연구보고서 2016-020

SW안전 관리 관점에서의 기반시설 보호 법제 개선 연구

Research on Improvement of Infrastructure Protection Legislation from SW Safety Management Perspective

박태형/진회승/권헌영/백승조/주문호

2017.04.

SPRi 소프트웨어정책연구소

이 보고서는 2016년도 미래창조과학부 정보통신·방송연구개발사업의 연구결과의 보고서 내용은 연구자의 견해이며, 미래창조과학부의 공식입장과 다를 수 있습니다.

목 차

표 목 차

그 림 목 차

요 약 문

1. 제 목

SW안전 관리 관점에서의 기반시설 보호 법제 개선 연구

2. 연구 배경 및 목적

SW에 대한 활용성과 의존성이 증가하는 SW 중심사회가 발전함에 따라 SW의 오류 등으로 인한 사고 발생 가능성과 피해 규모도 상당한 수준으로 확대될 것으로 예상된다. 따라서 문제가 생길 시 국가·사회·경제에 큰 영향을 미칠 수 있는 국가주요기반시설의 SW 안전을 확보하기 위한 제도 혁신의 필요성이 요구되게 되었다.

본 연구의 주요 목적은 주요기반시설에서 활용되는 SW의 안전을 확보하기 위해, 안전관리 관점에서 기반시설 보호 법제도의 개선 방향 및 개정안을 마련하고자 하는 데 있다.

3. 연구의 구성 및 범위

본 연구는 첫 번째로 SW 안전의 의의와 정책 체계를 이해한 뒤, 국내 및 해외 주요국의 주요기반시설 보호 관련 법제를 분석하여 국내외 기반시설 안전보호 체계의 전체 흐름과 본 연구의 분석 초점을 파악한다. 안전관리 관점의 국가재난관리 활동 단계를 분석하기 위하여 (예방-대비-대응-복구)의 국가재난관리 활동 단계별 정의와 범위를 분석하고 이에 따라 각 국의 법률 조항들을 안전관리 관점에서 분석 및 분류한 뒤 결과에 따른 시사점을 도출한다. 마지막으로, 도출된 시사점을 통해 SW 안전 확보를 위한 국내 법제도 개선 방안의 입법을 위한 입법 체계를 정립하고, 본 연구의 최종 결과로 공공분야 소프트웨어 안전 강화와 지능정보사회 전반의 안전성 제고를 위한 정보통신기반보호법 개정안과 소프트웨어 안전 관리에 관한 법률 제정안을 제안하도록 한다.

4. 연구 내용 및 결과

안전관리 관점의 법제 분류 기준은 ‘국가기반체계 보호관련 중앙재난안전대책본부 운영 및 상황관리 규정’에서 정의하고 있는 (예방-대비-대응-복구)의 4단계

안전관리 활동을 기반으로 구성하였고, 이와 관련한 보고서 및 논문 등의 연구를 토대로 세부 분류 단계 및 내용을 수립하였다.

수립한 분류 기준을 통해 국내 기반보호 법제의 중심이 되는 법인 『재난 및 안전관리 기본법』과 『정보통신기반보호법』, 그리고 국가주요기반시설의 분야 중 원자력 안전과 관련된 법률들을 대표적으로 선별하여 분석하였다. 해당 법률들을 분석 및 분류한 결과, 대부분의 조항들이 안전관리 기구 및 조직 구성, 안전관리 체계 마련, 안전점검 및 안전조치, 안전관련 기반 조성, 안전관리 계획 수립 등 잠재적인 위험을 예측하고 사전 조치를 취함으로써 위험으로부터 발생할 피해 규모를 최소화시키는 활동들인 예방 단계에 집중되어 있는 것으로 나타났다. 예방 단계에 속하는 조항들이 공통적으로 전체 조항의 절반 이상을 차지한 것으로 보아, 우리나라의 국가 안전보호 법제 조항들이 예방 활동을 바탕으로 구성되어 있다는 사실을 알 수 있었으며, 이는 정부가 오래토록 추진해온 예방 위주의 재난/사고 관리 대책의 성과라고 생각된다. 또한 각 법제 분류에 대한 결과를 통해 안전관리 관점의 세부 분류 단계별 활동 흐름을 파악할 수 있었으며, 각각의 법률의 목적이나 필요에 따라 타 법률들 보다 안전관리 관점의 각 단계별로 체계적으로 구성된 부분들은 SW 안전 전반을 규율할 수 있는 법제를 새로 정립할 시 더욱 집중적으로 참조할 수 있을 것으로 생각된다. 추가적으로 기존 법제의 분석 및 분류를 통해 SW 안전에 대한 규율이 추가적으로 필요한 부분들을 파악하기에 용이하였으며, 이러한 검토 과정을 통해 자칫 중복 규제가 되어 기관 및 기업들의 업무 효율성 저하로 이어질 가능성을 줄일 수 있을 것이다.

해외 주요국의 주요기반시설 보호 법제의 분석 결과, 국내는 법률을 기반으로 대부분의 국가기반시설의 안전을 규율하고 있었지만 해외 주요국들은 계획이나 가이드라인을 통해 실행력의 신속성을 확보하고자 하는 경향이 존재하였다. 미국, 영국, 독일은 공통적으로 법제 분류 기준의 큰 틀인 예방, 대비, 대응, 복구의 안전관리 관점에 입각하여 국가재난 및 비상사태에 대한 대비 체계를 구축하고 있었으며, 해당 분석 및 분류를 통해 각 국의 기반시설 보호 체계의 강점과 우리나라의 법 구성 시 참고할 점들을 엿볼 수 있었다.

국내외 기반보호체계 법률 분석 결과, 각 국가마다 재난 대비 차원, 안보 차원, 외부침해사고 대비 차원 등의 다양한 관점에 기반한 법제 체계를 갖추고 있었지만, 그 중 SW의 내부결함으로 인한 사고 대비 등 SW 안전 관리의 내용을 포괄하여 규정할 수 있는 법률 및 세부 조항을 가지고 있지는 않았다. 따라서 국가주요기반시설의 안전을 규율하는 법률 내에 SW와 관련될 수 있는 조항들을 도출하고 SW의 범위와 유형을 정립하여 국가주요기반시설의 SW 안전 전반을 규율할 수 있는 법제 제정 및 개선의 필요성을 확인할 수 있었으며, 이러한 사항을 반

영하여 법제 개선안을 제안하였다.

본 연구는 최종적으로 SW 안전 확보를 위한 법제도 개선방안 연구를 통하여 공공분야 소프트웨어 안전 강화와 지능정보사회 전반의 안전성 제고를 위한 정보통신기반보호법 개정안과 소프트웨어 안전 관리에 관한 법률 제정안을 제시하였으며, 실제 개정안 및 제정안은 부록으로 첨부하였다.

SUMMARY

1. Title

Research on Improvement of Infrastructure Protection Legislation from a SW Safety Management Perspective

2. Background and Purpose of the Research

In the SW-oriented society where the application dependency of SW is increasing, it is expected that the possibility of the accident caused by SW errors and the damage scale will be increased to a considerable extent. Therefore, there is a need for institutional innovation for the safety of SW, which is used in major infrastructure, which may have a great impact on the country, society, and economy.

The main purpose of this research is to establish the direction and amendment of the Infrastructure Protection Act from a viewpoint of safety management in order to ensure the safety of SW used in major infrastructure.

3. Composition and Scope of the Research

This research firstly analyzes the significance of SW safety and its policy system and then analyzes the main flow of the domestic and overseas infrastructure security protection Acts and policies. In order to analyze the steps of national disaster management activities in terms of safety management (preventive - prepared - response - recovery), we study the definition and scope of national disaster management activities in stages and analyze and classify legal provisions of each country in terms of safety management and then derive implications based on the results.

As a final result of this research, we propose an amendment to the Information Communication Infrastructure Protection Act and an enactment of the Act on Software Safety Management to enhance the security of the public domain software and the safety of the intelligent information society as a whole.

4. Contents and Results of the Research

The legal classification standard of the safety management viewpoint is based on the 4th stage safety management activities defined in the Domestic Disaster Safety Management Regulations (Prevention-Preparedness-Response-Recovery), and detailed steps and contents have been established based on the researches and reports related to the above.

Through the classification criteria established, we have selected and analyzed the law that is central to the domestic protection law: 『Information Communication Infrastructure Protection Act』, 『Disaster and Safety Management Basic Law』, and laws related to nuclear safety, part of major national infrastructure. As a result of analyzing and categorizing these laws, most provisions have been focused on preventive measures, which are activities that minimize potential damage from risks by predicting potential risks and taking precautions such as establishment of safety management organization and organization, establishment of safety management system, safety inspection and safety measures, establishment of safety related foundation, establishment of safety management plan, etc. As the provisions of the precautionary stage occupied more than half of the total clauses in common, it was found that the provisions of the National Security Protection Legislation in Korea are focused on the preventive stage. This is the outcome of the prevention - oriented disaster / accident management measures that the government has long pursued. In addition, through the results of each legal classification, we were able to grasp the activity flow according to the detailed classification stages of the safety management viewpoint, it is believed that the parts that are organized more systematically than the other laws according to the purpose and necessity of each law can be referred more intensively when a new legal system that regulates SW safety is newly constituted. Moreover, analysis and classification of existing legislation made it easier to identify areas where additional discipline for SW safety is needed, and also this review process can reduce the possibility of reducing the efficiency of organizations and companies by duplicating regulations.

As a result of analysis of major infrastructure protection legislation of overseas major countries, Domestic governments have regulated the safety of most national infrastructure based on law, but major foreign nations have tended to secure the speed of implementation through planning and guidelines. The United States, Great Britain, and Germany have systems based on the perspective of safety management of prevention, preparation, response, restoration to prepare for national disasters and emergencies. Through the analysis and classification, we can get a glimpse of the strengths of the infrastructure protection system in each country and the points to be referred to when constructing laws in our country.

As a consequence of legal analysis of domestic and overseas infrastructure protection system, each country have a legislative system based on various points of view such as disaster preparedness level, security level, and dimension for external infiltration, but it does not have laws and detailed provisions that can encompass the contents of SW safety management, such as accident prevention, due to internal defects of SW. Therefore, it is necessary to establish and improve the legal system that can regulate SW safety of major national infrastructures through drawing up provisions that may be relevant to the SW within the law governing the safety of major national infrastructure and establishing the scope and type of SW.

Through the study on the improvement of the legal system to secure SW security, we proposed the amendment plan of information communication infrastructure protection law to enhance security of public sector software and enhance safety of intelligent information society as a whole and legislation for software safety management. Plus, actual amendments and enactments are attached as appendices.

CONTENTS

제1장 서 론

제1절 연구의 배경 및 필요성

1. SW 중심사회의 발전과 위험성 증대

미래창조과학부는 2014년 7월 21일 발표한 'SW 중심사회 실현전략' 에서 SW 중심사회를 'SW가 혁신과 성장, 가치창출의 중심이 되고 개인·기업·국가의 경쟁력을 좌우하는 사회' 라고 정의하였다. 즉, 현대사회는 SW가 사회전반에 광범위하게 사용되고 국가 주요 인프라, 교통, 생활, 재난 관리 등 국민의 생명과 안전에 직결되는 분야에 필수적으로 사용되고 있다는 것이다. 이에 따라 주요 산업들의 운영이 SW에 의존하는 비율이 높아지고 있으며, SW를 어떻게 운영하고 관리하는가가 SW 중심사회의 핵심 화두가 되고 있다.

SW에 대한 활용성과 의존성의 증가는 자연스럽게 SW의 복잡도의 증가로 이어지며 이는 오류 및 취약점 발생으로 인한 위험성을 증대시키게 된다. 따라서 항공, 철도, 원자력 등 주요 기반 산업에서 이용되는 SW의 오류 등으로 인한 사고 발생 가능성과 피해 예상 규모도 상당한 수준으로 확대될 것으로 예상된다. 나아가, 이와 연계되어 주요 국가기반시설에서의 SW로 인한 사고가 발생된다면 국가·사회·경제에 큰 피해를 미치고, 나아가 국민의 안전 신뢰성을 하락시킬 것이다. 실제로 2016년 5월 미국에서 발생한 테슬라 자율 주행 자동차 사망사고, 2016년 국내 인천 도시철도 시스템 결함으로 인한 사고 등이 발생하고 있는 것으로 볼 때, SW의 오류로 인한 사고 위험은 더 이상 단순한 우려가 아니라 현실로 다가오고 있다.

2. 본 연구의 필요성

국가는 국가기반시설에서 활용되는 SW의 안전 확보를 통하여, 국민의 안전을 보장하고 국가의 온전한 책무를 수행할 필요가 있다. 의료, 금융, 교통, 에너지 등 국민생활의 안전과 밀접한 관련이 있는 다양한 분야의 기반시설들은 가장 안전하게 보호되어야 하며 이를 위해서는 기반시설에서 활용되는 SW의 안전 확보가 요구될 것이다. 이를 위해 지금까지는 심층적으로 논의되지 않았던 주요기반시설의 SW에 대해 안전관리의 관점에서 논의하고 연구할 필요성이 있을 것으로 생각된다.

SW 중심사회가 본격적으로 도래하기 전에 만들어진 현재의 국내 기반시설 체계와 법제는 SW 안전에 대한 관념을 충분히 반영하지 못하고 있는 실정이며, 기반시설 일반에 대한 분야와 SW가 활용되는 기반시설 분야에 대한 개념 정립이 미비하며 서로간의 명확한 관계가 정립되지 않고 있다. 때문에 국가가 이를 규제하고 관리함에 있어 혼선이 생길 수밖에 없는 구조를 갖추고 있으며, 기반시설의 SW 안전과 유관된 사고에 대한 컨트롤 타워도 부재하여 이에 대한 유기적인 대응이 쉽지 않다.

이와 같은 문제들을 해결하기 위해 주요 기반시설의 SW 안전을 확보하기 위한 제도 혁신이 필요하며, 주요 기반사업의 SW 안전을 망라적으로 다룰 수 있는 관련 법안이 필요하다. 정보통신 분야의 해킹 및 침해사고 대응에 대한 사고 예방과 피해 최소화에 대해서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」과 세부 지침 및 가이드라인을 통해 어느 정도 기반이 마련되어 있는 상황이나, 주요 기반시설의 SW 안전 전반을 규율할 수 있는 법체계는 아직 미비한 상황이기 때문에 이를 개선할 수 있는 기존 기반보호법안의 개정이나 SW 안전 관련 새로운 법의 제정이 요구된다.

제2절 연구의 목적 및 목표

1. 본 연구의 목적

[그림 1-1] 본 연구의 필요성 및 목표

본 연구는 문제가 발생할 시 국가·사회·경제에 중대한 피해를 미칠 수 있는 주요 기반시설에서 활용되는 SW의 안전을 확보하기 위해, 안전관리 관점에서 기반시설 보호 법제도의 개선 방향 및 개정안을 마련하고자 하는 데 목적이 있다.

2. 본 연구의 목표 및 세부 추진 사항

본 연구에서는 국내 기반보호 법제와 해외 주요국의 기반보호 법제 현황을 분석하고 안전관리 관점(예방-대비-대응-복구)으로 해당 법제들을 분류하도록 하며, 이를 종합 분석하여 도출되는 시사점을 토대로 하여 국내 주요기반시설의 SW 안전을 확보하기 위한 법령의 개정안 및 제정안을 만드는 것을 목표로 한다.

국내 주요기반시설의 SW 안전을 확보하기 위한 법제 개선의 목표를 달성하기 위해서, 본 연구에서는 다음과 같이 세부적인 목표를 네 가지로 구체화하였다.

[그림 1-2] 본 연구의 목적 및 세부 추진 사항

- SW 안전의 의의와 정책 체계의 이해
- 국내 및 해외 주요국의 주요기반시설 보호 관련 법제 분석
- 안전관리 관점(예방-대비-대응-복구)에서의 법률 분류 결과 도출
- 법률 분류 결과로부터의 시사점 도출 및 법제 개선방안 제시

3. 연구의 범위

- SW 안전의 의의 및 정책 체계 분석

지능정보사회에서의 SW의 활용 현황과 역기능을 탐색함으로써 정보사회에서의 SW 활용 동향 및 효과를 분석하였다. 또한 국내외 SW 안전 관련사고의 사례를 조사하여 제시함으로써 SW 안전 관련사고의 피해 정도 및 심각성을 인지시킴과 동시에 법제 개선의 필요성을 도출할 수 있도록 하였다. 추가적으로, SW 안전의 의의와 방향성을 탐색하기 위하여 SW 안전성 확보를 위한 국가의 역할 수행의 필요성을 도출하였고 안전 개념을 정립하였으며 SW 안전의 효과적 관리체계 구축의 필요성을 제시하였다.

SW 정상적 운용을 위한 회복력과 SW 활용의 지속성이 요구됨에 따라 SW 안전 분석은 위험 관리의 관점을 반영해야 함을 주장하였고, 위험 관리를 위한 종합적·입체적 문제해결 체계의 구조화 필요성을 분석하였다. 이에 대한 이론적 근거를 뒷받침하기 위하여 울리히 벡의 '위험 사회(risk society)론' 을 분석하여 연구의 이론적 기반을 마련하였으며, 이를 통해 위험 사회내의 안전성 확보를 위한 국가의 역할을 분석하였다. 또한 안전규제수단으로서의 '제조물 책임' 법 이론을 분석하여 제조물 책임과 SW 안전을 위한 규율체계의 연결 관점에서의 분석도 진행하였다.

추가적으로, SW 안전의 정책적 의미와 구조 분석하기 위해 국가 운용의 필수적인 기반시설의 SW 안전과 국민생활의 안정을 위한 SW 안전 확보에 대한 논의를 진행하였다.

- 국내 기반시설 안전보호 체계 및 법률 조사/분석

국가중요기반시설 안전보호 체계 분석하기 위해 대한민국 헌법으로부터의 안전보호 법체계 구성과 국가기반체계의 시설·기능·시스템 보호를 위해 규정된 보호 대상 시설 정의 및 범위를 조사하였다. 또한 재해 및 재난 관련 법제, 주요국가기반시설 보호 체계, 주요정보통신기반시설 보호 체계의 동향을 조사하여 국내 기반시설 안전

보호 체계의 전체 흐름과 본 연구의 분석 초점을 파악하도록 하였다.

안전관리 관점의 국가재난관리 활동 단계를 분석하기 위하여 (예방-대비-대응-복구)의 국가재난관리 활동 단계별 정의와 범위를 분석하고 주요 내용을 살펴본다. 해당 분석을 토대로 도출해낸 분류 기준을 통해 국내의 「재난 및 안전관리 기본법」과, 「정보통신기반보호법」의 법률 조항들을 안전관리 관점에서 분석하고 분류하였다. 추가적으로, 주요 산업 도메인 중 가장 안전에 대한 위험성이 높다고 생각되는 분야인 원자력 분야의 법률 조항들을 안전관리 관점에서 분석하고 분류하여 시사점을 도출하고자 하였다.

- 해외 주요국 기반시설 안전보호 체계 및 법률 조사/분석

미국, 영국, 독일의 주요기반시설 법제 개관을 이해하고 기반시설의 안전을 보호하기 위한 각 국의 법령들을 분석하였다. 분석된 해외 주요국들의 법제 목록에 대하여 국내 법제 분석에서 적용된 동일한 분석기준을 활용하여 해외 주요국들의 기반시설 안전보호 체계를 각각 안전관리 관점의 단계로 나누어 분석하여 시사점을 도출하도록 하였다.

- SW 안전 확보를 위한 법제도 개선 방안 연구

SW 안전 확보를 위한 법제도 개선 방안을 구체적이고 명확하게 제시하기 위하여 관련 법제도 입법을 위한 입법체계를 우선적으로 정립하였다. 이를 기반으로 정보통신기반보호법 개정을 위한 입법체계와 소프트웨어 안전 관리에 관한 법률 제정을 위한 입법체계를 각각 분석하여 법제도 개선의 당위성과 전문성을 확보하고자 하였다. 또한 주요 제도개선 과제 선정하여 향후 제도 개선이 이루어지는 과정에서 집중적으로 연구 및 논의해야할 부분을 제시하였고 효율적이고 빠른 입법을 위한 입법 전략에 대한 제언도 포함하였다.

- 법제 개정안 및 제정안 도출

본 연구의 최종 결과로 공공분야 소프트웨어 안전 강화와 지능정보사회 전반의 안전성 제고를 위한 정보통신기반보호법 개정안과 소프트웨어 안전 관리에 관한 법률 제정안을 제안하였으며, 실제 개정안 및 제정안은 부록으로 첨부하였다.

제2장 SW 안전의 의의와 정책 체계

제1절 SW 안전의 개념

1. 지능정보사회에서의 SW 활용

산업의 발달과 고도화는 “정보”라는 것의 가치를 측정하기조차 어려울 만큼 중요한 것으로 만들어 놓았다. 정보가 가지는 가치가 높아지게 되면서 사회의 시스템 자체가 이를 중심으로 변이하기 시작했고, 이러한 정보화가 가져다주는 효과에 대해서 집중하게 되었다. 기본적으로 정보화는 가상의 네트워크로 대상들이 연결될 수 있는 기계적인 기반이 형성되고 이를 통해 효과적으로 정보를 운용할 수 있는 소프트웨어의 발전을 통해서 달성되었다. 이러한 소프트웨어를 통한 정보의 활용에 의존한 사회는 내용적 측면에서 정보 활용의 질적·양적 확대, 기술적 측면에서 기계적 기반을 보다 정밀하고 효과적으로 진화하도록 끊임없이 성장하고 있는 중이라고 할 수 있다.

소프트웨어의 활용을 통해 이룰 수 있는 가장 단순하면서 유익한 효과로는 인간의 물리적인 행동양식에 있어서의 간소화를 들 수 있으며, 물리적인 제약의 해소로 인한 접근의 용이함으로 말미암아 형평과 참여의 확대를 이룰 수 있다. 결국 사회 속 인간의 삶의 질을 향상시키는 수단으로서 소프트웨어가 활용되는 것이며 수단으로서 기능한다는 것이다.

최근에는 지능정보 및 인공지능 기술과 이의 근간이 되는 데이터활용기술(ICBM;IoT, Cloud Computing, Big Data, Mobile)을 융합하여 인간의 고차원적 정보처리 능력을 구현하는 기술[1]이 제조업과 서비스, 사회에 체화되면서 산업과 사회가 지능화 되는 경향을 보이고 있는데, 이러한 변화의 핵심에는 SW의 발전과 기능 확장에 있다고 할 것이다. 지능정보기술이 산업뿐만 아니라 개인들의 삶에 직접적으로 영향을 미치게 되면서 SW와 인간의 삶의 연결성과 의존성은 보다 긴밀해 질 것이 명확하다.

1) 인공지능 기술과 이의 근간이 되는 데이터활용기술(ICBM;IoT, Cloud Computing, Big Data, Mobile)을 융합하여 인간의 고차원적 정보처리 능력을 구현하는 기술

2. 역기능과 SW 안전

SW 활용 환경의 발달과 확장으로 인하여 우리 삶의 편리성이 일정 수준 이상으로 제고되었지만, 이러한 환경 안에서의 생활이 새로운 문제들을 발생시켰다. HW적 우수성 보다는 SW기술 우수성이 제품 우위 결정의 핵심요인으로 대두되면서, 제품 성능에 대한 SW비중이 증가하였다. 이에 따라 동일 제품에 대해 SW복잡도는 급격히 증가하고 있다. 예를 들어, 과거 X라인의 코드가 자동차에 쓰인 반면, 현재는 X라인의 코드가 쓰이고 있다. 이처럼 제품기능의 SW의존도 증가는 SW복잡성의 증가와 비례하게 SW로 인한 오류 및 취약성으로 인한 위험성 증가를 초래하였다. SW가 사회 전반에서 핵심적으로 이용되면서 SW의 기술력이 집적되면서 복잡도가 증가하고, SW의 오류 및 취약점 발생으로 인하여 위험성이 커지게 된 것이다. 국내외 SW 안전사고의 사례를 살펴보면 그 피해의 정도와 심각성이 얼마나 크고 중요한 것인지 알 수 있다.

1) 해외 SW 안전 관련사고 사례

- 미국 북동부 대정전(2003년)

2003년 8월 14일, 미 북동부지역과 캐나다 온타리오 주에 대정전 사고가 일어나, 주민 4천만명과 온타리오 주 100만명의 주민이 피해를 입은 사례이다.

대정전의 근본적인 이유는 오하이오 주에 위치한 퍼스트에너지 사의 경고 시스템에서 발생한 SW버그 때문임이 밝혀졌으며, SW의 오류가 미 역사상 최대 규모의 정전으로 이어졌다.

- 테락-25 사건(1980~1987년)

1985년 6월 미국 방사선치료 장비인 테락-25를 사용해 치료를 받은 환자가 보통 치료에 사용되는 방사선량의 약 100배 정도의 방사선에 노출되어 사망한 사례이며, 87년 까지 총 3명의 사망자와 3명의 방사선 후유 장애 피해자가 발생하였다.

테락-25 사건은 X-ray를 안전하게 환자에게 제공할 수 있도록 하는 턴테이블을 제어하는 SW에서 오류가 발생해 저에너지 전자선과 고에너지 전자선의 변경을 인지하지 못한 것이 원인으로 밝혀졌으며, 방사선 치료기인 테락-25가 무사고 기록을 갖는 이전 모델인 테락-20을 기반으로 만들어졌고 이로 인한 SW에 대한 지나친 과신으로 SW안전성 검사가 이루어지지 않은 점이 문제가 되었다.

- 파나마 국립 암 연구소 계산 오류 (2000년)

미국의 Multidata Systems International사가 제작한 치료 계획 작성용 SW를 사용한 파나마 국립 암 연구소에서 방사선치료에서 조사되는 방사선량의 계산 오류로 인해 5명의 환자가 사망하였고 약 20명이 과잉조사에 의한 심각한 건강 피해를 입은 사례이다.

문제가 된 치료 계획 SW(RTP/2 vers.2.11)의 경우 부정확한 데이터 입력을 허용하였고 이로 인해 치료시간 계산 착오가 발생하였다.

- 밴쿠버 증권거래소 계산오류 (1982~1983년)

1982년 1월 밴쿠버 증권거래소가 새로운 주가지수를 발표하여, 22개월이 지난 1983년 11월까지 심각한 불경기나 외환위기가 없었음에도 주가지수가 절반으로 떨어진 사례이다.

주가지수 계산 SW는 주가지수의 소수점 네 번째 자리를 반올림하지 않고 버리도록 개발되어 하루에 수천 번 씩 누적되는 계산이 22개월간 누적되어 주식시장의 침체를 불러일으켰다.

- 일본 항공관제시스템 장애 (2003년)

2003년 3월 1일 도쿄 항공교통관제부에서 비행계획 정보처리 컴퓨터 시스템의 장애로 전국의 항공기 이륙이 불가능해짐에 따라 전국 57개 공항에서 약 27만 명이 피해를 입은 사례이다.

문제의 비행계획 정보처리 컴퓨터 시스템(FDP:Flight Plan Data Processing System)에서 데이터 영역의 환경을 넘어선 데이터 입력을 부정처리로 간주해 시스템 전체가 다운되는 소프트웨어상의 문제가 발생하였고, 이로 인한 전국 항공관제시스템 기능 정지가 사고 원인이 되었다.

- 워싱턴 지하철 추돌사고 (2009년)

2009년 6월 22일 역 진입을 위해 선로에 정차해 있던 열차를 뒤따르던 열차가 추돌

하여 탈선하는 사고가 발생하여, 이 사고로 인해 기관사를 포함한 9명이 사망하였고 70여명이 중경상을 입었다.

시스템 오류로 인해 뒤따라오던 열차를 정지시키지 못함과 더불어 노후화된 열차의 제동장치 시스템 교체가 제대로 이루어지지 않아 긴급제동 시스템도 작동되지 않았던 점이 사고의 원인으로 밝혀졌다.

- 유럽 아리안5호 폭파 (1996년)

1996년 6월 4일 프랑스에서 유럽우주기관이 발사한 상업용 우주선 아리안5호가 발사한지 40초 후 엔진 출력 과잉으로 공중에서 폭파하여 유럽 10여 개국이 10년 동안 들인 노력과 우주선 자체 손해비용 5억 달러 규모의 피해가 발생하였다.

사고의 원인은 64비트 숫자 값을 16비트 정수로 변환하는 과정에서 일어난 SW 버그로, 수치 오버플로우로 인한 오류가 비행 컴퓨터의 파괴를 초래하였다.

- 도요타 자동차 급가속 (2014년)

2004년부터 도요타 자동차의 일부 모델에서 급가속에 대한 불만이 접수되었고 2005년에는 운전자가 사망하는 사건까지 발생하였다. 결국 2010년부터 차량 급발진으로 인한 여러 번의 소송이 이어졌고, 2014년 3월 19일 미 연방 법무부는 도요타와 12억 달러의 제소 전 합의금에 동의했다고 발표하였다.

도요타 자동차의 급발진 원인은 전자제어장치(ECU)에 내장된 SW 결함에 의한 것으로 조사되었으며, 또한 급가속 발생 시 이를 막을 수 있는 안전 계층에도 결함이 발견되었다.

- 테슬라 자율 주행 차 사망 사고 (2016년)

2016년 5월 7일 미국 플로리다 고속도로에서 자율주행 모드로 운전 중이던 테슬라 차량이 급히 좌회전 하던 대형트레일러의 차량 밑에 깔려 운전자가 탑승자가 사망하는 사건이 발생하였다.

사건 당시 강한 태양빛에 의해 자동주행 센서가 트레일러의 흰색 옆면을 인식하지 못하였고 이 때문에 자동 급제동 시스템이 작동하지 못하였다.

- 에어버스 군 수송기 추락사건 (2015년)

2015년 5월 9일 스페인에서 시험 비행 중이던 에어버스 사의 군사수송기 A400M이 추락하는 사건이 발생하였다. 기체의 ECU SW 문제로 엔진에 연료 공급이 차단된 것을 원인으로 비행 중 엔진이 정지 상태에 빠져 추락한 사건이다.

- 대한항공801편 추락사건 (1997년)

1997년 8월6일 대한민국을 떠나 괌 아가나 국제공항에서 착륙 실패로 인한 추락으로 승객 237명과 승무원 17명을 합쳐 총 254명 둥 228명이 사망하고 26명이 부상을 입은 사고가 발생하였다.

가장 큰 사고의 원인으로는 기장의 판단 착오이지만, 괌 국제공항의 최저 안전고도 경고 시스템(MSAW)이 제도로 작동하지 않은 것도 문제로 밝혀졌다. MSAW소프트웨어의 치명적인 결함이었던 인식 반경 문제가 해결됐더라면 참사를 막았을 수도 있었을 것이다.

- 일본 지진 오보 사건 (2016년)

2016년 8월 1일 일본 도쿄에서 매그니튜드 9.0, 최대진도 7의 긴급 지진속보가 54개의 전력회사를 포함한 특정 사업자에게 전해졌다. 또한 지진속보 어플 이용자 약 500만 명 이상이 지진 오보로 인해 불안에 떨었고 수도권 일대 모든 철도 운행이 장시간 중단되었다.

오보의 원인은 전파 장애로 인한 지진 관측기의 전원시스템 오류로, 작은 SW의 문제 하나가 수백만 명을 공포에 몰아넣은 사례라고 볼 수 있다.

2) 국내 SW 안전 관련사고 사례

- 한국은행 전산망 사고 (2004년)

2004년 4월 2일 오후 3시30분부터 5시간동안 한국은행과 은행 등 131개 금융 회사간 전산망이 다운되어 금융전산결제가 마비되는 사태가 발생하였다.

단말기 관리프로그램과 중계서버운용 소프트웨어간의 충돌로 인해 전산망 연결이

끊어진 것으로, SW결함이 사고의 원인으로 밝혀졌다.

- 인천 도시철도 시스템 결함 (2016년)

2016년 8월 3일 무인 원격제어시스템으로 운행되는 인천철도 2호선은 출입문 정위치로부터 25cm 내에 정차해야만 문이 열리도록 설계됐지만 정 위치에서 65cm 지난 지점에 멈춰 문이 열리지 않아 승객들이 전동차 내부 비상스위치를 이용해 강제 개방 후 하차하게 되었다.

신호 장치의 통신장애로 인한 잇따른 정위치 정차 실패, 이 외에도 출력이상, 통신장애등 시스템 SW결함으로 인한 사고가 계속 발생하고 있다.

- KTX 운행 장애 (2011년)

2011년 2월 25일 부산에서 서울로 향하던 KTX 106호 열차가 경기도 화성시 반원 터널을 지나는 구간에서 멈춰서 40분간 운행이 중단되었다. 열 감시센서의 오작동으로 인한 운행 장애 사례로 승객들의 불편을 초래한 사례이다.

- 제주항공 지연 (2016년)

2016년 2월 19일 김해공항에서 제주공항으로 출발 예정이던 제주항공 항공편이 50분 지연된 것을 시작으로 전국에서 총 50여 편의 출발이 지연됐으며 다음날인 20일에도 총 20여 편의 항공기의 이착륙이 지연되었다.

제주항공에 예약발권 시스템을 공급하는 시타(SITA)사에서 시스템을 점검하는 과정에서 오류가 발생한 것이 비행기 지연의 원인으로 분석되었다.

- 현대자동차 리콜 사태(2015년)

2015년 2월 17일부터 현대자동차 그랜저 하이브리드 차량 총 1만604대의 리콜이 실시되었다.

리콜의 원인은 SW코딩 실수에서 비롯된 것으로, 브레이크액이 부족해도 브레이크액 부족 신호를 전송할 CAN(Controller Area Network)통신주소가 잘못 입력돼 있어 경고등이 작동하지 않았다. 코딩 한 줄의 실수가 기업의 큰 경제적 손실과 이미지 실추를

불러일으킨 사례라고 볼 수 있다.

<표 2-1> 국내외 SW 안전 관련사고 사례

국가	년도	분야	사고 사례
해외	1996	항공	• 유럽 아리랑5호 폭파
	1997	항공	• 대한항공801편 추락사건
	1980~1987	의료・방사선	• 테락-25 사건
	1982~1983	금융	• 벤쿠버 증권거래소 계산 오류
	2000	의료・방사선	• 파나마 국립 암 연구소 계산 오류
	2003	전력	• 미국 북동부 대정전
	2003	항공	• 일본 항공관제시스템 장애
	2009	철도	• 워싱턴 지하철 추돌사고
	2014	자동차	• 도요타 자동차 급가속
	2015	항공	• 에어버스 군 수송기 추락사건
	2016	자동차	• 테슬라 자율 주행 차 사망 사고
	2016	재난	• 일본 지진 오보 사건
국내	2004	금융	• 한국은행 전산망 사고
	2011	철도	• KTX 운행 장애
	2015	자동차	• 현대자동차 리콜 사태
	2016	항공	• 제주항공 지연
	2016	철도	• 인천 도시철도 시스템 결함

3. SW 안전의 의의

SW 중심사회에서 위험관리와 통제는 국가와 사회의 책임으로서 인식할 필요가 있으며, 안정성 확보를 위한 국가의 역할 수행을 위한 제도적·기술적·행정적 노력이 요구된다. 우리사회의 SW 의존도를 생각해보면, 단순히 공공부문이나 주요기반 시설에서의 SW 활용의 안전만을 고려해야 하는 것이 아니라, SW를 활용하는 전반의 안전 상태를 유지하는 것이 요구된다.

여기서 안전이란, 인적 요인에 의한 위험의 발생과 기타 인위적인 위험요인을 배제하는 것, 혹은 이와 같은 위협 요인에 대한 충분한 대비가 되어 있는 것을 의미한다. 일반적인 안전은 예상되는 위험에 대한 방지 및 대비책에 집중되어 있지만, SW안전의 경우 내부 SW오류로 인한 SW reliability(혹은 Quality)문제와 보안 문제도 고려하여야 할 것이다.

즉, SW의 이용관계 전반의 안전을 보장하고 이를 이용한 국민생활의 편리성과 국가발전의 기초를 일상적으로 유지하는 것이 SW안전의 기본 개념이며, 이를 위해서 SW 안전을 위한 정밀하고 효과적인 관리체계를 구축하는 것이 필요하다.

4. SW 안전을 위한 위험 관리

SW 안전 확보를 위한 위험 관리는 SW의 정상적 운용을 위한 회복력[2]을 갖출 수 있도록 체계를 구성하여야 한다. SW 안전 관리는 위협과 침해에 대응해서 예측, 수인, 대응, 복구 각각의 단계별로, 정부, 민간, 개인의 협력체계를 구축하여 최소한의 필수적인 SW 활용의 지속성을 유지하는 체계를 마련하는 것을 핵심으로 한다. SW를 활용하는 네트워크로 연결된 사회에서는 공격(침해)이나 위협을 전제하여, 이에 대한 예방 차원의 조치(백신 & 안티스파이웨어 등)를 사전적으로 취하는 것도 중요하나, SW에 대한 기술적 침해 위협의 특성상 완벽한 방어가 전제되지 아니한 만큼 '사건'의 발생 시(혹은 '후') 기술적 대응을 포함한 종합적이고 입체적인 문제해결(인력, 예산, 조직, 자원 등) 체계를 구조화 하는 것이 필요한 것이다. 이를 위해서는 기술적 조치뿐만 아니라 인간 행동과 규범, 기술 통제 및 기계 대 기계 상호 작용을 고려하여 원치 않는 결과발생의 예방을 위한 활동과 프로세스를 관리하여야 한다. 뿐만 아니라, 위험(위협)에 대한 인식과 평가를 통하여 위험을 분배하고 이전하거나 제거하는 등

2) World Economic Forum, 『Partnering for Cyber Resilience』, 2012, Wolrd Economic Forum, pp.14.

무력화 하는 일련의 활동이 유기적으로 이루어 질 수 있도록 하는 대응 체계를 사전에 구축해 두어야 할 것이다.

제2절 SW 안전의 이론적 근거와 연원

1. 위험사회의 위험관리의 책임

울리히 벡(Beck, Ulrich)에 의하여 설명되고 있는 위험사회(risk society)란 현대사회의 특징을 분석하기 위해 만들어낸 개념으로서, 극단적으로 단순화 하자면 산업화·근대화 등을 통하여 기술발달과 물질적 풍요가 달성되는 만큼 내재된 위험도 커진다는 것을 의미한다. 울리히 벡은 그의 저서 「위험 사회 - Risikogesellscaaft」에서 현대사회의 위험은 그저 재앙이 많아 졌다는 단순한 현상의 변화가 아니라, 재앙이 사회 속의 하나의 구조적 요소가 되었다고 설명하고 있다. 즉, 예외적 위험이 아닌 일상적 위험 —생태학적 재앙, 핵 위기, 실업과 금융대란, 환경파괴, 지구온난화 등— 이 만연하는 사회라는 의미이다. 이는 과학기술의 획기적인 발전을 통해 많은 물질적인 풍요를 누리게 됨과 동시에, 그에 대한 대가로 우리가 살아가는 데 있어서 위험도가 증가하게 된 현대 사회의 특성을 나타내는 방법이라고 할 수 있다. 이러한 위험사회논의는 위에서 열거한 물리적 위험뿐만 아니라, 인간 생활의 피로도를 극대화하는 방식 또는 권리나 재산의 침해하는 방식으로 작용하여 심리적인 타격으로까지 확대되는 현상을 설명할 때에도 충분히 의의가 있다. 특히, SW에 의존하여 기술 진보의 혜택을 다양한 분야에서 향유하고 있는 현재 SW에 대한 위협과 침해상황 또한 구조적인 위험으로서 국가와 사회의 책임 있는 대응이 요구되는 지점이라고 할 수 있다.

제도적 관점에서 위험사회의 평가와 행정상의 위험관리의 문제는 곧 국가와 사회의 책임으로서 한 영역으로 인식되게 되는 것이며, 안정성 확보를 위한 국가의 예방적 역할의 수행 및 위험관리(위협과 침해에 대응)를 위해 입법이라는 수단(근거 마련)을 사용하게 되고, 최종적으로 국가의 안전성 보장에 대한 책임은 입법 작용을 담당하는 의회에 있다는 것을 의미한다.[3] 즉, 위험사회에서는 위험을 하나의 구조로 인식함으로써 국가와 사회는 위험의 발생을 억제하기 위하여 스스로의 역할에 관한 성찰이 이루어지며, 위험예방의 작용을 강구하게 되는데, 위험예방 수단을 마련하는 방식은 입법을 통하여 이루어지며, 법치국가에서의 입법기능은 의회에 있으므로 그 책임과 역할이 의회에 주어진 다는 것이다.

결국 위험을 예측하거나 경험하는 등 인식하게 되면 국가 및 행정은 위험방지 및 관리를 위해 규범적 대응(입법 작용)을 하게 되는데, 법률이 가지는 추상성[4]이나 입법

3) 강문수, “위험사회에서의 입법”, 「토지공법연구」제32집, 한국토지공법학회, 2006, 342면.

절차의 한계[5]를 가지기 때문에 다양한 원칙과 입법형식[6]을 통해 구현되고 있으나, 근본적으로 행정법상의 위험관리를 위하여 추상적 위험에 대한 대응방안을 입법적으로 구현하는 경우 국가권력(공권력)의 과잉된 행사로 기본권이 축소되고, 국가에 의한 또 다른 위험이 야기될 수 있는 부작용도 존재하므로 이러한 관점의 이해도 충분히 이루어져야 하는 것이다.

즉, 위에서 살펴본 SW 안전을 구현하기 위한 국가의 제도적 대응으로서 SW 안전법제의 형성이 요구되는 것이다. 이러한 입법형성의 근거를 활용하여 국민의 생활안전과, 국가의 발전을 안정적으로 구현할 수 있도록 지원하는 SW 안전관리에 관한 입법을 고려할 수 있을 것이다.

2. 제조물 책임과 SW의 안전성 확보

제조물 책임이란 제조되어 시장에 유통된 상품(제조물)의 결함으로 인하여 그 상품의 이용자 또는 제3자의 생명, 신체나 재산에 손해가 발생한 경우에 제조자 등 제조물의 생산, 판매과정에 관여한 자의 과실 유무에 관계없이 제조자 등이 그러한 손해에 대하여 책임을 지도록 하는 법이론을 의미한다. 이는 시장에 제품을 제조하여 유통시킨 제조업자가 소비자의 안전에 대해 요구되는 여러 가지 작위의무를 이행하지 못함으로 인하여 생명, 신체 또는 재산상의 손실을 입은 자에게 행한 위법행위에 대한 일반불법행위법상의 책임을 지우면서 나온 것이었는데, 이때 제조업자가 지는 책임은 과실을 요건으로 하였다가(과실책임), 현재의 제조물책임에서는 무과실책임 내지 엄격

---

4) 성문법령이 가지고 있는 추상적인 특성은 법률규정이 인간사회의 모든 관계들을 사사건건 규율하는 것이 아니라 해당 사안들의 유사점을 도출하고, 일반화하여 해당하는 경우를 법령에 규정된 내용에 맞추어 규율하는 방식을 사용하고 있는 것이다. 이러한 법령의 여지는 입법자의 입장에서 보편적으로 사전에 예상 가능한 분쟁상태 또는 법률관계의 명확한 구분이 필요한 영역까지 가능할 것이라 생각된다. 이러한 예상의 범위를 넘어서는 획기적인 사건들의 발생이 법적공백을 초래하고 질서가 유지되고 있는 상태의 법률관계를 불안하게 만드는 것이다. 특히 최근의 과학기술의 발전은 법제도가 준비되지 않았음에도 불구하고 서비스 수요가 발생하고 그와 더불어 기대하지 못한 통제범위 밖의 분쟁들이 발생하는 사례가 빈번하게 일어나고 있다.

5) 물리적으로 입법(제정)이나 개정을 위해서는 의견수렴 과정과 법률의 내용에 대한 정련과정이 필수적으로 부여되어야 하고 그렇게 함으로써 헌법에 배치되지 않으면서 입법목적을 달성할 수 있는 효과적인 입법이 달성될 수 있기 때문이다. 법률이 가지는 정책적 목적과 필요성을 충족시키기 위한 과정이 입법과정 속에 녹아 있다고 보아야 하는 것이다. 그러나 이러한 물리적인 "시간"의 필요는 단순히 감내하여야 할 어쩔 수 없는 부분으로 치부되어서는 안될 것이다. 신속하게 법적 판단을 요하는 사안의 경우에는 개정이나 입법 절차를 두고 기다릴 수 없을 만큼 당사자에게 커다란 가치가 달려있는 문제일 것이기 때문이다. 또한 현대의 입법수요는 우선 그 양이 대단히 많고 그 분야 또한 추상적이고 상징적인 선언적 입법으로부터 극히 전문적이고 기술적인 입법에 이르기까지 그 범위가 매우 넓으며, 입법수요의 분출도 예측하지 못한 계기로부터 급작스럽게 이루어지고 그 빈도 역시 상당히 잦다고 할 수 있다. 이러한 방대한 양과 다양한 요구가 입법체계에 투입되는 것에 비하여 입법체계내의 전환과정을 거친 산출의 양과 질이 보잘 것 없고, 입법수요에 신속하게 대응하지 못한다면 이는 입법체계에 위협이 될 수 있다.

6) 강문수, “위험사회에서의 입법”, 「토지공법연구」제32집, 한국토지공법학회, 2006, 346-352면 참조.

책임을 인정하는 것이다.

제조물책임은 사고발생 이후에 관한 문제로서 일차적 목적이 소비자의 피해에 대한 금전적 배상이지만, 궁극적으로는 생산자로 하여금 위험을 예측하여 해결책을 세우도록 하고, 생산자가 소비자의 피해배상에 지출하는 비용, 즉 사회적 비용을 제품의 안정성 향상에 투자토록 유도하는 사후적 안전규제수단이라고 할 수 있다.[7)]

제조물 책임법 상 "결함"이란 제조물에 통상적으로 기대할 수 있는 안전성이 결여되어 있는 것이나 제조물이 원래 의도한 설계와 다르게 제조·가공됨으로써 안전하지 못하게 된 경우를 의미한다[8)]. 이 때, 제조업자의 면책 항변사유는 공급 당시 법령에서 정하는 기준을 준수하였음에도 결함이 발생할 경우이며, 면책 항변사유의 실권은 결함의 존재를 알고도 손해발생을 방지하기 위한 적절한 조치를 하지 아니한 경우라고 볼 수 있다. 그러나 일반 제조물 탑재 SW에서의 결함의 개념과 기반시설에 탑재된 SW 결함의 개념이 관점에 따라 상이할 수 있고, 책임에 대한 부과 내용도 다를 수 있기에 관련 법안의 혁신안을 제시하기 이전에 해당 차이점에 대한 분석과 연구가 선행되어야 할 것이다.

국민들의 일상적인 SW 활용의 안전을 보장하기 위해서는 상용 SW의 품질을 향상하고 지속적인 유지관리가 이루어질 수 있도록 해야 한다. 뿐만 아니라, SW 사용의 전제가 되는 여러 요건(통신망 및 통신서비스의 이용 등)들의 안전 또한 고려되어야 한다. 제조물 책임의 법리는 이러한 SW 활용 환경의 위험요소를 확인하고, 위험을 억제하고 SW 활용의 안정성을 유지할 수 있는 대응방안을 마련하는 형태로 규율체계를 확장할 필요가 있다. 특히 SW의 활용은 사적 관계에서도 자유롭게 이루어지는데, SW의 생산 및 보급, 이용이라는 일련의 서비스 과정에서 위협에 대처할 수 있는 역량을 갖춘 자는 제조자 혹은 제공자에게 있는 것이 일반적이다. SW의 안전한 사용 이외의 자체적 결함이 존재하거나 위협에 대응할 수 있는 평가 기준을 만족했다는 구체적 입증이 되지 아니하는 경우 사업자에게 일정한 책임을 부여하여 연결된 SW 사용관계에서 안전관리 면밀하게 이루어질 수 있도록 할 수 있을 것이다.

---

7) 사전적 안전규제로서 사고 예방을 위한 안전기준의 제정과 사업에 대한 인가·허가 또는 검사 등은 국가의 역할로서 공적 영역의 수단이라고 할 수 있다.

8) 제조물 책임법 제2조(정의) 2. "결함"이란 해당 제조물에 다음 각 목의 어느 하나에 해당하는 제조상·설계상 또는 표시상의 결함이 있거나 그 밖에 통상적으로 기대할 수 있는 안전성이 결여되어 있는 것을 말한다.
가. "제조상의 결함"이란 제조업자가 제조물에 대하여 제조상·가공상의 주의의무를 이행하였는지에 관계없이 제조물이 원래 의도한 설계와 다르게 제조·가공됨으로써 안전하지 못하게 된 경우를 말한다.
나. "설계상의 결함"이란 제조업자가 합리적인 대체설계(代替設計)를 채용하였더라면 피해나 위험을 줄이거나 피할 수 있었음에도 대체설계를 채용하지 아니하여 해당 제조물이 안전하지 못하게 된 경우를 말한다.
다. "표시상의 결함"이란 제조업자가 합리적인 설명·지시·경고 또는 그 밖의 표시를 하였더라면 해당 제조물에 의하여 발생할 수 있는 피해나 위험을 줄이거나 피할 수 있었음에도 이를 하지 아니한 경우를 말한다.

제3절 SW 안전의 정책적 의미

1. 국가 운용의 필수적인 기반 시설에 대한 SW 안전

SW중심사회에서는 국민들의 기본적 삶이 유지하기 위해 필요한 공공서비스 또한 SW를 활용한다. SW가 중심이 되어 해당 서비스가 운용되는 것이 현재의 지능정보사회의 현실인 것이다. 고로 국민생활의 기초 혹은 필수적 유지를 위하여 국가운영에 필요한 SW의 안전 확보를 고려해야만 할 것이다. 이는 우리 사회가 활용하는 모든 SW에 대한 안전을 대상으로 하는 것이 아니라, 국민의 생활 안전(생명, 신체, 재산)을 위해 필수적으로 국가가 제공하는 각종 물리적, 논리적 서비스가 최소한 유지될 수 있도록 하는 범위 내의 SW 안전을 대상으로 해야 할 것이며, 국가가 적극적으로 공권력을 행사할 수 있는 영역인 공적영역(공공부문)이 그 구체적인 관리 대상이 되어야 한다.

2. 국민생활의 안정을 위한 SW 안전 확보

지능정보사회에서의 SW간 연결은 최종이용자인 개별 인격들에게까지 이어지기 마련이다. 이렇듯 SW 활용의 범위가 공적 영역 혹은 국가 기반체계에 국한되는 것이 아니고, 일반 사용자에게까지 확장되어 있는 만큼 이를 이용하는 국민들에게 불편함이 발생하지 않도록 SW의 안전 상태를 보장하는 것이 필요하다. SW 이용관계 전반의 안전을 관리하고 규율하기 위해서는 국가가 단순히 공적영역에 한하여 역할 수행으로는 한계가 있기 때문에 SW를 생산하거나 제공하는 사업자, SW를 이용하는 이용자에게도 특별한 책임과 역할을 부여할 필요가 있다. 이러한 경우 국민의 기본권을 제한하지 아니하는 방식으로 책임 부여를 설계하여야 한다.

제4절 소결

SW중심사회의 도래로 사회 속 인간의 삶의 질을 향상시키는 수단으로서 SW의 활용도가 상당히 높아졌지만, 이러한 사회에서의 생활에서 이전에는 존재하지 않았던 새로운 차원의 문제들이 증가하고 있다. 이러한 문제들은 특히 국민의 생명과 신체 재산을 상당히 위협할 수 있는 정보통신, 에너지, 교통, 금융, 원자력 등과 관련한 국가기반시설에도 발생할 수 있기에 이에 대비한 대응책의 마련이 더욱 시급한 것이다. 실제로 최근 몇 년 동안 국내외에서 SW로 인해 발생한 대규모 사고 사례들은 무수히도 많이 발생하고 있는 중이다.

이 때문에 우리는 근본적인 SW 안전 대책을 마련하기 위한 법제개선방안을 마련하기 위한 선행 연구로써 울리히 벡의 위험사회론과, 제조물 책임과 관련한 법이론을 분석하였다. 위험사회론의 분석을 통하여 SW중심사회에서 증가하는 위험 책임의 분배와SW 안전을 실제적 구현을 위하여 국가의 제도적 대응으로서 SW 안전 법제의 형성이 요구됨을 알 수 있었다. 또한 제조물 책임 법이론의 분석을 통하여 SW가 탑재된 제조물 혹은 시설에 대한 책임 부과에 대한 균형적 시각과 고려하여야 할 요건들을 검토하였다.

결론적으로 본 연구에서 국가 운용의 필수적인 시설인 국가중요기반시설들에 대한 SW 안전 확보를 통하여 국민생활의 안정을 도모하고자 하며, 이를 위해 국내외의 주요기반시설 보호 법제를 분석분류함을 통해 SW법제 마련을 위한 시사점을 도출하고 개선 방안을 제시하고자 한다.

제3장 국내 기반시설 보호 법제 분석

제1절 국가주요기반시설 안전보호 체계

1. 국가 안전보호를 위한 법체계

대한민국 헌법은 제34조 6항의 ‘국가는 재해를 예방하고 그 위험으로부터 국민을 보호하기 위하여 노력하여야 한다’라는 조항을 통하여 국가가 재해로부터 생길 수 있는 위험으로부터 국민을 보호해야한다는 의무를 명확히 명시하고 있다. 해당 헌법 조항에 따라 국가는 각종 재난으로부터 국토를 보존하고 국민의 생명·신체 및 재산을 보호하기 위하여 『재난 및 안전관리 기본법』을 두고 있고, 그 아래 재난안전 및 기본법 제22조 및 동법 시행령 제26조를 통하여 국가 재난 및 안전관리의 기본방향을 설정하는 최상위 계획인 ‘국가안전관리기본계획’을 두고 있다. 특히 전자적 침해행위와 주요정보통신기반시설과 관련된 분야에서는 주요정보통신기반시설의 보호에 관한 대책을 수립·시행하며 이를 안정적으로 운용하여 최종적으로 국가의 안전과 국민생활의 안정을 보장하기 위한 『정보통신기반보호법』을 별도로 규정하고 있다.

또한 국가기반체계를 직·간접적으로 구성하는 시설·기능·시스템 보호를 위한 체계들도 다양한 법률을 통하여 규율되어 있으며, 법률 내에 대상 시설의 지정 목적과 범위, 방법이 상세히 규정되어 있다. 세부 법률에 따른 규정 시설 범위는 다음과 같다.

<표 3-1> 국가기반체계 관련 시설물의 지정범위

법률	조항	규정 시설	정의
국토의 계획 및 이용에 관한 법률	제2조	기반시설	• 교통시설, 공간시설, 유통·공급시설, 공공·문화체육시설, 방재시설, 보건위생시설, 환경기초시설
사회기반시설 민간투자법	제2조	사회 기반시설	• 각종 생산 활동의 기반이 되는 시설, 해당 시설의 효용을 증진시키거나 이용자의 편의를 도모하는 시설 및 국민생활 편익을 증진시키는 시설

시설물의 안전관리에 관한 특별법	제2조	시설물	• 건설공사를 통하여 만들어진 구조물과 그 부대시설
		1종시설물	• 도로·철도·항만·댐·교량·터널·건축물 등 공중의 이용편의와 안전을 도모하기 위하여 특별히 관리할 필요가 있거나 구조상 유지관리에 고도의 기술이 필요하다고 인정하여 대통령령으로 정하는 시설물
		2종시설물	• 1종시설물 외의 시설물로서 대통령령으로 정하는 시설물
재난 및 안전관리 기본법	제26조	국가 기반시설	• 국가기반체계를 보호하기 위하여 계속적으로 관리할 필요가 있다고 인정되는 시설
	제27조	특별관리 대상시설	• 중앙행정기관의 장 또는 지방자치단체의 장이 재난이 발생할 위험이 높거나 재난예방을 위하여 계속적으로 관리할 필요가 있다고 인정되는 시설 및 지역 중에서 대통령령으로 정하는 바에 따라 지정하는 시설
통합방위법	제2조	국가 중요시설	• 공공기관, 공항·항만, 주요 산업시설 등 적에 의하여 점령 또는 파괴되거나 기능이 마비될 경우 국가안보와 국민 생활에 심각한 영향을 주게 되는 시설

• 『국토의 계획 및 이용에 관한 법률』 (‘기반시설’ 규정)

『국토의 계획 및 이용에 관한 법률』(이하 ‘국토법’이라 함) 제2조 제6호에서 ‘기반시설’을 교통시설, 공간시설, 유통·공급시설, 공공·문화체육시설, 방재시설, 보건위생시설, 환경기초시설로 분류하고 있으며 동법 시행령 제2조(기반시설)에 따른 세부 시설들은 <표 3-2>과 같다.

<표 3-2> 국토법에 따른 기반시설의 분류 및 세부 시설

분야	세부 시설
교통시설	• 도로·철도·항만·공항·주차장·자동차정류장·궤도·운하, 자동차 및 건설기계검사시설, 자동차 및 건설기계운전학원
공간시설	• 광장·공원·녹지·유원지·공공공지
유통·공급 시설	• 유통업무설비, 수도·전기·가스·열공급설비, 방송·통신시설, 공동구·시장, 유류저장 및 송유설비
공공·문화 체육시설	• 학교·운동장·공공청사·문화시설·체육시설·도서관·연구시설·사회복지시설·공공직업훈련시설·청소년수련시설
방재시설	• 하천·유수지·저수지·방화설비·방풍설비·방수설비·사방설비·방조설비
보건위생시설	• 화장시설·공동묘지·봉안시설·자연장지·장례식장·도축장·종합의료시설
환경기초시설	• 하수도·폐기물처리시설·수질오염방지시설·폐차장

• 『사회기반시설 민간투자법』(‘사회기반시설’ 규정)

『사회기반시설 민간투자법』은 제2조에서 ‘사회기반시설’을 각종 생산 활동의 기반이 되는 시설, 해당 시설의 효용을 증진시키거나 이용자의 편의를 도모하는 시설 및 국민생활의 편익을 증진시키는 시설로 정의하고 있다.

해당 법에서 말하는 ‘사회기반시설’의 범위는 『도로법』 제2조에 따른 도로 및 도로의 부속물, 『철도사업법』 제2조에 따른 철도, 『도시가스사업법』 제2조에 따른 가스공급시설 등 총 49개 법률에 따른 다양한 시설들을 포함한다. 또한 『국가회계기준에 관한 규칙』 제14조에서도 ‘사회기반시설’에 대하여 국가의 기반을 형성하기

위하여 대규모로 투자하여 건설하고 그 경제적 효과가 장기간에 걸쳐 나타나는 자산으로서, 도로, 철도, 항만, 댐, 공항, 기타 사회시설 및 건설 중인 시설로 정의하여 국가 재정활동 중에 발생하는 유·무형자산 외의 시설자산이라고 정의하여 재정상태표에 표기되는 모든 시설을 포괄하도록 하고 있다.

- 『시설물의 안전관리에 관한 특별법』('1·2종 시설물' 규정)

『시설물의 안전관리에 관한 특별법』 제2조에서는 '시설물'을 건설공사를 통하여 만들어진 구조물과 그 부대시설이라고 정의하고, '1종시설물'을 도로·철도·항만·댐·교량·터널·건축물 등 공중의 이용편의와 안전을 도모하기 위하여 특별히 관리할 필요가 있거나 구조상 유지관리에 고도의 기술이 필요하다고 인정하여 대통령령으로 정하는 시설물로, '2종시설물'을 1종시설물 외의 시설물로서 대통령령으로 정하는 시설물로 정의하고 있다.

시설물은 동법 제10조의2(시설물의 안전등급 지정 등)에 따라 정밀점검이나 정밀안전진단을 실시하고, 그 시설물의 안전등급을 지정하여야만 하며 안전등급 기준은 동법 시행령 제11조의5(안전등급 기준)에 따라 A등급(우수), B등급(양호), C등급(보통), D등급(미흡), E등급(불량)으로 평가하도록 되어있다.

- 『재난 및 안전관리 기본법』('국가기반시설' 규정)

『재난 및 안전관리 기본법』 제26조(국가기반시설의 지정 및 관리 등)에서는 '국가기반시설'을 국가기반체계를 보호하기 위하여 계속적으로 관리할 필요가 있다고 인정되는 시설로 정의하고 있다.

동법 제25조의2(재난관리책임기관의 장의 재난예방조치)에서는 재난관리책임기관의 장이 소관 관리대상 업무의 분야에서 재난 발생을 사전에 방지하기 위하여 국가기반시설의 관리에 대한 예방조치를 취하도록 규정하고 있다.

- 『재난 및 안전관리 기본법』('특별관리대상시설' 규정)

『재난 및 안전관리 기본법』 제27조(특별관리대상시설등의 지정 및 관리 등)에서는 '특정관리대상시설'을 중앙행정기관의 장 또는 지방자치단체의 장이 재난이 발생할 위험이 높거나 재난예방을 위하여 계속적으로 관리할 필요가 있다고 인정되는 시설

및 지역 중에서 대통령령으로 정하는 바에 따라 지정하는 시설이라고 정의하고 있다.

동법은 특별관리대상시설을 보호하기 위하여 재난 발생의 위험성을 제거하기 위한 장기·단기 계획의 수립·시행, 그에 따른 안전점검 또는 정밀 안전진단, 그밖에 특정관리대상시설 등의 관리·정비에 필요한 조치를 취하도록 규정하고 있다.

- 『통합방위법』(‘국가중요시설’ 규정)

『통합방위법』은 적의 침투·도발이나 그 위협에 대응하기 위하여 국가 총력전의 개념을 바탕으로 국가방위요소 통합·운용에 필요한 통합바위 대책 수립·시행에 대한 규정을 담고 있으며, 제2조에서 ‘국가중요시설’을 공공기관, 공항·항만, 주요 산업시설 등 적에 의하여 점령 또는 파괴되거나 기능이 마비될 경우 국가안보와 국민생활에 심각한 영향을 주게 되는 시설이라고 정의하고 있다.

국가중요시설 지정 및 방호 훈령 제5조(국가중요시설의 대상)에 따르면 국가중요시설의 지정 범위는 <표 3-3>과 같다. 국가중요시설은 시설의 기능·역할의 중요성과 가치의 정도에 따라 기곤, 산업, 전력, 방송, 정보통신, 교통, 수원의 분야에서 가·나·다 등급으로 구분하여 보호되고 있다.

<표 3-3> 통합방위법의 국가중요시설 지정 범위

번호	국가중요시설의 대상
1	• 주요 국가 및 공공기관시설
2	• 철강, 조선, 항공기, 정유, 중화학, 방위산업, 대규모 가스·유류 저장시설 등 주요 산업시설
3	• 원자력 발전소, 대용량 발전소 및 변전소 등 주요 전력시설
4	• 전국 및 지역권 방송국, 송신·중계소 등 주요 방송시설
5	• 국제위성지구국, 해저통신중계국, 국가기간전산망, 전화국 등 주요 정보통신시설
6	• 철도 교통관제 센터 및 지하철 종합사령실, 교량, 터널 등 주요 교통시설
7	• 주요 국제·국내선 공항
8	• 대형 선박의 출·입항이 가능한 항만
9	• 대형 취수·정수시설 및 다목적 댐 등 주요 수원시설

10	• 종합적인 체계를 갖춘 연구시설, 핵연료 개발 연구시설 등 국가안보상 중요한 과학연구시설
11	• 교정·정착지원 시설
12	• 전력, 통신 상수도, 가스 등을 수용하고 있는 대도시 주요 지하공동구 시설
13	• 기타 적에 의해 점령 또는 파괴되거나 기능이 마비될 경우 국가안보 및 국민생활에 심대한 영향을 미치는 시설

2. 재해 및 재난 관련 법제

우리나라의 재해 및 재난과 관련한 법제의 발전은 1970년대부터 시작 되었고, 현재에 이르기까지의 법제 발전 단계는 크게 4단계로 나눌 수 있다.

- 1970년대 : 사회적 재난과 관련된 민방위기본법이 처음 제정되고 정비된 시기
- 1980~1990년대 : 자연재해 및 인적재난과 관련하여 농어업재해대책법, 소방법, 철도법, 도로법, 건축법 등 분야별 개별 법령들이 제정되고 정비된 시기
- 1990년대 후반 : 여러 가지 자연적 재해와 인적 재난이 상당히 많이 일어나면서, 분야별 법률들을 통합적으로 관리해야할 필요성이 생김에 따라 자연재해 관련 사항은 자연재해대책법으로, 인적재난 관련 사항은 재난관리법으로 통합
- 2000년대 초반 : 재해와 재난을 관리하는 체계에 대한 연구가 더욱 진행되고, 통합적 법령의 필요성이 더욱 대두되면서, 자연재해 및 인적재난을 종합적으로 규율할 수 있는 『재난 및 안전관리 기본법』이 제정

『재난 및 안전관리 기본법』제3조에 따르면 '재난'이란 국민의 생명·신체·재산과 국가에 피해를 주거나 줄 수 있는 것으로서 재난의 종류를 '자연재난'과 '사회재난'으로 나누고 있다.

- 자연재난 : 태풍, 홍수, 호우(豪雨), 강풍, 풍랑, 해일(海溢), 대설, 낙뢰, 가뭄, 지진, 황사(黃砂), 조류(藻類) 대발생, 조수(潮水), 화산활동, 소행성·유성체 등 자연우주물체의 추락·충돌, 그 밖에 이에 준하는 자연현상으로 인하여 발생하는 재해
- 사회재난 : 화재·붕괴·폭발·교통사고(항공사고 및 해상사고를 포함한다)·화생방사고·환경오염사고 등으로 인하여 발생하는 대통령령으로 정하는 규모 이상의

피해와 에너지 · 통신 · 교통 · 금융 · 의료 · 수도 등 국가기반체계의 마비, 「감염병의 예방 및 관리에 관한 법률」에 따른 감염병 또는 「가축전염병예방법」에 따른 가축전염병의 확산 등으로 인한 피해

『재난 및 안전관리 기본법』제3조 3항은 '재난관리'를 재난의 예방·대비·대응·복구를 위하여 행하는 모든 활동을 말한다고 규정하고 있으며, 이에 따라 재난관리 관련 법령은 이러한 재난관리와 관련 되는 모든 법령들을 포괄한다고 볼 수 있다.

재난을 관리할 수 있는 다양한 활동들을 규정함으로써 『재난 및 안전관리 기본법』의 목적을 달성하기 위하여, 재난의 종류와 분야에 따라 『자연재해대책법』, 『지진·화산재해대책법』 등의 재난 관련 법률들이 제정되어 있다.

- 『자연재해대책법』

『자연재해대책법』은 태풍, 홍수 등 자연현상으로 인한 재난으로부터 국토를 보존하고 국민의 생명·신체 및 재산과 주요 기간시설을 보호하기 위하여 자연재해의 예방·복구 및 그 밖의 대책에 관하여 필요한 사항을 규정하고 있다.

해당 법은 『재난 및 안전관리 기본법』의 목적에 따라 국가에게 자연재해의 예방 및 대비에 관한 종합계획을 수립하여 시행할 책무를 부여하고, 그 시행을 위한 최대한의 재정적·기술적 지원을 요구하고 있다. 동법은 제1장 총칙, 제2장 자연재해의 예방 및 대비, 제3장 재해정보 및 비상지원, 제4장 재해복구, 제5장 방재기술의 연구 및 개발, 제6장 보칙, 제7장 벌칙의 내용을 담고 있다.

- 『지진·화산재해대책법』

『지진·화산재해대책법』은 지진·지진해일 및 화산활동으로 인한 재해로부터 국민의 생명과 재산 및 주요 기간시설을 보호하기 위하여 지진·지진해일 및 화산활동의 관측·예방·대비 및 대응, 내진대책, 지진재해 및 화산재해를 줄이기 위한 연구 및 기술개발 등에 필요한 사항을 규정하고 있다.

해당 법은 『재난 및 안전관리 기본법』의 목적에 따라 지진재해 및 화산재해로부터 국민의 생명과 재산, 주요 기간시설을 보호하기 위하여 지진·지진해일 및 화산활동을 관측·예방·대비 및 대응, 내진대책, 지진·화산재해를 줄이기 위한 연구 및 기술개

발 등에 대한 계획을 수립하여 시행할 책무를 부여하고, 그 시행을 위한 재정적·기술적 지원을 요구한다. 동법 제1장 총칙, 제2장 지진·지진해일 및 화산활동 관측, 제3장 예방과 대비, 제4장 내진대책, 제5장 대응, 제6장 지진·화산재해경감을 위한 연구와 기술개발, 제7장 보칙, 제8장 벌칙 등으로 구성되어 있다.

그 외 재해구호법, 급경사지 재해예방에 관한 법률, 농어업재해대책법, 재해경감을 위한 기업의 자율 활동 지원에 관한 법률, 재해위험 개선사업 및 이주대책에 관한 특별법, 저수지·댐의 안전관리 및 재해 예방에 관한 법률, 소하천정비법 등 다양한 재난 위험 분야들과 관련하여 '자연재난'과 '사회재난'을 대비하고 관리하기 위한 다양한 법률이 제정되어 있다.

국가 및 사회에서 발생할 수 있는 다양한 재난 및 사고를 담당하는 재난관리주관기관은『재난 및 안전관리 기본법』 시행령 (별표 1의3)을 통해 지정되어 있으며 재난 및 사고의 세부 유형별 주관기관 지정은 <표 3-4>과 같다.

<표 3-4> 재난관리주관기관별 담당 재난 및 사고 유형

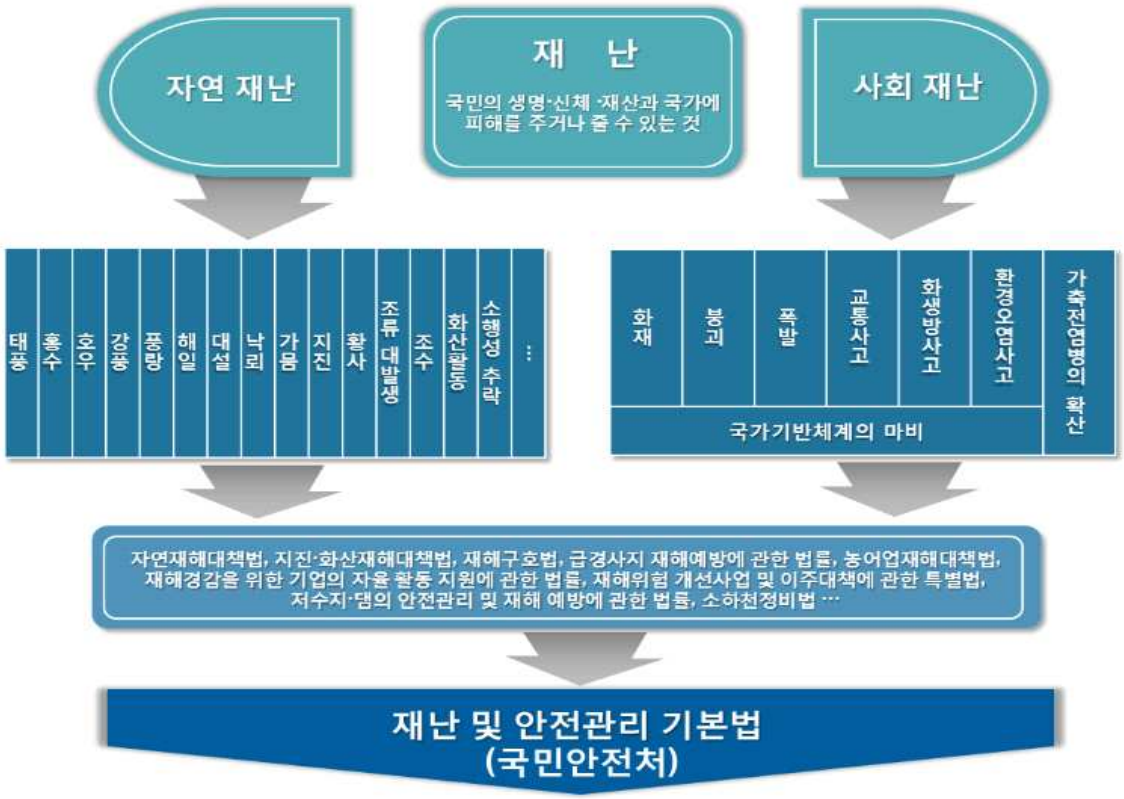
재난관리주관기관	재난 및 사고의 유형
교육부	• 학교 및 학교시설에서 발생한 사고
미래창조과학부	• 우주전파 재난 • 정보통신 사고 • 위성항법장치 전파혼신
외교부	• 해외에서 발생한 재난
법무부	• 교정시설에서 발생한 사고
국방부	• 국방시설에서 발생한 사고
문화체육관광부	• 경기장 및 공연장에서 발생한 사고
농림축산식품부	• 가축 질병 • 저수지 사고
산업통상자원부	• 가스 수급 및 누출 사고 • 원유수급 사고 • 원자력안전 사고 • 전력 사고 • 전력생산용 댐의 사고

보건복지부	• 감염병 재난 • 보건의료 사고
환경부	• 수질분야 대규모 환경오염 사고 • 식용수 사고 • 유해화학물질 유출 사고 • 조류 대발생 • 황사
고용노동부	• 사업장에서 발생한 대규모 인적 사고
국토교통부	• 국토교통부가 관장하는 공동구 재난 • 고속철도 사고 • 국토교통부가 관장하는 댐 사고 • 도로터널 사고 • 식용수 사고 • 육상화물운송 사고 • 지하철 사고 • 항공기 사고 • 항공운송 마비 및 항행안전시설 장애
해양수산부	• 조류 대발생 • 조수 • 해양 분야 환경오염 사고 • 해양 선박 사고
국민안전처	• 공동구 재난 • 정부중요시설 사고 • 화재·위험물 사고, 내륙에서 발생한 유도선 등의 수난 사고 • 다중 밀집시설 대형ㅅ고 • 풍수해·지진·화산·낙뢰·가뭄으로 인한 재난 및 사고로서 다른 재난관리주관기관에 속하지 아니하는 재난 및 사고 • 해양에서 발생한 유도선 등의 수난 사고
금융위원회	• 금융 전산 및 시설 사고
원자력안전위원회	• 원자력안전 사고 • 인접국가 방사능 누출 사고
문화재청	• 문화재 시설 사고
산림청	• 산불 • 산사태

재난관리주관기관이 지정되지 아니한 재난 및 사고에 대해서는 중앙재난안전대책본부장이 『정부조직법』에 따른 관장 사무를 기준으로 재난관리주관기관을 정한다.

재난관리주관기관 중 특히 국민안전처는 『재난 및 안전관리 기본법』 제6조(재난 및 안전관리 업무의 총괄 · 조정)에 따라 국가 및 지방자치단체가 행하는 재난 및 안전관리 업무를 총괄 · 조정하도록 규정되어 있는 모든 재난(자연 · 안전 재난)을 통합적으로 조정 · 지원하고 있으며, 중앙재난안전대책본부 및 중앙사고수습본부를 통한 실질적인 재난 컨트롤 타워 역할을 수행하고 있다.

[그림 3-1] 재난의 종류 및 관련 재난 관련 법 체계



3. 주요국가기반시설 보호 체계

1) 국가기반시설 보호 체계 개관

국가 안전보호를 위한 법체계에서 다루었듯이, 국가기반체계를 직 · 간접적으로 구성하는 시설 · 기능 · 시스템 보호를 위해 다양한 법률에서 정의하고 있는 시설들은 다음과 같다.

- 기반시설(국토의 계획 및 이용에 관한 법률)

- 사회기반시설(사회기반시설 민간투자법)
- 1·2종시설물(시설물의 안전관리에 관한 특별법)
- 국가기반시설(재난 및 안전관리 기본법)
- 특별관리대상시설(재난 및 안전관리 기본법)
- 국가중요시설(통합방위법)

그 중에서도 국가 주요시설의 차원에서 재난과 안전에 관련된 사항을 총괄적으로 규율하고 있는 『재난 및 안전관리 기본법』에서 정의하고 있는 '국가기반시설' 이 국가 안전보호 체계 전체에서 가장 우선적이고 중점적으로 보호되어야하는 부분이라고 할 수 있다.

2) 국가기반시설의 지정

국가기반시설은 『재난 및 안전관리 기본법』 제26조(국가기반시설의 지정 및 관리 등)에 의해 다음과 같이 지정된다.

『재난 및 안전관리 기본법』

제26조(국가기반시설의 지정 및 관리 등)

관계 중앙행정기관의 장은 소관 분야의 기반시설 중 제3조제1호 나목에 따른 국가기반체계를 보호하기 위하여 계속적으로 관리할 필요가 있다고 인정되는 시설(이하 "국가기반시설"이라 한다)을 다음 각 호의 기준에 따라 조정위원회의 심의를 거쳐 지정할 수 있다.

1. 다른 기반시설이나 체계 등에 미치는 연쇄효과
2. 둘 이상의 중앙행정기관의 공동대응 필요성
3. 재난이 발생하는 경우 국가안전보장과 경제·사회에 미치는 피해 규모 및 범위
4. 재난의 발생 가능성 또는 그 복구의 용이성

『재난 및 안전관리 기본법』 시행령

제30조(국가기반시설의 지정 등)

관계 중앙행정기관의 장은 소관 재난관리책임기관의 장이나 해당 시설 관리자의 의견을 들어 법 제26조제1항 각 호와 별표 2의 기준에 적합하게 국가기반시설을 지정하여야 한다.

국가기반시설은『재난 및 안전관리 기본법』시행령 제30조(국가기반시설의 지정 등)과 (별표2)를 통해 세부적으로 지정되며, 에너지・정보통신・교통수송・금융・보건의료・원자력・환경・식용수・정부중요시설 총 9가지 분야로 나눠진다.

<표 3-5> 국가기반시설의 분야별 지정기준

분야	지정기준
에너지	• 전력, 석유, 가스 공급에 필요한 생산, 공급시설과 비축시설
정보통신	• 교환기 등 주요 통신장비가 집중된 시설 및 정보통신 서비스의 전국 상황 감시시설, 국가행정을 운영, 관리에 필요한 기간망과 주요 전산 시스템
교통수송	• 인력 수송과 물류 수송을 담당하는 체계와 실제 운용하는 데에 필요한 교통, 운송시설 및 이를 통제하는 시설
금융	• 은행 및 투자매매업, 투자중개업을 운영에 필요한 시설 또는 체계
보건의료	• 응급의료서비스를 제공하는 시설과 이를 지원하는 혈액관리 업무를 담다하는 시설
원자력	• 원자력시설의 안정적 운영에 필요한 주제어장치가 집중된 시설과 방사성폐기물을 영구 처분하기 위한 시설
환경	• 폐기물관리법에 따른 생활폐기물 처리를 위한 수집부터 소각, 매립까지의 계통상의 시설

식용수	• 식용수 공급을 위한 담수부터 정수까지 계통상의 시설
정부 중요시설	• 중앙행정기관이 입주하고 있는 주요 시설

3) 분야별 국가기반시설 보호 체계

‘국가기반체계 보호지침’에 기술되어 있는 국가기반시설에 대해 분야별로 발생할 수 있는 재난의 유형들은 다음과 같다.

〈표 3-6〉 국가기반시설 분야별 발생 재난 유형

분야	재난 유형
에너지	• 에너지 생산, 저장, 공급시설장애 • 운영중단, 수급차질 등
정보통신	• 정보통신시스템 장애 • 정보통신시스템 운영중단 등
교통수송	• 교통, 수송시설 기술적장애 • 설비, 통제시스템 기술적 장애 • 교통, 수송의 운영중단
금융	• 금융전산망, 증권거래시스템 마비 • 종사자의 파업으로 인한 기능 마비
보건의료	• 의료정보시스템 마비 • 보건, 의료 종사자의 의료서비스 중단
원자력	• 원자력시설 및 설비의 기술적 장애 • 기술적 장애로 인한 운영중단
환경	• 생활폐기물 처리시설의 장애 및 운영중단

식용수	• 상수원 및 상수도 계통상의 시설 및 설비로 인한 운영중단 • 수질오염
정부 중요시설	• 테러, 정전, 시설붕괴 등으로 인한 업무중단 등

‘재난관리주관기관별 담당 재난 및 사고 유형’과 ‘국가기반시설 분야별 발생 재난 유형’을 종합적으로 검토하여 분야별 국가기반시설에 발생되는 재난에 대한 책무를 갖게 될 재난관리주관기관을 도출시켜보면 <표 3-7>과 같다. 해당 표에는 각 분야별 국가기반시설 보호 체계와 관련되어 영향을 끼칠 수 있는 관련 법률들을 함께 검토하여 정리하였다.

<표 3-7> 국가기반시설 관련 기관과 법률

분야	재난관리주관기관	관련 법률
에너지	산업통상자원부	• 도시가스사업법 • 집단에너지사업법 • 신에너지 및 재생에너지 개발・이용・촉진・보급 촉진법
정보통신	미래창조과학부 방송통신위원회	• 전기통신기본법 • 전원개발촉진법 • 정보통신망 이용촉진 및 정보보호 등에 관한 법률 • 국가정보화기본법
교통수송	국토교통부 해양수산부	• 항공법 • 항공안전기술원법 • 군용항공기 비행안전성 인증에 관한 법률 • 항공보안법 • 항공우주산업개발 촉진법 • 안공운송사업 진흥법 • 항공・철도사고조사에 관한 법률 • 도시철도법 • 철도건설법 • 철도사업법 • 한국철도공사법

		• 도시철도시설 안전기준에 관한 규칙 • 철도안전법 • 철도산업발전기본법 • 도로법
금융	금융위원회 기획재정부	• 한국은행법 • 한국산업은행법 • 한국수출입은행법 • 민법 • 상법
보건의료	보건복지부	• 공공보건의료에 관한 법률
원자력	원자력안전위원회	• 원자력 안전법 • 한국원자력안전기술원법 • 원자력시설 등의 방호 및 방사능 방재 대책법 • 원자력안전위원회 설치 및 운영에 관한 법률 • 원자력손해배상법 • 생활주변방사선 안전관리법 • 원자력 진흥법
환경	환경부 산림청	• 폐기물관리법 • 도시공원 미 녹지 등에 관한 법률 • 수질 및 수생태계 보전에 관한 법률 • 가축분뇨의 관리 및 이용에 관한 법률 • 자원의 절약과 재활용촉진에 관한 법률
식용수	국토교통부 환경부	• 댐건설 및 주변지역지원 등에 관한 법률 • 수도법 • 하수도법 • 하천법 • 어촌어항법
정부 중요시설	국민안전처 행정자치부	• 국민보호와 공공안전을 위한 테러 방지법 • 초고층 및 지하연계 복합건축물 재난관리에 관한 특별법 • 건설산업기본법

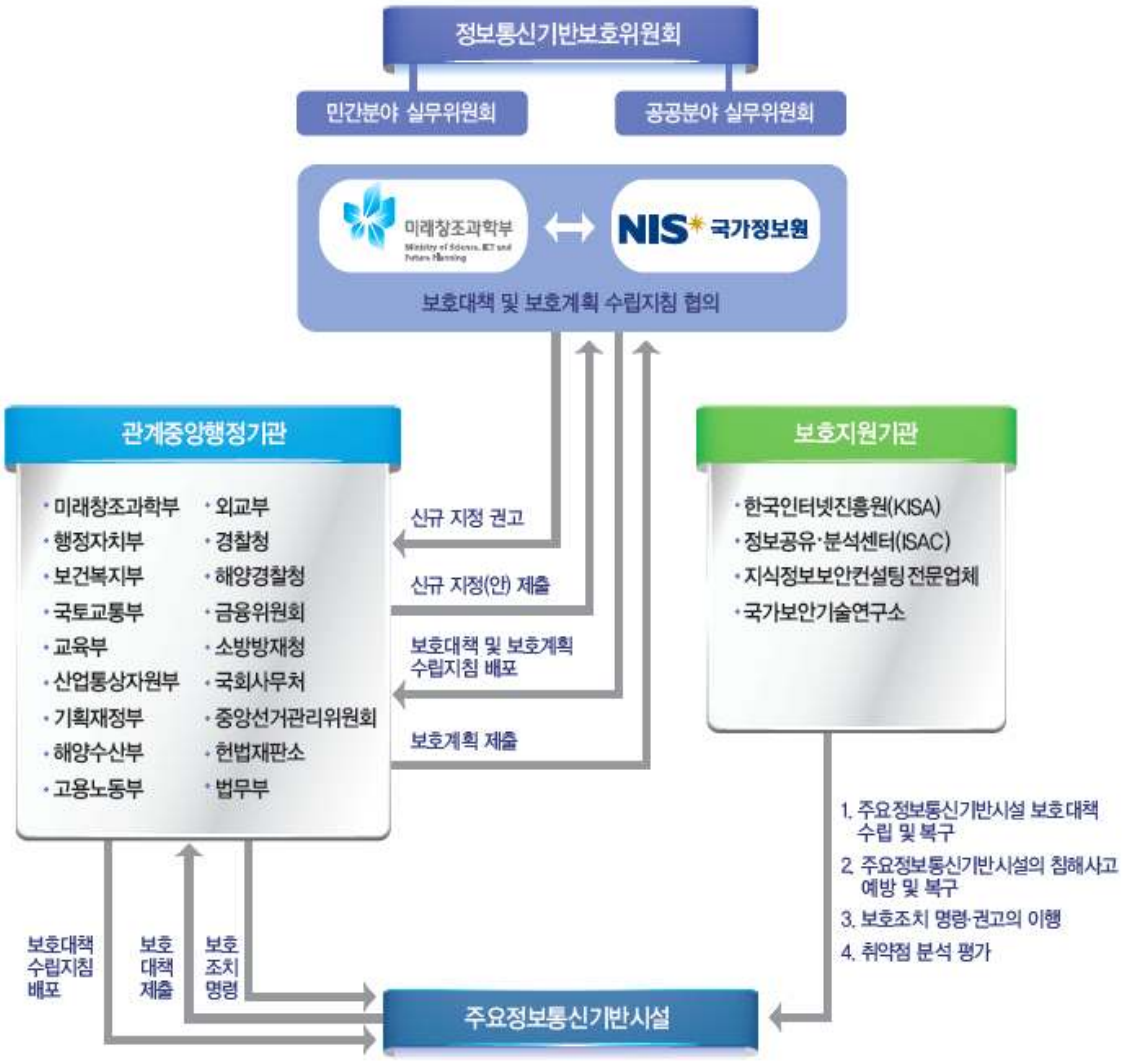
4. 주요정보통신기반시설 보호 체계

1) 정보통신 기반보호 체계 개관

정보화가 빠른 속도로 진전되면서 방송·통신, 금융, 의료 등 주요 국가기반시설들의 정보통신기술 및 서비스에 대한 의존도가 심화되고 있다. 이에 따라 소프트웨어의 기능 오류나 전자적 침해행위 등으로 인한 재난 및 사고가 발생할 가능성이 증가하였고, 국가주요시설에 일어날 수 있는 큰 피해에 대비한 체계적인 정보통신 기반보호 체계가 필요하게 되었다.

[그림 3-2] 주요정보통신기반보호 추진체계

(출처 : 한국인터넷진흥원, 정보통신기반보호 가이드라인, 2016)



이에 대한 국가 차원의 대책으로, 정부는 2001년 국가적으로 중요한 정보통신기반시설을 보호하기 위해 『정보통신기반보호법』을 제정하였고, 해당 법에서 규정하는 보호 체계에 따라 주요정보통신기반시설의 안정적인 관리 및 운영이 이루어지도록 하고 있다.

정보통신 기반보호 추진 체계 내에서 정보통신기반보호위원회는 정보통신기반 보호 정책 수립과 시행을 총괄·조정함으로써 관계중앙행정기관 간 침해사고 예방 및 대응 업무가 상호 협력 및 보완될 수 있도록 하고 있다. 또한 정보통신기반보호위원회를 효율적으로 운영하고 지원하기 위해 '정보통신기반보호 실무위원회'를 두어, 정보통신기반보호위원회에 제출된 안건과 정보통신기반보호위원회로부터 지시받은 사항을 검토·심의하게 하는 등 정보통신기반보호위원회의 효율적인 운영을 돕고 있으며, 이와 독립적으로 관계 중앙행정기관은 주요정보통신기반시설을 지정하고, 관리기관이 제출한 주요정보통신 기반시설 보호대책을 검토한 후 보호계획을 수립·시행하는 역할을 하고 있다.

주요정보통신기반시설에 대한 일차적인 보호책임이 있는 관리기관은 침해사고를 예방하고 대응하기 위해 해당 시설에 대한 취약점 분석·평가를 수행하고 보호대책을 마련하는 등의 업무를 수행하고 있다. 주요정보통신기반시설을 보호하기 위한 실제 지원기관으로는 한국인터넷진흥원, 국가보안기술연구소, 정보공유·분석센터, 정보보호 전문서비스 기업이 있으며, 해당 지원기관들은 주요정보통신기반시설 보호대책의 수립 및 침해사고 예방·복구 등에 대한 기술적 지원을 수행한다.

2) 주요정보통신기반시설의 지정

『정보통신기반보호법』제2조 1항에 따라 '정보통신기반시설'이란 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리 시스템 및『정보통신망 이용촉진 및 정보보호 등에 관한 법률』제2조1항 제1호의 규정에 의한 정보통신망을 말한다.

주요정보통신기반시설은 『정보통신기반보호법』제8조(주요정보통신기반시설의 지정 등)을 통해 지정하고 있다.

『정보통신기반보호법』

제8조(주요정보통신기반시설의 지정 등)

중앙행정기관의 장은 소관분야의 정보통신기반시설중 다음 각호의 사항을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다.

1. 당해 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가 사회적 중요성
2. 제1호의 규정에 의한 기관이 수행하는 업무의 정보통신기반시설에 대한 의존도
3. 다른 정보통신기반시설과의 상호연계성
4. 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해 규모 및 범위
5 . 침해사고의 발생가능성 또는 그 복구의 용이성

즉, 정리하자면 정보통신기반시설은 기능장애나 시설파괴 등으로 인하여 국민의 기본생활과 경제안정에 중대한 영향을 미치게 되는 시설을 말하며, 이는『정보통신기반보호법』제2조 제2항에 규정된 '전자적 침해행위'의 대상이라고 볼 수 있는 것이다.

또한 동법 제8조에 규정된 지정요건을 종합하여 보면 전자적 침해행위인 침입·교한·마비·파괴의 대상은 물리적 시설과 아울러, 정보를 수집·가옥·저장·검색·송신 또는 수신하는 정보통신체제의 기능상 장애를 야기하는 정도와 그 파급효과를 고려하여 정하도록 되어있다.

3) 분야별 주요정보통신기반시설 보호 체계

정부는 『정보통신기반보호법』에 따라 국가안보 및 경제사회에 미치는 영향 등을 고려하여 각 부처 소관의 중요 시스템에 대해 주요정보통신기반시설로 지정(2016.1, 385개)하여 관리하고 있다.

<표 3-8> 주요정보통신기반시설 지정분야

분 야	해당 시설
행 정	국가정보서비스망, 지자체 인터넷 및 업무시스템 등
금 융	은행 인터넷뱅킹시스템, 증권사사이버트레이딩시스템 등
통 신	인터넷접속망, VoIP, IPTV 서비스 등
에너지	발전제어감시시스템, 송변전SCADA 시스템 등
상수도	상수도 정수 제어시스템 등
의 료	건강보험관리시스템, 병원정보시스템 등
교 통	운항정보관리시스템, 철도운영 종합관제시스템 등
기 타	선거정보통신시스템, 국민연금관리시스템 등

제2절 안전관리 관점의 법률 분류 기준 수립

1. 국가재난 안전관리 활동의 단계별 정의

안전관리 관점에서 기반시설 보호 법제도를 분석하기 위해서는 안전관리의 관점을 대변할 수 있는 법률 분류 체계 및 기준이 필요할 것이다. 이를 위해 국가기반체계 내에서 안전관리에 대해 어떤 관점과 정의를 가지고 있는지 알아볼 필요가 있으며, 해당 내용과 관련 연구를 기반으로 하여 안전관리 관점의 법 분석 기준을 수립하고자 한다.

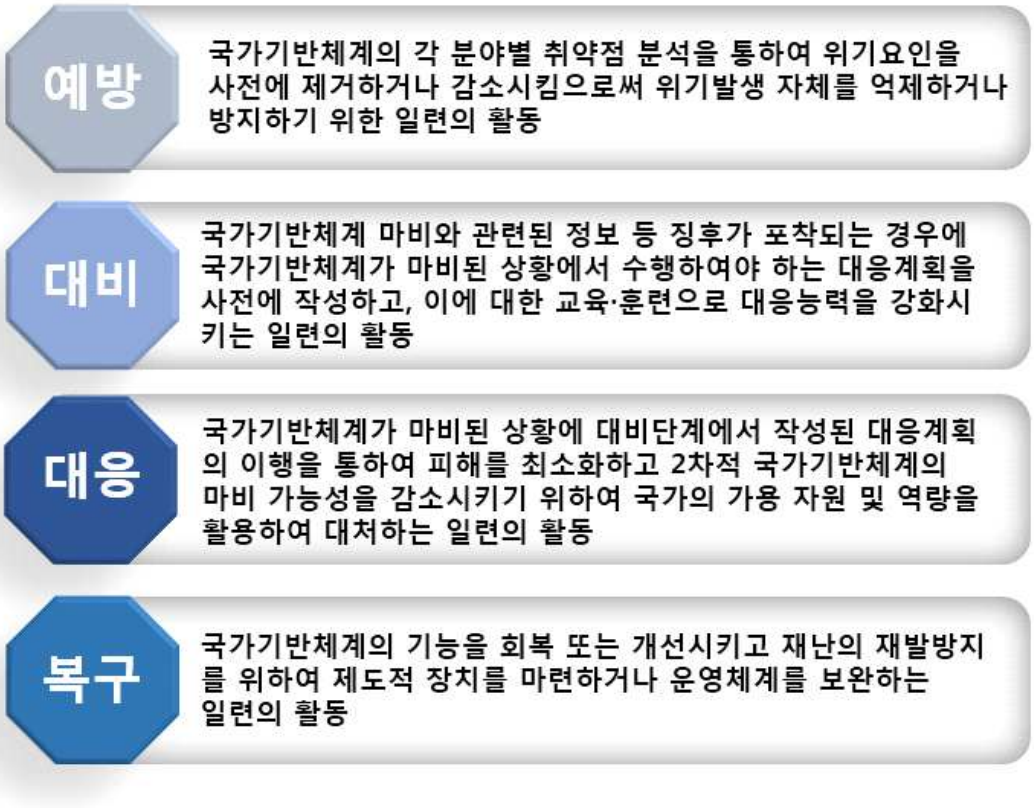
『재난 및 안전관리 기본법』제3조에서는 '재난관리'와 '안전관리'에 대한 용어의 뜻을 명확하게 정의하고 있다.

- 재난관리 : 재난의 예방·대비·대응·복구를 위해 행하는 모든 활동
- 안전관리 : 재난이나 그 밖의 각종 사고로부터 사람의 생명·신체 및 재산의 안전을 확보하기 위하여 하는 모든 활동

이를 통해 알 수 있듯이, 국가기반체계에 대한 재난관리 및 안전관리 활동은 국민의 생명·신체 및 재산의 안전에 대한 핵심적인 보호 활동인 국가기반체계보호활동으로 대변할 수 있을 것이며, 국가기반체계보호활동은 국가기반체계에 마비를 초래하는 상황을 사전에 대비하고 보호해야 하는 활동으로 기본법에 의한 재난관리 및 안전관리 활동이 총합된 종합적인 사전대비체제에 의한 활동체계라고 할 수 있을 것이다.

안전관리 관점의 국가재난관리 활동을 단계별로 나누어 분석해보기 위하여 (예방-대비-대응-복구)의 4단계로 구성된 활동 체계별 세부 정의를 자세히 살펴보고자 한다. 『재난 및 안전관리 기본법』 제14조 및 동법 시행령 제15조 내지 제17조의 규정에 의해 국가기반체계보호관련 중앙재난안전대책본부의 운영 및 상황관리에 필요한 사항을 규정하기 위해 제정된 '국가기반체계 보호관련 중앙재난안전대책본부 운영 및 상황관리 규정'에서 정의하고 있는 국가재난관리의 4단계 활동의 정의는 다음과 같다.

[그림 3-3] 국가재난안전관리 활동의 정의



2. 안전관리 활동의 단계별 내용

- 예방 단계(Mitigation)

재난 예방은 잠재적 또는 가상적 위험을 예측하고 이를 사전에 방지하기 위한 노력을 기울이는 단계로 재난이 실제로 발생하기 전에 그 발생을 예방하거나 또는 사전 조치를 취함으로써 피해규모를 최소화시키는 과정이라고 볼 수 있다[9]. 예방 단계는 각종 재난으로부터 발생하는 사회적, 경제적 피해를 감소시키려는 단계로, 직면하게 될 재난을 극복할 수 있는 국가적 능력의 향상에 초점을 두어야 하며[10], 체계적인 예방을 위해서는 재난의 발생 가능성과 피해를 줄이려는 노력이 주가 되며 장기적인 전략을 사용해야 할 필요성이 있다[11]. 이를 위해서는 사회적 대비능력을 향상시켜 손실과 재해의 충격을 완화하기 위한 대책과 사회 인프라의 물리적 강화 및 효율적

9) 나채준, 재난환경 변화에 따른 과학적 재해관리체계 강화를 위한 법제연구, 한국법제연구원, 2012
10) Godschalk, David R. & Brower, David J, Mitigation Strategies and Integrated Emergency Management. Public Administrative Review, 1985, pp. 60-73.
11) Petak. W, Emergency Management: A Challenge for Public Administration. Public Administration Review, 1985

투자를 포함하는 정부의 책무성이 요구된다.

장기적인 관점에서 실효성 있는 예방 활동이 되기 위해서는 국가핵심기반시설이나 서비스 등을 규정하거나 유형화하고 위기 발생 시 기반 시설과 서비스 등을 보호하기 위한 대응 기준과 운영방향을 설정하여야 한다. 또한 국가기반체계에 위기적인 상황이 발생할 경우 협력 유관기관의 설정 및 조정, 홍보 전략 및 정책 지원 방안 등을 수립하여야 하며[12], 국내외적으로 발생하는 위기 현상을 분석하고 대응 사례를 철저하게 분석함으로써 국내에서 발생할 경우 순차적으로 대응할 수 있는 매뉴얼을 개발하거나, 법적·제도적 장치를 마련함으로써 안정적인 국가기관체계 보호를 수행할 수 있도록 정책 집행을 수행해야 할 것이다[13].

- 대비 단계(Preparedness)

재난의 대비단계는 위기발생시의 대응활동을 사전에 준비하기 위한 대응 능력을 개발하고 신속한 준비태세를 확립시키는 단계를 말한다. 대비단계에서는 재난 발생 시 수행해야 할 사항들을 사전에 계획하고 준비함으로서 위기 대응 능력을 향상시키고, 재난 발생의 경우 즉각적으로 대응할 수 있도록 하여야 한다.

이를 위해서는 재난관리능력의 향상, 재난관리 전문 인력 양성, 재난유형별 대응 매뉴얼 확립과 이에 대한 교육 및 훈련, 재난발생 가능성이 높은 분야에 대한 집중적인 관리 등이 필요하다[14]. 재해 위험요소평가, 계획, 조직, 정보전달 및 경보 체계, 자원, 대응조직 및 구조 확보, 공공교육 및 훈련, 연습 등이 포괄적인 대비 단계에 포함된다고 볼 수 있을 것이다.

재난 대비는 수동적인 대비와 능동적인 대비로 구분할 수 있으며, 수동적인 대비는 재난발생 시 행동지침 작성, 구호품의 준비, 동원인력 및 장비 목록의 작성 등이고, 능동적인 대비는 대비계획의 작성, 재해위험 감시활동, 대응요원과 지역주민의 훈련 등이 해당될 수 있다[15].

- 대응 단계(Response)

대응 단계는 재난이 진행되는 단계에서 즉응적인 적실성(relevancy)이 가장 강조되는

12) 전라북도 국가기반체계 혁신방안, 전북발전연구원, 2005
13) Godschalk & Brower, 앞 책, pp. 60-73.
14) 나채준, 앞 책, p. 25
15) 효율적인 국가기반체계 보호를 위한 연구, 행정안전부, 2008, p. 211

단계로[16], 재난이 발생하였을 경우 인명을 구조하고 재산을 보호하는 활동을 말한다. 대응 단계에서는 예방, 대비활동과 연계하여 재난으로 인한 제2차 피해의 발생을 줄이고 복구단계에서 발생할 수 있는 문제들을 미리 최소화하는 활동들이 요구된다.

구체적 활동으로는 피해자 보호 및 구조조치, 피해상황파악 및 응급복구, 응급치료, 피해자 수용시설의 확보 및 관리, 재산보호, 보안 및 치안유지, 응급복구계획 등이 포함될 수 있을 것이다[17].

- 복구 단계(Recovery)

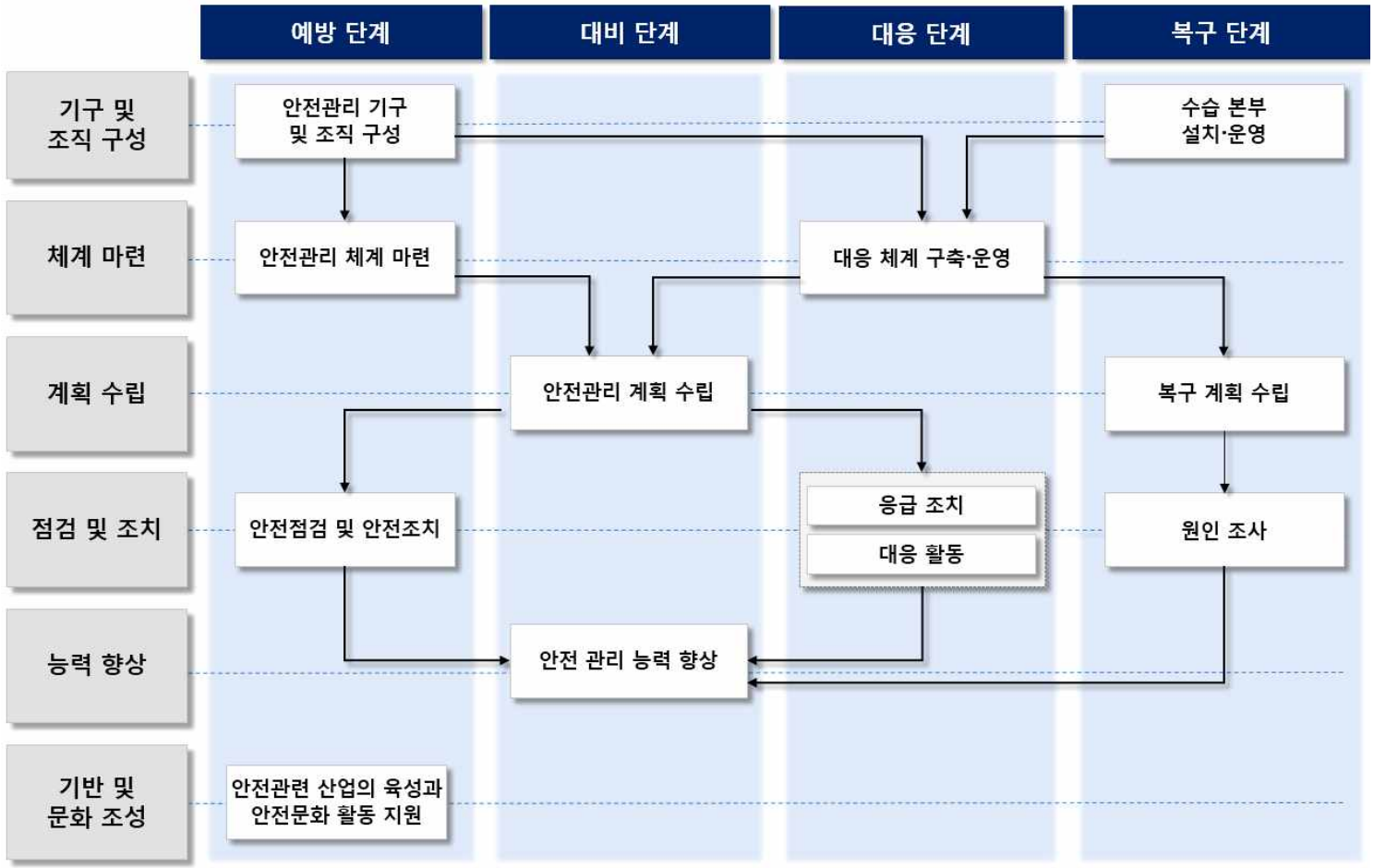
재해관리 단계의 마지막으로 피해지역이 재난발생 직후부터 재난발생 이전단계로 회복될 때까지의 장기적인 활동 단계를 말한다. 해당 단계는 재난 발생으로 인한 피해를 재난발생 이전 수준으로 복구시키고, 재난관리제도개선 및 체계개선을 통해 재난의 재발을 방지하는 일련의 활동을 포함한다.

복구 단계는 일반적으로 피해를 입은 피해지의 시설물 복구 작업, 사회기반시설의 복원, 피해보상은 물론 중장기 복구계획의 수립과 복구장비 및 복구예산의 확보, 피해상황의 집계, 재난발생의 원인 및 문제점 조사, 개선안 마련 및 재발방지책의 마련 등이 포함될 수 있을 것이다[18].

16) 행정안전부, 앞 책, p. 211
17) 나채준, 앞 책, p. 26
18) 나채준, 앞 책, p. 26

3. 안전관리 관점의 법률 분류 기준 도출

[그림 3-4] 안전관리 관점의 세부 분류 단계별 활동 흐름도



안전관리 활동의 단계별 내용을 기반으로 재난관련 법률 및 안전관련 법률들을 취합 및 검토하여 각 단계별로 공통적으로 들어갈 수 있는 활동들에 대해 대분류 및 소분류로 나누어 정리하여 보았다. 단계별 조치들이 갖는 공통적인 요인들을 크게 분류해보면 기구 및 조직 구성, 체계 마련, 계획 수립, 점검 및 조치, 능력 향상, 기반 및 문화 조성으로 나눌 수 있었다. 각 단계별 세부 조치 활동의 소분류는 위 흐름도와 같으며, 아래는 각 활동을 구분할 수 있는 기준에 대해 기술하였다.

1) 예방 단계

- 안전관리 기구 및 조직 구성

각종 관리위원회, 조정위원회, 협력위원회, 보호위원회 등의 기구를 구성하고 관련된 기능을 수행하는 조직을 구성하도록 규정하는 조치들이 포함된다.

- 안전관리 체계 마련

각종 본부, 상황실, 자문단, 대응단 등 안전관리를 실질적으로 수행할 수 있는 체계를 구성하고 관련 임무를 부여하는 조치들이 포함된다.

- 안전점검 및 안전조치

안전관리와 관련된 계획, 집행계획에 적합하게 실제적으로 안전관리가 수행되고 있는지를 확인하는 각종 안전점검 및 안전조치에 해당하는 내용들이 포함된다.

- 안전관련 산업의 육성과 안전문화 활동 지원

안전과 관련한 산업을 육성하여 안전이 유지되고 관리될 수 있는 기반을 조성하도록 하는 조치들과, 국민들의 안전에 대한 인식이 함양될 수 있도록 하는 안전문화 활동 지원 정책들이 포함된다.

2) 대비 단계

- 안전관리 계획 수립

중앙정부 및 지방정부가 수립하는 안전관리와 관련된 기본계획, 집행계획을 포함하며, 재난관리기준, 안전기준 등 안전을 점검할 때 필요한 기준에 대한 내용이 포함된다.

- 안전관리 능력 향상

안전관리와 관련된 매뉴얼 작성이나 안전을 위한 교육·훈련이 포함되며, 장기적인 관점에서의 안전관리 능력 향상 정책인 관련 인력 양성 정책들도 포함된다.

3) 대응 단계

- 대응 체계 구축·운영

재난이나 사고가 일어난 직후, 국가가 이를 대응할 수 있는 체계를 구축하고 운영하는 조치들과 관련된 내용이 포함된다.

- 응급조치

국민의 생명이나 건강이 위험할 수 있는 상황이 발생할 때 가장 우선적으로 긴급하게 대응하여야하는 사항들에 대한 조치가 포함된다.

- 대응 활동

상황 보고, 기록 관리, 통지 등 재난이나 사고에 대응하여 필수적으로 취하여야하는 사항들에 대한 조치가 포함된다.

4) 복구 단계

- 수습 본부 설치·운영

재난이나 사고를 수습하기 위해 상황을 효율적으로 관리하고 수습하기 위한 본부 설치에 관한 내용이 포함된다.

- 복구 계획 수립

재난이나 사고를 복구하기 위하여 수습 본부 등이 수립·시행하여야 하는 계획에 대한 내용이 포함된다.

- 원인 조사

재난이나 사고가 일어난 원인을 분석하고 추후 발생할 여지를 줄이기 위한 내용을 포함하며, 전체 대응 과정에 대한 재분석 수행에 대한 조치들도 포함될 수 있다.

제3절 재난 및 안전관리 기본법 분석

1. 제정 배경 및 의의

크고 작은 각종 재난이 빈번하게 발생함에 따라 개별법에 흩어져 있던 재난 관련 제도를 통합하고, 국가와 지방자치단체의 재난 대응체계 확립 등 체계적인 재난 관리를 위해 1995년 7월 18일 법률 제4950호로 『재난관리법』을 제정하여 2004년까지 운영해왔다. 그러나 참여정부 출범을 앞두고 대구지하철 방화사고가 발생함에 따라 국가적 재난 관리가 체계적이지 않다는 문제가 제기되었고, 이에 따라 2003년 3월 17일에 국가재난관리시스템기획단이 발족하여 각종 개선대책을 마련하기 시작하였다. 해당 개선 대책의 일환으로 2004년 3월 11일에 기존의 『재난관리법』을 폐지하고, 『자연재해대책법』의 일부 내용을 통합하여 최종적으로 『재난 및 안전관리 기본법』을 제정하게 된 것이다.

『재난 및 안전관리 기본법』은 각종 재난으로부터 국민의 생명·신체 및 재산을 보호하기 위하여 기존의 재연재해를 다루던『자연재해대책법』과 인적재난을 다루고 있던 『재난관리법』 등으로 다원화되어 있던 재난 관련 법령의 주요 내용을 통합하여 구성되어 있다. 『재난 및 안전관리 기본법』의 통합 제정은 국가 및 지방자치단체의 재난에 대한 대응관리체계를 확립하고, 각 부처에 분산된 안전관리 업무를 총괄·조정할 수 있도록 그 기능을 보강하는 등 재난의 예방·대비·대응·복구·긴급 구조 등에 관한 사항을 총괄적으로 규정함으로써 재난 및 안전관리에 관한 기본법의 지위를 가지게 된 데 그 의의가 있다고 볼 수 있다.

2. 주요 내용

『재난 및 안전관리 기본법』은 각종 재난으로부터 국토를 보존하고 국민의 생명·신체 및 재산을 보호하기 위하여 국가와 지방자치단체의 재난 및 안전관리체제를 확립하고, 재난의 예방·대비·대응·복구와 안전 문화활동, 그밖에 재난 및 안전관리에 필요한 사항을 규정함을 목적으로 한다[19]. 또한 동법은 재난을 예방하고 재난이 발생한 경우 그 피해를 최소화하는 것이 국가와 지방자치단체의 기본적 의무임을 확인하고, 모든 국민과 국가·지방자치단체가 국민의 생명 및 신체의 안전과 재산보호에 관련된 행위를 할 때에는 안전을 우선적으로 고려함으로써 국민이 재난으로부터

19) 재난 및 안전관리 기본법 제1조 참조

안전한 사회에서 생활할 수 있도록 함을 기본이념으로 하고 있다[20].

국무총리를 위원장으로 하는 중앙안전관리위원회(이하 "중앙위원회"라 한다)를 통하여 안전관리에 관한 중요 정책과 국가안전관리기본계획을 논의하도록 하였으며, 중앙위원회는 부처 간 협의·조정 등의 역할을 부여하였다[21]. 중앙위원회는 중앙위원회에 상정될 안건을 사전에 검토하고 부처 간 협의·조정 사항 중 경미한 사항의 협의·조정 등을 책임질 수 있도록 중앙위원회에 안전정책조정위원회(이하 "조정위원회"라 한다)를 두도록 한다[22]. 중앙위원회의 가장 큰 기능은 국가안전관리계획 및 집행계획을 심의하는 것으로, 국무총리가 대통령령으로 정하는 바에 따라 국가의 재난 및 안전관리업무에 관한 기본계획(이하 "국가안전관리기본계획"이라 한다)의 수립지침을 작성하여 관계 중앙행정기관의 장에게 시달하여야 한다[23]. 이와 별개로 관계 중앙행정기관의 장은 국가안전관리기본계획에 따라 그 소관 업무에 관한 집행계획을 작성하여 조정위원회의 심의를 거쳐 국무총리의 승인을 받아 확정하고, 재난관리책임기관의 장에게 시달하여야 한다[24]. 국민안전처장관은 해당 국가안전관리계획과 그 집행계획에 따라 시·도의 재난 및 안전관리업무에 관한 계획(이하 "시·도안전관리계획"이라 한다)의 수립지침을 작성하여 이를 시·도지사에게 시달하도록 규정되어 있다[25]. 시·도지사는 이에 따라 확정된 시·도안전관리계획에 따라 시·군·구의 재난 및 안전관리업무에 관한 계획(이하 "시·군·구안전관리계획"이라 한다)의 수립지침을 작성하여 시장·군수·구청장에게 시달하여야 한다[26].

또한 동법은 대규모 재난의 대응·복구(이하 "수습"이라 한다) 등에 관한 사항을 총괄·조정하고 필요한 조치를 하기 위하여 국민안전처에는 중앙재난안전대책본부(이하 "중앙대책본부"라 한다)를 두며, 중앙대책본부의 본부장(이하 "중앙대책본부장"이라 한다)은 국민안전처장관으로 지정하도록 규정하고 있다. 중앙대책본부장은 대규모재난이 발생하거나 발생할 우려가 있는 경우에 대통령령으로 정하는 바에 따라 실무반을 편성하고, 중앙재난안전대책본부상황실을 설치하는 등 해당 대규모재난에 대하여 효율적으로 대응하기 위한 체계를 갖추어야 할 책임을 가진다[27]. 관계 중앙행정기관의 장은 소관 분야의 기반시설 중 국가기반체계를 보호하기 위하여 계속적으

20) 동법 제2조 참조
21) 동법 제9조 참조
22) 동법 제10조 참조
23) 동법 제22조 참조
24) 동법 제23조 참조
25) 동법 제24조 참조
26) 동법 제25조 참조
27) 동법 제14조 참조

로 관리할 필요가 있다고 인정되는 시설(이하 “국가기반시설”이라 한다)을 조정위원회의 심의를 거쳐 지정하여야 하고[28], 중앙행정기관의 장 또는 지방자치단체의 장은 재난이 발생할 위험이 높거나 재난예방을 위하여 계속적으로 관리할 필요가 있다고 인정되는 시설 및 지역을 특정 관리대상 시설 및 지역(이하 “특정관리대상시설등”이라 한다)으로 지정하도록 규정되어 있다[29].

3. 안전관리 관점의 법률 분류

1) 예방 단계

- 안전관리 기구 및 조직 구성

(제4조) 재난 및 안전관리 업무의 총괄·조정

국민안전처장관은 국가 및 지방자치단체가 행하는 재난 및 안전관리 업무를 총괄·조정한다.

(제9조) 중앙안전관리위원회

재난 및 안전관리에 관해 재난 및 안전관리에 관한 중요 정책에 관한 사항, 국가안전관리기본계획에 관한 사항 등을 심의하기 위하여 국무총리 소속으로 중앙안전관리위원회를 둔다.

(제10조) 안전정책조정위원회

중앙위원회에 상정될 안건을 사전에 검토하고 다음 각 호의 사무를 수행하기 위하여 중앙위원회에 안전정책조정위원회를 둔다.

(제11조) 지역위원회

지역별 재난 및 안전관리에 관한 다음 각 호의 사항을 심의·조정하기 위하여 특별시장·광역시장·특별자치시장·도지사·특별자치도지사 소속으로 시·도 안전관리위원회를 두고, 시장·군수·구청장 소속으로 시·군·구 안전관리위원회를 둔다.

---

28) 동법 제26조 참조
29) 동법 제27조 참조

(제12조의2) 안전관리민관협력위원회

조정위원회의 위원장은 재난 및 안전관리에 관한 민관 협력관계를 원활히 하기 위하여 중앙안전관리민관협력위원회를 구성·운영할 수 있다.

(제12조의3) 중앙민관협력위원회의 기능 등

중앙민관협력위원회는 재난 및 안전관리 민관협력활동에 관한 협의, 재난 및 안전관리 민관협력활동사업의 효율적 운영방안의 협의, 평상시 재난 및 안전관리 위험요소 및 취약시설의 모니터링·제보, 재난 발생 시 인적·물적 자원 동원, 인명구조·피해복구 활동 참여, 피해주민 지원서비스 제공 등에 관한 협의의 기능을 가진다.

- 안전관리 체계 마련

(제14조) 중앙재난안전대책본부 등

대통령령으로 정하는 대규모 재난의 대응·복구 등에 관한 사항을 총괄·조정하고 필요한 조치를 하기 위하여 국민안전처에 중앙재난안전대책본부를 둔다.

(제16조) 지역재난안전대책본부

해당 관할 구역에서 재난의 수습 등에 관한 사항을 총괄·조정하고 필요한 조치를 하기 위하여 시·도지사는 시·도재난안전대책본부를 두고, 시장·군수·구청장은 시·군·구재난안전대책본부를 둔다.

(제18조) 재난안전상황실

국민안전처장관, 시·도지사 및 시장·군수·구청장은 재난정보의 수집·전파, 상황관리, 재난발생 시 초동조치 및 지휘 등의 업무를 수행하기 위하여 다음 각 호의 구분에 따른 상시 재난안전상황실을 설치·운영하여야 한다.

(제26조) 국가기반시설의 지정 및 관리 등

관계 중앙행정기관의 장은 소관 분야의 기반시설 중 제3조제1호나목에 따른 국가기반체계를 보호하기 위하여 계속적으로 관리할 필요가 있다고 인정되는 시설(이하 “국

가기반시설“이라 한다)을 각 기준에 따라 조정위원회의 심의를 거쳐 지정할 수 있다.

(제27조) 특별관리대상시설등의 지정 및 관리 등

중앙행정기관의 장 또는 지방자치단체의 장은 재난이 발생할 위험이 높거나 재난예방을 위하여 계속적으로 관리할 필요가 있다고 인정되는 시설 및 지역을 대통령령으로 정하는 바에 따라 특정 관리대상 시설 및 지역(이하 “특정관리대상시설등“이라 한다)으로 지정하여야 한다.

(제33조의3) 재난관리 실태 공시 등

시장·군수·구청장은 전년도 재난의 발생 및 수습 현황, 재난예방조치 실적, 재난관리기금의 적립 현황, 현장조치 행동매뉴얼의 작성·운용 현황 등의 사항이 포함된 재난관리 실태를 매년 1회 이상 관할 지역 주민에게 공시하여야 한다.

(제74조의2) 재난관리정보의 공동이용

재난관리책임기관·긴급구조기관 및 긴급구조지원기관은 재난관리업무를 효율적으로 처리하기 위하여 수집·보유하고 있는 재난관리정보를 다른 재난관리책임기관·긴급구조기관 및 긴급구조지원기관과 공동 이용하여야 한다.

(제75조) 안전관리자문단의 구성 운영

지방자치단체의 장은 재난 및 안전관리업무의 기술적 자문을 위하여 민간전문가로 구성된 안전관리자문단을 구성·운영할 수 있다.

(제76조의2) 안전책임관

국가기관과 지방자치단체의 장은 해당 기관의 재난 및 안전관리업무를 총괄하는 안전책임관 및 담당직원을 소속 공무원 중에서 임명할 수 있다.

(동법 시행령 제12조의5) 재난긴급대응단의 구성 및 임무 등

법 제12조의3제3항에 따른 재난긴급대응단은 중앙민관협력위원회에 참여하는 유관기관, 단체·협회 또는 기업에서 파견된 인력으로 구성한다.

- 안전점검 및 안전 조치

(제29조) 재난방지시설의 관리

재난관리책임기관의 장은 관계 법령 또는 제3장의 안전관리계획에서 정하는 바에 따라 대통령령으로 정하는 재난방지시설을 점검·관리하여야 한다.

국민안전처장관은 재난방지시설의 관리 실태를 점검하고 필요한 경우 보수·보강 등의 조치를 재난관리책임기관의 장에게 요청할 수 있다. 이 경우 요청을 받은 재난관리책임기관의 장은 신속하게 조치를 이행하여야 한다.

(제29조의2) 재난 사전 방지조치

국민안전처장관은 법 제25조의2제1항에 따라 재난 발생을 사전에 방지하기 위하여 다음 각 호의 사항이 포함된 재난발생 징후 정보를 수집·분석하여 관계 재난관리책임기관의 장에게 미리 필요한 조치를 하도록 요청할 수 있다.

(제30조) 재난예방을 위한 긴급안전점검 등

국민안전처장관 또는 재난관리책임기관의 장은 대통령령으로 정하는 시설 및 지역에 재난이 발생할 우려가 있는 등 대통령령으로 정하는 긴급한 사유가 있으면 소속 공무원으로 하여금 긴급안전점검을 하게 하고, 국민안전처장관은 다른 재난관리책임기관의 장에게 긴급안전점검을 하도록 요구할 수 있다. 이 경우 요구를 받은 재난관리책임기관의 장은 특별한 사유가 없으면 요구에 따라야 한다.

(제31조) 재난예방을 위한 안전조치

국민안전처장관 또는 재난관리책임기관의 장은 제27조제3항에 따른 안전점검 결과 또는 제30조에 따른 긴급안전점검 결과 재난 발생의 위험이 높다고 인정되는 시설 또는 지역에 대하여는 대통령령으로 정하는 바에 따라 그 소유자·관리자 또는 점유자에게 다음 각 호의 안전조치를 할 것을 명할 수 있다.

(제32조) 정부합동 안전 점검

국민안전처장관은 재난관리책임기관의 재난 및 안전관리 실태를 점검하기 위하여 대통령령으로 정하는 바에 따라 정부합동안전점검단을 편성하여 안전 점검을 실시할 수 있다.

(제39조) 안전조치명령

법 제31조제1항에 따라 국민안전처장관 또는 재난관리책임기관의 장은 안전조치에 필요한 사항을 명하려는 경우에는 안전점검의 결과, 안전조치를 명하는 이유, 안전조치의 이행기간 등의 사항이 적힌 안전조치명령서를 제38조제1항에 따른 시설 및 지역의 관계인에게 통지하여야 한다.

(동법 시행령 제33조의2) 재난관리체계 등에 대한 평가 등

국민안전처장관은 대통령령으로 정하는 바에 따라 대규모재난의 발생에 대비한 단계별 예방·대응 및 복구과정, 재난에 대응할 조직의 구성 및 정비 실태, 안전관리체계 및 안전관리규정, 재난관리기금의 운용 현황 등을 정기적으로 평가할 수 있다.

(동법 시행령 제34조의2) 특정관리대상시설등의 안전등급 및 안전점검 등

재난관리책임기관의 장은 제31조제2항에 따라 지정된 특정관리대상시설등을 제32조제1항에 따른 특정관리대상시설등의 지정·관리 등에 관한 지침에서 정하는 안전등급의 평가기준에 따라 다음 각 호의 어느 하나에 해당하는 등급으로 구분하여 관리하여야 한다. (A등급: 안전도가 우수한 경우, B등급: 안전도가 양호한 경우, C등급: 안전도가 보통인 경우, D등급: 안전도가 미흡한 경우, E등급: 안전도가 불량한 경우)

(동법 시행령 제34조의3) 특정관리대상시설등에 대한 자체안전점검

자체안전점검시설의 관계인은 해당 자체안전점검시설에 대하여 「건축법」 제22조에 따른 사용승인을 받은 후 10년이 되는 날을 기준으로 2년마다 법 제27조제3항에 따른 안전점검을 실시하여야 한다.

- 안전관련 산업의 육성과 안전문화 활동 지원

(제66조의2) 안전문화 진흥을 위한 시책의 추진

중앙행정기관의 장과 지방자치단체의 장은 소관 재난 및 안전관리업무와 관련하여 국민의 안전의식을 높이고 안전문화를 진흥시키기 위한 다음 각 호의 안전문화활동을 적극 추진하여야 한다.

(제71조) 재난 및 안전관리에 필요한 과학기술의 진흥 등

정부는 재난 및 안전관리에 필요한 연구·실험·조사·기술개발 및 전문인력 양성 등 재난 및 안전관리 분야의 과학기술 진흥시책을 마련하여 추진하여야 한다.

(제71조의2) 재난 및 안전관리기술개발 종합계획의 수립 등

국민안전처장관은 제71조제1항의 재난 및 안전관리에 관한 과학기술의 진흥을 위하여 5년마다 관계 중앙행정기관의 재난 및 안전관리기술개발에 관한 계획을 종합하여 조정위원회의 심의와 「과학기술기본법」 제9조제1항에 따른 국가과학기술심의회의 심의를 거쳐 재난 및 안전관리기술개발 종합계획을 수립하여야 한다.

(제72조) 연구개발사업 성과의 사업화 지원

국민안전처장관은 연구개발사업의 성과를 사업화하는 「중소기업기본법」 제2조에 따른 중소기업이나 그 밖의 법인 또는 사업자 등에 대하여 시제품의 개발·제작 및 설비투자에 필요한 비용의 지원, 연구개발사업의 성과로 발생한 특허권 등의 설정·허락 또는 그 알선, 사업화로 생산된 재난 및 안전 관련 제품 등의 우선 구매 등의 지원을 할 수 있다. 이 경우 중소기업에 대한 지원을 우선적으로 실시할 수 있다.

2) 대비 단계

- 안전관리 계획 수립

(제22조) 국가안전관리기본계획의 수립 등

국무총리는 대통령령으로 정하는 바에 따라 국가의 재난 및 안전관리업무에 관한 기

본계획의 수립지침을 작성하여 관계 중앙행정기관의 장에게 시달하여야 한다.

(제23조) 집행계획

관계 중앙행정기관의 장은 제22조제4항에 따라 시달받은 국가안전관리기본계획에 따라 그 소관 업무에 관한 집행계획을 작성하여 조정위원회의 심의를 거쳐 국무총리의 승인을 받아 확정한다.

(제23조의2) 국가안전관리기본계획 등과의 연계

관계 중앙행정기관의 장은 소관 개별 법령에 따른 재난 및 안전과 관련된 계획을 수립하는 때에는 국가안전관리기본계획 및 제23조에 따른 집행계획과 연계하여 작성하여야 한다.

(제24조) 시·도안전관리계획의 수립

국민안전처장관은 제22조제4항에 따른 국가안전관리기본계획과 제23조제1항에 따른 집행계획에 따라 시·도의 재난 및 안전관리업무에 관한 계획의 수립지침을 작성하여 이를 시·도지사에게 시달하여야 한다.

(제25조) 시·군·구안전관리계획의 수립

시·도지사는 제24조제3항에 따라 확정된 시·도안전관리계획에 따라 시·군·구의 재난 및 안전관리업무에 관한 계획의 수립지침을 작성하여 시장·군수·구청장에게 시달하여야 한다.

(제34조의3) 국가재난관리기준의 제정 운용 등

국민안전처장관은 재난관리를 효율적으로 수행하기 위하여 다음 각 호의 사항이 포함된 국가재난관리기준을 제정하여 운용하여야 한다.

(제34조의7) 안전기준의 등록 및 심의 등

국민안전처장관은 안전기준을 체계적으로 관리·운용하기 위하여 안전기준을 통합적으로 관리할 수 있는 체계를 갖추어야 한다.

(제34조의9) 재난대비훈련 기본계획 수립

국민안전처장관은 매년 재난대비훈련 기본계획을 수립하고 재난관리책임기관의 장에게 통보하여야 한다.

- 안전관리 능력 향상

(제34조의5) 재난분야 위기관리 매뉴얼 작성 운용

재난관리책임기관의 장은 재난을 효율적으로 관리하기 위하여 재난유형에 따라 다음 각 호의 위기관리 매뉴얼을 작성·운용하여야 한다. 이 경우 재난대응활동계획과 위기관리 매뉴얼이 서로 연계되도록 하여야 한다.

(제35조) 재난대비훈련 실시

국민안전처장관, 중앙행정기관의 장, 시·도지사, 시장·군수·구청장 및 긴급구조기관의 장은 대통령령으로 정하는 바에 따라 매년 정기적으로 또는 수시로 재난관리책임기관, 긴급구조지원기관 및 군부대 등 관계 기관과 합동으로 재난대비훈련(제34조의5에 따른 위기관리 매뉴얼의 숙달훈련을 포함한다)을 실시하여야 한다.

(제55조) 재난대비능력 보강

국가와 지방자치단체는 재난관리에 필요한 인력·장비·시설의 확충, 통신망의 설치·정비 등 긴급구조능력을 보강하기 위하여 노력하고, 필요한 재정상의 조치를 마련하여야 한다.

(제66조의5) 대국민 안전교육의 실시

중앙행정기관의 장 및 지방자치단체의 장은 안전문화의 정착을 위하여 대국민 안전교육 및 학교·사회복지시설·다중이용시설 등 안전에 취약한 시설의 종사자 등에 대하여 대통령령으로 정하는 바에 따라 정기적으로 안전교육을 실시할 수 있다.

(제66조의6) 안전교육 전문인력 양성 등

국가 및 지방자치단체는 안전교육 전문인력의 양성을 위하여 안전교육 전문인력의 수급 및 활용에 관한 사항, 안전교육 전문인력의 육성 및 교육훈련에 관한 사항, 안전교육 전문인력의 경력관리와 경력인증에 관한 사항 등과 관련한 시책을 수립·추진할 수 있다.

3) 대응 단계

- 대응 체계 구축·운영

(제36조) 재난사태 선포

국민안전처장관은 대통령령으로 정하는 재난이 발생하거나 발생할 우려가 있는 경우 사람의 생명·신체 및 재산에 미치는 중대한 영향이나 피해를 줄이기 위하여 긴급한 조치가 필요하다고 인정하면 중앙위원회의 심의를 거쳐 재난사태를 선포할 수 있다.

(제38조의2) 재난 예보·경보체계 구축·운영 등

재난관리책임기관의 장은 사람의 생명·신체 및 재산에 대한 피해가 예상되면 그 피해를 예방하거나 줄이기 위하여 재난에 관한 예보 또는 경보 체계를 구축·운영할 수 있다.

- 응급조치

(제37조) 응급조치

제50조제2항에 따른 시·도긴급구조통제단 및 시·군·구긴급구조통제단의 단장과 시장·군수·구청장은 재난이 발생할 우려가 있거나 재난이 발생하였을 때에는 즉시 관계 법령이나 재난대응활동계획 및 위기관리 매뉴얼에서 정하는 바에 따라 수방(水防)·진화·구조 및 구난(救難), 그 밖에 재난 발생을 예방하거나 피해를 줄이기 위하여 필요한 응급조치를 하여야 한다

(제38조) 위기경보의 발령 등

재난관리주관기관의 장은 대통령령으로 정하는 재난에 대한 징후를 식별하거나 재난 발생이 예상되는 경우에는 그 위험 수준, 발생 가능성 등을 판단하여 그에 부합되는 조치를 할 수 있도록 위기경보를 발령할 수 있다.

- 대응 활동

(제14조의2) 수습지원단 파견 등

중앙대책본부장은 국내 또는 해외에서 발생한 대규모재난의 수습을 지원하기 위하여 관계 중앙행정기관 및 관계 기관·단체의 재난관리에 관한 전문가 등으로 수습지원단을 구성하여 현지에 파견할 수 있다.

(제20조) 재난상황의 보고

시장·군수·구청장, 소방서장, 해양경비안전서장, 제3조제5호나목에 따른 재난관리책임기관의 장 또는 제26조제1항에 따른 국가기반시설의 장은 그 관할구역, 소관 업무 또는 시설에서 재난이 발생하거나 발생할 우려가 있으면 대통령령으로 정하는 바에 따라 재난상황에 대해서는 즉시, 응급조치 및 수습현황에 대해서는 지체 없이 각각 국민안전처장관, 관계 재난관리주관기관의 장 및 시·도지사에게 보고하거나 통보하여야 한다. 이 경우 관계 재난관리주관기관의 장 및 시·도지사는 보고받은 사항을 확인·종합하여 국민안전처장관에게 통보하여야 한다.

(동법 시행령 제24조) 재난상황의 보고

법 제20조에 따른 재난상황의 보고 및 통보에는 재난 발생의 일시·장소와 재난의 원인, 재난으로 인한 피해내용, 응급조치 사항, 대응 및 복구활동 사항, 향후 조치계획 등의 사항이 포함되어야 한다.

(제70조) 재난상황의 기록 관리

재난관리책임기관의 장은 소관 시설·재산 등에 관한 피해상황을 포함한 재난상황 등을 기록하고, 이를 보관하여야 한다. 이 경우 시장·군수·구청장을 제외한 재난관리책임기관의 장은 그 기록사항을 시장·군수·구청장에게 통보하여야 한다.

4) 복구 단계

- 수습 본부 설치·운영

(제15조의2) 중앙 및 지역사고수습본부

재난관리주관기관의 장은 재난이 발생하거나 발생할 우려가 있는 경우에는 재난상황을 효율적으로 관리하고 재난을 수습하기 위한 중앙사고수습본부를 신속하게 설치·운영하여야 한다.

- 복구 계획 수립

(제59조) 재난복구계획의 수립·시행

재난관리책임기관의 장은 제58조제2항에 따른 피해조사를 마치면 지체 없이 자체복구계획을 수립·시행하여야 한다. 다만, 제58조제3항에 따라 중앙재난피해합동조사단이 편성되어 피해상황을 조사하는 경우에는 제2항에 따라 중앙대책본부장으로부터 재난피해복구계획을 통보받은 후에 수립·시행할 수 있다.

- 원인 조사

(제69조) 정부합동 재난원인조사

국민안전처장관은 재난이나 그 밖의 각종 사고의 발생 원인과 재난 발생 시 대응과정에 관한 조사·분석·평가를 효율적으로 수행하기 위하여 재난안전분야 전문가 및 전문기관 등이 공동으로 참여하는 정부합동 재난원인조사단을 편성하고, 현지에 파견하여 원인조사·분석을 실시할 수 있다.

4. 법제 분류 결과 및 시사점

<표 3-9> 안전관리 관점에서의 「재난 및 안전관리 기본법」 법제 분류 결과

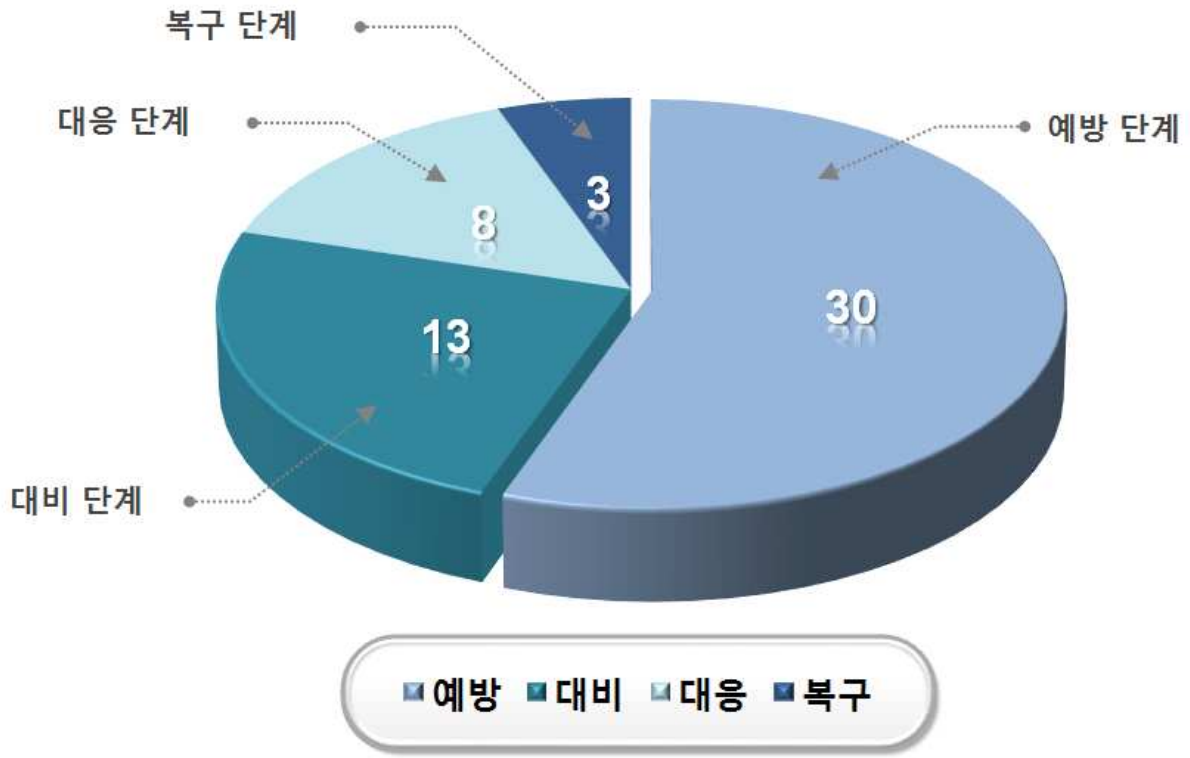
안전관리 단계	세부 활동 영역	법률 조항	내용
예방 단계	안전관리 기구 및 조직 구성	제4조	• 재난 및 안전관리 업무의 총괄조정
		제9조	• 중앙안전관리위원회
		제10조	• 안전정책조정위원회
		제11조	• 지역위원회
		제12조의2	• 안전관리민관협력위원회
		제12조의3	• 중앙민관협력위원회의 기능
	안전관리 체계 마련	제14조	• 중앙재난안전대책본부 등
		제16조	• 지역재난안전대책본부
		제18조	• 재난안전상황실
		제26조	• 국가기반시설의 지정 및 관리 등
		제27조	• 특별관리대상시설등의 지정 및 관리 등
		제33조의3	• 재난관리 실태 공시 등
		제74조의2	• 재난관리정보의 공동이용
		제75조	• 안전관리자문단의 구성 운영
		제76조의2	• 안전책임관
		시행령 제12조의5	• 재난긴급대응단의 구성 및 임무 등
	안전점검 및 안전 조치	제29조	• 재난방지시설의 관리
		제29조의2	• 재난 사전 방지조치

		제30조	• 재난예방을 위한 긴급안전점검 등
		제31조	• 재난예방을 위한 안전조치
		제32조	• 정부합동 안전 점검
		제39조	• 안전조치명령
		시행령 제33조의2	• 재난관리체계 등에 대한 평가 등
		시행령 제34조의2	• 특정관리대상시설 등의 안전등급 및 안전점검 등
		시행령 제34조의3	• 특정관리대상시설 등에 대한 자체안전점검
	안전관련 산업의 육성과 안전문화 활동 지원	제66조의2	• 안전문화 진흥을 위한 시책의 추진
		제71조	• 재난 및 안전관리에 필요한 과학기술의 진흥 등
		제71조의2	• 재난 및 안전관리기술개발 종합계획의 수립 등
		제72조	• 연구개발사업 성과의 사업화 지원
대비 단계	안전관리 계획 수립	제22조	• 국가안전관리기본계획의 수립 등
		제23조	• 집행계획
		제23조의2	• 국가안전관리기본계획 등과의 연계
		제24조	• 시도안전관리계획의 수립
		제25조	• 시· 군·구안전관리계획의 수립
		제34조의3	• 국가재난관리기준의 제정 운용 등

		제34조의7	• 안전기준의 등록 및 심의 등
		제34조의9	• 재난대비훈련 기본계획 수립
	안전관리 능력 향상	제34조의5	• 재난분야 위기관리 매뉴얼 작성 운용
		제35조	• 재난대비훈련 실시
		제55조	• 재난대비능력 보강
		제66조의5	• 대국민 안전교육의 실시
		제66조의6	• 안전교육 전문인력 양성 등
대응 단계	대응 체계 구축·운영	제36조	• 재난사태 선포
		제38조의2	• 재난 예보경보체계 구축· 운영
	응급조치	제37조	• 응급조치
		제38조	• 위기경보의 발령 등
	대응 활동	제14조의2	• 수습지원단 파견 등
		제20조	• 재난상황의 보고
		시행령 제24조	• 재난상황의 보고
		제70조	• 재난상황의 기록 관리
복구 단계	수습 본부 설치·운영	제15조의2	• 중앙 및 지역사고수습본부
	복구 계획 수립	제59조	• 재난복구계획의 수립시행
	원인 조사	제69조	• 정부합동 재난원인조사

『재난 및 안전관리 기본법』의 법률 조항들을 안전관리 관점의 분류 기준으로 분류한 결과, 예방 단계는 안전관리 기구 및 조직 구성 활동 6개 조항, 안전관리 체계 마련 활동 10개 조항, 안전점검 및 안전조치 활동 9개 조항, 안전관련 산업의 육성과 안전문화 활동 지원 4개 조항으로 가장 많은 수의 조항인 총 30개 조항에 걸쳐 규율하고 있었다. 대비 단계에서는 안전관리 계획 수립 활동 8개 조항, 안전 관리 능력 향상 활동 5개 조항으로 총 13개 조항을 통해 규율하고 있었다. 반면 대응 단계는 대응 체계 구축·운영 활동 2개 조항, 응급 조치 활동 2개 조항, 대응 활동 4개 조항인 총 8개 활동으로 예방 및 대비 단계보다는 적은 조항을 가지고 있었다. 복구 단계도 이와 마찬가지로 수습 본부 설치·운영 활동, 복구 계획 수립 활동, 원인 조사 활동 각각 1개 조항씩으로 적은 조항을 통해 규율하고 있었다. 이를 그래프로 나타내면 다음과 같다.

[그림 3-5] 「재난 및 안전관리 기본법」의 안전 관리 단계별 조항 개수 (단위:개)

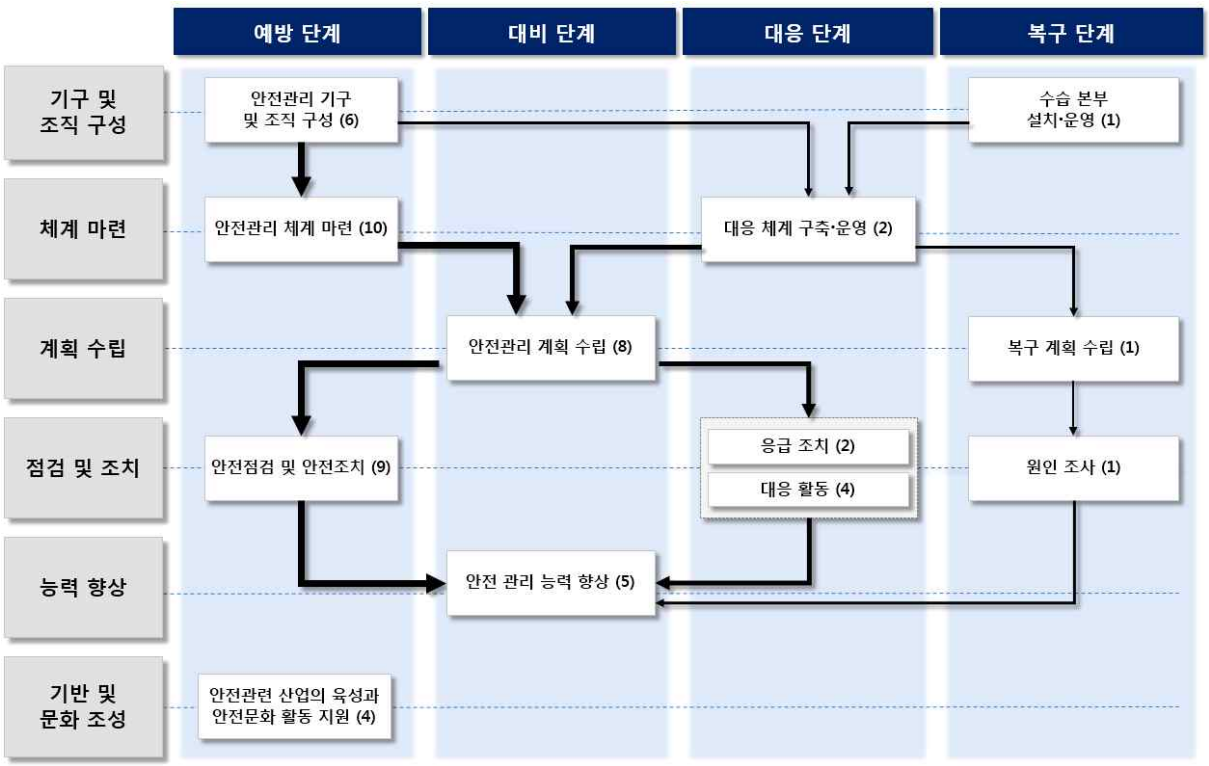


안전 관리 관련 조항 총 54개 조항 중 예방 단계의 활동이 절반을 넘는 30개 조항을 차지하는 것으로 보아 정부가 안전 관리와 관련된 기구 및 조직을 구성하고 체계를 마련하고, 안전 점검 및 조치를 하는 활동들에 상당한 노력을 하고 있다는 것을 알 수 있었다. 이에 못지않게 대비 단계에 속하는 활동인 안전 관리 계획들을 수립하는 것과

다양한 훈련 및 교육을 통한 안전 관리 능력 향상에도 많은 조항들을 두고 있다는 점을 알 수 있다. 반면 대응 단계와 복구 단계 내의 활동들은 예방 및 대응 단계에 비하면 개수는 적지만 재난 사태 선포, 대응 체계 구축, 수습 본부 설치로 이어지는 재난 대응 과정이 체계적으로 구성되어 있으며, 복구 계획 및 원인 조사에 대한 활동들도 규율되어 있어 충분한 안전 관리 체계를 취하고 있다고 볼 수 있다.

『재난 및 안전관리 기본법』의 안전관리 관점의 세부 분류 단계별 활동 흐름도를 그려보면 [그림 3-6]과 같다. 예방 단계와 대비 단계 간 활동들의 흐름이 확연히 두드러지는 것을 볼 수 있다. 동법의 법률 조항 분석 및 분류 결과를 통하여 향후 SW 안전과 관련한 법률 제정안을 구성할 시에 예방 및 대비 단계에 포함되는 조항들의 내용과 각 조항 간 유기적인 관계의 흐름들을 적극 참조할 필요가 있다. 예를 들어, SW안전 관련법을 제정할 시 소프트웨어 안전 관리 위원회를 설치하고 적합한 기능을 부여하며 관련 체계와 계획을 수립하고자 할 시에, 『재난 및 안전관리 기본법』의 안전관리 기구 및 조직 구성 활동에 포함되는 중앙안전관리위원회, 안전정책조정위원회, 지역위원회, 안전관리민관협력위원회, 중앙민관협력위원회 등의 설치 및 구성에 대한 조항들과 안전관리 체계를 마련되고 관련 계획 수립으로 이어지는 흐름들을 참조할 수 있을 것이다.

[그림 3-6] 「재난 및 안전관리 기본법」의 안전관리 관점의 세부 분류 단계별 활동 흐름도



또한 활동 흐름도에 따르면 예방 단계의 안전점검 및 안전조치 활동, 대응 단계의 응급 조치 및 대응 활동, 복구 단계의 원인 조사 활동의 결과들이 종합적으로 반영되어 대비 단계의 안전 관리 능력 향상 단계로 흘러들어가는 것을 볼 수 있다. 각 단계의 결과들을 토대로 위험들을 찾아내고 이에 대한 해결 방안들을 반영하여 위기 관리 매뉴얼 작성, 재난대비훈련, 안전 교육, 전문인력 양성 등의 안전 관리 능력이 다시금 향상되도록 하는 선순환 구조를 취하고 있는 것이다. SW 안전법 제정 시에도 이러한 사항을 참조하여 소프트웨어의 개발 단계부터 폐기 단계까지의 체계에 안전 관리의 선순환 구조를 포함시킬 필요가 있다.

제4절 정보통신기반보호법 분석

1. 제정 배경 및 의의

우리나라는 2000년도 당시 정보통신과 관련한 보호를 위해 『전기통신기본법』,『정보화촉진기본법』,『정보통신망 이용 촉진 등에 관한 법률』,『국가정보원법』,『보안업무규정』등의 법률 및 규정이 존재하였지만, 이들은 주로 물리적 측면의 시설보호를 중심으로 규정되어 있었고, 사이버 공격에 대비하여 정보통신기반시설의 취약점을 평가하고 이에 대한 범국가적 예방대책을 수립·시행할 수 있는 근거법령은 미비한 상태에 있었다. 때문에 정보통신망에 대한 침해사고가 발생할 시에 대비한 관계 기관의 유기적이고 신속한 대응체제가 마련되어 있지 않았으므로, 주요정보통신기반시설 보호를 위하여 새로운 법체계가 마련되어야 한다는 공감대가 형성되기 시작하였다.

결국 2000년 2월 25일 당시 열린 "사이버테러방지 관계장관 회의"에서 『정보통신기반보호법』을 제정하기로 결정하였고, 이에 따라 2000년 3월부터 정보통신부 산하 관계 연구기관과 10여명으로 구성된 실무연구반에서 만든 제정안을 가지고 총 6회에 걸친 회의를 운영한 결과 논의된 쟁점을 반영하여 2001년 1월 26일 『정보통신기반보호법』이 제정되었다. 동법은 2007년 개정으로 인해 주요정보통신기반시설의 지정대상이 국가 및 공공기관뿐만 아니라 민간이 운영, 관리하는 정보통신기반시설까지 포함되어 사이버침해행위 발생 시 국가안보, 국민의 기본생활 및 경제안정에 중대한 영향을 미치게 되는 국가안전보장·행정·국방·치안·방송통신·운송·에너지 등의 업무와 관련된 전자적 제어, 관리시스템과 정보통신망이 포함되게 되었다는데 의의가 있다.

2. 주요 내용

『정보통신기반보호법』은 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안전을 보장하는 것을 목적으로 한다[30].

동법에 의하면 "정보통신기반시설"이라 함은 국가안전보장·행정·국방·치안·방송통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및『정보통신망 이용촉진 및 정보보호 등에 관한 법률』제2조 제1항 제1호의 규정에 의한 정보통신망

30) 정보통신기반보호법 제1조 참조

을 말하며, “전자적 침해행위”란 정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위를 말한다[31].

동법은 주요정보통신기반시설의 보호정책의 조정, 보호계획의 종합·조정, 보호 계획의 추진 실적 관련 사항, 보호 계획의 보호와 관련된 제도의 개선에 관한 사항 등을 심의하기 위하여 국무총리 소속하에 정보통신기반보호위원회를 두도록 규정하고 있으며[32], 주요정보통신기반시설을 관리하는 기관의 장은 취약점 분석·평가의 결과에 따라 소관 주요정보통신기반시설을 안전하게 보호하기 위한 예방, 백업, 복구 등 물리적·기술적 대책을 포함한 주요정보통신기반시설보호대책을 수립·시행하도록 규정하고 있다[33]. 또한 관계중앙행정기관의 장은 제출받은 주요정보통신기반시설보호대책을 종합·조정하여 소관분야에 대한 주요정보통신기반시설에 관한 보호계획을 수립·시행하여야 하는데, 그 내용은 주요정보통신기반시설의 취약점 분석·평가, 주요정보통신기반시설의 침해사고에 대한 예방 및 복구대책 등의 사항을 포함해야 한다[34]. 중앙행정기관의 장은 소관분야의 정보통신기반시설 중 당해 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성, 기관이 수행하는 업무의 의존도 등을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다[35].

3. 안전관리 관점의 법률 분류

1) 예방 단계

- 안전관리 기구 및 조직 구성

(제3조) 정보통신기반보호위원회

주요정보통신기반시설의 보호에 관한 사항을 심의하기 위하여 국무총리 소속하에 정보통신기반보호위원회를 둔다.

(동법 시행령 제9조) 정보보호책임자의 지정 등

31) 동법 제2조 참조
32) 동법 제3조, 제4조 참조
33) 동법 제5조 참조
34) 동법 제6조 참조
35) 동법 제8조 참조

관리기관의 장은 소관 주요정보통신기반시설의 보호 업무를 담당하는 4급·4급상당 공무원, 5급·5급상당 공무원, 영관급장교 또는 임원급 관리·운영자를 정보보호책임자로 지정하여야 한다.

(동법 시행령 제11조) 정보보호책임관의 지정 등

관계중앙행정기관의 장은 주요정보통신기반시설 보호업무를 담당하는 과장급 공무원을 정보보호책임관으로 지정하여야 한다.

- 안전관리 체계 마련

(제8조) 주요정보통신기반시설의 지정 등

중앙행정기관의 장은 소관분야의 정보통신기반시설중 관리하는 기관이 수행하는 업무의 국가사회적 중요성, 기관이 수행하는 업무의 의존도 등을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다.

(제16조) 정보공유 · 분석센터

금융·통신 등 분야별 정보통신기반시설을 보호하기 위하여 취약점 및 침해요인과 그 대응방안에 관한 정보 제공, 침해사고가 발생하는 경우 실시간 경보·분석체계 운영 등의 업무를 수행하고자 하는 자는 정보공유·분석센터를 구축·운영할 수 있다.

- 안전점검 및 안전 조치

(제9조) 취약점의 분석·평가

관리기관의 장은 대통령령이 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석·평가하여야 한다.

(제10조) 보호지침

관계중앙행정기관의 장은 소관분야의 주요정보통신기반시설에 대하여 보호지침을 제정하고 해당분야의 관리기관의 장에게 이를 지키도록 권고할 수 있다.

(제11조) 보호조치 명령 등

관계중앙행정기관의 장은 제출받은 주요정보통신기반시설보호대책을 분석하여 별도의 보호조치가 필요하다고 인정하는 경우나, 통보된 주요정보통신기반시설보호대책의 이행 여부를 분석하여 별도의 보호조치가 필요하다고 인정되는 경우, 해당 관리기관의 장에게 주요정보통신기반시설의 보호에 필요한 조치를 명령 또는 권고할 수 있다.

- 안전관련 산업의 육성과 안전문화 활동 지원

(제24조) 기술개발 등

정부는 정보통신기반시설을 보호하기 위하여 필요한 기술의 개발 및 전문인력 양성에 관한 시책을 강구할 수 있다.

정부는 정보통신기반시설의 보호에 필요한 기술개발을 효율적으로 추진하기 위하여 필요한 때에는 정보보호 기술개발과 관련된 연구기관 및 민간단체로 하여금 이를 대행하게 할 수 있다. 이 경우 이에 소요되는 비용의 전부 또는 일부를 지원할 수 있다.

2) 대비 단계

- 안전관리 계획 수립

(제5조) 주요정보통신기반시설보호대책의 수립 등

주요정보통신기반시설을 관리하는 기관의 장은 취약점 분석·평가의 결과에 따라 소관 주요정보통신기반시설 및 관리 정보를 안전하게 보호하기 위한 예방, 백업, 복구 등 물리적·기술적 대책을 포함한 관리대책을 수립·시행하여야 한다.

(제6조) 주요정보통신기반시설보호계획의 수립 등

관계중앙행정기관의 장은 제5조의 규정에 의하여 제출받은 주요정보통신기반시설보호대책을 종합·조정하여 소관분야에 대한 주요정보통신기반시설에 관한 보호계획을 수립·시행하여야 한다.

(동법 시행령 제10조) 주요정보통신기반시설보호계획의 수립 등

관계중앙행정기관의 장은 전년도 주요정보통신기반시설보호계획의 추진실적과 다음 연도의 주요정보통신기반시설보호계획을 매년 10월 31일까지 위원회에 제출하여야 한다.

3) 대응 단계

- 응급조치

(제14조) 복구조치

관리기관의 장은 소관 주요정보통신기반시설에 대한 침해사고가 발생한 때에는 해당 정보통신기반시설의 복구 및 보호에 필요한 조치를 신속히 취하여야 한다.

- 대응 활동

(제13조) 침해사고의 통지

관리기관의 장은 침해사고가 발생하여 소관 주요정보통신기반시설이 교란·마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관, 수사기관 또는 인터넷진흥원에 그 사실을 통지하여야 한다. 이 경우 관계기관등은 침해사고의 피해확산 방지와 신속한 대응을 위하여 필요한 조치를 취하여야 한다.

4) 복구 단계

- 수습 본부 설치·운영

(제15조) 대책본부의 구성 등

위원회의 위원장은 주요정보통신기반시설에 대하여 침해사고가 광범위하게 발생한 경우 그에 필요한 응급대책, 기술지원 및 피해복구 등을 수행하기 위한 기간을 정하여 위원회에 정보통신기반침해사고대책본부를 둘 수 있다.

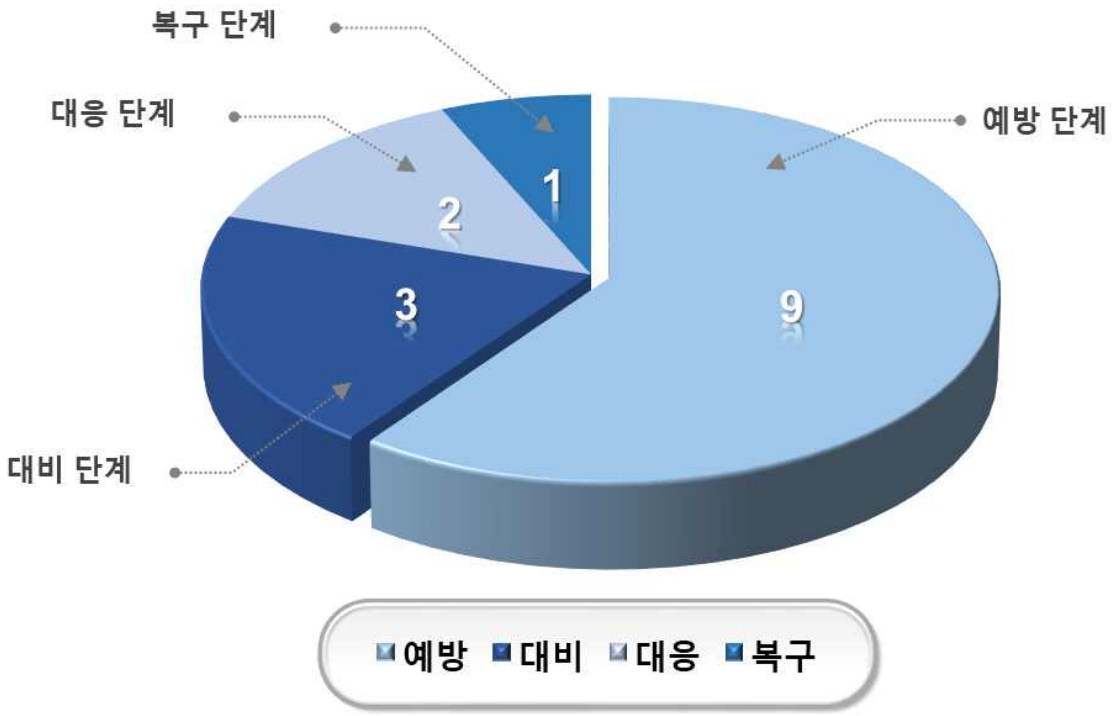
4. 법제 분류 결과 및 시사점

<표 3-10> 안전관리 관점에서의 「정보통신기반보호법」 법제 분류 결과

안전관리 단계	세부 활동 영역	「정보통신기반보호법 」 법률 조항
예방 단계	안전관리 기구 및 조직 구성	• (제3조) 정보통신기반보호위원회
		• (동법 시행령 제9조) 정보보호책임자의 지정 등
		• (동법 시행령 제11조) 정보보호책임관의 지정 등
	안전관리 체계 마련	• (제8조) 주요정보통신기반시설의 지정 등
		• (제16조) 정보공유·분석센터
	안전점검 및 안전 조치	• (제9조) 취약점의 분석·평가
		• (제10조) 보호지침
		• (제11조) 보호조치 명령 등
	안전관련 산업의 육성과 안전문화 활동 지원	• (제24조) 기술개발 등
대비 단계	안전관리 계획 수립	• (제24조) 기술개발 등
		• (제6조) 주요정보통신기반시설보호계획의 수립 등
		• (동법 시행령 제10조) 주요정보통신기반시설보호계획의 수립 등
	안전관리 능력 향상	-
대응 단계	대응 체계 구축·운영	-
	응급조치	• (제14조) 복구조치
	대응 활동	• (제13조) 침해사고의 통지
복구 단계	수습 본부 설치·운영	• (제15조) 대책본부의 구성 등
	복구 계획 수립	-
	원인 조사	-

『정보통신기반보호법』의 법률 조항들을 안전관리 관점의 분류 기준으로 분류한 결과, 예방 단계는 안전관리 기구 및 조직 구성 활동 3개 조항, 안전관리 체계 마련 활동 2개 조항, 안전점검 및 안전조치 활동 3개 조항, 안전관련 산업의 육성과 안전문화 활동 지원 1개 조항으로 가장 많은 수의 조항인 총 9개 조항에 걸쳐 규율하고 있었다. 대비 단계에서는 안전관리 계획 수립 활동과 관련된 3개 조항만 존재하였다. 대응 단계도 응급 조치 활동 1개 조항, 대응 활동 1개 조항으로 총 2개의 조항으로 구성되었으며, 복구 단계는 수습 본부 설치·운영 활동과 관련한 1개 조항으로 구성되어 있었다. 이를 그래프로 나타내면 다음과 같다.

[그림 3-7] 「정보통신기반보호법」의 안전 관리 단계별 조항 개수 (단위:개)

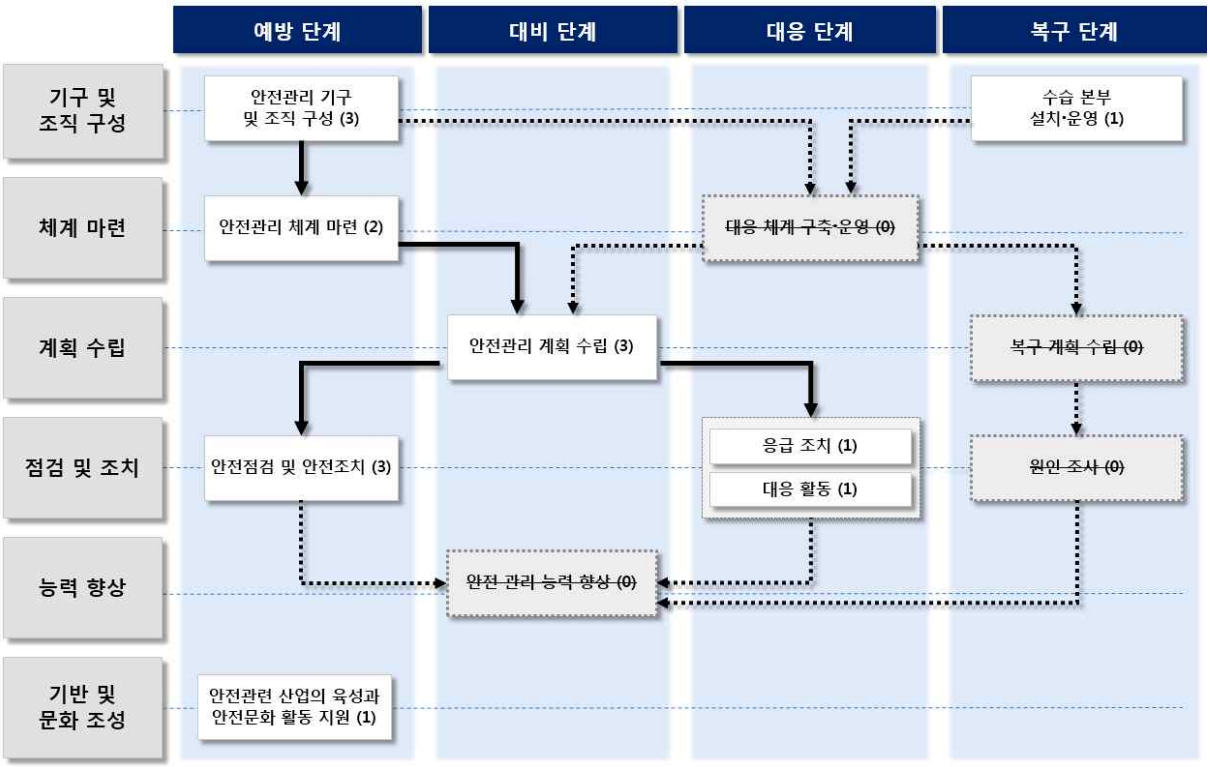


『정보통신기반보호법』도 『재난 및 안전관리 기본법』과 마찬가지로 안전 관리 관련 조항 총 15개 조항 중 예방 단계의 활동이 절반을 넘는 9개 조항을 차지하는 것으로 보아 정부의 재난 및 사고 관리 대책들이 대부분 예방 위주로 편성되어 있는 것을 알 수 있다.

동법의 세부 분류 단계별 활동 흐름도를 보면 안전 관리 능력 향상 활동, 대응 체계 구축·운영 활동, 복구 계획 수립 활동, 원인 조사 활동에 대한 조항은 빠져있음을 알 수 있다. 이는 정보통신기반시설의 안전을 규율하고 있는 대상의 특성상 법률로 규율

하기 힘든 부분이 존재하기 때문인 것으로 생각되며, 관련된 세부 사항들은 시행 규칙 및 가이드라인 수준에서 다루고 있다.

[그림 3-8] 「정보통신기반보호법」의 안전관리 관점의 세부 분류 단계별 활동 흐름도



동법은 정보통신기반보호위원회 구성, 정보보호책임자 지정, 정보보호책임관 지정 등의 조항을 통해 기구 및 조직을 구성하고 주요정보통신기반시설의 지정과 정보공유·분석센터의 구축을 통해 안전관리 체계를 마련하도록 되어 있다. 특히나 정보통신시설과 관련하여 취약점의 분석·평가를 실시하여 위험을 관리하고자 하고 있다. 또 하나의 특징은 기술개발이라는 조항을 통하여 전문인력 양성에 대한 시책을 강구하고 정보보호 기술개발과 관련된 연구기관과 민간단체를 지원할 수 있도록 했다는 것이다. SW 안전 관련법 제정안에도 소프트웨어 안전 관리 역량 강화를 위한 인력 양성과 관련한 조항과 소프트웨어 안전 관리에 필요한 기술개발 및 기술수준 향상을 위한 시책 마련에 대한 조항을 구성할 때 이에 대한 부분을 참고할 필요성이 있다.

또한 동법의 취약점 분석에 관한 조항들과 침해사고 통지 및 복구에 관한 내용들은 SW 안전법의 안전관리 기준과 손해방지조치에 대한 규율을 구성할 시 상당히 중요하게 다뤄져야할 부분이기 때문에 해당 내용들을 반드시 포괄할 수 있도록 심도 있게 검토해야 할 것이다.

제5절 원자력 안전 관련 법 분석

1. 원자력 안전 관련 법 체계

원자력의 안전을 규율하는 법률로는 「원자력안전법」, 「원자력안전위원회 설치 및 운영에 관한 법률」, 「원자력시설 등의 방호 및 방사능 방재 대책법」, 「원자력손해배상법」, 「생활주변방사선 안전관리법」 등이 있다. 이러한 원자력의 안전과 관련한 법률들은 행정부의 법규명령(대통령령과 부령)에 의해 구체화된다. 즉, 「원자력안전법」에서 위임한 사항을 정하는 「원자력안전법시행령」이 있고, 법률과 시행령에서 위임한 사항 및 동 법령의 집행에 관한 사항을 정하는 부령으로 「원자로시설 등의 기술기준에 관한 규칙」, 「방사선안전관리 등의 기술기준에 관한 규칙」, 「원자로시설 안전관련설비의 공급자 등 검사에 관한 규정」, 「부적합사항의 보고에 관한 규정」, 「원자력시설의 검사지적사항 처리에 관한 규정」, 「원자력통제교육에 관한 규정」 등이 있다.

원자력안전에 관한 보다 구체적인 사항은 행정규칙인 원자력안전위원회의 고시 형식으로 제정되어있는데, 이들 고시는 기술기준의 해석 또는 세부사항을 규정하는 것으로 현재 70여 개의 고시가 존재한다. 이보다 구체적인 사항은 전문적인 기술지원기관인 한국원자력안전기술원, 한국원자력통제기술원, 한국원자력의학원 등의 규제지침 형식으로 제정된다. 규제지침은 기술기준의 충족을 위해 허용 가능한 방법, 조건, 사양 등을 규정하고 있으며 기술기준 및 규제기준 등에 근거하여 업무별 세부 수행 방법 및 절차를 기술한 지침서인 심사·검사 지침서가 있다[36].

2. 주요 내용

2011년 후쿠시마 원전사고로 우리나라의 원자력 안전에 관한 규범체계에 대한 조정 필요성이 제기되어 1958년 제정된 기존의 원자력에 관한 기본법이었던 「원자력법」이 2011년 7월 「원자력진흥법」과 「원자력안전법」으로 분화되었다. 이러한 변화는 원자력을 안전하게 이용하기 위해서 무엇보다 안전규제의 독립이 요구되고, 국제원자력기구의 안전에 관한 기본원칙 및 원자력안전에 관한 협약 등에서 천명하듯이 원자력안전기구의 독립성을 확보하기 위한 것이었다.

36) 한국정보통신기술협회, “SW 안전진단 제도화 연구”, 2015, 73pg.

따라서 원자력안전에 관한 직접적 규범으로 제정된 「원자력안전법」은 원자력 안전의 독립성을 확보하고 관련 국제 규약의 내용을 충실하게 이행하기 위한 조항들로 구성되어 있다. 동법은 원자력 안전관리에 관한 사항은 원자력안전위원회가 주관하도록 하였으며, 원자력 이용 및 진흥체제와 원자력 안전규제체제를 분리함으로써 원자력안전규제의 독립성을 확보하여 방사선에 의한 재해의 방지와 공공의 안전을 도모할 수 있도록 하였다. 또한 동법은 원자력안전종합계획의 수립, 원자력안전전문기관의 설립, 원자력 관련 시설 및 핵물질 등에 관한 안전조치와 수출입통제 등의 업무를 효율적으로 추진하기 위한 한국원자력통제기술원의 설립을 통해 원자력과 관련된 각종 활동에 대한 허가 및 승인 체계를 갖추고 있다.

원자력 안전 관련 법 체계 내에는 「원자력안전법」이외에도 그 하위 수준으로 다양한 목적을 위해 만들어진 행정규칙들이 존재한다. 「원자력안전법」제15조 3에 따른 부적합사항 보고를 이행하는데 필요한 절차 및 방법을 규정하는 것을 목적으로 하는 「부적합사항의 보고에 관한 규정」, 원자력관계시설 및 사업자등에 대한 검사에 따른 지적사항의 처리 및 관리에 관한 사항을 규정하는 것을 목적으로 하는 「원자력시설의 검사지적사항 처리에 관한 규정」, 원자로 및 관계시설과 핵연료주기시설의 위치·구조·설비·성능·운영·품질보증·해체 및 사고관리에 관한 기술기준을 규정하는 것을 목적으로 하는 「원자로시설 등의 기술기준에 관한 규칙」, 원자력통제교육에 관하여 필요한 사항을 정하고 있는 「원자력통제교육에관한규정」이 이에 해당한다고 할 수 있다.

3. 안전관리 관점의 법률 분류

「원자력안전법」 및 동법 시행령, 그리고 해당 법의 행정규칙들에 포함된 조항들을 전체적으로 분석하여 안전관리 관점의 법률 분류를 실시하였다.

1) 예방 단계

- 안전관리 기구 및 조직 구성

「원자력안전법」(제5조) 원자력안전전문기관

위원회의 감독하에 원자력안전관리에 관한 사항을 전문적으로 수행하기 위하여 원자력안전전문기관을 둘 수 있다.

「원자력안전법」(제53조의2) 방사선안전관리자

허가사용자 및 신고사용자는 방사선 안전관리에 관한 다음 각 호의 업무를 수행하기 위하여 대통령령으로 정하는 바에 따라 방사선안전관리자를 선임하여 방사성동위원소 등의 사용개시 전에 이를 위원회에 신고하여야 한다. 신고한 사항을 변경하려는 때에도 또한 같다.

「원자력안전법 시행령」(제82조의2) 방사선안전관리자의 선임 등

허가사용자 및 신고사용자는 사업소마다 방사선안전관리자를 선임하여야 하며, 선임한 방사선안전관리자를 변경하거나 해임한 때에는 지체 없이 새로운 방사선안전관리자를 선임하여야 한다.

- 안전관리 체계 마련

「원자력안전법」(제5조) 원자력안전전문기관

위원회의 감독하에 원자력안전관리에 관한 사항을 전문적으로 수행하기 위하여 원자력안전전문기관을 둘 수 있다.

「원자력안전법」(제6조) 한국원자력통제기술원의 설립

원자력 관련 시설 및 핵물질 등에 관한 안전조치와 수출입통제 등(이하 “원자력통제“라 한다)의 업무를 효율적으로 추진하기 위하여 한국원자력통제기술원(이하 “통제기술원“이라 한다)을 설립한다.

「원자력안전법」(제7조의2) 한국원자력안전재단의 설립

원자력 및 방사선 안전기반 조성 활동을 효율적으로 지원하기 위하여 한국원자력안전재단(이하 “안전재단“이라 한다)을 설립한다.

- 안전점검 및 안전 조치

「원자력안전법」(제8조) 실태조사

위원회는 원자력안전정책을 효율적으로 추진하기 위하여 원자력안전에 관한 실태조사를 실시하여야 한다. 이 경우 위원회는 대통령령으로 정하는 기관 또는 단체로 하여금 실태조사를 실시하게 할 수 있다.

「원자력안전법」(제16조) 검사

발전용원자로설치자, 공급자 및 성능검증기관은 발전용원자로 및 관계시설의 건설, 특정핵물질의 계량관리에 관한 사항을 대통령령으로 정하는 바에 따라 위원회의 검사를 받아야 한다.

「원자력안전법」(제22조) 검사

발전용원자로운영자, 공급자 및 성능검증기관은 발전용원자로 및 관계시설의 운영, 특정핵물질의 계량관리에 관한 사항을 대통령령으로 정하는 바에 따라 위원회의 검사를 받아야 한다.

「원자력안전법」(제23조) 주기적 안전성평가

발전용원자로운영자는 대통령령으로 정하는 바에 따라 발전용원자로 및 관계시설의 안전성을 주기적으로 평가하고, 그 결과를 위원회에 제출하여야 한다.

「원자력안전법」(제26조) 운영에 관한 안전조치 등

발전용원자로운영자가 발전용원자로 및 관계시설을 운영할 때에는 대통령령으로 정하는 바에 따라 인체 · 물체 및 공공의 안전을 위하여 필요한 조치를 하여야 한다.

「원자력안전법」(제37조) 검사

핵연료주기사업자는 핵연료주기시설의 설치 및 운영, 특정핵물질의 계량관리에 관한 사항을 대통령령으로 정하는 바에 따라 위원회의 검사를 받아야 한다.

「원자력안전법」(제40조) 운영에 관한 안전조치 등

핵연료주기사업자가 그 시설을 운영할 때에는 인체 · 물체 및 공공의 안전을 위하여 대통령령으로 정하는 바에 따라 안전조치를 하여야 한다.

「원자력안전법」(제47조) 검사

핵연료물질사용자는 핵연료물질의 사용 또는 소지, 특정핵물질의 계량관리에 관한 사항을 대통령령으로 정하는 바에 따라 위원회의 검사를 받아야 한다.

「원자력안전법」(제56조) 검사

허가사용자 및 업무대행자는 방사성동위원소등의 생산・판매・사용・이동사용 또는 대행업무를 대통령령으로 정하는 바에 따라 위원회의 검사를 받아야 한다. 다만, 대통령령으로 정하는 바에 따라 검사가 면제되는 경우에는 그러하지 아니하다.

「원자력안전법」(제59조의2) 발주자의 안전조치 의무

방사선투과검사를 위하여 제53조에 따라 방사성동위원소등을 이동사용하는 경우 방사선투과검사를 의뢰한 발주자(이하 “발주자“라 한다)는 발주자의 사업장에서 방사성동위원소등을 이동사용하는 방사선작업종사자가 과도한 방사선에 노출되지 아니하도록 위원회규칙으로 정하는 바에 따라 안전한 작업환경을 제공하여야 한다.

「원자력안전법」(제61조) 검사

제작 또는 수입한 방사선기기는 대통령령으로 정하는 바에 따라 위원회의 검사를 받아야 한다. 다만, 대통령령으로 정하는 바에 따라 검사가 면제되는 경우에는 그러하지 아니하다.

「원자력안전법」(제65조) 검사

방사성폐기물관리시설등건설・운영자는 방사성폐기물관리시설등의 설치・운영, 방사성폐기물의 저장・처리・처분, 특정핵물질의 계량관리에 관한 사항을 대통령령으로 정하는 바에 따라 위원회의 검사를 받아야 한다.

「원자력안전법」(제77조) 검사

원자력관계사업자는 승인을 받아 제작·수입된 운반용기 및 사용 중인 운반용기를 대통령령으로 정하는 바에 따라 위원회의 검사를 받아야 한다. 다만, 대통령령으로 정하는 바에 따라 검사가 면제되는 경우에는 그러하지 아니하다.

「원자력안전법」(제80조) 검사

판독업무자는 판독업무 등을 대통령령으로 정하는 바에 따라 위원회의 검사를 받아야 한다.

「원자력안전법」(제91조) 방사선장해방지조치

원자력관계사업자는 방사선장해를 방지하기 위하여 대통령령으로 정하는 바에 따라 다음 각 호의 조치를 하여야 한다.

1. 방사선량 및 방사성오염의 측정

2. 건강진단

3. 피폭관리

4. 방사성물질의 방출량 및 피폭방사선량을 가능한 한 합리적으로 낮게 유지하기 위하여 필요한 조치

「원자력안전법 시행령」(제27조) 사용 전 검사

발전용원자로설치자는 원자로시설의 공사 및 성능에 대하여 각 공정별로 위원회의 검사를 받아 이에 합격한 후가 아니면 해당 시설을 사용하여서는 아니 된다.

「원자력안전법 시행령」(제31조) 품질보증검사

위원회는 발전용원자로설치자가 제출한 품질보증계획서에 따라 그 품질보증에 관한 업무를 수행하는지를 검사할 수 있다.

「원자력안전법 시행령」(제31조의2) 공급자 등 검사

위원회는 공급자 및 성능검증기관에 대하여 다음 각 호의 사항을 검사할 수 있다.

1. 안전관련설비의 설계·제작·성능검증 관련 사항이 법 제11조에 따른 허가기준에 적합한지 여부에 관한 사항

2. 법 제15조의2에 따른 안전관련설비 계약 신고 내용과 관련된 사항

3. 법 제15조의3에 따른 부적합사항 보고에 관한 사항

4. 그 밖에 위원회가 필요하다고 인정하는 사항

「원자력안전법 시행령」(제35조) 정기검사

발전용원자로운영자는 원자로시설의 운영 및 성능에 관하여 총리령으로 정하는 검사대상 및 검사방법에 따라 정기적으로 검사를 받아야 한다

「원자력안전법 시행령」(제50조) 정기검사

정련사업자는 총리령으로 정하는 바에 따라 정기적으로 위원회의 검사를 받아야 한다.

「원자력안전법 시행령」(제55조) 시설검사

가공사업자는 가공시설(변환시설을 포함한다. 이하 같다)의 공사 및 성능에 관하여 위원회의 검사를 받아야 한다

「원자력안전법 시행령」(제57조) 품질보증검사

위원회는 가공사업자가 법 제35조제3항에 따라 제출한 품질보증계획서에 따라 그 품질보증에 관한 업무를 수행하는지를 검사할 수 있다.

「원자력안전법 시행령」(제58조) 정기검사

가공사업자는 가공시설의 성능에 관하여 총리령으로 정하는 바에 따라 정기적으로 위원회의 검사를 받아야 한다. 다만, 다른 법령에 따라 전문검사기관으로 지정을 받은 기관이 실시한 검사의 내용과 중복되는 경우에는 검사를 생략할 수 있다.

「원자력안전법 시행령」(제63조) 사용 전 검사

사용후핵연료처리사업자는 사용후핵연료처리시설의 공사 및 성능에 관하여 위원회의 검사를 받아야 한다.

「원자력안전법 시행령」(제65조) 정기 검사

사용후핵연료처리사업자는 사용후핵연료처리시설의 성능에 관하여 총리령으로 정하는 바에 따라 정기적으로 검사를 받아야 한다.

「원자력안전법 시행령」(제73조) 시설검사

핵연료물질사용자는 핵연료물질 사용시설 등에 대하여 위원회의 검사를 받아야 한다. 그 사용시설 등을 변경하는 경우에 해당 사용시설 등에 대해서도 또한 같다.

「원자력안전법 시행령」(제75조) 정기검사

사용후핵연료처리사업자는 사용후핵연료처리시설의 성능에 관하여 총리령으로 정하는 바에 따라 정기적으로 검사를 받아야 한다.

「원자력안전법 시행령」(제85조) 시설검사

허가사용자는 방사성동위원소등의 생산시설·사용시설·분배시설·저장시설·보관시설·처리시설 및 배출시설(이하 “사용시설등“이라 한다)을 설치 또는 변경한 경우에는 해당 시설에 대하여 위원회의 검사를 받아야 한다.

「원자력안전법 시행령」(제88조) 정기검사

허가사용자는 사용시설등의 시설 및 그 운영에 관하여 총리령으로 정하는 바에 따라 정기적으로 위원회의 검사를 받아야 한다.

「원자력안전법 시행령」(제101조) 사용 전 검사

방사성폐기물관리시설등건설·운영자는 방사성폐기물관리시설등의 공사 및 성능에 관하여 위원회의 검사를 받아야 한다.

「원자력안전법 시행령」(제103조) 정기검사

방사성폐기물관리시설등건설·운영자는 방사성폐기물관리시설등의 설치·운영 및 방사성폐기물의 저장·처리·처분에 관하여 총리령으로 정하는 바에 따라 정기적으로 위원회의 검사를 받아야 한다.

「원자력안전법 시행령」(제104조) 처분검사

방사성폐기물관리시설등건설·운영자는 방사성폐기물을 처분하려면 위원회가 정하는 바에 따라 처분검사를 받아야 한다.

「원자력안전법 시행령」(제115조) 판독검사

판독업무자는 판독시설의 설치·운영 및 판독 성능에 대하여 총리령으로 정하는 바에 따라 위원회의 검사를 받아야 한다.

「부적합사항의 보고에 관한 규정」(제6조) 불일치 사항의 평가

모든 불일치 사항은 가능한 이른 시일 내에 부적합사항 보고 요건에 해당되는지 여부가 평가되어야 한다. 다만, 이 평가에 소요되는 기간은 발견된 날부터 최대 30일이 넘어서는 아니 된다.

「원자로시설 등의 기술기준에 관한 규칙」(제76조) 검사

사업자는 품질에 영향을 미치는 업무가 지시서·절차서 및 도면에 따라 수행되었는지를 확인하기 위한 검사계획을 수립·시행하여야 한다.

「원자로시설 안전관련설비의 공급자 등 검사에 관한 규정」(제3조) 계획검사

원자력안전위원회는 매년 12월 말까지 다음 해의 연간 검사계획을 수립한다.

「원자로시설 안전관련설비의 공급자 등 검사에 관한 규정」(제5조) 검사방법

검사는 서류검토, 현장 확인 또는 수검자와의 면담 등을 통해 이뤄지며, 중요한 제작 및 시험 공정에 대하여는 입회검사를 할 수 있다.

2) 대비 단계

- 안전관리 계획 수립

「원자력안전법」(제3조) 원자력안전종합계획의 수립

「원자력안전위원회의 설치 및 운영에 관한 법률」 제3조에 따른 원자력안전위원회(이하 "위원회"라 한다)는 원자력이용에 따른 안전관리(이하 "원자력안전관리"라 한다)를 위하여 5년마다 원자력안전종합계획(이하 "종합계획"이라 한다)을 수립하여야 한다.

「원자력안전법」(제4조) 종합계획의 시행

위원회는 확정된 종합계획을 관계 부처의 장에게 통보하여야 하며, 위원회와 관계 부처의 장은 종합계획에 따라 소관 사항에 대하여 5년마다 부문별 시행계획을 수립하고, 부문별 시행계획에 따라 연도별 세부사업추진계획을 수립·시행하여야 한다.

「부적합사항의 보고에 관한 규정」(제5조) 이행관리체계

사업자는 이 규정을 이행하기 위하여 필요한 조직, 책임부여, 이행절차 등이 포함된 관리체계를 수립하여야 하며, 이를 절차서 등으로 문서화하여야 한다.

「원자로시설 등의 기술기준에 관한 규칙」(제12조) 안전등급 및 규격

안전에 중요한 구조물·계통 및 기기는 안전기능의 중요도에 상응하는 안전등급 및 규격에 따라 설계·제작·설치·시험·검사되어야 한다. 안전등급 및 등급별 규격은 원자력안전위원회가 정하여 고시한다.

「원자로시설 등의 기술기준에 관한 규칙」(제59조) 화재방호계획

발전용원자로운영자는 영 제41조제1항제4호의 규정에 의하여 화재예방·감지 및 진화를 위하여 원자력안전위원회가 고시하는 바에 따라 화재방호계획을 수립하고 이를 이행하여야 한다.

「원자로시설 등의 기술기준에 관한 규칙」(제62조) 방사선방호계획

발전용원자로운영자는 방사선방호계획과 관련하여 다음 각호의 조치를 취하여야 한다.

1. 원자로시설의 운영중 종사자 및 주민의 방사선피폭을 가능한 한 최소화하기 위하여 방사선피폭을 일으키는 모든 활동을 관리·평가하는 방사선방호계획을 수립할 것

2. 방사선방호계획은 원자로시설의 설계 및 운전과 관련하여 방사선방호에 대한 충분한 지식 및 실무경험을 갖춘 보건물리요원에 의하여 이행되도록 하고, 보건물리요원은 발전소종사자가 피폭을 낮추도록 노력하고 필요시 수행하여야 할 보호조치를 숙지하도록 교육 및 훈련을 받게 할 것

3. 방사선방호계획의 내용 및 이행상태를 주기적으로 평가하고, 이에 위반된 사항이 발생할 경우 즉시 재발방지 조치를 할 것

「원자로시설 등의 기술기준에 관한 규칙」(제63조) 시험·감시·검사 및 보수

발전용원자로운영자는안전 관련 구조물·계통 및 기기의 안전기능 및 성능을 설계시 가정하고 의도한 대로 유지하기 위하여 안전의 중요도를 고려한 시험·감시·검사 및 보수 계획을 수립하여야 하며, 원자력안전위원회가 정하여 고시하는 바에 따라 조치를 취하여야 한다.

「원자로시설 등의 기술기준에 관한 규칙」(제69조) 품질보증 계획

사업자는 원자로의 건설·운영 등의 업무개시 전에 품질보증계획을 수립하고 이를 지침서·절차서 또는 지시서 등의 서류로 작성하여야 한다.

「원자로시설 등의 기술기준에 관한 규칙」(제85조의21) 사고관리전략 및 이행체계

사고관리전략은 다음 각 호의 기준에 적합하여야 한다.

1. 사고관리를 위해 유지·복구되어야하는 필수안전기능을 정의하고, 인적요소를 고려한 제반 조치사항을 포함할 것

2. 사고관리 전략의 기술적 근거와 절차서·지침서 작성방법 및 유지관리계획을 포함할 것

「원자로시설 등의 기술기준에 관한 규칙」(제85조의22) 사고관리능력의 평가

사고관리계획은 사고관리에 관한 설비, 사고관리 전략 및 이행체계 등 사고관리 능력을 평가하여 다음 각 호를 달성하는 것을 목표로 수립되어야 한다.

- 안전관리 능력 향상

「원자력안전법」(제106조) 교육훈련

원자력관계사업자는 방사선작업종사자와 방사선 관리 구역에 출입하는 사람에게 대통령령으로 정하는 바에 따라 원자력이용에 따르는 안전성 확보 및 방사선장해방지에 필요한 교육 및 훈련을 실시하여야 한다.

「원자력안전법 시행령」(제148조) 방사선작업종사자 및 수시출입자 교육

원자력관계사업자는 방사선작업종사자에 대해서는 신규교육과 정기교육을 실시하여야 한다. 이 경우 신규교육은 작업 종사 전에 실시하여야 한다.

「원자력안전법 시행령」(제148조의2) 교육계획의 제출

안전재단은 매년 11월 30일까지 다음 각 호의 사항이 포함된 다음 해의 기본교육계획을 위원회에 제출하고, 위원회의 승인을 받아야 한다.

1. 연간 교육일정, 교육과정, 교육대상, 과정별 이수과목과 시간 등에 관한 사항

2. 예산 및 결산에 관한 사항(교육훈련분야만 해당한다)

3. 강사, 교육시설·장비 현황 및 확충계획

4. 교육비 및 교재비에 관한 사항

5. 교육의 평가방법 및 결과에 따른 조치사항

「원자력안전법 시행령」(제148조의3) 방사선관리구역 출입자 교육

원자력관계사업자는 법 제106조제1항에 따라 방사선관리구역에 출입하는 사람에 대해서는 출입할 때마다 방사선장해방지 등에 대하여 안전수칙을 알려주는 등 필요한 교육을 실시하여야 한다.

「원자력통제교육에 관한 규정」(제6조) 교육계획의 수립

교육주관기관의 장은 다음 각 호의 사항을 포함한 다음연도 통제교육계획을 수립하여 매년 12월 31일까지 원자력안전위원회에 제출하여야 한다.

1. 교육일시 및 장소
2. 기관별 교육대상 인원
3. 교과 과목별 강사
4. 주요 교육내용을 포함한 교육프로그램
5. 교육방법 및 기자재 활용계획
6. 기록의 유지

「원자력통제교육에 관한 규정」(제8조) 교육시간, 내용 및 방법

교육시간 및 내용은 「원자력안전법 시행규칙」(이하 “규칙“이라 한다) 제141조제2항 관련 별표 6에 따라 실시한다.

「원자력시설 등의 기술기준에 관한 규칙」(제55조) 자격 및 훈련

발전용원자로운영자는 적합한 자격을 갖춘 자가 발전소 업무에 종사하도록 조치를 취하여야 한다.

「원자력시설 등의 기술기준에 관한 규칙」(제57조) 인적 요소의 관리

발전용원자로운영자는 발전소를 운영함에 있어 인적 오류를 낮출 수 있도록 인적 요소에 의한 사고 및 사고근접 사례를 설비 및 절차서에 반영하고, 직무 수행능력의 저

하를 방지하도록 관리하여야 한다.

「원자력시설 등의 기술기준에 관한 규칙」(제85조의23) 사고관리 교육 훈련

사고관리계획의 유효성을 유지하기 위하여 수립되는 교육 및 훈련계획은 다음 각 호의 기준에 적합하여야 한다.

1. 사고관리 조직의 구성원에 대하여 그 책임 및 권한에 상응하는 교육을 주기적으로 실시할 것

2. 사고관리 전략 및 이행체계의 유효성을 확인할 수 있는 훈련을 2년 이내의 주기로 실시할 것

3) 대응 단계

- 응급조치

「원자력안전법」(제74조) 사고의 조치 등

원자력관계사업자 또는 원자력관계사업자로부터 방사성물질등의 운반을 위탁받은 자는 방사성물질등의 운반 또는 포장 중에 발생할 수 있는 사고에 대비하여 총리령으로 정하는 바에 따라 비상대응계획을 수립·시행하여야 한다.

「원자력안전법 시행령」(제110조) 사고 시의 조치 등

원자력관계사업자나 방사성물질등의 운반을 위탁받은 자가 제1항에 따른 사고가 발생한 경우에 하여야 할 안전조치에 대해서는 제136조를 준용한다. 원자력관계사업자나 방사성물질등의 운반을 위탁받은 자는 제1항제5호 또는 제6호의 사고가 발생한 경우에는 그 지역을 관할하는 경찰관서에 즉시 신고하여야 한다.

「원자력안전법 시행령」(제134조) 피폭저감화 조치

원자력관계사업자가 하여야 할 조치는 다음 각 호와 같다.

1. 방사선작업종사자 또는 수시출입자가 방사선장해를 받았거나 받은 것으로 보이는 경우에는 지체 없이 의사의 진단 등 필요한 보건상의 조치를 하고, 그 방사선장해의 정도에 따라 방사선관리구역 출입시간의 단축, 출입금지 또는 방사선피폭 우려가 적은

업무로의 전환 등 필요한 조치를 하여야 한다.

2. 방사선관리구역에 일시적으로 출입하는 사람이 방사선장해를 받았거나 받은 것으로 보이는 경우에는 지체 없이 의사의 진단 등 필요한 보건상의 조치를 하여야 한다.

「원자력안전법 시행령」(제135조) 방사선장해를 받은 사람 등에 대한 조치

원자력관계사업자가 하여야 할 조치는 다음 각 호와 같다.

1. 방사선작업종사자 또는 수시출입자가 방사선장해를 받았거나 받은 것으로 보이는 경우에는 지체 없이 의사의 진단 등 필요한 보건상의 조치를 하고, 그 방사선장해의 정도에 따라 방사선관리구역 출입시간의 단축, 출입금지 또는 방사선피폭 우려가 적은 업무로의 전환 등 필요한 조치를 하여야 한다.

2. 방사선관리구역에 일시적으로 출입하는 사람이 방사선장해를 받았거나 받은 것으로 보이는 경우에는 지체 없이 의사의 진단 등 필요한 보건상의 조치를 하여야 한다.

- 대응 활동

「원자력안전법」(제15조3) 부적합사항 보고

원자력관계사업자는 원자력이용시설의 정상운전 및 비정상상태(사고의 경우는 제외한다)에서 원자력이용시설에 종사하는 방사선작업종사자 및 수시출입자와 시설 주변 주민의 방사선피폭을 최소화하기 위하여 위원회가 정하는 바에 따라 다음 각 호의 조치를 하여야 한다.

1. 방사선 작업 특성에 부합하는 방호조치

2. 방사선차폐 및 시설의 적절한 배치

3. 선량 저감에 효과적인 재료 및 기기의 사용

4. 적절한 작업공간의 확보

「원자력안전법」(제103조의2) 정보공개의무

위원회는 공공의 안전을 도모하기 위하여 원자력이용시설에 대한 건설허가 및 운영허가 관련 심사결과와 원자력안전관리에 관한 검사결과 등 대통령령으로 정하는 정보를 적극적으로 공개하여야 한다. 다만, 국가의 중대한 이익을 현저히 해칠 우려가 있

는 경우 공개하지 아니할 수 있다.

「부적합사항의 보고에 관한 규정」(제7조) 부적합 사항의 통지

제2조제1항제2호가목에 의한 부적합사항으로 판정된 경우 및 제6조제1항에 따른 평가를 통하여 제2조제1항제2호나목에 의한 부적합 사항으로 판정된 경우는 그 판정이 완료된 후 가능한 이른 시일 내에 경영진 또는 책임 있는 직원(이하 "보고책임자"라 한다)에게 그 사실이 통지되어야 한다. 다만, 이 통지에 소요되는 기간은 판정이 종료된 날부터 근무일 기준 최대 2일이 넘어서는 아니 된다.

「부적합사항의 보고에 관한 규정」(제8조) 보고

보고책임자는 제7조에 따라 통지 받은 경우에는 늦어도 다음 근무일 이내에는 별지 서식에 따른 보고서를 작성하여 원자력안전위원회에 제출하여야 한다.

4) 복구 단계

- 수습 본부 설치·운영

「원자로시설 등의 기술기준에 관한 규칙」(제47조) 비상대응시설 및 설비

① 원자로시설에는 방사선비상사고를 대비한 비상대응시설을 설치하여야 한다.

② 원자로시설에는 사고상황시 원자로시설내의 모든 사람들에게 경보 및 지시를 전달할 수 있도록 적절한 경보 및 방송장치를 설치하여야 한다.

③ 원자로시설에는 비상등이 구비된 안전한 대피경로가 갖추어져야 한다.

④ 방사선비상대응시설의 위치·크기·구조·거주성 및 관련설비(원자로시설의 비정상상태를 신속히 탐지하기 위하여 안전에 중요한 정보를 제공하는 설비를 포함한다)는 원자력안전위원회가 정하여 고시한다.

- 복구 계획 수립

「원자력안전법 시행령」(제136조) 장해방어조치 및 보고

원자력관계사업자가 하여야 할 안전조치는 다음 각 호와 같다.

1. 지진·화재·홍수·태풍 및 유해가스 누출 등의 재해로 인하여 원자력이용시설의

안전성이 위협을 받고 있거나 방사선작업종사자가 안전운영과 관련된 직무를 수행하는 데에 위협을 받을 경우에는 그 원인을 제거하고 피해 확대 방지를 위한 조치를 하여야 한다.

2. 원자력이용시설 등의 고장 등이 발생하여 원자력이용시설의 안전성이 위협을 받을 경우에는 고장 등의 원인을 제거하여 정상상태로 복구하여야 한다. 다만, 정상복구가 불가능할 경우에는 고장 등의 확대 방지를 위한 조치를 하여야 한다.

3. 방사성물질이 비정상적으로 누설되어 시설경계(제한구역경계가 설정되어 있는 경우에는 제한구역경계를 말한다)에서 공기 중 및 수중 농도가 위원회가 정하는 배출관리기준에 따른 제한값을 초과하거나 방사선작업종사자 또는 수시출입자가 선량한도를 초과하여 피폭된 경우에는 다음 각 목의 조치를 하여야 한다.

4. 법제 분류 결과 및 시사점

<표 3-11> 안전관리 관점에서의 원자력 관련 법제 분류 결과

안전관리 단계	세부 활동 영역	원자력 안전 관련 법률 조항
예방 단계	안전관리 기구 및 조직 구성	• 「원자력안전법」(제5조) 원자력안전전문기관
		• 「원자력안전법」(제53조의2) 방사선안전관리자
		• 「원자력안전법 시행령」 (제82조의2) 방사선안전관리자의 선임 등
	안전관리 체계 마련	• 「원자력안전법」(제5조) 원자력안전전문기관
		• 「원자력안전법」(제6조) 한국원자력통제기술원의 설립
		• 「원자력안전법」(제7조의2) 한국원자력안전재단의 설립
	안전점검 및 안전 조치	• 「원자력안전법」(제8조) 실태조사
		• 「원자력안전법」(제16조) 검사
		• 「원자력안전법」(제22조) 검사
		• 「원자력안전법」(제23조) 주기적 안전성평가
		• 「원자력안전법」(제26조) 운영에 관한 안전조치 등
		• 「원자력안전법」(제37조) 검사
		• 「원자력안전법」(제40조) 운영에 관한 안전조치 등
		• 「원자력안전법」(제47조) 검사
		• 「원자력안전법」(제56조) 검사
		• 「원자력안전법」(제59조의2) 발주자의 안전조치 의무
		• 「원자력안전법」(제61조) 검사

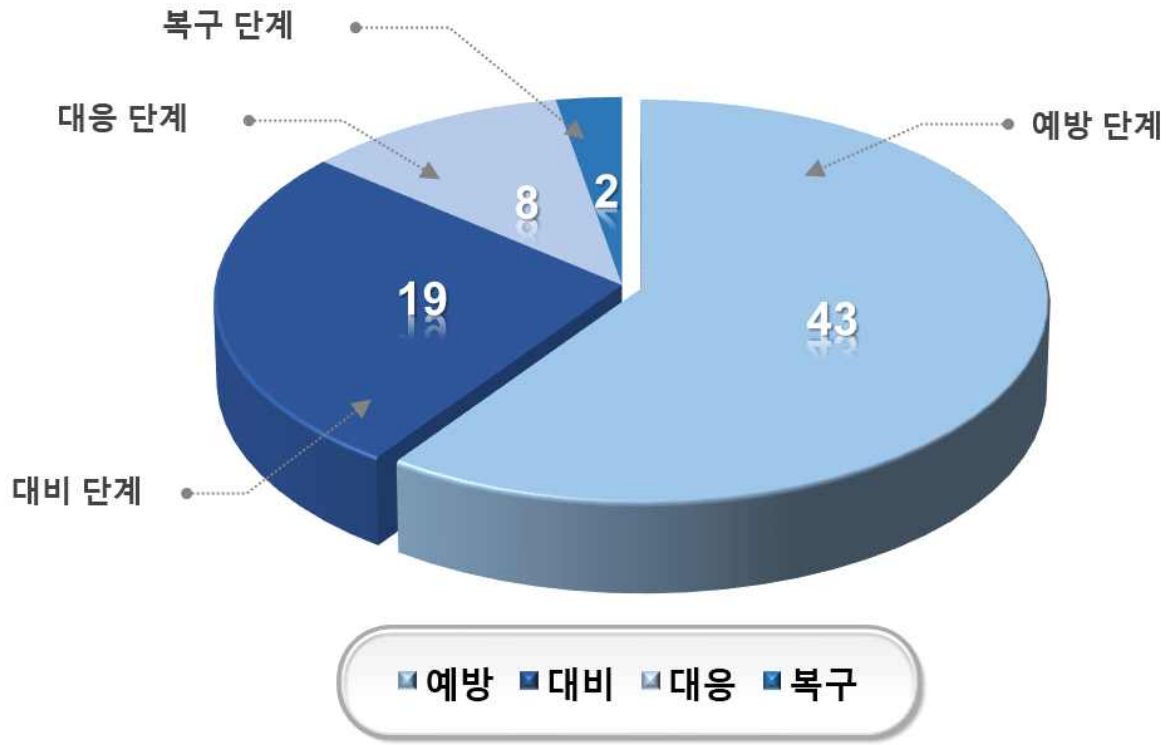
		• 「원자력안전법」(제65조) 검사
		• 「원자력안전법」(제77조) 검사
		• 「원자력안전법」(제80조) 검사
		• 「원자력안전법」(제91조) 방사선장해방지조치
		• 「원자력안전법 시행령」(제27조) 사용 전 검사
		• 「원자력안전법 시행령」(제31조) 품질보증검사
		• 「원자력안전법 시행령」(제31조의2) 공급자 등 검사
		• 「원자력안전법 시행령」(제35조) 정기검사
		• 「원자력안전법 시행령」(제50조) 정기검사
		• 「원자력안전법 시행령」(제55조) 시설검사
		• 「원자력안전법 시행령」(제57조) 품질보증검사
		• 「원자력안전법 시행령」(제58조) 정기검사
		• 「원자력안전법 시행령」(제63조) 사용 전 검사
		• 「원자력안전법 시행령」(제65조) 정기 검사
		• 「원자력안전법 시행령」(제73조) 시설검사
		• 「원자력안전법 시행령」(제75조) 정기검사
		• 「원자력안전법 시행령」(제85조) 시설검사
		• 「원자력안전법 시행령」(제88조) 정기검사
		• 「원자력안전법 시행령」(제101조) 사용 전 검사
		• 「원자력안전법 시행령」(제103조) 정기검사
		• 「원자력안전법 시행령」(제104조) 처분검사
		• 「원자력안전법 시행령」(제115조) 판독검사
		• 「부적합사항의 보고에 관한 규정」 (제6조) 불일치 사항의 평가
		• 「원자로시설 등의 기술기준에 관한 규칙」(제76조) 검사
		• 「원자로시설 안전관련설비의 공급자 등 검사에 관한 규정」(제3조) 계획검사
		• 「원자로시설 안전관련설비의 공급자 등 검사에 관한 규정」(제5조) 검사방법
	안전관련 산업의 육성과 안전문화 활동 지원	-
대비 단계	안전관리 계획 수립	• 「원자력안전법」(제3조) 원자력안전종합계획의 수립
		• 「원자력안전법」(제4조) 종합계획의 시행
		• 「부적합사항의 보고에 관한 규정」(제5조) 이행관리체계

		• 「원자로시설 등의 기술기준에 관한 규칙」 (제12조) 안전등급 및 규격
		• 「원자로시설 등의 기술기준에 관한 규칙」 (제59조) 화재방호계획
		• 「원자로시설 등의 기술기준에 관한 규칙」 (제62조) 방사선방호계획
		• 「원자로시설 등의 기술기준에 관한 규칙」 (제63조) 시험・감시・검사 및 보수
		• 「원자로시설 등의 기술기준에 관한 규칙」 (제69조) 품질보증 계획
		• 「원자로시설 등의 기술기준에 관한 규칙」 (제85조의21) 사고관리전략 및 이행체계
		• 「원자로시설 등의 기술기준에 관한 규칙」 (제85조의22) 사고관리능력의 평가
	안전관리 능력 향상	• 「원자력안전법」(제106조) 교육훈련
		• 「원자력안전법 시행령」 (제148조) 방사선작업종사자 및 수시출입자 교육
		• 「원자력안전법 시행령」(제148조의2) 교육계획의 제출
		• 「원자력안전법 시행령」 (제148조의3) 방사선관리구역 출입자 교육
		• 「원자력통제교육에 관한 규정」(제6조) 교육계획의 수립
		• 「원자력통제교육에 관한 규정」 (제8조) 교육시간, 내용 및 방법
		• 「원자력시설 등의 기술기준에 관한 규칙」 (제55조) 자격 및 훈련
		• 「원자력시설 등의 기술기준에 관한 규칙」 (제57조) 인적 요소의 관리
		• 「원자력시설 등의 기술기준에 관한 규칙」 (제85조의23) 사고관리 교육 훈련
대응 단계	대응 체계 구축・운영	-
	응급조치	• 「원자력안전법」(제74조) 사고의 조치 등
		• 「원자력안전법 시행령」(제110조) 사고 시의 조치 등
		• 「원자력안전법 시행령」(제134조) 피폭저감화 조치
		• 「원자력안전법 시행령」 (제135조) 방사선장해를 받은 사람 등에 대한 조치
	대응 활동	• 「원자력안전법」(제15조3) 부적합사항 보고
		• 「원자력안전법」(제103조의2) 정보공개의무
		• 「부적합사항의 보고에 관한 규정」 (제7조) 부적합 사항의 통지

		• 「부적합사항의 보고에 관한 규정」(제8조) 보고
복구 단계	수습 본부 설치·운영	• 「원자로시설 등의 기술기준에 관한 규칙」 (제47조) 비상대응시설 및 설비
	복구 계획 수립	• 「원자력안전법 시행령」(제136조) 장해방어조치 및 보고
	원인 조사	–

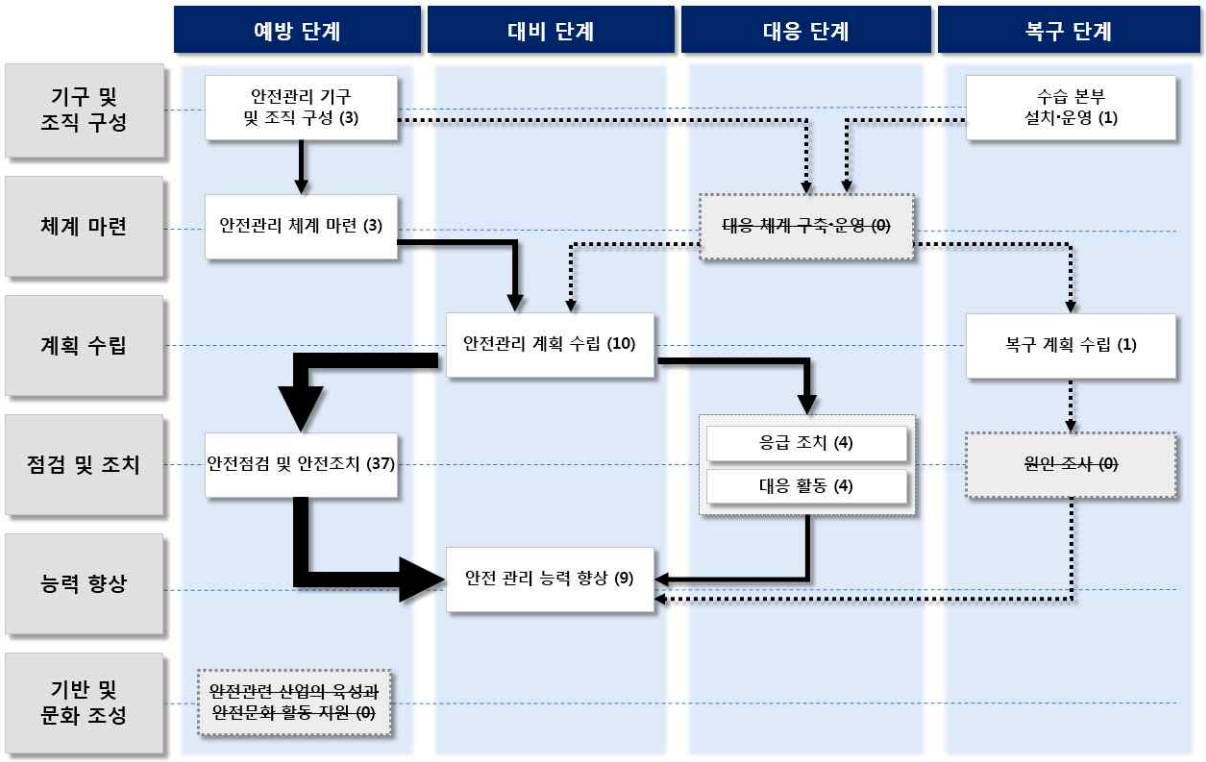
원자력 안전 관련 법률 조항들을 안전관리 관점의 분류 기준으로 분류한 결과, 예방 단계는 안전관리 기구 및 조직 구성 활동 3개 조항, 안전관리 체계 마련 활동 3개 조항, 안전점검 및 안전조치 활동 37개 조항으로 가장 많은 수의 조항인 총 43개 조항에 걸쳐 규율하고 있었다. 대비 단계에서는 안전관리 계획 수립 활동과 관련된 10개 조항, 안전 관리 능력 향상 9개 조항으로 총 19개 조항이 존재하였다. 대응 단계는 응급조치 활동 4개 조항, 대응 활동 4개 조항으로 총 8개로 분석되었으며, 복구 단계는 수습 본부 설치·운영 활동 1개 조항, 복구 계획 수립 활동 1개 조항으로 분석되었다. 이를 그래프로 나타내면 다음과 같다.

[그림 3-9] 원자력 안전 관련 법의 안전 관리 단계별 조항 개수 (단위:개)



원자력 분야는 사고가 발생하였을 시 국민들의 생명과 직결될 수 있는 분야로, 거의 모든 주요국들의 국가중요기반시설 도메인에 포함시키고 있는 중요한 분야이다. 따라서 우리나라도 다양한 법률을 통해 원자력 안전에 대한 규율을 하고 있으며, 안전관리의 측면에서도 많은 조항들을 삽입해놓은 것을 알 수 있었다.

[그림 3-10] 원자력 안전 관련 법의 안전관리 관점의 세부 분류 단계별 활동 흐름도



하지만 한번 사고가 발생하면 막대한 피해가 예상되어, 사고 자체의 발현 확률을 최대한 제거하는 것이 가장 바람직한 원자력 분야의 특성상, 원자력 안전 관련 법률 및 행정규칙들은 안전관리 단계 중 예방 및 대비 단계에 압도적으로 많은 수의 조항을 두고 있었다. 특히 예방 단계의 안전점검 및 안전조치에 해당하는 활동에서 검사, 실태조사, 주기적 안전성 평가, 방지 조치, 사용전 검사, 품질보증 검사, 정기검사, 시설검사, 처분검사, 판독 검사 등 다양한 형태의 점검 규정을 두어 점검 체계를 정밀하게 구축하는 데 초점이 맞춰져 있었다. 또한 대비 단계에 해당하는 다양한 원자력 안전 관련 계획의 수립을 통해 이러한 점검 및 조치 활동들이 효율적으로 수행될 수 있도록 하고 있었으며, 인적 요소로 인한 재난 발생을 방지하기 위해 다른 분야보다 특히 인적 교육에 많은 조항을 할애하고 있는 것을 볼 수 있었다.

다만 우리나라에서 원자력 관련한 대형 사고가 발생한 적이 아직 없었기 때문에

대부분의 조항들이 예방 및 대비에 지나치게 치중되어, 대응 체계 구축·운영에 대한 내용, 복구 단계의 원인 조사에 대한 내용이 포함되어 있지 않다는 점은 향후 보완되어야할 점으로 생각된다.

현재 원자력 부분의 SW 안전과 관련되어 구체적으로 법령에서 명시하고 있는 부분은 없었다. 하지만 원자력 분야는 SW 결함 등으로 인해 발생할 위험의 크기가 상당하며 실제 Stuxnet[37]과 같은 대규모의 APT공격이 이루어질 수 있는 분야이기에 원자력과 관련된 SW를 점검하고 규율할 수 있는 규정을 정립하는 것이 필요하다고 할 수 있다. 이를 위해 SW 안전 관련법을 제정한다면, 원자력 분야가 가지는 특성들을 면밀히 검토하여야 할 것이며, 특히 안전점검 및 안전조치 활동에 집중되어 있는 다양한 형태의 조항들에 SW 점검 및 조치에 대한 내용을 어떻게 적용하고 중복성을 최소화할 지에 대해서도 심도 있는 분석이 필요할 것이다.

37) 발전소 등 전력 설비에 쓰이는 지멘스의 산업자동화제어시스템(PCS7)만을 감염시켜 오작동을 일으키거나 시스템을 마비시키는 신종 웜 바이러스다. 원자력, 전기, 철강, 반도체, 화학 등 주요 산업 기반 시설중 지멘스사의 산업자동화제어시스템에 침투해 오작동을 일으키거나 시스템을 마비시킬 수 있다. 2010년 7월 동남아 지역에서 처음으로 발견된 뒤 이란 부셰르 원전과 관련된 컴퓨터 3만대와 중국의 주요 사회간접자본시설(SOC)까지 감염시켰다.

제6절 소결

우리나라는 ‘국가는 재해를 예방하고 그 위험으로부터 국민을 보호하기 위하여 노력하여야 한다’ 는 헌법 제34조 6항을 기반으로 하여, 재난과 관련한 사항은 『재난 및 안전관리 기본법』으로, 전자적 침해행위와 주요정보통신기반시설과 관련된 사항은 『정보통신기반보호법』을 통하여 보호하고 있었다. 국가기반체계를 직·간접적으로 구성하는 시설·기능·시스템 보호를 위한 체계들도 다양한 법률을 통하여 규율되어 있었으며, 법률 내에 대상 시설의 지정 목적과 범위, 방법이 상세히 규정되어 있었다.

분석된 국내 주요기반시설 보호 법제를 분석하기 위하여 『재난 및 안전관리 기본법』 제14조 및 동법 시행령 제15조 내지 제17조의 규정에 의해 제정된 ‘국가기반체계 보호관련 중앙재난안전대책본부 운영 및 상황관리 규정’ 에서 정의하고 있는 국가재난관리의 4단계 활동인 (예방-대비-대응-복구) 단계를 기반으로 안전관리 관점의 법률 분류 기준을 수립하였다. 수립한 분류 기준으로 국내 재난 안전 관리와 관련한 총괄적인 내용을 담고 있는 『재난 및 안전관리 기본법』과 정보통신기반시설에 대한 안전 관리를 규율하는 『정보통신기반보호법』, 국가중요기반시설의 도메인 중 사고가 생겼을 시 가장 큰 피해가 발생할 수 있는 대표 도메인인 원자력 안전에 관한 법에 대해 분석하였다.

분석 결과, 공통적으로 예방 단계에 해당하는 활동에 대한 조항의 개수가 전체 안전관리 관련 조항 중 50% 이상을 차지하였다. 대비 단계의 조항도 상당한 수를 차지하여 예방 및 대비 단계의 조항을 모두 합치면 전체 안전 관리 관련 조항의 70% 이상을 차지하는 것을 볼 수 있었다. 즉 안전관리 기구 및 조직 구성, 안전관리 체계 마련, 안전관리 계획 수립, 안전점검 및 안전조치, 안전 관리 능력 향상, 안전관리 산업의 육성과 안전문화 활동 지원 활동에 대한 체계적인 규율이 마련되어 있다는 것이다. 이는 정부가 오래토록 추진해온 예방 위주의 재난/사고 관리 대책의 성과라고 보여진다.

따라서 SW 안전을 위한 법 개정이나 제정안을 구성할 시 예방 및 대비 단계의 구성체계들을 비중 있게 분석하고 SW 안전에 대한 규율이 추가적이 필요한 부분을 도출해야 할 필요가 있다. 또한 자칫 중복 규제가 되어 기관들의 업무 효율성 저하로 이어져 새로운 법률 제·개정의 근본적 목적이 퇴색되지 않도록 기존 법률과 중복되는 규율이 없도록 하여야 할 것이다.

제4장 해외 주요국 주요기반시설 보호 법제 분석

제1절 미국의 주요기반시설 법령 분석

1. 미국 주요기반시설 보호 법제 개관

1) 배경 및 연혁

미국은 1803년 뉴햄프셔주의 화재참사를 지원하기 위해 의회법이 제정된 이후, 1905년대까지 홍수통제법, 재해구호법 등을 제정하며 재난관리관련 법제도를 구축하기 시작하였다. 그 이후 1960년대와 1970년대에 들어서 국가홍수보험법 제정 및 자연재해 위험정보 및 분석센터를 설립하고, 1979년 카터대통령에 의해 연방재난관리청(FEMA: Federal Emergency Management Agency)을 신설하였고, 1988년에는 Stafford 재난구호 및 긴급지원법을 제정하여 방재시스템의 기능 향상을 추진하였다. 21세기에 들어서 정보통신기술의 발전으로 현대사회의 기술 의존성이 높아짐에 따라, 국가 기반시설이 물리적, 전자적 수단에 의한 공격에 취약함을 인식하면서 1996년 클린턴 행정부는 물리적 및 사이버 위협이 국가 기반시설에 미치는 위험도 평가와 대응조치를 목적으로 전 국가적 대책을 본격적으로 모색하기 시작하였다.

클린턴 정부의 자세한 정책들을 살펴보면, 우선 행정명령(Executive Order 13010) “주요 기반시설 보호(Critical Infrastructure Protection)” 의 발표를 통하여 관련 대통령 위원회(각 부처로 구성)와 테스크 포스팀(FBI, 국방부, NSA 등)을 구성하여 임무 수행을 지시하였고 주요 기반시설로 전력시스템, 가스와 오일의 저장 및 수송, 은행과 금융, 교통, 상수도 공급 시스템, 비상서비스(의료, 경찰, 화재, 구급), 정부의 연속성을 지칭하였으며, 대통령 소속 ‘주요정보통신기반시설보호위원회(PCCIP, President’s Commission on Critical Infrastructure Protection’)를 구성, 취약성과 위험의 분석 및 평가, 법정책적 사안 도출, 종합적 국가정책 및 집행전략 권고 등의 임무를 수행토록 하였다[38].

그 후 미국은 1998년 PCCIP의 핵심으로 ‘정책지침 63호(PDD-63, Presidential Decision Directive 63)’ 을 발표하였고 ‘국가핵심기반시설 보증위원회(NIAC, National Infrastructure Assurance Council)’, ‘국가핵심기반시설 보호센터(NIPC, National

38) 정보통신정책연구원, 정보통신기반보호법 제정관련 기초연구, 2000, 36pg.

Infrastructure Protection Center)' 등 기반시설 보호를 위한 정책의 기반이 되는 조직들을 설립하였다. 특히 미국의 기반시설보호 정책은 2001년 9월 11일 뉴욕 세계무역센터 테러사고 이후 급격히 강화되었다는 점이 특징이다. 이를 통해 국민들의 국토안보 환경 및 국가안보에 대한 의식 또한 크게 향상되었다.

이에 따라 2001년 10월 행정명령 13228에 의하여 '국토안보국(Office of Homeland Security)' 이 신설되고, 행정명령 13231에 따라 '국가 핵심기반시설 보호를 위한 대통령 자문위원회(President's Critical Infrastructure Protection Board)' 설립되었다. 2002년에는 '국토안보법(Homeland Security Act of 2002)' 에 의거한 '국토안보부(DHS, Department of Homeland Security)' 와 행정명령 13260에 따라 '국토 안전보장 자문위원회(Homeland Security Advisory Council)' 을 설립하여 22개 연방정부 기관을 통합하여 국토안보 업무를 명확하고 효율적으로 계속하기 위한 조직구조 수립하게 된다. 그리고 이듬해인 2003년 연방재난관리청은 국토안보부 산하 기관으로 소속으로 들어가게 된다.

2003년에는 국가안보를 위한 대통령 훈령(HSPD, Homeland Security Presidental Directve) 7호에 근거하여 2006년 '국가기반보호계획(NIPP, the National Infrastructure Protection Plan)' 이 발표된다. NIPP는 주요기반시설의 보호를 위한 미션들을 정하고, 그 실행을 위해 필요한 법률, 국가전략, 국가안보에 관한 대통령령에 따른 활동들이 상호 협조적이고 통합적, 유기적으로 진행될 수 있는 구조를 제시하고 있으며, 2006년, 2009년 발행에 이어 현재 2013년 개정된 버전[39]에 따라 미국의 기반시설 보호체계가 추진되고 있다.

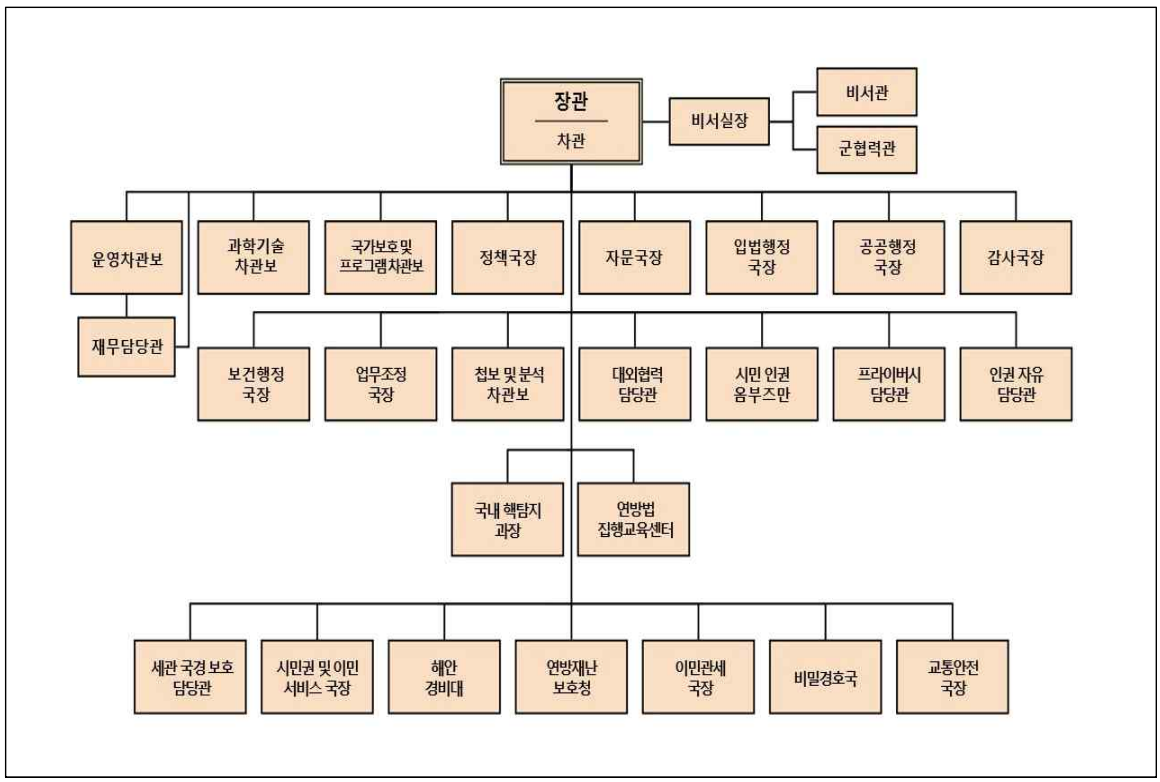
2) 주요기반시설 보호체계

미국의 재난관리는 국토안보부(DHS)와 연방재난보호청(FEMA)이 총괄하여 수행한다. 국토안보부는 국토안보를 담당하고 있는 100개 이상의 정부기관을 통합한 단일 안전관리부처로서 다양한 위협으로부터 유연하게 국가와 국민의 안전을 보장할 수 있도록

39) 2013년에 개정된 NIPP는 부제를 'Partnering for Critical Infrastructure Security and Resilience'로 설정하여 주요기반시설의 보호와 복구를 위한 협업 체계를 중심으로 하고 있으며, 2009년의 NIPP와는 다음과 같은 차이점을 보이고 있음; ① 국토안보와 주요 기반시설 보호를 위한 보안 및 복원력 강화, ② 주요 기반시설 위험관리 프레임 워크를 갱신하고, 예방/보호/완화/대응 및 복구의 단계별 분야에서 만반의 준비를 위한 임무를 할당, ③ 공공 및 민간 부문이 공동으로 결정한 주요 기반시설 국가 우선순위를 설정하는 절차 수립, ④ 주요 기반시설 관련 기업의 물리 및 사이버 위험 관리 시스템 통합, ⑤ 주요 기반시설 보안 및 복구와 국제협력의 중요성 명시, ⑥ 지역별 협력을 위한 국가 계획 및 국가적/지역사회적 차원에서 대비 목표 달성을 위한 지원, ⑦ 개별 센터 및 협력체 등 우선 순위에 따라 보안 및 복구를 위한 단계별 행동 요령 제공, US National Infrastructure Protection Plan, 2013, 4pg.

국경, 교통, 항만 및 국가핵심기반체계를 보호하는 조직으로 구성되어 있다.

[그림 4-1] 미국 국토안보부 조직도, 국토안보부(www.dhs.gov), 2016.



장관을 정점으로 장관을 보조하는 차관(Deputy Secretary)이 있으며, 참모(Chief of Staff)로 비서관(Executive Secretariat)과 군협력관(Military Advisor)이 있다. 그리고 차관(Under Secretary)을 장으로 하는 운영국 등 18개의 자체부서가 있으며, 해안경비대(U.S. Coast Guard) 등 7개의 부서가 국토안보부의 업무를 집행한다.

국토안보부는 정보분석국, 기반시설보호국, 생화학무기 관리국, 국경안전국, 비밀경호국, 연방재난보호청이 주요 업무를 담당하고 있다. 정보분석국은 다수의 요인으로부터 국토의 안보정보를 종합하여 분석하는 부처이며, 기반시설보호국은 위협과 대비에 대하여 주정부, 민간기업, 미국 국민과 정보를 교류할 수 있는 부처이다. 생화학무기 관리국은 생화학테러와 대량살상무기로부터 미국민을 보호하는 노력을 통합 관리, 운영하는 역할을 하며 국경안전국은 재난과 위기발생시 초기 대응을 위한 훈련 및 장비 보급 수행하고 있다. 비밀경호국은 테러리스트들의 활동 중단을 위해 안전요원들의 현장 활동을 활성화하는 역할을 하며 연방재난보호청은 연방정부의 위기관리 대응활동을 관리할 수 있는 부처이다. 마지막으로 연방재난보호청은 1961년 설립된 민방위청을

모태로 하여 다섯 개의 연방정부기관이 통폐합되어 1979년 신설되었다. 이는 자연재난과 인위적 재난을 전담하는 대통령 직속 전문기관으로 운용되어 왔으나 9.11 테러 이후 국토안보부로 소속이 변경 되었다.

연방재난보호청은 국가재난대응체계 프로그램의 운영을 통하여 자연 및 인적 재난관리를 전문적으로 담당하고 있으며, 피해경감(Mitigation), 대비(Preparedness), 대응(Response) 및 복구(Recovery) 영역에서 그 권한을 행사하고 핵심 역할을 수행하고 있다. 재난 및 비상사태와 관련되는 제반 기획, 대비훈련, 피해경감, 대응 및 복구 지원을 도우며 지방정부와 긴밀한 협조 아래 재해 및 재난 발생 시 기술적 지원과 교육을 담당한다. 연방긴급대응계획(FRP)을 통한 연방정부 차원의 지원의 조정 역할을 하기도 한다.

연방재난보호청의 조직 및 업무는 다음과 같다.

<표 4-1> 연방재난보호청의 조직별 주요 업무,
연방재난관리청(www.fema.gov), 2016.

구 분	내 용
대응, 복구국	재난 대비 계획 수립 및 훈련, 재난 대응 및 복구, 화학 및 방사능 물질 사고 대응
연방보험관리국	홍수보험프로그램 관리, FEMA의 완화프로그램 실행
연방소방국	화재 및 응급의료서비스 제공, 국립소방학교 운영, 국립비상교육센터 운영 등
대외협력국	국회와 정부기관간 관련 업무, 재난 관련 국제 업무 추진
정보기술서비스국	FEMA의 각종 운영프로그램 관리, 응용 프로그램의 개발 및 정보기술 지원
행정, 지원 기획국	FEMA의 인적자원관리, 전산시스템 기능 유지보수 및 재정관리
지방 운영기관(10개)	재난에 대한 지역별 예방활동, 재난발생시 긴급 대응 및 비상사태 관리 교육

미국의 주요기반시설 보호체계를 종합적으로 다루고 있는 정책은 국가기반시설보호계획(NIPP, National Infrastructure Protection Plan)이다. 2009년에 발표된 NIPP는 연방의 자금제공과 자원들의 취약성을 경감시키고(Mitigate vulnerabilities), 위협을 저지하고(Deter threats), 공격과 그 외 사고의 피해를 최소화하기 위하여(Minimize consequences) 국가 우선순위의 목표와 기반체계 보호를 위해 필요한 조건들과 그 운용 방안을 서술하고 있다. 앞서 언급하였다시피 NIPP에서는 국토안보부를 국가기반보호 총괄기관으로 지정하고 있으며, 동 계획에서는 정부와 민간분야의 노력을 조정하기 위한 수단으로서 파트너십 모델을 제시하고, 정부 내 의견조율을 위한 정부조정위원회(GCC, Government Coordinating Council)를 설치하여 종합적인 보호체계를 구축하도록 하고 있다.

이처럼 미국의 기반시설 보호체계는 통합적인 보호체계를 명시, 설명하고 있는 NIPP와 함께 분야별 세부 계획(SPP, Sector-Specific Plans)을 통해 상세히 정하고 있다. SPP는 16개의 주요 기반시설 각각의 부문에 따라 계획되는데, 정부 및 해당 업계가 협업하여 SSP를 개발하여 현장의 문제를 반영하고 있고, NIPP가 실행될 수 있는 구체적 방법을 제시하고 각 정부의 각 부문이 주, 지방 국토보안 전략과 기반 보호프로그램을 개발, 실행, 현행화 할 수 있도록 하는 국가적 체계를 제시한다. 특히, 각 부문의 특성을 고려하여 부문 간 역할과 책임, 상호의존성, 정보공유, 조정과 파트너십을 설정하고 조직화하는 역할이 주된 역할이며 이는 4년마다 갱신되어 각 분야에서 지속적으로 발전하는 위협에 효율적으로 대응할 수 있도록 보장한다. 미국의 주요기반시설 보호체계는 이러한 NIPP와 SPP에 따라 몇몇 구조 간[40] 유기적인 관계를 통해 효율적으로 작동하고 있는 것이다.

미국의 정보공유 및 협업 구조는 다음과 같다.

- SCCs(분야별 조정 위원회, Sector Coordinating Councils)

SCC는 각 부문별 구체적인 쟁점에 관한 전략, 정책, 활동에 대하여 자율적으로 구성, 운영되는 민간분야 조정 위원회로, 해당 분야의 의견을 대변함으로써 부문별 주요 기반시설에 대한 보안 및 복구 정책의 조정 및 계획과 관련, 정부와 민간의 협업 구조에 중요한 협력 지점이 된다. 특히 SSA 및 관련 GCC와 협력하여 해당 분야의 모든 핵심

40) 정보공유 및 협업 구조(Sector Coordinating Structures), 범 분야 협업 구조(Cross-Sector Coordinating Structure), 정보공유분석구조(Information Sharing and Analysis Organizations), 주요 기반시설 협력 자문위원회(Critical Infrastructure Partnership Advisory Council), 주요 기반시설 보호 및 복구를 위한 정보 공유 체계(Information Sharing for Critical Infrastructure Security and Resilience)

기반시설 보안 및 복구에 관한 활동, 문제 해결을 위한 분야별 정책 및 계획 수립을 맡고 있다. 예를 들어, 해당 분야의 신흥 위협이나 그에 대한 대응/복구 작업에 시설의 소유자, 운영자 및 공급 업체, 정부와 전략적 의사소통 및 조정을 결정하거나 정보 공유 체계를 갖추지 못한 분야에 대한 지원을 수행한다. 또한, 국가 계획 및 부문별 계획(SSP)의 개정, 수립 과정에 참여하고 국토안보부(DHS)에 연간 보고서를 제출하고 주요 기반시설의 보안 및 복구 계획, 훈련, 교육, 인식제고 및 관련 활동도 수행 한다. 이외에도 사이버 보안 실무 그룹, 위험 평가, 전략 및 계획 등 효과적인 사이버 보안 구현을 위해 공공, 민간 부문과 정보를 공유하는 역할, 각 부문의 정부 지원에 대한 요구사항 등을 협의하는 역할, 분야별 연구개발결과 및 요청사항을 정부에 제공하는 역할 등 다양한 역할을 수행하고 있다.

- GCCs(정부 조정 위원회, Government Coordinating Councils)

GCC는 분야별, 정부 간, 타 관할 구역 간 조정의 역할을 수행하며, 개별 부문의 운영 환경에 따라 연방 및 SLTT(State, Local, Tribal, and Territorial)의 대표로 구성된다. GCC는 국토안보부, 분야별 담당 기관(SSA) 및 다양한 정부 기관과의 협업을 통해 각 부문별 부처 간 전략적 소통 및 조정 역할을 수행하며 NIPP 및 SSP의 개발 및 개정과 관련된 작업에 참여하기도 한다. 또한 부문 내 정부 기관 간 문제 해결 및 조정을 수행하며 물리적, 전자적 위험 관리 프로세스의 개발 및 채택 장려하는 역할을 한다. 때에 따라서는 SSC의 임무를 지원하기도 한다.

- SSA(분야별 담당 기관, Sector-Specific Agencies)

PDD-21은 각 SSAs의 역할 및 책임에 관하여 규정하고 있다. SSA는 국토안보부 및 기타 유관 연방 기관, 주요 기반시설 관리자 등과 협업하여 PDD-21에 따른 명령을 수행하도록 되어있다. 특히 미국은 자연적, 인적, 사회적 재난을 별도 구분하지 않고 보호 대상을 중심으로 구분하여 국가안보 및 공공보건, 안전, 경제 활성화 등을 위한 필수적인 요소로서 핵심기반 및 주요자산(CIKR)의 보호 및 회복력(Resiliency) 확보를 중요시하고 있다[41].

이에 따라 구분되는 보호대상과 소관 부처는 다음과 같다.

41) US National Infrastructure Protection Plan, 2013,

<표 4-2> 미국의 기반분야별 시설보호 소관 부처(SSA, Sector-Specific Agencies), 미 국토안보부, www.dhs.gov/sector-specific-agencies, 16.11.22.

보호대상 기반 분야	소관 부처
Chemical	국토안보부(DHS)
Commercial Facilities	국토안보부(DHS)
Communications	국토안보부(DHS)
Critical Manufacturing	국토안보부(DHS)
Dams	국토안보부(DHS)
Defense Industrial Base	국방부(DOD)
Emergency Services	국토안보부(DHS)
Energy	에너지부(DOE)
Financial Services	재무부(DOT)
Food and Agriculture	농무부, 보건후생부(DOA, DHHS)
Government Facilities	국토안보부, 총무청(DHS, GSA)
Healthcare and Public Health	보건후생부(DHHS)
Information Technology	국토안보부(DHS)
Nuclear Reactors, Materials, and Waste	국토안보부(DHS)
Transportation Systems	국토안보부, 교통부(DHS, DOT)
Water and Wastewater Systems	환경보호청(EPA)

미국의 주요기반시설 보호체계는 범 분야 협업 구조라는 특징을 보인다. CICSC(주요기반시설 범분야 조정 위원회, Critical Infrastructure Cross-Sector Council)가 해당 구조의 핵심이다. CICSC는 CC의 의장과 부의장으로 구성된 민간 협의회로 주요 기반시설의 보안 및 복구를 지원하기 위해 다른 분야간 주권, 이익관계 등 문제와 상호 협력 관계를 조정한다. FSLC(연방 고위 위원회, Federal Senior Leadership Council)는 연방정부의 주요 기반시설 보안 및 복구 관련 소통, 협력 증진과 조정 역할을 담당하며, SSA 및 타 연방 부서/기관의 고위 공무원으로 구성된다.

SLTTGCC(지자체 조정 위원회, State, Local, Tribal and Territorial Government Coordinating Council)는 주, 지역, 인가된 부족 조직, 지역사회 등 기관의 대표들로 구성되며, 참여 기관들간 소통 및 협력을 촉진하고 주 및 지방 정부의 지침, 전략 및 프로그램에 대하여 대표권을 갖고 관여함으로써 조정의 역할 수행한다. 또한 RC3(지역 협력체 조정 위원회, Regional Consortium Coordinating Council)는 공공 및 민간 부문에서 주요 기반시설의 보호, 복구 등 대응력 제고를 위해 지역 다자간 그룹 및 연합 구성된 위원회이다.

미국은 사고 및 위기에 대한 정보를 빠르게 공유하고 대처하기 위해 ISACs(정보공유분석구조, Information Sharing and Analysis Organizations)을 운영하고 있다. 정보공유분석센터 등 정보공유조직은 여러 분야 및 기타 그룹의 정보 운영 및 제공, 정부와 민간 부문간 정보 공유 촉진과 같은 역할 수행한다. 정보공유분석센터는 1984년에 운영된 국가통신조정센터(NCC, National Coordinating Center for Communications)를 기원으로 하고 있으며, 1999년 재정서비스 분야의 정보공유분석센터(Financial Services ISAC)가 최초로 창설된 이래로 현재 16개의 정보공유분석센터[42]가 운용 중이다. 연합체로는 정보공유분석센터 위원회(ISAC Council)[43]를 구성하고 있다. 정보공유분석센터는 각 분야에 특화되어 사고, 위협, 취약점 정보를 전파하는 것 외에도 사고정보를 수집, 분석하여 경보 발령 및 보고를 기본 임무로 가지고 있고 이 외에 각 분야의 위협 식별 및 영향에 대한 연구, 사이버/물리 등 모든 형태의 위협에 관한 정보를 교환, 공유하는 플랫폼의 역할 등을 수행한다.

미국은 2006년 국토안보부에 의해 주요 기반시설 보호 관련 논의에 공동으로 참여하고, 관련 계획 수립 및 지원을 위하여 CIPAC(주요 기반시설 협력 자문위원회, Critical Infrastructure Partnership Advisory Council)도 설립하였다. CIPAC는 의견 간 합의나 연방 정부에 공식 권고안을 제출하는데 필요한 주요 기반시설 관련 문제에 대한 심의 및 자문을 수행하며 정상 상태 및 사고 대응 중 주요 기반시설 보안 및 복구와 관련된 활동에 대한 논의를 진행하기도 한다. 더불어 각 부문 별 세부 문제에 관한 정보를 계획, 조정, 교환을 돕고 NIPP 및 SSP 등 국가적 정책 및 계획 수립, 시행에 참여하기도 한다.

---

42) Communications ISAC (NCC), Electric Sector ISAC (ES-ISAC), Emergency Management and Response ISAC (EMR-ISAC), Financial Services ISAC (FS-ISAC), the National Health ISAC (NH-ISAC),Highway ISAC, Information Technology ISAC (IT-ISAC), Maritime ISAC, Multi-State ISAC (MS-ISAC), Nuclear Energy Institute (NEI), Public Transit ISAC (PT-ISAC), Real Estate ISAC, Research and Education ISAC (REN-ISAC), Supply Chan ISAC (SC-ISAC), Surface Transportation ISAC (ST-ISAC), WaterISAC

43) SACC. 2012. US National ISAC Council Website, (2016.12.02.)

미국은 주요 기반시설 보호 및 복구를 위한 정보 공유를 위한 시스템도 체계적으로 갖추고 있다. NICC and NCCIC(국가 기반시설 협동대응 센터 및 국가 사이버안전 통신 통합센터, National Infrastructure Coordinating Center and National Cybersecurity and Communications Integration Center)는 PDD-21에 의해 설립된 센터로, NICC는 물리적 기반시설, NCCIC는 전자적 기반시설에 관한 보호 업무를 수행한다. NICC는 주요 기반시설 정보를 수집 및 정리하여 전 수준의 의사 결정권자에게 정보를 제공함으로써 정상 상태, 경보 강화 및 사고 대응시 신속하고 정확한 정보를 바탕으로 의사 결정을 가능토록 하며 24시간 정보 공유, 분석 및 사고 대응을 수행하여 정부, 민간 및 국제적 관계에서 정보를 공유하고 대응 및 완화 활동에 참여하여 사고의 영향을 줄이며, 각 부문의 보안 상태 및 사고를 방지하기 위한 전략적·전술적 계획을 수립한다.

감시국(NOC Watch), 첩보국(Intelligence Watch and Warning), 연방재난보호청의 국가감시센터(National Watch Center)와 국가대응협력센터(National Response Coordination Center) 및 국가기반시설 협동대응센터(National Infrastructure Coordinating Center)로 구성된 NOC(국가작전센터, National Operations Center)는 국토안보부의 주요 계획을 담당하고 있다. 국가작전센터는 천재 지변, 테러 행위 또는 기타 인위적인재해 발생 시 연방 정부 및 각 지방자치단체(SLTT)에 재난 상황 모니터링 결과 및 현황을 보고하며, 중대한 테러 및 재난 관련 정보를 정부 의사 결정자에게 전달한다.

마지막으로 FBI의 관리 하에 있는 NCIJTF(National Cyber Investigative Joint Task Force)는 사이버 위협 조사와 관련된 정보를 개발, 공유하고 주요 기반시설에 대한 위협에 대응하기 위해 관련 활동을 조정 및 통합하는 역할을 수행하고 있다. 이를 통해 국토안보부 및 주, 지방, 국제적 기관의 대표가 참여하여 협동 구조를 통해 사이버 위협 상황을 포괄적으로 파악이 가능하다.

이러한 미국의 주요기반시설 보호체계는 다음과 같이 신속한 대응 및 협업을 위한 유기적 구성을 이루고 있다.

[그림 4-2] US National Infrastructure Protection Plan, 2013, 11pg.

3) 주요기반시설 지정 현황

2013년 12월 2일 발표된 '정책지침 21호(PDD-21, Presidential Decision Directive)'는 주요 기반시설의 보안 및 복구에 관한 내용을 다루면서 다음과 같이 미국의 주요 16개 기반 분야를 지정하고 있다[44]. 이는 국가 안보, 통치, 경제적 생명력, 일상생활의 기반이 되는 분야로 매우 정교하고 복잡한 시설(Facilities), 체계(System), 기능(Functions)을 의미하며, 상호의존적으로 함께 작동하는 인적 자산, 물리적 시스템, 사이버 시스템을 포함한다. 미국의 국가기반체계 분류는 2008년에 제철 및 철강 등을 제

44) US National Infrastructure Protection Plan, 2013, 9pg.

조하는 주요 제조업(Critical Manufacturing)을 포함하여 총 16개 분야로 구성되어 있으며, 특히 주요 보호자산의 개념을 도입하여 핵심체계를 위협하지는 않으나 지역적 재난이나 국민의 긍지·신뢰에 손상을 주는 대상물도 지정하여 관리하고 있다[45].

<표 4-3> U.S. Critical Infrastructure Sectors, NIPP, 2013

국가기반체계 분류	세부 보호 대상
화학 (Chemical)	식품 및 농업 (Food and Agriculture)
상업 (Commercial Facilities)	정부 시설 (Government Facilities)
통신 (Communications)	공공 보건 복지 (Healthcare and Public Health)
주요 제조업 (Critical Manufacturing)	정보 기술 (Information Technology)
댐 (Dams)	원자력 발전 및 처리 시설 (Nuclear Reactors, Materials, and Waste)
국방 산업 (Defense Industrial Base)	교통 시스템 (Transportation Systems)
응급 서비스 (Emergency Services)	금융 서비스 (Financial Services)
에너지 (Energy)	수자원 관리 시스템 (Water and Wastewater Systems)

이러한 주요기반분야는 다시 국방, 경제, 안전에 주요한 영향을 미칠 수 있는 시설이나 시스템으로서의 핵심기반 보호대상(CI)과 주요 국가자산 보호대상(KR)으로 구분된다.

<표 4-4> 미국 국토안보부 주요 임무 및 보호대상, 행정안전부, 2009.

구 분	세부 내용
업무	• 생필품 및 필수 서비스 제공(essential goods & services) • 유관기관 협업체계 구축 및 운영(interconnectedness & operability) • 공공 안전 및 보호(public safety & security)

45) 류지협, 임익현, 황의진, “국가기반체계의 통합적 관리 연구”, 한국재난관리표준학회, 2009, 67-72pg.

핵심업무영역	• 정보수집 및 경보(intelligence & warning) • 국경 및 수송체계 보호(border & transprtation security) • 국내 대테러 대책(domestic counter-terrorism) • 핵심 기반시설 및 국가 주요자산 보호(protecting critical infrastructure & key assets) • 재앙적 테러리즘 방어(defending against catastrophic terrorism) • 비상사태 준비 및 대응(emergency preparedness & response)
핵심 기반시설 보호대상(CI)	• 농업・식품(agriculture & food) • 물 및 물처리 시스템(water & water treatment) • 공중보건(public health) • 긴급서비스(emergency services) • 방위산업기초(defense industrial base)
주요 국가자산 보호대상(KR)	• 국가적 유물・유적 및 상징물(national monuments & icons) • 댐(dams) • 정부시설(government facilities) • 상업적 거래시설(commercial facilties)

2. 주요기반시설 보호 관련 법령

1) 미국의 기반보호법제 개관

미국의 기반보호법제는 제정법으로서 국토안보법, 국토안보법 내의 핵심기반정보보호법 및 사이버보안 강화법, 연방정보현대화법(舊 연방정보보호법), 재난 완화법, 사이버보안 연구개발법 등과 행정규칙으로서 기반보호와 관련한 대통령령(Executive Order) 및 국가 안보에 관한 대통령령(Presidential Decision Directives)[46]과 각종 계획 및 전략 등으로 구성된다. 이들은 서로 유기적 관련을 가지며 전반적인 주요 기반시설

46) 국토안보분야의 PDD-63(주요기반보호), HSPD-5(국내사고관리), HSPD-7(주요기반시설 지정, 우선순위 설정 및 보호), HSPD-8(국가재난대비) 등

보호를 위한 법제 체계를 구성한다. 연방정부의 정보시스템 및 정보보호를 위하여 연방 정부의 각 기관들로 하여금 보안프로그램을 개발, 실행토록 하는 연방정보보호법은 NIPP의 부처별 정부시설보호계획(Government Facilities Sector-Specific Plan)과 관련이 있다고 볼 수 있다[47].

2) 국토안보법 (Homeland Security Act of 2002)

국토안보법은 총 17장으로 구성되고 있다 : 국토안보부(제1장), 정보분석과 기반시설보호(제2장), 국토안보지원에서의 과학기술(제3장), 국경교통안전국(제4장), 비상대비와 대응(제5장), 미국과 기타 정부조직들의 군대구성원을 위한 자선기금의 처리(제6장), 운영(제7장), 비연방 실체들과의 조정·감사관·대통령 경호실· 해안경비대· 총칙(제8장), 국토안보회의(제9장), 정보보안(제10장), 법무부 부서(제11장), 항공회사 전쟁위험 보험 법령(제12장), 연방 노동력 개선(제13장), 테러대응을 위한 항공기 조종사의 무장(제14장), 전환(제15장), 항공교통안전과 관련된 기존 법률(제16장), 관련 규정 및 기술적 개정(제17장).

이 중 정보분석과 기반시설보호(Information Analysis and Infrastructure Protection)를 다루고 있는 제2장은 다음과 같이 구성된다.

- 제1절은 정보분석기반시설보호국(Subtitle A - Directorate for Information Analysis and Infrastructure Protection: Access to Information)을 규정한 제201조와 정보에 대한 접근을 규정한 제 202조로 규정
- 제2절은 주요기반시설정보(Subtitle B - Critical Infrastructure Information)에 관하여 제211조부터 제215조까지 5개의 조문으로 구성

- 제211조는 요약 제목이고, 제212조는 정의, 제213조는 주요기반시설 보호프로그램을 지정하고, 자발적으로 공유된 주요기반시설정보보호를 규정한 제214조, 조치에 대한 사권은 없다는 내용을 규정한 제215조로 구성됨

- 제3절은 정보보안(Subtitle C - Information Security)에 관한 내용을 규정하고 있으며, 제221조부터 제225조까지 5개 조문으로 구성

- 제221조는 정보공유절차, 제222조는 프라이버시 책임자, 제223조는 비연방 사이버보안 강화, 제224조는 Net guard, 제225조는 사이버보안 강화법(Cyber Security

47) 한국인터넷진흥원, "미국, 영국, 독일의 기반보호법 체계에 관한 연구", 2010, 21pg.

Enhancement Act of 2002)을 규정하고 있음

- 제4절은 과학기술실(Subtitle D – Office of Science and Technology)에 관하여 규정하고 있으며, 제231조부터 제237조까지 7개의 조문으로 구성

- 제231조는 과학기술실의 설립과 과학기술실장, 제232조는 과학기술실의 임무와 의무, 제233조는 법집행기술의 정의, 제234조는 미국 법무연구소 과학기술실의 폐지, 직무의 이관, 제235조는 국가법집행 및 교정기술센터, 제236조는 법무부 내 기타 실체들과의 조정, 제237조는 미국법무연구소와 관련된 개정을 다루고 있음

특히 국토안보법은 그 내용에 핵심기반 정보보호법(Critical Infrastructure Information Act 섹션 211~)과 사이버보안 강화법(Cyber Security Enhancement Act 섹션 225~)를 포함하여 아래와 같은 내용들을 정하고 있다. 핵심기반 정보보호법[48]은 주요기반정보(Critical Infrastructure Information)을 '일반적으로 공중에 존재하지 않으며 중요기반 또는 보호 대상 시스템의 안전과 관련 있는 정보'로 정의하는데, 이는 주요 기반시설에 대한 실제적인, 잠재적인 또는 위협적인 피해를 주는 것으로서 연방, 주, 지방법을 위반하거나 서로 다른 주간의 상업적 교류를 해치거나 또는 공중 보건과 안전을 위협하는 것에 관한 정보이다. 또한 보안시험, 위험평가, 위험관리계획, 위험감사 등과 같은 주요기반 또는 보호대상시스템에 대해 계획되거나 이미 시험, 예측되었거나 취약성 평가 등 주요기반 또는 보호시스템에 대한 방해, 약화, 또는 무기력화에 대항하는 능력에 관한 정보와 방해, 약화, 무력화에 대응하는 수리, 회복, 재건설, 보험 또는 지속성 등 주요기반시설 또는 그 보호시스템에 관해 계획되거나 과거의 운영상 문제점 및 해결책에 관한 정보를 포함한다.

보호시스템이란, 어떠한 서비스, 물리적 또는 전자적 시스템, 과정 및 절차로서 직간접적으로 주요기반시설의 기능 실행에 영향을 주는 것으로, 물리적 또는 전자적 시스템으로서 컴퓨터와 컴퓨터 시스템, 통신망 또는 하드웨어나 소프트웨어, 진행 지침 및 전송, 저장 중에 있는 정보를 포함한다[49]. 또한 자발적으로 제공되는 중요기반정보에

48) 6 U.S.C. §131-134

49) The term "protected system"- (A) means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure; and (B) includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage, Critical Infrastructure Information Act, 6 U.S.C. §131 (6)(B), 2002.

대한 보호 규정을 명시하여 정보 제공자의 보호를 위한 장치를 두고 있다[50].

사이버보안 강화법[51]은 프라이버시 보호, 양형위원회에 대해 컴퓨터 범죄에 대한 세밀한 기준 작성 및 강화된 형벌을 적용하도록 하고 있다. 사이버공격자가 고의 또는 과실로 법률을 위반하여 심각한 신체적 상해를 기도하거나 유발하는 경우 20년 이하의 징역 또는 벌금을 부과하며 사람의 생명 및 신체에 대한 위협이 수반되는 긴급 상황의 경우 인터넷서비스사업자(ISP)가 연방, 주 또는 지방 정부기관에 정보를 지체없이 공개할 수 있도록 규정한다. 비상시 ISP는 통신내용 및 관련 기록을 법집행기관에 제공하도록 명시하고 있어, 비상상황 발생시 정부기관은 ISP에 관련 내용의 제공을 요구할 수 있고[52], 사이버보안 전략 연구 및 개발, 연방 사이버 장학금, 사이버안보 산학협동 TF, NIST의 사이버안보 연구 개발 등 연구 개발 및 지원과 사이버안보 근로자 평가, 사이버안보 기술 표준 향상, 국제 표준 협력, 사이버안보 인식 제고 및 교육 등 전반적으로 연구 개발 및 표준/기준 수립에 관한 내용도 포함하고 있다.

3) 연방정보보호법 (Federal Information Security Management Act of 2002)[53]

2002년 제정된 연방정보보호법(FISMA)은 연방 정부의 운용을 지원하는 주요 정보자원을 관리하는 종합적 틀을 제공하고, 고도로 네트워크화된 연방의 정보환경을 인식, 국가안보 관련기관과 법집행기관 전반의 정보보안 활동을 관리, 조정 및 감독하는 기능을 법제화한 것이다. 연방정부 관련 정보보안활동의 관리, 감독권은 국토안보부에 부여하고 있다. 연방정보 및 정보시스템의 보안강화를 위한 관련 지침 및 표준을 개발, 제정하는 국립기술표준원(NIST)을 설립하고, 연방정보 보안의 기능을 담당하도록 하고 있으며, NIST는 연방 정보 및 정보시스템의 보호를 위한 필요 최소한의 통제장치 개발, 유지, 연방 기관의 정보보호 프로그램 감독 및 개선을 위한 메커니즘을 제공한다. 연방정보보호법은 민간 분야 정보 보호를 위해 민간에서 개발한 하드웨어 및 소프트웨어 등을 각 연방정부 기관이 선택, 사용하도록 인정하고 있기도 하다.

2014년 12월 연방정보보호법은 연방정보현대화법(Federal Information Security Modernization Act of 2014)로 개정되어 다음과 같은 내용을 포함하게 되었다. 국토안보부(DHS) 장관에게 관리예산처(OMB) 국장을 지원하도록 권한을 부여하여 연방정부의

50) 한국인터넷진흥원, “미국, 영국, 독일의 기반보호법 체계에 관한 연구”, 2010, 30pg.
51) 6 U.S.C. §145
52) 정준현, 지성우, “국가안전보장을 위한 미국의 반사이버테러법제에 관한 연구: 애국자법과 국토안보법을 중심으로”, 미국헌법연구 제20권 제2호, 2009, 232-233pg.
53) 2014년 12월 연방정보보호현대화법(Federal Information Security Modernization Act of 2014)로 개정되었으나, 일반적인 내용을 정리하고, 개정된 부분을 소개한다.

정보시스템에 대한 기관의 정보보호 활동 이행을 관리할 수 있도록 하였고, 국토안보부(DHS) 장관은 국립표준기술연구소(NIST)의 자문을 통해 정부기관 관계자들과 회의를 소집하여 정보보안을 위한 정부차원의 노력을 협의하고 관계 기관의 운영 및 기술지원을 제공하여야 할 뿐만 아니라 관리예산처(OMB) 국장에 의해 개발된 정책, 표준, 가이드를 구현한 기관들의 운영지침[54]을 감독하여야 한다. 또한 연방정부기관의 매년 의회에 기관보고 시 기존의 주요정책 및 회계정보뿐만 아니라 보안요구사항과 위협, 보안사고, 규정준수에 관한 세부사항까지 보고하도록 의무가 확대되었다.

관리예산처(OMB) 국장은 정부기관의 보고사항에 적용되는 주요 사고가 무엇인지에 대한 가이드를 제공하여야 하며 국토안보부(DHS) 장관과 협의하여 연방정부기관의 정보보호 정책과 활동의 효과를 매년 의회에 보고하도록 해야 한다. 연방정부기관은 데이터 침해 통지 정책과 지침을 정기적으로 업데이트 하여야 하며 침해사고 발생 시 연방정부기관은 신속하게 의회에 통지를 하여야 하며, 통지는 침해사고를 발견한 날로부터 30일을 넘을 수 없으며 통지내용에는 침해사고에 대한 정보를 반드시 포함하여야 한다. 관리예산처(OMB) 국장은 FISMA 제정일로부터 1년 이내에 관리예산규칙(Budget Circular A-130)[55]를 개정하도록 하여 비효율적이거나 낭비예산 보고를 없애고 연방정부기관의 정보보호 담당자가 정보시스템의 보호를 위해 더 많은 자원을 할당할 수 있도록 해야 한다. 회계감사원장은 기관장들과 감사관들이 직무를 다할 수 있도록 기술적 지원을 제공하도록 하고 연방정보보안사고센터(the Federal Information Security Incident Center)에서는 기관을 지원하기 위해 사이버 위협, 취약점, 보안사고에 대한 정보를 제공을 위한 기능 업데이트 수행해야 한다.

4) 재난 구제와 비상지원법 (Robert T. Stafford Disaster Relief and Emergency Assistance Act of 1988)

미국은 1988년 재난구호법(Disaster Relief Act)을 확대하고, 개정한 법으로 재난 원조에 필요한 자원을 확보하고 있으며 주와 지방정부, 그리고 지역 주민들의 재난에 대한 지원을 주목적으로 한다.

재난 구제와 비상지원법은 대규모 재난 발생으로 주정부나 지방정부의 응급대처능력으로 대응이 어려울 경우 주정부와 지방정부는 연방정부에 지원을 요청할 수 있고, 연

54) 운영지침(Binding operational directives) : 정보 보안 위협, 취약성 또는 위험으로부터 연방 정보와 정보시스템을 보호할 목적으로 FISMA 2014에서 정의된 강제사항

55) 1996년 클린저 코헨 법(the Clinger-Cohen Act)에 따른 연방정부 자원의 관리를 위한 정책이며 2000년 마지막으로 업데이트됨

방정부는 재난 복구를 위해 필요한 자원을 지원한다. 또한 대통령은 대규모 재난 발생 시 비상사태를 선포할 수 있으며, 각급 정부, 일정 요건을 갖춘 NGO 등에 대하여 연방기관들이 지원할 수 있는 계획을 수립할 수 있다.

5) 재난 완화법 (Disaster Mitigation Act of 2000)

2000년 미국은 재난 예방과 재난으로 인한 피해 감소를 목표로 주정부와 지방정부의 책임을 강화하는 것을 목적으로 재난 구제와 비상지원법을 개정한 재난 완화법을 제정하였다. 이 법을 근거로 연방은 재난 예방과 재난 경감 기금에 대한 계획을 수립할 수 있으며, 수립된 계획을 기반으로 재난 발생 전과 후에 자금 지원이 가능해져 재난 예방의 효과를 높일 수 있었다. 특히 지방정부에게 재난 예방에 대한 노력을 강조하여, 지방정부가 연방으로부터 재난구호기금을 받기 위해서는 재난 예방 계획을 수립하도록 명시하고 있고, 이러한 계획 수립에 있어 엄격한 가이드라인을 제시하고, 주정부, 지방정부, 지역정부는 이를 의무적으로 따라야 하며, 연방재난청(FEMA)은 이런 가이드라인에 따라 수립된 지역의 예방 계획을 검토하고 승인하는 역할을 수행하도록 하였다.

6) 사이버보안 연구개발법

미국 사이버보안 연구개발법은 연방 의회가 사이버 보안 분야의 연구 및 개발에 대하여 5년 동안 약 9억 3백만 달러를 사용할 수 있도록 규정하고 있다[56]. 국립과학재단(NSF)과 국가기술표준원(NIST)이 해당 예산을 사용하는데 협력할 수 있어, 컴퓨터와 사이버 보안에 관한 연구와 교육에 지원이 가능하며 연구 개발 및 운영 절차, 심사 절차를 구체적으로 규정함과 동시에 민간연구기관 등 구체적 지원대상과 지원프로그램 내용도 명시하고 있다.

7) 기타 대통령령

1998년 PDD(Presidential Decision Directive)-63을 통해 주요기반시설에 대한 범정부적 보호체계를 마련하였으며, 국가 주요기반 보호를 위한 전략 개발이 연방 정부를 중심으로 이루어지기 시작하였다. 2001년 9.11 테러 이후 행정명령 제13231호는 PDD-63

56) Brock Read, "House Votes to Authorize Greater Spending on Computer-Security Research", *Chron, of Higher Educ,* Nov. 29, 2002, 29pg.

을 대부분 계승하여 주요기반시설에 대한 사이버상 위협에 초점을 맞추게 되었다.

HSPD(Homeland Security Presidential Directive)는 특정한 프로그램과 활동을 위한 국가 정책과 행정의무 사항을 제시하고 있는 지침이다. 최초에 발행된 것은 911 직후 국토안보 자문위원단을 구성하기 위한 것으로 시작하여 테러 공격으로부터 미국을 보호하여 피해를 최소화하기 위한 조치들을 포함한 내용들이 여러 차례 발행되고 있다. HSPD-3는 국토안보자문시스템(Homeland Security Advisory System)에 관한 내용으로서 연방, 주, 지방, 지역 정부 그리고 미국 국민들에게 테러공격에 대한 정보를 퍼뜨리기 위한 의무사항 제시하고 있다. HSPD-5는 국내사고관리(Management of Domestic Incidents)에 관한 내용으로서 국내 사태 관리에 대한 국가적 접근을 다루고 있으며, HSPD-7은 기반시설 보호에 관한 가장 중요한 국가안보대통령령으로서 기반 보호 미션에 초점을 두고 HSPD-7을 통해 각각의 분리된 권한 근거와 국가안보에 관한 대통령령들이 국가적 접근방법의 각 부분으로 결속되어 있으며, 해당 령을 통해 NIPP의 개발을 의무화하고 있다. 특히 HSPD-7은 2003년 12월 발행되어 국가 기반 보호를 강화하는 미국 정책을 수립하였으며, 이를 통해 국토안보부, SSA, 기타 연방부처와 기관, 주, 지방, 부족, 영역 정부, 지역 파트너, 민간 및 다른 기반 보호 파트너와의 역할과 책임을 정하고 있다는 점에 의의가 있다고 할 수 있다. HSPD-8은 국가준비태세(National Preparedness)에 관한 내용으로서 테러공격, 국가적 재난 등에 필요한 적정 대비체제를 확보하는데 초점을 두고 있다. 기타 HSPD-9는 농업 및 식량(Defense of the United States Agriculture and Food)에 관한 내용이고, HSPD-10은 생물학적 방어(Biodefense for the 21st Century), HSPD-19는 테러범의 폭발물과의 전투(Combating Terrorist Use of Explosives in the United States), HSPD-20은 국가 지속 정책(National Continuity Policy), HSPD-22는 국내 화학 방어(Domestic Chemical Defense)를 내용으로 하고 있다.

3. 안전관리 관점의 법률 분류[57)]

1) 예방 단계

- 안전관리 기구 및 조직 구성

「애국자법(Patriot Act)」(42 U.S.C. §5195)

미국 애국자법은 거시적 시각에서 기반보호의 중요성과 정책방향을 정하고 있는데, 동법은 분석기관으로 국가기반시설 시뮬레이션·분석센터를 두어 국가기반시설의 예기치 못한 위험의 시사점, 재난 발생 시 예상 반응 등을 도출하도록 규정되어 있다.

「연방정보현대화법(FISMA of 2014)」(44 U.S.C. §3556)

연방정보현대화법(FISMA of 2014)은 연방정보보안사고대응센터(Federal Information Security Incident Center)를 통해 기관들의 정보시스템이 보안 사고에 대하여 탐지하고 관리할 수 있도록 기술적 지원의 수행을 규정하고 있다.

「국토안보법(Homeland Security Act)」(6 U.S.C. §144)

국토안보법(Homeland Security Act)에 따라 미국은 지역전문가를 활용하여 지역사회 정보시스템 및 전기통신망 공격 대응을 전문적으로 지원하는 조직을 구성하도록 규정되어 있다.

- 안전관리 체계 마련

「국토안보법」(6 U.S.C. §112)

국토안보법에 따라 국토안보부장관은 주 및 지방 정부 조정실을 통해 주 정부 및 지방 정부, 민간 기관과의 적절한 계획, 준비, 훈련 및 연습 활동, 국토안보와 관련된 통신 및 통신 시스템, 경고 및 정보의 배포를 조정하고, 특별보좌관의 도움을 받아 민간 부문 주요기반시설 보호를 위한 실행방법을 개발, 촉진하여야 한다.

57) 개별 조항이 안전관리 단계에 해당되는 법률들이 있어 앞서 정리한 미국의 기반보호시설 보호 관련 법률에 포함되지 아니한 법률이 일부 포함됨

「사이버보안 연구개발법(The Cyber Security Research and Development Act)」

(44 U.S.C. §3543)

사이버보안 연구개발법(The Cyber Security Research and Development Act)에 따라 백악관 예산관리처(OMB)는 정보보안 표준·지침을 개발하고 그 시행을 감독하도록 규정되어 있다.

「사이버보안 연구개발법」(15 U.S.C. §7408)

사이버보안 연구개발법에 따라 연구개발에 관한 법률을 별도로 제정하게 하며, 사이버보안 연구개발법에서 연구 지원 방안, 프로그램 운영 절차 및 심사절차를 구체적으로 정하도록 규정하고 있다.

「전자정부법(E-Government Act)」(15 U.S.C. §278g-3)

전자정부법(E-Government Act)에 따라 미국은 탐지에 관하여 무엇을 개발하여 지원하는지 그 대상을 명시하여, 국가표준기술원(NIST)이 탐지지침을 포함한 정보시스템 표준, 지침, 관련 방법, 기법을 개발하도록 정하고 있다.

「전자정부법」(44 U.S.C. §3546)

전자정부법은 국가보안시스템 운영·통제기관과 연방정보보안사고센터간 정보공유를 별도로 명시하여 국가보안시스템의 특성에 맞는 적정한 정보공유를 법제화하고 있다.

- 안전점검 및 안전 조치

「애국자법」(42 U.S.C. §5195)

애국자법은 기반시설의 구성 시스템에 모델링·시뮬레이션·분석을 통해 예기치 못한 위험의 시사점, 재난 발생 시 예상 반응 등을 도출하여 국가기반시설에 대한 안전점검을 하도록 되어 있다.

「사이버보안 연구개발법」(44 U.S.C. §3545)

사이버보안 연구개발법(The Cyber Security Research and Development Act)에 따라

각 연방기관은 매년 소관 기관의 정보보안 프로그램 및 실무에 대해 프로그램과 실무의 효과를 판단하기 위해 독자적 평가를 수행하고, 해당 결과를 매년 예산관리처장에게 제출하며, 중앙정보국(CIA) 및 국방부가 통제하는 시스템에 대한 평가는 별도 의회의 소관 위원회에만 제출하도록 되어있다.

「전자정부법」(44 U.S.C. §3544)

전자정부법에 따라 각 연방기관은 소관 업무 및 자산을 지원하는 정보 및 정보시스템의 무단접속, 사용, 공개, 방해, 수정 또는 파괴로 인해 야기될 수 있는 위해의 위험과 규모를 주기적으로 평가해야 한다.

「국토안보법」(6 U.S.C. §182)

국토안보법에 따라 국토안보부 과학기술담당차관은 테러리스트 공격 탐지 관련 기술 및 시스템 평가 역할을 담당하도록 명시하고 있다.

- 안전관련 산업의 육성과 안전문화 활동 지원

「국토안보법」(6 U.S.C. §182)

국토안보법에 따라 국토안보부 과학기술담당차관은 테러리스트 공격 탐지 관련 기술 및 시스템의 연구·개발 역할을 담당하도록 명시하고 있다.

2) 대비 단계

「애국자법」(42 U.S.C. §5195)

미국은 애국자법을 통해 거시적 시각에서 기반보호의 중요성과 정책방향을 고려하여 모든 상황에서 연방정부의 본질적 기능을 지속시킬 수 있는 종합적이고 효과적인 계획을 수립하도록 하고 있다.

「국토안보법」(6 U.S.C. §121)

국토안보법에 따라 국토안보부의 정보분석 및 기반보호 담당차관은 주요 기반시설을 안전하게 하기 위한 포괄적 국가 계획을 수립하도록 하고 있다. 그러한 국가 계획의 보호대상은 전력 생산, 발전 및 배전 시스템, 정보 기술 및 전기통신시스템, 전자 재정

및 재산 기록 저장소, 비상 대비 통신 시스템 및 기타 물리적 자산, 기술적 자산을 포함한 미국의 핵심 자원으로 규정하고 있다.

「국토안보법」(6 U.S.C. §121)

국토안보법은 주요 기반시설 보호를 위한 국가 계획에서 나아가 국토안보부 정보분석 담당차관과 기반보호 담당차관은 핵심자원 및 주요 기반시설을 보호하기 위한 대책을 수립하는 것을 권고하고 있다.

「연방정보현대화법」(44 U.S.C. §3554)

연방정보현대화법은 연방 기관의 책무 중 하나로 보안 사고에 대한 탐지, 대응, 복구 방안을 설명하는 내용을 포함한 연간 보고서를 제출하도록 하고 있다.

- 안전관리 능력 향상

「국토안보법」(6 U.S.C. §112)

국토안보법에 따라 국토안보부장관은 주 및 지방 정부 조정실을 통해 주 정부 및 지방 정부, 민간 기관과의 적절한 준비, 훈련 및 연습 활동을 수행하여야 한다.

3) 대응 단계

- 대응 체계 구축・운영

「정보개혁 및 테러예방에 관한 법률(Intelligence Reform and Terrorism Prevention Act of 2004)」(TITLE IV - TRANSPORTATION SECURITY)

정보개혁 및 테러예방에 관한 법률(Intelligence Reform and Terrorism Prevention Act of 2004)은 교통, 운송 보안에 관한 장(TITLE IV - TRANSPORTATION SECURITY)에서 대응 및 복구를 위한 책임과 관련 이슈들을 정리한 국가전략을 수립하도록 규정하고 있다.

「국토안보법」(6 U.S.C. §133)

국토안보법은 국가기반시설 경보의 경우 반드시 정부가 직접 주도하여 전파할 수 있

는 체계를 구축하도록 명시하고 있다.

「국토안보법」 TITLE V - EMERGENCY PREPAREDNESSE AND RESPONSE

(6 U.S.C. §144)

국토안보법의 제5장은 '비상대비와 대응' 에 관한 내용을 규정하고 있다. 해당 장은 비상대비대응 차관 및 차관의 책무, 핵사고 대응, 보건관련 활동들의 수행, 비상 대응 시 국가의 민간분야망 이용에 관한 규정, 사용기술, 재화 및 서비스의 이용에 관한 내용을 규정하고 있다.

- 응급조치

「정보개혁 및 테러예방에 관한 법률」(TITLE IV - TRANSPORTATION SECURITY)

정보개혁 및 테러예방에 관한 법률은 국가테러대응위원회의 보고서에 민간 및 공공분야의 긴급 구조, 작업의 복구 등에 관한 내용을 포함하도록 하고 있다.

- 대응 활동

「정보개혁 및 테러예방에 관한 법률」(TITLE IV - TRANSPORTATION SECURITY)

정보개혁 및 테러예방에 관한 법률은 미국에 대한 테러 발생 시 사후 대응, 소관 기관의 책임과 의무 등을 규정하고 있다.

4) 복구 단계

- 수습 본부 설치·운영

「재난 완화법(Disaster Mitigation Act)」(42 U.S.C. §5172)

재난 완화법(Disaster Mitigation Act)은 연방 정부로 하여금 미국민에게 재난 관련 복구를 위한 재정적 지원을 수행하도록 규정하고 있다.

- 복구 계획 수립

「정보개혁 및 테러예방에 관한 법률」(TITLE IV - TRANSPORTATION SECURITY)

정보개혁 및 테러예방에 관한 법률은 전반적으로 미국에 대한 테러 발생 시 세부적인 복구 절차 마련 방안에 대한 포괄적인 규정을 명시하고 있다.

「국토안보법」(6 U.S.C. §422)

국토안보법에서는 테러리즘이나 핵, 생물학, 화학, 또는 방사능 공격으로부터의 방어 또는 복구를 위한 조달을 규정하고 있다.

5. 법제 분류 결과 및 시사점

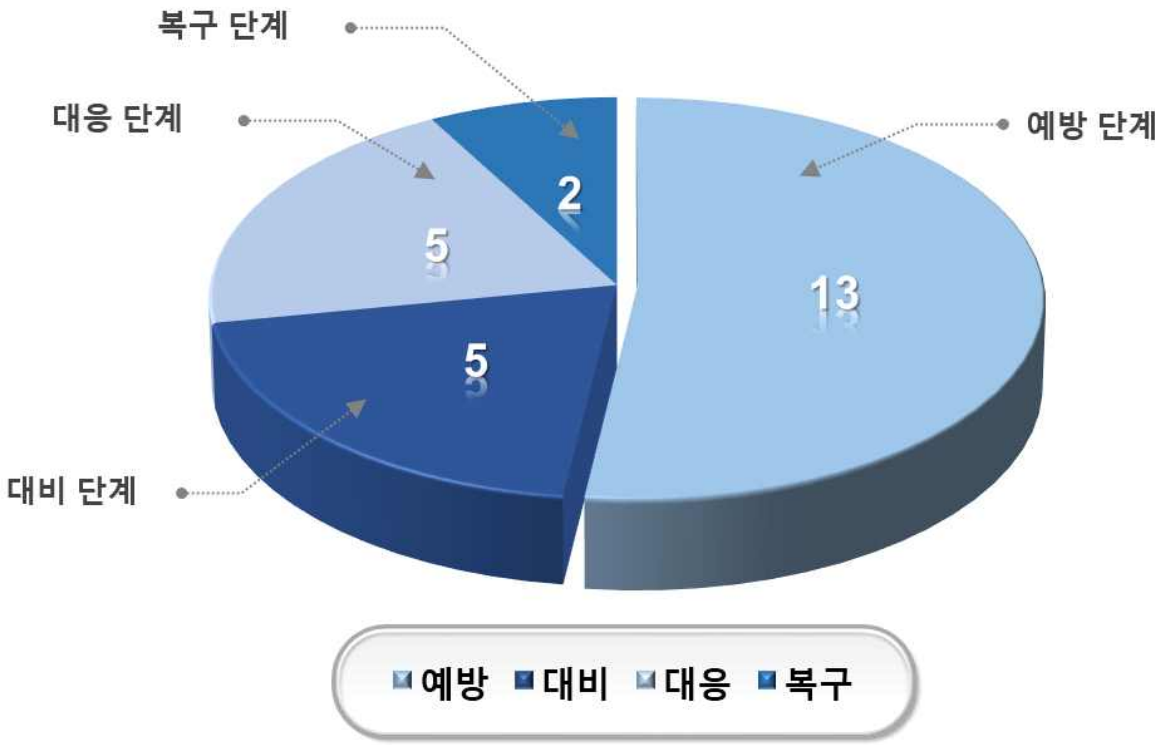
〈표 4-5〉 안전관리 관점에서의 미국의 주요기반시설 보호 법제 분류 결과

안전관리 단계	세부 활동 영역	미국 주요기반시설 보호 법제 법률 조항	내용
예방 단계	안전관리 기구 및 조직 구성	「애국자법」 (42 U.S.C. §5195)	• 국가기반시설 시뮬레이션·분석 센터 구축
		「연방정보현대화법」 (44 U.S.C. §3556)	• 연방정보보안사고대응센터 구축
		「국토안보법」 (6 U.S.C. §144)	• 지역사회 정보시스템 및 전기통신망 공격 대응을 전문 지원하는 조직 구성
	안전관리 체계 마련	「국토안보법」 (6 U.S.C. §112)	• 민간부문 주요기반시설 보호를 위한 실행방법의 개발·촉진
		「사이버보안 연구개발법」 (44 U.S.C. §3543)	• 정보보안 표준·지침을 개발하고 그 시행을 감독
		「사이버보안 연구개발법」 (15 U.S.C. §7408)	• 사이버보안 관련 연구 지원 및 프로그램 운영 절차, 심사절차 마련
		「전자정부법」 (15 U.S.C. §278g-3)	• 정보시스템의 표준, 지침, 관련 방법, 기법 개발 요구
		「전자정부법」 (44 U.S.C. §3546)	• 국가보안시스템 운영·통제기관과 연방 정보보안사고센터간 정보 공유 법제화
	안전점검 및 안전 조치	「국토안보법」 (6 U.S.C. §192)	• 주요기반 취약성 감소를 위해 배치된 시스템의 유효성 분석·모델링·시뮬레이션 실시
		「사이버보안 연구개발법」 (44 U.S.C. §3545)	• 정보보안 프로그램 및 실무에 대한 독자적 평가 수행

		「전자정부법」 (44 U.S.C. §3544)	• 소관 업무 및 자산을 지원하는 정보 및 정보시스템에 야기될 수 있는 위해 및 위험 규모를 주기적으로 평가
		「국토안보법」 (6 U.S.C. §182)	• 공격 탐지 관련 기술 시스템의 평가 역할 부여
	안전관련 산업의 육성과 안전문화 활동 지원	「국토안보법」 (6 U.S.C. §182)	• 공격 탐지 관련 기술 시스템의 연구·개발 역할 부여
대비 단계	안전관리 계획 수립	「애국자법」 (42 U.S.C. §5195)	• 연방정부의 본질적 기능을 유지시킬 수 있는 계획 수립
		「국토안보법」 (6 U.S.C. §121)	• 주요기반시설을 안전하게 보호하기 위한 포괄적 국가 계획 수립
		「국토안보법」 (6 U.S.C. §121)	• 핵심자원 및 주요기반시설을 보호하기 위한 대책 수립 권고
		「연방정보현대화법」 (44 U.S.C. §3556)	• 보안 사고에 대한 탐지, 대응, 복구 방안을 포함하는 연간 보고서 제출
	안전관리 능력 향상	「국토안보법」 (6 U.S.C. §112)	• 민간부문 주요기반시설 보호를 위한 훈련 및 연습 활동 수행
대응 단계	대응 체계 구축·운영	「정보개혁 및 테러예방에 관한 법률」(TITLE IV)	• 대응 및 복구를 위한 책임과 관련된 이슈들을 정리한 국가 전략을 수립하도록 규정
		「국토안보법」 (6 U.S.C. §133)	• 정부는 기반시설에 위험이 발생할 시 경보 체계를 발동
		「국토안보법」 (6 U.S.C. §144)	• 비상 대응 시 국가의 민간망 이용 가능
	응급조치	「정보개혁 및 테러예방에 관한 법률」(TITLE IV)	• 민간 및 공공 분야의 긴급구조, 작업 복구에 관한 내용 규정
	대응 활동	「정보개혁 및 테러예방에 관한 법률」(TITLE IV)	• 테러 발생 시 사후 대응 방안을 포괄적으로 규정
복구 단계	수습 본부 설치·운영	「재난완화법」 (42 U.S.C. §5172)	• 연방 정부로 하여금 미국민에게 재난 관련 복구를 위한 재정적 지원을 수행하도록 규정
	복구 계획 수립	「정보개혁 및 테러예방에 관한 법률」 (TITLE IV)	• 테러 발생 시 복구 절차를 포괄적으로 규정
		「국토안보법」 (6 U.S.C. §422)	• 테러리즘, 핵, 생물학, 화학 또는 방사능 공격으로부터의 복구를 위한 조달 규정
	원인 조사	-	-

미국은 국가중요기반시설 보호에 있어 분야마다, 목적마다, 사안마다 다양한 법률을 통해 규율하고 있기 때문에 다양한 법률을 망라적으로 분석하여 분류하는 작업이 필요하였다. 미국 주요기반시설 보호 법제의 안전 관련 법률 조항들을 안전관리 관점의 분류 기준으로 분류한 결과, 예방 단계는 안전관리 기구 및 조직 구성 활동 3개 조항, 안전관리 체계 마련 활동 3개 조항, 안전점검 및 안전조치 활동 4개 조항, 안전 관련 산업의 육성과 안전문화 활동 지원 1개 조항으로 가장 많은 수의 조항인 총 13개 조항에 걸쳐 규율하고 있었다. 대비 단계에서는 안전관리 계획 수립 활동과 관련된 4개 조항, 안전 관리 능력 향상 활동 1개 조항으로 총 5개 조항이 존재하였다. 대응 단계는 대응 체계 구축·운영 활동 3개 조항, 응급 조치 활동 1개 조항, 대응 활동 1개 조항으로 총 5개로 분석되었으며, 복구 단계는 수습 본부 설치·운영 활동 1개 조항, 복구 계획 수립 활동 2개 조항으로 분석되었다. 이를 그래프로 나타내면 다음과 같다.

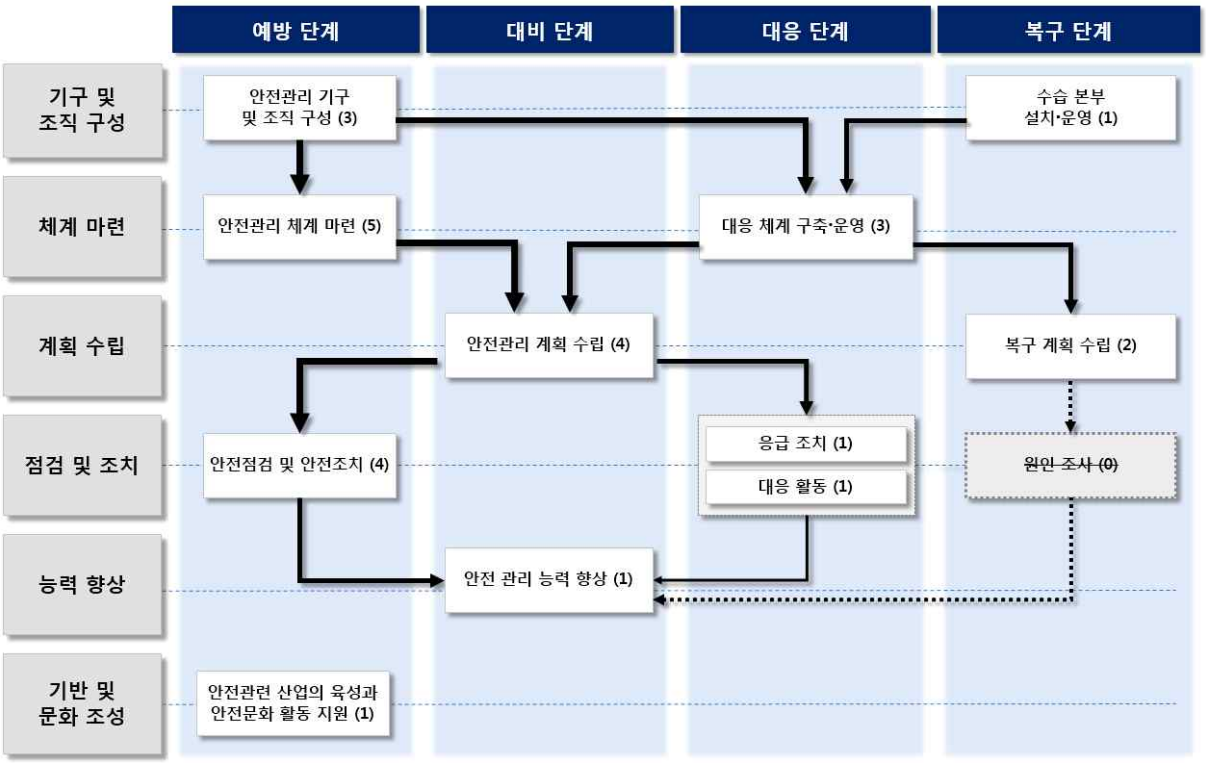
[그림 4-3] 미국 주요기반시설 보호 법제의 안전 관리 단계별 조항 개수 (단위:개)



미국은 자연적으로 일어난 재난이나 전자적 침해로 인한 피해보다는 주로 적들의 테러로부터 발생한 사고에 대한 안전 관리에 초점을 맞춘 법률이 많았다. 또한 실제 발생한 Case가 많기 때문에 국가 계획과 법률에서는 추상적인 역할 부여와 원칙 위주

로 기술되어 있고, 실질적으로는 가이드라인을 통하여 실행력의 신속성을 확보하고 있는 것으로 보인다. 또한 원자력, 교통 수송, 에너지, 금융 분야 등 각 분야별로 연구되고 있는 계획, 표준화 작업 등 선진화된 부분이 많기에 미국의 각 분야별 주요기반시설 안전관리 규율 체계를 추가적으로 검토하고 참고할 필요성이 있을 것이다.

[그림 4-4] 미국 주요기반시설 보호 법제의 안전관리 관점의 세부 분류 단계별 활동 흐름도



예방 및 대비 단계에 법률 조항이 치중되어 있는 우리나라와 비교해서, 미국은 4단계의 안전 관리 단계에 법률 조항들이 비교적 골고루 분포되어 있었다. 물론 법률 조항의 수 자체는 예방 단계가 확실히 많았지만, 실제 재난이나 테러 사건을 많이 겪은 국가인 만큼, 우리나라에는 비교적 미비하게 갖추어져 있는 대응 및 복구 단계에 대하여 세세한 절차와 대응 거버넌스 등이 더욱 체계적으로 갖추어져 있었다. 특히 SW의 안전에 대한 사안은 모든 안전 관리 단계에 대한 체계를 망라적으로 다루고 있는 국토안보법 중 핵심기반 정보보호법(Critical Infrastructure Information Act 섹션 211~)과 사이버보안 강화법(Cyber Security Enhancement Act 섹션 225~)을 집중적으로 참고할 필요가 있을 것으로 생각된다.

제2절 영국의 주요기반시설 법령 분석

1. 영국 주요기반시설 보호 법제 개관

1) 개요

영국은 유럽 안에서도 안전규제에 관한 이슈에 대해 가장 민감한 국가 중 하나이며, 규제완화 움직임 속에서도 안전과 관련한 각종 규제가 지속적으로 신설되고, 체계적으로 관리가 이루어지고 있다[58].

영국의 안전규제는 위험물안전규제, 산업안전규제, 식품안전규제 전자장비안전규제, 가스설비안전규제, 승강기안전규제, 원자력규제, 설비공급안전규제, 가스사용 및 저장안전규제와 같은 주요시설 및 시설물에 대한 안전규제 뿐만 아니라 장난감안전규제부터 가구안전규제까지 위험이 발생할 가능성이 있는 대부분의 사안에 대해서 법률로 규정하고 있다[59]. 각 규제의 대상 및 집행권한은 사안에 따라 각기 다른 관련 부처에 소관을 두고 있으며, 이들 모두를 통합적으로 관리하는 부처나 기관은 없는 상황이다.

하지만, 산업안전분야의 규제사안에 대해서는 보건안전청(HSE)에서 통합적으로 관리[60]하고 있으며 원자력과 관련한 안전규제에 관해서도 별도의 기구를 설치하여 규제권한을 부여하고 있다. 이처럼, 사안의 삼각성 및 사고 위험성과 관련한 측면에서 각별한 주의를 요하는 분야에 한해서 특별관리가 행해지고 있는 것이다. 특별관리가 필요한 시설 및 시설물에는 국가의 중요기반시설도 포함되어있으며, 영국의 경우 중요국가기반시설(Critical National Infrastructure: CNI)이 국가존속에 매우 중요하다는 인식하에 여 타 시설과는 별도로 지정하여 관리하고 있다. CNI에 문제가 발생하는 경우 경제적 측면뿐만 아니라 사회전체의 측면에서 큰 혼란을 초래하기 때문에 이들을 별도로 지정하여 관리하는 것은 중요한 의미를 갖는다고 볼 수 있다.

중요국가기반시설에 대한 보호는 2000년대 초반까지 주로 정보기관의 역할로 인식되어왔고, 민간영역에서는 그나마 1999년 12월 20일에 설립된 국가기반보호조정센터(National Infrastructure Security Co-ordination Centre: NISCC)에서 관련 업무를 담당해왔다. NISCC는 주요국가기반시설 보호를 위한 기구로서 민간 부문에 속한 주요국가기반시설 조직들뿐만 아니라 정부부처 안에 있는 기존의 기반보호 관련 업무들을 통합

58) 권영빈, 영국의 사회적 안전규제, 2014년 2/4분기 국내외 규제 동향지, 2014, 25-34
59) https://www.gov.uk/
60) http://www.hse.gov.uk/aboutus/inthepublicinterest/

및 조정하고, 정부부처간의 조율을 담당하는 기능을 갖는 센터로서 활약하였다.

중요국가기반시설에 대한 보다 효과적인 보호와 관리를 위해 영국은 NISCC와 MI5에 소속되어있던 국가보안권고센터(National Security Advice Centre: NSAC)를 통합하여 모든 범위를 아우르는 범정부기구인 국가기반시설 보호센터(Centre for the Protection of National Infrastructure: CPNI)를 설립하였다. 특히 영국 정부는 기반시설 보호가 사이버 공간에서의 보안문제와 긴밀하게 연계되어있음을 인식하고, 최근 일어나고 있는 사이버 공간에서의 보안문제에 대해 심각성반영하여 2015 국가 안보 전략 (The 2015 National Security Strategy: NSS)을 통해 사이버 위협이 영국의 이익에 가장 큰 위험 중 하나라는 것을 재확인하였다.

NSS는 사이버 위협에 대처하고 사이버 보안 분야에 있어서 전 세계에서 우위를 점하기 위한 영국 정부의 결정을 발표하였고, 그 약속을 이행하기 위해 2016 년 11 월 1 일 2016-2021 국가 사이버 보안 전략을 발표하였다. 이 전략의 핵심이 되는 기관으로 영국정보통신본부(Government Communications Headquarters:GCHQ)산하에 국가 사이버 보안 센터(National Cyber Security Centre: NCSC)를 신설하였다. 특히 NCSC는 CPNI와의 협력관계를 구축하고 있으며, 중요국가기반시설의 정보통신 네트워크, 데이터 및 시스템의 보호와 같은 사이버영역에 관한 보안을 담당하도록 하였다.

2) 주요기반시설 보호체계

영국의 주요기반시설 보호 체계는 크게 정보기관에 의한 보호 체계와 정부 및 민간부문에 의한 보호체계로 나뉘어진다.

- MI5

영국의 국가정보기구(intelligence machinery)의 구성은 내각사무처의 중앙정보기구(central intelligence machinery based in the Cabinet Office), MI6, 정보통신본부(GCHQ), MI5, 국방정보국(DIS) 및 통합테러분석센터(JTAC)로 이루어진다. 위 의 기관은 각각의 특화 된 분야로 나뉘어 활동하며 정보통신기반시설을 포한한 중요국가기반시설에 대한 보호와 관련한 업무는 MI5가 수행하도록 되어있다. 이러한 MI5는1989년 보안서비스법이 제정되면서 중요기반시설보호와 관련한 핵심기구로서 그 역할과 책임을 명확히 하고, 중요기반시설보호와 관련한 업무 및 활동에 대한 법적 근거를 얻게 되면서 영국의 중요기반시설 보호 체계를 확립하는 계기가 되었다.

보안서비스법은 간첩활동이나 테러 및 국가체계를 위협하는 활동 등으로부터 영국의 안전 보호를 목적으로 하는 MI5의 기능을 규정한다. MI5는 기반보호와 관련해 국가기관에 대한 보안대책을 담당하며, 2000년대 테러법에서 정의한 테러에 대한 대응, 첩보대책 등 과 같은 주요기반시설 보호와 관련한 다양한 역할을 수행한다.

- CPNI

MI5에의한 중요기반시설 보호와는 별개로 민간 영역에서의 국가중요기반시설보호에 관해서는 2007년에 기존의 민간영역 기반보호역할을 담당하였던 NISCC와 MI5에 소속되었있던 NSAC를 통합하여 CPNI를 설립하였으며, CPNI는 모든 민간 영역의 중요기반시설 보안업무를 총괄 담당한다. 이는 기존의 MI5가 담당해 왔던 민간영역의 기반보호 업무를 CPNI에게 귀속시켜 국가안보영역과 민간영역을 분리시킨 것으로, 중요기반시설의 많은 부분이 민간에서 운영하고 있다는 점을 상기하면 영국 내의 중요기반시설 보호에 있어서 가장 중요한 역할을 하고 있는 것은 CPNI라고 할 수 있다.

CPNI는 국가기반시설을 운영하는 민간 기업 및 조직에 대한 보안관련 자문 제공하고 있으며, 각 개별 공공기관과 밀접한 관계를 맺고 있다. 특히 중요국가기반시설의 보전을 위한 테러공격에 취약한 요소들을 사전에 점검하고 대비하는 것에 중점을 두고 있다. 또한 경찰조직과도 밀접한 관련성을 가지고 있고, 특히 '경찰 대테러안전국(National Counter Terrorism Security Office(NaCTSO)'과 긴밀한 파트너십을 형성하여 CPNI가 중요기반시설에 대한 적절한 어드바이스를 행하는데 많은 도움을 주고 있다. CPNI에서 다루는 국가 기반이란 국가가 올바르게 기능하고 국민들의 일상 생활에 많은 부분 의존하는 필수불가결한 시설, 시스템, 사이트, 정보, 사람, 네트워크 및 프로세스를 말하며, 또한 의존도에 있어서 필수적 요소는 부족하지만 민간영역에서의 핵이나 화학분야처럼 공공의 잠재적 위험요소가 높기 때문에 보호가 필요한 분야를 국가 기반으로서 지정하고 있다.

영국에는 총 13개의 국가 기반 분야(화학, 핵, 통신, 국방, 응급서비스, 에너지, 금융, 식품, 정부, 건강, 우주, 운송, 물)가 있으며 응급서비스 분야의 경우 세부적으로 경찰, 구급차, 소방서 그리고 해안 경비대로 나눌 수 있다. 위의 각 부문에는 해당 부문을 책임지는 하나 이상의 소관부처(Lead Government Department: LGD)가 있으며, 중요기반시설에 대한 안전을 보장하고 있는 것이다. 하지만 13가지의 국가 인프라 분야가 모두 중요국가기반시설(CNI)에 포함되는 것은 아니며, CNI에 대한 영국 정부의 공식 정의는 국가 인프라(시설, 시스템, 부지, 재산, 정보, 인력, 네트워크 및 프로세스)의 중요

한 요소인 필수 서비스의 가용성, 전달성 혹은 무결성에 큰 악영향을 미쳐 결과적으로 심한 경제적 손실 또는 생명의 상실이라는 심각한 사회적 결과를 초래하는 분야를 말한다. 이러한 관점에서 CPNI는 영국의 중요국가기반시설을 13개의 국가 기반 분야에서 화학, 핵, 국방, 우주를 뺀 9개의 분야로 정의하고 있다[61].

<표 4-6> 영국의 중요국가기반시설 및 소관부처

부문		세부분야	소관부처
통신		데이터통신, 음성통신, 메일, 공공정보, 무선통신	상업기술규제개혁부 (Department for Business, Innovation and Skills)
응급 서비스	경찰	구조 및 치안	내무부 (Home Office)
	구급차		보건부 (Department of Health)
	화재		지역사회정부부 (Department for Communities and Local Government)
	해안경비		교통부 (Department for Transport)
에너지		전력, 가스, 석유	에너지기후관리부 (Department for Energy and Climate Change)
금융		자산관리, 금융시설, 투자은행, 주식거래소, 소매은행	재무부 (HM Treasury)
식량		생산, 수입, 가공초리, 배송, 소매	환경농촌식품 및 식품인증처 (Department for the Environment, Food & Rural Affairs and Food Standards Agency)
정부		청사, 지역 및 지방정부, 의회 및 사법, 국가안보	내각부 (Cabinet Office)
보건		건강관리, 공중위생	보건부 (Department of Health)

61) 영국의 국가 중요기반시설 범위 설정의 기준은 국민들의 일상생활에서 높은 의존도를 갖는 기본적 서비스 공급 및 국가의 기능을 유지하기 위해 필요한 시설, 시스템, 사이트, 네트워크를 말함

교통	항공, 해상, 철도, 도로	수송부 (Department for Transport)
물	식수, 하수	환경농촌식품부 (Department for the Environment, Food & Rural Affairs)

CPNI는 물리적공격(physical attack), 내부공격(insider attacks), 전자적 공격(electronic attacks)의 세 가지 측면에서 기반시설보호에 대비하고 있으며, 특히 최근 정보통신기술의 발달과 사이버 공격기술의 진보에 따른 전자적 공격의 증가에 대비하기위해 각별한 주의를 줌과 동시에 사이버범죄 및 사이버보안과 관련한 기관과의 긴밀한 연계가 이루어지고 있다. 이러한 사이버범죄 및 사이버안보와 연계관된 기관으로는 CPNI의 소관부처인 내무부 산하기관인 국가범죄수사국(NCA)이 있다. 내무부는 테러범죄 및 반사회적 위험으로부터 사회를 지키며, 주요 기반시설의 보호와 입국관리, 테러대응, 경찰 통솔 등을 담당하고 있는 정부부처로서 국가범죄수사국(NCA)과 CPNI를 통해 영국에서 발생하는 주요 사이버범죄와 주요기반시설 대상의 물리적, 전자적 공격으로부터 보호 업무를 담당하고 있다. 또한 내각부에서는 정부의 목표 달성을 위해 총리를 지원하는 핵심적인 역할을 담당하는 기관으로 내각의 업무를 지원하고 정부 내 각 부처 간의 연계와 정책 시행을 위해 노력하고 있는 정부부처[62]들이 있고, 사이버보안과 관련해서는 정보보증중앙지원기구(CSIA), 사이버보안청 (OCSIA), 민간비상대비사무처(CSS) 등과 연계되어 있으며 최근에는 국가사이버보안센터(NCSC)와의 긴밀한 관계구축으로 기반시설에 관한 사이버 보안에 노력하고 있다.

- NCSC

2015 국가 안보 전략 (The 2015 National Security Strategy: NSS)을 바탕으로 2016년 10월 설립한 국가사이버보안센터(National Cyber Security Centre: NCSC)의 주요 목적은 사이버 공간의 안전성을 개선하여 영국에 대한 사이버 보안 위험을 줄이는 것이며, 영국의 각 기관, 기업 및 개인과 협력하여 정확하며 일관된 사이버 보안 자문의 제공을 통해 사이버 안전을 관리를 담당하고 있다.

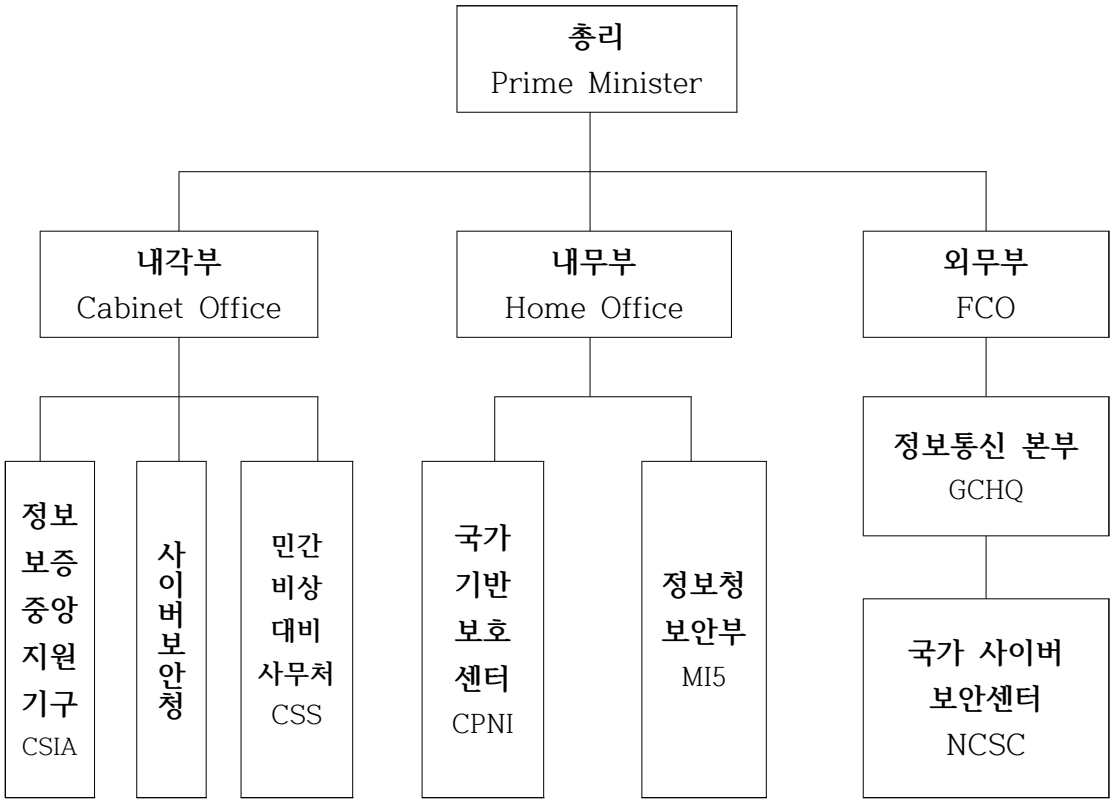
NCSC는 IT 및 온라인상에서의 민원 서비스와 같은 공공 부문에서의 사이버 보안에

62) https://www.cpni.gov.uk

관한 조언, 지침 및 지원을 제공에 중점을 두고 있으며 여기에는 중앙 및 지방 정부, 보건 및 사회 복지, 응급 서비스 등이 포함된다. NCSC가 영국의 모든 공공 기관과 직접적인 관계를 맺을 수 없으므로 특히 위험이 높은 네트워크, 시스템 및 서비스에 대한 맞춤식 지원과 각 기관이 이러한 지원에 접근하기 용이하도록 돕고 있는 상황이다.

NCSC의 업무 대상은 크게 3부류로 나뉘는데, 공공분야(The public), 단체(Organisations), 정부 및 중요국가기반시설(Government and the Critical National Infrastructure)이 이에 해당한다. 특히 중요국가기반시설 보호에 있어서 물리적, 인적 보안문제에 앞장서고 있는 CPNI와 함께 외부공격 및 내부사고로부터의 복구에 힘쓰고 있으며 주요 네트워크 기반을 소유하고 운영하는 조직, 관련 주요 정부 부처, 규제 기관 및 정책 결정자등 과 긴밀히 협력하고 있다. 또한 위에서 나열한 중요국가기반시설을 소유 및 운영하는 자들에게 보안 위험을 관리하는 데 필요한 물적, 인적 지원을 수행한다. NCSC가 중요국가기반시설에 제공하는 서비스는 주로 해당 분야의 특정 요구사항을 충족시키기 위해 조정되지만, 일반적인 지침의 대부분은 중요국가기반시설(CNI)전반에 관련이 있는 위협 정보 및 사고 관리 지침과 관련이 있다[63].

<표 4-7> 영국의 기반시설 보호 체계



63) https://www.ncsc.gov.uk

3) 기반시설 안전규제 제도

영국은 자연적 혹은 인위적으로 발생 가능한 위험이 존재하는 사안에 대해 안전규제를 도입하고 각 규제의 대상 및 집행권한은 사안에 따라 각기 다른 부처가 담당하고 있다. 특히 CPNI에서 중요국가기반시설 보호를 총괄하고 있지만, CPNI의 역할은 각 기관 및 사업자에게 조언과 가이드라인을 제공하는 수준이며 결국 영국에서 중요국가기반시설의 안전과 관련하여 실질적인 업무를 담당하는 것은 각 중요국가기반시설 부문의 소관부처라고 할 수 있을 것이다. 따라서 산업보건안전법이 비록 직접적으로 중요국가기반시설의 보호를 명시하고 있지는 않지만 각 중요국가기반시설의 관리자가 산업보건안전법에 의거한 안전규정을 따르는 경우가 일반적이다.

산업안전보건규제는 고용연금부(Department for Work and Pentions, DWP)가 1974년 제정된 산업안전보건법(Health and Safety at work etc Act, HSWA)에 의거 별도로 보건안전청(Health and Safety Executive, HSE)을 설립하는 등 다른 안전관련 규제와는 달리 좀 더 체계화하여 구축한 제도이다. 산업안전보건규제의 핵심 기구라고 할 수 있는 보건안전청(HSE)은 산업현장에서 노동자의 산재, 사망, 질병 등 사고위험을 예방하기 위한 감시, 규제, 캠페인 등의 활동과 노동자의 건강, 복지를 증진시키기 위한 제반 활동을 실시하고 있으며, 일부 중요국가기반시설에서의 안전을 보장하기위해 활동하고 있다.

<표 4-8> 영국 보건안전청의 활동 내용

보건안전청의 활동 내용
1. 산업보건안전의 증진을 위한 기준 마련
2. 기준의 집행
3. 연구수행 및 자문
4. 질의 응답 및 정보제공

2. 주요기반시설 보호 관련 법령

1) 보안서비스법

보안서비스법은 상술한바와 같이 1989년에 제정되어 MI5(Security Service)의 역할과 책임을 정하였으며, 이에 따라 MI5가 최초로 법적기반을 얻게 됨과 동시에 MI5의 기능을 국가의 안전, 특히 외국의 첩보기관에 의한 간첩활동이나 테러 및 민주정치체계를

위협하는 활동 등으로부터 영국의 안전을 보호하는 것으로 규정하고 있으며, 이러한 업무를 내무부 장관(the Secretary of State)의 책임 하에 실시할 것을 규정하고 있다.

동 법의 주요 내용으로 MI5의 역할을 국가의 안전보호에 두고 있으며, 구체적으로 1장에서는 '국가의 안전을 보호하는 것, 특히 첩보활동(espionage), 테러활동 및 사보타주로부터의 위협, 외국세력의 에이전트활동으로부터의 위협 및 정치적, 산업적 또는 폭력적 수단에 의한 의회민주주의의 전복이나 약체화를 위한 활동의 위협으로부터 국가의 안전을 보호하는 것'을 MI5의 주요 목표로 정하고 있다. 또한 이러한 목표를 달성하기 위해 수행해야 할 구체적인 목표로는 (i) 테러 시도의 억지, (ii) 외국의 첩보활동 및 기타 은밀한 활동으로 부터 영국의 손해 예방, (iii) 확산국이 대량파괴무기에 연관되는 물질, 기술, 전문지식을 조달의 억지, (iv) 새로운 위협과 재발할 수 있는 위협의 감시, (v) 정부의 취약한 정보 및 자산과 함께 중요한 국가기반시설의 보호, (vi) MI6 및 GCHQ가 법령에서 정하고 있는 기능수행의 지원 및 (vii) MI5의 능력 강화 등으로 정하고 있다[64].

보안서비스법이 중요한 의미를 갖는 이유는 중요국가기반시설의 보호와 직접적으로 관련 있는 법이기 때문이며, 동 법은 MI5뿐만 아니라 현재 영국의 중요국가기반시설의 전반적인 보호를 담당하고 있는 CPNI의 설립에 법적 근거를 부여하고 있다.

2) 2000년대 테러 관련 법

2000년 영국은 이미 기존의 대 테러 관련 법률을 개정하고 다양한 형태의 테러 행위에 적용 가능한 법률을 제정하지만, 2001년 미국에서 발생한 9.11테러 이후 이슬람 과격파의 테러대상에 영국이 포함된다는 지적이 등장함에 따라 영국의 테러 대응 및 기반시설 보호 강화에 대한 움직임이 일어났다. 2001년 반테러, 범죄 및 안전보장법(Anti-Terrorism, Crime and Security Act 2001)은 테러에 관한 기본법으로 테러 위기에 대처하기 위한 정부 및 기관의 권한을 효과적으로 발휘 할 수 있도록 다양한 테러 대책 방안을 포함하였으며 특히 항공기, 생화학 물질, 핵 과 관련한 주요시설 및 설비에 대한 보다 엄격한 규제체계 구축과 안전 규정을 마련하였다.

2005년 테러방지법(Prevention of Terrorism Act 2005)은 2001년 반테러, 범죄 및 안전에 관한 법률을 개선한 것으로 동 법은 내무대신에게 테러혐의자에 대한 규제명령을 내릴 수 있는 권한을 부여하고 있으며, 테러 관련행위에 직간접적인 연관 혐의를

64) 미영독 기반보호법제 연구, 188면.

받는 자에 대한 규제명령에 영국인도 포함시키고 있다.

2006년 테러법(Terrorism Act 2006)은 2005년 7월 발생한 런던 자살테러 사건을 계기로 새로운 유형의 테러에 대응하기 위한 개정으로 만들어진 법이며, 동 법에서는 (1) 방사능 물질 등의 장치나 재료를 만들거나 소유하는 행위, (2)장치나 재료를 오용하거나 시설에 손상을 입히는 행위, (3)장치나 물질 또는 시설과 관련한 위협을 하는 테러 행위, (4)핵시설 등에 대한 침입 등 주요기반시설과 연관된 형사 범죄 유형이 추가되었다.

3) 산업보건안전법

산업보건안전법에는 중요국가기반시설에 대한 보호가 직접적으로 명시되어있지는 않지만 영국의 중요국가기반시설로 지정되어 있는 교통분야, 보건분야, 식량분야, 에너지분야 등에 대한 안전규제를 정하고 각 분야의 사업자가 이러한 안전규제를 따르고 있다는 점에서 산업보건안전법에 의거한 규제들은 중요국가기반시설 보호와 관련 있다고 할 수 있다.

1960년대 및 70년대 초에 재해율이 급증하고 폭발 등으로 인한 대형재해가 빈발하였지만 안전·보건관계법이 5개 부처와 9개 감독기관에서 일관성 없이 집행됨으로서 관계기관간의 업무의 경계가 모호하고 감독기능이 중복되었으며, 일부 분야에 대해서는 지방정부의 전문성 결여로 인한 문제가 다발적으로 발생하였다. 이에 따라 각 부처에 산재되어 있는 안전·보건관계법 중 유사 감독기능을 종합하여 일원화된 강력한 행정력을 발휘하고, 효율적인 안전보건정책 수행 및 중복규제를 없애기 위해 1970년 특별위원회(Robens Committee)의 보고서에 따라 안전보건 관계법령을 통합하여 1974년에 작업장보건안전법(Health and Safety at Work etc. Act)을 제정하였다. 이것은 보건안전법 제정 이전의 특정분야, 특정위험에 적용하는 대부분의 법에 대해 일정부분은 계속해서 그 효력을 유지하되 점차 하나의 법으로 통합하고 세부사항은 기술관련 시행령(Regulation)이나 지침(Guide)으로 정하고, 단일화된 감독기구를 통하여 집행하도록 한 것이다. 보건안전법 적용 대상으로는 영국내의 근로자, 자영업자 및 공공주민을 포함 모든 사람 및 제조업, 학교, 병원, 철도, 광산 등 위험이 높은 대부분의 업종에 적용하고 있다. 보건안전법 적용 특별 제외 대상으로는 원자력, 일반차량에 의한 교통안전, 서비스업종 및 군시설 등 특별한 분야이거나 위험이 적은 업종만 제외하되 필요한 경우 이들 업무분야와도 협조체계를 유지하고 있다(특히, 원자력에 관해서는 The Ionising Radiations Regulations, Nuclear Material (Offences) Act, The Nuclear

Generating Stations (Security) Regulations 등 별도의 법률을 통해 안전규제를 시행하고 있음). 또한 사업장에서 배출하는 유해물질로부터 환경오염을 방지하도록 하여, 이 법의 적용을 받는 사업장은 약 174만개소, 근로자수는 약 2,320만명으로 확대되었고, 사업장을 출입하는 일반인도 보호대상에 포함하고 있다[65].

보건안전위원회(Health and Safety Commission : HSC)는 1974년 보건안전법의 제정을 계기로 설립된 정부기관으로 국무대신이 HSC의 위원장 및 HSC의 위원을 임명한다. HSC의 구성은 총 9명으로 근로자대표(노동조합연합) 3인, 사용자대표(영국 산업연맹) 3인, 그리고 중앙부처 대표 1, 지방자치단체 대표 1인, 소비자 단체 대표 1인으로 구성된다. HSC의 임무는 정책집행 우선순위 결정등 위원회 및 보건안전청(HSE)의 업무 총괄[66], 안전보건관련 연구 및 조사 수행, 정보 및 자문제공, 유해위험물질 관리, 산업보건의에게 자문을 제공하고 근로자의 건강관리를 담당하는 근로자 보건자문센타(Employment Medical Advisory Service) 운영, 안전보건에 관한 규칙 제정, 안전보건법령 심사위원회 활동(※ HSC의 업무영역에서 소비자 안전 및 식품안전, 해상 및 항공안전, 대기오염은 제외), 안전보건정책 결정, 중장기 계획 수립 및 연간 사업계획을 작성 등이 있다.

보건안전청 (Health and safety Executive : HSE)은 영국의 보건안전법(HSWA)을 집행하는 독립된 정부기구로 1974년에 제정된 보건안전법에 의해 각 부처의 안전보건업무를 통합하여 1975년에 설립되었고, 노동연금부(DWP) 소속이지만 보건안전위원회(HSC)만의 감독을 받으며, 노동연금부는 단순히 의회에 대한 창구역할을 수행한다. HSE의 기능은 HSC에서 결정된 정책에 따라 안전보건법의 내용을 적용하기 위한 감독 및 연구, 산업안전보건 정책개발을 담당하는 것이며, 더불어 새로운 형태의 위험에 대응하기 위한 안전보건 법규·기준의 제정, 안전보건관련 법규, EU 법규, 지침 등의 집행 그리고 전반적인 국민의 안전보건에 대한 감독 조사 및 개선을 수행하는 것을 주 업무로 한다[67].

4) 비상대비 시민보호법

영국의 경우 재난안전 관리가 초기단계부터 지방자치단체가 주관하며 미국과 같이 강력한 정부 조직이 담당하고 있지 않고, 재난관리에 관한 법이나 제도 역시 민방위법

65) 노동부, 주요선진국의 산업안전보건분야에 있어서 노사참여 및 협력 제도와 운영에 관한 연구 - 영국, 독일, 프랑스, 스웨덴을 중심으로, 2003, 123면
66) HSWA 1974, 2(7)
67) 주요선진국의 산업안전보건분야에 있어서 노사참여 및 협력 제도와 운영에 관한 연구, 124-125면

을 바탕으로 발전해왔고, 비상대비 체계는 1920년에 제정되어 현재 2004년에 개정된 비상대비 시민보호법(Civil Ctingencies Act 2004)을 기본법으로 운용되고 있다[68].

비상대비법 제1조는 비상사태의 아래의 의미들을 정의하고 있다.

(a) 영국 내의 어디에서든지 인간 복지에 심각한 피해를 줄 수 있는 사건 또는 상황(인간의 생명에 대한 손실, 질병 및 상해, 주거소실, 재산피해, 재화 물 에너지 또는 연료의 공급 중단, 통신체계의 붕괴, 교통 및 운송시설의 붕괴, 보건서비스의 중단 등[69])

(b) 영국의 내의 어디에서든지 환경에 심각한 피해를 줄 수 있는 사건이나 상황(생물학적, 화학적 또는 방사능 물질로 인한 공기, 수중, 토양 오염, 동식물 생태계의 파괴 등)

(c) 영국의 안보에 심각한 피해를 줄 우려가 있는 전쟁 또는 테러

이처럼 비상대비법에서 지정하고 있는 비상사태란, CPNI에서 담당하는 중요국가기반시설(CNI)의 내용을 포함하고 있으며, 국가위기에서의 기반시설 보호 관련법이라 할 수 있을 것이다.

비상대비법은 크게 1,2부로 나뉘며 1부에서는 비상대응 및 비상대비와 관련한 지방차원에서의 시민보호 관련법규를, 2부에서는 1920년 비상대응권에 관한 법을 개정하여 새롭게 비상대응권을 규정하고 있다. 지방차원에서의 비상대응 처리기관은 제1차 및 제2차 대응처리기관(재난안전 책임기관)으로 구분이 되나 이 두 기관 모두 지방경찰의 행정관할구역에 기반을 둔 지방복구대책위원회(Local Resilience Forums)를 구성하면서 위기상황에 대응하고 있다. 특히, 비상대비법의 부칙에는 중요국가기반시설인 응급서비스, 보건, 시설물(전력, 가스와 같은 에너지 관련 시설물), 교통 및 수송의 정의와 관련 책임관리 기관을 명시하여 국가 기반시설 보호의 중요성을 담고 있다. 또한 비상대비법 시행령으로는 산업기반시설에 대한 위기재난 관리규정(Control of Major Accident Hazards Regulations, COMAH), 송유관안전규정(Pipelines Safety Regulations), 방사능 사고대비 주민홍보규정(Radiation Emergency Preparation and Public Information Regulations, REPPIR) 등 다양한 규정이 있으며, 국가중요기반시설보호와 관련한 시행령이 포함되어 있다.

---

68) 한국지방자치학회, "주요 국가의 재난 및 위기 안전관리 체계 연구," (서울: 행정안전부, 2008. 12.), p. 89.
69) 추가 설명을 위해 주요기반시설에 해당하는 교통, 보건, 에너지 등에 대해 부칙에서 연관 법을 나열하고 있음

3. 안전관리 관점의 법률 조항 검토

영국의 기반시설 보호관련 법은 미국처럼 상세히 규정하고 있지 않으며, 주로 책임기관이 수립한 계획을 통해 개별적으로 수행되고 있기 때문에 세세한 법률 조항을 통해서는 구체적인 체계와 활동내용을 자세히 파악하기가 힘든 측면이 있다. 따라서 비상대비법에 의거한 비상대비 체계와 국가의 안전관점에서 이루어지는 계획과 원칙 위주로 영국의 예방, 대비, 대응 및 복구 활동들을 우선 망라적으로 서술한 뒤, 본 연구에서 제시한 분류 기준에 해당하는 활동들로 세분화 시켜보도록 하겠다.

안전이라는 관점에서 영국은 비상대비법(Civil Contingencies Act)에 의거하여 크게 비상예방대비 계획(Emergency Planning)체계와 비상대응 및 복구 계획(Contingency Planning) 체계로 나누어 재난 및 국가위기로부터 국가의 안전을 지키기 위해 노력하고 있다. 비상대비 계획은 비상사태에 대비하기 위한 위험성평가(risk assessment), 업무지속관리계획(business continuity)을 근간으로 업무를 수행하며, 비상대응 복구계획은 비상대비법에 근거하여 제1차 위기재난 책임기관이 중앙정부수준, 지역수준, 기초정부수준으로 비상 복구 계획을 수립하고 시행한다.

영국의 통합비상관리(Integrated emergency management, IEM)체계는 주로 예견(anticipation), 평가(assessment), 예방(prevention), 대비(preparation), 대응(response), 복구(recovery)의 6개 분야로 활동을 구분하고 있다. 본 연구의 분류 기준에 적용한다면 영국의 예견(anticipation), 평가(assessment), 예방(prevention) 분야는 예방 단계로 분류할 수 있을 것이고, 대비(preparation), 대응(response), 복구(recovery) 활동은 각각 대비 단계, 대응 단계, 복구 단계에 해당한다고 볼 수 있다.

영국의 안전 관리에 관한 계획은 크게 일반비상계획과 특별비상계획으로 구성되어 있다. 일반비상계획은 위기재난 발생에 대하여 재난관리책임기관으로 하여금 가능한 넓은 범위의 시나리오에서 위기재난과 관련하여 기능을 담당하고 있기 때문에 일반적으로 대부분의 유형에서 동일하게 일어날 수 있는 유형의 위기재난에 대비하고 있다. 또한 일반비상계획의 각 요소는 비상사태의 성격에 따라 선택적으로 취합하여 상황에 맞게 활용되며, 때에 따라 특별 비상계획을 뒷받침하는 역할을 수행한다. 일반비상계획의 주요 프레임워크로는 조직 전반에 걸친 인식 제고, 조직 내에서의 훈련과 위기상황 연습과 비상사태에 대비할 수 있는 충분한 인력 및 자원의 확보를 주 내용으로 삼고 있다.

특별비상계획은 재난관리책임기관이 일반비상계획 및 지원 능력이 해당 위기에 적절

한지 판단하고 일반비상계획으로는 적절하지 않다고 판단될 시, 특별비상 계획을 적용하도록 되어있다. 특별비상계획은 특정 상황에 대해 일반비상계획보다 상세하게 기술되어 있으며, 구체적인 절차를 계획하여 특정상황이나 시나리오와 연관된 조직들 간의 유기적이고 통합적인 응급대응을 하는 것을 목적으로 한다. 또한 특정상황에 알맞은 구체적인 훈련과 위기상황 연습을 계획하여 대중에게 특정상황에 대비하기 위해 필요한 정보를 제공하고자 한다.

비상대비법의 시행 프로그램 제 6장에 명시된 업무지속관리 계획(Business Continuity Management)은 비상사태 시 각 기관들의 업무가 중단되지 않고 지속할 수 있도록 관리하는 계획으로, 국민들의 일상생활이 파괴되지 않도록 하기 위한 재난 초기 대응 계획의 일부이다. 이는 비상대비법에 의거하여 재난관리책임기관이 계획하여 시행하고 있다.

재난 및 위기는 그 종류나 방식이 시대적 배경에 따라 다른 형태를 취하기 때문에 비상대비계획이 한번 수립되고 끝나는 것이 아니라 계속해서 위험성을 평가하고 개선해야한다. 이에 따라 영국의 재난안전 관리의 핵심이자 실질적인 역할을 담당하는 지방정부는 매년 각 지방의 위험성 평가를 실시하고 개선점을 강구하고 있다.

비상대비계획이 완전함을 갖추기 위해서는 반드시 훈련과 연습이 동반되어야하며, 특히 비상계획이 실제 현실에서는 효과가 없는 탁상공론의 계획은 아닌지 테스트하는 계획을 수립되어야 한다. 이에 영국은 가장 신속하게 비상사태에 대비해야 할 지방정부가 시민에 대한 비상사태 선포 및 관련정보의 제공을 수행할 수 있도록 훈련하고 있으며, 특히 소방공무원의 교육훈련을 위한 소방대학(Fire Service College)과 긴급사태계획대학(Emergency Planning College)의 교육기관을 통해 고도의 지식과 기술을 연마하고 있다.

영국의 비상대응 및 복구계획은 크게 중앙정부 수준의 비상대응복구계획과 지역수준의 비상대응복구 계획으로 나뉠 수 있다. 중앙정부 수준의 비상대응복구계획인 정부의 비상대응 복구계획은 주로 화학 및 방사능 등에 대한 긴급대처, 전염병과 같은 광범위한 위기에 대한 대응, 신속한 긴급 경보 발령 및 위기 정보 제공 등 지방정부 수준에서 대처하기 힘든 광범위하고 위험성이 매우 높은 사안에 대한 대응 및 복구 계획을 수립하고 전국적인 업무를 수행하고 있다. 반면 지역수준의 비상대응복구 계획은 지역단위에서 주로 재난관리책임기관과 긴급구조기관, 중앙정부 상호간의 협력조정 역할을 중심으로 임무를 수행하고 있으며, 잉글랜드 지역(총 9개 지역)을 기반으로 지역비상대응위원회와, 지역복구팀이 수립하고 시행하는 지역일반대응계획, 중앙정부의 지방통

합행정청이 수립하고 시행하는 업무지속관리 계획, 그리고 각 지역의 비상대응복구계획과 지역기반의 비상대비 역량 등을 고려하여 작성하는 지역역량조정계획 등으로 운영하고 있다[70]. 특히, 수도 런던의 경우 중요성을 감안하여, 내각실 산하에 별도로 런던시 재난복구팀을 운영하고 있으며, 런던시장, 런던경찰청, 런던 교통경찰국, 런던 소방청이 유기적으로 담당 업무를 수행 그밖에도 비상사태 대비 인력 및 물자 동원 계획과 소요 물자 비축 계획을 실시하고 있다[71].

4. 법제 분류 결과 및 시사점

위와 같이 크게 비상대비법에 의거하여 구성된 영국의 비상대비 체계와 안전 관리 활동 계획들에 대하여 본 연구에서 제시한 분류 기준인 예방, 대비, 대응, 복구 단계로 세분화하여 분류한 결과는 <표 4-9>과 같다.

<표 4-9> 안전관리 관점에서의 영국의 주요기반시설 보호 법제 분류 결과

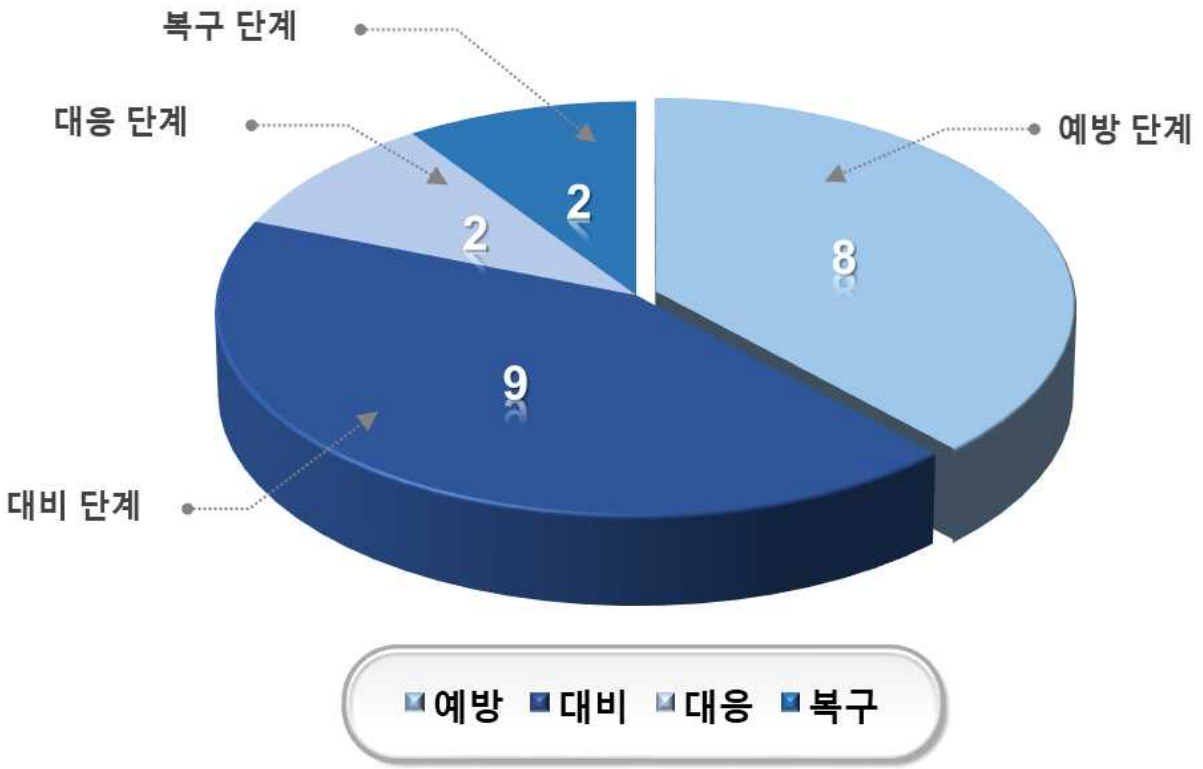
안전관리 단계	세부 활동 영역	영국 주요기반시설 보호 법제 법률 조항
예방 단계	안전관리 기구 및 조직 구성	• 재난관리 책임기관 지정
		• 긴급구조기관 지정
		• 지역비상대응위원회 구성
		• 지역복구팀 구성
	안전관리 체계 마련	• 특정 비상상황에 대비하기 위해 필요한 정보 공유·제공 체계 마련
	안전점검 및 안전 조치	• 위험성 평가 실시
		• 평가 결과에 따른 개선점 강구
	안전관련 산업의 육성과 안전문화 활동 지원	• 비상사태에 대비할 수 있는 충분한 인력 및 자원의 확보

70) 이재은, "재난환경 변화에 따른 과학적 재해관리체계 강화를 위한 법제 연구 - 영국, 독일편", 한국법제연구원, 글로벌 법제전략 연구 12-22-④-3, 2012, 42-70면.
71) 비상대비 소요물자 비축 계획은 우리나라처럼 상세하게 규정되어 있지는 않다.

대비 단계	안전관리 계획 수립	• 일반 비상계획 수립
		• 특별 비상계획 수립
		• 업무지속관리 계획(BCM) 수립
		• 지역일반대응계획 수립
		• 지역역량조정계획 운영
	안전관리 능력 향상	• 조직 전반에 걸친 안전관리 인식 제고
		• 조직 내 훈련 및 위기상황 연습
		• 테스트플랜 구축 및 훈련 계획 수립
		• 소방대학과 긴급사태계획대학의 인재 육성 및 교육 훈련
대응 단계	대응 체계 구축・운영	• 비상사태 시 정부의 비상사태 선포 및 관련 정보 제공 수행
		• 비상사태 대비 인력 및 물자 동원 계획 실시
		• 비상사태 시 소요 물자 비축 계획 실시
	응급조치	• 특정 상황이나 시나리오와 연관된 조직들 간의 유기적이고 통합적인 응급 대응 수행
	대응 활동	-
복구 단계	수습 본부 설치・운영	• 비상사태 시 정부 및 기관 간 신속한 협력 조정 장려
	복구 계획 수립	• 비상대비법에 근거한 비상 복구 계획 수립・시행
	원인 조사	-

영국 주요기반시설 보호 법제의 안전 관련 계획 및 조치들을 안전관리 관점의 분류 기준으로 분류한 결과, 예방 단계는 안전관리 기구 및 조직 구성 활동 4개, 안전관리 체계 마련 활동 1개, 안전점검 및 안전조치 활동 2개, 안전관련 산업의 육성과 안전 문화 활동 지원 1개로 총 8가지의 활동이 기술되어 있었다. 대비 단계에서는 안전관리 계획 수립 활동 5개, 안전 관리 능력 향상 활동 4개로 총 9가지의 활동이 기술되어 있었다. 대응 단계는 대응 체계 구축·운영 활동 3개, 응급 조치 활동 1개로 총 4가지의 활동으로 분석되었으며, 복구 단계는 수습 본부 설치·운영 활동 1개 활동이 기술되어 있었다. 이를 그래프로 나타내면 다음과 같다.

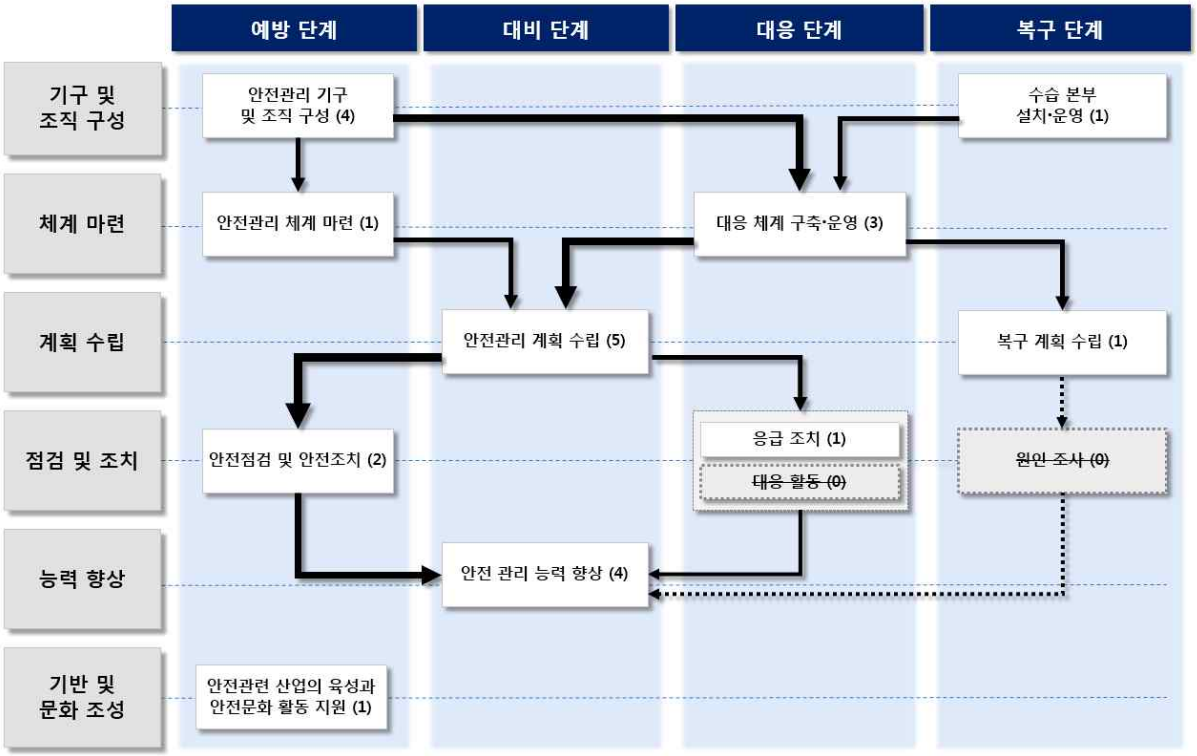
[그림 4-5] 영국의 주요기반시설 보호 법제의 안전 관리 단계별 기술된 항목의 개수 (단위:개)



영국은 다른 국가들과는 다르게 대비 단계에 대한 내용이 전체 안전 관리 조치의 절반에 가까울 정도로 많은 사항을 포함하고 있었다. 특히 일반 비상계획과 특별 비상계획을 중심으로 하여 업무지속관리 계획(BCM). 지역일반대응계획, 지역역량조정계획 등으로 내려오는 다양한 목적과 범위의 안전관리 계획 수립 체계가 탄탄히 잡혀있었다. SW 안전 관련법의 제·개정을 검토할 시에도, 국가안전관리기본계획을 기반으로 한 우리나라의 여러 가지 안전관리 계획들과 영국의 체계적인 계획 구조를 참고하여

사각지대를 최소화시킬 수 있는 포괄적인 소프트웨어 안전 관리 계획 마련을 위한 조항을 구성할 수 있도록 해야 할 것이다.

[그림 4-6] 영국 주요기반시설 보호 법제의 안전관리 관점의 세부 분류 단계별 활동 흐름도



또한 영국은 대비 단계에 속하는 안전 관리 능력 향상 활동에도 큰 노력을 쏟고 있었다. 조직 내 훈련 및 위기상황에 대한 연습뿐만 아니라 명확한 테스트플랜을 구축하고 훈련 계획을 수립하도록 법에 명시하고 있으며, 안전관리 인식 제고를 위한 규정도 두어 전 국민, 전 직원에 대한 안전 문화 확산에도 신경을 쓰고 있었다. 더군다나, 소방공무원의 교육훈련을 위한 소방대학, 긴급사태계획대학의 교육기관을 통해 고도의 지식과 기술을 연마하고 있는 점은 우리나라의 안전 관리 인력 양성 정책 수립에 있어서도 긍정적으로 검토해보아야 할 것이다.

제2절 독일의 주요기반시설 법령 분석

1. 독일 주요기반시설 보호 법제 개관

1) 배경 및 연혁

1990년 10월 3일 통일을 이룬 독일은 국가 재난관리 체계에 대한 수정을 통해 정부 단위를 연방(Bund)정부, 주(State)정부. 지역(Kreis)정부, 시 정부로 단계적으로 분류하여 운영하게 되었다. 독일은 1997년 민방위법 개정을 통해 국가 재난 관리, 안전대책, 주요 기반시설 보호 등에 대한 업무를 재정비 하였다. 민방위법(Zivilschutzgesetz: ZSG) 이외에도, 연방기술지원청 지원법적 관계 규정에 관한 법률(Gesetz zur Regelung der rechtsverhältnisse der Helfer der Bundesanstalt Technisches Hilfswerk: THW-HelgRG), 보호 목적을 위한 수리시설 영역의 안전 확보에 관한 법률(Gesetz über die Sicherstellung von Leistungen auf dem Gebiet der Wasserwirtschaft für Zwecke der Verteidigung: WasSiG), 제1차 수질오염방지법(Erste Wassersicherstellungsverordnung: WasSV 1), 제2차 수질오염방지법(Zweite Wassersichers tellungsverordnung: WasSV 2) 등의 안전관점에서 국가와 국민을 보호하기 위한 법률을 제정하였다[72].

2001년 미국에서 발생한 9.11. 사태는 유럽에서도 대테러 안전에 대한 필요성을 느끼게 하였고, 독일어서도 본격적으로 기반보호 계획과 정책에 관한 논의가 시작되었다[73]. 독일은 안전이 강조되는 국제적 논의의 추세에 직접적인 영향을 받아 2005년부터 기반보호 관련 정부문서를 발표하기 시작했다. 특히 정보기반보호를 위한 국가계획(2005), 주요 기반보호 권고 대책(2005), 민간기업과 부처를 위한 주요기반시설 위기 대응 관리 지침(2008), 주요기반보호를 위한 국가전략(2009)등을 바탕으로 독일 정부의 기반보호에 관한 기초 프레임워크가 제시되었다.

또한 정보통신 기술의 발전에 따라 정보통신 기반시설에 대한 보호가 필요해 졌고, 독일통신법(Telekommunikationsgesetz), 전자상거래통합법(EIGVG)과 텔레미디어법(Telemediengesetz), 독일전자서명법(Gesetz über Rahmenbedingungen für elektronische Signaturen: Signaturgesetz - SigG)을 통해 정보통신 기반시설 보호와 관련한 보호 조항을 신설하였다. 이 외에도 정보통신기반보호를 위한 일반적인 규정으로 독일형법(strafgesetzbuch: StGB)과 형사소송법(Strafproze ß ordnung: StPO)에 관련조항을 두고

72) 재난환경 변화에 따른 과학적 재해관리체계 강화를 위한 법제 연구 - 영국, 독일편, 72-73면
73) 미영독 기반보호법제 연구, 222면

있으며, 처벌행위를 규정하고 있다.

이러한 각종 규정에도 불구하고 국가 기반시설에 대한 침해사고는 증가하였고 특히 현실에서의 물리적 공격이 아닌 사이버 공격으로 인한 사고가 증가하였다. 이에 따라 2015년 사이버 보안 위협의 피해로부터 국가의 중요한 기반시설(Critical Infrastructure)을 보호하기 위해 연관 분야의 사이버 보안조치를 도입하고 관련 내용을 규제하는 새로운 IT보안법을 제정하게 되었다.

2) 주요기반시설 보호체계

독일 기반보호의 중추를 담당하는 기관으로는 내무부(BMI)와 그 산하의 연방정보보호청(BSI), 연방시민보호 및 재난지원청(BBK), 연방 범죄수사국(BKA)과 연방경제기술부(BMWI)등이 있다. 그 외에도 법무부(BMJ), 국방부(BMVg) 등 기반보호 담당기관 이외의 기관들이 기반보호를 위해서 일반적인 역할을 수행하고 있다[74]. 특히 국가주요기반시설의 보호에 있어서 연방정보보호청(BSI)과 연방시민보호 및 재난지원청(BBK)의 역할이 가장 대표적으로 각각 사이버 공격에 대한 정보통신 기반시설의 보호와 재난 위기관리 관점에서 바라보는 기반시설 보호라는 관점에서 역할을 분담하고 있다. 또한 2002년에 구성된 AG KRITIS는 BMI, BSI, BBK의 요원들로 구성된 위기대책반으로 독일 내 기반 시설을 침해하는 위협에 대응한 시나리오를 상정하여 그 내용을 가상적으로 꾸미고, 이에 대한 주요 사회 기반 분야의 취약성을 분석하는 일 뿐만 아니라 이에 대한 대응책을 제시하고, 조기경보 시스템을 구축하는 내용도 포함하는 등 국가차원의 주요기반시설보호(CIP)와 주요정보통신기반시설보호(CIIP) 에 대한 책임을 지고 있다[75].

독일은 국가 및 국민 보호를 위한 재난관리 기본 방침을 내세우고 있으며, 연방계획으로 정부기능의 연속성 보장, 국민보호, 물자 조달 등 위기상황에서 사회기능이 지속될 수 있도록 노력하고 있다. 독일 헌법에서는 재난 방지 영역의 입법시에 연방이 관할권을 지닌다고 명시하고 있다. 그러나 실질적인 법률 이행은 연방의 위임을 받은 행정 내에서 개별 연방 주(State)를 통해서 이루어지고 있으며, 연방의 과제는 연방내무성(BMI), 관할권 내에 있는 여타 행정 부처, 기술지원단(THW)및 연방행정청(Bundesverwaltungsamt)에 의해 이행되고 있다

74) 미영독 기반보호법제 연구, 218면.
75) 미영독 기반보호법제 연구, 225면.

<표 4-10> 독일의 주요기반시설 보호 관련 기관

구분	관련부서	
주요기반시설보호에 관한 직접적인 업무를 담당하는 행정기관	연방 내무부	Federal Ministry of the Interior (BMI)
	연방 정보안전청	Federal Office for Information Security (BSI)
	연방 시민보호 및 재난구조청	Federal Office of Civil Protection and Disaster Assistance(BBK)
	연방 범죄수사국	Federal Criminal Police Agency (BKA)
	연방 경찰청	Federal Police(BPOL)
	내무부소속 위기대응팀	task force for critical infrastructure protection (AG KRITIS) at BMI in 2002
	연방 경제기술부	Federal Ministry of Economics and Technology
	연방 네트워크 관리청	Federal Network Agency
주요기반시설보호에 관한 간접적인 업무를 담당하는 행정기관	연방 총리실	Federal Chancellery
	연방 법무부[76]	Federal Ministry of Justice
	연방 외무부	Federal Ministry of Foreign Affairs
	연방 국방부[77]	Federal Ministry of Defense
	연방 정보국	Federal Intelligence Service (Bundesnachrichtendienst,BND)
	헌법 보호청	Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz, BfV)
	기타 민간영역	private sector

- 연방 내무부 - Federal Ministry of the Interior (Bundesministerium des Innern; BMI)

연방내무부는 독일 내 안보를 담당하는 주관부처로서 주요기반보호 및 주요정보통신기반보호와 관련된 업무를 수행하고 있으며, 재난 발생시 시민보호의 차원에서 물리적 보호 뿐만 아니라 IT 및 사이버상의 정보보안과 관련된 각종 정책을 입안하고 조정하고 있다. 독일연방내무부는 광범위한 임무를 띠고 있으며, 이 중에는 중요국가기반시설의 보호를 포함해 국가 내부의 안전을 지키는 일을 수행하고 있다. 연방내무부의 목표는 범죄가 일어나기 전에 테러리스트의 공격이나 그 외의 다른 형태의 범죄 등으로부터 국가를 보호하는 것이다. 국가의 모든 구성원은 필요하다고 생각되면 범죄의 원인을 파악하거나, 그것을 가능한 한 빨리 인식할 수 있도록 하기 위해서 동 기관에 알릴 권리와 의무가 있다.

BMI의 구성은 크게 내각과 의회 부분 담당, 국제담당, 언론 보도 대변인, 편집 사무실 등을 포함하는 비서진으로 구성된 장관실과 국무담당, 정보기술 분야 연방정부 위원장 등으로 구성되고, 수많은 조직으로 구성되어 각각의 임무를 수행하고 있다. 특히 주요기반시설 보호와 관련한 내부 조직으로는 다음과 같은 부처가 존재한다.

① Z부처 - 중심적 업무

Z부처는 연방행정부로 다른 부처나 관련기관들이 업무를 수행하는 것에 필요한 인적, 물적, 재정적 자원의 보호를 담당하고 있다. 이러한 기능은 직원, 조직, 예산상의 문제, 내부적 서비스를 담당하는 부서들에 의해서 최초로 수행되며 Z부처는 그 중심적인 업무를 담당하고 있다[78].

② 정보사무실장 - IT 전략, 관리 및 보안

IT전략과 관련된 업무는, 연방내무부의 IT정책과 보안은 정보사무실장 이 관리하고 있다. 그 업무는 정보사회를 위해서 BMI와 정치적으로 협동하는 것에 중점을 두고 있으며, 지역사회 사업을 체계적이고 세계적으로 발전시키는 역할을 담당하고 있다. 즉, 독일의 IT산업과 관련된 일에 대해서는 가장 앞서서 활동하고 있으며, 연방행정을 위한 연방 정부의 협동, 자문기구로서(KBSt) 정보사무실장 부서를 할당하고 있다. 더욱이 수년 간 신뢰할 수 있는 조언을 하는 것과 더불어, 자문기구로서의 중요한 사무로 연

76) http://www.bmj.bund.de/enid/4e02aa38526e9a3069072ac5fa5dbc01,0/aktuelles_13h.html. Official Journal of the European Union, L 69/67-71, 16 March 2005, http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2005:069:SOM:en:html.
77) http://www.bmvg.de/portal/a/bmvg.
78) 미영독 기반보호법제 연구, 229면.

방의 중요한 IT 기본시설을 구축을 목표로 하고있다(IVBB Berlin-Bonn Information Network, IVBV Information Network of the Federal Administration, Federation Porta l)[79].

한편, 전자서명 또는 인터넷보안으로서의 IT보안과 관련된 문제는 연방 정보안전청(BSI)에서 담당 하고 있다.

③ Öffentliche Sicherheit 부처 - 공공의 안전[80]

ÖS(Öffentliche Sicherheit) 영역은 기반보호와 관련해서는 가장 직접적 인 임무를 수행하는 부처라고 할 수 있으며 공공안전분야 전반을 담당하고 있다.

<표 4-11> 내각부 ÖS부처 영역별 관할 내용

영역구분	관할내용	세부영역
ÖS Ⅰ	경찰 업무	1. 일반경찰업무, 범죄의 조절과 예방, 보안업무
		2. 심각하고 조직적인 범죄
		3. 경찰 정보 조직, 내부의 보안정보 구조, 연방범죄 치안활동, 보안분야의 자료 보호
		4. 국제범죄공조, 유럽연합, 유럽경찰
ÖS Ⅱ	반테러리즘	1. 반테러리즘의 법률과 일반적인 문제, VIP와 행정기관의 보호
		2. 국제적 반테러리즘의 문제
		3. 외국인에 의한 테러리즘과 극단적 범죄
		4. 국가적 반테러리즘, 정치적 동기의 범죄
ÖS Ⅲ	헌법의 보호에 관련된 문제	1. 헌법의 보호를 위한 연방공동체의 체계에 관한 법률적, 일반적 업무
		2. 정보통신기술 ; 특별한 기술과 군사술, 명령, 조정, 기능적 장비와 부수물
		3. 기밀문서의 보관과 파괴행위로의 보호, 지능적 범죄, 사무 실 보안, 국가보안기관
		4. 좌, 우파 영역에서의 테러리즘에서의 헌법의 보호와 관련된 일
		5. 교통, 해상, 항공 보안, 핵 설비, 장비와 운송의 보안과 보호

79) 미영독 기반보호법제 연구, 233면.
80) 미영독 기반보호법제 연구, 234-235면.

④ B부처 - 연방경찰관련

B부처는 연방경찰의 활동을 다방면으로 협조하고 조정하는 역할을 맡고 있다. 또한 이와 더불어 연방경찰의 수장에게 조언을 함으로서, 정책 구상과 행정사이 에서 조율적인 역할을 수행하고 있으며, 일반 업무, 행정, 예산, 연방경찰의 39,000명의 직원들의 위법사항을 감시한다. 이들의 주된 업무는 철도 와 국경, 항공안전, 조직과 특별한 부분의 업무, 행정업무와 서비스이다[81].

<표 4-12> 내각부 B부처 영역별 관할 내용

영역구분	관할내용	세부내용
B1	일반정책과 법률문제	• 조직, 의료, 안전 서비스
B2	자원과 예산의 계획	• 연방 경찰의 효율적인 업무 조장
B3	일반 경찰과 조직상의 문제	• 항공기 안전
B4	국경 주변의 경찰의 일	• 국제경찰사무소(IPM)
B5	정보통신	• 정보와 통신 기술, 보안 권한과 조직의 무선통신 감독
B6	기술과 군사학	• 명령, 조정, 운영 장비와 기타 시설물

⑤ KM부처 - 위기관리 및 시민보호

KM부처는 위기관리와 시민보호를 담당하고 있다. 각 연방기관들의 국가적 위기관리에 관련된 업무, 즉 다양한 내각과 조직과 행하는 업무의 조화를 위한 일들을 책임지고 있다. 또한 이 부서는 시민을 보호하고 연방차원에서 재난을 관리하는 일을 수행하며, 특히 기반시설의 보호를 위해 기타 연방정부 및 기업과 협력하고 업무를 조정하고 있으며, 특별한 보안과 안전 규정, 즉 무기법, 안전관리규정, 폭발물에 대한 법률조항의 준비를 포함한 다양한 규제방안을 구상하고 있다.

또한 연방 시민보호 및 재난 구조청에 대한 원조(Bundesamt f□□r Bev lkerungsschutz und Katastrophenhilfe, BBK)와 연방 정보기술 보안청(Bundesamt fur Sicherheit in der Informationstechnik; BSI)를 전 문적으로 보조하고, 그 합법성에대해 관리 감독을 수행하고 있다[82].

81) 미영독 기반보호법제 연구, 235-236면.

<표 4-13> 내각부 KM부처 영역별 관할 내용

영역구분	관할내용
KM1	• 위기관리통합센터
KM2	• 시민보호의 연방사무실과 재난 원조, EU와 NATO의 재난 관리업무
KM3	• 기술적 지원 및 국제관계
KM4	• 중요한 기반시설 보호
KM5	• 무기와 폭발물 규정, 특별 안전법
KM6	• 소통, 지휘 통제 센터

- 연방 정보기술 보안청 - Federal Office for Information Security (Bundesamt fur Sicherheit in der Informationstechnik; BSI)

정보 기술에 대한 의존도가 높을수록 보안 문제가 더 중요해지고 있으며, 컴퓨터 고장, 오용 또는 파괴가 초래할 수 있는 혼란과 관련한 각종 위협에 대응하기 위해 1991년 설립된 연방정보기술보안청(BSI)은 독일의 IT보안을 개선하는 데 기여하는 임무를 지고 정보기술의 적용 시 보안 위험을 조사하고 구체적인 경우 상응하는 보안대책을 개발하고 있다.

IT 문제의 복잡성으로 인해 BSI가 직면하는 업무는 매우 광범위하며 정보 기술 사용과 관련된 위험 및 위협에 대한 정보를 제공하고 적절한 해결방안을 모색하고 있다. 이러한 작업에는 산업계와 협력하여 IT 보안 심사와 평가 및 IT 시스템 개발을 포함하고 있다. 기술적으로 안전한 정보 및 통신 시스템에서도 부적절한 관리 또는 부적절한 사용의 결과로 위험과 손상이 발생할 수 있기 때문에 위험을 최소화하거나 피하기 위해 BSI의 서비스는 다양한 대상을 상대로 한다. 즉, 정보 기술의 제조업체, 유통 업체 및 사용자 모두를 대상으로 조언하고 있으며 정보를 제공한다.

IT위협의 증가와 변화는 BSI에 새로운 사고방식과 행동방식을 요구하고 있다. BSI는 앞서 설명한 임무 및 새로운 위험에 대해 효과적인 보호수단을 개발하여 이를 적시에 실천하기 위해서 국내외 다른 기관의 전문가들뿐만 아니라 기업들과도 긴밀하게 협력하고 있다. 새로 설립된 부서들이 새로운 임무의 의미를 정당하게 평가하고 항상 폭넓은 전문지식을 활용할 수 있는 데 기여하고 있다. BSI는 특히 인증(Zertifizierung), IT보

82) 미영독 기반보호법제 연구, 236면.

안관리(IT-Grundschutz) 및 암호기술(Kryptotechnologie) 분야에서의 능력을 활용하여 새로운 보안 위협에 효과적으로 대처할 수 있는 토대를 만들고 있다. 장래에는 BSI가 더 적극적으로 활동하게 될 것이다. 앞에서 말한 임무 외에도 연방정부의 IT보안 가이드가 업무의 중심 구성요소가 된다. BSI 홈페이지(www.bsi.bund.de) 에서는 최신의 보안예보안내, 정보기술 보안에 관계있는 온라인서비스와 기타 정보를 제공한다. IT 보안관리(IT-Grundschutz), 인증/인정(Zertifizierung/Akkrediti erung), 인터넷보안(Internetsicherheit), 중요 인프라 보호(Schutz Kritischer Infrastrukturen) 같은 BSI의 핵심주제에 대해 풍부한 온라인서비스와 여러 가지 전문주제 BSI 연구보고서를 제공한다[83].

<표 4-14> BSI의 주요 업무 내용

<table>
<tr><th colspan="2">BSI 주요 업무</th></tr>
<tr><td rowspan="6">어플리케이션 보안과 주요기반시설[Security of applications and critical infrastructures]</td><td>기본적 보안 요건 및 보안게이트웨이(방화벽), 네트워크 기반시설 및 어플리케이션에 대한 실제적 솔루션의 개발</td></tr>
<tr><td>IT 보안 테스트 및 IT시스템에 대한 평가를 수행, 관련 보안시스템의 개발</td></tr>
<tr><td>공공기관 운영 컴퓨터망의 취약점 분석</td></tr>
<tr><td>컴퓨터바이러스, 인터넷 보안, 주요 정보통신기반, IT기반시설보호</td></tr>
<tr><td>주요 기반시설에 사용되는 IT 보호 개선책 강구</td></tr>
<tr><td>컴퓨터긴급대응팀(CERT-Bund)의 운영, IT 상황센터(IT 위협상황평가) 운영</td></tr>
<tr><td colspan="2">네크워크 보안[Security of networks (including CERT Bund, IT situation center, and IT crisis management center, and early warning systems)]</td></tr>
<tr><td colspan="2">암호기술[Cryptographic technology]</td></tr>
<tr><td colspan="2">신기술[New technologies (e.g., biometrics:생체인식, RFID)]</td></tr>
</table>

83) 미영독 기반보호법제 연구, 241-242면.

- 연방 시민보호 및 재난구조청 - Federal Office of Civil Protection and Disaster Assistance (Bundesamt für. Bevölkerungsschutz und Katastrophenhilfe; BBK)

연방 시민보호 및 재난구조청은 주요기반시설보호(CIP)와 긴 급상황대비 정보시스템 구축하기 위해 BMI의 산하기관으로서 2004년에 신설된 기관이다. 주요 업무는 시민의 안전과 재산보호, 공동상황실센터(GMLZ)와 시민보호 및 재난보호를 위한 전문정보시스템(FIS), 긴급비상정보시스템(deNIS), 연방지역의 재난경보, ABC의 정책, 독일인 희생자 및 유족 조정국, 위기관리와 긴급 상황 기획 및 시민보호를 위한 재교육 등이다.

연방 시민보호 및 재난지원청은 청장과 부청장 및 4개국으로 구성되어있으며, 국가 재난 관리에 신속히 대응하기 위한 연방정부의 핵심적인 기관이며, 주정부와 민간기관과의 정보 교류와 협력적 시스템을 구축하는 조정기능과 재난 발생에 대한 예방 관리에 노력하고 있다. 특히, 국가 위기 상황에 대비하여 국민 보호를 위한 기획과 사전 준비, 연방정부와 주정부의 협력에 대한 기획과 사전 준비, 외국에서자국민이 위기 상황에 처한 경우에 행정적, 심의적, 의학적 협의와 조정을 담당하는 중추적인 역할을 하는 것이 주요 업무이다.

BBK의 조직 중 기반체계와 관련하여 주요 핵심기반시설 보호센터가 있어 위험상황 분석 및 핵심기반시설 보호 업무를 수행한다. 주요 핵심기반시설 보호센터는 위험상황 분석, 에너지, 물, 정보통신 기술, 교통시 설 등의 보호를 목적으로 1)각 주 및 도시별로 주요 재난을 파악하고 위험을 분석해서 BBK로 보고하는 위험분석 및 평가센터, 2)에너지센터, 3)물(식용수)관리센터, 4)통신정보체계 보호센터, 5)교통체계보호 센터 등 5개 부서로 구성되어있다. 특히 긴급비상정보시스템(deNIS)은 일반인을 위해 조직되어 잠재적인 긴급 상황에 관한 정보를 제공하며, 긴급 상황에 대한 주의경보와 웹서 비스를 제공한다. 비상 정보 체제의 핵심 요소는 모든 정보 자료를 수집하고 선별하며, 국민에게 위기관리에 대한 정보를 신속히 제공하는 중추적 서버 기능을 하는 것이다. 따라서 사이버 통합운영정보시스템의 큰 장점은 재난 관리에 대한 신속한 정보 수집, 상황 분석 및 체계적인 대응에 보다 더 적극적으로 대처할 수 있다는 것이다. 동시에 예방 차원에서 국가 위기 상황이 발생하면연방정부 및 주정부의 내부 정보망을 통하여 정보를 신속하게 지원한다.이와같이비상정보체계는예측할수없는위험상황에서다양한 정보 제공과 대응력을 높이는 데 효과적이다.

그밖에 긴급 상황 시 여러 관련 공공기관간의 정보 공유 및 자원할당의 기능을 수행하며, 시민 보호 및 재난발생시 피해를 줄이기 위한 훈련, 응급의학, 재난의 경고 및 전파, 시민보호를 위한 연구의 수행, 시민들의 재난대응능력 향상을 이한 조치, 각 기

관들의 참여를 유도하며 국제협력에 관한 임무도 아울러 수행 하고 있다.

또한 위기관리, 비상계획 및 시민보호를 위한 학술원(AKNZ)은 연방행정청에 소속된 재난 관련 교육 및 재교육을 실시하고 있으며, 재난 영역에서 시민 보호와 재난 보호의 지도와 연구프로젝트의 기획, 실행 및 평가에 대한 이론적, 경험적 질을 높이려고 노력하고 있다. 또한 실제 재난상황에서 연습 훈련을 할 수 있는 몇 개의 시설을 갖추고 있다. 주요 임무로는 시민 재난 보호의 지도력 향상, 시민 재난 보호에 대한 국내외의 발표된 자료 평가, 국내외 재난 및 대규모 재난 손실에 대한 평가, 학술 연구 및 연구 프로젝트의 실행과 평가, 기술과 인프라 구조에 대한 집행 및 평가, 민·군 합동 훈련의 실행 및 평가, 연방행정청, 연방정부와 주정부의 위원회 및 유럽총회와의 협력 관계 등이 있다.

- 연방 범죄수사국 - Federal Criminal Police Agency (Bundeskriminalamt; BKA)[84]

연방범죄수사국은 정보통신기술과 관련하여 범죄를 수사하는 기관으로서 BMI의 산하기관으로 주요기반시설 파괴행위 수사를 담당하고 있다. BKA는 독일의 대내외의 안전을 위협하는 범죄와 국민의 생명, 건강에 위협적인 요소 또는 사회기능을 해치는 주요기반시설의 파괴와 관련된 범죄의 기소를 위한 1차적인 역할을 수행하며 정보통신기술과 관련된 범죄를 수사하는 중추 기관의 역할을 담당하고 있다.

- 연방경제기술부 - Federal Ministry of Economics and Technology (Bundesministerium für Wirtschaft und Energie; BMWi)[85]

연방경제기술부는 경제 및 주요기반시설보호(CIP)를 위한 감독청으로 주로 경제정책 부문과 주요기반시설 부문에 대한 감독을 수행하고 있다. 이 때 주요기반시설 분야에 대한 감독은 연방망관리청(BnetzA)이 행하고 있다. 에너지부문과 관련하여서도 BMWI는 에너지공급의 안정을 위한 보장책임을 지고 있으며, 독일 기본법 제87조(에너지 공급의 안정화를 위한 프레임워크의 개발 - 적절한 통신기반시설 및 서비스공급 보장의 책임)에 따라 적절한 통신기반시설 및 서비스를 제공이 이루어지도록 시스템을 구축할 책임을 진다.

BMWI는 8개의 분과로 조직되어 있으며, 이 중 통신 및 우편정책 제6분 과에서 주요

84) http://www.bka.de.
85) http://www.bmwi.de

정보통신 기반시설보호를 위한 임무를 수행하고 있다. 제6분과는 IT 정책 및 정보보호를 주로 담당하고 있으며, 세부적으로는 담당하는 분야는 IT 통신 및 우편정책에 관한 국제이슈, 통신산업의 일반적 이슈, 연방 망관리청의 감독, 유럽 ICT정책, 국제 ITC정책, 주파수 정책, 보안이슈, 비상사태대응, 관련법령정비, 정보사회미디어 정책, 디지털 통합정책, 융합 ICT개발, ICT 표준화 정책 등이 있다.

- 연방망관리청 - Federal Network Agency (Bundesnetzagentur; BNetzA)[86]

연방망관리청[Federal Network Agency(BNetzA)]은 통신, 우편, 전기, 에너지 산업 분야의 네트워크의 안전을 보호하기 위한 기관으로, 기존의 전기통신, 우편 규제청(Regulierungsbehörde für Telekommunikation und Post; RegTP)이 2005년 연방 망관리청(BNetzA)으로 개편된 것이다.

BNetzA는 정보통신분야 주요기반시설 안전보호를 위하여 BMWI와 공조 관계를 유지하며, 정기통신망 보호에 있어서 주요 책임기관으로서의 임무를 수행한다. 동 기관의 구성은 망관련 산업분야의 사업지원, 정보기술 및 보안, 통신규제, 주파수할당, 우편정책, 통신기술정책, 번호할당, 에너지정책, 철도정책 등을 담당하는 부서로 구성되어 있다.

3) 국가 중요기반시설 지정

독일은 핵심기반시설(CI: Critical Infrastructure)을 '고장 또는 손실로 공공 안전 또는 사회적 중요성에 대한 심각한 붕괴, 그리고 지속적인 공급체계에 결함을 초래할 수 있는 국가적으로 중요성이 있는 조직 또는 시설'로 정의하고 있다. 독일의 핵심기반체계 보호를 위한 국가전략(National Strategy for Critical Infrastructure Protection) 보고서에서는 핵심기반시설을 지정하는 기준이 되는 '위험도(Criticality)'를 '사회적으로 중요한 재화 및 서비스를 제공하는 공 급 수단의 기능상 결함이나 중단의 영향으로 기반시설의 중요성을 나타내는 상대적인 척도'로 정의하고 있다 .

독일에서 기반시설은 국가 공동체를 위하여 중요한 의미를 지니고 있는 조 직 및 시설로서 소멸되거나 방해를 받게 되는 경우 지속적으로 공급부족이 발생하거나 공공의 안전에 심각한 장애 또는 다른 극단적인 결과를 가져올 수 있는 시설로 정의하고 있다(행정안전부,208a:174). 독일은 공공복지를 위해 중요한 조직체계 및 제도의 파괴 또

86) http://www.bundesnetzagentur.de/enid/6c28cf7e908c093de1d8973191d1ed59,0/xn.html.

는 중단은 공 공 안전 또는 다른 극적인 사회적 중요성들에 장기간에 걸친 공급 병목과 큰 혼란을 초래함을 국가적으로 인식하고 다음과 같이 중요기반시설 보호대상 분야를 분류하여 관리하고 있다[87].

<표 4-15> 독일의 중요기반시설 분류 현황

분야	세부분야
교통수송	• 항공, 해상교통, 철도, 지역교통, 운하, 도로, 우편시스템
에너지	• 전력, 원자력, 가스, 유류
위험물질	• 화학 및 생물학적 물질, 유해물질 운송 등
통신 및 정보기술	• 통신, 정보기술 분야
금융 및 보험	• 은행, 보험, 금융서비스 제공자, 주식거래소
서비스	• 비상, 건강과 구조서비스, 시민보호, 음식 및 식수공급, 쓰레기처리
행정부 및 사법시스템	• 행정부 및 사법시스템(경찰, 군 포함)
기타	• 방송, 주요 연구기관, 상징적 빌딩, 문화적 자산 등

기반시설의 약 80%는 민간에서 소유하고 있으며, 비상계획도 각 기반시설 소유주가 우선적으로 내부 비상계획을 수립하는 것을 원칙으로 하고 있다. 시장 또는 군수는 관내에 소재하고 있는 기반시설에 대한 외부 비상 계획을 수립하고, 이를 수정, 보완해야 한다(행정안전부,208a:176).

87) 행정안전부, 효율적 국가기반체계 보호를 위한 연구, 2008, 59면.

2. 주요기반시설 보호 관련 법령

1) 재난관리에 관한 법

독일의 재해 및 재난 관련 연방 법률로는 민방위법(Zivilschutzgesetz; ZSG)이 안전관리기본법이라 할 수 있다.

<표 4-16> 독일 민방위법의 구성

독일 민방위법
제 1장(제1조~제4조): 일반규정
제 2장(제5조): 자력구조
제 3장(제6조): 국민경보
제 4장(제7조): 대피시설
제 5장(제10조): 체류 규정
제 6장(제11조~14조): 민방위 재난 방지
제 7장(제15조~18조): 건강 보호를 위한 조치
제 8장(제19조): 문화재 보호를 위한 조치
제 9장(제20조~제22조): 조직 및 조력자
제 10장(제23조): 민방위 비용
제 11장(제24조): 과태료 규정
제 12장(제25~27조): 종결 규정

독일은 민방위법(1997년 개정)에 의거하여 연방총리가 위원장인 연방안보 위원회가 국가 위기관리 관련 정책 및 관련업무의 총괄 협의와 조정기능을 수행한다[88]. 2002년 '국민 보호를 위한 신전략'에 의해 '연방 시민보호 재난 지원청'설립에 관한 법률이 제정되었고 이에 근거하여 연방내무부 산하 연방 시민보호 재난지원청(BBK)에서 재난관리 업무를 담당하게 되었다(행정안전부,208b:58).

88) 재난환경 변화에 따른 과학적 재해관리체계 강화를 위한 법제 연구 - 영국, 독일편, 73면

2) 정보통신기반보호에 관한 법

기반시설 중 정보통신분야의 경우 정보통신기반보호를 위한 안전에 관한 조치들은 '연방 정보기술 안전청 설치법'상 연방 정보기술 안전청(BSI)이 담당하며 정보통신 관련 시장규제,고객보호,무선방송송신,주파수정책,보편 적 서비스, 통신비밀, 정보보호 및 공적 안전 등을 위한 권한은 정보통신법 (TKG :Telekommunikationsgesetz) 및 연방통신망청법 상의 연방 네트워크 관리청(BNetzA)이 담당한다(BBK,209;한국인터넷진흥원,2010:9)에서 담당한다[89].

독일의 법률은 정보보안과 관련, 개인정보보호에 대해서는「연방데이터보호법(BDSG)」이 규율하고 일반적인 우편•통신•전화 등과 관련된 정보보안의 경우에는「정보통신법」(TKG : Telekommuni-kationsgesetz)이 규율하고 있다. 또한 정보통신기술시스템의 안전성에 대한 심사•평가•인증 등 정보화기술의 안전성과 관련된 업무수행 권한은「연방정보기술안전청설치법」에 두고 있다. 독일 영토 내에서 국민에 대하여 직접적 인구속력을 갖고 있는「정보통신법」을 포함한 각종 독일 정보통신 관련 법률은 유럽연합의 지침(EU-Richtlinie)에 의해 일정한 기간 내에 국내 입법화를 하여야 하는 의무를 부담하기 때문에 EU지침도 독일 정보통신 관련 법제에 포함된다고 할 수 있다.

「정보통신법(TKG)」은 2004년 제정되어 2005. 3월 개정된 법으로서 정부기관이 기밀누설 방지, 데이터의 안전성 확보 및 네트워크 침해사고 방지를 위해 인터넷통신사업자(ISP)와 정보통신 서비스를 제공하는 모든 책임자에게 고객정보에 대한 정부의 접근요청 시 이를 지원해 주도록 하고 있으며 이러한 데이터는 정부의 감시기관이 직접 접근할 수 있도록 규정하고 있다.

특히 제2조 제2항 제9조에는 '공적안전' 의 이익이 보장되어야 함을 명백히 하고 있는 바, 개개인의 권리에 대한 침해가 발생하기도 하지만 다른 한편으로는 국가이익도 보장해야만하기 때문에 공적안전의 이익을 강조하되, 가능한 한 개인에 대한 규제를 최소화 하여 정보보호와 통신비밀 및 공적안전에 관한 규정이 이러한 목적에 기여하도록 균형을 유지하고 있다. 따라서 제7장의 비밀, 정보보호 및 공공안전에 관한 규정에서 특히 공공안전을 위해 사업자들이 긴급전화가 가능하도록 할 의무, 기술적 보호대책과 감시가 가능한 방법을 마련할 의무 및 정보제공 의무를 지게 하여 국가 본연의 기능을 수행할 수 있도록 사업자 등에 대한 자료요구 권한, 사업자들의 관련 시설 지원 의무 등을 구체화하고 있다.

89) http://www.gesetze-im-internet.de/tkg_2004/BJNR119000004.html.

「연방정보기술안전청설치법」은 연방정보기술안전청(BSI)의 설립 근거법으로서 독일 연방 내무부 산하의 국가기관으로서 실무상 정보통신의 안전영역에 대한 관할권을 가진 가장 중요한 기관으로 활동하도록 정하고 있다. 특히 이법에서는 평가•인증업무는 물론, 정보통신기술시스템의 연구와 개발, 그리고 정보통신시스템 및 내용의 심사를 통한 안전성 위험 조사 및 정보통신시스템 안전성 검사, 평가와 인증서의 발급, 정보통신시스템의 허가를 비롯하여 국가기관 및 민간기관에 대한 기술지원 및 자문을 제공토록 규정하고 있다.

관련 조직으로 연방정보기술안정청(BSI)은 전신인 1950년대에 설치된 '중앙암호제도실' 로서 연방 행정정보의 안전성 및 고유직무와 국외 비밀정보의 수집 분석 등 업무를 수행해 왔다. 1987년에는 컴퓨터 안전성을 그 관할범위에 포함시킨데 이어 업무범위 확대 등 기관의 중요성을 고려하여1989년에 '중앙정보기술안전실' 로 명칭을 변경하고 업무영역도 종래의 협소한 국가적 사무의 범위를 넘어 정보기술의 사법적 적용 및 안전성에 이르기까지 업무대상에 포함시켜서 기구를 확대하였다. 이어 1991. 1. 1일 시행된 '연방정보기술안전청설치법' 에 의해 내무부장관 관할하의 '연방정보기술안정청' 은 연방 상급 관청으로 되었고 조직도 연방내무부의 직무 영역에편입되었다. 이렇듯 독일은 사이버안전기관의 설립근거와 조직의 활동사항을 법률(BSIG)로 규정하고 있다.

3) 독일형법(Strafgesetzbuch: StGB) 및 형사소송법 (Strafproze ordnung: StPO)

독일 형법(StGB)에 따르면, 정보통신기반보호를 위한 일반적인 규정으로 서 독일형법 제263a조와 제303b조[90]에 따라 컴퓨터를 이용한 범죄 행위의 처벌에 관한 규정을 두

90) StGB § 303b Computersabotage. (1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er
1. eine Tat nach § 303a Abs. 1 begeht,
2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder
3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,
wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
(2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe. (3) Der Versuch ist strafbar.
(4) In besonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter
1. einen Vermögensverlust großen Ausmaßes herbeiführt,
2. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,
3. durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen

고 있다. 동법 제263a조[91]에서는 컴퓨터 사기 에 관한 내용을, 제303b조에서는 컴퓨터 사보타지에 관한 내용을 담고 있다. 특히 제303b조는 컴퓨터를 이용하여 정보통신 시설을 운용할 수 없게 만드는 행위 등을 처벌하는 내용을 담고 있다.

또한 독일 형사소송법(StPO) 제100a조 제1문은 통신서비스의 사용자가 형법상의 범죄행위를 저질렀다는 충분한 의심이 가는 경우, 형사소추관청 (Strafverfolgunsbeh rde)에게 통신을 감청할 수 있는 권한을 부여하고 있다.524) 이러한 범죄행위에 속하는 것으로는 정보통신기반시설과 같은 국가 시설에 대한 범죄행위와 그 밖의 개인적 법익에 대한 범죄행위 등이 포함 된다. 여기서 통신감시조치 등은 피고인이나 피고인과 관련된 자들에 대해 이루어질 수 있다. 동 조치들은 동법 제100b조 제1항 제1문에 따라 법관의 영장이 발부되고, 시간적인 여유가 없는 경우에는 예외적으로 검사가 명할 수 있도록 하고 있다. 다만 그 후 지체 없이 법관의 확인을 받아야 한다. 감 시조치의 기간은 3개월 이내로, 감시조치의 이유가 존속하는 경우 각각 매 번 3개월까지 연장할 수 있다. 감시조치가 종료된 후에는 관계자에게 통보해야 하며, 형사소추 목적이 더 이상 존재하지 않는 경우에는 이로 인한 수집한 정보는 폐기해야 한다[92]. 이러한 형사법상의 규정들은 기반시설파괴행위에 대하여 일반적 범죄행위의 처벌에 관한 범주에서 기반시설보호와 관련된 법규로 볼 수 있다.

4) IT보안법

2015년 중반 독일의 IT 보안법(IT-Sicherheitsgesetz)이 통과되었고 IT 보안법은 다수의 기존 법을 개정하고 IT 보안 및 통보 의무를 도입했다. 주로 “핵심 기반시설 운영자“를 대상으로 하며, 웹 사이트 운영자와 같은 원격 미디어 서비스 제공 업체에 대한 IT 보안 의무가 강화되었다.

---

oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt.
(5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

91) StGB § 263a Computerbetrug. (1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.
(2) § 263 Abs. 2 bis 7 gilt entsprechend.
(3) Wer eine Straftat nach Absatz 1 vorbereitet, indem er Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
(4) In den Fällen des Absatzes 3 gilt § 149 Abs. 2 und 3 entsprechend.

92) 미영독 기반보호법제 연구, 282-283면.

IT보안법에서 말하는 핵심 인프라(중요기반시설)는 시설의 운영중단 또는 손상으로 인해 공공안전에 심각한 위험을 초래할 수 있는 시설을 의미하며 그 범위는 교통, 건강, 물, 유틸리티, 통신 사업 자뿐만 아니라 금융 및 보험 회사등 사회의 주요기능을 담당하는 주요 핵심 영역으로 각 분야에 대한 강력한 정보보안 표준을 마련하고 해당 영역의 사업자 등에게 운영지침을 준수할 것을 요구하며, 2000여개 이상의 필수 서비스 제공을 담당하는 업체들을 그 수범자로 규율하고 있다[93].

- 에너지 : 50 만 명이 넘는 시민이 주거 및 체재하는 범위 내 전기, 가스, 연료, 난방유 및 지역 난방 부문의 공급 시설
- 정보 기술 및 통신 : 50 만 명이 넘는 시민들의 음성 및 데이터 전송, 데이터 저장 및 처리 분야의 시설
- 물 : 50 만 명이 넘는 시민들이 주거 및 체재하는 범위에서 식용수와 폐수 부문의 시설
- 식품 : 50 만 명이 넘는 시민에게 제공하는 식품생산, 가공 및 무역 분야의 시설
- 운송 및 교통; 건강; 재정 및 보험 : 향후 추가 될 예정[94]

IT보안법을 통해 최소한의 사이버 보안 표준에 대한 인증 및 독일 연방 정보 보호청(Federal Office of Information Security; 이하 BSI) 허가를 얻기 위한 기업과 연방 정부 기관의 시스템 마련을 촉구하였고, 연방정부는 기관 내 이를 위한 담당 업무기관을 설치하여야하며, 기업의 경우 시스템 마련 및 보고의무를 지니게 되었다. 또한 독일 연방정보안전청(BSI)의 주요 역할과 권한을 확장하고, 중요 인프라에 대한 사이버 공격의 보고 및 이에 대한 평가의 수행의 역할을 명시하였다.

이러한 새로운 IT 보안법에 대하여 독일의 내무부장관 Thomas de Maizière는 공공 및 내부 보안의 핵심 구성 요소로써 IT 보안영역에서의 중요한 절차로써 기능하게 될 것이라고 설명하였다.

93) 한국정보화진흥원, 개인정보보호 주간동향, 제108호 2015년 7월 24일, 4-5면.
94) Watson Farley & Williams, BRIEFING- The New German It Security Act, February 2016, pp.1-6.

3. 안전관리 관점의 법률 분류

독일은 다수의 법을 통해 안전관리 관점에서의 국가 기반시설 보호를 하고 있다. 특히 연방국가의 특성상 연방이 담당하는 부분과 주에서 담당하는 부분이 나뉘어 있으며 한국의 기반시설 보호 체계와는 다른 점이 존재한다. 대표적인 국가기반보호 관련법으로 민방위법에 의한 위험대비 체제가 존재하나 민방위법은 광범위한 법으로 국가중요기반시설에 특화한 법이라고는 할 수 없을 것이다. 독일의 주요기반시설보호는 위에서도 언급했듯이 BSI와 BBK가 담당하고 있다. BBK는 그 업무가 주요기반시설 뿐만 아니라 모든 국가 재난 및 위험과 관련하여 범위가 광범위하지만 이와 다르게 BSI는 정보통신기반시설의 보호와 밀접한 연관을 갖고 있으며 현대사회의 주요기반시설의 특화한 보호대책을 강구하고 있다. 특히 소프트웨어와 관련한 국가 기반시설 보호라 하면 BSI가 담당하는 정보통신기반보호가 대표적이라 할 수 있다. 따라서 연방 정보기술안전청 설립에 관한 법률[95]을 분석하는 것은 독일의 주요정보통신기반보호의 안전관리 구조에 대한 이해에 상당한 도움이 될 것이다. 따라서 BSI설립에 관한 법률(BSI Act - BSIG) 조항들을 안전관리 관점으로 분석 및 분류해보고자 한다.

1) 예방 단계

- 안전관리 기구 및 조직 구성

(§1) 연방 정보기술안전청 설치

연방정부의 정보기술에 대한 안전에 대한 사항을 총괄하기 위하여 연방 정보기술안전청을 설치하도록 한다.

(§4) IT보안을 위한 중앙 사무국

IT보안에 대한 사안들을 총괄적으로 관리하기 위한 중앙 사무국을 설치하도록 한다.

(§12) 연방정부 부처 최고 정보 책임자 회의

연방정부의 정보기술에 대한 사항과 관련 문제 시 결정이 필요한 사항에 대해 효율적인 처리와 합리적인 결정을 위하여 연방정부 부처 최고 정보 책임자 회의를 구성해

95) BSI Act - BSIG 2009

야 한다.

- 안전관리 체계 마련

(§3-(1)-13) 타 기관 지원 및 연계

a) 경찰과 검찰 당국이 합법적으로 명령 한 임무를 수행한다. b) 헌법 보호를 위한 당국 테러리스트 활동의 감시 또는 정보 분석 및 평가에 대한 연방 및 주법에 의해 허가 된 활동을 수행한다. c) 연방 정보국 (Federal Intelligence Service)으로부터의 합법적인 임무를 수행한다.

- 안전점검 및 안전 조치

(§4-(2)-1) 취약점 분석 및 평가

IT 보안에 대한 위협을 방지하기 위해 필요한 모든 정보를 수집하고 평가하고 특히 보안 취약점, 악성 소프트웨어, IT 보안에 대한 공격 시도의 추이 분석과 공격에 성공하기 위한 수단을 분석한다.

(§3-(1)-2) 예방조치

보안 위험 및 보안 예방 조치에 관한 정보 수집 및 분석 필요에 따라 다른 기관에 결과를 제공하여 업무를 수행하거나 그들의 안보 이익을 보존한다.

(§3-(1)-5, §6) 정보 기술 시스템의 보안 테스트 및 평가

정보 기술 시스템의 보안 테스트 및 평가를 통해 보안 인증서를 발급하고, IT보안 표준 준수 가이드라인을 제시한다.

- 안전관련 산업의 육성과 안전문화 활동 지원

(§3-(1)-3) 정보기술사용과 관련된 보안 위험 연구

보안 예방 조치의 일환으로 정보 기술 프로세스 개발 및 IT 보안 제품 (IT 보안 제품) 의 연구를 법적 의무에 포함한다.

(§3-(1)-4) IT 보안 표준제시

보안 테스트 및 평가를 위한 기준 및 절차를 정하고 평가도구 개발과 구성 요소를 평가하는 방법을 제시한다.

2) 대응 단계

- 대응 체계 구축·운영

(§3-(1)-15) 위기 대응 및 조정을

위기를 인식하고 위기 대응 및 조정을 위한 민간 업계와 연계한 정보 인프라를 구축한다.

- 응급조치

(§4-(2)-2) 통지

침해사고 및 공격 발생 시 연방 당국에 즉각 관련 사실을 통지하도록 되어있다.

4. 법제 분류 결과 및 시사점

독일의 『BSI설립에 관한 법률』 조항들을 안전관리 관점의 분류 기준으로 분류한 결과, 예방 단계는 안전관리 기구 및 조직 구성 조항 3개, 안전관리 체계 마련 조항 1개, 안전점검 및 안전조치 조항 4개, 안전관련 산업의 육성과 안전문화 활동 지원 조항 2개로 총 10개의 조항이 있는 것으로 분석되었다. 대응 단계는 대응 체계 구축·운영 조항 1개, 응급 조치 조항 1개로 총 2개의 조항이 기술되어있었다.

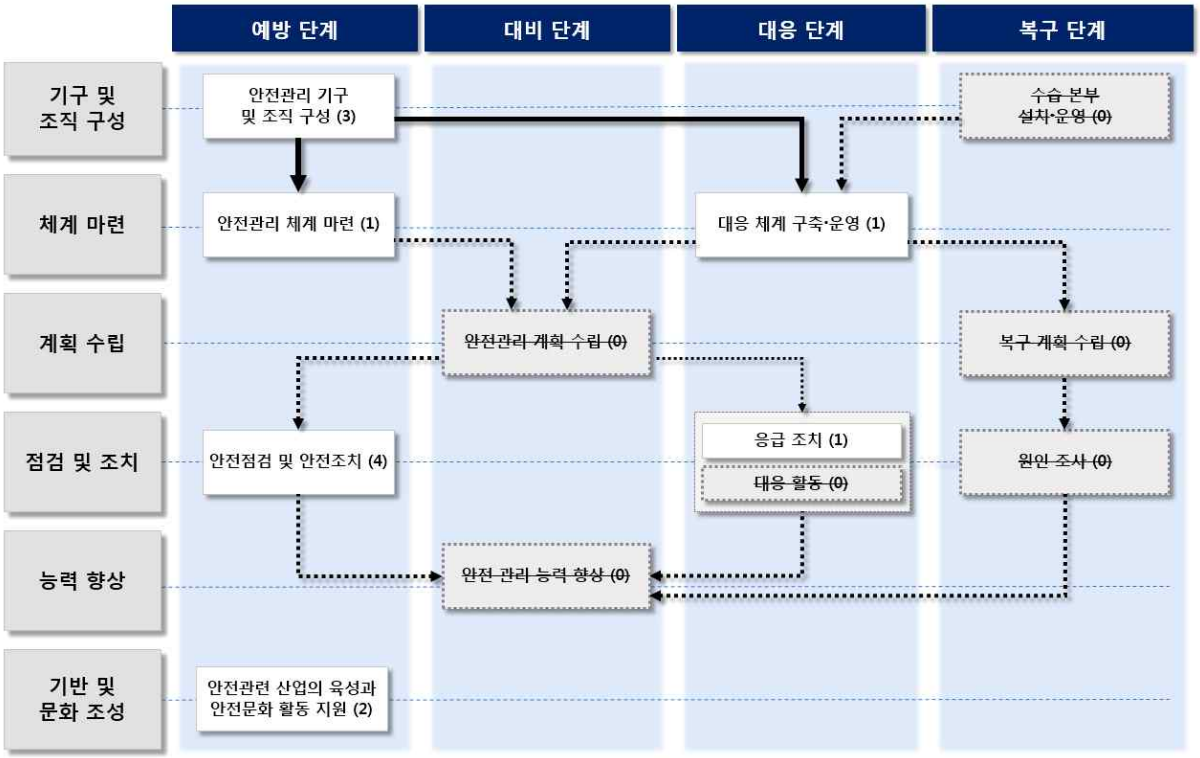
『BSI설립에 관한 법률』은 예방과 대비에 대한 역할을 주로 맡고 있는 BSI의 설립과 기능에 대해 규율하는 법률이기 때문에 대비 단계와 복구 단계에 해당하는 조항은 포함되어 있지 않았다. 『BSI설립에 관한 법률』에 기재되어 있지 않은 대비 단계와 복구 단계에 해당하는 규율에 대해서는 BSI, BBK 등 기반보호와 직접적, 간접적 연관을 갖는 각 기관들에서 발표하는 지침이나, 연방 내무부의 국가 중요기반시설보호에 관한 CIP전략을 통해 규율되고 있다. 특히 대응 및 복구에 있어서는 민방위법에 의한 안전관리 체계와 연동하여 규율되고 있다.

『BSI설립에 관한 법률』의 조항들을 안전관리 관점에서 분류한 결과는 다음과 같다.

<표 4-17> 안전관리 관점에서의 독일「BSI설립에 관한 법률」조항 분류 결과

안전관리 단계	세부 활동 영역	법률 조항	내용
예방 단계	안전관리 기구 및 조직 구성	§1	• 연방 정보기술안전청 설치
		§4	• IT보안을 위한 중앙 사무국 설치
		§12	• 연방정부 부처 최고 정보 책임자 회의 구성
	안전관리 체계 마련	§3-(1)-13	• 타 기관에 대한 지원 및 연계 체계 마련
	안전점검 및 안전 조치	§4-(2)-1	• 취약점 분석 및 평가
		§3-(1)-2	• 보안 위험 및 보안 예방 조치 수행
		§3-(1)-5, 6	• 정보 기술 시스템의 보안 테스트 및 평가
	안전관련 산업의 육성과 안전문화 활동 지원	§3-(1)-3	• 정보기술사용과 관련된 보안 위험 연구
		§3-(1)-4	• IT 보안 표준제시
대비 단계	안전관리 계획 수립	-	-
	안전관리 능력 향상	-	-
대응 단계	대응 체계 구축·운영	§3-(1)-15	• 위기 대응 및 조정을 위한 인프라 구축
	응급조치	§4-(2)-2	• 침해사고 및 공격 발생 사실 통지
	대응 활동	-	-
복구 단계	수습 본부 설치·운영	-	-
	복구 계획 수립	-	-
	원인 조사	-	-

[그림 4-7] 독일 「BSI설립에 관한 법률」의 안전관리 관점의 세부 분류 단계별 활동 흐름도



독일 『BSI설립에 관한 법률』은 예방 단계에 해당하는 활동에 대한 조항들이 대다수를 차지하였는데, 특히 연방 정보기술안전청, IT보안 중앙 사무국, 최고 정보 책임자 회의에 대한 구성 및 운영에 대한 부분은 우리나라에서도 SW 안전 관리 위원회와 그 기능 및 운영에 대한 내용을 제정할 시 참고할 수 있을 것이다. 또한 경찰, 검찰, 연방 정보국 사이의 유기적인 지원 및 연계 체계가 잡혀있는 점도 SW 안전 관련 사고의 비상 대응 시 협조요청에 대한 사항에 대한 조항을 신설할 때 본받을 수 있는 부분이다. 안전과련 산업의 육성과 안전문화 활동 지원에 해당되는 IT 보안 표준제시 조항도 눈여겨볼 만 하다. 동법의 해당 조항과 미국의 NIST에서 연구하고 있는 표준 제시와 같은 부분은 빠르게 변화하는 SW 중심 사회에서 SW 안전 산업의 제도적 기반을 구축하고 명확한 소프트웨어 안전 개념을 공유하기 위하여 상당히 중요한 부분이기 때문에 우리나라에서도 SW안전관리원(가칭)과 같은 기관을 설립하여 SW 안전 관리 시스템 구축을 위한 기술표준, 방법, 구축 단계 및 절차를 지원하는 기능을 부여하는 것이 바람직할 것으로 생각된다.

제5장 SW 안전 확보를 위한 법제도 개선 방안

제1절 개관

국내외 기반시설보호 관련 법제들을 분석해본 결과, 공통적으로 국가들은 재난 대비 차원, 안보 차원, 외부침해사고 대비 차원 등의 관점으로는 관리 체계를 일부 마련하고 있으나, SW의 내부결함으로 인한 사고 대비, SW 안전 관리의 관점의 보호 체계는 대부분 미비한 실정인 것을 알 수 있었다. SW 안전 확보를 위한 활동이 미비한 원인 또한 SW 안전 관리의 실질적 수행을 위한 법적 근거가 갖추어지지 못한 것이 중요 원인 중 하나라고 지적된다.

SW 중심 사회가 본격적으로 도래하기 전에 만들어진 현재의 국내 기반시설보호 법제도는 SW 안전에 대한 관념을 충분히 반영하지 못하고 있는 것으로 보인다. 대부분의 국가 안전보호를 위한 법제 내에는 SW의 내부결함 등으로 인해 생길 수 있는 문제들에 대한 위험 관리 조치들을 수행할 수 있도록 적용할 수 있는 조항이 거의 없으며, 이 때문에 국가가 SW 안전 관리의 관점에서 기반시설을 규제하고 관리할 수 없고 유관 사고에 대한 유기적인 대응도 불가하다. 해당 문제들을 해결하기 위하여 주요기반시설의 SW 안전을 확보하기 위한 법제도의 변화가 요구되며, 주요기반사업의 분야별로 산재되어 있는 SW의 안전을 관리 및 규율할 수 있는 법안 마련이 필요함을 알 수 있었다.

이는 전자적 침해행위에 대비한 주요정보통신기반시설 보호에 관한 내용을 다루고 있는『정보통신기반보호법』의 일부 내용을 추가·수정하여 SW 안전 관리의 관점을 포괄할 수 있도록 개정하는 방법으로 개선될 수 있을 것이며, 나아가 기존의 한정되어 있었던 국가의 규율 범위를 확장하여, 주요기반시설의 SW 안전 전반을 망라적으로 규율할 수 있는 일반법을 제정하는 방안을 고려해볼 수도 있다.

본 장에서는 SW 안전 확보를 위한 법제도 개선 방안을 구체적으로 제시하기 위하여 실제 입법 성공을 위한 법제의 배경과 목적을 명확히 하여 입법체계를 정립하고, 현 법제에서 미비한 부분에 대한 주요 제도개선 과제를 도출하고자 한다. 또한 법안 통과 확률과 절차적 효율성을 높이기 위하여 구체적 입법전략을 제시하여 향후 실제 입법 과정에 도움을 주고자 한다.

제2절 입법체계 정립

1. 정보통신기반보호법 개정을 통한 공공분야 소프트웨어 안전 강화

실현 가능한 규범 적용 영역으로서 공공부문의 소프트웨어 중심의 안전 관리체계 보완하여야 한다. 정보통신기반보호법은 '정보통신 기반시설'을 중심으로 물리적, 논리적 보호를 예정하고 있는데, 특정 시설, 혹은 대상이 되는 물리력을 통제하고 운용하는데 활용되는 소프트웨어의 안전 관리가 요청되는 상황에서 보호 대상의 확장 혹은 전문화 하는 형태로 개선 필요한 상황이다.

공공분야는 구체적 의무사항을 정하기 용이하고, 해당 의무사항의 준수여부에 관한 검토 및 점검도 법으로 정하여 관리가 가능하다. 또한 안전 기준의 준수, 안전 점검, 취약점 분석 평가, 사고 대응을 위한 역할 분담 및 권한 조정 등 수범 대상을 공공기관 등으로 한정하는 경우 규범 형성을 효율적으로 추진할 수 있다. 이 때문에 필수적 공공부문의 소프트웨어의 기능이 유지되면, 최소한의 국민생활이 보장될 수 있으므로 안전 관리의 대상을 필요최소한의 범위로 한정할 수 있다. 그러나 법률로 민간영역에서 사적(私的) 행위로 소프트웨어를 선택하고 활용하는 내용 까지 규율하는 것은 적합하지 않을 수 있다는 평가나 현실적으로 가능하지 않다는 견해도 존재할 수 있음을 고려하였다. 이에 국민 생활의 기본적 요건이 달성될 수 있을 정도의 기반 시설의 안전을 확보하는 차원에서 소프트웨어 안전 관리의 범위를 한정한 개정 방향을 설정하였다.

2. 소프트웨어 안전 관리에 관한 법률 제정을 통한 지능정보사회 전반의 안전성 제고

지능정보사회에서 소프트웨어의 활용 범위가 국민생활 전반으로 확장되고 있다. 소프트웨어의 활용 범위가 주요 기반 시설에 한정되는 것이 아닐 뿐만 아니라, 국민들의 일상에서도 소프트웨어의 부재로 인해 발생 가능한 생명, 신체, 재산상의 피해가 예상 되는 만큼 우리 사회 전반에 대한 소프트웨어 안전 관리가 요청되고 있는 상황이다.

또한 소프트웨어에 대한 의존성이 심화되는 만큼 소프트웨어의 운용 가능성을 확보하는 측면의 안전 관리 방안이 요청된다. 지능정보사회에서의 소프트웨어의 역할은

그 중요성이 상당하고, 새로운 산업혁신의 동력으로 여겨지는 만큼 소프트웨어의 안정적 활용 가능성을 보장하는 것이 국가의 역할 범위 안에 포섭된다고 할 수 있을 것이다. 이 때문에 구조적 위험을 제거하고 안전하게 소프트웨어 활용의 편익을 향유할 수 있도록 국가의 역할과 책임을 법률로서 선언하고 확정하는 것이 필요하다.

결국, 최종적으로는 소프트웨어 안전 관리 차원의 일반 규율(법률)이 필요할 것이며 해당 규율을 통해 정보보호 및 정보보안 중심의 관리 체계에서 소프트웨어 중심의 관리 체계로의 전환과 소프트웨어의 개발·보급 및 산업적 관리에 한정되었던 국가의 역할 확장을 도모하여야 할 것이다.

제2절 주요 제도개선 과제

1. 침해 사고 및 위기에 대한 예방, 대응 및 복구의 체계화

소프트웨어 안전 관리의 구조를 예방, 대비, 대응 및 복구의 체계로 구성하고 각 단계별 관리방법에 관해 구체적으로 규율하여야 할 필요가 있다. 개별 단계에서 요구되는 프로세스를 상세하게 마련하고 준수하도록 하여 구조적인 침해나 위기로 인한 사고 발생을 최소화하여야 하며 구체적 단계별 요구사항이 상이한 만큼 세분화된 안전 관리를 통한 소프트웨어 안전 관리의 질적 효과 제고가 필요하다. 소프트웨어 안전 관리에 관한 연구 및 대응 기술 개발 등도 이와 같은 체계에 맞추어 개발할 수 있도록 정책적으로 연계시켜야 하며, 사고발생의 억제와 사고 발생 이후 소프트웨어 운용의 항상성을 함께 고려할 수 있는 체계의 구축이 요구된다.

국가 및 사회의 유지를 위해 필요한 중요분야별 소프트웨어의 기능이나 주요 관리 대상이 상이한 만큼 특성을 고려한 예방 체계 구축도 필요하다. 소프트에어의 활용 범위 및 사용 대상이 개별 분야마다 상이한 만큼 요구되는 소프트웨어의 안전성 기준을 구체적으로 정할 수 있도록 해야 하며, 소프트웨어의 기계적 안전성 등에 관하여 점검하고 조사할 수 있도록 하여 침해 기술의 발전에 대응하여 안전수준을 적절히 유지하고 있는지에 대한 분석과 검토가 선행되어야 한다.

또한 실효성 있는 대비를 위한 탐지업무의 수행과 신고 및 통지 의무를 마련해야 한다. 침해 위협이나 위기 발생의 양태가 특정되지 아니하고, 복잡성을 띠는 것이 특징인 만큼 유연한 대응을 위해 침해나 위기와 관련한 포괄적인 정보의 수집 및 분석이 요청되며, 소프트웨어안전관리시스템 구출을 통해 위기 예측 및 분석을 실시하

여야 한다. 빅데이터 기술 활용 등으로 탐지 역량을 강화하는 방안도 고려할 수 있을 것이다.

소프트웨어 안전 관리의 핵심이 예방에 있는 것이 사실이나, 현실적으로 소프트웨어의 운용 상태를 유지하는 것도 필요하므로, 필요최소한의 지속적인 운용가능성을 확보할 수 있는 긴급하고 영향력 있는 대응체계를 갖출 필요가 있다. 이를 위해서는 사고 발생 및 징후 발견에 대한 신고 및 통지 의무 마련하여야 하고, 사고대응 매뉴얼(안전관리지침) 설정을 통해 효과적인 대응체계를 구성하여야 하며 대응 및 복구에 관한 과정을 기록으로 남겨 향후 대응에 있어 개선사항을 발굴해야 한다. 나아가 사고 대응 훈련, 긴급대응이 요청되는 경우의 특례 등을 정하여 유연하고 실효성 있는 소프트웨어 안전 관리 체계 마련되도록 해야 할 것이다.

신속한 복구를 위한 지휘체계의 법정화 및 중요분야별 협력체계 마련도 필수적이다. 미래창조과학부와 소프트웨어안전관리원의 전문적 복구 지원 하에 사고와 관련한 사실조사 및 실태조사 실시를 통한 원인 규명 및 안전 관리 개선 사항 분석이 필요하다. 또한 이를 토대로 개선 요구사항의 발굴과 안전 관리 체계의 발전이라는 선순환 구조를 구축하는 것이 바람직하다.

2. 안전한 소프트웨어 관리체계 수립을 위한 컨트롤 타워 정립

공공부분이 정보통신기반보호법 및 국가사이버안전관리규정에 따라 관리되고 민간부분은 정보통신기반보호법 및 관련 법령에 따라서 미래창조과학부 장관이 필요한 사항은 관장함에 있어 발생하는 비효율 및 안전관리를 위한 지휘체계의 혼란이 존재할 것으로 예측된다. 또한 침해사고가 발생하는 경우, 공공과 민간을 구분하지 않고 동시성을 가지고 무차별적으로 효과를 발생하는데 비하여, 관리체계가 규범적으로 분리되어 있어 집행의 일관성을 기대하기 어렵고, 신속한 대응을 요구하는 소프트웨어 안전 관리의 특성에 적합하지 않는 구조라는 비판이 있어왔다.

고로, 소프트웨어 관련 정책을 총괄하고 및 정보보호와 정보보안 기술을 전담하는 중앙행정기관인 미래창조과학부를 중심으로 구체적인 연구 및 위기대응 역할을 수행하는 소프트웨어안전관리원을 설립하여 직관적이고 일관성 있는 정책 수립과 집행, 구체적 안전 관리 업무 수행이 연계될 수 있도록 구성하였다. 미래창조과학부장관은 침해사고 및 위기 대응을 위한 각종 시책 및 안전 관리 방안의 마련뿐만 아니라, 적극적 침해요소의 배제행위를 위한 역추적 및 탐지체계를 구성할 수 있도록 하여 소

프트웨어 안전과 관련한 총체적인 역무를 가질 수 있도록 하였다.

또한 국가사이버안전규정에 근거하여 국가정보원장이 구성하여 운영하던 국가사이버안전센터기능과 관계없이 소프트웨어안전관리시스템을 구성하고 탐지 업무 등에 활용하도록 하여 혹여 발생할 수 있는 권한 남용 및 제한과 관련하여 국회의 접근 및 감시 가능성을 확보하도록 하였다.

기존의 정보보호와 관련하여 한국인터넷진흥원이 인터넷진흥 및 개인정보보호 일부, 국제협력과 정보보호 및 사고대응 업무 등을 가지고 있으나, 소프트웨어 안전 관리와 관련하여 전문영역을 구축하여 전담할 수 있는 소프트웨어안전관리원을 새롭게 설립하여 전문적이고 구체적인 역할(침해 탐지, 대응 및 위기 억제, 사고 조사 등)을 수행하도록 하였다.

3. 기술 인력의 전문성과 직접 고용에 관한 법정화

소프트웨어 안전 관리 직무를 수행함에 있어 전문성을 확보하여, 관리 인력의 질적 담보를 갖추고, 직무의 안정성과 연속성, 보안성을 만족시키기 위해 직접 고용을 하여 신분을 보장하는 형태의 고용관계 사항을 법정화하였다.

기술적 수요 등과 관련해서는 그 변경가능성을 고려하여 시행령에서 구체적으로 확정하도록 위임하였으며, 조직 경영의 효율을 이유로 안전 관리 직무 수행을 제3자에게 위탁하는 경우 발생하는 불이익과 사고 발생 가능성의 악영향이 보다 크다고 판단, 직접고용으로 직무 만족도를 제고하고 안전 관리 직무 수행의 전문성을 적극 활용하도록 하였다.

4. 안전기술의 보급과 전문 인력의 양성

소프트웨어 안전 관리와 관련하여 침해 기술의 발전에 대응하고, 위기 발생의 변수를 보다 정확히 예측하기 위하여 관련 기술의 연구와 보급이 지속적으로 유지 관리될 필요가 있다. 이에 소프트웨어안전관리원으로 하여금 기술의 조사 및 연구를 지원하도록 하여 기술력을 제고하고 해당 기술내용을 토대로 침해 대응 및 안전 보장을 위한 훈련을 실시 지원케 해 기술의 연구과 현실 안전 관리 역무의 실현에 통일성을 갖도록 하였다. 구체적 기술력이 사업자에게도 연계되도록 하여 공공 및 민간 전반의

기술적 안전 관리 역량이 강화 되도록 한 것이다. 또한, 전문 인력의 지속적 양성을 위하여 미래창조과학부 장관으로 하여금 교육프로그램을 개발하고 교육부 등 관계 부처와 협의하여 대학 및 연구소 등을 활용해 전문성을 확보할 수 있도록 하였다.

제3절 입법 전략 제시

1. 정부 및 의원 입법과정의 고려

입법추진은 정부 및 의원입법의 방법 중에서 선택할 수 있으며, 헌법 제52조[96]는 정부에게 법률안제출권을 부여하고 있다. 실제로, 입법과정에서 정부제출 법률안의 통과비율은 매우 높은 편에 속한다.

정부가 법률안을 입안하는 과정은 국회의원이나 정당의 경우에 비하여 다소 복잡하며, 다음과 같은 순서로 진행된다.

- 해당 부처 내 담당부서의 입법정보 수집·분석과 입법정책의 결정
- 초안(부처안)의 작성
- 관계부처와의 협의 및 의견수렴
- 당정협의
- 입법예고
- 규제개혁위원회 심사 등 각종 사전심사
- 부처의 원안결정
- 법제처 심사
- 차관회의·국무회의 심의
- 대통령 재가 및 국회제출

이러한 과정에서 명확한 입법필요성과 골자가 강도 높게 심사·검토되고, 법안의 내용에 따라 부처협의 과정상 알력과 주도권 다툼이 대부분 도출되므로 결국 입법을 추진하는 담당부처의 역량과 의지가 입법성공의 열쇠라 할 수 있다.

한편, 의원입법을 통하게 되면 비교적 간소한 절차와 함께 사회공감대 형성여부와 의원역량에 따라 강력한 추진력을 얻을 수 있다는 점에서 정부입법에 비해 강점이라

96) 헌법 제52조 국회의원과 정부는 법률안을 제출할 수 있다.

할 수 있을 것이다.

2. 정부입법

정부입법은 주무부처의 법령안 성안 및 검토과정이 완료되면 중앙부처와 지방자치단체 등 관계기관과의 협의 후 의견수렴을 거치게 된다. 이 과정에서 국회에서의 원활한 입법추진의 필요성이 있거나 정치적 현안이 포함된 경우 당정협의를 거칠 수 있다.

이러한 과정을 통해 법률안이 지속적으로 수정·보완되며, 이후 국민의 다양한 의견수렴을 위해 긴급한 경우를 제외하고 기간은 20일 이상 동안 입법예고를 시행하고 법률(안)을 확정하게 된다. 확정된 법률안은 규제심사위원회의 규제심사 및 성별·부패영향평가를 실시하여 관련된 사항의 수정과 삭제과정을 거치며, 최종안에 대하여 입법내용의 현실·적법 타당성과 국정과제와의 합치성 여부, 상위법이나 관련 제도간의 상충 여부 등 실질적인 사항과 그 자구·체계 등 형식적 사항에 대한 심사를 위하여 법제처 심사를 거친다. 법제처 심사를 원활하게 통과하면, 차관회의(국무회의에 상정될 의안의 중요사항 사전심의)와 국무회의를 거쳐 대통령의 최종재가에 따라 국회 소관 상임위에 제출된다.

국회입법과정에서 공청회를 개최하거나 이해관계인의 의견을 청취하며, 법제사법위원회와 본회의를 통과하면 정부에 재차 이송되어 다시 국무회의와 대통령재가를 거쳐 법제처를 통해 공포되면 입법절차는 완료되게 된다. 각 입법절차별 소요기간은 아래 표와 같다.

<표 5-1> 정부입법과정 진행단계별 소요기간
(*는 법령에 따라 일정하지 않은 경우)

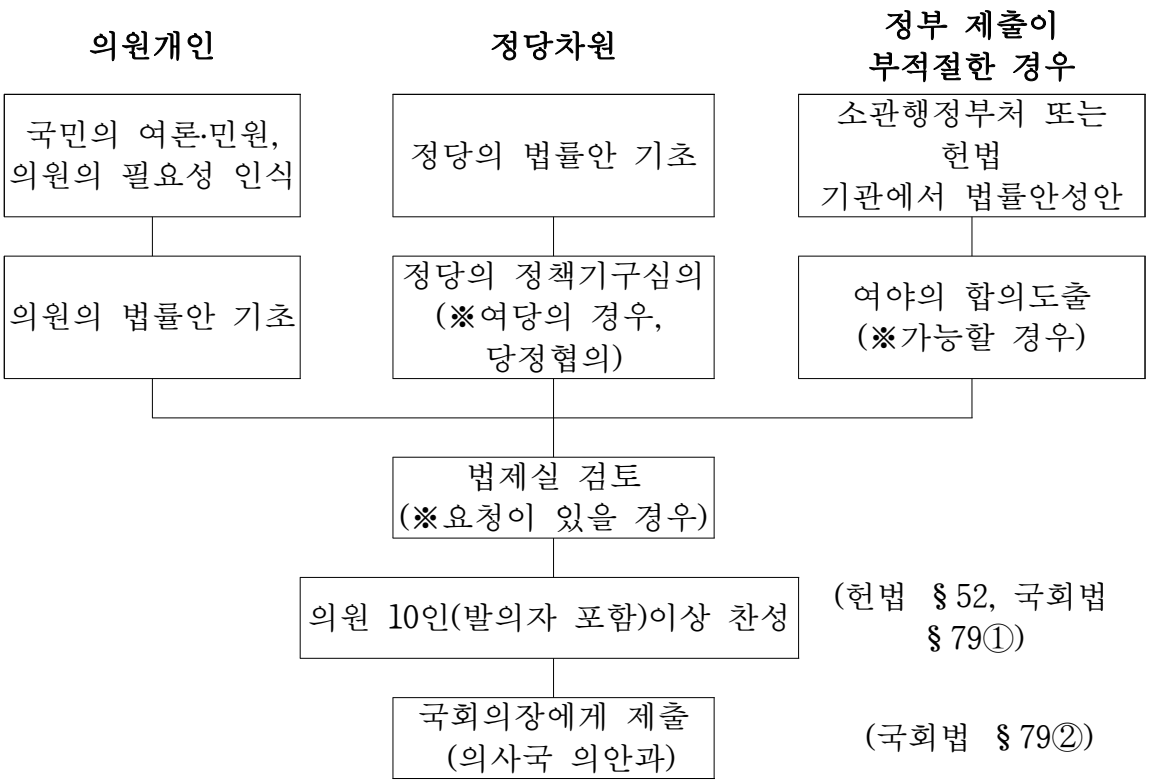
입법절차	소요기간
소관부처 법령안 초안 작성	약30 ~ 60일*
관계기간 협의	약30 ~ 60일*
입법예고 등	약20 ~ 40일 (국민의견 수렴을 위해 공청회를 거치는 경우가 많음)
법제처 심사	약20 ~ 30일*
차관회의 상정·통과	7 ~ 10일
국무회의 상정·통과	5일

대통령재가·법제처 송부	7 ~ 10일
국회 과정	30 ~ 60일(장기간 계류되는 경우는 예외)
관보게재의뢰·공포	3 ~ 4일

3. 의원입법

의원입법은 ① 순수의원발의 형식의 경우, ② 정부 또는 제3자가 기초하여 제공하는 안을 근간으로 의원이 입안하여 제출하는 경우, ③ 정부가 마련한 안을 의원을 통하여 제출하는 경우, ④ 연구원, 관련단체 등이 마련한 법률초안을 의원을 통하여 제출하는 경우 등 그 입안과정이 다양한 것이 특징이다.

<표 5-2> 의원발의법률안의 입법과정



의원개인이 마련한 입법안의 입법절차의 경우 국민의 여론·민원, 의원의 필요성 인식에 따라 법률안의 기초안을 마련하고, 필요한 경우 법제실의 검토를 통해 체계나 자구에 대한 보완작업을 실시하게 된다. 마련된 법률안은 의원 10인(발의자 포함) 이상의 찬성을 통해 국회의장에게 제출되며, 소관 상임위에 회부되어 필요할 경우 공청회 개최 및 이해관계인의 의견 청취하고, 법제사법위원회와 본회의를 거쳐 정부에 이송된

후 국무회의와 대통령 재가를 거쳐 공포된다.

한편, 정당차원의 법률안 마련은 정당이 법률안의 기초를 마련하고, 정당의 정책기구 심의(여당의 경우 당정협의)를 거쳐 법률안이 마련된다는 사항 외에 이후 절차는 위와 동일하며, 기타의 경우에도 의원개인이 마련하는 입법안의 입법절차와 대동소이하다.

4. 입법절차별 장·단점

1) 정부입법의 경우

- 관계부처 협의를 통한 실무연계 및 전문성 확보

정부입법을 추진하는 경우 해당 규범의 시행으로 인한 공공기관의 의무이행 사항 및 행정절차에 관하여 구체적인 규제체계의 영향평가 등을 통한 검토가 가능하다. 직접적으로 행정청의 의무이행에 관한 사항이므로 현실적이고 전문적인 검토가 가능할 것이다. 이는 현장에 적합한 수용력 있는 규제 설계가 가능하다는 의미이며, 규제설계에 있어서 보다 전문성 있는 규범 형성이 이루어질 수 있다.

- 의견수렴 등의 절차 수행으로 인한 시간 소요

위와 같이 다양한 부처의 복합적인 의견이 반영되는 경우 이를 다시 수용할지 여부를 판단하고, 부당한 주장을 선별하는 등의 절차를 거쳐야 하는 만큼 입법절차를 완료하는 데 있어 시간이 상당히 소요될 수 있다.

시급한 환경 변화에 대응하는 정책 입법의 경우 부처 등을 설득하고, 이해를 구하는 절차로 인하여 정책 수요를 적정한 시기에 만족할 수 있는지 여부에 관하여 확실성이 저조해 질 수 있을 것이다.

- 행정편의적 요소의 의견 제기

행정 내부에서 마련한 법률안에 관하여 의견 수렴을 거치다 보니, 공공데이터법과 같이 적극행정을 요하는 규범사항에 관하여 행정 편의적인 개선의견이 다수 발생할 가능성이 있다.

소극적 행정으로 인하여 당초의 정책 목적을 이루지 못할 수도 있고, 이를 극복하기 위하여 설득을 거치는 절차를 이행하는 경우에는 위에서 제기한 바와 같이 적정한

정책 수요를 달성할 수 있는 시기를 놓치는 부작용이 있을 수 있다.

2) 의원입법의 경우

- 민주적 정당성 확보

국회는 대의기관으로서 국민에게 적용되는 법률을 형성하는 역할을 본래적으로 수행하며, 국민의 의사를 대변하는 국회를 통해 형성된 법률의 내용은 기본적으로 국민생활의 편의를 확보하고, 공공데이터의 이용환경을 이용자 친화적으로 개선하는데 그 내용적 기반을 둘 것으로 예정할 수 있다.

원칙적으로 국무회의를 거쳐 국회로 송부되는 정부입법의 방식 또한 국회 본회의를 거쳐 가결 여부가 결정되는 만큼 규범의 설계 및 법률안의 형성이 국회의원을 통해 이루어지는 경우 민주적 정당성이 보다 두텁게 확보된다고 할 수 있을 것이다.

- 절차적 효율성

형식상 법률개정에 이르는 과정에 있어서 의원입법의 절차가 정당한 절차를 생략하거나 간소화 하는 것은 아니다. 하지만, 국회의 본래 역할이 국민의 권리의무와 관련된 법률의 제정에 관한 사항인 만큼 정부입안의 과정과 같이 권리 침해적 요소가 있는지 여부에 관하여 심사하거나 평가하는 과정이 추가되지 않고, 본래의 국회 입법 형성 절차에 따르게 된다. 이러한 경우 정부입법의 과정에 비해 특이사항이 없는 경우 신속한 법률개정의 효과를 기대할 수 있을 것이다.

5. 정책 제언

소프트웨어 안전 관리에 관한 법률의 내용 및 정책 환경이 아직까지는 공공의 의무 이행을 강제하는 성격의 규범적 효과를 가져야 민간에서의 소프트웨어 안전 환경이 조성될 수 있을 것으로 기대되는 만큼 미래창조과학부의 정책적 판단과 방향을 구현한 내용을 통해 의원입법을 추진하는 것이 보다 효과적인 목적 달성을 이룰 수 있을 것으로 기대된다.

또한, 신속하게 입법을 완료하여 새로운 정책 컨트롤 타워의 구성 등을 도모한다는 측면에서도 바람직하다고 판단된다.

제5장 결론

본 연구는 문제가 생길 시 국가·사회·경제에 중대한 피해를 미칠 수 있는 주요기반시설에서 활용되는 SW의 안전을 확보하기 위해, 안전관리 관점에서의 기반시설 보호 법제도 개선 방향 및 개정안을 마련하는 것을 목적으로 수행되었다. 해당 목적을 달성하기 위해 우선적으로 SW 안전의 의의와 정책 체계를 이해하고자 하였으며, 국내 및 해외 주요국의 주요기반시설보호 법제를 분석하고, 안전관리 관점으로 분류하는 작업을 통해 새로운 법제를 만들기 위한 시사점 및 개선 방향을 도출하였다.

안전관리 관점의 법제 분류 기준은 '국가기반체계 보호관련 중앙재난안전대책본부 운영 및 상황관리 규정' 에서 정의하고 있는 (예방-대비-대응-복구)의 4단계 안전관리 활동을 기반으로 구성하였고, 이와 관련한 보고서 및 논문 등의 연구를 토대로 세부 분류 단계 및 내용을 수립하였다.

수립한 분류 기준을 통해 국내 기반보호 법제의 중심이 되는 법인 『재난 및 안전관리 기본법』과 『정보통신기반보호법』, 그리고 국가주요기반시설의 분야 중 원자력 안전과 관련된 법률들을 대표적으로 선별하여 분석하였다. 해당 법률들을 분석 및 분류한 결과, 대부분의 조항들이 안전관리 기구 및 조직 구성, 안전관리 체계 마련, 안전점검 및 안전조치, 안전관련 기반 조성, 안전관리 계획 수립 등 잠재적인 위험을 예측하고 사전 조치를 취함으로써 위험으로부터 발생할 피해 규모를 최소화시키는 활동들인 예방 단계에 집중되어 있는 것으로 나타났다. 예방 단계에 속하는 조항들이 공통적으로 전체 조항의 절반 이상을 차지한 것으로 보아, 우리나라의 국가 안전보호 법제 조항들이 예방 단계에 집중되어 있다는 사실을 알 수 있었으며, 이는 정부가 오래토록 추진해온 예방 위주의 재난/사고 관리 대책의 성과라고 생각된다. 또한 각 법제 분류에 대한 결과를 통해 안전관리 관점의 세부 분류 단계별 활동 흐름을 파악할 수 있었으며, 각각의 법률의 목적이나 필요에 따라 타 법률들 보다 체계적으로 구성된 부분들은 SW 안전 전반을 규율할 수 있는 법제를 새로 구성할 시 더욱 집중적으로 참조할 수 있을 것으로 생각된다. 기존 법제의 분석 및 분류를 통해 SW 안전에 대한 규율이 추가적으로 필요한 부분들을 파악하기에 용이하였으며, 이러한 검토 과정을 통해 자칫 중복 규제가 되어 기관 및 기업들의 업무 효율성 저하로 이어질 가능성을 줄일 수 있을 것이다.

해외 주요국의 주요기반시설 보호 법제는 국내와 같은 안전관리 관점의 법제 분류

기준을 적용하여 분류해보았지만, 각 국의 법 체계 특성상 동일한 수준의 결과를 얻어내는 것은 쉽지 않았다. 국내는 법률을 기반으로 대부분의 국가기반시설의 안전을 규율하고 있었지만 해외 주요국들은 계획이나 가이드라인을 통해 실행력의 신속성을 확보하고자 하는 특성 등이 존재하였기 때문이다. 그러나 해외 주요국들도 공통적으로 법제 분류 기준의 큰 틀인 예방, 대비, 대응, 복구의 안전관리 관점에 입각하여 국가재난 및 비상사태에 대한 대비 체계를 구축하고 있었으며, 해당 분석 및 분류를 통해 각 국의 기반시설 보호 체계의 강점과 우리나라의 법 구성 시 참고할 점들을 엿볼 수 있었다.

국내외 기반보호체계 법률 분석 결과, 각 국가마다 재난 대비 차원, 안보 차원, 외부침해사고 대비 차원 등의 다양한 관점에 기반한 법제 체계를 갖추고 있었지만, 그 중 SW의 내부결함으로 인한 사고 대비 등 SW 안전 관리의 내용을 포괄하여 규정할 수 있는 법률 및 세부 조항을 가지고 있지는 않았다. 따라서 국가주요기반시설의 안전을 규율하는 법률 내에 SW와 관련될 수 있는 조항들을 도출하고 SW의 범위와 유형을 정립하여 국가주요기반시설의 SW 안전 전반을 규율할 수 있는 법제 제정 및 개선의 필요성을 확인할 수 있었다.

본 연구는 SW 안전 확보를 위한 법제도 개선방안 연구를 통하여 공공분야 소프트웨어 안전 강화와 지능정보사회 전반의 안전성 제고를 위한 정보통신기반보호법 개정안과 소프트웨어 안전 관리에 관한 법률 제정안을 제시하였으며, 실제 개정안 및 제정안은 부록으로 첨부하였다. 제시한 해당 법률안에 침해 사고 및 위기에 대한 예방·대응 및 복구의 체계화, 안전한 소프트웨어 관리체계 수립을 위한 컨트롤 타워의 정립, 기술 인력의 전문성과 직접고용에 관한 법정화, 안전기술의 보급과 전문 인력의 양성과 같은 현 국내 법제의 주요 제도개선 과제들을 포함시키어 향후 쟁점이 될 수 있는 사항들을 우선적으로 포괄하고 있는 법안이라고 할 수 있을 것이다. 또한 본 연구에서 제안한 법제 개선안은 학계, 연구계, 실무계 등 폭넓은 분야의 전문가로 구성한 연구자문진의 의견 수렴과정을 거쳐 법제 개정안 및 제정안 도출의 절차적·내용적 정당성을 확보하고자 노력하였다.

해당 법률 개선안이 실제 기반시설의 SW 안전보호 체계 개선 작업의 시작점이 될 개정입법추진 과정의 이론적 토대로 활용될 수 있을 것으로 생각되며, 입법과정에서 제기될 다양한 의견들을 반영하고 대응하기 위한 기초 자료로 활용되기를 기대한다.

참 고 문 헌

국내 문헌

1) 강문수, “위험사회에서의 입법”, 「토지공법연구」 제32집, 한국토지공법학회, 2006.
2) 권영빈, “영국의 사회적 안전규제”, 2014년 2/4분기 국내외 규제 동향지, 한국행정연구원, 2014.
3) 김경호, “지방자치단체 재난관리체계의 단계별 개선방안에 관한 연구 : 대구광역시 사례를 중심으로”, 「한국행정논집」, 제22권 제1호, 2010.
4) 김윤명, 박태형, 이현승, “소프트웨어산업 진흥법 개정 연구”, 소프트웨어정책연구소, 2015.
5) 나성욱, 윤미영, 김태순, 김정아, “SW중심 안전사회 실현 추진전략 수립을 위한 정책연구”, 한국정보화진흥원, 2015.
6) 나채준, “재난환경 변화에 따른 과학적 재해관리체계 강화를 위한 법제연구”, 한국법제연구원, 2012.
7) 류지협, 임익현, 황의진, “국가기반체계의 통합적 관리 연구”, 한국재난관리표준학회, 2009.
8) 박태형, 김태호, 박강민, 임영모, 김윤명, “SW 안전 체계 확보와 중점 추진과제”, 소프트웨어정책연구소, 2015-022호, 2016.
9) 배병황, 강원영, 김정희, “영국의 사이버보안 추진체계 및 전략 분석”, Internet & Security Focus, 한국인터넷진흥원, 2014.
10) 이재은, “재난환경 변화에 따른 과학적 재해관리체계 강화를 위한 법제 연구 - 영국, 독일편”, 글로벌 법제전략 연구 12-22-④-3, 한국법제연구원, 2012.
11) 정준현, 지성우, “국가안전보장을 위한 미국의 반사이버테러법제에 관한 연구: 애국자법과 국토안보법을 중심으로”, 미국헌법연구 제20권 제2호, 2009.
12) 홍종현, 조용혁, “정보통신기반보호법령의 개선방안에 대한 연구”, 한국법제연구원, 2014.
13) 국가정보원, 미래창조과학부, 방송통신위원회, 행정자치부, “2016 국가정보보호백서”, 2016.
14) 노동부, “주요선진국의 산업안전보건분야에 있어서 노사참여 및 협력 제도와 운영에 관한 연구 - 영국, 독일, 프랑스, 스웨덴을 중심으로”, 노동부, 2003.
15) 소프트웨어정책연구소, “소프트웨어 안전(Safety) 산업 동향 조사”, 2015.
16) 중앙안전관리위원회, 국민안전처, “국가안전관리기본계획(2015~2019)”, 2015.
17) 전북발전연구원, “전라북도 국가기반체계 혁신방안”, 2005.
18) 정보통신정책연구원, “정보통신기반보호법 제정관련 기초연구”, 정보통신정책연구원, 2000.
19) 한국인터넷진흥원, “미국, 영국, 독일의 기반보호법 체계에 관한 연구”, 2010.
20) 한국인터넷진흥원, “주요정보통신기반보호 강화 방안 마련”, 2013.

21) 한국인터넷진흥원, “정보통신기반 보호법제 연구”, 2013.
22) 한국정보통신기술협회, SW 안전진단 제도화 연구, 2015.
23) 한국정보화진흥원, 개인정보보호 주간동향, 제108호, 한국정보화진흥원, 2015.
24) 한국지방자치학회, “주요 국가의 재난 및 위기 안전관리 체계 연구“, 행정안전부, 2008
25) 행정안전부, “효율적인 국가기반체계 보호를 위한 연구”, 2008
26) 행정안전부, “국가기반체계 보호지침 및 평가지표 개발 연구”, 2009.
27) 행정안전부, “선진 안전문화 정착을 위한 제도 개선 연구”, 2012.
28) 행정안전부, “국가기반체계 보호전략 개발연구”, 2012.
29) 행정안전부, “효율적 국가기반체계 보호를 위한 연구”, 행정안전부, 2008.

해외 문헌

1) Anti-terrorism, Crime and Security Act 2001.
2) Brock Read, “House Votes to Authorize Greater Spending on Computer-Security Research”, Chron, of Higher Educ, 2002.
3) BSI Act - BSIG 2009.
4) Civil Contingencies Act 2004.
5) Disaster Mitigation Act of 2000.
6) Federal Information Security Modernization Act of 2014.
7) Godschalk, David R. & Brower, David J, “Mitigation Strategies and Integrated Emergency Management”, Public Administrative Review, 1985.
8) Health and Safety at Work etc. Act 1974.
9) HM Government, “2016-2021 National Cyber Security Strategy“, 2016.
10) HM Government, “National Security Strategy and Strategic Defence and Security Review 2015 - A Secure and Prosperous United Kingdom“, 2015.
11) Homeland Security Act of 2002.
12) Petak. W, “Emergency Management: A Challenge for Public Administration”, Public Administration Review, 1985.
13) Prevention of Terrorism Act 2005.
14) Robert T. Stafford Disaster Relief and Emergency Assistance Act of 1988.
15) Security Service Act 1996.
16) Security Service Act 1989.
17) Security Management Act of 2002.
18) StGB: Strafgesetzbuch.
19) TKG: Telekommuni-kationsgesetz.
20) Terrorism Act 2000.
21) Terrorism Act 2006.
22) The Cyber Security Research and Development Act of 2002.

23) United States, “National Infrastructure Protection Plan”, 2013.

24) Watson Farley & Williams, BRIEFING- The New German It Security Act, February 2016

25) World Economic Forum, 『Partnering for Cyber Resilience』, 2012.

26) ZSG: Zivilschutzgesetz.

[부록 1] 정보통신기반보호법 개정(안)

제2조(정의)

1. “정보통신기반시설“이라 함은 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호의 규정에 의한 정보통신망과 이를 운용할 수 있는 소프트웨어를 말한다.

2의 2. “위기”란 자연적·인위적 원인 혹은 그 외의 즉각적으로 규명하기 어려운 원인으로 소프트웨어가 절취, 훼손 또는 위·변조됨으로써 본래의 운영 목적을 수행할 수 없도록 그 기능이 파괴·정지되는 등 무력화되는 상황을 말한다.

3.“침해사고“란 전자적 침해행위 및 위기로 인하여 발생한 사태를 말한다.

제10조의 2(소프트웨어 안전 기준의 마련)

① 기반시설에 사용되는 소프트웨어는 대통령령으로 정하는 구조 및 장치가 그 사용에 필요한 성능과 기준(이하 ‘중요 업무별 안전기준’이라 한다)에 적합하여야 한다.

② 기반시설에서 사용하는 소프트웨어가 중요 업무별 안전기준에 적합하지 아니한 경우 그 사용을 하지 못한다.

③ 중요 업무별 안전기준에 관하여 필요한 사항은 미래창조과학부령으로 정한다.

제10조의 3(사고 대응 훈련)

① 미래창조과학부장관은 사고 발생에 대비하여 개인 및 단체·법인, 공공기관이 참여하는 침해사고 대응 훈련을 실시할 수 있다. 이 경우 미래창조과학부장관은 사전에 훈련 일정, 내용 및 훈련 실시 후 결과 통보 등에 관한 사항을 훈련 참여 대상기관 및 개인에 통보하여야 하며, 해당 기관의 장과 개인은 특별한 사유가 없는 한 훈련에 참여하여야 한다.

② 미래창조과학부장관은 제1항에 따른 훈련 결과, 사고 대응이 미흡하다고 판단되는 훈련참여기관의 장에 대하여 시정조치를 요청할 수 있다. 이 경우 특별한 이유가 없는 한 해당기관의 장은 요청에 따라야 하며, 3월 이내에 시정조치 결과를 미래창조과학부장관에게 통보하여야 한다.

③ 그 밖에 사고 대응 훈련의 실시와 관련하여 필요한 사항은 대통령령으로 정한다.

제12조의 2(침해사고 대응 원칙)

① 누구든지 침해사고의 발생이나 침해 및 위기의 징후를 발견하였을 때에는 그 사실을 미래창조과학부장관이 정하는 방법에 따라 신고하여야 한다.

② 미래창조과학부장관은 제1항의 신고를 받은 경우 사고 및 관련 징후에 관하여 기반시설의 관리 책임 있는 자에게 통보하여 자체적으로 긴급하게 대응할 수 있도록 하여야 한다.

③ 누구든지 침해사고로 인하여 피해가 발생한 경우 제10조의 2의 보호지침에 따른 대응 조치를 취하여야 한다.

④ 관리기관의 장은 소프트웨어 사고 발생 혹은 징후 발견시부터 복구에 이르기까지의 과정을 기록으로 남겨 보존하여야 한다.

제13조의 2(사고 대응)

관계중앙행정기관의 장은 침해가 발생할 우려가 있거나, 위기 상황일 경우 즉시 침해행위의 무력화 및 역탐지 등의 조치를 취하여야 한다.

제15조의 2(안전관리 체계의 개선)

① 미래창조과학부장관은 기반시설의 침해사고가 발생하는 경우 해당 소프트웨어의 결함, 소프트웨어 안전 장비의 미비 등으로 인하여 사고가 발생하였는지의 여부 등 소프트웨어 사고의 원인을 조사하여야 한다.

② 미래창조과학부 장관은 제1항의 조사결과 개선이 필요한 사항이 발생한 경우 이에 대한 대응방안 및 재발 방지 대책을 마련하여 보급하여야 한다.

[부록 2] 소프트웨어 안전 관리에 관한 법률(안)

제1장 총칙

제1조 (목적)

이 법은 소프트웨어 중심 사회(지능정보사회)에서 대한민국의 안전보장을 위하여 행하는 국민, 국가 및 공공기관, 법인 및 단체 등 국가 공동체 구성원의 활동에 관한 사항을 정함으로써 국민생활의 안정과 국가발전에 이바지함을 목적으로 한다.

제2조 (정의)

이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. “소프트웨어” 란 소프트웨어산업 진흥법 제2조 제1호에 따른 소프트웨어를 의미한다.

2. “공공기관“이란 국가기관, 지방자치단체 및 「국가정보화 기본법」 제3조제10호에 따른 공공기관을 말한다.

3. “침해” 란 정보기술 등 전자적 수단을 이용하여 정보를 절취, 훼손 또는 위・변조 하는 등의 위해를 가하거나, 중요 소프트웨어에 대한 불법침입・교란・마비・파괴 등 피해를 일으키는 일체의 침해행위와 정보통신기술을 활용하여 행하는 일체의 공격행위를 의미한다.

4. “위기” 란 자연적·인위적 원인 혹은 그 외의 즉각적으로 규명하기 어려운 원인으로 소프트웨어가 절취, 훼손 또는 위·변조됨으로써 본래의 운영 목적을 수행할 수 없도록 그 기능이 파괴・정지되는 등 무력화되는 상황을 의미한다.

5. “사고” 란 침해 및 위기 등의 이유로 소프트웨어가 정상적으로 운용되지 아니하여 사회·경제적 혼란이 발생한 상태를 의미한다.

6. “안전” 이란 소프트웨어가 가지고 있는 본래의 목적에 따른 정상적인 운용 가능성이 확보된 상태를 의미한다.

7. “탐지” 란 사고에 대한 대응과 예방을 위하여 관련 정보를 수집, 처리 및 가공

등 분석하고 전파 및 공유하는 등의 행위를 의미한다.

8. “복구”란 사고로 인한 소프트웨어를 안전 상태로 전환하기 위해 필요한 일련의 활동을 의미한다.

제3조 (다른 법률관의 관계)

소프트웨어의 안전에 관하여 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다.

제4조 (기본원칙)

① 국가 및 공공기관, 국민은 소프트웨어 안전을 위한 책임 있는 주체로서 소프트웨어 안전을 위한 각종 조치 및 대응에 적극적으로 참여하여야 한다.

② 국가 및 공공기관은 소프트웨어 안전을 위한 업무 수행 및 활동 등에 관하여 성실하게 기록을 관리하고 필요한 경우 정보를 공개하는 등 투명성을 제고하여야 한다.

③ 국가 및 공공기관은 탐지활동 등 침해 및 위기 예방 활동과 대응 조치시 법률에 따라 적법한 절차에 따라야 한다.

제5조 (소프트웨어 안전 관리를 위한 책무)

① 국가는 침해 및 위기를 예방하고 사고로 인한 피해를 줄이기 위하여 노력하여야 하며, 발생한 피해를 신속히 대응·복구하기 위한 전략을 수립·시행하여야 한다.

② 공공기관은 소프트웨어 안전을 위하여 국가가 수립한 전략에 따라 예방 활동을 실시하고, 소관 소프트웨어에 대하여 안전성을 확보하고 유지하여야 하며, 침해 및 위기 발생 시 이법에서 정하는 바에 따라 국가의 지휘 및 조정 하에 적극적으로 대응할 책임이 있다.

③ 국민은 국가 및 공공기관이 침해 및 위기에 대응하는 업무를 수행할 때 최대한 협조하여야 하고, 자기가 소유하거나 관리하는 소프트웨어 등으로부터 사고가 발생하지 아니하도록 노력하여야 한다.

제2장 소프트웨어 안전 관리를 위한 정책 수립 및 시행

제6조 (소프트웨어 안전 관리 정책 수립 및 시행)

① 미래창조과학부장관은 3년마다 다음 각 호의 사항에 따라 소프트웨어 안전 관리를 위한 정책을 수립하여 제8조에 따른 소프트웨어안전위원회의 심의·의결을 거쳐 확정한 후 이를 대통령령으로 정하는 관계 공공기관의 장에게 전달하여야 한다.

1. 소프트웨어 안전 관리를 위한 기본목표와 추진방향

2. 부문별 소프트웨어 안전 관리 사항 및 이를 위한 추진 과제

3. 소프트웨어 안전과 관련한 국·내외 환경 분석 및 기술 동향

4. 소프트웨어 안전 관리에 관련된 기술 개발 촉진에 관한 사항

5. 소프트웨어 안전 관련 제도 및 법령의 개선에 관한 사항

6. 소프트웨어 안전을 위한 탐지 및 복구 조치 등과 관련하여 필요한 교육·훈련에 관한 사항

7. 소프트웨어 안전 관리를 위하여 필요한 투자 및 재원조달 계획

8. 소프트웨어 안전 관리를 위한 국제협력에 관한 사항

9. 소프트웨어 안전 기술 및 보안 산업의 육성 및 인력양성에 관한 사항

10. 지난 전략의 성과에 대한 평가 및 개선 사항

11. 그 밖에 소프트웨어 안전 관리를 위하여 필요한 사항

② 제1항의 소프트웨어 안전 관리 정책 중 대통령령으로 정하는 중요한 사항을 변경·추가하는 경우에도 제8조에 따른 소프트웨어안전위원회의 심의·의결을 거쳐 변경한다.

③ 미래창조과학부장관은 제1항에 따라 확정된 소프트웨어 안전 관리 정책을 원활하게 추진하기 위하여 관계 중앙행정기관 등에 협조를 요청할 수 있다. 이 경우 요청을 받은 중앙행정기관의 장 등은 특별한 사유가 없는 한 이에 따라야 한다.

④ 그 밖에 정책의 수립 및 시행을 위하여 필요한 사항은 대통령령으로 정한다.

제7조 (소프트웨어 안전 관리 시행계획 수립 및 시행)

① 관계 공공기관의 장은 제6조제1항에 따라 전달받은 소프트웨어 안전 관리 정책에

따라 소관 업무에 관한 집행계획을 다음 각 호의 사항을 포함하여 작성한 후 미래창조과학부장관에 통보하여야 한다.

1. 제6조제3항의 소프트웨어 안전 관리 정책에 포함된 사항의 해당 연도 집행계획

2. 소관 정보통신시스템의 소프트웨어 취약점 분석·평가에 관한 사항

3. 소프트웨어 침해에 대한 예방, 백업, 복구대책에 관한 사항

4. 직전 연도의 소프트웨어 안전 관리 활동에 대한 성과평가

5. 해당 연도 소프트웨어 안전 관리와 관련된 예산운용계획

6. 그 밖에 소프트웨어 안전 관리 정책의 집행 및 과제의 추진을 위하여 필요한 사항

② 미래창조과학부장관은 제1항에 따라 전달받은 집행계획을 소프트웨어안전위원회에 제출하고, 위원회의 심의·의결을 거쳐 확정하여야 한다. 집행계획 중 대통령령으로 정하는 중요한 사항을 변경하는 경우에도 또한 같다.

③ 미래창조과학부장관은 제1항에 따른 집행계획의 수립에 필요한 지침을 작성·배포할 수 있다.

④ 미래창조과학부장관은 제2항에 따른 집행계획의 이행여부를 진단하고 평가할 수 있다.

⑤ 그 밖에 집행계획의 수립 및 시행을 위하여 필요한 사항은 대통령령으로 정한다.

제8조 (소프트웨어 안전 관리 위원회)

① 소프트웨어 안전 관리에 관한 중요사항을 처리하기 위하여 국무총리가 위원장이 되는 소프트웨어안전위원회(이하 “안전위원회”라 한다)를 설치한다.

② 안전위원회의 위원은 부위원장 2명을 포함하여 25명 이내의 위원으로 구성한다.

③ 안전위원회의 부위원장은 미래창조과학부장관과 제2호의 위원 중 국무총리가 지명하는 사람이 공동으로 되고, 위원은 다음 각 호의 사람이 된다.

1. 중앙행정기관의 장과 공공기관의 장 및 정무직 공무원 중에서 대통령령으로 정하는 사람

2. 소프트웨어 안전에 관한 학식과 경험이 풍부한 사람 중에서 국무총리가 위촉

하는 사람

④ 제3항제2호에 따라 위촉된 위원의 임기는 2년으로 하고 1차에 한하여 연임할 수 있다. 다만, 위원의 사임 등으로 새롭게 위촉된 위원의 임기는 전임 위원의 남은 임기로 한다.

⑤ 안전위원회에 상정할 안건을 미리 검토하고 안전위원회가 위임한 안건을 심의하기 위하여 안전위원회에 실무위원회를 두며, 실무위원회 소속으로 안건 심의 등을 지원하기 위하여 분야별 전문위원회를 둘 수 있다.

⑥ 안전위원회 및 실무위원회, 분야별 전문위원회의 구성과 운영에 필요한 사항은 대통령령으로 정한다.

제9조 (소프트웨어 안전 관리 위원회 기능)

① 안전위원회는 다음 각 호의 사항을 심의·의결한다.

1. 소프트웨어 안전 관리 정책의 수립 및 집행계획의 확정·변경에 관한 사항

2. 소프트웨어 침해 및 위기와 관련한 중요사항

3. 소프트웨어 안전 관련 법·제도 수립 및 개선

4. 공공기관간 소프트웨어 안전 관리와 관련한 권한과 업무의 조정에 관한 사항

5. 제24조제1호에 따른 보안관제의 범위 및 방법에 관한 사항

6. 공공기관의 소프트웨어 위기 대응과 관련한 각종 활동의 감독·감사 및 평가에 관한 사항

7. 기타 소프트웨어 안전 관리를 위한 각종 업무 추진과 관련하여 심의·의결이 필요한 사항

② 안전위원회의는 제1항 각 호의 사항을 심의·의결하기 위하여 필요한 경우 공공기관이나 그 밖의 법인·단체 및 관계 전문가 등에게 자료제출을 요청하거나 의견을 수렴할 수 있으며, 요청을 받은 기관과 법인·단체 및 개인은 이에 성실히 응하여야 한다.

③ 안전위원회는 제3항에 따라 감독·감사 및 평가한 결과 법률에 위반된 사실이 확인된 경우에 해당 위반 사실을 관계기관에 통보하고 책임자에 대하여 징계를 요구할 수 있다.

제3장 소프트웨어 안전 관리 체계

제1절 소프트웨어 안전 기준

제10조 (소프트웨어 안전 기준의 마련)

① 정보통신기반 보호법 제2조제1호에 의한 정보통신기반시설 및 대통령령으로 정하는 중요 기반시설(이하 ‘기반시설’이라 한다)에 사용되는 소프트웨어는 대통령령으로 정하는 구조 및 장치가 그 사용에 필요한 성능과 기준(이하 ‘중요 업무별 안전기준’이라 한다)에 적합하여야 한다.

② 기반시설에서 사용하는 소프트웨어가 중요 업무별 안전기준에 적합하지 아니한 경우 그 사용을 하지 못한다.

③ 중요 업무별 안전기준에 관하여 필요한 사항은 미래창조과학부령으로 정한다.

제11조 (소프트웨어 안전 관리의 직접 수행)

① 기반시설을 관리하는 기관의 장은 대통령령이 정하는 자격기준에 따라 기반시설의 소프트웨어에 대한 안전 관리를 담당하는 자를 정하고 해당 업무를 제3자에게 위탁해서는 아니 된다.

② 미래창조과학부장관은 매년 2회 이상 실시하는 제1항의 담당자를 위한 소프트웨어 안전 관리 교육을 마련하여야 한다.

제2절 소프트웨어 안전점검 및 평가

제12조 (소프트웨어 안전진단)

① 기반시설의 장은 기반시설에서 사용되는 소프트웨어의 경우 도입 이전에 중요 업무별 안전기준에 적합한지 여부에 관하여 진단을 실시하여야 한다.

② 제1항의 안전 진단과 관련하여 절차 및 방법, 점검 인력 구성과 관련하여 대통령령으로 정하는 바에 따른다.

제13조 (소프트웨어 안전실태의 평가)

① 미래창조과학부장관은 매년 대통령령으로 정하는 공공기관 및 안전위원회의 심의·의결을 통해 정한 법인을 대상으로 소프트웨어 안전 관리 실태 및 소프트웨어의 안전성에 관하여 대통령령으로 정하는 바에 따라 평가하여야 한다.

② 미래창조과학부장관은 제1항에 따른 평가결과를 안전위원회와 국무회의에 보고한 후 이를 대통령령이 정하는 공공기관의 장 및 안전위원회의 심의·의결을 통해 정한 법인에 통보하고 공표하여야 하며, 안전위원회가 개선이 필요하다고 권고한 사항에 대하여는 해당 공공기관 및 법인에 시정요구 등의 조치를 취하여야 한다.

③ 미래창조과학부장관은 제2항에 따른 권고 및 시정요구를 시정에 필요한 기간을 정하여 통보하며 기간이 경과한 후 이행여부에 관하여 결과를 확인하여야 한다.

제14조 (사업자의 의무)

① 소프트웨어를 제작 및 제공 하는 사업자는 소프트웨어를 보급하거나 소프트웨어를 이용한 서비스를 제공하고자 하는 경우 다음 각 호의 의무를 모두 성실히 이행하여야 한다.

1. 소프트웨어 및 소프트웨어를 이용한 서비스의 기술적·관리적 보증범위와 한계 및 손해배상의 범위에 관한 고지 및 설명

2. 소프트웨어 안전 확보를 위한 수단의 설치 또는 제공(최초 설치 후 수정 및 보완 설치를 포함한다) 및 해당 서비스의 내용에 관한 명시적인 이용자의 동의

3. 소프트웨어 및 소프트웨어를 이용한 서비스와 다른 서비스의 제공 및 설치 또는 이용하는 계약을 하는 경우 이에 관한 명시적인 이용자의 동의

4. 소프트웨어 안전 확보를 위한 수단의 제거에 관한 기술적 지원

5. 소프트웨어를 제작 및 제공 하는 사업자 및 해당 업무책임자의 성명, 주소, 연락전화번호, 이메일 주소 등 고충처리체계의 수립

② 소프트웨어를 제작 및 제공 하는 사업자는 자신이 보급 또는 제공하는 소프트웨어 안전 확보를 위한 수단 관하여 그 객관적 기술능력을 과장하거나 허위로 광고하여 이용자를 유인하여서는 아니 된다.

③ 미래창조과학부장관은 소프트웨어를 이용하는 자를 보호하고 소프트웨어를 제작 및 제공 하는 사업의 질서를 위하여 필요한 경우 제1항 각 호의 사항에 관하여 사업자가 준수하여야 할 기술적·관리적 기준을 정하여 고시할 수 있다.

④ 미래창조과학부장관은 제3항의 고시를 위반한 사업자에 대하여 그 시정을 명할 수 있다.

제3절 소프트웨어 사고 예방

제15조 (소프트웨어 위기 예측 및 분석)

① 미래창조과학부장관은 탐지와 침해 및 위기 대응을 위해 각종 침해 및 위협 정보를 수집하고 공유할 수 있는 소프트웨어 안전 관리 통합·분석·공유 시스템(이하 “소프트웨어안전관리시스템” 이라 한다)을 구축하고 운영하여야 한다.

② 미래창조과학부장관은 대통령령으로 정하는 관계 공공기관의 장에게 소프트웨어안전관리시스템의 구축과 운영에 필요한 정보 제공 및 시스템의 연계 등의 협력을 요청할 수 있으며, 이 경우 요청을 받은 공공기관의 장은 특별한 사유가 없는 한 이에 따라야 한다.

③ 그 밖에 소프트웨어안전관리시스템의 구축 및 운영 등에 관하여 필요한 사항은 대통령령으로 정한다.

제16조 (위협 행위에 대한 단속 및 대응)

① 누구든지 다음 각 호의 소프트웨어 안전을 위협하는 행위를 하여서는 아니된다.

1. 접근권한을 가지지 아니하는 자가 기반시설에 접근하거나 접근권한을 가진 자가 그 권한을 초과하여 저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위

2. 기반시설에 대하여 정보를 파괴하거나 기반시설의 운영을 방해할 목적으로 컴퓨터바이러스·논리폭탄 등의 프로그램을 투입하는 행위

3. 기반시설의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보처리에 오류를 발생하게 하는 행위

② 미래창조과학부장관은 제1항 각 호의 행위를 발견하는 즉시 위협행위의 대상이

되는 기관의 장에게 통보하여 대응할 수 있도록 하며, 행위자에 관한 정보를 수사기관 등에 공유하여야 한다.

제4절 소프트웨어 사고 대응

제17조 (소프트웨어 사고 대응 원칙)

① 누구든지 소프트웨어 사고의 발생이나 침해 및 위기의 징후를 발견하였을 때에는 그 사실을 미래창조과학부장관이 정하는 방법에 따라 신고하여야 한다.

② 미래창조과학부장관은 제1항의 신고를 받은 경우 사고 및 관련 징후에 관하여 해당 소프트웨어의 관리 책임 있는 자에게 통보하여 자체적으로 긴급하게 대응할 수 있도록 하여야 한다.

③ 누구든지 소프트웨어 사고로 인하여 피해가 발생한 경우 제19조의 안전관리지침에 따라 대응 조치를 취하여야 한다.

④ 대통령령으로 정하는 공공기관의 장은 소프트웨어 사고 발생 혹은 징후 발견시부터 복구에 이르기까지의 과정을 기록으로 남겨 보존하여야 한다.

제18조 (사고 대응)

공공기관의 장은 침해가 발생할 우려가 있거나, 위기 상황일 경우 즉시 소프트웨어 안전 관리지침에서 정하는 바에 따라 침해행위의 무력화 및 역탐지 등의 조치를 취하여야 한다.

제19조 (긴급 대응 체계)

① 기반시설을 관리하는 관리기관의 장은 사고발생 시 타 관리기관의 장에게 소프트웨어의 안전을 위한 역무를 수행하는 자의 파견 및 사고 대응을 위한 활동의 참여를 요청할 수 있다. 이 경우, 파견된 자는 사고에 대응하는 관리기관의 장의 지휘에 따르도록 한다.

② 제1항의 요청을 받은 관리기관의 장은 소관기반시설의 안전 관리를 위한 최소한의 인원을 제외하고 파견 및 사고대응에 응해야 한다.

③ 미래창조과학부 장관은 대통령령으로 정하는 규모 이상의 사고에 해당하거나, 해당 관리기관이 자체적으로 대응하기에 어렵다고 판단하는 경우 소프트웨어안전관리원장으로 하여금 기술적 대응에 한하여 직접 지휘하도록 할 수 있다. 소프트웨어안전관리원장이 사고에 관하여 기술적 대응을 직접 지휘하는 경우 제1항에 따라 파견된 자는 소프트웨어안전관리원장의 지휘에 따른다.

④ 미래창조과학부 장관은 사고에 대한 원활한 대응체계 마련을 위해 기반시설을 관리하는 관리기관 간 소프트웨어 안전 관리 활동을 지원할 수 있다.

제20조 (사고 대응 훈련)

① 미래창조과학부장관은 사고 발생에 대비하여 개인 및 단체·법인, 공공기관이 참여하는 소프트웨어 사고 대응 훈련을 실시할 수 있다. 이 경우 미래창조과학부장관은 사전에 훈련 일정, 내용 및 훈련 실시 후 결과 통보 등에 관한 사항을 훈련 참여 대상기관 및 개인에 통보하여야 하며, 해당 기관의 장과 개인은 특별한 사유가 없는 한 훈련에 참여하여야 한다.

② 미래창조과학부장관은 제1항에 따른 훈련 결과, 사고 대응이 미흡하다고 판단되는 훈련참여기관의 장에 대하여 시정조치를 요청할 수 있다. 이 경우 특별한 이유가 없는 한 해당기관의 장은 요청에 따라야 하며, 3월 이내에 시정조치 결과를 미래창조과학부장관에게 통보하여야 한다.

③ 그 밖에 사고 대응 훈련의 실시와 관련하여 필요한 사항은 대통령령으로 정한다.

제21조 (안전관리지침)

① 미래창조과학부장관은 사고 발생에 대한 대응 방법 등을 포함하는 소프트웨어 안전 관리에 관한 지침을 정하여 고시하여야 하며, 공공기관의 장은 이를 준수하여야 한다.

② 중앙행정기관의 장은 제1항의 지침에 근거하여 개별·특수한 세부지침을 마련할 수 있으며, 기술발전 상황 등을 고려하여 주기적으로 수정·보완하여야 한다.

제4절 소프트웨어 복구

제22조 (소프트웨어 복구조치)

① 개인 및 단체·법인, 공공기관의 장은 침해로 인하여 소프트웨어에 대한 피해가 발생한 때에는 해당 소프트웨어의 복구 및 보호에 필요한 조치를 신속히 취하여야 한다.

② 공공기관의 장은 제1항의 침해가 발생한 경우 그 원인과 피해내용 등에 관하여 신속히 사고조사를 실시하여야 하며, 누구든지 사고조사를 완료하기 전에 침해와 관련된 자료를 임의로 삭제·훼손·변조하여서는 아니 된다. 이 경우 공공기관의 장은 미래창조과학부장관에게 사고조사와 관련한 협조를 요청할 수 있다.

③ 개인 및 단체·법인, 공공기관의 장은 제1항의 규정에 의한 복구 및 보호조치를 위하여 필요한 경우 소프트웨어안전관리원의 장에 지원을 요청할 수 있다.

④ 미래창조과학부장관 및 소프트웨어안전관리원의 장이 제2항 및 제3항의 규정에 의한 지원요청을 받은 때에는 피해복구가 신속히 이루어질 수 있도록 기술지원 및 인력파견 등 필요한 지원을 하여야 하고, 피해확산을 방지할 수 있도록 해당 개인 및 단체·법인, 공공기관의 장과 함께 적절한 조치를 취하여야 한다.

⑤ 미래창조과학부장관은 제4항의 지원이 있는 경우 소프트웨어안전관리원에 필요한 범위 내에서 예산 및 장비 등의 지원을 할 수 있다.

제23조 (사실조사·실태조사)

① 미래창조과학부장관은 소프트웨어 안전 관리를 위하여 공공기관과 필요한 경우 안전위원회의 심의·의결로 정한 개인, 민간 단체·법인에 대하여 정기적인 실태조사를 실시할 수 있다.

② 미래창조과학부장관은 제22조에 따른 침해 및 위기발생에 대한 사고조사 외에 문제되는 상황이 발생한 때 사실조사를 실시할 수 있다.

③ 제1항 및 제2항에 따른 조사의 실시 방법에 관하여 구체적인 사항은 대통령령으로 정한다.

제24조 (안전관리 체계의 개선)

① 미래창조과학부장관은 기반시설의 소프트웨어 사고가 발생하는 경우 해당 소프트웨어의 결함, 소프트웨어 안전 장비의 미비 등으로 인하여 사고가 발생하였는지의 여

부 등 소프트웨어 사고의 원인을 조사하여야 한다.

② 미래창조과학부 장관은 제1항의 조사결과 개선이 필요한 사항이 발생한 경우 이에 대한 대응방안 및 재발 방지 대책을 마련하여 보급하여야 한다.

③ 미래창조과학부장관은 제1항에 따른 조사결과 및 개선사항과 재발 방지 대책 등을 제15조의 소프트웨어안전관리시스템에 등록하여야 한다.

제4장 소프트웨어 안전 관리 기반조성

제25조 (소프트웨어안전관리원의 설립)

① 미래창조과학부장관은 침해 및 위기에 대한 탐지 업무를 지원하고 효과적인 침해 방지 기술 및 안전 보장 방안을 개발하기 위하여 소프트웨어안전관리원(이하 “관리원”이라 한다)을 설립한다.

② 관리원은 법인으로 한다.

③ 관리원은 다음 각 호의 업무를 수행한다.

1. 소프트웨어 안전 관리 정책 및 시행계획의 수립·시행지원

2. 침해 방지 및 위기 대응을 위한 기술의 조사·연구의 지원

3. 상시적인 트래픽 유동량 감시 등 탐지업무의 지원

4. 소프트웨어안전관리시스템 구축을 위한 기술표준, 방법, 구축 단계 및 절차의 지원

5. 침해 대응 및 안전 보장을 위한 훈련의 지원

6. 소프트웨어 안전을 위한 민간 협력 및 국제협력 지원

7. 소프트웨어 안전 전문인력 양성을 위한 사업

8. 침해에 대한 기술 분석 및 긴급한 대응방안 전파업무 지원

9. 침해 대응 및 위기 억제 업무의 지원

10. 공공기관 등의 위기 대응 수준 조사지원

11. 공공기관 및 민간의 침해 탐지 및 피해신고 접수 업무

12. 다른 법령에서 관리원의 업무로 정하거나 기술원에 위탁한 사업

13. 그 밖에 공공기관 등의 장이 위탁하는 사업

④ 국가기관 등은 관리원의 설립, 시설 운영 및 업무 추진 등에 필요한 경비에 충당하기 위하여 관리원에 출연할 수 있으며, 정부는 기술원의 설립 및 운영 등을 위하여 필요한 국유재산을 무상으로 대여할 수 있다.

⑤ 관리원은 지원을 받으려는 공공기관 등에 그 지원에 드는 비용의 전부 또는 일부를 부담하게 할 수 있다.

⑥ 관리원에 관하여는 이 법 및 「공공기관의 운영에 관한 법률」에서 정한 것을 제외하고는 「민법」 중 재단법인에 관한 규정을 준용한다.

⑦ 관리원이 아닌 자는 소프트웨어안전관리원의 명칭 및 혼란을 야기하는 유사명칭을 사용하지 못한다.

⑧ 제1항부터 제7항까지에서 규정한 사항 외에 관리원의 설립과 운영에 필요한 사항은 대통령령으로 정한다.

제26조 (소프트웨어 안전 책임관)

① 대통령령으로 정하는 공공기관의 장은 해당 기관의 소프트웨어 안전 관리에 관한 업무를 총괄하는 책임관 및 실무담당자를 임명하고 이를 미래창조과학부장관에게 통보하여야 하며, 책임관 및 실무담당자를 변경한 경우도 이와 같다.

② 소프트웨어 안전 책임관 및 실무담당자는 해당 기관의 업무와 관련하여 다음 각 호의 사항을 담당한다.

1. 소프트웨어 안전 관리 시책의 총괄조정 및 지원

2. 소관 기반시설의 소프트웨어 안전 관리 업무

3. 소프트웨어 안전 관리를 위한 정보 수집, 제15조의 소프트웨어안전관리시스템에 정보제공 및 시스템 연계

4. 침해 및 위기 대응 훈련 총괄 및 지원

5. 침해 및 위기 대응 및 피해 복구관련 업무총괄

6. 그 밖에 소프트웨어 안전 관리를 위한 관련 업무

③ 제1항에 따른 기관 등은 기관의 소프트웨어 안전 관리를 전담하는 조직 및 인력을 둘 수 있으며, 이 경우 전담하는 조직은 제24조의 관리원에 긴밀히 협조하여야 한

다.

제27조 (인력양성 및 교육홍보)

① 미래창조과학부장관은 소프트웨어 안전 관리 역량 강화를 위해 전문 인력을 양성하고 국민의 소프트웨어 안전에 관한 인식 제고를 위하여 다음 각 호의 시책을 추진할 수 있다.

1. 소프트웨어 안전 관리 관련 전문인력의 확보 및 양성

2. 소프트웨어 안전 인식제고를 위한 교육프로그램의 개발 및 투자

3. 교육부, 미래창조과학부, 국민안전처 등 관계 중앙행정기관과 연계된 전문인력 양성 사업의 발굴

4. 그 밖에 전문인력 양성, 교육 및 홍보 등에 관하여 필요한 사항

② 미래창조과학부장관은 제1항제1호에 따른 전문인력의 양성을 위하여 대통령령으로 정하는 바에 따라 연구소, 대학 그 밖의 기관을 소프트웨어 안전 관리 전문인력 양성기관으로 지정할 수 있다.

제28조 (연구개발 및 보급)

① 정부는 소프트웨어 안전 관리에 필요한 기술개발과 기술수준의 향상을 위하여 다음 각 호의 시책을 추진할 수 있다.

1. 소프트웨어 안전 관리 기술 수요조사 및 동향분석 등에 관한 사항

2. 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등 침해·위협 정보기술의 동향조사 및 분석

3. 소프트웨어 안전 관리에 관한 기술의 개발·보급·확산 사업

4. 우수신기술의 선정 및 지원과 시범사업 적용

5. 소프트웨어 안전 관리 기술의 민간 확산

6. 그 밖에 소프트웨어 안전 관리 관련 기술개발 및 기술향상 등에 관하여 필요한 사항

② 제1항제4호의 시범사업 결과 대통령령으로 정하는 수준의 성과평가 결과를 얻은

우수신기술의 경우 제20조의 위기 대응 훈련에 우선 활용할 수 있다.

③ 미래창조과학부장관은 제1항에 따른 사항을 효과적으로 연구개발하기 위하여 제24조에 따른 관리원을 전문기관으로 지정할 수 있다.

④ 그 밖의 소프트웨어 안전 관리 기술의 연구개발에 관한 절차·방법 등 세부사항은 미래창조과학부장관이 따로 정한다.

제29조 (국제협력)

정부는 침해 방지 및 위기관리에 관하여 국제적 동향을 파악하고, 국제기구·단체 및 외국과의 협력을 증진하기 위하여 다음 각 호의 업무를 수행할 수 있다.

1. 소프트웨어 안전 관리를 위한 상호간 협력체계 구축
2. 소프트웨어 안전 관리 기술에 관한 정보의 교류와 공동대응
3. 소프트웨어 안전 관리 전담인력의 상호간 파견교육
4. 분야별, 권역별 소프트웨어 안전 관리에 관한 국제 협력체계 강화
5. 그 밖에 소프트웨어 안전 관리를 위한 국제협력에 관한 사항

제30조 (소프트웨어 안전기술 및 관련 산업 육성)

미래창조과학부장관은 소프트웨어 안전 관리를 위한 관련산업의 육성 시책을 효과적으로 추진하기 위하여 관련 전문기관 및 민간단체로 하여금 이를 수행하게 할 수 있으며, 이에 필요한 예산을 지원할 수 있다.

제31조 (포상)

① 미래창조과학부자관은 침해 및 위기 발생시 피해확산 방지에 기여하는 등 적절한 조치를 취하였거나, 소프트웨어 안전 관리에 이바지한 공로가 인정되는 공무원 또는 공공기관 임직원, 관련분야 법인·단체 및 개인을 선정하여 포상할 수 있다.

② 제1항의 공로에는 이 법에 따른 실태조사 및 감독·평가사항, 각종 대응훈련 등에서 우수한 성과를 나타낸 경우가 포함된다.

제5장 보칙

제32조 (협조요청)

① 미래창조과학부장관은 다음 각 호의 어느 하나에 해당하는 경우 다른 공공기관에 행정응원 및 협조를 요청할 수 있다.

1. 법령 등의 이유로 독자적인 직무 수행이 어려운 경우

2. 인원·장비의 부족 등 사실상의 이유로 추가적인 업무 협조가 필요한 경우

3. 다른 공공기관이 관리하고 있는 문서(전자문서를 포함한다)·통계 등 행정자료가 직무 수행을 위하여 필요한 경우

② 제1항의 행정응원 및 협조요청을 받은 기관은 다음 각 호의 어느 하나에 해당하는 경우 요청을 거부할 수 있다.

1. 다른 공공기관이 보다 능률적이거나 경제적으로 응원할 수 있는 명백한 이유가 있는 경우

2. 행정응원으로 인하여 고유의 직무 수행이 현저히 방해 받을 것으로 인정되는 명백한 이유가 있는 경우

제33조 (비밀엄수 의무)

이 법에 따라 소프트웨어 안전 관리 업무에 종사하거나 종사하였던 자는 그 직무상 알게 된 비밀을 타인에게 누설하거나 직무상 목적 외에 이를 사용하여서는 아니 된다.

제34조 (권한의 위임·업무의 위탁)

미래창조과학부장관은 이 법에 따른 권한의 일부를 대통령령으로 정하는 바에 따라 시·도지사 등에게 위임하거나, 업무의 일부를 제25조의 관리원에 위탁할 수 있다.

제35조 (벌칙 적용에서의 공무원 의제)

제34조에 따라 권한을 위탁받은 사무에 종사하는 자는 「형법」 제122조부터 제135조까지의 규정에 따른 벌칙의 적용에 있어서는 이를 공무원으로 본다.

제6장 벌칙

제36조(벌칙)

① 제16조제1항의 규정을 위반하여 기반시설을 교란·마비 또는 파괴한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다.

② 제1항의 미수범은 처벌한다.

제37조(벌칙)

다음 각 호에 해당하는 자는 5년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처한다.

1. 제14조제2항의 규정을 위반하여 정당하게 소프트웨어를 이용하는 자에게 피해를 발생시킨 자

2. 제18조제4항 및 제21조제2항의 규정을 위반하여 사고와 관련된 자료를 임의로 삭제·훼손·변조한 자

2. 제33조의 비밀 엄수 의무를 위반한 자

제38조(과태료)

① 다음 각 호의 어느 하나에 해당하는 자는 2천만원 이하의 과태료에 처한다.

1. 제14조제1항 각 호의 의무를 위반한 자

② 다음 각 호의 어느 하나에 해당하는 자는 천만원 이하의 과태료에 처한다.

1. 제20조제2항에 따른 시정조치 결과를 통보하지 아니한 자

③ 제1항 및 제2항에 따른 과태료는 대통령령으로 정하는 바에 따라 미래창조과학부장관이 부과·징수한다.

④ 제3항에 따른 과태료 처분에 불복이 있는 자는 그 처분의 고지를 받은 날부터 30일 이내에 미래창조과학부장관에게 이의를 제기할 수 있다.

⑤ 제3항에 따라 과태료 처분을 받은 자가 제4항에 따라 이의를 제기한 때에는 미래

창조과학부장관은 지체 없이 관할 법원에 그 사실을 통보하여야 하며, 그 통보를 받은 관할법원은 「비송사건절차법」에 따른 과태료의 재판을 한다.

⑥ 제4항에 따른 기간 이내에 이의를 제기하지 아니하고 과태료를 납부하지 아니한 때에는 국세 또는 지방세 체납처분의 예에 따라 이를 징수한다.

부 칙

제1조(시행일) 이 법은 공포 후 6개월이 경과한 날부터 시행한다.

연구보고서 2016-020

SW안전 관리 관점에서의 기반시설 보호 법제 개선 연구

2017년 05월 인쇄
2017년 04월 발행

발행처 정보통신산업진흥원 부설 소프트웨어정책연구소
경기도 성남시 분당구 대왕판교로712번길22 A동 4층
Homepage: www.spri.kr

ISBN : 978-89-6108-381-2

주 의

1. 이 보고서는 소프트웨어정책연구소에서 수행한 연구보고서입니다.
2. 이 보고서의 내용을 발표할 때에는 반드시 소프트웨어정책연구소에서 수행한 연구결과임을 밝혀야 합니다.

ISBN : 978-89-6108-381-2