



LEGAL UPDATE

자동차 사이버보안 관리체계 의무화

- '자동차 관리법'을 통해 사이버보안 확보 및 SW 업데이트 안전관리 -

국토교통부에서는 '자동차관리법'을 개정하여 자동차 사이버보안관리체계와 자동차 소프트웨어 업데이트 안전조치에 대한 자동차 제작사의 의무사항과 관련기관인 국토교통부의 권한을 규정하였습니다. 이는 2020년 자동차 사이버보안 국제 표준을 반영할 수 있는 제도적 기반을 마련한 것인 바, 개정의 주요내용을 살펴보겠습니다.

1. 개정배경

가) 자동차 사이버보안 위협

자동차가 점차 소프트웨어 중심으로 발전해 가고 있음으로 인해 보안 위협이 증대되고 있습니다. 현재까지는 자동차 해킹으로 금전/인명 피해가 크게 발생한 사례는 알려진 바 없으나 연구기관이나 화이트해커가 실제 차량을 대상으로 모의해킹을 시연한 사례는 다수 공유되었습니다. 자동차의 전자제어장치가 증가함에 따라 소프트웨어 중심 자동차(SDV, Software-Defined Vehicle)로 전환되고 통신과 연결이 증가하게 되면서 자동차 불법제어 및 프라이버시 침해 등 사이버보안 취약점과 위협이 증대되고 있습니다. 자동차에 대한 사이버공격의 피해는 즉각적인 인명 사고로 이어질 수 있다는 점에서 자동차 사이버보안의 확보가 필요합니다.

시기	내용
'22.05.	테슬라의 저전력 블루투스(BLE) 통신의 취약점을 이용하여 차량을 훔치는 해킹 시연
'21.08.	테슬라 오토파일럿의 차선 유지기능의 취약점을 이용하여 차량이 오인식하지만, 운전자는 인식하지 못하는 페이크 차선을 통해 공격 가능성을 시연
'20.11.	테슬라 모델 X의 블루투스 취약점을 이용하여 테슬라 모델 X를 훔치는 것이 가능함을 시연
'20.08.	드론 등을 통해 디지털 스크린에 짧은 시간의 이미지를 송출하여 자율주행 AI 시스템을 속일 수 있는 팬텀 공격을 시연
'19.12.	테슬라 차량에 탑재된 카메라 데이터 관련 딥러닝 알고리즘의 취약점을 이용하여 의도적으로 오작동을 유발하는 해킹 시연

'17.04.	보쉬의 차량 진단용 OBD(On-Board Diagnostics)의 취약점을 이용하여 블루투스 범위 내에서 차량의 엔진을 멈출 수 있는 취약점 발견
'15.07.	크라이슬러 지프체로키의 커넥티드 시스템의 취약점을 이용하여 원격으로 차량제어권을 탈취하여 원격 조정을 시연, 140만 대 리콜

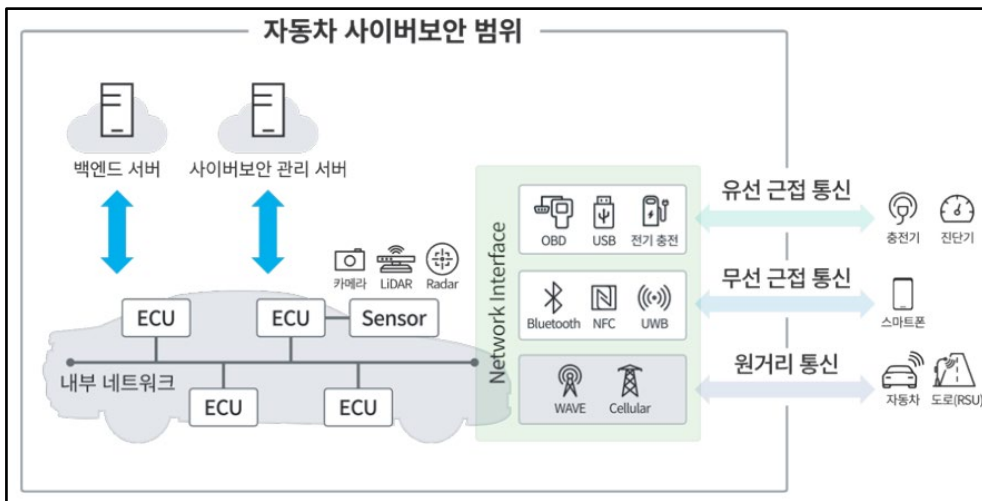
[표1] 자동차 모의해킹 시연 사례

(출처: 국회입법조사처_자동차 해킹방지를 위한 사이버보안 기준 수립 현황과 과제 22.12.28)

나) 자동차관리법 개정배경

이에 따라 2015년부터 자동차 사이버보안에 대한 연구가 본격화되었고 2020년 6월 WP.29 총회에서 자동차 사이버보안 기준(UNR NO. 155)이 채택되었습니다. 주요 내용은 자동차 제작사들은 차량 사이버보안 관리를 위한 사이버보안관리체계(CSMS: Cyber Security Management System)를 갖추고 차량 형식에 대한 위험 평가 및 관리를 수행하며, 승인/시험 기관은 제작사가 CSMS를 갖춘 경우 인증서발급, 차량 위험평가 관리가 적절할 경우 형식승인을 하는 것입니다.

그리고 지난 1월 25일 '자동차관리법' 개정안이 국회 본회의를 통과하였습니다. '자동차관리법' 개정안은 자동차 제작사의 사이버보안 및 소프트웨어 업데이트 안전관리 조치를 의무화하는 것으로서, 2020년 국제 자동차 사이버보안 국제 표준¹을 반영하는 제도적 기반을 마련한 것입니다.



[그림 1] 자동차에서 사이버보안 고려 환경(출처:국토교통부 자동차 사이버보안 가이드라인)

2. 주요내용

가) 자동차 사이버보안 관리체계 인증제도 도입

개정안에서는 자동차 사이버보안 관리체계를 위한 자동차 제작사의 의무와 국토교통부의 권한을 각각 정의하였습니다. 사이버보안 관리체계는 자동차 제작부터 폐차할 때까지 자동차 생애주기에 걸쳐 사이버 위협 요소를 상시 모니터링하고 위협 발생 시에는 이에 신속히 대응하기 위한 조직/수단/절차 일체를 포함합니다.

¹ 자동차 사이버보안 관련 국제 기준 UN Regulation 155/166, 자동차 국제기준 제정기구(UNECE WP.29)

'△자동차 제작사'는 자동차 제작에 앞서 사이버보안 관리체계를 구축하여 국토교통부 인증을 획득해야 하고, 인증사항 변경 시 변경인증을 받아야 할 의무가 있습니다. '△국토교통부'는 제작사의 사이버보안 관리체계가 적절하게 수립되었는지를 확인/인증하고 인증후에도 관리체계의 안전성/신뢰성을 확인하기 위해 관련 자료 제출을 요구하고 기준에 부적합 확인 시 인증취소나 효력정지를 할 수 있습니다.

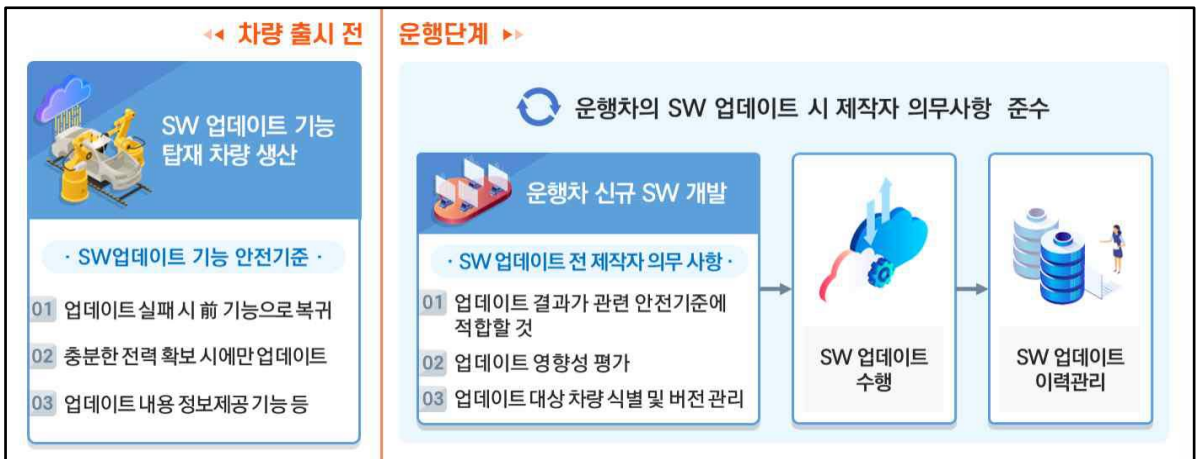


[그림2] 자동차 사이버보안 제도 체계(출처:국토교통부)

나) 소프트웨어 업데이트 안전관리 조치 의무화

자동차 제작사가 소프트웨어 업데이트를 통해 성능개선 등을 목표로 하는 경우, 안전성을 보장해야 합니다. 즉, 제작사는 업데이트 이전에 해당 장치 및 기능이 정상적으로 작동하고 안전기준에 부합하는지 확인하며, 업데이트 시에는 사용자에게 관련 정보를 공지하고 보안 및 안전성을 확보해야 합니다.

국토교통부는 소프트웨어 업데이트에 대한 제작사의 이행 여부를 성능시험대행자(한국교통안전공단)를 통해 조사하고, 부적절한 업데이트에 대해서는 시정조치를 명할 수 있다. 따라서 소프트웨어 업데이트는 안전성 확보를 위한 제작사의 책임 아래 이루어져야 하며, 정부는 그 이행 여부를 철저히 검토하여 필요 시 조치를 취할 수 있습니다.



[그림3] 자동차 소프트웨어 업데이트 제도 체계(출처:국토교통부)

다) 자동차 사이버보안 제도화 로드맵(국제기준 포함)

2024년 7월 EC유럽연합과 일본에서는 모든 신차에 자동차사이버보안을 적용할 예정이며, 국내 자동차 사이버보안은 자체적인 자기인증 방식을 유지하며 자동차 관리법 하위법령 개정, 자동차 사이버보안 안전기준 마련 등을 통해 추진될 예정입니다. 참고로 국내에서는 2020년 자동차 사이버보안 가이드라인이 제정되었으나, 2024년 자동차 관리법이 개정되면서 사이버보안체계가 의무화될 수 있는 기반이 본격적으로 마련되었습니다. 이를 통해 앞으로 자동차 사이버보안 관련 하위법령이 개정되고, 2027년부터는 국내의 모든 자동차에 사이버보안 체계가 적용될 것으로 예상됩니다.

	~ 2017년	2018년	2019년	2020년	2021년	2022년	2023년	2024년
UN WP.29 CS/OTA (사이버보안)	사이버보안 기술 권고안 * 사이버보안 원칙, 위협 완화방안			자동차 사이버보안 기준 (UN Reg. No.155) 채택('20.6)	국제기준 발효('21.1)	세계기술기준(GTR) 논의		
		(부록) 사이버보안 기준안 (형식승인)	테스트단계 검증					
국내 제도화		자동차 사이버보안 지침 세미나 ('19.11)		자동차 사이버보안 가이드라인 ('20.12)	자동차관리법 개정	하위법령 개정	자동차 사이버보안 법규/안전기준 시행 추진	
미 국	첨단 자동차를 위한 사이버보안 모범사례('16.10)				GTR 논의 참여			
EC 유럽연합						신 차종 대상 ('22.7)		모든 신차 대상 ('24.7)
일본					자율주행자동차 대상('21.1)	신 차종 대상 ('22.7)		모든 신차 대상 ('24.7)

[그림4] 자동차 사이버보안 제도화 로드맵(출처:국토교통부 자동차 사이버보안 가이드라인)

3. 시사점

자동차의 전자제어장치가 늘면서 자동차 사이버보안 취약점과 위협이 증대되고 있습니다. 해외에서는 2020년 자동차사이버보안 기준(UNR NO.155)의 제정에 따라 사이버보안체계 수립이 진행되었음에 반해, 국내에서는 그간 제도화가 지연되었으나 금번 개정된 자동차 관리법이 자동차 사이버보안관리체계 의무화와 소프트웨어 업데이트 의무화를 명문화하였습니다. 자동차산업의 사이버보안체계의 수립은 국민의 생명과 안전을 위해 필수적이며 이와 더불어 자동차 프라이버시 정책 또한 국제적으로 이슈가 되고 있는 만큼 추가 입법 및 국내/외 업계 동향을 살펴볼 필요가 있습니다.

화우 정보보호센터는 오랜 경험과 축적된 노하우를 기반으로 기업 고객을 위한 최적의 솔루션을 안내해 드리고 있습니다. 정보보호 관련 법령의 해석 및 그 대응과 정보보호 기술적 자문(해킹 진단, 보안취약점) 등 포괄적인 올인원(All-in-One) 서비스를 제공하고 있습니다. 관련하여 문의사항이 있으신 경우 언제든지 화우에 연락하여 주시기 바랍니다.

Contacts

이근우

파트너변호사

T. (+82) 2 6003 7558

E. klee@hwawoo.com

이광욱

파트너변호사

T. (+82) 2 6003 7535

E. kwlee@hwawoo.com

이수경

파트너변호사

T. (+82) 2 6182 8132

E. sgyi@hwawoo.com

정호선

변호사

T. (+82) 2 6182 8548

E. junghs@yoonyang.com

백재환

전문위원

T. (+82) 2 6182 8366

E. jhb@hwawoo.com

지재원

연구위원

T. (+82) 2 6003 7568

E. jwji@yoonyang.com