법제분석지원 연구 14-21-②

신청기관	국가사이버안전센터

정보통신기반보호법령의 개선방안에 대한 연구

홍종현 · 조용혁

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

법제분석지원 연구 14-21-②

신청기관	국가사이버안전센터

정보통신기반보호법령의 개선방안에 대한 연구

홍종현 · 조용혁

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

정보통신기반보호법령의 개선방안에 대한 연구

A Study on the improvement of the act on the protection of the Information and Communications Infrastructure

연구자 : 홍종현(한국법제연구원 부연구위원)
Hong, Jong-Hyun

조용혁(한국법제연구원 초청연구원)
Cho, Yong-Hyuk

2014. 9. 30.

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

요 약 문

Ⅰ. 배경 및 목적

□ 분석의 배경과 목적

○ 최근 IT 정보화가 고도로 발달하면서 해킹, 디도스 공격 등 전자적 침해행위로부터 정보통신망을 안정적으로 보호하여 사이버 보안과 국가안보를 지켜야 할 필요성이 증대됨

○ 남북대치상황에 있는 우리나라의 경우 사이버 테러 위협이 빈발하고 있고, 이는 개인정보의 보호 및 국민생활의 안정을 위하여 강력한 보호지원이 요청되고 있음

○ 전자적 침해행위의 특성상 사후적 대응보다는 사전예방을 위한 국가적 차원의 보호 및 지원방안에 대한 법제분석 및 개선방안의 마련이 절실히 요구됨

□ 법제분석 방법

○ 본 연구는 「정보통신기반보호법」과 동법 시행령의 문제점을 분석하기 위하여 법령체계를 논리적으로 재구성하고 관련 법제와의 관계를 중심으로 조문별로 규율내용의 타당성을 분석함

○ 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「보안업무규정」, 「국가사이버안전관리규정」 등에 대한 검토를 통하여 사이버 안보 영역에서의 법제도와 정책과의 연계성을 검토함

Ⅱ. 주요 내용

□ 「정보통신기반보호법」의 의의 및 기능(제2장)

○ 「정보통신기반보호법」의 규율대상 및 적용영역 등에 대한 검토를 통하여 입법목적과 그 정당성 근거에 대한 논증

○ 「정보통신기반보호법」의 제·개정과정을 검토함으로써 주로 문제가 되었던 실체법적 쟁점들과 더불어 관할 부처에 대한 조직법적 검토를 병행하여 제시함

□ 주요정보통신기반시설에 대한 보호체계(제3장)

○ 주요정보통신기반시설의 지정 및 지정권고(제8조, 제8조의2)

- 분화된 보호체계의 장점과 단점을 둘러싼 논란 정리

○ 관리기관의 취약점 분석(제9조) 및 보호대책의 수립(제5조)

○ 국가적 차원의 관여와 지원

- 보호대책 이행여부의 확인(제5조의2)

- 보호계획의 수립 및 통보(제6조)

- 보호지침의 제정 및 보호조치의 명령 및 권고(제10, 11조)

□ 주요정보통신기반시설에 대한 보호지원(제4장)

○ 국가적 차원에서 이뤄지는 보호지원의 정당성과 한계

○ 주요정보통신기반시설을 보호하기 위한 조직

- 정보통신기반보호위원회의 구성 및 운영(제3, 4조)

- 침해사고 대책본부(제15조) 및 정보공유분석센터(제16조)

○ 주요정보통신기반시설 및 관리기관 등에 대한 보호지원

- 주요정보통신기반시설에 대한 기술적 지원(제7조)
- 관리기관에 대한 재정적·행정적·기술적 지원(제25조)
- 기술개발(제24조) 및 국제협력(제26조) 등

Ⅲ. 기대효과

□ 학술적 효과

○ 주요정보통신기반시설에 대한 침해사고의 사후복구 및 형사적 대응체계에 대한 검토는 제외하였으나, 사전적 예방체계에서 문제될 수 있는 조직법적, 절차법적, 실체법적 쟁점들을 체계적으로 정리함

□ 정책적 효과

○ 최신의 사이버안보정책과 관련 법제의 연계성 강화를 위한 개선방안 제시

주제어 : 정보통신기반시설, 기술적 지원, 전자적 침해행위, 보호지원, 사이버 안보 등

Abstract

Ⅰ. Background and Purpose

□ Background and purpose of this study

○ The necessity of protecting the information and communications infrastructure - “Critical Information Infrastructure Protection(CIIP) - has been increased nowadays with the frequent occurrence of intrusion by electronic means, for example hacking and DDos attack due to the IT technology development.

○ Especially the Republic of Korea is in armistice state with the North Korea, so that the threat of cyber-terror comes out seriously and regularly and the protection of critical information and communication infrastructure is important to keep the safety of the nation and the stability of the life of people.

○ Because of the specific characteristics of the intrusions by electronic means, the precautionary protection of the information and communications infrastructure is more meaningful than its posteriori control so that this study is focused on the national assistance to protect it from the hacking and DDos attack etc.

□ Methodology

○ In this study, I analyzed the current situation and problems of the Legal Institution of the information and communications infrastructure

- “Critical Information Infrastructure Protection(CIIP)” with the relating legal system, for example the “Act on the Promotion of the Information and Communications Network Utilization and Information, etc.” and the “Regulation on the national cyber-security”

Ⅱ. Main Contents

□ The Significance and Function of the “ACT ON THE PROTECTION OF INFORMATION AND COMMUNICATIONS INFRASTRUCTURE” (Chapter Ⅱ)

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

○ With analyzing the history of enacting and revising this act, I would review the legal issues discussed in congress and by many scholars through the view of substantial and organization law.

□ The legal system of protecting the critical information and communications infrastructure (Chapter Ⅲ)

○ Designation of the Critical Information and Communications Infrastructure (Article 8) and the Recommendation for its Designation (Article 8-2) with reviewing the argumentation of the diversified protecting system

○ The Analysis and Evaluation of the Vulnerabilities (Article 9) and the Establishment of Measures to Protect the Critical Information and Communications Infrastructure(Article 5) by management organization

○ The National Guidance and Assistance

- Ascertaining Implementation of Measures to Protect Critical Information and Communications Infrastructure (Article 5-2)
- Establishment of Plans for Protecting Critical Information and Communications Infrastructure (Article 6)
- Protection Guidelines (Article 10) & Orders or Recommendation for the Protection Measures (Article 11)

□ The Support for Protection of Critical Information and Communications Infrastructure (Chapter Ⅳ)

○ The necessity and legitimacy of national support and its limits

○ The organization to protect the Critical Information and Communications Infrastructure

- Committee for Protection of Information and Communications Infrastructure (Article 3)
- Organization of Headquarters for Countermeasures (Article 15)
- Information Sharing and Analysis Center (Article 16)

○ The Support for Protection of Critical Information and Communications Infrastructure

- The technological assistance on the critical information and communication infrastructure (Article 7)

- The Government may, with respect to a management organization, transfer technology necessary for protecting critical information and communications infrastructure, and provide equipment and other necessary support (Article 15)

- Technological Development etc (Article 24) & International Cooperation (Article 26)

Ⅲ. Expected Effect

□ Academic effect

○ Although this study excludes the posteriori countermeasure such as criminal punishment, fine or penalty etc., it dealt with the legal issues regarding the organization, procedures and substantial regulation on the management organization of the critical information and communication infrastructure systematically.

□ Effect in Policy

○ It suggest the improvement of the act and statute on the critical information and communication infrastructure protection for strengthening inter-connection between policy and legal system in the area of cyber security.

Key Words : Act on the protection of the critical information and communication infrastructure, Technical Assistance (Support), Intrusion by electronic means, Support to protect critical information and communication infrastructure, Cyber-security.

목 차

제 1 장 서 론

제 1 절 연구의 목적과 대상

우리나라에서 일반적인 정보통신망의 보호에 관한 법률은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 기본법으로 하여 각 분야별 그리고 적용대상별로 개별적으로 규정을 두고 있다. 그러나 기존의 정보보호법제는 정보통신망과 정보시스템에 대한 규제의 중복 또는 공백 문제, 역할 분담의 적정성, 원활한 국제적 협력네트워크 미실시 등 다양한 문제점이 노출되고 있다.

이에 대처하기 위하여 정보통신망과 정보통신기반시설 등 보호대상을 명확히 규정하고, 침해사고대응체계 및 절차를 구체적으로 규율하며, 관련 담당기관들 상호간의 적절한 역할분담과 민간업체에 대한 지원을 통한 정보보안의 실효성 확보 등이 중요한 이슈로 등장하고 있다. 그리고 이와 더불어 개별 이용자의 보호를 통한 정보보안에 대한 인식과 신뢰제고, 국제적 공조체계 구축 등 IT 환경 변화를 수용하는 법체계의 정비가 요청되고 있다. 특히, 최근 빈발하고 있는 해킹, DDoS 공격사건, 개인정보 유출사고 등은 정보보안법제에 대한 문제가 심각하다는 인식을 확산시켰고, 이에 따라 현행 정보보안법제의 개선방안을 마련하여야 한다는 공감대가 확산되고 있는 것이다.

그 중에서도 국가의 기반시설이라고 할 수 있는 주요정보통신기반시설에 대한 보호를 규율하고 있는 「정보통신기반보호법」에 대한 개선방안을 마련하여야 한다는 요청이 강력하게 제기되고 있다. 특히, 정부는 지속적으로 빈발하고 있는 사이버위협에 대하여 2013년 7월 4일 「국가 사이버안보 종합대책」을 마련하여 발표하였다. 이는 한편으로는 정보보안법제 전반에 대한 체계정당성을 검토하여 기본법과 개별법의 관계를 체계적으로 정비하는 거시적 작업이 필요하고, 다른

한편으로는 정보통신기반시설의 중요성과 침해사고 발생시의 국가적·사회적 파급효를 고려할 때 "사이버안보종합대책"과 「정보통신기반보호법」의 연계성을 강화하는 방향으로 개정방안을 수립하는 미시적 작업을 동시에 필요로 하는 것이다.

본 연구의 주된 목적은 「정보통신기반보호법」 및 동법 시행령·시행규칙의 현황 및 문제점을 분석하고, 이에 대한 개선방안을 도출하기 위한 것이다. 이를 위하여 정보보안법제의 전반적인 체계를 분석하고, 관련 규정들의 중복규제의 가능성, 정보통신기반보호체계의 관련기관들의 유기적 협조체계 운영 및 역할분담 문제 등을 검토할 것이다. 이러한 진단을 바탕으로 하여 「정보통신기반보호」과 동법 시행령의 문제점을 분석하고 개선방안을 제시하고자 한다.

제 2 절 연구의 방법

오늘날 정보통신(IT)기술이 발달하면서 현대사회에서 사이버 보안이 차지하는 비중은 날이 갈수록 증가하고, 개인정보보호와 정보보안과 관련된 이슈는 지속적으로 제기되고 있다. 그러나 이는 법제도적으로 완벽하게 방지하거나 해결될 수 있는 문제가 아니고, 정보통신기술의 발전에 상응하여 정보보안 기술개발과 보안전문인력의 양성 등 실질적 대응체계를 구축하여야 하는 과제로서 지속적인 관심과 노력이 수반되어야 하는 것이다. 특히, 정보화 사회에서 국가의 주요기반시설은 정보통신기술이 도입된 새로운 운영시스템과 융합하게 될 가능성이 높아지게 되고, 이에 따라 정보통신망을 이용한 전통적인 국가기반시설에 대한 침해사고의 위협도 높아지고 있다. 따라서 「정보통신기반보호법」은 민·관·군 분야를 포괄하는 예방체계를 갖추면서 정보통신기반시설에 대한 침해사고가 발생할 경우 즉각적으로 대응할 수 있는 실효성 있는 법제도의 근간으로서 작동할 수 있어야 한다.

이를 위하여 본 연구는 주요 정보통신기반시설의 현황 및 문제점을 분석하고 관련법제의 분석을 통한 개선방안을 모색하는데 집중하고자 한다. 2001년 「정보통신기반보호법」이 제정되기까지의 과정과 그 이후의 개정 논의에서 문제된 쟁점들을 고찰하고, 특히 정부조직이 개편되는 것과 맞물려 정보통신기반 보호체계가 개편되는 과정을 간략하게 검토할 것이다. 이러한 정보통신기반보호법제의 발전과정을 법사학적 관점에서 고찰하는 것은 매우 다양한 논의들을 나열하여 소개하는 데 그치지 않고, 문제된 쟁점들을 재검토함으로써 앞으로 개선방안을 모색하는데 도움이 될 수 있는 시사점을 발견하기 위한 것이다.

이를 위하여 현행법제의 분석을 집중적으로 수행할 것이다. 우선, 「정보통신기반보호법」에 초점을 맞추어 그 규율대상과 규율내용을 명확히 하고, 그와 충돌하거나 중복될 수 있는 관련 법령규정을 분석할 것이다. 즉, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「재난관리기본법」, 「통신비밀보호법」, 「국가정보원법」 등과 아울러 「보안업무규정」, 「국가사이버안전관리규정」 등을 체계적으로 검토할 것이다.

이를 위하여 「정보통신기반보호법」과 동법 시행령의 조문들을 체계적으로 검토하고자 한다. 제2장에서는 법률의 제정취지와 적용범위 등을 법 제1조(입법목적)과 제2조(정의)를 통하여 살펴보고 그 규범적 의미와 한계 등을 논의할 것이다. 이와 더불어 법 제정과정 및 개정과정을 간략히 살펴봄으로써 「정보통신기반보호법」의 입법배경 및 향후 개선방안 마련의 시사점을 도출하게 될 것이다.

제3장에서는 이를 바탕으로 하여 「정보통신기반보호법」의 보호체계를 논의할 것이다. 이는 「정보통신기반보호법」의 핵심적인 규율내용으로서 주요정보통신기반시설로 지정 또는 지정권고(제8조, 제8조의2)되는 것에서부터 시작하여 주요정보통신기반시설로 지정될 경우에 부담하게 되는 절차적 규율을 단계별로 논의한다. 이는 주요정보통신기반시설에 대한 사전적 예방체계를 구성하는 것으로서 관리기관이 자

율적으로 취약점 분석(제9조)과 보호대책(제5조)을 수립하는 것과 국가에서 보호지원을 위하여 보호대책의 이행여부의 확인(제5조의2), 보호계획의 수립 및 통보(제6조), 보호지침의 제정(제10조), 보호조치의 명령 및 권고(제11조) 등의 관계를 연계하여 살펴본다.

그 중에서도 국가적 보호체계의 핵심적 내용이라고 할 수 있는 것은 제4장에서 별도로 논의하게 될 것이다. 이를 위하여 우선 국가적 차원의 보호지원이 정당하고 규범적으로 요청되는 것인지에 대하여 논증하고, 조직법적 차원에서 검토하여야 할 정보통신기반보호위원회(제3조, 제4조)와 침해사고대책본부(제15조), 정보공유분석센터(제16조) 등의 문제점과 개선방안을 살펴본다. 그리고 주요정보통신기반시설에 대한 보호지원(제7조), 관리기관에 대한 지원(제25조) 그리고 기술개발(제24조) 및 국제협력(제26조) 등을 입체적으로 분석하여 개선방안을 제시하고자 하였다.

이와 더불어 주요정보통신기반시설에 대한 침해사고의 사후복구와 형사적 대응체계에 대한 규율이 중요한 한 축을 담당하고 있다. 이를 위하여는 침해사고의 유형과 전자적 침해행위의 금지에 대한 규율내용 그리고 사후대응을 위한 처벌규정 및 비밀유지의무와 과태료 등을 살펴보아야 하는데, 이는 연구의 범위에서 제외하고자 한다.[1] 그리고 해외 주요국가의 정보통신기반보호법제 및 정책적 분야에 대한 검토는 자세하게 살펴보는 것은 지면관계상 생략하고 향후 관련 분야의 연구를 지속하여 최신의 외국법제를 검토하기를 기약한다.

이와 같은 단계적 검토를 통하여 현행 「정보통신기반보호법」의 문제점을 분석하고, 이에 대한 개선방안을 다각적이고 종합적인 관점에

1) 참고로 전자적 침해행위(해킹 등)의 특성상 가해자를 파악하기 어려운 관계로 사문화될 가능성이 높을 것으로 보이지만 우리나라에서는 지난 서울시장 보궐선거에서 선거관리위원회 DDos 공격을 한 사건이 「정보통신기반보호법」 위반에 대한 처벌이 한 건 있었다. 이에 대하여는 대법원 2013.4.26. 선고 2012도15257 판결 ; 서울고등법원 2012. 11. 30 선고 2012노3434판결 참조.

서 모색할 것이다. 「정보통신기반보호법」 개정안 마련을 위하여 법령 입안기준에 따른 법제분석, 전문가 자문 및 워크숍 개최, 관련 정책과 법제에 관한 분석, 입법대안 제시 및 정책부서와 연계된 맞춤형 연구 성과를 발굴하여 제시한다. 본 연구는 법제연구에 초점이 맞추어져 있으므로 법사학적 연구(법안의 제정과정 및 개정과정에서 논란이 된 쟁점 분석), 입법평가(법체계적 정당성 검토를 위한 규정의 중복 또는 다른 법규정과의 관계 분석) 등을 통하여 현행 우리나라의 「정보통신기반보호법」의 문제점과 개선방안을 검토하고자 한다.

제 2 장 정보통신기반보호법의 개요

제 1 절 정보통신기반보호법의 의의 및 기능

Ⅰ. 정보통신기반보호법의 의의

1. 정보통신기반보호법의 입법목적

「정보통신기반보호법」은 제1조(입법목적)에서 "이 법은 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적으로 한다"고 규정하고 있다. 이는 "① 전자적 침해행위 대비, ② 주요정보통신기반시설의 보호에 관한 대책 수립·시행 및 안정적 운용 그리고 ③ 국가의 안전과 국민생활의 안정 보장"으로 요약할 수 있다. 즉, 해킹, 바이러스, 전자기파 등 각종 전자적 침해행위로부터 정보통신기반시설을 보호하기 위하여 이에 대응할 수 있는 조직 및 보호체계를 구축하고 그에 대한 취약점의 분석·평가와 이에 기초한 보호대책의 수립·이행 등을 규율하기 위한 것이다.

구글(Google), 야후(Yahoo), CNN 등 유명 사이트나 청와대 등 중요한 국가정보사이트의 해킹사례 그리고 멜리사, CIH, 러브 바이러스, 나비다드 바이러스 등의 유포 혹은 DDoS 공격 등에서 볼 수 있듯이 전자적 침해행위를 사후적 형사처벌만으로 대응하기에는 한계가 있다. 인터넷을 이용한 전자적 침해행위의 특성상 범죄자를 추적하고 적발하는 것은 사실상 어렵기 때문이다. 따라서 정보통신기반시설에 대한 규율은 사후적 대응보다는 사전예방 중심의 보호체계로서 규율되는 것이 바람직한 것이다.[2)]

2) 「정보통신기반보호법」은 전자적 침해행위와 침해사고의 사전예방의 측면에 중

따라서 「정보통신기반보호법」은 해킹, 컴퓨터바이러스 등 정보통신기술을 이용하여 주요 정보통신기반시설에 대한 침해행위로부터 전자적 제어·관리시스템과 정보통신망을 효과적으로 보호하기 위한 조직과 보호체계를 구축하고, 이를 통하여 전자적 침해행위를 예방하고 대처하기 위한 법률이라고 할 수 있다. 이 보고서에서는 주요 정보통신기반시설을 보호하기 위한 조직법적 쟁점과 아울러 보호체계(예방 및 대응)의 문제를 중심으로 살펴보게 될 것이다.

2. 입법목적의 특수성과 구체화의 한계

법 제1조에 명시된 입법목적과 관련하여 다음과 같은 점에서 문제가 제기될 수 있다. 우선, "전자적 침해행위 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써"라는 내용은 맥락상 "전자적 침해행위에 대비하기 위하여 보호대책을 수립·시행한다"는 의미로 해석하는 것이 합리적이다.[3)]

그리고 이를 통하여 달성하고자 하는 일차적 목적은 "정보통신기반시설을 안정적으로 운용하는 것"이고, 궁극적 목적은 "국가의 안전과 국민생활의 안정을 보장하는 것"으로 정리할 수 있다. 이는 「정보통신기반보호법」이 '정보통신법제'와 '국가안보에 관한 법제'의 성격을 함께 갖고 있음을 보여 준다. 따라서 한편으로는 정보통신법과 국가안보에 관한 법체계와 공동의 기초 내지 근거를 공유하고 있고, 다른 한편으로는 그 법제들과는 다른 특수성이 있다는 점이 고려되어야 한다.

이와 관련하여 다음과 같은 문제제기가 있을 수 있다. 즉, 「정보통

점이 놓여 있기는 하지만, 사후대응(복구지원, 처벌 등)에 대한 규율도 존재한다. 이에 대하여는 법 제13조(침해사고의 통지), 제14조(복구조치), 제28조(처벌), 제30조(과태료) 등 참조.

3) 법에서는 정보통신기반시설 관리기관의 장이 자율적으로 수립·시행하는 "보호대책의 수립"을 명시하고 전면에 내세우고 있지만, 그 이면에는 국가가 지원하는 보호지침, 보호계획 등이 작용하고 있음에 유의하여야 한다. 이는 일체를 이루어 주요정보통신기반시설에 대한 보호체계를 구성하게 된다.

신기반보호법」의 특성을 고려하여 보다 구체적이고 명확한 입법목적을 규정하는 것이 보다 바람직하다는 것이다. “국가의 안전과 국민생활의 안정을 보장하는 것”은 모든 국가작용의 기본원칙이고 존재근거이기 때문에 「정보통신기반보호법」이 지향하여야 하는 고유한 목표를 잘 드러내지 못하고 있다. 이를 위하여 “사이버 안보”와 같은 개념을 입법목적으로 명시하거나 “사이버공격을 예방하고, 사이버 위기(테러) 발생시 신속하고 적극적으로 대처하는 것”으로 명확히 규정하는 법률안이 지속적으로 제기되고 있는 실정이다.[4]

그러나 일상적인 언어용례상 사이버안보, 사이버보안, 정보보호, 정보보안 등의 용어를 뚜렷한 구별 없이 혼용하고 있고 이들 용어에 대한 명확한 법적 개념정의는 합의되지 못하고 있다. 또한 “사이버 안전”, “사이버 안보” 등의 개념을 법제화하기 위하여 국제적 차원에서 일반적으로 이에 대한 명시적으로 합의가 이뤄진 것은 없는 것으로 보인다.[5] 주요정보통신기반시설의 보호체계는 일반적인 정보통신망의 그것과는 다르다는 점을 고려한다면 이는 국가안보에 관한 법제로서의 성격이 더욱 강조되어야 할 것이고, “국가의 안전을 보장하는 것”을 목적으로 한다는 점을 명시하는 것이 적절하고, 이를 더욱 구체화하는 것은 어려울 수 있다는 점을 인정하여야 할 것이다.[6] 따라서 이

4) 이러한 맥락에서 제18대 국회에서는 『국가 사이버위기관리법안』이 발의되었다가 임기만료로 폐기된 바 있고, 제19대 국회에서는 『국가 사이버안전 관리에 관한 법률안(하태경 의원 대표발의)』과 『국가 사이버테러 방지에 관한 법률안(서상기 의원 대표발의)』이 계류되어 있다. 이는 “사이버안전 관리”, “사이버테러 방지”와 같은 개념을 도입하면서도 “국가의 안전보장과 이익보호”라는 표현을 마지막에 사용하고 있다.

5) 이에 대하여는 박노형, “사이버안전 관련 국제규범의 정립을 위한 연구”, 「안암법학」 제37호, 안암법학회, 2012, 795~822(797)쪽 참조.

6) 사이버 안보와 관련된 「정보통신기반보호법」의 체계는 일반적인 정보통신보호법제, 재난관리체계와 구별되어야 한다. 이 영역은 청와대가 콘트롤 타워 역할을 맡고, 국정원(NIS)이 정책총괄을 담당하고 있다는 사실을 통하여도 추론될 수 있다. 이에 대하여는 『제4장 제1절 주요정보통신기반시설에 대한 국가적 보호지원의 정당성』 참조.

하에서는 사이버 안보, 사이버 보안, 정보보호, 정보보안 등에 대한 개념정의는 논외로 하고, 국가안보를 위하여 정보통신기반시설에 대한 국가적 차원의 보호가 갖는 의미와 기능적 측면을 중심으로 하여 논의를 진행하고자 한다.

Ⅱ. 정보통신기반보호법의 기능(제2조)

앞에서 살펴본 바와 같이 이 법은 일차적으로 (내·외부의) 각종 전자적 침해행위로부터 주요 정보통신기반시설을 보호하기 위한 것이다. 그리고 이를 통하여 '국가의 안전'과 '국민생활의 안정'을 보장하는 것을 목적으로 한다. 이는 현대 위험사회(Risikogesellschaft)에서 등장하고 있는 다양한 위험요소로부터 국민의 안전권과 국가안보를 동시에 보장하여야 함을 의미하는 것으로 해석할 수 있다.[7)]

국민의 안전권은 다음과 같이 논증될 수 있다.[8)] 우선, '안전'이라는 개념은 시대에 따라 달라질 수 있는데, 현대 사회에서의 안전에는 전통적인 안전 개념인 생명과 신체에 대한 안전만이 아니라 사회적인 안전 및 생태계적 안전도 포함하는 개념으로 확대되었다.[9)] 그리고 국가는 국민의 생명·신체의 안전 등의 기본권을 보호할 의무를 부담한다.[10)] 따라서 국민은 국가에 대한 기본권으로서의 안전권 보장을 요구할 수 있다.[11)]

---

7) 위험사회에 대한 논의는 Ulrich Beck(홍성태 역), 『위험사회 : 새로운 근대성을 향하여』, 새물결, 2014 참조.

8) 「정보통신기반보호법」 제1조(입법목적)에서는 "국민생활의 안정"이라고 표현하고 있으나, 법학계의 일반적 논의상 편의상 이를 "국민의 안전권"으로 표현하기로 한다.

9) Isensee, Josef, Das Grundrecht auf Sicherheit, 1983. S. 3(홍완식, "안전권 실현을 위한 입법정책", 「유럽헌법연구」 제14호, 유럽헌법학회, 2013. 12, 229쪽에서 재인용).

10) 기본권보호의무에 대한 논의는 아직 명쾌히 정리되었다고 하기는 어려우나, 헌법 제10조 제2문(국가의 기본권 보장의무)의 표현과 헌법재판소 2009. 2. 26. 선고 2005헌마764 결정 등을 통하여 인정되고 있다.

11) 송석윤, 『헌법과 사회변동』, 경인문화사, 2007. 8, 3쪽 참조.

그리고 국가의 안전보장, 즉 안보는 국가의 존립, 헌법의 기본질서의 유지 등을 포함하는 개념으로서 국가의 독립, 영토의 보전, 헌법과 법률의 기능, 헌법에 의하여 설치된 국가기관의 유지 등의 의미로 이해되고 있다.[12] 즉, 국가안보는 국가의 구성요소와 헌법의 기본질서와 국가기관 등에 대한 각종 위험으로부터 국가의 기능을 유지·강화하기 위한 것이다. 이는 헌법 제37조 제2항 기본권 제한의 3가지 목적 중 첫 번째 사유로서 기본권 제한을 정당화하는 근거로서 작용하고 있다.

그런데 이를 단순히 도식화하여 국민의 안전권과 국가안보를 기본권과 그에 대한 제한사유로서 정리하면 「정보통신기반보호법」의 의의와 기능은 반감되고 만다. 오늘날 전자적 침해행위로부터 정보통신기반시설을 보호하는 것은 그 사회적 파급효과 등을 고려할 때 국가안전보장이 안전권을 제한하는 것을 정당화하는 사유로만 작용한다고 이해하는 것은 합리적이지 않기 때문이다. 해킹, 바이러스 등 전자적 침해행위로부터 사이버 안전을 보장하는 것은 원활한 정보의 유통을 가능하게 하고, 21세기 정보화 사회에서 국민들이 안심하고 인터넷 정보통신망을 이용할 수 있도록 하는 여건과 환경을 제공한다. 따라서 국가안전을 보장하는 것은 단지 그와 관련된 기본권 제한, 의무부과를 정당화하는 사유로만 이해되어서는 안 되고, 개별 국민의 안전권을 실질적으로 보장하기 위한 기본적 전제조건으로서 작용하는 객관적 질서로서의 측면을 함께 고려하여야 할 것이다.[13]

---

12) 헌법재판소 1992. 2. 25. 선고 89헌가104 결정(전원재판부).

13) 이는 오늘날 기본권의 주관적 권리로서의 성격과 객관적 가치질서로서의 성격을 동시에 인정하는 기본권의 이중성 이론에 따른 접근방법 혹은 이해체계라고 할 수 있다. 기본권의 이중성 이론에 대하여는 조한상, "기본권의 성격 : 주관적 성격과 객관적 성격", 「법학논총」 제21집, 숭실대학교 법학연구소, 2009. 2, 225~248(232 이하) 쪽 참조.

Ⅲ. 정보통신기반보호법의 적용대상 : 정보통신기반시설

1. 정보통신기반시설의 의의 및 요건

정보통신기반시설은 법 제2조 제1호에서 "국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조 제1항 제1호의 규정에 의한 정보통신망"이라고 규정하고 있다. 즉, 이는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조에 규정된 '정보통신망'을 준용하고 있고, 이는 연쇄적으로 「전기통신사업법」 제2조에서 규정하는 "전기통신설비"에 대한 규정을 참조하여 해석하여야 한다.

이러한 관련 규정들을 종합하면 정보통신기반시설은 "국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템과 전기통신설비(전기통신을 하기 위한 기계·기구·선로 기타 전기통신에 필요한 설비)를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제'를 의미한다. 따라서 실질적 요건은 "전자적 제어·관리시스템"과 "정보통신망(정보통신체제)"로 정리할 수 있다.

그리고 형식적 요건으로는 「정보통신기반보호법」 제8조 각호에 규정된 요건을 고려하여 정보통신기반시설로 '지정'될 것을 요한다. 즉, 이는 "기능장애나 시설파괴 등으로 인하여 국민의 기본생활과 경제안정에 중대한 영향을 미치게 되는 정보통신기반시설로서 본법에 의해 지정된 정보통신기반시설"을 의미한다.[14] 즉, 이는 정보통신망 중에서

14) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조 제7호에 따르면 전자

도 법 제2조 제2호에 규정된 '전자적 침해행위'의 대상(객체)이다. 그리고 법 제8조에 규정된 지정요건을 고려하여 보면 전자적 침해행위인 침입·교란·마비·파괴의 대상은 물리적 시설과 아울러, 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제의 기능상 장애를 야기하는 정도와 그 파급효를 고려하여 정하도록 되어 있음을 알 수 있다.

2. 정보통신기반시설에 대한 기준설정의 문제점

정보통신기반시설의 실질적 요건과 형식적 요건을 종합하여 해석하여 보면 다음과 같은 문제점들이 나타난다. 첫째, 실질적 요건과 관련하여 법령체계상 연쇄적인 개념의 준용은 「정보통신기반보호법」의 적용대상인 정보통신기반시설에 대한 이해의 혼란을 가중시킨다. 즉, 전자적 제어·관리시스템, 정보통신망, 정보통신체제, 정보시스템 등 다양한 개념은 대체로 인터넷, 인트라넷과 컴퓨터를 기반으로 하는 정보통신(IT)시스템 등을 지칭하는 것으로 보이지만 명확하게 파악하기 어려운 용어이기 때문이다. 현행법상 '정보통신(망)'의 개념은 대체로 "「전기통신사업법」 제2조 제2호에 따른 전기통신설비 또는 컴퓨터 등을 이용하거나 활용한 정보의 수집·가공·저장·처리·검색·송신·수신 및 서비스 제공 등과 관련되는 기기·기술·서비스 및 산업 등 일련의 활동과 수단"으로 정의되고 있다.[15]

적 침해행위의 객체로서 "정보시스템"이라는 표현도 등장한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조 (정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

7. "침해사고"란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다.

15) 이는 「정보통신 진흥 및 융합 활성화 등에 관한 특별법」 제2조 제1항 제1호와 「정보통신산업진흥법」 제2조 제1항 제1호와 제4호, 「전자정부법」제2조 제1항 제10호 등에서 규율되고 있음을 발견할 수 있다.

둘째, 형식적 요건과 관련하여 그 지정기준은 정보통신기반시설은 해킹, 컴퓨터바이러스, 논리・메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 공격을 당하는 대상 중에서도 “기능장애나 시설파괴 등으로 인하여 국민의 기본생활과 경제안정에 중대한 영향을 미치게 되는 정보통신기반시설”이므로 이는 객관적으로 명확하게 판단할 수 있는 성격의 기준이 아니라 (주관적) 가치판단이 결부될 수밖에 없는 문제이다. 따라서 법 제8조 5항에서 위원회의 심의를 의무적으로 받도록 하고 있으므로, 법 제4조에서도 정보통신기반심의위원회의 기능(관장사항)으로 “정보통신기반시설의 지정”에 관한 사항을 독립된 호에 명시하는 것이 보다 더 바람직할 것으로 보인다.[16]

셋째, 정보시스템과 물리적 시설을 엄밀하게 구별하여 규율하기 어려운 문제점이 있다. 즉, 정보통신기반시설을 해석함에 있어서 물리적 시설은 제외하고 정보를 수집・가공・저장・검색・송신 또는 수신하는 정보통신체제만을 의미하는 것으로 좁게 해석하는 것이 옳다는 견해와 정보통신(IT)기술의 발달로 전송・교환설비가 통합되는 추세로, 외부전용망을 통해 시스템이 원격으로 제어되는 경우 전송시설을 파괴하여 전체적인 시스템 장애나 마비를 가져올 수 있으므로, “통신구를 포함한 전송・선로설비를 포함”하는 의미에서 넓은 의미로 이해하는 것이 타당하다는 견해가 대립될 수 있다.[17] 이를 구체적으로 살펴보면 주요 사회기반시설을 전자적 방식으로 제어・운영・관리하는 데 관계되는 ‘제어・운영시스템’과 ‘정보시스템’, 통신망시설 중 ‘교환설비’와 ‘전송설비’까지 모두 포함하여 정보통신기반시설의 보호대책을 수립・시행하는 것이 보다 합리적일 것이다.

16) 정보통신시설의 지정(제8조)권한은 중앙행정기관의 장에게 있고, 지정권고(제8조의2)에 관한 권한은 미래창조과학부 장관(민간부문)과 국가정보원장(공공부문)에게 분점되어 있다. 이에 대하여는 『제3장 제1절 주요정보통신기반시설의 지정 및 지정권고』 참조.

17) 이에 대하여는 사단법인 정보통신법 포럼,『정보통신기반 보호법제 연구』, 한국인터넷진흥원, 2013. 10. 78~79쪽 참조

※ 정보통신기반시설의 운영과 관련되는 정보통신(IT)시스템의 구성요소

○ 제어·운영시스템 : 사회기반시설을 직접적으로 제어·운영하는 데 관계되는 시스템으로서, 마비되면 사회기반시설이 제공하는 서비스 자체가 중단되는 시스템.
예) 전력부문의 변·발전 및 송·배전시스템, 통신부문의 망관리시스템 및 교환시스템 등

○ 정보시스템 : 마비되더라도 사회기반시설의 제공이 중단되지는 않으나 업무에 중대한 혼란을 초래하는 시스템
예) 경영정보시스템, 금융부문의 입·출금·이체관련 시스템, 예약·과금관련 시스템 등

○ 통신망
- 교환설비 : 제어·운영·정보시스템 간 통신신호를 교환하는 데 필요한 설비(교환기, 라우터)
- 전송설비 : 통신신호 전송에 관련되는 설비(전송단국장치, 중계장치, 다중화장치, 분배장치)
- 선로설비 : 통신신호를 전송하는데 사용하는 매체(전주, 관로, 통신구, 배관, 맨홀, 배선반)

넷째, 공공부문과 민간부문의 통합적 규율에 따른 문제이다. 원칙적으로 이 법은 대한민국의 모든 국민(자연인과 법인)에게 적용된다. 즉, 국가, 지자체 등 공공부문에 한정하지 않고 민간부문도 정보통신기반시설의 관리기관으로서 중요한 역할을 하는 경우가 있을 수 있기 때문에 이 법령에서 규정하고 있는 의무들을 부담하게 된다. 정보통신기반시설은 정부(국방, 행정, 치안) 또는 공사(전력, 가스, 에너지)가 운영하는 경우도 있으나, 금융·통신·항공 등 주요 정보통신기반시설에 대한 민영화가 추진됨에 따라 전자적 침해행위로부터 보호해야 할 민간 정보통신기반시설의 범위가 점차 확대되고 있기 때문이다.

특히, 클라우드 컴퓨팅 데이터 센터나 인터넷데이터센터(IDC)와 같이 침해사고가 발생할 경우 사회경제적 파급효과가 큰 새로운 형태의 민간분야의 정보통신망이 나타나고 있다. 이에 따라 민간부문에서 운영하는 기반시설이 마비될 경우, 그 사회경제적 영향력이 매우 클 뿐만 아니라, 정보시스템의 상호연결성으로 인하여 우회적 침투경로가 될 가능성이 있다. 따라서 민간 정보통신기반시설 운영자에게도 정보통신망의 안정성 확보 등 일정한 부담 내지 의무를 부과할 필요성이 제기되어 공공부문뿐만 아니라 민간부문도 법 제정 당시부터 그 적용범위에 포함하게 된 것이다. 그러나 이로 말미암아 정보통신기반의 보호체계는 분리되었고, 분화된 보호체계는 사이버 안보정책의 총괄 및 조정을 필요로 하게 되었다.[18]

3. 정보통신망을 통한 의사소통의 자유와 한계

「정보통신기반보호법」이 공공분야와 민간분야를 아우르는 정보통신기반시설을 보호하기 위한 단일법제로서 입안된 이유는 오늘날 정보통신사회에서 사이버 안보는 매우 중요한 의미를 갖고 있기 때문이다. 현대 정보화 사회에서는 정보통신망에 기반하여 거의 모든 공공기반시설들을 운영되고 있으므로 이에 대한 전자적 침해행위에 대비하는 것은 질서유지, 국가안전보장을 위하여 필수적이라고 할 수 있다.

정보통신망에서 자유로운 정보의 유통과 매개는 필수적이다. 이를 위하여 모든 인터넷 이용자들은 타인의 개인정보를 침해해서는 안 되고, 자신의 정보를 침해하지 않아야 한다는 한계 내에서 사이버상 활동의 자유를 향유한다. 이는 헌법 제21조 제1항에서 언론의 자유가 뉴미디어를 포함하는 의사소통(Communication)의 자유로 해석되지만,

18) 공공부문과 민간부문을 나누어 각각 국가정보원과 미래창조과학부 장관이 전담하고 각 중앙행정기관의 장과 협업하는 시스템으로 이해하면 이는 이원화된 체계이고, 공공부문 중에서 국방부문은 국방부 장관이 전담하게 되어 있다는 점을 고려하면 삼원화된 체계로 파악할 수도 있을 것이다. 이는 법 제8조의2 참조.

제4항에서 타인의 명예나 권리 또는 공중도덕이나 사회윤리를 침해하여서는 아니 된다는 한계가 동시에 규율되고 있는 것과 유사하다.

이와 같이 주요 정보통신기반시설에 대한 보호는 모든 인터넷 이용자들의 활동과 보안조치에 영향을 받기 때문에 일종의 "공공재(public good)"적 성격을 갖고 있으므로, 무임승차로 인한 시장실패의 가능성이 내재된 것으로 평가되고 있다.[19] 그리고 어떤 정보통신망에 접속한 다른 인터넷 이용자들이 사이버 공격을 당한 컴퓨터 시스템의 소유자에 대하여 책임을 부담하는 것은 아니기 때문에, 사이버 보안 조치를 강화한 컴퓨터 시스템이나 네트워크의 소유자들이 유형적 이익을 향유하는 것도 아니다.[20] 왜냐하면 과학기술의 발전으로 인하여 새로운 위험원이 등장하면 그 파급효과를 즉시 파악할 수 없는 경우가 대부분이고, 침해사고의 원인규명도 명확하게 할 수 없는 경우가 많기 때문에 특정인에 대하여 책임을 부담시키기 곤란하기 때문이다.

이와 같이 공공재적 성격을 갖고 있는 사이버 안보는 21세기 정보통신사회의 도래와 더불어 매우 중요한 환경적 요인으로 작용하게 되었고, 의사소통(언론)의 자유, 영업의 자유, 정보기본권 등과 관련하여 매우 중요한 헌법적 의미를 갖게 되었다. 특히 사이버 안보는 한편으로는 국가안보의 한 요소로서 기본권 제한의 근거와 한계로서의 의미를 갖고, 다른 한편으로는 다양한 기본권의 보장과 실현을 위한 전제로서 작용하게 된 것이다. 따라서 오늘날 정보통신망에 대한 침해사고를 예방하며 안정적이고 원활한 정보통신망의 작동(정보의 유통과정 전반)을 보장하는 것이 국가적 과제로서 강력하게 요청되고 있다.

---

19) Ross Anderson, "Why Information Security is Hard - An Economic Perspective." In: Proceedings of the 17th Annual Computer Security Applications Conference, New Orleans, LA(2001). ; 이는 http://www.acsac.org/2001/papers/110.pdf, (최종방문 2014년 10월 24일).

20) Hal R. Varian, "System Reliability and Free Riding." In: Proceedings of the First Workshop on Economics and Information Security. May 16-17. University of California, Berkeley(Feb. 2001) (the latest version Nov. 30, 2004) 이에 대하여는 http://people.ischool.berkeley.edu/~hal/Papers/2004/reliability (최종방문 2014년 10월 24일) 참조

4. 주요정보통신기반시설에 대한 강력한 국가적 보호

이미 앞에서 살펴본 바와 같이 「정보통신기반보호법」은 정보통신기반시설을 보호함으로써 그 시설을 안정적으로 운영하여 국가안보와 국민생활의 안정을 도모하기 위한 것이므로 사이버 안보법제에서 중요한 의미를 갖게 된다. 이와 관련하여 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』 제45조는 "정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치"를 취할 의무를 정보통신서비스의 제공자에게 부과하고, 미래창조과학부 장관이 정보보호지침을 정하여 고시하고 이를 준수하도록 권고할 수 있도록 규정하고 있다.[21] 즉, 이에 따르면, ① 미래창조과학부 장관은 정보통신서비스 제공자가 이행하여야 할 기술적·물리적·관리적 보호조치를 구체적으로 고시로 정하여 정보통신서비스 제공자에게 그 이행을 권고할 수 있고, ② 정보통신서비스 제공자는 해당 고시를 준수하여야 한다.

21) 정보통신서비스 제공자에 대한 정보보호조치를 이행하도록 권고하는 지침은 2001년 1월 (구) 정보통신부에서 마련한 『정보통신서비스 정보보호지침』이 시초로 알려져 있다. 2003년 1월 25일 인터넷 침해사고가 발생하여 ISP, 쇼핑몰 등의 낮은 보안수준이 사회적 문제로 지적되자, 2004년 1월 29일 정보통신망법을 개정하여 정보보호 안전진단제도가 도입되면서 『정보통신서비스 정보보호지침』이 폐지되고, 『정보보호조치 및 안전진단 방법, 절차, 수수료에 관한 지침(정보통신부 고시 제2004-54호)』이 공표·시행된 바 있다. 그 이후에 이 지침은 (구) 방송통신위원회 고시로 제·개정되었으나, 2013년 1월 "정보보호 안전진단 제도"가 폐지되면서, 『정보보호에 관한 지침』으로 전부 개정되었다. 이에 따라서 현재 정보보호 안전진단 제도와 관련된 규정은 일괄 삭제되었고, 정보통신서비스 제공자가 마련하여야 하는 기술적·물리적·관리적 보호조치 등 정보보호조치의 구체적 내용이 규정되었다. 그 법적 성격에 대하여는 ① 비권력적 행정작용에 해당하는 행정지도적 성격으로 파악하는 견해와 ② 고시(행정규칙)의 형식이지만 대외적인 구속력이 있는 법규명령으로서의 효력을 갖는다는 견해가 대립할 수 있을 것이나 대외적 구속력을 인정하기는 어려울 것으로 보이고 실무적으로 바람직하지 않을 것으로 판단된다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조(정보통신망의 안정성 확보 등) ① 정보통신서비스 제공자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다.

② 미래창조과학부장관은 제1항에 따른 보호조치의 구체적 내용을 정한 정보보호조치에 관한 지침(이하 "정보보호지침"이라 한다)을 정하여 고시하고 정보통신서비스 제공자에게 이를 지키도록 권고할 수 있다. [개정 2012.2.17, 2013.3.23 제11690호(정부조직법)]

③ 정보보호지침에는 다음 각 호의 사항이 포함되어야 한다.

1. 정당한 권한이 없는 자가 정보통신망에 접근·침입하는 것을 방지하거나 대응하기 위한 정보보호시스템의 설치·운영 등 기술적·물리적 보호조치
2. 정보의 불법 유출·변조·삭제 등을 방지하기 위한 기술적 보호조치
3. 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적·물리적 보호조치
4. 정보통신망의 안정 및 정보보호를 위한 인력·조직·경비의 확보 및 관련 계획수립 등 관리적 보호조치

그러나 정보통신서비스 제공자가 정보보호지침에 따른 (기술적·물리적·관리적) 보호조치를 이행하지 않은 경우에 시정명령을 내리거나 과태료 등 제재조치를 부과하는 법적 근거가 미비하여 실효성을 확보할 수 없다는 문제가 제기되고 있다. 법령의 해석만으로는 미래창조과학부 장관이 이 조항을 위반한 정보통신서비스 제공자에게 시정조치를 내릴 수 있는지 불분명하기 때문이다.[22]

22) 이에 반하여『정보통신망 이용촉진 및 정보보호 등에 관한 법률』제28조에 규정된 "개인정보의 보호조치"는 그 실효성을 확보하기 위한 다양한 장치를 두고 있다. 즉, 정보통신서비스 제공자가 개인정보보호조치를 이행하지 않은 경우에는 정통망법 제76조 제1항에 의거하여 과태료가 부과되고, 이로 인해 개인정보 누출 등의 사고가 발생한 경우에는 과징금(법 제64조의3 제1항 제6호)과 형벌(법 제73조 제1호)을 부과할 수 있다. 이는『개인정보보호법』제64조와 제75조 제1항 제13호에서도 그 근거를 찾아볼 수 있다.

이와 달리 정보보호지침의 대외적 구속력을 인정하여 이에 위반할 경우에 시정조치를 명령할 수 있다고 보는 견해도 제기될 수 있다. 이에 따르면 정보보호지침의 준수 및 이행정도는 동법 제45조 제1항의 위반여부를 판단하는 중요한 판단기준이 될 수 있고, 정통망법 제64조 제4항에 근거하여 시정조치의 명령 및 그 사실에 대한 공표명령 등을 부과할 수 있다. 즉, 정보보호지침에서 준수하도록 권고하고 있는 사항을 전혀 이행하지 않거나 그에 상응하거나 대체하는 보호조치를 마련하지 않은 경우 법 제45조 제1항에서 정보통신서비스제공자에게 부과하고 있는 의무를 불이행한 것으로 판단할 수 있다는 것이다.

그러나 정통망법 제64조에 따라서 시정조치를 명령하는 것이 가능하다고 할지라도 그 시정조치를 이행하지 아니하는 정보통신서비스 제공자에 대하여 과태료 처분을 할 법적 근거는 없기 때문에 그 실효성을 확보할 수 있는 수단이 미흡하다는 점은 여전히 문제로 남아 있다. 정통망법 제76조 제1항 제12호에 따르면 과태료의 적용범위를 한정하고 있으므로 제45조 제1항을 위반한 정보통신서비스 제공자에 대하여 과태료 내지 벌칙을 부과할 수는 없는 것이다.[23]

현실적으로 정보통신서비스 제공자가 침해사고를 당하지 않은 상태에서 시정조치명령을 내리는 것은 바람직하지 않을 수도 있다. 즉, 침해사고가 발생한 경우에 정보통신서비스 제공자가 정보보호지침을 이행하지 않은 것을 지적하고 시정조치 명령을 부과하는 것이 현실에 적합하다. 그러나 이는 자칫 침해사고가 발생하지 않도록 일차적으로 사업자에게 정보통신망의 안정성 확보의무를 부과하고 미래창조과학부 장관이 정하는 정보보호지침의 준수를 권고하는 입법취지를 유명무실하게 만들 수 있을 것이다.

---

23) 그러나 『전기통신사업법』 제90조 제1항에 따르면, "『정보통신망 이용촉진 및 정보보호 등에 관한 법률』 위반에 대한 시정조치 명령을 받은 부가통신사업자에 대하여는 영업정지 내지 영업정지에 갈음하는 과징금을 부과할 수 있는 근거규정"은 마련되어 있다. 이는 부가통신사업자만 적용하는 규정이다.

이러한 쟁점들을 종합적으로 고려하여 보면 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」과 「정보통신기반보호법」의 기본적인 차이를 논리적으로 도출해낼 수 있을 것이다. 전자는 ① 정보통신망의 안정성을 확보하는 과제(임무)를 정보통신서비스 제공자에게 일차적으로 부과하고 있고, ② 정부(미래창조과학부 장관)이 "정보보호지침"을 정하여 고시하지만 그 구속력 및 위반에 대한 제재는 매우 미약한 것을 알 수 있다. 후자 역시 ① 관리기관의 장이 자율적으로 보호대책을 수립·시행하는 상향식 구조에 의거하고 있지만 ② 국가가 개입할 수 있는 범위가 폭넓게 규정되어 있다. 즉, 보호대책 이행여부의 점검(제5조의2), 보호계획의 수립(제6조), 보호지침(제10조)과 보호조치 명령·권고(제11조), 보호지원(제7조), 관리기관에 대한 지원(제24조) 등을 통하여 국가적 보호와 지원이 필수적으로 요청되는 것이다.

제 2 절 정보통신기반보호법 제정과정

Ⅰ. 정보통신기반보호법 제정의 역사적 배경

21세기에 접어들면서 지식정보사회의 도래와 함께 일반 국민들의 인터넷 이용이 보편화되면서 글로벌 네트워크 사회로의 진전이 급속하게 진행되었다. 이에 따라서 과거에는 물리적이고 기계적인 방식으로 관리하던 기반시설들(전기, 가스, 수도, 교통, 댐, 행정, 금융 등) 전반에 점차 정보통신시스템이 접목되고 활용되게 되었다.

그러나 정보통신 시스템에 의존하는 비중이 높아질수록 그에 따른 부작용도 나타나고 있다. 즉, 정보통신망이 정상적으로 운영되지 않으면 사회 주요기능이 마비될 위험성이 있는 것이다. 특히, 최근에는 인터넷 정보통신망을 해킹하거나 컴퓨터바이러스와 악성코드를 유포하는 방식으로 개인정보를 유출, 위·변조 또는 파괴하고 DDos 공격을 하는 등 사이버 테러가 빈발하고 있는데, 이와 같은 사이버 공격은

단지 해당 정보통신망을 파괴하고 개인정보를 누출하는 데 그치지 않고 정보의 안전한 생성과 유통과정 전반에 악영향을 끼칠 뿐만 아니라 국가(주요 기반시설)에 대한 국민의 신뢰와 안전을 해할 수 있다는 점에서 심각한 문제로 대두되었던 것이다.

이와 관련하여 미국은 1996년 「국가정보기반보호법(National Information Infrastructure Protection Act)」을 제정하였다. 이에 따르면 컴퓨터 시스템과 정보의 비밀성·무결성을 보호하기 위하여 미국에 해가 되거나 외국에 이익이 되는 정보를 부정으로 획득하는 자와 국가 컴퓨터 시스템의 운용에 위해를 가하는 자를 처벌한다. 또한 1998년 6월 주요 기반시설에 대한 범정부적 보호체계를 구축하고자 「대통령명령 63호(Presidential Decision Directive No. 63)」를 제정하여 시행하고 있고, 2000년 1월에는 「PDD 63」에 의거하여 추진해 온 주요 정보기반 보호정책을 토대로 하여 21세기 사이버 보안대책으로서 주요 정보기반 보호를 위한 종합대책인 “국가정보시스템보호대책”을 수립하여 시행하고 있다.[24]

일본에서도 컴퓨터 시스템(정보통신망)에 대하여 부정한 방법으로 접근하는 것 자체를 처벌할 수 없는 규율의 흠결을 보완하기 위하여 정보통신망과 관련된 범죄를 방지하고 정보화 사회의 건전한 발전을 목적으로 하는 「부정 액세스 행위금지 등에 관한 법률」을 2000년 2월 13일부터 제정·시행하고 있다. 이와 더불어 전체 성(省)·청(廳)의 국장급 회의인 정보보안대책추진회의와 민간 전문가의 회합을 설치·운영하고, 내각에는 정보보안대책을 종합적으로 추진하기 위한 정보보안대책추진실과 각 성(省)·청(廳)의 보안대책에 관한 기술적인 조사,

24) 미국에서는 2000년도에 사이버 해킹에 대한 규제, 사생활 및 기밀에 대한 보호방안, 국가안보 및 중요 정보통신기반구조 보호, 컴퓨터 범죄에 대한 국제적인 수사공조 및 처벌 등을 그 내용으로 하는 인터넷 무결성 및 주요정보통신기반구조보호법이 제안되었다. 21세기 이후 미국에서 논의된 정보통신기반 보호법제의 변화에 대하여는 사단법인 정보통신법 포럼, 『정보통신기반 보호법제 연구』, 한국인터넷진흥원, 2013. 10, 4~20쪽 참조.

조언 등을 행하는 전문 조사팀을 설치하였다.

그러나 우리나라에서는 사이버 공격에 대한 체계적이고 종합적인 대응을 위한 근거법령이 미비한 상태였다. 2000년도 당시 「전기통신기본법」, 「정보화촉진기본법」, 「정보통신망 이용 촉진 등에 관한 법률」, 「국가정보원법」, 「보안업무규정」 등에 산재한 규정들을 검토해 보면, 이들은 주로 물리적 측면의 시설보호를 중심으로 규정되어 있었고, 사이버 공격에 대비하여 정보통신기반시설의 취약점을 평가하고 이에 대한 범국가적 예방대책을 수립·시행할 수 있는 근거법령은 찾을 수 없었다. 그리고 정보통신망에 대한 침해사고 발생시 관계 기관의 유기적이고 신속한 대응체제가 마련되어 있지 않았으므로[25] 주요 정보통신기반시설 보호를 위하여 새로운 법체계가 마련되어야 한다는 공감대가 형성되기에 이르렀다.

결국 2000년 2월 25일 당시 박태준 국무총리 주재로 "사이버테러 방지 관계장관 회의"가 개최되었고, 범정부 차원에서 사이버테러에 대한 종합적 대책을 추진하기로 합의하였으며 당시 정보통신부가 국가·공공부문과 민간부문의 정보통신기반시설에 대한 보호대책을 종합적으로 보호하기 위한 「정보통신기반보호법」을 제정하기로 결정하였다. 이에 따라 2000년 3월부터 한국정보보호센터, 정보통신정책연구원, 한국전자통신연구원, 한국전산원 등 정보통신부 산하 관계 연구기관과 10여명으로 구성된 실무연구반에서 「정보통신기반보호법(시안)」을 마련하였고, 사회 각계각층의 의견을 수렴하기 위하여 2000년 5월부터 학계 7명, 법조계 1명, 산업계 2명, 연구계 4명, 관계관 6명 등

25) 이와 관련하여 「보안업무규정」은 이미 오래전부터 국가정보원이 국가기관 또는 공공기관에 대한 정보보안업무를 수행해 왔고, 정보보호와 관련된 주관기관으로서 중요한 권한과 책임을 지고 있음을 보여준다. 그러나 민간시설에 대하여는 규정의 흠결이 있었던 점 역시 부인할 수 없다. 이와 같이 정보통신기반시설의 보호체계에 있어서의 민·관의 구별문제 그리고 실무총괄·조정기관의 문제 등은 제정 당시부터 중요한 쟁점이었다. 이에 대하여는 『제4장 제1절 Ⅰ. 사이버 테러의 빈발과 사이버 안보정책의 변화』에서 후술하기로 한다.

총 20명의 관련 전문가로 '정보통신기반보호법 제정위원회'가 구성되었다. 여기에서 총 6회에 걸쳐 회의를 운영한 결과 논의된 쟁점을 반영하여 「정보통신기반보호법(제정안)」을 마련하였다.

정보통신기반보호법 제정안에 대하여 2000년 7월부터 9월까지 전문가 및 일반 국민들의 폭넓은 의견수렴을 위하여 공청회 개최, 관계기관 의견조회, 입법예고 및 규제신설의 타당성 심사 등이 이뤄졌고, 국회에서 격론을 거쳐 2001년 1월 26일 마침내 「정보통신기반보호법」이 제정되기에 이르렀다.

Ⅱ. 정보통신기반보호법의 제정의 기초 및 정책적 변화과정

정보통신기반보호법 제정과정에서 눈에 띄는 연구결과로는 2000년 7월 13일 정보통신부 주최, 한국정보보호센터 주관으로 개최된 『정보통신기반보호법 제정을 위한 토론회』 자료집과 2000년 12월 정보통신정책진흥원에서 발간된 『정보통신기반보호법 제정관련 기초연구』가 있다. 토론회 자료집에는 주요 쟁점별로 학계와 실무계의 검토결과를 담고 있고[26], 정보통신정책진흥원의 연구보고서는 당시 정보통신기반보호법안 제정추진과정에서 문제된 쟁점들과 향후 발전방향을 검토한 바 있다.

그 이후 정보통신망을 이용한 해킹과 사이버테러 등 사이버 위협에 대응하기 위해 정부는 2004년 국정원 산하 '국가사이버안전센터'를 설립하고, 「국가사이버안전 관리규정(대통령 훈령 제141호, 2005. 1. 31)」을 제정・시행하고 있다. 그러나 민・관・군 분야의 위협정보 공유는 물

26) 토론회 자료집에는 정보통신부 정보보호기획과장이 정보통신기반보호법의 제정배경을 설명함에 이어서 김동욱 교수(서울대학교 행정대학원)이 "주요 정보통신기반시설의 지정 및 관리제도", 박균성 교수(경희대 법과대학)가 "주요 정보통신기반시설의 보호조직 및 체계", 이상돈 교수(고려대학교 법과대학)가 "주요 정보통신기반시설 침해행위에 대한 규제방안" 그리고 박영우 박사(한국정보보호센터 선임연구원)가 "정보통신기반시설 보호를 위한 지원방안"을 발표한 내용이 수록되어 있다.

론, 국가와 공공기관간의 협력 부족 및 타 법률과의 상충시 효력이 제한되는 등 사이버보안업무를 수행함에 한계를 드러내고 있다. 따라서 국가를 위협하는 사이버위협에 효율적으로 대처하기 위하여 민·관·군 사이버 안전 정책을 종합적으로 기획·조정하고 지휘체계를 일원화하는 추진체계를 정비할 필요성이 강력하게 제기되고 있다.

우리나라의 사이버 안보법제는 정보보호에서 시작되었다. 처음에는 주로 국가기밀 보호를 위한 국가·공공기관 위주의 정보통신보안체계로 유지되어 오다가 1995년부터 정부 차원에서 정보화 사업을 본격적으로 추진하면서『전산망보급확장과 이용촉진에 관한 법률』과 민간분야의 정보보호 수요증가에 따른『정보화촉진기본법』을 제정하여 이를 근거로 한국정보보호진흥원을 신설하는 등 정보보호체계를 확충하였다. 2001년에는 사이버 침해행위로부터 국가와 국민생활의 안전을 보장하기 위해『정보통신기반보호법』을 제정·시행하였지만, 2003년 1월 25일 인터넷 대란이 발생하여 전국적으로 8시간 동안 인터넷이 중단되어 은행거래는 물론, 대부분의 전산망이 마비되는 대혼란을 야기하는 등 국가적 차원의 신속한 대응에 한계를 보인 일도 있었다.

이 일을 계기로 하여 국가기반시설과 인터넷 정보통신망의 침해사고를 조기에 탐지하고 피해확산을 방지하기 위하여 관련기관 간의 정보공유를 통한 신속한 공동대응체제를 구축하여야 한다는 요청에 따라 2003년 12월 정보통신부 산하 한국정보보호진흥원에 '인터넷침해사고 대응지원센터'를 설치하여 민간분야의 정보보호를 담당하도록 하고, 2004년 2월에는 국가안보 차원에서 대응이 필요하다고 판단하여 국가안전보장회의(NSC) 사무처의 주관으로 국가정보원 소속으로 사이버안전센터(NCSC, National Cyber Security Center)를 신설하는 등 범정부적인 사이버안보관리체계를 구축하였다.

이에 이어서 2004년 7월 정부는 사이버공간의 위기를 전쟁, 재해, 재난 등과 함께 국가위기관리 차원에서 다루어야 한다는 데 공감하

고, '핵심기반분야'에 사이버 안전을 포함하여 『국가위기관리기본지침(대통령훈령 제124호)』을 제정하였으며, 이를 근거로 2004년 9월 『사이버안전분야 위기관리표준메뉴얼』도 마련하였다. 그리고 2004년도에는 주요 국가기관에 대한 해킹사고가 빈번하게 발생함에 따라 NSC 중심의 비상시 사이버위기관리업무를 담당할 정보보안전문기관으로서 국가정보원의 역할과 위상이 강화되어야 한다는 요청이 대두하였고, 해킹 등 사이버사고는 민·관·군을 구분할 수 없을 뿐만 아니라 사전예방이 중요하다는 점에서 각 분야와 기관을 막론하고 정보공유 등 업무협조 강화가 절실히 요구되었다. 이에 따라 당시 노무현 대통령은 '국가 차원에서 사이버안전업무를 총괄하는 기관을 정하고 이를 규범화할 것'을 지시하였고, 이에 국가정보원장을 의장으로 하고 외교통상부, 법무부, 국방부, 행정자치부, 정보통신부, 국가안전보장회의 사무처 등의 차관급을 위원으로 하는 '국가사이버안전전략회의'의 설치, 유관기관 간 정보공유 및 업무협조 강화 등을 명시한 『국가사이버안전관리규정(대통령 훈령 제141호)』이 2005년 1월 31일 제정·시행되었다.[27]

27) 이와 관련하여 김귀남 교수(경기대 교수, 한국융합보안학회장)는 "2004년 국정원 산하에 국가사이버안전센터를 설립하고, 대통령 훈령인 국가사이버안전관리규정을 제정하여 국가 사이버테러 대응 업무를 수행토록 했다. 당시 민주당이 국가 사이버위기 대응의 중요성을 인식하고 사이버안전센터를 설립한 것에 대해 그간 칭찬을 보내왔다, 그리고 지난 정부 초기 국정원 개혁이 논의될 때에 당시 민주당에서 국정원 직무에 '사이버안전업무'를 포함한 국정원법 개정안을 제시한 적이 있다고 들은 바 있다. 그런데 최근 야당 일부에서 '사이버테러대응 업무가 국정원의 역할이 아니다'라면서 '정부부처 내에 새로운 본부를 신설하든지 미래부에 적절한 부서를 만들어 대응하는 것이 옳다'는 입장이 언론에 보도되고 있다. 사이버테러 대응이 국정원의 역할이 아니라면, 민주당은 10년 전에 집권했을 당시 국정원 산하에 사이버안전센터를 설립하지 않았어야 했다. 그리고 그 후 10년간의 세월이 흐르는 동안에라도 국정원의 사이버안전 업무, 즉 사이버공격에 대응하는 업무를 수행하지 못하도록 입법화했어야 했다"라고 비판하면서 "국가 사이버안보는 여야간 정쟁의 소재가 아니라 세계 경쟁의 구도에서 우리나라의 역할과 위상을 높일 수 있는 문제"라는 점을 강조한다.

현재 우리나라의 사이버 안보는 대체로 「국가사이버안전관리규정」을 기반으로 하고 있고, 범국가적인 사이버안보체계의 수립 및 개선, 기관간 역할 조정 등 사이버안보에 관한 중요사항을 심의하기 위한 '국가사이버안전전략회의'와 전략회의의 효율적 운영을 위한 '국가사이버안전대책회의'를 설치하여 사이버안전업무를 수행하고 있다.

국가사이버안전전략회의는 국가사이버안전에 관한 중요사항을 심의하고, 의장은 국가정보원장으로 하고, 위원은 "기획재정부차관, 미래창조과학부차관, 교육부차관, 외교부차관, 통일부차관, 법무부차관, 국방부차관, 안전행정부차관, 산업통상자원부차관, 보건복지부차관, 국토교통부차관, 금융위원회 부위원장, 대통령비서실 사이버안전 담당 수석비서관, 국가안보실 사이버안전 담당 비서관, 국무조정실 국무차장"으로 구성되어 있다. 그리고 국가사이버안전전략회의는 1. 국가사이버안전체계의 수립 및 개선에 관한 사항, 2. 국가사이버안전 관련 정책 및 기관간 역할조정에 관한 사항, 3. 국가사이버안전 관련 대통령 지시사항에 대한 조치방안, 4. 그 밖에 전략회의 의장이 부의하는 사항을 심의한다(규정 제6조). 이는 우리나라의 사이버안보정책 전반을 심의하는 기구이고, 이를 보좌하기 위하여 국가정보원 차장을 위원장으로 하고, 관련 부처의 실·국장을 위원으로 하는 국가사이버안전대책회의가 구성되어 있다.

Ⅲ. 제정과정에서 나타난 쟁점사항

2001년 1월 26일 법률 제6383호로 제정되고 2001년 7월 1일부터 시행된 「정보통신기반보호법」은 정부에서 2000년 11월 20일에 발의한 법률안이 통과된 것이다. 2000년 12월 4일 과학기술정보통신위원회에 '정보통신기반보호법안'이 상정되어 심의되는 과정에서 심도 있는 논의가 이뤄졌고, 동년 12월 8일 수정안이 제출·의결되었다. 당시 안병엽 정보통신부장관이 이 법안을 국회에 나와 제안설명하였고, 이에

대하여 여·야 의원들 사이에서 견해의 대립과 이견조정이 이뤄졌다.

법안의 대부분은 원안 내용대로 통과되었고, 대체로 타당한 입법으로 평가되었다. 다만 ① 용어정의와 관련하여 "정보통신기반시설"에 관한 정의만 규정하고 있어, 법안의 명칭인 "정보통신기반보호법"의 "정보통신기반"과 동일한 의미인지 불분명하다는 지적, ② 국무총리 산하 정보통신기반보호위원회의 심의사항(제4조) 중 취약점 분석·평가에 관한 사항은 관리기관의 장이 평가하도록 되어 있고 주요정보통신기반시설보호계획에 포함되는 사항이므로 동 계획 심의시 취약점 분석·평가에 관한 주요사항도 심의가 가능하므로 위원회의 심의사항에서는 삭제하는 것이 바람직하다는 지적, ③ 입법부와 사법부의 경우에는 중앙행정기관의 장들 중에서 누가 정보통신기반시설로 지정할 수 있는지에 대한 우려, ④ 외부 기관에 취약점 분석·평가를 의뢰하는 경우에도 관리기관의 필요에 따라 기관 내부의 전담반을 계속 유지할 수 있는 가능성을 열어두는 것이 바람직하다는 지적 등이 제기되어 원안의 일부 내용이 수정되기도 하였다.[28]

그리고 원안에서 대폭 수정된 내용은 다음과 같다. 이는 「법안및청원심사소위원회」에서 반영된 사항으로서, "국가안보에 중요한 도로·지하철·공항·전력시설 등 주요정보통신기반시설의 관리기관의 장은 국가보안업무를 수행하는 기관의 장에게 우선적으로 기술적 지원을 요청하도록 하고, 다만 국가안보에 현저하고 급박한 위험이 있는 경우 등에는 국가보안업무를 수행하는 기관의 장이 관계중앙행정기관의 장과 협의하여 지원할 수 있도록 예외규정을 신설하기로 수정의결 하였음"이라고 밝히면서 법 제7조 제2항을 수정가결하였다.

그런데 이와 더불어 수정안 제7조 제3항이 신설되면서 이에 대한 대응조치로서 "국가보안업무를 수행하는 기관의 장은 제1항 및 제2항의 규정에도 불구하고 금융 정보통신기반시설 등 개인정보가 저장된

28) 이에 대하여는 전하성(국회 수석전문위원), 『정보통신기반보호법안 심사보고서』, 국회 과학기술정보통신위원회, 2000. 12, 5~17쪽 참조.

모든 정보통신기반시설에 대하여 기술적 지원을 수행하여서는 아니된다"는 제7조 제3항이 함께 신설되어 관리기관의 장이 요청하는 경우(제1항) 또는 국가안보에 현저하고 급박한 위험이 있고, 관리기관의 장의 요청을 기다려서는 위해를 회복할 수 없다고 판단되면 국가보안업무를 수행하는 기관의 장이 직권으로 기술적 지원을 할 수 있는 경우(제2항)에도 기술적 지원을 할 수 없도록 하여 개인정보가 저장되어 있는 주요 정보통신기반시설에 대한 기술적 지원을 원천적으로 차단하는 결과를 낳게 되었다.[29)]

이 규정의 입법취지는 실제적 조화의 원리에 비추어 볼 때 국민의 안전권과 개인정보 보호의 가치가 충돌하는 것을 형량하는 과정에서 국가안전보장의 필요에 의한 개입을 원천적으로 차단하고 개인정보보호를 절대적으로 보호하고자 한 것으로 평가할 수 있다. 그러나 헌법 제37조 제2항은 기본권제한적 법률유보를 규정하고 있기 때문에 국가안보를 위해 비례의 원칙에 맞게 기본권을 제한할 수 있음을 인정하고, 우리 법제에 따르면 제한할 수 없는 절대적 기본권은 존재하지 않는다.[30)], 그리고 이는 관리기관이 스스로의 판단에 의하여 보호지원을 요청하는 것을 차단하는 불합리한 결과를 낳을 위험성이 있다.

29) 현대 위험사회에서의 사이버 안보와 국가에 의한 기술적 지원의 필요성을 검토하면서 국가보안업무의 전문성과 역량에 비추어 볼 때 기술적 지원의 필요성과 가능한 범위 내지 한계에 대하여 좀 더 구체적으로 검토한 내용은『제4장 제3절 Ⅰ. 주요정보통신기반시설의 보호지원(법 제7조)』참조.

30) 생명권에 대하여도 제한을 가하는 사형제도에 대하여 본질내용침해금지원칙에 반하는 것이 아닌가 하는 논란이 빚어지고 있으나, 헌법재판소에서는 사형제도를 합헌이라고 결정한 바 있다. 실제적으로 다양한 영역(통신비밀보호법, 개인정보보호법, 전자금융거래관리법, 독점규제 및 공정거래에 관한 법률 등)에서 개인정보보호에 대한 제한과 한계가 이뤄지고 있음에 비추어볼 때 타당한지 의문이다.

제 3 절 정보통신기반보호법의 개정 및 그 주요쟁점

Ⅰ. 제1차 개정(2002. 12. 18. 일부개정, 법률 제6796호)

기존 정보통신기반보호법은 '정보보호전문업체'를 "정보통신부장관"이 지정하도록 되어 있었다. 그런데 그 명칭이 정보보호전문업체로 되어 있어 정보보호산업 전체를 포괄하는 전문업체라는 의미로 오해될 소지가 많으므로, 이 법에서 부여하고자 하는 업무와 기능에 맞게 정보보호전문업체가 수행하는 업무가 정보보호컨설팅 업무임을 분명히 하기 위하여 그 명칭을 '정보보호컨설팅전문업체'로 변경하는 개정이었다.

Ⅱ. 제2차 개정(2005. 3. 31. 일부개정, 2006. 4. 1. 시행, 법률 제7428호)

과거 「회사정리법」·「화의법」·「파산법」·「개인채무자회생법」은 각 적용대상이 다르고, 회생절차도 회사정리절차와 화의절차로 이원화되어 있는 등 형평성이나 효율성의 측면에서 문제가 많다는 지적이 지속적으로 제기되어 왔으므로, 이들을 1개의 법률로 통합하여 통일적인 도산법 체계를 완성하여 효율성을 높이고자 하였다. 이에 따라 정보통신기반보호법 제18조 제1호 나목중 "파산자"를 "파산선고를 받은 자"로 개정하였다.

Ⅲ. 제3차 개정(2007. 12. 21. 일부개정, 2008. 6. 22. 시행, 법률 제8777호)

해킹, 컴퓨터바이러스 등 악성프로그램 유포를 비롯한 전자적 침해행위의 수법이 급속히 발전하고 그 피해가 급증하고 있으므로 주요정보통신기반시설을 신속하고 효과적으로 보호하기 위하여 정보통신부장관과 국가보안 업무를 수행하는 기관의 장 등 대통령령이 정하는 국가기관의 장이 중앙행정기관에 주요정보통신기반시설의 지정을 권고할 수 있도록 하고, 주요정보통신기반시설 보호대책의 이행 여부를 확인할 수 있도록 하고, 정보보호컨설팅전문업체에 대한 지정을 취소하려는 경우에는 반드시 청문절차를 거치도록 하는 등 현행 제도의 운영상 나타난 일부 미비점을 개선·보완하기 위하여 개정되었다.

첫째, 주요정보통신기반시설 보호대책에 관한 사후관리체계가 개선되었다. 기존 「정보통신기반보호법」은 주요정보통신기반시설 보호대책·계획의 수립과 시행에 관한 사항만 규정하고 있고 사후관리를 위한 확인이나 점검 등에 관한 사항이 없어 보호대책 및 보호계획이 형식화될 우려가 있어 사후관리체계를 마련할 필요성이 있었기 때문에, 법 제5조의2를 신설하여 정보통신부장관과 국가보안 업무를 수행하는 기관의 장 등 대통령령이 정하는 국가기관의 장으로 하여금 보호대책 이행 여부 확인을 수행할 수 있는 근거를 마련하는 한편, 관계 중앙행정기관의 장은 보호대책 이행 여부 확인 결과를 분석하여 별도의 보호조치가 필요하다고 인정하는 경우에는 관리기관에 보호조치 명령을 할 수 있도록 하였다. 이를 통하여 관리기관의 주요정보통신기반시설 보호대책에 대한 이행 여부를 확인함으로써 보호대책의 실효성을 확보하고, 주요정보통신기반시설의 안정적 운용을 보장하며, 국가안전 및 국민생활안정을 도모할 수 있을 것으로 기대되었다.

둘째, 법 제7조 제1항을 개정하여 보호지원(기술적 지원)을 요청할

수 있는 관리기관 및 지원사항의 범위를 확대하였다. 기존 정보통신기반보호법은 기술적 지원을 요청할 수 있는 주체를 국가기관 또는 지방자치단체의 장인 관리기관으로 한정하고 있어 다수의 민간 주요정보통신기반시설은 기술적 지원을 요청할 수 없는 문제점이 발견되었다. 따라서 전문기관 등에 기술적 지원을 요청할 수 있는 관리기관의 범위를 국가기관 또는 지방자치단체의 장인 관리기관으로부터 모든 관리기관으로 확대하고, 요청할 수 있는 지원사항에 관계 중앙행정기관의 장이 명령·권고한 보호조치 이행을 추가하였다. 이와 같이 민간부문의 주요정보통신기반시설에 대한 전문기관의 기술적 지원을 통하여 주요정보통신기반시설의 보호가 더욱 강화될 것으로 기대되었다.

셋째, 주요정보통신기반시설 지정방식을 개선하기 위하여 법 제8조의2를 신설하여 정보통신부장관과 국가보안 업무를 수행하는 기관의 장 등 대통령령이 정하는 국가기관의 장이 주요정보통신기반시설을 발굴하여 중앙행정기관의 장에게 주요정보통신기반시설로 지정하도록 권고할 수 있는 근거를 마련하였다. 다양한 인터넷 침해사고로부터 정보통신기반시설의 보호를 강화하여야 함에도 불구하고 각급 관리기관이 주요정보통신기반시설의 지정에 소극적인 현실에 비추어 주요정보통신기반시설 지정을 독려하고 활성화할 수 있는 제도적 장치를 마련하여야 할 필요성이 제기되었기 때문이다.

넷째 정보보호컨설팅전문업체에 대한 지정을 취소하려는 경우에 반드시 청문절차를 거치도록 하여 당사자의 참여를 보장함으로써 지정취소처분을 신중하게 하도록 하고, 사업자의 권익보호 및 권리구제에 만전을 기하기 위하여 법 제21조 제2항을 신설하였다.

Ⅳ. 제4차 개정(2008. 2. 29. 타법개정, 법률 제8852호, 2008. 6. 22. 시행) 및 제5차 개정(2009. 5. 22. 타법개정, 법률 제9708호, 2009. 8. 23. 시행)

이명박 대통령 당선 이후 정부조직을 개편하면서 행정자치부 장관은 행정안전부 장관으로, 정보통신부 장관은 지식경제부 장관으로 개정하였다. 이에 따라 행정안전부 장관과 지식경제부 장관이 정보통신기반보호법의 주관부서로 역할을 수행하도록 제4차 개정에서 반영되었다.

제5차 개정에서는 「정보통신산업진흥법」 개정에 따라 「정보통신기반보호법」 제9조 제3항 제3호를 「정보통신산업진흥법」 제33조에 따라 지정된 지식정보보안 컨설팅전문업체로 개정하고, 제30조 제2항에 따른 과태료의 부과·징수권을 행사할 수 있는 기관으로 과거에는 "관계중앙행정기관의 장 또는 행정안전부장관·지식경제부장관(이하 "부과권자"라 한다)"라고 규정되어 있던 것을 "관계 중앙행정기관의 장 또는 행정안전부 장관"으로 간소하게 규정하였다.

Ⅴ. 제6차 개정(2013. 3. 23. 타법개정, 법률 제11690호, 2013. 3. 23. 시행)

2013년도 박근혜 대통령 당선 이후 정부조직을 개편하면서 정보통신기반보호법의 업무관할을 재조정하게 되었다. 제6차 개정에서는 제3조 제3항 중 "국무총리실장"을 "국무조정실장"으로 개정하고, 제5조 제3항 및 제8조 제4항 중 "행정안전부장관"을 각각 "안전행정부장관"으로 명칭을 변경하였다.

개정의 핵심내용은 제5조의2(주요정보통신기반시설보호대책 이행 여부의 확인) 제1항부터 제3항까지, 제6조 제4항(주요정보통신기반시설

보호대책 및 주요정보통신기반시설보호계획의 수립지침 통보), 제7조 제1항(기술적 지원), 제8조의2(주요정보통신기반시설의 지정권고) 제1항·제2항, 제9조 제4항(취약점의 분석·평가에 관한 기준을 정하고 관계 중앙행정기관의 장에게 통보), 제16조 제3항(정보공유분석센터의 통지사항 통보) 및 제30조 제2항(과태료 부과권자) 중 "행정안전부장관"을 각각 "미래창조과학부장관"으로 개정하여 행정안전부 장관의 업무를 대부분 미래창조과학부 장관에게 이관하였다.

이외에도 제9조 제3항(취약점 분석·평가기관) 제1호 중 "한국정보보호진흥원"을 "한국인터넷진흥원(이하 "인터넷진흥원"이라 한다)"으로 개정하였다. 이는 2001년 7월 설립된 한국정보보호진흥원과 2004년 7월 설립된 한국인터넷진흥원이 2009년 7월 (구) 정보통신국제협력진흥원과 함께 한국인터넷진흥원으로 통합되었기 때문에 이와 같은 조직통합과정을 반영하여야 했기 때문이다.[31] 이에 따라서 제13조 제1항 전단, 제14조 제2항 본문, 같은 조 제3항 및 제15조 제4항 "보호진흥원"을 "인터넷진흥원"으로 개정하였다.

Ⅵ. 정보통신기반보호법 개정과정 검토의 시사점

정보통신기반보호법은 2001년 처음 제정되어 현재까지 6차례 개정되었는데, 그 중에서 중요한 사항의 내용을 개정한 것은 2007년 제3차 개정이었고, 그 이외에는 정부조직법 개정 등 타법률의 개정에 따라서 일부 그 내용이 변경되거나 관할 기관이 바뀐 것에 불과하다. 이는 한편으로는 정보통신기반보호법의 기본적 골격 내지 체계가 제

31) 제5차 개정은 2009년 5월에 이뤄졌고, 한국인터넷진흥원으로 일원화하는 조직통합은 2009년 7월에 이뤄졌기 때문에 당시 법개정 작업에서는 이 변화상황이 반영되지 못하였다가 2013년 제6차 개정에 이르러서야 개정사항이 반영된 것으로 보인다. 그럼에도 불구하고 2009년 7월부터 실제 운영과정에서는 (구) 한국정보보호진흥원의 업무를 이관받은 한국인터넷진흥원에서 정보통신기반보호임무를 수행한 것으로 보인다.

정 당시와 현재까지 크게 변하지 않고 일관되게 유지되었다는 것이고, 다른 한편으로는 업무와 기능의 변화 없이 그 담당기관이 정부조직 개편에 따라 이관되었다는 것을 의미한다.

<정보통신기반보호법의 개정추이>

구 분	개정 주요내용
법률 제6796호, 2002.12.18, 일부개정	· 정보보호전문업체가 수행하는 업무가 정보보호 컨설팅 분야의 업무임을 분명히 하기 위하여 그 명칭을 정보보호컨설팅전문업체로 변경
법률 제7428호, 2005.3.31, 타법개정	· 결격사유 중 법인의 임원항목에서 파산자의 명칭을 파산선고를 받은 자로 변경(법 제18조1항)
법률 제8777호, 2007.12.21, 일부개정	· 주요정보통신기반시설 보호대책에 관한 사후관리 체계의 개선(법 제5조의2 신설 및 법 제11조제2호) · 보호지원을 요청할 수 있는 관리기관 및 지원사항의 범위 확대(법 제7조제1항) · 주요정보통신기반시설 지정방식의 개선(법 제8조의2 신설) · 청문절차의 도입(법 제21조제2항 신설)
법률 제8852호, 2008.2.29, 타법개정	· 정보통신기반보호위원회 위원장: 국무조정실장→국무총리실장 · 간사역할 기관(보호계획 수립 및 지정 등): 행정자치부장관→행정안전부장관 · 정보보호컨설팅전문업체의 지정: 정보통신부장관→행정안전부장관
법률 제9708호, 2009.5.22, 타법개정	· 제17조(정보보호컨설팅전문업체의 지정) 조항 삭제
법률 제11690호, 2013.3.23, 타법개정	· 정보통신기반보호위원회 위원장: 국무총리실장→국무조정실장 · 간사역할 기관(보호계획 수립 및 지정 등): 행정자치부장관→미래창조과학부장관

김대중 대통령과 노무현 대통령 집권기간 중에는 민간 부문에서 '정보통신부'가 중요한 역할을 담당하였다면, 이명박 대통령 집권기간 중에는 '행정안전부'가 전자정부사업과 재난관리 등에 있어서 중요한 업무를 담당하면서 '지식경제부'가 정보보호컨설팅 전문업체의 인증 등을 통하여 보완하는 구조였다. 그리고 최근 박근혜 대통령의 취임 이후 정부조직 개편에 따라서 '미래창조과학부'를 신설하고 민간부문을 담당하게 하였다. 그러나 이와 같은 행정조직 개편과정에서 국가보안업무를 수행하는 기관(국가정보원)은 법 제정 당시부터 일관되게 정보통신기반보호업무를 담당하여 왔고, 그 과정에서 사이버 안보 및 정보보안의 전문성과 역량을 제고하여 왔음을 발견할 수 있다.

	민간부문에 대한 보호대책이행여부 확인, 지침수립, 보호지원, 지정권고 등	공공부문에 대한 보호대책이행 여부 확인, 지침수립, 보호지원, 지정권고 등	제8조 제4항	제17조
2001. 1. 26. 제정	정보통신부 장관	국가정보원	행정자치부 장관(지방자치단체의 장이 관리·감독하는 기관의 정보통신기반시설은 지자체장과 협의하여 주요정보통신기반시설로 지정하거나 지정취소할 수 있다)	정보통신부장관 (제 5 장 정보보호컨설팅 전문업체의 지정 등)
제1차 개정 2002. 12. 18. 개정				
제2차 개정 2005. 3. 31. 개정				
제3차 개정 2007. 12. 21. 개정				

	민간부문에 대한 보호대책이행여부 확인, 지침수립, 보호지원, 지정권고 등	공공부문에 대한 보호대책이행 여부 확인, 지침수립, 보호지원, 지정권고 등	제8조 제4항	제17조
제4차 개정 2008. 2. 29. 개정	행정안전부 장관		행정안전부 장관	2009. 5. 22 정보통신 산업진흥 법 제정 당시에는 지식경제 부 업무 (현재 미래창조 과학부)
제5차 개정 2009. 5. 22. 개정				
제6차 개정 2013. 3. 23. 개정	미래창조과학부 장관		안전행정부 장관	

그리고 현실적으로 우리나라 정보통신기반시설의 지정현황을 살펴보면 대략 공공부문의 비중(70%)이 민간부문(30%)에 비하여 상당히 높다. 즉, 공공부문의 비중이 매우 높은 우리나라의 여건에서 국가정보원이 정보통신기반시설에 대한 보호업무를 일관되게 수행하여 왔고, 그 과정에서 해당 업무에 대한 역량과 전문성을 제고하여 왔음을 알 수 있다. 이는 피라미드식 위계질서에 기반하고 있는 관료제의 조직체계에서 한 발 벗어나 국가안보 및 사이버 안보 업무를 전문적으로 수행하는 보안전문기관이 필요하다는 점을 반증한다.

이에 기초하여 국가정보원이 전자적 침해행위에 대응하고 사이버 안보 실무를 총괄하는 조정기관으로서 국가 (사이버)안보와 국민생활의 안정에 기여할 수 있는 방향으로 2013년 7월에 "국가사이버안보 종합대책"이 수립·시행되기에 이르렀다. 이와 관련하여 사이버 안보에 대한 정책적 변화를 법적으로 뒷받침할 수 있도록 관련 법제를 정비하는 것이 강력하게 요청되고 있는 것이다.[32]

32) 이에 대하여는『제4장 제1절 Ⅱ. 사이버안보법제의 체계적 정비방안』에서 후술하기로 한다.

제 3 장 정보통신기반보호시설의 보호체계

제 1 절 정보통신기반시설의 지정 및 지정권고

Ⅰ. 주요정보통신기반시설의 지정(제8조)

1. 지정의 의의 및 효과

「정보통신기반보호법」의 적용대상은 대부분 '주요정보통신기반시설'이다.[33] "정보통신기반시설"에 대한 정의는 제2조에 있지만, "주요정보통신기반시설"로 지정하기 위한 절차와 기준 등은 제8조에 규정되어 있으므로 종합적으로 고려하여야 하는 것이다. 법 제8조 제1항에 따르면 중앙행정기관의 장은 소관분야의 정보통신기반시설 중 5가지 기준을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다.

주요정보통신기반시설로 지정된 이후에는 「정보통신기반보호법」이 본격적으로 적용되어 다양한 의무를 부담한다. 우선, 사전예방단계에서 주요정보통신기반시설로 지정처분을 받은 관리기관의 장은 대통령령이 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석·평가하여야 한다(법 제9조). 그리고 그 결과에 따라서 소관 주요정보통신기반시설을 안전하게 보호하기 위한 물리적·기술적 대책을 포함한 관리대책(보호대책)을 수립·제출·시행한다(법 제5조 제1항). 관리기관의 장이 중앙행정기관의 장이 아닌 경우에는 정보보호책임자를 지정하여야 한다(법 제5조 제4항).[34]

---

33) 법 제1조(목적)에서부터 "주요정보통신기반시설의 보호에 관한 대책"이라고 표현하고 있고, 대부분의 규정에서 등장하는 표현은 법 제8조의 규정에 의하여 지정된 "주요정보통신기반시설"이다. 그러나 제2조(정의) 제1호, 제16조(정보공유분석센터), 제24조(기술개발 등), 제26조(국제협력)에서는 "정보통신기반시설"이라는 표현을 사용하여 (지정되지 않은 정보통신기반시설에 대하여도) 적용할 수 있을 것으로 보인다.

34) 이외에도 정보통신기반시설의 관리기관의 장은 자료제출요청에 응할 의무(제5조

그리고 사후대응체계에서 관리기관의 장은 침해사고의 통지의무(법 제13조), 복구 및 보호에 필요한 조치를 신속히 취할 의무(법 제14조), 특별한 사유가 없는 한 침해사고의 대응을 위한 협력과 지원요청에 응할 의무(법 제15조 제4항) 등을 부담하게 된다.

마지막으로 주요정보통신기반시설의 관리기관에 대한 국가의 개입과 보호지원이 있을 수 있다. 즉, 보호지원의 요청(법 제7조), 복구 및 보호조치 지원요청권(법 제14조 제2항), 관리기관에 대한 기술의 이전, 장비의 제공 그 밖의 필요한 지원(제25조) 등을 받을 수 있는 것이다.

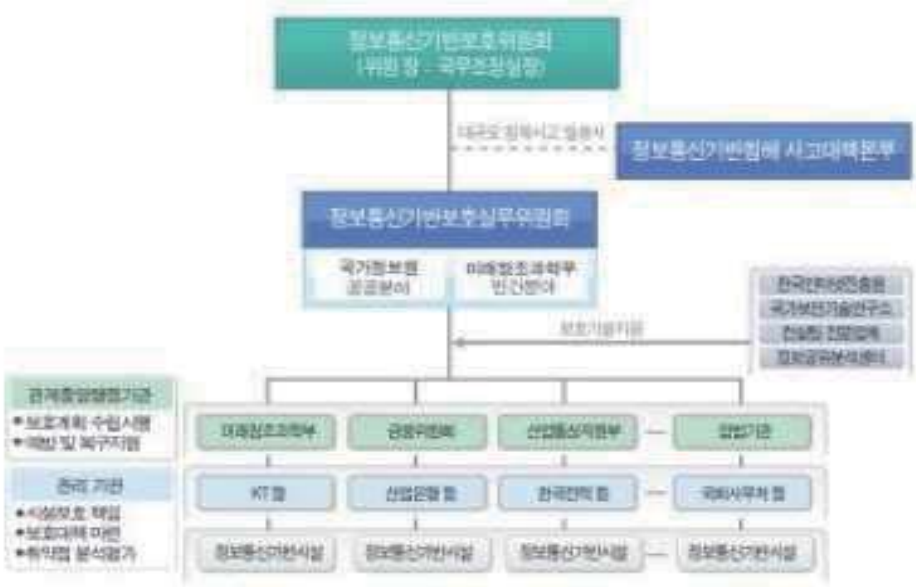
2. 지정권자

이와 같이 주요정보통신기반시설로 지정되면 정보통신기반보호법이 본격적으로 적용되어 해당 정보통신기반시설의 보호체계 내에 편입되게 된다. 따라서 주요정보통신기반시설로 지정하는 권한을 보유하는 자가 누구인지는 법적으로 매우 중요한 문제로 대두된다. 법 제8조와 시행령 제14조는 정보통신기반시설의 소관 부처인 각 '중앙행정기관의 장'으로 하여금 주요정보통신기반시설의 지정여부와 관련한 평가기준을 자체적으로 마련하도록 하고, 이를 지정대상시설의 관리기관의 장에게 통보하도록 하고 있다. 즉, 현행 정보통신기반보호법과 동법 시행령은 각 중앙행정기관별로 자체적으로 '정보통신기반시설 지정기준'을 마련하도록 함으로써 소관 분야별로 개별적 판단에 의하여 지정여부와 관련한 평가기준이 마련되도록 하고 있다.

이와 관련하여 다음과 같은 쟁점이 제기될 수 있다. 첫째, 지정권한을 각 중앙행정기관의 장이 갖고 있고, 지정여부와 관련된 평가기준도 자체적으로 마련하고 있으므로 이는 보호체계를 각 중앙행정기관의 소관별로 분화시키게 된다. 이는 각 중앙행정기관에서 지나치게

의2 제2항), 이행여부의 확인결과 수령(제5조의2 제3항), 보호지침 준수권고(제10조)와 보호조치의 명령 또는 권고(제11조)를 받게 되는 등의 부담을 지게 된다.

적극적으로 정보통신기반시설을 과잉 지정하거나 소극적으로 정보통신기반시설의 지정을 거부하거나 지연시키는 경우에 문제를 야기할 수 있다.[35] 이에 대처하기 위하여 전자의 경우에는 법 제8조 제5항에 따라서 중앙행정기관의 장이 제1항 및 제3항의 규정에 의하여 지정하고자 하는 경우에는 정보통신기반위원회의 심의를 받아야 하고, 후자의 경우에는 법 제8조의2(지정권고)가 규정되어 있는 것이다.



[출처 : 2014 국가정보보호백서][36]

이와 같이 각 중앙행정기관별로 소관별로 정보통신기반시설의 관리기관을 감독하고, 각 분야별로 미래창조과학부, 국가정보원 그리고 국

35) 주요 정보통신 기반시설의 지정을 할 때 발생하는 보호체계를 구축, 유지, 관리 및 감독하기 위하여는 예산 및 자원의 할당을 고려하여 의사결정을 할 수 밖에 없고, 경제논리와 함께 정무적 판단을 고려할 수밖에 없다. 이로 말미암아 주요정보통신기반시설로 필수적으로 지정되어야 마땅함에도 불구하고 지정이 보류되어 다른 행정기관 또는 지방자치단체와 보호수준이 상응하지 않은 관계로 일부 보안이 취약한 영역을 계속 남겨 놓게 되어 다른 기관의 정보보호노력까지 무위로 만드는 위험성이 나타날 수도 있을 것이다.

36) 한국인터넷진흥원, 『2014국가정보보호백서』, 152쪽 참조. 이에 대하여는 인터넷 사이트http://isis.kisa.or.kr/ebook/ebook2014_pop.html (최종방문 2014년 10월 24일)

방부가 일정한 역할을 담당하고 있는 '분화된 보호체계'에 대한 문제 제기가 이뤄지고 있다. 주요정보통신기반시설의 지정권한을 각 중앙행정기관의 장의 권한으로 규정하지 말고, 정보통신기반보호위원회에 집중시키는 것이 바람직하다는 견해가 제기되고 있다.

이에 따르면 "현행 정보통신기반보호법 제8조 제5항에 따르면 지정 및 지정취소와 관련하여 위원회의 심의를 받고, 해당 관리기관의 의견청취를 하도록 규정되어 있을 뿐이다. 따라서 각 중앙행정기관(정부부처)은 서로 다르지 않은 동일한 기준과 잣대로 이를 지정하고 이에 대한 보호대책을 구축, 유지, 관리 및 감독하기 위한 예산 및 자원의 할당을 각 기관이 반드시 확보할 수 있도록 보장하여 사이버 안보관리체계의 효과성을 증대시키는 것이 바람직하다. 즉, 중층적인 지정과정 및 보호체계를 단순화하여 주요정보통신기반시설에 대한 보호체계를 운영하는 것이 보다 효율적"일 것이라고 한다.[37]

이러한 논의가 등장하게 된 배경은 중앙행정기관의 자율성과 책임성을 보장하면서 정보통신기반시설을 안전하게 관리하고자 하는 것이 정보통신기반보호법의 목적이지만 관계중앙행정기관의 의지가 부족하면 주요정보통신기반시설로 지정이 이뤄지지 않았고, 이에 대처하기 위하여 지정'권고' 제도를 도입하였지만 이는 강제력을 담보하기 어렵기 때문이다. 따라서 각 중앙행정기관이 소관별로 정보통신기반시설의 관리기관을 감독하고, 소관분야별로 미래창조과학부, 국가정보원 그리고 국방부가 일정한 역할을 담당하는 '분화된 보호체계'에 대한

37) 이경호 교수(고려대학교 정보보호대학원)는 "주요 정보통신 기반시설의 지정은 별도의 전문위원회를 두어 전국적으로 같은 기준과 잣대로 국가 및 사회 전반에 미치는 위험의 정도에 따라 피해규모를 분석하여 일괄 지정하고 이에 대한 보호대책을 구축, 유지, 관리 및 감독하기 위한 예산 및 자원의 할당을 각 기관이 반드시 확보 하도록 하여 사이버안전체계의 효과성을 증대시키고, 중복되거나 과잉 체계의 구축을 회피하여 본래의 취지에 맞는 주요 정보통신 기반시설에 대하여 보호체계를 운영함이 바람직"하다는 견해를 피력한 바 있다. 이에 대하여는 이경호, "정보통신기반보호법 개정안 마련시의 고려사항", 「정보통신기반보호법령 개선방안 연구 워크숍(Ⅰ) 자료집」, 한국법제연구원, 2014. 6, 25쪽 참조.

문제가 제기되면서 주요정보통신기반시설의 지정권한을 정보통신기반보호위원회에 집중하는 것이 바람직하다는 것이다.

그러나 현행 정보통신기반보호법이 각 중앙행정기관이 법 제8조에 규정된 요건과 기준에 따라서 주요정보통신기반시설(의 관리기관)을 지정하고 이에 대한 보호대책을 구축, 유지, 관리 및 감독하도록 함으로써 각 관리기관들의 자율성과 책임성을 보장하고자 하는 입법취지를 고려해 보면 정보통신기반보호위원회에서 획일적으로 지정권한을 행사하는 것은 부적절하다. 또한, 위원회 산하에 전문위원회들 두고 지정에 관한 지정권한을 위임하는 것도 현행 보호체계의 근간을 무너뜨리기 때문에 이 또한 문제가 있다고 할 수 있겠다. 이와 같이 지정(취소)권한을 집중적으로 개편할 경우에는 불필요한 갈등과 논란을 야기할 위험성이 있으며 정보통신기반보호위원회의 법적 지위 및 실무상 운영방식 등을 고려하여 보면 심의기관 이상의 지위를 인정하는 것은 부적절하다.[38]

분화된 보호체계를 전제로 하고 '자율성과 책임성'이라는 정보통신기반보호법의 입법취지를 유지하는 개선방안으로서 지정권고(미래창조과학부, 국가정보원), 지정(중앙행정기관), 지정단위 선정 및 지정여부 평가(관리기관), 지정여부 심의(위원회) 등으로 구성되어 있는 현행 규율체계를 그대로 유지하면서 별도의 '지정평가위원회'를 구성하는 것을 생각해볼 수 있을 것이다.

'지정평가위원회'는 정보통신보안업무와 관련된 전문가들로 인력풀을 구성하여 정보통신기반보호위원회가 주요정보통신기반시설로 지정할지 여부를 심의하기 이전에 임의로 선발한다. 이는 미래창조과학부와 국가정보원이 지정권고한 주요정보통신기반시설과 각 중앙행정기관에서 지정하고자 하는 주요정보통신기반시설에 대하여 위원회 심의

38) 이는 2013년 7월 발표된 국가사이버안보종합대책의 내용과도 체계적 정합성이 떨어진다.

를 받기 전에 지정의 필요성과 타당성 등을 평가하여 중앙행정기관과 관리기관의 의도적 지정회피 또는 불필요한 과잉지정을 막을 수 있을 것으로 예상된다. 지정평가위원회는 무엇보다도 공정성과 객관성이 담보되어야 하므로 평가위원회 인력풀 구성 및 인력풀에서의 해당 위원 선발은 보안을 전제로 하는 등 공정성과 객관성을 담보할 수 있는 여러 장치가 선행되어야 할 것이다. 이를 통하여 '자율성과 책임성'을 제고할 수 있도록 소관사무별로 정보통신기반보호체계를 관리하는 현행 체계를 유지하면서 그 '효율성'을 위하여 실무상 총괄 및 조정기능을 보완·강화할 수 있을 것으로 기대된다.

둘째, 현행 정보통신기반보호법 제8조 제4항에 따르면 "지방자치단체의 장이 관리·감독하는 기관의 정보통신기반시설에 대하여는 안전행정부장관이 지방자치단체의 장과 협의하여 주요정보통신기반시설로 지정하거나 그 지정을 취소할 수 있다"고 규정하고 있다. 즉, 지방자치단체가 관리·감독하는 기관의 정보통신기반시설의 지정권한은 안전행정부 장관이 보유하도록 규정하고 있는 것이다. 이는 각 지방자치단체장이 정보통신기반시설의 관리·감독하는 정보통신기반시설의 관리기관에 대한 지정권한을 행사하도록 하면 각급 지방자치단체에서 종합적 관점에서 조정을 하는 것이 불가능하다는 점을 고려한 것이다. 정보통신기반보호위원회 구성원 및 각 자치단체별로 산재하는 정보통신기반시설의 관리기관들을 종합하여야 할 필요성 등을 고려하여 안전행정부 장관이 지방자치단체의 장을 대리하여 지정권한을 행사하는 것으로 이해한다면 해당 규정이 법 제정당시부터 같은 취지로 규정되어 있었던 이유를 부인하기 어려울 것이다.[39] 다만, 지방자치단체

39) 이는 법 제정당시부터 지방자치단체의 장이 관리·감독하는 기관의 정보통신기반시설에 대하여는 행정자치부 장관(김대중, 노무현 전 대통령 재임당시), 행정안전부 장관(이명박 전 대통령 재임당시) 그리고 안전행정부장관(현재 박근혜 대통령 재임)이 - 명칭만 바뀌었을 뿐 - 지방자치단체의 장과 협의하여 주요정보통신기반시설로 지정하거나 그 지정을 취소할 수 있도록 규정되어 있다.

장이 관리·감독하는 기관의 정보통신기반시설을 지정하고자 할 경우에는 지방자치단체장의 의견을 가급적 존중하는 방향으로 협의절차를 운용하는 것이 바람직할 것으로 생각된다.

3. 지정기준 및 지정절차

(1) 지정기준

현행 「정보통신기반보호법」 및 동법 시행령에 의거한 '주요정보통신기반시설'의 지정기준은 법 제8조 1항과 시행령 제14조에 따라, 전술한 5가지 기준에 의해 평가되는데 지정평가의 기준표는 '각 중앙행정기관의 장'이 마련하여 지정대상시설관리기관의 장에게 통보하도록 하고 있다.[40] 이는 지정대상시설관리기관의 장과 해당 업무를 수행하는 담당자들이 1차적으로 직접 해당 시설의 중요성을 평가할 수 있도록 한 것이다. 즉, 중앙행정기관은 해당 분야의 특수성을 반영하여 항목별 질문 문항의 내용을 추가 또는 제외하거나, 질문항목별 가중치도 달리 부여할 수 있다. 그리고 지정의 필요성을 결정하는 기준(일정점수 이상, 총점대비 몇 % 이상, 최고점수 몇 개 이상과 같은 기준)도 각 중앙행정기관의 장이 결정할 수 있다.

(가) 정보통신기반시설에 의하여 수행하는 업무의 국가사회적 중요성

당해 사회기반시설이 갖는 기능이 국가안보와 얼마나 직결되며 국민의 생명 위험에 얼마나 직접적인 영향을 갖는가, 그리고 사회기반시설이 공적으로 의무적으로 제공되는 것인가, 다른 사회기반시설로 대체가 가능한가 등에 관한 사항이다.

40) 이들 항목의 반영비율은 중앙행정기관의 장이 소관분야의 특수한 사정을 고려하여 규정하고 관리한다.

(나) 수행하는 업무의 정보통신기반시설에 대한 의존도

정보통신시설의 장애가 사회기반시설의 장애로 연결되는 비중, 사회기반시설의 서비스 중 정보통신기반시설의 기여도 등에 관한 사항이다.

(다) 다른 정보통신기반시설과의 상호연계성

연계되는 호스트의 수와 외부와의 송수신 트래픽량 등에 관한 사항을 포함한다.

(라) 정보통신기반시설의 침해시 국가안보와 경제사회에 미치는 피해 규모 및 범위

정보통신기반시설의 국가안보와의 직결성 및 시설의 이용자의 규모와 빈도, 서비스의 지역적 범위 및 경제사회의 정보통신기반시설 의존도에 관한 것이다.

(마) 정보통신기반시설의 침해 또는 그 복구의 용이성

복구에 소요되는 시간, 투입인력, 기술수준, 경제적 비용 등과 대체 정보통신기반시설 이용가능성 등이다.

(2) 지정절차

제1단계에서 중앙행정기관의 장은 주요정보통신기반시설의 지정여부에 관한 평가기준(지정평가기준)과 지정방침을 마련하여 소관분야 지정대상시설 관리기관의 장에게 시달하게 된다.

제2단계에서는 지정대상시설의 관리기관의 장은 지정단위를 선정하고 관련된 세부시설의 범위를 선정한다. 또한 시설관리기관의 장은 중앙행정기관이 통보한 평가기준을 근거로 주요정보통신기반시설 지정여부를 평가하게 되며, 그 결과를 중앙행정기관의 장에게 통지한다.

제3단계에서는 중앙행정기관의 장은 지정대상시설 관리기관의 장이 통지해 온 평가결과에 대해 그 적정성 여부를 분석하고 검토한 후 소

관분야의 정보통신기반시설 중 전자적 침해행위로부터 보호할 필요성이 있다고 인정되는 시설을 정보통신기반보호위원회에 주요정보통신기반시설 지정 심의(안)으로 상정하게 된다.

제4단계에서는 정보통신기반보호위원회는 중앙행정기관의 장이 제출한 시설지정(안)을 심의·의결하게 되고, 제5단계에서 중앙행정기관의 장은 위원회의 심의 결과에 따라 소관분야 주요정보통신기반시설을 지정한 경우에 해당 관리기관의 장에게 그 사실을 통보하고 이를 즉시 관보에 고시하게 된다.[41]

4. 지정대상

주요정보통신기반시설은 국가·공공기관 뿐 아니라 민간부문이 관리하는 정보통신기반시설 중에서 지정한다. 즉, 전자적 침해행위가 발생하면 국가안전보장과 국민의 기본생활 등에 중대한 영향을 미치게 되는 등 5가지 기준을 고려하여 정보통신기반시설(전자적 제어·운영시스템과 정보통신망) 중에서 위원회 심의를 거쳐서 지정하게 된다.[42]

이와 관련하여 법 제정 당시 주요정보통신기반시설에 등급을 부여하여 차등적인 보호의무와 관리절차, 침해시 처벌강도를 등급별로 구분하여 규정할지 등에 대한 검토가 이뤄졌다. 그러나 주요정보통신기반시설에 대한 보호의무를 차등적으로 적용하고자 하는 시도는 정보

41) 다만, 국가안전보장을 위하여 필요한 경우에는 위원회의 심의를 받아 이를 고지하지 아니할 수 있다.

42) 법 제7조 제2항은 "국가안전보장에 중대한 영향을 끼치는 정보통신기반시설"로서 다음과 같은 시설을 예시하고 있다. 이에 따르면 ① 도로, 지하철, 공항 시설. ② 전력, 가스, 석유 등 에너지·수자원 시설. ③ 방송중계, 국가지도통신망 시설, ④ 원자력, 국방과학, 첨단방위산업관련 정부출연연구기관의 연구시설 등이다. 이와 유사한 취지로 2013년 2월 6일 조명철 의원이 발의한 "정보통신기반보호법 일부개정법률안" 제8조 제1항은 "이 경우 도로·철도·항만·공항 등의 교통시설, 방송·통신시설, 수도·전기·가수 등의 공급설비, 금융·투자·기금 관련기관, 병원·보건·의료시설 등과 관련된 정보통신기반시설의 경우에는 가급적 주요정보통신기반시설로 지정하도록 노력하여야 한다"고 하여 지정확대를 위한 규정을 두고자 하였다.

통신(IT)기술의 급격한 발전속도를 감안한다면 불가능하고, 등급분류 기준을 설정하고 그 기준에 따라 객관적으로 등급을 부여하는 것이 기술적으로 매우 어려우므로 등급별로 구분하지 않기로 결정하였다.

그러나 최근에는 주요정보통신기반시설을 향후 확대하고 정보보안 산업을 육성하고자 하는 정책적 변화가 예상되고 있으므로 선택과 집중을 위하여 등급별로 차등화된 보호체계를 운영하는 것이 강력하게 요청되고 있는 상황이다. 이를 위하여는 법체계 전반을 재구성하여야 할 것이다. 예컨대 주요정보통신기반시설과 핵심정보통신기반시설이라는 개념을 구별하여 제2조(정의)에 규정하는 방안 혹은 제8조에서 지정기준과 등급을 별도로 규정하여 주요정보통신기반시설(제2급 정보통신기반시설)과 핵심정보통신기반시설(제1급 정보통신기반시설)을 구분하여 지정하는 방안 등을 생각해 볼 수 있다. 그리고 그 이후의 사전예방 및 사후대응체계에서 각종 의무와 보호지원의 범위 등을 달리 규율하여야 할 것이다.

Ⅱ. 주요정보통신기반시설의 지정권고(법 제8조의2)

1. 신설배경

종래 주요정보통신기반시설의 지정은 법 제8조에 의하여 중앙행정기관의 장이 소관분야의 정보통신기반시설 중 개괄적인 지정기준을 정하여 자체적으로 주요정보통신기반시설을 지정하고 있었다. 즉, 애초부터 주요정보통신기반시설로 지정될 경우에 다양한 의무가 부과되는 등 업무부담으로 인하여 각급 관리기관들은 주요정보통신기반시설로 지정되는 것에 소극적이었다.[43] 따라서 각 중앙행정기관의 장이

43) 2001년 7월 법 시행 이후 주요정보통신기반시설로 지정된 시설은 1차 2001년 4개 부처 23개 시설, 2차 2002년 5개 부처 66개 시설에 불과하였고, 3차 2004년 (구)정보통신부 소관 7개 시설, 4차 2005년 중앙선거관리위원회 소관 1개 시설, 5차 2006년 (구)정보통신부 소관 5개 시설이 추가되었을 뿐이다.

주요정보통신기반시설의 지정권한(제8조)을 적정하게 행사하지 않을 경우에 대한 대응책이 필요하게 되었고, 그 지정을 독려할 수 있는 제도적 장치를 마련할 필요성이 제기되었다.

결국 당시 정보통신부 장관(현재 미래창조과학부 장관)과 국가정보원장 등이 각 관할영역별로 주요정보통신기반시설을 발굴하여 중앙행정기관의 장에게 주요정보통신기반시설로 지정하도록 권고할 수 있도록 하여 그 지정을 활성화할 수 있는 근거를 마련하기 위하여 2007년 12월 제3차 개정을 통하여 법 제8조의2가 도입되었다. 즉, 국가정보원장 등은 주요정보통신기반시설지정 조사반을 두고, 주요정보통신기반시설로 지정할 필요성을 검토하여 중앙행정기관의 장에게 주요정보통신기반시설로 지정하도록 권고할 수 있는 법적 근거가 마련되었던 것이다. 2012년에는 동법 시행령 제16조의2를 마련하여 미래창조과학부와 국정원의 지정권고의 협의 및 지정절차 등을 규정하였다.

2. 의의 및 기능

「정보통신기반보호법」은 중앙행정기관이 미래창조과학부 또는 국가정보원으로부터 주요정보통신기반시설의 지정을 권고받은 경우 중앙행정기관의 장은 - 지정절차와 마찬가지로 - 시행령 제13조에 의한 지정단위 선정, 제14조에 따른 자체평가 및 제15조에 따른 심사절차를 거쳐서 지정여부를 결정하고, 그 심사결과를 지정권고한 미래창조과학부장관 또는 국가정보원장에게 통보한다. 지정권고의 대상은 정보통신기반보호법 제8조에 명시된 5가지 지정기준을 바탕으로 하여 세부분야별 기준과 평가요소에 대한 세부지표에 의하여 조사반이 선정한다. 지정권고의 절차는 시행령 제16조의2에 규율되어 있다.[44]

44) 구체적으로 주요정보통신기반시설 지정대상을 선정하기 위해 공공・민간분야별로 '주요정보통신기반시설지정조사반'을 두고, 각 조사반은 주요정보통신기반시설 지정 필요성을 검토한다(시행령 제16조의2 제1항). 한편, 조사반은 검토결과 주요정보통신기반시설로 지정할 필요성이 있다고 판단하는 경우에는 미래창조과학부장관

법 제8조의2에서 미래창조과학부장관 또는 국가정보원장이 각 중앙행정기관의 장에게 주요정보통신기반시설로의 지정을 '권고'하는 것은 주요정보통신기반시설의 보호와 관련한 전문성을 갖고 범정부차원에서 조정·총괄 역할을 하는 기관들(미래창조과학부와 국정원)이 개입하여 주요정보통신기반 보호체계에 흠결이 생기지 않도록 유도·조종하기 위한 것으로 평가할 수 있다.[45]

3. 문제점 및 개선방안

첫째, 지정권고의 주체에 대한 문제가 있다. 법 제8조의2는 "미래창조과학부장관과 국가정보원장 등"이 지정권고를 할 수 있도록 규정되어 있는데, 시행령 제16조의2는 "미래창조과학부장관과 국가정보원장"으로 규정하고 있다. 즉, 시행령 제16조의2에서 "법[46] 제9조의2 제2항 각 호의 구분에 따른 관할별로" 조사반으로 하여금 지정의 필요성을 검토하게 하고, 그 검토결과를 바탕으로 각 중앙행정기관의 장과 협의하여 지정을 권고하도록 하고 있는데, 국방부장관은 국방 분야 정보통신기반시설을 관할하고, 이에 대한 중앙행정기관의 장 역시 자신이므로 지정권고를 할 필요 없이 지정의 필요성이 있다고 판단하는 경우 스스로 법 제8조에 의거하여 지정하면 된다는 점을 고려한 것으

등에게 그 결과를 보고한다. 미래창조과학부장관 또는 국가정보원장이 정보통신기반시설 관할 중앙행정기관의 장에게 주요정보통신기반시설로 지정하도록 권고하면, 권고를 받은 중앙행정기관의 장은 60일 이내에 지정 여부를 결정하여 미래창조과학부장관 또는 국가정보원장에게 통보하도록 하고 있다.

45) 앞에서 살펴본 바와 같이 법 제8조에서 지정권한을 각 중앙행정기관의 장에게 소관별로 부여한 것은 보호체계를 집중형이 아니라 분산형으로 설계한 것이다. 이는 각 부처별로 자율성과 책임성을 제고하기 위한 것으로 볼 수 있다. 그러나 이로 인한 효율성 저하를 방지하기 위하여 조정·총괄기능이 필요하고, 미래창조과학부와 국정원이 정보통신기반보호시설을 지정권고하는 것은 현대행정의 유도적·조종적 특성을 반영한 것으로 보인다.

46) 시행령 제16조의2 제1항에서 "법 제8조의2"는 맞게 표현되어 있으나 "제9조의2" 앞에는 '법'이라는 표기를 하지 않고 있다. 이는 명백한 흠결이므로 "법 제9조의2"로 명기하는 것이 바람직할 것이다.

로 보인다. 따라서 법 제8조의2에서 “등”을 삭제하는 것이 바람직할 것이다.[47]

둘째, 권고기관과 각 중앙행정기관과의 관계에서 다음과 같은 문제가 나타날 수 있다. 즉, 조사자료요청(법 제8조의2 제2항)에 응하지 않을 경우, 지정권고 이전의 협의절차에서 논의할 사항(시행령 제16조의2 제2항) 그리고 지정여부를 결정하여 통보할 때(시행령 제16조의2 제3항) 중앙행정기관의 장이 지정권고에 응하지 아니하는 경우에 이견을 조정하는 방식 등에 대한 규정이 마련되어 있지 않다. 이에 대하여는 의도적으로 규율의 공백을 두고 협의에 의하여 해결해나가는 것이 업무수행상 보다 편리할 수도 있으나, 필요하다면 이에 대한 절차규정 등을 마련하는 것이 필요할 수도 있을 것이다.

Ⅲ. 지정취소

제8조에 따라서 지정된 주요정보통신기반시설의 국가·사회적 중요성 등이 상실되어 지정을 취소하여야 하는 경우도 있을 수 있는데, 이에 대한 규율은 법 제8조 제3~5항에 규정되어 있다. 우선, 지정취소의 요건과 관련하여 동조 제3항에 따르면 “관리기관이 해당 업무를 폐지·정지 또는 변경하는 경우”만을 규정하고 있는데 미흡한 것으로 보인다. 따라서 “제8조 제1항 각 호의 사항(지정기준)을 고려하여 지정을 취소할 수 있다”는 규율도 삽입하는 것이 필요할 수 있다.

둘째, 지정취소는 중앙행정기관의 장이 직권으로 하거나, 해당 관리기관의 신청에 의하여 한다. 이와 관련하여 제8조의2는 “지정”을 권고하는 내용만 규정되어 있는데, 향후 주요정보통신기반시설의 지정대상을 확대할 경우에는 지정권고기관에서 관할별로 주요 정보통신기반

47) 법 제8조의2는 2007년 12월 제3차 개정시 신설되면서 (민간, 공공, 국방부문별) 기존의 3원화된 보호체계를 유지하였고, 시행령 제16조의2는 제도를 운영하는 과정에서 절차규정 등의 필요에 의하여 2012년에 신설되었다는 점을 고려한다면, 시행령이 법률보다 합리적으로 규정되어 있다는 점을 이해할 수 있다.

시설로 지정운영할 필요성이 있는지 여부 등을 심사하여 “지정취소”를 권고할 수 있는 길을 마련할 필요성이 제기될 수도 있다. 매년 증가하기만 하는 모든 주요정보통신기반시설에 대하여 보호대책 이행여부의 확인, 보호지원 등을 수행하는 것은 효율적이지도 않고 업무부담을 지나치게 가중시킬 것이기 때문이다.

셋째, 지정취소의 절차적 문제가 있을 수 있다. 중앙행정기관의 장이 지정취소를 하고자 하는 경우에 정보통신기반위원회의 심의를 받아야 하고, 그 대상이 되는 관리기관의 장을 위원회에 출석하게 하여 그 의견을 청취할 수 있도록 하고 있다. 그런데 의견청취를 재량사항으로 정한 것이 적절한지 의문이다. 「행정절차법」 제22조에 따르면 의견청취(청문)를 하도록 규정하고 있는데, 동법 제22조 제3항에서 “당사자에게 의무를 부과하거나 권익을 제한하는 처분을 할 때에는 당사자에게 의견제출의 기회를 주어야 한다”고 규정한 취지를 고려한다면 지정 및 지정취소가 당사자에게 갖는 파급효과를 고려할 때 의견청취는 반드시 하는 것이 합리적일 것이다. 만약 신규지정 혹은 지정취소의 심의대상이 많다면 서면으로라도 의견진술의 기회를 부여할 수 있도록 운영의 묘를 살릴 필요가 있을 것이다.

제 2 절 자율성을 기반으로 하는 사전예방체계

Ⅰ. 취약점의 분석・평가(법 제9조)

1. 의의 및 기능

취약점의 분석 및 평가는 정보통신기반시설에 구축된 정보통신망과 정보시스템 및 그 콘텐츠의 기밀성, 무결성, 가용성 등을 변형하거나 왜곡시킬 수 있는 사이버 테러 등 위협요인에 대하여 정보통신시스템의 취약점을 분석・평가함으로써, 그 위험을 최소화할 수 있는 보호

대책을 작성하는 데 필요한 정보를 제공함으로써 분야별 보호계획 및 종합대책을 수립하는 근거를 제공하기 위한 것이다. 즉, 정보통신기반시설에 대한 체계적인 보호대책 및 보호계획을 수립·시행하기 위하여는 정밀한 취약점 분석 및 평가에 기초하여야 한다. 따라서 취약점의 분석·평가(법 제9조)는 보호대책(제5조, 제5조의2)과 보호계획(제6조)보다 조문체계상 뒤에 위치하고 있으나, 논리적으로 그에 선행하여 논의하는 것이 타당하다.

취약점의 분석 및 평가는 "주요정보통신기반시설 관리기관의 장"이 수행하는 것을 원칙으로 하고, 필요한 경우에는 외부 전문기관에 취약점 분석·평가를 의뢰할 수 있도록 규정하고 있다. 이는 관리기관이 자체적으로 취약점 분석·평가의 전문인력과 관련 기술을 확보하기가 쉽지 않고, 이를 외부 전문기관에 위탁할 경우 평가의 전문성과 객관성을 확보할 수 있기 때문이다. 따라서 향후 취약점 분석·평가 업무를 외부 전문기관에게 위탁하는 것을 의무화하거나 적용대상 및 비중을 확대할 경우에는 정보보호산업을 진흥·육성하기 위한 중요한 법적 근거가 될 수 있을 것이다.

이에 해당하는 외부의 전문기관은 법 제9조 제3항에 규정되어 있다.[48] 이는 법 제7조(주요정보통신기반시설의 보호지원)의 위임규정인 시행령 제12조와 거의 동일하다. 입법이유서를 분석해 보면, "제2호에 규정된 정보공유·분석센터가 설립되어 있는 분야인 경우에는 해당

48) 정보통신기반보호법 제9조(취약점의 분석·평가) ③ 관리기관의 장은 제1항의 규정에 의하여 취약점을 분석·평가하고자 하는 경우에는 다음 각호의 1에 해당하는 기관으로 하여금 소관 주요정보통신기반시설의 취약점을 분석·평가하게 할 수 있다. 다만, 이 경우 제2항의 규정에 의한 전담반을 구성하지 아니할 수 있다.
1. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조의 규정에 의한 한국인터넷진흥원
2. 제16조의 규정에 의한 정보공유·분석센터(대통령령이 정하는 기준을 충족하는 정보공유·분석센터에 한한다)
3. 정보통신산업 진흥법」 제33조에 따라 지정된 지식정보보안 컨설팅전문업체
4. 「정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조의 규정에 의한 한국전자통신연구원

정보통신기반시설의 특성을 보다 잘 파악하고 있는 각 분야별 정보공유·분석센터가 그 취약점을 분석·평가하는 것이 보다 합리적이므로 정보공유·분석센터가 취약점 분석·평가업무를 수행할 수 있도록 한 것이고, 「정보통신산업진흥법」에 의거하여 지정된 '지식정보보안 컨설팅전문업체'도 취약점 분석·평가업무를 수행할 수 있게 함으로써, 정보보호산업의 육성을 도모하고자 한 것"이다.

그렇다면 정보통신기반시설의 보호지원(법 제7조)과 취약점 분석·평가(법 제9조)의 내용이 중복되는 것은 아닌지 혹은 유의미한 차이를 발견할 수 있는지에 대한 논증이 필요할 것이다. 만약 취약점 분석·평가를 하여 보안수준에서 미비한 부분이 발견되어 기술적 지원으로 이어지게 된다면, 법 제9조 제3항과 시행령 제12조를 통합하여 법령체계의 통일성과 조문의 경제성 등을 제고할 수 있을 것이다.

그리고 이와 관련하여 한국전자통신연구원(법 제9조 제3항 제4호)과 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조에 따라 설립된 한국전자통신연구원의 국가보안기술 연구·개발을 전담하는 부설연구소(시행령 제12조 제4호)의 일부의 표현상 차이가 있는데, 이는 "ETRI 부설 국가보안기술연구소"를 의미하고 다른 기관을 지칭하는 것이 아닌 것으로 보인다.[49] 이를 통일적으로 규율하는 것이 명확성의 원칙상 오해의 소지를 줄일 수 있는 등 수범자의 입장에서 더욱 바람직할 것으로 생각된다.

2. 주기 및 절차

(1) 취약점 분석·평가의 시기 및 주기

취약점 분석·평가의 시기 및 주기는 시행령 제17조에 상세히 규정되어 있다. 즉, 주요정보통신기반시설로 새로이 지정된 경우 관리기관

49) 이와 관련하여 변재일, "사이버보안강화 명목의 정보 권력 용인할 수 없어", 「국회보」 제558호, 국회사무처, 2013. 5, 50~53(53)쪽 참조.

의 장은 지정 후 6개월 이내에 취약점 분석·평가를 실시하여야 한다. 그러나 관리기관의 장이 소관 주요정보통신기반시설 지정 후 6월 이내에 동 시설에 대한 취약점의 분석·평가를 시행하지 못할 특별한 사유가 있는 경우에는 관할 중앙행정기관장의 승인을 받아 지정 후 9개월 내에 실시하여야 한다.

그리고 관리기관의 장은 소관 주요정보통신기반시설이 지정된 후 당해 주요정보통신기반시설에 대한 최초의 취약점 분석·평가를 한 후에는 매년 취약점의 분석·평가를 실시한다. 다만, 소관 주요정보통신기반시설에 중대한 변화가 발생하였거나 관리기관의 장이 취약점 분석·평가가 필요하다고 판단하는 경우에는 1년이 되지 아니한 때에도 취약점의 분석·평가를 실시할 수 있다.

이를 규정한 취지는 취약점 분석·평가업무의 중요성과 기술발전속도 등을 고려하여 매년 주기적으로 실시하도록 한 것으로 보인다. 즉, 이 업무는 해당 관리기관에게 상당한 업무부담과 비용을 발생시킬 것이기 때문에 중요한 사항으로서 법률에 규정된 것이고, 주기 내에 추가적으로 취약점 분석·평가를 실시하기 위한 사유를 제한적으로 규정(중대한 변화의 발생)한 것으로 평가할 수 있다.

(2) 취약점 분석·평가의 절차

취약점 분석·평가절차는 다음과 같은 5단계로 진행된다.

(가) 1단계: 전담반의 구성 및 취약점 분석·평가계획 수립

법 제9조 제2항에 따르면 “관리기관의 장은 대통령령이 정하는 바에 따라 취약점을 분석·평가하는 전담반”을 구성하여야 하고, 시행령 제18조 제1항에서는 “법 제9조 제2항의 규정에 의하여 관리기관의 장은 취약점을 분석·평가하기 위한 전담반을 구성”하는 내용을 규정하고 있다. 이는 관리기관의 장이 수행하는 취약점 분석·평가의 중요성에 비추어 “전담반”에 대한 법률적 위임근거와 시행령을 통하여 이

를 구체화하도록 한 것으로 보인다. 이에 따라 시행령 [별표 1]은 취약점 분석·평가 전담반의 구성기준을 정하고 있다.

[별표 1]

취약점 분석·평가 전담반 구성기준(제18조 제1항 관련)

구성원	역할 또는 경력·자격기준
반장(정보보호책임자)	취약점 분석·평가 시행의 총괄
관리기술 담당	관리적·물리적 정보보호 등 조직의 정보보호관리체계의 관리·운영경력 소유자, 정보시스템 감리 경력자
메인프레임 담당	중형급이상의 컴퓨터 관리 경력자
응용프로그램 담당	해당기관의 주요정보통신기반시설에 대한 핵심 프로그램 개발·유지보수 경력자
서버 담당	유닉스, 리눅스, Windosw-NT등 각종 서버관련 기술 보유자
정보보호 담당	정보보호시스템 평가 및 운영자, 정보보호정책·위험분석 또는 취약점 점검·평가 등의 보안관리기술 경력자
네트워크 담당	WAN, LAN, NMS 및 무선통신등에 관한 기술 및 각종 통신 프로토콜 기술 보유자

* 비고 : 관리기관은 소관 주요정보통신기반시설의 특성에 따라 전담반 구성요건을 고려하여 취약점 분석·평가를 수행할 수 있는 적정 인원의 전문인력을 확보하여야 한다.

전담반은 각 관리기관의 정보보호책임자(법 제5조 제4항)를 반장으로 하고, 분석·평가의 객관성과 실효성을 확보하기 위해 주요정보통신기반시설의 관리·운영자와 정보보호에 전문가들로 구성한다. 즉, 정보통신기반보호법 시행령 [별표 1]의 "취약점 분석·평가 전담반 구성기준"을 마련한 취지는 취약점 분석·평가의 전문성과 공정성을 확보하기 위한 것이다.

이와 같이 전문자격을 갖춘 인력으로 구성되도록 법으로 정하여진 전담반이 구성된 이후 취약점 분석·평가기준(법 제9조 제4항)에 따라서 소관 주요정보통신기반시설의 취약점 분석·평가의 수행방법, 점검항목, 절차, 기간, 소요예산 등을 포함한 취약점 분석·평가계획을 수립하고, 이를 관리기관의 장에게 보고한 후 시행하게 된다.

(나) 2단계: 취약점 분석·평가 대상 선별

제2단계에서는 취약점 분석·평가 대상 주요정보통신기반시설의 구성 및 업무내용을 확인하여 평가범위를 확정하게 된다. 이 때 취약점 분석·평가와 이에 따른 보호대책 수립이 필요한 주요정보통신기반시설의 세부자산을 선별하여 그 목록 및 구성도를 작성하고, 각 자산별로 중요도를 부여한다.

< 세부자산 분류기준(예시) >

· 물리적 자산, 소프트웨어, 정보/데이터, 인적 자산, 무형자산 등
· 세부자산은 담당자 면담, 실사, 문서검토 등을 이용하여 선별함.

(다) 3단계 : 위협요인 및 취약점 분석

주요정보통신기반시설에서 실제로 문제가 발생하였거나 또는 발생될 수 있는 위협요인을 식별하고, 각 위협요인별 발생원인·발생빈도와 침해시 파급효과 등을 분석한다. 이를 위하여 소관 정보통신기반시설에 발생할 수 있는 위협요인과 취약점을 식별하고, 그 특수성을 고려하여 점검이 필요한 취약점 점검항목을 마련한다. 그리고 식별된 취약점별로 그 존재여부 및 취약성 정도를 확인·분석한다.

전담반은 관리기관에서 보유하거나 정보보호지원기관 등이 개발한 '취약점 탐지도구'를 이용하여선정한 점검항목에 대한 취약점을 탐지한다. 탐지도구를 이용한 방법 이외에도 관리기관의 인적, 물리적, 관리적 보호체계의 취약점에 대한 구조적 분석도 수행한다.

(라) 4단계 : 기존의 보호대책 분석 및 취약점 평가

위협요인, 취약점에 대한 기존 보호대책의 적합성, 효율성 등에 대한 문제점을 파악하고 분석한다. 그리고 위협요인과 취약점의 상관관계, 침해사고 발생가능성, 침해사고 발생시 조직에 미치는 영향, 새로이 필요하거나 보완되어야 할 보호대책(정보보호시스템의 구축방안), 그 효과성과 경제성 그리고 기존 보호대책과의 연계성 등을 평가하게 된다.

(마) 5단계 : 보호대책의 수립(제5조)

취약점의 분석·평가결과와 자체적으로 점검한 보호대책을 비교·검토하여 그 중에서 가장 효과적인 보호대책을 수립하고, 그 대책을 구체적으로 집행할 수 있는 방안을 마련한다.

3. 범위 및 항목

중앙행정기관의 장이 지정한 주요정보통신기반시설의 구성요소는 각 관리기관의 주요정보통신기반시설 성격에 따라 구체적인 평가범위 및 대상이 다를 수 있다. 여기에서 중요한 점은 각 관리기관이 자체적으로 주요정보통신기반시설의 기술적 사항과 관리·운영사항을 참조하여 취약점 분석·평가항목을 가감하여 실시할 수 있다는 것이다.

구체적인 평가의 범위 및 대상으로는 전자적 제어·운영시스템[50], 정보시스템[51], 통신시스템(네트워크 장비)[52] 등을 들 수 있다. 첫째,

50) 이는 사회기반시설을 직접적으로 제어·운영하는데 관계되는 시스템으로, 마비되면 사회기반시설이 제공하는 서비스가 중단되는 시스템으로서, 전력부문의 발전 및 송·배전시스템, 항공부문의 관제통신시스템, 항만부문의 항만운영정보시스템, 금융부문의 입·출금·이체관련 시스템, 통신망 관리시스템 및 교환시스템 등이 이에 해당한다.

51) 이는 마비되더라도 사회기반시설의 제공이 중단되지는 않으나 업무와 국민생활에 중대한 혼란을 초래하는 시스템으로서 경영정보시스템, 철도·항공·통신 등의 예약·과금관련 시스템, 주민등록 또는 국세관련 시스템 등이 이에 해당한다.

52) 이는 전자적 제어·운영·정보시스템간 통신신호를 교환하는 데 필요한 설비(교환설비)와 통신신호의 전송에 관련되는 설비(전송설비)를 의미한다. 이에 해당하는

기술적 사항으로는 주요 정보의 기밀성을 보장하기 위한 메카니즘(암호화), 비인가자에 의한 네트워크 접근을 통제하기 위한 침입차단 및 침입탐지시스템 등 정보보호시스템의 설치, 그리고 관리기관 서비스 이용자와의 정보유통시 송·수신자의 신원확인 및 송·수신 정보의 무결성 확보를 위한 공인전자서명인증체계 구축 등에 관한 사항이 포함된다.

둘째, 주요정보통신기반시설의 관리·운영과 관련하여 주요정보통신기반시설 보호를 위한 전문인력·조직 편성, 기반시설 보호에 관한 교육·훈련 등의 적정성, 주요정보통신기반시설에 출입자 통제, 침해사고 발생시 대응체계의 적정성 등에 관한 사항이 포함된다.

4. 정 리

취약점 분석·평가업무는 실무상 전문적이고 기술적인 사항이 많은 관계로 정확히 파악하기 어려운 측면이 있다. 그러나 법체계 측면에서 살펴보면 취약점 분석·평가(법 제9조)에 기초하여 보호대책의 수립(법 제5조), 보호대책 이행여부 확인(법 제5조의2), 보호계획의 수립(제6조)과 보호지침의 제정(제10조) 그리고 보호조치 명령·권고(제11조) 그리고 보호지원(법 제7조) 및 관리기관에 대한 지원(법 제25조)으로 이어지는 프로세스를 고려할 때 이는 보호체계의 출발점으로서 중요한 의미를 갖는다. 즉, 이는 법 제8조에 따라서 정보통신기반시설로 지정될 경우 관리기관의 장에게 첫 단계로 부과되는 의무로서 다음과 같은 이중적 의미를 갖게 된다.

것으로서 교환기, 라우터 등 전송단국장치, 중계장치, 다중화장치, 분배장치 등을 들 수 있을 것이다. 그러나 통신시스템 중 선로설비(통신신호를 전송하는데 사용하는 매체로서 전주, 관로, 통신구, 배관, 맨홀, 배선반 등)는 소방법 등 타 관련 법령에 규정이 있는 경우 이에 따르고, 정보통신기반보호법에 따른 취약점 분석·평가 대상에서 제외하는 것이 선택과 집중을 위하여 합리적일 것이다.

첫째, 취약점 분석·평가는 국가 주도로 이뤄지는 것이 아니라, 관리기관의 장이 자체적으로 전담반을 구성하여 하는 것을 원칙으로 하고 예외적으로 외부 전문기관에게 위탁할 수 있도록 하고 있다는 점이다. 이에 따르면 관리기관의 장은 취약점 분석·평가단계에서 법령이 정하고 있는 기준을 준수하는 테두리 내에서 상당한 자율성을 누리게 된다.[53] 이는 각 관리기관이 자체적으로 주요정보통신기반시설의 기술적 사항과 관리·운영사항을 참조하여 취약점 분석·평가항목을 가감하여 실시할 수 있다는 점에서도 잘 드러난다.

둘째, 관리기관의 장으로 하여금 자체적으로 취약점 분석·평가를 실시하도록 의무화하고 있기 때문에 이는 해당 사업자에게 큰 부담으로 작용할 수 있다. 정보통신기반시설 지정 후 6개월(승인을 얻은 경우에는 9개월) 이내에 실시하여야 하고 그 후 매년 정기적으로 실시하도록 되어 있는데, 자체적으로 전담반을 구성하는 경우에는 인건비와 사업비가 들 것이고 외부 전문기관에 위탁할 경우에는 수수료를 부담하여야 할 것이기 때문이다.[54]

---

53) 법 제9조 제4항에서 취약점 분석·평가에 관한 기준을 미래창조과학부장관, 관계중앙행정기관의 장 및 국가정보원장이 협의하여 정하도록 하고 있는데, 이를 위반할 시의 제재방안(예컨대 제30조) 등이 마련되어 있지 않다는 점에서 법적 구속력이 없고 사실상의 구속력만을 갖는다고 해석할 수밖에 없을 것이다.

54) 이와 관련하여 정보통신기반시설로 지정된 이후 6개월(특별한 사유가 있으면 9개월) 이내에 취약점 분석·평가를 하고 매년 정기적으로 시행하는 것이 적절한 주기인지에 대한 판단이 필요할 것이다. 예를 들어 향후 정보통신기반시설로 지정되는 대상이 확대되면 그에 따라서 외부 전문기관도 확대되어야 하는데, 적정한 수의 "지식정보보안컨설팅 전문업체"가 지정되지 않는다면 취약점 분석·평가업무의 질이 하락할 위험성이 있다. 한국인터넷진흥원과 한국전자통신연구원은 단독기관이기 때문에 논외로 한다. 이와 반대로 정보보안기술의 발전속도가 매우 빠르게 진행되거나 사이버 테러가 빈발하면 주기를 더욱 단축시켜야 할 필요성이 있을 것이다. 이와 같이 취약점 분석·평가의 주기도 관리기관의 부담, 취약점 분석·평가기관의 숫자, 역량 및 전문성과 같은 내부적 요인과 아울러 IT 기술의 발전속도 및 사이버 안보환경 등과 같은 외부적 요인들을 종합적으로 고려하여 결정하여야 하는 문제이다.

대부분의 정보통신기반시설은 그 사업규모가 매우 크기 때문에 해당 정보통신망의 유지·관리비용이 적지 않게 드는 상황이고, 정보보안시스템을 구축하거나 교체하는 비용도 한계성장에 직면한 오늘날 민간사업자들에게 적지 않은 부담이 되고 있다. 그러므로 이와 관련하여 관리기관에 대한 지원(법 제25조) 대책을 실질화하는 것이 필요할 것이다.[55]

Ⅱ. 주요정보통신기반시설보호대책의 수립 등(제5조)

앞에서 살펴본 바와 같이 주요정보통신기반시설을 관리하는 기관의 장은 취약점 분석·평가결과에 따라서 소관 주요정보통신기반시설을 보호하기 위한 물리적·기술적 대책을 포함한 관리대책을 수립·시행할 의무와 정보보호책임자를 지정할 의무를 부담하게 된다. 법률 제5조에 규정된 의무는 정보통신기반시설 관리기관의 장에게 부여되는 의무인 동시에 관리기관의 자율성과 책임성을 제고하기 위하여 유보된 사항이라고 평가할 수 있다.[56]

1. 보호대책의 수립·시행 및 제출

주요정보통신기반시설 관리기관의 장은 제9조 제1항에 따른 취약점 분석·평가의 결과에 따라 보호대책(주요정보통신기반시설을 안전하게 보호하기 위한 물리적·기술적 대책을 포함한 관리대책)을 수립하여 관할 중앙행정기관의 장에게 매년 8월 31일까지 제출하여야 하고

55) 이에 대하여는『제4장 제3절 Ⅲ. 관리기관에 대한 지원』참조.

56) 정보통신기반보호법의 규율체계는 주요정보통신기반시설의 보호책임은 일차적으로 해당 정보통신기반시설의 관리기관에게 부여되고, 정보통신기반시설의 보호가 자율적으로 달성되지 않는 한도 내에서 보충적으로 국가의 개입이 행해지는 것을 전제로 하는 것은 일방적인 국가주도적 방식으로 보호체계를 운영하는 것이 바람직하지 않을 수 있고 민간부문의 자율성을 일차적으로 전제하고 공공부문의 보호지원이라는 민관협력이 중요하다는 점을 고려한 것이다.

(법 제8조 제1항, 시행령 제8조)[57], 지방자치단체의 장이 관리·감독하는 주요정보통신기반시설보호대책은 안전행정부장관에게 제출하도록 되어 있다(법 제8조 제3항).

법 제5조에 규정된 "정보통신기반시설보호대책"은 다음과 같은 의미를 갖는다. 이는 한편으로는 취약점 분석·평가결과(제9조)에 따라서 자체적으로 수립되는 것이고, 다른 한편으로는 주요정보통신기반시설을 관리하는 중앙행정기관의 종합적·조정적 계획수립(제6조)에 대한 기초자료가 된다. 그리고 기술적 대책과 함께 물리적 대책을 포함하도록 명시하고 있기 때문에 보호대책의 수립범위를 고려하면 「정보통신기반보호법」은 "물리적 시설"도 규율하는 것이다.

법 제5조 제1항에 따라서 관리기관의 장이 수립하는 "주요정보통신기반시설보호대책"은 "주요정보통신기반시설을 안전하게 보호하기 위한 물리적·기술적 대책을 포함한 관리대책"으로서 이는 물리적 대책과 기술적 대책을 포함한 관리대책을 의미한다. 그러나 법 제7조(보호지원)에서 국가에 요청할 수 있는 것은 기술적 지원에 한하여 인정되고 있다는 점에서 차이가 있다. 그리고 이와 관련하여 최근에는 데이터 중심의 보호대책에 중점을 두어야 한다는 취지의 개정안이 발의된 바 있다.[58] 이를 정리해 보면 당사자가 자율적으로 보호대책을 마련하여야 하는 영역과 국가가 보호지원을 할 수 있는 범주에는 차이가 있고, 최근에는 정보보호의 비중이 더욱 강조되고 있는 것이다.

---

57) 제출기한의 적정성 문제는 『제3장 제2절 Ⅳ. 3. 보호계획 수립일정과 예산주기의 연계』에서 후술한다.

58) 2013년 5월 30일 권은희 의원이 대표발의한 「정보통신기반보호법 일부개정법률안」에 따르면 "현행법은 관계중앙행정기관의 장으로 하여금 소관분야에 대한 주요정보통신기반시설에 관한 보호계획을 수립·시행하도록 하고 있으며, 침해사고에 대한 예방 및 복구대책에 관한 사항을 본 계획에 포함하도록 하고 있으나, 시설중심의 대책에 그치고 있어 **관리 정보의 백업시스템 구축 및 복구 등 데이터중심의 관리대책**을 명문화할 필요가 있음. 이에 침해사고에 대한 데이터의 안전한 관리 및 복구를 위하여 관리대책에 **관리 정보의 백업시스템 구축 및 복구**를 포함"하여 이를 명시적으로 규정하고자 한다.

그리고 관리기관의 장은 중앙행정기관의 장에게(법 제5조 제2항) 그리고 지방자치단체의 장은 안전행정부 장관에게(법 제5조 제3항)에게 보호대책을 제출하면 관계 중앙행정기관의 장은 법 제6조 제1항에 의하여 보호대책을 종합·조정하여 소관분야에 대한 보호계획을 수립·시행하여야 한다. 이는 사전예방의 보호체계에서 각 관리기관이 (사이버 안보에 관한) 위험을 분담하고 있는 영역 또는 자체적으로 수행하여야 하는 임무는 취약점을 분석·평가하고 보호대책을 수립·시행하며 정보보호책임자를 지정·운영하는 것이고, 그 다음 단계부터는 국가의 보호지원이 이뤄지는 영역이라고 평가할 수 있다.[59]

이와 관련하여 현행법상 미래창조과학부장관과 국가정보원장의 역할이 중요하다. 그들은 ① 보호대책 및 보호계획의 수립지침을 정하여 관계 중앙행정기관의 장에게 통보할 것이고(법 제6조 제4항), ② 관리기관에 대하여 주요정보통신기반시설보호대책의 이행여부를 확인할 수 있으며(법 제5조의2 제1항) ③ 확인을 위해 필요한 경우에는 관계중앙행정기관의 장에게 자료제출을 요청하거나 이행여부 확인결과를 통보할 수 있다(법 제5조의2 제2~3항). 그리고 ④ 관계중앙행정기관 장은 소관분야의 주요정보통신기반시설에 대하여 보호지침을 제정하고 관리기관의 장에게 이를 지키도록 권고(법 제10조 제1항)할 수 있고, ⑤ 정보통신기반보호위원장이 보완명령을 발하여 관리기관이 기술적 지원(법 제7조)을 받도록 하는 방안도 마련되어 있다.[60]

이와 같이 복합적이고 다층적인 메카니즘을 통하여 각 관리기관의

59) 법 제6조 제4항에서는 "미래창조과학부장관과 국가정보원장은 협의하여 주요정보통신기반시설보호대책(및 주요정보통신기반시설보호계획)의 수립지침을 정하여 이를 관계중앙행정기관의 장에게 통보할 수 있다"고 규정하고 있는데 이는 각 관리기관의 장에게 직접 통보하는 것은 아니지만, 관계 중앙행정기관의 장을 통하여 관리기관이 자율적으로 보호대책을 수립·시행하는데 작용할 것이므로 논리적으로 엄격히 판단하면 사전적인 국가의 개입과 관여라고 평가할 수도 있을 것이다.

60) 법 제7조 제1항은 정보통신기반보호위원회 위원장이 보완명령을 발하면 관리기관의 장이 "기술적 지원을 요청할 수 있다"는 재량규정으로 되어 있을 뿐이다.

장이 수립·시행하는 보호대책이 국가적 차원에서 요구하는 정보통신기반시설에 대한 보호수준에 미달할 경우에는 보완 또는 시정할 수 있을 것이다. 이와 같은 규율체계는 각 관리기관의 자율성과 책임성을 존중한다는 장점을 갖고 있지만, 규율내용을 체계적·종합적으로 검토하지 않으면 이해하기 어렵다는 문제점을 동시에 갖고 있다.

2. 정보보호책임자의 지정

관리기관의 장은 주요정보통신기반시설의 보호에 관한 '정보보호책임자'를 지정하여야 한다. 이에 관하여 필요한 사항은 필요한 사항은 대통령령으로 정하도록 위임하였다. 즉, 관리기관의 장은 소관 주요정보통신기반시설의 보호 업무를 담당하는 4급·4급상당 공무원, 5급·5급상당 공무원, 영관급장교 또는 임원급 관리·운영자를 정보보호책임자로 지정하여야 하고, 관할 중앙행정기관의 장에게 통지하여야 한다. 정보보호책임자가 총괄하는 업무는 시행령 제9조 제2항에 규정되어 있다. 즉, 법률 차원에서는 정보보호책임자를 반드시 선정하도록 정하고 있을 뿐, 그 자격, 권한과 의무, 업무와 기능 등 세부사항은 시행령 제9조에서 규정하고 있는 것이다.

그런데 법 제5조 제4항 단서에서 "다만, 관리기관의 장이 관계 중앙행정기관의 장인 경우에는 그러하지 아니하다"고 규정하고 있다. 이는 관리기관의 장이 중앙행정기관의 장인 경우에는 정보보호책임관(법 제6조 제5항)을 지정한다는 점을 고려하여 규정된 것으로 보인다. 즉, 중앙행정기관은 정보보호책임관(제6조) 그리고 중앙행정기관이 아닌 관리기관과 민간부문에서는 정보보호책임자(제5조)가 보호대책 수립 등의 임무를 수행하는 것으로 해석하는 것이 합리적일 것이다.[61]

61) 특히 시행령 제9조 제1항을 보면 "4급·4급상당 공무원, 5급·5급상당 공무원, 영관급장교 또는 임원급 관리·운영자를 정보보호책임자로 지정"하도록 되어 있는데, 중앙행정기관이 아닌 공공기관은 4~5급(상당) 공무원, 국방부문은 영관급 장교, 민간부문은 임원급 관리·운영자를 지정하도록 한 취지로 해석되어야 할 것이다.

Ⅲ. 주요정보통신기반시설보호대책 이행여부의 확인

1. 배 경

2007년 12월 정보통신기반보호법이 대폭 개정되어 주요정보통신기반시설 보호대책에 관한 사후관리체계가 개선되었다. 기존의 정보통신기반보호법은 주요정보통신기반시설 보호대책·계획의 수립과 시행에 관한 사항만 규정하고 있고 사후관리를 위한 확인 또는 점검 등에 대한 규정이 없어서 보호대책 및 보호계획이 형식화될 우려가 있었다. 이에 대처하기 위하여 법 제5조의2를 신설하여 당시 정보통신부장관과 국가보안업무를 수행하는 기관의 장(국정원장) 등 대통령령이 정하는 국가기관의 장으로 하여금 보호대책 이행 여부를 확인할 수 있는 근거를 마련한 것이다.[62]

법 제5조의2의 다음과 같은 기능을 수행한다. 첫째, 법 제5조에 따라서 각 관리기관이 자율적으로 수립하도록 규정되어 있는 보호대책의 실효성을 확보하고, 주요정보통신기반시설의 안정적 운용을 보장하며, 국가안전 및 국민생활안정을 도모하고자 하는 것이다. 둘째, 이를 위하여 법 제5조의2는 미래창조과학부장관과 국가보안 업무를 수행하는 기관의 장 등 대통령령이 정하는 국가기관의 장으로 하여금 보호대책 이행 여부 확인을 수행할 수 있는 근거(자료제출요청 및 결과통보)를 마련하고 있다. 국가의 관여와 개입(보호지원)은 각 관리기관의 권리제한 또는 의무부과를 야기할 수 있는 법규사항이므로 법률상 명시적인 근거가 필요하고, 법에 규정된 절차와 방식을 준수하여야 하기 때문이다. 셋째 관계 중앙행정기관의 장은 보호대책 이행여부 확인결과를 분석하여 별도의 보호조치가 필요하다고 인정하는 경

62) 2007년 12월 제3차 개정은 정보통신기반보호법의 상당부분을 개정하였고, 2008년 8월부터 시행되었다.

우에는 법 제11조에 의거하여 관리기관에 보호조치 명령을 할 수 있다. 즉, 이와 같은 체계적이고 종합적인 검토를 통하여 법 제5조의2에 규정된 “보호조치 이행여부의 확인”의 의미를 살펴볼 수 있다.

2. 이행여부 확인의 대상 및 절차

미래창조과학부장관, 국가정보원장 및 국방부장관은 다음과 같은 구분에 따른 관할 주요정보통신기반시설에 대한 관리기관의 주요정보통신기반시설보호대책 이행 여부를 확인할 수 있다.

미래창조과학부장관	민간분야 주요정보통신기반시설 (제5조 제4항 제2호에 따른 주요정보통신기반시설)
국가정보원장	공공분야 주요정보통신기반시설 (제5조제4항제1호에 따른 주요정보통신기반시설) (제3호의 국방 주요정보통신기반시설은 제외한다)
국방부장관	국방 분야 주요정보통신기반시설

이와 같이 미래창조과학부장관, 국가정보원장 및 국방부장관은 주요정보통신기반시설보호대책의 이행 여부를 확인하기 위하여 필요한 자료의 제출을 제2항의 구분에 따른 관할 주요정보통신기반시설 관리기관에 요청하고, 해당 주요정보통신기반시설보호대책에 따른 보호조치의 세부내용을 확인·점검할 수 있다. 이 경우에 미래창조과학부장관과 국가정보원장은 미리 확인절차 등에 관하여 관계중앙행정기관의 장과 협의하여야 하고, 미래창조과학부장관, 국가정보원장 및 국방부장관은 확인절차 등에 관하여 해당 관리기관에 통보하여야 한다.

그리고 미래창조과학부장관, 국가정보원장 및 국방부장관은 법 제5조의2에 따른 주요정보통신기반시설보호대책 이행여부 확인을 위하여 필요한 경우에는 시행령 제12조에 따른 “주요정보통신기반시설 보호

지원기관”에 지원을 요청할 수 있다. 주요정보통신기반시설보호대책 이행 여부의 확인에 관한 세부 사항은 미래창조과학부장관과 국가정보원장이 협의하여 정한다.

3. 이행여부 확인결과의 보고 등

미래창조과학부장관, 국가정보원장 및 국방부장관은 주요정보통신기반시설보호대책의 이행 여부 확인 결과를 “정보통신기반보호위원회”에 보고하여야 한다. 그리고 미래창조과학부장관, 국가정보원장 및 국방부장관은 주요정보통신기반시설보호대책의 이행 여부 확인 결과 보완이 필요하다고 판단되는 관리기관에 대해서는 개선을 권고할 수 있다(시행령 제9조의3 제2항).

이와 관련하여 법 제5조의2 제3항에 따르면 중앙행정기관의 장에게 이행여부의 확인결과를 통보하도록 되어 있는데 반하여, 시행령 제9조의3 제2항에 따르면 관계 중앙행정기관의 장을 통하지 않고 직접 관리기관에 대하여 개선권고를 하는 것이 규제순응성과 체계정당성 등에 있어서 문제를 일으킬 수도 있을 것이다. 즉, 정보통신기반보호법이 전제하고 있는 분화된 보호체계와 법률우위의 원칙을 고려하면 법률 제5조의2 제3항에서 “보호대책의 이행 여부를 확인한 결과의 통보를 관계중앙행정기관의 장에게 통보할 수 있다”면 시행령 제9조의3 제2항에 규정된 “개선권고”도 관계중앙행정기관의 장을 통하여 관리기관에 전달되도록 하는 것이 바람직할 것으로 생각된다. 그리고 개선권고의 효력은 이에 불응할 경우에 강제력을 담보할 수 없으므로 “정당한 사유가 없는 한 이에 따라야 한다”와 같은 규정을 삽입하는 것이 바람직할 수도 있을 것이다.

그리고 법 제5조의2에 따라서 미래창조과학부장관과 국가정보원장은 주요정보통신기반시설보호대책의 이행 여부 확인 결과를 다음 연도의 주요정보통신기반시설보호대책 및 주요정보통신기반시설보호계

획의 수립지침에 반영할 수 있다(시행령 제9조의3 제3항). 이는 주요정보통신기반시설 보호대책에 관한 사후관리체계의 개선을 통한 실효성 있는 정보통신기반시설보호대책 및 계획을 수립·시행하고자 하는 중요한 규정이라고 할 수 있다.

이행여부의 확인주기는 - 취약점 분석·평가와 달리 - 명확히 규정되어 있지 않으나 시행령 제9조의3 제3항의 취지를 고려할 때 매년 정기적으로 실시하는 것으로 해석할 여지가 있다.[63] 그러나 제5조의2 제1항(확인할 수 있다)은 임의적 재량조항으로 규정되어 있으므로 상시적으로 필요한 경우에 보호대책의 이행여부를 확인할 수 있는 것으로 해석하는 것이 합리적일 것이다.

그리고 제5조의2 제3항에 따르면 보호대책 이행여부의 확인결과를 점검받은 관리기관에게 반드시 통보하도록 규정하지 않고, 통보할 수 있다는 재량조항으로 규정되어 있다. 이는 제10조에 규정된 보호조치의 명령 또는 권고에 관한 권한으로 연결되어 보호대책을 제대로 이행하지 않은 경우에는 관리기관에 feed-back이 이뤄질 것이기 때문에 큰 문제가 없을 것으로 보인다.

마지막으로 시행령 제9조의3 제4항을 통하여 "미래창조과학부장관과 국가정보원장은 주요정보통신기반시설의 보호지원을 효율적으로 하기 위하여 주요정보통신기반시설보호대책의 이행 여부 확인 결과를

63) 이와 관련하여 2013년 2월 6일 조명철 의원이 대표발의한 「정보통신기반보호법 일부개정법률안」에 따르면 "1년에 최소 2회 이상 주요정보통신기반시설보호대책의 이행 여부를 확인하도록 하고, 이를 관계중앙행정기관의 장에게 통보하도록 의무를 부과하여 기반시설의 정보보호 조치를 강화하며, 도로·철도·항만·공항 등의 교통시설, 방송·통신시설, 수도·전기·가스 등의 공급설비, 금융·투자·기금 관련 기관, 병원·보건·의료시설 등과 관련된 정보통신기반시설의 경우에는 가급적 주요정보통신기반시설로 지정하도록 노력하게 하는 등 현행법의 미비점을 개선·보완하려는 것"이 주요 개정이유로 적시되어 있다. 이는 제5조의2 제1항을 "관리기관에 대하여 주요정보통신기반시설보호대책의 이행 여부를 확인할 수 있다"에서 "매년 2회 이상 정기적으로 확인하여야 한다"로 개정하는 안이다. 그러나 실무적으로 수백여개의 정보통신기반시설을 현재의 조직과 인력으로 1년에 2회 이상 정기적으로 확인하고 점검하는 것은 - 조직과 인력을 대폭 늘리지 않는 한 - 사실상 불가능할 것이다.

서로 제공"하도록 하여 유기적 협력체계를 구축하게 되어 있다. 이와 관련하여 공공부문과 민간부문 상호간 정보공유의 실익이 극대화될 수 있는 운영의 묘를 살리는 것이 필요할 것이다. 다만, 국가기밀에 관한 사항은 공개의 대상에서 제외하는 것이 바람직할 것이다.[64]

Ⅳ. 주요정보통신기반시설 보호계획의 수립 등

1. 의의 및 기능

관계 중앙행정기관의 장은 관리기관에서 수립·제출한 주요정보통신기반시설보호대책을 종합·조정하여 소관분야에 대한 주요정보통신기반시설보호계획을 수립·시행하여야 한다(법 제6조 제1항). 이는 앞서 살펴본 각 관리기관의 장이 취약점 분석·평가(법 제9조) 결과에 따라 보호대책을 수립하고 이를 관계중앙행정기관의 장에게 제출(법 제5조)한 것을 종합·조정하는 프로세스를 설명하고 있다. 그런데 보호대책을 제출하는 것은 제5조 제2항뿐만 아니라 제5조 제3항에 의하여 제출되는 경우도 있으므로 다음과 같이 제6조를 개정하여야 규율의 흠결이 없도록 개선할 수 있을 것으로 기대된다.

그리고 보호계획은 위원회의 심의사항으로서 관계 중앙행정기관의 장은 전년도 보호계획 추진실적과 다음 연도의 보호계획을 위원회에 제출하여야 하고(법 제6조 제2항), 그 내용은 정보통신기반보호법의 주요내용을 모두 포함하고 있다고 할 수 있을 정도로 매우 포괄적이고 광범위하다(법 제6조 제3항). 법 제6조 제2항의 규율내용은 시행령

64) 「공공기관의 정보공개에 관한 법률」 제4조 제3항은 "국가안전보장에 관련되는 정보 및 보안 업무를 관장하는 기관에서 국가안전보장과 관련된 정보의 분석을 목적으로 수집하거나 작성한 정보에 대해서는 이 법을 적용하지 아니한다"고 명시적으로 규정하여 정보공개의 대상에서 국가기밀을 제외하고 있다. 국가안보와 관계된 군사기밀보호법, 국가정보원법, 공공기록물관리에 관한 법률 등에서도 이와 유사한 규정을 찾아볼 수 있다. 이러한 법의 취지를 고려하여 이행여부의 확인결과가 국가안보와 관계된 경우에는 공유하지 않을 수 있는 근거를 마련하는 것이 필요하다.

제10조에서 구체적으로 규정되어 있다. 주요정보통신기반시설은 '단절된 개별 단위의 전산시스템 보호'보다는 '상호 연결된 정보통신망의 보호'가 중요하기 때문에 정보통신시스템의 단절 없는 상호 연동이 중요하고, 주요정보통신기반시설보호계획은 각 분야별로 서로 긴밀하게 연결되어야 하므로 각 중앙행정기관의 장에게 각 소관 분야별로 기본적인 보호계획을 수립·시행할 의무를 부과하고 있는 것이다. 그럼에도 불구하고 각 분야별로 분화된 보호체계의 특성상 이들 역시 각 중앙행정기관별로 차별적으로 규율될 경우에 나타날 수 있는 문제점을 사전에 방지하기 위하여 미래창조과학부장관과 국가정보원장은 협의하여 주요정보통신기반시설보호계획의 수립지침을 정하여 이를 관계중앙행정기관의 장에게 통보할 수 있다(법 제6조 제4항).

그리고 이 업무를 원활하게 수행하기 위하여 정보보호책임관을 지정하도록 하고 있는데, 이는 법 제6조 제5항과 시행령 제11조에서 구체적으로 규정하고 있다. 중앙행정기관의 장은 관리기관의 장이 수립·제출한 보호대책을 종합·조정하여 주요정보통신기반시설보호계획을 수립·시행하는데 이는 1) 주요정보통신기반시설의 취약점 분석·평가에 관한 사항, 2) 주요정보통신기반시설의 침해사고에 대한 예방 및 복구대책에 관한 사항, 3) 기타 주요정보통신기반시설 보호에 관하여 필요한 사항 등을 모두 포함한다(법 제6조 제3항). 이 과정에서 실무적으로는 정보통신기반시설 관리기관의 '정보보호담당자'가 '정보보호담당관'에게 보호대책을 제출하고, '정보보호담당관'이 보호계획을 작성하는 것이다.

2. 보호계획 수립방법에 대한 평가 : 상향식 의사결정의 적절성

이와 같이 정보보호계획을 수립하는 것은 주요정보통신기반시설에 대한 관리기관의 장이 자율적인 취약점 분석·평가가 이루어진 후 취약점 해소 및 완화를 위한 보호대책을 각 관리기관의 장(정보보호담

당자)이 작성·제출하고, 중앙행정기관의 장(정보보호담당관)은 이를 종합·조정하여 주요정보통신기반시설보호계획을 수립하는 상향식 절차에 의한다.

보호계획 수립에 있어서 상향식 의사결정구조에 의하는 이유는 정보보안분야의 높은 기술적 특성으로 인하여 현재의 기술수준, 보호대책, 취약점 등이 제대로 파악되지 않는 상태에서 하향식으로 '분야별 보호계획'이나 '종합보호계획'을 작성하는 것은 불가능하기 때문이다. 따라서 취약점의 분석·평가, 보호대책 그리고 이를 종합·조정한 분야별 보호계획 수립으로 이어지는 상향식 절차가 필요하다. 다만, 분야별보호계획 종합·조정이 단순한 제출자료의 취합이 되지 않기 위하여 사전에 주요정보통신기반시설보호대책 및 주요정보통신기반시설보호계획의 수립지침을 체계적으로 마련하여 중앙행정기관의 장에게 통보하고 있다.

이와 같이 정보통신기반시설보호계획을 수립함에 있어서 관리기관의 장이 수립한 보호대책을 기초로 하여 중앙행정기관의 장이 정보통신기반보호위원회의 심의를 거쳐서 확정하는 방식은 국가적 개입의 보충성 원리에 기인한다. 즉, 정보통신기반시설의 보호책임은 일차적으로 정보통신기반시설의 관리기관에 부여되고 기반시설의 보호대책이 자율적으로 달성되지 않는 한도 내에서 정부의 개입이 행해지는 것으로 하는 것이 바람직하기 때문이다. 특히 정보통신기반시설에 대한 침해사고가 발생하면 당해 시설의 운영·관리주체에게 큰 손해를 야기하고, 시설의 안정에 대한 이용자(일반 국민)의 신뢰를 상실하게 되므로 이에 대한 보호조치가 중요하다는 점에 대하여는 이의를 제기할 수 없을 것이다. 그리고 정보통신기반시설의 안정성을 확보하기 위하여 타율적 규제를 우선한다면 관리기관이 이를 준수하고 수용하는데 한계와 부담으로 작용할 것이므로 규제목적을 제대로 달성하기 어렵고 규제비용이 많이 들게 되는 문제점이 나타나게 될 것이다.

그럼에도 불구하고 관리기관의 자율적 규제만 남기고 정부에 의한 규제를 완전히 배제할 수는 없다. 특히 주요 정보통신기반시설에 대한 침해는 국가안전보장과 국민의 생활에 중대한 영향을 끼치는 등 사회적 파급효가 크기 때문에 정부는 정보통신기반시설보호에 무관심할 수 없고, 정보통신기반시설을 전자적 침해행위로부터 보호하기 위한 적절한 지원과 규제가 요청되는 것이다. 따라서 정보통신기반보호법은 상향식 규제수립절차와 자율성 보호 그리고 보충성의 원리에 입각하여 규율이 이뤄지고 있다.

그러나 이와 관련하여 미래창조과학부장관과 국가정보원장은 협의하여 주요정보통신기반시설보호대책 및 주요정보통신기반시설보호계획의 수립지침을 정하여 이를 관계중앙행정기관의 장에게 통보할 수 있도록 규정되어 있고(법 제6조 제4항), 이는 실제 운영과정에서 지침이 갖는 사실상의 구속력에 의하여 이는 대체로 준수되고 있다. 이는 마치 예산법제에서 기획재정부가 예산편성지침을 시달하면 각 중앙행정기관은 지침의 한계 내에서 자율적으로 예산사업의 우선순위와 예산규모를 자율적으로 편성할 권한을 보유하는 Top-down 방식의 제도운영과 유사하다고 평가할 수도 있는 것이다.

(어감상의 문제가 선입견으로 작용할 수 있겠지만) 하향식으로 규율구조 자체를 전환하는 것이 각 관리기관의 자율성을 보장하는 데 더욱 바람직하고,「정보통신기반보호법」관련규정은 일반적으로 상향식으로 마련되어 있다고 평가되고 있지만 실제 규율현실을 반영하여 이를 체계적으로 다음과 같이 정비하는 것이 바람직할 것이다.

3. 보호계획 수립일정과 예산주기의 연계

분야별 보호계획을 작성하는 중앙행정기관은 보호계획에 담긴 대책들을 시행하기 위한 예산사업에 대한 우선순위를 명확히 하고 중앙행정기관의 예산요구서 작성에 있어서 보호계획을 사업내역으로 반영하

여야 한다. 그리고 정보통신기반위원회의 심의도 각 분야별 주요정보통신기반시설보호계획에서 국가적 차원의 지원대책이나 예산사업을 결정하는 것에 비중을 둘 필요가 있고, 위원회의 결정사항이 예산편성 과정에 효과적으로 반영될 수 있어야 하므로, 취약점 분석·평가 - 보호대책 - 보호계획의 수립 - 위원회 심의 - 보호계획의 확정으로 이어지는 일정이 예산순기와 맞게 조정되는 것이 바람직하다.

현재 예산순기는 「국가재정법」과 「국회법」등의 개정으로 변화되고 있다. 「헌법」 제54조 제2항에 따르면 정부는 '회계연도 개시 90일 전(10월 2일)'까지 예산안을 편성하여 국회에 제출하도록 되어 있고, 국회는 '회계연도 개시 30일 전(12월 2일)'까지 예산안을 심의·확정하도록 되어 있다. 그러나 국가재정법 개정으로 정부가 국회에 예산안을 제출하는 시점은 '회계연도 개시 120일 전(9월 2일)'으로 앞당겨지게 되었고, 순차적으로 2014년도부터 3년간 '정부의 예산안제출시점'을 매년 10일씩 앞당겨서 국회의 예산심의권을 실질화하고자 하였다.

그리고 이와 더불어 중요하게 고려할 사항은 ① 기획재정부에서 각 부처에 다음 연도 부처별 지출한도와 예산안편성지침을 시달하는 시점은 4월 30일까지이고, ② 각 부처에서 예산요구서를 작성하여 기획재정부에 제출하는 시점은 6월 30일이라는 점이다. 그리고 ③ 5월에는 기획재정부가 각 부처의 전년도 예산집행실적을 종합하여 감사원의 검사를 받아 결산보고서를 국회에 제출하도록 되어 있다. 즉, 각 부처는 5~6월 동안 예산요구서를 작성하여 기획재정부에 제출하고, 국회는 이를 9~11월에 심의하여 12월 2일까지 확정하여야 하는 것이다.

현행 「정보통신기반보호법」의 기한규정은 다음과 같다. ① 미래창조과학부 장관과 국가정보원장이 다음 연도의 주요정보통신기반시설보호대책 및 주요정보통신기반시설보호계획의 수립지침을 작성하여 이를 관계중앙행정기관의 장에게 통보하는 기한(법 제6조 제4항, 시행령 제10조 제2항)은 5월 31일, ② 각 관리기관에서 다음 연도의 주요정보

통신기반시설보호대책을 수립하여 관계 중앙행정기관의 장에게 제출하는 기한(법 제5조 제1항, 시행령 제8조)은 8월 31일, ③ 전년도 보호계획의 추진실적과 다음 연도의 정보통신기반시설보호계획을 제출하는 시점(법 제6조 제2항, 시행령 제10조 제1항)은 10월 31일 그리고 ④ 중앙행정기관의 장이 다음 연도의 주요정보통신기반시설보호계획의 확정시점(시행령 제10조 제3항)은 12월 31일이다.

그런데 이는 헌법과 국가재정법상의 예산주기를 고려하면 지나치게 늦은 감이 없지 않다. 대표적으로 위원회의 심의를 거쳐서 보호계획을 확정하는 시점은 12월 31일이나, 이는 이미 국회에서 예산안을 심의·확정한 시점(12월 2일) 이후이므로 예산사업으로 반영되지 않은 사업내역을 추가하거나, 예산에 반영된 사업내용 또는 규모를 위원회의 심의과정을 통하여 혹은 중앙행정기관의 장이 변경하는 것은 불가능할 것이기 때문이다. 따라서 보호계획의 수립일정은 다음과 같은 수준으로 명확하게 하는 것이 보다 바람직할 것으로 보인다.[65]

1) 전년도 주요정보통신기반시설보호계획의 추진실적 제출 (1. 31)

2) 정보통신기반시설보호대책 및 정보통신기반시설보호계획의 수립지침 통보 (4. 30) / 부처별 지출한도액 및 예산안편성지침 통보시점과 맞추어 조정함

3) 정보통신기반시설보호대책의 수립 및 제출 (관리기관 → 중앙행정기관) (5. 30) / 전년도 보호계획의 추진실적도 함께 제출하여 결산과정에 반영하여 성과판단[66]

65) 이에 대한 규율은 현행 법령에 규정된 사항은 법률과 시행령을 동시에 개정하여야 할 것이다. 즉, 법 제5조 제1항, 제6조 제2항과 4항 그리고 시행령 제제8조, 10조 제1~3항 등이 그러하다. 그 이외의 사항은 대체로 동법 시행령에서 규율하면 충분할 것으로 판단된다. 그리고 박스 안에 제시한 일정은 개략적인 기한을 설정한 것이고, 이에 대하여는 각 부처 실무에서의 운영과정 등을 확인 및 의견회람하여 그 적정성을 재검토하는 것이 필요할 것으로 판단된다.

4) 정보통신기반시설보호계획의 수립 및 제출 (중앙행정기관 → 위원회) (6. 30) / 예산요구서의 제출시점에 맞추어 각 부처별 보호계획과 예산요구서의 내역 조정

5) 정보통신기반위원회 심의 및 심의결과 통보 (8. 20) / 정부가 국회에 예산안을 제출하기 직전에 정보통신기반위원회와 기획재정부가 협의하여 예산안에 위원회의 심의내용을 반영할 수 있는 절차를 마련할 필요성이 있을 수 있음

6) 다음 연도 정보통신기반시설보호계획 확정 (12. 31) / 국회가 예산을 확정한 후에 예산사업의 내역이 조정된 결과를 반영하여 각 부처에서 다음 연도의 보호계획을 확정하여 집행을 준비함.

4. 정보보호책임관(CISO : Chief Information Security Officer)

법 제6조 제5항과 시행령 제11조에 의거하여 각 부처 내에 소관 정보통신기반에 관한 보호를 담당하는 정보보호책임관을 둔다. 이는 각 부처의 정보화 기능을 강화하고, 소관 부처의 정보통신기반시설보호사업을 통합·조정하여 체계적이고 책임 있는 사업 추진을 가능하게 하기 위한 것이다. 즉, 정보보호책임관은 정보통신기반시설보호필요성에 대한 인식을 제고하고 보호업무의 효율적 추진을 위해 필요하다.

정보보호책임관은 정보통신기반시설에 대한 위협요소를 사전에 파악하고 분석하여 이를 경고하고, 정보보호책임관들 상호간의 협의를 통해 안전한 전자정부를 구축하기 위한 기반을 마련하며, 민간부문과의 협력 및 공조체제를 구축하는 업무를 수행한다.

66) 법 제6조 제1항에 따르면 전년도 추진실적을 다음 연도의 보호계획과 함께 10월 31일까지 위원회에 제출하도록 되어 있는데, 전년도 추진실적은 국가재정법상 결산기한인 5월 31일보다 그 이전에 제출되도록 하는 것이 합리적일 것이다. 이를 통하여 전년도 추진실적의 결산과 차년도 보호계획수립의 feed-back이 이뤄질 수 있고, 개선소요를 반영할 수 있을 것이기 때문이다.

정보보호책임관이 총괄하는 업무는 시행령 제11조에 열거적으로 규정되어 있다. 그리고 각 부처에 정보보호책임관은 관리자급 공무원으로 지정하여 '정보화책임관'의 지휘하에 각 부처의 소관 분야별 주요정보통신기반시설보호계획의 수립·시행과 각 관리기관의 보호업무 지원을 체계적이고 효율적으로 추진하도록 한다. 중앙행정기관의 장은 주요정보통신기반시설 보호업무를 담당하는 과장급 공무원을 '정보보호책임관'으로 지정하여야 한다.

그리고 정보통신기반보호법상 '정보보호책임관'은 국가정보화기본법에 따른 '정보화책임관'과 다른데, 정보통신기반보호법은 관계 중앙행정기관의 장이 정보보호책임관을 지정하도록 되어 있다는 점에서 모든 국가기관과 지방자치단체장이 지정하는 정보화책임관(1급 공무원)과는 차이가 있다.

제 4 장 정보통신기반시설의 보호를 위한 국가적 보호지원

제 1 절 주요정보통신기반시설에 대한 국가적 보호지원의 정당성

Ⅰ. 사이버 테러의 빈발과 사이버 안보정책의 변화

정부는 2013년 3월 20일에 발생한 방송사와 금융기관 등을 대상으로 한 '3. 20. 사이버테러'를 계기로 정부는 동년 4월 11일'국가사이버안전 전략회의'를 개최하여 『국가 사이버안보 종합대책』을 수립키로 논의하고, 청와대, 국정원, 미래·국방·안행부 등 16개 관계부처가 참여하여 종합대책을 수립하였다. 그 와중에 '6. 25. 사이버공격' 등 국가안보를 위협하는 각종 사이버 테러가 지속적으로 발생하였고 이에 대처하기 위하여 범국가 차원의 역량을 결집하여 관계부처 합동으로 『국가 사이버안보 종합대책』을 마련하여 시행한다고 동년 7월 4일 발표하였다.

이 종합대책에는 각종 사이버위협에 총력 대응할 수 있도록 '국가사이버안전센터'를 중심으로 관계부처간 협력공조와 민간 전문가의 참여를 확대해 나가는 한편, 청와대의 컨트롤타워 기능과 부처별 역할을 명확히 하여 기관간의 업무혼선과 중복을 최소화하고자 하였다. 사이버공간을 영토·영공·영해에 이어 국가가 수호할 또 하나의 영역으로 선언하고, "선진 사이버안보 강국 실현"을 목표로 사이버안보 강화를 위한 4대 전략을 수립하였다. 4대 전략(PCRC)이란, 1. 사이버위협 대응체계 즉응성 강화(Promptness), 2. 유관기관 스마트 협력체계 구축(Cooperative), 3. 사이버공간 보호대책 견고성 보강(Robust), 4. 사이버안보의 창조적 기반(Creative)을 조성하는 것을 의미한다.[67]

67) 이에 대하여는 2013년 7월 5일 한국뉴스투데이 기사 "박근혜 정부, 국가 사이버

최근에 발표된 사이버안보 종합대책의 핵심은 '컨트롤타워' 기능을 행사하는 주체(주관기관)이다. 이에 따르면 컨트롤 타워는 청와대가 맡고, 실무를 총괄·조정하는 기능은 국가정보원이 담당하게 한 것이다. 이에 대한 평가는 다소 엇갈리는 것으로 보인다. 한 언론은 "컨트롤타워를 청와대로 격상했다는 것은 이런 문제를 해결하자는 강력한 의지의 표현이다. 또 사이버안보를 몇몇 정부 부처 소관의 일이 아닌 국가적인 사안으로 보기 시작했음을 의미한다. 사이버안보 위기가 날로 고조된 상황에서 늦게나마 다행스러운 인식 전환이다. 철저한 사이버안보 대응 체계 구축의 시발점이 돼야 한다. 청와대가 전면에 나섰지만 실질적인 지휘를 국가정보원이 한다. 국정원이 사실상의 컨트롤타워인 셈이다. 청와대 - 국정원 - 유관부처 - 민간으로 이어진 지휘체계로 지휘 혼선이 사라지면 실시간 대응 속도도 빨라질 것이다. 기관 간 사이버위협정보를 공유하는 정보시스템 구축 등과 함께 부처 간 공조에도 탄력이 붙을 것이다"이라고 긍정적으로 평가했다. 이와 동시에 "국가정보원이 중심에 서면서 민간 시장이 위축될 가능성이 있다"는 우려도 동시에 제기했다. 이에 따르면 "보안 통제와 시장 육성은 어찌 보면 이율배반적"이라며 "시장을 아는 민간 전문가 의견을 적극 청취해야 한다"는 주장도 함께 나타나고 있는 것이다.[68]

또 다른 매체는 "주요정보통신기반시설이 확대되면 보안컨설팅 전문업체 지정도 덩달아 늘어나고, 국내 보안시장의 확대로 이어질 것"으로 예측하였다. 이에 따르면 "정보보호관리체계(ISMS) 인증 의무대상이 기존 250여개에서 500여개로 늘어남에 따라 보안컨설팅 시장 활성화도 기대"되고, "아직까지 확대 적용되는 대상의 기준은 나오지 않았으나, 의무대상에서 제외됐던 연매출액 100억원 이하인 영세 VIDC,

안보 종합대책 수립"(http://koreanewstoday.co.kr/detail.php?number=29126) 참조(2014년 10월 24일 최종방문).

68) 2013년 7월 5일 전자신문 "[사설] 사이버안보, 통제와 시장 균형점 찾을 때"(http://www.etnews.com/news/opinion/2793739_1545.html) 참조(2014년 10월 24일 최종방문).

정보통신서비스 사업자들이 포함될 가능성이 높아 보인다"는 예상도 등장하였다.[69]

원래 2004년 국가사이버안전관리체계의 출범 초기에는 국가안전보장회의(NSC) 사무처가 일정 부문 사이버 안보의 컨트롤타워 역할을 수행하였다. NSC 사무처 아래 정책조정실, 전략기획실, 정보관리실, 위기관리센터 등 4개 조직이 운영되었고, 이를 통하여 정보공유 및 경보발령, 사고대응, 상황처리업무 등 유관기관 조정을 통하여 범정부적 대응체계가 가동되었다. 그러나 2008년 이후 민간, 공공, 국방 분야에 대한 사이버 보안업무가 여러 조직으로 흩어져 이들을 총괄적으로 관리할 수 있는 핵심조직이 없고 조정하지 못하는 문제가 있었다.

결국 2013년 수립·시행된 국가 사이버안보 기본정책에 따르면 청와대가 컨트롤타워 역할을 수행하기로 하였다. 미국이 백악관에 '사이버안보조정관(Cyber-Security Coordinator)'을 두고 국가안보의 차원에서 컨트롤타워 역할을 수행하고 있듯이 우리나라에서도 기관 간 조정을 위해 청와대에서 그 역할을 수행하는 것이 바람직할 것이다.[70] 그리고 실무에서 총괄업무를 담당하는 국정원의 임무가 상당히 중요하다.

---

69) 2013년 7월 5일 디지털데일리 기사 "국가 사이버안보 종합대책…사실상 국정원이 사이버안보 총괄"(http://www.ddaily.co.kr/news/news_view.php?uid=106442) (2014년 10월 24일 최종방문).

70) 이명박 대통령 시절에는 IT 및 과학기술 담당 보좌관을 두고 사이버 보안 관련 업무도 수행토록 하였지만, 정보보안전문가들은 IT와 과학기술 전반을 관장하면서 국가안보 차원에서 접근하여야 하는 사이버 안보업무까지 관장하기는 어려울 것이라는 의견을 밝힌 바 있다. 2013년 2월 14일 ZDNet Korea 기사 "신설 국가안보실, 사이버 안보가 빠졌다" (http://www.zdnet.co.kr/news/news_view.asp?artice_id=20130213183429, 2014년 10월 24일 최종방문) 참조 ; 그리고 2008년 1월 이명박 대통령의 인수위는 위기관리센터인 NSC사무처 폐지를 발표하고 국가위기관리 전담 최고 조직(컨트롤타워)를 폐지했다. 위기관리 분야를 정부 업무 기관 평가 항목에서 제외했다. 국가가 직접 통솔하는 위기 관리 부문도 안보 분야로 국한하고 비안보분야는 각 주관 부처에 분산했다. 하지만 금강산 관광객 박왕자씨 피격 사건과 일본 원전 사고 등이 연이어 발생하자 결국 국가위기관리센터를 복원했다. 이후에는 국가위기관리실로 확대했다. 이에 대하여는 2014년 5월 28일 뉴시스 기사 "류희인 전 청와대 국가안전보장회의 사무차장 겸 위기관리센터장 서울대 강연"(http://www.newsis.com/ar_detail/view.html?ar_id=NISX20140528_0012947490&cID =10202&pID=10200, 2014년 10월 24일 최종방문) 참조.

국가정보원은 민간과 공공분야의 정책조정을 주 임무로 하고 보안정책의 실무를 총괄하는 기관으로서 각급 유관기관들의 협력을 극대화할 수 있는 조정자 역할을 충실히 수행하여야 할 것이다.

Ⅱ. 사이버 안보법제의 체계적 정비방안

현재 우리나라의 사이버 안보와 관련된 법제는 나름대로 부처별 기능과 특성에 맞추어져 있다. 이는 사이버 공격 등 전자적 침해행위에 대응하면서 그 대응체계가 지속적으로 수정·보완되고 정비되어 왔기 때문일 것이다. 이를 위해 「정보통신기반보호법」은 관리기관과 이를 감독하는 중앙행정기관 그리고 각 부문별로 미래창조과학부, 국가정보원, 국방부 등 매우 복잡한 단계구조를 전제하고 있고 이를 통하여 국가의 보충적 개입과 보호지원이 가능하도록 되어 있다.

전통적으로 사이버 안보에 대한 법적 규율과 정보화(정보이용의 촉진 및 진흥) 법제는 매우 밀접히 연관되어 있어서 법제도의 혼란과 아울러 관련 법령을 해석함에 어려움이 항시 존재하고 있다. 따라서 사이버 안보정책은 정보화의 부수정책으로 인식할 것이 아니라, 독자적 영역으로 보고 국가안보의 관점에서 체계적으로 정비할 필요가 있다. 이를 위해서 현재 각종 법령과 규정, 규칙들에 등장하는 사이버 안보와 관련된 법제와 전통적인 정보화 법제의 수행체계를 구별하고 사이버 안보법제의 통합적인 집행체계가 구축되어야 한다.

우선 법치국가원리에 부합하도록 중요사항이라 할 수 있는 사이버 안보정책의 총괄기관을 법률로 지정하여 이에 관련된 기관간의 업무협조는 물론, 보호계획의 수립 및 보고체계의 통합, 사이버침해사고 대응을 위한 각 기관별 책임과 역할을 명시하는 등 정책집행체계를 과감히 개편하는 방안을 검토하여 법제를 정비하여야 한다. 이를 위하여 청와대가 사이버 안보의 컨트롤 타워 역할을 하고 국가정보원이 실무를 총괄하는 “사이버 안전 종합대책”에 부합하는 방향으로 관련

법제도를 정비를 하는 것이 합리적일 것이다. 즉, 국가정보원, 미래창조과학부, 안전행정부, 국방부, 검찰 및 경찰 등에 분산된 사이버 안전에 대한 임무를 총괄하고, 효율적·유기적으로 연계하여 기능할 수 있는 컨트롤 타워로서의 기능을 청와대가 실질적으로 수행할 수 있도록 법제를 정비하여야 할 것이다. 특히 사이버 안전을 침해하는 사고가 발생하여 국가안보를 위협하는 상황에 대응하기 위한 법집행체계를 명확히 하고 이를 법령에 명시하여 업무 관할영역에 대한 기관간의 이견과 행정낭비를 최소화하는 것이 필요하다.[71] 그리고 주요정보통신기반시설 관리기관의 경영활동을 지원하기 위하여 인센티브를 제공하는 방안도 생각해 볼 수 있다.[72]

Ⅲ. 사이버침해 대응체계 개관

국가적 차원의 사이버 안보 국가기밀과 군사·외교정보를 포함한 국가안보정보는 물론 산업기밀 정보 등까지도 함께 보호하는, 국익과 직결된 업무로서 국민의 안전한 삶에 직접적인 영향을 미치고 있다. 그렇기 때문에 우리나라의 사이버 안보는 '정부조직법'을 비롯한 다양한 법령에 기반하여 다양한 기관들이 분야별로 분담하여 업무를 수행하고 있는 바, 주로 국가정보원, 미래창조과학부, 국방부, 수사기관(검

71) 정보통신망 이용촉진 및 정보보호 등에 관한 법률의 경우 정보통신망 이용촉진 등 정보화 관련사항과, 정보통신망의 안전성 확보 등의 정보보안 관련사항, 개인정보보호 관련사항이 하나의 법률안에서 규율되고 있다. 그리고 국가정보화기본법, 전자정부법, 정보통신기반보호법, 정보통신망법, 국가사이버안전관리규정 등을 검토해 보면 보호시설에 대한 보호계획을 이중·삼중의 보호계획수립, 보호대책의 이행여부 또는 보고서 제출 등 중복행정으로 인한 낭비적 요소가 적지 않다. 이를 개선하기 위하여는 공공분야 정보보안 관리실태 평가 및 민간부문의 정보보호관리체계 인증심사시 주요정보통신기반시설에 대한 취약점 분석·평가를 받은 경우에는 중복되는 항목을 제외하는 등 절차를 간소화하는 방안 등을 생각해 볼 수 있을 것이다.

72) 예컨대 중앙행정기관과 지방자치단체의 정부업무평가 및 공공기관의 경영평가에 정보보안 실태평가결과 반영비율을 확대하고, 정부업무평가 및 경영평가의 세부항목에 "정보통신기반보호활동"과 관련된 사항을 확대반영하는 방안 등을 생각해볼 수 있을 것이다.

찰 및 경찰) 등이 각 기능별로 업무를 담당한다.

그 중에서도 국가정보원은 「정부조직법」 제15조에 의거하여 대통령 소속 하에 국가안전보장과 관련되는 정보·보안 및 범죄수사에 관한 사무를 담당할 목적으로 각급 기관에 대한 정보 및 보안업무의 기획, 조정업무(「국가정보원법」 제3조)를 수행한다. 또한, 「국가안전보장회의법」 제10조에 의거하여 국가안보와 관련된 국내외 정보를 수집·평가, 이를 국가안전보장회의에 보고함으로써 심의에 협조하여야 한다. 그리고 국가정보원은 「정보및보안업무기획조정규정(대통령령 제21214호)」, 「보안업무규정」에 의거하여 각급 기관에 대한 보안업무를 수행하고, 「국가사이버안전관리규정」에 의거하여 사이버 보안정책 총괄 및 위협정보 수집·분석, 대응 업무를 수행한다.

이와 같이 국가사이버안전관리체계는 기본적으로 국가정보원이 담당하고 있음을 부인할 수 없다. 이는 「국가정보원법」, 「보안업무규정」, 「정보 및 보안업무 기획조정규정」과 「정보통신기반보호법」, 「전자정부법」 등 관련 법령에 의해 국가 정보보안업무의 기획·조정 및 보안정책 수립 시행 등 국가·공공기관에 대한 정보보안업무를 담당하고 있는 것이다. 특히 「국가사이버안전관리규정」 제5조에 따르면 사이버 안보정책 및 관리에 대해 국가정보원장이 관계 중앙 행정기관의 장과 협의, 이를 총괄·조정하는 등 국가정보원은 국가사이버안전관리업무를 수행하는 전담기관이라고 할 수 있다.[73]

이를 뒷받침하기 위하여 국가정보원장 소속 하에 국가 사이버 안전에 관한 중요사항을 심의하기 위하여 '국가사이버안전전략회의'를 설

73) 국가사이버안전관리규정 제5조(국가사이버안전정책 및 관리) ① 국가사이버안전과 관련된 정책 및 관리에 대하여는 국가정보원장이 관계 중앙행정기관의 장과 협의하여 이를 총괄·조정한다. <개정 2012.1.2>
② 국가정보원장은 제1항에 따른 총괄·조정 업무를 효율적이고 체계적으로 수행하기 위하여 관계 중앙행정기관의 장과 협의하여 국가사이버안전기본계획을 수립·시행한다. <신설 2012.1.2>
③ 국가정보원장은 제2항에 따른 국가사이버안전기본계획을 원활하게 추진하기 위하여 관계 기관에 예산 반영 등에 관한 협조를 요청할 수 있다. <신설 2012.1.2>

치・운영하고,[74] 효율적 운영을 위하여 '국가사이버안전대책회의'[75]와 '국가사이버안전센터'[76]를 두고 있다.

Ⅳ. 침해사고의 특성과 국가정보원의 역할

현재 사이버 안보와 관련된 법제도의 정비는 다음과 같은 점들을 반드시 고려하여야 한다. 첫째, 산발적인 기관별 사이버안보정책 추진의 문제점을 극복하기 위하여 노력하고 있는 미국과 일본 등 해외 주요 선진국의 사이버 관련 정책의 추진과정에서 알 수 있듯이, 사이버안보의 중심적인 역할 수행을 위한 조직 및 추진체계에 관한 법적 지위를 확보하여야 한다. 둘째, 관련 기관 간 정보공유 및 예・경보체계와 관련된 법제정비가 필요하다.[77] 셋째, 국가사이버안전을 위한 중장

74) 이는 우리나라 사이버 안보의 중요한 정책심의기구라고 할 수 있다. 이에 대하여는 「국가사이버안전관리규정」 제6조 참조 ; 다만 그 의장은 국가정보원장이고 위원회의 위원은 각 정부부처의 차관 및 대통령비서실 사이버안전 담당 수석비서관, 국가안보실 사이버안전 담당 비서관, 국무조정실 국무차장 등이기 때문에 「정보통신기반보호법」 제3조에 의거한 국무총리 소속 하의 정보통신기반보호위원회(위원장 국무조정실장, 위원은 차관급 공무원)와의 관계가 문제될 수 있을 것이다.

75) 이에 대하여는 「국가사이버안전관리규정」 제7조 참조.

76) 이에 대하여는 「국가사이버안전관리규정」 제8조 참조 ; 국가사이버안전센터(National Cyber Security Center : NCSC)는 사이버공격에 대한 국가차원의 체계적인 대응을 위해 2004년 2월 설립된 기관으로서 정보통신망에 대한 24시간 사이버 위협정보를 수집・분석・전파하는 국가 종합상황실을 운영하면서 각종 사이버공격에 대한 예방・대응활동과 피해확산 방지에 주력한다. 또한 국가・공공기관 등 공공분야를 대상으로 사이버위협에 대한 수준별 경보발령 등 각종 사이버공격에 대응하고 24시간 네트워크 보안관제를 통해서 사이버 공격 정보를 수집・분석하여 각급기관에 전파한다. 그 주요임무는 1. 국가사이버안전정책의 수립, 2. 전략회의 및 대책회의의 운영에 대한 지원, 3. 사이버위협 관련 정보의 수집・분석・전파, 4. 국가정보통신망의 안전성 확인, 5. 국가사이버안전매뉴얼의 작성・배표, 6. 사이버공격으로 인하여 발생한 사고의 조사 및 복구 지원, 7. 외국과의 사이버위협 관련 정보의 협력 등이고, 국가정보원장은 국가 차원의 사이버위협에 대한 종합판단, 상황관제, 위협요인 분석 및 합동조사 등을 위해 사이버안전센터에 민・관・군 합동대응반(이하 "합동대응반"이라 한다)을 설치・운영할 수 있다.

77) 예컨대 사이버테러 대응기구들 간 정보공유의 법적 근거 확보 및 해당 정보의 오・남용을 막기 위한 제도적 장치가 필요하고, 사이버공격 위협에 대응하기 위한 국가차원의 예・경보체계의 도입・시행에 관한 사항이 규정되어야 할 것이다.

기적 관점에서의 정책과 기술에 대한 연구 및 핵심기술 개발을 위한 재정지원 등에 관한 규정이 필요하다.[78]

이와 같은 규범적 요청은 사이버 테러의 특성에 기인한다. 사이버위기는 태풍과 같은 자연재해로부터 오는 재난이 아니라 국가혼란 등의 목적을 가진 특정인이나 집단에 의하여 이루어지기 때문에 국가안전보장의 관점에서 접근하여야 한다. 따라서 사이버 안전의 관리체계는 재난관리체계와 구별되어야 하고, 전방위적으로 나타날 수 있는 문제이기 때문에 부처간 협업이 매우 중요하다. 각 중앙행정기관은 소관업무에 따라 이에 대응하여야 하고, 국가정보를 전문적으로 지키는 보안기관은 이에 대한 기술적 역량과 전문성을 바탕으로 보호지원과 실무를 조정·총괄하는 임무를 수행하여야 하는 것이다.[79]

현대 사회에서 사이버 공격과 테러는 일상적인 것이 되어 버렸고, 다양한 정치적·경제적 이유로 말미암은 사이버 공격이 등장하고 있다. 이러한 상황에서 사이버 공격에 대한 효과적인 대응체제를 구축하여야 하고, 총괄기관을 두는 것을 두려워해서는 안 될 것이다.[80] 사이버안보종합대책과 법제의 연계성을 강화하고 효과적으로 안전한 사이버 환경을 확보하기 위한 개선방안이 절실한 시점이다.

---

78) 이에 대하여는 『제4장 제3절 Ⅱ. 관리기관에 대한 지원』 참조. 이와 관련하여 국가사이버안전관리규정 제5조 제3항은 관계 기관에 예산반영 등에 관한 협조를 요청할 수 있게 규정되어 있으나, 대통령 훈령에 근거하여 예산요구를 하는 경우 그 실효성이 문제될 위험성이 있다.

79) 사이버 공격에 대응하기 위한 전문성, 노하우, 기술력 등은 단기간에 확보될 수 없고, 특별한 충성심과 희생이 필요하다. 외국에서도 사이버 안보 업무를 담당하는 직원을 선발하는 기준으로 반드시 적성평가를 거치도록 규정하고 있다. 순환근무원칙상 주기적으로 인사이동을 해야 하는 일반부처에서는 IT 보안업무를 지속적으로 수행하여 최신의 기술적 역량을 축적하기에 부적절하다. 2013년 7월 발표된 "국가사이버안보 종합대책"은 청와대가 콘트롤 타워를 맡고 국가정보원이 실무를 총괄하는 내용의 사이버 안전관리체계를 구축하였는데, 이는 각 부처와 관리기관의 임무와 역할을 강조하고, 각 기관의 자율성과 책임성을 강화하기 위한 것이다.

80) 이에 대하여는 2013년 4월 6일 중앙일보 "국가사이버안전관리, 누가 하나" (http://article.joins.com/news/article/article.asp?total_id=11151710&cloc=olink|article|default, 2014년 10월 24일 최종방문) 참조.

제 2 절 정보통신기반보호와 관련된 조직

Ⅰ. 정보통신기반보호위원회

1. 입법취지

「정보통신기반보호법」 제3조는 정보통신기반시설의 보호에 관한 사항을 심의하기 위하여 '정보통신기반보호위원회'를 규정하고 있다. 이는 정부조직법 제5조에 의거한 합의제 행정기관[81]으로서, 주요사회기반시설의 운영·제어와 관련된 정보통신기반시설의 보호임무는 각 부처와 관련되어 있기 때문에 범정부적 차원에서 효과적으로 정책을 수립·시행하기 위해 국무조정실장을 위원장으로 하고 관계부처 차관급 공무원 등을 위원으로 하는 '정보통신기반보호위원회'를 설치하였다.[82]

「정보통신기반보호법」 제정 당시에는 「정보화촉진기본법」(현재 국가정보화기본법) 상의 '정보화추진위원회'가 존재하고 있었다. 이는 정보화촉진 등에 관한 사항을 심의하기 위하여 국무총리 소속하에 설치된 위원회인데, '정보화추진위원회'는 정보통신기반시설에 대한 보호대책을 심의할 경우 전문성이 부족하고[83], 범국가적 대응체계 구축

81) 합의제(Kollegial) 행정기관으로서 각 부처의 이해관계를 신중하게 조정하는 장점이 있으나, 영미법에서 나타나는 독립행정기관으로서의 '독립규제위원회(Independent Regulatory Committee)'가 아니라는 점에 유의하여야 할 것이다.

82) 2001년 본 법률의 제정 당시 사무국 구성에 관한 의견도 있었으나, 국가와 공공기관의 사이버테러 대응 업무는 국가정보원이 주관하고, 민간의 동 업무는 구 정보통신부(현재 미래창조과학부)가 지원하고 있어, 정보통신기반보호위원회 구성시 양 부처중 단일 부처로의 사무국 구성이 곤란할 것으로 예상되고, 이를 운영하기 위하여는 상시 근무하는 인력이 필요하게 되는 등 불필요한 조직확대가 예상되어 위원회로 구성하기로 합의하였다.

83) 제 8 조 (정보화추진위원회) ① 정보화촉진 등에 관한 사항을 심의하기 위하여 국무총리소속하에 정보화추진위원회를 둔다.
② 위원은 위원장·부위원장을 포함하여 25인 이내로 한다.
③ 위원장은 국무총리가 되고, 부위원장은 재정경제부장관이 되며, 위원은 국회사무총장·법원행정처장·관계행정기관의 장중에서 위원장이 위촉하는 자로 한다. 다만, 국회사무총장과 법원행정처장은 제9조에서 정한 위원회의 심의사항이 당해 기

에 한계가 있으므로, 정보화 촉진 및 진흥업무와 달리 사이버 위협요인에 따라 관련 부처가 유기적이고 신속하게 대응해야 할 필요성이 있어 별도의 위원회를 구성·운영하는 것이 바람직하므로 '정보통신기반보호위원회'를 별도로 설치하게 된 것이다.[84]

2. 구성 및 운영 등

(1) 구성방식

정보통신기반보호위원회의 구성에 관한 규정을 살펴보면 '위원장'은 법률에서, '위원'은 법률이 시행령에 위임하여 규정하고 있다. 그리고 '간사'는 법률상 근거 없이 시행령에서 규정하고 있을 뿐이다. 위원장은 국무조정실장이 되고, 위원은 "대통령령이 정하는 중앙행정기관의 차관급 공무원과 위원장이 위촉하는 자로 한다"고 하면서 시행령에서 "기획재정부차관, 미래창조과학부차관, 외교부차관, 법무부차관, 국방부차관, 안전행정부차관, 산업통상자원부차관, 보건복지부차관, 고용노동부차관, 국토교통부차관, 해양수산부차관, 국가정보원 차장, 금융위원회 부위원장, 방송통신위원회 상임위원"을 규정하고 있다. 간사는 국무조정실의 정보통신기반시설 보호업무를 담당하는 고위공무원단에 속하는 공무원이 된다.

이와 관련하여 정보통신기반보호위원회의 위원장이 제4차 개정(2008. 2)에서 국무총리실장으로 격상되었다가, 제6차 개정(2013. 3)에

관의 업무와 관련되어 있어 협조가 필요하거나 기타 필요한 경우에 한하여 위원회에 출석한다.

④ 위원회에 간사 1인을 두되, 간사는 국무조정실장이 된다.

84) 2013년 신규 제정된 「정보통신 진흥 및 융합 활성화 등에 관한 특별법」에서도 '정보통신 진흥 및 융합 활성화'를 위하여 국무총리 산하에 "정보통신전략위원회"를 두고 있으나, 이와 동일한 문제점이 노출되어 별도의 정보통신기반위원회를 운영하고 있다. 따라서 청와대 국가안전보장회의(NSC)와의 관계, 국무총리실의 정보화추진위원회 그리고 국정원장 소속의 사이버안전전략회의 등과의 관계 정립도 문제될 수 있을 것이다.

서 국무조정실장으로 재조정된 바 있다. 이와 같이 국무총리 산하에 정보통신기반보호위원회가 구성되도록 한 이유는 범정부 차원의 협력체계가 구성될 필요가 있었기 때문일 것이다. 다만, 2013년 발표된 사이버안보종합대책에서 청와대가 콘트롤 타워 역할을 맡기로 하였다는 점을 고려한다면 정보통신기반시설 보호의 중요성을 고려하여 소속을 변경할 필요가 있을 수 있다.[85]

(2) 운영방식

정보통신기반보호위원회의 운영에 관한 규정은 법 제3조 제5항에 의하여 시행령에 위임되어 있다. 시행령 제3조 제4항부터 제7조(운영세칙)까지 규율하고 있는 내용은 운영에 관한 규정이라고 할 수 있는데 주요내용은 다음과 같다.

정보통신기반보호위원회의 위원장은 회의를 소집하고, 그 의장이 된다. 위원장이 부득이한 사유로 직무를 수행할 수 없는 때에는 위원장이 지명하는 위원의 순으로 그 직무를 대행한다. 위원회의 회의를 소집하고자 하는 때에는 회의 일시·장소 및 부의사항을 회의개최 7일 전까지 각 위원에게 서면 또는 전자문서로 통지하여야 한다. 단, 긴급을 요하거나 부득이한 사유가 있는 경우에는 그러하지 아니하다. 위원장은 법 제4조(위원회의 기능) 각호의 규정에 의한 사항의 심의를 위하여 필요하다고 인정되는 경우에는 관련 전문가 또는 전문기관의 장으로 하여금 그에 관한 검토보고를 하게 할 수 있다. 위원회는 재적위원 과반수의 출석과 출석위원 과반수의 찬성으로 의결한다.

85) 대통령 산하의 위원회를 설치하는 것은 매우 어려운 일이지만, 2013년 발표된 사이버안보종합대책에 따르면 청와대 국가안보실이 사이버 안전에 대한 컨트롤 타워의 역할을 맡기로 하였으므로, 정책과 법제의 연계성을 강화하기 위하여는 대통령 소속 하에 정보통신기반보호위원회를 설치하는 것이 보다 합리적일 것으로 생각된다. 다만, 이와 같이 법개정이 이뤄지지 못한다 하더라도 실무상 국가정보원이 총괄 및 조정기능을 보완하여 각 중앙행정기관과 주요정보통신기반시설의 관리기관들이 자신들의 보호역량을 강화할 수 있도록 하는 것은 현행법의 테두리 내에서 사이버 안보종합대책을 수립·시행하는 취지에 부합하는 것으로 평가할 수 있다.

(3) 실무위원회의 설치 및 운영

실무위원회는 정보통신기반위원회의 효율적 운영을 위하여 설치한 것이므로 크게 보면 운영에 관한 규정의 일부라고 할 수 있으나, 그 의미와 비중을 고려하여 별도로 설명하고자 한다. 실무위원회의 중요성에 비추어 그 설치근거가 법률 제3조 제4항에 마련되어 있고, 세부적인 사항은 시행령 제5조에서 자세하게 규정하고 있다.

공공분야를 담당하는 실무위원회와 민간분야를 담당하는 실무위원회는 각각 위원장 1명을 포함한 25명 이내의 위원으로 구성한다. '공공분야 실무위원회의 위원장'은 국가정보원 차장이 되고, '민간분야 실무위원회의 위원장'은 미래창조과학부 제2차관이 되며, 각 실무위원회 위원장은 해당 실무위원회의 회의를 소집하고 그 의장이 된다. 각 실무위원회의 위원은 다음 중 어느 하나에 해당하는 사람 중에서 각 실무위원회의 위원장이 임명하거나 위촉한다.[86] 그리고 각 실무위원회의 사무를 처리하기 위하여 각 실무위원회에 간사 1인을 두되, 간사는 실무위원회 위원장이 지명하는 소속 공무원이 된다. 실무위원회의 운영에 관하여는 시행령 제3조 제2항부터 제5항까지 그리고 제4조를 각각 준용한다.[87]

86) 실무위원회 위원장은 "법 제8조에 따라 지정된 주요정보통신기반시설을 관할하는 중앙행정기관의 고위공무원단에 속하는 공무원 또는 그에 상당하는 공무원 또는 주요정보통신기반시설을 관리하는 기관의 임원 또는 직원" 중에서 위원을 임명하거나 위촉한다.

87) 즉, 실무위원회 위원장이 부득이한 사유로 직무를 수행할 수 없는 때에는 실무위원회 위원장이 지명하는 위원의 순으로 그 직무를 대행한다. 각 실무위원회의 회의를 소집하고자 하는 때에는 회의 일시·장소 및 부의사항을 회의개최 7일전까지 각 위원에게 서면 또는 전자문서로 통지하여야 한다. 다만, 긴급을 요하거나 부득이한 사유가 있는 경우에는 그러하지 아니하다. 실무위원회 위원장은 법 제4조 각 호의 규정에 의한 사항의 심의를 위하여 필요하다고 인정되는 경우에는 관련 전문가 또는 전문기관의 장으로 하여금 그에 관한 검토보고를 하게 할 수 있다. 그리고 실무위원회는 재적위원 과반수의 출석과 출석위원 과반수의 찬성으로 의결한다.

공공분야 실무위원회	o 공공분야 실무위원회 위원장 : 국가정보원 차장 o 국가・지방자치단체・공공기관이 관리하는 주요정보통신기반시설 - 중앙행정기관・지방자치단체 및 그 소속 기관의 장이 관리하는 주요정보통신기반시설 - 국회・법원・헌법재판소・중앙선거관리위원회 및 그 소속 기관의 장이 관리하는 주요정보통신기반시설 -「전자정부법」제2조 제3호에 따른 공공기관이 관리하는 주요 정보통신기반시설
민간분야 실무위원회	o 민간분야 실무위원회 위원장은 미래창조과학부 제2차관 o 민간분야 주요 정보통신기반시설

각 실무위원회는 다음의 구분에 따른 주요정보통신기반시설의 보호에 관하여 위원회의 심의를 지원한다. 또한 다음의 구분에 따른 주요정보통신기반시설의 보호에 관하여 위원회가 위임하거나 위원회의 위원장이 지시한 사항을 검토・심의한다.

3. 기 능

법 제4조는 정보통신기반보호위원회의 기능과 역할을 구체화하여 심의 대상을 명확히 규정하고자 하였다. 정보통신기반보호위원회의 심의대상으로 ① 주요정보통신기반시설 보호정책의 조정에 관한 사항, ② 제6조 제1항에 따른 주요정보통신기반시설에 관한 보호계획의 종합・조정에 관한 사항, ③ 제6조 제1항에 따른 주요정보통신기반시설에 관한 보호계획의 추진 실적에 관한 사항, ④ 주요정보통신기반시설 보호와 관련된 제도의 개선에 관한 사항, ⑤ 그 밖에 주요정보통신기반시설 보호와 관련된 주요 정책사항으로서 위원장이 부의하는 사항을 규정하였다. 이와 같이 심의대상을 구체화함으로써 정보통신기반보호위원회로부터 실무위원회로 위임되거나 실무위원회의 지원이 필요한 대상도 심의대상으로 구체화되었다고 평가할 수 있다.

제5호에서 “그 밖에 주요정보통신기반시설 보호와 관련된 주요 정책사항으로서 위원장이 부의하는 사항”을 포괄적으로 규정하여 정보통신기반시설 보호와 관련된 정책을 전반적으로 심의할 수 있게 되어 있음을 알 수 있다. 그러므로 위원장이 직권으로 부의하여 무엇이든 주요정보통신기반시설 보호와 관련된 주요 정책사항을 심의할 수 있게 되어 있는 것이다. 그러나 입법론적으로 보면 위원회에 심의기능만 갖고 있고, 의결기능이 없다는 점은 아쉬운 점이 있다. 위원회에서 심의한 내용을 실제 각 정부부처에서 정보통신기반보호정책으로 수립되고 보호계획의 수립지침을 통하여 각 관리기관의 보호대책에 반영될 것이지만, 이는 각 관리기관의 자발적 협력을 전제로 한다.

4. 문제점

현행「정부조직법」제26조에 따르면 현 정부는 17개 부처로 구성되어 있는데,「정보통신기반보호법 시행령」제2조에 따르면 ‘교육부’, ‘통일부’, ‘문화체육관광부’, ‘농림축산식품부,’ ‘환경부’, ‘여성가족부’ 등 6개 부처의 차관은 정보통신기반보호위원회 위원으로 열거되어 있지 않다. 이와 같이 시행령을 통하여 한정적 열거방식으로 규율한 이유는 주요정보통신기반시설을 관리하는 정부부처를 명확히 규정하고 향후 그 지정을 추가하거나 제외시키는 사유가 발생하면 입법기술상 탄력적으로 대응하기 위한 것으로 보인다.[88] 따라서 주요정보통신기반시설을 관리·감독하는 부처는 이에 포함하여 규율하는 것이 바람직할 것으로 판단된다.[89]

이를 종합적으로 고려하면 입법기술상 열거적 방식으로 각 부처의 명칭을 나열하는 것보다는 “정부조직법상 각 부처의 차관(단, 주요정

88) 현행 규정방식과 마찬가지로 열거적 규율을 지속할 경우에는 정부조직법이 개정될 때마다 이에 따라서 시행령도 개정작업이 계속 뒤따를 수밖에 없을 것이다.

89) 특히 최근에 교육부장관은 비경제분야를 총괄하는 부총리로 승격되었고, 교육부에서 관장하는 “NEIS 시스템”이 정보통신기반시설로 지정되었다는 점을 고려한다면 ‘교육부차관’도 정보통신기반보호위원회 위원으로 인정하는 것이 타당할 것이다.

보통신기반시설을 관리·감독하지 않는 중앙행정기관은 제외할 수 있다)"으로 규율하는 것이 조문의 간결성, 경제성 원칙에 부합할 것으로 보인다.[90] 다만, 시행령 제2조 12호(국가정보원 차장), 13호(금융위원회 부위원장) 그리고 14호(방송통신위원회 상임위원)은 부처의 차관이라고 할 수 없으므로 이들은 별도로 규정할 필요가 있을 것이다.

Ⅱ. 침해사고 대책본부의 구성(법 제15조)

1. 의의 및 기능

주요정보통신기반시설에 대한 침해사고에 즉시 대응하기 위하여 관계부처 및 기관의 협력조직으로 침해사고대책본부를 구성하였다. 정보통신기반보호위원회에 사무국과 같은 상설기구를 두고 있지 않는 대신 정보통신기반시설에 대한 침해사고 발생 시 응급대책, 기술지원 및 피해복구 등을 수행하기 위한 (비상설) 기구는 필요하기 때문이다.

침해사고 대책본부 침해사고가 설치되는 사유인 "주요정보통신기반시설에 대하여 침해사고가 광범위하게 발생한다"는 의미는 법 제12조와의 관계를 고려하여 해석해 보면 "다수의 정보통신기반시설의 운용이 교란, 마비 또는 파괴되어 정상적인 정보통신기반시설의 기능에 장애가 발생"하여야 한다. 즉,'교란'은 운영이 중단되지는 않더라도 부당한 정보처리결과를 야기하게 하는 경우를 비롯하여 정상적으로 운영되지 않는 것을 의미하고, '마비'는 주요정보통신기반시설이 작동을 멈추어 운영의 중단을 가져오는 것을, '파괴'는 주요정보통신기반시설에 손상을 가져오는 모든 경우를 의미한다.

90) 기획재정부, 법무부 등은 그 산하에 주요정보통신기반시설 관리기관을 갖고 있지는 않으나 예산의 확보 및 수사권 등이 주요정보통신기반시설의 보호체계에서 매우 중요한 의미를 갖고 있기 때문에 위원으로 구성되어 있다는 점을 고려한다면 "제외할 수 있다"는 방식의 재량규정이 바람직할 것이다.

2. 구성방법과 비상설기구의 문제점

대책본부의 구성은 대통령령으로 정하고, 대체적으로 미래창조과학부, 국가정보원, 수사기관의 공무원 등 유관기관 직원들로 구성된다. 즉, 이에 대한 협력체계를 살펴보면, 대책본부장은 관계 중앙행정기관의 장, 관리기관의 장 그리고 한국인터넷진흥원장에게 주요정보통신기반시설 침해사고의 대응을 위한 협력과 지원을 요청할 수 있으며, 협력과 지원을 요청받은 관계 행정기관의 장 등은 특별한 사유가 없는 한 이에 응하여야 한다(법 제15조 제4항).

정보통신기반침해사고대책본부는 주요정보통신기반시설에 대한 광범위한 침해사고가 발생한 경우, 정보통신기반보호위원회의 위원장이 한시적으로(응급대책, 기술지원 및 피해복구 등을 수행하기 위한 기간을 정하여) 설치할 수 있다. 대책본부를 상설화하고자 하면 별도의 조직이 구성되어 인력과 예산 등이 필요하고, 기존 조직과의 업무중복으로 인한 마찰이 우려된다는 이유로 비상설로 편성된 것이다.

그러나 최근 정보통신기반시설에 대한 중대한 침해사고가 수시로 발생하고 있으므로, 비상설조직으로 구성하여 운영하는 것이 바람직한 것인지에 대한 재검토가 필요할 것이다. 즉, 중대한 침해사고가 발생할 때마다 이에 대응하기 위하여 정보통신기반보호위원회 산하에 대책본부를 설치하고 기능별 실무반을 한시적 기구로 구성하는 것이 적절한지를 재검토하고 정보통신기반보호위원회의 법적 지위와 소속 등과 관련하여 사이버 안보 종합대책과의 연계성을 강화하는 방향을 모색하여야 할 것이다.

3. 구성 및 체계상의 문제

우리 현행법제에는 사이버 안보 및 정보보호와 관련된 규정이 산재하고 있고, 이로 말미암아 각 기관이 사이버 안보 및 정보보호와 관

련된 업무를 수행함에 있어 관할사항이 충돌하는 것으로 오인될 우려가 제기되고 있다. 침해사고 대책본부를 구성함에 있어서도 다양한 기관이 함께 참여하는 것은 이러한 오해를 확대시킬 위험성이 있다는 점에서 명확하게 그 기능 및 업무를 되짚어볼 필요가 있을 것이다.

우선, 안전행정부는 「전자정부법」과 「개인정보보호법」 등을 관장하고 있다. 즉, 전자에 의거하여 정보기술을 활용하여 행정기관 및 공공기관의 업무를 전자적으로 처리하여 행정업무를 효율적으로 수행하도록 하고, 후자에 따라서 공공분야와 민간부문을 아울러서 개인정보를 보호하는 업무를 담당하고 있다. 그리고 「재난 및 안전관리기본법」상 사회적 재난에 대처하기 위하여 중앙안전대책위원회에 사고대책본부가 설치되어 있으나, 앞에서 살펴본 바와 같이 재난관리체계와 정보통신기반보호체계는 구별하여야 하고, 주요정보통신기반에 대한 침해사고에 대한 대응에서 중요한 것은 피해확산방지, 침해자 검거, 복구조치로서 고도로 전문적이고 기술적인 사항이며 신속한 대응을 요구하므로 별도의 관리·보호체계에 의하도록 하고 있다.

그리고 미래창조과학부와 방송통신위원회는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 의거하여 “민간분야의 정보보호 정책 총괄, 민간분야의 사이버안전 정책 총괄 관련 제도·지침 수립, 사이버 안전 예방, 정보수집·분석·전파, 침해사고 긴급대응 등 민간부문 사이버 위협 대응” 등을 관장하고 있다.

이와 같이 관련 법령과 대통령 훈령 등을 분석해 보면 정보보호와 사이버 안보(전자적 침해행위로 말미암은 침해사고 대응)는 개념상 분리되어 있다. 안전행정부는 「정부조직법」, 「전자정부법」, 「개인정보보호법」 등에 의거하여 전자정부 및 정보보호에 관한 업무를 관리하지만, 침해사고에 대한 대응기능은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「국가사이버안전관리규정」 등에 의거하여 미래창조과학부와 국가정보원에서 담당하고 있는 것이다. 실제로 DDoS

침해사고 발생시 그에 대한 대응체계는 국가정보원(공공부문 및 총괄)을 중심으로 미래창조과학부(민간부문), 국방부(국방부문) 등이 부문별로 담당하고 있고, 안전행정부는 정부통합전산센터를 관리하는 기능을 담당할 뿐이다.

이에 대한 개선방안을 모색하기 위하여 주요국의 정보보호기반시설 보호체계를 비교법적으로 검토하여 볼 필요가 있을 것이다. 본 연구보고서에는 지면의 한계상 비교법적 연구는 진행하지 않을 것이다. 다만, 기존의 연구결과[91]를 참조하여 보면 주요국가에서는 사이버 안보의 총괄기관을 분명하게 정하여 권한과 책임을 부여하고, 중앙행정기관의 장 상호간 그리고 관리기관과의 유기적 협력관계를 구축하기 위한 실질적 대책을 마련하는 등 사이버 안보와 관련된 법제도를 지속적으로 정비하여 투명성과 효율성을 제고하고 있음을 알 수 있다.

Ⅲ. 정보공유・분석센터(법 제16조)

정보통신시스템은 금융・통신・운송・에너지 등 분야별로 시스템의 특성이 다르며, 이에 따라 보호대책이 상이할 수 있다. 미국을 중심으로 유럽, 일본 등 외국 정부는 각 분야별 정보통신시스템의 특성에 맞게 민간에서 자율적으로 전자적 침해행위에 대한 예방・대응시스템인 “정보공유분석센터(Information Sharing Analysis center : ISAC)”의 설립을 적극적으로 장려하고 지원하고 있다. 이는 각국 정부가 모든 주요정보통신기반시설의 침해행위를 파악하고 보호대책을 수립하기 곤란하다는 점을 인식하고 있기 때문이다.

우리 정부도 정보공유・분석센터(ISAC)의 설립을 활성화하기 위하여 설립 전 규제는 두지 않고 설립・운영에 따른 기술적 지원을 하되, 설립 후 정상적 운영을 위하여 필요한 규제를 가하는 것을 원칙

91) 이는 호서대학교 산학협력단, 『정보통신기반보호 강화 방안 마련』, 한국인터넷진흥원, 2013, 37~108쪽.

으로 하고 있다. 즉, 정보공유·분석센터 구축시 관할 중앙행정기관의 장에게 업무종사자의 인적사항 등 정보공유·분석센터의 구성·운영 등에 관한 세부적인 사항을 포함하여 조직의 개요를 통지하도록 하고 있는 것이다. 과거에는 설립 후 통보하도록 하는 사후통보제로 운영하였으나, 이제는 통지로 명칭이 변경되었다. 그리고 통지의무를 이행하지 않은 경우에는 그 의무를 담보하는 차원에서 과태료를 부과(제30조 제1항 2호)하도록 규정하고 있다.

이와 같이 법 제16조는 우리나라 정부가 각 분야별로 침해사고 발생 시 경보·대응, 취약점 및 침해요인에 대한 대응정보, 정보보호시스템 평가, 정보보호교육 및 훈련서비스 등을 제공하는 "정보공유분석센터"의 설립을 장려하고 지원하도록 규정하고 있다. 특히, "정보공유분석센터"에 제공되는 이용자의 침해사고와 관련된 정보는 법률규정, 법원의 명령 또는 영장에 의하지 않고는 누구도 요구할 수 없도록 하여 그 비밀성을 보장하고 있다.

정보공유·분석센터(ISAC)의 분야별로 누구나 자유로이 설립할 수 있으며, 업무종사자의 인적사항 등 대통령령이 정하는 구축·운영 등에 관련된 사항을 관계 중앙행정기관에게 통지하도록 하였고(법 제16조 제2항, 시행령 제24조), 업무수행현황에 대한 종합적인 파악 및 관리를 위하여 중앙행정기관의 장은 정보공유분석센터의 장으로부터 통지받은 사항을 다시 미래창조과학부 장관에게 통지하도록 규정하고 있다(법 제16조 제3항). 그리고 동 센터는 정보통신기반시설에 관한 취약점 및 침해사고 등 각 분야 시설의 비밀정보를 취급하므로, 각 중앙행정기관이 해당 분야의 "정보공유분석센터" 구축을 장려하면서 그에 대한 기술적 지원을 할 수 있다고 규정하고 있다(법 제16조 제4항).

또한, 정보공유·분석센터는 주요정보통신기반 관련 정보가 집결·교류되는 곳이므로, 이와 관련하여 침해사고가 발생하는 경우에는 그 피해에 따른 파급효과가 매우 심각할 것이므로 정보공유·분석센터를

엄격하게 관리할 필요성이 있다. 따라서 법 제27조 제4호는 정보공유분석센터의 관리·운영인력에 대하여 비밀준수의무를 부과하고, 법 제29조는 비밀을 누설한 자에 대하여 엄격한 처벌을 규정하고 있다.

여기에서 특기할만한 것은 정보공유·분석센터에 관한 규율체계를 분석해 보면 국가 또는 공공기관 부문이 아니라 금융·통신 등 분야의 민간부문 정보통신기반시설을 전제하고 관계 중앙행정기관과 미래창조과학부에 대한 규율만 존재한다는 것이다. 그리고 시행령 제24조 제1항에 따르면 정보공유분석센터의 장은 "미래창조과학부령이 정하는 정보공유·분석센터구축통지서"에 따라서 30일 이내에 각 중앙행정기관의 장에게 통지하도록 되어 있는데, 미래창조과학부령으로 통지서 양식을 정하고 다른 중앙행정기관의 장에게 통지하도록 하는 것이 체계상 적절한 것인지에 대하여는 재검토해 볼 필요가 있다.

제 3 절 정보통신기반시설에 대한 국가적 개입과 지원

Ⅰ. 주요정보통신기반시설의 보호지원(제7조)

1. 의 의

보호계획 및 보호대책에 대한 지원의 일환으로 주요정보통신기반시설 관리기관을 직접적으로 지원하기 위한 규정으로서 법 제7조(주요정보통신기반시설의 보호지원)와 제25조(정부의 기술적 지원) 등이 마련되어 있다. 이에 따르면 미래창조과학부장관과 국가정보원장 등 또는 대통령령이 정하는 전문기관에게 주요 정보통신기반보호에 관한 보호대책의 수립, 침해사고 예방 및 복구, 보호조치 명령·권고의 이행에 대한 기술적 지원을 수행하게 하고 있다.

과거 「정보통신기반보호법」은 기술적 지원을 할 수 있는 주체를 국가기관 또는 지방자치단체의 장인 관리기관으로 한정하고 있어 민간 정보통신기반시설 관리기관의 장은 기술적 지원을 요청할 수 없는 문제점이 있었다. 이에 따라 2007년 개정을 통하여 전문기관 등에 기술적 지원을 요청할 수 있는 주체를 국가기관 또는 지방자치단체의 장인 관리기관으로부터 모든 관리기관으로 확대하고, 요청할 수 있는 지원사항에 관계 중앙행정기관의 장이 명령·권고한 보호조치 이행을 추가하였다. 다수의 주요정보통신기반시설을 차지하고 있는 민간 주요정보통신기반시설에 대한 전문기관의 기술적 지원을 통하여 주요정보통신기반시설의 보호를 강화시키려는 개정의도가 있었던 것으로 보인다.

2. 관리기관의 요청에 의한 기술적 지원(제1항, 제2항 본문)

법 제7조에서 규정하고 있는 기술적 지원의 요건은 제1항에서 “관리기관의 장이...기술적 지원을 요청할 수 있다”는 것을 원칙으로 하고 있다. 그리고 제2항 본문은 “국가정보원장에게 우선적으로 지원을 요청하여야 하는” 경우와 대상을 명시하고 있다. 즉, 법 제7조 제1항은 관리기관의 장이 기술적 지원을 요청할 수 있는 권리를 규정하고 있고, 제7조 제2항은 관리기관의 장이 기술적 지원을 요청하여야 하는 의무를 규정한 것이다.

먼저 제1항을 살펴보면 관리기관의 장이 기술적 지원을 요청할 수 있는 요건으로 2가지 경우를 규정하고 있다. 첫째, 관리기관의 장이 (자체적으로) 필요하다고 인정하거나, 둘째 정보통신기반보호위원회의 위원장이 특정 국가기관 또는 지방자치단체의 주요정보통신기반시설 보호대책의 미흡으로 국가안보나 경제사회전반에 피해가 우려된다고 판단하여 그 보완을 명하는 경우이다. 즉, 관리기관이 자율적으로 판단하는 경우와 타율적으로 기술적 지원을 요청하는 경우로 나누어 볼 수 있다. 이와 관련하여 정보통신기반보호위원회 위원장이 ‘보완’을

명하는 경우 이외에 시행령 제9조의3 제2항에 따라서 미래창조과학부장관 또는 국정원장이 '개선권고'를 하는 경우에도 관리기관의 장이 기술적 지원을 요청하도록 하여야 한다는 견해가 제기될 수 있다.

그리고 기술적 지원을 수행하는 기관은 "미래창조과학부장관과 국가정보원장 등 또는 필요한 경우 대통령령이 정하는 전문기관의 장"으로 규정되어 있는데, 이들 상호간의 관계 내지 우선순위 그리고 관할의 구분이 법문상 명확하게 드러나지 않는다는 문제점이 있다. 또한 "대통령령이 정하는 전문기관"은 시행령 제12조에서 "주요정보통신기반시설 보호지원기관의 범위"라는 표제 하에 4개의 기관을 규정하고 있는데, 제2호 "정보공유·분석센터"와 제3호 "지식정보보안 컨설팅 전문업체"는 그 범위가 다소 불명확한 점이 있다.[92]

마지막으로 기술적 지원의 업무는 주요정보통신기반시설의 보호대책의 수립, 침해사고 예방 및 복구 그리고 제11조에 따른 보호조치 명령·권고의 이행으로 열거되어 있다. 따라서 기술적 지원의 범위는 한정적으로 규정되어 있다고 평가할 수 있으나, 이 업무를 수행하기 위하여 필요한 제반사항을 기술적으로 지원하기 위한 구체적인 사항은 법률해석에 의하여 매우 넓게 인정될 수 있는 여지가 있다.

그리고 제7조 제2항 본문에서 "국가안전보장에 중대한 영향을 미치는 다음 각 호의 주요정보통신기반시설에 대하여 관리기관의 장이... 기술적 지원을 요청하는 경우에는 국가정보원장에게 우선적으로 그 지원을 요청하여야 한다"고 규정하고 있다. 이에 해당하는 정보통신기반시설은 "1. 도로·철도·지하철·공항·항만 등 주요 교통시설, 2.

92) 정보공유분석센터는『정보통신기반보호법 시행령』별표 2 비고 제2호 및『정보통신기반보호법 시행규칙』제2조에 의거하여 마련된『취약점 분석·평가를 수행하는 정보공유·분석센터의 기준 및 기준심사에 관한 고시』(미래창조과학부고시 제2013-38호)에 따라서 승인심사를 받게 되는데, 그 요건으로 정보보호컨설팅 수행실적(고시 제8조)을 요구하고 있다. 그리고 정보공유분석센터와 지식정보보안 컨설팅 전문업체는 둘 다 미래창조과학부의 심사를 거쳐서 승인(지정)되고 있다. 따라서 이를 특별히 구별하여야 할 필요성이 있는지 의문이다.

전력, 가스, 석유 등 에너지・수자원 시설, 3. 방송중계・국가지도통신망 시설, 4. 원자력・국방과학・첨단방위산업관련 정부출연연구기관의 연구시설"을 명시하고 있는 바, 이에 해당하는 시설의 관리기관의 장은 국가정보원장에게 기술적 지원을 요청하여야 하는 의무를 부담하고 있는 것이다. 현실적으로 이 규정에 따른 요청의무를 이행하지 않는 경우에 제재수단이 없기 때문에 그 실효성을 확보하기 위한 규정(위반시 제재수단 또는 과태료 부과 등)을 규정하는 방안을 생각해 볼 수 있을 것이다.[93]

3. 국가정보원장의 직권에 의한 지원(제2항 단서)

제7조 제2항 단서에 따르면 "국가안전보장에 현저하고 급박한 위험이 있고, 관리기관의 장이 요청할 때까지 기다릴 경우 그 피해를 회복할 수 없을 때에는 국가정보원장은 관계중앙행정기관의 장과 협의하여 그 지원을 할 수 있다"고 규정하고 있다. 따라서 이는 관리기관의 장이 요청하지 않은 경우라도 긴박한 상황(국가안전보장에 현저하고 급박한 위험, 관리기관의 장이 요청할 때까지 기다릴 경우 그 피해를 회복할 수 없을 때)으로 인하여 국가정보원장의 직권(판단)에 의하여 지원을 할 수 있는 근거규정이라고 할 수 있다.

이 경우에도 국가정보원장은 관계 중앙행정기관의 장과 협의하는 사전적 절차를 반드시 거쳐야 하는 행정내부적 통제장치가 마련되어 있다.[94] 그러나 '협의'라는 절차는 '합의'와 달리 상대방의 의견을 구하고 논의를 거치기만 하면 되고, 의사의 합치에 이를 것을 요하는 것은 아니기 때문에 내부적 통제장치로서 불충분한 것이 아니냐는 비

93) 주요 정보통신기반시설 관리기관의 장이 국정원장에 대한 기술적 지원 요청의무를 해태하였다고 하여 국정원장이 과태료를 부과할 수 있는 권한을 인정하기 어려우므로 제재수단으로서 과태료 규정을 두는 것이 어렵다고 판단할 수도 있을 것이다. 이와 관련하여 『제6장 정보통신기반보호법령의 개선 및 그 기대효과』 참조.

94) 이에 대한 구체적 규율은 시행령을 통하여 마련하는 것이 필요할 것이다.

판이 제기될 수 있다. 그러나 제2항에 규정된 내용이 긴박한 상황적 요건임을 감안한다면 정당화될 수 있는 여지가 있을 것이다.

문제의 핵심은 "긴박한 상황에 대한 해석 및 판단을 누가 어떻게 할 것이냐"로 귀결될 것이다. 특히, '국가안전보장에 현저하고 급박한 위험'이 어느 정도의 국가긴급사태를 의미하는지 그리고 '관리기관의 장이 요청할 때까지 기다릴 경우 그 피해를 회복할 수 없을 때'는 어떻게 판단할 것인지에 대하여는 명확하고 구체적인 기준을 마련하여 적용하는 것이 매우 어려운 일이다.

따라서 이 문제는 지원을 하는 주체인 국가정보원장이 판단하여 기술적 지원 여부를 결정할 수밖에 없고, 이를 둘러싼 문제가 사법적 분쟁으로 비화될 가능성이 없다.[95] 결국 이에 대한 문제가 발생하면 법적 문제가 아니라 정치적 논쟁이 제기될 것이다. 따라서 이를 예방하기 위하여 법 제7조 제2항 단서의 국가정보원장이 직권으로 기술적 지원을 할 수 있는 권한은 그 발동요건에 대한 엄격한 해석에 의거하여 행사되어야 하고, 관계 중앙행정기관의 장과의 '협의'절차는 긴급사태가 발생한 상황에서 국가정보원장이 기술적 지원을 하는 필요성과 정당성에 대한 논증과 설득이 충분히 이뤄져야 한다는 요청으로 이해하고 그 취지에 맞도록 운영하여야 할 것이다.

---

95) 국가정보원장이 긴박한 상황이라고 판단하여 "1. 도로·철도·지하철·공항·항만 등 주요 교통시설, 2. 전력, 가스, 석유 등 에너지·수자원 시설, 3. 방송중계·국가지도통신망 시설, 4. 원자력·국방과학·첨단방위산업관련 정부출연연구기관의 연구시설"의 관리기관에 대하여 기술적 지원을 하는 경우에, 해당 관리기관의 장이 국가정보원의 기술적 지원조치에 대하여 위법성을 다투는 행정소송을 제기하는 것은 판단여지이론에 비추어볼 때 어려울 것이고, 관리기관이 갖는 헌법상 또는 법률상 권한을 침해하거나 침해할 현저한 우려가 인정되지 않으므로 권한쟁의심판을 청구할 수도 없으며, 기본권을 직접적으로 침해하는 것이 아니므로 헌법소원을 청구할 수 있는 가능성도 없는 것이다. 마지막으로 정보통신기반보호법이 헌법에 위반되는지 여부에 대한 논란이 제기될 수 있는데, 이는 보호지원의 요건 및 절차를 구체적으로 규정하고 있으므로 비례성의 원칙 또는 명확성 원칙 등에 위배된다고 보기도 어려울 것이다.

4. 기술적 지원의 한계(제3항)

이와 같이 주요정보통신기반시설에 대한 보호지원을 위하여 기술적 지원을 하는 경우에 있어서 “국가정보원장은 금융 정보통신기반시설 등 개인정보가 저장된 모든 정보통신기반시설에 대하여 기술적 지원을 수행하여서는 아니 된다”는 한계가 설정되어 있다. 이는 2007년 법을 개정하면서 기술적 지원을 요청하는 관리기관의 범위를 과거에는 국가기관 또는 지방자치단체의 장에서 한정하던 것을 민간 부문도 포함하여 모든 관리기관으로 확대하는 과정에서 개인정보보호를 위하여 국가정보원장은 개인정보가 저장된 모든 정보통신기반시설에 대하여 기술적 지원을 수행하지 못하도록 금지하는 규정이 함께 신설된 것이다.

그러나 최근 정보통신기반시설을 보호하기 위한 기술적 지원을 하는 과정에서 이 한계규정은 매우 심각한 장애물이 되고 있다. 왜냐하면 개인정보가 저장되지 않은 정보통신기반시설을 찾기 어려울 정도로 오늘날 정보통신망 혹은 시스템은 대부분 개인정보를 보유하고 있기 때문에 정보통신기반시설의 보호를 지원하기 위한 기술적 지원 자체를 원천적으로 차단하고 있는 동 규정으로 말미암아 기술적 지원이 불가능하게 되었기 때문이다.

이와 더불어 이 규정은 다음과 같은 해석상의 논리적 오류를 안고 있다. 우선, 국가정보원장으로 적용주체가 한정되어 있으므로 개인정보가 저장된 정보통신기반시설 관리기관의 장은 “미래창조과학부장관 또는 대통령령이 정하는 전문기관의 장”에 대하여 기술적 지원을 요청할 수 있고, 국정원장을 제외한 보호지원기관은 기술적 지원을 할 수 있다는 반대해석이 가능하다. 그러나 이들을 차별적으로 규율하는 합리적 사유를 찾기 어려우므로 평등원칙에 위반될 가능성이 높다. 즉, 기술적 지원을 수행하는 과정에서 개인정보가 유출될 위험이 있으므로 금융정보통신기반시설 등 개인정보가 저장된 모든 정보통신기

반시설에 대한 기술적 지원을 금지하여야 한다는 이유라면 유독 국가정보원만 제외하고, 다른 보호지원기관은 기술적 지원이 허용되는 것을 정당화할 수 없는 것이다.

그리고 앞서 살펴본 바와 같이 이는 개인정보보호에 절대적인 가치를 부여하고 있고, 원칙적으로 당사자가 자율적으로 정보통신망의 안정성을 확보하여야 하고, 주요정보통신기반시설의 경우에 예외적으로 국가가 개입하여 보호지원을 수행하도록 하되, 그 예외를 또 다시 설정하여 실제적으로 보호지원을 수행하지 못하도록 원천적으로 차단하는 규정을 둔 것이므로 체계적 정당성이 매우 의심스러운 것이다.

최근 2014년초 KB와 NH 등 금융기관의 개인정보유출사건 등으로 인하여 금융위원장이 지정하는 은행과 증권사에 대한 취약점 분석·평가 등 금융 정보통신기반시설에 대한 관리감독체계를 카드·보험사에 대하여도 확대하자는 논의와 6월 4일 지방선거를 하루 앞두고 KBS에서 출구조사 결과가 사전에 외부에 공개된 것이 해커의 소행이므로 방송사도 정보통신기반시설로 지정하여 외부의 전자적 침해행위로부터 보호하여야 한다는 논의 등을 종합하여 보면 현실적으로“개인정보가 저장된 정보통신기반시설에 대하여 기술적 지원”을 아예 차단하기는 어려울 것으로 보인다.[96] 특히, 검찰, 공정거래위원회, 국세청, 금융감독원의 금융거래정보요구권[97]과 비교하여 보면 국가기관으로서

96) 2014년 6월 24일 중앙일보 기사 “공인인증서 발급업체가 개인정보 유출” (http://article.joins.com/news/article/article.asp?total_id=15057956&cloc=olink|article|default, 2014년 10월 24일 최종방문) 참조. 이에 따르면 “주민등록번호 등 핵심 정보를 취급하는 공인인증서 발급 업체가 고객들의 개인정보 관리조차 제대로 못해 유출하는 사고가 발생하였고, 한국정보인증(KICA)에서 공인인증서를 발급받은 사용자 가운데 13명의 주민등록번호, 휴대전화 번호 등이 인터넷 포털 네이버에 수개월 간 노출됐던 것으로 확인됐다. 한국정보인증의 관계자에 따르면 인증서 발급 고객 중 정부의 공인전자메일 계정을 신청한 고객들의 정보를 처리하는 과정에서 에러가 발생해 암호화되지 않은 정보가 노출됐다”며 현재는 해당 웹문서를 삭제했고, 개인정보가 인터넷에 노출된 13명에 대해서는 손해배상을 하겠다고 밝혔다. 이에 대해 한국인터넷진흥원 관계자는 “전자서명법·정통망법 등 유관 법률에 따라 책임을 물을 방안을 미래부 등 소관부처와 협의중”이라고 한다.

금융정보와 개인정보에 접근할 수 있는 가능성이 허용된 기관들과 금지된 국가정보원 사이에 차별적으로 규율하는 합리적 사유가 있는지 의문이다.[98]

2001년 법 제정당시 국회 회의록을 분석하여 보면, 국가정보원이 기술적 지원을 이유로 과거 독재정권 시절의 불법적인 민간사찰을 할 수도 있다는 우려로 말미암아 국가안보를 위하여 국정원이 직권으로 기술적 지원을 할 수 있다는 제7조 제2항이 소위에서 추가되면서 이에 대한 대응책으로 제7조 제3항을 신설하여 "금융 정보통신기반시설 등 개인정보가 저장된 모든 정보통신기반시설"에 대하여 기술적 지원을 원천적으로 금지하는 규정을 신설하였음을 알 수 있다.

그러나 이제는 2001년 「정보통신기반보호법」 제정당시와는 사정이 달라졌고, 개인정보를 보호하기 위한 법체계가 상당히 정비되었다. 즉, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 지속적으로 개정되어 개인정보의 누출(법 제27조의3), 타인비밀의 침해·누설(법 제49조) 등을 처벌하는 조항이 신설되었고, 「개인정보보호법」은 2011년 3월 29일 제정되어 동년 9월 30일부터 시행되어 개인정보에 대한 강력한 보호체계가 마련되었다. 따라서 금융 정보통신기반시설 등 개인정보가 저장된 정보통신기반시설에 대하여도 '관리기관의 요청'이 있거나 '긴박한 상황'이 있는 경우에는 정보통신기반시설의 보호를 위한 기술적 지원을 수행할 수 있도록 하는 것이 합리적이다.

이와 관련하여 기술적 지원에 대한 절차적 정당성과 적법성을 확보할 수 있는 보완장치를 마련하여 기술적 지원이 가능하도록 허용하는 방안을 생각해 볼 수 있다. 첫째, "기술적 지원"의 개념을 보다 명확

97) 이에 대하여는 '독점규제 및 공정거래에 관한 법률' 제50조 제5항, '금융실명거래 및 비밀보장에 관한 법률' 제4조 제1항 제4호, 제2항 등 참조.

98) 이에 대하여는 오일석·김소정, "사이버 공격에 대한 전쟁법 적용의 한계와 효율적 대응방안", 「법학연구」 제17집 제2호, 인하대학교 법학연구소, 2014. 6, 119~161(148)쪽 참조.

하게 정의하면서 이는 주요정보통신기반시설의 보호를 위한 취지에서 이뤄지는 것임을 분명히 밝혀야 할 것이다. 이를 위하여 시행령에서 '기술적 지원을 할 수 있는 사항'을 구체적이고 명확하게 규정하는 방안을 고려해 볼 수 있는데, 정보통신기반시설의 보안시스템이 기술적 안전성을 확보하고 있는지 여부 또는 개인정보를 처리하는 과정에서 이를 암호화하여 외부에 유출되지 않도록 - 최신의 보안기술수준에 적합하게 - 보호하고 있는지 여부를 확인하는 방식 등 기술적 지원의 구체적 수단을 시행령에 열거적으로 규정함으로써, 이를 통하여 개인정보의 불법적인 수집・유출・활용 등에 대한 우려를 불식시킬 수 있을 것으로 기대된다.

그리고 이와 더불어 제27조(처벌규정)에 기술적 지원과정에서 획득한 정보(비밀)를 유통하거나 누설하는 행위를 처벌하는 규정을 신설하는 것도 고려해 볼 수 있을 것이다. 만약 국가정보원 직원, 미래창조과학부 공무원, 전문기관의 직원 등이 정보통신기반시설의 관리기관에 기술적 지원을 하는 과정에서 개인정보를 수집하여 이를 위법하게 유통시키거나 부당한 목적으로 사용하는 경우에는 - 전자서명법, 개인정보보호법 또는 정보통신망 이용촉진 및 정보보호 등에 관한 법률 - 보다 강력한 처벌을 하는 규정을 신설하는 방안이 가능할 것이다.

그러나 「개인정보보호법」 제6조에서 "개인정보 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다"고 규정하고 있고, 제15조(개인정보의 수집・이용), 제16조(개인정보의 수집 제한), 제17조(개인정보의 제공), 제18조(개인정보의 목적 외 이용・제공 제한), 제19조(개인정보를 제공받은 자의 이용・제공 제한) 등을 고려한다면 이에 대한 유사한 취지의 규정을 「정보통신기반보호법」에 도입하는 것은 합리적이라고 보기 어려울 것이다.[99] 그리고 이를 위반한 경우에 대한 과태료와 벌칙은 「개인정보보호

99) 이외에도 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제27조의3(개인정

법」 제71조와 제75조 등에 규정되어 있으므로 이에 따라서 처벌할 수 있으므로 「정보통신기반보호법」에 불법적인 개인정보의 수집 및 누출 등에 대한 처벌근거를 신설하고자 한다면 그에 대한 처벌을 별도로 규정할 필요성(가중처벌)이 먼저 논증되어야 할 것이다.

절차적 관점에서는 국가정보원이 개인정보가 저장된 정보통신기반 체계시설에 대하여 기술적 지원을 수행할 때 지원절차를 사전에 협의하고, 기술적 지원을 하는 과정에 해당 관리기관의 임원 또는 정보보호책임자(법 제5조 제4항)가 함께 입회하여 국가정보원 등이 해당 기관의 개인정보를 불법적으로 수집·유통하는 것은 아닌지 등을 확인하도록 하는 절차적 규정을 마련하는 방안도 고려할 수 있다.

만약 이와 같은 내부적 통제장치가 불충분하다면 외부적 통제장치로서 법원의 허가를 받도록 하는 방안을 생각해 볼 수 있을 것이다. 최근 검찰, 공정거래위원회, 국세청 등이 압수·수색을 하는 과정에서 자료제출명령 또는 영치를 할 때 임의제출과 관련하여 피조사자가 동의하지 않는 경우에 이를 증거로 삼을 수 없는 등의 문제가 자주 발생하고 있기 때문이다. 그러나 법원의 영장을 받도록 하는 이유는 신체의 자유, 주거의 자유, 통신의 자유 등이 제한되는 경우에 이에 대한 특별한 정당화의 필요하기 때문에 영장주의를 규정하고 있는 것인데, 주요정보통신기반시설에 대한 '기술적 지원'의 문제를 이와 동일한 쟁점으로 파악하는 것은 적절하다고 보기 어려울 것이다.

보 누출 등의 통지·신고)에 따르면 "정보통신서비스 제공자등은 개인정보의 분실·도난·누출 사실을 안 때에는 지체 없이 다음 각 호의 모든 사항을 해당 이용자에게 알리고 방송통신위원회에 신고하여야 한다." 이에 따른 통지사항은 "1. 누출등이 된 개인정보 항목, 2. 누출등이 발생한 시점, 3. 이용자가 취할 수 있는 조치, 4. 정보통신서비스 제공자등의 대응 조치, 5. 이용자가 상담 등을 접수할 수 있는 부서 및 연락처"이고 세부사항은 대통령령으로 정하며 위반시 3천만원 이하의 과태료가 부과된다(동법 제76조). 그리고 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제49조는 "누구든지 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하여서는 아니 된다"는 규정을 두고 있고, 이에 위반시 "5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다"는 벌칙규정이 마련되어 있다(동법 제71조).

이러한 쟁점을 종합적으로 고려하여 다음과 같은 법 제7조의 개정안을 다음과 같이 생각해 볼 수 있다. 제1안은 현행 정보통신기반보호법 제7조의 규율방식을 유지하면서 개인정보를 보호하는 내용을 제7조의2를 신설하여 현행법의 문제점을 보완하는 방식으로 입안하였다. 즉, 제7조는 관리기관이 보호지원을 요청할 수 있는 경우(제1항)와 의무적으로 요청하여야 하는 경우(제2항)를 나누어 규율하고, 기존의 제7조 3항은 삭제하며 제7조의2에서는 개인정보보호조치의 수립・시행 및 준수 그리고 불법적인 개인정보의 수집 등을 금지하는 명문규정을 두는 것이다.[100] 그리고 제2안은 기존의 규율체계를 유지하면서 제3항을 개정하여 "개인정보를 저장한 주요정보통신기반시설"에 대한 기술적 지원시 개인정보보호시책을 강구하여 시행하도록 하면서, 그 실효성을 확보하도록 주의를 기울이게 하는 규정을 두는 것이다.[101]

이러한 법제도의 정비와 아울러 주요정보통신기반보호법의 취지와 입법목적을 올바르게 실현하기 위하여는 보호지원 등을 실질화하여 정보통신기반시설의 안정적 운용을 보장하고, 각종 침해사고를 예방하여 사이버 보안수준을 제고함으로써 국민생활의 안정을 이루고 신뢰를 얻어야 할 것이다. 민주적 법치국가에서 법제도의 성공적인 운영은 국민의 참여와 신뢰를 바탕으로 하여 가능한 것이기 때문이다.

Ⅱ. 관리기관에 대한 지원(법 제25조)

1. 배경 및 주요내용

오늘날 정치・경제・사회 전반에 걸친 인터넷 확산과 주요 기간산업에 대한 ICT 기술 의존도가 심화됨에 따라서 주요정보통신기반시설로 지정될 필요성이 있는 기관(시설)이 증가하는 추세이다. 이를 위하

100) 이에 대하여는 오일석, "위험분배의 원칙에 입각한 정보통신기반보호체계의 개선방안", 「법학논집」, 이화여자대학교 법학연구소, 2014. 9, 293~327(319)쪽 참조.
101) 이에 대하여는 『제6장 정보통신기반보호법령의 개선 및 그 기대효과』 참조.

여 정부에서는 사이버 보안수준을 강화하기 위하여 정책적으로 주요정보통신기반시설 지정을 2017년까지 400여개로 그 대상을 확대하고자 추진하고 있으나, 관리기관의 입장에서는 보호체계로 편입될 경우 각종 의무를 부담하여야 하므로 지정에 소극적인 현실이다.[102]

정보통신기반을 보호를 위하여서는 규제성질의 의무보다는 지원과 자발적 참여 유도가 더 효율적이다. 현대행정법의 특징은 규제행정보다는 조종과 지원방식을 유도행정의 비중이 높아지고 있다는 점이다. 위와 같은 취지에서 법 제25조는 정보통신기반시설을 보호하기 위하여 공공기관과 민간단체 등을 불문하고 관리기관에 대하여 필요한 기술의 이전, 장비의 제공 등 그 밖의 필요한 지원을 할 수 있도록 규정하고 있다.

2. 문제점

그러나 이 규정을 자세히 검토하면 지원주체를 "정부"로 명시하고 재량적 성격의 선언적 규정이라는 점을 알 수 있다. 이로 말미암아 보호대책의 수립지원, 침해사고의 예방·복구, 보호조치의 이행 등을 위한 구체적 지원근거가 미약하여 관계 중앙행정기관(부처)에서는 예산확보가 곤란한 측면이 있을 것이다.[103] 그리고 주요정보통신기반시

102) 이와 관련하여 주요정보통신기반시설로 지정될 경우에는 취약점 분석·평가, 보호대책의 수립 등 인력·예산이 수반되는 법적 의무부담이 발생하고, 다른 사이버 보안을 위한 규제와 중복되고 확인점검을 받는 것이 업무의 간섭으로 인식되어 관리기관 측에서는 지정을 반대하고 있다. 2013년 공영방송사인 KBS는 노조를 중심으로 주요 정보통신기반시설로 지정되는 것을 적극 반대하였으며, 2011년 정유사 등 에너지 기업은 법 제7조 제2항에 규정된 매우 중요한 국가적 기반시설이라고 평가할 수 있는데 주요정보통신기반시설로 지정되지 못하였다.

103) 각 부처별로 정보통신기반보호법 제25조에 의거하여 주요정보통신기반시설을 보호하기 위한 예산요구서를 작성하여 신청하더라도 우선순위에 대한 판단에서 후순위로 밀리게 되어 1차적으로는 기획재정부 2차적으로는 국회에서 삭감되는 예가 적지 않았다. 예컨대 중앙행정기관 망분리 사업은 2005년부터 국가정보원에서 각 부처별로 자체적으로 추진하도록 보호대책의 이행을 권고하였으나, 2006~2007년 망분리사업예산을 배정받은 기관이 전무하였고, 결국 2008~2010년간 당시 행정안

설로 지정되었다 하더라도 보호대책의 수립을 위한 취약점 분석·평가, 정보보호기술을 사용한 제품 및 서비스의 보급, 전담인력 및 조직 보강 등을 위한 정부 차원의 실질적인 보호지원은 미흡하였던 것으로 평가된다. 예를 들어 2008년부터 2012년까지 5년간 안전행정부 소관 주요정보통신기반시설에 대한 취약점 분석·평가사업은 84건에 불과하였다. 따라서 정보통신기반시설로 지정되어 관리기관으로 되면 제공받을 수 있는 인센티브를 보다 구체적으로 명확하게 규정할 필요성이 있다. 위험분배의 원칙상 주요정보통신기반시설로 지정됨에 따라 부담하여야 하는 경제적 비용과 업무부담에 대한 적절한 보상이 이뤄져야 한다.

이와 관련하여 정부의 지원과 민간부문의 협력을 결합시키는 것이 중요할 것이다. 특히, 금융·통신 등 각 분야별 정보통신기반시설 보호를 위하여 정보보호기술의 교류 및 정보통신기반 침해사고에 대응하기 위한 민간단체의 자발적 움직임을 장려할 수 있을 것이다. 대상기관에 대한 지원 내용은 취약점 분석·평가에 관한 기술지원, 정보보호보험회 가입지원, 시스템 보안장비의 제공, 정보보호수준 인증마크제 도입 등을 들 수 있다.

그리고 이 내용을 규정한다면 법률보다는 시행령으로 규정하여 탄력적 대응이 가능하게 하여야 하는데, 미래창조과학부와 국가정보원 중에서 어디를 지원기관으로 정할 것인지? 민간부문과 공공기관을 나누어 보호지원체계도 이원화할 것인지? 만약 국가사이버보안기본정책에 의거하여 정책총괄기관을 국가정보원으로 일원화한다면 국가정보원이 국가재정법 제40조의 독립기관으로서 예산을 요구하고 배정받아 사용하고, 그 성과와 내역을 국회 정보위원회에서 결산받게 되는데, 국회 정보위원회가 R&D 예산 혹은 기술지원, 장비구입 등의 예산을

전부의 전자정부지원사업으로 일괄하여 추진한 사례가 있다. 이는 분화된 보호체계가 추진력을 갖기 위해서는 일정부분 통합적인 조정·총괄기능에 의한 보완이 필요함을 보여주는 중요한 사례로 평가할 수 있을 것이다.

심사하고 결산하는 것이 과연 합리적인 것인지 의문이다. 국가정보원의 업무의 특성을 고려하여 예산심의와 결산심사도 국회 정보위원회에서 비공개로 비밀리에 진행하는 것이 가능하고 필요하다는 논증이 필요할 것이다.

3. 개선방안

이와 같은 난제를 해결하기 위하여 관리기관 등에 대한 지원체계는 국가정보원보다는 중앙 행정기관(정부부처)에서 하는 것이 각 부처별로 이뤄지는 예산요구 및 기재부의 예산편성 그리고 국회의 예산심의 등에 있어서 합리적이고 예측가능한 경로에 의할 수 있다는 점에서 보다 수월할 것으로 보인다. 그리고 각 부처별로 지원사업을 시행하기 위한 예산편성을 요구하는 것보다는 일원화하여 지원예산을 분배받고 이를 사업시행자에게 재분배하는 것이 원활한 업무추진을 위해 가능하고 필요할 것이다. 따라서 주요정보통신기반시설의 관리기관에 대한 지원사업은 미래창조과학부가 주도하여 지원사업의 공고, 제안서 접수 및 사업시행과 예산집행 그리고 결산까지 제반 업무를 총괄하여 수행하도록 하는 것이 현실적이고 합리적인 개선방안이 될 수 있을 것이다.

이와 더불어 공공부문과 민간부문의 협력적 네트워크를 구축하기 위하여 정보통신기반보호위원회의 심의를 거쳐서 미래창조과학부와 국가정보원이 합의하여 지원사업을 수행하도록 하는 절차규정이 필요할 것이다. 그리고 그 실시결과(성과)를 정보통신기반보호위원회에 보고하도록 하여 범정부적 차원의 협력체계가 유기적으로 작동할 수 있도록 하는 것이 중요할 것으로 생각된다.

이외에도 법 제11조에 따른 관리기관의 장이 보호조치의 명령 또는 권고를 받게 된 경우에 이를 집행하기 위하여 상당한 비용을 부담하여야 할 수도 있는데 이를 국가적 차원에서 지원할 필요성이 제기될 수

도 있다. 특히, 보호조치 명령 또는 권고를 준수한 관리기관의 장은 정보통신기반시설의 보호를 위한 선관주의 의무를 다한 것으로 추정하는 규정을 마련하는 방안도 고려해 볼 수 있을 것이다.[104]

이외에도 주요정보통신기반시설에 대한 전자적 침해행위(침해사고)가 발생한 경우에 배상보험제도를 마련하는 방안도 생각해볼 수 있다. 국내외 보험사(AIG, LIG, 메리츠 등)에서는 개인정보유출 배상책임, 전자금융거래 배상책임보험 등 특정분야에 한정된 보험상품을 개발하여 시판중이다. 이들을 통합한 사이버 테러사고와 관련된 보험상품을 개발·운용하거나, 재보험시장을 통하여 책임범위를 한정하고 위험을 재분배하는 방안 그리고 현재 약 300여개의 정보통신기반시설을 관리하는 기관(민간사업자 포함)들을 회원으로 하는 공제조합을 조직하는 방안[105] 등을 고려해 볼 수 있을 것이다.

Ⅲ. 기술개발 및 국제협력

1. 기술개발(법 제24조)

정보통신기반을 보호하기 위한 실질적 요소인 정보보안기술을 개발할 수 있는 전문인력은 정보통신기반보호를 위하여 매우 중요하기 때문에, 기술개발의 촉진 및 장려 등을 위하여 기술개발 및 전문인력 양성에 관한 조항을 두었다. 정부는 정보통신기반시설을 보호하는 데

104) 선관주의 의무를 다한 것으로 추정하는 것은 피해자 쪽에서 관리기관의 고의 또는 과실로 말미암아 침해사고가 발생하였다는 것을 입증하지 못하는 한 면책되는 것으로 운용할 수 있는 입증책임의 완화 내지 경감에 대한 규정을 의미하게 된다. 즉, 피해자들이 관리기관의 고의·과실을 입증해야 하는 부담을 지게 된다.

105) 공제조합의 운영 및 설치방안에 대하여는 오일석, “위험분배의 관점에 기초한 정보통신기반보호법 개선 방안”, 「법학논집」, 이화여자대학교 법학연구소, 2014. 9, 293~327(313)쪽 참조 ; 이와 관련하여 초기에는 Super Fund와 같이 국가가 일부 출연하고 그 이후에는 회원(관리기관)들의 회비(수수료) 등을 결합하여 민관협력 방식의 사이버 보안활동을 전개해나가는 것이 가능할 것이다.

필요한 기술의 개발계획을 수립·시행하여야 하고, 정보보호 기술개발을 효율적으로 추진하기 위하여 필요한 때에는 관련 연구기관 또는 민간단체에 의하여 수행하게 할 수 있도록 하고 있으며, 정보보호와 관련된 연구기관 또는 민간단체가 연구개발(R&D) 사업을 수행하는데 소요되는 비용의 전부 또는 일부를 지원할 수 있도록 하였다. 이외에도 미래창조과학부장관이 정보통신기반보호를 위해 필요한 전문인력의 양성과 국민의 인식제고를 위하여 필요한 교육 및 홍보를 시행한다.

현재 정보통신기반시설을 보호하기 위하여 필요한 기술의 개발 및 전문인력 양성시책은 존재하는지 정확히 파악하기 어려운 점이 있다. 정부가 주어로 되어 있는데, 누가 시책을 강구하는 주체인지 명확하지 않다. 예산을 요구하기 위한 선언적 규정에 불과한 것일 가능성이 높다. 다만, 기술개발의 주체가 대체로 민간 보안기업이므로 현재로서는 주로 미래창조과학부가 될 가능성이 높을 것으로 보인다.[106]

106) 기사를 검색해 보면 2013년 7월 미래창조과학부와 한국인터넷진흥원(KISA)에서 '라온시큐어'라는 ICT 보안기관을 사이버 보안전문가로 양성하는 교육기관으로 지정했다는 기사가 발견되고, 2014년 2월 4일 미래창조과학부와 국방부가 과학기술 및 사이버 전문인력 양성과 활용에 대한 업무협약(MOU)을 체결하면서 이에 따라 국방부와 미래부는 국방과학분야 이공계 우수인재와 최정예 정보보호 전문인력의 양성, 해당분야 군 복무, 전역 후 관련 분야 취·창업을 지원하는 '학위/양성교육-군 복무-취·창업' 연계 프로그램을 통해 국방과학기술 발전 및 정보보호 역량강화와 더불어 국가 창조경제를 선도해 나갈 전문인력을 양성하고 활용하기 위해 협력하기로 하였다는 기사가 발견된다.. 한국형 탈피오트인 「과학기술전문사관」은 2014년부터 매년 20명 규모로 모집하여, 국방과학 관련 분야에 대한 교육을 포함한 학사과정을 이수하고, 졸업 후 장교로 임용하여 국방과학연구소(ADD) 연구인력 등으로 복무토록 하는 방안을 검토 중이고, 「사이버 전문인력」중 부사관·병은 금년에 소요인력 확정(매년 20여명 내외) 및 교육과정 개발을 진행할 예정이며, 2015년에 1기 교육생을 선발-양성하여 2016년부터 관련 부대 및 기관에서 군 복무를 하게 될 예정이라고 한다. 이와 더불어 장교급 「사이버 전문인력」은 고려대 '사이버국방학과' 졸업생(연 30명)이 2016년부터 임관할 예정이다. 이에 대하여는 2014년 2월 4일 정책브리핑 자료 "과학기술및사이버 전문인력 양성활용 MOU 체결" (http://www.korea.kr/policy/pressReleaseView.do?newsId=155942416&call_from=extlink, 2014년 10월 24일 최종방문) 참조.

문제의 핵심은 이에 대한 재정지원은 예산항목(계정)은 잡혀 있는 것인지? 보조금 사업으로 수행하는지 공공기관 등을 설립하여 출연금을 지급하는지 등에 대한 확인이 필요한데, 이에 대한 자료 접근이 어려운 실정이다. 이 부분은 향후 예산안 및 결산안(성과계획서 등 포함) 분석을 통하여 추가 연구가 필요할 것으로 보인다. 다만 이 규정을 보다 구체화할 수 있는 방법으로는 지원주체를 “정부”로 할 경우에는 포괄적인 선언규정에 그칠 가능성이 높으므로 기술개발을 지원하는 사업을 주도하는 기관을 구체적으로 명시하고, “예산의 범위 안에서 지원할 수 있다.” 혹은 “보조(출연)할 수 있다”고 명시하거나, 또는 방송통신발전기금의 지출대상으로 지원사업을 명시하는 방법 등을 고려해 볼 수 있다. 그리고 가능하면 이 부문은 기술개발 및 전문인력 양성 지원사업도 앞에서 살펴본 “관리기관 등에 대한 지원(법 제25조)”으로 통합하여 함께 규율하는 방안을 고려해 볼 필요가 있을 것이다.

2. 국제협력(법 제26조)

법 제26조는 정보통신기반시설의 보호에 관한 국제적 동향을 파악하고, 정보통신기반 보호를 위한 국제협력을 추진하게 하였다. 정보통신망(인터넷)의 특성상 정보통신기반시설은 국제적으로 상호연동되어 있는 네트워크에 개방되어 있고, 이는 국외로부터의 전자적 침해 행위로부터 취약한 상태이다. 대부분의 침해사고는 국외에 있는 IP를 통하여 전자적 공격이 이루어지고 있다. 따라서 효과적인 정보통신기반시설의 보호를 위하여 국제적 협력의 필요성이 반드시 요구된다.

제 5 장 정보통신기반보호법령의 개선 및 그 기대효과

본 연구보고서는 현대 사회에서 국가안보의 한 축을 담당하고 있는 사이버 안보의 중요한 비중을 차지하고 있는 정보통신기반시설에 대한 법제도의 문제점과 개선방안을 검토하고자 하였다. 이는 일반적인 정보통신망에 대한 보호체계와 달리 관리기관의 자율적인 보호대책의 수립과 아울러 국가적 보호와 지원이 광범위하게 이루어지고 있음을 알 수 있다. 그리고 이에 대한 전자적 침해행위로 인한 침해사고가 발생하고 난 이후의 사후적 대응체계보다는 사전적 예방대책을 중심으로 보호체계가 구성되어 있음을 발견할 수 있다.

그리고 연구자는 논의의 체계적 흐름 및 지면관계상 사후적 대응체계에 대한 형법 및 행정벌을 중심으로 한 처벌규정에 대한 검토는 논외로 하였으나, 이에 대하여는 향후 별도로 연구를 진행할 수 있는 기회를 가질 수 있기를 희망해 본다. 또한 금번 선행연구를 통해 제기된 문제점과 지면의 제약상 다루지 못한 다른 쟁점들을 분석하여 종합적인 정보통신기반보호법의 개정안을 도출하는 것이 바람직할 것이다. 이에 본 연구보고서의 결론은 본문에서 정보통신기반보호법령을 검토한 결과 식별된 문제점과 이에 대한 개선방안을 종합적으로 정리하는 것으로서 갈음하고자 한다.

주요정보통신기반시설을 지정 또는 지정 취소를 하고자 하는 경우에 위원회의 심의를 받아야 하는데「행정절차법」제22조의 취지를 고려하여 관리기관의 장을 출석하게 하여 의견을 들을 수 있다는 법 제8조 제5항을 의무적으로 규정하는 것이 보다 바람직할 것이다.

현 행	개 정 안
제 8 조(주요정보통신기반시설의 지정 등) ⑤ 중앙행정기관의 장이 제1항 및 제3항의 규정에 의하여 지정 또는 지정 취소를 하고자 하는 경우에는 위원회의 심의를 받아야 한다. 이 경우 위원회는 제1항 및 제3항의 규정에 의하여 지정 또는 지정취소의 대상이 되는 관리기관의 장을 위원회에 출석하게 하여 그 의견을 들을 수 있다.	**제 8 조(주요정보통신기반시설의 지정 등)** ⑤ 중앙행정기관의 장이 제1항 및 제3항의 규정에 의하여 지정 또는 지정 취소를 하고자 하는 경우에는 위원회의 심의를 받아야 한다. 이 경우 위원회는 제1항 및 제3항의 규정에 의하여 지정 또는 지정취소의 대상이 되는 관리기관의 장을 위원회에 출석하게 하여 그 의견을 들어야 하고, 불가피한 경우에는 의견을 서면으로 제출할 수 있다.

선택과 집중을 위하여 정보통신기반시설을 1급과 2급으로 구분하여 지정하는 방안은 다음과 같이 법률을 개정하고, 시행령 차원에서 구체적인 구별기준과 유형 및 이에 해당하는 시설을 지정(취소)하는 절차를 규율하는 방안을 생각해 볼 수 있다.

현 행	개 정 안
제 8 조(주요정보통신기반시설의 지정 등) ⑦ 주요정보통신기반시설의 지정 및 지정취소 등에 관하여 필요한 사항은 이를 대통령령으로 정한다.	**제 8 조(주요정보통신기반시설의 지정 등)** ⑦ 주요정보통신기반시설은 제1항의 요건을 고려하여 1급과 2급으로 나누어 구분하며, 구체적인 구별기준, 유형 및 지정 및 지정취소 등에 관하여 필요한 사항은 이를 대통령령으로 정한다.

법 제8조의2와 관련하여 지정권고의 주체에 대한 규율의 통일성을 위하여 시행령의 내용이 더욱 규율영역에 적합하고 합리적이므로 법

률의 표현을 정비하기 위하여 개정할 필요가 있을 것이다. 그리고 이와 관련하여 지정취소를 권고할 수 있는 내용을 함께 규정하는 것이 필요하다면 다음과 같이 개정할 수 있다.

현 행	개 정 안
제 8 조의2(주요정보통신기반시설의 지정권고) ① 미래창조과학부장관과 국가정보원장등은 특정한 정보통신기반시설을 주요정보통신기반시설로 지정할 필요가 있다고 판단되는 경우에는 중앙행정기관의 장에게 해당 정보통신기반시설을 주요정보통신기반시설로 지정하도록 권고할 수 있다.	**제 8 조의2(주요정보통신기반시설의 지정 또는 지정취소의 권고)** ① 미래창조과학부장관과 국가정보원장은 특정한 정보통신기반시설을 주요정보통신기반시설로 지정하거나 그 지정을 취소할 필요가 있다고 판단되는 경우에는 중앙행정기관의 장에게 해당 정보통신기반시설을 주요정보통신기반시설로 지정 또는 지정취소하도록 권고할 수 있다.
② 미래창조과학부장관과 국가정보원장등은 제1항에 따른 권고를 위하여 필요한 경우에는 중앙행정기관의 장에게 해당 정보통신기반시설에 관한 자료를 요청할 수 있다.	② 미래창조과학부장관과 국가정보원장은 제1항에 따른 권고를 위하여 필요한 경우에는 중앙행정기관의 장에게 해당 정보통신기반시설에 관한 자료를 요청할 수 있다.
③ 제1항에 따른 주요정보통신기반시설의 지정 권고 절차, 그 밖에 필요한 사항은 대통령령으로 정한다.	③ 제1항에 따른 주요정보통신기반시설의 지정 또는 지정취소의 권고 절차, 그 밖에 필요한 사항은 대통령령으로 정한다.

명확성의 원칙에 비추어 볼 때 취약점 분석·평가기관에 대한 규율의 일관성과 통일성을 확보하기 위하여 법 제9조 제3항은 다음과 같이 개정하는 것이 바람직할 것이다.

현 행	개 정 안
제 9 조(취약점의 분석・평가) ③ 관리기관의 장은 제1항의 규정에 의하여 취약점을 분석・평가하고자 하는 경우에는 다음 각호의 1에 해당하는 기관으로 하여금 소관 주요정보통신기반시설의 취약점을 분석・평가하게 할 수 있다. 다만, 이 경우 제2항의 규정에 의한 전담반을 구성하지 아니할 수 있다. 1.「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제52조의 규정에 의한 한국인터넷진흥원(이하 "인터넷진흥원"이라 한다) 2. 제16조의 규정에 의한 정보공유・분석센터(대통령령이 정하는 기준을 충족하는 정보공유・분석센터에 한한다) 3.「정보통신산업 진흥법」제33조에 따라 지정된 지식정보보안 컨설팅전문업체 4.「정부출연연구기관 등의 설립・운영 및 육성에 관한 법률」제8조의 규정에 의한 한국전자통신연구원	**제 9 조(취약점의 분석・평가)** ③ 관리기관의 장은 제1항의 규정에 의하여 취약점을 분석・평가하고자 하는 경우에는 다음 각호의 1에 해당하는 기관으로 하여금 소관 주요정보통신기반시설의 취약점을 분석・평가하게 할 수 있다. 다만, 이 경우 제2항의 규정에 의한 전담반을 구성하지 아니할 수 있다. 1.「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제52조의 규정에 의한 한국인터넷진흥원(이하 "인터넷진흥원"이라 한다) 2. 제16조의 규정에 의한 정보공유・분석센터(대통령령이 정하는 기준을 충족하는 정보공유・분석센터에 한한다) 3.「정보통신산업 진흥법」제33조에 따라 지정된 지식정보보안 컨설팅전문업체 4.「정부출연연구기관 등의 설립・운영 및 육성에 관한 법률」제8조의 규정에 의한 한국전자통신연구원<u>의 국가보안기술 연구・개발을 전담하는 부설연구소</u>

그리고 보호대책 이행여부 확인 결과 보완이 필요하다고 판단되는 관리기관에 대해서 개선을 권고하는 내용은 동법 시행령 제9조의3 제2항에 규정되어 있는데, 이는 법 제5조의2 제3항의 규율내용과 조화롭게 운용하기 위하여 다음과 같이 개정방안을 생각해 볼 수 있다.

이에 따르면 기존 시행령 제9조의3 제2항에 규정된 방식 - 미래창조과학부 장관과 국가정보원장 등이 직접 관리기관에 대하여 개선권고를 하는 것 - 을 지양하고, 중앙행정기관의 장을 통하여 공공부문인 경우에는 개선명령을 내리고, 민간부문인 경우에는 개선권고를 하는 것이 보다 적절할 것이다. 그리고 “정당한 사유가 없는 한 이에 따라야 한다”는 규정을 추가하여 개선권고의 실효성을 확보하고자 하였다.

현 행	개 정 안
제 5 조의2(주요정보통신기반시설 보호대책 이행 여부의 확인) ③ 미래창조과학부장관과 국가정보원장등은 제1항에 따라 확인한 주요정보통신기반시설보호대책의 이행 여부를 관계중앙행정기관의 장에게 통보할 수 있다.	**제 5 조의2(주요정보통신기반시설 보호대책 이행 여부의 확인)** ③ 미래창조과학부장관과 국가정보원장등은 제1항에 따라 확인한 주요정보통신기반시설보호대책의 이행 여부를 관계중앙행정기관의 장에게 통보할 수 있고, 그 확인 결과 보완이 필요한 관리기관에 대하여 개선명령 또는 권고하도록 할 수 있다. 이 경우에 관리기관은 정당한 사유가 없는 한 이에 따라야 한다.

이에 따라 시행령 제9조의3 제2항에 규정된 개선권고는 법 제5조의2 제3항에 규율하는 대신 삭제하고, 제4항에서 공공과 민간부문의 상호간 정보공유를 통하여 유기적 협력체계를 구축할 수 있는 근거규정이 마련되어 있는 바, 국가기밀에 해당하는 경우에는 정보공개의 대상에서 제외할 수 있는 근거를 함께 규율하는 것이 합리적일 것이므로 다음과 같은 개정안을 생각해 볼 수 있을 것이다.

현 행	개 정 안
제 9 조의3(주요정보통신기반시설 보호대책 이행 여부 확인 결과 보고 등) ② 미래창조과학부장관, 국가정보원장 및 국방부장관은 법 제5조의2에 따른 주요정보통신기반시설보호대책의 이행 여부 확인 결과 보완이 필요하다고 판단되는 관리기관에 대해서는 개선을 권고할 수 있다.	**제 9 조의3(주요정보통신기반시설 보호대책 이행 여부 확인 결과 보고 등)** ② (삭제)
④ 미래창조과학부장관과 국가정보원장은 법 제7조에 따른 주요정보통신기반시설의 보호지원을 효율적으로 하기 위하여 주요정보통신기반시설보호대책의 이행 여부 확인 결과를 서로 제공하여야 한다.	④ 미래창조과학부장관과 국가정보원장은 법 제7조에 따른 주요정보통신기반시설의 보호지원을 효율적으로 하기 위하여 주요정보통신기반시설보호대책의 이행 여부 확인 결과를 서로 제공하여야 한다. 단, 국가기밀에 해당하는 경우에는 공개하지 아니할 수 있다.

관계 중앙행정기관의 장은 관리기관에서 수립·제출한 주요정보통신기반시설보호대책을 종합·조정하여 소관분야에 대한 주요정보통신기반시설보호계획을 수립·시행하여야 한다(법 제6조 제1항). 이는 각 관리기관의 장이 취약점 분석·평가(법 제9조) 결과에 따라 보호대책을 수립하고 이를 관계중앙행정기관의 장에게 제출(법 제5조)한 것을 종합·조정하는 것이다. 그런데 보호대책을 제출하는 것은 제5조 제2항뿐만 아니라 제5조 제3항에 의거하여 제출되는 경우도 있으므로 다음과 같이 개정하여야 규율의 흠결이 없도록 개선할 수 있을 것이다.

현 행	개 정 안
제 6 조(주요정보통신기반시설보호계획의 수립 등) ① 관계중앙행정기관의 장은 제5조 제2항의 규정에 의하여 제출받은 주요정보통신기반시설보호대책을 종합·조정하여 소관분야에 대한 주요정보통신기반시설에 관한 보호계획(이하 "주요정보통신기반시설보호계획"이라 한다)을 수립·시행하여야 한다.	**제 6 조(주요정보통신기반시설보호계획의 수립 등)** ① 관계 중앙행정기관의 장은 제5조 제2항 <u>및 제3항</u>의 규정에 의하여 제출받은 주요정보통신기반시설보호대책을 종합·조정하여 소관분야에 대한 주요정보통신기반시설에 관한 보호계획(이하 "주요정보통신기반시설보호계획"이라 한다)을 수립·시행하여야 한다.

보호계획의 수립일정의 적정성에 대한 검토는 앞에서 언급한 개요 수준에서 정리하고, 이를 수정하기 위하여는 법 제5조 제1항, 제6조 제2항과 4항 그리고 시행령 제8조, 10조 제1~3항 등을 전면적으로 개정하여야 한다는 점만을 언급하고 넘어가고자 한다.

정보통신기반보호위원회의 조직과 구성방식에 대하여는 사이버안보 종합대책과의 연계성을 강화하고 규율의 간결성과 명확성 등을 위하여 다음과 같은 개정안을 생각해 볼 수 있을 것이다.

현 행	개 정 안
시행령 제 2 조(정보통신기반보호위원회의 위원) 「정보통신기반 보호법」(이하 "법"이라 한다) 제3조제3항에서 "대통령령이 정하는 중앙행정기관의 차관급 공무원"이란 다음 각 호의 사람을 말한다. 이 경우 차관급 공무원이 2명 이상인 기	시행령 제 2 조(정보통신기반보호위원회의 위원) 「정보통신기반 보호법」(이하 "법"이라 한다) 제3조제3항에서 "대통령령이 정하는 중앙행정기관의 차관급 공무원"이란 다음 각 호의 사람을 말한다. 이 경우 차관급 공무원이 2명 이상인 기

현 행	개 정 안
관은 해당 기관의 장이 지정하는 사람을 말한다. 1. 기획재정부차관 2. 미래창조과학부차관 3. 외교부차관 4. 법무부차관 5. 국방부차관 6. 안전행정부차관 7. 산업통상자원부차관 8. 보건복지부차관 9. 고용노동부차관 10. 국토교통부차관 11. 해양수산부차관 12. 국가정보원 차장 13. 금융위원회 부위원장 14. 방송통신위원회 상임위원	관은 해당 기관의 장이 지정하는 사람을 말한다. 1. 정부조직법상 각 부처의 차관 (단, 주요정보통신기반시설을 관리·감독하지 않는 중앙행정기관은 제외할 수 있다) 2. 국가정보원 차장 3. 금융위원회 부위원장 4. 방송통신위원회 상임위원

법 제7조(주요정보통신기반시설에 대한 보호지원)에 대한 문제점과 개선의 필요성은 이미 본론에서 상세히 논증하였다. 개인정보가 저장된 주요정보통신기반시설에 대한 보호지원을 원천적으로 차단하는 것은 불합리하므로, 개인정보를 보호하면서 보호지원을 실시할 수 있는 법제도적 개선방안을 마련하고 이를 위반할 시에는 「개인정보보호법」과 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 도입된 규정들에 의거하여 처벌된다는 점을 명확히 함으로써 개인정보가 저장된 주요정보통신기반시설에 대하여도 국가적 차원의 보호지원이 원활하게 이뤄질 수 있도록 하여야 할 것이다.

(1안) 개인정보보호에 관한 규율을 별도의 조문(법 제7조의2)으로 신설하여 분리하여 규율하는 방안

현 행	개 정 안
제 7 조(주요정보통신기반시설의 보호지원) ① 관리기관의 장이 필요하다고 인정하거나 위원회의 위원장이 특정 관리기관의 주요정보통신기반시설보호대책의 미흡으로 국가안전보장이나 경제사회전반에 피해가 우려된다고 판단하여 그 보완을 명하는 경우 해당 관리기관의 장은 미래창조과학부장관과 국가정보원장등 또는 필요한 경우 대통령령이 정하는 전문기관의 장에게 다음 각 호의 업무에 대한 기술적 지원을 요청할 수 있다. 1. 주요정보통신기반시설보호대책의 수립 2. 주요정보통신기반시설의 침해사고 예방 및 복구 3. 제11조에 따른 보호조치 명령·권고의 이행 ② 국가안전보장에 중대한 영향을 미치는 다음 각 호의 주요정보통신기반시설에 대한 관리기관의 장이 제1항에 따라 기술적 지원을 요청하는 경우 국가정보원장에게 우선적으로 그 지원을 요청하여야 한다. 다만, 국가안전보장에 현저하고 급박한 위험이 있	**제 7 조(주요정보통신기반시설의 보호지원)** ① 관리기관의 장은 필요하다고 인정하거나 위원회의 위원장이 특정 관리기관의 주요정보통신기반시설보호대책의 미흡으로 국가안전보장이나 경제사회전반에 피해가 우려된다고 판단하여 그 보완을 명하는 경우 미래창조과학부장관, 국가정보원장 또는 필요한 경우 대통령령이 정하는 전문기관의 장에게 다음 각 호의 업무에 대한 기술적 지원을 요청할 수 있다. 다만, 관리기관의 장이 국가정보원장에 대하여 기술적 지원을 요청하는 경우에는 관계 중앙행정기관의 장의 승인을 받아야 한다. 1. 주요정보통신기반시설보호대책의 수립 2. 주요정보통신기반시설의 침해사고 예방 3. 주요정보통신기반시설의 침해사고 복구 4. 제11조에 따른 보호조치 명령·권고의 이행 ② 국가안전보장에 중대한 영향을 미치는 다음 각 호의 주요정보통신기반시설에 대한 관리기관의 장이 제1항에 따라 기술적 지원을 요청

현 행	개 정 안
고, 관리기관의 장이 요청할 때까지 기다릴 경우 그 피해를 회복할 수 없을 때에는 국가정보원장은 관계중앙행정기관의 장과 협의하여 그 지원을 할 수 있다. 1. 도로・철도・지하철・공항・항만 등 주요 교통시설 2. 전력, 가스, 석유 등 에너지・수자원 시설 3. 방송중계・국가지도통신망 시설 4. 원자력・국방과학・첨단방위산업관련 정부출연연구기관의 연구시설 ③ 국가정보원장은 제1항 및 제2항에 불구하고 금융 정보통신기반시설 등 개인정보가 저장된 모든 정보통신기반시설에 대하여 기술적 지원을 수행하여서는 아니된다.	하는 경우 국가정보원장에게 우선적으로 그 지원을 요청하여야 한다. 다만, 국가안전보장에 현저하고 급박한 위험이 있고, 관리기관의 장이 요청할 때까지 기다릴 경우 그 피해를 회복할 수 없을 때에는 국가정보원장은 관계 중앙행정기관의 장과 협의하여 그 지원을 할 수 있다. 1. 도로・철도・지하철・공항・항만 등 주요 교통시설 2. 전력, 가스, 석유 등 에너지・수자원 시설 3. 방송중계・국가지도통신망 시설 4. 원자력・국방과학・첨단방위산업관련 정부출연연구기관의 연구시설 **제 7 조의2(주요정보통신기반시설의 보호지원과 개인정보보호)** ① 미래창조과학부장관과 국가정보원장은 개인정보가 저장된 모든 주요정보통신기반시스템에 대한 기술적 지원을 제공하는 경우 해당 개인정보를 보호하기 위한 모든 조치를 강구하여야 한다. ② 대통령령이 정하는 전문기관의 장이 기술적 지원을 하는 경우에도 미래창조과학부 장관 과 국가정보원장이 협의하여 고시하는 개인정

현 행	개 정 안
	보보호조치를 준수하여야 한다. ③ 기술적 지원을 수행하는 모든 기관(직원 포함)은 개인정보를 불법적으로 수집・활용・유출하여서는 아니 된다.

(2안) 기존의 규정과 유사하게 규율하면서 개인정보가 저장된 시설에 대한 보호지원을 원천적으로 차단한 규정은 삭제하고 개인정보의 불법수집・활용・유출 등의 행위양태를 금지시키는 개정방안

현 행	개 정 안
법 제 7 조(주요정보통신기반시설의 보호지원) ① 관리기관의 장이 필요하다고 인정하거나 위원회의 위원장이 특정 관리기관의 주요정보통신기반시설보호대책의 미흡으로 국가안전보장이나 경제사회전반에 피해가 우려된다고 판단하여 그 보완을 명하는 경우 해당 관리기관의 장은 미래창조과학부장관과 국가정보원장등 또는 필요한 경우 대통령령이 정하는 전문기관의 장에게 다음 각 호의 업무에 대한 기술적 지원을 요청할 수 있다. 1. 주요정보통신기반시설보호대책의 수립 2. 주요정보통신기반시설의 침해사고 예방 및 복구 3. 제11조에 따른 보호조치 명령・	**법 제 7 조(주요정보통신기반시설의 보호지원)** ① 관리기관의 장이 필요하다고 인정하거나 위원회의 위원장이 특정 관리기관의 주요정보통신기반시설보호대책의 미흡으로 국가안전보장이나 경제사회전반에 피해가 우려된다고 판단하여 그 보완을 명하는 경우 해당 관리기관의 장은 미래창조과학부장관과 국가정보원장등 또는 필요한 경우 대통령령이 정하는 전문기관의 장에게 다음 각 호의 업무에 대한 기술적 지원을 요청할 수 있다. 1. 주요정보통신기반시설보호대책의 수립 2. 주요정보통신기반시설의 침해사고 예방 및 복구 3. 제11조에 따른 보호조치 명령・

현 행	개 정 안
권고의 이행 ② 국가안전보장에 중대한 영향을 미치는 다음 각 호의 주요정보통신기반시설에 대한 관리기관의 장이 제1항에 따라 기술적 지원을 요청하는 경우 국가정보원장에게 우선적으로 그 지원을 요청하여야 한다. 다만, 국가안전보장에 현저하고 급박한 위험이 있고, 관리기관의 장이 요청할 때까지 기다릴 경우 그 피해를 회복할 수 없을 때에는 국가정보원장은 관계중앙행정기관의 장과 협의하여 그 지원을 할 수 있다. 1. 도로·철도·지하철·공항·항만 등 주요 교통시설 2. 전력, 가스, 석유 등 에너지·수자원 시설 3. 방송중계·국가지도통신망 시설 4. 원자력·국방과학·첨단방위산업관련 정부출연연구기관의 연구시설 ③ 국가정보원장은 제1항 및 제2항에 불구하고 금융 정보통신기반시설 등 개인정보가 저장된 모든 정보통신기반시설에 대하여 기술적 지원을 수행하여서는 아니된다.	권고의 이행 ② 국가안전보장에 중대한 영향을 미치는 다음 각 호의 주요정보통신기반시설에 대한 관리기관의 장이 제1항에 따라 기술적 지원을 요청하는 경우 국가정보원장에게 그 지원을 요청하여야 한다. 다만, 국가안전보장에 현저하고 급박한 위험이 있고, 관리기관의 장이 요청할 때까지 기다릴 경우 그 피해를 회복할 수 없을 때에는 국가정보원장은 관계중앙행정기관의 장과 협의하여 그 지원을 할 수 있다. 1. 도로·철도·지하철·공항·항만 등 주요 교통시설 2. 전력, 가스, 석유 등 에너지·수자원 시설 3. 방송중계·국가지도통신망 시설 4. 원자력·국방과학·첨단방위산업관련 정부출연연구기관의 연구시설 ③ 제1항 및 제2항에 따라서 기술적 지원을 수행하는 모든 기관(직원 포함)은 개인정보를 불법적으로 수집·활용·유출하여서는 아니 된다.

그리고 보호지원의 실효성을 확보하기 위하여 법 제7조 제2항에 규정된 보호지원을 요청하여야 하는 의무를 위반할 경우에 과태료를 부과할 수 있는 근거규정을 두는 것이 요청될 수 있다. 다만, 국가정보원장은 과태료 부과권자가 될 수 없으므로 이에 대하여는 미래창조과학부장관이 과태료를 위탁하여 징수하도록 하는 것이 필요할 것이다.

현 행	개 정 안
제30조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자는 1천만원 이하의 과태료에처한다. 1. 제11조에 따른 보호조치 명령을 위반한 자 2. 제16조제2항의 규정에 의한 통지를 하지 아니한 자	**제30조(과태료)** ① 다음 각 호의 어느 하나에 해당하는 자는 1천만원 이하의 과태료에처한다. 1. 제7조 제2항에 따른 보호지원 요청의무를 위반한 자 2. 제11조에 따른 보호조치 명령을 위반한 자 3. 제16조제2항의 규정에 의한 통지를 하지 아니한 자
② 제1항의 규정에 의한 과태료는 대통령령이 정하는 바에 따라 관계중앙행정기관의 장 또는 미래창조과학부장관(이하 “부과권자”라 한다)이 부과·징수한다.	② 제1항의 규정에 의한 과태료는 대통령령이 정하는 바에 따라 관계중앙행정기관의 장 또는 미래창조과학부장관(이하 “부과권자”라 한다)이 부과·징수한다. 단, 제1항제1호의 경우에는 미래창조과학부장관이 국가정보원장을 대신하여 부과·징수한다.

법 제25조에 규정된 관리기관에 대한 지원은 다음과 같이 지원주체를 명확히 하고 대상사업을 구체화할 필요가 있을 것이다. 그리고 법 제24조에 규정된 기술개발 및 전문인력 양성에 관한 시책을 강구하고 관련 비용을 지원하는 내용을 함께 규율하는 것이 가능할 것이므로 다음과 같이 개정안을 마련하는 것이 가능할 것이다.

현 행	개 정 안
제24조(기술개발 등) ① 정부는 정보통신기반시설을 보호하기 위하여 필요한 기술의 개발 및 전문인력 양성에 관한 시책을 강구할 수 있다. ② 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. **제25조(관리기관에 대한 지원)** 정부는 관리기관에 대하여 주요정보통신기반시설을 보호하기 위하여 필요한 기술의 이전, 장비의 제공 그 밖의 필요한 지원을 할 수 있다.	**제24조(관리기관에 대한 지원)** ① 중앙 행정기관의 장은 관리기관에 대하여 주요정보통신기반시설을 보호하기 위하여 사업을 수행하기 위하여 필요한 기술의 이전, 장비의 제공 그 밖의 필요한 기술적·행정적·재정적 지원을 할 수 있다. ② 미래창조과학부 장관은 주요정보통신기반시설의 보호를 위하여 필요한 사업(이하 '기반보호지원사업'이라 한다)이 있을 경우에 위원회의 심의를 받은 후 관계 중앙행정기관의 장에게 관리기관을 지원하도록 권고할 수 있다. 이를 위하여 기반보호지원사업의 공고, 제안서 접수 및 사업시행과 예산요구, 집행 및 결산 등의 업무는 미래창조과학부 장관이 수행한다. ③ 미래창조과학부 장관은 국가정보원장과 합의하여 기반보호지원사업의 주요내용, 시행방법 등을 정하고 정보통신기반보호위원회에 보고한다. ④ 기반보호지원사업이 종료된 이후 미래창조과학부 장관과 국가정보원장등은 각 소관사무별로 사업시행의 성과를 정리하여 정보통신기반보호위원회에 보고한다. ⑤ 기반보호지원사업의 선정·관리 등 필요한 사항은 대통령령으로 정한다.

현 행	개 정 안
	시행령 제24조의2(기반보호지원사업의 선정 등) ① 법 제24조 제3항에서 정하고 있는 “기반보호지원사업”은 다음 각 호를 의미한다. 1. 제9조에 따른 취약점 분석·평가 2. 제5조에 따른 보호대책의 수립 3. 제10조에 따른 보호지침의 제정 및 통보 4. 제11조에 따른 보호조치의 명령 또는 권고를 이행하기 위한 사업 5. 사이버 보안장비(정보통신보안설비, 망분리장치 등)와 보안 소프트웨어(백신 등)의 구매 6. 정보통신기반보호 전문 컨설턴트 지원 7. 신규 보안기술의 연구·개발 지원(R&D) 8. 사이버 침해사고의 배상보험제도의 운영 9. 위원회의 심의를 거쳐서 주요정보통신기반시설의 보호를 위하여 필요하다고 인정받은 사업 ② 관계 중앙행정기관의 장은 기반보호지원사업을 수행하기 위하여 주요정보통신기반시설 관리기관에게 필요한 경비의 일부 또는 전부를 출연·보조하거나 융자할 수 있다. 단, 민간부문에 대한 보호지원에 대하여는 미래창조과학부 장관의 고시로 세부사항을 정한다.

참 고 문 헌

1. 단행본

사단법인 정보통신법 포럼, 『정보통신기반 보호법제 연구』, 한국인터넷진흥원, 2013

송석윤, 『헌법과 사회변동』, 경인문화사, 2007

국가정보원·미래창조과학부·국가보안기술연구소·한국인터넷진흥원, 『2014국가정보보호백서』

호서대학교 산학협력단, 『정보통신기반보호 강화 방안 마련』, 한국인터넷진흥원, 2013

Ulrich Beck(홍성태 역), 『위험사회 : 새로운 근대성을 향하여』, 새물결, 2014

2. 논 문

박노형, “사이버안전 관련 국제규범의 정립을 위한 연구”, 「안암법학」 제37호, 안암법학회, 2012, 795~822쪽.

조한상, “기본권의 성격 : 주관적 성격과 객관적 성격”, 「법학논총」 제21집, 숭실대학교 법학연구소, 2009. 2, 225~248쪽.

변재일, “사이버보안강화 명목의 정보 권력 용인할 수 없어”, 「국회보」 제558호, 국회사무처, 2013. 5, 50~53쪽.

오일석 · 김소정, “사이버 공격에 대한 전쟁법 적용의 한계와 효율적 대응방안”, 「법학연구」 제17집 제2호, 인하대학교 법학연구소, 2014. 6, 119~161쪽.

오일석, “위험분배의 원칙에 입각한 정보통신기반보호체계의 개선방안”, 「법학논집」, 이화여자대학교 법학연구소, 2014. 9, 293~327쪽.

Isensee, Josef, Das Grundrecht auf Sicherheit, 1983. S. 3(홍완식, 안전권 실현을 위한 입법정책, 유럽헌법연구 제14호, 유럽헌법학회, 2013. 12, 229쪽)

3. 판 례

헌법재판소 2009. 2. 26. 선고 2005헌마764 결정

헌법재판소 1992. 2. 25. 선고 89헌가104 결정(전원재판부).

4. 언론기사 및 기타 인터넷 상 자료

Hal R. Varian, “System Reliability and Free Riding.” In: Proceedings of the First Workshop on Economics and Information Security. May 16-17. University of California, Berkeley(Feb. 2001) (the latest version Nov. 30, 2004) 이에 대하여는 http://people.ischool.berkeley.edu/~hal/Papers/2004/reliability (최종방문 2014년 10월 24일)

Ross Anderson, “Why Information Security is Hard - An Economic Perspective.” In: Proceedings of the 17th Annual Computer Security Applications Conference, New Orleans, LA(2001). 이에 대하여는 http://www.acsac.org/2001/papers/110.pdf 참조, (최종방문 2014년 10월 24일).

전하성(국회 수석전문위원), 『정보통신기반보호법안 심사보고서』, 국회 과학기술정보통신위원회, 2000. 12

2013년 2월 14일 ZDNet Korea 기사 “신설 국가안보실, 사이버 안보가 빠졌다” (http://www.zdnet.co.kr/news/news_view.asp?artice_id=2013-0213183429) (2014년 10월 24일 최종방문)

2013년 2월 6일 조명철 의원이 대표발의한「정보통신기반보호법 일부개정법률안」

2013년 4월 6일 중앙일보 “국가사이버안전관리, 누가 하나”(http://article.joins.com/news/article/article.asp?total_id=11151710&cloc=olink|article|default, 2014년 10월 24일 최종방문)

2013년 7월 5일 디지털데일리 기사 “국가 사이버안보 종합대책…사실상 국정원이 사이버안보 총괄”(http://www.ddaily.co.kr/news/news_view.php?uid=106442) (2014년 10월 24일 최종방문).

2013년 7월 5일 전자신문 “[사설] 사이버안보, 통제와 시장 균형점 찾을 때”(http://www.etnews.com/news/opinion/2793739_1545.html) 참조(2014년 10월 24일 최종방문).

2013년 7월 5일 한국뉴스투데이 기사 “박근혜 정부, 국가 사이버안보 종합대책 수립”(http://koreanewstoday.co.kr/detail.php?number=29126) 참조(2014년 10월 24일 최종방문).

2014년 2월 4일 정책브리핑 자료 “과학기술및사이버 전문인력 양성 활용MOU 체결” (http://www.korea.kr/policy/pressReleaseView.do?newsId =155942416&call_from=extlink, 2014년 10월 24일 최종방문)

2014년 5월 28일 뉴시스 기사 “류희인 전 청와대 국가안전보장회의 사무차장 겸 위기관리센터장 서울대 강연”(http://www.newsis.com/ar_detail/view.html?ar_id=NISX20140528_0012947490&cID=10202&pID=10200) (2014년 10월 24일 최종방문)

2014년 6월 24일 중앙일보 기사 “공인인증서 발급업체가 개인정보 유출” (http://article.joins.com/news/article/article.asp?total_id=15057956&cloc=olink|article|default, 2014년 10월 24일 최종방문)