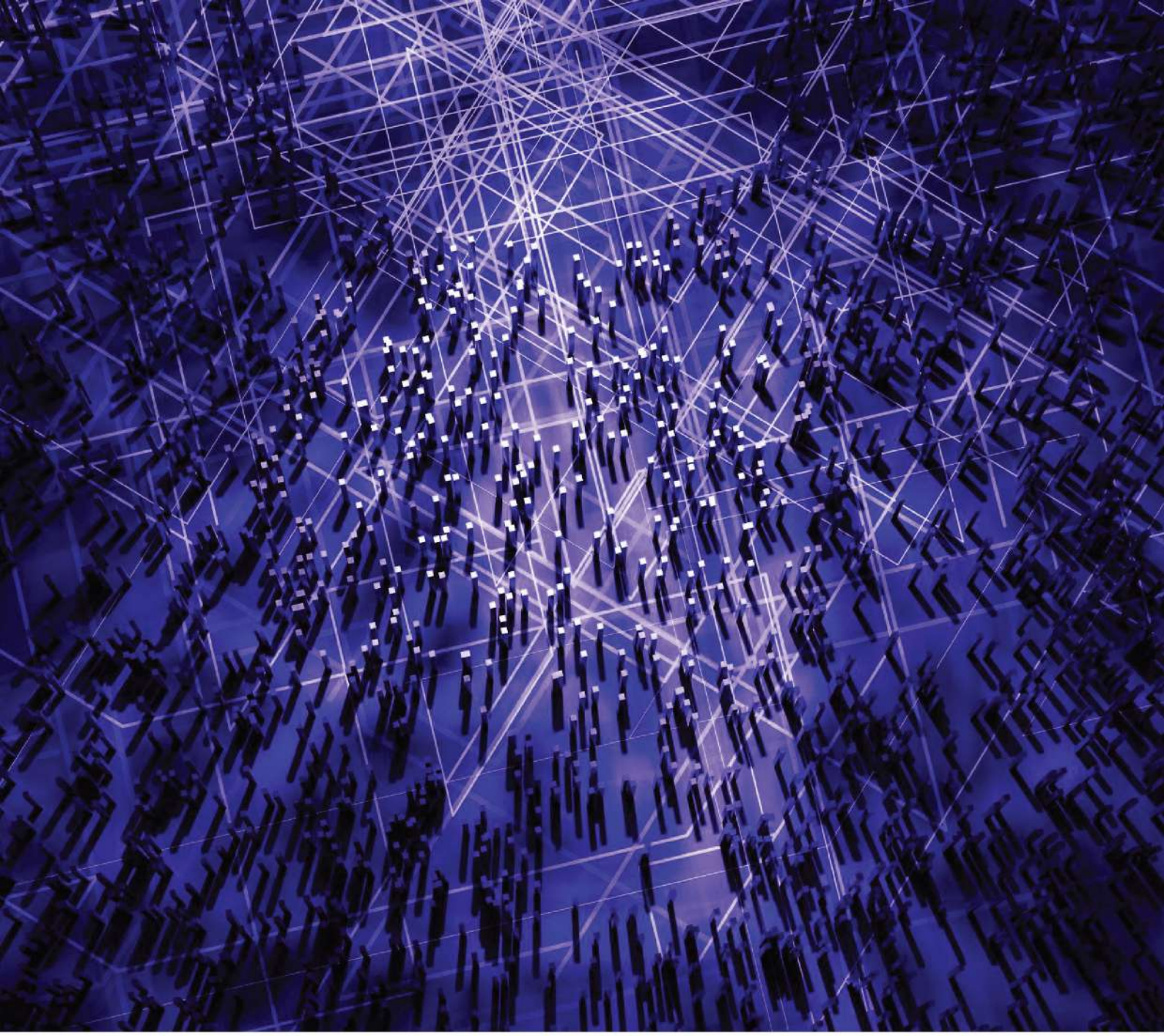


人類證明

在亞太地區建構數位信任與詐騙韌性的人類網絡架構

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

關於本白皮書

本白皮書由東南亞公共政策研究所（Southeast Asia Public Policy Institute）與日本信任與安全協會（JTSA）合作，並在人類工具（Tools for Humanity）的支持下共同研究撰寫，旨在探討亞太地區之數位信任現況。

本白皮書所呈現的資訊和分析,基於對相關利害關係人的訪談、公開資訊以及作者專業分析。JTSA 所提供之策略性貢獻，特別是田中清隆關於治理、互操作性和風險導向的「人類證明」（Proof of Humanity, PoH）實施架構所提出之見解，對本白皮書之形成具有重要助益。

本白皮書內容不代表人類工具之立場。本文件亦非針對特定政策、立法或法規進行全面性法律評析，使用時應審慎理解其範圍與限制。

目錄

執行摘要

網路詐騙已發展為高度產業化、跨境運作之犯罪活動。全球網路犯罪經濟規模現已超過 10 兆美元，每年因詐騙造成的經濟損失超過 1 兆美元。除此之外，詐騙行為亦對受害者心理健康造成長期衝擊、削弱公眾對數位服務之信任，並大量消耗執法與監理資源。

亞太地區同時為詐騙活動主要受害市場與運作樞紐。東南亞地區存在大規模的詐騙活動，其運作往往涉及人口販運；日本和韓國等先進市場則面臨投資詐騙與身分冒用詐騙之顯著增加。這個問題具有區域連動性，亟需跨經濟體協調因應。

人工智慧（AI）擬聲／語音克隆、深度偽造技術加速詐騙手段專業化與規模化；自動化帳戶建立機制使詐騙者能低成本大量接觸潛在受害者；加密貨幣和即時支付系統則加速資產變現，降低攔截機會。

然而，同樣的科技亦可透過強化完善數位身分驗證、鑑別訊號和隱私保護措施來增強信任。前提在於必須建立明確之治理架構與透明機制，以避免新興技術被濫用。

- 現行執法與宣導措施雖屬必要，但不足以因應大規模合成身分與自動化濫用問題。可持續之反應機制，需建立雙層數位信任架構：

數位身分（數位 ID）： 回答「你是誰？」的問題，適用於受監管環境（金融、電子化政府）的非匿名、KYC（認識你的客戶 / 客戶盡職調查）憑證。

- **人類證明（PoH）：** 回答「你是獨一無二的真人嗎？」的問題，可於開放的跨平台環境中使用的隱私保護訊號，在這些環境中，身分的完全揭露既不需要也不可取。

PoH 不能取代數位身分，而是一個補充層。其目的在於將信任擴展到網路上大多數詐騙活動發生的區域（社交、即時通訊、市場），在保護用戶隱私的同時，減少虛假或合成帳戶和機器人驅動的濫用行為。最近的發展強調有必要在基於信任和安全的框架內部署 PoH，並需確保它能夠應對自動化和大規模濫用，而不是被誤解為使用者意圖或可信度的保證。

在亞太地區，各國政府已建構起強大的數位身分體系，加強了受監管產業的 KYC 和問責制。然而，大多數詐騙活動源自於社群媒體、即時通訊和網路商場等未受監管的區塊，而數位身分並不適用於此。PoH 的獨特價值正體現在此：透過隱私保護型人類符記和基於設備的驗證等機制，PoH 可以限制大量虛假帳戶的創建，打擊機器人驅動的詐欺活動，並在受害者成為目標之前，加強真實的人類網絡。為了確保這些技術的成功應用，需要明確的安全保障、使用者控制權和治理結構，以防止濫用、保護匿名性並維護公眾信任。

案例概覽

• 日本 — 個人編號（My Number）： 國家驗證的獨特性已實現大規模應用，但數次資料處理事件對其信任度構成挑戰；可能作為混合模型的基礎起點，將政府身分證與隱私保護身分驗證相結合，用於政府服務以外的隱私保護驗證。

• 韓國 — 實名制： 金融、電信和電子化政府的深度整合有效地成為 PoH 代理機制；但隱私 / 公民自由方面的擔憂制約了其成功，從而推動了用戶控制、去中心化身分驗證的發展。

• 馬來西亞 — 國家數碼身份（MyDigital ID、推廣中）： 與國家註冊系統聯繫的生物辨識憑證；經設計的治理之路徑與隱私權保護身分驗證原則高度契合，但需要有力的保障措施和公眾信任才能實現規模化。

• 菲律賓 — 菲律賓身分識別系統 （PhilSys、快速擴展）： 透過數位身分下載和電子驗證實現快速大規模普及；展示了類似 PoH 的運作功能，同時也需要維持治理和使用者教育的同步發展。

有效的詐騙韌性需要多層保障：受監管的互動與已驗證的身分掛鉤，以及由保護隱私的人類證明機制加固的開放平台。透明度、互操作性和使用者控制是貫穿始終的關鍵要素。中立的治理機制，無論是標準制定機構、業界中介機構或是多方利益相關者框架，對於將國家要求轉化為全球平台的營運實踐至關重要。

政策建議

• **將數位身分和 PoH 融入防詐騙策略：**在金融、電子商務和通訊流程中嵌入獨特性檢查，以遏制身分冒用、合成身分和機器人濫用，並以信任和安全為導向進行部署，同時採取保障措施防止過度依賴。

• **支援保護隱私且可互操作的標準：**將生物辨識 / 憑證認證與加密技術（例如零知識證明）結合，在適當情況下保護匿名性並實現跨境可用性，同時確保 PoH 不會被挪用於追蹤或剖繪使用者。

• **促進區域政策對話與協調：**利用 APEC 企業諮詢委員會、G20 數位普惠金融高級原則和聯合國數位經濟倡議等平台，協調目標、分享證據，並在各領域試行基於 PoH 的驗證，包括沙盒測試，以評估可用性、包容性和比例性。

詐騙暴露了結構性的信任赤字。將數位身分和 PoH 架構結合，並輔以強大的隱私保護、治理和互操作性，可以大規模提高濫用成本，同時保護使用者權利，加速亞洲邁向更安全、更包容的數位經濟之路。

引言：網路詐騙的氾濫與政策缺口

隨著社會和經濟擁抱數位科技，網路犯罪的規模和複雜程度也呈現爆炸性成長。全球網路犯罪經濟規模現已超過 10 兆美元，相當於全球第三大經濟體（以 GDP 計算）。[1] 詐騙是一種特殊的、日益猖獗的網路犯罪，消費者每年因詐騙損失超過 1 兆美元。[2] 然而，其代價遠不止於此：受害者的心理健康和福祉遭受長期損害，人們對數位服務和數位經濟的信心受到削弱，公共資源也被轉移到執法、宣傳和國家網路安全工作。[3]

亞洲的雙重角色

在全球詐騙猖獗的背景下，亞太地區影響最為嚴重。所謂的「殺豬盤」騙局、投資詐騙或愛情詐騙尤其猖獗。詐騙分子利用社交工程技術與受害者建立聯繫，誘騙其付款或投資。這些詐騙活動通常透過社群媒體或即時通訊服務發起，由跨國犯罪集團經營的專門詐騙中心進行大規模詐騙活動。

東南亞處於這經濟體系的中心：既是詐騙受害者的來源，也是向非監管地區進行詐騙活動的樞紐。同時，此區域也是勞動力的來源地，其中許多人也是人口販運的受害者。[4,5]

同時，亞太地區的先進市場，例如台灣、日本和韓國，也與此情勢密切相關：這些經濟體信任度高、數位化程度高，其消費者經常成為投資詐騙和身分冒用詐騙的目標，而且這些經濟體的公民也曾被誘騙至海外詐騙中心[6] 這些情勢共同突顯了該地區的危機不僅是局部性的，也是整個亞洲相互連結的挑戰之一部分，需要先進經濟體和受人口販運影響的國家共同採取協調一致的應對措施。[7]

科技：既是推動者，也是解決方案

科技從根本上改變了詐騙的經濟模式，即使是資源最豐富的政府也難以跟上詐騙手段的快速演變。首先，說服手段已經產業化。人工智慧、語音克隆和深度偽造正被武器化，用於實施詐騙：超過 42 % 的金融領域詐騙企圖與人工智慧有關。[8] 這些工具可以提供高度逼真的腳本、圖像和多語言通話，使得相對缺乏經驗的操作者能夠按照經過 A/B 測試優化的劇本，實施長期的「投資」或愛情騙局。

其次，規模化幾乎已趨近於無限：自動建立帳戶、SIM 卡農場和跨平台工具使小型團隊能夠在幾小時內透過社群媒體、即時通訊和電話聯繫數百萬人，同時還可以利用機器人和推薦系統來識別易接受的受眾。 [9]

第三，犯罪者在資產變現方面的創新手段不斷加速。加密貨幣基礎設施、金融科技管道、車手網絡和跨鏈混合器使得資金能夠快速轉移和混淆，而即時支付和分散的 KYC/KYB 機制則縮小了傳統銀行的攔截窗口。[10]

結果是數位經濟中存在結構性信任赤字：犯罪分子採用和調整新工具的速度，遠超過政府和監管機構的反應速度。

然而，如果大規模部署並輔以安全保障措施，這些助長濫用的科技也能重建信任。

• 更強大的數位身分和實體保障，包括對個人、設備和企業進行隱私保護驗證，SIM 卡 / 號碼信譽，以及針對高風險流量提供更高保障的選項，都可以提高大規模定向攻擊的成本。

• 內容和通訊的真實性訊號，例如圖像和視訊的加密溯源、語音和訊息的已驗證來電者/寄件者框架，以及強化的廣告和帳戶完整性控制，則可以降低身份冒用的成功率。

• 跨平台和支付網路的隱私保護訊號共享有助於檢測組織性濫用，而即時支付風險評分和「冷卻期」摩擦成本機制（確認收款人、加強審核、延遲結算可疑轉帳等）可以在執行環節減少損失。

• 以受害者為中心的模型—快速取締途徑、更快的資金追回機制以及明確識別受脅迫工人為受害者的途徑—必須與執法相輔相成，才能打破剝削的循環。[11]

因此，科技既是犯罪活動的驅動，也是解決問題必要的一部分。政府、平台和金融機構必須以與犯罪分子創新速度相同的速度不斷採用和更新防禦科技，因為詐騙不僅是網路犯罪事件，更是數位經濟中更深層結構性信任缺失的徵兆。[12]

如果詐騙暴露了網路信任的脆弱性，那麼可靠的數位ID就是修復這種脆弱性的最有效工具之一。數位身分透過提供可驗證的交易或互動背後的真實身分訊息，提高了濫用行為的成本，同時支持更安全的數位經濟。下一節將探討數位身分旨在解決的問題、相關科技以及正在該區域出現的政策應對措施。

數位信任的兩層架構：數位身分與人類證明

打擊詐騙需要多層信任體系。執法和提高大眾意識至關重要，但永續的進展取決於身分和認證機制，其能夠堵住犯罪分子大規模利用的漏洞。數位ID 和 PoH 代表了這種信任基礎設施的兩個互補、但本質上不同的層面。數位身分透過將個人與銀行和政府認可的、經過驗證的真實身份聯結起來，回答「你是誰？」這個問題；而人類證明則透過在不洩露身分的情況下確認人性及其獨特性來回答「你是人類嗎？」這個問題。數位身分是非匿名的，適用於銀行和電子化政府等受監管的環境；而人類證明是匿名但可驗證的，用於保障開放的數位空間，在這些空間中，完全揭露身分既不需要，也不可取。兩者共同建構了一個平衡的基礎，既支持數位經濟中的問責制，也支持隱私保護。

人類證明不能取代國家數位身分系統；它是補充性的、保護隱私的一層，可以將信任擴展到數位環境中，那些完整的身份驗證既不可行，也不可取的區塊。

科技：既是推動者，也是解決方案

數位身分解決方案有多種形式，每種形式都針對不同的風險：

- **基於憑證的數位身分系統**依賴數位化核發且可驗證的憑證。這些憑證通常源自政府核發的身分證件或銀行、電信業者或大學等可信任機構，用於安全地驗證姓名、年齡或國籍等身分屬性。這些憑證可以儲存在數位錢包中，並在各種服務中使用，從而實現可重複使用，且保護隱私的數位互動，其安全性遠高於簡單地將掃描文件連結到登入憑證。[13]

- **生物辨識認證透**過指紋或臉部特徵等獨特的生理或行為特徵，驗證使用服務的人士是否與先前註冊的人士相符。即使密碼或裝備等其他憑證外洩，生物辨識認證也能有效防止未經授權的存取。需要注意的是，生物辨識驗證使用者身份，本身並不能確認其身分。[14]

- **混合數位身分模型**結合了多種要素，例如政府頒發的憑證和生物辨識驗證，以創建可重複使用、高安全性的數位身分。這些系統旨在支援跨平台互操作性、高強度身份驗證和隱私控制。[15]

所有系統均支援 KYC 功能，且從設計上為不匿名，因為它們旨在確保受監管生態系統內的可追溯性、合規性和問責制。

亞太地區的政策應對

數位身分科技無法單獨地成功；它們需要相應的政策框架來制定標準、保障隱私並促進廣泛應用。在實踐中，這意味著：

- 明確的監管認可，使數位身分在金融交易、合約和公共服務中具有法律效力。
- 健全的保障措施來保護個人數據，包括對安全儲存、限制使用、以及在發生濫用時提供補救機制的需求。
- 公私和跨業界之採用，確保不僅政府認可數位身分，而且平台、銀行和公用事業機構（這些機構往往處於詐騙的第一線）也認可其身分。

在整個東南亞地區，各國政府正穩步推動數位身分系統，將其作為建立更值得信賴的數位經濟的基礎。

- 泰國的國家數位身分（NDID）平台將銀行、電信業者和政府機構連接在一個聯邦框架內。[16]

- 印尼和菲律賓正在推行與普惠金融和社會服務相關的國家電子身分計畫。

- 越南已開始在其電子化政府入口網站嵌入生物辨識驗證。

儘管成熟度各不相同，但區域政策的重點正從建構國家系統，轉向探索互操作性。政策制定者日益認識到，人口流動、移民和貿易往來需要能夠跨境識別的身份證明，而不是僅在國內有效。在較先進的經濟體中，全面的國家認同框架已經建立，並正朝著更深層的整合方向發展。

- 新加坡的 SingPass 是存取銀行、醫療保健和電子商務的基礎。[17]

- 韓國正將其國民登記系統擴展為一個完全數位化的身份平台，該平台整合了電子化政府服務、金融交易和手機身分驗證。

- 日本的 My Number 系統為每位居民提供一個唯一的 12 位數字識別符，該標識符正日益與醫療保健、稅務和行政服務連結。[18] 日本目前也在努力將其應用範圍擴展到金融服務和跨境身分識別。

這些發展軌跡在範圍和速度上各不相同，但它們共同展現國家級身份驗證如何超越安全登入，發展成為數位經濟制度的支柱。同時，也可為考慮國內實施或區域互操作性的東盟各國政府模式提供參考。

同時，這些經驗也突顯了僅靠政府行動是不夠的。數位身分的有效性最終取決於其與更廣泛的數位生態系統的整合，而這需要政府、金融機構和科技平台之間的合作。

數位身分在打擊詐騙中的角色

數位身分科技是在打擊詐騙和詐欺時，最有前景的系統性工具之一。透過以可驗證、非匿名的方式對個人、裝置和組織進行身份驗證。數位身分系統可以減少身分冒用、限制匿名性並提高濫用的成本。雖然並非萬能靈藥，但它們構成了具備 KYC 功能的數位信任基石，確保受監管的交易和服務與真實、可問責的個人或實體掛鉤。

填補詐騙分子利用的漏洞

詐騙活動正是利用驗證漏洞滋生。詐騙分子利用機器人和虛假帳戶以極低的成本傳播訊息，部署深度偽造和語音克隆來冒充可信任人士，並劫持合法帳戶來欺騙受害者。跨平台身份驗證的薄弱或不一致意味著這些攻擊的成功率遠高於預期。

數位身分在監管方面填補了這個漏洞：透過將數位互動與已驗證的身分綁定，犯罪者更難匿名作案，而受害者、企業和監管機構則更容易信任與他們在網路上交易的對象。然而，大多數詐騙活動都源自於不受監管的領域，例如社群媒體、即時通訊應用和非正式商場，而 KYC 系統在此並不適用。應對這些環境需要不同的、保護隱私的方法，例如「人類證明」。

然而，即使是最強大的數位身分系統也無法完全解決由虛假帳戶和自動化濫用引發的詐騙問題。這種差距促使人們對「人類證明」等新興概念產生了濃厚的興趣，這些概念探索在無需個人識別的情況下，驗證用戶真實性的隱私保護方法。

人類證明：概念與政策意義

「人類證明」的定義

人類證明（PoH）代表了一種新興且不斷發展的增強數位信任的方法。它通常被定義為一種旨在防止多個虛假身份的系統，提供可驗證的保證，確保線上行為者是真人而非自動化機器人或偽造身份。[19] 與簡單的帳戶註冊或人機驗證不同，PoH 旨在提供一種持久、可重複使用的人性訊號，該訊號可以在不同平台和服務中被識別，並無需揭露不必要的個人資料，從而為在數位生態系中，奠定更值得信賴的人類網絡之基礎。

重要的是，PoH 不會取代或與國家數位身分系統競爭。相反，它透過解決信任問題的不同層面來補充這些系統，驗證使用者是否為真人，而不是確認使用者是誰。

從概念上講，PoH 與其他數位安全保障機制有所不同。傳統的數位身分框架透過將個人與姓名或國民登記號碼等已驗證屬性連結，來回答「你是誰？」這個問題。密碼或多要素驗證碼等身份驗證工具可以在帳戶建立後對其進行保護，但它們無法一開始就阻止虛假或合成個人資料的建立。近二十年來，人機驗證（CAPTCHAs）試圖透過測試使用者是否能夠解決謎題來彌補這一缺陷，以此作為判斷使用者是否為真人的指標。然而，隨著機器人和人工智慧工具的性能日益超越人類，此類驗證的有效性已逐漸下降，亦對合法使用者造成不便（摩擦成本）。相較之下，PoH 回答的是「你是真人嗎？」這個問題，這種安全保障形式與更廣泛的身份驗證、機器人攻擊防護、及區塊鏈社群所稱的「女巫攻擊防護」等功能相似。從這個意義上講，PoH 是旨在平衡數位生態系統中真實性、隱私性和可擴展性的一系列創新之一部分。

PoH 驗證的形式

人類證明系統可以透過多種方式實現，每種方式提供的安全性和隱私保護等級各不相同。以下表格概述了主要的 PoH 驗證形式及其實踐的運作方式。

PoH 驗證類型	運作方式	使用者體驗	應用範例
基於生物特徵（保護隱私）	一次性活體檢測（例如，眨眼/轉頭）。系統會發出一個加密的「人體符記」，無需儲存或共享生物特徵資訊。	類似於解鎖手機的簡短一次性驗證；不會洩露任何身份資料。	防止大量虛假帳戶；為處理金融或高風險交易的平台提供高安全性的 PoH。
基於裝置/硬體	設備認證確認其為真實、非模擬的設備；無需識別身分即可實現「一人一機」的綁定。	嵌入註冊流程的背景調查，無需生物特徵資訊。	限制機器人農場；減少即時通訊應用程式、社群媒體或遊戲平台中的自動帳號創建。
基於互動/挑戰	使用者完成類似活體偵測的提示或加密挑戰。機器人無法可靠地完成這些反應性任務。不使用生物辨識數據。	簡單的人機互動任務（例如，受控動作、定時提示），但跟傳統人機驗證比起更不會煩擾。	適用於社交平台和線上社群，無需身份或生物識別資訊即可阻止虛假帳號。
基於社交/信任網絡的認證	使用者由受信任的社群成員或信譽網路進行驗證；平台將此驗證轉換為 PoH 訊號。	來自已驗證使用者/社群的輕量級認可或確認。	適用於點對點市場、零工平台或社群為基礎的驗證環境。

表 3.1：人類驗證（PoH）的驗證形式

「人類證明」如何協助打擊詐騙

儘管 PoH 仍是一個新穎的概念，但它在打擊詐騙和詐欺方面具有潛在的價值。如今，網路詐騙的猖獗得益於規模效應：人口販運者和犯罪團夥創建成千上萬個虛假帳戶來誘騙受害者、自動化「殺豬盤」詐騙，或經營車手帳戶網絡。大規模、低成本地製造數位身分的能力降低了詐騙成本，同時也使平台和監管機構難以檢測惡意活動。相較之下，PoH 可以透過加強真實的人類網絡來改變這種局面，從而限制合成或自動化身分的大規模傳播。

原則上，PoH 可以在帳戶建立或交易環節設置摩阻點，從而限制虛假帳戶的擴散速度和規模。

可驗證的人性可以發揮以下幾個作用：

1. 防止虛假個人資料在愛情、求職或投資詐騙中作為誘餌。與其在受害者上當受騙後才被動地採取措施打擊詐欺帳戶，PoH 可以從一開始就減少詐欺帳戶的數量。

2. 減少透過車手帳戶進行的交易以**保護金融系統。**銀行和支付網路通常難以區分合法用戶和詐騙帳戶；可重複使用的人性化訊號可以加強現有的 KYC 和 AML 安全措施，而無需不斷揭露個人資料。

3. 增強人們對數位商務和線上社群的信任。在詐騙和冒名頂替行為侵蝕信任的市場中，能夠驗證買家、賣家或社群成員是否為真人，最終可能有助於恢復人們對點對點交易、零工平台和社交空間的信心。

保障措施與治理

保障措施至關重要，以確保 PoH 本身不會淪為監視工具。新興模型強調隱私保護設計。加密證明和零知識方法使用戶能夠在不洩露底層身分數據的情況下證明其人性。身分驗證（行為者是否為人類？）與身分揭露（行為者是誰？）之間的區別對於維護跨司法管轄區的權利和信任至關重要。保障措施還需要強力的治理：由監管機構、標準制定機構或多方利害關係人審核的監督有助於防止 PoH 訊號被挪用於侵入式追蹤或剖繪。

同時，使用者權利和包容性也是重要的。驗證應是自願的、透明的、可撤銷的，且個人能夠理解並控制其 PoH 訊號的使用方式。年齡驗證機制等輔助工具可以在無需揭露敏感資訊的情況下保護未成年人，而多種驗證途徑有助於避免將沒有智慧型手機、生物識別裝置或穩定網路的人排除在外。PoH 的公信力最終取決於它能否在尊重隱私、確保易取性，以及與區域數位信任承諾保持一致的前提下提升安全性。

然而，僅靠技術保障是不足的。有效的 PoH 部署需要能夠反映亞太地區數位生態系統實際情況的治理結構。國家數位身分系統遵循國內規則運作，而大多數真實的用戶互動，以及大多數涉及隱私敏感的風險，都發生在全球性平台上。由於這種結構性差距，政府與平台之間的直接整合往往難以實現。通常需要一個中立的治理層：獨立的互操作性中介機構能夠實踐需求、召集利害關係人，並在大規模應用之前支援安全測試。

這些中介機構可以協助確保以技術上可行、尊重隱私、且符合國家框架和跨平台環境的方式實施 PoH。它們可以將國內標準轉化為運作指南，主持多方利益相關者就隱私和可審核性的討論，並協助建立沙盒環境，使 PoH 能夠在不給用戶或平台帶來意外風險的情況下安全試用。

另一項保障與公眾信任有關。PoH 是一個新概念，不同於數位身份、身份驗證或 eKYC 。對此有誤解會很容易引發對監控或數據使用的擔憂。因此，能力建構與科技本身同等重要。中立的中介機構、產業組織和公民社會網絡可以協助解釋隱私保護設計的運作方式，並強調 PoH 回答的是「你是人類嗎？」這個問題，而不洩漏「你是誰？」，並提供負責任實施的實用指導。透過有效的溝通和使用者教育，精心設計的 PoH 系統最終能轉化為人們樂於接受的工具。

最後，PoH 必須嵌入一個信任和安全框架中。驗證使用者是真人並不能保證使用者的意圖是安全的。亞太地區許多最具危害性的詐騙，例如投資詐騙、身份冒用詐騙和長篇社交工程手段，都是由真人操作者實施的。因此，PoH 應該作為其他安全訊號的補充，而不是替代。應用 ISO/IEC 25389（安全框架）等框架有助於確保 PoH 的適當使用：

- 作為抵禦自動化和規模化攻擊的多層防禦之一；
- 與用於檢測人為威脅的行為和信譽訊號相結合；
- 提供清晰的實施指導，以避免過度依賴。

因此，PoH 不是替代系統，而應作為一項補充性創新，進行先導性推動，以加強現有的身份框架。如果設計和治理得當，它可以幫助測試在高風險數位環境中驗證真實用戶的新方法，並為更大規模的推廣應用提供證據。更廣泛地說，可互操作且尊重權利的 PoH 框架可以補充國家數位身分識別計劃，支持跨境身分識別，並為亞太地區打擊詐騙和詐欺的區域合作提供新的信任基準，也可幫助各國建立能夠抵禦現代網路犯罪規模和速度的、具有韌性、可驗證的人類網絡。下一節將探討亞太地區的國家層級經驗，以思考如何在實務中實施 PoH。

案例研究：先進科技的實踐

在亞洲，各國政府已建構起健全的數位身分基礎，用於驗證公民在公共和金融服務中的身分。然而，大多數詐騙活動發生在這些監管體系之外：在匿名性盛行的社交、即時通訊和內容平台上。

新興的PoH科技提供了一種將數位身分的可靠性擴展到這些開放環境的方法，在不洩露個人數據的情況下確認使用者的身分和獨特性。以下案例研究將探討日本、韓國、馬來西亞和菲律賓這四個經濟體如何透過其國家系統建構類似 PoH 的驗證要素，以及它們的經驗帶給未來於詐騙韌性策略的啟示。

日本：個人編號（My Number）系統與信任挑戰

日本的 My Number 系統於 2016 年啟動，為每位居民分配一個獨特的 12 位數識別碼，用於稅務、社會安全和災害應變等用途。[20] 該系統旨在統一行政數據並提高效率，並透過 My Number 卡擴展到數位領域 - 一種智慧身分證，可為電子政府服務、醫療保健和金融交易提供安全的線上身分驗證。[21] 至 2025 年，已發行超過 9 千萬張 My Number 卡，覆蓋超過 70 % 的人口。然而，由於服務整合不均衡以及持續存在的信任問題，數位應用仍然有限。[22]

雖然 My Number 以全國規模提供了經過驗證的獨特性，但它仍然是一個傳統的身份系統，而不是 PoH 框架。其驗證基於政府註冊和文件驗證，缺乏 PoH 科技特有的隱私權保護或加密保障。然而，日本的經驗顯示，如果與現代化的隱私增強機制結合，國家支持的獨特性驗證可以作為擴展數位信任和預防詐欺的基礎。

同時，日本的發展軌跡也顯示了中心化身分系統在打擊詐騙上的限制。大多數網路詐騙和身分冒用行為發生在監管較少的環境中，例如社群媒體、即時通訊和電商平台。這些平台雖然遵循一般的消費者和內容法規，但卻不在日本的身份鏈結保障機制的覆蓋範圍內。此外，諸如 2023 年健康保險記錄錯誤鏈結等資料處理事件削弱了公眾的信任，並重新引發了關於隱私、監管和問責制的討論。[23] 這些案例表明，在擴大身分驗證的使用範圍方面，信任而非科技仍然是限制因素。日本的隱私文化，乃由圍繞匿名性的強勢社會規範和對國家資料處理的謹慎態度所塑造，此使得社會接受度成為部署任何新型驗證機制（例如 PoH）的關鍵因素。

為應對這項挑戰，日本政府推出了更強力的治理和互操作性措施，力求將基於 My Number 卡（JPKI）的身份驗證擴展到銀行、SIM 卡註冊和電子商務等私營區塊。[24] 如果能夠透明地實施，日本的身份驗證系統有望發展成為一種混合型數位信任模型：在國家驗證的基礎上鞏固合法身份，同時透過保護隱私的加密方法實現類似 PoH 式的獨特性證明。這種發展將使日本能夠將可信賴身分與可擴展的、尊重隱私的驗證鏈結，從而增強抵禦詐騙的能力，並提升大眾對數位經濟的信心。[25]

韓國：數位身分整合與實名認證

韓國擁有全球最先進、最一體化的數位身分生態系統之一，其核心是連接銀行、電信和電子政府服務的國家電子身分基礎設施。[26]韓國的身份框架以 1968 年推出的居民登記號碼（RRN）系統為基礎，經過實名認證、生物識別認證和公鑰基礎設施等多層發展，為快速成長的網路經濟提供了支持。[27] 數位身分證（2020 年）和行動性駕照（2022 年）標誌著韓國從紙本證件向全數位證件過渡的里程碑。[28] 至 2025 年止，有超過 5000 萬韓國人每天使用數位認證，透過 PASS、Kakao、Naver 或Samsung Pass，存取金融、政府和私營部門的服務。

這種跨平台的身分之深度整合是韓國實名制和網路安全制度的核心，該制度要求個人在進行大多數線上交易之前驗證其合法身分。這些機制實際上構成了一個PoH層，確保數位行為者對應真實、獨特的個人，並顯著減少詐欺、虛假身份和自動化濫用。公共系統和私有系統之間的互操作性帶來了高度信任，並使韓國的金融身分詐欺率在全球處於較低水平。[29]

然而，韓國的模型也揭露了高度中心化的弊端。強制實名制以及電信、金融和政府機構之間的數據共享引發了人們對隱私和公民自由的擔憂。大規模數據外洩事件，包括信用機構和電商平台的資料洩露，加劇了公眾對給予同意和資料最小化的質疑。[30] 政策制定者加強了《個人資訊保護法》（PIPA）的保護力度，並啟動了數位身分先導計畫（2023 年）做為反應，以探索去中心化、使用者控制的身分驗證。這是朝著更注重隱私權保護之模型所邁出的重要一步。

韓國的經驗既展現了國家為基石的 PoH 系統之優勢，也揭示了其限制。韓國將合法身分認證、生物辨識保障和有互操作性的信任框架結合，為防範詐騙和建構數位信任提供了一個強大的模板。然而，韓國引起的討論也突顯了人們對能夠提供更強隱私保護和用戶控制權的方法日益增長的興趣。這些原則與新興的PoH科技的發展方向不謀而合。隨著韓國不斷精煉其數位信任架構，未來的發展重點可能會從嚴格執行實名制轉向較均衡的模型，既驗證真實用戶身份，又維護個人權利和對數位經濟的信心。

馬來西亞：國家數碼身份（MyDigital ID）與邁向生物辨識信任之路

馬來西亞的 MyDigital ID 計畫標誌著在建立統一的、由國家支持的數位身分框架方面邁出了重要一步，讓公眾和私人服務的存取流程更精簡。該系統根據「數位身分藍圖」於 2024 年啟動，將為每位居民分配一個與國民登記局 （NRD）資料庫連結的生物辨識數位憑證。[31] 該系統利用臉部辨識和安全認證，讓用戶能夠在電子政府入口網站、銀行、電信業者和其他線上服務中驗證身分。與內陸稅收局（LHDN）和部分金融機構的早期先導計畫已為預計於 2025 年在全國範圍內全面推廣奠定了基礎。

與以往的 ID 系統不同，MyDigital ID 旨在同時作為憑證和驗證層，無需重複揭露個人資訊即可進行驗證。透過錨定在經驗證的生物特徵記錄之身分，它為PoH式驗證奠定了基礎，確保每個數位帳戶都對應一個真實、唯一的個人。隨著馬來西亞在各領域推廣數位驗證，它面臨著與其他經濟體相同的挑戰：如何在開放的、用戶驅動的環境中建立信任，因為在這些環境中，完全揭露身分既不現實也不可取。從這個意義來說，MyDigital ID 可以作為未來 PoH 機制的骨幹，以保護隱私且可互操作的方式驗證人性和獨特性。

該計劃還直接反應了馬來西亞日益嚴重的詐騙和數位詐欺問題，這些問題隨著行動銀行和電子商務的普及而增加。在受監管的生態系統中，可信任身分層有助於減少身分冒用和虛假帳戶，而 PoH 式驗證最終可以將這些保護措施擴展到不受監管的領域，例如網路商場、社群媒體和數位支付。這些領域往往是詐騙的溫床。

然而，該系統的推出引發了公眾對隱私、數據保護和治理的討論。民間團體對中心化生物辨識數據儲存以及其存取權限超出預期用途時可能導致的濫用表示擔憂。[32] 政府成立了數位身分指導委員會作為反應，重申了對《個人資料保護法》（PDPA）的遵守，並強調了與 MySejahtera 和馬來西亞國家銀行監管下的 eKYC 系統的互操作性。[33] 這些措施旨在確保實施過程透明化、有負責，並贏得公眾信任。

如果實施過程中輔以明確的安全保障和使用者控制，MyDigital ID 有望發展成為 PoH 創新領域值得信賴的身份基礎。這個結合了經驗證的生物辨識、使用者同意和安全的互操作性的架構，展現了新興經濟體如何將經驗證的獨特性和包容性融入數位信任框架。對於東南亞而言，馬來西亞的經驗突顯了以治理為主導的身份發展，可以如何彌合傳統數位身分系統與未來 PoH 模型之間的差距，並在增強詐騙韌性的同時，維護隱私和公眾信任。

菲律賓：菲律賓身分識別系統（PhilSys）的快速推廣

菲律賓身分識別系統 （Philippine Identification System，PhilSys）已成為東南亞發展最快的數位身分計畫之一。PhilSys 於 2018 年根據第 11055 號共和國法令設立，為每位公民和居民分配一個獨特的 12 位數 PhilSys 號碼 （PSN），該號碼由生物識別數據（包括面部、指紋和虹膜掃描）支持。[34] 該計畫由菲律賓統計局 （PSA） 管理，旨在改善公共服務取得、促進普惠金融並確保數位交易安全。至 2025 年底，已有超過 8 千萬菲律賓人註冊，其數位版身分證（可透過 eGovPH 應用程式和 national-id.gov.ph 取得）已被政府機構、銀行和私人平台廣泛接受。[35]

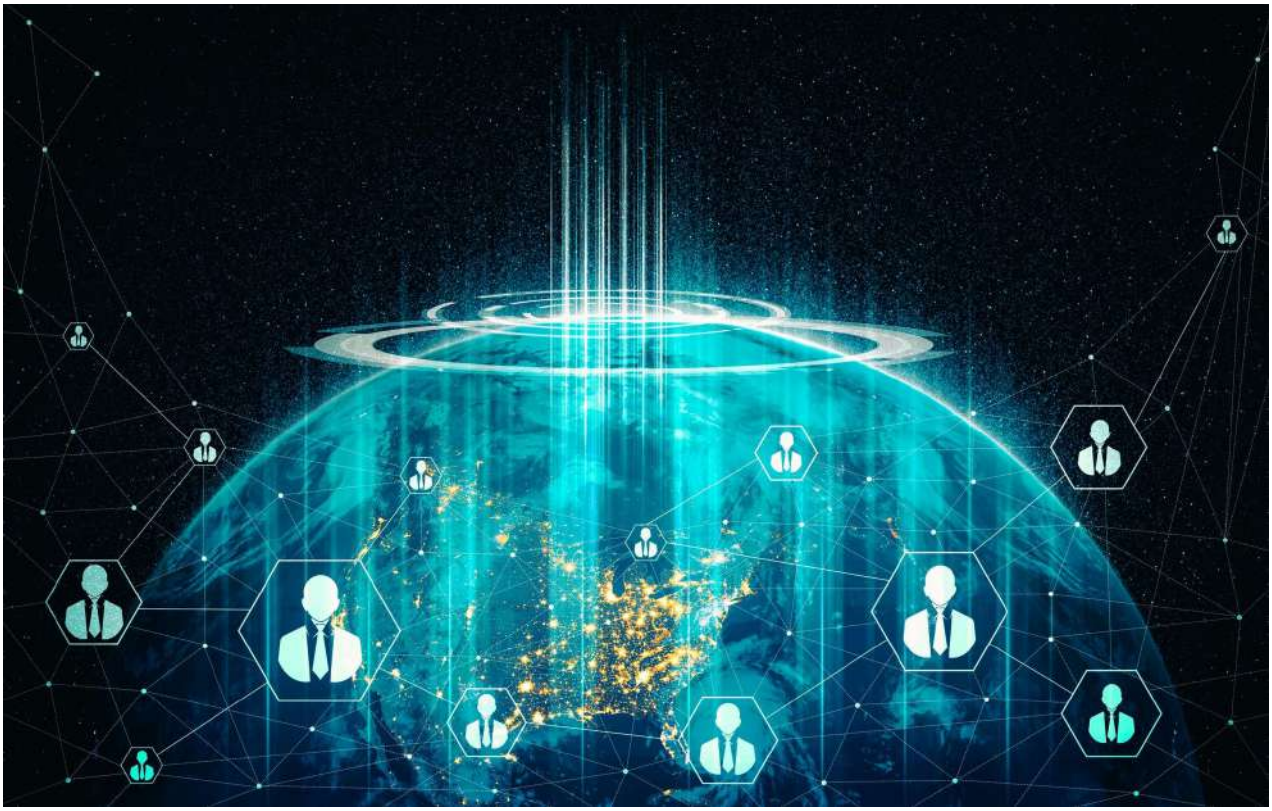
此次快速部署標誌著該區域在建立可信賴身分方面達到了重要的里程碑。透過已驗證的生物特徵與永久的唯一識別碼之連結，PhilSys 有效地創建了一個政府錨定的獨特性證明層，從而防止重複註冊和偽造身分。它與金融機構、電信業者和政府系統的整合，可視為早期大規模的 PoH 實踐，確認每個已驗證的用戶都對應一個真實、獨特的個體。eVerify 入口網站支援基於二維 （QR） 碼的即時身分驗證，將此保障擴展到數位支付、社會安全和 SIM 卡註冊等領域。[36]

快速部署同時也帶來了新的治理和隱私挑戰。技術性錯誤、卡片製作延誤和數據處理問題引起了公眾的關注，而對中心化生物識別儲存和不透明數據共享的擔憂，則促使人們呼籲加強安全保障。[37] 菲律賓統計局和國家隱私委員會 （NPC） 已採取應對措施，加強監管，採用更嚴格的加密標準，並在 eGovPH 框架中嵌入基於同意的存取協議。[38]

菲律賓的經驗既展現了快速擴展數位信任的潛力，也揭示了其中的風險。其規模和互操作性顯現新興經濟體是如何能夠越級發展，建立支持普惠金融和減少詐欺的身份驗證之基礎建設。然而，這項推廣也強調信任必須與科技同步發展：公眾信心取決於可見的問責制、透明的數據治理和使用者控制權。隨著 PhilSys 持續成熟，它為符合 PoH 理念的創新提供了一個寶貴的試驗平台，示範如何透過經驗證的獨特性，並結合強力的隱私和包容性保障措施，增強東南亞數位經濟的詐騙韌性和以人為本的信任。

案例研究要點

這四個案例共同展現了亞洲經濟體建構獨特性證明的基礎建設之不同路徑。日本和韓國展示了先進的監管環境如何大規模地將身分驗證制度化，但結果卻截然不同：日本的 My Number 系統顯現當數據治理失效時，公眾信任的脆弱性，而韓國的實名制則突顯了身分、金融和科技深度整合的效率及其風險。在東南亞，馬來西亞的 MyDigital ID 和菲律賓的 PhilSys 展現了兩種新興模型：一種強調精心設計的治理，另一種則優先考慮快速推廣和普及。這四個案例都呈現出一個共同的模式： PoH 式的驗證方式只有在與透明度、互操作性和使用者控制權做連結時，才能確保數位身分系統能夠增強，而不是削弱公眾對網路安全的信心。



結論與建議

詐騙和網路詐欺已成為亞太地區數位信任的主要威脅。儘管各國數位身分系統，無論日本的 My Number 至菲律賓的 PhilSys，在邁向經驗證且具包容性之身分體系方面已有進展，它們主要仍是行政工具，而非即時、防詐欺的手段。新興的PoH科技為這些系統提供了一個重要的補充層：它讓用戶能夠在數位平台、金融服務和通訊網絡中，證明自己是獨一無二的人類使用者，而無需透露個人識別資訊。透過增加保護隱私的人類證明訊號，PoH 可以應對傳統數位身分系統無法偵測到的自動化和大規模濫用。因此，將 PoH 整合到數位身分生態系統中，既可以增強抵禦詐騙的韌性，又可以提升公眾對數位交易的信心，同時還能保持強大的隱私保護。

正如「保障措施和治理」一節所強調的，負責任的 PoH 部署需要基於風險的設計、明確的使用者保護措施以及與現有身分生態系統的精心協調。基於這些原則，該區域各國政府可以：

• **將數位身分和 PoH 科技融入防詐騙策略：**將獨特性證明驗證嵌入金融、電子商務和通訊平台，以降低身分冒用、機器人驅動的詐欺和合成身分風險，同時確保適度、便捷的部署，並符合 ISO/IEC 25389 等安全框架。

• **支援隱私保護和互操作性標準：**鼓勵生物辨識保障與加密隱私保護結合的區域框架之發展，確保經驗證的獨特性不會損害使用者匿名性或跨境可用性，**並且 PoH 訊號不會被挪用於追蹤或剖繪使用者。**

• **促進區域政策對話與協調：**利用現有機制，例如 APEC 企業諮詢委員會、G20 數位普惠金融高級原則以及聯合國主導的數位經濟倡議，協調政策目標，分享最佳實務，並探索跨領域、基於 PoH 的先導框架，包括建立可控沙盒機制，使政府和平台能夠在廣泛應用前，在高風險環境中測試 PoH。

這些措施將有助於在亞洲建立一個更值得信賴、以人為本的數位生態系統。在這個生態系統中，驗證能夠在不損害隱私的前提下加強安全性，保障措施和治理框架能夠確保負責任的使用，而區域合作能把身份系統，從行政性登記系統，轉變為增強詐騙韌性和促進數位普惠的積極工具。

参考文献

[1] Cybersecurity Ventures. n.d. “The World’s Third Largest Economy Has Bad Intentions—And It’s Only Getting Bigger.” 2025 8 月取得。 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.” 2025 8 月取得. 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.” 2025 8 月取得。 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/912490WP0Digit00Box385330B00PUBLIC0.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] OECD, Digital Government in Korea: Enabling a Smart and Inclusive Society, 2023, p. 45.
[30] 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.
[31] Malaysia Digital Economy Blueprint (MyDIGITAL), Digital Government Division, Ministry of Communications and Digital, "Digital Identity Blueprint," Government of Malaysia, 2024.
[32] Malay Mail, "Privacy Advocates Raise Concerns over Centralised Biometric Database," 5 April 2024.
[33] Ministry of Communications and Digital (KKD), "Formation of Digital ID Steering Committee," 15 February 2024; Bank Negara Malaysia, e-KYC Implementation Guidelines, revised 2023.
[34] Republic Act No. 11055, "An Act Establishing the Philippine Identification System (PhilSys Act)," Official Gazette of the Republic of the Philippines, August 2018.
[35] 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.
[36] PSA, "PhilSys eVerify Portal Launch and QR Verification Capabilities," 2024.
[37] Rappler, "Privacy Concerns Mount over National ID Data Sharing," 22 June 2024; Philippine Star, "National ID Delays, Data Glitches Spur Criticism," 10 May 2024.
[38] National Privacy Commission (NPC), "NPC Advisory on Data Protection Standards for the National ID System," 2024; PSA, "Enhanced Security Measures for ePhilID Rollout," 2024.