침해사고 분석을 통한 기반시설 보호 강화 모델 연구

윤오준* · 한복동* · 박정근* · 서형준** · 신용태***

요 약

최근 한수원을 대상으로 한 해킹 협박과 원전자료 공개 사고는 국가·사회 기능유지를 위한 기반시설의 보호 및 관리에 대한 중요성을 인식시켰다. 그러나 이들 기반시설에 대한 사이버보안 활동이나 제도가 여전히 미흡한 실정이기 때문에 향후 유사한 침해사고는 지속 발생할 가능성이 있으며 심지어 심각한 피해를 유발할 우려도 있어 우리 국민들은 불안해하고 있다. 특히 북한이 6개의 해킹조직으로 6,800여명의 해커를 운영하면서 불법자금 획득과 에너지·교통 등 기반시설까지 해킹하여 심리전까지 구사하고 있어 우리의 국가안보에 직접적인 위협이 되고 있다. 이에 본 논문에서는 최근 국내외 기반시설에서 발생한 침해사고 사례, 그에 따라 수립된 대책의 이행과정과 현행 기반시설 보호제도의 운영상 미비점을 분석, 평가하여 기반업무 수행체계 재정립, 기반시설 지원 강화 및 의무 부과, 보안점검 및 대응훈련 강화 등 우리나라의 기반시설 보호 강화를 위한 개선방안을 제시하고자 한다.

A Study on Models for Strengthening Infrastructure Protection through Analysis of Cyber Intrusions

Yoon Oh Jun* · Han Bok Dong* · Park Jeong Keun* · Seo Hyung Jun** · Shin Yong Tae***

ABSTRACT

The hacking threats made against the Korea Hydro & Nuclear Power(KNDP) and the leakage of critical information on nuclear power safety raised the public awareness on the importance of protecting and managing national infrastructure necessary for sustaining the state and society. Cyber security activities and relevant institutions in the ROK, however, are still insufficient, because of which there is a possibility that similar incidents would reoccur and cause serious damages. Hence, a grave and direct threat is posed to the national security of the ROK. In this thesis, I would like to give my analysis and assessment on the recent cyber intrusions against infrastructure at home and abroad, measures established in response and their implementation, and the deficiency of the existing infrastructure protection system ; and lastly propose measures to reinforce infrastructure protection of the ROK.

Key words : Infrastructure, Cyber security, Cyber intrusions, Comprehensive Measures,

접수일(2015년 9월 30일), 게재확정일(2015년 10월 16일)

* 숭실대학교 IT정책경영학과
** 한국전자통신연구원 부설연구소(책임저자)
*** 숭실대학교 컴퓨터학부(교신저자)

1. 서 론

2014년 12월부터 2015년 8월초까지 원전반대그룹을 사칭한 해커가 한수원을 대상으로 한 해킹 협박과 원전자료 공개 사고는 우리 국민들에게 국가 운영을 위한 핵심정보시스템의 보호에 대한 관심을 불러일으키기에 충분했다. 우리나라는 2009년 이후 정부기관은 물론 금융·방송사 등 기반시설에 대해 파괴와 혼란을 야기하는 디도스공격과 사이버테러가 빈번히 발생하고 있으며[11], 미국·일본 등 선진국도 연방기관·연금기구에 대한 해킹[12][10] 등 피해는 예외가 아니어서 향후 개인신상정보를 포함한 중요정보의 유출 위험과 해킹 문제는 국내외에서 지속적으로 큰 이슈가 될 것이며 국제안보적 측면에서도 큰 위협으로 다가올 것이다.

이런 사이버위협에 대비하는 차원에서 그 동안 우리 정부는 기반시설을 포함한 주요기관의 사이버침해사고 대응과정에서의 미비점을 개선하기 위해 범국가적인 여러 종합대책을 수립하여 시행해오고 있다[11]. 특히, 한수원 해킹 협박 사고를 계기로 수립한 '국가사이버안보태세 강화 종합대책'에는 기반보호위원회 운영을 국무조정실에서 국가안보실로 이관하고, 제어시스템의 안전성을 확보하기 위해 검증제도를 도입하며 관련 보안기술도 개발하는 등 기반시설 관리 강화 내용이 다수 포함되어 있다[8]. 또한 2001년 이후「정보통신기반보호법」을 제·개정하면서 기반시설별 취약점 분석·평가, 보호대책 및 계획 수립·시행, 이행여부 확인 및 침해사고 대응 등 적극적으로 보호활동을 수행하고 있다.

그러나 일련의 사고를 계기로 정부의 기반시설 보호 강화에 대한 지속적인 제도개선, 예산투자 등으로 전반적인 사이버보안 수준이 향상되었다고는 하나 공격기법은 고도화되어 사고는 끊임없이 발생하고 있고 심지어 그 발생 가능성도 날로 증대될 위험에 처해있어 우리 국민들은 여전히 불안해하고 있는 실정이다. 특히, 우리나라는 남북한이 정치·군사적으로 첨예하게 대치하고 있는 상황에서 북한이 당 및 군 산하에 6개의 해킹조직으로 1,700여명의 핵심해커와 5,100여명의 지원인력을 운영하면서[11] 불법 도박사이트 운영 등을 통한 통치자금 획득 시도[14]와 점차 에너지·교통 등 국가운영 및 사회기능을 유지하는 기반시설까지 해킹하여 심리전까지 구사하고 있어 우리의 국가안보에 직접적인 위협이 되고 있다.

이에 본 논문에서는 최근 국내외 기반시설에서 발생한 침해사고 사례를 분석해보고 그에 따라 수립된 대책의 이행과정과 현행 기반시설 보호제도의 운영상 미비점을 평가해 봄으로써 우리나라의 기반시설 보호 강화를 위해 개선해야 할 방안을 제시하고자 한다.

2. 관련 연구

2.1 국내 기반시설 대상 사고사례

2.1.1 한수원 해킹 협박

2014년 12월 한수원 직원을 대상으로 악성코드가 포함된 이메일을 발송하여 시스템 파괴를 시도하였고 그중 PC 5대의 하드디스크가 파괴되는 피해를 입었으며, 해커가 사전에 확보한 한수원의 원전관련 자료를 미끼로 원전 가동중단과 금전을 요구하는 등 여러 차례 협박을 시도한 사이버심리전 형태의 사이버공격이 발생하였다[11]. 또한 2015년 7월13일에는 원전 설계도면 관련자료 추가공개에 이어 8월3~4일간에는 청와대·국방부 등 정부의 내부 기밀문건이라고 하면서 출처불명의 자료를 공개하며 정부 정책에 대한 국민들의 불신과 계층간 사회적인 갈등을 야기하려고 시도하였다[13].

2.1.2 방송 및 금융기관 사이버테러

2013년 3월20일 KBS·MBC·YTN 등 3개 방송사와 농협·신한·제주은행 등 금융권의 PC, 서버 등 시스템이 악성코드에 감염되어 48,800여대가 파괴되면서 방송사에서는 직원들의 PC가 멈췄고, 금융기관에서는 인터넷 뱅킹, 영업점 창구업무, 자동화기기(ATM) 사용 등이 일시 중단되면서 관련 거래가 수시간 가량 중단되었으며 그 피해액이 무려 8,672억원에 달하는 것으로 추정되었다[11]. 이후 4월10일 민·관·군 사이버위협 합동대응팀은 이번 사이버테러의 수법과 접속기록을 정밀 조사한 결과 북한 정찰총국의 소행인 것으로 결론내렸다고 발표하였다[2].

2.1.3 농협 전산망 사이버테러

2011년 4월12일에 7개월간 준비한 APT 공격으로 농협 내부 전산시스템 270대가 파괴되어 4월30일까지 농협 업무 일부가 마비된 사건이 발생했다. 검찰은 5월3일 악성코드 구조, 공격IP 등의 증거자료를 제시하며 북한의 소행이라고 최종 발표하였으며, 이 사건은 단일기업 내부망에서 발생한 APT 침해사고와 관련하여 외주협력업체(한국IBM)의 노트북 보안관리 부실과 금융기관 등 민간기업에 대한 보안관제를 실시하지 않아 사이버공격을 탐지하고 차단하는데 미흡하였다는 문제점이 대두되었다[11].

2.2 해외 기반시설 대상 최근 사고사례

2.2.1 미국의 연방인사관리처 전산망 해킹

2015년 4월말부터 미국 각 부처 공무원의 보직, 근무평가, 건강 등 신상자료를 관리하는 연방인사관리처(OPM, Office of Personnel Management)의 전산시스템이 해킹을 당해 전・현직 연방공무원 및 지원자 2,510만명(신원조회 요청자 1,970만명, 가족・배우자 180만명 포함)의 개인정보가 유출된 것으로 추정된다고 보도되었는데 유출된 정보는 소셜시큐리티번호, 학・경력, 가족・지인, 전과여부, 재정상황 등 민감한 정보를 포함하고 있다. 이번 해킹의 배후는 중국이며 인민해방군 소속 해커들이 미국의 광범위한 인물정보를 수집하고 있다고 전하면서 정부의 강력한 대응을 촉구하였으며 지난 7월10일 캐서린 아출레타 처장은 결국 사임하였다[12].

2.2.2 일본의 연금시스템 사이버공격

일본의 연금기구 시스템이 2015년 6월2일 사이버공격을 받아 약125만건의 연금정보가 유출되었는데 유출된 정보는 개인에게 할당된 기초연금번호와 생년월일, 이름이라고 한다. 사고는 학술기관 직원을 가장해 보낸 이메일에 포함된 바이러스에 감염되면서 발생했는데 '세미나 초대장'이라고 적힌 이메일을 열어본 연금기구 직원의 컴퓨터가 바이러스에 감염되면서 이와 연결된 파일공유서버에 저장된 정보가 통째로 유출된 것으로 알려졌다. 그러나 연금수령액 등을 관리하는 시스템은 네트워크로 연결되지 않았다고 한다[10].

2.2.3 제어시스템 사이버테러

제어시스템은 폐쇄망으로 운영되어 과거에는 조작실수로 인한 피해가 일부 발생하였으나 최근에는 USB메모리, 웹 게시판 등 정보통신 서비스와 연결되어 운영되면서 사이버테러가 자주 발생하고 있으며 주요 사고 분야는 원전, 수자원, 교통 등이다. 대표적 사례로는 2010년9월 이란 나탄즈 원전 제어시스템에 스턱스넷 바이러스가 침투하여 원심분리기의 기능이 일부 마비된 사건이 발생하였는데 공격자(국가)에 대한 논란이 일기도 하였다[17]. 또한, 영국 캠브리지대학의 연구진이 2015년 5월에 발표한 분석보고서(Lloyd's Emerging Risk Report 2015)에 따르면 산업제어시스템 대상 해킹사고는 주로 가스공급시설, 자동차공장, 정수처리시설, 발전제어시설 등에 대한 공격이 지속적으로 발생하고 있으며, 침투경로는 외부 네트워크, 노트북, 원격제어장치, USB메모리 등 다양한 방법이 사용되고 있음을 알 수 있다[9].

2.3 해외 기반시설 보호 제도 최근 동향

2.3.1 미국

미국은 2013년 2월 오바마 대통령의 행정명령(제13636호)에 따라 중요 기간시설에 대한 사이버보안 체계 개선을 추진하였다. 상무부 산하 국가표준기술연구원(NIST)은 2014년 2월12일 기간시설에 대한 사이버보안 활동표준과 모범적 관행 등을 체계화한 '핵심 기간시설 사이버보안 체계개선 프레임워크'(Framework for Improving Critical Infrastructure Cybersecurity)를 발표하였다[6]. 주요 내용으로 첫째, 현재의 사이버보안 실태와 미래의 바람직한 상태를 비교하고, 둘째, 개선 가능한 사항을 확인하고 우선순위를 부여하며, 셋째, 개선노력을 평가하고 대내외적 의사소통 등을 제시하고 있다. 구체적으로 위협확인, 방어, 탐지, 대응, 복구로 구성된 핵심기능을 점검하고, 위협 인식수준과 처리과정 등 실행단계를 평가하며, 전체적인 보안관리 실태를 보여주는 프로파일 작성 등의 체계를 권고하고 있다. 한편 동 프레임워크는 기간시설 운영자들이 자발적으로 준수토록 권고하고 있으나 사고조사시 일종의 규범으로 작용할 수 있다는 점에서 사실상 규제장치 성격을 내포하고 있다.

또한, 미국은 국토안보부(DHS)가 연방정부의 기반시설 보호활동 및 정책을 담당토록 하고 있으며 2009년 10월 DHS 산하에 국가사이버안보/통신통합센터(NCCIC, National Cybersecurity and Communications Integration Center)를 설치하고 미국 정부를 상대로 한 각종 사이버위협 정보를 수집하여 대응하며 민간 및 공공의 기반시설 보호를 위해 위협정보를 신속하게 공유하고 있는데 NCCIC의 산업제어시스템 침해사고대응팀(ICS-CERT)은 주요 기반시설의 산업제어시스템 침해사고에 대한 대응 및 예방업무를 수행하고 있다[11].

2.3.2 일본

일본은 최근 세계적으로 다양한 사이버위협이 심각해지면서 정보통신망 정비와 정보통신기술의 활용 진전에 맞춰 자국의 사이버보안 확보를 위해 2014년 11월6일에 「사이버보안기본법」을 제정하였다. 동법은 사이버보안 시책에 관한 기본이념, 국가・공공기관 등의 책무, 사이버보안전략본부 설치 등을 담고 있다. 기반시설 보호와 관련해서는 중요사회기반사업자(국민생활 및 경제활동에 중대한 영향을 미치는 사업을 하는 자)로 하여금 서비스의 안정적 제공을 위해 사이버보안 확보 노력을 책무로 규정하고 국가・지자체 등 다양한 주체와의 협력과 연계를 강조하고 있으며 이를 위해 국가는 사이버보안 기준 책정, 연습 및 훈련, 정보공유 등 시책을 강구토록 하고 있다.[7]

3. 우리의 기반시설 보호 실태

3.1 기반시설 보호 정책 및 제도

3.1.1 「정보통신기반보호법」상 주요 내용

동 법은 전자적 침해행위로부터 주요 정보통신 기반시설을 보호하기 위한 대응체계, 기관별 활동 등을 규정하고 있는데 기반보호위원회 설치, 공공・민간 주관부처, 기반시설 지정・해제, 보호계획 및 대책 수립・시행, 침해사고 조사・복구 등을 포함하고 있다. 주요 내용으로 첫째, 국무총리 소속하에 정보통신기반보호위원회를 두고 위원장은 국무조정실장, 위원은 차관급 공무원으로 구성하며 위원회의 효율적 운영을 위해 공공・민간분야 실무위원회를 두고 공공은 국정원, 민간은 미래부가 주관토록 하고 있다. 둘째, 평시 기반보호 업무처리 절차로서 관계중앙행정기관의 기반시설 지정・해제, 관리기관의 취약점 분석・평가 및 보호대책 수립, 관계중앙행정기관의 보호계획 수립, 국정원・미래부 주관의 이행여부 확인 등이 있다. 셋째 침해사고 발생시 관리기관은 관계기관에 사실을 통지하고 복구조치를 하게 되며 광범위하게 발생한 경우 위원회의 위원장은 침해사고대책본부를 구성・운영할 수 있다[15].

<표 1> 기반보호법상 기반보호 내용

구 분	주 요 내 용
체 계	o 기반보호위원회(위원장 국무조정실장) 운영 o 실무위원회(공공 : 국정원, 민간 : 미래부) 운영
예 방	o 기반시설 지정 및 해제 o 취약점 분석·평가, 보호대책(계획) 수립·시행 o 보호계획 수립지침 통보 및 보호지침 권고 o 관리기관 대상 보호대책 이행여부 확인
대 응	o 침해사고 사실 통지 및 복구조치 o 광범위한 침해사고 발생시 대책본부 구성·운영

3.1.2 사이버안보 종합대책상 기반보호 내용

2011년 3.4DDoS공격, 농협 전산망 사이버테러 사고를 계기로 범정부 차원에서 수립한 '국가 사이버안보 마스터플랜'에는 국가사이버안전센터에 '민・관・군 사이버위협 합동대응팀'을 구축키로 하였다. 전력·금융 등 핵심 기반시설의 보안을 강화하기 위해 내부정보를 암호화하고 망 분리를 추진키로 하였고, 제어시스템의 취약점을 개선하기 위해 테스트베드를 구축키로 하였다. 또한 외주협력업체의 보안관리를 위해 기관 출입시 장비 반출입 통제, 입찰에서 용역사업 종료 시까지 단계별 보안대책을 수립, 시행토록 하였다[1].

2013년 3.20 방송・금융 사이버테러와 6.25 사이버공격 사고이후 마련된 '국가 사이버안보 종합대책'에는 청와대(평시에는 미래전략수석실, 위기시에는 국가안보실)를 컨트롤타워로 하고 국정원이 실무를 총괄하며, '주의' 경보 이상시 사이버위기 대책본부를 운영

토록 대응체계를 재정립 하였으며, 주요 민간기업 대상 정보보호 관리체계(ISMS) 인증대상 확대, 업무망 인터넷 분리, 전력·교통 등 분야별 특화된 위기대응훈련, IDC·의료기관 등을 포함한 주요 기반시설을 2017년까지 400개로 지속 확대 지정해 나가기로 하였다. 또한 외주협력업체가 내부정보 유출 등 보안사고 유발시 입찰제한 등 책임을 부가키로 하였다[3].

2014년12월 한수원 해킹 사고이후 마련된 '국가 사이버안보태세 강화 종합대책'에는 사이버안보 컨트롤타워 기능을 국가안보실로 통합하고, 각급기관의 보안조직과 인력을 보강하여 자체 보안관리 체제로 전환해 나가기로 했다. 특히, 기반보호위원회를 국무조정실에서 안보실로 이관하고 침해사고 대책본부장을 안보실장이 임명토록 변경하였다. 기반시설의 제어시스템에 대한 안전성을 검증할 수 있는 제도를 도입하며, 제어시스템의 보안취약점 분석기술과 보호기술 개발 등 기반시설의 핵심기능 유지를 위한 기술적 대책도 강화해 나가기로 하였다[8].

<표 2> 종합대책상 기반보호 내용

구 분	주 요 내 용
마스터플랜 (2011년)	o 민·관·군 사이버위협 합동대응팀 운영 o 기반시설 내부정보 암호화 및 망 분리 o 제어시스템 테스트베드 구축 o 외주협력업체 단계별 보안대책
종합대책 (2013년)	o 컨트롤타워 : 청와대, 실무 총괄 : 국정원 o ISMS 인증대상 확대 o 업무망 인터넷 분리 o 테마별 특화된 위기대응훈련 강화 o 기반시설 지정 확대(2017년 400개) o 사고유발 외주협력업체 입찰제한
종합대책 (2015년)	o 사이버안보 컨트롤타워 안보실로 통합 o 기반보호위원회 안보실 이관 o 제어시스템 안전성 검증제도 도입 o 제어시스템 취약점 분석 및 보호기술 개발

3.2 기반시설 관리상 문제점

3.2.1 기반시설 지정 등 수행체계 미흡

정부에서는 기반시설의 사이버보안 강화를 위해 우선 대상시설을 지속적으로 확대하여 지정(2017년까지 400개)할 계획이나 관리주체인 운영기관들은 법적인 보호의무의 부담을 이유로 지정에 비협조적이고 소극적인 입장을 유지하고 있어 문제가 되고 있다. 일례로 2013년 방송·금융기관 사이버테러 사고 이후 미래부에서 KBS 등 방송사를 대상으로 지정을 추진하였으나 노조 등의 조직적인 반발로 지정 추진이 중단된 바도 있다[4].

또한, 관리기관의 경우 실질적인 기반시설 보호수준 제고보다는 「정보통신기반보호법」에서 정한 취약점 분석·평가 등 최소한의 의무준수 사항이나 별도의 큰 노력없이 달성 가능한 수준 위주의 부실한 내용을 보호대책 추진과제로 수립하여 주관부처의 이행여부 확인시 책임회피 수단으로 악용하는 등 제도적 취지가 훼손되고 있다.

침해사고가 광범위하게 발생하여 침해사고대책본부를 구성·운영할 경우 기반보호위원장이 사고발생 관할 중앙부처와 협의하여 대책본부장을 임명토록 하고 있으나 인력 활용이나 기술능력이 부족한 부처의 경우에는 대책본부 운영의 실효성이 의문시되고 있다.

3.2.2 기반시설 지원 및 의무사항 미비

기반시설로 지정되면 시스템에 대한 취약점 분석·평가, 보호대책 수립·시행, 주기적 이행여부 확인 수감 등 업무수행에 따라 인력과 예산이 추가로 소요되고 정부의 간섭을 받게 된다. 그래서 관리기관의 입장에서는 기반시설 지정 자체에 미온적일 수밖에 없으며 유관한 기반시설간에도 사이버위협에 대한 정보공유의 필요성은 인정하면서도 실질적인 시스템 구축은 미흡한 실정이다.

또한, 기반시설에 대한 침해사고가 발생하여 교란·마비·파괴 사실을 인지한 경우 관리기관은 관계 행정기관, 수사기관에 통지토록 되어 있으나 '인지한 경우'의 명확한 시점을 특정하기가 어려운데다 침해사실을 통지하지 않더라도 처벌규정이 없어 실효성이 떨어지고 있는 실정이다. 반면 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」은 침해사고 발생시 신고하지 않을 경우 정보통신서비스제공자에게 1천만원의 과태료를 부과하고 있어 형평성을 잃고 있다[16].

2011년 농협전산망 테러나 2014년 한수원 해킹사고는 기반시설 관리기관이나 이를 지원하는 외주협력업

체의 직원이나 노트북 관리에 대한 문제점을 지속 제기하고 있으나 이들이 취급하는 민감한 내부운영정보에 대한 비밀유지 의무나 위반시 처벌에 관한 규정이 없어 유사사고가 지속 발생되고 있는 실정이다.

3.2.3 침해사고 예방을 위한 점검・훈련 부족

기반시설 보호대책에 대한 강력한 이행을 담보하기 위해 마련한 주관부처의 이행여부 확인제도가 기반시설의 지정이 양적으로 대폭 확대되고 전문분야가 추가되면서 확인점검에 많은 시간이 소요되고 분야별 전문기술이 필요함에 따라 점차 업무무담으로 작용하고 있어 개선이 필요하다.

기반시설에 대한 침해사고가 점증함에 따라 예방차원의 사전 점검이나 해커의 시스템 침투에 대비한 모의훈련 등이 필요하여 안보상황 발생 등 유사시 긴급점검과 을지연습 등 계기시에 민간분야 일부와 공공분야 기반시설 위주로 모의훈련을 실시하고 있다. 그러나 법적 근거 미비로 관리기관에서 적극적인 자세를 견지하지 않아 실전에서 제대로 대응할 수 있는 실질적 훈련이 미흡한 실정이다. 실례로 모 통신사 디도스공격시 대응매뉴얼에 따라 사이버대피소로 우회를 시도하였음에도 불구하고 사전에 시스템 전환 등 점검과 훈련을 해보지 않아 70여분간 장애가 지속되어 서비스가 중단된 사고가 발생한 바 있다.

4. 기반시설 보호 강화 개선방안

4.1 기반업무 수행체계 재정립

기반시설 신규 지정 추진시 해당기관의 고의적인 회피를 방지하고 기존 시설에 대한 보호대책이나 보호계획 수립을 실효성 있게 하기 위해 기반시설 보호절차를 개선해야 한다. 우선 보호대책이나 보호계획이 공공・민간 주관부처의 수립지침에 미흡할 경우 기반보호위원회 또는 관계중앙행정기관 또는 주관부처가 관리기관(관계중앙행정기관 포함)에게 보완을 요청할 수 있도록 해야 한다. 둘째, 관계중앙행정기관에 의한 기반시설 신규지정 또는 지정취소에 대한 심사결과가 객관성, 타당성, 공정성을 훼손하였다고 판단될 경우 기반보호위원회가 재심사를 요청할 수 있도록 기반보호위원회의 기능을 강화하여야 한다. 셋째, 일정수준 이상의 보호수준을 확보하기 위해 주관부처가 기술적, 관리적 기준을 정할 수 있도록 하고 그에 따라 관리기관은 이를 준수토록 하여야 한다. 넷째, 광범위한 침해사고 발생시 구성하는 침해사고 대책본부를 실질적이고 효과적으로 운영하기 위해서는 본부장을 공공・민간 주관부처가 각각 수행하되 필요시 기반시설 소관 중앙부처와 합동으로 운영토록 개선할 필요가 있다.

한편, 한수원 해킹 협박 사고이후 기반보호위원회를 총리소속에서 대통령소속으로 이관하면서 위원장을 국무조정실장에서 국가안보실장으로 변경하자는 의견이 대두된 바 있는데, 이는 안보실에 기존의 위기관리 기능에 기반시설 보호까지 통합하는 것으로 사이버안보 분야의 컨트롤타워 강화 측면에서 긍정적인 효과가 기대되나 안보실은 그 역할에 있어 모든 현안에 간섭 또는 통제보다는 부처간 이견조정이나 중장기적 안보전략 수립 등에 중점을 두어야 할 것이다.

4.2 기반시설 지원 강화 및 의무 부과

기반시설은 안보・경제・사회적으로 중요성이 인정되어 특별히 관리하는 시설이기 때문에 관리기관들의 적극적인 사이버보안 활동과 보안투자를 유도하고 정보공유・분석센터(ISAC)를 에너지, 의료, 교통 등 분야별로 다양화하기 위해 정부차원에서 재정적・기술적 지원을 뒷받침할 필요가 있으며 이를 위해 기반시설에 대한 인센티브 지원사업을 수행해야 한다.

또한, 침해사고 사실에 대한 통지의무 범위를 교란, 마비, 파괴 등 피해사실 인지여부와 관계없이 침해사고가 발생한 즉시 통지할 수 있도록 명확하게 규정해야 하며, 관리기관의 책임성 강화를 위해 침해사고 통지를 해태한 경우에는 과태료를 부과하고 과실을 감추기 위해 고의로 은닉한 경우에는 벌칙을 부과토록 할 필요가 있다.

아울러 기반시설의 관리기관이나 외부에 위탁하는 용역업체 직원 등 기반시설 관리에 종사하는 모든 인원에 대해서는 내부정보 유출방지와 보안유지를 위해 비밀유지 의무를 명확히 부여하고 위반시 처벌토록 제도화할 필요가 있다.

4.3 보안점검 및 대응훈련 강화

기반시설의 수가 점진적으로 확대되고 전문분야가 증가됨으로써 공공·민간 주관부처가 수행하는 기반시설의 보호대책 이행여부 확인업무의 부담을 해소해 나갈 필요가 있다. 이를 위해 기반시설 소관부처의 인적, 기술적 업무 수행능력을 고려하여 관계중앙행정기관에게도 기반보호위원회의 심의를 거쳐 이행여부 확인 권한을 부여할 필요성이 있다.

또한, 기반시설에 대한 침해사고를 사전에 예방하고 사고발생시 확산을 방지하는 등 대응능력 강화를 위해 유사시 대비 긴급점검이나 계기시 모의침투훈련 등을 실시할 수 있도록 법적 근거를 마련할 필요가 있다. 그렇게 함으로써 공공분야 기반시설은 물론 상대적으로 보안이 취약한 민간분야 기반시설에 대한 취약점을 발견하여 조기에 개선 조치하고 아울러 점진적으로 실전에 대비하는 태세를 제고해나가야 한다.

5. 결 론

본 논문에서는 최근 발생한 기반시설의 전산망 침해사고 사례, 이를 토대로 수립된 종합대책과 법령상 보호제도에 대해 살펴보았다. 그 동안 관계기관의 적극적인 보호 활동으로 기반시설의 사이버보안 수준이 향상되었다고 하나 제도적·관리적 미흡으로 인한 일부 미비점이 존재하고 있다. 점차 고도화되는 북한 등의 사이버위협에 효과적으로 대응하기 위해 국가 차원의 개선 방안으로 합리적 지정·해제, 실질적 보호대책 수립 등 기반업무 수행체계 재정립, 기술적·재정적 지원은 강화하되 의무 부과, 침해사고 예방·대응을 위한 점검 및 훈련 강화 등을 제시하였으며 이의 철저한 이행을 통해 기반시설에 대한 침해사고를 미연에 방지하거나 사고 발생시 피해를 최소화하여 사이버안보 강화에 기여할 수 있을 것이다.

참고문헌

[1] 방통위, “정부, 국가 사이버안보 마스터플랜 수립”, 보도자료, 2011.8.8.

[2] 임화섭, “북한 8개월간 준비해 3.20 사이버테러 감행”, 연합뉴스, 2013.4.10.

[3] 미래부, “정부, 국가 사이버안보 종합대책 수립”, 보도자료, 2013.7.4.

[4] 오상도, “반대하는 지상파방송사의 이유있는 행보 : 주요 정보통신기반시설 지정에 대한 문제 제기”, 한국방송협회 방송문화 제383호, 2013.8

[5] 박상돈 등, “사이버안보 추진체계의 제도적 개선과제 연구”, 한국융합보안학회 논문지 제13권 제4호, 2013.9.

[6] KISA, “NIST, 사이버보안 프레임워크 최종본 발표”, Internet & Security Biweekly, 한국인터넷진흥원, 2014.2.

[7] 강달천, “일본, 사이버보안기본법의 제정”, 인터넷법제동향 제86호, 한국인터넷진흥원, 2014.11.

[8] 국무조정실 등, “국가 사이버안보 태세 역량 대폭 강화한다”, 보도자료, 2015.3.17

[9] Centre for Risk Studies, “Annex A : Cyber attacks against Industrial Control Systems since 1999”, Lloyd’s Emerging Risk report 2015, 영국 캠브리지대학, 2015.5.

[10] 김창욱, “日 연금시스템 ‘사이버공격’ 당했다”, 전자신문 13면, 2015.6.3.

[11] 윤오준 등, “사이버공격 대응 분석을 통한 사이버안보 강화 방안 연구”, 한국융합보안학회 논문지 제15권 제4호, 2015.6.30

[12] 김동필, “OPM<연방인사관리처> 해킹은 사이버 진주만 공격”, LA중앙일보, 2015.7.13.

[13] 김인순, “원전반대그룹 청와대 등 해킹했다 주장”, 전자신문, 2015.8.4

[14] 서동일, “북, 도박SW에 백도어 설계, 승부조작해 거액 빼돌린 듯”, 동아일보, 2015.9.7.

[15] 정보통신기반보호법, 법률 제13013호, 2015.1.20. 일부개정, 2015.7.21. 시행

[16] 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 법률 제13280호, 2015.3.27. 일부개정, 시행

[17] 국가정보원·미래창조과학부 등, “2015 국가 정보보호 백서”, 2015.4.

[저 자 소 개]

윤 오 준 (Oh-jun Yoon)

1990년 2월 서울대학교 학사
2013년 8월 건국대학교 정보통신 대학원 석사
2015년 3월 숭실대학교 IT정책경영 학과 박사과정

email : ojyoon27271@naver.com

한 복 동 (Bok-dong Han)

1992년 2월 한밭대학교 학사
1997년 8월 숭실대학교 정보과학 대학원 석사
2015년 3월 숭실대학교 IT정책경영 학과 박사과정
2012년~ 한국교통대학교 교수

email : shhan@ut.ac.kr

박 정 근 (Jeong-keun Park)

1993년 2월 전북대학교 학사
2015년 2월 한양대학교 경영전문 대학원 석사
2015년 3월 숭실대학교 IT정책경영 학과 박사과정

email ; Jeong.keun.park@sap.com

서 형 준 (Hyung-jun Seo)

1997년 2월 광운대학교 컴퓨터공학과 학·석사
2015년 2월 연세대학교 컴퓨터과학과 박사
2006년~현재 한국전자통신연구원 부설연구소 선임연구원

email : hjseo@ensec.re.kr

신 용 태 (Yong-tae Shin)

1985년 2월 한양대학교 학사
1994년 2월 美아이오아대학교대학원 컴퓨터공학과 석·박사
1994년 美미시간주립대 교수
1995년~숭실대학교 컴퓨터학부 교수

email : shin@ssu.ac.kr