정 보 보 호 학 회 지
제 25 권 제 3 호, 2015. 6

# 국내 정보통신기반보호법과 일본 사이버 보안 기본법에 대한 비교를 통한 고찰

한 도 석*, 한 덕 호** 염 흥 열***

요 약

최근 발생한 3.20 사이버 테러나 6.25 사이버 공격은 우리나라의 주요정보통신시설을 목표로 하였으며, 공격방법은 점점 지능화되고 첨단화 되어가고 있다. 특히 한수원(한국수력원자력) 해킹 사건으로 기반시설에 대한 보안의 중요성은 점점 커지고 있다. 기반시설에 대한 해킹은 다른 전산망 해킹 및 바이러스 유포 등에 의한 피해보다 인명 피해와 경제적 손실이 크므로 더 큰 이슈가 되고 있다. 이러한 이유로 국내에서는 정보통신기반시설의 중요성을 알고 2001년부터 『정보통신기반보호법』을 제정하여 중요성이 높은 시설을 주요정보통신기반시설로 지정하여 보호하고 있다. 또한 최근 일본에서는 국내의 『정보통신기반보호법』과 유사한 『사이버 보안 기본법』을 2014년 11월 6일에 채택하였다. 이에 따라 본 논문에서는 국내의 『정보통신기반 보호법』과 일본의 『사이버 보안 기본법』에 대하여 비교를 통해 고찰하고자 한다.

## Ⅰ. 서 론

오늘날 컴퓨터와 통신 기술의 급속한 진전은 고도의 정보통신망 구축을 가능하게 하였고, 국가·공공기관을 비롯하여 금융권, 기업체 그리고 개인에 이르기까지 각종 정보를 공유하게 함으로써 사회 전반에 큰 변화를 가져오게 하였다[1]. 하지만 이와 더불어 3.20 사이버 테러나 6.25 사이버 공격과 가장 최근 발생한 한수원 해킹 사건은 정보화로 야기되는 역기능 폐해가 심각하다.

이러한 사고를 예방하기 위해 국내에서는 2001년부터 『정보통신기반보호법』을 제정하여 국내의 중요성이 있는 시설을 정보통신기반시설로 지정하여 국가차원에서 관리를 하고 있다.

그리고 주요정보통신기반시설을 보호하기 위한 연구도 다양하게 이루어지고 있다. 5개 프로세스에 대한 품질 관리 방안을 마련하고 주요정보통신기반시설 관리기관을 위한 취약점 분석·평가 관련 연구[2]와 국내 주요정보통신기반시설에 대한 보호체계를 살펴보고 선진국에서 추진 및 시행하고 있는 보안대책과 계획을 분석하여 개선방안을 도출하고 국내 주요정보통신기반시설에 적합한 맞춤형 보호대책을 제시한 연구 논문[3] 등이 있다.

기반시설의 중요성이 점점 커지는 가운데 2014년 11월 6일 일본 중의원은 『사이버 보안 기본법』을 채택하였다. 이러한 일본의 행동은 사이버 보안 전략본부를 신설함으로써 범부처 사이버 보안 정책을 통합하고 체계화하며 2020년 도쿄 올림픽을 앞두고 마련된 성격이 강하다[4].

본 논문에서는 국내의 『정보통신기반 보호법』과 일본의 『사이버 보안 기본법』에 대하여 비교를 통해 고찰하고자 한다.

## Ⅱ. 관련 연구

2장에서는 국내의 전자적 침해행위로부터 주요정보통신기반시설의 보호에 관한 대책을 수립·시행하기 위하여 2001년 제정한 『정보통신기반 보호법』과 일본의 범부처 사이버 보안 정책을 통합 및 체계화하기 위해 2014년 11월 6일 채택된 『사이버 보안 기본법』에 대한 주요 내용을 서술한다.

본 연구는 미래창조과학부 및 한국인터넷진흥원의 “고용계약형 정보보호 석사과정 지원사업”의 연구결과로 수행되었음
* 순천향대학교 일반대학원 융합서비스보안학과 석사과정생 (hds_ei@naver.com)
** 순천향대학교 일반대학원 융합서비스보안학과 석사과정생 (cherub1218@naver.com)
*** 순천향대학교 정보보호학과 교수 (hyyoum@gmail.com, 교신저자)

### 2.1. 『정보통신기반보호법』(한국)[5]

『정보통신기반 보호법』에서는 주요정보통신기반시설의 안정적인 관리 및 운영이 이루어지도록 [그림 1]과 같이 정보통신기반 위원회를 운영하고 있다.

다음으로 『정보통신기반 보호법』에 대한 주요내용을 서술한다.

· 제1장 총칙

제1조(목적) 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 시설을 안정적으로 운용하여 국가의 안전과 국민생활의 안정을 목적

제2조(정의) 법에서 사용하는 '정보통신기반시설', '전자적 침해행위', '침해사고' 용어의 정의

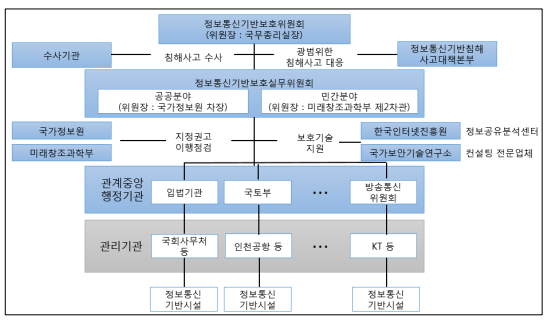
· 제2장 주요정보통신기반시설의 보호체계

제3조(정보통신기반위원회) 정보통신기반보호위원회의 구성 방법에 관한 내용

제4조(위원회의 기능) 주요정보통신기반시설 보호정책의 조정, 보호계획의 종합·조정, 보호계획의 추진실적, 보호와 관련된 제도의 개선, 주요 정책사항으로서 위원장이 부의하는 사항에 관하여 심의

제5조(주요정보통신기반시설보호대책의 수립 등) 주요정보통신기반시설을 관리하는 기관의 장은 취약점 분석·평가의 결과에 안전하게 보호하기 위한 (예방, 백업, 복구 등) 물리적·기술적 대책을 포함한 관리대책을 수립·시행

제5조의2(주요정보통신기반시설보호대책 이행 여부의 확인) 국가기관의 장은 관리기관에 대하여 주요 정보통신기반시설보호대책의 이행 여부를 확인, 자료 제출을 요청, 이행 여부를 관계중앙행정기관의 장에게 통보




〔그림 1〕 정보통신기반시설 보호체계[3]

제6조(주요정보통신기반시설보호계획의 수립 등) 관계중앙행정기관의 장은 주요정보통신기반시설보호대책을 종합·조정하여 소관분야에 대한 주요정보통신기반시설에 관한 보호계획(취약점 분석·평가, 침해사고에 대한 예방 및 복구대책, 보호에 관한 필요한 사항이 포함된 내용)을 수립·시행하고 위원회에 추진실적과 연도별 계획을 제출하여 심의, 주요정보통신기반시설의 보호에 관한 업무를 총괄하는 자를 지정

제7조(주요정보통신기반시설의 보호지원) 관리기관의 주요정보통신기반시설보호대책의 미흡으로 국가안전보장이나 경제사회전반에 피해가 우려 될 때 관련 전문기관의 장에게 업무(보호대책의 수립, 침해사고 예방 및 복구, 보호조치 명령·권고의 이행)에 대한 기술적 지원을 요청

· 제3장 주요정보통신기반시설의 지정 및 취약점 분석

제8조(주요정보통신기반시설의 지정 등) 수행 업무의 국가사회적 중요성, 업무의 정보통신기반시설에 대한 의존도, 상호연계성, 침해사고 발생 시 피해규모 및 범위, 침해사고의 발생가능성 또는 복구의 용이성을 고려하여 주요정보통신기반시설로 지정 및 취소와 관련된 규정 및 내용

제8조의2(주요정보통신기반시설의 지정 권고) 특정한 정보통신기반시설을 주요정보통신기반시설로 지정에 관한 내용

제9조(취약점의 분석·평가) 관리기관의 장은 정기적으로 소관 주요정보통신기반시설의 취약점을 전담반을 구성(한국인터넷진흥원, 정보공유·분석센터, 지식정보보안 컨설팅전문업체, 한국전자통신연구원 예외)하여 분석·평가하여 관계중앙행정기관의 장에게 통보

· 제4장 주요정보통신기반시설의 보호 및 침해사고의 대응

제10조(보호지침) 관계중앙행정기관의 장은 소관분야의 주요정보통신기반시설에 대하여 보호지침을 제정(기술의 발전 등을 감안하여 주기적으로 수정·보완)하고 이를 지키도록 권고

제11조(보호조치 명령 등) 대책을 분석하여 별도의 보호조치가 필요한 경우나 대책의 이행 여부를 분석하여 별도의 보호조치가 필요하다고 인정하는 경우 관계중앙행정기관의 장은 해당 관리기관의 장에게 주요정보

통신기반시설의 보호에 필요한 조치를 명령 또는 권고

제12조(주요정보통신기반시설 침해행위 등의 금지) 접근권한 없는 사람의 주요정보통신기반시설에 접근하거나 접근권한 있는 사람의 권한을 초과하여 데이터를 조작·파괴·은닉 또는 유출하는 행위, 주요정보통신기반시설에 대한 데이터 파괴와 바이러스·논리폭탄 등의 프로그램을 투입하는 행위, 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보처리에 오류를 발생하게 하는 행위에 대한 금지

제13조(침해사고의 통지) 주요정보통신기반시설의 침해사고가 발생하여 인지한 때에는 관계 행정기관, 수사기관 또는 인터넷진흥원에 통지하고 관계기관 등은 침해사고의 피해확산 방지와 신속한 대응을 위하여 필요한 조치(정부는 예산의 범위 안에서 복구비 등 재정적 지원 가능)를 취함

제14조(복구조치) 관리기관의 장은 주요정보통신기반시설에 대한 침해사고가 발생한 때에는 해당 기반시설의 복구 및 보호조치(필요한 경우 관계중앙행정기관의 장 또는 인터넷진흥원 장에게 지원 요청 가능)를 신속히 취하고 피해확산을 방지할 수 있도록 관리기관의 장과 함께 적절한 조치를 취함

제15조(대책본부의 구성등) 침해사고가 광범위하게 발생한 경우 필요한 응급대책, 기술지원 및 피해복구 등을 수행하기 위한 기간을 정하여 위원회에 정보통신기반 침해사고대책본부(대책본부)를 구성하고 운영에 관한 내용

제16조(정보공유·분석센터) 금융·통신 등 분야별 정보통신기반시설을 보호하기 위한 취약점 및 침해요인과 그 대응방안에 관한 정보 제공, 침해사고 발생 시 실시간 경보·분석체계 운영에 업무를 수행하고자하는 경우 정보공유·분석센터를 구축·운영 가능(정부는 구축을 장려하고 관련된 기술적 지원 가능)

· 제6장 기술지원 및 민간협력 등

제24조(기술개발 등) 정보통신기반시설을 보호하기 위한 필요한 기술의 개발(정보보호 관련된 연구기관 및 민간단체 대행하고 소요되는 비용을 전부 또는 일부 지원 가능) 및 전문 인력 양성에 관한 시책 강구

제25조(관리기관에 대한 지원) 정부는 관리기관에 대하여 주요정보통신기반시설을 보호하기 위해 기술의 이전, 장비의 제공, 그 밖의 필요한 지원 가능

제26조(국제협력) 국제적 동향을 파악하고 국제협력을 추진하고 촉진하기 위해 관련기술 및 인력의 국제교류와 국제표준화 및 국제공동연구개발 등에 관한 사업을 지원 가능

제27조(비밀유지의무) 위원회 및 실무위원회, 주요정보통신기반시설에 대한 취약점 분석·평가업무를 하는 기관, 침해사고의 통지 접수 및 복구조치와 관련 업무를 하는 관계기관, 정보공유·분석센터에 해당하는 기관에 종사 또는 종사했던 자에 대한 비밀 누설 금지

· 제7장 벌칙

제28조(벌칙) 주요정보통신기반시설을 교란·마비 또는 파괴한 자는 10년 이하의 징역 또는 1억 원 이하의 벌금, 미수범은 처벌

제29조(벌칙) 비밀 누설한 자는 5년 이항의 징역, 10년 이항의 자격정지 또는 5천만 원 이하의 벌금

제30조(과태로) 보호조치 명령을 위반, 규정에 의한 통지를 하지 아니한 자는 1천만 원 이하의 과태료와 관련된 부과·징수, 또는 이의 제기에 대한 내용

· 부칙(생략)

### 2.2. 『사이버 보안 기본법』(일본)[6]

『사이버 보안 기본법』에서 안정적인 관리 및 운영이 이루어지도록 [그림 2]와 같이 사이버 보안 전략본부 기능과 권한 체계도[4]가 있다.

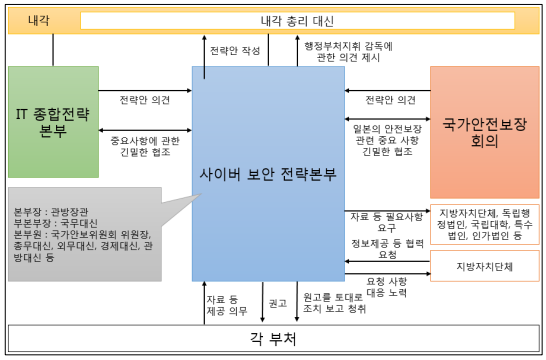
다음으로 『사이버 보안 기본법』에 대한 주요내용을 서술한다.

· 제1장 총칙

(목적) 제1조 사이버 보안에 관한 시책에 관한 기본이념을 정하고, 국가 및 지방 공공 단체의 책임 등을 명확히 하고, 사이버 보안 전략 보안에 관한 시책의 기본이 되는 사항을 규정, 사이버 보안 전략 본부를 설치함으로써 경제 사회의 활력 제고 및 지속적인 발전과 국민이 안전하고 안심하고 살 수 있는 사회의 실현을 도모

(정의) 제2조 법에서 사용하는 '사이버 보안', '전자적 방식', '전자적 기록 매체'에 대한 용어 정의

(기본 이념) 제3조 사이버 보안에 관한 시책의 추진은 정보의 자유로운 유통을 보장하지만, 사이버 보안 위협에 대해 국가, 지방 공공 단체, 중요한 사회 기반 사




〔그림 2〕 사이버 보안 전략본부 기능 및 권한 체계도〔4〕

업자(국민 생활 및 경제활동의 기반, 중지 또는 저하된 경우 국민생활이나 경제 활동에 막대한 영향을 미치는 사업) 등의 다양한 주체의 협력을 통해 적극적으로 대응하는 것을 취지

2 사이버 보안에 관한 시책의 추진은 국민에 대한 인식을 높이고, 자발적 대응 촉구, 피해를 방지하고 피해로부터 신속하게 복구를 취지

3 사이버 보안에 관한 시책의 추진은 인터넷 기타 고도정보통신 네트워크의 정비 및 정보 통신 기술의 활용에 경제 사회를 구축하기 위한 노력 추진을 취지

4 사이버 보안에 관한 시책의 추진은 국제 사회의 공동의 과제, 사이버 보안 국제 질서의 형성과 발전을 위해 선도적인 역할을 취지(국제적 협조 하에)

5 사이버 보안에 관한 시책의 추진은 고도정보통신 네트워크 사회 형성 기본법의 기본 이념을 배려

6 사이버 보안에 관한 시책의 추진에 있어 국민의 권리를 부당하게 침해하지 않도록 유의

(국가의 책무) 제4조 국가는 사이버 보안에 관한 종합적인 시책을 수립하고 실시 할 책무

(지방 공공 단체의 책무) 제5조 지방 공공 단체는 국가와의 적절한 역할 분담을 통해 사이버 보안에 관한 자주적인 시책을 수립하고 실시 할 책무

(중요한 사회 기반 사업자의 책무) 제6조 중요한 사회 기반 사업자는 서비스를 안정적이고 적절하게 제공하기 위해 보안의 중요성에 관심과 이해를 높이고, 사이버 보안의 확보, 국가 또는 지방 공공 단체가 실시하는 사이버 보안에 관한 시책에 협력

(사이버 관련 사업자 다른 사업자의 책무) 제7조 사이버 관련 사업자는 사업 활동과 관련하여 사이버 보안의 확보, 국가 또는 지방 공공 단체가 실시하는 사이버 보안에 관한 시책에 협력

(교육 연구 기관의 책무) 제8조 대학 또는 기타 교육 기관은 사이버 보안의 확보, 인재 육성, 연구 및 성과의 보급, 국가 또는 지방 공공 단체가 실시하는 사이버 보안에 관한 시책에 협력

(국민의 노력) 제9조 국민은 사이버 보안에 관심과 이해를 높이고, 사이버 보안 확보에 필요한 주의를 기울이도록 노력

(법제상의 조치 등) 제10조 정부는 사이버 보안에 관한 시책을 실시하기 위한 법제 상, 재정 상, 세재 상의 조치를 강구

(행정 조직의 정비 등) 제11조 국가는 행정 조직의 정비 및 행정 운영의 개선에 노력

· 제2장 사이버 보안 전략

제12조 정부는 시책의 종합적이고 효과적인 추진을 위해 사이버 보안에 관한 기본 계획(사이버 보안 전략)을 정함

(제12조 관련 내용) 사이버 보안에 관한 시책의 기본적인 방침, 사이버 보안 확보, 촉진 등의 종합적이고 효과적인 추진에 필요한 사항에 대한 것들을 사이버 보안 전략에 포함

정부는 수립한 사이버 보안 전략을 국회에 보고, 인터넷 등으로 공표하고 정부는 전략에 필요한 경비의 자금의 확보 조치를 강구

· 제3장 기본적 시책

(국가 행정 기관 등의 사이버 보안의 확보) 제13조 사이버 보안 관련 국가의 행정 기관 및 독립 행정 법인의 사이버 보안에 대한 통일적인 기준을 수립, 국가 관련 악의적인 활동 모니터링 및 분석, 사이버 보안 연습과 훈련, 국내외 관계 기관과 위협에 대응, 국가의 행정 기관과 행정법인 또는 특수법인 등 사이의 사이버 보안 정보 공유와 필요한 시책을 강구

(중요한 사회 기반 사업자 등의 사이버 보안 확보의 촉진) 제14조 국가는 중요한 사회 기반 사업자 등의 사이버 보안 관련 기준의 책정, 연습 및 훈련, 정보 공유, 활동 촉진 등 필요한 시책을 강구

(민간 사업자 및 교육 연구 기관 등의 자발적인 활동의 촉진) 제15조 국가는 중소기업자 외의 민간 사업자 및 대학 또는 교육기관의 사이버 보안의 중요성에 대한

관심과 이해, 사이버 보안에 필요한 정보의 제공 및 조언에 필요한 시책을 강구

2 국가는 국민이 일상생활에서 전자계산기 또는 인터넷 기타 고도 정보 통신 네트워크 이용에 있어 사이버 보안에 관한 정보의 제공 및 조언에 필요한 시책을 강구

(다양한 주체의 연계 등) 제16조 국가는 관계 부처 상호간의 연계 강화, 다양한 주체들이 상호 협력하여 사이버 보안 시책에 종사 할 수 있도록 필요한 시책을 강구

(범죄의 단속과 피해의 확대 방지) 제17조 국가는 사이버 보안 범죄 단속 및 피해 확대 방지에 필요한 시책을 강구

(우리나라의 안전에 중대한 영향을 미칠 우려가 있는 사건에 대응) 제18조 국가는 사이버 보안사건 중 중대한 영향을 미칠 우려가 있는 것들에 대해 관계 기관 체제의 충실 강화, 상호 협력 강화, 역할 분담의 명확화를 위해 필요한 시책을 강구

(산업의 진흥 및 국제 경쟁력 강화) 제19조 국가는 사이버 보안 관련 산업이 고용 기회를 창출 할 수 있는 산업이 될 수 있도록 사이버 보안 관련 첨단적인 연구 개발의 추진, 기술의 고도화, 인재 육성 및 확보, 경영 기반 강화 및 새로운 사업의 개척, 기술의 안전성 및 신뢰성에 관한 규격, 국제 표준화 등의 필요한 시책을 강구

(연구 개발의 추진 등) 제20조 국가는 사이버 보안 연구 개발 및 기술 등의 추진 및 성과의 보급을 도모하기 위해 사이버 보안 관련 기초 연구 및 기반적인 기술 연구 개발의 추진, 연구자 및 기술자의 육성, 국가시험 연구 기관, 대학, 민간 등의 연계 강화, 연구개발을 위한 국제 협력 등의 필요한 시책을 강구

(인력 확보 등) 제21조 국가는 대학, 고등 전문학교, 전수 학교, 민간사업자와 연계 협력을 통해 사이버 보안에 관한 사무에 종사하는 자의 적절한 처우 확보에 필요한 시책과 인재의 확보, 양성 및 자질 향상을 위해 자격 제도의 활용, 젊은 기술자 양성에 필요한 시책을 강구

(교육 및 학습의 진흥, 보급 계발 등) 제22조 국가는 국민에 대한 사이버 보안 관심과 이해, 교육 및 학습의 진흥, 계몽 및 지식의 보급과 관련된 시책과 추진할 수 있도록 기간의 지정 및 기타 필요한 시책을 강구

(국제 협력의 추진 등) 제23조 국가는 사이버 보안 분야에 대해 국제간의 신뢰 관계 구축 및 정보공유 추진, 국제 기술 협력 지원, 범죄의 단속과 관련된 국제 협력 추진 등을 위한 필요한 시책을 강구

· 제4장 사이버 보안 전략 본부

(설치) 제24조 사이버 보안에 관한 시책을 효과적 추진을 위해 사이버 보안 전략 본부 설치

(소장 사무 등) 제25조 전략 방안의 작성 및 추진, 평가, 사건에 대한 시책의 평가, 당해 연도 지침의 작성 및 시책 평가 등 종합적인 조정에 관한 사무를 주관함

(조직) 제26조 본부의 조직 구성원에 대한 내용

(사이버 보안 전략 본부장) 제27조 본부의 장은 내각관방 장관으로 정하고 사무를 총괄 직원을 지휘 감독

(제27조 관련 내용) 본부장은 관계 행정 기관의 장에게 자료, 정보가 필요한 경우 권고, 취한 조치에 대한 보고를 요구, 특별한 경우 총리대신에게 규정에 의한 조치를 취하도록 의견을 진언 가능

(사이버 보안 전략 부본부장) 제28조 부본부장은 국무대신으로 정하고 본부장의 직무를 도움

(사이버 보안 전략 본부 원) 제29조 사이버 보안 전략 본부 직원 구성에 관한 내용

(자료 제공 등) 제30조 관계 행정 기관은 본부에 사이버 보안 관련 자료 또는 정보를 적시에 제공하고 본부에 대해 사이버 보안에 관한 자료, 정보의 제공, 설명 등 필요한 협력

(자료의 제출 기타 협력) 제31조 본부는 지방 자치단체, 독립 행정 법인, 국립대학 법인, 학장 대학 공동이용 기관, 이사장, 특수 법인, 인가법인 등 누구에게나 사이버 보안 사건이 발생한 경우 관련 자료 제출, 의견의 개진, 설명 등 필요한 협력을 요구 또는 요청 가능

(지방 공공 단체의 협력) 제32조 지방 자치 단체는 본부에 정보 제공 또는 기타 협력을 요청 가능하고 본부는 이에 응하도록 노력

(사무) 제33조 본부에 관한 사무 처리·관리에 관한 내용

(주임 대신) 제34조 생략.

(정령에의 위임) 제35조 법에 정하는 것 외에 본부에 필요한 사항은 대통령령으로 정함

· 부칙(생략)

## Ⅲ. 『정보통신기반 보호법』과 『사이버 보안 기본법』의 비교를 통한 고찰

3장에서는 2장에서 서술한 한국의 『정보통신기반보호법』과 일본의 『사이버 보안 기본법』에 대한 주요 내용을 바탕으로 비교를 통해 『정보통신기반보호법』에 대하여 고찰해본다.

〔표 1〕 유사한 법령

| 『정보통신기반 보호법』 | 『사이버 보안 기본법』 |
|---|---|
| (목적) | (목적) |
| (정의) | (정의) |
| (정보통신기반위원회) | (설치), (조직), (사이버 보안 전략 본부장), (사이버 보안 전략 부본부장), (사이버 보안 전략 본부 원) |
| (위원회의 기능) | (소장 사무 등) |
| (주요정보통신기반시설 보호대책의 수립 등), (주요정보통신기반시설 보호대책 이행 여부 확인) | (자료 제공 등), (자료의 제출 기타 협력) |
| (주요정보통신기반시설 보호계획의 수립 등) | (국가의 책무), 제2장 사이버 보안 전략 |
| (주요정보통신기반시설의 보호지원) | (지방 공공 단체의 책무), (지방 공공 단체의 협력) |
| (주요정보통신기반시설의 지정 등) | (기본 이념) 제3조, (중요한 사회 기반 사업자의 책무), (사이버 관련 사업자 다른 사업자의 책무) |
| (주요정보통신기반시설의 지정 권고) | (중요한 사회 기반 사업자의 책무), (사이버 관련 사업자 다른 사업자의 책무), (우리나라의 안전에 중대한 영향을 미칠 우려가 있는 사건에 대응) |
| (취약점의 분석·평가) | (국가 행정 기관 등의 사이버 보안의 확보), (중요한 사회 기반 사업자 등의 사이버 보안 확보의 촉진), (민간 사업자 및 교육 연구 기관 등의 자발적인 활동의 촉진) |
| (보호조치 명령 등) | 제3장 기본적 시책과 유사함 |
| (주요정보통신기반시설 침해행위 등의 금지) | (범죄의 단속과 피해의 확대 방지) |
| (기술개발 등), (관리기관에 대한 지원) | (중요한 사회 기반 사업자의 책무), (사이버 관련 사업자 다른 사업자의 책무), (교육 연구 기관의 책무), (다양한 주체의 연계), (연구 개발의 추진 등) |
| (국제협력) | (국제 협력의 추진 등) |

### 3.1. 『정보통신기반 보호법』과 『사이버 보안 기본법』 비교

아래의 [표 1]에서는 『정보통신기반 보호법』과 『사이버 보안 기본법』에 대하여 정확하게 일치하지 않지만 여러 가지 법령의 조합으로 유사하거나 그 법령 자체로 유사한 내용을 나타낸 것이다.

[표 1]의 유사한 법령에 관한 내용 중에서 주요한 비슷한 내용은 한국의 “위원회”와 일본의 “사이버 보안 전략 본부”가 유사하며 역할 및 기능 또한 비슷하다고 할 수 있다. 또한 한국의 “주요정보통신기반시설보호대책의 수립”에 대한 내용은 일본에서 “자료 제공과 자료 제출 기타 협력”이란 법령으로 명시하고 있다. “주요정보통신기반시설보호계획의 수립”은 완벽하게 유사하지 않지만 “제2장 사이버 보안 전략”과 유사하다고 볼 수 있다.

특히 한국의 “주요정보통신기반시설의 지정과 지정 권고”에 대한 법령은 일본의 법령에서는 직접적인 언급이 없었지만 여러 가지 법령의 조합으로 지정과 지정 권고가 될 수 있도록 구성되어 있는 것을 확인 할 수 있었다.

[표 2]에서는 『정보통신기반 보호법』과 『사이버 보안 기본법』의 내용 중에서 차이가 나는 법령이나 유사한 내용이 없는 법령을 서술하였다.

특히 도출한 차이가 나는 관련 법령 내용들은 포괄적으로 보면 『정보통신기반 보호법』과 『사이버 보안 기본법』에 서로 유사한 내용이 있지만 법령에서 용어에 대한 직접적인 언급을 하지 않은 법령을 [표 2]에 서술했다.

〔표 2〕 차이가 나는 법령

| 국가(관련법) | 관련 법령 |
|---|---|
| 한국 『정보통신기반보호법』 | (보호지침) |
| | (침해사고의 통지) |
| | (복구조치) |
| | (대책본부의 구성 등) |
| | (정보공유·분석센터) |
| | (비밀유지의무) |
| | (벌칙), (과태료) |
| 일본 『사이버 보안 기본법』 | (교육 연구 기관의 책무) |
| | (국민의 노력) |
| | (법제상의 조치 등) |
| | (행정 조직의 정비 등) |
| | (인력 확보 등) |
| | (교육 및 학습의 진흥, 보급 계발 등) |

### 3.2. 비교를 통한 『정보통신기반 보호법』에 대한 고찰

· (교육 연구 기관의 책무)

국내의 『정보통신기반 보호법』에서는 주요정보통신기반시설과 관계행정기관에 대한 언급은 있지만 대학 또는 기타 교육 기관에 대한 사이버 보안에 관한 인재 육성, 사이버 보안 연구 및 성과 보급 등과 같은 협력하는 내용이 직접적으로 언급되어 있지 않아 '교육 연구 기관'과 관련된 내용 추가가 필요하다.

· (국민의 노력)

일본의 '국민의 노력'이라는 법령은 국내의 법령에도 반드시 필요한 법이라고 생각한다. 국내의 사이버 보안 교육 등은 대부분 관련 직군 또는 관계 행정기관 사람들에게만 치중되어 있다. 이러한 교육 형태를 법령으로 제정하여 모든 국민에 대하여 사이버 보안의 중요성과 관심과 이해를 높이고, 사이버 보안 확보에 필요한 주의를 제고하여야 한다.

· (법제상의 조치 등)

국내의 법령 내용에는 '법제상의 조치 등'에 대한 것이 내포되어 있다고 볼 수 있다. 하지만 '사이버 보안에 관한 정책을 위한 필요한 법제상, 재정상, 세제상의 필요한 조치를 강구'라는 직접적인 언급을 통해 조금 더 국가기반 보안에 탄력적인 대응이 필요하다고 생각한다.

· (행정 조직의 정비 등)

'행정 조직의 정비 등'의 내용 역시 국내 법령 내용에 없어도 충분히 가능하다고 본다. 하지만 국가기반 시설을 목표로 해킹이 일어날 경우 일반적 해킹과는 달리 범국가적 재난이 될 수 있으므로 『정보통신기반 보호법』의 법령에 관련 내용을 제정하여 범국가적 위협에 대하여 대응 할 수 있도록 행정 조직을 탄력적으로 운영할 필요가 있다.

· (인력 확보 등)

현재 국내의 기업 정보보호 실태[7]는 정보보호 예산 편성이 5% 미만이거나 지출하지 않는다. 그러므로 보안 인력에 대한 투자가 낮다고 볼 수 있다. 하지만 일본의 『사이버 보안 기본법』의 '인력 확보 등'이라는 법령에서는 사이버 보안 관련 사무에 종사하는 자의 직무 및 직장 환경에 대해 적절한 처우 확보에 필요한 시책을 강구해야 한다고 명시하고 있다. 이러한 직접적인 언급을 통해 고급 보안 인력 확보에 도움이 될 수 있다고 생각한다.

· (교육 및 학습의 진흥, 보급 계발 등)

일본의 '교육 및 학습의 진흥, 보급 계발 등'이라는 법령은 국내의 『정보통신망법』의 제11조에 존재하고 있다. 하지만 주요정보통신기반시설에 대한 보안의 중요성도 국민들에게 인식제고가 필요하기 때문에 『정보통신망법』과는 다른 '기반시설에 대한 보안과 관련된 컨텐츠'를 활용한 '교육 및 학습의 진흥, 보급 계발 등'의 법령이 『정보통신기반 보호법』에도 필요하다고 생각한다.

## Ⅳ. 결 론

본 논문에서는 서로 성격이 비슷한 한국의 『정보통신기반 보호법』과 일본의 『사이버 보안 기본법』의 법령 내용 비교를 통해 『정보통신기반 보호법』에 대하여 고찰하였다.

한국의 '정보통신기반보호위원회'와 일본의 '사이버 보안 전략 본부'가 기능과 역할이 비슷하다고 볼 수 있다. 또한 법령을 비교해 본 결과 한국은 '침해사고의 통지', '복구조치', '벌칙', '과태료' 등 세부적인 내용까지 다루는데 반해 일본은 '기본이념', '책무', '기본적 시책'과 같은 내용에 모든 것이 포함되어 사각지대가 없도록 법령을 제정하였다.

앞으로 어떠한 법이 국가기반시설의 보안에 효과적인 도움이 되는지 확실히 알 수는 없다. 하지만 국가기반시설에 대한 보안이 점점 중요해지는 시점에서 사각지대 또는 부족한 법령을 개정하여 국민의 안전에 이바지하도록 연구가 필요하다.

향후 『정보통신기반 보호법』과 『사이버 보안 기본법』에 대한 법령 이외에 국내 「보호지침」, 「시행령」, 「시행규칙」과 대응하는 것들의 비교·분석에 대한 연구가 필요하다.

## 참 고 문 헌


[1] 이남훈, 정윤정, 김인중, “정보통신기반시설의 보안위험분석 프로세스를 통한 취약점 분류”, *한국통신학회 학술대회논문집*, 2003(7), pp. 1564-1567, 2003

[2] 박순태, 이완석, 노봉남, “주요정보통신기반시설 보호를 위한 취약점 분석·평가 관리 방안”, *한국정보보호학회학술지*, 19(6), pp. 32-40, Dec. 2009

[3] 배효빈, 엄정호, 김태경, 정태명, “주요정보통신기반시설에 대한 사이버 위협을 예방하기 위한 맞춤형 보호체계 구축”, *보안공학연구논문지*, 10(6), pp. 643-654, Dec. 2013

[4] *일본 사이버 보안 기본법 채택...사이버 보안 전략 본부 신설로 범부처 사이버 보안 정책 추진 사령탑 역할 기대*, 정보통신방송해외정보(CONEX), Nov. 2014

[5] *정보통신기반 보호법*, 국가법령정보센터, Nov. 2014

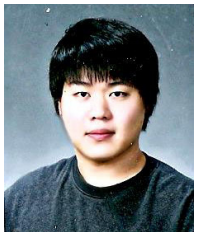
[6] *사이버 보안 기본법안*, The House of Representatives Japan(중의원), Nov. 2014

[7] *정보보호 준비도 평가 기술설명회*, 한국인터넷진흥원(KISA), Aug. 2014


## 〈저 자 소 개〉


**한 도 석 (Do-Seok Han)**
학생회원

2012년 8월 : 강원대학교 정보통신공학과 졸업
2014년 3월~현재 : 순천향대학교 융합서비스보안학과 석사과정
관심분야 : 경량암호, 개인정보보호, 의료정보보호, 보안정책



**한 덕 호 (Deok-Ho Han)**
학생회원

2012년 2월 : 동국대 전산원 졸업
2014년 3월~현재 : 순천향대학교 융합서비스보안학과 석사과정
관심분야 : 경량암호, 개인정보보호, 스마트 그리드

**염 흥 열 (Heung-Youl Youm)**
종신회원

한양대학교 전자공학과 학사 졸업
한양대학교 대학원 전자공학과 석사 졸업
한양대학교 대학원 전자공학과 박사 졸업
1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 정교수
1997년 3월~2000년 3월 : 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월 : 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재 : 한국정보보호 학회 총무이사, 학술이사, 교육이사, 총무이사, 논문지편집위원 위원장, 수석부회장(역), 학회장 (2011), 명예회장(현)
2005년~2008년 : ITU-T SG17 Q.9 Rapporteur(역)
2006년 11월~2009년 2월 : (구) 정통부 정보보호 PM/정보통신연구진흥원 정보보호전문위원
2009년 5월~현재 : 국정원 암호 검증위원회 위원
2009년~현재 : ITU-T SG17 부의장/SG17 WP2 의장
관심분야 : 인터넷 보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜