Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.1, Feb. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.1.123

미국 사이버보안 인력 양성 법·규정 분석을 통한 국내 법·규정 개선 방안 연구

홍 순 좌,[1†] 김 준 수[2‡]
[1,2]ETRI 부설연구소(책임연구원, 실장)

A Study on the Laws and Regulations in Korea through the Analysis of Cybersecurity Workforce Developing Laws and Regulations in U.S.

Soonjwa Hong,[1†] Joonsoo Kim[2‡]
[1,2]The Attached Institute of ETRI(Principal Researcher, Manager)

요 약

1987년 컴퓨터보안법에서 연방기관 인력의 컴퓨터보안 인식 및 실무 훈련을 의무화한 것이 미국의 사이버보안 인력 양성 정책의 시작이라고 볼 수 있다. 법률 제·개정이 곤란한 경우, 인사관리처(OPM) 규정과 예산관리국(OMB) 회람 등을 통해 인력 양성 정책을 강화해왔다. GISRA 2000, FISMA 2002 법률이 10여 년간 사이버보안 인력 양성에 대한 중심 역할을 수행했다. 이후 기술 발전 및 정책적 보완 필요성으로 FISMA 2014를 제정하였으며, 사이버보안 인력에 대한 법률은 2차례에 걸쳐 제정하는 등 미국 연방기관에서 사이버보안 인력의 중요성이 더욱 증대되었다. 미국 사이버보안 인력 양성 법·규정 등의 검토·분석을 통해 인력양성의 핵심 비교 항목을 도출하여 우리나라의 법·규정과 비교하여 개선방안을 제시하고자 한다.

ABSTRACT

In 1987, Computer Security Act was enacted, requiring computer security awareness and practical training for federal workforce. This is the beginning of US development of federal cybersecurity workforce. It has been strengthening the development of federal cybersecurity workforce policy by establishing OPM regulations and OMB circulation in cases where it is difficult to define by law. Through GISRA 2000 and FISMA 2002, which has been improved, it played a central role for development of federal cybersecurity workforce for more than 10 years. Since then, FISMA 2014 has been enacted as a necessity for supplementing technology and policy. In 2014, the importance of cyber security personnel in US federal agencies has been increased even more, by enacting a single law on cybersecurity workforce twice. We will review the current state of Korea's development of cybersecurity workforce by reviewing and analyzing the development and federal cybersecurity workforce in the United States.

Keywords: Computer Security Act, FISMA 2002&2014, Federal Cybersecurity Workforce Assessment Act

I. 서 론

미국의 사이버보안 관련 법률은 1987년 컴퓨터보안법을 시작으로 약 25종 이상의 법률이 제정되어 시행되고 있다[1]. 이러한 법률들은 국가차원의 사이버보안 역량 제고를 위해 조직 강화, 예산 책정 등 정책적인 추진이 가능한 기반을 제공하며 백악관 예산관리국(Office of Management and Budget,

Received(11. 07. 2019), Modified(01. 03. 2020), Accepted(01. 03. 2020)

† 주저자,hongsj@nsr.re.kr
‡ 교신저자, joonsoo@nsr.re.kr(Corresponding author)

OMB), 국토안보부(Department of Homeland Security, DHS), 인사관리처(Office of Personnel Management, OPM), 국립표준기술연구소(National Institute of Standards and Technology, NIST)를 중심으로 연방기관들이 적극적으로 참여할 것을 의무화하고 있다.

본 논문은 이와 같은 사이버보안 법률들을 검토하여 인식제고(awareness), 훈련(training), 교육(education) 등이 규정된 법조항을 기반으로 사이버보안 인력 양성에 연관된 법을 식별하였으며, 이와 관련하여 연방기관 재직인력에 대한 인사관리에 연관된 OPM 규정, 정책 집행에 요구되는 OMB 회람(circular) 등을 함께 검토하였다.

사이버보안은 IT와 함께 발전해 온 분야이므로 컴퓨터 및 네트워크의 등장을 통해 사회적으로 활용되기 시작한 1980년대를 그 시점으로 보는 것이 누구에게나 보편적인 개념이라고 생각된다. 사이버보안에 관한 미국 연방 법률을 살펴보면 비밀을 소통할 수 있도록 암호(cryptography)가 포함된 "국가보안시스템(national security system)"은 별도 법률 및 규정으로 통제한다고 밝히고 있으며, 법·규정 등을 살펴보면 사이버보안 분야에서 암호를 포함하지 않는 것이 일반적이다[2]. 이러한 근거가 미국에서 암호기술 분야 인력양성 분야는 별도로 다루어지며 국가차원의 사이버보안 분야 인력양성에서는 제외한다고 할 수 있다.

미국의 경우 사이버보안의 명칭이 정립되기까지 1980년대에는 컴퓨터보안, 네트워크 보안이 사용되었고, 1990년대에는 IT 용어의 등장과 더불어 정보보안, 정보보증(information assurance) 등의 용어가 사용되었으며, 90년대 후반기 인터넷의 등장 및 초고속인터넷의 발전에 따라 정보전(information warfare)이라는 새로운 용어가 등장하였다. 사이버보안(cybersecurity)이 2000년대에 들어서서 법률에서 공식적으로 처음 등장하였으며, 이후 모든 국가 법·제도·정책 문서의 포괄적인 용어로 정착되어 사용되고 있다. 우리나라의 경우에도 더 이상 혼란을 주지 않도록 용어에 대한 재정립이 필요하다[3].

또한 미국의 법률을 살펴보면 기본적으로 사이버보안은 연방기관의 정보시스템 또는 IT 시스템을 보호하는 것을 목적으로 하고 있으며, IT 전문능력을 갖춘 인력이 사이버보안 전문인력이 되는 것이 기본이다. 우리나라의 경우 IT와 사이버보안이 별개 교육과정으로 편성되는 경향이 있으나, 기본적으로 IT 능력을 갖춘 인력에게 사이버보안 능력을 갖출 수 있도록 하는 연계 교육과정이 요구된다고 할 수 있다. 우리나라와 대조적으로 미국의 경우 IT 교육과정을 이수한 인력을 기반으로 사이버보안 과정을 이수하도록 하는 방식이 기본적 방식으로 정착되었다고 볼 수 있다.

사이버보안 인력양성에 관련하여 식별된 법률 8종, 규정 4종은 Table 1.과 같다.

사이버보안 인력 양성에 대해서는 연구 주체에 따라 다양한 관점이 존재한다. 교육 연구자들은 중-고-대학교 교육과정 개선 관점에서 접근하여, 정보보호 전공 학과의 교과목 개선[3,4,5]이나 산업체 직무에 적합한 교육과정 설계[6,7,8] 등의 제안을 한다. 정책 및 법-제도 연구자들은 국가차원의 포괄적인 사이버보안 정책 관점에서 접근하여[10,11], 4차 산업시대를 대비한 사이버보안 전문인력 양성의 중요성을 개념적 차원에서 강조하고 있다.

하지만, 이러한 개념적 주장이 국가차원의 체계적인 인력양성 방법론 모색을 위한 실질적 논의로 이어지지 못하고 있는 것이 우리의 현실이다. 이는 여러 가지 원인이 있으나, 그 중에서도 국가차원의 정책적인 노력이 부족함이 가장 큰 원인이다. 국가차원의 정책적인 노력은 법률로 규정되어야 가장 큰 실천력

Table 1. Laws and regulations related Cybersecurity workforce development in U.S.

Year	Acts
1987	Computer Security Act of 1987
1992	OPM Federal personnel regulations 5 CFR Part 930 Revision
1996	OMB Circular A-130
2000	Government Information Security Reform Act(GISRA 2000)
2002	Federal Information Security Management Act(FISMA 2002)
2004	OPM Federal personnel regulations 5 CFR Part 930 Revision
2014	Federal Information Security Modernization Act(FISMA 2014)
	Cybersecurity Workforce Assessment (CWAA 2014)
	Cybersecurity Enhancement Act of 2014
2015	Federal Cybersecurity Workforce Assessment Act(FCWAA 2015)
2017	OPM Government-wide Cybersecurity Data Standard Codes
2018	Cybersecurity and Infrastructure Security Agency Act of 2018(CISA 2018)

이 보장되는 것이 국가의 기본이므로 우리나라도 이에 대한 노력이 필요하다. 이를 위해서 전 세계적으로 가장 체계적인 사이버보안 인력양성을 위한 노력을 추진해온 미국의 연방 법률을 살펴보고 국내 법률 체계와의 비교를 통해서 사이버보안 인력 양성 법률 체계 개선방안을 살펴보는 방법이 가장 효과적이라 할 수 있을 것이다.

본 논문에서는 미국 연방 사이버보안 인력양성 관련 법·규정 12종을 기반으로 국내 사이버보안 인력양성 관련 법·규정을 상호 비교한다. 이와 같은 관점에서 접근 방법의 기존 연구에서 없었던 관계로 새로운 비교·분석 방법을 제안하고 국내 법·규정의 발전 방안을 제시한다. Ⅱ장에서는 12종의 법·규정에 대해 사이버보안 인력양성 관련한 세부 내용을 살펴본다. Ⅲ장에서는 12종의 법·규정의 특성을 분석하여 비교 그룹·항목을 식별 및 도출하여, 이 기준에 근거하여 12종의 법·규정을 분류해 본다. Ⅳ장에서는 사이버보안 인력양성에 대한 국내 법·규정을 식별하고 앞서 도출된 비교 항목을 기반으로 비교해 본다. 이를 통해서 국내 법·규정 관점에서의 국가 사이버보안 인력양성 법·규정의 미흡한 부분을 식별하여 발전 방향을 제시한다. 마지막으로 Ⅴ장은 결론으로 마무리한다.

Ⅱ. 미국 사이버보안 인력양성 법·규정 현황

2.1 2000년 이전 시대(1987년~1999년)

1980년대는 애플 I, II의 등장을 통해 개인 PC의 서막을 여는 시대였으며, 마이크로소프트 DoS 운영체제와 결합된 IBM PC는 기존 중앙집중식 대용량 메인프레임 중심을 개인으로 이동하는 IT 시대의 신기원이라고 할 수 있다. 1990년대는 마이크로소프트 윈도우즈의 독점적 지위 확보, 인터넷의 대중화와 웹의 개발 및 보편적 사용이 등장한 시대로서, 이 시기는 인터넷의 대중화를 통해 정보보안 시대를 열었던 때로 볼 수 있다[1].

2.1.1 컴퓨터보안법(1987)[12]

1987년 미국 연방의회는 사이버보안 법률의 시초라 할 수 있는 컴퓨터보안법을 제정하였다. 이 법에서 다루는 주요내용은 연방기관이 중요한 정보를 보호하기 위한 기본적인 사이버보안 조치를 취하도록 보장하기 위해 제정되었다.

이 법률에서 NIST는 연방기관에서 사용되는 컴퓨터보안에 관한 프로그램을 제공함과 동시에 연방정부 컴퓨터 시스템의 운영에 관계되는 연방기관 직원 훈련을 목적으로 하고 있다. 컴퓨터보안법은 법률로서 연방기관 인력에 대해 사이버보안 훈련을 실시할 것을 처음으로 규정하였다는 의미를 갖고 있다. 이 법은 2002년 연방정보보안관리법(FISMA 2002)으로 대체되었다[1].

이 법에 의거하여 모든 연방기관은 컴퓨터 시스템을 다루는 직원에게 컴퓨터보안 인식(awareness), 컴퓨터보안 실습(practice)을 주기적으로 실시할 것을 의무화하였다. 즉, 이법에 의거하여 연방기관 직원들을 대상으로 사이버보안(컴퓨터보안) 훈련 의무화를 시작하였으며, NIST와 OPM이 협의하여 연방기관의 컴퓨터보안 훈련에 대한 가이드라인의 개발 및 지원하는 것을 규정하였다.

2.1.2 OPM 연방규정 일부 개정(1992)

연방기관 인력을 종합적으로 관리하는 OPM은 1992년에 연방인사규정인 "Federal personnel regulations, 5 CFR Part 930, "Employees Responsible for the Management or Use of Federal Computer Systems"을 공표하였다. 이 규정에서 컴퓨터보안법에 의거한 컴퓨터보안 훈련 가이드라인에 따라 훈련을 제공할 것을 규정하고 있다. 또한 이 가이드라인 세부내용의 시행에 대해 연방정부 규정으로 명문화 및 의무화 하였다[13].

이 규정의 훈련 대상자는 다음과 같다.

> o 현 직원 및 고용 후 60일 이내인 신입직원
> o 기관의 IT 보안환경 및 절차에 심각한 변화에 직면 하거나 민감한 정보를 다루는 새로운 직무를 맡은 직원
> o 정보의 민감도에 따른 주기적인 훈련이 요구되는 직원

1990년 초, 사이버보안 훈련에 대한 정책 추진상황을 보면, 우선 컴퓨터보안법으로 사이버보안 훈련을 의무화하였고, NIST는 관련한 컴퓨터보안훈련 가이드라인(NIST SP 500-172, 1989)을 발표하였다. 이것은 OPM이 가이드라인의 강제화를 위해 연방규정으로 공식화한 것을 의미하며, 이때부터 NIST는 IT 또는 사이버보안 분야에서 표준화의 한계를 인식하고 가이드라인으로 기술변화에 대응하는

전략을 추진해 왔다고 볼 수 있다. 우리나라도 정책에 있어 의회, 정부 및 NIST의 사이버보안 정책 추진방법을 검토하여 장점을 도입할 필요가 있다고 생각된다.

2.1.3 OMB 회람 A-130 (1996)

OMB Circular A-130, 연방정보자원관리(management of federal information resources) 부록 Appendix Ⅲ내의 연방자동화정보자원보안(security of federal automated information resources) 절에서 NIST에게 컴퓨터보안훈련 가이드라인을 업데이트 하도록 명령하고 있다[13].

> - page 17 -
> a. Department of Commerce. The Department of Commerce, through NIST, is assigned the following responsibilities consistent with the Computer Security Act. ・・・
> 2) Review and update, with assistance from OPM, the guidelines for security training issued in 1988 pursuant to the Computer Security Act to assure they are effective.

컴퓨터보안법이 최신 IT 기술을 반영하지 않고 있으므로 OMB Circular A-130를 개정하여 신속하게 조치하는 방식을 채택하고 있다.

2.2 2000년대(2000년~2009년)

이 시기는 인터넷 대중화를 넘어서 초고속 인터넷과 모바일 기술의 보급이 시작되는 시대로서 사이버공간이 국가 안보의 중요한 영역으로 인식되었으며, 각국은 국가 역량 강화의 일환으로 사이버보안을 인식하기 시작하였다.

2.2.1 정부정보보안개혁법(GISRA 2000)[14]

정부정보보안개혁법(Government Information Security Reform Act, GISRA 2000)은 연방기관의 기관장에게 소속 직원들 훈련을 의무화하며, 최고정보책임자(Chief Information Officer, CIO)에게 책임을 부여하고 있다. CIO는 정보보안 중요 책임자를 지정하여 직원들에 대한 훈련을 책임지고 감독하는 권한을 규정하고 있다. 또한 정보보안 위험에 연관된 인력과 기관의 정책과 절차를 준수해야 하는 인력에게 반드시 보안 인식 훈련을 시킬 것을 규정하고 있다.

이 법에서 NIST의 역할과 책임을 다음과 같이 구체적으로 강화하였다.

> o 보안시스템 및 검증 프로그램을 위한 방법 및 기술 개발을 포함하여 연방정보시스템 보안을 위한 표준 및 지침을 개발, 발행, 검토 및 보완한다.
> o 컴퓨터 보안 인식 및 컴퓨터 보안 실무 교육을 위한 지침을 개발, 발행, 검토 및 보완하며, OPM의 도움을 받는다.
> o 해당 기관의 응용 프로그램 및 시스템 보안 계획 개발에 도움이 되는 보안 계획 지침을 기관에 제공한다.
> o 다른 시스템과 상호 연결될 때 효율적인 통제와 관련하여 기관에 지침과 지원을 제공한다.
> o IT 시스템의 보안 취약성을 평가하고, 그러한 취약성이 확인된 즉시 연방 기관에 알려준다.

또한 이 법률에서 OPM의 역할과 책임을 다음과 같이 구체적으로 명시하고 있다.

> o 연방 직원을 위한 컴퓨터 보안 교육에 관한 인사관리규정을 검토 및 보완한다.
> o 컴퓨터 보안 인식 및 컴퓨터 보안 모범 사례에 대한 교육 지침을 보완하고 유지 관리하는 데 있어 상무부(NIST를 의미)를 지원한다.
> o 연방정부가 지원하는 인력 및 훈련 계획을 보장하기 위해 인력 및 훈련 이니셔티브(법에 의해 허가된 장학금·동호회 포함)를 제공한다.
> o 직원에게 제공되는 지속적인 정보보안 교육 및 훈련의 적절한 자원을 보유하고 있어야 한다.
> o 기관의 요구를 충족시킬 수 있는 자격을 갖춘 정보보안 전문가(프로페셔널)를 적절하게 확보해야 한다.

2.2.2 연방정보보안관리법(FISMA 2002)[15]

일반적으로 2001년 9.11은 미국의 안보체계와 사이버보안을 강화하는 21세기 가장 중요한 사건으로 알려져 있다. 국토안보부의 설립의 근거인 국토안보법(2002)과 함께 제정된 연방정보보안관리법(Federal Information Security Management Act of 2002, FISMA 2002)은 미국 연방기관의 사이버보안을 강화한 기본적인 법으로 자리매김하게 되었다. 이 법은 전자정부법(E-Government Act of 2002)의 부속절인 Title III(Information Security)을 지칭하는 것이다. FISMA 2002는 모든 연방기관이 최소한의 기본적인 사이버보안 조치를 취하기 위한 것이며, 이 법에서도 NIST를 연방기관 시스템 보안을 위해 사용되는 보안 가이드라인 및 지침을 개발하는 기관으로 지정하였다.

NIST is responsible for **developing standards and guidelines**, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems.

FISMA 2002에는 NIST의 임무와 권한 등을 좀 더 세부적으로 규정하는 특징이 있으며, 이 법을 통해 NIST는 사이버보안 분야의 가장 중요한 책임기관으로 자리 잡게 되었다고 할 수 있다.

5번째 섹션인 연방기관의 책임에서 재직 직원에 대한 교육 및 훈련을 다음과 같이 규정하고 있다.

(a) IN GENERAL-각 기관장은 다음을 수행해야 한다.
(4) 기관장은 본 절의 요구사항 및 관련 정책, 절차, 표준 및 지침을 준수 할 수 있도록 충분한 훈련을 받은 인원을 확보해야 한다.
(b) AGENCY PROGRAM
(4) 기관의 운영 및 자산을 지원하는 정보시스템의 계약자 및 기타 사용자를 포함한 인원에게 정보를 제공하는 보안 인식 훈련(security awareness training)
(A) 그들의 활동과 관련된 정보 보안 위험
(B) 이러한 위험을 줄이기 위해 고안된 기관 정책 및 절차를 준수할 책임

2.2.3 OPM 연방규정(CFR) 일부 개정(2004)

FISMA 2002에 의거하여 정보보안 인식과 훈련 요구사항을 반영한 NIST SP 800-50을 2003년 발표하였다. 이를 기준으로 2004년 6월 OPM은 연방 인사규정을 개정하였다. 이 규정(5 CFR Part 930.301)은 "정보 시스템을 관리 또는 사용하는 직원에 대한 정보보안 책임"을 부여하고 연방기관이 가이드라인에 명시된 훈련을 제공할 것을 규정하고 있으며, 주요 요구사항은 다음과 같다[16].

o 정보보안 인식 및 훈련 계획 수립.
o 중요한 정보보안 책임이 있는 직원을 식별하고 NIST 표준 및 가이드라인에 따라 역할 별 훈련을 제공
o 매년 한번 이상 연방정보시스템의 사용자에게 정보보안 인식자료를 볼 수 있도록 조치
o 다음 재직자에게 훈련을 제공
- 경영진, CIO, , 프로그램 및 기능 관리자
- 정보보안 프로그램 관리자, 감사자, 기타 보안 관련 직원
- IT 기능 관리 및 운영 인력
o 조직의 정보시스템에 대한 접근을 허용하기 전 모든 신규 직원에게 정보보안 인식·훈련 제공
o 직원이 사용·처리하는 정보 민감성을 기반으로 기관에서 결정한 주기에 따라 직원에게 정보보안 훈련을 제공
o 기관 정보시스템 환경과 절차에 중대한 변화 또는 직원에게 추가 역할별로 훈련이 필요한 직책을 맡을 때 훈련을 제공

2.3 2010년대(2010년~2019년)

2000년대 말에 등장한 스마트폰이 본격적으로 일상생활에 보급이 되어 대부분의 사람들의 필수품이 되었다. 전 세계는 인터넷에 대한 의존도가 더욱 심화되었고, 각국의 사이버보안 경쟁도 극에 달하고 있는 시대이다. 미국은 2013년 스노든 사건 등으로 인해 사이버보안 체계의 급격한 변화가 시작되었다. 비밀로 유지되었던 미국의 사이버공격 전략, 기술 개발 등이 스노든 및 위키리크스 등의 문건 공개 등을 통해 공식적으로 인정할 수밖에 없는 상황이었다. 이로 인해 사이버보안 관련 법률이 2014년부터 본격적으로 제정되었던 상황도 이들 사건들과 연관성이 있다고 추정할 수 있다. 이 사건과 무관하게 FISMA 2002의 비현실적인 부분을 조정하기 위해 개정을 준비해 왔으며, 스노든 사건은 법률 개정을 앞당기는 계기가 되어 FISMA 2014로 개정하였으며 조직과 권한·행위 등을 통한 사이버보안 강화를 주요 주제로 다루었다.

2010년대 들어서 사이버보안 전문 인력 양성에 대해 그 중요성이 더욱 증대되어, 독립 법률로 제정하여 국가 정책을 이끌어갈 정도로 미국은 이 분야에 대한 적극적인 투자를 통해 세계 최고의 경쟁력을 확보하고자 노력하고 있다. 우리나라의 경우도 이에 대한 정책 등을 면밀히 검토 및 고려하여 화이트해커 양성이라는 단순한 구호 대신 실효성 있는 사이버보안 전문 인력 양성 정책을 수립하고 실천해야 할 것으로 생각된다.

2.3.1 연방정보보안현대화법(FISMA 2014)[17]

미국은 1987년 컴퓨터보안법을 통해 본격적으로 사이버보안에 대한 법률을 제정하기 시작하였다. 초고속 인터넷의 보급과 IT기술의 비약적인 발전으로 인해 해커에 의한 사이버공격이 국가 안보에 지대한 영향을 미치기 시작한 1990년대 말부터 미국은 각 부처 중심으로 사이버보안 대책을 수립하여 왔다. 2002년 미국은 연방정보 및 시스템을 보호하기 위해 FISMA 2002를 제정하였다. 미국 연방정부는 국가 차원의 일원화된 사이버보안의 중요성을 인식하여 백악관의 OMB와 NIST에 법적 임무를 부여하여 제도, 인력, 기술을 포괄하는 사이버보안체계를 정립하여 지속적으로 추진해 왔다. 12년간 지속하던 FISMA 2002의 미비점을 개선하기 위해 연방정보

보안현대화법(Federal Information Security Modernization Act of 2014, FISMA 2014)을 공표하였다.

미국 사이버보안 체계는 1997년 컴퓨터보안법, 2002년 연방정보보안관리법, 2014년 연방정보보안 현대화법 등 강력하고 구체적인 연방법을 기반으로 발전해 왔다. FISMA 2002는 국가차원의 일원화된 사이버보안 개선을 위해 예산관리국(OMB) 중심의 사이버보안 관리체계를 구축하였으며 각 연방기관은 FISMA 관련 업무 수행을 의무화 하였다[18][19].

FISMA 2014의 사이버보안 인력양성 분야는 FISMA 2002와 특별하게 변화가 없었으며, 다음 절에 나오는 사이버보안 인력 평가법에서 보듯이 별도의 법률로 제정되는 추세가 될 정도로 국가차원의 중요한 이슈가 되었다고 할 수 있다.

2.3.2 사이버보안 인력 평가법(2014)[20]

사이버보안 인력 평가법(Public Law 113-246, "Cybersecurity Workforce Assessment Act," December 18, 2014)은 DHS 소속 사이버보안 인력에 대한 정기적인 평가를 규정하고 있다.

PUBLIC LAW 113-246—DEC. 18, 2014

SECTION 1. SHORT TITLE.
This Act may be cited as the "Cybersecurity Workforce Assessment Act".
SEC. 2. DEFINITIONS.
SEC. 3. CYBERSECURITY WORKFORCE ASSESSMENT AND STRATEGY.
SEC. 4. CYBERSECURITY FELLOWSHIP PROGRAM.

이 법에서 사이버보안 교육 국가전략(National Initiative for Cybersecurity Education, NICE)에서 제안한 국가 사이버보안 인력 프레임워크를 도입하여 사이버보안 범주(category)와 전문영역(cpecialty area)을 정의하고 있다.

국토안보부 장관은 180일 이내에 DHS 소속 사이버보안 인력에 대해 평가하고 3년 동안 매년 평가할 것을 규정하고 있다. 또한 새로운 종합인력개발을 규정하고 있으며 사이버보안 인력의 역량 강화와 인원 충원 대책 등에 대해 규정하고 있다.

이 법은 국토안보부장관이 포괄적인 사이버보안 인력 전략을 수립하는 것을 내용으로 한 법률로서, 사이버보안 인력 역량을 전체적으로 확인하고, 사이버보안인력 강화를 위한 중장기 전략을 마련하며, 사이버보안 우수 인력의 사전채용을 통한 인적역량 강화 추진을 그 목적으로 한다.

2.3.3 사이버보안강화법(2014)[21]

사이버보안강화법(Public Law 113-274, "Cybersecurity Enhancement Act of 2014," Dec 18, 2014)은 공공 및 민간 부문이 연구 개발, 인력 준비(workforce preparedness) 및 대중 인식제고(public awareness) 측면에서 사이버보안을 개선하기 위해 함께 협력하도록 권고하고 있다.

TITLE Ⅰ-PUBLIC-PRIVATE COLLABORATION ON CYBERSECURITY
TITLE Ⅱ-CYBERSECURITY RESEARCH AND DEVELOPMENT
TITLE Ⅲ-EDUCATION AND WORKFORCE DEVELOPMENT
TITLE Ⅳ-CYBERSECURITY AWARENESS AND PREPAREDNESS
TITLE Ⅴ-ADVANCEMENT OF CYBERSECURITY TECHNICAL STANDARDS

"Title Ⅲ 교육 및 인력 개발"에서 연방 사이버보안 인력 발굴 및 채용을 위해서 사이버보안 경진대회(competition and challenge) 지원, 연방사이버장학금서비스프로그램 추진을 규정하고 있다.

사이버 위험 감소를 위한 표준과 대응절차 등을 수립하고, 연구개발 능력 향상, 인력 양성 및 교육, 인식 제고 등을 수행할 목적으로 이 법을 제정하였다. 이 법은 국립표준기술연구소(NIST)에 부여되었던 임무를 법제화하였고 공공·민간 파트너십을 강화하도록 법률을 제정하였다.

또한 사이버보안 인력 양성 측면을 매우 구체적으로 규정하였다. 상무부, 국립과학재단, 국토안보부는 OPM과 협의하여 사이버보안 혁신을 주도할 인력을 육성하도록 사이버보안 경진대회를 지원하고, OPM은 경진대회 수상자에게 정부기관의 인턴십 또는 기타 직무 등의 기회를 제공하도록 규정하고 있다.

국립과학재단은 사이버장학 프로그램을 운영하며, 수혜자 조건으로 장학금 수혜기간과 같은 기간 동안 연방기관 및 주·지방정부 기관에서 사이버보안 업무에 근무하는 것에 동의하여야 한다. 또한 NSF는 장학금 사업의 결과인 인력채용 성과를 정기적으로 평가하고 그 내용을 의회에 보고하여야 한다.

NIST는 사이버보안 인식제고와 준비를 강화하기 위하여 다음과 같은 프로그램을 준비하여야 한다. 또한 NIST는 연방정부 사이버보안 인식제고 프로그램

을 지원하는 전략 계획을 수립하며 5년 단위로 의회에 보고한다.

일반 CTF 대회는 화이트 해커들이 참여한 공격 중심인 반면, 2015년부터 이 법을 근거로 미국 내에서 활성화된 사이버보안 경진대회는 방어역량을 갖춘 인재 발굴 및 양성을 위한 경진대회가 다양하게 개최되고 있다. 또한 국립과학재단이 보조금 등을 지원하는 사이버보안 인력양성 프로그램이 다양하게 운영되기 시작하였다.

2.3.4 연방 사이버보안 인력평가법(2015)[22]

사이버보안법(Cybersecurity Act of 2015)은 2015년 12월 승인된 2016 회계연도 통합세출법(Consolidated Appropriations Act of 2016)의 DIVISION N에 있는 법률이다. 이 사이버보안법에는 다음과 같이 4종의 법률을 포함하고 있다.

① 사이버보안 정보공유법
② 국가 사이버보안 보호 개선법
③ 연방 사이버보안 개선법
④ 연방 사이버보안 인력 평가법

DIVISION N— CYBERSECURITY ACT OF 2015
TITLE I—CYBERSECURITY INFORMATION SHARING
"Cybersecurity Information Sharing Act of 2015"
TITLE II—NATIONAL CYBERSECURITY ADVANCEMENT
Subtitle A—National Cybersecurity and Communications Integration Center
"National Cybersecurity Protection Advancement Act of 2015"
Subtitle B—Federal Cybersecurity Enhancement
"Federal Cybersecurity Enhancement Act of 2015"
TITLE III—FEDERAL CYBERSECURITY WORKFORCE ASSESSMENT
"**Federal Cybersecurity Workforce Assessment Act of 2015**"

오바마정부 7년간의 사이버보안 강화 정책에 대한 준비를 반영하여 법적으로 공고히 하고자, 의회와 협력하여 2015년 12월에 사이버보안법을 발효할 수 있었다. 이 법을 통해 국가의 사이버보안 역량을 강화하는 데 필요한 중요한 도구를 제공하고 특히 민간기업도 기업간은 물론 정부와도 수월하게 사이버 위협 정보 공유를 하게 되었다.

사이버보안법 주요 내용은 첫째 민·관 사이버보안 정보공유체계 구축이며, 둘째 국토안보부 국가사이버보안통신통합센터(National Cybersecurity and Communications Integration Center, NCCIC)의 기능 강화 및 연방정부 사이버보안 강화 조치이다. 셋째 연방정부 사이버보안 인력 수요 평가·관리와 넷째 국제 사이버보안 강화, 긴급 서비스 사이버보안 강화, 보건의료산업 분야 사이버보안 개선, 연방컴퓨터시스템 보안강화 등을 규정하고 있다.

사이버보안법의 부속으로 제정된 연방 사이버보안 인력 평가법(2015)에서 연방정부의 사이버보안 인력에 대한 수요를 평가하고 관리를 강화하는 법률을 규정하고 있다.

NICE에 대한 법적인 근거는 2014년 사이버보안 강화법에서 규정한 국가 사이버보안 인식 및 교육 프로그램의 일환임을 연방 사이버보안 인력평가법에서 규정하고 있으며, 법적 근거를 확보하여 NICE에 필요한 더욱 강력한 추진 동력을 확보할 수 있었다.

사이버보안인력평가법(2014)에서 NICE 국가사이버보안 인력 프레임워크를 도입하여 사이버보안 범주(category)와 전문 영역(specialty Area)을 미리 정의하였으며, 여기서는 이보다 하위 영역인 직무역할(work role)을 정의하였다. 사이버보안 인력평가법이 DHS 소속 인력을 대상으로 한 반면, 이법은 연방기관 소속 전 직원을 적용 대상으로 하고 있어서 주무기관을 OPM으로 규정하고 있다.

OPM은 NIST와 협의하여 NICE를 따르는 코딩 구조(coding structure)를 개발할 것을 규정하고 있다. 코딩 구조는 연방직원에 대한 고용코드를 부여하는 것으로, 이법에서는 사이버보안 및 관련 인력에 대한 코드를 부여하는 것을 규정하고 있다. 각 연방기관은 사이버보안 및 관련 직원들에게 코드를 부여하는 절차를 마련하여 시행하도록 규정하고 있다.

OPM은 사이버 관련하여 시급히 요구되는 직무역할 식별하고 각 연방기관에 지침을 하달하도록 규정하고 있따. 또한 연방기관의 사이버보안 인력의 부족 현황을 파악하여 보고서를 작성하여 의회에 제출하도록 규정하고 있다.

2.3.5 OPM 사이버보안코드부여 지침(2017)[23]

2013년 이후 연방기관들은 정부 사이버보안 데이터 표준 코드(government-wide cybersecurity data standard codes)를 부여받아 왔다. 그 코드는 NICE Cybersecurity Workforce Framework의 7개 범주, 33개 전문분야로 분류·정의하고 있었다.

2015년 연방 사이버보안 인력 평가법에 의거하여 OPM은 NICE 코딩 구조를 구현하고 정보 기술,

사이버 보안 또는 기타 사이버 관련 기능의 수행을 요구하는 모든 연방 민간 직위(federal civilian positions)를 식별하는 절차를 수립해야 하였다.

연방 사이버보안 인력평가법에 따라 OPM은 2017년 1월 4일부로 IT, 사이버보안 및 사이버 관련 기능에 연계한 연방 직원 직위에 새로운 사이버보안 코드를 부여하는 지침을 공표하였다. 모든 연방기관들은 사이버보안 직위에 대해 새로운 인사코드를 2017년1월까지 적용할 것을 명시한 바에 따라 OPM이 제정하여 공표한 것이다.

2.3.6 사이버보안 및 기반보호기관법 (CISA 2018)[24]

사이버보안 및 기반보호기관법(Cybersecurity and Infrastructure Security Agency Act)은 국토안보법(2002)를 개정하여 연방기관의 사이버보안을 담당하는 국가보안프로그램국(NPPD, National Protection and Programs Directorate)을 독립적인 CISA로 확대 개편하는 것이 주 내용이다. 2017년 12월 19일 미국기술위원회(American Technology Council, ATC)에서 보고한 "Report to the President on Federal IT Modernization")에 따라 보안 기능 운영 센터로의 접근을 보장하기 위한 국토안보부 계획을 의회에 보고할 것을 명시하고 있다[25].

사이버보안 인력 관련하여 기존에 제정된 법률인 사이버보안 인력 평가법 등 관련 조항들과의 비교 분석을 통해 CISA 2018이 어느 정도 충족하는 가에 대한 보고서를 90일 이내에 제출할 것을 의무화 하였다. 이러한 점은 미국 법률체계의 가장 큰 특징으로 법률상 충돌 및 이견 해결에 그치는 것이 아니라 실제 집행기관의 현실을 반영하도록 조치한 것이다.

III. 미국 사이버보안 법·규정의 효과성 기반의 분석 방법 제안

기존 연구에서 사이버보안 인력양성 법·규정 비교·분석 방법이 없는 관계로, Ⅱ장에서 살펴본 12종의 법·규정을 기반으로 국내 사이버보안 인력양성 관련 법·규정을 상호 비교하기 위해서 새로운 방법을 제안한다. 이 장에서는 법·규정 기준으로 상호 비교 가능한 항목을 식별하는 방법과 도출된 항목을 기반으로 12종의 법·규정을 분석한다. Ⅳ장에서 사이버보안 인력양성에 대한 국내 법·규정을 식별하고, 이 장에서 도출된 비교항목을 기반으로 비교·분석을 수행한다.

3.1 비교 항목 선정 및 미국 법·규정 분석

미국의 법률 및 규정에서 사이버보안 인력 양성과 관련된 법·규정을 검토하여 각 고유 항목을 식별하여 사이버보안 인력 양성의 법·규정으로서 타당한 항목들을 구분하여 향후 법·규정으로서의 구성 방안에 대해 비교할 수 있는 비교 항목(comparing item)으로 선정한다. 앞에서 미국의 사이버보안 인력 관련한 법(8종)·규정(4종) 12종을 살펴보았으며, 각 내용들 중 상호 비교가 가능한 비교 항목을 분석하는 것이 필요하다.

다음은 12종의 법·규정 등에서 규정하는 사이버보안 인력 양성 정책 관련 사항들을 식별하였다.

(1) 컴퓨터보안법, 1987 (L1)
- o 훈련 대상 : 컴퓨터 시스템 담당 연방기관 직원
- o 훈련 내용 : (1) 사이버보안 인식, (2) 사이버보안 훈련
- o 지원 기관 : NIST 훈련 지원기관 지정
- o 지원 내용 : 연방 컴퓨터보안 훈련 가이드라인 개발 및 배포
- o 관련 기관 : NSA, OMB

(2) OPM 연방규정, 1992 (R1)
- o 근거 : Computer Security Act of 1987
- o 참고 : NIST SP 500-172(Computer Security Training Guidelines, 1989)
- o 훈련 대상 : 연방기관 훈련 대상자 세분화
  - (1) 현 직원 및 고용 후 60일 이내인 신입직원
  - (2) 심각한 기관 IT 보안환경·절차 변화에 직면하거니 민감한 정보를 다루는 새로운 직무를 맡은 직원
  - (3) 정보 민감도에 따른 주기적 훈련이 요구되는 직원
- o 관련 기관 : OPM, NIST

(3) OMB Circular A-130 (1996), (R2)
- o 근거 : Computer Security Act of 1987
- o 관련 기관 : OPM, NIST
- o 개정 지시 : NIST SP 500-172 개정 지시

(4) 정부정보시스템개혁법, 2000 (L2)
- o 개정 지시 : OPM에게 연방규정 개정 지시
- o 훈련 책임 : 연방기관장이 CIO에게 위임, CISO 개념 도입
- o 지원 기관 : 상무부(NIST) 지원 명기하며, NIST 역할과 책임을 구체적 강화
- o 관련 기관 : OPM OPM의 역할과 책임을 구체적으로 명시
- o 인력 현황 보고 : GISRA Annual Reort to Congress (2001~2003) 내 포함

(5) 연방정보보안관리법, 2002 (L3)
- o 훈련 대상 : 연방기관 직원, 연방기관 계약자, 기타 사용자
- o 훈련 책임 : (1) 연방기관장에게 부여, 훈련을 받은 인력확보, (2) 보안 인식 훈련 의무화한 기관 프로그램 운영
- o 지원기관 : NIST 임무 구체화, NIST 산하 ITL CSD, ASD 신설의 근거 법률
- o 인력 현황 보고 : FISAM 2002 Annual Reort to Congress (2004~2014) 내 포함

(6) OPM 연방인사규정 개정, 2004 (R3)
- o 근거 : GISRA 2000
- o 참고 : NIST SP 800-50(2003) 반영

(7) 연방정보보안현대화법, 2014, (L4)
- o 인력 현황 보고 : FISAM 2014 Annual Reort to Congress (2015~2018) 내 포함
  * 다른 내용은 FISMA 2002와 동일한 내용

(8) 사이버보안 인력 평가법, 2014 (L5)
- o 참고 : NIST SP800-16 2′nd Draft(2013)
- o 훈련 대상 : DHS 소속 사이버보안 담당직원
- o 인력 평가 : 대상 인력에 대한 주기적 평가
- o 직무 정의 : NICE Category, Specialty Area 정의
- o 인력 전략 : DHS 장관 사이버보안 인력 양성 전략 수립

(9) 사이버보안 강화법, 2014 (L6)
- o 지원 기관 : NIST, NSF, DHS
- o 민간 지원 : (1)사이버보안 경진대회, (2)인턴십, (3)장학금·복무

(10) 연방사이버보안 인력평가법, 2015(L7)
- o 훈련 대상 : 모든 연방기관 인력으로 확대
- o 인력 평가 : 대상인력에 대한 주기적 평가
- o 국가 정책 : NICE 법적 근거 명시
- o 직무 정의 : NICE Work Role 정의

(11) OPM 사이버보안코드부여 지침, 2017 (R4)
- o 근거 : 연방 사이버보안 인력 평가법(2015)
- o 훈련 대상 : 연방 사이버보안 직무 인력 코드 규격 확립

(12) 사이버보안·기반보호기관법, 2018 (L8)
- o 참고 : NIST SP800-16 3′nd Draft(2014)

상기와 같이 12개 법·규정을 세부적으로 분석한 결과 사이버보안 인력양성을 위해 필요한 비교 항목을 15종으로 식별할 수 있었다. 15종에 해당되는 비교항목들은 훈련 대상, 훈련 내용, 지원 기관, 지원 내용, 관련 기관, 근거, 참고, 개정 지시, 훈련 책임, 인력 현황 보고, 인력 평가, 직무 정의, 인력 전략, 민간 지원, 국가 정책 등으로 분류할 수 있다.

3.2 비교 항목 도출

사이버보안 인력을 양성하기 위한 분야를 특성별로 비교그룹을 주체, 도구, 대상자, 목표, 기타의 5가지로 분류할 수 있다.

첫 번째 비교그룹에 해당되는 〔1〕주체에 해당되는 비교 항목은 다음과 같다.
- o 〔1-1〕지원 기관 : 인력양성 표준, 가이드라인, 기술 등을 지원하는 기관의 지정 유무,
  * 미국의 경우 NIST
- o 〔1-2〕관련 기관 : 인력양성을 위해 주관, 예산 지원 등을 위해 지정된 기관 유무
- o 〔1-3〕훈련 책임 : 인력에 대한 훈련을 책임지는 직위의 지정 유무

두 번째 비교그룹인 〔2〕도구에 해당되는 비교 항목은 다음과 같다.
- o 〔2-1〕연방 지원 : 연방기관 대상으로 훈련에 필요한 각종 지원 내용 *표준, 가이드, 기술 등
- o 〔2-2〕민간 지원 : 학교 등을 대상으로 훈련에

필요한 각종 지원 내용 * 장학금, 인턴십 등
- o 〔2-3〕직무 정의 : 대상 인력의 구체적 직무 규정 유무
- o 〔2-4〕인력 평가 : 대상 인력에 대한 정기 또는 비정기 평가 유무
- o 〔2-5〕인력 전략 : 대상 인력에 대한 인력 양성 전략 수립 유무
- o 〔2-6〕국가 정책 : 국가 정책에 대한 법적인 근거 유무

세 번째 비교그룹인 〔3〕대상에 해당되는 비교 항목은 훈련 대상자 식별 유무에 해당되는 〔3-1〕훈련 대상 한 가지만 식별 할 수 있었다.

네 번째 비교그룹에 해당되는 〔4〕목표에 해당되는 비교 항목은 다음과 같다.
- o 〔4-1〕훈련 내용 : 훈련 대상자가 수행해야할 구체적인 훈련 내용 유무
- o 〔4-2〕인력 보고 : 훈련 대상 인력에 대한 보고서 작성을 통한 보고 의무화 유무

다섯 번째 비교그룹에 해당되는 〔5〕기타는 분류하기 곤란한 항목을 모아둔 것으로 다음과 같다.
- o 〔5-1〕근거 : 이 법·규정의 근거 유무
- o 〔5-2〕참고 : 이 법·규정의 참고 유무
- o 〔5-3〕개정 지시 : 법, 규정, 가이드, 표준 등의 개정 지시 유무

이와 같이 5개 그룹을 기반으로 위에서 식별한 12종의 법·규정 별로 식별한 15개 비교 항목을 정리하면 Table 2.와 같다.

Table 2. Comparing groups and items for analyzing laws and regulations related cybersecurity workforce development

Groups	Items	Descriptions
〔1〕 Subjects	〔1-1〕Supporters	Designation of institutions to support workforce development standards, guidelines, and technologies * (ex) NIST in the U.S.
	〔1-2〕Related Agencies	Is there a designated agency for supervising, funding, etc. for the workforce development ?
	〔1-3〕Training Responsibility	Designate a position to be in charge of training workforce?
〔2〕 Tools	〔2-1〕Federal Supports	Is there any support for training for federal agencies? * Standards, guides, technology, etc.
	〔2-2〕Civilian Supports	Is there any kind of support required for training in schools? * Scholarship, internship, etc.
	〔2-3〕Defining Work Roles	Detailed regulations for the target workforce' work role?
	〔2-4〕Workforce Assessment	Regular or occasional assessments of the target workforce?
	〔2-5〕Workforce Plan	Is there a development plan for the target workforce?
	〔2-6〕Nationwide Policy	Legal basis for national policy?
〔3〕 Targets	〔3-1〕Training Targets	Identifying training targets?
〔4〕 Goals	〔4-1〕Training Contents	Specific training to be performed by the trainee?
	〔4-2〕Workforce Report	Reporting duty for reporting on the workforce?
〔5〕 Others	〔5-1〕Precedence	Any basis for these laws and regulations?
	〔5-2〕References	Any references for these laws and regulations?
	〔5-3〕Revision Order	Orders to amend laws, regulations, guides, standards, etc.?

3.3 법·규정의 비교 분석

5개 비교그룹 및 15개 비교 항목을 기준으로 12개 법·규정을 적용한 결과는 다음과 같다.
- o 〔1-1〕지원기관
  - NIST는 5개 법률에서 규정
  - DHS, NSF는 1개 법률에서 규정
- o 〔1-2〕관련기관
  - OPM은 3개 법률에서 규정
  - NIST는 2개 법률, NSA, OMB는 1개 법률
- o 〔1-3〕훈련책임 : 3개 법률이 연방기관장 규정
- o 〔2-1〕연방지원 : 1개 법률에서 훈련 가이드라인을 지원할 것을 규정
- o 〔2-2〕민간지원 : 1개 법률에서 (1)사이버보안 경진대회, (2)인턴십, (3)장학금· 복무를 규정
- o 〔2-3〕직무정의
  - 1개 법률에서 NICE Category, Specialty Area 규정
  - 1개 법률에서 NICE Work Role 규정

o 〔2-4〕인력평가 : 2개 법률에서 대상 인력에 대한 주기적 평가 규정
o 〔2-5〕인력전략 : 1개 법률에서 DHS 사이버보안 인력 양성 전략 수립을 규정
o 〔2-6〕국가정책 : 1개 법률에서 2010년 시작된 NICE 법적 근거 명시
o 〔3-1〕훈련대상
- 컴퓨터 시스템을 다루는 연방기관 직원은 1개 법률에서 규정
- 연방기관 훈련 대상자 세분화는 1개 법률에서 규정
- 연방기관 직원, 연방 기관 계약자 및 기타 사용자는 2개 법률에서 규정
- DHS 소속 사이버보안 담당직원은 1개 법률에서 규정
- 모든 연방기관 인력은 1개 법률에서 규정
- 연방 사이버보안 직무인력 코드 확립은 1개 법률에서 규정
o 〔4-1〕훈련내용 :1개 법률에서 (1) 사이버보안 인식 및 사이버보안 훈련 규정
o 〔4-2〕인력보고
- 1개 법률 : GISRA Report(01~03)
- 1개 법률 : FISMA Report(04~14)
- 1개 법률 : FISMA Report(15~18)
o 〔5-1〕근거
- 2개 법률 : 컴퓨터보안법(1987)
- 1개 규정 : GISRA 2000
- 1개 법률 : 연방사이버보안인력평가법(2014)
o 〔5-2〕참고
- 2개 규정 : NIST SP800-50(2003)
- 1개 법률 : NIST SP800-16 2′nd Draft(2013)
- 1개 법률 : NIST SP 800-16 3′nd Draft(2014)
o 〔5-3〕개정지시
- 1개 규정 : NIST SP 500-172
- 1개 법률 : OPM 연방규정

상기와 같이 분석된 내용을 비교 항목별로 Table 3.와 같이 정리할 수 있다. 8개 법률과 4개 규정을 사이버보안 인력 양성을 위한 실행력을 평가하고자 15개의 비교 항목을 기준으로 세부내용을 살펴본 결과 모든 분야가 법적으로 적합하게 규정되었음을 확인할 수 있었다.

Table 3. Details of U.S. laws and regulations based on comparing items

Comparing Items	Descriptions
[1-1]Supporters	o 5 Laws : NIST o 1 Law : DHS, NSF
[1-2]Related Agencies	o 3 Laws : OPM o 2 Laws : NIST o 1 Law : NSA, OMB
[1-3]Training Responsibility	o 3 Laws : Agency Head
[2-1]Federal Supports	o 1 Law : Training Guideline
[2-2]Civilian Supports	o 1 Law : (1) Cybersecurity Competition, (2) Internship, (3) Scholarship・Service
[2-3]Defining Work Roles	o 1 Law : NICE Category, Specialty Area o 1 Law : NICE Work Role
[2-4]Workforce Assessment	o 2 Laws : Periodic assessment of target workforce
[2-5]Workforce Plan	o 1 Law : DHS Cybersecurity Workforce Develpoment Strategy
[2-6]Nationwide Policy	o 1 Law : legal basis of NICE started in 2010
[3-1]Training Targets	o 1 Law : Federal agency employees dealing with computer systems o 1 Law : Identify federal workforce to train o 2 Laws : Federal agency employees, federal agency contractors, and other users o 1 Law : DHS cybersecurity workforce o 1 Law : All Federal workforce o 1 Law : Establishing work roles codes of federal cybersecurity workforce
[4-1]Training Contents	o 1 Law : (1) Cybersecurity Awareness (2) Cybersecurity Training
[4-2]Workforce Report	o 1 Law : GISRA Report(01~03) o 1 Law : FISMA Report(04~14) o 1 Law : FISMA Report(15~17)
[5-1]Precedence	o 2 Laws : Computer Security Act(1987) o 1 Regulation : GISRA 2000 o 1 Law : FCWAA 2015

Comparing Items	Descriptions
[5-2]References	o 2 Regulations : NIST SP 800-50(2003) o 1 Law : NIST SP 800-16 2'nd Draft(2013) o 1 Law : NIST SP 800-16 3'nd Draft(2014)
[5-3]Revision Order	o 1 Regulation : NIST SP 500-172 o 1 Law : OPM Federal regulations

Table 4.는 비교항목과 법·규정 분포를 시각적으로 보여주기 위해 작성한 표로서, 전반적으로 비교항목들이 고르게 분포되는 현상을 발견할 수 있다. 연방 사이버보안 인력양성 관련하여 필요한 구체적인 내용들이 다양한 법·규정에서 상호보완적으로 규정하고 있음을 알 수 있다. 이와 같은 맥락에서 다음 Ⅳ장에서는 이 장에서 제안된 방법론을 기반으로 국내 법·규정을 분석하여 현재의 국내 상황을 인식할 수 있으며, 발전 방향을 알 수 있다.

Table 4. Distribution of U.S. laws and regulations based on comparing items

CI	L1	R1	R2	L2	L3	R3	L4	L5	L6	L7	R4	L8	계
1-1	√			√	√		√		√				5
1-2	√	√	√	√									4
1-3				√	√		√						3
2-1	√												1
2-2									√				1
2-3								√		√			2
2-4								√		√			2
2-5								√					1
2-6										√			1
3-1	√	√			√		√	√		√	√		7
4-1	√												1
4-2				√	√		√						3
5-1		√	√			√					√		4
5-2		√				√		√				√	4
5-3			√	√									2
계	5	4	3	5	4	2	4	5	2	4	2	1	41

Ⅳ. 한국 사이버보안 인력양성 법·규정 현황 및 분석

미국 사이버보안 인력양성 법률·규정 등과 비교한다면 우리나라는 경우 사이버보안을 다루는 독자 법률이 없는 현실이다. 기존 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 정보통신기반보호법, 개인정보보호법 등에 사이버보안 개념이 있을 뿐 인력양성 관련 내용이 부족하며, 국가사이버안전관리규정이 교육에 대해 언급하는 조항을 포함하고 있다. 상대적으로 사이버보안 인력 양성을 위해서는 강력한 법률 및 규정이 뒷받침 되어야 하는 것이 국제적으로 기본 상식이 되어가고 있는 현실을 감안한다면 우리나라도 늦었지만 이제라고 인력 양성에 대해 체계적인 법 제정 관점에서 접근해야 할 것으로 생각된다.

4.1 사이버보안 관련 법률 현황

우리나라의 사이버보안을 규율하는 일반법은 없고, 각 분야별 개별법이 존재하고 그 개별법에 근거하여 사이버공격에 대응하고 있다. 물론 공공과 민간을 포괄하는 「정보통신기반보호법」과 「국가정보화기본법」이 있다. 그렇지만, 정보통신기반보호법은 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 정보통신망법의 정보통신망(=정보통신기반시설) 가운데 중앙행정기관의 장이 지정한 '주요정보통신기반시설'에 대한 전자적 침해행위로 인하여 발생한 사태, 즉 '침해사고'를 규율대상으로 하고 있다. 그리고 「국가정보화기본법」은 국가·지방자치단체·공공기관 등 공공부문과 정보통신서비스제공자, 정보통신 관련 제조업자, 웹접근성 품질인증기관, 광대역통합정보통신기반의 원활한 구축과 이용촉진의 홍보, 국제협력, 기술개발 등 업무전담기관 등 민간부문을 규율대상으로 한다. 그렇지만, 규율대상이 제한적이어서 사이버보안을 위한 일반법으로 기능하기는 어렵다[18].

미국 연방법률과 비교를 위해서 주로 공공부문에의 사이버보안 관련 법률 및 규정은 다음과 같다.

(1) 전자서명법(1999.7.1)
(2) 정보통신기반 보호법(2001.7.1)
(3) 정보통신망법(2001.7.1) - 정보통신망 이용촉진 및 정보보호 등에 관한 법률
(4) 전자금융거래법(2001.7.1)
(5) 전자정부법(2007.3.1)
(6) 국가정보화 기본법(2009.8.23)
(7) 개인정보 보호법(2011.9.30)
(8) 국가사이버안전관리규정(2005.1.31)

우리나라의 사이버보안 관련 법률은 적용 분야에 따른 개별법이 주를 이루고 있다. 다음과 같이 법률별로 적용 분야를 살펴보면 다음과 같다.

(KL1) 전자서명법 : 공인인증기관 및 인증체계

(KL2) 정보통신기반 보호법 : 정보통신기반시설
(KL3) 정보통신망법 : 정보통신망 및 관련 정보
(KL4) 전자금융거래법 : 금융기관을 포함한 전자금융거래
(KL5) 전자정부법 : 전자정부를 사용하는 행정 및 정보시스템
(KL6) 국가정보화 기본법 : 국가기관 또는 자치단체의 정보
(KL7) 개인정보 보호법 : 개인정보
(KR1) 국가사이버안전관리규정 : 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망에 대한 사이버공격

우리나라의 법률 중 사이버보안 중심으로 제정된 법률은 정보통신망기반 보호법, 개인정보보호법, 국가사이버안전관리규정이 유사하게 분류될 수 있다. 다른 법은 정보통신망 및 기반시설, 전자금융, 전자정부, 정보화 등 정보시스템 및 정보를 운영하는 것을 우선으로 규정하고 있다. 사이버보안 관련 대응, 조직, 인력 등을 체계적으로 규정한 법률은 미국 법률들에 비해 상당히 미흡한 편이다[1].

4.2 사이버보안 인력 양성 관련 법률 현황

우리나라 법률에는 사이버보안 인력 양성에 대한 규정이 매우 미흡하며, 있다고 해도 선언적인 내용으로 강제력 및 실천력이 부족하다고 할 수 있다.

전자서명법의 경우 다음과 같이 전자서명 관련 전문인력 양성에 대해 다음과 같이 규정하고 있으나, 전자서명 인력에 대한 정의가 애매하며 구체적인 추진에 대한 강제력이 부족한 실정이다.

> 제26조의4(전자서명 기술개발 및 인력양성)
> 과학기술정보통신부장관은 전자서명의 이용촉진에 필요한 기술개발 및 전문인력양성을 위하여 다음 각호의 사항을 추진한다. <개정 2008. 2. 29., 2013. 3. 23., 2017. 7. 26.>
> 1. 전자서명 관련 기술수준의 조사, 기술의 연구·개발 및 활용에 관한 사항
> 2. 전자서명 관련 기술협력 및 기술이전에 관한 사항
> 3. 전자서명에 관한 기술정보의 제공 및 관련 기관·단체와의 협력에 관한 사항
> 4. 전자서명 관련 전문인력의 수급실태조사 및 전문인력양성을 위한 지원사항
> 5. 그 밖에 전자서명에 관한 기술개발 및 인력양성에 필요한 사항
> [본조신설 2001. 12. 31.]

정보통신기반 보호법에서는 다음과 같이 전문인력 양성을 규정하고 있으나, 실효성을 담보하기에는 선언적인 내용이다.

> 제6장 기술지원 및 민간협력 등
> 제24조(기술개발 등) ①정부는 정보통신기반시설을 보호하기 위하여 필요한 기술의 개발 및 전문인력 양성에 관한 시책을 강구할 수 있다.

정보통신망법은 IT 인력양성에 대해서 다음과 같이 규정하고 있으므로 사이버보안 인력양성을 직접적으로 규정하고 있다고 볼 수 없다.

> 제11조(정보통신망 응용서비스의 개발 촉진 등)
> ② 정부는 민간부문에 의한 정보통신망 응용서비스의 개발을 촉진하기 위하여 재정 및 기술 등 필요한 지원을 할 수 있으며, 정보통신망 응용서비스의 개발에 필요한 기술인력을 양성하기 위하여 다음 각 호의 시책을 마련하여야 한다.
> 1. 각급 학교나 그 밖의 교육기관에서 시행하는 인터넷 교육에 대한 지원
> 2. 국민에 대한 인터넷 교육의 확대
> 3. 정보통신망 기술인력 양성사업에 대한 지원
> 4. 정보통신망 전문기술인력 양성기관의 설립·지원
> 5. 정보통신망 이용 교육프로그램의 개발 및 보급 지원
> 6. 정보통신망 관련 기술자격제도의 정착 및 전문기술인력 수급 지원
> 7. 그 밖에 정보통신망 관련 기술인력의 양성에 필요한 사항
> [전문개정 2008. 6. 13.]
>
> 제52조(한국인터넷진흥원)
> ③ 인터넷진흥원은 다음 각 호의 사업을 한다.
> 4. 정보통신망의 이용 및 보호를 위한 홍보 및 교육·훈련
> 6. 정보보호산업 정책 지원 및 관련 기술 개발과 인력양성

전자정부법도 정보화인력 양성 규정이므로 사이버보안 인력 양성과는 관계가 없다고 볼 수 있다.

> 제5조(전자정부기본계획의 수립)
> ② 제1항에 따른 전자정부기본계획(이하 "전자정부기본계획"이라 한다)에는 다음 각 호의 사항이 포함되어야 한다.
> 12. 그 밖에 정보화인력의 양성 등 전자정부의 구현·운영 및 발전에 필요한 사항
> 제53조(정보화인력 개발계획의 수립 등) ① 중앙사무관장기관의 장은 공무원의 정보화 역량 향상 및 정보자원의 효율적인 관리 등을 도모하기 위하여 정보화인력 개발계획 및 전문인력의 양성, 자격제도 등에 관한 시책을 수립·추진할 수 있다.
> ② 중앙행정기관 및 지방자치단체의 장은 제1항의 정보화인력 개발계획에 따라 자체 추진계획을 수립·시행하여야 한다.
> ③ 제1항 및 제2항에서 규정한 사항 외에 정보화인력의 개발 등에 필요한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 및 대통령령으로 정한다.

개인정보보호법은 다음과 같이 개인정보 보호를 위한 전문인력 양성이라는 선언만이 있으므로 실행력에 있어서 한계를 갖는다고 할 수 있다.

> 제9조(기본계획) ① 보호위원회는 개인정보의 보호와 정보주체의 권익 보장을 위하여 3년마다 개인정보 보호 기본계획(이하 "기본계획"이라 한다)을 관계 중앙행정기관의 장과 협의하여 수립한다. <개정 2013. 3. 23., 2014. 11. 19., 2015. 7. 24.>
> ② 기본계획에는 다음 각 호의 사항이 포함되어야 한다.
> 6. 개인정보 보호를 위한 전문인력의 양성

법률이 아닌 행정규칙의 일종인 국가사이버안전관리규정이 사이버보안 인력 양성을 가장 잘 규정하고 있다. 그러나 법률이 아니므로 국가기관 및 공공기관의 실천력 확보에는 한계를 가진다.

> 제4조(사이버안전 확보의 책무) ①중앙행정기관의 장은 소관 정보통신망에 대하여 안전성을 확보할 책임이 있으며 이를 위하여 사이버안전업무를 전담하는 전문인력을 확보하는 등 필요한 조치를 강구하여야 한다.
> ② 관계 중앙행정기관의 장은 소관 공공기관 및 지방자치단체의 장으로 하여금 제1항의 규정에 의한 전문인력의 확보 등 필요한 조치를 강구하도록 하여야 한다.
>
> 제16조(인력양성 및 교육홍보) ①관계 중앙행정기관의 장은 사이버안전의 기반 조성에 필요한 기술인력을 양성하고 국민의 인식제고를 위하여 다음 각호의 시책을 강구하여야 한다.
> 1. 사이버안전 관련 전문기술인력의 확보 및 양성
> 2. 사이버안전 교육프로그램의 개발 및 투자
> 3. 그 밖에 전문인력 양성, 교육 및 홍보 등에 관하여 필요한 사항
> ② 국가정보원장은 관계 중앙행정기관의 장이 사이버안전과 관련한 전문인력의 양성, 교육 및 홍보를 위하여 필요한 지원을 요청하는 경우 이에 대하여 지원할 수 있다.

4.3 법·규정의 비교 분석

미국의 사이버보안 인력 양성 관련 법·규정의 분석을 위해 제시한 비교항목인 〔표 2〕에 근거하여 국내 사이버보안 관련 법(7종) 규정(1종)을 적용하여 비교한 결과는 Table 5.와 같다.

비교 항목에 부합하는 국내 법률 조항은 발견할 수 없었다. 다만, 대통령훈령인 사이버안전관리규정의 제4조(사이버안전 확보의 책무)②항에서 중앙행정기관의 장이 전문인력 확보 등 필요한 조치를 강구하도록 규정하여 훈련의 책임을 명시하고 있다([1-3]Training Responsibility). 제16조(인력양성 및 교육홍보)②항에서 국가정보원장이 사이버안전과 관련한 전문인력의 양성, 교육에 대한 지원을 행정기관의 장이 요청할 경우 지원할 수 있다고 소극적으로 규정하고 있다. 이와 같이 2개의 비교항목에 대해서 국내 법·규정에서 식별할 수 있었다.

Table 5.의 비교항목에는 없지만 전문인력 양성에 대한 필요성을 알리는 캠페인 성격의 선언에 대해 정보통신기반보호법의 "정보보호인력 양성 선언"과 개인정보 보호법의 "개인정보 보호를 위한 전문인력의 양성을 기본계획에 포함" 등이 있다.

Table 5. Details of Korean U.S. laws and regulations based on comparing items

Comparing Items	Descriptions
[1-1]Supporters	One Regulation : National Intelligence Service
[1-2]Related Agencies	None
[1-3]Training Responsibility	One Regulation : Executive Agency Head
[2-1]Federal Supports	None
[2-2]Civilian Supports	None
[2-3]Defining Work Roles	None
[2-4]Workforce Assessment	None
[2-5]Workforce Plan	None
[2-6]Nationwide Policy	None
[3-1]Training Targets	None
[4-1]Training Contents	None
[4-2]Workforce Report	None
[5-1]Precedence	None
[5-2]References	None
[5-3]Revision Order	None

Table 6. Distribution of Korean laws and regulations based on comparing items

CI	L1	L2	L3	L4	L5	L6	L7	R1	계
1-1								√	**1**
1-2									
1-3								√	**1**
2-1									
2-2									
2-3									
2-4									
2-5									
2-6									
3-1									
4-1									
4-2									
5-1									
5-2									
5-3									
계								**2**	**2**

Table 6.은 국내 법·규정을 15개 비교항목에 적용하여 분포 현황을 보여주고 있으며, 2개 항목 외에는 전혀 식별되지 않음을 확인할 수 있다. 이는 미국 연방 법률·규정을 기반으로 비교·분석한 결과로 국내 법·규정의 특별한 상황을 반영하지 않았으므로 향후 연구에서 추가적인 조건 및 상황 등을 반영한 연구 및 보완이 필요하다.

V. 결 론

약 30여년 동안 추진되어 왔던 미국의 사이버보안 인력양성 정책에 대해서 법률, 규정, OMB Circular-A 등을 살펴본 결과, 의회, OPM, OMB, NIST 중심으로 법률·규정의 실현을 담당해 왔음을 알 수 있었다. 미국 연방기관의 사이버보안 인력 양성 관점에서 분석한 결과, 가장 특이한 점은 법률로써 그 추진근거를 명확히 규정한다는 것으로, 1987년 제정된 컴퓨터보안법을 시작으로 8종의 법률을 통해 사이버보안 인력양성에 대한 추진 근거를 마련하였으며 사이버보안법(2015) 내의 연방사이버보안인력평가법이 최신 근거에 해당하는 법률의 가치를 지닌다.

미국 법·규정의 특징은 단순 명료하게 정리된다는 것이다. 예산권을 가진 OMB 중심으로 대통령(백악관)의 리더십이 발휘되고 있으며, 정부부처(DHS, OPM 등), 연방기관(NIST, NSF 등) 지정도 명확히 하여 제도에 대한 실천력이 강화될 수 있는 근거로 볼 수 있다. 또한 법 적용대상 기관인 연방기관들의 의무를 명확히 하고, FISMA 연례 보고서를 의회에 제출(FY2000 ~ FY2017)하여 의회의 확인 및 점검을 의무화하였다.

미국 사이버보안 인력 양성을 포함한 법(8종)·규정(4종)을 통해 도출된 비교항목 15종을 적용하여 분석한 결과 각종 법·규정의 내용들이 오랜 기간 동안 인력 양성에 필요한 항목에 고르게 적용되었다는 것을 확인할 수 있었다. 우리나라의 경우 15개 비교항목 중 사이버안전관리규정이 2개 비교항목만을 만족하는 현실을 인식하고, 본 논문에서 제안한 사이버보안 인력 양성 비교 항목을 만족시킬 수 있도록 국가차원의 적극적인 관심과 관련한 정책을 마련하여 지속적이며 일관성 있게 추진해야 할 것이다.

References

[1] Soonjwa Hong, "A Study on US Federal Law for Enhancing National Cyber Security", The Korea Institute of Information Security and Cryptology 29(3), pp. 51-65, June 2019.

[2] Public Law 107- 347, "E-Government Act of 2002 Tile III. Information Security Federal Information Security Management Act of 2002", Dec. 2002.

[3] Soonjwa Hong, "A Study on the Frame- work of Comparing New Cybersecurity Workforce Development Policy Based on the ATE Programs of U.S.", Journal of the Korea Institute of Information Security & Cryptology 28(1), pp. 249-267, Feb. 2018.

[4] Sangho Park, A Study on the Design of Knowledge System for Information Security Professional Training, Master's Thesis, Sangmyung University, Feb. 2016.

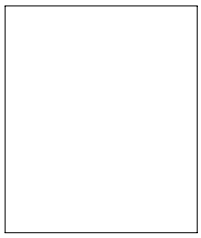
[5] Wonhyung Park and Seongjin Ahn, "Enhancing Education Curriculum of Cyber Security Based on NICE", KIPS Transactions on Computer and Communication Systems 6(7), pp.321-328, July 2017.

[6] Wongyu Lim and Seongjin Ahn, "A Study on Improvements of the Information Security Department via the Curriculum Analysis", The Journal of Korean Association of Computer Education 17(6), pp. 51-65, Nov. 2014.

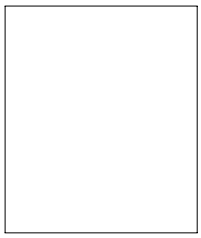
[7] Jeong-Ho Song and Hwang-Rae Kim, "A Study on the NCS based Curriculum for Educating Information Security Manpower", Journal of the Korea Academia-Industrial Cooperation Society 17(11), pp. 537-544, Nov. 2016.

[8] Hyojik Lee, Onechul Na, Soyoung Sung, and Hangbae Chang, "A Design on Information Security Core Knowledge for Security Experts by Occupational Classification Framework", The Journal of Society for e-Business Studies 20(3), pp. 113-125, Aug. 2015.
[9] Min-Jeong Kim, Haeni Lee, Shin-Jeong Song, and Jinho Yoo, "A Study on the Curriculum of Department of Information Security in Domestic Universities and Graduate Schools and Comparison with the Needs of Industry Knowledge", Journal of The Korea Institute of Information Security & Cryptology 24(1), pp. 195-205, Feb. 2014.
[10] Yoon K.S. and Lee S, "The Problems and Alternatives of Information Security in the Korean Public Sector", Korean Public Management Review 31(4), pp. 195-216, 2017.12.
[11] Hong, Jun Ho and You, Hyun Woo, "A Study on white hacker training and activation plan", Law Review 17(4), pp. 463-515, Dec. 2017.
[12] Public Law 100-235, "Computer Security Act of 1987," Jan. 1988.
[13] NIST SP 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model, Apr. 1998,
[14] Public Law 106‐398, "National Defense Authorization Act for Fiscal Year 2001, Subtitle G—Government Information Security Reform", Oct. 2000.
[15] Public Law 107- 347, "E-Government Act of 2002 Tile III. Information Security Federal Information Security Management Act of 2002", Dec. 2002.
[16] NIST SP 800-16 Revision 1 (3rd Draft), A Role-Based Model for Federal Information Technology/ Cybersecurity Training, Mar. 2014.
[17] Public Law 113-283, "Federal Information Security Modernization Act of 2014", Dec. 2014.
[18] Yeon Soo Lee and Su- yeon Lee, "A Study on Comparison and Development of Cyber Security Related Legal System in Major Nations", The Korea Association of National Intelligence Studies 1(2), pp. 35-116, 2009.
[19] KISA, A Comparative Law Study on the Cybersecurity Response System, KISA-WP-2015-0042, pp. 18-19, Dec. 2015.
[20] Public Law 113-246, "Cybersecurity Workforce Assessment Act," Dec. 2014.
[21] Public Law 113-274, "Cybersecurity Enhancement Act of 2014," Dec. 2014.
[22] Public Law 114-113, "Cybersecurity Act of 2015," Dec. 2015.
[23] OPM, "Memorandum on Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions", Jan. 2017.
[24] Public Law 115-278, "Cybersecurity and Infrastructure Security Agency Act of 2018", Nov. 2018.
[25] American Technical Council, Report to the President on Federal IT Modernization, Dec. 2017.

〈저 자 소 개〉



홍 순 좌 (Soonjwa Hong) 정회원
1989년 2월: 숭실대학교 전산학과 졸업
1991년 2월: 숭실대학교 전산학과 석사
2005년 8월: 충남대학교 컴퓨터과학과 박사
1991년 2월~2000년 1월: 국방과학연구소(ADD) 선임연구원
2000년 2월~현재: 한국전자통신연구원 부설연구소 책임연구원
〈관심분야〉 사이버보안 인력양성 정책, 미래 IT・보안기술, 사이버보안 기술・위협 분석, 국내외 정보보호 법・정책



김 준 수 (Joonsoo Kim) 정회원
2002년 2월: 서울대학교 전기공학부 졸업
2005년 12월: Univ. of Texas at Austin 전기 및 컴퓨터공학과(공학석사)
2011년 8월: Univ. of Texas at Austin 전기 및 컴퓨터공학과(공학박사)
2011년 8월~2014년 9월: Intel Co. 근무
2014년 9월~현재: 한국전자통신연구원 부설연구소 선임연구원/실장
〈관심분야〉 정보보호, 사이버보안 교육·훈련, 사이버 훈련장, 사이버위협 시뮬레이션, 국내외 정보보호 법·정책, 미래 IT·보안기술