사이버 보안 분야 주요 기업의 시장 성과와 ICT 공급망 관련 정책 동향

Market Performance of Major Companies in Cybersecurity and Policy Trends in Information and Communication Technology Supply Chain

안춘모 (C.M. Ahn, cmahn@etri.re.kr) 기술경제연구실 책임연구원
유영상 (Y. Yoo, heyyoo@etri.re.kr) 기술경제연구실 연구전문위원

ABSTRACT

Cyberthreats and crimes have become common in society and demand the adoption of robust security measures. Financial cybercrimes, personal information breaches, and spam messages are now prevalent, while companies and nations face an increasing number of cyberthreats and attacks such as distributed denial of service, ransomware, and malware. As the overall socioeconomic landscape undergoes digitalization powered by big data, cloud computing, and artificial intelligence technologies, the importance of cybersecurity is expected to steadily increase. Developed nations are actively implementing various policies to strengthen cybersecurity and providing government support for research and development activities to bolster their domestic cybersecurity industries. In particular, the South Korean government has designated cybersecurity as one of the 12 nationwide strategic technology sectors. We examine the current landscape of cybersecurity companies and the information and communication technology supply chain, providing insights into the domestic cybersecurity market and suggesting implications for South Korea.

KEYWORDS 공급망 보안, 기업 현황, 사이버 보안

Ⅰ. 서론

5G, 빅데이터, 클라우드, AI 등 첨단 정보통신기술의 인프라화와 더불어 COVID-19의 창궐은 우리 사회와 경제의 디지털 전환을 급속도로 앞당기고 있다. 비대면화가 일상이 되면서 현실 공간을 대신할 수 있는 사이버 공간 속에서 업무를 처리하며 신규 서비스와 부가가치를 창출하고, 나아가 현실공간과의 연계성 강화로 사이버 공간은 새로운 범주의 생활 공간이 되고 있다.

* DOI: https://doi.org/10.22648/ETRI.2024.J.390305
* 본 연구는 한국전자통신연구원 연구운영지원사업의 일환으로 수행되었음[24ZF1100, 국가 지능화 기술정책 및 표준화 연구].

사이버 공간은 사용자들에게 다양한 편익과 편리함을 제공하지만, 컴퓨터 바이러스, 랜섬웨어, 멀웨어, 피싱, 악성앱, DDoS, 제로데이공격 등 다양한 사이버 공격을 통해 개인정보 침탈, 금전취득, 물류망 셧다운 등 부정적인 상황도 역시 발생시키고 있다. 실제로, 미국의 정부 부처 및 기업이 해킹당한 SolarWinds 공급망 공격[1], 미국 남동부 지역의 휘발유 공급을 중단시켰던 Colonial Pipeline 랜섬웨어 감염[2] 등 사이버 공간의 위협과 취약성이 현실세계를 크게 위협하고 있는 실정이다.

사이버 공간을 다양한 위협 · 공격으로부터 보호하는 것은 필요조건을 넘어서 현대 사회경제행위의 필수 사안이 되었다. 사이버 보안은 현재 네트워크, 클라우드, 모바일, IoT 등 대부분의 영역에서 반드시 포함시켜야 하는 인프라적 성격을 가진 부문이다. 보안의 위상은 과거 해커들에 의한 침해 · 위협 발생 후 사후 대응이 주된 행위였다면, 현재는 사이버 공격에 대한 탐지뿐만 아니라 사전 예방을 위한 SW 해킹 취약지점 식별, 사고 후 복구 · 추적, 회복탄력성 확보 등 사전적이며 포괄적인 대응체계를 지향하고 있다[3].

사이버 보안 강화를 위해 미국과 EU 등에서는 이미 적극적인 정책 마련을 진행 중이다. 미국은 2023년 3월 국가사이버안보전략(National Cybersecurity Strategy)을 마련하여 '사회 기반 시설 보호'와 'SW 벤더에 대한 책임 부여' 등을 강조하고 있으며[4], EU는 NIS2 지침, CER 지침, 사이버 회복탄력성 법안(Cyber Resilience Act) 등 범유럽 관점에서 활발한 입법적 노력을 진행하고 있다[5-7]. 특히 미국은 공급망 보안을 위한 행정명령 EO-14028을 발표 후, SBOM 도입, 안전한 SW 도입을 위한 권고사항 등을 명시적으로 제시하여 자국 내 정부 SW 보안을 위해 강력한 공급망 보안 정책을 추진 중에 있다[8]. 또한, 제로트러스트, 클라우드, IoT, 국방의 선제적 안보 등 다양한 범주의 보안 형태가 논의되고 있다.

우리나라에서도 사이버 보안 역량 제고를 위해 정부와 기업들이 다양한 정책 · 전략을 마련하고 있다. 정부에서는 사이버 보안을 디지털전환 시대 필수기반 기술로 인식하고 12대 국가전략기술로 지정하였으며, ▲데이터 · AI 보안, ▲디지털취약점 분석 · 대응, ▲네트워크 · 클라우드 보안, ▲산업 · 융합 보안 기술을 중심으로 임무중심 전략로드맵을 수립하였다. 특히 SBOM 체계, 보안 특화 AI언어모델(LLM), 양자내성암호, 제로트러스트 등 글로벌 시장과의 보안 역량 동조화를 추진할 예정이다[3].

본고에서는 디지털 전환 진전에 따라 인프라적 영역으로서 중요성이 더해지는 사이버 보안 부문에 참여하고 있는 기업들의 시장 동향을 파악하고, 최근 사이버 위협 · 공격의 주요 영역인 ICT 공급망 부문의 보안 정책에 대해서도 검토하고자 한다.

II. 사이버 보안 활동 기업 동향

사이버 보안은 산업 부문의 인프라적 성격을 가짐에 따라 참여하는 기업들은 지향하는 기술과 서비스에 따라 그 특성을 달리하고 있다. 즉, 모든 영역에서 비즈니스를 전개하기보다 다른 기업들과 차별화된 점을 내세우며 자사의 가치를 높이고 있다. 예를 들면, 방화벽, DDos, ID제어 등 기존 영역에서 강점을 보이는 기업도 있으며, 클라우드 보안, 제로트러스트, AI보안 등 최근의 기술을 기반으로 성장하는 기업들도 있다. 본 장에서는 이렇게 다양한 포지셔닝으로 사이버 보안 시장에 참여하는 기업들의 현황을 정리해 보고자 한다.

1. 글로벌 사이버 보안 기업 동향

표 1[9]과 같이 현재 상장된 IT보안기업 중 시가

표 1 글로벌 IT 보안 기업 시가총액 동향(2024. 3. 14. 기준)

(단위: 억 달러, USD)

순위	기업명	매출 (억 달러, 2003)	시가 총액	price	국가	사업부문
1	Palo Alto Networks	68.93	922	285.2	미국	• 진보된 방화벽 및 클라우드 기반 맞춤형 제품 • 네트워크, 엔드포인트 보안에 강점을 가짐
2	CrowdStrike	22.41	777	321.1	미국	• 2011년 설립 • 클라우드 워크로드, 엔드포인트 보안, 위협 인텔리전스, 사이버 공격 대응 서비스 등을 제공
3	Fortinet	53.05	515	67.6	미국	• 2000년 설립하였으며, 네트워크 경계 보안에 강점 • 방화벽, 엔드포인트 보안, 침입 탐지 시스템 등 보안 솔루션 개발 및 판매
4	Cloudflare	3.6	320	94.6	미국	• 콘텐츠 전송 네트워크 서비스, 클라우드 사이버 보안, DDoS 완화 및 ICANN 인증 도메인 등록 서비스 등 제공
5	Zscaler	5.25 (2024.1)	294	195.9	미국	• 2007년 설립 • 기업 클라우드 보안 서비스를 제공하며 강점을 가진 것으로 평가
6	Check Point Software	24.2	195	166.5	이스라엘	• 1993년 설립하였으며, 방화벽 전문 기업 • 네트워크 보안, 엔드포인트 보안, 클라우드 보안, 모바일 보안, 데이터 보안 등 IT 보안 SW와 HW 제품을 제공
7	Okta	6.1 (2024.1)	177	105.9	미국	• 2009년 설립하였으며, 접근 관리 전문 • Best for Access Management
8	Leidos Holdings	154.4	171	126.4	미국	• 미국의 국방, 항공, 정보 기술 및 생물 의학 연구 회사, 방위 산업 부문 최대 IT 서비스 제공업체
9	Akamai	38.1	163	107.9	미국	• 콘텐츠 전송 네트워크, 사이버 보안 및 클라우드 서비스
10	Gen Digital	9.5	135	21.2	미국	• 다국적 SW 회사로 사이버 보안 SW 및 이와 관련된 서비스를 제공

출처 Reproduced with permission from [9].

총액[1)2)]이 가장 큰 기업은 Palo Alto Networks이다. 본 기업은 진보된 방화벽 및 클라우드 기반 맞춤형 제품을 개발하고 있으며, 네트워크, 엔드포인트, 원격 자산 공격에 강한 보안 역량으로 68.9억 달러의 매출(2023년), 시가총액 922억 달러로 평가된다. 2위는 CrowdStrike로서 엔드포인트 보안과 서비스에서 강점을 가진 것으로 평가받으며, 22.4억 달러의 매출과 777억 달러의 시가총액을 보이고 있다. Fortinet은 네트워크 경계 보안이 강점으로 평가되며, 53억 달러의 매출, 515억 달러의 시가총액을 보였다. 이외에 Cloudflare는 WAF, DDoS, CDN, DNS 등을 주 사업으로 하며 시가총액 320억 달러, Zscaler는 클라우드 보안 우수 기업으로 시가총액 294억 달러, Check Point는 방화벽에 강점을 보이는 이스라엘 기업으로서 195억 달러의 시가총액을 보이고 있다. 시가총액 상위 5개 기업은 주로 네트워크, 클라우드, 엔드포인트 보안, 방화벽 등 최근 수요가 발생하는 영역에서 시장 경쟁력을 확보하고 있는 것으로 파악된다. 시가총액 상위 40개 기업의 대부분은 미국 기업이지만, 이스라엘 4개 기업, 영국 2개, 일본 · 프랑스 · 독일·인도 각각 1개 기업도 포함하고 있다[9].

1) 시가총액 관점에서 세계 1위 기업은 Microsoft로서 3.1조 달러, Apple은 2.7조 달러, NVIDIA 2.2조 달러, Alphabet (Google) 1.8조 달러, Amazon 1.8조 달러 순으로 나타난다 (2024.3.19. 기준)[11].

2) 빅테크 기업 가운데 IT보안 기업으로 분류 가능한 기업은 Microsoft(Window 보안), IBM(진보된 암호), CISCO(통합 네트워크 보안) 등 빅테크 기업, Trellix(비상장 기업, 9.4억 달러 매출(2020)) 등 다양하다[9].

표 2 2019~2023년 3사분기 간 10억 달러 이상의 M&A(상위 10개)

딜 공개 일	피 M&A 기업	사업 분야	M&A 기업	딜 금액 (10억 달러)	M&A 형태
2Q22	VMware	Security management	Broadcom Inc.	61.0	Acquisition
3Q23	Splunk	Security operations	Cisco	28.0	Acquisition
3Q21	Proofpoint	Content security	Thoma Bravo	12.3	Take Private
3Q19	Symantec Enterprise Security Business	Endpoint security	Broadcom Inc.	10.7	Acquisition
3Q22	Avast	Network security	NortonLifeLock	8.1	Merger
2Q22	SailPoint	Identity and access management	Thoma Bravo	6.9	Acquisition
1Q21	Auth0, Inc.	Identity and access management	Okta, Inc.	6.5	Acquisition
2Q22	Datto	Data security	Kaseya	6.2	Acquisition
3Q22	Micro Focus	Application security	OpenText	6.0	Acquisition
2Q22	Mimecast	Cloud security	Permira	5.8	Take Private

출처 Reproduced with permission from [15].

글로벌 사이버 보안 유니콘 기업 수도 2019년 8개에서 2022년 59개로 빠르게 성장하는 추세이다[10]. 2023년에도 Tanimum(기업용 차세대 보안), Lacework(클라우드 보안) 등이 기업가치 90억 달러, 83억 달러[3]로 평가받고 있으며, 이 중 Snyk(애플리케이션 및 클라우드 보안), Wiz(클라우드 보안 인텔리전스) 등은 이미 규모가 커져 유니콘을 졸업했다고 평가받고 있다[11].

사이버 보안 기업의 성장에 따라 전통 빅테크를 중심으로 보안기업들의 인수합병도 활발하게 일어나고 있다. 2022~2023년 주목받은 M&A로서는 2023년 9월 Cisco가 Splunk를 280억 달러에 한 인수 계약[4)5)][12-14], 2022년 9월 구글 클라우드가 Mandiant[6]를 54억 달러에 인수한 사례[14] 등으로 적지 않은 금액에 인수합병이 이루어진 사례이다. 2019~2023년 3사분기까지의 보안기업에 대한 M&A 중 10억 달러 이상은 표 2와 같이 총 37건으로 추산되며, 이 중 Broadcom이 VMware를 인수한 610억 달러가 가장 크고, Cisco의 Splunk 인수가 280억 달러로서 두 번째 규모이다. 다음으로 사모펀드인 Thoma Bravo가 Proofpoint를 123억 달러에 인수하였으며, 역시 Broadcom의 Symantec Security Business 인수가 107억 달러로 진행되었다[15].

2. 국내 사이버 보안 기업 동향

국내 사이버 보안 기업들 중 가장 큰 매출을 보이는 기업은 안랩이다. 2023년 매출[7]은 2,298억 원, 영업이익은 323억 원, 영업이익률은 14.1%를 기록하였다. 2023년 매출 1천억 원 이상인 국내 사이버 보안 기업으로 시큐아이, 이글루코퍼레이션, 오픈베이스, 윈스 등이 있다.

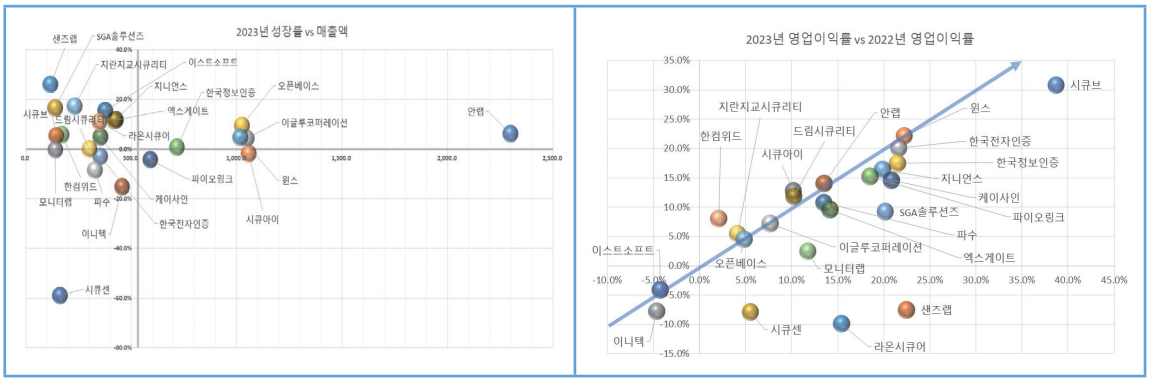
3) Tanium은 2015년 3월, Lacework는 2021년 1월 현황 자료이다.

4) 본 인수는 Cisco가 인공지능 경쟁력과 차세대 AI 기반 보안 사업을 강화하려는 목적이라고 분석되고 있다[12].

5) 특히, Cisco는 Splunk 이외에도 2023년 7월 기업 보안 플랫폼 업체 Oort, 5월 AI 기반 클라우드 보안 플랫폼 Armorblox 등 2023년 상반기 9건의 M&A를 진행한 바가 있다[13].

6) 위협 인텔리전스 분석 전문업체이다. 2020년 말 발생한 SolarWinds 공격을 처음 발견하였다[14].

7) 국내 사이버 보안 기업의 2023년 매출은 금융감독원 전자공시시스템(DART)을 통해 조사하였다.



출처 Reproduced from [16,17].

그림 1 국내 사이버 보안 기업 현황(2023년 성장률 vs 매출액, 2023년 vs 2022년 영업이익률)

국내 사이버 보안 기업의 2023년 성장률 대비 매출액을 비교하면 그림 1에서 보듯이 안랩, 이글루코퍼레이션 등이 매출 규모가 큰 기업이고, 지란지교시큐리티, 이스트소프트, 엑스게이트 등은 성장률이 빠른 기업들로 볼 수 있다. 영업이익률 관점에서는 대부분의 기업이 2022년 성장률을 2023년에도 유지하고 있다. 특히 시큐브, 윈스, 한국전자인증 등은 2년 연속 높은 성장률을 보이고 있으나, 이에 반해 샌즈랩, 라온시큐어, 시큐센 등은 2022년 플러스 성장세가 2023년 마이너스 성장으로 전환되었음을 알 수 있다.

Ⅲ. ICT 공급망 보안 현황 분석

1. ICT 공급망 위협 및 공격 현황

최근 ICT 공급망 위협과 공격으로 기업 중요 정보 해킹, 악성 SW 배포 등이 발생하거나, 국가의 중요 기반 시설이 멈추는 사례도 발생하고 있다. 대표적인 사례로는 2020년 SolarWinds 공급망 공격, 2021년 Kaseya 랜섬웨어 유포[8][18], Apache Log4j 취약점[9] 공격[19] 등으로 미국 정부 및 기업들이 피해를 입었으며, 동년 발생한 Colonial Pipeline 랜섬웨어 감염으로 미국 북동부 휘발유 공급이 실제로 중단되는 물리적 피해가 발생하기도 하였다. HW 공급망 공격 사례로는 2018년 발표된 Supermicro 서버 보드 해킹 사건이 대표적이며 미국 내 30여 개 기업과 정부에게 큰 충격을 주었다.

ICT 공급망이란 ICT 제품(SW/HW) · 서비스를 주요 대상으로 하는 공급망[10][20]을 의미한다[21]. ICT의 급격한 혁신은 ICT 공급망 구성 시 전자 · 디지털 제품 및 SW의 활용 확대, 아웃소싱과 패키지 도입 등 분업화된 SW 개발 절차, 오픈소스 활용 증가 등이 전개되었다. 이러한 변화는 결국 ICT 공급망 자체의 계층화 · 복잡화를 가져오고, 공격 표면의 확대, 공급망 SW 검증의 어려움을 발생시켜 ICT 공급망 전체에 보안 취약성을 증대시키고 있다. ICT 공급망의 이러한 취약성은 공급자 입장에서는

8) Kaseya는 미국 IT 및 보안 관리 서비스 업체이며, 러시아와 연계된 해킹그룹 레빌(REvil)이 고객사의 소프트웨어 업데이트 관리를 돕는 '카세야VSA'를 공격한 사례이다.

9) Log4j는 JAVA 기반으로 서버와 응용프로그램의 로그 생성을 위해 사용하는 유틸리티로서, 공격 성공 시 피해 서버에서 공격자가 의도하는 명령어를 직접적으로 실행 가능하다.

10) ISO/IEC 28001:2007에서는 공급망(Supply Chain)을 구매 주문 시 원재료의 소싱(Sourcing)에서 시작하여 제품 및 관련 서비스의 제조, 가공, 취급 및 배송을 통해 구매자까지 확장되는 자원 및 프로세스의 연결 집합으로 정의한다[20].

멀웨어, 사회공학 등을 통해 공급망을 손상시키고, 수요자 입장에서는 피싱, 개인데이터 유출 등의 손실을 초래한다.

주목할 점은 기존 공급망 공격의 목적이 많은 경우 금전 탈취를 지향한 악성 해커 중심의 범죄 행위였다면, 현재는 해킹을 주된 업으로 삼는 단체가 중심이 되며, 특히 국가의 지원을 받는 공급망 공격[11)] [22]을 통해 조직적으로 암호화폐 탈취, 국가 안보 교란, 기밀 정보 해킹 등이 발생하고 있다는 점이다.

2. 공급망 보안을 위한 주요국 정책

가. 미국

미국이 공급망 보안 정책을 본격적으로 추진한 것은 바이든 대통령이 서명한 행정명령 EO-14028, 「Executive Order on Improving the Nation's Cybersecurity」로부터 비롯되었다고 평가받고 있다(2021년 5월 12일)[23]. 행정명령 EO-14028의 주된 지시사항은 정보 공유, 제로트러스트 아키텍처 이행, SBOM 개시 등 국가의 사이버 보안 강화를 위한 다양한 시책을 포함하고 있다. 이 중 행정명령 4절은 「SW 공급망 보안 강화」에 관한 내용이며, NIST가 표준, 절차 및 기준을 참조하여 SW 공급망 보안을 강화하기 위한 다양한 지침을 특정 시점까지 게시할 것을 요구하고 있다. 표 3은 행정명령에 적시된 다양한 시책 중 주요 내용을 정리하였다. 우선적으로 연방정부 관점에서 관리할 EO-Critical SW를 정의하고, 공급자에 대해서는 NIST의 요구사항에 명확히 대응할 수 있도록 가이드라인(NISTIR 8397, SSDF ver 1.1, IoT 라벨링, SP 800-161 Rev.1, Self-Attestation Form 등)

11) SolarWinds 해킹은 러시아 정보기관과 연관이 있는 러시아 해커 그룹 Cozy Bear로 추정되고 있으며, Kaseya 해킹은 REVil그룹, Log4Shell은 북한의 라자루스 그룹, 이란, 중국과 연결된 그룹이 악용한 것으로 알려져 있다[1,22].

표 3 행정명령 EO-14028 4절의 SW공급망 강화를 위한 주요 시책

날짜	보고서 명 등 목적
'21.6	• [정의] Publish definition of EO-critical software[24] • EO-Critical SW는 연방 정부에서 사용하는 주요 SW 제품에 대한 보안 기준을 개발하기 위해 행정명령에서 도입한 개념 • EO-Critical SW로 지정된 SW는 연방 정부가 SW를 구매 및 관리하는 방법을 포함하여 추가적인 활동이 필요하며, 기업은 보안 조치 적용 필요
'21.7.	• [안전한 SW 개발-가이드라인](NISTIR 8397) Publish guidance Recommending Minimum Standards for Vendor or Developer Verification(Testing) of Software Under Executive Order(EO) 14028(4r)[25] • 공급업체의 소스코드 테스트에 대한 지침 게시를 지시하고 있으며, 이에 따라 NIST는 SW 공급업체 또는 개발자 검증을 위한 최소 표준을 권장하는 문서를 개발 • 본 가이드라인에는 벤더나 개발자에 의한 SW 검증 시에 추천되는 11개의 최저 기준 제시
'21.9.(초안) '22.2.(최종)	• [안전한 SW 개발 프레임워크](SP 800-218) SSDF Ver 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities[26] • 초기 SSDF*에는 보안 SW 개발 실무 문서를 기반으로 하는 기본적이고 건전하며 안전한 SW 개발 실무 세트 * Secure Software Development Framework
'22.2.	• [공급망 보안-가이드라인] Software Supply Chain Security Guidance Under Executive Order(EO) 14028[27] • 연방 기관이 SW 조달에 대한 위험 기반 결정을 내리는 데 사용할 수 있는 형식으로 SW 생산자로부터 필요한 정보를 얻을 수 있도록 돕기 위한 것 • 본 지침의 범위는 SW가 포함된 제품뿐만 아니라 펌웨어, 운영 체제, 애플리케이션, 애플리케이션 서비스(예: 클라우드 기반 소프트웨어)를 포함하는 SW의 연방 기관 조달로 제한
'22.2.	• [IoT-가이드라인] Cybersecurity Labeling for Consumers: Internet of Things(IoT) Devices and Software(February 4, 2022)[28] • 사물 인터넷(IoT) 소비자 장치 및 SW 개발 관행(Practice)의 사이버 보안 기능에 대한 두 가지 라벨링 프로그램을 시작하도록 지시 • 소비자 IoT 제품의 사이버 보안 라벨링에 대한 권장 기준과 소비자 SW의 사이버 보안 라벨링에 대한 권장 기준을 발표
'22.5.	• [공급망 보안-가이드라인] NIST SP 800-161 Rev. 1, Cyber Supply Chain Risk Management Practices for Systems and Organizations[29] • 본 문서의 목적은 공급망 전반에 걸쳐 사이버 보안 위험을 관리하는 데 도움이 되도록 기업 전반에 걸쳐 위험 관리 프로세스를 식별, 평가, 선택 및 구현하고 통제를 완화하는 방법에 대한 지침을 기업에 제공하는 것
'22.9.	• OMB Memo 22-18/OMB Memo 22-16[30] • 연방정부에 SW를 납품하는 공급자에게 EO 및 SSDF에서 요구하는 NIST 보안 SW 개발 가이드를 준수할 것을 요구하며, 이를 증명할 수 있는 자체증명(Self Attestation)을 반드시 제출함을 요구

'24.3.	• Secure Software Development Attestation Form [31] • 자체 증명 양식 • 연방정부에 SW를 납품하기 위한 최소한의 안전 SW 개발 증명 문서

출처 Reproduced from [24-31].

을 구성하였으며, 정부기관 관계자에 대해서도 안전한 SW 조달을 위한 가이드라인을 제시하였다.

나. EU

EU는 디지털 시대 변화에 대응하여, 사이버 보안을 디지털 정책 성공을 위한 핵심으로 간주하고 다양한 입법적 노력을 진행 중이다. ICT 공급망 보안과 관련하여 ENISA는 24가지 SW 공급망 공격과 그 결과를 검토한 「공급망 보안 공격 증가 이해」라는 제목의 보고서를 발표하고[26], 조직이 시행해야 할 권장사항을 공유하였다. 이를 기반으로 EU는 「Cyber Resilience Act(CRA)」[12][32]를 제안하였다. 본 법안은 "SW나 HW 제품, 원격 데이터 솔루션 및 시장에 별도로 출시될 수 있는 그 구성요소"에 적용되며, 설계 단계에서 노후화에 이르기까지 제품 수명 주기 전반에 사이버 보안 내재화를 위한 표준, 적합성을 준수해야 함을 명시화하고 있다.[13]

다. 일본

일본은 「사이버 보안 기본법」을 기반으로 추진 중인 사이버 보안 기본 전략과 연차 전략을 개정하면서 공급망 보안에 대한 실질적인 시책을 추진 중에 있다.

2021년 9월 3번째로 개정되어 발표된 일본의 「사이버 보안 기본 전략」 중 공급망 보안 정책으로는 공급망 리스크에 대응하기 위한 기술 검증 체제 정비(SW·HW 검증기술의 연구개발 및 실용화)가 있다[33].

2023년 7월 연차계획 「사이버 시큐리티 2023」이 발표되면서 SBOM의 중요성을 언급하고 있으며, 특히 OSS 보급 확대에 따른 통신분야에서의 SBOM 도입이 급선무임을 지적하고 있다. 본 계획에서는 SBOM 도입의 글로벌 흐름에 비해, 일본에서는 SBOM 관리를 실용화하고 있는 기업은 적고, 현재 일본의 상황을 개념 · 용어로서 인지되기 시작한 단계로 평가하고 있다[34].

3. 국내 ICT 공급망 보안 정책 현황

국내에서는 이미 공공기관을 중심으로 시큐어코딩의 필요성과 대응 체계, 공급망 보안 강화를 위한

표 4 국내 ICT 공급망 보안 정책 추진 현황

연도	주요 내용
'11~현재	행정안전부를 중심으로 「SW 개발보안 가이드」를 구축하고 활용 중[35]
'19	「국가 사이버 안보 전략」[36]과 「국가 사이버 안보 기본계획」[37] 중 「안전한 주요정보통신기반시설 운영을 위한 보안 검증·점검체계구축」
'21.2	K-사이버방역 추진 전략 중 공급망 보안점검 기준 및 점검도구 개발·보급(1,000개, ~'23년) 등 추진[38]
'21.8	SW개발보안허브 개소
'22.5	윤석열 정부 출범 시 사이버 보안을 국정과제로 선정. Zero Trust 등 신 보안체계 도입의 본격 검토
'22.10	제로트러스트·공급망 보안 포럼 발족[39]
'22.12	인터넷기반자원공유(클라우드) 보안인증(CSAP) 등급제 고시 개정안 고시
'23.6	의료기기 사이버 보안 허가·심사 지원 사항
'23.6	SW 공급망 보안체계 구축을 위한 실증사업 착수[40]
'23.7	IoT 보안인증제도 개선안 시행
'23.9	「정보보호산업의 글로벌 경쟁력 확보 전략」[41] 중 SW 공급망 공격에 능동적으로 대응하고, 해외 무역 장벽에 대비하기 위한 SW 공급망 보안점검·대응 인프라 구축(2024~) 등 추진

출처 Reproduced from [35-41].

12) 본 법안은 유럽 의회의 승인을 받았으며(2024.3.12.), 이사회의 채택만 남은 상황이다[35].

13) 제품을 기능, 사용목적, 영향범위 등에 따라 'Class I, Class II, 기본(Default)' 3개의 범주로 분류하고 Class I과 II의 경우 보다 엄격한 리스크관리 수행을 명시하고 있다.

제도적 접근이 활발히 이루어지고 있으나, 집중화된 공급망 보안 정책은 최근에 많이 시도되고 있는 상황이다. 표 4는 그동안 추진되어 온 우리나라의 공급망 보안 유관 시책들이며, 특히 2022년 신정부 출범을 계기로 '제로트러스트 공급망 보안 포럼' 발족, 'SW 공급망 보안체계 구축을 위한 실증사업' 등을 통해 본격적으로 공급망 보안을 지향하는 정책이 추진되고 있음을 알 수 있다.

ICT 공급망 관련하여 이에 적합한 보안 표준 및 관리체계를 규율하는 법령은 아직 미진한 상황이다. 현행 국내 법령은 일반적인 해킹 · DDoS 등 사이버 침해 행위를 방지하려는 목적으로 제정된 법률이 각각 개별법의 분산된 형태로 구현되어 「정보통신망법」, 「SW진흥법」, 「정보통신기반보호법」[14] 등이 있으며, 내용 자체는 다소 일반적인 보안관리 조항들로 선언적 성격을 가진다. 세부적인 제도로는 '주요 정보통신기반시설 보호 제도', '보안 적합성 검증 제도', '공공기관 정보 시스템 구축 · 운영 지침' 등이 운영되고 있다.

국내에서 추진되는 공급망 보안 R&D는 주로 HW 공급망 보안에 집중되어 있으나, 최근에는 SW 공급망 보안을 위한 R&D도 다양해지는 상황이다. 현재 ETRI는 「시스템 · 디바이스의 HW 공급망 위협 대응 핵심기술 개발('20~'24)」, 「임베디드 시스템 악성코드 탐지 · 복원을 위한 RISC-V 기반 보안 CPU 아키텍처 핵심기술 개발('21~'24)」을 추진 중이며, 고려대는 「고신뢰 온-디바이스 딥러닝 가속기 설계를 위한 물리채널 기반 취약점 검증 및 대응기술 개발('21~'24)」을 진행 중이다. SW 공급망 보안 측면에서는 고려대가 「SW 공급망 보안을 위한 SBOM 자동생성 및 무결성 검증기술 개발('22~'25)」을 추진하고 있다. 이외에 쿤텍, 고려대, ETRI 등 국내 민간 기업, 대학 · 연구기관에서 일부 개념 검증 수준의 취약점 탐지기술과 공급망 공격에 대한 대응 체계를 다루는 연구가 진행되고 있다. 쿤텍은 ETRI의 펌웨어 분석기술을 활용하여 BOM 추출, 분석, 취약점 자동 탐지 기술 개발을 추진하고 있으며[42], 고려대에서는 하드웨어 백도어 탐지 기술을 제안하고 있다.

Ⅳ. 국내 사이버 보안 개선을 위한 제언

본 글에서는 사이버 보안 분야의 국내외 기업의 시장 성과, 인수합병, ICT 공급망 보안 정책 등을 간략히 정리해 보았다. 마지막으로 우리나라 사이버 보안 역량과 경쟁력을 높이기 위한 주요 과제에 대해 제언하고자 한다.

우선, 국내 주요 기반시설 보호를 위한 지속적인 제도 체계화를 진행해야 한다. 미국은 이미 기반 시설에 대한 사이버 공격을 받은 경험이 있다. 국가 기반시설에 대한 공격은 단순한 이익 편취의 수단을 넘어선 국가 안보에 대한 위협 행위이다. 우리나라에서는 「정보통신기반 보호법」에 따라 주요 정보통신기반시설에 대한 침해사고 발생 시 통지의무와 대응 미진 시 과태료 처분 등이 가능하나, 주요 기반시설을 포괄하는 종합적인 제도는 아직 미비한 상황이다. 현재 2024년 2월 발표된 「국가 사이버안보 전략」에는 「3. 국가 핵심인프라 사이버 복원력 강화」 전략을 마련하고 있다[43]. 이에 따라, 빠른 시일 내 상기 전략을 구현하는 기본법 제정이나 거버넌스 구축, 선제적 대응 체계 구축을 위한 적극적인 시책이 필요하다.

두 번째로, HW 공급망 강화를 위한 종합적 연구

14) 2023년 4월 11일 정필모 의원이 대표발의한 「정보통신기반 보호법」 일부개정법률안이 국회에서 가결되었다. 본 법률에서는 주요정보통신기반시설에 대한 침해사고가 발생한 경우 관계 중앙행정기관의 장이 관리기관의 장에게 해당 정보통신기반 시설의 복구 및 보호조치 명령을 할 수 있도록 하고, 이를 불이행한 경우 과태료를 부과하도록 하고 있어, 침해사고 대응에 대한 강제성을 부여하였다.

개발 계획 마련과 적극적 정부 지원이 필요하다. 현재 국내 HW 공급망 보안은 국가 · 공공 기관에 도입되는 IT보안제품에 대해 국가정보원의 보안적합성 검증체계를 중심으로 진행하고 있다. 그럼에도 HW 검증체계는 성능측정에만 치중하고 있다는 평가이다[44]. 이를 위해 코드분석, 역공학 등 HW 취약점 분석을 위한 연구개발 확대, 도메인 중심의 HW 공급망 보안 경험 확보 등의 단계적 접근법을 시급히 시행하여야 할 것이다.

사이버 보안은 디지털 전환 사회에서 건전한 사회경제적 생활과 안보를 위해 필수적인 영역이다. 이에 미국, EU 등에서는 사이버 보안의 주도권 확보를 위해 정책적, 제도적, 기술적 역량을 집중하고 있다. 국내에서도 사이버 보안 부문을 12대 전략기술로서 정책적 지원을 아끼지 않고 있다. 앞으로 정부를 비롯한 산학연 모든 주체의 지속적인 협력과 노력이 더욱 중요해질 것이다.

용어해설

랜섬웨어 피해자의 데이터 또는 장치를 잠그고 피해자가 공격자에게 몸값을 지불하지 않으면 계속 잠기거나 더 나쁜 상태로 만들겠다고 위협하는 멀웨어의 일종(IBM)

사회공학 보안학적 측면에서 기술적인 방법이 아닌 사람들 간의 기본적인 신뢰를 기반으로 사람을 속여 비밀 정보를 획득하는 기법(위키피디아)

제로데이공격 제로데이위협이라고도 하며, 컴퓨터SW의 취약점을 공격하는 기술적 위협으로, 해당 취약점에 대한 패치가 나오지 않은 시점에서 이루어지는 공격(위키피디아)

약어 정리

CDN	Content Delivery Network
CER	Critical Entities Resilience
CISA	Cybersecurity and Infrastructure Security Agency
CSAP	Cloud Security Assurance Program
DDoS	Distributed Denial-of-Service
DNS	Domain Name System
ENISA	European Union Agency for Network and Information Security
IoT	Internet of Things
LLM	Large Language Model
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
OSS	Open Source Software
RISC	Reduced Instruction Set Computer
SBOM	Software Bill of Materials
WAF	Web Application Firewall

참고문헌

[1] IT World, "'누가, 언제, 무엇을 해킹했는가' 솔라윈즈 공급망 공격 타임라인," 2021. 4. 7.

[2] 소만사, "DarkSide 랜섬웨어 – 미 석유공급 기업 '콜로니얼 파이프라인' 공격 및 마비 초래," 2021. 6.

[3] 과학기술정보통신부 보도자료, "추격자를 넘어 초격차로, 12대 국가전략기술 로드맵 완성 및 핵심 프로젝트 선정," 2024. 2. 1.

[4] 백악관, National Cybersecurity Strategy, 2023. 3.

[5] EU, NIS 2 Directive: Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, 2022. 12. 14.

[6] EU, Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, 2022. 12. 14.

[7] EU, Cyber Resilience Act, 2022. 9. 15., https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

[8] The White House, Executive Order 14028: Improving the Nation's Cybersecurity, 2021. 5. 12.

[9] CompaniesMarketCap 홈페이지, https://companiesmarketcap.com/it-security/largest-companies-by-market-cap/#

[10] KISA, 사이버 대연합 보고서, 2023. 10. 20.

[11] Failory, Top 62 Cyber Security Unicorns in 2024, 2024. 1. 22., https://www.failory.com/startups/cyber-security-unicorns#26-kaseya

[12] 조선일보, "시스코, 스플렁크 37조원에 인수," 2023. 9. 22.

[13] CSO, Top Cybersecurity M&A Deals for 2023, Dec. 15, 2023., https://www.csoonline.com/article/574521/top-cybersecurity-manda-deals-for-2023.html

[14] 이코노미스트, “보안 강화하는 구글, 54억 달러에 맨디언트 인수,” 2022. 3. 10., https://economist.co.kr/article/view/ecn202203100080

[15] OMDIA, Cybersecurity Mergers & Acquisition Tracker – 3Q23, 2023. 10.

[16] 보안뉴스, “다시 돌아가는 보안기업 상장 시계…정부 보안산업 투자로 상승세,” 2023. 9. 15.

[17] 보안뉴스, “사이버 보안 상장기업 20곳 2022년 매출 분석해보니…85% 매출 증가,” 2023. 4. 17.

[18] 서울경제, “美 카세야도 당했다…러 연계 해커 랜섬웨어 공격,” 2021. 7. 4.

[19] 보안뉴스, “로그4셸 공격 건수 분석해보니…Log4j 취약점 공격은 현재진행형!,” 2022. 5. 5.

[20] ISO/IEC 28001:2007, Security Management Systems for the Supply Chain.

[21] UNIDIR, Supply Chain Security in the Cyber Age: Sector Trends, Current Threats and Multi-Stakeholder Responses, 2000.

[22] 연합뉴스, “러 미국 기업 공격 러 해킹그룹 ‘레빌’ 소탕, 조직원 수사,” 2022. 1. 14.

[23] White House, The President’s Executive Order (EO) 14028 on Improving the Nation’s Cybersecurity, 2021. 5. 12.

[24] NIST, Definition of Critical Software Under Executive Order (EO) 14028, 2021. 10. 13.

[25] NIST, Recommended Minimum Standards for Vendor or Developer Verification (Testing) of Software Under Executive Order (EO) 14028, 2021. 7. 7.

[26] NIST SP 800-218, Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, 2022. 2.

[27] NIST, Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e, 2022. 2. 4.

[28] NIST, Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software, Created Jul. 8, 2021, 2022. 2. 4.

[29] NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, 2022. 5.

[30] OMB M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices, 2022. 9. 14.

[31] CISA, Secure Software Development Attestation Form, 2024. 3. 18.

[32] https://www.european-cyber-resilience-act.com/

[33] NISC, 사이버 시큐리티 전략(각의결정), 2021. 9. 28.

[34] NISC, 사이버 시큐리티 2023 (2022년도 연차 보고·2023년도 연차 계획), 2023. 7. 4.

[35] 행정안전부, KISA, “전자정부 SW 개발·운영자를 위한 소프트웨어 개발보안 가이드,” 2021. 11.

[36] 국가안보실, “국가 사이버안보 전략,” 2019. 4.

[37] 관계부처 합동, 국가 사이버안보 기본계획, 2019. 9. 3.

[38] 과학기술정보통신부, K-사이버방역 추진전략, 2021. 2.

[39] 과학기술정보통신부, 제로트러스트 공급망 보안 정책포럼 발족식, 2022. 10. 26.

[40] 전자신문, “과기정통부, SW공급망 보안체계 실증사업 착수,” 2023. 6. 27.

[41] 과학기술정보통신부, 정보보호산업의 글로벌 경쟁력 확보 전략, 2023. 9.

[42] 데이터넷, “쿤텍·ETRI, 펌웨어 분석 활용 BoM 기술로 HW 공급망 보호,” 2022. 7. 21.

[43] 국가안보실, “국가 사이버안보 전략,” 2024. 2.

[44] 김권일, 김지원, “4차 산업혁명 기술 도입에 따른 하드웨어 공급망 위협과 대응 방안,” 한국산업보안연구, 제10권 제2호, 2020.