사이버 복원력 동향 분석

추동균[1], 김진[2], 유진호[3]
[1]상명대학교 경영학과 박사
[2]상명대학교 지능·데이터융합학부 교수
[3]상명대학교 경영학부 교수
cdg1608@smu.ac.kr, jinkim@smu.ac.kr, jhyoo@smu.ac.kr

Cyber Resilience Trend Analysis

Dong Gyun Chu[1], Jin Kim[2], Jinho Yoo[3]
[1]Division of Business Administration, Sangmyung University
[2]Big Data Convergence Major, Sangmyung University
[3]Division of Business Administration, Sangmyung University

요 약

디지털 기술의 지속적인 발전으로 여러 서비스를 제공함과 동시에 갈수록 고도화된 사이버 공격으로 인해 다양한 사이버 위험에 노출될 수 있다. 이에 본 연구에서는 사이버 공격 발생 시 신속한 사이버 복원력 확보를 위해 해외 주요국 및 기관의 관련 정책과 동향을 분석해 보고자 한다.

1. 서론

본 연구의 목적은 국민 생활에 밀접한 디지털 기술을 활용에 있어 다양한 서비스에 대한 사이버 공격 발생 시 신속한 사이버 복원력을 확보하기 위함이며 이를 달성하기 위해 해외 주요국과 글로벌 기관들의 사이버 복원력 관련 정책에 대해 조사하고 분석하여 시사점을 도출하고자 한다.

2. 사이버 복원력 해외 주요국 정책 동향

2-1. 미국

미 행정부는 이러한 국가안보 차원의 사이버 전략 수행을 위해 2018년 CISA(Cyber security and Infrastructure Security Agency) 설립 이래 최초로 향후 3년간 기관의 미션과 국가 사이버 보안 수준 강화의 이정표 역할을 할 'CISA Strtegic Plan 2023 ~ 2025'를 발표하였다[1].이 전략 계획은 CISA가 통합 기관으로서의 임무를 달성할 수 있도록 추진할 4가지 목표를 정의하고 있으며 그중 목표2: 위험감소 및 복원력(risk reduction and resilience)'를 통해 사이버 복원력에 대해 설명하고 있다. 이것은 사이버 공격이나 자연적 위험 및 물리적 위협 등 새로운 위협과 중단에 대비하여 리스크를 줄이고 보안 역량을 강화하기 위함이며 6가지의 세부 과제를 제시하고 있다.

<표 1> 미국 CISA 전략계획의 사이버 복원력

2. 위험감소 및 복원력	(2-1) 기반시설, 시스템, 네트워크에 대한 가시성 확대
	(2-2) CISA의 위험 분석 기능 및 방법론 개선
	(2-3) CISA의 보안·위험 완화에 대한 지침 개선 및 영향력 강화
	(2-4) 기반시설 및 네트워크의 보안·복원력 측면에서의 이해관계자 역량 강화
	(2-5) CISA의 위험 및 사고에 대한 대응 능력 향상
	(2-6) 선거 인프라의 위험 관리 활동 지원

2-2. EU

2022년 9월 15일, EU는 유럽연합 내 디지털 제품의 사이버 보안을 강화하고 기존의 사이버 보안 규제 격차를 해소하기 위한 법률 초안인 사이버 복원력법(Cyber Resilience Act)을 제시하였으며, 제안된 규제는 디지털 요소가 포함된 유무형 제품(커넥티드 디바이스, 비 임베디드 소프트웨어 등)에 광범위한 수평적 규제 프레임 워크를 적용하여 전체 디지털 공급망에 사이버 보안 표준을 적용하였다[2].

사이버 복원력법은 연결된 기기와 같은 유형의 디지털 제품과 연결된 기기에 내장된 소프트웨어 제품과 같은 비유형의 디지털 제품을 대상으로 하며, 본질적으로 EU 시장에서의 인터넷과 인터넷 연결된 소프트웨어에 연결된 디지털 제품을 대상으로 하고 있다. 사이버 복원력법은 적용 대상 제품을 크게 'Class Ⅰ', Class Ⅱ', 'Unclassified or Default'이렇게 3가지 범주로 나눈다. Default 범주는 중대한 사이버 보안 취약점이 없는 제품에 적용한다.

리스크 범주	제품 및 서비스 예시	
Class I	• 신원 확인 및 접속 관리 소프트웨어 • 브라우저 / • 비밀번호 관리자 • 악성 소프트웨어 감지 • 가상 민간 네트워크 활용 제품 • 네트워크 관리, 조정, 모니터링, 리소스 관리 도구 • 보안 정보 및 이벤트 관리 시스템 • 업데이트 및 패치 관리 도구 • 원격 접속 소프트웨어	• 모바일 기기 및 어플리케이션 관리 소프트웨어 • 물리적 네트워크 인터페이스 • 마이크로 컨트롤러 • NIS2 지침에 묘사된 필수적인 주체에 의해 활용되기 위한 IC 및 게이트 배열 • 운영 체제, 방화벽, 라우터, 모뎀, 마이크로프로세서, 산업 자동화 및 통제 시스템, Class II에 속하지 않는 산업 IoT
Class II	• 운영체제 • 하이퍼바이저와 컨테이너 런타임 시스템 • 공공 키 인프라와 디지털 인증 발행자 • 산업용 방화벽 • 산업용 침투 감지 및 예방 시스템 • 일반 목적 마이크로프로세서 • 프로그램 가능 로직 컨트롤러와 보안 부품을 위한 마이크로프로세서	• 산업용 라우터, 모뎀, 스위치 / • 보안 부품 • 하드웨어 보안 모듈 / • 보안 암호프로세서 • 스마트카드, 리더, 토큰 / • 스마트 계량기 • NIS2 지침에 묘사된 필수적인 주체에 의해 활용되는 산업용 자동화 및 통제 시스템 • NIS2 지침에 묘사된 필수적인 주체에 의해 활용되는 산업 IoT • 로봇 센싱 및 작동기 부품 및 로봇 컨트롤러

(그림 1) EU 사이버 복원력 법안에 따른 제품 분류

2-3. 영국

최근 영국 정부는 2025년 달성을 목표로 하는 '국가사이버전략(National Cyber Strategy) 2022'를 발표하였으며 영국이 계속하여 책임감 있고 민주적인 사이버 영향력의 선도국으로서 사이버 공간을 통해 자국의 이익을 보호하고 증진하는 것을 비전으로 제시하였으며 이를 달성하기 위한 목표를 제시하였다[3]. 이를 위해 5가지 전략 축을 제시하고 있으며 이중 '전략축 2'는 회복력 있고 번영하는 디지털 영국 구축을 목표로 하고 있으며 이를 달성하기 위해 크게 3가지 관점을 제시하고 있다.

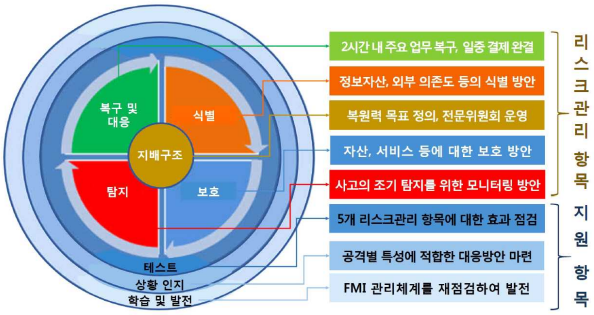
2-4. 프랑스

프랑스 정부는 우크라이나-러시아 전쟁을 계기로 유럽 방위 및 전략적 자율성의 범위하에 전쟁에 대한 대비 태세 강화와 동맹을 강화하기 위한 노력을 명시하였다. 'Nationale Strategique 2022(국가전략 2022)'발표를 통해 군사적 억지력과 더불어 사이버 위협으로부터 강력한 복원력을 확보하고 긴장관계에 있는 글로벌 사이버안보 거버넌스의 주도권과 전략적 연대를 명시하였다[4]. 국가전략의 10대 목표 중 '4번째 최고 수준의 사이버 복원력 확보'를 명시하였으며 이를 달성하기위해 3가지 과제를 제시하였다.

3. 사이버 복원력 관련 해외 주요 기관 동향

3-1. CPMI-IOSCO

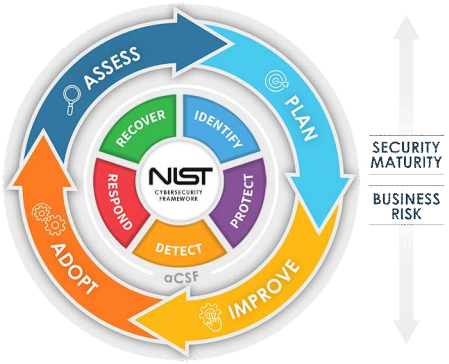
CPMI는 국제결제은행(BIS) 산하 지급결제 및 시장인프라 위원회(Committee on Payments and Market Infrastructures)로 IOSCO(국제증권감독기구, International Organization of Securities Commissions)와 공동으로 FMI(금융시장 인프라, Financial Market Infrastructure)의 사이버 복원력 제고를 위해 FMI 대응, 감독당국의 업무수행 등에 필요한 사항등을 정리하여 2016년 사이버 복원력 Guidance를 발표 하였다[5]. 이를 통해 통해 국제기준인 금융시장 인프라에 관한 원칙(PFMI)을 기반으로 사이버공격에 대비하여 마련해야 하는 업무 복원력 관련 조치사항 및 그에 대한 충족도 측정을 위한 세부 권고사항 등을 명시하였다. CPMI-IOSCO는'사이버복원력 Guidance'를 통해 사이버 복원력 제고를 위한 5개의 주요 리스크 관리 항목과 3개 지원 항목으로 구성된 관리체계를 제시 하였다. FMI에 대한 사이버공격의 범위가 매우 광범위한 점을 감안하여 금융당국, 금융기관, IT업체, 수사기관 등 관련기관간 협력 강화 필요성을 강조하였다.



(그림 2) CPMI-IOSCO 사이버복원력 체계 개요

3-2. NIST 사이버보안 프레임워크

NIST(미국 국립표준기술연구소)는 사이버 보안 관련 리스크를 관리하기 위해 관련 표준, 지침 및 모범사례 등을 포함한 프레임워크를 지난 2013년부터 발표하여 지속적인 발전을 해오고 있으며 이것은 사이버 보안 업계의 세계적으로 널리 인정받는 평가기준으로 여겨지고 있다[6]. NIST의 사이버보안 프레임워크는 우선순위 결정, 유연하고 효율적인 비용 접근 방식을 통해 중요 핵심 인프라를 보호하고 복원력 제고를 위한 주요 방법론이 될 수 있음을 제시하고 있다. NIST 사이버 보안 프레임워크는 조직이 사이버 보안 프로그램을 시작하거나 개선하는 데 도움을 준다. 사이버 보안 프레임워크는 효과적인 것으로 알려진 사례를 바탕으로 제작하였기 때문에 조직의 사이버 보안 상황을 개선하는데 도움을 줄 수 있다. 또한 사이버 보안 프레임워크는 내·외부 이행 관계자들 사이에서 사이버 보안에 대한 소통을 촉진한다. 더 큰 규모의 조직에서는 사이버 보안 위험 관리와 기업의 위험 관리 프로세스를 통합하고 조율하는데 도움을 준다. NIST의 사이버 보안 프레임워크는 5가지 핵심 기능(식별, 보호, 탐지, 대응, 복구)들로 구성된다.



(그림 3) NIST 사이버보안 프레임워크

3-3. IACA(국제선급협회)

해사업계에 ICT 기술이 도입·융합됨으로써 해상 사이버 위협 및 리스크가 증가하고 있다. 특히, 최근 발생한 해상 사이버공격 사례는 선박, 항만, 육상 인프라 등 해상물류체계가 사이버 공격의 주요 표적이 되고 있다. 특히 해상 비즈니스 환경이 인공지능(AI), 블록체인, 빅데이터, 디지털 트윈, 사이버보안, 스마트 센싱, 5G 등 정보통신기술(ICT)이 도입·융합됨으로써 변화하고 있는 실정이다[7]. 해상업계의 이러한 디지털화는 사이버 위협과 위험을 높이는 요인이 되고 있으며 최근 여러 해상 운송 및 물류 시스템 인프라의 사이버 공격이 빈번해 지고 있어 점점 해상물류체계가 사이버 공격의 주요 표적이 되고 있음을 알 수 있다. 러한 사이버 위협에 대응하기 위해 국제선급협회(International Association of Classification Societies: IACS)는 신조선과 선박에 탑재되는 기자재 시스템 사이버보안 통합 요구사항(Unified Requirement:UR)을 수립하였으며, 이를 기반으로 2024년 각 선급에서는 선박 건조 시 조선소 및 제조사에 사이버보안 관련 요건 준수를 강제화할 예정이다.

<표 2> IACS 선박 사이버 리스크 관리를 위한 5가지 요소

기능요소	요구사항
식별 (Identify)	선상 시스템, 사람, 자산, 데이터 및 기능 사이버 리스크를 관리하기 위한 조직적 이해를 개발
보호 (Protect)	사이버 사고로부터 선박을 보호하고 운송 연속성을 극대화하기 위한 적절한 보호 장치를 개발 및 구현
탐지 (Detect)	선상에서 사이버 사고의 발생을 탐지하고 식별하기 위한 적절한 조치를 개발하고 구현
대응 (Respond)	선내에서 탐지된 사이버 사고에 대해 조치를 취하기 위한 적절한 조치 및 활동을 개발 및 구현
복구 (Recover)	사이버 사고로 인해 손상된 운송에 필요한 모든 기능 또는 서비스를 복구하기 위한 적절한 조치 및 활동을 개발하고 구현

IACS는 UR(통합요구사항)발표를 통해 선박의 설계, 건조, 시 운전 및 운영 등 전 생애주기 동안 운영기술(OT) 및 정보 기술(IT) 시스템의 사이버 레질리언스를 목표로 5가지 사이버 리스크 관리 기능요소를 정의 하였다.

4. 결론 및 향후 연구

본 연구는 사이버 위험에 있어 사고를 사전에 예측하고 탐지하여 회피할 수 있는 시스템을 구축함과 동시에, 실제 사고 발생 시 이를 견뎌내고 신속히 복구 및 회복할 수 있는 체계를 수립하는 것을 목표로 하고 있다. 이에 사이버 복원력 관련하여 해외 주요국 정책 및 글로벌 기관들의 동향을 조사하였다. 이를 통해 향후 국내 사이버 복원력 강화를 위한 방법론 구축, 제도 및 법적인 관점의 개선 방안 제언으로 연구를 확장할 수 있으며 본 논문에서 조사한 동향 조사·분석이 향후 연구의 기초자료로 활용될 수 있을 것이다.

사사표기

본 논문은 2023년도 상반기 방송통신정책연구(디지털 서비스의 사이버 복원력 확보 방안 연구)의 지원을 받아 수행한 연구임.

참고문헌

[1] 오일석 외, “미국사이버전략의 평가와 전망”, INSS전략보고, 2022.09. No.175

[2] Kir Nuthi, “An Overview of the EU’s Cyber Resilience Act”, Center For Data Innovation, 2022

[3] HM Government, “National Cyber Strategy”, 2022

[4] Secrétariat général de la défenseet de la sécurité nationale, “Revue nationale stratégique”, 2022

[5] 유희준, “최근 국제 논의동향을 반영한 국내 FMI의 사이버복원력 강화 방안”, 서울, 동화인쇄공사, 2016

[6] Christophe Bertrand et al., “Bolstering Your CyberResiliencewith Veritas”, Enterprise Strategy Group, 2021

[7] 임정규, “해상 사이버보안 국제선급협회 동향”, 주간기술동향, 2053호, 2p-12p, 2022