Research Report

연구보고서 2018-012

소프트웨어 안전(Safety) 산업 동향 조사

Software Safety Industry Trends Study

진회승/송지환/권영환/정영철/주민규/임인종/최정윤

2018.12

SPRi 소프트웨어정책연구소

이 보고서는 2018년도 과학기술정보통신부 정보통신·방송 연구 개발사업에서 지원받아 제작한 것으로 과학기술정보통신부의 공식입장과 다를 수 있습니다.

목 차

표 목 차

그 림 목 차

요 약 문

1. 제 목

2018년 국내 소프트웨어 안전(Safety) 산업 동향 조사

2. 연구 목적 및 필요성

본 연구의 목적은 2년간 변화된 국내 소프트웨어 안전 산업 동향을 조사하여 기존 연구와 비교·분석하여 핵심성공요소(CSF)를 도출하고, 최근 이슈화 되고 있는 주요 기술 중 소프트웨어 안전이 중요시 되고 있는 기술인 자율주행차, 드론에 대한 해외 주요국의 정책, 글로벌 TIC 시장현황을 조사 한 후, 국내 현황과 비교·분석을 통해 국내 소프트웨어 안전 산업 및 문화를 제고를 위한 신뢰성 있는 자료를 작성한다.

3. 연구의 구성 및 범위

본 연구는 총 7장으로 구성되어 있다.

제 1장에는 소프트웨어 안전 산업동향 조사 연구의 배경과 필요성, 목적, 본 연구를 수행한 연구 수행 방법을 제시한다.

제2장과 3장에는 자율주행차와 드론 관련 법·제도, 기관, 지침/가이드와 해외 TIC[1] 시장 현황을 조사하고 분석한다. 최근 급격히 변화하거나 새롭게 중요성이 증가하는 산업인 자율주행차 및 드론 관련 해외 주요국(미국, 유럽연합, 독일, 영국, 중국, 일본)의 법·제도 및 정책 동향과 소프트웨어 안전에 대한 표준 및 가이드를 중점적으로 조사하였다.

제4장에는 국내 소프트웨어 안전 산업동향을 분석한다. 이번 조사에서는 2016년에 정립된 프레임웍(Framework)을 기반으로 조사 모수를 늘리고, 조사 항목을 최신 동향을 반영하여 보완하였다. 조사 그룹별 조사 대상에서 소프트웨어 안전 학계·정부, 소프트웨어 안전 컨설팅 그룹의 경우 소프트웨어 안전과 직/간접적으로 연관이 많은 대상을 선정하여 조사를 실시하였고, 소프트웨어 안전 개발·사용자그룹의 경우는 소프트웨어 안전과 직/간접적으로 연관이 많은 기업을 우선 선정하였고 추가로 소프트웨어 안전 직/간접적으로 낮더라도 주요 업종별 대표기업의 경우 조사 대상으로 선정하여 산업 전반적인 소프트웨어 안전 개념의 이해 및 인지도를 조사하였다.

---

1) TIC(Testing, Inspection and Certification) 기업이라고도 부른다.

제5장과 제6장에는 소프트웨어 안전 확보를 위한 요인을 분석하고 국내 소프트웨어 안전 산업 활성화 방안을 제시하였다.

제7장에서는 결론과 향후 과제에 대해 제시하였다.

4. 연구 내용 및 결과

이머징(Emerging) 산업인 자율주행차, 드론에 대한 정부의 활동(법・제도, 국가기관, 표준 제정)의 측면과 기능/소프트웨어 안전 측면의 2가지 주제에 대해 미국, 유럽연합(EU), 독일, 영국, 중국, 일본 등의 국가를 조사하였다.

- 법・제도/규정

1. 이머징 산업은 특성상, 대부분의 해외 주요 국가에서는 프레임워크 수준의 법・제도를 제정하거나 제정 중에 있었는데, 주요 내용은 해당 산업에 대한 정의, 규제 범위, 규제 구분, 규제 기관 및 규제 기관의 권한, 안전 및 책임에 대한 포괄적 가이드라인 등이다. 해당 산업을 선도하기 위해 각 국은 법・제도를 다소 느슨하게 적용하여 규제 보다는 지원 및 산업활성화 방향으로 제정되어 있었다.

2. 국가별 산업 환경, 국민 정서 등의 중요시 하는 부분이 달라, 법・제도가 상이하게 제정되는 경우도 있었는데, 자율주행차의 경우 독일은 사고 시 차량 운전자가 사고에 대한 책임이 있다고 명시한 반면, 영국은 자율 주행 시 발생하는 차량 사고에 대해 차량 운전자에 대한 책임을 묻지 않았다. 미국은 기능안전, 연방/주 간 권한 및 책임 등에 대해 주안점을 두고 있었다. 일본의 경우 산업 측면에서 자율주행 관련 표준을 선점하기 위해 자율주행 기능 중심으로 가이드라인을 제시하였다.

3. 융복합적인 성격을 띠고 있는 산업의 경우, 법・제도에서 타 산업 제도를 활용하거나, 참조하는 경우가 많았다.

- 관리 기관

1. 이머징 산업인 자율주행차, 드론에 대해 모두 기존 정부의 관리 기관이 관리 영역을 확대하여 관리하며, 이머징 산업 및 전통적인 산업 모두 규정 제정, 관리/감독, 지침/가이드 연구 및 지원, 관련 산업 성장 지원 등을 하고 있다.

2. 융복합적인 성격(항공, 자율주행차, 드론 등)을 띄고 있는 산업의 경우, 주관 기관은 타

기관(정부 기관, 연구 기관, 사설 기관 등)과 법・제도 제정, 관리/감독, 지침/가이드 제정 등의 분야에서 긴밀한 협업을 하고 있었다. 또한, 이러한 협업은 업무 주관 관점 보다는 업무 조정 관점에서 진행되는 경우가 많았다.

- 기능/소프트웨어 안전 표준, 지침, 가이드

1. 전통적 안전 관련 산업은 안전 표준, 지침, 가이드가 상세하게 기술 되어 있었으며, 국제 표준 또한 존재하고 있었다. 반면, 이머징 산업은 아직 이러한 표준, 지침, 가이드가 없었고, 심지어 국제 표준이나 각 국가별 표준도 없는 상황이었다.

2. 이머징 산업은 새로이 만들고 있는 표준 일부 영역에 전통 안전 관련 산업의 표준을 활용하라고 권고하고 있었는데, 자율주행차는 ISO 26262, 드론의 경우 항공 표준인 DO-178 등이 있었다.

해외 및 국내 TIC 시장에 대해서 조사한 결과 주요 시사점을 도출하였다.

- 해외 TIC 시장은 높은 수익성이 보장되는 안정적인 시장이며, 사업 지역/영역 확장, 기술경쟁력 강화를 위한 M&A 활발히 진행 중이다.

전방 시장이 규제 시장인 관계로 안정된 성장세가 유지될 것으로 보인다. 또한 사업상 Risk 및 투자비가 적기 때문에 높은 수익성 유지가 가능하다.

- 시장 내/외부 변수들의 변화 방향이 대체로 TIC 시장 성장에 긍정적이며, 해외 TIC 시장은 앞으로도 안정적으로 성장할 것으로 전망된다.

시장 내외부 변수의 긍정적 영향과 시장 안정성/수익성을 바탕으로 ’23년까지 연 5%씩 성장이 예상된다.

- 국내 TIC 시장은 여전히 성장이 제한적일 것으로 보인다.

국내 사업자들은 해외 사업자들보다 경험이 부족하여 경쟁력이 떨어져 공공 부문에서 민간 부문으로 확장은 어려울 것으로 보이며, 민간 부문으로의 확장을 추진하더라도 민간 부문의 드론, 자율주행 등 신산업 관련 전방시장이 해외에 비해 더딘 발전 또는 낮은 경쟁력을 보여 양쪽 모두 성장 또는 확장이 어려울 수 있다.

국내 소프트웨어 안전 산업 동향 분석 결과 도출된 주요 시사점을 6개 카테고리(법・제도,

인증・매뉴얼・표준, 인력・교육, 조직・기관, 사업 환경 개선, 프로세스)로 구분하여 분석 및 정리하였다.

1) 소프트웨어 안전분야 학계・정부(Governing Sector)

법・제도 측면에서는 소프트웨어 안전사고 발생 시 대응체계와 사후 처리에 대한 내용을 법제화할 필요가 있다. 그리고 제4차 산업혁명과 함께 급부상한 주요 기술분야 (인공지능, 빅데이터 등)에 대한 규제나 가이드라인 수립이 필요하다.

인증・매뉴얼・표준 측면에서는 국가 전략사업과 연계한 중점 표준화 추진 분야에 대한 장기적 지원과 국제표준 전문가 양성이 중요하다.

인력・교육 측면에서는 산업별 도메인 지식을 보유한 소프트웨어 안전 분야 인력양성이 필요하다는 의견이 2015년, 2016년에 이어 지속적으로 제기되었다.

조직・기관 측면에서는 소프트웨어 안전 전문가를 보유한 전문기관 설립이 필요하다는 의견이 2015년부터 지금까지 지속적으로 제기되었다.

사업 환경 개선 측면에서는 TIC 기업의 역량향상을 위해 공공부문에서 소프트웨어 안전 프로젝트 참여기회를 최대한 제공하여야 하며, 소프트웨어 안전이 적용된 제품의 가치를 인정해주는 사회적 인식이 확산되어야 한다.

프로세스 측면에서는 특정 부처 영역에서 소프트웨어 안전관련 문제가 발생했더라도 해당 조사반에 소프트웨어 전문가가 포함된 범부처 차원의 통합적 대응을 할 수 있는 체계가 필요하다.

2) 소프트웨어 안전분야 사업기업(Supervising Sector)

법・제도 측면에서 소프트웨어 안전분야 법・제도의 구체화에 대한 요구가 2016년과 마찬가지로 매우 높게 나타났다.

인증・매뉴얼・표준 측면에서는 소프트웨어 품질 중심의 기존 인증제도보다는 위험원 분석, 위험저감 방안 등이 요구사항과 설계단계에 반영되었는지 여부를 판단하는 것을 더욱 중요시하는 것으로 나타났다.

인력・교육 측면에서는 산업별 도메인 지식을 갖춘 소프트웨어 안전 전문가가 수요에 비해 부족하므로 소프트웨어 개발자 재교육, 전문 프로그램 운영 등을 통해 소프트웨어 안전

전문가를 양성해야 한다. 가장 필요가 분야가 위험분석가로 나타났다.

조직・기관 측면에서는 소프트웨어 안전관련 전문가를 보유한 전문기관의 신설을 통해 소프트웨어 안전관련 사안에 대한 총괄적인 조정을 담당하는 것이 필요하다.

사업 환경개선 측면에서는 다양한 산업 도메인 레퍼런스 확보가 향후 중요한 경쟁요소로 작용할 것이며, 해외 시장 진출을 위해 국제표준, 외국어, 실무경험을 갖춘 인력이 중요하다는 의견이 주를 이루었다.

프로세스 측면에서는 기존 품질관리 차원의 통합테스트에서 안전 및 품질예방 차원의 위험도 분석에 대한 중요도가 점차 높아지고 있는 것으로 조사되었다.

3) 소프트웨어 개발사용자(End User Sector)

법/제도 측면에서는 일반 사용자 기업이 소프트웨어 안전과 관련된 활동이나 시스템 (프로세스, 매뉴얼, 인증 등)을 갖추기 위해서는 원가 측면의 부담이 발생하기 때문에, 소프트웨어가 사업의 핵심이면서 이미 법/제도로 안전 준수가 강제화된 기업들 외 일반 소프트웨어 사용 기업들은 자발적 도입이 어려워 소프트웨어 안전에 대한 국가 차원의 일정 비율 비용 부담이나, 관련된 혜택을 제공해 달라는 의견이 있었다.

또한 일반 사용자 기업들 입장에서는 원가 부담을 최소화하는 것이 일반적인 경영 활동 방향이라 소프트웨어 안전 도입에 소극적이거나 동기 부여가 어려우므로, 법/제도 측면에서 최소한의 수준에서 준수해야 할 소프트웨어 안전 수준을 구체화/강제화하여야 한다는 의견도 있었다.

인증/매뉴얼/표준 측면에서는 대부분 신생 기업이나 대기업의 2차, 3차 하청으로 단계가 내려갈수록 인증/매뉴얼/표준이 필요하나 도입이 어려운 경우가 많았다. 이러한 기업들은 필수적으로 필요한 영역에서 기업 내부적으로 소프트웨어 안전 관련한 활동을 수행하고 있었는데, 국가 차원에서 소프트웨어 안전 전문가 양성이나 도구를 지원해 준다면 도움이 될 것이라는 의견이 있었다.

인력/교육 측면에서는 기업이 자발적으로 소프트웨어 안전 관련한 내부 전문가를 양성하거나 교육을 추진하기 어려우므로, 국가에서 소프트웨어 안전 관련한 체계적인 교육이나 전문가 양성 과정을 지원해 주기를 기대하였다.

조직/기관 측면에서는 소프트웨어 안전과 관련한 문제나 어려움을 해결하기 위한 정부의

소통 창구가 여러 조직에 분산되어 문제 해결의 진행이 어려운 상황이라 소통 창구의 일원화가 필요하다고 주장하였다.

사업 환경개선 측면에서는 소프트웨어 안전과 관련한 사고 이력이나 시험 이력/노하우 등의 확보가 필요한데, 개별 기업 내부적으로 이를 확보/관리하기에는 인적, 금전적 자원의 조달이 어려워 국가 차원의 소프트웨어 안전관련 사고 이력, 시험 정보 수집 및 공유 플랫폼을 지원해 달라는 의견이 있었다.

프로세스 측면에서는 대부분의 기업들이 소프트웨어 안전 관련한 사항이나 요구사항들을 제품/서비스 기획 초기 단계부터 암묵적으로 반영하고 있는 것으로 확인되었다.

본 조사를 통해 법・제도, 관리기관, 소프트웨어 안전 표준, 지침, 가이드 측면의 3개 측면에서 소프트웨어 안전 확보를 위해 나아가 방향을 제시하였다.

1) 법・제도

이머징 산업을 포함한 대부분의 산업의 경우, 국내 산업 발전과 해외 선도를 위해 이를 적극적으로 지원, 육성하는 방향성이 필요한데, 공공안전이 필수적인 일부 경우를 제외 하고는 법/규제를 느슨하게 하여 산업이 자발적으로 활동할 수 있는 기회를 최대한 보장하도록 하는 것이 필요하다. 또한, 해외 동향을 참고하되, 국내 산업, 문화, 국민 정서 등을 고려하여, 법・제도 규정이 필요하다. 타 산업 분야 법・제도를 적극 참고하고 활용해야 한다. 국가 발주 프로젝트에 소프트웨어 안전 포함 의무화, 공공부문의 소프트웨어 안전성 요구사항 준수 규정 법제화, 안전 중요 산업별 특성을 반영한 소프트웨어 안전관련 법・제도 상세화 , 사전예방 및 재발 방지를 위한 원인분석 및 사후 처리, 국가 소프트웨어 안전을 총괄할 수 있는 체계의 법제화가 필요하다. 소프트웨어 안전 산업 환경 개선을 위해서는 소프트웨어 및 소프트웨어 안전 대가 현실화, 소프트웨어 안전 전문가 육성 및 연구에 대한 지원이 필요하다. 정부기관은 소프트웨어 안전 법・제도/규정에 대한 제안 역할을 수행하는 전담조직을 신설하고 소프트웨어 안전 관련 정부 소통 창구를 일원화할 필요가 있다.

2) 관리기관

최근 해외 동향에서 보았듯이, 주요 산업들이 고도화되고 융복합화되면서, 여러 산업 도메인을 걸쳐서 영향을 주고받는 경우가 급증하고 있다. 기존 정부기관은 산업별로 나누어져

각 해당 분야별로 전문적인 규제, 관리, 지원 등을 하고 있으나, 융복합화 되는 현 시점에서는 기존 전문성 및 역할을 유지하면서, 이를 보완해야 할 필요가 대두된다.

소프트웨어 안전의 경우, 소프트웨어 지식도 중요하지만 우선적으로 해당 산업 분야의 지식(도메인 지식)이 필수적이며, 최근 이머징 산업인 자율주행차, 드론 등의 산업 분야 융복합화가 급격히 진행되고, 소프트웨어 안전이 핵심적인 부분이라 소프트웨어 안전을 위해서는 여러 산업 분야 국가 기관뿐만 아니라 산업체, 연구기관의 협업은 필수적이다.

소프트웨어 안전 관리 기관에서는 국가 소프트웨어 안전 프레임웍 및 방향 수립, 국가 프로젝트의 소프트웨어 안전 부분 요건 기본 요건 정의 및 관리, 공공 부문 소프트웨어 안전성 요건 정의 및 관리, 사전예방 및 재발 방지를 위한 원인분석 및 사후 처리 등으의 활동을 수행해야 한다. 또한 국내 소프트웨어 연구 및 정책, 가이드, 지침을 제안하고, 소프트웨어 안전 인력 육성에 힘써야 한다.

3) 소프트웨어 안전 표준, 지침, 가이드

기존 소프트웨어 안전 관련이 높은 산업은 국내에서도 소프트웨어 안전 표준, 지침, 가이드가 상세히 정리되어 있고 해외 표준도 존재하고 있으나, 이머징 산업의 경우 국내, 해외 모두 표준, 지침 등이 없는 상황이다. 이러한 융복합적인 이머징 산업이 지속적으로 나타나고 성장할 것으로 예상되므로, 특히 소프트웨어 안전이 중요한 융복합 이머징 산업의 경우 선도적인 차원에서의 소프트웨어 안전 표준, 지침, 가이드 제정이 시급한 상황으로 보인다.

5. 정책적 활용 내용

본 조사에서는 해외 안전선진국의 안전 관련 법제도와 산업현황, 국내 소프트웨어 안전 산업 동향을 조사하고 국내 안전 산업의 문제점과 나아갈 방향 제시하여 소프트웨어 안전 정책의 기초자료로 활용할 수 있다.

6. 기대효과

본 자료는 소프트웨어 안전 산업 활성화하는데 정책 마련의 기초자료가 되며, 안전이 중요한 산업에서 소프트웨어 안전이 확보된 융복합을 통한 새로운 서비스가 정착하는 기반을 제공할 것이다.

SUMMARY

1. Title: Software Safety Industry Trends Study

2. Purpose and Necessity of the Research

The purpose of this study is to provide reliable data for enhancing the domestic software safety policies. The study covers the survey the changing trends of the domestic software safety industry over the past two years and derive the key success factors (KSF) by comparing the policies of overseas major countries on software safety and global TIC market situation

3. Composition and Range

In Chapter 1, we present the background, purpose of the research on the software safety industry trends, and the way of the research carried out in this study.

In Chapters 2 and 3, we investigate laws, institutions, guidelines on software safety and overseas TIC (Testing, Inspection and Certification) companies.

In Chapter 4, we analyze the domestic software safety industry trends.

In Chapters 5 and 6, we analyze the factors for ensuring software safety and suggested ways to activate the domestic software safety industry.

In Chapter 7, we present conclusions and future work.

4. Main Contents and Results

Based on the survey framework established in 2016, this survey was made by increasing the number of surveyed sectors and revising / supplementing the survey items for each sector by reflecting the latest trends. For the overseas TIC market, the business performances of major TIC companies in 2017, their perspective on the market, the attractiveness factors of the TIC market were studied.

The following three areas are derived from the benchmarking results of self-driving cars and drones: laws and regulations, management institutions, safety standards and guidelines.

For, Laws and Regulations, Emerging industries have been in the process of enacting or enacting framework-level laws and regulations in most of the major foreign countries. The main contents are the definition of the industry, the scope of regulation, the division of regulations, the authority of regulators and regulators, and comprehensive guidelines for safety and liability. Major foreign countries established rule and regulations loosely to provide support and revitalize the industry. There were cases where laws and systems were enacted differently, with different emphasis placed on industrial environments and national sentiment. In the case of industries with complex characteristics, there were many cases where laws and systems used or referred to other industrial systems.

Emerging industries like Self-driving cars and drones are all managed by existing government management institutions.

The traditional software safety-related industries have detailed safety standards, guidelines, and guides, and there were also international standards. On the other hand, the emerging industry has yet to have such standards, guidelines, and guides, and even international or national standards. Emerging industries were encouraging to utilize the standards in traditional safety-related industries like ISO 26262 for autonomous vehicles and DO-178 for drones.

The major implications of the survey on foreign and domestic TIC markets are as follows:

- Overseas TIC markets are stable markets with high profitability.
- Changes in internal/external variables are generally positive for growth in the TIC market.
- The overseas TIC market is expected to grow steadily in the future
- Domestic TIC market still seems to have limited growth

The main implications of the analysis of domestic software safety industry trends are divided into 6 categories (law/system, certification/manual/standard, manpower/education, organization / institution, industrial environment improvement, process).

Category	Governing Sector	Supervising Sector	End User Sector
Law / System	• Legalization and Institutionalization of software safety-related responses and follow-up measures	• Need to clarify the laws and systems related to software safety by industry	• Help to reduce the cost of introducing/ enhancing corporate software safety
	✓ Need to clarify high-level software safety-related laws and systems that may include various industrial characteristics		
certification /manual /standard	• Need to support international standardization from a strategic/long-term perspective	• Applying Software safety is more important than formal certification	• For most start-ups and small companies, certification / manual / standard are insufficient
	✓ Need government to support and train standard experts to lead international standardization ✓ High-use manuals and tools on site are necessary		
manpower / education	• Deepening of labor shortage related to software safety • Need to train software safety experts	• Lack of software safety experts • Need to train software safety experts	• Need to support training of practitioners of companies using software
	✓ Due to lack of software safety experts, training of professional manpower is urgent		
organization / institution	• Need to establish a professional agency with software safety capability	• Need to establish professional organizations with software safety experts	• Communication channel for overall complaints of software including software safety is necessary
	✓ Establishment of specialized institutes with expertise in software safety is necessary		

industrial environment improvement	• Need to provide references related to software safety in the public sector	• Industry-specific references are key competitive elements	• National level collection and sharing platform are required
	✓ Continuing efforts to secure domestic and international references regarding software safety ✓ Need to raise social awareness about the importance of software safety		
process	• government response is required in case of software safety-related issues	• Increase the importance of risk analysis in software safety processes	• Accident history related to software safety
	✓ Increase the importance of proactive risk analysis rather than integration testing in software safety processes		

5. Policy use

This study investigates safety related legislation, overseas and domestic software safety industry trends, and presents problems and directions for the domestic safety industry, and can be used as a basis for software safety policy.

6. Research Implication and Expected Effects

This document will serve as the basis for policy making in the activation of the software safety industry and provide the basis for the establishment of new convergence services through the software safety in safety-critical industries.

CONTENTS

제1장 서론

제1절 개요

1. 배경 및 필요성

최근 이슈인 주요 IT 기술과 소프트웨어 안전의 발전이 단순 인간 생활을 편리함과 즐거움을 제공해 주는 수준을 넘어 인간의 재산, 신체 및 생명에 영향을 미칠 수 있는 가능성에서 최근에는 실제로 그러한 가능성이 현실화되는 상황이 도래함으로써, 소프트웨어 안전은 이제 체험 가능한 수준으로 급속히 우리의 생활에 파고들고 있는데, 최근 몇 건의 자율주행차 사고에 따른 운전자의 사망 사건과 AI(인공지능)의 군사용도 개발, 드론의 테러 활용 가능성 증대 등이 그것이다.

2015년, 2016년에 걸친 2차례 소프트웨어 안전 동향 조사 후, 2년이 지난 2018년에 소프트웨어 안전 동향 조사를 수행하는 이유는 국내에서는 소프트웨어 안전 분야가 대부분의 산업에서 조금씩 인식이 개선되고 있음에도 여전히 생소한 개념으로 받아들여지고 있으며, 최근 이슈인 AI(인공지능), 자율주행차, 드론 등의 IT 기술 및 환경의 변화도 초-중기 단계로 1-2년 단위로 많은 발전이 이루어지고 있어, 매년보다는 격년 조사가 국내의 느린 소프트웨어 안전 인식 변화 및 빠른 IT 기술 변화를 감안하여 적합할 것으로 판단되었기 때문이다.

2015년 소프트웨어 안전 동향 조사에서는 조사 프레임웍 정의, 조사 대상 선정 및 조사항목 정의 등을 통해 기본 조사의 틀을 수립하여, 처음으로 국내 소프트웨어 안전 산업 동향을 파악하고, 해외 주요 TIC(Testing, inspection and certification) 기업 트렌드와 주요 산업 도메인(자동차, 철도, 우주항공, 원자력)별 해외 주요국(미국, 영국, 독일, 일본 등)의 소프트웨어 안전 관련 법제도, 주요 표준 등을 조사하여 이를 국내 현황과 비교 분석하였다.

2016년 소프트웨어 안전 동향 조사에서는 주요 산업 도메인으로 의료 부문 해외 주요국의 소프트웨어 안전 정책을 추가하여 조사하고, 국방 관련 소프트웨어 안전 표준을 조사하였고, 최근 이슈가 되고 있는 자율주행차 관련 미국 도로교통안전국(NHTSA)에서 세계 최초로 발표한 자율주행차 정책[2]에서 성능 가이드라인을 조사하였다. 국내

2) Federal Automated Vehicles Policy

안전 산업 분석에서는 소프트웨어 안전관련 학계・정부 전문가, 소프트웨어 안전분야 사업기업, 소프트웨어 개발・사용 기업 등을 인터뷰 및 설문조사하였다.

2. 목적

본 연구의 목적은 2년간 변화된 국내 소프트웨어 안전 산업 동향을 조사하여 기존 연구와 비교・분석하여 핵심성공요소(CSF)를 도출하고, 최근 이슈화 되고 있는 주요 기술 중 소프트웨어 안전이 중요시 되고 있는 기술인 자율주행차, 드론에 대한 해외 주요국의 정책, 글로벌 TIC 시장현황을 조사 한 후, 국내 현황과 비교분석을 통해 국내 소프트웨어 안전 산업 및 문화를 제고를 위한 신뢰성 있는 정책 기초 자료를 제공하기 위함이다.

제2절 연구방법 및 범위

1. 국내 소프트웨어 안전 현황 조사 방법

이번 조사에서는 2016년에 정립된 프레임웍(Framework)을 기반으로 각 조사 섹터별(조사 모수를 늘리고, 각 섹터별 조사 항목을 최신 동향을 반영하여 수정/보안 하는 등으로 현행화하였다. 조사 섹터별 조사 대상은 소프트웨어 안전 학계・정부(Governing Sector), 소프트웨어 안전 컨설팅(Supervising Sector) 그룹의 경우 소프트웨어 안전과 직/간접적으로 연관이 많은 대상을 선정하여 조사를 실시하였고, 소프트웨어 안전 개발・사용자(End User Sector) 그룹의 경우는 소프트웨어 안전과 직/간접적으로 연관이 많은 기업을 우선 선정하였고 추가로 소프트웨어 안전 직/간접적으로 낮더라도 주요 업종별 대표기업의 경우 조사 대상으로 선정하여 산업 전반적인 소프트웨어 안전 개념의 이해 및 인지도를 조사하였다.

1) 범위 및 대상

조사 범위는 2016년 사용된 국내 조사 프레임웍을 토대로 각 그룹별 정의를 정제화하여, 소프트웨어 안전 학계・정부(Governing Sector), 소프트웨어 안전 컨설팅(Supervising Sector), 소프트웨어 안전 개발・사용자(End User Sector) 그룹으로 구분하

여 동향조사를 실시하였다.

[그림 1-1] 국내 소프트웨어 안전 현황 조사 프레임웍

주요 변화로는 국내 산업 전반적으로 소프트웨어 안전에 대한 인식 및 대응 현황을 파악하기 위해, 소프트웨어 안전 개발·사용자(End User Sector) 그룹에 대한 정의를 소프트웨어가 설치된 제품 및 서비스를 제공하거나 활용하는 주체로 확대하였다. 따라서 조사 범위가 기존 소프트웨어 안전 관련이 많은 제품/서비스/인프라를 제공 및 사용하는 주체들(2016년 조사 범위)에서 소프트웨어를 통해 제어하고 운영하는 제품/서비스/인프라를 제공 및 사용하는 주체(2018년 조사 범위)로 확대되었다.

<표 1-1> 2016년 대비 2018년 조사 그룹별 정의 및 조사범위 비교

조사그룹	구분	2018년 조사	2016년 조사
소프트웨어 안전 학계・정부 (Governing Sector)	정의	• 변화없음	• 소프트웨어 안전성 확보를 위한 정책적/학술적 차원의 역할을 수행하는 주체
	범위	• 변화없음. 추가로, 소프트웨어 안전과 관련이 높은 산업 도메인(자동차, 철도, 원자력 등)에 속한 주요 연구 기관 포함	• 소프트웨어 안전 관련 법・제도 제정 기관 • 소프트웨어 안전 연구/표준 수행 기관
소프트웨어 안전 컨설팅 (Supervising Sector)	정의	• 변화없음	• 소프트웨어 테스팅, 검사/인증 등의 활동을 통해 소프트웨어 안전을 점검하는 주체
	범위	• 소프트웨어 안전 전문 기업 중심(변화없음)	• TIC 기업(소프트웨어 테스팅, 검사 및 인증 산업 종사 기업)과 소프트웨어 안전 전문 기업(제품의 기능 안전 산업 종사 기업)
소프트웨어 안전 개발・사용자 (End User Sector)	정의	• 소프트웨어가 설치된 제품 및 서비스를 제공하거나 활용하는 주체	• 제품 및 서비스 등에 소프트웨어 안전을 활용하는 주체
	범위	• 소프트웨어를 통해 제어하고 운영하는 제품/서비스/인프라를 제공 및 사용하는 주체	• 소프트웨어 안전 관련이 많은 제품/서비스/인프라를 제공 및 사용하는 주체

소프트웨어 안전 학계・정부(Governing Sector)에 대한 정의는 2016년 사용된 ‘소프트웨어 안전성 확보를 위한 정책적/학술적 역할을 수행하는 주체’을 변경 없이 사용하였으나, 조사 대상의 경우 기존의 정부 기관 및 학계뿐만 아니라 소프트웨어 안전과 관련이 높은 도메인(자동차, 철도, 원자력 등)에 속한 주요 연구 기관을 포함 시켜 보다 폭넓은 조사를 수행하였다.

소프트웨어 안전 컨설팅(Supervising Sector)은 소프트웨어 테스팅, 검사/인증 등의 활

동을 통해 소프트웨어 안전을 점검하는 주체로써 TIC 기업(소프트웨어 테스팅, 검사 및 인증 산업 종사 기업)과 소프트웨어 안전 전문 기업(제품의 기능 안전 산업 종사 기업)을 대상으로 하였다.

2) 조사항목

이번 조사는 2015년, 2016년 시계열적 비교 분석을 위해, 조사 항목의 큰 틀을 바꾸기 보다는 세부 질의 항목에서 답변이 어려운 질문을 삭제 또는 명확화하고, 설문 대상자가 답변을 꺼리는 질문에 대해서는 간접적인 질문을 통해 우회화 하고, 유사한 질문 통합 등을 통해 정제 및 고도화에 주안점을 두었다. 주요 추가 질문으로는 시장 관점에서 국내 소프트웨어 안전에 활성화 가능성을 조사하기 위해, 소프트웨어 안전 시장 관점(Market)의 질문들을 추가하였다.

소프트웨어 안전 학계・정부의 경우 소프트웨어 안전에 대한 정의 및 개념과 법・제도/정부의 역할과 소프트웨어 안전 활동 관련 표준화 동향 및 필요 사항과 소프트웨어 안전 관련 국내시장 현황 및 전망 등을 물었고, 마지막으로 세계적인 소프트웨어 안전 동향 및 시장에 대하여 질문하였다.

소프트웨어 안전 컨설팅은 인터뷰 대상 업체의 주요 고객 및 주요 제공 서비스 산업군 및 보유 역량 등과 같은 기업 일반 현황과 소프트웨어 안전에 대한 개념, 소프트웨어 안전 확보를 위한 프로세스 및 인프라, 소프트웨어 안전 산업 시장에 대한 현황 및 견해, 소프트웨어 안전 산업 활성화를 위한 지원요청 사항 등을 조사하였다.

소프트웨어 안전 개발・사용자의 경우 주요 소속 산업군, 제품/서비스를 개발 및 사용하는 과정에서 소프트웨어 안전을 담보하기 위한 인력/조직 체계, 프로세스 및 인프라, 정부 지원 요청 사항 등을 조사하였다.

<표 1-2> 조사 대상별 조사 항목

조사 대상	주요 조사 항목
소프트웨어 안전 학계・정부 (Governing Sector)	• 소프트웨어 안전 정의 및 개념 • 소프트웨어 안전 법・제도/정부 문제점 및 개선방안 • 소프트웨어 안전 표준화 및 국내/외 활동 • 소프트웨어 안전 시장 현황 및 전망 • 해외 대비 국내 여건 차이 분석 및 차이 극복 방안
소프트웨어 안전 컨설팅 (Supervising Sector)	• 소프트웨어 안전 정의 및 개념 • 기업현황: 주요 제공 서비스, 서비스 제공 산업분야 및 고객현황, 전문가 및 인증 확보, 해외 대비 국내 기업 차이 분석 및 극복 방안, 해외 진출 시 필요 역량 • 프로세스 현황: 예방, 탐지, 대응, 사후 활동 • 소프트웨어 안전 산업/시장: 산업 구분에 대한 견해, 진입 장벽, 시장 전망 • 인프라 측면: 표준/매뉴얼, 인력/조직, 시스템 • 지원 요청 사항: 법・제도, 인력 및 시장 개발 측면
소프트웨어 안전 개발・사용자 (End User Sector)	• 소프트웨어 안전 정의 및 개념 • 인력/조직 체계: 소프트웨어 안전사고 예방/대응 관리 조직 및 역할, 내부 보유 전문 인력/자격요건 현황, 소프트웨어 안전 관련 표준/매뉴얼 보유 현황 • 소프트웨어 안전 예방점검 활동: 소프트웨어 개발/도입/변경 시 소프트웨어 안전 사전 점검 활동 • 소프트웨어 안전 대응관리 활동: 소프트웨어 안전사고 발생 시 대응 방안 및 사후관리 방안 • 지원 요청 사항: 법・제도, 인력 및 시장 측면

3) 조사방법 및 경과

이번 조사는 소프트웨어 안전과 관련이 높은 설문 대상의 경우 최대한 일대일 대면 인터뷰를 수행하였고, 부득이 한 경우 전화로 사전 설명 후, 설문 조사를 수행하였다. 소프트웨어와 안전과 관련이 보통이거나 낮은 대상의 경우는 주로 설문 조사를 수행하였는데, 설문 답변의 신뢰도를 높이기 위해 일부 대상은 일대일 대면 인터뷰를 수행하기도 하였다.

<표 1-3> 국내 현황 조사 대상 및 조사 경과

구분	조사 대상	조사 경과
소프트웨어 안전 학계・정부 (Governing Sector)	• 대학: 4개 • 주요 도메인별 연구/공공 기관: 7개	• 6개 방문 인터뷰 • 5개 설문 인터뷰 • **총 11개 조사 수행**
소프트웨어 안전 컨설팅 (Supervising Sector)	• 기능 및 소프트웨어 안전 컨설팅: 9개	• 1개 방문 인터뷰 • 8개 설문 인터뷰 • **총 9개 조사 수행**
소프트웨어 안전 개발・사용자 (End User Sector)	• 우주항공: 3개 • 의료: 4개 • 자동차: 7개 • 철도: 1개 • 국방: 0개 • 원자력: 1개 • 정보통신: 17개 • 도로교통: 2개 • 일반: 37개	• 19개 기업 방문 인터뷰 • 53개 기업 설문 인터뷰 • **총 72개 조사 수행**

이번 조사에서는 총 92개의 대상에 대해 설문 및 대면 인터뷰 조사를 실시하였다. 소프트웨어 안전 학계・정부 그룹의 경우, 대학 4개 주요 도메인별 연구/공공기관 7개로 총 11개 대상에 대해 설문 조사를 수행하였는데, 그룹의 특성상 구조화된 설문보다는 주요 조사 내용 근간으로 해서 자유롭게 묻고 답하는 식의 일대일 대면 인터뷰를 주로 진행하였으나, 일부 대상의 경우 간략한 설문지를 제공하여 설문에 답하면서 인터뷰를 수행하는 방식으로도 진행하였다. 소프트웨어 안전 컨설팅 그룹의 경우, 총 9개 대상에 대해서, 구조화된 설문지를 사용하여 설문을 수행하되 비대면 방식으로 진행되었는데, 이는 이 그룹의 특성상 모수가 작고 지난 조사 대비 변화가 설문 대상 기업의 변화가 거의 없으며, 해당 대상 기업 대부분은 이미 2차례 대면 인터뷰를 통해 본 설문의 취지 및 내용에 대해 충분히 알고 있기 때문이었다. 소프트웨어 안전 개발・사용자 그룹은 총 72개 대상에 대해 설문 조사를 실시하였는데, 자동차, 철도, 우주 항공 등의 소프트웨어 안전과 관련이 높은 도메인의 기업은 대면 설문 조사를 수행하였고, 안전과 관련이 낮은 기업은 비대면 설문 조사를 수행하였다.

2. 해외사례 조사방법

기 조사에서 수행하였던 주요 산업 도메인별(철도, 국방, 원자력 등) 표준 및 주요 선진국의 안전 보장 활동 대부분 조사되었고, 2년간 변화가 많지 않아, 기 조사된 해외 주요국의 소프트웨어 안전 활동을 정리하고, 최근 급격히 변화하거나 새롭게 중요성이 증가하는 산업인 자율주행차 및 드론 관련 해외 주요국(미국, 유럽연합, 독일, 영국, 중국, 일본)의 법·제도 및 정책 동향과 소프트웨어 안전에 대한 표준 및 가이드를 조사하였다. 마지막으로 소프트웨어 안전 관련 개발, 컨설팅 기업 [3]동향을 조사하였다. 특히, 기존 조사 대비 TIC 시장 동향에 대해 보다 깊은 조사를 하여, 시장 특징, 시장 규모, 성장률뿐만 아니라 해외 시장의 내/외부 변화 방향, 국내 TIC 사업자들의 성장 과정 및 한계, 국내 TIC 산업 전망 및 Risk 등을 조사하였다.

1) 범위 및 대상

이번 조사에서는 새로운 기존 도메인에 포함시켜 법·제도를 제정하기에는 모호하면서, 급격한 기술 발전이 이루어지고 있어 이와 관련된 법·제도, 기술 표준 등의 제정이 시급한 자율주행차 및 드론 산업 분야 관련 해외 주요국의 법·제도, 정책 및 관련 주요 기관을 조사하고 소프트웨어 안전 관련 동향을 조사하였다.

또한, 2016년, 2015년 2년에 걸친 조사에서 소프트웨어 안전이 중요한 산업 도메인[4]에 대한 소프트웨어 안전 표준, 해외 주요국[5]의 법·제도, 정책, 관련 주요 기관 등이 조사되었으므로, 이번 조사에서는 소프트웨어 안전이 중요한 산업 도메인별 해외주요국의 안전 활동(법·제도, 정책, 관련 기관 등)을 종합 정리하였다.

해외 TIC 시장에 대해서는 2016년 조사에서 확인한 TIC 시장 및 사업자 분류 기준에 맞춰 2017년 TIC 시장의 주요 사업자들의 경영 성과와 이들이 시장을 바라보는 시각이 무엇인지, TIC 시장의 매력 요인은 무엇인지, 향후 성장 가능성에 대한 전망은 어떠한지에 대해 조사하였다.

---

3) TIC(Testing, Inspection and Certification) 기업이라고도 부른다.
4) 자동차, 철도, 항공, 원자력, 의료, 국방
5) 미국, 유럽연합, 영국, 독일, 중국, 일본

2) 조사항목

자율주행차의 경우, 미국, 영국, 독일, 중국, 일본의 자율주행차 관련 법·제도 현황 및 간략히 법·제도에 대한 주요 내용을 조사하고, 정부 부처 및 역할, 관련 정책, 그리고 기능 또는 소프트웨어 안전 기술 가이드 등을 조사하였다.

드론의 경우도, 자율주행차와 유사하게, 미국, 유럽연합, 중국, 일본을 포함한 총 4개국에 대한 드론 관련 법·제도 현황 및 법·제도 주요 내용을 간략히 조사하고, 정부 부처 및 역할, 관련 정책, 그리고 기능 및 소프트웨어 안전 기술 가이드를 조사하였다. 자율주행차와 달리 드론의 경우 유럽연합을 추가 조사한 이유는 드론의 경우 유럽연합 법·제도가 최근 제정된 반면, 자율주행차는 법·제도가 아직 제정되어 있지 않고, 다만 로드맵 정도만 존재하기 때문이다.

주요 산업 도메인별 해외 주요국의 소프트웨어 안전 법·제도 및 활동 정리는 2015년, 2016년 조사 내용을 토대로 일부 업데이트 된 부분을 반영하여 수행되었다. 정리한 산업 도메인으로는 자동차, 철도, 원자력, 항공의 4 부문이며, 정부활동(법·제도·지침), 관련조직, 표준의 3가지 구분으로 정리하였다.

해외 TIC 시장 동향에 대해서는 우선 '17년 기준 글로벌 시장의 전체 규모를 조사하였고, Barclays[6]를 비롯한 다양한 연구 기관, 컨설팅 기업의 견해/Report를 참고하여 성장률을 예측하여 '23년까지의 시장 규모를 추정하였다. 또한, 시장 점유율이 큰 시장의 선도사업자 10개사를 찾아내고 이들의 경영 성과 및 시장 점유율, 인수합병 동향을 조사하였다.

6) 바클리즈(Barclays PLC)는 영국에 본사를 둔 글로벌 금융 서비스 기업

<표 1-4> 2018년 선진사례 조사 범위 및 항목

범위	조사 대상	조사 항목
자율주행차	• 미국, 독일, 영국, 중국, 일본	• 법·제도 제정 및 적용 현황 • 담당기관 및 역할 (Roles and Responsibilities) • 관련 지침 및 표준
드론(Drone)	• 미국, 유럽연합, 중국, 일본	• 법·제도 제정 및 적용 현황 • 담당기관 및 역할 (Roles and Responsibilities) • 관련 지침 및 표준
주요국의 소프트웨어 안전 활동	• 산업 도메인: 자동차, 철도, 원자력, 의료, 항공 • 주요 국가: 미국, 유럽연합, 독일, 영국, 일본	• 법·제도 제정 및 적용 현황 • 담당기관 및 역할 (Roles and Responsibilities) • 관련 지침 • 국제 또는 국가별 표준
해외 TIC 시장	• 해외 TIC 사업자 중 시장 점유율 상위 사업자 10개사	• 시장 규모 및 성장 예측 • 시장-사업자 구성 및 점유율 • 주요 사업자 및 경영 성과

3) 조사 방법 및 경과

선진사례 조사 방법은 인터넷을 활용한 문헌 및 홈페이지 조사를 토대로 이루어졌는데, 인터넷 문헌의 경우 국가별 법·제도 제정 관련 홈페이지를 방문하여, 진행 중이거나 발효된 관련 법·제도를 조사하였는데, 본 조사의 특성상 기능 안전 및 소프트웨어 안전과 관련된 문항에 중점을 두어 조사하였다. 통상 상위 수준의 법에서는 기능 및 소프트웨어 안전에 관련된 내용이 직접적으로 언급된 경우가 없어, 상위법에서는 기술 및 기능 관련 포괄적인 요구 사항 등을 조사하고, 지침 및 가이드 수준에서 기능 및 소프트웨어 안전을 요구하는 직/간접적인 내용을 조사하였다. 그리고 이러한 법·제도, 지침/가이드를 준수하기 위한 기관들과 기관들 간의 역할을 조사하고, 기술/기능 및 소프트웨어 안전 표준에 관련된 부분은 국제 표준화 기관[7] 에서 발행된 기술 표준 등을 조사하였다.

홈페이지 조사는 각 국 주 담당 기관 홈페이지 방문하여, 기능/소프트웨어 안전을 점

7) ISO, IEEE, IEC 등

검 및 인증을 위한 절차, 요구사항, 신청서 및 체크리스트 등을 조사하였다. 더불어, 2019년 9월까지 나온 주요 뉴스 등을 조사하여, 최신 법·제도, 기술, 담당기관 등의 활동, 변화 내용 등을 확인하여 반영하였다.

해외 TIC 시장에 대해서는 Barclays를 비롯하여 다수의 해외 연구 기관, 컨설팅 기업의 Report를 조사하였으나, Report 내용의 깊이가 얕고 연구 기관별 시장을 바라보는 시각과 전망이 서로 상이하여, 일부 신뢰할 수 있거나 기관들 간 일관된 예측을 보이는 부분을 제외하고는 시장 점유율 상위 10개 기업의 2017년 사업보고서를 분석하여 직접 조사하였다.

제2장 해외 선진사례 조사

제1절 자율주행차 관련 정책 및 지침/가이드 동향

1. 미국

1) 정부 활동

미국의 자율주행차 정책은 연방 정부 및 주정부로 나누어져 진행되고 있는데, 급격히 발전하는 자율주행차 기술로 인하여 기존 자동차 부문과 달리 연방 및 주정부의 권한 및 역할이 모호한 부문이 있는데, 특히 자율주행차 운영에 관련 운전자에 대한 운전 허가 및 운행을 관장하는 주정부와 시험 및 운영 단계 자율주행차 운행을 장려하려는 연방 정부의 방향 등이 겹치면서 권한 및 역할에 대한 정리가 필요한 상황이다.

• 연방정부의 자율주행차 관련 활동

연방 정부의 자율주행차 관련 활동은 크게 법률 제정과 도로교통안전국의 자율주행차 관련 활동을 들 수 있다.

첫째로 법률 제정의 경우 크게 SELF Drive Act와 AV START Act 2가지를 꼽을 수 있는데, SELF Drive Act의 경우 2017년 9월에 법안이 하원에서 가결 되었고 상원의 결의를 기다리고 있으며, AV START Act 의 경우 현재 상원의 반대로 법안이 수정 중에 있다.

SELF Drive Act (HR 3388)[8]

SELF Drive Act의 주목적은 자율주행차 정착을 위한 규제완화 및 관련 위원회 구성인데, 주요 내용으로는 연방정부의 선수권 확대[9], 연방자동차 안전기준(FMVSS)[10] 업데이트, 연방자동차 안전기준 적용 예외 규정, 연방 자율주행차 자문 위원회 등이 있다.

8) https://www.congress.gov/bill/115th-congress/house-bill/3388
9) Expansion of Federal Pre-emption
10) Federal Motor Vehicle Safety Standards

연방정부의 선수권 확대는 자율주행차 운행관련 주정부의 규제를 주정부가 제한하는 것인데, 만일 주정부가 자율주행차 운행을 제한하려고 시도하면 SELF Drive Act를 적용하여 주정부의 시도를 연방법으로 제한하는 것이다. 전통적으로 자동차 운전자에 대한 운전 허가 및 운행을 평가하고 허가하는 권한을 주정부가 가지고 있기 때문인데, 현재까지는 주정부가 자율주행차 운행을 제한하는 방향으로 법률을 제정한 적은 없었다.

연방자동차 안전기준 업데이트는 자율주행차를 고려하여 안전 표준 업데이트 프로세스를 시작하라고 요구 하는데, 특이할 점은 특정 안전 표준을 요구하거나 규정하지 않는 대신, 도로교통안전국(NHTSA)로 하여금 필요할 경우 특정 안전 표준에 대해 연구하도록 규정해 놓고 있다. 또한, 자율주행차 개발 업체로 하여금 안전 보증 증서를 도로교통안전국에 제출 하도록 규정해 놓고 있다.

연방자동차 안전 기준 예외 부분은 연방 정부가 자율주행차를 출시하려는 차량 제조업체로 하여금 특정 안전 표준의 면제를 제공하는 방법에 대한 최신 정보를 제공하도록 하고 있는데, 현재는 년 2,500건으로 제안되어 있지만 점진적으로 년 100,000건으로 증가될 예정이다.

법안의 마지막 부분에서는 미교통부(DOT)[11]에게 자율주행차 관련 지침 및 조언을 제공하는 자율주행차 자문위원회[12]를 구성하도록 요구하는데, 이 위원회는 비즈니스, 학계 및 독립 연구원, 주 및 지방 당국, 안전 및 소비자 옹호자, 엔지니어, 노동 단체, 환경 전문가, 미 도로교통안전국 및 장관이 지정한 회원들로 구성되어 진다. 위원회의 소위원회는 장관이 임명하는 15 명 이상 30 명 이하인 위원으로 이루어진다.

AV START Act

이 법안은 자율주행차 시대에 예상되는 새로운 위험을 공급자 측면의 규제, 정부의 감독 및 소비자 교육 등을 통해 예방하는 것을 목표로 한다. 이 법안의 주요 내용은 강화된 안전 관리 감독, 연방정부/주정부/지방정부의 역할 강화, 신규 개발 자율주행차량의 시장 진출 규제 축소, 트럭 및 버스의 경우 현재 상태 유지, 사이버 보안 강화, 차량 안전 및 데이터 공유 강화, 소비자 교육 증진, 장애인의 이동성 강화 등이 있다. 이 법안은 2017년 10월 상업 위원회[13]에서 만장일치로 통과되었으나, 신규 자율주행차의 시장 진입 시 느슨한 규제로 인한 사고의 위험, 개인정보 보안의 우려[14] 등의 이유

11) DOT: Department of Transportation
12) highly-automated vehicle advisory council
13) the Commerce Committee

로 상원에서 반대하고 있어 법안 수정이 진행되고 있는 중이다.

총 22개 섹션으로 구성된 이 법안은 자율주행차의 범위를 10,000 파운드[15] 이하 무게의 SAE International J3016에 의해 정의된 자율주행 시스템 3, 4, 5등급[16]을 장착한 차량에 대한 것으로 정의하고, 자율주행차의 테스트, 상업화, 안전을 위한 정책, 기술, 사회이슈, 차량 제조사가 작성해야 하는 문서 요구사항, 신규 소비자 교육 프로그램을 연구하기 위한 위원회, 실무그룹과 전문가 패널을 지정하도록 하고 있다. 또한, 이 법안은 연방 자동차 안전 표준(FMVSS[17]) 중 어떠한 부분이 자율주행차량에 관련되어 업데이트 되어야 될지에 대한 연구를 하도록 요구하고 있으며, 나아가 주 또는 지방 정부가 자율주행차량 시스템 디자인, 제작 또는 성능 표준에 대해 규제하는 것을 금지하는 하고 있는데, 상기 경우가 아닌 부분은 기존의 도로교통안전국과 주정부와의 권한과 역할을 유지하도록 하고 있다.

둘째로, 도로교통안전국의 자율주행차 관련 주요 활동으로는 2016년에 처음으로 발표한 '연방 자율주행차 정책[18]', 2017년 이를 업데이트한 '자동화된 운전 시스템: 안전을 위한 비전[19]' 그리고 2018년 10월 4일에 발표한 '미래 운송의 대비: 자율주행차 3.0'[20]이 있다. 2017년 업데이트된 가이드에서는 자동차 업계, 기술 업계, 민간 시민 및 특수 이익 단체 등의 의견을 수렴하여 개정하였는데, 여기서는 자율 운전 시스템 개발자를 위한 전반적인 안전 및 테스트 방법론, 사이버 보안, 사생활 보호, 사고 후 행동, 소비자 교육 및 훈련 등의 여러 주제에 대한 가이드를 제공한다. 또한, 자율주행차 관련 주정부와 연방정부 간 권한 및 책임, 법률 제정에 대한 모범 사례를 제공하는데, 미 운수부[21]는 연방자동차안전기준(FMVSS)를 만들고 집행하여 자동차 안전 규제에 대한 책임을, 주 정부는 차량 면허, 등록, 교통 단속, 검사 및 보험을 관할 하는 것으로 정의하고 있다. 이 가이드의 영향으로 SELF Drive Act와 AV START Act 모두, 도로교통안전국(NHTSA)이 자율주행차의 설계, 제작 및 성능을 규제하는 독점 정부기관으로 지정하고 있다.

---

14) 이 법안에서는 데이터 프라이버시(Data Privacy)에 대한 언급이 없다.
15) 약 4.5톤 (4,535 kg)
16) SAE Level 3: Conditional automation, SAE Level 4: High automation, SAE Level 5: Full automation
17) Federal Motor Vehicle Safety Standards
18) Federal Automated Vehicle Policy
19) Automated Driving Systems: A Vision for Safety
20) Preparing for the Future of Transportation: Automated Vehicle 3.0 이며, 본 연구 일정 과계상(2018년 10월 25일 완료) 다루어지지 않았다.
21) Department of Transportation

<표 2-1> 연방정부 vs 주정부의 권한

도로교통안전국의 권한	주 정부의 권한
• 신규차량 및 차량 부품에 대한 연방차량안전표준(FMVSS) 제정 (차량 판매전 제조사가 반드시 준수에 대한 증명 필요) • 연방차량안전표준(FMVSS) 준수 강제화 • 안전 관련 결함과 연방차량안전표준 미준수 관련 리콜 및 처리를 조사/관리 • 대중을 대상으로 차량 안전 이슈를 교육하고 소통	• 관할 구역 내 차량 등록 및 운전면허증[22] 발급 • 교통 법규 제정 및 집행 • 안전 점검 실시 • 차량 보험 및 책임 규제

• 주정부의 자율주행차 관련 활동

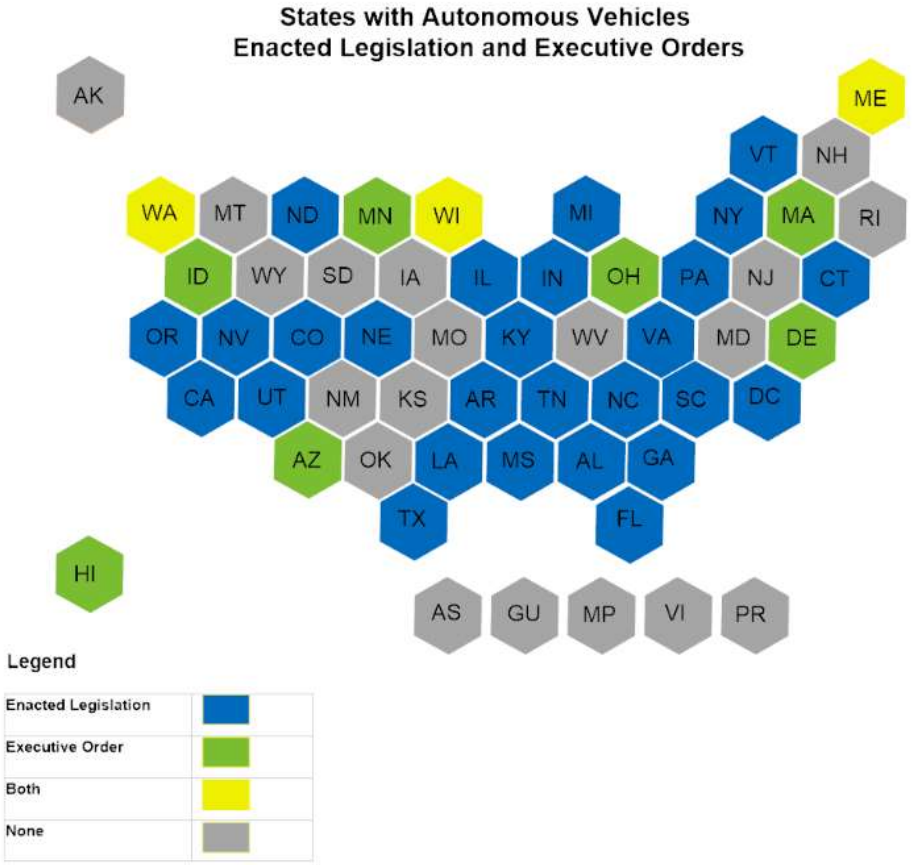
주정부의 자율주행차 관련 법 제정도 적극적인데, 네바다(Nevada)주가 2011년 처음으로 자율주행자 운행 법안을 통과한 이후, 2018년 6월 기준 21개 주[23]가 자율주행차 운행에 대한 법안을 통과시켰고, 10개의 주[24]가 주지사의 행정 명령을 발표했다. 앞서 서술 했듯이, 현재까지는 이들 주정부의 법 / 행정 명령 대부분이 자율주행차 운행을 촉진하는 방향으로 되어 있다.

22) 사람 대상

23)Alabama, Arkansas, California, Colorado, Connecticut, Florida, Georgia, Illinois, Indiana, Louisiana, Michigan, New York, North Carolina, North Dakota, Pennsylvania, South Carolina, Tennessee, Texas, Utah, Virginia, Vermont, Washington D.C

24)Arizona, Delaware, Hawaii, Idaho, Maine, Massachusetts, Minnesota, Ohio, Washington, Wisconsin

[그림 2-1] 미국 주별 자율주행차 관련 법 제정 및 행정 명령 현황



자료: NCSL. (2018). “Autonomous Vehicles ¦ Self-Driving Vehicles Enacted Legislation.“

2) 기능/소프트웨어 안전 지침, 가이드, 표준

자율주행차 관련 기능/소프트웨어 안전 지침, 가이드, 표준은 명확하게 정의되어 있지 않은 상태이다. 이유는 현재 자율주행차 기술이 급격히 발전하고 있어, 이를 만족하는 지침, 가이드, 표준이 정립되어 있지 않고, 성급히 특정 지침, 가이드, 표준을 정할 경우 다양한 기술 발전 가능성에 저해가 될 수 있기 때문이다. 따라서, 현재는 상세한 기능/소프트웨어 안전 지침, 가이드, 표준보다는 상위 수준의 요구사항, 절차, 규정 등을 제시하고 있는 수준이다.

도로교통안전국(NHTSA)가 2017년 발표한 ‘자동화된 운전 시스템: 안전을 위한 비전’에서 자발적 가이드로 제시된 12개의 안전 요소 중, 첫 번째 요소로 시스템 안전에 대한 가이드가 포괄적으로 제시되어 있다. 여기서는 전체 개발 프로세스는 도로 차량의 기능적 안전 프로세스 표준[25]과 같은 산업 표준을 채택하고 따라야 하며 시스템

의 전체 운영 설계 영역 (즉, 작동 매개 변수 및 제한 사항)을 종합적으로 포함해야 하며, 개발 기업은 ISO (국제 표준화기구) 및 SAE International과 같은 공인 된 표준 개발 기관 (해당되는 경우)의 자발적인 지침, 모범 사례, 설계 원칙 및 표준과 타 산업 (우주, 항공, 국방 등)에 활용되는 여러 표준 및 프로세스 등도 함께 적용할 것을 권장하고 있다. 또한, 차량 설계 시 설계/검증 프로세스에는 자동주행시스템[26] 에 대한 위험 분석[27] 및 안전 위험 평가[28]와 오작동 처리를 위한 설계 중복 및 안전 전략을 기술 할 것을 권고한다. 이를 위해, 소프트웨어 개발, 확인 및 검증에 중점을 두고, 소프트웨어 개발 프로세스는 소프트웨어 업데이트 시 예기치 않은 결과를 감지/해결하기 위해 잘 계획되고, 제어되고, 문서화 되어야 하며, 철저하고 측정 가능한 소프트웨어 테스팅은 체계적이고 문서화 된 소프트웨어 개발 및 변경 관리 프로세스를 보완하는 동시에 소프트웨어 버전 릴리스에 포함되어야 한다고 권고한다. 자동차 개발 기업은 인공 지능 및 기타 관련 소프트웨어 기술 및 알고리즘의 진화, 구현 및 안전성 평가를 모니터링하여 자동운전시스템의 효율성 및 안전성을 향상하도록 장려하고 있다.

상기 내용에서 보았듯이, 자율주행차 관련 기능/소프트웨어 안전은 기존 자동차 지침/가이드/표준에 국한되지 않고 필요할 경우 가능한 모든 관련 산업(우주, 항공, 국방 등)의 기준을 사용하라고 권고하고 있으며, 상세한 지침/가이드/표준 보다는 개발 요구사항, 프로세스, 문서화 등에 대한 상위 수준의 권고를 하고 있다.

2. 영국

1) 정부 활동

영국 정부는 자율주행차의 성공적인 개발 및 정착을 위해, 법・제도 제정, 자율주행차 연구 기관 설립, 연구 지원, 가이드 및 지침 발표 등의 활동을 하고 있다. 법・제도 부분에서는 자율 및 전기자동차 법(AEV Act)[29]을 제정하여, 자율주행차 사고 관련 법적 책임, 차량 충전 인프라 등에 대한 사회/인프라 구축을 위한 제도적 기반을 마련하였고, 조직/부처적인 활동으로는 커넥티드/자율주행차량 센터(CCAV)[30]를 설립하였고,

25) Functional Safety Process Standard
26) ADS: Automated Driving System
27) Hazard Analysis
28) Safety Risk Assessment
29) Automated and Electric Vehicles act
30) CCAV: Centre for Connected and Autonomous Vehicles

규정/가이드 및 연구 활동으로는 자율주행차 테스트 가이드[31]를 제정하여 자율주행차 테스트 관련한 정책 및 기술적인 요구 사항을 제시하고, 커넥티드/자율 차량에 대한 사이버보안 원칙[32] 등을 발표하였다.

• 자율 및 전기자동차 법(AEV Act)

2018년 7월에 자율주행 및 전기 차량 법안(AEV Act)이 통과되었다. 이 법률의 주 내용은 사고 발생 시 법적 책임, 전기차 충전 및 충전 인프라 등에 대한 내용을 담고 있다. 특히, 이 법은 일부 또는 전혀 운전자의 관리/감독 없이 운행되는 자율 차량에 대한 사고 발생 시 법적 책임에 대한 부분을 상세하게 다루고 있는데, 주요 내용으로는 (a) 자율주행차[33]에 의해 부상당한 제 3자가 피해 보상을 위해 다른 법적 수단 (예 : 생산물 배상 책임 청구)에 의지하지 않고 보험업자에게 청구할 수 있음을 보장하고, (b) 자율 주행 모드일 경우 운전자 또한 탑승자로 간주하여 (a)의 권리를 운전자에게도 보장하고, (c) 보험자가 '사고와 관련하여 부상당한 당사자에게 책임질 수 있는 타인'에 대해 기여 과실에 대해 청구할 수 있도록 하였는데, 여기에는 차량 소프트웨어 설계자 또는 차량 제조업체 등이 포함될 수 있도록 하였다. 이에 따라, 자율차량 운행 사고 발생 시 피해자에 대한 보상은 명확해지고, 책임 및 보상의 의무는 운전자에게서 차량을 제조하거나 관련 소프트웨어를 개발한 업체로 전가 되었다. 소프트웨어 관련된 부분은 소프트웨어의 불법 개조와 안전에 필수적인(Safety Critical) 소프트웨어를 업데이트[34] 하지 않아 발생하는 사고에 대해 책임 면책이 제한되거나 없어진다고 규정하였다. 즉, 소프트웨어 불법 개조를 알고도 행하거나, 안전에 필수적인 소프트웨어 업데이트를 알고도 하지 않은 경우 보험가입자가 책임을 지도록 하고 있다.

• 커넥티드/자율주행차량 센터(CCAV)

자율주행차에 대한 개발 및 테스트 분야의 선도적인 위치를 유지한다는 취지로 교통부 및 경제/에너지/산업 전략부[35]의 협업을 통해 2015년 설립된 이 센터는 정책 및 규

31) The pathway to driverless cars: a code of practice for testing
32) Principles of cyber security for connected and automated vehicles
33) 영국에서는 자율주행차량에 대한 용어로 CAV(Connected and Autonomous Vehicles)를 사용한다.
34) 이 법률에서 안전에 필수적인 소프트웨어를 업데이트에 대한 정의를 소프트웨어를 업데이트하지 않을 경우 차량 사용이 안전하지 않는 것으로 다소 모호하고 포괄적으로 정의 하고 있다.
35) Department for Transport, Department for Business, Energy & Industrial Strategy

정 등을 개발하고, 200만 파운드 가량의 자금을 자율주행차 개발, 시연, 적용 등에 투자하고 있으며, 자율주행차 관련 정부 기관 간 업무조율을 수행하며, 여러 이해관계자들에 대한 단일 창구를 제공한다.

2) 기능/소프트웨어 안전 지침, 가이드, 표준

현재 영국에서는 자율주행차 안전 관련 기능/소프트웨어 안전 지침, 가이드, 표준은 존재하지 않고 특별히 규정하려 하고 있지 않은데, 이는 급속한 기술 발전이 진행되는 시점에 성급한 규제로 인한 기술 개발을 저해하지 않기 위해서이다.

3. 독일

1) 정부 활동

독일은 자율주행차 관련하여 가장 발빠르게 움직이고 있는 국가인데, 2017년 자율운행 관련 내용을 도로교통법을 개정하는 형태로 제정했으며, 이와 동시에 자율주행 관련 윤리 가이드를 제정하였다. 특이한 점은 독일의 자율주행차 관련된 법이나 가이드는 자율운행 시 운전자의 행동 양태 및 책임, 그리고 윤리적인 요소에 주안점 두고 있으며, 차량의 자율주행 시스템이나 기능에 대한 요구사항은 기존과 같이 차량에 대한 형식승인에 대한 체계를 적용하고 있는 점이다. 특히 독일은 유럽연합(EU) 수준의 법규정이 없는 상황에서 자율주행차 시장을 선도하기 위해, 국가 차원에서의 법제도 제정 및 정비를 추진하고 있다.

- 도로교통법 8차 개정[36)]

독일은 2017년 6월 8차 도로교통법 개정을 통해 자율주행 관련 내용을 처음으로 포함 시켰는데, 이 개정에서는 자동 운전 기능과 관련하여 독일 최초로 법적 한도를 설정하고, 고도화/완전 자동화 된 운전 기능을 자동차에 구현할 수 있는 기본 틀을 제시하면서, 자동 운전 승인을 위한 규제 기반을 마련하였다. 이를 통해, 자율주행 시스템에 대한 법적 확실성, 승인 및 신뢰를 강화하려고 하였다. 이번 개정의 특징은 자율주

36) Achtes Gesetz zur Änderungen des Straßenverkehrsgesetzes, 2017.06.21. 8차 개정

행 시스템을 보유한 차량에 대한 허가에 대한 규정은 변함이 없고[37], 차량 운전자에 대한 행동 양태를 규정한 점이다.

주요 내용으로는 고도화/완전[38] 자동화된 자동 운전 기능을 자동차에 적용하는 것에 대한 승인 여부[39], 운전자의 권리와 의무의 변경[40], 법령을 제정 할 권한[41], 독일 내 차량 보유자 책임은 기존 체계를 유지하지만, 책임 최대 금액은 두 배로 증가되며[42], 고도로 자동화 된 주행 기능을 갖춘 자동차의 데이터 처리에 대한 조항이 통합[43] 등이 있다.

이 법에 따르면, 운전자는 항상 '자동차 운전자'[44]로 간주되고, 승객으로 간주되지 않으므로, 항상 사고에 대한 책임이 있다. 다만, 사고가 시스템 고장에 근거한 경우, 책임을 면책되며, 이 경우 차량 제조업체가 책임을 지게 된다. 차량 소유자는 시스템 고장 발생 시에도 현장 사고 피해자에게 책임을 물어야 하지만, 제조사의 보상을 요구할 수 있다.

운전자는 새로운 법규에 따라 휠에서 손을 떼고 차량을 주행 제어 할 수 있으나, 항상 주의/지각을 유지해야 하며, 시스템 경고 또는 운전자 판단해서 상황이 수동 제어가 필요한 경우 곧바로 차량에 대한 제어권을 가져야 한다. 즉, 운전자는 차량 자동 운전 시에도 항상 경계 및 차량에 대한 통제권을 유지해야 한다. 또한, 자동 운전 시스템이 작동 중 일 때 항상 블랙박스가 기록해야 하는데, 이 기록을 6개월간 의무 보관해야 하며 사고 관련 기록은 3년간 보관해야 한다.

자율주행 차량에 대한 허가 규정은 기존 허가 시스템의 토대 하에 고도화/완전 자동 주행 시스템 기능의 요구사항을 충족할 수 있도록 개별 승인을 수정하는 방향으로 개정되었는데, 차량의 도로 운행을 위해서는 자율주행 정도에 상관없이 운행 허가, 개별 승인, 또는 EC 형식 승인 등을 요구하고 있다. 또한, 자율 주행 관련 기능은 관련 국제 규정 요구 사항을 충족하거나 Directive 2007/46/EC Article 20의 형식 승인 면제 요건을 충족 해야 한다고 명시하고 있다.

---

37) 기존 유럽연합의 차량 승인 제도인 형식 승인 제도 적용
38) 자율주행 등급 SAE 3, 4
39) 도로교통법 섹션 1a;: 고도/완전 자동화된 운전 기능이 의도된 대로 사용될 경우 사용이 허락된다.
40) 도로교통법 섹션 1a와 1b
41) 도로교통법 섹션 6, 63a
42) 도로교통법 섹션 12
43) 도로교통법 섹션 63a
44) Fahrzeugführer

• 자율 운행 관련 윤리 가이드라인[45)]

독일 연방 운송 / 디지털 인프라부[46)]는 2017년 6월 자율 운행 윤리 가이드라인을 만들어 발표했는데, 여기서는 총 20개의 윤리 가이드라인을 제시하면서, 개인에 대한 보호는 다른 모든 실용적 고려 사항들보다 우선한다고 전제하고, 목적은 운전의 위험성을 완전히 제거하는데 있으며, 자동화된 시스템의 운행 면허가 사람의 운전과 비교하여 위험이 낮다고 확인되지 않은 이상 정당화될 수 없다고 명시했다. 이 가이드에서 정부는 공공 도로 환경에서 도입되고 허가된 커넥티드 자율자동차 시스템 안전에 대한 보장책임이 있으며, 사고 회피를 위해 차량 운행 인허가 및 모니터링이 필요하다고 했다. 더불어, 모든 기술적 예방 조치에도 불구하고 피할 수 없는 것으로 판명된 위험한 상황에서 법적으로 보호된 이익의 균형을 이루는 부분에서 인간의 생명을 보호하는 것이 최우선 과제이므로, 기술적으로 사고 회피가 불가능할 경우, 시스템은 사람의 상해를 예방할 수 있다면 사고 발생 시 사람 대신 동물이나 재산의 손상/손실을 선택하도록 프로그램되어야 한다고 했다. 또한, 사고 회피가 불가능할 경우 개인적인 특징(연령, 성별, 신체적 또는 정신 상태)에 기초하여 희생자를 선택 또는 구분하는 것도 금지되어야 한다고 명시했다.

• 자율주행차 형식 승인[47)]

도로교통법 8차 개정에서는 모든 자동차는 자율주행 수준과 무관하게 형식 승인을 받아야 한다고 명시했다. 또한, 기존 형식 승인 시스템을 토대로 고도화/완전 자동화[48)]된 운전 기능의 요구 사항을 충족시키기 위해 개별 승인 시스템을 수정하여 적용 할 것을 요구했는데, 고도화/완전 자동화된 운전 기능을 포함한 차량의 통합 승인(Whole Approval)은 가능하나, EC 형식 승인을 통한 EU 회원국 전체에 대한 일괄(en bloc) 승인은 아직 가능하지 않다. 대안으로 차량에 대한 기본적인 승인을 받은 후[49)], 추가적

45) Ethics Commission Automated and Connected Driving
46) Bundesministerium für Verkehr und digitale Infrastruktur
47) Type Appoval
48) 자율 주행 SAE 3, 4 단계
49) 기본 형식 승인을 받은 자율 운전 기능 보유 차량은 운전 기능이 국제 기술 규정에 의해 규제되고 있지 않아도 공공도로에서 운행이 가능한데, 이 경우 개정된 도로교통법규의 규정에 적용을 받지 않고 일반 도로교통법을 적용 받는다

인 절차를 통해 고도화/완전 자동화된 운전기능에 대한 별도의 승인(개별 승인)을 받을 수 있다. . 이러한 개별 승인은 독일에서 적용되는 국제 규정의 요구 사항을 충족해야하거나 Framework Directive 2007 / 46 / EC 제 20 조[50]에 따라 EC 형식 면제 승인을 받도록 요구하고 있다. 현재 고도화/완전 자동화 된 운전기능에 적용 가능한 국제 규약이 없으므로[51] 독일에서 자율주행 차량 허가를 받기 위해서는 EC 면제 형식 승인을 받는 것이 필요하다. 따라서 차량 및 차량 부품 제조자는 독일연방자동차청[52]에 승인요청서를 제출하면, 독일연방자동차청은 서류 검사 후 문제가 없을 경우 사전 승인 후, EU정부에 EC 형식승인 면제 요청을 한다. EU 위원회는 관련 적절한 승인 절차를 거친 후, EC 형식승인 면제를 승인하고, 독일연방자동차청은 사전 승인을 EU 전체 국가에 통용되는 EC 형식승인 면제로 변경하여 적용한다.

2) 기능/소프트웨어 안전 지침, 가이드, 표준

현재까지 독일에서 별도의 자율 주행 차량에 사용되는 자동 운전 시스템 기능/소프트웨어 안전에 대한 기술에 대한 지침, 가이드, 표준이 마련되어 있지 않은 상황이다. 다만, 제8차 도로교통법 개정안에서 명시했듯이 자율주행차량도 기존의 다른 차량과 마찬가지로 기존 차량 승인 제도인 형식 승인 제도에 적용을 받는다고 하였으므로, 기존 차량 형식 승인에 필요한 기능/소프트웨어 안전 지침, 가이드, 표준은 구체적으로 명시되어 있지 않고 차량 전기/전자 부품 또는 시스템 제작 시 준수해야 하는 기본 표준으로 ISO 26262 등이 제시되고 있다[53].

4. 중국

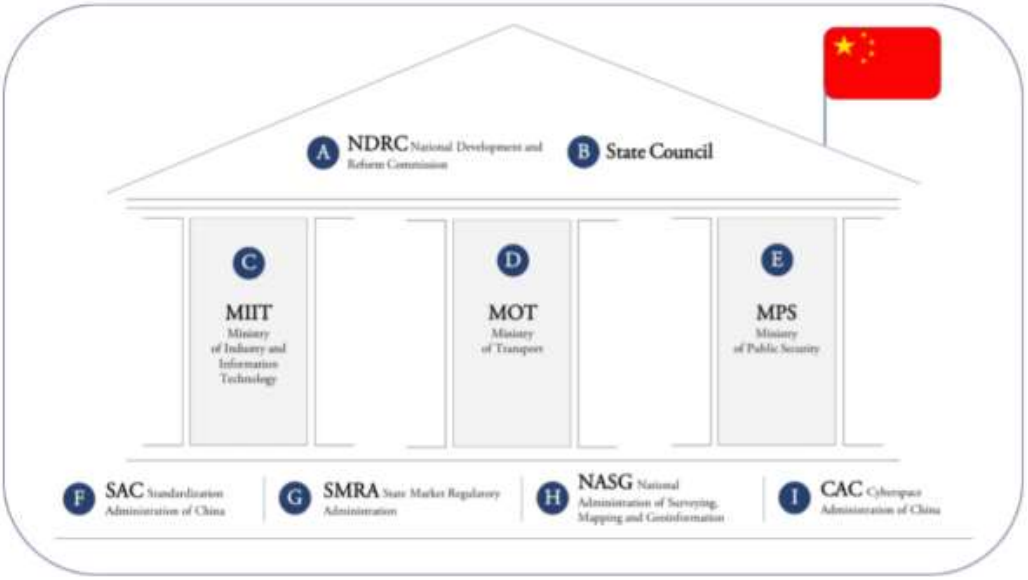
1) 정부 활동

자율주행차 관련 중국 정부의 주요 활동은 자율주행차 비전/전략 수립, 관련 기술 표

50) EC 형식 승인 면제
51) 현재, UN/ECE Regulation No. 79에서 자동 운전 기능에 관련 된 기술 요구 사항을 추가하는 개정 작업 중에 있다.
52) Kraftfahrt-Bundesamt
53) 예를 들어, UNECE Regulation No.100 Electric Vehicle Safety의 경우, 준용해야할 Functional Safety 국제 표준으로 ISO 26262를 포함하고 있다. (출처. 2015년 국내 소프트웨어 안전 산업 동향 조사 p.19)

준 수립, 관련 기관 설립 등이 있는데, 국가발전개혁위원회[54]에서 자율주행차에 대한 비전/전략을 수립하면, 산업정보통신부[55], 교통운송부[56], 공안부[57]의 3개 정부 중앙 부처가 자율주행차 개발 및 테스트 관련 규정 및 정책을 제정하는데, 특히 산업정보통신부가 자율주행차 관련 규정 제정, 차량 형식 승인 등의 가장 많은 역할을 수행하고 있으며, 교통운송부는 교통 인프라, 도로 운송 관리 등의 업무, 공안부는 도로교교통 안전 및 차량 등록에 관한 업무를 수행하고 있다. 이들 부처와 함께. 중국표준화관리국(SAC)[58], 국가시장감독관리총국[59], 국가측회지도신식국[60], 사이버공간관리국[61]의 기관들이 자율주행차 관련 실제 업무를 수행하고 있는데, 중국표준화관리국(SAC)은 산업정보통신부와 함께 자율주행차 개발 관련 국가표준을 제정하고 있다.

[그림 2-2] 자율주행차 관련된 중국 주요 정부 부처



자료: GIZ. (2018). “Defining the Future of Mobility: Intelligent and Connected Vehicles (ICVs) in China and Germany. “

- 지능형 차량 개발 및 혁신 전략[62] 초안

54) 國家發展和改革委員會 (국가발전개혁위원회 National Development and Reform Commission)
55) 工業和信息化部 (MIIT, Ministry of Industry and Information Technology)
56) 交通运输部 (MOT, Ministry of Transport)
57) 公安部 (MPS, Ministry of Public Security)
58) 国家标准化管理委员会 (SAC, Standardization Administration of China)
59) SMRA, The State Market Regulatory Administration
60) NASG, The National Administration of Surveying, Mapping and Geoinformation
61) CAC, The Cyberspace Administration
62) 智能汽车创新发展战略 (Strategy for Innovation and Development of Intelligent Vehicles)

2018년 1월에 국가발전개혁위원회에서 발간한 지능형 차량 개발 및 혁신 전략 초안에서 자율주행차에 대한 3단계 비전을 제시하고 있는데, 1단계인 2020년까지 중국은 자율주행차에 대한 체계적인 규제 체계를 수립하고, 중국 신차의 50%가 부분 또는 완전 자동 기능을 갖추며, LTE-V2X 차량용 무선 통신 네트워크를 대도시 고속도로 90%에서 사용할 수 있도록 목표하고 있으며, 2 단계인 2025년까지 생산되는 모든 새 차량의 거의 100%가 지능형이며 차세대 무선 통신 네트워크 (5G – V2X)가 작동하는 것을 목표로 하고, 2030년까지 중국은 ICV[63]의 세계적인 리더가 되는 것을 목표로 하고 있다.

• 텔레매틱스 산업의 표준 시스템 개발을 위한 국가표준

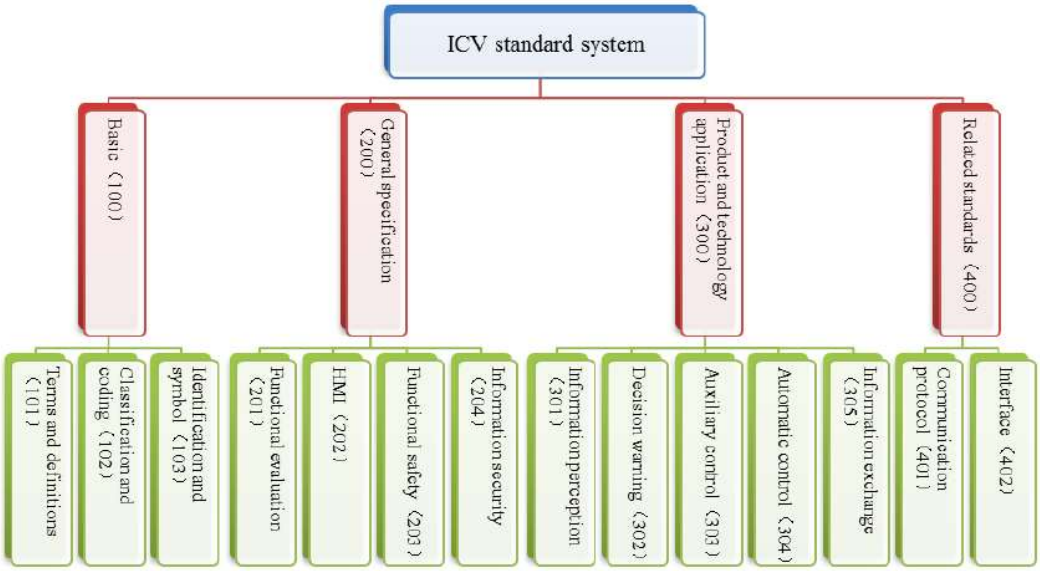
2017년 12월 산업정보통신부와 중국표준화관리국은 협업을 통해 자율주행 시스템 개발 프레임워크 제공을 위해, 텔레매틱스 산업의 표준 시스템을 개발하기 위한 국가 표준[64] – 1. 전반적인 요구 사항, 2. 지능화된 커넥티드 차량, 3. 정보통신, 4. 전자 제품 및 서비스의 총 4개의 국가 가이드라인을 발표하였다. 이 가이드라인의 개발 계획은 총 2단계로 이루어져 있는데, 1 단계인 2020년까지 자동화된 운전 수준 1-3을 지원하는 30개의 자율주행차 핵심 표준을 마련하고, 2 단계인 2025년까지 자동화 된 운전 수준 1-5를 지원하기 위한 100개 이상의 핵심 표준을 갖추는 것을 목표로 하고 있다.

• 자율주행차 촉진을 위한 국가 혁신 플래폼

국가발전개혁위원회는 2017년 12월 자율주행차 촉진을 위해 국가 혁신 플랫폼을 수립했는데, 주 목적은 자율주행차 개발의 장애물을 극복하고 국가 전략의 효과적인 실행을 보장이다. 주 역할은 자율주행차와 관련된 정책 입안을 촉진하고 연구를 촉진하는 것이며, 협의회, 자문위원회, 연구소[65]로 구성되어 있다.

63) Intelligent and Connected Vehicles
64) 国家车联网产业标准体系建设指南 (the National Guidelines for Developing the Standards System of the Telematics Industry (Overall Requirements)
65) 국가 자율주행차 연구소. 2017년 12월 산업정보통신부에 의해 설립됨. 총 21개의 자율주행차 관련 기업으로 구성됨

[그림 2-3] 중국 자율주행차 표준 시스템 프레임워크



MIIT & CSA. (2017). "Guideline for Developing National Internet of Vehicles Industry Standard System (Intelligent & Connected Vehicle)."

[그림 2-4] 자율주행차 표준 시스템

Functional safety (203)						
203-1	Functional safety for road vehicles (Parts 1-10)	GB	Recommended	PublishedGB/T 34590-2017(Parts 1~10)	ISO	ISO 26262
203-2	Failure protection requirements and evaluation methods for intelligent &connected vehicle man-machine interaction interface system	GB	Recommended	In preliminary research	PWI	
203-3	Functional safety requirements for automotive interaction interface	GB	Recommended	In preliminary research	PWI	
203-4	Functional safety requirements for automotive information sensing system	GB	Recommended	In preliminary research	PWI	
203-5	Functional safety requirements for vehicle decision warning system	GB	Recommended	In preliminary research	PWI	
203-6	Functional safety requirements for vehicle assist control system	GB	Recommended	In preliminary research	PWI	

자료: MIIT & CSA. (2017). "Guideline for Developing National Internet of Vehicles Industry Standard System (Intelligent & Connected Vehicle). "

2) 기능/소프트웨어 안전 지침, 가이드, 표준

자율주행차 관련 텔레매틱스 산업의 표준 시스템 개발을 위한 국가 표준 중, 지능화된 커넥티드 차량 가이드라인 부문[66]은 기본영역, 일반사양, 제품 및 기술 어플리케이션, 관련표준의 총 4개 영역으로 되어 있고, 일반사양의 상세 영역 중 하나로 기능안전이 제시되어 있다.

특히, 가이드의 4번째 부분인 관련 표준 영역에서 주요 영역별 필요 표준 및 유관 국제 표준과 각 표준별 현재 개발 현황 등이 표시되어 있는데, 기능안전 부분에 대한 필요 표준은 총 6개로 되어 있다. 이 중 첫 번째로 차량 기능안전 표준[67] 이 개발되어 있는데. 이 중 차량의 기능안전 파트 6 '소프트웨어 개발에 대한 표준[68](Road Vehicles – Functional Safety – Part 6: Product development at the software level)' 에서 기능안전을 위한 소프트웨어 개발 표준이 제시되어 있으며, 관련 유관 국제 표준으로 ISO 26262가 명시되어 있다. 나머지 5개의 기능 안전 표준은 현재 초기 연구 중으로 나타나 있다.

5. 일본

1) 정부 활동

자율주행차 관련한 산업의 육성은 일본 정부가 주도하는 제4차 산업혁명의 한 주제로써, 일본 정부에서는 전후방 산업 측면, 교통 측면에서 자율주행차 관련 산업을 활성화하면서도 자율주행차와 기존의 사람이 운전하는 방식의 자동차 및 자율주행차와 보행자 간 조화로운 운행 및 안전을 보장할 수 있도록 다양한 법률 및 정책을 수립하고 이행하고 있다.

자율주행자동차 관련된 법률 제정 및 정책 수립은 국토교통성에서 주도하고 있는 것으로 파악되어, 주로 일본 국토교통성(国土交通省) 홈페이지에서 정책 안내 및 언론에의 발표/홍보 자료를 조사하였고, 관련된 법률은 일본 정부에서 제공하는 법률 정보 조회 시스템인 e-Gov.에서 직접 법조문을 조사하였다. 또한 정책이나 법령에 내포된

66) Guideline for Developing National Internet of Vehicles Industry Standard System (Intelligent & Connected Vehicle)
67) Functional Safety for road vehicles (Part 1 – 10)
68) GB/T 34590-2017

정책적 사상 및 방향, 민간에서 해당 법령이나 정책을 수용하는 시각에 대해서는 일본 경제신문 등의 언론 발표/공시 자료를 수집하고 분석하였다.

- **자율주행차 관련 정책 수립 배경**

일본의 자율주행자동차에 대한 정책을 이해하기 위해서는 우선 그 배경에 대해 이해할 필요가 있다. 먼저 거시적 측면에서 살펴보면, 일본 사회는 인구의 지속적 감소, 노령 인구의 지속 증가로 생산 인구의 감소와 생산성이 하락하는 문제가 심해지는 상황에서, 새로운 가치 및 고부가 가치의 신산업을 육성해야 할 필요가 대두되었다. 또한 교통안전 측면에서 노령 인구가 증가함에 따라 노령 운전자들의 안전 문제가 주목받기 시작했다. 건강/보건과는 달리 노령 운전자가 야기할 수 있는 교통안전 상 문제는 이들 자신의 안전뿐만 아니라 상대 운전자나 보행자, 재물에 확대되기 때문이다.

교통/자동차 산업 측면의 첫 번째 자율주행차 관련 정책 수립의 배경은 굳이 노령 운전자의 증가를 걱정하기 이전에 현재 이미 교통 사고의 97%가 운전자 측 문제로부터 발생하고 있는 상황[69]에서 교통사고 예방이 최우선적으로 해결할 문제로 꼽히고 있다는 점이다. 정부에서는 자율주행 기술의 도입 및 상용화를 통해 운전자로부터 기인하는 사고를 저감할 수 있을 것으로 예상하고 있다.

두 번째 배경으로는 도로 확장 대비 차량 보급 대수 증가율이 높은 상황에서 교통 혼잡도 증가가 불가피할 것으로 예상되는 상황이라 교통 혼잡의 예방 필요성이 중요하게 부각되고 있다는 점이다. 이를 위해 정부에서는 IoT를 연계한 즉각적/체계적 교통 신호 제어를 통해 교통 흐름을 효율화하려고 하고 있고, 궁극적으로는 교통 혼잡을 방지하는 시스템을 구축하여 사회적 비용을 절감하려는 목표도 가지고 있다.

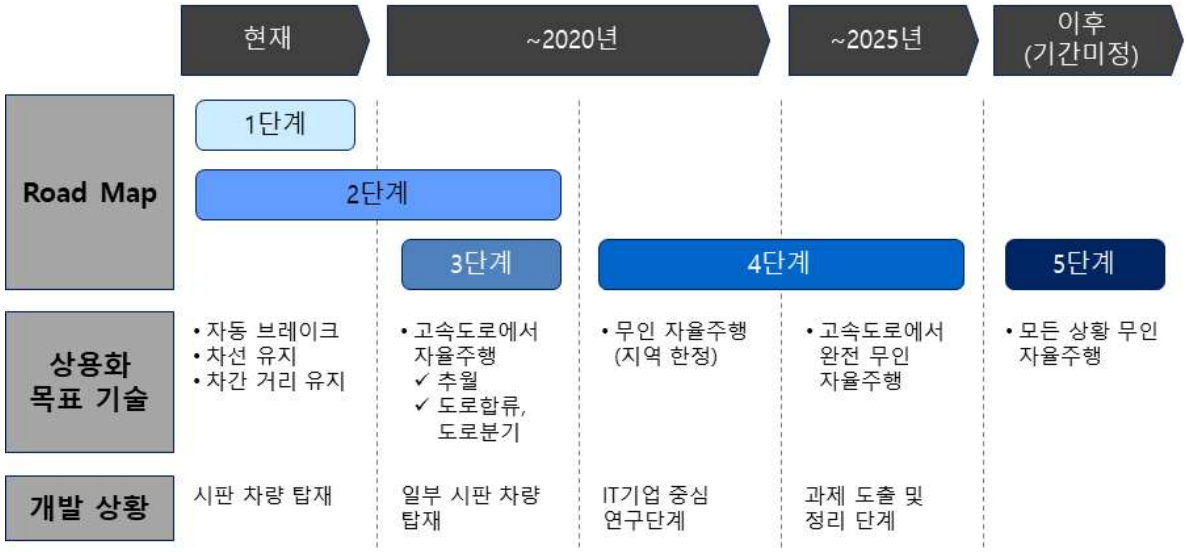
마지막 배경으로는 일본 자동차 산업의 경쟁력을 강화해야 하는 상황에 직면해 있다는 점이다. 해외에서는 테슬라를 중심으로 전기자동차와 자율주행자동차 기술을 발전시키고 있고 벤츠나 BMW 등 기존 대형 자동차 메이커들도 최근에는 관망의 자세에서 적극적 자율주행 기술 개발에 참여하고 있는 실정이다. 이에 맞춰 일본 자동차 메이커들도 미래를 대비하여 경쟁력을 갖춰야 할 상황에 직면해있다.

- **자율주행차 발전 계획**

69) 국토교통성 발표 '17.6월 "自動運転の実現に向けた国土交通省の取り組み(자동 운전의 실현을위한 국토 교통성의 대처)" 자료 인용(http://www.mlit.go.jp/common/001227121.pdf)

앞서 살펴본 바와 같이, 자율주행차의 필요성 및 중요성이 대두됨에 따라 국토교통성에서는 자율주행차와 관련된 중장기적인 목표와 전략을 수립하였다. 최종 목표는 모든 상황에서 운용 가능한 무인 자율주행 기술을 개발하는 것인데, 당장 현재의 기술 수준은 사람의 운전을 보조하는 수준의 걸음마 단계인 관계로, 중장기적인 기술 발전 계획을 5단계로 나누어 수립하였다.

[그림 2-5] 일본 자율주행차 발전 로드맵 ('17년)



자료: 自動運転に関する国土交通省の取り組み, Japan Automobile Manufacturers Association, 2018; 国土交通省, 2017

자율주행 기술의 최초 1단계는 현 시점을 포함하는 단계이다. 1단계에서는 운전자가 운전대를 잡고 운전하는 것을 전제로 운전자를 보조하는 기능과 관련된 기술을 개발하고 있다. 예를 들면 차간 거리를 유지하는 기술 및 차간 거리가 예외적으로 좁혀질 경우 자동으로 브레이크를 거는 기술 등이다.

이후 '19년 ~ '20년 이전까지 자율주행 2단계의 기술을 개발할 계획이다. 2단계 기술로는 1단계 개발 완료된 기술을 기반으로 운전자 감시 하에 자율주행 시스템이 주행 상황에 대한 판단과 운전을 자동으로 진행하는 것으로 목표로 한다. 관련 기술로는 1단계에서 개발한 차간 거리 유지 기술 및 자동 브레이크 기능을 고도화하고, 고속도로에서 자율주행 시스템이 추월과 도로합류 또는 분기진출을 보조하는 기술 개발을 계획 중이다.

3단계에서는 이러한 기술들의 수준을 높이는 것과 운전자가 자율주행 시스템이 운전하는 도중에 개입할 상황을 최소화하도록 하는 수준의 기술 개발을 목표로 하고 있다.

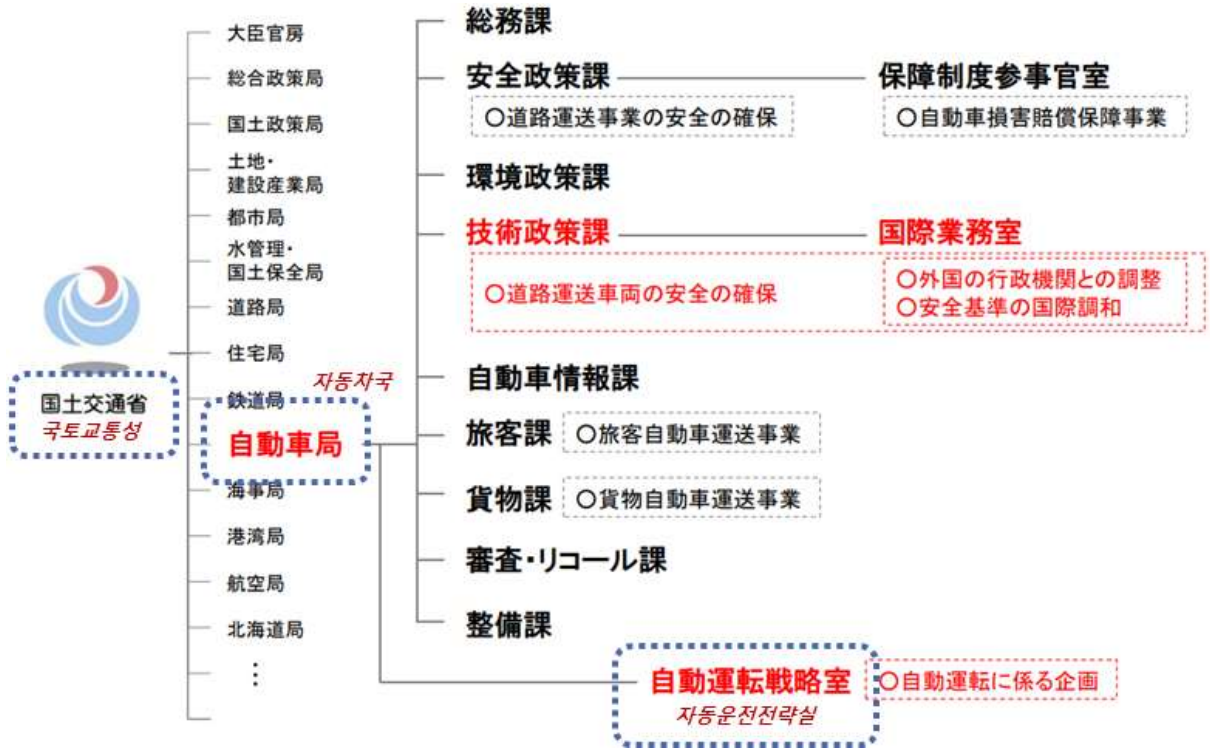
‘20년까지 자율주행 3단계를 달성한 이후로는 ‘20년부터 자율주행 4단계 기술 개발을 착수하여 ‘25년까지 완료한다는 계획이다. 자율주행 4단계의 초기에는 자동차 제조업자 또는 연구기관 중심으로 초반에는 안전하고 고립된 써킷[70]에서 안전하게 주행할 수 있는 무인 자율주행 기술을 개발하고, 중후반부터는 이 기술을 기존 사람이 운전하는 자동차가 다니는 고속도로에서 주행할 수 있도록 상용화할 수 있도록 한다는 계획이다. ‘25년 이후로는 자율주행 5단계로 모든 상황에서 완전 무인 자율주행 기술을 개발한다고 계획을 세웠으나, 구체적인 일정은 아직 미정인 상황이다.

- **자율주행차 관련 정부 조직 현황**

국토교통성에서는 자율주행 자동차 발전을 가속화하기 위하여 ‘16년 12월 ‘자동운전전략실’ 을 신설하였다. 해당 부서는 자율주행의 실용화와 이에 수반되는 제도, 정책의 선제적 추진을 위해 설립되었다. 이를 위해 실장은 국토교통대신이 겸임하도록 하여 지위를 높였고, 기술 개발, 표준 제정에 관여하는 기술정책과가 있음에도 기술정책과 산하에 편입시키지 않고 국토교통부 자동차국의 바로 아래에 위치하게 하여 기술정책과와 같은 계위의 지위를 부여하였다. 이러한 조직 구성 방식 및 조직간 관계를 통해 자율주행 기술의 실현 및 상용화에 일본 정부가 적극적으로 대응하겠다는 의지를 확인할 수 있다.

70) 자동차나 오토바이 등의 시험 주행 목적 환상 도로 (環狀道路)

[그림 2-6] 일본 자율주행차 관련 조직



자료: 自動運転に関する国土交通省の取り組み, Japan Automobile Manufacturers Association, 2018; 国土交通省, 2017)

- **자율주행차 관련 정책 현황**[71]

국토교통성에서는 자율주행과 관련하여 현재 다음과 같은 세 가지 방향을 고려하여 정책을 수립하였다.

첫 번째는 자율주행 기술을 실현할 환경을 정비하는 것이다. 이를 위해 정부에서는 자율주행 차량 관련 국제적 기술 표준화를 UN 차량안전기준 및 G7 교통장관회의에서 협의된 내용에 맞추어 추진한다는 방향과 자율주행 운전 중 발생한 차량 사고에 대한 배상 책임과 주체를 정하는 배상 규칙을 수립한다는 방향을 세워 놓았다.

두 번째로는 자율주행과 관련된 기술의 개발 및 보급을 진행한다는 것이다. 이를 위해 HW 및 소프트웨어 측면의 자율주행 관련 차량기술을 개발하며, 해당 차량기술 발전에 맞추어 도로 및 교통체계를 수정/보완한다는 계획이다.

마지막으로 자율주행 기술을 실증하고 상용화한다는 것이다. 이를 위해 자율주행차량의 운행 범위를 점진적으로 확대할 계획인데, 우선은 교통 환승 시 최종단 구간에서

71) 출처: 自動運転に関する国土交通省の取り組み(자동운전에 대한 국토교통성의 대응), Japan Automobile Manufacturers Association, 2018; 国土交通省(국토교통성), 2017

자율주행 기술을 우선 적용하고(ラストマイル自動運転, 우리나라의 마을버스 운행 구간), 교통이 비교적 덜 복잡하고, 도로가 직선화되어 있는 뉴타운 지역 내 대중교통 수단에 적용하며, 탄력적으로 기간제로 자율주행 버스 등을 도입한다는 계획이다.

이러한 방향과 앞서 살펴본 자율주행 기술 개발 로드맵의 단계, 시기에 맞추어 2017년 말까지 자율주행 환경 정비 중심의 두 가지 정책을 수립하였다.

먼저 '자율주행차량의 도로(공도) 주행을 허용한다'는 정책이다. 자율주행차량의 도로주행에 대해서는 현재 G7 교통장관회의에서 자율주행 3단계, 4단계 수준의 유인 자율주행 기술을 상용화한다고 합의하고, UN 산하 WP29(세계 자동차 규제 조화 포럼)에서 자율주행 3단계, 4단계 안전 기준과 관련하여 자동 조타(차선 유지) 기능과 자동 브레이크 기능을 도입하는 것을 논의한 수준으로 아직 국제 표준에 대해서도 명확히 정의된 바가 없다. 이러한 상황에서 일본 국토교통성에서는 국제 표준 수립을 선점하기 위해 '17년 2월에 '핸들 및 액셀/브레이크 페달이 갖춰지지 않은 자율주행자동차의 도로주행을 허용한다'는 내용의 규칙을 공표하였다.(かじ取装置に係る協定規則 第79 号 개정)

두 번째 정책으로는 자율주행차량의 사고 발생 시 배상 규칙을 정하는 중으로, '16년 11월 해당 내용과 관련한 민/관 연구회를 설치하였고, 해당 내용을 검토하여 '17년까지 그 방향을 정하는 것으로 계획되어 있다.

국토교통성 중심으로 일본 정부에서는 자율주행 관련된 기술 개발을 장려하기 위해 자율기술 친화적인 정책만 내놓는 것으로 보이나, 그와는 반대의 규제도 신설하였다. '17년 10월에 공표된 정책으로 '운전자가 자동 조타 기능을 사용하여 차선 유지 지원 기능을 이용하는 경우, 운전대에서 손을 놓고 65초가 경과한 후에는 자율주행에서 수동운전으로 강제 자동 전환'하라는 정책이 그것이다.

그 내용을 간략히 살펴보면, 운전자가 운전대를 잡은 상태에서 자율주행시스템의 차선 유지 기능의 도움을 받아 운행하는 중[72], 운전자가 운전대에서 손을 놓은 후 15초가 경과할 경우 운전자에 경고를 주고, 추가 50초가 경과하면 자율주행 모드를 정지시키고 강제로 수동 운전하도록 하였다. 이 정책은 신형 차량인 경우에는 '19년 10월

72) 운전자의 의무를 규정한 도로교통법 70조에 따르면, "차량 운전자는 그 차량의 핸들, 브레이크 장치를 확실하게 작동하며, 도로, 교통 및 차량 상황 에 따라 타인에게 위해를 미치지 않는 속도와 방법으로 운전해야한다" 고 규정되어 있는데, 일반적으로 운전대에서 손을 놓지 않는다는 의미로 해석되어 적용된다.(道交法70条,「車両等の運転者は、当該車両等のハンドル、ブレーキその他の装置を確実に操作し、かつ、道路、交通及び当該車両等の状況に応じ、他人に危害を及ぼさないような速度と方法で運転しなければならない」)

이후 생산 차량부터 적용되고, 기존 차량은 '21년 4월 이후 생산 차량에 적용되며, 중고 차량은 그 대상에서 제외되도록 하였다.

국토교통성 입장에서는 도로 주행에 있어서의 아직 실증/검증되지 않은 AI 기술에 대한 안전장치로써 제시한 첫 정책이나, 시장에서는 자율주행차 관련 기술이 이제 막 시작인 단계인데 정부에서 규제부터 발표하였다며 대부분 부정적인 견해보이고 있어, 아직 초기 단계인 자율주행 기술 개발을 위한 데이터 축적이 제대로 이루어지지 않을 것에 대한 우려와 AI 설계 복잡도가 증가하여 이에 대한 검증 또는 추가적인 기술 개발에 대한 투자/가속이 둔화될 것을 우려하는 목소리가 높다.

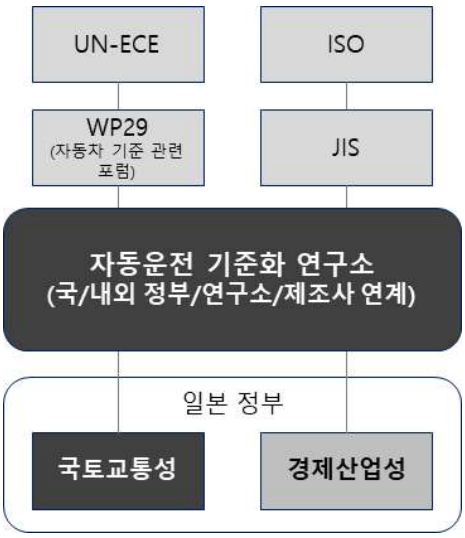
2) 기능/소프트웨어 안전 지침, 가이드, 표준

자율주행과 관련한 표준은 일본 정부에서 직접 관여하지 않고, '자동운전 기준화 연구소'라는 정부 설립 기관을 주축으로 참여하고 있는데, 이 기관은 정부 부처 중 국토교통성 및 경제산업성과 UN-ECE 산하 WP29 포럼(세계 자동차 규제 조화 포럼) 및 ISO-JIS, 타 국가 개별 정부, 타 국가 연구소, 일본 국내/외 자동차 제조 기업들을 연계하며 자율주행 관련 지침/가이드/표준을 주도하고 있다.

자율주행에 대해서는 아직 국제 표준도 없고 논의만 진행 중인 상황이나, 자율주행 기술에 뒤쳐져 있다는 일본 정부의 위기의식 및 제4차 산업 혁명 관련한 기술 표준을 선점하겠다는 의지가 반영되어 세계 최초로 자율주행 3단계, 4단계 해당되는 요구사항을 정의하고 그에 대한 가이드라인을 수립하였다.[73]

73) 출처: 自動運転丶安全要件で開発促進 国際標準狙う(자동 운전, 안전 요구 사항 개발 촉진 국제 표준 노린다),日本経済新聞(니혼게자이신문), 2018.6, 자동운전차의 안전기술 가이드라인, 국토교통성, 2018.9

[그림 2-7] 일본의 자율주행 관련 표준/지침/가이드라인 설정 주체



자료: 自動運転に関する国土交通省の取り組み, Japan Automobile Manufacturers Association, 2018; 国土交通省, 2017)

그 내용으로는 자율주행 시스템(AI 기반 소프트웨어)이 자율주행차에 사고가 발생할 수 있다고 판단할 경우에는 운전자에게 문제가 있음을 통지하도록 하고, 그와 관련한 주행 데이터를 수집하고 기록하도록 한 것과 자율주행시스템이 주행 장소와 기후 조건을 자동으로 판단하여 주행 조건을 직접 결정하도록 한 사항이 포함된다.

가이드 라인의 내용 중 주행 조건에 대해서는 자율주행 시스템을 설계하는 주체가 운행 설계 내역(Operational Design Domain)에 자율주행 시스템이 작동하는 조건에 대해 아래와 같은 사항들을 정의하도록 열거하고 있는데, 상위 수준의 가이드 라인인 관계로 정의할 대상만 제시되고 그 상세 내용이나 예시는 제공되지 않고 있다.(‘18년 10월 1일 기준)

- 도로 조건: 고속도로/일반 도로 구분, 차선 수, 차선 유/무 여부, 자동차 전용 도로 여부
- 지리 조건: 도시 지역, 산간 지역, 자동운행 구역 등
- 환경 조건: 날씨/기상 조건, 주간/야간 제한 여부 등
- 기타 조건: 속도 제한, 신호 정보 등 교통 인프라 연계의 필요/불필요 여부, 특정된 경로의 운행 한정 등

<표 2-2> 2018년 자율주행차 국가별 비교_1

	미국	영국	독일
정부 활동	• 연방정부: 법률 제정 및 도로교통안전국의 자율주행차 관련 활동 • SELF Drive Act • AV START Act • 도로교통안전국: ‘자동화된 운전 시스템: 안전을 위한 비전’ • 주정부: 대부분 자율주행차 운행을 촉진하는 방향	• 법·제도 제정, 자율주행차 연구 기관 설립, 연구 지원, 가이드 및 지침 발표 등의 활동 • 자율 및 전기자동차 법(AEV Act)	• 도로교통법 8차 개정: 자율운행 관련 내용 추가 • 자율주행 관련 윤리 가이드 제정 • 자율주행차 형식 승인
관련 조직	• 도로교통안전국(NHTSA)	• 커넥티드/자율주행차량 센터(CCAV)	• 독일연방자동차(Kraftfahrt-Bundesamt)
표준	• 필요할 경우 가능한 모든 관련 산업(우주, 항공, 국방 등)의 기준을 사용하라고 권고	• 자율주행차 안전 관련 기능/소프트웨어 안전 지침, 가이드, 표준은 존재하지 않으며 특별히 규정하는 활동 없음	• 자율주행차의 자동 운전 시스템 기능/소프트웨어 안전 지침, 가이드, 표준이 마련되지 않음

<표 2-3> 표 2018년 자율주행차 국가별 비교_2

	중국	일본
정부 활동	• 자율주행차 비전/전략 수립, 관련 기술 표 준 수립, 관련 기관 설립 • 지능형 차량 개발 및 혁신 전략 초안 • 텔레매틱스 산업의 표준 시스템 개발을 위한 국가표준 • 자율주행차 촉진을 위한 국가 혁신 플래폼	• 세계 최초로 자율주행 3단계, 4단계 해당되는 요구사항 정의 및 가이드라인 수립
관련 조직	• 국가발전개혁위원회(National Development and Reform Commission) • 산업정보통신부((MIIT) • 교통운송부(MOT) • 공안부(MPS) • 국표준화관리국(SAC) • 국가시장감독관리총국(SMRA) • 국가측회지도신식국(NASG) • 사이버공간관리국(CAC)	• 국토교통성(国土交通省) • 자동운전 기준화 연구소
표준	• 지능화된 커넥티드 차량 가이드라인에 유관 국제 표준으로 ISO 26262가 명시	• 표준 명확히 정의된 바 없음

제2절 드론 관련 법·제도, 기관, 지침/가이드 동향

1. 미국

1) 정부 활동

2012년 연방항공청(FAA)[74] 현대화 및 개혁법(FMRA)이 제정되면서 무인 항공기 관련

74) Federal Aviation Administration

법제도가 정비되기 시작했는데, FMRA Public Law 112-95 Section333에서 무인항공기에 제한적으로 비행을 허가하였고, Section 336에서 취미 및 오락 목적용 무인항공기에 대한 안전 규정을 제정하였다. 나아가 2015년 2월 교통부(DOT)[75]와 연방항공청(FAA)은 협업을 통해 소형 무인 드론 시장 활성화를 목적으로 한 무인항공기시스템(UAS) 규제권고안(NPRM, Notice of Proposed Rulemaking)을 마련하고, 2015년 10월 아마존, 구글X[76], 월마트, 고프로, DJI, 인텔 등 사업자를 포함해 관련 연합, 단체, 담당 공무원 등 총 26개 기관이 참여하는 태스크포스(TF)를 구성하고, 그간 몇 번의 회의와 수정안을 거쳐, 2016년 6월 상업용 드론 운영 규칙인, 소형 무인항공기 규정(The Small Unmanned Aircraft Regulations/Rules)인 FAR Part 107을 발표[77]하였는데, 이 규정으로 상업용 드론의 비행규제가 간소화 되었다.

본 조사는 25Kg 이하[78]의 소형 무인 드론[79] 관련된 규정 및 안전 활동에 대해서 조사하였는데, 미국 드론 정책은 2018년 이전에는 오락 목적용 드론(Model Aircraft)에 대해서는 규제 및 등록의 필요성이 없으나 2018년 국가방어수권법[80]에 따라 모든 드론이 등록 대상이 되었다. 드론은 사용 목적에 따라 다른 법/규정의 적용을 받는데 1. 취미 또는 오락 목적용 드론은 FMRA[81] Section 336와 14 CFR[82], Part 101, Subpart E, Special Rule for Model Aircraft 규정의 적용을 받으며, 2. 취미 또는 상업적 목적용 드론은 FMRA Section 333와 14 CFR Part 107, 소형무인항공기시스템(sUAS)[83]의 적용을 받는다.

• 취미 또는 오락 목적용 무인 드론(Model Aircraft) 규정

25kg 이하의 취미 및 오락 목적용 무인 드론은 FMRA[84] Section 336와 14 CFR[85], Part 101, Subpart E, Special Rule for Model Aircraft 규정의 적용을 받는데, 주요 내용은 다음과 같다.

---

75) Department of Transportation
76) X Development LLC(이전의 Google X)는 2010년 1월 구글이 설립한 미국 비밀(일부) 연구 개발 시설 및 조직
77) http://www.itnews.or.kr/?p=18959 미국 소형 무인항공기(드론) 규정 '제107편' 집중 분석
78) Less than 55 lbs
79) Unmanned Aircraft
80) National Defense Authorization Act for Fiscal Year 2018
81) FAA Modernization and Reform Act of 2012
82) Code of Federal Regulation
83) small Unmanned Aircraft System
84) FAA Modernization and Reform Act of 2012
85) Code of Federal Regulation

- 지역 사회 기반 안전 지침 준수. 전국 커뮤니티 기반 조직 프로그램 내에서 비행
- 드론 등록
- 시야 범위 내에서 비행
- 타 항공기 근처에서 절대 비행 금지
- 공항 5마일 이내에서 비행 전 공항 및 항공 교통 관제탑에 통보
- 긴급 상황 시 비행 제한

Model Aircraft에 대한 정의는 1. 대기 중에서 지속적인 비행 가능하고, 2. 항공기를 조정하는 사람의 시야 내에서 비행하며, 3. 취미 및 오락 목적으로 비행하는 것을 말한다.

• 취미 또는 상업 목적용 무인 드론(sUAS)

25kg 이하의 취미 또는 상업 목적용 무인 드론은 FMRA Section 333와 14 CFR Part 107, sUAS의 적용을 받는데, 주요 내용은 다음과 같다.

- 미연방항공청(FAA)에서 원격 파일럿 인증 취득
- 시야 범위 내에서 비행
- 타 항공기 근처 또는 사람 위 비행 금지
- 미연방항공청(FAA) 허가 없이 공항 근처 통제된 영공으로 비행 금지
- 일광 또는 시민박명(Civil Twilight) 시에만 400피트 이하에서 비행

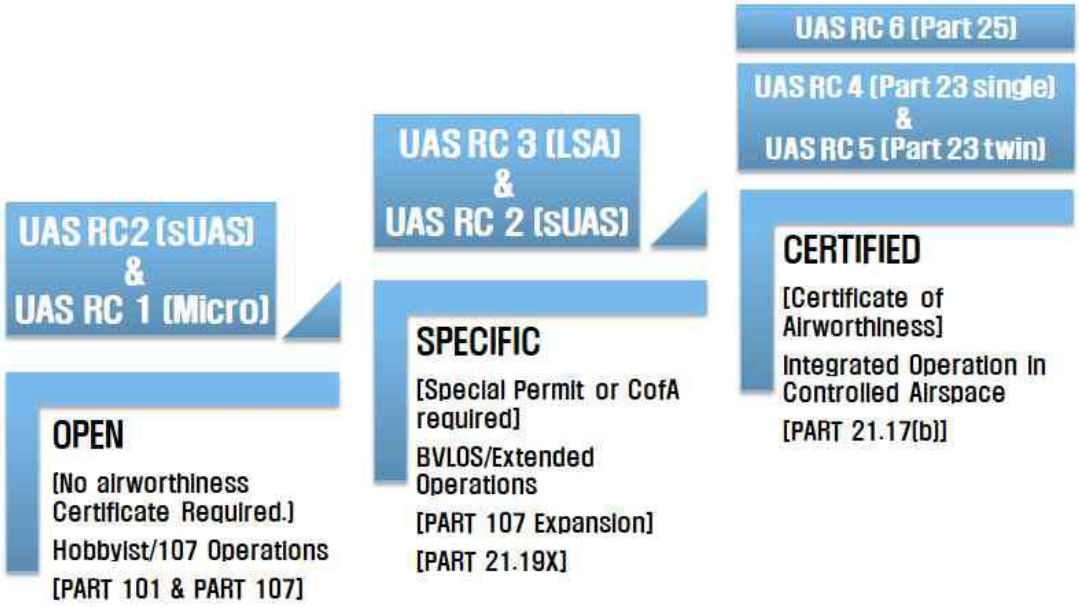
• 미연방항공청(FAA)

연방항공청은 드론 안전 관련 법을 제정하며, 드론을 운행하는 사람들에 대한 자격을 부여하고, 모든 드론에 대한 등록을 관장하고 있다. 주요 역할로는 안전성을 향상을 위한 민간항공 규제, 신규 항공 기술을 포함한 민간 항공 산업의 육성 및 개발, 민간 및 군용 항공기 모두에 대한 항공 교통관제 및 항법 시스템 개발 및 운영, 국가공역체계 및 민간항공의 연구 및 개발, 항공의 항공기 소음 및 기타 환경 영향을 제어하는 프로그램 개발 및 실시, 미국 상업용 우주 운송 규제 등으로 직접 규제, 연구 및 기술 개발, 산업 육성 및 개발, 시스템 운영 등 다양한 역할을 수행하고 있다.

2) 기능/소프트웨어 안전 지침, 가이드, 표준

연방항공청(FAA)은 통고사항(Advisory Circular 107-2)에서 취미 또는 상업용 드론(sUAS)의 개발 및 운영을 위한 자격 요건에 대한 가이드 기준을 발표했는데, 취미 또는 오락용 드론(Model Aircraft)는 포함되지 않는다. 여기서 규정의 적용 기준, sUAS 운행 제한 가이드, 원격 운행 인증, 유지 및 검사 등에 대한 내용을 다루고 있다. 이 통고사항에서는 항공 기준으로 DO-178을 참고문헌으로 사용[86]하고 있는데, DO-178(최신은 DO-178C)은 항공기에 탑재되는 소프트웨어의 안전성을 높이기 위한 목적으로 개발된 항공기 시스템 및 장비 (감항) 인증에 대한 소프트웨어 가이드 국제 표준이다. 따라서, 취미 또는 오락용 드론(Model Aircraft)에 대해서는 소프트웨어 안전에 대한 가이드 등이 존재하지 않고, 취미 또는 상업용 드론(sUAS)에 대해서는 DO-178이 권고되고 있다.

[그림 2-8] 미국 무인항공기 감항인증체계



자료: 유병선. 신동진. 장재호· 박정민· 강자영(2018), 원격 조종 항공기 시스템의 인증 표준화 전략

86) Chapter 2. Reference 2.3.4 RTCA, Inc. Documents (current editions).

2. 유럽(EU)

1) 정부 활동

- 유럽항공안전청(EASA)[87]

유럽(EU)은 유럽항공안전청(EASA)이 드론에 대한 안전 인증 및 표준 등에 활동을 하고 있는데, EUROCAE[88], ASD-STAN[89], ASTM[90] 등 유럽 및 주요 표준기관들 뿐만 아니라 ICAO RPAS 패널[91], JARUS[92], FAA[93] 등과도 국제적 공조를 통해 드론 감항 증명에 대한 표준화를 추진하고 있다. 2009년 발간된 무인항공기 감항증명 정책서(policy statement: airworthiness of UAS) E.Y013-01은 무인항공기의 환경보호를 포함한 형식증명에 대한 일반 원칙을 확립한다. 이 정책서의 목표는 무인항공기 민간 감항 적용 촉진에 있다. 개방범주(Open)[94] 및 특정범주(Specific)[95]는 2015년 기술적 의견에 기반한 개정안고시(NPA; notice to proposed amendment), 2016년 프로토타입 규정, 전문가 그룹을 통한 실무 작업을 거쳐, 2018년 2월 EASA Opinion No 01/2018로 제안되고, 2018년 7월 유럽위원회[96]에서 (EU) 2018/1139으로 승인되고 발표되었다.

유럽항공안전청의 주요 역할로는 규정 및 인증 조정, 단일 EU 항공 시장 개발, 기술 항공 규칙 작성, 항공기 및 구성요소의 형식 인증, 항공 제품을 설계, 제조 및 유지 관리 회사 승인, EU 국가에 안전 감독 및 지원 제공(예: 항공 운영, 항공 교통 관리), 유럽 및 글로벌 안전 표준 촉진, 유럽 내 안전성을 개선하기 위해 국제 이해관계자들과 협력 등이 있다.

- (EU) 2018/1139

이 규정은 EU 내에서 민간 항공 안전에 대한 높은 수준의 일관성을 설정 및 유지하며, 상품, 인력, 서비스 및 자본의 자유로운 이동을 촉진하고, 항공 관련 사업자에게

87) European Aviation Safety Agency
88) European Organisation for Civil Aviation Equipment
89) AeroSpace and Defence Industries Association of Europe - Standardization
90) American Society for Testing and Materials
91) Remotely Piloted Aircraft Systems Panel (RPASP)
92) Joint Authorities for Rulemaking on Unmanned Systems
93) Federal Aviation Administration
94) [그림 2-9 참조]
95) [그림 2-9 참조]
96) European Council

평등한 경쟁 기회를 제공하고, 타 국가(EU회원국 외) 및 항공 당국과의 적절한 협력을 확립하고, 인증 및 다른 관련 문서의 상호 승인의 촉진을 목표로 한다. 이 규정은 조건별 항공기의 설계, 생산, 유지 보수 및 작동은 물론 원격으로 항공기를 제어하는 엔진, 프로펠러, 부품, 비장착 장비 및 장착 장비에 적용되나 민간 항공 안전에 대한 제한된 위험을 고려하여, 단순 설계, 주로 국지적인 기반에서 운용되는 항공기, 자체 제작 및 매우 적은 수로 제작되는 드론에 대해서는 회원 국가가 자체적으로 규제하는 것으로 하였다. 또한, 무인 항공기에 대한 운영 질량과 관계없이, 무인 항공기의 등록과 그 운용자에 관한 요건을 규정하고 있다. 이 법은 유럽항공청이 유럽위원회에 모든 크기의 드론에 대해 규제를 위한 기술 전문 지식을 제안할 수 있도록 했다. 이러한 유럽 전체에 적용되는 첫 번째 민간용 드론 규정은 혁신적인 규제 방법에 기초하고 있는데, 규정은 최대한 단순하게 유지되고, 운영상의 특정 위험에 중점을 두고 있다.

이 법은 유럽항공안전청(EASA)에서 발행한 A-NPA 2015-10 및 Concept of Operations for Drones에서 제시된 비율 및 위험 기반의 드론 구분을 채용하여 Open, Specific, Certified Category의 3개 범주로 나누어 규제하고 있는데, 구체적으로 살펴보면 아래의 그림과 같이, 1. Open Category의 경우는 위험이 높지 않고, 항공청 관여가 필요 없으며, 육안으로 보이는 범위에서 운행해야 하며, 공항 및 민감한 지역의 운행이 제한되며, 2. Specific Category의 경우, Open보다 위험이 높고, 운행 매뉴얼과 함께 운행 허가가 필요하며, 안전 평가에 기반한 드론, 인력, 장비의 구체적인 자격이 필요하며, 3. Certified Category의 경우, 유인비행과 유사한 규정에 적용받으며, 유럽항공안전청(EASA)와 다른 기관의 승인을 받아야한다.

[그림 2-9] 3가지 범주의 드론

자료: 유럽항공안전청

2) 기능/소프트웨어 안전 지침, 가이드, 표준

유럽항공안전청(EASA)에서 발행한 Concept of Operations for Drones에서 Open Category에 포함되어 감항능력(airworthiness) 인정이 요구되지 않는 드론이라도, 산업 안전 표준이 적용될 수 있다고 했다. 특히, 인구 밀집 지역에서 드론 운영자가 최대 고도 및 비행 금지 구역 등을 준수하도록 지원하기 위해 EN[97]와 같은 적절한 산업 표준을 준수해야 한다고 명시했다. Specific Category에 포함되는 드론의 경우 운영자는 위험 평가 (EASA가 제공하는 표준화 된 방법인 SORA[98] 사용) 및 완화 조치를 정의하거나, EASA 또는 해당 국가 항공 당국이 정의한 특정 시나리오를 준수하는지 확인 후, 항공국으로부터 허가를 받을 수 있는데, SORA에서 드론에 대한 기술적 이슈 부분에 시스템 안전[99] 관련 고려 항목이 포함되어 있다. 하지만, 현재까지 드론에 대한 명확한 기능/소프트웨어 안전에 대한 지침, 가이드, 표준은 없다.

97) European Norms
98) Specific Operations Risk Assessment
99) System Safety

3. 중국

1) 정부 활동

- 중국 민용 항공 총국(CAAC)[100]

중국은 CIVIL AVIATION LAW OF THE PEOPLE'S REPUBLIC OF CHINA에 의거 CAAC에서 민용 드론[101]에 대한 규정 제정 및 규제 권한을 가지고 있다. 중국 민용 항공 총국은 2017년 5월 Administrative Regulation on Registration for Unmanned Aircraft Owner을 제정하여, 250g 이상 되는 모든 드론에 대해 CAAC에 드론 소유자는 소유자 실명을 등록해야 하며, 7 kg 이상의 드론은 CAAC에 라이센스를 취득할 것을 규제화했다. 관련 주요 규정은 아래와 같다.

- 최대고도: 120m 이하. 이상일 경우 CAAC의 라이센스 필요
- 최대거리: 시야 범위 내 비행 (VLOS)
- 최대무게: 250g 이상 소유자 필명 등록. 7 kg 이상은 CAAC 라이센스 필요
- 비행금지 구역: 비해 금지 구역에서 비행 금지. 예외는 CAAC 허가 필요
- 상업용 드론: CAAC의 라이센스 필요
- 보험: 보험 가입 필요

100) 中國民用航空局, Civil Aviation Administration of China
101) 민용 드론은 군사, 경찰, 관세 목적 이외에 사용되는 모든 드론을 말한다.

[그림 2-10] 드론 구분 표준

Class	Net Weight (kg)	Take-off Weight (kg)
I	0 < W ≤ 1.5	
II	1.5 < W ≤ 4	1.5 < W ≤ 7
III	4 ≤ W ≤ 15	7 < W ≤ 25
IV	15 < W ≤ 116	25 < W ≤ 150
V	Plant protection (agriculture/crop-related) drones	
VI	Unmanned airship	
VII	BVLOS Class I and II	
XI	116 < W ≤ 5700	150 < W ≤ 5700
XII	W > 5700	

자료: CAAC(2018), Low-Altitude Connected Drone Flight Safety Test Report

2) 기능/소프트웨어 안전 지침, 가이드, 표준

자율주행차와 마찬가지로, 드론 관련 표준 기술은 중국표준화관리국(SAC)에서 제정하여 제시하는데, 2017년 8월 중국표준화관리국은 '드론을 위한 표준 시스템 제작 가이드[102]'를 발표했는데, 여기서 드론 산업의 표준 체계를 수립하는 데 필요한 목표와 개발 단계를 상세히 기술하였다. 1단계(2017년~2018년)는 드론 시스템의 시장 요구 사항을 충족하는 것을 목표하는데, 여기에는 드론 업계 감독 요구에 대한 지원, 드론 표준 시스템의 사전 개발, 중요 표준 개발에 중점을 두고 있다. 2단계(2019년~2020년)는 드론 표준 시스템 개발을 점진적으로 촉진하는 것을 목표로 하는데, 2020년까지 300개 이상의 드론 시스템 규격의 제정 및 개정으로 드론 산업의 표준 시스템이 적절히 보완 및 완성될 것을 목표로 한다. 이러한, 표준은 모든 기본, 관리 및 기술 표준을 다루며 산업 애플리케이션 요구 사항을 준수한다. 이 가이드에서 제시한 드론 시스템 표준은 A)기본기준, B)관리기준, C)기술표준, D)산업 애플리케이션 표준의 4 가지 파트로 나누어지고, 각 파트는 다시 서브 파트로 구성되어 있는데, A)기본기준의 세부 파트로

102) Guideline on Building a Standard System for Unmanned Aircraft (无人驾驶航空器系统标准体系建设指南)

AE)안전이 있으며, 이 세부파트로 AEA)시스템안전, AEB)부품안전, AEC)정보안전, AED)기타 으로 구성되어 있다. AEA)시스템안전 필요 표준은 총 5가지 항목이며, 모두 시급히 개발 필요로 구분되어 있다.

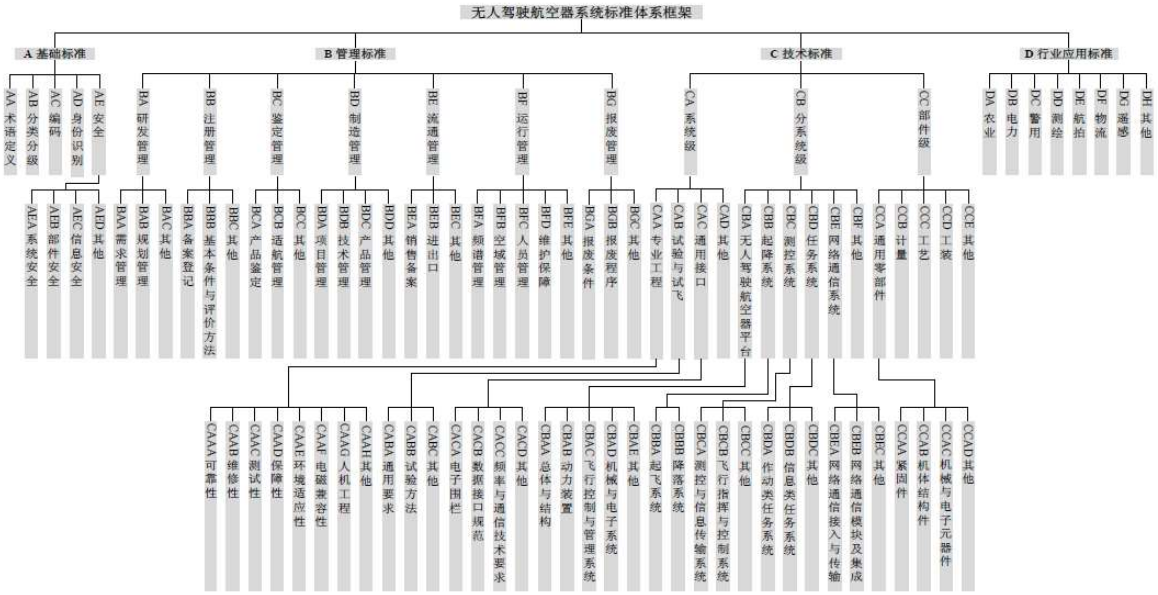
<표 2-4> 드론 시스템 안전 관련 필요 표준

표준번호	표준명	비고
AEA01	• 민간 멀티 로터 무인 공중 차량 시스템 안전 요구 사항	긴급히 개발 필요
AEA02	• 민간인 고정익 무인 공중 차량 시스템 안전 요구 사항	
AEA03	• 민간 무인 헬리콥터 시스템 안전 요구 사항	
AEA04	• 민간 조명 및 소형 멀티 로터 무인 공중 차량 시스템의 안전 설계 요구 사항	
AEA05	• 시민 무인 공중 차량을 위한 OID[103] 기반 보안 인증 아키텍처	

이 가이드라인에는 필요 표준이 총 267개로 제시되었고, 이 중 현재 기준 16개의 표준이 개발 완료 되었고, 46개는 긴급히 개발 필요, 205개가 향후 개발 예정으로 정리되어 있다.

103) Object Identifier

〈표 2-5〉 드론 시스템 표준 체계



자료: SAC (2017), ”드론을 위한 표준 시스템 제작 가이드”

4. 일본

1) 정부 활동

일본 정부는 드론과 관련해서는 정책 유형에 따라 관련된 정부 부처의 역할을 분담시켰다. 우선 드론 산업의 육성과 관련된 정책은 ‘경제산업성’에서 주도하도록 하였다. 드론 운용 환경, 관련 기술 상용화 환경에 대한 정비, 운항과 관련된 기술의 개발, 무인 드론 운용 기술 개발, 드론 또는 드론의 충돌로 인한 사고 방지 기술의 개발이 해당된다.

그 다음 드론의 활용/운용 정책은 활용 목적과 부합하는 정부 조직이 담당하도록 하였다. 예를 들면 농업 분야의 드론 운용/활용은 농림수산성에서 담당하는 식이다. 이러한 정부 부처간의 역할 분담에 있어 공통적인/일관된 특성이 확인되었는데, 경제산업성에서 제시하는 가이드라인과 국토교통성 주도로 개정한 항공법을 준용하되, 각 산업별 드론 운용 목적에 부합하도록 정책 내용을 수정하거나 추가하는 방식으로 정책을 제정하는 것이다.

마지막으로 드론의 운용을 규제하는 것은 국토교통성에서 담당한다. 드론의 운용을 제한하는 법안이 ‘15년 발효되어, 이에 근거하는 드론 인허가 관련 규제 및 드론 운

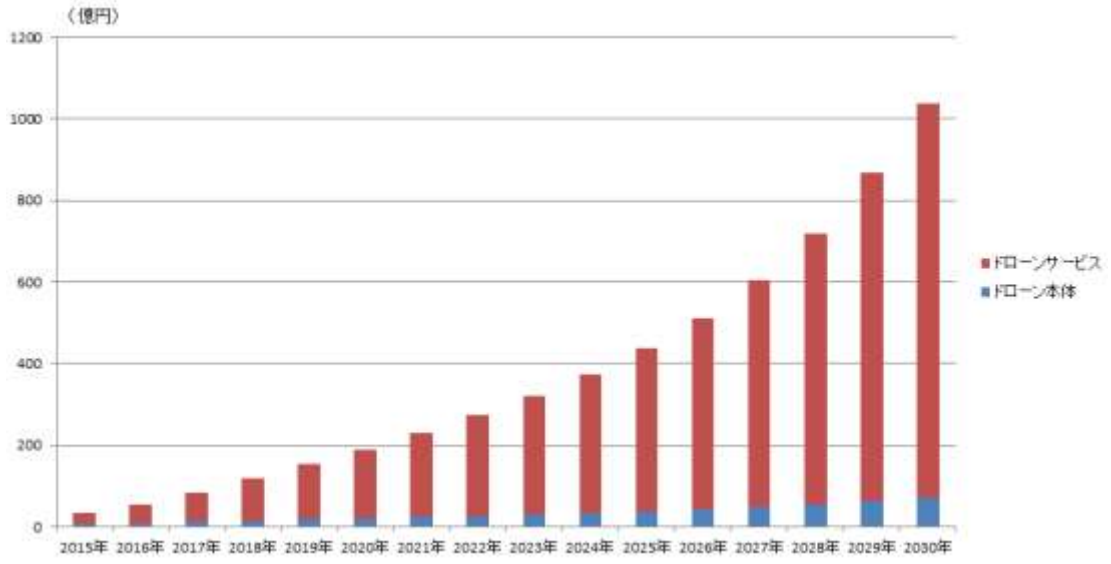
용 가능 지역 규제, 드론 관련 사고 대응 규칙 등을 국토교통성에서 담당하고 있다.

이렇게 다양한 정부 조직에서 유형별, 목적별 정책이 산재되어 있어, 경제산업성과 국토교통성의 정책을 중심으로 조사하되, 누락될 여지나 사회적/산업적으로 유의미하다고 판단된 경우 관련된 정부 부처를 찾아 내용을 추가로 조사하였다. 그래서 각 정부 부처 홈페이지에서 정책 안내 및 언론에의 발표/홍보 자료를 조사하였고, 일본 경제신문 등의 언론 발표/공시 자료를 수집하고 분석하였다.

- **드론 관련 정책 수립 배경[104]**

우선 드론 시장은 민간과 공공 부문 모두 보급이 급격히 증가하면서 '30년까지 시장 규모가 천억엔 이상으로 성장할 것으로 보이는 시장이다. 주로 서비스 중심의 시장 증가가 예상되는데, 농림수산업, 관광, 산업 등 민간 영역에서부터 순시/점검 등의 공공/공익 목적의 서비스까지 활용 영역이 지속 증가하고 규모도 증가할 것으로 예상된다.

[그림 2-11] 일본 드론 시장의 성장 예측



자료: 30年に千億円市場　業務用ドローン(니혼게자이신문), 2015.7

현재는 주로 공공 서비스 측면에서 드론의 활용이 활발히 이루어지는데, 주로 교량 등 인프라 점검에서 비용의 절감이나 데이터 수집 및 판정의 정확도 향상을 위해 사용하며, 비상 시를 위해 지진 등 재해 발생 시 재난망 사업과 연계하여 드론을 기지국

104) 참고: 국토교통성 정책 개요, 2018; 경제산업성 정책 개요, 2018

으로 활용하거나 구마모토 지진이 발생했을 때처럼 재난 지역의 정보 수집이나 물자 전달을 위해 활용하고 있다.

그러나 민간 부문에서의 레저용도로 보급되고 있는 드론은 명확한 규제/통제가 없어 사고나 부작용이 우려되고 있다. 이러한 우려가 현실화되었던 것이 '15년 일본 총리 관저에 세슘을 실은 드론이 추락한 사건이다. 총리 관저 및 그 일대는 비행금지 구역이었음에도 소형 드론을 이용하여 침투한 사건이라 이후 항공법 개정에 영향을 미친 것으로 파악된다. 또한, 아직 다행히 사고가 발생하지는 않았지만 드론과 일반 항공기 간 충돌로 인한 사고도 우려되는 상황이었다.

이에 일본 정부는 드론의 성장에 따른 관련 산업 육성이라는 과제와 드론 보급에 따른 안전사고 문제를 동시에 해결해야 하는 상황을 직면하였고, 우선은 드론 관련한 산업 육성, 운용, 규제를 각기 다른 정부 부처에 할당하였다.

- **드론 산업 육성 전략 및 정책 현황**

경제산업성에서는 경기 활성화를 위하여 4대 전략과제를 제시하였다. 산업 안전 강화, 중소기업의 국내외 신규 수요 개척, 글로벌 경기 부진에 대한 극복, 제4차 산업 혁명을 대비하기 위한 미래에 대한 투자가 그 것인데, 과제 중 제4차 산업 혁명을 대비하기 위한 미래에 대한 투자의 세부 과제가 드론과 관련이 있다. 드론 관련 전략과제로는 '자동운전, 로봇/무인항공기 제조 등 중점 산업의 플랫폼화' 가 있는데, 이를 위해 일본이 보유한 상대적으로 높은 수준의 인프라(인적/물적)를 활용할 수 있는 민/관 로드맵을 수립하고, 프로젝트를 조성하며, 산업이 성장할 수 있도록 규제 개혁을 추진한다는 내용이다.

이 과제의 실행을 위해 경제산업성에서는 매년 민/관 관련자를 소집하여 회의를 개최하고 드론 산업 육성에 대한 로드맵을 발표하였는데, '18년 발표한 로드맵은 아래와 같다.

[그림 2-12] 드론 산업 육성 목표 및 전략

자료: 경제산업성 드론 전략 로드맵(空の産業革命に向けたロードマップ 2018), 2018

경제산업성에서는 2018년까지 드론 기술개발 1단계로 유인 조종하는 기체의 개발을 목표로 하였다. 2단계 및 3단계는 '18년에 시작하여 ' 19년까지 완료하는 것으로 계획을 세웠는데, 2단계의 목표는 유인 조종 기술에 일부 자동/자율 비행 기술을 접목하는 것이고, 3단계 목표는 드론이 무인 지대에서 무인(자동) 비행하는 것이다.

이를 위해 2018년에는 드론 관련한 민/관 공동의 기술적, 법·제도적 요구사항을 전반적으로 수집할 계획이고, 드론 운용의 핵심 기술인 전파 관련한 제도, 기술을 검토/정비할 계획이다. 또한, 운용 정보를 수집하는 DIPS(드론 정보 기반 시스템)을 구축하여 이미 운영 중에 있다. 그리고 이러한 정부의 지원이 아직 성숙하지 않은 드론 관련 기술의 발전에 방해 요인이 되지 않도록 하기 위해 드론 관련 규제 샌드 박스를 신설하기로 하였다.

기술적으로는 드론의 무인화 기술을 개발하고, 무선 전파 기술을 활용한 운항관리시스템(UTMS)를 구축하고, 장기적으로 충돌 회피 기술 및 원격 기체 식별 및 위치 파악 기술의 개발에 착수하기로 '18년도의 계획을 세워 두었다.

'19년에는 ' 18년의 세부 수행 과제들을 고도화하는 개념으로 수행하게 되어 있는데, 우선 '18년에 수집한 드론 관련 요구사항을 분석하여 드론 제조 및 등록, 안전에 대한 심사 방안을 설계할 예정이다. 또한 자동차 메이커에서 운영하는 시범주행 서킷과 같은 개념의 테스트 필드를 후쿠시마에 건설할 계획이고, 전파 관련한 제도/기술

검토 내역을 토대로 전파 관련 제도를 정비할 계획이다.

기술적으로는 무인화 기술을 실증 가능한 수준까지 개발 완료하도록 지원할 예정이고, 충돌 회피, 운항 관리 시스템은 실증을 통해 상용화 가능성을 따져볼 예정이다. 또한 지속적으로 지체 및 통신 기술의 안정성과 신뢰성을 확보하도록 할 예정이다.

중기적으로는 2020년대 중반까지, 무인 자율비행을 지원하기 위하여 사람이 개입하지 않기 위한 요건 및 기술적으로 충족해야 할 사항을 발굴하고 해법을 모색할 예정이고, 드론 관련한 국제 표준을 국내 도입하여 일본화한 표준으로 정립할 예정이다. 또한 드론 자체의 추락을 방지하는 기술과, 추락 또는 충돌 자체를 회피할 수 있는 기술을 개발할 예정이다.

궁극적으로는 인구 고밀도 지역에서도 드론이 자율비행할 수 있는 수준의 기술 개발이 목표인데, 경제산업성에서는 이러한 기술 개발을 지원하고 필요한 정책, 법・제도 정비를 추진할 계획이다.

- **드론 관련 분야별 운용 계획**[105]

산업별 드론 육성 정책을 살펴보면 앞서 배경에서 살펴본 바와 같이, 산업 또는 드론 활용 목적에 따라 담당 정부 부처가 달라지며 내용도 정부 부처 간 조율에 따라 미묘하게 달라질 수는 있으나, 공통적으로 명확한 정책을 정의하기보다는 정부의 간섭을 최소화하는 가이드라인 수준에서 정책을 결정하고 있다.

105) 출처: 경제산업성 정책회의: 부처간 회의, 민관 협의회 회의록 (2018)

<표 2-6> 각 산업별 드론 육성 및 운용 계획

구분	정책 내용 또는 진행 중 사항
물류	• ’17년 물류용 드론 포트 시스템 실증 실험 • ‘18년 민간 사업자 드론 활용 화물 운송 가이드라인 제정
측량 (3차원 측량)	• ‘15년 UAV (항공 사진 측량)을 이용한 공공 측량 매뉴얼 제정 • ‘17년 AV 탑재형 레이저 스캐너를 이용한 공공 측량 매뉴얼 제정
재해 대응	• 재해 지역 생존자 수색, 기자재 반송 작업 시험적 투입 사례만 존재 • ‘19년 ‘드론 등을 활용 한 야간 재해 발생 시 신속한 구조 활동 기술과 초창기의 안전 관리 기술에 관한 연구’ 과제 수행 예정
농림수산업	• 이전부터 농업은 농약 살포, 임업은 산림자원 조사, 수산업은 밀렵 감시에 드론 활용 중 • ‘15년 항공법 개정에 따라 위 활동이 위법하게 될 수 있어 규제 완화/예외 추진 (검토회 통해 내용 정리 후 국토교통성과의 조정 추진)
인프라 유지관리	• 일부 인프라 점검 작업 시험적 투입 사례 확인 • 민/관 참여 ‘드론 활용 인프라 유지 관리’ 세미나 지원 • 인프라 유지보수에 드론 활용하기 위한 기술적 요구사항 (배터리, 전파 등) 정의 중
경비업	• 경비업법 상 드론 활용 규제는 없음 • 경비업에서 드론 활용할 수 있도록 제도적 지원안 수립 예정

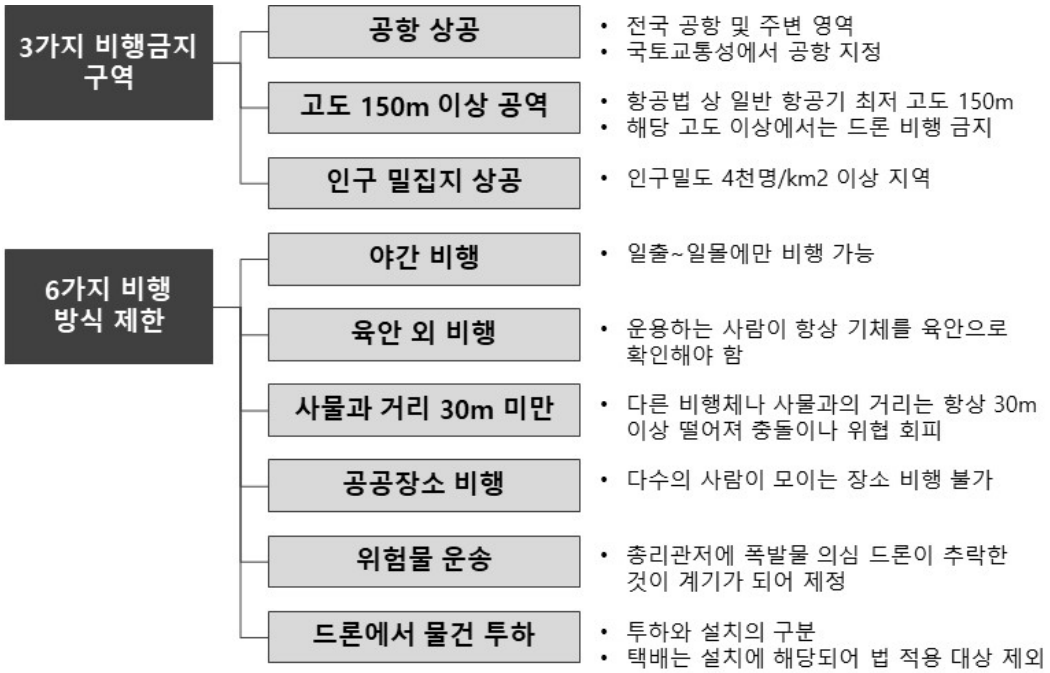
자료: 경제산업성 정책회의: 부처 간 회의, 민관 협의회 회의록, 2018

- **드론 관련 규제 현황**

앞서 언급한 바와 같이, 드론을 이용한 테러나 일반 항공기와의 충돌 등 사고가 발생하면 다른 교통수단에서 발생하는 사고보다 피해 규모가 더 클 수 있어 드론의 육성 정책과 동시에 규제 법령도 제정하게 되었다.

현재까지는 드론의 운용을 제한하는 법안과 그에 따른 시행 규칙 등이 입안되었는데, 모두 개정된 ‘항공법’에 의거하고 있다.(‘15년 개정) 개정된 항공법에 따르면, 드론은 앞으로 3가지 비행 금지 구역에서의 운용이 금지되고, 4가지 비행 방식에 대해 제한을 받게된다.

[그림 2-13] 개정 항공법에서 규정한 드론 관련 금지 사항



자료: 항공법, e-Gov.
(http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=327AC0000000231_20170530_428AC0000000051&openerCode=1)

2) 기능/소프트웨어 안전 지침, 가이드, 표준

자동 운전되는 무인 항공기의 안정성을 확보하기 위한 표준의 근거는 현재 경제산업성에서 공표한 ‘차세대 로봇 안전성 확보 가이드라인, 07년’에서 비롯된다. 일본 정부에서는 드론이 로봇에서 비롯된 하위 범주로 간주하고 있어 드론에 대한 가이드라인은 아직 명확히 정의된 바가 없어 우선적으로 기존에 존재하는 가장 유사한 정책을 적용했는데, 드론도 자동 운전하는 로봇으로 간주하여 해당 가이드라인을 적용한 것으로 보인다.

이에 따라 그동안 드론에 적용한 국제 표준도 주로 로봇에 관련된 것이었다. 예를

들면 ISO10218 및 ISO10218:1992가 대표적으로 적용되는 표준인데, ISO10218은 산업용 로봇 안전 표준이고 ISO10218:1992는 좀 더 포괄적인 로봇에 대한 안전 기준이다. 또한 ISO12100도 적용되는데 이는 기계류 안전에 대한 표준이고, ISO14121은 위험 평가 표준이다.

그래서 일본 정부는 2020년대 중반까지 드론 독자적인 국제 표준의 생성에 참여하며, 드론만의 특화된 국제 표준이 정의될 경우 이를 일본에 도입하여 표준화한다는 계획을 가지고 있다.

<표 2-7> 2018년 드론 국가별 비교

	미국	유럽	중국	일본
정부 활동	• FMRA Public Law 112-95 Section333: 무인항공기에 제한적으로 비행 허가 • Section 336: 취미 및 오락 목적용 무인항공기에 대한 언전 규정 제정	• (EU) 2018/1139: 이 법은 유럽항공청이 유럽 위원회에 모든 크기의 드론에 대해 규제를 위한 기술 전문 지식을 제안할 수 있도록 했다. • 비율 및 위험 기반의 드론 구분 채용	• Administrative Regulation on Registration for Unmanned Aircraft Owner • 중국표준화관리국(SAC)에서 드론 관련 표준 기술 제정	• 항공법: 드론의 운용을 제한하는 법안이 2015년 발효 • 드론 관련 전략과제: 자동운전, 로봇/무인항공기 제조 등 중점 산업의 플랫폼화
관련 조직	• 연방항공청(FAA)	• 유럽항공안전청(EASA)	• 중국 민용 항공 총국(CAAC) • 중국표준화관리국(SAC)	• 경제산업성

표준	• 취미 또는 상업용 드론(sUAS)에 대해 DO-178이 권고	• SORA에서 드론에 대한 기술적 이슈 부분에 시스템 안전 관련 고려 항목 포함 • 현재 드론에 대한 명확한 기능/소프트웨어 안전에 대한 지침, 가이드, 표준 없음	• 드론을 위한 표준 시스템 제작 가이드에 시스템 표준 포함: 세부 파트인 AEA)시스템안전 필요 표준은 총 5가지 항목이며, 모두 시급히 개발 필요로 구분	• 드론에 대한 표준 가이드라인은 아직 명확히 정의되지 않음 • 드론을 로봇으로 간주하여 해당 가이드라인 적용 • 드론만의 특화된 국제 표준이 정의될 경우 이를 일본에 도입하여 표준화한다는 계획

제3절 주요 산업 도메인별 해외 주요국의 소프트웨어 안전 활동

여기서는 2015년, 2016년 ‘소프트웨어 안전 산업 동향 조사’에서 조사된 안전이 중요한 주요 산업 도메인인 자동차, 철도, 원자력, 항공 부분에 대해 해외 주요국의 소프트웨어 안전 활동을 일부 업데이트 후, 종합하여 표로 정리하였는데, 해외 주요국(미국, EU(유럽), 독일, 영국, 일본 등)의 활동을 정부활동(법·제도 포함), 관련조직, 안전표준의 3가지 영역으로 정리하였다.

1. 자동차

<표 2-8> 자동차 부문 해외 주요국의 안전 활동

	미국	유럽	일본
정부 활동	• 제조물 책임법(Products Liability Law)에 근거하여, 제조사가 안전사고 발생 시 예상되는 소송에 대비하여 안전 표준에 따른 자동차의 설계 및 제조를 유도 • NHTSA의 자국 자동차 판매에 대한 안전 표준 준수 여부 활동 수행. 필요 시 리콜이나 벌금형의 제재 조치	• 자동차 판매 전, 형식승인을 통한 검사를 수행하고, EEC/ECE 법규의 인가를 받은 다음, 각 나라의 인증을 받아야 판매 가능 • 유럽 자동차 형식승인 지침인 2007/46/EC 사용 • 제조물 책임법(Products Liability Law)에 근거하여, 제조사가 안전사고 발생 시 예상되는 소송에 대비하여, 안전 표준에 따라 자동차를 설계하고 제조하도록 유도	• 정부 연구 기관이 표준 해석, 공통 활동 및 문서 제작 등의 선도적 역할 수행
관련 조직	• NHTSA	• UNECE(United Nation Economic Commission for Europe) • 영국 형식승인 기관: Vehicle Certification	• JARI(Japan Automobile Research Institute: 일본 자동차 연구기관

		Agency • 독일 형식승인 기관: Kraftfahrt-Bundesamt (KBA). Federal Motor Transport Authority 등	• JAMA(Japan Automobile Manufacturers Association: 일본 자동차 제조사 협회)
표준	• 제조물 책임법에서 최신 기술 사용 요구: 글로벌 설계 표준으로 인정받고 있는 ISO 26262를 준수	• UN/ECE Regulation No.100 Electric Vehicle Safety에서 준용해야할 기능 안전 국제 표준으로 ISO 26262 명시	• 정부 연구 기관과 완성차 및 자동차 부품 업체 등이 협력하여, ISO 26262 도입

2. 철도

<표 2-9> 철도 부문 해외 주요국의 안전 활동

	미국	유럽
정부 활동	• 미 연방철도국(Federal Railroad Administration: FRA)은 2010년 성과 중심의 안전 규정을 발표 • 49 CFR Part 236 Subpart H: 프로세스 기반의 시그널 및 철도 통제 시스템 개발 표준 • 49 CFR Part 236 Subpart I: PTC(Positive Train Control System)	• 유럽연합에서 철도 안전 및 상호운용 관련 지침(Directive 2004/49/EC, 2008/57/EC)을 제정 • ERA(European Railway Agency)에서 기술 사양서(TSI: Technical Specifications for Interoperability)를 제공 • 각 회원국은 관련 지침에 의거해서 자국의 철도관련 법・제도를 개정/ TSI를 근간으로 기술적 요구사항을 제정하여 운영
관련 조직	• 미 연방철도국(Federal Railroad Administration: FRA)	• ERA(European Railway Agency) • Notified Body(정부에서 인증받은 철도 인증 조직) • National Safety Authority(정부 안전 관련 기관) • Investigating Body(사고 및 사건 조사 조직)

		• Infrastructure Manager(철도 인프라 및 안전 관리 조직)
표준	• FRA 규정: AREMA 2011 C&S Manual, IEEE 1483 & 1474, MIL STD 882C • 소프트웨어 및 시스템 관련 안전 보증 표준: AREMA, 2011 C&S Manual Part 17.3.1, 17.3.2, 17.3.3	• 기술 사양서에 포함된 규정: EN 50128 / IEC 62279

3. 원자력

<표 2-10> 원자력 부문 해외 주요국의 안전 활동

	미국	영국	독일
법/ 제도	• 10 CFR Part 50 (Domestic Licensing of Production and Utilization Facilities, 제조와 이용시설의 국내 허가)를 통해 고의적 위법에 대해 NRC가 개별적으로 강제 조치 • NRC는 10 CFR Part 50의 Appendix B (Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants)에 QA 요구사항 설정	• 목표설정체계(Goal-Setting regime)를 운영 • 보건 안전법(H소프트웨어A, Health and Safety at Work etc. Act 1974), 에너지법 2013 및 원자력설치법 1965에 의하여 ONR 관리 감독 • 목표설정체계 ONR:규제책임, 사용권자:안전보증책임 • ONR의 SAP(Safety Assessment Principle) 가이드로 평가 수행	• 원자력법/ 법령, KTA 표준

관련 조직	• NRC (Nuclear Regulatory Commission, 원자력규제위원회)이 발의한 연방 규정에 의해 관리	• 원자력 규제 활동은 대표적으로 ONR(Office of Nuclear Regulation, 원자력규제사무국)이 원자력 규제	• 표준화 활동은 DKE와 VDI에서 수행 • 원자력규제기관은 BMUB (Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit, 환경, 자연 보호, 건설 및 원자력 안전에 대한 연방정부부처)가 • BMUB 하위 조직: BFS (Bundesamt für Strahlenschutz, 방사선보호연 방사무국)
표준	• IEEE Std 7-4.3.2-2003 (원자력 발전소의 안전 시스템에서 디지털 컴퓨터에 대한 표준 기준) • Regulatory Guide 1.152를 통하여 컴퓨터의 기능과 설계 요구사항에 대한 규정 준수 방법 소개	• IEC 60880을 주요 레퍼런스로 사용. 그러나 원자력 발전소의 소프트웨어에 적용하는 특정 표준 없음	• KTA의 원자력 기술 지침에 독일의 I&C (Instrument and Control) 기능과 설비 안전 요구사항 명문화 • DIN(독일표준연구소)은 국제표준인 IEC 880을 국가표준으로 채택 • 컴퓨터나 소프트웨어에 특화된 지침으로, DIN은 DIN IEC 880을 소프트웨어 V&V에 사용되는 주요 표준으로 사용

4. 항공

<표 2-11> 항공 부문 해외 주요국의 안전 활동자료

	미국	유럽
법/제도	• FAR (Federal Aviation Regulations)에 전자 설비 또는 시스템을 사용하는 디지털 컴퓨터 기술에 대한 규제준수 증명 방법으로 DO-178B 사용 가능 • FAA Order 8110.49 DO-178B에 대한 승인절차 가이드라인 배포	• 미국과 유사한 체계와 표준 적용
관련 조직	• FAA(Federal Aviation Administration, 미국연방항공청) • NASA(National Aeronautics and Space Administration, 미국우주항공국)	• EASA (European Aviation Safety Agency, 유럽항공안전기구) • JAA (Joint Aviation Authorities, 유럽항공연합) • CAA (Civil Aviation Authority, 민간항공기구)
표준	• 우주항공: NASA 표준체계 적용 • NASA 표준: NPR-STD-8719.13(소프트웨어 표준), NPR-GB-8719.13 (소프트웨어 가이드북) • 상용항공: DO-178B/ED-12B 적용 • 국방 표준: MIL-STD 498	• 상용항공: DO-178B/ED-12B 적용

제4절 해외 선진사례 조사 시사점

이머징(Emerging) 산업인 자율주행차, 드론에 대한 정부의 활동(법・제도, 국가기관, 표준 제정)의 측면과 기능/소프트웨어 안전 측면의 2가지 주제에 대해 미국, 유럽연합(EU), 독일, 영국, 중국, 일본 등의 국가를 조사하였고, 전통적으로 안전이 중요한 산업 분야인 자동차, 철도, 원자력, 항공 부분의 정부 활동과 소프트웨어 안전에 대해 조사하였다. 조사 결과 시사점은 법・제도/규정, 관리기관, 기능/안전 표준, 지침, 가이드의

3가지 영역으로 정리하였다.

• 법・제도/규정

1. 이머징 산업은 특성상, 대부분의 해외 주요 국가에서는 프레임워크 수준의 법・제도를 제정하거나 제정 중에 있었는데, 주요 내용은 해당 산업에 대한 정의, 규제 범위, 규제 구분, 규제 기관 및 규제 기관의 권한, 안전 및 책임에 대한 포괄적 가이드라인 등 이다.

2. 국가별 산업 환경, 국민 정서 등의 중요시 하는 부분이 달라, 법・제도가 상이하게 제정되는 경우도 있었는데, 자율주행차의 경우 독일은 사고 시 차량 운전자가 사고에 대한 책임이 있다고 명시한 반면(독일은 완전 자율 주행의 개념은 아직 법에서 고려하고 있지 않았다), 영국은 자율 주행시 발생하는 차량 사고에 대해 차량 운전자에 대한 책임을 묻지 않았다. 또한, 독일의 경우 자율 주행시 우려되는 윤리의 문제에 대해서 고민하고, 이를 법・제도에 반영하였고, 미국은 기능안전, 연방/주 간 권한 및 책임 등에 대해 주안점을 두고 있었다. 일본의 경우 책임과 윤리적 문제 측면보다는 산업 측면에서 자율주행 관련 표준을 선점하기 위해 자율주행 기능 중심으로 가이드라인을 제시하였다. 철도의 경우도 화물운송을 중시하는 미국과 승객 운송을 중시하는 유럽의 산업 환경이 달라, 법・제도/규정 상이하게 제정되어 있었다.

3. 융복합적인 성격을 띄고 있는 산업의 경우, 법・제도에서 타 산업 제도를 활용하거나, 참조하는 경우가 많았다.

4. 이머징 산업의 경우, 해당 산업을 선도하기 위해 각 국은 법・제도를 다소 느슨하게 적용하여 규제 보다는 지원 및 산업활성화 방향으로 제정되어 있었다. 특히, 안전 규정에서 기능적인 표준, 기술에 대한 명시가 명확히 되어 있지 않은데, 이는 현재 개발 중이기도 하지만, 현 상황에서 성급하게 표준, 기술을 명시할 경우 기술 발전 저해를 우려하여 의도적으로 포괄적으로 명시한 경우도 있었다.

• 관리 기관

1. 이머징 산업인 자율주행차, 드론에 모두 기존 정부의 관리 기관이 관리 영역을 확대하여 관리하게 되었다.

2. 정부 기관의 역할은 이머징 산업 및 전통적인 산업 모두 규정 제정, 관리/감독, 지

침/가이드 연구 및 지원, 관련 산업 성장 지원 등이 있었다.

3. 융복합적인 성격(항공, 자율주행차, 드론 등)을 띄고 있는 산업의 경우, 주관 기관은 타 기관(정부 기관, 연구 기관, 사설 기관 등)과 법·제도 제정, 관리/감독, 지침/가이드 제정 등의 분야에서 긴밀한 협업을 하고 있었다. 또한, 이러한 협업은 업무 주관 관점 보다는 업무 조정 관점에서 진행되는 경우가 많았다.

- 기능/소프트웨어 안전 표준, 지침, 가이드

1. 전통적 안전 관련 산업은 안전 표준, 지침, 가이드가 상세하게 기술 되어 있었으며, 국제 표준 또한 존재하고 있었다. 반면, 이머징 산업은 아직 이러한 표준, 지침, 가이드가 없었고, 심지어 국제 표준이나 각 국가별 표준도 없는 상황이었다.

2. 이머징 산업은 새로이 만들고 있는 표준 일부 영역에 전통 안전 관련 산업의 표준을 활용하라고 권고하고 있었는데, 자율주행차는 ISO 26262, 드론의 경우 항공 표준인 DO-178 등이 있었다.

3. 이머징 산업의 경우 대부분의 국가가 표준, 지침, 가이드 수립을 위해 국제 표준 협회 및 유관 국제 기관 등과 긴밀하게 협업하고 있었다.

제3장 해외 TIC 시장 현황 조사

제1절 TIC 시장에 대한 정의 및 조사 방식

TIC란 'Testing, Inspection and Certification'의 줄임말로, 'Testing'은 '생산된 제품 또는 결과물이 절차에 따라 만들고자 하는 목적과 부합하는지 시험하는 활동'을 의미하고, 'Inspection'은 '생산된 제품 또는 결과물, 제품 또는 결과물의 설계 내용 및 생산 과정, 생산 또는 설치에 대해 검사하는 활동'을 의미하며, 'Certification'은 '앞에서 언급한 제품 또는 생산물과 생산 과정, 생산을 위한 생산 체계 및 관리 체계, 생산 활동과 관련한 사람에 대한 제 3자의 증명을 인증하는 활동'을 의미한다.

이 3가지 활동은 과거부터 기업의 내부에서 필요에 의해 자체적으로 시행하였으나 약 100년 이전부터 점차로 이를 위탁받아 전문적으로 대행해주는 서비스 사업자가 등장하며 최근에는 일반 기업들이 이들에게 TIC 관련된 업무를 위탁하는 추세로 진행하고 있어, 최근에는 TIC 전체 수요의 약 40%를 TIC 전문 서비스 사업자들이 아웃소싱하고 있는 것으로 파악되고 있는데,[106] 본 보고서에서는 TIC 관련된 업무를 위탁받아 대행하거나 관련된 서비스를 제공하는 사업을 기업의 주된 사업으로 하는 사업자들을 TIC 기업이라고 칭하였다.

본 보고서의 조사 대상인 소프트웨어 안전 분야는 이러한 TIC의 영역에 포함되는 개념으로, TIC 기업에서 제공하는 서비스 유형 중 소프트웨어 안전 관련 영역이 존재하여 TIC 기업의 조사를 통해 소프트웨어 안전 관련한 영역의 규모 및 특성을 파악하고자 하였다. 그러나 TIC 기업에서 소프트웨어 안전과 관련한 사업의 매출이나 공헌이익 등, 직접 성과를 측정 또는 추정할 수 있는 자료 또는 정보가 없었기 때문에 소프트웨어 안전 영역만의 조사 대신 TIC 산업 전반에 대해 조사를 진행하였다. 이는 일반적으로 TIC 기업들의 사업 구성이 전방 산업[107]에 맞춰 식품, 의료, 생활 등과 같은 식으로 구분되어 있고 공통 기능/서비스 측면의 소프트웨어 안전 분야는 별도 사업부로 분리되어 있지 않아 각 전방 산업에 조금씩 포함되어 있기 때문이다. 다만, 향후 소프트웨어 안전의 중요도가 높아지고 AI와 같이 독자적인 사업 영역을 구축하는 소프트웨

106) TIC Market Overview, Bureau Veritas, 2018
107) 최종 소비자를 대상으로 영업하는 업종들

어 분야, I아이템이 증가한다면 독자 시장으로의 조사가 가능할 것으로 보인다.

또한 국내 TIC 시장이 아직 다른 소프트웨어 관련 산업 대비 규모가 작고 사업자들이 대부분 영세한 특성상 국내 시장에 대한 조사보다는 해외 TIC 시장 및 사업자 중심으로 조사하였다.

먼저 국내에서 설립하여 국내 원자력, 철도, 전기발전 산업 영역에서 성장한 기업들의 경우 대부분 정부 중심의 Captive 사업(전속 사업[108]) 하에서 사업을 영위해 왔기 때문에 아직 그 규모가 중견기업 이하, 중소기업인 경우가 많았다. 이러한 기업들은 규모가 영세하여 대부분 외감법[109] 상 외부감사 대상이 아니었으며, 이에 따라 경영성과나 상황에 대해 공시해야 할 의무가 없다. 만약 이들 기업에 대한 조사를 진행하려면 소프트웨어 관련한 사업의 담당자뿐만 아니라 재무와 경영관리를 담당하는 임원의 인터뷰나 이들을 통한 기업 내부 현황에 대한 조사가 필요한데 이는 본 조사의 범위를 넘어서는 것이라 불가능하였다.

그 다음으로 해외 TIC 사업자가 국내에 진출하여 설립한 국내 법인의 경우에는 대부분이 유한회사 형태였는데, 유한회사는 외감법상 외부감사를 통한 정보 공개의 대상에서 제외되어 있어 조사할 수 없었다. 이들 경영진에 대한 접촉이나 재무상 성과, 경영관리 현황에 대한 조사는 국내 TIC 기업 조사가 가지는 한계와 같기 때문이다. 단, 외감법의 개정으로 ‘18년 11월 이후부터는 유한회사라고 하더라도 외부감사의 대상이 될 수 있어 현재 조사가 불가능한 외국계 TIC 한국 법인 중 일부는 ’20년 이후 경영성과 정도의 정보는 조사가 가능할 것으로 예상한다. 이에 따라 국내 TIC 기업에 대해서는 설문의 내용을 기반으로 해외 TIC 기업의 조사 내용과 간략히 비교하는 수준으로 분석을 진행하였다.

정보 수집 및 조사가 제한적인 국내 TIC 시장과는 달리, 해외 TIC 시장은 규모가 국내보다 매우 크고, 상위 선도 사업자의 경우 조단위 경영성과를 보이며 다국적 기업 형태의 사업을 하고 있는데, 이들은 투자자들을 위해 연단위 사업보고서를 비롯하여 각종 재무 정보 및 사업 내용, 전략에 대해 비교적 상세히 정보를 공개하고 있다. 물론 소규모 해외 TIC 사업자들은 정보를 공개한 내용이 없거나 부실한 경우도 많지만, 시장의 형성 및 구성, 미래에 변화할 방향에 대해서는 주로 상위 선도 사업자들에 의해 이루어지고 있어 선도 사업자만을 조사 대상으로 정해도 TIC 시장을 충분히 대표할 수 있다고 보았다. 그래서 해외 TIC 시장의 ‘17년 매출 기준 상위 선도 사업자 10

108) 일반적으로 고객/발주/매입처 대상 영업권을 보장받아 사업하는 형태를 지칭
109) 주식회사의 외부감사에 대한 법률, 국가법령정보센터

개사들을 중심으로 이들의 사업보고서 및 TIC 산업 관련한 전문 리서치 기관들의 보고서를 바탕으로 조사를 진행하였다.

제2절 해외 TIC 시장 구성 및 선진사업자 현황

1. 해외 TIC 시장 구성

1) 과거의 성장 동인

과거 TIC 사업의 성장 동인을 전방 산업을 비롯하여 전 세계 경제 관련한 거시적 측면과 주요 TIC 기업의 내부 경영 상황 측면에서 살펴보았다.

우선 거시적 측면에서 살펴보면, 첫 번째 성장 동인은 TIC 산업의 전방 시장, 즉 고객사들이 분포하는 시장은 전부 규제 시장이었다는 점이다. 규제는 한번 설정되면 특별한 사유가 없는 한 지속하는 특성이 있어, 규제에서 비롯한 규제 시장도 한번 형성되면 사라지거나 위축되기가 어려워 장기간 안정적인 시장을 형성하게 된다. 이러한 규제는 주로 원자력 중심의 에너지 관련 산업이나 철도 산업, 자동차 산업 등 전통적으로 Safety가 강조되며 장기간 운영 경험이 축적되어 누적된 규제가 상당히 많다는 특징을 가진다. 최근에는 미국이 트럼프 대통령이 당선된 이후 보호무역주의로의 회귀를 선언하고, 중국에 대한 관세장벽을 신설하는 등 규제가 늘어날 조짐을 보여 시장의 성장세가 더욱더 굳건하게 유지될 것으로 보인다.

두 번째로 전 세계적으로 제4차 산업 혁명이 추진되고 있다는 점이다. 미국과 일본, 유럽 등 주요 선진국들이 제4차 산업 혁명을 새로운 성장 동력으로 제시하면서 주요 방향과 육성 대상 산업 아이템들이 발표되었는데, 공통으로 AI 중심의 전기자동차, 자율주행자동차, 드론이 포함되어 있었다. 이는 TIC 시장에 있어 새로운 전방 시장이 형성된다는 의미였으며, 아직 육성 대상 기술이나 시장이 완벽히 형성되지 않은 상황을 고려하면 향후 TIC 업계에 신사업 먹거리는 충분히 공급될 것으로 예상된다.

기업 내부 경영 상황 측면에서 과거 TIC 시장의 성장 동인을 고려해 보면, 첫 번째로 낮은 리스크를 꼽을 수 있다. 앞서 살펴본 바와 같이 신 보호무역주의의 대두 및 강화 추세에 영국 그렌펠타워 화재 사건[110], 독일의 폭스바겐사 디젤 게이트 사건 등

110) '17년 6월 14일 새벽 1시경 런던 래티머 로드에 있는 24층짜리 아파트, 그렌펠 타워(Grenfell

으로 안전 측면의 규제가 강화되고 있고, 규제라는 것이 한번 설정되면 사라지거나 약화되기 어려운 특성이 있어 TIC 기업 입장에서는 특별한 시장 개척 노력이 없이도 저절로 전방 시장이 확대 및 유지되므로 특별한 경영상 실수/실패가 없는 한 사업의 지속성은 보장되기 때문이다. 또한 TIC 시장의 서비스 공급 특성을 고려할 수 있는데, 고객사와 TIC 기업과의 계약은 주로 건당 계약이 아닌 기간 계약이면서, 1년 미만보다는 1년 이상의 장기 계약으로 진행한다는 점이다. TIC 기업은 이를 통해 장기간 안정적인 매출을 보장받을 수 있어 경영상 Risk가 적다고 볼 수 있다.

또한 두 번째 성장 동인은 기업의 투자비(CAPEX)가 타 산업보다 상대적으로 낮다는 점이다. 이는 TIC 사업이 서비스업이라는 특징에서 비롯되는데, 최초 사업 시작할 당시 갖춰야 할 최소한의 자산 (기술, 소프트웨어, Tool 등)을 제외하고는 규제나 표준이 변하지 않는 이상 기존 설비, 자산을 지속 활용할 수 있고 추가적인 투자 비용이 작다는 점이다. 이는 타 산업 대비 매년 지출하는 비용 중 감가상각의 비중 및 비용을 줄일 수 있고, 이를 통해 투자 현금흐름을 좋게 만들어 단기적인 손익과 현금흐름의 재무성과 모두를 극대화할 수 있다. 또한 이러한 적은 투자비용과 단기적 높은 성과는 타 산업 대비 월등히 높은 수익률(IRR[111])을 보장한다. 게다가 거시적으로 살펴본 바와 같이 규제 시장이라 시장의 변동성이 작다는 점과, 타 산업 대비 경기 변동에 민감하지 않는다는 점도 적은 투자비용 대비 높은 수익성을 보장하는 성공 요소라고 볼 수 있다.

세 번째로 낮은 원자재 매입 부담을 들 수 있다. 앞서 언급한 바와 같이, TIC 사업이 주로 서비스업인 관계로 매입할 원자재가 거의 없다는 것이다. 최근 신보호무역주의로 강화되고 있는 무역장벽과 재해, 경기 변동으로 발생하는 큰 폭의 원자재 가격변동의 영향으로 타 산업은 원가 변동에 기인한 경영 성과의 부침이 심하지만, TIC 산업은 원자재 매입이 없어 원가 측면에서 안정적이고 일관된 흐름을 보여준다. 경영자 입장에서는 외부 변수로 인한 경영 성과 변동 폭이 작으므로, 내부 요인에 대해서만 집중하여 합리화, 절감 정책을 추진할 수 있고 비용 통제가 용이하므로 일관된 경영 정책을 펼칠 수 있다.

Tower)에서 일어난 화재 사건으로, 발화 원인은 4층 한 세대에서 폭발한 냉장고때문인 것으로 밝혀졌는데, 안전 설비의 부족과 대피 지침의 오류, 가연성 자재 사용으로 인해 4층부터 24층까지 전소(全燒)하였고, 이로 인해 사망 72명, 실종 1명, 부상 약 70여명이 발생한 사고였다.

111) Internal Rate of Return: 투자비용 대비 현금흐름을 은행의 이자율 개념으로 산출한 수익률 지표

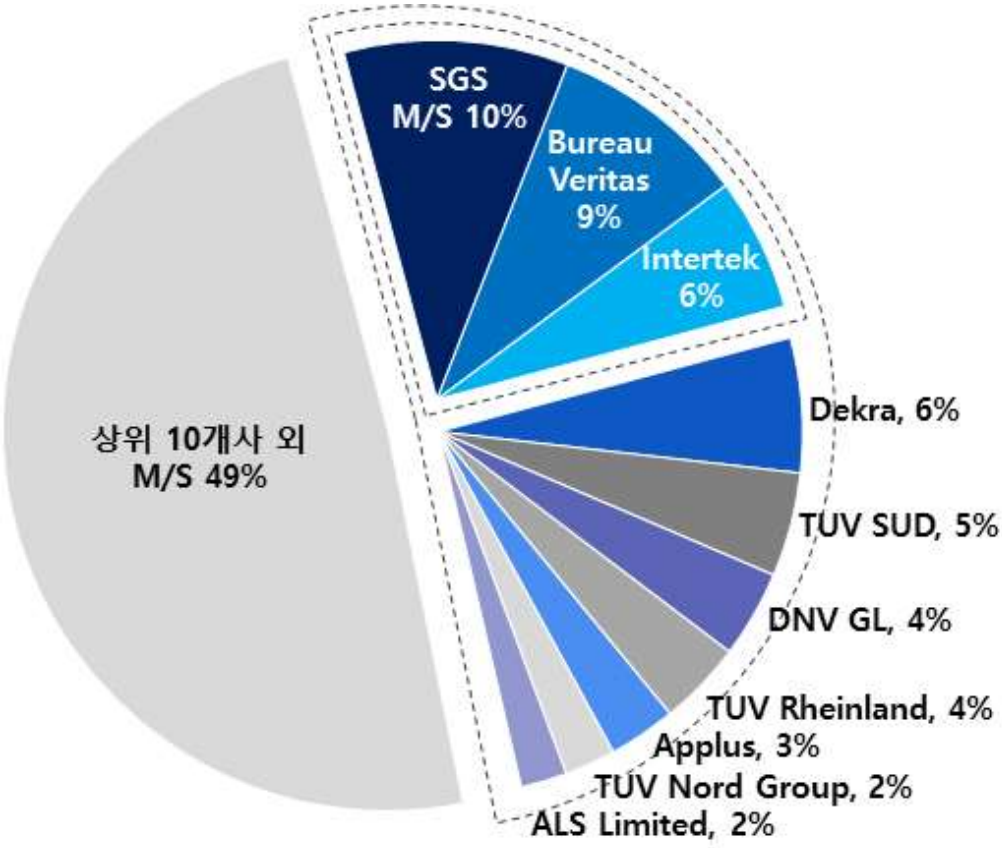
2) ‘17년 시장 구성 및 특성

TIC 시장의 구성은 2016년 조사의 연장 선상에서 조사하였다. 2016년 조사 결과, 10개 정도의 소수 사업자들이 시장의 절반에 가까운 비율을 점하고 있었는데, 2017년 조사에서도 이러한 현상은 거의 변동 없이 지속되는 것으로 확인되었다. 매출 기준 상위 10개 사업자를 선정한 결과, 이들은 SGS, Bureau Veritas, Intertek, Dekra, TUV SUD, DNV GL, TUV Rheinland, Applus, TUV Nord Group, ALS Limited였으며, 이들의 시장 점유율은 총 51%로 절반이상이었고, 위 열거한 순서대로 시장 점유율이(총매출 규모) 높았다. 특히 SGS, Bureau Veritas, Intertek의 3개사는 이들의 시장점유율 합계가 전체 시장 규모의 25%에 달하는 과점 형태를 보였다.

종합적으로 살펴봤을 때 TIC 시장은 지속해서 과점 시장이면서 파편화된 시장 특성을 보인다. 이는 앞서 살펴본 바와 같이 안정적, 지속적 성장하는 시장이면서 경영상 Risk가 적고 투자비 대비 수익성이 높은 사업이라는 점에서, 일정 수준 이상의 규모를 가지거나 경영 환경이 안정된 기업들은 자본 시장으로부터의 자본 조달이 쉬워 자본 시장에서 조달한 대규모 자본을 바탕으로 인수/합병을 통해 규모를 키우고 다국적 기업화하는 경향에서 비롯된다. 실제로 다수의 중간 순위 시장점유율을 보이는 기업들은 시장 및 사업 분야 확대를 목적으로 사모펀드[112]에 인수되거나 사모펀드로부터 투자를 받은 상황이었으며, 시장의 최상위 사업자들은 수십개 이상의 국가에 진출하여 글로벌 시장을 대상으로 하는 다국적 기업이었다. 이러한 특성상, 현시점에서도 TIC 시장에서 인수합병이 활발히 일어나고 있는 것으로 보인다.

112) 비공개적으로 소수의 투자자로부터 돈을 모아 기업을 사고 파는 것을 중심으로 운영되는 펀드

[그림 3-1] 2017년 TIC 시장 구성, 사업자별 시장점유율



자료: TIC outlook, Barclays (2018), 매출 상위 10대 기업 ' 17년 Annual Report

2. 시장 선도 사업자

앞서 살펴본 바와 같이, 시장은 상위 10개 사업자 중심으로 성과가 편중되어 있고 그 중에서도 상위 3개 사업자의 실적이 독보적으로 우수한 관계로, 본 조사에서는 해당 3개 사업자인 SGS, Bureau Veritas, Intertek 3개사에 대해서만 '17년 동향을 조사하기로 하였다.

1) 시장 1위 사업자 SGS

SGS는 2017년 6.3BN USD의 매출을 올렸다. 이는 한화 기준 약 9조원 규모[113]로 2017년 TIC 시장 규모를 61BN USD로 추정할 경우, 약 10%에 해당되는 시장점유율을 보인다. 이는 2016년 매출에서 5.4% (YoY[114]) 증가한 것으로 향후 '23년까지 예측한 연평균 시장 성장률 5%와 유사한 수준인 것으로 판단된다. 연평균 시장 성장률과 시

113) 2017년 연평균 환율인 1 USD 당 1,110원 적용
114) Year Over Year 약자, 이전 연도 대비 당해 연도 성장률을 나타냄

장 규모 추산에 대한 자세한 내용은 다음 절에서 다룰 예정이다.

수익성 측면에서는 영업이익률이 15.3%로 높은 단기적 수익성을 보였다. 금액으로는 영업이익이 969M USD로, 한화로 환산하면 약 1조 1천억 원에 해당하는 규모이다. 전년도 영업이익률과 비교하면 2016년 영업이익률과 2017년 영업이익률은 둘 다 15.3%로 같았는데, 이는 SGS가 과점 시장의 최상위 사업자이면서 시장 선도적 위치와 높은 수익성을 바탕으로 경영이 안정되어 있음을 보여주는 것이다.

주요 사업 분야로는 매출 기준으로 에너지/화학(18%), 식생활(16%), 소비재/유통(15%) 분야가 전체 사업에서 차지하는 비중이 절반에 가까웠다. 나머지 사업으로는 산업재(14%), 광물(11%), 교통/운수(9%), 환경/건강(8%), 인증발급/관리(5%), 공공분야(4%)로 구성되어 있었다.

최근 사업 및 경영상 주요 활동으로는 전자제품에 대한 통신망 이용 사물통신 관련 인증 및 표준 사업 추진, 식품에 대한 새로운 미국의 안전 기준 대응, EU의 정보 보호 규제에 대한 대응을 추진하거나 완료하였다.

SGS는 향후 디지털 제품 또는 디지털 관련된 서비스 산업의 인증 분야의 성장을 예상하고 있어 로봇, 드론, 자율주행차량, 3D 프린터 분야의 매출 확대를 추진하고 있다. 이를 위해 TIC 4.0이라는 새로운 비전과 전략을 수립하고 Cloud 등 신기술 기반의 디지털화를 추진하며 이를 통해 사업 경쟁력 확보 및 신규 시장 창출을 기대하고 있다.

[그림 3-2] SGS의 Business Portfolio, 2017년

자료: SGS, 2017년 사업 보고서

2) 시장 2위 사업자 Bureau Veritas

Bureau Veritas는 2017년 약 4.7BN Euro의 매출을 올렸다. 이는 한화로 환산하면 약 6조 2천억 원 규모[115]로 약 9%대의 시장 점유율을 보여, 1위 사업자인 SGS와는 약 2조 8천억 원 정도의 격차가 확인되었다. 전년도 대비해서는 매출이 약 3% 증가하였는데, SGS의 성장률(YoY) 5%보다는 조금 낮은 성장률을 보였다. 영업이익률은 15.2%로 타 산업 대비 높은 편이고, 1위 사업자인 SGS와도 비슷한 수준으로 판단되나, 전년도 대비해서는 거의 1%P 하락한 것으로, 당사의 매출과 영업이익만으로 판단할 경우 2016년 대비하여 2017년에는 경영 성과가 조금 미진한 것으로 보인다.

주요 사업 분야는 건설/인프라, 식생활, 산업재에 대한 품질 인증 사업으로, 이 3가지 사업 분야는 전체 사업 실적의 70% 가까이 차지하였다. 사업별로 매출에서 차지하는 비율을 살펴보면, 건설/인프라에 대한 감리/품질 검토 사업이 24%, 생활용품 및 식품의 인체 미치는 영향 및 안전 검사 사업이 23%, 산업재와 산업 현장에 대한 안전 인증이 23%, 일반 유통되는 소비재에 대한 안전 인증이 14%, 해양 선박 등의 건조 품질/안전 검수 분야가 8%, 인증 발급 및 관리 사업이 8% 순으로 나타났다.

[그림 3-3] Bureau Veritas의 Business Portfolio, 2017년

자료: Bureau Veritas, 2017년 사업보고서

지역별로는 아시아 지역 매출 비중이 31%로 유럽의 34% 보다는 조금 낮았으나, 조직 규모나 진출한 사업장 개수는 아시아 지역이 1위로, 향후 회사의 사업 비중이 아시

115) 2017년 연평균 환율인 1 유로(Euro, €) 당 1,320원 적용

아 지역으로 이동할 것임을 보여주고 있다. 이는 국가별로 나누어 매출 비중 순위를 살펴보면 명확한데, 중국이 2017년 국가 단위 매출 1위(19%)를 보인다.

Bureau Veritas의 향후 성장 전략은 다음의 몇 가지로 압축될 수 있다. 먼저 대형 글로벌 다국적 고객사와의 전략적 제휴를 통해 영업을 효율화한다는 것이다. TIC 사업은 국가별 법·제도상 규제를 바탕으로 차이가 발생하므로 국가 단위로 다른 시장이라고 볼 수 있는데, 글로벌 사업장을 보유한 다국적 기업을 공략할 경우, 다수의 시장을 한 번에 공략할 수 있으므로 영업의 효율화가 가능하다고 보는 것이다.

두 번째로는 대륙 권역별, 국가별 시장 환경 특성에 맞춰, 특정 국가나 권역에서 축적한 사업 역량과 Best Practice를 타 지역으로 확산시킨다는 전략이다. 이를 통해 Bureau veritas의 전반적인 품질의 향상을 도모하고, 글로벌 품질 표준화를 이뤄 품질 측면 경쟁력을 강화하겠다는 것이다.

기타 생산성 향상을 통한 운영 효율화, 인수합병을 통한 외형 확장 및 시장 점유율을 확대하는 전략을 추진할 계획이다.

3) 시장 3위 사업자 Intertek

Intertek는 2017년 약 2.7BN Euro의 매출을 올렸다. 이는 한화로 약 3조 5천억원 규모[116]로써 약 6%대의 시장 점유율에 해당한다. 전년도 대비해서는 매출이 약 8% (YoY) 증가하는 성과를 보였으며, 영업이익률은 14.2%로 전년 대비는 0.2%P 하락하였는데, 매출의 급격한 증가 대비 비용 증가를 효과적으로 억제한 결과 타 경쟁사 대비 나쁘지 않은 성적을 기록하였다.

Intertek는 사업부를 크게 3가지 영역으로 나눴는데, 2017년 매출 기준으로 전자제품 및 통신, 건설, 인프라, 운송 등의 분야를 담당하는 제조업 분야에서 59%를 차지하였고, 화물, 무역, 농업 생산물 관련한 국제 무역 분야에서 23%를 차지하였다. 채굴, 광물 생산과 관련한 원자재 분야가 가장 작은 18%의 성과를 올렸는데 이는 원자재 분야의 매출이 전년대비 8.6%가 감소하였기 때문으로 보인다.

최근 사업 및 경영상 주요 활동으로는 드론을 이용한 검사 기술을 개발하고, Connected Car[117] 인증 사업을 육성하고 있으며, 중장기적으로 에너지, 건설/인프라

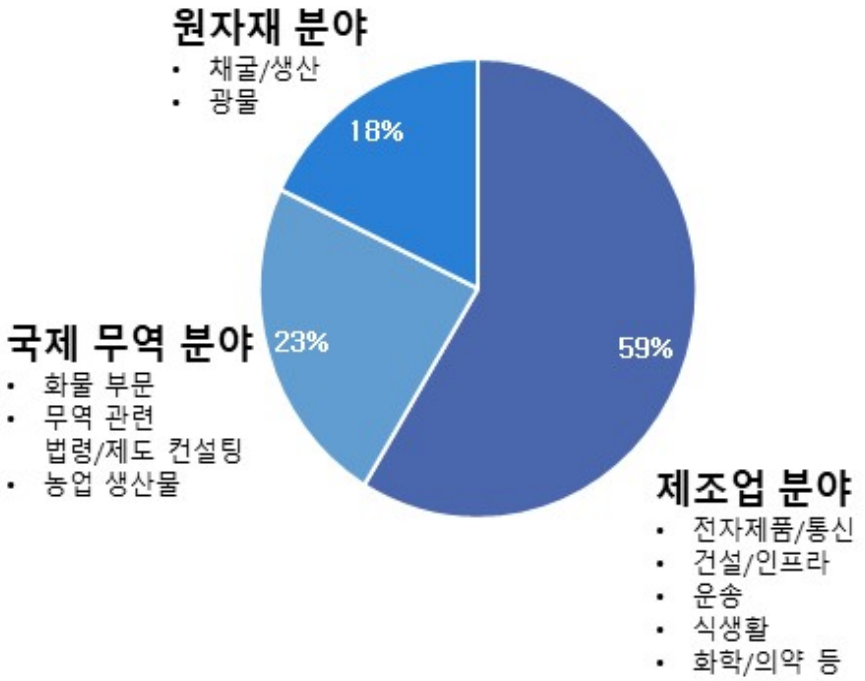
116) 2017년 연평균 환율인 1 유로(Euro, €) 당 1,320원 적용

117) 차량에 무선 네트워크 기기를 내장하여 인터넷 접속이 가능한 차량임. (전기차/내연기관자동차와 같은 차량 동력/구동방식과는 무관함)

분야에 신기술을 개발하고 적용하여 경쟁력을 강화한다는 계획을 하고 있다.

그 외에 향후 성장을 위해 잠재 시장 발굴 강화 전략을 추진할 계획이다. 사업 보고서에 따르면, Intertek는 현재의 TIC 시장의 4배 규모의 잠재 시장이 존재할 것으로 추정하고 있다. 잠재 시장을 경쟁사보다 먼저 선점하여 매출 및 시장 점유율 증대를 꾀한다는 전략이다. 또한 글로벌 진출 국가, 영역의 확장과 적극적 현지화를 통해 영업 경쟁력을 강화하고, TIC와 연계한 보증(Assurance)[118] 영역을 포괄하는 토탈 서비스 역량을 강화하고, 기술 및 인적 투자를 통해 본원적 역량을 강화한다는 전략을 추진할 계획이다. 이를 위해 최근 KJ Tech 및 Acumen Security를 인수했다고 발표하였다.

[그림 3-4] Intertek의 Business Portfolio, 2017년



자료: Intertek, 2017년 사업보고서

118) 기업이 사업을 지속하는 데 있어 영향을 주는 요인 또는 변수들을 찾고 이들의 위험성을 최소화시키거나 제거하는 활동

제3절 해외 TIC시장 전망

1. 해외 TIC 시장 내/외부 변수의 변화 방향[119)]

다음으로는 시장의 외부적, 내부적 변화를 유발하는 변수를 살펴보고 향후 5년 ~ 10년 정도의 변화 방향을 고려하여 TIC 시장에 어떤 영향을 줄 수 있는지 검토하였다. TIC 시장에의 영향은 긍정적이거나 부정적인 영향의 두 가지로 나누어 예측하였다.

TIC 시장에 영향을 줄 수 있는 외부 변수로는 전방 시장인 제조/서비스업 전반의 변화 동향을 검토하여, '아웃소싱 성장', '신흥 시장 부상', '브랜드 보호 강화', '공급망 글로벌화' 라는 방향을 도출하였다. 또한 국가의 '법·제도 등 규제 강화', 국가 간 '보호무역주의 강화' 도 TIC 시장에 영향을 줄 수 있는 중요 요인으로 검토하였다.

내부 변수로는 TIC 사업자들의 공통된 화두인 'Digital TIC'에 대해 검토하였다. Digital TIC는 제4차 산업 혁명 화두에 맞추어 TIC 사업 측면에서 기여할 수 있는 영역, 역량을 발굴하고 사업화한다는 비전이다.

<표 3-1> 시장 내/외부 변수 변화 방향 및 TIC 시장에의 영향

구분	변화 방향	내용	TIC 시장에의 영향
외부 변수 변화 방향	아웃소싱 증가	• 글로벌 전체 시장의 약 40%가 아웃소싱 • In-house에서 아웃소싱이 점차 확대되는 추세	긍정적
	국가별 법·제도 강화	• 글로벌 자동차 기업의 배기가스 스캔들과 영국 그렌펠 타워 화재 배경 • 자발적 준수에서 국가적 강제화 진행중	긍정적
	신흥 시장 부상	• 다국적 TIC 기업들이 개발도상국 중심 신규 지역 진출 추세 • 대표적으로 중국	긍정적

119) Barclays, TIC Trend Report, 2018; TIC 주요 사업자 10개사 2016년, 2017년 사업보고서 참고

	브랜드 보호 강화	• 글로벌 소비자들의 품질과 안전에 대한 의식 변화 • 품질과 안전 기준으로 고객사 브랜드 가치 평가	긍정적
	공급망 글로벌화	• 고객사들의 원자재 조달, 제품 판매의 글로벌화에 따라 검사/인증의 글로벌 지원 역량 중요시	긍정적
	보호무역주의 확산	• 국제 무역량 감소에 따른 TIC 계약 감소 우려	부정적
		• 보호무역을 위한 진입장벽 강화로 새로운 수요 창출	긍정적
내부 변화 방향	Digital TIC	• 드론, Big Data 등 새로운 기술 요소를 도입하여 경쟁력 강화	긍정적

Barclays, TIC Trend Report, 2018; TIC 주요 사업자 10개사 2016년, 2017년 사업보고서

시장 내/외부 변수들의 변화 방향과 TIC 시장에의 영향을 종합적으로 검토한 결과, 글로벌 시장 법·제도 강화 및 전방 산업 필요성 증가 등의 변화는 전반적으로 TIC 시장에 긍정적 영향을 미칠 것으로 예상된다. 물론 보호무역주의 확산에 의해 국제 무역량이 감소하여 일부 TIC 사업 분야의 매출 감소가 발생할 수는 있으나, 오히려 각국 규제가 강화되어 새로운 수요가 창출되거나 글로벌 사업자가 국가별 경쟁력 강화나 점유율 확대를 위해 지역단위 인수/합병이 증가할 것으로 예상된다.

2. 해외 TIC 사업자들의 인수/합병 (M&A) 동향

1) 2017년 대표적 인수/합병 사례[120]

TIC 사업이 높은 수익성과 낮은 Risk로 지속적 성장이 확실시되는 관계로 TIC 산업으로 새로운 투자와 자본의 유입이 지속적으로 이루어지고 있으며, TIC 시장의 중/상위권 시장 점유율을 보이는 사업자들은 우수한 현금 동원력을 통해 신규 사업 영역을 확장하거나, 시장 점유율을 증대시키기 위해 인수/합병에 적극적으로 나서고 있다.

120) 출처: SGS, Element, Eurofin 각 사 2017년 사업보고서, 홈페이지 공시 자료

- **SGS의 Transparency-One 지분 투자 (20%)**

SGS의 경우, 업계에서 추진하는 'Digital TIC' 방향에 맞춰 'TIC 4.0' 이라는 선도적 비전을 선포하였다. 이는 제4차 산업 혁명에서 생겨나는 새로운 사업 Item에 대응하여 TIC 사업 모델을 확장한다는 개념으로, 이를 위해 Big Data, Cloud 등 새로운 기술을 도입하여 정보 수집/분석 역량을 확보하겠다는 전략이다.

이러한 전략을 실현하기 위해 SGS는 Big Data와 Cloud 등의 기술을 보유한 기업을 물색하였고, 그중 Transparency-One이라는 식품, 소매업을 대상으로 Cloud 기반의 공급망 정보를 수집, Big Data 분석으로 이력을 추적하는 플랫폼을 운영하는 기업을 발굴하여, 인수/합병 사전 단계로 지분 투자를 진행하였다.

이번 투자를 통하여 SGS는 Transparency-One의 지분을 20% 인수하였는데, 일반적으로 기업의 경영 상황을 살펴보기 위한 수준의 지분 투자였으며 특별한 사업상 Risk나 문제가 없는 한, 경영권 인수를 위한 추가 투자가 진행될 것으로 보인다. 이번 투자를 통해 Cloud 및 Big Data, 암호화폐 관련 기술에 대한 파트너십을 확보하였고 SGS 내부적으로는 3D 프린터, AI 등의 새로운 분야의 시장 창출은 물론 기존 인증 사업의 역량 강화에도 도움을 줄 것으로 기대하고 있다.

- **Element의 Exova 인수 및 합병**

Element사는 미국을 중심으로 성장해온 항공 및 운송 분야 전문 TIC 기업으로, '11년 ~ ' 17년까지 연평균 매출 성장률이 25%에 달하는 고성장을 기록한 회사이다. 대주주는 사모펀드로서, TIC 시장의 안정성과 TIC 시장의 성장률을 웃도는 Element사의 성장성에 주목하여 Element사의 인수 이후에도 매출/고객/사업부문 확대를 위한 추가적 인수/합병을 추진 중이다.

'17년에는 지리적 시장의 확장과 고객 확장을 위해 Exova의 인수 및 합병을 추진하였다. Exova는 주로 유럽 시장을 중심으로, 보건 및 항공, 운송, 에너지, 건설 분야 TIC 전문 기업으로, 이번 합병 결과를 통해 Element사는 매출 총 7억 달러, 고객 수는 양사 기존 고객 통합으로 4만 고객을 확보하였다.

- Eurofin의 EAG 인수

Eurofin은 식품/제약/환경 분야 테스팅 전문기업으로, 경쟁력 강화를 통한 매출 증대와 기술 포트폴리오를 다변화하기 위한 일환으로 유사 사업 Item을 보유한 EAG를 인수하였다. EAG는 Materials & Engineering Science 분야에서 시장 점유율 1위인 기업으로, 무기/유기 재료의 테스팅을 전문으로 하는 기업이었다. Eurofin과는 테스팅이라는 사업 분야가 유사하고, Eurofin의 사업 Item인 식품/제약과 EAG의 사업 Item인 무기/유기 재료 간 유사성이 인수를 통한 기술/역량의 공유라는 시너지를 기대하게 하였다. 결과적으로 Eurofin에서는 일단 이번 인수 완료를 통해 '18년도 매출에 2백만 달러 증대 효과를 기대하고 있는 것으로 알려졌다.

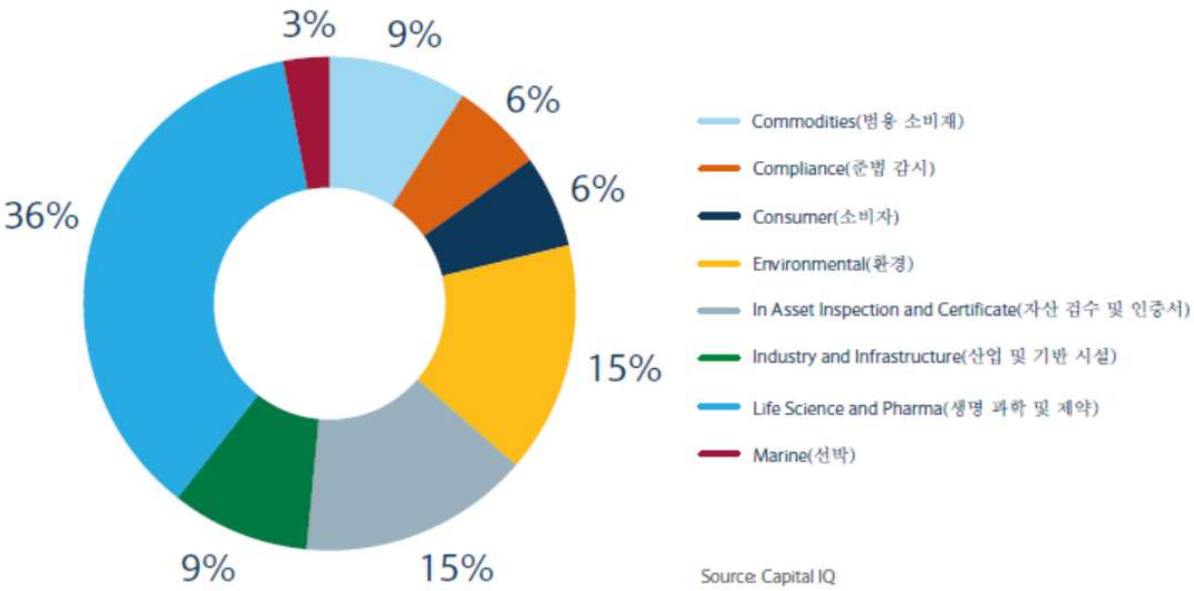
2) 해외 TIC 산업 전반적인 인수/합병 흐름

2017년 연간 이루어진 인수/합병을 산업 영역별로 구분하여 어떤 영역에서 활발히 인수/합병이 이루어졌는지 살펴보았는데, 이를 파악하기 위하여 기업의 인수/합병이 일어날 경우 피인수 기업의 사업부 별로 나누어 그 건수를 세고, 그 전체의 수의 합으로 사업 분야별 백분율을 계산하였다.

2017년 인수/합병이 가장 활발하게 발생한 산업 영역은 생명 공학 및 제약 분야로서 전체 발생 건수의 약 40%가 해당 분야에서 발생하였다. 그 다음은 자산 검수 및 인증 분야와 환경 분야로 각각 15%씩 해당 분야에서 차지하였다. 이를 통하여 향후 많은 기업들의 사업 영역의 무게 중심이 해당 분야들로 이동할 것으로 예상되며 기업들은 인수/합병 외에도 해당 영역의 역량 확보를 위해 인력 채용, 기술 개발 등의 노력을 쏟을 것으로 예상된다.

3. 해외 TIC 시장 성장에 대한 전망[121)]

[그림 3-5] 산업 분야 별 인수/합병 건 단위 비중



자료: Barclays (2018), TIC Market Prospection Report; Capital IQ (2017), M&A across Sectors

현재의 시장 규모는 얼마이며, 향후 성장 추이는 어떻게 될 것인지 예측하기 위하여 다수의 TIC 시장에 대한 여러 기관들의 Report와 견해들을 참고하였으나, 2017년 해당 연도의 시장 규모 추산부터 기관별로 달라 시장 선도 사업자들의 Annual Report를 참고하여 직접 시장 규모를 추산하였다. 본 연구를 통해 추정한 시장은 정부에서 자체적으로 시행하고 있는 사업들이나 기업 내부에서 조달하는 서비스 시장의 규모(인소싱, Insourcing)은 제외하고 TIC 전문 기업들이 수주하는 아웃소싱(Outsourcing) 시장만을 대상으로 하였다.

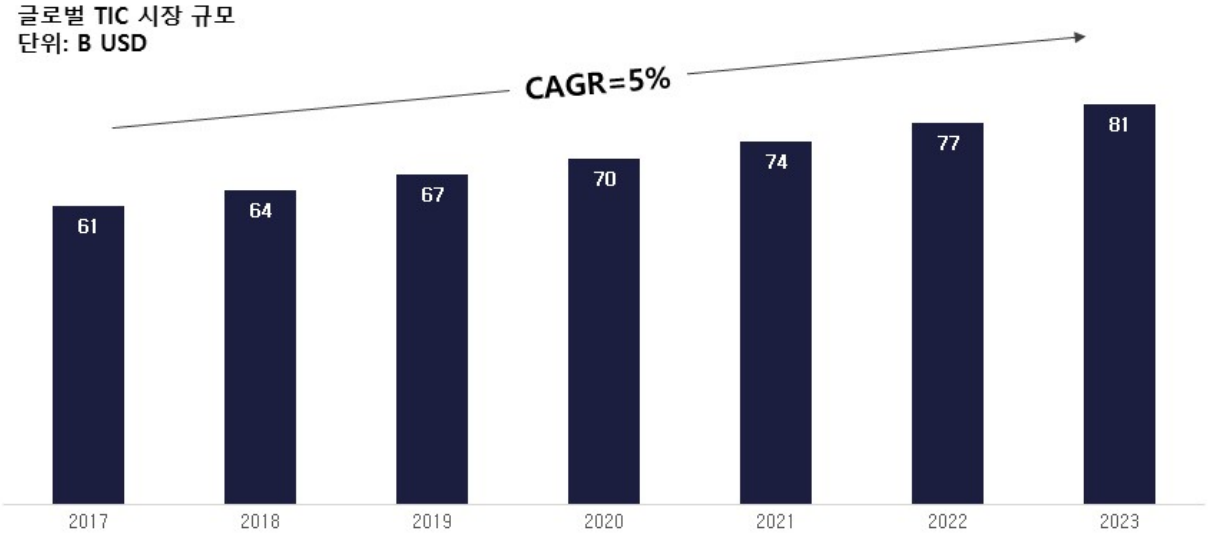
2017년 시장의 규모를 추산한 결과, 글로벌 전체시장은 약 61BN USD, 한화로 약 67조원 규모로 파악되었다. 이는 업계 Leading 기업인 SGS, Bureau Veritas, Intertek의 3개사 ' 17년 매출 합계액을 전체 시장 규모의 25%로 가정하여 역으로 시장 규모 산출한 결과이다.

위에서 추산한 2017년의 시장 규모를 바탕으로, 다수 기관의 Report를 참고한 결과, 대부분 기관에서는 2023년까지의 시장 규모 성장률을 연평균 5.0% ~ 5.5% 수준으로

121) 참고: Barclays, 2018; Markets and Markets, 2018; Market Research Future, 2018; Transparency Market Research, 2018; Market Watch, 2018; TIC 주요 기업 2017년 사업보고서 등

예측하고 있었는데, 앞서 살펴본 시장 변수의 변화 방향이 대부분 TIC 시장 성장에 긍정적이라는 의견과, 선도 사업자들의 매출 증가율이 5% 이상인 점을 고려하면 합리적이며 타당성이 있다고 판단된다. 다만, 기관들이 제시한 값들의 범위가 기관별로 차이를 보이므로, 보수적인 자세로 연평균 5.0%의 성장률을 가정하였고, 이를 적용하여 2023년의 시장 규모를 예측한 결과 81BN USD, 한화로 약 90조원의 시장이 형성될 것으로 예상하였다.

[그림 3-6] 해외 TIC 시장 성장 전망



자료: Barclays, 2018; Markets and Markets, 2018; Market Research Future, 2018;

제4절 해외 TIC 사업자와 국내 TIC 사업자와의 비교

1. 국내 TIC 사업자들의 성장 과정 및 한계

국내 TIC 사업자들은 해외와 비교하여 아직 그 역사가 길지 않다. 이번 조사 대상 기업은 소프트웨어 안전 컨설팅, 소프트웨어 안전 관련 도구, 소프트웨어 안전 국제 표준 관련 인증 지원의 9개사였는데, 한국SGS의 국내 법인 설립은 1979년으로 가장 앞서지만 해외 기업이 국내에 진출한 경우이므로 실제 국내 자본으로 설립한 기업인 한컴MDS(구 MDS테크놀로지)를 국내 TIC 기업의 시작으로 보는 것이 타당하며 해당 기업의 설립 연도가 1994년이라 국내 TIC 산업은 짧게는 약 20년 정도, 길게 봐야 약 40년의 역사를 가진다고 볼 수 있다. 이는 해외의 100년 이상 된 기업들과 비교해보면

아직 초기 시장 형성 단계로 보는 것이 타당하다고 생각된다.

약 20년 ~ 40년의 기간 동안 국내 TIC 사업자들은 TIC 사업 분야를 전문적으로 하기는 어려웠다. 업계 관계자의 인터뷰에 따르면, 대다수의 사업자들이 초기부터 TIC 전문 기업으로 시작하였던 것은 아닌 것으로 보이며 원자력이나 철도, 방위산업 등 공공분야의 사업을 수주하면서 제품 개발 과정에서 테스팅하던 역량을 바탕으로 TIC 사업 분야로 전문성을 키워갔다고 보인다.

문제는 이들 공공 분야 사업이 국가가 발주하는 종속 사업인 관계로(Captive Business) 국가 규제로부터 발생하는 사업만 진행하다 보니 연속성이 결여되어 TIC 사업만을 지속해서 하기에는 어려움이 있었고, 공공 부문 사업 특성 상 수익성이 높지 않아 전문성을 키우는 데는 한계가 있었다고 보인다.

또한 이들 TIC 사업 병행 기업이 공공 부문 외 민간 부문으로 사업을 확장하려고 해도, 이미 한국 시장에 진출해 있는 해외 TIC 기업 대비 대응이 빠르고, 협의가 쉽다는 점 외에는 해당 분야 사업 수행 경험이 상대적으로 부족하여 경쟁력이 떨어지는 상황이다.

2. 국내 TIC 산업 전망 및 Risk

업계 관계자 인터뷰에 따르면, 최근 탈원전 기조에 따라 원자력 분야의 수요가 줄어들 수 있는 점이 관련된 국내 TIC 사업자들에게 위기가 될 수 있는 부정적 요인으로 꼽혔다. 다만 에너지 수요는 감소하지 않았고 오히려 계속 증가한다는 점을 고려한다면, 신재생 에너지와 같이 원자력 에너지의 대체 에너지 부문에서 TIC 서비스 수요가 증가할 수 있어 전적으로 부정적으로 보기에는 무리가 있다.

또 다른 견해로는 제4차 산업 혁명의 주요 요소들과 관련하여, 해외보다 국내 관련 산업계의 발전이 더디기 때문에 해외 TIC 사업자보다는 해당 산업 분야 실적 확보가 부족하거나 확보하기에 불리하여 국내 TIC 사업자들의 경쟁력이 뒤처질 것이라는 우려가 있었다. 드론의 경우 국내 기술 수준은 미국과 같은 선도 시장의 사업자 대비 군수 부문은 약 15%, 민수(소형) 부문은 35% 뒤처지고 있다고 파악되었으며[122], 실례로 '17년 평창 동계 올림픽 기념행사에서 국내 기업이 아닌 해외 기업의 기술과 제품으로 드론 비행을 시연한 바 있다. 자율주행자동차도 마찬가지인데, 비전과 시장진입 전략, 파트너십, 생산 전략, 기술, 매출/마케팅/유통, 제품 품질 및 신뢰성 등 10가지 평가 지

122) '한국 드론, 소프트웨어 기술력 키워야 훨훨 난다', 경향비즈, 2018.2

표에 따라 자율주행시스템을 개발하고 있는 세계 주요 19개 업체의 경쟁력을 조사한 결과, 국내 최대 완성차 제조 사업자의 경쟁력은 해외 선도 사업자들보다 다소 뒤처지고 있다는 연구 결과를 확인하였다.[123)]

마지막으로 국내 TIC 시장이 해외 TIC 시장보다 규모가 작다보니 자본의 조달이 어렵고, 일부 사업자를 제외하고는 경영성과나 그와 관련된 정보를 얻기 어려워 자본 시장의 주목을 받지 못하고 있는 점이 자본 확충을 통해 새로운 사업이나 영역으로 확장 및 발전하는 데 걸림돌이 되고 있다고 보인다.

제5절 TIC시장 전망에 대한 시사점

해외 및 국내 TIC 시장에 대해서 살펴본 결과 다음과 같은 시사점을 도출하였다.

- **해외 TIC 시장은 높은 수익성이 보장되는 안정적인 시장이다.**

전방 시장이 규제 시장인 관계로 안정된 성장세가 유지될 것으로 보인다. 또한 사업상 Risk 및 투자비가 적기 때문에 높은 수익성 유지가 가능하다.

이러한 사업 특성에 힘입어 소수의 시장 선점 선도 사업자들의 규모가 크게 성장하여, 매출 상위 10개 사업자가 시장의 50% 이상을 점유하는 과점 시장이 되었다. 이로 인해 대형 사업자의 신규 시장 진출은 어려우며, 소규모 기존 사업자들을 대상으로 중대형 사업자들의 인수/합병이 활발히 이루어지고 있다.

- **시장 내/외부 변수들의 변화 방향이 대체로 TIC 시장 성장에 긍정적이다.**

산업 전반적 아웃소싱 증가 및 안전에 대한 법·제도 강화, 중국으로 대표되는 신흥시장 부상, 공급망 글로벌화가 TIC 산업 성장을 견인할 것으로 예상된다. 보호무역주의 강화로 일부 무역업 분야 수요의 소폭 감소가 예상되나, 오히려 지역단위 M&A, 글로벌화는 확대가 예상된다.

123) '자율주행자동차 최근 동향 및 시사점', 정보통신기술진흥센터, 2018.4

- **사업 지역/영역 확장, 기술경쟁력 강화를 위한 M&A 활발히 진행 중이다.**

SGS는 Digital TIC 달성을 위한 Big Data, Cloud 기술확보를 위해, 식품 분야에서 Cloud/Big Data 기술 기반으로 공급망 정보를 수집하고 유통 이력을 추적하는 Platform을 보유한 Transparency-One에 지분을 인수하였다. SGS의 이번 지분 인수율은 약 20%로, 3~5년의 경영실적 판단 후 인수/합병 추진이 예상된다.

Element는 미국 중심에서 글로벌로 지역 확대를 위해 다국적 TIC기업 Exova의 인수 및 합병을 완료하였다. Element는 이를 통해 고객의 확장 및 매출의 증대 효과를 누릴 수 있었다.

Eurofin은 신규 사업 Item 확장 및 기술 Portfolio 확대를 위해 인접 분야 기업인 EAG를 인수하였다. Eurofin은 주로 식품/의약품 분야 테스팅 기업이었고, EAG는 무기/유기 재료에 대한 테스팅 전문 기업이라 이번 합병을 통해 TIC의 근본 기술 및 서비스 범주가 늘어나게 되었다.

- **해외 TIC 시장은 앞으로도 안정적으로 성장할 것으로 전망된다.**

시장 내외부 변수의 긍정적 영향과 시장 안정성/수익성을 바탕으로 ’23년까지 연 5%씩 성장이 예상된다. (’17년 시장 규모 67조원 → ‘23년 90조원)

- **국내 TIC 시장은 여전히 성장이 제한적일 것으로 보인다.**

국내 사업자들은 해외 사업자들보다 경험이 부족하여 경쟁력이 떨어져 공공 부문에서 민간 부문으로 확장은 어려울 것으로 보이며, 민간 부문으로의 확장을 추진하더라도 민간 부문의 드론, 자율주행 등 신산업 관련 전방시장이 해외에 비해 더딘 발전 또는 낮은 경쟁력을 보여 양쪽 모두 성장 또는 확장이 어려울 수 있다.

제4장 소프트웨어 안전 산업 동향 분석

본 장에서는 소프트웨어 안전 분야를 3가지 영역으로 구분하여 산업동향을 세밀히 살펴보고자 하였다. 우선 소프트웨어 안전성 확보를 위한 정책적/학술적 역할을 수행하는 주체인 소프트웨어 안전 분야 학계・정부(Governing Sector), 둘째는 컨설팅 테스팅 검사/인증 등을 통해 소프트웨어 안전을 점검하는 주체인 소프트웨어 안전 컨설팅(Supervising Sector), 마지막으로 소프트웨어가 설치된 제품 및 서비스를 제공하거나 활용하는 주체인 소프트웨어 안전 개발・사용자(End User)이다.

제1절 소프트웨어 안전 분야 학계・정부(Governing Sector)

1. 개요

소프트웨어 안전 학계・정부 분야는 2016년도와 같이 ‘소프트웨어 안전성 확보를 위한 정책적/학술적 역할을 수행하는 주체’라는 정의를 변경 없이 사용하였다.

금번 조사대상의 경우 기존의 정부 기관 및 학계뿐만 아니라 소프트웨어 안전과 관련이 높은 도메인(자동차, 철도, 원자력, 해양 등)에 속한 주요 연구 기관을 포함시켜 산업별로 좀 더 전문적인 조사를 수행하였다. 총 조사대상은 11개로 대학교 4개와 연구기관 7개로[124] 구성되었다.

본 조사를 위한 설문은 2016년 설문지를 토대로 일부 항목의 수정보완을 통해 5개 영역(소프트웨어 안전의 정의와 개념, 법・제도・정부, 표준화, 국내 시장현황, 해외 시장현황)으로 구성하였다.

조사방식은 인터뷰 대상으로 대면 인터뷰를 수행하는 것을 원칙으로 하였으나 불가한 경우에 한해 전화와 이메일을 활용하여 진행하였다.

124) 인터뷰 대상에 대한 상세 정보는 개인정보보호 요청 등으로 인해 익명으로 처리 하였다.

2. 인터뷰 상세내역

1) 소프트웨어 안전 정의와 개념

소프트웨어 안전의 정의는 인터뷰 대상자들의 의견을 종합해본다면 2016년과 마찬가지로 소프트웨어 안전은 인명이나 재산상 피해를 주는 사고 발생을 회피하기 위한 능동적인 방안을 포함하는 것으로 정의할 수 있다.

소프트웨어 안전의 개념에 대해서도 대부분 소프트웨어 품질과는 별도의 개념으로 파악하며 향후 소프트웨어 안전 분야가 정립되면 품질까지도 포함하는 개념으로 발전할 것이라는 의견이 많았다.

2) 법・제도/정부

(1) 소프트웨어 안전을 위한 법・제도 수정필요 항목 및 개선방향

2016년에도 안전이 기존 주요 산업분야와 더불어 Emerging 기술 및 산업(인공지능, 자율자동차 등) 대한 법제도의 체계적 정비의 중요성을 강조하였던 것처럼 금번 조사에서도 산업분야별 특성을 반영한 상세한 법제도화의 중요성을 재차 강조하였다.

또한 소프트웨어 안전사고의 발생 방지를 위한 예방 차원의 법・제도뿐만 아니라 사고 발생 시 전문가 집단의 문제점 분석과 사후 처리 방안에 대한 내용도 포함되어야 한다는 의견이 있었다. 일례로 최근 발생한 BMW 차량화재와 관련하여 소프트웨어 오류라는 진단도 있었으나 민간합동조사단[125]에 소프트웨어전문가가 포함되지 않아 정확한 문제점 분석이 이루어지지 않았다. 때문에 소프트웨어 안전관련 사고와 관련해서는 소프트웨어 전문가를 포함시키는 강제조항이 필요할 것으로 파악된다.

125) 한국교통안전공단은 BMW화재 관련 조사를 위해 민관합동조사단을 화재, 엔진, 법률, 자동차 전문가 및 소비자 단체 등 민간위원 총 20명으로 구성하였으나, 소프트웨어 전문가는 포함되지 않음(교통환경뉴스, 2018.8.31. 참조)

<표 4-1> 안전을 위한 법·제도 수정필요 항목 및 개선방향

주요 의견
• 법·제도를 통한 소프트웨어 안전사고를 미연에 방지하는 것도 중요하지만 사고 발생 후 재발을 방지하기 위한 사후처리 시스템의 구축도 중요함. 법·제도에서 소프트웨어 안전성에 대한 요구사항 뿐 아니라 사고 발생 시 대응과 사후 처리에 대한 항목들도 제시 필요 • 산업별로 적용되는 소프트웨어가 상이하므로 산업별로 특화된 소프트웨어 안전 인증체계 구축과 관련된 항목 추가가 필요. 산학연관 전문가집단, 이해관계자, 일반인 등을 대상으로 의견을 수렴하여 법·제도화를 추진해야 함 • 재난 및 안전관리기본법의 안전기준의 분야 및 범위 중 정보통신분야에 소프트웨어 안전과 관련된 내용이 반영되어야 하며, 소프트웨어 안전과 관련된 시스템 점검, 절차, 조사단 구성 등의 상세한 내용도 포함하여야 함 • 일부 산업분야에서는 소프트웨어 안전 분야에 대해 설계적합성부터 시험결과까지 검사기관의 확인을 제도화하고 있음. 타 산업분야에도 이처럼 전문검사기관의 소프트웨어 안전성 점검을 제도화하여야 하며 구체적인 안전성 기준과 적용 가이드라인 등을 상세하게 제시할 필요가 있음

(2) 소프트웨어 안전을 위한 국가 차원의 대응 체계

사회 전체적으로 소프트웨어 안전의 비중이 높아짐에 따라 소프트웨어 안전의 중요성이 높아지고 있지만 아직 국가 차원의 체계적인 대응은 부족한 것으로 파악되었다. 2016년과 금번 조사에서도 지속적으로 소프트웨어 안전을 위한 범국가적인 컨트롤 타워를 마련하는 것이 시급한 것으로 나타났다.

〈표 4-2〉 소프트웨어 안전을 위한 국가 차원의 대응 체계

주요 의견
• 사회 시스템 전반에 소프트웨어가 높은 비중을 차지함에 따라 소프트웨어 안전이 확보되지 않으면 국가 기반시설(수송, 금융, 통신 등)의 심각한 위험이 발생할 수 있으므로 국가 차원의 대응체계는 반드시 필요 • 현재 소프트웨어 안전을 전담하는 컨트롤 타워가 없어 부처별로 사안별 대응하고 있는 실정임. 소프트웨어 전문역량을 보유한 전문기관이 소프트웨어 안전사고 유형, 규모, 원인, 분야 등을 고려하여 체계적인 대응 체계 수립 필요

(3) 소프트웨어 안전을 위한 부처 및 기관의 역할

소프트웨어 안전 분야가 각 부처별로 산재하여 있는 만큼 우선 부처별로 소프트웨어 안전과 관련된 내용을 구체화하고 부처별 협업을 통해 총괄적인 관점의 관련 정책수립과 수행을 하는 것이 필요하다.

〈표 4-3〉 소프트웨어 안전을 위한 부처 및 기관의 역할

주요 의견
• 정부 부처 및 기관은 정책 수립 및 행정지원 역할을 하고 소프트웨어 안전에 대한 총괄관리는 별도의 전문기관이 담당하여야 함 • 정부 부처 및 기관들이 담당하고 있는 산업 분야에서 소프트웨어 안전관련 법/규제 개발 적용 및 가이드 마련 필요 • (산업부, 중기부) 소프트웨어 개발주체의 소프트웨어 안전 메커니즘 기술개발 지원, 산업/기술별 특성에 따른 소프트웨어 안전 적용방안 개발 지원 (국토부) 교통, 물류, 항공, 발전 등 국가기반시설에 대한 소프트웨어 안전 메커니즘 법/규제 개발 (과기부) 새로운 소프트웨어 안전 메커니즘 원천기술 개발 • 소프트웨어 안전이 요구되는 산업 분야별 참여자들이 교류할 수 있는 장을 마련해 주어야 함

3) 표준화

우리나라의 소프트웨어 안전분야 표준화는 해외 시장점유율이 높은 자동차, 원자력 산업 분야의 글로벌 참여 가능성이 높을 것으로 예측되어, 이는 2016년과 동일한 의견이 유지되었다.

이외에도 현재 국가기술표준원을 중심으로 표준화 활동 및 정책을 추진하고 있으나 표준화 활동의 특성상 대부분 개별 표준화 활동 위원을 중심으로 진행되어 국제 표준화 활동은 파편적으로 이루어지고 있다는 의견이 있었다.

국제 표준화 활동은 장기적인 지원이 필요하므로 다양한 국제 표준화 분야 중 공공성이 높은 분야는 국가 전략사업과 연계하여 중점 표준화 추진 분야를 선정해야한다. 그리고 국내 산학연 보유 기술 및 국제 표준화 선도를 위해 해당 산업의 기술적 전문성, 기술 토의 주도를 위한 외국어 역량, 해외 표준화 단체화의 네트워킹 역량 등을 보유한 표준화 인력 양성 및 표준화 추진 활동을 지원해야 한다는 의견도 제시되었다.

<표 4-4> 소프트웨어 안전관련 표준화 현황

주요 의견
• 국제적으로 시장점유율이 높은 자동차, 원자력 산업 분야 등은 글로벌 표준 참여 가능성이 높음 • 현재 국가기술표준원을 중심으로 표준화 활동 및 정책을 추진하고 있으나 표준화 활동의 특성상 대부분 개별 표준화 활동 위원을 중심으로 진행되어 국제 표준화 활동은 파편적으로 이루어지고 있음 • 국제 표준화 활동은 장기적인 지원이 필요하므로 다양한 국제 표준화 분야 중 공공성이 높은 분야는 국가 전략사업과 연계하여 중점 표준화 추진 분야를 선정하고 국내 산학연 보유 기술 및 국제 표준화 선도를 위한 전략적 표준화 인력 양성 및 표준화 추진 활동을 지원해야 함 • 주로 국가기술표준원, TTA, 대학교, 공공연구기관 등이 국제 표준화 활동에 참여하고 있음. 하지만 실제 상용화 개발경험이 없거나 산업 수요를 고려하지 않은 이론적 표준화 활동에 치중하는 경우도 존재 • 실제 소프트웨어 안전 부분을 개발 및 상용화하는 공공연구기관의 핵심 인력들이 TC(Technical Commit), SC(Submit Commit) 등에 참여하여 국제 표준화 활동에 영향력을 행사할 수 있도록 정부차원의 지원이 필요 • 향후 기업 경쟁력은 물론 더 나아가 국가의 기술 주도권 확보를 위해서

는 국제표준 전문가를 양성하고 민간에서는 그에 걸 맞는 대우를 해주는 것이 필요

4) 국내시장

2015년과 2016년의 국내시장 현황 조사내용 중 선진사 대비 TIC 기업의 역량부족, 전문인력 부족, 소프트웨어 안전에 대한 인식 부족 등 크게 변화된 것이 없는 부분도 있었다. 하지만 제4차 산업 혁명의 주요 기술의 등장에 따라 소프트웨어 안전의 중요성이 높아지고 그에 따라 관련 시장도 성장할 것이라는 의견이 눈에 띄게 많아졌다.

〈표 4-5〉 소프트웨어 안전관련 국내시장 현황

구분	주요 의견
국내 소프트웨어 인증 및 컨설팅 사업 현황	• 국내 TIC 기업은 소프트웨어 안전관련 레퍼런스가 부족하여 프로젝트에 참여하지 못하는 경우가 많고 레퍼런스를 만들기 위해 저가로 수주하고 품질이 낮은 결과물을 산출하여 역량을 축적하지 못하는 악순환이 반복되고 있는 실정 • 일부 TIC 기업은 해외 표준 문서를 번역하여 단순 정보만을 제공하는 경우가 많이 있으며, 전문성 결여와 시험기간과 비용문제로 고객사들의 불만이 종종 발생
소프트웨어 안전측면의 국내 시장 전망	• 소프트웨어 산업의 중요성 및 관련 제품이 지속적으로 증가하고 소프트웨어 시스템의 복잡도 역시 급격히 증가함에 따라 소프트웨어 안전관련 인증, 시험, 컨설팅 등의 관련 산업 확대가 필수적 • 제4차 산업혁명 등 산업현장에서 소프트웨어가 차지하는 비중이 지속적으로 높아질 것으로 예상되어 소프트웨어 안전관련 국내 시장도 성장할 것으로 예상

소프트웨어 안전의 활성화 방안	• 제품 인증 시 소프트웨어 안전 테스트를 의무적으로 실시하고 소프트웨어 안전 테스트 전문기관 도입 및 정부지원을 통한 업계 부담 최소화 • 민간분야의 자율적인 시장 확립 유도보다는 초기에는 관련 법/규제/지침 등을 선제적으로 마련하여 정부 주도의 소프트웨어 안전 정책을 주도하고 소프트웨어 공학 교육 프로그램 내 소프트웨어 안전 분야를 신설하고 교육을 지속적으로 확대하여야 함 • 소프트웨어 안전이 적용된 제품의 가치를 제대로 평가해주는 사회적 분위기가 필요함 • 소프트웨어 안전 전공인력이 거의 없이 인력난이 심각함. 인력양성이 산업과 연계되어야 함. 소프트웨어 전공자에 대한 재교육을 통해 소프트웨어 안전전문인력을 양성하는 방안도 검토 필요
산학연 연계 방안	• 소프트웨어 안전 전문인력 양성, 공동 기술개발 등을 통한 산학연 공동협의체 운영 등 • 국내외 표준화 전문 인력 양성 프로그램 공동 추진과 산업현장 적용을 위한 소프트웨어 안전 시험, 검증, 인증 전 분야에 걸친 소프트웨어 안전 메커니즘 기술 개발 및 산업계 현장 적용 필요

5) 해외시장

선진국은 표준화/인력양성/검증시스템/검증도구 등 소프트웨어 안전의 전체적인 부분에 대해 체계적인 절차를 보유하고 있지만 국내에서는 아직 미흡한 부분이 많다. 때문에 국내 소프트웨어 기반 기술에 대한 육성이 필요하며 이를 기반으로 한 소프트웨어 안전 메커니즘 설계 및 적용이 순차적으로 진행되어야 한다.

<표 4-6> 소프트웨어 안전관련 해외시장 현황

주요 의견
• 해외 법·제도를 무조건 수용하기 보다는 현재 국내 소프트웨어 안전 기술의 성숙도를 고려해서 단계적으로 도입해야 함 • 국내 소프트웨어 기반 기술에 대한 육성이 필요하며 이를 기반으로 한 소프트웨어 안전 메커니즘 설계 및 적용이 순차적으로 진행되어야 함 • 최근 제4차 산업혁명의 주요 기술인 인공지능, 빅데이터 등에 대해 규제나 가이드라인이 전무한 상태임. 예를 들어 딥러닝의 경우 어떤 데이터를 학습을 시키는 가에 따라 소프트웨어의 특성(안전)이 좌우되므로 소프트웨어의 성능뿐 아니라 데이터에 대한 검증 가이드라인 및 규제가 필요함 • 공공분야에서 안전관련 발주를 할 때 안전기능, 위험분석, 산출물에 대한 유지보수 안전검증 등 요구사항을 제시하고 검증해야 함

3. 요약

본 절에서는 소프트웨어 안전 전문기업을 대상으로 조사한 내용을 2015년과 2016년의 조사내용과 연계하여 법·제도, 인증·매뉴얼·표준, 인력·교육, 조직·기관, 산업환경개선, 프로세스로 구분하여 다음과 같은 시사점을 도출하였다.

우선 법·제도 측면에서는 소프트웨어 안전사고 발생 시 재발을 방지하기 위한 사후처리의 구체적인 방안에 대한 법·제도화가 필요하다. 소프트웨어 안전사고를 사전에 방지하는 것도 중요하지만 안전성에 대한 요구사항 뿐 아니라 사고 발생 시 대응과 사후 처리에 대한 내용을 법제화할 필요가 있다. 그리고 제4차 산업혁명의 주요 기술인 인공지능, 빅데이터 등과 관련된 규제나 검증 가이드라인이 필요하다.

인증·매뉴얼·표준 측면에서는 국제 표준화 활동은 단기적으로는 수행할 수 없으므로 다양한 국제 표준화 분야 중 국가 전략사업과 연계하여 중점 표준화 추진 분야를 설정하고 장기적 관점에서 지원을 해야 한다. 그와 더불어 국제표준 전문가도 양성하여야 한다.

인력·교육 측면에서는 소프트웨어 안전 전공자가 거의 없이 인력난이 심각하므로 산업과 연계된 인력양성이 필요하다. 소프트웨어 안전 인력양성은 2015년과 2016년부터 지속적으로 강하게 요구되고 있는 사안임에도 불구하고 아직 개선된 사항이 없어 금번 조사에서도 공통적으로 문제점을 지적하였다.

조직·기관 측면에서는 소프트웨어 안전을 총괄할 수 있는 역량을 갖춘 전문기관 신설이 필요하다. 소프트웨어 안전 인력양성과 더불어 2015년부터 지금까지 계속 요청되는 사항으로 소프트웨어 안전 전문가들을 보유한 전문기관 신설이 필요한 것으로 판단된다.

業 환경개선 측면에서는 TIC기업들이 갖춰야 할 주요 경쟁력인 소프트웨어 안전 프로젝트 레퍼런스 확보가 어려운 만큼 공공부문에서 최대한 기회를 제공토록 해야 한다. 그리고 소프트웨어 안전이 적용된 제품의 가치를 인정해주는 사회적 인식이 확산되어야 한다.

프로세스 측면에서는 국가차원의 소프트웨어 안전 문제 발생 시 주관 부처의 개별 대응이 아닌 범정부적 차원의 통합적인 문제해결이 필요하다. 그러기 위해서는 해당 조사반에 소프트웨어 안전 전문가가 포함되어 발생원인 분석, 사후 대응 방안 수립 등 일련의 과정에서 주요한 역할을 할 수 있도록 해야 한다.

제2절 소프트웨어 안전분야 사업 기업(Supervising Sector)

1. 개요

소프트웨어 안전분야 사업 기업의 산업동향 조사를 위해서 2016년도와 같이 국내 TIC(Testing, Inspection and Certification, 안전사업포함) 시장에서 활동하는 기업을 그 대상으로 하였다.

본 조사를 위한 설문은 2016년 설문지를 토대로 일부 항목의 수정·보완과 소프트웨어 안전 산업/시장에 대한 내용을 추가하여 총 4개 분야(기업 일반 현황, 소프트웨어 안전 프로세스 현황, 소프트웨어 안전 산업/시장에 대한 견해, 소프트웨어 안전 인프라 현황 및 요구사항)로 구성되었다.

대상 기업들의 주요 사업 영역은 소프트웨어공학 컨설팅, 소프트웨어 품질 향상을 위한 프로세스(Process), 제품(Product), 전문인력(People) 측면의 솔루션 제공, 소프트웨어 테스팅 자동화 도구 및 서비스 개발 및 공급, 임베디드 소프트웨어 테스팅 솔루션 제공, 엔지니어링 시뮬레이션, 각종 인증 지원 등으로 TIC 시장의 주요한 역할을 수행 중이다.

조사대상 기업은 총 9개로 평균 사업운영기간이 19년이고 매출규모가 평균 약 473억

원[126]으로 업무 전문성을 보유하고 업계 대표성을 지닌 기업들을 대상으로 하였다.

조사방식은 기업의 임원 혹은 실무부서 담당자를 대상으로 대면 인터뷰를 수행하는 것을 원칙으로 하였으나 불가한 때에만 전화와 이메일을 통해 인터뷰를 진행하였다.

설문내용은 4개 분야에 대해 18개의 문항과 그 하위 39개 세부문항을 통해 상세한 내용을 파악하였으며, 설문문항 이외에도 TIC 업계의 다양한 VOC(Voice of Customer)를 취합하여 정량적/정성적 인터뷰를 병행하였다.

본 조사에서는 조사기업의 수가 크지 않기 때문에 결과의 정량적 지표는 값보다는 추세를 파악하는 지표로 제공되었다. 그러나 국내 소프트웨어 안전 컨설팅 기업의 모수가 크지 않고, 본 조사에 속한 기업들이 국내 소프트웨어 안전 컨설팅 기업을 대표하도록 가능한 조사 대상을 선정하여 조사 결과의 객관성을 높이도록 구성하였다.

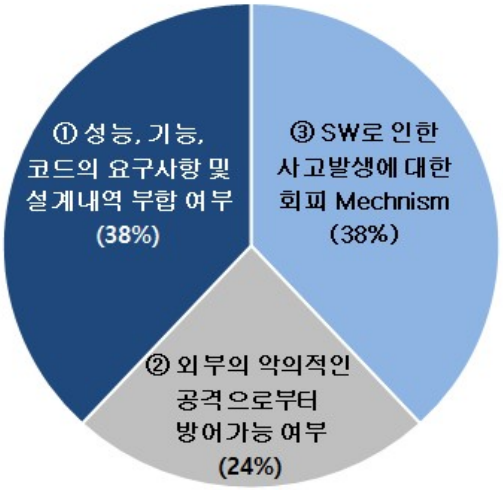
2. 기업일반 현황

1) 소프트웨어 안전 개념

소프트웨어 안전의 개념에 대해서는 38%가 ‘소프트웨어 안전은 성능, 기능, 코드가 요구사항에 부합하는지 여부’를, 38%는 ‘소프트웨어 안전은 예기치 못한 외부 환경 변화에 의하여 소프트웨어가 원인이 된 사고가 발생하는 것에 대한 회피 메커니즘(Mechanism) 보유 여부’를 선택하였으며, 나머지 28%가 ‘소프트웨어 안전은 외부의 악의적 공격으로부터 방어할 수 있는지 여부라고 응답하였다. 2016년 조사에서는 소프트웨어 안전을 보안(Security)관점으로 파악하여 ②번 문항을 선택한 응답률이 50%로 가장 많았으나 금번 조사에서는 그 수치가 줄어지고 품질과 회피 Mechanism으로 파악한 응답률이 높아 소프트웨어 안전에 대한 정확한 인식이 확산되고 있음을 알 수 있었다.

126) 2018년 신설기업 1개社 제외

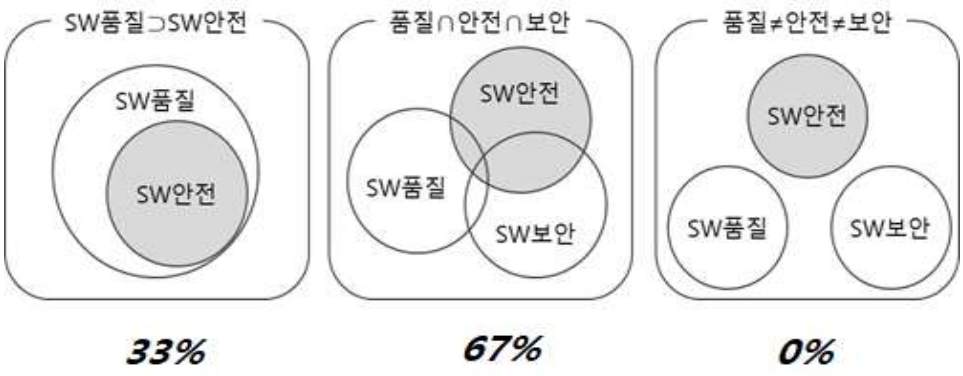
[그림 4-1] 소프트웨어 안전 개념 인식



2) 소프트웨어 안전, 품질, 보안의 관계

소프트웨어의 안전(Safety), 품질(Quality), 보안(Security)의 관계에 대해서 상호 독립적인 것이 아니라 소프트웨어 안전이란 3개 분야 간의 공통적인 요소로 구성되는 통합적 개념으로 파악하는 것이 67%로 대부분이었고 일부(33%)는 소프트웨어 안전과 보안의 공통요소를 품질이 포함하는 것으로 파악하였다.

[그림 4-2] 소프트웨어 안전-품질-보안의 관계



3) 고객 현황 및 요구사항

소프트웨어 안전 분야의 사업을 수행하는 기업의 주요 고객들은 주로 자동차(21%), 철도(18%), 원자력(15%), 정보통신(13%), 우주항공(8%), 의료(8%), 기타(18%) 등에 고루 분포되어 있었다.

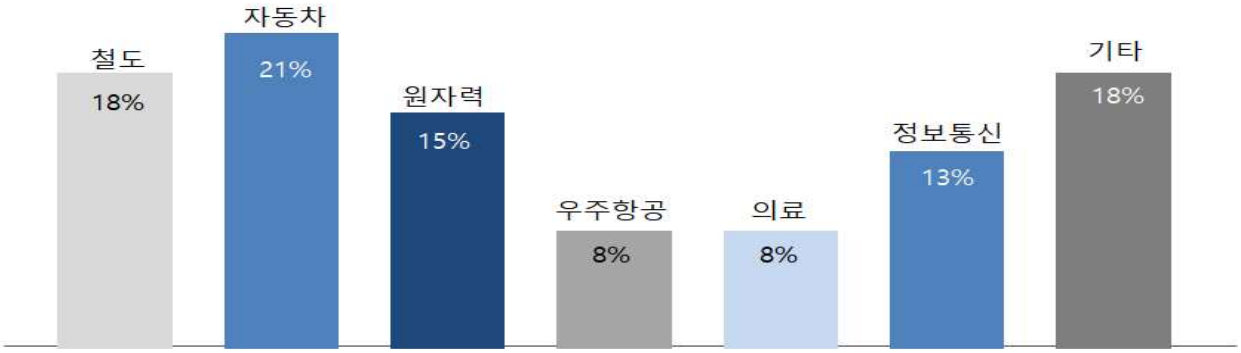
2015년도 조사에서는 자동차(44%), ICT/전자(28%), 국방/철도(17%), 금융(11%)으로 자동차 산업 중심으로 분포되어 있었으나, 2016년도 조사에서 자동차(16.7%), 철도(16.7%), 원자력(13.9%), 우주항공(13.9%), 의료(13.9%), 정보통신(13.9%), 기타(11.1%)로 자동차가 지속적으로 높았지만 전산업 분야로 분포되는 경향을 보였다. 특정 업체에 대해서는 특정 산업만을 서비스하고 있었으나, 전체 업체를 기준으로는 산업분야가 골고루 분포되는 것으로 파악되었다. 지속적해서 자동차 산업분야가 가장 높은 비중을 차지하고는 있지만 기타 산업(전력, 수자원, 방산, 빅데이터/인공지능 등)의 비중이 눈에 띄게 높아지고 분야 또한 다양해지고 있는 추세이다.

대상 기업의 고객사에 제공하는 서비스 및 상품의 유형으로는 ‘품질, 안전 및 인증 지원 컨설팅’이 29%로 가장 큰 비중을 차지하고 있었다. 이어 ‘품질, 안전 진단 관련 도구 판매’(21%), ‘용역 중심의 품질, 안전 서비스’(21%), ‘도구 기반의 품질, 안전 서비스’(18%), ‘수출요건지원컨설팅, 독립안전성 평가, 제품 안전성 인증 등 기타’(11%) 순으로 조사되었다. 서비스에 대한 상세 조사에서는 컨설팅의 형태나 용역을 형태로 위험 분석, 안전 아키텍처 설계, 테스트, 안전 프로세스 관련 지원을 하고 있는 것으로 나타났다. 또한 안전 관련 조직 및 프로세스 전반에 관한 서비스도 하고 있었다. 해외지사 기업의 경우는 인증관련 업무를 주로 하고 있었으며, 국내 기업의 경우는 아직은 안전 제품의 시험을 주로 하는 기업도 있었다.

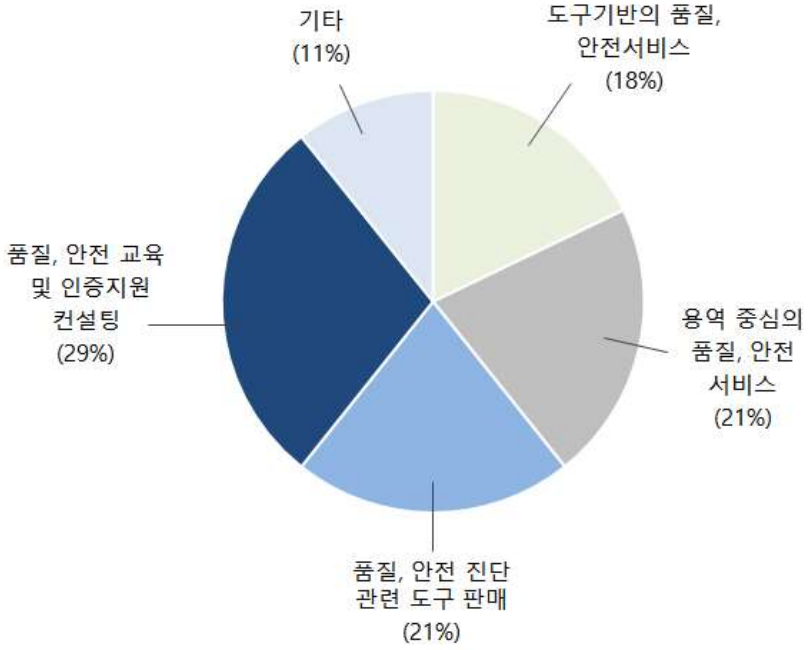
2015년에는 고객이 소프트웨어 안전에 대한 인식이 낮아 관련 서비스 및 상품이 구체화하지 않은 상황이었다. 2016년 조사에서는 ‘도구 기반의 품질, 안전 서비스’가 30%로 가장 높은 순위를 차지하였고 ‘품질, 안전 진단 관련 도구 판매’가 20%로 가장 낮은 순위를 차지하였으나, 금번 조사에서는 도구 판매가 두 번째로 높은 순위로 나타났다.

그리고 서비스 및 상품이 특정 분야에 치우침 없이 고르게 분포되어 안정적인 포트폴리오를 구성하고 있는 것으로 보인다.

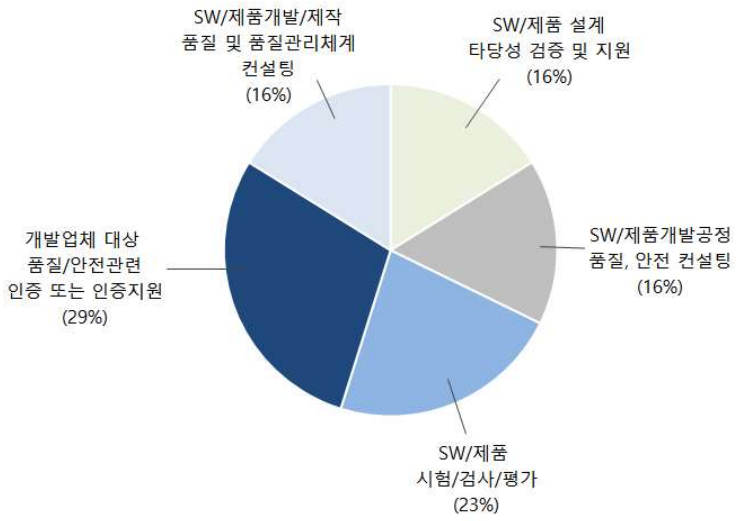
[그림 4-3] 주요 고객 산업군 분포 비중



[그림 4-4] 고객사 제공하는 서비스 및 상품의 유형



[그림 4-5] 고객사에 제공하는 서비스 및 상품의 주요 내용



4) 소프트웨어 안전 매뉴얼 혹은 도구(Tool) 보유 현황

2015년에는 산업 내에서 소프트웨어 안전에 대한 서비스가 활성화되어 있지 않은 만큼 관련 매뉴얼이나 Tool이 안전보다는 품질 측정 중심의 Tool이 대부분이었다. 하지만 2016년부터는 조사대상 기업 대부분이 소프트웨어 안전 관련 매뉴얼과 Tool을 보유하고 있는 것으로 나타났다.

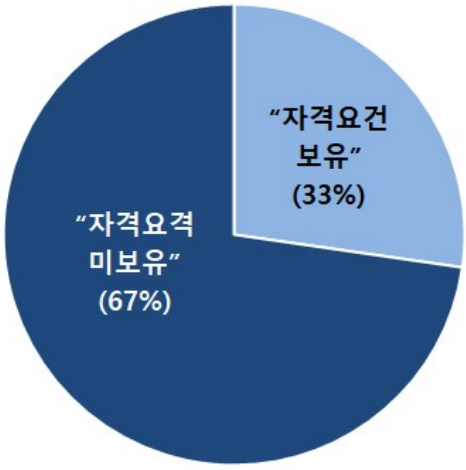
금번 조사에서는 대상 기업 모두가 소프트웨어 안전 매뉴얼 혹은 Tool을 보유하고 있다고 응답하였다. 또한 위험분석, 검증, 설계, 인증대응, 신뢰성 등 다양한 프로세스를 포괄할 수 있는 표준 매뉴얼 혹은 Tool이 활용되고 있으며 고객사별 요구사항에 따라 매뉴얼 커스터마이징(Customizing)을 통해 제공하고 있었다. 도구의 종류에는 안전 컨설팅을 주로 하는 기업의 경우는 시스템 안전 분석 툴, 소프트웨어 안전 분석 툴, 소프트웨어 역공학 툴, 전사적 프로젝트/프로세스 관리 툴 등이 있었다. 시험을 위한 도구로는 코딩 규칙 검증, 코드 기반 시험도구 도구, 오류 삽입 검증 도구 등이 있었다. 특이하게 위험분석을 위한 부품신뢰성 데이터베이스를 가지고 있는 업체도 있었다.

그런데도 국제표준 요구사항이 반영된 매뉴얼이나 Tool, 산업 도메인별 혹은 부품별 안전요건이 반영된 매뉴얼 등의 필요성은 지속해서 요구되고 있다.

5) 소프트웨어 검・인증 업무 수행 시 필요한 자격증이나 자격요건 여부

소프트웨어 인증/검증(또는 소프트웨어 안전) 관련 업무 수행 시 투입인력을 대상으로 필요로 하는 자격증이나 자격요건에 대해서는 33%만이 필요하다고 응답하였으며, 나머지 67%는 공식 자격증이나 자격요건이 아닌 자체적인 규정이나 프로젝트 수행경력을 통해 투입인력을 결정하고 있었다.

[그림 4-6] 소프트웨어 인증/검증 업무 수행 시 필요한 자격증이나 자격요건 유무



이는 소프트웨어 안전과 관련하여 공인 자격증이 없고 민간 기업에서 발급하는 자격증이 대부분이기 때문에 자격취득도 쉽지 않고 산업도메인별로 요구하는 소프트웨어 안전에 대한 내용이 달라 실제 해당 산업의 이해도나 프로젝트 참여경험 등 실무적 역량이 더욱 중요한 것으로 판단된다. 이러한 업계 분위기는 2015년과 2016년에 이어 금번 조사에서도 지속하고 있다.

단 인증업체에서는 자격증을 만들어 인증 사업의 타 기관의 진입을 막는 역할을 유지하는 기능으로 사용하기도 했다.

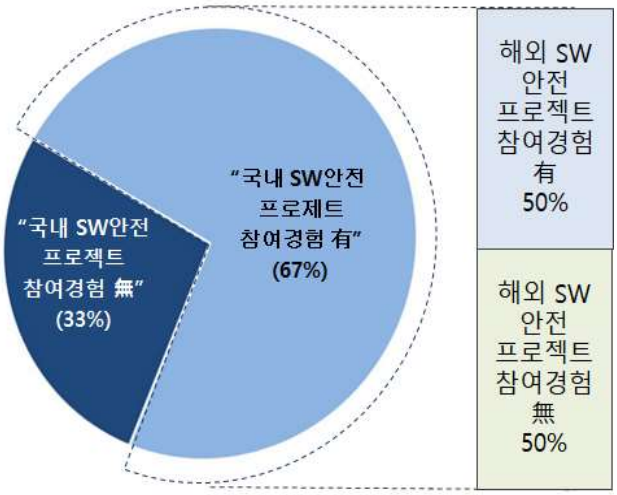
6) 소프트웨어 안전 프로젝트 참여 현황

최근 3년간 국내에서 소프트웨어 안전 프로젝트를 수행한 경험을 보유하고 있는 기업은 67%였으며, 기업별로 참여인력의 편차(최소 3명~최대 200명)가 큰 것으로 나타났다. 이 중에서 50%만이 해외 소프트웨어 안전 프로젝트 경험을 보유한 것으로 파악되어 소프트웨어 안전과 관련된 레퍼런스를 구축하는 것이 쉽지 않음을 알 수 있었다.

이러한 산업토대에 다양한 프로젝트 경험 및 레퍼런스를 보유한 해외 플레이어(Player)들의 국내진입이 활발한 만큼 국내 업체들도 다양한 산업군별로 소프트웨어

안전 프로젝트의 레퍼런스 구축이 시급한 실정이다.

[그림 4-7] 소프트웨어 안전 프로젝트 참여 현황



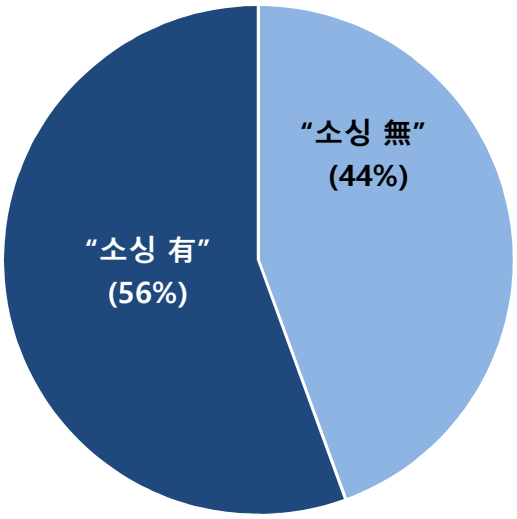
7) 해외사업자의 소싱(Sourcing) 유무

해외 선진사업자를 소싱하고 있는 기업은 56%이며, 소싱 이유로는 선진사의 레퍼런스 확보, 전문인력의 우수성, 국내외 사업의 공동수주 등이 주요한 목적이었다. 그 중에서도 국내에서는 소프트웨어 안전 프로젝트 경험을 갖춘 엔지니어를 구하기 쉽지 않아 해외사업자 소싱을 하는 경우가 많았다.

한가지 특이한 소싱이유는 컨설팅 업체의 경우는 인증이 할 수 없기 때문에, 해외 소싱을 하고 있었는데, 국내 업체의 제한점 중에 하나가 아직은 소프트웨어 인증에 대해서는 사업 영역 개척을 못하고 있다는 점이다.

또한 대부분의 기업들은 소프트웨어 안전 선진기업과의 기술 파트너쉽, 국제컨퍼런스, 대상기업 조사 등을 통해 소싱을 하고자 하는 계획을 수립 중이었다. 기술 역량 증진을 위해 유럽의 인증 전문기관 보다는 인증과 더불어 실제 도메인에서 관련 작업을 수십 년 이상 한 업체들을 가능한 소싱하여 그 노하우를 전수 받으려는 기업도 있었다. 해외 기업과의 활동은 프로젝트 별로 하는 계약을 하는 기업도 있었으며, 전략적 제휴를 통한 기술역량을 강화하는 기업도 있었다. 글로벌 업체의 국내 지사의 경우는 각 국가별로 프로젝트 특성에 따라 국가 간 리소스를 공유하기도 했다.

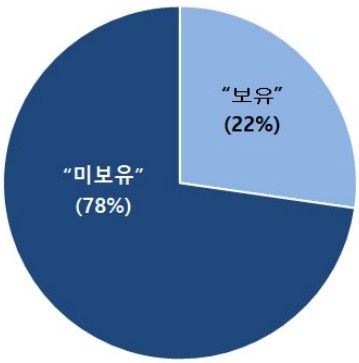
[그림 4-8] 해외사업자의 브랜드/인력/노하우 소싱 유무



8) 소프트웨어 안전 인증/검증관련 특허보유 현황

소프트웨어 인증/검증과 관련된 특허를 보유한 기업은 22%에 불과하다. 소프트웨어 안전은 특허나 정형적인 매커니즘보다는 시스템의 특성, 운영환경, 사용자 등에 따른 기술역량이 상이하여 특허로 해당 기업의 기술력을 평가하는 것은 무리가 있다고 보인다. 실제로 조사기업 중 매출기준 Top3 기업의 특허보유 현황은 '0' 건으로 시장 영향력과 기술력이 반드시 특허의 보유와 비례하지 않음을 알 수 있었다. 단, 도구를 개발하는 업체의 경우는 도구 관련 기술 특허를 가지고 있는 업체도 있었다.

[그림 4-9] 소프트웨어 안전/검증관련 특허 보유현황



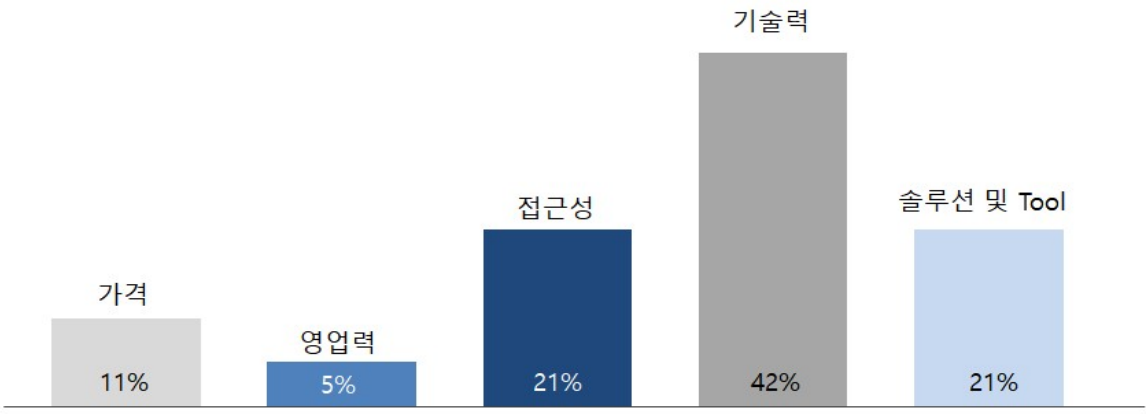
9) 경쟁사 대비 경쟁우위

선진기업 혹은 국내 경쟁사 대비 강점 혹은 경쟁우위에 대해 가장 많은 기업이 기술력(42%)이라고 응답했으며, 접근성(21%), 솔루션 및 Tool(21%), 가격(11%), 영업력(5%)로 조사되어 기업별로 자사의 기술력 수준이 높다고 평가하였다.

소프트웨어 품질 및 안전관련 사업을 영위하는 국내 기업들은 오랫동안 해당 분야에서 역량을 구축하여온 만큼 2015년과 2016년의 조사결과와 마찬가지로 프로세스 관리 및 관련 도구 활용에 강점을 보유하고 있다고 자부하였다.

하지만 향후 선진기업 수준의 경쟁력을 확보하기 위해 보완이 필요한 역량에 대해서는 56%의 기업이 해당 분야 전문인력의 확보 및 양성에 대해 중요성을 강조하였다. 기술 역량 부분에서 지속적으로 강화해야 하는 부분을 도메인 지식의 축적이라 하여, 소프트웨어 안전을 위해서는 소프트웨어 안전 매커니즘에 관한 기술도 중요하나, 관련 도메인 기술이 필수적임을 확인할 수 있었다.

[그림 4-10] 경쟁사 대비 경쟁우위



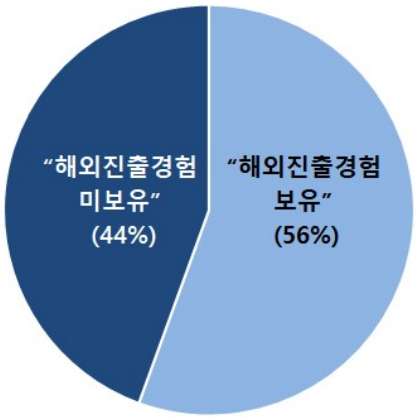
10) 소프트웨어 안전관련 사업의 해외진출 경험

소프트웨어 안전과 관련하여 국내기업이 해외로 진출한 경험은 조사대상 기업의 절반을 다소 웃도는 수준인 56%로 조사되었다.

소프트웨어 안전관련 사업의 해외진출 국가로는 중국이 가장 많은 비중을 차지하였

고 미국, 인도, 일본, 요르단 등의 국가들이 그 뒤를 이었다. 또한 해외진출의 배경은 발주처의 요청이 가장 높았으며, 기업 자체적으로 적극적인 해외시장 진출 개척을 위한 목적은 단 1개 기업만이 존재하였다. 이처럼 발주처 요청에 의한 수동적인 해외진출이 대부분이고 기업 자체적인 해외 진출은 미흡한 실정이다.

[그림 4-11] 소프트웨어 안전관련 해외진출 경험

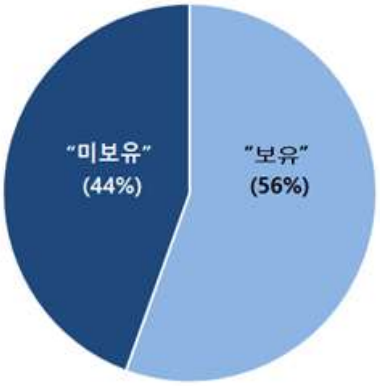


11) 소프트웨어 안전 사업관련 해외진출 계획 유무

소프트웨어 안전 사업과 관련하여 해외로 진출하기 위한 계획을 수립 중인 기업은 56%로 나타나 해외시장에 대한 관심이 높은 것으로 판단된다. 이는 2015년에는 약 60%의 기업이 2016년에는 57%의 기업이 해외 진출을 계획 중인 것으로 파악되어 해외 시장 진출에 대한 기업들의 노력은 꾸준히 지속하고 있는 것으로 보인다.

주로 일본, 중국, 동남아 지역에 진출을 준비 중이며, 도구판매와 컨설팅 서비스를 제공할 예정이다. 이러한 해외진출을 위해 필요한 역량으로는 현지언어로 의사소통이 가능한 엔지니어 확보를 가장 많이 언급하였으며, 국제표준의 요구사항 이해, 소프트웨어 설계경험 등도 제시되었다. 또한 해외진출을 위해 해외인허가 제도 조사, 제품의 현지화 및 판매망 확보, 현지인 채용 등을 준비 중이다. 그 때문에 기술기반 외국어능력, 소프트웨어 설계경험, 국제표준 이해능력 등의 역량이 있어야 하는 것으로 조사되었다.

[그림 4-12] 소프트웨어 안전관련 해외진출 계획 유무



3. 소프트웨어 안전프로세스 현황

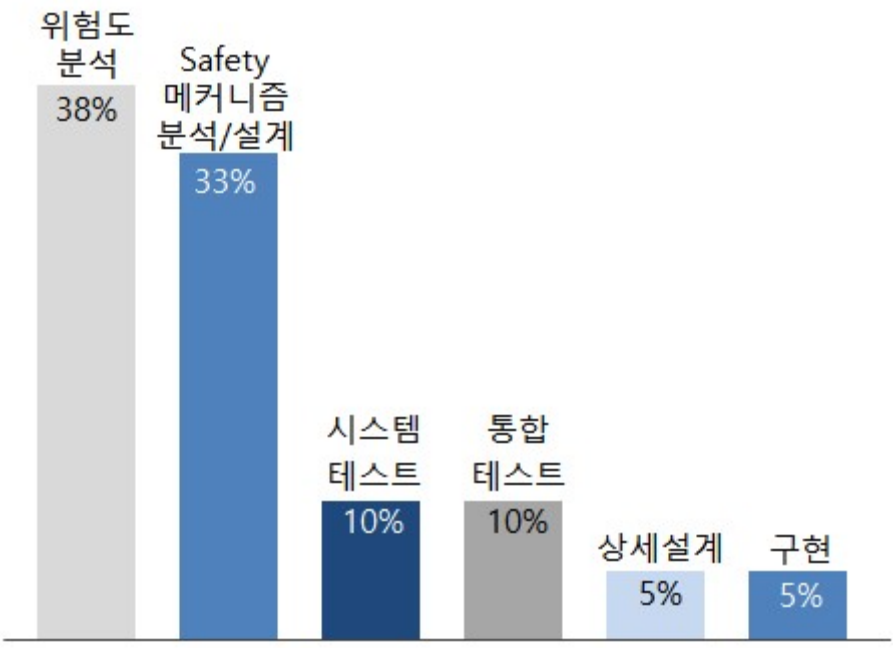
1) 소프트웨어 안전프로세스의 주요 활동

소프트웨어 품질, 테스트, 인증 등 소프트웨어 안전 프로세스관점에서 가장 중요한 활동이 2016년 조사에서는 통합 테스트(22%), 위험도 분석(15%), Safety 메커니즘 분석/설계(14%), 상세 설계(14%), 시스템 테스트(14%), 구현(14%), 기타(7%)로 나타났다.

이번 조사에서는 위험도 분석(38%), Safety 매커니즘 분석/설계(33%), 통합 테스트(10%), 시스템 테스트(10%), 상세설계(5%), 구현(5%)로 나타났다.

이처럼 품질관리차원의 통합테스트에서 안전 및 품질예방 차원의 위험도 분석으로 중요도가 바뀐 것은 소프트웨어 안전을 확보하기 위해서는 제품 제작을 위한 각 모듈 및 반제품에 탑재된 소프트웨어들이 통합되었을 때를 가정하여 수행하는 통합 테스트보다 초기 시스템 엔지니어링 단계에서부터 이양되는 Hazard/Risk 요소로부터 다양한 안전 요구사항을 개발하는 것이 중요하다는 인식이 확산되었기 때문으로 파악된다. 위험도 분석에서 가장 중요한 지식 중의 하나가 도메인 지식이라는 조사결과가 있어, 안전 확보를 위해서는 지속적으로 도메인 지식과 소프트웨어 안전 기술을 융합하는 것이 필요하다는 분석이 나온다. 위험도 분석을 통한 안전 요구사항은 안전 매커니즘, 분석 설계에 적용되며, 안전 요구사항이 충돌이 날 때는 이를 우회할 수 있는 다른 방안이 마련되어야 한다고 조사되었다.

[그림 4-13] 소프트웨어 안전을 위한 주요 활동

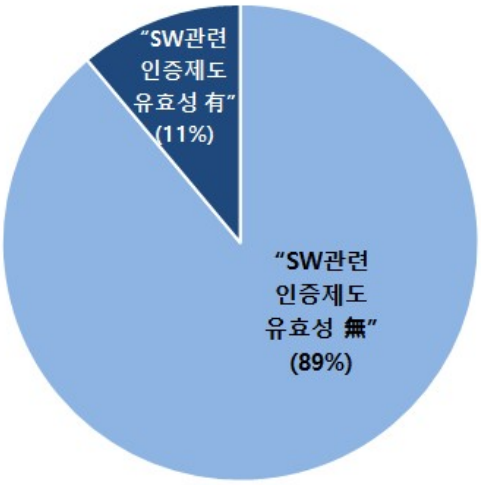


2) 소프트웨어관련 인증제도의 소프트웨어 안전성 확보 효과성 여부

현재 국내에 적용중인 소프트웨어관련 인증제도(Good Software인증, Software Process인증 등)가 소프트웨어 안전성 확보에 효과적인가에 대한 질문에 대해 대부분 '그렇지 않다(89%)'고 응답하여 현존하는 인증제도가 시장에서 실질적인 영향력을 발휘하지 못하고 있음을 알 수 있었다. 이처럼 '그렇지 않다'고 응답한 비율이 2015년과 2016년에 각각 76%와 57%였던 것에 비해 대폭 상승한 것으로 보아 인증제도만으로는 소프트웨어 안전에 대한 요구사항을 만족시키기 어렵다는 인식이 확산되고 있는 것으로 보인다.

GS인증, SP인증은 인증제도는 최소한의 안전성 보장이나 소프트웨어 역량이 부족한 신생기업이나 중소벤처기업에게는 기본적 가이드를 제공하는 기능도 있다. 하지만 기존 소프트웨어관련 인증은 본원적으로 소프트웨어 품질을 중심으로 하므로 소프트웨어 안전의 개념을 충족하기는 어려움이 있으며, 해당 인증들에는 내재적 위험원을 대응하기 위한 안전조치(Safety measure)의 설계가 반영되어 있지 않다는 한계점이 있다. 그 때문에 위험분석 결과에 따른 적합성 및 위험저감 방안 등이 요구사항과 설계에 반영되었는지를 평가하는 프로세스가 필요하다.

[그림 4-14] 소프트웨어관련 인증제도의 소프트웨어 안전성 확보 효과성 여부

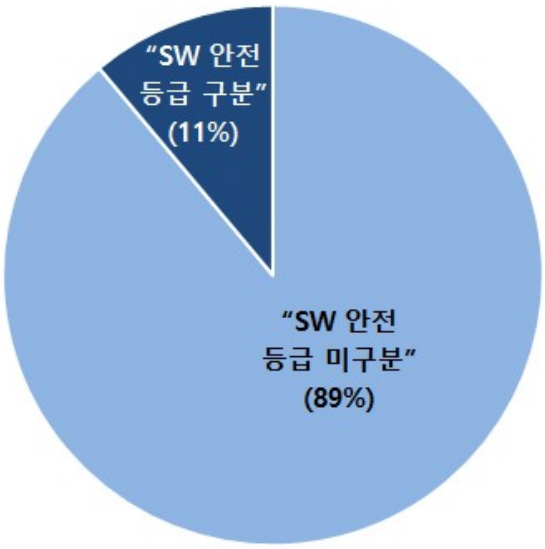


3) 소프트웨어 안전 등급/수준의 지정 및 구분 여부

소프트웨어 안전에 대한 등급/수준을 지정 혹은 구분하여 서비스를 수행하는가에 대한 질문에 89%의 기업이 등급/수준을 고객사의 요구사항에 맞춰 제공 중이라고 응답하였다. 2016년 조사에서도 86%의 기업이 '그렇다'라고 응답하여 산업별로 소프트웨어 안전 관련 등급/수준을 지정 및 구분하여 수행하는 하는 것이 일반화된 것으로 파악되었다.

산업 도메인별로 별도의 국제표준이 존재하여 각각 상이한 다른 수준을 요구하며 특히 수출기업은 국제표준에 부합하는 등급채택이 필수인 경우가 많다. 예를 들면 자동차 산업 도메인에 포함되는 기업들은 대부분 자동차위험등급(ASIL, Automotive Safety Integrity Level)의 A~D(A:안전이 별로 중요하지 않은 레벨, B/C:안전이 중요한 레벨, D:안전이 가장 중요한 레벨) 전체단계를 준수하고 있었다. 철도나 항공 등도 각 도메인의 안전 표준에 맞는 안전 무결성 등급을 설정하고, 그에 따라 제품에 대한 컨설팅 서비스를 진행하고 있었다.

[그림 4-15] 소프트웨어 안전 등급/수준의 지정 및 구분 여부



4. 소프트웨어 안전 산업/시장에 대한 견해

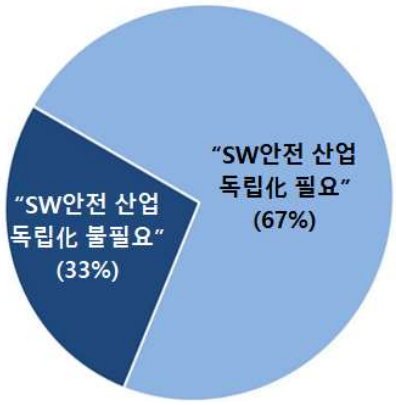
1) 소프트웨어 안전관련 산업의 독립적 산업化 필요성

소프트웨어 안전관련 산업이 독립적인 산업으로 존재하여야 하는가에 대한 질문에는 67%의 기업이 필요하다고 응답하였으며, 현재는 산업초기 수준으로 최소 5년 이상 성숙하여야 독립된 산업으로 형성이 가능할 것이라는 의견이 대부분이었다.

소프트웨어 안전산업이 독립적으로 존재하여야 하는 이유로는 기존 소프트웨어산업과 기술적으로 다르고 해당 산업분야별로 소프트웨어 안전 전문가를 보유하기가 어렵기 때문이다. 이러한 소프트웨어 안전산업이 독립적인 산업으로 형성되기 위해서는 우선적으로 소프트웨어 안전 산업이 정의되어야 하며, 산업별 안전제도의 법제도 구체화, 안전성관리 시스템 의무화, 안전관련 시스템 개발 시 안전 표준준수 및 평가 반영, 안전사고 원인분석 및 재발방지를 위한 대책 등이 필요할 것으로 조사되었다.

안전관련 산업이 독립적일 필요가 없다는 기업은 소프트웨어안전을 다른 분야와 구분하여 수행이 어려워 안전 활동, 안전 전문가의 별도 관리가 안되기 때문이라고 대답했다. 결국 소프트웨어 안전을 독립적 산업으로 분리하는 것에 찬성하거나 반대하는 의견의 내는 양측이 소프트웨어 안전 수행에 대한 어려움을 토로하고 있었으며, 이 어려움은 소프트웨어 안전 관련 전문가의 양성과 보유에서 기인하는 것으로 파악하였다.

[그림 4-16] 소프트웨어 안전관련 산업의 독립적 산업化 필요성 여부

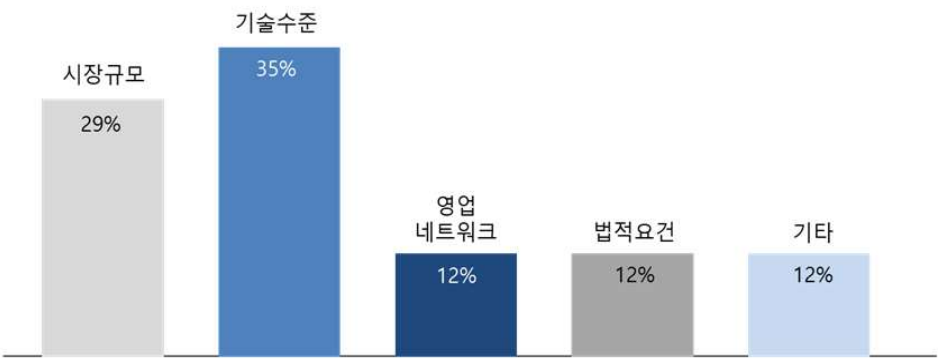


2) 소프트웨어 안전관련 분야의 진입장벽

소프트웨어 안전관련 분야의 진입장벽으로는 품질/테스트/인증 등 SW안전관련 필요 기술수준이라고 응답한 비율이 35%로 가장 높았고 작은 시장규모(29%), 영업네트워크(12%), 법적요건(12%), 기타(12%) 등으로 조사되어 기술적 역량이 가장 중요한 산업분야임을 알 수 있었다. 또한 기타에는 '인식전환'을 진입장벽이라고 응답한 비율이 높았다.

현재는 국내 소프트웨어 안전관련 산업/시장은 기술 요구수준이 높은 반면 시장 규모가 크지 않아 사업 참여자에게 매력도가 낮은 분야로 판단된다. 그러나 제4차 산업혁명에 따라 소프트웨어가 자동차, 철도, 로봇 등의 안전관련 산업의 하드웨어를 제어하게 됨에 따라 소프트웨어 안전이 중요해지고, 소프트웨어 안전 시장은 확대될 것으로 예측하였다.

[그림 4-17] 소프트웨어 안전관련 분야의 진입장벽



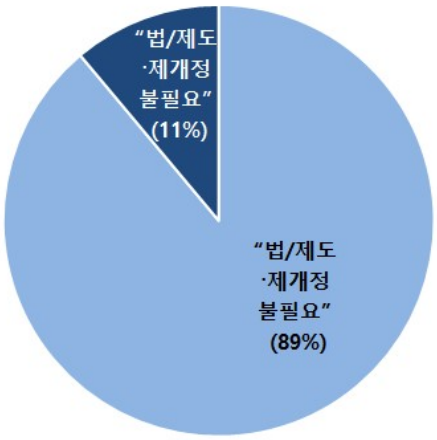
5. 소프트웨어 안전 인프라 현황 및 요구사항

1) 소프트웨어 안전관련 법·제도 제·개정 필요성

현재 영위하고 있는 비즈니스가 강화되기 위해 소프트안전관련 법·제도의 제·개정이 필요한지에 대한 질문에 대부분이 '그렇다(89%)'라고 응답하였다. 2016년 조사에서도 비슷한 수준인 86%가 법·제도 제정 및 변경의 필요성에 동의한 만큼 법·제도의 개선이 아직도 미흡한 것으로 판단된다.

이러한 법·제도의 제·개정 시 필요한 사항으로는 산업별 소프트웨어 안전관련 법제도 구체화, 소프트웨어 안전관련 전문기관 신설, 소프트웨어 신뢰성/보안성 가이드 준수에 대한 철저한 관리·감독, 운영기관/운영사의 안전성 요구사항에 대한 준수 규정, 소프트웨어 안전 확보를 검증할 수 있는 정부 자체적인 소프트웨어 안전 전문인력 확보, 사고관리체계 마련 등이 제시되었다.

[그림 4-18] 소프트웨어 안전관련 법/제도 제·개정 필요성



2) 소프트웨어 안전관련 전문가 수급 현황

소프트웨어 안전과 관련하여 다양한 산업분야별 수요가 있으나 해당 분야의 전문성을 갖춘 전문가를 찾기가 매우 어렵다는 것이 공통적인 의견이었다. 또한 전문가 분야를 세부적으로 구분한다면 위험분석가의 확보 및 양성이 가장 시급하였고 이어 개발자, 안전검증자, 안전관리자의 순으로 파악되었다.

<표 4-7> 소프트웨어 안전관련 전문가 필요순위

분류	업무 내용	우선순위
위험분석가	시스템 전반 또는 하드웨어나 소프트웨어의 요구사항에 대해 성능, 물리적 특성, 환경조건 등을 고려하여 위험원을 분석(hazard analysis)하고 위험 정도를 평가	1
개발자	안전관련 활동에 대한 이해가 높고, 기능안전 개발에 대한 지식・경험이 있는 소프트웨어개발자	2
안전검증자	소프트웨어 프로세스와 개발된 소프트웨어가 할당된 안전무결성수준(SIL)을 포함하여 표준의 요구사항에 부합하는지를 평가	3
안전관리자	개발 산출물 작성부터 형상관리, 안전기능 추적성 확보, 시스템 운영 기록 확보 등 시스템 개발 시 안전 프로세스를 관리	4

안전 전문가 양성을 위해서는 역할별로 교육제도, 운영제도, 인증제도 등을 포괄적으로 운영하며, 교육, 운영, 인증의 선순환 고리를 만드는 것이 중요하다고 조사되었다. 또한 체계적인 교육을 위한 전문 교육기관, 대학, 기업이 연계하여 교육 프로그램을 개발하고 개설해야 한다고 조사되었다.

3) 소프트웨어 안전산업의 활성화를 위한 정부차원 지원 요구사항

소프트웨어 안전산업의 활성화를 위해 정부 차원에서 법・제도 정비 및 상세화, 전문인력의 양성, 시장의 확대 등이 필요한 것으로 조사되었다.

<표 4-8> 소프트웨어 안전산업 활성화를 위한 정부차원 요구사항

구분	내용
법・제도	• 소프트웨어 안전규제 강화 • 소프트웨어 안전관련 법・제도 구체화 • 사전/사후 안전 피드백 체계 수립 • 소프트웨어 안전 총괄 전문기관 신설 • 소프트웨어 안전 확보를 위한 개발비용 및 인건비 산정 현실화 • 공공시스템의 안전표준 준수 및 평가 제도화 • 산업별 안전성 관리 시스템 도입 의무화
인력	• 도메인별 안전 분석가 양성 • 소프트웨어 개발자 재교육 • 소프트웨어 안전 전문가 양성 및 처우 개선 • 소프트웨어 안전관련 자격증 신설 • 소프트웨어 안전관련 교육과정 운영 • 운영기관/운영사의 소프트웨어 안전 관리자 지정 • 정부 조직 내 소프트웨어 안전 관련 전문가 확보
시장	• 외산 안전분석 Tool의 국산화 및 국산 Tool의 해외수출 지원 • 소프트웨어 안전관련 인식 제고 • 기업의 소프트웨어 안전 산업 투자유도 • 중소기업 소프트웨어 안전 기술 향상 지원 • 산업별 신기술에 대한 안전과 보안 지식 습득 • 국내 소프트웨어 안전산업의 보호 • 인증/컨설팅 산업의 지원

6. 요약

본 절에서는 소프트웨어 안전 전문기업을 대상으로 조사한 내용을 2015년과 2016년의 조사내용과 연계하여 법・제도, 인증/매뉴얼, 인력・교육, 조직・기관, 산업환경개선, 프로세스로 구분하여 다음과 같은 시사점을 도출하였다.

시사점 도출에 앞서 2016년 대비 2018년 조사항목별로 변화된 내용을 다음 표에 정

리하였다.

<표 4-9> 2016년 대비 2018년 조사항목별 변화 내용

항목	2016	2018
소프트웨어 안전개념	• 보안(Security)관점으로 파악(50%)	• 품질(Quality)가 38%, 회피메커니즘이 38%, 보안(Security)가 24%로 정확한 인식이 확산
고객 산업군 분포	• 자동차, 철도 등 주요 산업분야의 비율이 높았으나 전산업에 고른 분포 경향	• 여전히 주요 산업에 비율이 높았으나 emerging(빅데이터, 인공지능 등)산업분야 등 고객군 다양화 추이
제공 서비스 및 상품유형	• 도구 기반의 품질, 안전 서비스가 가장 높음	• 서비스 및 상품이 특정 분야에 치우침 없이 고르게 분포

법·제도 측면에서는 소프트웨어 안전관련 법·제도의 제·개정에 대한 요구가 높다. 이는 2016년, 이번 조사에서 지속해서 법·제도의 제·개정에 대한 필요성을 제기하고 있으나 개선은 미흡한 것으로 판단된다. 구체적으로는 산업별 소프트웨어 안전관련 법·제도 구체화, 소프트웨어 안전 전문기관 신설, 공공부문 소프트웨어 안전성 요구사항에 대한 준수 규정 법제화 등의 요구사항이 있었다.

인증/매뉴얼 측면에서는 우선 소프트웨어 품질중심의 인증은 안전성 확보에 큰 도움이 되지 않는다는 의견이 지배적이다. 기존 인증(GS인증, SP인증)은 본원적으로 소프트웨어 품질을 중심이기 때문에 위험원 분석, 위험저감 방안 등이 요구사항과 설계에 반영되었는지 여부를 판단하는 것이 중요하다.

그리고 전체 기업이 소프트웨어 안전과 관련된 노하우와 지적자산을 체계화한 매뉴얼과 Tool을 보유하고 있다. 해당 매뉴얼 등은 대부분 소프트웨어 안전 전체 프로세스를 대상으로 하며 고객사별 요구사항에 따라 커스터마이징을 통해 활용하고 있다.

인력·교육 측면에서는 소프트웨어 안전분야 전반에 걸쳐 산업별/국가별 실무 경험을 갖춘 전문가가 부족하다. 소프트웨어 안전분야 전문가에 대한 수요는 높은 편이지만 산업 도메인별 지식기반의 전문가를 찾기가 어려운 실정으로 정부차원에서 소프트웨어 개발자 재교육, 전문 프로그램 운영 등을 통해 전문인력을 양성해야 할 것으로

판단된다.

조직·기관 측면에서는 소프트웨어 안전관련 전문가를 보유한 전문기관의 신설이 필요하다. 소프트웨어 안전에 대해 오너십(Ownership)을 보유한 전문기관의 부재로 유사시 적절한 대응 불가하고 정부부처별로 소프트웨어 안전에 대한 이해도가 달라 소통의 어려움 존재하기 때문이다.

業 환경개선 측면에서는 분야별로 4가지 시사점을 도출하였다. 첫째, 다양한 산업 도메인에 대한 노하우 축적 및 레퍼런스 확보가 향후 중요한 경쟁요소가 될 것이다. 둘째, 국내 소프트웨어 안전관련 시장은 기술요구수준 대비 시장 규모가 크지 않아 시장 매력도가 부족하다. 셋째, 해외시장 진출을 위해서는 국제표준, 외국어, 실무경험 등을 갖춘 전문인력이 필요하다. 넷째, 소프트웨어 안전관련 산업은 일반 소프트웨어산업과는 기술적으로 상이하고 다르고 산업분야별 전문가 확보가 어려워 독립산업化 되는 것이 타당하다.

프로세스 측면에서는 소프트웨어 안전 프로세스에서 사전 위험분석의 중요성이 증대되었다는 것이다. 소프트웨어 안전 프로세스 중 가장 중요한 활동이 ‘16년에는 통합테스트였지만 ’17년에는 위험도 분석으로 나타났다. 이는 기존 QC차원의 통합테스트에서 안전 및 품질 예방 차원의 위험도 분석으로 이전되었다는 것을 의미한다.

제3절 소프트웨어 개발/사용자 (End User Sector)

1. 개요

조사 대상은 국내에 사업장이 위치하는 법인 사업자들 중 TIC 사업을 영위하는 기업들을 제외한 나머지 공기업 및 사기업을 대상으로 하였는데, 금번 조사에서는 2016년 조사 대상인 소프트웨어를 개발하는 기업에서 확장하여 소프트웨어를 사용하는 기업까지를 End User로 포함시켜 조사하였다.

지난번 조사와는 달리 전통적으로 소프트웨어 안전이 중요한 산업인 원자력, 철도, 우주항공, 의료, 도로교통, 자동차 산업을 비롯하여, 금번 조사에서는 반도체 제조, 전자제품제조, 화장품 제조, 의류제조, 농축산, 해양, 기계제조, 물류, 금융 등의 제조나 서비스의 일반 산업군까지 조사 대상 영역을 확장하였다. 단, 기존 조사에서 국방 분야 기업을 조사했었으나, 금번 조사에서는 적절한 대상 기업을 물색하지 못해 조사에

서 제외하였다.

설문은 2016년 조사에 사용한 설문을 기반으로 일부 문항에 대해 응답률을 높일 수 있으며 유의미한 결과를 도출할 수 있도록 개정하였고, 이전 조사 결과 상세화 또는 변화가 기대되는 항목에 대해서는 관련한 질문을 추가하였다.

예를 들면 소프트웨어 안전에 대한 개념을 묻는 질문의 경우 소프트웨어 품질과 소프트웨어 안전의 범주 또는 차이점에 대해 질문하였는데, 2016년 조사에서는 소프트웨어 안전이 소프트웨어 품질의 일부 이거나, 서로 일부 같거나, 서로 완전히 다르다는 개념의 유형만을 보기로 제시한 반면, 이번 조사에서는 이러한 유형들 외에도 소프트웨어 안전과 소프트웨어 품질이 서로 같을 수도 있음을 보기에 추가로 포함시켰다.

또한 2016년의 조사가 소프트웨어가 제품/서비스에만 직접적으로 관련이 있는 기업들을 대상으로 조사하여 질문도 해당 기업들의 제품/서비스에만 국한되었던 반면, 이번 조사에서는 소프트웨어를 이용하는 제조 공정까지도 소프트웨어 안전의 관리 대상에 포함시켜 질문하였다.

또한 1:1 면담 방식으로 진행하는 경우, 응답자에게 항목 별 질문의 의도를 설명하고 응답자가 선택한 답변의 사유를 물어 최대한 그 의도를 확인하고 분석에 활용하도록 하였다.

<표 4-10> End User 대상 질문 내역

영역	질문 내용	문항 구성
소프트웨어 안전 개요	• 소프트웨어 안전 개념 및 범주 • 소프트웨어 안전 관련 보유 국제인증, 조직, 인원 등	• 7개 문항 • 9개 세부 문항
소프트웨어 안전 예방점검 활동	• 소프트웨어관련 안전사고 방지를 위한 기업 내/외 활동 및 이를 위해 지출하는 비용 규모 등	• 9개 문항 • 3개 세부 문항
소프트웨어 안전 대응관리 활동	• 사고 대응체계 보유 여부 및 관련한 소프트웨어측면 대응체계 현황 • 소프트웨어 기인 사고사례 정보 수집 및 활용 현황	• 7개 문항 • 5개 세부 문항

소프트웨어 안전에 대한 정책 요구사항	• 소프트웨어 안전 관련 정부지원 현황 • 정부에 지원을 요청하는 사항	• 3개 문항 • 3개 세부 문항

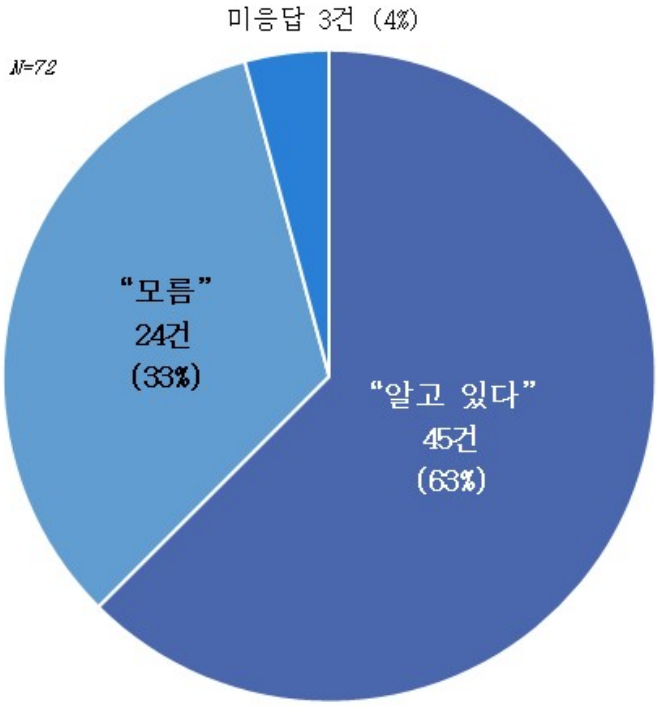
2. 소프트웨어 안전 개요

1) 소프트웨어 안전 개념의 인식

소프트웨어 안전의 개념을 알고 있었는지 묻는 질문에 대해 응답자 72명 중 60% 이상인 45명의 응답자가 본 설문 이전부터 ‘알고 있다’라고 응답하였다. ‘알고 있다’고 응답한 응답자의 특성을 살펴보면, 이들이 종사하는 산업은 자동차 제조업, 자동차 부품 제조업, 소프트웨어개발 또는 시스템 구축 사업, 발전 등 에너지 생산 또는 에너지 관련 플랜트 구축 사업, 전자제품 제조업 등이었고, 대부분 기업 자체적으로 소프트웨어를 연구하고 있거나 소프트웨어 자체가 제품이라서, 또는 소프트웨어가 기업의 생산과정 또는 결과물(제품)에 중대한 역할을 하거나 영향을 미치기 때문에 본 설문 이전부터 소프트웨어 안전에 대해 들어봤거나 개념을 알고 있었다고 응답하였다.

‘모른다’라고 대답한 응답자는 응답하지 않은 3명을 제외한, 72명 중 약30%인 24명이었다. ‘모른다’고 응답한 응답자 특성은 심층 인터뷰를 통해 크게 3가지로 확인되었다. 먼저 응답자들이 속한 기업들 중 일부 기업들은 소프트웨어개발이 필요한 경우 외부 협력사에 위탁을 맡기는 것이 일반적으로, 기업 내부에 소프트웨어개발 및 관리에 대한 역량이 부족한 경우가 많았고, 일부 기업들은 업력이 오래된 제조업체들로 한번 설비 투자하면 대부분 10년 이상 사용하거나, 최근 경기 부진으로 새로운 설비를 구입한 경험이 없고, 과거부터 보유한 설비 대부분이 기능에 소프트웨어가 기여하는 정도가 작아 소프트웨어 안전이 제조 및 생산에 직접적인 관련이 적은 관계로 소프트웨어 안전 개념에 대해 잘 모른다고 답변하였다. 또 다른 일부 기업들은 대기업 군으로, 회사 규모가 클수록 조직과 직무가 세분화되는 관계로, 본인이 소프트웨어 안전 또는 관련된 인증을 담당하는 실무자가 아닌 경우 잘 모른다는 답변을 하는 경향이 있었다.

[그림 4-19] 소프트웨어 안전에 대한 개념 인식

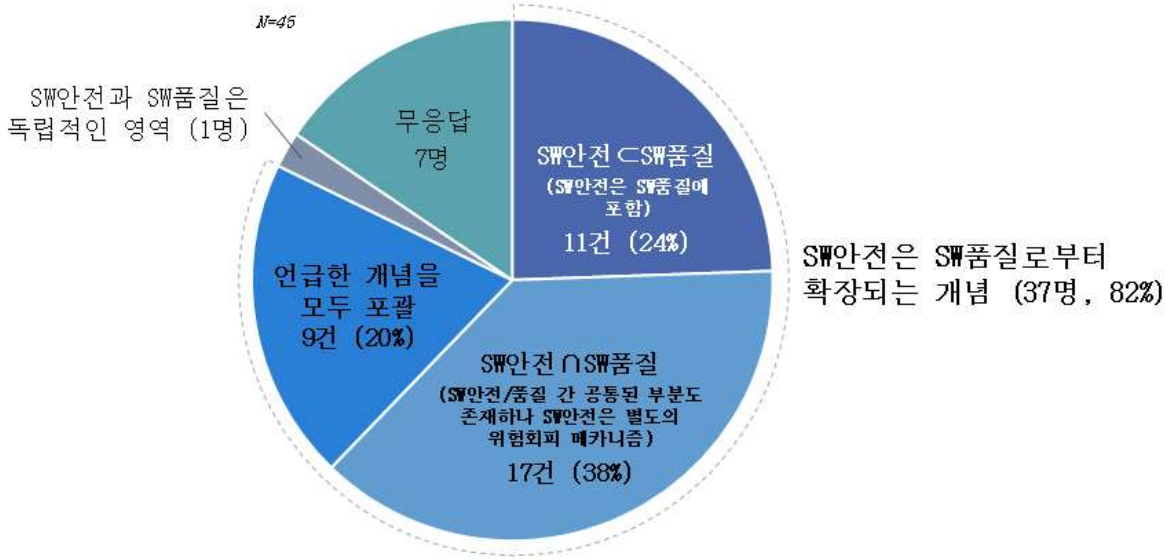


2) 소프트웨어 안전 범주에 대한 견해

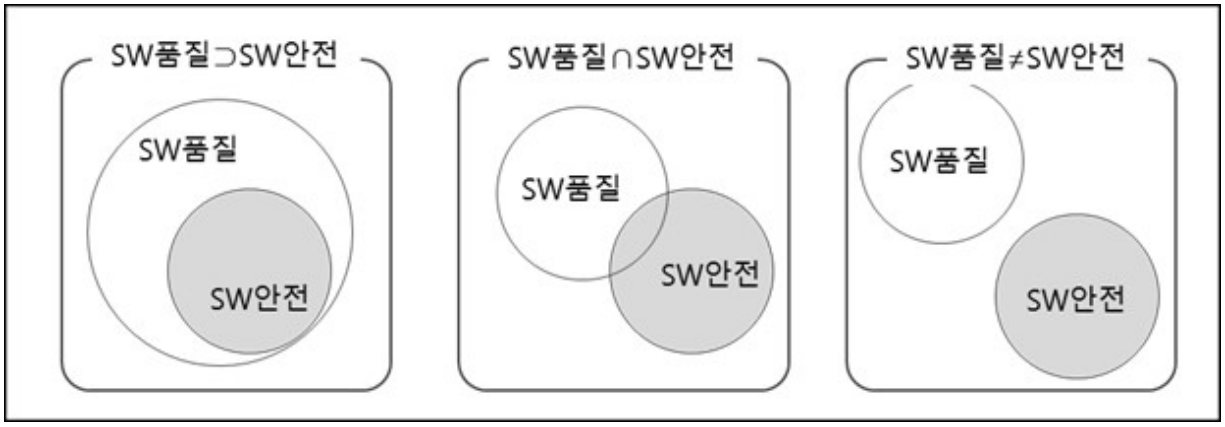
소프트웨어 안전에 대해 사전 인지하고 있는 응답자들에 한하여, 소프트웨어 안전의 범주에 대해 질문하였다. 전반적으로는 80% 이상의 대다수의 응답자들이 소프트웨어 안전은 소프트웨어 품질로부터 파생/확장되는 개념이라고 보았으며, 가장 많은 응답자들이 소프트웨어 안전/품질 간 공통된 부분도 존재하나 소프트웨어 안전은 별도의 위험회피 메카니즘이라고 답하여 이제는 어느 정도 소프트웨어 안전이 소프트웨어 품질 개념으로부터 독립하여 독자적인 영역을 구축하고 있다고 보인다.

이전 조사와 비교하면, 2015년도의 조사에서는 주로 소프트웨어 안전은 소프트웨어 품질과 동일한 개념 또는 소프트웨어 안전은 소프트웨어 품질과 확연히 구분되는 개념이라는 의견이 대다수였고, 2016년도의 조사에서는 주로 소프트웨어 안전은 소프트웨어 품질과 공통된 부분도 존재하나 사람 생명에 직/간접적으로 연관되어야 한다는 의견이 다수 있었는데, 본 2018년도 조사에서는 소프트웨어 안전은 소프트웨어 품질로부터 발전하여 독립 영역을 형성해 가는 중이라는 의견이 다수였다.

[그림 4-20] 소프트웨어의 범주에 대한 견해



[그림 4-21] 소프트웨어 품질과 안전의 관계



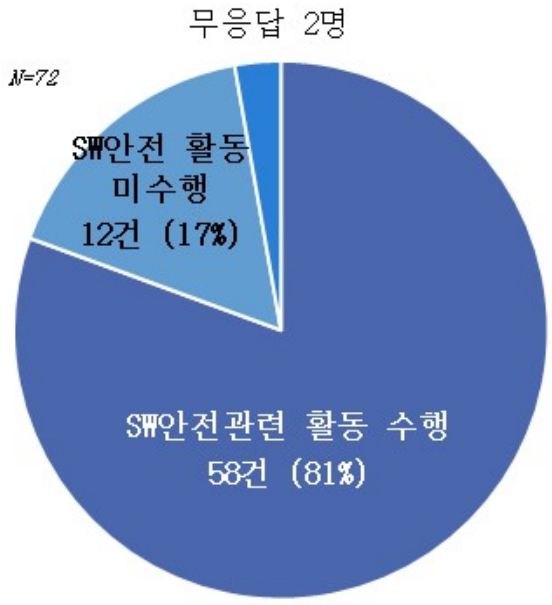
3) 소프트웨어 안전 활동 수행 사유

본 조사는 기존 소프트웨어 안전이 기업의 생산/서비스와 직결되는 산업군(철도, 원자력, 에너지 등) 외 타 산업군의 기업 실무자도 포함하여 조사하였기에, 설문 대상자가 속한 기업 중 소프트웨어 안전과 관련한 활동을 수행하는지 먼저 확인하였다. 또한 이전 질문의 응답 중 소프트웨어 안전 영역은 응답자 본인의 업무가 아닌 경우가 다수 확인되었는데, 이러한 경우 응답자가 본인의 업무/직무에 대해서만 응답하여 결과가 제한적일 수 있어서 본인 업무 외 타 조직 포함하여 기업 전체 사업, 운영 활동 측면의 소프트웨어 안전 활동 수행 여부에 대한 응답을 요청하였다.

전체 72명의 응답자 중 소속 기업에서 소프트웨어 안전과 관련한 활동을 하고 있다고 답한 응답자는 58명으로 전체의 81%, 소프트웨어 안전과 관련한 활동을 하고 있지 않다고 답한 응답자는 12명으로 전체의 17%로 확인되었다.

위의 소프트웨어 안전에 대해 사전에 인지하고 있는가에 대한 질문에 대해서는 사전에 그 개념을 '알고 있다'는 응답이 63%였으나, 소속 기업에서 소프트웨어 안전 활동을 하고 있는가에 대한 질문에 대해서는 '소프트웨어 안전 관련 활동을 수행하고 있다'는 의견이 81%로, 소프트웨어 안전의 개념에 대한 인식보다 기업 전반적인 소프트웨어 안전 활동 수행률이 높은 것으로 확인되었다. 이는 기업들이 과거부터 자율적/자발적으로 소프트웨어 안전 활동을 수행해오고 있었다는 것으로 해석할 수 있다.

[그림 4-22] 기업 차원의 소프트웨어 안전 활동 수행 여부



3) 소프트웨어 안전 활동 수행 사유

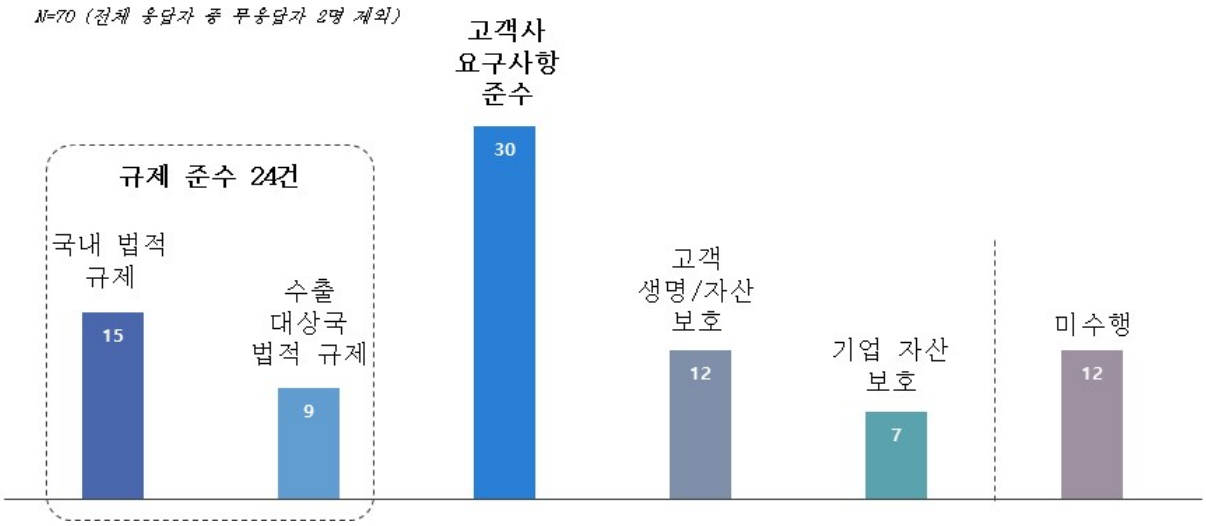
소프트웨어 안전 활동을 수행하지 않고 있다는 응답자 12명 및 미응답자 2명을 제외하고 총 58명이 소프트웨어 안전 활동을 하고 있다고 응답하였고, 그 사유에 대해 하나 이상의 응답을 하였다.

기업이 소프트웨어 안전 관련한 활동을 수행하는 사유로는 '고객사 요구사항 준수를 위해'라는 응답이 총 30건으로 가장 많았고, 그 다음으로 '국/내외 법적 규제 준

수를 위해 ‘라는 응답이 24건, ’ 고객의 생명과 자산을 보호하기 위해’ 라는 응답이 12건, ‘기업 자산을 보호하기 위해’ 라는 응답이 7건의 순서로 나타났다.

소프트웨어 안전 관련 활동을 수행하지 않는다는 기업에 대해서도 그 사유를 조사하였는데, 소프트웨어 안전 관련한 활동이 매출에 도움을 주지 않으면서 추가적인 비용을 부담해야 하기 때문에 수행하지 않는다거나, 경영진이 무관심하여 수행하지 않고 있다는 사유를 확인하였다.

[그림 4-23] 기업의 소프트웨어 안전 활동 사유 (복수 응답)



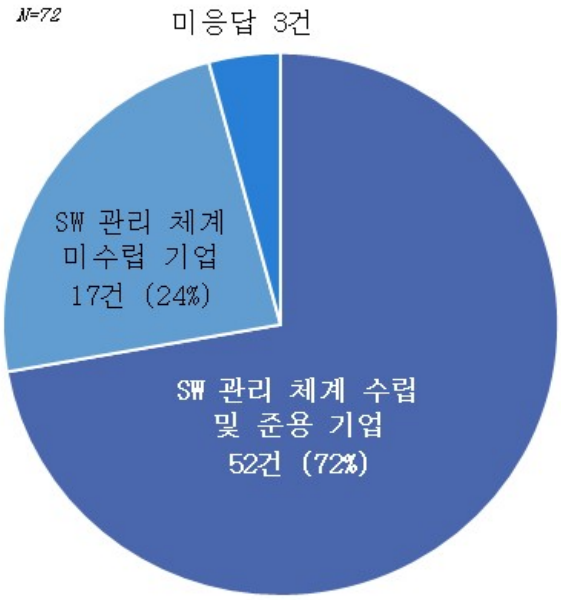
4) 소프트웨어 개발/운영/관리 규정 및 절차 보유, 준용 여부

기업 내 소프트웨어를 개발, 운영 또는 관리하는 규정과 절차를 보유하고 실제 업무에 준용하고 있는지 총 72명의 조사 대상자에게 질문하였고, 이에 52명(72%)의 응답자가 ‘소프트웨어 개발/운영/관리 규정 및 절차를 보유하고 있으며, 실제 업무에 이를 준용하고 있다’ 고 대답하였다. 이들 응답자가 속한 기업은 규모 측면에서 공기업, 대기업에서부터 중견기업, 중소기업까지 다양하게 나타나서 기업 규모와 소프트웨어 개발/운영/관리 체계 보유 여부와는 큰 차이가 없는 것으로 보이고, 산업 측면에서도 소프트웨어 개발업 및 시스템 구축업 외에도 자동차 제조업, 통신서비스업, 금융서비스업, 전자제품이나 전기, 반도체 제조업 등 거의 전 산업에 걸쳐 많은 기업들이 소프트웨어 개발/운영/관리 규정 및 절차를 수립하고 업무에 적용하는 것으로 확인하였다.

단, ‘소프트웨어 개발/운용/관리 규정 및 절차를 보유하고 있지 않거나 업무에 준용

하지 않는다 ‘라고 답한 응답자 17명(24%)이 속한 기업들은 규모와 산업 측면에서 일정한 특성을 보였는데, 우선 규모 측면에서는 주로 중견기업이나 중소기업으로 사업의 규모가 작은 기업들이 많아 이들 기업 내부적으로 일정 수준의 관리 역량을 갖추기는 인력과 예산 측면에서 부담되는 상황으로 파악되었고, 일부 대기업 계열사도 존재하였으나 이들은 모회사나 계열사에 IT서비스를 제공하거나 아웃소싱하는 Captive 사업 위주라 관리 수준을 향상시킬만한 니즈가 없는 것으로 확인되었다. 산업 측면에서는 제조업의 기업 비율이 높았는데, 이들이 생산하는 제품이나 제공 서비스의 IT의존도가 상대적으로 낮아 관리 체계를 갖춰야 할 동기부여가 미흡한 것으로 확인되었다.

[그림 4-24] 소프트웨어 개발/운영/관리 체계 보유 및 준용 여부



5) 소프트웨어 개발/운영/관리 규정 및 절차 보유 기업의 소프트웨어 안전 관리 범위

소프트웨어의 개발/운영/관리 규정과 절차를 보유하고 업무에 적용하는 기업들의 소프트웨어 측면의 안전 관리 범위를 조사한 결과, 부품/제품을 개발하거나(23건) 해당 제품을 테스트하는 과정에서 소프트웨어 상 안전을 확인/검토한다는 응답이(25건) 가장 많았다. 이는 기업의 생산 활동 또는 제품 생애주기 상 개발/테스트 같은 초기 단계에 집중적으로 소프트웨어의 안전 여부 및 그 수준을 관리하는 것으로 해석할 수 있다.

그 다음으로는 개발이 완료된 부품/제품의 인증을 획득하거나(12건) 소프트웨어에 기인한 안전사고에 대응하는(13건) 방식으로 사후적인 소프트웨어 안전을 관리한다는 응답이 많았다.

그 외 소프트웨어 안전 관리 범위를 최소화하기 위해 부품/제품을 개발하는 대신 이미 소프트웨어 안전이 검증 완료된 부품/제품을 구입하여 사용한다는 응답도 8건이 있었고, 기타 부품/제품의 소프트웨어 안전에 대해 외주 기업에 전담시키는 등의 응답도 존재하였다.

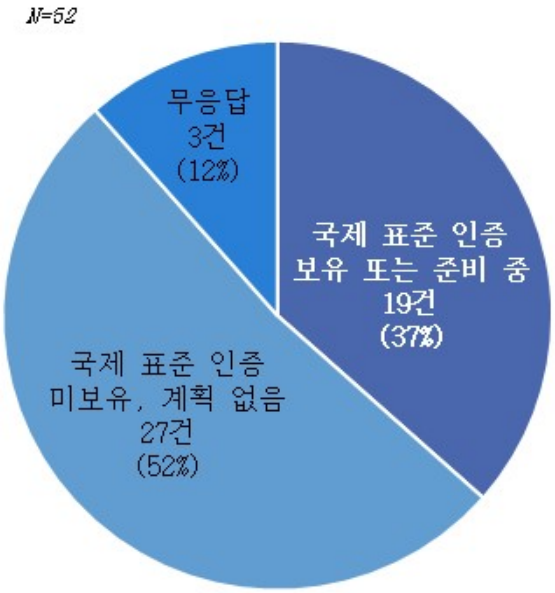
[그림 4-25] 소프트웨어 개발/운영/관리 규정 및 절차 보유 기업의 소프트웨어 안전 관리 범위 (복수 응답)

6) 소프트웨어 개발/운영/관리 규정 및 절차 보유 기업의 국제 표준 인증 확보 여부

앞서 소프트웨어 개발/운영/관리 규정과 절차를 보유하고 있다는 응답자들을 대상으로 국제 표준 인증의 확보 또는 확보 준비 중인 상황을 확인한 결과, 약 절반은 아직 국제 표준 인증을 보유하고 있지 않고 국제 표준 인증 확보 계획도 없는 것으로 확인되었고, 약 40%의 기업은 국제 표준 인증을 보유하고 있거나 확보를 준비 중인 것으로 확인되었다.

보유하거나 확보 준비 중인 인증은 산업 별로 차이가 존재하였는데, 소프트웨어를 개발하거나 시스템 구축을 주 사업으로 하는 기업들의 경우 ISO 20000, 의료기기 제조업인 경우 ISO 13458, 자동차 관련 제조업인 경우 ISO 26262를 보유하거나 확보 추진 중인 것으로 확인되었다.

[그림 4-26] 국제 표준 인증 보유 또는 확보 준비 여부

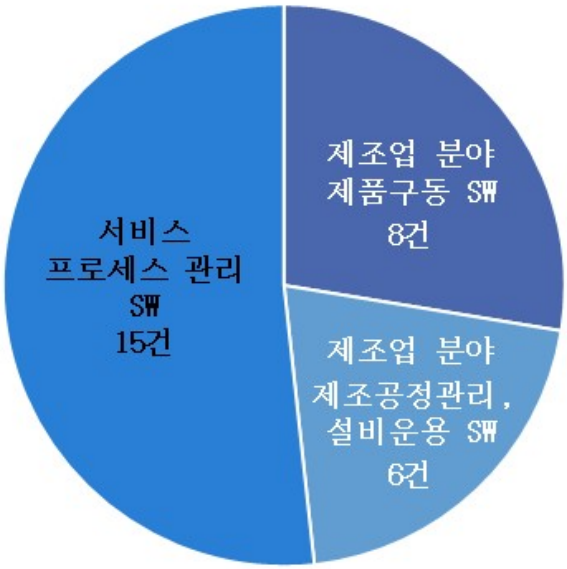


7) 소프트웨어 개발/운영/관리 규정 및 절차가 적용되는 분야

앞서 소프트웨어 개발/운영/관리 규정과 절차를 보유하고 있다는 응답자 52명을 대상으로 그러한 규정과 절차가 적용된 소프트웨어가 실제로 활용되는 분야를 질문한 결과 잘 모르거나 응답하지 않은 인원이 23명이어서 이들을 제외한 29명에게만 답변을 수집하였다.

이들이 응답한 소프트웨어 개발/운영/관리 규정 및 절차의 적용 분야는 금융산업, 정보통신 서비스업 등 주로 서비스업은 프로세스 관리 소프트웨어(15건), 의료기기 제조, 항공부품 제조, 자동차 제조 등의 제조업은 제품 구동 소프트웨어(8건), 에너지 생산, 반도체 제조 등의 제조업은 제조 공정관리 또는 설비운용 소프트웨어(6건) 영역이었다.

[그림 4-27] 소프트웨어 개발/운영/관리 규정 및 절차 적용 분야



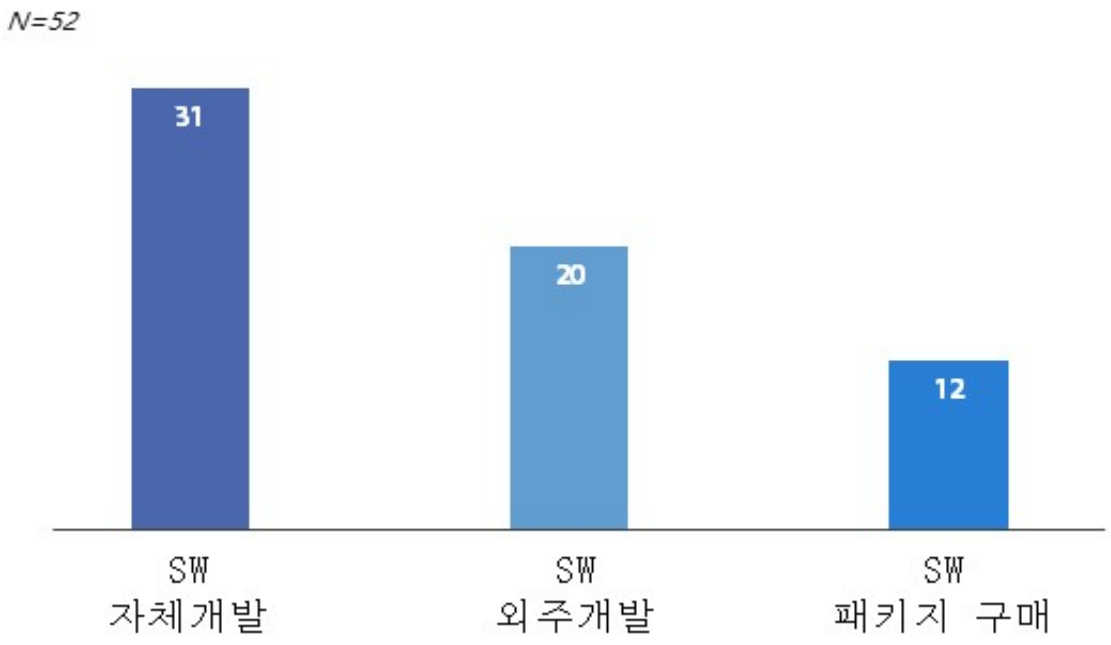
8) 소프트웨어 개발/운영/관리 규정 및 절차 보유 기업의 소프트웨어 조달 방식

소프트웨어 개발/운영/관리 규정과 절차를 보유한 기업이 실제로 업무 프로세스 용도 또는 부품/제품에 장착되는 소프트웨어는 어떻게 조달하고 있는지 확인하였다.(52명 대상) 기업의 소프트웨어 조달 방식은 한가지만이 아니라 다양한 방식으로 조달할 수 있기에 현재 소프트웨어를 조달하고 있는 모든 방식에 대해 조사하였고, 그 결과 가장 많이 이용하는 방법은 소프트웨어를 사내에서 자체 개발하는 방식으로 확인되었다.(31건) 이 경우 그 소프트웨어가 사업이나 제품에 있어서 매우 중요한 역할을 하는, 소위 'Mission Critical Software'이기 때문에 기업의 지적 자산 차원에서 외부로부터 조달하는 것은 지양하고 내부 역량 중심으로 소프트웨어를 조달한다는 특징이 있었다.

그 다음으로 많이 사용하는 방식은 소프트웨어를 외주 개발하는 방식이었다.(20건) 주로 'Business Support Software' 라고 불리는데, 상기의 'Mission Critical Software' 보다는 중요도가 낮지만 기업을 운영하는데 있어 고객 정보를 비롯한 거래 정보 수집과 처리에 필수적인 소프트웨어로, 응답자들의 대부분은 지적 자산의 대상으로는 고려하지 않아 외부에서 조달하여도 문제가 없다고 생각하나, 각 기업별 사업 특성, 경영철학, 시장에 대한 관점, 내부 정책이 서로 달라 상용 소프트웨어를 이용하기는 어려운 경우가 많기 때문에 외부 업체와 계약을 맺고 개발을 의뢰하여 조달한다고 한다.

소프트웨어 패키지를 구매하여 사용한다는 응답이 가장 적었으나(12건), 해당 소프트웨어 종류가 회계 등의 전사자원관리(ERP), 정보계(BI/DW)와 같이 업무가 정형화되어 있거나 단순 기능 중심의 소프트웨어들인 관계로 사업 환경이나 내부 정책 등의 변화와 크게 무관하여 한번 도입하면 오래 사용할 수 있기 때문에 응답 빈도가 낮았던 것으로 판단된다. 또한 이러한 사유로 굳이 별도의 인력과 시간을 들여 개발하기보다는 경제성 측면에서 사용 소프트웨어 패키지를 구매하여 사용하고 있었다.

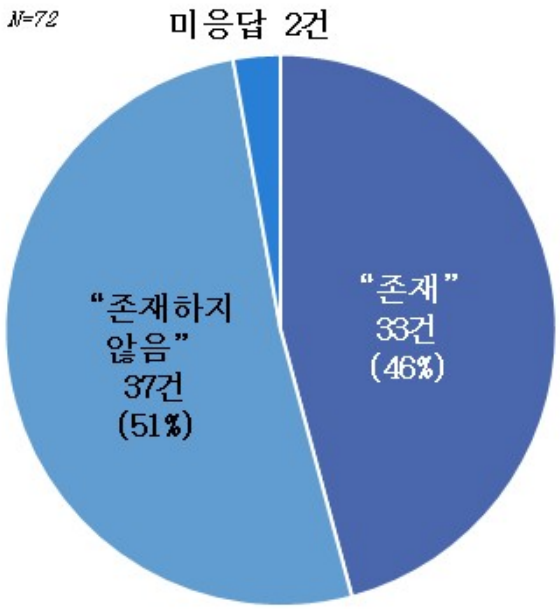
[그림 4-28] 소프트웨어 개발/운영/관리 규정 및 절차 보유 기업의 소프트웨어 조달 방식



9) 기업 내 소프트웨어 안전 담당 부서 또는 담당자 존재 여부

기업 내 소프트웨어 안전을 담당하는 부서가 별도로 존재하는지, 또는 전담 조직이 없다면 담당자가 지정되어 있는지에 대한 질문에 대해서는 총 응답자 72명 중 절반 이상인 37명이(51%) ‘조직/담당자가 존재하지 않는다’ 고 답했고, ‘존재한다’ 라고 답한 응답자도 33명(46%)에 달해 큰 차이가 없었고, 응답자 유형을 살펴보면 계열사 관계인 기업들 간에도 모회사 응답자는 ‘존재하지 않는다’ 고 답한 반면, 자회사 응답자는 ‘존재한다’ 고 답하거나 같은 산업군임에도 A 기업 응답자는 ‘존재한다’ 고 답한 반면, B기업 응답자는 ‘존재하지 않는다’ 라고 답해 일정한 동향이나 규칙성을 찾기는 어려웠다. 이는 일반적으로 직무에 대한 조직과 담당자 지정 여부는 기업의 경영 환경 또는 조직 철학에 결정되는 데 기인한 것으로 판단된다.

[그림 4-29] 기업 내 소프트웨어 안전 담당 부서 또는 담당자 존재 여부



10) 기업 내 소프트웨어 안전 담당 부서 또는 담당자 지정 현황

위 설문의 응답자를 대상으로 조직명 및 인원 현황을 조사한 결과, 제조업과 서비스업이 유의미한 차이를 보였다. 서비스업의 경우 기업의 규모와는 크게 상관없이 정보통신업 사업자이면서 소프트웨어 개발 또는 시스템 구축 사업을 하는 사업부서의 소규모 조직으로 소프트웨어 안전을 담당하는 조직을 두고 수명 내외 규모로 운영하고 있었으며, 예외적으로 수십명 단위의 별도 사업부로 운영하는 기업도 간혹 존재하였다.

제조업의 경우에는 대기업일수록 소프트웨어 안전 관련한 조직의 규모가 컸는데 어떤 전자제품 제조기업의 경우에는 사업부 수준으로 200명 이상 규모로 운영 중인 경우도 있었고 일반적인 제조업인 경우에도 최소 10명 이상의 조직을 운영 중이었다. 또한 이들 조직은 소프트웨어 안전이 주업무는 아니고, 제품의 품질을 관리하는 QC(Quality Control) 관련된 조직이 대부분이었다.

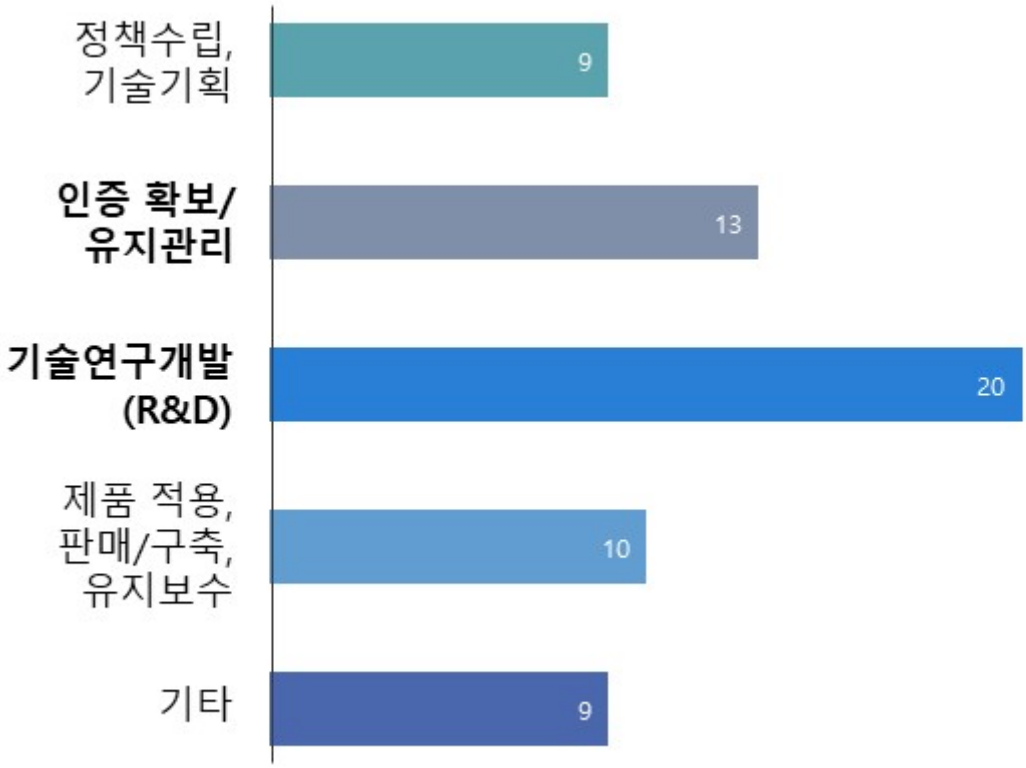
<표 4-11> 소프트웨어 안전 담당 조직 및 담당자 현황

산업분류	기업형태	주사업/관련사업	소프트웨어 안전담당조직	조직인원수
서비스업 (정보통신업)	대기업	소프트웨어개발/SI	보증/테스트팀	확인불가
	대기업		통합품질혁신팀	수명 내외
	중소기업		소프트웨어부	수명 내외
	중견기업	소프트웨어개발	SE사업본부	90여명
	중소기업	소프트웨어개발	연구소	수명 내외
제조업	대기업	전자제품제조	SE그룹	200명 이상
	대기업	자동차/부품 제조	(미상)	20~30명
	대기업	화장품 제조	정보전략부서	10여명 내외
	대기업	반도체 제조	PI그룹	10여명 내외
	대기업	반도체 제조	QC조직	십수명
	중견기업	교통 신호장치	RAMS팀	수명 내외
	중소기업	의료기기	소프트웨어개발팀	수명 내외

11) 소프트웨어 안전 관련한 업무 영역

소프트웨어 안전을 담당하는 조직 및 담당자가 수행하는 업무 유형이 무엇인지에 대해 질문하였다. 그 결과, 소프트웨어 안전을 담당하는 주로 품질 관련 조직에서 수행하는 업무 중 소프트웨어관련된 업무는 기술연구개발(R&D)와 소프트웨어 안전 관련된 인증을 확보하고 인증의 갱신 및 관리 업무가 주된 것으로 확인되었다. 기술연구개발 업무는 주로 자동차, 철도 등의 제조업에서 고객사가 요구한 사항이나 수출 등을 위해 인증을 획득해야 하는 상황인 경우, 영업 또는 생산 조직에서는 이러한 종류의 업무에 대해 대응하기 어려워 품질 관리 관련한 조직에서 이러한 상황에 대응하기 위한 개발, 시험, 서류 준비 등의 업무를 수행하는 것으로 확인되었다. 또한 인증의 획득과 사후 관리 업무도 주된 업무 중 하나로 파악되었는데, 앞서 고객사 요구사항 또는 수출을 위해 대상국가에서 요청한 인증을 획득한 이후에도 새롭게 보완을 요구하는 사항이나, 달라지는 법・제도/표준에 맞춰 인증을 갱신하는 업무도 품질 관리를 담당하는 조직에서 부수적으로 수행하는 것으로 파악되었다.

[그림 4-30] 소프트웨어 안전 수행 조직의 소프트웨어 안전 관련한 업무 유형



12) 정보통신산업진흥원의 ‘소프트웨어 안전성 공통개발 가이드’ 인지 여부

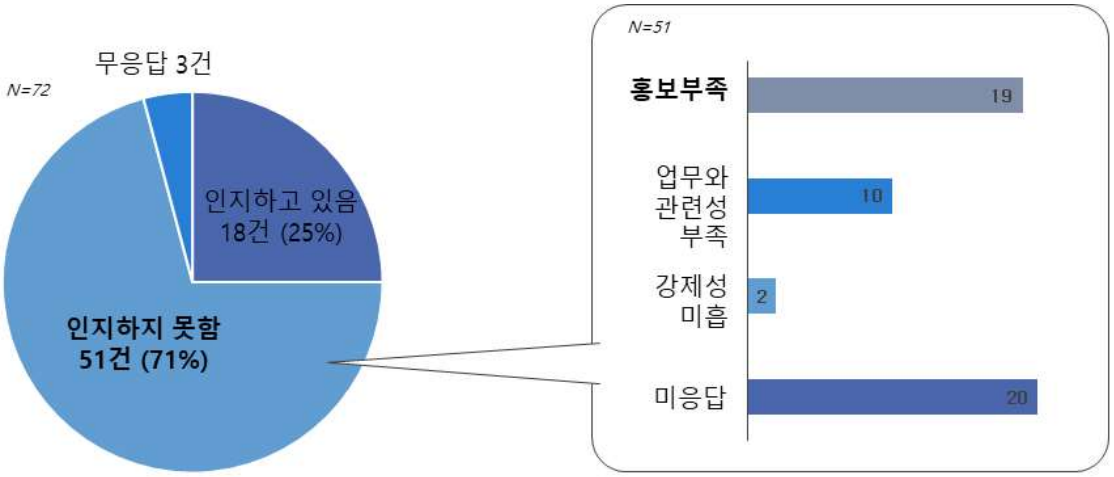
정보통신산업진흥원에서는 ‘소프트웨어 안전성 공통개발 가이드’를 작성하여 배포하고 있으나, 과거부터 소프트웨어 안전이 중요하게 작용했던 기업들 외에는 대부분의 기업들이 해당 가이드의 존재를 잘 모르고 있었다. 70% 이상의 응답자가 해당 가이드를 ‘모른다’고 응답하였는데, 추가로 해당 가이드가 잘 알려지지 못한 이유가 무엇일까에 대해 질문한 결과 그동안 ‘홍보 부족’이 가장 큰 이유인 것으로 뽑혔다. IT 부서의 담당자나 소프트웨어 안전 담당자가 아니더라도 기업 내에서 직/간접적으로 소프트웨어나 시스템의 개발에 참여하게 되는데 해당 가이드가 사전에 충분히 일반 기업들에 홍보가 되고 노출이 되었다면 해당 가이드의 명칭은 들어봤었을 것이라는 의견이었다.

또다른 의견으로는 홍보 부족보다는 제도적 강제성이 부족하여 적극적으로 전파되지 않았거나, IT직무의 실무자라고 하더라도 업무와 직접적인 관련성이 부족하여, 한 번

들어봤을 수는 있지만 기억을 하지 못하는 것일 수도 있다는 의견이 있었다.

'소프트웨어 안전성 공통개발 가이드'를 인지하고 있는 담당자는 18명으로, 전체 응답자의 약 25%에 해당하였는데, 이들은 해당 가이드를 소프트웨어 개발 가이드로 사내 전파하고 제품 설계 또는 양산 단계 테스트 등에 적용하고 있었다.

[그림 4-31] 소프트웨어 안전성 공통개발 가이드 인지 여부



13) 소프트웨어 안전을 업무에 적용할 경우 필요한 사항

전체 조사 대상자에게 소프트웨어 안전을 업무에 적용한다고 가정할 경우, 필요한 사항이 무엇일지에 대한 질문을 하였다. 그 결과는 제조업과 서비스업이 명확한 차이가 있어 구분하여 정리하였다.

먼저 제조업의 경우 대부분의 산업군 전반에 걸쳐 소프트웨어 안전과 관련한 인력의 육성 및 충원이 필요하다는 의견이 있었다. 이는 제조업 입장에서 전통적으로 소프트웨어는 부수적이고 핵심이 아니라는 인식이 있어 기업 내부적으로 인재를 육성하거나 충원하는데 인색했었기 때문인 것으로 보이며, 이러한 업계 전반적인 인식의 변화가 단기간에 이루어지기 어려울 것으로 전망된다.

또한 제조업 분야에서는 고객사의 소프트웨어 안전에 대한 필요성 인식이 필요하다는 의견이 있었는데, 이는 달리 해석하면 고객사에서 소프트웨어 안전에 대해 필요성을 인식하고 추가되는 비용과 시간에 대한 부담을 지는 것에 대한 당위성을 부여해 달라는 의견이었다. 철도 관련된 제조업 분야에서 이러한 의견이 나왔는데, 이는 비단

철도 산업 분야에만 국한된 것이 아니라 전 산업 공통된 의견으로 보아야 할 것으로 생각된다.

서비스업계에서는 주로 소프트웨어의 개발이나 시스템 구축을 전문으로 하는 정보통신업계와 인터넷 뱅킹 등 서비스에 있어 소프트웨어가 핵심인 금융/보험업계에서 의견을 제시하였는데, 소프트웨어의 품질 향상 및 관리 차원에서 소프트웨어 안전을 보장할 수 있도록 제도화/강제화가 필요하다는 의견이 대다수였다.

그 이유는 기업 입장에서는 소프트웨어 안전과 관련된 활동이 비용으로 인식되기 때문인데, 다시 말해 일부 법/제도 측면에서 요구되거나 고객사에서 요구되는 경우가 아닌 기업들은 소프트웨어 안전 관련 활동이 매출과는 크게 영향이 없기 때문이다.

이에 대해서는 국내 소프트웨어 개발 및 시스템 구축 업계의 현실이 전제되어 있는 것으로 생각되는데, 국내 시장에서는 기업들이 정보통신 분야 아웃소싱 등에 사용하는 비용이 해외보다 매우 적고, 항상 품질 유지보다는 원가 절감의 대상으로만 인식되어 온 것과 해당 기업들 내부적으로는 경영진의 소프트웨어 안전에 대한 인식 부족에 기인한 것으로, 구조적인 해결 없이 업계 내부에서 자체적으로 해결하기는 어렵다고 판단했기 때문인 것으로 보인다.

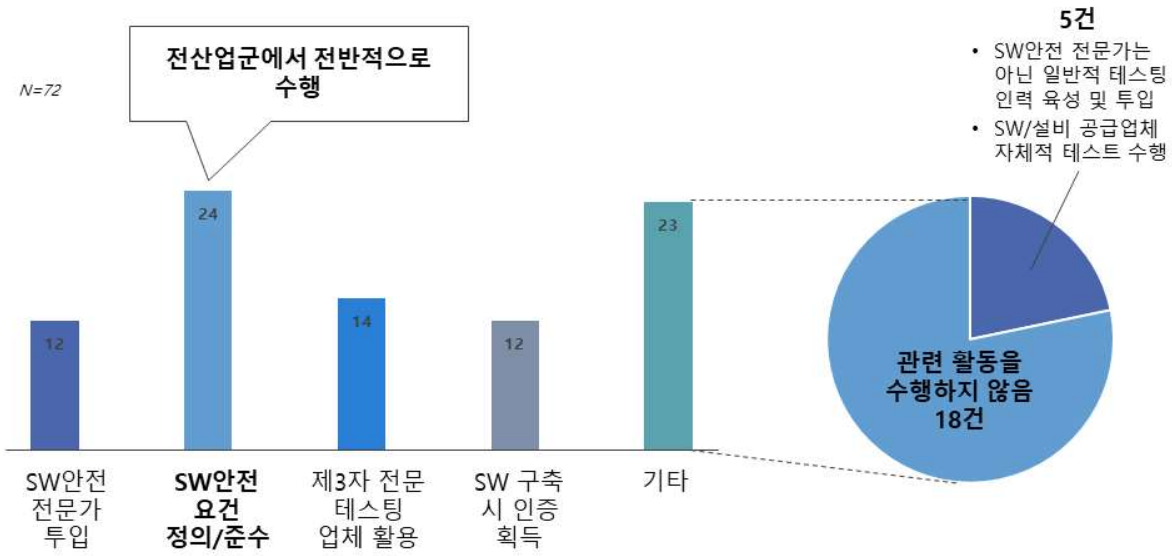
3. 소프트웨어 안전 예방점검 활동

1) 소프트웨어 안전사고 예방을 위한 활동

기업들은 'Safety Critical Software'[127]의 기능 오류로 인해 안전사고가 발생하는 것을 방지하기 위하여 소프트웨어 안전 요건을 명확하고 구체적으로 정의하고 이를 준수하는 것을 최우선적으로 시행하고,(24건) 그 다음으로는 기업 내부가 아닌 외부의 전문 테스팅 업체를 활용하여 검수하는 것으로(14건) 확인되었다.

127) 응용 소프트웨어, 각종 부품/제품에 탑재된 Embedded 소프트웨어 등을 모두 포함하여, Safety상 미흡한 요건으로 인해 인명/재산 등 막대한 손실을 초래할 수 있는 소프트웨어의 통칭

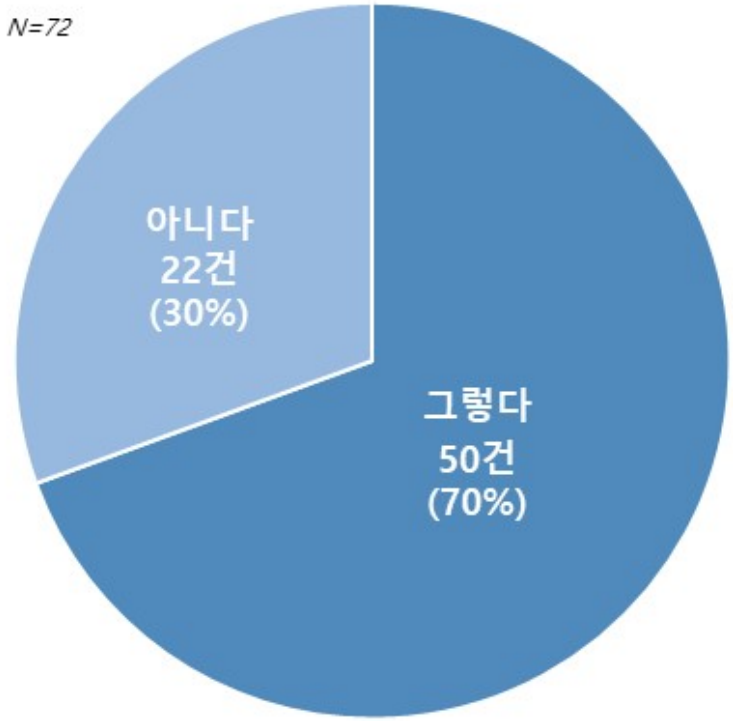
[그림 4-32] 소프트웨어 기능 오류로 인한 안전사고 예방을 위한 활동 (복수 응답)



2) ‘Safety Critical Software’에 대한 소프트웨어 안전 검증 활동

우선 생산 또는 관리하는 부품/제품에 Safety Critical Software가 포함되어 있다고 응답한 기업은 전체 응답자의 70%에 달하는 50명이었다.

[그림 4-33] 생산 또는 관리하는 부품/제품에 ‘Safety-critical Software’ 포함된 기업



이들 응답자 50명에 대해 ‘Safety Critical Software’에 대한 소프트웨어 안전 검증 활동 여부를 질문한 결과, 검증 활동을 수행한다는 답변은 다수의 응답자인 29명(58%)가 “수행한다”고 답변하였고, 일부 14명의 응답자가 “수행하고 있지 않다”라고 답하였다. “수행한다”라고 답변한 기업들의 유형으로는 주로 원자력, 철도, 우주항공, 의료, 자동차 등 전통적으로 Safety-critical Software가 탑재되거나 해당 소프트웨어를 생산하던 기업들이었다. “수행하고 있지 않다”라고 답변한 일부 응답자는 주로 소프트웨어를 모기업으로부터 하청받아 생산하는 기업들로, 최종 사용자(End User)인 고객사의 해당 소프트웨어 사용 환경, 최종 제품의 형태를 잘 알지 못하여 이러한 답변을 한 것을로 보인다.

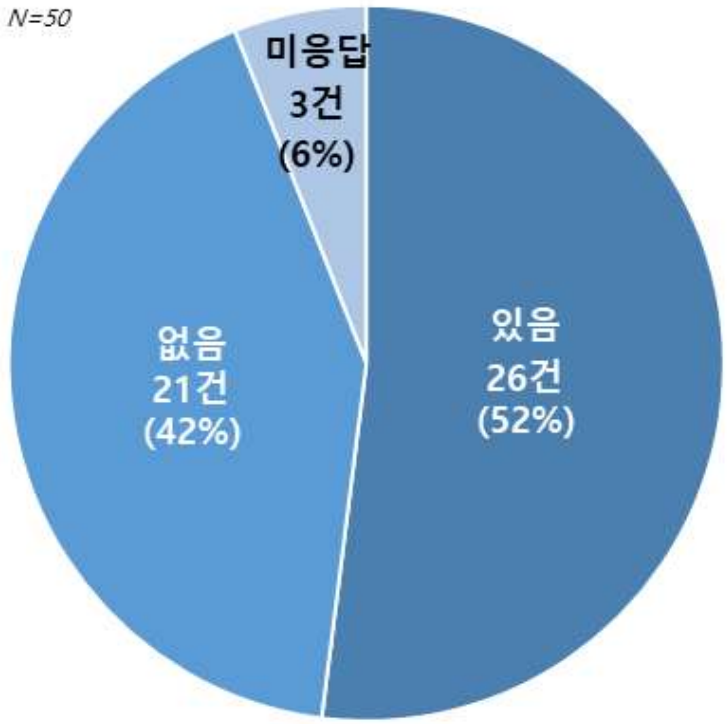
3) ‘Safety Critical Software’와 관련한 표준 및 지침 보유 여부

동일한 응답자 50명에 대해 ‘Safety Critical Software’ 검수에 대한 기업 내부적인 표준 또는 지침의 구비여부를 질문하였다. 이에 대해 ’ 보유하고 있다’ 고 답한 응답자 비율은 약 50%로, 이들은 대부분 철도나 에너지 등 전통적으로 소프트웨어 안전에

대해 법적/제도적 안전장치 및 개입이 지속적으로 이루어졌고, 기업 내부적으로도 관리체계가 완비되어 있던 산업이었다.

‘보유하고 있지 않다/없다’ 고 답한 사업체 중에는 원자력, 에너지 생산 등 전통적으로 소프트웨어 안전이 중요한 산업군임에도 불구하고 중소기업인 경우 해당 표준과 인증 획득에 소요되는 내부 역량 및 비용과 같은 리소스의 부담으로 아직 갖춰지지 않은 경우들이 있었다. 또한 일부 대기업 계열사나 관계사라 기업 규모가 큰 경우에도, 해당 대기업의 직접적인 하청을 수행하는 것이 아닌, 2, 3차 공급사 역할을 하는 경우가 많아 ‘Safety Critical Software’를 다룸에도 불구하고 인증에 대해서는 크게 필요성을 인식하지 못하는 것으로 확인되었다.

[그림 4-34] ‘Safety Critical Software’와 관련한 표준 및 지침 보유 여부



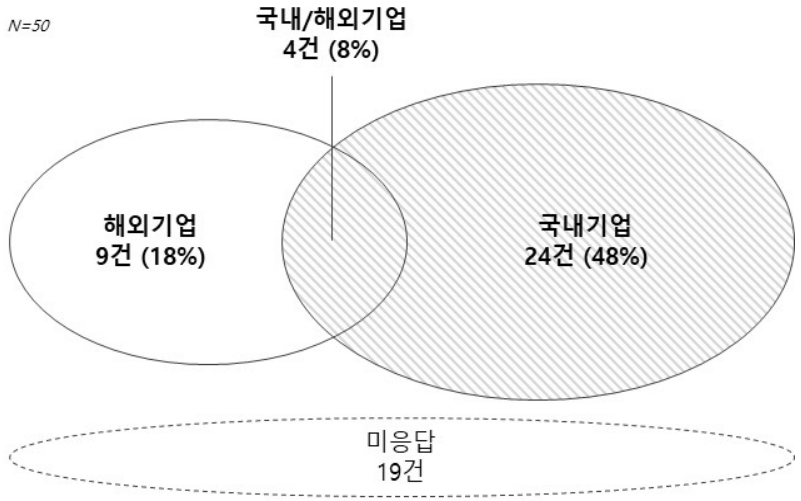
4) ‘Safety Critical Software’ 검수 참여 협력사 유형

‘Safety Critical Software’를 다루는 기업들에 한하여, ‘Safety Critical Software’ 검증 활동 수행 시 외부 업체를 활용하는 경우, 국내/해외 중 어떤 업체를 활용하는지 질문하였다.

응답자 명 50중 국내 TIC 업체만을 이용한다는 응답자는 24명이었고, 해외 TIC 기업

만을 이용한다는 응답자는 9명이었다. 또한 국내/해외 TIC 업체를 모두 이용한다는 응답자는 4명에 불과하였다. 이를 통해 'Safety Critical Software' 검증을 위해 외부 역량을 활용할 필요가 있는 경우, 대부분의 기업들은 국내 TIC 업체를 활용하는 것으로 보인다. 이는 해외 TIC업체의 경우는 대기업 위주로 활동하는 것으로 조사되었으며, 건수보다는 건당 비용이 큰 것으로 유추된다.

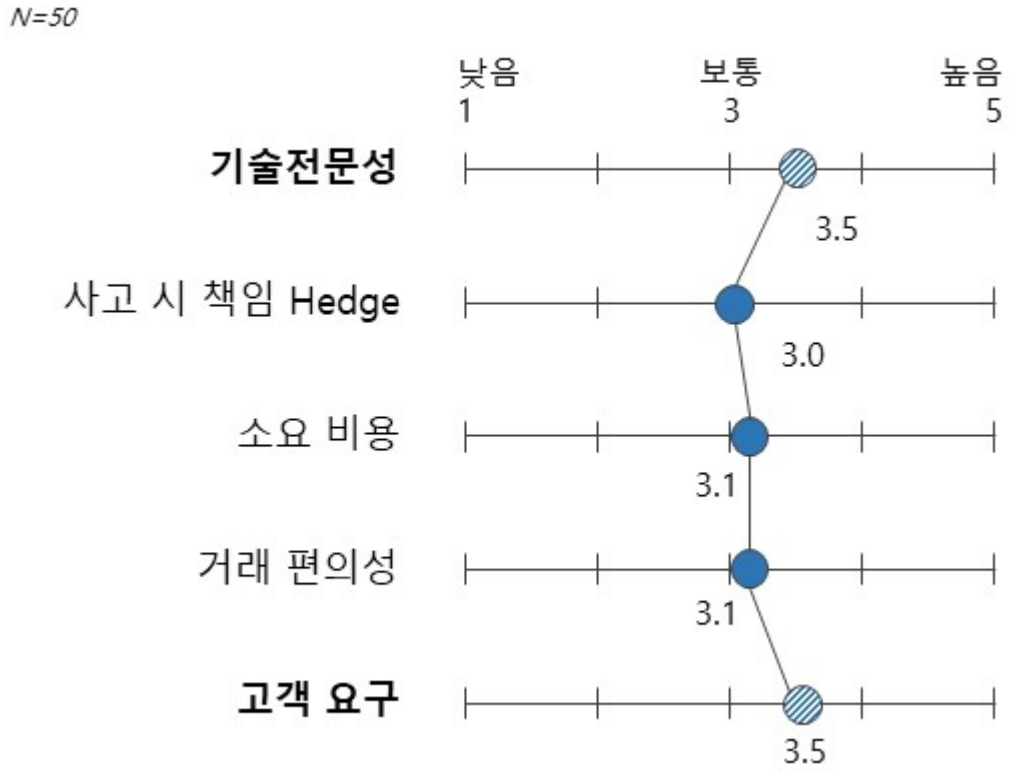
[그림 4-35] Safety-Critical SW 검증활동을 수행 시 활용하는 외부 업체 유형



5) 'Safety Critical Software' 검수 시 협력사 활용 사유

동일한 50명의 응답자들을 대상으로, 기업들이 'Safety Critical Software' 검수에 외부 협력사를 활용하려고 하는 목적을 5점 척도로(1점 ~ 5점 사이 선택) 평가해 본 결과, 해당 협력사가 보유한 기술의 전문성과 고객의 요구로 인한 활용이 3.5점으로 가장 큰 활용 목적인 것으로 확인이었다. 이는 소프트웨어 안전과 관련하여 요구사항에 대한 구현여부를 확인하는 기술 역량을 내부에서 단기간에 보유하기 어려운 관계로, 고객의 요구나 법·제도적 필수 조건인 상황에서 당장은 외부 협력사를 사용하고 있거나, 어차피 내부 역량 육성을 위해서는 장기간의 시간 소요와 인적 투자가 필요한데 그 시간과 비용 대비 외부에서 조달하여 사용하는 것이 합리적이라는 판단에서 비롯된 니즈라고 볼 수 있다.

[그림 4-36] ‘Safety Critical Software’ 검수 시 협력사 활용 사유



6) ‘Safety Critical Software’ 구축/운영 시 소프트웨어 안전 강화를 위해 사용하는 비용 규모

먼저 ‘고정비’와 ‘변동비’로 나누어 생각해 볼 수 있다. ‘고정비’인 경우에는 대부분 응답자들이 ‘인증 비용’과 ‘인건비’의 지출을 꼽았다. ‘인증 비용’의 경우 인증 획득이 반드시 필요한 기업에서 주로 발생하는데, 자동차 산업 등 신제품의 출시나 제품 Lifecycle이 짧아 회전율이 빠른 기업일수록 매년 지출하는 ‘인증 비용’의 금액이 컸다. 응답 기업은 대체로 ‘인증 비용’으로 연간 수천만원 ~ 10억원 이내 금액을 지출한다고 답했다.

두 번째로 고정비 중에 큰 비중을 차지하는 것은 ‘인건비’로, 철도 등과 같이 ‘Safety Critical Software ‘에 요구되는 수준이 높을수록 지출 금액이 증가하는 경향을 보였다. 응답 기업들은 대부분 소프트웨어 안전 영역에 10 ~ 20 MM[128] 정도가 소요되며, 연간 1MM 당 평균적으로 약 7천만원 소요되어, 최대 14억원 정도 지출한다고

128) Men Month, 월단위 업무량을 지칭

응답하였다.

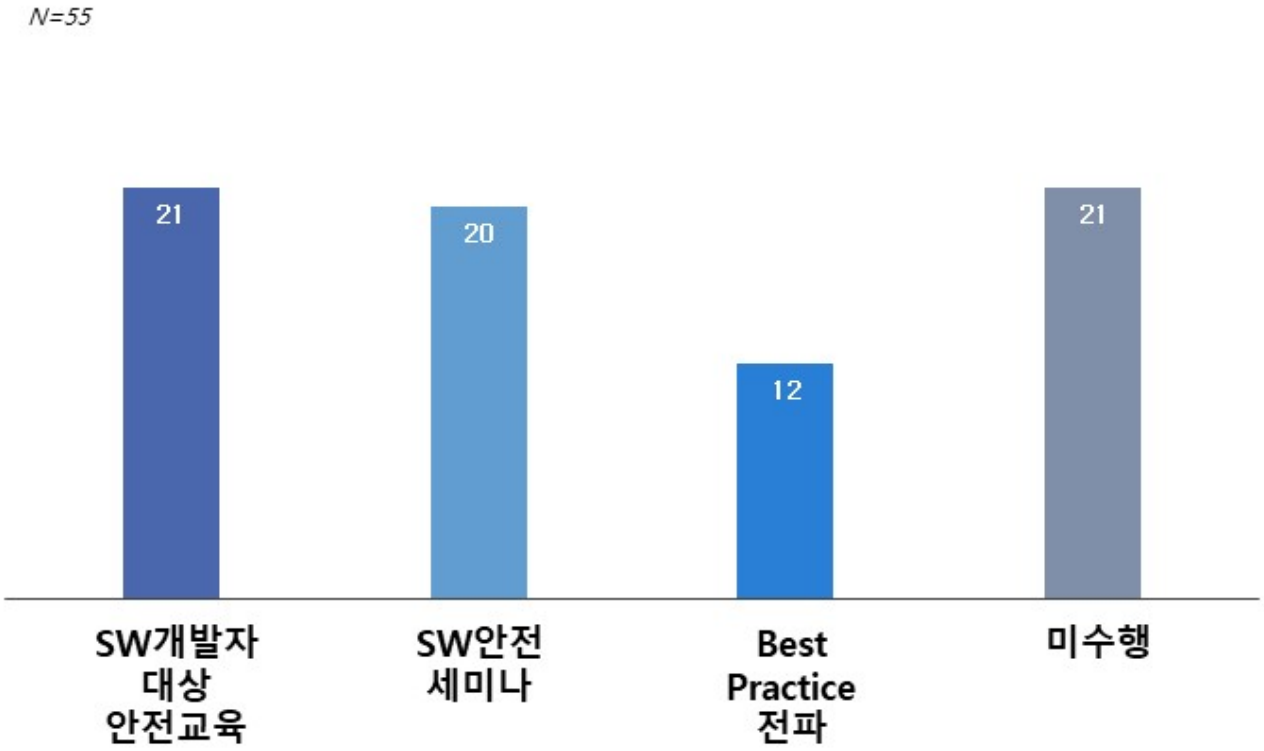
‘변동비’의 경우에는 ‘CAPEX(자본지출, Capital Expenditure)’와 ’OPEX(운영비, Operating Expenditure)’로 구분해서 질문하였다. ’ CAPEX ‘는 주로 공공/대기업인 경우 소프트웨어 안전을 위해 일정 부분을 암묵적으로 지불하고 있었고, 요구되는 ‘Safety Critical Software’ 수준에 따라 총 투자비용 중 소프트웨어 안전에 투자하는 비율은 상이하였으나, 대체로 프로젝트 당 소프트웨어 안전을 위해 투자비용의 약 3% ~ 10%의 비율을 할애하는 것으로 파악되었다.

‘OPEX’의 경우에는 주로 소프트웨어 개발 또는 테스팅을 외부 협력사를 통해 수행하는 기업에서 발생하는 경우가 많았다. 비용은 명시적으로 확인되지 않았으나, 최대 30% 이내 지출하는 것으로 추정되었다. 일부 예외적인 사례로, 특정 기업에서 개발한 소프트웨어가 통신망을 이용하는 경우 소프트웨어 안전을 테스팅하는 업체에서 회선당 600원을 부과하는 경우도 확인되었다.

7) 소프트웨어 안전 교육을 위해 수행하는 활동 유형

미응답자 17명을 제외하고, 55명의 응답자가 소프트웨어 안전 교육을 위해 수행하는 활동의 유형을 묻는 질문에 답하였다. 이중 21명은 소프트웨어 안전 교육 자체를 사내에서 수행하지 않는다고 답하였고, 나머지 34명의 응답자 중에서는 ‘소프트웨어 개발자 대상 안전교육을 실시한다’ 라는 의견이 21건으로 가장 많았다. 또한 ‘소프트웨어 안전 세미나’를 개최한다는 답변도 20건으로 거의 비슷하였고, ‘선진 사례 전파(Best Practice 전파)’ 한다는 응답은 12건에 불과하였다. 이는 아직까지 기업 외부에서 벌어지는 활동에 대해서는 기업 내부적으로 수용할 상황이나 역량이 미흡하거나 외부로부터의 소프트웨어 안전 관련한 최신 정보의 전달 및 공유가 충분히 이루어지지 않았다고 보여 진다.

[그림 4-37] 소프트웨어 안전 교육을 위해 수행하는 활동 유형 (복수 응답)



‘소프트웨어 개발자 대상 안전교육을 실시하지 않는다’ 고 대답한 응답자들은 그 이유로써, 대부분 사내에서는 교육을 하지 않아 외부 교육으로 대체하거나, 소프트웨어 안전에 대하여 교육할 강사나 내부 역량이 축적되지 않았다는 이유, 임원이나 인사 담당자가 사내 소프트웨어 안전 교육에 대한 필요성을 인식하지 못하고 있다는 이유를 들었다.

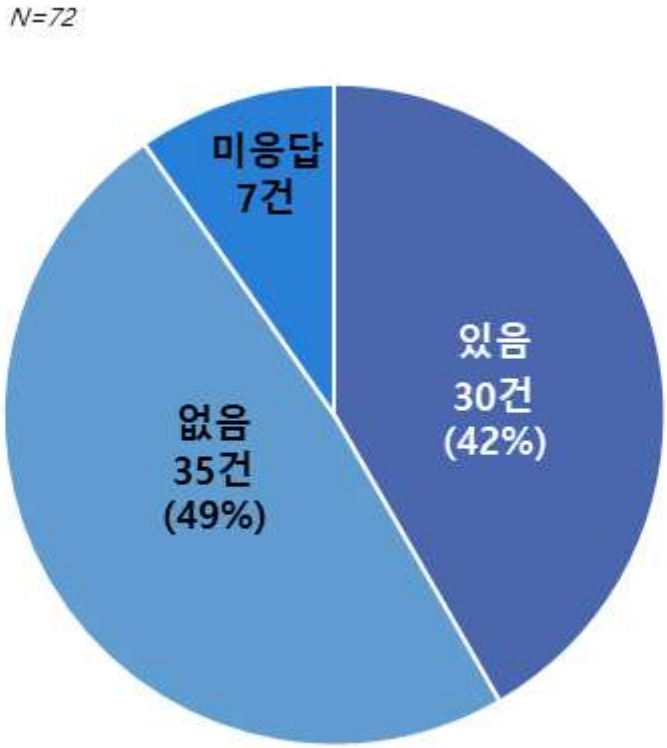
4. 소프트웨어 안전 대응관리 활동

1) 기업 생산 제품 사고 시 대응 시나리오 보유 여부

기업에서 판매한 제품과 상품 관련한 사고가 발생할 경우 약 40%인 30명의 응답자가 사고 대응하는 시나리오를 정의하고 있다고 대답하였다. 이들은 대부분 철도, 에너지/화학, 자동차, 의료기기 제조업과 같이 사고가 발생할 경우 고객의 신체나 재산에 중대한 문제를 야기할 수 있으며, 나아가 사회적 문제와 기업의 존폐까지 결정지을 수 있는 사업자들이었고, 일부는 대기업을 대상으로 소프트웨어를 공급하거나 시스템 구

축 사업을 하는 사업자들로, 사고 발생 시 고객사에 중대한 금전적 손실을 입힐 수 있어 사고 대응 시나리오를 정의해 두고 있다고 대답하였다. 또 다른 사업자 유형으로는 금융업 사업자들로 인터넷 기반의 서비스를 제공하는 관계로 네트워크나 소프트웨어의 문제로 서비스 중단 시 고객의 재산상 중대한 손실을 입힐 수 있기 때문에 사고 대응 시나리오를 보유하고 있다고 응답하였다.

[그림 4-38] 기업 생산 제품 사고 시 대응 시나리오 보유 여부



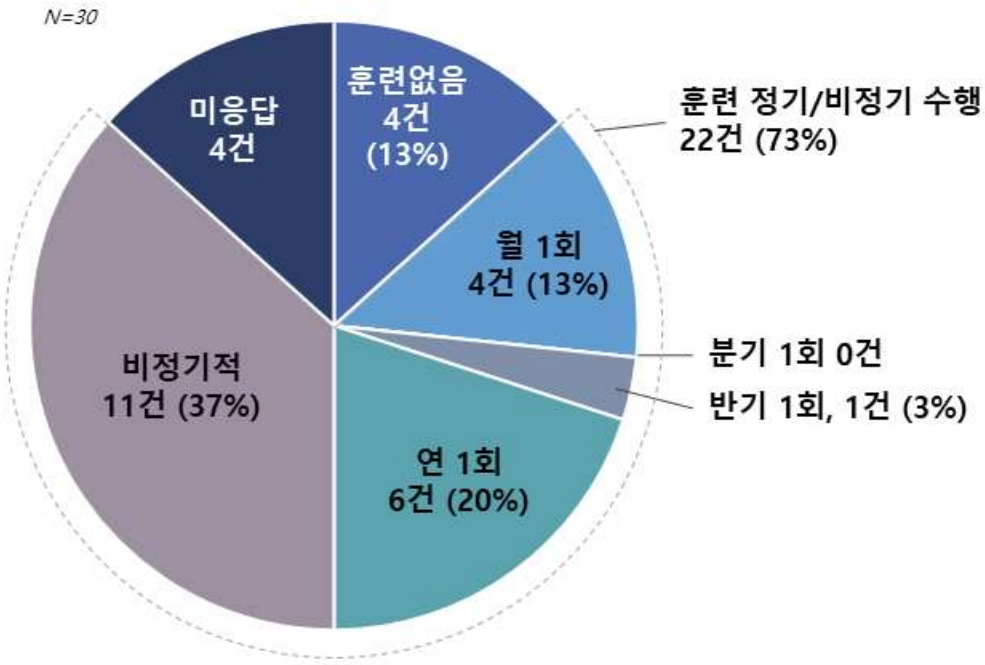
반면, 위 산업군에서도 일부 기업들은 금융업, 자동차제조업, 반도체제조업 사업자이면서도 사고 대응 시나리오를 보유하지 않고 있다는 응답을 하였는데, 이는 이들 기업이 대기업이라서 조직/기능이 세분화되어 있어 응답자가 해당 업무/기능을 담당하거나 담당했던 경험이 없어 부정적인 응답을 했을 가능성이 있다.

사고 대응 시나리오를 보유하지 않고 있다는 응답 중에는 중견 이하의 소규모 기업 또는 신생 기업이 다수 포함되어 있어, 사고 대응 시나리오까지 준비하기에는 인력/예산이 부족하거나 아직 사고를 겪어보지 않아 그 필요성을 느끼지 못하는 것이라고 추정할 수 있다.

2) 사고 대응 시나리오 시 해당 시나리오에 따른 훈련 수행 여부

사고 대응 시나리오를 보유하고 있다고 응답한 응답자 30명을 대상으로, 사고 대응 훈련을 실시했던 경험이나 주기적으로 실시하고 있는지 질문하였다. 응답자의 약 70%가 과거부터 현재까지 훈련을 수행했던 경험이 있는 기업이 있으며, 이중 절반은 비정기적으로 훈련을 수행하고 있다고 하였고, 절반은 최소 연 1회 이상 훈련을 실시한다고 답변하였다.

[그림 4-39] 소프트웨어 안전사고 대응 훈련 수행 여부



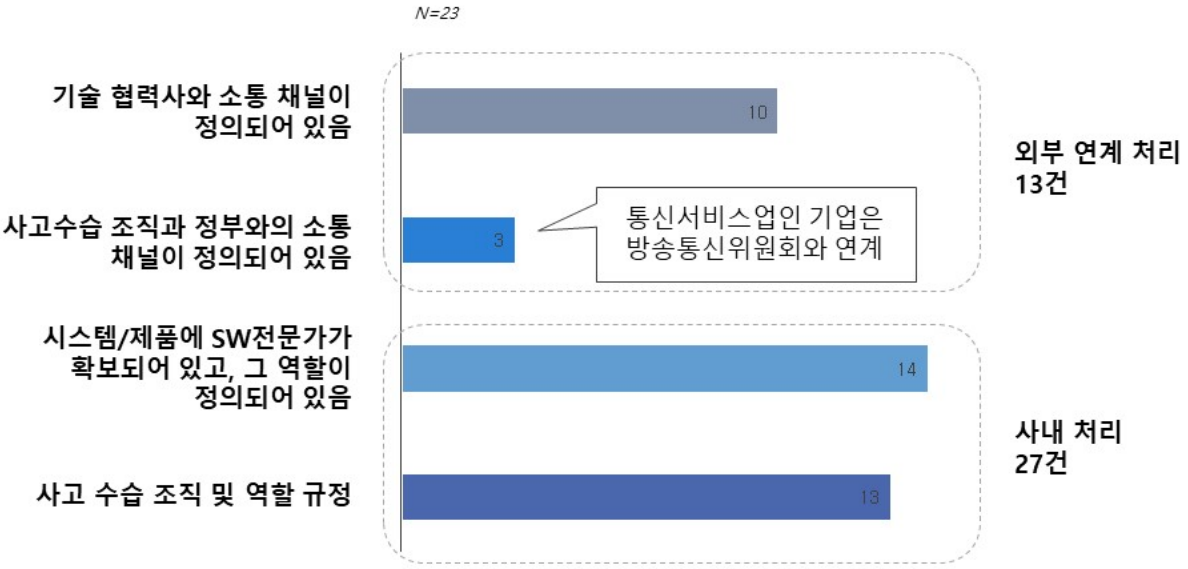
과거부터 최소 1회 이상 훈련을 수행했던 기업들의 속성을 살펴본 결과, 산업군이나 인력, 매출 규모에 있어 일정한 규칙성은 없었으며, 각 기업별 상황 및 특성에 따라 훈련 빈도나 주기를 조정하는 것으로 판단되었다.

3) 소프트웨어 안전사고 대응 시나리오 대상 영역

사고 대응 시나리오를 보유하고 있는 기업 중 소프트웨어 관련한 시나리오도 보유하고 있는지를 질문하였는데, 약 80% 가까이 소프트웨어 관련 시나리오도 보유하고 있었다. 이들은 특히 제조업 및 서비스업 중에서도 관제 기능이 필요한 산업들로서, 항

공, 기계, 자동차, 전자제품, 반도체, 에너지/화학 분야 제조업이거나, 시스템 구축 또는 아웃소싱을 전문으로 하는 서비스업 사업자인 것으로 확인되었다.

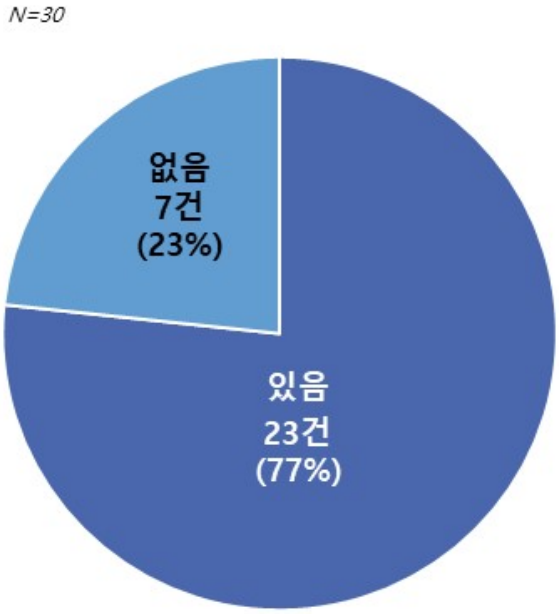
[그림 4-40] 소프트웨어 관련 사고 대응 시나리오 적용 대상 (복수 응답)



약 20%는 소프트웨어 관련 시나리오는 가지고 있지 않다고 대답하였는데, 기업 속성을 살펴본 결과, 보유하고 있다고 응답한 기업과 산업군, 매출 규모나 다른 속성에서 별다른 차이점을 찾지 못하였다. 다만 응답자 대부분이 대기업에 속해 있고, 이들의 지위나 상황이 특정 직무를 담당하는 것으로 보아 소프트웨어 관련 직무/부서의 경험이 부족하거나 기업 내부 교류가 없어 정보 부족으로 부정적 답변을 한 것으로 보인다.

정보에 대한 공유는 소프트웨어 사고 대응 시나리오를 보유하고 있는 기업에 있어서도 마찬가지로 문제인 것으로 보인다. 소프트웨어 사고 대응 시나리오가 적용되는 항목이 무엇인지에 대한 질문에 대해, 대부분의 응답자들이 사내 처리에 집중되어 있다고 응답하였다. 주로 시스템/제품에 소프트웨어 전문가가 할당되어있는 수준이거나, 사고 수습 조직/역할이 규정되어 있는 정도로, 외부 전문가 또는 정부와 소통이 준비되어 있는 경우는 상대적으로 적었다. 이로 인해 소프트웨어 관련한 사고의 이력 및 해결 노하우는 해당 경험을 보유한 기업의 내부에서만 공유되며, 국가 차원의 정보 수집/축적 및 공유는 이루어지기 어렵다는 현실을 보여준다.

[그림 4-41] 사고 대응 시나리오 보유 기업 중 소프트웨어 관련 시나리오 보유 여부



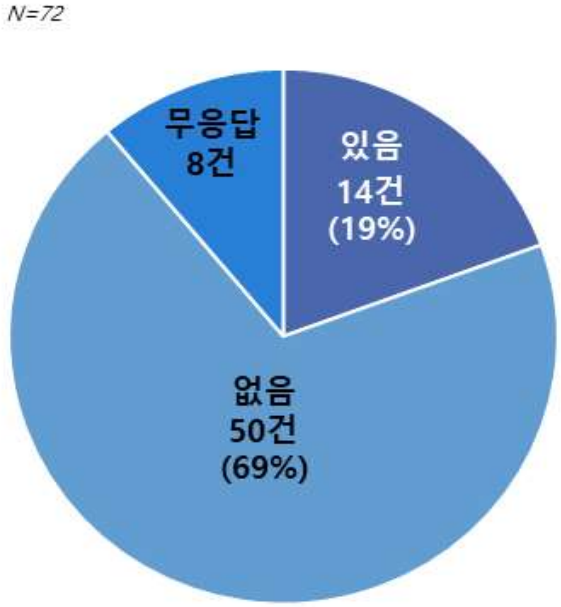
4) 소프트웨어 안전사고 경험 여부

과거부터 현재까지 기업의 내/외부에서 소프트웨어 관련한 안전 사고를 경험하였는지를 묻는 질문에 대해서는 약 20% 만이 경험이 있다고 답하였다. 이들이 속한 산업군을 살펴 보면, 아웃소싱 전문 정보통신업, 에너지/화학/반도체/디스플레이 제조업, 물류/유통/운수업, 금융업 등 다양한 산업군에 걸쳐 있었다.

제조업인 경우 주로 설비 제어 관련한 소프트웨어 안전사고 경험을, 아웃소싱인 경우 관제/제어 오류로 인한 사고, 금융업인 경우 지진과 같은 재해 또는 소프트웨어 오류로 인한 서비스 중단 사고를 경험하였다고 답하였다.

이러한 소프트웨어 안전사고로 인해 기업의 재산상 피해가 발생하거나, 고객 또는 고객사에 금전적 피해를, 제조업인 경우 생산인력의 인명 피해까지 발생했었다는 응답이었다.

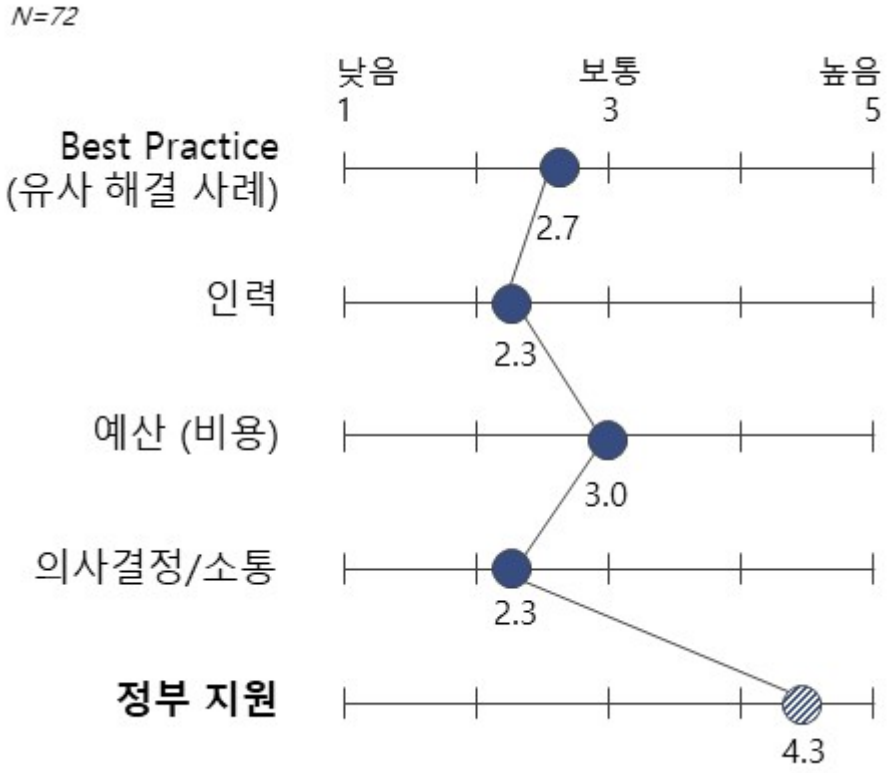
[그림 4-42] 기업 내/외부적으로 소프트웨어 안전사고 경험 보유 여부



5) 소프트웨어 안전사고 시 사고 수습을 위해 필요한 사항 및 중요도

소프트웨어 안전사고가 발생하는 경우 사고 수습을 위해 필요한 사항은 무엇이며 각 필요한 사항의 중요도를 평가해 달라는 질문에 대해 대다수의 응답자들은 '정부 지원'을 가장 중요한 사항으로 평가하였다. 다른 사항들에 비해 '정부 지원'은 4.3점의 높은 중요도를 보였는데, 정부 지원이 중요한 사유는 기업들이 소프트웨어 안전사고가 발생하였을 때 내부적으로만 처리하기가 어려워 정부가 개입하여 사고 처리에 대한 통제와 사고에 따른 책임 소재 규명 및 배상에 대해 공정하게 판결해 주기를 원하기 때문이었다.

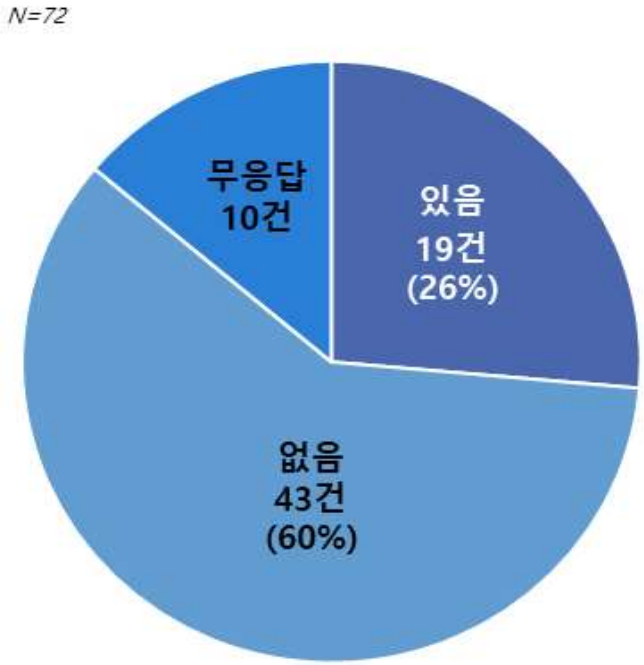
[그림 4-43] 소프트웨어 안전사고 발생 시 수습을 위해 필요한 사항 및 그 중요도



6) 소프트웨어 안전 검증활동 관리 툴 또는 시스템 보유 여부

소프트웨어 안전에 대한 검증활동을 관리하는 툴 또는 시스템을 보유하고 있느냐는 질문에 대해서는 약 30%가 보유하고 있다고 응답하였다. 그러한 툴 및 시스템으로는 소프트웨어 개발 사업 분야에서는 소프트웨어 안전을 진단하는 외산 상용 소프트웨어이거나, 형상관리 툴, 정적/동적 테스팅 툴이었고, 제조업에서는 공정이나 제품과 관련한 안전분석 툴, 특히 의료기기 제조업인 경우에는 IEC62304를 준용하는 자가 검증 시스템을 운용하고 있었다.

[그림 4-44] 소프트웨어 안전 검증활동 관리 툴/시스템 보유 여부

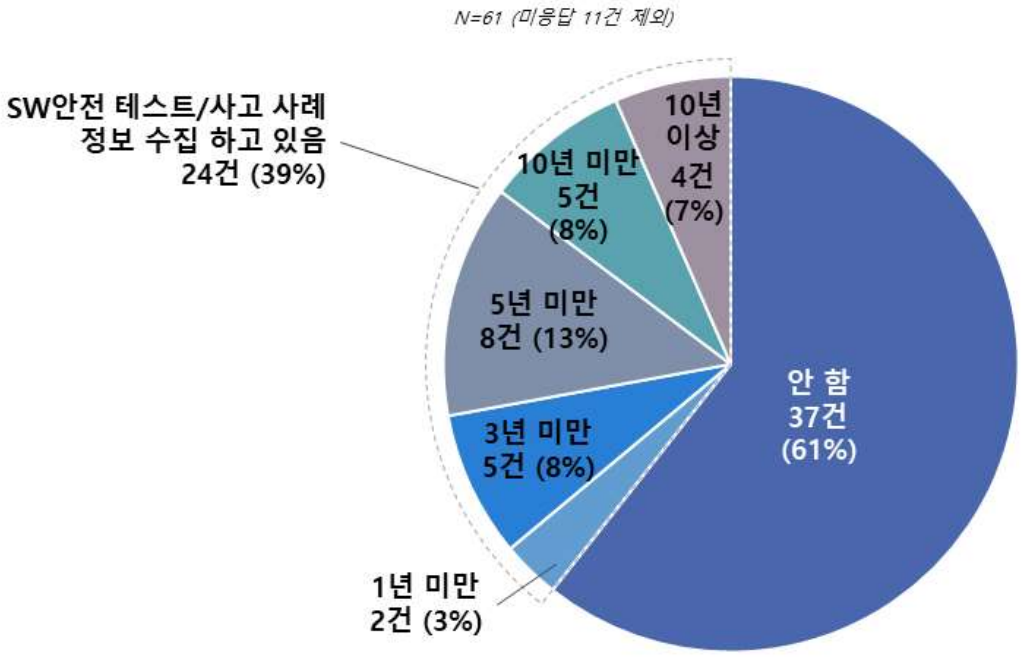


7) 소프트웨어 안전 테스트 및 사고 사례 정보 수집 여부

소프트웨어 안전 관련한 테스트 이력, 안전사고 발생 원인/결과, 처리방안 등의 사례 정보를 수집하고 있는지, 있다면 몇 년간 수집하고 있는지를 질문하였다. 그 결과 약 40%가 소프트웨어 관련한 테스트 및 안전사고 이력을 수집하고 있었다. 이들은 대체로 업력이 오래될수록 해당 정보를 수집하고 있다고 답하여 업과 수집 기간 간 상관관계가 있는 것으로 보인다.

문제는 이들이 그동안 이력 정보를 축적하였더라도, 정보 수집의 범위와 데이터의 품질이 부실하다는 의견이 많아 활용 가능성이 의문스러우며, 전체의 약 60%에 가까운 응답자들이 소프트웨어 안전과 관련한 테스트/사고 이력을 수집하지 않고 있었다라고 응답하였기에, 향후에는 이력 정보 미수집 기업들에 대한 소프트웨어 안전 관련 테스팅 및 사고이력 수집을 장려할 수 있는 방안과 이력 정보를 수집하더라도 활용을 전제한, 상세한 데이터의 수집이 필요할 것으로 보인다.

[그림 4-45] 소프트웨어 안전 테스트 및 사고 사례 정보 수집 여부

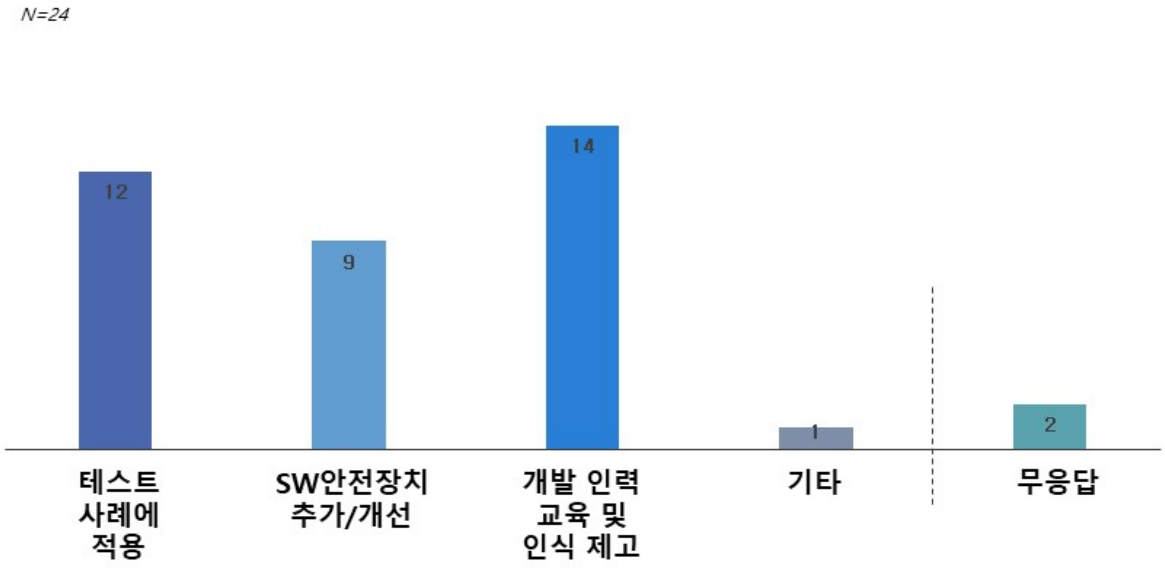


8) 소프트웨어 안전 테스트 및 사고 사례 정보 활용 수준 및 방법

그럼에도 소프트웨어 안전 관련 테스트 및 사고 사례 정보를 수집하고 있는 기업들은 수집한 이력정보를 어떻게 활용하고 있는지 조사하였다. 가장 많은 수가 응답한 활용 방안은 ‘개발 인력 교육 및 인식 제고에 활용’ 하는 방법으로 이는 주로 컨설팅, 금융, 유통, 농축산업 등 소프트웨어 안전의 중요도가 높지 않은 경우에 해당하였다.

그다음으로 많은 선택을 받은 방법은 ‘테스트 사례에 적용한다’ 와 ‘소프트웨어 측면 안전장치를 추가하거나 개선한다’ 는 방법이었는데, 주로 항공, 자동차, 반도체 제조업 및 원자력발전업과 같이 소프트웨어 안전의 중요도가 높은 산업이었다.

[그림 4-46] 소프트웨어 안전 관련 테스트 및 사고 사례 정보 활용 방법 (복수 응답)



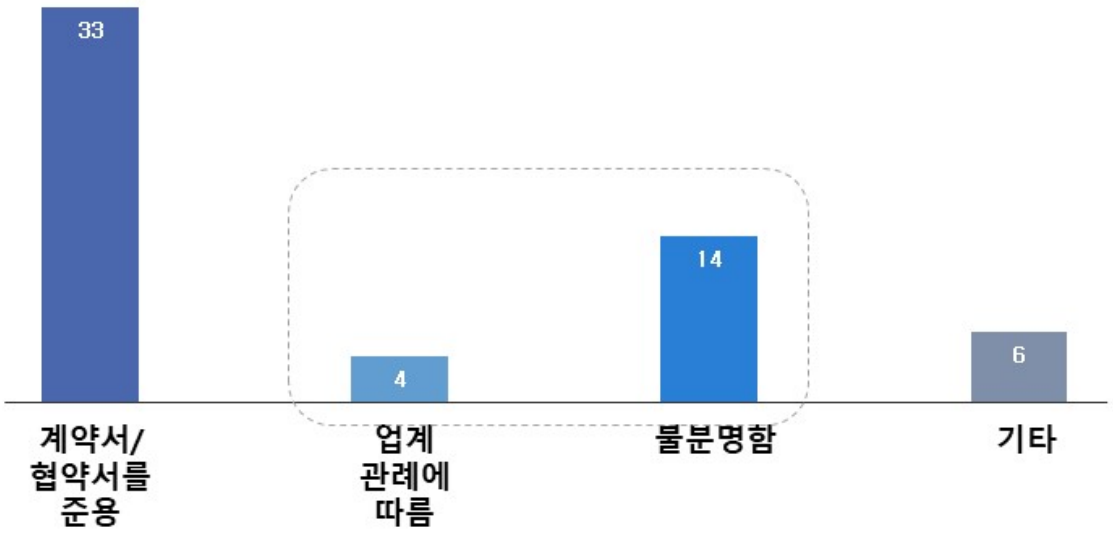
9) 소프트웨어 안전 문제 발생 시 책임 소재 규명 및 보상 방식

사용 중이거나 제품에 포함된, 즉 공급하거나 공급받은 소프트웨어 안전에 문제가 발생하였을 경우, 책임 소재는 어떻게 규명하고 보상은 어떤 방식으로 이루어지는가에 대한 질문을 하였다.

대부분의 경우에는 계약서 또는 협약서에 정한 기준을 준용하여 처리한다는 의견이었다. 이 경우 응답자들은 대부분 소프트웨어 안전에 대한 문제가 발생했거나 직간접적으로 경험했었던 업력이 오래된 기업이거나 대기업군에 속하는 기업들이었다.

이에 반해, 업계 관례에 따르거나, 처리 방식이 불분명하다라고 응답한 경우에는 주로 신생 기업이거나 규모가 작은 중소기업이라 안전사고를 아직 겪지 않았거나 안전사고의 처리 방식까지 정의할 정도의 여유가 없는 기업들이 해당되었고 일부는 소프트웨어 안전 문제가 기업 자신 또는 고객의 재산/인명 상 별다른 영향을 끼치지 않기 때문에 특별히 정의된 바가 없다는 의견도 있었다.

[그림 4-47] 소프트웨어 안전 문제 발생 시 책임 소재 규명 및 보상 방식 (복수 응답)



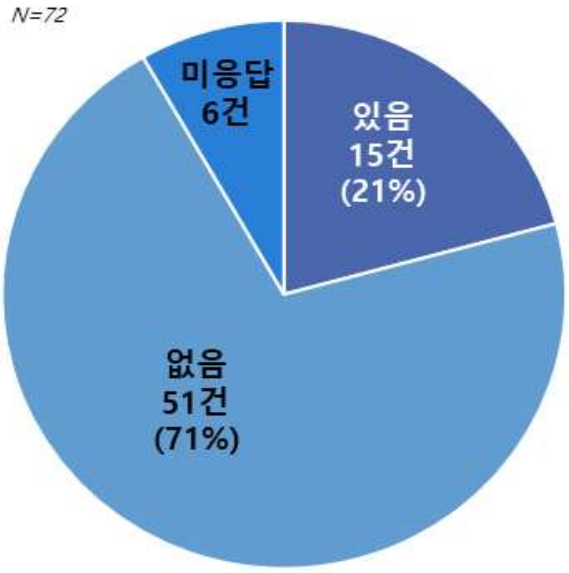
5. 소프트웨어 안전 관련 정책 요구사항

1) 정부의 소프트웨어 안전 관련 홍보자료, 보고서, 간행물 접촉 여부

정부에서 발간한 소프트웨어 안전과 관련한 홍보자료 또는 보고서, 간행물 등을 접한 경험이 있는지에 대한 질문에 대해서는 대다수가 경험이 없다고 응답하였다.(70%) 경험이 있다고 응답한 기업들은 대기업군의 정보통신 관련 시스템 구축 또는 아웃소싱 기업이거나 소프트웨어 개발 전문 기업 또는 국책 연구기관과 관련이 있는 경우였다.

따라서 정부의 소프트웨어 안전 관련한 규칙이나 정책을 홍보하기 위해서는 중소기업을 비롯하여 비 정보통신 분야 기업들에 대한 전파 계획을 세워야 할 것으로 보인다.

[그림 4-48] 소프트웨어 안전 관련한 정부 제공 자료 접한 경험 보유 여부



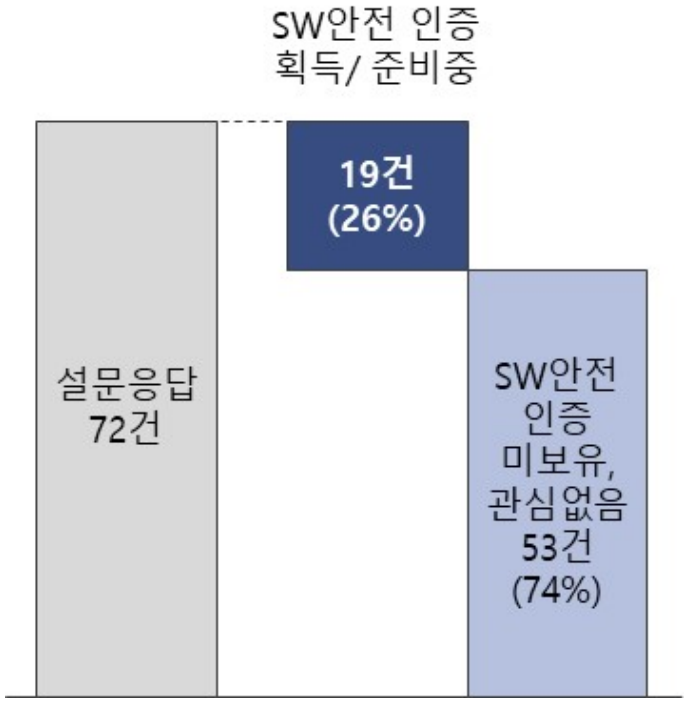
2) 소프트웨어 안전 인증에 대한 정부 정책적 지원 경험 여부

소프트웨어 품질을 포함한 소프트웨어 안전 인증을 받기 위해 준비하는 과정에서 정부의 정책적인 지원을 받은 경험이 있는지 질문하였다. 해당 질문에 대해서는 앞서 살펴본 ‘소프트웨어 개발/운영/관리 규정 및 절차 보유 기업의 국제 표준 인증 확보 여부’ 질문에 대해 소프트웨어 안전 인증을 획득했거나 준비 중이라고 응답했던 기업에 한해 분석하였다

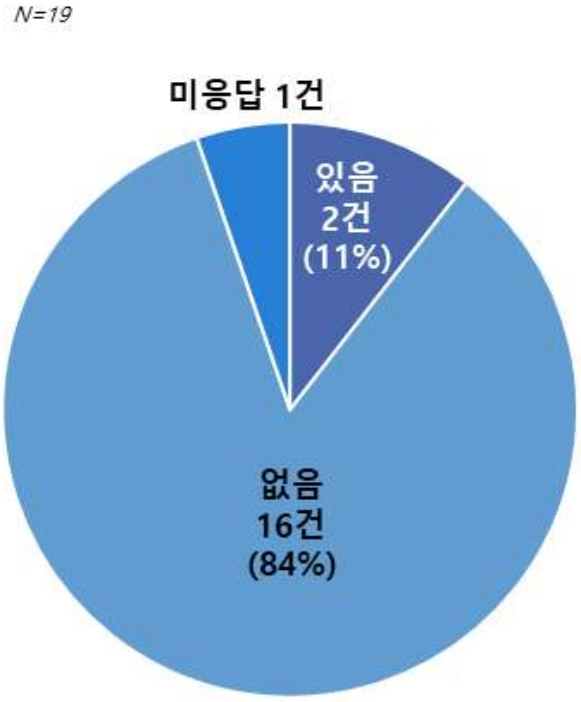
그 결과 있다고 응답한 19명 중에서도 소프트웨어 안전 인증을 획득하거나 준비하는 과정에서 정부 지원을 받았다고 응답한 인원은 2명에 불과하였고 나머지 응답자들은 대부분 지원을 받은 경험이 없다고 응답하였다.

정부 지원을 받은 경우에도 그 내역을 살펴보면 CMMI와 같이 소프트웨어 안전과는 관련이 낮은 소프트웨어 품질에 대한 인증 획득 지원을 받았던 것으로 보인다.

[그림 4-49] 소프트웨어 개발/운영/관리 규정 및 절차 보유 기업의 국제 표준 인증 확보 여부



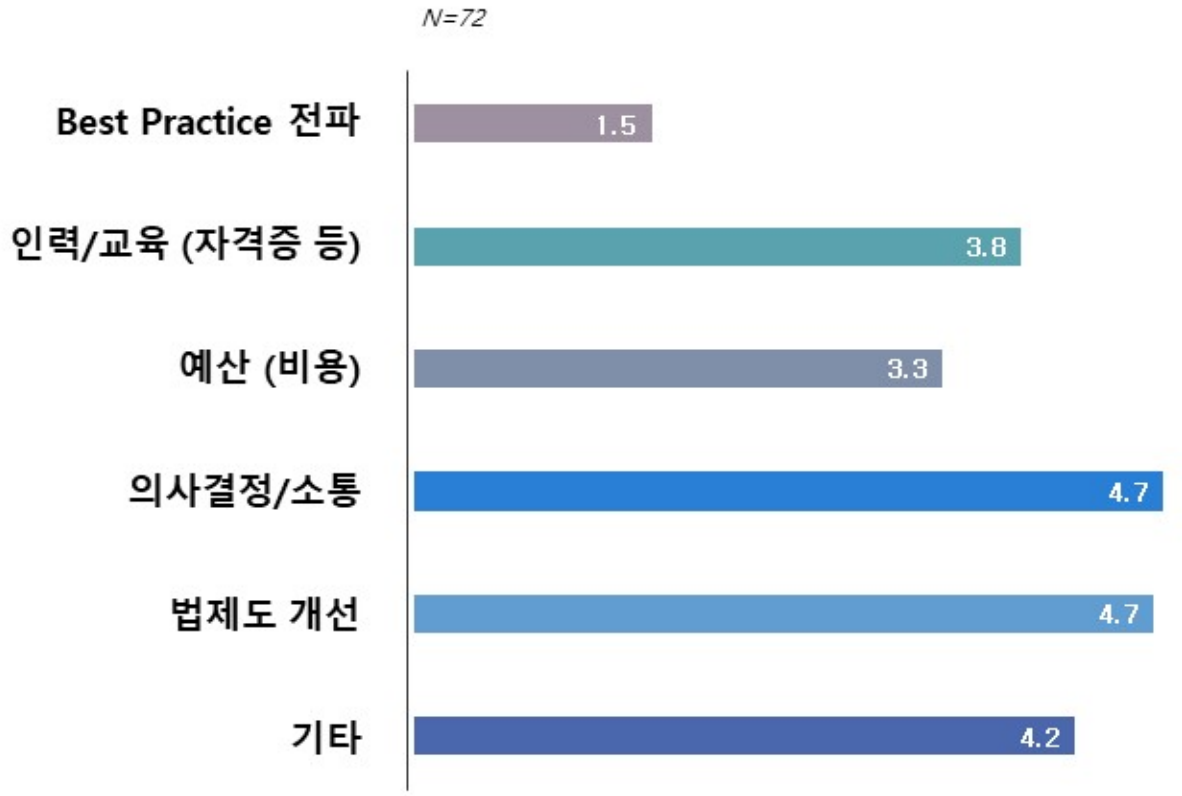
[그림 4-50] 소프트웨어 안전 인증에 대한 정부 정책적 지원 경험 여부



3) 향후 소프트웨어 안전 인증에 대한 정부 지원 시 필요한 영역 및 중요도

본 설문에 응답한 기업들은 소프트웨어 안전과 관련하여 향후 문제가 발생하여 지원을 받거나 정책적 필요가 있어 요청하거나 지식을 공유받을 수 있도록 ‘정부와 소통할 수 있는 채널’에 대한 지원을 최우선적으로 필요로 하는 것으로 확인되었다. 그와 동시에 소프트웨어 안전과 관련한 ‘법·제도적 지원 또는 강제화’를 필요로 하는 것으로 파악되었다. 기타 의견으로는 ‘국가주도 테스팅 기관을 설립’해 달라, ‘소프트웨어 안전 또는 테스팅 관련 지식의 국가주도 수집 및 공유’를 요청하였다.

[그림 4-51] 정부 지원 필요 영역 및 중요도



4) 소프트웨어 안전 수준 제고 및 관련 제품 판매 활성화 위한 정부 지원 필요사항

응답자들은 크게 표준에 대한 지원, 법·제도적 지원, 금전적 지원, 교육에 대한 지원을 요청하였다.

<표 4-12> 소프트웨어 안전 제고 및 소프트웨어 안전 준수 기업에 대한 정부의 지원/개선 필요사항

구분	개선 및 지원 요청 사항
표준에 대한 지원	• Global 수준의 Standard, Guide 제공 필요
법·제도 측면 지원	• 소프트웨어 안전 제도/규제/창구 일원화 (자율주행차는 현재 국토부와 경찰청에서 분담) • 소프트웨어 안전 제도에 대한 적극적 홍보 요청 • 최소 공공기관, 공공사업에 필수 적용하도록 제도화 • 소프트웨어 안전 적용에 따른 충분한 납기 제공/연장
금전적 지원	• 소프트웨어 안전 도입을 위한 중소기업 지원금 필요
교육에 대한 지원	• 소프트웨어 안전에 대한 실무자 교육 지원

6. 시사점

1) 법·제도 측면

우선 소프트웨어 안전에 대한 법·제도 체계가 완비된 산업들을 중심으로 하여 소프트웨어 안전 표준 및 지침이 구비된 상황이라 그 외 기업들은 자발적인 노력을 기울이지 않는 이상 소프트웨어 안전 관련한 표준 및 지침을 자체적으로 확보하기 어려운 상황이므로, 정부 주도로 전산업 공통적으로 적용될 수 있는 큰 틀의 소프트웨어 안전 관련한 법·제도의 제정이 필요하다.

두 번째로 '최소 공공기관, 공공사업에 소프트웨어 안전 관련 요구사항을 필수 포함하도록 제도화' 해달라는 정부 대상 요청을 접수하였는데, 이는 일반 기업들에게 소프트웨어 안전에 대한 홍보 및 인식을 제고할 수 있는 기회로 보인다.

세 번째로는 '소프트웨어 안전 제도/규제 담당부서 및 문의/민원 창구 일원화' 해달라는 요청을 접수하였다. 자율주행차량의 경우 현재는 국토부와 경찰청에서 업무를 나누어 진행하고 있는데, 일반 기업의 입장에서는 민원의 처리 주체도 불명확하고 진

전도 더디다고 생각하고 있었다. 이에 따라 소프트웨어 안전과 관련한 정부 소통 창구 일원화 및 홍보가 필요하다고 생각된다.

2) 인증/매뉴얼 측면

첫 번째로 소프트웨어 안전 국제 표준 인증 획득 기업 중 정부 지원받은 곳은 소수에 불과하며, 지원받은 인증도 소프트웨어 품질 관련 인증 불과한 실정으로, 소프트웨어 안전에 대한 인증 지원과 그에 따른 기업체들 대상 홍보 강화가 필요하다.

두 번째는 사고 발생 시 인명/재산 손실 규모가 클 수 있는 대기업 중심으로 소프트웨어 안전 사고 대응 시나리오를 구비하려는 경향이 있는데 사회 전반적으로 소프트웨어 사용 분야와 중요도가 증가하고 있는 상황을 고려한다면, 인명/재산 손실 규모가 그리 크지 않다고 응답한 중소기업들의 손실도 산업이나 업종 단위로 합산할 경우 손실이 클 수 있어 중소기업, 신생기업 대상 범용의 표준적 소프트웨어 안전 가이드 지원이 필요하다.

세 번째로는 두 번째 의견과 연계하여, 중견 이하 신생 기업일수록 소프트웨어 안전 관련 규정/절차, 사고대응 시나리오를 보유하지 않는 비율이 높은데, 이를 개선하기 위해 산업별 소프트웨어 안전사고 대응 시나리오 우수 사례를 발굴하고 이를 공유하는 플랫폼을 제공하는 것이 필요하다.

3) 조직・기관 측면

일반적으로 기업 규모와 소프트웨어 안전 조직/인력 규모는 서로 비례관계인 것으로 확인되었으며, 보통 소프트웨어 품질 관리 조직에서 소프트웨어 안전 담당하는 것으로 확인되었다. 또한 내부 소프트웨어 안전 담당 조직이 없는 경우 외부 TIC 업체를 활용하고 있었는데 기술전문성과 고객요구로 주로 국내 TIC 기업 활용하고 있는 것으로 확인되었는데, 중소기업에서는 비용 문제로 외부 TIC 업체를 활용하기도 어려운 실정이라 정부의 지원을 요청하였다.

중소기업의 고충을 해결하며 소프트웨어 안전을 도입할 수 있도록 다음의 두가지 방법을 고려할 수 있다.

한 가지 방법은 소프트웨어 안전 담당조직/담당자를 두기 어려운 중소기업에 대한

외부 역량 활용할 수 있도록 예산/알선을 지원하는 방식이다. (현재 중소기업을 대상으로 하고 있는 컨설팅 쿠폰 제도를 참고)

다른 방법으로는 중소기업 대상 소프트웨어 안전 검증 기능 포함 QC/QA 대행기관을 지원하는 방법도 고려할 수 있다.

4) 인력・교육 측면

소프트웨어 안전 관련 활동은 대부분 고객사 요구사항 준수나 규제준수를 위해 수행중이나, 여전히 소프트웨어중요도가 낮은 일부 전통적 제조업 분야에서는 소프트웨어 안전에 대해 인식이 부족한 상황이다. 또한 대기업과 같이 기업의 규모가 커지고 기능/조직 세분화될수록 경영진 및 전담자 외에는 소프트웨어 안전에 대한 인식이 부족한 경향을 보이는데, 이를 해결하기 위해 기업들의 경영진 층 대상으로는 전경련 등의 협회를 활용하고, 중소기업의 실무자들 대상으로는 교육 기회를 제공하여 소프트웨어 안전에 대해 산업 전반 대상 홍보를 강화하는 것이 필요하다.

두 번째로 대다수의 기업들은 소프트웨어 안전 관련 사고이력을 수집하지 않고 있다.(수집 기업 40% 불과) 또한 소프트웨어 안전 사고이력을 수집하더라도 대부분 사내 공유에 국한되며, 외부 공유 또는 국가차원 공유는 미흡하며 주로 사내 개발 인력 교육에만 활용하고 있는 실정이다. 이를 개선하기 위해서는 소프트웨어 안전 중요도 높은 경우 테스트 사례나 소프트웨어 안전장치 추가/개선에 활용하면서, 소프트웨어 안전 사고이력의 수집 확대 및 수집 데이터의 범위/품질 관련 전반적 관리 수준을 향상하도록 장려하고, 국가적 소프트웨어 안전 사고이력, 테스팅 노하우 수집 및 공유 플랫폼을 지원하는 것이 필요하다.

5) 사업 환경 개선 측면

본 조사의 응답자들은 소프트웨어 안전사고 발생 시 사고 수습을 위해 정부의 개입이 가장 필요하다고 응답하였다. 정부의 개입에 대한 요청은 두가지로 볼 수 있는데 먼저 사고 수습에 대한 정부의 통제를 요구하였고, 두 번째로는 책임에 대한 규명 및 배상 시 정부가 개입하여 공정한 결과를 낼 수 있도록 도와달라는 것이라. 이를 위해서는 먼저 소프트웨어 안전 관련 민원을 접수할 수 있는 소통 창구를 마련하는 것이

필요하다고 보인다.

또한 소프트웨어 안전을 일선 기업의 영업환경에 적용하기 위해서는 발주처의 충분한 납기/예산 제공이 필요하다. 이는 소프트웨어 안전이 일반적으로 수익을 창출하기 보다는 원청 기업에 비용으로 작용하기 때문인데, 이를 개선하기 위해서는 우선적으로 소프트웨어 안전에 대한 산업 전반 대상 홍보 강화가 필요하다고 보인다.

6) 프로세스 측면

소프트웨어 안전 관련 프로세스 보유 기업은 대부분 소프트웨어 품질이 사업 성과에 중대한 영향을 미치는 대기업, 정보통신업, 금융 분야 기업이며, 저부가가치 제품 생산하는 비정밀 설비 사용 제조업은 소프트웨어개발/운영/관리 프로세스를 비롯하여 소프트웨어 안전 관련 프로세스 확보가 미흡한 실정이므로, 전통적 제조업 분야에서 소프트웨어 안전과 관련한 프로세스 확충/개비할 수 있는 지원이 필요하다.

또한 소프트웨어 안전은 주로 제품 개발 및 테스트 단계에서 집중 관리되고 있었는데, 소프트웨어 안전 관리 품질을 향상시키기 위해서는 소프트웨어 안전 관리 프로세스 범위를 제품 개발 초기 단계에서 이후 단계까지 E2E 확장할 수 있도록(인증 및 사고 대응까지 포괄하는 프로세스) 유관 기관의 지원을 제공하는 것이 필요하다.

제4절 종합분석

본 절에서는 앞서 살펴본 소프트웨어 안전분야 학계・정부(Governing Sector), 소프트웨어 안전분야 사업기업(Supervising Sector), 소프트웨어 개발사용자(End User Sector) 각각의 영역별로 도출된 주요 시사점을 6개 카테고리(법・제도, 인증・매뉴얼・표준, 인력・교육, 조직・기관, 산업환경개선, 프로세스)로 구분하여 분석 및 정리하였다.

이러한 과정을 통해 3개 영역에서 공통적으로 중요한 사항으로 조사된 내용을 체계적으로 요약 및 정리하고 해당 내용을 제5장 Key Success Factor 정의 및 개선 방향 도출의 참고자료로 활용하여 분석과 개선안의 연계성을 강화하였다.

1. 소프트웨어 안전분야 학계・정부(Governing Sector)

법・제도 측면에서는 소프트웨어 안전사고 발생 시 대응체계와 사후 처리에 대한 내용을 법제화할 필요가 있다. 그리고 제4차 산업혁명과 함께 급부상한 주요 기술분야(인공지능, 빅데이터 등)에 대한 규제나 가이드라인 수립이 필요하다.

인증・매뉴얼・표준 측면에서는 국가 전략사업과 연계한 중점 표준화 추진 분야에 대한 장기적 지원과 국제표준 전문가 양성이 중요하다.

인력・교육 측면에서는 산업별 도메인 지식을 보유한 소프트웨어 안전분야 인력양성이 필요하다는 의견이 2015년, 2016년에 이어 지속적으로 제기되었다.

조직・기관 측면에서는 소프트웨어 안전 전문가를 보유한 전문기관 설립이 필요하다는 의견이 2015년부터 지금까지 지속적으로 제기되었다.

業 환경개선 측면에서는 TIC 기업의 역량향상을 위해 공공부문에서 소프트웨어 안전 프로젝트 참여기회를 최대한 제공하여야 하며, 소프트웨어 안전이 적용된 제품의 가치를 인정해주는 사회적 인식이 확산되어야 한다.

프로세스 측면에서는 특정 부처 영역에서 소프트웨어 안전관련 문제가 발생했더라도 해당 TFT에 소프트웨어 전문가가 포함된 범부처 차원의 통합적 대응을 할 수 있는 체계가 필요하다.

2. 소프트웨어 안전분야 사업기업(Supervising Sector)

법・제도 측면에서 소프트웨어 안전분야 법・제도의 구체화에 대한 요구가 2016년과 마찬가지로 매우 높게 나타났다.

인증・매뉴얼・표준 측면에서는 소프트웨어 품질중심의 기존 인증제도보다는 위험원 분석, 위험저감 방안 등이 요구사항과 설계단계에 반영되었는지 여부를 판단하는 것을 더욱 중요시하는 것으로 나타났다. 그리고 소프트웨어 안전과 관련된 노하우와 지적자산을 체계화한 매뉴얼과 Tool을 대부분 보유하고 있으며 고객사의 요구사항에 따라 커스터마이징하여 활용하고 있다.

인력・교육 측면에서는 산업별 도메인 지식을 갖춘 소프트웨어 안전 전문가가 수요에 비해 부족하므로 소프트웨어 개발자 재교육, 전문 프로그램 운영 등을 통해 소프트웨어 안전 전문가를 양성해야 한다.

조직·기관 측면에서는 소프트웨어 안전관련 전문가를 보유한 전문기관의 신설을 통해 소프트웨어 안전관련 사안에 대한 총괄적인 조정과 커뮤니케이션을 담당하는 것이 필요하다.

業 환경개선 측면에서는 다양한 산업 도메인 레퍼런스 확보가 향후 중요한 경쟁요소로 작용할 것이며, 해외 시장 진출을 위해 국제표준, 외국어, 실무경험을 갖춘 인력이 중요하다는 의견이 주를 이루었다.

프로세스 측면에서는 기존 QC 차원의 통합테스트에서 안전 및 품질예방 차원의 위험도 분석에 대한 중요도가 점차 높아지고 있는 것으로 조사되었다.

3. 소프트웨어 개발사용자(End User Sector)

법/제도 측면에서는 일반 사용자 기업이 소프트웨어 안전과 관련된 활동이나 시스템(프로세스, 매뉴얼, 인증 등)을 갖추기 위해서는 원가 측면의 부담이 발생하기 때문에, 소프트웨어가 사업의 핵심이면서 이미 법/제도로 안전 준수가 강제화된 기업들 외 일반 소프트웨어 사용 기업들은 자발적 도입이 어려워 소프트웨어 안전에 대한 국가 차원의 일정 비율 비용 부담이나, 관련된 혜택을 제공해 달라는 의견이 있었다.

또한 일반 사용자 기업들 입장에서는 원가 부담을 최소화하는 것이 일반적인 경영활동 방향이라 소프트웨어 안전 도입에 소극적이거나 동기 부여가 어려우므로, 법/제도 측면에서 최소한의 수준에서 준수해야 할 소프트웨어 안전 수준을 구체화/강제화하여야 한다는 의견도 있었다.

인증/매뉴얼/표준 측면에서는 대부분 신생 기업이나 대기업의 2차, 3차 하청으로 단계가 내려갈수록 인증/매뉴얼/표준이 필요하나 도입이 어려운 경우가 많았다. 이러한 기업들은 필수적으로 필요한 영역(제조 공정이나 프로그램 테스팅 등)에서 기업 내부적으로 소프트웨어 안전 관련한 활동을 수행하고 있었는데, 국가 차원에서 소프트웨어 안전 전문가 양성이나 Tool을 지원해 준다면 도움이 될 것이라는 의견이 있었다.

인력/교육 측면에서는 기업이 자발적으로 소프트웨어 안전 관련한 내부 전문가를 양성하거나 교육을 추진하기 어려우므로, 국가에서 소프트웨어 안전 관련한 체계적인 교육이나 전문가 양성 과정을 지원해 주기를 기대하였다.

조직/기관 측면에서는 소프트웨어 안전과 관련한 문제나 어려움을 해결하기 위한 정부의 소통 창구가 여러 조직에 분산되어 문제 해결의 진행이 어려운 상황이라 소통 창구의 일원화가 필요하다고 주장하였다.

業 환경개선 측면에서는 소프트웨어 안전과 관련한 사고 이력이나 테스팅 이력/노하우 등의 확보가 필요한데, 개별 기업 내부적으로 이를 확보/관리하기에는 인적, 금전적 자원의 조달이 어려워 국가 차원의 소프트웨어 안전 관련 사고 이력, 테스팅 정보 수집 및 공유 플랫폼을 지원해 달라는 의견이 있었다.

프로세스 측면에서는 대부분의 기업들이 소프트웨어 안전 관련한 사항이나 요구사항들을 제품/서비스 기획 초기단계부터 암묵적으로 반영하고 있는 것으로 확인되었다.

4. 종합분석

3개 영역별로 도출된 주요 시사점을 6개 카테고리로 구분하여 다음 표에 요약 및 정리하였다.

〈표 4-13〉 종합분석 시사점 요약

항목	Governing Sector	Supervising Sector	End User Sector
법・제도	• 소프트웨어 안전관련 대응 및 사후처리 방안 법・제도화 필요	• 산업별 소프트웨어 안전관련 법・제도의 구체화 필요	• 기업 측면 소프트웨어 안전 도입/강화에 따른 비용 부담 경감 • 법/제도적 강제화를 통한 소프트웨어 안전 최소 수준 보장 필요
	✓ 다양한 산업별 특성을 포함할 수 있는 상위관점의 소프트웨어 안전관련 법・제도 구체화 필요		

<table>
<tr><td rowspan="2">인증·
매뉴얼
·표준</td><td>• 전략적/장기적 관점의 국제 표준화 지원 필요
• 국제표준 전문가 양성 필요</td><td>• 형식적 인증보다 소프트웨어 안전요소 반영이 중요
• TIC업계에서 매뉴얼과 Tool의 활용이 일반화</td><td>• 신생 기업, 대기업의 하청 아래 단계로 내려갈수록 인증/매뉴얼/표준 구비 미흡
• 기업 내부적으로 필요에 의해 자체적으로 수행</td></tr>
<tr><td colspan="3">✓ 국제 표준화 주도를 위한 정부의 지원 및 표준전문가 양성 필요
✓ 현장에서 활용성 높은 매뉴얼과 Tool의 제작 필요</td></tr>
<tr><td rowspan="2">인력·
교육</td><td>• 소프트웨어 안전관련 인력난의 심화
• 소프트웨어 안전 전문가 양성 필요</td><td>• 소프트웨어 안전관련 전문가 부족
• 소프트웨어 안전 전문가 양성 필요</td><td>• 소프트웨어 사용 기업 실무자 교육 지원 필요</td></tr>
<tr><td colspan="3">✓ 소프트웨어 안전관련 전문가가 부족한 실정으로 전문인력 양성이 시급</td></tr>
<tr><td rowspan="2">조직·
기관</td><td>• 소프트웨어 안전역량을 보유한 전문기관 신설 필요</td><td>• 소프트웨어 안전전문가가 포함된 전문기관 신설필요</td><td>• 소프트웨어 안전 포함 소프트웨어 전반적 민원에 대한 소통 창구 필요</td></tr>
<tr><td colspan="3">✓ 소프트웨어 안전관련 전문성을 보유한 전문기관의 신설 필요</td></tr>
<tr><td rowspan="2">산업
환경
개선</td><td>• 공공부문의 소프트웨어 안전관련 레퍼런스 제공 필요
• 소프트웨어 안전의 가치 에 대한 사회적 인식 제고 필요</td><td>• 산업별 레퍼런스가 중요한 경쟁요소
• 해외시장 진출을 위한 전문인력 확보 필요</td><td>• 사고 이력, 노하우 정보의 수집이 개별 기업 단위로는 어려우므로 국차 차원의 수집 및 공유 플랫폼 필요</td></tr>
<tr><td colspan="3">✓ 소프트웨어 안전관련 국내외 레퍼런스 확보를 위한 노력 지속 필요
✓ 소프트웨어 안전의 중요성에 대한 사회적 인식 제고 필요</td></tr>
</table>

프로세스	• 소프트웨어 안전관련 문제 발생 시 범정부차원의 대응 필요	• 소프트웨어 안전 프로세스에서 사전 위험분석의 중요성 증대	• 소프트웨어 안전과 관련한 사고 이력은 제품 기획 초기 단계부터 적용하고 있음
	✓ 소프트웨어 안전 프로세스에서 통합테스트보다 사전 위험분석의 중요성 증대		

제5장 Key Success Factor 정의 및 개선 방향 도출

제1절 Key Success Factor

1. Key Success Factor 정의

국내 소프트웨어 현황 분석 결과 및 해외 벤치마킹 결과 확인한 선진 사례, 해외 TIC 시장의 변화 방향을 토대로, 시장/사업자, 인적/물적 자원, 관리 체계 및 표준 관점에서 국내 소프트웨어 안전 분야의 미래 발전 모습이나 Vision에 대해 정의하였다.

먼저 시장 및 사업자 측면에서는 사회 전반적, 산업 전반적으로 소프트웨어 안전에 대해 기업의 비용이나 시간, 인력을 할애하는 것에 대해 경영진과 실무자가 당위성을 인식하는 것을 미래 모습으로 정했다. 또한 제품/서비스에 소프트웨어가 일정 부분 또는 중요한 부분을 차지하는 경우 소프트웨어 안전에 대한 필요성을 인식하고 안전을 사업자 스스로 지키고 관리하는 것으로 상정하였다. 해외 TIC 시장의 변화 흐름 및 세계 시장 동향을 고려하여 제4차 산업 혁명을 촉진하는 자율주행자동차, 드론 등의 소프트웨어를 사업의 핵심으로 하는 신산업의 성장이 예상되어 소프트웨어 안전 분야도 기존 원자력, 철도, 국방 등 전통적 산업 분야에서 탈피하여 신산업 분야로 진출할 것으로 예상하였다. 마지막으로 국내 TIC 사업자들이 국내 및 해외 소프트웨어 안전 프로젝트 경험을 축적하고 해당 역량을 바탕으로 해외 진출하는 것을 최종 모습으로 하였다.

인적/물적 자원 측면에서는 소프트웨어 안전과 관련한 자산 확보 수준을 정의하였다. 인적 측면에서는 소프트웨어 안전 역량과 동시에 특정 산업 분야에 대한 개괄적 이해, 사업에 대한 이해를 모두 갖춘 인재상을 이상적인 목표로 하였고, 이들이 그러한 지식을 배경으로 소프트웨어를 사용하는 산업 현장의 말단까지 진출하여 현장에서 소프트웨어 안전을 적용하고 관리하는 모습을 최종 목표로 하였다. 또한 기업의 생산/판매/관리 활동에서 발생하는 소프트웨어 안전과 관련한 각 종 사례/이력이 국가차원에서 축적되고 자산화되어 다시 기업들에게 공유되는 순환 구조의 지식 공유 플랫폼을 갖추는 모습을 최종 미래 모습으로 상정하였다.

관리체계 및 표준 측면에서는 한국의 소프트웨어 전문가가 소프트웨어 안전과 관련한 국제 기구/회의에 참가하여 표준 제정 시 국내 소프트웨어 안전 산업에 도움이 되

는 방향의 의견을 반영하거나, 국제 표준에 대해 충분히 이해하여 국내 표준에 반영하거나 국내 소프트웨어 안전 관련한 사업체들에 해당 내용을 전파하는 것을 최종 미래 모습으로 정의하였다. 정부의 역할에 대해서는 소프트웨어 안전사고 대응 체계를 수립하고 소프트웨어 안전사고 발생 시 책임소재 규명과 피해보상 판정에서 공정한 중간자 역할을 수행하고, Safety Critical 소프트웨어를 사용하는 전 산업분야에 대해 소프트웨어 안전 체계 적용을 추진하고 이를 관리하는 역할을 수행하는 것으로 정의하였다. 민간 부문의 역할에 대해서는 산업계에서 자발적으로 소프트웨어 안전 표준과 관련한 인증을 확보하려고 노력하고, 이를 통해 사회 전반적인 안전 수준을 강화하는데 기여하고, 기업의 수출 경쟁력을 강화하는 것으로 최종 목표를 정했다.

이러한 소프트웨어 안전의 최종 목표, 발전 모습을 달성하기 위한 Key Success Factor를 정의하였다. 먼저 시장 및 사업자 측면에서, 소프트웨어 안전에 대한 지출에 대해 기업 경영자의 인식 변화와 제품/서비스가 소프트웨어를 매개로 하는 경우 안전에 대한 필요성의 인식을 제고하기 위해서는 ‘소프트웨어 안전에 대한 필요성 인식’ 전환/제고가 필요하다고 보았다. 인공지능, 자율주행자동차, 드론과 같이 제4차 산업 혁명의 주요 사업들에 맞춰서는 ‘소프트웨어 분야의 신산업과 접목된 소프트웨어 안전 사업 Item의 발굴’을 핵심 성공 요인으로 보았다. 또한 국내/외 소프트웨어 안전 경험을 축적하고 축적된 역량을 바탕으로 국내 TIC 기업들이 해외로 진출하기 위해서는 ‘소프트웨어 안전 Reference 확보’가 핵심이라고 보았다.

인적/물적 자원 측면에서는 소프트웨어 안전 역량과 산업 지식을 겸비한 인력 육성을 위해 ‘소프트웨어 안전 역량 확보’가 핵심이라고 보았고, 이러한 인력이 산업 현장 말단까지 침투하여 소프트웨어 안전을 적용하기 위해서는 ‘소프트웨어 안전 전문가 Pool을 확보하고 그 수급을 안정화’ 시켜는 것이 핵심이라고 보았다. 또한 소프트웨어 안전과 관련한 기업 내외부 축적된 지식을 국가 차원에서 관리하고 공유하기 위해서는 ‘소프트웨어 안전 지식 공유 플랫폼 구축’이 반드시 필요하다고 보았다.

관리체계 및 표준 측면에서는, 소프트웨어 안전 관련한 국제 표준 수립 협의에 참여하고 의견을 제시하기 위해 ‘소프트웨어 안전 국제표준 전문가 육성’이 핵심 성공 요인이라고 보았고, 소프트웨어 안전사고 대응 체계 수립 및 사고 발생 시 조정자 역할을 할 정부 추진체 및 소통 창구 제공을 위해서는 ‘Safety Critical 소프트웨어사용 전 산업분야에 소프트웨어 안전 체계 적용 산업별 소프트웨어 안전 도입/개비 지원’이 핵심이라고 보았다. 또한 산업 전반적 소프트웨어 안전 표준 인증 확보 통한 사회 전반적 안전 강화, 수출 경쟁력 강화를 위해서는 ‘소프트웨어 안전 표준 인증 지원’

이 핵심 성공 요인이라고 정의하였다.

<표 5-1> 소프트웨어 안전의 Key Success Factor 정의

구분	소프트웨어 안전 발전 모습/비전(Vision)	Key Success Factor
시장 및 사업자	• 소프트웨어 안전에 대한 리소스(인력/비용) 할애 타당성 인식 • 제품/서비스가 소프트웨어를 매개로 하는 경우 안전에 대한 필요성 공감대 형성 • 제4차 산업혁명을 촉진하는 소프트웨어중심 신산업 성장(AI 등)에 맞춰 원자력, 철도 등 전통적 소프트웨어 안전 분야 탈피, 신분야 개척 • 국내/외 소프트웨어 안전 경험 및 축적 역량 바탕 해외 진출	• 소프트웨어 안전 필요성 인식 • 소프트웨어분야 신산업 접목 소프트웨어 안전 사업 발굴 • 소프트웨어 안전 Reference 확보
인적/물적 자원	• 소프트웨어 안전 역량과 산업 지식을 겸비한 인력 양성 • 산업 현장 말단까지 소프트웨어 안전 역량 겸비한 인력 공급 • 소프트웨어 안전 관련 지적 자산의 국가 차원 공유	• 소프트웨어 안전 역량 확보 • 소프트웨어 안전 전문가 Pool 확보 및 수급 안정화 • 소프트웨어 안전 지식 공유 플랫폼 구축

관리체계 및 표준	• 소프트웨어 안전 관련한 국제 표준 수립 협의 참여 • 소프트웨어 안전사고 대응 체계 수립 및 사고 발생 시 조정자 역할 • Safety Critical 소프트웨어사용 전 산업분야에 소프트웨어 안전 체계 적용 • 산업 전반적 소프트웨어 안전 표준 인증 확보 통한 사회 전반적 안전 강화, 수출 경쟁력 강화	• 소프트웨어 안전 국제표준 전문가 육성 • 소프트웨어 안전 정부 추진체 및 소통 창구 제공 • 산업별 소프트웨어 안전 도입/개비 지원 • 소프트웨어 안전 표준 인증 지원

제2절 개선 방향

1. 개선 방향 정의

이상적인 목표나 비전으로부터 Key Success Factor를 도출하였으나, 실제 달성 가능한 목표와는 수준 차이가 있어 선진 사례를 통해 중장기적 목표를 설정하고 현재 수준과의 차이를 분석하여(Gap Analysis) 개선 방향/과제를 도출하였고, 이를 통해 총 16개 개선 방향/과제를 도출하였다.

도출된 전략 과제를 3대 개선 전략 영역으로 구분하였다.

[그림 5-1] KSF-개선방향-3대 개선 전략 도출

<표 5-2> KSF와 선진사례 국내 현황 비교 분석을 통한 개선방향 도출

KSF	목표 수준/선진 사례	현황	개선방향
소프트웨어 안전 필요성 인식	• 안전 검증이 기업활동 전제 조건 • 소프트웨어 안전도 안전 검증의 필수 요소로 인식 • 생산물에서 생산과정으로 소프트웨어 안전 인식 확대	• 소프트웨어 안전이 중요한 산업 외에는 소프트웨어 안전 낮은 인지도 • 소프트웨어 안전에 대해 비용 지출 최소화/지양 양상 • 중소기업 경영 여건 상 소프트웨어 안전에 투입할 여력 부족	• 사전예방 및 재발방지 체계 수립 및 강제화 • 중소기업 대상 소프트웨어 안전 체계 도입 지원

소프트웨어분야 신산업 접목 소프트웨어 안전 사업 발굴	• 해외 TIC 사업자들의 AI, 3D Printer 등 신산업 분야 개척 • Cloud, Big Data 기술 기반Digital TIC로의 전환	• 국내에서는 전통적 소프트웨어 안전 필요 산업(원자력, 철도, 국방) 외 소프트웨어 안전 도입 미흡	• 공공부문 발주 사업에 소프트웨어 안전 포함 • 제4차 산업 분야 육성 정책에 소프트웨어 안전 내용 포함
소프트웨어 안전 Reference 확보	• 국내 TIC사업자들의 해외 Reference 축적 (성숙 시장 노하우 습득)	• 해외 사업 경험 보유 기업 비율 50% 불과	• 국가 전략사업 연계 해외 Reference 확보 지원 • 기존 소프트웨어관련 인력의 교육을 통한 소프트웨어 안전 역량 제고
소프트웨어 안전 역량 확보	• 소프트웨어 안전 및 산업 지식을 겸비한 인재 양성	• 산업별/국가별 지식 및 실무경험 보유자 부족	
소프트웨어 안전 전문가 Pool 확보 및 수급 안정화	• 소프트웨어 안전 전문가 Pool 운영 • 소프트웨어 안전 실무자 안정적 공급	• 이전 조사와 마찬가지로 소프트웨어 안전 전문인력 부족	
소프트웨어 안전 지식 공유 플랫폼 구축	• 소프트웨어 안전 관련 검증/테스팅 이력, 안전사고 처리이력 축적 및 공유 • 정부 주도 데이터 수집 및 분석 플랫폼 구축 사례 (일본 드론 정보 관리 시스템 등)	• 소프트웨어 안전사고 이력 수집/관리 기업 소수 불과 (40% 미만) • 주로 기업 내부 전파/공유되어 노하우 사장 • 수집 데이터도 양과 품질면에서 활용 어려운 상황	• 소프트웨어 안전 관련 테스팅/사고이력 수집 시스템 구축 • 사례 분석 결과 기업 공유 • 정부 정책 수립 시 소프트웨어 안전 관련 사례 분석 결과 활용

소프트웨어 안전 국제표준 전문가 육성	• UN, ISO, IEC 등 국제표준 제정 관련 기구 참여 • 국제 표준의 국내 표준화 또는 국내 산업 반영	• 국제 표준 기구 참여 한국 인력 부족 • 국제 표준의 국내 표준 반영, 산업 반영 시차 발생	• 국제 표준 기구의 국내 전문가 참여 • 소프트웨어 안전 표준 연구전담 기관 운영
소프트웨어 안전 정부 추진체 및 소통 창구 제공	• 신산업 육성을 위해 느슨한 법/규제 적용 (가이드라인 수준) • 융복합 성격 사업에 대해 정부부처간, 정부/민간 협의체 구성	• 소프트웨어 안전 관련 정부 지침, 가이드 전파 미흡 • 소프트웨어 안전 관련 정부 소통 채널 불명확, 정부 기관별 업무 분산 민원 처리 장시간 소요	• 소프트웨어 안전 관련 민간 교육/전파 실시 • 소프트웨어 안전 관련 정부 소통 협의체 구성 및 정부 채널 단일화
산업별 소프트웨어 안전 도입/개비 지원	• 미국/유럽/일본은 정부 주도 산업별 소프트웨어 안전 표준 및 문제 발생 방지를 위한 관리 체계, 법/규제 도입 • 업계 자발적 소프트웨어 안전 도입 움직임	• 원자력 등 일부 분야 제외 소프트웨어 안전 법/규제 정비 미진 • 산업계 자발적 안전 지향 움직임 미흡 • 제조업 분야, 중소기업 소프트웨어 안전 인식 및 관리 취약 • 특히 제조업 분야 설비 투자 둔화로 소프트웨어 안전 도입 지연	• 산업 육성 정책과 문제발생 방지 위한 규제 병행 • 제조업 분야 소프트웨어 안전 도입 지원 방안 수립

소프트웨어 안전 표준 확보 지원	• 생산과정/제품에 소프트웨어적용하는 기업들의 소프트웨어 안전 인증 획득	• 소프트웨어 인증 확보 기업 소수 불과 (40% 미만) • 중소기업의 소프트웨어 안전 인증 확보 여력 부족 (예산, 인력) • 소프트웨어 안전 관련 인증 획득 시 정부 지원 미흡	• 중소기업 소프트웨어 안전 인증 획득 지원

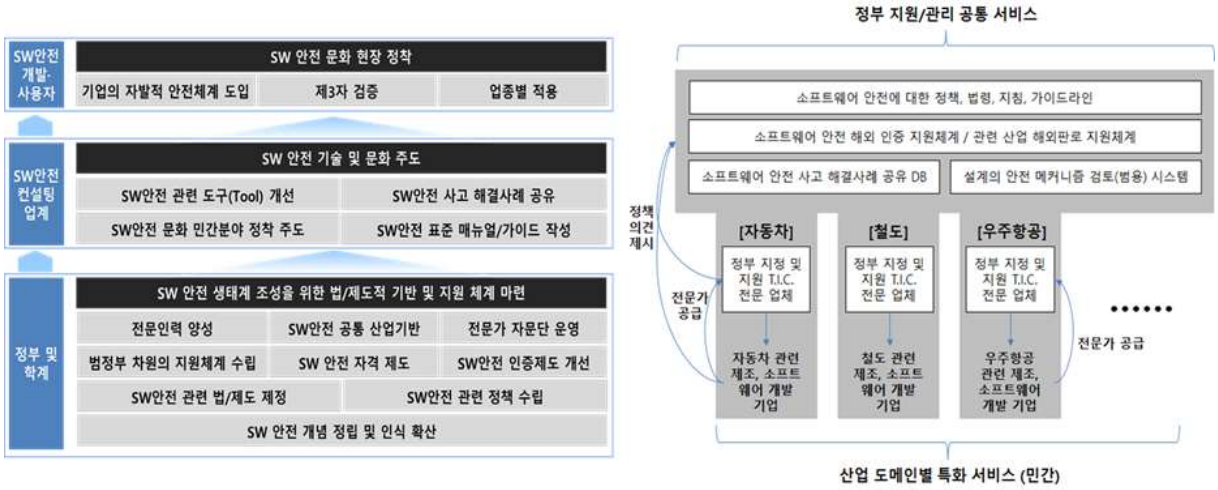
제6장 국내 소프트웨어 안전 산업 활성화 방안

제1절 개요

국내 소프트웨어 현황 분석 결과 및 해외 선진 사례 분석 등을 토대로, 각 분야별 핵심성공요소(KSF)[129]를 도출하였고, 이를 핵심성공요소 별 국내 소프트웨어 현황 분석 결과와 해외 선진 사례 분석 결과를 비교분석하여(Gap Analysis) 주요 개선 과제를 도출하였다. 도출된 개선 과제를 법·제도, 관리 기관, 표준/규정/가이드의 측면에서 국내 소프트웨어 안전 산업 활성화 전략 및 과제를 도출하였고, 이를 토대로 미래 모형을 그려 보았다.

2015년 및 2016년 조사에는 주요 3대 Player (정부 및 학계 부문, 소프트웨어 안전 컨설팅 부문, 소프트웨어 개발·사용자 부문)을 아우르는 국가 차원의 개선전략 및 미래모형과 이를 지원하기 위한 범정부 소프트웨어 안전 플랫폼(안) 등이 제시 되었는데, 국내의 소프트웨어 안전 산업 및 정책 등의 환경은 큰 변화가 없어 기존 개선전략 및 미래모형은 큰 변화가 없다.

[그림 6-1] 국가 차원의 3 Layer 미래 전략 및 범정부 소프트웨어 안전 플랫폼



자료: 2016년 소프트웨어 안전 산업 동향

129) Key Success Factor

제2절 활성화 방안

소프트웨어 안전 산업은 비자발적인 특성을 가지고 있으며, 현재 국내 소프트웨어 산업이 아직 태생 단계인 관계로 일차적으로 정부 차원의 선도가 필수적인 부분이다. 따라서 이번 연구에서는 정부 차원에서 국내 소프트웨어 안전 산업을 선도하고, 업 환경을 변화 시키며, 나아가 세계적으로 선도하기 위해 필요한 전략 및 미래모형에 대해서 그려보았는데, 법・제도, 관리기관, 소프트웨어 안전 표준, 지침, 가이드 측면의 3개 측면에서 미래모형을 제시하였다.

1. 법・제도

기존 연구에서는 소프트웨어 안전 법・제도 제정이 필요하다고 했다면, 이번 조사에서는 좀 더 구체적으로 어떠한 법・제도가 필요하며, 어떠한 방향성을 가져야 되는지 제시해 보았다.

• 법・제도 제정 방향성

이머징 산업을 포함한 대부분의 산업의 경우, 국내 산업 발전과 해외 선도를 위해 이를 적극적으로 지원, 육성하는 방향성이 필요한데, 공공안전이 필수적인 일부 경우를 제외 하고는 법/규제를 느슨하게 하여 산업이 자발적으로 활동할 수 있는 기회를 최대한 보장하도록 하는 것이 필요하다. 또한, 해외 동향을 편승하되, 국내 산업, 문화, 국민 정서 등을 고려하여, 법・제도 규정이 필요하다. 타 산업 분야 법・제도를 적극 참고하고 활용해야 한다. 이머징 산업 분야의 경우, 산업 태동기에 발전을 위한 초석이 될 수 있도록, 산업에 대한 정의, 규제 범위, 규제 기관 및 책임/권한, 안전에 대한 상위 수준의 포괄적 법・제도 제정이 필요하다.

1. 법・제도의 규제 수준을 낮게 하여, 국내 산업이 자발적으로 발전 지원
2. 해외 동향을 고려하되, 국내 산업, 문화, 정서를 고려
3. 타 산업 분야 법・제도 적극 참고 및 활용
4. 이머징 산업의 경우, 산업 정의, 규제 범위, 규제 기관, 안전 책임에 대한 부분

을 제시하는 법·제도 우선 제정 필요

• 법·제도 내용

3번의 소프트웨어 안전 산업 조사를 통해 도출된 법·제도 부분 주요 내용을 개선 방안으로 정리하면 아래와 같다.

1. 국내 소프트웨어 안전을 위한 법·제도

가) 국가 발주 프로젝트에 소프트웨어 안전 포함 의무화

나) 공공부문의 소프트웨어 안전성 요구사항 준수 규정 법제화

다) 안전 중요 산업별 특성을 반영한 소프트웨어 안전관련 법·제도 상세화

라) 사전예방 및 재발 방지를 위한 원인분석 및 사후 처리 법제화

마) 국가 소프트웨어 안전을 총괄 할 수 있는 체계 법제화

2. 국내 소프트웨어 안전 산업 업 환경 개선을 위한 법·제도

가) 이머징 산업 분야 법·제도화 (소프트웨어 안전 포함)

나) 소프트웨어 및 소프트웨어 안전 대가 현실화

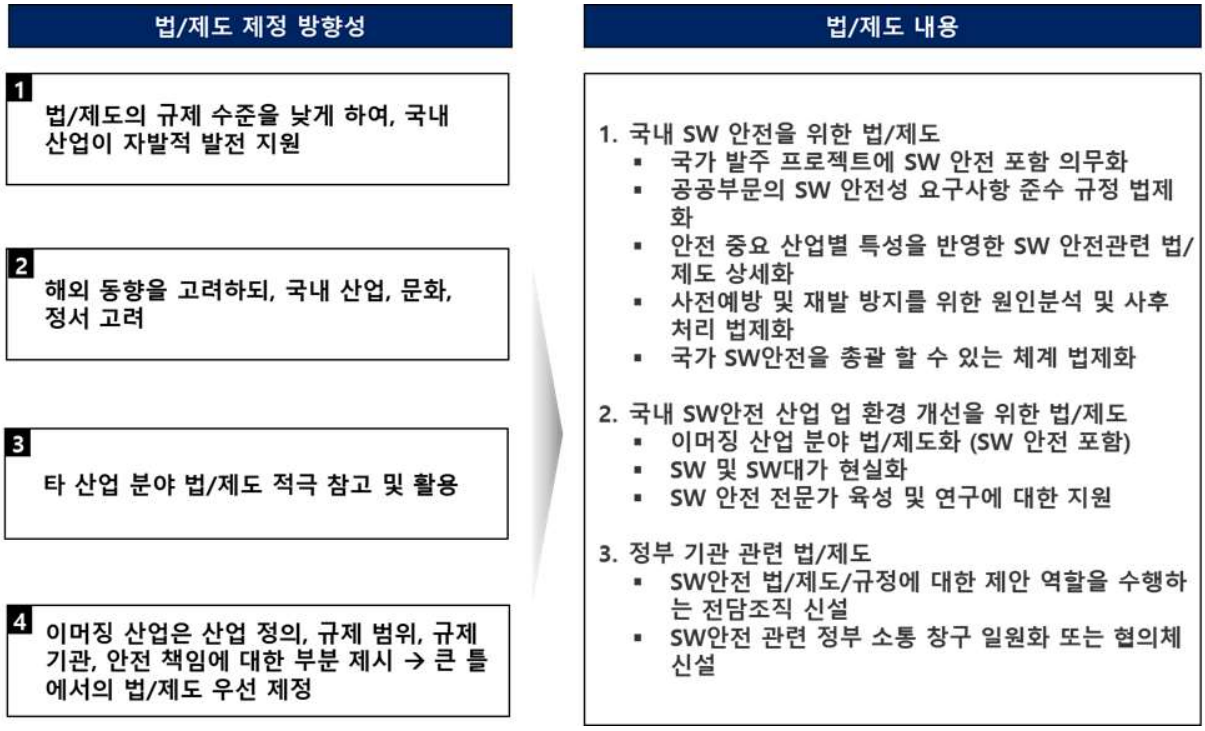
다) 소프트웨어 안전 전문가 육성 및 연구에 대한 지원

3. 정부 기관 관련 법·제도

가) 소프트웨어 안전 법·제도/규정에 대한 제안 역할을 수행하는 전담조직 신설

나) 소프트웨어 안전 관련 정부 소통 창구 일원화 또는 협의체 신설

[그림 6-2] 소프트웨어 안전 법·제도 제정 방향성 및 주요 내용



2. 관리기관

최근 해외 동향에서 보았듯이, 주요 산업들이 고도화 되고 융복합화 되면서, 여러 산업 도메인을 걸쳐서 영향을 주고받는 경우가 급증하고 있다. 기존 정부기관은 산업별로 나누어져 각 해당 분야별로 전문적인 규제, 관리, 지원 등을 하고 있으나, 융복합화 되는 현 시점에서 이를 기존 전문성 및 역할을 유지하면서, 이를 보완해야 할 필요가 대두된다. 해외 사례에서는 이를 보완하기 위해 2가지의 방안으로 진행되고 있는데, 1. 국가 기관, 산업체, 표준 기관 등이 모인 협의체 구성, 2 타 국가 기관, 산업체, 표준 기관의 참여하여, 주관 기관이 이를 조정하여 협업하는 방안이 그것이며, 2가지 방안이 동시에 진행되는 경우도 있었다.

소프트웨어 안전의 경우, 소프트웨어 지식도 중요하지만 우선적으로 해당 산업 분야의 지식(도메인 지식)이 필수적이며, 최근 이머징 산업인 자율주행차, 드론 등의 산업 분야 융복합화가 급격히 진행되고, 소프트웨어 안전이 핵심적인 부분이라 소프트웨어 안전을 위해서는 여러 산업 분야 국가 기관뿐만 아니라 산업체, 연구기관의 협업은 필

수적이다.

상기 트렌드를 고려한 관련기관의 요건 및 주요 활동은 아래와 같다.

- 요건

1. 소프트웨어 개발, 테스트에 대한 역량 보유
2. 협업 및 업무 조율 역량 보유
3. 법·제도 등 정책에 대한 연구, 분석, 제안 능력 보유
4. 해외 관련 기관과 교류 및 정책 협업을 위한 역량 보유

- 주요활동

1. 국가 소프트웨어 안전 관리 및 보장 활동

가) 국가 소프트웨어 안전 프레임웍 및 방향 수립

나) 국가 프로젝트의 소프트웨어 안전 부분 요건 기본 요건 정의 및 관리

다) 공공 부문 소프트웨어 안전성 요건 정의 및 관리

라) 국가 발주 프로젝트에 소프트웨어 안전 포함 의무화

마) 사전예방 및 재발 방지를 위한 원인분석 및 사후 처리

바) 소프트웨어 안전 관련 정부 단일 소통 창구

2. 국내 소프트웨어 연구 및 정책, 가이드, 지침 제안

가) 소프트웨어 안전 관련 법·제도, 정책, 가이드, 지침 등을 연구

나) 타 기관, 산업, 연구소의 소프트웨어 안전 연구 지원 및 협업

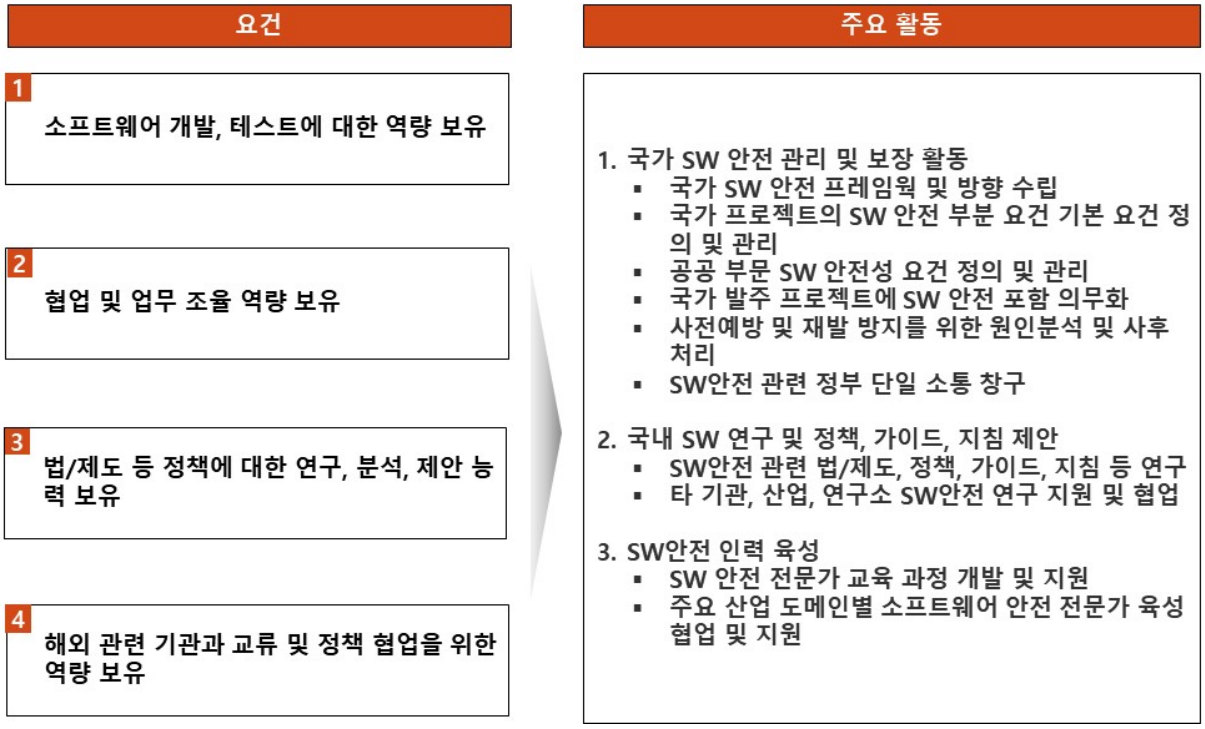
3. 소프트웨어 안전 인력 육성

가) 소프트웨어 안전 전문가 교육 과정 개발 및 지원

나) 주요 산업 도메인별 소프트웨어 안전 전문가 육성 협업 및 지원

3. 소프트웨어 안전 표준, 지침, 가이드

[그림 6-3] 소프트웨어 안전 관리기관 주요 요건 정의 및 활동



기존 소프트웨어 안전 관련이 높은 산업은 국내에서도 소프트웨어 안전 표준, 지침, 가이드가 상세히 정리되어 있고 해외 표준도 존재하고 있으나, 이머징 산업의 경우 국내, 해외 모두 표준, 지침, 가이드가 없는 상황이다. 또한 향후, 이러한 융복합적인 이머징 산업이 지속적으로 나타나고 성장 할 것으로 예상되므로, 특히 소프트웨어 안전이 중요한 융복합 이머징 산업의 경우 선도적인 차원에서의 소프트웨어 안전 표준, 지침, 가이드 제정이 시급한 상황으로 보인다. 이러한 요구에 부합하는 소프트웨어 안전 표준, 지침, 가이드 개발을 위한 전략이 필요한데, 여기서는 이러한 개발을 위한 전략을 제시하였다.

- 개발 전략

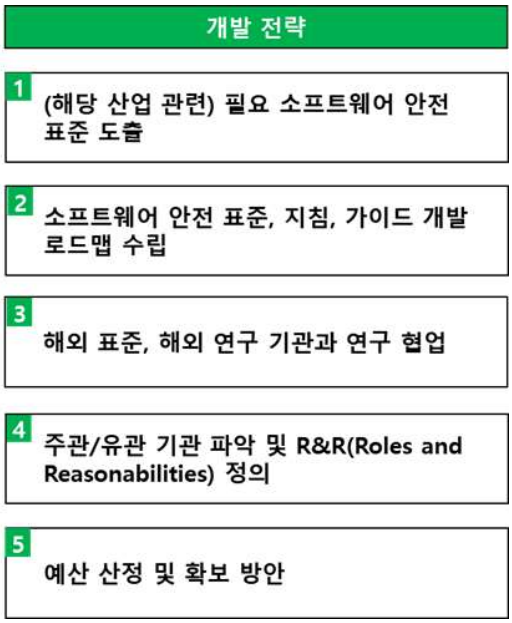
1. (해당 산업 관련) 필요 소프트웨어 안전 표준 도출
2. 소프트웨어 안전 표준, 지침, 가이드 개발 로드맵 수립

3. 해외 표준, 해외 연구 기관과 연구 협업

4. 주관/유관 기관 파악 및 R&R(Roles and Reasonabilities) 정의

5. 예산 산정 및 확보 방안

[그림 6-4] 소프트웨어 안전 표준, 지침, 가이드 개발 전략



제7장 결론 및 향후 과제

2018년 조사에서는 2016년, 2015년 대비 소프트웨어 안전에 대한 국내 산업의 이해 및 인지도가 다소 높아 진 걸로 조사되었다. 특히 소프트웨어 안전과 무관한 산업의 기업에 대한 조사 범위를 확대 했음에도 불구하고 소프트웨어 안전에 대한 인식이 높아 진 것은 고무적으로 해석된다.

이번 국내 현황 조사 결과에 대한 답변은 기존 조사 대비해서 크게 달라 진 것은 없었는데, 이는 첫째로는 국내 소프트웨어 안전 법·제도, 기관 측면의 변화가 아쉽게도 3년 전과 비교하여 지금도 큰 변화가 없어 아직 성장을 위한 제도적 토양이 마련되어 있지 않았고, 두 번째는 소프트웨어 안전 산업이 가지는 특성 상, 소프트웨어 안전에 대해 대응 하는 방법 또한 기존 대비 큰 차이가 나지 않았다. 예를 들면, 소프트웨어 안전에 대한 수요가 큰 분야는 안전이 중요한 산업인 자동차, 항공, 원자력, 철도 등에 집중되어 있었고, 소프트웨어 안전 활동을 수행 하는 이유도 고객사의 요구(구매처의 요구), 정부의 규제 등으로 자발적이기 보다는 비자발적 강제화 요건 기인하는 경우가 많았다.

비자발적 강제화 요인에 의해 움직이는 소프트웨어 안전 활동은 국내 제조/서비스 기업이 해외 수출 또는 국내 안전 중요 산업 분야에 제품/서비스를 제공할 때, 자체적으로 수행하는 경우도 있지만, 국내외 소프트웨어 안전 전문 기업(Supervising Sector)을 활용하여 소프트웨어 안전 컨설팅, 테스팅, 인증 등의 활동을 하는 경우가 많았다. 특히, 국내외 소프트웨어 안전 전문 기업을 활용할 경우, 이를 제공하는 형태는 국내 소프트웨어 안전 전문 기업 단독, 해외 전문 기업 단독, 국내외 기업이 함께 수행하는 경우 등 여러 가지 형태로 나타났는데, 특히 해외 전문 기업 단독 또는 협력으로 국내 소프트웨어 안전 서비스를 수행하는 주된 이유는 국내 소프트웨어 안전 전문 기업이 해당 분야의 글로벌 레퍼런스 및 전문 인력 부족으로 조사 되었다. 이는 비단 2018년에 국한된 결과가 아닌 지난 조사에서도 유사한 결과로 도출된 내용이기도 하다.

이러한 비자발적 특성 및 국내 시장 규모를 감안한다면, 국내 소프트웨어 안전 활동의 성장 및 정착이 산업 분야별로 자발적으로 가능하기 보다는 초기 단계에는 법/규제의 강제화를 통한 산업 및 사회적인 인식 정착 및 저변화가 선행 되어야 한다고 판단된다. 특히, 안전이 중요한 이머징(Emerging) 산업 분야의 경우 다수의 해외 선진국

은 큰 틀에서의 중장기 발전 로드맵(Roadmap) 및 법·제도를 만들고 있어, 국내에서도 시급하게 최소한 큰 틀에서의 발전 로드맵 및 법·제도를 제정하여, 이머징 산업이 안정적으로 성장할 수 있는 제도적 토양을 마련하는 것이 필요하다.

법·제도적인 틀을 제정함과 동시에 이를 전문적으로 수행할 기관이 필요한데, 이 기관은 해외 사례에서 조사되었듯이, 법·제도 연구 및 제정, 안전 표준 수립 및 법·제도 제정을 위한 유관 기관과의 협업, 국내 소프트웨어 안전 정착을 위한 규제 활동을 수행해야 하는데 각 산업 도메인의 지식이 필수적인 소프트웨어 안전의 특성상 이 기관은 각 분야별 소프트웨어 안전에 대한 규제 활동을 수행하기보다 각 산업 도메인별 규제 기관과 협업하여 이들 기관이 소프트웨어 안전 활동을 잘 수행할 수 있도록 가이드하거나 이들 기관이 타 유관 기관과 협업이 필요 할 때 이를 전체적으로 조율해 주는 역할을 수행하는 것이 바람직하다.

앞에서도 밝혔듯이, 3년 전과 비교하여 국내 소프트웨어 안전 활동은 조금씩 활발해지고 있긴 하나 해외 선진국의 활동에 비해 여전히 부족한 바가 많은데, 이를 위해서는 시급하게 법·제도 및 전문 기관이 우선적으로 만들어져 제도적인 활동 기반이 마련되어야 하며, 이를 토대로 지난 연구 결과 제시한 국내 소프트웨어 안전 활동 정착을 위한 로드맵 수립 및 전략 과제 수행, 그리고 범정부 플랫폼을 통해 국내 산업에 적용하고 성장 발전 시켜야 할 것으로 생각된다.

[그림 7-1] 소프트웨어 안전 발전 로드맵

참 고 문 헌

국내 문헌

SPRi (2017), 『소프트웨어 안전(Safety) 산업 동향 조사』

유병선・신동진・장재호・박정민・강자영 (2018),『원격 조종 항공기 시스템의 인증 표준화 전략』

한국경제연구원, (2016), 『우버 비즈니스 모델의 정책적 시사점』

해외 문헌

30年に千億円市場　業務用ドローン (니혼게자이신문), 2015.7, https://www.nikkei.com/article/DGXMZO88951410W5A700C1000000/

Act, AV START. "S. 1885, 115th Cong. (2017)."

Act, SELF DRIVE. "HR 3388, 115th Cong.(2017)."

Automated and Electric Vehicles Act 2018, Available: http://www.legislation.gov.uk/ukpga/2018/18/contents/enacted

Barclays (2018), TIC Market Prospection Report; Capital IQ (2017), M&A across Sectors

Barclays, 2018; Markets and Markets, 2018; Market Research Future, 2018;

Barclays, TIC Trend Report, 2018; TIC 주요 사업자 10개사 2016년, 2017년 사업보고서

Bundesministerium für Verkehr und digitale Infrastruktur. (2017), "Ethics Commission Automated and Connected Driving."

Bundesrepublik Deutschland. (2017). "Straßenverkehrsgesetz." Available: https://dejure.org/gesetze/StVG/.htm

Bureau Veritas, 2017년 사업보고서

CAAC(2018), Low-Altitude Connected Drone Flight Safety Test Report

CCAV. (2018). "UK Connected & Autonomous Vehicle Research & Development Projects."

Congress, U. S. "National defense authorization act for fiscal year 2018." (2017).

"Department for Transport & Department for Transport and the Centre for Connected and Autonomous Vehicles, (2016c). ""Pathway to Driverless Cars: Proposals to support advanced driver assistance systems and automated vehicle technologies.""

Department for Transport. (2015a). "The Pathway to Driverless Cars: A Code of Practice for testing."

FAA Modernization and Reform Act of 2012, Public Law 112-95, Sec. 903, US Government Printing Office, Feb. 2012. Available: https://www.congress.gov/112/plaws/publ95/PLAW-112publ95.pdf

GIZ. (2018). "Defining the Future of Mobility: Intelligent and Connected Vehicles (ICVs) in China and Germany."

https://www.gleisslutz.com/en/automated%20driving.html-0

Intertek, "2017년 사업보고서"

Japan Automobile Manufacturers Association. (2018). "自動運転に関する国土交通省の取り組み"

MIIT & CSA. (2017). "Guideline for Developing National Internet of Vehicles Industry Standard System (Intelligent & Connected Vehicle)."

Morris, R., & Thurston, G. (2015). "Registration and Marking Requirements for Small Unmanned Aircraft. Technical Report RIN 2120-AK82, Federal Aviation Administration."

NCSL. (2018). “Autonomous Vehicles: Self-Driving Vehicles Enacted Legislation.“

NHTSA. (2017). “Automated Driving Systems 2.0: A Vision For Safety.“

SAC. (2017). “드론을 위한 표준 시스템 제작 가이드“

SGS, 2017년 사업 보고서

Taeihagh, A., & Lim, H. S. M. (2018). “Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks.“ Transport Reviews, 1-26.

TIC outlook, Barclays. (2018). “매출 상위 10대 기업 ’17년 Annual Report“

UK Department for Transport. (2017). The Key Principles of Cyber Security for Connected and Automated Vehicles.

경제산업성 드론 전략 로드맵, 2018

경제산업성 정책회의: 부처간 회의, 민관 협의회 회의록, 2018

교통환경뉴스, 2018.8.31.

国土交通省(국토교통성), 2017

유럽항공안전청

自動運転 `安全要件で開発促進 国際標準狙う(자동 운전, 안전 요구 사항 개발 촉진 국제 표준 노린다),日本経済新聞(니혼게자이신문), 2018.6, 자동운전차의 안전기술 가이드라인, 국토교통성, 2018.9

自動運転に関する国土交通省の取り組み(자동운전에 대한 국토교통성의 대응), Japan Automobile Manufacturers Association, 2018

항공법,e-Gov. http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=327AC0000000231_20170530_428AC0000000051&openerCode=1)

부록 1 : 소프트웨어 안전분야 학계·정부(Governing Sector) 설문지

1. SW 안전에 대한 정의와 개념을 어떻게 보시는지 설명을 부탁드립니다.

2. 법/제도/정부

- SW 안전을 위해 법/제도를 추가하거나 수정되어야 할 항목이 있다면 어떠한 것들이 있으며, 어떤 식으로 개선되어야 합니까?
- SW 안전 관련 국가 차원의 대응 체계가, 필요하다고 보십니까? 필요하다면, 어떠한 식으로 구성되어야 한다고 보십니까?
- SW 안전의 종합관리 차원에서 정부 내의 각 부처와 기관들은 각각 어떠한 역할이 필요하다고 보십니까?

3. 표준화

- SW 안전 관련된, 국제 표준화 활동은 어떠한 것들이 있으며, 동향은 어떠한가요?
- 국제 표준화 제정에 우리나라가 참여하고 있다면, 어떤 부분이며 참여하고 계신 분들이나 단체는 어떠한 것들이 있나요?
- 국제 표준화 제정과 관련하여, 정부의 지원이 필요하다면 어떠한 것들이 있을까요?

4. Local(Market)

- 국내 SW 인증 및 컨설팅 사업의 현황에 대해서는 어떻게 보십니까?
  - 개별 기업측면에서의 개선 필요사항은 무엇이고, 인프라 측면에서의 필요사항은?
- SW 안전이란 측면에서 향후 국내 시장의 전망은 어떻게 보십니까?
- SW 안전을 시장원리로 뿌리내리고, 산업적으로 활성화하기 위해서 어떠한 환경이 조성 혹은 지원되어야 한다고 보십니까?
- 산/학/연 연계차원에서 SW 안전을 위해 공동으로 모색할 부분이 있다면 무엇입니까?

5. Global

- SW 안전측면에서, 선진국 여건과 국내 여건을 비교해 가장 큰 Gap은 무엇이라고 보십니까?
- 선진국의 SW안전 관련 법/제도 중, 국내에 도입이 필요한 것들은 어떠한 것들이 있으며, 어떠한 식으로 도입 되는 것이 바람직 할까요?
- 선진국의 SW안전 체계(국가차원의 프로세스, 조직/R&R) 중, 국내 도입이 필요한 것들은 어떠한 것들이 있으며, 어떤 식으로 도입하는 것이 바람직 할까요?
- 선진국은 SW 안전관련 Time과 Cost를 수반한 다양한 절차와 요건을 요하고 있는데, 국내에는 어떻게 준용하는 것이 적합한지 의견을 주시기 바랍니다.
- 선진국/선진사와 같은 수준에 도달하기 위해 필요한 것은 무엇이라고 보십니까?

부록 2 : 소프트웨어 안전분야 사업기업(Supervising Sector) 설문지

Ⅰ. 기업 일반 현황

1. 귀사에서 정의하는 SW 안전(Safety)의 개념은 무엇입니까? (다중 선택 가능)

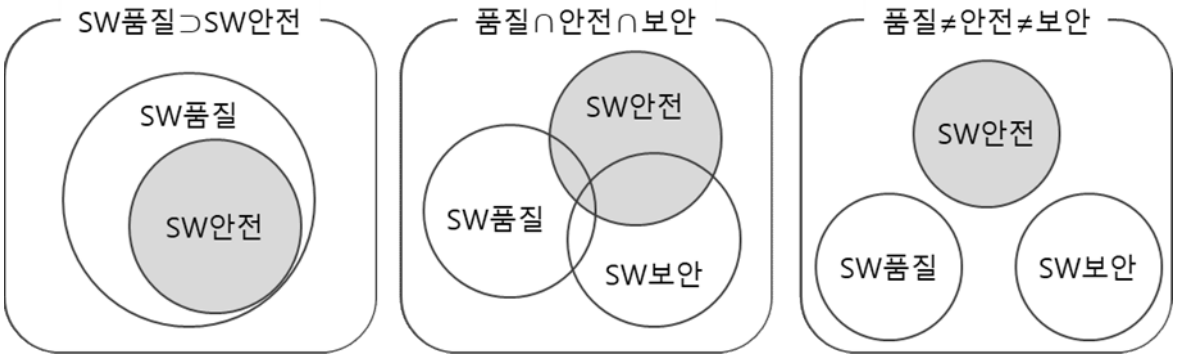
① SW안전은 성능, 기능, 코드가 요구사항 및 설계내역에 부합하는지 여부 (품질관점)

② SW안전은 외부의 악의적 공격으로부터 방어할 수 있게 어 있는지 여부 (보안관점)

③ SW안전은 예기치 못한 외부 환경 변화에 의하여 소프트웨어가 원인이 된 사고가 발생하는 것에 대한 회피 Mechanism 보유 여부

2. SW 안전(Safety), SW 품질(Quality), SW 보안(Security)의 관계를 그림으로 그린다면, 어떻게 표현 될 수 있나요?

(예시)



3. 귀사의 SW 인증/검증 관련 주요 고객의 산업군과 고객사는 어디입니까? (복수 선택 가능)

① 철도 ② 자동차 ③ 원자력 ④ 우주항공 ⑤ 의료 ⑥ 정보통신(IT서비스)

⑦ 기타 ( )

※ 고객사 :

3-1. 고객사에서 SW인증/테스트/검사/안전에 대하여 의뢰하는 대상은 어떠한 것들이며, 어떠한 항목에 대해서 주로 요청하고 있습니까?

3-2. 위 해당 산업에서 준수하고 있는 국내/외 안전관련 표준이 있습니까? 있다면 무엇입니까?

3-3. 귀사에서 고객사에 제공하는 서비스, 상품 유형을 선택해주시기 바랍니다. (다중선택 가능)

① 도구(Tool) 기반의 품질, 안전 서비스

② 용역 중심의 품질, 안전 서비스

③ 품질, 안전 진단 관련 도구(Tool) 판매

④ 품질, 안전 교육 및 인증 지원 컨설팅

⑤ 기타 ( )

3-4. 서비스/상품의 주요 내용 또는 주요 업무를 모두 선택해주시기 바랍니다. (다중선택 가능)

① 개발된 소프트웨어/제품에 대한 시험/검사/평가 (성능, 신뢰성 등)

② 소프트웨어/제품 개발/제작에 대한 품질 및 품질관리체계 컨설팅

③ 개발업체 대한 품질/안전 관련 인증 또는 인증 지원

④ 소프트웨어/제품 설계 타당성 검증 및 지원

⑤ 소프트웨어/제품 개발 공정에 대한 품질, 안전 관점 컨설팅

⑥ 기타( )

4. SW안전(품질/테스트/인증 등 포함) 관련한 매뉴얼이나 Tool이 존재합니까?

① 그렇다 ② 그렇지 않다

4-1. 존재한다면 어떠한 영역이며, 활용은 어떻게 하고 있습니까?

4-2 존재한다면, 각 서비스별로 어떠한 Tool이 있습니까?

4-3. SW안전을 위해 추가로 필요한 표준/매뉴얼은 무엇입니까?

5. 귀사에서 SW인증/검증(또는 SW안전) 업무 수행 시 이에 대하여 필요한 자격증이나 자격요건이 있습니까? 있다면 어떠한 것들이 있습니까? (예. SW Safety, SW 테스팅 등)

5-1. 귀사는 상기 분야 별, 몇 명의 자격증 보유자가 계십니까? 자격증을 발급한 기관 또는 기업은 어디입니까? (도메인-자격증-발급기관-인원수)

5-2. 실제 SW안전 프로젝트에 참여한 인력은 얼마나 있습니까? (국내 / 국외 Project 구분) (최근 3년간)

5-3. 해외사업자의 브랜드/인력/노하우를 소싱하고 계십니까?

① 그렇다　② 그렇지 않다

5-4. 소싱하고 있다면, 어떠한 이유로 소싱하고 계시며, 비중은 어느정도 입니까?

5-5. 해외사업자의 브랜드/인력/노하우를 소싱하기 위해 어떠한 계획 혹은 수행을 하고 있습니까?

5-6. SW안전 전문가 확보/육성을 귀사가 계획하거나 수행하고 있는 부분은 무엇입니까?

6. 귀사가 보유한 SW 인증/검증 (또는 SW안전 메커니즘) 관련 특허가 있다면 무엇입니까?

7. SW안전(품질/테스트/인증 등 포함) 산업에서 국내 선진 Player는 누구이며, 해당 Player의 강점은 무엇이라고 보십니까? 해외 선진 Player는 누구이며, 해당 Player의 강점은 무엇이라고 보십니까?

7-1. 귀사가 해외 선진 기업 또는 국내 경쟁사 대비 강점/경쟁우위는 무엇입니까?

① 가격

② 영업력 (영업인력 역량, 고객과의 관계)

③ 접근성(거리, 시간, 인력 등)

④ 기술력(특허 등)

⑤ 솔루션 및 Tool

7-2. (국/내외) 선진 기업 수준의 경쟁력을 확보하기 위하여 귀사가 보완해야 할 역량/경쟁요소는 무엇입니까?

8. 귀사는 SW안전 사업 관련하여 해외 진출 경험이 있거나, 해외에 진출한 상태입니까?

①예　② 아니오 (8번 질문으로 이동)

8-1. 어느 국가에 어떤 형태, 어떤 사업 영역으로 진출했거나 진출 중입니까? (예. 2017년 초반, UAE의 원전 XXX설계, 현지 합자회사 설립)

8-2. 해외 진출 동기는 무엇입니까? (예. 발주처의 요청으로)

8-3. 해외 진출 과정 또는 진출한 이후 애로 사항 또는 정부차원에서 지원이 필요한 사항이 있었습니까?

9. 귀사의 SW안전 사업 관련하여 해외진출 계획이 있습니까?

① 그렇다 ② 그렇지 않다

9-1. 그렇다면 어떤 지역에, 어떤 제품과 서비스를 계획 (또는 제공)하고 계십니까?

(예: 중국의 인프라를 대상으로 한 안전 컨설팅, 개발도상국에 대한 국내 인증시스템 체계 구축지원)

9-2. 해외 진출을 위해 갖춰야 할 역량은 무엇이라고 생각하십니까?

9-3. 해외 진출을 위해 진행 또는 준비하고 있는 사항은 무엇입니까?

Ⅱ. SW안전 프로세스 현황

1. 귀사의 제품개발 혹은 컨설팅 시 비용과 기간측면에서 'SW안전' 이 차지하는 비중은 얼마나 됩니까?

① 0 -10% 미만 ② 10 - 20% 미만 ③ 20 - 30% 미만

④ 40 - 50% 미만 ⑤ 50 % 이상

1-1. 위 설문에서 'SW안전' 이 구분되기 어렵다면 그 이유는 무엇입니까?

2. 다음 중 SW안전 (품질/테스트/인증 등 포함) 관점에서 가장 중요하다고 판단되는 활동은 무엇입니까?

① 위험도 분석 ② Safety 메카니즘 분석/설계 ③ 상세설계

④ 구현 ⑤ 시스템 테스트 ⑥ 통합 테스트 ⑦ 기타 ( )

2-1. 그렇게 판단하신 이유는 무엇입니까?

3. 현재, 국내에서 적용되고 있는 소프트웨어 관련 인증 제도(GS인증, SP인증 등)은 소프트웨어

안전성 확보에 효과적이라고 보십니까? (안정성 측면, 산업내 통용성 측면, 글로벌적으로 통용되는지 등)

① 그렇다 ② 그렇지 않다

3.1 ‘그렇다’ 면, 어떠한 부분이 효과적인지 구체적으로 기입해 주십시오

3-2. ‘그렇지 않다’ 면, 어떠한 부분이 보완되어야 할 것으로 생각되십니까?

4. 귀사가 서비스를 제공하는 해당 산업 분야별로, 품질처럼 SW안전에 대한 등급/수준 등을 지정 혹은 구분하여 서비스를 수행하고 계십니까?

① 그렇다 ② 그렇지 않다

4-1. ‘그렇다’ 면, 어떠한 수준의 안전등급까지 서비스를 하고 있으며, 해당 프로세스는 어떤 과정입니까?

[참고] IEC 61508 국제표준에서는 안전무결성 수준 - SIL(Safety Integrity Levels) 1~4 단계의 레벨이 있으며, 주어진 모든 조건하에 있는 안전관련 시스템이 주어진 시간 내에 요구되는 안전기능을 만족스럽게 수행할 수 있는 확률로 정의됩니다.

(예) High Rate Demand 안전관련 기능에 대한 사용이 계속적으로 발생시 적용 (센서류 등)

Low Demand Rate 안전관련 기능 사용빈도수가 대략 년1회 미만 발생시 적용 (에어백 등)

4-2. ‘그렇지 않다’ 면, 그 이유는 무엇입니까? 또한, SW안전을 위해 어떠한 등급 체계 및 방식이 필요하다고 보십니까?

Ⅲ. SW안전 산업/시장에 대한 견해

1. SW안전 관련 산업이 독립적 산업으로 존재해야 한다고 생각하십니까?

① 그렇다 ② 그렇지 않다 (1-4. 로 이동)

1-1. 만일 ‘그렇다’ 면, 이유는 무엇입니까?

1-2. 만일 ‘그렇다면’, SW안전을 독립적 산업 분야로 간주한다면, 현재의 성숙도는 어느 수준이라고 생각하십니까? 앞으로 독립적 산업 분야가 되려면 얼마나 더 기간이 필요하다고 생각하십니까?

1-3. 만일, ‘그렇다면’, SW안전이 독립적 산업분야로 발전하기 위해서 기존의 법/규제의 어떤 부분이 어떻게 개선되어야 한다고 생각하십니까?

1-4. 만일 ‘그렇지 않다면’, SW안전이 독립적 산업 분야로 발전하기 어렵다면, 어떤 (기존의) 산업 분류에 포함되어야 한다고 생각하십니까?

2. 현재 국내 SW안전 관련 분야의 진입장벽은 무엇이라고 생각하십니까?

① 작은 시장 규모 ② 갖춰야 할 기술 수준 ③ 영업 네트워크

④ 법적 요건 (예. 국내 사업자만 가능, 일정 규모 이상의 자본금, 인력, 역량, 설비 등)

⑤ 기타 ( )

2-1. 향후 SW분야 시장이 확대될 것으로 예측하시나요? 만일 그렇다면, 시장 확대의 주요 동인은 무엇으로 생각하십니까? (예. 최소 1조원 규모의 시장 형성 등)

Ⅳ. SW안전 인프라 현황 및 Needs

1. [법/제도] 현재 영위하고 있는 비즈니스가 강화되기 위해 현재의 법/제도 차원에서 추가적인 제정이나 변경이 필요하다고 보십니까?

① 그렇다 ② 그렇지 않다

1-1. SW 안전을 위한 법/제도의 제정/변경의 방향과 필요한 내용은 무엇인지 의견을 주시기 바랍니다.

2. [인력/조직] SW안전 전문가 확보/육성을 위한 설문입니다.

2-1. 국내에서 SW안전 관련 전문가 수급은 어떠한 상황이라고 생각하십니까?

① 전문가가 충분히 많다. ② 전문가 Pool 규모와 수요가 거의 비슷하다.

③ 수요 대비 전문가가 부족하다. ④ 현재는 전문성을 가진 인력이 거의 없다.

2-2. 국내 SW안전 전문가 확보/육성이 필요한 영역은 어느 부분이라고 생각하십니까?
영역별로 (육성에 투입해야 할 리소스의) 가중치를 부여하여 답변하여 주시기 바랍니다.

분류	세부 내용	가중치
위험분석가	시스템 전반 또는 HW 나 SW 의 요구사항에 대해 성능, 물리적 특성, 환경 조건 등을 고려하여 위험원을 분석(hazard analysis)하고 위험 정도를 평가(risk assessment)	
안전관리자	개발 산출물 작성부터 형상관리, 안전기능 추적성 확보, 시스템 운영 기록 확보 등 시스템 개발 시 안전 프로세스를 관리	
안전검증자	SW 프로세스와 개발된 SW 가 할당된 안전무결성수준(SIL)을 포함하여 표준의 요구사항에 부합하는지를 평가	
개발자	안전 관련 활동에 대한 이해가 높고, 기능안전 개발에 대한 지식·경험이 있는 SW 개발자	
합 계		**100**

2-3. 국가에서 전문가 확보/육성관련 지원해야 할 사항은 무엇입니까?

3. 추가로, SW안전 산업의 활성화를 위해 중요한 부분과 국가 차원에서 지원되어야 할 사항을 다음 각각의 측면에서 어떠한 부분인지 기술하여 주시기 바랍니다.

3-1. 법/제도 측면

3-2. 인력 측면

3-3. 시장 측면

※ 이상 모든 설문에 응해 주셔서 대단히 감사합니다. 보내 주신 의견은 국가SW안전 산업 동향 조사에 유용하게 활용하겠습니다.

부록 3 : 소프트웨어 개발사용자(End User Sector) 설문지

Ⅰ. SW안전 개요

1. (개념)귀하는 ‘SW안전’에 대해서 들어 보셨거나, 그 개념에 대해서 이미 알고 계십니까?

① 알고 있음 ② 모름

‘SW안전’ 이란,

소프트웨어 품질에 기반하지만 감내하기 어려운 수준의 사고 발생 시, 이를 회피하는 능동적인 방안(Safety Mechanism / Functional Safety)까지 포함한 개념

- 귀하께서 현재 생각하시는 ‘SW안전’에 대한 정의를 아래 항목에서 선택해주시기 바랍니다. 이와 더불어 본 설문 내 모든 질문에서 사용되는 ‘SW안전’에 대한 용어에 아래 선택하신 개념을 적용해 주시기 바랍니다.

① SW안전은 SW품질에 포함 (즉, SW품질로 생각)

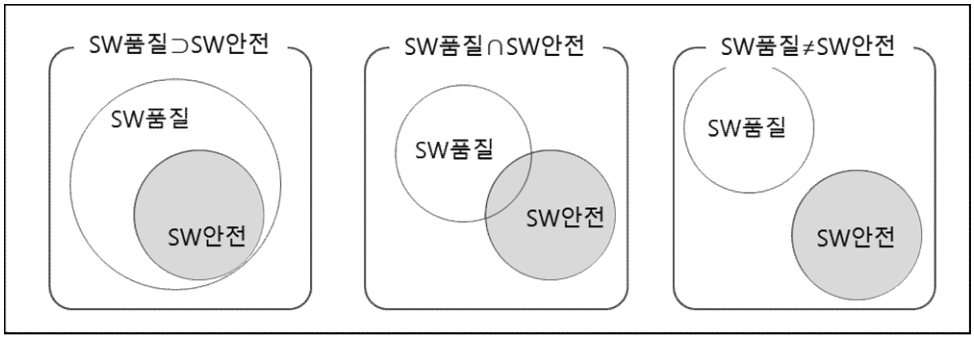
② SW안전과 SW품질 간 공통된 부분은 존재하나 SW안전은 별도의 위험회피 메카니즘

③ SW안전과 SW품질은 독립적인 영역

④ 위 ①부터 ③까지의 개념을 모두 포괄

※ SW품질이란?(IEEE) : 기능명세서의 적절한 구현성 등 주어진 요구사항을 만족시킬 수 있는 SW의 총체적인 특징과 제품의 특성 (The totality of features and characteristics of a software product that bear on its ability to satisfy given needs: for example, conform to specifications.)

※ SW품질 vs. SW안전



2. 귀사에서 SW 안전과 관련된 활동을 수행하고 있다면 어떤 이유에서입니까?

① 국내 법적 규제로 ② 수출 대상국 법적 규제로 ③ 고객사 요구사항 준수를 위해

④ 고객의 생명/재산 보호를 위해 자체적으로 ⑤ 회사의 자산 보호를 위해 자체적으로

⑥ 수행하고 있지 않다. (수행하지 않는 이유)

3. (표준)귀사는 SW 개발/운영/관리 규정과 절차를 수립하고, 이에 따라 SW 개발 및 운영 업무를 수행하고 있습니까?

① 예 ② 아니오

- 위 항목이 "① 예"을 선택했다면, SW안전 관련한 관리범위(Coverage)는 어디까지 규정되어 있습니까?

① SW안전 부품/제품 구입 ② SW안전부품/제품 개발 ③ 테스트

④ SW안전 부품/제품 인증 ⑤ SW안전 사고 대응

⑥ 기타 ( )

- 자체 규정/절차 이외에, 별도로 국제표준인증(CMMI 혹은 ISO20000 등)을 취득했거나 준비 중 이십니까?

① 예(국제표준인증 종류 :) ② 아니오

- 귀사에서 상기 SW가 어디에 적용되고 있나요? (적용 환경 및 적용 대상) (복수 선택 가능)

- 적용 환경 예) 제조/생산환경에서 설비 또는 공정관리, 관제
- 적용 대상 예) 부품/모듈/제품

- SW는 어떻게 조달하고 있습니까?

① 자체 개발 ② 외주 개발 ③ 패키지 구매

4. (조직)귀사의 상기 SW안전 업무를 담당하는 부서 및 담당자가 있습니까?

① 예 ② 아니오

- 부서가 존재한다면 부서명( ), 부서원수 ( )

- 부서가 존재한다면 해당 부서의 역할은 무엇입니까? ( )

5. (업무)귀사에서 수행하는 SW안전 관련 업무기능에 대하여 현재 수행중인 업무를 기입하시기 바랍니다

번호	SW안전 업무명	수행내용/수행인력
1	SW안전 정책수립, 기술 기획	
2	SW안전 인증 확보/유지관리	
3	SW안전 관련 기술개발/R&D	
4	제품(S/W) 대상 SW안전 적용, 판매/구축, 유지관리	
5	기타 (답변자 임의 지정 업무)	

6. 귀사에서는 「SW 안전성 공통개발 및 가이드」에 대해 인지하고 계십니까?

① 예 ② 아니오

- 인지하고 계시다면 실제 업무에 활용도는 어느 정도 입니까? ( )

- 인지하지 못하고 있었거나, 활용도가 낮다면 무슨 이유 때문 인가요? ( )

※ SW 안전성 공통개발 가이드 : 정보통신산업진흥원에서 SW 기능안전성을 도입하고자 하는 다양한 산업분야의 프로젝트에 공통적으로 활용이 가능한 내용들을 포함한 가이드

7. (의견)귀사에서 SW안전 영역을 업무에 적용한다 가정 시, 핵심적으로 필요한 부분 또는 적용 방향에 대한 의견을 주시기 바랍니다.

Ⅱ. SW안전 예방점검 활동

1. (구축)귀사는 Safety-Critical SW 구축/변경/운영 시, SW 기능오류로 인한 안전사고(인명, 재산 피해)를 예방하기 위하여 어떤 활동을 수행하고 있습니까? (다중선택 가능)

① Safety-Critical SW 구축 시, 별도의 SW안전 전문가 투입(사내인력 또는 외부업체)

② SW안전에 관련된 요건 정의 및 준수

③ 제3자 전문 테스팅 업체 활용

④ Safety-Critical SW 구축 시 인증

⑤ 기타 ( )

참고) 본 설문에서 ‘SW안전 중요대상 (Safety-Critical SW)’이라 함은, SW요건자체가 Safety상의 미흡한 이유로 인명/재산 등 막대한 손실을 초래할 수 있는 SW를 의미합니다. (응용 SW, 각종 부품/제품에 탑재된 Embedded SW 등을 모두 포함)

2. 귀사가 생산/관리하고 제품에 ‘Safety-Critical SW’가 포함되어 있습니까?

번호	대상 SW 명	주요 기능	비고
1.			
2.			
3.			
…			

3. (검증활동) 3번에서 Safety Critical SW가 있다고 답하셨다면, 귀사는 ‘Safety-Critical SW’에 대하여 요건설계, 테스트, 인증 등 적절한 SW안전을 위한 검증활동을 수행하고 계십니까?

① 수행하고 있음 ② 수행하지 않음

4. (인증)귀사의 Safety-Critical SW 관련 국내/해외 인증이 있다면, 무엇이 있습니까?

(예. ISO26262 자동차 부문, DO178C 항공부문 등)

5. (표준)Safety-Critical SW 검수에 대한 회사 내부의 표준 또는 지침을 보유하고 있습니까?

① 있음　　② 없음

6. (표준)회사의 표준 또는 지침을 보유하고 있다면, 그것을 준수하기 위해 협력사(ex. 부품업체 등)와 어떠한 활동을 하고 있습니까?

(　　)

7. (검증)Safety-Critical SW 검증활동을 수행 시 외부업체를 활용하는 경우, 어떤 업체를 활용하고 있습니까?

① 국내업체　　② 해외업체

위 업체의 활용 이유를 아래에 표시해 주십시오.

구분	평가	수준
기술전문성		(낮다) 1 ------- 2 ------- 3(보통) ------- 4 ------- 5 (높다)
사고시책임		(낮다) 1 ------- 2 ------- 3(보통) ------- 4 ------- 5 (높다)
소요비용		(낮다) 1 ------- 2 ------- 3(보통) ------- 4 ------- 5 (높다)
거래편의성		(낮다) 1 ------- 2 ------- 3(보통) ------- 4 ------- 5 (높다)
고객의 요구		(낮다) 1 ------- 2 ------- 3(보통) ------- 4 ------- 5 (높다)

- 상기 이유 이외의 경우가 있다면 설명 부탁 드립니다.

(　　)

8. (비용) Safety-Critical SW 구축/운영 시, SW안전을 강화하기 위해 사용하는 비용은 어느 정도입니까? (ex. 전문가 투입, 테스트, 인증 등에 소요되는 비용)

- SW안전 소요비용 : (　　)

(※예시 : 년간 1,000만원 / 년간 10M/M투입 / 전담인력 과장 1명, 프로젝트 당 x%, 연간 IT개발 비용의 x% 등)

9. (사전대응)귀사에서는 SW안전 교육을 위해 어떠한 활동을 수행하고 있습니까?

① SW개발자 대상 안전교육　② SW안전관련 세미나　③ BP(Best Practice) 전파

④ 기타(　　)　⑤ 안하고 있다면 이유는?(　　)

Ⅲ. SW안전 대응관리 활동

1. (시나리오)귀사의 제품과 관련된 사고에 대한 대응 시나리오를 보유하고 있습니까?

① 있음　　② 없음

- 귀사는 회사 사고 대응 훈련을 정기적으로 수행하고 있습니까?

① 없음　② 월1회　③ 분기1회　④ 반기1회　⑤ 년1회　⑥ 비정기적

2, (절차)대응 시나리오가 있다면, SW 관련 영역이 있습니까?

① 있음　　② 없음

- SW 관련 영역이 있다면, 적용되는 항목을 선택해 주십시오. (다중선택가능)

① 사고 수습 조직 및 역할이 규정되어 있음

② SW사고를 유발한 시스템/제품에 대한 SW전문가가 확보되어 있고 역할이 정의되어 있음

③ (공공기업 대상) 사고수습 조직과 정부와의 소통채널이 규정되어 있다면, 정부의 소통채널 부처는 ( )임

④ 사고와 관련된 부품/제품의 기술 협력사와 소통채널이 규정되어 있음

- 대응 시나리오 및 처리 활동에서 개선해야 할 사항은 무엇이 있습니까?

( )

3. (사고수습)현재까지 귀사는 내•외부적으로 SW안전 관련 사고의 경험이 있습니까?

① 있음 ② 없음

- 만일 겪으셨다면, 사고의 내용, 원인, 피해규모는 어느 정도 입니까?

( )

- 사고수습을 위해 중요하다 생각하는 순서대로 번호를 기입하여 주십시오.

( )Best Practice : 유사 해결사례

( )인력

( )예산(비용)

( )의사결정/소통

( )정부지원

( )기타 :

4. (검증)SW안전에 관한 전반적인 검증활동을 관리하는 툴 또는 시스템을 보유하고 있습니까? 있다면, 관리 항목은 무엇인지 작성 바랍니다.

① 있음 (시스템 및 관리항목:) ② 없음

5. (사례)SW안전 테스트 및 사고사례정보를 수집/축적하고 있습니까? 몇 년 간의 정보가 수집/축적되어 있습니까?

① 없음 ② 1년미만 ③ 3년미만 ④ 5년미만 ⑤ 10년미만 ⑥ 기타(년)

6. (사례)SW안전 테스트 및 사고사례정보를 어떻게 활용하고 있습니까? (다중선택 가능)

① 테스트 케이스에 적용 ② SW안전장치 추가 및 개선

③ 개발인력의 교육 및 인식 제고 ④ 기타( )

7. (책임)SW안전 문제 발생 시 협력사와의 책임 소재 규명 및 보상은 어떻게 처리합니까?

① 계약서 혹은 협약서 ② 업계 관례 ③ 불분명함 ④ 기타( )

Ⅳ. SW안전에 관한 정책 요구사항

1. (정부정책)SW안전과 관련하여 정부에서 제공하는 홍보자료, 보고서, 간행물 등을 접한 적이 있습니까?

① 있음　　② 없음

- 있었다면 어떠한 종류였습니까?

2. (정부지원)귀사는 SW품질(예: SP인증)을 포함한 SW안전관련 인증을 위한 정부의 정책적인 지원을 받으신 경험이 있습니까?

① 있음　　② 없음

- 정부지원을 받았다면 그 만족도는 어떻습니까?

① 충분　② 적정　③ 부족

- 향후 정부지원을 받는다면, 어느 부문에 대한 지원이 가장 필요한지 순서대로 번호를 기입하여 주십시오.

(　)Best Practice : 유사 해결사례 (.　　)

(　)인력/교육 (예. 자격증 등.　　)

(　)예산(비용) (.　　)

(　)의사결정/소통 (.　　)

(　)법제도 개선

(　)기타 :

참고) 정부의 SW프로세스 품질인증(‘SP인증’)을 위한 정책적 지원 : SP 인증획득에 관심있는 기업을 대상으로 인증심사 준비내용등을 진단하여 인증심사 준비를 효율적으로 할 수 있도록 지원 (원내소속 ‘SP 인증심사원’ 이 신청기업을 방문하여 인증제도 , 심사절차 설명 등 상담)

SW프로세스 품질인증(‘SP인증’)제도 : 기업의 SW개발단계별 작업절차 및 산출물 관리 역량 등을 분석하여 SW개발 프로세스 역량수준을 평가・인증하는 제도

3. (정부지원)기업에서 SW안전성을 제고하고 SW안전 제품의 제조 및 판매/수출을 위하여, 정부의 지원 및 개선 사항이 있으면 의견을 작성해 주시기 바랍니다.

주 의

1. 이 보고서는 소프트웨어정책연구소에서 수행한 연구보고서입니다.
2. 이 보고서의 내용을 발표할 때에는 반드시 소프트웨어정책연구소에서 수행한 연구결과임을 밝혀야 합니다.

95000
9 788961 084369
ISBN 978-89-6108-436-9 (PDF)