

치안정책리뷰

POLICE SCIENCE INSTITUTE REVIEW

발행인 최종상 편집인 김영수 전화 041-968-2794 FAX 041-968-2989

AI 분석 기술을 활용한 연구·수사기관의 전화금융사기(보이스피싱) 수사기법 개발 연구

권 두 언

보이스피싱 범죄, 데이터 기반 수사정보분석의 중요성
-초임 경제팀 수사관의 열정이 만들어낸 작은 기적-

경찰대학 경찰학과
김 지 온 교수

전문가 제언

자연어처리 딥러닝 모델을 활용한 보이스피싱 범죄
수사기법

치안정책연구소 범죄수사연구실
김 혜 진 실장

보이스피싱 범죄 해결을 위해 연구되고 있는 과학기술

치안정책연구소 스마트치안지능센터
장 광 호 경정
김 희 두 경위
김 창 식 경사
최 주 현 경장

보이스피싱 대응과 피해자 구제

동국대학교 국제정보보호대학원
황 석 진 교수

자유기고

모바일 등 디지털 문서에 대한 위조 및 행사혐의에
대한 대법원 법리 적절성 검토
-디지털시대 형법상 위조 혐의 문제점 검토 중심으로-

12사단 군사경찰대대
김 호 군사경찰대대장

연구소 소식



경찰대학
KOREAN NATIONAL POLICE UNIVERSITY



Total Solutions in Policing

치안정책연구소

보이스피싱 범죄, 데이터 기반 수사정보분석의 중요성

- 초임 경제팀 수사관의 열정이 만들어낸 작은 기적 -

김 지 온

경찰대학 경찰학과 교수

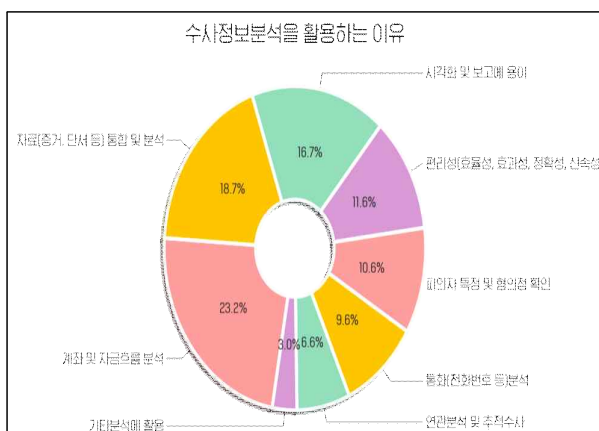


서론

제작년 그러니까 2021년 초가을쯤이었던 것으로 기억한다. 경찰대학 37기 졸업생에게 연락이 왔다. 그해 4월에 경제팀에 발령을 받고 다른 팀원에게 인계받은 보이스피싱 사건을 어떻게 수사를 진행해야 할지 몰라 방치하고 있었는데 이제 제대로 수사를 해보고 싶다는 것이었다. 사건 수사의 첫 단추를 풀기 위한 관건은 보이스피싱 사기범들과 대포통장 명의자 사이의 의심되는 연관관계를 찾는 것이었다. 그리고 이를 위해 필연적으로 진행해야 하는 절차가 보이스피싱 관련자들의 통화내역과 계좌내역을 분석해야 하는 데이터 기반의 수사정보분석이었다. ‘수사정보분석’이란 통신자료 등 수사과정에서 수집되는 다양한 유형의 수사자료를 분석하는 행위를 말한다(김지온, 2019).

실제 약 335명의 경찰청 소속 수사관들을 대상으로 설문조사를 진행한 결과 약 33%의 응답자가 통화/계좌내역 분석을 위해 수사정보분석을 진행한다고 응답하였다(김지온·우병관, 2022).

<그림 1> 수사정보분석을 활용하는 이유



또한 가장 많이 활용하는 프로그램은 데이터 간 연관관계를 네트워크 형태로 효과적으로 시각화 해주는 i2(information image)라고 답변하였다.

범행을 부인하고 있는 대포통장 명의자들이 실제 보이스피싱 범죄에 관여되어 있다는 사실을 밝히기 위해 대용량 디지털 데이터에 대한 수사정보분석은 이제 선택이 아닌 필수가 되었다. 중고차 딜러를 사칭해 피해자로부터 금원을 편취한 보이스피싱 조직범죄 사건에서 수사정보분석이 어떻게 사건 해결의 실마리를 제공할 수 있었는지 지금부터 알아보도록 하자.

사건 개요

본 사건 보이스피싱 범죄조직은 중고차를 팔려고 인터넷 거래 사이트에 매물을 올리는 사람들에게 ‘원하는대로 값을 쳐주겠다’고 접근하였다.

자동차 매도자에게는 자동차 세금과 보험료를 달내기 위해 약 2,300만원으로 다운계약서를 작성하면 실제로는 3,100만원을 주겠다고 속이고, 이러한 사정을 전혀 알지 못하는 자동차 딜러에게는 매도자의 지인을 사칭하여 매도자가 2,300만원이라는 잔값에 중고차를 판매하려고 한다고 양쪽으로 거짓말을 하였다.

범인들은 범행이 들통날 것을 염려해 매도자에게는 자동차 딜러는 다운계약서에 대해 전혀 모르기 때문에 그런말을 해서는 안된다며 입막음을 시키기도 하였다.

거래가 끝나면 피해자에게 연락하여 딜러가 차값으로 보내준 돈을 보내면 약속한 금액을 송금해주겠다고 속이고 돈만 챙겨 잠적하는 수법으로 전국 피해자 21명에게 약 5억원의 사기행각을 벌였다.

데이터 기반 수사정보분석

담당 수사관은 대출을 받기 위해서 통장과 접근체체를 양도하였을 뿐이라고 변명하고 있는 본건 사기 범행에 이용된 통장 명의자 3명이 실제 보이스피싱 범죄에 관여되어 있을 것이라고 의심하였다.

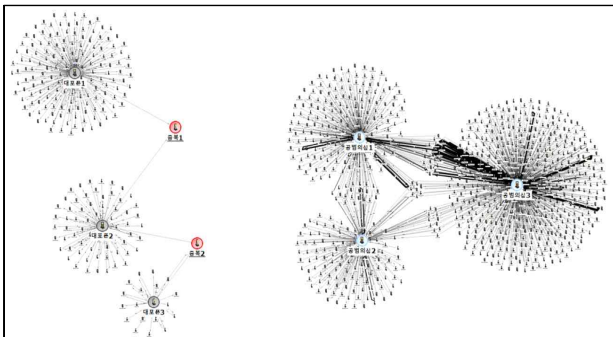
추가 수사를 진행할 수 있는 의심점을 찾기위해 보이스피싱 범죄에 이용된 대포폰 3대와 위 공범의심자 3명의 휴대전화 3대의 통화내역상 연관관계에 대한 분석과 대상자들 명의의 5개 계좌에 대한 분석을 의뢰하였다.

<표 1> 분석대상 수사정보

통신정보	- 대포폰 1 : 010-210-1800, 대포폰 2 : 010-00-5800 (각각 2021. 3. 30. ~ 7. 30.) - 대포폰 3 : 010-800-4500 (2021. 4. 13. ~ 5. 14.) - 임○○ : 010-00-1700, 이○○ : 010-00-4000, 왕○○ : 010-00-6900 (각각 2021. 2. 28. ~ 8. 31. 6개월간)
계좌정보	- 이○○ (카뱅) 3300813 (2021. 3. 1. ~ 4. 13. 거래내역) - 임○○ (카뱅) 33008103, (기업) 339001017 - 왕○○ (카뱅) 94002469, (농협) 351002593 ※ 임○○, 왕○○ 각각 2021. 1. 1. ~ 8. 27. 거래내역

먼저 본건 보이스피싱 공범 혐의자인 임○○, 이○○, 왕○○의 통화네트워크(1집단)와 주범들이 피해자와 참고인에게 사기전화를 걸 때 사용한 대포폰 3대(2집단)의 연관관계를 ‘발신번호-착신번호’ 간의 일원 연결망(1-mode network) 네트워크로 시각화하고 스펀문자 등 명백하게 사건 관련성이 없는 전화번호를 삭제한 결과 아래와 같이 두 집단의 연관관계는 나타나지 않았다.

<그림 2> 1, 2 집단 간 ‘발신번호-착신번호’ 연결망

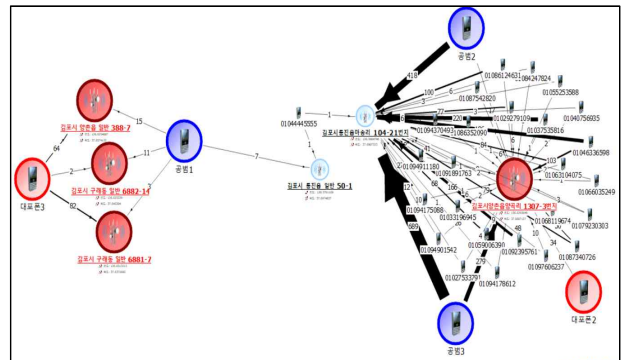


1) 한가지 유형의 노드 간의 관계로 구성된 연결망으로 네트워크의 구조적 분석에 유리하다.

두 개 집단이 서로 연결되지 않는다는 것은 공범 혐의자들이 실제 사기 주범들과 직접적인 통화는 하지 않았다는 사실을 뒷받침한다.

그래서 다음단계로 1집단과 2집단의 위치적 연관성을 살펴보기 위해 ‘발신번호-발신기지국’ 간의 이원 연결망(2-mode network)을 아래와 같이 시각화 하였다.

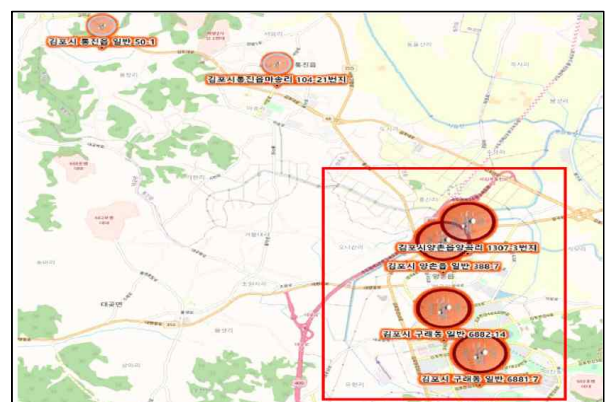
<그림 3> 1, 2 집단 간 ‘발신번호-발신기지국’ 연결망



그 결과 1 집단 공범혐의자들과 2 집단 보이스피싱 주범들이 모두 접속한 김포시 구래동과 양촌읍 소재 휴대전화 기지국 4개소를 확인할 수 있었다.

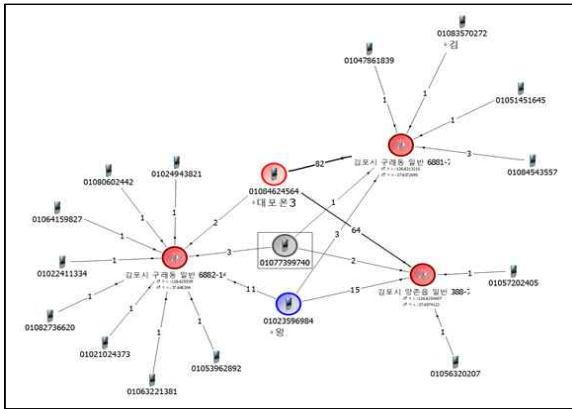
공범혐의자 3명의 주거지가 김포시 통진읍 일대인 것으로 볼 때 김포시 구래동과 양촌읍에 본건 보이스피싱 사기조직의 은신처나 사무실이 있을 것으로 의심되었다.

<그림 4> 보이스피싱 사기조직 사무실 추정장소



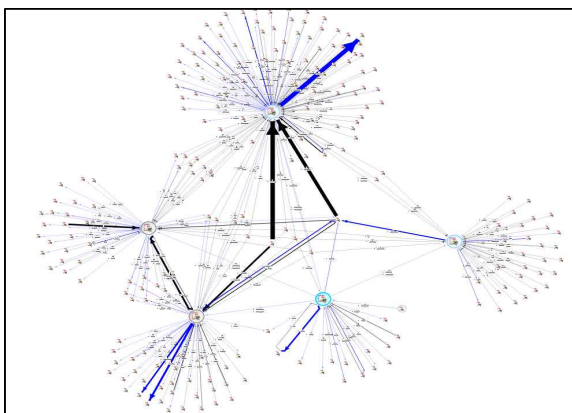
수사기관의 보이스피싱 사무실 추적을 돕기 위해 위 의심지역 기지국에서 전화를 사용한 다른 의심번호도 아래와 같이 추출할 수 있었다.

<그림 5> 보이스피싱 공범 의심번호 추출 결과



다음으로 1 집단 공범의심자 3명의 자금흐름을 분석하기 위한 계좌 5개의 거래 네트워크를 시각화한 결과는 다음과 같다.

<그림 6> 1집단 계좌거래 네트워크 시각화 결과



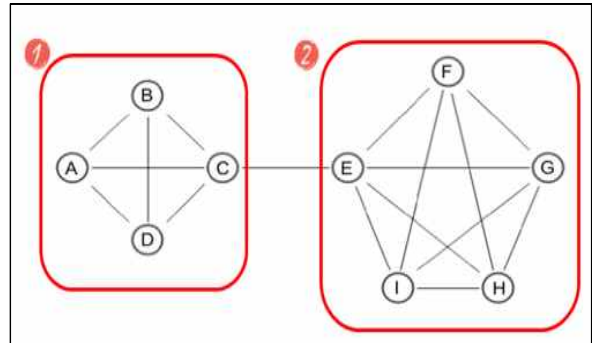
위 계좌거래 중 1집단 공범의심자들이 사용한 다수의 계좌와 거래가 있는 의심계좌를 도출하기 위해 사회연결망분석 원리 중 하위집단(cohesive subgroup) 분석원리를 활용하였다.

i2에서 제공하는 하위집단 분석원리 중 클러스터 찾기 기능을 활용하였는데, 클러스터 찾기 기능의 경우, 하나의 네트워크 집단을 두 개의 다른 집단으로 분할하기 위해 삭제해야 할 링크의 개수를 의미하는 링크 연결성 단계를 기반으로 하위집단을 추출한다.

아래 <그림7>을 기준으로 설명한다면, A, B, C, D 그룹(1그룹)은 연결성 단계가 3이고, E, F, G, H, I 그

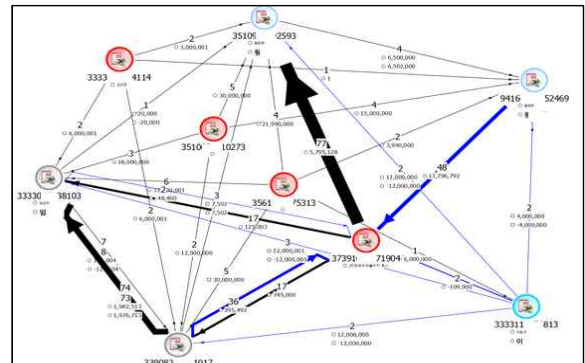
룹(2그룹)은 연결성 단계가 4이다. 만약 연결성 단계 임계값이 3으로 지정되면 1, 2 그룹이 모두 식별되고, 연결성 단계 임계값이 4로 지정되면 2그룹만 식별되게 된다.

<그림 7> 클러스터 찾기 원리



<그림6>의 계좌네트워크의 하위집단을 도출한 결과 추가 수사가 필요한 혐의 계좌는 아래와 같이 약 4개의 노드(빨간색 프레임)가 확인되었다.

<그림 8> 계좌거래 네트워크 하위집단 추출결과



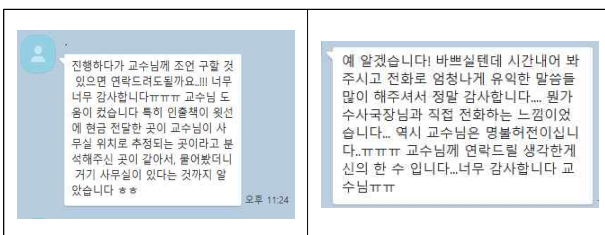
위와 같이 보이스피싱 범죄발생 초기에 수집되는 통화, 계좌내역 등 다양한 디지털 정보 간 연관관계를 효과적으로 분석하면 답보상태에 빠진 사건에 대한 추가 수사를 진행할 수 있는 실마리나 새로운 범죄 혐의점을 찾아낼 수 있다.

결론

필자가 분석 결과를 회신해준 이후 몇 개월이 지나

담당 수사관에게 연락이 왔다. 본건 보이스피싱 범죄 인출책이 뒷선에 현금을 전달한 장소가 <그림4>의 사무실 추정 위치와 같았고 인출책을 대상으로 이를 추궁하여 자백을 받았다는 것이었다. 이들은 수사기관의 검거를 피하기 위해 사기 전화는 그때그때 호텔을 변경해가며 이용하였고, 수익금을 인출하여 분배하고 범죄를 공모하는 장소로 총책의 은신처를 활용하였는데 그 장소가 바로 <그림4>에서 추천한 김포시 구래동 일대에 위치하고 있었다.

<그림9> 담당수사관이 필자에게 보낸 카카오톡 메시지



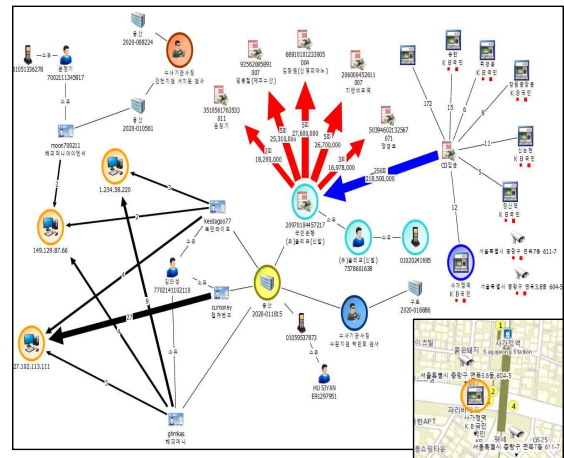
결국 사건 수사가 확대되어 해당 경찰서에서는 전담 수사반을 꾸리게 되었고, 약 1년여간의 수사 끝에 본건 보이스피싱 사기범들 12명을 검거하여 사건을 해결할 수 있었다.

시도 경찰청도 아닌 민원사건이 많은 경찰서에서 보이스피싱 범죄를 제대로 수사한다는 것은 결코 쉬운 일이 아니다.

본 사건은 초임 수사관의 열정과 이를 뒷받침해준 데이터사이언스 기반의 수사정보분석이 만들어낸 그야말로 작은 기적이었다.

현재 정보통신기술기반의 조직범죄를 효과적으로 분석하기 위해 일부 시도청에서는 아래와 같이 연관관계 기반의 데이터베이스를 구축하여 대용량 수사정보간의 연관관계를 신속·정확하게 분석해 나가고 있다.

<그림10> 데이터베이스 기반 수사정보분석 예



이러한 분석에는 가설적추론, 사회연결망분석, 공간 분석, 그래프 데이터베이스 방법론 등이 적용되며 관련 연구도 확대되고 있다. 최근에는 AI를 적용한 자연어처리 기술도 수사에 접목되고 있는 등 치안 데이터 사이언스 분야가 더욱 발전하고 있다.

4차 산업혁명 시대 초연결 위험사회에 급변하는 범죄에 대응하기 위해 수사기관도 과학치안에 대한 연구와 투자를 늘려야 한다.

아울러 수사의 완성은 언제나 사람이듯이 결국 중요한 것은 과학치안 전문가를 양성하고 그들이 활약할 수 있는 조직과 무대를 만들어 주는 것이다. 이를 위해 경찰은 직급 중심의 관료사회에서 직위 중심의 전문가 조직으로 거듭나야 한다. 전문가가 존중받는 문화는 경찰이 인재가 떠나는 조직이 아닌 인재가 모여드는 조직으로 변모하는데 가장 중요한 밑거름이 될 것이다.^[PSI]

< 참고문헌 >

- 1) 김지은 (2019). 사회연결망 분석원리의 범죄 수사상 활용방안에 관한 연구. *디지털포렌식연구*, 13(2), 87-107.
- 2) 김지은, 우병관 (2022. 7.). 사이버탐지 및 분석기술에 대한 탐색적 연구. *한국치안행정논집*, 19(3), 57-76
- 3) 박노섭, 김지은[†], 김창식, 박성미 (2020). 범죄수사 검증모델과 시각화 방안에 대한 연구. *경찰법연구*, 19(4), 9-36.
- 4) 강정환, 김지은(2021). 사이버위협범죄 연결망분석 기법에 대한 연구. 연세대학교 산학협력단.

자연어처리 딥러닝 모델을 활용한 보이스피싱 범죄 수사기법 연구

김 혜 진

경찰대학 치안정책연구소 범죄수사연구실장



서 론

어눌한 한국어 억양을 가진 범죄자에 의한 우스꽝스러운 사기라는 세간의 가벼운 인식과 달리, 보이스피싱은 막대한 규모의 경제적 손실과 심각한 인명피해를 발생시키는 중범죄이다. 경찰청 통계에 따르면, 2006년 100억원 수준이었던 보이스피싱 피해 금액은 2011년 1,000억원 수준으로 10배 넘게 급증했고, 2017년에는 2,500억, 최근인 2020년에는 7,000억을 기록해 역대 최고 수준의 피해 규모를 보였다. 또 다른 관계부처인 금융감독원의 통계에 따르면, 2016년 45,921건이었던 전기통신금융사기의 발생 건수가 2019년에는 72,488건으로 무려 57% 증가했음을 확인할 수 있다. 2021년 코로나-19의 확산과 강력한 사회적 거리 두기 정책의 시행으로 인해 비대면 활동, 온라인 범죄가 함께 증가하면서 보이스피싱 범죄의 확산과 수법의 교묘함 또한 심화되고 있는 실정이다.

금융사기범죄의 경우, ‘치고 빠지기’ 전략을 구사하기 위해 범죄자들이 철저하게 점조직의 형태로 활동하기 때문에, 빠르고 일관성 있는 수사 데이터베이스의 구축이 필수적이다. 통상적으로 보이스피싱 조직은 중국에서 활동하는 중앙총책을 중심으로 전산기술팀, 텔레마케터팀, 대포통장팀, 대본팀, 현금인출팀, 송금팀으로 구성되는데, 총괄자를 제외한 팀 간 정보공유가 철저히 차단되어 있어 조직원 중 일부를 검거하더라도 공범을 검거하기 위해서는 범행 수법과 피해자 유형 등 세부내역을 교차 검토해 구성원 간의 연결점을 파악해야 한다. 더불어 전국에서 발생하고 있는 사건들 중 동일 범죄조직에 의한 소행임을 파악하는 여죄 추정 과정에서 사건에 대한 상세 정보는 반드시 필요한 자료라 할 수 있다. 피의자 검거에 유용하다는 이점에서 한발 더 나아가, 범죄 피해자 특성

정보(연령, 성별과 같은 인구통계학적 정보, 거주지와 같은 지리 정보)를 대량으로 수집하는 기술이 있을 경우, 잠재적 피해대상과 범죄 발생 다발 지역을 세부적으로 특정할 수 있어 보이스피싱 범죄 예방 활동에도 큰 도움을 기대할 수 있다.

본 연구에서는 경찰청에서 그동안 수기로 작성했던 보이스피싱 범죄 DB의 자동 구축을 위해 자연어처리 딥러닝 모델을 개발하였다. 구체적으로 피해자 진술조서에서 3가지 유형의 정보(사건정보, 수사기관정보, 피해자정보)를 자동으로 인식, 추출하는 것을 목표로 하였다. 이후 완성된 자연어처리 모델을 실제 범죄 데이터에 적용하여 결과물의 정확도를 평가하고, 정확도 향상을 위한 개선사항을 파악하였다. 이러한 자연어처리 인공지능 모델 연구는 수사자료의 시의성 있는 활용에서 더 나아가, 해당 범죄로 인해 촉발된 각종 불필요한 사회적 비용(보이스피싱 범죄 불안감에서 촉발된 금융 산업에 대한 시민들의 불신, 정부와 통신기업들이 범죄예방을 위해 사용하는 직간접적인 비용과 시간 등)을 경감시키는데 중요한 역할을 할 수 있을 것으로 예측된다.

연구방법

본 연구는 그동안 수기로 작성되어 정확성과 신속성을 담보하기 어려웠던 경찰청 보이스피싱 사건자료의 한계점을 인식하고, 텍스트화된 수사 정보를 자동 수집하는 자연어처리 인공지능 모델을 실험적으로 개발함으로써, 실무현장에서 활용할 수 있는 프로그램과 연구방법론을 제안하고자 한다. 구체적인 방법론은 다음과 같다. 첫째, 수사자료 보안을 위해 PDF(Portable Document Format) 형식으로 저장된 진술조서 문치들을 이미지 파일로 일괄 변환하고, 해당 이미지를 광학

문자 인식(Optical Character Recognition; OCR) 엔진을 통해 기계가 인식할 수 있는 텍스트로 변환한다.

둘째, 정보 처리 및 수집의 효율성 향상을 위해 보이스피싱 피해자 진술조서를 ① 피해자·접수정보 영역과 ② 사건정보 영역으로 구분한다. 셋째, 자연어처리 기술을 활용하여 앞서 분리된 진술조서의 피해자·접수정보 영역에서 각 5종의 피해자 정보(피해자 성명, 피해자 전화번호, 피해자 주민번호, 피해자 직업, 피해자 주거지)와 2종의 접수정보(사건접수번호, 사건접수관서)를 추출한다.

넷째, 개체명 인식 학습을 통해 완성된 인공지능-사전 모델을 기반으로 진술조서의 사건정보 영역에서 7종의 사건정보(범행 수법, 피해 금액, 범죄사용번호, 사칭기관, 사칭인물, 특이사항, SNS유형)를 추출한다. 마지막으로 최종 추출된 14종의 사건정보, 수사기관 정보, 그리고 피해자 정보들의 정확도를 평가하고, 완성된 인공지능 모델의 개선사항에 대해 논의하도록 한다.

연구결과

데이터의 전처리 작업을 통해 피해자 진술조서 텍스트의 기본 정제를 완료한 후, 보이스피싱 범죄조직이 사칭한 기관과 인물 정보를 자동 인식하기 위해 학습한 KO-BERT 모델의 성능을 한국어해양대학교 개체명 데이터 검증 셋(n=931)을 통해 사전 평가했다. 평가지표로 정밀도(Precision)¹⁾, 재현율(Recall)²⁾, F1-Score³⁾를 사용하였다. 분류하고자 한 태깅 셋 중 사칭 인물(PER)은 F-1 Score가 .95와 .94로 상당히 높았고, 사칭 기관(ORG)은 F-1 Score가 .89와 .88로 산출되어 인물 태깅보다는 상대적으로 낮았지만, 객관적

1) 정밀도(Precision) $p = \frac{TP}{TP+FP}$, 해당 수식에서 TP는 True Positive, TF는 False Postive, FT는 False Negative, FF는 True Negative 를 의미

2) 재현율(Recall) $r = \frac{TP}{TP+FN}$

3) F1- Score = $2 * \frac{p * r}{p + r}$, Precision과 Recall의 조화평균으로 값이 높을수록 성능이 높음

인 정확도 수치가 상당히 높은 것으로 평가되었다.

완성된 딥러닝 모델과 사전·규칙기반의 자연어처리 모델을 통합적으로 프로그래밍하여 서울경찰청에서 제공한 100건의 실제 피해자 진술조서에 적용하였을 때 추출된 정보의 정확도또한 높은 수준의 성능을 보였다. 범죄조직이 사칭한 인물의 인식 정확도는 .80(100건 중 80건의 진술조서에서 정확한 정보를 추출)로, 검증 셋에 비해 성능이 일부 약화 된 것을 확인할 수 있었으나, 범죄조직이 사칭한 기관의 인식 정확도는 .94로 검증 셋에서의 정확도와 유사한 것을 알 수 있다. 그 외 수사 정보 항목들은 사전·규칙기반의 자연어처리 모델을 적용하여 피해 금액을 제외한 모든 항목에서 .90 이상의 성공적인 정보 추출율을 보였다.

연번	사칭인물	사칭기관	SNS	특이점	원금금액	범죄사용번호	접수번호	접수 경찰서	피해자 이름	피해자 주민등록번호	피해자 직업	피해자 전화번호	피해자 주
1	김복자	씨티은행	카카오톡		5000000	010	2021-02	중부서	김복자	31-12	대리사	010	
2	이준진	강북경찰서 금융감독원 동양지점			580000		2021-05	영동서	이준진	31-12	회사원	010	
3	이준수	씨티은행	카카오톡		1400000		2021-05	중부서	이준수	31-12	보통직업	010	
4	이준서	롯데캐피탈 기업은행 우리카드은행	카카오톡		6000000	010	2021-04	노원서	이준서	31-12	전직업	010	
5	이준형	중앙직업 신한은행	카카오톡	상용권	5400000	010	2021-04	중부서	이준형	31-12	회사원	010	
6	유민준	중앙직업 우리카드은행	카카오톡		3000000	010	2021-02	중부서	유민준	31-12	공무원	010	
7	정현영	신한은행			1400000		2021-05	강서서	정현영	31-12	무직	010	
8	정현우	토트캐피탈 씨티은행 신한캐피탈은행			1200000	010	2021-03	성동서	정현우	31-12	회사원	010	
9	이승현	세아금융고 현대카드 금융감독원	카카오톡		7000000	010	2021-02	송파서	이승현	31-12	보통직업	010	
10	정지민	국민카드 우리카드 국민은행 우리은행			6000000		2021-05	강동서	정지민	31-12	무직	010	
11	정지민	국민카드 우리카드 국민은행 우리은행			1400000	010	31-12	도봉서	정지민	31-12	무직	010	
12	정지민	신한은행 중앙 직할업 우리카드은행			2500000	010	2021-04	중부서	정지민	31-12	대학생/학생	010	
13	정지민	KB 국민은행 우리카드은행	카카오톡		3000000	010	2021-04	강동서	정지민	31-12	대학생/학생	010	
14	정지민	우리카드은행 씨티은행			7000000		2021-05	강남서	정지민	31-12	사무직	010	
15	이준호 윤재은	국민은행 신한은행 한국 국민은행	카카오톡		8500000	010	2021-05	강남서	이준호 윤재은	31-12	회사원	010	
16	이준호 윤재은	국민은행 신한은행 한국 국민은행	카카오톡		3000000	010	2021-05	성동서	이준호 윤재은	31-12	고수	010	
17	이준호 윤재은	국민은행 신한은행 한국 국민은행	카카오톡		6000000	010	2021-05	중부서	이준호 윤재은	31-12	무직	010	
18	이준호 윤재은	국민은행 신한은행 한국 국민은행	카카오톡		9600000		2021-02	노원서	이준호 윤재은	31-12	대학생/학생	010	
19	정호민	신한카드 신한 캐피탈 신한은행	카카오톡		2600000		2021-04	송파서	정호민	31-12	대학생/학생	010	
20	이준호 윤재은	국민은행 신한은행 한국 국민은행	카카오톡		2000000	010	2021-05	성동서	이준호 윤재은	31-12	대학생/학생	010	
21	정호민	신한카드 신한 캐피탈 신한은행	카카오톡		5500000	010	2021-05	도봉서	정호민	31-12	무직	010	

<그림 1> 진술조서에서 추출된 수사 정보 예시

결론

전화금융사기는 개인의 금전적 손해뿐만 아니라 금융 인프라에 대한 지역사회의 전반적인 신뢰를 손상시켜 불필요한 사회적 비용을 발생시키는 심각한 범죄다. 전자통신기기의 대중화와 디지털 신기술(예를 들어 대포폰, 악성 앱 등)의 부정 사용 등 급격히 변화하고 있는 치안환경을 감안하면 형사사법기관의 보이스피싱에 대한 종합적이고 신속한 대응이 그 어느 때 보다 시급한 시점이라 하겠다.

본 연구는 그동안 실무 수사관에 의해 수기로 작성되었던 보이스피싱 사건 데이터베이스의 자동 구축을 위해 자연어처리-인공지능 모델을 개발하는 것을 목표로 하였다. 인공지능 기술 개발을 통한 정확하고 효

울적인 보이스피싱 범죄 데이터베이스의 구축은 전화 금융사기 예방·수사 컨트롤 타워로서 경찰청의 역할과 기능을 확대해 줄 뿐만 아니라, 정보 공유를 통한 관계 부처⁴⁾간 공조를 촉진해 실효성 있는 종합 대책의 설립을 앞당겨 줄 것으로 기대된다.

더불어 전화금융사기 범죄는 조직 수뇌부가 주로 해외에 거점을 두고 있어 범죄자들의 검거·환수를 통한 피해자의 경제적 회복이 쉽지 않은 범죄 중 하나이다. 즉, 범죄를 초기에 예방하는 것이 무엇보다 중요하다. 인공지능 기술을 활용하여 대량의 범죄 수법 데이터베이스를 완성하면, 보이스피싱 범죄 의심번호를 사전에 빠르게 탐지하고, 통화를 차단하는 등 다양한 형태의 범죄 예방정책을 시의성 있게 도입할 수 있을 것으로 예상된다.

마지막으로 최근 확대되고 있는 신종 보이스피싱 수법은 스마트기기 사용에 익숙한 젊은 세대도 빈번하게 피해를 입을 만큼 정교하게 진화하고 있다. 보이스피싱 예방법 전파가 필수적인 시점에 새롭게 구축된 범죄 피해자 데이터베이스는 잠재적 피해 가능성이 높은 사람들을 대상으로 한 보이스피싱 범죄 예방 지식의 명확한 전달에도 활용될 수 있을 것으로 기대된다.^{PSI}

4) 경찰청, 대검찰청, 금융감독위원회, 방송통신위원회, 과학기술정보통신부, 인터넷진흥원, 금융보안원 등을 포함한다

보이스피싱 범죄 해결을 위해 연구되고 있는 과학기술

장광호 경정 · 김희두 경위 · 김창식 경사 · 최주현 경장
경찰대학 치안정책연구소 스마트치안지능센터



서론

보이스피싱 범죄 발생의 증감 여부는 범죄 수익을 창출하기 위한 범죄 단체 나름의 노력과 그 반대로 범죄 발생을 막기 위한 민·관의 노력이 충돌했을 때 결과의 관점에서 바라볼 수 있다.

최근에는 범죄에 대한 전방위적 대응의 필요성이 어느 정도 인정되어 기관 간 협력 체계를 갖춘 보이스피싱 대응 범정부 TF라는 시스템 속에서 정부 차원의 활발한 대응이 이뤄지고 있고, 정부의 강력한 단속과 수사 그리고 통신·금융 분야의 특별 대책 등을 추진한 결과 '22년 보이스피싱 발생 건수·피해 금액이 전년 대비 30%가량 대폭 감소*하였다

* 범죄발생 : 30,982건('21년) → 81,832건('22년)피해금액 : 7,744억('21년) → 5,438억('22년)

그런데도 장기적으로 봤을 때 아직 보이스피싱 범죄는 진화하고 있으며, 여전히 과거 수법에 의해 피해를 보는 사람들이 있고 다시 어떤 신기술에 의해 새로운 수법이 탄생하여 피해자를 양산하게 될지 모르는 위험성을 배제할 수 없다.

이러한 우려의 상황에서 보이스피싱 범죄를 해결하기 위하여 치안정책연구소는 인공지능 기반 보이스피싱 대응 플랫폼 개발, 휴대전화 부정 이용 방지 기술 개발 사업 등 여러 채널을 통한 국가 R&D와 기술 개발 사업 등에 참여하며 다양한 기관과 협업 연구를 수행하고 있다. 따라서 이 장에서는 우리 연구소가 참여했거나 현재 진행 중인 과제의 내용에 대한 상세 설명을 통해 과학기술 연구·개발을 통해 보이스피싱 범죄를 어떻게 대응하고자 노력하고 있는지 기술해보고자 한다.

범죄의 특성을 고려한 대응 전략과 기술 수요

먼저 과학기술 개발의 관점에서 범죄를 해결하기 위해서는 어떤 기술 요소가 수요가 될 수 있는지 파악해야 한다. 이를 위해 경찰관 362명을 상대로 한 폴넷 설문 조사를 통해 보이스피싱 범죄 대응의 어려움과 기술·정책적으로 해결해야 하는 문제가 무엇인지 조사하였으며, 보이스피싱 수사 전문가 20명을 상대로 한 심층 인터뷰를 통해 보이스피싱 수사 단계를 상세히 나누고 단계 내에서 일어나는 어려움을 정의하여 이에 대한 해결 방법을 정리하였다. 그 결과, 보이스피싱 대응 범죄에서 필요한 대응 전략을 크게 세 가지로 구분하고, 이에 따른 기술 수요를 나열할 수 있었다. 보이스피싱 대응을 위한 기술 수요는 크게 ①피해자와의 상호작용을 고려한 보이스피싱 범죄의 사전 탐지와 차단 기술 ②효율적인 범인 추적 등 방법을 고안하고 확산하기 위한 전문가 수사기법을 추천하는 기술 ③음성-텍스트 정보 등 비정형 데이터를 활용한 범죄 정보 검색 기술로 파악되었다.

피해자와의 상호 작용을 고려한 보이스피싱 범죄의 사전 탐지와 차단 기술

보이스피싱 범죄는 주로 피해자의 단말기에 수신되는 콜센터의 문자나 전화로부터 시작되기 때문에 이를 빠르게 탐지하거나 차단해주는 기술이 개발되어 적극적으로 활용된다면 범죄 예방에 많은 도움이 될 것이다. 이를 위해서는 피해자의 휴대전화에서 불상의 범인으로부터 수신하는 문자/통화, 악성 URL 정보에 대해 보이스피싱 범죄 행위를 감지하는 기술이 필요한데, 통신망을 통해 전송되는 음성 정보에 대한 범죄 여부 탐지 기술이나 문자에 대한 스미싱·불법 정보 탐지 기술 그리고 피해자의 단말기 내 정보를 탈취해

가는 악성 앱에 대한 탐지 기술 등이 이에 속한다.

최근에는 이러한 탐지 행위 자체를 잘 수집된 과거 범죄 데이터를 통해 자연어처리와 음성 정보 처리 분야의 딥러닝 기술로 학습시켜 자동으로 탐지하도록 하는 기술이 연구되고 있으며, 기계음으로 합성하여 사람의 목소리처럼 흉내 내는 행위도 감지하기 위해 가짜 합성 음성 탐지 기술도 함께 연구되고 있다.

과거에는 악성 전화번호에 대한 리스트를 관리하여 해당 번호를 차단하는 일종의 범죄 이용 번호 리스트 구축과 같은 방법에서 그쳤으나, 탐지 기술은 더욱더 재빠르고 다양하게 변화하는 수법에도 대응해야 하므로 딥러닝 기술을 활용해 AI가 자동으로 탐지하는 기술을 개발하는 쪽으로 발전하고 있다.

다만 이러한 기술을 활용할 때의 가장 중요한 관건은 탐지의 정확도 및 속도와 사생활 침해 방지이다. 이를 위해서는 정확도 높은 모델의 개발을 위한 실제 환경 데이터가 필요하며, 또한 탐지 모델이 경량화되어 단말기에 내장된 채로 자동으로 스마트폰 기본 앱으로 설치되는 방식이 필요하다. 치안정책연구소의 경우, '21년 '시티즌 코난' 이라는 앱을 개발, 악성 앱 설치 시 이를 자동으로 탐지하는 룰 기반의 기술이 적용되어 앱 서버에서 탐지한 후, 사용자 휴대폰에 알림을 주도록 설정되는 서비스를 시행하고 있다.

이외에도 사용자의 휴대폰에 수신되는 악성 문자를 일반 문자와 구분하여 피싱 문자임을 탐지해주는 머신러닝 기술도 개발되어 서비스되고 있으며, 112 신고에서 보이스피싱 범죄와 관련하여 특정 수법을 분류하는 딥러닝 분류 기술과 특정 수법에 해당하는 키워드를 추출해주는 사전 기반의 자연어처리 기술을 통해 재난 문자와 유사한 형식으로 앱 사용자에게 배포되는 서비스를 시행하고 있다.



<그림 1> 보이스피싱 사전 탐지와 차단 기술

효율적인 범인 추적 등의 방법을 고안하고 확산하기 위한 전문가 수사기법 추천 기술

수사관들은 보이스피싱 범죄 단체의 점조직 형태, 인출-전달책들의 지능화된 수법으로 대부분 사건에 대해 더는 추적이 불가능하여 수사를 중단하게 되는 경우가 많고, 진척이 힘든 상황을 인지하면서도 수사 시 사건 접수와 피해자 진술 청취, CCTV 수사라는 반복된 행위를 하기에 어려움을 토로하는 경우가 많다.

이에 더해 경력이 많지 않은 수사관의 경우 효과적 인 기법이나 절차별 방법을 추천받아 막힘 없이 수사를 진행하기를 원하고, 경험이 많은 수사관의 경우 밀려오는 사건 수와 비교해 턱없이 부족한 인력으로 인해 조서 작성, 접수 등 반복된 업무에 대한 자동화 도입 필요성을 제기하였다. 한편 최근 AI 기술은 단순한 인식의 범위를 벗어나 추론의 영역으로 나아가고 있다. 과거의 기술이 사람보다 높은 정확도로 문서나 글을 분류해주어 세상을 놀라게 했었다면 이제는 일반적인 지식에 대해 사람의 질문에 적절한 답변을 알아서 생성해내는, 심지어 사람보다 더 그럴듯하게 문장을 생성해내는 모델이 세상에 공개된 것이다. 인공지능

능 전문가들은 이미 인공지능이 인간의 단순한 분류 작업과 같은 노동을 대신해주는 것에 더하여 지능을 필요로 하는 지식 노동의 영역을 대신해 줄 수 있는 시대가 올 것이라고 말하고 있다.



<그림 2> ChatGPT

현재 인간의 최신 기술을 이용하면 경험 많은 수사관이 원하는 사건의 자동 접수나 일부 조서 작성은 자동화가 가능하며, 생성적 AI 모델이 경찰 업무에 특화되어 개발된다면 기법 추천과 같은 지능적 요소들도 구현 가능한 기술 개발의 범위에 포함이 될 수 있다. 다만 현재 수준의 초거대 AI 기반 언어 생성 모델의 단점으로 지적되고 있는 점 중 하나는 어떤 질문에 대하여 막힘없이 그럴듯한 답변을 생성해주는 것이지만, 명확한 근거나 사실에 기반한 답변이 아니며 옳은지 그른지를 판단해 줄 수 없다는 점이다. 이러한 문제는 전문성이 필요한 분야에 적용 시 더욱 극명하게 드러나는데, 경찰의 경우 법률적 판단이나 정확한 상황 인지가 필요하므로 현재의 Chat GPT와 같은 일반적인 언어 생성 모델은 이 과정에 크게 도움이 될 수 없다고 보아야 한다.

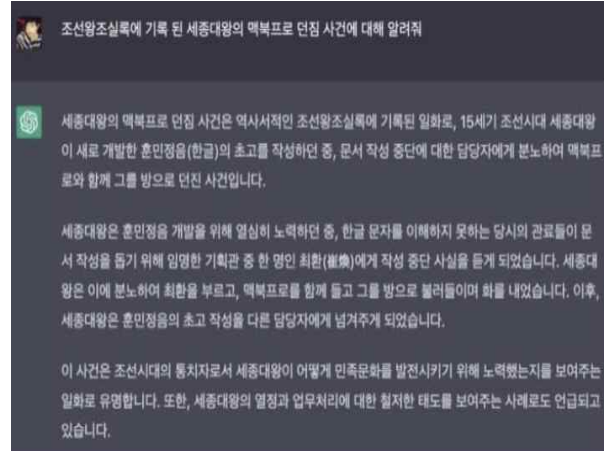
When did France gift Lithuania Vilnius TV tower?

France gifted Lithuania the Vilnius TV tower in 1980.

What prompted the French government to provide the gift?

The French government provided the gift as a gesture of friendship and solidarity with the Lithuanian people, who had recently declared independence from the Soviet Union.

- 1) 실제로 Vilnius TV tower는 France와 전혀 관련이 없고 해당 건물은 1980년도에 지어졌다고 하며, 한글로 세종대왕의 맥북프로 던짐 사건을 질문하여도 황당한 답변이 도출된 사례를 발견함



<그림 3> ChatGPT의 hallucination problem*에 대한 국내·외 사례 1).

* hallucination problem : 생성 AI가 잘못된 정보를 사실인 양 답변하는 현상

이와 같은 문제를 해결하기 위해서는 도메인 지식이 충분히 축적된 지식 그래프와 다양한 상황에 관련된 질문 답변이 주어진 전문가용 데이터가 있어야 하며, 답변에 해당하는 근거가 되는 문서가 함께 근거로 마련되어 있어야 한다. 또한 이런 데이터를 활용해 전문가와 상호작용이 가능한 형태의 생성 모델이 개발되어야 한다.

수사 전문가와 상호작용이 가능한 수사기법 추천 시스템은 상당한 연구와 시행착오가 선행되어야 할 장기 과제에 속하는 분야이며, 치안정책연구소는 보이스피싱 R&D를 통해 이와 같은 개발을 가능한 형태로 개념화하기 위한 연구에 착수하였다. 치안정책연구소는 먼저 아래와 같은 단계를 거쳐 수사기법 추천 시스템을 개발하기로 목표로 하고 있다.

전문가와 상호작용이 가능한 수사기법 추천 시스템

1) 전문가 심층 인터뷰를 통한 CTA(Cognitive Task Analysis) 테이블 작성 : 범죄 수사과정에서 단계별로 겪는 어려움과 전문가 해결 노하우에 대한 조사	1차년도 완료
2) 인터뷰 스크립트·매뉴얼 및 수사기법 자료 수집을 통해 지식 베이스 구축	2차년도('23) 구축 목표
3) 지식 베이스를 수사 시나리오	2차년도('23)

별로 지식 그래프 형태 시각화한 화면 개발(수사기법 탐색 화면)	POC 목표
4) ODQA(Open Domain Question Answering)이 가능한 검색 기능 개발	향후 목표
5) ChatGPT와 같이 질문에 바로 답변을 생성하되, 근거 문서를 함께 찾는 모델 개발	

음성-텍스트 정보 등 비정형 데이터를 활용한 범죄 정보 검색 기술

보이스피싱 범죄 수사 시 핵심이 될 수 있는 수사 단서는 셀 수 없을 정도로 많다. 그러나 점조직 형태로 일어나는 범죄의 특성상 범행으로 생겨난 흔적들은 일관성 있게 정형화된 형태로 드러나지 않고 다양한 출처와 경로, 파편화된 비정형의 정보를 통해 존재할 것이다.

가령, 특정 콜센터의 단원 역할을 맡은 범인이 특정 시나리오에 의해 수십 명의 피해자를 기망하여 금원을 편취하였다고 했을 때, 피해자들의 피해 내역은 각각 다른 범죄 사건으로 취급되어 형사사법정보시스템 내 데이터베이스에 저장되어 있을 것이다. 심지어 아직 형사사법 정보망 내에 저장되지 않은 연관 단서들이 피해자나 제삼자의 휴대폰, 인터넷 커뮤니티, 채팅방 등 어디에든 존재하고 있을 수 있다.

위와 같은 상황은 보이스피싱 범죄를 수사하는 수사관에게 가장 힘든 부분으로 작용한다. 범죄가 발생하는 상황을 미리 인지하는 것도 불가능할뿐더러, 조직 검거를 위해서 정보원의 진술로 범인의 신상을 파악할 수 있는 단서들을 얻게 되었다 할지라도, 효율적이고 완전한 정보 검색이 이루어지지 않는다면 범인의 신원, 범행 내역을 입증할 피해자 정보, 범죄 사실 등을 제대로 수집할 수가 없기 때문이다. 따라서 보이스피싱 범죄와 관련한 다양한 비정형 정보를 수집, 저장, 분석할 수 있도록 시스템을 구성해야 한다.

위와 같이 범죄자를 특정하고, 범행 사실을 입증할 수사의 단서를 모으는 과정에서 범죄 정보 검색(Information Retrieval) 기술은 가장 필요한 수요 중

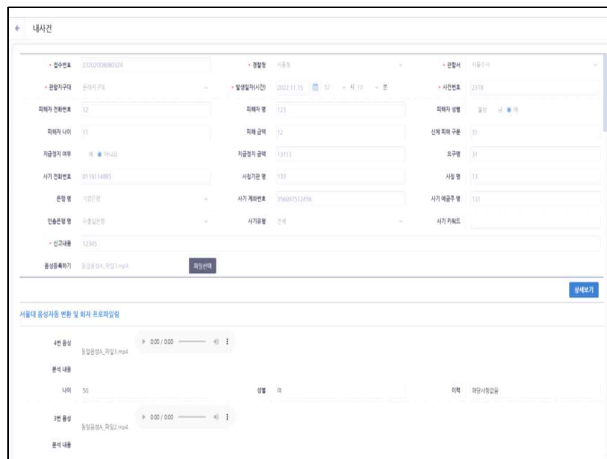
하나이다.

먼저, 텍스트에 대한 정보 검색 기술은 과거 단순 키워드 매칭에서 더욱 다양하고 진보된 기술이 등장하고 있다. 진보된 기술들은 검색자가 입력한 단어에 해당 문서를 찾는 매칭 방식이 아니라, 검색자의 의도를 파악한 의미적 유사성에 기초한 계산 방식을 검색에 활용한다. 이러한 계산에는 최근 몇 년간 급격히 발전한 자연어처리 분야 인공지능 기술 중 하나인 트랜스포머 구조의 인코더 기반 언어모델이 가장 널리 활용되고 있다. 구글이나 네이버 등 가장 대표적인 인터넷 기반의 웹 문서 검색 엔진들 또한 언어모델 기반의 기술이 활용된다고 알려져 있다.

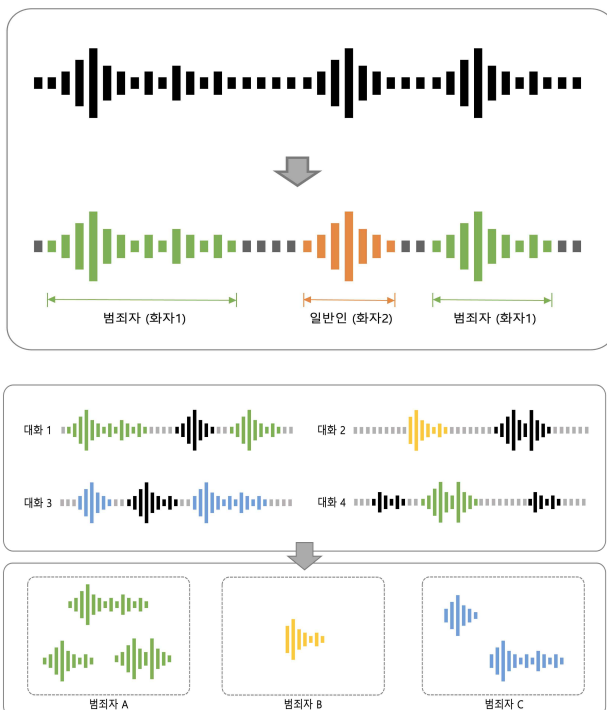
치안정책연구소는 보이스피싱 R&D에서 해당 기술을 활용하여 보이스피싱 범죄 사실이나 피해자-범인 간의 통화 녹취록 전사 텍스트에서 유의미한 정보 또는 검색하고자 하는 정보와 유사한 정보를 신속하게 찾아주는 기술을 연구하고 있다. 현재의 KICS 시스템에서 가장 문제로 지적되는 점 중 하나는, 보이스피싱 관련 피해 진술 조서나 수사 보고서 등에서 검색을 할 수 없어 정확한 사건 검색을 할 수 없다는 것이다. 다수 수사관이 동시에 많은 양의 검색을 하려면 효율적인 검색 기술이 필요하기 때문이다. 따라서 현재 연구되는 기술은 서버나 검색 속도상의 걱정 없이도 효율적이고 빠르게 방대한 양의 문서를 검색하면서도 수사관의 검색 의도에 맞게 결과를 제시해주는 기술이다. 앞으로 범죄 관련 비정형 정보가 더 수집되고 저장됨으로써 기존보다 더 방대한 양의 문서 베이스가 만들어진다면, 해당 기술을 범죄 정보 검색에 활용해야 하는 필요성은 더욱 커지게 될 전망이다.

또한 텍스트 변환 이전 콜센터에서 피해자와 상호 작용하면서 생기는 최초의 데이터는 범인의 목소리가 담긴 녹취 데이터이다. 녹취 데이터의 음성 정보는 텍스트와는 다른 방식으로 기술이 적용되지만, 궁극적인 목적은 동일 목소리를 기반으로 범죄자를 인식하거나 찾아야 한다는 점에서 같다. 음성 정보 처리를 활용한 인공지능 기술은 주로 화자 분리, 화자 인식, 화자 특성에 대한 프로파일링, 음성 정보의 텍스트화(Speech-to-Text) 기술이 존재한다. 이러한 기술들을

활용하여 지속해서 발생하는 보이스피싱 범죄의 범인 목소리 데이터를 유형화하고 유형화한 데이터를 저장하여 검색에 활용하거나 동일범으로 인식하도록 기술을 구성한다면 향후 보이스피싱 범죄 수사에서 커다란 역할을 담당할 것이다.



<그림 4> 서울대 보이스피싱 음성 STT 기술



<그림 5> 부산대 화자 음성 분리 및 군집화 기술

결론

최근 몇 년 동안 보이스피싱 범죄가 크게 줄어들지 않고 계속 증가하며 발생했던 이유는 범죄 조직이 새로운 정책이나 예방 활동에도 불구하고 이를 다시 빠져나가기 위한 새로운 장치를 개발하였고, 결국 범행을 지속할 수 있는 환경에 쉽게 놓여있었기 때문이라고 판단할 수 있다. 또한 언론에서 확인되는 최근 몇 가지 사례*를 살펴보다라도 여전히 보이스피싱 범죄 조직이 얼마나 쉽게 사회적 차단 망을 빠져나가고, 수법을 교묘하게 바꿀 수 있었는지 단적으로 확인할 수 있다.

* 범죄 단체의 수법 사례

팀뷰어 어플 사용하여 휴대폰을 원격제어 함으로써 대출 신청, 계좌 내 전액 송금하도록 하는 새로운 수법 사용

시티즌 코난 앱을 사칭하는 악성앱을 개발하여 경찰관을 사칭한 후 금원편취하는 수법 사용

인터넷 전화의 앞자리가 피해자의 스마트폰에 노출 시키면 피해자의 지인 번호인 것처럼 속일 수 있다는 점을 악용, 피해자의 지인인 것처럼 번호 변작 발송

삼성전자 계열 스마트폰의 CNC 기능을 활용하여 번호 변작 발송

이처럼 여전히 쉽게 보이스피싱 범죄가 일어날 수 있는 이유는 사회의 새로운 기술들을 빠르게 흡수한 범죄 단체가 이를 범죄에 악용하고 국가기관은 나중에 인지한 뒤 해결책을 마련할 수밖에 없는 형태이기 때문이거나, 미리 악용이 예상되어 현재 기술로도 바로 조치할 수 있는 문제들임에도 불구하고 개인의 사생활 침해나 기관 간 정보공유 협력이라는 문제를 먼저 해결해야 하는 어려움에 놓인 상태로 부족한 정책을 만들 수밖에 없었기 때문이었다. 이러한 문제를 해결하기 위하여 정부 차원에서 범죄에 대한 전방위적인 대응을 이뤄내고 있으며, 민·관·연은 협업하여 급격히 발전되는 인공지능·IT 기술을 활용, 범죄 단체를 막기 위한 연구개발을 진행하고 신기술들의 악용 사례를 막기 위한 전략을 세우고 있다.

이처럼 변모되는 사회 변화에 대응하기 위해서 과학기술을 범죄로 악용하는 것을 차단하기 위한 노력이 선행되어야 한다는 논의가 크게 부각 되고 있고, 이에 따라 향후 기술 개발을 위한 노력은 앞으로 더욱 활발해질 것으로 보인다.[PSI](#)

보이스피싱 대응과 피해자 구제

황 석 진

동국대학교 국제정보보호대학원 교수



서론

보이스피싱이 최초로 등장한 2006년 이후 보이스피싱 근절을 위한 정부의 노력에도 관련 범죄는 진화하여 매년 수천억 원의 피해가 발생하였고 최근까지 피해액은 4조에 육박하고 있다. 진화하는 보이스피싱 범죄에 대응코자 정부는 보이스피싱 대응 방안과 보이스피싱 엄단을 국정과제로 발표¹⁾하고 대응하고 있다. 최근 보이스피싱은 기존의 금융기관을 통한 사례가 어려워지면서 대면 편취형과 가상자산을 이용하는 유형과 계좌지급 정지를 악용한 통장 협박 등의 새로운 유형의 보이스피싱이 등장하였다.

하지만 새로운 유형의 보이스피싱 대응에 한계가 있고 제도적 불비로 인하여 많은 피해자들이 구제받지 못하는 실정이며 금전적 피해와 더불어 피해 사실을 주변에 알리면 비난받는 경우도 발생하여 피해자들은 이중적인 고통을 부담하고 있다.

예방과 대응에 초점을 맞추는 것은 당연한 일이나 피해가 발생한 피해자를 위해서 피해금 회복과 정신적 트라우마를 치유하는 것도 중요할 것이다.

최근 코로나로 인하여 생활 환경이 변화하였고 대면 소통보다는 비대면 소통이 발달하는 환경에서 보이스피싱은 이러한 비대면 소통을 역이용하는 범죄라고 할 수 있다.

보이스피싱은 일상생활 속 깊고 광범위하게 퍼져있는 악성 바이러스(malicious virus)와 같이 암적인 존재로서 철저한 대응과 모두의 노력을 통하여 근절해야 하며 대비책이 미흡한 경우 코로나(COVID-19)처럼 사회적 파급력과 사회적 비용은 계속 증가할 것이며 피

해자의 고통은 더욱 가중될 것이다.

보이스피싱 범죄에 대한 주요 문제점과 제도적 대응 방안, 피해자 구제에 대하여 몇 가지 제언을 하고자 한다.

보이스피싱

1. 개요

보이스피싱은 음성(voice)과 개인정보(private data), 낚시(Fishing)의 합성한 용어로서 주로 금융기관이나 관공서, 수사기관, 국세청 등을 사칭하여 개인의 금융정보를 탈취하여 범죄에 사용하거나 수사기관을 사칭하여 특정 범죄에 연루되었다고 기망하는 경우도 있고 대환대출²⁾을 통하여 기존의 대출을 갚아야 새로운 대출이 가능하다고 기망하여 금전을 편취하는 등의 수법이다.

이처럼 피싱(phishing)범죄는 보이스피싱(voice phishing) 외에도 파밍(pharming), 스미싱(smishing)으로 구분할 수 있고 피싱 사기는 무차별적으로 개인정보를 불법으로 취득하여 사기를 치는 대표적인 금융범죄라고 할 수 있다.³⁾ 유명 금융회사 홈페이지를 모방한 가짜 사이트로 사용자를 유인해 개인정보나 금융정보를 빼가는 범죄다. 인터넷 메일을 이용해 피싱을 하면 파밍(Pharming)이라 하고, 전화를 이용하면 보이스피싱(voice phishing), 문자메시지(Text Message)를 이용하면 스미싱(Smishing)이라고 부르고 있으며 사기 범죄로 규정하고 있다.⁴⁾

1) 보이스피싱 범죄 정부합동수사단 출범, 범부처 보이스피싱 방지대책 시행(2022. 9)

2) 금융기관 등으로부터 대출을 받아 종전의 대출금을 갚는 것

3) 강현중, 피싱에 대한 분석 및 대응방안에 대한 연구, 융합보안논문지, 14(5), 2014, 61-70p.

4) 윤행성/곽대경, '보이스피싱의 예방과 대책마련을 위한 연구', 한국형사정책연구원, 2009, 19-20p.

[표 1] 보이스피싱의 유형⁵⁾

구 분	사칭 기관	수 법
불특정 다수	경찰, 검찰, 법원	범죄 사건 연루조사, 개인정보유출 등
	금융감독원, 은행, 카드사	금융정보유출, 카드대금 등
	우체국	우편물, 택배, 카드반송 등
	건강보험공단, 연금공단, 국세청	연금, 보험료, 세금환급 등
	통신회사	전화요금 환급 등
특정인	피싱 사이트형	공공기관, 은행 등
	협박형	폭력조직
	지인 사칭형	가족, 친구, 직장동료 등
	의무 부과형	동창회, 대학교 등

2. 현황

1) 발생 및 검거현황⁶⁾

구분	합 계				기관사칭형				대출사기형			
	발생건수	피해(억원)	검거건수	검거인원	발생건수	피해(억원)	검거건수	검거인원	발생건수	피해(억원)	검거건수	검거인원
2018	34,132	4,040	29,952	37,624	6,221	1,430	4,673	5,491	27,911	2,610	25,275	32,131
2019	37,667	6,398	39,276	48,713	7,219	2,506	5,487	6,045	30,448	3,892	33,791	42,666
2020	31,681	7,000	34,051	39,324	7,844	2,144	4,297	4,797	23,833	4,856	29,754	34,521
2021	30,982	7,744	27,647	26,397	7,017	1,741	1,954	1,895	23,965	6,003	25,693	24,500
2022	21,832	5,438	24,522	25,030	8,930	2,077	4,103	4,500	12,902	3,361	20,419	20,538

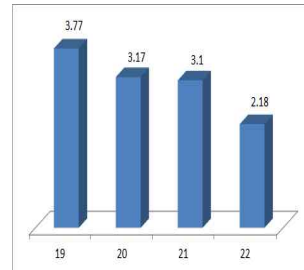
보이스피싱은 처음 발생한 ‘06년 이후 피해가 꾸준히 증가하였으나 ’ 22년 보이스피싱 발생 건수 및 피해 금액이 ‘21년 대비 30% 가까이 감소하였다.

5) 최관/김민지, ‘한국 보이스피싱 범죄의 진행과정에 관한 연구’, 경찰학연구. 통권43호, 247p

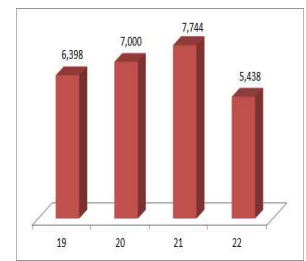
6) 국무조정실 보도자료, ‘22년 보이스피싱 피해 발생, 16년 만에 큰 폭으로 감소, 2023. 2.1.

2) 발생건수 및 피해금액 현황⁷⁾

발생건수(만건)



피해금액(억원)



3. 대응

1) 국내

정부는 보이스피싱 대응을 위하여 범정부 TF를 구성하여 운영하고 철저한 사전 예방을 통하여 피싱사이트 및 변작기 탐지, 불법거래 게시물 탐지·삭제를 강화하고 대포폰 대량 개통을 차단하기 위하여 개통 가능한 회선수 제한, 단말기 자체 국외 발신번호 표시 개선 등의 예방 조치를 실시하고 있다.⁸⁾ 경찰은 악성 앱· 문자, 대포폰·통장 등 생성에서 유통까지 전방위적 단속을 실시하고 민관 협업을 통하여 범행수단을 적극적으로 차단하고 있다.

금융권은 비대면 계좌개설 시 실명확인 방법의 '1원 송금' 방식을 개선⁹⁾하여 적용하는 등 본인확인 절차를 강화하였고 보이스피싱 피해발생 우려 시 피해자가 본인명의 계좌를 일괄 선택·제한할 수 있도록 계좌통합관리서비스 시스템도 운영하고 있다.

또한 지연인출제¹⁰⁾와 개인정보 노출자 사고 예방시스템¹¹⁾, 전자금융거래의 제한, 거래의 모니터링, 전화

7) 금융감독원 보도자료, ‘제2차 금융분야 보이스피싱 대응방안’, 2023. 2. 28.

8) 국무조정실 보도자료, ‘22년 보이스피싱 피해 발생, 16년 만에 큰 폭으로 감소, 2023. 2.1.

9) 인증번호 입력 유효시간 단축(15분 이내) 및 ‘계좌 개설용’ 문구 표기

10) 대표적인 대응 정책으로 계좌에서 1회에 100만 원 이상의 금액이 송금·이체되어 입금된 경우 입금된 때로부터 해당 금액 상당액 범위 내에서 30분간 자동화기기(CD/ATM기 등)를 통한 인출·이체가 지연되는 제도

11) 금융소비자의 노출된 개인정보를 타인이 이용해 명의도용 금융거래를 시도하는 것을 방지하는 시스템

번호 이용정지 제도¹²⁾도 함께 운영하고 있다.

2) 해외

(1) 미국

미국에서는 무작위로 전화를 걸어 수신자에게 ‘제 목소리가 들리세요?(Can you hear me?)’ 라고 묻고 수신자가 ‘예(Yes, Sure, Ok)’라고 대답하면 금융사기에 걸려드는 사기가 성행하였다. 사기범은 수신자의 대답을 녹음하여 각종 물건 구입에 사용하고 소비자가 구매에 동의했다는 증거로 녹음한 음성을 활용하는 수법을 이용하며 정부기관을 사칭하여 사회 보장 번호와 인적사항 등 개인정보를 탈취하기도 한다.¹³⁾

미국의 23개의 주와 관에서는 온라인 피싱(phishing) 사기를 특정 범죄로 취급하고 이를 엄격히 금지하고 발생한 범죄를 처벌하도록 하고 있다. 인터넷 웹사이트, 전자우편, 기타 인터넷을 이용하여 해당 사업자의 권한 또는 승인 없이 사업자로 사칭하여 개인신원 확인정보를 요구하거나 타인으로 하여금 이를 제공하도록 유도하는 행위를 불법으로 규정하고 있는 ‘피싱 사기방지법(Anti-phishing Act)’은 캘리포니아 외 7개 주에서 명시적으로 입법화하였고, 그 외의 주에서는 ‘스파이웨어’ 또는 ‘컴퓨터 범죄’ 관련 법규를 통해 규정하고 있다.¹⁴⁾

예방 및 사후 구제를 위한 방안으로 보안 혹은 신용 동결법(Security or Credit freeze law), 원상 복구 규정, 부과 벌금 펀드 등을 운영하고 있다.¹⁵⁾

으로 해당 시스템에 등록된 개인 정보는 금융회사에 공유되어 금융거래 시 본인확인에 주의를 기하도록 함으로써 사고를 예방하는 시스템

- 12) 전기통신금융사기에 이용된 전화번호를 확인한 때 과학기술정보통신부에 전화번호에 대한 전기통신역무 제공 중지를 요청하여 추가적인 피해를 예방하는 시스템을 운영하고 있다.
- 13) 이은진, ‘전기통신금융사기 구제에 관한 연구(피해금 환급 방안을 중심으로)’, 고려대 법무대학원, 석사학위논문, 37면, 2018년
- 14) 강성복/윤종민, ‘전기통신금융사기 법제에 관한 분석적 고찰’, 「과학기술과 법」 제3권 제2호, 충북대학교 법학연구소, 9-10면, 2012년
- 15) 최창수, ‘미국의 온라인피싱방지법과 시사점’, 「법조」 제63권 제10호, 법조협회 2014년

대부분의 주에서는 ‘피싱사기방지법’을 위반할 경우 일정한 벌금을 부과할 수 있도록 하고 있으며 일부 주에서는 벌금이 동법 취지에 부합하도록 징수된 벌금으로 펀드를 조성, 운영하기 위한 근거 규정을 두고 있다.

(2) 일본

일본은 예금계좌에 돈을 송금 또는 입금하는 것을 후리코메(振り込め)라고 하는데 사기로 예금 계좌에 돈을 입금시켜 편취한다는 의미로 전자금융사기를 후리코메(振り込め) 사기라고 하며 특수사기¹⁶⁾로 분류하여 대응하고 있다. 2004년에 특수사기 사건이 발생한 후 매년 꾸준히 발생하고 있으며 2021년도 피해가 282.0억 엔이 발생하였다.¹⁷⁾

[표2 특수사기 발생건수 및 피해금액 추이]

(단위:건, 억엔)

구 분		'15년	'16년	'17년	'18년	'19년	'20년	'21년
특수사기 전체	건수	13,824	14,154	18,212	17,844	16,851	13,550	14,498
	금액	482.0	407.7	394.7	382.9	315.8	285.2	282.0

자료출처 : 금융감독원 동경사무소

피해액은 사상 최고였던 2014년(565.5억 엔)에서 절반으로 감소하였으나 여전히 노인 등 취약계층을 대상으로 한 피해가 높은 수준으로 발생하고 있다.

노인을 대상으로 하는 사례가 많아 일본 대형 은행들은 아예 일정 연령 이상의 노인들의 ATM 송금을 제한하는 방안을 검토한 사례도 있다.¹⁸⁾

일본도 피싱사기 예방 캠페인을 벌이고 있으며, 대포통장과 대포폰의 부정사용 방지를 위해 금융기관과 통신회사가 협력하여 개설 및 양도시에 철저한 본인

- 16) 피해자에게 전화를 거는 등 대면하는 일 없이 신뢰하게 만들어, 지정한 예금계좌에 이체 그 밖에 방법에 의해 불특정다수로부터 현금 등을 속여 빼앗는 범죄(현금 등을 협박해서 빼앗는 공갈 및 틈을 봐서 현금카드 등을 절취하는 절도를 포함)
- 17) 금융감독원 동경사무소 ‘2021년 일본의 보이스피싱 등 특수사기 현황’, ‘22.09.
- 18) 한겨레, ‘보이스피싱 막아라’...일본 대형 은행들, 노인 ATM 송금 제한 추진, 2017.8.31. <<http://www.hani.co.kr/arti/international/japan/809107.html>>, 2023. 4. 8. 최종방문

확인 의무를 실시하고 있다.¹⁹⁾ 피해의 회복을 위해서는 2007년 제정된 “범죄 이용 예금 계좌 등에 관계된 자금에 의한 피해 회복 분배금의 지불 등에 관한 법률” : 犯罪利用預金口座等に係る資金による被害回復分配金の支払等に関する法律(‘전자금융사기 피해자 구제법’으로 칭하기로 한다.)²⁰⁾을 통해 예금보험기구가 피해금 환급 업무를 담당하고 있다.

주요 문제점

1. 피해 회복의 한계

현행 「전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법」(이하 ‘통신사기피해환급법’)에서 피해구제를 받을 수 있는 범위는 자금의 이체, 송금 행위에 한정되어 있고 최근 대면 편취형의 경우도 관련 법의 개정²¹⁾을 통하여 적용하도록 추진하고 있다. 또한 ‘제2차 금융분야 보이스피싱 대책’ 발표를 통하여 가상자산을 이용한 보이스피싱 피해구제와 간편송금을 이용한 보이스피싱과 계좌의 일부 지급정지를 악용한 통장협박의 피해자 구제를 추진하고 있다.²²⁾

이러한 정부의 대응에도 피해자의 금전적 피해회복에는 한계가 발생한다. 피해구제를 위하여 범죄에 악용된 계좌에 잔액이 남아 있어야 채권소멸 절차 등을 밟아 피해환급금의 결정 및 지급을 받는 방법이나 범죄에 가담한 관련자를 대상으로 손해배상 청구를 통하여 피해 회복이 가능하다.

19) 안성훈, ‘해외 각국의 보이스피싱 범죄 발생 및 대응실태 연구 : 미국, 일본, 대만, 중국을 중심으로’, 대검찰청 형사1과, 158-159면, 2016년

20) 예금계좌로의 입금 등을 이용한 사기 등의 범죄행위에 의한 피해자에 대한 피해회복분배금의 지불 등과 관련하여 예금 등과 관련된 채권의 소멸 수속 및 피해회복분배금의 지불 절차 등을 정하여 피해자의 재산적 피해의 신속한 회복에 이바지한다(犯罪利用預金口座等に係る資金による被害回復分配金の支払等に関する法律 第1條 定義)

21) 서울신문, ‘보이스피싱 대응 민당정 협의회...여 통신사기피해환급법 3월 국회서 처리하기로’, 2023. 2.28. <https://www.seoul.co.kr/news/newsView.php?id=20230228500190&wlog_tag3=naver>, 2023. 4. 1방문

22) 금융위원회 보도자료, ‘제2차 금융분야 보이스피싱 대책 발표’, 2023. 2.27

범죄에 악용된 통장의 잔액이 없거나 범죄자가 검거되지 않은 경우, 검거가 되어도 변제능력이 없는 경우에는 실질적 피해 구제에 한계가 있다.

[표 3 보이스피싱 피해 현황]

(단위 : 억원, 건, %, %p)

구 분	'17년	'18년	'19년	'20년	'21년	전년대비 증감률
피해금액 ¹⁾	2,431	4,440	6,720	2,353	1,682	△28.5
환급액	598	1,011	1,915	1,141	603	△47.2
환급률	24.6	22.8	28.5	48.5	35.9	△12.6
피해자수	30,919	48,765	50,372	18,265	13,204	△27.7

주)피해구제신청접수(1차 계좌)기준임

2. 국제공조 수사의 한계

보이스피싱 범죄 집단은 대부분 해외에 거점을 두고 있는 경우가 많고 해외 IP나 전화번호 등을 추적하여도 현지 출장을 통한 현장 조사의 어려움이 있으며 또한 국제공조를 통한 대응에도 관련 국가의 협조 유무와 지리적 한계 등이 발생하는 등 신속한 국제공조 수사도 한계가 발생한다.

3. 최신수법에 대한 대응

보이스피싱 범죄의 사전 단계는 불특정 다수나 특정인에게 전화나 문자, 이메일 등을 통하여 특정 기기를 사칭하거나 대출을 알선하는 내용으로 피해자를 유인한다. 수사기관의 수사로 범행에 사용된 휴대폰이나 컴퓨터 등의 로그기록(Log記錄)²³⁾을 추적할 수 있으나 해당 휴대폰의 IMEI²⁴⁾, 컴퓨터의 MAC 주소²⁵⁾를 변작하여 추적을 회피하고 악성 APP을 설치하여 진위 여부를 확인하고자 금융회사나 수사기관에 전화를 하더라도 보이스피싱 조직으로 통화가 연결되는 사례도

23) 로그기록(log記錄) : 사용자가 특정 시스템에 접속하기 위해 본인임을 알리고 등록하면서 남는 기록, 누가, 언제, 어떻게 시스템에 접근해 무엇을 했는지 컴퓨터에 자동 저장되는 전산 운영 정보, [두산백과]

24) IMEI(International Mobile Equipment Identity) : 휴대폰화 국제 고유 식별번호,

25) MAC(Media Access Control)주소 : 통신을 위해 랜카드 등에 부여된 주소

있고, 원격제어 APP을 설치하도록 유도하여 피해자 휴대폰의 금융정보를 탈취하거나 직접 실행하여 금융을 편취하는 등의 신종수법도 발생하고 있으나 이런 범죄 수법에 대한 대응은 한계가 있다.

개선방향

1. 사기 방지 기본법 제정

보이스피싱은 대표적인 민생범죄이며 악성 사기 범죄라고 할 수 있다. 보이스피싱 등의 범죄에 대한 접수 창구 단일화 및 사기정보를 통합하여 사기정보분석원을 설립하고 체계적이고 전문적 분석을 통한 차단, 수사, 예방의 종합적인 대응을 위한 범정부적 통합체계가 마련되어 보이스피싱 등의 범죄를 철저히 대응할 수 있도록 사기방지기본법을 제정해야 한다.

2. 피해자 구제 방안 강화

보이스피싱 피해구제의 실효성을 강화하는 차원에서 보이스피싱 보험을 확대하여 금융기관의 「예금자보호법」처럼 모든 금융기관에서 보이스피싱 예방 보험을 의무적으로 가입하고 보장금액의 범위도 최대 3,000만 원까지 상향하여 운영하도록 한다. 해당 보험료²⁶⁾는 최소한으로 금융기관이 1차 부담하고 기간이나 보장액에 따라 신용카드 포인트, 예금 이자와 각종 마일리지 등으로 자동 납부하게 한다면 실질적인 보험계약자의 부담은 없을 것이다.

3. 사기방지 예방 교육의 의무화

사기범죄 예방을 위하여 유관기관과 각 지자체와 기업에서 정기적인 사기방지예방 교육을 진행하여야 한다. 경찰청은 사기방지 예방을 위한 전문가를 양성하고 일정 근로자 이상 사업장의 필수적으로 이수하도록 하는 법정 의무교육²⁷⁾에 포함하여 운영하여야 하

며 특히 사기 피해 취약 계층에 대하여 교육을 집중적으로 병행하여야 한다.

4. 피해자에 대한 적극적 치유

보이스피싱 범죄 등의 사기 피해자가 주변인에게 자신의 피해 사실을 알리는 순간 피해 사실에 대한 비난을 받는 경우가 있다. 보이스피싱 범죄로 금전적 손해가 발생하여 가족을 포함한 주변인에게 창피해지고 우울증, 두려움, 불편함 등 심지어는 극단적인 선택을 하는 경우도 발생한다. 피해자의 정신적 안정을 위하여 “사기범죄 피해 치유센터”를 운영하고 추가로 전화 상담과 온라인 기반 실시간 채팅 및 게시판 상담을 제공하여 365일(24시간) 운영되는 전국 단위의 치유센터 운영이 필요하다.

결론

보이스피싱 범죄는 비대면 소통 범죄로 피해자의 정신적, 경제적 고통이 가중되며 피해 회복에 대한 이슈가 계속 발생되고 있다. 취약계층에 대한 홍보 및 교육을 통하여 보이스피싱 예방과 피해자에 대한 치유센터를 운영하여 피해자의 정신적 피해를 치유해야 한다.

보이스피싱 범죄는 대표적인 민생침해범죄이며 악성 바이러스처럼 사회 전반에 퍼져 여러 피해자를 양산하고 다수인에게 씻을 수 없는 상처와 트라우마를 안겨준다. 보이스피싱이 근절되지 않는다면 사회적 파급력과 사회적 비용은 계속 증가할 것이며 사회 전반에 퍼져있는 불신은 정상적인 사회생활에 악영향을 미칠 것이다.

정부의 노력만으로는 보이스피싱 범죄를 근원적으로 차단할 수는 없을 것이다. 개인과 국가가 함께 보이스피싱 범죄에 대하여 적극적으로 대응하여 보이스피싱 범죄를 근절시키고 사회질서가 확립되기를 소원해 본다.^{PSI}

26) ○○보험회사에서 금융사고보상보험을 운영하고 있으며 연5,600원으로 약300만원을 보장함

27) 법정 의무교육 : 성희롱예방교육(「남녀고용평등법」 제13조), 개인정보보호교육(「개인정보보호법」 제28조), 산업안전보건교육(「산업안전보건법」 제31조), 퇴직연금교육

(「퇴직급여법」 제32조), 장애인인식개선교육(「장애인고용촉진 및 직업재활법」 제86조

모바일 등 디지털 문서에 대한 위조 및 행사혐의에 대한 대법원 법리 적절성 검토

- 디지털시대 형법상 위조 혐의 문제점 검토 중심으로 -

김 호

12사단 군사경찰대대장(군사법경찰관, 법학박사)



서 언

최근 모바일 수단 등 디지털 환경을 이용한 문서 위변조 및 부정행사 등의 범죄가 증가하고 있는 사회적 분위기에서 일련의 법원 판결들이 변화하고 있는 시대적 흐름을 제대로 반영하고 있지 못하다는 의견이 적지 않다.

즉, 과거와 같이 종이나 도화 재질의 문서보다 사진이나 이미지 등 파일형태의 전자문서의 이용이 활성화되고 있으며 이에 따라 범죄경향 역시 디지털 형태의 문서를 위변조하거나 전자적 형태의 문서를 부정 사용하는 등의 불법이 만연하고 있지만 법원은 아직도 전통적인 수준에서 문서 부정사용, 위변조 및 행사 등에 얽매어 전통적인 법리기준에서 판단하고 있다는 것이다.

따라서 본 글에서는 현재 문서에 관한 죄를 규정하고 있는 형법상의 범죄들에 대하여 대법원의 법리에 관하여 살펴보고 디지털 시대에 있어 어떠한 문제가 있는지 검토하고자 한다.

형법상 문서에 대한 인정 기준

(1) 법원의 인정기준

먼저 법원은 형법상 문서에 관한 죄에 있어서 다음과 같은 기준을 정립하여 적용하고 있다. 즉, “문서에 관하여 문자 또는 이에 대신할 수 있는 가독적 부호로 계속적으로 물체상에 기재된 의사 또는 관념의 표시인 원본 또는 이와 사회적 기능, 신용성 등을 같게 볼 수 있는 기계적 방법에 의한 복사본으로서 그 내용이 법률상, 사회생활상 주요 사항에 관한 증거로 될 수 있는 것” 이라고 정의한다.¹⁾

(2) 형법 규정에서의 문서 범위

다음으로 형법 규정에서는 문서의 범위에 관하여 “공문서이든 사문서이든 위조, 변조 등의 형법상 범죄혐의 인정에 있어서 원본 문서 외에도 전자복사기, 모사전송기(팩스 등) 기타 이와 유사한 기기를 사용하여 복사한 문서 또는 도화의 사본도 문서 또는 도화로 본다.”²⁾고 규정하고 있다.

디지털문서 부정사용 및 위조 등 혐의 인정 여부

(1) 디지털문서에 대한 범죄혐의 부정 입장

가. 공문서부정행사 부정³⁾

운전면허증 신분확인 교부시 직접 면허증이 아닌 스마트폰으로 남의 것을 촬영한 이미지 파일을 제시한 것만으로 공문서 부정행사죄가 되는지에 대하여 대법원은 이미지 파일은 공문서가 아니므로 범죄가 성립되지 않는다고 무죄 판결을 내린 바 있는데, 사건의 내용을 살펴보면 피고인은 운전면허가 취소되자 몰래 서울지방경찰청장 명의로 발급된 타인의 운전면허증을 피고인의 휴대전화에 내장된 카메라로 촬영하여 그 이미지 파일을 휴대전화에 보관한 상태로 운전을 하다가 경찰관으로부터 운전면허증의 제시를 요구받고 피고인의 휴대전화에 저장된 이미지 파일을 제시하였다가 기소되었다.

이에 대하여 대법원은 자동차 등의 운전자가 경찰 공무원에게 다른 사람의 운전면허증 자체가 아니라

1) 대법원 2004도788 판결 참조

2) 형법 제237조의2(복사문서 등) 이 장의 죄에 있어서 전자복사기, 모사전송기(팩스 등) 기타 이와 유사한 기기를 사용하여 복사한 문서 또는 도화의 사본도 문서 또는 도화로 본다

3) 대법원 2018도2560 판결 참조

이를 촬영한 이미지 파일을 휴대전화 화면 등을 통하여 보여주는 행위는 운전면허증의 특정된 용법에 따른 행사라고 볼 수 없는 것이어서 그로 인하여 경찰 공무원이 그릇된 신용을 형성할 위험이 있다고 할 수 없으므로 이러한 행위는 결국 공문서부정행사죄를 구성하지 아니한다고 판시하였다. 즉, 이미지 파일형태의 문서 등에 대하여 형법상 처벌대상인 문서로 간주하지 않는 것으로 볼 수 있다.

나. 문서위조 및 행사 등⁴⁾

컴퓨터 스캔으로 만든 자격증의 이미지파일에 대하여 대법원은 형법상의 처벌대상인 문서가 아니라고 하는데 본 사건은 피고인이 컴퓨터 스캔 작업을 통하여 만들어낸 공인증개사 자격증의 이미지 파일이 문제된 사안으로 이에 대하여 대법원은 형법상 문서에 관한 죄에 있어서 문서라 함은 문자 또는 이에 대신할 수 있는 가독적 부호로 계속적으로 물체상에 기재된 의사 또는 관념의 표시인 원본 또는 이와 사회적 기능, 신용성 등을 동일시할 수 있는 기계적 방법에 의한 복사본으로서 그 내용이 법률상, 사회 생활상 주요 사항에 관한 증거로 될 수 있는 것을 말하고 컴퓨터 모니터 화면에 나타나는 이미지는 이미지 파일을 보기 위한 프로그램을 실행할 경우에 그때 마다 전자적 반응을 일으켜 화면에 나타나는 것에 지나지 않아서 계속적으로 화면에 고정된 것으로는 볼 수 없으므로 형법상 문서에 관한 죄에 있어서의 문서에는 해당되지 않는다고 판단하였다.

추가로 또 다른 사건인 국립대학교 교무처장 명의의 졸업증명서 파일을 위조하였다는 사안에 대하여서도 대법원은 문서 자체가 아니라 문서를 스캔한 이미지 파일을 조작해도 이미지 파일은 문서가 아니므로 문서 위조가 아니라고 보았는데 앞서 제시한 법리와 마찬가지로 졸업증명서 파일은 그 파일을 보기 위하여 일정한 프로그램을 실행하여 모니터 등에 이미지 영상을 나타나게 하여야 하므로 파일 그 자체는 형법상 문서에 관한 죄에 있어서의 문서에 해당되지 않는다고 하여 이 사건 공소사실에 대해 무죄를 선고한 것은 정당하다고 판시하였다.

(2) 디지털문서에 대한 범죄혐의 인정 입장

앞서 기술한 것과 달리 디지털문서에 대한 위변조 및 행사 등을 인정하는 대법원 입장이 있는데 우선 사건내용을 살펴보면 피고인이 휴대전화 신규 가입신청서를 위조한 후 이를 스캔한 이미지 파일을 제3자에게 이메일로 전송한 사안⁵⁾에서 대법원은 이미지 파일 자체는 문서에 관한 죄의 문서에는 해당하지 않으나 이를 전송하여 컴퓨터 화면상으로 보게 한 행위는 이미 위조한 가입신청서를 행사한 것에 해당하므로 위조사문서행사죄가 성립한다고 판단하였다.

세부적으로 위 사건을 설명하자면 피고인은 PC방에서 인터넷 쇼핑사이트인 ‘G-마켓’에 들어가 휴대전화기 구입신청을 하면서 인터넷에 게시된 KTF 신규 가입신청서 양식에 컴퓨터를 이용하여 타인의 인적사항 및 계좌번호, 청구지 주소 등을 입력하고 이를 출력한 다음 신청서 용지 하단 고객명란과 서명란에 타인을 기재함으로써 행사할 목적으로 권한없이 권리의무에 관한 사문서인 타인 명의 휴대전화 신규 가입신청서를 위조하고 해당 가입신청서를 이미지화한 후 이메일로 전송하여 위조한 사문서를 행사하였다.

이에 대하여 대법원의 판단 논리에 따르면 위조된 문서를 제시 또는 교부하거나 비치하여 열람할 수 있게 두거나 우편물로 발송하여 도달하게 하는 등 위조된 문서를 진정한 문서인 것처럼 사용하는 한 그 행사의 방법에 제한이 없으며 위조된 문서 그 자체를 직접 상대방에게 제시하거나 이를 기계적인 방법으로 복사하여 복사본을 제시하는 경우는 물론 모사전송의 방법으로 제시하거나 컴퓨터에 연결된 스캐너(scanner)로 읽어 들여 이미지화한 후 전송하여 컴퓨터 화면상에서 보게 하는 경우도 행사에 해당하여 위조문서행사죄가 성립한다고 보았다.

그런데 특이하게 이와 유사한 사례이지만 혐의를 인정하지 않는 대법원 판결이 있었는데⁶⁾본 사례는 인정사례 항목에 기술하였으나 결론상으로는 불인정 사례에 해당하기는 하나 본질적으로 법리에 다소 해석 차이의 여지가 많아 앞의 인정사례와 비교를 위하

4) 대법원 2008도1013 판결, 2010도6068 판결 참조

5) 대법원 2008도5200 판결 참조

6) 대법원 2007도7480 판결 참조

여 인정사레 항목에 기술하였음) 당시 대법원은 컴퓨터 화면상 이미지는 전자적 반응을 프로그램 실행시에만 한시적으로 나타내므로 계속적이지 않아 형법상 문서로 볼 수 없다고 본 것으로 해당 사건내용을 살펴보면 피고인은 자신의 집에서 사귀고 있던 이성에게 피고인의 나이와 성명을 속이는 용도로 행사할 목적으로 권한 없이 컴퓨터로 ‘XX’, ‘70****’을 작성하여 출력한 다음 피고인의 주민등록증 성명란 ‘YY’라는 글자 위에 위와 같이 출력한 ‘XX’라는 글자를, 주민등록번호란 ‘64****’라는 글자 위에 위와 같이 출력한 ‘70****’이라는 글자를 각 오려붙인 다음, 이를 컴퓨터 스캔 장치를 이용하여 스캔함으로써 이미지 파일을 생성하는 방법으로 복사하여 컴퓨터 모니터로 출력함으로써 화면에 이미지가 나타나도록 하는 방법으로 공문서인 강남구청장 발행의 주민등록증을 위조하고 해당 주민등록증 이미지가 저장되어 있는 파일을 타인에게 보내는 이메일에 마치 진정하게 성립한 것 처럼 첨부, 전송하여 열람하도록 함으로써 컴퓨터 모니터에 위와 같이 위조한 주민등록증의 이미지가 나타나도록 함으로써 이를 행사하였다.

위의 사안에 대하여 대법원은 컴퓨터 모니터 화면에 나타나는 이미지는 이미지 파일을 보기 위한 프로그램 실행할 경우에 그 때마다 전자적 반응을 일으켜 화면에 나타나는 것에 지나지 않아서 계속적으로 화면에 고정된 것으로는 볼 수 없으므로, 형법상 문서에 관한 죄에 있어서의 ‘문서’에는 해당되지 않는다고 판단하였다.

그러나 필자가 위의 대법원 판단 논거를 검토해보면 앞서 이미지 파일을 문서로 볼 수 없다는 법리적 논거만으로는 전자의 대법원 판결과 배치된다는 점에서 다소 논란이 있어 이러한 점 외의 부분을 짚어보자면 우선 해당 사례에서의 문서 위조 수준이 조잡하여 이러한 위조 정도로는 위험성이 있다고 보기 어려워 혐의가 인정되기 어렵다고 보는 것이 합리적인 것이며 조금만 주의를 기울이면 수신자가 알아차릴 수 있었을 것을 기대할 수 있다고 할 것이며 또한 추가로 주민등록증 사용목적은 고려할 때 주민등록법⁷⁾상

공식적인 목적으로 신분확인 용도인 점을 감안할 때 단순히 개인이 사귀는 이성에게 나이를 속일 목적으로 개인에게 제시하는 주민등록증 이용행위가 주민등록법상 주민등록증의 불법사용이라고 보기 어려워 무죄로 판단하는 것이 더욱 타당하지 않을까 한다.

법원의 태도에 대한 검토 및 결론

앞서 살펴본 것과 같이 법원의 일관적인 태도는 형법상의 문서에 관한 죄에 대하여 말하는 문서란 지속적인 형태가 유지될 수 있어야 한다는 점을 중시하는 것으로 보인다. 즉, 모바일을 포함한 디지털 형태의 이미지 파일 등은 문서로서의 성질을 인정할 수 없다는 것이다.

그러나 이와 같은 대법원의 태도는 디지털 환경을 살아가는 현 시대의 흐름을 반영하지 못하는 측면이 있다고 할 수 있다.

실제 금융기관들의 경우 스마트폰으로 계좌 개설시 고객에게 주민등록증 등 신분증을 사진촬영하여 전송하여 개인 인증절차를 진행하며 심지어 대출의 경우도 신분증 사진파일을 제공하여 비대면으로 이루어지고 있는 것이 현실이다.⁸⁾

또한 디지털 시대로의 전환시기에 모바일 주민등록증이나 운전면허증 등 전자형태 신분확인 절차는 이미 현실화되어 진행 중으로 행정안전부에 따르면 2022.7.28.부터 전국 운전면허시험장 27곳과 경찰서 258곳에서 모바일 신분증 발급이 이루어지고 있고 주민등록증 역시 정부24 홈페이지에서 안드로이드 앱 버전과 아이폰용 앱 버전을 다운로드받아 설치가 가

기관, 지방자치단체, 공공단체, 사회단체, 기업체 등에서 해당 업무를 수행할 때에 다음 각 호의 어느 하나에 해당하는 경우로서 17세 이상의 자에 대하여 성명·사진·주민등록번호 또는 주소를 확인할 필요가 있으면 증명서류를 붙이지 아니하고 주민등록증으로 확인하여야 한다. 다만, 대통령령으로 정한 경우에는 그러하지 아니하다. 1. 민원서류나 그 밖의 서류를 접수할 때 2. 특정인에게 자격을 인정하는 증서를 발급할 때 3. 그 밖에 신분을 확인하기 위하여 필요할 때

8) 신분증 사본에 쉽게 뚫린다. 스마트폰 금융시대 구명난 보안(2022.4.29., 이성일 기자, MBC, <http://n.news.naver.com/article/214/0001193643>)

7) 주민등록법 제25조(주민등록증 등의 확인) ① 국가

능한 실정이다.

그러나 이러한 모바일 신분증은 디지털 파일 형태로 해당 화면을 다른 스마트폰으로 재촬영하여 편집하여 악용시 별도의 QR 코드 인증을 확인하지 않는 상당수 중소도매점 등에서는 청소년이 이를 이용하여 성인인 것처럼 주류나 담배를 구매하는 등의 불법을 자행하거나 범죄자들이 타인의 신분증임에도 자신의 것인 양 사용하여 원래 신분인 피해자에게 금전적 손해를 입히는 피해양산이 확대되는 수단이 되고 있기도 하다.⁹⁾

즉, 대법원의 현재 논리는 디지털 시대로의 급속한 환경변화를 제대로 반영하고 있다고 보기 어려운 것으로 현재의 형법상 위조 및 문서 부정행사의 범위에 복사문서 등을 포함하도록 법률을 개정한 것이 지난 1995년이라는 점을 감안(당시에도 복사기나 팩스가 도입되면서 시대적 법률환경 변화를 감안하여 복사문서 등을 포함하도록 개정)하면 위조 문서 등의 범위에 디지털 이미지 파일을 포함하지 않는다는 취지의 대법원 법리는 진중하게 재고가 필요할 것으로 보인다.

물론, 정부 차원에서도 법률개정 등 디지털 시대에 부합한 형법상의 문서 위조나 부정행사에 대한 문서 범위 변경 노력이 병행되어야 할 것이다. 즉, 현재의 형법 제237조의2를 개정하여 “이 장의 죄에 있어서 전자복사기, 모사전송기(팩스 등) 기타 이와 유사한 기기를 사용하여 복사한 문서 또는 도화의 사본 및 전자기기나 정보통신망 등을 이용하여 생성된 이미지 등 파일도 문서 또는 도화로 본다” 등으로 보다 현실적인 개정노력이 있어야 한다는 것이다.

지금까지 간단하게나마 모바일 등 디지털 형태의 문서에 관한 위변조와 부정행사 등에 대한 대법원의 법리 기준을 살펴보고 문제점을 검토해보았다. 법은 국가와 사회를 지탱하고 유지하는 역할을 하므로 함부로 임의해석하거나 마구잡이로 개정을 해서도 안되지만 시대를 반영하여 변화하지 않으면 현실과 괴리된 문제가 발생하는 것을 방지하는 우를 범하게 된다

는 점을 명심하여 보다 적극적인 차원에서의 대응을 위하여서라도 관계 기관에서 법률개정 시도와 함께 유사사건에 대하여 수사기관과 공소기관에서 보다 면밀하게 법리를 보강하여 대법원의 판단이 변화할 수 있도록 노력하기를 기대한다.[PSI](#)

9) 위변조 많은 모바일 신분증, 본격적으로 사용하기엔 아직 일러(2022.9.15., 이상혁 기자, 아이러브 PC 방)

연구소 소식

■ 영국 런던대학(UCL)과의 공동연구 추진

지난 4월 13일, 영국 런던대학(UCL)의 벤 브래드포드(Ben Bradford) 교수가 경찰학 연구협력 사업 추진을 위하여 치안정책연구소를 방문하였습니다.

이번 연구협력 주제는 ‘경찰 정당성 확보를 위한 절차적 정의 모델 구축’으로, 연구협력 민주적 경찰활동 모델을 구축한 후 치안 현장에 적용할 수 있도록 △경찰활동·홍보 정책 수립 △경찰관 교육방향 설정 △경찰 내부 조직문화 개선 방향에 적극적으로 활용할 계획입니다.



■ 전라북도자치경찰위원회 · 한국과학기술연구원 · 한국전자기술연구원과 업무협약 체결

지난 3월 30일 치안정책연구소는 전라북도 자치경찰위원회, 한국과학기술연구원, 한국전자기술연구원과 과학치안 활성화를 위한 업무협약을 체결하였습니다. 각 기관은 ▲과학치안 연구개발사업 추진 ▲수요개발 치안현장 적용기술 개발 ▲지역특화 치안문제 해결을 위한 아이디어 발굴 ▲과학치안 관련 정보 공유 및 정책자문 ▲지역치안발전을 위한 파트너십 구축 ▲과학치안 저변확대를 위한 세미나 공동 개최 등에 협력하기로 하였습니다.

이번 협약으로, 과학기술을 활용한 치안문제해결 연구개발 사업을 통해 지역 치안문제를 적극적으로 해결해 나갈 계획이며, 각 기관의 축적된 연구개발 노하우를 바탕으로 급변하는 치안환경에 선제적으로

대응할 수 있는 체계를 마련해 치안역량을 강화할 수 있을 것으로 기대됩니다.



■ 『국제경찰학 연구동향 리뷰 Vol.2』 출간



치안정책연구소(국제경찰 지식센터)에서는 외국 경찰의 다양한 정책 및 제도에 관한 학술적 연구를 분석하여 「국제 경찰학 연구동향 리뷰」 제2호를 발간하였습니다.

“실력 있고 당당한 경찰, 국민이 신뢰하는 안심공동체”를 만들기 위해 각 기능에서 노력을 다하고 있는 치안정책 실무자, 경찰관, 연구자들에게 인사이트를 제공할 수 있기를 희망합니다. 해당 자료는 치안정책연구소 홈페이지에서 자료를 열람하실 수 있습니다.

(<https://www.psi.go.kr/police/main.do>)

■ 치안 안전데이터 분석 경진대회 개최

지난 2월 28일 치안정책연구소와 대전·세종·충남(이하DSC) 지역 혁신 플랫폼이 공동으로 「제1회 지역 치안 안전 데이터 분석 경진대회」 시상식을 개최하였습니다

이번 경진대회에서는 4차 산업혁명 시대에 발맞춘

지역 치안 안전 데이터를 분석하여 우수한 아이디어를 발굴함으로써 지역 치안에 이바지하는 기술을 개발하기 위해 총 122팀이 참여하여 ‘DSC 교통사고 및 보이스피싱 분석 및 예측’을 주제로 진행하였습니다.

최종 6개 팀을 우수작으로 선발한 결과, ‘대상’은 신용평가모형을 통해 교통사고 위험지수와 등급을 산출하여 교통사고 예방 및 관련 정책을 제안한 ‘스트릿 교통과이티(양문일, 박희진, 최성원)’팀이 수상하였습니다.



■ 박재풍 경찰패널연구센터장 제18대 한국공안행정학회 신임 학회장 취임



지난 1월 한국공안행정학회를 이끌어갈 새 수장에 경찰대학 치안정책연구소 박재풍 경찰패널연구센터장이 선출되었습니다. 위 학회는 1987년 창립되어, 현재 약 700여 명의 박사급 회원들로 구성되어 경찰학·교정학·범죄학·범죄심리학 등 다양한 사회과학 영역에서 활동을 전개하고 있으며, 한국연구재단 등재학술지인 한국공안행정학회보를 발간하고 있습니다. 박재풍 경찰패널연구센터장의 한국공안행정학회장 취임을 축하하며, 건승을 기원합니다.

■ 2023년도 치안정책연구소 책임연구과제

치안정책연구소는 국내 유일의 치안종합 연구기관으로 효과적인 경찰활동에 필요한 정책수립과 연구개발에 노력하고 있습니다. 2023년도에도 새로운 치안 트렌드에 맞춰 효율적인 경찰활동에 이바지할 수 있는 연구성과를 도출하기 위해 시의적절한 연구주제들을 선정하여 연구를 진행하고자 합니다. 2023년 치안정책연구부의 책임연구과제로 아래와 같은 주제가 채택되었습니다. 연구주제와 관련하여 문의 또는 고언을 주실 분들은 아래 연락처로 언제든지 연락해주시길 바랍니다.

(chajj76@police.go.kr, 041-968-2794)

연번	과제명	연구관
1	자율방범대 법률 시행에 따른 운영 실효성 증대를 위한 교육 및 보상 방안 연구	강용길 조정혜
2	역량기반 교육 전환을 위한 경찰 위기관리 역량 모델 연구	조정혜 강용길
3	경찰의 안보수사 업무영역 및 조직 재정비 방안	권오국
4	인파사고 관리의 새로운 정책 방향	황규진
5	경제안보 확립을 위한 중요 산업기술 유출 방지 및 보호 강화방안	성진기
6	외국인에 의한 마약류 국내 유입 원인 분석을 통한 경찰의 실효적 대응	김학신
7	층간소음범죄의 특성과 경찰의 대응방안에 관한 연구	김성희
8	가정폭력이 강력범죄(미수, 치사)로 발전하는 요인에 관한 연구	김혜진
9	경찰서 통합수사팀 확대 실시의 착안점	정웅
10	형사 전자소송 실질화를 위한 법제도 개선 방안에 관한 연구	차종진
11	한국경찰의 개인 및 조직특성에 관한 패널연구	박재풍 박주혁
12	경찰 정당성 확보를 위한 절차적 정의모델 구축	박재풍 박주혁

■ 치안정책연구소 2023년 상반기 전입직원

2023년 상반기 경찰대학 치안정책연구소에 연구업무 및 기획·행정업무를 위해 총 13명의 신규 직원이 전입하였습니다. 향후 치안정책 및 치안과학기술 연구영역에서의 왕성한 활동을 기대합니다.

구분	전입자	
치안정책 연구부	권도이 연구관(국제경찰지식센터장) 황규진 연구관(사회안전·안보연구실) 조정혜 연구관(법·정책연구실)	
과학기술 연구부	송경호 연구관(스마트치안지능센터) 김창식 연구관(스마트치안지능센터) 이서영 연구관(스마트치안지능센터)	
기획운영과	이윤석 경정 김정현 경사 박성근 경감 김학곤 경사 김병순 경사 이혜인 경장 김윤덕 행정관	

「치안정책리뷰」 원고 모집 공고

본 지에 실린 내용은 집필자 개인의 견해로서 치안정책연구소의 공식입장과 다를 수 있습니다. 치안정책리뷰는 치안정책연구소 홈페이지에서 다운로드 받으실 수 있습니다. (www.psi.go.kr)

□ 원고모집 안내

치안정책리뷰에서는 다양한 치안관련 원고를 모집합니다. 심사를 통해 게재된 원고에 대해서는 소정의 원고료, 또는 기념품을 드립니다. 많은 참여 부탁드립니다.

□ 보내실 내용

- 치안관련 논문 요약본
- 치안정책관련 칼럼
- 일선 현장의 이야기
- 해외 경찰관련 자료 및 경찰활동 사례
- 기타 치안정책관련 동향 및 의견

□ 보내실곳

- 담당 연구관 : 차종진(편집팀)
- e-mail : chajj76@police.go.kr
- 메신저 등 : 치안정책연구소 차종진 연구관 (041-968-2794)