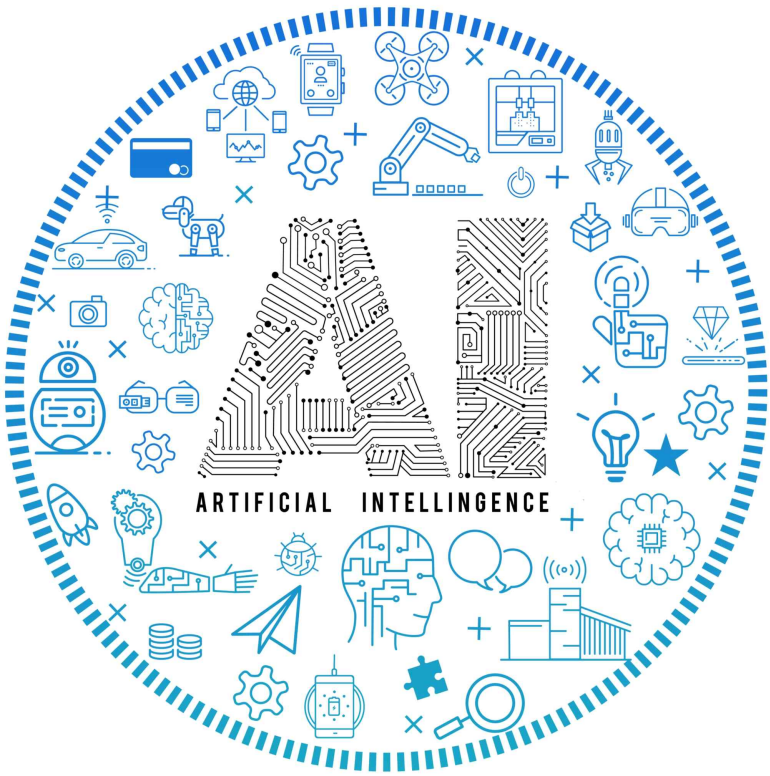
AI(인공지능) 분야

– 사이버보안 –

국가별 규제·정책 동향 중심으로



산업통상자원부
국가기술표준원

TBT 종합지원센터
R&I Center

이슈 요약

– 가천대학교 조영임 교수–

규제 개요

* 본 이슈리포트는 글로벌 AI 사이버보안 규제 동향 및 현안에 대해 서술하였으며, 규제 개요 및 경과는 그 중 대표적인 유럽연합의 인공지능 법(AI Act)를 주제로 작성하였음

규제 목적

유럽연합은 주요 국가 중 최초로 인공지능(AI)에 대한 포괄적이고 구속력 있는 규제를 공개하여, AI가 사람의 안전이나 인권에 위협을 가하는 것을 법안을 통해 사전에 방지하고자 함

> **2021년 EU AI Act 초안 발표 배경**
>
> 2021년 4월 21일, 유럽 집행위원회(European Commission, EC)는 EU의 가치, 기본권, 원칙을 존중하고 법적 불확실성을 제거하기 위해 인공지능 사용이 가져올 고위험 요인을 명시하는 한편, 규제로 인해 기술 개발의 과도한 제약요건이 되지 않게 최소 필요조건으로 EU AI Act를 제안함

규제 요지

– 유럽 집행위원회(EC)는 2018년 4월 '유럽을 위한 인공지능'에 대한 커뮤니케이션을 발표한 이후 산업 부문의 디지털 전환정책을 추진

– '미래세대 보호를 위한 법적 과제 4'에 따르면, 유럽연합은 중장기적 정책 기조와 인공지능에 대한 안전 및 책임 문제에 대한 분석 의견을 제시

– 동 법안은 '유럽의 디지털 미래 구상전략' 의견서에서 발표된 정책 방향에 따라 제안

> **유럽의 디지털 미래 구상전략의 3가지 축**
>
> ① **(사람을 위한 기술 전략)** 인간에게 궁극적으로 이로운 방식의 AI 개발 및 사이버 위협으로부터의 보호 등
> ② **(공정하고 경쟁력 있는 디지털 경제)** 온라인 서비스/플랫폼의 규범 확립, 책임 강화 및 유럽 내 기업 간 공정경쟁, 데이터 접근성 보장 등
> ③ **(개방적이고 민주적이고 지속 가능한 사회)** 시민들의 데이터 리터러시를 배양하고 '유럽 건강 데이터 공간'을 구축

적용범위

– 유럽연합 내에서 AI 시스템을 출시하거나 서비스를 도입하는 모든 제공자

– 유럽연합 내에 위치하는 AI 시스템의 사용자

– AI 시스템이 생성한 결과물이 유럽연합 내에서 사용될 시, 제3국에 위치한 AI 시스템의 제공자 및 사용자도 규제 대상

시행일

법안은 2024년 8월 1일 발효되었으나, 실제 적용은 발효일로부터 2년 후인 2026년 8월부터 적용

규제동향 및 현안

EU CIoT 보안 표준

- 유럽연합 무선기기 지침(RED)과 관련, 사이버보안 규제가 강화되고 있으며 IoT 기기가 사이버공격의 주요 대상 중 하나가 되어 보호 표준 중요성이 더 높아짐
- 소비자 제품에 대한 우수한 보안 기준을 지원하며, 기본 암호 없음, 취약성 공개 정책 구현, 소프트웨어 업데이트 유지 등 상위 3가지 권장사항 제공 및 소비자 IoT 장치에 대한 특정 데이터 보호 조항이 포함

제조업체

- (필수조항) **33개 요구사항** 이행
- (권장사항) 35개 항목을 모두 구현하는 제품 설계. 제조업체는 다른 기관과 협력하여 ETSI EN 303 645 시험 및 적합성 선언(AoC)을 실시해, 소비자에게 보다 큰 확신을 심어 향후 잠재적인 규제 준수 요구사항을 충족할 수 있음

중요성

- 소비자 IoT 사이버보안 및 데이터 보호를 다루는 14개 영역을 포함하는 표준으로 제조업체와 IoT 이해 당사자가 얻을 수 있는 달성 가능한 단일 기준

구성

- 소비자 IoT를 위한 13가지 사이버보안 영역
  - 범용 디폴트 암호사용 금지
  - 취약성 보고서 관리 수단 이행
  - 소프트웨어 최신 상태로 유지
  - 민감한 보안 매개 변수를 안전하게 보관
  - 안전한 통신
  - 노출된 공격 표면 최소화
  - 소프트웨어 무결성 보장
  - 개인정보 보안 보장
  - 전력공급 중단에 대한 시스템 복원력 확보
  - 시스템 원격 측정 데이터 검토
  - 사용자가 쉽게 개인정보를 삭제할 수 있도록 보장
  - 손쉬운 디바이스 설치 및 유지 보수
  - 입력 데이터 유효성 검사

시사점 및 대응방안

시사점

- 신기술과 새로운 보안 정책의 도입(인공지능, 제로 트러스트)에 따른 사이버보안 환경의 복잡성 심화로 기업 보안 전략 재정비 필요
- 사이버공간의 환경변화에 능동적 대응 및 중장기적인 기술개발과 안전한 디지털 사회 구현을 위한 거버넌스 수립과 국제 공조 체계 확립 필요

대응 방안

- 사이버 공격을 적극적·선제적으로 방어하는 방식으로 진화하거나, 전 세계적으로 보안 패러다임 전환기를 고려하여 중장기적 관점에서 R&D 포트폴리오의 다변화 필요
- 제로 트러스트, 사이버 복원력, 공급망 보안 등 정책적 분야의 개념 확립, 기반 연구를 통해 기술적 정의와 목표를 명확히 설정하여 중장기적인 지원이 필요
- 개인정보보호·데이터 보안 분야에 집중(총투자액의 22.8%)되어 있어, 보안 기술·산업 변화를 고려한 투자 분야의 다변화가 필요

사이버보안-정부 R&D 투자

- 과거 5년간 정부 R&D과제 투자액의 31.6%가 개인정보보호 분야에, 중점 분야를 기준으로 24.6%가 데이터・AI 보안에 집중
- DX/AX에 따른 기술·산업의 융·복합을 고려하여 산업제어시스템(총투자액의 18.2%차지) 분야 외의 다양한 산업 도메인을 고려한 융합보안 분야의 투자 강화가 요구됨

목차

1 규제 개요

규제 개요

규제명

EU 인공지능 법(EU AI Act)*

* 본 이슈리포트는 글로벌 AI 사이버보안 규제 동향 및 현안에 대해 서술하였으며, 규제 개요 및 경과는 그 중 대표적인 유럽연합의 인공지능 법(AI Act)를 주제로 작성하였음

도입 배경

유럽연합(European Union, EU)은 주요 국가 중 최초로 인공지능에 대한 포괄적이고 구속력 있는 규제안을 공개하였으며, AI가 사람의 안전이나 인권에 위협을 가하는 것을 법안을 통해 사전에 방지

- 유럽 집행위원회(European Commission, EC)는 2018년 4월 '유럽을 위한 인공지능'에 대한 커뮤니케이션을 발표한 이후 산업 부문의 디지털 전환정책을 추진
- '미래세대 보호를 위한 법적 과제 4*'에 따르면, EU는 중장기적 정책 기조와 인공지능에 대한 안전 및 책임 문제에 대한 분석 의견을 제시
  * 미래세대 보호를 위한 법적 과제 4 – 인공지능에 대한 유럽연합의 규제체계와 대응 전략을 중심으로
- 동 법안은 '유럽의 디지털 미래 구상전략' 의견서에서 발표된 정책 방향에 따라 제안됨

> **2021년 EU AI Act 초안 발표 배경**
>
> 2021년 4월 21일, EC는 EU의 가치, 기본권, 원칙을 존중하고 법적 불확실성을 제거하기 위해 인공지능 사용이 가져올 고위험 요인을 명시하는 한편, 규제로 인해 기술 개발의 과도한 제약요건이 되지 않게 최소 필요조건으로 EU AI Act를 제안함

규제목적

유럽연합은 주요 국가 중 최초로 인공지능(AI)에 대한 포괄적이고 구속력 있는 규제를 공개하여, AI가 사람의 안전이나 인권에 위협을 가하는 것을 법안을 통해 사전에 방지하고자 함

- AI 솔루션을 시장에 출시하는 데에 드는 비용을 줄이고, 관련 기술의 개발을 과도하게 방해·제한하는 것을 방지하고, AI와 관련된 위험설 및 문제를 해결하기 위한 최소 요건을 명시함

- 위험 기반 접근방식에 따라 위험성이 높은 인공지능 시스템에 더욱 엄격한 요건 적용
- 위험성이 낮은 AI 시스템에는 가벼운 수준의 의무를, 고위험 AI 시스템에는 영향평가 등 추가적인 의무사항을 적용, 용인할 수 없는 위험성이 있는 인공지능 시스템은 EU 내 사용 금지
- 인지 행동 조작, 소셜 스코어링, 프로파일링 기반 치안 예측, 생체인식정보를 사용하여 인종·종교·성적 취향 등 특정 범주로 사람을 분류하는 시스템 등은 EU에서 사용할 수 없음
- 범용 AI(General Purpose AI, GPAI) 시스템의 경우 시스템적 위험을 내포하지 않은 AI 시스템은 가벼운 수준의 의무를 부과하나, 시스템적 위험을 내포할 경우 추가적인 요건을 준수하도록 의무화

시행일

동 법안은 2024년 8월 1일 발효되었으나, 실제 적용은 발효일로부터 2년 후인 2026년 8월부터 적용

2 규제 경과

사이버보안 의무화 추진 경과

의무화 추진 배경

- 우리 사회 전분야의 데이터·네트워크 의존도 확대, 인공지능·클라우드 등 SW 신기술 등장, 해킹 조직의 전문화 등 대내외적인 변화로 사이버 공격의 위험성 점차 심화되고 있으며, 사이버 공격에 인공지능 기술이 접목됨과 동시에 지능형 지속 공격 등 예측이 어려운 방식으로 진화, SW 공급망·클라우드에 악성코드를 심어 공격하는 등 공격 분야 역시 확대되고 있음
- 고도로 진화하는 사이버 위협에 대응한 차세대 기술 개발 및 보안 패러다임 변화가 요구되며, 주요 기업·국가의 기술·산업 경쟁력 강화를 위한 각국의 적극적인 대응 전략 마련 중임
- 주요국은 기술 패권 경쟁 심화와 AX/DX에 따른 신·변종 보안 위협에 대응하고, 사이버보안 산업을 육성하기 위해 국가적 지원을 추진 중
- 미국·영국 등 주요국의 사이버안보 전략은 전통적인 대응 차원을 넘어 공격자 식별 및 예방적 조치 등 적극적 사이버 방어 측면을 강조
- 한국도 「국가 사이버안보 전략」 발표, '사이버보안'을 12대 필수전략 기술 중 하나로 선정하는 등 차세대 정보보호 기술·산업을 선도

규제와 표준화의 도전과제

- AI 기술이 빠르게 발전하여 기존 규제 체계를 빠르게 넘어가는 상황이므로, 엄격한 규제 준수를 위한 비용이 중소기업에게 큰 부담 요소임
- 현재 대부분의 규제는 사후 대응에 초점을 두고 있으므로 예방적 보안 조치가 부족한 상황인 것이 도전과제가 될 수 있음

AI 사이버보안 규제의 핵심 요소

① 데이터 시큐리티
- (규제 요소)
  - 데이터 보호 및 암호화(예: GDPR, General data protection regulation)
  - 데이터 중독 공격 방지 및 데이터 신뢰성 검증

② 모델 시큐리티
- (규제 요소)
  - AI 모델의 안전성과 견고성 평가
  - 모델 역공학 방지 및 지적 재산 보호

③ 적대적 공격 방어
- (규제 요소)
  - 적대적 예제, 데이터 조작, 악의적 알고리즘 공격에 대한 방어 체계 의무화
  - AI 시스템 배포 전 보안 테스트 요구

④ 윤리 및 투명성
- (규제 요소)
  - AI 시스템의 설명 가능성(Explainability) 및 투명성 의무화
  - 윤리적 이슈(편향, 차별) 사전 평가

3 규제 동향 및 현안

사이버보안 규제 동향

유럽연합

- AI 법안 (AI Act)
  * 2021년에 발표된 유럽 최초의 AI 규제 법안으로, AI 시스템의 위험도를 기반으로 분류(예: 고위험, 제한적 위험)
  * 고위험 AI 시스템(예: 의료, 금융, 생체인식)에 대해 엄격한 사이버 보안 요구사항 부과
  * 데이터 보안, 적대적 공격 방어, 데이터 정확성 검증 의무화 포함
- 네트워크 및 정보보안 지침(NIS2 Directive)
  * 필수 서비스 운영자를 포함한 AI 시스템의 보안 및 사이버 복원력을 강화
  * 주요 디지털 인프라 제공자는 적절한 보안 조치를 취해야 함

영국

- 국가 AI 이니셔티브 법안 (National AI Initiative Act, 2020)
  * AI 연구 및 개발에서 보안과 윤리적 문제를 고려하도록 규정
  * AI 모델의 보안 평가 및 적대적 공격 방어를 연구 대상으로 지정
- 연방 무역 위원회(FTC, Federal Trade Commission)의 가이드라인
  * AI 기반 시스템이 소비자 데이터를 안전하게 처리할 것을 요구
  * 허위 또는 불완전한 AI 보안 조치에 대한 책임 부과

중국

- 인터넷 정보 서비스 알고리즘 규제 (2021)
  * AI 알고리즘의 보안 검토 및 심사를 의무화
  * 알고리즘이 공공질서, 보안, 데이터 보호 규칙을 준수하도록 규제
- 사이버 보안법 (Cybersecurity Law)
  * 중요 정보 인프라에 사용되는 AI 시스템의 데이터 보호와 보안 강화를 요구
  * 국가 보안 평가 기준 도입

정책 동향

해외 정책 동향

사이버 공격의 위험성 점차 심화되고 있으며, 사이버 공격에 인공지능 기술이 접목됨과 동시에 지능형 지속 공격 등 예측이 어려운 방식으로 진화, SW 공급망·클라우드에 악성코드를 심어 공격하는 등 공격 분야 역시 확대되고 있음

- 고도로 진화하는 사이버 위협에 대응한 차세대 기술 개발 및 보안 패러다임 변화가 요구되며, 주요 기업·국가의 기술·산업 경쟁력 강화를 위한 각국의 적극적인 대응 전략 마련 중임
- 주요국은 기술 패권 경쟁 심화와 AX/DX에 따른 신·변종 보안 위협에 대응하고, 사이버보안 산업을 육성하기 위해 국가적 지원을 추진 중

– 미국·영국 등 주요국의 사이버안보 전략은 전통적인 대응 차원을 넘어 공격자 식별 및 예방적 조치 등 적극적 사이버 방어 측면을 강조

국가	내용	
1. 미국	「국가 사이버보안 전략(National Cybersecurity Strategy, NCS)」	- 국익 증진 및 경쟁력 확보, 향후 글로벌 공동 대응을 위한 방향성을 제시 * 바이든 정부 출범 이후의 사이버 위협 대응 전략들을 통합·계승하는 새로운 종합 전략으로, 연방정부의 역할 강화 및 실질적 보안 수준 강화를 목표로 함 - 국가 사이버안보 및 인공지능 이니셔티브 정책, 사이버 안보 개선 행정명령(EO-14028), 5G 보안*)을 위한 국가 전략 등 주요 내용을 반영 * ①핵심 인프라 시설 보호, ②사이버 위협 행위자 교란·해체, ③사이버보안 및 복원력 증진, ④안전한 차세대 기술개발을 위한 투자, ⑤사이버 위협 공동대응을 위한 국제 협력 - 전략별 실행계획 및 책임기관, 목표 시기를 공개, 대통령실 소속 국가 사이버 국장실(ONCD) 주도하에 오픈소스 SW 보안 솔루션 개발('23.7)
	CISA (사이버보안·인프라보안국)	- CISA는 사이버 방어, 중요 인프라 보안 및 사이버 회복력 확보 방안을 중심으로 「CISA 사이버보안 전략 계획」을 발표 - 「CISA 전략계획('23~'25)」을 발표('22.9), 전담 기관이 가지는 주요 기반 시설 보호 및 주·연방정부와의 협력 역할을 강조 - 바이든 대통령의 행정명령*) 후속 조치로 'AI를 위한 첫 번째 로드맵'을 발표, 사이버보안 관점에서 AI에 대한 5가지의 접근 방식을 제시 * 국토안보부가 전세계적으로 AI 안전 표준 채택을 촉진, 미국 네트워크와 중요 기반시설을 보호하며 AI로 인한 위험을 줄이고 숙련된 인재 유치를 지원('23.10)
	NIST (국립표준기술연구소)	- '14년 오바마 정부에서 제시한 사이버보안 프레임워크(Cyber Security Framework, CSF)를 대외환경 변화에 맞게 현행화하여 CSF2.0을 발표('24) - 오바마 행정부의 사이버 위협 대응 강화 관련 행정명령*('13.2)의 후속 조치로 NIST 주도로 민·관 협력을 통해 주요 기반시설 사이버보안 개선을 위한 프레임워크(CSF 1.0)을 발표('14) *「국가 주요 기반 시설의 사이버 위협 대응 강화」를 위한 행정명령(EO 13636) → (트럼프 행정부)「연방 네트워크와 주요 기반시설의 사이버보안 강화」를 위한 행정명령(EO 13800, '17.5)을 통해 정부 기관의 사이버보안 위험 관리에 CSF 도입을 의무화 - 사이버보안 환경변화와 국내외 활용 수요 반영을 위해 다양한 부문의 의견을 수렴하여 사이버보안 프레임워크를 최신화(CSF 2.0, '24.2)

		- 제로 트러스트의 정의, 원칙, 보안 위협 등을 기술한 '제로 트러스트 아키텍처(Zero Trust Architecture, SP800-207)' 발표('20.8) - (바이든 행정부) 행정명령(EO10428)*을 통해 연방정부의 사이버보안 현대화를 위한 제로 트러스트 전략 채택('21.5) - (사이버보안, 인프라보안청 CISA) 정부 기관 도입을 위한 '제로 트러스트 성숙도 모델 1.0' 발간 * Executive Order 10428 – Improving the Nation's Cybersecurity
	마크워너, 톰 틸리스 상원의원	- 인공지능 관련 보안·안전 사고 및 위험추적 처리 절차 개선 등에 관한 "인공지능 관련 보안 안전사고 및 위험·추적 관리와 기타 목적을 위한 법률안"5 발의 - (S4230) 안전한 인공지능 법(Secure Artificial Intelligence Act of 2024), '24.5.1
		(주요 내용) - 인공지능 취약성 DB 개선 및 보안 취약점의 특성 식별 관리 및 개발 - 인공지능 보안 안전, 사고를 추적하고 관리할 수 있도록 사고 구축에 포함할 사고 선별 및 사고 익명화 등 수행 - 공통 취약성 및 노출 프로그램 관련 절차개선 및 자발적 합의 표준 평가 - 국가안보국은 사이버안보 협력 센터 내에 인공지능 안전 센터 설치
2. 유럽연합	주변국의 군사적 분쟁에 따른 유럽 내 국방·안보적 관점의 사이버보안 경계 태세 강화 및 복원력 확보를 위한 주요 전략·정책 준비, 발표 중 1. 러시아-우크라이나 전쟁으로 사이버 위기 대응 강화 필요성 확대, 전력·에너지망, 운송 시설 등 디지털 의존성 확대에 따른 위협 대응을 위한 「EU 사이버방어정책」 발표('22.11) - ▲강력한 사이버 방어를 위한 공동 대응 체계 마련, ▲EU 국방 생태계 확보, ▲사이버 방어역량 강화 투자, ▲문제해결을 위한 파트너십 강화 등 국방·안보적 차원의 대응 전략 중심 - 사이버 방어역량 강화를 위한 생태계 조성 및 투자 확대, 사이버 커뮤니티(국방, 민간, 법, 집행, 외교 등) 간 조정·협력을 강화하기 위한 정책 추진 2. 유럽 전반의 사이버보안 수준 향상을 통해 집단적 회복력 강화 및 안전한 디지털 환경조성을 위해 「사이버복원력법」('22.9), 「사이버연대법」('23.5) 등 입법과제 추진 - 디지털 인프라 신뢰성 확보 및 기업의 경쟁력 강화를 위해 SW 및 디지털제품에 대한 개발·생산·유통 등 생애주기 또는 최소 5년 이상의 보안 업데이트를 의무화 * 제품을 기능, 사용 목적, 영향범위 등에 따라 'Class I, Class II, 기본(Default)' 3개의 범주로 분류하고 Class I과 II의 경우, 보다 엄격한 리스크관리 수행 명시 - 사이버 공격의 신속한 대응 역량 확보를 위해 ▲EU 사이버보안 쉴드 설계, ▲사이버 비상 메커니즘 구축, ▲사이버보안 리저브 설립 등을 주요 골자로 「사이버연대법」 제안('23.4)	

3. 영국	사이버보안 의무화	- PSTI법(제품 안전 및 통신 인프라 법)에 명시된 요구사항을 의무화 이행('24.4.29) - (배경) 커넥티드 제품의 증가와 함께 악성 활동의 증가로 인해 소비자용 커넥티드 제품이 주요 범위 - (요구사항) 3개 그룹(비밀번호, 지원 기간, 취약점 보고) - 요구사항은 PSTI 법에 따라 평가될 수도 있지만,「소비자 IoT의 사이버보안」이라는 ETSI EN 303 645 표준에 따라 평가가 이루어질 수 있음 → 요구사항을 준수하고 자체 신고함
	NCSC (국가 사이버보안센터)	- 제로 트러스트 아키텍처 설계·구축의 가이드라인으로 '제로 트러스트 아키텍처 설계 원칙 1.0' 발표('21.7)
4. 중국	(정책 방향) 세계강국의 기술 패권 경쟁 속에서 미국의 압박에 따른 자국 중심의 정책을 추진 1. 미국의 첨단기술 기업에 대한 규제가 전방위적으로 확대되면서 ▲데이터 국지화, ▲소스코드 공개, ▲기술 이전 강요 등 사이버보안 이슈 부각 - (미국) 기술 안보를 내세워 중국 첨단기업의 수출입 규제, 특히 디지털 무역 활성화에 장애 요소인 데이터 국지화를 반대 -「데이터보안법」('21.09)과「개인정보보호법」('21.11) 등 법·제도적 근거를 바탕으로 중국에서 수집한 데이터 및 개인정보의 역외 이전을 제한, 외교적 수단으로 활용 ※ (데이터보안법) 유형별 데이터 제도를 통해 사이버 안전과 디지털 산업의 발전 기반을 마련 (개인정보보호법) 법률의 개별 규정에서 보호하던 개인정보의 정의와 규정을 구체화 2. (국가인터넷정보판공실)「사이버보안법」을 5년만에 개정하며 네트워크 운영 보안의 일반규정을 위반하는 행위에 대한 법적 책임을 명시('22.9) - 기존 네트워크 운영 보안에 관한 법적 제도 시행 상황을 고려하여, 네트워크 운영 보안 의무를 저버리거나 사이버 위협을 가하는 행위의 처벌 강도를 조정 * 핵심 정보 인프라 운영자의 위법 행위에 대한 처벌 규정을 개선 및 네트워크 정보 보안 의무를 위반하는 행위에 대한 법적 책임을 통합 - 개인정보보호법에서 규정한 법적 책임 제도를 수정하여, 기존의 개인정보보호관련 법적 책임 제도가 기타 법률 적용을 받도록 할 방침	
5. 일본	(정책 동향) 정부가 제정한 상위 법령에 따른 국가적 차원의 거버넌스 구축하고,「사이버시큐리티전략」을 비롯한 주요 정책을 지속해서 현행화 진행 1. '21년부터 디지털사회 실현을 위해「디지털사회 형성 기본법」수립, 디지털청 설치 등 추진 중으로 중점 분야로 '사이버보안' 중요성 강조 -「사이버시큐리티기본법」제정 후, 내각 총리를 최고책임자로 하는 '사이버시큐리티전략본부'를 설치·운영 및 안전한 사이버공간 구현을 위해 '디지털청'과 협력 중 -「사이버시큐리티기본법」제정 전후로, 대내외 사이버 환경변화에 대응하기 위해 핵심 정책인「사이버시큐리티전략」을 3년 단위로 개정 2. (사이버시큐리티전략본부 산하, 사이버보안센터)「사이버시큐리티전략」에 따른「사이버보안 2024」발간('24.07) -「사이버보안기본법」에 명시된 정책 목적*과 '21년「사이버보안전략」의 추진 방향에 따른 '23년도의 실적과 '24년도의 중점 추진 계획**을 제시 * ①경제사회의 활력 향상 및 지속적 발전, ②국민이 안심하고 안전하게 생활할 수 있는 사회 실현, ③국제사회의 평화 및 안전의 확보와 일본의 안보에 기여 ** 사이버 공격을 미연에 방지하는 능동적 방어 시스템 구현 법안의 수립 방침을 처음 명	

	시하고, 각 주체의 자체적인 대응책, 주요 인프라 사업자, 기업 등의 대응 능력 강화 방안을 제시 - 국가의 전반적인 사이버보안 대응 능력을 유럽과 미국 등 주요 강국 수준으로 확보하기 위해 종합적인 국가 전략 수립 3. (디지털청) 제로 트러스트 아키텍처 개념, 적용 방침, 적용 순서, 정책 등을 정의한 '제로 트러스트 아키텍처 적용 정책' 발표('22.6)
6. 홍콩	1. AI 데이터보호 지침 발표 - 생성형 인공지능을 활용하는 기업을 대상으로 최초의 개인 데이터 보호 지침을 발표 - 위험성 평가 수행, 적절한 수준의 인적 감독, 모델 학습을 위해 수집되는 개인 데이터 최소화를 강조, 내부 AI 거버넌스 위원회를 설립하며 최고 경영진이 이끄는 것을 권고함 - 생성형 AI 솔루션을 사용하는 기업은 위험 평가 수행, 적절한 인적 감독 수준 결정, 모델 훈련을 위해 수집되는 개인 데이터의 양 최소화 등 개인 데이터를 보호하기 위해 다양한 조치를 취해야 함
7. 말레이시아	1. AI 기술의 확산 및 발전과 함께 수반되는 문제에 대응하고자 AI 관련 입법을 진행 및 추진 - (2024 사이버보안법) 법안이 상원 만장일치로 통과('24.4.3) - (목적) 사이버보안 관리를 위한 조치, 표준 및 절차를 정하여 국가 사이버보안 환경 개선 목적
8. 인도네시아	1. AI 관련 규제가 기술 혁신을 거부하는 형태가 아닌, 기술로 인하여 발생할 수 있는 부정적 영향을 최소화하고 AI의 이점을 극대화할 수 있도록 하는 것을 목표로 다양한 규제 방안을 마련 중 - AI 기술 개발 장려를 위하여 "국가AI전략 2020-2045"를 마련하여 다양한 부문에서의 AI 기술 개발 전략을 제시함 - 2024년 중반까지 유네스코의 RAM AI(AI 준비도 평가 방법론) 평가를 받으며, 안전하고 책임 있는 AI 거버넌스를 구축 예정

국내 정책 동향

전략 기술화를 통한 기술 역량 강화와 차세대 신산업으로써 국내 생태계 조성 및 글로벌 경쟁력 제고를 위한 지원 정책 발표

구분	내용
2. 주요 전략	- 한국 및 해외 주요국은 고도화 중인 사이버 공격에 대한 억지력 제고를 위한 능동적 방어 전략으로 억제 중심의 기술 확보와 사후 복원력 확보에 집중하는 패러다임 전환 - 사전에 사이버 공격 식별 및 공격 경로 예측하여 활동 초기에 차단하고, 사고 발생 시 빠른 회복(복구·적응)을 위한 메커니즘을 확보할 수 있는 기술 개발에 집중 - 사이버 공격에 선제적으로 대응할 수 있는 데이터(개인정보)·인공지능·클라우드 등 신기술과 SW 공급망 및 취약점 분석을 통한 보안 기술력 확보 중요성 강조 - 민간·공공의 보안 강화 목적을 위한 5대 핵심 전략 설정 ①사이버 공격 대응, ②사이버 복원력 확보, ③개인정보보호, ④제로 트러스트 구현, ⑤인공지능 보안

<table>
<tr><td>2. 중점 분야</td><td colspan="2">- 전통적으로 형성된 사이버보안·정보보호 산업 생태계 분야와 글로벌 경쟁력 확보를 위한 차세대 보안기술에 국가적 차원의 투자 확대
- 사이버보안 산업은 정보보호를 위한 기술 및 정보보호 기술이 적용된 제품을 개발·생산·유통 및 관련 서비스를 제공하는 산업으로 정의하며 3개 영역으로 구분
* 정보보호 산업 범위: ①정보 보안(클린인터넷경제) ②물리보안(안전안심생활) ③융합보안(안전성강화)
-「국가전략기술 임무중심 전략로드맵-사이버보안」 ▲핵심 보안기술 자립화 ▲국민생활 안전망 ▲제로트러스트 대응 등을 위해 확보가 필요한 4대 중점기술 제시('24)
* 사이버보안 4대 중점기술: ①데이터·AI 보안, ②디지털 취약점 분석 및 대응, ③네트워크·클라우드 보안, ④산업·가상 융합보안
- 전통적인 사이버보안(정보보호) 산업 구분과「국가전략기술 전략로드맵」에서 제시한 중점기술을 합하여 5대 중점 분야(13개 세부기술)로 분류 추진</td></tr>
<tr><td rowspan="3">3. 정책 동향</td><td>윤석열 정부</td><td>-「120대 국정과제」를 통해 사이버안보 대응 역량 강화의 국정 방향을 제시
-「대한민국 디지털 전략」에서 디지털 사회 구현의 핵심으로 정보보호의 중요성 강조
- 국정과제에서 국가 안보 태세 유지와 산업·기술·인재 경쟁력 향상을 위해 사이버보안 분야에 범정부 차원의 협력체계 공고화 방안 제시
* (사이버보안 역량 강화) 보안클러스터 모델의 지역거점 확산으로 기업 성장 지원, 10만 사이버보안 인재 양성(~'26년)
-「대한민국 디지털 전략」 기술 패권에 대응하기 위한 6대 디지털 혁신기술* 중 하나로 사이버보안을 설정, 최적화된 R&D 협력 방식 및 인력 양성 구축 방안 제시
* 사이버전, 미래 기술(6G, 양자 등)에 대비한 지능형 보안 핵심기술 및 데이터 보안 원천기술 확보 및 4대 방어 기술 개발 목표(미국 대비: 88.6%('20) → 93%('27) 역량 달성)</td></tr>
<tr><td>「정보보호산업의 글로벌 경쟁력 확보 전략」</td><td>- 제로 트러스트, 공급망 보안 등 新보안체계 적용·확산, 미래형 융합보안 시장 개척 및 AI 보안·사이버보안·정보보호 분야의 차세대 기술·산업 경쟁력 제고
-「K-시큐리티 얼라이언스」 민·관 협력을 통한 통합보안 모델 개발
-「K-시큐리티 클러스터 벨트」 국내 정보보안 산업의 시설 및 투자 확충, 인재 양성 활성화
-「K-시큐리티 랩」 신흥시장 진출 가속화를 위한 현지 플랫폼 구축</td></tr>
<tr><td>「2024 국가 사이버안보 전략」</td><td>- '생성형 AI와 같은 ICT 신기술에 대응하고, 북한의 사이버 공격을 악의적 행위 및 위협으로 명시하여 안보 관련 대응을 강화하는 새로운 전략
- (3대목표) ▲공세적 사이버 방어 및 대응 ▲글로벌 리더십 확장 ▲건실한 사이버 복원력을 설정, 이를 실현할 5대 전략과제* 제시
* 5대 전략과제: ①공세적 사이버 방어 활동 강화, ②글로벌 공조체계 구축, ③국가핵심 인프라 사이버 복원력 강화, ④신기술 경쟁 우위 확보, ⑤업무 수행 기반 강화</td></tr>
<tr><td></td><td>대통령 직속 디지털 플랫폼 정부위원회</td><td>- 국가적 차원의 '제로 트러스트 도입 추진 계획'('23.4) 및 과기정통부의「제로 트러스트 가이드라인 1.0」 발표('23.7), 국내 도입을 위한 기반 구축</td></tr>
</table>

4 시사점 및 대응 방안

시사점

보안 전략 재정비

신기술과 새로운 보안 정책의 도입(인공지능, 제로 트러스트)에 따른 사이버보안 환경의 복잡성 심화로 기업 보안 전략 재정비 필요

- 생성형 AI 같은 기술이 공격자들에게 유리한 도구로 작용하고 피싱, 맞춤형 악성코드 개발, 가짜 정보 유포 등 공격 기법 정교화 예측 필요
- 기업들의 사이버보안 전략 재정비 및 새로운 기술 대응 방안이 요구되며, 생성형 인공지능의 잠재적 위협완화를 위한 기술적, 조직적 대응책 마련 시급
- 사이버보안 분야에서 인력 부족 문제는 지속해서 악화되고, 중소기업들이 사이버보안 위협에 더욱 취약해질 수밖에 없는 실정으로, 영세 기업의 취약성 심화 및 해결방안 필요

거버넌스 수립 및 국제 공조 체계 확립

사이버공간의 환경변화에 능동적 대응 및 중장기적인 기술개발과 안전한 디지털 사회 구현을 위한 거버넌스 수립과 국제 공조 체계 확립 필요

- 미국, EU, 일본 등 주요 선도국은 10여년 전부터 사이버보안 관련 주요 법령 수립, 국가 차원의 거버넌스를 구축하여 체계적인 국가 전략을 수립하고 기술·산업 주도
- 정부는 「국가 사이버안보 전략」 개정('24) 및 사이버보안 정책을 강화하고 있으나, 국가 차원의 거버넌스와 중장기적인 실행계획의 연속성 확보 필요

R&D 포트폴리오의 다변화

사이버 공격을 적극적·선제적으로 방어하는 방식으로 진화하거나, 전 세계적으로 보안 패러다임 전환기를 고려하여 중장기적 관점에서 R&D 포트폴리오의 다변화 필요

- 개인정보보호·데이터 보안 분야에 집중(총투자액의 22.8%)되어 있어, 보안 기술·산업 변화를 고려한 투자 분야의 다변화가 필요
- 제로 트러스트, 사이버 복원력, 공급망 보안 등 정책적 분야의 개념 확립, 기반 연구를 통해 기술적 정의와 목표를 명확히 설정하여 중장기적인 지원이 필요
- DX/AX에 따른 기술·산업의 융·복합을 고려하여 산업제어시스템(총투자액의 18.2%차지) 분야 외 다양한 산업 도메인을 고려한 융합보안 분야의 투자 강화가 요구됨

대응 방안

잠재적 리스크 대비

법률/규제 전문가의 지식 및 경험을 충분히 활용, 잠재적 리스크를 파악하고 이에 대한 대비책을 세움으로써 AI 관련 사이버보안 규제 위험을 효과적으로 완화 진행

- 기업은 사용 중인 AI 시스템을 모니터링하고, 수집된 정보의 투명성을 확인하며, AI 시스템이 편향적으로 작동하거나 금지되는 행위를 하지 않는지 지속적으로 모니터링

AI 거버넌스 구축

위험을 체계적으로 관리할 수 있는 AI 거버넌스 및 데이터 관리체계 구축

- 사이버보안을 국가적 안보 개념으로 격상, 단순 대응에서 위협 행위자의 식별 및 사전예방적 보안인 적극적 사이버 방어 개념으로 전환 및 국제 협력 강화 필요
- 사이버 공격 및 침해사고에 따른 회복탄력성이 요구됨에 따라 사이버 위협에 신속한 대응 및 복원할 수 있는 기술 구축 진행
- 진화하는 사이버 공격 유형을 분석(랜섬웨어 공격, 피싱, 공급망 복합 공격, 제로데이 공격, OS 및 ICS, IoT 환경에서의 사이버 공격 등) 적절한 대응을 위해 사이버 위협을 신속하게 탐지하고 대응

보안 및 안전

보안 시스템에 내장형 인텔리전스를 갖추어, 악의적인 입력으로 인해 쉽게 어긋나지 않고 올바르고 확고한 판단을 내리는 데 적응하도록 설계

- (정부) 법적 및 규제체계의 강화, 주요 인프라 보호, 국제 협력을 통한 사이버 복원력 구축 지원
- (기업) 데이터 백업 및 복구 계획수립, 보안 인프라 개선, 지속적인 모니터링과 직원 교육 등 진행

5 모니터링 출처

기관	내용
유럽전기통신표준협회 (ETSI)	사이버보안 https://www.etsi.org/technologies/cyber-security
	소비자 IoT 보안 https://www.etsi.org/technologies/consumer-iot-security
	인공지능(SAI) 보안 https://www.etsi.org/technologies/securing-artificial-intelligence
유럽표준위원회 (CEN-CENELEC)	CEN-CENELEC JTC 21 '인공 지능' https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/artificial-intelligence/
영국 AI안전 연구원	고급 AI 거버넌스를 가능하게 하는 엄격한 AI 연구 https://www.aisi.gov.uk/
미국의회	인공지능 보안법 발의 https://www.congress.gov/bill/118th-congress/senate-bill/4230?q=%7B%22search%22%3A%22
세계법제정보센터	유럽연합_AI법_영문본(2024.03.13.가결)
KDI 경제교육・정보센터	세계 최초로 통과된 EU「AI법」, 우리 기업의 대응 방향은?, 2024-06
SCMP	홍콩, 최초의 AI 데이터 보호 지침 발표, 더 많은 규정 준수 확인 약속, 2024-06-11
전자신문인터넷 (ETNEWS)	산업부 주도 'AI활용 진흥법' 만든다...6대 분야별 전략 마련, 2024-05-09
한국과학기술 기획평가원	기술동향브리프(2024-150호, 2024 사이버보안: 주요 전략 및 중점 분야)
대통령실 국가안보실	국가 사이버안보전략(2024년 2월, 대통령실 국가안보실)

주 의

○ 본 보고서는 산업통상자원부 국가기술표준원의 무역기술장벽(Technical Barriers to Trade, TBT) 대응 활동의 일환으로 최신 규제 정보를 제공하기 위해 작성되었습니다.

○ 본 보고서는 TBT종합지원센터의 동의 없이 무단 배포 및 변경할 수 없으며, 상업·법률적 판단 근거로 활용될 수 없습니다.

○ TBT종합지원센터에서 운영 중인 KnowTBT 포털을 통해 더 많은 해외 기술규제 정보를 제공 받을 수 있습니다(www.knowtbt.kr).

Tel. : 02-3487-7758 **Fax** : 02-571-0003 **E-mail** : tbt@kotica.or.kr