https://doi.org/10.33778/kcsa.2023.23.5.035

국내 사이버위협 정보공유 확산 방안에 관한 연구
- 국내 정보보호 산업 생태계 활성화를 중심으로 -

윤 준 희*, 허 지 용**, 김 화 경**, 신 용 태***

요 약

디지털 인프라가 증가하면서 모든 영역에서 연결과 융합이 빠른 속도로 진행되고 있는 가운데 국가 성장 지속을 위해 사이버 침해, 즉 해킹으로부터 안전을 담보하는 것이 무엇보다 중요하다. 이에 사이버침해 대응의 기본이 되는 사이버위협 정보공유에 있어서 저해 요인들을 살펴보고 효율성을 제고할 수 있는 방안을 제시한다. 우선 정보공유에 있어서 정부, 정보보호업체, 중소기업·개인 3개 분야로 구분하고 분야별의 입장에서 요구사항을 확인한다. 이를 보완하고 상호 간에 사이버 보안 강화 및 경제적 이득이 될 수 있는 방안을 모색해본다. 그리하여 정부는 사이버위협 정보 출처 다변화, 중소기업·개인은 사이버보안의 강화, 정보보호업체는 수요가 창출되는 '사이버위협 정보공유 → 중소기업·개인 사이버보안 강화 → 정보보호 산업 수요창출'로 이어지는 선순환 구조의 정보보호 산업 생태계가 조성되도록 정책을 제안하고자 한다. 연구결과는 국가 사이버안보 강화를 위한 정책 수립에 도움이 되기를 기대한다.

Measures to Spread Domestic Cyber Threat Information Sharing and Revitalize the Information Security Industry Ecosystems

Joon-Hee Yoon*, Ji-Yong Huh**, Hwa-Kyung Kim**, Yong-Tae Shin***

ABSTRACT

As digital infrastructure increases connections and convergence progress rapidly in all areas, and it is most important to ensure safety from cyber infringement or hacking to continue national growth. Accordingly, it examines the obstacles to cyber threat information sharing, which is the basis for responding to cyber infringement, and suggests ways to improve efficiency. First of all, information sharing is divided into three areas: the government, cyber security companies, small and medium-sized enterprises and individuals and the requirements are checked from their respective positions. We will supplement this and explore ways to strengthen cybersecurity and provide economic benefits to each other. Therefore, national and public organizations will propose policies to create an cybersecurity industry ecosystem with a virtuous cycle that leads to diversification of cyber threat information sources, strengthening cybersecurity for general companies and individuals, and creating demand for the cybersecurity industry. The results of the study are expected to help establish policies to strengthen national cybersecurity.

Key words : Cyber Threat Information Sharing, Cybersecurity, Cybersecurity Ecosystem, Virtuous Cycle, Cybersecurity policy

접수일(2023년 07월 25일), 수정일(1차:2023년 09월 14일), (2차:2023년 09월 20일), 게재확정일(2023년 10월 16일)

* 숭실대학교/IT정책경영대학원(주저자)
** 숭실대학교/IT정책경영대학원(공동저자)
** 숭실대학교/IT정책경영대학원(공동저자)
*** 숭실대학교 컴퓨터학부 교수(교신저자)

1. 서 론

디지털 인프라가 증가하면서 모든 산업 영역에서 연결이 빠른 속도로 진행, 국가 성장 지속을 위해 사이버 침해(해킹)로부터 안전을 담보하는 것이 무엇보다 중요하다. 윤석열 정부의 110대 국정과제 중 하나로 '국가 사이버안보 대응역량 강화'를 선정하고, 대통령은 2022. 7월 제 11회 정보보호의날 기념식 축사에서 "사이버 공격은 민간과 공공을 구별하지 않고 무차별적으로 위협하고 있다"며 "튼튼한 사이버 안보를 통해 안전한 디지털경제를 구축하고, 민간과 공공이 긴밀히 협력해 사이버 대응태세를 공고히 해야 한다"고 강조한 바 있다. 예측이 불가능하고 새롭게 발생하는 사이버 공격에 대해서는 피해 회복을 할 수 있는 복원력과 함께 사이버침해 피해 예방을 위한 사이버위협 정보 공유가 강조되고 있다.

이에 국내 공공·민간·금융 분야 사이버위협 정보공유 실태를 살펴보면 국가정보원은 '국가 사이버위협 정보 공유 시스템(NCTI, National Cyber Threats Intelligence)'으로 국가·공공기관과 정보를 공유하고 있다. 한국인터넷진흥원은 '사이버위협 분석·공유시스템(C-TAS, Cyber Threats Analysis & Sharing)'으로 민간 기업 및 보안 업체와 사이버 위협 데이터를 확대·공유하고 있다. 금융보안원은 '이상 금융거래 탐지시스템(FDS:Fraud Detection System)'을 통해 금융권과 실시간으로 공유하고 있다. 국내는 사이버위협 정보 공유 시스템 연계가 확장되는 단계이다.

기업·단체 등은 이와 같은 사이버위협 정보공유를 통해 본래 취지인 새로운 사이버위협에 대한 탐지와 방어가 가능하다. 하지만, 위협정보 공유가 증가하면서 다음과 같은 문제점이 부각되고 있다. 첫째, 사이버위협 정보에 개인이나 기관을 식별할 수 있는 데이터가 포함되거나 권한이 없는 제3자에게 유출에 대한 우려 등 법적 문제이다. 둘째, 사이버위협 정보(데이터)를 제공받는 측에서는 시스템에 바로 적용하기 위해 데이터를 재가공해야 하는 비효율성 등 데이터 표준화 문제이다. 셋째, 사이버위협 정보(데이터)량의 증가는 정보 과잉 현상이 발생, 필요한 정보를 추출해야하는 문제이다. 이러한 문제점들은 사이버위협 정보공유를 통한 사이버위협 대응 역량 강화를 체감하기 어렵게 만들고 있는 실정이다. 이에 따라 본 논문에서는 사이버위협 정보 제공자인 민·관·금융기관과 위협정보를 활용하는 기업·단체·개인, 정보보호업체 간에 일방적인 정보 제공자·수급자 관계를 벗어나 상호간의 이득이 되는 사이버위협 정보 활용 방안에 중점을 두었다.

2. 관련 연구

본 장에서는 사이버위협 정보공유의 개념 및 관련 용어 정의를 기술한다. 다음으로 사이버위협 정보의 공유 현황을 살펴보고 사이버위협 정보 관련 법·규정에 대해 서술한다. 마지막으로 사이버위협 정보공유와 관련된 선행 연구에서 제기한 문제점을 정리한다.

2.1 사이버위협 정보 및 용어 정의

2.1.1 사이버위협 정보

"사이버공격·위협"이란 해킹, 컴퓨터 바이러스, 서비스거부, 전자기파 등 전자적 수단에 의하여 정보통신기기, 정보통신망 또는 이와 관련된 정보시스템을 침입·교란·마비·파괴하거나 정보를 위조·변조·훼손·절취하는 행위 및 그와 관련된 위협을 말한다[1].

사이버안보 위협 정보로서 ① 사이버안보 위협의 발생시각, 사이버안보위해자와 피해자를 식별하기 위한 인터넷프로토콜 주소(IP)와 네트워크카드주소(MAC), 정보통신서비스 아이디(ID) ② 사이버안보 위협으로 인하여 발생한 패킷 ③ 그 밖에 사이버안보 위협에 관련된 취약점, 공격기법, 피해내역을 식별하기 위하여 필요한 정보라 나열한다[2].

사이버 위협이란 사이버 공간에서의 악의적인 공격 등을 통해 발생할 수 있는 잠재적인 위협을 뜻하며 개인이나 조직의 자산에 심각한 손실을 발생시킬 수도 있다. 사이버위협 정보는 대응기관이 위협을 탐지하거나 방어하는 데 활용할 수 있는 사이버 위협에 대한 구체적인 정보를 의미한다[3].

사이버위협정보(Cyber Threat Intelligence)란 조직의 자산에 손실 또는 잠재적인 위협이 될 수 있는 지식, 문맥, 메커니즘, 식별자에 대한 주체의 실행 가능한 조언 또는 의사결정을 지원하는 정보를 의미한다[10].

사이버위협 정보는 "비인가 접근, 파괴, 폭로 또는 정보의 변경 그리고 서비스 거부 등을 통해 조직의 업무, 자산, 개개인, 국가 의 정보 시스템에 악영향을 미칠 수 있는 상황이나 이벤트 정보"이다. 사이버위협 정보는 기관이 위협을 탐지하거나 방어에 도움이 되는 정보를 의미한다[4].

<표. 1> 사이버위협 정보의 정의[5].

구분	내용	상세내용
공격자 정보	공격을 발생시킨 주체	o 외부 IP o 내부 IP o 메일 송신자 o URL o 악성코드
공격 방법	실제 공격에 사용된 방법	o IDS 회피 o Anti-Virus 회피
공격 대상	공격을 받는 자산	o 자산 IP o 시스템 o 데이터베이스 o 응용프로그램 o 데이터
공격의 목적(의도)	공격의 의도된 목적	o 네트워크 마비 o 정보 수집 o 정보 탈취 o 악성코드 은닉 o 서비스 마비
취약점 정보	공격에 이용된 취약점	o CVE(Common Vulnerability and Exposure)
대응 방법	공격에 대응하기 위한 방법	o 보고서
탐지 방법	공격을 탐지 위한 방법	o Snort/Yara 탐지규칙 o S/W 버전 o 설정값

2.1.2 정보보호

"정보보호"란 ① 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지 및 복구하는 것 ② 암호·인증·인식·감시 등의 보안기술을 활용하여 재난·재해·범죄 등에 대응하거나 관련 장비·시설을 안전하게 운영하는 것의 활동을 위한 관리적·기술적·물리적 수단(정보보호시스템)을 마련하는 것을 말한다[6].

2.1.3 정보보호 산업

"정보보호산업"이란 정보보호를 위한 기술(이하 "정보보호기술"이라 한다) 및 정보보호기술이 적용된 제품(이하 "정보보호제품"이라 한다)을 개발·생산 또는 유통하거나 이에 관련한 서비스(이하 "정보보호서비스"라 한다)를 제공하는 산업을 말한다[6].

2022년 전체 정보보호산업 매출액은 총 16,180,400백만 원으로 2021년 대비 16.7% 증가하였다. 이중 정보보안 매출액은 2021년 4,549,734백만 원에서 2022년 5,617,174백만 원으로 23.5% 증가하였다. 정보보안 제품은 네트워크보안 솔루션(1,508,712백만 원), 정보보안 관련 서비스에서는 보안 컨설팅(572,644백만 원)의 매출 비중이 높은 것으로 나타났다[7].

2022년 정보보호산업 수출액은 총 2,206,315백만 원으로 2021년 2,076,780백만 원 대비 2022년에는 6.2% 증가한 것으로 조사되었다. 정보보안 수출액은 2021년 152,604백만 원에서 2022년 155,267백만 원으로 1.7% 증가하였다. 정보보안의 경우 수출 비중의 46.5% 정도가 미국에서 발생하고 있으며, 24.7% 정도가 기타 국가에서 발생하는 것으로 나타났다[7]

2025년까지 정보보호산업은 전체 매출액 20조 원, 300억 이상 기업 100개, 16만 5,000명의 인력 양성을 목표로 설정하였다[8].

2.1.4 정보보호 기업

"정보보호기업"이란 정보보호산업과 관련된 경제활동을 영위하는 자를 말한다[6]. 정보보호 기업을 법률용어로 정리하자면 사이버침해에 대해 보안기술을 활용하여 대응하거나 관련 장비·시설을 안전하게 운영하는 관리적·기술적·물리적 수단을 마련하기 위해하는 정보보호기술이 적용된 제품을 개발·생산 또는 유통하거나 이에 관련한 서비스를 제공하는 자이다.

국내 소재 정보보호 기업은 총 1,283개(정보보안 531개, 물리보안 752개)로 종업원 수가 100인 미만인 기업은 정보보안 85.7%, 물리보안 91.9%로 전체의 89.4%를 차지하고 있다[7]. 그 중에 70.1%는 자본금 10억 미만의 규모이다[8].

2.1.5 보안관제

사이버공격·위협을 즉시 탐지·대응하는 것을

“보안관제(保安管制)”라 한다고 명시[1], “보안관제”란 정보통신기기 등을 안전하게 운영하기 위해 사이버 안보 위협행위를 실시간 탐지 및 분석하여 즉시 대응하는 일련의 업무라고 정의[2], 보안관제 업무 수행을 통해 사이버 위협 정보를 생산하고 공유하며 처리하고 있다. 즉 조직 내에 악성 코드가 감염된 시스템을 탐지하고, 제거하고, 피해 범위를 추적하고 재발 방지를 위해 해당 사실과 대처법을 공지함으로써 조직 내에서 위협 정보 공유 업무를 수행하고 있다.[4]

2.1.6 정보보호 전문서비스 기업

정보보호 전문서비스 기업 제도는 「정보통신산업진흥법」에 따른 지식정보보안 컨설팅 전문업체 지정제도를 말하며, 주요정보통신기반시설에 대한 취약점 분석 및 보호대책 수립 업무를 지원하기 위하여 정보보호컨설팅 분야에서 전문능력과 신뢰성을 갖춘 민간업체를 지정하여 양질의 정보보호서비스를 제공하기 위한 것으로 2001년부터 시행하였다. 2022년 12월 기준 28개 전문기업이 활동하고 있다.[9]

2.1.7 보안관제 전문업체

2010년 4월 「국가사이버안전관리규정」에 국가·공공기관의 보안관제센터 구축 의무화 규정을 마련하였다. 2010년 12월 「보안관제 전문업체 지정 등에 관한 공고」를 발표하였다. 2017년 10월 「보안관제 전문기업 지정 등에 관한 공고」를 개정하였다. 보안관제 전문기업 지정기준은 기술인력 15명 이상, 자기자본 20억 원 이상, 업무수행능력 평가를 기준점수 이상 통과하여야 한다. 2022년 12월 기준 20개 기업이 활동하고 있다.[9]

2.2 사이버위협 정보공유 현황

2.2.1 국가·공공 분야

대규모 사이버 공격 시 민·관·군 간 정보공유로 신속한 상황파악·공동대응을 통한 피해 확산을 방지하기 위하여 2016년부터 ‘국가사이버위협 정보공유시스템(NCTI,National Cyber Threat Intelligence)’을 구축하여 운영하고 있으며, 2020년 10월부터 방산업체·국가핵심기술보유기업 등 국익 및 국가안보와 직결되는 민간 산업분야와 정보공유 협약을 체결하고 인터넷 기반의 정보공유시스템(KCTI, Korea Cyber Threat Intelligence)을 구축하여 정보서비스를 진행하고 있는 등 사이버안보 정보의 허브 역할을 수행하고 있다. 2023년 1월 1일 기준 국가·공공기관 326개 및 방산업체를 비롯한 153개 민간기업이 정보공유시스템을 이용 중이며, 범국가 차원의 사이버위협 대응 체계를 갖추는 것을 목표로 한다[9].

2.2.2 민간 분야

한국인터넷진흥원은 한국인터넷진흥원은 사이버 공격에 효과적으로 대응하기 위하여 2014년 8월부터 사이버위협정보 분석·공유(C-TAS, Cyber Threat Analysis & Sharing) 시스템을 운영하고 있다. 2022년 12월 말 기준 정보통신·제조·금융업 등 총 2,161개 기업이 참여하고 있으며, 4억 2천 5백만여 건의 사이버위협 정보를 공유하고 있다. C-TAS에 참여하는 회원사는 공유된 악성코드 및 사이버위협 정보를 분석하고 특징을 추출하여 보안제품 업데이트 등에 사용하고 있으며, 악성URL 및 IP정보는 자사 보안정책에 적용하여 유해 트래픽 차단에 활용하고 있다. C-TAS는 2021년 12월, 개방형 체계로 전환하면서 보안실무자와 관리자 등 직급과 업무 특성에 따른 다양한 형태의 맞춤형 정보를 제공하고 있다. 또한 문자(SMS)나 알림톡(SNS)를 통하여 긴급 대응이 필요한 정보 제공 등 긴급 상황 전파 체계 서비스도 제공하고 있다[9].

2.2..3 금융 분야

금융보안원(FSI, Financial Security Institute)은 금융보안연구원과 금융결제원·코스콤의 금융정보공유·분석센터(ISAC, Information Sharing and Analysis Center) 기능을 통합하여 2015년 4월 출범하였다. 금융보안원은 금융회사에서 발생한 이상금융거래정보를 다른 금융회사와 실시간으로 공유하는 이상금융거래정보공유 체계(FISS, Fraud Information Sharing System)을 운영하고 있다. 2022년 97개 금융회사와 전자금융업자가 이상금융

거래 정보공유 업무에 참여하고 있으며, 184건의 이상금융거래 정보를 공유하여 약 104억 4천여만 원의 금융소비자 피해를 예방하였다. 금융보안원은 금융회사에서 발생한 이상금융거래정보를 다른 금융회사와 실시간으로 공유하는 이상금융거래정보공유체계(FISS, Fraud Information Sharing System)를 구축·운영하고 있으며, 악성파일 실시간 탐지 체계를 구축하여 악성파일 공격을 조기에 탐지·차단하고 있다. 또한 '보이스피싱 척결 종합방안'(2020. 6.)에 따라 시중은행과 대형전자금융업자 등을 중심으로 보이스피싱 예방·대응을 위한 기술적 방안을 마련하였으며, 2021년 금융·통신·보안분야 유관 전문기관과 협력하여 '범금융권 보이스피싱 사기정보 공유시스템'을 구축하였다[9].

2.2.4 기타

첫째, 정보통신 ISAC은 한국정보통신진흥협회(KAIT)가 2002년 3월부터 9개 기간통신사업자를 회원으로 취약점 컨설팅, 민간분야 주요정보통신기반시설 보호 지원을 시행 중이다. 둘째, 행정 ISAC은 한국지역정보개발원(KLID)이 2013년 2월부터. 17개 시·도· 지자체 대상 보안관제, 취약점 분석평가, 컨설팅 등을 시행 중이다. 셋째, 의료 ISAC은 사회보장정보원(SSIS)이 2018년 11월부터 43개 진료정보 문서저장소 및 민간 의료기관 상시 보안관제, 정보공유, 침해대응, 보안교육 및 훈련을 시행 중이다[9].

2.3 사이버위협 정보공유에 관한 법·규정

대통령령인 '사이버안보 업무규정'은 2020.12.31. 제정되었으며 제6조 ①항에 "국가정보원장은 사이버안보 관련 정보를 중앙행정기관 등에 배포·공유하기 위하여 정보공유시스템을 구축·운영할 수 있다." 라고 명시하고 있다[1].

2021. 11월 김병기의원이 "국가사이버안보법안"을 제안 하였으나 회기 종료로 폐기 되었다. 법안의 제11조(정보의 공유)에서 국제 및 국가배후 해킹조직 등 사이버안보 정보, 침해사고에 관한 정보, 국방·금융·진료 정보침해에 관한 정보, 조사 결과에 관한 정보, 사이버안보 위협행위 예방에 활용될 수 있는 정보에 대해 공유하고 상호 협력하여야 한다는 내용이 있다. 또한 제14조(통합보안관제체계의 구축 등)에서는 보안관제를 통해 자동적으로 처리되는 사이버안보 위협행위의 탐지·대응 정보를 발생시각, 인터넷프로토콜 주소(IP)와 네트워크카드 주소(MAC), 아이디(ID), 패킷, 그 밖에 사이버안보 위협에 관련된 취약점, 공격기법, 피해내역을 식별하기 위하여 필요한 정보에 대해 필요한 범위 수집·이용할 수 있다고 명시하고 있다[2].

2.4 사이버위협 정보공유의 문제점

첫째, 산업계에서 성공적인 위협 정보 공유 모델이 없고, 정보의 수요자가 되기를 원하지만 공급자의 역할을 수행하는 데는 소극적이다. 그 요인으로는 "법 제도 문제"와 "민감 정보 공유", "공유 정보의 품질", "경영진의 태도" 등의 요인이 존재한다[11]. 둘째, 국내 보안 산업 군에서는 아직 위협 공유 체계를 가지고 있지 않다. 글로벌 보안 업체에서 CTA(Cyber Threat Alliance) 를 구성하여 정보를 공유하고 있지만 한국의 경우 자체 국산 보안제품의 사용률이 높아 국내 보안 업계 내에서 위협 정보 공유 및 분석의 필요성이 높다고 볼 수 있다[4]. 셋째, 지방자치단체 사이버침해대응센터 대상 조사를 통한 문제점은 다음과 같다. 한국지역정보개발원, 국가정보원 등 상위 관제단위와의 원활하지 않은 정보공유, 발생하는 이벤트의 증가로 처리에 한계 존재, 공유시스템에 정보를 공유하는 것은 평가항목으로 정보과잉 현상이 발생하여 오히려 필요한 정보를 찾기 어렵다고 나타났다[13].

선행 연구의 문제점을 종합해 보면 ①사이버위협 정보에 개인이나 기관을 식별할 수 있는 데이터가 포함되거나 권한이 없는 제3자에게 유출에 대한 우려 등 법적 문제이다. 개인정보 및 기업과 관련된 민감한 정보가 권한이 없는 제3자에게 유출되는 등 법적 문제가 발생할 가능성 ②사이버위협 정보(데이터)를 제공 받는 측에서는 시스템에 바로 적용하기 위해 데이터를 재가공해야 하는 비효율성 등 기업별로 사이버위협 정보의 규격이 달라 데이터

표준화 필요 ③사이버위협 정보(데이터)량의 증가는 정보 과잉 현상이 발생, 필요한 정보를 추출해야 하는 사이버위협 정보 과잉 현상 발생 ④기타, 중소기업은 대기업과 비교하여 상대적으로 정보보호 역량과 전담 인력이 부족하고 또는 위협정보 수집·가공 시스템을 도입할 경제적 여력이 없어 사이버침해 대응에 취약이다. 이러한 문제점들은 사이버위협 정보공유를 통한 사이버위협 대응 역량 강화를 체감하기 어렵게 만들고 있다.

3. 사이버위협 정보공유의 개선방안 및 정보공유 주체별 요구사항

3.1 사이버위협 정보공유의 개선방안

첫째, 법적 이슈인 법정 위반사항에 대한 면책 보장을 하는 방안으로 ①가칭 '사이버위협 정보 유통법' 등 개인정보보호법 위반을 조각할 수 있는 특별법을 제정하는 방법. ② 정보보호산업의 경쟁력 강화와 안전한 정보통신 이용환경 조성을 위해 제정한 '정보보호산업법'에서 사이버위협정보의 유통 활성화를 위한 조항을 삽입하여 개정하는 방법. ③국회 발의 중인 "국가사이버안보법안"에 나열한 사이버안보 위협 정보의 활용 범위를 확대하여 입안하는 방법 등이 있다.

둘째, 표준화 이슈는 사이버위협 정보를 구조화하는 표현 규격으로 조직별로 수집하여 보유한 비표준 형태의 사이버위협 정보(CTI: Cyber Threat Intelligence)를 누구나 분석, 해석하여 활용할 수 있도록 체계화된 구조로 ①CTI의 전송 데이터 표준은 한국정보통신기술협회(TTA)이 2018.6월 제정한 표준 STIX(Structured Threat Information eXpression) 준용 ②CTI의 데이터 전송 표준은 2021.12월 제정한 TAXII(Trusted Automated Exchange of Intelligence Information) 표준을 준용한다[3].

셋째, 위협정보 과잉 이슈는 수집·가공 등 사이버위협 정보 과잉이 발생하는 경우에 정부나 보안관제 전문기업 등 전문 기관에서 데이터를 전달하여 AI분석기법으로 재가공하여 활용하도록 한다. 한편 위협 대응 시스템 미보유 중소기업·개인에 대해서는 과학기술정보통신부(KISA)가 지원 중인 중소기업 대상 정보보호 제품 지원 서비스인 '백업 서버' 및 '보안 솔루션' 도입에 적극 지원하여 공급가액 대비 정부지원:수요기업 = 9:1로 정부지원 최대금액을 초과할 경우, 초과분은 수요기업이 부담하는 방법 등을 활용한다.

<표. 2> 과학기술정보통신부(KISA)의 중소기업 대상 정보보호 제품 지원 서비스 예[14].

서비스	개요	내용	22년
랜섬웨어 데이터금고	데이터 백업 지원, 랜섬웨어 피해 예방	·클라우드 백업 100 GB(6개월~1년) ·백업 서버(NAS) 구축 지원 10TB	5,000 개
정보보호 컨설팅 및 보안솔류션 지원	·정보보호 컨설팅 ·네트워크, 시스템, 정보유출, 암호·인증, 보안관리 분야 보안 솔루션 지원	·컨설팅 결과를 기반으로 보안솔루션 도입 비용 지원	600 개
클라우드 기반 보안서비스	SECaaS(클라우드기반 보안서비스) 지원	정보보호 자가진단 서비스 및 클라우드 기반 보안서비스 도입 비용 지원	700 개

3.2 사이버위협 정보공유 주체별 요구사항

첫째, 정부는 개인정보 및 기업과 관련된 민감한 정보 등의 유출에 대한 막연한 두려움 등의 사유로 정부 차원의 사이버위협 정보공유는 활성화가 미흡한 상태라고 볼 수 있다. 하지만 정부는 가능한 많은 사이버위협 데이터를 수집·분석하여 신속하게 양질의 정보를 생산·배포하여 사이버침해에 대응함으로서 국민의 안전과 재산 보호를 해야 한다. 이러한 목적을 달성하기 위하여 가능한 많은 위협정보 수집출처가 필요하다.

둘째, 정보보호 업체, 특히 보안관제업체는 대기업 등 고객사가 민감한 정보의 외부 유출에 대한 실정법 위반으로 고소할 수 있다는 위험 부담으로 고객사로부터 입수한 사이버위협 정보를 타 기관·기업에 제공하거나 적용에 어려움이 있다. 게다가 단순 탐지 이벤트 등 법적 문제가 없는 데이터를 공유하는 것은 불필요한 정보 과잉을 야기하여 위협정보 수집출처의 업무를 가중하는 결과를 초래할 수 있

다. 이에 사이버위협에 적극 대응하고 경쟁력을 갖추기 위해서는 가능한 많은 고객사로부터 사이버 위협 정보를 입수하는 한편 다른 고객사간에 공유가 되도록 제도적 뒷받침이 필요하다.

셋째, 중소기업·개인은 위협정보 수집·가공 시스템 구매 및 정보보호 서비스가 필요하지만 정보보호 역량과 전담인력 부족뿐만 아니라 투자 대비 실익이 없다고 판단하여 경제적 부담으로 간주하는 경향이 있다. 한편, 위협정보 수집·가공 시스템을 보유하고 있어도 다른 사이버위협 정보 제공자로부터 정보 입수는 호의적이나 기업 내부에서 입수되는 사이버 위협 정보에 대한 공유에는 취약점 노출 및 대외 이미지 손상 등을 사유로 소극적일 수밖에 없다. 이에 기업·개인으로부터 수집되는 사이버 위협 데이터의 익명성 보장 등 대안이 필요하다.

상기 요구사항을 요약하면 ①정부는 사이버위협 정보공유 수집처 다원화, ②정보보호업체는 지속적 수요 및 고객사 사이버위협 정보의 수집·활용, ③ 중소기업·개인에게는 경제적 부담 완화가 필요하다.

4. 사이버위협 정보공유 확산 및 정보보호 산업 생태계 활성화 방안

첫째, 중소기업·개인은 정부가 지원 중인 백업 서버 및 보안 솔루션 도입과 함께 위협정보 수집이 가능한 네트워크 보안제품을 순차적으로 도입한다. 정부는 추가적으로 침입탐지시스템(IDS) 등 네트워크 보안제품을 정부:중소기업·개인 = 9:1 매칭 펀드 방식으로 지원한다. 중소기업·개인이 정보보호 업체 특히 보안관제 전문기업과 사이버 위협정보 활용을 약정 형식으로 합의를 하면 보안관제 전문기업의 서비스를 무상으로 지원받는다. 단, 정보보호 제품·보안관제 전문기업은 중소기업·개인이 선택한다. 그리하여 중소기업·개인은 비용이 절감과 함께 양질의 정보보호 서비스를 받는 일거양득의 효과를 누릴 수 있다. 이러한 서비스는 사이버침해에 의한 업무 방해와 금융자산 유출을 예방할 수 있다. 게다가 사이버침해에 대한 두려움에서 벗어나 경제 활동에 몰두할 수 있는 심리적 안정감을 얻는다.

둘째, 정보보호업체는 백업 서버 및 보안 솔루션, 침입탐지시스템(IDS) 등 네트워크 보안제품을 중소기업의 규모에 따라 적합한 맞춤형 정보보호제품 제작 등 수급에 차질 없도록 공급한다. 특히 보안관제 전문기업은 사이버 위협정보 활용에 합의한 중소기업·개인 대상 보안관제 서비스를 무상으로 지원한다. 그리하여 정보보호 업체는 중소기업에 정보보호 제품에 대한 안정적인 수요 확대로 저가 고품질의 제품을 생산하게 되어 기술 경쟁력을 확보할 수 있다. 한편 보안관제 전문업체는 중소기업·개인으로부터 사이버위협 정보 수집·활용을 보장 받음으로서 위협정보의 양적 확대가 가능하다. 이를 바탕으로 고객사인 국가·공공기관, 대기업에 양질의 정보보호 서비스 제공이 가능해진다.

셋째, 정부는 기존 매칭 펀드 방식으로 지원 중인 중소기업 대상 정보보호 제품 지원 서비스를 확대하여 '네트워크 보안제품' 및 '보안관제 서비스'를 추가하며 예산을 점차 확대한다.

이를 통해 보안관제 전문업체 및 중소기업·개인 등 다양한 수집처로부터 대량의 사이버위협 정보를 입수할 수 있다. 이 정보들은 빅데이터 기술을 활용할 수 있는 기초 데이터가 된다. 사이버위협 정보 빅데이터는 AI 기술을 적용·발전시켜 사이버 위협에 대한 예측 모델 개발도 가능할 기회를 맞이한다.

이것은 금융거래 위해 정보, 가상자산 불법 취득 정보 및 랜섬웨어 정보 등 국민의 자산 보호와 관련된 사이버위협 정보부터 국가 차원에서 대응해야 할 위협정보 생산까지도 부가적으로 가능해지며 이는 곧 국가의 사이버위협 대응 역량 강화로 이어질 것이다.

5. 결론

본 연구의 목적은 정보공유 주체로서 정부, 정보보호업체, 중소기업·개인 3개 분야로 구분하고 상호간에 경제적 이득과 함께 국가적으로 사이버위협 대응 역량 강화가 될 수 있는 것이었다. 이에 정부는 사이버위협 정보 출처 다변화, 중소기업·개인은

사이버보안의 강화, 정보보호 업체는 지속적 수요 창출 방안 모색, ‘사이버위협 정보공유 → 중소기업·개인 사이버보안 강화 → 정보보호 수요 창출’로 이어지는 선순환 구조의 정보보호 산업 생태계를 조성할 수 있는 방법론을 제시하였다. 연구결과는 국가 사이버안보 강화를 위한 정책 수립에 활용될 수 있을 것이다.

다만 추가적으로 보완해야 할 점으로는 첫째, 사이버위협 정보를 제공하는 정보보호업체, 중소기업·개인에 대해 위협정보 공유의 지속성을 유지하기 위해 적절한 보상 체계를 제공해야 하는 것이다. 이를 위해서는 공정한 사이버위협 정보 평가와 이를 바탕으로 한 보상이 주어져야 하는 과제가 있다. 둘째, 정보공유로 급격하게 증가하는 사이버위협 이벤트를 처리하기에는 한계가 존재한다. 따라서 정부, 정보보호업체는 보안관제 대상의 규모와 특성에 적합한 맞춤형 AI 보안관제가 가능하도록 기술을 개발하고 지원해야 하는 과제가 있다.

끝으로 향후 연구 과제로는 사이버위협 정보공유 활성화 실행을 보장할 수 있는 전제 조건에 대한 연구이다. 즉, 정부의 예산 반영 의지, 중소기업·개인의 사이버위협 정보 제공에 대한 의지, 정보보호업체의 정부·대기업 등 고객사 대상 사이버위협 정보 제공 의지이다. 이에 관해 향후 각 정보공유 주체별 정보보호 산업 생태계 활성화로 이어질 수 있는 법·제도와 함께 정보공유 플랫폼 등 기술적인 연구가 이어져야할 것이다.

참고문헌

[1] 국가정보원, “사이버안보 업무규정”, 제2조 ①항. 제14조 ①항.

[2] 김병기의원 발의 “국가사이버안보법안” 제11조-제14조, 2021.

[3] 김종현, “STIX/TAXII 기반의 사이버위협 정보 공유 표준화동향”. TTA저널, 11월호, 2019.

[4] 박지백, 최병환, 조학수, “사이버 위협 정보의 공유 활성화 방안”, 한국통신학회지, 제25권, 제7호, pp. 41-48, 2018.2018.7.

[5] 이용균, ”지능적이고 자동화된 사이버위협정보 공유 모델 연구”, 고려대학교 정보보호대학원 박사학위논문, pp. 111-112, 2016.

[6] 정보보호산업법 제2조(정의) ①-1~ 3.

[7] 한국정보보호산업협회, ″2023 국내 정보보호산업 실태조사″, pp. 30-34, 2023.

[8] 관계부처 합동, ″제2차 정보보호산업 진흥계획(2021 ~ 2025)″, 2020.6.

[9] 관계부처 합동, ″2023 국가정보보호백서″, pp. 24-2, 43, 52, 84, 111-118, 159-161, 162-163, 2023.

[10] 김하영, 김태성 ″국내 사이버위협 정보 공유에 영향을 미치는 요인″, 정보보호학회논문지, 제27권, 제5호, pp. 1167-1188, 2017.

[11] 정보통신단체표준(국문표준), ″사이버보안 정보 공유 협상절차″,pp. 1-2, 2011.

[12] 최정민, ‘사이버침해대응센터 운영실태와 개선과제‘, 국회입법조사처 NARS 입법 정책, 제97호., pp.39-40, 2021.

[13] 과학기술정보통신부, 한국인터넷진흥원, ″2022년, 달라지는 정보보호 제도와 지원 사업”, pp. 12-13, 2022.

〔저자소개〕

윤 준 희 (Joon-Hee Yoon)
2019년 2월 건국대 정보보호학 석사
2023년 9월 숭실대 IT정책경영학 박사 재학중
email : jhmom21088@gmail.com

허 지 용 (Ji-Yong Huh)
2021년 2월 숭실대 컴퓨터공학과 석사 학위 취득
2023년 9월 숭실대 IT정책경영학과 박사과정 재학중
email : sangkmii@naver.com

김 화 경 (Hwa-Kyung Kim)
2023년 2월 숭실대 IT정책경영학과 석사학위 취득
2023년 9월 숭실대 IT정책경영학과 박사과정 재학중
email : kimhk@seoilen.com

신 용 태 (Yong-Tae Shin)
1990년 12월 美 Iowa대 컴퓨터과학과 석사학위 취득
1994년 5월 美 Iowa대 컴퓨터과학과 박사학위 취득
2023년 9월 숭실대 컴퓨터과학부 교수 재직중
email : kimhk@seoilen.com