人間であることの証明

APACにおけるデジタル信□と詐欺耐性の□化へ向けた人間中心のネットワ□クの構築

2025年12月

Japan Trust & Safety Association
一般社団法人トラスト＆セーフティ協会

Southeast Asia
Public Policy Institute

本稿について

本稿は、東南アジア公共政策研究所 [Southeast Asia Public Policy Institute] が、一般社団法人トラスト＆セーフティ協会（JTSA）と協力し、Tools for Humanityの支援を受けて、アジア太平洋地域のデジタル信頼の状況を探るために研究・作成したものである。提示された情報と分析は、関連する利害関係者へのインタビュー、公開情報、および著者による分析に基づいている。

JTSAの貢献は主にガバナンス、既存規格や制度との相互運用性、リスクに応じた人間であることの証明（Proof of Human）の実装に関する領域において行われ、田中清隆氏の洞察は、本稿の執筆に大きく寄与した。なおJTSAは日本を含む各国の政策、法律、または規制に関する分析や評価に関与していない。また本稿はJTSA会員社の意見を代表するものではない。

本稿は、Tools for Humanityの意見を代表するものではない。政策、法律、または規制を網羅的に検討することを意図したものではなく、その範囲と制限を慎重に考慮して使用する必要がある。

目次

エグゼクティブ・サマリー

オンライン詐欺は、産業化され、国境を越えて展開される事業へと発展している。世界のサイバー犯罪経済は現在10兆米ドルを超える規模に達しており、年間1兆米ドル超が詐欺による損失とされる。金銭的損失にとどまらず、詐欺は人々のメンタルヘルス、社会の信頼を侵食し、法執行機関の資源を消耗させている。アジア太平洋地域は、主要な標的であると同時に、運営上も中核的な拠点である。東南アジアでは、人身取引と結び付いた大規模な詐欺拠点が存在し、日本や韓国といった先進市場では、投資詐欺やなりすまし詐欺が相次いで発生している。問題は地域全体にまたがり、相互に関連しており、各国・各経済圏を横断した協調的な対応が求められている。

AIによる音声クローンやディープフェイクは大規模かつ効率的に人をだますことを可能にし、自動化されたアカウント生成は接触対象を拡大させ、暗号資産や即時決済は収益化を加速させている。他方で、同じ技術に基づき、より高度な本人確認、真正性を示すシグナル、プライバシーを保護するセーフガードを通じて信頼を強化することも可能である。その際、新たなリスクを防止するためのガバナンスと透明性の確保が必要である。

既存の取り締まりと啓発の取り組みは必要だが、犯罪者が合成または自動化されたアイデンティティを安価に何千も作成できる状況では不十分である。持続的な前進のためには、詐欺行為者が悪用する隙間を埋める二層のデジタル信頼が必要である。

- **デジタルアイデンティティ（デジタルID）：** 「あなたは誰か」という問いに答えるもので、金融やデジタル行政などの規制領域で利用可能な、非匿名かつKYC対応の資格情報。

- **人間であることの証明（Proof of Human、以下「PoH」という。）：** 「あなたは実在する固有の人間か」という問いに答えるもので、完全な本人情報の開示が不要または望ましくない、オープンかつプラットフォーム横断的な環境で利用可能なプライバシー保護型のシグナル。

PoHはデジタルIDの代替ではない。PoHはデジタルIDを補完する層であり、詐欺の多くが発生するインターネット領域（ソーシャルメディア、メッセージング、マーケットプレイス）に信頼を拡張するものである。ユーザーのプライバシーを保持しつつ、偽造・合成アカウントやボットによる不正行為を抑制することが可能となる。最近の動向は、信頼と安全に基づく枠組みの中でPoHを導入することの検討意義を示している。自動化や大規模な不正行為への対処を目的としつつ、ユーザーの意図や信頼性を保証するものと誤解されないように、そのメリットと限界について正確な理解を行う必要がある。

アジア太平洋地域で、各国政府は強固なデジタルID基盤を構築し、規制分野におけるKYCおよび説明責任を強化してきた。しかし、詐欺行為の大半は、ソーシャルメディア、メッセージング、オンラインマーケットプレイスといった非規制領域で発生しており、そこではデジタルIDは適用されない。PoHが独自の価値を発揮するのはこの領域である。プライバシー保護型のヒューマン・トークンやデバイスベースの検証といった仕組みにより、PoHは大量の偽アカウント生成を抑制し、ボット主導の詐欺オペレーションを妨害し、被害者が標的とされる前の段階で真正な人間中心のネットワークを強化することが可能である。これらの技術が有効に機能するには、明確なセーフガード、ユーザーによるコントロール、そして不正利用を防止し、匿名性を保護し、社会の信頼を維持するガバナンス体制が必要である。

사례 개요

- **日本 - 社会保障・税番号制度（マイナンバー制度）：** 公的な登録に基づき全国規模で一意性を確認する仕組みを備える一方、データ取り扱いをめぐる事案により信頼が揺らいだ経緯もある。政府発行IDとPoHを組み合わせ、行政サービスの枠を超えてプライバシーに配慮した検証を可能とするハイブリッド型モデルの基盤となり得る。

- **韓国 - 実名制度:** 金融、通信、デジタル行政にわたり深く統合されており、事実上PoHの代替的機能を果たしている。一定の成果を上げる一方で、プライバシーや市民的自由をめぐる懸念も存在し、ユーザー主導型・分散型認証への関心が高まっている。

- **マレーシア - MyDigital ID（展開中）：** 公的登録制度と連動した生体認証付き資格情報。設計段階からガバナンスを組み込む方向性はPoHの原則に沿っているが、拡張するには強固なセーフガードと社会の信頼が必要である。

- **フィリピン - PhilSys（急速展開）：** デジタルIDのダウンロードおよび電子的検証を通じて迅速かつ大規模な普及を実現。運用面でPoH的機能を示しているが、同時にガバナンスとユーザー教育を並行して推進する必要性も示している。

詐欺への耐性を効果的に高めるには、多層的な保証が必要である。規制対象となるやり取りは検証済みのアイデンティティに基づいて担保されるべきであり、オープンプラットフォームはプライバシー保護型の人間であることの証明によって強化されるべきである。透明性、相互運用性、ユーザーによるコントロールは、これらを横断的に支える基盤的要素である。標準化団体、業界仲介機関、マルチステークホルダー型の枠組みなどの中立的なガバナンスメカニズムは、各国の要件をグローバルプラットフォーム上の運用慣行へと転換するうえで極めて重要となろう。

政策提言

- **デジタルIDとPoHを詐欺防止戦略に統合：** 金融、電子商取引、通信フローに一意性の証明チェックを組み込み、なりすまし、合成アイデンティティ、ボットによる不正利用を抑制する。その際、信頼と安全に基づく導入指針に従い、過度の依存を防ぐセーフガードを整備する。

- **プライバシー保護型かつ相互運用可能な標準をサポート：** 生体認証や資格情報による保証を暗号技術（ゼロ知識証明など）と組み合わせることで、適切な場合に匿名性を保護し、越境利用を可能にする。同時に、PoHを追跡またはプロファイリングに転用できないようにする。

- **地域の政策対話と協調を促進：** APECビジネス諮問委員会、デジタル金融包摂に関するG20ハイレベル原則、国連のデジタル経済関連イニシアチブなどのプラットフォームを使用して、目標の整合化、エビデンスの共有、PoHを活用した検証の分野横断的な試行を進める。併せて、サンドボックスを通じた実証を行い、ユーザー利便性、包摂性、適切性を評価する。

詐欺は構造的な信頼の欠如を露呈させている。強固なプライバシー、ガバナンス、相互運用性を備えたデジタルIDとPoHアーキテクチャを組み合わせることで、ユーザーの権利を維持しながら大規模な不正行為のコストを引き上げることができ、アジアにおけるより安全で包括的なデジタル経済への移行を加速させることができる。

はじめに： 詐欺のまん延と政策 ギャップ

社会や経済がデジタル技術を受け入れるにつれ、オンライン犯罪の規模が拡大し、手口が高度化している。世界のサイバー犯罪経済は現在10兆米ドルを超える規模に達しており、GDPで世界第3位の経済圏に匹敵する[1]。詐欺は拡大しているサイバー犯罪の類型であり、消費者の被害額は年間1兆米ドルを超えている[2]。しかし、そのコストは金銭的な損失にとどまらない。被害者はメンタルヘルスと生活の質への永続的な害を経験し、デジタルサービスとデジタル経済への信頼が侵食され、法執行、啓発活動、各国のサイバーセキュリティ対策に公的資源が振り向けられる[3]。

アジア太平洋地域が果たす二重の役割

詐欺が世界的に流行する中で、アジア太平洋地域は最も深刻な影響を受けている。いわゆる「豚の屠殺（ピッグ・ブッチャリング）」型詐欺、すなわち投資詐欺またはロマンス詐欺は特に広まっている。詐欺行為者がソーシャルエンジニアリング手法を用いて被害者との関係を構築し、被害者をだまして支払いや投資を行わせるものである。多くの場合、ソーシャルメディアまたはメッセージングサービスを通じて開始され、国境を越えて活動する組織犯罪シンジケートが専用の詐欺拠点から大規模な詐欺行為を行う。

東南アジアはこの経済圏の中心に位置している。詐欺被害者の供給源であると同時に、規制の行き届いていない地域での活動拠点でもあり、労働者の供給源でもある。労働者の多くは人身売買の被害者でもある[4,5]。一方、台湾、日本、韓国などのアジア太平洋地域の先進市場もこのダイナミクスと密接に結びついている。

信頼度が高く、デジタル化が進んだ経済圏であり、消費者が頻繁に投資詐欺やなりすまし詐欺の標的となっている。また、自国民が海外の詐欺拠点に誘い込まれる事例もある[6]。このダイナミクスは、地域の危機がローカルな問題ではなく、アジア全体にまたがる相互に関連する課題の一部であることを示している。そのため、先進国と人身売買の影響を受けた国々の双方を橋渡しする、連携した対応が必要である[7]。

テクノロジー：加害を可能にする存在であり、解決策でもある

テクノロジーは詐欺の経済構造を根本的に変えており、最も資源に恵まれた政府でさえ、急速に進化する手口に追いつくのに苦慮している。

第一に、人をだます働きかけが産業化している。人工知能、音声クローニング、ディープフェイクが詐欺に利用されており、金融セクターにおける詐欺の試みの42%超がAIによるものとされている[8]。これらのツールは、多言語で極めて現実味の高い台本、画像、通話を生成することができ、A/Bテストを通じて洗練された手法に基づく「投資」詐欺やロマンス詐欺といった長期型のスキームを、比較的熟練度の低いオペレーターでも実行できるようにしている。

第二に、拡大の上限が事実上なくなっている。アカウントの自動生成、いわゆるSIMファーム、プラットフォーム横断的なツールの活用により、少人数のグループでもソーシャルメディア、メッセージング、電話で数時間で数百万人に接触できる。また、ボットやレコメンデーションシステムを駆使して反応しやすい対象者を特定できる[9]。

第三に、収益化における犯罪者側のイノベーションが加速している。暗号通貨インフラ、フィンテックチャネル、いわゆるマネーミュールのネットワーク、クロスチェーンミキサーにより、資金の迅速な移動と難読化が可能になっている。さらに、即時決済の普及やKYC/KYB体制の分断・ばらつきにより、従来の銀行システムにおける介入・遮断のための時間的余裕が縮小している[10]。

その結果、デジタル経済において構造的な信頼の欠如が生じている。犯罪者は政府や規制当局が対応するよりも早く新しいツールを採用・適応している。

不正行為を可能にするこれらのテクノロジーも、セーフガードを講じて大規模に導入されれば、信頼の回復に資する可能性がある。

● デジタルアイデンティティおよびエンティティ認証の強化（人、デバイス、事業者のプライバシーを保護した本人確認、SIM/電話番号のレピュテーション管理、高リスクフローに対する高保証レベルの選択肢の導入）は、大量標的型攻撃のコストを引き上げることができる。

● コンテンツと通信の真正性シグナルの導入（画像や動画の暗号学的来歴証明、音声通話とメッセージにおける発信者/送信者認証の枠組み、広告とアカウントの完全性を強化する管理体制など）は、なりすましの成功率を低減できる。

● プライバシーを保護したシグナル共有をプラットフォームや決済ネットワーク間で行うなら、組織的な不正行為を検知する役に立つ。また、リアルタイム決済のリスクスコアリングと「クーリングオフ」のような摩擦措置（受取人確認、追加確認の実施、疑わしい送金の決済遅延）により、実行段階での損失額を削減できる。

● 被害者中心のモデル（迅速なテイクダウン手続、迅速な資金回収の仕組み、強要された労働者を被害者として特定する明確な手続）を法執行の取り組みと併せて導入することが、搾取の循環を断ち切るために必要である[11]。

したがって、テクノロジーは犯罪活動を可能にするものであると同時に、解決策の不可欠な部分でもある。政府、プラットフォーム、金融機関は、犯罪者が革新を重ねるのと同じペースで防御的技術を継続的に採用・更新する必要がある。なぜなら、詐欺は単なるサイバー犯罪事案ではなく、デジタル経済における構造的な信頼の欠如の表れだからである[12]。

詐欺がオンライン上の信頼の脆弱性を明らかにしているのだとすれば、信頼できるデジタルアイデンティティ（ID）はそれを修復する最も明確な手段の一つである。取引ややり取りの背後にいる主体について検証可能な保証を提供することで、デジタルIDは不正行為のコストを引き上げるとともに、より安全なデジタル経済を支える。次のセクションでは、デジタルIDが解決を目指す課題、その関連技術、地域における新たな政策対応について検討する。

デジタル信頼の二層構造：デジタルアイデンティティと人間であることの証明

詐欺と戦うには、多層的な信頼の仕組みが必要である。法執行と啓発活動は不可欠だが、持続的な進展は、犯罪者が大規模に悪用する抜け穴を埋めるアイデンティティと真正性のメカニズムに依存する。デジタルアイデンティティ（デジタルID）と人間であることの証明（PoH）は、この信頼インフラを構成する、相互補完的でありながら本質的に異なる二つの層である。デジタルIDは「あなたは誰か」という問いに答えるものであり、個人を銀行や政府が認識した検証済みの現実世界のアイデンティティと結び付ける。一方、PoHは「あなたは人間か」に答えるものであり、本人の身元を明かすことなく、人間であることと一意性を確認する。前者は匿名ではなく、銀行やデジタル行政などの規制環境に適している。後者は匿名性を保ちながら検証可能であり、完全な身元開示が必要でも望ましくもないオープンなデジタル空間を保護する。両者を組み合わせることで、デジタル経済における説明責任とプライバシーの両方を支える、バランスの取れた基盤が構築される。

PoHは、各国のデジタルID制度に取って代わるものではない。むしろ、完全な本人確認が現実的でない、あるいは望ましくないデジタル環境の領域に信頼を拡張するための、プライバシーを保護した補完的な層である。

デジタルID技術の形態

デジタルIDソリューションは複数の形式で存在し、それぞれ異なるリスクに対処している。

- **クレデンシャル型のデジタルIDシステム**は、デジタルで発行された検証可能な資格情報（クレデンシャル）に基づいている。これらは多くの場合、政府発行の身分証明書や、銀行、携帯電話通信事業者、大学などの信頼できる機関に由来し、氏名、年齢、国籍などの身元属性を安全に証明する。こうしたクレデンシャルはデジタルウォレットに保存し、複数のサービス間で提示することができる。これにより、スキャン文書をログイン資格情報にひも付けるだけの方法よりもはるかに堅牢で、再利用可能かつプライバシーを保護するデジタル上のやり取りが実現する [13]。

- **生体認証**は、サービスにアクセスする人が、あらかじめ登録した本人と一致するかどうかを確認するものであり、指紋や顔の特徴などの固有の身体的または行動的特性を使用する。これにより、パスワードやデバイスなどの他の認証情報が侵害された場合でも、不正アクセスを防ぐことができる。重要なこととして、生体認証はユーザーの真正性を確認するものであって、それ自体が身元を確認するものではない [14]。

- **ハイブリッド型デジタルIDモデル**は、政府発行のクレデンシャルと生体認証など複数の要素を組み合わせて、再利用可能で高い保証レベルを備えたデジタルアイデンティティを作成する。これらのシステムは、プラットフォーム間の相互運用性、強固な認証、プライバシー管理を支えるように設計されている [15]。

これらはいずれも、規制されたエコシステム内での追跡可能性、コンプライアンス、説明責任を意図しているため、KYC対応であり、設計上匿名ではない。

APACにおける政策対応

デジタルID技術は単独では機能し得ず、基準の設定、プライバシーの確保、幅広い普及を促進する政策的枠組みを必要とする。具体的には、次のことを意味する。

- 規制上の明確な位置付け。デジタルIDが金融取引、契約、公共サービスにおいて法的効力を持つようにするため。
- 個人データを保護するための強固なセーフガード（安全な保管、利用目的の限定、不正使用があった場合の救済手続に関する要件を含む）。
- 官民および分野横断的な導入。デジタルIDが政府だけでなく、詐欺の最前線に立つことの多いプラットフォーム、銀行、公共事業者によっても認識されるようにする。

東南アジア全域で、各国政府は、信頼性の高いデジタル経済の基盤として、デジタルID制度の整備を着実に進めている。

- タイの国家デジタルID（NDID）プラットフォームは、銀行、通信事業者、政府機関をフェデレーテッド型の枠組みで連携させている[16]。

- インドネシアとフィリピンは、金融包摂と社会サービスと連動した全国的な電子ID制度を展開している。

- ベトナムは、電子政府ポータルに生体認証による本人確認を組み込み始めている。

成熟度に差があるものの、地域における政策の重点は国内制度の構築から相互運用性の検討へと移行しつつある。越境移動、移住、貿易の流れが拡大する中で、国内だけでなく国境を越えて認識されるIDが必要であるとの認識を政策立案者は強めている。

より先進的な経済では、政府による包括的ID制度がすでに整備されており、さらなる統合の深化に向けた取り組みが進んでいる。

- シンガポールのSingPassは、銀行、ヘルスケア、電子商取引へのアクセスの基盤となっている[17]。

- 韓国は、住民登録制度を電子政府サービス、金融取引、モバイル認証を統合した包括的なデジタルID基盤へと拡張している。

- 日本のマイナンバー制度は、すべての居住者に一意の12桁の識別番号を付与しており、医療、税務、行政サービスとの連携が進んでいる[18]。さらに、金融分野での活用拡大や国境を越えた認識に向けた取り組みも進行中である。

これらの取り組みは範囲や進度こそ異なるが、全国規模の資格情報基盤が、安全なログイン手段を超えてデジタル経済の制度的基盤へと発展し得ることを示している。また、国内実装や地域的相互運用性を検討するASEAN諸政府にとっての参照事例となっている。

同時に、これらの経験は、政府の取り組みだけでは不十分であることを示唆している。デジタルIDの有効性は最終的に、政府、金融機関、テクノロジープラットフォーム間の協力を通じて、広範なデジタルエコシステム全体に統合されるかどうかにかかっている。

詐欺対策におけるデジタルアイデンティティの役割

デジタルID技術は、詐欺や不正行為に対抗する最も有望な制度的手段の一つである。人、デバイス、組織を検証可能で非匿名の方法で認証することで、デジタルIDシステムはなりすましを抑制し、匿名性を限定し、不正行為のコストを引き上げる。万能な解決策ではないものの、KYCに対応可能なデジタル信頼の基盤として機能し、規制対象となる取引やサービスが、説明責任のある実在する個人または法人に結び付けられることを担保する。

詐欺行為者が悪用する隙間を埋める

詐欺は、本人確認の隙間につけ込んで拡大する。詐欺行為者は、ボットや偽アカウントを使用してわずかなコストでメッセージを拡散し、ディープフェイクや音声クローンを用いて信頼できる個人になりすまし、正規のアカウントを乗っ取って被害者から金銭をだまし取る。プラットフォーム間での認証の強度が弱く、または一貫していないと、こうした攻撃の成功率が本来よりも高まる。

デジタルIDは規制が及ぶ領域でこの隙間を埋める。デジタル上のやり取りを検証済みの身元情報に結び付けることで、犯罪者が匿名で活動することが難しくなり、被害者・企業・規制当局がオンライン上の相手を信頼しやすくなる。しかし、詐欺の大半は、ソーシャルメディア、メッセージングアプリ、非公式なマーケットプレイスといった非規制領域で発生しており、KYC制度が適用されない。こうした環境に対処するには、人間であることの証明（PoH）のようなプライバシーを保護する別のアプローチが必要である。

もっとも、最も強固なデジタルID制度でさえ、偽アカウントや自動化された不正行為による詐欺に完全に対処することはできない。この隙間を背景に、個人識別を必要とせずにユーザーが本物であることを確認する、プライバシー保護型の手法としてPoHなどの新しい概念への関心が高まっている。

人間であることの証明（PoH）：概念と政策的意義

PoH の定義

PoHは、デジタル信頼を強化する発展途上の斬新なアプローチである。一般的に、複数の偽のアイデンティティの作成を防止する仕組みと定義されており、オンライン上の主体が自動化されたボットや架空のアイデンティティではなく実在する人間であることを検証可能な形で保証する[19]。単なるアカウント登録やCAPTCHAによる確認とは異なり、PoHは人間であることを示す持続的かつ再利用可能なシグナルを提供することを目指す。このシグナルは必要以上の個人データを開示することなく、複数のプラットフォームやサービス間で認識できるものであり、デジタルエコシステム全体で信頼性の高い人間中心のネットワークを構築する基盤となる。

重要なこととして、PoHは各国のデジタルID制度に取って代わったり、競合したりするものではない。むしろ、信頼の問題における異なる層に対応することで、それらを補完する。すなわち、ユーザーが誰であるかを確立するのではなく、ユーザーが人間であることを検証する。

概念的に、PoHはデジタル保証の他の層とは異なる。従来のデジタルID枠組みは、「あなたは誰か」という問いに答えるものであり、氏名や国の登録番号などの検証済みの属性に個人を結び付ける。パスワードや多要素認証コードなどの認証ツールは、作成されたアカウントを保護するが、そもそも偽プロファイルや合成プロファイル自体の作成を防ぐものではない。約20年にわたり、CAPTCHAは人間であることを確認するためユーザーがパズルを解けるかどうかを試すことで、その隙間を埋めようとしてきた。しかし、ボットやAIツールが人間を上回る性能を示すようになるにつれて、その有効性が低下しており、正規のユーザーにとって利用上の負担が生じてもいる。対照的に、PoHは「あなたは人間か」という根源的な問いを取り扱う。この種の保証は、検証可能な資格情報、ボット対策、ブロックチェーン分野でシビル耐性（sybil resistance）と呼ばれる取り組みとも方向性を共有している。この意味で、PoHはデジタルエコシステムにおける真正性、プライバシー、拡張性の均衡を図ろうとする一連のイノベーションの延長線上に位置付けられる。

PoH の検証形態

PoHの仕組みは、いくつかの方法で実装することができ、それぞれ保証の強度やプライバシー保護の水準が異なる。以下の表では、PoHの主な検証形態と、それぞれが実務上どのように機能するかを整理している。

PoH検証の種類	仕組み	ユーザー体験	ユースケースの例
生体認証型（プライバシー保護型）	一度限りのライブネス確認（例：まばたきや顔を動かす動作）。システムは生体情報を保存・共有せず暗号技術に基づく「ヒューマントークン」を発行。	携帯電話のロック解除に似た1回限りの短い検証。ID データは開示されない。	偽アカウントの大量作成を防止。金融取引や高リスク取引を扱うプラットフォームでの高保証PoH。
デバイス/ハードウェア型	デバイス証明によりエミュレートされていない実在のデバイスであることを確認。身元情報を特定せずに「1人の人間 = 1台のデバイス」という紐付けが可能。	登録手続きに組み込まれたバックグラウンドチェック。生体情報は不要。	ボットファームを抑制し、メッセージングアプリ、ソーシャルメディア、ゲームプラットフォームでの自動アカウント作成を減少させる。
インタラクション/チャレンジ型	ユーザーは、ライブネス確認に類する指示への対応や、ボットが確実に実行できない暗号学的なチャレンジ・レスポンス課題を実行する。生体情報は使用しない。	単純な人間のインタラクション課題（例：制御された動作、時間制限付きの指示）だが、従来のCAPTCHAよりもはるかに負担が少ない。	ソーシャルプラットフォームやオンラインコミュニティにおいてIDや生体情報を求めずに合成プロファイルを阻止するのに有用である。
ソーシャル/ウェブ・オブ・トラスト型証明	ユーザーは信頼できるコミュニティメンバーまたはレピュテーションネットワークによって確認され、プラットフォームはそれをPoH信号に変換する。	検証済みユーザー/コミュニティからの簡易的な確認。	ピアツーピア型マーケットプレイス、ギグプラットフォーム、コミュニティベースの検証環境。

表3.1：PoHの検証形態

PoHが詐欺対策にどのように役立つか

PoHはまだ新しい概念だが、詐欺や不正行為との戦いにおいて一定の意義を有し得る。今日のオンライン詐欺は規模の拡大に依拠している。人身売買組織や犯罪グループは、幾千もの偽アカウントを作成して被害者を誘い込み、いわゆるロマンス投資詐欺を自動化し、あるいはマネーミュール口座のネットワークを運営している。デジタル上の人物像を低コストかつ大量に作り出せることは、不正行為のコストを引き下げる一方で、プラットフォーム事業者や規制当局による悪意ある活動の検知能力を圧倒している。対照的に、PoHは真正な人間のネットワークを強化し、合成または自動化されたアイデンティティの大規模な拡散を抑制することで状況のバランスを是正する助けとなり得る。

原理的に、PoHはアカウント作成または取引の時点で一定の摩擦を導入することで、偽アカウントの拡散の速度と規模を抑制する可能性がある。

人間であることを検証可能にする仕組みは、いくつかの役割を果たし得る。

1. ロマンス詐欺、求人詐欺、投資詐欺における「餌」となる**偽プロフィールを防ぐ。**被害者が引き込まれた後に事後的にアカウントを削除する対応に頼るのではなく、PoHは最初から不正アカウントの供給そのものを減らすのに役立つ。

2. マネーミュール口座を通じた取引の流れを減らすことで**金融システムを保護する。**銀行や決済ネットワークは、正当なユーザーと不正なアカウントを区別するのに苦慮している。人間であることを示す再利用可能な証明情報は、個人データを繰り返し開示させることなく、既存のKYCおよびAMLセーフガードを補強し得る。

3. デジタル商取引とオンラインコミュニティへの信頼を強化する。詐欺やなりすましによって信頼を損なわれている市場では、買い手、売り手、またはコミュニティメンバーが実在する人間であることを確認できれば、将来的にピアツーピア取引、ギグワークプラットフォーム、ソーシャル空間への信頼を回復するのに役立つ可能性がある。

セーフガードとガバナンス

PoH自体が監視の手段とならないようにするには適切なセーフガードが不可欠である。新しいモデルでは、プライバシーを保護する設計を重視している。暗号学的証明とゼロ知識証明の手法により、ユーザーは基礎となる身元データを開示することなく人間であることを示すことができる。身元の確認（主体は人間か）と身元の開示（主体は誰か）を区別することは、各法域において権利と信頼を維持するうえで重要である。セーフガードには強固なガバナンスも必要である。規制当局、標準化団体、またはマルチステークホルダーによる監査などの監督体制は、PoHのシグナルが侵入的な追跡やプロファイリングに転用されるのを防ぐ助けとなる。

同様に重要なのが、ユーザーの権利と包摂性である。検証は任意であり、透明性が確保され、取り消し可能でなければならない。個人が自らのPoHシグナルの利用方法を理解し、管理できることが必要である。年齢確認などの補完的な仕組みは、機微な情報の開示を求めることなく未成年者を保護し得る。また、スマートフォン、生体認証、安定した通信環境を持たない人々を排除しないよう、複数の検証経路を用意することも重要である。最終的にPoHの信頼性は、プライバシーを尊重し、アクセシビリティを確保し、デジタル信頼に対する地域の取り組みと整合しつつ、安全性を向上させられるかどうかにかかっている。

しかし、技術的なセーフガードだけでは不十分である。効果的なPoHの導入には、APACにおけるデジタルエコシステムの現実を反映したガバナンス構造が必要である。各国のデジタルID制度は国内のルールの下で運用されているが、実際のユーザーのやり取りやプライバシー上のリスクのほとんどはグローバルなプラットフォームで発生している。この構造的ギャップのために、政府とプラットフォーム間の直接的な統合だけで対応することは現実的でないことが多い。中立的なガバナンス層がしばしば必要である。要件を翻訳し、関係者を集め、大規模導入前の安全なテストを支援できる、相互運用を担う独立した仲介主体である。

このような仲介主体は、PoHが技術的に実現可能であり、プライバシーを尊重し、国内の枠組みとプラットフォーム横断的な環境の両方と整合する形で実装されることを確保する助けとなる。国内基準を運用上の指針へ落とし込み、プライバシーと監査可能性に関するマルチステークホルダーの議論を主催し、ユーザーやプラットフォームに意図しないリスクを与えることなくPoHを安全に試行できるサンドボックス環境を整備できる。

もう一つのセーフガードは社会の信頼に関わるものである。PoHは、デジタルアイデンティティ、認証、eKYCとは異なる新しい概念であり、誤解が生じれば、監視やデータ利用に関する懸念を容易に招きかねない。そのため、能力構築は技術そのものと同じほど重要である。中立的な仲介主体、業界団体、市民社会ネットワークは、プライバシー保護型設計がどのように機能するかを説明し、PoHが「あなたは誰か」を明かすことなく「あなたは人間か」という問いに答えるものであることを強調し、責任ある実施のための実務的指針を提示する役割を担い得る。十分なコミュニケーションとユーザー教育があってこそ、うまく設計されたPoH制度を社会は安心して受け入れることができる。

最後に、PoHは信頼と安全の枠組みの中に位置付けなければならない。ユーザーが人間であることを確認しても、その意図が安全であることを保証するわけではない。投資詐欺、なりすまし詐欺、長期的なソーシャルエンジニアリング型詐欺など、APACで特に被害の大きい詐欺の多くは、実在する人間のオペレーターによって実行されている。そのため、PoHは他の安全性シグナルを代替するのではなく、補完するものであるべきである。ISO/IEC 25389（安全な枠組み）などの既存の枠組みを適用することで、PoHが適切に使用されることを確保できる。具体的には次の点を確保する必要がある。

- 自動化と大規模攻撃に対する多層的防御の一層として活用すること
- 人間による脅威を検知する行動シグナルやレピュテーションシグナルと併用すること
- 過度の依存を避けるため明確な実装指針を設けること

したがって、PoHは既存の本人確認枠組みを補強する補完的イノベーションとして試行するべきであり、代替手段として位置付けるべきではない。慎重に設計・管理されれば、リスクの高いデジタル環境で実在のユーザーを検証する新しい方法を試すのに役立ち、大規模展開で機能し得る方法に関するエビデンスを蓄積することが可能となる。広い視点では、相互運用可能で権利を尊重するPoH枠組みは、各国のデジタルID施策を補完し、越境的な認識を支援し、APAC全域にわたる詐欺・不正対策の地域協力のための新たな信頼基盤を提供し得る。こうして各国が現代のオンライン犯罪の規模と速度に耐え得る検証可能で強靭な人間中心のネットワークを構築するのを助ける。

次のセクションでは、APAC各国の事例に目を向け、PoHが実務上どのように実装され得るかを検討する。

ケーススタディ：先進技術の実践

アジア各国で政府は、公共サービスや金融サービス向けに、市民の本人確認を行う強固なデジタルID基盤を構築してきた。しかし、詐欺の大半は、こうした規制された制度の外側で、つまり匿名性が支配的なソーシャルメディア、メッセージング、コンテンツプラットフォームで発生している。新たに登場している人間であることの証明（PoH）技術は、個人データを明らかにすることなく人間であることと一意性を確認することで、デジタルアイデンティティの信頼性をこうしたオープンな環境へ拡張する方法を提供している。以下のケーススタディでは、日本、韓国、マレーシア、フィリピンの4つの経済圏が自国の制度を通じてPoHに類似する検証要素をどのように構築しているかを検証するとともに、その経験が今後の詐欺耐性戦略にどのような示唆を与えるかを検討する。

日本：マイナンバー制度と信頼の課題

2016年に開始された日本の社会保障・税番号制度（マイナンバー制度）は、税務、社会保障、災害対応を目的としてすべての居住者に一意の12桁の識別番号を付与している [20]。行政データの統合と効率化を目指して設計されたこの制度は、マイナンバーカードの導入によってデジタル領域へ拡張された。電子政府サービス、医療、金融取引における安全なオンライン認証を可能にするICカード型の身分証である [21]。2025年までに、人口の70%超をカバーする9,000万枚超のカードが発行されているが、サービス連携のばらつきや根強い信頼上の懸念により、デジタル利用は限定的にとどまっている [22]。

マイナンバー制度は全国規模で一意性を検証する仕組みを提供しているが、PoH枠組みというより従来型の身元確認制度としての性格が強い。確認は政府による登録と書類確認に基づくものであり、PoH技術に特徴的なプライバシー保護や暗号学的保証を備えているわけではない。それでも、日本の経験は、国による一意性確認が、現代的なプライバシー強化の仕組みと組み合わさることで、デジタル信頼と詐欺防止の基盤となり得ることを示唆している。

同時に、日本が経験したことは、中央集権的な身元確認制度のみでは詐欺対策に限界があることも示している。オンライン詐欺となりすましの大半は、規制の緩い環境（ソーシャルメディア、メッセージング、電子商取引）で発生している。これらのプラットフォームは、消費者保護およびコンテンツ規制の枠内で運営されているが、日本のID連動型の保証の仕組みの外側に位置している。一方、2023年の健康保険情報の誤ひも付け問題などのデータ管理事案は、社会の信頼を揺るがし、プライバシー、監督、説明責任をめぐる議論を再燃させた [23]。こうした事例は、技術ではなく信頼こそが、検証済みIDの活用拡大における主要な制約条件であることを示している。匿名性を重視する社会的規範と国によるデータ管理への慎重な姿勢によって形成された日本のプライバシー文化では、PoHなどの新しい検証手法を導入する上で社会的受容が決定的に重要となる。

これに対応して、政府はガバナンスと相互運用性の強化を進め、マイナンバーカードに基づく認証（JPKI）を銀行、SIM登録、オンライン商取引などの民間分野へ拡張する方向で検討を行っている [24]。透明性を確保した形で実装されれば、日本は公的な本人確認を基盤としつつ、プライバシーに配慮した暗号技術によりPoH型の一意性証明を可能にする、ハイブリッド型のデジタル信頼モデルへ発展し得る。そのような進化を通して日本は、信頼できるIDと拡張可能かつプライバシー配慮型の検証を結び付け、デジタル経済における詐欺への耐性と社会の信頼の両方を強化することができる [25]。

韓国：デジタルID統合と実名確認

韓国は、銀行、通信、電子政府サービスを結ぶ全国的な電子ID基盤を中核とする、世界でも高度かつ統合度の高いデジタルIDエコシステムを運営している[26]。1968年に導入された住民登録番号（RRN）制度を基盤とした韓国のID枠組みは、実名確認、生体認証、公開鍵基盤（PKI）といった層を重ねながら発展し、急成長するオンライン経済を支えてきた[27]。デジタルIDカード（2020年）とモバイル運転免許証（2022年）の導入は、紙媒体から完全なデジタル資格情報への移行を象徴する節目となった[28]。2025年までに、5,000万人超の韓国人が毎日デジタル認証を使用して、PASS、Kakao、Naver、Samsung Passを介して金融、政府、民間サービスにアクセスしている[29]。

このようなプラットフォーム横断的なID統合は、韓国の実名制およびサイバーセキュリティ体制の中核となっており、ほとんどのオンライン取引の前に法的IDの確認が必要である。これらの仕組みは事実上のPoH層として機能し、デジタル上の主体が実在する一意の個人に対応することを保証し、不正行為、合成ID、自動化された不正利用を大幅に抑制している。公的・民間システム間の相互運用性は高い信頼水準を生み出し、金融分野におけるID詐欺の発生率も国際的に低い水準である[30]。

しかし、韓国モデルは強力な中央集権性に伴うトレードオフも示している。実名義務や、通信、金融、政府機関間のデータ共有は、プライバシーと市民的自由をめぐる懸念を引き起こしてきた。信用情報機関や電子商取引プラットフォームからの大規模な情報漏えいは、同意とデータ最小化をめぐる世論の懐疑を増幅させている[31]。これに対応して、政策当局は個人情報保護法（PIPA）の下で保護措置を強化し、ユーザーが管理する分散型認証を模索するデジタルIDパイロット（2023年）を開始した。プライバシー保護に重きを置いたモデルへの重要な一歩と位置付けられる[32]。

韓国の経験は、国を基盤とするPoH制度の強みと限界の両方を示している。法的ID確認、生体認証保証、相互運用可能な信頼枠組みを組み合わせた仕組みは、詐欺防止とデジタル信頼の強化に向けた有力な参考モデルとなり得る。他方で、韓国での議論は、より強力なプライバシー保護とユーザー主導の管理を提供するアプローチへの関心が高まっていることを示している。この原則は、新興のPoH技術の方向性と整合する。今後、韓国がデジタル信頼のアーキテクチャを洗練させる過程で、厳格な実名強制よりも、デジタル経済における個人の権利と信頼を維持しながら実在するユーザーを確認する、バランスのとれたモデルへと重点が移っていく可能性がある。

マレーシア：MyDigital IDと生体認証型信頼への道

マレーシアのMyDigital ID構想は、公共・民間の両サービスへのアクセスを簡素化することを目的とした、国主導の統合デジタルID枠組みへ向けた重要な一歩である。2024年にデジタルIDブループリントの下で開始されたこの制度では、国家登録局（NRD）のデータベースにひも付いた生体情報連動型のデジタル資格情報を各居住者に付与する 。顔認識と安全な認証を使用することで、個人は電子政府ポータル、銀行、通信事業者、その他のオンラインサービスで本人確認をすることができる。内国歳入庁（LHDN）と一部の金融機関とのパイロット運用を経て、2025年の全国展開が予定されている [34]。

従来のID制度とは異なり、MyDigital IDは資格情報であると同時に検証レイヤーとしても機能する設計であり、個人情報を繰り返し開示することなく認証を可能にする。検証済みの生体情報記録に基づいてIDを確立することで、PoH型の検証に近い要素を備え、各デジタルアカウントが実在する一意の個人に対応することを保証する。分野横断的にデジタル検証を拡張する中で、マレーシアも他国と同様、完全な身元開示が現実的でも望ましくもない、ユーザー主導のオープン環境に信頼をどう拡張するかという課題に直面している。この意味で、MyDigital IDは将来的に、プライバシー保護と相互運用性を両立しつつ人間であることと一意性を確認するPoH型の仕組みの基盤となり得る。

この取り組みは、モバイルバンキングや電子商取引の普及に伴って増加している詐欺やデジタル不正への対応でもある。信頼できるIDレイヤーは、規制されたエコシステム内でのなりすましや偽アカウントの抑制に寄与し得る。また、PoH型の検証は将来的に、オンラインマーケットプレイス、ソーシャルメディア、デジタル決済など、詐欺が多く発生する非規制領域にも保護を拡張できる可能性がある。

しかし、その導入はプライバシー、データ保護、ガバナンスをめぐる公的な議論を引き起こしている。市民社会団体は、生体情報の中央集約的保管や、想定外の目的へデータ利用が拡大された場合の誤用の可能性に懸念を示している [35]。これに対し政府は、デジタルID運営委員会を設置し、個人データ保護法（PDPA）への遵守を再確認するとともに、中央銀行の監督下にあるMySejahteraやeKYC制度との相互運用性を強調している [36] 。これらの措置は、透明性、説明責任、社会の信頼を確保しながら実装を進めることを目的としている。

明確なセーフガードとユーザーによるコントロールが確保されれば、MyDigital IDはPoHイノベーションのための信頼の高いID基盤へと発展し得る。検証済み生体情報、ユーザー同意、安全な相互運用性を組み合わせたそのアーキテクチャは、新興国がデジタル信頼枠組みにおいて一意性と包摂性をどのように組み込めるかを示している。東南アジアにとって、マレーシアの経験は、ガバナンス主導のID整備が従来型デジタルIDと将来のPoHモデルとの間のギャップを埋め、プライバシーと社会の信頼を維持しながら詐欺耐性を強化する可能性を示唆している。

フィリピン：PhilSysの迅速な展開

フィリピン身分証明制度（PhilSys）は、東南アジアで最も迅速に展開されたデジタルID施策の一つとなっている。2018年に共和国法第11055号に基づき創設された制度で、国民および居住者一人ひとりに、生体情報（顔認証、指紋、虹彩）に裏付けられた12桁の固有のPhilSys番号（PSN）を付与する。[37] 制度はフィリピン統計庁（PSA）が管理しており、公共サービスへのアクセス向上、金融包摂の促進、安全なデジタル取引の実現を目的としている。2025年末までに8,000万人超のフィリピン人が登録し、デジタル版ID（eGovPHアプリおよびnational-id.gov.phを通じて利用可能）は政府機関、銀行、民間プラットフォームにおいて広く受け入れられるようになっている。[38]

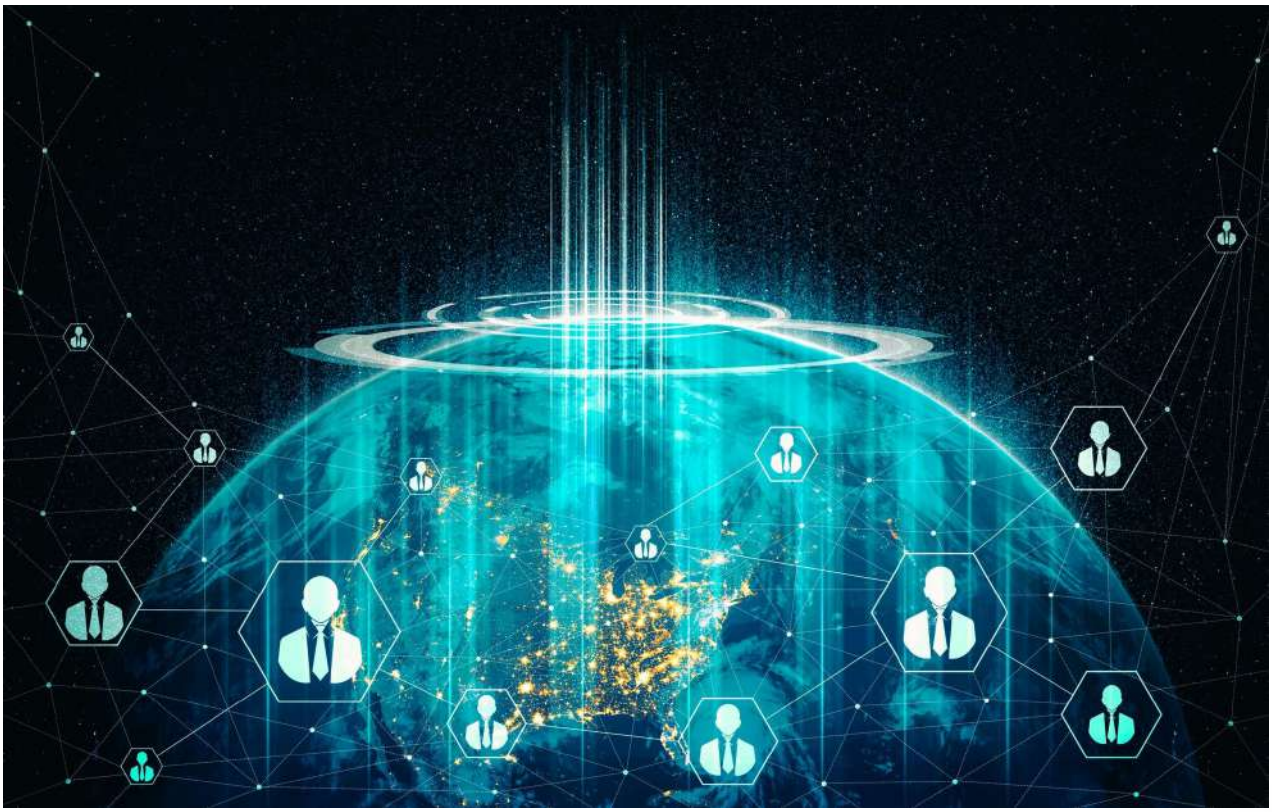
この急速な展開は、信頼できるID基盤の構築という地域的課題における重要な節目である。検証済みの生体情報を恒久的かつ一意の識別子にひも付けることで、PhilSysは重複登録や合成IDを防ぐ、公的制度を基盤とする一意性証明レイヤーを実質的に形成している。金融機関、通信事業者、政府システムとの統合は、PoHの大規模導入の先行事例となっており、検証済みユーザーが実在する一意の個人であることを確認する機能を果たしている。QRコードによるリアルタイム認証を可能にするeVerifyポータルは、この保証をデジタル決済、社会的保護制度、SIM登録へと拡張している。[39]

一方で、急速な導入は新たなガバナンスおよびプライバシー上の課題も浮き彫りにしている。技術的エラー、カード発行の遅延、データ取扱いに関する問題は社会の注目を集め、中央集約型の生体情報保管や不透明なデータ共有に対する懸念から、より強固なセーフガードを求める声も上がっている。[40] これに対し、PSAおよび国家プライバシー委員会（NPC）は監督体制の強化、暗号化基準の厳格化、eGovPH枠組みにおける同意ベースのアクセス管理の組み込みなどを進めている。[41]

フィリピンの事例は、急速なデジタル信頼基盤の拡張がもたらす可能性とリスクの双方を示している。その規模と相互運用性は、新興国が検証済みIDインフラへと一足飛びに移行し、金融包摂と不正防止を推進できることを示している。他方で、信頼は技術とともに進化しなければならないことも明らかである。社会の信頼は、可視的な説明責任、透明性の高いデータガバナンス、ユーザーによるコントロールに依存している。PhilSysの成熟過程は、PoHと整合的なイノベーションを検証する貴重な試金石となっており、強固なプライバシー保護および包摂のセーフガードと組み合わされた「検証された一意性」が、東南アジアのデジタル経済における詐欺耐性と人間中心の信頼を強化し得ることを示している。

ケーススタディからの示唆

取り上げた4つの事例は、アジア各国がいかに異なる経路を辿って一意性証明の基盤を構築しているかを示している。日本と韓国は、先進的な規制環境の下で、検証済みIDを大規模に制度化することが可能であることを示している。ただし、その帰結は対照的である。日本のマイナンバー制度は、データガバナンスが揺らいだ場合に社会の信頼が脆弱になり得ることを示している。一方、韓国の実名制度は、ID、金融、テクノロジーの高度な統合がもたらす効率性を示す一方で、そのリスクも浮き彫りにしている。東南アジアに目を向けると、マレーシアのMyDigital IDとフィリピンのPhilSysは、新興国における2つのモデルを提示している。前者はガバナンスを設計段階から組み込む慎重なアプローチを重視し、後者は迅速な展開とアクセス拡大を優先する戦略を採っている。4事例に共通して見られるのは、PoHに類する検証メカニズムは、透明性、相互運用性、ユーザーによるコントロールと組み合わされたときに最も効果的に機能するという点である。デジタルID制度はオンラインの安全性に対する社会の信頼を損なうのではなく、むしろ強化する必要がある。



結論および提言

詐欺およびオンライン不正は、アジア太平洋地域におけるデジタル信頼を左右する重大な脅威となっている。日本のマイナンバー制度からフィリピンのPhilSysに至るまで、各国のデジタルID制度は、検証可能で包摂的なアイデンティティの確立という目標を前進させてきた。しかし、それらは主として行政目的のツールであり、リアルタイムの不正防止を目的とした仕組みではない。新たに登場している人間であることの証明（PoH）技術は、こうした制度を補完する重要な層を提供する選択肢の一つとなりうる。すなわち、デジタルプラットフォーム、金融サービス、通信ネットワークにおいて、個人識別情報を開示することなく、「実在する一意の人間である」ことを証明することを可能にするアプローチである。プライバシーを保護しつつ人間であることの証明を付加することで、従来のデジタルID制度では検知が想定されていなかった自動化・大規模化された不正行為に対処することができる。したがって、PoHをデジタルIDエコシステムに統合することは、強固なプライバシー保護を維持しながら、詐欺への耐性を高め、デジタル取引に対する社会の信頼を強化することにつながり得る。

「セーフガードとガバナンス」のセクションで強調したように、責任あるPoHの導入には、リスクに応じた設計、明確なユーザー保護、既存のIDエコシステムとの慎重な整合が必要である。これらの原則を踏まえ、域内各国政府は次のような取り組みを進めることができる。

- **デジタルIDとPoH技術を詐欺対策戦略に統合する：** 金融、電子商取引、通信プラットフォームに一意性証明を組み込み、なりすまし、ボット主導の不正、合成IDのリスクを低減する。同時に、導入はリスクに見合った範囲で行い、利用者に過度な負担を与えず、ISO/IEC 25389などの既存の安全枠組みに整合する形で実施する。

- **プライバシー保護型かつ相互運用可能な標準を支援する：** 生体認証による確実性と暗号技術によるプライバシー保護を組み合わせた地域的枠組みの策定を促進する。これにより、検証された一意性がユーザーの匿名性や越境利用の可能性を損なわないようにするとともに、**PoHシグナルが追跡やプロファイリングに転用されないことを確保する。**

- **地域的な政策対話と協調を促進する：** APECビジネス諮問委員会、「デジタル金融包摂に関するG20ハイレベル原則」、国連のデジタル経済関連イニシアチブなど既存の枠組みを活用し、政策目標の整合、ベストプラクティスの共有、PoH対応型認証の分野横断的なパイロット枠組みの検討を進める。あわせて、高リスク環境での限定的なサンドボックスを通じ、政府やプラットフォームが本格導入前にPoHを検証できる環境を整備する。

これらの取り組みを総合的に進めることにより、アジアにおいて信頼度が高く、人間中心のデジタルエコシステムの構築に資することが期待される。すなわち、検証がプライバシーを損なうことなく安全性を強化し、セーフガードとガバナンス枠組みが責任ある活用を担保し、地域協力によってID制度が単なる行政登録基盤から詐欺耐性とデジタル包摂を支える能動的なインフラへと進化することにつながり得る。

参考文献

[1] Cybersecurity Ventures. n.d. "The World's Third Largest Economy Has Bad Intentions—And It's Only Getting Bigger." Accessed August 2025. https://cybersecurityventures.com/the-worlds-third-largest-economy-has-bad-intentions-and-its-only-getting-bigger/.
[2] Feedzai. 2024. "GASA Global State of Scams Report: $1T Lost to Scams." Accessed August 2025. https://www.feedzai.com/blog/gasa-global-state-of-scams-report-1t-lost-to-scams/.
[3] GSMA. 2025. Fraud and Scams Safety Report. London: GSMA. https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2025/02/Fraud-and-scams-safety-report.pdf.
[4] UNODC, Inflection Point: Global Implications of Scam Centres (2025), p. xx, https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf
[5] Global Initiative, CRIME CYBER SCAM OPERATIONS IN SOUTHEAST ASIA (May 2025), https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf
[6] "A New Human Trafficking Trend Emerges from Myanmar," The Japan Times, April 2, 2025, https://www.japantimes.co.jp/news/2025/04/02/japan/crime-legal/myanmar-scam-human-trafficking/
[7] "They were forced to scam others worldwide. Now thousands are detained on the Myanmar border," AP News, March 9, 2025, https://apnews.com/article/myanmar-thailand-scam-centers-trapped-humanitarian-c1cab4785e14f07859ed59c821a72bd2
[8] Signicat. 2024. "Fraud Attempts with Deepfakes Have Increased by 2137% over the Last Three Years." Accessed August 2025. https://www.signicat.com/press-releases/fraud-attempts-with-deepfakes-have-increased-by-2137-over-the-last-three-year.
[9] CSIS, Cyber Scamming Goes Global: Unveiling Southeast Asia's High-Tech Fraud Factories, December 12, 2024, https://www.csis.org/analysis/cyber-scamming-goes-global-unveiling-southeast-asias-high-tech-fraud-factories
[10] TRM Labs, The Illicit Crypto Ecosystem Report (2022), https://www.trmlabs.com/resources/reports/the-illicit-crypto-ecosystem-report-2022.
[11] Meta, "Cracking Down on Organized Crime Behind Scam Centers," November 21, 2024, https://about.fb.com/news/2024/11/cracking-down-organized-crime-scam-centers/
[12] TRM Labs, 2025 Crypto Crime Report, https://www.trmlabs.com/reports-and-whitepapers/2025-crypto-crime-report
[13] World Bank, Digital Identity Toolkit (World Bank), section on credential and smart card-based eIDs. https://documents1.worldbank.org/curated/en/147961468203357928/pdf/912490WP0Digit00Box385330B-00PUBLIC0.pdf
[14] Financial Action Task Force (FATF), Guidance on Digital Identity (Paris: FATF/OECD, March 2020), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity.pdf (discussion of biometric authentication as part of digital ID assurance).
[15] SITA and PRISM, Biometric Digital Identity: The Next Step in Seamless Travel and Government Services (2023), https://www.sita.aero/globalassets/docs/other/biometric-digital-identity-govt-services-prism-report.pdf
[16] OECD, National Digital Identity (NDID) Platform (Thailand), https://www.oecd.org/content/dam/oecd/en/topics/policy-issues/tax-administration/thailand-national-digital-identity-platform.pdf
[17] "Digital Identity Spotlight: Singapore," 1Kosmos, https://www.1kosmos.com/identity-management/digital-identity-spotlight-singapore/
[18] "Digital identity systems around Asia compared as Taiwan seeks path forward," BiometricUpdate, https://www.biometricupdate.com/202102/digital-identity-systems-around-asia-compared-as-taiwan-seeks-path-forward
[19] Kleros, Proof of Humanity (PoH) Documentation, "Proof of Humanity (PoH) is a sybil-resistant registry of humans, combining social verification with video submission to create a trusted list of real humans," https://docs.kleros.io/products/proof-of-humanity
[20] Government of Japan, Cabinet Office, "Outline of the Social Security and Tax Number System (My Number System)," 2016, https://www.cao.go.jp/bangouseido/english/.
[21] Ministry of Internal Affairs and Communications (MIC), "Overview of the Social Security and Tax Number System," updated 2024.

[22] Digital Agency of Japan, My Number Card Statistics Portal, "Number of My Number Cards Issued," updated October 2025; "Japan's My Number cards hit 90m issuance but trust issues persist," Nikkei Asia, 12 July 2025.
[23] "Japan suspends some My Number links after health-insurance data mix-up," Reuters, 28 May 2023
[24] "Japan aims to link My Number to banking and SIM registration," Japan Times, 9 March 2024.
[25] "Fix the flaws in the My Number system," Japan Times (editorial), 2 June 2023; Digital Agency, "Efforts to Enhance Trust in the My Number System," 2024.
[26] Ministry of the Interior and Safety (MOIS), "Overview of the Resident Registration System," Government of the Republic of Korea, 2023.
[27] Korea Communications Commission (KCC), Real-Name Verification Policy in the Digital Environment, 2022.
[28] Ministry of Land, Infrastructure and Transport (MOLIT), "Launch of the Mobile Driver's License Service," press release, January 2022.
[29] Korea Internet & Security Agency (KISA), "Status of Digital Authentication Use in Korea," 2024; Yonhap News, "PASS App Surpasses 50 Million Users in Korea," 9 May 2025.
[30] OECD, Digital Government in Korea: Enabling a Smart and Inclusive Society, 2023, p. 45.
[31] Korea JoongAng Daily, "Massive Data Leaks Raise Questions About Security Practices," 4 February 2023; Korea Times, "Credit Bureau Fined over Data Breach Affecting Millions," 15 April 2023.
[32] MOIS, "Digital Identity Pilot Project for Secure Authentication," 2023; Personal Information Protection Commission (PIPC), "Amendments to the Personal Information Protection Act," December 2023.
[33] Malaysia Digital Economy Blueprint (MyDIGITAL), Digital Government Division, Ministry of Communications and Digital, "Digital Identity Blueprint," Government of Malaysia, 2024.
[34] Department of National Registration (Jabatan Pendaftaran Negara, JPN), "Implementation of MyDigital ID Pilot with LHDN and Financial Institutions," press release, June 2024.
[35] Malay Mail, "Privacy Advocates Raise Concerns over Centralised Biometric Database," 5 April 2024.
[36] Ministry of Communications and Digital (KKD), "Formation of Digital ID Steering Committee," 15 February 2024; Bank Negara Malaysia, e-KYC Implementation Guidelines, revised 2023.
[37] Republic Act No. 11055, "An Act Establishing the Philippine Identification System (PhilSys Act)," Official Gazette of the Republic of the Philippines, August 2018.
[38] Philippine Statistics Authority (PSA), PhilSys Dashboard: Registration and Issuance Data, updated October 2025; Inquirer.net, "Over 80 Million Filipinos Registered for National ID—PSA," 14 September 2025.
[39] PSA, "PhilSys eVerify Portal Launch and QR Verification Capabilities," 2024.
[40] Rappler, "Privacy Concerns Mount over National ID Data Sharing," 22 June 2024; Philippine Star, "National ID Delays, Data Glitches Spur Criticism," 10 May 2024.
[41] National Privacy Commission (NPC), "NPC Advisory on Data Protection Standards for the National ID System," 2024; PSA, "Enhanced Security Measures for ePhilID Rollout," 2024.