2026.03.23.

KiRi 리포트

미국 인터넷 범죄 동향과 보험산업의 대응

| 글로벌 이슈 |

김혜란 연구원

요 약

미국 인터넷 범죄 피해 규모가 2024년 사상 최고치를 기록한 가운데, 인터넷 범죄 유형이 전통적인 해킹·랜섬웨어 중심의 사이버 공격에서 금융 관련 사이버 사기로 이동하고 있음. 특히, 60대 이상 고령자를 대상으로 하는 자산 탈취 범죄와 암호화폐를 매개로 한 범죄가 급증하고 있음. 이러한 변화에 대해 보험회사는 사이버 보험 특약 확대, 약관 내 하위 한도설정 또는 면책조항으로 대응하고 있음

○ 디지털 전환이 가속화되면서 미국 내 인터넷 범죄 피해 규모는 2024년에 사상 최고치를 기록함[1)]

- 2024년 인터넷 범죄 신고 건수는 859,532건에 달했으며, 총 피해액은 전년 대비 33% 증가한 166억 달러로 역대 최대 수준임
- 최근 5년간 신고 건수는 연평균 약 83만 건으로 완만한 증가세를 보였으나, 피해액은 급격히 확대됨
  - 2020년 약 41억 달러였던 피해액은 2024년 166억 달러로 4배 이상 증가하였으며, 이는 범죄 빈도보다 건당 피해 규모가 급격히 확대되고 있음을 의미함

○ 인터넷 범죄 유형은 전통적인 해킹·랜섬웨어 중심의 사이버 공격에서 금융 관련 사이버 사기로 이동하고 있음

- 2024년 사이버 공격 신고는 약 26만 건, 피해액은 약 15.7억 달러로 집계됨
  - 사이버 공격이란 시스템 마비, 데이터 탈취 등을 목적으로 하는 기술적 침해 행위로 핵심인프라 부문에서 4,800건 이상의 공격이 발생했으며, 주로 랜섬웨어와 데이터 유출 중심이었음
- 반면, 같은 기간 금융 관련 사이버 사기는 약 33만 건이 보고되었으며, 피해액은 137억 달러로 전체 피해액의 83%를 차지함
  - 금융 관련 사이버 사기는 인터넷이나 디지털 기술을 활용해 금전, 데이터, 신원 정보 등을 탈취하거나 위조 상품·서비스를 만들어 내는 방식으로 이루어짐
  - 피해액 기준으로는 투자사기(65.7억 달러)가 가장 많고, 기업 이메일 침해(27.7억 달러), 기술지원 사기(14.6억 달러), 개인정보 침해(14.5억 달러) 순임
- 특히 투자사기는 최근 3년간 급격히 증가하였으며, 전통적 인터넷 범죄인 랜섬웨어의 피해액은 감소하는 것을 볼 때 범죄 유형이 변화하는 특징이 있음
  - 투자사기는 2022년 30,529건(33.1억 달러)에서 2024년 47,919건(65.7억 달러)으로 피해액이 2배 이상 확대됨
  - 동기간 랜섬웨어는 2,385건(3,400만 달러)에서 3,156건(1,200만 달러)으로 건수는 증가하였으나 피해액은 감소함

1) Internet Crime Complaint Center(2024), "IC3 Annual Report"

〈그림 1〉 미국 인터넷 범죄 신고 건수 및 피해액 추이(2020~2024년)〈그림 2〉 미국 연령별 인터넷 범죄 신고 건수 및 피해액(2024년)

자료: IC3(2024), "IC3 Annual Report"를 바탕으로 저자가 작성함 자료: IC3(2024), "IC3 Annual Report"를 바탕으로 저자가 작성함

○ 60대 이상 고령층을 대상으로 하는 자산 탈취 범죄가 빠르게 증가하고 있으며, 암호화폐를 매개로 한 범죄도 급증하고 있음

- 2024년 60세 이상 신고 건수는 147,127건, 피해액은 약 48억 달러로 전체 연령대 중 고령층은 신고 건수의 27%, 피해액의 42%를 차지함
  - 이는 전년 대비 신고 건수는 46%, 피해액은 43% 증가한 수치임
  - 최근에는 현금 송금을 유도하는 기술지원 사기, 가족의 위기를 가장한 음성 기반 금융 사기 등이 고령층을 대상으로 확산됨
- 암호화폐를 매개로 한 범죄 피해액은 약 93억 달러에 달하며, 이 중 60세 이상 고령층의 피해액이 30%를 넘음
  - 암호화폐는 투자 사기·로맨스 사기·피싱 등과 결합하여 피해액이 확대되고 있는데, 특히 고령층에서 암호화폐 관련 손실만 28억 달러를 초과하여 이는 연금 및 은퇴자산 보호와 직결되는 문제로 볼 수 있음
- 또한 자금이 국경을 초월하여 이동하는 특성이 강화되고 있음
  - 2024년 기준 200개 이상 국가에서 신고가 접수되었으며, 주요 해외 송금 목적지는 홍콩, 베트남, 멕시코 등임

○ 이러한 인터넷 범죄에 대해 일부 보험회사는 사이버 보험에 AI 기반 신원 사칭 등에 대한 보장을 특약으로 추가하는 반면, 일부 보험회사는 약관 내 하위 한도를 설정하거나 면책조항을 도입함[2)]

- 의료 및 금융서비스 분야의 데이터 보호법은 기업들이 위험관리 전략에 사이버 보험을 포함하도록 유도하고 있음[3)]
- 미국 인슈어테크 기업 Coalition은 2025년 12월 딥페이크로 인한 피해 발생 시 대응 및 복구 비용을 보장하는 딥페이크 대응 보증 조항을 사이버 보험에 추가함[4)]
- 코로나19 이후 랜섬웨어 공격이 급증하자 보험회사는 보험료를 대폭 인상하고, 자기부담금 상향, 약관 내 하위 한도(Sub-limit)를 설정하는 등 조건을 강화하였으며, 그 결과 인수 심사 절차가 개선되고, 사이버 보안 수준도 향상됨
- 일부 보험회사는 보안 유지 의무 불이행 또는 준수 의무 위반을 사이버 보험 면책조항에 포함하여, 피보험자가 최소한의 보안 기준을 유지하지 못한 경우 발생한 손해에 대해서는 보장을 배제하기도 함

2) NAIC(2024. 10. 15.), "Report on the Cyber Insurance Market"
3) Reinsurance News(2025. 7. 9.), "AM Best maintains stable outlook for global cyber insurance in 2025 amid growth, AI, and rising threats"
4) Coalition(2025. 12. 9.), "Coalition Adds Deepfake Response Endorsement to its Cyber Insurance Policies Globally"