미국 사이버안보 정보공유법(CISA)의 규범적 의의

박 상 돈*

요 약

2015년 12월부터 미국에서 시행된 사이버안보 정보공유법(Cybersecurity Information Sharing Act of 2015)은 미국의 사이버안보 입법 활동이 맺은 가장 큰 결실 중 하나이다. 정보공유의 활성화는 한국의 사이버안보 추진체계 개선과제 중 하나로서 향후 한국의 사이버안보 법제도 개선에서 중요하게 다루어야 할 사항이며, 사이버안보법 정보공유법의 연구로부터 많은 시사점을 도출할 수 있다. 그럼에도 불구하고 사이버안보 정보공유법의 내용을 구체적으로 다루면서 그 규범적 의미를 확인하는 국내의 선행연구를 찾기 어렵다. 따라서 용어 정의, 정보공유 절차 수립 및 여건 마련, 민간의 자발적 정보공유 촉진, 행정부에 대한 견제 및 의회 보고, 기타 사항이라는 다섯 가지 범주별로 사이버안보 정보공유법의 내용을 확인하고 규범적 의미와 시사점을 모색하고자 하였다. 사이버안보 정보공유법은 자율성에 기초한 정보공유를 활성화하는 동시에 정보공유 과정에서 초래될 수 있는 부작용을 제거하는 장치를 마련하고 있다. 향후 한국의 사이버안보 법제도 정비에서 사이버안보 정보공유법의 규범적 의미와 시사점을 적절히 활용하는 것이 필요하다.

The Normative Meaning of Cybersecurity Information Sharing Act(CISA) of 2015

Sangdon Park*

ABSTRACT

The Cybersecurity Information Sharing Act(CISA) of 2015, enacted in December 2015, is one of the greatest achievements of cybersecurity legislation in the United States. The promotion of cybersecurity information sharing is one of the tasks to improve cybersecurity governance in Korea. So it is an important issue to be addressed in cybersecurity legislation in Korea in the near future. CISA has many implications for cybersecurity legislation in Korea. Nevertheless, it is difficult to find preceding research that explain the content of CISA and study its normative meaning in Korea. Therefore, in this paper, the contents of the CISA is identified and its normative meaning and implication is found in five categories: definition of terms, establishment of information sharing procedures and conditions, promotion of voluntary information sharing by the private sector, checks on the executive branch and report to the Congress, and other matters. CISA facilitates information sharing based on willingness, while eliminating the side effects that may arise in the information sharing process. It is necessary to appropriately apply the good points of CISA to the cybersecurity legal system in Korea.

Key words : Information Sharing, Cybersecurity Act, CISA, DNI, DHS

접수일(2017년 3월 4일), 게재확정일(2014년 3월 21일)

* 국가보안기술연구소(NSR)

1. 서 론

기존의 선행연구에서[1][2][3] 나타나는 주장들을 살펴보면, 한국에서 사이버공간의 안전을 보장하기 위한 법제도 정비의 필요성에 대한 공감대는 이미 형성되어 있는 상태이며[4], 정보공유 체계의 정립 및 활성화는 한국의 사이버안보 추진체계 개선과제 중 하나로서 중요한 사항이다[5]. 따라서 한국의 사이버안보 법제도 개선에서도 정보공유에 관한 사항을 다루어야 할 필요성이 크다. 그러한 점에서 CISA라는 약칭으로 잘 알려진 미국의 사이버안보 정보공유법(Cybersecurity Information Sharing Act(CISA) of 2015)은 많은 참고가 될 수 있을 것이다. 그럼에도 불구하고 현재 시행중인 사이버안보 정보공유법의 내용을 구체적으로 다루면서 규범적 의미와 시사점을 검토하는 국내의 선행연구는 의외로 찾아보기 어렵다. 사이버안보 정보공유법의 내용이 최종적으로 확정되어 시행되기 시작한 2015년 12월 이후의 관련 선행연구들은[6][7] 연구주제를 사이버안보 정보공유법에만 초점을 맞추지 않고 개요 수준의 간단한 언급에 그치기 때문에 사이버안보 정보공유법에 대한 본격적인 연구로 보기에는 한계가 있다.

사이버안보 정보공유법은 미국 의회에 계류되었던 사이버안보 관련 주요 법안들을 2016년도 통합세출예산법 통과과정에서 일괄 처리한 사이버안보법(Cybersecurity Act of 2015)의 일부로서 2015년 12월에 의회에서 통과되고 시행되기 시작하였다. 사이버안보법에 포함된 사이버안보 관련 법안들은 여러 가지가 있으나 그 중에서도 사이버안보 정보공유법이 가장 핵심적인 요소라고 할 수 있다. 사이버안보 정보공유법은 총 11개의 세션으로 구성되어 있다. 그 중에서 제목에 관한 섹션(sec. 101)을 제외한 용어 정의(sec. 102), 연방정부에 의한 정보공유(sec. 103), 사이버안보위협 예방·탐지·분석·완화를 위한 권한 부여(sec. 104), 연방정부에 대한 사이버위협지표 및 방어적 조치 공유(sec. 105), 법적 책임으로부터의 보호(sec. 106), 정부 활동 감독(sec. 107), 해석 및 선취(sec. 108), 사이버안보위협 보고(sec. 109), 국방 비밀의 전파에 대한 제한의 예외(sec. 110), 유효기간(sec. 111) 등의 섹션들을 대상으로 하여 내용에 따른 체계적 분류를 시도하면 용어 정의, 정보공유 절차 수립 및 여건 마련, 민간의 자발적 정보공유 촉진, 행정부에 대한 건제 및 의회 보고, 기타 사항이라는 다섯 가지 범주로 묶을 수 있다. 이하에서는 상기한 다섯 가지 범주별로 사이버안보 정보공유법의 내용을 확인하고 규범적 의미와 시사점을 검토하고자 한다.

2. 용어 정의

2.1 주요 내용

사이버안보 정보공유법은 여러 가지 용어들의 정의를 명시하고 있으며, 그 중에서 특히 중요한 용어들의 정의는 다음과 같다.

적정 연방 주체(appropriate federal entities)란 상무부, 국방부, 에너지부, 국토안보부, 법무부, 재무부, 국가정보국을 의미한다. 사이버안보 목적(cybersecurity purpose)이란 사이버안보 위협 및 보안취약성으로부터 정보시스템 또는 정보를 보호하는 목적을 의미한다(6 U.S.C. §1501(4)). 사이버안보 위협(cybersecurity threat)이란 정보시스템 또는 정보의 보안, 가용성, 기밀성, 완전성에 악영향을 미치는 시도를 야기하면서 정보시스템상에서 이루어지거나 정보시스템을 이용하는 행위를 의미한다(6 U.S.C. §1501(5)).

사이버위협지표(cyber threat indicator)란 사이버안보 위협 또는 보안취약성 관련 기술 정보를 수집하기 위하여 전송되는 변칙적 통신패턴을 포함한 악의적 정찰, 보안통제 및 보안취약성 확인을 무력화하는 방법, 보안취약성의 존재를 표시하는 변칙적 활동을 비롯한 보안취약성, 정보시스템 또는 정보에 대한 합법적 사용자를 이용하여 해당 사용자가 알지 못하는 사이에 보안 통제를 무력화하거나 보안취약성을 악용하는 방법, 악의적 사이버 명령 및 통제, 사고에 의하여 야기되는 실제적·잠재적 피해, 그 밖에 사이버안보 위협의 기타 징후로서 법률상 공개가 금지된 바 없는 사항, 상기 사항들의 조합을 설명하거나 식별하는데 필요한 정보를 의미한다(6 U.S.C. §1501(6)). 방어적 조치(defensive measure)란 알려져 있거나 의심이 드는 사이버안보 위협 또는 보안취약성을 탐지·예방·완화하기 위하여 정보시스템 또는 그러한 정보시스템에 저장·소유되거나 정보시스템을 경유하는 정보에 적용되는 활동, 기기, 절차, 서명, 기술 및 기타 조치를 의미한다(6 U.

S.C. §1501(7)). 보안취약성(security vulnerability)이란 보안통제 무력화를 야기할 수 있는 하드웨어, 소프트웨어, 프로세스 및 절차의 속성을 의미한다(6 U.S.C. §1501(17)).

2.2 의미 및 시사점

사이버안보 정보공유법은 주목할 만한 여러 가지 용어들의 정의를 제시하고 있다. 특히 사이버위협지표의 구체적인 내용을 열거한 것은 향후 한국의 관련 법제도 정비에 많은 참고가 될 수 있을 것이다. 그러한 세부적인 열거에도 불구하고 '그 밖에 사이버안보 위협의 기타 징후'라는 유형을 별도로 명시한 것은 시시각각 변화하는 사이버안보 위협 환경에 대비하기 위하여 불가피하게 정한 것으로 보인다. 그러한 점을 고려하면 향후 한국의 관련 법제도에서 유사한 표현이 있는 경우에 명확성이 없다는 이유로 해당 조항을 배척하는 것은 신중할 필요가 없지 않다.

3. 정보공유 절차 수립 및 여건 마련

3.1 주요 내용

3.1.1 연방정부에 의한 정보공유

국가정보국, 국토안보부, 국방부, 법무부는 연방정부가 보유한 정보들을 대상으로 하는 다음의 정보공유 사항에 관한 절차를 적정 연방 주체와 협의하여 공동으로 마련하여야 한다. 첫째, 기밀로 분류된 사이버위협지표와 방어적 조치(defensive measure)를 관련 연방 주체와 비연방 주체와 공유하는 것을 촉진하는 절차이다.

이 경우 정보공유 대상 주체들은 비밀취급인가를 지녀야 한다(6 U.S.C. §1502(a)(1)). 둘째, 기밀 취급이 해제된 사이버위협지표와 방어적 조치 및 사이버위협 관련 정보를 관련 연방 주체 및 비연방 주체와 공유하고 그러한 주체들이 해당 정보들을 정당하게 사용하는 것을 촉진하는 절차이다(6 U.S.C. §1502(a)(2)). 셋째. 기밀에 해당하지 않는 사이버위협지표와 방어적 조치를 공개적으로 공유하는 절차이다((6 U.S.C. §1502(a)(3)). 넷째, 사이버안보 위협으로 인한 악영향을 예방·완화하는 것에 관한 정보를 공유하는 절차이다(6 U.S.C. §1502(a)(4)). 다섯째, 소규모 기업이 직면하는 도전에 주의를 기울이는 취지에서 사이버안보 모범사례를 공유하는 것을 촉진하는 절차이다(6 U.S.C. §1502(a)(5)). 마련된 상기 절차들은 국가정보국이 의회에 제출한다(6 U.S.C. §1502(c)).

3.1.2 연방정부에 대한 사이버위협지표 및 방어적 조치 공유

법무부와 국토안보부는 연방정부가 사이버위협지표 및 방어조치를 수령하는 것에 관한 절차를 적정 연방 주체와 협의하여 수립하여야 한다. 해당 절차는 자동화된 실시간 공유절차, 역량 감사, 권한없는 행위를 한 연방 정부의 공무원과 고용인 및 대리인에게 적용되는 적절한 제재를 포함하여야 한다. 또한 법무부와 국토안보부는 연방정부와의 지표 공유를 수행하는 주체들이 참고하는 가이드라인을 개발하여야 한다. 해당 가이드라인은 사이버안보위협과 직접적으로 관련이 없는 개인정보가 포함될 개연성이 낮은 사이버 위협 지표를 식별하는 방법을 포함한다(6 U.S.C. §1504(a)).

법무부와 국토안보부는 개인정보의 수령·보유·사용·전파를 제한하기 위한 목적으로 프라이버시 및 시민 자유 가이드라인을 마련하고 최소한 2년 이내의 주기로 재검토하여야 한다. 해당 가이드라인은 기밀 및 기타 민감한 국가안보정보를 보호하는 것을 고려하는 사이버위협지표 전파 단계를 포함하여야 한다(6 U.S.C. §1504(b)).

국토안보부는 국방부, 법무부, 국가정보국, 상무부, 에너지부, 재무부 등 다른 적정 연방 주체와 협력하여 국토안보부 내부의 두 가지 프로세스를 개발한다. 첫째, 국토안보부가 어느 비연방 주체로부터라도 실시간으로 사이버위협지표와 방어적 조치를 수령하는 프로세스이다. 둘째. 공유된 지표 및 방어적 조치를 자동화된 방법을 통하여 적정 연방 주체가 실시간으로 수령하는 것을 보장하는 프로세스이다. 상기 프로세스는 비연방주체가 이메일 또는 전자매체, 인터넷 웹사이트, 정보시스템간의 자동화된 실시간 수단을 통하여 연방정부와 공유하는 위협지표 및 방어적 조치를 수신하는 것이어야 한다. 다만 사전에 공유되고 유의미한 사이버위협을 묘사하는 사이버위협지표, 또는 그러한 지표

에 기초한 방어적 조치의 개발에 관한 연방 주체와 비연방주체 간 통신, 사이버위협에 관하여 연방규제기관과 피규제기관 간 통신은 예외이다. 상기 프로세스는 통신, 기록, 기타 정보의 합법적인 공개를 제한하거나 금지하지 않는다. 그러한 정보에는 알려지거나 혐의가 있는 범죄행위 보고, 자발적으로 또는 법적으로 강제되는 연방 수사 참여, 법에 명시되거나 승인된 계약사항의 일부로서 이행되는 사이버위협지표 및 방어적 조치의 제공이 포함된다(6 U.S.C. §1504(c)(1)).

법 시행일(2015년 12월 18일)로부터 90일 이내에 국토안보부는 의회에 국토안보부의 정보공유 역량이 완전히 운용되는지 여부에 대한 검증결과를 제출하여야 한다. 국토안보부의 검증결과 제출 이후에 대통령은 상무부, 에너지부, 법무부, 재무부, 국가정보국이 국토안보부의 정보공유 역량 및 프로세스 외에 추가적으로 정보공유 역량 및 프로세스를 개발하도록 지시할 수 있다. 지시 이후에 대통령은 해당 지시의 필요성에 관한 검증결과 및 설명을 의회에 제출하여야 한다(6 U.S.C. §1504(c)(2)). 국토안보부는 국토안보부의 정보공유 프로세스를 일반에 공표하고 공표된 프로세스에 접근할 수 있도록 보증하여야 한다(6 U.S.C. §1504(c)(3)).

연방정부와 공유하는 사이버위협지표 및 방어적 조치, 주정부 및 지역정부와 공유하는 사이버위협지표는 자발적으로 공유가 이루어지며, 일반인에게 공개되거나 제공되지 않는다(6 U.S.C. §1504(d)(3)).

정부에 제공된 사이버위협지표와 방어적 조치는 다음의 목적만을 위하여 연방기관 및 연방공무원에게 공개되고, 이들이 보유·사용할 수 있다. 첫째, 정보시스템, 정보시스템에 저장·소유되거나 정보시스템을 경유하는 정보를 사이버위협지표 및 보안취약성으로부터 보호하기 위한 경우이다. 둘째, 사이버위협지표 및 보안취약성을 식별하기 위한 경우이다. 셋째, 테러리스트의 활동이나 대량살상무기의 사용과 같이 사망 또는 심각한 신체적·경제적 위험을 유발하는 주요 위협을 대응하거나 예방·완화하기 위한 경우이다. 넷째, 성적 학대나 물리적 안전에 대한 위협과 같이 미성년자에 대한 심각한 위협을 대응·수사·기소하거나 예방·완화하기 위한 경우이다. 다섯째, 사망 또는 심각한 신체적·경제적 위험을 유발하는 공격 또는 사기 및 명의도용, 간첩행위 및 검열, 거래비밀에 관한 공격을 예방·수사·중지·기소하기 위한 경우이다. 정부기관은 합법적 활동을 수행하거나 법적 표준을 준수하는 비연방주체에 대한 규제에 공유된 사이버위협지표와 방어적 조치를 이용하여서는 아니된다(6 U.S.C. §1504(d)(5)).

3.2 의미 및 시사점

사이버안보 정보공유법에 의한 일차적인 요구사항이자 전체 내용을 한마디로 요약하는 표현은 정보공유 절차의 수립이다. 사이버안보 정보공유법에 의하면 국가정보국, 국토안보부 등 유관기관이 공동으로 각종 연방정부가 보유한 정보를 대상으로 하는 정보공유절차를 마련하고, 국가정보국이 의회에 제출하도록 하였다. 바꾸어 말하면 연방정부가 보유한 정보들을 공유하는 활동에서는 정보공동체를 대표하는 국가정보국이 중심적인 기능을 담당하면서 의회에 대하여 행정부를 대표한다는 의미를 내포한다.

이러한 점은 정보기관의 활동에 일정 수준의 비밀성이 있다는 점보다 정보공유의 본질이 정보를 다루는 업무이고 그러한 업무의 수행이 정보기관 본연의 기능이라는 점에 더욱 주목한 것으로 보인다. 이에 따라 국가정보국 등이 공동으로 연방정부에 의한 사이버위협지표 및 방어적 조치 공유에 관한 세부 사항을 마련하여 발표한 바 있다[8].

연방정부가 보유한 정보를 공유하는 절차의 수립에서는 정보공동체의 대표인 국가정보국이 중요한 역할을 담당하는 반면에 연방정부가 정보를 수령하는 절차의 수립에서는 국토안보부가 일차적으로 중요한 역할을 담당한다. 다만 이 경우에도 다른 적정 연방 주체와 협의가 필요하기 때문에 적정 연방 주체 중 하나인 국가정보국은 배제되지 않는다. 또한 국가정보국은 정보 수령 프로세스의 대상에도 포함되며, 정보공유 역량 및 프로세스를 개발할 수도 있도록 정하고 있다. 따라서 정보기관과 민간의 정보공유는 양방향으로 이루어질 수 있다. 그러한 정보공유는 개인정보보호를 비롯하여 국민의 권리 보호에 적절한 장치와 병행되는 것이 바람직하다. 따라서 사이버안보 정보공유법에서는 프라이버시 및 시민 자유 가이드라인을 수립하도록 정하고 있으며, 이에 따라 미국은 2016년 6월에 새로운 가이드라인을 발표하였다[9].

4. 민간의 자발적 정보공유 촉진

4.1 주요 내용

4.1.1 사이버안보위협 예방·탐지·분석·완화를 위한 권한 부여

민간 주체들은 사이버안보 목적으로 자신이 보유한 정보시스템을 모니터링할 수 있으며, 법적으로 승인되거나 서면동의가 있으면 다른 민간 주체 또는 정부의 정보시스템을 모니터링할 수 있다(6 U.S.C. §1503(a)). 또한 민간 주체들은 사이버안보 목적으로 자신이 보유한 정보시스템에 대한 방어적 조치를 취할 수 있으며, 법적으로 승인되거나 서면동의가 있으면 다른 민간 주체 또는 정부의 정보시스템에 대한 방어적 조치를 취할 수 있다(6 U.S.C. §1503(b)).

비연방 주체들은 사이버안보 목적으로 다른 주체들이나 연방정부와 사이버위협 지표 및 방어적 조치들을 공유할 수 있다. 정보의 수령자는 공유된 사이버위협 지표와 방어적 조치를 공유하고 사용함에 있어서 법적 제한사항들을 준수하여야 한다(6 U.S.C. §1503(c)).

모니터링, 방어적 조치, 지표 공유를 수행하는 주체들과 연방정부는 권한없는 접근 및 취득으로부터 보호하기 위한 보안 통제를 활용하여야 하며, 개인정보 및 특정인을 식별할 수 있는 정보와 같이 사이버안보위협 지표와 직접적으로 관련되지 않는 정보를 제거하여야 한다(6 U.S.C. §1503(d)).

민간 주체들이 사이버안보 목적에서 사이버위협지표나 방어적 조치를 교환하거나 제공하는 행위는 반독점법의 적용에서 제외된다. 또한 민간 주체들이 사이버안보 목적에서 사이버위협 예방, 조사, 완화에 관하여 조언을 교환하거나 제공하는 행위도 반독점법의 적용이 배제된다. 상기한 바와 같은 반독점법 적용 배제는 경쟁기업간 가격담함 미 할당, 독점 및 독점 시도, 보이콧, 가격정보·고객목록·기타 미래 경쟁계획 관련 정보 교환 등에는 적용되지 않는다(6 U.S.C. §1503(e)).

4.1.2 법적 책임으로부터의 보호

사이버안보 정보공유법에 정한 바에 따라 정보시스템을 모니터링한 민간 주체들은 법적 책임(liability)을 면한다(6 U.S.C. §1505(a)). 또한 사이버안보 정보공유법에 정한 바에 따라 또는 국토안보부의 정보공유 프로세스에 기초하여 발표된 명시적인 절차와 예외사항에 일치하는 바에 따라 연방정부와 사이버위협지표 또는 방어적 조치를 공유한 민간 주체들은 법적 책임을 면한다(6 U.S.C. §1505(b)).

사이버안보 정보공유법은 정보를 공유할 의무 또는 그러한 정보 수신에 기초하여 행동하거나 경고할 의무를 창설하는 것으로 해석되지 않는다(6 U.S.C. §1505(c)).

4.1.3 해석 및 선취(先取)

사이버안보 정보공유법에 따른 어떠한 내용도 연방 주체가 비연방 주체로 하여금 연방 주체 또는 다른 비연방 주체에게 정보를 제공하도록 요구하는 것이 허용된다고 해석되지 않으며(6 U.S.C. §1507(h)), 자발적 활동에 참여하지 않는 바에 대한 책임을 지운다고 해석되지 않는다(6 U.S.C. §1507(i)).

4.2 의미 및 시사점

정보공유에 관한 법률이 있다는 것이 무조건 정보를 공유할 의무를 지운다는 의미가 되지는 않으며, 그러한 취지는 사이버안보 정보공유법 중 해석 및 선취에 관한 내용에서 잘 나타난다. 즉 사이버안보 정보공유법을 근거로 하여 강제로 정보를 제공하도록 요구할 수는 없으며, 정보공유는 자발적인 정보 제공에 기초하여야 한다는 의미로 보아야 한다, 이러한 점에서 자발적인 정보공유가 이루어질 수 있는 여건의 마련이 필수적으로 요구된다.

사이버안보 정보공유법은 민간 주체들이 스스로 자신의 정보시스템을 모니터링할 수 있고, 일정한 요건을 충족한 경우에는 다른 주체들의 정보시스템도 모니터링할 수 있게 하였다. 이는 각 민간 주체들이 스스로를 지키는데 필요한 탐지활동을 할 수 있는 법적 근거를 제공한다는 의미가 있다. 특히 자신의 소유가 아닌 정보시스템에 대한 모니터링이 허용되는 길을 열어놓았다는 점에서 특이점이 있다. 그와 동시에 개인정보의 보호 등에 필요한 사항들을 준수하도록 하여 권리 침해를 방지함으로써 정보공유를 꺼리지 않도록 하는 장치도 마련하고 있다.

사이버안보법에서 정보시스템을 모니터링하거나 정

보를 공유한 민간 주체들에게 법적 면책을 부여하는 사항을 정하는 것은 기업 등 민간 주체의 적극적 참여를 촉진하고자 하는 의도라고 해석할 수 있다. 여기서 주목할 점은 모니터링이나 정보공유 과정에서 법률이 정한 바에 따르는 등으로 정당한 객관적 요건을 갖춘 경우에 한하여 면책이 적용된다는 것이다. 다시 말하자면 합법적인 범주의 행위이기 때문에 면책되는 것이며, 단지 선한 의도의 행위라는 이유만으로 면책되는 것이 아니다.

5. 행정부에 대한 견제 및 의회 보고

5.1 주요 내용

5.1.1 정부 활동 감독

적정 연방 주체는 의회에 본 법의 실행에 관한 보고서를 제출하여야 한다. 해당 보고서는 실시간 정보공유의 효용성 평가, 사이버위협지표 및 방어적 조치의 적절한 분류 여부 평가, 민간 부문과 사이버위협지표 및 방어적 조치를 공유하기 위하여 연방정부가 승인한 비밀취급인가 통계, 국토안보부 정보공유 프로세스를 통하여 수신된 사이버위협지표 및 방어적 조치의 수 및 수신자인 연방 주체의 목록 등을 포함한다(6 U.S.C. §1506(a)).

적정 연방 주체의 감사관은 행정부가 수행하는 본 법에 따른 사항의 이행에 관한 보고서를 의회에 2년마다 제출하여야 한다. 해당 보고서는 공유된 사이버위협지표 및 방어적 조치에 기초한 연방정부의 활동(해당 사이버위협지표 공유가 시기적절한 방법으로 이루어졌는지 여부, 공유 이후의 사용 및 전파의 적절성에 대한 평가 등을 포함), 특정인의 개인정보 또는 특정인이 식별되는 정보로서 사이버안보 위협과 직접적인 관련이 없는 정보에 대한 비연방주체와 연방정부 간 공유 여부에 대한 평가, 정부가 비공개·보유·사용하도록 승인된 정보에 대한 공격에 대한 연방정부의 기소에 활용된 공유 정보의 수 등을 다룬다(6 U.S.C. §1506(b)).

회계감사원은 연방정부가 사이버위협지표 및 방어적 조치에서 개인정보를 제거하는 활동에 관한 보고서를 법 시행일로부터 3년 이내에 의회에 제출하여야 한다(6 U.S.C. §1506(c)).

5.1.2 사이버안보 위협 보고

국가정보국은 의회에 사이버위협에 관한 보고서를 제출하여야 한다(6 U.S.C. §1508(a)). 해당 보고서는 미국과 다른 국가 간 미국의 국가안보·경제·지적재산권에 대한 사이버위협 관련 정보공유 및 협력관계 현황에 대한 평가, 주된 위협이 되는 국가 및 비국가행위자의 목록, 미국 정부의 대응 및 예방 역량, 정보공동체(intelligence community)에 즉시 도움이 될 수 있는 민간 부문 기술 등 미국의 역량을 강화시킬 수 있는 추가적인 기술에 대한 평가 등을 포함한다(6 U.S.C. §1508(b)).

5.2 의미 및 시사점

국토안보부, 국가정보국 등 유관부처·기관이 정보공유 관련 활동 내역을 밝히는 보고서를 의회에 제출하는 과정을 통하여 사이버안보 정보공유 활동의 투명성이 보장될 수 있는 장치가 마련된다. 특히 각 부처·기관의 감사관의 책임 하에 불필요한 개인정보 공유 여부에 대한 평가가 이루어지고 그 결과가 의회에 보고됨으로서 국민의 권리 보호에 많은 기여를 할 것으로 보인다.

국가정보국이 의회에 제출하는 사이버안보위협 보고서는 정보공유 활동의 내역을 밝히는 것이 아니라 공유된 정보를 바탕으로 도출되는 객관적 위협상황 그 자체를 대상으로 하여 전문가적 관점에서 정리하고 분석한 것이라고 할 수 있다. 이러한 보고서를 제출하고자 하면 위협상황에 대한 정보를 취합하는 허브 역할을 하는 동시에, 제반 정보를 종합적으로 분석하는 최종 책임을 정보기관이 담당하는 것이 요구된다. 결국 행정부 내부의 정보공유체계에서는 국가정보국을 대표로 하는 정보공동체가 정보의 최종적인 수령자 및 분석자의 기능을 담당한다는 의미를 내포한다. 한편 사이버안보위협이 의회에 보고되도록 하여 사이버안보 정보공유의 결과물이 행정부 내부에서 폐쇄적으로 활용되지 않고 국민이 선출한 대표인 의회도 활용할 수 있도록 함으로써 투명성 확보에 기여한다.

6. 기타 사항

6.1 주요 내용

6.1.1 국방 비밀의 전파에 대한 제한의 예외

국방부는 정보의 전파에 대한 군법상의 제한에도 불구하고 본 법에 의하여 사이버위협지표 및 방어적 조치의 공유가 허용된다(6 U.S.C. §1509).

6.1.2 유효기간

사이버안보 정보공유법에서 정하는 제반 사항의 유효기간은 2025년 9월 30일이나, 그 이전에 사이버안보 정보공유법에 의하여 승인된 활동 또는 그에 따라 획득된 정보에 대하여는 계속 유효하다(6 U.S.C. §1510).

6.2 의미 및 시사점

국방부에 적용되는 정보공유 허용 명시 규정은 민정 분야와 구분되는 군사 분야에 한정되는 군의 고유한 역할에도 불구하고 정보공유가 군에게도 열려있는 영역이라는 의미로 볼 수 있다. 그러한 입장은 정보공유 절차 수립에 국방부가 참여하는 것에서도 간접적으로 입증된 바가 있다. 다만 민간의 정보를 공유할 수 있다는 점과 평시에 민간에 대한 처분적 활동이 가능하다는 점이 동의어는 아니다.

한편 앞에서 살펴본 바와 같이 기본적으로 사이버안보 정보공유법은 정보공유 절차의 내용을 직접적으로 명시하는 것이 아니라 정보공유 절차를 수립할 것을 요구하면서 그에 수반되는 제반 사항들을 정하는 것으로 보아야 한다. 따라서 사이버안보 정보공유법이 정하는 사항은 본래 일종의 한시법이고, 기한에 맞추어 사이버안보 정보공유법이 정한 바를 준수하면서 정보공유절차를 수립하여야 하지만, 그 결과로서 시행된 정보공유절차와 그에 따라 다루어진 정보들은 유효기간에 구애받지 않고 유효하다고 할 수 있다.

7. 결 론

2009년 이래로 미국의 사이버안보 입법 활동의 주안점은 사이버공격행위에 대한 처벌 강화보다 피해의 발생과 확산을 최소화하기 위한 근본적인 추진체계 개선에 중점을 두었다[10]. 사이버안보 정보공유법의 통과와 시행은 최근 미국의 사이버안보 입법 활동이 맺은 가장 큰 결실 중 하나이다. 사이버안보 정보공유법은 자율성에 기초한 정보공유를 근간으로 하면서, 정보공동체를 대표하는 국가정보국이 사이버안보를 위한 정보공유에서 중요한 역할을 담당하게 하고 있음을 할 수 있다. 한편 민간의 정보시스템 모니터링과 정보공유를 활성화하는 여건을 마련하여 정보공유를 활성화하고, 정보공유 과정에서 초래될 수 있는 부작용을 제거하기 위한 장치도 마련하고 있다. 이러한 사이버안보 정보공유법의 의의는 한국의 사이버안보 법제도 정비에도 시사하는 바가 크다고 할 수 있다.

2017년에 미국의 정권교체가 발생하고 트럼프 행정부가 출범함에 따라 향후 미국의 사이버안보 정책 기조가 변화하고 관련 법제도가 변경될 가능성을 배제할 수는 없다. 그러나 실제적인 변화가 있기 이전에는 여전히 현행 법률이 적용되는 것이다. 만약 변화가 있더라도 현재 시행 중인 법제도 내용을 구체적으로 파악하고 분석한 결과가 없다면 향후 변화가 발생하는 경우에 새로운 변화의 의미를 찾아내기가 용이하지 않다. 따라서 근래 미국의 사이버안보 입법에서 주요한 변화 중 하나로서 현재 시행 중인 사이버안보법의 핵심요소인 사이버안보 정보공유법에 대한 연구는 여전히 유효하며, 특히 한국의 향후 입법에 대한 교훈을 찾아내고자 하는 의도에서는 더욱 그러하다. 이러한 연구를 통하여 한국의 정보공유 제도의 개선에 필요한 더욱 발전적인 성과로 향하는 가교가 만들어지는 것이다.

참고문헌

[1] 육소영, “사이버보안법의 제정 필요성에 관한 연구: 미국법과의 비교를 중심으로”, 공법학연구, 제11권 제2호, pp. 313-335, 2010.

[2] 정준현, “고도정보화사회의 국가사이버안보 법제에 관한 검토”, 법학논총, 제37권 제2호, pp. 441-473, 2013.

[3] 오길영, “사이버 ‘테러’ 대응체제의 문제점과

개선방향", 민주법학, 제54호, pp. 461-484, 2014.

[4] 박상돈, "종합적 사이버보안 법률 제정에 관한 시론적 연구: 미국의 입법동향을 중심으로", 입법과 정책, 제6권 제2호, pp. 5-36, 2014.

[5] 박상돈·김인중, "사이버안보 추진체계의 제도적 개선과제 연구", 융합보안 논문지, 제13권, 제4호, pp. 3-10, 2013.

[6] 조정은, "사이버테러 대응법제에 관한 연구", 토지공법연구, 제74집, pp. 295-315, 2016.

[7] 윤오준·조창섭·박정근·서형준·신용태, "사이버위협정보 공유 활성화를 위한 관리적·기술적 개선모델 연구", 융합보안 논문지, 제16권, 제4호, pp. 25-34, 2016.

[8] 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, 2016.

[9] The Department of Homeland Security, The Department of Justice, Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015, 2016.

[10] 박상돈, 박현동, 홍순좌, "미국 사이버보안 입법의 신경향 연구", 정보·보안 논문지, 제11권, 제4호, pp. 19-29, 2011.

[저 자 소 개]

박 상 돈 (Sangdon Park)
2002년 성균관대학교 법학사
2004년 성균관대학교 법학석사
2016년 성균관대학교 법학박사
현재 국가보안기술연구소(NSR) 선임연구원
email : sdpark@nsr.re.kr