電子証明書等に関わる法人等のアイデンティティ管理

デジタル庁（準備中）トップ　デジタル庁について　法令　新卒採用　中途採用　お知らせ

- 政府情報システムに関わるアイデンティティ管理の計画策定全般
- 住民制度、公的個人認証、マイナンバー制度に関わる個人のアイデンティティ管理もしくはGビズID、商業登記電子証明書等に関わる法人等のアイデンティティ管理
- 行政事務と住民・事業者向けシステム、住民・事業者向けシステム間をつなぐ国のシステムを理解した上での、業務プロセスの見直し、移行計画の立案、変革の推進
- 国民・事業者向けサービスや各省庁のシステムにおける利便性の高い安全な識別・認証の仕組みづくり
- 各省庁や地方公共団体の専門家と連携した横断的なプロジェクトの推進

応募条件

必須条件

- デジタル庁の設置に向けた理念、ミッション、基本的考え方への強い共感
- 社会全体のデジタル化に向けて、業務を人任せにせず、当事者意識をもって課題を解決していくマインド
- 「全体の奉仕者」たる国家公務員に求められる高い倫理観
- 不特定多数の利用者を対象とした大規模サービスの構築経験5年以上
- 大規模組織における情報システムの構築運用経験5年以上
- 大規模組織におけるID管理又はID管理支援経験3年以上
- 大規模Webサービスのシングルサインオンにかかわる設計・運用経験
- 個人情報保護の内部規定やプライバシーポリシーの策定・運用経験
- 住民制度、公的個人認証、マイナンバー制度、もしくはGビズID、商業登記電子証明書等の行政手続における事業者認証システムに関する基礎的な理解

歓迎条件

- 大規模アイデンティティ管理、不正対策などの経験
- 大規模組織または複数組織を横断するデータ連携基盤の構築、運用経験
- 日本及び海外の主要国における認証業務やデジタル署名等の関連業務に対する深い理解
- 政府や地方公共団体等の公的機関における調達支援経験

※なお、以下に該当する者は応募できませんので、予め御了承ください。

（a）日本国籍を有しない者

デジタル庁

【I_01】アイデンティティスペシャリスト

デジタル庁

応募する

Identity/Privacy

仕事概要

【募集背景・業務内容】
デジタル庁では、マイナンバーカード及びスマートフォン向けのマイナンバーカード機能搭載の普及を促進し、本人確認サービス・認証サービス・電子署名サービス等アイデンティティに係るサービスを提供することで、行政手続きを円滑にするための取り組みを行っております。今後、諸外国で導入が進んでいるスマートフォン向けの次世代サービスの導入等による更なるサービス性の向上が求められます。 アイデンティティスペシャリストは、先端的な技術動向を把握した上でデジタルアイデンティティに係る各サービスの将来像を描き、 各種ID技術やPKI技術の関係するサービス・プロダクトについて継続的な改善を行い、安定的なサービス運用をリードすることで、国民の利用拡大を図る役割を担っていただきます。

具体的な業務内容は、以下の通りです。
・マイナンバーカードを利用した認証及びスマートフォン向けマイナンバーカード機能搭載に関する技術支援
・ID/認証基盤としてのマイナンバーカード関連サービスに関する技術支援
・次期 JPKI システムの更改に関する支援 ・次期マイナンバーカード検討の支援
・Common Criteria認証取得におけるセキュリティ監査の支援
・ISO/IEC, IETF, W3C, FIDO Alliance, OpenID Foundation 等の標準化動向の英文仕様書の調査
・EU Digital Identity Wallet関連、Mobile Driver’s License 関連の動向や外部仕様及び内部仕様の調査

デジタル庁

【I_02】プライバシーデザイナー

デジタル庁

応募する

Identity/Privacy

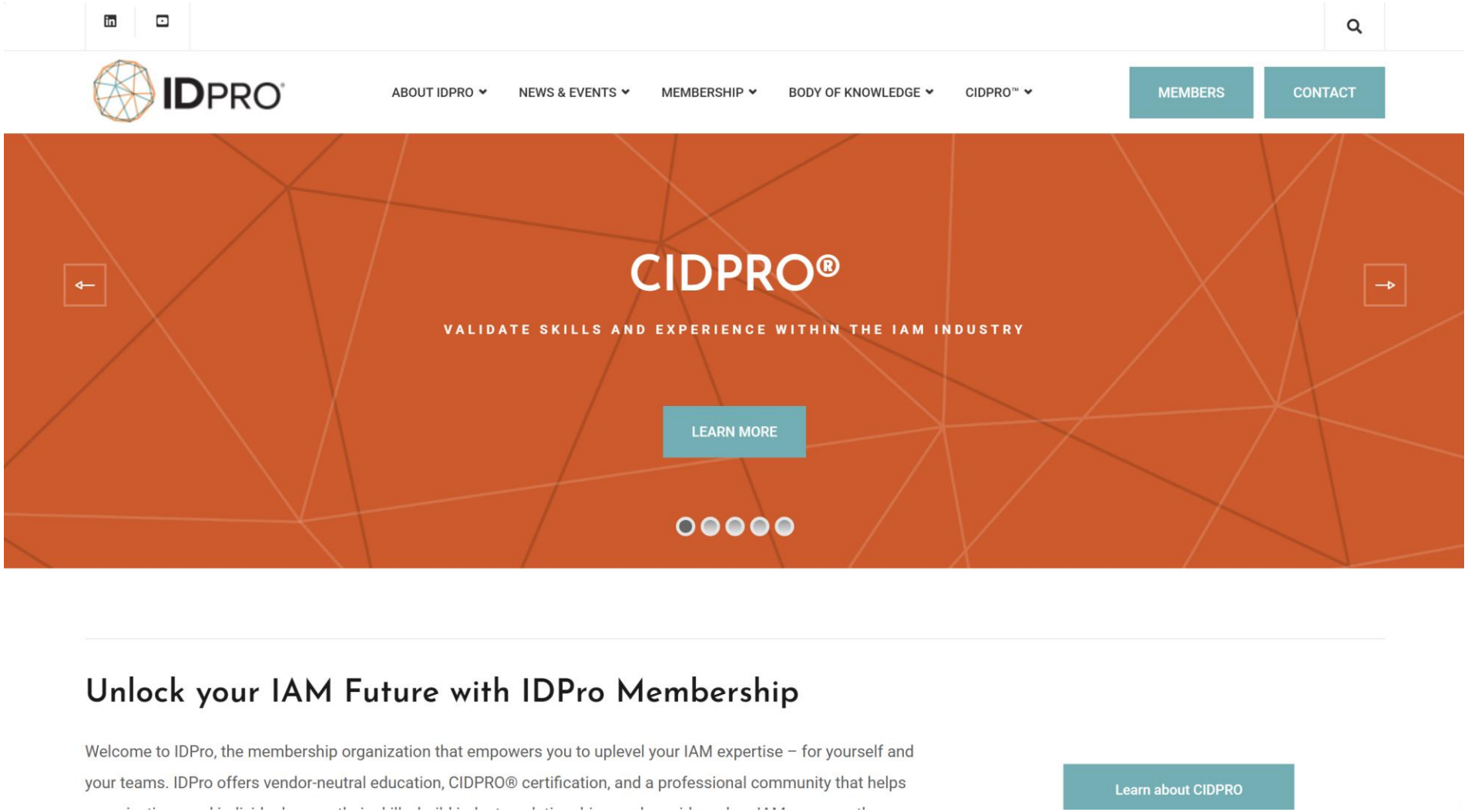
仕事概要

【募集背景・業務内容】
デジタル庁では「誰一人取り残されない、人に優しいデジタル化を」をミッションに掲げ、一人一人のニーズに合った行政サービスの提供に取り組んでいます。プライバシーデザイナーは、プライバシーに配慮した行政サービスを設計・提供すべく、庁内外の関係者との連携を取りながら、デジタル庁におけるプライバシー保護の取り組みをリードする役割を担います。

具体的にはご経験やご志向を踏まえて以下のような業務をご担当いただきます。
- デジタル庁が所管する制度についてプライバシーや個人情報保護の観点での諸課題の検討
- データマッピングやプライバシー影響評価、プライバシーバイデザインの支援
- プライバシーポリシーの作成や継続的な改善
- プライバシーガバナンスの取り組みの推進
- 行政機関、地方公共団体、民間事業者、利用者等からの照会対応の支援
- 個人情報漏洩などのインシデント対応の支援
- プライバシーに係る庁内の教育や啓発活動の支援
- 標準化の推進やガイドラインの作成
- 庁内外のステークホルダーとの連携

歓迎スキル

・ビジネスレベルの英語力
・サービスの利用規約及びプライバシーポリシーに係る知見
・関連法・制度に係る知見
・標準化コミュニティへのコミット、標準化仕様の実装に関連した認証認可システム開発に携わった経験
・公的個人認証制度及びJPKIに関連するシステム構築に携わった経験
・マイナンバーカードの認証または電子署名機能を利用したシステムの開発経験
・CIDPRO Certification取得者



https://idpro.org/cidpro/

歓迎スキル

- ビジネスレベルの英語力
- サービスの利用規約及びプ
- 関連法・制度に係る知見
- 標準化コミュニティへのコ
- 公的個人認証制度及びJPKI
- マイナンバーカードの認証
- CIDPRO Certification取得

システム開発に携わった経験

経験

デジタルアイデンティティや
プライバシーに
興味がある方は是非

2日目 2015.05.22（fri）

多目的ホールで実施　ホテルシーモアにて実施　パラレルセッション　コンテスト関連　セキュリティ道場関連　企業展示

	交通機関のご案内 バス(8:30発)：ホテルシーモア → オフィシャルホテル経由 → Big・U			
9:50～ 10:00	開演（本日のご案内と連絡事項など）			
10:00～ 11:00	講演 「ＪＣ３の設立と法執行機関との連携」 竹本佳史氏 （日本サイバー犯罪対策センター）	パラレル セッション 林達也 氏 （株式会社レピダム）	コンテスト決勝戦 午前の部	
11:05～ 12:05	講演 「組織における内部不正をいかに防止するか」 小松文子 氏 （IPA）	真武信和 氏 （グリー株式会社） 研修室4		

2日目 2015.05.22（fri）

多目的ホールで実施 | ホテルシーモアにて実施 | パラレルセッション | コンテスト関連 | セキュリティ道場関連 | 企業展示

	交通機関のご案内 バス(8:30発)：ホテルシーモア → オフィシャルホテル経由 → Big・U			
9:50～ 10:00				
10:00～ 11:00	「ＪＣ３の設立 （日本サイバー犯罪対策センター）		ム）	コンテスト決勝戦 午前の部
11:05～ 12:05	講演 「組織における内部不正をいかに防止するか」 小松文子 氏 （IPA）	真武信和 氏 （グリー株式会社） 研修室4		

10年ぶり2度目の
白浜シンポジウム
(奇しくも同日5/22)

これがわたしの

アイデンティティ

です

First of all / まず最初に

「デジタルアイデンティティ」は
「セキュリティ」より
"圧倒的"に
広い概念です

分野の広大さの一部
(セキュリティと接点のありそうなところ)

技術	運用	エコシステム	法・制度・権利等
• 認証(AuthN) • 認可(AuthZ) • OpenID Connect • パスキー/FIDO	• 本人確認=(身元確認・当人認証) • アカウントライフサイクルマネジメント • 監査可能体制・ガバナンス	• ID連携/IDフェデレーション • トラストフレームワーク	• 個人情報保護法 • プライバシー

セキュリティと
デジタルアイデンティティの関係

- 『セキュリティ』の単語が差す範囲の広さ

- 『デジタルアイデンティティ』の単語が差す意味と目標の広さ

セキュリティと
デジタルアイデンティティの関係

- 『セキュリティ』の単語が差す範囲の広さ
  - 個だけではなく、組織じゃ社会の動向も含む

- 『デジタルアイデンティティ』の単語が差す意味と目標の広さ
  - 権利や人権等も含め「個」の保護やその扱いに関する領域が広い
  - (本当は人だけではない)

セキュリティと
デジタルアイデンティティの関係

- 『セキュリティ』の単語が差す範囲の広さ
  - 個だけではなく、
- 『デジタルアイデ 標の広さ
  - 権利や人権等も 頂域が広い
  - (本当は人だけで

デジタルアイデンティティは
物理とデジタルを
接合する概念

目的と手段、そしてデジタルでの成熟

- セキュリティそのものは「目標」ではなくあくまで「手段」
- 「デジタルアイデンティティ」や「プライバシー保護」は目標足りえる
  - そして、これを実現する「手段」が「セキュリティ」
- 組織の柵などや世間の動向・トレンド・バズワードなど、そして何より関係者の多大なる努力と貢献によって「セキュリティ」は一定の市民権を得た
- しかし、手段と目的を取り違えてはいけない
- 何事も目的が明確でなくてはいけない
- 『セキュリティの市民権を得る過程のその経験』を我々はまだ持っている
  - 大変だったが、同じように『デジタルアイデンティティが市民権を得る』為の知見・経験を持っているはず
  - (これは実はプライバシーも同じ)

デジタルアイデンティティはデジタル社会を目指す人類の今後の重大目標

- 社会における アイデンティティ
- デジタル 社会における デジタル アイデンティティ

- セキュリティは、それを保護する手段
  - そして認証技術は、単に本当にその一端に過ぎない
- セキュリティの領域が広がると、アイデンティティをカバーする範囲も少しずつ増えるはず

OECDのRecommendationから…

- Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (**1980**)　　(25年…4半世紀)
  - https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188
- Recommendation of the Council on the Governance of Digital Identity (**2023**)　　(何年かかるか…)
  - https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491

Case Study

SBI証券問題(2020)

- 2020/09/16に、ネット証券最大手のSBI証券において、6人の証券口座から9,864万円が不正に流出した
- 送金先は、ゆうちょ銀行の5口座と三菱UFJ銀行の1口座
  - いずれも証券口座の顧客と同一名義だが、第三者が不正に開いたもの
  - 口座開設時は、偽造した保険証などの本人確認書類が使われていた

(SBI証券の6口座に不正ログイン 9864万円被害：朝日新聞デジタル (asahi.com) より)

証券会社問題再び(2025)

- 2025年1月ごろから、いわゆるID Theft / アカウント詐取での不正ログインによる金融犯罪事案の発生が急増

金融庁
Financial Services Agency

文字サイズ

サイト内検索 Google 提供

ホーム | 金融庁について | 報道・広報 | 政策・審議会 | 法令・指針等 | 金融機関情報

ホーム > 金融庁からのお願い・注意喚起 > インターネット取引サービスへの不正アクセス・不正取引による被害が急増しています

ポスト

令和７年４月３日
（令和７年５月８日更新）
金融庁

インターネット取引サービスへの不正アクセス・不正取引による被害が急増しています

○　実在する証券会社のウェブサイトを装った偽のウェブサイト（フィッシングサイト）等で窃取した顧客情報（ログインIDやパスワード等）によるインターネット取引サービスでの不正アクセス・不正取引（第三者による取引）の被害が急増しています。

	2025年1月	2025年2月	2025年3月	2025年4月	合計
不正取引が発生した証券会社数（社）	2	2	5	9	ー
不正アクセス件数	65	43	1,420	4,852	6,380
不正取引件数	39	33	687	2,746	3,505
売却金額	約0.8億円	約１億円	約129億円	約1,481億円	約1,612億円
買付金額	約0.7億円	約0.6億円	約128億円	約1,308億円	約1,437億円

	2025年1月	2025年2月	2025年3月	2025年4月	合計
不正取引が発生した証券会社数（社）	2	2	5	9	ー
不正アクセス件数	65	43	1,420	4,852	6,380
不正取引件数	39	33	687	2,746	3,505
売却金額	約0.8億円	約１億円	約129億円	約1,481億円	約1,612億円
買付金額	約0.7億円	約0.6億円	約128億円	約1,308億円	約1,437億円

手口とされている手法 (未検証)

(以下、報道等からのまとめであり不正確な可能性がある)

金融ISAC...
犯罪...
警察...

1. 「**銀行**口座X(出金用)」の入手
    1. 偽造した身分証明書等で銀行口座を開設、または第三者からの銀行口座買取
2. 「証券口座Y(売り用)」の入手
    1. 偽造した身分証明書等で証券口座を開設、または第三者からの証券口座買取
3. 「証券口座A(購入用)」の詐取 (認証情報の不正入手)
    1. 各種手法で、「すでに実在する第三者(被害者)の証券口座へのアクセス権を詐取
4. 株価操縦
    1. 口座A(購入用)に不正にログインし、流動性の低い海外株や日本の小型株を購入し株価を吊り上げる
    2. 株価が十分に上昇したタイミングで、口座Y(売り用)で同じ株式の売り注文を出し、板取引で約定
5. **出金**
    1. 口座A(購入用)は、犯罪者のものではないので損失を抱えた株が残り、口座X(売り用)で利益を確定させ、不正に取得した銀行口座Xに**出金**

「証券口座「乗っ取り」の全貌と犯罪阻止への一手、犯行グループが株売却に使っている口座の特定を急げ」(https://toyokeizai.net/articles/-/876277) を参考、及び当該記事執筆者 カウリス株式会社 代表取締役 島津敦好氏の協力による / なお、修文による文責は登壇者にあります

何が起きていたのか？ 何が恐ろしいか？

- 巨大金銭的被害の生じる犯罪 (もちろん)
- 相場操縦 (以前よりも物凄く容易な)
- マネーロンダリング？
- 「それなりの規模の金額を動かすことが出来る効率の良さと確率の高さ」

- (今回はなさそうだが) 個社の株価暴落による業務妨害も可能そう
- この瞬間、どのぐらいの証券口座が攻撃者の手中にあるのか…？

「証券口座「乗っ取り」の全貌と犯罪阻止への一手、犯行グループが株売却に使っている口座の特定を急げ」(https://toyokeizai.net/articles/-/876277) を参考、及び当該記事執筆者 カウリス株式会社 代表取締役 島津敦好氏の協力による / なお、修文による文責は登壇者にあります

銀行・証券口座の課題

- 偽造した身分証明書などを活用して銀行口座を開設し、その銀行口座を入出金先に指定して売り用の証券口座も不正に開設するケース
- 口座開設者がそのまま不正売買に使うケース
- 第三者（他の犯行グループ）に譲り渡すケース
- 転売目的で銀行口座と証券口座を同時に作り、犯行グループに高額の値段で譲り渡す顧客も一定数いるものと思われる
- SNSなどを通じて口座を不正に買い取るケース
  - SNSに書き込まれている「買い取り募集」の多くは銀行口座だが、信用金庫・信用組合の口座や証券口座、暗号資産アカウント、クレジットカードなどの書き込みも多数存在する

「証券口座「乗っ取り」の全貌と犯罪阻止への一手、犯行グループが株売却に使っている口座の特定を急げ」(https://toyokeizai.net/articles/-/876277) を参考、及び当該記事執筆者 カウリス株式会社 代表取締役 島津敦好氏の協力による / なお、修文による文責は登壇者にあります

オンライン犯罪の手口の進化

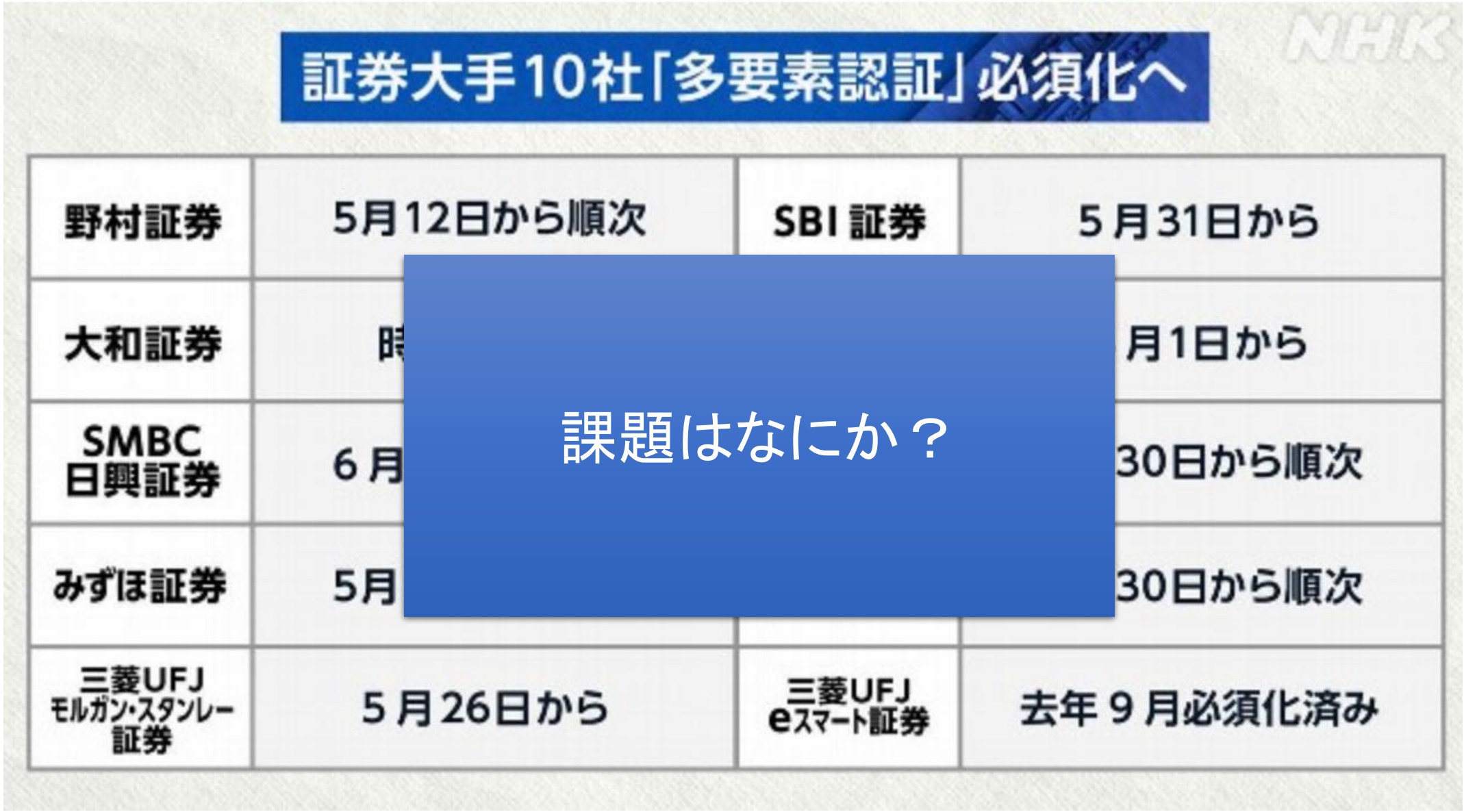
- 最近のオンライン犯罪は、分業化が進んでいることが特徴の1つ
  - 身分証明書を偽造するグループ、口座を開設するグループ、フィッシングなどでログインID等を詐取するグループ、実際の不正取引を行うグループ、出金後にマネーロンダリング（資金洗浄）をするグループなど
  - さらに、それぞれの犯行グループがAIなどのテクノロジーやSNSなどを活用しているほか、金融業の知見も持ち合わせている。
  - 近年、金融犯罪被害が急増しているのは、こうした分業体制の下で相当な人数が関与しているためだと思われる
- 社会はオンライン・デジタルに全く追いついていない
  - 今後、もっともっと手口は進化し、高度化することが容易に予測される
  - デジタルの手段が、物理社会を変容させている（分業・トクリュウ等）

「証券口座「乗っ取り」の全貌と犯罪阻止への一手、犯行グループが株売却に使っている口座の特定を急げ」（ https://toyokeizai.net/articles/-/876277 ）を参考、及び当該記事執筆者 カウリス株式会社 代表取締役 島津敦好氏の協力による / なお、修文による文責は登壇者にあります

セキュリティ的にはどうか？

- 端的にいって証券会社の怠慢という側面は否めない
  - 言語バリアによる甘えも正直あっただろう
    (稚拙なフィッシング文面等で我々は出遅れている)
- 更に、厳しい言い方をすると、「出口」である銀行口座開設時のスキーム、つまり「本人確認」のプロセスの課題も大きい
- 2020年にも問題が起きていたにも関わらず、という点も罪深い
- 特に、証券口座開設部分はまだしも、証券口座へのオンラインアクセス時の認証部分に関しては、度々問題視されていた
- ただし、証券取引は一刻も早く手続きをしたいインセンティブが存在しうるため、複雑な認証手段を導入しにくかったであろうことは想像に難くない
- が…

https://www3.nhk.or.jp/news/html/20250520/k10014808601000.html



課題はなにか？

https://www3.nhk.or.jp/news/html/20250520/k10014808601000.html

楽天証券 @RakutenSec · 5月12日

【重要】ログイン追加認証（多要素認証）サービスの仕様変更について

この度、当社のログイン追加認証（多要素認証）サービスに関しまして、セキュリティ強化のため以下の通り仕様を変更いたしました。

①発行された認証コードは、1回ログインに失敗すると無効になります。
②連続で3回認証に失敗した場合、口座をロックさせていただきます。

引き続きセキュリティ対策の強化に努めてまいりますので、何卒ご理解賜りますようお願い申し上げます。

楽天証券 @RakutenSec · 5月12日

6月1日より、ログイン追加認証（多要素認証）が全チャネル必須になります。
詳細は以下よりご確認ください。
r10.to/hgwl5T

また、ログイン追加認証（多要素認証）サービスの詳細は以下よりご確認ください。
r10.to/hgh9uO

4 10 32 2万

オカダリョウタロウ @okdt · 5月12日

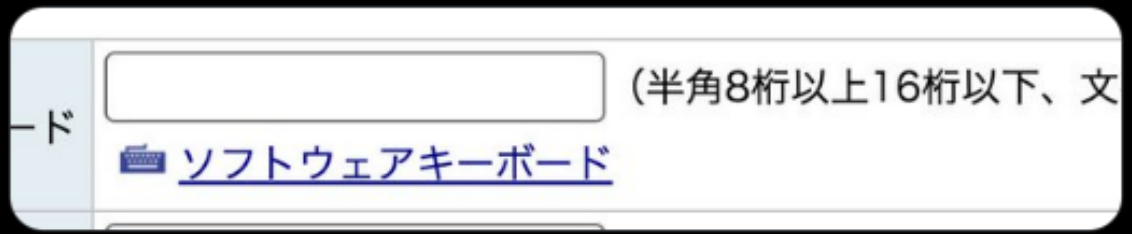
現状のパスワードポリシー「半角8桁以上16桁以下」、これひどいので、変えてください

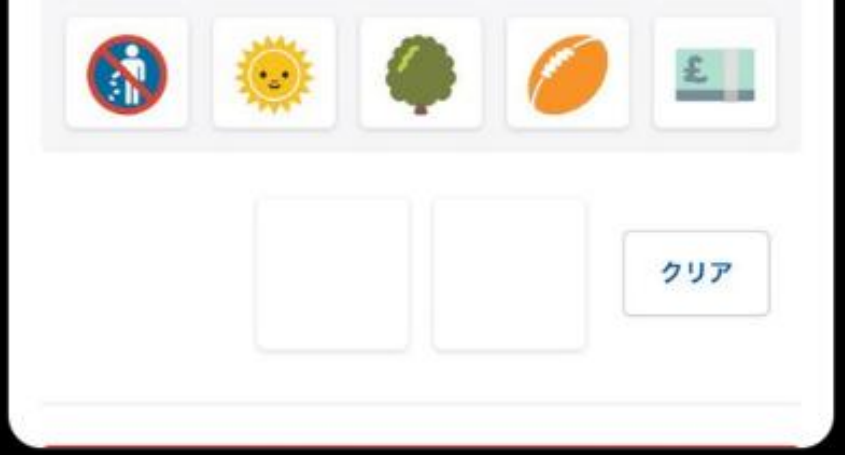
8桁以上->15桁以上、そして最大桁数は、64桁は最低でも許容してください。

文字種に関する制限をやめてください。

NIST 800-63B参照
OWASP ASVS 5.0

> @RakutenSec

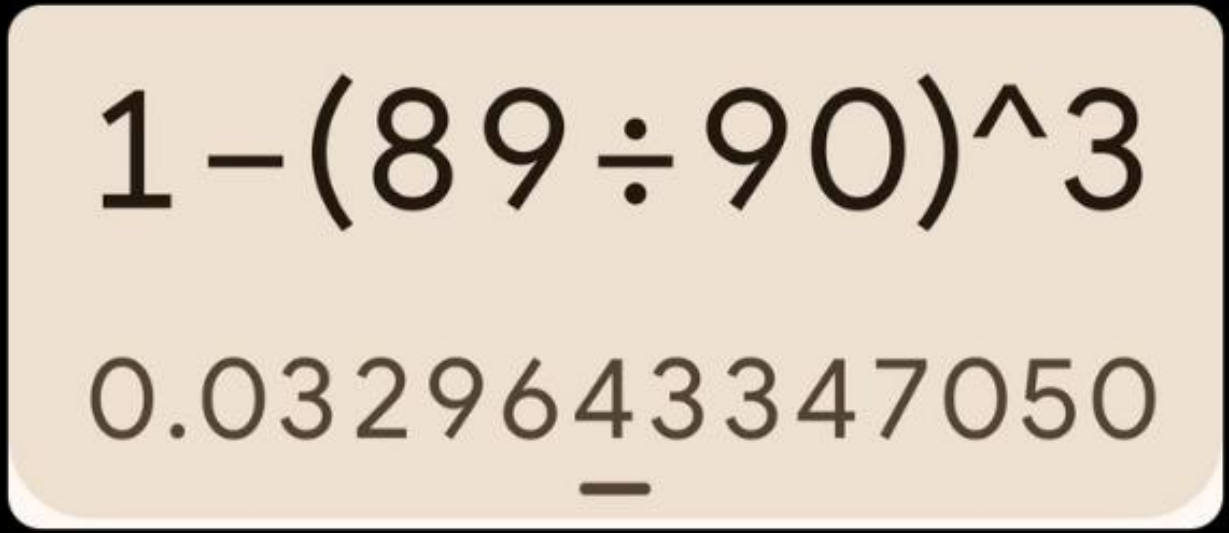




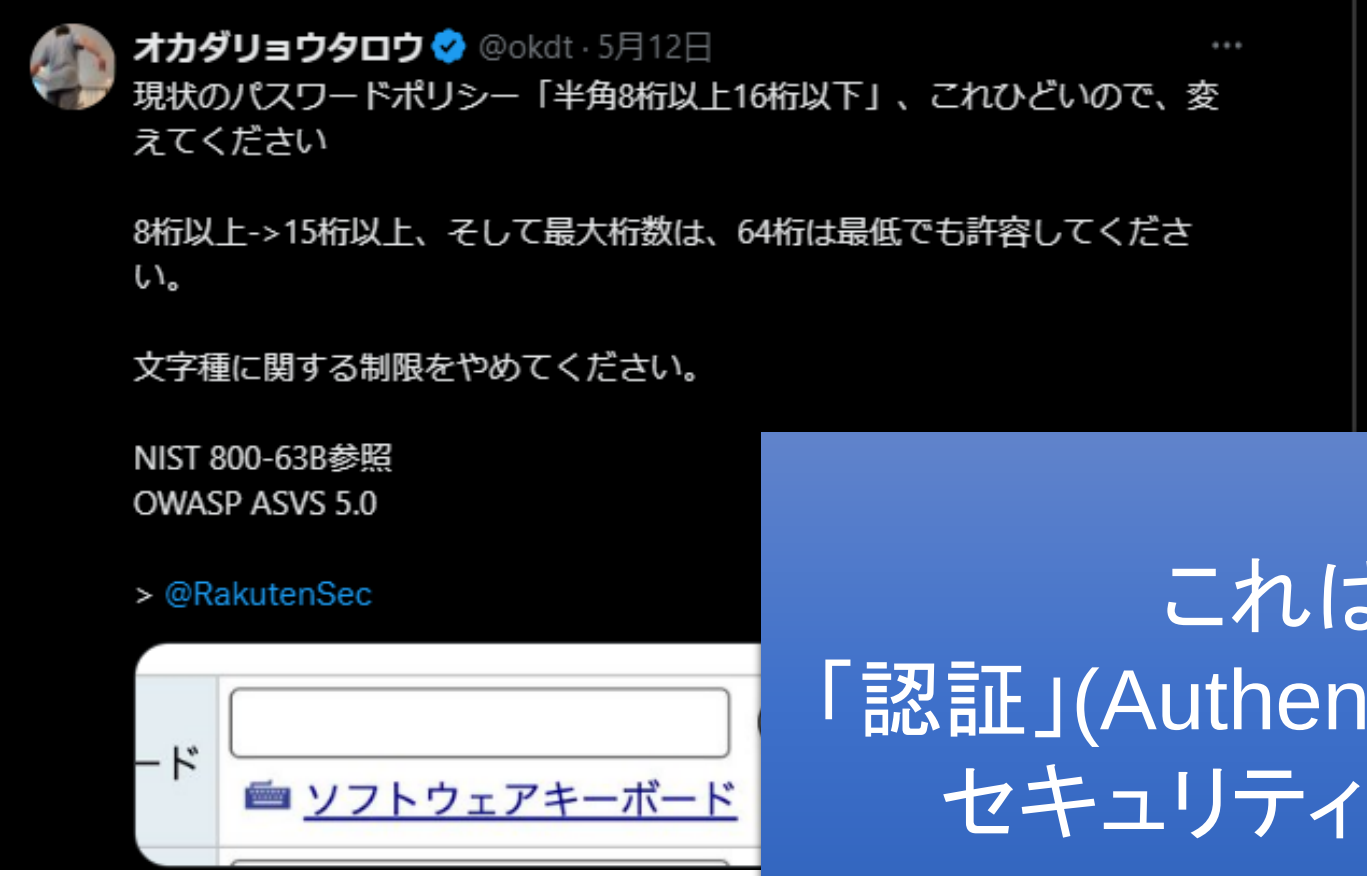
100 531 1,031 28万

よこちょ｜"損しない"優待株の選び方
@yokocho_yutai

これでも3%以上の確率で突破できちゃうんだよな...



午後6:16 · 2025年5月12日 · **1.1万** 件の表示



これは
「認証」(Authentication)で
セキュリティの範疇

情報の流通とその課題

- (先に本件に関する余談)
  - 認証機能を後から直すのは本当に大変なので、設計はきちんと専門家に任せましょう
  - …専門家の数が全く足りてないという問題は忘れることにします

- これは攻撃すべき優先順位評価の情報になっている
- 一方、犯罪になると情報に統制がかかる
  - これは仕方がないこと
  - だが…

実害があったかは不明だが、日経新聞が攻撃手法を対策より先に報道したケース等もある

デジタルアイデンティティ的にはどうか？

- そもそも『本人確認(身元確認・当人認証)は難しい』
- そしてその上に『どんどん難しくなっている』

- 業法的には、「犯罪収益移転防止法」と「携帯電話不正防止法」が代表的だが、他にもいわゆる「本人確認」を必要とするものは多々存在する
- (銀行)口座が安全に作られていればかなり問題は解決する
  - オンライン化とか進めるからいけないんだ！☺ (「デジタル」の課題)
- 個別事例をここで上げるのは忍びないので割愛するが、長年アイデンティティ領域にかかわる中で、日々の本人確認の杜撰さには、正直目を覆うばかりである (特に身元確認)

身元確認の難しさ (一部)

- 本人確認書類の偽造対策の訓練等はどうなっているのか
  - 銀行窓口ではトレーニングがあると聞くが(未確認です)、
    本来資格であってもおかしくないレベル
- 女性の容貌確認の難しさ (性的差別の意図ではなく文化の話です)
  - 「特定の人物になるのは難しいけど、自分でない誰かになるのは簡単」
    (化粧をする複数女性(プロ含む)からのヒアリング)
  - 化粧なしを条件にしている身分証明書の写真から、化粧している人を本当に見分けられるか？
- 近年ではマスクの問題も
- 良い身分証明書は、身元確認が難易度が高く対面を要求するケースも多いことから、結果的に寿命が長いものが多い
  - (という矛盾的状況)
  - 結果的に、容貌の変化に追従しにくいという欠点がある

今までの本人確認(身元確認・当人認証)

身元確認	・利用開始時(登録)	・本人確認書類 ・写真付き？ 対面？ ・メールアドレスとパスワード？
当人認証	・利用時	・ID/Password (記憶できるレベルのもの)

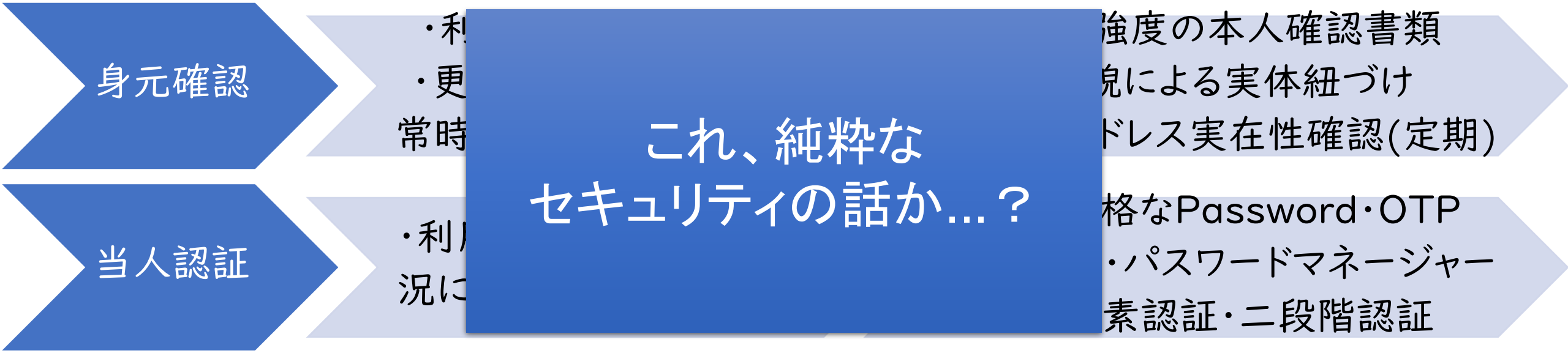
- 時間的連続性のない『断面での確認行為』

現在の本人確認(身元確認・当人認証)

身元確認	・利用開始時は入念に ・更に開始時だけでなく 常時継続・リスクベースで	・高い強度の本人確認書類 ・容貌による実体紐づけ ・メールアドレス実在性確認(定期)
当人認証	・利用時はUXを考慮し状 況に応じた強度で動的に	・ID/厳格なPassword・OTP ・パスキー・パスワードマネージャー ・多要素認証・二段階認証

- 『継続的な身元確認と当人認証・リスクベースでの常時評価』
- いわゆるOngoing KYCとContinuous Authentication
- B2Cの方がB2B(Enterprise)よりも進んでいる

現在の本人確認(身元確認・当人認証)



- 『継続的な身元確認と当人認証・リスクベースでの常時評価』
- いわゆるOngoing KYCとContinuous Authentication
- B2Cの方がB2B(Enterprise)よりも進んでいる

IDそしてDigital Identityとは？

『アイデンティティ』

日本人は大体何故か「アイデンティティ」という単語を知っている

でも、それを明確に言語化できますか？

日本語難しい

- 突然ですが「カタカナ」というのは素晴らしい文化
  - 「アイデンティティ」と記述し発音し扱うことが出来る
- 日本語は往々にして多義的
  - すぐいろいろなものが混ざる (混ぜるな危険)
- センスのある訳語とセンスのない訳語
  - 『認証』"Authentication" ? "Certification" ?
  - 『信頼』"Trust" ? "Confidence" ? "Reliance" ? "Faith" ? "Dependence" ? "Credence" ? "Assurance" ? "Reliability" ?
- 訳語っぽいのを見たら原語を想像するようにすると良い
  - 特にBuzz Wordっぽい奴とか!

アイデンティティ：Identity

Identity

- ID+Entity.....ではない(らしい)
- IDは略語

Digital Identity、例えば…

法人	個人	(家族)
National ID	to Consumer	for Enterprise

ID...???

Identity Document:
身分証明書

IDentifier:
識別子

Identity etc...

Identity:　　自己像 (??)

- ペルソナ、等...

Identification:　　識別

- 対象と他の違いを認識して区別する行為

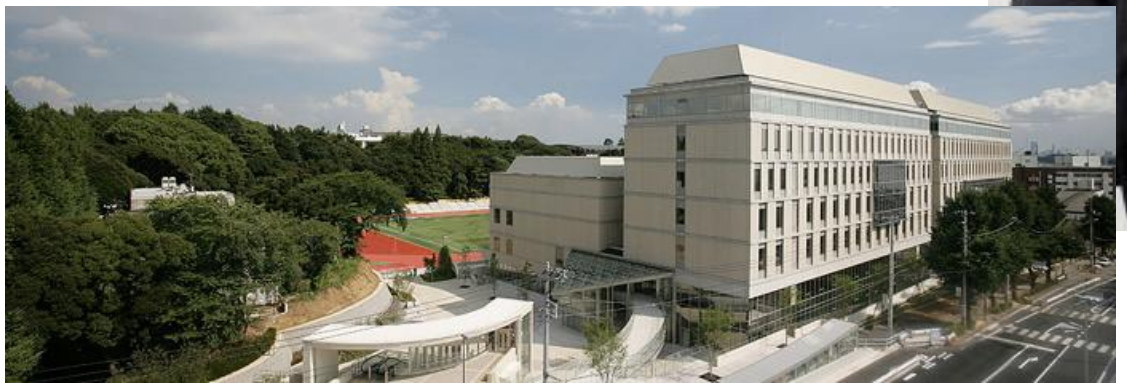
Identifier:　　識別子(ID)

- 識別に使う情報
- 結果的に、ひとつの体系の中ではユニークであることが想定される

Identity Proofing:　　身元確認

- 識別・特定する為の元となる実体(Entity)の確認行為

実体 / Entity



属性 / Attribute

- 慶應義塾大学 大学院 メディアデザイン研究科
  後期博士課程 (大学院生)
- 非常勤国家公務員
- 企業役員
- 元OpenID Foundation Japan理事
- アイデンティティおっさん
- 50代前半
- テックスタートアップ

属性 / Attribute

- 慶應義塾大学
  後期博士課程
- 非常勤国家公
- 企業役員
- 元OpenID Foundation Japan理事
- アイデンティテ
- 50代前半
- テックスタート

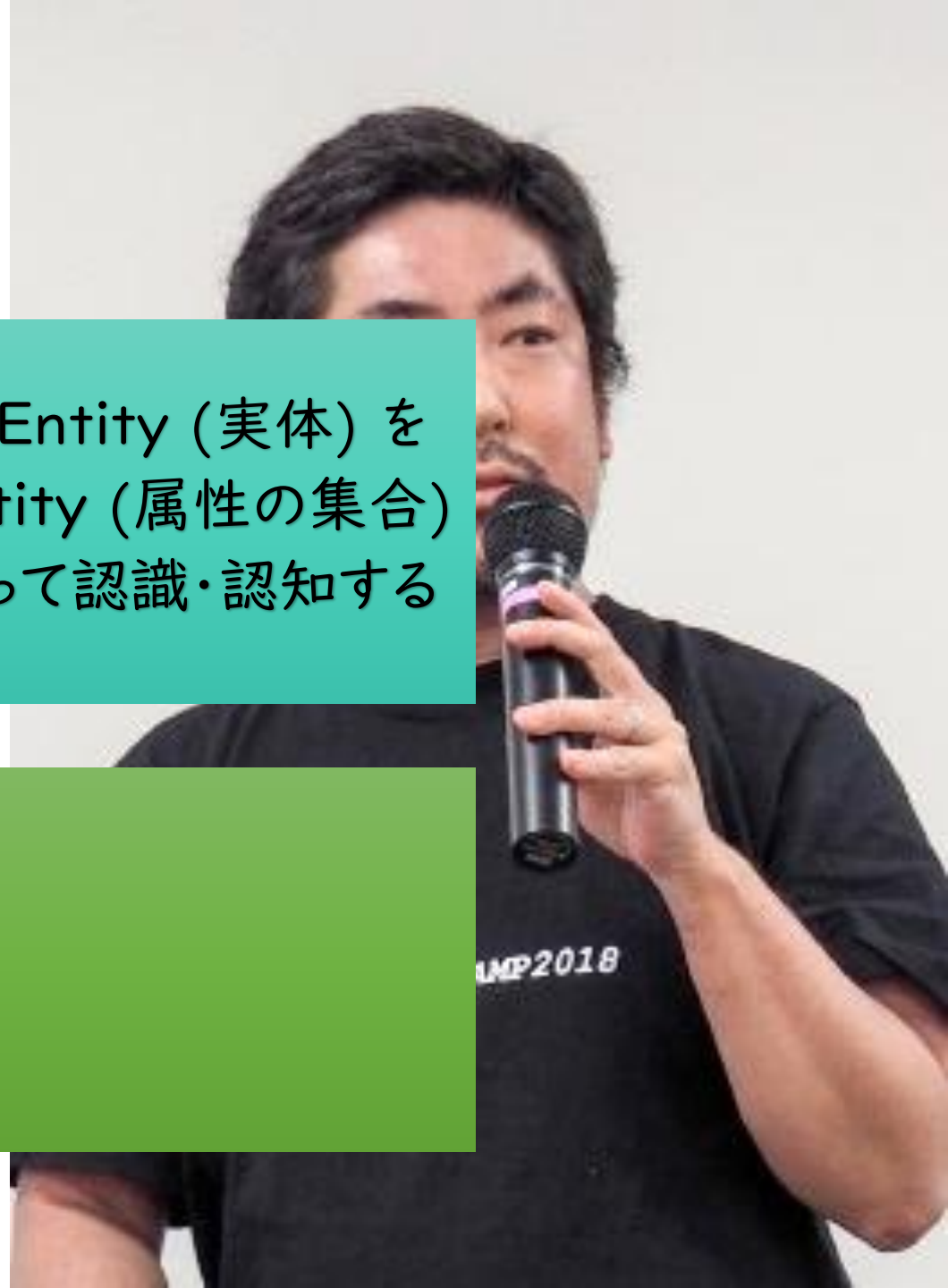
Identity = 属性の集合 (ISO/IEC 24760)

属性 / Attribute

- 慶應義塾大学
  後期博士課程
- 非常勤国家公
- 企業役員
- 元OpenID Foundation Japan理事
- アイデンティテ
- 50代前半
- テックスタート

Identity = 属性の集合 (ISO/IEC 24760)

人はEntity (実体) を Identity (属性の集合) によって認識・認知する



属性 / Attribute

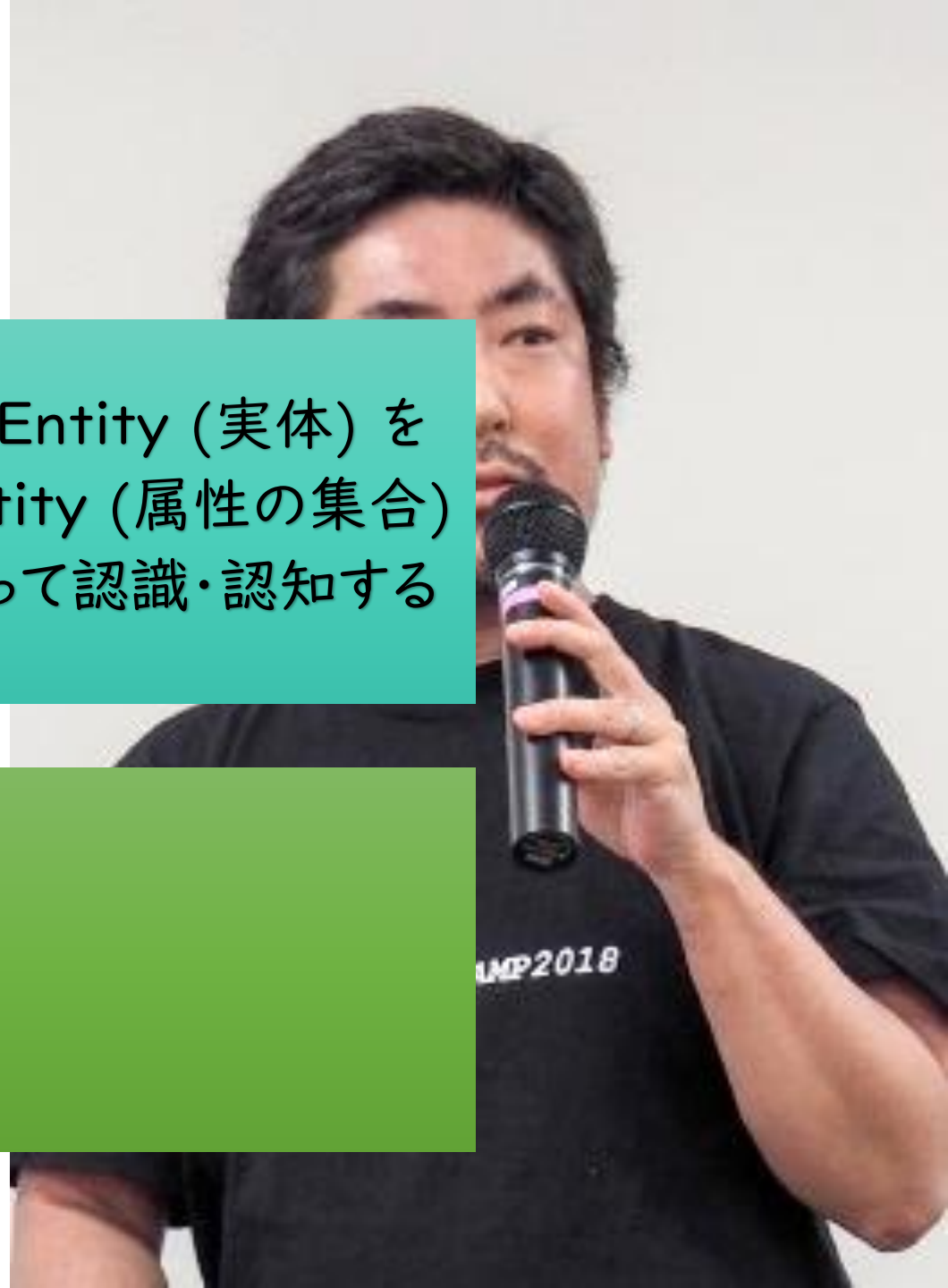
- 慶應義塾大学
  後期博士課程
- 非常勤国家公
- 企業役員
- 元OpenID Foundation Japan理事
- アイデンティテ
- 50代前半
- テックスタート

Identity = 属性の集合 (ISO/IEC 24760)

人はEntity (実体) を Identity (属性の集合) によって認識・認知する

1つのEntityに

Identityは複数存在



属性 / Attribute

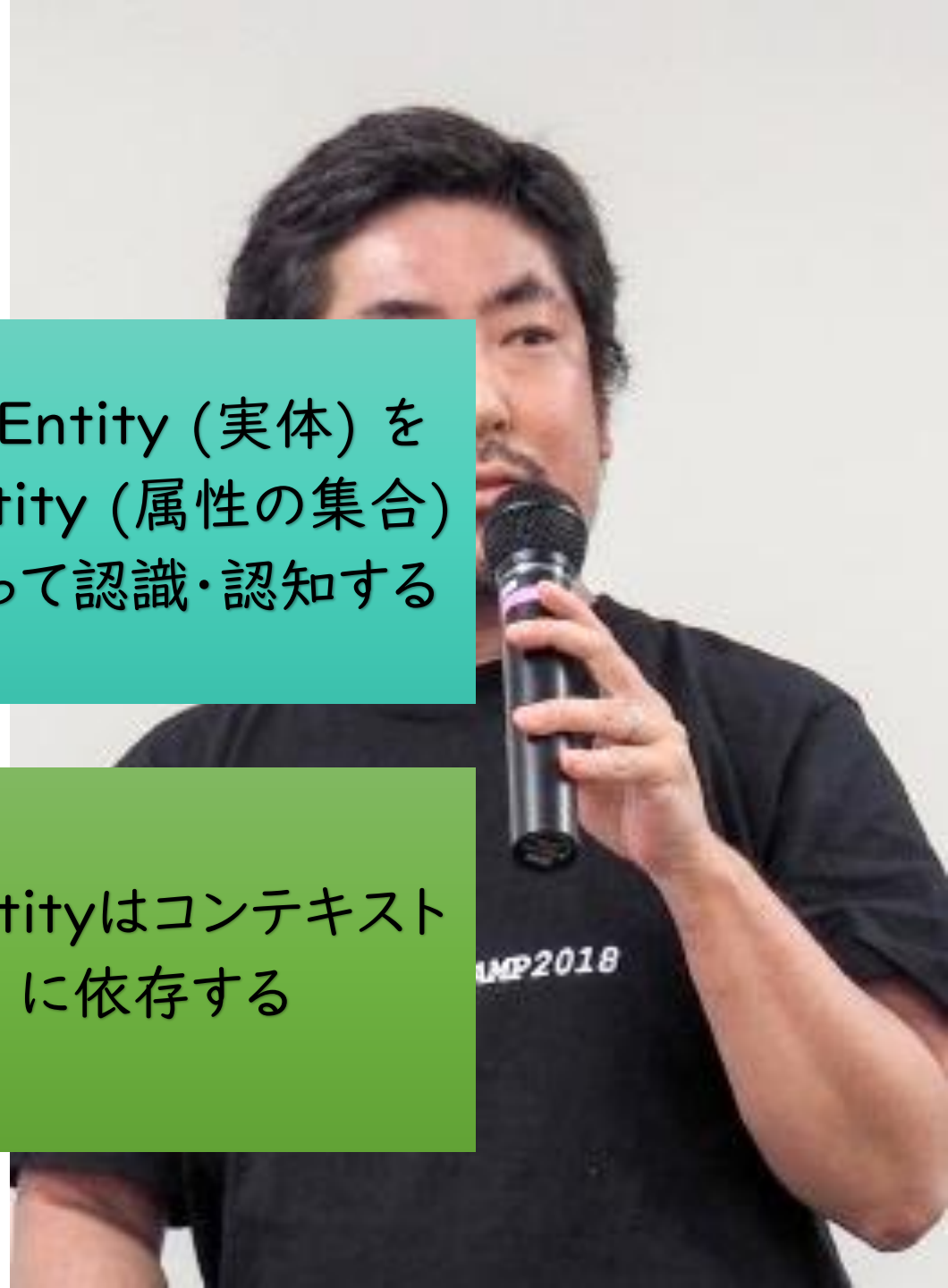
- 慶應義塾大学
  後期博士課程
- 非常勤国家公
- 企業役員
- 元OpenID Foundation Japan理事
- アイデンティテ
- 50代前半
- テックスタート

Identity = 属性の集合 (ISO/IEC 24760)

人はEntity (実体) を Identity (属性の集合) によって認識・認知する

1つのEntityに Identityは複数存在

Identityはコンテキストに依存する



さて、この話と情報システムの関係は？

- アイデンティティマネジメント(IdM)という単語のいい加減さ
  - アカウントマネジメントのことだと思っていませんか？
  - 認証情報管理でもないはずなんですよ？
  - (少ししっかりしているとデバイスマネジメントまで視野に入っているかも)
- X.500/509の罪、LDAPの嘘
  - 未だにこの呪い・呪縛から逃れられていない人は多い
    - PKIの罪の詳細は、長くなる上に戦争になるので今日は許してください☺
  - 冷静に考えればDirectory Serviceは属性の集合ではあるが…

さて、この話と情報システムの関係は？

- アイデンティティマネジメント(IdM)という単語のいい加減さ
  - アカウントマネ…か？
  - 認証情報管理…
  - (少ししっかり…で視野に入っているかも)
- X.500/509の…
  - 未だにこの呪い・呪縛から逃れられていない人は多い
    - PKIの罪の詳細は、長くなる上に戦争になるので今日は許してください☺
  - 冷静に考えればDirectory Serviceは属性の集合ではあるが…

デジタルアイデンティティは
デジタル環境で人やモノを
どう扱うかの為の概念

デジタルアイデンティティに関する文書

- ISO/IEC 29115: "Entity authentication assurance framework"
  - ITU-T X.1254: "Entity authentication assurance framework"
- NIST SP800-63-3 "Digital Identity Guidelines"
  - OIDF-Jによる翻訳版あり
- NIST SP800-63-4 Initial Public Draft
  - OIDF-Jによる翻訳版あり
- NIST SP800-63-4 Second Public Draft
- DS-500 デジタル庁「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」(2019版)
  - 現在、改定作業中(202x版)

必読書籍

- 「デジタルアイデンティティー 経営者が知らないサイバービジネスの核心」
  - 崎村 夏彦 (著)
  - https://www.amazon.co.jp/dp/4296109901
- 「デジタルアイデンティティのすべて」
  - Phil Windley「Learning Digital Identity」訳書
  - 富士榮尚寛 (監訳)
  - 柴田健久、花井杏夏、宮崎貴暉、塚越雄登、田島太朗、名古屋謙彦、村尾進一、瀬在翔太、松本優大、安永未来、池谷亮平 (訳)
  - https://www.amazon.co.jp/dp/4814400985

デジタル庁 DS-500

行政手続におけるオンラインによる本人確認の手法に関するガイドライン (2019)

- SP800-63-3(Draft)ベース
  https://www.digital.go.jp/resources/standard_guidelines#ds500

行政手続におけるオンラインによる本人確認の手法に関するガイドライン (202x)

- 現在改定作業中: おそらくSP800-63-3から4への論点整理では1番まとまっている
- 令和6年度版の「改定に向けたとりまとめ」は、単にNIST SP800-63に囚われず、日本の動向に合わせてより良い改善がなされている (ページ数とか!)
  - 「改定に向けたとりまとめ（令和6年度（2024年度））」
  - 「改定に向けた中間とりまとめ（令和5年度（2023年度））」
  - 「改定に向けた中間とりまとめ（令和4年度（2022年度））」

デジタル庁 DS-500

行政手続におけるオンラインによる本人確認の手法に関するガイドライン (2019)

- SP800-63-3(Draft)ベース
  https://www.digital.go.jp/resources/standard_guidelines#ds500

行政手続におけるオンライ…イドライン (202x)

- 現在改定作業中: おそ…理では1番まとまっている
- 令和6年度版の「改定…P800-63に囚われず、日本の動向に合わせて…ジ数とか!)
  - 「改定に向けたとりまとめ（令和6年度（2024年度））」
  - 「改定に向けた中間とりまとめ（令和5年度（2023年度））」
  - 「改定に向けた中間とりまとめ（令和4年度（2022年度））」

これはあくまで
「行政手続きにおける」
ガイドラインです
(と言いつつ民間も大いに
参考にするのですが)

とりまとめより

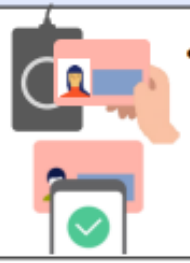
本人確認ガイドラインの主要な改定ポイント

1章 はじめに	**① ガイドラインの適用対象と名称の見直し** • デジタルによる本人確認の機会がオンラインだけでなく対面にも拡大していることなどを踏まえ、対面の本人確認も適用対象に含める。これにあわせてガイドライン名称も変更する。
	② 検討にあたる「基本的な考え方」を定義 • 対象とする手続等の特性に応じた手法が選択できるよう、「事業目的の遂行」「公平性」「プライバシー」「ユーザビリティ及びアクセシビリティ」「セキュリティ」の5つの観点から「基本的な考え方」を定義。
2章 本人確認の枠組み	**③ 本人確認の基本的な枠組みを定義** • 身元確認や当人認証などの基本概念を説明する2章を新設し、「フェデレーション」の概念を新たに盛り込む。さらに、本人確認の実装モデルとして「連携モデル」及び「非連携モデル」を定義する。
3章 本人確認における 脅威と対策	**④ 脅威と対策の最新化、保証レベルの見直し** • 国内外の脅威の動向、最新の技術動向、米国NIST SP 800-63-4（2pd）での改定内容等を踏まえ、身元確認、当人認証及びフェデレーションにおける想定脅威と手法例を最新化する。 • 身元確認保証レベル及び当人認証保証レベルの位置づけと対策基準を脅威への耐性の観点から見直す。
4章 本人確認手法の 検討方法	**⑤ リスク評価プロセスの全面的な見直し** • 「基本的な考え方」の5つの観点から採用する手法の評価、調整、例外措置の検討等を行うプロセスを追加する。あわせて複雑な判定フローは廃止し、保証レベル判定までのプロセスをできる限り単純化する。

とりまとめより

身元確認保証レベルの見直し　―　全体概要

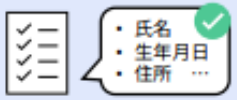
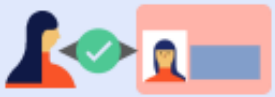
- 昨今の脅威動向を踏まえ、身元確認保証レベルは「ICチップ等によるデジタル的な検証の有無」を、保証レベルの差として表現できるように改定する。また低リスクの手続・サービス向けの保証レベルとして「レベル1」を定義※する。（※現行ガイドラインの「レベル1」は「身元確認なし」の位置づけであったが、今回の改定で簡易的な身元確認を行うレベルとして再定義する。）

保証レベル	保証レベルの位置づけ	
	本人確認書類の検証手法	申請者の検証手法
身元確認 保証レベル3	 ・ICチップ等による**デジタル的な検証を必須**とし、**偽造や改ざんに対する厳格な耐性**を確保するレベルとする。 （「デジタル的な検証」：発行者によって付与されたデジタル署名等による暗号学的な検証を行うこと。）	 ・本人確認書類の盗用に対し、**容貌の確認**又は**暗証番号による検証**を必須とする。 **暗証番号:** ＊＊＊＊ ・本人確認書類の貸し借りに対しては、対象手続のリスクに応じた個別検討※を行うこととする。 ※ 暗証番号のみでは本人確認書類の貸し借りを検知できないため、貸し借りのリスクを許容できない場合は「容貌の確認」の追加実施等を検討する。
身元確認 保証レベル2	 ・本人確認書類の**物理的な券面の検査等も許容**する。ただし検証強度を考慮しカメラ越しや複写物による検査（非対面での券面検査）は不可とし、一定の耐性を確保する。	
身元確認 保証レベル1	 ・保証レベル2までの手法に加えて、**非対面での券面検査（カメラでの撮影、複写物の郵送等）も許容**する。偽造・改ざんへの簡易的な耐性をもつレベルとして位置付ける。	 ・保証レベル2までの手法に加えて、**本人確認書類に記載された住所等に確認コードを送付することでの間接的な検証**も許容する。 （例：当該住所に居住していることをもって、本人確認書類との紐づきを確認する 等）

とりまとめより

身元確認保証レベルの見直し　―　各レベルの対策基準

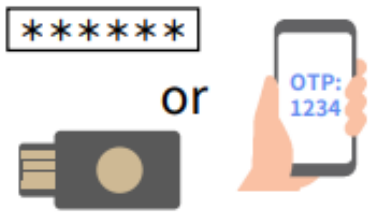
- 前述の「位置づけ」に基づき、各レベルの対策基準を以下のとおり定義する方針とする。
  ※対策基準はあくまで基準であり、同等の脅威耐性を確保できる場合は他の手法等により代替してもよいものとして定義する。

保証レベル	対策基準（青字：上位レベルとの相違点）		
	属性情報の収集 	**本人確認書類の検証** 	**申請者の検証** 
身元確認保証レベル3	本人確認書類の電子的な読取り	デジタル署名の検証	以下のいずれか • 容貌の確認（対面） • 容貌の確認（非対面） • 暗証番号等による検証
身元確認保証レベル2	（収集手法は任意とする）	以下のいずれか • デジタル署名の検証 • **信頼できる情報源への照会** • **券面の物理的検査（対面）**	
身元確認保証レベル1	（収集手法は任意とする）	以下のいずれか • デジタル署名の検証 • 信頼できる情報源への照会 • 券面の物理的検査（対面） • **券面の物理的検査（非対面）**	以下のいずれか • 対面での容貌確認 • 非対面での容貌確認 • 暗証番号等による検証 • **確認コードの送付による検証**

とりまとめより

当人認証保証レベルの見直し

- 当人認証保証レベルについては大幅な変更は行わないが、フィッシング攻撃など最新の脅威動向、技術動向、国民向けの行政手続等において想定されるリスク等を考慮し、脅威耐性の観点から各レベルの対策基準を一部見直す。

保証レベル	対策基準	
	認証要素	脅威への耐性要件
当人認証 保証レベル3	**「公開鍵暗号に基づく認証器」を含む多要素認証** 例） • 暗証番号付きのICカード • パスキー 	• **フィッシング耐性（必須）** 「必須」：全ての利用者に対してフィッシング耐性をもつ認証方式を適用する ＋ • 保証レベル2の耐性
当人認証 保証レベル2	**多要素認証** 例） • 暗証番号付きのICカード • パスキー • パスワード ＋ワンタイムパスワード 	• **フィッシング耐性（推奨）** 「推奨」：フィッシング耐性をもつ認証方式を利用者に対して提供し、その利用を推奨するが、他の認証方式についても選択可能とする • **認証器等の盗用に対する耐性** ※ICカードやパスワード等の認証要素のうち一つが盗用された場合の耐性 ＋ • 保証レベル1の耐性
当人認証 保証レベル1	**単要素認証**（又は多要素認証） 例） • パスワード • ワンタイムパスワード • USB接続型セキュリティキー • 又は保証レベル2以上の手法 	• 盗聴 • リプレイ攻撃 • オンライン上での認証情報の推測

犯罪対策閣僚会議「国民を詐欺から守るための総合対策」のとりまとめについて

公開日:2024年6月21日

「パスキー」や「DMARC」等、具体的に技術名が出てくる踏み込んだ内容

令和6年（2024年）6月18日、総理大臣官邸で第39回犯罪対策閣僚会議が行われ、「国民を詐欺から守るための総合対策」がとりまとめられました。
総合対策では、マイナンバーカードに関連した施策として、マイナンバーカードのICチップを活用し、確実に本人確認を行い犯罪を防止する、以下の内容が盛り込まれました。

- 携帯電話や電話転送サービスの契約時の本人確認において、本人確認書類の券面の偽変造による不正契約が相次いでいることから、犯罪収益移転防止法、携帯電話不正利用防止法に基づく非対面の本人確認手法を、マイナンバーカードの公的個人認証に原則として一本化し、対面においても、マイナンバーカード等のICチップ情報の読み取りを義務付ける。
- マッチングアプリアカウントを悪用し、利用者を信用させるなどして、詐欺被害につながっている事案が確認されていることから、マッチングアプリ事業者に対し、アカウントの開設時に公的個人認証サービス等による、より厳密な本人確認を実施するなど、自主的な不適正利用対策に取り組むよう働き掛ける。

犯罪対策閣僚会議では『いわゆる「闇バイト」による強盗事件等から国民の生命・財産を守るための緊急対策』を踏まえて令和7年4月22日に取り組み状況と共に2.0に更新されている

参考資料

- 国民を詐欺から守るための総合対策（本文）
- 犯罪対策閣僚会議 | 首相官邸ウェブサイト

「国民を詐欺から守るための総合対策2.0」からの引用・抜粋

- 3「ID・パスワード等の窃取・不正利用対策」(目次より抜粋)
  - (2) ID・パスワードやクレジットカード情報の不正入手対策
    - ア フィッシングサイトに誘導するメールやSMSへの対策
      - (ｳ) 送信ドメイン認証技術（DMARC等）への更なる対応促進<再掲> 2⑵イ(ｲ) (P.21)
    - イ ID・パスワード等の窃取対策
      - (ｱ) パスキーの普及促進 (P.21)

https://www.kantei.go.jp/jp/singi/hanzai/kettei/240618/honbun.pdf より

「国民を詐欺から守るための総合対策2.0」からの引用・抜粋

- (ウ) パスキーの普及促進
  - 総合対策において、次世代認証技術の１つであるパスキーの普及のため、金融機関やEC事業者等の事業を所管する省庁に対して、その導入等の促進を要請し、同要請を踏まえ、関係省庁から所管する事業者等へ各種要請を行っているところ、フィッシングによる被害の中には、送金時等の二段階認証に必要なSMS認証コードをリアルタイムに盗み取って行う手口が発生していることから、引き続き、関係省庁と連携し、関係事業者等が参加する各種講演会等の機会を捉え、パスキーの有用性について説明を行うなど、その普及に向けた取組を実施する。

https://www.kantei.go.jp/jp/singi/hanzai/kettei/250422/honbun-1.pdf より

「犯罪による収益の移転防止に関する法律施行規則の一部を改正する命令案」に対する意見の募集について

令和9年4月1日施行

要はいわゆる「ホ方式」の廃止

e-GOV パブリック・コメント

トップ | パブリック・コメント制度について | 案件一覧 | ヘルプ

トップ ＞ 案件一覧 ＞ 「犯罪による収益の移転防止に関する法律施行規則の一部を改正する命令案」に対する意見の募集について

「犯罪による収益の移転防止に関する法律施行規則の一部を改正する命令案」に対する意見の募集について

受付締切

facebook (旧Twitter)

※この案件については、すでに意見募集は終了していますので、意見・情報の提出はできません。

カテゴリー	警察
案件番号	120250002
定めようとする命令などの題名	犯罪による収益の移転防止に関する法律施行規則の一部を改正する命令
根拠法令条項	犯罪による収益の移転防止に関する法律（平成19年法律第22号）第４条第１項及び第２項（これらの規定を同条第５項の規定により読み替えて適用する場合を含む。）並びに第４項並びに第６条第１項
行政手続法に基づく手続か	行政手続法に基づく手続

案の公示日	2025年2月28日
受付開始日時	2025年2月28日0時0分
受付締切日時	2025年3月29日23時59分
意見提出が30日未満の場合その理由	

意見募集要領（提出先を含む）	意見公募要領 PDF 意見公募要領別紙 PDF
命令などの案	【案文】犯罪による収益の移転防止に関する法律施行規則の一部を改正する命令案 PDF
関連資料、その他	
資料の入手方法	警察庁情報公開室にて閲覧可能
備考	
問合せ先（所管省庁・部局名等）	警察庁刑事局組織犯罪対策部組織犯罪対策第一課 電話：03-3581-0141 (内線4492)

戻る

生成AIと文書偽造

EXPERT USED CHATGPT-4O TO CREATE A REPLICA OF HIS PASSPORT IN JUST 5 MINUTES BYPASSING KYC

Pierluigi Paganini April 06, 2025

A researcher used ChatGPT-4o to create a replica of his passport in just five minutes, realistic enough to deceive most automated KYC systems.

https://securityaffairs.com/176224/security/chatgpt-4o-to-create-a-replica-of-his-passport-in-just-five-minutes.html
https://x.com/01ra66it/status/1908803056374030765

「情報システムにおける」EntityとIdentityの関係

ISO/IEC 24760-1:2019 から引用

3.1 General terms

- 3.1.1 entity
  - item relevant for the purpose of operation of a domain (3.2.3) that has recognizably distinct existence
  - Note 1 to entry: An entity can have a physical or a logical embodiment.
  - EXAMPLE:A person, an organization, a device, a group of such items, a human subscriber to a telecom service, a SIM card, a passport, a network interface card, a software application, a service or a website.
- 3.1.2 identity / partial identity
  - set of attributes (3.1.3) related to an entity (3.1.1)
  - Note 1 to entry: An entity can have more than one identity.
  - Note 2 to entry: Several entities can have the same identity.
  - Note 3 to entry: ITU-T X1252[13] specifies the distinguishing use of an identify. In this document, the term identifier implies this aspect.
- 3.1.3 attribute
  - characteristic or property of an entity (3.1.1)
  - EXAMPLE:An entity type, address information, telephone number, a privilege, a MAC address, a domain name are possible attributes.
- 3.1.4 identifier
  - attribute or set of attributes (3.1.3) that uniquely characterizes an identity (3.1.2) in a domain (3.2.3)
  - Note 1 to entry: An identifier can be a specifically created attribute with a value assigned to be unique within the domain.
  - EXAMPLE:A name of a club with a club-membership number, a health insurance card number together with a name of the insurance company, an email address, or a Universal Unique Identifier (UUID) can all be used as identifiers. In a voter's register, the combination of attributes name, address and date of birth is sufficient to unambiguously distinguish a voter.

ISO/IEC 24760-1:2019(Google翻訳)

3.1 一般用語

- 3.1.1 エンティティ
  - ドメイン (3.2.3) の運用目的に関連する、認識可能な明確な存在を持つアイテム
  - エントリの注記 1: エンティティは、物理的または論理的な形態を持つことができます。
  - 例: 人、組織、デバイス、そのようなアイテムのグループ、通信サービスの加入者、SIM カード、パスポート、ネットワーク インターフェイス カード、ソフトウェア アプリケーション、サービス、または Web サイト。
- 3.1.2 アイデンティティ / 部分的なアイデンティティ
  - エンティティ (3.1.1) に関連する属性の集合 (3.1.3)
  - エントリの注記 1: エンティティは、複数のアイデンティティを持つことができます。
  - エントリの注記 2: 複数のエンティティが同じアイデンティティを持つことができます。
  - エントリの注記 3: ITU-T X1252は、アイデンティティの区別的な使用を規定しています。このドキュメントでは、識別子という用語はこの側面を意味します。
- 3.1.3 属性
  - エンティティ (3.1.1) の特性またはプロパティ
  - 例:エンティティ タイプ、アドレス情報、電話番号、特権、MAC アドレス、ドメイン名は、属性として考えられます。
- 3.1.4 識別子
  - ドメイン (3.2.3) 内の ID (3.1.2) を一意に特徴付ける属性または属性セット (3.1.3)
  - エントリの注記 1: 識別子は、ドメイン内で一意になるように割り当てられた値を持つ、特別に作成された属性です。
  - 例:クラブ名とクラブ会員番号、健康保険証番号と保険会社名、電子メール アドレス、またはユニバーサル ユニーク識別子 (UUID) はすべて、識別子として使用できます。有権者名簿では、名前、住所、生年月日の属性の組み合わせで、有権者を明確に区別できます。

ISOにおけるidentityの定義(英日)を修文

- アイデンティティ
  - エンティティに関連する属性の集合
    - エントリの注記 1: エンティティは、複数のアイデンティティを持つことができます。
    - エントリの注記 2: 複数のエンティティが同じアイデンティティを持つことができます。
    - エントリの注記 3: ITU-T X1252[13] は、アイデンティティの区別的な使用を規定しています。このドキュメントでは、識別子という用語はこの側面を意味します。
- identity
  - set of attributes related to an entity
    - Note 1 to entry: An entity can have more than one identity.
    - Note 2 to entry: Several entities can have the same identity.
    - Note 3 to entry: ITU-T X1252[13] specifies the distinguishing use of an identity. In this document, the term identifier implies this aspect.

ISOにおけるidentityの定義(英日)を修文

- アイデンティティ
  - エンティティに関連する属性の集合
    - エントリの注記 1:
      数のアイデンティ
      きます。
    - エントリの注記 2:
      ティが同じアイデ
      ができます。
    - エントリの注記 3:
      X1252[13]は、
      区別的な使用を対
      ドキュメントでは、識別子という用語は
      この側面を意味します。

- identity
  - set of attributes related to an entity
    - ntry: An entity can
      han one identity.
    - ntry: Several
      have the same
    - ntry: ITU-T
      specifies the
      ng use of an
      this document, the
      term identifier implies this
      aspect.

『エンティティに関連する属性の集合』=
『アイデンティティ』

ISOにおけるidentityの定義(英日)を修文

- アイデンティティ
  - エンティティに関連する属性の集合
    - エントリの注記 1:
      数のアイデンティ
      きます。
    - エントリの注記 2:
      ティが同じアイデン
      ができます。
    - エントリの注記 3:
      X1252[13]は、
      区別的な使用を
      ドキュメントでは、
      この側面を意味します。

- identity
  - set of attributes related to an entity
    - try: An entity can
      an one identity.
    - try: Several
      have the same
    - try: ITU-T
      pecifies the
      g use of an
      his document, the
      er implies this
      aspect.

めちゃくちゃシンプル

デジタル社会とデジタルアイデンティティ

- 社会のデジタル化に合わせて我々もデジタル化していっている(既に)
  - @lef も明らかに自分のアイデンティティ
- 精緻なbitの制御によって、システム＝「系」に上においては、アイデンティティはシンプルに定義出来る

- デジタル社会と物理社会との違いは、実は大きい
  - プライバシーは明らかにデジタル社会のせいで侵害の度合いを大きくした
  - まだまだ未成熟で混沌とした世界
- もしアカウントがBanされたら
  - その領域での人権が失われるに等しい

デジタルアイデンティティを取り巻く動向

OECD Recommendation of the Council on the Governance of Digital Identity(2023)

OECD.org Data Publications **OECD Legal Instruments** More sites News Job vacancies

OECD Legal Instruments

Login

Home About Full list Advanced search Adherences Key figures FR

OECD/LEGAL/0491
Adopted on:
08/06/2023

Text
Background information
Related document(s)
Committee(s)
Date(s)/Reference(s)
Related instrument(s)
Adherents

Download/Print Booklet
Share Link

Recommendation of the Council on the Governance of Digital Identity

In force Recommendation Governance; Science and Technology

THE COUNCIL,

HAVING REGARD to Article 5 b) of the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960;

HAVING REGARD to the standards developed by the OECD in the area of electronic authentication, regulatory policy and governance, agile regulatory governance, international regulatory co-operation, protection of privacy and transborder flows of personal data, cross-border co-operation in the enforcement of laws protecting privacy, digital government strategies, cryptography policy, internet policy making, digital security, children in the digital environment, and open government;

HAVING REGARD to the technical standards developed by other fora, such as the European Committee for Standardization (CEN), European Telecommunications Standards Institute (ETSI), the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the United States National Institute of Standards and Technology (NIST) and the World Wide Web Consortium (W3C), as well as related work undertaken by the European Commission, the Financial Action Task Force (FATF), the United Nations Commission on International Trade Law (UNCITRAL), and the World Bank;

RECOGNISING that effective, usable, secure and trusted digital identity systems can enhance privacy, facilitate inclusion and simplify access to a wide range of services, and thereby contribute to social and economic value;

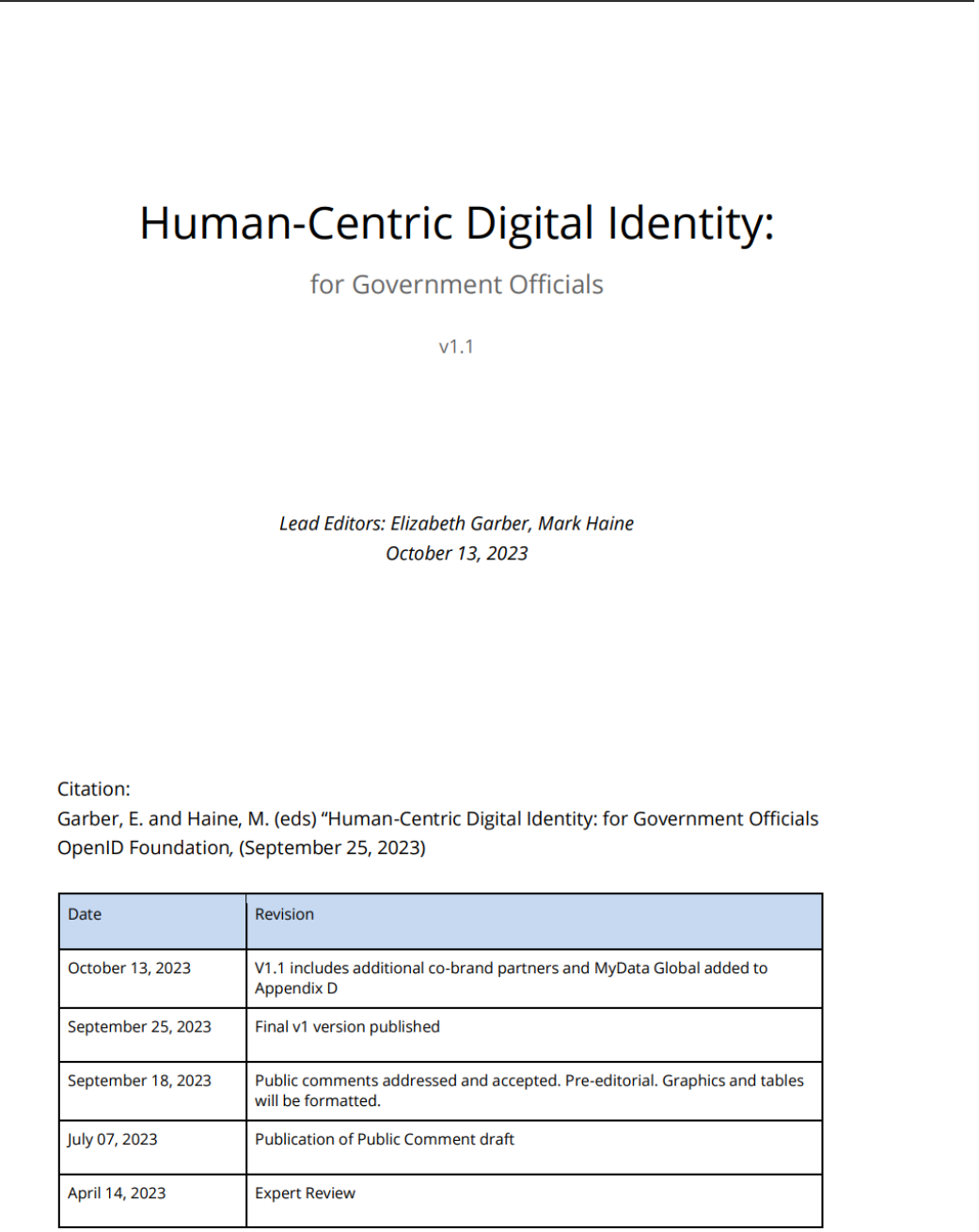
RECOGNISING that digital identity can transform the way service providers operate and interact with their users, both in-person and online, by providing an optional alternative to physical credentials as part of a seamless omni-channel experience;

RECOGNISING that the governance, design and implementation of digital identity systems should be rooted in democratic values and respect for human rights;

RECOGNISING the need to ensure the accessibility, affordability, usability, and equity of digital identity solutions for all, continually promoting the inclusion of vulnerable groups and minorities;

RECOGNISING that the rapidly evolving technology landscape creates the need for governments to regularly evaluate and assess the opportunities and risks of new technologies and architectural paradigms, including cost-benefit analyses as well as environmental, privacy, data protection, ethical and human rights impact assessments, complemented by open and transparent processes for mitigating the harms of any potential unintended consequences;

- 「デジタルアイデンティティのガバナンスに関する理事会勧告」(仮訳)
  - https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491
  - https://www.sakimura.org/2023/06/5324/ (日本語仮訳等)
- "Digital identity refers to a set of electronically captured and stored attributes and/or credentials that can be used to prove a feature, quality, characteristic, or assertion about a user, and, when required, support the unique identification of that user;"
- デジタルアイデンティティとは、ユーザーに関する特徴、品質、特性、または主張を証明するために使用でき、必要な場合はそのユーザーの一意の識別をサポートすることができる、電子的に捕捉および保存された一連の属性および／またはクレデンシャルを指す；
- "XI.INVITES Adherents to disseminate this Recommendation at all levels of government."
- XI.採用国に対し、この勧告を政府のあらゆるレベルで普及させることを要請する。
- "XIII.INSTRUCTS the Public Governance Committee to:"
- XIII.パブリック・ガバナンス委員会に次の事項を指示する：



Human-Centric Digital Identity:

for Government Officials

v1.1

Lead Editors: Elizabeth Garber, Mark Haine
October 13, 2023

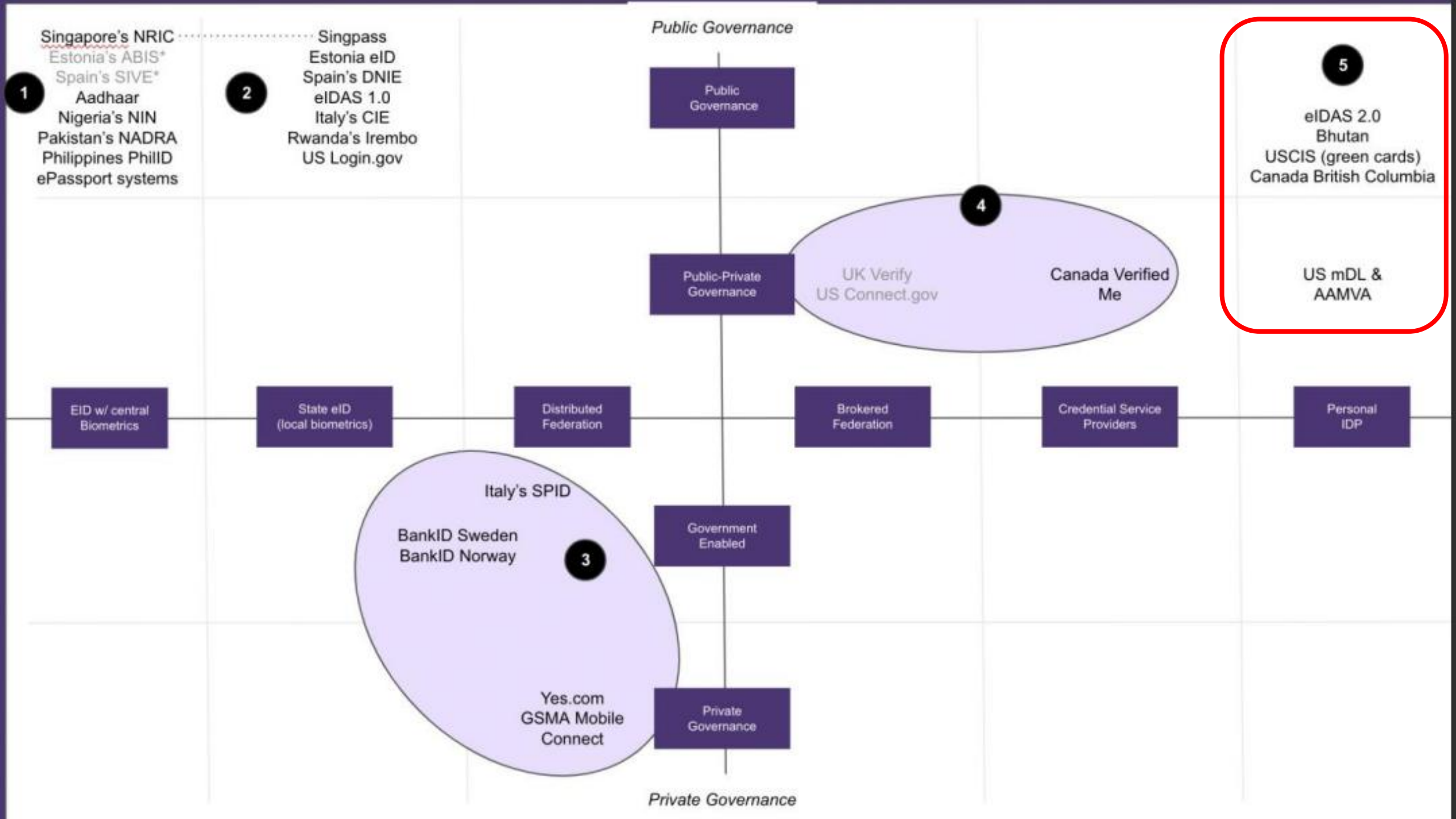
Citation:
Garber, E. and Haine, M. (eds) "Human-Centric Digital Identity: for Government Officials OpenID Foundation, (September 25, 2023)

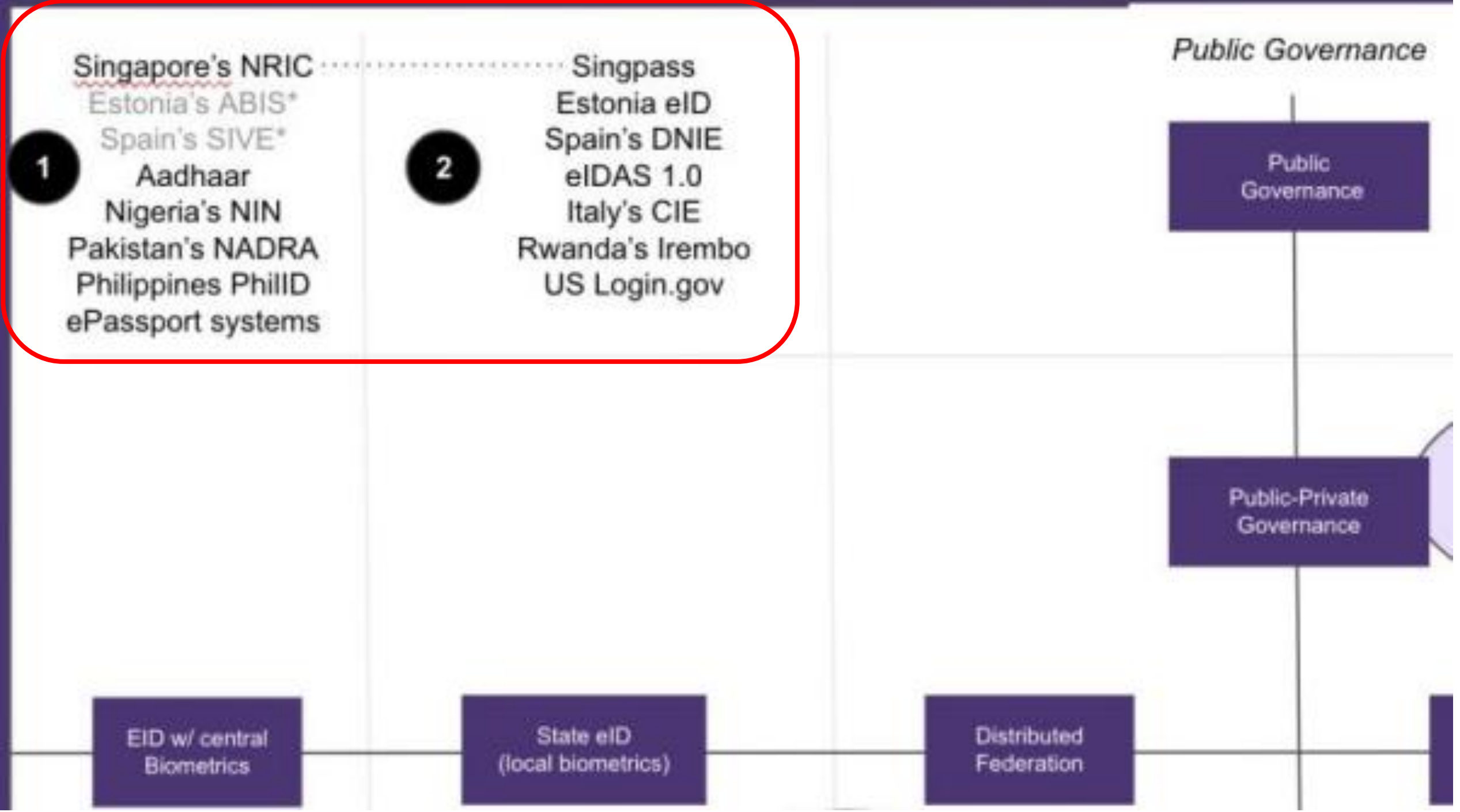
Date	Revision
October 13, 2023	V1.1 includes additional co-brand partners and MyData Global added to Appendix D
September 25, 2023	Final v1 version published
September 18, 2023	Public comments addressed and accepted. Pre-editorial. Graphics and tables will be formatted.
July 07, 2023	Publication of Public Comment draft
April 14, 2023	Expert Review

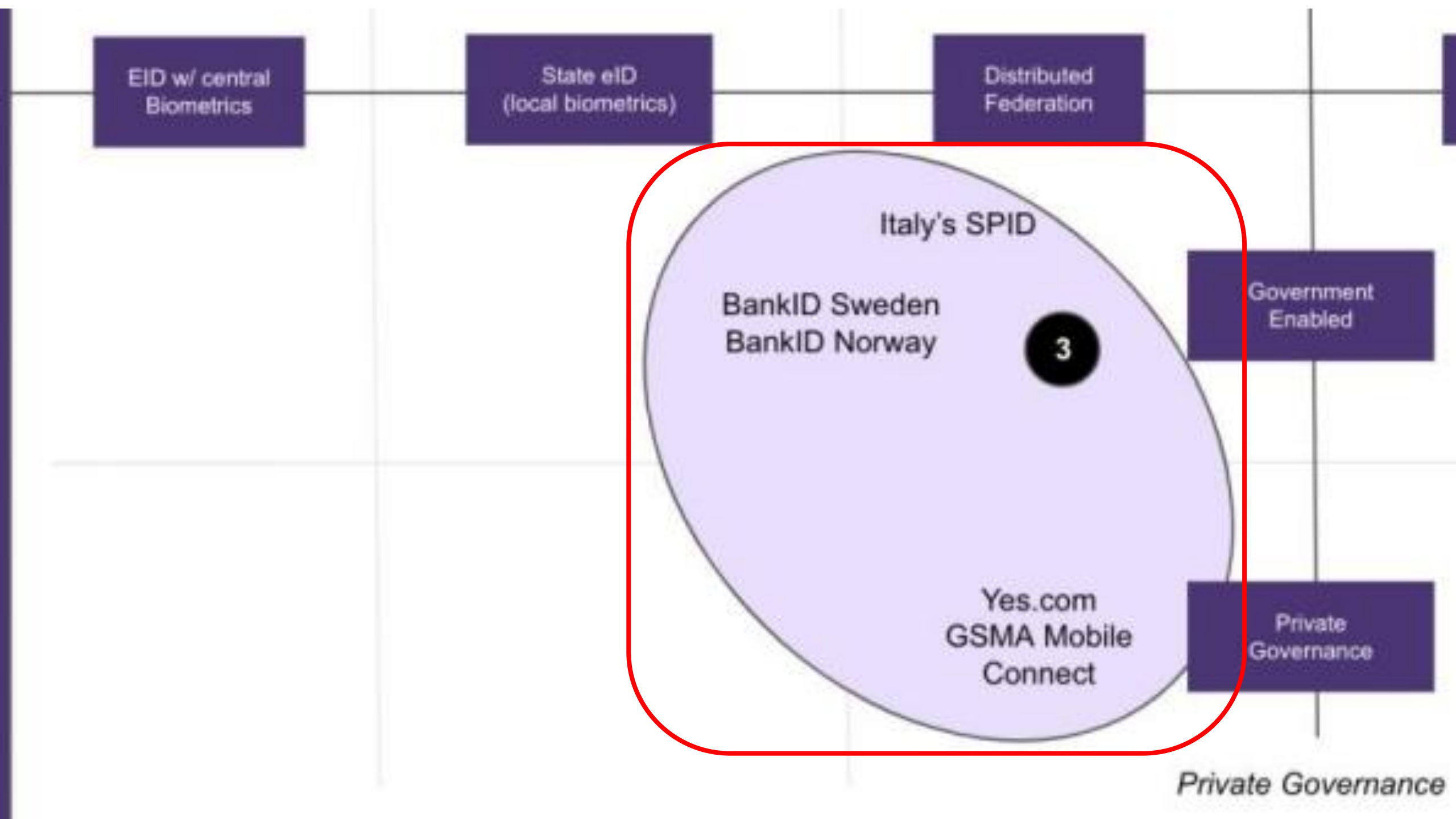
1

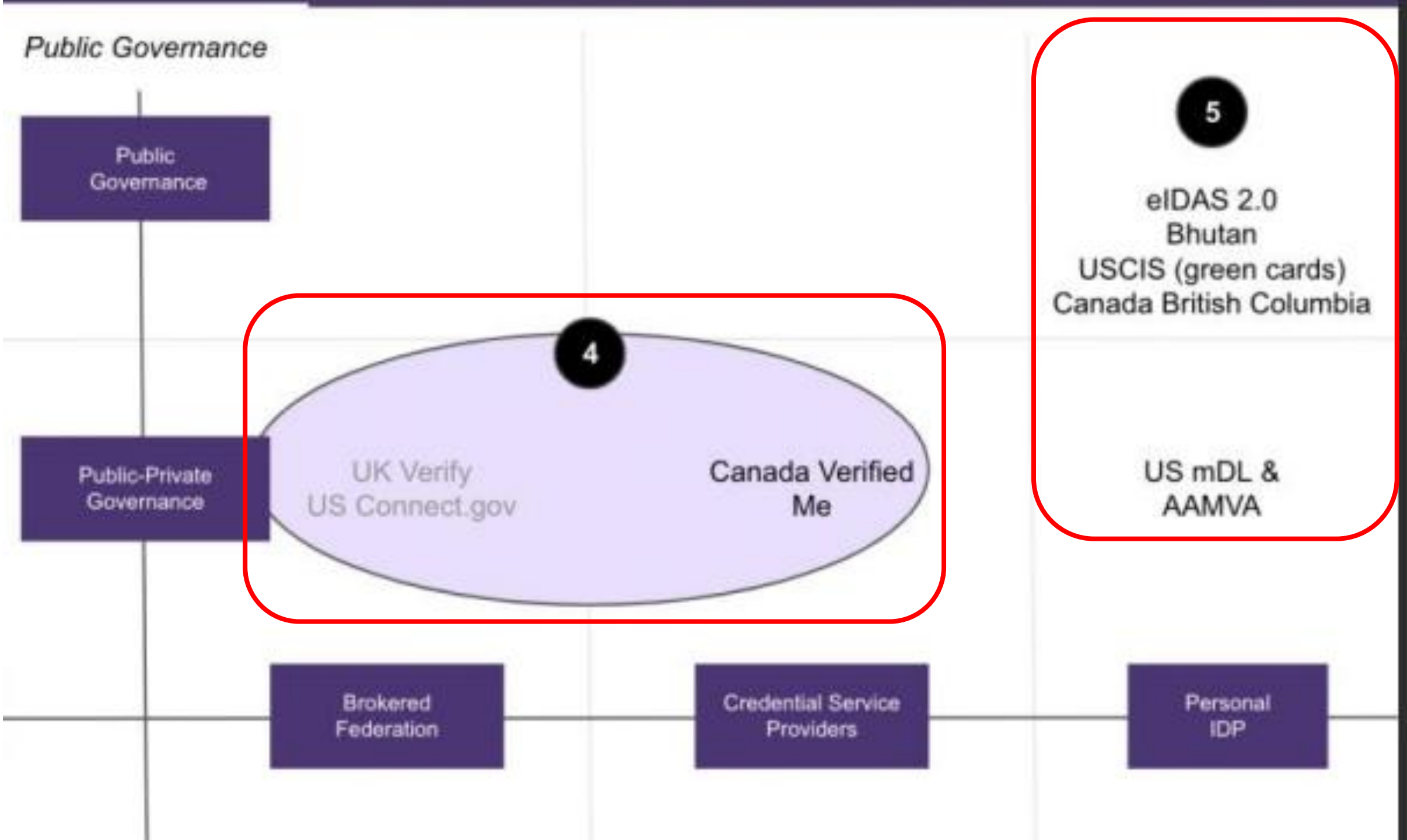
Human-Centric Digital Identity
a Primer for Government Officials

- Announcing the "Human-Centric Digital Identity: for Government Officials" Final Whitepaper
  - https://openid.net/human-centric-digital-identity-whitepaper/
  - https://openid.net/wp-content/uploads/2023/10/Human-Centric_Digital_Identity_Final-v1.1.pdf
- "Paradigm 5: The Emerging Wallet-Based Paradigm"


Public Governance
Singapore's NRIC
Estonia's ABIS*
Spain's SIVE*
Aadhaar
Nigeria's NIN
Pakistan's NADRA
Philippines PhilID
ePassport systems
1
Singpass
Estonia eID
Spain's DNIE
eIDAS 1.0
Italy's CIE
Rwanda's Irembo
US Login.gov
2
Public Governance
Public-Private Governance
Private Governance
Government Enabled
4
UK Verify
US Connect.gov
Canada Verified Me
3
Italy's SPID
BankID Sweden
BankID Norway
Yes.com
GSMA Mobile Connect
5
eIDAS 2.0
Bhutan
USCIS (green cards)
Canada British Columbia
US mDL & AAMVA
EID w/ central Biometrics
State eID (local biometrics)
Distributed Federation
Brokered Federation
Credential Service Providers
Personal IDP
Private Governance


Singapore's NRIC
Estonia's ABIS*
Spain's SIVE*
1
Aadhaar
Nigeria's NIN
Pakistan's NADRA
Philippines PhilID
ePassport systems
2
Singpass
Estonia eID
Spain's DNIE
eIDAS 1.0
Italy's CIE
Rwanda's Irembo
US Login.gov
Public Governance
Public Governance
Public-Private Governance
EID w/ central Biometrics
State eID (local biometrics)
Distributed Federation


EID w/ central Biometrics
State eID (local biometrics)
Distributed Federation
Government Enabled
Private Governance
Italy's SPID
BankID Sweden
BankID Norway
3
Yes.com
GSMA Mobile Connect
Private Governance


Public Governance
Public Governance
Public-Private Governance
Brokered Federation
Credential Service Providers
Personal IDP
4
UK Verify
US Connect.gov
Canada Verified Me
5
eIDAS 2.0
Bhutan
USCIS (green cards)
Canada British Columbia
US mDL & AAMVA

Strategic Objectives and Activities

Strategic Objectives reflect NIST's priorities and define specific areas of focus. They address the drivers previously defined in this document and provide a means to evaluate our work for alignment with national and organizational goals.

Accelerate Implementation and Adoption of Mobile Driver's Licenses (mDL) and User Controlled Digital Credentials

Advance international standards, implementation guidance, and interoperability efforts to promote increased and accelerated adoption of mDL and other forms of interoperable digital credentials. Initial efforts will focus on advancing mDL in line with the National Cybersecurity Strategy, but will progress to evaluation and integration of other standards-based credentials (such as verifiable credentials) into an interoperable wallet.

Short Term	Long Term (pending resources)
Develop Privacy and Security Considerations for mDL Implementation	**Execute NCCoE Project – Accelerating adoption of Mobile Driver's License Technology**
Contribute to ISO/IEC 18013-5, mDL Reference Implementation	**Execute NCCoE Project – Implementing Multiple Interoperable Credential Types**
Contribute to ISO/IEC 23220 Building Blocks for Identity Management via Mobile Devices	**Develop Draft Guidance for use of Digital Wallets and Portable Digital Credentials**
Contribute to ISO/IEC 18013-7, mDL for Unattended Use Cases	

Digital Identity Wallet

- 背景動向
  - EU Digital Identity WalletやアメリカmDL等、各国で動きが出てきているところ
    - EUはeIDAS 2.0においてEU DIWをeIDの重要なパーツとして位置づけ、民間も交えたコンソーシアムも組成
  - GoogleもGoogle Walletをリブランディングし、Appleもアメリカ内で特定の州でのmDLアプリを配布済み
  - 国際標準化では、ISO/IEC 18013-5 (mDL), ISO/IEC 23220(策定中)などが関連
  - 更に、Linux Foundationの下に、Walletの"open source engine"を作る組織を発足 (2022)し、ITU-Tと連携
    - OpenWallet Foundation (https://openwallet.foundation/)
    - OpenWallet Forum (https://www.itu.int/en/ITU-T/extcoop/openwalletforum/Pages/default.aspx)
  - デジタル庁の重点計画や「日EUパートナーシップ」等でも言及され、DIW PoCやDIW Advisory Boardも実施されている

Digital Identity Wallet

- 背景動向
  - EU Digital Id
    - EUはeIDAS
      ソーシアムも
  - GoogleもGoo
    のmDLアプリを
  - 国際標準化で
    が関連
  - 更に、Linux Fo
    発足 (2022)
    - OpenWalle
    - OpenWalle
      T/extcoop/
  - デジタル庁の重点計画や「日EUパートナーシップ」等でも言及され、DIW PoCや DIW Advisory Boardも実施されている

ど出てきているところ
定づけ、民間も交えたコン

カ内で特定の州で

220(策定中)など

gine"を作る組織を

)

識別子でも認証そのものでもなく、まさに
「デジタルアイデンティティ」
に関わる技術

Digital Identity Wallet アドバイザリーボード (令和6年度報告書)

デジタル庁　ホーム　一般の方　行政・事業者の方　プレスルーム　Language　検索　すべてのメニュー

デジタル・アイデンティティの拡大に向けた取組

デジタルにおいて「人、法人、モノ等」の「身元、資格、属性等」を確立・証明するデジタル・アイデンティティの利活用は、デジタル社会におけるトラストを確保・向上するための基礎であり重要な要素です。
デジタル・アイデンティティの社会実装と適切かつ有効な活用の拡大、また国民が安心してこれらを利活用できるためのガバナンスに関する施策を検討・実施しています。

Digital Identity Wallet（DIW）

個人・法人が自身の属性や資格情報等を、自ら保存・管理し提示できる仕組み及びアプリ（ウォレット）である「Digital Identity Wallet」について、プライバシー向上や手続のデジタル完結への寄与などが期待されています。その社会実装および国民が安心して利活用できるためのガバナンス等の施策を実施しています。

Digital Identity Wallet（DIW）アドバイザリーボード

外部有識者によるアドバイザリーボードを開催し、今後のDIWの社会実装に向けた施策検討の参考・前提として、そのメリットやリスク、論点の検討及び整理を実施しました。

- 令和6年度DIWアドバイザリーボード報告書（PDF／8,301KB）

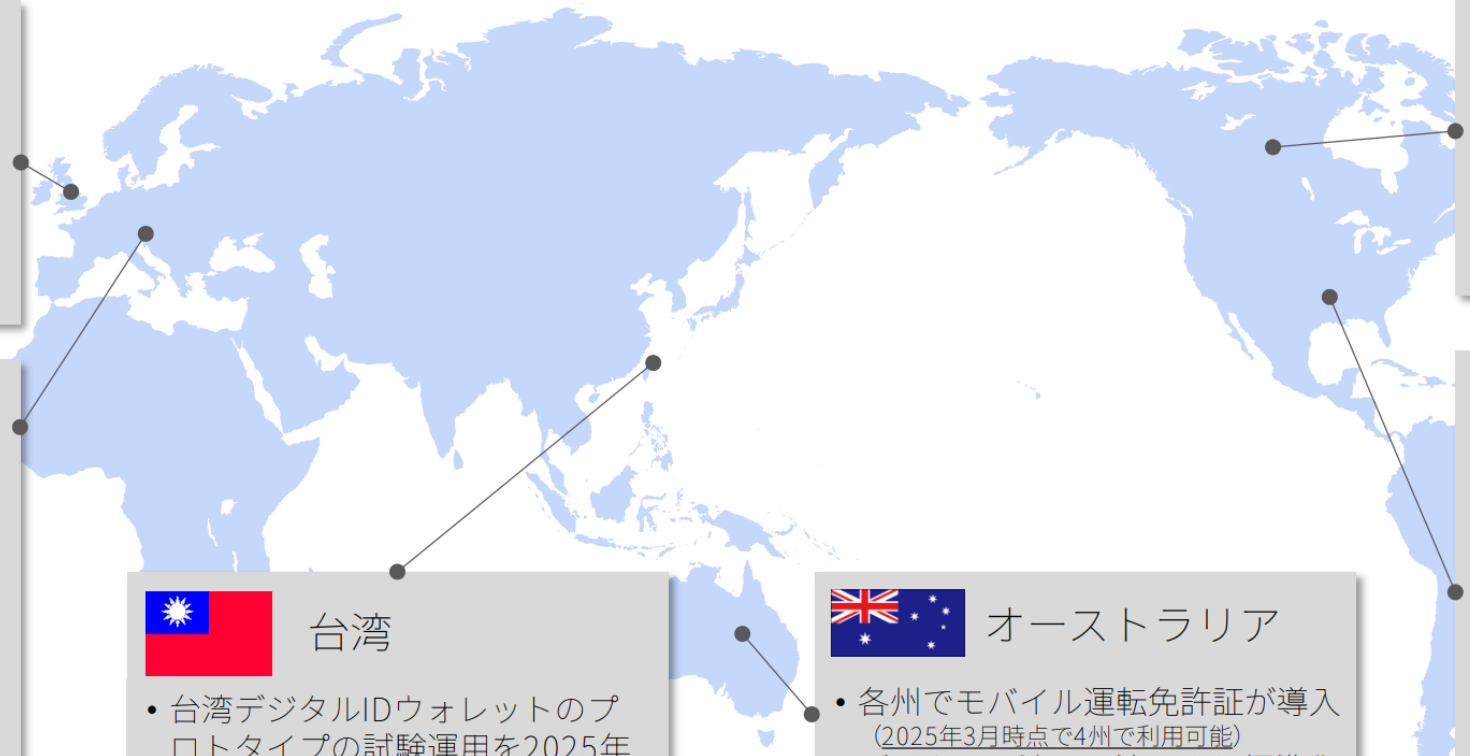
https://www.digital.go.jp/policies/trust

報告書より

DIWに関する諸外国の動向　ー　サマリー

- DIWに関する動向は近年活発化しており、EUや米国はじめ様々な国・地域でDIWに関連する議論が進められている。 2024年度の主な動向は以下のとおりである。

世界の各国・地域等におけるDIWに関する動向（2024年度の主な動向を抜粋）



英国

- 運転免許証や退役軍人カードを保存できるGOV.UK Walletを2025年にリリース予定。

EU

- 2024年4月に公布されたEU規則に基づき、EU加盟国はEU DIWを市民に今後提供
- 大規模パイロットが進められ、デモ動画などが公開

台湾

- 台湾デジタルIDウォレットのプロトタイプの試験運用を2025年12月までに開始予定

オーストラリア

- 各州でモバイル運転免許証が導入（2025年3月時点で4州で利用可能）
- デジタルID法の可決により標準化と相互運用が進められる見込み

カナダ

- ケベック州政府がデジタルIDウォレットを作成・提供することを発表（サイバーセキュリティ&デジタル戦略2024-2028より）

米国

- モバイル運転免許証（mDL）の導入を推進中（2025年3月時点で15州以上で利用可能）
- 一部の空港で国内線のTSAセキュリティチェックにてmDL利用可能。今後全ての空港への拡大が目標

DIW: 様々な領域での動き

Apple, Google
(Smart Phone)

国策・政府的ID
(EU/アメリカ/etc...)

ISO/IEC
(国際/
デジュール標準)

OpenWallet
Foundation
(オープン/
デファクト標準...?)

Digital Identity Wallet...?

eIDAS2.0での
EUDIW

ISO的
DIW

Apple/Google
におけるWallet

その他...?

Digital Identity Wallet...?

Digital Identity Wallet...?

DIW: 話者の注目点

いわゆる選択的属性・情報開示 (Selective Disclosure)

対面におけるデジタル証明(書)の検証

スマートフォン普及時代の証明の在り方

ユーザーセントリックなデジタルアイデンティティ

- あえてSSIとまではいいませんが、軸足の変動は起きている

デジタルアイデンティティと
セキュリティの複雑な関係

デジタルアイデンティティとセキュリティの複雑な関係

- デジタルアイデンティティを扱うにあたって、技術や運用においてセキュリティという手段は非常に大事
- デジタルアイデンティティは監査やプライバシー等とも強く関係がする
- 一方、デジタルアイデンティティは、モノや特に"人"を扱う分野であり、ロジカルにテクニカルに割り切れない部分も多い
- 更に、法律や人権的な側面もあり、私企業の判断だけでは整理が出来ない部分も増えていくことが予測される
- デジタルな社会が、技術が進歩すればするほど、デジタルアイデンティティの影響範囲と重要性は今後、どんどん増していく

デジタルアイデンティティを守る手段としての認証強度等の話

- 「パスキー対応どうするか」が直近の課題
- この瞬間は自分「だけ」で考えて何かやるのは悪手
  - 専門家「達」の知見を集約して、攻撃者側に圧力をかけていくべき
  - エントロピーの計算を自分でやっていたらその時点で終わってる(オレオレ認証)
- ベストプラクティスに従う
  - 例えば今、パスワードマネージャーと連携出来ない認証はクソ
  - PCとスマホ、Webとアプリ、やるべきことを考えるだけでも大変
- 攻撃者の情報を共有して対応していく (高難易度…)
- 技術のトレンドやガイドライン等を必死に追いかける
- デジタルアイデンティティの死守は、過渡期でもあり、
  ある意味で攻撃者との戦争の最前線でもある

具体例：多要素認証手法と権利について

そもそもパスワード(記憶)は個人のもの	もちろん生体情報も個人のもの	…私物スマートフォンは？
• 脳の私的記憶というリソースを提供している • ⇒仕事に使ってる	• 誰にも渡せないぐらい大事なセンシティブ情報 • ⇒仕事に使ってる	• 認証の３要素(知識情報/生体情報/所持情報)のうち所持だけ • 特殊なのはコストの問題(所有権!)

2030年に向けて

- 実際、Digital Identity関連領域は、2024年に激動した
  - 国際でも国内でも
  - 行政でも民間でも
  - 技術でも制度でも
- 2025年はおそらく目に見える形で社会に影響を及ぼす
  - パスキー、個情法、etc...
- 今後…
  - EU eIDAS 2.0の施行
  - NIST SP800-63-4 (Final)の発行
  - そしてもちろん
    Digital Identity Walletの普及

2030年
向けて

- 実際、Digital Identity関連領域は、2024年に激動した
  - 国際でも国内でも

デジタルアイデンティティは
デジタル社会の礎に

る形で社会

al)の発行

  - そしてもちろん
    Digital Identity Walletの普及

Please contact me !!

mailto: lef@parongo.com
twitter: @lef

PARONGO

— internet security company —