한국ITS학회논문지 J. Korea Inst. Intell. Transp. Syst.

자율협력 주행 도로교통 보안기관 설립 및 운영을 위한 방안 연구

A Study on the Establishment and Operation of Autonomous Cooperative Road Traffic Security Institutions

김 모 세* · 김 기 천**

* 주저자 : 건국대학교 컴퓨터공학과 석사과정
** 교신저자 : 건국대학교 컴퓨터공학부 교수

Mose Kim* · Keecheon Kim*

* Dept. of Computer Engineering, Konkuk University

† Corresponding author : Keecheon Kim, kckim@konkuk.ac.kr

Vol. 22 No.1(2023)
February, 2023
pp.208~218

pISSN 1738-0774
eISSN 2384-1729
https://doi.org/10.12815/kits.2023.22.1.208

Received 5 December 2022
Revised 8 December 2022
Accepted 13 December 2022

요 약

자율주행 자동차에 대한 연구가 활발하게 진행되고, 상용화를 위한 시도가 각 나라에서 진행되고 있다. 우리나라에서도 자율협력 주행의 상용화를 위해 국토교통부의 주관하에 인프라 구축 사업이 진행되고 있다. 자율협력 주행을 위한 안전한 인프라 구축을 위해서는 인프라를 구성하는 요소에 대한 보안 운영을 담당하는 보안 기관의 존재가 필수적이다. 하지만 현재 한국에 해당 역할을 진행할 수 있는 도로교통 보안기관이 존재하지 않는다. 본 논문에서는 도로교통 보안 기관 설립 및 운영방안을 마련하기 위해 현재 운영 중인 국내의 다른 보안 기관 그리고 관련 법안 정보통신기반 보호법과 주요 정보통신 기반시설 보호지침을 분석하고, 이를 분석한 결과를 바탕으로 C-ITS의 체계에 적절하게 현행법의 수정 방향을 제시하여, C-ITS 도로교통 보안 기관 설립 및 운영방안을 제안한다.

핵심어 : 자율협력주행, C-ITS, 보안 기관

ABSTRACT

Research on autonomous vehicles is being actively conducted, and the effort to commercialize them is underway in several countries. In Korea, platform construction projects are being carried out under the supervision of the Ministry of Land, Infrastructure, and Transport to achieve autonomous cooperative driving. To enable a flawless infrastructure, there is a requirement to build a safe security agency responsible for the secure operations of the entire process. However, there is no traffic ISAC in Korea that performs these roles. This paper analyzes related bills and acts of the other domestic security institutions currently in operation. Based on these results, we suggest appropriate directions to modify the current laws related to the C-ITS system. Finally, we propose a suitable plan to establish and operate a C-ITS ISAC.

Key words : Cooperative autonomous driving, Coperative Intelligent transport systems, ISAC

Ⅰ. 서 론

1. 개요

현재 산업계 및 학계에서 자율주행 자동차에 대한 관심도가 꾸준히 증가함에 따라 국내외 기업들과 더불어 국가에서도 자율주행을 진행하기 위한 사업을 진행하고 있다. 완전한 자율주행을 위해서는 결국 네트워크 기술이 핵심기술로 작용해야 한다. 자율주행 및 협력 주행 기술은 자동차를 비롯해 도로 위의 모든 인프라와 양방향 통신을 진행하는 [1]V2X 기술이 필요하다. 도로 위의 인프라와 더불어 차량이 진행하는 통신에 대한 보안은 사람의 생명에 직접적으로 연결되어 있기 때문에 철저하게 관리되어야 한다. 하지만 현재 국내에는 도로교통을 위한 보안 기관은 존재하지 않는다. 이러한 문제를 해결하기 위해 현재 국토교통부는 도로교통 보안 기관을 설립하기 위한 기준을 만들어가고 있다(NIS, 2021). 본 논문에서는 도로교통 보안 기관 설립 및 운영을 위해 국내의 다른 보안 기관 분석 및 국내 법안을 분석하여 도로교통 보안 기관의 설립 방안을 도출하고자 한다.

Ⅱ. 국내 현황분석

1. 국내 보안 기관 분석

보안 기관은 정보통신 기반 보호법 제16조에 의거하여 설립되어 주요 정보통신기반시설에 대한 취약점 분석 및 대응 체계에 대한 운영을 하여 침해 사고 발생 시 취약점 및 침해요인과 이에 대한 대응 방안 및 각종 정보를 제공하여 주요정보통신기반시설에 대한 취약점분석 평가 및 보호 대책 수립 업무를 수행한다. 국내의 대표적인 보안 기관으로 의료 [2]ISAC과 금융보안원이 존재한다. 의료 시스템과 금융 시스템은 많은 차이를 가지고 있고, 그에 따라 갖는 특징 또한 다르다. 그렇기 때문에 분야별 특징을 활용하여 그에 맞는 보안 시스템을 가지고 보안 기관을 운영한다. 각 분야에 활용되는 시스템을 분석해보고 C-ITS를 위해 설립하고자 하는 보안기관도 다른 보안기관과 마찬가지로 안전한 운영을 위해 설립해야 하는 보안 기관의 특징을 분석해보고자 한다.

1) 의료 ISAC

의료 ISAC은 정보통신기반 보호법제16조(정보공유 및 분석센터)에 따라 의료분야 정보보호의 강화를 위하여 공동보안관제센터가 설립되었다.의료 ISAC에서는 회원기관의 정보시스템에 대한 사이버 침해 대응 보안 관제 서비스를 제공한다. 제공되는 서비스로는 보안 로그분석, 네트워크 트래픽 분석, 웹페이지 모니터링 등이 있다. 또한, 사이버 위협 정보공유를 통해 침해사고 및 최신 위협에 대응을 진행하고, 침해사고 발생 시 긴급조치 지원 및 복구 지원을 통해 대응한다. 이러한 과정을 원활하게 진행하기 위해서 정보보호 핵임자는 모의 훈련 및 교육을 통해 보안기관의 운영을 한다. 또한, 보안관제 맞춤형 보고서 작성을 위해 신청기관에서 매월 발생하는 보안위협에 대해 심층 분석을 진행하고 그 중 유효한 보안 위협에 대해 기관이 실질적으로 조치할 수 있는 대응 가이드와 국내외 보안위협 동향 및 의료 센터 전체에서 탐지된 보안 위형베 대해 사전 예방을 위한 대응 가이드를 제공한다(MOHW, 2019).

1) V2X: Vehicle to Everything
2) ISAC: Information Sharing & Analysus Center(공동보안관제센터)

2) 금융보안원

다른 보안기관인 금융보안원은 금융보안 관제를 진행하는 곳으로 빅데이터 기반 보안 관제 기법을 통해 금융권에 대한 사이버 위협을 탐지 및 방지한다. 금융보안원은 사이버 위협에 대응하기 위해 각각의 사이버 위협을 탐지하고 분석하여 연계 기관에 실시간으로 정보를 공유한다. 금융권에 사이버 공격이 발생한 경우 분석을 위해 증거 수집 및 디지털 포렌식을 통해 사고의 원인을 조사한 후, 피해의 확산과 재발을 방지하기 위해 각각 기관들이 대응 방안을 수립하는 것을 도와준다. 또한, 취약점 분석 및 평가 진행을 위해 금융권에서 사용되는 네트워크 장비, 웹 애플리케이션 등의 다양한 정보시스템에서 발생할 수 있는 취약점을 발견하고 분석하여 침해 사고를 방지한다(FINANCIAL SECURITY INSTITUTE, 2019). 이러한 절차와 대응 방안을 가지고 있는 의료 ISAC과 금융보안원을 벤치마킹하여 도로교통을 위한 보안 기관을 설립하여야 한다.

3) 한국인터넷진흥원 사이버 침해대응본부

한국인터넷진흥원의 사이버침해 대응 본부는 정보보호 기반의 안전한 서비스 제공을 위해 사이버 위협에 대해 예방 및 공격 대응 체계를 강화하고 국내외 유관 기관 및 협력 기관에 정보를 공유한다. 한국 인터넷 진흥원의 사이버 침해 대응 본부는 앞서 언급한 정보보안 서비스를 위해 정보보호 침해사고에 대한 대응, 분석, 예방 작업 및 위협 정보 공유・협력을 진행한다. 각각의 작업별 세부 사항은 다음과 같다. 365일 24시간 신속한 인터넷 침해사고 대응을 위한 종합상황실 운영과 인터넷 이상징후 모니터링을 하고, 해킹, 랜섬웨어 등 침해사고 원인 분석 및 확인된 악성 사이트 차단을 통한 피해 확산·재발 방지를 위한 기술지원을 진행한다. 또한, 위협 정보의 공유・협력을 위해 여러 산업 분야에서 수집된 정보의 공유를 기반으로 주변 기관 및 협력 기관 사이버 위협 AI·빅데이터의 분석 및 공동활용체계 구축한다(KISAInsight, 2021).

2. 국내 법안 분석 및 개선안 도출

지능형 도로교통 기관의 운영을 위한 보안 기관은 주요 정보 통신 기반 시설에 해당한다. 따라서 과기정통부 소관의 정보통신기반 보호법과 국토교통부 소관의 주요 정보통신 기반 시설 보호지침의 내용을 준수하여 설립 및 운영이 이루어져야 한다.

1) 과기정통부 소관 정보통신기반 보호법

과기정통부 소관 정보통신기반 보호법은 다음과 같은 목적으로 제정되었다. “이 법은 전자적 침해행위에 대비하여 주요 정보통신 기반 기설의 보호에 관한 대책을 수립 및 시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민 생활의 안정을 보장하는 것을 목적으로 한다.” 정보통신기반 보호법은 앞서 언급된 바와 같이 전자적 침해행위에 대비하여 주요 정보통신기반시설의 보호에 관한 방안을 시행하기 위해 규정되고 있다(Ministry of science and ICT, 2020). C-ITS 체계를 완성하는 V2X 시스템에서 차량은 주행하면서 중앙 인프라 및 현장 인프라를 구성하는 기반 시설들과 실시간으로 양방향 통신을 통하여 안전한 자율협력 주행이 이루어지기 때문에 C-ITS를 구축하는 기반 시설은 정보통신기반시설로서 안전한 자율협력 주행 도로교통 체계를 위해서 정보통신기반 보호법을 기반으로 구성 시설에 대한 보호가 이루어져야 한다.

<Table 1> Act on the protection of information and communications infrastructure

Article	Detail
1	“The purpose of this Act is to operate cirtical information and communications infrastructure in a stable manner by formulating and implementing measures concerning the protection of such infrastructure, in preparation for intrusion by electronic means, thereby contributing to the safety of the nation and the stability of the life of people.“

2) 국토교통부 소관 주요정보통신기반 기반시설 보호지침

국토교통부 소관의 주요정보통신 기반시설 보호지침은 다음과 같은 목적으로 제정되었다. “이 지침은 정보통신기반 보호법 제10조에 따라 국토교통부장관이 관할하는 주요 정보통신 기반시설을 각종 전자적 침해행위로부터 보호하기 위하여 해당 주요정보통신기반시설 관리 기관의 장이 준수하여야 할 정보보호에 관란 구체적 사항을 목적으로 한다.” 주요정보통신기반시설 보호지침은 앞서 언급된 바와 같이 전자적 침해행위에 대비하여 해당 주요정보통신기반시설 관리기관의 장이 준수하여야 할 정보보호에 관한 구체적 사항을 시행하기 위해 규정되고 있다(MOLIT, 2020). 과기 정통부 소관 정보통신기반 보호법과 마찬가지로 안전한 C-ITS 인프라를 구축하기 위해 기반시설의 보호지침이 필수적으로 요구된다.

<Table 2> Guidelines for protection of Information and communication infrastructure

Article	Detail
1	“The purpose of this guideline is to prescribe specific matters concerning information protection to be observed by the head of the relevant management agency in order to protect the information and communication infrastructure under the Minister’s jurisdiction from various electronic infringement“

3) 국내 법안 개선방안 도출

기존 국토교통부 소관의 보호지침체는 C-ITS의 자율협력주행도로교통의 안전한 운행을 위한 보안기관의 기준이 존재하지 않는다. 그렇기 때문에 앞서 언급한 정보통신기반 보호법과 주요정보통신기반시설 보호지침을 참고하여 상위법인 정보통신기반 보호법 보다 보안기관 설립 및 운영에 직접적인 영향을 주는 주요정보통신기반 시설 보호지침을 C-ITS의 자율협력주행 도로교통의 특징을 위해 법안의 개선 방향을 제시하고자 한다. 현재 국토교통부 소관 주요정보통신 기반 시설 보호지침의 보호 체계에 대해 언급하는 제4조에는 C-ITS의 특성상 차량을 포함한 V2X 체계를 구성하는 모든 기반 시설과 양방향 통신을 하면서 자율 협력 주행을 하므로 C-ITS를 구성하는 인프라 시설마다 각기 다른 보호 대책이 필요하다. 즉, “각 인프라 별 보호 대책”이 존재해야 한다. 제7조에는 정보보호책임자의 지정에 관한 내용이 언급되고 있다(Seoul Facilities Corporation, 2021). C-ITS의 특성상 국민의 안전확보가 최우선적으로 이루어져하기 때문에 C-ITS의 보안 담당 즉 “정보보호책임자의 권한 및 책임”에 대한 상세 내용을 규정해야 한다. 보호지침의 지정 및 취약점 분석 부분에서 제14조와 관련하여 취약점 전담반의 구성원 및 역할, 기준에 언급한다. 하지만, 현재 명시되어 있는 자격 기준으로는 C-ITS를 위한 원활한 수행을 진행할수 있다고 보기 힘들다. C-ITS 서비스를 제공하기 위해 국가에서 채택하고 있는 통신기술에는 무선랜 IEEE 802.11p 와 하이브리드 V2X 통신을위한 I5S-G5, 고속 모바일 애플리케이션 기술을 기반으로 하고 있으며 계속해서 새로운 프로토콜이 등장하고 있다. 이 외에도 차량과 통신을 하기 위한 IoT 기기 및 5G 네트워크에 사용될 프로토콜에 대한 이해가 담당자에게 필수적으로 요구될 것이다. 네트워크 뿐만 아니라 C-ITS에서의 서버 또한 기존의 방식이 아닌 짧은 시간 안에 자율주행 자동차의 요청에 회신을 줄 수 있는 연산이 요구되며 이를 충족하기 위해 각 기지국의 세분화된 서버

에서 에지 컴퓨팅을 수행하고 이를 중앙에서 관리할 서버로 클라우드가 채택될 가능성이 높기 때문에 구종 기술 보유자로는 C-ITS 환경에 필요한 요구를 충족시키기 힘들며, 이에 따라 새로운 자격 기준이 마련되어야 한다. 마지막 항목으로 보호 및 침해사고의 대응 부분 관련하여 보호지침 제20조 제1항의 내용에 C-ITS의 측성을 고려하여 침해 사고 발생 시 사고의 통지가 인프라를 구성하는 모든 기반 시설에 통지되어야 한다. 즉, “침해 사고 통지의 범위 확대” 및 “빠른 전달을 위한 기반 시설 간에 연락망 구성”이 필요하다.

<Table 3> The improvement of domestic guideline

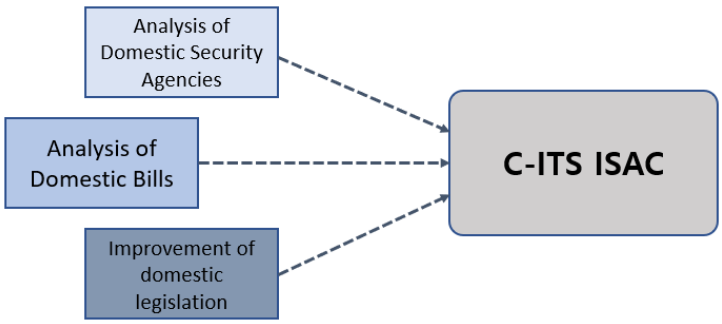
Article	Details
4	Guidelines for protection of information and communication infrastructure
7	Designation of the manager of information protection
20	Notification of the infringement accident

Ⅲ. 도로교통 보안기관 설립 및 운영

1. 도로교통 보안기관 설립 및 운영방안

1) 도로교통 보안기관 설립의 타당성

자율협력 주행을 위한 기술 및 정책의 개발이 계속해서 진행되고 있다. 자율협력 주행 시스템을 완성하기 위헤서는 C-ITS 인프라의 구축이 필수적이다. 각각의 인프라는 V2X 시스템을 구성하는 기반 시설로 도로 위의 차량과 직접적인 통신 연결을 통해 자율협력 주행이 진행된다. 자율협력 주행은 사용자의 안전과 직접적으로 연결되기 때문에 시스템 운영을 위한 보안체계가 존재해야만 하고, 보안체계에 대해 시스템을 정의하고 운영을 할 수 있는 기관이 필요하다. 본 논문에서 이러한 역할을 진행하는 도로교통 보안기관의 설립 및 운영방안을 제안하고자 한다.



<Fig. 1> Establish of C-ITS ISAC

2) 도로교통 보안기관 설립 및 운영방안

정보통신기반 보호법에 따라 관리기관 업무의 절차는 1)정보통신기반시설지정, 2)취약점 분석 및 평가, 3) 보호대책 계획 수립, 4) 보호대책 이행점검 순으로 이루어진다. 이때 C-ITS 도로교통의 보안기관의 설립 및 운영은 관리기관과 유사하게 1) 취약점 분석, 2) 보호대책 계획수립, 3) 보호대책 이행점검 순으로 업무절차

가 진행된다. 본 논문에서는 2장에서 언급한 “정보통신기반 보호법”과 국토교통부 소관 “주요정보통신기반시설 보호지침”을 기반으로 C-ITS 도로교통 보안기관의 운영을 위한 고시안을 제시한다(NIS, 2019). 보안 기관의 운영을 위해서는 크게 4가지 항목이 필수적으로 요구된다. 기반 시설에 대한 기준 및 보안 점검 사항, 보안담당자(정보보호책임자)의 업무, 보안 위협 사항에 대한 대처, 마지막으로 보안 침해 사고에 대한 대응이다. 이렇게 4가지 항목에 관한 사항이 정의되어야 보안 기관의 정상적인 운영이 가능해진다. 후에 각 보안 기관 별 특성에 따라 다른 항목에 대해 추가가 가능하다. 본 논문에서 제시하는 고시안은 C-ITS를 위한 도로교통 환경의 보안 기관의 설립 및 운영에 목적을 두고 있다.

도로교통 보안 기관의 운영을 위한 사항 중 기반 시설 기준 및 보안 점검 사항에서는 자율주행 기반 시설에 대한 기준과 보호대책의 포함 사항이 포함되어야 한다. 해당 내용은 본 논문에서 제안하는 고시안의 제1조 및 제2조에 포함된다.

제1조(자율주행 기반 시설 기준) “자율주행 기반시설의 보안을 담당하는 기관은 자율주행과 관련이 있는 법인, 기관, 또는 단체, 다체 기관의 보안을 위하여 수행되어야 하는 기준을 제시 및 실행하는 기관(이하 ”보안기관“ 이라 한다)으로서 자율주행에 관련된 기반 시설들은 다음 각 목의 기준이 맞아야 한다. 다만, 특수한 경우에는 국토교통부 장관이 정하는 바에 따라 다음 각 목의 기준 중 일부 기준을 면제할 수 있다.”제1조에 포함된 각 호는 다음과 같다. <가> 보안기관은 자율주행과 관련된 기반 시설의 보안 기준 제시 및 검증을 위한 기관일 것. <나> 국제적 기준에 맞는 보안시스템을 구축 유지할 것. <다> 보안 업무에 필요한 시설, 검사 장비 보관시설을 갖출 것. <라> 자율주행 기반시설의 보안 기준 시험 항목 및 자율주행 기반 시설의 보안 검사를 할 수 있는 장비를 갖출 것. 제2조(보호대책 포함사항) “보안 기관에서의 기관의 장(이하 ”보안 기관의 장“이라 한다)의 업무는 자율주행 기반시설의 보안 관련 기관시설 및 관리 정보를 안전하게 보호하기 위한 예방, 백업 복구 등 물리적, 기술적 대책을 포함한 관리대책(이하 ”주요정보통신기반시설보호대책“이라 한다)을 수립 및 시행하여야 한다. 주요정보통신기반시설 보호 대책에는 다음 각 호의 사항이 포함되어야 한다. 제2조에 포함된 각 호는 다음과 같다. <가>.소관 주요정보통신기반시설 보호목적 및 대상 시설을 정의할 것 <나>정보보호체계 및 관리 대책을 수립할 것 <다> 취약점 분석,평가 및 점검 대책을 수립할 것 <라> 침해사고 및 재해, 재난발생시 대응 및 복구 대책을 수립할 것 <마>전자적 침해행위 예방을 위한 관리, 물리, 기술적 보안 대책을 수립할 것 <바>정보보호교육, 훈련 계획을 수립할 것 <사>그 밖에 주요정보통신기반시설의 보호를 위하여 필요한 사항을 수립할 것

<Table 4> Infrastructure criteria and security checks

Article	Details
1	Guidelines for protection of information and communication infrastructure
2	Designation of the manager of information protection

보안 담당자의 업무에는 정보보호 책임자의 자격요건 및 업무와 보안 업무 절차서에 관한 내용이 포함되어야 한다. 해당 내용은 본 논문에서 제안하는 고시안의 제3조, 제4조 및 제5조에 포함된다.

제3조(정보보호책임자의 자격요건) ”보안기관의 장은 소관 주요정보통신기반시설의 보호에 관한 업무를 총괄하는 자(이하 “정보보호책임자”라 한다)를 지정한다. 정보보호책임자의 자격요건은 제3조에 포함된 각 호에 언급된다. <가>다음의 어느 하나에 해당하는 자격을 가진 정보보호책임자를 둘 것 1)정보보호 또는 정보기술 분야의 국내 또는 외국의 석사학위 이상 학위를 취득한 사람 2)정보보호또는 정보기술 분야의 국내 또는 외국의 학사학위를 취득한 사람으로서 정보보호 또는 정보기술 분야의 업무를 3년이상 수행한 경력이

있는 사람 3)정보보호 또는 정보기술 분야의 국내 또는 외국의 전문학사학위를 취득한 사람으로서 정보보호 또는 정보기술 분야의 업무를 5년 이상 수행한 경력이 있는 사람 4)정보보호 또는 정보기술 분야의 업무를 10년이상 수행한 경력이 있는 사람 5)정보보호 관리체계 인증심사원의 자격을 취득한 사람 6)해당 정보통신서비스 제종자의 소속인 정보보호 관련 업무를 담당하는 부서의 장으로 1년이상 근무란 경력이 있는 사람. 제4조(정보보호책임자의 업무) “보안기관의 장에 의해 지정된 정보보호책임자의 업무는 다음과 같다.”<가> 주요정보통신기반시설 보호대책의 수립 및 시행 <나>주요정보통신기반시설 보호업무에 대한 기술적 지원의 요청 <다>.취약점 분석, 평가 및 전담반 구성 <라>.주요정보통신기반시설의 보호에 필요한 조치 명령 도는 권고의 이행 <마>.침해사고의 통지 <바>주요정보통신 기반시설의 복구 및 보호에 필요한 조치 <사>그밖에 다른 법령에 규정된 주요정보통신기반시설의 보호 업무에 관한 사항. 제5조(보안 메뉴얼 및 업부 절차서) “보안 기관에서의 업무는 자율주행 기반 시설의 보안 관련 업무수행에 대한 기술적인 사항을 총괄 관리하는 정보보호책임자의 주도하에 보안시스템의 이행과 유지 등에 필요한 사항을 기술한 문서(이하 ”보안 메뉴얼“ 이라 한다)와 보안 업무의 업무별 운영, 수행 및 관리 등의 절차를 제공하는 문서(이하”업무 절차서“ 이라 한다.)를 활용하여 진행되어야 한다.” 제5조에 포함된 각 호는 다음과 같다.<가>보안기관의 장은 보안기관의 운영기준에 따라 보안 매뉴얼 및 업무 절차서를 작성하여햐 하며, 관련 업무를 수행할 것. <나>정보보호책임자는 운영기준의 변경이 발생할 경우 보안 매뉴얼 또는 업무 절차서를 지속적으로 갱신할 것. <다>보안 업무 사항 중 일시적으로 보안 업무를 수행할 수 없는 경우에는 정보보호책임자 및 팀장급 담당요원에게 즉시 보고할 것. <라>보안기관의 정보보호책임자로 선임된 자는 다음 각호의 사항을 성실히 준수하여햐 한다. 1) 보안요원(팀장급 담당 보안 요원 포함) 또는 사용 종사자의 보안 업무 수행에 대한 기술적 지도와 감독을 이행할 것. 2)보안 업무 관리를 위한 기획, 점검 및 평가를 실시할 것. 3)보안 요원(팀장급 보안 요원 포함) 또는 사용 종사자에 대하여 보안에 대한 교육, 훈련을 연2회 이상 실시할 것, 다만, 보안 요원(팀장급 보안 요원 포함) 또는 상용 종사자가 국가표준기본봅 시행령에서 지정한 교육기관에서 교육을 수료한 경우 연1회 교육으로 간주할 수 있다. <마>보안 메뉴얼 및 업무 절차서에 따라 시행된 보안 업무의 결과에 관한 서류를 작성, 비치 및 보존하여야 한다.

<Table 5> The work of protection officer

Article	Details
3	Qualifications of the information protection officer
4	Duties of the information protection officer
5	Security manual and business procedures

보안 위협 사항에 대한 대처 항목에는 취약점에 대한 분석 및 평가, 침해사고의 통지와 복구 및 보호 조치에 대한 내용이 포함되어야 한다. 해당 내용은 본 논문에서 제안하는 고시안의 제6조, 제7조 및 제8조에 포함된다.

제6조(취약점 분석 및 평가) ”보안 기관의 장은 취약점 분석 및 평가를 위해 전담반을 구성하고 전담반을 구성하는 때에는 별표의 사항을 고려하여 취약점 분석 및 평가의 객관성과 실효성을 확보할 수 있도록 하여야하고, 취약점 분석 및 평가 기준에는 다음 각항의 사항이 포함되어야 한다.“ 제6조에 포함된 각 호는 다음과 같다. <가> 취약점 분석 및 평가 절차를 수립할 것. <나> 취약점 분석 및 평가의 범위 및 항목을 수립할 것. <다> 취약점 분석 및 평가의 방법을 수립할 것. 제7조(침해 사고의 통지) ” 보안 기관의 장은 6조에 뜨른 취약점 분석 및 평가를 실시한 경우에는 그 결과를 반영하여 다음 각 항의 조치(이하 “보완조치”라 한다.)를

하여야 한다. 제7조에 포함된 각호는 다음과 같다.<가> 각종 보호 조치, 절차 및 방법 등의 재검토 및 수정과 보완할 것. <나> 시설, 장비의 개축 및 보수 또는 설치할 것. <다> 그 밖에 분석, 평가 또는 점검 결과를 반영한 조치할 것. 제8조(복구 및 보호 조치) “ 보안 기관의 장은 침해 사고가 발생하여 소관 주요 정보통신기반 시설이 교란, 바비 또는 파괴된 사실을 인지한 때에는 장관, 관계 행정기관, 수사기관 또는 인터넷 진흥원(이하 ”관계기관 등“이라 한다.)에 그 사실을 통지하여야 한다.

<Table 6> Responding to security threats

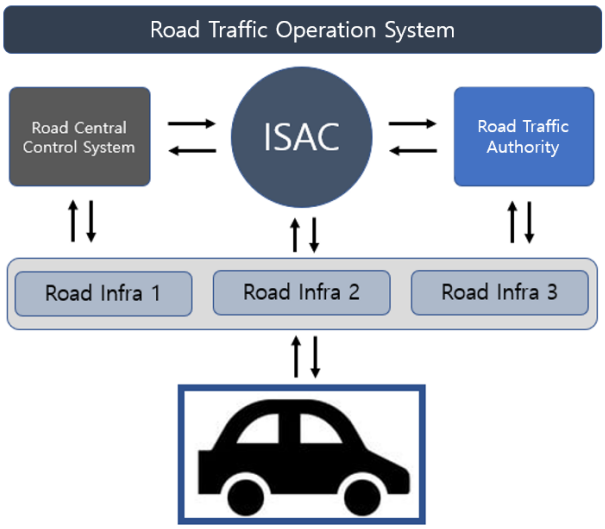
Article	Details
6	Vulnerability analysis and evaluation
7	Notice of infringement accident
8	Recovery and protection measures

보안 침해사고에 대한 대응 항목에는 침해사고에 대한 예방 대책 수립 및 대응조치, 연락체계 구축과 보안기관 장의 행동지침에 대한 내용이 포함되어야 한다. 해당 내용은 본 논문에서 제안하는 고시안의 제9조, 제10조, 제11조, 제12조, 제13조 및 제14조에 포함된다.

제9조(침해 사고 예방대책 수립) ”보안 기관의 장은 소관 주요 정보통신 기반시설에 대한 침해 사고가 발생한 때에는 해당 정보통신 기반 시설의 복구 및 보호에 필요한 조치를 신속히 취하여야 한다. 제9조에 포함된 각호는 다음과 같다. <가> 보안 기관의 장은 제1항에 따른 복구 및 보호 조치를 위하여 필요한 경우 장관 또는 인터넷 진흥원의 장에게 지원 요청 가능. 다만, 특수한 경우에는 국가정보원장에게 그 지원을 우선적으로 요청한다. <나> 장관 또는 인터넷 진흥원의 장은 <가>항에 따른 지원 요청을 받은 때에는 피해 복구가 신속히 이루어질 수 있도록 기술지원 등 필요한 지원을 하여야 하고, 피해 확산을 방지할 수 있도록 보안기관의 장과 함께 적절한 조치를 취해야 한다. 제10조(침해 사고 예방대책 수립) “ 보안 기관의 장은 주요 정보통신 기반시설 보호지침 제4조 제3항 제5호의 침해사고 예방 대책을 수립하는 경우에는 다음 각호의 사항을 고려하여야 한다.” 제10조에 포함된 각 호는 다음과 같다. <가> 시스템 네트워크 관리 및 보호대책. <나> 정보보호시스템 구축에 관한 대책. <다> 전산 자료에 대한 백업 조치 등. <라> 바이러스 방지대책. <마> 접근통제에 관한 대책. <바> 그 밖에 침해 사고 예방을 위한 대책. 제11조(연락체계 구축) “ 보안기관의 장은 소관 주요정보통신기반시설에 대한 전자적 침해 사고가 발생한 경우 신속히 대응하고 관계 기관에 알리기 위해 필요한 연락체계를 구축하여야 한다. 제11조에 포함된 각호는 다음과 같다. <가> 연락 체계에는 국토교통부 정보보호책임관과 정보통신기반 보호법 제13조에 따른 관계 행정기관, 수사기관 및 인터넷 진흥원이 포함되도록 할 것. 제12조(침해 사고 대응 조치) ” 관리기관의 지정 단위 책임자는 전자적 침해 사고의 징후가 있거나 전자적 침해 사고의 발생을 인지한 때에는 이를 즉시 정보 보호 책임자에게 보고하여야 한다.“ 제13조(침해 사고 대응 조치) ” 정보 보호 책임자는 소관 주요 정보통신 기반시설에 대한 전자적 침해사고의 발생 및 징후를 보고 받거나 인지한 때에는 이를 관리기관의 장 및 정보보호 책임관에게 즉시 보고하고 필요한 조치를 하여야 한다. 다만 교란, 마비 또는 파괴가 일어나지 않는 경미한 침해 사고의 발생 및 징후는 보고하지 아니할 수 있다. 제14조(보안 기관의 장의 행동 지침) “ 정보통신기반 보호법 제7조 제2항에 따른 국가안정보장 관련 주요 정보통신 기반시설 보안 기관의 장은 장관 및 국가 정보원장에게 전자적 침해 사고에 관한 보고사항을 신속히 통보하여야 하고, 보안 기관의 장은 제12조부터 제14조까지의 규정에 따른 사항을 포함하여 전자적 침해사고 발생에 따른 대응 절차 및 방법에 관하여 필요한 사항을 정하여야 한다.

<Table 7> Response to security incidents

Article	Details
9	Establish of measures to prevent infringement accident_1
10	Establish of measures to prevent infringement accident_2
11	Establish of a liaison system
12	Response to infringement accident_1
13	Response to infringement accident_2
14	Guidelines for the head of ISAC



<Fig. 2> Road traffic operation system with ISAC

3) 보안 기관 설립 및 운영 방안 근거 자료

보안 기관 설립 및 운영방안의 근거 자료는 다음과 같다. 보안기관 운영방안 제1조 자율주행 기반시설 기준에 <가>항은 “정보통신기반 보호법의 제8조 제1항 제1호”,<나>항은 “정보통신기반 보호법 제8조 제1항 제3호”, <다>와 <라> 항은 “주요 정보통신기반시설 보호지침의 제4조 제3항 제5호”를 참고하였다. 운영방안 조항 제2조 보호대책 포함사항의 <가>, <나>, <다>, <라>, <마>, <바>, <사> 항은 “주요정보통신기반시설 보호지침 제4조를” 참고하였다. 운영방안 조항 제3조 정보보호책임자의 자격요건에 <가>항은 “정보통신망이용촉진 및 정보보호 등에 관한 법률 시행령 제36조의7 제2항”을 참고하였다. 운영방안 제4조 정보보호책임자의 <가>, <나>, <다>, <라> ,<마>, <바>, <사>항은 “주요정보통신기반시설 보호지침 제7조”를 참고하였다. 운영방안 제5조 보안 메뉴얼 및 업무 절차서의 <가>, <나>, <다>, <라>, <마>항은 “주요정보통신기반시러 보호지침 제18조”를 참고하였다. 운영방안 제6조 취약점 분석 및 평가의 <가>, <나>, <다> 항은 “주요정보통신기반시설 보호지침 제14조”를 참고하였다. 운영방안 제7조 침해사고의 통지의 <가>, <나>, <다> 항은 “주요정보통신기반시설 보호지침 제16조”를 참고하였다. 운영방안 제8조 복구 및 보호 조치는 “주요정보통신기반시설 보호지침” 제 20조를 참고하였다. 운영방안 제9조 침해사고 예방대책 수립의 <가>, <나> 항은 “주요정보통신기반시설 보호지침 제20조”를 참고하였다. 운영방안 제10조 침해사고 예방대책 수립의 <가>, <나>, <다>, <라>, <마>, <바> 항은 “주요정보통신기반시설 보호지침 제 22조”를 참고하였다. 운영방안 제11조 연

락체계 구축의 가항은 “주요정보통신기반시설 보호지침 제23조”를 참고하였다. 운영방안 제12조,제13조 침해사고 대응 조치와 제14조 보안기관의 장의 행동지침은 “주요정보통신기반시설 보호지침”을 참고하였다.

<Table 8> The establish and operation system of road traffic ISAC

Article	Details
1	Autonomous driving infrastructure criteria
2	Protective measures
3	Qualifications of the information protection officer
4	Duties of the information protection officer
5	Security manual and business procedures
6	Vulnerability analysis and evaluation
7	Notice of infringement accident
8	Recovery and protection measures
9	Establish of measures to prevent infringement accident_1
10	Establish of measures to prevent infringement accident_2
11	Establish of a liaison system
12	Response to infringement accident_!
13	Response to infringement accident_2
14	Guidelines for the head of ISAC

Ⅴ. 결 론

C-ITS 자율협력 주행 도로교통 체계를 위한 보안 기관의 설립 및 운영방안 마련을 위해 국내 타 보안 기관을 분석하여 각 시스템 별 필요한 보안 요구사항 및 안전한 운영방안에 대하여 분석을 진행하였고, 국내 관련 법안인 과기정통부 소관 정보통신기반 보호법 및 국토교통부 소관 주요 정보통신기반시설 보호지침의 분석 및 C-ITS 도로교통 체계를 위한 개선안을 도출하여 도로교통 보안 기관의 운영 및 설립 방안에 대해 제안하였다. 다만, 운영방안 고시안의 경우 실질적인 기관의 운영을 진행하면서 실무에 필요한 사항들을 추가해야 한다. 즉 실제로 운영되는 보안 기관의 실정에 맞춰서 해당 운영방안의 개선이 필요하다(NIS, 2020).

C-ITS를 위한 보안 기관의 설립은 단순히 기관의 운영 측면뿐만 아니라, 다양한 방면에서의 긍정적인 효과를 불러올 것이다. 보안 기관 설립의 긍정적인 효과는 크게는 국가의 안전과 국민의 안전부터 기관의 운영 및 기술적, 경제적 효과까지 기대할 수 있다(KISA, 2019b). 운영적인 측면에서는 보안 기관을 통하여 탐지 및 대응의 효율성을 극대화하고 침해 사고의 신속한 공유를 통해 피해 확산의 예방이 가능하다. 또한, C-ITS에 적합한 정보보호 관리체계 수립을 통하여 정보보호 수준 향상 및 보안 강화 유도와 도로에서 발생하는 보안 사고에 대한 즉각적인 대응이 가능하다. 기술적인 부분에서는 전문화된 보안기관을 통해 보안 사각지대 해소와 보안 사고 예방 및 피해 최소화가 가능하다(KISA, 2022). 경제적인 효과로는 정보서비스에 대해 안전이 보장된 서비스 제공을 위한 기반 조성을 통해 국민의 신뢰도가 향상되고, 안전한 C-ITS를 통해 사고 발생이 줄어서 그에 대한 재산 및 인명 피해가 최소화된다(KISA, 2019a). 마지막으로 C-ITS의 보안 안전성의 확보를 통한 자율주행 시장의 이용률이 증가할 것이다.

ACKNOWLEDGEMENTS

본 연구는 국토교통부 교통 물류 연구사업의 연구비 지원(22TLRP-B155270-0420682073250004)에 의해 수행되었습니다.

REFERENCES

Financial Security Institute(2019), *Financial Security Agency Introduction*, p.3.

Korea Internet & Security Agency(KISA)(2019a), *Smart Traffic Cyber security*, pp.1-10.

Korea Internet & Security Agency(KISA)(2019b), *System Guide for designation and reporting of chief information protection officer*, pp.3-19.

Korea Internet & Security Agency(KISA)(2022), *Domestic and Foreign Location Information Industry Trend Report*, pp.1-12.

Korea Internet & Security Agency(KISA)Insight(2021), *A Study on the Spread and Security Issues of the Virtual Convergence Economy*, p.6.

Ministry of Health and Welfare(MOHW)(2019), *Introduction of Medical ISAC*, p.6.

Ministry of Land, Infrastructure and Transport(MOLIT)(2020), *Guidelines for Protection of Major Information and Communication Infrastructure*, p.1.

Ministry of Science and Information & Communications Technology(ICT)(2020), *Information of Communication Infrastructure Protection Act*, p.1.

National Intelligence Service(NIS)(2019), *National Information Protection White Paper*, p.20.

National Intelligence Service(NIS)(2020), *National Information Protection White Paper*, p.8.

National Intelligence Service(NIS)(2021), *National Information Protection White Paper*, p.13.

Seoul Facilities Corporation(2021), *Information Security Promotion Plan*, pp.1-14.