ISSN 2951-2727

치안과학기술리뷰

Police Science Technology Review

통권 5호 | 2023. 10. VOL.02

부제 : 스마트치안과 AI

경찰대학 치안정책연구소

치안과학기술리뷰

통권 5호 | 2023. 10. VOL.02

CONTENTS

만든 사람들
발행처 / 치안정책연구소
발행인 / 최종상
편집인 / 배순일
편집위원 / 장광호
임경원
김희두
송경호
이상옥
김창식
김완중
최주현
김재후
이서영
문의 / 스마트치안지능센터
041.968.2397
발행일 / 2023년 10월 16일
디자인·인쇄 / 디자인글꽃

https://www.psi.go.kr

스마트치안지능센터의 발자취와 갈 길

치안정책연구소 과학기술연구부 스마트치안지능센터장 장광호

Ⅰ 부서의 연혁

치안정책연구소는 1980년부터 경찰대학 부설 연구기관이었다. 경찰대학 교육에 대한 연구를 하는 것이 주 임무였다. 역할이 크게 두 번 정도 변했다. 1997년 경찰 개혁이 화두였던 때다. 경찰의 제도 개선, 법령 검토 등에 대해 정책 연구가 활발해졌다. 경찰대학 부설이지만, 경찰청 부서들에게서 연구 요청을 받고 연구 결과를 환류하게 되었다. 두 번째 변화는 2015년이다. 경찰법 개정으로 경찰청도 과학기술연구를 할 수 있는 정부부처가 되었다. 과학기술 연구를 관리하고 평가하고 직접 연구할 부서가 필요했다. ICT, 화학, 교통공학 등 과학기술연구 인력을 채용하고, 부서를 갖춰나갔다.

스마트치안지능센터는 과학기술 연구 조직의 가장 큰 기대를 받았던 조직이다. 조직을 어떻게 구성해서 무엇을 할지 기획연구를 했다.[1] 경찰의 부서 창립치고는 드문 일이다.

당시 기본 구상은 경찰의 모든 데이터를 모아서, 통합 분석하는 기술 조직을 지향했다. 당시 연구소장이었던 민갑룡 전 경찰청장에 따르면 '경찰청 특정 부서가 데이터를 통합하면 빅브라더, 정보 침해 등 쟁점이 있을 수 있으니, 연구소에서 통합 분석을 해야 한다'는 취지였다.

경찰의 주요 데이터(KICS, 112, 교통, 과학수사, 사이버 등)를 모아서 분석하고, 직접 기술 연구는 물론, 경찰과 국민들이 활용할 수 있는 서비스를 제공하는 것도 목표로 했다. 3년간 100억 원 정도를 투입해 인프라를 구축하고 연 5억 운영비를

1) 치안정책연구소, 스마트치안지능센터 설립 기본구상 (2016.12)

투입하기로 계획했다. 총경이 부서장이 되어 연구직(9명), 경찰관(4명)이 센터를 만들기로 했다.

필자는 2018년 치안정책연구소에서 일하기 시작했다. 스마트치안지능센터를 구성하고자 당시 치연에 발령받은 임기제 공무원(4명)과 비정규 TF로 시작했다. 2019년 경찰관 9명을 경찰청에서 정원 조정으로 배치하여 정식으로 발족했다. 운영예산은 2019년부터 매년 시험연구비 1.5억 원을 받아 SW 임대, 출장비, 자문비 등 운영했다.

경찰청 데이터는 112신고데이터를 연계해 전송받고 있다. 사실상 빅데이터로서 안정적으로 분석할 수 있는 유일한 데이터이다. 112상황실의 열린 자세와 지원에 깊이 감사드린다. KICS 데이터는 형사사법전자화촉진법 상 수사 목적 외에는 사용할 수 없다. 2019년 전화사기 분석을 위해 관련 데이터만 1회 제공받았다. 우리 센터는 필자를 비롯 수사경과 경찰관들이 여러 명 있고, 현장에서 요청하는 사건을 분석하는 일을 하고 있다. 그런 역할을 인정받아 KICS데이터를 연계하고자 했으나, 법령 해석의 차이, 보안 장비 설치 요청, 경찰청 수사운영담당관의 통제하에 데이터를 사용해야 한다는 지침 등에 따라 연계를 하지 못했다. 과학수사·사이버 부서 역시 KICS 연계데이터로 같은 방침을 따르고 있다.

KICS를 비롯 경찰청 데이터를 추가 연계하기 위해서는 법률 개정 뿐 아니라, 조직 문화의 변화, 우리 센터의 역량 발전이 필요하다.

Ⅱ 역량 발전 과정

데이터 분석 부서를 운영한다는 것은 오랜 시간의 계단을 만들어 한발 한발 딛고 올라가는 것과 비슷하다. 112 데이터를 활용해 치안에 활용할 AI를 개발하는 지난 과정을 돌아보자. 데이터 연계를 위해서도 오랜 시간의 협의와 연계장비의 구축 등 인프라를 구성했다. 전송받은 귀중한 데이터를 분석

※ 2016년 구상(왼쪽)과 현 실정과의 비교(오른쪽)

하기 위해 우리 센터가 분석할 수 있는 기본 SW를 배워야 했다. 경험이 없고 기술 역량이 부족한 신임 연구자들이 처음부터 배워서 걸음마하게끔 기다려 주지 않기에 전문 역량을 갖춘 협력 연구기관들과 협업했다. 한국전자통신연구원(ETRI)이 대표적이다. 이곳은 112신고 등을 활용해 시공간 범죄 위험을 분석하고, 신고량을 예측하며, 신고내용을 AI로 자동 분류하는 기술을 만들었다.[2] 공학자들의 연구를 견식하며 그들이 개발한 소스 코드를 실제 112신고에 적용하는 것을 배우면서 역량을 키웠다.

우리 센터는 경찰 데이터를 반출하지 않고, 치연 안에서 분석한다. 협력 기관이 샘플 데이터로 개발한 프로그램을 실제 데이터와 사건에 적용하는 것을 우리 역할로 한다. 이 과정을 통해 기술을 습득하고 R&D에서 그친 산출물을 사실상 실용화할 수 있다. 차량번호판 분석 시스템이 대표적이다. 전자통신연구원이 주관한 과제[3]의 세부 산출물인 NPDR(Number Plate Deep Resolution)을 센터에서 1년간 작동해보면서 절차를 확립하고 경찰 내부망에 정보화시스템으로 만들어냈다.

수탁연구를 참여하면서 습득한 역량을 제안해서 과기정통부 기금 사업이나 연구개발을 주관했다. 2020년부터 3년간 지능정보사회진흥원(NIA)에서 지원하는 스마트치안빅데이터 플랫폼을 구축했다.[4] 2016년 설립 기본구상에서 제시한 인프라를 정부 예산으로 확보하지 못했기에 기금 사업을 통해 데이터 분석 기반을 만들려 했다.

2021년부터는 실제 현장과 시민들에게 서비스를 제공해봤다. 전화사기대응 시스템[5]이다. 관련 분야에서 활동하는 기업을 관리해 112신고나 민간에서 수집하는 악성앱 등을 경찰관들이 분석하게 하고, 시티즌코난이라는 악성앱 탐지 어플을 제공했다.

2022년에는 국가연구과제 주관기관을 맡았다. 빅데이터 기반 보이스피싱 정보수집 및 수사지원 시스템이다. 녹음음성, 공개 데이터를 활용해 경찰이 활용할 기술을 만드는 것이 목표이다. 경찰 내 연구기관이 책임자이기에 112신고 등을 활용해 범죄 발생을 추적하고, 실제 사건 녹음음성과 데이터를 활용하고 있다. 공학 연구기관들을 참여 기관으로 구성하고, 전체 분석 개발의 방향을 정하고, 실제 데이터에 적용해 성능을 높이는 역할을 하고 있다. 치연의 존재 의의에 맞는 역할을 하고 있다고 자부한다.

지난 5년간 책상 하나 없이 시작했던 첫 시작을 생각하면 감개무량하다. 모두 동료들 덕분이다. 따뜻하면서도 컴퓨팅 학자로서 연구를 놓지 않는 배순일 과학기술연구부장님의 지도 덕택이다. 현장에서 데이터 분석의 갈증을 느끼고 출범 원년 멤버로서 함께 해준 김희두 경위 역할은 엄청나다. 협력 기관이 제출한 소스를 이해하고 적용하면서 시스템을 만들어 간 것은 김 경위 역할이 대부분이다. NPDR을 고도화하고 있고 센터와 다른 부서, 기관과의 소통에 기여하는 최주현 경장은 센터의 분위기를 밝게 해준다. 김완중 행정관은 쟁점이 많은 빅데이터 플랫폼 사업을 묵묵히 이끌어 궤도에 올려주었다. 이상옥 경사는 복잡 다양한 인프라를 정비해주고 산출물이 많아지는 시기에 점점 더 많은 역

2) 정보통신기획평가원 과제, 「범죄 위험 상황 초기 인지 및 대응 시스템 개발」, 2018~2021

3) 정보통신기획평가원 과제, 「다중로그 기반, 범죄대응 플랫폼 개발」, 2017~2019

4) 2020~2022, 지능정보사회진흥원, 스마트치안 빅데이터 플랫폼 및 센터 구축 사업

5) 2021년, 지능정보사회진흥원, AI 기반 전화사기대응 플랫폼 구축 사업

할을 해주고 있다. 보이스피싱 대응 연구의 실무를 맡아 커다란 참여집단을 밀어가고 있는 김창식 경사와 김대호, 김서연 연구원께 감사드린다. 112데이터의 음성-문자 전환을 비롯, 비정기적으로 제시하는 연구수요를 관리하는 이서영 순경의 영입은 센터의 행운이다. 경찰관 중심으로 장기 근무자들이 많은 센터의 취지상 과학연구부의 서무를 맡아주는 송경호 경위에게는 앞으로 국제 치안 기술 협력 역할도 기대하고 있다. 전화사기 악성앱 시티즌 코난을 피싱 통화, 인터넷사기, 몸캠피싱, 로맨스피싱 등으로 고도화하는 서비스를 기획한 김재후 행정관은 어마어마한 쟁점을 견뎌가며 병원에 2번씩이나 다녀왔다.

모두에게 감사하고, 송구하다. 6년째 한 자리를 지키며 많은 이들이 머물다 갔다. 데이터분석이 그리 멋진 일이 아니다. 데이터 수집이 업무의 70%이다. 누군가에게 사정하고 설득하고 부탁한다. '연구-행정-사업자'를 오가는 일상이다. 빅데이터, 인공지능은 사람의 판단을 자동화하고 대신하는 것을 지향한다. 사람보다 나은 컴퓨터를 만들려면 뛰어난 사람이 있어야 한다. 뛰어난 사람은 영입하거나 육성한다. 충남 아산에 있는 공무원 조직에서 뛰어난 사람을 쉽게 영입하겠나? 의욕과 학습능력이 있는 이들과 함께 익히며 육성하고 성장해야 한다. 데이터 연구기관의 역량이란 고성능 컴퓨터나 분석 SW가 아니라 오랫동안 경험과 실력을 키워온 사람이다.

Ⅲ 가야 할 방향

지난 5년간 기반을 닦았다. 인프라 구축을 위해 외부 과제를 수탁해 여러 목표를 동시에 운영했다. 앞으로는 지금 해오고 있는 분야의 실력을 높혀야 한다. 키워드는 AI, 디지털 범죄, 스마트치안 플랫폼이다.

첫째, AI 연구를 심화해야 한다. 가상 데이터에 적용하는 AI는 활용도가 떨어진다. AI는 실제 사례로 학습해야 한다. 실제 경찰데이터와 범죄데이터를 활용하는 우리 센터가 반드시 해야 한다. 경찰 내외 어디에서도 하기 어렵다. 기관에 실제 데이터를 맡길 수 없다. 경찰이 쓰는 문서를 이해해서 분류하고 생성하는 치안 자연어 AI를 개발하고 있다. NPDR 등 영상 AI 등도 연마하고 있는 영역이다.

둘째, 디지털범죄에 대한 대응이다. 오프라인의 범죄는 거의 줄어들고, 보이스피싱, 스미싱, 인터넷사기, 몸캠피싱, 로맨스스캠, 디지털성범죄가 일상이다. 기술은 자본과 욕망에 따라 움직이는데 디지털 범죄는 자본과 욕망이 들끓는 곳이다. 범죄는 디지털 전환하고 있다. 상하이, 연변, 선진, 필리핀, 베트남, 일본 등에의 외곽에서 피싱범들이 콜센터를 차리고, 시나리오를 기획한다. 월 3억 원을 들여 대용량 서버를 운영한다. 범죄조직이 인공지능과 디지털 플랫폼을 활용하는데 경찰 활동은 전환하고 있나? 디지털 범죄에 대한 경찰활동을 선제적으로 대응하는 기술 개발을 해야 한다.

셋째, 스마트치안 플랫폼이다. 경찰데이터를 직접 운영하는 스마트치안지능센터와 영상·음성·문서 등 영역에서 기술력을 갖춘 기업과 연구기관이 협업하는 연계 체제이다. 보이스피싱 등 디지털범죄에 대응하는 기술을 공동 개발하고 데이터 플랫폼을 통해서 데이터를 주고받을 수 있다면 대국민 안전에 기여할 것이다.

이런 목표를 공유하며 지나온 지난 5년보다 보람있고 성장하는 5년을 만들어가길 바란다. 새로운 목표를 향해 함께 걸어가기 위해 무엇이 필요할까? 애정과 관심이다.

거대한 데이터, 대용량 서버보다 귀중한 것이 발전할 역량과 의욕을 갖춘 사람이다. 인공지능, 빅데이터…모두 사람이 하는 일이다. 동료들을 가치있게 인정하고, 서로 다른 일을 하는 이들에 대한 따뜻한 관심이 필요하다.

지나온 5년이 동료들 덕택이었듯 앞으로 5년도 동료들의 힘으로 발전하리라 믿는다. PSI

보이스피싱에 대한 기술적 접근

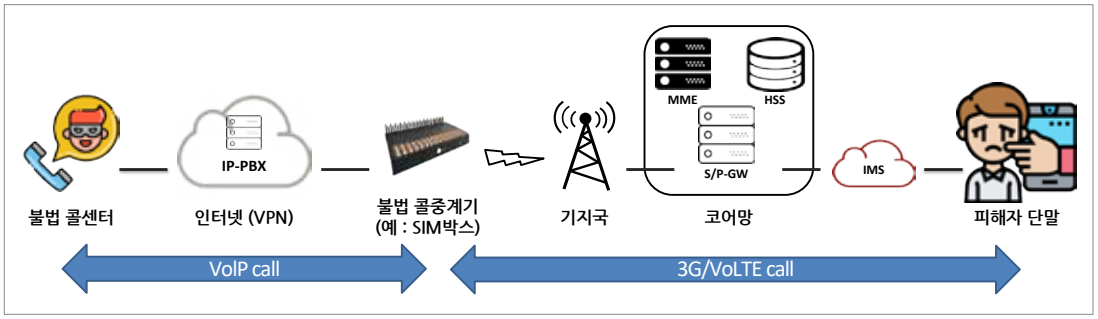
한국과학기술원 전기 및 전자공학부 정교수 김용대

I 보이스피싱 범죄

보이스피싱은 국내에서 매년 수천억의 피해를 입히고 있다. 정부와 통신사는 수년간 다양한 기술을 개발하며 이를 방어하려 노력을 했으나 그때마다 범죄자들은 새로운 우회 방법을 개발하여 왔다. 본고에서는 보이스피싱 범죄에 대해 기술적으로 분석을 하고 우회가 어려운 예방, 추적 등의 해결책에 대해 알아보고 향후 기술 발전 방향에 대해 논의한다.

1. 보이스피싱 범죄 현황

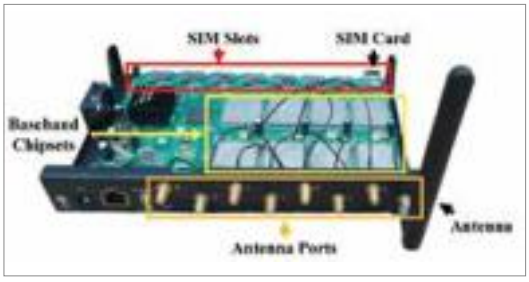
2006년부터 급증한 것으로 알려진 보이스피싱은 2011년 피해액이 437억에서 2021년에는 7,700억으로 지난 10년간 17.6배 증가하였다. 정부, 경찰청, 통신사는 보이스피싱 대응을 위하여 다양한 예방, 방지 및 수사 기법들을 개발해 왔으나 범죄자들은 이를 피하기 위한 기술을 계속 개발해 왔다. 본 고에서는 먼저 보이스피싱에 대한 몇 년 간의 기술적 변화에 대해 요약해 본다. 그리고 이들 기술을 바탕으로 단말과 네트워크에서 보이스피싱 범죄를 탐지, 예방, 추적할 수 있는 기술에 대한 다양한 방향성에 대하여 논하고자 한다.



〈그림 1〉 보이스피싱 범죄의 네트워크 구성도

2. 보이스피싱 범죄 기술

〈그림 1〉은 가장 대표적인 보이스피싱 범죄에 대한 시스템 구성도이다. 그림에서 VoIP call 구간은 인터넷 전화 구간으로 불법 콜센터는 주로 한국 이외의 장소에서 설치되어 운영된다. 그림에서 불법 콜중계기라고 불리우는 시스템은 인터넷 전화(VoIP Call)을 3G 혹은 VoLTE 기반의 이동통신 전화로 변환하여 주는 시스템을 의미하며, 현재까지도 가장 많이 사용되는 콜중계기는 심박스이다. 과거에는 해외에서 직접 인터넷 전화를 통해서 보이스피싱을 했었으나 해외 발신 통화를 표시하고 070 전화를 사람들이 직접 안 받게 되면서 심박스가 주요 통신 수단으로 이용되고 있다. 심박스는 국경을 인터넷 전화를 통하여 통과하여 이동통신 과금우회를 할 수 있어, 유럽에서는 주로 과금회피사기(Bypass Fraud)에 많이 사용되었었다.



〈그림 2〉 심박스

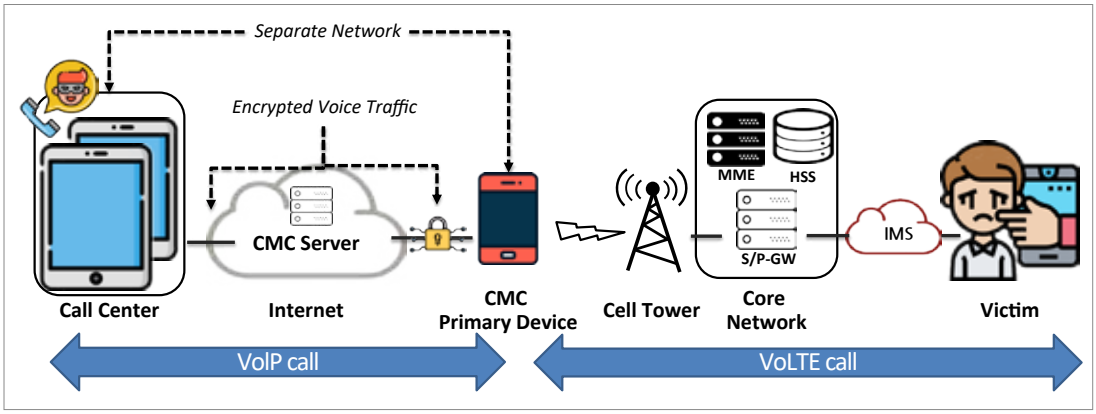
심박스는 〈그림 2〉에서 보는 것과 같이 다수의 안테나, 이동통신 칩셋, 심카드 슬롯, 그리고 이더넷 포트로 구성되며 심카드 슬롯에는 주로 심카드가 꽂힌다. 최근에는 심박스에 심카드를 직접 장착하는 대신 심뱅크라는 장비를 해외에 두고 원격으로 심카드 관련 연산을 수행한다. 뿐만 아니라 다수의 심박스의 운용을 편하게 하기 위하여 심서버라는 소프트웨어를 이용하여 원격에서 다수의 심박스를 관리한다. 초기에는 64회선 등 다수의 회선을 포함한 심박스 장비가 주로 사용되다가 시간이 가면서 작은 회선 수를 갖는 심박스를 "쉽게 돈 벌 수 있는 부업"등으로 유도해 가정에 설치를 하도록 하는 경우도 많이 보이게 되었다.

〈그림 3〉은 전반적인 보이스피싱 범죄의 진행에 대해 설명을 하고 있다. 제일 먼저 개인 정보 유출 등을 통하여 피해자를 선정한다. 예를 들어 저축은행 고금리 대출자 등이 타겟이 될 수 있다. 다음에 피해자에게 전화를 해서 사회 공학적 기법을 이용하여 신뢰를 얻는다. 예를 들어, 고금리 대출을 저금리 대출로 바꾸어 주는 것 같이 피해자가 필요로 하는 것을 제공한다. 범죄자는 이미 피해자의 다양한 개인 정보를 가지고 있어 조금 더 신뢰를 할 수 있는 시나리오를 작성할 수 있다. 피해자들은 시나리오에 속아 통화 하이재킹 기능이 포함된 악성앱을 설치한다. 이 기능은 현재는 통신사 권한을 갖

〈그림 3〉 보이스피싱 범죄의 일반적 진행

는 앱만 쓸 수 있는 기능으로 개선이 되었으나 과거 API를 이용할 경우 현재도 구현이 가능하다. 보이스피싱 공격자들은 시나리오로 설득을 시키고 악성 앱 설치를 유도한다. (예를 들어, 재난지원금을 받고 싶으면 이 앱을 설치해 달라고 한다.) 앱 설치 후에는 오고 가는 모든 통화에 대해 제어가 가능하다. 특히, 은행, 경찰, 검찰 등에 대한 통화가 이들 기관 대신 모두 해외 콜센터로 연결이 된다. 따라서 의심을 하던 보이스피싱 피해자도 은행, 경찰, 검찰과 통화를 했다고 생각하여 의심이 안심으로 바뀌는 결과를 낳게 한다. 악성앱은 안드로이드 API에서 허용된 기능을 이용하여 오는 전화나 가는 전화의 전화 번호를 수정한다. 즉, 114에 전화를 하더라도 해외 보이스피싱 콜센터로 통화가 될 수 있는 기능을 구현하고 있다. 이러한 전화 탈취 기능은 피해자의 의심을 해소하는 결정적 역할을 하는 것으로 알려져 있다. 충분히 설득이 되면 범죄자들은 송금이나 대면으로 피해자로 부터 편취를 하게 된다.

심박스를 대신하여 2~3년 전부터 삼성 기기에서 지원이 되는 CMC(Call and Message Continuity) 기능을 이용한 보이스피싱 또한 늘어나고 있다. (<그림 4> 참고) 이 기능은 심박스 대신 휴대폰을 게이트웨이로 이용한다. 그리고 해외 콜센터의 인터넷 전화는 태블렛 같이 심카드가 없는 장비로 대체된다. 통화를 위해서 3G를 사용할 수 밖에 없었던 심박스의 경우 3G를 사용하는 기기가 거의 없어 LTE를 사용하는 다른 기기와 다른 3G 주파수의 전파 탐지를 통하여 추적을 할 수 있었다. 하지만 CMC를 사용하는 경우 LTE 혹은 5G 신호를 이용



〈그림 4〉 CMC 기술을 이용한 보이스피싱

하기 때문에 다른 기기와 주파수 측면에서 구분하기 힘든 점이 있다. 뿐만 아니라 콜센터와 제조사의 CMC 서버와의 통신, 서버와 휴대폰과의 통신이 암호화되어 있어 단순 심박스를 이용할 때보다 이 방법은 좀 더 분석이 힘들다. 그렇지만 제조사의 지원이 있을 경우 수사에 더 큰 도움을 줄 수 있다. 뿐만 아니라 최근 발표된 정부 정책은 보이스피싱에 사용된 휴대폰을 기기 식별 번호를 이용하여 네트워크 접속을 막을 수 있게 되었다. 이로 인하여 휴대폰을 이용하는 CMC 기반의 방식이 심박스를 이용하는 방식보다 덜 효과적인 것으로 분석되고 있다.

Ⅱ 보이스피싱 범죄 해결책

1. 단말기 기반의 해결책

모든 보이스피싱 범죄는 피해자의 휴대폰 단말기를 통해서 이루어지므로 예방을 위하여 가장 좋은 플랫폼은 휴대폰 단말기라고 생각한다. 휴대폰 단말기에 탑재되는 솔루션은 일반 앱 개발 회사, 통신사, 제조사, 운영체제 제조사 등 다양한 레벨에서 구현이 가능하다. 악성앱이 설치될 수 있는 휴대폰은 에코 시스템의 개방성을 이용한 안드로이드 휴대폰 밖에 없기 때문에 운영체제는 안드로이드라고 가정한다.

우리나라의 다양한 앱 개발사들이 보이스피싱 악성앱 탐지 솔루션등을 개발하고 있으며 안티바이러스 회사들 또한 악성 코드 탐지의 일환으로 악성앱을 탐지하고 있다. 최근 조사[1]에 따르면 16.4% 정도의 보이스피싱용 악성앱들이 탐지되었다. 이들의 탐지율이 높다고 할 지라도 휴대폰에서 안티바이러스를 사용하는 경우는 거의 없기 때문에 그리고 누구나 보이스피싱의 대상이 될 수 있기 때문에 단말기에 설치되는 보이스피싱 솔루션은 운영체제 회사, 플랫폼 회사, 통신사들이 설치하는 선탑재 앱에 포함되어야 한다고 생각한다. 불행히도 운영체제 회사인 구글은 (대부분 우리나라 문제인) 국내의 보이스피싱용 앱 탐지 혹은 기능의 방지에 큰 관심이 없는 것으로 보인다. 사실 가장 많은 리소스에 접근할 수 있는 회사가 구글이라 이 부분은 매우 안타까운 일이다. 그렇지만 통신사들과 일부 휴대폰 제조사가 관심이 있는 것은 매우 고무적인 일이다. 이 장에서는 통신사들과 제조사가 할 수 있는 해결책에 대해 간단하게 논하고자 한다.

이들은 안드로이드 API를 사용하는 앱의 경우, 어떤 권한으로 어떤 API를 쓰는지는 알 수 있지만 구체적으로 어떤 파라메터로 그 API를 부르는지는 알 수가 없다. 몇몇 통화용 앱들이 비슷한 API를 쓰는 경우가 많아 API 만을 봐서는 오탐이 생길 가능성이 높다. 이런 이유로 지난 조사[1]에서도 AOSP에서 파라메터들을 볼 수 있다고 가정을 했지만 이런 방어는 구글만이 가능하다. 따라서 오탐을 줄이면서 악성앱을 줄이는 솔루션은 반드시 필요하다. 물론 통신사와 제조사 입장에서는 프라이버시 문제가 있을 수 있기 때문에 클라우드보다는 온디바이스 탐지가 조금 더 선호된다고 생각한다.

악성 앱 탐지 이외에 단말기에서 고려할 수 있는 솔루션으로는 통화 내용을 자동으로 분석하고 사용자에게 경고를 주는 시스템이다. 물론 통화 내용을 클라우드에서 분석을 하면 프라이버시 침해 문제가 생기므로 온디바이스에서 구현이 필요하다. 이 기술은 크게 STT(Speech-to-Text, 즉 목소리를 텍스트로 바꾸는 기술), 그리고 텍스트를 이해하고 기존 시나리오와 매칭을 하는 자연어 처리 기술이 필요하다. 최근 LLM 등의 발전과 함께 자연어 처리 기술이 비약적으로 발전을 했고, 따라서 위 두 가지 기술을 클라우드를 이용해 구현한다면 그

리 어려워 보이지 않는다. 다만 이 기술을 온디바이스에 구현을 해야 하고, 온디바이스 솔루션의 경우 배터리 소모가 최소화되어야 하는 부분이 중요한 숙제로 남아 있을 것 같다. 다만 최근까지 자연어 처리의 비약적 발전은 내용을 분석하고 사용자에게 경고를 줄 수 있는 시스템 또한 가능할 것으로 보인다.

온디바이스에서 선탑재 프로그램을 이용하여 악성앱을 탐지하고 보이스피싱 시나리오를 탐지하는 것이 시급하지만 어려운 숙제로 남아있다.

2. 네트워크 기반의 해결책

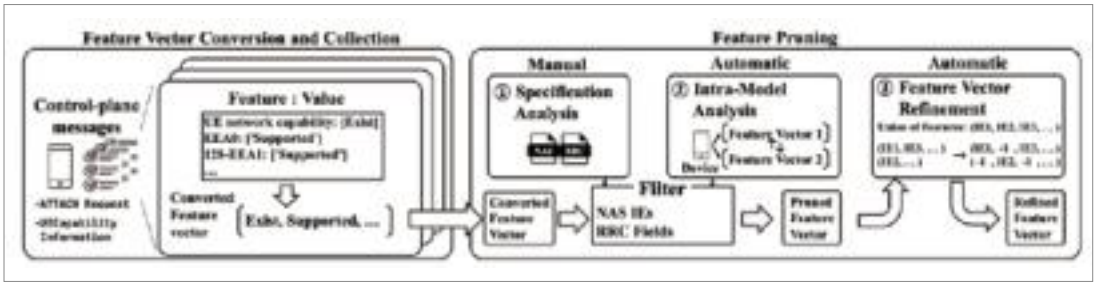
보이스피싱의 가장 중요한 특징은 이동통신을 이용하는 범죄라는 것이다. 따라서 다양한 해결책이 이동통신을 매개로 구현 가능하다고 생각한다. 본 장에서는 이동통신을 이용한 해결책에 대해 생각해 보고자 한다.

심박스는 이동통신 기지국과 코어망에게는 휴대폰 같아 보인다. 이더넷에 연결이 되어 있으므로 인터넷에서 보면 임베디드 기기 같아 보인다. 심박스를 이용하는 모든 행위가 불법인 것은 아니다. 예를 들어 콜센터 혹은 해외지사 등에서 심박스를 이용할 수 있다. 문제는 보이스피싱에 사용된 심박스를 찾아내는 것이 궁극적 목표라고 할 수 있다.

보이스피싱 예방에 쓸 수 있는 가장 강력한 방법은 심박스가 이동통신 네워크에 접근을 할 때 탐지를 하고 접속을 못하게 하면 된다. 물론 이 경우 앞에서 언급한 합법적인 사용자에 대해 어떻게 하느냐에 대한 문제가 존재한다. 이를 해결하기 위해서 합법적으로 사용을 하고자 하는 사업자는 등록을 하고 사용을 하는 심박스등록제를 실시하면 된다. 이 경우 등록하지 않고 사용하는 심박스는 네트워크에 접속을 못하게 하면 된다. 그럼 어떻게 심박스와 다른 이동통신 기기의 구별이 가능할까? 휴대폰 등은 매우 비싼 베이스밴드를 쓰고 매년 다양한 기능 추가를 하는 것에 반하여 심박스들은 그런 노력을 하는 것이 힘들다.

카이스트 연구팀은 이동통신 제어평면의 메세지를 이용하여 심박스와 휴대폰을 구분할 수 있음을 입증하였고[2], 이를 이동통신사에서 실제 실험하여 이동통신 네트워크에서 탐지하려는 노력을 하고 있다.

두 번째로 이동통신 네트워크에서 가능한 해결책은 물리적 위치 추적이다. 현재 심박스는 3G 통신을 사용하고 대부분의 휴대폰은 4G LTE나 5G를 이용하기 때문에 신호적으로 구분이 가능하다. 그렇지만 LTE나 5G 통신 기기를 사용할 경우 위치 추적은 어렵다. 이 경우 많은 이동통신 기기 중 특정한 기기를 어떻게 찾느냐가 어려운 문제로 남는다. 이 기술을 구현하는 데는 몇 가지 큰 어려움이 있다. 먼저 특정 사용자의 이동통신 ID를 알아



〈그림 5〉 핑거프린트 생성 방법

내는 방법이다. 이 문제는 전화 번호로부터 이동통신 ID를 알아내는 기존 연구들로 부터 힌트를 얻을 수 있다. [3, 4] 두 번째 어려움은 실제로 위치 추적 기술을 개발하는 것이다. 어떻게 특정 사용자의 위치를 추적할 수 있을까? 여기에서 가장 중요한 힌트는 모든 휴대폰은 기지국으로 상향 신호를 보낸다는 것이다. 언제 어느 주파수에 상향 신호를 보내는 지 알 수 있다면 특정 사용자의 신호를 구분할 수 있고, 이 신호를 구분할 수 있다면 지향성 안테나 등을 이용하여 위치 추적 기술을 개발할 수 있을 것으로 생각한다. 기술적 난이도는 상당히 높을 것으로 생각하지만 방향 탐지 산업이 일반적으로 하는 일이 특정 신호에 대한 위치 추적이므로 완전히 새로운 연구 방향이라고 생각하지는 않는다.

세 번째는 보이스피싱에 사용하는 심박스가 연결하는 심서버의 인터넷 주소를 알아내는 것이 중요하다. 이 경우 국제 공조 등을 이용하여 해외에 직접 수사를 할 수 있기 때문이다. 문제는 피해자 신고로 부터 이동통신 식별자는 알아낼 수 있겠지만 유선 인터넷 주소를 알아 낼 수 있는가 하는 것은 어려운 문제로 남아 있다. 그렇지만 이 문제 또한 다양한 해결이 가능할 것으로 생각한다. 심박스 한 대를 물리적으로 압수한 경우 이 심박스가 연결하는 심서버의 인터넷 주소를 알 수 있다. 혹은 통화 내용에 특정 패턴의 네트워크 트래픽을 주입하여 그 패턴을 유선 인터넷에서도 찾을 수 있다. 이 기술을 네트워크 워터마킹이라고 하고 과거에 Tor 등에 대한 연구를 위해서 사용되었었다.

보이스피싱을 위해 이동통신은 핵심적인 인프라이다. 핑거프린팅을 통한 심박스 접근 제어, 물리적 위치 추적, 네트워크 워터마킹은 보이스피싱 예방, 수사를 위한 핵심적인 네트워크 기술이라고 생각한다.

Ⅲ 결론

본 고는 보이스피싱 기술의 변화에 대하여 먼저 살펴보았다. 심박스, CMC 로 대표되는 지난 몇 년간의 기술은 앞으로 또 어떻게 변할 지 정확하기 알기는 힘들다. 그리고 우리는 단말과 네트워크에서 보이스피싱에 대한 해결책에 대하여 살펴 봤다. 단말기 해결책은 빠른 시간 내에 구현이 될 경우 예방에 큰 도움이 될 것으로 생각한다. 보이스피싱은 이동통신을 이용할 수 밖에 없기 때문에 네트워크 기반 해결책은 보이스피싱 해결을 위해 가장 중요한 연구주제라고 생각한다. 본 고에서 제시하는 3가지 해결책이 빨리 구현이 되어 예방 및 수사에 도움이 되기를 바란다. 2021년 7,700억 원의 피해를 줬던 보이스피싱 범죄는 서민들에게 다양한 어려움을 주고 있다. 기술적으로 범죄자의 변화를 예측하는 계층적 기술 개발(Layerd Defense)을 통하여 보이스피싱에 대한 기술적 해결이 실제로 이루어 지기를 바란다. [1] PSI

1) 본 고는 2021년 Security@KAIST 보안의 현재와 미래 세미나 발표자료를 바탕으로 작성되었으며, 2023년 OSIA ST&R 저널 내용이 재수록 되었음.

참고 문헌

[1] 김용대, “보이스피싱: 범죄, 예방, 탐지, 추적 …”, Security@KAIST 보안의 현재와 미래 2021 세미나

[2] Joongyum Kim, Jihwan Kim, Seongil Wi, Yongdae Kim, Sooel Son. HearMeOut: Detecting Voice Phishing Activities in Android. 20th ACM International Conference on Mobile Systems, Applications, and Services (MobiSys) 2022.

[3] BeomSeok Oh*, Junho Ahn*, Sangwook Bae, Mincheol Son, Yonghwa Lee, Min Suk Kang, and Yongdae Kim (*: co-first author), Preventing SIM Box Fraud Using Device Fingerprinting, Network and Distributed Systems Security Symposium (NDSS ’23).

[4] D. F. Kune, J. Koelndorfer, N. Hopper, and Y. Kim, Location leaks on the GSM air interface, Network and Distributed Systems Security Symposium (NDSS ’12).

[5] Byeongdo Hong, Sangwook Bae, and Yongdae Kim, GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier, Network and Distributed Systems Security Symposium (NDSS ’18).

■ 이 논문(글)은 2023년도 정부(경찰청)의 재원으로 지원받아 수행된 연구 결과임[내역사업(과제)명: 네트워크 기반 보이스피싱 탐지 및 추적 기술 개발 / 연구과제번호: PR10-03-020-22]

파편화된 정보를 모아 동일 범죄 조직을 찾아낸다 : 보이스피싱 범죄 유사도 분석 알고리즘 연구

치안정책연구소 과학기술연구부 스마트치안지능센터 김희두

I 서론

경찰의 보이스피싱 범죄 수사의 목적은 궁극적으로 범죄 조직을 검거하고, 그중 핵심 총책으로 확인된 용의자의 형량을 높이는 것이다. 보이스피싱 범죄 수사에서는 이와 같은 결과를 만들기 위해 여죄 발굴과 증거자료 수집 단계를 가장 중요한 부분 중의 하나로 여기고 있다.

한편, 최근 인공지능 기술이 급격하게 발달함에 따라 범인들이 남긴 음성, 텍스트를 활용해 동일 범죄를 추정하는 인공지능 기술들이 많이 개발되고 있다. 주로 사건마다 드러난 특징을 추출하여 범죄 유사도라는 척도로 비교하는 접근 방식이다. 그러나 각 기술들은 수집된 정보량의 제한으로 단일 기술만으로는 동일성을 정밀하게 측정하기가 힘들다는 한계가 존재한다. 가령 A 사건의 수사 중 목소리만으로 높은 유사도가 측정된 B 사건을 찾아도, 범죄의 시기나 사용 수법이 다르면 같은 범죄로 추정하기 힘들다. 그렇지만 같은 목소리로 추정되는 범죄를 수사 대상에서 제외하는 것도 수사관에게는 부담이 된다. 아직 알지 못하는 단서가 더 있을 수 있기 때문이다.

보이스피싱 범죄분석에 특화된 유사도 측정 알고리즘에 관한 연구는 이같이 단일 특징으로 측정하는 유사도 기술의 한계점을 극복하고자 하는 연구이다. 만약 유사도 측정에서 많이 사용되는 딥러닝 기반의 임베딩 추출 기술을 중첩적으로 사용할 수 있다면 다중 특징값 조합 방식의 동일 범죄 추정 알고리즘의 설계가 가능하다.

위와 같은 알고리즘의 효과는 범인의 목소리, 사칭 수법, 범인의 발화패턴이 모두 유사한 사건을 찾

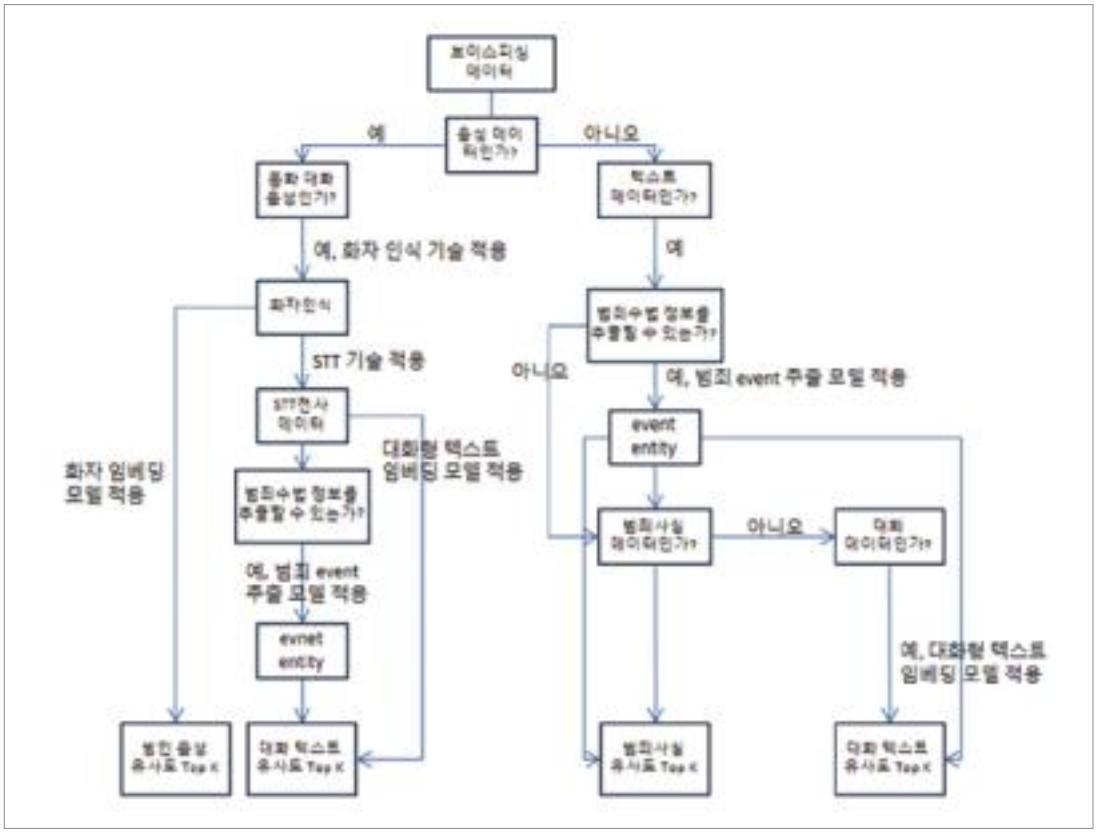
는 방법이 단일 특징만으로 검색된 수백 건의 사건보다 신뢰도가 높은 상태로 우선하여 수사 대상에 포함할 수 있다는 점을 보여줌으로써 입증할 수 있다. 본 연구개발의 End Product인 내부망 수사지원시스템의 핵심 아이디어로 자리 잡을 수 있는 이 알고리즘은 곧 보이스피싱 사건 처리의 속도와 동일 사건 추정의 신뢰도를 기존보다 높일 수 있는 혁신적인 방안이 될 것이다.

Ⅱ 추론 알 고리즘의 설계

보이스피싱 범죄의 동일 사건 추정 분석을 위해서는 <그림 1>과 같이 검색용 데이터베이스를 구축하기 위한 데이터 통합 알고리즘과, 새로운 입력데이터와 기존의 통합 데이터를 비교하여 동일 사건을 추론하는 유사도 측정 알고리즘을 종합하여 설계할 필요가 있다. 먼저 데이터 통합을 위해서는 (1)보이스피싱 데이터 수집, (2)유형에 따른 다중 특징 추출 기술의 적용, (3)엔티티 참조를 통한 데이터베이스 통합의 과정을 거친다. 보이스피싱 범죄는 범인의 음성, 콜센터에서 사용한 대본, 계좌 이체 및 통신 내역 등의 단서를 남긴다. 이 정보들은 사건 기록의 형태로 경찰에 접수되어 저장되거나, 피해 사실을 공유하는 인터넷 커뮤니티 등으로 모두 흩어진다. 따라서 단서를 종합할 수 있는 데이터를 여러 출처에서 수집하여 같은 저장소에 모으는 것이 필수적이다.

두 번째로, 수집된 데이터들은 동일 킷값으로 참조할 수 있는 엔티티가 존재하지 않는 상태이기 때문에 다중 특징 추출 기술을 이용해 범행일시, 장소, 사칭 수법, 범인의 성별, 나이, 목소리 특징들을 다양하게 추출한다. 추출한 정보를 바탕으로 동일 값을 기반으로 테이블을 병합하고 중복을 제거(merge and perge)하는 개체 식별 및 결합(Entity Resolution)의 과정을 거친다. 요약하면 음성, 경찰 범죄정보, 인터넷 정보를 모아 딥러닝 기반 특징을 추출하고, 결합해 DB를 만드는 것이다.

〈그림 1〉 보이스피싱 데이터의 통합과 동일 조직 추정



〈그림 2〉 보이스피싱 동일 범죄 조직 추정 알고리즘

입력데이터를 사용하여 동일 사건을 추론하기 위해서는 <그림 2>와 같이 설계된 알고리즘에 따른 추론 과정이 필요하다. 먼저 통합 데이터베이스 내에서 입력으로 들어오는 정보의 속성을 음성과 텍스트로 구분한 뒤, 데이터베이스 내의 동일 유형의 데이터와 비교하여 유사도를 측정한다. 이때 텍스트의 경우에는 대화 형태의 텍스트와 범죄 사실 요약 형태의 텍스트에 따라 언어모델을 이용해 서로 다른 임베딩 값을 추출하여 유사도를 측정할 수 있다. 음성은 화자 인식한 화자별 임베딩 값으로 유사도를 측정한다. 언어 모델을 활용해 범죄의 수법 정보를 추출한 뒤 고유의 특징값으로 활용할 수 있도록 별도의 필드를 구성하는 event detection 또는 event coding 기술을 응용한다면 추출된 정보를 비정형의 음성과 텍스트 데이터와 결합하여 유사도를 측정할 수 있다. 예를 들어, 보이스피싱 데이터는 전문 경험이 있는 수사관들의 레이블링 방식을 따를 때 사칭 기관, 사칭명 등 기망 수법에 따른 범죄 개체명을 추출할 수 있다. 대면편취, 계좌이체 방식 등의 편취 방법에 따른 범죄 event를 분류할 수 있다.

추출된 특징값들은 언어모델 또는 딥러닝 모델의 신경망을 통과하여 추출한 임베딩 값에 해당한다. 해당 벡터들을 cosine similarity와 같은 벡터 간 거리 측정 방법을 이용해 유사도를 측정할 수 있다. 계산한 유사도 값들에 따라 사건들을 검색할 수 있다. 각 사건의 상세 정보를 조회하여 가장 유사한 사건을 선별해 낼 수 있다.

이 분석 기술을 활용할 수 있는 분야는 다음과 같다. 첫째, 이미 검거한 범인들이 과거에 어떤 범죄를 저질렀는지 추가 범행을 밝힐 수 있다. 둘째, 현재 수사하고 있는 사건이 어떤 범죄들과 같은지 그룹화할 수 있다. 그룹화한 범행의 단서를 모아 범인 검거에 활용할 수 있다. 셋째, 발생하고 있는 범죄시도의 데이터(녹음음성, 문자, 사진파일)등을 대조해서 피싱범죄시도를 밝히는 위험탐지 서비스에 활용할 수 있다. 위험탐지 서비스를 위해서는 수집한 통합DB의 유사도측정 알고리즘 외에 '위험도 등급'을 판단하는 기술을 더 연구해 활용해야 할 것이다.

Ⅲ 유효성 검증 방법

다중 특징값 추출 기반 유사도 알고리즘의 유효성을 향후 객관적으로 검증하기 위해 다음과 같은 실험과 검증 방법의 구성을 제안할 수 있다. 먼저, 구축된 보이스피싱 통합 데이터베이스에 대해 목소리·수법·사건개요 등 특징값들을 딥러닝 모델을 통해 벡터 공간에 표상하여 인덱스로 저장한다. 다음으로, 새롭게 발생한 사건에 의해 보이스피싱 데이터가 추가된다면 <그림 2>와 같은 알고리즘으로 추출된 임베딩 값을 이용해 각각의 특징에 따른 유사 사건을 검색한다. 마지막으로, 새로운 사건으로부터 추출된 벡터값을 검색의 쿼리로 하였을 때 DB에서 검색된 사건 중 실제 수사관이 여죄로 채택한 사건이었는지 여부에 따라 정확도를 측정하게 된다.

Ⅳ 맺음말

이번 리뷰에서는 보이스피싱 데이터의 범죄 분석 관점의 특성을 고려한 다중 특징 추출 기술을 조합하여 통합 보이스피싱 범죄 데이터베이스를 구축하고, 새로운 데이터를 입력받았을 때 동일한 사건을 찾아냄으로써 동일 범죄 조직을 추정할 수 있는 딥러닝 기술 활용 알고리즘 연구 내용을 소개했다.

현재 수사관들은 엑셀을 이용해 개별적으로 사건 목록을 관리하는데, 각 사건에는 획득한 정보 유형과 정보량이 달라 육안으로 직접 동일 여부를 필터링하는 비효율적인 수사 방식으로 어려움을 겪고 있다. 이번 연구에서 개발된 알고리즘을 이용해 실제 수사 시스템의 기능이 개발된다면 더욱 효율적인 범죄 수사가 가능해질 것으로 기대한다. PSI

보이스피싱 음성 분석 모델을 이용한 사기범 음성 분석

국립과학수사연구원 오디오포렌식연구실 공업연구사 박남인

I 개요

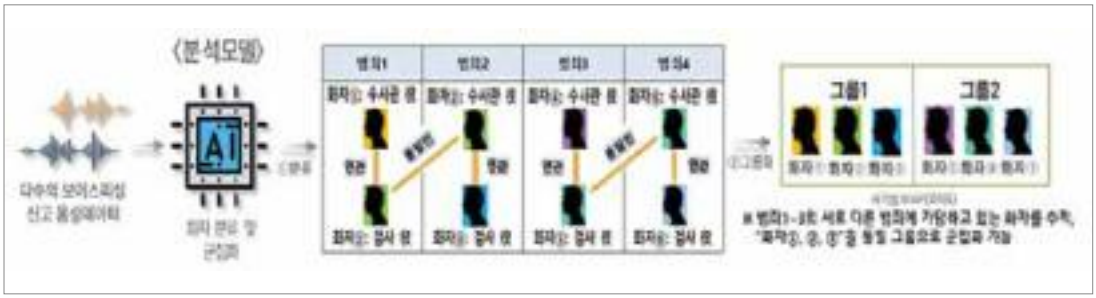
보이스피싱 첫 피해가 신고된 2006년 이후, 현재까지 보이스피싱은 우리 사회에 심각한 문제로 대두되고 있다. 최근 국무조정실 보이스피싱 대응 범정부 TF팀에서 발표한 자료에 따르면, 범죄발생률은 '21년 30,982건 대비 '22년 21,832건으로 약 30% 가량 대폭 감소하였다고 발표하였으나, 여전히 보이스피싱으로 인한 피해금액은 연간 5,000억 이상 발생하고 있다[1]. 보이스피싱 범죄로부터 국민들의 재산을 보호하기 위해, 정부는 강력한 단속과 수사, 그리고 통신 및 금융분야의 특별 대책을 추진하고 있다. 최근 '시티즌코난', '피싱아웃', '스마트피싱보호' 및 '피싱아이즈' 등와 같은 보이스피싱 범죄 예방을 위한 보이스피싱 예방관련 스마트폰 어플리케이션도 개발되고 있다. 국립과학수사연구원은 1988년부터 음성분석실을 기반으로 음성 증거물로부터 음질 개선, 오디오 파일 위변조 분석 및 화자 인식 등 감정 업무를 수행하고 있다[2][3]. 2016년 5월에는 국립과학수사연구원과 금융감독원이 '보이스피싱 근절을 위한 업무협약'을 체결하였으며, 국립과학수사연구원과 금융감독원은 수집된 보이스피싱 사기범의 음성뿐만 아니라 검거한 보이스피싱 범죄자의 음성을 분석에 활용하고 있다. 따라서, 수집된 보이스피싱 음성 정보에 대해 화자를 정확히 인식하고 검증, 식별할 수 있는 모델의 구축과 분석이 요구된다.

Ⅱ 세계최초 보이스피싱 음성 분석 모델

〈그림 1〉 개발된 보이스피싱 음성 분석 시스템

’22년 행정안전부 공공 빅데이터 분석사업 과제(과제명: ‘보이스피싱 사기범 식별 등 과학수사를 위한 음성 데이터 분석’)로 선정되어, 행안부 통합데이터분석센터와 국립과학수사연구원 협업으로 〈그림 1〉의 ‘세계 최초 보이스피싱 음성 분석 모델’[4]을 개발했다. 해당 모델로 2015년부터 2023년 3월까지 신고된 약 12,323개의 보이스피싱 음성 데이터에 대해 범죄자 음성 정보만을 사용해서 범죄 가담자 및 범죄 조직을 그룹화하는 데에 성공하였다.

〈그림 2〉 보이스피싱 음성 모델은 단일 범죄자의 음성 일치 여부뿐 아니라, 보이스피싱 범죄조직의 특성상 역할(수사관, 검사 등)을 나누어 그룹별로 활동하고 있다는 점을 착안, 범죄에 연루된 범죄자들을 군집화할 수 있다.



〈그림 2〉 보이스피싱 음성 데이터를 활용한 범죄자 조직 분석 개념도
(https://mobile.newsis.com/view.html?ar_id=NISX20230710_0002369813 그림 발췌)

Ⅲ 보이스피싱 음성 분석 모델의 성능 분석

〈표 1〉 보이스피싱 음성 분석 모델의 성능 측정 결과

구분(비교 대상)		기존 국과수 모델	새로운 모델
		판독률 (%)	판독률 (%)
1차 검증 (국과수 실제 범죄관련 음성 데이터 활용)		38.4	65.0
2차 검증	평소발성 대 평소발성	29.8	53.8
	위장발성 대 위장발성	20.1	39.5
	평소발성 대 위장발성	23.2	43.0
	무선통화녹음 대 일반녹음	29.5	49.6
	무선통화녹음 대 유선통화 녹음	46.8	62.8
	모든 환경통합	22.8	43.6
1차 및 2차 성능 평균		28.7	51.0 (+22.3%p)

개발된 보이스피싱 음성분석 모델의 성능평가를 위해, 판독률(%)을 측정하였다. 판독률이란, 동일화자로부터 발성된 음성에 대해 동일화자로 판독할 수 있는 비율을 의미한다. 개발된 모델은 2차에 걸쳐 성능 검증이 수행되었는데, 1차 검증에서 실제 국립과학수사연구원에서 최근 3년간 실제 의뢰된 사건 중 신원이 확인된 약 150명의 650여 개의 음성데이터, 2차에서는 약 200명으로 구성된 1,100여 개의 별도 음성데이터를 사용하여 다양한 상황 가정하에 검증한 결과, 〈표 1〉에서 보는 바와 같이 기존 외산 분석모델 대비 약 77% 향상된 성능이 확인되었다. 판독된 결과 정확도는 약 97%로 측정되었다.

Ⅳ 보이스피싱 음성 분석 결과

2022년부터 2023년까지 경찰(충청남도경찰청, 서울특별시경찰청) 및 금융감독원에 피해 신고된 음성 파일, 총 2,347개를 분석했다. 그 중 음성 파일이 아닌 파일, 중복 신고된 파일, 음성의 길이가 짧은 경우를 제거하여 1,752개 보이스피싱 범죄자(남성:1,315개, 여성:437개) 음성을 추출하였다. 화자분리(Speaker diarization)는 허깅페이스에 공개된 화자분리 모델(pyannote-audio)[5]을 활용하여 각 보이스피싱 음성에서 피해자 음성(1인)과 범죄자 음성(최대 2인)을 분리하였다.

〈표 2〉는 1,752개의 보이스피싱 범죄자 음성을 활용하여 개발된 음성 분석 모델을 통한 결과이다. 가담 범죄를 추적하여 동일 범죄 집단(2명이상)으로 군집화 결과, 23개 범죄조직, 52명이 가담한 것을 확인된다.

〈표 3〉은 보이스피싱 범죄자별 범죄 가담횟수를 보여준다. 특정 화자는 최대 19회 범죄에 가담했고, 2회 이상 재범한 경우가 전체 파일에서 약 61%이다. 보이스피싱재범 비율이 높기에, 보이스피싱 범죄자 음성 데이터베이스 구축이 필요하다.

〈표 2〉 범죄조직 규모 및 가담 범죄 수

조직규모	인원	2명	3명	4명
	조직수	18개	4개	1개
가담 범죄수(건)		97	30	9

〈표 3〉 범죄자별 범죄 가담 횟수(2건 이상)

범죄건수	인원수	범죄건수	인원수
2건	170명	8건	3명
3건	88명	9건	2명
4건	45명	12건	2명
5건	18명	16건	1명
6건	10명	19건	1명
7건	4명	총 건수: 1,063 총 인원: 344명	

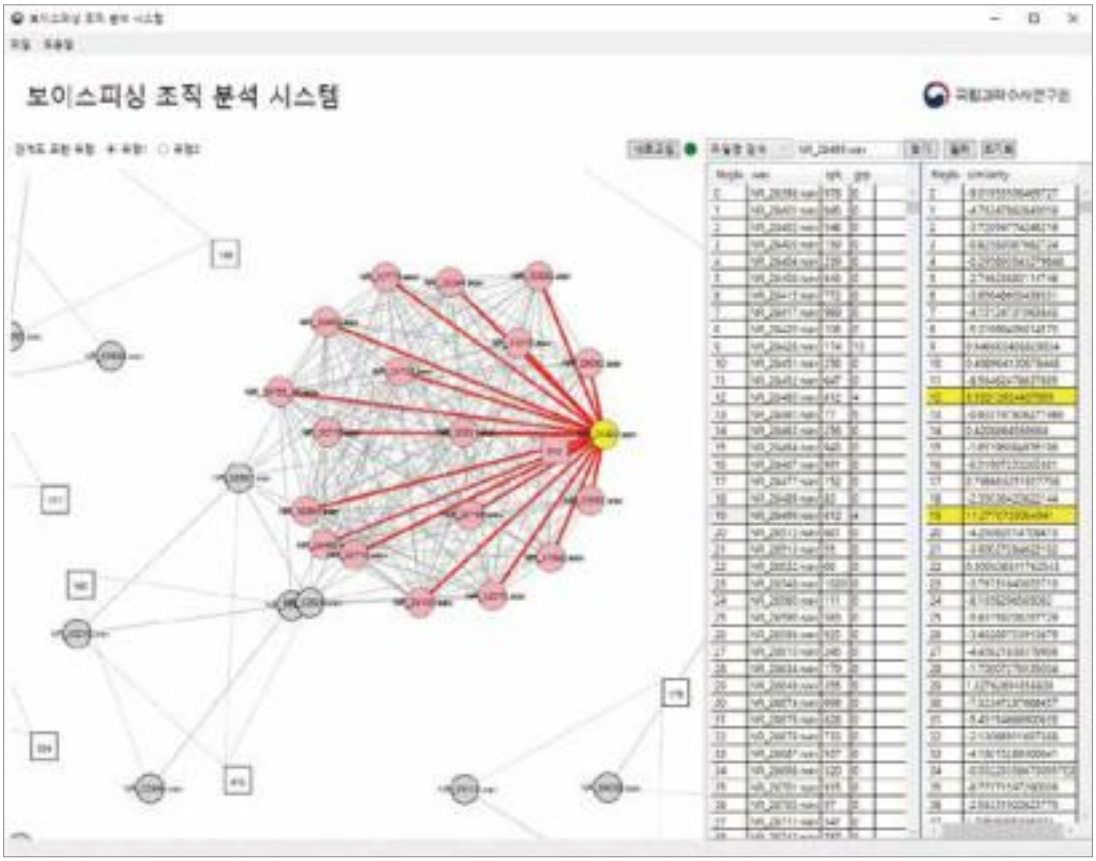
1. 보이스피싱 음성 분석 결과에 대한 시각화

<그림 3>은 보이스피싱 범죄자 음성 유사도 등을 시각화한 결과이다. 좌측엔 파일명, 화자 ID('skp') 및 동일 범죄 그룹ID('grp') 정보이고, 우측엔 파일 간 음성 유사도를 기반으로 모든 파일에 대한 화자 유사도이다. 각 노드(node)는 파일명, 에지(edge)는 각 파일 간에 유사성 여부이다. 파일 간의 유사도가 '6.2'보다 크면, 유사하다고, 각 노드를 연결했다. 특정 파일의 노드에 커서를 놓게 되면, 해당 파일과 유사성이 높은 파일의 노드 사이에 적색으로 에지의 색을 구분했다.

좌측 파일명을 검색하면, 우측의 파일 간 연결을 확인할 수 있다. 'NR_28499.wav'를 선택하게 되면, 해당 파일의 노드는 노란색으로 표시되고, 'NR_28499.wav'와 유사성이 확인되는 파일들의 노드는 분홍색으로 표시된다.

2. 기대 효과 및 정책 활용

개발된 세계최초 보이스피싱 음성 분석모델은 실제 사건 수사에 활용할 수 있다. 2023년 2월말부터 국립과학수사연구원에서 보이스피싱 범죄를 포함한 전화금융사기 음성 분석 감정 업무에 적용하였다. 국과수 오디오 포렌식 감정 중 '23. 상반기 기준, 전세대출사기 사건 등 39건의 사기 사건 1,440



〈그림 3〉 보이스피싱 범죄자 관계망 분석 결과

점의 자료에 화자식별 적용하여 보험사기 및 대출사기 등과 같은 사건을 해결하였다. 2023년 7월 11일 국립과학수사연구원에서 각급 수사기관 24명 대상으로 오디오 포렌식 교육을 통해 수사기관에 개발된 음성 분석 모델을 전파했으며, 경찰대학 치안정책연구소와 협조하여 경찰들이 사용할 수 있는 전화사기수사지원시스템에 탑재할 계획이다. 학술교류 및 홍보를 통한 해외 보급도 계획 중이다.

추후 보이스피싱 음성과 발신 전화번호(차명폰 번호)를 포함한 분석을 강화하여 범죄 조직을 정밀하게 군집화할 예정이다. 보이스피싱 범죄자의 음성 데이터베이스를 구축하여, 보이스피싱 조직의 검거에 효과적으로 기여할 것을 기대한다. **PSI**

참고 문헌

[1] 국무조정실. (2023. 02. 01). 보이스피싱 대응 범정부 TF 회의 [보도자료]. https://www.opm.go.kr/opm/news/press-release.do?-mode=view&articleNo=152623&srSearchVal=%EB%B3%B4%EC%9D%B4%EC%8A%A4%ED%94%BC%EC%8B%B1&article.offset=0&articleLimit=10

[2] 박남인, 전옥엽, 김태훈, 이중, "보이스피싱 음성 파일에 대한 법과학적 화자 분석 방법의 적용 사례," 디지털포렌식연구, 13 (1), 20.

[3] 박남인, 이지우, 김진환, 임재성, 나기현, 전옥엽, "삼성 스마트폰에서 생성된 통화녹음파일에 대한 위변조 검출을 위한 법과학적 분석 방법," 디지털포렌식연구, 16 (1), 2022.

[4] S. H. Mun, J.-W. Jung, M. H. Han, and N. S. Kim, "Frequency and multi-scale selective kernel attention for speaker verification," In proc. of IEEE Spoken Language Technology Workshop (SLT), pp548-554, 2022.

[5] A. Radford, J. W. Kim, T. Xu, G. Brockman, C. McLeavey, II. Sutskever, "Robust Speech Recognition via Large-Scale Weak Supervision," *arXiv preprint arXiv:2212. 04356, 2022.*

■ 이 논문(글)은 행정안전부 주관 국립과학수사연구원 중장기과학수사감정기법연구개발(R&D)사업의 지원을 받아 수행한 연구임 (NFS2023DTB03)

시티즌코난 : 보이스피싱 예방의 골든타임과 개선점을 중심으로

치안정책연구소 스마트치안지능센터 김재후

I 연구의 배경과 필요성

치안(Policing)이란, 미래 예측적 및 분석적 연구활동을 함으로써 발생 가능한 범죄위험에 대한 대응방안을 모색하는 것이다. 이러한 치안연구는 4차 산업혁명에 비례하여 진화하는 범죄, 즉 범죄의 전문화 및 광역화에 미리 대응함으로써 국민의 안녕과 평온을 보장하는 초단이 된다.

스마트치안지능센터의 주된 업무 중 하나는 경찰 데이터 분석 연구, R&D 사업 등을 통해 다양한 범죄 문제들을 예측하고 선제대응함으로써 시민들에게 질 좋은 치안환경을 제공할 뿐만 아니라, 과학기술을 활용하여 경찰활동을 전략적으로 지원하는 것이다. 이를 말해주듯, 우리 센터에서는 차량번호 판분석(NPDR), 보이스피싱 수사지원 연구, 시티즌코난 등 부서의 임무를 충실히 수행하고 있다.

이중 시티즌코난은 시민들의 삶뿐만 아니라 지구대·파출소 등 경찰 현장에 가장 잘 자리매김한 앱으로 생각된다. 시티즌코난은 올해로 출시된지 3년이 된 보이스피싱 악성앱 탐지 어플로써, 다운로드 290만 건, 악성앱 탐지 18만 건 등의 성과를 올리고 있다. 이번 치안과학기술리뷰를 통해 시티즌코난을 다시 한번 되짚어보고 고도화 및 지능화되는 보이스피싱의 단계별 특징을 살펴봄으로써 시티즌코난이 앞으로 나아가야 할 방향을 제시하고자 한다.

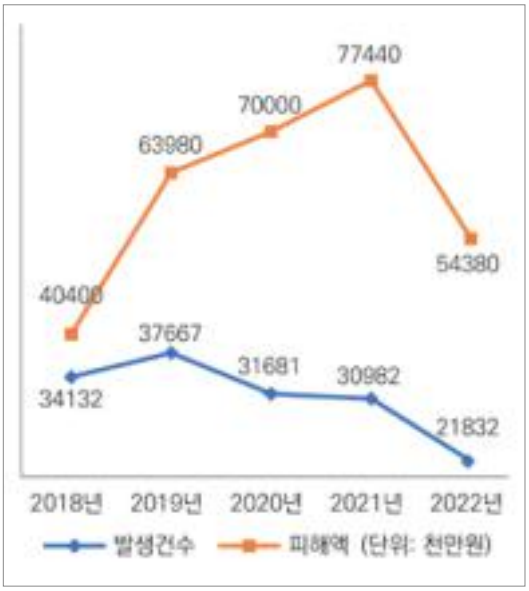
Ⅱ 시티즌코난 개요

1. 과학기술과 범죄

우리는 4차 산업혁명을 통해 눈부신 과학기술의 발전을 이끌었다. 이는 전통적인 산업과 비즈니스 모델을 혁신할 뿐만 아니라, 우리 사회와 경제 전반에 지대한 영향을 미쳤다. 특히, 4차 산업혁명의 결과로 가상 현실(virtual reality, VR), 인공지능, 사회적 연결 등 기술과 디지털 혁신은 우리 삶의 질을 한층 더 높였다. 그러나 과학기술의 발달 그 이면에는 딥페이크 범죄, 메신저 앱을 통한 성범죄 등 범죄의 고도화 및 전문화로도 이어졌다. 과학기술을 악용한 범죄가 늘어감에 따라, 순찰, 단속, 수사 등 전통적 경찰활동을 뛰어넘어 고도화된 범죄 위험을 초기에 제압하는 선제적 경찰활동(Proactive Policing)의 필요성이 대두되었다.

2. 보이스피싱 추이

보이스피싱(Voice Phishing)은 전화금융사기 중 한 가지 수법으로서 전화 등을 통해 피해자의 개인정보를 빼내거나 금전을 사취하는 행위를 의미한다(김대호, 한지혜, 장광호, 2023). 보이스피싱은 과학기술을 악용하여 새롭게 생겨난 많은 범죄 중 하나이며 예방의 중요성을 다시 한번 일깨우는 범죄이다. 최근 5년간 우리나라 보이스피싱 발생 추이를 살펴보면, 2018년 34,132건, 2019년 37,667건, 2020년 31,681건, 2021년 30,982건, 2022년 21,832건으로 2018년과 2019년까지 증가 추세를 보이다가 2020년부터 2022년까지 감소 추이를 나타내고 있다(그림 1). 피해액의 경우, 2018년 4,040억 원, 2019년 6,398억 원, 2020년 7,000억 원, 2021년 7,744억 원, 2022년 5,438억 원으로 2018년부터 2021년까지 증가 추이를 나타냈지만 2022년은 감소했음을 알 수 있다.



〈그림 1〉 연도별 보이스피싱 증감 추이
출처: 경찰청. 보이스피싱 통계자료(2023)

3. 시티즌코난

앞서 살펴본 바와 같이 전화·통신·전자상거래 시스템의 발전으로 인해 보이스피싱 발생 및 피해가 심화되고 있음을 알 수 있다. 이와 비례하여 보이스피싱을 예방하기 위한 사회적 관심도 자연스럽게 증가했으며 TV, 라디오, 경찰활동 등 보이스피싱 예방법을 연일 알렸다. 하지만 피싱 범죄자들은 피해자의 특성, 사회문화적 상황 등에 발맞춰 범죄수법을 교묘히 변화시켰으며 피해는 더욱 커져갔다. 지능화 및 고도화되는 전화사기에 대해 범죄 상황을 실시간으로 파악하여 선제적으로 대응할 방안이 필요했다. 이러한 상황 속에서 경찰대학 치안정책연구소 스마트치안지능센터는 한국형 자연어 기반 전화금융사기 분석기(Korea Overwatcher for

phising NLP ANalysis, KONAN)인 시티즌코난을 개발하였다. 시티즌코난은 시민용 전화사기 악성앱 탐지앱으로써, 핸드폰 안의 모든 보이스피싱 악성앱을 찾아 보이스피싱을 막는 역할을 한다(그림 2). 실제로 전화사기 의심 신고를 받고 출동하는 경찰관들이 피해자 핸드폰에 시티즌코난을 설치하고 악성앱 설치 여부를 판단하여 보이스피싱을 방지한 사례가 다수 존재한다.

〈그림 2〉 시티즌코난 화면

Ⅲ 보이스피싱 과정과 골든타임

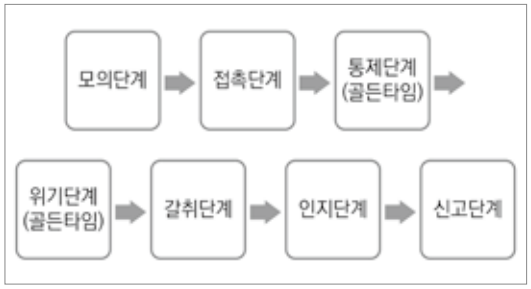
1. 보이스피싱 과정

보이스피싱은 총 7단계로 나눠 볼 수 있다(그림 3). 첫 번째, 모의단계에서는 디지털 범죄의 방법을 모의하는 단계이다. 두 번째, 접촉단계에서는 피해자에게 전화, SNS 등을 활용하여 사칭 및 투자를 유도하는 단계이다. 세 번째, 통제단계에서는 문자를 통해 계좌번호, 악성앱 링크, 가입 유도 웹링크 등의 정보를 피해자에게 전달하는 단계이다. 네 번째, 위기단계에서 범죄자는 계좌번호를 알려주거나 웹사이트 가입, 악성앱 설치를 통해 개인정보 및 금융정보를 얻을 수 있는 초석을 마련한다. 다섯 번째, 갈취단계에서 범죄자는 피해자가 보낸 금액을 인출하거나 가입 웹사이트, 악성앱을 통해 개인정보, 금융정보를 갈취한다. 여섯 번째, 인지단계에서는 피해자가 사이버범죄 피해를 인지하는 단계이며 마지막 단계인 신고단계에서 피해자는 112 혹은 사이버수사대에 범죄피해를 신고한다.

2. 보이스피싱의 골든타임

갈취단계부터는 실질적인 보이스피싱 범죄가 발생한 단계로, 피싱 범죄에 대한 사후조치 및 대응을 해야 하는 단계이다. 하지만 피싱 범죄가 발생한 후부터는 금융 및 수사기관의 공조, 법제도적 문제 등 여러 요인으로 인해 피해회복의 한계가 분명하다(이기수, 2018). 보이스피싱에 대한 예방이 더욱 강조된다. 보이스피싱의 7단계 중 통제단계와 위기단계는 사전조치가 가능한 단계로써, 보이스피싱 범죄를 사전예방할 수 있는 '골든타임'이다. 구체적으로, 통제단계에서는 범죄자가 피해자에게 링크, 악성앱 등 피싱 범죄에 대한 유인수단을 보낸

다. 위기단계는 피해자가 사이트를 가입하거나 악성앱 설치, 피해 금액을 송금하는 단계이다. 이 두 단계에서는 범죄자가 피해자에게 문자, 이미지 등의 피싱 정보를 전송함으로써 본격적으로 피싱이 시작된다. 그런데 만약 피해자가 범죄자로부터 피싱 정보를 받았을 때 시티즌코난이 피싱 정보에 대한 위험성을 인식 및 탐지하여 본인이나 경찰에게 인지시킨다면, 범죄피해를 충분히 방지할 수 있다. 즉, 범죄자가 문자 등을 통해 피해자에게 계좌번호, 웹 및 악성앱 링크 등의 피싱 정보를 전달하여 피싱을 유도할 때, 피싱 범죄와 연관된 범죄 데이터베이스가 존재한다면, 피해자가 피싱 정보를 받았을 때 탐지 및 경고를 통해 피싱 범죄의 사전예방 가능성이 증가한다. 따라서 이 두 단계는 보이스피싱 피해를 방지할 수 있는 골든타임으로써 예방의 필요성이 대두되는 단계이다.



〈그림 3〉 보이스피싱 7단계

Ⅳ 맺음말

과학기술의 발전으로 보이스피싱 범죄는 다양성, 복잡성, 비예측성이 한층 더 강화되었다. 보이스피싱뿐만 아니라, 스미싱, 인터넷 사기 등과 같이 최근 전화금융사기는 전화 혹은 문자만이 사용되지 않는다. 예컨대, 부업 및 투자 상담, 로맨스스캠 등 SNS를 활용하여 보이스피싱 범죄를 저지르기도 한다. 지금도 피해자의 상황에 맞춰 수단과 방법이 다양해지고 있으며 앞으로도 그럴 것이다(윤해성, 2010).

다양한 수단과 속이는 방법도 변화하고 있다. 분명 눈부신 과학기술 발달의 이면에는 범죄의 지능화와 고도화가 내포되어 있다. 이를 증명하듯, 최근 5년간 보이스피싱 피해액은 전반적인 증가 추이를 보이며 국가적 재난 수준에 이르렀다. 이에 대응하기 위해 우리 연구소에서는 관련 연구를 통해 보이스피싱 악성앱 탐지 어플인 시티즌코난을 개발했다. 짧은 기간 동안 다운로드 수와 사용자가 늘어났으며 피싱에 활용되는 악성앱을 탐지하고 범죄를 방지하는 사례가 다수 발생했다. 이로 인해 시민, 경찰 등 사용자들의 호평을 받을 수 있었지만, 몇 가지 보완 및 고도화해야 할 점을 파악할 수 있었다.

현재 시티즌코난은 보이스피싱 관련 ① 악성앱만을 탐지할 수 있으며 ② 실시간 탐지가 되지 않는다. 즉, 피싱, 스미싱, 인터넷 사기에서 나오는 음성·이미지·URL 등 다양한 피싱 범죄를 막을 수 없으며 수동으로 어플을 실행하여 검사 버튼을 눌러야만 악성앱 탐지가 된다. 하지만 앞서 설명한 바와 같이 보이스피싱 7단계 중 통제단계와 위기단계는 피싱 범죄가 본격적으로 시작되는 단계이다. 이 시기는 사전대응이 절실히 필요한 골든타임으로써, 실시간 탐지뿐만 아니라 악성앱 외에 여러 피싱 범

죄수단을 차단할 수 있어야 한다. 만약 이러한 보완점들이 개선되어 고도화된다면 조금 더 질 좋은 치안환경을 제공할 수 있을 것이다. 더욱이 과학기술의 발달로 인해 현재 시티즌코난의 보완점들이 실현불가능한 것도 아니다. 따라서 추후 시티즌코난의 기능 개선을 통해 보이스피싱으로부터 더 안전한 삶을 살 수 있을 것을 기대한다. **PSI**

참고 문헌

[1] 김대호, 한지혜, 장광호 (2023). 스마트치안을 통한 보이스피싱 피해구제 연구. 한국경찰연구, 22(1), 27-52.
[2] 윤해성 (2010). 보이스피싱 범죄 대응방안 고찰. 법학논고, 34, 237-266.
[3] 이기수 (2018). 최근 보이스피싱의 범죄수법 동향과 법적 대응방안. 범죄수사학연구, 4(2), 3-19.

국민체감형 치안안심 플랫폼「안심24」 구축 방안

㈜메타로직컨설팅 대표이사/공학박사 변종봉

Ⅰ 개요

보이스피싱 및 인터넷사기 등 디지털 금융범죄(경찰청 기준 사이버 금융범죄와 사이버 사기)의 피해가 매년 큰 폭의 증가세를 나타내고 있다.

보이스피싱의 피해금액은 2021년 약 7,744억 원에서 2028년 약 1조 7천7백억 원 규모로 증가할 것으로 예상되고, 인터넷사기의 피해금액은 2021년 약 2,707억 원에서 2028년 약 6천1백억 원 규모로 증가할 것으로 예상된다.

두 범죄로 인한 사회·경제적 비용까지 포함하면 사회 전반에 매우 심각한 손실을 유발하고 있는 것이 사실이다.

〈그림 1〉 보이스피싱 피해추이(경찰통계연보)

〈그림 2〉 인터넷사기 피해추이(경찰통계연보)

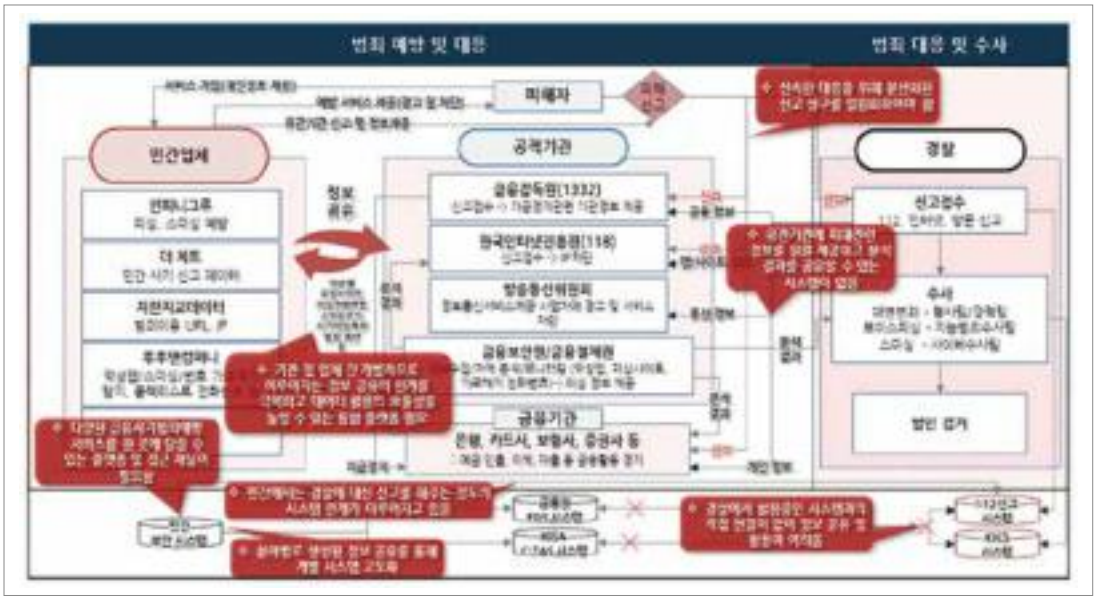
스마트폰을 활용하거나 온라인 공간상에서 발생하는 범죄가 늘어나면서 과거 전통적인 공공의 활동 방식으로는 한계에 봉착했다고 할수 있다.

오프라인 범죄는 범인이 피해자를 물색하고 조우해서 범행을 저지르는 과정이 구분되지만, 디지털 범죄는 범죄 도구의 개발, 유인프로그램 배포, 개인정보 탈취 등 과정의 구분이 어려운 경우가 대부분이다.

<그림 3>에서 보는바와 같이 현재 상황은 민간·공공에서 보이스피싱, 스미싱 등 신고를 포함한 다양한 금융사기 관련 서비스를 제공하고 있으나 정보의 범람화로 인해 피해자가 원하는 서비스를 일괄되게 제공받기가 어려운 실정이다.

따라서, 경찰과 유관 공공기관, 민간단체가 적극적인 협조체계를 마련할 필요가 있는데, 예를 들면, 피해접수, 범죄수사 등 경찰의 역할과 더불어 피해회복, 추가 피해예방 등 공공-민간(금융·통신·포털 등)의 역할이 반드시 필요하다.

경찰-공공-민간이 온·오프라인을 융합해서 범죄가 심각해지기 전에 선제적으로 협업할 수 있으려면 하나의 통합적인 플랫폼이 구축되어야 한다.



〈그림 3〉 디지털범죄 대응상황 현황분석

Ⅱ 치안안심 플랫폼 개념구상

디지털 금융범죄에 대한 각 기관별 현재의 업무 및 시스템 현황을 분석한 결과 아래 <표 1>과 같은 주요 이슈를 파악할 수 있었다.

앞서 도출된 환경분석, 현황분석 이슈 및 Key Finding을 바탕으로 R(Regulation), P(Process), O(Organization), S(System)으로 분류하고 이를 종합하여 국민체감형 치안안심 플랫폼을「안심24(가칭)」로 정의하고 <그림 4>와 같이 기본개념을 구상하였다.

〈표 1〉 디지털 금융범죄 주요현황분석결과

구분	주요이슈
디지털 범죄 예방 프로세스	• 범죄 유형에 따라 프로세스 및 부서별로 별도의 시스템을 운영
디지털 범죄 예방·업무 정보자원 운영조직	• 경찰내부 운영조직 분석, 경찰내부에서도 정보 공유가 어려움 • 민간의 최신 기술을 도입한 시스템이 긴요 • 추후 원채널로 자료 공유 및 시스템 연계를 위한 플랫폼 구축 및 관리 운영할 별도의 전담조직 필요
내·외부 이해관계자 요구사항 조사	• 서울시, 금융보안원 공공 기관들은 법적인 제약으로 서비스 제공이 어려울 것으로 판단
관련 시스템 및 데이터분석	• 범죄 유형에 따라 프로세스 및 부서별로 별도의 시스템을 운영 • 112시스템, 시티즌코난, KICS 스마트치안 빅데이터 플랫폼에서 보유중인 데이터는 개인 정보보호 등으로 인한 시스템간 데이터 연계의 한계성 존재

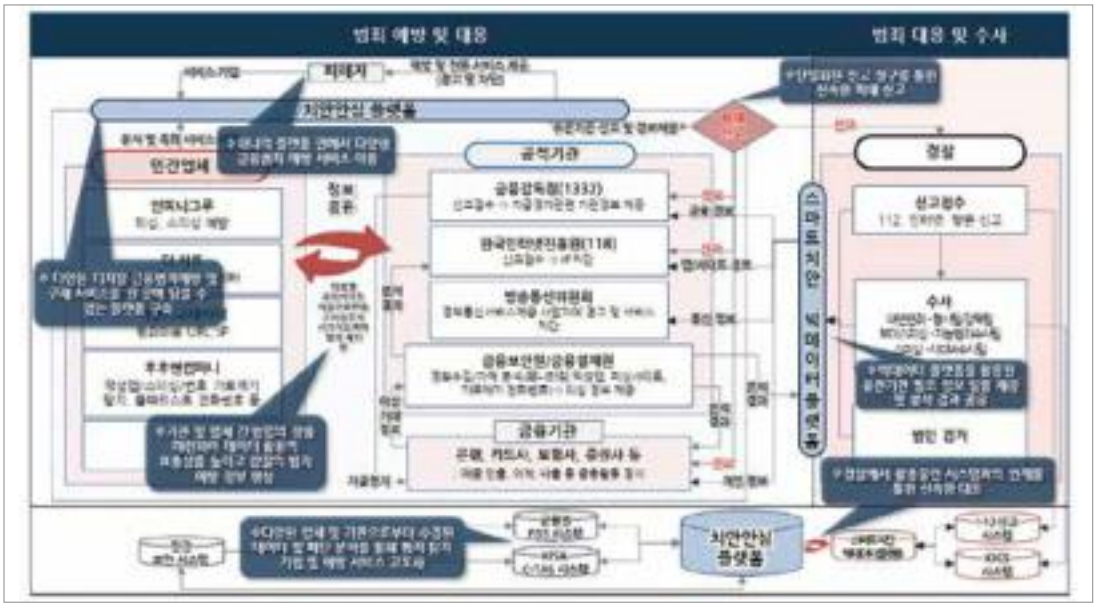
〈그림 4〉 국민체감형 치안안심 플랫폼「안심24」 개념구상(안)

Ⅲ 「안심24」아키텍처 설계(안)

보다 세부적인 아키텍처 설계를 위하여 우선 디지털 금융범죄의 유형을 파악하고 각 상황별 대응안을 마련하여야 한다. <그림 5>와 같이 디지털 금융범죄는 그 유형에 따라 사이버 금융범죄(메신저 이용 사기, 스미싱 등)와 사이버 사기(직거래 사기, 게임 사기 등)로 분류할 수 있다.

앞서 <그림 3>에서 파악된 대응상황별 문제점을 개선하기 위하여 <그림 6>과 같은 서비스 모델을 구상하였다.

〈그림 5〉 디지털 금융범죄 유형별 대응방안



〈그림 6〉 디지털금융범죄 대응프로세스(BA)

첫째, 디지털 금융범죄 예방 및 실시간 차단 서비스 제공한다. 이를 세분화 하면 악성 앱(IP, URL), 사칭 사이트(이미지) 탐지, 경고 및 차단 서비스, 보이스 피싱 전화통화, 스미싱 문자(메일, 메시지) 탐지, 경고 및 차단 서비스, 사기 의심 정보(전화번호, 계좌번호) 진위 여부 판독 및 확인 서비스, 안전 거래 서비스 등으로 구분된다.

둘째, 단일 채널 피해 신고 및 신속 구제 요청(대응) 서비스를 개발한다.

셋째, 유형별/단계별 대응 절차 안내 및 신고/구제 요청 건에 대한 진행 과정과 상태를 확인할 수 있는 대시보드를 개발한다.

디지털 금융범죄 원천차단 및 신속 대응 원스톱 서비스의 사용자 기능은 사전예방과 안전거래, 신고 및 피해지원 등으로 구성하였다.

경찰 및 유관기관에서는 범죄 예방 및 대응에 필요한 다양한 정보가 담긴 데이터를 개별적으로 수집 및 분석하고 있다. 기관별 효과적인 예방과 전문적인 대응을 위해서는 분야별로 생성된 정보의 공유를 통해 개별 시스템을 고도화 할 필요가 있다. 현재 경찰대학 치안정책연구소는 스마트치안 빅데이터 플랫폼을 통해 다양한 정보와 데이터를 가공하고 분석하여 범죄 예방에 활용할 수 있는 여건을 마련하고 있다.

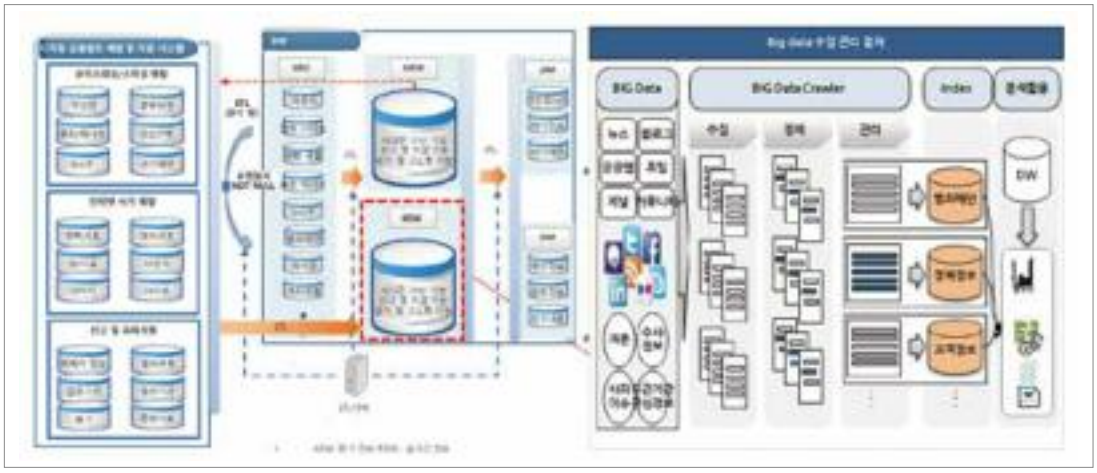
〈그림 7〉 응용 아키텍처(AA) 설계(안)

〈그림 8〉 데이터 아키텍처(DA) 설계(안)

「안심24」의 데이터 아키텍처는 〈그림 8〉과 같이 첫째, 범죄 패턴 분석을 통한 예방 알고리즘을 개선하여 유형별 특성을 도출하고, 프로세스 상 예방 취약점을 개선토록 한다.

둘째, 악성 앱 분석을 통한 범죄 기술 트렌드를 파악하고 이에 대한 대응 기법을 고도화한다. 안전한 샌드박스 내에서 악성 앱 및 스미싱 문자 실행 분석을 통한 범죄 이용 사이트/IP/URL/C&C 서버를 차단하고, 기타 정형/비정형 빅데이터 분석을 통한 디지털 금융범죄 예방 기능 고도화와 유관 기관과의 관련 정보 수집과 공유 및 데이터 분석을 통한 모니터링을 실시한다.

디지털 금융범죄 예방 및 대응을 위해서는 주요 공공기관과 전문 기술을 가진 여러 곳의 민간기관으로부터 데이터 수집 및 전송을 통한 데이터 연계가 이루어져야 한다. 〈그림 9〉는 이러한 데이터들이 DW 형태로 통합되는 모델을 제시한다.



〈그림 9〉 데이터웨어하우스(DW) 설계(안)

<표 2>는 디지털 금융범죄와 관련하여 수집하고 있는 데이터를 각 보유기관별로 파악한 것으로 향후 데이터 연계의 대상이 될 수 있으며, <표 3>은 수집된 데이터를 전송하여 범죄에 대응할 수 있는 정보내역이다.

〈표 2〉 수집데이터 보유기관 및 정보내역

보유기관		정보내역
공공	금융감독원	피해자와 피의자 간 통화 내용, 범죄 이용 계좌번호, 범죄 피해 추이, 신고/접수 건 진행상황 정보
	금융보안원	악성 애플리케이션 분석 내용(유형, 작동 내용, 주요 유포지, URL, IP, C&C 서버 등)
	한국인터넷진흥원	범죄 이용 전화번호, 범죄 이용 인터넷 사이트(URL, IP), 신고/접수 건 진행상황 정보
	스마트치안지능센터	사이버 금융범죄 및 사이버 사기 통계 정보
	경찰청	사이버 금융범죄 및 사이버 사기 관련 신고 정보(범죄 패턴 분석용), 신고/접수 건 진행상황 정보
민간	더 치트	민간 사기 의심 신고 정보(사용자 계정, 이름, 계좌번호, 전화번호 등)
	후후앤컴퍼니	AI 실시간 통화분석, 발신번호 변조(심박스 변조), 블랙리스트 전화번호, 문자/메신저 내 URL 위험도 정보
	지란지교데이터	악성 애플리케이션 분석 내용(유형, 작동 내용, 주요 유포지, URL, IP, C&C 서버 등)
	S2W	다크 웹 내 디지털금융범죄 관련 정보
	AMGINE	인터넷 사이트 게시판 내 디지털금융범죄 관련 정보

〈표 3〉 전송데이터 보유기관 및 정보내역

보유기관		정보내역
공공	금융감독원	범죄 이용 계좌번호, 범죄 패턴 및 피해 추이, 피해 신고 내용
	금융보안원	악성 애플리케이션 분석 내용(유형, 작동 내용, 주요 유포지, URL, IP, C&C 서버 등)
	한국인터넷진흥원	범죄 이용 전화번호, 범죄 이용 인터넷 사이트(URL, IP), 피해 신고 내용
	스마트치안지능센터	사이버 금융범죄 및 사이버 사기 패턴 분석 정보
	경찰청	범죄 및 피해 신고 내용
민간	후후앤컴퍼니	AI 실시간 통화분석, 발신번호 변조(심박스 변조), 블랙리스트 전화번호, 문자/메신저 내 URL 위험도 정보
	지란지교데이터	악성 애플리케이션 분석 내용(유형, 작동 내용, 주요 유포지, URL, IP, C&C 서버 등)
	S2W	다크 웹 내 디지털금융범죄 관련 정보
	AMGINE	인터넷 사이트 게시판 내 디지털금융범죄 관련 정보

Ⅳ 「안심24」구축 단계별 이행방안

디지털 공간에서의 범죄는 향후 지속적으로 다양화, 복합화될 전망이다. 따라서 국민이 체감할 수 있는 치안안심 서비스에 이와 같은 모든 범죄의 유형들이 지속적으로 다루어져야 한다.

앞서 자세히 다루었던 디지털 금융범죄와 함께 디지털 성범죄, 신변위협 범죄 등에 대해서도 다양한 의견을 수렴하여 장기적인 이행과제를 도출하였다. 도출된 총 8개의 이행과제를 대상으로 평균 10년차 이상의 IT전문 컨설턴트들이 참여하여 과제의 중요도(50%)와 실현가능성(50%)을 기준으로 평가한 결과 <표 4>에서 나타난 바와 같이 과제별 우선순위를 판단할 수 있었다. 연구결과를 토대로 디지털 범죄가 사전에 예방되고 신속하게 대응될 수 있도록 성공적인 「안심24」가 구현되기를 기대한다. PSI

〈표 4〉 이행과제별 우선순위 평가결과

No.	이행 과제	중요도(50%)				실현가능성(50%)			종합	순위
		전략적 중요도	시급성	개선 효과	평균	제도적 용이성	기술적 용이성	평균		
1	디지털 금융범죄 예방 시스템 구축	5	5	5	5	3	5	4	4.5	1
2	디지털 금융범죄 DW기반 데이터 분석 시스템 구축	5	4	5	4.67	3	5	4	4.33	2
3	디지털 성범죄 신고 시스템 구축	5	5	5	5	2	5	3.5	4.25	3
4	메타데이터 개발·품질관리 시스템 구축	4	4	5	4.33	3	5	4	4.17	4
5	(신변보호) 긴급구제 안전 시스템 구축	3	4	4	3.67	3	5	4	3.83	6
6	(신변보호) 내·외부 통합 표준연계체계 구축	3	3	4	3.33	3	5	4	3.67	7
7	디지털 금융범죄 관련 인프라 구축	4	4	4	4	3	5	4	4	5
8	디지털 성범죄 관련 인프라 구축	4	4	4	4	3	5	4	4	5
9	신변보호 서비스 관련 인프라 구축	3	4	4	3.67	2	5	3.5	3.58	8

참고 문헌

[1] 국민체감형 치안안심 플랫폼 구축 정보화전략계획(ISP), NIA(2023)

알아두면 쓸모있는 CCTV 수사의 핵심 기술 : 차량번호판 분석시스템(NPDR)

치안정책연구소 과학기술연구부 스마트치안지능센터 최주현

Ⅰ 시스템 개발의 배경과 필요성

우리나라는 세계에서 손꼽히는 CCTV 대국이다. 국내에서는 2002년 서울 강남구 범죄 취약 지구에 CCTV 5대 설치를 기점으로 범죄 예방 및 검거, 시민 안전을 목적으로 한 공공기관 CCTV가 빠르게 보급되기 시작했다. 지난 해 말 기준 전국의 CCTV는 160만대에 달한다. 민간에 설치된 CCTV와 차량에 설치된 블랙박스 수를 더하면 이 숫자는 더 커진다. 골목골목에 CCTV가 설치되고 차량마다 블랙박스가 달리면서 현장에서는 '수사의 80%는 CCTV가 한다'는 말이 돌 정도다. 하지만 범행 장면이 담긴 CCTV 영상을 확보했다고 문제가 해결되는 것은 아니다. 현재 시중에 보급되는 CCTV는 최소 21만 화소부터 최대 800만 화소 이상으로 이루어져 있다. 보편적으로 41만 화소 CCTV를 사용하는데, 이는 10m 정도만 떨어져도 얼굴 식별이 불가능한 수준의 저화질이라고 한다.

지난 4월 서울교통공사는 서울지하철 1~8호선 객차 내 설치된 CCTV는 총 4552대이며, 이 중 41만 화소가 1716대, 200만 화소가 2836대인 것으로 집계했다. 이는 서울 지하철 내 CCTV 10대 중 4대가 사람 얼굴도 식별하기 힘든 수준인 것이다. 일례로, 22년 11월 서울지하철 내에서 성추행 혐의를 받은 남성이 지하철 역 내의 CCTV의 화질이 좋지 않아 피고인과 동일인인지 확신할 수 없다는 이유로 무죄판결을 받았다.[1] 이렇게 저화질 영상이나 야간일 경우 피의자가 범죄를 저질렀다고 확신하기 힘들거나 피의자조차 특정하기 어려워 CCTV

1) 2019도11967 성폭력범죄의처벌등에관한특례법위반

수사는 원점으로 돌아간다. 이처럼 열악한 CCTV 영상 속에서 수사의 결정적 단서가 되는 범인의 얼굴이나, 차량 번호판을 특정할 수 있는 프레임을 찾기란 쉽지 않은 과정이다.

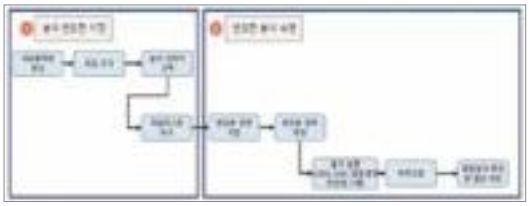
이러한 치안현장에서의 문제를 과학기술로 해결하기 위해 스마트치안지능센터는 그간 R&D인 과제로 개발한 산출물(차량번호판 AI 분석 기술)을 현장 부서에서 신속한 범죄 대응이 가능하도록 설계하고 개발하여 22년부터 현재까지 시스템 시범 운영 중에 있다. 본 리뷰는 AI기반 차량번호분석시스템(NPDR)을 소개하고, 1년간 시범 운영하며 차량번호분석시스템이 현장에서 활용된 대표적인 사례, 보다 빠른 피의자 특정을 위해 추가 연구·개발 계획에 대해 소개한다.

Ⅱ AI기반 차량번호판 분석시스템이란?

치안정책연구소 스마트치안지능센터에서 운영 중인 AI기반 차량번호판 분석시스템인 NPDR (Number Plate Deep Resolution)은 영상처리 및 AI 분석 기술을 활용하여 화질이 열악한 자동차 번호판 촬영 이미지에서 자동차 번호를 복원, 추출하는 시스템이다.

〈그림 1〉 NPDR Client 분석 화면

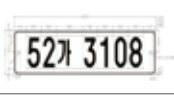
AI기반 차량번호분석시스템(NPDR)을 사용하기 위해선 먼저 경찰청 내부망 연계시스템 바로가기 중 AI기반현장지원(차량번호판분석)을 접속하여 사용신청 후 NPDR Client(사용자용 프로그램)를 설치하여야 한다. 다음으로 클라이언트를 실행하고 경찰 내부망 아이디, 비번을 입력하면 〈그림 1〉과 같이 분석 작업을 위한 분석 툴이 실행된다.



〈그림 2〉 NPDR Client 주요 프로세스

1 먼저 분석 툴을 실행 후 분석 작업명과 구형, 일반, 신형으로 구분된 번호판을 필수적으로 입력하면 분석 작업을 실행할 수 있는 환경으로 구성된다.

번호판 종류는 3종류로 구성되어 있는데 짧은 7자리는 구형, 긴 7자리는 일반, 긴 8자리는 신형 번호판으로 구분하였다. 현재 한 줄로 된 번호판 영역만 지원되며 두 줄로 이루어진 번호판은 23년 NPDR 시스템 고도화 사업을 통해 개발 중이다.

구형 번호판 (335mmx155mm)	일반 번호판 (520mmx110mm)	신형 번호판 (520mmx110mm)
		

〈그림 3〉 NPDR Client 분석 가능한 번호판 종류

2 다음 파일 추가 아이콘을 선택하여 분석을 원하는 이미지(jpg, png 지원) 또는 동영상(avi 지원)을 파일 편집을 통해 이미지 추출하여 선택 시

메인 분석창에 선택한 분석 이미지가 출력된다. 파일 추가 아이콘 옆 다중 이미지 추가 아이콘을 선택 시 2개 이상 분석 이미지 선택이 가능하다. 다중으로 선택된 분석 대상은 작업리스트에 자동으로 등록된다.

3 세 번째는 메인 분석 창에 표출된 사진에서 번호판 영역을 확정하는 단계이다. 사각형, 선, 점 그리기 도구를 통해 번호판 영역 확정을 지원하고 있다. 번호판 영역 확정 다음 단계에서는 번호판 영역 숫자 편집화면에서 자동으로 숫자 영역을 분할해 주는데 번호판 크기에 맞춰 영역이 정확하게 나뉘어 지면 추천 결과 값의 정확도가 높아진다. 이미지의 각도 등에 의해 숫자 영역의 위치가 어긋날 경우 영역 박스 안에 있는 4개의 점을 이용하여 번호판 크기를 조정해 주면 된다. 번호판 영역 숫자 편집 창에서 최종적인 번호판 영역을 편집하고 번호판 확정을 선택하면 분석을 위한 준비는 끝났다.

4 분석 버튼을 선택 시 기본, 심층 분석, 종합 결과가 한 번에 실행된다. 종합 결과에서 인식 종합결과, 복원 종합결과, 인식&복원 종합결과를 확인할 수 있다. 분석 결과는 1위~3위까지 랭크로 표기된다. 또한 색상 적합도를 통해 분석율의 정확도를 나타낸다.

5 차종(승용, 승합, 화물, 특수자동차), 용도(운수사업용, 비사업용), 색상을 선택하면 AI 분석결과와 차적조회 데이터간 일치하는 데이터를 조회하고 차적결과 유무를 통해 분석 결과 번호판의 실존 여부를 확인할 수 있다. AI 분석결과뿐만 아니라 차량번호 추가지정을 통해 사용자 지정 데이터 값도 함께 조회할 수 있다. 차량번호 추가 지정 버튼을 통해 입력파일 양식을 내려 받아 앞번호, 가운데 한글, 뒷 번호를 양식에 맞게 입력하면 사용자 지정 데이터를 입력할 수 있다.

Ⅲ 발전 방안

2020년 한국전자통신연구원(ETRI)과 R&D 협업을 통해 개발하여 연구소 내 전문 분석관이 번호판 분석 작업을 통해 기술 검증 후, '21년 시범 운영에 필요한 필수 기능들을 선별, 추가 개발하여 '22년 실제 치안현장에 활용도 높은 서비스 제공을 시작하였다. 시스템의 활성화를 위해 찾아가는 사용자 교육 및 경진대회를 진행하였고 현재 시스템 사용자 수는 1623명('23. 9. 기준)으로 우수 사례도 발굴하였다.

NPDR 시스템 활용 우수 사례
1) 뺑소니 용의차량의 번호를 차량번호 분석시스템을 활용하여 특정, 피의자 조기 검거
2) 프레임 에버리징(이미지 중첩), 스마트 리사이즈(무손상 이미지 확대)기능과 선명도·화질개선 작업 및 화질개선한 이미지를 분석에 활용하여 차량번호 종합 일곱자리 제공, 절도 피의자 검거에 기여
3) 차량번호분석시스템 결과를 바탕으로 차종 및 색상 등을 고려하여 보이스피싱 수거책 차량 번호 특정
4) 지역 및 문자 특정이 불가한 상태에서 차량번호 분석시스템과 TCS 조합 등을 통해 절도 피의자 검거 기여
5) 야간에 촬영된 블랙박스 영상으로 빛 반사 등으로 영상정보가 손실되어 육안으로 번호판 식별이 불가한 상태에서 차량번호 분석시스템과 디지털 포렌식 소프트웨어를 활용하여 용의자 의심 차량 특정에 기여
6) 원거리에서 촬영된 CCTV로 차종 및 번호판 식별이 불가한 상태에서, 차량번호 분석시스템과 디지털 포렌식 소프트웨어 활용 및 차량 디자인 분석을 통해 공갈 피의자 특정에 기여

1. NPDR 시스템 발전 방안

위와 같이 NPDR 분석시스템을 활용하여 용의자를 특정·검거한 사례도 있지만 NPDR 시스템이 피의자 특정 시 핵심적인 시스템으로 거듭나기 위해선

현장의 목소리를 반영한 개선이 필요하다. 차량번호판 분석 지원 및 시스템 시범운영을 통해 모아진 개선 사항을 아래와 같이 정의하였다.

AI기반 차량번호 분석시스템 고도화 案
1) 영상의 특성을 반영한 영상처리 기법 적용
2) 일관적·객관적인 결과 값이 도출될 수 있도록 시스템 개선 필요
3) 모델의 정확도 향상 및 기능 확장을 통한 기술 고도화 도모
4) 영상정보의 부재로 의미있는 정보를 얻기가 곤란한 경우 공백 처리

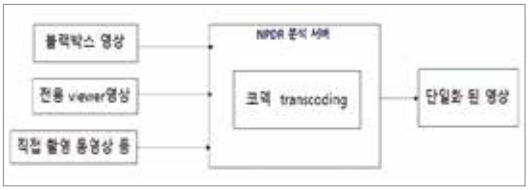
치안정책연구소는 1),3)안을 '23년 NPDR 기능 고도화 범위로 잡고 12월 완수 목표로 진행 중에 있다.

2. '23년 NPDR 시스템 고도화 사업

AI기반 차량번호판 분석시스템 고도화 사업을 통해 개선되는 기능에 대해 소개한다.

사업 추진 범위
1) 다양한 수집 방법에 따른 단일화된 영상 데이터 전처리 방법 구축(동영상 핸들링 도구 적용)
2) 딥러닝 기반 이미지 화질 개선 체계 구축을 통한 차량번호판 영역 설정 환경 개선
3) NPDR Client에서는 지원하지 않는 차량번호판의 차량번호 인식 솔루션제공

현장에서 사건이 발생했을 때, 증거자료를 수집하는 방법은 개개인 또는 환경에 따라서 달라진다. 녹화 장비에서 직접 촬영하거나 블랙박스나 방범용 CCTV 장비에서 USB로 백업받는 등 다양하게 이루어진다. USB로 받은 영상 및 SD 카드 영상은 재생 가능하도록 파일을 변환하거나 전용 플레이어를 사용하여야 영상 재생이 가능하다. 이런 경우 NPDR 시스템에 동영상 파일 분석 지원이 불가하여 전용 플레이어 재생화면을 캡쳐하여 해당 이미지로 분석을 진행하게 된다. 문제는 스크린샷 방법에 따라 화질이 심각한 손상을 입게 된다는 것이다. 이러한 문제를 해결하기 위해 NPDR 고도화 사업을 통해 다양한 수집 데이터 지원 체계 구축을 통한 단일화된 분석 전처리 단계를 지원한다.



〈그림 4〉 분석 전처리 단계 표준화

현재 경찰에서 흐릿한 차량번호판 분석을 위해 SCAS를 통해 본청·시도청 영상분석관에게 분석 의뢰하거나, 내부망 NPDR 시스템에 접속하여 사용자가 직접 분석할 수 있다. NPDR시스템의 경우 사용자가 직접 분석하여 결과를 즉시 볼 수 있다는 장점은 있지만 사용자가 영상 특성에 따른 영상처리 기법에 대한 지식이 없는 경우 영상에서 의미있는 정보를 획득하기가 쉽지 않다는 단점도 있다. 이에 치안정책연구소는 분석 결과의 신뢰성 향상을 위해 본청·시도청 영상분석관을 대상으로 영상의 특성에 따른 영상처리기법에 대한 노하우를 학습하고 시스템에 반영할 방안에 대해 논의 중에 있다. 뿐만 아니라 고도화 사업을 통해 낮은 해상도와 작은 이미지에 대한 화질 개선을 위한 여러 알고리즘 학습도 진행 중에 있으며 이는 차량번호판 영역 설정 환경을 개선할 것으로 기대된다.

마지막으로, NPDR Client에서는 지원하지 않는 차량번호판의 한글(용도, 지역)인식 솔루션개발을 위해 지난 7월, 치안정책연구소는 차량번호판데이

터 셋 제작 용역을 통해 12만건 이상의 학습 데이터 셋을 구축하였고, 구축 데이터를 활용하여 한글 검출을 위한 모델 학습을 진행하고 있다. 이는 차량의 용도가 특정되지 않거나 피의자 불특정 시 핵심적인 기능을 할 것으로 예상된다.

Ⅳ 향후 계획

현재 차량번호판 인식 기술은 주차장 자동출입을 위한 차량번호판 인식 제품, 체납 차량 번호인식 시스템 제품 등에 주로 활용되어 상용화가 이루어지고 있는 반면 차량 색상이나 모양 등 외관 특성을 이용한 차량 인식 기술은 아직 개발 진행되고 있는 분야이다. 자동차를 활용하여 피의자를 특정하기 위해서는 차량번호뿐만 아니라 차종 또한 필수적으로 분석되어야 한다. 이에는 많은 준비가 필요하겠으나, NIA에서 주관하는 인공지능 학습용 데이터 구축 사업을 활용하거나 자체 데이터 구축 사업을 통해 데이터를 축적하고 알고리즘을 단계별로 세분화하고, 필요에 따라 전체 알고리즘을 구성함으로써 자동차 사진 및 영상만으로 필요한 정보를 추출하고 제공하는 AI기반 차량 인식 시스템이 개발된다면 치안현장에서의 활용도가 훨씬 높아질 것이라고 생각된다.

Ⅴ 맺음말

NPDR 시스템은 AI(인공지능)를 활용한 과학적 현장지원 시스템 개발 필요성 대두와 함께 과학치안 R&D 산출물을 실용화한 대표적인 시스템이다. 아직 TRL 9단계 중 7단계, 실용화 단계로 현장에서 성능과 신뢰성을 평가받아 표준화 및 인허가 취득(8단계) 후 본격적인 운영으로 나아가야 한다. 실증 분석을 넘어 시스템 운영으로 가는 갈림길에서 현장 수사관들의 호응도 및 활용도는 중요한 척도가 된다. 이를 위해서는 다양한 부서들과 협의를 진행하는 것뿐만 아니라 편리하게 사용할 수 있으면서도 성능 좋은 시스템이 뒷받침되어야 한다. 이러한 시스템이 탄생할 수 있게 담당 연구자로서 현장과 기술에 귀 기울여 NPDR 시스템이 과학 치안의 좋은 선례가 되기를 기대하며 오늘도 노력한다.

PSI

인공지능 기반 차량 번호판 분석 기술

㈜에이치오아이씨티 연구소장 권영선

Ⅰ 연구의 배경과 필요성

차량을 이용한 범죄와 CCTV등을 활용한 교통 시스템 발전에 따라 차량 번호판 인식 및 분석에 대한 관심이 높아지고 있다. 차량 번호판 인식 및 분석 기술은 수집된 CCTV 또는 이미지를 수동 또는 자체 머신비젼용 지능형 모듈, AI기반의 딥러닝 등을 활용해 차량 번호판을 추적하는 기술이다.

차량 번호판의 경우 차량을 특정할 수 있는 고유한 정보로 차량 추적에 활용이 가능하여, 차량을 이용한 범죄시, 해당 차량의 이동 경로를 추적할 수 있는 실마리가 되어 빠른 용의자 검거에 활용될 수 있다. 과거에는 고비용의 자체 지능형 모듈 개발을 통해 번호판 분석이 이루어졌으나, 높은 구축 비용과 다양한 환경에서 수집된 손상 이미지나 낮은 해상도의 이미지는 분석이 어려웠다. 딥러닝은 이러한 손상되거나 원거리의 작은 이미지, 낮은 해상도 이미지 등의 복잡한 환경에서도 높은 정확성을 가지는 결과를 제공하여, 비교적 낮은 비용으로 정확한 분석이 가능하다.

본 리뷰에서는 NPDR 고도화에 적용될 AI 딥러닝 기술을 활용한 자동차 번호판 인식 및 분석 방법에 대해 소개하고자 한다.

Ⅱ AI 딥러닝을 활용한 번호판 분석 고도화 개요

1. AI 딥러닝을 활용한 번호판 인식 개선 방향

AI 딥러닝 이미지 처리 기술의 발전에 따라 손상되거나 식별이 어려운 차량 번호판 식별까지 가능해졌다. 현재 현장에 차량번호 분석 시스템(NPDR)이 적용되면서, 식별이 어려웠던 흐릿한 번호판 분

석이 가능해짐에 따라 신속한 범죄 대응으로 많은 도움이 되고 있다. NPDR 적용 이후 AI딥러닝 이미지 처리 기술이 발전함에 따라 야간 또는 원거리의 이미지도 학습된 이미지를 활용하여 비교적 선명한 이미지로 보정할 수 있게 되었다. 이러한 딥러닝 이미지 보정 기술을 NPDR에 추가 적용하여 다양한 환경에서 수집된 이미지에 대한 복원 작업을 진행함으로서 분석 정확도를 높이고자 한다.

2. 분석 정확도 개선을 위한 적용 기술 개요

현재 수동으로 진행되는 이미지 전처리 과정을 딥러닝 기반의 이미지 처리 기술을 적용하여, 보정된 이미지를 통해 차량 번호판 자동 분석의 정확도를 높여주고, 분석관이 보정된 이미지를 통해 분석된 결과와 비교해 볼 수 있도록 구성하고자 한다.

다양한 딥러닝 이미지 보정 및 분석 기술을 Optional하게 적용할 수 있도록 구성하여, 다양한 상황에 대해 적합한 딥러닝 모델을 적용할 수 있어 분석의 정확도를 높인다.

흐릿한 이미지나 흔들린 이미지의 복원에 적합한 NAFNet 모델을 활용한 Deblurring과 기존의 ESRGAN에 다양한 전처리와 열화 기법 단계가 추가된 Real-ESRGAN 모델이 적용된 super resolution 기술을 제공한다. 또한 객체 탐지(Object Detection) 기술 적용을 통해 이미지에 대한 번호판 영역 자동 식별 기능을 탑재하여, 수동으로 지정하기 어려운 번호판 영역을 자동 식별할 수 있도록 한다. 이처럼 다양한 조합으로 이미지 분석이 가능한 환경을 조성하고자 한다. 해당 내용 적용 시 분석관의 판단에 다양한 정보를 제공할 수 있고, 손상된 이미지를 1차 전처리, 2차 딥러닝을 이용한 이미지 복원, 3차 분석을 진행할 수 있으므로 차량 특정이 더욱 빠르고 정확해질 수 있다.

Ⅲ AI 딥러닝 이미지 처리 기술 기반의 번호판 보정 및 추출

AI 딥러닝을 활용한 차량 번호판 분석 기술은 열악한 이미지를 원본 이미지와 유사하도록 보정하는 복원 기술과, 이미지 패턴을 분석하여 결과를 추론하는 이미지 분석 기술로 구분된다.

1. 이미지 복원 기술

이미지 분석 기술을 적용하기 전에 이미지 복원 기술을 활용하여 이미지를 보정하는 단계를 거침으로써 이미지 분석의 정확도를 향상시킬 필요가 있다.

이미지 Deblur 기술은 흐린 이미지의 선명도를 개선하기 위한 혁신적인 방법으로 주목을 받고 있다. Blur는 주로 카메라의 움직임, 초점 오류 등에 의해 발생한다. 이를 극복하기 위해 합성곱 신경망(Convolutional Neural Network)을 기반으로 훈련된 모델을 활용하여 Blur 효과를 역전시키는 것이 목표이다. Deblur 모델을 효과적으로 훈련 시키기 위해서는 흐린 이미지와 해당 이미지의 선명한 버전으로 이루어진 대량의 훈련 데이터가 필수적이다.

〈그림 1〉 Blur 처리된 원본 이미지

〈그림 2〉 Deblur 모델 적용 결과

〈그림 3〉 저해상도 원본 이미지

이미지 초해상도(Super-Resolution) 기술은 저해상도(Low Resolution) 이미지를 고해상도(High Resolution) 이미지로 복원하는 기술로서 딥러닝 모델을 활용하여 세부 정보를 풍부하게 만들어 시각적 품질을 향상시키는 것이 목표이다. Super-Resolution 모델을 훈련 시키기 위해서는 고해상도 이미지와 해당 이미지의 저해상도 버전으로 이루어진 대량의 훈련 데이터가 필수적이다. 이 훈련 중 원본 이미지와 재생성된 이미지를 사이의 품질 차이를 측정하여 최대 신호 대 잡음비(Peak Signal-to-Noise Ratio) 지수가 높을수록 보다 높은 이미지 품질을 나타낸다.

$$PSNR = 10 \cdot log_{10}(\frac{MAX^2}{MSE})$$

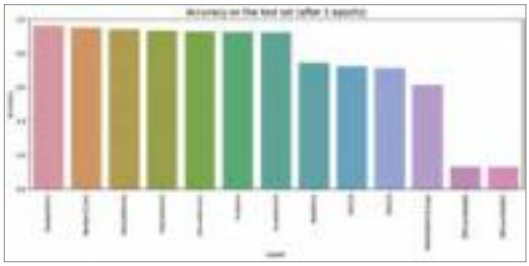
PSNR 계산에서 MAX는 이미지의 최대 픽셀 값을 나타내며, MSE는 원본 이미지와 재생성된 이미지 간의 픽셀 단위 오차를 나타낸다.

〈그림 4〉 Super-Resolution x4 모델 적용 결과

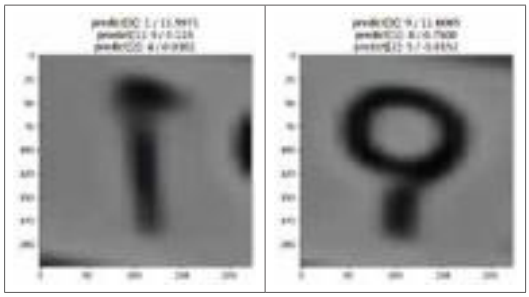
2. 이미지 분석 기술

이미지 분석 기술은 이미지 복원 기술을 적용한 이미지에 대하여 패턴을 분석하여 이미지를 사전 정의된 범주로 분류하거나 이미지 내에서 객체의 위치를 검출하는 작업이 가능하다.

이미지 분류 기술은 주어진 이미지를 사전에 정의된 범주로 분류하는 것이 목적으로 한다. 이미지 분류 모델은 주어진 훈련 데이터를 이용하여 이미지의 특징과 패턴을 학습하여, 이를 바탕으로 새로운 이미지에 대한 예측을 수행한다. 이미지 분류 모델의 종류 다양하나, 학습 설정에 따라 정확도의 차이를 보일 수 있다.



〈그림 5〉 알고리즘별 번호판 데이터 셋 학습 정확도



〈그림 6〉 이미지 분류 모델 적용 결과

이미지 객체 검출 기술은 이미지 내에서 훈련된 특징과 패턴을 가진 객체를 검출하여 바운딩 박스로 지정하고 사전에 정의된 범주로 식별하는 것을 목적으로 한다. 이미지 객체 검출 모델은 한 이미지 내에서 다수의 객체를 동시에 식별하는 다중 객체 감지가 특징을 가진다.

〈그림 7〉 이미지 객체 검출 모델 적용 결과

이미지 분류와 이미지 객체 검출은 사전에 정의된 범주에 따라 이미지를 분류하는 것이 비슷하나, 두 모델의 결정적인 차이가 있다. 이미지 분류는 전체 이미지에 대한 분류로서 최종적으로 한 가지의 결과로 예측되며, 이미지 객체 검출 모델은 이미지 일부에서 객체를 검출하여 한 이미지 내에서 다수의 객체를 동시에 검출하여 여러 가지의 결과를 반환한다.

Ⅳ 맺음말

AI 딥러닝을 활용한 차량 번호판 분석 및 인식은 데이터셋과 딥러닝 모델의 발전에 따라 지속적으로 발전해 왔으며, 활용 범위가 넓어지고 있다. 현재 NPDR에 Deblurring과 super resolution, 객체 탐지 기술을 적용함으로써 손상된 번호판 이미지 분석이 가능하다. 추후 차량번호 분석 시스템(NPDR)에 더욱 다양한 AI 딥러닝 이미지 분석 모델 적용을 통해 손상되거나 낮은 화질의 차량 번호판 이미지에 대한 분석 정확도가 높아질 것으로 예상된다. PSI

음성인식 기술의 발전과 전망

다윈인텔리전스 이사 김영훈

I 음성인식 기술의 배경과 필요성

인간의 음성은 언어를 표현하고 정보를 전달하는 가장 강력한 수단 중 하나이다. 그러나 음성 데이터를 컴퓨터가 이해하고 처리하기 위해서는 문자 형태로 변환해야 한다. 이러한 목적을 달성하기 위해 사용되는 기술 중 하나가 바로 음성인식 기술인 STT(Speech-to-Text)이다. 음성인식 기술은 음성을 텍스트로 변환하는 기술로 음성인식, 음성번역, 음성합성 등 다양한 분야에서 활용되고 있다. 음성인식은 현대 사회에서 다양한 분야에서 활용되며 그 혁신적인 성과로 많은 주목을 받고 있다.

대표적으로 음성인식 기술이 사용된 분야는 의료 분야, 교육 분야, 콜센터 등이 있다. 의료 분야에서는 의사들이 환자의 진단 및 치료 과정을 기록하기 위해 음성 녹음을 텍스트로 변환할 수 있다. 의료 정보의 정확성과 효율성을 증가시킬 수 있다는 강점이 있다. 교육 분야에서는 온라인 강의나 교육 자료를 음성 또는 동영상으로 제공하는 경우, 음성인식 기술을 사용하여 수강생들에게 텍스트 형식의 내용을 제공할 수 있다. 마지막으로 콜센터에서는 상담원과 고객의 실시간 상담 내용을 상담원이 실시간으로 확인하여 시끄러운 환경 또는 이해하기 어려운 사투리도 문자로 확인하여 보다 정확하고 빠르게 고객을 응대할 수 있다.

또한, 음성인식 기술은 다양한 분야에서 필요로 한다. 음성으로 명령을 내리는 대화형 AI 서비스 또는 스피커, 전화 상담, 회의록 작성 등에서 활용된다. 특히 경찰, 병원, 소방서 등과 같은 응급 상황에서는 민원인이 긴장하거나 흥분상태 또는 주변 환경이 시끄러운 경우가 많다. 그래서 더욱 응급 상황에서는 실시간 음성인식 기술이 필요로 한다. 음성을 문자로 변환하여 응급 상황을 접수하는 직원이 보다 정확하고 빠르게 상황을 인지하고, 필요한 서비스를 제공하여야 한다.

Ⅱ 음성인식 기술의 개요

음성 문자 변화 기술, 음향 모델링은 음성 신호의 음향 특성을 캡처하는 음성인식 시스템의 핵심 구성요소이다. 기존 음성인식 시스템은 음향 모델링을 위해 HMM(Hidden Markov Model)을 사용했지만 최근 기술 발전으로 CNN(Convolution Network), RNN(Recurrent Neural Network) 및 Transformer 기반 모델과 같은 딥 러닝 기술에 중점을 두었다. 이러한 딥 러닝 모델은 특히 시끄러운 환경과 다양한 억양을 처리할 때 정확도와 견고성이 크게 향상되었다. 언어 모델링은 음성 신호의 언어적 맥락을 캡처하는 데 초점을 맞춤 음성인식 시스템의 또 다른 중요한 구성요소이다. 전통적인 n-gram 모델은 언어 모델링에 널리 사용되었지만 최근 연구에서는 RNN, LSTM(Long Short-Term Memory) 네트워크 및 언어 모델링을 위한 Transformer 기반 모델과 같은 보다 발전된 기술을 탐구했다. 이러한 고급 언어 모델링 기술은 대화체 음성, 어휘 외 단어 및 도메인별 언어 처리에 있어 개선을 보였다. 디코딩은 음향 및 언어 모델의 출력을 최종 문자 출력으로 변화하는 프로세스이다. Hidden Markov 모델 기반 Viterbi 디코딩과 같은 전통적인 디코딩 알고리즘이 널리 사용되었지만 최근 발전은 별도의 음향 및 언어 모델이 필요하지 않은 엔드 투 엔드(End-to-End) 음성인식 시스템에 중점을 두고 있다.

딥 러닝 기술을 사용하여 음성 신호를 문자에 직접 매핑하는 엔드 투 엔드 음성인식 시스템은 정확성과 효율성 측면에서 유망한 결과를 보였다. 음성 문자 변환의 응용에서 음성 전사 서비스인 STT 변환은 음성 언어를 서면 텍스트로 자동 변환할 수 있는 전사 서비스에서 널리 사용되었다. 이는 의료, 법률, 미디어 등 문서화, 콘텐츠 생성 및 접근성에 필사본 서비스가 중요한 산업에서 중요한 응용 분야를 갖고 있다. AI 가상 비서인 Amazon의 Alexa, Apple의 Siri, 삼성전자의 빅스비와 같은 AI 가상 비서는 음성 명령을 처리하고 응답을 제공하기 위해 음성인식 기술에 크게 의존한다. STT 변환을 통해 이러한 AI 가상 비서는 음성 언어를 이해하고 그에 따라 응답할 수 있어 매우 편리하고 사용자 친화적이다.

고객 서비스에서 STT 변환은 고객 서비스 어플리케이션에 사용되어 고객과의 자동화된 음성 기반 상호 작용을 한다. 여기에는 콜 센터 운영, 음성 기반의 보이스봇 또는 챗봇, 가상 고객 서비스 상담원 등의 서비스가 포함되어 있어 보다 효율적이고 개인화된 방식으로 고객 문의를 처리하고 도움을 줄 수 있다. 의료분야에서 STT 변환은 의료 녹음, 음성 기반 환자 기록 관리, 음성 제어 의료 장치에 사용될 수 있는 중요한 응용 분야를 가지고 있다. STT 변환으로 의료 전문가는 음성 명령을 사용하여 환자 정보를 효율적으로 캡처하고 의료 기록에 접근하여 환자 치료 및 작업 흐름 효율성을 향상시킨다.

접근성 도구에 STT 변환이 사용되어 청각 장애가 있는 개인이 정보에 더 쉽게 접근할 수 있다. 이를 통해 비디오, 팟케스트 및 기타 멀티미디어 컨텐츠의 음성 언어를 문자로 변환할 수 있으므로 청각 장애가 있는 개인이 컨텐츠에 접근하고 이해할 수 있다.

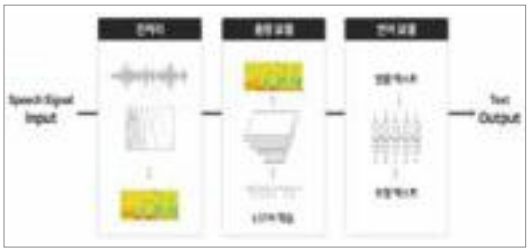
STT 변환의 상당한 발전에도 불구하고 몇 가지 과제와 한계가 여전히 존재한다. 주요 과제 중 하나는 시끄러운 환경에서의 정확도이다. 현재 STT 기술을 보유하고 있는 업체들은 혼잡한 장소나 배경 소음이 있는 환경과 같은 시끄러운 환경에서 음성 신호를 정확하게 인식하는 데 어려움을 겪는 경우가 많다. 그리고 화자 분할이다. 다수의 사람들이 대화를 할 때 각각의 화자를 분할하여 음성을

문자로 변환해야 하는데 이러한 기술적인 부분에서는 아직까지도 많은 어려움을 겪고 있다. 특히 회의록을 작성하는 경우나 다수의 사람들이 대화를 하는 경우 말하는 화자를 분할하여 음성을 문자로 변환해야 우리에게 보다 편리하고 좋은 기술이 될 수 있다.

Ⅲ 음성인식 기술 방법

1. STT 기술

음성 인식 기술의 원리는 기본적으로 음성에 대한 파형을 분석하는 것에서부터 시작한다. 1/1000초 단위로 음성을 작게 잘라 그 파형을 신호 처리를 통해 10개 이상의 숫자로 변환한다. 이 숫자들은 성대 진동 횟수, 입모양에 따라 결정되는데, 이러한 데이터들이 특정 패턴으로 인식되어 언어를 처리한다. (그림 1)[1]



〈그림 1〉 음성인식 과정

STT를 위한 데이터에는 크게 음향학적 관점과 언어학점 관점으로 볼 수 있다. 음향학적 관점은 말하는 화자, 공간, 소음 등의 환경적인 데이터가 주를 이루고 언어학점 관점에서는 어휘, 문맥, 문법 등을 모델링하기 위한 언어 데이터가 주를 이룬다.

STT는 크게 음성/언어 데이터로부터 인식 네트워크 모델을 생성하는 오프라인 학습 단계와 사용자가 발성한 음성을 인식하는 온라인 탐색 단계로 나눌 수 있다. STT 엔진은 음성과 언어 데이터의 사전 지식을 사용해서 음성 신호로부터 문자 정보를 출력하는데 이 때 해석이라는 차원에서 STT 알고리즘을 디코더(Decoder)라고 부른다. 디코딩 단계에서는 학습 단계 결과인 음향 모델(Acoustic Model), 언어 모델(Language Model)과 발음 사전(Pronunciation Lexicon)을 이용하여 입력된 특징 벡터를 모델과 비교, 스코어링(Scoring)하여 단어 열을 최종 결정 짓는다. 음향 모델링은 해당 언어의 음운 환경별 발음의 음향적 특성을 확률 모델로 대표 패턴을 생성하는 과정이고, 언어 모델링은 어휘 선택, 문장 단위 구문 구조 등 해당 언어의 사용성 문제에 대해 문법 체계를 통계적으로 학습하는 과정이다. 또한 발음 사전 구축을 위해서는 텍스트를 소리 나는 대로 변화하는 음소 변환(Grapheme-to-Phoneme) 구현 과정이 필요하며, 표준 발음을 대상으로 하는 발음 변화 규칙만으로는 방언이나 사용자의 발화 습관과 어투에 따른 다양한 패턴을 반영하기 어려운 경우가 있어 별도의 사전 구축이 필요하다.

2. STT 성능

STT의 성능은 데이터 베이스 크기와 품질에 비례하여 향상될 수 있다. 상용 서비스에 적용되는 음향 모델의 대부분 확률 통계 방식인 HMM 기반으로 이루어졌고, 2010년대 들어서면서 딥 러닝 기반으로 HMM/DNN 방식으로 단어 인식 오류를 개선하여 20%의 성능 향상을 이루어냈다. 이는 기존 HMM의 각 상태 확률 분포를 모델링하는 데 사용되는 GMM(Gaussian Mixturt Model)을 DNN으로 대체하는 것이다. 그 외의 모델 구분 단위, 단위

별 학습 자료 자동 생성 및 모델 결합을 통한 문장 인식 확장 등은 HMM에서의 방식을 다수 그대로 사용하는 반면 DNN을 추정해야 하는 파라미터가 많아 학습 시간이 많이 소요된다.

최근에는 시퀀스투시퀀스(Sequence-to-Sequence) 방식의 RNN 기반으로 속도와 성능 면에서 좋은 결과를 보이고 있다. 음성 인식에서도 엔드 투 엔드 학습 방식의 발전으로 일련의 오디오 특징을 입력으로 일련의 글자 또는 단어들을 출력으로 하는 단일 함수를 학습할 수 있게 되었다.

또한 CTC(Connectionist Temporal Classification)이라는 모델로 입력 데이터와 레이블 사이의 음성 정렬 정보가 없어도 학습이 가능하다. 이와 같은 다양한 딥 러닝 학습법을 통해 계속해서 음성 인식의 성능은 향상되고 있다.

Ⅳ 맺음말

음성 인식 기술은 딥 러닝을 통해 비약적 발전을 거듭했다. 그러나 아직 한국어의 경우, 인식 단위로 의사 형태소로 사용하기 때문에 후처리 모듈에서 인식 결과를 어절 단위로 재구성하는 과정이 필요하며, 일반적으로 숫자나 영문의 경우 변화해 주는 텍스트 정규화 과정 또한 필요하다. 또한 음성 인식 결과가 완벽하지 않기 때문에 오류 보정을 위한 노이즈 채널 모델과 같은 후처리 방식을 적용하여 그 정확도를 향상시킨다. 외부에서 제공하는 음성 인식 API를 사용하는 경우에는 음성 인식 엔진이 블랙박스였지만, 선순환적으로 언어 모델을 구성하는 데 후처리 보정 기술을 적용한다면 별도의 처리 과정의 부담을 줄이면서 인식 성능의 향상도 가져갈 수 있을 것이다.

음성 인식 기술의 도입으로 우리 생활에서 많은 곳에 영향을 미칠 것으로 기대한다. 회의록 작성, 콜센터 직원의 업무 효율성 향상, 응급 상황 시 대응 처리 속도 향상 등 다양한 분야에서 긍정적인 효과를 가져올 것으로 예상한다. 특히 경찰, 병원, 소방서 등 응급 상황 경우에는 음성 인식 기술의 성능이 좋아진다면, 응급 환자의 신고 전화가 시끄러운 환경이나 발신자가 당황하여 정신이 없어 말을 또박또박 하지 못하고 얼버무린다고 해도, 딥 러닝 기술로 성능이 좋아진 음성 인식 기술의 도입으로 빠르게 대응할 수 있을 것으로 기대할 수 있다.

PSI

참고 문헌

[1] V. M. Reddy, T. Vaishnavi and K. P. Kumar, "Speech-to-Text and Text-to-Speech Recognition Using Deep Learning," 2023 2nd International Conference on Edge Computing and Applications (ICECAA), Namakkal, India, 2023, pp. 657-666.

[2] R. A. K, T. Triveni, V. N R, V. K and R. B M, "Speech to Text App Customized for Police Functioning in Different Languages," 2023 4th International Conference for Emerging Technology (INCET), Belgaum, India, 2023, pp. 1-4.

[3] 조진관. (2019). 빅데이터 기반 음성언어 처리 기술에 관한 연구. 한국지식정보기술학회 논문지, 14(4), 391-399.

[4] 음성 언어 처리 기술, 어디까지 왔나. 국립국어원

현장경찰관 법집행력 강화를 위한 실감형 가상훈련 프로그램 개발

㈜스코넥엔터테인먼트 부사장 최정환

Ⅰ 연구의 배경과 필요성

최근 가속화하고 있는 사회·경제적 환경의 변화는 경찰의 역할에 대해 새로운 도전에 직면할 것을 요구하고 있다. 특히 우리 사회는 스마트기기의 대중화와 더불어 소셜 네트워크 서비스(Social Network Services, 이하 SNS)가 확산되면서 사회 복잡성의 증대로 인해 더 많은 이해관계와 가치들이 상충되고 있으며, 여기에 사회 양극화로 인한 집단 간·계층 간의 갈등과 불평등 문제와 같은 기존 사회문제들이 고착화됨과 동시에 새로운 기술 발전에 따라 등장한 사이버 범죄와 같은 신종범죄와 사회문제들도 지속적으로 양산되고 있다. [1)]

이러한 영향으로 현대사회에서 경찰의 임무는 규제 행정적 법집행(law enforcement)수준에 머무르지 않고 적극적인 범죄예방(crime prevention)과 대국민 서비스 제공 등으로 그 범위가 더욱 확대되고 있으며, [2)] 최근에는 '4대 사회악 예방', '사회안전망 구축' 등과 같은 안전 관련 정책과 함께, 각종 대형사고와 안전사고 등으로 인해 사회 안전에 대한 국민들의 관심이 높아지면서, 사건·사고 발생 시 최우선 접점인 경찰에게 각종 사회현상에 대한 법적, 절차적 지식을 바탕으로 한 전문적이고 책임 있는 임무 수행을 요구하고 있다. [3)] 특히, <그림 1> 112 신고 유형이 보여주는 것과 같이 112신고를

1) 이승민. (2013). 스마트기기와 SNS 활용이 사회자본 형성에 미치는 영향 연구. 한국문헌정보학회지, 47(2), 161-180.

2) 이승주. (2012). 경찰행정 정책과정의 시민참여에 관한 연구. 한국공안행정학회보, 21(4), 189-222.

3) 전대욱. (2013). 지방자치단체의 생활안전(4대악) 역할 및 대응시스템 구축방안. 한국지방행정연구원.

중심으로 신고 접수 및 사건 처리 절차가 점차 세분화·구체화되고 있으며, 이에 따른 정확한 업무처리가 이루어지지 않을 경우에는 즉각적인 민원 제기로 이어지는 상황에 직면하고 있기도 하다.

〈그림 1〉 112 신고 유형

이와 같이 현대의 경찰은 범죄의 예방과 범인 검거라는 기본 임무에 더하여 범인 검거 과정 및 사후 조치 절차에 대한 정당성 확보 등 복합적인 업무 처리를 요구받고 있는 것이다.

공무수행 중 경찰이 범인에게 피습당하거나 교통사고 등으로 부상을 입는 경우가 최근 5년 동안 1만 건에 달하는 것으로 나타나고 있으며, 같은 기간 경찰이 공무를 수행하다 순직한 경우도 81건으로 조사되었다. 부상 원인으로는 4,660건을 차지한 안전사고가 가장 많았으나(45%), 현장에서 범인으로부터 피습당하거나(2875건/28%), 교통사고를 당한 경우(2546건/25%)도 절반 이상을 차지한다.[4] 범죄·사고 현장에서의 경찰의 안전은 항상 위협받고 있어, 안전사고 및 범인 피습에 대응한 현장 경찰의 현장지원 장비 개발 및 교육·훈련 시스템이 시급한 상황이다.

현재 경찰청에서는 신임교육, 재직자 교육 등 경찰에서 시행되는 교육·훈련 전반을 포괄하는 교육·훈련계획을 수립·시행하고 있으며 최근에는 가상현실 기술을 활용하는 방향도 중요시 되고 있다.[5] 특히 다양한 현장상황에 대해 신속 정확히 판단 조치해야 하는 만큼 실제와 유사한 상황 속에서 몸으로 익히는 참여형, 체득형 교육을 하는 것이 중요하다는 인식에서이다.

스코넥엔터테인먼트를 주관으로 2020년 4월부터 연구 개발되어 진행된 경찰청 R&D 사업 '현장 경찰관 법집행력 강화를 위한 실감형 가상훈련 프로그램 개발'은 앞서 이야기한 현장 경찰관들이 위협받고 있는 안전사고와 범죄 예방에 대응 가능한 교육·훈련 시스템을 개발하는 목표와, 다음의 2가지 기준의 개발방향으로 잡았다. 첫째는 가상현실 기술을 적용하여 실제와 유사한 사건 현장을 재현하여 현장 대응능력을 높이는데 중점을 두었고, 둘째는 인재개발원등 교육센터에 가지 않고, 신임 및 재직경찰관들이 근무하고 있는 현장(경찰서, 파출소)에서 직접 사용 할 수 있는 '이동형 VR 훈련 시스템'으로 만들고자 하였다.

본 고에서는 이러한 신임 및 재직 경찰관들이 현장에서 바로 훈련이 가능한 VR 훈련 시스템을 개발하는 과정에서 기존의 현장 대응 매뉴얼을 기반으로 하는 교육체계 구축과 훈련 시스템 및 콘텐츠 개발에서의 효과성 검증을 위한 기능적, 기술적 이슈들에 대해 살펴보고자 한다.

Ⅱ 이동형 VR 훈련 시스템

본 연구를 통한 '이동형 VR 훈련 시스템' 개발의 목적과 기대되는 효과는 반복적 교육·훈련을 통하여 현장 경찰관의 현장 대응능력[6]을 향상 시키는

4) http://www.safekoreanews.com/27147

5) 정효승, 라성룡, 전태완 and 정회룡. (2022). 경찰 교육·훈련을 위한 가상현실 기반 시뮬레이터. 스마트치안연구, 3(2), 32-36.

6) 현장 대응능력 : 특정한 상황에서 원칙과 기준에 따라 필요한 조치를 수행할 수 있는 능력

것에 있으며, 실제 상황과 유사한 상황에 대한 반복적인 교육을 통하여 긴급한 현장에서의 빠른 판단과 대처능력을 증대 하고, 경찰 업무와 관련된 다양한 VR 콘텐츠 마련으로 실제와 유사한 환경이나 상황을 반복적으로 구현하여 교육함으로써 경찰 업무 수행 시 나타날 수 있는 각종 안전사고가 감소되는 것에 기대를 하고 있다.

본 연구의 '이동형 VR 훈련 시스템'에는 다음의 4가지의 개발 범위를 포함하고 있다.

1) 교육·훈련 체계구축
2) 시나리오 적용 및 평가체계 구축
3) 교육·훈련 체계에 맞춘 VR 콘텐츠 개발
4) 이동형 훈련 시스템 및 훈련용 장비 개발

1. 교육·훈련 체계구축

교육·훈련 체계 구축의 첫 단계는 교육·훈련 대상자를 구체화 하고, 대상자의 행위의 원칙과 기준을 세워 그 기준에 맞는 교육·훈련 목표를 도출하고 그에 맞는 시나리오가 반영된 교육·훈련 콘텐츠를 개발하여 교육·훈련 결과에 평가지표에 따라 평가가 되도록 하는 일련의 내용을 개발하는 것이다. <그림 2>

〈그림 2〉 교육·훈련 체계

본 연구에서의 교육·훈련 대상자는 신임 및 재직 현장 경찰관(임무 : 현장에서 초동조치를 함으로써 주민생활의 안전과 평온을 확보)으로 하였으며, 지구대, 파출소, 치안센터, 분소, 초소 및 소속 경찰관과 지역경찰업무 담당부서 실무자를 말한다.

현장 대응 능력의 판단기준이기도한 교육·훈련의 목표는 경찰 교육기관 커리큘럼, 2020 경찰백서, 치안전망 2021, 경찰범죄통계 등을 참고하여 경찰청에서 지향하는 치안활동 주요 분야 등을 탐색하여 가장 중심이 되는 법집행의 공정성을 기반으로 4가지의 기준(① 인권 존중 : 시민/개인, ② 현장에서의 소통 :시민/공동체, ③ 직무의 성실성 : 업무/개인, ④ 동료와의 협업 : 업무/공동체)으로 잡았다. <그림 3>

〈그림 3〉 교육·훈련 목표

2. 시나리오 적용 및 평가체계 구축

'행위의 원칙과 기준을 통해 지역경찰관들의 현장 대응능력의 향상'이라는 명확한 학습 목표 아래, 시나리오 반영요소를 도출하여 시나리오별 업무 매뉴얼에 따른 체크리스트에 더하여 행위의 원칙과 기준을 평가하기 위해 시나리오별 딜레마 상황을 제시하고 시나리오별 현장의 목소리를 추가적으로 분석하였다.

그래서 상기와 같이 연구된 교육·훈련 목표를 반영한 교육·훈련 체계에 따라 시나리오 개발진행과정에 <그림 4>와 같이 인재개발원과 현장 경찰관의 SOP자문위원회를 구성하여 진행하였다.

〈그림 4〉 SOP자문 위원회 회의

그리고 현장대응능력 판단기준에 근거하여 시나리오 적용 포인트를 도출하고 이를 평가 지표로 하는 평가 체계를 구축 하였다. (예 : 가정폭력 대응 시나리오)

〈그림 5〉 시나리오 적용 포인트 도출 구조

본 연구에서 개발된 시나리오는 8종으로 다음 <표 1>과 같다.

〈표 1〉 개발된 시나리오 8종

개발내용	번호	시나리오 제목	시나리오 요약
VR 교육· 훈련 시나리오	1	가정폭력 조치	남편의 가정폭력 대응 조치
	2	주점흉기 난동대응	주점에서 술을 마시고 있던 손님이 사람들이 자신을 한심하게 쳐다봤다며 욕을 하며 난동에 대한 조치
	3	집단폭력 대응	피해자가 골목길을 지나가던 중 실수로 가해자1의 어깨를 침. 가해자1은 피해자에게 시비를 걸었고, 지나가던 행인이 신고에 의한 조치
	4	치매노인 응급조치	치매 노인이 택시를 탔는데 목적지도 제대로 말하지 못하여, 택시기사가 근처 지구대로 치매노인을 데리고 온 건에 대한 조치
	5	정신질환자 응급입원	휴일 낮, 어떤 남자가 도로에 뛰어들려고 한다는 신고에 대한 조치
	6	스토킹 피해대응	귀갓길에 자신을 따라오는 남성이 있다는 피해여성의 신고에 대한 조치
	7	데이트 폭력조치	모르는 남자가 현관문을 두드리며 문을 발로 차며 고성을 지르고 있다. 빨리 와달라"신고에 대한 조치
	8	아동학대 조치	옆집 주민의 아동학대 의심 상황에 대하여 신고 접수된 건에 대한 조치

3. 교육·훈련 체계에 맞춘 VR 콘텐츠 개발

콘텐츠 구성은 현장에서 직접 조치하고 있는 4단계의 대응이 가능 하도록 구성 하였다. <그림 6>

〈그림 6〉 콘텐츠 4단계 구성

[1단계 준비] 순찰차 안에서 녹취록 청취

〈그림 7〉 신고내용 청취 구현화면

[2단계 대처] 대처 플로우

현장 진입 관련 안내사항 고지 후 대처하여야 하는 내용에 따른 대처내용을 분기로 구성하여 훈련자의 대처에 대한 평가가 이루어진다. 이하에 흉기난동에 대한 물리적 대응으로 대처를 하여야 하는 상황에서의 대처 플로우와 콘텐츠 구성을 예로 설명한다.

〈그림 8〉 대처 플로우 (예: 물리적 대응관련)

〈그림 9〉 물리적 대응 대처단계 구현화면

[3단계 사후조치] 사건을 종결하고 발생보고 및 보고서 작성하는 플로우로 진행된다.

〈그림 10〉 사후조치 구현화면

[4단계 평가] 콘텐츠 구성의 경우 평가표를 기반하여 평가 점수 기록하고 저장된다.

〈그림 11〉 훈련 결과화면

본 연구에서 개발된 8종의 시나리오를 기반으로 앞서 설명한 4단계의 구성으로 콘텐츠를 다음과 같이 개발하였다.

1) 가정폭력 조치

〈그림 12〉 가정폭력 조치

2) 흉기난동 대응

〈그림 13〉 흉기난동 대응

3) 치매노인 보호조치

〈그림 14〉 치매노인 보호조치

4) 집단폭력 대응

〈그림 15〉 집단폭력 대응

5) 정신질환자 조치

〈그림 16〉 정신질환자 응급조치

6) 스토킹 피해 대응

〈그림 17〉 스토킹 피해 대응

7) 아동학대 조치

〈그림 18〉 아동학대 조치

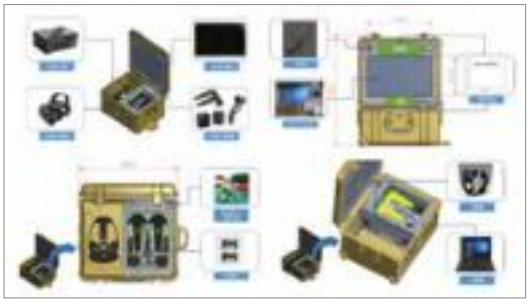
8) 데이트폭력 조치

〈그림 19〉 데이트폭력 조치

4. 이동형 훈련 시스템 및 훈련용 장비 개발

1) 이동형 훈련 시스템

경찰지구대, 파출소에서 훈련시스템을 자가운영하기 위한 조건 및 환경 선행 연구를 통하여 필요한 공간 및 이동형 훈련 시스템의 사이즈 등을 연구하여 제작하였다.

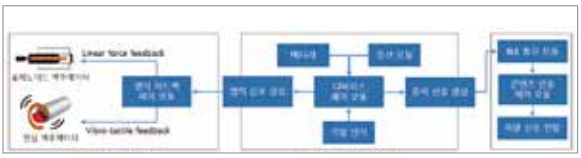


〈그림 20〉 이동형 하드웨어 정치 설계

〈그림 21〉 이동형 훈련시스템 사용 예 (서울 망우파출소)

2) 훈련용 장비 개발

본 연구는 훈련용 장비로는 경찰훈련을 위해 삼단봉 형태의 햅틱 디바이스와, 리볼버와 테이저건의 반발력과 삼단봉의 타격감을 제공하기 위한 EMS 밴드를 설계하고 제작하여 콘텐츠 내에서 연계하여 햅틱 피드백을 제공하는 것을 목표로 하드웨어 및 피드백 신호 제어, 콘텐츠 연계용 소프트웨어를 개발하였다. VR 콘텐츠 연계용 햅틱 디바이스의 시스템 구조는 햅틱 디바이스에서 방아쇠에 의한 격발을 인식하면 비쥬얼 피드백을 위해 VR 콘텐츠와 연계되어 동작 신호를 전달하며, 햅틱 피드백을 위해 햅틱 제어 모듈과 연계되어 햅틱 피드백을 생성하도록 설계하였다. 〈그림 22〉



〈그림 22〉 햅틱 디바이스의 전체 시스템 구조

햅틱 피드백을 위한 액추에이터의 위치 및 무게를 고려하여 햅틱 디바이스의 외형과 구조를 고려한 제작 실험 수행하였으며, 햅틱 설계에 따른 추가적인 타격감 변화를 구현하기 위해 ① 솔레노이드 액추에이터로 직접 타격하는 방식과 ② 고탄성 스프링을 압축 후 간접 타격하는 방식의 2가지 방식으로 연구를 진행하였으며, 사용 가능한 공간은 손잡이와 실린더 부분을 활용하여 설계를 고려하여 본 훈련 시스템에 사용하는 3종(권총, 테이저 건, 삼단봉)의 훈련용 장비를 개발하였다. <그림 23>

<그림 23> 훈련장비 개발

Ⅲ 맺음말

본 연구에서 개발한 현장 경찰 교육·훈련에 최적화된 '이동형 VR훈련 장비'를 통해 경찰관의 효율적인 교육·훈련이 가능하여 경찰관의 안전과 초기 대응에 성공률이 높아져 경찰의 사회적 인식이 높아지고 경찰을 비롯한 사회 치안훈련방법의 새로운 패러다임이 되기를 바라며 특히 다음의 2가지 부분에서 효과가 있을 것으로 기대된다.

첫째 경찰의 현장 법 집행력의 강화 목표로 하고 있어 사회적으로 경찰의 공권력 상승이 예상되며, 신임 경찰관에게 가상현실 콘텐츠로 경험하지 못한 치안현장의 위험성을 판단하도록 하며 이에 따른 초동대처법을 습득 가능 하고, 일선의 치안현장에 보급하기 위한 콘텐츠 개발을 통해 상황대처 훈련이 가능하여, 실제 사건 발생 시 안전하게 대처할 수 있는 능력을 배양 가능하다.

둘째, 8종의 훈련시나리오와 지능적으로 발전하는 NPC를 통해 치안현장을 대처할 시 위험성 인지 및 자기 방어 기술을 습득할 수 있으며, 혼란스러울 수 있는 실제 치안현장에서의 대응절차를 VR콘텐츠에서 미리 체험하여 다양한 치안현장에서의 절차적 대응능력을 배양 가능하다.

POLICE ONE

<그림 24> 이동형 VR 훈련 시스템 상표

본 연구의 결과물인 '이동형 VR 훈련 시스템'은 <그림 24>와 같이 "POLICE ONE"으로 상표 등록하고, 2021년 2022년 연속 국제치안산업대전(그림 25)에 참석하여 홍보 활동을 하였으며, 체험 참가자의 앙케이트 에서는 92%가 '실제현장에 도움이 될 것 같다. 교육 기관에 도입을 원한다'라는 결과가 나왔다.

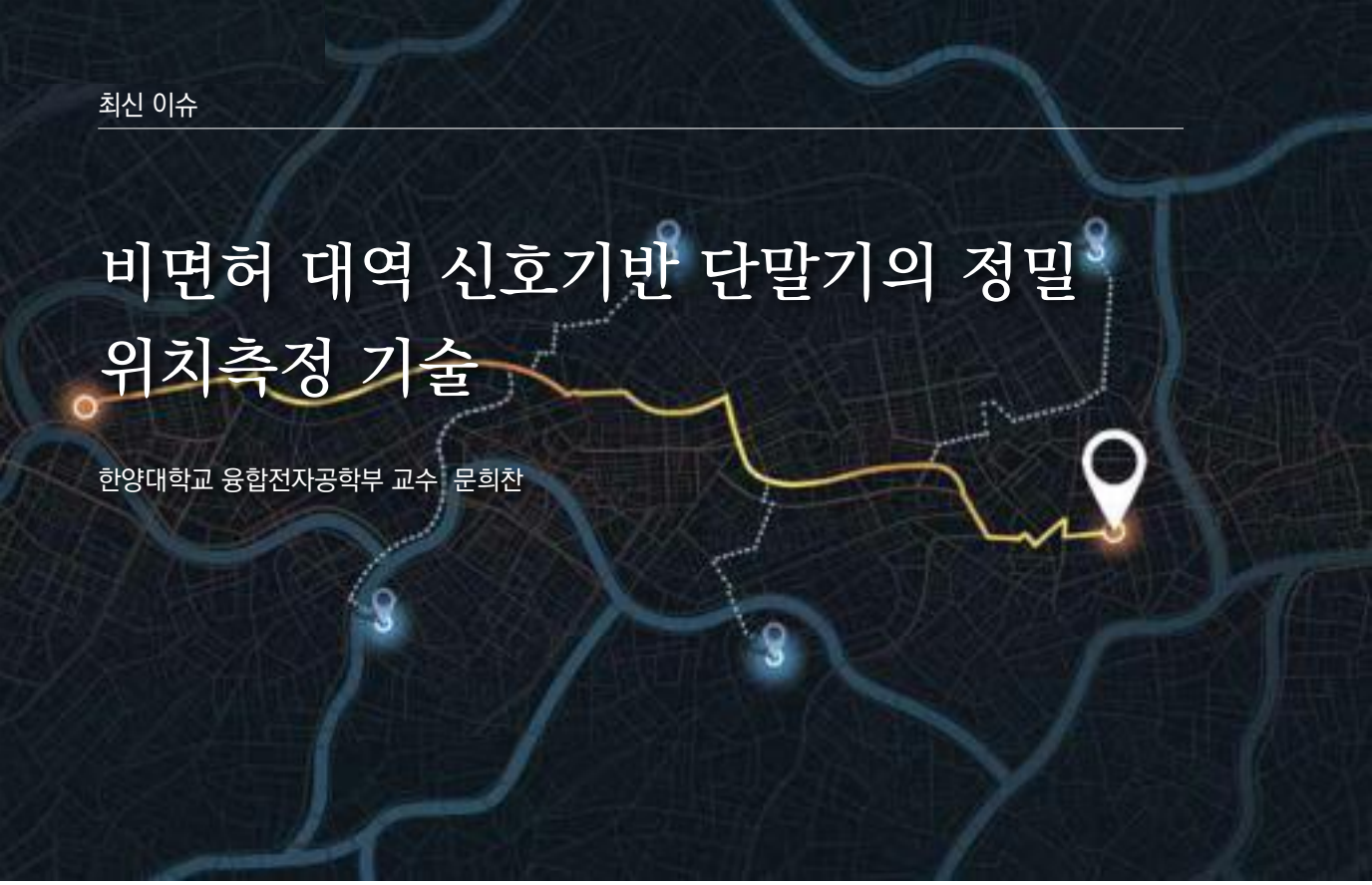
〈그림 25〉 2022 국제치안산업대전

본 시스템이 실제 많은 현장의 경찰서 파출소 등에 교육·훈련용으로 활용되어 도움이 되는 사례로 남을 수 있기를 기대한다. PSI

참고 문헌

[1] 이승민. (2013). 스마트기기와 SNS 활용이 사회자본 형성에 미치는 영향 연구. 한국문헌정보학회지, 47(2), 161-180.
[2] 이승주. (2012). 경찰행정 정책과정의 시민참여에 관한 연구. 한국공안행정학회보, 21(4), 189-222.
[3] 전대욱. (2013). 지방자치단체의 생활안전(4대악) 역할 및 대응시스템 구축방안. 한국지방행정연구원.
[4] Safe Korea News : http://www.safekoreanews.com/27147
[5] 정효승, 라성룡, 전태완 and 정회룡. (2022). 경찰 교육·훈련을 위한 가상현실 기반 시뮬레이터. 스마트치안연구, 3(2), 32-36.

■ 이 논문(글)은 2020~2022년도 정부(경찰청)의 재원으로 지원받아 수행된 연구 결과임. [내역사업(과제) 명: 효율적인 치안활동을 위한 현장지원 기술개발 (현장경찰관 법집행력 강화를 위한 실감형 가상훈련 프로그램 개발) / 연구개발과제 번호: PR08-02-00-20]



비면허 대역 신호기반 단말기의 정밀 위치측정 기술

한양대학교 융합전자공학부 교수 문희찬

I 서론

범죄, 재난·재해 및 실종 등의 긴급구조 상황에서 골든타임 확보에 구조대상자의 정확한 위치파악이 필수적이다. 그러나 많은 사건·사고에서 구조대상자의 정확한 위치파악을 못하여 골든타임을 놓치는 사례가 빈번히 발생하고 있다. 실제로 112로 구조를 요청하였을 때, 종래의 긴급구조 측위시스템을 통하여 측정한 구조대상자가 소지한 이동단말기 위치의 수평오차 범위는 50m 또는 그 이상의 수준이며, 건물 내에서 몇 층에 있는지 파악하는 것은 매우 어렵다. 또한 외산폰, USIM 이동폰 등 다수의 이동단말기는 그 위치 오차가 수백 m 이상으로 증가한다.

현재의 측위기술은 기지국 기반, GPS 및 Wi-Fi 신호 기반으로 이동단말기의 위치를 파악한다[1][2]. 그러나 기지국 기반의 측위기술은 기지국 간 간격이 멀기 때문에 500m 수준 또는 그 이상으로 오차 범위가 크다. GPS 및 Wi-Fi 기반의 측위기술은 주변 환경에 따라 성능의 열화가 심해질 수 있다. GPS 기반의 측위기술은 터널 또는 실내와 같은 장소에서 위성신호 수신이 어려워서 위치파악이 불가능하다[3]. Wi-Fi 기반의 측위기술 역시 오차 범위가 크고, Wi-Fi가 설치되지 않는 장소에서 위치파악이 어렵다[4]. 과거 30년간 구조대상자가 소지한 이동단말기의 위치를 파악하는 기술 연구가 지속적으로 진행되었으나, 현재 기술의 수준으로 골든타임 이내에 그 위치를 파악하는 것이 매우 어려운 현실이다.

미국의 FCC (Federal Communication Comission)는 긴급구조 상황에서 이동단말기의 위치에 대해 수평오차 50m, 수직오차 +/- 3m를 만족하는 기술을 미국전역에 2025년 서비스 하도록 이동통신 사업자에게 명령하고 있다[5]. 그러나 이 조건을 만족하는 기술이 아직 미국에서 개발되지 않

은 상태이다.

최근에 위치측정의 대상이 되는 타겟단말기에게 무선신호를 전송하도록 하고, 구조대원이 타겟단말기가 전송하는 무선신호를 측정하는 신호측정기를 사용하여 그 위치를 파악하는 기술이 개발되었다. 타겟단말기가 LTE와 같은 이동통신 신호 또는 WiFi 또는 블루투스 등의 비면허대역 신호를 전송하게 할 수 있다[6][7]. 이 글에서는 그 중 타겟단말기가 비면허대역 신호를 전송하는 정밀측위 기술에 대해 살펴보자 한다.

Ⅱ 비면허 대역 신호기반 타겟단말기 정밀측위 기술

위치를 파악하고자 하는 타겟단말기가 전송하는 무선신호를 탐지하여 타겟단말기의 위치를 파악하는 것이 가능하다. 구조대원은 신호측정기를 소지하고 타겟단말기가 전송하는 무선신호를 측정하여 그 위치를 파악한다. 타겟단말기가 전송하는 무선신호로 Wi-Fi 또는 블루투스 등의 비면허대역 신호를 사용할 수 있다.

<그림 1>은 비면허대역 신호를 측정하여 타겟단말기의 위치를 측정하는 측위시스템 구성도이다. 구조대상자는 사전에 본인이 소유한 타겟단말기(스마트폰 또는 스마트워치)에 긴급구조 측위를 지원하는 앱(APP) 프로그램을 설치한다. 긴급구조가 필요한 상황이 되면 구조대상자는 소지한 타겟단말기를 통해 구조요청을 할 수 있다. 긴급구조 상황에서, 해당 타겟단말기는 주기적으로 비면허대역 신호를 전송한다. 구조대원은 이 비면허대역 신호를 측정하는 신호측정기를 소지하고 구조 구조대상자의 위치를 파악한다. 위치측정서버는 타겟단말기와 신호측정기 사이의 제어 및 신호 측정 관련 정보를 교환하도록 돕는 역할을 수행한다. 또한, 위치측정서버는 신호측정기가 측정한 측정결과를 수신하고 이를 바탕으로 타겟단말기의 위치를 계산하고, 이 정보를 다시 신호측정기에 전송한다. 신호측정기는 디스플레이 등의 인터페이스를 통해 구조대원에게 타겟단말기의 위치정보를 알린다.

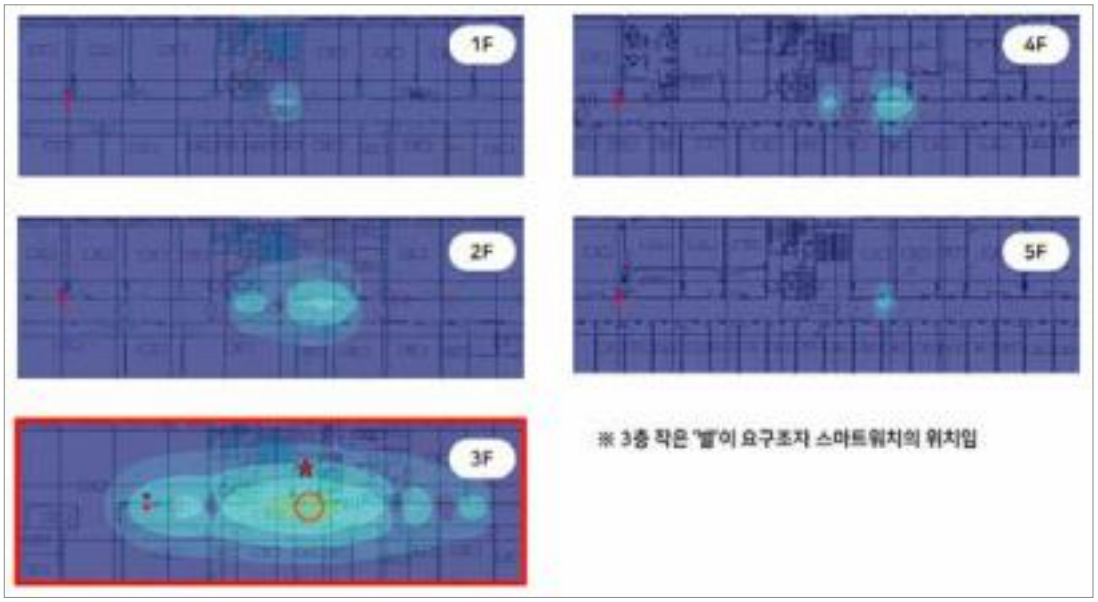
〈그림 1〉 비면허대역 신호기반 정밀 위치측정 기술의 구성도

<그림 1>의 측위기술에서 타겟단말기의 비면허 대역 신호를 활성화하는 것은 두 가지의 다른 방법이 가능하다. 하나의 방법은 타겟단말기의 사용자가 구조요청을 하여 활성화하는 것이 가능하다. 이 방법은 신변보호대상자 등이 구조요청을 하는 상황 등에서 유용하게 사용될 수 있다. 또 다른 방법은 구조대원이 실종자의 탐색 등을 위해 외부에서 활성화 하는 것이 가능하다. 이 방법은 치매환자의 실종과 같은 상황 등에서 유용하게 사용될 수 있다.

타겟단말기의 비면허 대역의 신호가 활성화 되면 구조대원이 타겟단말기의 대략적인 위치에 신호측정기를 소지하고 타겟단말기에 대한 탐색을 수행한다. 신호측정기는 여러 가지 형태로 구현이 가능하다. 한 가지 가능한 구현 방법으로 구조대원이 평소에 사용하는 스마트폰에 앱 프로그램을 설치하는 형태로 구현하는 것이다. 구조대원이 평소에 사용하는 스마트폰을 활용하므로 낮은 비용으로 비면허대역 정밀측위 기술을 보급할 수 있다. 또 다른 방법으로 고성능 전용 신호측정기를 개발하는 것이다. 전용 신호측정기는 스마트폰에 앱 프로그램을 설치하여 사용하는 방법과 비교하여 3배 이상의 먼 거리에서도 타겟단말기의 신호를 검출하고 정확한 위치파악을 할 수 있다는 장점이 있다.

Ⅲ 비면허 대역 신호기반 정밀측위 실험결과

비면허대역 신호를 사용하여 타겟단말기의 위치를 파악하는 실험을 다양한 환경에서 수행하였다. <그림 3>에 타겟단말기를 5층 건물의 한 위치에 놓고, 신호측정기를 사용하여 그 위치를 파악한 결과의 한 예시를 도시한다. <그림 2>의 실험에는 타겟단말기로 스마트워치를 사용하였다. 스마트워치가 블루투스 신호를 측위를 위해 송신하고, 신호측정기는 이 블루투스 신호를 측정하여 스마트워치의 위치를 파악하였다.



<그림 2> 비면허대역 신호 기반 타겟단말기의 건물내 위치 탐색 실험결과

<그림 2>의 결과는 신호측정기를 소지한 구조대원들이 각 층별로 탐색하여 타겟단말기가 전송하는 신호의 세기를 등고선의 형태로 건물의 도면위에 표시한 것이다. <그림 2>의 결과는 3층에 빨간색의 작은 별의 위치에 타겟단말기(스마트워치)를 놓고 실험하였고, 측정한 신호의 세기의 최대값이 되는 위치에 빨간색 원을 표시하였다. <그림 2>의 결과에서 3층의 타겟단말기 근처에서 가장 강한 신호가 검출되었음을 살펴볼 수 있다. 그리고 타겟단말기가 위치한 층에서 한 층 위/아래에서도 타겟단말기의 신호가 어느 정도 검출이 가능하지만, 그 신호의 세기가 크게 감소함을 살펴볼 수 있다.

타겟단말기가 전송하는 비면허 대역 신호를 신호측정기로 측정하여 10m 이내의 오차로 타겟단말기의 위치를 파악할 수 있음을 확인하였다. 또한, 다양한 건물들에 대한 탐색 실험에서 타겟단말기가 위치한 층을 찾아낼 수 있음을 확인할 수 있었다.

Ⅳ 결론

범죄, 재난, 실종 등 다양한 긴급구조 상황에서 골든타임이내에 구조대상자의 정확한 위치를 파악하는 것은 매우 중요한 일이다. 현재의 기술로 구조대상자의 위치를 정확히 파악하는 것은 한계가 있다. 그러나 위치측정의 대상이 되는 타겟단말기가 블루투스 또는 Wi-Fi와 같은 비면허 대역신호를 전송하게 하고, 구조대원이 신호측정기로 이 신호를 측정해 타겟단말기의 위치를 10m 이내의 오차로 파악할 수 있다. 특히, 비면허대역의 신호를 활용하는 것은 이동통신 사업자의 협조 없이도 간단한 앱 소프트웨어를 설치하여 빠른 시간에 실용화가 가능하다. 추가적으로 국내외 표준화를 통해 이 기능을 스마트폰 또는 스마트워치 등의 기본 앱 또는 OS (Operating System)에 탑재하는 것을 추진한다면 긴급구조 상황 뿐 아니라 분실한 휴대폰 찾기 등의 다양한 위치기반 서비스에 활용하는 것이 가능하다.

또한, 이동통신 사업자의 협조를 통해 타겟단말기가 전송하는 LTE 등의 이동통신 신호에 대한 측정을 추가적으로 결합하여 타겟단말기의 위치를 파악한다면, 긴급구조 상황에서 위치파악이 어려워 안타까운 사고가 발생하는 것을 해소할 수 있을 것으로 전망한다. PSI

참고 문헌

[1] S. Razavi, F. Gunnarsson, H. Rydén, A. Busin, X. Lin, X. Zhang, S. Dwivedi, I. Siomina, and R. Shreevastav, "Positioning in cellular networks: Past, present, future," in Proc. IEEE Wireless Commun. Networking Conf. WCNC, 2018, pp. 1-6.

[2] D. Corral-De-Witt, E. V. Carrera, J. A. Matamoros-Vargas, S. Munoz-Romero, J. L. Rojo-Álvarez, and K. Tepe, "From E-911 to NG-911: Overview and challenges in Ecuador," IEEE Access, vol. 6, pp. 42578-42591, 2018.

[3] Z. M. Kassas, J. Khalife, K. Shamaei, and J. Morales, "I hear, therefore I know where I am: Compensating for GNSS limitations with cellular signals," IEEE Signal Process. Mag., vol. 34, no. 5, pp. 111-124, 2017.

[4] M. Porretta, P. Nepa, G. Manara, and F. Giannetti, "Location, location, location," IEEE Veh. Technol. Mag., vol. 3, no. 2, pp. 20-29, 2008.

[5] Federal Commmunication Commission, Sixth report and order on reconsideration, FCC 20-98, July 17, 2020.

[6] H. Moon, "Position measurement system for mobile terminal," US patent 11,445,331, Sep. 13, 2022.

[7] 문희찬, 박효순, 무선통신을 이용한 단말기의 위치측정 장치 및 방법, 특허출원 1020220096368, 2022.

■ 이 논문(글)은 2019년도 정부(경찰청)의 재원으로 지원받아 수행된 연구결과임[과제명: LTE 신호기반 요구조자 정밀측위 기술개발 / 연구개발과제번호: 2019001291].

치안과학원 설립의 의의와 운영 전략

한국행정연구원 선임연구위원 조세현

Ⅰ 들어가며

신기술이 급속하게 발전하는 만큼 이를 악용한 범죄는 그 수법 또한 빠르게 진화하고 있다. 디지털 기술을 활용한 보이스 피싱, 디지털 성범죄, 사이버 폭력 등은 온오프라인을 넘나들며 국민에게 막대한 피해를 입히고 있다. 그 외에도 마약, 총기 등 위험 물질의 디지털 제조, 자율주행차를 해킹한 교통사고, 블록체인을 이용한 범죄수익 은닉 등 기술 기반 미래 신종 범죄 위험이 예상되고 있다.

한편 살인, 강도, 강간, 절도, 폭력 등 체감 치안에 영향이 큰 범죄가 감소('20년 39만 건 → '21년 34만 건/13.3%)하였음에도 불구하고 국민들의 체감안전도는 하락('20년 77.7% → '21년 76.5%)하였다. 또한 OECD '정부기관 신뢰도 조사(Trust in Public Institutions)'에서 우리나라 국민들의 경찰에 대한 신뢰도는 OECD 평균인 72%보다 상당히 낮은 57%에 불과하다(OECD, 2021). 범죄의 감소에도 불구하고 국민들의 체감 치안이 감소하는 것은 다양한 원인이 있겠지만 경찰의 현장 대응 미흡이나 범죄 피해자에 대한 신변보호의 불충분성 등으로 국민의 생명과 신체를 안전하게 보호하지 못한 사건들이 다수 발생했기 때문일 것이다.

과학치안은 이러한 환경변화에 경찰이 적극적으로 대응하기 위한 중요한 전략이다. 기존의 노동집약형 경찰활동 수행을 위한 인력확대로는 이러한 환경 변화에 효과적으로 대처할 수 없고 과학적·공학적 방식, 기술, 장비를 범죄예방, 현장 대응, 수사 과정에 활용함으로써 경찰의 역량을 증강시킬 필요가 있다. 이를 통해 더욱 적극적이고 선제적으로 국민을 범죄로부터 보호할 수 있다.

Ⅱ 치안과학원 설립 방안

1. 왜 정부기관이어야 하는가

치안과학원의 설립은 과학기술을 활용한 선제적 경찰활동과 경찰 역량의 증강 기반을 마련할 수 있는 정책 수단 가운데 하나이다. 민간에서 AI, 로봇, 자율주행, 3D 등 다양한 기술 개발이 이루어지고 있음에도 불구하고 정부에서 과학치안 기반 마련을 위한 기능을 수행해야 하는 이유는 과학기술 적용 대상이 갖는 보안성 및 과학기술의 현장적용성 때문이다. 예를 들어 AI 기술을 활용한 선제적 범죄·위험 예측과 근거기반의 정책 수립을 위해서는 데이터 확보 없이는 불가능하다. 인터넷 공간의 공개된 데이터로 학습한 AI는 실제 사건에서 유용하게 적용되기 어렵다. 따라서 수사 데이터, 112 신고데이터, 과학수사 데이터 등 외부로 반출하기 어려운 실제 데이터를 활용하여 분석해야 한다. 형사사법기관 중 가장 많은 데이터를 보유하고 있으며 선제적 경찰활동을 위해 가장 다양한 방법으로 데이터를 관리하고 처리할 수 있는 기관은 경찰이고, 민감한 데이터이므로 경찰 내부의 전문성을 가진 조직이 전문성을 갖추고 분석하여야 하는 것이다.

AI 기술개발은 민간이나 국가출연연구기관에서도 수행하고 있으나 모델을 실제로 활용하고 성능평가 등 효과성 수준의 관리는 경찰청 내부 조직에서 실시할 필요가 있다. 또한 치안 분야 현장 전문지식을 가진 경찰청 내부 전문기관이 치안 데이터의 특성과 구조에 대한 이해를 바탕으로 인프라를 운영할 필요가 있다. 민간 군수기업이 무기개발을 하고 국방과학연구소가 군사기밀 등을 다루면서 국방부와 민간의 중간 역할을 수행하고, 각 부대에서 신형 무기를 실제 시험 운영 시 연구를 수행하는 것과 동일한 논리이다.

경찰의 현장대응력을 높이기 위한 다양한 기술과 장비의 활용에 있어서도 정부의 기능 수행이 요구된다. 경찰의 현장대응력을 높임으로써 국민의 신체와 생명을 보호를 하기 위해서는 현장 중심형 모사 실험이 가능한 교육 장비와 시설이 필요하다. 예를 들어 자율주행 로봇에 마네킹을 설치하고 자율주행로봇이 AI를 활용해 범죄자의 도주 패턴을 학습할 수 있는 기술을 개발하여 무빙타겟을 대상으로 한 현장 훈련이 가능하다고 가정해 보자. 이 경우에도 실제 범죄자 도주 데이터의 활용을 통한 성능향상은 경찰조직 내부의 전문기관이 수행해야 하는 것이다.

한편 과학치안의 영역에 대한 법·제도적 근거 또한 정부가 수행해야 할 분야이다. 최근 서현역 사건, 신림동 흉기난동 사건과 같이 다양화·흉폭화되는 범죄 현장에서 효과적 대응을 위한 경찰장비 제공이 필요한 상황인데, 이를 위해서는 성능검사, 안전성 검사, 위험도 연구 및 표준화가 필요하다. 경찰의 현장대응력을 높이는 동시에 국민에게 위해를 끼치지 않아야 하는 기준의 마련은 민간이 아닌 정부가 수행해야 하는 역할이다. 이러한 기준 마련을 위한 전문성을 정부가 갖고 있지 못하다면 정부는 장비를 구매할 시에도 민간 납품업체가 제출하는 성적서에 의존할 수 밖에 없다. 따라서 국가 기관이 직접 성능기준 마련 및 운용성 차원에서 실증·검증을 정기적으로 수행하여 경찰활동의 안전성과 효과성, 나아가 국민안전을 담보할 필요가 있다. 기준 마련, 표준화, 성능평가 등은 공학적 전문성이 요구되는 바, 정부기관으로서의 정체성을 가진 연구기관이 그 기능을 수행해야 한다.

2. 치안과학원의 미션, 비전, 전략

치안과학원은 현재 경찰청 2차 소속기관인 치안정책연구소의 기능을 확대, 개편하여 독자적 치안연구 기능을 강화하는 방식으로 설립할 필요가 있다. 현재의 치안정책연구소는 경찰대학 부설기관이지만 주요 기능은 경찰대학의 수요에 맞춰 수행하는 것이 아니라 경찰청의 수요에 부응하여 정책연구와 과학기술연구를 수행하고 있다. 그러나 경찰대학의 부설기관인 조직 편제의 특성상 인력과 예산의 확보 과정에서 우선순위에 밀림에 따라 미래 치안정책환경에 선제적으로 대응하는 연구주제 발굴이나 경찰 현장에서의 연구 수요에 민첩하게 부응하기 어렵다. 또한 경찰관의 행정업무 투입에 따른 연구 지원 업무 전문성 및 효율성 저하, 승진체계가 없는 전문경력관 연구직의 직무동기 부여 및 우수인력 유치의 한계, 연구인력 규모 및 전공 분야 다양성 부족으로 인한 치안연구 수요 대응의 어려움, 임기제 공무원에 의한 업무 수행으로 연구 및 사업 연속성 저하와 같은 문제점이 있다.

다만 치안정책연구소는 정책연구기관으로 출발한 조직의 연혁에 의해 경찰청과의 유기적 관계 속에서 정책지원 기능 수행 역량 축적, 경찰 외부에서 수행하기 어려운 치안 정책·과학기술 연구를 수행할 수 있는 구조, 정책·과학기술 연구가 공존하는 조직이라는 강점이 있다. 따라서 정책과 과학기술 간 융합적 연구를 수행할 수 있는 강점을 십분 활용하여 치안과학원 조직을 설계하고 운영함으로써 치안환경 변화에 적극 대응할 수 있을 것이다.

현재의 치안정책연구소가 가진 단점을 보완하고 강점을 적극 활용하여 치안정책연구소를 경찰청 1차 소속기관 치안과학원으로 승격, 새로운 미션과 비전, 전략을 구축함으로써 경찰활동 패러다임의 전환을 선도할 필요가 있다. 정책과 과학기술 연구의 융합적 수행을 치안과학원의 정체성으로 확보하고 “과학치안과 치안정책의 최고 전문성으로 국민안전을 실현”하는 것을 치안과학원의 새로운 미션으로 채택하여야 할 것이다. 그리고 과학치안 기반의 선제적 경찰활동으로의 패러다임 전환을 강조하기 위하여 “첨단과학기술기반 치안과 선제적 경찰활동을 선도하는 전문연구기관”을 새로운 비전으로 선택할 수 있을 것이다.

치안과학원은 치안현장 지향, 치안 정책 지원, 과학치안 선도라는 세 가지 전략을 마련하여 기관 고유 및 핵심고객 중심의 연구를 수행할 필요가 있다. 첫째, 경찰의 현장대응역량을 제고하는데 실질적인 도움이 되는 치안 현장 지향 연구를 수행해야 한다. 특히 자치경찰제의 시행으로 지역 경찰의 다양한 치안서비스 개발, 여성·아동·청소년 등 범죄취약계층의 안전을 위한 실질적 대응책 마련을 지원하기 위한 연구 수요가 발생할 것으로 예측된다. 따라서 경찰 및 경찰청 뿐만 아니라 지역 주민과 지방자치단체까지 치안과학원의 주요 고객으로 확대하기 위한 거버넌스 구축 마련이 필요할 것이다.

둘째, 경찰조직 및 정책역량 강화를 지원하는 연구 수행으로 치안 정책을 지원해야 한다. 경찰청의 1차 소속기관이라는 강점을 가지고 다양한 데이터를 활용하여 근거기반 치안 정책 제언을 위한 연구를 수행하여야 할 것이다. 또한 새롭게 경찰조직에 진입하는 세대의 특성을 반영한 조직문화, 계급 중심의 경직된 경찰 조직의 애자일한 구조로의 변화, 디지털 기술을 활용한 경찰 직무 변화에 따른 조직 효율화 진단 등 기존 경찰 조직 패러다임으로는 대응할 수 없는 연구 수요를 적극 발굴하여 선제적 연구를 수행해야 할 것이다. 무엇보다도 정책연구와 과학연구가 공존하는 조직의 정체성에 기반, 과학기술의 경찰활동 현장 적용을 위한 법·제도 연구를 심도 있게 추진해야 한다. 완전자율주행차의 도로주행에 따른 도로교통법 개정이 대표적인 예이다.

셋째, 과학기술기반 치안을 선도해야 한다. AI

를 활용한 수사지원, 범죄예측, 현장 대응 과정에서 경찰과 국민을 함께 보호할 수 있는 과학기술 개발·도입을 위한 연구를 수행할 필요가 있다. 특히 범죄예측 및 대응과 관련하여 출시된 기술이 있을 경우 직접 개발하기 보다는 치안 현장 적용성을 평가하고 신속 도입을 지원하는 기능을 수행하여야 할 것이다. 이를 위해서는 최신의 기술 악용 범죄를 신속하게 분석하고 선제적으로 대응하기 위한 기술 동향 분석, 산·학·연 치안R&D 결과물의 경찰현장 실증 활성화를 위해 경찰청 담당국관 및 경찰관서와 연계역할을 해야 한다. 이와 같은 기능 수행을 바탕으로 신기술의 신속한 현장 확산뿐만 아니라 치안 산업생태계 조성의 기반이 되어 기술 사업화 지원, 특허 창출 지원 등 시장 파급력 성과까지 창출할 수 있을 것이다.

Ⅲ 나가며

치안환경 변화에 선제적·능동적으로 대응하기 위해서는 조직 설립만으로 충분하지 않다. 지금까지 제시한 전략을 활용하여 차별적이면서도 경찰현장에 실질적으로 도움이 되는 연구성과를 창출하기 위해서는 무엇보다도 치안과학원의 연구자들이 경찰청의 데이터를 활용할 수 있도록 시스템·데이터 연계의 법·제도적·기술적 기반 구축이 선행되어야 한다. 또한 현재의 전문임기제 인력, 경찰의 순환보직에 의한 연구 수행 체계를 벗어나 다양한 분야의 전문 연구 인력이 안정적으로 연구에 임하여 기관 미션 달성과 성과 창출에 지속적으로 기여할 수 있도록 해야 할 것이다. 마지막으로 기관이 승격될 경우 연구행정 선진화가 반드시 필요하다. 예산이 증가하면서 연구행정 부담이 가중될 것이므로, 연구역량을 가진 전문인력과 일반행정직이 연구 기획 및 전략을 기획 부서에서 수행함으로써 연구기획조정 역량을 강화할 수 있는 기반을 마련해야 할 것이다. PSI


치안정책연구소

치안정책연구소
POLICE SCIENCE INSTITUTE
[31539] 충청남도 아산시 신창면 황산길 100-50 경찰대학 치안정책연구소
스마트치안지능센터 T. 041.968.2397 https://www.psi.go.kr/

ISSN 2951-2727