자율협력주행 인증관리기준 제정안

1. 제정이유

자율협력주행 환경에서 차량 및 인프라는 해킹, 개인정보 침해, 데이터 오전송 등 다양한 통신 위협에 노출되어 있어 보안성 확보가 필요함에 따라, 인증서가 발급된 차량 및 인프라만 통신을 허용하기 위하여 인증관리체계를 구축하고, 인증업무의 방법·절차, 인증기관 시설기준, 인증서 유효기간 등 자율협력주행 인증업무에 관한 사항을 세부적으로 규정하고자 함

2. 주요내용

가. 인증관리센터·인증기관·검증기관의 업무 및 역할 규정(안 제4조부터 제7조)

- 인증관리센터는 인·검증기관의 인증서 발급·관리, 정보 및 기록 유지, 인증업무 관련 교육 등의 역할 규정
- 인증기관은 가입자 인증서의 발급·갱신·폐지, 인증서 유효성 확인, 소속기관 업무 실태점검 및 개선사항 권고 등 업무 수행, 인증기관·인증업무준칙 등 정보 공고, 인증업무에 관한 기록 보관·관리 등 의무
- 검증기관은 이상행위정보를 분석·검증, 이상행위정보·기록 관리

나. 가입자 관련 사항(안 제8조, 제18조 및 제19조)

- 인·검증기관은 가입자 정보를 보호할 의무
- 가입자는 인증서 발급·재발급·폐지 신청 또는 정보변경 시 인증기관에

정확한 정보제공 의무

- 허위 또는 잘못된 정보제공 시 발생하는 손해·손실 책임

다. 자율협력주행 인증협의회 구성·운영(제11조)

- 인증업무 운영을 위한 정책, 제도개선·정비, 기관 간 상호연계 등 협의

라. 자율협력주행 인증서(안 제13조부터 제15조)

- 인증서의 종류를 인증업무 수행기관용 인증서, 등록인증서, 보안인증서로 구분하고, 인증서의 유효기간 및 효력을 규정

마. 자율협력주행 인증업무(안 제16조부터 제17조)

- 인증기관은 가입자 신원을 확인하는 절차를 거쳐야 하고, 온라인을 통해 직접 신청한 자에게 인증서 발급을 원칙으로 함

바. 시설기준 및 정보 관리방법(안 제20조 및 제21조)

- 인증기관과 검증기관이 갖추어야 하는 시설 및 장비의 세부기준
- 시설, 장비 및 정보의 안전성 확보를 위하여 취하여야 할 기술적·관리적·물리적 조치 등 관리방법 규정

3. 참고사항

가. 관계법령 : 「자율주행자동차 상용화 촉진 및 지원에 관한 법률」

나. 예산조치 : 별도조치 필요 없음

다. 합　　의 : 해당사항 없음

라. 기　　타 : 1) 제정 고시, 별첨

2) 특기할 사항 없음

국토교통부고시　제2023-433호

자율협력주행 인증관리기준

제1장　총　칙

제1조(목적) 이 기준은 「자율주행자동차 상용화 촉진 및 지원에 관한 법률」 제28조, 제30조, 제34조, 같은 법 시행령 제25조, 제26조 및 같은 법 시행규칙 제18조제2항에 따라 자율협력주행 인증업무의 안전성과 신뢰성 확보를 위하여 자율협력주행 인증관리기준의 세부사항을 정함을 목적으로 한다.

제2조(적용범위) 이 기준은 자율협력주행 인증서 발급・관리 등 인증업무를 수행하는 인증기관・검증기관과 가입자에게 적용한다.

제3조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

1. "자율협력주행 인증시스템"이란 인증기관 및 검증기관이 개발, 설치, 운영, 관리하는 전산장비, 소프트웨어, 어플리케이션, 데이터 및 이와 관련된 모든 장치를 말한다.
2. “가입자 등록정보”란 자율협력주행 인증서를 받으려는 자가 인증기관에 제출한 신청서, 신원확인을 위해 제출한 서류 및 증명서 등의 사본 그리고 기타신청에 필요한 전자적 기록 등을 말한다.
3. “자율협력주행전자서명검증키(공개키)”라 함은 자율협력주행 인증업무의 전자서명을 검증하기 위하여 이용하는 전자적 정보로 인증서

내에 포함되는 정보를 말한다.

4. “자율협력주행전자서명생성키(개인키)”라 함은 자율협력주행 인증업무의 전자서명을 생성하기 위하여 이용하는 전자적 정보로 가입자가 보유하는 정보를 말한다.

5. “인증서 폐지목록(CRL : Certificate Revocation List)”이란 인증서 효력이 상실된 인증서의 목록으로 인증기관에서 주기적으로 발급·게시하는 전자적 정보를 말한다.

6. “자율협력주행 인증업무준칙(CPS : Certificate Practices Statement, 이하 “인증업무준칙”이라 한다)”이란 「자율주행자동차 상용화 촉진 및 지원에 관한 법률」(이하 "법"이라 한다) 제31조제1항에 의해 인증기관이 자율협력주행 인증관리기준(이하 “인증관리기준”이라 한다)에 따라 작성한 문서를 말한다.

7. “이상행위정보”란 자율협력주행 인증장치의 고장 등으로 자율협력주행 과정에서 발생하는 비정상적인 정보를 말한다.

8. “이상행위보고서”란 인증기관으로부터 인증서를 발급받은 자동차 및 노변기지국이 이상행위정보로 탐지하여 검증기관에 전송하는 정보를 말한다.

제2장 자율협력주행 인증관리체계

제4조(인증관리센터의 기능) ① 법 제27조제2항 및 시행령 제23조에 의해 설치된 자율협력주행 인증관리센터(이하 "인증관리센터"라 한다)

는 자가서명(Self-signed)하여 인증서를 발급하는 자율협력주행 인증관리체계상 최상위인증기관을 말한다.

② 인증관리센터는 인증관리체계의 효율적 운영을 위해 다음 각 호의 업무를 수행한다.

1. 인증기관 및 검증기관 인증서 발급·관리 등 자율협력주행 인증업무
2. 인증기관 및 검증기관의 인증서와 인증서 폐지목록 게시
3. 인증관리센터가 생성한 모든 인증서와 인증서 폐지목록의 보관
4. 인증기관 관리에 관련된 정보 및 기록의 유지 등
5. 자율협력주행 인증관리체계에 속하는 기관 및 가입자에 대한 자율협력주행 인증업무 관련 교육
6. 법 제27조제1항에 따른 자율협력주행 인증 관련 업무
7. 기타 최상위인증기관으로서 자율협력주행 인증업무와 관련하여 필요하다고 인정되는 업무

제5조(인증기관의 역할) ① 인증기관은 다음 각 호의 업무를 수행한다.

1. 신청자 및 가입자의 신원확인
2. 신청자 인증서의 발급, 가입자 인증서의 갱신, 폐지 및 인증서 폐지목록 게시 등 자율협력주행 인증업무
3. 해당 인증기관에서 발급한 인증서의 유효성 확인
4. 가입자 정보 및 기록에 대한 관리
5. 인증업무의 안전성과 신뢰성을 확보하기 위한 소속기관의 업무 운영 실태점검 및 개선사항 권고

6. 기타 인증기관으로서 필요하다고 인정되는 업무

② 인증기관은 인증관리센터에서 발급한 인증서를 이용하여 자율협력주행 인증업무를 수행하여야 한다.

제6조(인증기관의 책임과 의무) ① 인증기관은 인증서의 신뢰성이나 유효성에 영향을 미칠 수 있는 다음 각 호의 정보를 누구든지 확인할 수 있도록 공고하여야 한다.

1. 인증기관에 대한 정보

2. 인증업무준칙 정보

3. 인증서 폐지목록 정보

4. 기타 인증업무 수행 관련 정보 등

② 인증기관은 해당 인증기관용 인증서의 자율협력주행전자서명생성키를 안전하게 저장·관리하여야 하며, 자율협력주행전자서명생성키의 안전성이 취약하다고 판단될 경우 인증관리센터로부터 인증서를 재발급받아야 한다. 이 경우, 인증서를 재발급받은 인증기관은 신규 인증서를 활용하여 기존에 발급한 가입자 인증서를 모두 재발급하여야 한다.

③ 인증기관은 해당 인증기관용 인증서의 자율협력주행전자서명생성키가 분실·훼손 또는 도난·유출된 경우, 즉시 인증관리센터에 통보하고 자율협력주행 인증업무의 안전과 신뢰성을 확보할 수 있는 대책을 마련하여야 한다.

④ 인증기관은 다음 각 호에 해당하는 자율협력주행 인증업무에 관한

기록을 안전하게 보관·관리하여야 한다.

1. 인증서 신청, 발급, 폐지 등에 관한 사항

2. 인증서

3. 인증서 폐지목록(CRL)

4. 인증서 폐지 관련 정보(폐지 결정자, 폐지 사유 등)

5. 인증기관의 자율협력주행전자서명생성키 생성 및 관리에 관한 사항

6. 기타 자율협력주행 인증업무 관련 사항

⑤ 인증기관은 자율협력주행 인증업무 관련 기록의 안전성 및 신뢰성을 위하여 주기적인 백업 정책 및 감사기록 점검 계획을 수립하고 이를 시행하여야 한다.

⑥ 인증기관은 발급한 인증서와 관련하여 다음 각 호의 내용을 보증하여야 한다.

1. 인증서에 포함된 내용이 인증기관에 등록된 사실

2. 인증서가 법 및 같은 법 시행령, 인증업무준칙 등을 준수하여 발급된 사실

3. 인증서 폐지목록 및 인증서 상태 확인의 정확성

제7조(검증기관의 역할) ① 법 제29조제1항에 따라 지정된 검증기관은 다음 각 호의 업무를 수행한다.

1. 인증기관으로부터 인증서를 발급받은 자동차 및 노변기지국이 이상행위정보로 탐지하여 전송하는 정보를 수집, 분석 및 검증

2. 가입자 인증서의 효력 정지 및 폐지 요청 등 자율협력주행 검증업

무

3. 이상행위정보 및 기록에 대한 관리

4. 기타 검증기관으로써 필요하다고 인정되는 업무

② 검증기관은 인증관리센터에서 발급한 인증서를 이용하여 검증업무를 수행하여야 한다.

제8조(가입자 정보보호) ① 인증기관과 검증기관은 자율협력주행 인증업무 수행과정에서 얻게 되는 가입자 정보 및 운영과정에서 생성되는 중요자료에 대해 법원의 명령과 같은 특별한 경우를 제외하고는 인증업무 이외 목적으로 이용하거나 공개하지 말아야 한다.

② 인증기관과 검증기관은 자율협력주행 인증업무 수행과정에서 얻게 되는 가입자 정보를 「개인정보 보호법」에 따라 보호해야 한다.

제9조(인증서 발급, 재발급 및 폐지 신청거부 금지) 인증기관은 특정한 사유 없이 가입자 또는 인증서 발급 신청자의 인증서 발급, 재발급 및 폐지 신청을 거부할 수 없으며 거부할 경우 그 사유를 밝혀야 한다.

제10조(인증기관 운영 실태확인) ① 국토교통부장관은 자율협력주행 인증업무의 안전성과 신뢰성을 확보하고 가입자 정보를 보호하기 위하여 필요한 경우 인증기관에 자료 제출을 요구하거나 인증업무 운영실태를 확인할 수 있다.

② 제1항에 따른 자율협력주행 인증업무 운영실태를 확인할 경우에는 그 계획 등을 사전에 해당 인증기관에 통보한다.

③ 인증기관은 운영실태 점검에 따른 개선사항을 이행하여야 하며, 조

치결과를 국토교통부장관에게 통보하여야 한다.

④ 인증기관은 인증서 발급 및 이용현황 등 연간 운영현황을 다음 연도 1월 31일까지 국토교통부장관에게 통보하여야 한다.

제11조(인증협의회) ① 인증관리센터는 범국가적 자율협력주행 인증업무의 효율적 수행을 위하여 인증기관, 국가정보원 및 민간전문가 등으로 자율협력주행인증협의회(이하 "인증협의회"라 한다)를 구성·운영할 수 있다.

② 인증협의회는 다음 각 호의 사항을 협의한다.

1. 자율협력주행 인증업무 운영을 위한 인증정책
2. 자율협력주행 인증의 이용확산을 위한 제도의 개선 및 관계 법령의 정비에 관한 사항
3. 인증기관 간 상호연계 및 국제협력에 관한 사항
4. 기타 자율협력주행 인증의 안전성과 신뢰성 확보 및 이용촉진을 위해 필요한 사항

③ 그 밖의 인증협의회의 구성·운영에 관하여 필요한 사항은 인증관리센터의 장이 별도로 정한다.

제12조(알고리즘 취약성에 대한 통보 및 조치) ① 인증기관은 자율협력주행 인증업무에 이용하고 있는 자율협력주행인증용 알고리즘이 안전하지 않다고 인지하는 경우에 지체 없이 이를 인증협의회, 국가정보원 및 인증관리센터에 통보하고 해당 알고리즘으로 생성한 가입자 인증서를 폐지해야 한다.

② 인증관리센터와 인증기관은 누구든지 제1항의 사실을 확인할 수 있도록 공고한 뒤, 신뢰성 확보 대책을 강구하여야 한다.

제3장 자율협력주행 인증서

제13조(인증서 종류) 인증서는 발급대상에 따라 다음 각 호와 같이 구분한다.

1. 인증기관, 검증기관 등 인증업무 수행기관용 인증서
2. 등록인증서
3. 보안인증서

제14조(유효기간) ① 인증서의 최대 유효기간은 최상위인증기관 인증서 24년, 인증·검증기관 인증서 12년, 등록인증서 6년, 보안인증서 8일로 하며, 이를 초과하지 않는 범위 내에서 이용범위 및 기술의 안전성 등을 고려하여 인증관리센터와 협의하여 인증기관이 정한다.

② 각 인증기관은 인증기관 인증서 유효기간 만료 전에 이용범위 및 기술의 안전성 등을 인증관리센터와 협의하여 기존 인증서의 유효기간을 연장할 수 있다.

제15조(인증서의 효력) 인증서는 발급받은 날로부터 유효기간 동안 효력을 유지한다. 단, 법 제36조에 따른 사유가 발생한 때에는 그 효력이 소멸한다.

제4장 자율협력주행 인증업무

제16조(신원확인) 인증기관은 인증서의 신뢰성 확보를 위하여 가입자 정보에 대한 정확성 및 가입자 신원을 확인하는 절차를 거쳐야 한다.

제17조(인증서 발급) ① 인증기관은 신원확인 절차를 거친 인증서 발급 신청자에게만 인증서를 발급하여야 한다.

② 인증서는 인증서 발급 신청자가 온라인으로 직접 발급받는 것을 원칙으로 한다. 단, 특정한 사유로 신청자가 온라인으로 직접 발급받을 수 없는 경우 신청자 동의를 얻어 인증기관 등에서 안전한 방법으로 인증서를 발급하여 신청자에게 전달할 수 있다.

③ 가입자는 등록인증서의 유효기간이 만료되기 1년 전부터 만료일까지 갱신하여 유효기간을 연장할 수 있다. 단, 보안인증서의 경우 갱신하여 유효기간을 연장할 수 없다.

④ 가입자는 다음 각 호에 해당하는 경우 인증서를 재발급받을 수 있으며, 인증서 재발급 절차는 신규 발급절차와 동일하다.

1. 인증서의 유효기간이 지난 경우
2. 가입자의 자율협력주행전자서명생성키가 손상·유출 또는 변경되었다고 우려될 경우
3. 가입자 등 인증서 관련 정보가 변경된 경우

제5장 가입자의 의무와 책임

제18조(가입자 의무) ① 가입자는 다음의 경우에 정확한 정보 및 사실만을 인증기관에 제공해야 한다.

1. 인증서 발급, 재발급, 폐지 신청

2. 인증서 상에 기재된 가입자 정보변경 등

② 가입자는 자신의 자율협력주행전자서명생성키, 인증서 등을 안전하게 관리하여야 한다.

제19조(가입자 책임) 가입자는 본 고시에서 정한 의무를 위반 또는 인증서와 관련하여 허위 또는 잘못된 정보의 제공, 인증서 관리 부주의로 인하여 발생하는 손해와 손실 등에 대한 책임을 져야 한다.

제6장 시설기준 및 정보의 관리방법

제20조(시설 및 장비의 세부기준) ① 인증기관이 자율협력주행 인증업무를 원활히 수행하기 위하여 갖추어야 하는 시설 및 장비의 세부기준은 별표1과 같다.

② 검증기관이 자율협력주행 인증업무를 원활히 수행하기 위하여 갖추어야 하는 시설 및 장비의 세부기준은 별표2와 같다.

제21조(시설, 장비 및 정보의 관리방법) 인증기관과 검증기관이 시설, 장비 및 정보의 안전성 확보를 위하여 취하여야 할 기술적·관리적 및 물리적 조치 등의 관리방법은 별표3과 같다.

제7장 기 타

제22조(재검토기한) 국토교통부장관은 이 고시에 대하여 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 2023년 1월 1일 기준으로 매

3년이 되는 시점(매 3년째의 12월 31일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부 칙

이 고시는 발령한 날부터 시행한다.

■ [별표 1] 인증기관의 시설 및 장비에 관한 세부기준

1. 가입자 등록정보 관리 설비

1.1 가입자 식별기능

1.1.1 인증서 DN(Distinguish Name, 이하 "DN"이라 한다) 체계에 따라서 DN을 부여하는 기능

1.2 가입자 등록정보 관리기능

1.2.1 등록정보를 입력·접근·변경·삭제하는 기능

1.2.2 정보통신망을 통하여 전송되는 등록정보에 대한 암호화 및 전자서명 기능

1.3 감사 및 보안 기능

1.3.1 등록정보 내역에 대한 감사기록 생성·보존 기능

1.3.1.1. 등록정보를 입력·접근·변경·삭제한 사실, 시각, 행위자에 관한 내역에 대한 감사기록을 생성·보존하는 기능

1.3.1.2. 감사기록을 백업하는 기능

1.3.2 다음의 위협에 대처할 수 있는 기능

1.3.2.1. 감사기록의 위·변조 및 삭제 위협에 대처하는 기능

1.3.2.2. 등록정보 관리 소프트웨어의 위·변조 및 삭제 위협에 대처하는 기능

1.3.2.3. 등록정보 관리 소프트웨어의 불법적인 사용에 대처하는 기능

1.3.2.3.1. 운영관리자 및 감사관리자에 대한 역할 구분 및 접근통제 기능

1.3.2.3.1.2. 기타관리자가 있을 경우 이에 대한 역할 구분 및 접근통제 기능

1.3.2.4. 등록정보에 대한 위·변조, 삭제 및 유출 위협에 대처하는 기능

1.4 등록정보 관리 소프트웨어의 형상관리 기능

1.5 가입자 등록정보 보관 설비

1.5.1 인증기관은 가입자 등록정보를 보관하기 위하여 인증기관 내에 사무공간과 분리되어 있고 출입통제장치가 설치되어 있는 별도의 공간에 잠금장치가 있는 캐비닛 또는 금고를 구비하여야 한다.

2. 인증서 생성·발급·관리설비

2.1 인증서 생성·발급 설비

2.1.1 인증서 생성·발급 기능

2.1.1.1. 가입자의 인증서 발급 요청 처리 기능

2.1.1.1.1. 자율협력주행전자서명생성키(개인키)가 가입자에게 속한다는 사실 확인 기능

2.1.1.1.2. 가입자 자율협력주행전자서명검증키(공개키)에 대한 유일성 검사 기능

2.1.1.1.3. 정보통신망을 통하여 인증서 발급요청 시 기술규격을 준수하여 처리하는 기능

2.1.1.2. 다음의 사항에 대한 인증서 생성정책 설정 기능

2.1.1.2.1. 전자서명 알고리즘

2.1.1.2.2. 인증서 유효기간

2.1.1.2.3. 이용범위 또는 용도

2.1.1.2.4. 인증서 확장필드

2.1.1.3. 인증서 생성 및 생성정책 설정 기능을 구분하여 별도의 관리자를 두고 각각에 대한 접근통제를 수행하는 기능

2.1.1.4. 인증서를 생성하는 기능

2.1.1.4.1. 설정된 생성정책에 따라 인증서를 생성하는 기능

2.1.1.4.2. 자율협력주행전자서명생성키(개인키) 및 자율협력주행전자서명검증키(공개키) 생성·관리 설비의 전자서명 기능을 이용하여 인증서를 생성하는 기능

2.1.1.4.3. 인증서 생성기능

2.1.1.5. 인증서에 대하여 다음의 사항을 조회하는 기능

2.1.1.5.1. 전자서명 알고리즘

2.1.1.5.2. 인증서 유효기간

2.1.1.5.3. 가입자 및 발급자 DN

2.1.1.5.4. 이용범위 또는 용도

2.1.1.5.5. 인증서 확장필드

2.1.1.5.6. 인증서 효력 정지 및 폐지 여부

2.1.2 인증서 효력 정지 및 폐지목록 생성·관리 기능

2.1.2.1. 가입자의 인증서 효력 정지, 효력회복 및 폐지 요청을 처리하는 기능

2.1.2.1.1. 효력 정지, 효력회복·폐지의 구분, 요청 일자 및 사유 등을 기록하는 기능

2.1.2.1.2. 대상 인증서의 상태가 요청처리에 적절한지 확인하는 기능

2.1.2.1.3. 정보통신망을 통하여 인증서 효력 정지 및 폐지 요청 시 처리하는 기능

2.1.2.1.4. 정보통신망을 통하여 인증서 효력 정지 및 폐지 요청·처리 시 송·수신 정보에 대한 전자서명기능

2.1.2.2. 다음의 사항에 대하여 인증서 효력 정지 및 폐지목록 생성정책을 설정하는 기능

2.1.2.2.1. 전자서명 알고리즘

2.1.2.2.2. 다음 발급일자

2.1.2.2.3. 인증서 효력 정지 및 폐지목록 확장필드

2.1.2.2.4. 다음 발급일자 이전 자동갱신 또는 알림기능

2.1.2.3. 인증서 효력 정지 및 폐지목록 생성정책 설정 기능과 인증서 효력 정지 및 폐지목록 생성기능을 구분하여 별도의 관리자를 두고 각각에 대한 접근통제를 수행하는 기능

2.1.2.4. 인증서 효력 정지 및 폐지목록을 생성하는 기능

2.1.2.4.1. 자율협력주행전자서명생성키(개인키) 및 자율협력주행전자서명검증키(공개키) 생성·관리설비의 전자서명 기능을 이용하여 인증서 효력 정지 및 폐지목록을 생성하는 기능

2.1.2.4.2. 인증서 효력 정지 및 폐지목록 프로파일이 인증서 효력 정지 및 폐지목록을 생성하는 기능

2.1.2.5. 인증서 효력 정지 및 폐지목록에 대하여 다음의 사항을 조회하는 기능

2.1.2.5.1. 전자서명 알고리즘

2.1.2.5.2. 발급일자 및 다음 발급일자

2.1.2.5.3. 효력 정지 및 폐지된 인증서 일련번호

2.1.2.5.4. 인증서의 효력 정지 및 폐지일시, 사유

2.1.2.5.5. 인증서 효력 정지 및 폐지목록 확장필드

2.1.3 가입자인증서 등의 보관

2.1.3.1. 가입자의 공인인증서와 그 효력 정지 및 폐지에 관한 기록을 해당 공인인증서의 효력이 소멸한 날부터 10년 동안 보관하는 설비

2.1.3.2. 원격지 저장설비에 관한 사항

2.1.3.2.1. 가입자의 인증서와 그 효력 정지 및 폐지에 관한 기록을 보관하는 10Km 이상의 원격지 저장설비

2.1.3.2.2. 원격지 저장설비에 대한 물리적인 출입통제장치와 캐비닛 등의 잠금장치

2.1.3.2.3. 원격지 저장설비에 대한 접근내역을 감사기록하고 이를 보관하는 기능

2.1.3.2.4. 원격지 저장설비에 대한 침입감시장치

2.1.4 감사 및 보안 기능

2.1.4.1. 인증서의 내역에 대한 감사기록을 생성·보존하는 기능

2.1.4.1.1. 인증서의 발급·효력정지·효력회복·폐지·정책설정에 관한 내역에 대한 감사기록을 생성·보존하는 기능

2.1.4.1.2. 감사기록을 백업하는 기능

2.1.4.2. 다음의 위협에 대처할 수 있는 기능

2.1.4.2.1. 감사기록의 위·변조 및 삭제 위협에 대처하는 기능

2.1.4.2.2. 인증서 생성·발급 소프트웨어의 위·변조 및 삭제 위협에 대처하는 기능

2.1.4.2.3. 인증서 생성·발급 소프트웨어의 불법적인 사용에 대처하는 기능

2.1.4.2.3.1. 정책관리자, 운영관리자 및 감사관리자에 대한 역할 구분 및 접근통제 기능

2.1.4.2.3.2. 기타관리자가 있을 경우 이에 대한 역할구분 및 접근통제 기능

2.1.5 인증서 생성·발급 소프트웨어의 형상관리 기능

2.1.6 인증서 생성·발급 설비의 이중화

2.1.6.1. 동일한 기능을 갖는 인증서 생성·발급 설비의 이중화

2.1.6.2. 이중화된 인증서 생성·발급 설비를 이용한 비상시 복구기능

2.2 인증서 공고·유효성 확인 설비

2.2.1 인증서, 인증서 효력 정지 및 폐지목록을 공고하는 기능

2.2.1.1. 인증서, 공인인증서 효력 정지 및 폐지목록을 등록·삭제하는 기능

2.2.1.2. 인증서, 인증서 효력 정지 및 폐지목록을 검색할 수 있는 기능

2.2.1.3. 감사 및 보안 기능

2.2.1.3.1. 인증서, 인증서 효력 정지 및 폐지목록 등록·삭제 내역에 대한 감사기록

2.2.1.3.1.1. 인증서, 인증서 효력 정지 및 폐지목록 등록·관리한 사실, 시각, 행위자에 관한 내역에 대한 감사기록을 생성·보존하는 기능

2.2.1.3.1.2. 감사기록을 백업하는 기능

2.2.1.3.2. 다음의 위협에 대처할 수 있는 기능

2.2.1.3.2.1. 감사기록의 위·변조 및 삭제 위협에 대처하는 기능

2.2.1.3.2.2. 인증서, 인증서 효력 정지 및 폐지목록 공고 소프트웨어의 위·변조 및 삭제 위협 등에 대처하는 기능

2.2.1.3.2.3. 인증서, 인증서 효력 정지 및 폐지목록 공고 소프트웨어의 불법적인 사용에 대처하는 기능

2.2.1.3.2.3.1. 운영관리자 및 감사관리자 등에 대한 역할 구분 및 접근통제 기능

2.2.1.3.2.3.2. 기타관리자가 있을 경우 이에 대한 역할 구분 및 접근통제 기능

2.2.1.3.2.4. 인증서, 인증서 효력 정지 및 폐지목록에 대한 위·변조, 삭제 및 유출 위협에 대처하는 기능

2.2.1.4. 인증서, 인증서 효력 정지 및 폐지목록 공고 설비의 이중화

2.2.1.4.1. 동일한 기능을 갖는 인증서, 인증서 효력 정지 및 폐지목록 공고 설비 이중화

2.2.1.4.2. 이중화된 인증서, 인증서 효력정지 및 폐지목록 공고 설비를 이용한 비상시 실시간 복구기능

2.2.2 인증서 유효성 확인 기능

2.2.2.1. 인증서 유효성 여부를 제공하는 기능

2.2.2.2. 감사 및 보안 기능

2.2.2.2.1. 인증서 유효성 확인 내역에 관한 감사기록을 생성·보존하는 기능

2.2.2.2.1.1. 인증서 유효성 확인을 한 사실, 시각, 요청자에 관한 내역에 대한 감사기록을 생성·보존하는 기능

2.2.2.2.1.2. 감사기록을 백업하는 기능

2.2.2.2.2. 다음의 위협에 대처할 수 있는 기능

2.2.2.2.2.1. 감사기록의 위·변조 및 삭제 위협에 대처하는 기능

2.2.2.2.2.2. 인증서 유효성 확인 소프트웨어의 위·변조 및 삭제 위협 등에 대처하는 기능

2.2.2.2.2.3. 인증서 유효성 확인 소프트웨어의 불법적인 사용에 대처하는 기능

2.2.2.2.2.3.1. 운영관리자 및 감사관리자에 대한 역할구분 및 접근통제 기능

2.2.2.2.2.3.2. 기타관리자가 있을 경우 이에 대한 역할구분 및 접근통제 기능

2.2.2.3. 인증서 유효성 확인 소프트웨어의 형상관리 기능

2.2.2.4. 인증서 유효성 확인 설비의 이중화

2.2.2.4.1. 동일한 기능을 갖는 인증서 유효성 확인 설비 이중화

2.2.2.4.2. 이중화된 인증서 유효성 확인 설비를 이용한 비상시 실시간 복구기능

3. 보호설비

3.1 네트워크·시스템 보안설비

3.1.1 네트워크 보안 기능

3.1.1.1. 이중화된 네트워크 설비

3.1.1.1.1. 두 개 이상의 네트워크 회선

3.1.1.1.1.1. 물리적으로 분리된 두 개 이상의 네트워크 회선을 사용

3.1.1.1.1.2. 서로 다른 두 개 이상의 ISP(또는 IX)로부터의 회선을 사용

3.1.1.1.1.3. 하나의 회선에 장애가 발생하더라도 자율협력주행 인증업무를 지속적으로 제공할 수 있는 기능

3.1.1.1.1.4. 네트워크 회선을 인증체계에 필요한 용도로 사용

3.1.1.1.2. 두 개 이상의 경로(path)를 제공하는 내부망 구성

3.1.1.1.2.1. 하나의 경로에 이상이 발생하더라도 공인인증업무를 지속적으로 제공

3.1.1.1.2.2. 라우터를 이중화하여 사용

3.1.1.2. 네트워크 보안설비

3.1.1.2.1. 침입차단시스템

3.1.1.2.1.1. 침입차단시스템의 이중화

3.1.1.2.1.2. 침입차단소프트웨어의 사용

3.1.1.2.1.3. 인증체계에 필요한 접근통제규칙 설정 기능

3.1.1.2.1.4. 침입차단시스템에서 처리한 기록의 저장 및 백업 기능

3.1.1.2.2. 침입탐지시스템

3.1.1.2.2.1. 침입탐지소프트웨어의 사용

3.1.1.2.2.2. 모든 트래픽에 대한 점검 및 침입탐지 기능

3.1.1.2.2.3. 새로운 패턴의 침입유형에 대해 지속적으로 패턴 업데이트를 하는 기능

3.1.1.2.2.4. 침입이 탐지되었을 경우 이를 관리자에게 알리는 기능

3.1.1.3. 네트워크 및 시스템 관리설비

3.1.1.3.1. 실시간으로 네트워크 및 시스템의 상태를 점검할 수 있는 시스템 또는 장비

3.1.1.3.2. 인증시스템의 프로그램 또는 프로세스 동작 여부를 점검할 수 있는 시스템 또는 장비

3.1.1.4. 기타

3.1.1.4.1. 스위치, 라우터 등의 네트워크 장비에 대한 접근제어 기능

3.1.1.4.2. 감사기록·보존 기능

3.1.1.4.2.1. 네트워크 장비에서 생성하는 접근·설정·트랩 등에 관한 내역

3.1.2 시스템 보안 기능

3.1.2.1. 안전하고 신뢰성 있는 인증시스템

3.1.2.1.1. 관리자별로 계정 분리 설정 및 접근통제

3.1.2.1.2. 자율협력주행 인증업무에 필요한 사용자 등록

3.1.2.1.3. 시스템 운영 목적에 적합한 소프트웨어만 설치

3.1.2.1.4. 시스템 운영 목적에 적합한 프로그램 또는 프로세스만 실행

3.1.2.1.5. 프로그램에 대한 패치 수행

3.1.2.1.6. 운영체제(OS)에 대한 패치 수행

3.1.2.1.7. 시스템 및 관련 소프트웨어에 대한 유지보수 계약 체결 여부

3.1.2.2. 인증시스템 운영에 관한 정보에 대한 감사기록을 생성·보존하는 기능

3.1.2.2.1. 시스템 시동/정지

3.1.2.2.2. 자율협력주행 인증업무에 필요한 프로그램의 시작/종료

3.1.2.2.3. 루트 및 사용자의 로그인/아웃

3.1.2.3. 기타 설비

3.1.2.3.1. 자율협력주행 인증업무에 필요하여 운영하고 있는 웹 서버, 네임 서버, 메일 서버 등에 대하여 3.1.2의 가목 및 나목을 준수

3.2 물리적 보안설비

3.2.1 인증시스템 운영실

3.2.1.1. 인증시스템을 안전하게 운영할 수 있는 별도의 통제구역 설치

3.2.1.1.1. 다음의 인증시스템을 별도의 운영실로 분리

3.2.1.1.1.1. 전자서명키 관리, 인증서 생성·관리 기능을 제공하는 시스템은 동일 운영실에 설치할 수 있으나 다른 설비와는 별도 운영실로 분리

3.2.1.1.1.2. 인증서 공고기능을 제공하는 설비는 다른 설비와는 별도 운영실로 분리

3.2.1.1.2. 인증시스템 운영실의 외벽(인증시스템 운영실의 외부와 맞닿은 면)은 외부

침입으로부터 자율협력주행 인증업무의 제공에 필수적으로 요구되는 인증시스템을 보호할 수 있도록 설계

3.2.1.1.2.1. 외벽 재질은 벽돌 또는 철근 콘크리트로 축조되어 있거나, 철골구조물에 3T 이상의 철판으로 용접

3.2.1.1.2.2. 외벽은 천장, 바닥까지 완전하게 마감

3.2.1.1.3. 운영실을 분리할 수 있도록 인증시스템 운영실의 내벽(인증시스템 운영실의 내부 벽면) 설계

3.2.1.1.3.1. 인증시스템 운영실의 내벽 및 복도와 맞닿은 내벽의 재질은 벽돌로 축조되어 있거나, 철골구조물에 1.8T 이상의 철판으로 용접 또는 철제 케이지로 용접

3.2.1.1.3.2. 내벽은 천장, 바닥까지 완전하게 마감(소방법상의 환풍구는 허용 가능함) 하거나 출입방지 기능이 있는 철제 케이지를 사용

3.2.1.1.4. 인증시스템 운영실 출입문의 물리적인 출입통제 기능

3.2.1.1.4.1. 유리문의 경우 강화유리

3.2.1.1.4.2. 일반문의 경우 강화 및 방화기능

3.2.1.2. 강화유리 창문, 통풍창의 차폐막

3.2.1.2.1. 창문이 설치되어 있는 경우

3.2.1.2.1.1. 창문은 강화유리 또는 강화필름으로 코팅한 유리 사용

3.2.1.2.1.2. 창문을 통하여 복도 또는 하나의 운영실에서 다른 운영실로 침입할 수 없

도록 운영실을 연결하는 창문 및 창문 외부의 지지대 제거

3.2.1.2.1.3. 건물 외부에서 내부가 들여다보이지 않도록 코팅 등의 처리

3.2.1.2.2. 통풍창이 설치되어 있는 경우

3.2.1.2.2.1. 통풍창의 크기가 사람이 통과할 수 있을 경우 차폐막 설치

3.2.2 다중출입 통제장치

3.2.2.1. 인증시스템 운영실에 대한 출입을 통제하고 감사기록 기능을 갖는 출입통제 장치

3.2.2.1.1. 비인가자가 인증시스템 운영실에 접근할 수 없도록 하는 물리적인 출입통제

3.2.2.1.2. 출입통제장치는 다음의 정보에 대한 감사기록

3.2.2.1.2.1. 일련번호

3.2.2.1.2.2. 사건의 유형, 성공/실패 여부 및 실패 시 원인

3.2.2.1.2.3. 일자 및 시각

3.2.2.1.2.4. 행위자

3.2.2.2. 생체특성기반과 소지 기반의 신원확인 기능을 결합하여 사용하는 출입통제 장치

3.2.2.2.1. 생체특성기반 신원확인(지문인식, 홍채인식 등)

3.2.2.2.2. 소지 기반 신원확인(열쇠, 카드 등)

3.2.2.3. 인증시스템 운영실에 접근 시, 다른 사람이 대신 들어가거나 따라 들어가는 행위를 방지하는 설비

3.2.2.4. 정전 시에도 출입통제 및 감사기록이 가능하도록 하는 기능

3.2.3 침입감지·경보 및 감시·통제 장치

3.2.3.1. 인증시스템 운영실에 대하여 물리적인 침입을 감지하고 이를 경보하여 주는 장치

3.2.3.1.1. 침입감지 및 경보 기능

3.2.3.1.1.1. 운영실 내에 진동감지장치, 음향감지장치 등의 침입감지장치 설치

3.2.3.1.1.2. 침입감지장치에 이상이 발생했을 때 이를 감지하는 기능

3.2.3.1.1.3. 침입감지장치가 침입을 감지하였을 경우 관리자에게 즉각 알리는 기능

3.2.3.1.2. 침입감지·경보장치와 연결된 침입 발생 위치 확인 기능

3.2.3.2. 인증시스템 운영실을 감시·통제하고 이에 대한 감사기록 기능을 갖는 장치

3.2.3.2.1. 침입감시 기능

3.2.3.2.1.1. CCTV 설치

3.2.3.2.1.2. 감시장치는 24시간 실시간으로 감시하는 기능

3.2.3.2.1.3. CCTV시스템은 모든 출입행위에 대하여 녹화하는 기능

3.2.3.2.1.4. CCTV시스템에 대한 접근통제기능

3.2.3.2.1.5. CCTV시스템 관리용 패스워드에 대한 보호기능

3.2.3.2.2. 다중출입통제장치로부터의 출입현황정보 확인 기능

3.2.3.2.2.1. 정당한 관리자만이 감사기록을 조회

3.2.3.2.2.2. 시간별, 행위자별, 사건의 종류 등의 다양한 조건에 따라 감사기록 검색 기능

3.2.3.2.2.3. 출입통제시스템 감사기록 저장공간 소진에 대한 대책

3.2.3.2.2.4. 출입통제시스템에 대한 접근통제 기능

3.2.3.2.2.5. 출입통제시스템 관리용 패스워드는 시스템에 암호화하여 저장하는 기능

3.2.3.2.2.6. 감사기록을 백업하는 기능

3.2.4 물리적 잠금장치

3.2.4.1. 물리적 보안설비 내의 인증시스템에 대한 접근을 물리적으로 통제하는 보안 캐비닛

3.2.4.2. 전자서명생성정보, 가입자의 공인인증서 등 중요자료에 대한 접근을 물리적으로 통제하는 금고 또는 잠금장치가 설치된 캐비닛

3.2.4.3. 잠금장치 열쇠를 별도의 잠금장치가 있는 보관함 또는 캐비닛에 관리

3.2.5 재해 예방설비

3.2.5.1. 화재 발생 시 이를 조기에 감지하고 진화하는 설비

3.2.5.1.1. 화재 경보장치

3.2.5.1.1.1. 연기감지장치, 온도감지장치 등의 화재경보장치를 설치

3.2.5.1.2. 화재 소화장치

3.2.5.1.2.1. 소규모 및 대규모 화재에 대처할 수 있도록 설치

3.2.5.1.2.2. 오동작에 대처할 수 있는 기능

3.2.5.1.2.3. 화재소화장치 동작 시 타 시스템에 악영향을 미치지 않는 소화약제 사용

3.2.4.2. 수재 예방설비

3.2.4.2.1. 인증시스템, 침입차단시스템 및 네트워크설비 등이 물에 노출되지 않도록 바닥으로부터 이격하여 설치

3.2.4.2.2. 콘센트 등 전원접속장치는 바닥으로부터 이격하여 설치

3.2.4.3. 정전 발생 시 지속적인 인증업무의 수행이 가능토록 일정 기간 전원을 공급하여 주는 전원 공급설비

3.2.4.3.1. 자가 발전설비 및 무정전 전원공급장치

3.2.4.3.1.1. 정전 발생 시 지속적인 인증업무의 수행이 가능하도록 30분 이상 전원을 공급해줄 수 있는 장치

3.2.4.3.1.2. 자가발전설비의 경우 추가적인 연료의 보충 없이도 2시간 이상 발전하여 전원을 공급해 줄 수 있는 기능

3.2.4.4. 온도 및 습도를 일정하게 유지하기 위한 항온항습장치 설치

3.2.4.5. 기타

3.2.4.5.1. 물리적 보안설비 내에 각종 전원 장비에 대한 접지시설

3.2.4.5.2. 물리적 보안설비 내에 비상시를 대비한 유도등 및 유도표지 설치

■ [별표 2] 검증기관의 시설 및 장비에 관한 세부기준

1. 자율협력주행 과정에서 발생하는 정보의 이상 유무를 탐지·판단할 수 있는 설비

1.1 이상행위보고서를 수신·저장할 수 있는 설비

1.1.1 자율협력주행 과정에서 발생하는 이상행위보고서를 수신하는 기능

1.1.2 자율협력주행 과정에서 발생하는 이상행위보고서를 저장하는 기능

1.1.2.1. 이상행위보고서의 저장 기능

1.1.2.1.1. 이상행위보고서의 수신일시

1.1.2.1.2. 이상행위보고서의 유형

1.1.2.1.3. 이상행위보고서의 생성일시

1.1.2.1.4. 이상행위보고서의 생성위치

1.1.2.1.2. 이상행위보고서의 조회 기능

1.1.2.1.2.1. 이상행위보고서의 수신일시

1.1.2.1.2.2. 이상행위보고서의 유형

1.1.2.1.2.3. 이상행위보고서의 생성일시

1.1.2.1.2.4. 이상행위보고서의 생성위치

1.2 이상행위정보 유무를 분석·검증·판단할 수 있는 설비

1.2.1 자율협력주행 과정에서 발생한 이상행위보고서를 분석하는 기능

1.2.1.1. 이상행위 판단에 필요한 이상행위로 탐지된 정보를 이상행위보고서에서 추출하는 기능

1.2.1.2. 추출한 이상행위로 탐지된 정보를 저장하는 기능

1.2.1.3. 추출한 이상행위로 탐지된 정보의 백업 및 복구기능

1.2.2 이상행위로 탐지된 정보의 이상 유무를 판단하는 기능

1.2.2.1. 자율협력주행 정보의 이상 유무 판단을 위한 검증절차를 수행하는 기능

1.2.2.2. 판단한 자율협력주행 정보의 이상 유무 결과를 저장하는 기능

1.2.2.3. 판단한 자율협력주행 정보의 이상 유무 결과의 백업 및 복구기능

1.3 이상행위정보의 발생 원인을 분석하고 필요한 조치를 취할 수 있는 설비

1.3.1 이상행위의 발생 원인을 분석하는 기능

1.3.1.1. 자동차나 자동차 부품의 설계, 제조 또는 성능상의 문제로 발생한 이상행위정보

1.3.1.2. 그 밖에 원인으로 발생한 이상행위정보

1.3.2 최종 판단된 이상행위정보에 대한 후속조치 기능

1.3.2.1. 인증서의 효력정지나 폐지가 필요하다고 판단된 이상행위 발생 차량의 인증서를 결정하는 기능

1.3.2.2. 인증서의 효력정지나 폐지를 인증관리센터와 인증기관에 요청하는 기능

1.3.2 인증서의 효력 정지나 폐지가 필요한지 판단하는 기능

1.3.3 이상행위 가입자의 인증서 폐지가 필요하다고 판단하는 경우 이상행위 가입자에 발급된 유효한 모든 인증서의 폐지를 인증관리센터와 인증기관에 요청하는 기능

1.3.4 이상행위정보 발생의 원인이 자동차나 자동차 부품의 설계, 제조 또는 성능상의 문제인지 판단하는 기능

1.4 감사 및 보안 기능

1.4.1 이상행위보고서 내역에 대한 감사기록 생성·보존 기능

1.4.1.1. 이상행위보고서 관련 입력·접근·변경·삭제한 사실, 시각, 행위자에 관한 내역에 대한 감사기록을 생성·보존하는 기능

1.3.1.2. 감사기록을 백업하는 기능

1.4.2 다음의 위협에 대처할 수 있는 기능

1.4.2.1. 감사기록의 위·변조 및 삭제 위협에 대처하는 기능

1.4.2.2. 이상행위보고서 및 이상행위정보 관리 소프트웨어의 위·변조 및 삭제 위협에 대처하는 기능

1.4.2.3. 이상행위보고서 및 이상행위정보 관리 소프트웨어의 불법적인 사용에 대처하는 기능

1.4.2.3.1. 운영관리자 및 감사관리자에 대한 역할 구분 및 접근통제 기능

1.4.2.3.2. 기타관리자가 있을 경우 이에 대한 역할 구분 및 접근통제 기능

1.4.2.4. 이상행위보고서 및 이상행위정보에 대한 위·변조, 삭제 및 유출 위협에 대처하는 기능

1.5 이상행위 탐지·판단 소프트웨어 형상관리

1.6 이상행위 관련 정보 보관 설비

1.6.1 검증기관은 이상행위 관련 정보를 보관하기 위하여 검증기관 내에 사무공간과 분리되어 있고 출입통제장치가 설치되어 있는 별도의 공간에 잠금장치가 있는 캐비닛 또는 금고를 구비하여야 한다.

2. 보호설비

2.1 네트워크·시스템 보안설비

2.1.1 네트워크 보안 기능

2.1.1.1. 이중화된 네트워크 설비

2.1.1.1.1. 두 개 이상의 네트워크 회선

2.1.1.1.1.1. 물리적으로 분리된 두 개 이상의 네트워크 회선을 사용

2.1.1.1.1.2. 서로 다른 두 개 이상의 ISP(또는 IX)로부터의 회선을 사용

2.1.1.1.1.3. 하나의 회선에 장애가 발생하더라도 자율협력주행 검증업무를 지속적으로 제공할 수 있는 기능

2.1.1.1.1.4. 네트워크 회선을 검증체계에 필요한 용도로 사용

2.1.1.1.2. 두 개 이상의 경로(path)를 제공하는 내부망 구성

2.1.1.1.2.1. 하나의 경로에 이상이 발생하더라도 검증업무를 지속적으로 제공

2.1.1.1.2.2. 라우터를 이중화하여 사용

2.1.1.2. 네트워크 보안설비

2.1.1.2.1. 침입차단시스템

2.1.1.2.1.1. 침입차단시스템의 이중화

2.1.1.2.1.2. 침입차단소프트웨어의 사용

2.1.1.2.1.3. 검증체계에 필요한 접근통제규칙 설정 기능

2.1.1.2.1.4. 침입차단시스템에서 처리한 기록의 저장 및 백업 기능

2.1.1.2.2. 침입탐지시스템

2.1.1.2.2.1. 침입탐지소프트웨어의 사용

2.1.1.2.2.2. 모든 트래픽에 대한 점검 및 침입탐지 기능

2.1.1.2.2.3. 새로운 패턴의 침입유형에 대해 지속적으로 패턴 업데이트를 하는 기능

2.1.1.2.2.4. 침입이 탐지되었을 경우 이를 관리자에게 알리는 기능

2.1.1.3. 네트워크 및 시스템 관리설비

2.1.1.3.1. 실시간으로 네트워크 및 시스템의 상태를 점검할 수 있는 시스템 또는 장비

2.1.1.3.2. 검증시스템의 프로그램 또는 프로세스 동작 여부를 점검할 수 있는 시스템 또는 장비

2.1.1.4. 기타

2.1.1.4.1. 스위치, 라우터 등의 네트워크 장비에 대한 접근제어 기능

2.1.1.4.2. 감사기록·보존 기능

2.1.1.4.2.1. 네트워크 장비에서 생성하는 접근·설정·트랩 등에 관한 내역

2.1.2 시스템 보안 기능

2.1.2.1. 안전하고 신뢰성 있는 검증시스템

2.1.2.1.1. 관리자별로 계정 분리 설정 및 접근통제

2.1.2.1.2. 자율협력주행 검증업무에 필요한 사용자 등록

2.1.2.1.3. 시스템 운영 목적에 적합한 소프트웨어만 설치

2.1.2.1.4. 시스템 운영 목적에 적합한 프로그램 또는 프로세스만 실행

2.1.2.1.5. 프로그램에 대한 패치 수행

2.1.2.1.6. 운영체제(OS)에 대한 패치 수행

2.1.2.1.7. 시스템 및 관련 소프트웨어에 대한 유지보수 계약 체결 여부

2.1.2.2. 검증시스템 운영에 관한 정보에 대한 감사기록을 생성·보존하는 기능

2.1.2.2.1. 시스템 시동/정지

2.1.2.2.2. 자율협력주행 검증업무에 필요한 프로그램의 시작/종료

2.1.2.2.3. 루트 및 사용자의 로그인/아웃

2.1.2.3. 기타 설비

2.1.2.3.1. 자율협력주행 인증업무에 필요하여 운영하고 있는 웹 서버, 네임 서버, 메일 서버 등에 대하여 2.1.2의 가목 및 나목을 준수

2.2 물리적 보안설비

2.2.1 검증시스템 운영실

2.2.1.1. 검증시스템을 안전하게 운영할 수 있는 별도의 통제구역 설치

2.2.1.1.1. 다음의 검증시스템을 별도의 운영실로 분리

2.2.1.1.1.1. 이상행위 판별, 인증서 폐지 목록(CRL) 관리기능을 제공하는 시스템은 동일 운영실에 설치할 수 있으나 다른 설비와는 별도 운영실로 분리

2.2.1.1.1.2. 인증서 공고기능을 제공하는 설비는 다른 설비와는 별도 운영실로 분리

2.2.1.1.2. 검증시스템 운영실의 외벽(인증시스템 운영실의 외부와 맞닿은 면)은 외부 침입으로부터 자율협력주행 검증업무의 제공에 필수적으로 요구되는 검증시스템을 보호할 수 있도록 설계

2.2.1.1.2.1. 외벽 재질은 벽돌 또는 철근콘크리트로 축조되어 있거나, 철골 구조물에 3T 이상의 철판으로 용접

2.2.1.1.2.2. 외벽은 천장, 바닥까지 완전하게 마감

2.2.1.1.3. 운영실을 분리할 수 있도록 검증시스템 운영실의 내벽(검증시스템 운영실의 내부 벽면) 설계

2.2.1.1.3.1. 검증시스템 운영실의 내벽 및 복도와 맞닿은 내벽의 재질은 벽돌로 축조되어 있거나, 철골 구조물에 1.8T 이상의 철판으로 용접 또는 철제 케이지로 용접

2.2.1.1.3.2. 내벽은 천장, 바닥까지 완전하게 마감(소방법상의 환풍구는 허용 가능함) 하거나 출입방지 기능이 있는 철제 케이지를 사용

2.2.1.1.4. 검증시스템 운영실 출입문의 물리적인 출입통제 기능

2.2.1.1.4.1. 유리문의 경우 강화유리

2.2.1.1.4.2. 일반문의 경우 강화 및 방화기능

2.2.1.2. 강화유리 창문, 통풍창의 차폐막

2.2.1.2.1. 창문이 설치되어 있는 경우

2.2.1.2.1.1. 창문은 강화유리 또는 강화 필름으로 코팅한 유리 사용

2.2.1.2.1.2. 창문을 통하여 복도 또는 하나의 운영실에서 다른 운영실로 침입할 수 없도록 운영실을 연결하는 창문 및 창문 외부의 지지대 제거

2.2.1.2.1.3. 건물 외부에서 내부가 들여다보이지 않도록 코팅 등의 처리

2.2.1.2.2. 통풍창이 설치되어 있는 경우

2.2.1.2.2.1. 통풍창의 크기가 사람이 통과할 수 있을 경우 차폐막 설치

2.2.2 다중출입 통제장치

2.2.2.1. 검증시스템 운영실에 대한 출입을 통제하고 감사기록 기능을 갖는 출입통제 장치

2.2.2.1.1. 비인가자가 검증시스템 운영실에 접근할 수 없도록 하는 물리적인 출입통제

2.2.2.1.2. 출입통제장치는 다음의 정보에 대한 감사기록

2.2.2.1.2.1. 일련번호

2.2.2.1.2.2. 사건의 유형, 성공/실패 여부 및 실패 시 원인

2.2.2.1.2.3. 일자 및 시각

2.2.2.1.2.4. 행위자

2.2.2.2. 생체특성기반과 소지 기반의 신원확인 기능을 결합하여 사용하는 출입통제장치

2.2.2.2.1. 생체특성기반 신원확인(지문인식, 홍채인식 등)

2.2.2.2.2. 소지 기반 신원확인(열쇠, 카드 등)

2.2.2.3. 검증시스템 운영실에 접근 시, 다른 사람이 대신 들어가거나 따라 들어가는 행위를 방지하는 설비

2.2.2.4. 정전 시에도 출입통제 및 감사기록이 가능하도록 하는 기능

2.2.3 침입감지·경보 및 감시·통제 장치

2.2.3.1. 검증시스템 운영실에 대하여 물리적인 침입을 감지하고 이를 경보하여 주는 장치

2.2.3.1.1. 침입감지 및 경보 기능

2.2.3.1.1.1. 운영실 내에 진동감지장치, 음향감지장치 등의 침입감지장치 설치

2.2.3.1.1.2. 침입감지장치에 이상이 발생했을 때 이를 감지하는 기능

2.2.3.1.1.3. 침입감지장치가 침입을 감지하였을 경우 관리자에게 즉각 알리는 기능

2.2.3.1.2. 침입감지·경보장치와 연결된 침입 발생 위치 확인 기능

2.2.3.2. 검증시스템 운영실을 감시·통제하고 이에 대한 감사기록 기능을 갖는 장치

2.2.3.2.1. 침입감시 기능

2.2.3.2.1.1. CCTV 설치

2.2.3.2.1.2. 감시장치는 24시간 실시간으로 감시하는 기능

2.2.3.2.1.3. CCTV시스템은 모든 출입행위에 대하여 녹화하는 기능

2.2.3.2.1.4. CCTV시스템에 대한 접근통제기능

2.2.3.2.1.5. CCTV시스템 관리용 패스워드에 대한 보호 기능

2.2.3.2.2. 다중출입통제장치로부터의 출입현황정보 확인 기능

2.2.3.2.2.1. 정당한 관리자만이 감사기록을 조회

2.2.3.2.2.2. 시간별, 행위자별, 사건의 종류 등의 다양한 조건에 따라 감사기록 검색 기능

2.2.3.2.2.3. 출입통제시스템 감사기록 저장공간 소진에 대한 대책

2.2.3.2.2.4. 출입통제시스템에 대한 접근통제 기능

2.2.3.2.2.5. 출입통제시스템 관리용 패스워드는 시스템에 암호화하여 저장하는 기능

2.2.3.2.2.6. 감사기록을 백업하는 기능

2.2.4 물리적 잠금장치

2.2.4.1. 물리적 보안설비 내의 검증시스템에 대한 접근을 물리적으로 통제하는 보안 캐비닛

2.2.4.2. 전자서명생성정보, 가입자의 공인인증서 등 중요자료에 대한 접근을 물리적으로 통제하는 금고 또는 잠금장치가 설치된 캐비닛

2.2.4.3. 잠금장치 열쇠를 별도의 잠금장치가 있는 보관함 또는 캐비닛에 관리

2.2.5 재해 예방설비

2.2.5.1. 화재 발생 시 이를 조기에 감지하고 진화하는 설비

2.2.5.1.1. 화재 경보장치

2.2.5.1.1.1. 연기감지장치, 온도감지장치 등의 화재경보장치를 설치

2.2.5.1.2. 화재 소화장치

2.2.5.1.2.1. 소규모 및 대규모 화재에 대처할 수 있도록 설치

2.2.5.1.2.2. 오동작에 대처할 수 있는 기능

2.2.5.1.2.3. 화재 소화장치 동작 시 타 시스템에 악영향을 미치지 않는 소화약제 사용

2.2.5.2. 수재 예방설비

2.2.5.2.1. 검증시스템, 침입차단시스템 및 네트워크 설비 등이 물에 노출되지 않도록 바닥으로부터 이격하여 설치

2.2.5.2.2. 콘센트 등 전원접속장치는 바닥으로부터 이격하여 설치

2.2.5.3. 정전 발생 시 지속적인 검증업무의 수행이 가능토록 일정 기간 전원을 공급하여 주는 전원 공급설비

2.2.5.3.1. 자가 발전설비 및 무정전 전원공급장치

2.2.5.3.1.1. 정전 발생 시 지속적인 검증업무의 수행이 가능하도록 30분 이상 전원을 공급해줄 수 있는 장치

2.2.5.3.1.2. 자가발전설비의 경우 추가적인 연료의 보충 없이도 2시간 이상 발전하여 전원을 공급해 줄 수 있는 기능

2.2.5.4. 온도 및 습도를 일정하게 유지하기 위한 항온항습장치 설치

2.2.5.5. 기타

2.2.5.5.1. 물리적 보안설비 내에 각종 전원 장비에 대한 접지시설

2.2.5.5.2. 물리적 보안설비 내에 비상시를 대비한 유도등 및 유도표지 설치

■ [별표 3] 인증기관 및 검증기관 시설, 장비 및 정보의 관리방법

1. 정보보호정책 및 조직

번호	항목	내용
1.1	정보보호 정책 수립 및 관리	정보보호위원회의 승인을 받아 정보보호 정책을 제·개정하고 이를 문서화한다.
1.2	정보보호 조직 구성 및 운영	정보보호 업무 총괄 관리 책임이 있는 자를 정보보호 책임자를 지정하고 정보보호 활동을 체계적으로 이행할 수 있는 실무조직 또는 정보보호위원회를 구성·운영한다.

2. 자산 관리

번호	항목	평가 내용
2.1	정보자산 식별 및 분류	조직의 업무특성에 따라 정보자산 분류 기준을 수립하여 자율협력주행 인증업무 범위 내 모든 정보자산을 식별·분류하고 중요도를 산정한 후 문서화하여 최신으로 관리한다.
2.2	자산 관리 및 통제	분류된 자산 및 정보자료는 위험으로부터 적절한 수준의 보호를 받을 수 있도록 통제절차를 마련하고 유지한다.

3. 인적보안

번호	항목	평가 내용
3.1	직무 적합성 검토	자율협력주행 인증업무를 수행하는 직무에 대한 요건, 역할 등을 직무기술서로 명시하여야 하며, 자율협력주행인증업무 담당자에 대한 신원확인 등 업무 적합성 여부 검토 절차를 마련한다.
3.2	역할 구분	권한 오남용, 고의적 행위 등으로 발생할 수 있는 피해 방지를 위해 역할 구분기준을 수립하고 시행한다.
3.3	보안서약서 작성	자율협력주행 인증업무를 수행하는 모든 직무 관련자(임시직원이나 외부자 포함)는 기밀 유지 등에 대한 보안서약서를 작성한다.
3.4	보안 교육	자율협력주행 인증업무를 수행하는 모든 직무 관련자는 보안 정책 및 절차 등에 대한 교육을 받아야 한다.
3.5	외부자 보안	외부 서비스를 이용하거나 외부자에게 업무를 위탁하는 경우, 정보보호 요구사항을 관련 계약서 등에 명시하고, 명시된 요구사항을 준수하고 있는지 주기적으로 점검 또는 감사한다.

4. 물리적 보안

번호	항목	내용

4.1	물리적 보호	인증서 발급 등 중요 설비는 별도의 통제구역에 타 시스템과 물리적으로 분리되는 등 안전한 시설에 위치되고, 사고 및 재난(화재, 수해, 전기적 이상 등) 등을 방지할 수 있는 방안을 마련한다.
4.2	출입통제	중요설비에는 허가된 인원만 출입 가능하도록 물리적 접근통제(출입통제 장치, 다중 신원확인 절차 등) 방안을 마련하고, 접근하는 모든 인원의 출입 날짜・시간 등을 기록・관리한다.
4.3	침입 감지 및 감시	자율협력주행인증시스템 운영실에 대한 물리적인 침입을 감지・경보하기 위한 방안을 마련하고, 시설의 출입・내부 활동을 CCTV 등 카메라를 통해 모니터링한다.
4.4	반・출입 통제	장비, 문서, 휴대용 저장매체 등의 반・출입 통제 정책을 수립하고 반・출입 시 이력을 작성한다.

5. 운영 보안

번호	항목	내용
5.1	운영절차 수립 및 준수	자율협력주행 인증시스템 및 보안시스템 운영을 위한 운영절차를 수립하고 변경사항을 반영하여야 하며, 해당 절차를 준수한다.
5.2	시스템 및 서비스 관리	운영 시스템을 개발 및 테스트 시스템으로부터 분리하고 안전한 보안 설정, 성능・용량・상태 모니터링, 안전한 인수 및 유지보수 절차 수립・이행, 무결성 검증 등의 보호조치를 수행한다.
5.3	악성코드 예방・탐지・대응	악성코드 예방・탐지・대응을 위한 보안시스템을 운영하고, 운영체제 및 소프트웨어의 패치・업데이트에 대한 정책과 절차를 수립하고 이를 이행한다.
5.4	침해사고 대응	비상연락체계, 사고 발생 시 보고 절차, 대응 및 복구 절차, 신고 절차 등을 포함한 사고 대응 정책을 마련한다.

6. 접근통제

번호	항목	내용
6.1	접근통제 정책	자율협력주행 인증시스템 및 보안시스템의 접근통제 절차, 역할 및 접근권한, 특정 업무수행을 위해 요구되는 인원수 등이 포함된 접근통제 정책을 수립한다.
6.2	접근권한 관리	인증시스템, 보안시스템, 중요정보에 접근하기 위한 공식적인 사용자 등록・취소, 접근 권한 관리 절차를 마련하고, 정기적으로 업데이트한다.
6.3	비인가자 시스템 접근 금지	시스템에 대한 접속 권한은 허가된 네트워크 서비스에서 사용자 인증 절차에 의해 통제되어야 하며, 비인가자가 자율협력주행 인증업무와 관련된 네트워크, 서버, 데이터베이스 등의 시스템에 접근할 수 없도록 한다.

7. 개발 보안

번호	항목	내용
7.1	시스템 변경 관리	시스템 개선 및 신규 시스템 도입 시 통제절차를 수립하고, 변경사항 적용 시 테스트 수행 등 안전성을 확인한다.
7.2	프로그램 소스코드 보호	프로그램 소스 라이브러리 접근통제와 소스코드 등에 대한 형상관리를 수행한다.

8. 업무 연속성 관리

번호	항목	내용
8.1	업무 연속성 계획	장애 및 재해로부터 업무 연속성 확보를 위해 위험 평가에 기초한 업무 연속성 계획을 마련하고, 정기적으로 테스트하여 변화사항을 업데이트한다.
8.2	백업 및 원격지 시설	장애 및 재해 발생 시 핵심업무가 복구될 수 있도록 대체 백업 시설을 마련하고, 보안 수준은 메인 시설과 동등한 수준으로 통제한다.

9. 감사 로그

번호	항목	내용
9.1	감사로그 생성	인증서, 암호화 장치 등과 관련된 감사로그를 생성하고 위험 평가 및 관계 법령에서 요구되는 특정한 기간 동안 보관한다.
9.2	감사로그 관리	감사로그의 무결성 검증, 승인되지 않거나 의심되는 기록에 대해 주기적으로 검토하고, 백업・접근통제 등 관리 절차를 마련한다.