Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.4, Aug. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.4.907

트럼프 행정부의 주요기반시설 사이버보안 정책분석에 관한 연구

김 근 혜†‡
고려대학교 정보보호대학원

A Study on the Analysis of Trump Administration Cybersecurity Policy: Focusing on Critical Infrastructure

Geunhye Kim†‡
School of Cybersecurity, Korea University

요 약

본 연구는 트럼프 행정부에서 발표한 행정명령, 사이버보안 전략, 법안을 분석함으로써 트럼프 행정부 출범이후 미국의 주요기반시설에 관한 사이버보안 정책을 분석한다. 분석결과, 첫째, 백악관의 역할이 약화되고 국토안보부가 국가 사이버보안 기능을 총괄하게 되었다. 둘째, 트럼프 행정부는 주요기반시설의 정의를 확대함으로써 주요기반시설 사이버보안 분야에서 정부의 역할을 확대하였다. 셋째, 필요시 정부가 민간 주요기반시설의 운영에 관여할 수 있음을 밝히고 있다. 이러한 정책방향은 백악관의 견해보다는 국토안보부와 전문 관료들의 견해가 적극적으로 반영된 것으로 오바마 행정부의 정책을 보완·개선하는 방향으로 진행되었다. 트럼프 행정부의 사이버보안 정책을 분석한 학술연구는 많지 않다. 트럼프 행정부의 주요기반시설의 사이버보안 정책에 대한 분석결과는 한국의 사이버보안 정책에도 시사점을 제공할 수 있을 것이다.

ABSTRACT

The purpose of this study is to understand the cybersecurity policies and critical infrastructure protection of the United States through analyzing Donald Trump's administration executive orders, the national cyber strategy, and the legislation. The analysis has three findings. First, the Department of Homeland Security (DHS) became a main agent in the cybersecurity while the role of the White House was reduced. Second, Trump's administration expanded its role and mission in the policy area by extending the meaning of critical infrastructure. Third, in the case of cyber threats, the government can be involved in the operation of critical infrastructures in the private sector. The opinions of the professional bureaucrats and DHS were more reflected in the direction of the cybersecurity policy than those of the White House. In contrast to Barack Obama's administration, the Trump administration's cybersecurity strategies were not much studied. This study provides insights for improving cybersecurity policies and critical infrastructure protection.

Keywords: Trump Administration, Obama Administration, Critical Infrastructure, Cybersecurity Policy, Department of Homeland Security

Received(05. 08. 2019), Modified(07. 10. 2019), Accepted(07. 10. 2019)

† 주저자, geunhyekim1@gmail.com
‡ 교신저자, geunhyekim1@gmail.com(Corresponding author)

I. 서 론

주요기반시설 시스템의 직·간접적 IT시스템 사용의 증가는 주요기반시설의 규모를 더욱 크고 복잡하게 만들었다. 이에 따른 취약점도 증가하게 되었는데 주요기반시설은 새로운 사이버 공격대상으로써 이들을 표적으로 하는 사이버 공격은 최근 10년간 급격하게 증가하였다. 이로 인해 국가가 치명적인 피해를 입을 것이라는 우려 역시 확산되었으며[1] 주요기반시설 보호를 위한 사이버보안 정책의 수립은 국가 사이버 보안전략의 최우선 과제가 되었다.

2017년 1월에 출범한 트럼프 행정부의 주요기반시설 관련 사이버보안 정책은 행정명령 발표를 시작으로 국토안보부의 사이버보안 전략 등을 통해 윤곽이 드러나기 시작했다. 정책 규모면에서 점차 국가전략 프로젝트의 일환이 되고 있는[2] 미국의 사이버보안정책에서 기념비적인 법안으로 평가받는[3] '사이버보안 및 기반시설보호를 위한 전문기관 설립법'의 입법화는 트럼프 행정부의 주요기반시설에 대한 사이버보안 정책의 방향성을 뚜렷하게 보여주고 있다. 본 연구는 오바마 행정부 기간 내내 국내에서 주요기반시설을 포함한 미국의 사이버보안 정책분석이 적극적으로 이루어졌던 것과는 대조적으로 트럼프 행정부는 집권3년차 넘어서는 시점에 이미 사이버보안 정책이 연달아 발표되고 있음에도 불구하고 학술분석이 적극적으로 이루어지지 않고 있다는데 의문점을 가지고 트럼프 행정부의 사이버보안 정책, 그 중에서도 주요기반시설과 관련한 주요 정책을 분석하는데 목적이 있다. 본 연구는 트럼프 행정부에서 발표한 행정명령, 사이버보안 전략, 법안 등을 통해 트럼프 행정부의 주요기반시설의 사이보안 정책을 다각적 측면에서 분석하고자 한다. 이러한 분석에는 오바마 행정부의 주요기반시설 관련 사이버보안 정책의 추진동향과 평가, 두 행정부 정책의 비교분석이 포함되어 있다.

II. 오바마 행정부의 사이버보안 정책

2.1 주요기반시설 관련 사이버보안 정책 추진동향

오바마 행정부는 집권초기 미국의 정부기관들이 외부의 사이버공격에 대응력을 갖추지 못하고 있으며 국가차원의 사이버보안 대책이 시급하다고 판단했다.[1] 오바마 행정부는 2009년 사이버공간정책리뷰(Cyberspace Policy Review)[4]를 발표하고 국가 사이버보안 강화정책을 추진하였다. 리뷰는 국토안보부가 중심이 되어 사이버보안 역량평가, 취약점 분석, 국가 정보보안 계획, 정보보호 매트릭스 개발과 같은 주요기반시설 관련 사이버보안 정책을 추진할 것이라고 밝히고 있다[5]. 리뷰의 계획을 보다 구체화하기 위하여 국토안보부는 2011년 사이버 보안전략인 '안전한 사이버미래를 위한 청사진'(Blueprint for a secure cyber future)을 발표하기도 하였다.[2] 한편, 오바마 행정부는 주요기반시설의 보안강화를 위해 의회에서 발의했던 사이버정보공유 및 보호법(Cyber intelligence Sharing and Protection Act)과 사이버 보호법(Cyber Security Act of 2012)의 법제정이 모두 실패하자 2013년 2월 행정명령(Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity)[3]과 정책지침(Presidential Policy Directive (PDD) 21, Critical Infrastructure Security and Resilience)[4]을 발표하고 이를 바탕으로 주요기반시설의 사이버보안 정책체계를 정비하였다. 전문가들은 EO 13636과 PPD 21이 오바마

1) 2007년 선거기간부터 당시 오바마 대통령 후보는 온라인 네트워크 위험이 핵무기나 생화학 공격과 비슷한 수준의 위험성을 가지고 있기 때문에 당선 후 사이버보안 정책을 적극적으로 시행할 것이라고 밝혀왔다[6]. 취임 이후 오바마 대통령은 부시 행정부의 사이버공간 수석 관리자였던 멜리사 해서웨이(Melissa Hathaway)를 사이버보안 점검단장으로 임명하여 미 연방정부의 사이버보안 상황 전반을 파악하고 보완대책을 마련을 위한 보고서 작성을 지시했다[7].

2) 본 보고서가 제시한 목표는 다음과 같다[8]. (1) 사이버 위험 노출 감소 (2) 대응 우선순위 수립 및 복구 보장 (3) 상황공유 및 인식유지 (4) 회복력 증대

3) 오바마의 행정명령은 다음과 같은 사항들을 지시하고 있다[9]. (1) 기술 중립적이며 자발적인 사이버보안 프레임워크를 개발할 것 (2) 사이버보안 관행 채택을 장려할 것 (3) 사이버 위협 정보공유와 관련하여 공유의 양, 공유의 적시성, 공유내용 품질의 향상을 도모할 것 (4) 모든 주요 계획에 개인정보보호 및 시민자유의 보호를 적용 하여 주요기반시설을 보호 할 것 (5) 기존 규제를 사용하여 사이버보안을 증진시킬 것

4) 정책지침은 다음의 사항들을 지시하고 있다[10]. (1) 주요기반시설의 물리적 측면과 사이버안보적 측면 모두를 실시간으로 처리할 수 있는 상황인식 기능을 개발할 것 (2) 주요기반시설의 보안오류 혹은 보안실패로 인해 발생하는 필연적이며 예기치 못한 결과에 대해 이해할 것 (3) 공공과 민간의 파트너십을 평가하고 발전시킬 것 (4) 국가 주요기반시설 보호계획을 발전시킬 것 (5) 포괄적인 연구개발을 계획하고 개발할 것

행정부의 주요기반시설 사이버보안 정책수행의 실질적인 가이드라인이 되었다고 설명한다[1]. EO 13636는 주요기반시설의 보호체계 구축을 위한 사이버보안 프레임워크의 개발과 보급을 핵심 목적으로 하고 있다. PPD21은 주요기반시설 보호와 관련하여 정부 핵심 부처들의 역할과 의무를 명확히 하는 것을 주요 내용으로 하고 있다[5]. 2015년 12월에는 미국의 최초 정보공유법안인 사이버보안 정보공유법(CISA, Cybersecurity Information Sharing Act)의 제정을 공식적으로 발표했다. 이 법안은 민간기업, 주정부, 연방정부가 사이버보안과 관련하여 위협정보를 공유하고 이에 따른 인센티브를 제공하는 것을 주요내용으로 하고 있다.

한편, 오바마 행정부는 사이버보안과 관련한 모든 정책추진을 백안관이 중심이 되어 총괄·조정하는 방식으로 운영되었는데[11] 국가안보위원회(NSC, National Security Council) 산하 사이버안보국(Cyber security Directorate)의 사이버안보 조정관(Cybersecurity coordinator)이 국토안보부(DHS), 국가안보국(NSA), 연방수사국(FBI), 국무부(DOS), 상무부(DOC)와 같은 개별조직들의 사이버보안 업무수행을 총괄했던 것이 대표적인 사례이다[11]. 주요기반시설의 경우도 사이버보안 컨트롤타워인 백악관의 주도적인 정책결정 아래 주요기반시설 관련 사이버보안의 임무를 국토안보부가 수행하는 방식이었다.

2.2 오바마 행정부 주요기반시설 사이버보안 정책의 특징과 한계

오바마 행정부는 취임 직후부터 사이버보안을 정부 우선순위 정책으로 선언한 미국 최초의 행정부이다. 매년 오바마 행정부의 연두교서(State of the Union Address)에는 사이버보안의 중요성이 언급되어 있다. 집권 8년간 오바마 행정부의 사이버보안 정책은 다음과 같이 정리된다. 첫째, 공공 및 민간부문의 사이버보안 수준을 높이는 것, 둘째, 미국 또는 동맹국을 겨냥한 악의적인 사이버활동을 저지하고 와해하는 것, 셋째, 사이버보안 사고가 발생했을 때 효과적으로 대응하고 복구하는 것[12]. 오바마 행정부는 사이버공간정책리뷰를 바탕으로 정책 이니셔티브, 정책보고서, 행정명령, 입법 활동과 같은 다양한 방식으로 사이버보안 정책을 추진해왔다[13]. 전문가들은 오바마 행정부가 사이버보안을 최우선 과제로 삼고 포괄적 시도를 한 것을 크게 인정하고 이러한 노력에 긍정적인 평가를 내린다. 그러나 그럼에도 불구하고 정부기관이나 민간영역을 더 안전하게 만드는 목표는 달성하지는 못했다고 평가한다[13-14].

특히, 주요기반시설과 관련하여 오바마 행정부의 적극적인 사이버보안 조치에도 불구하고 성공적이었다고 평가하지 못하는 이유에 대해 다음과 같이 설명한다. 첫째, 주요기반시설의 대부분을 차지하고 있는 민간 기업들이 가지고 있는 정부와의 협력에 대한 거부감을 해소하지 못하여 결과적으로 민관 파트너십이 실패한 것, 둘째, 주요기반시설의 범위 정의가 협소화여 포괄적 정책추진에 실패한 것, 예를 들어 에너지, 전기, 운송과 같이 주요기반시설이지만 민간영역으로 분류되는 외부산업의 경우 정부가 적극적인 사이버보안 조치를 취하는데 제한적이었다는 점, 셋째, 주요기반시설의 사이버보안 논의의 상당 부분이 정보공유에만 집중되어 있었다는 점, 마지막으로 의회의 비협조로 인해 입법을 통한 정책추진보다는 행정부를 통해 일해야만 했다는 점 등이다[15].

전문가들은 이러한 평가를 바탕으로 차기정부는 오바마 행정부보다 더 포괄적인 사이버보안 정책을 개발해야한다고 제언했다. 또한, 사이버보안과 관련하여 정부가 사생활, 국가보안, 동맹국가와의 관계, 민간영역과의 협력 등 다양한 상충 관계에서 명확한 입장을 보여주어야 한다고 설명했다. 마지막으로 오바마 행정부의 정책결과물을 토대로 차기행정부는 사이버공간을 어떻게 다루어야 하는지에 대해 근본적으로 재고해 볼 필요가 있다고 조언했다[15].

III. 트럼프 행정부의 사이버보안 정책

3.1 주요기반시설 관련 사이버보안 정책 추진동향

3.1.1 연방정부의 네트워크와 핵심기반시설의 사이버보안에 관한 행정명령 (Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure 13800)

트럼프 행정부가 주요기반시설의 사이버보안 역량 강화를 위해 공식적으로 발표한 첫 번째 정책은 2017년 5월에 발표한 '연방정부의 네트워크와 핵심기반시설의 사이버보안에 관한 행정명령'(EO 13800)[16]이다. EO 13800은 연방정부차원에서

다루어야 할 네트워크 사이버보안, 주요기반시설에서 다루어야 할 사이버보안, 국가차원에서 다루어야 할 사이버보안 정책을 설명하고 있으며 주요 정부부처의 임무, 책임, 보고를 지시하고 중앙 집중화 된 정책수행을 강조하고 있다[17]. 주요기반시설 관련 사이버보안 정책의 주요 내용은 다음과 같다.

- 사이버공격을 받은 주요기반시설을 지원할 방안을 모색할 것
- 주요기반시설 운영주체의 사이버위험 관리이행 투명성을 증진시키고 이를 검토할 것
- 주요기반시설 운영주체가 사이버공격에 유연하게 대응할 수 있도록 인터넷의 복원력과 통신환경을 개선 할 것
- 사이버사고 및 사고여파에 대응하는데 필요한 역량을 검토하고 평가할 것
- 방위산업 부문의 위험을 판별하고 위험을 최소화 할 수 있는 계획을 대통령에게 보고할 것

트럼프 행정부의 사이버보안에 대한 기조를 확인할 수 있는 첫 번째 공식발표라는 점에서 본 행정명령은 전문가들 사이에서 많은 관심과 다양한 평가를 받았다. 행정명령을 긍정적으로 바라보는 그룹은 컴퓨터나 일부 부서 등 국한된 범위의 보안강화 조치가 아니라 근본적인 조치라고도 평가했다. 행정조치를 부정적으로 바라보는 그룹은 아이디어는 좋지만 여전히 가이드라인 없이 권고수준에 그치며 강제성 있는 대책을 제시하지 못했다는 면에서 현실반영이 충분치 못하다고 비판했다[18].

3.1.2 미 국토안보부의 사이버보안 전략 (U.S. Department of Homeland Security Cybersecurity Strategy)

미 '국토안보부의 사이버보안 전략'[19]은 트럼프 행정부 2년차인 2018년 5월 15일에 발표되었다. 2017 년 국방수권법(NDAA, National Defense Authorization Act of 2017)[5]에 따라 위임된 국

Table 1. DHS Cybersecurity Strategy 2018

Pillar	Goal and Objective
Risk Identification	Goal 1: Assess Evolving Cybersecurity Risks. Understanding the evolving national cybersecurity risk posture to inform and prioritize risk management activities.
Vulnerability Reduction	Goal 2: Protect Federal Government Information Systems. Reducing vulnerabilities of federal agencies to ensure they achieve an adequate level of cybersecurity.
	Goal 3: Protect Critical Infrastructure. Partnering with key stakeholders to ensure that national cybersecurity risks are adequately managed.
Threat Reduction	Goal 4: Prevent and Disrupt Criminal Use of Cyberspace. Reducing cyber threats by countering transnational criminal organizations and sophisticated cyber criminals.
Consequence Mitigation	Goal 5: Respond Effectively to Cyber Incidents. Minimizing consequences from potentially significant cyber incidents through coordinated community-wide response efforts.
Enable Cybersecurity Outcomes	Goal 6: Strengthen the Security and Reliability of the Cyber Ecosystem. Supporting policies and activities that enable improved global cybersecurity risk management.
	Goal 7: Improve Management of DHS Cybersecurity Activities. Executing our departmental cybersecurity efforts in an integrated and prioritized way.

5) 970페이지에 달하는 이 법안에는 상원 국토안보 및 행정부 담당 위원장 론 존슨(Ron Johnson (R-Wis.))과 공동위원장인 톰 카퍼(Tom Carper (D-Del.))가 공동 발의한 국토안보부 책임법(DHS Accountability Act) 일부가 포함되어 있다. 존슨위원장은 2017년 국방수권법에서 국토안보부의 책임과 관련한 많은 조항들이 승인될 수 있도록 추진했으며 본 법안에 대해서 국토안보부를 보다 효과적이고 효율적으로 만들기 위한 조치라고 평가하고 있다[20]. 특히, 본 법안에서 조항 1912(SEC. 1912. Cybersecurity Strategy for the Department of Homeland Security)는 국토안보부의 사이버 보안전략을 의회에 제출할 것과 관련한 요청사항을 다음과 같이 명시하고 있다[21]. 첫째, 사이버보안 전 범위의 성공적 임무수행을 위해 전략적 목표를 세우고 우선순위를 넣을 것, 둘째, 사이버보안 조사기능, 사이버보안 연구 및 개발, 국제 사이버보안 파트너들과의 협력 이행에 관한 사항들을 새로운 전략에 포함할 것, 셋째, 새로운 사이버보안 전략수립 시 미 국토안보부의 이전 사이버보안 전략(Blueprint for a Secure Cyber Future, 2011), 회계연도 2014-2018년에 발표된 국토안보부의 전략 계획, 그리고 가장 최근에 나온 4년 주기 국토안보리뷰(Quadrennial Homeland Security Review)등을 검토하고 이를 바탕으로 새로운 사이버보안 전략을 수립할 것, 넷째, 법안이 통과 된 이후 90일 이내로 국토안보부의 새로운 사이버 보안전략 보고서를 의회에 제출할 것, 다섯째, 국토안보부가 사이버 보안전략을 수립한 이후에는 90일 이내로 전략 목표, 계획된 타임라인 등을 사용하여 의회에 구현계획을 제시할 것

토안보부의 새로운 보안전략은 사이버 보안위험을 평가하고 위험관리의 우선순위를 결정하는 것을 최우선으로 권장하고 있다. 또한, 연방정부의 정보 시스템을 보호하고 기관의 취약성을 줄이며 이해관계자들과 협력하여 주요기반시설을 보호할 것을 주요 목표로 삼고 있다. 미 국토안보부는 국내의 사이버보안 위험을 전략적으로 관리하기 위해 국토안보부가 사용할 수 있는 광범위한 자원과 기능을 활용할 수 있는 혁신적인 방안을 강구해야 한다고 강조하고 국가 전반의 위험을 관리하기 위한 축(pillar), 주요목표(Goal), 세부목표(objective)를 제시하고 있다.

3.1.3 미국의 국가 사이버전략 (National Cyber Strategy of the United States of America)

트럼프 행정부는 2018년 9월 '국가사이버안보전략'[22]을 발표하였다. 연방 정보 보안책임자(CIO, Chief Information Officer)인 그란트 슈나이더(Grant Schneider)는 성명에서 이 전략이 2003년 이후 미국이 15년 만에 발표한 완전히 새로운 사이버전략이라고 설명했다[23]. 이 보고서는 트럼프 행정부가 국가 네트워크, 시스템, 데이터 전반에서 사이버보안을 어떻게 운영할 것인가에 대해 개괄하고 있다. 특히 이 보고서는 정부기관을 표적으로 하는 적대적 사이버 공격이 기하급수적으로 증가하고 있음에도 불구하고 정당화된 대처방법이 제한적이었음을 지적한다[24]. 따라서 악의적 사이버 공격을 행하는 국외의 행위자를 저지 할 수 있는 국가의 능력을 강화함으로써 강력한 사이버보안 태세를 통해 미국의 평화를 유지할 것이라고 주장한다. 한편, 보고서는 향후 국토안보부를 중심으로 미국의 국가 사이버보안 체계를 확립하고 사이버보안을 총괄할 것이라고 밝히고 있으며 국토안보부가 사이버보안 관련 연방기업들을 관리, 감독하는 중앙허브 기관으로써 적극적으로 기능할 것이라고 설명하고 있다[22]. 보고서는 기반시설을 보호하기 위한 우선순위 조치(Priority Actions)로 1) 책임과 의무 개선, 2) 국가위험 식별에 따른 우선순위 결정 3) 사이버보안 기능 제공자로서 정보통신 기술 제공업체 활용, 4) 미국의 민주주의 보호, 5) 사이버보안 투자증진, 6) 연구 및 개발 투자 우선순위 결정, 7) 운송, 해상, 우주공간의 사이버보안 개선을 꼽았다.

Table 2. National Cyber Strategy 2018

Pillar	Goal and Objective
Protect the American people, the homeland and the American way of life	• Secure federal networks and information • Secure critical infrastructure • Combat cybercrime and improve incident reporting
Promote American property	• Foster a vibrant and resilient digital economy • Foster and protect U.S. ingenuity • Develop a superior cyber security workforce
Preserve peace through strength	• Enhance cyber stability through norms of responsible state behavior • Attribute and deter unacceptable behavior in cyberspace
Advance American influence	• Promote an open, interoperable, reliable and secure internet • Build international cyber capacity

3.1.4 사이버보안 및 기반시설보호를 위한 전문기관 설립법 (CISA, Cybersecurity and Infrastructure Security Agency Act of 2018)

'사이버보안 및 기반시설보호를 위한 전문기관 설립법'은 2018년 11월에 트럼프 대통령의 최종승인으로 채택되었다. 이 법안은 2002년에 제정된 국토안보법(Homeland Security Act)[6]을 개정한 것으로 국토안보부 내 국가보안 프로그램국(NPPD, National Protection and Programs Directorate)을 사이버보안 및 기반시설보호를 위한 전문기관(CISA, Cybersecurity and Infrastructure Security Agency)[25]으로 승격하여 사이버보안을 담당하는 새로운 조직으로 창설한다는 내용을 포함하고 있다. 전문가들은 이 법안 통과의 의미에 대하여 다음과 같이 설명하고 있다. 첫째, 사이버보안에 대한 국토안보부의 리더십이 강화될 것이다. 법안 개정을 통해 국가보안 프로그램국이 연방기관으로서 권한을 부여 받으면 향후 더 많은 정책자금을 운용할

6) 2002년 11월에 제정된 국토안보법은 2001년 9.11테러 이후 미국 본토를 다양한 위협으로부터 보호하기 위한 제도적 장치의 정비를 주요 내용으로 하고 있다. 이 법을 근거로 2003년 3월 국토안보부가 신설되었으며, 기존에 여러 연방 부처와 기관에 산재되어 있던 비대칭, 재래식 위협, 보안, 재해, 재난, 국경 출입 및 모든 국토안보기능과 관련 업무가 국토안보부로 집중 및 이관되었다. 이후 국토안보부는 사이버 테러 및 위협 방지의 필요성을 인식하고 2005년, 2007년에 조직개편으로 국가보호 프로그램단을 통해 사이버보안 관련 업무를 수행해 왔다[28,29].

수 있고 관련 정부조직에 업무지시를 적극적으로 요청할 수 있게 된다[26]. 둘째, 국가보안 프로그램국이 적극적으로 정부기관과 민간조직·기업과의 조정을 담당하게 됨으로써[27] 국토안보부의 사이버보안 임무와 역할이 확대·강화되고 궁극적으로는 미국의 국가 사이버보안을 전적으로 국토안보부가 담당하게 될 것이다.

3.2 트럼프 행정부 주요기반시설 사이버보안 정책의 특징과 평가

3.2.1 내용적 특징

트럼프 행정부는 오바마 행정부의 주요기반시설의 사이버보안을 강화하려는 노력이 당대에는 효과적이었을지라도 사이버공간의 특성상 정책의 변화와 업데이트가 필요하다고 인식했다[18]. 트럼프 행정부는 주요기반시설을 포함한 사이버보안 전략을 발표하면서 현재 당면한 새로운 위험들을 관리 가능한 수준으로 낮추어 효과적으로 방어하는 것이 목표이라고 설명한 바 있다[18]. 이러한 트럼프 행정부의 주요기반시설의 사이버보안 강화정책을 가장 구체적으로 살펴볼 수 있는 보고서는 국토안보부의 사이버 보안전략보고서[19]이다. 본 보고서의 내용적 특징은 다음과 같다. 첫째, 민간부문의 광범위한 참여와 협력을 다루고 있다. 본 전략은 모든 목표와 세부조치에서 사이버보안 위험을 공동으로 해결하기 위해 민간영역의 참여와 연계를 다루고 있으며 정부부처와 민간과의 향상된 정보공유 체계를 다루고 있다. 또한, 국토안보부가 주요기반시설 관련 이해관계자들과 사이버보안 정보를 수집, 분석, 공유하기 위해 자동화 된 메커니즘을 어떻게 구축하고 확장할 것인지에 대해 설명하고 있다. 그러나 사이버 위협상황 시 정부가 요청할 경우 민간은 신속하게 정보를 기밀 해제하고 정부에게 제공해야 할 필요성을 설명하고 있다. 둘째, 현시점에서 주요기반시설이 당면한 새로운 사이버위협을 지적하고 해결방안을 모색하고 있다. 대표적으로 사물인터넷(IoT, Internet of Things)보안을 다루고 있는데 보고서는 2020년까지 200억 개가 넘는 장치가 인터넷에 연결될 것으로 예상하고 있으며 이것이 새로운 보안 문제를 야기하고 중요한 국가위험을 초래할 수 있다고 언급한다. 따라서 연결된 디바이스의 소프트웨어 및 하드웨어 구성요소의 잠재적 위험을 완화할 필요성을 강조하고 있으며 공급망 위험을 완화하기 위한 추가적인 임무를 설명하고 있다. 셋째, 사건발생 후 적극적 대응을 위한 높은 신뢰관계 구축에 대해 다루고 있다. 국토안보부는 민간영역과의 신뢰할 수 있는 관계를 구축하여 자발적으로 사건을 보고하고 피해자 통보를 강화하고자 한다. 이를 통해 잠재적 피해자에게 사이버사건을 알리는 일관된 프로세스를 개발할 것을 담고 있다. 마지막으로, 회복력 있는 네트워크 육성 및 공급망 확보를 다루고 있다. 보고서는 최근 발생한 대부분의 사이버사건이 소프트웨어나 하드웨어의 취약성과 관련되어 있음을 지적하면서 네트워크 사업자가 상용제품의 공급업체에 의존하고 있음을 설명한다. 국토안보부는 정보기술, 통신, 사이버보안 서비스 및 기타 커뮤니티와 협력하여 보안인식을 장려하고 취약성을 최소화하며 공급망 위험해결과 같은 사이버 보안성과를 실현할 것을 주요 내용으로 담고 있다[19].

3.2.2 추진 체계적 특징

트럼프 행정부 취임 이후 사이버보안 관련 추진체계가 백악관에서 국토안보부로 다시 이전되면서[7] 상대적으로 국토안보부의 역할과 권한이 더욱 강화되었다. 미국의 보안 전문가들은 주요기반시설과 관련한 미국의 사이버보안 전략 추진체계가 국토안보부가 강조하는 주요 개념 중의 하나인 노력의 통합개념(Unity of effort)에 맞추어져 있다고 설명한다[30]. 노력의 통합 개념은 미국 국토안보부가 모든 재난에 적용 가능한 통합재난관리를 위해 제시한 다섯 가지 핵심원칙중의 하나로[31][8] 보다 통일된 방식으로 업무를 수행할 수 있는 환경을 설정하기 위한 업무체계 방식이다. 전 국토안보부 장관 제이 존슨(Jeh Johnson)은 노력의 통합개념이 부서 전체의 전문성과 자원을 집중하여 다양한 임무를 효과적으로 수행 할 수 있게 하는 가장 효율적인 방법 중의 하나라고 설명한바 있다[32]. 이러한 노력의 통합적 접근은 연방정부 부처들과의 일관된 목표수행뿐만 아니라 국토안보부에 사이버보안 기능을 집중시켜 일관되

7) 부시 행정부에서는 실무부처들이 사이버보안 관련 소관업무를 담당하는 가운데 신설된 국토안보부가 총괄기능을 수행하였다[5].

8) 그 외에 약속된 파트너십(Engaged Partnership), 계층적 대응(Tiered Response), 확장 가능하고 유연하며 적응 가능한 운영 능력(Scalable, flexible, and Adaptable Operational Capacities), 상시대응 준비(Readiness to Act)가 있다 [35].

고 효과적인 정책을 수행하고 민간 기업과의 적극적인 파트너십을 확대 및 강화하고자 하는 의도가 포함되어 있다[33]. 한편, 국토안보부의 역할을 확대하고 임무를 집중시키려는 의도는 트럼프 행정부에서 발표하는 여러 사이버보안 정책에서 반복적으로 확인할 수 있다. 2018년 9월에 발표된 미국의 국가 사이버전략은 국토안보부의 역할과 범위의 확대에 대해 설명하고 있다. 특히, 보고서는 미 국방성(DoD)과 미국 정보 커뮤니티(IC, U.S. Intelligence Community)시스템이 운영하는 네트워크를 제외하고는 국토안보부에 모든 역할을 집중시켜 연방기관과 기타조직들의 네트워크를 더욱 안전하게 보호할 것이라고 설명하고 있다. 이를 위해 필요시 국토안보부가 사이버보안 목적으로 대행정보 시스템에 접근할 수 있고 시스템 보호가 필요하다고 생각될 때는 직접 보호조치를 취할 수도 있다고 명시하고 있다. 또한, 해상, 운송, 우주와 관련 주요기반시설 보안 역시도 국토안보부가 맡게 될 것이라고 설명하고 있다[34]. 기존의 국토안보부내에서 사이버보안 관련 실무를 수행하던 국가보안 프로그램국을 사이버보안 및 기반시설보호를 위한 전문기관으로 승격시키는 법안을 통과시킨 것 역시 같은 의도로 파악할 수 있다.

3.2.3 범위적 특징

미 트럼프 행정부의 주요기반시설 사이버보안의 또 다른 특징은 범위 정의의 변화이다. 국토안보부 장관 닐슨(Kirstjen Nielsen)은 다음과 같이 말하고 있다[35].

"디지털 보안은 이제 개인 및 물리적 보안으로 수렴하고 있으며 사이버 적대국이 미국 전체 구조를 위협 할 수 있음이 분명하다....국토안보부는 보다 포괄적 사이버보안 전략을 채택함으로써 접근 방식부터 다시 생각하고 있다....우리는 특정 자산에 대한 방어를 넘어서 생각해야하며 대기업에서부터 주택 소유자에 이르기까지 모든 사람들에게 적들의 위험이 영향을 미치는 현실을 직면해야 한다. 우리의 전략은 국토안보부가 미국의 네트워크를 방어하고 새로운 사이버위협들이 존재하는 디지털 전장에서의 독창적인 역량을 활용하는 방법에 대해 설명하고 있다"

트럼프 행정부는 주요기반시설 범위의 정의를 국가 전반에 걸친 포괄적 범위로 새롭게 채택하였다. 이는 영국이나 EU에 비해서도 훨씬 더 포괄적인 정의이다[36]. 이러한 범위 정의의 확대는 주요기반시설에 대한 사이버보안이 특정자산과 시스템의 방어에 그치는 것이 아니라 그 위험이 시민 모두에게 영향을 미칠 수 있음을 전제로 주요기반시설에 대한 국가 역할의 중요성을 강조하고 있음을 의미하다. 트럼프 행정부의 주요기반시설 범위의 확대는 새롭게 다변화하는 사이버위협 상황에서 독창적 역량방안을 모색한 결과라 볼 수 있다[37].

IV. 결 론

4.1 오바마 행정부와 트럼프 행정부의 주요기반시설 사이버보안 강화정책 비교분석

트럼프 행정부에서 발표한 국가안보전략(NSS, National Security Strategy, 2017)[38], 국가 사이버전략(2018), 국방부 사이버전략(DoD Cyber Strategy, 2018)[39]을 살펴보면 외부에서 들어오는 사이버공격에 대한 국가의 대응방식, 사이버공간에 대한 국가의 안보관등 많은 부분에서 트럼프 행정부의 입장은 오바마 행정부와 그 기조를 명백히 달리하고 있다. 트럼프 행정부는 핵심 국정기조인 '미국우선주의'를 사이버공간을 포함한 국가 안보전략에도 최우선적으로 반영하고 있다.[9] 그러나 주요기반시설의 사이버보안 정책의 경우 오바마 행정부의 정책과 차별성을 두기 보다는 기존의 정책을 보완·개선하는 방향으로 진행되었다. 이것은 지난 8년간 사이버보안을 우선순위정책으로 두었던 오바마 행정부에서 정책을 수행한 전문 관료들과 국토안보부 조직의 견해가 적극적으로 반영된 정책 결과물이라고 할 수 있다.[10] 이러한 정책추진 방향아래 오바마 행정부와

9) 트럼프 행정부는 '국가안보전략'과 '국가 사이버 전략'에서 사이버공간에서 국가행위자들의 책임 있는 행위를 강조했으며, 부적절한 행동에 대해서는 대응수준에 그치는 것이 아니라 책임을 부과하겠다는 정책기조를 강하게 보여준다. 이렇듯 강력한 대응을 바탕으로 하는 억제적 정책기조는 2018년 9월에 발표된 미 국방부 사이버전략 보고서에도 동일하게 나타난다.

10) 트럼프 행정부의 국토안보부 사이버 보안전략의 경우 국방수권법 2017에 의해 만들어졌으며, 이 법안은 트럼프 행정부 취임 이전에 이미 통과되었다(2016년 12월 26일). 이 법안에 국토안보부 책임법(DHS Accountability Act)을 포함시키기 위해 국토안보부는 많은 노력을 해왔다. 국방수권법 2017년 법안이 통과된 이후 당시 국토안보부 장관인 제이 존슨은 언론을 통해 감사문을 기고하기도 했다[40]. 국방수권법에 따라 국토안보부의 사이버 보안전략은 90일내에 의회에 제출될 예정이었으나 새롭게 들어서는 트럼프

비교했을 때 트럼프 행정부의 주요기반 시설 관련 사이버보안 정책의 특징은 다음과 같다. 첫째, 정책추진체계의 변화로 백악관의 역할이 약화되고 국토안보부가 중심이 되어 국가 사이버보안 정책의 총괄기능을 수행하게 되었다. 오바마 행정부의 경우 기반시설 관련 사이버보안 정책은 물론 모든 국가 사이버보안 정책이 백악관을 중심으로 수행되었다. 그러나 트럼프 행정부는 점점 더 광범위해지고 복잡해지는 사이버환경을 관리하는 데 있어 통일되고 중앙 집중화 된 방식으로 임무를 수행할 수 있는 환경을 설정하여 정책임무의 효율성을 높이기 위해 국토안보부가 주요기반시설의 사이버보안 컨트롤타워로서 책임과 권한을 전적으로 부여하는 방식을 선택하였다.

둘째, 주요기반시설 범위의 정의를 확대함으로써 기반시설 사이버보안을 위한 정부의 역할과 임무범위를 확대하였다. 오바마 행정부 당시 주요기반시설의 범위정의는 상당히 제한적이었으며 이는 소극적인 정책추진의 결과로 이어졌다. 트럼프 행정부는 기반시설의 정의를 국가전반으로 확장함으로써 주요기반시설의 사이버보안 정책이 특정자산과 시스템 방어에 그치는 것이 아닌 포괄적이고 광범위한 국가의 역할로 이어져야 함을 강조하고 있다.

셋째, 정부가 민간 주요기반시설의 운영에 관여할 수 있음을 밝히고 있다. 트럼프 행정부는 국가사이버전략과 사이버 보안전략보고서를 통해 사이버 위협상황에서와 같이 국가가 필요할 경우 민간영역에 개입할 가능성과 필요성을 언급하고 있다. 오바마 행정부는 주요기반시설의 90퍼센트 이상을 차지하는 민간기업들과의 파트너십을 위해 사이버보안 논의의 대부분을 정부와 민간기업의 정보공유에 집중하였다. 그럼에도 불구하고 권고사항 수준의 행정명령, 법안제정(CISA, Cybersecurity Information Sharing Act 2015)에도 불과하기 제대로 실행되지 않는 정보공유와 민간협력[11]으로 정책효과가 미비하다는 평가를 받았다. 트럼프 행정부도 정부와 민간의 협력과 파트너십, 정보공유의 중요성을 여전히 강조하고 있다. 그러나 정부가 필요하다고 여길 경우 비록 민간영역의 주요기반시설이라 할지라도 개입의지를 밝힘으로써 자발적인 협력과 파트너십을 강조하는 것에서 유사시 정부의 정책을 강제하는 것으로 정책방향이 전환되었다.

4.2 연구결론 및 시사점

본 연구는 트럼프 행정부의 주요기반시설과 관련한 사이버보안 강화정책을 트럼프 행정부에서 발표한 행정명령, 정책보고서, 법안을 토대로 분석하였다. 요약하면, 트럼프 행정부의 주요기반시설 사이버보안 정책은 주요기반시설의 범위정의를 확대하여 국가의 책임과 역할을 강조하고 이를 수행하기 위해 기존에 주요기반시설의 사이버보안 임무를 담당했던 국토안보부에 정부의 책임과 권한을 최대한 집중시킨 것이라고 볼 수 있다.

오바마 행정부 당시 주요기반시설의 사이버보안에 대한 정책실패는 공공연하게 논의 되어왔으며, 책임기관을 국토안보부가 아닌 다른 기관으로 이전해야한다는 주장까지 거론되었다.[12] 따라서 오바마 행정부 이후 취임한 트럼프 행정부에서 발표한 주요기반시설의 사이버보안 관련 주요정책들은 기존의 비판에 대

행정부와의 의견조율을 위해 14개월 늦게 제출되었다. 한편, 전문가들은 '사이버보안 및 기반시설보호를 위한 전문기관 설립법'의 경우도 사이버보안 영역의 정부 권한을 통합하기 위한 국토안보부의 오랜 설득의 결과로 평가하고 있다[27].

11) CISA 2015 법안 통과이후 넥스트거브(Nexgov)의 조셉 막스(Joseph Marks)는 2018년 7월까지 오직 6개의 회사 및 기타 비영리 단체만이 정부와 데이터를 공유하고 있다고 보도했다. 보고에 따르면 당시 190개 민간기업과 약 60개의 연방기관은 사이버 위협 데이터를 공유하지 않고 있었다[27].

12) 오바마 행정부 당시 국토안보부는 사이버보안 관련 정책수행의 효과와 조직기능의 효율성에 있어 많은 의구심과 비판을 받아왔다. 대표적으로 미국의 주요 싱크탱크 기관으로 알려진 국제전략연구소(CSIS, The Center for Strategic and International Studies)의 사이버정책대책위원회(Cyber Policy Task Force)가 2017년 1월에 발표한 '제45대 대통령을 위한 사이버보안 의제 보고서'(From Awareness to Action - A Cybersecurity Agenda for the 45th President)가 있다. 이 보고서는 트럼프 행정부가 보다 나은 사이버보안 환경을 만들어나가는 데 있어서 활용 가능한 정책 및 자원, 조직의 정책이행에 대하여 구체적 비전과 목표를 제시하는 가운데 오바마 행정부 시기 사이버보안 영역의 선도 기관 역할을 했던 국토안보부를 강도 높게 비판하고 있다. 보고서는 국토안보부가 지난 10년간 미 행정부 사이버보안의 핵심기관이었지만 국가안전보장국(NSA, National Security Agency)와 비교했을 때, 그 노력이 충분하지 못하다고 평가한다. 사이버보안과 관련한 조직적 혁신이 이루어지지 않고 정책 역시도 제대로 작동하지 않는다면 이제는 사이버보안 기능의 핵심 역할을 국토안보부에서 다른 기관으로 옮길 때라고 보고서는 주장했다[41].

한 트럼프 행정부와 국토안보부의 고민을 여실히 담고 있다고 볼 수 있다.

한국의 경우 주요기반시설 정보통신망 및 정보시스템의 주요정보통신기반시설의 보호를 목적으로 2001년 정보통신기반 보호법을 제정하여 국가적 차원의 주요기반 보호체계를 구축하고 있다[1]. 이후 지속적으로 법 개정을 통하여 미비점을 개선하고 보완하며 운영되고 있으나 주요기반시설을 둘러싼 빠른 기술적 변화 양상을 감안할 때, 현재 한국이 주요기반시설에 관하여 탄력적인 운영을 하고 있다고 보기에는 어려운 측면이 많다. 정보통신기반보호법 수립 당시 23개였던 주요 정보통신 기반시설은 현재 385개로 확대되어 관리되고 있다. 점차 빨라지는 환경의 변화와 다양해지는 사이버 공격위험에서 한국의 주요기반시설에 대한 정책적 관리가 제대로 이루어지는가에 대해서는 많은 의구심이 들 수밖에 없다. 트럼프 행정부의 주요기반시설 관련 사이버보안 정책의 집중화된 정책이행방식, 임무와 범위의 확대, 보다 적극적인 정부의 역할, 빠른 인터넷 환경변화에 따른 정부정책의 시의성은 한국의 주요기반시설 관련 사이버보안 정책에도 많은 시사점을 제공할 수 있을 것으로 기대된다.

References

[1] Jiyeon Yoo and Nayoung Jeong, "A study on the policy direction of critical infrastructure risk response in the changing digital environment: a comparative study of the USA's policy," *Journal of Security Engineering*, 14(1), pp. 59-76, 2017.

[2] "NPPD, under the U. S. department of homeland security, is one of the nation's overall security officers," Boan News, https://www.boannews.com/media/view.asp?idx=58589, Dec. 13, 2017. [Retrieved from 6th July, 2019]

[3] U. S. Department of Homeland Security, "Factsheet: cybersecurity and infrastructure security agency," The Department of Homeland Security: Washington, DC., 2018.

[4] The White House, "Cyberspace policy review: assuring trusted and resilient information and communications infrastructure," The White House: Washington, DC., 2009.

[5] Eunji Song and Wonyoung Kang, "U. S. Obama administration's second term cybersecurity policy," Internet & Security Focus: KISA, 2014.

[6] "Obama's government manages cybersecurity directly," Etn News, http://www.etnews.com /20090211018 0, Feb. 12, 2009. [Retrieved from 6th July, 2019]

[7] "Cyber-attacks against U. S. government," Digital Times, http://cyberbureau.police.go.kr/board/boardView.do?board_id=cyber&id=3593&page=15&mid=030201, Feb. 18, 2009. [Retrieved from 11th July, 2019]

[8] U. S. Department of Homeland Security, "Blueprint for a secure cyber future: the cybersecurity strategy for the homeland security enterprise," The Department of Homeland Security: Washington, DC., 2011.

[9] B. H. Obama, "Executive order 13636: improving critical infrastructure cybersecurity," The White House: Washington, DC., 2013.

[10] B. H. Obama, "Presidential policy directive 21: critical infrastructure security and resilience (PPD-21)," The White House, Office of the Press Secretary: Washington, DC., 2013.

[11] Sangbae Kim, "International comparison of national cyber security strategies: examples of four countries around the Korean peninsula and three major European countries," Institute of International Studies at Seoul National University: Seoul, 2017.

〔12〕 "Obama's cyber legacy: he did (almost) everything right and it still turned out wrong," Nextgov, https:/ /www.nextgov.com/cybersecurity/2017/01/obamas-cyber-legacy he-did-almost-everything-right-and - it-still-turned-out-wrong/134612/, Jan. 27, 2017. 〔Retrieved from 2th August, 2019〕

〔13〕 "Obama's cybersecurity legacy: good intentions, good efforts, limited result," CSO, https://www.csoonline.com/article/3162844/security/obamas - cybersecurity - legacy - good- intentions-good - efforts-limited-results.html, Apr. 2, 2017. 〔Retrieved from 27th July, 2019〕

〔14〕 "Obama's cybersecurity plan is mean to secure his legacy," WIRED, https://www.wired.com/2016/02/obamas-cybersecurity - plan-is - meant-to-secure-his-legacy/, Feb. 10, 2016. 〔Retrieved from 11th August, 2019〕

〔15〕 "Sidetracked: Obama's cybersecurity legacy," World Politics Review, https://www. world politicsreview.com/articles/17468/sidetracked- obama-s-cybersecurity-legacy, Dec. 15, 2015. 〔Retrieved from 11th August, 2019〕

〔16〕 D. J. Trump, "Executive order 13800: strengthening the cybersecurity of federal networks and critical infrastructure," The White House: Washington, DC., 2017.

〔17〕 "White house issues cybersecurity order," Norton Rose Fulbright: Data Protection Report, https://www.dataprotectionreport.com/2017/05/ white-house-issues-cybersecurity-order/, May. 11, 2017. 〔Retrieved from 2th August, 2019〕

〔18〕 "Trump administration plans a new cybersecurity strategy," Boan New, https:// www.boannews.com/media/viewasp?idx =57811, Nov. 1, 2017. 〔Retrieved from 12th July, 2019〕

〔19〕 U. S. Department of Homeland Security, "U. S. department of homeland security cybersecur ity strategy," The Department of Homeland Security: Washington, DC., 2018.

〔20〕 "Many DHS 'unity' initiatives to continue under 2017 NDAA," Federal News Network, https://federalnewsnetwork.com/ legislation/2016/12/many - dhs-unity - initiatives - continue-2017-ndaa/, Dec. 27, 2016. 〔Retrieved from 12th July, 2019〕

〔21〕 U. S. Congress, Public Law 114 - 328, "National Defense Authorization Act for Fiscal Year 2017," The US Congress: Washington, DC., 2016.

〔22〕 D. J. Trump, "National cyber strategy of the United States of America," The White House: Washington, DC., 2018.

〔23〕 "President Trump releases national cybersecurity strategy," Becker's Hospital Review, https://www. beckershospital review. com/hospital-management - adminis tration/president-trump - releases - national - cybersecurity - strategy.html, Sep. 24, 2018. 〔Retrieved from 3th August, 2019〕

〔24〕 "Trump launches new national cyber strategy," AXIOS, https:// www.axios.com/ trump-national-cyber-strategy-9b6604a1-2521-4543-8d61-64c0f785e118.html, Sep. 21, 2018. 〔Retrieved from 2th August, 2019〕

〔25〕 U. S. Congress, Public Law 115-278, "Cybersecurity and Infrastructure Security Agency Act of 2018," The US Congress: Washington, DC., 2018.

〔26〕 "US cybersecurity and infrastructure agency: Trump signs bill to place new agency under DHS," Hashed Out. https://www. thesslstore. com/blog/us-cybersecurity-and-infrastructure-agency-trump-signs-bill-to-place-new-agency-

under-dhs/, Nov. 19, 2018. [Retrieved from 5th August, 2019]

[27] "The cybersecurity 202: Trump set to make a new DHS agency the top federal cyber cop," The Washington Post, https://www. washingtonpost.com/ news/powerpost/paloma/ the-cybersecurity202/2018/11/16/the-cybersecurity-202-trump-set-to-make-a-new-dhs-agency-the-top-federal-cyber-cop/ 5bedb9a71b326b3929054867/?utm_term=.92c3b366fd3e, Nov. 16, 2018. [Retrieved from 2th August, 2019]

[28] Taeyong Yoon, "Border security system and the role of national intelligence," *The Korea Association of National Intelligence Studies,* (6)1, pp. 85-128, 2012.

[29] Sanghyun Lee, "Cybersecurity laws in the U. S.: focusing on responses from the legislative, the judicial, and the executive body," *Internet and information Security*, (3)1, pp. 109-131, 2012.

[30] "Unity of effort key to DHS' new cybersecurity strategy," Federal News Network, https://federalnewsnetwork.com/hearings-oversight/2018/05/unity-of-effort-key-to-dhs-new-cybersecurity-strategy/, May. 15, 2018. [Retrieved from 8th March, 2019]

[31] LIG consulting, "A study on the operation of the central countermeasures headquarters and establishment of the role system," The Ministry of Public Administration and Security: Seoul, 2011.

[32] "Ali Mayorkas on leading a unity of effort at DHS," Govloop, https://www. govloop. com/ community/blog/ali-mayorkas-leading-unity-effort-dhs/, Oct. 26, 2015. [Retrieved from 8th March, 2019]

[33] "Reform agenda for the department of homeland security," Forbes, https:// www. forbes.com/ sites/realspin/2017/01/27/reform-agenda-for-the-department-of-homeland-security/#7d416ed62a31, Jan. 27, 2017. [Retrieved from 6th April, 2019]

[34] "New national cyber strategy message: deterrence through U. S. strength," Government Technology, http://www. govtech.com/ blogs/lohrmann-on-cybersecurity/new-national-cyber-strategy-message-deterrence-through- us-strength.html, Sep. 29, 2018. [Retrieved from 6th April, 2019]

[35] National Disaster Management Research Institute, "Research topics on developing the national intergrated resonse system in Korea - Focused on emergency response," National Disaster Management Research Institute: Seoul, 2009.

[36] "DHS releases its cybersecurity strategy," Wiley Rein, https:// www. wileyrein.com/ newsroom-articles-DHS_Releases_Its_ Cybersecurity _ Strategy.html, May. 16, 2018. [Retrieved from 4th August, 2019]

[37] "US department of homeland security unveils new cyber security strategy," Computing, https://www.computing.co.uk/ctg/news /3032492/us-department-of-homeland-security-unveils-new-cyber-security-strategy, May. 17, 2018. [Retrieved from 4th August, 2019]

[38] The White House, "National security strategy of the United States of America," The White House: Washington, DC., 2017.

[39] U. S. Department of Defense, "Cyber strategy," The Department of Defense: Washington, DC., 2018.

[40] "DHS on the passage by congress of the FY 2017 NDAA (Learn More)," American Security Today, https://americ

an security today.com/ dhs-passage-congress - fy-2017-ndaa-learn/, Dec. 27, 2016. [Retrieved from 6th April, 2019]
[41] "A cybersecurity agenda for the 45th president," Center for Strategic & International Studies, https://www.csis.org/news/cybersecu rity-agenda - 45th-president, 2017. [Retrieved from 22th December, 2018]

〈저자소개〉

김 근 혜 (Geunhye Kim) 정회원
2009년 2월: 이화여자대학교 정치외교학과 학사(정치학사)
2011년 2월: 이화여자대학교 정치외교학과 석사(정치학석사)
2019년 2월: 고려대학교 정보보호대학원 (공학박사)
2019년 4월~현재: 고려대학교 정보보호대학원 연구교수
〈관심분야〉 개인정보보호정책, 사이버국방 및 안보정책, 정보보호정책, IT융합정책