(2024. 8. 14)

산업분석 Vol. 138

미국의 중국산 커넥티드카 사이버보안 규제 영향

정책전략실
장홍창 선임연구원

KATECH Insight

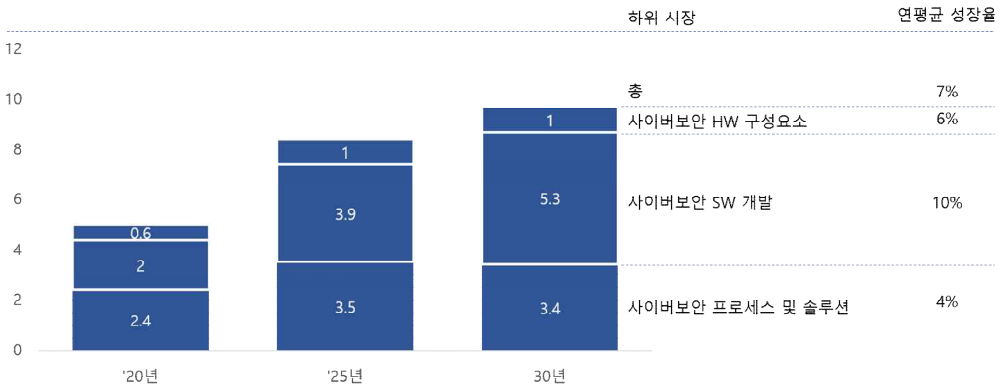
◈ 미국은 중국산 커넥티드카 기술 사용을 규제하는 사전규제 도입안을 공고하였으며, 향후 규제 대상 범위를 확대 해석 시 공급망 변경이 필요하여 자동차 업계에 혼란을 유발할 가능성 제기

◈ 동시에 UNR155(車 사이버보안 UN 규제)를 통한 글로벌 사이버보안 요구사항이 확대 중이나, 국내 중소 부품기업의 준비가 부족한 상황으로 적극적인 인력양성·컨설팅·평가 장비 등 지원 필요

» 현재의 車는 ADAS·커넥티드 기능의 구현을 위해 지속해서 내외부 연결성이 확대되고 있으며, 이에 따라 주요 브랜드 차량 보안 문제 증가와 동시에 車 사이버보안 산업이 고성장 중

- 최근 판매 차량의 ADAS·커넥티드 기능 탑재로 차량 내외부 통신 범위가 확대되어, 車 사이버 공격은 차량 내에만 국한되지 않고 통신 기능이 연결된 클라우드·네트워크 전체에 피해 확산 가능
- 이미 대다수 글로벌 자동차 OEM社에서 사이버보안 문제가 발생하고 있으며, 이를 방지하기 위한 車 사이버보안 산업이 36.6억달러('23년)→97~118억달러('30년) 규모로 고성장 전망
  - 테슬라·폭스바겐·BMW·닛산·미쓰비시 등 주요 OEM社 다수에서 해킹 혹은 보안 취약 사례가 보도되었고, 백도어(인증되지 않은 사용자가 몰래 설치한 통신 연결 기능) 문제의 경우 검출이 매우 어려운 상황
  - Precedence Research社는 車 사이버보안 산업이 36.6억$('23년)→118억$('30년)로 성장할 것으로 추정하였으며, McKinsey社는 49억$('20년)→97억$('30년)로 시장이 성장하고 특히 보안 SW의 비중 증가 예상

▌자동차 사이버보안 산업 규모 및 구성▐



* 출처: McKinsey

» 미국은 中 커넥티드카 기술이 국가안보를 위협할 것으로 보고 사전규제 도입안을 공고하였고, 향후 규제 범위에 따라 車 산업 전체의 공급망 변경 조치 필요성 제기

- 美 상무부는 우려국 커넥티드카 기술 사용을 규제하는 잠정규정을 알리고 적용 범위를 결정하기 위한 규칙제정 사전통지(ANPRM)를 개시하여 우방국 및 관련 업계 의견을 수렴

- 바이든 美 대통령은 우려국*이 미국 내 커넥티드카를 통한 데이터 수집 및 인프라 교란 등의 활동이 국가안보에 위협이 될 것으로 보고, 상무부에 커넥티드카 산업 현황을 조사하고 조치 요청('24.2.29)

* 우려국에 중국, 러시아, 이란, 쿠바, 북한, 베네수엘라(니콜라스 마두로 정부)를 포함

- 미국 상무부는 커넥티드카에 필수적인 정보통신 부품 관련 설계·개발·제조·공급하는 기업 중 우려국가의 소유·통제·관할에 있는 기업의 기술 사용을 규정하는 사전규제 도입안 공고(ANPRM) 개시('24.3.1)
- 현재 ANPRM 기술 정의에서의 커넥티드카는 사실상 현재 판매되는 차량 대부분을 지칭하고 있고, 기술의 범위 또한 불특정하여 향후 데이터를 생성하는 센서·소재·기타 부분품까지 포함할 가능성 존재
- ANPRM에는 커넥티드카 정의, 공급망, 데이터 수집 등의 보안 위협 요인과 관련된 질의가 포함되어 있으며, 배경과 질의 내용을 분석해 볼 때 과거 중국 화웨이 제재 형식과 일부 유사하게 진행 예상
- 美 상무부는 중국산 커넥티드카 SW 및 통신 모듈 사용 제한 방안을 '24.8월에 발표할 것으로 공개

• **美 상무부의 커넥티드카 사전규제 도입안 공고에 대한 총 57개 공개의견이 등록되었으며, 미국 기관들은 규제의 취지에 동의하는 반면 車 업계에서는 제재 대상 부품 범위 확대에 대한 우려 표명**

* 전체 의견 중 공개의견 57개(비영리기관 30개, 부품·관련 기업 13개, 익명·개인 7개, 완성차社 기업 4개, 정부 3개)가 등록되었고, 이 중 美 기관 의견이 가장 많으며 한국을 포함한 EU·독일·네덜란드·호주 등 우방국 의견 등재

- 포드는 규제의 취지에 강한 동의를 하였으나 규제 범위 제품의 공급망 변경에 따른 비용 문제를 지적하였고, 폭스바겐은 공급망 변경 비용 문제 우려 및 규제 관련 업계 지원 프로그램 제안
- NXP는 사이버보안 문제를 기존 국제 표준을 통해 해소할 수 있음을 지적하고 규제 범위를 부품에 확장 시 개발 비용 상승을 우려하였으며, 웨이모는 업계에서 적응할 시간과 혼란을 방지할 임시 규칙제정 권장

» 글로벌 주요국은 UNR155를 중심으로 완성차·부품기업에 사이버보안 요구사항을 확대 중

• **해외 주요 국가들은 UNR155*를 채택하여 車·부품 기업에 대한 최소 요구사항을 확대하고, 글로벌 車 기업은 ISO/SAE 21434에 기반하여 확장한 범위에서 사이버보안 강화 노력 중**

* UNECE(유럽경제위원회) 산하 자동차 기준 국제조화 회의 WP.29는 자동차 사이버보안 관련 법규인 UNR(UNECE Regulation) 155를 제정하여 사이버보안 관리체계(CSMS) 및 형식승인 의무화

- UNECE WP.29 회원·채택 국가 약 60개국은 신차 판매 시 CSMS 인증을 의무화 및 보안대책을 요구하고 있으며, 국내에서는 국토교통부가 車 사이버보안 가이드라인 및 자동차관리법을 개정하여 사이버보안 강화 중

* EU는 '24.7월부터 유럽 지역 내 출시되는 모든 차량에 대하여 CSMS 인증을 취득하고 형식승인 요구

▌글로벌 차량 사이버보안 규정 및 표준 비교 ▐

구분	채택 국가	내용
UNR155	약 60개국 (미국, EU, 영국, 한국, 일본 등)	· 사이버보안 형식승인 및 CSMS 인증 의무 규정('22.7월) · 조직 및 차량 수준 요구사항을 정의
GB & GB/T	중국	· 차량 사이버보안 관련 기술적 요구사항 규정 · 중국은 100개 이상의 커넥티드카 관련 표준을 적용 예정
ISO/SAE 21434	- (국제 표준)	· 차량 엔지니어링 관련 첨단 사이버보안 국제 표준 · 사이버보안 관리 입증을 위한 가이드라인 및 결과물 생성 방법 제공 * UNR155, GB & GB/T는 해당 표준을 참고하여 구성
NHTSA	미국	· 법적 구속력이 없는 자발적 자동차 산업 사이버보안 모범 실무 지침 · 차량 제조사 및 부품사가 해당 지침을 검토하여 적용하도록 권장

* 출처: Argus 자료 참고하여 저자 재작성

» 국제적 車 사이버보안 요구사항 급증에 더하여 미국은 중국산 커넥티드카 규제로 자국 중심의 車 산업으로 재편하고자 하지만, 국내 중소 車 부품기업의 대응에 보완 필요

- **미국은 커넥티드카 사이버보안을 계기로 차량용 이차전지 산업과 유사하게 자국 산업을 보호하고 중국 기업을 견제하여 글로벌 헤게모니를 가져오려는 전략으로 해석**
- **국내 주요 OEM·Tier1 기업은 글로벌 사이버보안 규제 대응이 가능하지만, 이외 중소 Tier1·2 이하 기업 및 미래차 부품 전환 기업은 사이버보안의 중요성 인지 부족과 동시에 대응 여건 부족**
  - 글로벌 사이버보안 요구사항 증가에 따라 국내 Tier1 이하 부품기업에도 CSMS 인증을 위한 보안 목표 도출 방법론(TARA), 프로세스 정립, SW 문서화 체계(SBOM) 등 다양한 방법론 도입이 요구
  - 주요 OEM·Tier1 기업은 글로벌 규제 대응하기 위한 역량을 갖추고 있으나, 대다수 중소 Tier1·2 이하 기업은 글로벌 기준의 최소 요구사항만을 충족하거나 대응 역량이 충분하지 않은 상황

    * 완성차 기업 중 독일 3社가 높은 사이버보안 기술 수준과 규제 대응 역량을 보유한 것으로 평가되고 있으며, 글로벌 차량용 반도체 사이버보안 기술은 NXP, 인피니언, 마이크론 등이 사이버보안에 적극 대응 중

» 미국의 중국산 사이버보안 기술 규제를 국내 자동차 부품 수출 기회로 연결하고, 국내 車 부품기업의 사이버보안 대응 역량 강화를 위해 적극적 기술 컨설팅 및 인력양성 요구

- **중국의 車 부품기업 외에도 중국의 기술 및 부품 등을 활용하는 글로벌 자동차 부품기업이 영향을 받을 것으로 예상이며, 금번 제재 대상이 되는 제품을 중심으로 우리나라 기업의 확장 필요**

  * 일례로 車 반도체 등을 판매하는 대만 팹리스 기업은 중국 내 공장에서 위탁생산하여 제재 대상에 포함 추정
- **국내에 車 사이버보안 기술이 부족함에 따라 전주기 대상 사이버보안 기술 개발이 요구되고, 자체 대응이 어려운 자동차 부품 중소기업을 대상으로 보안 컨설팅 및 평가 장비 지원 요구**
  - 글로벌 자동차 사이버보안 요구사항에 맞춰 국내 기술 공백을 진단하고 기술 고도화를 추진해야 하며, 부품기업은 UNR155·ISO21434 기반 사이버보안 관리체계(CSMS) 및 보안 강화 방안 마련 필요
  - 내수 비중이 높은 국내 대다수 부품社은 사이버보안에 대한 중요성과 경각심을 가지지 못하고 있어 공공부문에서 미래차 부품을 양산하거나 사업화를 진행 중인 기업을 대상으로 컨설팅, 교육, 평가 장비 지원 요구
- **현재 국내 사이버보안 인력은 주요 OEM·Tier1 기업을 중심으로 집중되어 있어, 부족한 사이버보안 SW 개발 인력을 중심으로 중소 Tier2 이하 기업까지 인력이 공급될 수 있도록 인력양성 필요**
  - 국내 사이버보안 기술은 IT 산업을 중심으로 경쟁력을 갖추고 있으나 車 산업으로 확산되지 못하는 상황
  - 현재 국내 車 사이버보안 전문인력은 주요 OEM·Tier1 기업을 중심으로 집중되어 있고 전체가 대략 천명 이상*으로 추산됨에 따라 Tier2 이하로도 인력이 공급될 수 있도록 추가 인력양성 요구

    * 직접적으로 자동차 사이버보안 기술을 구현할 수 있는 인력 기준으로 자체 추정
  - 글로벌 요구수준을 만족하는 사이버보안 적용을 위해서 기존 개발 자원 대비 120~130% 투입이 필요하며, 다양한 역할의 사이버보안 인력*이 필요하고 특히 사이버보안 SW 전문인력이 수요가 높은 상황

    * 차량 사이버보안 관련 직무는 제어기 보안 기능 설계, 차량 보안 시스템·인프라 개발, 프로세스 엔지니어링, 보안 취약점 분석, 보안 평가·심사 등이 필요(출처: 현대모비스)
  - 인력양성 시 단발성 교육이 아닌 부품기업에서 실질적인 보안 전문가를 분야별로 양성할 수 있도록 전문가 교육과 기업 컨설팅 지원을 병행하여 실무 전문가 양성과 글로벌 사이버보안 규제 대응 지원 필요