https://doi.org/10.33778/kcsa.2023.23.5.091

특허데이터를 활용한 자동차 사이버보안 강화방안 연구
- 특허분석을 통해 자동차 사이버보안 강화필요한 신규기술 탐색 및 보안요구사항 탐색 -

곽 동 한*, 권 헌 영**

요 약

최근 차량은 다양한 ICT 기술을 도입하고 활용하는 방향으로 변화하고 있다. 이에 따라 자동차에는 다수의 소프트웨어가 설치되었고, 그에 따라 해킹 등 사이버 보안 위협 문제가 발생되고 있다. 이 때문에 각국은 자동차 사이버보안 확보를 위한 법규정을 마련하고 있으며, 법규정 내 위협기술에 대해 리스크 완화방안 준비가 강제되고 있다. 다만 자동차 기술의 발전 속도에 비해 법규정의 제정은 상대적으로 느릴 수 밖에 없기에, 지속적으로 자동차 기술 발전 트렌드 파악을 통해 법규정을 개정할 필요가 있다. 본 연구에서는 최신 자동차 사이버보안 특허출원을 탐색 및 분석하여 신규로 자동차 사이버보안의 보완이 필요한 기술 분야를 탐색한다. 또한 신규 기술분야에 대해서는 위협기술, 보안요구사항을 특허분석을 통해 제시하고자 한다. 본 연구는 자동차 사이버보안이 강화될 필요가 있는 기술분야를 사전에 도출함으로써, 법규정 개정의 필요성에 대한 논리를 제공하고, 자동차 제조사로 하여금 발생 예상되는 위협기술을 사전에 준비할 수 있도록 하는데 기여하고자 한다.

A Study on Strengthening of Vehicle Cybersecurity based on Patent Data
- Searching New Technologies to be Strengthened in the Vehicle Cybersecurity and Security Requirements based on Patent Analysis-

Dong-Han Kwak*, Hun-Yeong Kwon**

ABSTRACT

Vehicles are changing in the direction of utilizing various ICT technologies. Accordingly a number of software ha s been installed in vehicles, resulting in cybersecurity threats such as hacking. So each country is preparing legal re gulations to secure vehicles cybersecurity. However, the enactment of legal regulations is bound to be relatively slo w compared to the speed of development of vehicles technology, so it is necessary to revise the legal regulations by continuously monitoring of vehicles technology development trends. In this study, we search and analyze the latest v ehicles cybersecurity patent applications to explore new technologies that require supplementation of vehicles cyberse curity. Threat technologies/security requirements for new technologies are presented through patent analysis

Key words : Vehicle, Cybersecurity, Patent, Electric Vehicle, BlockChain, UAV

접수일(2023년 05월 17일), 수정일(1차: 2023년 08월 19일), (2차: 2023년 09월 10일), 게재확정일(2023년 10월 16일)

* 고려대학교 정보보호대학원 석사수료 (주저자)
** 고려대학교 정보보호대학원 교수 (교신저자)

1. 서 론

최근 자동차는 센서를 통한 객체인식기술, 무선/이동 통신기술 등 다양한 ICT 기술을 도입·활용하는 방식으로 변화되고 있다. 자동차 기능의 향상과 운행의 효율 등을 확보할 수 있게 되었지만 하드웨어로만 구성되어 있던 자동차에 소프트웨어가 탑재되면서 동시에 해킹 등의 보안 위협 문제도 발생하게 되었다. 해킹 등의 보안 위협은 운전자, 동승자, 보행자 등의 생명에 직접적인 영향을 줄 수 있기 때문에 보안 위협의 예방이 필수적으로 요구된다. 이러한 이유로 각 국가에서는 자동차 사이버보안 확보를 위한 법규정을 마련하고 법규정 내 자동차 사이버보안과 관련된 기술을 제시하고 해당 기술에 대한 위협, 및 그 위협에 대한 대응방안을 강구하고 있다.

2020년 6월 UNECE 자율주행, 커넥티드 분과 GRVA(Working Party on Automated/Autonomous and Connected Vehicles)의 CS/OTA Task Force(UN Task Force on Cyber Security and Over-The-Air issues)의 자동차 사이버보안 법규정(UN Regulation No.155, Cybersecurity Regulation, 이하 “UNR. 155”)[1]이 UN 총회에서 채택되었다. 동 법규정[1]은 6개월 간 협정국가에게 회람된 후, 최종 확정 및 발효되었다.

UNR.155 법규정[1]의 Annex5(이하 “Annex5”)에서는 자동차 사이버보안 위협과 관련된 기술 및 완화방안을 규정하고 있다. 각 제조사는 자동차 사이버보안 형식승인을 받기 위해서는 CSMS의 프로세스가 Annex5의 위협 기술 및 완화방안에 대해 안전하다는 것을 증명해야 한다. 자동차 사이버보안 가이드라인[2] 등에 따르면, 동 Annex5에 제시되는 위협 기술 및 완화방안은 한국, 일본, 중국 등의 자동차 사이버보안 법규정 혹은 가이드라인에서, 그대로 내용을 인용하고 있다. 따라서 현 시점에 전 세계 주요 국가의 자동차 제조사가 대비하고 있는 자동차 사이버보안 위협기술로는 Annex5 위협 기술에 한정한다고 볼 수 있다. 자동차 사이버보안 위협에 대한 기술 내용로는, 차량 관련 백엔드 서버에 대한 기술, 통신 채널 관련 차량에 대한 기술, 업데이트 프로세스 관련 차량의 기술, 사이버공격을 가능하게 하는 의도하지 않은 인간의 행위와 관련된 차량에 대한 기술, 외부 연결 및 통신에 관한 차량에 대한 기술, 차량 데이터/코드에 대한 기술 등이 있다.

다만 마련된 법규정이 빠르게 발전하는 자동차 기술 속도로 인해 예측 못한 사이버보안 위협 문제를 제대로 반영하지 못할 가능성이 있다. 따라서 자동차 사이버보안 업계는 전방위적인 모니터링을 통해 새로운 기술에 의한 신규 보안위협 기술 발굴 및 완화방안 수립을 위해 노력해야 할 필요가 있으며, 해당 보안위협에 대해 법규정을 지속적으로 업데이트 개정할 필요가 있다.

한편 특허제도의 본질은 발명자 보호를 통해 산업발전을 도모하는 것이다. 제품을 개발하는 기업체 입장에서는 연구원들의 기술개발 결과물을 보호하여 제품에 내재된 아이디어에 대한 독점권을 확보함으로써 기업체의 이익을 증대하는 것이다. 이런 관점에서 보면 기업체에 특허권이 있다는 것은 제품을 개발하고 있다는 것으로 볼 수 있으며 근 시일 내에 제품이 시장에 공급되어 사용자가 이를 사용할 가능성이 있음을 예측할 수 있다.

본 연구에서 자동차 사이버보안 기술에 대한 특허출원이 자동차 연구개발의 산출물이라는 점을 이용하여, 연구개발에 따른 제품이 양산될 수 있음에도 아직 법규정 등에서 다루고 있지 않는, 즉 자동차 사이버보안 강화 및 보완이 필요한 신규 기술분야를 특허출원의 분석을 통해 도출하고, 더불어 특허출원의 분석을 통해 위협기술 및 보안요구사항을 제안하고자 한다.

2. 관련 연구

기존 자동차 사이버보안 위협기술 관련 연구를 중심으로 관련 연구들을 살펴보도록 한다.

과학기술정보통신부 외[3]에서는 자율주행차 보안모델(이하, “자율주행차 보안모델[3]”)을 공개하며, Annex5에 규정된 보안위협에 따라 보안요구사항을 도출하고, 이에 대한 완화방안을 제공하고 있다. 또한 자율주행자동차에서 제공될 수 있는 각종 서비스, 예컨대 셔틀 및 온-디맨드 서비스, 카쉐어링 서비스 등에 대한 보안위협, 보안요구사항 등을 제시하고 있다. 그리고 정임영[4]은 자율주행 자동

차 위험과 이에 대한 방어방안을 분석하였고, 특히 자율주행 자동차의 위험 중, 커넥티드 카 기능으로 인한 사이버 위협에 의한 위험과 자율주행 기능으로부터 비롯되는 위험에 초점을 맞추어 분석하였다. 또한 이슬기롬 외[5]은 Annex5에서 제시하는 7개 위협기술에 대해 공격 시나리오를 제안하고 있다. 즉 위 연구들의 경우에는 기존 Annex5에서 제시하고 있는 사이버위협만을 기반으로 요구사항 개선, 공격 시나리오 등을 제시하고 있다.

다만 송태진 외[6]의 경우에는 자율주행차 혹은 전기차, ITS 인프라, 전기 충전 인프라 등 모빌리티 환경을 구성하는 구성요소별 사이버 보안 연구 동향을 파악하고 해당 연구 동향 분석 결과를 바탕으로 자율협력주행 환경에서 전기자동차 주행시 발생되어질 다양한 보안 이슈에 대해 제시하고 있으나, 모빌리티 환경을 ACES(Automation, Connected, Electrification and Sharing)로 한정하여 보안 이슈를 도출하는 한계를 가지고 있다.

또한 자동차 사이버보안 특허출원을 이용한다는 점, 자동차 사이버보안 강화가 필요한 신규 기술분야를 도출한다는 점, 신규 기술분야에 대한 위협기술 및 보안요구사항을 특허출원 분석을 통해 도출한다는 점에 대해서는 관련 연구가 없는 것으로 조사되었다.

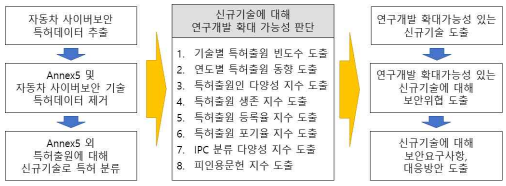
3. 자동차 사이버보안 특허데이터 분석

3.1 연구 방법

본 연구에서는 자동차 사이버보안 특허데이터를 통해 전세계 발명자, 자동차 회사, 자동차 부품 회사들의 관심사를 도출하여 추가로 제품 연구개발 가능성 및 제품 시장 사용 가능성을 예측하고, 이를 기초로 자동차 사이버보안 법규정에 추가적으로 필요한 위협기술 분야를 발굴하여 현재 법규정의 개선 필요성을 도출하고자 한다.

세계 많은 발명자들은 자신의 아이디어를 권리화하기 위해 특허출원을 신청하고, 심사를 통해 특허권을 획득한다. 그리고 일반적으로 발명은 현재 시장에 나와 있는 제품, 서비스에 대한 내용보다는 미래 시장을 타겟으로 문제점을 예측하고 그에 대한 해결책을 제시하여야 특허성을 인정받을 수 있다. 본 연구에서는 이러한 특허에 대한 성질, 즉 미래 시장, 미래 제품을 타겟으로 특허출원이 신청된다는 점에 착안하여, 최근 5년 내에 세계 각국에서 특허출원한 자동차 사이버보안 발명을 검토하여 자동차의 최신 기술동향을 파악 및 반영함으로써, 자동차 사이버보안 기술의 강화 방안을 도출하고자 한다.

특히 다양한 특허지표를 통해 지속적으로 추가 사이버보안 연구개발이 진행될 것으로 판단되는 신규 기술분야를 도출하고 이에 대한 보안위협, 보안요구사항 및 대응방안을 각 특허출원 등을 참조하여 도출하고자 한다.



(그림 1) 연구방법론

먼저 특허DB(윈텔립스)에서 키워드을 활용하여 자동차 사이버보안 특허데이터를 추출한다. 특허출원서는 서지사항, 발명의 설명(발명의 명칭 포함), 청구범위, 요약서, 도면으로 구성되어 있으며, 키워드 분석은 발명의 명칭, 청구범위, 요약서를 대상으로 해당 키워드가 포함되어 있는지 검색하는 방법을 의미한다. 검색조건으로는 2017년1월1일부터 2022년8월31일까지, 한국, 미국, 일본, EP, PCT(국제협력조약)의 공개 특허출원을 대상으로 하였다. (키워드 : [(차량 자동차 vehicle car automobile (auto* adj mobile)) and ((사이버 near 보안) or (cyber near security) cybersecurity (security and (computer computing program* virus* (mal* adj ware) hacking attack*)) security cyber 보안 해킹 바이러스)])

그리고 검색특허 중 노이즈를 제거하고 유효특

허만을 추출하고, 유효특허들에 대해서, Annex 5에서 제시하는 자동차 사이버보안 기술에 해당하는 특허출원을 제거한다. 그리고 자율주행차 보안모델[3]에 기재된 자동차 공유서비스 등 각종 어플리케이션과 관련된 자동차 사이버보안 관련 기술분야(이하, “APP 사이버보안 기술”)도 제거한다. 그리고 Annex5 및 자율주행차 보안모델[3]의 기술분야에 속하지 않은 특허데이터는 발명의 요지를 기반으로 새로운 기술분류를 도출하고 도출된 기술분류에 따라 분류한다.

3.2 사이버보안 특허출원 신규기술 도출 결과

특허DB(윈텔립스) 내 특허데이터 중 키워드를 활용하여 총 36,222건의 자동차 사이버보안 특허데이터를 검색하였다. 검색된 특허출원 중 노이즈(차량 사이버보안과 관련없는 특허출원)을 제외하고, 또한 Annex5 및 자율주행차 보안모델[3]에서 제시하는 기술분야 특허출원을 제외한 결과, 분류되지 않은 자동차 사이버보안 특허출원은 226건이 도출되었다.

도출된 특허출원 226건은, 전기차와 관련된 사이버보안 기술(이하, “전기차 사이버보안 기술”), 생체인식과 관련된 자동차 사이버보안 기술(이하, “생체인식 사이버보안 기술”), 블록체인을 이용한 자동차 사이버보안 기술(이하, “블록체인 사이버보안 기술”), UAV(Unmanned Aerial Vehicle) 사이버보안 기술(이하, “UAV 사이버보안 기술”)에 대한 내용을 담고 있었다.

<표 1> 신규기술 분류별 유효특허 빈도수

출처	신규기술 분류	빈도수
특허 데이터 에서 도출	전기차 사이버보안 기술	51
	생체인식 사이버보안 기술	74
	블록체인 사이버보안 기술	15
	UAV 사이버보안 기술	86
신규기술 유효특허 합계		226

3.3 신규기술 사이버보안 강화 필요성 검토

신규기술 유효특허에 대해서는, Annex5 및 자율주행 보안모델[3]에 해당하는 유효특허들과 비교하여 사이버보안 강화 필요성을 검토한다. 검토방법으로는 특허데이터를 이용하여 신규기술이 연구개발이 지속적으로 확대될 가능성이 있는지 조사한다. 연구개발이 지속적으로 확대될 가능성이 있는지에 대해서는, 특허출원 빈도수 동향 지수, 연도별 특허출원 동향 지수, 특허출원인 다양성 지수, 특허출원 생존 지수, 특허출원 등록율 지수, 특허출원 포기율 지수, IPC 분류 다양성 지수, 피인용문헌 지수를 이용한다.

특허출원 빈도수 동향 지수는 특허출원의 빈도수를 이용한 지수로, 특허출원 빈도수가 높을수록 연구개발이 활발히 일어났고, 그에 따라 제품 양산도 곧 이루어질 것이라고 해석할 수 있다. 100건 이상 특허출원한 기술분야에는 5점을, 50건~100건 사이 특허출원한 기술분야에는 4점을 부여했고, 50건 이하로 특허출원한 기술분야는 빈도수 측면에서 의미가 없다고 판단하여 0점을 부여하였다. 연도별 특허출원 동향 지수는 최초 특허출원의 시점을 이용한 지수로, APP. 사이버보안 특허출원은 2018년부터 특허출원이 공개되었기에 4점을, 블록체인 사이버보안은 2019년부터 특허출원이 공개되었기에 5점을 부여함으로써, 추가로 연구개발이 활발히 발생될 것이라는 점을 표현하였고, 나머지 기술분야는 2017년 이전부터 특허출원을 진행하여 0점을 부여하였다.

특허출원인 다양성 지수, 특허출원 생존 지수, 특허출원 등록율 지수, 특허출원 포기율 지수, IPC 분류 다양성 지수, 피인용문헌 지수의 경우는 가장 높은 데이터를 가진 상위 기술분야 5개에 5점부터 1점까지 점수를 부여했고, 나머지 기술분야의 경우에는 0점을 부여했다.

특허출원인 다양성 지수는 각 기술분야 내 특허출원 빈도수 및 특허출원인 수의 비율을 이용한 지수로, 비율이 낮을수록 다양한 특허출원인이 관심을 보이는 것으로 판단할 수 있으므로 향후 연구개발 확대 가능성이 높을 것으로 해석할 수 있다. 블록체인 사이버보안 기술, 서버 사이버보안 기술, 전기차 사이버보안 기술, APP. 사이버보안 기술, 업데이트 사이버보안 기술이 각각 1.07, 1.15, 1.21, 1.31, 1.40의 지수가 도출되어, 5점부터 1점으로 점수를 부여받았다. 나머지 기술분야는 1.4

0을 초과하여 0점을 부여받았다.

특허출원 생존 지수는 각 기술분야 내 특허출원의 계속 여부를 이용한 지수로, 생존하고 있는 특허출원이 많을수록 현재 기준으로 연구개발 및 제품 양산을 위해 지속적으로 투자하고 있는 것으로 해석할 수 있다. 차량 내부 사이버보안 기술, APP. 사이버보안 기술, 업데이트 사이버보안 기술, UAV 사이버보안 기술, 통신채널 사이버보안 기술이 각각 82.9%, 82.9%, 82.8%, 81.8%, 81.3%의 생존율을 형성하여, 5점부터 1점으로 점수를 부여받았다. 나머지 기술분야는 81.3% 미만으로 0점을 부여받았다.

특허출원 등록율 지수는 각 기술분야 내 특허출원의 등록율, 즉 선행성을 이용한 지수로, 등록율이 높을수록 추가적인 연구개발 투자가 있을 것으로 해석할 수 있다. 서버 사이버보안 기술, UAV 사이버보안 기술, 업데이트 사이버보안 기술, 외부연결 사이버보안 기술, APP. 사이버보안 기술이 각각 100%, 100%, 95.5%, 95.1%, 95.1%의 등록율을 형성하여, 5점부터 2점으로 점수를 부여받았다. 나머지 기술분야는 95.1% 미만으로 0점을 부여받았다.

특허출원 포기율 지수는 각 기술분야 내 특허출원의 포기 여부를 이용한 지수로, 포기율이 높을수록 향후 연구개발 투자가 증대될 수 있는 것으로 해석할 수 있다. 서버 사이버보안 기술, 전기차 사이버보안 기술, UAV 사이버보안 기술, 외부연결 사이버보안 기술, 차량내부 사이버보안 기술, APP. 사이버보안 기술이 각각 30.8%, 25.0%, 18.2%, 16.8%, 13.9%, 13.9%의 포기율을 형성하여, 5점부터 1점으로 점수를 부여받았다. 나머지 기술분야는 13.9% 미만으로 0점을 부여받았다.

IPC 분류 다양성 지수는 각 기술분야 내 특허출원의 IPC 분류 개수를 이용한 지수로, IPC 분류 개수가 클수록 추가적인 연구개발 가능성이 높은 것으로 해석할 수 있다. 전기차 사이버보안 기술, 블록체인 사이버보안 기술, APP. 사이버보안 기술, 생체인식 사이버보안 기술, 외부연결 사이버보안 기술, UAV 사이버보안 기술이 각각 4.1, 4, 3.7, 3.5, 3.4, 3.4의 지수를 형성하여, 5점부터 1점으로 점수를 부여받았다. 나머지 기술분야는 3.4 미만으로 0점을 부여받았다. (예컨대 전기차 사이버보안 기술에 해당하는 특허출원은 51건이며, 각 특허출원에 부여된 IPC 개수의 평균값이 4.1임)

피인용문헌 지수는 각 기술분야 내 특허출원이 인용되는 횟수를 이용한 지수로, 인용되는 횟수가 클수록 해당 기술분야의 연구개발이 활발하다는 것으로 해석할 수 있다. 업데이트 사이버보안 기술, UAV 사이버보안 기술, 블록체인 사이버보안 기술, 전기차 사이버보안 기술, 차량내부 사이버보안 기술이 각각 2.31, 1.68, 1.50, 1.11, 1.06의 지수를 형성하여, 5점부터 1점으로 점수를 부여받았다. 나머지 기술분야는 1.06미만으로 0점을 부여받았다. (예컨대 업데이트 사이버보안 기술에 해당하는 특허출원은 42건(A)이며, 각 특허출원이 피인용된 문헌의 전체 수는 67건(B)이며, B를 A로 나눈 결과값임. 다만, 매해 피인용된 문헌 전체값의 평균값으로 나눔으로써 연도별 특징이 아닌, 기술별 특징을 도출하고자 했음)

<표 2>는 기술분야별로 지수에 대한 점수를 부여하고 이를 합산하여, 향후 사이버보안 연구개발이 확대될 가능성이 높은 기술분야, 추가 연구개발 가능성이 중간인 기술분야, 추가 연구개발 가능성이 낮은 기술분야를 도출하였다. 이를 통해 신규기술 분야가 추가로 연구개발이 확대되어 사이버보안을 강화할 필요가 있는지 검토하였다.

검토 결과에 따르면, 신규 사이버보안 기술 중에서 전기차 사이버보안 기술, 블록체인 사이버보안 기술, UAV 사이버보안 기술이 추가로 연구개발이 확대될 가능성 높은 것으로 도출되었고, 이하 세 사이버보안 기술의 강화방안에 대해 기술해 보도록 한다.

즉 신규 사이버보안 기술 중 향후 연구개발 확대가능성이 높다는 것은 제품화될 가능성이 높다는 것이므로, 이에 대해 사전에 사이버보안 강화방안을 도출해 보도록 하겠다.

<표 2> 연구개발 확대 가능성 도출 지수표

기술	서버	통신 채널	업데이트	외부 연결	차량 내부	APP.	전기차	생체 인식	블록 체인	UAV
기술 출처	Annex5					자율차 보안모델	신규기술			
특허출원 빈도수 동향 지수 (4~5점)	0	5	0	5	5	0	4	4	0	4
연도별 특허출원 동향 지수 (4~5점)	0	0	0	0	0	4	0	0	5	0
특허출원인 다양성 지수 (1~5점)	4	0	1	0	0	2	3	0	5	0
특허출원 생존 지수 (1~5점)	0	1	3	0	5	5	0	0	0	2
특허출원 등록율 지수 (1~5점)	5	0	3	0	2	2	0	0	0	5
특허출원 포기율 지수 (1~5점)	5	0	0	2	1	1	4	0	0	3
IPC 분류 다양성 지수 (1~5점)	0	0	0	1	0	3	5	2	4	1
피인용문헌 지수 (1~5점)	0	0	5	0	1	0	2	0	3	4
지수 점수 합계	14	6	12	8	14	17	18	6	17	19
연구개발 확대 가능성	**중간**	**낮음**	**중간**	**낮음**	**중간**	**높음**	**높음**	**낮음**	**높음**	**높음**

4. 신규기술에 대한 자동차 사이버보안 강화방안

신규기술 중, 자동차 사이버보안 법규정 관점에서는 향후 적극적인 연구개발을 통해 기술개발 및 제품양산이 예상되는 연구개발 가능성이 높은 기술분야인, 전기차 사이버보안 기술, UAV 사이버보안 기술, 블록체인 사이버보안 기술에 대해서는 사전에 사이버보안 강화방안을 논의할 필요가 있을 것이다. 이하에서는 3개 기술분야별로 특허출원 등을 이용하여 보안위협, 보안요구사항, 대응방안을 제시하도록 한다.

보안위협 및 보안요구사항은 추가 연구개발 가능성이 높은 기술분야 내 특허출원 중 영향도가 높은 특허출원을 이용하도록 한다. 즉 영향도가 높은 특허출원은 제품 적용 가능성이 높기 때문에 이에 대한 대응방안을 강구할 필요가 있다. 영향도가 높은 특허출원은 피인용문헌수, 패밀리 국가수, IPC 분류 개수, 특허출원 생존 여부, 발명자 수 등을 고려하도록 한다. 그리고 대응방안으로는 자율주행차 보안모델[3]에서 제시하고 있는 유사 대응방안을 도입하여 제시하고자 한다.

4.1 전기자동차 사이버보안 강화방안

전기차 사이버보안 기술의 경우, 영향도 높은 특허출원 3건을 추출하였고, 각 특허출원의 특허내용, 특허내용에 따라 도출가능한 보안위협을 도출하였다.

<표 3> 전기차 사이버보안 주요 특허출원 내용 및 보안위협

출원번호	보안위협
US 16/291342	(4-1) 차량 내부 및 충전기 해킹을 통해 전류,전압,공진,임피던스가 해킹될 수 있음 (4-2) 각종 정보(전류, 전압 등) 사용에 대한 권한 통제가 되지 않은 경우 전산자원 오남용에 의해 로그 파일의 변조 등 무결성이 손상될 수 있음
PCT-CN2019-097282	(2-1) 외부에서 내부망 접근시 암호화통신 및 이중인증을 하지 않을 경우, 통신 구간의 정보유출 또는 비인가접속의 위험이 존재하여 안전메시지에 대한 해킹이 가능함 (2-2) 배터리잠금 해제에 대한 권한 통제

	가 되지 않은 경우 전산자원 오남용에 의해 로그파일의 변조 등 무결성이 손상될 수 있는 위험이 있음 (2-3) 외부에서 배터리교체 인프라에 접근시 암호화 통신 및 이중 인증을 하지 않을 경우 통신 구간의 정보 유출 또는 비인가 접속의 위험이 존재함
US 16/0049 33	(3-1) NFC통신에 있어 전기차 충전 플러그 잠금 해제 요청 정보 미암호화시 스니핑에 의한 정보 유출 위험이 있음 (3-2) 전기차 충전 플러그 잠근 해제 정보에 대한 권한 통제가 되지 않은 경우 로그파일의 위변조 등 무결성이 손상될 수 있는 위험이 있음 (3-3) 차량 내부 제어기 해킹을 통해 각종 요청메시지가 해킹될 수 있음

다음으로 <표 3>에서는 도출된 보안위협에 대해 유사 유형의 보안위협을 그룹핑하여 보안요구사항 및 대응방안을 <표 4>와 같이 도출해 보았다. 각 보안요구사항에 대한 대응방안은 자율주행자동차 보안모델[3]에서 제시하고 있는 대응방안을 참조하여 수립하였다.

4.2 무인항공차량 사이버보안 강화방안

무인항공차량 사이버보안 기술의 경우, 영향도 높은 특허출원 3건을 추출하였다. 그리고 각 특허출원의 특허내용, 특허내용에 따라 도출가능한 보안위협을 도출하였다.

<표 5> UAV 보안 주요 특허출원 내용 및 보안위협

출원번호	보안위협
PCT-US 2018-032 606	(1-1) UAV와 서버간에 통신에 있어 UAV 식별정보 미암호화시 스니핑에 의한 정보 유출 위험이 있음 (1-2) 서버에서 UAV 식별정보에 대한 암호화 알고리즘과 암호화키 관리가 취약하여 악의적인 사용자에게 노출될 경우 비인가자에 의해 사용자정보가 변조될 수 있음
US 16/61 9672	(2-1) UAV와 제어 플랫폼간에 통신에 있어 중요정보 미암호화시 스니핑에 의한 정보 유출 위험이 있음 (2-2) 외부에서 내부망에 접근시 암호화 통신 및 이중인증을 하지 않을 경우, 통신구간의 정보유출 또는 비인가 접속의 위험이 존재하여 중요정보에 대한 해킹이 가능함
PCT-US 2019-031 513	(3-1) 센서유닛, UAV, 네트워크 간에 통신에 있어 위치 정보 미암호화시 스니핑에 의한 정보 유출 위험이 있음 (3-2) 외부에서 내부망 접근시 암호화 통신 및 이중인증을 하지 않을 경우, 통신구간의 정보유출 또는 비인가 접속의 위험이 존재하여 UAV 위치정보에 대한 해킹이 가능함

다음으로 <표 5>에서 도출된 보안위협에 대해 유사 유형의 보안위협을 그룹핑하여 보안요구사항 및 대응방안을 <표 4>과 같이 도출해 보았다. 각 보안요구사항에 대한 대응방안은 자율주행자동차 보안모델[3]에서 제시하고 있는 대응방안을 참조하여 수립하였다.

4.3 블록체인 차량 사이버보안 강화방안

블록체인 자동차 사이버보안 기술의 경우, 영향도 높은 특허출원 3건을 추출하였다. 다만 특허내용으로 판단컨대 블록체인 기술 자체는 위협기술이라기 보다는 사이버보안의 대응책으로 이용되고 있으므로, 블록체인 자동차 사이버보안 기술에 대한 강화방안에서는 별로도 보안위협 및 보안요구사항을 파악하지 않고 적용분야를 도출하고, 해당 적용분야에서 블록체인 자동차 사이버보안이 활용될 수 있음을 제시하고자 한다.

<표 6> 블록체인 자동차 사이버보안 특허출원 내용 및 적용분야

1	출원번호	EP 2017-186406
	세부기술	블록체인을 이용한 ECU 보안 강화 (운전보조시스템)
	적용분야	운전보조시스템 ECU에 의한 동작 명령의 보안을 위해 이용
2	출원번호	JP 2019-162256
	세부기술	자동차 주행기록을 블록체인을 이용하여 저장
	적용분야	주행기록정보(서비스 제공자인덱스/차량제조사인덱스/차량인덱스/운전자인덱스+주행기록정보)에 대한 보안을 위해 사용
3	출원번호	US 16/569325
	세부기술	차량 CAN, EDR, ECU, OBD 데이터를 블록체인을 이용하여 보호
	적용분야	차량 CAN, EDR, ECU, OBD 데이터에 대한 보안을 위해 사용

<표 4> 전기차 및 UAV 사이버보안 보안위협, 보안요구사항 및 대응방안

구분	보안위협 No.	보안위협 설명	보안요구사항	대응방안
전기차사이버보안	1-1, 3-3	전기차, 충전스테이션 내 ECU/CPU 해킹	전기차, 충전스테이션 내부 제어기 보안 강화	▶ 내부시스템 내 ECU/CPU와 CCU, CGW, 내부 통신모듈 간 통신 보안 강화
	1-2	전기차, 충전스테이션 로그파일 위/변조	전기차, 충전스테이션 로깅 정보 위/변조 방지	▶ 사용자/관리자에 의한 로그 파일 쓰기 권한 제한 ▶ 별도의 로그관리시스템 운영 ▶ 덮어쓰기 방지 매체를 사용
	2-1	서버, 전기차, 충전스테이션 간 통신 해킹 통해 사용자 도용, 충전량 조작	서버, 충전스테이션, 전기차 간 통신에 있어 외부에서 접속시 접근통제	▶ 외부에서 내부 네트워크 장비로의 원격 접속은 방화벽, 네트워크 장비 ACL 등으로 제한해야 함 ▶ 부득이하게 허용하는 경우 책임자 [사전|사후] 승인, 외부 접속 단말기를 최소한으로 제한 등의 대책 적용해야 함
	2-2	서버, 충전스테이션에 대한 무단 액세스로 개인정보 탈취	서버, 충전스테이션 암호키 관리	▶ 대상: KMS/HSM, 암호시스템관리서버, 암호키 주입기, WAS 등 키 보관/적재 시스템 ▶ 어플리케이션, 보안시스템 등 정보시스템에 적용되는 암호화 키관리
	2-3	전기차, 충전스테이션에 대한 외부 접속으로 해킹 발생	전기차, 충전스테이션에 대해 외부에서 접속시 접근통제	▶ 외부에서 내부 DBMS으로의 원격 접속은 제한해야 함 ▶ 부득이하게 허용하는 경우, 책임자 [사전|사후] 승인, 외부 접속 단말기를 최소한으로 제한 등과 같은 대책 적용해야 함
	3-1	서버, 전기차, 충전스테이션 간 통신 해킹으로 인해 사용자 도용, 충전량 조작	서버, 전기차, 충전스테이션 간 전송구간 암호화	▶ 전송 구간이 신뢰된 네트워크가 아닌 곳을 경유할 때에는 도청/변조/가로채기 등을 방지하기 위한 안전한 암호화 프로토콜 및 알고리즘을 사용하여 전송해야 함 ▶ 외부 기관 데이터 전송 시 전용선과 VPN 이용 ▶ 내부시스템 구간 암호화 : 암호화된 데이터를 전송하는 것을 원칙으로 하며, 최종위치에서 복호화해야 함
	3-2	서버, 충전스테이션, 전기차 간 통신 로그파일 위/변조	서버, 충전스테이션, 전기차 간 통신에 있어 로깅 정보 위/변조 방지	▶ 전송 구간이 신뢰된 네트워크가 아닌 곳을 경유할 때에는 도청/변조/가로채기 등을 방지하기 위한 안전한 암호화 프로토콜 및 알고리즘을 사용하여 전송해야 함 ▶ 외부 기관 데이터 전송 시 전용선과 VPN 또는 전용선 이용 ▶ 내부시스템 구간 암호화
UAV사이버보안	1-1, 2-1, 3-1	서버, UAV, 센서, 제어플랫폼 간 통신 해킹으로 인해 UAV 식별 도용, 비행정보 조작	서버, UAV, 센서, 제어플랫폼(비행관리시스템, 통합데이터 관리시스템, 서비스제공자) 간 전송구간 암호화	▶ 전송 구간이 신뢰된 네트워크가 아닌 곳을 경유할 때에는 도청/변조/가로채기 등을 방지하기 위한 안전한 암호화 프로토콜 및 알고리즘을 사용하여 전송해야 함 ▶ 외부 기관 데이터 전송 시 전용선과 VPN 또는 전용선 이용 ▶ 내부시스템 구간 암호화 : 암호화된 데이터를 전송하는 것을 원칙으로 하며, 최종위치에서 복호화해야 함
	1-2,	서버, 제어플랫폼에 대한 무단 액세스로 개인정보 탈취	서버, 제어플랫폼 내 암호키 관리	▶ 대상: KMS/HSM, 암호시스템관리서버, 암호키 주입기, WAS 등 키 보관/적재 시스템 ▶ 보안시스템 등 정보시스템에 적용되는 암호화 키관리
	2-2, 3-2	서버, UAV, 센서, 제어플랫폼에 대한 외부 접속으로 UAV 식별 도용, 비행정보 조작 등 해킹 활동	서버, UAV, 센서, 제어플랫폼 간 통신에 있어 외부에서 접속시 접근통제	▶ 외부에서 내부 네트워크 장비로의 원격 접속은 방화벽, 네트워크 장비 ACL 등으로 제한해야 함 ▶ 부득이하게 허용하는 경우 책임자 [사전|사후] 승인, 외부 접속 단말기를 최소한으로 제한 등의 대책 적용해야 함

5. 결 론

이상에서 살펴본 바와 같이, 자동차 사이버보안 이슈의 심각함으로 인해, 각 국가에서는 자동차 사이버보안 법규정을 제정하고 이를 통해 자동차 사이버보안을 강화하고 있다. 다만 최근 자동차 산업의 빠른 발전을 고려하면 지속적인 법규정 보완이 필요하다고 판단되며, 본 연구에서는 자동차 사이버보안 특허데이터 분석을 통해, 기존 법규 등에서는 상정되지 않은 신규기술인 전기차 사이버보안, 블록체인 사이버보안, 무인항공차량 사이버보안 강화의 필요성을 제안하고, 그에 대한 보안위협의 유형을 기술하고, 각 보안위협에 따른 완화방안을 제시하였다

특히 전기차 사이버보안 강화 필요성에 대해서는, 최근 전기차 시장의 확대와 동시에 전기차 해킹가능성 문제도 꾸준히 제시되고 있다. 2022년1월 뉴욕포스트에 따르면 독일국적 IT 전문가이자 보안업체 창업자인 다비드 콜롬보에 의해 테슬라 25대가 해킹되어 원격으로 차체 제어 및 주행까지도 가능하였다고 한다. 즉 자동차 해킹의 문제는 전기차에서도 피할 수 없는 문제가 되었다. 따라서 전기차 사이버보안 내용을 UNR.155에 반영하여 전기차 사이버보안은 반드시 강화되어야 한다고 판단된다.

지금까지 자동차 사이버보안 기술을 특허데이터를 통해 특허출원에 의해 제시되는 추가적인 사이버보안 기술에 대해 살펴보았다. 다만 특허출원은 시장에서 출시된 제품이나 서비스에 기반한다기 보다는 발명자에 의해 고안된 아이디어에 기반하므로, 특허출원에 근거하여 실제 상황에서의 사이버보안 기술을 도출하는 것에 한계가 있을 수 있다. 따라서 사이버보안 기술 도출에 대해 특허출원의 분석방법 외에도 다른 분석방법으로 보완하여 완성도를 높일 필요가 있을 것으로 판단된다.

본 연구는 사이버보안 위협을 자동차라는 키워드로 한정하여 특허데이터를 추출하였다. 다만, 미래에 어떠한 기술이 자동차에 적용되고 융합될지 예측하는 것은 쉽지 않을 것이므로, 향후에는 자동차 키워드로 한정하지 말고, 전자장치(ex.스마트폰)로 기술범위를 확장하여 자동차 사이버보안 위협기술을 폭넓게 탐색하는 연구를 진행할 필요가 있다.

또한 본 연구에서는 무인항공차량 특허출원을 기반으로 무인항공차량의 사이버보안 강화에 대해 논의해 보았다. 그러나 최근 자동차업계가 자동차 기업을 넘어서 모빌리티기업으로의 전환을 시도하면서, 2020년 현대차그룹의 CES 2020에서의 개인항공차량(PAV, Personal Aerial Vehicle) 콘셉트 모델 'S-A1' 공개[14], 2020년 토요타자동차의 '수직 이착륙 비행체(eVTOL)' 개발스타트업 '조비항공(Joby Aviation)'에 약 4500억원 투자[15], 2021년 제너럴 모터스(GM)의 수직 이착륙 방식의 미래형 비행 캐딜락 차량 공개[16], 2022년 폭스바겐그룹의 전기 수직 이착륙 UAM인 'V.MO'시제품 공개[17] 등이 시도되고 있다. 즉 현재 자동차업계는 개인항공차량에 많은 관심을 가지고 에 대해 투자하고 있다. 무인항공차량과 개인항공차량은 사람이 탑승한다는 측면을 제외하면 기본 컨셉 상으로는 유사하다고 판단되므로, 무인항공차량 사이버보안에 강화내용을 개인항공차량에 접목하여 개인항공차량 사이버보안의 강화가 필요할 것이라고 논리를 전개하는 것도 가능할 것이라고 판단된다.

참고문헌

[1] UNECE, “Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system : UN Regulation No.155”, 2021.

[2] 국토교통부, “자동차 사이버보안 가이드라인”, 2020.

[3] 과학기술정보통신부 · 한국인터넷진흥원(KISA), “자율주행차 보안모델”, 2021.

[4] 정임영, “자율주행자동차 위험 및 대응방안에 대한 고찰”, 한국콘텐츠학회, 제20권, 제6호, pp.90-98, 2020.

[5] 이슬기롬, 조세라, “ UNECE UNR.155 차량 사이버 보안 규제 대응을 위한 공격 시나리오 도출”, 한국자동차공학회 논문집, vol 29, no. 8, 통권 189호 pp.717-732, 2021.

[6] 송태진, 유용식, 조민제, 홍준호, “자율협력주행 전기차 환경에서 통합 사이버 보안 체계 정립 연구”, 대한교통학회지, vol. 39, no. 4, 통권 181호, pp. 493-515, 2021.

[7] 이은영, “자율주행자동차 사이버보안 법규 추진 동향”, 오토저널, 2020.

[8] 정승연, 강수영, 김승주, “자동차 개발 프로세스에서의 보안내재화 방법론”, 정보처리학회논문지, vol 9, no. 12, 통권 099호, pp.387-402, 2020.

[9] 장은진, 신승중, “자율주행 자동차의 시스템 보안 향상을 위한 새로운 데이터처리 기능 제안”, 한국인터넷방송통신학회, vol. 20, Issue 4, pp. 81-86, 2020.

[10] 이광구, 우현구, “레벨 4 자율주행자동차의 제작 안전 가이드라인에 대한 고찰”, 자동차안전학회지, vol. 13, no. 3, 통권 39호, pp.86-94, 2021.

[11] 박효정, 고정민, 정효주, 김경진, “자율주행 자동차를 위한 자동차 사이버 보안 가이드 개선에 관한 연구 : 자동차 라이프사이클 중심으로”, 한국산업보안연구학회논문지, 제12권, 제1호, p.329, 2022.

[12] 강동우, 원동호, 이영숙, 무인항공기의 안전한 도입을 위한 보안기능요구사항 개발”, 융합보안논문지, 제19권, 제4호, 2019.

[13] 이경환, 류갑상, “무인항공기 보안 취약점 개선을 위한 연구“, 스마트미디어저널, 제7권, 제3호, 2018.

[14] Biz watch, “[CES 2020]현대차, 우버 손잡고 하늘나는 차 만든다”, 2020.

[15] 전자신문, “토요타, 美도심항공기 스타트업에 4,574억원 투자”, 2020.

[16] IT Daily, “GM, 하늘을 나는 미래형 항공 캐딜락 차량 공개”, 2021.

[17] 매일경제, “현대차, 도요타, 폭스바겐, 도로 넘어 하늘서 한판 붙자”, 2022.

[18] IT Daily, “GM, 하늘을 나는 미래형 항공 캐딜락 차량 공개”, 2021.

[19] 최충현, “개인용 항공기(PAV), 한국과학기술기획평가원, 2021-5호, 2021.

[20] 심혜정, “도심 항공 모빌리티(UAM), 글로벌 산업 동향과 미래 과제”, 한국무역협회, 2021년 22호, 2021.

〔저자소개〕

곽 동 한 (Dong-Han Kwak)
2001년 2월 고려대학교 수학 학사
2023년 8월 고려대학교 정보보호대학원 석사 수료
email : kwakpat@gmail.com

권 헌 영 (Hun-Yeong Kwon)
2008년 3월 ~ 2015년 8월 광운대학교 법과대학 교수
2015년 9월 ~ 고려대학교 정보보호대학원 교수
email : khy0@korea.ac.kr