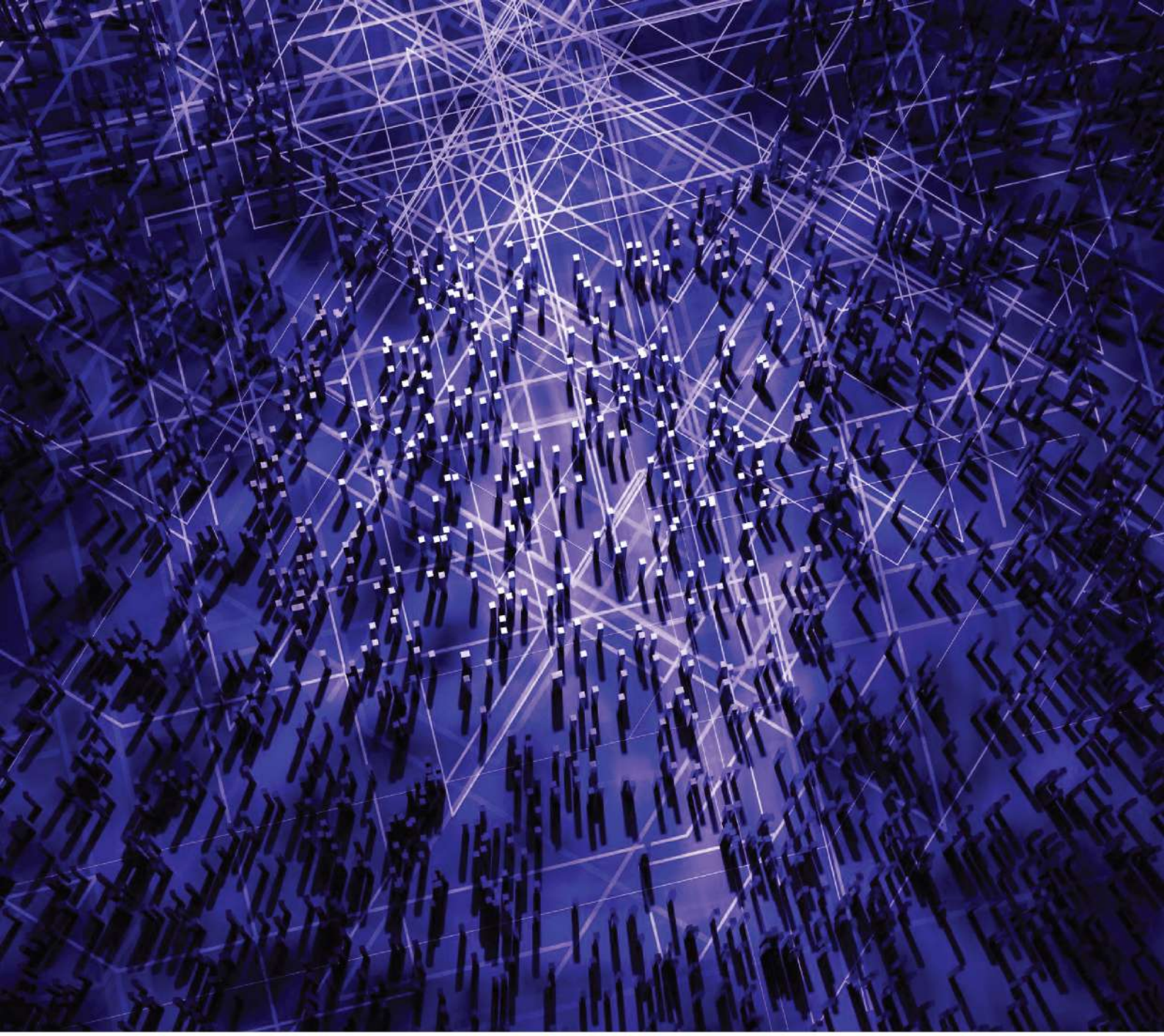


인간성 증명

아시아 태평양 지역의 디지털 신뢰 및 사기 방지를 위한 인적 네트워크 구축

2025년 12월

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

이 논문에 대하여

본 보고서는 아시아 태평양 지역의 디지털 신뢰 환경을 탐구하기 위해 동남아시아 공공정책연구소가 일본신뢰안전협회(JTSA)[1.1] [2.1]와 협력하여 Tools for Humanity의 지원을 받아 연구 및 작성했습니다. [3.1]제시된 정보와 분석은 관련 이해관계자 인터뷰, 공개 자료, 그리고 저자들의 분석을 기반으로 합니다. 특히 JTSA의 전략적 기여, 그중에서도 다나카 키요타카의 거버넌스, 상호운용성, 위험 기반 PoH 구현에 대한 통찰력은 본 보고서 작성에 큰 도움이 되었습니다.

본 보고서는 Tools for Humanity의 견해를 대변하는 것이 아닙니다. 정책, 법률 또는 규정에 대한 포괄적인 검토를 목적으로 작성된 것이 아니므로, 그 범위와 한계를 고려하여 신중하게 사용해야 합니다.

콘텐츠

핵심 요약

온라인 사기는 산업화된 국경 없는 범죄 행위로 진화했습니다. 전 세계 사이버 범죄 경제 규모는 현재 10조 달러를 넘어섰고, 매년 1조 달러 이상이 사기로 인해 손실되고 있습니다. 매년 사기로 인한 피해액만 1조 달러를 넘습니다. 개인의 정신건강과 사회 전반의 신뢰를 훼손하고 법 집행 및 규제 당국의 자원을 소모합니다. 아시아 태평양 지역은 사기 범죄의 주요 표적일 뿐만 아니라 범죄 활동의 중심지이기도 합니다. 동남아시아에서는 인신매매와 연관된 대규모 사기 조직이 활발하게 활동하고 있으며, 일본과 한국 같은 선진 시장에서는 투자 사기 및 신분 도용 사기가 급증하고 있습니다. 이러한 문제는 지역적이고 상호 연관되어 있으므로 여러 경제권에 걸친 공조 대응이 필요합니다.

인공지능 음성 복제와 딥페이크는 설득을 산업화했고, 자동 계정 생성은 대규모 접근을 가능하게 하였으며, 암호화폐와 즉시 결제는 수익 모델화에 속도를 붙였습니다. 그러나 동일한 기술들은 또한 발전된 신원 보증, 진위 확인 신호, 그리고 개인정보 보호 장치를 통해서 신뢰를 강화할 수 있고, 더불어 새로운 위험을 예방하기 위한 거버넌스와 투명성도 뒷받침되어야 합니다.

범죄자들이 손쉽게 수천 개의 가짜 또는 자동화된 신원을 만들어낼 수 있는 상황에서는 기존의 법 집행 및 인식 제고 노력은 필요하지만 충분하지 않습니다. 지속 가능한 발전을 위해서는 사기꾼들이 악용하는 허점을 메우는 두 가지 차원의 디지털 신뢰가 필요합니다.

●**디지털 신원(Digital ID):** "당신은 누구입니까?" 라는 질문에 답합니다. 금융, 전자정부 등 규제 환경에서 사용되는 익명 이 아닌, KYC(고객확인제도) 지원 자격 증명입니다.

●**인간성 증명 (PoH):** "당신은 실제로 존재하는 고유한 사람입니까?" 라는 질문에 답합니다. 이는 완전한 신원 공개가 필요하지도 바람직하지도 않은 개방형 플랫폼 환경에서 사용할 수 있는 개인정보 보호시그널입니다.

PoH는 디지털 ID를 대체하는 것이 아닙니다. PoH는 사기가 가장 많이 발생하는 인터넷 영역(소셜 미디어, 메시징 앱, 마켓플레이스)에 신뢰를 더하는 보완적인 기능으로, 가짜/합성 계정 및 봇을 이용한 악용을 줄이고 사용자 개인정보를 보호합니다. 최근에 발전된 상황에서는 PoH를 신뢰와 안전에 기반한 체계 내에서 구축해야 할 필요성이 나타납니다. 이는 자동화 및 대규모 악용 문제를 해결하면서도 사용자의 의도나 신뢰성을 보장하는 것으로 오해받지 않기 위함입니다.

아시아 태평양 전역에서, 정부는 규제 대상 부문에서 KYC(고객 신원 확인) 및 책임성을 강화하는 강력한 디지털 ID 기반을 구축해 왔지만, 대부분의 사기 행위는 디지털 ID가 적용되지 않는 소셜 미디어, 메신저, 온라인 마켓플레이스와 같은 규제되지 않은 영역에서 발생합니다. 바로 이 지점에서 PoH(인간성 증명)가 고유한 가치를 제공합니다. PoH는 개인정보 보호 기능을 갖춘 인간 토큰 및 기기 기반 인증과 같은 메커니즘을 통해 대량의 가짜 계정 생성을 제한하고, 봇을 이용한 사기 행위를 차단하며, 피해자가 표적이 되기 전에 진실된 휴먼 네트워크를 강화할 수 있습니다. 이러한 기술이 성공적으로 작동하려면 오용을 방지하고 익명성을 보호하며 대중의 신뢰를 유지하는 명확한 안전장치, 사용자 제어 및 거버넌스 구조가 필요합니다.

사례 개요

●**일본 - 마이 넘버:** 대규모 국가 인증 고유성 확보가 가능하지만 데이터 처리 사고로 신뢰성 문제가 제기되었습니다; 정부 서비스 외 분야에서도 개인정보 보호 인증을 위해서 정부 ID와 PoH(인간성 증명)를 결합한 하이브리드 모델의 기준점으로 활용할 수 있습니다.

●**대한민국 — 실명제:** 금융, 통신, 전자정부 전반에 걸친 심층적 통합이 사실상 PoH(인간성 증명)의 역할을 하지만, 개인정보 보호 및 시민적 자유에 대한 우려로 인해 성공에는 한계가 있고, 이로 인해 사용자가 직접 제어하는 탈중앙화 인증 방식에 대한 관심이 높아지고 있습니다.

●**말레이시아 — MyDigital ID(시행):** 국가 등록 시스템과 연동된 생체 인식 기반 인증 정보입니다. 설계에서부터 거버넌스를 반영하는 [15.1]것은 PoH 원칙과 잘 부합하지만, 확대를 위해서는 강력한 안전장치와 국민의 신뢰가 필요합니다.

●**필리핀 — PhilSys (신속한 확장):** 디지털 ID 다운로드 및 전자 인증을 통해서 빠르게 대규모로 도입되었습니다; PoH 와 유사한 운영 기능을 보여주는 동시에 거버넌스 및 사용자 교육을 신속하게 유지해야 할 필요성을 시사합니다.

사기 방지를 위한 효과적인 방어 체계 구축에는 다층적인 보증 체계가 필요합니다. 신원 검증을 거친 규제된 상호작용과, 사용자의 개인정보 보호를 위한 검증 절차를 통해 강화된 개방형 플랫폼이 필요합니다. 투명성, 상호운용성, 그리고 사용자 제어는 이러한 모든 요소를 아우르는 핵심 요소입니다. 표준화 기구, 업계 중개 기관 또는 다중 이해관계자 체계과 같은 중립적인 거버넌스 메커니즘은 국가의 요구 사항을 글로벌 플랫폼의 운영 관행으로 전환하는 데 매우 중요할 것입니다.

정책 권고 사항

● **디지털 ID 및 PoH를 사기 방지 전략에 통합.** 신뢰와 안전에 기반한 배포 및 과도한 의존을 방지하는 보호 장치를 통해 사칭, 가짜 신원 및 봇 악용을 억제하고 금융, 전자 상거래 및 커뮤니케이션 흐름에 고유성 증명 검사를 내장하십시오.

● **개인정보 보호 및 상호 운용 가능한 표준을 지원.** 생체 인식/자격 증명 보증을 암호화 기술(예: 영지식 증명)과 결합하여 적절한 경우 익명성을 보호하고 국경 간 사용 가능성을 활성화하되, PoH가 추적이나 프로파일링에 악용되지 않도록 보장합니다.

● **지역 정책 대화 및 조정을 촉진.** APEC 비즈니스 자문 위원회, G20 디지털 금융 포용을 위한 하이레벨 원칙, UN 디지털 경제 이니셔티브와 같은 플랫폼을 활용하여 동일한 목표를 만들고, 증거를 공유합니다. 또한 유용성, 포용성 및 비례성을 평가하기 위한 샌드박스 테스트를 포함시켜 [19.1]여러 부문에 걸쳐 PoH 기반 검증을 시범 운영합니다.

사기는 구조적인 신뢰 부족을 드러냅니다. 강력한 개인정보 보호, 거버넌스 및 상호 운용성을 기반으로 구현된 디지털 ID와 PoH 설계 구조는 사용자 권리를 보호하면서 대규모 악용에 대한 비용을 높여 아시아가 더욱 안전하고 포용적인 디지털 경제로 나아가는 길을 가속화할 수 있습니다.

서론: 사기 범죄의 만연과 정책적 공백

사회경제적으로 디지털 기술을 수용하면서 온라인 범죄는 급증하고, 수법은 다양해지고 있습니다. 전 세계 사이버 범죄 경제 규모는 현재 10조 달러를 넘어섰으며, 이는 GDP 기준 세계 3위 경제 규모에 필적합니다. [1] 사기는 사이버 범죄의 특정 유형으로, 증가하는 추세이며 소비자들은 매년 1 조 달러 이상을 사기 피해로 잃고 있습니다. [2] 하지만 그 피해는 금전적 손실에만 그치지 않습니다. 피해자들은 정신 건강과 복지에 지속적인 피해를 입고, 디지털 서비스와 디지털 경제에 대한 신뢰가 무너지며, 공공 자원은 법 집행, 인식 개선, 국가 사이버 보안 노력에 투입되고 있습니다. [3]

아시아의 이중적 역할

전 세계적으로 만연한 사기 범죄 중에서도 아시아 태평양 지역은 가장 큰 피해를 입고 있습니다. 이른바 '돼지 도살 사기', 투자 사기, 로맨스 사기 등 사기꾼들이 심리 기만 기법을 이용해 피해자와 관계를 맺고 금전적 지불이나 투자를 유도하는 수법이 특히 널리 퍼져 있습니다. [6] 이러한 사기는 대개 소셜 미디어나 메신저 서비스를 통해 시작되며, 국제적인 조직 범죄 집단이 운영하는 대규모 사기 조직에 의해 실행됩니다. [7]

기술: 가능성을 열어주는 도구이자 해결책

기술의 발전은 사기 행위의 경제적 구조를 근본적으로 바꿔놓았으며, 아무리 자원이 풍부한 정부라도 사기 수법의 급속한 진화에 대응하는 데 어려움을 겪고 있습니다. [4,5]

첫째, 설득 방법이 산업화되었습니다. 인공지능, 음성 복제, 딥페이크는 사기를 발생시키는 무기로 사용되고 있으며, 금융 부문 사기 시도의 42% 이상이 AI와 관련되어 있습니다. [8] 이러한 도구들은 매우 사실적인 대본, 이미지, 전화를 여러 언어로 제공할 수 있어, 상대적으로. 미숙한 운영자들도 A/B 테스트를 통해 다듬어진 플레이북을 활용하여 장기적인 "투자" 사기나 로맨스 사기를 행할 수 있게 합니다.

둘째, 확장성이 사실상 무한해졌습니다. 자동화된 계정 생성, SIM 팜, 크로스 플랫폼 도구를 통해 소규모 팀도 몇 시간 내에 소셜 미디어, 메신저, 전화 등 다양한 채널을 통해 수백만 명에게 연락할 수 있으며, 봇과 추천 시스템을 활용하여 호응이 좋은 잠재 고객을 찾아낼 수도 있습니다. [9]

셋째, 수익 모델 구축에 있어서 범죄 수법이 혁신적으로 진화하며 그 속도가 가속화되고 있습니다. 암호화폐 인프라, 핀테크 채널, 자금 세탁 네트워크, 크로스 체인 믹서는 자금의 신속한 이동과 은폐를 가능하게 하며, 즉시 결제와 파편화된 KYC/KYB 체계는 전통적인 은행 시스템에서 범죄를 차단하기 어렵게 합니다. [10]

그 결과 디지털 경제에서 구조적인 신뢰 부족 현상이 나타나고 있습니다. 범죄자들은 정부와 규제 기관이 대응할 수 있는 속도보다 훨씬 빠르게 새로운 도구를 도입 및 변형하고 있습니다.

동일한 기술이 악용되는 상황에서도 안전장치를 갖추고 대규모로 배포한다면 신뢰를 회복할 수 있습니다.

● 개인, 기기 및 기업에 대한 개인정보 보호 검증, SIM/번호 평판 관리, 고위험 트래픽에 대한 고보안 옵션 등 강화된 디지털 신원 및 개체 보증은 대규모 비용을 증가시킬 수 있습니다.

● 콘텐츠 및 통신에 대한 진위 확인 신호(예: 이미지 및 비디오의 암호화된 출처, 음성 및 문자에 대한 발신자/송신자 검증 체계, 강화된 광고 및 계정 무결성 제어)는 사칭 성공률을 낮출 수 있습니다.

● 플랫폼과 결제 네트워크 전반에 걸쳐 개인정보를 보호하는 신호를 공유하여 조직적인 악용을 확인할 수 있으며, 실시간 결제 위험 점수를 산정하는 것과 "숙려" 조치(수취인 확인, 강화된 검증, 의심스러운 이체에 대한 결제 지연)는 실행 시점에서 손실을 줄일 수 있습니다.

● 피해자 중심 모델, 즉 신속한 단속 절차, 더 빠른 자금 회수 시스템, 그리고 강제 노동 피해자를 식별하는 명확한 경로가 법 집행을 보완하여 착취의 악순환을 끊어야 합니다. [11]

따라서 기술은 범죄 활동을 가능하게 하는 동시에 문제 해결에 필수적인 부분이기도 합니다. 정부, 플랫폼, 금융 기관은 범죄자들이 혁신하는 속도에 맞춰 방어 기술을 지속적으로 도입하고 업데이트해야 합니다. 왜냐하면 사기는 단순한 사이버 범죄 사건이 아니라 디지털 경제에서 근본적이고 구조적인 신뢰 부족의 징후이기 때문입니다. [12]

사기가 온라인 신뢰의 취약성을 드러낸다면, 신뢰할 수 있는 디지털 신원(ID)은 이를 회복할 수 있는 가장 확실한 도구 중 하나입니다. 디지털 신원은 거래나 상호작용의 주체가 누구인지 검증되는 보증을 제공하여 악용 비용을 증가시키고 더 안전한 디지털 경제를 지원합니다. 다음 섹션에서는 디지털 신원이 해결하고자 하는 문제, 관련 기술, 그리고 지역에서 새롭게 부상하는 정책 대응 방안을 살펴봅니다.

디지털 신뢰의 두 가지 측면 : 디지털 신원과 인간성 증명

사기 행위를 막으려면 다층적인 신뢰 시스템이 필요합니다. 법 집행과 인식 제고는 필수적이지만, 지속 가능한 발전은 범죄자들이 대규모로 악용하는 허점을 막는 신원 및 진위 확인 메커니즘에 달려 있습니다. 디지털 신원(Digital ID)과 인간성 증명(Proof of Human, PoH)은 이러한 신뢰 인프라의 두 가지 상호 보완적이면서도 근본적으로 다른 측면을 보여줍니다. 디지털 신원은 개인을 은행과 정부가 인정하는 검증된 실제 신원과 연결함으로써 "당신은 누구입니까?"라는 질문에 답하고, 인간성 증명은 신원을 공개하지 않고 인간성과 고유성을 확인함으로써 "당신은 인간입니까?"라는 질문에 답합니다. 디지털 신원은 익명성을 보장하지 않아 은행이나 전자정부와 같은 규제 환경에 적합하고, 인간성 증명은 익명성을 보장하지만 검증이 가능하여 완전한 신원 공개가 필요하지도 바람직하지도 않은 개방형 디지털 공간을 보호합니다. 이 두 가지가 함께 작용하여 디지털 경제에서 책임성과 개인정보 보호를 모두 지원하는 균형 잡힌 기반을 구축합니다.

Proof of Human은 국가 디지털 신분증 시스템을 대체하는 것이 아니라, 완전한 신원 확인이 불가능하거나 바람직하지 않은 디지털 환경 영역에 신뢰를 확장하는 보완적이고 개인정보 보호적인 방식입니다.

디지털 신원 확인 기술의 형태

디지털 신원 확인 솔루션은 다양한 형태로 존재하며, 각각 다른 위험 요소를 해결합니다.

● **자격 증명 기반 디지털 신원 시스템은** 정부 발행 신분증이나 은행, 이동통신사, 대학과 같은 신뢰할 수 있는 기관에서 발급받은 디지털 방식으로 생성되고 검증 가능한 자격 증명을 활용하여 이름, 나이, 국적 등의 신원 정보를 안전하게 확인합니다. 이러한 자격 증명은 디지털 지갑에 저장하여 다양한 서비스에서 사용할 수 있으며, 단순히 스캔한 문서를 로그인 자격 증명에 연결하는 것보다 훨씬 강력하고 개인정보를 보호하는 재사용 가능한 디지털 상호 작용을 가능하게 합니다. [13]

● **생체 인증은** 지문이나 얼굴 특징과 같은 고유한 신체적 또는 행동적 특성을 사용하여 서비스에 접근하는 사람이 이전에 등록된 개인과 일치하는지 확인합니다. 이는 비밀번호나 기기와 같은 다른 자격 증명이 유출된 경우에도 무단 접근을 방지하는 데 도움이 됩니다. 중요한 것은 생체 인증은 사용자를 인증하는 것이지 신원을 확인하는 것은 아니라는 점입니다. [14]

● **하이브리드 디지털 신원 모델은** 정부 발행 신분증과 생체 인증 등 여러 요소를 결합하여 재사용 가능하고 보안성이 높은 디지털 신원을 생성합니다. 이러한 시스템은 플랫폼 간 상호 운용성, 강력한 인증 및 개인정보 보호 기능을 지원하도록 설계되었습니다. [15]

모두 KYC(고객확인제도)를 지원하며, 규제 대상 생태계 내에서 추적성, 규정 준수 및 책임성을 확보하기 위해 기획되었으므로 익명성을 보장하지 않습니다.

아시아 태평양 지역의 정책 대응

디지털 신분증 기술은 단독으로는 성공할 수 없으며, 기준을 설정하고 개인정보를 보장하며 광범위한 도입을 촉진하는 지원 정책 [5.1]체계가 필요합니다. 실제로 이는 다음과 같은 의미를 갖습니다.

- 디지털 신분증이 금융 거래, 계약 및 공공 서비스에서 법적 효력을 갖도록 명확한 규제가 필요합니다.
- 안전한 저장, 제한적 사용, 잘못 사용되었을 때의 구제 메커니즘이 필요하고, 개인 데이터 보호를 위한 강력한 안전장치가 있어야 합니다.
- 공공-민간 협력 및 크로스 섹터 간 도입을 통해 신분증이 정부뿐만 아니라 사기의 최전선에 있는 플랫폼, 은행 및 공공 서비스 기관에서도 인정되도록 해야합니다.

동남아시아 전역에서 각국 정부는 보다 신뢰할 수 있는 디지털 경제의 기반으로서 디지털 신분증 시스템을 꾸준히 발전시켜 나가고 있습니다.

● 태국의 국가 디지털 신분증(NDID) 플랫폼은 은행, 통신 사업자 및 정부 기관을 연합된 방식으로 연결합니다. [16]

● 인도네시아와 필리핀은 금융 포용 및 사회 서비스와 연계된 국가 전자 신분증 프로그램을 시행하고 있습니다.

● 베트남은 전자정부 포털에 생체인식 인증 시스템을 도입하기 시작했습니다.

지역별로 성숙도 수준에는 차이가 있지만, 지역 정책의 흐름은 국가 시스템 구축에서 상호 운용성 추구로 전환되고 있습니다. 정책 입안자들은 이동성, 이민, 무역 흐름 등으로 인해 국내뿐 아니라 국경을 넘어 인정받는 신분증이 필요하다는 점을 점점 더 인식하고 있습니다.

선진 경제권에서는 이미 포괄적인 국가 신분증 체계가 마련되어 있으며, 더욱 심층적인 통합을 향해 나아가고 있습니다.

● 싱가포르의 싱패스는 은행, 의료 및 전자상거래에 대한 접근을 허용하는 핵심적인 역할을 합니다. [17]

● 한국은 국가 주민등록 시스템을 전자정부 서비스, 금융 거래 및 모바일 인증을 통합한 완전한 디지털 신원 플랫폼으로 확대하고 있습니다.

● 일본의 '마이 넘버' 시스템은 모든 거주자에게 고유한 12자리 식별 번호를 제공하며, 이 번호는 의료, 세금 및 행정 서비스와 점점 더 연계되고 있습니다. [18] 또한, 금융 서비스 및 국경 간 인식 분야로 활용 범위를 확대하기 위한 노력도 진행 중입니다.

이러한 발전 경로는 범위와 속도에서 차이가 있지만, 국가 차원의 자격 증명 시스템이 단순한 보안 로그인을 넘어 디지털 경제의 제도적 기반으로 발전할 수 있음을 보여줍니다. 또한, 국내 시행이나 지역적 상호 운용성을 고려하는 ASEAN 정부 모델에 참고 모델이 됩니다.

동시에 이러한 경험들은 정부의 조치만으로는 충분하지 않다는 점을 보여줍니다. 디지털 신분증의 효과는 궁극적으로 정부, 금융 기관 및 기술 플랫폼 간의 협력을 통해 더 넓은 디지털 생태계에 통합되는 데 달려 있습니다.

사기 방지에 있어 디지털 신원의 역할

디지털 신원 확인 기술은 사기 및 부정행위에 대응하는 가장 유망한 시스템 도구 중 하나입니다. 디지털 신원 확인 시스템은 사람, 기기 및 조직을 검증 가능한 기명성으로 인증하도록 해 신분 도용을 줄이고 익명성을 제한하며 악용될 여지를 증가시킵니다. 만능 해결책은 아니지만, 디지털 신원 확인(KYC) 기능을 갖춘 신뢰의 기반을 형성하여 규제 대상 거래 및 서비스가 실제로 신뢰 가능한 개인 또는 단체와 연결되도록 보장합니다.

사기꾼들이 악용하는 허점 막기

사기는 검증 과정의 허점을 이용합니다. 사기꾼들은 봇과 가짜 계정을 이용해 거의 비용 없이 메시지를 퍼뜨리고, 딥페이크와 음성 복제 기술을 이용해 신뢰할 수 있는 인물을 사칭하며, 합법적인 계정을 탈취해 피해자들을 속입니다. 플랫폼 전반에 걸쳐 취약하거나 일관성이 없는 인증 방식 때문에 이러한 공격이 예상보다 훨씬 더 자주 성공합니다.

디지털 신원 확인(Digital ID)은 규제 측면에서 이러한 격차를 해소합니다. 디지털 상호 작용을 검증된 신원과 연결함으로써 범죄자들이 익명으로 활동하기 어렵게 만들고, 피해자, 기업 및 규제 기관이 온라인에서 거래하는 사람을 더 쉽게 신뢰하도록 합니다. 그러나 대부분의 사기는 소셜 미디어, 메신저, 비공식 시장과 같이 KYC 시스템이 적용되지 않고 규제가 없는 공간에서 발생합니다. 이러한 환경에 대응하기 위해서는 인간성 증명과 같이 개인정보를 보호하는 다른 접근 방식이 필요합니다.

아무리 강력한 디지털 신원 확인 시스템이라도 가짜 계정과 자동화된 악용으로 인한 사기를 완전히 막을 수는 없습니다. 이러한 한계로 인해 개인 식별 정보를 요구하지 않고 사용자의 실체를 확인하며 개인정보 보호 방식을 모색하는 '인간성 증명(Proof of Human)'과 같은 새로운 개념에 대한 관심이 높아지고 있습니다.

인간성 증명: 개념 및 정책적 관련성

‘Proof of Human’의 정의

인간성 증명 (Proof of Human,PoH) 은 디지털 신뢰를 강화하기 위한 새롭고 혁신적인 접근 방식입니다. PoH는 통상적으로 여러 개의 가짜 신원을 방지하고, 온라인 이용자가 자동화된 봇이나 위조된 신원이 아닌 실제 사람임을 검증된 방식으로 보장하는 시스템으로 정의됩니다. [19] 단순한 계정 가입이나 CAPTCHA 인증과는 달리, PoH는 필요한 개인 정보 이상을 공개하지 않고도 플랫폼과 서비스 전반에서 인식될 수 있는 지속적이고 재사용 가능한 인간성을 나타내는 신호를 제공하여 디지털 생태계 전반에 걸쳐서 더욱 신뢰할 수 있는 인간 네트워크의 기반을 구축하는 것을 목표로 합니다.

중요한 점은 PoH가 국가 디지털 신분증 시스템을 대체하거나 대적하는 것이 아니라는 것입니다. 오히려 PoH는 사용자가 누구인지 확인하는 것이 아니라 사용자가 사람인지 확인하는, 신뢰 문제의 다른 측면을 해결함으로써 기존 시스템을 보완합니다.

개념적으로 PoH는 다른 디지털 보안 방법과 차이가 있습니다. 기존의 디지털 ID 체계는 이름이나 주민등록번호와 같은 검증된 속성을 개인과 연결하여 “당신은 누구입니까?”라는 질문에 답합니다. 비밀번호나 다단계 인증 코드와 같은 인증 도구는 계정 생성 후에는 계정을 보호하지만, 가짜 또는 합성 프로필 생성 자체를 막지는 못합니다. 거의 20년 동안 CAPTCHA는 사용자가 퍼즐을 풀 수 있는지 여부를 통해서 인간성을 검증하는 방식으로 이러한 격차를 해소하려 했습니다. 그러나 봇과 AI 도구가 점점 더 인간을 능가하면서 CAPTCHA 의 효과는 떨어졌고, 정당한 사용자에게도 불편함을 초래했습니다. 이와 대조적으로 PoH는 “당신은 인간입니까?”라는 근본적인 질문에 답하며, 검증된 자격 증명, 봇 공격 방지, 블록체인 커뮤니티에서 다중 계정 공격 방어라고 부르는 광범위한 노력과 일맥상통하는 보안 방식입니다. 이러한 점에서 PoH는 디지털 생태계에서 진정성, 개인정보 보호, 그리고 확장성의 균형을 맞추는 것을 목표로 삼는 더 광범위한 혁신의 흐름에 소속됩니다.

PoH 검증 방식의 유형

PoH 시스템은 다양한 방식으로 실행될 수 있으며, 각각은 다른 층위의 검증과 보안을 제공합니다. 다음 표는 PoH 검증의 주요 방식 과 실제 작동 방식을 요약한 것입니다.

PoH 검증 유형	작동 방식	사용자가 경험하는 것	사용 예시 사례
생체인식 기반(개인정보 보호)	일회성 생체 인식 확인(예: 눈 깜빡임/고개 돌림). 시스템은 생체 정보를 저장하거나 공유하지 않고 암호화된 "인간 토큰"을 발급합니다.	휴대전화 잠금 해제 와 유사한 간단한 일회성 인증 절차이며, 신원 정보는 공개되지 않습니다.	대량의 가짜 계정을 방지합니다. 금융 거래 또는 고위험 거래를 처리하는 플랫폼을 위한 높은 수준의 보안 PoH입니다.
장치/하드웨어 기반	기기 인증은 실제 기기를 확인시켜주며, 사용자의 신원을 알 필요 없이 "한 사람 = 한 기기"로 연결할 수 있습니다.	가입 절차에 배경 조회 기능이 포함되어 있으며, 생체 정보는 필요하지 않습니다.	유령 계정 집단을 제한하고 메신저, 소셜 미디어 또는 게임 플랫폼에서 자동 계정 생성을 줄입니다.
상호작용/도전 과제 기반[1.1][2.1]	사용자는 봇이 안정적으로 수행할 수 없는 생체 인식과 유사한 프롬프트 또는 암호화된 질의-응답 인증을 완료합니다[3.1][4.1]. 생체 정보는 사용되지 않습니다.	간단한 인간 상호작용 작업(예: 제어된 동작, 시간 제한 프롬프트)을 수행하지만 기존 CAPTCHA보다 훨씬 덜 침해적입니다.	신분증이나 생체 정보를 요구하지 않고도 가짜 프로필 생성을 방지하여 소셜 플랫폼 및 온라인 커뮤니티에 유용합니다.
사회적/신뢰망 인증	사용자는 신뢰할 수 있는 커뮤니티 구성원 또는 평판 네트워크를 통해 검증되며, 플랫폼은 이를 PoH 신호로 변환합니다.	검증된 사용자/커뮤니티로부터의 간략한 추천 또는 확인.	P2P 마켓플레이스, 긱 플랫폼(단기 일자리 플랫폼), 커뮤니티 기반의 인증 환경.

표 3.1: Proof of Human (PoH) 검증 유형

‘PoH’가 사기 방지에 어떻게 도움이 되는가

아직은 새로운 개념이지만, PoH는 사기 및 부정행위와의 전쟁에서 중요한 의미를 지닙니다. 오늘날 온라인 사기는 규모의 경제를 통해 확산됩니다. 인신매매범과 범죄 조직은 피해자를 유인하기 위해 수천 개의 가짜 계정을 만들고, 돼지 도축 사기를 자동화하거나, 자금 세탁망을 운영합니다. 저렴하고 대량으로 디지털 페르소나를 만들어낼 수 있다는 점은 사기 비용을 낮추는 동시에 플랫폼과 규제 기관이 악의적인 활동을 확인하는 여력을 초과합니다. 이와 대조적으로 PoH는 진정한 인간 네트워크를 강화하고, 대규모로 확산되는 합성이나 자동화된 신원을 제한하여 이러한 불균형을 해소하는 데 도움을 줄 수 있습니다 .

원론적으로 PoH는 계정 생성 또는 거래 시점에 마찰을 일으켜 가짜 계정 확산 속도와 규모를 제한할 수 있습니다.

검증 가능한 인간성은 여러 가지 기능을 수행할 수 있습니다.

1. 가짜 프로필 차단. 로맨스, 고용, 투자 관련 사기에 사용되는 가짜 계정을 차단합니다. 피해자가 이미 속아 넘어간 후에 사후 조치를 취하는 대신, PoH는 처음부터 사기 계정의 생성을 줄이는 데 도움을 줄 수 있습니다.

2. 금융 시스템 보호. 자금 세탁 방지 계좌를 통한 거래 흐름을 줄여 금융 시스템을 보호합니다. 은행과 결제 네트워크는 종종 합법적인 사용자와 사기성 계정을 구분하는 데 어려움을 겪습니다. 재사용 가능한 인간성 신호를 통해서 개인 정보의 지속적인 공개 없이도 기존의 KYC 및 AML 보호 조치를 강화할 수 있습니다.

3. 디지털 상거래와 온라인 커뮤니티에 대한 신뢰 강화. 사기 및 사칭으로 신뢰가 무너진 시장에서 구매자, 판매자 또는 커뮤니티 구성원이 실제 인물인지 확인할 수 있다면 궁극적으로 P2P 거래, 긱 업무 플랫폼 및 소셜 공간에 대한 신뢰를 회복하는 데 도움이 될 수 있습니다.

안전장치 및 거버넌스

PoH 자체가 감시 도구가 되지 않도록 하기 위해서는 안전장치가 필수적입니다. 최근 등장한 모델들은 개인정보 보호를 중시하는 방식에 중점을 두고 있습니다. 암호화 증명과 정보 비노출 증명 방식은 사용자가 신원 정보를 노출하지 않고도 인간성을 증명할 수 있도록 합니다. 신원 확인 (행위자가 인간인가?)과 신원 공개 (행위자가 누구인가?)를 구분하는 것은 여러 관할권에 걸쳐 권리와 신뢰를 유지하는 데 매우 중요합니다. 또한, 안전장치에는 강력한 거버넌스도 필요합니다. 규제 기관, 표준화 기구 또는 다자간 이해관계자 감사를 통한 감독은 PoH 신호가 악의적인 추적이나 프로파일링에 이용되는 것을 방지하는 데 도움이 될 수 있습니다.

사용자 권리와 포용성 또한 매우 중요합니다. 인증은 자발적이고 투명하며 철회 가능해야 하며, 사용자는 자신의 PoH 신호가 어떻게 사용되는지를 이해하고 제어할 수 있어야 합니다. 연령 확인 메커니즘과 같은 보완적인 도구는 민감한 정보 공개 없이 미성년자를 보호할 수 있으며, 다양한 인증 경로를 통해 스마트폰, 생체인식 정보 또는 안정적인 인터넷 연결이 없는 사람들도 소외되지 않도록 할 수 있습니다. PoH의 신뢰성은 궁극적으로 개인정보 보호를 존중하고 접근성을 보장하며 지역 차원의 디지털 신뢰 구축 노력에 부합하면서 보안을 강화할 수 있는지 여부에 달려 있습니다.

하지만 기술적 안전장치만으로는 충분하지 않습니다. 효과적인 PoH 배포를 위해서는 아시아 태평양 지역의 디지털 생태계 현실을 반영하는 거버넌스 구조가 필요합니다. 국가 디지털 ID 시스템은 국내 규정에 따라 운영되는 반면, 대부분의 실제 사용자 상호작용과 보안 위험은 글로벌 플랫폼에서 발생합니다. 이러한 구조적 격차 때문에 정부와 플랫폼 간의 직접적인 통합은 단독으로는 실현 가능한 경우가 드뭅니다. 따라서 요구사항을 해석하고, 이해관계자를 모으며, 대규모 도입 전에 안전한 테스트를 지원할 수 있는 독립적인 상호운용성 중개자, 즉 중립적인 거버넌스 계층이 필요한 경우가 많습니다.

이러한 중개 기관은 PoH가 기술적으로 현실적이고 개인정보를 존중하며 국가 기틀 및 교차 플랫폼 환경 모두에 부합하는 방식으로 구현되도록 할 수 있습니다. 또한 국내 표준을 운영 지침으로 전환하고, 개인정보 보호 및 감사 가능성에 대한 다양한 이해관계자 논의를 주최하며, 사용자나 플랫폼에 의도치 않은 위험을 초래하지 않으면서 PoH를 안전하게 시험할 수 있는 샌드박스 환경을 조성할 수 있습니다.

또 다른 안전장치는 대중의 신뢰와 관련이 있습니다. PoH는 디지털 신원, 인증 또는 eKYC와는 구별되는 새로운 개념이므로 오해가 생기면 감시나 데이터 사용에 대한 우려가 쉽게 발생할 수 있습니다. 따라서 역량 강화는 기술 자체만큼이나 중요합니다. 중립적인 중개자, 업계 단체 및 시민 사회 네트워크는 개인정보 보호 설계가 어떻게 작동하는지 설명하고, PoH가 "당신은 누구입니까?"를 밝히지 않고 "당신은 사람입니까?"라는 질문에 답한다는 점을 강조하며, 책임감 있는 구현을 위한 실질적인 지침을 제공할 수 있습니다. 효과적인 소통과 사용자 교육은 궁극적으로 잘 설계된 PoH 시스템을 사람들이 편안하게 받아들일 수 있도록 만드는 핵심 요소입니다.

마지막으로, PoH는 신뢰 및 안전 체계 내에 포함되어야 합니다. 사용자가 사람임을 확인하는 것만으로는 사용자의 의도가 안전하다고 보장할 수 없습니다. 아시아 태평양 지역에서 발생하는 가장 심각한 사기 행위들, 예를 들어 투자 사기, 신분 도용 사기, 장기적인 심리기만적 수법 등은 대부분 실제 사람이 수행하는 것입니다. 따라서 PoH는 다른 안전 신호를 대체하기보다는 보완해야 합니다. ISO/IEC 25389(안전 체계)와 같은 체계를 적용하면 PoH가 적절하게 사용되도록 보장할 수 있습니다.

- 자동화 및 규모 확장에 대한 다층적 방어 체계로서;
- 인간에 의한 위협을 감지하는 행동 및 평판 신호와 함께;
- 과도한 의존을 피하기 위해 명확한 실행 지침을 제공합니다.

PoH는 기존 신원 확인 체계를 대체하는 것이 아니라 보완적인 혁신으로 시범 운영되어야 합니다. 신중하게 설계하고 관리한다면, PoH는 위험도가 높은 디지털 환경에서 실제 사용자를 확인하는 새로운 방법을 제안하고, 더 큰 규모로 적용 가능한 방안에 대한 근거를 제시하는 데 도움이 될 수 있습니다. 더 나아가, 상호 운용 가능하고 인권을 존중하는 PoH 체계는 국가 디지털 신원 확인 사업을 보완하고, 국경을 넘는 확인을 지원합니다. 또한 아시아 태평양 지역 전반에 걸쳐 사기 및 부정행위에 대해서 지역 협력을 통한 새로운 신뢰 기반을 제공합니다. 이는 각국이 현대 온라인 범죄의 규모와 속도에 대응할 수 있는 탄력적이고 검증 가능한 인적 네트워크를 구축하는 데 도움이 될 것입니다.

다음 섹션에서는 아시아 태평양 지역의 국가별 사례를 살펴보고 PoH가 실제로 어떻게 구현될 수 있는지 설명합니다.

사례 연구: 첨단 기술의 실제 적용

아시아 각국 정부는 공공 및 금융 서비스 이용 시 시민의 신원을 확인하는 강력한 디지털 신원 인증 시스템을 구축해 왔습니다. 그러나 대부분의 사기 행위는 이러한 규제 시스템 외부, 즉 익명성이 지배적인 소셜 미디어, 메신저, 콘텐츠 플랫폼에서 발생합니다. 새롭게 부상하는 인간성 인증(Proof of Human, PoH) 기술은 개인 정보를 노출하지 않고도 사용자의 인간성과 고유성을 확인하여 디지털 신원의 신뢰성을 이러한 개방형 환경으로 확장할 수 있는 방안을 제시합니다. 다음 사례 연구에서는 일본, 한국, 말레이시아, 필리핀 등 4개국이 국가 시스템을 통해 PoH 와 유사한 인증 요소를 구축하는 방식과, 이들의 경험이 미래의 사기 방지 전략에 어떤 의미를 갖는지 설명합니다.

일본: 마이 넘버 시스템과 신뢰에 관한 도전 과제

일본의 마이 넘버 시스템은 세금, 사회 보장, 재난 대응 등을 위해 모든 거주자에게 고유한 12자리 식별 번호를 부여합니다. [20] 행정 데이터 통합 및 효율성 향상을 목표로 설계된 이 시스템은 마이 넘버 카드를 통해 디지털 영역으로 확장되었습니다. 마이 넘버 카드는 전자 정부 서비스, 의료 서비스, 금융 거래 등에 안전한 온라인 인증을 가능하게 하는 스마트 ID입니다. [21] 2025년까지 9천만 장 이상의 카드가 발급되어 전체 인구의 70% 이상을 커버할 것으로 예상되지만, 서비스 통합의 불균형과 지속적인 신뢰 문제로 인해 디지털 사용은 여전히 제한적입니다. [22]

마이 넘버는 국가 차원에서 신원 확인을 보장하지만, PoH 체계가 아닌 전통적인 신원 확인 시스템입니다. 신원 확인은 정부 등록 및 문서 검증에 기반하며, PoH 기술의 특징인 개인정보 보호 또는 암호화 보장을 제공하지 않습니다. 그럼에도 불구하고 일본의 사례는 현대적이고 개인정보 보호 기능을 강화하는 메커니즘과 결합될 경우, 국가 차원의 신원 확인이 디지털 신뢰도를 높이고 사기를 방지하는 기반이 될 수 있음을 보여줍니다.

동시에 일본의 사례는 사기 방지에 있어 중앙식 신원 확인 시스템의 한계를 보여줍니다. 대부분의 온라인 사기 및 사칭 행위는 소셜 미디어, 메신저, 전자상거래와 같이 규제가 덜한 환경에서 발생합니다. 이러한 플랫폼들은 일반적인 소비자 및 콘텐츠 규제 내에서 운영되지만, 일본의 신원 연동 보증 체계 밖에 있습니다. 한편, 2023년 건강보험 기록 오연동 사태와 같은 데이터 처리 관련 사건들은 국민의 신뢰를 훼손하고 개인정보 보호, 감독, 책임에 대한 논쟁을 다시 불러일으켰습니다. [23] 이러한 사건들은 기술이 아닌 신뢰가 검증된 신원 사용 확대를 가로막는 제약임을 보여줍니다. 익명성에 대한 강한 규범과 국가 데이터 처리에 대한 신중한 태도로 형성된 일본의 개인정보 보호 문화는 PoH와 같은 새로운 검증 메커니즘을 도입하는 데 있어 사회적 수용을 불가피한 고려 대상으로 만듭니다.

이에 대응하여 일본 정부는 마이 넘버 카드 기반 인증 (JPKI) 을 은행, SIM 등록, 온라인 상거래 등 민간 부문 영역으로 확대 적용하기 위한 강화된 거버넌스 및 상호운용성 조치를 도입했습니다. [24] 투명하게 구현된다면 일본은 법적 신원을 국가 검증에 기반하면서, 개인정보 보호 암호화 방식을 통해서 PoH 스타일의 고유성 증명을 가능하게 하는 하이브리드 디지털 신뢰 모델로 시스템을 발전시킬 수 있습니다. 이러한 발전은 신뢰할 수 있는 신원과 확장되는 개인정보를 존중하는 검증을 연결해 사기 방지 및 디지털 경제에 대한 국민의 신뢰가 형성되도록 합니다. [25]

대한민국: 디지털 신분증 통합 및 실명 인증

대한민국은 은행, 통신, 전자정부 서비스를 연결하는 국가 전자신분증(e-ID) 인프라를 기반으로 구축된 세계에서 가장 발전되고 통합된 디지털 신원 생태계를 운영하고 있습니다. [26] 1968년 도입된 주민등록번호(RRN) 시스템을 기반으로, 한국의 신원 확인 체계는 실명 인증, 생체 인증, 공개키 인프라를 거쳐 빠르게 성장하는 온라인 경제를 지원하며 발전해 왔습니다. [27] 디지털 신분증(2020년)과 모바일 운전면허증(2022년)은 종이에서 완전한 디지털 신분증으로의 전환에 있어 중요한 이정표가 되었습니다. [28]2025년까지 5천만 명 이상의 한국인이 PASS, 카카오, 네이버, 삼성패스 등을 통해 매일 디지털 인증을 사용하여 금융, 정부, 민간 부문 서비스를 이용할 것으로 예상됩니다. [29]

이처럼 플랫폼 전반에 걸친 신원 정보의 심층적 통합은 한국의 실명제 및 사이버 보안 체제의 핵심 요소이며, 대부분의 온라인 거래 전에 개인의 법적 신원 확인을 의무화하고 있습니다. 이러한 메커니즘은 사실상의 '인간 성 증명 (Proof of Human, PoH)' 역할을 하여 디지털 행위자가 실제적이고 고유한 개인임을 보장하고 사기 행위, 가짜 신원, 자동화된 악용을 상당수 감소시킵니다[16.1]. 공공 및 민간 시스템 간의 상호 운용성은 높은 수준의 신뢰를 구축하고 전 세계적으로 가장 낮은 수준의 금융 신원 도용률을 달성하는 데 기여했습니다. [30]

그러나 한국의 모델은 강력한 중앙집권화의 단점도 드러냅니다. 실명 의무화와 통신, 금융, 정부 기관 간의 데이터 공유는 개인정보 보호 및 시민의 자유 침해 우려를 불러일으켰습니다. 신용정보 회사와 전자상거래 플랫폼의 데이터 유출을 포함한 대규모 데이터 유출 사고는 동의 및 데이터 최소화에 대해서 대중이 회의적인 시각을 갖게 했습니다. [31] 이에 대응하여 정책 입안자들은 개인정보보호법(PIPA)에 따른 보호 조치를 강화하고, 사용자가 직접 제어하는 분산형 인증을 제안하는 디지털 신원 시범 사업(2023년)을 시작했습니다. 이는 개인정보 보호에 더욱 중점을 둔 모델로 나아가는 중요한 발판입니다. [32]

한국의 사례는 PoH시스템 의 강점과 한계를 모두 보여줍니다. 검증된 법적 신원, 생체 정보 보증, 그리고 상호 운용 가능한 신뢰 체계의 결합은 사기 방지 및 디지털 신뢰 구축을 위한 강력한 모델을 제시합니다. 그러나 한국의 사례는 개인정보 보호와 사용자 통제권을 강화하는 접근 방식에 대한 관심이 높아지고 있음을 보여주며, 이는 새롭게 부상하는 PoH 기술의 방향과도 일맥상통합니다. 한국이 디지털 신뢰 체계를 발전시켜 나가는 과정에서, 미래의 발전 방향은 엄격한 실명 의무화보다는 개인의 권리와 디지털 경제에 대한 신뢰를 유지하면서 실제 사용자를 검증하는 균형 잡힌 모델에 더 초점을 맞출 가능성이 있습니다.

말레이시아: 마이디지털 ID와 생체인식 신뢰를 향한 길

말레이시아의 마이디지털 ID 사업은 공공 및 민간 서비스 접근성을 간소화하는 통합된 국가 지원 디지털 신원 체계를 구축하기 위한 중요한 발걸음입니다. 2024년 디지털 신원 청사진 (Digital Identity Blueprint)에 따라 출범한 이 시스템은 모든 거주자에게 국가등록국(NRD) 데이터베이스와 연동된 생체 인식 디지털 신분증을 발급합니다. [33] 얼굴 인식 및 보안 인증 기술을 사용하여 개인은 전자정부 포털, 은행, 통신 사업자 및 기타 온라인 서비스 전반에서 본인 인증을 할 수 있습니다. 국세청(LHDN) 및 일부 금융 기관과의 초기 시범 운영을 통해 2025년 전국적인 확대 시행을 위한 기반을 마련했습니다. [34]

기존의 신분증 시스템과 달리, 마이디지털 ID 는 자격 증명 및 검증 측면 역할을 동시에 수행하도록 설계되어 개인 정보를 반복적으로 공개하지 않고도 인증이 가능합니다. 신원이 검증된 생체 기록에 연결되어, 인간 성 증명(Proof of Human, PoH) 스타일의 검증 기반을 제공하며, 각 디지털 계정이 실제 고유한 개인과 일치함을 보장합니다. 말레이시아가 여러 분야에 걸쳐 디지털 검증을 확대함에 따라, 다른 경제권과 마찬가지로 완전한 신원 공개가 현실적으로 불가능하거나 바람직하지 않은 개방적이고 사용자 중심적인 환경에서 신뢰를 구축하는 데 어려움을 겪고 있습니다. 이러한 맥락에서 마이디지털 ID는 개인정보 보호를 유지하면서 상호 운용 가능한 방식으로 인간성과 고유성을 검증하는 미래의 PoH 메커니즘 의 핵심 기반이 될 수 있습니다.

이 시도는 모바일 뱅킹과 전자상거래 도입 증가와 함께 심화되고 있는 말레이시아의 사기 및 디지털 부정행위 문제에 직접적으로 대응하는 것입니다. 신뢰할 수 있는 신원 확인 체계는 규제된 생태계 내에서 신분 도용 및 가짜 계정 생성을 줄이는 데 도움이 될 수 있으며, PoH 방식의 검증은 궁극적으로 사기가 자주 발생하는 온라인 마켓플레이스, 소셜 미디어, 디지털 결제와 같은 규제가 미비한 공간으로 이러한 보호 기능을 확장할 수 있습니다.

하지만 이번 시행은 개인정보 보호, 데이터 보호 및 거버넌스에 대한 공개적인 논쟁을 불러일으켰습니다. 시민 사회 단체들은 생체 정보의 중앙식 저장과 데이터 접근 권한이 본래 목적 이상으로 확대될 경우 발생할 수 있는 오용 가능성에 대해 우려를 표명했습니다. [35] 이에 대응하여 정부는 디지털 ID 운영위원회를 설립하고, 개인정보보호법(PDPA) 준수를 재확인했으며, 말레이시아 중앙은행의 감독 하에 있는 [36] MySejahtera 및 eKYC 시스템과의 상호 운용성을 강조했습니다. 이러한 조치들은 시행이 투명성, 책임성 및 국민의 신뢰를 바탕으로 진행되도록 하기 위한 것입니다.

명확한 안전장치와 사용자 제어 기능을 갖춘다면, 마이디지털 ID는 PoH 혁신을 위한 신뢰 가능한 신원 적 기반으로 발전됩니다. 검증된 생체 정보, 사용자 동의, 그리고 안전한 상호 운용성을 결합한 이 구조는 신흥 경제국들이 검증된 고유성과 포용성을 디지털 신뢰 체계에 어떻게 접목할 수 있는지를 보여줍니다. 동남아시아의 경우, 말레이시아의 경험은 정부 주도의 신원 개발이 기존 디지털 ID 시스템과 미래의 PoH 모델 간의 격차를 해소하고, 개인정보 보호와 공공의 신뢰를 유지하면서 사기 방지 기능을 강화할 수 있음을 보여줍니다

필리핀: PhilSys 의 신속한 출시

필리핀 신분증 시스템(PhilSys)은 동남아시아에서 가장 빠르게 성장하는 디지털 신분증 시스템 중 하나입니다. 2018년 공화국법 제11055호에 따라 설립된 PhilSys는 모든 시민과 거주자에게 얼굴, 지문, 홍채 스캔을 포함한 생체 정보를 기반으로 하는 [37] 고유한 12자리 PhilSys 번호(PSN)를 부여합니다. 필리핀 통계청(PSA)이 관리하는 이 프로그램은 공공 서비스 접근성 향상, 금융 포용성 증진, 디지털 거래 보안 강화를 목표로 합니다. 2025년 말까지 8천만 명이 넘는 필리핀 국민이 등록했으며, eGovPH 앱과 national-id.gov.ph를 [38] 통해 이용 가능한 디지털 신분증은 정부 기관, 은행 및 민간 플랫폼 전반에서 널리 사용되고 있습니다.

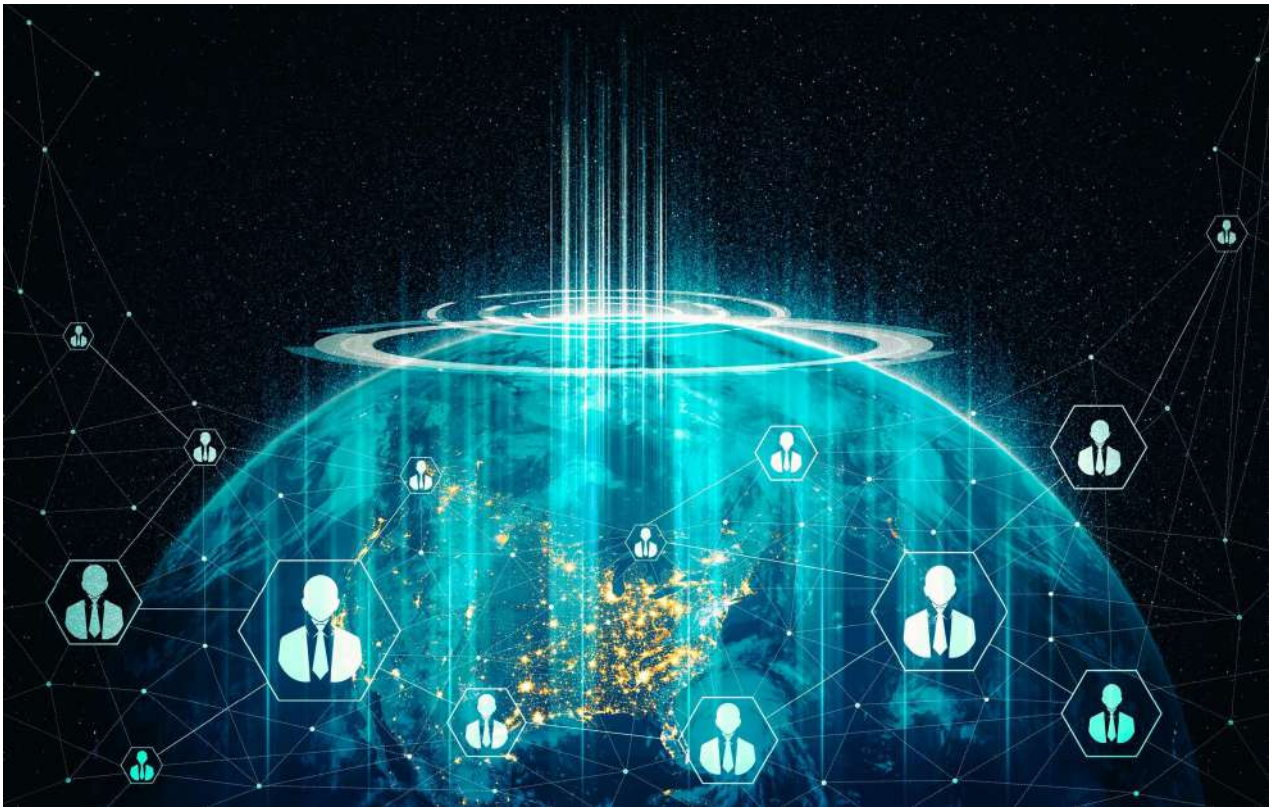
이번 신속한 도입은 신뢰할 수 있는 신원 확인을 위한 지역 차원의 노력에 있어 중요한 이정표가 될 것입니다. PhilSys는 검증된 생체 정보를 영구적이고 고유한 식별자와 연결함으로써, 중복 등록과 위조 신원 생성을 방지하는 국가 차원의 고유성 증명 체계를 효과적으로 구축합니다. 금융 기관, 통신 사업자, 정부 시스템과의 통합은 각 검증된 사용자가 실제 고유한 개인임을 확인하는 '인간성 증명(Proof of Human, PoH)' 의 초기 대규모의 아날로그 역할을 합니다. 실시간으로 QR 코드를 이용한 신원 확인을 가능하게 하는 eVerify 포털은 이러한 신뢰성을 디지털 결제, 사회 보장, SIM 카드 등록까지 확장합니다. [39]

동시에, 빠른 도입 속도는 새로운 거버넌스 및 개인정보 보호 문제를 야기했습니다. 기술적 오류, 카드 제작 지연, 데이터 처리 문제 등이 대중의 우려를 불러왔으며, 중앙 집중식 생체 정보 저장 및 불투명한 데이터 공유에 대한 우려는 더욱 강력한 보호 조치를 요구하는 목소리를 높였습니다. 이에 필리핀 공공안전청 (PSA)과 국가 개인정보보호위원회(NPC)는 감독 강화, 더욱 엄격한 암호화 표준 채택, 그리고 전자정부보건시스템 [40](eGovPH) 내에 동의 기반 접근 프로토콜을 도입하는 등의 조치를 취했습니다 . [41]

필리핀의 사례는 급속한 디지털 신뢰 확장의 가능성과 위험성을 모두 보여줍니다. 이 사례의 규모와 상호 운용성은 신흥 경제국이 금융 포용과 사기 감소가 가능한 신원 인프라로 어떻게 발전할 수 있는지를 보여줍니다. 그러나 이 사례는 신뢰 또한 기술과 함께 발전해야 한다는 점을 보여줍니다. 대중의 신뢰는 가시적인 책임성, 투명한 데이터 관리, 그리고 사용자 통제에 달려 있습니다. PhilSys가 지속적으로 발전함에 따라, 이는 PoH에 부합하는 혁신에 대한 가치있는 시도가 될 것입니다. 이 사례는 검증된 고유성이 강력한 개인정보 보호 및 포용성 안전장치와 결합될 때, 동남아시아 디지털 경제 전반에 걸쳐 사기 방지와 인간 중심적 신뢰가 어떻게 강화되는지를 보여줍니다.

사례 연구의 핵심 요점

이 네 가지 사례는 아시아 경제권이 신원 확인 인프라를 구축하는 데 있어 서로 다른 경로를 밟고 있음을 보여줍니다. 일본과 한국은 선진적인 규제 환경이 검증된 신원을 대규모로 제도화할 수 있는 방법을 보여주지만, 그 결과는 상반됩니다. 일본의 마이넘버 시스템은 데이터 거버넌스가 흔들릴 때 공공의 신뢰가 얼마나 취약한지를 보여주는 반면, 한국의 실명제도는 신원, 금융, 기술의 심층적인 통합이 가져올 효율성과 위험성을 보여줍니다. 동남아시아에서는 말레이시아의 마이디지털 ID와 필리핀의 필시스(PhilSys)가 두 가지 새로운 모델을 제안합니다. 하나는 신중한 설계에 기반한 거버넌스를 강조하는 모델이고, 다른 하나는 신속한 도입과 접근성을 우선시하는 모델입니다. 이 네 가지 사례 모두에서 공통적인 패턴이 나타납니다. PoH와 같은 검증은 투명성, 상호운용성, 사용자 제어 기능이 결합될 때 가장 효과적이며, 이를 통해 디지털 신원 시스템은 온라인 안전에 대한 대중의 신뢰를 약화시키는 것이 아니라 오히려 강화할 수 있습니다.



결론 및 제언

온라인 사기 및 부정행위는 아시아 태평양 지역 전반의 디지털 신뢰를 위협하는 주요 요인으로 자리 잡았습니다. 일본의 마이 넘버부터 필리핀의 PhilSys에 이르기까지 국가별 디지털 신분증 시스템은 검증된 포용적 신원 확인이라는 목표를 달성하는 데 기여했지만, 실시간 사기 방지 수단이라기보다는 주로 행정 도구에 그치고 있습니다. 새롭게 등장하는 인간성 인증(Proof of Human, PoH) 기술은 이러한 시스템에 중요한 보완 요소를 제공합니다. 개인 식별 정보를 공개하지 않고도 디지털 플랫폼, 금융 서비스, 통신 네트워크 전반에서 개인이 고유한 인간 사용자임을 증명할 수 있도록 지원합니다. PoH는 개인 정보 보호를 강화하는 인간 인증 신호를 추가함으로써 기존 디지털 신분증 시스템이 확인하기 어려웠던 자동화 및 규모화된 악용 사례를 해결할 수 있습니다. 따라서 PoH를 디지털 신원 생태계에 통합하면 강력한 개인정보 보호 장치를 유지하면서 사기 행위에 대한 복원력과 디지털 거래에 대한 대중의 신뢰를 모두 향상시킬 수 있습니다.

안전장치 및 거버넌스 섹션에서 강조했듯이, 책임감 있는 PoH 배포를 위해서는 위험 기반 설계, 명확한 사용자 보호, 그리고 기존 신원 확인 생태계와의 신중한 연계가 필요합니다. 이러한 원칙을 바탕으로 지역 정부는 다음과 같은 조치를 취할 수 있습니다.

- **디지털 ID 및 PoH기술을 사기 방지 전략에 통합.** 금융, 전자 상거래 및 통신 플랫폼에 고유성 검증 기능을 내장하여 신분 도용, 봇 기반 사기 및 합성 신원 위험을 줄이는 동시에 배포 과정이 비례성을 유지하고, 마찰을 최소화하며, ISO/IEC 25389와 같은 안전 체계에 부합하도록 보장합니다.

- **개인정보 보호 및 상호 운용 가능한 표준 지원.** 생체 인식 보증과 암호화 개인정보 보호를 결합한 지역 체계 개발을 장려하여, 검증 가능한 고유성이 사용자 익명성이나 국경 간 사용성을 방해하지 않고, PoH 신호가 추적이나 프로파일링에 악용될 수 없도록 합니다.

- **지역 정책 논의 및 조정을 촉진합니다.** APEC 비즈니스 자문 위원회, G20 디지털 금융 포용을 위한 하이레벨 원칙, UN 주도의 디지털 경제 이니셔티브와 같은 기존 메커니즘을 활용하여 정책 목표를 조율하고, 모범 사례를 공유하며, **정부와 플랫폼이 광범위한 도입에 앞서 고위험 환경에서 PoH를 테스트할 수 있는 통제된 샌드박스를 포함하여 여러 부문에 걸쳐 PoH 기반 검증을 위한 시범 체계를 모색합니다.**

이러한 조치들은 아시아에 더욱 신뢰할 수 있는 인간 중심적인 디지털 생태계를 구축하는 데 도움이 될 것입니다. 이런 생태계는 검증을 통해서 개인정보를 침해하지 않으며 보안을 강화합니다. 또한 안전장치와 거버넌스 체계를 통해 책임감 있는 사용을 보장합니다. 마지막으로 지역 협력을 통해 신원 확인 시스템이 행정 등록부에서 사기 방지 및 디지털 포용을 위한 능동적인 도구로 전환됩니다.

각주

[1] 사이버보안 벤처스(Cybersecurity Ventures) n.d. "세계 3위의 경제 부문은 악의적이며, 그 규모는 점점 더 커지고 있다." 2025년 8월 확인. https://cybersecurityventures.com/the-worlds-third-largest-economy-has-bad-intentions-and-its-only-getting-bigger/ .

[2] Feedzai. 2024. "GASA 글로벌 사기 현황 보고서: 사기로 인한 손실액 1조 달러." 2025년 8월 확인. https://www.feedzai.com/blog/gasa-global-state-of-scams-report-1t-lost-to-scams/ .

[3] GSMA. 2025. 사기 및 스캠 안전 보고서. 런던: 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, 변곡점: 사기 센터의 세계적 영향 (2025), xx쪽, https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf

[5] 글로벌 이니셔티브, 동남아시아의 사이버 범죄 사기 행위 (2025년 5월), https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf

[6] 미얀마에서 새로운 인신매매 동향 발생", 재팬 타임스 , 2025년 4월 2일, https://www.japantimes.co.jp/news/2025/04/02/japan/crime-legal/myanmar-scam-human-trafficking/

[7] 그들은 전 세계 사람들을 속일 수밖에 없었습니다. 현재 수천 명이 미얀마 국경에서 억류되어 있습니다." (AP 뉴스 , 2025년 3월 9일, https://apnews.com/article/myanmar-thailand-scam-centers-trapped-humanitarian-c1cab4785e14f07859ed59c821a72bd2)

[8] Signicat. 2024. "딥페이크를 이용한 사기 시도가 지난 3년간 2137% 증가했습니다." 2025년 8월 확인. https://www.signicat.com/press-releases/fraud-attempts-with-deepfakes-have-increased-by-2137-over-the-last-three-year .

[9] CSIS, 사이버 사기의 글로벌화: 동남아시아의 첨단 기술 사기 공장 실태 공개 , 2024년 12월 12일, https://www.csis.org/analysis/cyber-scamming-goes-global-unveiling-southeast-asias-high-tech-fraud-factories

[10] TRM Labs, 불법 암호화폐 생태계 보고서 (2022), https://www.trmlabs.com/resources/reports/the-illicit-crypto-ecosystem-report-2022 .

[11] Meta, "사기 센터 배후의 조직 범죄 단속", 2024년 11월 21일, https://about.fb.com/news/2024/11/cracking-down-organized-crime-scam-centers/

[12] TRM Labs, 2025년 암호화폐 범죄 보고서 , https://www.trmlabs.com/reports-and-whitepapers/2025-crypto-crime-report

[13] 세계은행, 디지털 신원 확인 툴킷 (세계은행), 자격 증명 및 스마트 카드 기반 전자 신분증(eID) 관련 섹션 . https://documents1.worldbank.org/curated/en/147961468203357928/pdf/912490WP0Digit00Box385330B-00PUBLIC0.pdf

[14] 금융행동특구(FATF), 디지털 신원 확인 지침 (파리: FATF/OECD, 2020년 3월), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity.pdf (디지털 신원 확인의 일환으로 생체 인증에 대한 논의).

[15] SITA 및 PRISM, 생체인식 디지털 신원: 원활한 여행 및 정부 서비스의 다음 단계 (2023), https://www.sita.aero/globalassets/docs/other/biometric-digital-identity-govt-services-prism-report.pdf

[16] OECD, 국가 디지털 신원(NDID) 플랫폼(태국), https://www.oecd.org/content/dam/oecd/en/topics/policy-issues/tax-administration/thailand-national-digital-identity-platform.pdf

17. 디지털 신원 집중 조명: 싱가포르", 1Kosmos, https://www.1kosmos.com/identity-management/digital-identity-spotlight-singapore/

18. 대만의 미래 방향을 모색하는 가운데 아시아 여러 국가의 디지털 신원 확인 시스템 비교" , BiometricUpdate , https://www.biometricupdate.com/202102/digital-identity-systems-around-asia-compared-as-taiwan-seeks-path-forward

19. Kleros, Proof of Humanity(PoH) 문서 , "Proof of Humanity(PoH)는 소셜 검증과 비디오 제출을 결합하여 실제 사람으로 구성된 신뢰할 수 있는 목록을 생성하는 시빌 공격 방지 인간 등록 시스템입니다." https://docs.kleros.io/products/proof-of-humanity

20. 일본 정부, 내각부 , "사회보장 및 납세자 번호 시스템(마이 넘버 시스템) 개요", 2016, https://www.cao.go.jp/bangouseido/english/.

21. 내무성(MIC), "사회보장 및 납세자 번호 제도 개요", 2024년 개정판.

22. 일본 디지털 에이전시, 마이 넘버 카드 통계 포털 , "마이 넘버 카드 발급 건수", 2025년 10월 업데이트; "일본 마이 넘버 카드 발급 9천만 장 돌파했지만 신뢰 문제는 여전히 남아 있다", 닛케이 아시아 , 2025년 7월 12일.

23. 일본, 건강보험 데이터 오류로 일부 마이넘버 연동 중단", 로이터 , 2023년 5월 28일

24. "일본, 마이넘버를 은행 업무 및 SIM 카드 등록과 연동하려 한다", 재팬 타임스 , 2024년 3월 9일.

25. 마이넘버 시스템의 결함을 개선해야 한다", 재팬 타임스 (사설), 2023년 6월 2일; 디지털 에이전시, "마이넘버 시스템에 대한 신뢰도 향상을 위한 노력", 2024년.

26. 행정안전부, "주민등록제도 개요", 대한민국 정부, 2023.

27. 한국방송통신위원회, 디지털 환경에서의 실명 확인 정책, 2022.

28. 국토교통부(MOLIT), "모바일 운전면허 서비스 출시", 보도자료, 2022년 1월.

29. 한국인터넷보안협회(KISA), "한국의 디지털 인증 사용 현황", 2024년; 연합뉴스, "PASS 앱, 한국 사용자 5천만 명 돌파", 2025년 5월 9일.

30. OECD, 한국의 디지털 정부: 스마트하고 포용적인 사회 구현 , 2023, 45쪽.

31. 코리아중앙데일리 , "대규모 데이터 유출로 보안 관행에 대한 의문 제기", 2023년 2월 4일; 코리아타임스 , "수백만 명에게 영향을 미친 데이터 유출로 신용정보업체에 벌금 부과", 2023년 4월 15일.

32. 정보통신부, "안전한 인증을 위한 디지털 신원 시범 사업", 2023년; 개인정보보호위원회(PIPC), "개인정보보호법 개정안", 2023년 12월.

33. 말레이시아 디지털 경제 청사진 (MyDIGITAL), 디지털 정부 부서, 통신디지털부, "디지털 신원 청사진", 말레이시아 정부, 2024.

34. 국가 등록부(Jabatan Pendaftaran Negara, JPN), "LHDN 및 금융 기관과 함께 MyDigital ID 파일럿 구현", 보도자료, 2024년 6월.

35. 말레이 메일 , "개인정보보호 지지자들이 중앙 집중식 생체인식 데이터베이스에 대한 우려를 제기하다", 2024년 4월 5일.

36. 정보통신디지털부(KKD), "디지털 ID 운영위원회 구성", 2024년 2월 15일; 말레이시아 중앙은행, e-KYC 시행 지침 , 2023년 개정.

[37] 필리핀 공화국 관보, 2018년 8월, 공화국 법률 제11055호, "필리핀 신분증 시스템(PhilSys) 설립에 관한 법률".

[38] 필리핀 통계청(PSA), PhilSys 대시보드: 등록 및 발급 데이터 , 2025년 10월 업데이트; Inquirer.net , "8천만 명 이상의 필리핀 국민이 국가 신분증에 등록 - PSA", 2025년 9월 14일.

[39] PSA, "PhilSys eVerify 포털 출시 및 QR 검증 기능", 2024.

[40] Rappler , "국가 신분증 데이터 공유에 대한 개인정보보호 우려 고조", 2024년 6월 22일; Philippine Star , "국가 신분증 발급 지연 및 데이터 오류로 비판 촉발", 2024년 5월 10일.

[41] 국가개인정보보호위원회(NPC), "국가 신분증 시스템 데이터 보호 기준에 관한 NPC 자문 보고서", 2024; 공안청(PSA), "ePhilID 도입을 위한 강화된 보안 조치", 2024.