법과 과학

2019년 6월호

과학수사의 중심

대검찰청 과학수사부

C O N T E N T S

한국-OSCE 사이버안보 컨퍼런스 참석

사이버수사과 수사관 서형호

2019년 5월 2일 대검찰청 과학수사부 사이버수사과 최승진, 서형호 수사관 2명은 서울시 중구 조선호텔에서 외교부 주관으로 열린 '제2차 한-OSCE 사이버안보 컨퍼런스'에 참석하였습니다.

이번 컨퍼런스는 첨단과학수사커뮤니티 '사이버안보법' 관련 의제를 발굴하고, 이와 관련하여 권위 있는 전문가와 인적네트워크를 형성하기 위함이었습니다.

OSCE는 Organization for Security and Cooperation in Europe의 약자로, 정치·군사 안보, 경제·환경안보, 인간안보를 종합적으로 고려하는 포괄안보 개념에 기초한 유럽-대서양 국가 간 안보협력기구로 우리나라는 1994년부터 OSCE 아시아협력동반자국 자격으로 참여했습니다.

2017년에 이어 두 번째로 열린 이번 회의에서 ▲지역 간 사이버안보 협력 ▲사이버공간에서의 국가행동 ▲주요기반시설 보호 ▲사이버안보 국제규범 마련 노력 등 다양한 주제를 논의하였습니다.

이중 개인적으로 인상 깊었던 주제는 조안나 브라이슨 교수의 'AI 머신러닝과 규제'와 조세핀 울프 교수의 '기술적 진보에 따른 사이버보안 전망'이었습니다.

조안나 교수는 '지능(Intelligence)이란 옳은 것을 **적당한 시기**에 하는 것'을 말하는데, '옳은 것'에는 '도덕적인' '윤리적인'이란 의미가 함축되어 있다고 설명하며, 인공지능 학습을 위한 머신러닝 시, 성차별적이거나 편견이 반영될 수 있어 주의가 필요하다고 하였습니다.

즉 인공지능을 학습시키기 위해 선별된 데이터들은 선별한 사람의 가치관이나 편견이 반영될 위험이 있고, 이는 편향된 인공지능을 만들 수 있다고 합니다.

인공지능은 사람의 작품이기에 사람에게 책임이 있으며, 인공지능의 작동에 대해 규제가 필요한 것이 아니라, 사람이 **인공지능 시스템을 만들고, 훈련하고, 모니터하는 과정에 적절한 규제**가 필요하다고 주장하였습니다.

조세핀 교수는 1983년 제작된 '워게임(WarGame)' 영화를 발표 첫머리에 언급하며, 인공지능으로 대체된 사회가 AI 오작동 및 해킹으로 큰 위험에 처할 수 있다고 경고하였습니다.

영화 워게임에서는, 미국의 핵발사 절차는 인공지능에 의해 자동적으로 진행되는데, 한 고등학생 해커가 우연히 개발자 PC에 침입한 후 게임으로 착각한 프로그램을 조작하며 핵발사가 시작됩니다.

자율주행자동차 시험 운행 중 보행자와 충돌한 인명사고, 시스템오작동으로 추락한 에티오피아 비행기 추락사고, 달리는 자율주행자동차를 원격 해킹하여 정지시키거나 경로를 변경시킨 사례를 언급하며 이제는 프로그램 오작동이나 해킹이 단순히 경제적 손실만이 아닌 현실세계에 인명사고를 일으킬 수 있기에 시스템 개발 및 보안에 신중을 기해야한다고 하였습니다.

이번 컨퍼런스 참석을 통해 사이버안보법 커뮤니티 의제 중 하나로 '기술진보에 따른 선진국 사이버보안법 동향파악'이 필요하다는 것을 알 수 있었고, 관련 전문가들과 사이버보안 관련 인적 네트워크를 형성하여 향후 관련 정보를 교환할 예정입니다.

제29회 KOBA(국제방송, 음향, 조명기기전시회) 참관

법과학분석과 연구사 정은혜

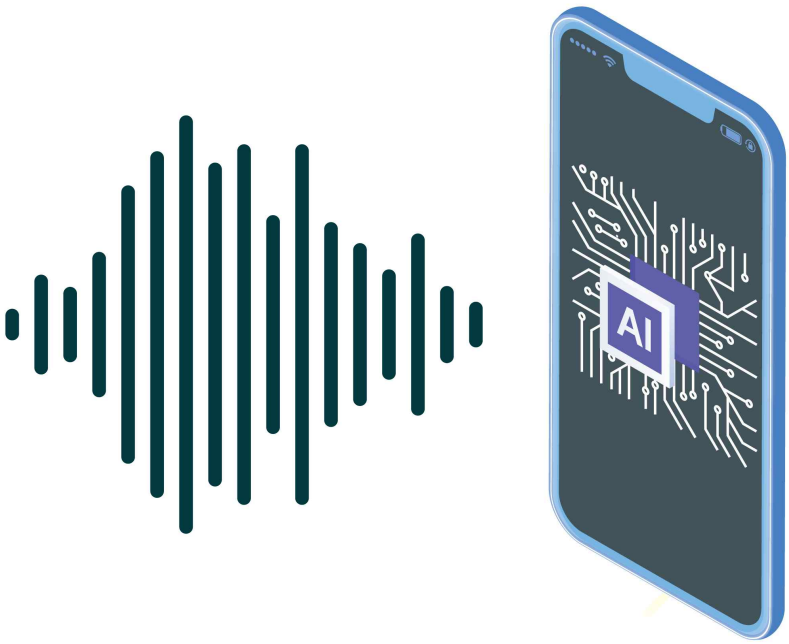
지난 5월 24일(금) 법과학분석과 멀티미디어분석실에서는 제29회 KOBA(국제 방송·음향·조명기기 전시회)에 다녀왔습니다. KOBA는 한국이앤엑스와 한국방송기술인연합회가 공동 주최하고 과학기술정통부, 산업통상자원부, 방송통신위원회 등 관련 기관 및 방송사의 후원으로 열리는 전시회로, 세계 각국의 우수한 방송, 영상, 음향, 조명 관련 장비들을 한 자리에 모아 전시 및 소개함으로 신규 멀티미디어 장비 및 기술 동향을 한 눈에 파악할 수 있는 좋은 기회의 장입니다.

저는 음성분석실에서 근무하는 감정관으로 음향 관련 장비들을 집중적으로 관람하였는데, 가장 눈에 띄었던 것은 방음 부스였습니다. 좋은 품질의 음성 자료를 녹음 및 분석하기 위해서는 방음 시설이 매우 중요한데, 벽체에 흡음 시설을 설치하는 것만으로도 방음 효과를 낼 수 있다는 것이 흥미로웠습니다. 또 방음부스에 직접 들어가 보니 전시회장의 소음이 확실히 차단되는 것을 직접 체험할 수 있었습니다. 추후에는 음성분석실 감정관 개개인이 주변 환경의 영향 없이 분석 업무를 할 수 있도록 개인용 방음부스가 설치되면 좋겠다는 생각도 들었습니다.

방음부스 뿐 아니라 녹음 시설 및 녹음을 모니터링 할 수 있는 콘솔, 오디오 인터페이스, 스피커 등도 대형부터 소형까지 여러 제품이 있었는데, 분석실에서 사용할 수 있는 제품이 어떤 제품일지, 각 제품을 머릿속에서 가상으로 음성분석실로 옮겨서 배치도를 그려보는 것도 즐거웠습니다. 그리고 감정관이 업무 시 항상 함께하는 친구 같은 존재인 헤드폰도 직접 착용해보지 않고는 본인에게 맞는지, 무겁거나 불편하지는 않은지, 음질은 어떤지를 알 수가 없기 때문에 다양한 제품들을 직접 써보고 청음해보는 시간을 가졌습니다. 그 중에 Audio Technica 사에서 나온 전문가용 헤드폰이 머리 지지대가 있어 착용감이 좋고 가볍고 편안해서 추후에 구매하리라 마음먹고 세부 스펙을 꼼꼼하게 확인하고 왔습니다. 또한 입사 전 대학원 시절부터 음성 실험의 용도로 주로 사용하던 휴대용 녹음 기기인 Marantz 및 Sound Device 등도 고품질 및 여러 채널로 녹음할 수 있도록 업그레이드된 제품이 출시된 것을 확인할 수 있었는데, 발전하는 기술 및 제품력을 시장 조사를 통해 직접 확인할 수 있어서 좋았습니다.

그 밖에 음성분석실 업무와 직접적인 관련이 있지는 않지만, AI 기술을 이용하여 음악을 재생하면 실시간으로 음악의 A, C, D코드 등을 화면에 띄워서 바로 바로 코드를 확인하면서 악기를 연주할 수 있는 앱이 출시되어 직접 체험하는 시간을 가졌습니다. 가수 故김광석 노래 기준 정확도가 90% 이상이라고 하였는데, 소리를 인식하고 음악의 코드를 실시간으로 출력할 수 있는 정도의 기술력이라면 빅데이터 학습을 통한 음성인식 및 화자인식 기술도 기존의 패턴 인식 방법을 사용하던 것에 비해 훨씬 정확도가 높아졌으리라 예상되었습니다. 또한 오디오 기술의 개발에 따라 디지털 녹음 파일도 거의 원음에 가깝게 구현하는 추세이므로, 음성의 동일인 여부 분석 시에 분석할 수 있는 음성 정보가 많아져서 이러한 흐름이 반갑기도 합니다. 다만 AI 기술이 화자 인증(Speaker Verification), 음성 변환(Voice Conversion) 등에 악용되어 하지도 않은 말을 한 것처럼 위조할 수 있는 가능성도 동시에 커지기 때문에 기술 개발 현황을 파악하고 이에 대한 대책을 선제적으로 마련하는 것이 필요하겠습니다.

당장의 분석 업무에만 정신을 쏟다 보면 자체 연구 및 멀티미디어 분야의 최신 기술 동향 파악에 소홀해지기가 쉬운데, 시간을 꼭 따로 내어 학회 및 전시회 등에 적극 참석하여 빠르게 변화하는 흐름을 놓치지 말아야겠다는 다짐을 하게 되는 시간이었습니다. 앞으로도 대검찰청 법과학분석과 멀티미디어분석실에서는 장비 및 기술 현황을 직접 확인하는 기회를 자주 가지고, 이를 업무에 적용하여 범죄 예방 및 실체적 진실 확인에 앞장설 수 있도록 하겠습니다.



IACIS BCFE 국외 훈련과정 참가

디지털수사과 수사관 이주연

지난 5월, 디지털포렌식 수사관 4명이 모여 약 2주간 미국 플로리다주 올랜도에서 함께 BCFE 교육 과정을 수료하고 돌아왔습니다. 이론과 실습이 병행되는 과정이라서 한 순간이라도 놓칠까 초집중 모드로 교육에 참여하였던 그 후기를 들려드릴까 합니다.

[교육장 외부 전경]

우선, IACIS(International Association of Computer Investigative Specialists)는 1989년 미국에서 설립된 비영리 기관으로 1991년부터 디지털포렌식 관련 공인 교육 및 자격 인증 과정을 운용해 왔습니다. 국제 교육·인증 기관으로서는 가장 널리 인정받고 있고, 전 세계에 걸쳐 약 70여개국 2천명이 넘는 멤버들이 글로벌 네트워크를 구축하며 디지털포렌식 분야에서 협력하고 있습니다.

저희는 그 중에서 IACIS의 CFCE(Certified Forensic Computer Examiner) 자격 인증을 받기 위해 BCFE(Basic Computer Forensic Examiner) 교육과정에 참가하였습니다. 미국 플로리다주 올랜도에 위치한 교육장에서 약 320명가량 되는 전세계 법집행기관 소속 수사관들과 함께 교육을 받았는데, 모두 열정적으로 참여하고 토론하는 것은 물론, 약 30명 가량 되는 분임 코치들의 도움으로 어려운 실습과정도 모두 무리 없이 해낼 수 있었습니다.

[교육장 내부 전경]

더 놀라웠던 것은 강사와 더불어 모든 코치(Coach)들이 현업에 있는 수사관들로서 이 과정에 자원해서 돕고 있었다는 것인데, 제 분임코치인 Michael은 예전에 본인도 이 자리에 있던 교육생이었고, 많은 도움을 받았다면서, 제게 조금이라도 도움이

되었다면 그걸로 만족한다고 하여 제가 남모르게 감동받았던 기억이 납니다.

교육 과정은 매일 08:00-17:00까지로, 컴퓨터 포렌식 수사관으로서 갖추어야 하는 컴퓨터 전반에 대한 기본 지식부터 부팅체계, 수체계, 디스크구조, 파일시스템(FAT, exFAT, NTFS), 윈도우 레지스트리, 아티팩트, 클라우드, 모바일 기기, IOT, 각종 분석기법 등 실무기법 전수에 이르기까지 총 35개 과정으로 진행되었습니다.

그 중에서 특히 안티 드론(Anti-Drone), 각종 사물인터넷(IOT) 기기 분석에 관한 내용은 포렌식팀에서 근무하는 저희로서도 새롭고 관심이 가는 주제였습니다. 우리에게 재미와 편리함을 가져다주는 이 작은 기기들의 등장이 법집행기관의 수사관으로서는 그리 달갑지만은 않을텐데요. 전세계적으로 무인항공기(Drone) 시장의 규모가 커지고, 사용자가 급격히 늘어남에 따라 그와 연관된 문제들이 많이 발생하고 있는데, 특히 2015년에는 상업용 드론이 미국 백악관 건물에 충돌한 뒤 추락한 적이 있고, 일본 도쿄에서는 방사성 물질이 담긴 드론이 아베 총리 관저 옥상에서 발견되기도 했습니다. 또한, 일부 세력에 의해 테러리즘에 악용되거나, 몰래카메라로 악용되어 민간인에게 피해를 입히기도 하니 디지털포렌식 수사관으로서는 확실히 관심을 가질 만한 주제라는 생각이 들었습니다.

애플워치나 갤럭시기어 같은 스마트워치, 피트니스 밴드, 스마트 스피커 등 사물인터넷(IOT) 기기의 등장도 마찬가지인데, 이미 미국에서는 살인사건의 피해자가 차고 있던 스마트워치의 데이터를 복구하여 심박수가 갑자기 높아진 시점을 범행시간으로 특정해 범인을 검거한 사례 등이 있었습니다.

하지만 그들 역시 문제의식은 있으나, 실제 수사관들이 이러한 기기들을 압수하여 분석하는 데에는 어려움이 많다는 점을 토로하였습니다. 저 역시 그에 공감을 하였고, 또한 우리도 이에 대응할 수 있도록 실용성 있는 연구를 계속하여, 그 결과 체계를 정립할 필요성이 있다고 생각하였습니다.

저희 출장자 전원은 약 2주, 총 76시간의 교육과정을 마치고, 각자의 위치로 돌아와 CFCE 자격인증 시험을 치르고 있습니다. 2019. 6.월부터 2020. 4월까지 약 10개월간 진행되는 시험으로 Peer Review Phase와 Certification Phase로 구성된 6개 단계의 시험 모두를 통과하면 CFCE 자격을 얻게 됩니다.

현재, 검찰의 디지털포렌식 수사관들은 CFCE 자격 뿐만 아니라, IACIS에서 인증하는 다양한 국제 자격을 보유하고 있습니다. 저 역시 앞으로의 10개월간 끝까지 최선을 다할 것이며, 나아가 검찰 내부에서 그 역량을 발휘할 수 있도록 꾸준히 노력하겠습니다.

ISCR(국제사이버범죄대응 심포지엄) 참석

사이버수사과 수사관 김은숙

'19. 5. 22.(수)부터 5. 24.(금)까지 3일간 동대문 JW메리어트 호텔 서울에서 '2019 국제 사이버범죄대응 심포지엄(ISCR : International Symposium on Cybercrime Response)이 개최되었습니다. 위 심포지엄은 경찰청 주관으로 매년 개최되는 사이버범죄대응 관련 법집행기관 국제회의입니다. 특히 올해는 20주년을 맞이하여 각국 법집행기관, 국제기구 및 글로벌 IT기업의 사이버 전문가들이 대거 참여한 자리였습니다. 3일 동안의 내용 중 첫째, 둘째 날에 진행된 세션별 주요 내용을 소개 해 보고자 합니다.

< 최신 사이버위협의 글로벌 현황 >

첫째 날은 공개 세션으로 **갠드크랩(Gandcrab) 랜섬웨어 위협(금융보안원)**에 대한 주제 발표가 있었습니다. 주요 내용은 도메인등록 이메일 및 메일전송에이전트(MTA : Message Transfer Agent)를 기반으로 국내 활동 중인 Gandcrab 랜섬웨어 유포그룹을 세 개로 프로파일링하여 이들의 연관관계를 소개하는 내용이었습니다.

갠드크랩 유포그룹은 다음과 같이 분류될 수 있습니다.

- **SPIDERCRAB(스파이더크랩) 유포그룹**은 유포이메일에 사용된 도메인들의 등록자 이메일 주소가 **mshuherk@gmail.com** 으로 동일하며 개설한 도메인들은 금융피싱사이트 개설에도 활용되는 등 주로 이메일을 통해 유포하는 제일 큰 조직입니다. **SmartSerialMail을 메일에이전트로** 사용합니다.
- **PEACRAB(피크랩) 유포그룹**은 이메일을 통해서 2019. 2.부터 활동한 유포조직입니다. 초반에는 미흡한 한글이메일을 유포에 사용하였으나 이후 한글문법이 자연스러워졌으며 헌법재판소 및 경찰서 등을 사칭하고 **PowerMTA를 메일에이전트**로 사용합니다.
- **SPRINGCRAB(스프링크랩) 유포그룹은** 악성 JS 파일을 정상파일로 위장하여 주로 웹사이트를 통해 유포합니다. 이메일헤더, 메일클라이언트, C&C 인프라구조(명령제어 서버, Command & Control) 등을 분석하여 공격에 대응 가능합니다.

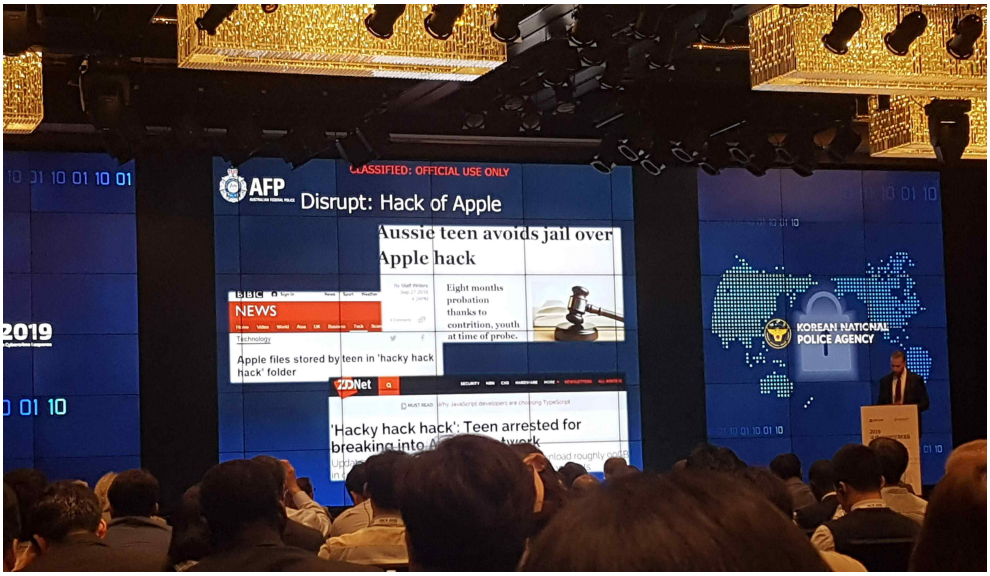
이어서 **가상화폐 범죄동향(체인알리시스-Chainalysis)**에 대한 내용으로 거래소 해킹 및 다크넷 마켓활동 등 이전년도 가상화폐의 범죄관련 통계와 2019 전망에 대한 발표였습니다. 2018년의 암호화폐 범죄사건 중 63%가 거래소해킹, 35%가 다크넷 마켓활동, 2%가 이더리움 사기범죄가 차지하고 있으며, 이 중 거래소해킹 사건이 가장 큰 문제입니다. 2011년부터 72건의 해킹사고가 발생하였고, 현재까지 총 19억달러가 탈취되고 가장 큰 해킹사건은 2018년 5억달러 피해가 발생한 coincheck 거래소 사건입니다.

다크넷 마켓은 다크넷에서 운영되고 암호화폐를 사용한다는 특징 외 인터페이스 및 벤더의 존재 등에서 일반 인터넷쇼핑몰과 유사한 형태를 띠고 있고 2017년 거래량은 약 7억 달러입니다. 그리고 피싱 등 이더리움 사기사건은 2018년 전년도에 비해 2배로 증가되었고 통계상 추이를 살펴보면, 사건의 수는 줄고 피해금액은 늘어나는 복합적인 형태로 진화되고 있다는 것입니다. 따라서 2019년 다크넷 마켓은 더욱 진화할 것이고, WhatsApp이나 Telegram 등 암호화된 메신저를 통한 은밀한 거래가 증가, 암호화폐 채굴 및 온라인도박 등 범죄유형은 더욱 다양화할 것으로 전망하고 있습니다.

그리고 **독일 BKA의 사이버 조직 혁신**이란 주제로 **독일 연방범죄수사경찰청(BKA)**에 대한 대한 소개 발표가 있었습니다. 현재 사이버범죄는 연방범죄수사경찰청 소속 9개의 과 중 중대 조직범죄과(SO)에서 수사하고 있으며, 아동음란물 관련 수사도 사이버범죄과에서 담당하고 있는데, 사건 발생 후 1시간 내 대응하고자 하지만 인력부족으로 어려움이 있다는 내용

입니다.

또한 4차혁명 관련 3개 부서(테러, IT, 사이버범죄)가 신설될 경우 BKA 산하 조직은 기존 9개에서 12개로 확대될 예정이며, 사이버범죄 수사의 중요성을 인지해 조직 개편 시 '사이버수사과'를 '사이버수사국'으로 승격시키고자 추진 중에 있습니다.

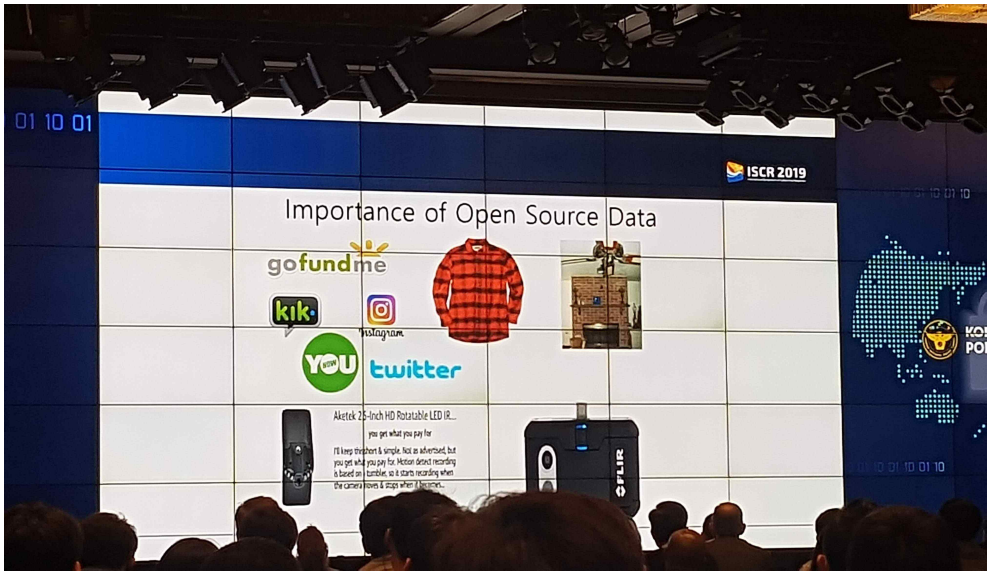


< 10대 소년의 애플 해킹 수사사례 >

둘 째 날은 비공개 세션으로 **AFP(Australian Federal Police, 호주연방경찰청)의 사이버범죄 대응전략과 가상통화, 다크넷 범죄에 대한 수사사례** 주제발표가 있었습니다. 업무용이메일보안 및 랜섬웨어를 주요 사이버범죄로 지목하며 10대 소년의 애플 해킹수사 및 국제협력을 통한 수사사례가 소개되었고 범죄의 규모, 데이터의 규모, 관할권 문제로 국가 간 협업의 중요성이 커지고 있다는 내용과 더불어 호주 정부의 사이버범죄 관련 우선순위가 소개 되었습니다. 그 우선순위는 개인 식별 정보, 기업이메일, 지적재산권, 민감 정보 도용, 현금출금서비스, 악성 프로그램, 랜섬웨어, 모바일 기기 정보탈취, 서비스 거부 공격, 사이버 판매사기입니다.

그리고 **가상통화 추적 수사기법 및 사례(미국 국세청)**를 통해 압수한 서버 등 데이터를 기반으로 수사를 확대한 경우가 소개되었습니다. 그리고 2017. 8. 아동포르노사이트 압수 및 사용자 수사사례(국내경찰과 협업한 경우), 압수된 암호화폐거래소 서버에서 마약사이트 클러스터와의 비트코인 거래를 추적하여 수사단서를 확보한 다크넷 마약공급책 수사사례, 그

외 압수영장을 통한 은행, 거래소, 이메일 및 오픈소스리서치(Open Source Research : 실수로 본인 실명 사용 등) 검색이용, Chat 로그, 인터넷 상 사용자 별명, 실명 계좌 정보를 통한 단서 확보 수사사례 발표도 있었습니다.



< 오픈소스리서치의 중요성에 대한 발표 화면 >

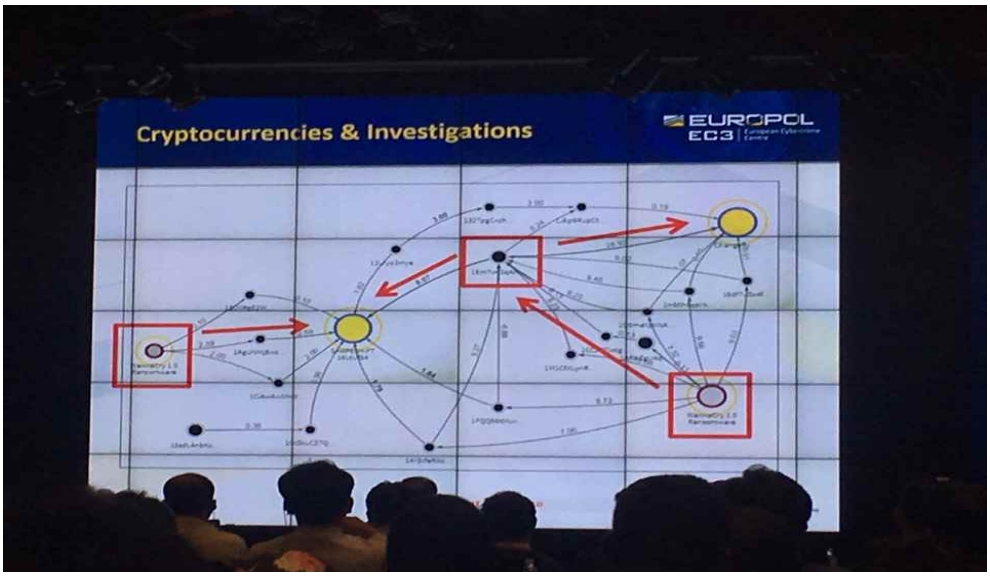
다크넷 수사기법 및 가상통화 자금 세탁(네덜란드 재정정보수사국) 주제발표가 있었는데, 다크넷을 이용한 범죄는 그 거래수단을 가상화폐로 이용하고 있습니다. 그 가상화폐는 현금 교환 또는 물품구매 할 때가 단서 확보 가능성이 높으며 그 수단으로는 거래소, 비트코인 ATM, 비트코인 카드결제를 들 수 있습니다.

< 비트코인 ATM 포렌식 소개 >

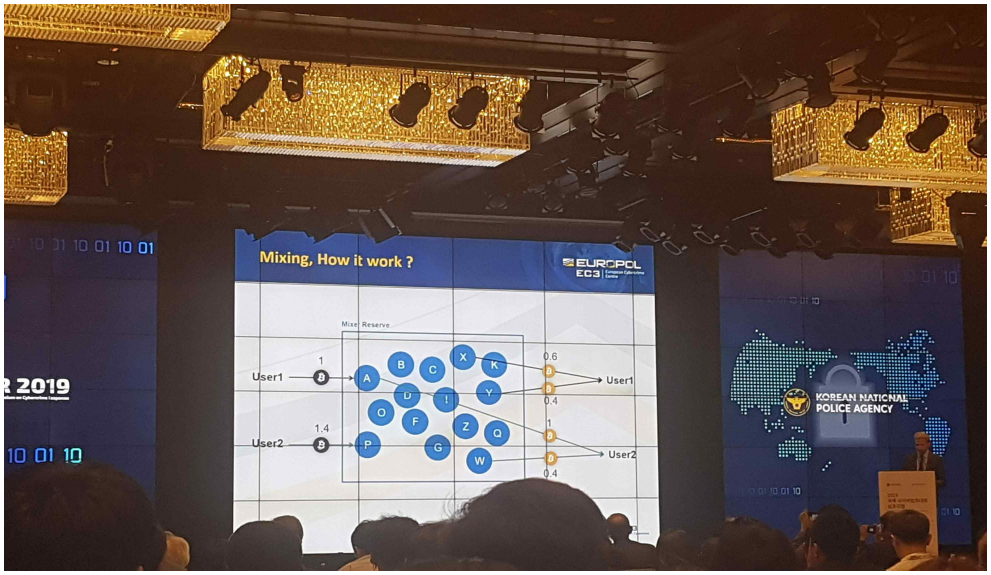
또한 비트코인 거래소 압수수색 및 ATM 포렌식으로 피의자를 특정하고 있는데, 비트코인 ATM 기기를 통한 마약 구매·자금세탁 흐름분석, ATM 트랜잭션(거래) 횟수 분석, 블록체인 분석을 통한 특정입니다. 특히, 블록체인 분석이란 분석자가 트랜잭션 거래(Undercover transaction)를 일으키는, 즉, 일회용 주소 사용을 통한 클러스터링 기법 분석을 말합니다.

암호화폐 거래는 주로 분산 플랫폼이 지원되며, 모네로처럼 익명성이 강한 암호화폐가 로컬 플랫폼 사용시 범죄 의심 가능성이 높습니다. 그 거래 흐름을 분석하는 소프트웨어 툴로는 PPM Advanced 툴이 있습니다. 또한 발표 당일 전날 이뤄진 Bestmixer.io 비트코인 믹싱 서비스 압수사례에 의하면, 믹싱 후 거래 DB를 확보한 것으로 Digital Intrusion Team을 이용하여 비트코인 믹싱서비스를 압수한 경우입니다. 이것은 웹사이트를 합법적으로 해킹한 후 사이트 폐쇄조치를 한 사례입니다. Digital Intrusion Team은 전문 화이트 해커팀으로 올해 3월부터 네덜란드가 전문 해커를 합법화한 이후 시행한 사이트 압수입니다.

그리고 **유럽 법집행기관의 블록체인·가상통화 관련 수사경험을 공유(유로폴 EC3)**한 자리가 있었습니다. 범죄에 사용되는 암호화폐 비율은 80% 비트코인, 17% 이더리움이며, 오래된 암호화폐 세탁 기법으로는 거래소, 갬블링(카지노 도박), 믹서이고 새로운 기법들로는 Unspent 주소, 스와핑, ICO, Prepaid 카드 등이 있다는 내용이었습니다.



< 블록체인·가상통화 관련 수사기법 >



< 비트코인 믹싱기법 화면 >

금번 사이버범죄 관련 법집행기관 심포지엄은 협력을 통한 사이버공간의 안전 확보를 위한 정보 공유의 장이었습니다. 이번 심포지엄 참석을 통해 각국의 사이버범죄 관련 수사기법과 최신 사이버위협 트렌드 그리고 그 대응전략과 각국의 대응 법제 및 정책, 가상통화와 다크넷 및 해킹·랜섬웨어 등에 대해 알아보는 좋은 기회가 되었습니다.

FBI/국가사이버포렌식훈련 사이버범죄 훈련 참석

사이버수사과 수사관 이인기

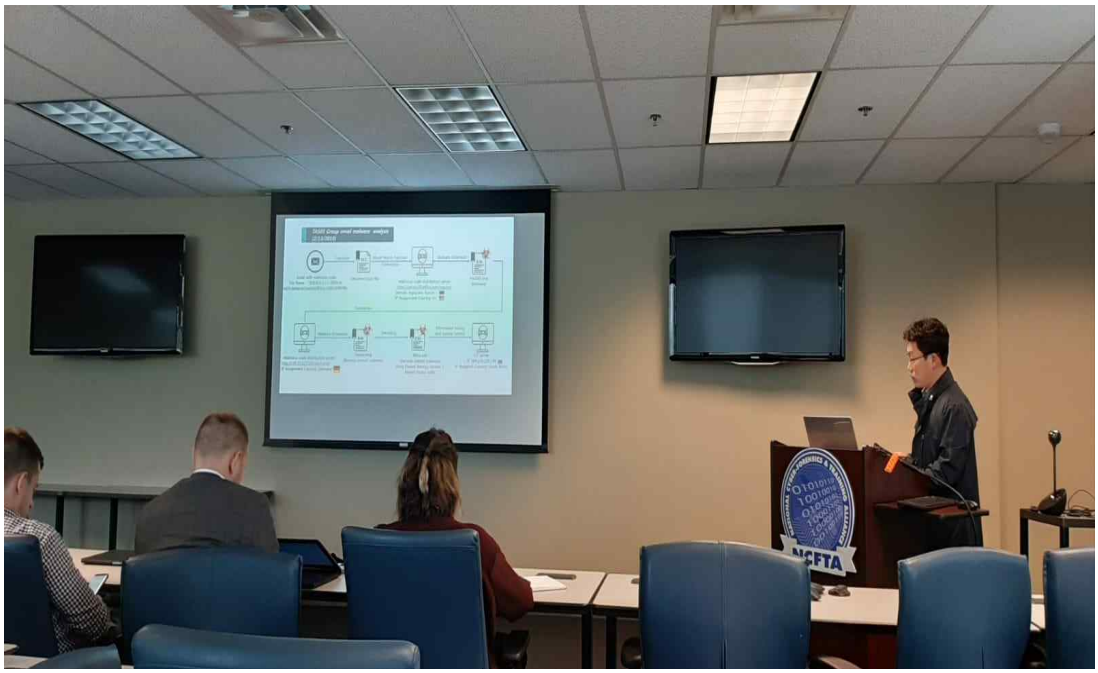
2019년 4월 28일부터 6월 8일까지 약 42일간 미국 피츠버그 소재 NCFTA(National Cyber-Forensics and Training Alliance)에서 주관하는 ITF(International Task Force) 훈련에 참가하였습니다.

NCFTA란 사이버위협에 대한 공동대응을 목적으로 2002년 설립된 비영리 조직으로 글로벌 사이버위협에 대응하기 위해 설립되었으며, 다양한 프로그램 운영을 통해 기업, 법집행기관, 해당 분야 전문가 그룹을 통해 수집된 정보를 관리하여 사이버공격 배후를 밝히고 법집행기관의 수사가 이루어질 수 있도록 지원을 하고 있습니다.

2019년 NCFTA에는 각국의 사이버수사를 담당하는 수사관 및 유로폴 등 총 22개국 24명의 수사관이 참석하여 각국의 사이버 수사현황 및 다양한 국가와 인적 네트워크를 형성할 수 있는 귀중한 시간을 가졌습니다.

< NCFTA 참가자 및 관계자 단체 사진 >

훈련에 참가한 수사관들은 각국의 사이버수사 현황 및 사례 발표를 통해 각국이 겪고 있는 중요 사이버범죄 현황에 대해 공감대를 형성하는 시간을 가졌으며, 특히 진행 중인 사이버범죄 사건에 대해 관련 국가의 협조를 현장에서 얻을 수 있어 사이버범죄에 있어 국제간 협력이 얼마나 중요한 것인지를 현장에서 체험할 수 있었습니다.



< 각국 사이버수사 사례 발표 사진 >

2019년 NCFTA-ITF의 중요 사이버범죄 수사활동은 BEC(Business Email Compromise), Phishing Kits, Operation Maelstorm에 초점을 맞춰 이루어졌습니다.

먼저, BEC 사이버범죄는 기업와 개인의 송금을 타킷으로 하며 범죄자는 불법적인 계좌 이체를 위해 소셜 엔지니어링 기술 또는 컴퓨터 침입 기술을 사용하여 피해자의 이메일 등의 접속 계정 정보를 탈취합니다.

IC3(Internet Crime Complaint Center) 보고에 따르면 BEC사기 사건은 150개국 이상에서 피해가 보고되고 있으며 편취된 금액은 115개국의 나라로 보내지고 있으며, 2013년 10월부터 2018년 5월까지 BEC사기 사건은 78,617건이 발생해 피해 금액은 125억 달러에 달한다고 합니다.

BEC사기와 관련 미국의 GOTU(Golbal Operation Targeting Unit)와 CIRFU(Cyber Initiative & Resource Fusion Unit)에서는 미국과 타 국가의 법집행을 통해 확보된 BEC 범죄자의 정보 등을 수집해 효과적인 BEC 범죄조직을 수사할 수 있도록 사용하고 있으며,

훈련 과정 중 각국 참가자들은 BEC 범죄와 관련해 수집된 정보를 검색할 수 있도록 별도의 접속서버를 마련해 주었습니다.

또한, Phishing Kits(피싱을 목적으로 사용되는 웹소스 등의 패키지 파일)과 관련해 NCFTA와 CIRFU는 대학 연구소 등 다양한 기관을 통해 전 세계 Phishing Kits 설치 정보를 수집하고 있으며 이렇게 수집된 정보를 바탕으로 Operation MaelStorm(사이버범죄 조직의 실체 증명, 연고지 파악, 범죄 예방 활동) 활동의 일환으로 각국의 참가자들은 나라별 확보된 Phishing Kits에 대한 수집내용을 바탕으로 함께 수사에 참여할 수 있는 경험을 하였습니다.

이번 교육을 통해 세계 각국에서 참여한 사이버전담 수사관과 상호협력을 위한 친목을 쌓는 중요한 시간을 가졌으며, 특히 사이버범죄에 있어 국제협력이 얼마나 중요한가를 현장에서 체험할 수 있는 뜻깊은 시간을 가질 수 있었습니다.

『알아두면 좋은 과학수사 상식』 ④

통신비밀보호법 관련 최근 헌법불합치 결정 살펴보기②

대검찰청 검찰연구관 김영미

저번 달에는 기지국 수사와 위치정보 추적자료에 대한 헌법불합치 결정에 대해 살펴보았습니다. 이번 달에는 패킷 감청에 대한 헌법불합치 결정에 대해 살펴보겠습니다. 2018. 8. 30. 헌법재판소는 통신비밀보호법 제5조 제2항 중 '**인터넷 회선을 통하여 송수신하는 전기통신**'에 관한 부분은 헌법에 합치되지 않고, 다만 2020. 3. 31.을 시한으로 개정될 때까지 계속 적용한다고 결정했습니다. 이른바 **패킷 감청에 대한 헌법불합치 결정**입니다.

> 제5조(범죄수사를 위한 통신제한조치의 허가요건)
> ② 통신제한조치는 제1항의 요건에 해당하는 자가 발송·수취하거나 송·수신하는 특정한 우편물이나 전기통신 또는 그 해당자가 일정한 기간에 걸쳐 발송·수취하거나 송·수신하는 우편물이나 전기통신을 대상으로 허가될 수 있다.

사안의 개요는 다음과 같습니다.

국가정보원은 A의 국가보안법위반 범죄수사를 위하여 A가 사용하는 휴대폰, 인터넷 회선 등 전기통신에 대해 법원으로부터 총 35차례 통신제한조치를 허가 받아 집행하였습니다.

이 중에는 **00연구소에서 B 명의로 가입된 주식회사 에스케이브로드밴드 인터넷 회선(서비스 번호 : 0000, ID :000)에 대하여 2013. 10. 9.부터 2015. 4. 28.까지 6차례에 걸쳐 행해진 통신제한 조치**가 포함되어 있는데, 이는 인터넷 통신망에서 정보 전송을 위해 쪼개어진 단위인 전기신호 형태의 패킷을 수사기관이 중간에 확보하여 그 내용을 지득하는 이른바 패킷감청이었습니다.

B는 인터넷 회선 감청을 목적으로 하는 통신제한조치에 대한 법원의 허가, 이에 따른 국가정보원장의 감청행위, 통신비밀보호법 제5조 제2항 등이 통신 및 사생활의 비밀과 자유 등을 침해한다고 2016. 3. 29. 헌법소원을 제기하였습니다.

헌법재판소는 인터넷 회선 감청의 특성을 고려하여 그 집행 단계나 집행 이후에 수사기관의

권한 남용을 통제하고 관련 기본권의 침해를 최소화하기 위한 제도적 조치가 제대로 마련되어 있지 않은 상태에서, 범죄수사 목적을 이유로 인터넷 회선 감청을 통신제한 조치 허가 대상 중 하나로 정하고 있어 **침해의 최소성 요건을 충족했다고 볼 수 없으며**, 이러한 여건 하의 패킷 감청은 개인의 통신 및 사생활의 비밀과 자유에 심각한 위협을 초래하므로 **법익의 균형성도 인정되지 않는다**고 하였습니다. 다만, **위헌성은 인터넷 회선 감청의 특성에도 불구하고 수사기관이 인터넷 회선 감청으로 취득하는 자료에 대해 사후적으로 감독, 통제할 수 있는 규정이 제대로 마련되어 있지 않다는 점**에 있으므로 법 개정 때까지 잠정 적용을 하도록 하였습니다.

패킷은 인터넷상 신속하고 효율적인 다량의 정보 전송을 위하여 일정한 단위로 쪼개어져 포장된 최적, 최소화한 데이터 단위입니다.

인터넷 회선 감청은 ISP가 허가 대상 인터넷 회선에 고정 IP를 부여하고, 해당 인터넷 회선에 흐르는 패킷을 중간에 수집, 복제한 후 재조합 절차를 거쳐 열람 가능한 형태도 전환됩니다.

그런데 전기통신사업자가 해당 인터넷 회선에 고정 IP를 부여한 다음 수사기관이 감청 집행을 한다 하더라도, 한 사람이 하나의 인터넷회선을 이용하는 경우는 거의 없고, 여러 사람이 하나의 인터넷회선을 공유하여 사용하는 경우가 대부분입니다. 공유기 등을 통하면 특정 인터넷 회선 이용자는 더욱 확대될 것입니다.

수사기관에 수집, 보관된 정보를 수사기관이 재조합 기술을 거쳐 직접 열람하기 전까지는 감청 대상자의 범죄관련 정보만을 구별해내는 것이 현재 기술적으로 가능하지 않습니다.

결국 **인터넷회선 감청은 법원이 허가하는 단계에서는 특정 피의자 내지 피내사자를 대상으로 하여 이들의 특정 인터넷 회선을 이용하여 송수신하는 전기통신 중 범죄 관련 정보로 감청 범위가 제한되어 허가가 이루어진다하더라도 실제 집행 단계에서는 감청 허가서에 기재된 피의자 내지 피내사자의 통신 자료 뿐만 아니라, 단순히 동일한 인터넷 회선을 이용할 뿐인 불특정 다수인의 통신자료까지 수사기관에 모두 수집, 저장된다는 문제점**이 있습니다.

미국은 전기통신비밀보호법(ECPA)에서 수사기관으로 하여금 법원이 요구하는 경우 주기적으로 감청 집행에 관한 경과보고서를 법원에 제출하도록 하고 있고, 감청 종료 직후 감청 자료를 감청을 허가한 판사에게 봉인, 제출하며, 감청자료의 보관 내지 파기

여부는 판사가 결정하도록 하고 있습니다. 또한 감청 종료 후 판사가 당사자에게 감청 집행 사실을 통지하고, 감청 집행 과정에서 수사기관의 위법이나 감청자료 공개 등으로 피해를 입은 당사자는 민사소송을 제기할 수 있습니다.

독일은 형사소송법에서 수사기관으로 하여금 법원에서 허가한 요건이 더 이상 존재하지 않을 경우 감청을 지체없이 종료하고 법원에 보고하도록 하고, 법원은 요건이 더 이상 존재하지 아니한 경우 처분의 중단을 명할 수 있습니다. 감청 종료 후에도 수사기관은 감청 결과를 법원에 보고하여야 하고, 감청집행결과 사적인 생활 형성의 핵심적 영역으로부터 인지한 사실임이 확인되면 그 사용이 금지되고, 해당 기록을 즉시 삭제하여야 합니다. 또한 감청 집행사실을 통지받은 당사자는 통지받은 때로부터 2주 내에 법원에 감청의 적법성 심사를 청구할 수 있습니다.

일본은 '범죄수사를 위한 통신방수에 관한 법률'에서 감청을 중단하거나 종료한 때에 입회인이 봉인한 기록매체를 영장을 발부한 법원에 제출하도록 하고, 허가 요건에 해당하지 않는 경우 법원이 해당 통신감청처분을 취소하고, 범죄와 무관하거나 감청에 위법이 있는 경우 기록을 삭제하도록 사후통제절차를 마련하고 있습니다. 또한 당사자는 자신이 어떠한 내용의 감청을 당했는지 확인하기 위하여 법원에 감청 기록 및 원기록 중 통신의 청취, 열람, 복사를 청구할 수 있고, 해당 통신감청에 관한 법원의 재판이나 수사기관의 처분에 대해 불복할 수 있습니다.

현재 법무부에서 국가정보원, 과기정통부, 대검찰청, 경찰청 등과 함께 TF를 구성하여 패킷 감청에 대한 사후 통제 방법에 대한 법률개정안을 마련하고 있습니다. 패킷감청이 어떻게 집행되며, 무엇이 문제인지에 대해 고민할 필요가 있습니다.

『세계의 법과학 기관』 ④

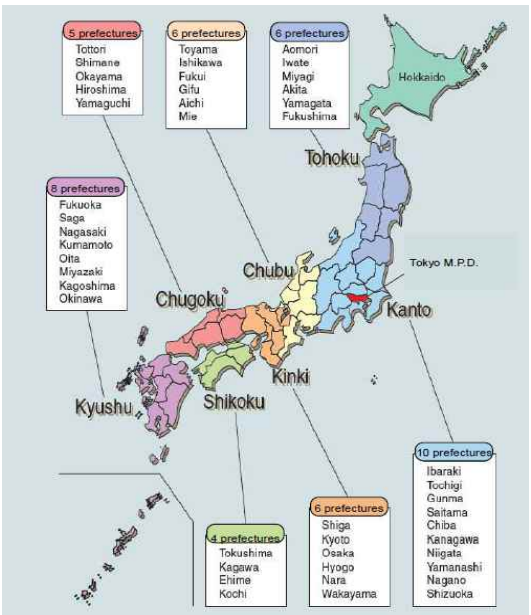
일본, 연구와 감정의 분리

법과학연구소장 이승환

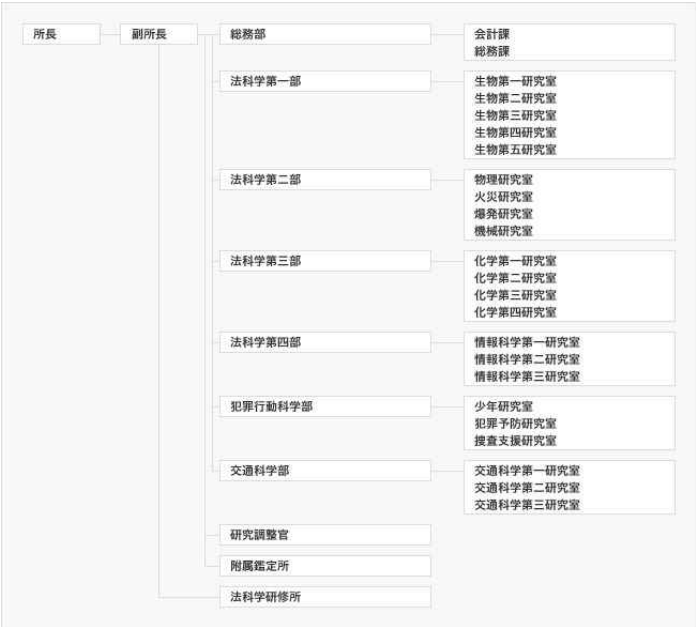
국가 기관의 종류나 기능이 우리나라와 많이 닮은 나라로 일본을 꼽지 않을 수 없습니다. 과학수사 분야도 예외는 아니어서 일본에는 우리나라 국립과학수사연구원과 기원이 비슷한 과학경찰연구소(National Research Institute of Police Science)가 존재합니다. 이 연구소는 1948년에 국가지방경찰본부 형사부 감식과에서 출범했습니다 (우리나라 국립과학수사연구원은 1955년에 내무부 치안본부에서 시작). 명칭으로만 보면 우리나라 국립과학수사연구원처럼 전국에 걸친 종합적인 감정서비스를 하는 기관으로 생각하기 쉽지만 이 연구소는 감정업무는 일부의 경우를 제외하곤 하지 않고 있으며 법과학 기술 R&D와 교육·연수를 주된 업무로 하는 기관으로 동경에 본원 하나만 두고 있습니다.

과학경찰연구소가 국가 경찰인 경찰청 소속으로 경찰법에 설립근거를 두고 있는 반면에 지방자치 경찰인 경시청(동경)이나 47개 도도부현(都道府縣) 경찰본부에는 별도로 각각의 과학수사연구소를 두어 사건 수사와 관련한 법과학 감정서비스를 맡고 있습니다.

전국의 과학수사연구소 감정 인력을 전부 합치면 1,100 여명이 넘는다고 하며 이 숫자는 사건현장에 투입되는 감식과 인원은 포함하지 않으므로 일본에는 우리나라 보다는 훨씬 많은 감정인력이 존재한다고 할 수 있겠습니다. 과학수사연구소는 주로 법의학(생물), 심리학, 문서감정, 물리학(공학), 화학 분야로 나뉘어지며 감정인력은 경찰직이 아닌 기술직 공무원으로 이루어져 있다고 합니다. 일본의 경우 부검은 각 의과대학의 법의학교실에서 맡고 있어 부검을 위한 별도의 조직은 가지고 있지 않은 것이 특징입니다.



다시 얘기를 과학경찰연구소로 돌려보겠습니다. 연구소는 총 6개 부 및 연구조정관, 부속 감정소, 법과학연구소 등으로 나뉘어 집니다. 연구를 담당하는 인원이 100여명이고 행정직을 합쳐도 총원이 150명 정도로 3만 5천 평방미터에 이르는 건물면적에 비해 상대적으로 적은 정예 인원으로 운영이 되고 있다고 할 것입니다. 부서의 구분을 적용이 되는 학문 분야별로 하고 있는 점이 흥미롭습니다.



법과학 제1부는 생물학을 근간으로 하는 분야에 대한 연구개발 업무를 담당합니다. 모발의 형태분석, 수퍼임포즈 등을 활용한 백골사체의 얼굴복원, 혈액형이나 체액흔 종류를 밝히는 최신 기술의 개발, 최신 DNA감정 기술의 도입 및 전파 등이 업무 영역에 해당합니다. 일본의 범죄자 DNA 데이터베이스에 입력되는 범죄자 시료는 직접 감정도 하여 결과를 경찰 DB운영부서로 전달하고 있습니다.

법과학 제2부는 물리학 및 공학 관련 부서입니다. 사진이나 비디오 영상에 대한 영상계측법, 식별, 복원 등으로, 화재사건의 발화원인 규명, 각종 폭발사건에 있어서 폭발현상의 규명, 폭발물 위력 등에 대한 사례 조사 및 연구가 주된 업무를 이루고 있습니다. 법과학 제3부는 화학연구 시설입니다. 각종 마약을 비롯한 남용약물의 분석법 연구, 독극물이나 환경오염 물질의 식별, 범죄 현장에서 발견되는 각종 미세증거물(유리, 섬유 등)의 화학적 분석을 통한 수사지원 등이 주된 업무를 이룹니다. 법과학 제4부는 심리분석, 문서감정, 음성분석 분야 등에 대한 연구 및 제한된 감정서비스를 수행하고 있습니다. 범죄행동과학부는 프로파일링 등 범죄자의 심리, 진술분석 등 피해자의 심리에 관한 조사를 통해 자료를 축적해 나가고 있으며 더 나아가 소년연구실을 두어 소년 비행의 원인이나 배경을 밝히는 조사 연구를 수행하고 범죄예방연구실, 인질사건 등에 관한 수사지원 연구실 등을 통해 사건의 해결뿐만 아니라 범죄의 특성 및 예방과 관련한 연구결과를 지속적으로 쌓아가고

있습니다. 교통과학부를 별도로 두고 사고 방지, 교통신호 제어 고도화, 배출가스 측정시스템 연구 등을 통해 교통안전 및 교통정책의 관리에도 기여하고 있습니다.

과학경찰연구소는 연구개발을 주 업무로 하는 만큼 높은 수준의 기술 개발을 위해 엑스레이 회절분석기, 핵 자기 공명장비 등 고가의 기초과학 장비도 공동 장비실을 두어 운영 중입니다. 연구소에서 축적된 연구결과 자료 및 모든 노하우는 지방의 과학수사연구소에 효과적으로 전수가 이루어져야 하기에 교육 및 훈련은 과학경찰연구소의 가장 중요한 기능 중 하나이며 이를 위하여 별도의 법과학연구소를 두고 있습니다. 연구소는 법과학 감정에 관한 실무 습득 위주의 연수를 실시합니다. 특히 교육 대상자들을 구분하여 신규 임용된 감정직원을 위한 코스(양성과), 5년 이상 실무경험자 코스(현임과), 고도의 지식 및 기술 전수를 위한 코스(전공과) 등을 개설하고 대상자의 수준에 맞는 훈련이 이루어지도록 하고 있습니다. 연간 약 600명 이상의 감정관 교육이 보통 2주 이상의 합숙 교육으로 별도로 설립된 기숙사에서 이루어집니다.

사실 일본의 법과학 수준이나 세부 사항은 국제적으로 잘 알려지지 않은 편입니다. 국제학술지 보다는 자국의 학술지에 연구논문을 많이 게재하는 점, 새로운 것을 받아들임에 대해 신중한 입장을 보이는 측면 등이 제한적인 요소라 할 것입니다. 국제학회 출장 등에서 만난 감정 전문가들로부터 느끼는 점은 이들이 모든 분야에 있어 기초를 매우 중시하고 있고 오래된 기술이라도 쉽사리 버리지 않고 개선하려고 노력하고 있으며 내실화 연구에 충실하다는 것이었습니다. 이러한 점이 연구와 교육기능 위주의 전문 기관을 키우게 된 배경이라고 할 수 있을 것 같습니다. 법과학 연구와 기술전수를 전문으로 하는 상위 개념의 기관이 우리나라에도 하나 필요하지 않은가 생각해 봅니다.

수학식 없는 인공지능 이야기

디지털수사과 사무관 박종훈

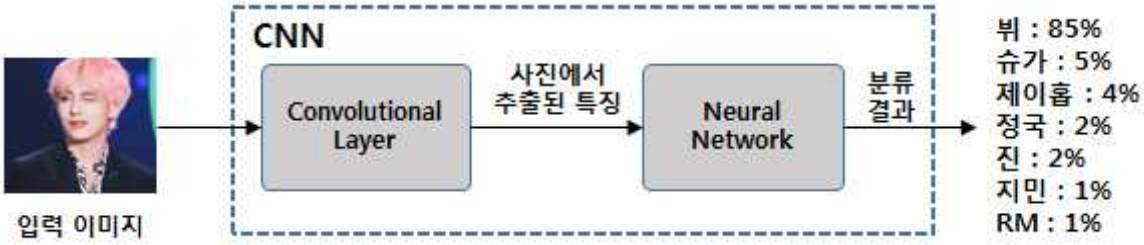
수학식 없는 인공지능 이야기

이미지 인식(객체 인식)·분류기법인 CNN이라는 인공지능 알고리즘을 수학식 없는 설명을 통해 인공지능에 대한 이해도를 높이고 활용방안을 모색해 봅니다.

인간이 가진 학습, 추론, 지각, 자연언어의 이해 등의 능력을 컴퓨터 프로그램으로 실현한 기술이 인공지능이라고 합니다. 지난 2016년 이세돌 9단과 구글의 알파고와의 대국에서 이세돌 9단이 완패(1승 4패) 이후 인공지능 또는 딥러닝이라는 이름으로 일반인에게 인공지능의 우수성이 알려지기 시작했습니다. 하지만 인공지능 연구는 1960년대부터 컴퓨터의 발전에 따라 계속되어왔고, 최근 컴퓨터 성능의 급속 발전으로 새로운 시작·전환점을 맞게 됩니다.

하지만 일반인이 이러한 인공지능이 어떻게 작동하는지, 원리는 무엇인지를 알려고 하여 인터넷 서핑이나 문서를 찾아봐도 난해한 수학식이나 전문 용어를 사용하여 작성된 자료를 보면 수포자(?)가 되곤 합니다. 여기서는 최대한 수학식을 없애고 인공지능 알고리즘의 일종(딥러닝 기반)인 CNN(Convolution Neural Network)에 대한 설명으로 컴퓨터가 어떻게 이미지(그림) 파일 내의 객체(사람, 사물, 동물 등) 인식하는가에 대해 알아보고, 사전정의된(pre-defined) 이미지인식 모델(vgg, resnet 등)을 사용하여 간단한 이미지 분류 테스트를 수행해봅니다.

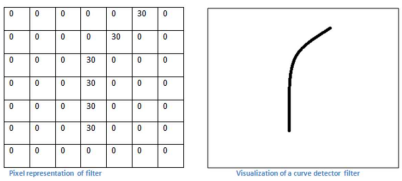
CNN은 전통적인 인공지능 알고리즘인 뉴럴 네트워크(Neural Network : 인간의 신경전달 구조를 모사하여 컴퓨터가 학습을 하는 구조) 앞에 여러 컨볼루션 계층(Convolution Layer)을 통해 입력 받은 이미지에 대한 특징(Feature)를 추출하고, 이렇게 추출된 특징을 기반으로 뉴럴 네트워크를 이용하여 분류하는 구조입니다.



컨볼루션 레이어는 특징을 추출하는 기능의 필터(Filter)와 이 필터의 값을 입력값으로 하는 연산의 출력값을 계산하는 활성화함수(Activation Function : 결과값을 참/거짓으로 나타내는 것이 아니라, 참에 가까워지면 참의 특정값, 거짓이면 거짓의 특정값에 가까워지는 형태로 출력하는 함수, 예: 활성화 함수 중 Sigmoid 함수는 참에 가까워지면 0.5 ~ 1, 거짓에 가까우면 0 ~ 0.5 사이의 값을 출력함)로 나뉘어 집니다. 필터의 출력값을 0, 1 같은 상수로 하지 않는 이유는 하나의 필터가 이미지의 특정 부분에 100% 일치하기는 어렵기 때문으로 볼 수 있습니다.

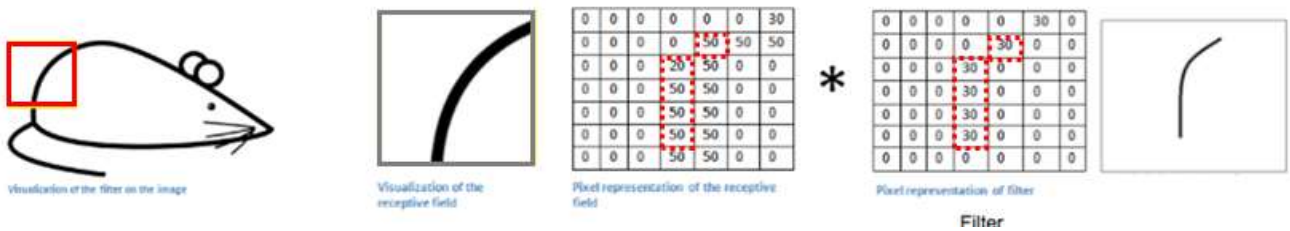
먼저 이미지 파일은 픽셀(pixel, 화소) 단위로 이루어져 있습니다. 가로x세로의 픽셀 수에 따라 해상도(resolution)를 나타내며 이를 수학의 N x N 행렬로 나타낼 수 있습니다. 각 픽셀은 RGB(Red, Green, Blue : 색의 3요소)값 등을 가질 수 있고 몇 byte를 하나의 픽셀로 계산하는가? 압축 했을 때 손실을 허용할 것인가? 등에 따라 bmp, jpeg, gif 등의 파일 포맷으로 나뉘어집니다.

필터 또한 작은 이미지 파일 형식(NxN 행렬)으로 되어 있고 그 특징이 입력 이미지에 있는지 없는지를 검출해 줍니다.



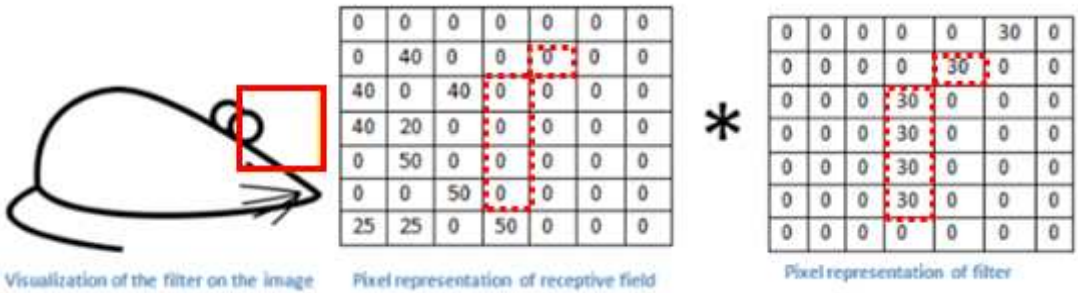
예를 들어 좌측과 같은 곡선을 검출해 주는 필터(이미지)가 있다고 하면 실제 실행 시에는 행렬로 변환하여 계산합니다.

아래 쥐 그림에서 좌측 상단의 이미지 부분에 필터를 적용한 결과 예시입니다.



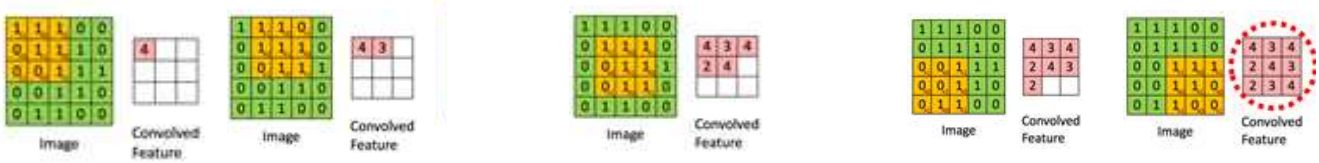
결과값은 = (50*30)+(50*30)+(50*30)+(20*30)+(50*30) = 6600

만약 아래 그림처럼 쥐 그림에서 아래와 같은 부분에 같은 필터를 적용해 보면,



결과값은 0에 수렴한다 할 수 있습니다. 즉 필터는 입력 데이터에서 그 특성을 가지고 있으면 큰 결과값이 나오고, 특성을 가지고 있지 않으면 결과값이 0에 가까운 값이 나오게 되어 입력 데이터가 그 특성을 가지고 있는지 여부를 알 수 있게 해줍니다. 실제로는 입력 이미지 데이터에는 여러 가지 특성이 있기 때문에 하나의 필터가 아닌 여러 개의 필터를 적용하게 됩니다.

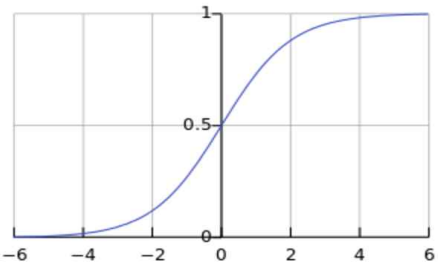
그렇다면 이 필터를 어떻게 전체 이미지에 적용할까? 아래 이미지를 보면 5x5 크기의 원본 이미지가 있다면 3x3 필터를 좌측 상단에서부터 왼쪽으로 한 칸씩, 그 다음 줄로 내려서 또 왼쪽으로 한 칸씩(필터 적용 간격을 stride라고 합니다) 적용(Convolve : 합성곱)해서 특징을 추출해 내고 그 결과를 (Convolved) Feature map 또는 Activation map 이라고 합니다.



그러면 이러한 필터는 어떻게 만들어질까요? CNN의 자체 기능으로 데이터를 넣고 학습시키면 자동으로 학습 데이터에서 특징을 인식하고 필터를 만들어냅니다.

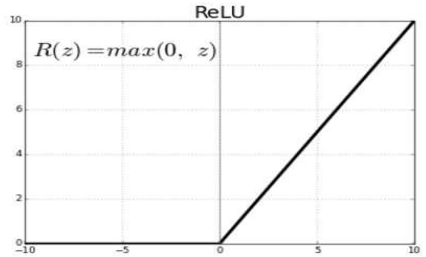
필터를 통해 Feature(Activation) Map이 추출되었으면, 이 Feature Map에 활성화함수(Activation Function)을 적용하게 됩니다. 위 쥐 그림에서 곡선 값의 특징이 들어가 있는지 아닌지에 따라 필터가 추출한 값이 들어가 있으면 6600, 없으면 0으로 나왔습니다. 이 정량값을 그 특징이 "있다 없다"의 형태로 바꿔주는 과정이 필요한데, 이것이 바로 활성화 함수입니다. 즉, 결과값이 참(True)/거짓(False)이 아닌 "참/거짓에 가깝다"라는 값으로 변환해 주어야 다른 특징들을 모두 검토하여 원본 데이터를 분류할 수 있습니다. 결과값이

0이나 1 같은 값이 나온다면 이렇게 인공지능 알고리즘(Neural Network)을 사용하여 학습할 필요 없이 산술연산 만으로도 간단히(그것도 빠르게) 결과값이 나오게 됩니다. 이러한 활성화함수에는 Sigmoid, ReLU 등이 사용됩니다. 뉴럴네트워크(CNN 등)에는 ReLU 함수가 주로 사용됩니다.



<Sigmoid 함수>

결과값이 참에 가까워지면 0.5 ~ 1 사이에서 1에 가까운 값을, 거짓에 가까우면 0 ~ 0.5 사이의 값을 리턴합니다.

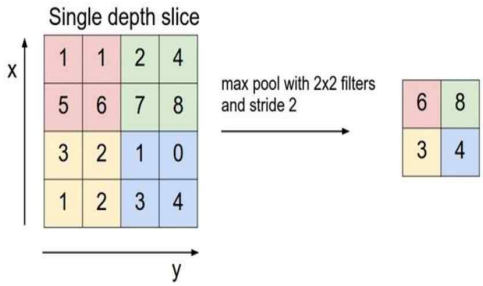


<ReLU 함수>

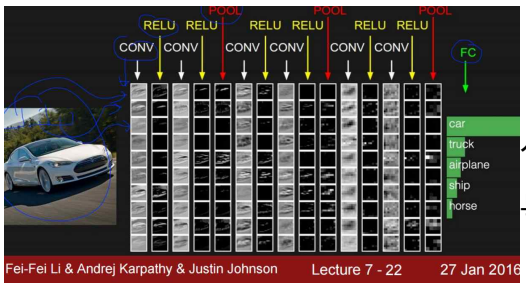
입력값이 양수(+)일 경우 입력값에 따라 결과값이 리턴(선형)되고, 입력값이 음수(-)이거나 0은 0의 값을 리턴합니다.

ReLU함수를 사용하는 이유는 "신경망에서는 Back Propagation(역전파)라는 방법을 사용하는데, sigmoid의 경우는 계층이 깊어질수록 뒤에서 앞으로 전달할 때 희석되기 때문"이라고 하지만, sigmoid의 경우는 0 ~ 1 사이의 값의 분류(이진 분류)에 적합하지만 ReLU의 경우 입력값이 크다면(특징이 명확하다면) 입력값과 같은 크기의 값이 네트워크로 전파되기 때문에 sigmoid 보다 다양하고 큰 값을 표현할 수 있어서 사용하는 것으로 보입니다.

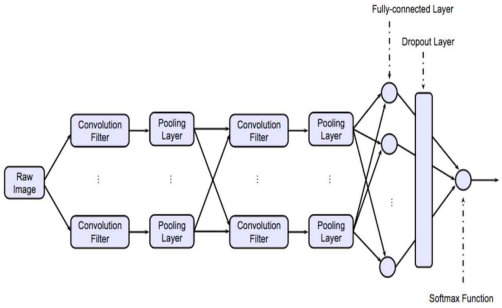
이렇게 컨볼루션널 레이어를 거쳐서 어느 정도 특징들이 추출되면 모든 특징을 가지고 판단할 필요는 없습니다. 인간이 고해상도 사진을 보고 물체를 판별할 수 있지만, 작은 사진을 가지고도 그 사진의 내용을 알 수 있는 것과 같은 원리입니다. 이러한 축약 과정을 sub sampling 또는 pooling 이라고 합니다. 이 축약 방법에서 많이 사용되는 것이 max pooling입니다. max pooling은 위의 activation map을 MxN크기로 잘라낸 후 가장 큰 값을 뽑아내는 방식입니다. 풀링은 매번 수행하는 것이 아니라 데이터 크기를 줄여, 컴퓨팅 리소스를 적게 사용하게 하거나, 데이터의 크기를 줄이면서 손실이 발생하기 때문에 과적합(Over fitting)을 방지(85%정도의 결과값으로 이미지를 식별/분류할 수 있다면 95%의 결과값을 위해 노력-Over fitting-하지 않아도 된다는 의미)할 수 있습니다.



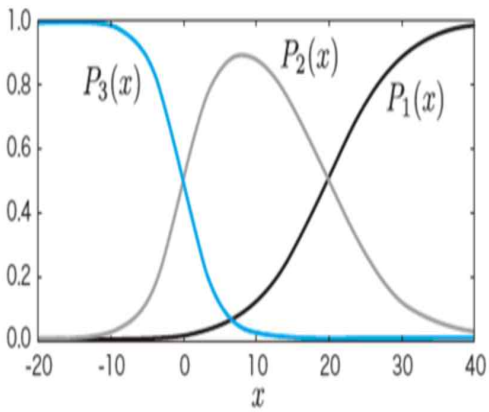
Max Pooling은 특징의 값이 큰 값이 다른 특징을 대표한다는 개념입니다.



이렇게 컨볼루션 레이어는 필터(Convolve), 액티베이션함수(ReLU), Pooling layer를 반복적으로 조합하여 특징을 추출합니다.

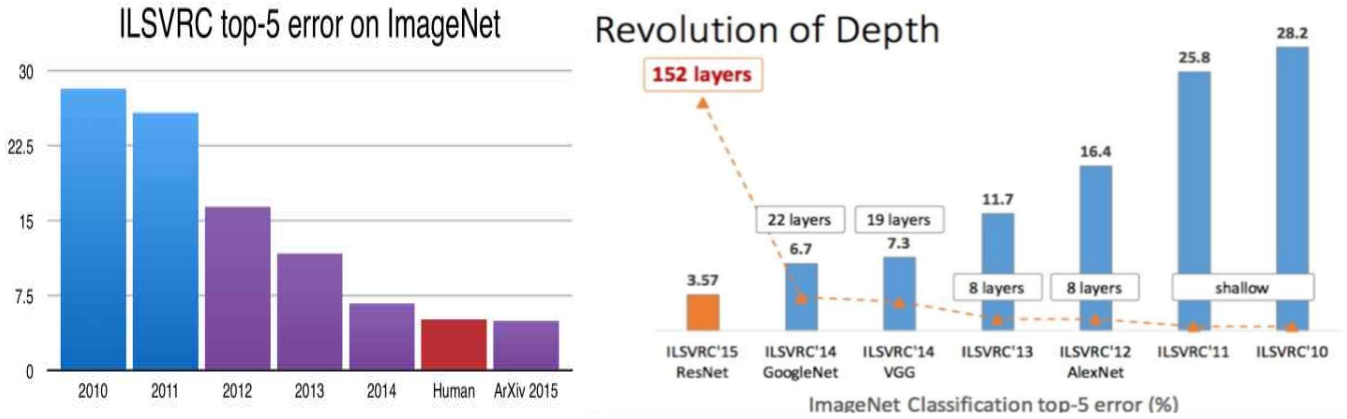


컨볼루션 계층에서 특징이 추출되면 이 추출된 특징값을 기존의 뉴럴 네트워크(인공 신경 지능망)에 넣어서 분류를 합니다. 왼쪽 그림 원형들이 분류 기능을 하는 신경망을 나타냅니다.



위 그림 마지막의 Softmax 함수는 여러 개의 분류를 가질 수 있는 함수입니다. P3(x)는 특징(feature) x에 대하여 P3일 확률, P1(x)는 특징 x에 대하여 P1일 확률입니다. Pn값은 항상 0 ~ 1.0의 범위를 가지며 P1+P2+P3...+Pn = 1.0입니다. 즉 맨처음 BTS 뷔의 이미지를 넣었을 때, 뷔일 확률은 0.85, RM일 확률은 0.01 식으로 표현됩니다.

이렇게 복잡한 내용을 어떻게 구현할 수 있을까요? 다행히 Google(tensorflow), Amazon(mxnet), Microsoft(CNTK) 등에서 CNN을 포함한 여러 인공지능 알고리즘(모델)을 구현할 수 있는 AI Framework를 공개하여 일반인도 사용할 수 있습니다. 하지만 기본적인 프로그래밍 언어(보통 Python을 사용), 사용되는 각종 수학적 지식, 대용량 데이터 처리 기법 등에 대한 기본 지식이 있어야 합니다.



특히 이미지 인식/분류에는 이미지넷(http://www.image-net.org)에서 주최하는 ILSVRC (Large Scale Visual Recognition Competition)이라는 대회를 개최하는데, 천만장의 이미지를 학습하여 15만장의 이미지를 인식하는 정답률을 겨루게 됩니다. 특징적인 것은 2014년 구글이 심층학습기법(Deep Learning : 이후 알파고의 알고리즘으로 발전) 기반의 CNN 구현으로 22개의 레이어로 6.7%의 오차율을 기록하였고, 이후 다른 곳에서도 심층 학습기법을 사용하여 2015년 마이크로소프트는 152개의 레이어로 3.57%의 오차율을 기록 하였습니다(인간의 평균 오차율은 5% 내외임).

하지만 이 대회에서 사용되는 인공지능 기법은 지도학습(Supervised Learning) 방법인데 이는 사람이 事前에 모든 이미지 파일을 카테고리별로 분류하여 이 분류 체계를 컴퓨터에게 학습시키는 방법입니다. ImageNet 대회의 경우 1,000개의 카테고리(주로 동물, 사물 중심)로 이미지들이 분류되어 있습니다.

그리고 ImageNet에서 좋은 성능을 보인 모델(vgg16, ResNet, Inception 등)들은 실행 시 여러 조건값(parameter : 필터의 크기, 종류, 활성화 함수 구현, 계층의 수 등)을 저장 하여 CNN 전 과정을 거치지 않고 이미지 분류 테스트해 볼 수 있게 공개되어 있습니다.

(pre-defined parameters)

그러면 이 사전정의된 조건값을 가지고 간단한 이미지 분류 테스트를 구현해 보겠습니다. 먼저, 인터넷에서 몇가지 pre-defined model paramenter 파일을 다운받습니다.(수백MB ~ 수십GB까지 큰 파일들입니다.) 다음, python 프로그래밍 언어를 설치합니다. Amazon에서 공개한 mxnet이라는 AI Framework를 설치합니다. mxnet에서 pre-defined model 테스트 파일 다운로드 후 python으로 실행합니다(다운로드는 글 마지막 참고 내역 참조).

<소스 코드>

```
vgg16,c = init("vgg16")
resnet152,c = init("resnet-152")
inceptionv3,c = init("Inception-BN")

#filename = sys.argv[1]
#filename = '/tmp/kcreator.jpeg'
#filename = 'D:/tmp/tiger.jpg'
#filename = 'D:/tmp/elephant.jpg'
filename = 'D:/tmp/BTS-v.jpg'

print ("********************** VGG16")
print (predict(filename,vgg16,c,5))
print ("********************** ResNet-152")
print (predict(filename,resnet152,c,5))
print ("********************** Inception v3")
```

BTS 뷔 이미지를 입력으로 설정

VGG16, ResNet-152, Inception v3 라는 pre-defined 모델로 분류 시도

<실행 결과>

VGG16은 'pajama(파자마)'라는 분류 : 74.7%

ResNet-152는 'kimono(기모노)' : 62.1%

Inception v3는 'bow(활 모양)' : 12.9%

BTS 뷔의 이미지는 ImageNet 경연용 이미지에 학습되어 있지 않아 학습되어 있는 '파자마(잠옷, N03877472)' 등으로 분류됩니다. 다음은 ImageNet의 '파자마' 에 속해 있는 이미지 파일들입니다.

<소스 코드>

```
vgg16,c = init("vgg16")
resnet152,c = init("resnet-152")
inceptionv3,c = init("Inception-BN")

#filename = sys.argv[1]
#filename = '/tmp/kcreator.jpeg'
#filename = 'D:/tmp/tiger.jpg'
filename = 'D:/tmp/elephant.jpg'
#filename = 'D:/tmp/BTS-v.jpg'

print ("********************** VGG16")
print (predict(filename,vgg16,c,5))
print ("********************** ResNet-152")
print (predict(filename,resnet152,c,5))
print ("********************** Inception v3")
print (predict(filename,inceptionv3,c,5))
```

코끼리 이미지를 입력으로 설정

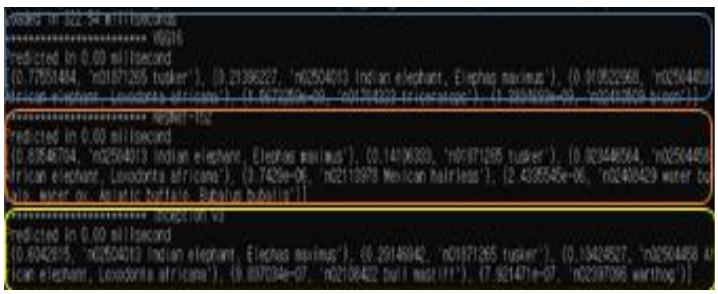
VGG16, ResNet-152, Inception v3 라는 pre-defined 모델로 분류 시도

<실행 결과>

VGG16은 'tusker(어금니 코끼리)' : 77.5%

ResNet-152는 'Indian Elephant' : 83.5%

Inception v3는 'Indian Elephant' : 60.4%



현실 세계에서는 수많은 이미지 파일을 사람이 선별/분류할 수 없습니다. 이렇게 정답이 주어지지 않은 상황에서 입력들이 주어졌을 경우 그 입력에 대한 결정을 하고, 새로운 입력이 들어올 경우 결과를 예측하는 모델을 비지도학습(Unsupervised Learning) 방법이라고 합니다. 이 경우 데이터의 양과 종류에 따라 각기 다른 분류체계를 구성할 수 있습니다. 자신이 원하는 분류체계를 기계학습을 통해 구한다는 것은 지난한 노력과 시행착오가 필요합니다. 특히 가설/모델 수립을 위해서는 데이터과학자(Data Scientist), 이에 대한 구현을 위해서는 프로그래밍 언어 및 AI Framework(Google tensorflow, Amazon mxnet 등)에 정통한 개발자 등이 반드시 필요합니다. 그리고 비지도학습은 지도학습에 비해 몇 십 ~ 몇백 배의 컴퓨팅 자원(서버, CPU, GPU, Memory 등)이 필요한 것으로 알려져 있습니다.

이제 빅데이터 처리와 인공지능 기술은 선택이 아닌 필수가 되었습니다. 압수된 대용량 디지털 정보에서 어떻게 지능적인 범죄혐의 분석을 할 것인가에 대한 고민을 시작할 때가 된 것 같습니다.

<참고 내역>

1. 딥러닝 - 초보자를 위한 컨볼루션 네트워크를 이용한 이미지 인식의 이해, 조대협, https://bcho.tistory.com/1149
2. 모두를 위한 머신러닝/딥러닝 강의, 김성훈, https://hunkim.github.io/ml
3. A beginner's guide to understanding Convolutional Neural Networks, Adit Deshpande,https://adeshpande3.github.io/adeshpande.github.io/A-Beginner's-Guide-To-Understanding-Convolutional-Neural-Networks/
4. Python download, https://www.python.org
5. tensorflow download, https://www.tensorflow.org
6. mxnet download, https://mxnet.apache.org
7. Pre-defined model download, https://github.com/onnx/models

『사건 속 법의학 이야기』 ⑤

아동 학대 그 오래된 역사

서울대학교 법의학 교수 유성호

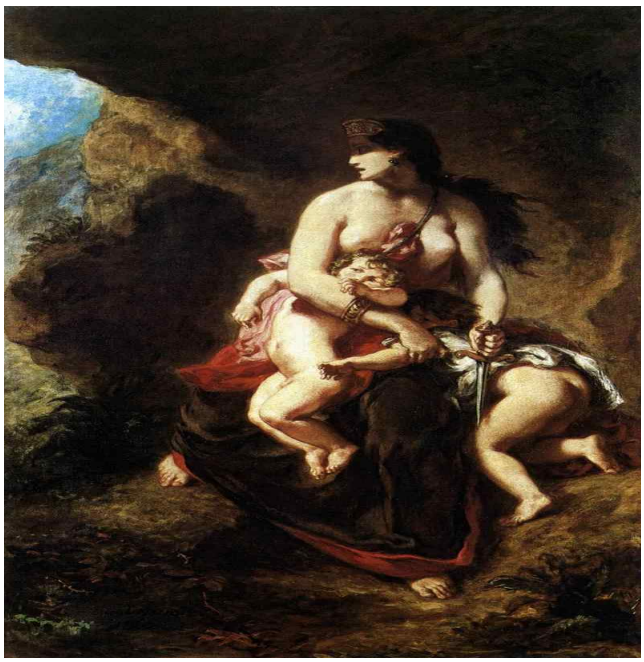
아이들의 밝은 웃음을 보면 이 세상에 천사가 있다면 아이일 것이라고 느껴진다. 보통의 부모라면 아기가 태어나는 순간 경외감과 함께 양육의 엄중함을 깊숙이 느끼게 된다. '아이 분유, 기저귀 값 벌어야 된다.' 라는 말을 하며 생계에 책임감을 가진다.

의학적으로는 1세 이하의 아이를 영아(infant)라는 용어로 분류하며, 부모의 손길이 가장 많이 필요한 시기라고 이야기 한다. 그러나 불행히도 법의학에 종사하다보면 1세 이하의 영아를 살해하는 영아살해(infanticide) 또는 자식살해(filicide)라는 단어에 익숙해지며, 다양한 사연들을 가진 사건들을 만나게 된다.

자식살해에서 많은 사람들이 어렴풋이나마 알고 있는 용어는 메데아(Medea) 또는 메데이아 콤플렉스일 것이다. 그리스 신화에서 메데이아는 남편 이아손(iason, 야손(jason)이라고도 함)에 대한 사랑 때문에 아버지의 뜻을 거스르면서 자신의 남동생 압시르토스(Absyrtos)를 제거하고, 남편 이아손이 자신을 배신하고 크레온(Kreon)의 딸 글라우케(Glauke, 크레우사라고도 함)를 부인으로 삼으려 하자 연적인 그녀와 그녀의 아버지를 불태워 죽이고 결국에는 남편에 대한 복수를 위해 자신의 두 아들마저 살해하는 악녀로 묘사된다. 메데이아가 두 아들을 살해한 사실을 알게된 남편 이아손은 "저주받을 여인이여! 자신이 낳은 자식을 칼로 찌르는 차가운 가슴을 갖은 여인이여, 나와 신과 이 세상 모든 인류로부터 저주받을 지어다."라고 말했다. 그러나 현대에 와서는 자신의 운명에 굴복하지 않고 스스로 운명과 투쟁하는 독립적이고 강한 인물상으로 재평가되기도 한다. 즉 자식들을 제 손으로 죽이지만 남성이 만들어낸 사회적 굴레에 저항하는 여성상으로 예술적 영감을 제공한 것이다. 그러나 자신의 자식을 살해했다는 충격적인 소재에서, 정신의학자들은 메데이아 콤플렉스라는 신조어를 만들어, 자신의 자녀를 죽이고자 하는 소망으로 자신의 남편에 대한 복수심이 근저에 깔려 있는 것으로 정의하였다. 이밖에 불우한 환경에서 자살 시도를 하는 부모 중 특히 어머니는 자녀를 독립된 하나의 인격으로 보기보다는 자식을 자신의 일부로 보는

경향이 있다. 자신이 느끼는 현실의 고통을 자신의 아이도 함께 하고 있다고 생각하며 불행한 운명에서 자신의 아이를 벗어나게 하려는 이타주의적 동기의 살인도 간혹 관찰된다.

실제 자식살해를 한 부모 89명을 대상으로 한 외국의 연구[1]에 의하면 상당수의 가해자에게 범죄의 가족력이 있었고, 가해자 스스로도 어려서 부모에게 학대를 받거나 15세 이전에 부모와 이별을 경험한 경우가 많았다. 범행을 저지른 어머니는 기혼인 경우가 많았고, 자식살해 당시 본인도 자살시도의 비율이 높았으며, 이후 자신의 범죄를 은폐하려 하지 않는 특성이 있었다고 보고되었다. 우리나라의 실제 사건에서 자식을 살해한 부모들은 사건 당시 매우 멍한 상태를 보이는 경우가 많으며 사건에 대해 감정 없이 기계적인 방식으로 고백하기도 한다. 특히 정신과적 문제가 있어 자식을 살해한 부모의 경우에는 자신의 범행을 숨기려 하지 않고, 대부분 범행 직후 주변 사람들에게 바로 도움을 청한다. 반면에 원하지 않았던 아이였거나 폭력을 저지르는 와중에 살해할 경우 범행이 발각되기 전까지 숨기려는 경향이 있으며 사고에 의한 사망을 주장하기도 한다.


<들라크루아, 격노한 메데이아, 1862년>

법의학자는 아이의 시신을 검사할 경우에는 더욱 집중하게 된다. 죽은 아이가 끝내 말하지 못한 이야기를 듣기 위해 더 큰 노력을 기울이게 된다.

첫 번째 이야기는 2000년대 서울의 한 종합병원에서 시작된다. 생후 11개월 된 아이는 10월의 어느 밤에 병원 응급실로 후송이 되었다. 한창 웃고 울면서 귀여움을 떨 시기에 의식을 잃은 상태로 신체의 반사가 거의 확인되지 않았다. 여러 검사를 통해 아이는 경막하 출혈(硬膜下出血)로 진단되었다. 경막하 출혈이란 머릿속 출혈로 머리뼈 안쪽의 뇌경막과 거미막 사이 공간에 출혈이 나는 것으로 대부분 외상(外傷)에 의해 발생한다. 주로 머리가

1) d'Orban PT. Women who kill their children. Br J Psychiatry 1979;134:560-71.

빠르게 움직이다가 갑자기 멈추게 되는 가속-감속의 기전에 의해 발생하고, 임상적으로 대부분 넘어짐(전도顚倒)의 상황이나 벽 등의 고정된 부위에 부딪히는 경우에서 관찰된다. 대학병원 담당 의사는 의아했다. 보통 넘어져 땅에 머리를 부딪치거나 벽에 머리를 굉장히 세게 박을 경우 생기는 경막하 출혈은 아이에게는 잘 발생하지 않기 때문이다. 의사는 새파랗게 젊은 20대 초반으로 보이는 아이 엄마에게 조심스럽게 물었다.

"아이가 언제부터 의식이 없었나요?"

"애가 잘 노는 것 확인하고 잠깐 분유를 준비하러 부엌에 갔다 오니 애가 자고 있어서 자나 했어요 근데 계속 깨지를 않아서..." 엄마는 눈 주위가 벌겋게 충혈된 채 대답했다.

"혹시 아이가 어디에서 떨어지거나 하지는 않았나요?"

의사는 재차 물었다.

"아니오. 흑흑 그런적 없었는데. 아!" 갑자기 생각이 난 듯 이야기를 계속했다. "우리 애가 아까 오전에 보행기 없이 걷다가 넘어져서 크게 울었긴 했는데...".

의사는 재차 물으려다 상태가 나빠졌다는 간호사의 응급 콜에 아이를 보러 돌아갔다. 수술이 진행되었고 몇 시간이 지난 아침에 아이 아빠가 나타났다. 아이 아빠는 고등학교를 막 졸업한 듯 한 젊은이였다. 전날 과음을 한 듯한 얼굴과 부스스한 머리카락을 한 채 물었다. "우리 애는 어떤가요? 수술은 잘되었나요?" 옆에서 엄마가 흐느끼고 있었다.

"일단 머릿속 출혈을 제거 하기 위해 응급 수술을 진행하였고 상태를 지켜봐야 할 것 같습니다." 아이 아빠는 눈물을 뚝뚝 흘렸다. 갑작스런 불행에 황망해 하는 젊은 부부의 모습이었다. 아이는 의식을 찾지 못하고 며칠 후 사망하였다. 담당 의사는 안타까움을 느꼈으나 다른 고민도 있었다.

보통 병원에서 사망하게 되면 사망진단서를 발급하게 된다. 사인(死因)란에 병으로 사망한 병사라 적으면 장례가 그대로 진행되게 된다. 의사는 고민하였다. 뭔가 석연치 않았다. 이 아이는 두 경우 모두 아니었다. 오른팔에 멍이 들어 있었지만 추락은 아니라고 생각했다. 고민하던 의사는 사인을 외인사(外因死)로 적어 놓았다. 절차에 따라 병원 행정실에서 경찰에 신고하였다. 출동한 경찰은 부모에게 질문을 했다.

"여기 의사 선생님이 외인사라고 하는데. 외인사라는 것은 자살, 타살, 사고사 뭐 이런거에요. 아이가 갑자기 사망해서 정신이 없으시겠지만 협조해 주십시오."

아이 엄마는 거세게 항의했다. “아이가 죽었는데 지금 무슨 경찰이 와서 이래라 저래라 하는 건가요? 우리 마음은 헤아리지도 않나요?”

아이 아빠도 합세했다. “아이가 죽은 마당에 지금 의사가 경찰 조사를 받게 하다니. 당신은 아이도 없어?” 말이 점점 거칠어 졌다. 의사는 후회하였다.

경찰은 부모를 달랬다. “아이가 넘어진 적 있지요?”

“네 어제 걷다가 넘어져서 울었어요.”

“그럼 그때 다쳤나 보네.” 경찰이 재차 확인했다.

사건은 그대로 사고사로 넘어가려고 했다. 최종 결정자는 검찰이었다. 검사는 경찰의 사건 보고를 보고 뭔가 이상했는지 부검을 지시했다.

부모들은 부검에 반대했다. 특히 어머니는 아이가 이미 죽었는데 주검에 다시 칼을 대는 부검은 부모들의 마음을 헤아리지 못한 처사라고 강하게 항의했다. 그러나 부검은 시행되었다.

병원에서 사망한 사람의 부검을 할 때에는 모든 의무기록과 검사 자료를 확인한 후 시작한다. 아이의 몸을 전체적으로 확인하였다. 오른팔과 오른손목에 멍자국이 있었다. 수술 전 자료에서 오른쪽 뇌 부위에 큰 경막하 출혈이 관찰되었다. 부검을 시작하고 아이의 머리 왼쪽 관자뼈(머리옆쪽의 뼈)의 골절과 오른쪽 뇌 부위의 경막하 출혈을 확인했다. 비교적 간단한 부검이었다. 사망원인은 머리손상. 가속-감속 즉 머리가 속도를 가지고 움직이다가 갑자기 멈추면서 발생한 손상이었다. 성인이 이럴 경우는 보통 술을 먹고 넘어진 경우가 많다. 그러나 어린이 특히 신장이 1미터 이하인 영아에서는 머릿속 혈관 질환이 있거나 추락 이외에 경막하출혈은 잘 볼 수가 없다.

경찰에게 담담하게 설명하였다.

“오른팔과 오른손목에 멍 자국으로 봐서 아이에게 살아있을 때 즉 생전 손상이 있었습니다. 머리 왼쪽 관자뼈에 골절과 함께 뇌의 오른쪽과 이마엽에 경막하 출혈로 있는 것으로 보아 추락 또는 벽에 머리를 세게 부딪친 것으로 보입니다. 그러니 다시 잘 조사해 보십시오.”

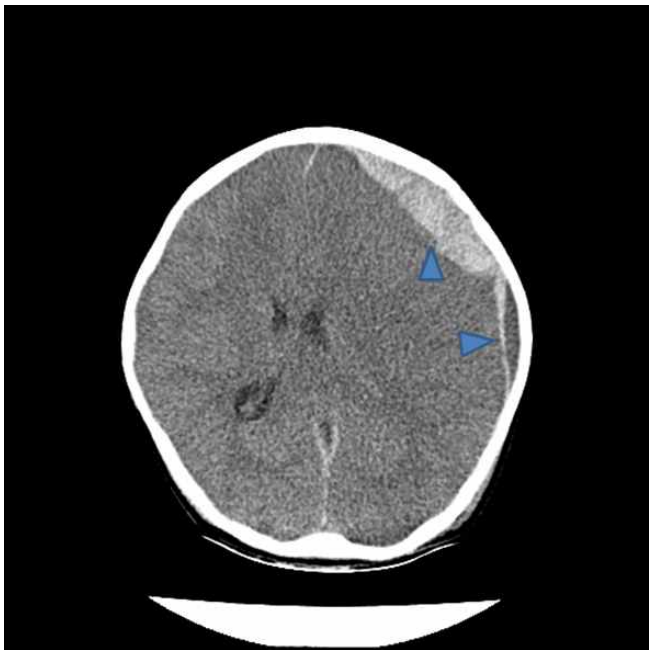
경찰은 유능하게 변했다. 아이 엄마에게 어떻게 질문을 하였는지 자백을 받아냈다. 아이와 부모가 사는 집을 조사해서 벽에 부딪힌 흔적도 찾았다.

아이 엄마의 진술은 안타까웠다. ‘고등학교를 막 졸업하고 아이가 생겨 어쩔 수 없이 결혼을

한 상황이 너무 싫었다. 그리고 남편은 변변한 직업도 없이 매일 술을 마셔 화가 나고 아이는 울어대서 벽에 딱 한번 던졌는데 아이가 조용해지더니 갑자기 의식을 잃었다'라고.

이런 현상은 전형적인 원치 않는 아이(Unwanted Child)에 대한 폭력이다. 부모의 자식에 대한 사랑보다 자신의 자기본위적인 욕구를 우선순위에 두는 데서 발생한다. 단지 부모가 원치 않았던 자식이라는 이유에서 행해진 것이다.

두 번째 이야기는 2013년 모 방송 프로그램 작가의 전화를 받으며 시작한다. 방송 작가는 '요즘 게시판을 달구는 뜨거운 이슈가 있는데 교수님께서 한번 봐주셨으면 한다'고 요청했다. 방송의 특성상 소재를 찾아서 이런 저런 게시판을 탐색하는 작가 분들의 노고를 알기에 바쁜 와중에도 자료를 잘 검토해 주는 편이다. 더욱이 27개월 아이의 사망과 관련된 점에서 흔쾌히 승낙을 했다. 자료를 검토하다 매우 놀랐다. 아이의 사망원인은 머릿속 출혈 중 경막하 출혈이었다. 많이 겪은 일이다. 그런데 아이의 머리에는 두 부위에 경막하 출혈이 있었다.



☞ 실제 아이의 대뇌 CT를 보면 왼쪽 대뇌에 두 개의 화살표가 시기가 다른 경막하출혈을 보여주고 있다.

이 사건은 2013년도 지방 대도시의 한 대학병원에서 시작되었다.

27개월 여자 아이가 대학병원 응급실에 실려 왔다. 여자아이는 태어나서 얼마 안 되어

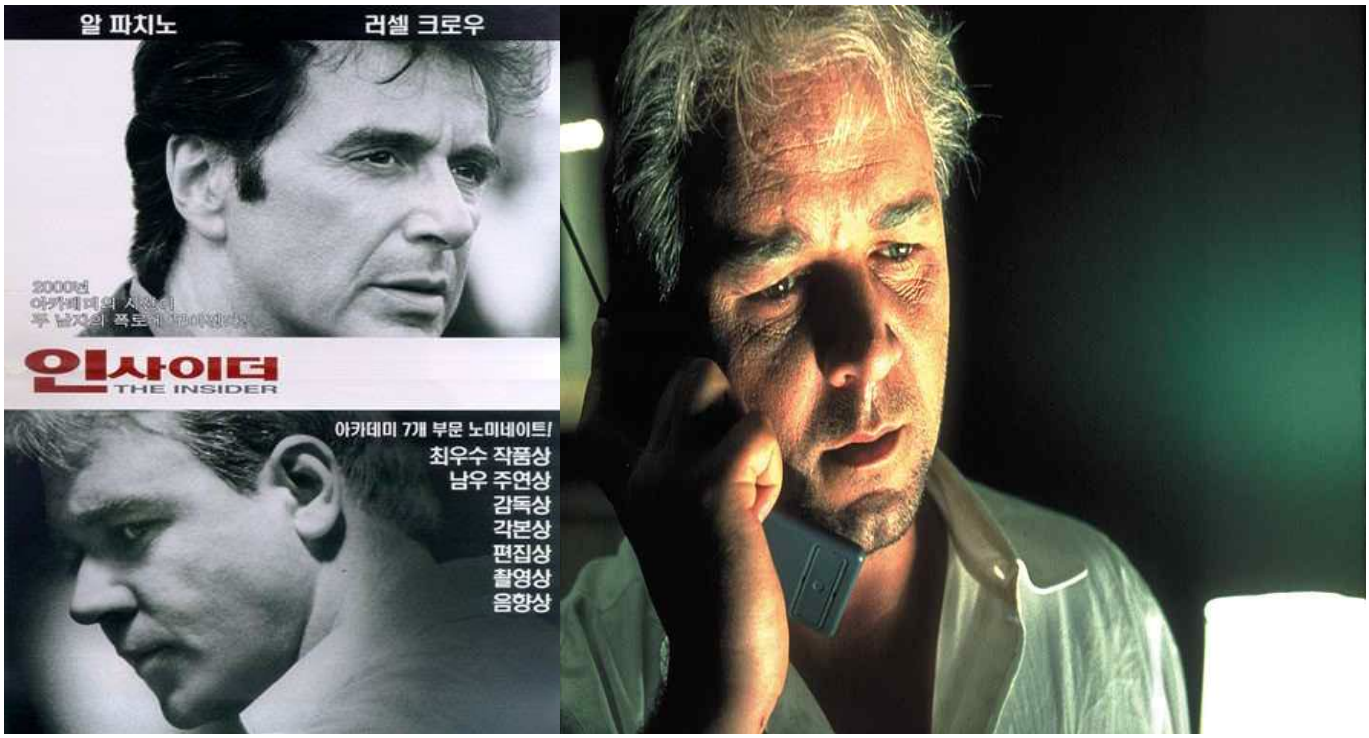
고모가 맡아 키웠다. 부모의 불화로 인해 갑자기 양육할 사람이 없어진 천사 같은 아이를 고모는 정성스레 보살폈다. 그러나 16개월이 지난 어느날 아이 엄마가 찾아와 자신이 직접 기르겠다고 한 후에 고모는 아이의 얼굴을 보지 못하였다. 아이는 병원에 치료를 받다 사망하였다. 의사는 사망진단서에 외인사로 기재하였다. 그러나 아이의 엄마는 죽은 아이의 시신을 데리고 퇴원했다. 아이의 엄마는 사망진단서를 전문적으로 써주는 의사에게 부탁하여 병사로 엉터리 시체검안서를 발급받았다. 아이는 화장(火葬)되어 한줌의 재로 세상에서 사라졌다. 아이의 육신은 사라졌지만 아이의 고모가 나섰다. 건강하고 밝았던 아이가 허망하게 죽었다는 것을 받아 들일 수 없어 게시판에 문제를 제기한 것이다.

아이의 영상 검사에서 발견된 뇌의 두 부위에 경막하 출혈은 아이의 나이로 보아서 참으로 이상한 것이었다. 서로 발생 시기가 달랐다. 급성뇌출혈과 시기가 좀 더 오래된 만성뇌출혈이 같이 있었다. 즉 시기를 두고 한 아이가 두 번 머리를 다친 것이다. 아이는 발육 상태가 좋지 않았다. 27개월된 아이의 신장이 1미터가 되지 않았다. 방송에서 인터뷰를 하였다. 경찰은 다시 수사를 시작했고 재판까지 일사천리로 진행되었다. 친모에게 4년의 실형, 같이 살던 동거인에게 10월의 징역이 선고되었다. 그리고 시신을 직접 검사하고 진단서를 발급한 의사에게는 허위진단서 작성에 책임을 물어 징역 1년 6월에 집행유예 2년이 선고되었다. 당연한 결과였다. 그러나 최근 그 사건이 일어난 지방도시를 방문해서 뜻밖의 이야기를 들었다. 그 의사가 지금도 여전히 같은 일을 하고 있다고 한다.

『영화로 본 수사관 일기』 ⑮

<인사이더>
- 우리의 정제된 언어로 수사의 지도(地圖)를 그리다

서울남부지검 수사관 강현식



기업 내부에서 일어나는 범죄에 대해서 가장 잘 알고 있는 사람은 바로 그 기업에 몸담고 있고, 그 안에서 범죄가 일어날 수 있도록 조력하거나 또는 가장 가까이에서 지켜본 내.부.자.일 것입니다. 그래서, 언론으로 접하게 되는 대형 기업범죄 수사의 단초는 이들 내부자를 통해서 제보된 첩보에서 비롯되기도 합니다.

보통의 경우 내부자 제보는 기업의 은밀한 불법정보를 공유한 자들의 충성도가 어떤 요인에 의하여 급속도로 냉각되거나 혹은 소속 업체의 부당한 처우로 인하여 점차 희석되는 경우 나타나는 게 일반적입니다. 하지만, 이런 내부자 제보는 약이 되기도 하지만, 때로는 검사나 수사관의 눈과 귀를 흐리는 독이 되기도 합니다.

내부자의 진술로 그려진 지도만 따라가다보면 막히는 지점마다 내부자의 진술을 빌어 움직여야 하기 때문인데, 애초부터 내부자에 의해 개시된 수사이다보니 중간쯤 가다보면 그들의 진술을 차단한 채 수사팀의 힘으로만 그 지도를 해석하기가 여간 어렵지 않기 때문이지요. 그래서인지, '제보자를 믿지 마라'는 잠언과도 같은 이 말을 잊은 채 내부자가 일러주는대로 따라갔다가 수사가 엉망이 되어버리는 과오를 범하기 쉽습니다.

영화 <인사이더>는 미국의 유명한 담배 제조회사에서 부사장으로 일하던 제프리 와이갠드 박사(러셀 크로우 분)가 '의사소통 능력 미달'이라는 뜻하지 않은 해고를 당하면서 시작합니다. 방송 시사프로그램 PD인 로웰 버그만(알파치노 분)은 익명의 제보자로부터 흡연자가 담배를 피울 경우의 화재 위험도에 관한 논문 한 편을 입수하게 되는데, 전문용어가 가득한 논문의 해석을 의뢰하기 위해 와이갠드 박사를 소개받게 되고, 이 과정에서 와이갠드 박사의 해고 사실을 전해 듣게 됩니다. 와이갠드 박사가 일하던 담배 제조회사에서 담배 판매율을 촉진시키기 위해 인체에 치명적인 암모니아 화합물을 담배에 넣는 것을 와이갠드 박사가 저지하려다 회사의 눈 밖에 나게 된 것. 결국, 버그만은 와이갠드 박사의 해고 사실에는 회사의 보이지 않는 압력이 있었다는 것을 의심하게 되고, 이를 조금씩 파헤쳐나가기 시작합니다.

우리는 위에서 언급한 줄거리만 들어도 무려 19년 전인 2000년경에 개봉한 영화이지만 지금과 별반 다르지 않은 상황 설정에 놀라게 됩니다. "내부자가 부당한 처우를 받았다→제3자에 의해 부당처우 사실이 밝혀진다"는 식의 사건전개는 내부자였던 인물이 자신의 문제를 직접 드러낼 경우 그 위험도가 크다는 상식이 자리잡고 있기 때문입니다. 영화에서도 회사의 압력에 두려워하며 침묵을 강요당하는 내부자가 다시 세상 밖으로 나올 수 있었던 것은 어느 한 저널리스트의 끈질긴 집념 때문이었으니까요.

하지만, 검사나 수사관은 내부자의 입보다 진실이 무엇인지를 판단할 수 있어야 하기에 다시 세상 밖으로 나온 내부자를 객관적으로 바라보아야 합니다. 그가 말하는 것이 진실한 것인지, 만일 진실한 것이라면 그 다음은 어떻게 나아가야 하는지를, 우리가 정제한 언어로 수사의 지도를 그려나가는 것. 그게 쉽지 않더라도 말이죠.

과학수사 대학(원)생 아이디어 공모전 입상작 소개 ⑥

- 우수상 성균관대학교 양성호 외 2명 -

과학수사기획관실 수사관 김희정

대검찰청 과학수사부에서는 2018. 10. 31. 개관 10주년을 기념하여 한국연구재단과 공동 주관으로 『4차산업혁명 시대의 과학수사 대학(원)생 아이디어 공모전』을 진행하였습니다.

공모작 총 60건 중 입상작 8건은 아래와 같습니다.

훈격	공모분야	대학명	제출자	작품명
대상	법과학분석	상명대학교	서건하외 1	영상촬영물에서의 생리 신호 모니터링 및 얼굴 표정 특징 기반 인공지능 심리분석 애플리케이션
최우수상	법과학분석	광주과학기술원	석영웅	범죄현장에서 미량의 시료로부터 신원 감별이 가능한 신속 DNA 분석용 휴대용 페이퍼 칩 시스템
최우수상	디지털수사	고려대	윤여경외 1	Cloud 기반의 WebOS 모바일 기기 압수 및 분석 방안
우수상	디지털수사	고려대	한승현	빅데이터 기반 유사범죄 해결방안에 대한 경우의 수 제시 및 추론
우수상	법과학분석	경북대	최다솜외 1	GAN 알고리즘을 적용한 쪽(조각) 지문 복구
우수상	사이버수사	성균관대	양성호외 2	가상화폐 익명성 추적을 위한 빅데이터 기반 이상거래탐지시스템 구축방안
우수상	기타	중앙대	이은지외 2	가상 범죄현장의 인공지능 범죄자 아바타
우수상	법과학분석	동아대	유홍연외 2	자연어처리를 이용한 담화 분석 기반의 과학수사 보조 시스템

이번호에는 우수상 수상작을 소개합니다.

○ 제출자 : 성균관대학교 양성호 외 2

○ 제목 : 가상화폐 익명성 추적을 위한 빅데이터 기반 이상거래시스템 구축방안

공모전 제안서

『4차 산업혁명 시대의 과학수사 대학(원)생 아이디어 공모전』
아 이 디 어 개 요

분 야	□ 법과학분석 □ 디지털수사 ■ 사이버수사 □ 기타 과학수사 관련 자유주제
제안명	가상화폐 익명성 추적을 위한 빅데이터 기반 이상거래탐지시스템 구축방안
제안 배경	현재 가상화폐의 국내 시장은 일평균 거래량이 1조에 달한다. 가상화폐가 가지는 익명성을 이용하여 범죄수익금 취득, 편법 증여 등의 탈세, 불법 해외송금으로 범죄에 악용하는 경우가 점차 증가하고 있다. 하지만 국내에 뚜렷하게 마련된 방법이 존재하지 않는다. 가상화폐를 범죄에 악용하는 지갑 주소를 사전에 미리 인지하여 차단하고 범행을 시도한 정황을 추적하는 시스템 모델을 제안하고자 한다.
주요 내용	아이디어의 핵심 기술은 전자금융 서비스에서 사용되는 FDS시스템(Fraud Detection System)을 빅데이터를 기반으로 가상화폐 거래의 이상 패턴을 학습하고 이상 거래 탐지에 접목시킨다는 점이다. 전형적인 이상 거래 행동은 같은 블럭안에 트랜젝션이 군집하는 경우, 특정 지갑주소에서 특정 시간단위로 코인이 이동하는 경우, A지갑 주소에서 여러 명에게 흩어진 가상화폐가 모여서 B지갑 주소에게 전달되는 등 다양한 패턴이 존재한다. 가상화폐가 거래될 때의 정보를 수집하여 DB에 저장한 뒤 빅데이터 기반 이상징후탐지시스템에 전송하여 위의 거래 패턴 양상을 가지는 주소를 탐지한다. 탐지된 이상거래를 수행한 지갑 주소를 모니터링하거나 거래를 정지하여 범죄자에 대한 추적 및 수사에 사용할 수 있다.
기대 효과 (요약)	현재 가상화폐를 이용한 범죄 자금 유통 및 세탁, 탈세 등을 시도하여도 이를 누가 했는지 특정할 수 있는 수사 방법이 특정되지 않은 상황이다. 이런 경우 범죄를 실행에 옮겨도 수사망을 피해 빠져나갈 수 있는 것 자체가 범죄 실행의 장벽을 낮추는 부정적인 영향을 줄 수 있다. 만약 가상화폐의 이상거래를 사전에 탐지할 수 있고, 탐지된 지갑 주소를 가지고 거래 내역, 가상화폐의 이동 경로 등을 추적할 수 있다면 이는 범죄를 사전에 예방하는 효과와 신속한 범인 검거에 도움이 될 것이다.

『4차 산업혁명 시대의 과학수사 대학(원)생 아이디어 공모전』

아 이 디 어 제 안 서

1. 개 요

2009년에 처음 등장한 비트코인을 시작으로 일반 화폐와 같은 통화가치를 가진 가상화폐들이 대거 등장하고 있다. 현재 가상화폐의 국내 시장은 1일 거래 금액만 1조 원에 가까운 거대한 자금이 몰려 있고 대기업들의 투자로 더욱 발전할 것으로 예상된다.
거대한 자본시장이 형성되면서 최근에는 가상화폐와 관련된 범죄가 눈에 띄게 증가하고 있다. 범죄에 악용되는 대표적인 이유는 **가상화폐가 가지는 익명성에 있다.** 가상화폐는 중앙 통제 시스템이 아닌 P2P 네트워크를 통해 익명성이 보장된 상황에서 쉽게 개인 간에 거래가 가능하다.
즉 불법적으로 자금을 유통할 때 일반 화폐보다 가상화폐를 사용하면 시간적 공간적으로 훨씬 수월하고 기존 금융제도 규제가 적용되지 않는다. 이미 가상화폐는 익명거래를 기반으로 범죄수익금 취득과 편법 증여 등의 탈세, 그리고 불법 해외송금 등의 수단으로 악용되고 있으며 수사기관에서는 이를 추적하기가 어렵다.

총계	탈취형(27.3%)		사기형(42.3%)		자금세탁형(30.4%)	
	해킹	컴퓨터사용사기	투자모집사기	유사수신	불법거래수단	피해금요구
714	86	109	168	134	82	135

▲ 2015년~2017년 6월 가상화폐 관련 주요 범죄현황[자료=경찰청]

표1.

기술의 발전은 새로운 사이버범죄 유형을 만들어 냈고, 범죄자의 검거는 갈수록 어려워지며 범행 사례는 더욱 급격히 늘어날 것으로 충분히 예상할 수 있다. 이는 전통적인 수사 기법이 아닌 사이버범죄의 특징을 고려하여 새로운 수사기법이 필요함을 의미한다.

본 제안서에서는 익명성을 가진 가상화폐의 거래를 추적하고 이를 데이터화하여 거래자가 이상 거래를 시도할 때 탐지하는 시스템을 논해보고자 한다. 먼저 가상화폐의 거래의 특성을 파악하고, 범죄에 악용되는 경우 어떤 거래 유형을 띄는지 확인한다.
이상거래가 발생할 경우 해당 지갑 주소의 거래를 중단 또는 추적하여 범죄 예방이나 범인 검거에 쓰일 수 있도록 하는 시스템 아키텍처를 제안하고자 한다.

2. 관련기술 현황 및 실행 전략 방안

2.1 관련 기술 현황

가상화폐 익명성 추적을 위한 빅데이터 기반 이상징후탐지시스템 구축 방안의 핵심 기반 기술은 **1) 가상화폐의 익명성을 악용하는 믹싱(Mixing)패턴을 추적하는 기술과 2) 빅데이터를 기반으로 이상거래를 탐지하는 FDS시스템기술 2가지**를 꼽을 수 있다.

첫째로 가상화폐의 익명성은 거래의 특성에서 나온다. 가상화폐를 거래하기 위해서는 관련 사이트에서 인터넷상의 지갑(Wallet)을 만들어야 한다. 이 지갑을 만들기 위해서는 거래소를 통하는 방법은 본인인증을 거치지만 개인이 직접 생성하는 방법은 본인인증을 거치지 않는다.

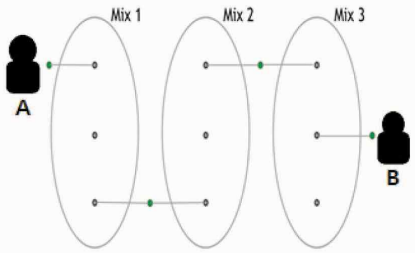


그림1. 믹싱기술을 이용한 가상화폐 이동경로

만약 A의 지갑에서 B의 지갑까지 가상화폐를 전달하려고 한다. 이때 A가 MIX1,2,3을 통해서 B에게 비트코인을 전달하는 믹싱 과정을 거친다면 가상화폐가 누구에게 갔는지 식별하는 것은 매우 어렵다. 그 이유는 거래 과정에서 지갑의 주소만 이전될 뿐 거래의 주체가 누구인지는 필요 없기 때문이다.

둘째로 이상거래 탐지시스템(Fraud Detection System)은 전자금융거래 시 불법 이체, 카드 거래 시 부정 사용 등 의심거래를 실시간으로 분석해 탐지하기 위한 시스템으로 2013년 7월 '금융전산 보안강화 종합대책'에서 카드사 이외에 은행, 증권 등으로 부정 사용 방지 모니터링 시스템을 자리 잡았다.

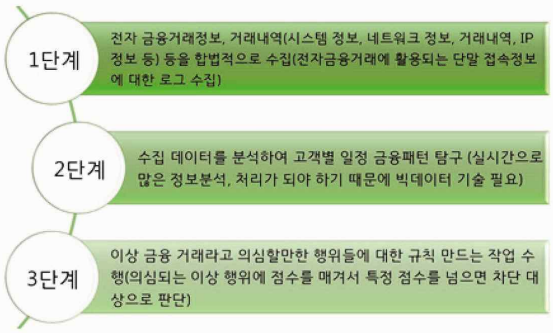


그림2. FDS 작동방식

즉 FDS 시스템은 일정한 패턴에서 벗어났을 때 경고하는 시스템이다. FDS시스템은 금융업종에 따라 도입 내용 및 성격이 다르다. FDS 시스템은 최근 이슈가 되고 있는 빅데이터 분석을 기반으로 하고 있다. 정형화된 여러 가지 패턴을 근거로 하는 룰 방식과 정상 패턴을 유형화한 뒤, 부정 사용 패턴과의 상관관계를 계량화해 점수를 매기는 스코어 방식을 접목해 개발된 시스템으로 의심스러운 금융거래를 사전에 탐지하고 대응하는 것에 사용되고 있다. 가상화폐 익명성 추적을 위한 빅데이터 기반 이상거래 탐지시스템 구축은 이렇게 믹싱 추적 기술과 FDS 시스템을 기반으로 한다.

2.2 이상징후 패턴 분석 및 실행 전략 방안

빅데이터 기반 이상징후탐지시스템은 다수의 사용자가 이용하는 소수의 주소에서 소수의 주소로 가상화폐가 이동하는 패턴의 지갑은 정상적인 거래로 인식 할 것이다.

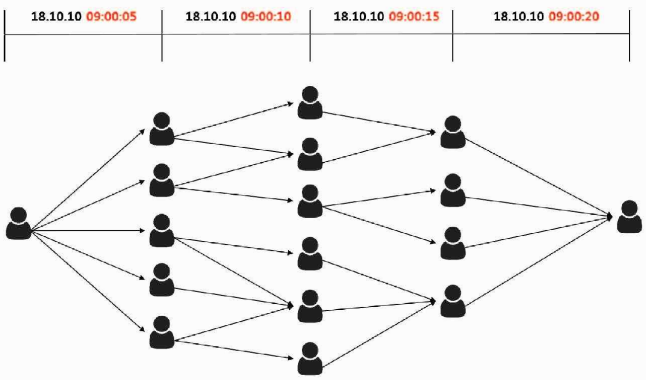


그림3. 특정한 지갑 주소에서 특정한 시간 단위로 가상화폐가 지속적으로 이동하는 이상 패턴

이상징후를 가지는 패턴은 다양한게 존재한다. 그 중 1) 소수의 주소에서 나온 자금이 다수를 거쳐 다시 소수의 주소로 들어가는 경우 2) 트랜젝션이 같은 블럭안에 군집하는 경우 3) 특정한 지갑 주소에서 특정한 시간 단위로 가상화폐가 지속적으로 이동하는 경우 총 3가지를 이상거래로 분류할 수 있다.
하지만 위와 같이 정상 거래 패턴이 아니라 가상화폐가 범죄에 이용될 수 있는 경우의 다양한 패턴을 이상 방식으로 학습하여 탐지하는 것을 목표로 한다. 빅데이터 기반 이상징후탐지시스템을 구축하고 해당 계좌를 추적하는 시스템을 구축한다면 현재 뚜렷한 대책이 없는 가상화폐 수사에 활용할 수 있을 것이라 예상한다.
3장에서는 정상적인 거래를 학습한 시스템이 어떤 과정으로 이상 패턴을 탐지하는지 동작 과정을 설명한다.

3. 주요 내용

3.1 빅데이터 기반 이상거래탐지시스템 동작 방식

빅데이터를 기반으로 한 이상거래 탐지 시스템의 동작방식은 크게 3가지로 나눠 설명 수 있다. 첫번째로 거래 기록을 수집한다.

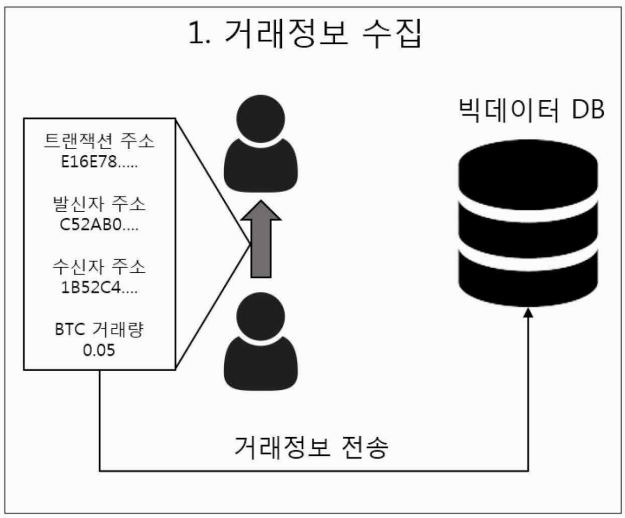


그림2. 가상화폐 거래시 발생하는 정보를 수집하여 DB에 저장

가상화폐 거래가 일어나면 해당 거래 장부를 실시간으로 빅데이터 DB에 저장시킨다. 거래 장부에는 트랜잭션 주소, 발신자의 지갑 주소, 수신자의 지갑 주소, 암호화폐 거래량, 출금 시간, 입금 시간 등이 기록되어 있다.

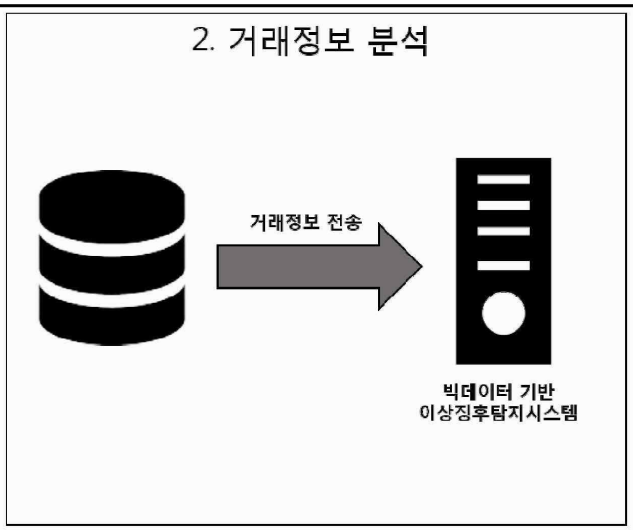


그림3. DB 수집정보를 빅데이터 기반 이상징후탐지시스템으로 전송 및 이상거래탐지 분석

빅데이터 DB는 수집된 거래 정보를 빅데이터 기반 이상징후탐지시스템으로 전송한다. 이상징후탐지시스템에서는 DB로부터 전달받은 거래 정보들의 패턴을 분석해서 정상거래의 형태를 파악한다. 그리고 정상거래의 형태를 기반으로한 패턴 룰을 제작한다.

제작된 패턴 룰로 인해 이후 이상징후탐지시스템은 DB로부터 전달받은 거래 정보를 패턴 룰과 대조하여 거래 형태의 정상여부를 판단한다. 시스템과리자는 해당 시스템에 접속하여 패턴 룰, 실시간 거래 여부 등을 확인할 수 있다. 그리고 이상징후탐지시스템에 의해 제작된 패턴 룰을 관리자가 수정하거나 추가할 수 있다.

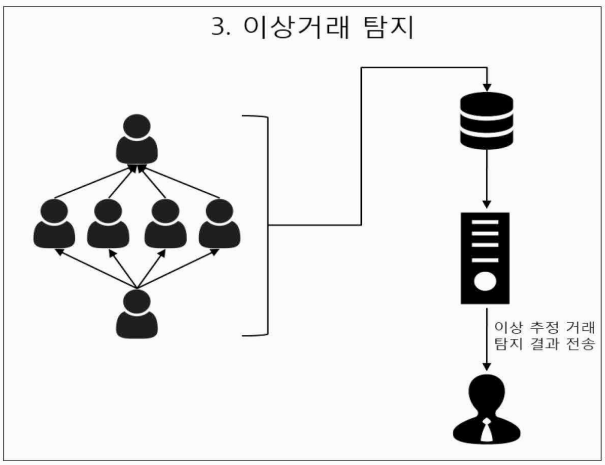


그림4. 이상거래가 탐지 발견시 해당 거래의 정보를 담당자에게 전송

DB로부터 거래 정보를 전송받는 이상징후탐지시스템은 가상화폐 믹싱 기법 등을 활용한 이상거래를 탐지 시 패턴 룰과 대조하여 기존의 거래와 차이점을 보이면 해당 거래 내용과 거래 형태 판단 여부를 관리자에게 알람, 문자 등을 전송한다. 관리자는 이상 추정 거래 탐지 결과를 전달받으면 이상징후탐지시스템으로 접속하여 해당 거래의 세부 정보를 파악하고 익명성 추적을 위한 거래자의 정보를 얻기 위해 거래를 중계한 가상화폐 거래소에 협조를 구한다.

3.2 가상화폐 추적기술

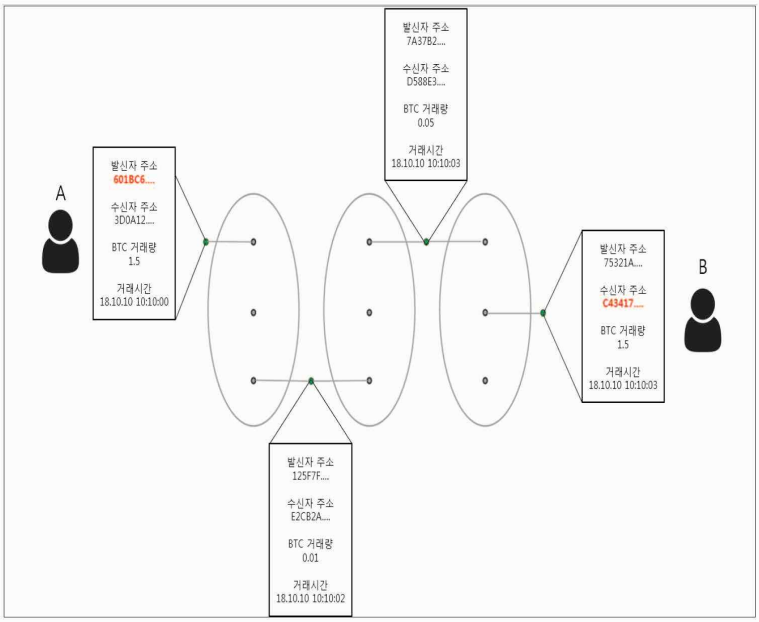


그림5. 이상거래가 탐지시 해당 거래의 정보를 담당자에게 전송

이상거래로 추정되는 케이스의 첫 거래 장부에 기록된 발신자의 지갑 주소와 가상화폐 거래량을 출발 기점으로 하여 케이스의 마지막 거래 장부에 기록된 수신자의 지갑주소와 가상화폐 거래량을 확인한다. 그리고 가상화폐 거래소로부터 발신자와 수신자의 지갑 주소를 보유한 사용자의 신원을 파악한다.

4. 아이디어의 가치

최근 들어 가상화폐는 큰 가치 상승과 다양한 범죄에 연관되어 미디어에 꾸준히 가상화폐들의 이름이 등장하면서 사회에 익숙해졌지만 가상화폐 기술의 등장은 채 10년이 되지 않았다. 가상화폐의 익명성 특징을 이용하는 범죄는 빠르게 늘어가고 있다.
위 3장에서 제시하는 가상화폐의 익명성을 추적하는 기술, 빅데이터 기반으로 이상거래 탐지시스템(FDS)을 구성하는 기반 기술은 각각의 분야에서 연구가 되고 있지만 **두 기술을 결합하여 이상거래를 추적여 범죄 수사에 활용할 수 있는 두드러지는 시스템은 존재하지 않는 것이 현실이다.**

현재는 가상화폐를 이용한 범죄 자금 유통 및 세탁, 탈세 등을 시도하여도 이를 누가 했는지 특정할 수 있는 수사 방법이 특정되지 않은 상황이다. 이런 경우 범죄를 실행에 옮겨도 수사망을 피해 빠져나갈 수 있는 것 자체가 범죄 실행의 장벽을 낮추는 부정적인 인식을 줄 수 있다.
만약 가상화폐의 이상거래를 사전에 탐지할 수 있고, 탐지된 지갑 주소를 가지고 해당 지갑의 거래 내역, 가상화폐의 이동 경로 등을 추적할 수 있다면 이는 범죄를 사전에 예방하는 효과와 신속한 범인 검거에 도움이 될 것이다.

5. 기대효과

오늘날 우리는 가상화폐 해킹 범죄로 인하여 거래소가 파산신청을 하고, 고등학생이 장난스럽게 발표한 비트코인 하드포크 계획으로 전 세계의 가상화폐 시장이 출렁거리는가 하면, 가상화폐를 구실로 하는 수만명이 피해를 입은 사기와 유사수신행위에 의한 피해자가 실제 발생하는 현실을 경험하고 있다. 대한민국은 아직 가상화폐가 법적인 제제 장치, 규제 수단이 존재하지 않는다. 하지만 기술의 발전은 막을 수 없고 멀지 않은 미래에 가상화폐는 많은 사람이 쉽고 다양하게 사용할 수 있다.

이런 미래에 앞서 가상화폐의 특징을 이용한 범죄에 대한 예방책을 강구해 놓지 않으면 현재까지 일어난 사건들보다 더 규모가 큰 가상화폐 관련 범죄가 일어나고 많은 이들이 피해볼 수 있는 상황이 벌어질 수 있다.
본 제안서에서 제시한 가상화폐 익명성 추적을 위한 빅데이터 기반 이상거래 탐지시스템이 개발되어 관련 업무가 체계적으로 이뤄지면 앞서 설명한 가상화폐 관련 범죄를 예방하는데 큰 도움이 될 것이다.

YTN science

[사이언스 CSI] 디지털 기기에서 결정적 증거를 찾는...멀티미디어분석

2019-05-27

■ 김동민 / 대검찰청 멀티미디어 분석실장

[앵커]

CCTV나 차량 블랙박스 같은 멀티미디어 기기들이 범죄 수사에서는 결정적인 증거가 되는데요.

그래서 이 속에 숨겨진 흔적들을 과학적으로 분석하고 복원하는 것이 정말 중요한데요.

오늘 <사이언스 CSI>에서는 '멀티미디어 분석'에 대해 알아보겠습니다. 대검찰청 멀티미디어 분석실 김동민 실장과 함께합니다. 안녕하세요?

대검찰청 멀티미디어 분석실, 모르시는 분들을 위해서 어떤 일을 하는 곳인지 설명 부탁드리겠습니다.

[인터뷰]

네, 저희 대검찰청 멀티미디어 분석실에서는 범죄 수사와 관련된 사진이나 영상, 음성 등 멀티미디어 파일을 과학적인 방법을 통해 분석하고 복원하는 업무를 하고 있는데요.

최근 범죄 수사에 있어 아주 중요한 역할을 담당하고 있습니다. 멀티미디어 분석실은 영상분석, 음성분석, 멀티미디어 복원으로 각 영역을 세부적으로 나누어 전문적으로 분석을 수행하고 있습니다.

[앵커]

방금 영상과 음성분석, 멀티미디어 복원까지 세 분야로 나눠서 업무를 담당하고 계신다고 하셨는데요.

우선 영상분석에 대해 이야기 나눠보겠습니다. 저희가 일단 일반인이니까 딱 들었을 때는 조작되거나 편집된 영상을 분석하는 것 같은데요. 구체적으로 어떤 업무를 담당하시나요?

[인터뷰]

네, 맞습니다. 그것 역시 영상분석의 일종인데요. 하지만 그 외에도 더욱 다양한 업무를 수행하고 있습니다.

영상분석은 크게 다섯 가지 주요 업무로 나눌 수 있는데요. 우선 왜곡되거나 화질이 좋지 않은 영상이나 이미지 자료가 있다면 다양한 방법으로 열화 성분을 제거하고 명료도를 향상해 원본 대비 선명한 자료를 획득하는 화질 개선 업무가 있습니다.

지금 화면에 나가는 영상을 보시면 CCTV 몇 대가 겹쳐서 어지럽게 보이는 것을 볼 수 있는데요.

이런 영상도 다양한 영상처리를 통해서 화질을 개선했고, 디멀티플렉싱을 통하여 CCTV 영상을 하나씩 분류할 수 있었습니다.

두 번째로는 다양한 영상처리를 통하여 자동차 번호나 특정 문자, 기호, 피사체의 행위 등 분석하는 업무를 하고 있는데요.

예를 들어 빨리 달리는 차의 경우 번호판을 식별하기 어려운데요. 이 역시 영상물의 개선과 분석을 통해 숫자나 문자를 판독합니다.

[앵커]

번호판의 문자를요…. 이런 영상처리를 통해서 다양한 범죄 사건을 해결할 수 있을 것 같아요. 또 어떤 업무를 담당하시나요?

[인터뷰]

세 번째로는 영상 또는 이미지에 촬영된 범인과 의심되는 용의자를 비교하고 분석하여 같은 사람인지 아닌지를 분석하는 '동일인 분석 업무'가 있고요.

네 번째로는 영상 또는 이미지상에서 촬영된 특정 물체나 인물의 신장을 분석하는 '길이 계측 업무'가 있습니다.

특히, 길이 계측 업무의 경우 X, Y, Z축의 정보를 활용해 3차원적으로 분석을 수행하고 있는데요. 그러면 물체의 크기나 인물의 신장을 좀 더 정확하게 계측할 수 있습니다.

마지막으로는 CCTV, 차량 블랙박스, 스마트폰 등 영상이나 사진이 삭제되었는지, 또는 조작이나 편집되었는지 분석하는 업무를 수행하고 있습니다.

지금 나가는 자료화면을 보시면 피해자의 진술로는 피의자가 라이터로 불을 냈다고 했지만, 이 라이터는 합성된 사진인 걸로 밝혀졌습니다.

피해자가 거짓말을 한 거죠. 이외에도 사진학적, 영상학적 감정이 필요한 부분을 적극적으로 지원하고 있습니다.

[앵커]

그러니까 영상 분석뿐만 아니라 사진까지도 분석하시는군요.

[인터뷰]

네, 영상에 사진도 다 포함되어 있습니다.

[앵커]

그렇군요. 다음으로 음성 분석에 대해 이야기 나눠볼 텐데, 저는 음성 분석을 들었을 때 실제 범인의 목소리가 담긴 영화였죠, '그 놈 목소리'가 떠오르기도 하더라고요.

그런데 사람의 목소리는 개개인의 특성이 담겨 있어서 또 다른 지문이라고 말하기도 하던데, 음석 분석이란 정확히 어떤 건가요?

[인터뷰]

네, 음성 분석은 납치나 협박, 전화사기 등 음성이 이용된 범죄에서 범인의 음성과 용의자로부터 채취된 음성을 성문분석이나 청취 분석, 음향분석 등으로 비교 분석하여 동일인 여부를 식별하는데요.

두 가지 음성을 한 번 비교해서 들려드리겠습니다.

"안녕하세요."

"안녕하세요."

[앵커]

아, 끝난 건가요?

[인터뷰]

네, 두 음성을 들어보시면 어떻습니까? 같은 사람으로 느껴지나요?

[앵커]

조금 다른 것 같기도 하고요.

[인터뷰]

지금 들으신 음성은 같은 사람은 아니고, 자매의 목소리 입니다. 처음 들었던 '안녕하세요' 음성이 첫 번째 사진으로 음파가 나타난 것이고요.

두 번째 음성이 두 번째 사진인데요. 성문을 비교하는 음파를 보면 간격이나 파동에 차이가 있는 걸 볼 수 있습니다.

[앵커]

네, 약간 달라요.

[인터뷰]

이런 부분을 통해서 동일인 여부를 감정하고 있습니다. 두 번째로는 보이스펜이나 녹음테이프, CD 등에 저장된 녹음이 원본인지 의도적으로 조작이나 편집되었는지 감정하는 '위변조 분석 업무'가 있고요.

녹음 품질이 불량한 자료에서 잡음을 제거하고 음성을 증폭하는 등 음성의 명료도를 향상하는 음질 개선 업무도 있습니다.

이 부분도 음성을 한 번 들어보고 가겠습니다.

[앵커]

잘 안 들리네요. 잡음이 많아요. 같은 음성인데, 확실히 명료하게 들리네요.

[인터뷰]

네, 이외에도 보이스피싱이나 유괴, 협박 사건 같은 경우는 신원을 알 수 없잖아요. 신원미상인 음성의 언어적 특징을 분석하여 출신 지역이나 특이한 언어습관, 연령대 등 신원을 추정하는 화자 프로파일링 업무를 수행하고 있습니다.

[앵커]

정말 음성만으로도 어떤 사람인지 파악하고, 범죄 분석에 활용될 수 있을 것 같다는 게 신기하네요.

그럼 마지막으로 멀티미디어 복원에 관해서 궁금한 게 많은데, 어떤 건지 설명해 주시죠.

[인터뷰]

멀티미디어복원은 CCTV, 차량 블랙박스 등의 디지털 저장 매체에서 삭제된 영상 또는 음성 데이터를 복원하여 멀티미디어 파일이 재생할 수 있도록 지원하고 있는데요.

지금 영상에 나오는 것처럼 특정 기기에 최적화된 복원프로그램을 자체 개발하여 영상을 복원하고 있습니다.

또한, 이외에도 손상된 멀티미디어 파일에 대한 복원과 화면이나 소리가 나오지 않는 경우 정상재생이 가능하도록 하는 업무를 지원하고 있습니다.

이외에도 멀티미디어 파일의 복원 및 재생과 관련하여 여러 가지 분석 사항들의 요청이 있을 수 있잖아요. 그럴 경우에 적극 수사 지원을 하고 있습니다.

[앵커]

말씀하신, CCTV나 차량 블랙박스는 요새 어떤 범죄 사건에 직결되고 각종 사고의 원인을 밝혀내는데 필수적인 자료잖아요.

멀티미디어 분석을 통해 다양한 사건을 해결하셨을 것 같은데요. 가장 기억에 남는 사건이 있다면 몇 가지만 소개 부탁합니다.

[인터뷰]

굉장히 많은 사건이 있는데요. 우선 두 가지 사건이 기억에 남습니다. 첫 번째 사건으로는 피의자가 모 대학교의 경찰행정학과에 재학 중인 경찰관 지망생이었는데요.

그런데 인근 CCTV나 차량 블랙박스에 촬영된 범인과 흡사하다는 이유로 강도상해 및 강제추행 혐의로 구속 송치된 사건입니다.

영상 감정을 통한 동일인 분석을 하여 범인과 다른 인물이라고 밝혀냈습니다.

[앵커]

다행이네요.

[인터뷰]

경찰관이 되고 싶은 꿈을 품고 성실히 학교생활을 하던 대학생의 억울한 누명을 벗겨줌으로써 검찰 본연의 기능인 국민의 인권 보호에 기여했다고 생각합니다.

[앵커]

보람을 느끼셨겠어요. 또 어떤 일이 있었나요?

[인터뷰]

두 번째는 최근 사건인데요, 2017년 필리핀 국가수사국(NBI)으로부터 의뢰를 받은 사건이 있습니다.

필리핀 범죄조직원에 의해서 50대 한국인 사업가가 피살당한 사건이었습니다. 필리핀 국가수사국에서 청부살인사건 수사와 관련하여 영상분석 지원요청이 왔습니다.

저희가 영상분석을 통하여 용의차량의 차종과 차량 번호를 밝혀내고 범인들의 신장을 계측하여 수사 지원해준 사례가 있었습니다.

이때 필리핀 국가수사국으로부터 감사하다는 메일을 받은 것이 가장 기억에 남습니다.

[앵커]

두 번째 사건 저도 기억이 나요, 이렇게 해결됐군요.

아무래도 피해자가 한국인이기도 하고, 이런 기술력이 더 좋기 때문에 요청하지 않았나 싶은데요.

[인터뷰]

아무래도 국제 협력을 통해서 서로 다양한 수사지원을 하면 굉장히 이쪽 분야에 도움이 될 수 있다고 생각하고 있습니다.

[앵커]

그렇군요. 자, 그럼 멀티미디어분석실에 있으면서 가장 보람된 일은 어떤 일이고, 앞으로의 계획은 무엇인지 말씀 부탁드리겠습니다.

[인터뷰]

아시다시피 최근, CCTV나 차량 블랙박스, 스마트폰 등 다양한 멀티미디어 기기의 발전과 보급이 급증함에 따라 사건 현장에서 이와 관련한 증거 자료를 수집하고 수사에 적극적으로 활용하는 추세인데요.

그래서 멀티미디어분석실의 역할이 나날이 중요해지고 있다고 생각합니다. 멀티미디어 분석을 통해 실체적 진실을 보다 정확하게 밝혀냄으로써 억울한 일을 당하는 사람이 없도록 피해자와 피의자의 인권 보호와 수사에 조금이라도 도움을 줄 수 있다는 점에서 가장 보람을 느끼고 있습니다.

다양한 멀티미디어기기의 급증과 범죄의 첨단화, 지능화 추세에 선제 대응을 하기 위하여 분석관(감정관)의 역할이 매우 중요한데요.

이를 위하여, 최신 기술이나 연구에 대한 지속적인 동향 분석이 필요하겠고요. 또한, 4차 산업혁명이라고 해서 인공지능기술(AI)을 접목한 첨단 분석기법에 대한 연구와 개발, 분야별 전문가 육성과 교육을 통해 '뛰는 범죄자 위에 나는 분석관'이 되기 위해 과학수사 역량 강화에 최선의 노력을 다하겠습니다.

[앵커]

국내 과학 수사가 이미 세계적인 수준이라고 하는데요. 한 단계 더 도약해서 사건의 진실을 밝히는 데 힘이 되어 주시길 바랍니다.

지금까지 대검찰청 멀티미디어분석실 김동민 실장과 함께했습니다. 오늘 말씀 고맙습니다.

세계 최고의 과학수사