미국 사이버보안법의 최근 동향*

- 「사이버보안 정보공유법」을 중심으로 하여 -

양 천 수**·지 유 미***

차 례

* 이 글은 필자들이 참여한 연구보고서 『안전한 지능정보사회 구축을 위한 정보보호 관련 법제도 개선방안 연구』, 과학기술정보통신부, 2018에서 필자들이 집필한 부분을 일부 바탕으로 하여 이를 대폭 수정 및 보완한 것입니다.

** 영남대학교 법학전문대학원 교수·법학박사·주저자
*** 대구대학교 DU인재법학부 조교수·법학박사·교신저자

접수일자 : 2018 4. 30. / 심사일자 : 2018. 5. 24. / 게재확정일자 : 2018. 5. 29.

Ⅰ. 서 론

이른바 ‘제4차 산업혁명’이 진행되면서 사회구조가 급격하게 변하고 있다. 과거에는 경험하지 못했던 새로운 사회 패러다임이 등장하고 있다. ‘초연결사회’와 ‘빅데이터사회’ 그리고 ‘지능정보사회’가 대표적인 예에 해당한다.[1] 특히 사물인터넷(IoT)을 통해 사회의 모든 것이 인터넷망으로 연결되는 초연결사회가 구현되면서, 예전에는 누리지 못했던 사회적 공리가 증대하고 있다. 이에 따라 사물인터넷 기술은 제4차 산업혁명을 선도하는 성장동력으로 각광받고 있다. 그러나 이렇게 현대사회가 초연결사회로 나아가면서, 새로운 위험 역시 늘어나고 있다. 무엇보다도 은밀한 개인정보를 포괄하는 정보침해의 위험이 비약적으로 증대하고 있다. 초연결사회가 실현되면서, 사물인터넷 기기 한 개만 해킹되어도 그 파급효과가 초연결망 전체로 확산되는 위험이 등장하고 있는 것이다. 이에 따라 사이버보안을 포괄하는 정보보호의 필요성과 중요성이 증대하고 있다. 사이버 공간, 인터넷 공간의 안정성이 부각되고 있는 것이다. 이에 정부는 과학기술정보통신부를 주축으로 하여 초연결사회의 정보침해 문제에 대응할 수 있는 정보보호 관련 법체계 구축을 모색하고 있다. 「정보통신망법」, 「정보통신기반 보호법」, 「정보보호산업법」을 핵심축으로 하는 정보보호 관련 법체계를 제4차 산업혁명 시대에 걸맞게 업그레이드 하고자 모색하고 있는 것이다. 그러나 그 방향성을 어떻게 설정해야 할지에 관해서는 여전히 고민을 하고 있는 것으로 보인다. 이러한 상황에서 해외 선진국의 법적 상황을 살펴보는 비교법적 검토는 우리가 정보보호 관련 법정책을 어떻게 펼쳐야 하는지에 관해 의미 있는 시사점을 제공할 것이다. 특히 사이버보안을 침해하는 행위에 대해 적극적인 대응입법을 하고 있는 미국의 법제는 우리가 참고할 만한 가치를 지니고 있다. 이러한 이유에서 이 글에서는 미국의 사이버보안법의 최근 현황, 그 중에서도 「사이버보안 정보공유법」을 분석함으로써 우리 정보보호 관련 법제도가 나아가야 할 방향에 의미 있는 몇 가지 시사점을 얻고자 한다.[2]

---

1) 이에 관해서는 양천수, 제4차 산업혁명과 법, 박영사, 2017, 4쪽 아래 참고.

Ⅱ. 우리 정보보호 관련 법제도 개관

미국의 사이버보안법을 분석하기 전에 우리 정보보호 관련 법제도가 어떻게 체계화되어 있는지 간략하게 개관해 보도록 한다.[3] 이는 비교법 연구의 출발점이 된다. 현재 정보보호와 관련을 맺는 중요한 법률로는 「국가정보화 기본법」, 「전자정부법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'으로 약칭함), 「정보통신기반 보호법」, 「정보보호산업의 진흥에 관한 법률」(이하 '정보보호산업법'으로 약칭함)을 들 수 있다.

1. 국가정보화 기본법

정보보호의 가장 기초가 되는 법으로서 「국가정보화 기본법」을 들 수 있다. 이는 개념 그대로 국가정보화의 기초를 이루는 법이다. 구체적으로 보면, 「국가정보화 기본법」은 "국가정보화의 기본 방향과 관련 정책의 수립·추진에 필요한 사항을 규정함으로써 지속가능한 지식정보사회의 실현에 이바지하고 국민의 삶의 질을 높이는 것을 목적"으로 하는 법이다(제1조). 여기서 알 수 있듯이, 「국가정보화 기본법」은 '지식정보사회'를 구축하는 데 필요한 법적 근거를 마련하는 것을 목적으로 한다. 이 점에서 「국가정보화 기본법」은 정보보호만을 목적으로 하지는 않는다. 그렇지만 「국가정보화 기본법」은 정보보호에 관한 법적 기초를 제공한다. 예를 들

2) 미국의 사이버보안법에 관한 기존연구로는 육소영, "사이버보안법의 제정 필요성에 관한 연구: 미국법과의 비교를 중심으로", 『공법학연구』 제11권 제2호, 한국비교공법학회, 2010; 박상돈·김인중, "한국과 미국의 사이버보안 단계별 법제도 비교 연구", 『융합보안 논문집』 제12권 제4호, 한국융합보안학회, 2012; 이상현, "미국의 사이버보안 법제: 입법부, 사법부, 행정부의 대응을 중심으로", 『Internet & information security』 제3권 제1호, 한국인터넷진흥원, 2012; 박노형, "미국의 사이버안전에 관한 법 제정 동향과 시사점", 『법제연구』 제46호, 한국법제연구원, 2014; 한국인터넷진흥원 (편), 사이버보안체계 강화를 위한 정보보호법제 비교법연구, 한국인터넷진흥원, 2015 등 참고.

3) 현행 법체계는 '정보보호'를 미국의 사이버보안에 상응하는 개념으로 설정한다. 다만 정보보호라는 개념이 적정한지에 관해서는 논란이 없지 않다. 이에 관해서는 정필운, "사이버보안이란 개념 사용의 유용성 및 한계", 『연세 의료·과학기술과 법』 제2권 제2호, 연세대 법학연구원, 2011, 1쪽 아래 참고.

어, 「국가정보화 기본법」은 정보보호에 관한 기본적 개념인 '정보', '정보통신', '정보보호', '정보통신윤리', '정보통신기반', '정보통신서비스', '정보통신서비스 제공자', '이용자' 등을 규정한다(제3조). 특히 정보보호 개념을 정면에서 규정하고 있다는 점이 주목할 만하다. 또한 「국가정보화 기본법」은 국가정보화가 초래하는 역기능을 방지하기 위해 정보이용의 안정성 및 신뢰성을 보장할 수 있는 방안을 국가 및 지방단치단체가 마련할 것을 규정한다. 이를테면 정보보호 시책 및 개인정보보호 시책을 수립할 것을 규정하고, 정보보호시스템에 관한 고시를 마련할 것을 규정한다(제37조-제39조). 이러한 점에서 보면, 「국가정보화 기본법」은 정보보호에 관한 법적 기초를 제공하는 법, 달리 말해 정보보호의 출발점에 해당하는 법이라고 말할 수 있다.

2. 전자정부법

「전자정부법」은 "행정업무의 전자적 처리를 위한 기본원칙, 절차 및 추진방법 등을 규정함으로써 전자정부를 효율적으로 구현하고, 행정의 생산성, 투명성 및 민주성을 높여 국민의 삶의 질을 향상시키는 것을 목적"으로 하는 법이다(제1조). 여기서 알 수 있듯이, 「전자정부법」은 전자정부 구현을 목적 및 대상으로 하는 법, 달리 말해 공공영역을 대상으로 하는 법이다. 「전자정부법」은 기본적으로 전자정부 구축 및 실현을 목적으로 하는 법이기에 정보보호와 직접적인 관련을 맺는 것처럼 보이지는 않는다. 「전자정부법」의 내용을 보면, 오히려 행정정보의 공동이용에 더욱 초점을 맞추고 있는 것으로 보인다(제4장). 그렇지만 「전자정부법」 역시 정보보호에 관한 규정을 담고 있다. 예를 들어, 「전자정부법」 제56조는 "정보통신망 등의 보안대책 수립·시행"이라는 표제 아래 다음과 같이 규정한다.[4]

4) 강조는 인용자가 추가한 것이다.

① 국회, 법원, 헌법재판소, 중앙선거관리위원회 및 행정부는 전자정부의 구현에 필요한 정보통신망과 행정정보 등의 안전성 및 신뢰성 확보를 위한 **보안대책**을 마련하여야 한다.
② 행정기관의 장은 제1항의 보안대책에 따라 소관 정보통신망 및 행정정보 등의 **보안대책**을 수립·시행하여야 한다.
③ 행정기관의 장은 정보통신망을 이용하여 전자문서를 보관·유통할 때 위조·변조·훼손 또는 유출을 방지하기 위하여 국가정보원장이 안전성을 확인한 **보안조치**를 하여야 하고, 국가정보원장은 그 이행 여부를 확인할 수 있다.
④ 제3항을 적용할 때에는 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관의 경우에는 해당 기관의 장이 필요하다고 인정하는 경우에만 적용한다. 다만, 필요하지 아니하다고 인정하는 경우에는 해당 기관의 장은 제3항에 준하는 **보안조치**를 마련하여야 한다.

이렇게 보면, 「전자정부법」 역시 부분적으로 정보보호와 관련을 맺는 법이라고 할 수 있다. 요컨대, 「전자정부법」은 공공영역, 특히 정부에서 행정정보를 보호하는 역할을 수행한다고 말할 수 있다.

3. 정보통신망법

정보통신망법은 "정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로" 하는 법이다(제1조).[5] 여기서 알 수 있듯이, 정보통신망법은 정보통신망을 이용하는 이용자의 개인정보를 보호하는 것을 주된 목적으로 한다. 또한 정보통신망의 안전한 이용 역시 보장하고자 한다. 이를 위해 정보통신망법은 정보통신서비스 제공자를 규율하는 다양한 규제장치를 마련하고 있다. 이처럼 정보통신망법은 정보통신서비스 제공자와 이용자를 주된 규율 및 보호대상으로 한다는 점에서 민간영역을

5) 정보통신망법에 관해서는 양천수, "정보통신망법 해석에 관한 몇 가지 쟁점", 『과학기술과 법』 제8권 제1호, 충북대 법학연구소, 2017, 1-33쪽 참고.

관할대상으로 삼는다. 이러한 근거에서 정보통신망법은 민간영역에서 정보보호 및 개인정보보호를 실현하고자 하는 법이라고 말할 수 있다.

4. 정보통신기반 보호법

「정보통신기반 보호법」은 "전자적 침해에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적"으로 하는 법이다(제1조).[6] 이를 통해 알 수 있듯이, 「정보통신기반 보호법」은 '전자적 침해'에 대비하여 주요정보통신기반시설의 안정성을 보호하고자 한다. 이때 정보통신망 역시 주요정보통신기반시설에 포함되므로, 「정보통신기반 보호법」이야말로 정보보호에 관해 가장 포괄적이면서 기본적인 내용을 담고 있는 법이라고 할 수 있다. 더군다나 주요정보통신기반시설은 공공영역뿐만 아니라 민간영역에서 관리하는 경우도 있으므로, 「정보통신기반 보호법」은 공공영역과 민간영역을 모두 관할하는 정보보호법이라고 말할 수 있다.

5. 정보보호산업법

「정보보호산업법」은 "정보보호산업의 진흥에 필요한 사항을 정함으로써 정보보호산업의 기반을 조성하고 그 경쟁력을 강화하여 안전한 정보통신 이용환경 조성과 국민경제의 건전한 발전에 이바지함을 목적"으로 하는 법이다(제1조).[7] 여기서 알 수 있듯이, 정보보호산업법은 기본적으로 정보보호산업을 대상으로 한다는 점에서 민간영역을 관할하는 법이라고 할 수 있다. 다만 「정보보호산업법」은 정보통신망법이나 정보통신기반보호법과는 차이가 있는데, 정보통신망법이나 「정보통신기반 보호법」이 전자적 침해로부터 정보보호를 실현하고자 하는 소극적·방어적인 법이라면,

6) 「정보통신기반 보호법」에 관해서는 홍종현, "정보통신기반보호법제의 개선방안 연구", 『법연』 제46호, 한국법제연구원, 2015 참고.

7) 「정보보호산업법」에 관해서는 박주석·문승일·송기민, "정보보호산업법상 정보보호산업 분쟁조정의 개선과제", 『보안공학연구논문지』 제14권 제4호, 보안공학연구지원센터, 2017 참고.

「정보보호산업법」은 정보보호산업을 진흥시킴으로써 정보보호를 실현하고자 하는 적극적인 법이라는 점이다. 물론 정보보호산업 육성이 목표로 하는 것은 궁극적으로는 완벽한 정보보호의 실현이라고 할 수 있다. 그 점에서 「정보보호산업법」 역시 정보보호 관련 법제도에 포함시킬 수 있다.

6. 중간결론

이상의 논의를 고려하면 현행 정보보호 관련 법제도는 다음과 같이 체계화할 수 있다. 정보보호 영역은 크게 공공영역과 민간영역으로 구분할 수 있다. 공공영역의 정보보호는 기본적으로 「전자정부법」이 관할한다. 이에 대해 민간영역은 정보통신망법이 관할한다. 「정보보호산업법」도 민간영역을 관할하는 정보보호법이라 할 수 있다. 한편 「정보통신기반 보호법」은 공공영역과 민간영역을 모두 포괄하는 정보보호법에 해당한다. 그리고 「국가정보화 기본법」은 정보보호에 관한 법적 출발점이자 토대를 이룬다.

Ⅲ. 미국의 사이버보안 관련 법체계 현황

그러면 미국은 우리의 정보보호에 상응하는 사이버보안에 관해 어떤 법체계를 갖추고 있는가? 아래에서는 지난 2014년 및 2015년에 제정된 미국의 사이버보안 관련 법제도를 중심으로 하여 논의를 전개하도록 한다. 미국의 사이버보안법은 지난 2014년에 중요한 계기를 맞는다. 2014년 12월 오바마(Barack Obama) 미국 전 대통령은 사이버보안에 관한 다섯 개의 법률에 서명을 한다. 「연방 정보보안 현대화법」(Federal Information Security Modernization Act of 2014),[8] 「국가 사이버보안 보호법」(National Cybersecurity Protection Act of 2014),[9] 「사이버보안 강화법」(Cybersecurity Enhancement Act of 2014),[10] 「국토안보부 사이버보안 인력채용 및 유지법」

8) Pub. L. No. 113-283, 128 Stat. 3073.
9) Pub. L. No. 113-282, 128 Stat. 3066.
10) Pub. L. No. 113-274, 128 Stat. 2971.

(DHS Cybersecurity Workforce Recruitment and Retention Act),[11] 「사이버보안 인력평가법」(Cybersecurity Workforce Assessment Act)이 그것이다.[12]

이러한 사이버보안 관련 입법은 부시(George W. Bush) 전 대통령이 서명한 「전자정부법」(E-Government Act of 2002)이 제정된 이후 처음이었다. 물론 「전자정부법」의 제정과 위의 다섯 가지 법률의 제정 사이에 사이버보안을 위한 입법시도가 전혀 없었던 것은 아니다. 특히 제112대 의회(2011~2012)부터 제113대 의회(2013~2014)에 이르기까지 사이버보안을 강화하고자 하는 입법시도가 광범위하게 이루어졌다. 그렇지만 2014년 12월에 위에서 언급한 다섯 가지 법률이 제정되기 이전까지는 이와 같은 입법시도들은 실패를 거듭하였다.

2014년 12월에 제정된 법률 중 특히 「연방 정보보안 현대화법」과 「국가 사이버보안 보호법」은 크게 두 가지에 초점을 맞추고 있다. 첫째는 사이버보안을 위한 연방정부의 활동을 중앙집권화하는 것이다. 둘째는 정부와 민간영역 사이의 정보공유를 강화하는 것이다. 이에 대해 「국토안보부 사이버보안 인력채용 및 유지법」과 「사이버보안 인력평가법」은 사이버보안에 관한 연방정부의 인력을 강화하는 데 그 주된 목적이 있다. 아래에서는 이러한 다섯 가지 법률을 살펴보도록 한다.

1. 연방 정보보안 현대화법

「연방 정보보안 현대화법」(Federal Information Security Modernization Act of 2014)은 사이버보안 관리에 관한 연방정부의 권한을 '국토안보부'(Department of Homeland Security: DHS)에 집중시키는 방향으로 「연방 정보보안관리법」(Federal Information Security Management Act of 2002)을 개정한 것이다.[13] 「연방 정보보안 현대화법」은 주로 다음과 같은 다섯 가지 목적을 지향한다. 첫째, 연방정부의 운영 및 자산을 뒷받침해주는 정보자원에 대한 보안 통제의 효과를 확실히 하는 기본 틀(framework)을 제

11) Pub. L. No. 113-277, 128 Stat. 2995.

12) Pub. L. No. 113-246, 128 Stat. 2880.

13) Lawrence J. Trautman, *CYBERSECURITY: WHAT ABOUT U.S. POLICY?*, 2015 U. Ill. J.L. Tech. & Pol'y 341, 371 (2015).

공한다. 둘째, 고도로 네트워크화 되어 있는 현행 연방의 컴퓨팅 환경을 인식하고, 전 정부적 차원에서 관련 정보의 보안 위험에 대한 효과적인 관리 및 감독을 제공한다. 셋째, 연방의 정보 및 정보시스템을 보호하기 위해 요구되는 최소한의 통제장치를 개발·유지하는 것을 가능하게 한다. 넷째, 연방기관의 정보 보안프로그램에 대한 향상된 감독 기제를 제공한다. 다섯째, 상업적으로 개발된 정보보안제품들이 주요 정보기반시설을 보호하기 위한 시장의 해법을 반영함으로써 정보보안을 실현할 수 있는 선진적이고, 역학적이며, 견고하고, 효과적인 해결책을 제공한다는 점을 인정하는 것이다.[14]

구체적으로 살펴보면, 우선 「연방 정보보안 현대화법」은 '예산관리국장'(Director of the Office of Management and Budget)에게 연방기관의 정보보안 정책 및 실무를 감독할 책임을 부과한다. 여기에는 정보보안에 관한 정책, 원칙, 기준 및 가이드라인을 개발하고 그 실행을 감독할 책임, 연방기관으로 하여금 그 기관이 수집·보관하거나 그 기관을 위해 수집·보관되는 정보 등에 무단으로 접속하거나, 또는 그와 같은 정보 등을 무단으로 사용, 공개 또는 파괴함으로써 야기된 피해의 위험 및 정도에 상응하는 보호장치를 제공하도록 요구하는 책임 등이 포함된다.[15] 다만 방위정보의 보안과 기밀정보의 보안에 관한 권한은 예산관리국장이 아닌 '국방부 장관'(Secretary of Defense)과 '국가정보국 국장'(Director of National Intelligence)에게 각각 위임된다.[16]

이에 반해 연방기관이 정보시스템을 보호하기 위해 정보보안 정책 및 실무를 이행하도록 하는 책임은 '국토안보부 장관'(Secretary of Homeland Security)에게 부여된다. 「연방 정보보안 현대화법」에 따르면, 정보보안 정책 및 실무의 이행을 위해 국토안보부 장관이 부담하는 가장 대표적인 책임으로 "구속력 있는 운영상 지침"(binding operational directive)의 이행을 감독하는 책임을 들 수 있다.[17] 여기서 "구속력 있는 운영상의 지침"

14) 44 U.S.C. 3551.
15) 44 U.S.C. 3553(a).
16) 44 U.S.C. 3553(e).
17) 44 U.S.C. 3553(b).

이란 이미 알려져 있거나 또는 합리적으로 예측할 수 있는 정보보안에 대한 위협·취약성·위험으로부터 연방정보 및 정보시스템을 보호하기 위해 연방기관에게 내리는 강제적 지시를 뜻한다.[18]

2. 국가 사이버보안 보호법

「국가 사이버보안 보호법」(National Cybersecurity Protection Act of 2014)은 국토안보부에 이미 존재하고 있던 '국가 사이버보안 및 통신 통합센터'(National Cybersecurity and Communications Integration Center: NCCIC)를 성문화하는 것을 주된 내용으로 한다.[19] 「국가 사이버보안 보호법」에 따르면, '국가 사이버보안 및 통신 통합센터'는 다음과 같은 기능을 수행한다. 먼저 연방 및 비연방기관을 위해 사이버보안 위험·사고·분석·경고에 관한 정보를 다각적으로 공유하도록 하기 위한 연방과 민간 간의 접점(interface)으로서 역할을 수행한다. 나아가 연방 및 비연방기관에 대한 사이버보안 위험 및 사고를 처리하기 위해, 상황에 대한 인식(situational awareness)을 연방정부 및 비연방기관 전체에 제공함으로써 통합적인 실시간 대응을 가능하게 한다. 마지막으로 요청이 있는 경우, 사이버보안 위험 및 사고와 관련하여 연방 및 비연방기관에 기술적 조력, 위기관리 지원 및 사고대응 능력을 시기적절하게 제공하는 등의 기능을 수행한다.[20]

한편 '국가 사이버보안 및 통신 통합센터'는 이러한 기능을 수행하기 위해 다음과 같은 권한과 책무를 수행해야 한다. 첫째, 가능한 한 사이버보안 위험·사고·분석에 관해 시기적절하고, 실용적이며, 유의미한 정보가 공유될 수 있도록 함과 동시에 분야를 초월하여 지속적, 협력적 그리고 포괄적인 조정(coordination)을 이끌어내야 한다. 둘째, 사이버보안 위험 및 사고에 관한 정보를 무단접속으로부터 적절하게 보호해야 한다. 셋째, '국가 사이버보안 및 통신 통합센터'의 활동이 미국 시민의 프라이버시

18) 44 U.S.C. 3552(b)(1)(a).
19) 6 U.S.C. 148(b).
20) 6 U.S.C. 148(c).

및 개인적 자유를 보호하는 모든 정책, 규제 그리고 법률에 부합해야 한다는 등의 원칙을 준수해야만 한다.[21]

3. 사이버보안 강화법

「사이버보안강화법」(Cybersecurity Enhancement Act of 2014)은 크게 "사이버보안을 위한 민관의 협력"(Title I), "사이버보안을 위한 연구 및 개발"(Title II), "사이버보안에 대한 교육 및 사이버보안 인력의 개발"(Title III), "사이버보안에 대한 인식 및 준비"(Title IV), "사이버보안을 위한 기술적 기준의 향상"(Title V)에 관해 규정한다. 아래에서는 이 중에서도 "사이버보안을 위한 민관의 협력"과 "사이버보안에 대한 인식 및 준비"를 중심으로 하여 「사이버보안강화법」의 내용을 살펴보도록 한다.

「사이버보안강화법」은 우선 사이버보안에 관한 민관의 협력을 강화하기 위해 상무부 장관(Secretary of Commerce)이 '국립표준기술원장'(Director of the National Institute of Standards and Technology)을 통해 주요기반시설에 대한 사이버 위험을 비용효율성이 높은 방법으로 감소시키기 위한 "자발적이고, 업계에 의해 유도되며, 합의에 기초를 두고 있는" 일련의 기준·가이드라인·모범실무·방법·절차·과정의 개발을 촉진하고 지원할 수 있도록 하고 있다.[22] 이를 위해 「사이버보안강화법」은 국립표준기술원장에게 다음과 같은 책무를 부과한다. 첫째, 관련 있는 민간분야의 직원이나 기관, 주요기반시설의 소유자나 보유자 등과 정기적으로 밀접하게 협력해야 한다. 둘째, 국가안보의 책임을 지고 있는 기관의 수장 등과 상의해야 한다. 셋째, 주요기반시설의 소유자나 보유자가 사이버 위험을 식별·평가·관리하기 위해 자발적으로 채택할 수 있는 융통성 있고, 반복 가능하며, 성과에 기반을 두고 있을 뿐만 아니라 비용효율성도 갖추고 있는 (정보보안 수단 및 통제를 포함하는) 방법을 찾아내야 한다. 넷째, 위에서 언급한 일련의 기준 등이 업계의 모범실무를 포함하고 자발적인 국제적 사이버보안 기준들에 가능한 한 부합하는 것이 될 수 있도록

21) 6 U.S.C. 148(e).

22) 15 U.S.C. 272(c)(15).

해야 한다.[23]

다음으로 「사이버보안강화법」은 국립표준기술원장에게 적합한 연방기관, 교육기관 등과 협의하여 사이버보안에 대한 인식 및 교육에 관한 프로그램을 지속적으로 조직화하도록 요구한다.[24] 이를 통해 「사이버보안강화법」은 사이버보안에 대한 인식과 준비의 정도를 강화시키고자 한다. 이때 사이버보안에 대한 인식 및 교육 관련 프로그램에는 다음과 같은 행위가 포함된다. 첫째, 국립표준기술원장이 인정한 사이버보안을 위한 기술적 기준 및 모범실무를 광범위하게 보급하는 행위, 둘째, 사이버보안을 위한 모범실무를 개인, 중소기업, 교육기관, 주정부나 지방정부가 이용할 수 있도록 하는 행위, 셋째, 사이버보안, 사이버안전 그리고 사이버윤리 등에 대한 대중의 인식을 고양시키는 행위, 넷째, 민간영역이나 연방정부, 주정부 등을 위해 숙련된 사이버보안 및 컴퓨터공학 인력을 준비·향상시키기 위해 교육의 모든 단계에서 공식적인 사이버보안 교육 프로그램을 지원해 주는 행위 등이 그것이다.

4. 국토안보부 사이버보안 인력채용 및 유지법

「국토안보부 사이버보안 인력채용 및 유지법」(DHS Cybersecurity Workforce Recruitment and Retention Act)은 국토안보부 안에서 이루어지는 사이버보안 관련 인력의 채용절차를 개선하고 이들에 대한 보수를 향상시키는 데 그 목적이 있다. 즉, 동법은 한정되어 있는 사이버보안 전문가를 고용하는 데 국토안보부가 '국가안전국'(National Security Agency)이나 '국방부'(Department of Defense)에 대해 경쟁우위를 점할 수 있도록 하려는 데 그 목적이 있는 셈이다.[25] 이를 위해 「국토안보부 사이버보안 인력채용 및 유지법」은 국토안보부 장관이 사이버보안에 관한 국토안보부의 역할을 다하는 데 필요한 경우 '비경쟁직'(excepted service)의 하나로 '조건부 직위'(qualified position)를 마련하여 개인을 이와 같은 직위에 임명하고, 그 직위에 대해 보수를 책정할 수 있도

23) 15 U.S.C. 272(e).

24) 15 U.S.C. 7451(a)

25) 이는 다시 말해, 사이버보안 전문가를 채용하는 데 국토안보부, 국가안전국, 국방부 사이에 치열한 경쟁이 이루어지고 있음을 보여준다.

록 허용한다.[26] 특히 이러한 조건부 직위에 대한 보수와 관련하여, 동법은 국토안보부 장관에게 국방부에서 유사한 사이버보안 업무를 수행하는 인력들에게 지급되는 보수에 상응하는 보수를 책정하도록 요구한다.[27]

5. 사이버보안 인력평가법

「사이버보안 인력평가법」(Cybersecurity Workforce Assessment Act)은 국토안보부로 하여금 사이버보안 인력에 대해 평가하고, 사이버보안 인력의 준비상태, 역량, 훈련, 채용 및 잔류를 강화할 종합적 전략을 개발하도록 요구한다. 좀 더 구체적으로 말하면, 국토안보부 장관은 「사이버보안 인력평가법」이 제정된 때로부터 180일 이내에 그리고 그 후 3년 동안 매년 국토안보부의 사이버보안 관련 인력을 평가해야 한다.[28] 이와 같은 평가에는 최소한 다음과 같은 내용이 포함되어야 한다. 첫째, 국토안보부의 사이버보안 임무를 충족시킬 국토안보부 내 인력의 준비상태 및 역량에 대한 평가, 둘째, 국토안보부 내에 사이버보안 관련 직위가 어디에 존재하는지에 대한 정보, 셋째, 어떤 사이버보안 관련 업무가 국토안보부의 정규직 직원, 독립 계약자, 다른 연방기관에 의해 고용된 개인에 의해 각각 행해지고 있는지와 어떤 사이버보안 관련 직위가 공석인지에 관한 정보 등이 그것이다.[29] 뿐만 아니라 「사이버보안 인력평가법」은 국토안보부 장관에게 동법이 제정된 때로부터 1년이 경과하기 이전에 국토안보부의 사이버보안 관련 인력의 준비상태, 역량, 훈련, 채용 그리고 잔류를 강화시킬 수 있는 포괄적인 전략을 개발하고, 이러한 전략을 유지하거나 또는 (필요한 경우에는) 갱신하도록 요구한다.[30]

---

26) 6 U.S.C. 147(b)(1).
27) 6 U.S.C. 147(b)(2).
28) 6 U.S.C. 146(a)(1).
29) 6 U.S.C. 146(a)(2).
30) 6 U.S.C. 146(b)(1).

Ⅳ. 사이버보안 정보공유법

1. 개 관

미국의 사이버보안법은 2015년에 이르러 새로운 전환을 맞게 된다. 독자적인 「사이버보안 정보공유법」(Cybersecurity Information Sharing Act of 2015: CISA)이 제정되었기 때문이다. 오바마 전 대통령은 2015년 12월 8일 일괄입법 형식의 '통합세출법안'(Consolidated Appropriations Act)에 서명하였는데, 여기에 「사이버보안 정보공유법안」이 포함되어 있었던 것이다.[31] 비교법적인 측면에서 볼 때, 유럽연합이나 독일, 일본, 중국 등은 아직 본격적이면서 독자적인 사이버보안 정보공유법을 갖고 있지 않다는 점에서, 이렇게 독자적인 「사이버보안 정보공유법」을 제정한 미국의 입법적 시도는 우리가 결코 간과해서는 안 될 부분이라고 말할 수 있다. 이러한 「사이버보안 정보공유법」은 다음과 같은 목적에서 제정되었다. 미국 연방의회는 「사이버보안 정보공유법」을 통해 공적 기관과 사적 기관이 '사이버위협 정보'(cyber threat information)를 공유하도록 장려하는 동시에 기밀정보, 정보출처 그리고 프라이버시 및 개인적 자유를 보호할 수 있는 사이버보안 정보에 대한 자발적 공유 절차를 창설하는 것이다.[32] 실제 「사이버보안 정보공유법」은 민간기관과 공적 기관 간의 관계를 직접적으로 다룬 최초의 사이버보안 관련 법제에 해당한다. 미국 연방정부의 입장에서는 이러한 관계를 다루는 것이 특별히 중요하게 여겨졌는데, 이는 특히 미국 주요기반시설의 상당부분이 민간에 의해 소유 및 운영되고 있다는 점에 기인한다.[33]

이러한 「사이버보안 정보공유법」의 주요 내용으로는 민간영역, 주정부 및 지방정부, 그리고 연방정부 간 사이버보안 관련 정보를 공유할 수 있는

---

31) Jamil N. Jaffer, *Carrots and Sticks In Cyberspace: Addressing Key Issues in the Cybersecurity Information Sharing Act of 2015*, 67 S.C.L.Rev. 585, 585-586 (2016).

32) The Department of Homeland Security & The Department of Justice, PRIVACY AND CIVIL LIBERTIES FINAL GUIDELINES: CYBERSECURITY INFORMATION SHARING ACT OF 2015, June 15, 2016, p. 3.

33) Jamil N. Jaffer, *supra* note 31, at 586.

권한을 강화하는 것을 들 수 있다. 아래에서는 「사이버보안 정보공유법」이 정보공유에 관해 규율하는 주요 내용을 구체적으로 살펴보도록 한다.

2. 「사이버보안 정보공유법」에 따른 공유대상 정보

아래에서 자세히 살펴보겠지만, 「사이버보안 정보공유법」에 따라 연방기관이 공유할 수 있는 사이버보안 정보와 비연방기관이 공유할 수 있는 사이버보안 정보의 범위는 다르다.[34]

「사이버보안 정보공유법」에 따르면, 연방기관은 '사이버위협 지표'(Cyber Threat Indicators: CTIs)와 '방어조치'(Defensive Measures: DMs) 이외에 사이버보안 위협에 관련된 정보나 동법이 허용하는 (정보)이용에 관한 정보도 공유할 수 있는 데 반해, 비연방기관은 오직 사이버위협 지표와 방어조치에 관한 정보만 공유할 수 있다. 아래에서는 연방기관과 비연방기관이 공통적으로 공유할 수 있는 사이버위협 정보에 해당하는 사이버위협 지표와 방어조치에 관해 구체적으로 검토하도록 한다.

(1) 사이버위협 지표

「사이버보안 정보공유법」에 따르면, 사이버위협 지표란 다음과 같은 사항을 묘사하거나 확인하는 데 필요한 정보를 의미한다.[35]

- 악의적 정찰,[36]
- 보안통제를 무력화시키거나 보안취약점을 악용하는 방법,
- 보안취약점,[37]
- 정보시스템 또는 그와 같은 시스템에 저장되거나, 그와 같은 시스템에 의해 처리되거나, 또는 그와 같은 시스템을 통과하는 정보에 합법적으로 접근할 수 있는 이용자로 하여금 자신도 모르는 사이

34) 여기에서 말하는 비연방기관에는 주정부, 지방정부 등 주 차원에서의 기관뿐 아니라, 민간기관까지도 포함된다. 비연방기관의 의미에 대해서는 CISA, Section 102(14) 참조.
35) CISA, Section 102(6).
36) 사이버보안 위협이나 보안취약점에 관한 기술적 정보를 수집할 목적에서 전송되는 것으로 보이는 이례적 패턴의 통신을 포함한다.
37) 보안취약점의 존재를 나타내는 것으로 보이는 이례적 활동을 포함한다.

에 보안통제를 무력화시키거나 보안취약점을 악용할 수 있도록 하는 방법,
- 악의적 사이버 지휘 및 통제,
- 사고에 의해 야기되는 현실적 또는 잠재적 위해,[38]
- (그 공개가 달리 법에 의해 금지되지 않는 경우) 기타 사이버보안 위협의 속성,
- 그리고 위에서 언급한 것들의 조합.

(2) 방어조치

「사이버보안 정보공유법」은 '방어조치'(Defensive Measure)를 "정보 시스템 또는 그와 같은 시스템에 저장되거나, 그와 같은 시스템에 의해 처리되거나 또는 그와 같은 시스템을 통과하는 정보에 적용됨으로써 이미 알려져 있거나 또는 의심이 되는 사이버보안 위협이나 보안 취약성을 감지, 예방 또는 경감시키는 행위·장치·절차·기호(signature)·기술·기타 조치"로 정의한다.[39] 다음은 이와 같은 방어조치의 대표적인 예가 된다.[40]

- 단체로 흘러들어가는 웹트래픽(web traffic)에서 악의적인 활동의 패턴을 찾아내는 컴퓨터 프로그램,
- 고유한 특징을 가지고 있는 '스피어 피싱 활동'(spear phishing campaign)을 감지하기 위해 회사의 침입 감지 시스템에 로드할 수 있는 기호,
- 악성 트래픽이 네트워크에 진입하는 것을 허용하지 않는 '방화벽 규칙'(firewall rule),
- 악의적 활동을 나타낼 수 있는 이례적 패턴들을 찾아내기 위한 것으로서 '네트워크 트래픽 캐시'(cache of network traffic)를 통해 검

38) 특정한 사이버보안 위협의 결과로 유출된 정보에 대한 묘사를 포함한다.

39) CISA, Section 102(7)(A).

40) 방어조치의 대표적인 예에 대해서는 The Department of Homeland Security & The Department of Justice, GUIDANCE TO ASSIST NON-FEDERAL ENTITIES TO SHARE CYBER THREAT INDICATORS AND DEFENSIVE MEASURES WITH FEDERAL ENTITIES UNDER THE CYBERSECURITY INFORMATION SHARING ACT OF 2015, June 15, 2016, p. 7.

색할 수 있는 알고리즘,

- 최종 사용자에 대한 이메일 전송 속도를 용납할 수 없을 정도로 낮추지 않으면서도, 자동화된 방법으로 재빨리 단체에 유입되는 'SMTP 트래픽'(Simple Mail Transfer Protocol)의 내용을 특정한 사이버보안 위협과 관련된 것으로 알려진 일련의 내용에 매칭(matching) 시키는 기술.

3. 연방정부에 의한 정보공유

「사이버보안 정보공유법」은 연방정부로 하여금 민간영역과 (기밀에 해당하든 그렇지 않든 간에) 사이버위협 정보의 공유를 가능하게 하고 또 촉진할 수 있는 절차를 개발하도록 요구한다. 구체적으로 「사이버보안 정보공유법」 Section 103은 '국가정보국장'(Director of National Intelligence), '국토안보부 장관'(Secretary of Homeland Security), '국방부 장관'(Secretary of Defense) 그리고 '법무부 장관'(Attorney General)이 적절한 연방기관의 책임자들과 협의하여 공동으로 다음과 같은 정보의 공유를 가능케 하고 촉진할 수 있는 절차를 개발하여 발표하도록 하고 있다.[41]

첫째, 연방정부가 소유하고 있는 **기밀에 해당하는 사이버위협 지표 및 방어조치에 관한 정보**를 기밀취급 인가(security clearance)를 받은 관련 연방기관 및 비연방기관의 대표자와 시기적절하게 공유한다.

둘째, 연방정부가 소유하는 **사이버위협 지표, 방어조치 그리고 사이버보안 위협 또는 「사이버보안 정보공유법」에 따라 허용되는 이용에 관한 정보로서 기밀이 해제되어 기밀이 아닌 수준으로 공유될 수 있는 사이버위협 정보**를 관련 연방기관 및 비연방기관과 시기적절하게 공유한다.

셋째, 연방정부가 소유하는 **기밀에 해당하지 않는 사이버위협 지표 및 방어조치**를 관련 연방기관, 비연방기관 그리고 적절한 경우에는 일반 공중과 시기적절하게 공유한다.

넷째, 연방정부가 소유하는 **사이버보안 위협 또는 「사이버보안 정보**

41) CISA, Section 103(a); 강조는 인용자가 추가한 것이다.

공유법』 아래에서 허용되는 이용에 관한 정보를 적절한 경우, 그와 같은 사이버보안 위협으로부터 발생하는 부정적인 효과를 방지하거나 감소시키기 위한 목적으로 해당 기관에 대한 사이버보안 위협과 관련하여 연방기관 및 비연방기관과 시기적절하게 공유한다.

다섯째, 연방정부가 소유하는 사이버위협 지표, 방어조치, 사이버보안 위협 또는 「사이버보안 정보공유법」 아래에서 허용되는 이용에 관한 정보를 지속적으로 분석한 것을 기초로 하여 개발된 **사이버보안 모범 실무**를 출판 등을 통해 정기적으로 공유한다.

(1) 기밀에 해당하는 '사이버위협 지표' 및 '방어조치'의 공유

기밀에 해당하는 사이버위협 정보를 공유할 수 있는가 여부는 정보수령인이 기밀취급 인가를 받았는지 여부에 의존할 수밖에 없다.[42] 이에 더하여 기밀정보를 공유하는 모든 연방기관은 이미 존재하고 있는 '분류기준'(classification standards)을 따라야 할 뿐 아니라, 다른 기관들과 공유할 수 있는 정보가 어떤 정보들인지를 결정할 때 '등급이 완화된 정보'(downgraded information)의 사용에 관한 취급제한을 준수해야만 한다.[43]

국토안보부의 '강화된 사이버보안 서비스'(Enhanced Cybersecurity Services)(이하에서는 'ECS'로 약칭) 프로그램은 연방정부가 소유하는 기밀에 해당하는 사이버위협 지표나 방어조치에 관한 정보를 기밀취급 인가를 받은 관련 연방 또는 비연방기관의 대표자들과 시기적절하게 공유하는 것을 지원해 주는 대표적인 절차이다. 이와 같은 국토안보부의 ECS 프로그램은 미국에 그 기반을 두고 있는 공적 기관이나 사적 기관이 '허가받지 않은 접근'(unauthorized access), '부당이용'(exploitation) 또는 '데이터 유출'(data exfiltration)로부터 자신들의 컴퓨터 시스템을 보호하고자 할

42) The Office of the Director of National Intelligence & The Department of Homeland Security & The Department of Defense & The Department of Justice, SHARING OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY THE FEDERAL GOVERNMENT UNDER THE CYBERSECURITY INFORMATION SHARING ACT OF 2015, February 16, 2016, p. 7.

43) *Id.*

때 도움을 주는 '자발적 정보공유 프로그램'이다. 국토안보부는 민감정보에 해당하면서 동시에 기밀정보에 해당하는 광범위한 사이버위협 정보에 접근하기 위해, 연방정부 전체에 걸쳐 활동하고 있는 사이버보안 관련기관들과 협력한다. 국토안보부는 이를 통해 획득한 정보를 기초로 해서 사이버위협 지표를 개발하고, 이를 자격을 갖춘 '상업용 서비스 제공자'(commercial service providers: CSPs)와 공유함으로써 그들의 고객을 더 잘 보호할 수 있도록 해준다. 이에 반해 상업용 서비스 제공자에 의해 감지된 사이버위협 및 말웨어 활동(malware activity)에 관한 정보는 이들 고객과 연방정부 간에 직접적으로 공유되지는 않는다.[44] 다만 상업용 서비스 제공자의 고객이 자발적으로 동의하는 경우, 상업용 서비스 제공자는 국토안보부와 제한적이고 익명화된 정보를 공유할 수 있을 뿐이다.

(2) 기밀이 해제되어 기밀이 아닌 수준으로 공유될 수 있는 사이버위협 정보의 공유

사이버위협 정보가 가능한 한 광범위하게 공유될 수 있도록 하기 위해, 연방정부에게는 정보수준을 격하하거나(downgrade), 기밀을 해제하거나(declassify) 또는 정보로부터 공유를 불가능하게 하거나 곤란하게 하는 부분을 제거하는 것(sanitize) 등이 장려된다.[45] 다음의 두 프로그램은 연방정부가 기밀을 해제하여 기밀이 아닌 수준에서 사이버위협 정보를 공유할 수 있도록 하는 대표적인 예이다.

1) 국토안보부의 '국가 사이버보안 및 통신 통합센터'

국토안보부에 소속된 '국가 사이버보안 및 통신 통합센터'(NCCIC)는 일상적으로 다른 연방기관들로부터 기밀에 해당하는 사이버위협 지표, 방어조치 및 사이버보안 위협에 관한 정보를 수령하여 이를 분석한다. 뿐만 아니라 기밀취급 인가를 받은 연방기관이나 비연방기관과 협의를 통해

44) 국토안보부의 이와 같은 ECS 프로그램에 대해서는 *Id.* 참고; 한편 'malware activity'란 컴퓨터 프로그램을 파괴하는 활동을 말한다. 쉽게 말해, 넓은 의미의 해킹에 해당한다.

45) *Id.* at 9.

NCCIC는 '취급제한'(classification restrictions)에서 허용하는 것보다 더 광범위하게 정보를 공유할 수 있는 요건을 별도로 인정할 수 있다.[46] 이 경우 NCCIC는 '지표 게시판'(indicator bulletins)이나 다른 채널을 통해 이해관계자와 그 정보를 공유하기 위해, 그와 같은 정보를 제공한 연방기관과 함께 그 정보의 수준을 격하하거나, 그 정보로부터 공유를 불가능 또는 곤란하게 하는 부분을 제거하거나 또는 기밀을 해제하기 위한 작업을 행할 수 있다.

2) FBI의 'Private Industry Notifications(PINs)'과 'Liaison Alert System(FLASH) Reports'

연방수사국(Federal Bureau of Investigation: FBI)은 'PINs'와 'FLASH reports'를 통해 민간영역에 '맥락 관련 정보'(contextual information)와 '기술 관련 정보'(technical information)를 전송하기 위해 이러한 정보의 기밀을 해제하는 작업을 한다.[47] PINs와 FLASH reports는 정보수령인이 위협을 확인하는 데 이용할 수 있는 높은 수준의 분석적 또는 기술적 정보와 함께 현재 생성 중인 사이버위협이나 경향에 관한 특수한 세부사항들을 민간의 산업영역에 전달한다. PINs가 위협에 관한 맥락 관련 정보를 제공하고 사이버위협에 관한 전략, 기술, 절차, 기타 정보를 포함하는 것이라면, FLASH reports는 계속 진행 중인 위협에 즉각적으로 대응할 수 있는 기술 관련 정보를 제공한다.

(3) 기밀에 해당하지 않는 '사이버위협 지표' 및 '방어조치'의 공유

일반적으로 연방기관들은 특정한 사이버위협 지표나 방어조치에 관한 '취급지시'(handling instructions)를 준수하는 한 기밀에 해당하지 않는 사이버위협 지표와 방어조치를 가능한 한 다른 연방기관이나 비연방기관들도 이용할 수 있도록 해야 한다.[48] 연방기관은 비연방기관으로부터 「사이

46) *Id.* at 9-10.

47) *Id.* at 10; 여기서 '맥락 관련 정보'란 어떤 맥락, 가령 어떤 웹트래픽이 해킹과 관련이 되는지에 관한 정보를 뜻한다. 이에 대해 '기술 관련 정보'란 이를테면 이러한 해킹에 대응하기 위해서는 어떤 기술적 수단을 사용해야 하는지에 관한 정보를 뜻한다.

버보안 정보공유법」 Section 105(c)에서 규정하는 실시간 방법 이외의 방법으로 사이버위협 지표나 방어조치를 수령한 경우에도, 법령을 준수하고 그 기관의 임무에 부합하는 방향으로 가능한 한 빨리 다른 적절한 연방기관에 이러한 사이버위협 지표 및 방어조치를 공유해 주어야만 한다.

이에 관해 국토안보부가 마련한 '자동화된 지표 공유(Automated Indicator Sharing: AIS) 제도'를 언급할 필요가 있다. AIS는 연방정부가 기밀에 해당하지 않는 사이버위협 지표 및 방어조치에 관한 정보를 민간영역과 공유할 수 있도록 하는 대표적인 프로그램이다. AIS는 국토안보부 자신이 개발한 사이버위협 지표와 방어조치를 다른 연방기관이나 비연방기관과 공유할 수 있도록 하는 프로그램이기도 하지만, 다른 연방기관이나 비연방기관 또한 스스로 네트워크 방어노력을 기울이던 중 발견한 위협지표들을 이러한 AIS를 통해 공유할 수 있다.

4. 비연방기관에 의한 정보공유

「사이버보안 정보공유법」은 정보공유를 강화하기 위해 민간기관에게도 정보공유에 관해 상당히 광범위한 권한을 부여한다. 구체적으로 보면, 정보공유 및 이용이 정보를 제공한 기관이 부여하는 합법적인 제한에 부합하고, 정보를 제공받은 기관이 그 정보를 사용, 보유 및 다시 공유하는 것이 법령상의 제한에 위배되지 않는 한, 「사이버보안 정보공유법」은 민간기관에게 다른 민간기관 및 연방정부와 사이버위협 지표와 방어조치를 공유하고,[49] 이렇게 공유된 위협지표 및 방어조치를 사이버보안의 목적으로 사용할 수 있는 권한을 부여한다.[50] 여기서 사이버보안의 목적이란 "사이버보안 위협이나 보안 취약성으로부터 정보 시스템 또는 그와 같은 시스템에 저장되거나, 그와 같은 시스템에 의해 처리되거나 또는 그와 같은 시스템을 통과하는 정보를 보호할 목적"을 의미한다.[51]

---

48) *Id.*

49) CISA, Section 104(c).

50) Jamil N. Jaffer, *supra* note 31, at 589.

51) CISA, Section 102(4).

(1) 비연방기관이 공유할 수 있는 정보

이처럼 「사이버보안 정보공유법」 Section 104(c)에 따르면, 비연방기관은 (다른 법령의 규정에도 불구하고) 사이버보안의 목적을 위해 사이버위협 지표나 방어조치를 공유할 수 있다. 따라서 사생활보호법(privacy laws) 등 다른 상충하는 법령이 있다 하더라도 「사이버보안 정보공유법」에 따라 이루어지는 정보공유를 제한할 수는 없다.[52] 하지만 「사이버보안 정보공유법」은 정보공유를 촉진하면서도 프라이버시를 보호하기 위해 비연방기관이 공유 당시에 첫째, 특정 개인의 개인정보에 해당한다거나 또는 특정 개인을 식별할 수 있는 정보에 해당한다는 사실을 알았고, 둘째, 그 정보가 사이버보안 위협과 직접적으로 관련된 것도 아니라면, 공유 이전에 그와 같은 정보를 사이버위협 지표나 방어조치에서 제외하도록 비연방기관에 요구하고 있다.[53]

두 번째 요건과 관련하여, 정보가 만약 사이버보안에 대한 위협을 감지 또는 예방하거나, 경감시키는 데 필요한 것이 아니라면 그와 같은 정보는 사이버보안 위협에 직접적으로 관련된 것이라 할 수 없다.[54] '스피어 피싱 메일'을 예로 들면, 그와 같은 이메일 발신자의 개인정보, 이메일 내의 악의적인 URL, 이메일에 첨부된 파괴소프트웨어 파일, 이메일의 내용 등은 사이버보안 위협에 직접적으로 관련된 것으로 인정될 수 있는 반면, 이메일 수신자의 이름이나 그의 이메일 주소 등은 사이버보안 위협에 직접적으로 관련되지 않은 개인정보로서 사이버위협 지표에서 제외되어야 한다.[55]

「사이버보안 정보공유법」 Section 105(a)(4)(B)(ii)는 비연방기관에게 이와 같이 공유 가능한 정보를 좀 더 명확하게 해주기 위해, 가이드라인에서 사이버보안 위협에 직접적으로 관련되지는 않으면서 사생활보호법에 의해 보호되는 정보의 유형을 제시하도록 요구하고 있다. 이에 따라 「사이버보안 정보공유법」에 의해 마련된 「연방정부와 사이버위협 지표 및 방어조치를 공유하는 비연방기관을 위한 안내」(Guidance to Assist

52) The Department of Homeland Security & The Department of Justice, *supra* note 40, at 7.
53) CISA, Section 104(d)(e).
54) The Department of Homeland Security & The Department of Justice, *supra* note 40, at 5.
55) *Id.*

Non-Federal Entities to Share Cyber threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015)에서는 다음과 같은 두 가지 유형의 정보를 사이버보안 위협에 직접적으로 관련되지 않으면서 동시에 사생활보호법에 의해 보호되는 정보의 대표적인 예로 제시한다.[56]

첫째는 사생활보호법에 의해 보호되는 건강관련 정보로서, 그 형식과 매체를 불문하고 사생활보호법이 적용되는 기관이나 그와 같은 기관의 사업상 파트너가 전송하거나 보유하는 개인을 식별할 수 있는 건강관련 정보이다.[57] 여기서 사생활보호법에 의해 보호되는 건강관련 정보는 (i) 개인의 과거, 현재 또는 미래의 육체적 또는 정신적 건강이나 상태, (ii) 개인에 대한 의료서비스의 제공, (iii) 개인에게 의료서비스를 제공한 데 대한 과거, 현재 또는 미래의 비용지급으로서 특정 개인을 나타내거나 또는 특정 개인을 나타내는 데 사용될 수 있을 것으로 믿을 합리적 근거가 존재하는 것과 관련된 정보를 의미한다.

둘째는 매우 민감하고 따라서 높은 정도의 규제를 필요로 하는 대부분의 금융정보가 여기에 해당한다. 이때 말하는 금융정보에는 은행계좌의 입출금내역, 대출 정보, 신용평가 보고서 등이 포함된다.

(2) 정보공유 방법

「사이버보안 정보공유법」 Section 104(c)는 비연방기관에게 연방기관 및 다른 비연방기관과 사이버위협 지표 및 방어조치를 공유할 수 있는 권한을 부여하고 있다. 동법 Section 105(c)는 특히 비연방기관이 이와 같은 정보들을 국토안보부가 운영하는 “권한 및 절차”(Capability and Process)를 통해 공유하는 것에 관해 규정하고 있다.[58] 정보가 공유되는 방법은 사이버위협 지표나 방어조치를 공유한 민간기관이 받게 되는 보호의 정도에 영향을 미치는데, 민간기관이 국토안보부의 ‘권한 및 절차’를 통하거나

56) *Id.* at 9.
57) 45 CFR 160.103.
58) The Department of Homeland Security & The Department of Justice, *supra* note 40, at 10.

또는 달리 「사이버보안 정보공유법」 Section 105(c)(1)(B)에서 허용하는 방법으로 연방정부와 정보를 공유하는 경우에는,[59] 동법 Section 106(b)가 적용되어 그와 같은 정보공유에 대해 법적 책임을 부담하지 않게 된다.[60] 「사이버보안 정보공유법」 Section 104(c)는 동법 Section 105(c)(1)(B)가 규정하는 정보공유 방법 외의 정보공유도 허용하고 있지만, 이처럼 Section 105(c)(1)(B)가 규정하는 방법 외의 방법으로 민간기관이 연방정부와 사이버위협 지표 및 방어조치를 공유하게 되면, 이러한 민간기관은 동법 Section 106(b)의 면책조항의 적용을 받지는 못하게 된다.[61] 그러므로 「사이버보안 정보공유법」상 비연방기관이 연방기관이나 다른 비연방기관과 사이버위협 지표 및 방어조치를 공유하는 방법은 다음과 같이 크게 국토안보부의 '권한 및 절차'를 통하는 방법과 그 이외의 방법 두 가지로 나누어 살펴볼 필요가 있다.

1) 국토안보부의 실시간 '권한 및 절차'를 통한 정보공유

「사이버보안 정보공유법」 Section 105(c)는 국토안보부 장관으로 하여금

59) 「사이버보안 정보공유법」 Section 105(c)(1)(B)는 국토안보부가 운영하는 '권한 및 절차'(Capability and Process)를 비연방기관이 공유하는 사이버위협 지표 및 방어조치를 연방정부가 수령하는 원칙적인 방법으로 규정한다. 물론 Section 105(c)(1)(B)는 (i) 관련된 사이버보안 위협에 대해 설명하거나 이미 공유된 사이버위협 지표에 근거하여 방어조치를 강구할 목적으로, 이미 이전에 공유된 사이버위협 지표에 관해 연방기관과 비연방기관 사이에 이루어지는 의사소통과 (ii) 규제대상이 되는 비연방기관이 규제주체인 연방기관과 사이버보안 위협에 관해 행하는 의사소통에 대해서는 예외를 인정한다.

60) 「사이버보안 정보공유법」 Section 106(b)는 "민간기관이 동법 Section 104(c)에 따라 사이버위협 지표나 방어조치를 공유 또는 수령하는 경우에, (1) 그와 같은 공유나 수령이 동법에 부합하고, (2) 사이버위협 지표나 방어조치를 특히 연방정부와 공유하는 경우에는, 그와 같은 사이버위협 지표나 방어조치가 동법 Section 105(c)(1)(B)에 부합하는 방법으로 이루어진 경우, 민간기관에 대해서는 그와 같은 정보공유를 이유를 소를 제기할 수 없고 만약 소가 제기되었다면 이는 각하"되어야 한다고 규정한다. 따라서 민간기관이 연방정부 이외의 기관과 정보를 공유하는 경우에는 「사이버보안 정보공유법」을 위반하지만 않으면 동법 Section 106(b)의 면책조항이 적용되는 데 반해, 연방정부와 정보공유를 하는 경우에는 그와 같은 정보공유가 「사이버보안 정보공유법」을 위반하지 않아야 할 뿐 아니라, 동법 Section 105(c)(1)(B)에서 규정하는 방법에 따라 정보공유가 이루어져야만 동법 Section 106(b)의 면책조항이 적용된다.

61) The Department of Homeland Security & The Department of Justice, *supra* note 40, at 10.

(민간기관을 포함하여) 비연방기관으로부터 사이버위협 지표 및 방어조치를 실시간으로 수령할 수 있는 '권한 및 절차'를 국토안보부 내에 개발하도록 요구하고 있다. 비연방기관이 이러한 '권한 및 절차'를 통해 국토안보부에 사이버위협 지표 및 방어조치를 공유하면, 국토안보부는 다시 그 정보를 자동화된 방법을 통해 다른 연방기관들에 전달한다.[62] 「사이버보안 정보공유법」 Section 105(c)(2)(A)에 따라 국토안보부 장관이 이와 같은 '권한 및 절차'가 완전하고 효과적으로 작동한다는 증명서를 연방의회에 제출하면,[63] 이는 자동화된 실시간 교환, 전자우편, 웹사이트 인터페이스(website interface)를 통해 비연방기관이 공유하는 사이버위협 지표 및 방어조치를 연방정부가 수령하는 방법이 된다.[64]

가. 자동화된 지표 공유(AIS)

비연방기관은 국토안보부의 '자동화된 지표 공유'(Automated Indicator Sharing: AIS) 제도를 통해 연방기관들과 사이버위협 지표 및 방어조치를 공유할 수 있는데, 이러한 국토안보부의 AIS는 민간부문, 주 및 지방정부 그리고 연방정부 사이에서 사이버위협 지표 및 방어조치가 시기절절하게 교환되는 것을 가능하게 한다.[65] AIS는 'Structured Threat Information eXchange'(STIX)와 'Trusted Automated eXchange of Indicator Information'(TAXII)을 사용하여 각각 사이버위협 지표 및 방어조치의 '포맷'(format)과 '교환'(exchange)을 위한 기술규격서(technical specification)를 활용한다.[66] 표준화된 영역(STIX)과 소통방식(TAXII)을 사용함으로써 국토안보부는 기관들이 서로 안전하고 자동화된 방법으로 사이버위협 정보를 공유할 수 있도록 한다.[67] AIS 참가자들은 AIS를 통해 사이버위협 지표와 방어조치를 공유하기 위해 국토안보부의 TAXII 서버와 소통할 'TAXII 클라이언트'

62) *Id.* at 12.

63) 「사이버보안 정보공유법」이 요구하는 바에 따라 국토안보부 장관은 2016년 3월 17일에 국토안보부 안에 마련된 '권한 및 절차'가 작동 가능함을 증명하였다.

64) The Department of Homeland Security & The Department of Justice, *supra* note 40, at 12.

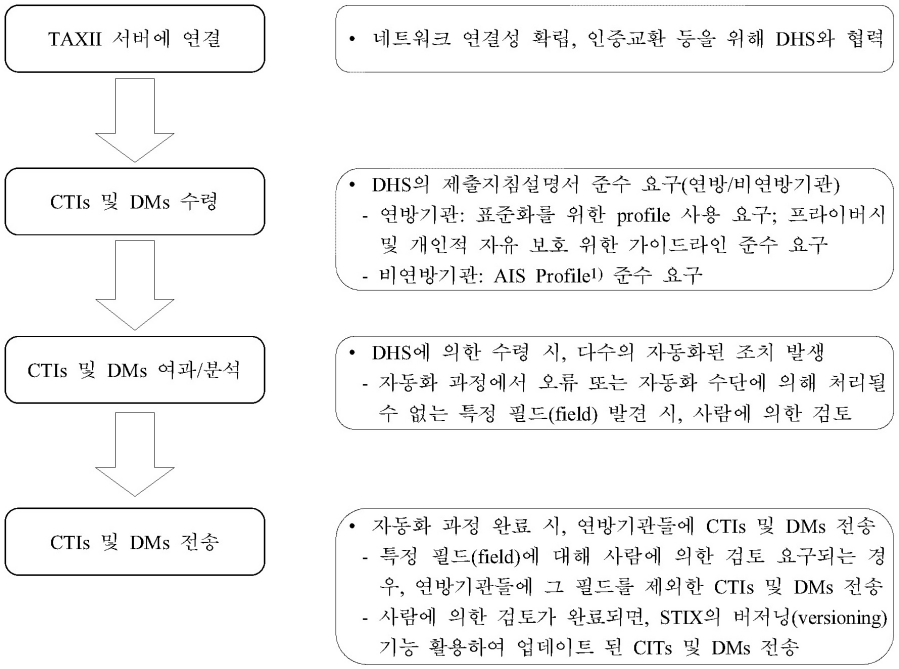
65) *Id.* at 13.

66) *Id.*

67) *Id.*

를 모집한다.[68] 이와 같은 AIS 참가자들은 AIS 이용약관을 작성하고, AIS를 통해 사이버위협 지표 및 방어조치를 제출하는 경우 반드시 제공되어야 하거나 또는 제공되어선 안 되는 정보의 유형들을 규정하고 있는 제출지침에 따라야 한다.[69] 일단 사이버위협 지표나 방어조치가 AIS에 의해 수령·분석·처리되면, AIS는 이와 같은 사이버위협 지표나 방어조치를 모든 AIS 참가자들과 공유한다.[70] 아래는 「사이버보안 정보공유법」 Section 105(c)가 규정하는 바에 따라 국토안보부의 AIS를 통해 연방정부와 사이버위협 지표 및 방어조치를 공유하는 과정을 나타낸 것이다.[71]

<표-1> 자동화된 지표 공유제도



68) *Id.*

69) *Id.*

70) *Id.*

71) 이에 대해서는 The Department of Homeland Security & The Department of Justice, FINAL PROCEDURES RELATED TO THE RECEIPT OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY THE FEDERAL GOVERNMENT, June 15, 2016, p. 3-9.

나. 웹 양식 작성을 통한 공유[72]

나아가 비연방기관은 국토안보부의 웹사이트에서 웹 양식을 작성함으로써 국토안보부의 '국가 사이버보안 및 통신 통합센터'(NCCIC)와 사이버위협 지표 및 방어조치를 공유할 수 있다.[73][74] 웹 양식으로 '국가 사이버보안 및 통신 통합센터'에 제출되는 사이버위협 지표 및 방어조치들 또한 「사이버보안 정보공유법」 Section 105(c)에 의해 구축된 국토안보부의 '권한 및 절차'의 일부로 인정되므로, 「사이버보안 정보공유법」 Section 106(b)의 면책조항이 적용될 수 있다.

비연방기관이 이처럼 웹 양식을 작성함으로써 사이버위협 지표 및 방어조치를 공유하면, 이는 먼저 국토안보부의 사이버위협 분석가에게 전달된다. 사이버위협 분석가는 첫째, 비연방기관에 의해 공유된 정보에 유효한 사이버위협 지표 및 방어조치에 관한 정보가 있는지, 둘째, 만약 그렇다면 혹시 그와 같은 사이버위협 지표 및 방어조치가 사이버보안 위협에 직접적으로 관련되지 않은 개인정보 또는 개인식별정보를 포함하고 있는 것은 아닌지를 검토한다. 이러한 검토가 끝나면 공유된 사이버위협 지표 및 방어조치는 국토안보부의 사이버위협 저장소로 이송되고, 사이버위협 저장소로 이송된 정보들은 적절한 연방기관들에 전달될 수 있도록 국토안보부의 TAXII 서버로 전송된다.[75]

---

72) AIS Profile은 국토안보부가 다른 연방기관과 협의를 거쳐 사이버위협 지표 또는 방어조치와 가장 직접적으로 관련되어 있다고 판단한 '입력필드'(input field)가 포함되도록 하는 데 그 목적이 있다. STIX 포맷이 수천 개의 필드들을 포함하고 있는데 반해, AIS Profile은 사이버보안 위협에 직접 관련되는 것으로 판단되고 「사이버보안 정보공유법」이 요구하는 바와 같이 프라이버시 및 개인적 자유를 보호하는 필드들의 부분집합이다. STIX 포맷과 AIS Profile의 차이점에 관해서는 *Id.* at 4.

73) The Department of Homeland Security & The Department of Justice, *supra* note 40, at 13.

74) 물론 앞에서 설명한 바와 같이, STIX와 TAXII를 이용한 자동화된 교환이 훨씬 선호되는 방법이다. The Department of Homeland Security & The Department of Justice, *supra* note 71, at 9.

75) 웹 양식 작성 이후의 이와 같은 일련의 과정에 대해서는 *Id.* at 9-10.

다. 이메일을 통한 공유

뿐만 아니라, 비연방기관은 국토안보부에 이메일을 보내는 방법을 통해 국토안보부의 '국가 사이버보안 및 통신 통합센터'와 사이버위협 지표 및 방어조치를 공유할 수 있다.[76] 국토안보부의 웹사이트에서 웹 양식을 작성하는 경우와 마찬가지로, 이메일을 통해 제출되는 사이버위협 지표 및 방어조치들 또한 「사이버보안 정보공유법」 Section 105(c)에 의해 구축된 국토안보부의 '권한 및 절차'의 일부로 인정되므로, 「사이버보안 정보공유법」 Section 106(b)의 면책조항이 적용될 수 있다. 이메일을 통한 정보공유에 대해서도, 앞에서 검토한 바 있는 웹 양식의 작성을 통한 정보공유와 마찬가지로, 사이버위협 분석가에게 전달 → 사이버위협 분석가에 의한 검토 → 사이버위협 저장소로 이송 → TAXII 서버로 전송이라는 동일한 과정이 적용된다.[77]

라. ISAC와 ISAO를 통한 공유

「사이버보안 정보공유법」 Section 104(c)에 따라 비연방기관은 '정보공유·분석센터'(Information Sharing and Analysis Centers: ISACs)나 '정보공유·분석기구'(Information Sharing and Analysis Organizations: ISAOs)를 통해서도 연방기관들과 사이버위협 지표 및 방어조치에 관한 정보를 공유할 수 있다.[78] 민간기관에 해당하는 ISACs나 ISAOs는 비연방기관으로부터 제출받은 사이버위협 지표 및 방어조치를 국토안보부를 통해 연방기관들과 공유할 수 있다. 「사이버보안 정보공유법」 Section 106(b)(1)에 따르면, 「사이버보안 정보공유법」에 부합하는 방법으로 ISAC나 ISAO와 사이버위협 지표나 방어조치를 공유한 민간기관은 그와 같은 정보공유에 대해 면책을 받을 수 있다. 뿐만 아니라, 「사이버보안 정보공유법」에 부합하는 방법으로 다른 민간기관과 정보를 공유한 ISAC나 ISAO에 대해서도 「사이버보안 정보공유법」 Section 106(b)(1)상의 면책조항이 적용될 수 있다.

76) The Department of Homeland Security & The Department of Justice, *supra* note 40, at 14.
77) The Department of Homeland Security & The Department of Justice, *supra* note 71, at 9.
78) The Department of Homeland Security & The Department of Justice, *supra* note 40, at 14.

이와 마찬가지로 「사이버보안 정보공유법」 Section 105(c)에 의해 구축된 국토안보부의 '권한 및 절차'를 통해 동법 Section 104(c)에 부합하는 방법으로 연방정부와 사이버위협 지표 및 방어조치를 공유한 ISAC나 ISAO도 「사이버보안 정보공유법」 Section 106(b)(2)에 따른 정보공유 그 자체에 대한 면책뿐만 아니라, 동법에 따른 다른 보호조항 및 예외조항의 적용을 받는다.[79]

2) 국토안보부의 '권한 및 절차' 이외의 방법을 통한 정보공유

「사이버보안 정보공유법」 Section 104(c)는 다른 법령의 규정에도 불구하고, 비연방기관으로 하여금 사이버보안의 목적으로 연방기관이나 다른 비연방기관과 사이버위협 지표 및 방어조치에 관한 정보를 공유할 수 있도록 하고 있다. 따라서 비연방기관은 앞에서 설명한 바와 같은 국토안보부의 '권한 및 절차'를 통하지 않고도 연방기관이나 다른 비연방기관과 사이버위협 지표 및 방어조치를 공유할 수 있다. 물론 비연방기관이 사이버위협 지표 및 방어조치를 연방기관과 공유하는 경우에는 「사이버보안 정보공유법」 Section 105(c)에서 규정하는 국토안보부의 '권한 및 절차'를 통해야만 동법 Section 106(b)(2)에서 규정하는 정보공유에 대해 면책혜택을 받을 수 있다. 지금까지 논의한 바를 정리하면 아래와 같다.

<표-2> 「사이버보안 정보공유법」상 비연방기관의 권한·요건 및 정보공유에 따른 법적 보호[80]

공유대상기관 & 공유방법		권한 조항	면책 조항	수령 기관	요건	법적 보호
연방 기관	105(c)(1)(B) 방법	§104(c) §105(c) (1)(B)	§106(b) (2)	국토 안보부	• 사이버보안 목적의 공유 §104(c) • CTIs & DMs의 공유	• 정보공유에 대한 면책 §106(b) • 공유대상에 대한 특권 포기 X

79) *Id.*

80) 이 표는 The Department of Homeland Security & The Department of Justice, *supra* note 40, at 19-20, 22를 참조하여 수정·보완한 것임.

공유대상기관 & 공유방법		권한 조항	면책 조항	수령 기관	요건	법적 보호
					§§104(c), 106(b)(2) • 보안통제의 실시 §104(d)(1) • 사이버 위협에 직접 관련되지 않은 개인정보 또는 개인식별 가능정보 제거 §§104(d)(2)(A), (B) • 국토안보부에의 제출 절차 준수	§105(d)(1) • 상업, 금융, 독점 정보 취급 §105(d)(2) • 정보공개법 적용 면제 §105(d)(3) • 일방적 의사 교환 취급 금지 §105(d)(4) • 규제 목적 사용 금지 §105(d)(5)(D)
	기타 방법	§104(c)	적용 없음	연방 기관	• 사이버보안 목적의 공유 §104(c) • CTIs & DMs의 공유 §§104(c), 106(b)(2) • 보안통제의 실시 §104(d)(1) • 사이버 위협에 직접 관련되지 않은 개인정보 또는 개인식별 능정보 제거 §§104(d)(2)(A), (B)	• 공유대상에 대한 특권 포기 X §105(d)(1) • 상업, 금융, 독점 정보 취급 §105(d)(2) • 정보공개법 적용 면제 §105(d)(3) • 일방적 의사 교환 취급 금지 §105(d)(4) • 규제 목적 사용 금지 §105(d)(5)(D)
비연방기관		§104(c)	§106(b)(1)	적용 없음	• 사이버보안 목적의 공유 §104(c) • CTIs & DMs의 공유 §§104(c), 106(b)(1) • 보안통제의 실시 §104(d)(1) • 사이버 위협에	• 정보공유에 대한 면책 §106(b) • 반독점법 미적용 §104(e)

공유대상기관 & 공유방법	권한 조항	면책 조항	수령 기관	요건	법적 보호
				직접 관련되지 않은 개인정보 또는 개인식별 가능정보 제거 §§104(d)(2)(A),(B)	

V. 시사점 - 결론을 대신하여

지금까지 미국의 사이버보안 관련 법제도를 개관하고 「사이버보안 정보공유법」을 분석해 보았다. 마지막으로 결론을 대신하여 미국의 사이버보안 관련 법제도에서 어떤 시사점을 읽어낼 수 있는지 살펴보도록 한다.

1. 개별적 법체계

먼저 확인할 수 있는 점은, 미국은 사이버보안에 관해 통합적인 법을 제정하지 않고, 우리처럼 개별적인 법률을 제정해 시행하고 있다는 점이다. 판덱텐 체계를 추구하는 대륙법 전통과는 달리, 상황에 적합하게 문제를 해결할 수 있는 개별법 방식을 지향하는 미국의 법적 전통을 잘 반영한 것이라 할 수 있다. 이렇게 보면, 사이버보안을 효과적으로 실현하기 위해 논리필연적으로 통합정보보호법이 필요한 것은 아님을 알 수 있다.[81] 그러나 이렇게 개별법 형식을 취하게 되면 법제도 자체에 체계적으로 접근하기 어렵다는 점에서 법제도의 체계성과 효율성이라는 측면을 고려할 때 문제가 있다는 것은 분명해 보인다.

2. 사이버보안의 중심적 거버넌스로서 국토안보부

다음으로 미국은 사이버보안에 관해 국토안보부를 중심적인 거버넌스

81) 이 논의에 관해서는 양천수, "제4차 산업혁명과 정보보호 법정책의 방향", 『공법학연구』 제18권 제4호, 한국비교공법학회, 2017, 369-395쪽 참고.

로 설정하고 있다는 것이다. 이는 「국가사이버보안 보호법」이 잘 보여준다. 이렇게 국가사이버보안 문제를 관할하는 중심적인 거버넌스를 설정함으로써 사이버보안 문제, 즉 정보보호 문제가 발생하였을 때 신속하고 통일적으로 대응할 수 있도록 하고 있다. 이는 정보보호에 관해 아직 중심적인 거버넌스를 갖추고 있지 않은 우리에게 시사하는 바가 크다. 우리나라는 현재 정보보호에 관해 다음과 같은 거버넌스를 갖추고 있다. 공공영역은 국가정보원이, 민간영역은 과학기술정보통신부가 정보보호를 관할한다. 그리고 개인정보보호는 대통령 소속의 개인정보보호위원회와 방송통신위원회가 관할한다. 그러나 이렇게 정보보호에 관한 거버넌스를 분리하는 것이 기능적인 면에서 바람직한지 의문이 없지 않다.

3. 독자적인 정보공유법 제정 및 시행

이어서 미국은 독자적인 「사이버보안 정보공유법」을 제정해 시행하고 있다는 점에 주목해야 한다. 현대 지능정보사회에서 발생하는 정보침해 문제에 효과적으로 대응하기 위해서는 그 무엇보다도 정보공유가 필요하다는 점은 비교법적 분석 등을 포함한 여러 측면에서 확인되고 있다. 특히 정보침해 및 보호에 관한 정보를 광범위하게 공유해야만 정보침해에 효과적으로 방어할 수 있는 각종 '방어조치' 역시 더욱 수월하게 개발될 수 있다는 점을 고려하면, 정보보호와 정보공유가 선순환관계를 맺는다는 점을 알 수 있다. 이러한 근거에서 볼 때 정보공유를 적극적으로 활성화할 수 있는 법적 토대와 지원이 필요하다. 이 점에서 독자적인 정보공유법을 제정해 시행하고 있는 미국의 입법태도는 우리에게 시사하는 바가 크다. 우리 역시 현대사회에서 발생하는 정보침해 문제에 적절하게 대응할 수 있는 독자적인 '정보보호를 위한 정보공유법'을 제정할 필요가 있다.

4. 정보공유의 대상·방법·참여주체

나아가 미국은 정보공유의 대상, 방법, 참여주체에 관해 아주 광범위하면서도 구체적인 방안을 제시한다. 첫째, 공유대상 정보를 유형화하면서 여기에서 개인정보를 배제하고 있다. 둘째, 연방기관과 주정부 같은 국가

기관 사이에서만 정보공유를 허용하는 것이 아니라, 국가기관과 민간 사이에서도 정보공유가 가능하도록 하고 있다. 셋째, 정보공유에 관한 중심적인 거버넌스로서 국토안보부를 설정하고 있다. 넷째, 국토안보부 소속으로 '권한 및 절차'(Capability and Process)라는 정교한 정보공유절차를 마련함으로써 정보공유가 신속하고 효과적으로 이루어질 수 있도록 하고 있다. 이는 앞으로 우리가 독자적인 정보공유 시스템을 마련해 운영하는 데 중요한 참고가 될 것이다.

5. 정보공유 프로그램

마지막으로 미국은 독자적이고 전문적인 정보공유 프로그램을 개발해 자동적이고 즉각적으로 정보공유가 이루어질 수 있도록 하고 있다. 말하자면, 정보공유에서도 '기술적·물리적 규제'(architectural regulation)를 사용하고 있는 것이다.[82] AIS, STIX, TAXII가 그런 예에 해당한다. 우리 역시 이 같은 정보공유 프로그램을 개발해 운영하는 것이 필요하다. 물론 당연히 이에 관한 법적 근거 역시 마련해야 한다.

82) '기술적·물리적 규제'에 관해서는 심우민, "정보통신법제의 최근 동향: 정부의 규제 개선방안과 제19대 국회 전반기 법률안 중심으로", 『언론과 법』 제13권 제1호, 2014; Lee Tein, *Architectural Regulation and the Evolution of Social Norms*, Yale Journal of Law and Technology 7 (1) (2005) 등 참고.

참고문헌

박노형, “미국의 사이버안전에 관한 법 제정 동향과 시사점”, 『법제연구』 제46호, 한국법제연구원, 2014.

박상돈·김인중, “한국과 미국의 사이버보안 단계별 법제도 비교 연구”, 『융합보안 논문집』 제12권 제4호, 한국융합보안학회, 2012.

박주석·문승일·송기민, “정보보호산업법상 정보보호산업 분쟁조정의 개선과제”, 『보안공학연구논문지』 제14권 제4호, 보안공학연구지원센터, 2017.

심우민, “정보통신법제의 최근 동향: 정부의 규제 개선방안과 제19대 국회 전반기 법률안 중심으로”, 『언론과 법』 제13권 제1호, 2014.

육소영, “사이버보안법의 제정 필요성에 관한 연구: 미국법과의 비교를 중심으로”, 『공법학연구』 제11권 제2호, 한국비교공법학회, 2010.

양천수, 제4차 산업혁명과 법, 박영사, 2017.

양천수, “정보통신망법 해석에 관한 몇 가지 쟁점”, 『과학기술과 법』 제8권 제1호, 충북대 법학연구소, 2017.

양천수, “제4차 산업혁명과 정보보호 법정책의 방향”, 『공법학연구』 제18권 제4호, 한국비교공법학회, 2017.

이상현, “미국의 사이버보안 법제: 입법부, 사법부, 행정부의 대응을 중심으로”, 『Internet & information security』 제3권 제1호, 한국인터넷진흥원, 2012.

정필운, “사이버보안이란 개념 사용의 유용성 및 한계”, 『연세 의료·과학기술과 법』 제2권 제2호, 연세대 법학연구원, 2011.

한국인터넷진흥원 (편), 사이버보안체계 강화를 위한 정보보호법제 비교법연구, 한국인터넷진흥원, 2015.

홍종현, “정보통신기반보호법제의 개선방안 연구”, 『법연』 제46호, 한국법제연구원, 2015.

Jamil N. Jaffer, Carrots and Sticks In Cyberspace: Addressing Key Issues in the Cybersecurity Information Sharing Act of 2015, 67 S.C.L.Rev., 2016.

Lee Tein, Architectural Regulation and the Evolution of Social Norms, Yale Journal of Law and Technology 7 (1), 2005.

Lawrence J. Trautman, CYBERSECURITY: WHAT ABOUT U.S. POLICY?, 2015 U. Ill. J.L. Tech. & Pol'y, 2015.

The Department of Homeland Security & The Department of Justice, PRIVACY AND CIVIL LIBERTIES FINAL GUIDELINES: CYBERSECURITY INFORMATION SHARING ACT OF 2015, June 15, 2016.

The Department of Homeland Security & The Department of Justice, GUIDANCE TO ASSIST NON-FEDERAL ENTITIES TO SHARE CYBER THREAT INDICATORS AND DEFENSIVE MEASURES WITH FEDERAL ENTITIES UNDER THE CYBERSECURITY INFORMATION SHARING ACT OF 2015, June 15, 2016.

The Office of the Director of National Intelligence & The Department of Homeland Security & The Department of Defense & The Department of Justice, SHARING OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY THE FEDERAL GOVERNMENT UNDER THE CYBERSECURITY INFORMATION SHARING ACT OF 2015, February 16, 2016.

The Department of Homeland Security & The Department of Justice, FINAL PROCEDURES RELATED TO THE RECEIPT OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY THE FEDERAL GOVERNMENT, June 15, 2016.

<국문초록>

오늘날 ‘제4차 산업혁명’을 통해 ‘초연결사회’가 구현되면서 새로운 사회적 공리와 더불어 위험 역시 증대하고 있다. 무엇보다도 은밀한 개인정보를 포괄하는 정보에 대한 침해의 위험이 비약적으로 증대하고 있다. 초연결사회가 실현되면서, 사물인터넷 기기 한 개만 해킹되어도 그 파급효과가 초연결망 전체로 확산되는 위험이 등장하고 있는 것이다. 이에 따라 사이버보안을 포괄하는 정보보호의 필요성과 중요성이 증대하고 있다. 사이버 공간, 인터넷 공간의 안정성이 부각되고 있는 것이다. 이에 정부는 초연결사회의 정보침해 문제에 대응할 수 있는 정보보호 관련 법체계 구축을 모색하고 있다. 그러나 그 방향성을 어떻게 설정해야 할지에 관해서는 여전히 고민을 하고 있는 것으로 보인다. 이러한 상황에서 해외 선진국의 법적 상황을 살펴보는 비교법적 검토는 우리가 정보보호 관련 법정책을 어떻게 펼쳐야 하는지에 관해 의미 있는 시사점을 제공할 것이다. 특히 사이버보안을 침해하는 행위에 대해 적극적인 대응입법을 하고 있는 미국의 법제는 우리가 참고할 만한 가치를 지니고 있다. 이러한 이유에서 이 글은 미국 사이버보안법의 최근 현황을 체계적으로 분석한다. 특히 미국이 최근 제정한 「사이버보안 정보공유법」을 집중적으로 분석한다. 「사이버보안 정보공유법」은 국가기관과 민간기관 사이의 정보공유에 관해 체계적이고 상세하게 규정한다. 정보공유야말로 현대 초연결사회에서 정보보호를 적절하게 실현할 수 있는 효과적인 방안이라는 점에서 정보공유를 적극 장려하는 미국의 「사이버보안 정보공유법」은 우리에게 시사하는 바가 적지 않다. 우리는 아직 독자적인 정보공유법을 갖추고 있지 않기 때문이다.

주제어 : 미국의 사이버보안법, 사이버보안 정보공유법, 정보보호, 사이버보안, 정보공유, 사이버위협 지표, 방어조치

Current Trends in the U.S. Cybersecurity Laws

Yang, Chun-Soo*·Jee, Yu-Mi**

As the 'hyper-connected society' has emerged through the 'Fourth Industrial Revolution, public interests as well as social dangers have increased. Above all, the risk of infringement of information, including confidential personal information, is dramatically increasing. As the hyper-connected society has been realized, even if only one of the internet devices is hacked, there would be a danger that the ripple effect of such a hacking spreads to the whole network. Therefore, the necessity and importance of information security, including cybersecurity, has been increasing. In other words, the stability of cyberspace and internet space is becoming more important. As a result, the Korean government is seeking to build a legal system related to information security, which would be able to cope with the information infringement problem in the hyper-connected society. However, it seems that the government is still struggling with the direction of building such a legal system. In this context, a comparative review examining the legal systems of advanced foreign countries will provide meaningful implications as to what kinds of legal policies we should devise and implement for information security. In particular, the U.S. legislative act that actively responds to the cybersecurity violations is worthy of reference. For this reason, this article systematically analyzes the current status of the U.S. cybersecurity laws. Especially, this article focuses on the "Cybersecurity Information Sharing Act of 2015"(hereinafter "CISA"), that was recently enacted by the U.S. congress. The CISA prescribes the systemic and detailed information-sharing between national and private entities. The CISA, that actively promotes information-sharing, is full of suggestions for us, in that information-sharing is an effective way to properly realize information security in today's hyper-connected society.

* Professor at Yeungnam University Law School, Dr. jur.
** Assistant Professor, Division of Law, Daegu University, Ph. D.

Key Words : U.S. cybersecurity laws, Cybersecurity Information Sharing Act of 2015, information security, cybersecurity, information-sharing, cyber threat indicators, defensive measures