JDFR Journal of Data Forensics Research
데이터포렌식연구, 2권 1호, 2025년 6월, 55-69면
Journal of Data Forensics Research, Volume 2, Issue 1, June 2025, Pages 55-69.
https://doi.org/10.12972/JDFR.2025.2.1.4
Print ISSN 3058-9460
Online ISSN 3058-9479

원저

메신저피싱 범행 전(全) 과정의 실증적 분석과 예방·수사 전략

전병하[1,2]

[1]부산경찰청 사이버범죄수사대 팀장, [2]경찰청 사이버 분야 책임수사관, 수사 동료강사

교신저자: 전병하, best024@police.go.kr

요약

본 연구는 메신저피싱 범죄의 실행 전 과정을 실증적으로 분석하고, 수사기관이 각 범행 단계에서 확보할 수 있는 핵심 단서와 대응 절차를 구조화된 형태로 제시하였다. 실제 피해자의 문자 메시지, 디지털 포렌식 자료, 금융 거래 내역, 인증서 발급 이력 등을 기반으로, 범행은 ▲정보 탈취 ▲금융정보 확보 및 자금 송금 ▲현금화의 세 단계로 구성되며, 각 단계에는 조직화된 실행 인력이 개입된 구조적 범죄 양상이 확인되었다.

특히 피해자가 인지하지 못한 증권계좌 개설, 보험 약관대출 실행, 스마트폰 초기화로 인한 디지털 증거 소실 등은 수사 현장에서 반복적으로 발생하는 핵심 장애요소로 파악되며, 이에 대응하기 위한 실무 수단으로 명의도용방지 서비스(Msafer), 계좌정보통합관리시스템, 금융인증서 발급 이력 조회 등의 디지털 도구를 제시하였다.

아울러 본 논문은 피의자 추적 수사의 실제 진행 과정을 정리하고, 초국경 디지털 범죄에 직면한 수사의 구조적 한계를 실증적으로 분석하였다. 이를 통해 수사 초기 대응 역량 강화를 도모하고, 유사 범죄의 예방과 제도적 보완에 기여할 수 있는 실천적 대안을 제시하고자 한다.

주제어

메신저피싱, 전기통신금융사기, 비대면 계좌 개설, 보험 약관대출, 디지털 증거, 인증서 발급 이력, 디지털 흔적 확보, 초기 증거 보존, 초동 수사 대응

Received: June 14, 2025
Revised: June 29, 2025
Accepted: June 30, 2025
Published: June 30, 2025

Original Article

Empirical analysis of messenger-phishing process and strategic approaches to crime prevention and investigation

Byeong-Ha Jeon[1,2]

[1]Team Leader, Cybercrime Investigation Division, Busan Metropolitan Police Agency, Republic of Korea
[2]Senior Investigator, Cybercrime, Korean National Police Agency; Instructor, Criminal Investigation, Republic of Korea

Corresponding Author: Byeong-Ha Jeon, best024@police.go.kr

ABSTRACT

This study provides an empirical analysis of the complete execution process of messenger-phishing crimes and systematically presents key evidence and procedural responses that investigative authorities can obtain at each stage of a crime. Drawing on actual case data, including victim text messages, digital forensic materials, financial transaction records, and certificate issuance histories, each crime is structured into three stages: information theft, financial access and fund transfer, and cash-out. Each stage reveals the characteristics of an organized criminal structure involving specialized personnel.

Notably, issues such as unauthorized securities account openings, insurance policy loans executed without the victim's awareness, and the loss of digital evidence due to smartphone resets are frequently encountered during investigations. As practical countermeasures, this study introduces relevant tools, including an identity theft prevention service (Msafer), an account information integration system, and digital certificate issuance tracking services.

Furthermore, this study outlines the actual investigative process of tracking suspects and empirically analyzes the structural limitations encountered in investigations of cross-border digital crimes. The study findings aim to strengthen early-stage investigative capabilities and provide practical recommendations for crime prevention and system improvement.

KEYWORDS

Messenger phishing, telecommunication-based financial fraud, non-face-to-face account opening, policy loan, digital evidence, certificate issuance history, digital trace preservation, initial evidence retention, early-stage investigation response

I. 서론

메신저피싱은 가족이나 지인을 사칭하여 피해자로부터 금융정보를 탈취한 뒤, 원격조작 프로그램을 통해 피해자의 스마트폰을 실질적으로 통제하고, 이후 금융기관 애플리케이션에 접속해 인증서를 발급받아 자금 이체나 대출을 실행하는 전기통신금융사기의 일종이다.

특히, 피해자에게 심리적 압박을 주는 사칭 메시지와 함께 '팀뷰어(TeamViewer)' 등의 원격 접속 앱 설치를 유도해 피해자의 기기를 완전히 장악하는 것이 핵심 수법으로 사용된다.

본 범죄 유형은 단기간에 고액 자금 탈취가 가능하고, 범행 수법이 조직화·체계화되는 양상을 보이므로, 피해자 보호와 수사 초기 단계에서의 대응이 매우 중요하다. 본 연구는 실제 수사 경험을 바탕으로 메신저피싱 범행의 전 과정을 시간 순으로 정리하고, 정보 탈취에서 현금 인출에 이르는 일련의 절차를 구조화하여 실증적으로 분석하였다.

특히 사건 접수 즉시 수사기관이 확보할 수 있는 주요 단서와 대응 포인트를 구체화함으로써, 초동 수사단계에서의 실무 수사관 대응 역량 제고를 목적으로 한다. 아울러, 명의도용 방지 서비스, 계좌정보통합관리 시스템, 금융인증서 발급 이력 조회 등 현실적으로 활용 가능한 예방 및 대응 수단을 제시하며, 이를 바탕으로 본 논문은 예방과 수사를 아우르는 실용적 메신저피싱 대응 전략을 제안한다.

II. 관련 연구 및 분석 사례의 출처

2.1. 분석 사례의 출처 및 실증적 기반

본 논문이 분석한 사건은 2022년 말 부산경찰청에 접수된 메신저피싱 사건으로, 본 논문 작성자가 해당 사건의 신고 접수부터 범행 흐름 분석, 피의자 추적 및 수사 종결까지의 전 과정을 직접 수사하며 확보한 일련의 실증 자료들을 기반으로 구성되었다. 이에 따라 본 연구는 단순 문헌 분석을 넘어서 실제 수사 사례에 기반한 실무 적용 가능한 분석 결과를 제공한다.

2.2. 메신저피싱 관련 선행연구 검토

메신저피싱에 관한 기존 연구들은 주로 지인 사칭 사례 분석, 피해 현황 통계, 예방 교육 방안 제시 등에 초점을 맞추어 수행되어 왔다. 대표적으로, 정제용·장준원·서준배(2022)[1]는 메신저피싱 피해 현황과 문제점을 정리하고, 자동 탐지 시스템 및 예방 교육을 대응책으로 제시하였다. 남소원·이학선·이상진(2022)[2]은 피해자의 경험 사례를 통해 사칭 메시지의 유형을 분류하고, 민간 및 공공기관의 협력 필요성을 강조하였다. 최연준·최승원(2021)[3]은 상황적 범죄예방이론을 적용하여 메신저피싱 범죄 흐름을 단계별로 분석하고 제도적 대안을 제시하였다.

또한, 정영호·하형준(2022)[4]은 수원지역 실제 사건 120건과 수사관 인터뷰를 바탕으로, 메신저피싱 수법의 진화 양상과 대응책의 실효성을 분석하였다. 이는 본 논문과 유사하게 실무 기반 수사자료를 활용하였다는 점에서 중요한 참고사례로 평가된다.

한편, 금융감독원[5], 금융결제원[6], 법무부[7], 한국형사법무정책연구원[8] 등 공공기관에서는 메신저피싱을 포함한 피싱 범죄의 통계 분석, 제도 개선안, 대응 매뉴얼 등을 지속적으로 발간하고 있으며, 이러한 자료는 수사 실무자에게 실질적인 가이드를 제공하는 데 기여하고 있다.

그러나 위 연구들은 대부분 예방 교육이나 제도 개선에 중점을 둔 점에서, 수사 실무 중심의

실행 분석이나 디지털 증거 확보 방안에 대한 실질적 고찰은 다소 부족한 실정이다. 이에 본 논문은 실제 사건 수사에서 확보된 문자 메시지, 포렌식 기록, 인증서 이력, 금융거래 내역 등 디지털 자료를 기반으로 범죄 전 과정을 구조화·실증 분석함으로써, 수사 실무자 관점에서의 대응 전략 수립에 실질적인 기여가 가능한 후속 연구로서의 의의를 갖는다.

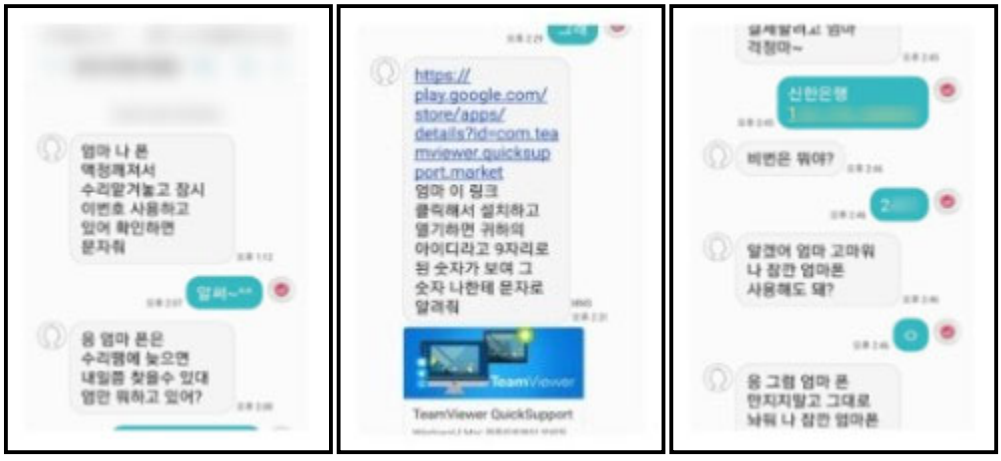
III. 범행 수법의 구조화

3.1. 정보 탈취 단계

피의자는 피해자의 딸 또는 가족을 사칭하여 문자메시지를 전송하며 범행을 시작한다. “폰 액정이 깨져 수리를 맡겨두고 있다”, “이 번호를 사용하고 있으니 문자로 연락해 달라” 등의 문구를 통해 피해자의 신뢰를 유도하고, 문화상품권 구매를 핑계로 피해자의 스마트폰에 ‘팀뷰어 퀵서포트(TeamViewer QuickSupport)’ 앱 설치를 요청한다.

피해자가 해당 앱을 설치하고 팀뷰어 ID를 전달하면, 피의자는 스마트폰의 원격조작 권한을 확보하게 된다. 이후 “충전 중이니 스마트폰을 엎어두고 당분간 사용하지 말라”는 요청을 통해 피해자의 추가 개입을 차단하며, 기기의 실질적 통제권을 장악한다. 이때 사용되는 언어는 명령조 문장이 아니라, 피해자의 자녀가 실제로 사용할 법한 일상적이고 감정 이입이 쉬운 표현들로 구성된다. “폰이 고장 났다”, “대신 문자로 얘기하자” 등은 부모 입장에서 일상적으로 마주칠 수 있는 상황으로 인식되며, 그 결과 피해자의 초기 경계심을 낮추는 효과가 있다.

이러한 표현 전략은 단순한 기망을 넘어, 피해자의 심리와 관계적 신뢰를 기반으로 설계된 사회공학적 언어 구조로 평가될 수 있다. 이는 보안 지식의 유무와 관계없이 누구나 속을 수 있는 구조적 설계이자, 메신저피싱 범죄의 초기 침투 성공률을 높이는 핵심 요소라 할 수 있다.



<Figure 1> 피해자가 수신한 문자메시지(※피해자 정보 탈취는 가족을 사칭한 문자에서 시작)

3.2. 금융정보 확보 및 계좌 탈취

피의자는 원격 접속 환경을 활용하여 피해자의 신분증 이미지, 계좌번호, 비밀번호 등의 민감정보를 확보한 뒤, 피해자의 주거래 은행 애플리케이션에 접속한다. 이 과정에서 모바일 OTP 및 금융인증서를 재발급 받아, 타행 간 자금 이체 및 계좌 잔액 조회 등의 핵심 권한을 확보한다.

이후 피의자는 피해자 명의로 비대면 방식의 증권계좌를 신규 개설하고, 이를 기반으로 공동

인증서를 발급받는다. 발급된 공동인증서는 보험사 애플리케이션에 로그인하여 약관대출을 실행하는 데 활용되며, 피해자는 대출이 실행되었다는 사실조차 인지하지 못한 상태에서 피해를 입게 된다.

나아가, 피의자는 인증 절차의 우회 및 분산을 목적으로 피해자 명의로 새로운 휴대전화번호를 비대면 방식으로 개통하고, 이를 추가 인증 수단으로 활용하기도 한다. 이 방식은 범행 속도를 높이고, 기존 단말 인증 실패 시 대체 경로로 작동하도록 설계된다.

특히 피해자 명의의 증권계좌를 범행 경로에 삽입하는 또 다른 목적은, 피해자가 범행 사실을 인지하더라도 최종 수취 계좌에 대한 지급정지 요청을 지연시키기 위한 '시차 전략'에 있다.

피해자의 자금은 본인도 모르는 명의 계좌를 경유한 후 최종 이체되므로, 자금 회수에 필요한 시간적 여유를 피의자에게 제공하는 효과가 발생한다.

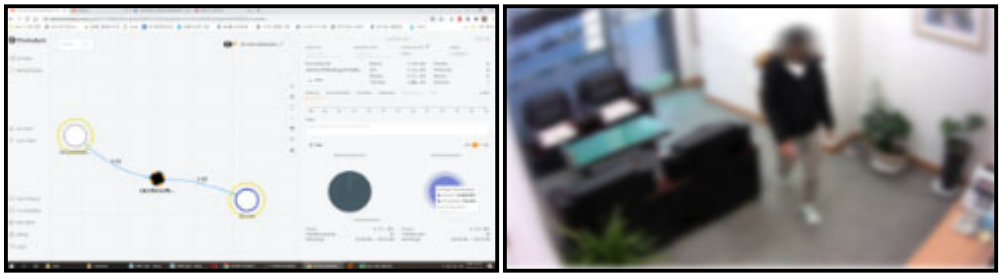
3.3. 자금 이체 및 현금 인출

피의자가 피해자의 인증 수단을 완전히 확보하게 되면, 피해자의 금융정보는 사실상 피의자의 자산처럼 실시간으로 운용된다. 이후 범행은 지체 없이 실행되며, 피해금은 동시에 복수의 경로를 통해 신속하게 분산·이동된다.

우선, 피해자의 계좌에서는 국내 가상자산 거래소의 가상계좌로 자금이 송금된다. 이는 단순 송금이 아니라 비트코인 등 가상자산의 구매를 목적으로 한 절차이며, 자산 구매 직후 해당 암호화폐는 해외 가상자산 거래소로 전량 이체된다.

이러한 방식은 범죄수익을 국내 금융기관의 지급정지 제도 범위 밖으로 회피시키기 위한 주요 수법으로, 수사기관이 자금 동결을 시도하기 이전에 디지털 자산화 및 국외 이전이 완료되는 구조를 따른다.

동시에, 피해자의 계좌 일부는 백화점 상품권 판매업자의 계좌로 송금되며, 실물 상품권은 범죄조직이 사전에 배치한 현장 수령 인력에 의해 즉시 수령된다. 이와 같은 복수 경로의 실행은 자금 회수 방해를 목적으로 정밀하게 설계된 구조로 평가된다.



<Figure 2> 피해금 이동 과정① (※좌측: 최종 해외 환전소 이동내역, 우측: 백화점 상품권 수령 현장)

또한, 일부 피해금은 피해자 명의로 개설된 증권계좌를 경유한 뒤, 일명 '대포통장'으로 분산 송금되며, 이후 전국 각지의 ATM과 해외 ATM을 통해 현금으로 인출된다. 특히 해외 ATM 인출은 필리핀 마닐라 소재 HSBC Quezon Avenue 지점에서 반복적으로 이루어졌으며, 동일 시간대에 수 회에 걸쳐 93만 원씩 분할 인출되는 방식으로 수행되었다.

이는 피해자의 카드 및 계좌가 해외에서 실시간으로 운용되었음을 입증하는 정황으로, 본 범행이 단순 온라인 송금에 그치지 않고 국제적 실행 체계를 기반으로 한 조직범죄적 특성을 갖고

있음을 시사한다.

연번	계좌번호	거래일자	거래시간	거래구분	취급점	출금적요	출금액	거래후잔액
1	356	202	06	체크	2	HSBC0852/QUEZONAVENU	931,492	
2	356	202	53	체크	2	HSBC0852/QUEZONAVENU	931,492	
3	356	202	35	체크	2	HSBC0852/QUEZONAVENU	931,492	
4	356	202	18	체크	2	HSBC0852/QUEZONAVENU	931,492	
5	356	202	01	체크	2	HSBC0852/QUEZONAVENU	931,492	
6	356	202	04	체크	2	HSBC0852/QUEZONAVENU	931,492	
7	356	202	48	체크	2	HSBC0852/QUEZONAVENU	931,492	

<Figure 3> 피해금 이동 과정② (※필리핀 마닐라 소재 HSBC Quezon Avenue 지점에서 반복 출금)

3.4. 다단계 현금화 체계와 조직적 실행구조

메신저피싱은 단순히 원격조작 애플리케이션을 통해 피해자의 금융정보를 탈취하는 수준에 그치지 않는다. 자금 이동 과정에서는 상품권 수령자, ATM 인출자, 해외 거래소 계정 운영자 등으로 구성된 다단계 실행조직이 사전에 배치되어 범행을 완결하는 구조를 가진다. 이는 단일 범죄자의 단발성 범행이 아니라, 조직화된 실행 체계에 기반한 복합적 범죄 행위임을 강하게 시사한다.

특히, 피해자도 모르게 피해자 명의로 개설된 증권계좌를 자금 이동 경로에 삽입함으로써, 피해자는 본인이 범행 사실을 인지하더라도 최종 수취 계좌에 대한 지급정지 요청이 지연되는 시간적 간극이 발생한다.

이러한 '시차 전략'은 피의자가 자금 이동을 마무리할 수 있는 여유 시간을 확보함으로써, 범행의 실질적인 현금화율을 높이는 핵심 기법으로 기능한다.

아울러, 다수의 피해자는 심리적 충격과 불안감으로 인해 스마트폰을 초기화한 상태에서 수사기관에 출석하는 사례가 빈번하게 확인된다. 이로 인해 문자 메시지, 인증번호 수신기록, 앱 설치 로그 등 핵심 디지털 증거 확보가 지연되거나 불가능해지는 문제가 발생한다. 그 결과 피해자는 본인 명의로 개설된 증권계좌, 실행된 약관대출, 가상자산 구매 및 송금 내역조차 인지하지 못한 채 진술하는 경우가 다수 보고되고 있다.

이러한 일련의 구조는 피의자가 기술적 침투, 심리적 설계, 물리적 실행을 통합적으로 수행하는 복합적 조직범죄체계에 기반하고 있음을 분명히 보여준다. 따라서 메신저피싱은 단순한 사기 사건이 아닌, 디지털 공간에서 정교하게 체계화된 '범죄공정(Process)'으로 이해되어야 하며, 이에 대응하기 위한 수사 전략의 구조화 및 제도적 보완이 시급히 요구된다.

Ⅳ. 메신저피싱 전 과정 실증분석

메신저피싱 범행은 전형적인 '가족 사칭 기반 전기통신금융사기'로 시작되지만, 피해자의 스마트폰을 완전히 장악한 이후에는 피해자의 인증 수단, 금융 계좌, 보험 계약까지 피의자가 모두 지배하는 형태로 전개된다. 본 장에서는 실제 사건에서 확보한 피해자의 문자메시지, 팀뷰어 로그, 금융사 인증 문자, 계좌 거래 내역, 포렌식 복구자료 및 압수영장 회신자료를 바탕으로 메신저피싱 범죄의 전체 과정을 시간 순으로 재구성하였다.

다음은 메신저피싱 범행의 전형적 흐름을 세 단계로 구분하여 요약한 도표이다.

<Table 1> 메신저피싱 범행의 전형적 흐름

범행유형	정보탈취	금융정보 확보·계좌탈취	자금이체·현금 인출
범행 내용	- 문자로 가족 사칭 - 신분증 사진·계좌번호·비밀번호 요구 - 팀뷰어 설치 통한 스마트폰 원격조작 권한 획득	- 주거래은행 앱 접속 - 금융인증서·공동인증서 재발급 - 증권계좌 신규 개설 - 보험 앱 접속 및 약관대출 실행 - 신규 휴대전화번호 비대면 개통	- 피해자 계좌에서 가상자산 구매 후 해외 거래소로 이체 - 상품권 송금 및 실물 수령 - 증권계좌 경유 후 대포통장 이체 - 국내·해외 ATM 인출

4.1. 범행 시작: 피해자 유인 및 팀뷰어 설치

이 범행은 주변에서 누구에게라도 일어날 수 있는 이야기로 시작된다. 피의자는 피해자의 딸을 사칭하여 친근하고 일상적인 문장으로 문자를 보낸다. 수리 중이라며 전화가 되지 않는다고 알리고, 대신 문화상품권을 대신 결제해달라며 점차 스마트폰 통제를 확보한다.

<Table 2> 문자메시지① – 피해자 유인 및 팀뷰어 설치 과정

연번	시간	문자메시지 내용
1	13:12:25	엄마 나 폰 액정깨져서 수리맡겨놓고 잠시 이번호 사용하고 있어 확인하면 문자줘
2	13:15:10	엄마 폰은 수리맡겨놔서 이 번호로 내일쯤 찾을 수 있대. 엄마 뭐하고 있어?
3	14:01:52	엄마 나 폰 안되니까 답답해 죽겠어 ㅠㅠ 이번호로 문자해줘
4	14:25:39	지금 바쁘면 나 부탁 하나만 해도 돼?
5	14:27:19	온라인 문화상품권 구매하려는데 인증이 안돼서 엄마 폰으로 결제 좀 해줄 수 있어?
6	14:27:39	간단해 앱 하나 깔고 내가 하면 돼 링크 줄게
7	14:31:11	https://play.*****/com.teamviewer.quicksupport.market앱 설치하고 거기 나오는 숫자만 알려줘
8	14:33:56	설치했어? 숫자 뭐야?
9	14:36:14	내가 지금 연결 중이니까 아무것도 누르지 말고 그냥 냅둬
10	14:39:29	엄마 연결됐어 고마워

4.2. 신분증 확보 및 계좌정보 탈취

피의자는 피해자의 스마트폰을 원격조작하게 된 후, 피해자의 신분증 사진과 계좌번호, 비밀번호를 요구한다. 이 과정에서도 피의자는 신뢰를 이용해 요청을 이어간다. 신분증이 필요하다며 캡처나 촬영을 유도하고, 계좌번호와 비밀번호를 따낸다.

<Table 3> 문자메시지② - 신분증 확보 및 계좌정보 탈취 과정

연번	시간	문자메시지 내용
1	14:40:14	엄마 인증 다시 하려면 신분증 앞면 필요하대 사진 좀 찍어줘
2	14:40:31	주민등록증 보내줘야한대 ㅠㅠ 바로 지울게
3	14:42:15	엄마 계좌 어디야? 예금주 이름이랑 번호 알려줘
4	14:42:36	111111111111 이거 맞아?
5	14:42:56	비밀번호는 2***이야?
6	14:48:24	폰 화면이 지금 안 보여 앱 잘못 깐 거 아니지?
7	14:49:10	엄마 그냥 폰 엎어두고 충전만 해줘. 내가 알아서 할게

4.3. 금융기관 접근 및 인증 절차 실행

인증 정보와 원격조작 환경을 확보한 피의자는 본격적으로 금융기관 앱에 접근한다. 인증서 재발급, 간편비밀번호 설정 등 일련의 인증 절차를 피해자 모르게 차례로 진행한다.

<Table 4> 인증절차 수행 및 금융기관 접근 로그 요약

연번	시간	문자메시지 내용
1	15:00:08	팀뷰어를 통한 화면 제어 재확인됨
2	15:03:21	주거래은행 앱 실행, 공동인증서 발급 메뉴 진입
3	15:04:43	OTP 인증번호 수신 (문자 내용: 489273)
4	15:07:02	금융인증서 신규 발급 요청 로그 확인됨
5	15:10:47	간편비밀번호 설정 완료 메시지 수신
6	15:13:56	한국투자증권 앱 최초 실행 및 로그인 시도
7	15:15:22	한국포스증권 로그인 성공 로그 발생
8	15:17:44	재인증 문자 11**** 수신 및 입력 완료 로그

4.4. 피해자 명의 신규 계좌 개설 및 보험 앱 접근

피의자는 피해자 명의로 증권계좌를 개설하고, 공동인증서를 발급받아 이를 보험 앱에 연동해 약관대출을 실행한다. 피해자는 이 대출 실행 사실을 전혀 인지하지 못한 상태로, 피해 직후에도 자신 명의 계좌에서 대출이 있었다는 것을 모르고 있었다.

<Table 5> 증권계좌 개설 및 약관대출 실행 과정 로그 요약

연번	시간	문자메시지 내용
1	15:18:50	증권사 계좌 개설 화면 진입 로그 기록됨
2	15:19:27	개인정보 입력 및 계좌 약관 동의 완료
3	15:20:14	공동인증서 발급 완료 및 자동 연동 처리됨
4	15:21:03	한국투자증권 계좌 개설 성공 확인 메시지 수신
5	15:22:48	보험사 앱 설치 및 로그인 시도 기록됨
6	15:23:15	약관대출 실행 버튼 클릭 확인 (10,000,000원)
7	15:24:07	대출금 피해자 주거래은행 계좌 입금 완료
8	15:26:35	새로운 휴대전화번호 개통 – 본인 명의 사용됨
9	15:28:01	새 번호로 2차 인증 요청 및 OTP 확인 로그 발생

4.5. 자금 분산 및 실시간 현금화

15:20경부터 피해자의 계좌에서는 자금이 가상자산 거래소, 백화점 상품권 판매업자, 전국 ATM, 해외 ATM 등으로 분산 이체되었다.

특히 백화점 상품권 송금 직후에는 실제 상품권을 수령하기 위해 현장에 등장한 제3자 인물이 확인되었고, 이는 범행이 사전에 조직적으로 준비되어 있었음을 강하게 시사한다.

해외 현금 인출은 필리핀 HSBC Quezon Avenue 지점 ATM에서 반복적으로 수행되었으며, 총 10여 차례에 걸쳐 동일 금액(93만 원)이 분할 출금된 정황이 확인되었다. 국내 인출은 서울, 경기 지역의 주요 은행 지점에서 다수 확인되었다.

<Table 6> 자금 분산 및 실시간 현금화 흐름 요약

연번	시간	문자메시지 내용
1	15:28:52	업비트 가상자산 거래소 가상계좌 입금 요청 기록됨
2	15:30:17	피해자 계좌에서 300만원 이체됨
3	15:31:03	업비트 거래소 계정 내 BTC 구매 로그 확인됨
4	15:33:41	BTC 전량 해외 거래소 전송 완료 확인됨
5	15:35:08	백화점 상품권 판매업자 계좌로 200만원 송금 완료
6	15:36:52	상품권 수령자 서울 ○○점 현장 등장 확인됨
7	15:39:10	증권계좌→타행 대포통장으로 500만원 분산 송금 확인됨
8	15:42:31	필리핀 HSBC Quezon Ave ATM 93만원 인출 로그 발생
9	15:45:47	경기 지역 ATM 인출 시도 및 성공 로그 총 3건 확인됨
10	15:50:18	수사기관 수사 개시 전, 전체 피해금 대부분 현금화 완료됨

이처럼 피해자의 자금은 복수의 경로를 통해 짧은 시간 내에 분산·이체되며, 실시간으로 현금화된다. 이는 메신저피싱 범죄가 수사기관의 개입 이전에 사실상 완료되는 구조적 특성을 보여주는 사례이며, 다음 절에서는 이러한 시점에서 수사기관이 직면하게 되는 실무적 제약과 대응 방안을 고찰하고자 한다.

4.6. 범행 종료: 피해자 인지 전 자금 대부분 현금화

전체 범행은 약 5시간 이내에 신속하게 완료되었으며, 피해자가 범행 사실을 인지해 금융기관에 연락하기도 전에 대부분의 자금이 이미 현금화된 상태였다.

피해자는 공포감과 혼란 속에서 스마트폰을 초기화하고 경찰서를 방문하는 경우가 많아, 문자메시지, 인증번호 수신기록, 앱 설치 내역 등 핵심 디지털 증거가 소실되기 쉽다.

그 결과, 증권계좌 개설, 약관대출 실행, 가상자산 구매 및 송금 내역조차 인지하지 못한 채 진술하는 사례가 빈번하다.

이러한 구조적 한계를 고려할 때, 수사기관은 초동 단계에서 피해자의 디지털 흔적을 신속히 확보하고, 명의도용 여부 및 계좌 흐름 확인 등 매뉴얼화된 절차를 통해 증거 단절을 최소화할 필요가 있다.

V. 피의자 추적과 초국경 수사의 한계

본 연구에서 분석한 메신저피싱 사건은 작성자가 해당 사건의 신고 접수부터 피의자 특정 및 수사 종결까지의 전 과정을 직접 수사하며 확보한 실증 자료를 기반으로 한다.

본 장에서는 확보된 단서와 수사 진행 흐름을 구조화하여 정리하고, 그 과정에서 드러난 초국경적 수사의 구조적 한계를 함께 고찰하고자 한다.

5.1. 피의자 특정 경로 및 추적 흐름

메신저피싱 수사는 스마트폰 포렌식 분석, 입수된 문자메시지, 금융거래 내역 등을 통해 실행 단계별 단서를 확보하는 데서 시작된다.

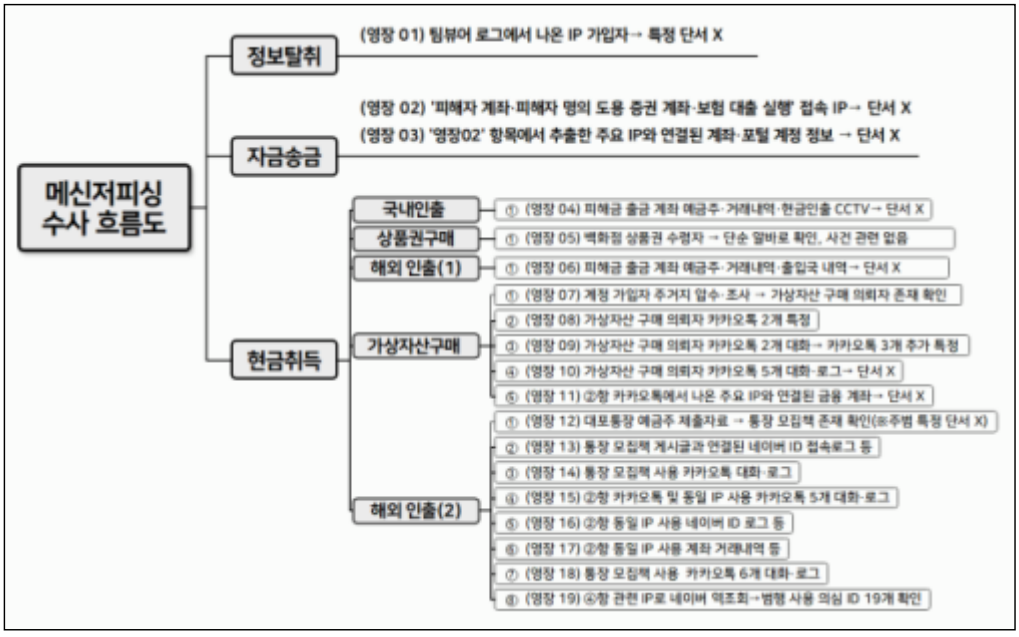
분석 결과, 범행은 ▲정보 탈취 ▲자금 송금(금융정보 확보 및 자금 송금) ▲현금 취득(국내외

현금화의 단계)으로 구분되며, 각 단계마다 실행 조직이 사전에 배치되어 있음을 확인할 수 있었다.

초기에는 피해자 스마트폰에 설치된 원격제어 앱(팀뷰어)을 통해 계정 접근과 자금 이체가 실행되었고, 이후 가상자산 거래소 및 백화점 상품권 환매, 해외 ATM 인출 등이 연쇄적으로 이루어졌다.

특히, 일부 자금은 필리핀 소재 ATM에서 수차례 인출되었고, 일부는 비트코인 계정으로 송금되며 실체 확인이 어려운 구조를 보였다.

그에 따라 수사기관은 계좌 거래내역, CCTV 자료, 모바일 메신저 접근기록 등 복합 자료를 수집하여 자금 흐름을 역추적하였으며, 본 논문에서는 이러한 수사 단서를 시각적으로 정리한 수사 흐름도를 함께 제시한다.



<Figure 4> 메신저피싱 사건 수사 흐름도

5.2. 수사의 구조적 한계

본 사건은 국내에서 실행되었으나, 범행 자금의 흐름이 해외로 확장되는 초국경적 특성을 보인다. 수사기관은 다양한 단서를 확보하였음에도 다음과 같은 구조적 제약에 직면하였다.

첫째, 피의자가 탈취한 자금은 최종 해외 가상자산 거래소로 송금되어 해당 자산의 흐름을 국내 수사기관이 실시간으로 추적하는 데에는 기술적·절차적 한계가 존재하였다.

둘째, 필리핀 등지의 해외 ATM을 통해 일부 자금이 인출된 정황은 포착되었으나, 인출에 사용된 계좌나 실행 인력의 구체적 신원은 확인에 어려움이 있었다.

셋째, 피의자가 사용한 접속 IP 주소는 대부분 해외 VPN 또는 가상 서버를 이용한 우회 접속 방식으로 확인되어, 실제 접속 위치를 특정하기 어려운 기술적 제약이 존재하였다.

넷째, 현장에 등장한 상품권 수령자, 국내외 ATM 인출자, 대포통장 명의자 등은 대부분 하부 실행 인력에 해당해, 이들과 조직 내부 총책 또는 기획 라인을 연결짓는 고리 확보에는 수사상 한계가 있었다.

다섯째, 전체 범행이 5시간 이내에 종결되는 고속 실행 구조였으며, 피해자는 범행 사실을 인지하기 전 대부분의 자금이 이미 현금화 또는 국외 송금된 상태였다. 특히, 피해자도 인지하지 못한 증권계좌를 경유한 자금 이동은 지급정지 요청 시점을 지연시키는 전략으로 활용되었다.

이와 같은 수사의 구조적 한계는 메신저피싱이 단순한 기술 기반 사기 유형을 넘어, 디지털 설계와 조직적 실행이 결합된 고도화된 범죄 공정임을 보여주는 대표적 사례라 할 수 있다.

이에 따라 다음 장에서는 이러한 한계를 실무적으로 보완하기 위한 수사 초기 대응 방안과 예방 전략을 종합적으로 제시하고자 한다.

Ⅵ. 예방 및 수사 실무 제언

메신저피싱 사건은 단시간 내 고도화된 절차로 이루어지며, 피해자가 범행 전개를 제대로 인지하지 못하는 사이 막대한 피해가 발생한다. 이러한 범죄에 대응하기 위해서는 피해 발생 초기 단계에서의 예방, 그리고 피해 발생 직후 수사기관의 체계적 조치가 병행되어야 한다.

본 장에서는 수사 실무에서 유용한 주요 점검사항을 기반으로 수사 초기 대응 매뉴얼과 확인 체계를 제안한다.

6.1. 피해자 명의로 개설된 신규 전화번호 확인

피의자는 인증번호 수신 및 모바일 OTP 발급을 위해 피해자 명의로 별도 휴대전화번호를 비대면 개통하는 경우가 많다. 피해자는 이 번호가 본인의 명의로 개설된 사실조차 인지하지 못하고 신고하는 경우가 대부분이다. 이로 인해 수사기관은 실사용 단말과 피의자 사용 단말을 구분하기 어려워진다. 이럴 때 '명의도용방지서비스(Msafer)'를 활용하면 피해자 명의로 개설된 모든 번호를 실시간으로 확인할 수 있다. 신규 번호를 조회하면 바로 확인되므로, 사전 확인 및 확대 방지에 매우 유효하다.

<Figure 5> 명의도용방지서비스(Msafer) 웹화면 (출처: msafer.or.kr)

6.2. 피해자 명의 증권계좌 개설 여부 확인

피해자는 대부분 본인의 명의로 개설된 증권계좌나 은행계좌가 있는지조차 알지 못한 채 신

고한다. 금융결제원의 '계좌정보통합관리서비스'를 활용하면 피해자 명의로 개설된 금융계좌를 통합적으로 조회할 수 있으며, 입출금 내역까지 수사 초기에 확인 가능하다.

특히 피해자가 모르는 상태에서 대출 실행이 이루어진 경우, 이 시스템을 통해 계좌 흐름을 추적하면 지급정지 결정 시점의 우선순위 판단에 큰 도움이 된다.

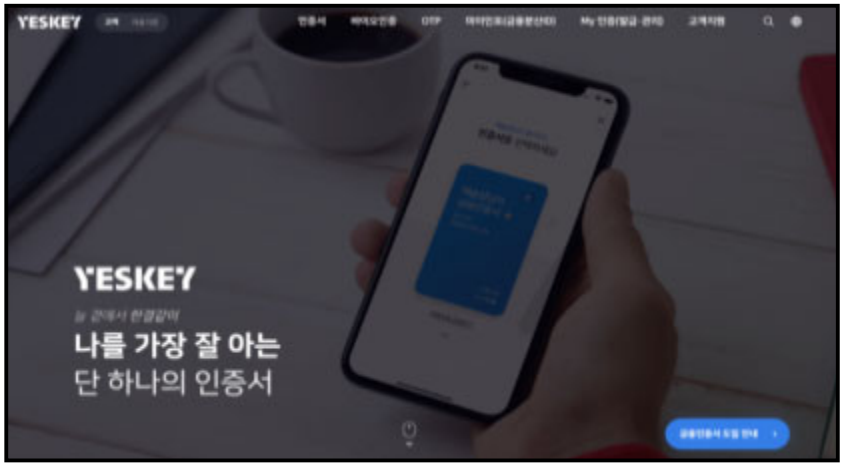
<Figure 6> 계좌정보통합관리서비스 웹화면 (출처: payinfo.or.kr)

6.3. 인증서 발급 이력 확인 및 접속 IP 추적

메신저피싱 범행에서는 피해자 명의로 공동인증서나 금융인증서가 추가 발급되는 경우가 많다. 보험사 앱, 증권사 등록 및 약관대출 실행 등 대부분의 절차에서 이 인증서가 필수로 요구된다.

금융결제원의 '금융인증센터'에서는 발급 시점의 IP 주소 및 단말기 정보까지 기록되므로, 피의자 특정의 핵심 디지털 단서로 활용 가능하다.

이 정보는 수사기관이 보유한 타 사건의 IP 주소, 기지국 접속 위치 정보 등과 교차 분석할 경우 피의자의 실질적 거주지 또는 인접 이동 경로를 파악하는 데 유용하다.



<Figure 7> 금융인증센터 웹화면 (출처: yeskey.or.kr)

6.4. 수사 실무자를 위한 통합 점검 매뉴얼 제안

사건 접수 단계에서 아래 세 가지 항목을 통합 점검 항목으로 설정하고 초기 수사과정에 반영하면, 메신저피싱 수사의 성과를 획기적으로 높일 수 있다.

<Table 7> 메신저피싱 사건 접수 시 통합 점검 항목 정리

구분	휴대전화 개통여부 (Msafer)	증권계좌 개설여부 (계좌통합조회)	인증서 발급여부 (금융인증센터)
시스템	한국정보통신진흥협회	금융결제원	금융결제원
주요 기능	실시간 명의 개통번호 확인	개설된 전체 계좌 조회	인증서 발급 시점, IP, 단말기 확인
수사 활용	번호 분산 여부 파악 및 차단	대포통장 경로 사전 탐지	피의자 특정 및 이력 추적 가능
예방 효과	명의 도용 방지 및 선제차단	자산 흐름 조기 인지	디지털 증거 확보 및 통합 수사 연계

6.5. 피해자 보호와 추가 피해 방지

사건 직후 피해자가 심리적 충격에 의해 스마트폰을 초기화하거나 주요 내용을 기억하지 못하는 사례가 많다. 수사기관은 이러한 상황을 대비해, 위에서 제시한 세 가지 시스템을 활용하여 피해자의 진술과 사실을 교차 확인해야 한다.

또한 경찰관 또는 수사관이 피해자의 진술로만 수사 경로를 판단하지 않도록 하고, 수사 초기부터 객관적인 로그 자료와 기관 기반 조회 시스템을 적극 활용해야 한다.

VII. 결론

본 연구는 메신저피싱 범죄의 실질적 전개 과정을 시간순으로 재구성하고, 사건 접수 초기부터 범행 완료 시점까지 수사 실무자가 마주하게 되는 주요 단서와 판단 포인트를 입체적으로 분석하였다. 메신저피싱은 단순한 '자녀 사칭' 단계에서 출발하지만, 이후 스마트폰 원격조작, OTP 및 인증서 탈취, 증권계좌 개설, 보험대출 실행, 자금 분산 및 국내외 인출에 이르는 다단계·조직적 금융범죄로 진화하고 있다.

특히 본 사례에서는 피해자가 범행을 인지하기 전 이미 자금 대부분이 실시간으로 현금화되었고, 일부 자금은 피해자조차 인지하지 못한 명의 계좌를 경유해 이동되었다. 이는 수사 초기의 판단 미흡이 치명적 피해로 직결될 수 있음을 상징적으로 보여주는 사례이다.

또한, 피의자 추적 과정에서 드러난 다양한 수사의 한계 역시 주목할 필요가 있다. 피의자는 해외 가상자산 거래소와 VPN, 대포통장, 실행 인력을 조직적으로 활용하였으며, 전체 범행이 약 5시간 내에 종결되는 고속 구조를 띠었다. 이로 인해 수사기관은 충분한 의지와 수사력을 투입하였음에도 불구하고 실질적인 피의자 특정이나 총책 추적에 한계를 경험하였다. 이는 메신저피싱이 단순한 기술 기반 사기가 아니라, 구조화된 디지털 범죄 공정(process)임을 보여주는 대표 사례라 할 수 있다.

이러한 범죄에 효과적으로 대응하기 위해서는 다음과 같은 인식 전환과 실무적 조치가 병행되어야 한다.

첫째, 메신저피싱은 '심리적으로 설계된 언어'와 '기술적으로 고도화된 실행 구조'가 결합된

복합 범죄로, 수사 실무에서도 단순 문자 사칭이 아닌 조직형 디지털 범죄로 인식되어야 한다.

둘째, 피해자의 스마트폰 초기화로 인한 디지털 증거 단절을 예방하기 위해, 사건 접수 초기부터 휴대전화 개통 여부, 계좌 개설 여부, 인증서 발급 여부 등을 통합적으로 점검할 수 있는 수사 매뉴얼이 필요하다.

셋째, 금융결제원, 한국정보통신진흥협회 등에서 제공하는 공공 인증 시스템과 계좌 통합조회 서비스는 단순 조회를 넘어, 디지털 단서 확보를 위한 핵심 수사 도구로 적극 활용되어야 한다.

넷째, 메신저피싱은 사칭, 인증, 자금 회수 등 역할이 분화된 조직적 실행 구조에 기반하므로, 이에 걸맞는 수사 역량과 부서 간 협업 체계, 제도적 대응 시스템이 함께 구축되어야 한다.

본 논문은 메신저피싱 사건을 수사 실무 관점에서 구조화하고, 실제 수사에 적용 가능한 예방·대응 전략을 제시함으로써, 향후 유사 사건 발생 시 수사 초기 대응력 향상과 피해 저감에 실질적으로 기여할 수 있을 것으로 기대된다.

참고문헌 (References)

[1] Jung J, Chang J, Suh JB. 2022. The current situation and problems of messenger phishing and measures to address it. Korean Security Journal, 72, 49-70. https://doi.org/10.36623/KSSR.2022.72.3

[2] Nam S, Lee H, Lee S. 2022. A study on countermeasures through messenger phishing experience analysis. Journal of The Korea Institute of Information Security and Cryptology, 32(5), 791-805. http://doi.org/10.13089/JKIISC.2022.32.5.791

[3] Choi YJ, Choi SW. 2021. Messenger phishing modus operandi in South Korea. Journal of Korean Public Police and Security Studies, 18(3), 241-258. http://doi.org/10.25023/kapsa.18.3.202108.241

[4] Jung YH, Ha HJ. 2022. Messenger phishing crime: Trends and responses. Criminal Investigation Studies, 8(1), 31-54. http://doi.org/10.46225/CIS.2022.6.8.1.31

[5] Financial Supervisory Service. 2021. Statistical analysis report on voice phishing damage. Financial Supervisory Service, Seoul, Korea.

[6] Korea Financial Telecommunications and Clearings Institute. 2022. Service and usage guide of the account information integrated management system. Korea Financial Telecommunications and Clearings Institute, Seoul, Korea.

[7] Ministry of Justice. 2020. Legal response study on telecommunications financial fraud. Ministry of Justice, Gwacheon, Korea.

[8] Korea Institute of Criminology and Justice. 2021. Improvement measures for the legal system on phishing crimes. Korea Institute of Criminology and Justice, Seoul, Korea.