주요국 사이버보안 정책 동향 및 시사점

Trends and Implications of Cybersecurity Policies in Major Countries

이재성 (J.S. Lee, jaeseonglee@etri.re.kr) 기술경제연구실 연구원
최선미 (S.M. Choi, sonia@etri.re.kr) 기술경제연구실 책임연구원
안춘모 (C.M. Ahn, cmahn@etri.re.kr) 기술경제연구실 책임연구원
유영상 (Y. Yoo, heyyoo@etri.re.kr) 기술경제연구실 책임연구원

ABSTRACT

Cyberspace is emerging as a critical domain requiring national-level governance and international cooperation owing to its potential financial and societal impacts. This research aims to investigate the cybersecurity policies from major countries for understanding with comprehensive perspectives. Global trends emphasize a comprehensive command-centered approach, with top leadership directing cybersecurity policies. Key policy areas include security across technology ecosystems, protection of critical infrastructure, and software supply chain security. Investment is being focused on zero-trust architectures, software bills, and new technologies like artificial intelligence. For countries like Korea, immediate response and adaptation to these trends are crucial to develop and enforce national cybersecurity policies.

KEYWORDS 거버넌스, 국가전략, 사이버보안, 투자전략

Ⅰ. 서론

디지털 기술은 일상의 변화와 기술·산업의 발전을 넘어 정치·경제·사회·문화 등 국가와 사회의 모든 부문에서 혁신의 기반이 된다. 글로벌 패권경쟁의 심화, 저성장·양극화의 위기, 기후변화 등 대내외적 변화와 위기에 대한 해법이자 국가 경쟁력과 지속가능한 발전의 근원으로 디지털 기술과 이를 활용한 사이버공간의 중요성이 그 어느 때보다 높다.

사이버공간은 다양한 하드웨어와 소프트웨어로 정의되는 컴퓨터 네트워크로, 연결성과 개방성이 급격히 확대되며 기하급수적으로 복잡한 구조를 띤다[1]. 무질서한 배열로 악의적인 공격자가 쉽게 숨어 악용할 수 있는 다양한 보안 취약점을 내포할 수 있으며, 최근 인공지능 등 혁신기술의 발전과 디지털 자산 거래 확대에 따라 중요성이 증가하고 관련 범죄가 급증하는 추세다.

'22년 하반기에는 랜섬웨어 감염으로 인해 의료, 상수도, 통신 등 주요 분야 피해가 지속해서 발생하였으며, 특히 의료 부문의 진료 중단으로 이러한 위

* DOI: https://doi.org/10.22648/ETRI.2023.J.380406
* 본 연구는 한국전자통신연구원 연구운영지원사업의 일환으로 수행되었음[23ZR1400, 국가 지능화 기술정책 및 표준화 연구].

표 1 사이버보안 개념 정의

NISTIR 8183 (2017) 공격을 방지, 감지 및 대응하여 정보를 보호하는 프로세스
NIST SP 800-160 Vol. 2 Rev. 1 (2021) 컴퓨터에서 처리 및 저장되는 정보의 기밀성, 무결성 및 가용성을 보장하는 조치 및 제어
NISTIR 8170 (2020) 사이버공격으로부터 사이버공간의 사용을 보호하거나 방어하는 능력
NISTIR 8074 Vol.2 (2015) 시스템의 기밀성, 무결성 및 가용성을 강화하기 위해 전자정보 및 통신 시스템과 여기에 포함된 정보의 손상, 무단사용, 악용 방지 및 필요한 경우 복원
NIST SP 800-53 Rev. 5 (2020), NISTIR 8323r1 (2023) 가용성, 무결성, 인증, 기밀성 및 부인 방지를 보장하기 위해 컴퓨터, 전자통신시스템, 전자통신서비스, 유선통신 및 전자통신(정보 포함)의 손상 방지, 보호 및 복원. 일례로 위치지정, 네비게이션, 타이밍 데이터는 사이버 시스템에서 생성되며 이의 생성에 사용되는 장치 및 시스템의 보호는 사이버보안의 일부로 간주

출처 Reproduced from [5-10].

협이 사람의 생명을 직접 위협하는 수준까지 확대된 것으로 알려져 파장이 컸다[2]. 가상자산 탈취로 인한 금전적인 피해 발생뿐만 아니라 개인정보 유출 등에 따른 사회적 혼란 역시 확대되고 있어 디지털화 진전에 따른 경제적 번영과 혜택의 전제가 사이버공간 전반의 안전성과 신뢰성 확보라는 점을 확인하였다.

사이버공간 관리 및 보안을 둘러싼 방대하고 복잡한 문제의 해결을 위해서는 공공, 민간 및 국제 이해 당사자 간의 협력이 필수적이며, 이러한 노력이 상호 강화되도록 조정이 필요하다. 그리고 이 조정의 중심에 국가사이버보안 정책이 있다.

본고는 날로 중요성을 더해가는 사이버공간의 보안 문제에 대한 개념을 정리하고, 주요국 국가전략 및 투자 방향을 조사·분석하여 향후 우리나라 사이버보안 전략 방향 수립을 위한 시사점을 도출한다.

II. 사이버보안 개념 및 현황

1. 사이버보안 개념

"사이버보안(Cybersecurity)" 문제가 갖는 본질적인 복잡성으로 인해 글로벌 공감대를 형성하는 단일 정의는 아직 존재하지 않는다[3,4]. 다만 각국의 정책입안자 및 관련 전문가들이 적용 분야와 상황에 따라 용어를 정의 후 활용하고 있어 이를 통해 개념을 가늠할 수 있다.

미국 연방정부는 국립표준기술연구소(NIST)를 통해 국제적으로 준용되는 사이버보안 분야 표준 및 지침을 제공 중이며, 이를 통해 표 1과 같은 다양한 사이버보안 개념들을 확인할 수 있다[5-10]. 분야별로 다소 차이는 있으나, 사이버보안을 가용성, 무결성, 인증, 기밀성 및 부인 방지를 보장하기 위해 각종 시스템 및 정보를 보호하거나 방어하는 역할로 정의한다.

국내에서는 과학기술정보통신부가 공고한 「정보보호산업의 진흥에 관한 법률(법률 제19351호)」의 "정보보호"가 유사한 개념이다. 정보보호는 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지 및 복구하고, 암호·인증·인식·감시 등의 보안기술을 활용하여 재난·재해·범죄 등에 대응하거나 관련 장비·시설을 안전하게 운영하는 것을 말한다[11]. 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 「정보통신망

이용촉진 및 정보보호 등에 관한 법률(법률 제18871호)」에 규정된 정보통신망을 포함하는 주요정보통신기반시설의 경우 「정보통신기반 보호법(법률 제18870호)」에 따라 전자적 침해행위에 대비한 별도의 보호 대책을 수립해 시행하고 있다[12,13].

그 외 국가정보원 「사이버안보 업무규정(대통령령 제31356호)」에서 "사이버안보 업무"로 국제 및 국가 배후 해킹조직 등 사이버안보 관련 정보의 수집·작성·배포와 중앙행정기관 등을 대상으로 하는 사이버 공격·위협에 대한 예방 및 대응을 포함해 규정한다[14].

본고는 사이버보안, 정보보호, 사이버안보 등으로 다양하게 언급되는 관련 용어를 "사이버보안(Cybersecurity)"으로 통칭하되 그 다양성과 복잡성을 고려해 단일한 개념으로 재정의하지는 않는다. 다만 디지털 심화 시대의 핵심 기반이자 국가안보적 중요성이 있는 필수 전략기술 부문임을 고려해 포괄적 관점으로 접근한다.

2. 국내 사이버보안 정책 현황

가. 거버넌스

국내 사이버보안 거버넌스는 현재까지 공공, 국방, 민간으로 구분하여 각각 국정원, 국방부, 과학기술정보통신부가 부문별로 대응해왔으며, 이러한 체계를 범정부 통합 대응 조직으로 모으고자 하는 움직임이 있다[15-19].

'22년 11월, 국가정보원이 입법 예고한 「국가사이버안보기본법안」 역시 이러한 움직임의 일환이다. 법안 심사 절차를 거쳐야 하는 과제로 실제 추진까지는 시일이 있으나, 법안 제목부터 거버넌스 구현 전반에 대한 관계자들의 이견이 있는 것으로 알려졌다[20].

통합대응 조직 마련이 범정부 관점의 협력체계를 공고화하는 본연의 목표를 반영해 추진될 수 있도록 도입 과정에서 세심한 조율과 검토가 필요한 것으로 파악된다.

나. 정책 동향

우리나라는 '22년 5월, 윤석열 정부 출범과 함께 표 2와 같이 사이버보안을 국정과제 내 포함하고, 범정부 협력체계 강화 및 기술패권 대응을 위한 준비를 본격화하였다. 국내 사이버보안 정책의 큰 흐름은 보안을 강화하되 이러한 변화가 산업 성장을 저해하지 않도록 다양한 산업 육성 정책을 병행 도입한다는 점이다.

제로 트러스트(Zero Trust) 신 보안체계 도입의 본격 검토는 보안 강화의 한 방편으로 두드러진다. 제로 트러스트는 신뢰성이 보장되지 않은 네트워크에서 서버, 데이터베이스 등 다양한 컴퓨팅 자원에 대한 지속적인 접근 요구에 최소한의 권한을 부여하고 동적 인증을 통해 접근 허가를 허용하는 방식이

표 2 국내 사이버보안 주요 정책 동향

연혁	전략	세부 내용
'22.05.	국정과제	범정부 차원 협력체계 공고화, 국가안보 태세 유지, 산업, 기술, 인재 경쟁력 제고
'22.09.	대한민국 디지털 전략	원천기술 확보, 4대 방어기술(억제, 보호, 탐지, 대응) 개발, 사이버戰 대응역량 확보
'22.10.	국가전략기술 육성방안	데이터·AI 보안, 네트워크·클라우드 보안, 디지털 취약점 분석·대응(공급망 보안), 신산업·가상융합 보안
'23.04.	전략적 사이버안보 협력 프레임워크	한·미 동맹의 안보 영역을 사이버공간까지 확장, 사이버 위협으로부터 국가 중요 인프라 보호

출처 Reproduced from [15-18].

다[21]. ’23년 관련 솔루션 개발 및 실증사업 추진, 안내서 개발 등 정책을 지원할 예정이다[22].

정보보호 대응체계도 고도화되는 추세다. ’22년 하반기 이후 국가중요기반시설을 확대 지정하여 보호 대책을 강화하고, 중소기업 등 정보보호 역량이 상대적으로 취약한 부문에 대해 찾아가는 보안서비스를 확대하는 등 예방 체계를 강화하고 있다[23].

산업 육성을 위한 규제개선 정책도 다양하다. 위장처리 등 사전 보안 처리가 필요한 국가 위성 정보 해상도 규제를 완화하여 위성 정보 활용 산업을 활성화하고, 클라우드 보안 인증을 상·중·하의 3등급으로 구분하여 등급별 차등화된 보안기준을 적용한다. 민감정보를 다루는 클라우드는 보안성을 높이고 보안위험이 상대적으로 낮은 공개 데이터를 다루는 클라우드의 보안 위협을 완화하는 방향이다. 평가 기준이 없어 인증을 획득하기 어려웠던 신기술 제품들에 대해 정보보호제품 신속확인제를 도입하여 혁신적인 제품을 빠르게 국방 등 민간기관 외 국가·공공기관에 도입할 기회도 확보한다. 신규 보안 위협에 선제적으로 대응 가능한 제품의 등장을 촉진해 보안을 강화할 뿐만 아니라 관련 기업 육성의 단초를 확보하기 위한 목적이다[24,25].

다. 투자 방향

’23년 과학기술정보통신부 예산 중 정보보호 및 보안과 관련된 예산은 264억 원으로 알려졌다. 정보보호 인력양성에 163억 원, 정보보호 시스템 평가 및 인증기반 강화에 22억 원, 디지털 융합보안 기반-디지털 안전 선도모델 개발에 38억 원, 디지털 융합보안 기반-양자기술 상용화 기반 조성에 41억 원이 배정된다[26].

또한, 사이버보안 패러다임 전환에 따른 기술패권 경쟁 대응을 본격화하기 위해 총 5년간 3,917억 원 규모의 예비타당성 사업 기획을 추진한다[27]. 사이버 위협 대응체계를 기존 보호, 탐지 위주의 수세적 방어 형태의 대응전략을 넘어 위협 행위자의 식별, 사전 예방적 조치 강화 등 보다 능동적·적극적인 형태로 전환하기 위한 것으로 공격 억지, 선제면역, 회복 탄력, 기반 조성의 총 4개 전략 분야에 대해 대비한다. 최종 통과까지 시일은 소요되겠지만, 날로 중요성을 더하는 사이버보안 분야 대응을 위한 기반 조성 준비를 시작했다는 점에서 의의가 높다.

III. 주요국 사이버보안 전략

1. 미국

가. 거버넌스

대통령을 최고 책임자로 하고, 국가안전보장회의(NSC)의 감독하에 국가사이버국장실(ONCD)이 사이버보안전략 및 이행계획을 개발하며, 관리예산국(OMB)과 협력해 이행을 조정한다[28]. 과학기술정책실(OSTP)은 과학기술 혁신 기반의 보안 전략을 담당하며 현재 및 혁신기술의 평가, 개발, 배치 및 거버넌스를 통해 사이버보안 기술의 국제 경쟁력을 강화하고 치명적 위험을 감소하는 데 집중한다. 사이버보안 및 인프라 보안국(CISA)이 사이버 방어, 중요 인프라 보안 및 탄력성 확보를 위한 역할을 맡고 있다[29].

나. 정책 동향

바이든 행정부는 ’23년 3월 새로운 ‘국가사이버보안전략’을 발표했다. 기존 ’18년 전략대비 기술생태계의 보안과 탄력성 확보 및 회복력 있는 미래를 위한 투자 비중 확대가 두드러진다.

먼저, 기술생태계의 보안과 탄력성 확보를 위한 방안으로 개인정보보호 권리 보장, IoT 보안 및 민간과 정부 간 보안 책임을 보다 명확히 하기 위한 노

력을 담는다. 보안 책임을 개인 사용자나 소규모 조직에 지나치게 전가하고 있는 구조적 차원의 문제를 다룰 뿐만 아니라 사이버공간에서의 무책임한 행동에 대해 국가에 책임을 묻고, 배후에 있는 범죄자 네트워크를 와해시키는 등의 적극적, 능동적 대응을 포함한다.

특히 소프트웨어 공급망 보안 강화 관련 이슈가 주요 주제로 다루어졌다. 안전한 개발 관행을 통한 소프트웨어 공급망의 보안 및 일련의 조치를 강화하는 추세에 따라 사이버 위협에 대한 연방 기술의 탄력성을 증가시키면서 기관 네트워크에서 검증되지 않은 기술을 활용하는 데 따른 위험을 최소화하는 데 중점을 두고 있다. 일례로 '23년 2월, 대통령실은 정부 장치에서 틱톡(TikTok)을 없애기 위한 각서를 발표했다[30]. 이에 정부 장치에서 틱톡 및 바이트댄스 유한회사(ByteDance Limited) 또는 이의 소유 법인이 개발하거나 제공하는 틱톡의 모든 후속 응용 프로그램이나 서비스가 금지되며, 관리예산국장은 CISA, 국가정보국장 및 국방부 장관 등과 협의하여 연방정보기술에서 틱톡을 제거해야 하는 기관을 위한 표준 및 지침을 개발하도록 하고 있다.

회복력 있는 미래를 위한 준비사항으로 글로벌 상호운용성과 표준 촉진, 양자정보시스템 및 인공지능을 포함한 컴퓨팅 기술, 생명공학 및 바이오 제조, 청정에너지 기술의 보안에 대한 투자 촉진 및 연구개발, 그리고 양자 이후 암호화로의 전환을 위한 계획 수립을 장려한다. 그 밖에도 클라우드 기반 기술과 장치 관련 보안 강화 및 디지털 ID 개발과 활용을 위한 생태계 구축 지원, 기타 인재 양성 관련 사항들을 다루고 있다[31].

특히 양자 이후 암호화 메커니즘으로의 전환 흐름에 주목할 필요가 있다. 양자컴퓨팅은 다양한 이점에도 불구하고, 국가 경제 및 안보에 심각한 위협을 초래할 것으로 예상되며, 충분한 크기와 정교함을 갖춘 암호분석 관련 양자컴퓨터 CRQC는 공개키 암호화 기법의 대부분을 해독할 수 있는 것으로 알려졌다. 따라서 CRQC가 사용 가능해지면 민간과 군사 통신을 위태롭게 하고, 중요한 인프라에 대한 감독이나 제어시스템을 약화하며, 대부분의 인터넷 기반 금융 거래에 대한 보안 프로토콜을 무력화할 수 있다. 이러한 위험에 대비하기 위해 미국은 2035년까지 암호화 시스템을 양자 후 암호화 체계로 순차 전환하고자 준비 중이다[32].

다. 투자 방향

미국은 '21년 5월 발표한 행정명령 14028 '국가 사이버보안 개선(Improving the Nation's Cybersecurity)'에 따라 패러다임 전환을 시작했다[33]. 정교해지는 사이버 공격에 대비하기 위해 보안을 최우선과제로 하여 연방 시스템 보호 강화 및 정부-민간 부문 간 정보 공유를 개선하고 전반적인 사이버보안 능력을 강화하는 것이 골자다. 이후 연방정부의 투자 역시 이와 일관된 방향으로 추진하고 있다.

국방 부문을 제외한 민간 부문 사이버보안 활동 관련 '24년 회계연도 지출은 전년 대비 13.7% 증가한 약 127억 달러 규모로 예상된다. 이 중 정부 부처 예산은 전체의 95% 규모인 121억 달러로, 국토안보부, 법무부, 재무부와 같이 중요 정보를 다루는 부처의 예산 비중이 크다. 표 3[34]과 같이 보호와 대응 부문의 예산 증가율이 상대적으로 높다. 보호는 악의적인 사이버 활동에 효율적으로 저항하고 정보의 공개나 변경을 방지하며, 무결성과 신뢰성을 유지하고 보안 제어와 대책의 유지, 평가 및 적용에 필요한 프레임워크를 구축하며, 승인된 사용자가 필요로 하는 때만 자원에 접근하거나 사용할 수 있게 하는 기능으로 제로 트러스트 구현 등과 관련이 높다. 데이터 침해나 기타 사이버보안 사고에 대해 포렌식 등을 통한 대응을 위한 일련의 준비 또는 조치사

표 3 NIST 프레임워크 활동별 부처 예산(백만 달러)

기능	FY 2023	FY 2024	증감(%)
식별(Identify)	3,435	3,500	1.9
보호(Protect)	4,392	5,058	15.2
탐지(Detect)	1,148	1,266	10.3
대응(Respond)	1,410	1,637	16.1
복구(Recover)	315	344	9.2
우선순위 관련	-	366	신규
부처 소계	10,700	12,170	13.7

출처 Reproduced from [34].

항 역시 강화될 것으로 예상된다.

투자 방향성은 관리예산국(OMB)과 국가사이버국장실(ONCD)이 공동 검토한 사이버투자 우선순위를 통해 더욱 명확히 알 수 있다. 표 4[34]와 같이 우선순위 관련 신규 배정 예산을 활용해 크게 정부 네트워크 방어 및 복원력 개선, 중요 인프라 방어를 위한 교차 부문 협력 심화, 디지털 기반 미래강화 부문에 투자한다.

R&D 우선순위 역시 큰 흐름에서 벗어나지 않는다. '24년 회계연도 예산에 대한 다중 기관 연구 및 개발 우선순위는 탄력적이고 안전한 통신을 우선시하고, 사이버 공격 및 공급망 공격으로부터 중요한 인프라와 민감한 네트워크를 방어하는 데 초점이 있다. 이를 위해 사이버보안의 기본 요소들, 개선된 인증 메커니즘, 제로 트러스트 아키텍처, 임베디드 시스템의 보안 및 복원력, 중요 인프라에 대한 이상 탐지, 소프트웨어 보안 및 침입 탐지에 대한 지원을 추진한다[35].

2. 유럽연합(EU)

가. 거버넌스

EU 집행위원회의 위원장을 최고 책임자로 정책적 의사결정을 진행하며, 그 결과를 반영해 유럽정보보호원(ENISA)이 범유럽 사이버보안 전략을 기획한다. 사이버 공격 대응, 중요 인프라 보안 및 탄력성 확보를 위한 역할은 유럽사이버보안센터(CERT-EU)가 수행한다[36].

'23년 4월, 기존 범유럽 사이버 위협 대응 협력체계의 근간이던 보안 연합(Security Union) 개념을 구체

표 4 2024 회계연도 사이버보안 투자 우선순위

투자 우선 분야		세부 내용
정부 네트워크 방어 및 복원력 개선	제로 트러스트	연방시스템의 방어력 향상을 위해 시스템 접근자에 대한 신뢰를 지속 평가 예정으로 FY 2024까지 목표 구현
	IT의 현대화	제로 트러스트 기반 클라우드 채택, 연방 차원의 제품, 서비스 및 표준 개발 배포, 공유 보안 기술 활용 및 NIST 보안 소프트웨어 개발 프레임워크 및 관련 지침을 소프트웨어 조달 및 개발 관행에 통합하는 등의 설계 기반 현대화 추진
중요 인프라 방어를 위한 부문 간 협력 심화	위험 관리 기관(SRMA)	SRMA와 CISA 및 연방사이버센터 등 기관 간 정보 공유 및 협력 공고화로 각 부문 내 집단적(정부 및 산업) 방어, 대응 및 복원력 향상
디지털 미래기반 강화	인프라 투자	사이버보안 위협을 해결하기 위한 프로젝트 검토 및 평가 지원, 기존 표준이 부족한 인프라 투자를 위한 성능 표준 개발 등 설계 및 구축 단계 전반 개선
	인적 자본	인사관리담당자 또는 최고정보책임자가 IT 및 사이버 전문가를 고용 및 교육할 수 있는 자원을 확보하고 관련 인력을 유지할 수 있도록 권한 지원
	기술 생태계	공급망을 위협하는 대상 품목 제거 또는 해당 품목의 특정 출처를 제외하는 방법에 관한 권장 사항을 만들기 위한 연방 조달 보안 위원회(Federal Acquisition Security Council) 설립 및 관련 투자

출처 Reproduced from [34].

화하여 'EU 사이버 연대법(European Cyber Solidarity Act)'을 채택했다[37]. 한층 강화된 거버넌스하에 사이버 위협 사건에 대한 범유럽 차원의 탐지 및 상황 인식 체계를 확보할 예정이다. 유럽 사이버 쉴드(European Cyber Shield)를 구축하고, 중대·대규모 보안 사고 대응 및 즉각적 복구를 위한 사이버 비상 메커니즘을 도입하는 것이 핵심이며, 관련 자금 지원을 명시하였다[37-42]. 부처 간 통합을 넘어 범유럽 차원의 대응을 위한 실행 도구로 상호 신뢰 관계와 정보 공유의 중요성을 강조한다[37].

나. 정책 동향

러시아-우크라이나 전쟁이 사이버전으로 확대되며 랜섬웨어 등으로 우크라이나 기반시설이 공격당했다. 이 사건으로 국가 간 중요 인프라의 연결성이 높은 유럽 역시 사이버 공격이 확산할 경우 상당한 타격을 입을 수 있다는 인식을 강화하는 계기가 되었다[40]. 이후 표 5와 같이 사이버보안 정책을 강화해 대응 중이다.

설비제어 관련 제품 및 서비스는 플랜트 산업뿐만 아니라 전력망, 상수도 네트워크 등과 같은 국가 중요 인프라에도 활용되고 있어 침해 시 파급력이 크므로 잠재적인 사이버 공격 고위험 부문으로 포함하고 제로 트러스트를 도입하여 네트워크 방어 및 복원력을 확보할 계획이다[38,39].

또한, 에너지, 디지털 인프라, 운송, 우주 부문 등, 국가 중요 인프라에 한해서는 사이버공간의 안전이 물리적 공간과 동등한 수준으로 보호되어야 한다고 인식해 모든 유형의 위협으로부터 안전을 확보할 수 있도록 준비하고 있다[41,42].

소프트웨어 공급망 보안에 대한 대책 필요성도 강조된다. '22년 9월에 발의된 '사이버복원력법'은 모든 디지털 제품에 소프트웨어 또는 서비스 개발에 사용된 모든 종류의 소프트웨어 정보를 담는 소

표 5 EU 사이버보안 주요 정책

연혁	핵심내용
'22.09.	EU 사이버복원력법(Cyber Resilience Act) 채택
	유럽 에너지 인프라를 표적으로 하는 랜섬웨어 공격 우려를 반영하며 디지털 요소를 포함하는 제품의 설계 및 개발 과정에 사이버보안 기준 준수 의무화
'22.11.	EU 사이버방어정책(EU Policy on Cyber Defence) 발표
	러시아의 우크라이나 침공으로 인해 증가하는 전력 및 에너지망, 네트워크, 운송 인프라, 우주 자산 등의 국가 중요 인프라에 대한 사이버 위협 대응과 위기관리 능력 강화
'22.12.	사이버보안지침 개정안(Network and Information System Directive 2.0) EU 관보 게재
	국가 중요 인프라를 새로운 규범 적용 대상에 포함하여 제로 트러스트 아키텍처와 AI 도입 추진
'22.12.	핵심 시설의 복원성 지침(Critical Entities Resilience Directive) EU 관보 게재
	국가 중요 인프라의 위협 유형으로 자연재해, 테러, 내부 위협 등과 함께 사이버보안을 포함하고 능동적이고 선제적인 대응 조치 강조
'22.12.	EU 보안연합전략 5번째 경과 보고서 발표
	NIS2 지침과 CER 지침을 보완하며 에너지, 디지털 인프라, 운송, 우주 부문에 우선하여 사이버보안 수준과 사이버 복원력 강화
'23.04.	EU 사이버연대법 채택
	사이버공격 피해의 신속한 복구를 위해 응집력 있는 협력 네트워크를 강조하며 AI 기반의 첨단 사이버 위협 플랫폼인 보안관제센터 네트워크를 구축하고 대규모 사이버 공격을 대비한 유럽 사이버 비상 협력 메커니즘 운영 예정

출처 Reproduced from [37-42].

표 6 EU 사이버보안 관련 기관별 예산(백만 유로)

구분	FY 2021	FY 2022	FY 2023
유럽 법집행협력청 (EUROPOL)	178.31	197.76	208.21
유럽 연구책임운영기관 (REA)	88.44	98.41	107.57
유럽 정보보호원 (ENISA)	24.48	38.63	22.25
유럽 경찰대학 (CEPOL)	9.38	10.85	11.21
총 예산	300.61	345.65	349.24

출처 Reproduced from [44-48].

프트웨어 자재 명세서(SBOM) 제출을 의무화했다[39]. 특히 공공서비스에 활용 중인 공개 소프트웨어 공급망 강화가 시급하다고 판단하여 '22년 2월부터 관련 시범 프로젝트를 수행 중이다[43].

다. 투자 방향

유럽 정보보호를 담당하고 있는 기관들의 예산은 표 6[44-48]과 같이 꾸준히 증가하는 추세로 실질적인 전략 이행을 위한 노력이 강화되고 있다.

EU의 사이버보안 관련 R&D는 호라이즌 유럽(Horizon Europe)의 투자 방향과 우선순위를 통해 그 핵심 방향을 살펴볼 수 있다.

표 7[49]에서 보듯이, 사이버보안 역량 개선(Increased Cybersecurity)을 목표로 '23년과 '24년 모두 사이버보안 플랫폼과 보안위협 모니터링 시스템 개발에 높은 우선순위를 두고 있으며, 이는 범유럽 통합 관제센터 운용 계획이 반영된 결과로 보인다. 인증, AI, 양자 이후 암호화 등 차세대 보안 기술 확보에도 예산을 투자한다.

투자 우선 분야 세부내용 외에도 '23년 1월부터 2년간 5.6백만 유로를 투입하여 디지털로 연결된 의료 기기의 사이버보안을 강화하고 제로 트러스트를 구현하는 ENTRUST 프로젝트가 추진 중이다[50]. '21년 12월부터 '23년 3월까지 1.4백만 유로를 투자해 블록체인 기반의 분산형 소프트웨어 자재 명세서(D-SBOM)를 개발하는 과제도 추진 중으로 다양한 분야에서 새로운 기술 도입을 시도하고 있다[51].

표 7 2023-2024 회계연도 Horizon Europe 사이버보안 투자 우선순위(Increased Cybersecurity 부문)

투자 우선 분야		세부 내용
FY 2023	1순위 (2,800만 유로)	보안 시스템, 보안 플랫폼, 디지털 인프라 분야
		중요 인프라의 사이버 복원력 지원 도구, 제로 트러스트 아키텍처, IoT 보안, AI 기반 사이버 위협 인텔리전스, 통신, 데이터 수집, 데이터 전송 및 처리를 포괄하는 보안 인프라
	2순위 (1,570만 유로)	개인정보 보호 및 인증 관리 기술
		개인정보 보호 및 ID 관리 기술 개선, 개인정보 보호 및 ID 관리 기술 사용성 개선, 개인정보 보호 기술 설계
	3순위 (1,500만 유로)	강건한 AI 시스템의 보안 기술
		적대적 공격에 대한 AI 보안 설계와 복원력 지원기술 개발, 복원력을 극대화하기 위해 머신러닝에 컨텍스트 인식 기술의 개발 중요성 강조
FY 2024	1순위 (3,700만 유로)	보안 위협 평가 도구의 개발
		복원력 있는 시스템 설계, 취약성, 소프트웨어 분석, 취약성 발견 및 동적 보안 평가에 대한 체계적이고 자동화된 연구, 신뢰할 수 있는 인증 기술의 개발, AI 기반 보안 서비스(이상 탐지, 예측 등)
	2순위 (2,340만 유로)	암호화
		양자 이후 암호화 알고리즘 구현, 양자 이후 알고리즘의 단계적 전환 추진

출처 Reproduced from [49].

3. 일본

가. 거버넌스

일본은 사이버보안 정책을 효과적으로 추진하기 위해 내각 총리를 최고 책임자로 산하에 사이버보안전략본부(Cybersecurity Strategic Headquarters, 이하 전략본부)를 설치 후 운영 중이다. 국가안보위원회(NSC)와 협업할 뿐만 아니라 디지털 전환을 추진 중인 디지털 에이전시(Digital Agency)와 정책 수립을 위해 긴밀히 협업하며 자유롭고 공정하며 안전한 사이버공간 확보를 위해 정부 역량을 결집한다[52]. 전략본부 산하 사이버보안센터(NISC)가 사무국 역할을 수행하며 금융 기관, 문부 과학성 등 유관부처와의 협업을 지원하고, 정부보안운영조정팀(GSOC), 사이버사건모바일지원팀(CIMAT) 등을 운영하며 실무를 지원한다.

나. 정책 동향

'21년 9월 28일, 일본은 디지털 전환과 사이버보안을 동시에 발전시키고, 사이버공간의 전반적인 안전과 보안을 보장하며 국가안보 관점의 추진력을 강화하기 위해 표 8과 같이 사이버보안 전략을 개정 발표하였다[53].

'22년 6월, 정보통신, 금융, 항공, 공항, 철도, 전력, 가스, 정부 행정 서비스, 의료, 수도, 물류, 화학, 신용, 석유 등 14개 국가 중요 인프라에 대한 사이버 공격의 파급력을 고려하여 관련 행동계획도 수립하였다. 장애대응체계 강화, 안전기준 등의 정비, 정보공유체계 강화, 리스크 관리, 방호기반 강화를 골자로 다양한 대비책을 마련하였으며 정부가 주도하되 중요 인프라 사업자 등이 자주적이며 적극적으로 사이버보안 확보를 위해 노력할 것을 규정한다[54].

'22년 10월 문부과학성은 디지털 사회 실현을 위한 중점계획 각료회의 결정에 따라 문부과학성의 향후 5개년 중장기계획도 발표했다. 바람직한 디지털 사회의 실현을 위해 각 부처에서 취급하는 정보자산을 모두 조사하고 분석한 뒤, 사이버공격으로 자산이 탈취되었을 때 초래하는 위험 수준을 평가하고 기존에 운영하고 있던 클라우드 기반 인증 서비스인 행정정보시스템 중 고위험 시스템을 대상으로 제로 트러스트 기반 인증체계를 도입하고 점차 확대할 예정이다[55].

다. 투자 방향

'23년 일본 정부의 사이버보안 예산은 표 9[56]에서 보듯이 총 1,379억 엔 규모로, '21년 814.6억 엔

표 8 일본 사이버보안 전략 2021 세부시책

목표: 경제사회 활력 제고 및 지속적 발전 방향: 디지털 전환과 사이버보안의 동시 추진	목표: 안전·안심 사회 실현 방향: 공공 공간화와 상호 연계, 통합적 안전·안심 확보
• 경영층 의식 개선 • 지역·중소기업의 디지털 전환과 사이버보안 지원 • 공급망 신뢰성 확보를 위한 기반 조성 • 디지털/보안 리터러시의 향상과 정착	• 국민·사회를 지키기 위한 사이버보안 환경 제공 • 디지털 개편 방향과 일관된 사이버보안 확보 • 정부기관 등 중요 인프라, 대학·교육연구기관 등 대응 강화 • 기관 간 정보 공유·연계와 사이버공격 대비 강화
목표: 국제사회의 평화 안정 및 국가안보 방향: 안전보장의 관점에서 대처 강화	기타: 횡단적·중장기적 시점의 시책
• 자유·공정하고 안전한 사이버공간 확보 • 방어력·억제력·상황 파악력 강화 • 국제 간 협력·연계	• 연구개발 추진 • 인재 확보, 육성, 활약 촉진 • 산학관 협력 강화 및 기술확산 제고

출처 Reproduced from [53].

표 9 정부 사이버보안 예산 부처별 비중(%, 억 엔)

구분	2021	2022	2023
방위성	37.1%	37.5%	64.0%
총무성	19.2%	19.1%	10.4%
문부과학성	13.0%	13.4%	8.1%
디지털청†	–	10.2%	6.0%
경제산업성	5.7%	5.5%	3.3%
경찰청	2.7%	5.5%	2.9%
후생노동성	2.7%	2.3%	1.9%
국토교통성	0.3%	1.0%	0.8%
내각관방	2.1%	2.1%	0.6%
외무성	0.6%	0.9%	0.5%
총 예산(억 엔)	814.6	919.3	1,378.9

출처 Reproduced from [56]. †: 디지털청은 2022년 신설됨

에 비해 크게 확대되었다. ’23년 예산 중 방위성의 비중이 큰 폭으로 증가한 점이 눈에 띈다[56].

’21년 R&D 투자 계획에 따르면 가까운 시일 내 사이버공간과 물리 공간을 융합하는 디지털 전환을 우선 추진할 계획이다[57]. 이 과정에서 네트워크 인프라 기술의 고도화와 신뢰성 확보를 동시에 추진할 계획이다.

양자 기술에 관한 기초연구와 함께 AI를 사이버보안 분야에서 적극적으로 활용할 계획이다. 디지털 전환 과정에서 보안 취약점이 많아질 수 있고 공격자의 수법도 고도화되고 있어 AI를 활용한 대응법 마련에 관심이 크다[57].

’22년 6월 내각부의 통합혁신전략추진회의는 ‘AI 전략 2022’를 발표하며 국가적 위기에 대한 대응력을 강화하는 목적으로, 자연재해와 같은 물리적 피해뿐만 아니라 설명 가능한 AI에 의한 보안 기술의 확립과 멀웨어 등 사이버공격에 빠르게 대응할 수 있는 자연어처리 모델의 기술개발을 계획하고 있다[58].

Ⅳ. 결론

디지털 기술로 구현된 사이버공간의 영역은 물리적 영역 못지않게 중요해지고 있다. 사이버공간에서 발생하는 피해는 재정적 손실로 이어지고 사회적 혼란을 촉발할 수 있어 국가 차원의 관리가 필요하다. 국가별 다소 차이는 있으나 개별 부처가 아닌 국가 차원의 역량을 결집해 지휘부를 중심으로 종합 대응하는 방향으로 거버넌스를 강화하는 추세

표 10 사이버보안 주요국 사례 비교

국가	거버넌스	정책 동향	투자 방향
미국	• 대통령(최고책임자) • 국가안전보장회의(최상위기관) • 국가사이버국장실(전략기획) • 사이버보안 인프라 보안국(전략실행)	• 기술생태계의 보안 및 탄력성 확보 • 보안 책임의 재배분 • 소프트웨어 공급망 보안 강화 • 상호운용성과 표준 촉진 • 양자 후 암호화 체계 확보	• 제로 트러스트 • IT 기반 현대화 • 네트워크 방어 및 복원력 개선 • 디지털 기반 강화 • 연방보안 조달 위원회 설립
유럽	• EU집행위원장(최고책임자) • EU집행위원회(최상위기관) • 유럽정보보호원(전략기획) • 유럽사이버보안센터(전략실행)	• 사이버보안 기준 준수 의무화 • 사이버위협 방어체계 강화 • 국가 중요 인프라 보호 • 소프트웨어 공급망 보안 강화 • 협력 네트워크 강화	• 제로 트러스트 • 소프트웨어 자재 명세서 • 위험 관리 및 평가 • 강건한 AI • 암호화 구현
일본	• 내각총리(최고책임자) • 내각관방(최상위기관) • 사이버보안 전략본부(전략기획) • 사이버보안센터(전략실행)	• 디지털 혁신과 사이버보안 역량 동시 확보 • 국가 중요 인프라 보호 • 장애대응체계 강화 • 정보공유체계 강화	• 제로 트러스트 • 위험 관리 및 평가 • 양자 및 AI 등 혁신기술 도입

다. 관련 부처 간 협력을 강화하고 상시 협의를 통해 국가 차원의 전략 및 정책을 정비할 뿐만 아니라 미래에 대비한 투자 방향을 수립하는 작업도 빠르게 진행 중이다.

본고는 사이버보안 정책이 비단 한 국가만의 문제가 아닌 국가 간 협력이 있어야 하는 주제임을 고려하여 표 10과 같이 우리나라와 밀접한 관계를 맺고 있는 미국, 유럽, 일본의 사이버보안 정책 동향을 조사하였다.

거버넌스 측면에서는 사이버보안 최고 책임자로 대통령, EU집행위원장, 내각관방장관 등 국가 최상위 지도부가 담당하고 있으며 관련 법령을 통해 체계적으로 역할을 부여해 일사분란한 대응체계를 갖추고 있음을 확인할 수 있다. 우리나라는 현재 거버넌스 관련 논의를 추진하고 있는 단계로 빠른 대응이 필요하다.

정책적으로는 기술생태계 전반의 보안 및 탄력성 확보, 보안 책임 강화, 국가 중요 인프라에 대한 보호 강화, 소프트웨어 공급망 강화 및 정책의 실효적 추진을 위한 참여 기관 간 정보 공유 강화 등이 두드러진다. 보안 강화를 위해 다양한 대응체계를 마련하고 규제 개선을 추진 중인 우리나라의 방향과도 큰 차이는 없으나, 추진 과정에서 국가 간 협력을 기반으로 하는 다양한 도입 표준이 나타날 수 있으므로 진행 추이를 지켜보며 국제 간 협력을 강화할 필요가 있다.

디지털화 진전을 전제로 제로 트러스트의 광범위한 도입, 소프트웨어 조달과 관련한 다양한 이슈에 대한 대응책 마련, AI와 양자 이후 암호화 등 신기술 대응 방안 마련 등에 향후 수년간 투자가 집중될 예정으로 우리 역시 관련 체계 마련 및 대응에 나서야 할 때이다.

사이버공간의 안전과 신뢰 확보는 선택지가 아니라 국가의 안위를 위한 필수적 기반으로 발빠른 대응이 시급하다.

용어해설

랜섬웨어 보안 취약점을 악용하여 네트워크 시스템을 이용 불가능하게 만들고 다시 액세스하기 위한 암호 해독 키를 제공하며 몸값을 요구하는 사이버공격 유형

소프트웨어 공급망 위협 타사 구성요소 및 오픈 소스 소프트웨어와 같이 소프트웨어에 의존성을 갖는 모든 경로의 요소를 통한 사이버공격 유형

양자컴퓨터 중첩 및 얽힘과 같은 양자 역학 현상을 활용해 기존 컴퓨터보다 기하급수적으로 빠르게 정보를 처리하는 고급 컴퓨팅 시스템

약어 정리

CIMAT	Cyber Incident Mobile Assistant Team
CISA	Cybersecurity and Infrastructure Security Agency
CRQC	Cryptoanalytically Relevant Quantum Computer
ENISA	European Union Agency for Network and Information Security
EU	European Union
FY	Fiscal Year
GSOC	Government Security Operation Coordination Team
IoT	Internet of Things
NISC	National center of Incident readiness and Strategy for Cybersecurity
NIST	National Institute of Standards and Technology
NSC	National Security Council
OMB	Office of Management and Budget
ONCD	Office of the National Cyber Director
OSTP	Office of Science and Technology Policy
SBOM	Software Bill of Materials
SRMA	Sector Risk Management Agencies

참고문헌

[1] Strategic Intent Statement for the Office of the National Cyber Director, ONCD.

[2] KISA, "2022 하반기 사이버 위협 동향 보고서," 2022. 12.
[3] 세계법제정보센터, 사이버안보법제 고찰, 2018.
[4] FAS, Cybersecurity: A Primer, CRS, 2022. 12. 8.
[5] NISTIR 8183, 2017.
[6] NIST SP 800-160 Vol. 2 Rev. 1, 2021.
[7] CNSSI 4009의 사이버 보안에 따른 NISTIR 8170, 2020.
[8] NISTIR 8074 Vol. 2, 2015.
[9] NISTIR 8323r1, 2023.
[10] NIST SP 800-53 Rev. 5, 2020.
[11] 정보보호산업의 진흥에 관한 법률(법률 제19351호).
[12] 정보통신망 이용촉진 및 정보보호 등에 관한 법률(법률 제18871호).
[13] 정보통신기반 보호법(법률 제18870호).
[14] 사이버안보 업무규정(대통령령 제31356호).
[15] 제20대 대통령직인수위원회, "윤석열정부 110대 국정과제," 2022. 5.
[16] 관계부처 합동, 대한민국 디지털 전략, 2022. 9.
[17] 과학기술정보통신부, 기술주권 확보를 통한 과학기술 G5 도약, 국가전략기술 육성 방안(안), 2022. 10. 28.
[18] 대통령실 보도자료, 한미 정상, 전략적 사이버안보 협력 문서 채택, 2023. 4. 27.
[19] 한국형사법무정책연구원, "「국가사이버안보 대응 역량강화」 국정과제 이행을 위한 법제기반 체계적 정비," 2022. 8.
[20] Newstof, "[윤석열미터 1년] 사이버안보기본법·통합방위법 제·개정 → 진행중," 2023. 4. 17.
[21] NIST SP 800-207.
[22] 과학기술정보통신부, 제로 트러스트 신보안체계 도입 본격 지원한다!, 2023. 4. 26.
[23] 과학기술정보통신부, 금품요구악성프로그램 대응체계 고도화 지혜 모은다, 2022. 9. 20.
[24] 과학기술정보통신부, 보안 규제개선으로 혁신적 신기술·서비스 공공도입 촉진, 2022. 8. 18.
[25] 과학기술정보통신부, 공공시장에 진출 가능한 정보보호 신속확인제품 첫 출시, 2023. 4. 16.
[26] 보안뉴스, 2023 국내외 보안시장 전망보고서, 2023.
[27] 과학기술정보통신부, 사이버보안 체계(패러다임) 전환에 따른 능동대응 기술 개발 방안 논의, 2023. 5. 16.
[28] https://www.whitehouse.gov/
[29] Cybersecurity and Infrastructure Security Agency, CISA Strategic Plan 2023-2025, 2022. 9.
[30] Executive Office of the President, M-23-13: No TikTok on Government Devices, Implementation Guidance, 2023. 2. 27.
[31] The Withe House, National cybersecurity Strategy, 2023. 3. 1.
[32] Executive Office of the President, M-23-02: Migrating to Post-Quantum Cryptography, 2022. 11. 18.
[33] The Withe House, Executive Order on Improving the Nation's Cybersecurity, 2021. 5. 12.
[34] Executive Office of the President, M-22-16: Administration Cybersecurity Priorities for the FY 2024 Budget, 2022. 7. 22.
[35] Executive Office of the President, M-22-15: Multi-Agency Research and Development Priorities for the FY 2024 Budget, 2022. 7. 22.
[36] op.europa.eu/webpub/eca/special-reports/hack-proofing-eu-institutions-05-2022/en/
[37] digital-strategy.ec.europa.eu/en/policies/cyber-solidarity
[38] eur-lex.europa.eu/eli/dir/2022/2555/oj
[39] eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454
[40] eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022JC0049
[41] eur-lex.europa.eu/eli/dir/2022/2557/oj
[42] European Commission, "Fifth Progress Report on the EU Security Union Strategy," Progress Report, 2022. 12. 13.
[43] joinup.ec.europa.eu/collection/fosseps/news/fosseps-project-launched
[44] European Commission, "European Cybersecurity Investment Platform," 2022. 10. 19.
[45] www.europol.europa.eu/about-europol/finance-budget
[46] eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32023B0228(09)
[47] commission.europa.eu/publications/european-research-executive-agency-financial-year-2023_en
[48] op.europa.eu/en/publication-detail/-/publication/27655ce4-b70f-11ed-8912-01aa75ed71a1/language-en
[49] European Commission, Horizon Europe Work Programme 2023-2024, 2023. 3. 31.
[50] cordis.europa.eu/project/id/101095634
[51] trublo.eu/projects/
[52] 사이버 시큐리티 전략본부, "일본의 사이버시큐리티 전략 2021(개요)," 2021. 9. 28.
[53] 사이버 시큐리티 전략본부, "사이버 시큐리티 전략," 2021. 9.
[54] 사이버 시큐리티 전략본부, "중요 인프라의 사이버 시큐리티와 관련된 행동 계획," 2022. 6. 17.
[55] 문부과학성, "문부과학성의 중장기 계획," 2022. 10.
[56] 사이버 시큐리티 전략본부, "정부의 사이버보안 관련 예산(5개년)," 2023. 4. 14.
[57] 사이버 시큐리티 전략본부, "사이버 시큐리티 연구개발 전략(개정)," 2021. 5. 13.
[58] 통합혁신전략추진회의, "AI전략 2022," 2022. 4.