2024.07.29

KIRI 리포트 | 이슈 분석 |

한미 사이버 사고 정보 공유 환경 비교 및 시사점

최창희 연구위원

요 약

미국 정부는 2015년부터 CISA법을 제정하여 연방정부가 사이버 사고 정보를 수집하고, 이를 민간에 공유하여 왔음. 미국 보험회사들은 연방정부와 사이버 사고 정보를 공유하며 이를 사이버 리스크관리에 활용하여 왔음. 우리나라에도 정부와 민간이 사이버 사고 정보를 공유하고 있으나 제도적 제약으로 활용도가 낮음. 사이버 리스크관리 강화와 사이버보험의 역할 제고를 위하여 일원화된 정보 수집·공유 체계 확립 등 민·관 사이버 사고 정보 수집·공유 관련 제도개선이 필요함

○ 미국 정부는 사이버 리스크관리 강화를 위하여 2015년부터 사이버 정보 공유법을 제정하고 사이버 사고 관련 정보를 수집하고 이를 민간에 공유하여 왔음

- 2012년 국가 보호 및 프로그램 이사회가 진행한 사이버보험 워크숍(이하 'NPPD(2012)'[1]) 참가자들은 연방정부가 사이버 사고 데이터 수집 및 공유에 주도적 역할을 수행해줄 것을 요청하였음
- 2015년 미국 정부는 사이버 정보 공유법(CISA법)을 제정하여 적정(Appropriate) 연방정부 부처가 사이버 사고 정보를 수집·공유하도록 하였음[2]
  - CISA법은 정보 공유 주체들을 개인정보유출 손해배상책임으로부터 보호하여 적극적인 정보 공유를 유도함[3]
  - CISA법에 따르면 연방정부는 개인의 사생활 보호 가이드라인에 따라 정보를 공유하여야 함[4]
- 특히 최근에는 주요 인프라에 대한 사이버 리스크관리 강화를 위하여 사이버 사고 보고를 의무화하는 CIRCIA를 도입하여 연방정부의 사이버 사고 정보 수집 권한을 더욱 강화하였음[5]
  - 미국 정부는 기존 제도의 복잡하고 중복된 사이버 사고 보고 체계와 민감 개인정보 유출 우려로 인한 보고 누락 등의 문제를 해결하기 위하여 CIRCIA법을 도입하였음[6]
- NCCIC와 CITTC는 각각 역할과 범위를 구분하여 사이버 사고 정보의 집적하고 공유함[7]

1) 국가 보호 및 프로그램 이사회(National Protection and Programs Directorate; NPPD); NPPD(2012), "Insurance Industry Working Session Readout Report", p. 15
2) 사이버 정보 공유법(Cybersecurity Information Sharing Act of 2015; CISA), 사이버보안 및 인프라보안국(Cybersecurity and Infrastructure Security Agency; CISA)과 구분하기 위하여 CISA법이라 함; CISA법, Sec. 102 참조함
3) CISA법, Sec. 106 참조함
4) CISA법, Sec. 105의 (b) 참조함
5) 중요기반시설의 사이버 사고 보고법(Cyber Incident Reporting for Critical Infrastructure Act; CIRCIA); Congressional Research Service(2024), "CIRCIA: Notice of Proposed Rule Making: In Brief", p. 4
6) Homeland Security(2023), "Harmonization of Cyber Incident Reporting to the Federal Government," p. 7
7) 김지선(2015), 「한국과 미국의 사이버위협정보 공유 입법안 비교 연구」, 고려대학교 대학원, 사이버국방학과, 석사논문, p. 62

- CISA 산하 NCCIC(National Cybersecurity and Communications Integration Center)는 연방정부와 민간의 사이버 사고 정보를 취급함
- CTIIC(Cyber Threat Intelligence Integration Center)는 정보기관의 사이버 위협 정보를 취급함

○ **미국 보험회사들은 금융 서비스 부문 정보 공유 및 분석 센터(FS-ISAC)를 설립하여 연방정부와 사이버 사고 정보를 공유하고 있음**

- CISA법은 연방정부가 허가받은 민간 대표 기관과 사이버 사고 관련 정보를 공유하는 것을 허용함[8)]
- 이에 여러 분야의 기업들이 정보 공유 및 분석 센터(Information Sharing and Analysis Centers; ISAC)를 설립하여 미국 정부로부터 사이버 사고 정보를 공유받고 있음
  - 화학, 자동차, 항공, 통신, 천연가스, 전기, 투표관리, 응급서비스, 금융 및 보험, 농업, 건강, IT, 해운, 대중매체, 국방, 에너지, 부동산, 교육 및 연구, 소매업, 우주, 교통, 수자원 등의 업체들이 ISAC을 설립하였음
- 보험회사들은 금융서비스 부문 정보 공유 및 분석 센터(Financial Services ISAC; FS-ISAC)를 통하여 미국 정부로부터 사이버 사고 관련 정보를 공유받아 이를 활용하고 있음

○ **우리나라는 국가사이버안전센터(NCSC), 사이버 위협정보 분석·공유 시스템(C-TAS System), 정보 공유·분석센터(ISAC) 등이 사이버 사고 정보를 수집·공유하고 있으며 여러 부처가 각각 사이버안전센터를 운영함**

- 국가정보원은 「국가사이버안전관리규정」 제14조에 의거하여 정부 및 공공기관의 사이버보안 업무를 총괄하는 국가사이버안전센터(National Cyber Security Center; NCSC)를 운영하고 있음
- 한국인터넷진흥원은 「정보통신망법」 제48조 2항에 의거하여 사이버 침해사고 정보를 수집하고 공유하는 사이버 위협정보 분석·공유 시스템(Cyber Threat Analysis and Sharing System; C-TAS)을 운영하고 있음
- 「정보통신기반 보호법」 제9조는 정보통신기반시설의 사이버 리스크관리를 위한 정보 공유·분석 센터(ISAC)의 운영에 관한 내용을 정하고 있음[9)]
  - 현재 정보통신, 금융, 행정 등 부분에서 ISAC이 운영되고 있음
- 우리나라의 경우 여러 부처(기획재정부, 과학기술정보통신부, 교육부, 외교부, 통일부, 법무부, 국방부, 행정안전부, 문화체육관광부, 방송통신위원회, 방위사업청, 경찰청, 환경부 외 다수)가 각각 사이버안전센터를 운영하고 있음[10)]

○ **우리나라의 사이버 사고 정보 공유 체계와 관련하여 일원화된 정보 수집·공유 체계의 부재, 참여자에 대한 개인정보보호 관련 법적 책임 감경 조항 부재, 낮은 활용률 등의 문제점이 제기되었음**

- 우리나라의 경우 구속력을 가지는 일원화된 사이버 사고 정보 수집·공유 체계가 없어 사이버 사고 정보 수집이 제한적이고 업종 간 사이버 사고 정보의 공유가 활발하지 않음[11)]

---

8) CISA법, Sec. 103 참조함
9) 김동희·박상돈·김소정·윤오준(2017), 「사이버 위협정보 공유체계 구축방안에 관한 연구」, 『융합보안 논문지』, 17(2), pp. 53~68
10) 김희연(2015), 「한중일 침해사고 대응체계 비교에 관한 연구」, 『정보과학회지』, 25(2), pp. 43~57

- CISA법이 사이버 사고 정보 공유에 참여하는 기관을 개인정보보호 관련 법적 책임으로부터 보호하여 주는 반면, 우리나라의 경우 그러한 조항이 없어 기관들이 참여에 소극적임[12)]
- 우리나라의 경우 국내외 사이버 위협 인텔리전스 서비스를 이용한 정보 공유가 저조함[13)]
  - 한국침해사고대응팀협의회 회원 73개 사 중 55%가 C-TAS를 이용하고, 국내·해외 사이버 위협 인텔리전스 서비스를 사용하는 비중은 각각 30.14%와 16.44%였음

○ **지금까지 사이버 리스크관리 강화를 위한 법 제정·개정 노력(일부 법이 사이버 사고 정보 수집·공유 체계 관련 내용 포함)이 지속적으로 이루어지고 있으나 입법교착으로 제도개선이 이루어지고 있지 못함[14)]**

- 국가사이버위기관리법안(18대, 공성진), 국가 사이버안전관리에 관한 법률안(19대, 하태경), 사이버위협정보 공유에 관한 법률안(19대, 이철우), 사이버테러 방지 및 대응에 관한 법률안(19대, 이노근), 국가 사이버안보에 관한 법률안(20대, 이철우) 등이 발의되었으나 결국 폐기되었음[15)]

○ **우리나라의 사이버 리스크관리 강화와 사이버보험의 역할 제고를 위하여 미국 사례를 고려한 사이버 사고 정보의 수집·공유 관련 제도개선이 필요함**

- 표준 리스크관리 절차(리스크 식별 → 평가 → 대응)에 따라 사이버 리스크관리를 하기 위하여 사이버 사고 정보의 집적·공유가 필수적임[16)]
- 사이버보험의 핵심 역할 중 하나는 사이버 리스크를 정량화하는 것인데, 이를 위하여 다양한 사이버 사고 정보가 필요함[17)]

---

11) 김동희·박상돈·김소정·윤오준(2017), 「사이버 위협정보 공유체계 구축방안에 관한 연구」, 『융합보안 논문지』, 17(2), pp. 63~64
12) 윤준희·허지용·김화경·신용태(2023), 「국내 사이버위협 정보공유 확산 방안에 관한 연구」, 『융합보안 논문지』, 23(5), pp. 35~43
13) 한국인터넷진흥원(2020), 「KISA cyber security issue report: Q4 2020」, pp. 38~44
14) 방휴·권헌영(2021), 「입법교착 요소로 분석한 사이버안보법 표류에 관한 연구」, 한국정보보호학회지, 31(4)
15) 괄호 안은 (국회 회기, 대표 발의 의원)임. 동 논문 발표 후 2022년에 발의된 「정보통신기반 보호법」 개정안(의안번호: 16829)도 폐기됨
16) 예를 들어 NIST의 Cybersecurity Framework(https://www.nist.gov/cyberframework/framework-version-10)임
17) NPPD(2012), "Insurance Industry Working Session Readout Report", p. 6, 28, 34, 37