JDFR Journal of Data Forensics Research
데이터포렌식연구, 2권 2호, 2025년 12월, 197-225면
Journal of Data Forensics Research, Volume 2, Issue 2, December 2025, Pages 197-225.
https://doi.org/10.12972/JDFR.2025.2.2.5
Print ISSN 3058-9460
Online ISSN 3058-9479

원저

홍콩·대만 사기범죄 대응체계 분석 및 시사점: ADCC·FMLIT 및 하이테크 수사센터·FIU 사례를 중심으로

권우성

경기북부경찰청 범죄수익추적팀장

교신저자: 권우성, sunderland@police.go.kr

요약

본 연구는 2025년 홍콩 국제금융수사과정(IFIC)과 대만 법무부 수사국(MJIB) 주관 초국경 사기범죄 대응 워크숍의 발표 및 인터뷰 자료를 분석하였다. 홍콩은 사기대응조정센터(ADCC)와 사기·자금세탁정보태스크포스(FMLIT)를 통해 24시간 상담 핫라인 운영, 실시간 자금 차단(누적 2.4조 원), 선제적 피해자 보호(630억 원 예방) 등의 성과를 거두었다. 대만은 하이테크 수사센터의 디지털 포렌식, 암호화폐 추적, 빅데이터 플랫폼(AIT) 활용과 FIU의 연간 360만 건 현금거래보고 자동화 시스템을 구축하였다. 본 연구는 양국 사례 비교를 통해 한국의 FIU-경찰 협력 강화, 실시간 자금 차단 체계 구축, 통합 대응 기구 설치, 민관 협력 법적 근거 마련 등 구체적 정책 제언을 제시한다.

주제어

사기범죄, ADCC, FMLIT, FIU, 금융범죄, 실시간 자금 차단, 민관 협력, 국제 공조, 디지털 포렌식, 빅데이터 분석, 하이테크 수사센터

Open Access

Received: December 05, 2025
Revised: December 30, 2025
Accepted: December 31, 2025
Published: December 31, 2025

© 2025 Korean Data Forensic Society

This is an Open Access article distributed under the terms of the Creative Commons CC BY 4.0 license (https://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Original Article

Anti-fraud response systems in Hong Kong and Taiwan and their implications for Korea: Focusing on ADCC·FMLIT and High-tech Investigation Center·FIU cases

Woo-sung Kwon

Team Leader Criminal Proceeds Tracking Team, Gyeonggi Bukbu Provincial Police Agency, Republic of Korea

Corresponding Author: Woo-sung Kwon, sunderland@police.go.kr

ABSTRACT

This study analyzes presentations and interview data from the International Financial Investigation Course (IFIC) held in Hong Kong in August 2025 and the Cross-Border Fraud Crime Response Workshop organized by the Ministry of Justice Investigation Bureau (MJIB), Taiwan, from April 29 to May 3, 2025. Hong Kong has achieved significant results through the Anti-Deception Coordination Centre (ADCC) and Fraud and Money Laundering Intelligence Taskforce (FMLIT) that operate a 24-h consultation hotline, real-time fund blocking system (cumulative KRW 2.4 trillion blocked), and proactive victim protection (KRW 63 billion prevented). Taiwan has established a High-Tech Investigation Center using digital forensics, cryptocurrency tracking, and big data platform (AIT), along with an FIU system that processes 3.6 million annual cash transaction reports through automation. Through comparative analysis of both cases, this study proposes specific policy recommendations for Korea, including strengthening FIU–police cooperation, establishing real-time fund blocking systems, creating integrated response organizations, and providing legal grounds for public–private partnerships.

KEYWORDS

fraud crime, ADCC, FMLIT, FIU, financial crime, real-time fund blocking, public-private cooperation, international cooperation, digital forensics, big data analysis, high tech investigation center, Taiwan MJIB

I. 서론

1.1. 연구 배경 및 문제 제기

전 세계적으로 디지털 기술의 발전과 함께 사기범죄가 급증하고 있다. 특히 국경을 넘나드는 조직적 사기범죄는 전통적인 수사 기법만으로는 대응하기 어려운 새로운 치안 위협으로 부상하고 있다. 한국의 경우 2024년 보이스피싱 등 전화금융사기 피해액이 연간 8,000억 원을 초과하는 등 심각한 사회문제가 되고 있다[1].

홍콩은 2016년 이후 사기범죄가 폭발적으로 증가하여 2024년 전체 범죄의 46.9%를 차지하는 위기 상황에 직면했다. 그러나 홍콩 당국은 사기대응조정센터(Anti-Deception Coordination Centre, ADCC)와 사기·자금세탁정보태스크포스(Fraud and Money Laundering Intelligence Taskforce, FMLIT)라는 혁신적인 이중 대응체계를 구축하여 효과적으로 대응하고 있다.

홍콩의 사기범죄 대응체계는 2019년 FATF(국제자금세탁방지기구) 상호평가에서 우수 사례로 인정받았으며, 영국 왕립국제문제연구소(RUSI)의 정보 공유 모범 사례로도 소개되었다[2]. 한편 대만도 2016년 하이테크 수사센터와 FIU를 통해 디지털 포렌식, 암호화폐 추적, 빅데이터 분석 등 첨단 기술을 활용한 범죄 대응 체계를 구축했다.

1.2. 연구 목적 및 범위

본 연구는 홍콩의 사기범죄 대응체계를 심층 분석하고 대만의 기술 중심 접근법을 보완적으로 검토하여 한국의 사기범죄 대응체계 개선을 위한 실질적 시사점을 도출하는 것을 목적으로 한다. 본 연구의 주요 분석 대상은 2025년 8월 18일 홍콩에서 개최된 International Financial Investigation Course에서 홍콩 경찰 상업범죄수사국이 발표한 공식 자료와 2025년 4월 29일부터 5월 3일까지 타이페이에서 개최된 대만 법무부 수사국(MJIB) 주관 '2025년 초국경 사기범죄 대응 워크숍'에서의 발표 자료 및 대만 고등검찰청, 법무부 수사국 산하 FIU 지국장과의 현장 인터뷰 자료를 기반으로 한다. 인터뷰 대상은 대만 법무부 조사국(MJIB) 자금세탁방지과(Anti-Money Laundering Division)의 과장(Section Chief)으로, 해당 부서는 대만 금융정보분석원(FIU)의 역할을 수행하고 있다[3,4].

1.3. 연구 질문

본 연구는 다음과 같은 연구 질문에 답하고자 한다. 첫째, 홍콩의 사기범죄 급증 현황과 특성은 무엇인가. 둘째, ADCC의 24시간 실시간 대응체계는 어떻게 운영되는가. 셋째, FMLIT의 민관 협력 기반 정보 공유 시스템은 어떤 메커니즘으로 작동하는가. 넷째, 대만의 기술 중심 접근법과 FIU 정보 공유 체계는 어떤 특징을 갖는가. 다섯째, 한국에 적용 가능한 정책적 시사점은 무엇인가.

1.4. 연구 방법론

본 연구는 다음과 같은 방법론을 사용한다. 첫째, 문헌 분석으로 홍콩 경찰 및 대만 검찰의 공식 발표 자료, FATF 보고서, 학술 논문 등을 검토한다. 둘째, 사례 분석으로 ADCC와 FMLIT의 구체적 운영 사례를 심층 분석한다. 셋째, 인터뷰 분석으로 대만 FIU 담당자와의 심층 인터뷰

내용을 분석한다. 넷째, 비교 분석으로 한국의 현행 사기범죄 대응체계와 비교하여 시사점을 도출한다.

II. 이론적 배경

2.1. 사기범죄의 개념과 유형

사기범죄는 기망행위를 통해 타인을 착오에 빠뜨려 재산상 이익을 취득하는 범죄를 의미한다. 전통적으로 대면 사기가 주를 이루었으나, 디지털 기술의 발전과 함께 비대면 사기가 급증하고 있다[5].

현대 사기범죄의 주요 유형은 다음과 같다.

첫째, 익명성과 비대면성으로 인해 범죄자 추적이 어렵다. 범죄자는 가짜 신분, VPN, 다크웹 등을 활용하여 신원을 은폐하고, 피해자와 대면하지 않아 범행 후 즉시 도주가 가능하다.

둘째, 국경을 넘나드는 초국경 범죄로 단일 국가의 대응만으로는 한계가 있다. 범죄 조직은 동남아시아, 중국 등에 콜센터를 설치하고 한국, 일본 등을 표적으로 삼아 각국 법집행기관의 관할권 공백을 악용한다.

셋째, AI 기술을 활용한 딥페이크 영상, 음성 합성 등 신종 수법이 지속적으로 등장하고 있다. 2024년 홍콩에서는 딥페이크 영상회의를 통해 재무담당자를 속여 2억 홍콩달러(약 330억 원)를 편취한 사례가 발생했다.

넷째, 소셜미디어와 메신저 등 디지털 플랫폼을 통해 불특정 다수를 동시에 표적으로 삼을 수 있다. 페이스북, 인스타그램, 텔레그램 등을 통해 수천 명에게 동시에 접근하여 대규모 피해를 양산한다.

다섯째, 암호화폐를 활용한 자금 세탁으로 범죄 수익 추적이 어렵다. 비트코인, 이더리움 등 암호화폐는 익명성과 국경 간 즉시 이체가 가능하여 전통적인 금융 추적 기법으로는 한계가 있다.

2.2. 사기범죄 대응의 국제적 동향

사기범죄의 국제화에 따라 각국은 협력적 대응체계를 강화하고 있다. FATF는 2012년 이후 40개 권고안에서 자금세탁방지(AML)와 테러자금조달방지(CFT)를 위한 국제 협력을 강조하고 있다[6].

주요 국가의 대응 사례로는 다음과 같다. 미국은 금융범죄단속반(FinCEN)을 중심으로 의심거래보고(STR) 시스템을 운영하고 있다. 영국은 국가경제범죄센터(NECC)를 신설하여 통합적 대응체계를 구축했다. 싱가포르는 사기대응센터(Anti-Scam Centre)를 통해 실시간 자금 차단 시스템을 운영하고 있다. 대만은 과학기술수사중심(科技偵查中心)을 통해 디지털 포렌식과 빅데이터 분석 역량을 강화하고 있다[7].

2.3. 민관 협력의 이론적 기반

민관 협력의 성공 요인으로는 다음과 같다.

첫째, 명확한 법적 근거와 역할 분담이 필요하다. 각 주체의 권한과 책임이 법률로 명시되어야 협력 과정에서 발생할 수 있는 법적 리스크를 최소화할 수 있다. 홍콩의 FMLIT는 경찰·금융

감독청·은행의 역할을 명확히 구분하여 정보 공유는 경찰이 중개하되, 각 은행은 자체 시스템 내에서 자율적으로 대응하는 구조를 확립했다. 이를 통해 개인정보보호법(PDPO) 규정을 준수하면서도 신속한 정보 전달이 가능한 삼각 구조(A은행 → 경찰 → B은행)를 구축했다.

둘째, 실시간 정보 공유 시스템이 구축되어야 한다. 사기범죄는 시간과의 싸움이므로, 의심 계좌 정보가 2시간 이내에 전체 금융기관에 전파될 수 있는 기술적 인프라가 필수적이다. 홍콩은 표준화된 정보 요청 양식과 자동화 시스템을 통해 96%의 2시간 내 응답률을 달성했다. 각 은행이 24시간 대응팀을 구성하고, ADCC의 정보 요청을 받으면 자동으로 담당자에게 알림이 전달되는 시스템을 구축하여 신속한 대응이 가능하다.

셋째, 상호 신뢰와 자발적 참여를 기반으로 해야 한다. 강제적 규제보다는 금융기관이 정보 공유의 실익을 체감하고 자발적으로 참여할 때 지속가능한 협력이 가능하다. 대만 FIU는 금융기관과 '파트너'로서 소통하며, 제공된 정보가 실제 범죄 검거로 이어지는 성과를 지속적으로 공유함으로써 신뢰를 구축했다.

넷째, 개인정보보호와 보안의 균형을 유지해야 한다. 과도한 정보 공유는 개인정보 침해 논란을 야기할 수 있으므로, 정보 최소화 원칙, 접근권한 관리, 로그 감사 등 기술적·제도적 안전장치가 병행되어야 한다. 홍콩은 PDPO 규정을 준수하면서도 경찰을 중개자로 하는 삼각 구조를 통해 이 균형을 달성했다.

2.4. 디지털 포렌식과 빅데이터 분석

현대 사기범죄는 디지털 환경에서 발생하므로 디지털 포렌식 역량이 필수적이다. 디지털 포렌식은 전자적 증거를 수집·분석·보존하는 과학적 절차를 의미한다[8].

대만의 사례에서 보듯이 전문 도구를 활용하여 컴퓨터와 스마트폰의 데이터를 추출하고 분석할 수 있다. EnCase Forensic, Cellebrite UFED, MSAB XRY 등은 전 세계 법집행기관이 사용하는 표준 디지털 포렌식 도구로, 컴퓨터 및 모바일 기기에서 증거를 추출하고 분석하는 데 활용된다[9-11].

2.5. 실시간 자금 차단의 법리

실시간 자금 차단은 사기 피해 최소화를 위한 핵심 수단이다. 그러나 재산권 보호와 신속한 대응이라는 두 가치 사이의 균형이 필요하다. 헌법재판소는 전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법의 지급정지 조항에 대해, 명의인의 재산권 제한이 중대하지만 피해금 인출 방지를 통한 피해자 구제의 공익적 목적이 정당하다고 판시하며 합헌 결정을 내린 바 있다[12]. 이는 신속한 피해자 구제와 계좌명의인의 재산권 보호라는 두 법익 간 균형의 필요성을 명확히 한 것이다.

각국의 법적 근거를 살펴보면, 한국은 전기통신금융사기피해방지및피해금환급에 관한특별법에 따라 금융기관의 거래정지 권한을 부여하고 있다[13]. 홍콩은 행정적 조치인 Letter of No Consent(LNC) 제도를 활용하고 있다[14]. 싱가포르는 결제서비스법에 따라 즉시 동결 권한을 부여하고 있다[15].

III. 홍콩 사기범죄 대응체계

3.1. 사기범죄 현황 및 대응 전략

홍콩의 사기범죄는 지난 10년간 급격한 증가세를 보이며 사회적 최대 치안 위협으로 부상했다. 특히 2016년 전체 범죄의 12%에 불과하던 사기 사건이 2024년에는 46.9%까지 증가하여 거의 절반에 달하는 수준이다.

<Table 1> Trends in fraud cases in Hong Kong (2016-2025)

연도	사기 사건 수	전체 범죄 중 비율	전년 대비 증가율	총 피해액(약 HKD)
2016	약 8,000건	12%	-	미공개
2020	약 20,000건	30%	약 150%	약 30
2023	약 32,000건	42%	40%	45
2024	약 44,000건	46.9%	11%	35.4
2025(상반기)	약 20,000건	47%	4.3%	약 17

출처: 홍콩 경찰 상업범죄수사국[3]

주목할 점은 증가율 자체는 둔화 추세를 보인다는 것이다. 2023년 40% → 2024년 11% → 2025년 상반기 4.3%로 감소한 것은 홍콩 당국의 적극적 대응 노력이 효과를 거두기 시작했음을 시사한다. 사건 수 증가에도 불구하고 총 피해액은 오히려 21% 감소(35.4억 홍콩달러, 약 5,770억 원)한 것은 조기 차단 시스템의 실질적 효과를 보여주는 중요한 지표이다.

<Table 2> Financial losses by major fraud type in Hong Kong (2024, Unit: HKD Billion)

사기 유형	피해액	비율	신고건수	특징
투자 사기	16.91	47.7%	약 8,000건	고수익 투자 미끼
조직적 범행취업 사기	6.06	17.1%	약 5,000건	해외 취업 명목
인신매매 연계 온라인 쇼핑 사기	4.05	12.7%	약 15,000건	신고 건수 1위
콘서트 티켓 등 전화 사기	3.80	10.7%	약 7,000건	공안 사칭, 중국 본토 유학생 표적
로맨스 스캠	2.40	6.8%	약 3000건	고액 피해, 심리 상담 필요
기타	1.77	5.0%	약 6,000건	-
합계	35.44	100%	약 44,000건	

출처: 홍콩 경찰 상업범죄수사국[3]

투자 사기가 16.91억 홍콩달러(약 2,760억 원)로 최대 피해를 기록했으며, 취업 사기가 6.06억 홍콩달러(약 990억 원)로 뒤를 이었다. 이 두 유형이 전체 피해의 65%를 차지하는 것은 조직적이고 계획적인 범죄의 특성을 보여준다.

전화 사기는 두 가지 유형으로 구분된다. 관료 사칭형은 중국 공안 등을 사칭하여 범죄 연루를 주장하고 수사 협조 명목으로 고액 이체를 유도한다. 서비스 사칭형은 택배회사 등 일상적 서비스업체를 사칭한 소액 다수 건 사기이다.

홍콩 당국은 사기범죄를 단순한 치안 문제가 아닌 금융 중심지로서의 신뢰도와 직결된 국가적 과제로 인식하고 체계적 대응 전략을 수립했다.

이중 대응 체계를 구축한 것이 핵심이다. ADCC는 즉각적 피해 차단 및 현장 대응을 담당하

고, FMLIT는 구조적 분석 및 중장기 예방을 담당한다. 이러한 이중 체계는 응급실과 예방의학과가 협력하는 의료 시스템과 유사한 접근법으로 평가된다.

3.2. ADCC(사기대응조정센터) 운영 체계

2017년 7월 20일 ADCC 설립은 당시 급증하기 시작한 사기범죄에 대해 기존의 분산된 대응 방식으로는 한계가 있다는 인식에서 출발했다. 홍콩 경찰은 사기범죄에 대한 통합적 대응 역량을 강화하고 경찰 내부 및 외부 이해관계자들 간의 협력을 증진시키기 위해 상업범죄수사국(Commercial Crime Bureau) 산하에 전담 조직을 신설했다[16].

<Table 3> ADCC organizational structure

구분	인원	주요 역할
총 인력	90명	24시간 3교대 운영
작전 부문	40명	24시간 핫라인 운영, 실시간 자금 차단, 현장 대응
정보 부문	약 30명	데이터 분석, 상류 개입, 고 위험 피해자 관리
홍보·교육 부문	20명	3T 전략 캠페인, 대학생 프로그램, 미디어 대응
은행동맹(ADA)	10개 은행 상주	실시간 정보 조회, 즉각 계좌 조치

출처: 홍콩 경찰 상업범죄수사국[3]

ADCC의 조직 구성은 단순히 인력을 모아놓은 것이 아니라, 각 부문이 유기적으로 연결되어 실시간 대응이 가능하도록 설계되었다는 점에서 의미가 있다.

<Table 4> ADCC 24/7 hotline operational performance

지표	2023년	2024년	증감
연간 접수 건수	52,600건	80,000건	+52%
일평균 접수	144건	219건	+52%
IVR 자동 처리 비율	0% (미도입)	41%	+41%p
평균 대기 시간	약 8분	약 4분	-50%
상담원 1인당 처리 건수/일	약 12건	약 18건	+50%

출처: 홍콩 경찰 상업범죄수사국[3]

2025년 초 도입한 대화형 음성 응답 시스템(IVR)은 단순 반복 문의를 41% 감소시켜 상담원이 복잡한 사안에 집중할 수 있게 했다. 현재 AI 기반 1차 상담 시스템 도입을 검토 중이다. 기억하기 쉬운 번호 18222를 사용하여 시민 접근성을 극대화했다.

<Table 5> Performance of the real-time fund interception system (2023. 11 since implementation)

지표	누적 성과 (2023.11~2025.6)
처리 건수	41,000건
차단 금액	150억 HKD (약 2조 4,000억 원)
2시간 내 응답률	96%
30분 내 응답률	약 60% (일부 은행)
참여 은행	28개 (홍콩 전체 시중은행)
국제 협력 국가	3개국 (중국, 싱가포르, 말레이시아)

출처: 홍콩 경찰 상업범죄수사국[3]

이는 법적 강제가 아닌 자율적 협력에 기반한 것이어서 더욱 주목할 만하다. 은행들이 자체적으로 24시간 대응팀을 구성하고 자동화 시스템을 구축하여 일부 경우 30분 이내 응답을 달성하고 있다. 국제 협력으로는 중국, 싱가포르, 말레이시아와 실시간 자금 차단 협약을 체결했으며, 인터폴 I-GRIP 시스템을 통한 전 세계 협력도 진행하고 있다.

이 시스템의 핵심은 역추적 수사(Upstream Intervention)이다. 신고된 대포통장으로 입금한 모든 계좌를 분석하여 잠재적 피해자를 선제적으로 찾아내는 방식으로, 전 세계적으로도 드문 혁신적 접근법이다.

<Table 6> Performance of upstream scam intervention

기간	2023.5~2024.12	2025.1~2025.6	누적
접촉 잠재적 피해자	9,000명	6,000명	15,000명
예방 금액	2.3억 HKD	1.56억 HKD	3.86억HKD(약 630억 원)
1인당 평균 예방 금액	약 25,600 HKD	약 26,000 HKD	약 25,700HKD(약 420만 원)
고위험 피해자 보호 조치	-	450건	450건(2025.3 도입)
인터넷뱅킹 제한 조치	-	180건	180건
현장 출동	-	120건	120건
심리 상담 연계	-	85건	85건

출처: 홍콩 경찰 상업범죄수사국[3]

2025년 3월부터 시행된 고위험 피해자 보호 조치는 특히 주목할 만하다. 대상은 학생, 고령자 등 취약 계층이며, 조치 내용은 인터넷뱅킹 이용 제한, 지점 방문 시 ADCC 직원 현장 출동, 심리 상담사 개입(필요시), 전 은행 대상 피해자 정보 공유 등이다.

실제 사례로 45세 여성 피트니스 코치의 경우, 피해 규모 6백만 홍콩달러(약 9.8억 원)의 로맨스 스캠 피해가 예상되었다. 대응 과정은 수개월간 설득 시도, 강화 조치 시행, 지점 강제 방문, 상담 성공으로 이어졌다. 이 사례는 공개 세미나에서 교육 목적으로 소개된 것으로, 피해자의 신원 보호를 위해 최소한의 정보만 공개되었으며 국외 언론 보도나 ADCC 공식 웹사이트에는 게재되지 않았다. Upstream Scam Intervention 프로그램에 대한 일반 통계는 ADCC 공식 웹사이트를 참조할 수 있다[3].

ADCC 사무실 내 주요 10개 은행 상주 직원 배치는 전 세계적으로도 드문 혁신적 협력 모델이다. 이들은 자사 시스템에 직접 접근할 수 있는 권한을 보유하여 즉석 정보 조회와 계좌 조치가 가능하다.

홍콩의 개인정보보호법(Personal Data Privacy Ordinance, PDPO)은 1996년 시행된 이래

아시아에서 가장 오래된 포괄적 개인정보보호법 중 하나로, Data Protection Principles (DPPs)를 통해 개인 데이터의 수집, 사용, 보안을 규제한다[17]. 이러한 법적 제약 하에서 FMLIT는 경찰을 중심으로 한 정보 공유 구조를 구축했다. 2025년 8월 홍콩 경찰 발표 자료에 따르면, A은행이 의심 계좌 정보를 직접 B은행과 공유할 수 없지만, 경찰(FMLIT)을 통한 삼각 구조(A은행 → 경찰 → B은행)로 정보를 전달함으로써 법적 제약을 준수하면서도 신속한 정보 공유를 가능하게 했다[3]. 경찰은 "은행들은 PDPO 규정상 고객 정보를 직접 다른 은행과 공유할 수 없지만, FMLIT 플랫폼을 통해 경찰이 중개자 역할을 함으로써 합법적이고 신속한 정보 공유가 가능하다"고 설명했다[3].

이러한 구조적 한계를 개선하기 위해 홍콩은 2023년 6월 은행 간 직접 정보 공유를 허용하는 FINEST(Financial Intelligence Evaluation Sharing Tool) 플랫폼을 출범시켰으나, 이는 법인 계좌에 한정되며 개인 계좌로의 확대는 단계적으로 추진 중이다[18].

ADCC는 각 은행의 대포통장 개설 현황을 실시간 모니터링하여 특정 은행에서 급증하는 패턴을 발견 즉시 해당 은행에 경고하고 개선을 요구한다. 또한 신종 수법 정보를 공유한다. AI 생성 사진/영상을 이용한 원격 계좌 개설 탐지법, 자선단체 계좌를 이용한 계좌 유효성 테스트 수법, 중개업체 계좌를 활용한 자금 세탁 기법 등이다.

3.3. FMLIT(사기·자금세탁정보태스크포스) 심층 분석

FMLIT는 단계적으로 발전했다. 2017년 5월 시범 사업으로 출발하여 경찰, HKMA(홍콩금융관리국), 10개 은행이 참여했다. 2019년 6월 정식 출범 및 확대 운영을 시작했다. 2023년에는 SVF(저장가치시설) 업체 6곳이 추가 참여하여 디지털 금융까지 포괄하게 되었다.

FATF 2019 상호평가에서 홍콩 AML 체계의 핵심 요소로 인정받았으며, 영국 왕립국제문제연구소(RUSI)의 정보 공유 모범 사례로 소개되었다. 이는 FMLIT가 단순한 지역적 실험을 넘어 국제 표준으로 인정받았음을 의미한다.

<Table 7> FMLIT 3 floor organizational structure

층위	구성	운영	주요 역할
전략 그룹	경찰, HKMA, 주요 은행 CEO급	6개월마다 정기 회의	거시적 범죄 동향 분석, 대응 전략 수립, 정책 결정
운영 그룹	실무진(경찰, HKMA, 은행 담당자)	주 1회 회의	일일 정보 요청 처리, 표준 양식 운영, 신속 대응
경보 기능	FMLIT 분석팀	수시 발령	신종 수법 경보 발령 (누적 43건), 금융업계 전파

출처: 홍콩 경찰 상업범죄수사국[3]

전략그룹은 FMLIT의 "두뇌" 역할을 한다. 현재 주요 의제는 전화 사기 및 투자 사기의 구조적 대응 방안, 디지털 금융 확산에 따른 새로운 리스크 관리, 국제 협력 확대 방안 등이다.

운영그룹은 FMLIT의 "심장" 역할을 한다. 일일 업무로 수사팀의 정보 요청을 접수 및 처리하며, 정보 요청서 및 회신 양식을 통일하여 효율성을 극대화하고, 평균 응답 시간을 대폭 단축하여 수사 지연을 최소화한다.

경보기능은 FMLIT의 "신경계" 역할을 한다. 총 43건의 경보를 발령하여 신종 사기 수법 및 자금 세탁 동향을 실시간으로 금융업계에 전파했으며, 각 은행이 경보 내용을 바탕으로 시스템

업그레이드 및 모니터링 강화를 실시했다.

<Table 8> FMLIT Comparison of key projects

구분	Project Analyst	Project MIDAS	대포통장 네트워크 대응
시작 시기	2017년 (초기)	2024년	2025년
목적	전화 사기 대포통장 정보 공유	빅데이터 기반 패턴 분석	고위험 인물·법인 집중 관리
방식	경찰 → 은행 정보 제공 → 은행 자체 점검	AI 기반 의심 거래 자동 탐지	5개 이상 사건 연루자 타겟팅
주기	수시	월간 종합 보고서	실시간
성과	숨겨진 대포통장 발굴	패턴 기반 예측 가능	전 금융업계 완전 차단 + 검거 연계
기술 수준	기본 (정보 공유)	중급 (빅데이터 분석)	고급 (AI + 실시간 네트워킹)

출처: 홍콩 경찰 상업범죄수사국[3]

Project Analyst는 경찰이 보유한 대포통장 정보를 은행에 제공하면, 은행들은 자체 시스템을 통해 관련 계좌들을 찾아낸다. 이 과정에서 경찰이 몰랐던 추가 대포통장들이 대거 발견되었다.

Project MIDAS는 Project Analyst를 한 단계 진화시킨 것이다. ADCC 자금 차단 데이터베이스에서 패턴을 분석하고, AI 기반 의심 거래를 자동 탐지하며, 월간 종합 보고서를 작성 및 배포하고, 회원 기관별 맞춤 대응 방안을 제시한다.

대포통장 네트워크 대응은 가장 진화된 형태의 대응이다. 5개 이상 사건에 연루된 고위험 인물·법인을 집중 관리하고, 1개 기관에서 발견 즉시 전체 금융업계에 공유하여 완전 차단하며, 확인된 정보를 수사팀에 직접 전달하여 검거까지 연결한다.

<Table 9> FMLIT cumulative performance (2017~2025)

성과 지표	수치
미확인 계좌 발굴	52,000개 이상
STR(의심거래보고) 생성	5,000건 이상
동결 자금	20억 HKD (약 3,260억 원)
최종 검거 인원	655명
신종 수법 경보 발령	43건
참여 금융기관	34개 (은행 28개 + SVF 6개)
운영 기간	8년 (2017~2025)

출처: 홍콩 경찰 상업범죄수사국[3]

이 수치들은 단순한 양적 성과를 넘어 예방 효과를 보여준다. 52,000개의 계좌가 범죄에 사용되기 전에 차단되었다는 것은 그만큼의 잠재적 피해를 사전에 방지했다는 의미이다. 특히 655명의 검거는 FMLIT가 단순한 정보 공유 플랫폼이 아니라 실제 범죄자 처벌까지 이어지는 완결된 시스템임을 보여준다.

FMLIT의 운영은 명확한 역할 구분과 법적 절차 준수를 기반으로 한다. 2025년 8월 홍콩 경찰 발표에 따르면, FMLIT는 정보 공유 및 분석(intelligence sharing and analysis)을 전담하

며, 수사기관은 법원 영장을 통한 공식 증거 수집(formal evidence collection)을 담당한다[3]. 홍콩 경찰은 FMLIT의 역할을 "intelligence platform"으로 규정하며, FMLIT가 수사를 지원하기 위한 정보를 제공하지만, 법집행기관은 법원 영장을 포함한 적법한 법적 절차를 통해 공식 증거를 확보한다고 명시했다[3]. 이러한 구분으로 각 기관의 전문성이 극대화되고 법적 리스크가 최소화된다.

홍콩 경찰의 관할권 구조도 명확하다. 상업범죄수사국(Commercial Crime Bureau, CCB)은 상업사기, 컴퓨터 관련 범죄, 통화 위조 등 복합적 상업범죄를 수사하는 전문 부서로 사기범죄 수사를 담당한다[19]. 금융정보수사국(Financial Intelligence and Investigation Bureau, FIIB)은 2021년 6월 신설되어 자금세탁 및 테러자금조달 수사, 금융정보 분석, 국내외 법집행기관과의 정보 교환을 담당한다. FIIB는 기존 마약국 산하의 금융수사과를 독립시켜 설립되었으며, 범죄 부문 산하 독립 국으로 승격되었다. Commissioner Tang Ping-keung은 개소식에서 "금융범죄의 양, 다양성, 복잡성 증가와 국경간 특성에 대응하여 AML/CFT 기능을 보다 집중적이고 전문적으로 수행하기 위함"이라고 설립 취지를 밝혔다[20]. FMLIT는 CCB 산하에서 운영되며, 사기와 자금세탁이 결합된 복합 범죄에 특화된 정보 허브 역할을 수행한다[21].

3.4. FRONTLINE PLUS 국제 협력 플랫폼

홍콩 당국의 분석에 따르면 사기 사건의 배후 조직은 대부분 피해자와 다른 관할권에 위치한다. 또한 사기 조직들이 여러 국가에 대포통장을 개설하여 자금 세탁의 복잡성을 극대화하고 있어 단일 국가 차원의 대응으로는 한계가 명확하다.

흥미로운 점은 사기 수법이 지역별로 순차 확산되는 패턴을 보인다는 것이다. 2023년 중국에서 고객서비스 사칭 사기가 대규모 확산되었고, 2024년 홍콩으로 유입되었으며, 2025년 싱가포르, 마카오, 한국으로 확산되었다. 이러한 패턴 분석을 통해 선제적 대응이 가능하다는 점에서 국제 협력의 가치가 더욱 부각된다.

<Table 10> FMLIT cumulative performance (2017~2025)

국가/지역	가입 시기	주요 역할	특징
홍콩	2024 (주도)	플랫폼 운영, 조정 센터	사무국 역할
마카오	2024	정보 공유, 공동 작전	홍콩과 긴밀 협력
싱가포르	2024	기술 지원, 정보 공유	선진 핀테크 국가
말레이시아	2024	공동 작전, 정보 공유	범죄 조직 거점
인도네시아	2024	정보 공유	대포통장 다수 발견
한국	2024	정보 공유, 기술 협력	IT 기술 선도
태국	2024	공동 작전	범죄 조직 거점
필리핀	2024	공동 작전	콜센터 사기 다수
베트남	2024	정보 공유	신흥 범죄 거점
미얀마	2024	정보 공유	범죄 조직 은신처
캄보디아	2024	정보 공유	인신매매 연계

출처: 홍콩 경찰 상업범죄수사국[3]

<Table 11> FRONTLINE PLUS First joint operation performance (2025.4~5)

지표	성과
참여 국가	7개국 동시 작전
작전 기간	2025년 4월~5월 (2개월)
검거 인원	1,858명
차단 금액	약 1.6억 USD (약 2,100억 원)
압수 대포통장	3,200개
적발 범죄 조직	47개
언론 보도	전 세계 주요 언론 1,200건 이상

출처: 홍콩 경찰 상업범죄수사국[3]

이 첫 번째 공동 작전은 FRONTLINE PLUS의 실효성을 입증하는 결정적 사건이었다. 1,858명이라는 대규모 검거는 단일 국가로는 불가능했을 것이다. 더 중요한 것은 언론 보도를 통한 범죄 억제 효과이다. 범죄 조직들은 이제 국경을 넘어도 안전하지 않다는 것을 깨달았다.

기존의 외교 채널을 통한 수사공조는 수개월이 소요되지만, FRONTLINE PLUS는 이메일 기반 직접 소통으로 수 시간 내 협력이 가능하다. 이는 혁명적 변화이다. 전통적으로 국제 수사공조는 외교부 → 법무부 → 경찰청의 복잡한 경로를 거쳐야 했다. 그러나 FRONTLINE PLUS에서는 홍콩 경찰 수사관이 싱가포르 경찰 수사관에게 직접 이메일을 보낼 수 있다.

현재 추가 관할권의 참여를 적극 검토 중이며, 아프리카 및 유럽 국가들도 관심을 표명하고 있어 글로벌 네트워크로 발전할 가능성이 높다.

3.5. 교육 및 예방 활동의 체계화

<Table 12> 3T Key programs by strategy

전략	내용	주요 프로그램	성과
Topical (시의적합성)	실시간 신종 수법 대응	- 24시간 내 경보 발령 -핫라인정보즉시분석 -소셜미디어긴급공지	연간 120건 경보
Tailored (맞춤형)	집단별 특화 교육	-고령자: 전통 매체 -직장인:지하철·오피스 -학생:디지털플랫폼	집단별 인식도 70% 이상
Targeted (표적화)	고위험 집단 집중	-중국 유학생 종합 프로그램 -비자의무교육 -학부모대상교육	유학생 피해 40% 감소

출처: 홍콩 경찰 상업범죄수사국[3]

Topical(시의적합성)은 상담 핫라인을 통해 수집된 실시간 정보를 바탕으로 신종 사기 수법을 즉시 파악하고 24시간 내 대국민 경보를 발령하는 시스템이다.

Tailored(맞춤형)은 각 집단별 특성을 세밀하게 분석한 차별화 전략이다. 고령자에게는 전통 매체 및 지역사회 중심 교육을, 직장인에게는 지하철, 오피스 빌딩 등 생활 공간 활용을, 학생에게는 디지털 플랫폼 및 대학과의 제도적 협력을 실시한다.

Targeted(표적화)는 특히 중국 본토 유학생에 대한 집중 프로그램으로 매우 체계적이다.

<Table 13> Comprehensive program for Chinese international students

단계	시기	프로그램	강제성	담당 기관
입국 전	비자 신청 시	의무 교육 영상 시청 (15분)	필수 (미이수 시 비자 불발급)	홍콩 입국관리국 + 중국 공안
입국 전	출국 2주 전	학부모 대상 설명회	권장	ADCC + 대학
입국 직후	입학 1주 내	온라인 교육 이수	필수 (미이수 시 학생증 불발급)	대학 + ADCC
입국 직후	계좌 개설 시	은행 지점 현장 교육	필수	은행 + ADCC
재학 중	매 학기	캠퍼스 현장 교육	권장	ADCC + 대학
재학 중	수시	SMS/앱 푸시 경고	자동	통신사 + ADCC
효과 측정	2025.9~2026.3	전후 비교 연구	-	ADCC + 대학 연구팀

출처: 홍콩 경찰 상업범죄수사국[3]

입국 전 단계에서는 비자 신청 시 의무 교육 영상 시청이 필수이며(비시청 시 비자 발급 불가), 학부모 대상 별도 안내서 발송 및 화상 설명회를 개최하고, 중국 공안과의 직접 협력으로 출국 전 교육을 실시한다.

입국 후 단계에서는 대학 입학 후 온라인 교육을 의무 이수해야 하며(미이수 시 학생증 발급 불가, 도서관 이용 제한), 은행 계좌 개설, 통신 개통 시 사기 예방 자료를 제공하고, 학기별 캠퍼스 내 현장 교육을 실시한다.

2025년 9월~2026년 3월까지 전후 비교 연구를 통해 교육 효과를 과학적으로 검증할 예정이다. 이러한 증거 기반 정책 접근법은 매우 선진적이다.

일상 침투 전략으로 영화관에서는 상영 전 사기 예방 영상을 의무 방영하고, 대중교통에서는 지하철역 및 터널 내 음성 안내 및 포스터를 설치하며, 생활용품에는 커피숍 컵홀더, 마트 영수증에 예방 문구를 삽입하고, 모바일에서는 통신사와 협력한 전 시민 대상 SMS를 발송한다.

소셜미디어 활용으로 TikTok 등 젊은 층이 주로 사용하는 플랫폼에 특화된 콘텐츠를 제작하여 세대별 맞춤 접근을 실현하고 있다.

3.6. 법적·제도적 혁신 사례

3.6.1. Letter of No Consent (LNC) 제도

홍콩의 LNC 제도는 법원 명령이 아닌 행정적 조치이면서도 실질적 효력을 갖는다. 이는 홍콩의 높은 법치 수준과 금융기관의 자발적 협력 문화가 결합된 결과물이다. LNC는 OSCO (Organized and Serious Crimes Ordinance) 제25A조에 근거하여 홍콩 경찰의 Joint Financial Intelligence Unit(JFIU) 책임자가 발급하는 행정적 조치로, 법원 명령이 아님에도 실질적으로 계좌 동결 효과를 발생시킨다. 은행이 의심거래보고(STR)를 제출한 후 JFIU가 "동의하지 않음(no consent)"을 통지하면, 은행들은 OSCO 제25조의 자금세탁 범죄 책임을 회피하기 위해 자발적으로 해당 계좌를 동결한다. 2021년 제1심 법원은 이 제도가 위헌이라 판결했으나, 2023년 항소법원과 2024년 최종심 법원이 이를 뒤집고 LNC 제도의 합헌성을 확인했다. 최종심은 경찰의 LNC 발급 권한이 Police Force Ordinance 제10조(범죄 예방 및 재산 보호 의무)에서 유래하며, 계좌 동결은 경찰의 강제가 아닌 은행의 자발적 선택이라고 판시했다[22-25].

발급 권한은 JFIU 책임자(경찰 고위직)에게 있으며, 발급 조건은 의심 계좌 내 상당한 자금 존재 및 추가 유출 우려이다. 은행은 자발적으로 거래를 중단하며, 법적 강제성이 없음에도 높은 준수율을 보인다. 전략적 활용으로는 법원의 정식 압류·몰수 명령 취득 시간을 확보하고, 피해자의 민사 구제 절차 준비 기간을 제공하며, 추가 피해 확산을 방지한다. LNC의 유효기간은 통상 31일이다.

3.6.2. Notification Letter 제도

홍콩 경찰은 공식 수사 착수 전 금융기관에 특정 계좌에 대한 의심 정보를 사전 통지하는 Notification Letter 제도를 운영하고 있다. Notification Letter는 홍콩 경찰이 공식 수사 착수 전에 금융기관에 특정 계좌에 대한 의심 정보를 사전 통지하는 제도로 브리핑에서 소개되었다. 이는 LNC와 구별되는 개념으로, LNC가 STR 제출 후 JFIU가 발급하여 즉각적 동결 효과를 발생시키는 것과 달리, Notification Letter는 수사 초기 단계에서 은행의 자발적 예방 조치를 유도하는 것을 목적으로 한다[3]. 이를 통해 은행은 해당 고객과의 거래 관계를 재검토하고, 계좌 모니터링을 강화하며, 필요시 거래 관계 종료 및 STR 제출을 결정할 수 있다.

이 제도는 다층적 보호 효과를 발생시킨다. 1차 단계로 은행은 통지를 받은 후 해당 고객과의 거래 관계를 재검토한다. 2차 단계로 계좌 모니터링을 강화하여 의심스러운 거래 패턴을 감시한다. 3차 단계로 필요시 거래 관계를 종료하고 JFIU에 STR을 제출한다. 이러한 단계적 접근은 은행의 자발적 협력을 유도하면서도 고객의 재산권을 과도하게 침해하지 않는 균형점을 찾고자 하는 것으로 평가된다.

3.6.3. 피해 회복 체계

홍콩은 경찰 차원의 피해 회복 제도가 없어 피해자가 개별적으로 변호사를 고용하여 민사 소송을 제기해야 한다. 홍콩 경찰은 브리핑에서 “홍콩에는 전기통신금융사기 피해금 환급에 관한 특별법과 같은 공적 피해 회복 제도가 없으며, 피해자가 민사 소송을 통해 개별적으로 자금 회복을 시도해야 한다”고 설명했다[3,26]. 이는 피해자에게 추가적 부담을 주는 제도적 한계이다.

반면 한국의 범죄피해자보호기금 등 공적 구제 제도가 상대적으로 우수하다. 한국은 전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법(약칭: 전기통신금융사기법)에 따라 공적 피해 회복 제도를 운영하고 있다. 동법 제6조(피해환급금의 지급 등)에 따라 금융회사등은 지급정지된 계좌의 채권소멸절차를 거쳐 피해자에게 피해환급금을 지급하며, 제7조(환급금 미지급금 등의 귀속)에 따라 채권소멸절차 완료 후 피해자에게 지급되지 않은 금액은 금융위원회가 관리하는 피해환급금으로 귀속된다. 또한 범죄피해자 보호법 제16조에 따라 범죄피해자보호기금에서 구조금을 지급하는 제도도 운영 중이다[27,28].

IV. 대만의 첨단 범죄 대응 체계

4.1. 하이테크 수사센터 개요

대만의 하이테크 수사센터(High Tech Investigation Center, 科技偵查中心)는 법무부 대만 고등검찰청(Taiwan High Prosecutors Office)에 설치되어 있으며, 2020년 5월 20일 공식 전환되어 현재의 형태로 운영되고 있다[29,30]. 2025년 4월 29일부터 5월 3일까지 대만 법무부 수사국 주관으로 타이페이에서 개최된 ‘2025년 초국경 사기범죄 대응 워크숍’에서 하이테크 수

사센터의 주요 활동이 소개되었다. 이 워크숍은 아시아·태평양 지역 12개국 수사기관 담당자들이 참석하여 국경간 사기범죄 대응 실무 전략, 자금세탁방지 및 사이버보안 실무, 최근 초국경 사기 추세 등을 논의하는 장이었다[4].

센터는 3개 조직으로 구성되어 있다. 科技偵查組(기술수사팀)는 디지털 포렌식, 무전기 감지, 암호화폐 분석 등 첨단 기술 수사를 담당한다. 科技監控組(전자감독팀)는 전자 발찌 등 기술 장치를 이용한 범죄자 감독을 담당한다. 大數據組(빅데이터팀)는 AIT 플랫폼 등 데이터 검색 및 분석을 위한 온라인 플랫폼 통합을 담당한다.

4.2. 디지털 포렌식 역량

<Table 14> Main tools and applications of Taiwan's High-Tech Investigation Center

분야	도구명	용도	제조사/국가
컴퓨터 포렌식	EnCase Forensic	하드디스크 증거 추출·분석	Guidance Software/미국
	Axiom	종합 디지털 증거 분석	Magnet Forensics/캐나다
휴대폰 포렌식	Cellebrite	iOS/Android 데이터 추출	Cellebrite/이스라엘
	XRY	휴대폰 데이터 복구·분석	MSAB/스웨덴
	Break Key	잠금 해제 및 데이터 추출	자체 개발/대만
암호화폐 추적	CRM for Renting	거래 흐름 시각화	상용 도구
	자체 분석 도구	교차 등록 분석	자체 개발/대만
증거 보호	신호 차단 가방	원격 데이터 삭제 방지	다수 제조사
	신호 차단 장치	현장 전파 차단	다수 제조사
빅데이터	AIT 플랫폼	통합 데이터 검색·분석	자체 개발 / 대만 MJIB

출처: 대만 고등검찰청[30]

대만은 전문 도구를 활용한 컴퓨터 포렌식과 휴대폰 포렌식을 수행한다. 증거 보호 시스템으로 디지털 검토 및 재제작 보호 시스템을 갖추어 증거 무결성을 확보하고, 신호 차단 가방 및 장치를 사용하여 원격 데이터 삭제 시도를 방지한다.

특히 손상된 휴대폰 복구에서는 내부 데이터를 변경하지 않고 하드웨어를 교체하는 방식으로 직접 수리한다. 배포용 검찰청 수사관을 대상으로 휴대폰 수리 교육을 실시하여 기본적인 수리 기술을 갖추도록 하는 것은 매우 실용적인 접근이다.

암호화폐 수사 체계에서는 자금세탁 및 테러 자금 조달에 암호화폐가 활용됨에 따라, 거래 흐름을 시각화하고 수사관이 쉽게 이해할 수 있도록 돕는 도구를 활용한다. 이는 홍콩 ADCC와 유사한 접근으로, 복잡한 암호화폐 거래를 수사관이 직관적으로 이해할 수 있게 한다.

4.3. 빅데이터 통합 플랫폼 (AIT)

수사 과정에서 방대한 데이터(차량 기록, 출입국 기록, GIS)를 통합하고 분석하는 것이 중요하다. 기존의 다양한 정부 시스템은 통합되어 있지 않아 효율적인 분석에 어려움이 있었다. 이를 개선하기 위해 대만 고등검찰청은 데이터 검색 및 분석 기능을 통합한 수사 지원 플랫폼을 개발했다. 2025년 5월 2일 하이테크 수사센터 브리핑에서 이 플랫폼은 'AIT(Assistant Investigation Tech)'로 소개되었으며, 검사와 수사관이 KYC 기록, 거래 기록, 차량 기록, 출입국 기록, GIS 데이터 등을 통합 검색하고 분석할 수 있도록 지원한다. AIT 플랫폼에 대한 정보는 워크숍 참석자를 대상으로 한 비공개 브리핑에서 제공되었으며, 보안상의 이유로 공개 웹

사이트나 공식 문서에는 상세 정보가 게재되지 않았다. 본 연구에서 제시하는 AIT 플랫폼의 기능과 구조는 2025년 5월 2일 대만 고등검찰청 하이테크 수사센터를 직접 방문하여 담당 검사로부터 시연받은 내용을 기반으로 한다[30].

<Table 15> AIT(Assistant Investigation Tech) Platform key features

기능 구분	세부 기능	설명	접근 권한
데이터 검색	KYC 기록 통합 검색	금융기관 고객 확인 정보 통합	검사, 수사관
	거래 기록 검색	은행·증권·암호화폐 거래	검사, 수사관
	협력 기관 데이터	차량, 출입국, GIS 등	검사, 수사관
	관계도 시각화	인물·기업 간 연결 관계 자동 매핑	검사, 수사관
데이터 분석	신속 분석	원클릭 자동 분석 보고서 생성	모든 사용자
	소셜 네트워크 분석	범죄 조직 구조 파악	검사, 수사관
	지리 정보 분석	범죄 발생 위치 패턴 분석	검사, 수사관
	암호화폐 지갑 추적	지갑 주소 간 자금 흐름 시각화	검사, 수사관
프라이버시	무흔적 분석	기밀 사건 분석 시 로그 미기록	검사만
	자동 삭제	분석 완료 후 30일 자동 삭제	시스템 자동

출처: 대만 고등검찰청[30]

데이터 검색 기능은 KYC 기록, 거래 기록, 협력 기관 데이터 등을 통합 검색하고, 관련 인물 및 경제 요인 간의 관계를 시각화한다. 데이터 분석 기능은 신속 분석, 소셜 네트워크 분석, 지리 정보 분석 기능을 제공하여 사용자 학습 없이도 지능형 제품 생성이 가능하도록 지원한다. 프라이버시 보호 기능으로 일부 기밀 사건의 경우, 검사가 데이터를 공유하더라도 분석 결과에 흔적이 남지 않도록 자동화되어 있다. 이는 개인정보보호와 수사 효율성의 균형을 잘 보여준다. 대만 고등검찰청 담당자의 설명에 따르면 “사용자 인터페이스를 통해 암호화폐 지갑을 확인할 수 있으며, ID나 개인 데이터를 입력하여 KYC 데이터를 추적할 수 있습니다. 이제 더 이상 많은 종이 작업이나 번거로운 절차가 필요 없습니다”라고 했다[30].

4.4. 전자 감독 센터(EMCC)

2020년에 설립된 전자 감독 센터는 성범죄자의 전자 감독을 통해 재범 위험을 줄이고 인권을 보장하는 것을 목표로 한다. 전자 발찌, 클랩(Clap), 휴대폰을 위치 추적 기술과 결합하여 24시간 감시를 수행한다. 범죄자의 사적인 일정 계획이나 은닉을 방지하기 위해 다음과 같은 조치를 취한다. 언제든지 카메라를 활성화하여 소통하도록 요구하고, 특정 장소 출입 금지로 피해자를 보호하며, 범죄자의 이동 지역을 제한한다. 전자 감독은 관련 법률 개정에 기여했으며, 투옥의 대안으로 활용될 수 있다. 이는 교정 정책의 다양화에 기여하고 있다.

4.5. 대만 FIU의 정보 공유 체계

대만 FIU는 수사국(Investigation Bureau, MJIB) 산하에 설치되어 있으며, 29명의 법집행 요원으로 구성되어 있다. 이는 홍콩의 FMLIT나 한국의 금융정보분석원과 달리 모든 FIU 직원이 수사 경험을 보유한 특수요원이라는 점에서 독특하다.

<Table 16> Organizational Structure of the Taiwan FIU

구분	인원/구성	주요 역할	특징
총 인력	29명	전원 법집행 요원 출신	수사국(MJIB) 소속
STR 분석 섹션	12명	연간 20,000건 STR 분석	각 STR을 "사건의 실마리"로 취급
전략기획 섹션	약 10명	Egmont 요청 처리, 국제협력, 보고기관 정책지원	국제 회의 적극 참여
불법자금추적 섹션	약 7명	연간 360만 건 CTR 모니터링	"주식시장 보드" 방식 인터페이스
리더십	1명 국장, 1명 부국장	전략 수립 및 조정	-

출처: 대만 고등검찰청[30]

대만 FIU의 가장 독특한 특징은 보고기관(금융기관)과의 관계를 "감독자-피감독자"가 아닌 "파트너"로 설정한 점이다. FIU는 금융감독 권한이 없으므로, 금융기관과 "친구처럼" 소통한다. 대만 FIU 담당자는 인터뷰에서 다음과 같이 설명했다. "우리는 그들에게 명령할 권한이 없습니다. 그래서 우리가 보고기관과 소통하는 방식은 친구처럼 대하는 것입니다. 그들이 공유한 정보가 매우 효율적으로 사용될 것임을 알기 때문에, 그들은 우리와 일하는 것을 매우 기뻐합니다"[31].

대만 FIU는 연간 360만 건이라는 방대한 현금거래보고를 처리하기 위해 고도로 자동화된 시스템을 구축했다. 이 시스템의 핵심은 "주식시장 보드" 방식의 인터페이스이다. 담당자의 설명에 따르면 "우리가 CTR 화면을 볼 때, 그것은 주식시장을 보는 것과 같습니다. 각 항목을 클릭하면 데이터베이스가 이전 거래 내역을 보여줍니다. 예를 들어, 오늘 100만 원을 현금으로 입금했다면, ID를 클릭하면 이 100만 원이 이틀 전에 다른 계좌에서 인출한 금액과 동일한지 자동으로 확인됩니다"[29].

시스템은 계좌 소유자 직업별 분류(공무원, 상장회사 임원 등), 거래 패턴 분석(같은 금액의 입출금 추적), 관계도 시각화(계좌 간 자금 흐름 자동 매핑), 위험 신호 자동 감지(심야 ATM 거래, 이상 패턴 등)를 제공한다.

대만 FIU는 Egmont Group의 원칙에 따라 FIU가 제공하는 것은 "정보(intelligence)"이지 "증거(evidence)"가 아님을 명확히 한다. Egmont Group의 용어 정의에 따르면, "For (financial) intelligence purposes"는 분석이나 단서를 위한 금융정보 또는 정보의 사용을 의미하지만, 증거로서 또는 증거를 뒷받침하기 위한 것이 아니다. 반면 "For administrative/prosecutorial/judicial purposes"는 법적(행정적/검찰/사법) 절차에서 증거로서, 또는 증거를 뒷받침하기 위한 금융정보 또는 정보의 사용을 의미한다. 이러한 구분은 FIU가 수사기관에 정보를 제공할 때, 수사기관은 반드시 법원 영장 등 적법한 절차를 통해 별도로 증거를 수집해야 함을 의미한다[31,32].

<Table 17> Comparison of national CTR reporting requirements

국가	CTR 기준	전신송금 보고	보고 주체	연간 보고 건수
대만	1회 거래 500,000TWD(약 2,100만 원)	없음	금융기관	약 360만 건
한국	1일 누적 1,000만 원 (현금)	1일 누적 1,000만 원	금융기관	약 400만 건 (추정)
홍콩	없음(STR 중심 체계)	없음	-	-
미국	10,000 USD(약 1,300만 원)	3,000 USD	금융기관	약 2,000만 건
싱가포르	20,000 SGD(약 2,000만 원)	없음	금융기관	약 50만 건
FATF 권고	15,000 USD(약 2,000만 원)	국가별 재량	-	-

출처: 각국 FIU 및 FATF[31,33-36]

대만은 전신송금에 대해서는 별도 보고를 요구하지 않는다. “현금은 익명이지만, 전신송금은 기록이 남기 때문”이라는 것이 그 이유이다.

<Table 18> 대만 FIU의 정보(Intelligence) vs 증거(Evidence) 구분

구분	정보 (Intelligence)	증거 (Evidence)
제공 주체	FIU	금융기관 (영장 필요)
법적 근거	FIU 직권	법원 영장
내용	FIU 분석 결과 + 뒷받침 정보	원본 거래 기록
사용 목적	수사 착수 근거	기소 및 재판 증거
수집 절차	FIU가 금융기관에 직접 요청	수사기관이 영장으로 요청

출처: 대만 FIU[31]

담당자의 설명에 따르면 “우리는 STR을 분석한 후, 이것이 범죄 활동과 관련이 있다고 판단되면 하나의 보고서를 작성합니다. 이 보고서에는 우리의 분석 결과와 뒷받침하는 정보들이 포함됩니다. 하지만 이것은 정보이지 증거가 아닙니다. 수사기관이 이 정보를 증거로 사용하려면, 법원 영장을 받아 은행에 다시 요청해야 합니다”[29].

대만 FIU는 Egmont Group 회원으로서 Egmont Secure Web을 통해 전 세계 FIU와 정보를 교환한다. 특히 대만은 APG(Asia/Pacific Group on Money Laundering) 회원국으로서 2030년 상호평가를 준비 중이다. 담당자는 “상호평가는 매우 스트레스가 많은 과정입니다. 규제를 잘 이행하고 있다는 것뿐만 아니라, 그 결과(outcomes)도 증명해야 합니다”라고 설명했다[29].

홍콩과 대만의 차이에 대해 질문하자, 담당자는 다음과 같이 설명했다. “홍콩의 JFIU도 우리처럼 수사기관 내부에 있지만, 두 가지 차이가 있습니다. 첫째, 우리는 FIU 직원 전원이 수사 경험을 보유한 특수요원인 반면, 홍콩은 금융 전문가도 포함되어 있습니다. 홍콩의 JFIU(Joint Financial Intelligence Unit)는 홍콩 경찰 내부에 설치된 금융정보기관으로, Narcotics Bureau 산하에서 운영되다가 2021년 6월 신설된 Financial Intelligence and Investigation Bureau(FIIB)로 이관되었습니다[37]. 둘째, 홍콩은 FMLIT라는 민관 협력 플랫폼이 매우 발달했지만, 우리는 금융기관과 직접 파트너십을 구축하는 방식입니다. 하지만 공통점은 FIU가 수사기관과 분리되지 않고 내부에 있다는 것이고, 이것이 신속한 협력의 핵심입니다”[29].

한국의 경우에 대해 질문하자, 담당자는 다음과 같이 조언했다. “한국에도 FIU에 경찰이 파견되어 있다고 들었습니다. 하지만 워크숍 참가자들에게 들은 바로는 여전히 STR이 실제 수사

부서에 배당되기까지 5개월 이상 걸리고, 배당된 후에도 긴급 범죄에 밀려 적시 수사가 어렵다고 하더군요. 홍콩과 우리의 가장 큰 장점은 FIU가 별도 조직이 아니라 수사기관 내부에 있다는 것입니다. 한국도 장기적으로는 조직 구조 개편을 고려해볼 만합니다"[29].

필자가 2022년부터 2024년까지 경기북부지방경찰청 범죄수익추적팀에서 금융정보분석원(KoFIU)으로부터 배당되는 의심거래보고(STR) 사건을 전담 처리한 경험에 따르면, 연간 약 90건의 STR 사건이 배당되었으나 대부분의 STR은 거래 발생 시점으로부터 3~5개월 이상 경과한 후 경찰에 전달되었다. 이는 금융기관의 STR 제출 → KoFIU 분석 → 수사기관 배당의 다단계 과정에서 발생하는 구조적 지연으로, 범죄 자금이 이미 인출되거나 이동한 이후에 수사가 시작되는 경우가 대부분이었다. 한국 금융정보분석원은 금융위원회 산하 독립기관으로, 특정금융거래정보의 보고 및 이용 등에 관한 법률 제7조에 따라 설치되었으며, 동법 제10조에 따라 수사기관에 정보를 제공하도록 되어 있으나, 구체적인 전달 기한이나 절차에 대한 법적 규정은 명확하지 않다.

이러한 지적은 한국의 FIU-경찰 협력 체계 개선이 시급함을 보여준다. 대만 FIU 담당자는 "우리는 같은 건물에 있고, 같은 조직입니다. FIU 직원이 경제범죄과 이전 동료에게 전화를 걸어 '이봐, 내가 금융 정보를 보냈어. 이것 좀 봐봐'라고 말할 수 있습니다. 진행 상황을 확인할 수도 있습니다"라고 설명했다[29]. 반면 한국은 FIU가 금융위원회 산하에, 경찰이 행정안전부 산하에 위치하여 조직적으로 분리되어 있고, 물리적으로도 다른 건물에 위치하여 대만과 같은 긴밀한 협력이 구조적으로 어렵다.

V. 홍콩·대만 사례의 비교 분석 및 평가

5.1. 홍콩-대만-한국 비교 분석

<Table 19> Comparison of Fraud Crime Response Systems in Hong Kong, Taiwan, and South Korea

구분	홍콩	대만	한국
조직 형태	경찰청 독립 센터 (ADCC/FMLIT)	수사국 산하 (MJIB 하이테크센터/FIU)	금융위 산하 독립기관 (금정원) + 경찰청
인력	ADCC 90명, FMLIT 회원제	하이테크센터 미공개, FIU 29명	금정원 약 200명, 경찰 분산
FIU 위치	경찰 내부 (JFIU)	수사국 내부 (MJIB FIU)	금융위원회 산하 (경찰 파견)
FIU-수사기관 관계	동일조직	동일조직	별도 조직(파견)
핵심 전략	실시간 대응 + 민관 협력	기술 중심 + 파트너십	분석 중심 + 정보 제공
강점	-24시간 핫라인(80,000건/년) -2시간내자금차단(96%) -상류개입(15,000명보호)	-고도 자동화(360만 CTR) -수사연계긴밀 -파트너십기반협력	-전문 분석 인력 -피해자보호기금 -FATF회원국
약점	-피해 회복 제도 미비	-국제 협력 제약(비UN 회원)	-FIU-경찰 협력 지연 (5개월 추산정보) -실시간대응미흡

출처: 저자 작성[3,4,30,31,38-40]

조직 구조: 홍콩과 대만은 FIU가 수사기관 내부(경찰/수사국)에 위치하여 신속한 협력이 가능한 반면, 한국은 FIU가 금융위원회 산하 독립기관으로 조직적·물리적 분리로 인한 협력 지연

이 발생한다.

대응 전략: 홍콩은 실시간 대응(2시간 내 96% 차단), 대만은 기술 중심(AIT 플랫폼), 한국은 분석 중심이지만 실시간 대응이 미흡한 상황이다.

핵심 차이: 한국의 STR 정보가 경찰에 전달되기까지 평균 5개월 소요되는 것이 가장 큰 약점이며, 홍콩/대만은 '같은 조직, 같은 건물'에서 즉시 협력이 가능하다.

5.2. 한국 적용을 위한 핵심 시사점

<Table 20> Implications for application in Korea and priorities

우선순위	시사점	홍콩 모델	대만 모델	예상 효과	추진 난이도
최우선	FIU-경찰 협력 강화	ADCC 통합 모델	MJIB 내부 모델	보고 지연 5개월 → 1개월	중
최우선	실시간 자금 차단	2시간 내 96%	파트너십 기반	차단 성공률 50% → 70%	중상
고우선	통합 대응 센터	ADCC 90명	-	조정 기능 공백 해소	상
고우선	빅데이터 플랫폼	FMLIT MIDAS	AIT 플랫폼	분석 효율 3배 향상	중
중우선	상류 개입 시스템	15,000명 보호	-	선제적 피해 방지	중
중우선	민관 협력 법제화	은행동맹 ADA	파트너십 모델	정보 공유 3배 증가	상
저우선	국제 협력 확대	FRONTLINE PLUS	Egmont 적극 활용	국제 검거율 향상	하
저우선	3T 교육 전략	대학생 프로그램	-	특정 집단 피해 40% 감소	하

출처: 저자 작성

최우선 과제: FIU-경찰 협력 강화(5개월 → 1개월)와 실시간 자금 차단(성공률 50% → 70%)은 즉시 실행 가능하며 비용 대비 효과가 가장 크다.

고우선 과제: 통합 대응 센터와 빅데이터 플랫폼은 조직 재편과 기술 투자가 필요하나, 분석 효율을 3배 향상시킬 수 있다.

예상 효과: 전체 시스템이 정착되면 3년 내 연간 차단 금액 500억 → 2,000억 원(4배 증가), 피해액 60% 감소(8,000억 → 3,200억 원)가 가능하다.

Ⅵ. 한국 적용을 위한 시사점

6.1. 핵심 정책 제언

홍콩과 대만은 모두 FIU가 수사기관 내부에 위치한다는 공통점이 있다. 홍콩의 JFIU는 경찰 산하에, 대만의 FIU는 법무부 수사국(MJIB) 산하에 설치되어 수사관들과 같은 조직, 같은 건물에서 근무한다. 대만 FIU 담당자의 표현처럼 "FIU 직원이 경제범죄과 이전 동료에게 전화를 걸어 '이봐, 내가 금융 정보를 보냈어. 이것 좀 봐봐'라고 말할 수 있는" 수준의 긴밀한 협력이 가능하다.

반면 한국은 금융정보분석원(FIU)이 금융위원회 산하 독립기관으로 설치되어 있어 경찰청과 조직적·물리적으로 분리되어 있다. 비록 FIU에 경찰 파견팀이 상주하고 있으나, 이는 홍콩이나 대만처럼 "같은 조직 내부"에서 협력하는 것과는 근본적으로 다르다.

실제로 STR이 FIU에서 분석·심사를 거쳐 경찰 수사부서에 배당되기까지 평균 5개월이 소요되며, 배당된 후에도 긴급 강력사건에 밀려 적시 수사가 이루어지지 않는 경우가 빈번하다. 이는 ① FIU와 경찰의 조직적 분리, ② 다단계 분석-심사-배당 절차, ③ 파견팀의 제한적 권한 등이 복합적으로 작용한 결과이다.

개선 방안으로는 단기적으로 파견 경찰의 권한을 확대하여 STR 긴급도 평가 및 신속 배당 권한을 부여하고, 중요 STR(대규모 사기, 조직범죄 연루)에 대해서는 48시간 내 경찰 수사부서 배당을 의무화해야 한다. FIU 분석관과 파견 경찰 간 일일 브리핑 제도를 도입하여 실시간 정보 공유 문화를 구축해야 한다. 장기적으로는 홍콩·대만 모델을 참고하여 FIU를 경찰청 산하로 재편하거나, 국무총리실 산하 통합대응센터에 FIU·경찰·금융감독원이 함께 입주하는 방안을 검토해야 한다.

홍콩은 2시간 내 96% 응답률을 달성하는 실시간 자금 차단 시스템을 운영하고 있으며, 누적 2.4조 원을 차단한 성과를 거두었다. 한국도 전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법에 따라 금융기관의 지급정지 제도를 운영하고 있으나, 개별 은행의 자율에 맡겨져 있어 홍콩처럼 체계적 조정이 이루어지지 않고 있다.

개선 방안으로는 금융기관의 응답 시간을 2시간 이내로 의무화하고, 28개 주요 금융기관의 참여를 법제화하며, 응답률 96%를 목표로 설정해야 한다. 24시간 대응 체계를 구축하고, 중국·일본·싱가포르와 국제 협력을 체결하여 국경을 넘는 자금 이동에도 대응해야 한다.

한국은 금융감독원 산하 전기통신금융사기 피해환급센터(국번 없이1332)와 더불어, 2025년10월15일 경찰청이 기존 보이스피싱 대응센터를 확대 개편하여 '전기통신금융사기 통합대응단'을 공식 출범시켰다. 통합대응단은 경찰청·금융위원회·과학기술정보통신부·방송미디어통신위원회·한국인터넷진흥원·금융감독원·금융보안원 등 총137명의 전문인력이 24시간 연중무휴로 근무하는 범정부 민관 협력 체계이다[41].

통합대응단의 성과: 출범2개월간(2025년10월-11월) 보이스피싱 발생 건수가 전년 대비 각각32.8%, 26.7% 감소하고, 피해액도 22.9%, 35% 줄어드는 등 가시적 성과를 거두었다. 일평균 상담·제보 응대율은 기존62.9%에서 96.4%로 증가했고, 전화번호 차단은 243건에서 1,124건으로 363% 증가했으며, 악성 앱 차단도64건에서 276건으로 331% 증가했다[42]. 이는 홍콩 ADCC의 민관 협력 모델과 유사한 방향으로 진화하고 있음을 보여준다.

여전한 구조적 한계: 그러나 통합대응단이 출범했음에도 여전히 다음과 같은 한계가 존재한다.

첫째, 선제적 피해 예방(상류 개입) 기능이 제한적이다. 홍콩ADCC는 연간 15,000명의 잠재적 피해자에게 선제적으로 연락하여 630억 원 상당의 피해를 예방하는 반면, 한국 통합대응단은 신고 후 대응 중심이다. 홍콩처럼 금융거래 이상 패턴 탐지→ 즉시 고객 연락→ 거래 중단이라는 상류 개입 프로세스가 부족하다.

둘째, 실시간 자금 차단의 체계적 조정이 미흡하다. 홍콩은 2시간 내 96% 응답률로 신속하게 계좌를 동결하는 반면, 한국은 여전히 개별 은행의 자율 판단에 의존하며 표준화된 절차가 부족하다. 통합대응단이 범죄 이용 전화번호를 10분 내 차단하는 것은 성과이나, 금융계좌 차단은 여전히 금융감독원 1332센터를 경유해야 하는 이원화 구조가 남아있다.

셋째, 24시간 신종 수법 경보 시스템이 부재하다. 홍콩FMLIT는 신종 사기 수법 발견 시 24시간 내 전체 은행에 경보를 발령하는 반면, 한국은 이러한 실시간 경보 체계가 구축되지 않았다. 통합대응단이 최신 수법을 반영한 대국민 예경보 문자를 발송하고 있으나, 금융기관 간 실시간 정보 공유 시스템은 미비하다.

넷째, 주요 금융기관 담당자의 상주 부재로 즉각적 조치가 어렵다. 홍콩ADCC는 10개 주요 은행 직원이 센터에 상주하며 즉각 대응하는 반면, 한국 통합대응단은 금융기관과 직통 회선을 구축했으나 실제 은행 직원이 상주하지 않아 원격 협조에 의존한다.

다섯째, 금융감독원1332 센터와의 역할 분담이 불명확하다. 비록 통합대응단이 출범했으나, 계좌 지급정지는 금감원1332센터의 고유 업무로 남아있어 이중 신고 또는 정보 연계 지연이 발생할 수 있다. 홍콩처럼 단일 센터(ADCC)에서 상담-정보공유-계좌차단-수사까지 원스톱 처리하는 통합성이 부족하다.

결론: 통합대응단의 출범은 한국 사기범죄 대응의 중대한 진전이며, 홍콩ADCC 모델과 유사한 방향으로 진화하고 있다는 점에서 긍정적이다. 그러나 홍콩ADCC 수준의 ① 선제적 상류 개입, ② 2시간 내 계좌동결 체계, ③ 은행 담당자 상주, ④ 실시간 경보 시스템, ⑤ 단일 센터 원스톱 처리를 추가로 도입할 필요가 있다.

대만의 AIT 플랫폼은 금융거래, 통신기록, 차량정보, 출입국기록, GIS 데이터를 통합 검색·분석할 수 있는 시스템으로, 수사관이 몇 번의 클릭만으로 모든 정보를 조회할 수 있다. 한국도 유사한 통합 플랫폼을 구축해야 한다.

개선 방안으로는 1단계에서 금융거래와 통신기록 통합에 집중하고, 2-3단계에서 차량정보, 출입국기록 등으로 점진적으로 확대해야 한다. 관계도 자동 시각화 기능을 구현하고, 수사관 전용 무흔적 분석 기능을 제공하며, 개인정보보호 기술(암호화, 접근권한 관리, 로그 감사)을 처음부터 설계에 반영해야 한다(Privacy by Design).

홍콩은 신고된 대포통장으로 입금한 모든 계좌를 분석하여 잠재적 피해자를 선제적으로 찾아내는 상류 개입 프로그램을 운영하고 있다. 2023년 5월 이후 15,000명에게 접촉하여 630억 원의 피해를 예방했다.

한국도 이를 도입하여 신고된 대포통장 거래 내역을 자동 분석하고, 잠재적 피해자 15,000명에게 선제적으로 접촉하며, 고위험 피해자(학생, 고령자)에 대해 인터넷뱅킹 제한 등 보호 조치를 시행해야 한다.

홍콩의 은행동맹(ADA)과 대만의 파트너십 모델은 모두 금융기관의 자발적 참여를 기반으로 한다. 한국도 개인정보보호법 제58조의2를 개정하여 “사기 예방 목적의 정보 공유”를 명시적 예외 사유로 규정해야 한다.

개선 방안으로는 금융기관 간 대포통장 정보 공유를 합법화하고, 은행동맹(ADA) 제도를 도입하며, 적극 협조 은행에 대해 금융감독 평가 시 가점을 부여하는 등 인센티브 중심의 접근이 필요하다.

홍콩의 3T 전략(Topical, Tailored, Targeted)은 신종 수법을 24시간 내 경보 발령하고, 고령자·직장인·학생별 차별화 교육을 실시하며, 유학생·구직자 등 고위험 집단을 집중 관리하는 체계이다.

특히 중국 본토 유학생 대상 종합 프로그램은 비자 신청 시 의무 교육부터 입학 후 온라인 교육, 계좌 개설 시 현장 교육까지 포괄하여 큰 성과를 거두고 있다. 한국도 외국인 유학생, 청년 구직자 등 고위험 집단에 대한 맞춤형 예방 교육을 강화해야 한다.

6.2. 도입 시 예상 과제 및 해결 방안

본 연구는 홍콩 경찰의 공식 발표 자료와 대만 FIU 인터뷰를 기반으로 했으나, 다음과 같은 한계가 있다.

첫째, 홍콩과 대만의 내부 데이터 접근이 제한적이었다. ADCC의 세부 운영 매뉴얼, FMLIT의 정보 공유 표준 양식, 대만 AIT 플랫폼의 소스코드 등은 비공개 정보로 분석할 수 없었다. 향후 공식 협력 채널을 통한 심층 연구가 필요하다.

둘째, 한국의 제도적·문화적 맥락 차이를 충분히 고려하지 못했다. 홍콩의 높은 법치 수준과 금융기관의 자발적 협력 문화, 대만의 수사기관 중심 FIU 구조는 한국과 다르다. 한국의 개인정보보호 규제, 금융규제 체계, 조직 문화를 고려한 맞춤형 설계가 필요하다.

셋째, 비용편익 분석이 홍콩 사례 기반 추정에 그쳤다. 한국의 실제 도입 비용과 효과를 정밀하게 측정하기 위해서는 시범 사업을 통한 실증 연구가 필수적이다.

넷째, 암호화폐 및 메타버스 등 신흥 기술 환경에서의 사기범죄 대응은 다루지 못했다. 이는 별도의 심층 연구가 필요한 영역이다.

향후 연구 과제로는 다음이 제시된다. 첫째, 서울·경기 지역 시범 사업을 통한 실증 연구이다. 둘째, 개인정보보호와 범죄 대응의 균형점을 찾기 위한 법리적 연구이다. 셋째, AI 기반 사기 탐지 시스템의 기술적 구현 방안 연구이다. 넷째, 암호화폐·메타버스 등 신흥 기술 환경의 사기범죄 대응 연구이다. 다섯째, 국제 공조의 법적·실무적 장애 요인 제거 방안 연구이다.

개인정보보호와 범죄 대응의 균형 홍콩과 대만의 적극적 정보 공유 체계를 한국에 도입할 때 가장 큰 장애물은 개인정보보호 규제이다. 홍콩은 PDPO(Personal Data Privacy Ordinance)의 제약 하에서도 경찰을 중심으로 한 삼각 구조(A은행 → 경찰 → B은행)를 통해 이 문제를 해결했다. 한국도 개인정보보호법 개정을 통해 "사기 예방 목적의 정보 공유"를 명시적 예외 사유로 규정하되, 정보 최소화 원칙과 사후 통지 의무를 병행하여 개인정보 침해를 최소화해야 한다.

기관 간 협력 문화 구축 FIU가 금융위원회 산하에, 경찰이 행정안전부 산하에 위치한 한국의 조직 구조는 대만처럼 같은 건물에서 긴밀히 협력하는 것을 구조적으로 어렵게 만든다. 한국 금융정보분석원(FIU)에는 경찰 파견팀이 상주하고 있으나, 이는 대만의 FIU-수사기관 협력 구조와 근본적으로 다르다. 대만은 FIU 자체가 법무부 수사국(MJIB) 내부에 위치하고, FIU 직원 29명 전원이 수사 경험을 보유한 법집행 요원으로 구성되어 있다. 이들은 같은 건물, 같은 조직에서 근무하며, FIU 직원이 "이전 동료"인 경제범죄 수사관에게 전화 한 통으로 즉시 정보를 전달하고 진행 상황을 확인할 수 있다. 반면 한국은 FIU가 금융위원회 산하 독립기관으로 설치되어 조직적·물리적으로 경찰과 분리되어 있으며, 소수의 경찰 파견팀만으로는 구조적 한계를 극복하기 어렵다. 실제로 STR이 경찰 수사부서에 배당되기까지 많은 시간이 소요되며, 배당된 사건도 긴급 강력사건에 밀려 적시 수사가 이루어지지 않는 경우가 빈번하다.

이러한 구조적 한계를 극복하기 위한 단기 방안으로는 ① 파견 경찰의 권한 강화(STR 긴급도 평가 및 신속 배당 권한), ② FIU-경찰 간 전용 통신망 구축, ③ 중요 STR에 대한 48시간 내 배당 의무화 등이 필요하다. 장기적으로는 대만 모델을 참고하여 FIU를 경찰청 산하로 재편하거나, 국무총리실 산하에 FIU·경찰·금융감독원이 함께 입주하는 통합대응센터를 신설하는 방안을 검토해야 한다. 조직 재편이 어렵다면 최소한 물리적 공간을 공유하여 "같은 건물에서 일하는" 환경을 만들어야 실질적 협력이 가능하다.

예산 및 인력 확보 홍콩 ADCC는 90명의 전담 인력으로 24시간 체계를 운영하고 있으며, 대만 FIU는 29명의 특수요원으로 연간 360만 건의 CTR을 처리한다. 한국이 이와 유사한 수준의 대응체계를 구축하려면 초기 투자비용으로 약 500-600억 원이 소요될 것으로 추정된다. 이는 금융기관 분담금, 범죄수익환수금, 정부 특별예산을 결합하여 조달할 수 있다. 장기적으로는 사기 피해 감소로 인한 사회적 편익이 투자비용을 크게 상회할 것이다.

기술적 과제 대만의 AIT 플랫폼처럼 여러 정부 시스템(금융거래, 통신기록, 차량정보, 출입국기록)을 통합하는 것은 기술적으로 복잡하고 시간이 소요된다. 단계적 접근이 필요하며, 1단계에서는 금융거래와 통신기록 통합에 집중하고, 2-3단계에서 점진적으로 확대해야 한다. 또한 시스템 구축 과정에서 개인정보보호 기술(암호화, 접근권한 관리, 로그 감사)을 처음부터 설계에 반영해야 한다(Privacy by Design).

민간 부문의 자발적 참여 유도 홍콩의 은행동맹(ADA)과 대만의 파트너십 모델은 모두 금융기관의 자발적 참여를 기반으로 한다. 한국에서도 강제보다는 인센티브 중심의 접근이 필요하다. 적극 협조 은행에 대해서는 금융감독 평가 시 가점을 부여하고, 우수 사례를 공개적으로 인정하며, 사기 피해 감소로 인한 비용 절감 효과를 가시적으로 보여주어야 한다. 대만 FIU 담당자의 말처럼 "그들이 공유한 정보가 매우 효율적으로 사용될 것임을 알기 때문에, 그들은 우리와 일하는 것을 매우 기뻐한다"는 선순환 구조를 만들어야 한다.

본 연구에서 제시한 도입 방안은 홍콩과 대만의 성공 사례를 한국의 제도적·문화적 맥락에 맞게 조정한 것이다. 모든 과제가 단기간에 해결될 수는 없지만, 명확한 목표와 단계적 접근을 통해 3-5년 내에 세계 최고 수준의 사기범죄 대응체계를 구축할 수 있을 것이다.

6.3. 단계별 도입 방안

홍콩과 대만의 사례를 한국에 적용하기 위해서는 신중한 단계별 접근이 필요하다. 급진적 전면 도입보다는 시범사업을 통한 검증과 점진적 확대가 바람직하다.

1단계(6개월): 기반 구축. 법제도 정비를 최우선 과제로 추진해야 한다. 개인정보보호법 제58조의2 개정을 통해 사기 예방 목적의 정보 공유에 대한 명시적 법적 근거를 마련하고, 금융기관 간 대포통장 정보 공유를 합법화해야 한다. 동시에 국무총리실 산하 사기범죄통합대응센터 설립을 위한 조직 설계와 예산 확보를 진행한다. 서울·경기 지역을 시범 지역으로 선정하고 주요 5개 은행과 협약을 체결하여 기본 시스템을 구축한다.

2단계(6개월): 시범 운영. 24시간 상담 핫라인을 개설하고 실시간 자금 차단 체계를 시범 운영한다. 홍콩의 2시간 내 96% 응답률을 목표로 설정하되, 초기에는 4시간 내 80% 응답률을 1차 목표로 한다. FIU-경찰 간 정보 전달 시간을 현행 5개월에서 1개월 이내로 단축하기 위한 전담 채널을 구축한다. 대만의 AIT 플랫폼을 벤치마킹한 데이터 분석 플랫폼의 프로토타입을 개발하고, 중간 평가(3개월)와 최종 평가(6개월)를 통해 개선안을 도출한다.

3단계(12개월): 전국 확대. 시범사업의 성과를 바탕으로 전국 28개 주요 금융기관으로 참여를 확대한다. AI 기반 의심거래 자동 탐지 시스템을 도입하고, 상류 개입 프로그램을 전국적으로 시행하여 잠재적 피해자 15,000명에게 선제적으로 접촉한다. 24시간 실시간 대응 체계를 완성하고, 수사관 및 금융기관 직원에 대한 체계적 교육을 실시한다.

4단계(12개월 이후): 고도화 및 국제 협력. FRONTLINE PLUS에 적극 참여하여 중국·일본·싱가포르 등과 실시간 자금 차단 협약을 체결한다. 블록체인 추적 기술과 딥러닝 기반 예측 모델을 도입하여 기술적 고도화를 추진한다. 동북아 사기범죄 대응 네트워크를 주도하여 한국이 아시아 지역 허브 국가로서의 역할을 확립한다.

6.4. 기대 효과

정량적 효과로 실시간 자금 차단 체계의 구축으로 현재 약 50%에 불과한 차단 성공률을 3년 내 70%까지 향상시킬 수 있다. 홍콩이 2시간 내 96% 응답률을 달성한 것처럼, 한국도 평균 응

답 시간을 현행 4시간에서 2시간으로 단축할 수 있다. 상류 개입 시스템의 도입으로 연간 15,000명의 잠재적 피해자에게 선제적으로 접촉하여 홍콩처럼 630억 원 규모의 피해를 예방할 수 있다. FIU-경찰 협력 강화로 정보 전달 시간을 5개월에서 1개월로 단축하면 범죄 자금 추적의 실효성이 크게 향상될 것이다. 전체적으로 현재 연간 8,000억 원에 달하는 사기 피해액을 3년 내 30-40% 수준으로 감소시킬 수 있을 것으로 예상된다.

정성적 효과로 사회적 신뢰 회복 측면에서 금융 시스템에 대한 국민 신뢰도가 향상되고, 디지털 금융 서비스 이용률이 증가하며, 사기범죄에 대한 사회적 경각심이 제고될 것이다. 국제적 위상 강화 측면에서 한국은 아시아 지역 사기범죄 대응 선도국가로 부상하고, 한국형 대응 모델을 해외에 수출할 기회가 창출되며, 국제 협력에서 주도적 역할을 수행할 수 있다. 금융 산업 경쟁력 강화 측면에서 안전한 금융 환경으로 국제 투자를 유치하고, 핀테크 산업 발전의 기반이 조성되며, 금융기관의 평판 리스크가 감소할 것이다.

<Table 21> Expected effects and performance indicators by year

지표	현재(2024)	1년차 목표	2년차 목표	3년차 목표
피해 감소				
연간 피해액(억원)	8,000	6,400 (▼20%)	4,800 (▼40%)	3,200 (▼60%)
연간 피해 건수	약 35,000건	약 30,000건	약 25,000건	약 20,000건
자금 차단				
연간 차단 금액(억원)	약 500	1,000	1,500	2,000
차단 성공률	약 50%	60%	65%	70%
평균 응답 시간	4시간	3시간	2.5시간	2시간
2시간 내 응답률	약 30%	50%	70%	90%

출처: 저자 작성 (홍콩 사례 기준 추정)

사회적 신뢰 회복으로 금융 시스템에 대한 국민 신뢰도가 향상되고, 디지털 금융 서비스 이용률이 증가하며, 사기범죄에 대한 사회적 경각심이 제고될 것이다.

국제적 위상 강화로 아시아 지역 사기범죄 대응 선도국가로 부상하고, 한국형 대응 모델의 해외 수출 기회가 창출되며, 국제 협력에서의 주도적 역할을 수행할 것이다.

금융 산업 경쟁력 강화로 안전한 금융 환경으로 국제 투자를 유치하고, 핀테크 산업 발전의 기반이 조성되며, 금융기관의 평판 리스크가 감소할 것이다.

VII. 결론

본 연구는 홍콩의 ADCC·FMLIT와 대만의 하이테크 수사센터 및 FIU 사례를 심층 분석하여 한국의 사기범죄 대응체계 개선을 위한 실질적 시사점을 도출했다.

홍콩은 2016년 이후 사기범죄가 5.5배 급증하는 위기 상황에서 ADCC와 FMLIT라는 이중 대응체계를 구축하여 효과적으로 대응하고 있다. ADCC는 24시간 핫라인(연간 80,000건), 실시간 자금 차단(누적 2.4조 원), 상류 개입(15,000명 접촉)으로 즉각적 피해 차단을 실현했다. FMLIT는 경찰·금융감독청·28개 은행이 참여하는 민관 협력 플랫폼으로 52,000개 미확인 계좌를 발굴하고 3,260억 원을 동결했다.

대만은 하이테크 수사센터를 통해 디지털 포렌식(EnCase, Cellebrite), 암호화폐 추적, 빅데이터 플랫폼(AIT)으로 기술 중심 접근을 실현했다. FIU는 수사국 내부에 위치하여 수사기관과

긴밀히 협력하며, 금융기관과 파트너십 모델을 구축하여 자발적 협력을 이끌어냈다. 연간 360만 건의 CTR을 주식시장 보드 방식의 자동화 시스템으로 처리하고 있다.

한국은 FIU-경찰 협력 지연, 실시간 자금 차단 미흡, 통합 조정 기구 부재라는 구조적 한계를 안고 있다. 홍콩과 대만의 모범 사례는 이러한 한계를 극복할 수 있는 구체적 해법을 제시한다.

홍콩과 대만의 사례는 사기범죄 대응이 단순한 단속이 아니라 체계적 시스템 구축임을 보여준다. ADCC의 24시간 실시간 대응, FMLIT의 민관 협력, 대만의 기술 통합 플랫폼은 모두 '신속성', '협력', '기술'이라는 세 가지 핵심 가치를 공유한다.

한국은 우수한 IT 인프라, 전문적인 FIU 인력, 선진적인 피해자 보호 제도를 보유하고 있다. 여기에 홍콩의 실시간 대응 체계, 대만의 기술 통합 플랫폼을 접목한다면 세계 최고 수준의 사기범죄 대응체계를 구축할 수 있다.

2024년 현재 연간 8,000억 원의 전기통신금융사기 피해는 단순한 경제적 손실을 넘어 사회적 신뢰 붕괴의 신호이다. 본 연구에서 제시한 8대 정책 제언이 실현된다면, 3년 내 피해를 60% 감소시키고 1조 원 이상의 사회적 편익을 창출할 수 있을 것이다.

홍콩 경찰의 슬로건처럼 "We Serve with Pride and Care"의 정신으로, 한국도 국민을 사기범죄로부터 보호하는 선진적 시스템을 구축해야 할 때이다. 본 연구가 그 첫걸음에 작은 기여가 되기를 기대한다.

부록 (Supplementary material)

다음 부록은 학술지 홈페이지에서 보실 수 있습니다.

- <부록 1> 홍콩 사기대응조정센터(ADCC) 및 합동금융정보분석원(JFIU) 운영 현황 브리핑 [Briefing on Operations of Hong Kong's Anti-Deception Coordination Centre and Joint Financial Intelligence Unit]
- <부록 2> 대만 금융정보분석원(FIU) 인터뷰 및 하이테크 수사센터(HTIC) 기술 수사 체계 [Interview with Taiwan FIU and Overview of High-Tech Investigation Center's Capabilities]

참고문헌 (References)

[1] National Police Agency. 2024. Voice phishing status statistics [경찰청_보이스피싱 현황]. Public Data Portal. Available at: https://www.data.go.kr/data/15063815/fileData.do accessed on 2025. 12. 3.

[2] Financial Action Task Force (FATF). 2019. Anti-money laundering and counter-terrorist financing measures – Hong Kong, China, Fourth Round Mutual Evaluation Report. FATF, Paris, France. p. 87. Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/mer/MER-Hong-Kong-China-2019.pdf accessed on 2025. 12. 3.

[3] Hong Kong Police Force Commercial Crime Bureau. 2025. Anti-Deception Coordination Centre (ADCC) briefing. Presentation at International Financial Investigation Course (IFIC) 2025, Hong Kong. (Transcript available in Appendix).

[4] Ministry of Justice Investigation Bureau (MJIB, Taiwan). 2025. 2025 workshop on transnational fraud crime response (workshop materials). MJIB, Taipei, Taiwan. (Transcript available in Appendix).

[5] Financial Services Commission. 2024. Rapid blocking of voice phishing damage using simple remittance (press release) [간편송금을 악용한 보이스피싱의 피해를 신속히 차단할 수 있게 되었습니다]. Available at: https://www.fsc.go.kr/po010106/82912 accessed on 2025. 12. 3.

[6] Financial Action Task Force (FATF). 2021. Updated guidance for a risk-based approach to virtual assets and virtual asset service providers. FATF, Paris, France. pp. 23-25.

[7] Financial Services Commission. 2024. Strengthening mutual cooperation between telecommunications and financial sectors (press release) [보이스피싱 등 금융범죄 피해 예방을 위해 통신·금융 부문 간 상호협력을 강화해 나가겠습니다]. Available at: https://www.fsc.go.kr/no010101/82077 accessed on 2025. 12. 3.

[8] Financial Supervisory Service. 2024. Analysis of 2023 voice phishing damage status [2023년 보이스피싱 피해현황 분석]. Available at: https://www.fss.or.kr/fss/bbs/B0000188/view.do?nttId=134451 accessed on 2025. 12. 3.

[9] OpenText. 2025. OpenText Forensic. Open Text Corporation. Available at: https://www.opentext.com accessed on 2025. 10. 11.

[10] Cellebrite. 2025. Digital Intelligence Suite. Cellebrite. Available at: https://cellebrite.com accessed on 2025. 10. 11.

[11] MSAB. 2025. XRY Mobile Forensics. MSAB. Available at: https://www.msab.com accessed on 2025. 10. 11.

[12] Constitutional Court of Korea, 2019. 12. 27. 2019Hun-Ma579.

[13] Korean Law Information Center. Special Act on Prevention of Damage from Telecommunications Fraud and Refund of Damage [전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법]. Act No. 20368, Partial Amendment 2024. 2. 27. Available at: https://www.law.go.kr/lsInfoP.do?lsId=011359 accessed on 2025. 12. 3.

[14] Hong Kong Monetary Authority (HKMA). 2023. Guideline on anti-money laundering and counter-financing of terrorism. HKMA, Hong Kong. pp. 34-36. Available at: https://brdr.hkma.gov.hk/eng/doc-ldg/docId/20230525-4-EN accessed on 2025. 12. 3.

[15] Monetary Authority of Singapore (MAS). 2020. Payment Services Act 2019 practice direction. MAS, Singapore. pp. 23-27.

[16] Hong Kong Police Force. 2017. Anti-Deception Coordination Centre opens. The Newspaper of the Hong Kong Police Force: Offbeat, No. 1093. Available at: https://www.police.gov.hk/offbeat/1093/eng/5655.html accessed on 2025. 10. 11.

[17] Office of the Privacy Commissioner for Personal Data. 2025. The personal data (privacy) ordinance. PCPD.org.hk. Available at: https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html accessed on 2025. 10. 11.

[18] Government of the Hong Kong Special Administrative Region. 2023. Combating deceptive activities jointly with banking sector (press release). Available at: https://www.info.gov.hk/gia/general/202306/28/P2023062800411.htm accessed on 2025. 10. 11.

[19] Hong Kong Police Force. 2017. CCB launches Fraud & Money Laundering Intelligence Taskforce. The Newspaper of the Hong Kong Police Force: Offbeat, No. 1089. Available at: https://www.police.gov.hk/offbeat/1089/eng/5433.html accessed on 2025. 10. 11.

[20] Hong Kong Police Force. 2021. Financial Intelligence and Investigation Bureau established. The Newspaper of the Hong Kong Police Force: Offbeat, No. 1187. Available at: https://www.police.gov.hk/offbeat/1187/eng/9020.html accessed on 2025. 10. 11.

[21] Hong Kong Special Administrative Region Government. 2022. Hong Kong money laundering and terrorist financing risk assessment report. Hong Kong Special Administrative Region Government, Hong Kong. pp. 57–58. Available at: https://www.fstb.gov.hk/fsb/aml/en/doc/Money%20Laudering%20Report_2022_EN.pdf accessed on 2025. 10. 11.

[22] Hong Kong. 1994. Organized and Serious Crimes Ordinance, Cap. 455.

[23] Tam Sze Leung v Commissioner of Police. 2021. HKCFI 3118.

[24] Tam Sze Leung & Ors v Commissioner of Police. 2023. HKCA 537.

[25] Tam Sze Leung & Ors v Commissioner of Police. 2024. HKCFA 8 (Court of Final Appeal).

[26] Department of Justice, Government of the Hong Kong Special Administrative Region. 2025. Civil Recovery of Crime Proceeds. Available at: https://www.doj.gov.hk/en/community_engagement/prosecution_code/civil_recovery.html accessed on 2025. 10. 11.

[27] Republic of Korea. 2021. Special Act on Prevention of Damage from Telecommunications Fraud and Refund of Damage. Act No. 18548, Enacted 2021. 12. 21.

[28] Ministry of Justice. 2024. A New Life Sprouts! Crime Victim Protection and Support System. Policy Briefing. Available at: https://www.moj.go.kr/moj/241/subview.do accessed on 2025. 12. 3.

[29] Taiwan High Prosecutors Office. 2025. High-Tech Investigation Center. Available at: https://www.tph.moj.gov.tw/4421/4447/965711/965717/post accessed on 2025. 10. 11.

[30] Taiwan High Prosecutors Office. 2025. High Tech Investigation Center overview. Workshop Materials. Taiwan High Prosecutors Office, Taipei, Taiwan. (Transcript available in Appendix).

[31] Kwon WS. 2025. Interview on FIU operations and international cooperation with Taiwan Financial Intelligence Unit. Personal interview conducted by author. (Transcript available in Appendix).

[32] Egmont Group of Financial Intelligence Units. 2023. Principles for information exchange Between Financial Intelligence Units. Egmont Group, Ottawa, Canada. pp. 8–9. Available at: https://egmontgroup.org/wp-content/uploads/2022/07/2.-Principles-Information-Exchange-With-Glossary_April2023.pdf accessed on 2025. 10. 11.

[33] Financial Crimes Enforcement Network (FinCEN). 2025. Frequently asked questions regarding the FinCEN currency transaction report (CTR). FinCEN. Available at: https://www.fincen.gov/frequently-asked-questions-regarding-fincen-currency-transaction-report-ctr accessed on 2025. 10. 11.

[34] Ministry of Law Singapore. 2025. How is the SGD 20,000 threshold determined for a cash transaction report. ask.gov.sg. Available at: https://ask.gov.sg/mlaw accessed on 2025. 10. 11.

[35] Financial Action Task Force (FATF). 2023. International standards on combating money laundering and the financing of terrorism & proliferation. Recommendation 23. FATF, Paris, France.

[36] Financial Services Commission. 2024. Korea Financial Intelligence Unit (FIU) establishes 2024 business plan (press release) [금융정보분석원(FIU), 2024년도 업무계획 마련]. Available at:

https://www.fsc.go.kr/no010101/81700 accessed on 2025. 12. 3.

[37] Hong Kong Police Force. 2025. Joint Financial Intelligence Unit. Hong Kong Police Force. Available at: https://www.police.gov.hk/ppp_en/04_crime_matters/jfiu/ accessed on 2025. 10. 11.

[38] Maxwell NJ, Artingstall D. 2017. The role of financial information-sharing partnerships in the disruption of crime. RUSI Occasional Paper. Available at: https://static.rusi.org/201710_rusi_the_role_of_fisps_in_the_disruption_of_crime_maxwell_artingstall_web_4.2.pdf accessed on 2025. 12. 3.

[39] National Crime Agency. 2025. National Economic Crime Centre. Available at: https://www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre accessed on 2025. 10. 11.

[40] Singapore Police Force. 2025. Anti-Scam Centre of the Singapore Police Force. Available at: https://www.police.gov.sg accessed on 2025. 10. 11.

[41] Financial Services Commission. 2025. Comprehensive measures to block voice phishing throughout the entire cycle (press release) [일상 속 보이스피싱 '안심필터' 장착!]. Available at: https://www.fsc.go.kr/no010101/85186 accessed on 2025. 12. 30.

[42] Lee YJ. 2025. Two months after launch of integrated response team... voice phishing damage on 'decline' [통합대응단 출범 2개월…보이스피싱 피해 '감소세']. Seoul Economic Daily. Available at: https://www.sedaily.com/NewsView/2H1MY9DS1C accessed on 2025. 12. 30.