정 보 보 호 학 회 지
제 29 권 제3호, 2019. 6

미국의 사이버보안 역량 강화를 위한 연방법률 발전 현황 분석

홍 순 좌*

요 약

미국의 사이버보안 관련 법률은 1987년 컴퓨터보안법이 제정되는 시점이 본격적인 시작이라고 할 수 있다. 1990년대에는 컴퓨터 및 인터넷의 발전으로 정보보안의 중요성이 대두되었으며 법률은 데이터 보호 및 프라이버시 중심으로 제정되었다. 2002년 국토안보부 설립을 위한 국토안보법의 제정을 통해 본격적인 국가 사이버보안 정책을 시작할 수 있는 토대를 마련하였다. 전자정부법(2002) 부속법률인 연방정보보안관리법(FISMA 2002)은 연방기관들의 사이버보안 관련 임무를 구체화하여 국가차원의 사이버위협 대응을 체계적으로 할 수 있었다. 2014년 연방정보현대화법(FISMA 2014)으로 개정되어 지난 10여년간의 시행착오를 바로잡는 노력을 진행하고 있다. 2015년 사이버보안법(Cybersecurity Act 2015), 2018년 사이버보안 및 기반구조보안기관법(CISA 2018)을 제정하여 국가 사이버보안 체계를 획기적으로 발전한 미국의 사이버보안 법률의 추진 현황을 살펴봄으로써 우리나라의 법체계의 발전방향에 대해 고찰해 보도록 한다.

Ⅰ. 서 론

1980년대는 개인 컴퓨터(Personal Computer, PC)의 등장으로 촉발된 컴퓨터 범죄사건을 대응하고 예방하기 위한 법률을 제정하는 시기였다. 이때는 컴퓨터라는 신종 정보관리 시스템의 관점에서 컴퓨터 보안(Computer Security) 시대를 열었던 시기라고 할 수 있다. 1990년대는 인터넷의 급속한 발전으로 하드웨어 장치 중심의 사고에서 정보(Information) 중심으로 보안을 생각하는 방향으로 전환되었으며, 이를 정보보안(Information Security)이 중심이 되었던 시대라고 할 수 있다.

2000년대에 들어와서 사이버공간이라는 개념이 등장하였으며, 국가 및 민간을 망라하여 정보시스템이 국가경제, 안보 등의 중심이 되었다. 세계 각국은 적성국 및 우호 국가를 가리지 않고 사이버상의 정보수집, 사이버 공격 등을 감행하고, 일반 민간인들은 익명성에 기대어 해킹을 무차별적으로 행하는 시대를 맞이하게 되었다. 2010년대는 스마트폰의 일반 대중화를 통해 모바일 시대로 진화하였으며, 각국은 더욱 심화된 사이버공간의 주도권을 확보하기 위해 세계2차 대전 후 냉전시대 만연했던 재래식 및 핵무기 경쟁에 버금가는 사이버무기 개발에 열을 올리는 시대로 전환되었다.

미국은 시대별로 국가차원의 사이버보안 분야의 대응을 가능하도록 효율적인 법률을 제정하여 사이버보안 분야의 방어 체계, 또는 심지어 공격을 포함하여 사이버보안 체계를 구축하도록 지원하였으며, 이를 기반으로 기술 개발 및 인력 양성에도 총력을 기울일 수 있도록 적극적인 지원을 해오고 있다.

시대별로 제정된 법률을 간략히 살펴봄으로써 미국의 사이버보안 체계 발전 현황을 파악할 수 있으며, 우리나라의 사이버보안 체계에 활용할 수 있는 법률적인 대응 방안을 도출하는데 밑거름이 될 수 있을 것으로 생각된다. [표 1]은 미국의 사이버보안에 관련하여 중요한 법률을 시기 순으로 정리하였다.

1980년대에는 컴퓨터 보안법(Computer Security Act of 1987)에서 보듯이 컴퓨터 보안과 함께 네트워크 보안이라는 용어가 사용되었다. 1990년대에는 IT 용어의 등장과 더불어 정보보안(information security), 정보보증(inform- ation assurance) 등의 용어가 사용되었으며, 90년대 후반기 인터넷의 등장 및 초고속인터넷의 발전에 따라 정보전(information warfare)이라는 새로운 용어가 등장하였다. 2000년대에 들어서 제정된 국토

* ETRI 부설연구소 사이버안전훈련센터(hongsj@nsr.re.kr)

〔표 1〕 US Federal Acts for Cybersecurity

Year	Act
1984	Small Business Computer Security and Education Act of 1984
1986	Computer Fraud and Abuse Act of 1986
1987	Computer Security Act of 1987
1995	Paperwork Reduction Act of 1995
1996	Clinger-Cohen Act of 1996(Information Technology Management Reform Act of 1996)
	National Information Infrastructure Protection Act of 1996
1999	Gramm-Leach-Bliley Act(Financial Services Modernization Act of 1999)
2000	Government Information Security Reform Act(GISRA 2000)
2002	Sarbanes-Oxley Act of 2002
	Homeland Security Act of 2002
	Cyber Security Enhancement Act of 2002
	Cyber Security Research and Development Act of 2002
	Federal Information Security Management Act(FISMA 2002)
2007	Department of Homeland Security Appropriations Act of 2007
	Energy Independence and Security Act of 2007
2009	Health Information Technology for Economic and Clinical Health Act(HITECH 2009)
2014	Cybersecurity Workforce Assessment Act of 2014
	Cybersecurity Enhancement Act of 2014
	National Cybersecurity Protection Act of 2014
	Federal Information Security Modernization Act(FISMA 2014)
2015	Federal Information Technology Acquisition Reform Act(FITARA 2015)
	Cybersecurity Act of 2015 · Cybersecurity Information Sharing Act · National Cybersecurity Protection Advancement Act · Federal Cybersecurity Enhancement Act · Federal Cybersecurity Workforce Assessment Act
2018	Cybersecurity and Infrastructure Security Agency Act of 2018
	NIST Small Business Cybersecurity Act of 2018

안보법(Homeland Security Act of 2002)은 부속절 ‘C-Information Security’ 내에 사이버보안 강화법(Cyber Security Enhancement Act of 2002)을 제정하였다. 이 법에서 보듯이 사이버보안 용어가 공식적으로 법에서 처음 등장하였으며 정보보안 내에 사이버보안을 포함시키는 개념으로 사용되었다. 이후 모든 국가 법·제도·정책 문서에서는 사이버보안(cybersecurity)이 가장 포괄적인 용어로 정리되어 사용되고 있다. 우리나라의 경우에도 더 이상 혼란을 피할 수 있도록 용어 재정립이 필요하다[5].

미국 법률 체계는 우리나라와 상이하므로 이에 대한 이해가 먼저 요구된다. 미국은 연방 국가이므로 연방법(Federal Law)과 주법(State Law)으로 구분되며, 일반적으로 미국 법이라 함은 연방법을 의미한다고 할 수 있다. 미국 법률의 최신 현황은 의회 도서관(Library of Congress, www.loc.gov) 소속된 미국의회법률사이트(www.congress.gov)에서 최신 입법 현황을 알아 볼 수 있다.

법안(bill)은 ① 발의(Introduced), ② 하원 승인(Passed House), ③ 상원 승인(Passed Senate), ④ 대통령 승인(To President), ⑤법률 확정(Became Law)과 같은 순서로 상태 추적(tracker)을 볼 수 있다. 많은 법안은 마지막 법률 확정 상태에 도달하지 못하고 폐기되어 다음 회기로 넘어가는 경우가 많다. 법률로 확정되면 “Public Law 회기번호-일련번호”로 명명된다. 미국 의회 회기는 2년 단위로 구성되는데, 하원의원 임기가 2년에 맞추어져 있다. 하원의원 선거가 2016년 11월 8일 실시되었던 115회 회기(2017~2018) 임기는 2017년 1월 3일부터 2019년 1월 2일까지이다.

115회기 중 18,726건의 법안이 상정되었으나 통과된 법률은 386건으로 약 2.1% 정도로 극히 적은 법안이 통과되었다. 114회기(2015~2016)에는 18,746건의 법안이 발의되었으나 약 1.8%인 329건이 법률로 확정되었다.

법률 내에 별도의 법률 명칭으로 불리는 경우가 일반적인 경우로 회계연도 통합세출법(Public Law 114-113, “Consolidated Appropriations Act of 2016”, December 18, 2015)은 Division A ~ Q까지 17개로 구성되어 있으며 그 중 DIVISION N에서 사이버보안법(Cybersecurity Act of 2015)을 규정하고 있다. 또한 사이버보안법 내에는 4개의 하위 법을 포함하는 방식으로 법률이 구성되어 우리나라의 법률체계와 다르므로 이에 대한 이해가 요구된다.

우리나라의 현행 법제는 부문별, 목적별로 개별법이 존재하고 있기 때문에 예상할 수 있을 정도의 사이버공격에는 대응할 수 있다. 그렇지만, 끊임없이 다양화·고

도화되고 있는 사이버공격에 탄력적으로 대응하기 위해서는 그에 따라 계속적으로 개별법이 만들어지거나 해당법률이 개정되지 않으면 더 이상 효과적인 대응능력을 확보하기 어렵다. 복합적으로 여러 부문 및 영역에 걸쳐 동시다발적으로 발생하고 있는 사이버공격의 양상에 비추어 볼 때, 현행 법제는 그 대응성이 떨어진다. 또한 급격하게 변화하는 사이버공격 기술에 대한 대응성을 높이는 것을 목적으로 법령을 개정하여 왔기 때문에 관련 법률 사이의 부정합성, 규율대상의 중복, 국가기관 등 관련 기관 사이의 권한의 중복 또는 충돌, 대응기관 및 관련 위원회의 과다한 설치 · 운영, 다양한 대응체계와 대응방법 등으로 인하여 사이버공격에 대한 체계적이고 통일적인 대응이 곤란하다[2].

본 논문은 10년 단위의 시대별로 미국의 사이버보안 관련 법제현황을 살펴보게 된다. 2장은 1980년대, 3장은 1990년대, 4장은 2000년대, 5장은 2010년 이후 현재까지 제정된 법률을 설명한다. 6장에서는 앞서 논의한 사항들에 대한 시사점과 결론을 맺는다.

Ⅱ. 1980년대 사이버보안 법률 현황

1970년대 말 애플 I, II의 등장을 통해 1980년대는 개인 PC의 서막을 여는 시대였으며, 마이크로소프트 MS-DoS 운영체제와 결합된 IBM PC의 등장은 기존 중앙집중식 대용량 메인프레임 중심을 개인으로 이동하는 IT 시대의 신기원이라고 할 수 있다. 이때의 주요 법률은 다음과 같이 3개 정도로 컴퓨터 사기 및 절도 등의 신종 범죄 등장에 따른 대응이 주된 목적이라고 할 수 있다.

2.1. 소기업 컴퓨터 보안 및 교육법(1984)[7]

1984년 제정된 소기업 컴퓨터 보안 및 교육법(PUBLIC LAW 98-362, "Small Business Computer Security and Education Act of 1984", July 16, 1984)에서 의회의 최신 정보기술에 대한 인식을 알 수 있는 사례이다.

미국 의회는 1984년도에 소규모 기업 사회에서 컴퓨터, 데이터 네트워크, 통신 장치 등을 포함한 정보 기술(information technology)의 의존도가 증가하고 확산되었으며 이 정보 기술은 소기업에 범죄 활동의 증가를 유발하였다고 인식하고 있다.

또한 소기업의 상황의 어려움을 인식하여 소기업의 정보 기술을 활용하여 경영을 개선하고, 소기업이 고의적 또는 의도하지 않은 조작이나 파괴로부터 그러한 기술을 보호하도록 교육하고 장려하는 것이다. 소기업에 있어 IT의 필요성과 위험성을 확인하여 교육을 강화할 것을 규정하였고, "Small Business Computer Security and Education Advisory Council"를 90일 이내 설립을 의무화하였다.

2.2. 컴퓨터 사기 및 오용 방지법(1986)[8]

1986년 제정된 컴퓨터 사기 및 오용 방지법(Public Law 99-474, “Computer Fraud and Abuse Act of 1986,” October 16, 1986)은 1984년도에 발의 되었던 “Building on the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984” 법안을 수정하여 재발의 하여 승인된 법률이다.

기존에 발의된 법안의 주 내용은 허가 없이 컴퓨터와 컴퓨터 네트워크에 액세스하고 사용하는 것을 불법으로 명시하기 위해 발의되었다. 컴퓨터 사기 및 오용 방지법에서 추가된 주요 내용은 허가 없이 데이터를 파괴하거나 훔친 패스워드를 배포하는 것과 같은 추가 조치를 불법으로 명시하였다.

1988년 코넬대학교 졸업생인 Robert Morris는 일명 “모리스 웜”으로 명명된 최초 컴퓨터 웜을 개발하여 전 세계 UNIX 시스템의 10%에 해당하는 6,000여대의 컴퓨터를 마비시켜 약 백만불의 피해를 초래한 혐의로 기소되었다. 이 사건을 일으킨 Morris는 컴퓨터 사기 및 오용 방지법에 의거하여 보호관찰 3년, 사회봉사 400시간, 10,050달러의 벌금 및 보호관찰 비용 지불의 처분을 받았다.

2.3. 컴퓨터 보안법(1987)[10]

사이버보안의 서막을 열어젖힌 법률은 1987년의 컴퓨터 보안법(Public Law 100-235, “Computer Security Act of 1987,” January 8, 1988)으로 서, 연방기관이 중요한 정보를 보호하기 위한 기본적인 사이버보안 조치를 취하도록 보장하기 위해 제정되었다. 이 법안에서 국가안보국(National Security Agence, NSA)의 지원을

통해 국립표준국(National Bureau of Standards, NBS)이 사이버보안 표준 개발의 주관기관(Lead Agency)으로 지정되었다. 이 법은 2002년 연방정보보안관리법(FISMA 2002)으로 대체되었다.

국가표준국은 법률로서 매년 예산을 책정하는데 1987년 NBS 예산 법(Public Law 99-574, "National Bureau of Standards Authorization Act for Fiscal Year 1987", OCT. 28, 1986)에서 1987년 예산 약 1억 2천 4백만$를 규정하였으며 다음과 같은 예산 분야 및 예산액을 지정하였다[9].

- o Measurement Research & Standards $36,582,000
- o Materials Science and Engineering $21,228,000;
- o Engineering Measurements & Standards $35,875,000
- o Computer Science and Technology $7,500,000
- o Research Support Activities $22,768,000.

4번째 컴퓨터 과학 및 기술 예산 7백 5십$만 중 1백만$을 컴퓨터보안 활동(Computer Security Activities)에 쓸 것을 의무화한 첫 법률이다.

Ⅲ. 1990년대 사이버보안 법률 현황

1990년대는 마이크로소프트의 윈도우즈는 PC 운영체제의 독점적 지위를 확보하였고, 인터넷의 대중화와 웹의 개발 및 보편적 사용이 등장한 시대로서, 이 시기는 인터넷의 대중화를 통해 정보보안 시대를 열었던 때로 볼 수 있다.

3.1. 문서감축법(1995)[11]

문서감축법(Public Law 96-511, “Paperwork Reduction Act of 1980,” Dec 11, 1980)은 1908년에 처음 제정되었으며, 1995년 문서감축법(Public Law 104-13, “Paperwork Reduction Act of 1995,” May 25, 1995)으로 개정하였다. 1995법에 정보수집 검토 프로세스, 정보자원 관리, 관련 정책 및 가이드라인을 시행하기 위해 백악관 관리예산국(Office of Management and Budget, OMB) 및 모든 연방기구와 의회 및 공공기관에 대한 책임을 부여하였다.

이 법을 근거로 정보 및 규제 업무국(Office of Information and Regulatory Affairs, OIRA)으로 알려진 사무소가 OMB에 설립되었다. 또한 이 법은 연방정부 기관 대상의 사이버보안 정책을 담당하는 책임 기관으로 OMB를 지정하여, OMB가 미국 연방기관의 사이버보안의 리더십을 확보하게 되었다.

3.2. Clinger-Cohen 법(1996)[12]

1996년 제정된 Clinger-Cohen Act(Divisions D and E, Public Law 104-106, “Clinger-Cohen Act of 1996,” February 10, 1996)는 사이버보안 정책 및 프로세스와 관련된 기관의 책임을 지정하고 있다. 이 법은 1996년 국방수권법(National Defense Authorization Act)내 5개의 디비전 중 ‘Division E－Information Technology Management Reform의 Title LI’이다. 연방정부가 IT를 획득, 사용 및 폐기하는 방법을 개선하기 위해 마련된 법인 정보기술관리개혁법(Information Technology Management Reform Act of 1996, ITMRA)을 부르는 별칭이 Clinger-Cohen Act이다.

이 법에서 집행기관이 정보자원의 획득 및 관리를 개선하기 위한 포괄적인 접근 방식을 수립함으로써 다음과 같은 정보 자원 관리 정책을 수립할 수 있도록 규정하고 있다.

- o 전략적 임무 지원을 위해 정보 자원 계획에 초점을 맞춘다.
- o 예산 수립 및 집행에 연계 된 자본 계획 및 투자 통제 프로세스 실행한다.
- o 정보 시스템에 투자하기 전에 자신의 업무 방식을 재고하고 재구성해야한다

3.3. 국가정보기반보호법(1996)[13]

국가정보기반보호법(Title II, Public Law 104-294, “National Information Infrastructure Protection Act,” October 11, 1996)은 산업스파이방지법(Economic Espionage Act of 1996)의 Title II에 해당하는 부속법으로, “18 U.S. Code § 1030 - Fraud and related activity in connection with computers”의 조항에서 컴퓨터 범죄의 정의를 확대하여 1986년의 컴퓨터 사기 및 오용 방지법을 보완하였다.

3.4. Gramm-Leach-Bliley법(1999)[14]

Gramm-Leach-Bliley Act(Title V, Public Law

106-102, “Gramm-Leach-Bliley Act of 1999,” November 12, 1999)의 “Title V - Privacy”에서 금융기관이 고객에 관한 모든 민감한 데이터의 기밀성을 보호하도록 요구하고 있다.

Gramm‐Leach‐Bliley Act(GLBA)는 금융서비스 현대화법(Financial Services Modernization Act of 1999)으로 불리기도 한다,

Ⅳ. 2000년대 사이버보안 법률

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.

국방수권법 2000(PUBLIC LAW 106‐65, National Defense Authorization Act for Fiscal Year 2000, OCT. 5, 1999)에서 핵무기 통제 담당 국장은 주관청의 모든 시설에 대한 물리적, 사이버 보안(cyber security) 및 자재의 보호, 통제 및 회계를 포함하여 주관청의 보안 프로그램을 개발하고 시행하는 책임을 진다라고 규정하고 있다. 여기서 "cyber security"가 법률에 처음 등장하고 있다[15].

2000년대에 들어서 법률 제목으로 “Cyber Security”, “Cybersecurity” 용어가 등장하였으며, 법령 내에서 혼재되어 사용되고 있으나, 향후 “Cybersecurity”로 통일되어 왔다.

4.1. 정부정보시스템개혁법(GISRA 2000)[16]

정부정보보안개혁법(별칭 “보안법”, Security Act of 2000)인 Government Information Security Reform Act(GISRA 2000)는 USC Title 44 Chapter 35를 개정하기 위해 만든 법(§3531 ~ §3536)으로 1995년 문서감축법(PRA 1995)을 개정하였으며 1987년의 컴퓨터보안법과 1996년의 정보기술관리개혁법(ITMRA 1996, Clinger-Cohen Act)을 강화 및 보강하였다. PRA 1995 및 Clinger-Cohen과 마찬가지로 보안법은 연방기관의 보안 프로그램 및 실무(practices)를 전체 프로그램, IT 관리 및 자본 계획 및 예산 프로세스에 연결하여 통합관리 하도록 한다.

PRA, 컴퓨터보안법, 정보기술개혁법에 분산되어 체계적으로 추진이 어려웠던 국가 차원의 연방기관 정보보안 강화를 위해 2년 동안 한시적으로 유지되는 보안법이 마련되었으며, 2001년 911테러 발생으로 인해 정보보안 강화를 위한 법적인 내용이 보다 구체적이며 실천적인 정책으로 자리 잡을 수 있었다. 보안법을 대체하기 위해 FISMA 2002가 제정되어 연방기관에 대한 정보보안 정책이 더 강화되어 시행될 수 있었다.

보안법은 보안 프로그램 관리, 구현, 평가의 세 가지 기본 구성요소를 기준으로 설명하고 있다. 첫 번째 구성요소는 관리적인 측면인데, 보안이 기술적 구성요소 보다도 핵심요소는 필수적인 관리 기능임을 인식해야 한다는 것이다. 우리나라 정보보안 현실에 대한 명확한 방향을 보여주는 방향타로 인식할 수 있다. 두 번째는 보안의 구현을 위해 IT 프로그램 및 관련 예산과 통합되어야 한다는 것을 강조한다. 기술적인 특장점이 아닌 프로그램 통합 및 예산 지원이 없다면 기관의 보안 구현이 어려워진다는 것을 인식하고 있다. IT 프로그램을 담당하는 CIO에게 보안이 기관의 전반적인 프로그램 및 엔터프라이즈 아키텍처와 적절하게 통합되도록 보장해야하는 책임을 부여하였다. 세 번째는 평가 분야로서, 프로그램 담당자와 CIO는 기관의 모든 IT 프로그램과 시스템에 대한 연간 보안 검토를 수행할 것을 규정하고 있다. 평가의 공정성을 위해 감사관(Inspector General, IG)은 기관의 보안 프로그램과 기관의 일부 시스템을 선별하여 독립적 평가를 수행하고 그 결과를 OMB에 보고하도록 규정하고 있다.

미국 연방정부는 보안법에서 규정한 3가지 구성요소에 대한 실천을 OMB 중심으로 회계연도 2001년부터 실시하였다. 이후로 FISMA 2002, FISMA 2014로 관련법이 개정되면서 CIO 중심의 기관 검토보고서와 IG 평가보고서를 각 기관들은 매년 OMB의 지침에 의거 작성하여 보고하고 있다. OMB는 각 기관의 보고서를 취합하여 정리하여 의회에 보고하는 방식으로 FY 2001부터 현재까지 추진하고 있다.

- o GISRA 2000(3년) : FY 2001~FY 2003
- o FISMA 2002(11년) : FY 2004~FY 2014
- o FISMA 2014(4년) : FY 2015~ FY2018

2000년 10월 30일 제정된 GISRA 2000에 의거하여

3개월 후인 2001년 1월 OMB는 각 기관들에게 GISRA 2000을 이행하도록 관련 구현 지침(Implementation Guidance)를 하달하였으며, 2001년 6월에는 보고서 작성을 지시하는 보고 지침(Report Instructions)을 하달하였다. 18년 동안 일관성 있게 국가 차원의 정보보안 강화를 위한 정책을 추진한 결과 미국은 세계에서 가장 체계적인 사이버보안 체계를 갖출 수 있었다. 또한 IT 보안 및 사이버보안 산업계의 글로벌 리더십도 확보하는데 있어 핵심역할을 수행하였다.

4.2. Sarbanes-Oxley 법(2002)[17]

Sarbanes-Oxley Act(Public Law 107-204, “Sarbanes-Oxley Act of 2002,” July 30, 2002)의 TITLE IV(Enhanced Financial Disclosures)에 포함된 “15 USC 7262, SEC. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS”에서 미국 기업을 대상으로 사이버보안 조치를 비롯한 내부통제에 대한 연간 단위의 평가(annual assessments)를 산출하는 요구사항이 포함되어 있다.

4.3. 국토안보법(2002)[18]

국토안보법(Titles II and III, Public Law 107-296, “Homeland Security Act of 2002,” November 25, 2002)은 사이버보안 위협 포함 각종 위협으로부터 국가를 보호하고 이러한 위협의 결과로 발생한 재난 대처를 위한 연방정부의 노력에 초점을 맞추는 국토안보부(Department of Homeland Security, DHS) 설립을 명시한 법이다.

국토안보법은 미국의 전체 국가기반을 보호하기 위한 법으로 17개 Title로 구성되며, 특히 사이버보안과 관련된 법률은 [표 2]와 같다. 이 법은 미국 연방기관들이 분야별로 각각 분담하고 있는 국토안전보장업무를 총괄하는 국토안보부를 설립하여, 정보기술을 활용하여 사이버 또는 물리적 공격으로부터 미국 영토를 방어하기 위해 주요기반보호를 국토안보의 핵심으로 인식하여 이를 실행하는 정보분석기반시설보호국(Directorate for Information Analysis and Infrastructure Protection, IAIP)을 설치하였다.

기존 FBI 국가기반시설보호센터(NIPC: National Infrastructure Protection Center), 상무부 주요기반보장국(Critical Infrastructure Assurance Office, CIAO), 국방부 국가통신시스템(National Communications System), GSA(General Services Administration) 연방컴퓨터사고대응센터(Federal Computer Incident Response Center) 등의 기구를 국토안보부로 통합하여 국토안보부가 주요기반시설의 보호와 사이버공격 대응에 대해 총괄하고 조정하도록 임무를 부여하였다.

〔표 2〕 Cybersecurity Laws in Homeland Security Act of 2002

Public Law 107-296, “Homeland Security Act of 2002,”
TITLE II－INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION
Subtitle A－Directorate for Information Analysis and Infrastructure Protection; Access to Information
Sec.201. Directorate for Information Analysis and Infrastructure Protection Sec.202. Access to information
Subtitle B－Critical Infrastructure Information
Sec.211. Short title Sec.212. Definitions Sec.213. Designation of critical infrastructure protection program Sec.214. Protection of voluntarily shared critical infrastructure information Sec.215. No private right of action
Subtitle C－Information Security
Sec.221. Procedures for sharing information Sec.222. Privacy Officer Sec.223. Enhancement of non-Federal cybersecurity Sec.224. Net guard Sec.225. Cyber Security Enhancement Act of 2002
Subtitle D－Office of Science and Technology
Sec.231. Establishment of office; Director Sec.232. Mission of office; duties Sec.233. Definition of law enforcement technology Sec.234. Abolishment of Office of Science and Technology of National Institute of Justice; transfer of functions Sec.235. National Law Enforcement and Corrections Technology Centers Sec.236. Coordination with other entities within Department of Justice Sec.237. Amendments relating to National Institute of Justice

4.4. 사이버보안강화법(2002)[18]

사이버보안강화법은 2002년 중반 하원에서 통과 후 상원에서 폐기되었으나, 국토안보법에 포함되어 통과되었다. Title II(Information Analysis and Infrastructure Protection) 내의 Subtitle C(Information Security)의 Sec. 225. Cyber Security Enhancement Act of 2002로 규정하고 있다.

이 법에서 양형위원회 관련 내용, 긴급 공개 예외, 선의의 예외규정, 불법장치의 인터넷 광고, 강화된 벌칙, 프라이버시 보호 등이 규정되어 있다. 사이버 공격자가 고의 또는 부주의로 법률을 위반하여 심각한 신체적 상해를 유발하거나 시도하는 경우에 벌금이나 20년 이하의 징역에 처하며, 공격자가 고의 또는 과실로 사망을 유발하거나 유발하고자 시도하는 경우에 유기 또는 무기징역에 벌금을 부과할 수 있도록 규정하여 신체의 상해나 생명의 위험과 관련된 컴퓨터 범죄의 처벌을 대폭 강화하고 있다[1].

4.5. 사이버보안 연구개발법(2002)[19]

사이버보안 연구개발법(Public Law 107-305, “Cyber Security Research and Development Act,” November 27, 2002)의 목적은 연방정부의 사이버보안 연구 및 개발 자금을 확대하는 것이며, 다음과 같은 연구・개발 지원 및 규제를 규정하고 있다.

- o 국립과학재단(NSF)주관의 연구보조금(research grants) 지원
- o NSF와 NIST에서 지원하는 연구단체 지원
- o NIST 개발 보안구성체크리스트를 통해 기관들이 컴퓨터 하드웨어, 소프트웨어 보안을 유지할 수 있도록 지원
  - * NIST 프로젝트인 **Federal Desktop Core Configuration (FDCC)**가 이에 해당됨
- o NIST가 설립한 컴퓨터 시스템 보안 및 개인 정보 보호 자문위원회(Computer System Security and Privacy Advisory Board, CSSPAB) 운영
  - * 추후 CSSPAB는 정보보안 및 개인정보보호 자문위원회(Information Security and Privacy Advisory Board, ISPAB)로 변경됨
- o 국립과학아카데미(National Academy of Science)의 핵심 기반시설에 대한 사이버보안 연구 지원
- o NSF와 NIST 간의 연방 사이버보안 R&D 노력의 조정

이 법의 제정일로부터 24 개월 이내에 NSF 이사장은 국가안보보좌관과 협의하여 의회에 수행하는 프로그램과 지원하는 단체 활동에 대한 보고서를 제출해야 한다고 규정하고 있다.

4.6. 연방정보보안관리법(FISMA 2002)[20]

연방정보보안관리법(Federal Information Security Management Act of 2002)은 전자정부법(Public Law 107-347, “E-Government Act of 2002”, December 17, 2002)의 Title III－Information Security를 부르는 별칭이다.

FISMA 2002는 모든 연방기관이 최소한의 기본적인 사이버보안 조치를 취하도록하기 위한 것이며, NIST를 연방기관(federal agency)의 시스템 보안을 위해 사용되는 보안 가이드라인 및 지침(guidance)을 개발하는 기관으로 지정했다. FISMA 2002는 다음과 같이 9개의 섹션으로 구성된다.

① 목적(§ 3541. Purposes)
② 정의(§ 3542. Definitions)
③ 디렉터의 권한과 기능(§ 3543. Authority and functions of the Director)
④ 연방기관의 책임(§ 3544. Federal agency responsibilities)
⑤ 연례 독립적 평가(§ 3545. Annual independent evaluation)
⑥ 연방 정보보안사고센터(§ 3546. Federal information security incident center)
⑦ 국가보안시스템(§ 3547. National security systems)
⑧ 세출 승인(§ 3548. Authorization of appropriations)
⑨ 현행법에 대한 영향(§ 3549. Effect on existing law)

FISMA 2002의 목적(§3541)은 총 6개의 항목으로 구성되어 있으며 세부 내용은 다음과 같다.

① 연방 운영 및 자산을 지원하는 정보자원에 대한 정보보안 통제의 효과를 보장하기 위한 포괄적인 (comprehensive) 프레임워크를 제공
② 현재의 연방 컴퓨팅 환경의 고도로 네트워크화 된 특성을 인식하고 민간인, 국가 안보 및 법 집행 공동체 전반에 걸친 정보보안 노력의 통제를 포함하여 관련 정보보안 위험에 대한 정부 차원의 효과적인 관리 (management) 및 감독(oversight)을 제공
③ 연방 정보 및 정보시스템을 보호하는 데 필요한 최소 통제(minimum controls)를 개발하고 유지 관리
④ 연방기관 정보보안 프로그램의 감독을 개선 할 수 있는 메커니즘을 제공
⑤ 상업적으로 개발된 정보보안 제품이 국가의 국방 및 경제 안보에 중요한 정보 인프라를 보호하기 위한 효과적인 정보보안 솔루션을 제공함을 인정
⑥ 상업적으로 개발된 하드웨어・ 소프트웨어 정보 보안 솔루션 중에서 선택하는 책임은 개별기관에 맡겨져야 함을 인식

FISMA의 목적에 대해 연방정부 및 기관에 대한 적용 방안을 분석해 보면 다음과 같은 내용을 제시하고 의무화하고 있다고 할 수 있다.

- o 정보보안 체계에 대한 프레임워크 개발을 의무화
- o 정부 중심의 중앙 관리 및 감독을 의무화
- o 정보보안의 최소 통제항목을 개발·적용할 것을 의무화
- o 보고서, 평가 등을 통한 정보보안 감독을 강화할 수 있는 메커니즘을 개발하여 적용할 것을 의무화
- o 민간 기업의 참여가 가능하도록 인증 및 인정 절차를 마련하도록 권고
- o 민간 기업 제품에 대한 공급 및 선택 권한은 개별 기관에게 권한을 부여하여 경쟁력을 높이며, 민간기업의 수익모델을 강화하는 정책

FISMA 2002를 근거로 모든 연방기관들은 1년 단위의 독립적인 평가를 수행하며 그 결과를 보고서 형태로 OMB에 제출하여야 한다. OMB는 제출된 기관들의 평가 보고서를 정리하여 의회에 보고하도록 규정하고 있다. 이와 같은 절차를 매년 반복하여 연방기관들의 사이버보안 수준을 높이도록 노력해 왔다.

4.7. 국토안보부 세출법(2007)[21]

국토안보부 세출법(Public Law 109-295, “Department of Homeland Security Appropriations Act, 2007,“ October 4, 2006)의 Title XVIII－Emergency Communications에서 사이버보안 요구사항을 포함하여 화학 시설 보안에 대한 새로운 규정을 요구했다.

4.8. 에너지 독립 보안법(2007)[22]

에너지독립보안법(Public Law 110-140, “Energy Independence and Security Act of 2007,” December 19, 2007)의 “TITLE V GENERAL PROVISIONS, SEC. 546. (1) (B) (i)”에서 NIST를 스마트 그리드에 대한 상호운용성 표준을 만드는 노력을 주도한 기관으로 지정하여 사이버보안의 중심 역할을 담당하는 NIST의 업무 범위는 스마트그리드를 포함하여 지속적으로 확대되고 있다.

4.9. 건강정보기술에 관한 법률(HITECH 2009)[23]

건강정보기술에 관한 법률(HITECH, Health Information Technology for Economic and Clinical Health Act of 2009)은 미국의 복구 및 재투자법(Public Law 111-5, “American Recovery and Reinvestment Act of 2009”, February 17, 2009) 내의 법률로서 [표 3]과 같이 구성된다.

이 법은 의료 데이터 위반에 대한 통지를 요구하고 의료 데이터의 불충분한 보호에 대한 처벌을 강화함으로써 건강보험 양도 및 책임에 관한 법(HIPAA 1996)을 토대로 구축되었다.

〔표 3〕 HITECH Act 2009

PUBLIC LAW 111-5— FEB. 17, 2009 American Recovery and Reinvestment Act of 2009
DIVISION A— APPROPRIATIONS PROVISIONS
TITLE XIII— CYBERSECURITY INFORMATION SHARING
SEC.13001. SHORT TITLE; TABLE OF CONTENTS OF TITLE. (a) SHORT TITLE.— This title (and title IV of division B) may be cited as the ‘‘**Health Information Technology for Economic and Clinical Health Act**’’ or the ‘‘**HITECH Act**’’.
DIVISION B— TAX, UNEMPLOYMENT, HEALTH, STATE FISCAL RELIEF, AND OTHER PROVISIONS
TITLE IV— MEDICARE AND MEDICAID HEALTH INFORMATION TECHNOLOGY; MISCELLANEOUS MEDICARE PROVISIONS

Ⅴ. 2010년대 사이버보안 법률

2000년대 말에 등장한 스마트폰이 본격적으로 일상생활에 보급이 되어 대부분의 사람들의 필수품이 되었다. 전 세계는 인터넷에 대한 의존도가 더욱 심화되었으며, 각국의 사이버보안 경쟁도 치열하게 전개되고 있는 시대이다.

2010년도 사이버보안 강화법(Cybersecurity Enhancement Act of 2010) 발의를 시작으로 2014년도에는 FISMA 2002를 개정한 FISMA 2014(Federal Information Security Modernization of 2014)외 3종의 법률, 2015년도에는 하위법률 4종을 포함하는 사이버보안법(Cybersecurity Act of 2015) 등 사이버보안 관련 법률이 급속히 확대 및 강화되었다.

미국은 2013년도 스노든 사건 등으로 인해 국가안보 체계의 급격한 변화가 시작되었다. 비밀로 유지되었던

미국의 사이버 공격 전략, 기술 개발 등이 스노든 및 위키리크스 등의 문건 공개 등을 통해 공식적으로 인정할 수 밖에 없는 상황이었다. 이로 인해 사이버보안 관련 법률이 2014년부터 본격적으로 제정되었던 상황도 이들 사건들과 연관성이 있다고 할 수 있다.

기존에는 FISMA 2002를 현실에 맞게 개정하여 FISMA 2014로 개정하였으며 조직과 권한・행위 등을 통한 사이버보안 강화를 주요 주제로 삼아왔다. 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 사이버보안 인력 경쟁력을 확보하고자 노력하고 있다.

우리나라도 이에 대한 정책 등을 면밀히 검토 및 고려하여 화이트해커 양성이라는 단순한 구호를 외치는 인력 양성 방향을 현실에 사이버보안 전문 인력 양성 정책을 수립하고 실천해가야 할 것으로 생각된다.

5.1. 사이버보안 인력 평가법(2014)[24]

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

이 법은 국토안보부 장관이 국토안보부의 사이버보안 인력들을 평가 하고 새로운 종합인력개발을 위해 제정된 법으로 사이버보안 인력의 체계 강화나 인원 충원 대책 등에 대해 규정하고 있다.

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

5.2. 사이버보안강화법(2014)[25]

사이버보안강화법(Public Law 113-274, “Cybersecurity Enhancement Act of 2014,” December 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.

이 법은 사이버 위험(cyber risks) 감소를 위한 표준과 대응절차 등을 수립하고, 연구개발 능력 향상, 인력 양성 및 교육, 인식 제고 등을 수행할 목적으로 2010년 법을 개정하였다. 이 법은 국립표준기술연구소(NIST)에 부여되었던 임무를 법제화하였고 공공・민간 파트너십을 강화하도록 법률을 제정하였다.

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

5.3. 국가사이버보안보호법(2014)[26]

국가사이버보안보호법(Public Law 113-282, “National Cybersecurity Protection Act of 2014,” December 18, 2014)의 목적은 국가사이버보안통신통합센터(National Cybersecurity and Communications Integration Center, NCCIC)의 책임을 규정하고 있다.

이 법은 국토안보법 “TITLE Ⅱ－INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION“을 개정하여 국가차원의 사이버안보 추진체계를 강화한 법으로서 NCCIC의 법제화를 규정하였다.

국가사이버보안보호법은 범국가적인 사이버안보실현을 위한 추진체계를 강화시킨 법률이다. NCCIC의 소속, 역할, 책임 범위를 법제화하여 사이버위협에 대한 구심점적인 역할을 수행할 수 있는 법적 근거를 마련하였다[3].

NCCIC는 국토안보부 NPPD(National Protection and Programs Directorate) 소속으로 국토안보부 차관보 관리하에 있다. US-CERT(US- Computer Emergency Response Team), NCC (National Coordinating Center for Commun- ications), ICS-CERT(Industrial Control Systems Cyber Emergency Response Team), NO&A(NCCIC Operations & Integration) 등의 기관이 NCCIC 산하에

있다.

5.4. 연방정보보안현대화법(FISMA 2014)[27]

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 사이버 안보의 중요성을 인식하여 백악관의 OMB와 NIST에 법적 임무를 부여하여 제도, 인력, 기술을 포괄하는 사이버보안체계를 정립하여 지속적으로 추진해 왔다. 2014년에 12년간 지속하던 FISMA 2002를 개정하여 연방정보보안현대화법(Public Law 113-283, “Federal Information Security Modernization Act of 2014,” December 18, 2014, FISMA 2014)을 공표하였다.

미국 사이버보안 체계는 컴퓨터보안법(1997), 연방정보보안관리법(FISMA 2002), 연방정보보안현대화법(2014) 등 강력하고 구체적인 연방법을 기반으로 발전해왔다. FISMA 2002는 국가차원의 일원화된 정보보안 개선을 추진하기 위해 OMB 중심의 관리체계를 구축하였으며 각 연방기관은 FISMA 관련 업무 수행을 의무화 하였다[1][2].

연방 기관들은 FISMA 2002의 목표를 달성하는 능력을 제한하는 몇 가지 문제에 봉착했다. 예를 들어, FISMA 2002는 법 집행에 책임이 있는 여러 연방기관을 지정했으나, 기관들은 끊임없이 증가하는 사이버 공격의 위협에 대처할 수 없었다. 이러한 도전 과제를 해결하기 위해 의회는 FISMA 2002를 업데이트하기 위해 FISMA 2014를 제정했다. 의회는 OMB와 미국 국토안보부(DHS)의 역할을 명확히 하고 체계화하기 위해 이 업데이트를 계획했다. 이는 OMB에 연방 기관 전반의 정보 보안을 감독하고 관리하는 권한을 부여했으며, 연방 시스템 모니터링을 통해 연방 사이버 보안의 운영 측면을 담당하는 기관으로 공식적으로 DHS를 설립했다. FISMA 2014는 또한 사이버 사건보고 과정에서 투명성을 제고하고 통일성을 확보함으로써 정부가 연방 데이터 위반을 관리하는 방식을 조정했다[3].

목적에서의 중요한 변화는 (44 U.S.C. §3551(4)) 연방기관 정보 보안 프로그램의 감독을 개선 할 수 있는 메커니즘을 제공하는데 있어서 보안성 강화를 위한 지속적인 진단(continuously diagnose) 및 개선을 수행하는 자동화 보안 도구(automated security tools)를 사용하는 것을 포함하고 있다는 것으로, 관리적인 측면에 기술적인 수단을 규정하는 내용이다. 이 의미는 자동화 도구에 대해 연방기관이 사용할 것을 규정하고 있으며, 이 조항으로 인해 자동화된 보안 진단 도구 분야에 관련된 기업의 결과물이 연방정부에 공급할 수 있는 계기를 부여하고 있다는 것이다.

전반적으로 국토안보부의 권한을 강화하여 일원화된 사이버보안 체계를 규정하고 있다. 연방정부의 사이버보안에 관련된 사무를 국토안보부로 대폭 이관하여 국토안보부의 권한 및 기능을 강화한 것이다. 국토안보부 권한 강화를 살펴보면 다음과 같다.

- o FISMA 2014의 가장 큰 변화는 연방정부의 정보보호 및 사이버안보에 관한 사무를 DHS로 대폭 이관하여 국토안보부의 권한 및 기능을 강화한 것이다.
- o DHS는 연방정보보안관리에 관한 OMB의 업무수행을 지원하고(44 U.S.C. §3553(b)(1))
- o OMB 표준과 가이드라인에 대한 운용지침을 수립하며, 연방기관의 수행 사항을 감독한다(44 U.S.C. §3553(b)(2)).
- o DHS는 연방기관의 정보보안 정책 실행을 모니터링하고(44 U.S.C. §3553(b) (3)), 정보보안 정책 실행의 효율성을 향상시키기 위해 연방기관들의 고위급 회의를 소집하여야 한다(44 U.S.C. §3553(b)(4)).
- o 정보보안 정책에 대한 범정부적 노력을 조정하고(44 U.S.C. §3553(b)(5)), 연방기관의 운영 및 기술에 관한 사항을 지원한다 (신설, 44 U.S.C. §3553(b)(6)).
- o 기존의 OMB에서 국토안보부로 이관된 연방정보보안사고센터(Federal information security incident center)3)의 역할을 증대하였다(44 U.S.C. §3556(a)(4)).
  - 연방정보보안사고센터가 사이버위협, 취약점, 사고 관련 정보를 각 기관에 제공하도록 하는 조항을 신설하여 기관들이 이를 위험평가에 활용할 수 있도록 하였다(44 U.S.C. §3556(a)(4)).

FISMA 2014는 사이버보안에 대한 연방기관의 책임을 변경하였으며, 그 주요 내용은 다음과 같다.

- o FISMA 2014는 사이버보안에 관한 각 연방기관의 책임과 역할을 조정하였다. 연방기관은 정보보안 관리절차를 기관의 전략계획, 운영계획, 예산계획과 통합하여 관리하여야 한다(44 U.S.C. §3554(a)(1)(C)). 정보보안 관리절차를 전략계획 및 운영계획과 통합하고 기존 법률에 예산 계획을 추가함으로써

연방기관의 정보보안 관리역할을 증대하였다.
- o 각 기관 경영자급(CIO 포함)은 기관의 정보보안 요구사항을 수행하여야 하고(44 U.S.C. §3554(a)(6)), 모든 직원들은 범 기관차원의 정보보안 프로그램을 준수하여야 한다(44 U.S.C. §3554(a)(7)).
- o 정기적 위험평가, 보안절차 테스트, 보안사고 탐지・보고・대응 등을 위한 정보보안 프로그램을 발전시키고 문서화하며 이를 실행하여야 한다.
- o 정보보안 프로그램 실행 시 자동화 도구(automated tool)를 활용할 것을 규정함으로써(44 U.S.C. §3554(b)(1)) 정보보안 관리의 효율성 증대하였다.
- o 보안사고 발생 시 기존과 달리 각 기관은 종래의 사고 통지 대상인 수사기관, 감사관, 대통령이 지정한 기관(국가안보시스템 포함), 기타 법률에 의하거나, 대통령이 지시한 기관 외에도 법무자문관, 의회 소관 위원회에게 사고를 통지하여야 한다(44 U.S.C. §3554(b)(7)(C)(iii)).
- o 각 기관들은 중대한 사고에 관한 연례보고서를 OMB, 국토안보부, 의회, 회계감사원에 제출하여야 한다(44 U.S.C. §3554(c)(1)(A)).

연례 독립평가의 실효성을 증대시키기 위하여 다음과 같은 내용을 보완하였다.

- o FISMA 2014는 회계감사원이 각 기관의 감사관 및 기관장에게 보안통제 및 보안절차에 대한 평가 등 기술적 조언을 제공하도록 하는 조항을 신설함으로써 연례 독립평가의 실효성을 증대시켰다(44 U.S.C. §3555(i)).
- o 기존의 회계감사원은 기관들의 정보보안 정책 및 훈련의 효과와 적절성, 법률에 의한 요구사항 준수를 평가하고 의회에 보고하는 역할만을 수행하였고 평가대상기관에게 이에 대한 기술적인 조언은 하지 않았다. 개정된 법률에서는 회계감사원이 연방기관의 정보보안 정책 효과와 법률 준수 여부 등에 대해 평가한 결과를 활용하여 연방기관에게 기술적 조언을 하도록 정함으로써, 평과결과를 활용한 장래의 정보보안개선이 가능하게 되었다.

기타 신설 및 변경사항은 다음과 같다.

- o OMB가 정보보안 프로그램 및 훈련 효과를 측정하기 위한 가이드라인을 수립할 것을 내용으로 하는 조항을 신설(44 U.S.C. §3555(j))
- o 기존 OMB가 CIA국장에게 위임하던 정보시스템 보안과 관련된 권한을 국가정보국장(DNI)에게 위임하도록 변경(44 U.S.C. §3553(e)(1)).
- o OMB의 역할 및 임무 부여
  - 정보보안사고가 발생하였을 때 사고의 중대성 여부를 판단하기 위한 가이드라인을 수립(44 U.S.C. §3558(b)(1))
  - 지속적 진단 기술과 기타 발전적인 보안 기술들이 각 기관에 제대로 적용되는지에 대한 평가를 의회제출 보고서에 포함(44 U.S.C. §3558(c)) * 연례 FISMA 보고서에 포함
  - 의회와 개인피해자에 대한 데이터 유출 통지 정책을 연방기관에 요구할 수 있음(44 U.S.C. §3558(d)(1)).
- o 기타 기관에 관한 변경내용은 다음과 같다.
  - 법무부장관, 정보공유커뮤니티 리더, DHS장관이 수사, 국가안보, 복구 등의 사유로 개인에 대한 사고 통지를 연기할 수 있게 하는 조항 신설(44 U.S.C. §3558(d)(2))
  - 연방정보자원관리지침(OMB Circular A-130)을 개정하여 불필요한 보고체계를 제거(44 U.S.C. §3558(f)(1))
  - 정보보안・프라이버시 자문위원회(Information Security and Privacy Advisory Board, ISPAB)는 국토안보부에 대한 자문을 수행하고 연간 보고서를 국토안보부에 제출하여야 한다(44 U.S.C. §3558(f)(2)).

미국 정부는 FISMA 2002를 시작으로 15년 넘게 지속적으로 사이버보안 체계를 발전시켜 왔다. 초기 연방기관의 비협조, 대중의 무관심, 예산부족 등으로 인해 많은 어려움에 봉착했으나 관련 기관들과의 소통 및 협조 등을 통해 세계에서 가장 체계적인 사이버보안 체계를 구축할 수 있었다.

5.5. 연방정보기술습득개혁법(FITARA 2014)[28]

국방수권법(Public Law 113-291, “National Defense Authorization Act for Fiscal Year 2015,” December 19, 2014)의 Title VIII, 이 법의 부제 D에는 H.R. 1232, 연방 정보 기술 습득 개혁법(Federal Information Technology Acquisition Reform Act, FITARA)의 일부가 포함되어 있다.

이 법은 사이버보안에 영향을 미칠 수 있는 연방정보기술관행, 특히 "연방 데이터 센터의 통합"에 몇 가지 변화를 요구했다.

5.6. 사이버보안법(Cybersecurity Act of 2015)[29]

사이버보안법은 회계연도통합세출법(Public Law 114-113, “Consolidated Appropriations Act of 2016”, December 18, 2015)의 DIVISION N에서 규정하고 있는 법으로 [표 4]에서 보듯이 4개의 하위 별도 법을 포함하고 있다.

2015년도에는 미국 인사관리처(OPM) 전산시스템 해킹사고(‘15년), 국세청 웹사이트 해킹사고(’15년), 보험회사 랜섬웨어 해킹사고(‘15년) 등 공공・민간 영역을 불문하고 미국을 대상으로 지속적인 사이버보안 침해사고가 발생하였다. 이에 따라 국가 전반의 사이버보

안 수준 강화를 위한 사이버보안 정보공유 실효성 강화, 민·관 정보공유 확대 요구가 증가하였다. 이에 '15년에 총 5개의 사이버보안 정보공유 법률안이 발의되어 이 중 사이버보안 정보공유법 (CISA, S.654), 사이버네트워크보호법 (PCNA, H.R.1560), 국가사이버보안보호증진법(NCPAA, H.R.1731)의 3개 법안이 상·하원에서 각각 통과되었으며, 마침내 12월 상원에서 통과된 사이버보안정보공유법(CISA)을 중심으로, 하원 통과 법안을 통합·조정한 수정(안)을 최종 반영한 2015년 사이버보안법(Cybersecurity Act of 2015)이 제정되었다.

〔표 4〕 US Federal Acts for Cybersecurity

Public Law 114-113, "Consolidated Appropriations Act of 2016"
DIVISION N— CYBERSECURITY ACT OF 2015
TITLE I—CYBERSECURITY INFORMATION SHARING ① **Cybersecurity Information Sharing Act of 2015**
TITLE II—NATIONAL CYBERSECURITY ADVANCEMENT
Subtitle A—National Cybersecurity and Communications Integration Center ② **National Cybersecurity Protection Advancement Act of 2015**
Subtitle B—Federal Cybersecurity Enhancement ③ **Federal Cybersecurity Enhancement Act of 2015"**
TITLE III—FEDERAL CYBERSECURITY WORKFORCE ASSESSMENT ④ **Federal Cybersecurity Workforce Assessment Act of 2015"**

사이버보안정보공유법(Cybersecurity Information Sharing Act, CISA)은 공공(public) 및 민간부문(private-sector) 조직 간의 사이버보안 위협 정보를 공유할 것을 권장했다. 국가정보국장(Director of National Intelligence, DNI), 국토안보부장관, 국방부장관 및 법무부장관은 연방기관과 비연방기관(민간기관, 주·지방정부 등 포함) 간 사이버위협 정보 공유를 의무화 하였다. 민간기관이 사이버보안 목적으로 정보시스템 및 정보를 모니터링, 방어조치를 취하고, 정보를 공유할 수 있는 법적 근거를 마련하였다. 민·관 사이버보안 정보공유체계 구축에 대한 내용은 다음과 같다.

- o 국가정보국장, 국토안보부장관, 국방부장관 및 법무부장관은 연방기관과 비연방기관(민간기관, 주·지방정부 등 포함) 간 사이버위협지표 및 방어조치에 관한 정보 공유 절차 구축 및 가이드라인을 마련 (§103)
- o 민간기관이 사이버보안 목적으로 정보시스템 및 정보를 ① 모니터링 및 ②방어조치를 취하고, ③ 정보를 공유할 수 있는 법적 근거를 마련(§104)
- o 국토안보부장관 및 법무부 장관은 연방정부 내에서의 정보공유체계를 구축하고,* 대통령은 민간기관과의 정보공유 역량·절차를 개발·실시하는 연방기관(국방부 제외)을 지정 가능 (§105)
  - * 국토안보부와 법무부는 공유받은 정보를 특정 연방기관(상무부, 국방부, 에너지부, 국토안보부, 법무부, 재무부 및 국가정보국)과 자동화된 방식으로 실시간 공유할 수 있도록 정책·절차 수립·공표
- o 민간 기관이 이 법에 따라 사이버위협지표와 방어조치를 모니터링, 공유·제공받는 행위는 소송의 원인(cause of action)이 되지 못하도록 규정하고, 반독점법에 따른 책임 면제 등 보호규정 마련 (§106)
- o 연방기관은 '사이버보안 목적'을 위해 사이버보안 위협이나 취약점을 확인하는 용도로만 공유 받은 사이버보안 정보를 사용하도록 제한
  - * 생명 또는 신체·재산상의 중대한 위해가 되는 위협 등 특정 범죄 관련한 법 집행 목적 등 일부 예외 인정

국가사이버보안보호강화법(National Cybersecurity Protection Advancement Act of 2015)은 국토안보부 NCCIC 기능을 강화하고 연방정부의 사이버보안을 강화하기 위한 조치를 규정하고 있다. NCCIC에 사이버보안 위협지표(cyber threat indicators), 방어수단(defensive measures), 사이버보안 위험(cybersecurity risks) 및 사고(incidents) 관련 정보를 공유하도록 기능을 부여하였다. 국토안보부 NCCIC 기능 강화 및 연방정부 사이버보안 강화조치로 다음과 같다.

- o 국토안보부의 '국가사이버보안정보통합센터(NCCIC)'에 사이버보안위협지표 및 방어조치 정보, 사이버보안 위험과 사고 관련 정보 공유 기능을 부여
- o 연방기관에 정보시스템 침입 식별·제거를 위한 사이버보안 계획을 수립·실행하도록 하고, 국토안보부장관은 연방네트워크 보안 강화를 위한 고성능 네트워크 보안 도구 활용 계획을 수립·실행

연방사이버보안강화법(Federal Cybersecurity Enhancement Act of 2015)에서 연방기관은 정보시스템 침입을 식별하고 제거하는 사이버보안 계획을 수립과 구현하도록 의무화하였으며, 국토안보부장관은 연방네트워크 보안 강화를 위한 고급 네트워크 보안도구(advanced network security tools) 활용 계획을 수립하고 실행할 것을 규정하고 있다.

연방사이버보안인력평가법(Federal Cybersecurity Workforce Assessment Act of 2015)에서 연방정부의 사이버보안 인력에 대한 수요를 평가하고 관리를 강화하는 법률을 규정하고 있다.

사이버보안법 2015 Title Ⅳ에서는 국토안보부는

NIST와 협력하여 모바일 장치 보안에 대한 연구를 강화할 것을 규정하였으며 90일 이내 국무부 장관은 사이버공간에 대한 미국의 국제적인 정책에 대한 포괄적인 전략을 수립할 것을 규정하였다. 국무부는 2016년 3월에 “"Department of State International Cyberspace Policy Strategy", March 2016” 보고서를 작성하여 제출하였다[30]. 국제 사이버 범죄자에 대한 정의와 각 부처의 조치사항을 규정하고 있으며 긴급서비스 및 의료산업 분야의 사이버보안을 개선할 것과 연방 컴퓨터 보안을 강화할 것을 규정하고 있다

5.7. 사이버보안 및 기반구조보안기관법(CISA 2018)[31]

CISA 2018 법은 국토안보법(2002)를 개정하여 연방기관의 사이버보안을 담당하는 국가보안프로그램국(NPPD, National Protection and Programs Directorate)을 독립적인 CISA로 확대 개편하는 것을 골자로 하고 있다.

CISA는 다음과 같이 3개의 부서로 구성된다.

- o Cybersecurity Division
- o Infrastructure Security Division
- o Emergency Communications Division

CISA는 국가차원에서 직면하고 있는 글로벌 사이버 위협에 효과적으로 대응하기 위해 정부 및 민간분야 전반의 협력을 해야한다는 인식을 통해 각종 대응 노력을 전개하는 것을 임무로 부여 받았다.

특이점은 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 계획에 대한 정보를 의회에 보고할 것을 명시하고 있다[32].

5.8. NIST 소기업사이버보안법(2018)[33]

미국은 국가 사이버보안 역량 강화를 위해서는 소기업의 사이버보안 대응 능력을 높이는 것이 중요하다는 것을 인식하고 있다. 이 법에서 NIST는 1년 내에 소기업의 사이버 보안 강화를 위한 가이드라인을 만들어 배포할 것을 규정하고 있다.

Ⅵ. 결 론

국가차원의 사이버보안 분야를 크게 정책, 기술, 인력의 세 가지 분야로 구분해 볼 수 있다. 미국은 IT 기술의 핵심 기업을 보유하고 있는 국가인 만큼 IT 관련 정책을 국가의 가장 중요한 발전의 요소로 다루면서 이에 대한 정책적인 적극 지원을 해왔다. IT 기술은 중요하고 많은 정보를 다루며 인터넷과 결합하여 국가의 기간시설로 성장해 왔으며, 이제는 경제, 안보, 문화 등과 아주 강한 결합을 하고 있다. 이에 대한 역기능이 정보절취, 도청, 해킹 등이 발생한 것은 필연적인 것으로, 특히 미국 대상의 사이버공격이 급증하고 있는 상황은 그만큼 해커들에게 있어 매력적이며 이익이 많이 발생하는 타겟이 되는 셈이다. 미국 연방정부는 이에 대한 대책을 정책적으로 차분하게 추진해 왔으며, 특히 법률(연방법 중심) 제정 현황을 살펴보면 미국의 의지와 정책 방향 등을 알 수 있는 단초를 찾을 수 있다.

1980년대 PC의 등장을 통해 컴퓨터 정보의 절취, 도난, 사기 등에 대한 범죄 대응이 초기에는 관심사였으며, 1990년대 들어서 인터넷의 발전으로 정보보안의 중요성이 대두되었다. 이 시기는 사이버보안(Cybersecurity)이라는 용어가 등장하기 이전 시대로 인터넷을 통한 민감 정보 등의 범죄활용을 대응하기 위한 법률이 중심이 되었다.

사이버보안에 대한 중요성 및 심각성은 2000년대 들어서 국토안보법, 사이버보안강화법, 사이버보안연구개발법 등이 제정되어 국가차원의 사이버보안 대응이 시작되었음을 알 수 있다. 특히 FISMA 2002는 연방기관 중심으로 사이버보안 대책을 실효성 있게 실천할 수 있는 계기가 되었으며, NIST가 사이버보안 표준, 기술, 지원 등에 있어서 중심역할을 담당하게 되었다. 2000년대는 FISMA를 기반으로 연방기관 대상의 사이버보안 대응능력 강화를 위해 규정된 절차를 적용하여 많은 시행착오를 겪었다고 할 수 있다.

2010년대 들어와서는 이전의 많은 경험과 오류를 확인하고 보완할 기회를 맞이했으며 이에 대한 준비를 한 것으로 보인다. 관련된 법은 사이버보안인력평가법, 사이버보안강화법, 국가사이버보안보호법, 연방 정보보안 현대화법이 2014년도에 제정되어 보다 세련되고 세밀한 정책을 추진할 수 있는 기반이 마련되었다. 특히 사이버보안법(Cybersecurity Act of 2015)은 가장 체계적

인 법으로 제정되어 미국의 사이버보안 정책 추진에 있어 그 기반을 지원하고 있다. 또한 CISA 2018을 통해 사이버보안과 기반구조보안에 대한 관리 주체를 일원화하여 그 효율성을 높이려 하였으며, 영세한 소기업에 대해 국가 기관인 NIST로 하여금 지원하도록 규정하였다.

이와 같이 30년 넘게 제정되어 온 미국의 사이버보안 분야 법률체계를 살펴보면서 구체적인 실행력을 우선하는 미국이라는 나라의 문화를 알 수 있었다. 연방법이 갖는 코드체계에 연관되어 법률간의 일관성이 지속적으로 유지되고 있으며, 법률의 조문들이 우리나라 법률의 모호성에 비교하면 구체적인 특성이 있어서 논쟁의 여지가 거의 발생하지 않음을 알 수 있었다. 사이버보안 분야는 IT 기술 의존도가 높으므로 변화의 속도가 매우 빠르므로 법률체계의 신속성과 정확성이 더욱 요구된다고 할 수 있다.

참 고 문 헌

[1] 이연수, 이수연, 윤석구, 전재성, 주요국의 사이버안전 관련 법 조직체계 비교 및 발전방안 연구. 국가정보연구 제1권 2호, pp. 35-116, 2009.

[2] 한국인터넷진흥원, 사이버보안체계 강화를 위한 정보보호법제 비교법 연구, KISA-WP-2015 -0042, pp. 18-19, 2015.12.

[3] 양정윤・박상돈・김소정, "미국의 법제도 정비와 사이버안보 강화: 국가사이버안보보호법 등 제・개정된 5개 법률을 중심으로", pp. 305-335, 2015. 12.

[4] 육소영, "사이버보안법의 제정 필요성에 관한 연구", 공법학연구, 제11권 2호, pp. 313-335, 2010.5.

[5] Soonjwa Hong, "A Study on the Framework of Comparing New Cybersecurity Workforce Development Policy Based on the ATE Programs of U.S.", Journal of KIISC VOL.28, NO.1, Feb. 2017.

[6] Commission on Enhancing National Cybersecurity, Report on Securing and Growing the Digital Economy, Dec. 1, 2016.

[7] PUBLIC LAW 98- 362, “Small Business Computer Security and Education Act of 1984", July 16, 1984.

[8] Public Law 99-474, “Computer Fraud and Abuse Act of 1986,” Oct. 16, 1986.

[9] Public Law 99-574, “National Bureau of Standards Authorization Act for Fiscal Year 1987", Oct. 28, 1986.

[10] Public Law 100-235, “Computer Security Act of 1987,” Jan. 8, 1988.

[11] Public Law 104-13, “Paperwork Reduction Act of 1995,” May 25, 1995.

[12] Public Law 104-106, “Clinger-Cohen Act of 1996,” Feb. 10, 1996.

[13] Public Law 104-294, “National Information Infrastructure Protection Act,” Oct. 11, 1996.

[14] Public Law 106-102, “Gramm-Leach- Bliley Act of 1999,” Nov. 12, 1999.

[15] PUBLIC LAW 106‐65, “National Defense Authorization Act for Fiscal Year 2000”, Oct. 5, 1999.

[16] PUBLIC LAW 106‐398, "National Defense Authorization Act for Fiscal Year 2001, Subtitle G−Government Information Security Reform“, OCT. 30, 2000

[17] Public Law 107-204, “Sarbanes-Oxley Act of 2002,” July 30, 2002.

[18] Public Law 107-296, “Homeland Security Act of 2002,” Nov. 25, 2002.

[19] Public Law 107-305, “Cyber Security Research and Development Act,” Nov. 27, 2002.

[20] PUBLIC LAW 107- 347, “E-Government Act of 2002 Tile III. Information Security Federal Information Security Management Act of 2002“, Dec. 17,2002.

[21] Public Law 109-295, “Department of Homeland Security Appropriations Act, 2007“, Oct. 4, 2006.

[22] Public Law 110-140, “Energy Independence and Security Act of 2007,” Dec. 19, 2007.

[23] Public Law 111-5, “Health Information Technology for Economic and Clinical Health Act,” Feb. 17, 2009.

[24] Public Law 113-246, “Cybersecurity Workforce Assessment Act,” Dec. 18, 2014.

[25] Public Law 113-274, “Cybersecurity Enhancement Act of 2014,” Dec. 18, 2014.
[26] Public Law 113-282, “National Cybersecurity Protection Act of 2014,” Dec. 18, 2014.
[27] PUBLIC LAW 113-283, “Federal Information Security Modernization Act of 2014“, Dec. 18, 2014.
[28] Public Law 113-291, “National Defense Authorization Act for Fiscal Year 2015,” Dec. 19, 2014.
[29] Public Law 114-113, “Cybersecurity Act of 2015,” Dec. 18, 2015.
[30] Department of State, "International Cyberspace Policy Strategy", March 2016.
[31] PUBLIC LAW 115-278, “Cybersecurity and Infrastructure Security Agency Act of 2018”, Nov.16,2018.
[32] American Technical Council, Report to the President on Federal IT Modernization, Dec.13, 2017.
[33] PUBLIC LAW 115-278, “NIST Small Business Cybersecurity Act of 2018”, Nov.16,2018.

〈저자소개〉

홍 순 좌 (Soonjwa Hong)

정회원

1989년 2월 : 숭실대학교 전산과 학사
1991년 2월 : 숭실대학교 전산과 석사
2005년 8월 : 충남대학교 컴퓨터과학과 박사
1991년 2월~2000년 1월 : 국방과학연구소(ADD) 선임연구원
2000년 2월~현재 : ETRI부설연구소 책임연구원
<관심분야> 국내외 사이버보안 인력 양성 법・정책, 미래 IT·보안기술, 사이버보안 기술・위협 분석, 국내외 정보보안 법・정책