디지털 보안에 대한 해외 주요국의 통상 규범 동향

Trends in Digital Security Policies and Trade Rules in Major Overseas Countries

김지은 (J.E. Kim, jekim0104@etri.re.kr) 통신정책연구실 기술원

ABSTRACT

Trade rules in service and digital sectors mainly focus on reducing regulatory uncertainties by improving transparency and minimizing unnecessary requirements. Recognizing the importance of digital trade rules and trade in information and communication technology (ICT) sectors, governments worldwide have rapidly adopted and expanded rules on free flow of data, personal data protection, electronic authentication, and cybersecurity. On the other hand, advances in technology have led governments to face multiple threats related to cybersecurity, intellectual property (including that related to source code and algorithms), and unauthorized access to proprietary information of their suppliers. This study presents digital trade rules related to digital security emphasizing cybersecurity, source code, and ICT products that use cryptography in different trade agreements. Additionally, it introduces various approaches that major countries are taking to both address digital security issues and seek balance between security enhancement and trade liberalization.

KEYWORDS digital security, digital trade agreement, 디지털 통상, 사이버 보안, 암호화 ICT 제품

Ⅰ. 서론

국제통상 규범은 시장의 자유화를 추구하며 국경 간 상품과 서비스, 정보의 이동이 자유롭고 차별 없이 이루어질 수 있도록 질서를 수립하는 역할을 한다[1]. 상품에 디지털 기술이 융합되면서 상품과 서비스의 명확한 경계가 허물어지고, 서비스 공급자와 소비자가 거래를 위해서 더 이상 대면할 필요가 없어졌다. 이처럼 디지털 영역에서는 실시간 거래나 정보의 이동이 더 빠르게 이루어진다. 동시에 시스템이 자동화되고 네트워크 간 연결성이 높아지면서 보안에 대한 우려와 이에 대한 정부의 적극적인 규제적 대응을 야기하기도 한다[2].

사이버 보안에 대한 위협은 디지털 공간에서 지식재산 및 개인정보를 훔치고, 가짜 정보를 의도적으로 생산하고 이를 확산시키거나, 통신, 교통, 전기와 관련된 주요 기반시설(Critical Infrastructure)을 파괴하고, 네트워크에 연결된 사물인터넷(IoT)을 공

* DOI: https://doi.org/10.22648/ETRI.2023.J.380401
* 본 연구는 과학기술정보통신부 및 한국방송통신전파진흥원의 2023년도 ICT 기금사업(방송통신 교류촉진 지원)의 일환으로 수행하였음[23MR1400, 방송통신 통상협상력 강화].

격하는 것 등 여러 형태로 나타날 수 있다[3].

최근 디지털 보안에 대한 관심이 집중되면서 사이버 보안과 관련된 규범은 강화되고 암호기법을 사용하는 정보통신기술제품에 적용되는 규범은 하드웨어의 범위를 넘어서 소프트웨어까지 포함하는 것으로 규범의 적용 대상이 확대되는 추세를 보이기도 한다[4].

본고에서는 국가별로 강화되는 디지털 보안 조치 및 규제에 대응하기 위해 수립된 디지털 분야의 보안 관련 통상 규범을 소개하고, 사이버 보안을 포함하여 해외 주요국의 디지털 보안 제도와 국제 무역협정 내 관련 규범 동향을 살펴보고자 한다.

II. 디지털 보안 강화를 위한 통상 규범

1. 사이버 보안 강화를 위한 협력

사이버 보안에 대한 규범은 포괄적·점진적 환태평양경제동반자협정(CPTPP: Comprehensive and Progressive Agreement for Trans-Pacific Partnership)에 포함되면서 CPTPP 이후 체결된 디지털 분야 협정에서 반복적으로 등장한다. CPTPP 전자상거래 챕터 제14.16조 '사이버 보안 사안에 대한 협력(Cooperation on Cybersecurity Matters)' 조항은 두 가지 측면에서 사이버 보안에 대한 협력의 중요성을 강조한다. 첫 번째는 컴퓨터 보안 사고 대응을 책임지는 국가 기관의 역량 구축의 중요성이고, 두 번째는 당사국이 다른 국가와 구축해놓은 협력 메커니즘을 활용하여 당사국의 전자적 네트워크에 영향을 미치는 악의적인 침입 또는 악성코드의 배포를 식별하고 완화하는 것의 중요성을 인정하는 것이다[5].

CPTPP의 '사이버 보안 사안에 대한 협력' 조항은 구속력이 없는 규범으로 협정 당사국 간 협력의 중요성을 인정하는 수준에 그쳤다. 하지만 당사국 간 협력 사안에 대해 종합적으로 다루는 '협력(Cooperation)' 조항이 같은 전자상거래 챕터 내에 있음에도 별도의 독립적인 조항으로 구성되어 있다는 것에 주목할 필요가 있다.

CPTPP 이후에 체결된 다자무역협정인 역내포괄적경제동반자협정(RCEP: Regional Comprehensive Economic Partnership) 제12.13조[6], 미국, 멕시코, 캐나다 간 체결한 무역협정인 USMCA(U.S.-Mexico-Canada Agreement) 제19.15조[7], 영국-호주 자유무역협정(FTA: Free Trade Agreement) 제14.20조[8] 그리고 미국-일본 디지털무역협정(USJDTA: U.S.-Japan Digital Trade Agreement) 제19조[9], 영국-싱가포르 디지털경제협정(UKSDEA: U.K-Singapore Digital Economy Agreement) 제8.61-L조[10]에도 사이버 보안 강화를 위한 협정 당사국 간 협력을 중요시하는 규범이 포함된 것을 확인할 수 있다.

2. 사이버 보안 강화를 위한 규제방식

USMCA의 사이버 보안 조항은 협력을 도모하는 것에 그치지 않고 사이버 보안 강화를 위한 당사국의 규제방식에 대한 명확한 정책적 목적을 포함한다. 사이버 보안 위협(Threat)은 지속해서 진화한다는 특성을 고려하여 이러한 위협에 대응하기 위해서는 위험기반접근방식(Risk-based Approach)이 처방적 규제(Prescriptive Regulation)보다 더 효과적임을 인정하도록 하는 조항을 추가하였다. 나아가 협정의 각 당사국에 사이버 보안 사건의 탐지, 대응 및 복구를 위해 자국 내 기업들이 위험관리(Risk Management) 모범사례와 합의된 표준(Consensus-based Standard)에 기반한 위험기반접근방식의 적용 및 채택을 장려하도록 노력해야 하는 의무를 부여한다.

위험기반접근방식의 규제방식에 대한 선호를 나타낸 규범은 영국-호주 FTA 제14.20조, USJDTA 제19조, UKSDEA 제8.61-L조에서도 찾아볼 수 있다.

3. 소스코드에 대한 접근 제한

정부의 무분별한 소스코드 공개 요청 또는 소스코드 유출 위험으로부터 사업자의 핵심 자산을 지키고 디지털 보안을 강화하기 위한 소스코드 관련 의무도 CPTPP를 통해 규범화되었다[5].

CPTPP 제14.17조 소스코드 규범은 자국 내 소프트웨어를 수입, 유통, 판매 또는 사용하는 것을 조건으로 정부가 소스코드에 대한 접근 또는 이전을 요구하지 못하도록 한다. 규범의 적용대상은 일반 대중이 소비자인 매스마켓(Mass Market)에서 판매되는 소프트웨어로 한정되고, 상업적 계약 내용에 의한 소스코드 제공 요구는 금지하지 않는다. 주요기반설비(Critical Infrastructure)에 이용되는 소프트웨어는 규범의 적용을 받지 않으며, CPTPP 협정 내 다른 규범과 불일치하지 않는 선에서 당사국의 법을 준수하기 위해 필요한 소스코드 수정을 요구하는 것은 가능하다. 마지막으로 특허 출원을 위한 요건 또는 특허 분쟁에 따라 사법기관이 소스코드에 대한 접근을 요구하는 경우는 승인되지 않은 접근에 대한 보호장치가 운영된다는 전제하에 허용된다.

CPTPP 이후에 체결된 자유무역협정과 디지털무역협정에서 소스코드 조항이 각 국가의 정부 정책을 반영하여 다양한 형태로 발전하는 것을 볼 수 있는데, USMCA 제19.16조와 같이 소스코드에 더하여 알고리즘까지 보호를 확대하는 규범 형태도 있고, 정부기관, 사법기관 또는 적합성평가기관 등 다양한 주체가 조사, 감독, 법 집행 등의 목적으로 필요한 경우 규제 권한을 가질 수 있도록 규범의 예외 영역을 확대한 형태의 UKSDEA 협정(제8.61-K조)도 찾아볼 수 있다.

4. 암호화 ICT 제품에 대한 접근 제한

WTO TBT(Technical Barriers to Trade) 협정은 모든 상품을 대상으로 기술규제로 야기될 수 있는 사업자에 대한 차별을 금지하고 기술규제가 보호무역의 수단으로 활용되지 않도록 하는 규범으로 구성되어 있다[11].

CPTPP TBT 챕터 부속서에는 7개의 세분화된 분야에 대한 분야별 규범을 추가적으로 규정한 것이 특징인데, 정보통신기술제품 분야에 암호기법을 이용하는 ICT 제품이 포함되어 있다[12]. 규범의 적용대상인 암호기법을 이용하는 ICT 제품(이하 '암호화 ICT 제품')은 상업용으로 설계된 상품을 의미하는 것으로 규정하고, 금융적 수단으로 이용되는 상품은 제외하였다.

이러한 암호화 ICT 제품에 대해 규범은 협정의 당사국이 제품의 제조업자 또는 공급자에게 제품의 제조, 판매, 유통, 수출 또는 사용에 대한 조건으로 특정 요건을 강제하는 기술규제 또는 적합성평가절차를 시행 또는 유지하는 것을 금지한다. 첫 번째 금지 요건은 제품의 암호기법과 관련하여 제조업자 또는 공급자에게 핵심이 되는 특정 기술, 생산 공정 또는 기타 정보에 대해 이전 및 접근을 요구하는 것이다. 두 번째 금지 요건은 자국 내 사업자와 파트너십을 요구하는 것이고, 마지막 금지 요건은 특정 암호화 알고리즘 또는 암호(Cipher)를 사용하거나 결합할 것을 강제하는 것이다.

암호화 ICT 제품을 제조하고 공급하는 사업자의 핵심 기술에 대한 유출이나 강제적 기술이전을 방지하고 이를 보호하기 위한 것이 규범의 원칙이다. 소스코드 규범과 유사하게 일부 정부 권한에 대해서는 예외적으로 인정하는데, 암호화 ICT 제품이 정부에 의해서 또는 정부를 위해서 제조, 판매, 유통, 수입 또는 사용되는 경우에는 규범을 적용하지

않음을 명확히 한다.

암호화 ICT 제품을 생산하는 사업자의 디지털 보안 및 핵심 기술 보호를 위해 정부의 접근을 최소화하기 위한 노력은 CPTPP 협정 이후 미국, 일본, 영국, 싱가포르가 체결한 다수의 디지털무역협정문에 포함되어 확산되고 있는 것을 확인할 수 있다[9,10].

Ⅲ. 디지털 보안 관련 주요국 입장 및 통상규범 동향

1. 미국

2013년 '주요기반시설(Critical Infrastructure)에 대한 사이버 보안 개선에 대한 행정명령'[13], 2017년 트럼프 행정부의 '연방 정부 네트워크와 주요 기반시설에 대한 사이버 보안 강화를 위한 행정명령'[14], 그리고 2021년 바이든 행정부가 내린 '국가 사이버 보안 개선을 위한 행정명령' 등은 사이버 보안에 대한 미국 행정부의 지속적인 관심과 우려를 보여준다[15].

국가 사이버 보안 개선을 위한 행정명령(EO 14028)은 특히 소프트웨어 공급망에 대한 보안 강화를 요구하는 내용을 포함하는데 소프트웨어 개발 및 공급 과정에서의 보안성 향상에 중점을 두고 있다. 행정명령에 따라 국가표준기술연구원(NIST)은 주요 소프트웨어(Critical Software)에 대한 정의와 주요 소프트웨어에 대한 안전조치, 소프트웨어 공급자가 준수해야 하는 최소 기준에 대한 가이드라인을 마련하고, 궁극적으로 자국의 소프트웨어 공급망의 보안성을 향상시킬 수 있는 방안 마련으로 이어졌다[16].

2022년 미국 사이버안보·인프라보호청(CISA: Cybersecurity and Infrastructure Security Agency)에서 발표한 'CISA 전략계획(CISA Strategic Plan 2023~2025)'은 사이버방어 능력을 강화하고 위험 감소 및 복원력을 증진하는 것을 핵심 목표로 규정한다. CISA 전략계획에는 주요 인프라 및 네트워크에 대해 사이버 공격으로부터 피해를 최소화하는 방안 마련 및 CISA의 위험 분석 기능 및 방법론 개선을 위한 과제도 포함한다[17].

미국은 보안 강화를 위한 정부의 규제 도입 필요성이 국경 간 자유로운 정보 이전과 무역을 제한할 수 있는 충분한 명분을 제공하고 있다는 점을 인지하고 있으며, 국제통상 규범 수립을 통해 최대한 시장 원칙을 해치는 않는 방향으로 각 정부가 정책을 수립하는데 기여할 수 있다는 입장을 유지하고 있다[18].

미국이 CPTPP 협정 당사국은 아니지만 CPTPP의 전신인 환태평양경제동반자협정(TPP: Trans-Pacific Partnership Agreement) 협상에 참여했던 국가라는 점에서 CPTPP 협정에도 미국의 디지털 통상 전략이 반영되었다고 볼 수 있다[19]. 2020년에 발효된 USMCA와 USJDTA에서 CPTPP 협정을 기반으로 규범이 구성되었지만, 일부 문안이 수정되거나 의무 수준 및 범위가 조정된 조항이 포함되어 있음을 확인할 수 있다. 디지털 분야에서의 보안 강화에 대한 미국 정부의 의지를 반영하듯 최근 미국이 체결한 두 개의 주요 협정에서는 디지털 보안과 연관된 사이버 보안, 소스코드, 암호화 ICT 제품 조항의 적용 대상 및 범위가 확대되거나 규범의 수준이 CPTPP 대비 높아졌다(표 1 참고)[5,7,9].

USMCA 및 USJDTA에서는 인정 조항 수준인 CPTPP 사이버 보안 규범 대신 당사국에 노력해야 하는 의무(Shall Endeavour)를 부여하는 규범을 포함하여 당사국의 의무 수준을 높이고, 사이버 보안 위협을 해결함에 위험기반접근방식이 처방적 규제방식보다 더 효과적임을 당사국 간 인정하도록 하였다. 추가로 당사국과 기업이 위험기반접근방식을 채택하도록 노력할 의무도 부여하였다.

표 1 미국 주도의 디지털 통상 협정 내 소스코드 규범 적용 대상 및 범위 비교

조항	협정	주요 내용
사이버 보안	CPTPP	• 컴퓨터 보안사고 대응을 담당하는 국가 기관의 역량 강화의 중요성 인정(Recognise) • 악의적인 침입 또는 악성 코드 배포의 식별 및 완화를 위해 기존 협업 메커니즘을 활용하는 것의 중요성 인정(Recognise)
	USMCA, USJDTA	• 국가기관의 역량 강화 및 기존 협업 메커니즘 활용을 위해 노력(Shall Endeavour) • 위험기반접근방식(Risk-based Approach)이 더 효과적일 수 있음을 인정(Recognise) • 당사국 및 자국 영토 내 기업에 위험기반접근방식 도입을 위해 노력(Shall Endeavour)
소스코드	CPTPP	• 소스코드 강제 이전 및 접근 금지 • 매스마켓(Mass Market)에 한정되며, 주요기반설비(Critical Infrastructure)에는 미적용 • 상업적 계약, 국내법 준용을 위한 요건, 특허 출원 또는 분쟁 관련 요건인 경우는 허용
	USMCA, USJDTA	• 소스코드 및 알고리즘 강제 이전 및 접근 금지 • 규제기관 및 사법당국의 특정 조사, 수사, 검사, 집행조치, 사법절차에 따른 요건인 경우는 허용
암호화 ICT	CPTPP	• TBT 협정문의 부속서로 포함 • 상업용 암호화 ICT 제품에 대해 암호기법에 관련된 특정한 기술, 생산 공정 또는 기밀 정보의 이전 및 제공, 파트너십 강요, 특정 암호 알고리즘 사용을 강제하는 기술규제(Technical Regulation) 또는 적합성평가절차(Conformity Assessment Procedure) 요구 금지
	USMCA	• TBT 협정문의 부속서로 포함 • 상업용 암호화 ICT 제품에 대해 암호기법에 관련된 특정한 기술, 생산 공정 또는 기밀 정보의 이전 및 제공, 파트너십 강요, 특정 암호 알고리즘 사용 강제 금지
	USJDTA	• 디지털무역협정의 일부로 포함 • 상업용 암호화 ICT 제품에 대해 암호기법에 관련된 특정한 기술, 생산 공정 또는 기밀 정보의 이전 및 제공, 파트너십 강요, 특정 암호 알고리즘 사용 강제 금지

출처 Reproduced from [5,7,9].

소스코드 보호와 관련하여 USMCA 및 USJDTA에서는 보호 대상에 알고리즘이 포함됨을 명시하여 규범의 적용 대상을 확대하였으며, 매스마켓에서 판매하는 소프트웨어로 한정하거나 주요기반설비에 사용되는 소프트웨어에는 적용을 배제한다는 문안을 삭제하여 예외 범위를 최소화하였다. CPTPP TBT의 부속서 일부로 포함하여 ICT 제품의 주요한 기술, 생산 공정, 기밀 정보 등을 보호하고자 했던 암호화 ICT 제품 조항에 대해서는 USMCA와 USJDTA를 통해 금지하는 당사국의 조치를 기술규제 또는 적합성평가절차로 한정하지 않고 당사국의 모든 조치로 확대 적용하여 규범에 명시된 특정 목적 외에는 상업용 ICT 제품에 대해 암호기법에 대한 이전 및 제공, 파트너십 강요, 특정 알고리즘 사용을 강제하지 못하도록 하였다.

2. 유럽연합

유럽연합에서는 디지털 요소를 포함하는 하드웨어 및 소프트웨어를 대상으로 보안 요구사항을 강화하는 법안이 추진되었다[20]. '유럽연합의 사이버 복원력 법안(EU Cyber resilience Act)'은 디지털 요소를 포함하는 하드웨어 및 소프트웨어에 필수적인 보안 능력을 갖추도록 요구하며, 디지털 제품의 설계, 개발 단계를 포함하는 전 생애주기 관리방식을 통해 제품의 보안성을 높이고, 하드웨어와 소프트웨어 생산자 모두가 규정을 준수할 수 있도록 일관성 있는 사이버 보안 프레임워크를 보장하는 것을 목표로 한다. 또한, 디지털 제품의 보안 속성에 대한 투명성을 강화하여 궁극적으로 비즈니스와 소비자가 디지털 제품을 안전하게 이용할 수 있도록 목표한다[21].

2022년 12월 유럽연합 의회 및 유럽 이사회는 유럽연합 전체에 적용되는 최초의 사이버 보안 법률인 Network and Information Security(NIS) 지침을 대체하는 NIS 2.0 도입을 승인하였으며, 유럽연합 전체의 사이버 보안 프레임워크를 전폭 개정하는 작업에 착수했다. NIS 2.0은 기존 대비 확장된 영역을 대상으로 사이버 보안 역량의 강화를 목적으로 에너지 시스템, 건강관리 네트워크, 교통 시스템 등의 주요기반시설을 집중적으로 관리하도록 하는 내용을 담고 있다. 지침은 국가 당국 간의 협력 촉진 및 공동 대응체계 구축을 위한 EU CyCLONe(European Cyber Crises Liaison Organisation Network) 설립의 기반을 제공하기도 하였다[22].

유럽연합이 WTO 전자상거래 공동선언문 협상에서 디지털통상 관련 규범에 대한 입장을 적극적으로 개진하고 있는 것과 달리, FTA에서는 디지털 무역에 대한 규범들을 종합적으로 포함하는 모습을 보이지는 않는다[23].

유럽연합은 캐나다('17년 발효), 일본('19년 발효), 싱가포르('19년 발효), 베트남('20년 발효), 그리고 영국('21년 발효)과 연달아 양자 무역협정을 체결하였지만, 소스코드를 다루는 조항은 일본 및 영국과의 협정에만 포함되어 있다.

유럽연합이 비교적 최근 체결한 무역협정인 유럽연합-일본 경제동반자협정(EPA: Economic Partnership Agreement)[24]과 유럽연합-영국 간 무역협력협정(TCA: Trade and Cooperation Agreement)[25]에도 암호기법을 이용한 ICT 장비, 인공지능, 데이터 혁신과 같은 디지털 분야 신규 규범은 포함되지 않았다.

캐나다, 싱가포르, 베트남이 CPTPP 당사국이고, 영국과 일본이 디지털 무역 규범 수립에 적극적인 국가라는 점을 고려하면 유럽연합이 디지털 분야에 대한 무역 규범을 수립하는 것에 상당히 신중한 입장임을 이해할 수 있다.

유럽연합과 일본 간 EPA와 유럽연합과 영국 간 TCA 협정의 디지털 분야 규범에서 공통적으로 포함된 소스코드 조항은 당사국에 협정체결 상대국의 사업자가 소유한 소프트웨어의 소스코드에 대한 이전 또는 접근을 요구할 수 없도록 규정하였는데, 규범의 적용 대상을 알고리즘으로 확대하지 않고 소스코드로 한정하였다. 이는 소스코드 외 알고리즘에 대한 접근 및 이전을 요구하는 것을 금지하도록 한 규범을 이미 수용한 바 있는 영국과 일본을 고려했을 때 주목할 만한 부분이다.

두 무역협정은 소스코드 원칙과 관련하여 경쟁법 위반에 따른 조치 또는 지식재산권의 보호를 위한 조치에 대해서는 정책 권한이 있음을 명백히 하였다. 또한, 유럽연합과 영국 간 협정에는 인증 절차에 필요한 소스코드 접근 및 이전에 대해서도 당사국이 조치를 취할 수 있도록 하였다. 사업자의 불공정한 행위와 지식재산권 침해에 대한 대응 그리고 적합성평가제도와 같은 인증 절차에 대한 국내 제도를 반영하기 위한 노력으로 볼 수 있다.

유럽연합-영국 TCA에는 사이버 보안과 관련하여 다양한 협력 방안을 모색하는 규범을 포함하고 있다. 일반적인 정보, 경험, 모범사례 등의 공유를 도모하는 조항 외에도 필요시 유럽연합의 컴퓨터비상대응팀(CERT-EU: Computer Emergency Response Team-European Union)과 영국의 컴퓨터비상대응팀이 협업하고, 유럽연합의 네트워크 및 정보보안 기구(ENISA: European Union Agency for Cybersecurity)의 역량 강화, 지식 습득, 교육 등에 영국이 참여할 수 있도록 하는 등의 유사 기관 간의 구체적 협력 방안을 포함하였다(표 2 참고)[25].

3. 영국

영국은 '국가 사이버 전략 2022(National Cyber

표 2 EU-영국 TCA 사이버 보안 관련 조항 및 주요 내용

조항	주요 내용
제703조 사이버 이슈에 대한 대화체(Dialogue)	• 정책 개발과 관련된 정보 공유를 위한 정기적인 대화체를 설립하도록 노력
제704조 사이버 이슈에 대한 협력	• 상호 이익이 있는 경우, 개방·자유·안정·평화·안전한 사이버 공간 유지를 위해 협력 • 국제기구 및 포럼에서 글로벌 사이버 회복력을 강화하고, 제3국이 사이버범죄에 효과적으로 대응할 수 있도록 역량 강화를 위해 협력
제705조 컴퓨터비상대응팀(CERT-EU)과 협력	• 양국의 컴퓨터비상대응팀은 일반적인 위협 및 취약성에 대응하기 위한 기술, 전술, 절차, 모범사례 등과 같은 방식에 대한 정보 공유를 위해 자발적이고 시기적절하게 상호 협력
제706조 EU 지침 2016/1148에 따라 설립된 협력 그룹(Cooperation Group) 특정 활동에 참여	• 네트워크 및 정보시스템의 안전을 보장하기 위한 역량 강화 관련 모범사례 공유 • 위험(Risk) 및 사건(Incident) 관련 정보, 경험, 모범사례 공유 • 네트워크 및 정보시스템의 안전을 보장하기 위한 역량 강화 관련 모범사례 공유 • 인식 개선, 교육 프로그램, 훈련 등에 대한 정보 및 모범사례 공유 • 네트워크 및 정보시스템 관련 R&D에 대한 정보 및 모범사례 공유
제707조 유럽 네트워크 및 정보보안 기구 (ENISA)와 협력	• 역량 강화, 지식 및 정보, 인식 개선 및 교육을 위해 협력

출처 Reproduced from [25].

Strategy 2022)'를 통해 향후 3년간 달성하고자 하는 다섯 가지 목표를 제시하였다[26]. 국내 기관 간 협업을 도모하고 사이버 전문 인력을 양성하여 영국의 사이버 생태계를 강화하고, 복원력을 갖춘 디지털 영국을 구축하는 것, 국가 암호화 기술 기업을 보호하는 전략을 포함하여 사이버 파워(Cyber Power)에 필수적인 기술을 선점하고 글로벌 리더십 및 영향력을 증진하는 것, 마지막으로 사이버 공간에서의 위협 요소에 효과적으로 대응하여 궁극적으로 국가 안보를 강화하는 것이 제시된 구체적인 목표이다.

브렉시트(Brexit) 이후 영국은 지금까지 70개 이상의 국가와 무역협정을 맺어왔으며, 영국-싱가포르 디지털경제협정(DEA: Digital Economy Agreement)과 같이 디지털 분야에 특화된 협정도 포함한다[27].

영국-싱가포르 DEA('22년 발효)와 영국-호주 FTA('23년 발효)의 사이버 보안 규범은 양 당사국이 사이버 보안 측면에서 당사국이 중요성을 인정하는 내용을 상세하게 담고 있다. 특히, 영국-싱가포르 DEA에서는 사이버 보안을 담당하고 있는 국가 기관의 역량 강화 및 협력 메커니즘을 강화하는 것 외에도 정보 공유 및 모범사례와 관련된 대화 채널을 유지하는 것, 사이버 위생(Cyber Hygiene) 수준을 높이고 국내 사이버 공간에 대한 보안성을 강화하기 위해 소비자가 사용하는 사물인터넷 장비 관련 기본 보안 표준에 대한 상호인정을 추진하는 것, 산·학·연 간 혁신적인 프로젝트 또는 사이버 보안 분야에 대한 공동 R&D를 추진하는 것을 포함한다.

위험기반접근방식이 준수사항을 나열하는 처방적 방식 또는 규정준수(Compliance-based) 방식보다 사이버 보안에 관하여 더 효과적인 대응 방식임을 인정하고, 개방적이고 투명한 산업 표준에 기반한 위험기반접근방식을 기업들이 도입할 수 있도록 독려하는 내용도 두 협정에 일관성 있게 담아내고 있다.

소스코드 규범에서는 소스코드 외 알고리즘까지 보호 대상으로 확대하였고, 소스코드 또는 알고리즘에 접근하고 공개를 요구할 수 있는 대상에 적합성 평가기관을 추가하였다. 적합성 평가기관을 규

제기관과 분리하여 다루고, 적합성 평가기관이 법에 따라 필요한 평가를 수행할 수 있도록 권한을 보장하는 방식이다.

영국-싱가포르 DEA는 암호화 ICT 제품 규범(제8.61조-I)에서 ICT 제품의 범위를 상품으로 한정하지 않아 동 규범이 서비스에도 적용될 수 있도록 하였으며, 기술규제 또는 적합성평가절차에 관련된 특정 조치가 아닌 정부의 모든 조치가 규범의 적용 대상이 되도록 하였다. 주요 규범의 적용 대상을 확대하는 대신 적용면제 범위를 구체적으로 명시하는 방식을 선택하여 필요한 정책 권한은 명확히 확보하는 방식을 추진한 것으로 이해할 수 있다(표 3 참고)[10].

표 3 영국-싱가포르 DEA 암호화 ICT 제품 규범 주요 내용

	영국-싱가포르 DEA (제8.61-I조)
적용 대상	ICT 제품
주요 규범	제조, 판매, 유통, 수입, 이용을 조건으로 다음의 요건 부여 금지 • 암호화에 관한 특정 기술, 생산공정, 정보의 이전 또는 접근 강제 • 자국 내 사업자와의 파트너십 강제 • 특정 암호화 알고리즘 사용 또는 결합을 강제
적용 면제	• 암호화 또는 암호화되지 않은 통신을 제공하도록 하기 위해 서비스 제공자에게 암호화를 사용할 것을 법적 절차에 따른 요구 조치 • 금융상품에 대한 규제 조치 • 정부의 소유 또는 통제하에 있는 네트워크 접속에 관한 조치 • 금융 서비스 제공자 및 금융시장의 감독, 조사, 심사에 관한 조치 • 정부를 위하거나 정부에 의한 암호화 ICT 제품을 제조, 판매, 유통 수입, 또는 사용하는 경우에 대한 조치 • 규제기관 및 사법기관이 조사, 검사, 검수, 법 집행, 사법절차의 진행을 위해 암호 기술 등에 대한 보존 또는 공개를 요구하는 조치 • 경쟁법에 의해 내려지는 교정조치 부과 및 집행의 목적으로 암호기술의 접근 또는 이전을 요구하는 조치

출처 Reproduced from [10].

4. 중국

중국은 인터넷과 인터넷에 연결되는 하드웨어 및 소프트웨어를 대상으로 보안과 관련된 높은 수준의 규제를 유지하고 있다[28].

국가사이버공간안전전략을 시작으로 사이버 보안법이 시행되었으며, 특히 사이버 보안법을 통해 네트워크 운영자 행위에 다양한 요건을 부과하고 있다[29].

2022년 9월 국가인터넷정보판공실은 사이버운영 안전과 관련된 기본 법률 책임을 보완하는 방향으로 사이버 보안법 개정을 진행하였다. 개정된 내용에 따르면 인터넷 운영자는 사이버안전 등급보호 제도의 요구에 따라 안전보호 의무를 이행해야 하고, 네트워크 제품과 서비스는 관련 국가표준의 강제성 요구에 부합해야 한다. 그리고 네트워크 핵심설비와 네트워크 안전 전용제품은 관련 국가표준의 강제성 요구에 따라 안전인증 합격 또는 안전 검측 요구에 부합한 후에야 판매 또는 제공이 가능하다[30].

WTO 전자상거래 공동선언문 협상에 중국도 참여하고 있으며, 중국은 2019년 4월에 전자상거래 협상 관련 자국 입장을 정리한 커뮤니케이션(Communication) 문서를 제출하였다. 커뮤니케이션 문서에서 중국은 전자상거래를 위한 건전한 환경 구축, 전자상거래를 위한 안전하고 신뢰할 수 있는 시장 환경 조성, 그리고 실용적이고 포괄적인 개발 협력 촉진이 필요함을 강조하고, 이를 달성하기 위한 구체적인 규범과 정책 방향성을 함께 제시하였다. 전자인증 및 서명, 전자 계약, 온라인 소비자 보호와 개인정보보호 등의 규범이 포함되어 있으며, 사이버 보안에 대한 제안도 있으나 각 국가의 인터넷 주권(Internet Sovereignty)을 존중해야 함을 우선적으로 명시하였다[31].

WTO 가입 이후 중국 또한 자유무역협정을 지속적으로 체결해왔지만 인터넷 서비스에 대한 접근, 데이터의 자유로운 이전, 컴퓨팅설비 위치 강제 금지, 소스코드와 같은 신통상규범을 포함하지 않거나 높은 수준의 의무를 부담하지 않는 방식으로 전자상거래 또는 디지털통상 분야에서 소극적인 태도를 유지하고 있다[28].

Ⅲ. 결론

ICT 기술이 발전함에 따라 클라우드 서비스, 사물인터넷, 인공지능 시스템, 자율주행 자동차와 같이 기존 제품과 서비스에 디지털 요소가 추가되고 다양한 기술이 융합되면서 상품과 서비스, 하드웨어와 소프트웨어 간 명확한 구분이 어려운 ICT 제품들이 국경 간 무역의 대상이 되고 있다.

디지털 분야에 대한 보안 조치 강화를 위해 각국 정부는 사이버 보안전략을 수립하고 사이버 보안법을 제정하고 있다. 구체적으로는 국가 인프라 또는 이용자에게 해를 끼칠 수 있는 위험요소를 최소화하기 위한 적합성평가제도를 시행하고, 인증을 요구하며, 필요한 경우 사업자의 소스코드 또는 알고리즘을 살펴보고 평가한다. 한편 디지털 분야의 보안 강화에 대한 필요성은 무역장벽을 높이고 보호주의적 무역 조치를 도입하는 것에 대한 명분을 제공한다.

전통적인 WTO 통상 규범이 직면한 한계와 디지털 보안에 대한 강화된 정부 조치에 대응하기 위해서 국제통상 규범 측면에서도 새로운 접근 방식이

표 4 디지털 보안에 대한 주요국 통상 규범 비교

	사이버 보안	소스코드	암호화 ICT 제품
미국	• 사이버 보안 사고 대응 담당 국가기관의 역량 강화를 위해 노력 • 사이버 보안 사고에 대응할 수 있도록 협력 메커니즘 강화 노력 • 위험기반접근방식 선호 • 기업에 위험기반접근방식 도입 장려	• 소스코드 및 알고리즘 보호 • 제한적인 정책권한 인정 범위 유지 – 규제기관 및 사법당국의 특정 조사, 수사, 검사, 집행조치, 사법절차에 따른 요건인 경우 포함	• 암호기법을 이용하는 상업용 상품(Goods)에 한정하여 규범 적용 • TBT 규정(기술규제, 적합성평가)에 한정하지 않고 모든 정부 조치로 확대하여 규범 적용 • 제한적인 정책권한 인정 범위 유지
유럽 연합	• 사이버 보안 사안에 대한 정보 공유 및 대화체 유지를 위해 협력	• 소스코드 보호로 제한 • 정책권한 인정 범위 확대 – 인증 절차에 따른 경우, 정부 조달 및 상업적 계약에 따른 경우, 경쟁 왜곡에 대한 조치에 따른 경우, 온라인 이용자의 공중안전보호를 위한 조치에 따른 경우, 지식재산권 보호를 위한 경우 등을 포함	규범 미채택
영국	• 정보 공유 및 모범사례 공유를 위한 대화체 유지 중요성 인정 • 보안 표준 관련 상호인정에 대한 중요성 인정 • 산·학·연 간 혁신 프로젝트 및 공동 R&D 추진의 중요성 인정 • 위험기반접근방식 선호	• 소스코드 보호로 제한 • 정책권한 인정 범위 확대 – 상업적 계약에 따른 경우, 오픈소스 라이센스인 경우, 적합성평가기관의 평가 절차에 따른 경우 등을 포함	• 암호화 ICT 제품을 상품으로 한정하지 않음 • 모든 정부 조치에 규범을 적용 • 정책권한 인정 범위 확대 – 규제기관 및 사법 당국이 조사, 수사, 검사, 집행조치, 사법절차에 따른 요건인 경우, 경쟁법에 따른 교정 요건인 경우 포함
중국	• 인터넷 주권 존중 • 컴퓨터 안전사고 대응을 담당하는 국가기관의 역량을 강화하고 협력 메커니즘을 활용하는 것의 중요성 인정	규범 미채택	규범 미채택

제시되고 있다. CPTPP 협정을 시작으로 무역 규범을 중요시하는 다수 정부의 지지를 받아 사이버 보안, 소스코드, 암호화 ICT 제품에 대한 규범은 이제 디지털 통상 협정에서 필수적으로 논의되는 사안으로 발전하였다.

표 4와 같이 우리나라의 주요 무역 상대국인 미국, 유럽연합, 영국, 중국은 디지털 보안에 대해 다양한 입장을 유지하고 있다. 디지털 보안에 대해서 인터넷 주권 등 최대한 정책 권한을 확보하고자 하는 중국을 제외하고는 국제통상 차원에서 당사국에 부여하는 의무를 보다 더 강화하고 있는 것을 확인할 수 있다.

사이버 보안 규범 측면에서는 무역장벽을 최소화하는 방식으로 위험기반접근방식을 채택하고, 협력의 범위를 점차 다양화하는 시도들이 이루어지고 있다. 소스코드 및 알고리즘에 대한 당사국의 접근을 금지하는 규범에 대해 미국과 유럽연합 및 영국과 입장에 차이는 있지만, 소스코드에 대한 무분별한 접근을 방지할 필요성이 있다는 것에는 합의가 이루어지고 있다. 마지막으로 암호화 ICT 제품 규범은 상품에 대한 기술규제 또는 적합성평가절차에 관련된 당사국의 조치를 제한하는 것에서 서비스에 대한 전반적인 조치로까지 규범의 적용범위가 확대되고 있다.

국제통상규범은 많은 국가가 동일한 규범을 수용하고 채택하여 확산되었을 때 비로소 그 진가를 발휘할 수 있다. 현재는 미국, 유럽연합, 영국 그리고 이 국가들과 무역협정을 체결한 국가인 일본, 싱가포르, 호주 등의 국가들이 제한적으로 디지털 보안 관련 규범들을 수용하고 있다. 앞으로는 디지털 보안과 관련된 규범 확산에 의지가 있는 국가들과 이미 관련 규범을 채택하고 있는 국가들이 협력하여 WTO 전자상거래 공동선언문 협상, IPEF, 다자 및 양자 무역협정 등 다양한 플랫폼을 활용하여 관련 이슈를 논의하고 규범화하기 위한 시도를 지속할 것으로 예상된다. 그리고 이러한 움직임은 국내외적으로 디지털 분야의 법과 제도를 형성하는 것에 적지 않은 영향을 미칠 수 있다는 점에서 신규 디지털 서비스에 대한 이용, 관리, 보안 관련 국내 제도 수립 시 해외 주요국의 무역협정 체결 현황 및 세부 내용에 대해서도 면밀하게 살펴볼 필요가 있다.

용어해설

IPEF 2022년 5월 공식 출범하여 인도태평양 지역의 총 14개국이 참여하고 있음. 무역, 공급망, 청정경제, 공정경제 분야에 대해 신통상이슈를 중심으로 규범과 협력을 논의하는 다자경제협력체

TBT 표준, 기술규정 및 적합성평가절차가 협정 당사국 사이의 상품교역에 불필요한 장애를 초래하지 않도록 보장하기 위한 것이며, WTO TBT 협정의 내용을 기반으로 투명성, 공동협력, 협의채널, 정보교환 등의 조항으로 구성

WTO 전자상거래 공동선언문 협상 1998년 2월 미국이 WTO 일반이사회에 전자상거래 무관세화에 대한 국제규범 제정을 공식적으로 제안하면서 시작되었으며, 2023년 현재 총 89개 WTO 회원국이 협상에 참여

약어 정리

CERT	Computer Emergency Response Team
CISA	Cybersecurity and Infrastructure Security Agency
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
ENISA	European Union Agency for Cybersecurity
IPEF	Indo-Pacific Economic Framework
RCEP	Regional Comprehensive Economic Partnership
TBT	Technical Barriers to Trade
TPP	Trans-Pacific Partnership Agreement
USJDTA	U.S.-Japan-Digital Trade Agreement
USMCA	U.S.-Mexico-Canada Agreement
WTO	World Trade Organization

참고문헌

[1] https://www.wto.org/english/thewto_e/whatis_e/inbrief_e/inbr_e.htm

[2] Neha Mishra, "The trade:(Cyber) security dilemma and its impact on global cybersecurity governance," J. World Trade, vol. 54, no. 4, 2020, pp. 567-590.

[3] J.P. Meltzer, "Cybersecurity, digital trade, and data flows: Re-thinking a role for international trade rules," Global Economy and Development, Brookings Institution, Working Paper 132, May, 2020.

[4] 김지은, "해외 주요국의 디지털 통상 정책 및 무역 협정 규범 동향," 전자통신동향분석, 제37권 제5호, 2022.

[5] https://www.dfat.gov.au/sites/default/files/14-electronic-commerce.pdf

[6] https://www.dfat.gov.au/sites/default/files/rcep-chapter-12.pdf

[7] https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf

[8] https://www.dfat.gov.au/trade/agreements/not-yet-in-force/aukfta/official-text

[9] https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf

[10] https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/UKSDEA

[11] 안덕근, 김민정, "국제통상체계와 무역기술 장벽," 박영사, 2018. 1. 30.

[12] https://www.dfat.gov.au/sites/default/files/8-technical-barriers-to-trade.pdf

[13] CISA, "Fact sheet: EO 13636 improving critical infrastructure cybersecurity and PPD 21 critical infrastructure security and resilience," Mar. 2013.

[14] CISA, "Executive order on strengthening the cybersecurity of federal networks and critical infrastructure," https://www.cisa.gov/topics/cybersecurity-best-practices/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure

[15] NIST, Improving the Nation's Cybersecurity: NIST's Responsibilities Under the May 2021 Executive Order, https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity

[16] NIST, Definition of Critical Software Under Executive Order(EO) 14028, White Paper, Oct. 13, 2021.

[17] https://www.cisa.gov/sites/default/files/2023-01/StrategicPlan_20220912-V2_508c.pdf

[18] World Trade Organization, "Joint statement on electronic commerce initiative," Mar. 2019.

[19] Congressional Research Service, "Digital trade and data policy: Selected key issues," CRS Report, Mar. 16, 2023.

[20] European Commission, "State of the union: New EU cybersecurity rules ensure more secure hardware and software products," Sept. 15, 2022.

[21] European Commission, "Proposal for a regulation of the european parliament and of the council on horizontal cybersecurity requirements for products with digital elements and amending regulation (EU) 2019/1020," Sept. 15, 2022.

[22] World Economic Forum, "New european union cybersecurity proposal takes aim at cybercrime," Sept. 28, 2022.

[23] World Trade Organization, "Joint statement on electronic commerce: EU proposal for WTO disciplines and commitments relating to electronic commerce," Oct. 2019.

[24] https://www.mofa.go.jp/files/000382106.pdf

[25] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/982648/TS_8.2021_UK_EU_EAEC_Trade_and_Cooperation_Agreement.pdf

[26] Policy Paper, National Cyber Strategy 2022 Pioneering a cyber future with the whole of the UK, 2022.

[27] https://www.gov.uk/government/collections/the-uks-trade-agreements

[28] H. GAO, "Across the great wall: E-commerce joint statement initiative negotiation and China," Artificial Intelligence and International Economic Law, Cambridge University Press, Cambridge, UK, 2021, pp. 1-19.

[29] 박민숙, 이효진, "중국의 사이버보안 정책연구," 대외경제정책연구원, 연구자료 20-03, 2020.

[30] 김연, "중국 사이버보안법 개정안 발표," 차이나 법률 정보, 한국무역협회 베이징지부, 2022. 9. 29.

[31] World Trade Organization, "Joint statement on electronic commerce, communication from China," Apr. 34, 2019.