2025년 1분기

인터넷·정보보호 법제동향

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

2025년 1분기
인터넷·정보보호 법제동향

CONTENTS

목차

PART I

「인공지능기본법」 제정과 해외 입법동향

1. 「인공지능기본법」 제정

○ 「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법(이하 '인공지능기본법')」 제정('25.1.21)하고, 하위법령 정비 작업을 추진 중

- 국내 '인공지능기본법'은 인공지능 추진체계 수립, 산업 진흥 기반 조성, 고영향/생성형 인공지능사업자 의무 등을 주요내용으로 하며, 이는 EU AI법에 이어 세계 두 번째로 제정된 인공지능기본법에 해당

※ 제22대 국회 제출된 19개 법안 통합·조정하여 과학기술정보방송통신위원회의 병합·심사 대안 마련 후, 본회의 통과('24.12.26)

- 과학기술정보통신부는 인공지능기본법의 원활한 시행 ('26.1.22 예정)을 위해, 시행령·시행규칙 및 고영향 인공지능 기준과 예시, 사업자 책무 방침, 인공지능 투명성 확보 의무 방침 등 규제 범위의 불확실성 해소를 위한 고시·가이드라인 마련 등 하위법령 정비계획을 발표(1.16)

〈 인공지능기본법 하위법령 정비 주요사항 〉

- 인공지능 기본법 시행령 및 시행규칙
- 고영향 인공지능 기준과 예시에 관한 방침(가이드라인) (제33조)
- 고영향 인공지능 사업자 책무 방침(가이드라인) (제34조)
- 인공지능 안전성 확보 의무 고시 (제32조)
- 인공지능 영향평가 방침(가이드라인) (제35조)
- 인공지능 투명성 확보 의무 방침(가이드라인) (제31조)

* 과학기술정보통신부 보도자료('25.1.16.) 참고

※ 국가인공지능위원회를 중심으로 산·학·연 전문가, 관계부처, 유관기관 등이 참여하는 5개 전담반 운영을 통해 분야별로 초안 마련 및 이해관계자 의견수렴 등 추진

- 한편, 방송통신위원회는 'AI 이용자 보호 종합계획' 수립 및 AI의 잠재적 위험성과 부작용으로부터 이용자 보호를 위한 'AI 이용자보호법*' 제정 추진계획을 발표(1.14)하는 등 AI 이용자 보호를 위한 대응책 추진 중

* AI 유형별 차등 규제, AI 생성물 표시제, 이용자 설명 요구권 보장, 분쟁조정 제도, AI 이용자 보호 업무 평가 등 제도 도입 검토 중

– 또한, 텍스트, 오디오, 이미지 등 생성형 인공지능 서비스 이용 과정에서 피해 방지를 위한 '생성형 인공지능 서비스 이용자 보호 가이드라인' 을 발표(2.28), 시행(3.28)하였고, 본 가이드라인은 시행일 기준, 2년마다 가이드라인에 대한 타당성 검토 후 개선조치 추진 예정

※ 생성형 인공지능, 생성형 인공지능 서비스, 개발사 및 서비스 제공자, 이용자, 생성형 인공지능 산출물 등 용어 규정, 4가지 기본원칙과 6가지 실행 방식, 실행 사례 등 제시

• 그 외에도 산업통상자원부(산업 AI 확산을 위한 10대 과제), 문화체육관광부(AI 저작권 제도개선 협의체 추진), 중소벤처기업부(인공지능 창업기업 육성을 통한 인공지능 활용·확산 방안) 등 다부처에서 AI 관련 정책을 추진

- 이에, 범정부 AI 정책을 주도하는 대통령 소속 '국가인공지능위원회'는 각 부처별 AI 관련 정책 추진 시 국가인공지능위원회와의 사전 협의를 통해 정책 조율이 필요하다는 원칙을 밝힘[1)]

「인공지능기본법」 주요내용

• **(추진체계 수립)** 과학기술정보통신부장관은 3년마다 인공지능 정책의 기본 방향 등을 설정하는 '인공지능 기본계획'을 수립·시행해야 하며, 이 경우 대통령 소속의 '국가인공지능위원회'의 심의·의결을 거쳐야 함

- 한편, 과학기술정보통신부장관은 인공지능 관련 정책의 종합적 업무 수행을 위하여 '인공지능정책센터'를 지정할 수 있으며, 인공지능 위험 관리를 위한 '인공지능안전연구소' 운영할 수 있음

구분	주요내용
인공지능 기본계획 수립 (제6조)	• 과기정통부장관은 인공지능기술 및 산업 진흥, 국가경쟁력 강화를 위하여 ▲인공지능, 인공지능기술, 인공지능산업 및 인공지능사회 정책의 기본 방향·전략 사항, ▲인공지능의 공정성·투명성·책임성·안전성 확보 등 신뢰 기반 조성 등을 포함한 '인공지능 기본계획(3년)'을 수립·시행하여야 함
국가인공지능위원회 설치 (제7조)	• 인공지능 관련 주요 정책 등을 심의 · 의결하기 위하여 5년간 한시적 기한을 정한 대통령 소속의 국가인공지능위원회 설치 – (심의·의결 사항) ▲인공지능 등 관련 정책·연구개발·투자 전략 수립, ▲인공지능 데이터센터 등 인프라 확충 방안, ▲제조업 · 서비스업 등 산업 및 공공부문에서의 인공지능 활용 촉진에 관한 사항, ▲인공지능 관련 국제협력 사항, 고영향 인공지능 규율 및 정책적 대응에 관한 사항 등
인공지능정책센터 지정 (제11조)	• 과기정통부장관은 인공지능 관련 정책의 개발과 국제규범 정립 · 확산에 필요한 업무를 종합적으로 수행하기 위하여 '인공지능정책센터' 지정
인공지능안전연구소 운영 (제12조)	• 인공지능 관련 위험으로부터 국민의 생명 · 신체 · 재산 등 보호 및 인공지능사회 신뢰 기반 유지를 위한 '인공지능안전연구소' 운영 가능

• **(인공지능기술 개발 및 산업 육성)** 인공지능기술 개발 등 지원 시책을 시행할 경우 중소기업 등을 우선 고려해야 하며, 인공지능 개발·활용 등에 사용되는 학습용데이터 및 인공지능데이터센터 활용 등에 관한 시책 수립 및 인공지능집적단지 지정 등을 통해 인공지능산업 진흥을 위한 지원 근거 마련

구분	주요내용
인공지능기술 개발 및 안전한 이용 지원 (제13조)	• 정부는 인공지능기술 개발 활성화를 위하여 ▲인공지능기술의 연구 · 개발, 시험 및 평가 또는 개발된 기술의 활용, ▲인공지능기술 확산, 협력 · 이전 등 기술의 실용화 및 사업화 등 사업 지원 가능 – 한편, 정부는 지능정보화기본법에 따른 ▲안전성 보호조치를 AI로 구현, ▲비상정지 기능을 인공지능제품·서비스에서 구현하기 위한 기술 연구 지원, ▲사생활 등 보호에 적합한 설계 기준 및 기술▲사회적 영향평가 실시 및 적용을 위한 연구개발 및 보급 사업 등을 지원할 수 있으며, 해당 결과를 누구든지 손쉽게 이용할 수 있도록 공개·보급해야 함 ※ 다만, 정부는 기술 개발자 보호를 위하여 필요 시 보호기간을 정하여 기술사용료를 받을 수 있도록 하는 등 보호할 수 있음

1) "국가AI위원회에 힘실린다…대통령 권한대행, 범정부 사전협의 강조" (전자신문, 2025.3.11.보도) https://www.etnews.com/20250311000267

구분	주요내용
학습용데이터 시책 수립 (제15조)	• 과기정통부장관은 인공지능의 개발 · 활용 등에 사용되는 학습용데이터의 생산 · 수집 · 관리 · 유통 및 활용 등 촉진을 위한 시책 추진 및 학습용데이터 구축사업 시행 가능 – 과기정통부장관은 학습용데이터를 통합적으로 제공 · 관리할 수 있는 '통합제공시스템'을 구축 · 관리하고 민간이 자유롭게 이용할 수 있도록 제공해야 함
인공지능집적단지 지정 등 (제23조)	• 인공지능 및 인공지능기술의 연구 · 개발 수행 기업, 기관이나 단체의 기능적 · 물리적 · 지역적 집적화 추진 가능
인공지능 데이터센터 관련 시책 추진 (제25조)	• 정부는 인공지능 데이터센터 구축·운영 활성화를 위한 시책을 추진해야 하며, ▲인공지능 데이터센터 구축 및 운영에 필요한 행정적·재정적 지원, ▲중소기업, 연구기관 등 인공지능 데이터센터 이용 지원 등의 업무를 수행할 수 있음

• **(인공지능 윤리원칙 및 신뢰성 확보 기준)** 정부는 인공지능 윤리원칙을 제정·공표할 수 있으며, 인공지능이 국민생활에 미치는 잠재적 위험을 취소화하기 위한 시책을 마련해야 함

– (인공지능 윤리원칙) ▲인공지능의 개발 · 활용 등 과정에서 사람의 생명, 신체, 정신적 건강 등에 해가 되지 않도록 하는 안전성과 신뢰성, ▲인공지능기술이 적용된 제품 · 서비스 등을 모든 사람이 자유롭고 편리하게 이용할 수 있는 접근성, ▲사람의 삶과 번영에 공헌을 위한 인공지능의 개발 · 활용 사항 등을 포함 (제27조)

※ 인공지능기술 연구 및 개발을 수행하는 사람이 소속된 교육기관 · 연구기관, 인공지능사업자 등은 윤리원칙을 준수하기 위하여 '민간자율위원회' 설치 가능(제28조)

– (인공지능 신뢰 기반 조성을 위한 시책 마련) ▲안전기술 및 인증기술의 개발 및 확산 지원, ▲인공지능사업자의 안전성 · 신뢰성 관련 자율적인 규약의 제정 · 시행 지원 등의 시책을 마련해야 함 (제29조)

• **(인공지능의 안전성·신뢰성 확보 지원 근거)** 정부는 인공지능기술의 표준화, 인공지능 안전성·신뢰성 검·인증 등 지원을 위한 실증기반 등의 구축·운영 및 자율적으로 추진하는 검·인증 등 활동 지원 가능

구분	주요내용
기술 표준화 (제14조)	• 정부는 인공지능기술, 학습용 데이터, 인공지능의 안전성 · 신뢰성 등과 관련된 표준화를 위하여 사업 추진 및 민간 부문에서 추진하는 인공지능기술 관련 표준화 사업에 필요한 지원 가능
인공지능 실증기반 조성 등 (제24조)	• 국가 및 지방자체단체는 인공지능사업자가 개발하거나 이전받은 기술의 실증, 성능시험, 인공지능 안전성 · 신뢰성 검 · 인증 등을 지원하기 위하여 시험, 평가 등에 필요한 시설 · 장비 · 설비 등('실증기반등')을 구축 · 운영할 수 있으며, 보유하고 있는 실증기반 등을 인공지능사업자에게 개방 가능
인공지능 안전성 · 신뢰성 검 · 인증 등 지원 (제30조)	• 과기정통부장관은 단체등이 인공지능의 안전성 · 신뢰성 확보를 위하여 자율적으로 추진하는 검증 · 인증 활동 지원을 위하여 ▲인공지능 개발 관련 가이드라인, ▲검·인증등 연구 및 시스템 등 구축·운영 지원 등 사업 추진 가능

• **(고영향 인공지능사업자 단독 의무)** 고영향 인공지능[2]은 사람의 생명, 신체의 안전 및 기본권에 중대한 영향을 미치는 등 그 중요도가 높기 때문에, 고영향 인공지능사업자는 다른 인공지능사업자에 비해 다양한 의무사항이 존재

※ EU AI법은 AI 시스템의 위험성을 기준으로 사업자의 책임 및 의무사항을 구분하는 '위험기반접근법'을 적용하므로 '고위험(high risk)' 용어를 사용 중이나, 가치중립적 단어 사용이 적절하다는 의견을 반영[3]하여 과학기술정보방송통신위원회 대안에서는 고영향(high impact) 단어로 변경·사용

구분	주요내용
사전 안전성·신뢰성 검·인증등 노력	• 고영향 인공지능 제공 시, 사전에 안전성·신뢰성 검 · 인증등을 받도록 노력하여야 함 (제30조제3항) – (국가기관등) 고영향 인공지능 이용 시 검 · 인증등을 받은 인공지능에 기반한 제품 또는 서비스를 우선적으로 고려해야 함 (제30조제4항)
사전 검토	• 인공지능 또는 AI를 이용한 제품 · 서비스 제공 시 고영향 인공지능 해당 여부 확인을 위한 사전 검토를 해야함 (제33조) – 필요 시, 과기정통부장관에게 고영향 인공지능 해당여부 확인을 요청할 수 있음(과기정통부는 전문위원회를 설치하여 관련 자문을 받을 수 있음) ※ 과기정통부장관은 고영향 인공지능의 기준과 예시 등에 관한 가이드라인 수립 및 보급 가능
안전성·신뢰성 확보 조치	• 고영향 인공지능 또는 이를 이용한 제품·서비스 제공 시, ▲위험관리방안 및 이용자 보호방안의 수립·운영, ▲기술적으로 가능한 범위 내 인공지능이 도출한 최종결과와 최종결과 도출 시 활용된 주요 기준, ▲인공지능의 개발 · 활용에 사용된 학습용데이터의 개요 등 설명 방안의 수립 · 시행, ▲안전성 · 신뢰성 확보 조치 내용을 확인할 수 있는 문서의 작성과 보관 등을 포함하는 조치 이행의무 (제34조) ※ 과기정통부장관은 해당 조치의 구체적인 사항을 정하여 고시하고, 인공지능사업자에게 권고할 수 있으며, 인공지능사업자가 타법에 따라 위에 준하는 조치를 이행한 경우에는 이행한 것으로 간주
기본권 영향평가	• 고영향 인공지능을 이용한 제품 또는 서비스를 제공하는 경우 사전에 사람의 기본권에 미치는 영향 평가를 위한 노력을 해야 함 – (국가기관등) 고영향 인공지능을 이용한 제품 또는 서비스 이용 시 영향평가를 실시한 제품 또는 서비스를 우선적으로 고려하여야 함 (제35조)

• **(투명성 확보 의무)** 고영향·생성형 인공지능사업자 또는 실제와 흡사한 가상 창작물의 결과물을 제공하는 인공지능사업자는 해당 제품·서비스 또는 결과물이 인공지능에 의해 생성되었다는 사실을 이용자에게 고지 또는 표시해야 함

– **(고영향·생성형 인공지능사업자)** 해당 인공지능 또는 이에 기반한 제품·서비스 제공 시 이용자에게 그 사실을 사전에 고지해야 하며, 해당 사실을 표시하는 등 투명성 확보의무가 있음

구분	주요내용
고영향 인공지능	• 고영향·생성형 인공지능을 이용한 제품·서비스 제공 시 해당 인공지능에 기반하여 운용된다는 사실을 이용자에게 사전에 고지해야 함 (제31조제1항)
생성형 인공지능[4]	• 생성형 인공지능 또는 이를 이용한 제품·서비스 제공 시, 해당 결과물이 생성형 인공지능에 의해 생성되었다는 사실을 표시해야 함 (제31조제2항)

2) '고영향 인공지능'은 사람의 생명, 신체의 안전 및 기본권에 중대한 영향을 미치거나 위험을 초래할 우려가 있는 인공지능시스템으로서, ▲에너지 공급, ▲먹는물의 생산 공정, ▲보건의료의 제공 및 이용체계의 구축 · 운영, ▲디지털의료기기의 개발 및 이용, ▲원자력시설의 안전한 관리 및 운영, 범죄 수사나 체포 업무를 위한 생체인식정보의 분석 · 활용, ▲채용, 대출 심사 등 개인의 권리 · 의무 관계에 중대한 영향을 미치는 판단 또는 평가, ▲교통수단, 교통시설, 교통체계의 주요한 작동 및 운영, ▲공공서비스 제공에 필요한 자격 확인 및 결정 또는 비용징수 등 국민에게 영향을 미치는 국가, 지방자치단체, 공공기관, ▲유아교육 · 초등교육 및 중등교육에서의 학생 평, ▲그 밖에 사람의 생명 · 신체의 안전 및 기본권 보호에 중대한 영향을 미치는 영역으로서 대통령령으로 정하는 영역 등 11개 영역 중 어느 하나의 영역에서 활용되는 것을 말함(제2조제4호)

3) 제22대 국회 제418회(정기회) 제3차 과학기술정보방송통신위원회(정보통신방송법안심사소위원회) 회의록 참고(2024.11.21.)

4) '생성형 인공지능'이란, 입력한 데이터(「데이터 산업진흥 및 이용촉진에 관한 기본법」 제2조제1호에 따른 데이터)의 구조와 특성을 모방하여 글, 소리, 그림,

- **(실제와 흡사한 가상 결과물을 제공하는 인공지능사업자)** 인공지능사업자는 인공지능시스템을 이용하여 실제와 흡사한 가상의 음향, 이미지 또는 영상 등의 결과물을 제공하는 경우, 해당 결과물이 인공지능시스템에 의하여 생성되었다는 사실을 이용자에게 고지 또는 표시하여야 함 (제31조제3항)

※ 단, 해당 결과물이 예술적 · 창의적 표현물이거나 그 일부를 구성하는 경우, 전시 또는 향유 등을 저해하지 않는 방식으로 고지 또는 표시할 수 있음

• **(학습 사용 누적 연산량 기준에 따른 인공지능시스템의 안전성 확보 의무)** 인공지능사업자는 학습에 사용된 누적 연산량이 일정기준 이상인 인공지능시스템의 안전성 확보를 위하여 ▲인공지능 수명주기 전반에 걸친 위험의 식별 · 평가 및 완화, ▲인공지능 관련 안전사고를 모니터링하고 대응하는 위험관리체계 구축 조치를 이행해야 함 (제32조제1항)

- 인공지능사업자는 안전성 확보 조치의 이행 결과를 과기정통부장관에게 제출해야 함 (제32조제2항)

• **(인공지능사업자 관리·감독)** 이용자 수, 매출액 등 일정 기준에 해당하는 인공지능사업자는 국내대리인을 지정·신고(제36조)해야 하며, 과기정통부장관은 고영향·생성형 인공지능 등 해당 사업자에 대해 관련 자료 제출 또는 소속공무원에게 필요한 출입조사(제40조)를 하도록 할 수 있음

- **(국내대리인 역할)** ▲인공지능 수명주기 전반의 위험 식별·평가 및 완화, ▲위험관리체계 구축사항(제32조제2항) 등 이행 결과 제출, ▲고영향 인공지능 해당 여부 확인(제33조제1항) 요청, ▲안전성 · 신뢰성 확보 조치(제34조제1항) 이행에 필요한 지원 사항 수행

- **(사실조사)** 과기정통부장관은 아래 표에 명시된 요건에 대한 위반 사항을 발견하거나 혐의가 있음을 알게 된 경우 또는 위반신고를 받거나 민원이 접수된 경우 인공지능사업자에 대해 관련 자료 제출 또는 소속 공무원의 출입조사 등을 할 수 있음

〈 사실조사 요건 〉

- 생성형 인공지능 또는 이를 이용한 제품·서비스 제공, 실제와 흡사한 가상의 창작물을 제공하는 경우 해당 사실을 고지·표시해야 하는 투명성 확보 의무 (제31조제2항 · 제3항)
- 일정기준 이상의 누적 연산량을 사용한 인공지능 안전성 확보 의무 (제32조제1항 · 제2항)
- 고영향 인공지능의 안전성·신뢰성 확보 조치 (제34조제1항)

※ 과기정통부장관은 조사 결과 위반 사실이 인정되는 경우, 인공지능사업자에게 해당 위반행위의 중지 또는 시정조치 명령 가능

• **(과태료 부과)** 고영향 인공지능, 생성형 인공지능 운용 사실에 대한 사전 고지의무(제31조제1항) 위반, 국내대리인 미지정한 자(제36조제1항), 중지 또는 시정명령 미이행 자(제40조제3항)에 3천만원 이하 과태료 부과

영상, 그 밖의 다양한 결과물을 생성하는 인공지능시스템 (제2조제5호)

2. 해외 주요국 최근 입법동향

1) EU

’24년 8월1일 발효된 AI법이 시행*됨에 따라, EU 집행위원회는 AI법 후속 가이드라인 2건 발표

• AI법은 AI의 특성 및 규범 성격에 따라 순차적으로 시행 중인 바, 우선 시행되는 ‘금지된 AI’규정과 관련하여 이를 구체화하는 ‘금지된 AI 사례에 대한 가이드라인(2.4)’ 및 ‘AI 시스템 정의에 대한 가이드라인(2.6)’을 발표하였고, 해당 가이드라인 모두 법적 구속력은 없음

〈AI법 시행일〉

’25.2.2 시행	’25.8.2 시행	’26.8.2 전면 시행
금지된 AI 규제 ▶	범용AI모델, 인증기관, 거버넌스, 벌칙 등 ▶	※ 단, 예외적으로 ‘고위험 AI 시스템에 대한 분류 규칙(제6(1)조)’의 경우 (’27.8.2 시행)

금지된 AI 행위에 대한 가이드라인[5)]

• **(목적)** 유럽의 가치와 기본권에 대한 잠재적 위험성으로 인하여 허용될 수 없는 것으로 간주되는 ‘금지된 AI’ 행위의 개요를 제공함으로써, AI 시스템 제공자 및 배포자 등의 AI법 준수를 촉진하기 위함

– 특히 유해한 조작, 사회적 스코어링 및 실시간 원격 생체 인식(RBI) 등을 구체적이고 중점적으로 설명

※ 범용 AI 시스템 및 의도된 목적을 가진 시스템에 대해서도 금지된AI 요건에 해당할 경우, 금지 사항이 적용

〈 금지된 AI 행위[6)] (법 제5조) 〉

금지된 AI 행위	주요내용
유해한 조작 및 속임수 제5조(1)(a)항	• 사람의 의식을 넘어서는 잠재의식적 기법이나 의도적으로 조작 또는 기만적인 기법을 사용하여 행동을 왜곡하거나 심각한 피해 유발 또는 그 가능성이 있는 목적 또는 효과를 내는 AI 시스템
취약점의 유해한 악용 제5조(1)(b)항	• 연령, 장애, 특정 사회적 또는 경제적 상황으로 인한 취약점을 악용하여 행동을 왜곡하거나 심각한 피해 발생 또는 발생 가능성이 있는 목적으로 또는 그 효과를 유발하는 AI 시스템
소셜 스코어링 제5조(1)(c)항	• 사회적 행동, 개인적 또는 성격적 특성을 기반으로 자연인 또는 집단을 평가하거나 분류하는 AI 시스템
개별 범죄 위험 평가 및 예측 제5조(1)(d)항	• 프로파일링 또는 성격 특성 및 특징만을 기반으로 범죄를 일으킬 위험을 평가하거나 예측하는 AI 시스템 (단, 범죄행위와 직접적으로 연결된 객관적이고 검증가능한 사실에 기반하여 인간에 대한 평가를 지원하는 경우는 제외)

5) EUROPEAN COMMISSION, “Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)”, (2025.2.4.)
6) 본 가이드라인에서 제시하고 있는 행위별 구체적 기준 및 예시는 [붙임] 참조

금지된 AI 행위	주요내용
무차별 스크래핑을 통한 얼굴 인식 데이터베이스 제5조(1)(e)항	• 인터넷이나 CCTV 영상에서 얼굴 이미지를 무차별 스크래핑하여 얼굴 인식 데이터베이스를 생성하거나 확장하는 AI 시스템
감정 인식 제5조(1)(f)항	• 직장이나 교육 기관에서 감정을 추론하는 AI 시스템 (단, 의료 또는 안전상의 이유는 제외)
생체 인식 분류 제5조(1)(g)항	• 인종, 정치적 의견, 노동조합 가입 여부, 종교적 또는 철학적 신념, 성생활 또는 성적 지향을 추론하거나 추론하기 위해 생체 데이터를 기반으로 사람을 분류하는 AI 시스템 (단, 법 집행 분야를 포함하여 합법적으로 취득한 생체 데이터세트의 라벨링 또는 필터링은 제외)
실시간 원격 생체 인식 ('RBI') 제5조(1)(h)항	• 법 집행의 목적으로 공개적으로 접근가능한 공간에서 실시간 원격 생체 인식 식별을 위한 AI 시스템 (단, 특정 피해자의 표적 검색, 테러 공격 등 특정 위협을 방지하거나 특정 범죄 용의자 검색에 필요한 경우는 제외) * 승인 등 추가 절차 요건은 AI법 제5조제2항~제7항에 명시되어 있음

• 금지된 AI 시스템이 '시장 출시', '서비스 개시' 또는 '사용'하는 경우에 금지 규정이 적용됨

※ 다만, 실시간 원격 생체 인식('RBI') 시스템(법 제5조1(h)항)은 '사용'되는 경우에만 금지된 AI 시스템에 해당

구분	주요내용
시장 출시 (법 제3조제9항)	• 인공지능 시스템을 EU시장에서 최초로 제공(상업적 활동 과정에서 유상 또는 무상으로 EU시장에 배포하거나 사용하기 위해' 시스템을 공급)하는 것 – 인공지능 시스템의 제공은 애플리케이션 프로그래밍 인터페이스('API')를 통한 시스템 및 서비스에 대한 액세스, 클라우드, 직접 다운로드, 물리적 사본 또는 물리적 제품에 내장되는 등 공급 방식에 관계없이 적용
서비스 개시 (법 제3조제11항)	• EU시장에서 설계 목적으로 처음 사용하기 위해 제공자가 배포자에게 AI 시스템을 직접 공급하거나 또는 자체적으로 사용하기 위해 AI 시스템을 공급하는 것 – 제3자에게 처음 사용하기 위한 공급뿐만 아니라 자체 개발 및 배포도 모두 포함
AI 시스템 '사용' (별도 정의 규정 없음)	– AI법에 명시적으로 정의되어 있지는 않지만, 시장에 출시되거나 서비스에 투입된 후 수명 주기의 모든 순간에 시스템을 사용하거나 배포하는 것을 포함하는 넓은 의미로 이해

• 한편, AI법은 제공자, 배포자, 수입자, 유통업자 등 다양한 범주의 사업자를 구분하고 있으나, 본 가이드라인은 금지된 AI행위의 범위를 고려하여 '제공자'와 '배포자'에 중점을 두고 있음

구분	주요내용
제공자 (법 제3조(3))	• 자연인 또는 법인, 공공기관, 기관 또는 기타 단체로서, AI 시스템을 개발하거나 개발하도록 하여 EU시장에 출시하거나 자신의 이름 또는 상표로 서비스하는 자 – EU 외부에 설립되거나 위치한 제공자의 시스템을 시장에 출시하거나 EU에서 서비스하는 경우 또는 AI 시스템의 결과물이 연합에서 사용되는 경우 * 제공자는 AI 시스템을 시장에 출시하거나 서비스를 제공하기 전에 모든 관련 요건을 충족하는지 확인해야 함
배포자 (법 제3조(4))	• 개인적 비영리 활동을 위한 것이 아닌 한, 자신의 권한 하에 AI 시스템을 사용하는 자연인 또는 법인, 공공기관, 기관 또는 기타 단체 – 배포자는 설립 장소 또는 소재지가 유럽연합 내에 있거나, 제3국에 있는 경우 인공지능 시스템의 결과물이 유럽연합 내에서 사용되는 경우 AI법의 적용 범위에 해당 * 법인을 대신하여 책임과 통제 하에 시스템을 운영하는 제3자(예: 계약업체, 외부직원)의 경우에도 법인은 여전히 배포자에 해당

AI 시스템 정의에 대한 가이드라인[7)]

• **(목적)** 본 가이드라인은 AI법상 AI 시스템에 해당하는지 여부를 판단하는데 도움을 제공하는 한편, 효과적인 법 적용 및 집행 촉진을 하기 위함

– 다만, AI 시스템의 다양성을 고려할 때 모든 잠재적 AI 시스템 의전체 목록을 제시하는 것은 불가능하므로, 궁극적으로 각 시스템별 특성에 따라 평가될 필요가 있음

• **(적용대상)** AI법은 'AI 시스템'의 정의(제3조제1항)를 충족하는 시스템에만 적용

〈 'AI 시스템' 정의 (법 제3조제1항) 〉

• 다양한 수준의 자율성으로 작동하도록 설계되고, 배포 후 적응력을 발휘할 수 있으며, 명시적 또는 암묵적 목표를 위해 수신한 입력으로부터 물리적 또는 가상 환경에 영향을 미칠 수 있는 예측, 콘텐츠, 권장사항 또는 결정과 같은 출력을 생성하는 방법을 추론하는 '기계기반시스템'을 의미

– 'AI 시스템' 정의는 광범위한 시스템을 포괄하는 것으로, SW시스템이 AI 시스템에 해당하는지 여부를 판단 시 ▲해당 시스템의 구체적인 아키텍처와 기능에 기반해야 하며, ▲AI 시스템 정의의 7가지 요소를 고려해야 함

– 한편, AI 시스템 정의는 AI 시스템의 주요 단계 ('배포 전 또는 구축 단계' 및 '배포 후 또는 사용단계') 를 모두 포괄하는 수명주기 기반 관점을 채택

※ 다만, AI 시스템의 주요 구성요소(7가지)가 수명주기 전단계에 걸쳐 지속적으로 존재할 필요는 없음

• 'AI 시스템' 정의의 7가지 요소에 대한 구체적인 설명은 다음과 같음

〈 AI 시스템의 구성요소 : 7가지 〉

구분	주요내용
①기계 기반 시스템	• 기계(machine)'는 AI 시스템을 작동할 수 있도록 하는 HW/SW 구성요소 모두를 포함하는 것으로, 즉, '기계 기반'이란 다양한 계산 시스템을 포괄함을 의미 ※ 모든 AI 시스템은 모델 학습, 데이터 처리, 예측 모델링, 대규모 자동화된 의사결정 등 기능 수행을 위해 기계가 필요하므로 기계기반에 해당
②다양한 수준의 자율성을 가지고 작동하도록 설계된 시스템	• 시스템 개발을 위한 머신러닝과 같은 특정 기술이나 모델 아키텍처가 아닌 시스템이 외부 환경과 상호작용하려는 능력으로서, 이 때 자율성 수준은 AI 시스템의 해당 여부를 판단하는 필수 조건에 해당 ※ AI 시스템의 추론 능력(예측, 콘텐츠, 권장사항, 물리적 또는 가상 환경에 영향을 미칠 수 있는 결정과 같은 결과물을 생성하는 능력)은 자율성 구현에 핵심적 역할로서, 자율성 개념의 핵심은 인간과 기계의 상호작용을 뜻함
③배포 후 적응력을 발휘할 수 있는 시스템	• '적응력'은 사용 중에 시스템의 동작을 변경할 수 있는 '자가 학습 기능'을 의미하며, 적응된 시스템의 새로운 동작은 동일한 입력에 대해 이전 시스템과 다른 결과의 생성이 가능 ※ AI 시스템이 처음 학습된 것 이상의 자동으로 학습 또는 새로운 패턴을 발견하거나, 데이터 관계 식별 능력이 AI 시스템 해당 여부를 결정하는 결정적 조건은 아님

7) EUROPEAN COMMISSION, "Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act)" (2025.2.6.)

구분	주요내용
④명시적 또는 암묵적 목표	• AI 시스템의 목적은 시스템 내부에 있으며, 수행되는 작업의 목표와 그 결과를 뜻함 – (명시적 목표) 개발자가 시스템에 직접 인코딩한 명확하게 명시된 목표 – (암시적 목표) 명시적이진 않으나, 시스템의 동작이나 기본 가정에서 추론할 수 있는 목표
⑤수신한 입력으로부터 예측, 콘텐츠, 권장 사항 또는 결정	• 시스템이 수신한 입력을 기반으로 머신러닝과 논리 및 지식 기반 접근 방식을 사용하여 예측, 콘텐츠, 권장 사항과 같은 출력을 생성하는 능력은 AI 시스템의 기본 작업으로서, 다른 형태의 SW와 구별되는 요소에 해당 (인공지능 시스템의 결과물은 '예측, 콘텐츠, 권장 사항, 결정' 크게 4가지 범주에 속하며, 각 범주별 인간의 개입 수준은 상이함) ※ '출력 생성 능력'과 '시스템이 생성할 수 있는 출력의 유형'은 AI 시스템의 기능과 영향의 핵심적 요소
⑥물리적 또는 가상 환경에 영향을 미칠 수 있는 결과물의 생성 방법을 유추하는 시스템	• '유추하는 능력'은 AI 시스템을 다른 유형의 시스템과 구별하는 핵심적이고 필수불가결 조건으로서, 물리적 및 가상 환경에 영향을 미칠 수 있는 예측, 콘텐츠, 권장 사항 또는 결정과 같은 결과물을 얻는 과정과 입력 또는 데이터로부터 모델이나 알고리즘, 혹은 둘 다를 도출하는 AI 시스템의 능력을 의미 * '추론, 산출물을 생성하는 방법'이란 시스템이 추론 가능한 AI기술을 통해 산출물을 도출하는 구축 단계를 의미 ※ 추론을 가능하게 하는 데 사용될 수 있는 기술에는 '특정 목표를 달성하는 방법을 데이터로부터 학습하는 기계 학습 접근 방식과 해결해야 할 과제의 인코딩된 지식 또는 상징적 표현을 통해 추론하는 논리 및 지식기반 접근방식'이 포함
⑦물리적 또는 가상 환경에 영향을 미칠 수 있는 시스템	• AI 시스템의 영향력이 유형의 물리적 객체(ex.로봇 팔), 디지털 공간, 데이터 흐름, SW 에코시스템을 포함한 가상 환경 전반에 영향을 미칠 수 있음

2) 미국

○ 트럼프 2기 행정부 출범 직후, AI의 안전과 보안성을 강조한 바이든 행정부의 '안전하고 신뢰할 수 있는 인공지능에 대한 대통령 행정명령[8]' 폐기에 서명 ('25.1.20)

• 트럼프 2기 행정부('25.1.20 출범)는 자국 우선주의를 기조로, 미국의 글로벌 AI 리더십과 지배력을 강조하며 바이든 행정부의 AI규제 정책 등을 신속히 폐기하는 등 AI 탈규제 및 산업 육성으로의 전환을 적극적으로 추진 중

〈 바이든 행정부, EO 14110 개요 〉

• AI의 안전하고 보안성 있고 신뢰할 수 있는 개발 및 사용을 위하여 8개 분야* 주요사항 제시
※ ① 새로운 AI 안전 및 보안 기준 제시 ② 개인정보 보호 ③ 평등 및 시민권 증진 ④ 소비자·환자·학생 지원 ⑤ 근로자 지원 ⑥ 혁신과 경쟁 촉진 ⑦ 미국의 국제적 리더십 향상 ⑧ 정부의 책임감 있고 효과적인 AI 사용 보장

• 특히, AI개발 시 AI의 내재적 위험성과 국가안보 위협 등을 고려하여 AI 안전 및 보안성 확보조치를 강조
– AI레드팀 테스트 수행, 이중용도 AI모델 개발 기업에게 연방정부에 대한 정보제공의무 부과, 국가안보 측면에서 사회·경제적으로 파급력이 큰 주요기반시설, CBRN[9] 무기 등을 대상으로 안전한 AI 운용을 위한 분야별 지침 수립 및 연방정부 보고 프로세스 구축 등 제시

8) Safe, Secure & Trustworthy AI ('23.10.30),
9) Chemical, Biological, Radiological and Nuclear(화학, 생물, 방사능, 핵)

새로운 AI 정책 방향을 제시한 '미국의 AI 주도권에 대한 장애물 제거 행정명령(EO 14179)'[18] 발표 ('25.1.23)

〈 미국의 AI 주도권에 대한 장애물 제거 행정명령(EO 14179) 주요내용 〉

구분	주요내용
목적 (제1조)	• 미국은 AI 분야의 글로벌 리더십을 유지하기 위하여 이념적 편향이나 조작된 사회적 의제로부터 자유로운 AI 시스템을 개발해야함 – 이를 위하여, AI 혁신을 저해하는 기존의 특정 AI 정책과 지침을 폐지함
정책 (제2조)	• 인간의 번영, 경제적 경쟁력 및 국가안보 증진을 위하여 미국의 글로벌 AI주도권을 강화하고 지속시키는 정책 방향 제시
정의 (제3조)	• '인공지능' 또는 'AI' 정의는 15 U.S.C.9401(3)을 따름 – 인공지능은, 인간이 정의한 목표에 따라 예측 수행, 추천 제공, 또는 현실/가상 환경에 영향을 미치는 결정을 내릴 수 있는 기계기반시스템 – 또한, 기계 및 인간 기반 입력을 사용하여, ▲현실 및 가상 환경 인지, ▲자동화된 방법으로 분석하여 이러한 인식을 모델로 추상화하고, ▲정보 또는 행동을 위한 선택을 공식화하기 위해 모델 추론을 사용하는 시스템을 의미
인공지능 실행 계획 개발 (제4조)	• 대통령 과학기술보좌관(APST)[10], AI 및 가상화폐 특별보좌관[11], 대통령 국가안보보좌관(APNSA)[12]은 180일 이내에 대통령 경제정책 보좌관[13], 대통령 국내 정책 보좌관[14], 관리예산실장(OMB)[15] 등 관련 연방 부처나 기구의 장과 협업해 제2조에 따른 정책 달성을 위한 '실행 계획(action plan)'을 수립하여 대통령에게 제출해야 함
기존 행정명령 철폐 이행 (제5조)	• APST, AI 및 가상화폐 특별보좌관 및 APNSA는 즉시 모든 기관의 수장들과 협의하여 폐지된 EO 14110과 관련된 정책, 지침, 규제, 명령 및 조치를 검토해야 함 • 관리예산실장(OMB)은 60일 이내에 과학기술보좌관(APST)와 협력하여 필요에 따라 M-24-10[16]및 M-24-18[17]을 미국의 글로벌 AI 지배력 유지 및 강화를 위한 정책과 일치하도록 수정해야 함

EO 14179의 후속조치로서, '인공지능 실행 계획' 관련 의견수렴 진행('25.2.25 ~ 3.15)

- EO 14179에 따라 미국의 AI 주도권을 유지·강화하기 위해 필요한 정책적 사항을 우선 설정하고, 불필요하고 과도한 요구 조치가 민간부문의 AI 혁신을 저해하지 않도록 보장

- 과학기술정책국(OSTP)은 하드웨어 및 칩, 데이터 센터, 에너지 소비 및 효율성, 모델 개발, 오픈 소스 개발, 응용 및 사용(민간 부문 또는 정부), AI 모델 출력의 설명 가능성 및 보증, 사이버 보안 등 새로운 '인공지능 실행 계획'에 포함되어야 할 최우선 정책 조치와 관련한 의견수렴을 추진

  ※ EO 14170 제4조에 따라, 인공지능 실행 계획은 180일 이내(2025년 7월 22일까지) 수립해야 함

10) The Assistant to the President for Science and Technology
11) The Special Advisor for AI and Crypto
12) The Assistant to the President for National Security Affairs
13) The Assistant to the President for Economic Policy
14) The Assistant to the President for Domestic Policy
15) The Director of the office of Management and Budget
16) Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence('24.3.28)
17) Advancing the Responsible Acquisition of Artificial Intelligence in Government('24.10.3)
18) Removing Barriers to American Leadership in Artificial Intelligence

3) 일본

○ 일본 정부는 '인공지능 관련 기술의 연구, 개발 및 활용 촉진에 대한 법안[19]' 의회 제출 ('25.2.28)

- 일본 정부는 인공지능 관련 기술의 역량 강화 및 AI 산업의 국제 경쟁력 향상을 위하여 거버넌스 체계 수립, 인공지능 전략본부 설치, 인프라 구축 등을 주요내용으로 한 '인공지능 관련 기술의 연구, 개발 및 활용 촉진에 대한 법안(AI법안)' 마련을 추진 중[20]

  - (기본원칙) 인공지능 관련 기술은 경제사회 발전, 국가안보, 신산업 창출 및 행정·민간분야 등 효율성 극대화를 추진할 수 있는 기술로서, ▲기초 연구부터 활용 단계까지 종합적이고 체계적으로 추진해야 하며, ▲인공지능 관련 기술의 연구, 개발 및 활용이 범죄 이용, 개인정보 유출, 저작권 침해 등 불법적인 목적 또는 방법으로 수행되는 것을 방지하기 위하여 기술 개발 과정에서의 투명성 등 기타 필요한 조치가 이뤄져야 함

  ※ '인공지능 관련 기술'이란, 인간의 인지, 추론 및 판단의 지적 능력을 인위적 방법으로 대체하는 기능을 구현하기 위해 필요한 기술 및 이러한 기술을 이용하여 입력된 정보를 처리하고 그 결과를 출력하는 기능을 구현하기 위한 정보처리 시스템 관련 기술을 의미

  - (국가 거버넌스 체계 수립) 인공지능 기술 개발 및 활용 촉진을 위한 기본방침, 정부의 역할 등을 명시한 기본계획 수립, 인공지능 전략본부 설치 등 국가 차원의 종합적 AI 거버넌스 체계를 수립

  ※ 내각은 인공지능 관련 기술의 연구 개발 및 활용 촉진에 관한 조치를 종합적·체계적으로 추진하기 위하여 '인공지능 전략본부'를 설치함

  - (사업자 책무) 인공지능 관련 기술을 활용한 제품 또는 서비스 개발자·제공자·사업 활동에 활용하는 자 및 기업은 기본원칙에 따라 인공지능 관련 기술의 적극적 활용을 통해 기업활동의 효율성을 고려하고, 신산업 창출을 위한 노력 및 정부·지방자치단체가 시행하는 정책에 협력해야 함

  - (시설·장비 개발 및 공유) 국가는 인공지능 관련 기술의 연구, 개발 및 활용에 필요한 대규모의 정보처리, 정보통신 및 전자 기록[21]을 제공하며, R&D 기관 및 사업자가 이용할 수 있도록 관련 시설·장비, 지적 인프라의 개발 및 공유 촉진을 위해 필요한 조치를 해야 함

  - (인재양성) 국가는 지방자치단체, 연구개발기관 및 사업자와 협력하여 인공지능 관련 기술에 대한 기초연구부터 활용 단계 전반에 걸쳐 전문 인재양성을 확보하기 위한 필요한 조치를 해야 함

  - (자료 제출 요구 등) 인공지능 전략본부는 사무 집행을 위해 필요한 경우 사업자를 대상으로 자료 제출, 의견 표명, 설명 제공을 요구할 수 있음

19) 人工知能関連技術の研究開発及び活用の推進に関する法律案
20) 본 법안은 정기국회 회기 내(6월)에 통과가 전망되고 있음
21) 전자적 방법, 자기적 방법 또는 기타 인간의 인지에 의하여 인식할 수 없는 방법으로 이루어진 기록으로서 전자컴퓨터에 의한 정보처리에 사용되는 기록을 의미

3. 시사점

○ 한국, AI 3대 강국 도약을 위한 '인공지능기본법' 제정을 통해 AI산업 발전을 위한 초석 마련

- 우리나라는 AI산업 환경을 조성하고, 안전하고 신뢰할 수 있는 인공지능을 제공하기 위하여 EU AI법에 이어 세계 두 번째로 한국형 인공지능기본법을 제정
  - 국가 AI 발전과 신뢰 기반 조성을 위한 추진체계 수립, 인공지능 연구개발·학습용데이터·인공지능 데이터센터·집적단지 등 인공지능 산업육성 지원, 고영향·생성형 인공지능에 대한 안전·신뢰 기반 조성[22]을 주요내용으로 함
  - 본 법의 주요 규제대상은 고영향 인공지능으로서 안전성·신뢰성·투명성 확보조치를 의무화하고 있으며, 생성형 인공지능, 학습 사용 누적연산량을 기준으로 한 인공지능의 경우에도 일부 의무사항을 규정
- 그러나 고영향 인공지능 개념의 모호함, 사업자 유형별 의무 차별화 미비, 해외 사업자와 국내 사업자 간 형평성 문제 등에 대한 의견[23]이 있으며, 특히 본 법의 핵심 규제대상인 고영향 인공지능의 판단 기준이 불명확하여 국내 인공지능 산업 발전 저해에 대한 우려가 제기됨
- 이에, 정부는 인공지능기본법의 제정 목적은 국가 AI 경쟁력 강화임을 강조하며, 규제 대상 및 수준에 대한 해석을 신중하게 접근할 것임을 밝히는 등 최소한의 규제 사항만을 포함하겠다고 발표[24]

○ AI 주도권 확보 경쟁을 둘러싼 글로벌 기술 패권 경쟁 심화

- EU는 미국 빅테크 기업의 AI 기술 독점을 견제하고, AI로 인한 시민의 안전과 권리 보호를 목적으로 세계 최초의 포괄적 AI규제 입법을 마련하였고, 최근 금지된 AI 시스템 사례 및 AI 시스템 정의에 대한 가이드라인을 발행하는 등 원활한 법 집행을 위한 후속조치가 계속해서 이뤄질 것으로 전망
- 반면, 미국은 트럼프 2기 행정부의 자국 우선주의 기조를 통해, 글로벌 시장에서의 AI 지배력 선점을 유지하기 위한 'AI 혁신 우선'으로 정책 방향을 선회하였고, 구체적인 AI실행 계획 마련을 추진 중

※다만, 바이든 행정부 AI행정명령(EO 14110)은 AI 인재 유치 등의 내용을 포함하고 있으나, 트럼프 2기 행정부 취임 이후 즉각 폐기됨으로써 향후 외국인의 미국 내 AI 산업 참여 제한이 우려되는 상황

- 이처럼, EU와 미국은 규제와 혁신 사이에서 정반대의 입장을 취했으나, 지난 2월 프랑스 파리에서 개최된 '인공지능 행동 정상회의(AI Action Summit 2025)'에서 EU는 기존의 엄격한 규제 준수 입장을 다소 완화하는 새로운 정책 방향을 시사함
  - 이는, EU가 기존의 강력한 규제 기조를 유지할 경우 미국, 중국 등 AI 산업에 막대한 투자를 통해 기술 발전 속도가 급격히 이뤄지고 있는 국가들에 비해 EU의 AI산업 발전 저해 및 유럽 기업들의 경쟁력이 현저히 떨어질 것을 우려한 입장이 반영된 것으로 보임

22) '인공지능 시대의 새로운 서막, 인공지능 기본법 국회 본회의 통과' (과기정통부 보도자료, 2024.12.26.)
23) "AI 기본법 보완 발의 잇따라… "완성도 높여야" (THE AI, 2025.3.10.보도) https://www.newstheai.com/news/articleView.html?idxno=7371
24) "유상임 장관, AI 기본법 '최소 규제' 가닥…AI 경쟁력 강화 '총력'", (이코노믹 데일리, 2025.3.11.보도) https://www.economidaily.com/view/20250311174838807

- 한편, 일본은 AI에 대한 규제보다 국가경쟁력 확보 방안으로서 AI산업 육성에 중점을 둔 방향으로 AI기본법 제정안 마련을 추진 중
  - 본 법안은 기본원칙으로서 인공지능 기술 개발 과정에서의 투명성 확보를 명시하고 있으며, 이는 인공지능의 위험성 관리 측면에서 안전성 확보의 필요성을 강조하고 있는 것으로 보임
  - 한편, 인공지능 전략본부는 사무 집행 필요 시 사업자를 대상으로 자료 제출, 설명 제공 등을 요구할 수 있다고 규정하고 있으나, 위반 시 제재조치 및 벌칙 규정이 부재하여 실효성에 대한 의문이 제기됨
  - 다만, 본 법안 추진 이전까지 AI 관련 사항은 가이드라인 제시에 불과하였으므로, 국가 차원에서 AI 연구 및 인재 육성 등을 골자로 한 본 법안의 제정 추진은 글로벌 시장에서의 일본 AI산업 경쟁력 확보를 위한 의지를 엿볼 수 있음

※ 지난해 일본 경제산업성(METI)과 총무성(MIC)은 'AI R&D 가이드라인', 'AI활용 가이드라인', 'AI원칙 구현을 위한 거버넌스 지침'을 통합·업데이트한 'AI 사업자 가이드라인(1.0)('24.4 발표)'에서 공통지침으로서 안전·보안 확보사항을 명시하고 있으나, 법적 구속력 없는 한계가 있었음

- 최근 중국은 오픈소스 생성형 AI인 딥시크를 공개하면서 미국 중심의 AI생태계를 위협하는 딥시크 쇼크를 일으켰으나, 딥시크 사용자 개인정보 유출 등 보안 우려로 미국을 중심으로 자국민의 딥시크 사용을 신속하게 제재

※ 중국 '데이터보안법'상 딥시크 사용자의 개인정보 등이 중국에 있는 딥시크 서버에 저장되며, 이때 중국 당국의 요청이 있을 경우 사업자는 이를 제공해야 하는 의무가 있음

AI 규제 수준은 최소화, 반면 AI 보안은 강조될 전망

- 전 세계적으로 국가의 미래 경쟁력 확보를 위해 AI혁신과 산업 발전에 총력을 기울이는 추세로, AI로 인한 위험을 통제하기 위한 안전성·신뢰성 및 투명성 확보의무 등 규제 수준은 가급적 최소화될 것으로 전망
  - AI 기술 및 산업을 주도하는 미국이 AI산업 발전에 저해되는 규제에 반대하는 상황에서, 세계 최초로 AI법을 제정한 EU도 동법을 엄격히 적용하는 것이 EU AI기업에 불리하게 작용될 가능성을 고려할 수 밖에 없음
  - 우리나라도 법을 통한 사업자 규제보다는 AI산업 발전에 초점을 둔 정책에 주력할 것으로 보임

- 한편, 지금까지 인공지능 위험은 국민의 생명·신체 및 재산에 대한 안전과 기본권 보호와 같은 포괄적인 안전·신뢰성 확보에 초점을 두고 논의되었으나, 앞으로 국가간 AI경쟁 격화, 첨단AI 기술을 이용한 국가 안보 침해 우려 등으로 AI보안(AI security)의 중요성이 부각될 것으로 보임

※ 러시아 '오버클러커스'는 AI기반 탐지 시스템이 핵잠수함의 은밀성을 무력화할 수 있음을 경고('25.1.7)[25]

  - 지난 2월, 영국은 2023년 세계 최초로 설립한 'AI 안전연구소(AI Safety Institute)'의 명칭을 'AI 보안연구소(AI Security Institute)'로 변경하면서, AI가 국가 안보 및 범죄에 미치는 위험으로부터 시민을 보호하는 것을 목표로 제시

※ AI기술이 화학 및 생물학 무기를 개발하는데 어떻게 사용될 수 있는지, 사이버공격을 수행하는데 어떻게 사용될 수 있는지, 사기 및 아동 성적 학대와 같은 범죄를 가능하게 하는 방법 등 심각한 AI위험에 초점을 맞출 것이라고 하면서, 국가사이버안보센터(NCSC)와 같은 국가 안보 커뮤니티와 협력을 강화할 것임을 밝힘

- 이에 AI보안성 확보를 위한 책임있는 개발·배포를 촉진하고 기술적 지원을 강화하는 한편, AI를 이용한 범죄행위에는 강력한 대응책 모색 필요

25) "AI가 해군력 판도 바꿔…핵잠수함의 스텔스 기술 무력화할 수도" (글로벌이코노믹, 2025.1.7. 보도)

붙 임 EU 집행위원회, '금지된 AI 행위에 대한 가이드라인' 주요내용 – '금지된 AI' 행위별 구체적 기준 및 예시

• **(유해한 조작 및 속임수)** AI 시스템은 1) 잠재의식을 의도적으로 조작하거나 기만하는 기술로서, 2) 사람 또는 집단의 행동을 실질적으로 왜곡하는 목적 또는 효과가 있으며, 3) 왜곡된 행동이 해당 개인, 타인이나 집단에 심각한 피해를 입히거나 그럴 가능성이 높은 경우 금지되어야 함

※ 해당 요건을 모두 충족해야 하며, 사용된 기법과 해당 사용자의 행동에 대한 중대한 왜곡, 해당 행동으로 인해 발생했거나 발생 가능성이 있는 중대한 피해 사이에 인과관계가 있어야 함

– 본 규정 관련, 시장 감시 당국은 각 사례의 구체적인 사실과 상황을 조사하여 AI 시스템이 배포한 잠재적, 의도적 조작 또는 기만적 기술이 '평균적' 개인의 의사 결정과 자율성 및 자유로운 선택을 현저하게 손상시킬 가능성을 평가하고 시스템이 상당한 피해를 야기할 우려 등 검토해야 함

〈 '유해한 조작 및 속임수(법 제5조(1)(a)항)'의 구체적 기준 〉

<table>
<tr><th>구분</th><th>주요내용</th></tr>
<tr><td colspan="2">■ 잠재의식을 의도적으로 조작하거나 기만하는 기법</td></tr>
<tr><td>잠재의식 기술</td><td>• 잠재의식 기법은 시청각 또는 촉각 매체를 통해 전달되는 자극을 통해 사용할 수 있으며, 미묘하기 때문에 인식하기 어려우나, 의식적으로 인지되지 않더라도 뇌에서 처리되어 행동에 영향을 미칠 수 있음
<table>
<tr><th>구분</th><th>예시</th></tr>
<tr><td>시각적 잠재의식 메시지</td><td>동영상 재생 중에 기술적으로 볼 수 있지만 의식적으로 인식하기에는 너무 빨리 깜박이는 이미지나 텍스트를 표시하거나 삽입하는 경우</td></tr>
<tr><td>청각적 잠재의식 메시지</td><td>소리나 언어 메시지를 낮은 음량으로 전달하거나 다른 소리에 가려져 청취자가 의식하지 못하는 경우</td></tr>
<tr><td>비가시적(Subvisual) 및 비가청적(Subaudible) 큐잉(Cueing)</td><td>사람의 눈으로 의식적으로 감지하기에는 너무 빠르게 깜박이는 시각적 자극(ex. 이미지) 또는 귀로 감지할 수 없는 음량 등 정상적인 조건에서 사람의 감각으로 전혀 감지할 수 없는 방식으로 자극을 전달할 수 있음</td></tr>
<tr><td>임베디드 이미지</td><td>뇌에서 처리되어 행동에 영향을 미칠 수 있는 다른 시각적 콘텐츠 내에 이미지를 숨기는 경우</td></tr>
<tr><td>잘못된 방향</td><td>인지적 편향과 주의력의 취약점을 악용하는 경우</td></tr>
<tr><td>시간조작</td><td>AI 시스템이 사용자와의 상호작용 과정에서 시간 조작을 일으켜 사용자의 행동에 영향을 미치고 조급함과 의존성을 유발하는 경우</td></tr>
</table>
• 빅데이터 분석, 신경 기술, 뇌-컴퓨터 인터페이스, 가상현실 등 AI 및 관련 기술의 급속한 발전으로 인해 잠재의식의 정교한 조작 위험과 무의식적인 방식으로 인간 행동에 효과적으로 영향을 미치는 경우
*(예시) AI는 사용자가 인지하지 못하는 사이에 은밀하게 사용자의 뇌를 훈련시켜 심각한 피해를 줄 수 있는 방식으로 매우 침입적이고 민감한 신경 데이터 정보(예: 개인 은행 정보, 내밀한 정보 등)를 공개하거나 유추하는 데 사용될 우려
• 새로운 기계-뇌 인터페이스와 드림 해킹 및 뇌 스파이웨어 같은 첨단 기술로도 확장될 가능성 농후</td></tr>
<tr><td>의도적으로 조작하는 기술</td><td>• AI법상 별도 정의 규정은 없으나, 개인의 자율성과 자유로운 선택을 훼손하는 방식으로 개인의 행동에 영향을 미치거나 변경 또는 통제하기 위해 설계되거나 객관적인 목적을 가진 기술
– 조작 기법은 일반적으로 인지적 편견, 심리적 취약성 또는 개인이 영향을 받기 쉬운 상황적 요인을 악용하도록 설계
*(예시) 불안과 정신적 고통을 증가시켜 사용자의 행동에 심각한 피해를 줄 정도로 영향을 주는 경우</td></tr>
<tr><td>속임수 기법</td><td>• AI 시스템에 의해 배포되는 '기만적 기술'은 개인을 속일 목적 또는 효과를 가지고 허위 또는 오도된 정보를 제시하고 개인의 자율성, 의사 결정 및 자유 선택을 저해하는 방식으로 행동에 영향을 미치는 것
*(예시) 합성 음성으로 사람이나 친척, 친구를 사칭하여 사기 및 심각한 피해를 입힌 AI 챗봇</td></tr>
</table>

<table>
<tr><th>구분</th><th colspan="2">주요내용</th></tr>
<tr><td colspan="3">■ 개인 또는 집단의 행동을 중대하게 왜곡할 목적 또는 효과가 있는 경우</td></tr>
<tr><td>행동의 중대한 왜곡</td><td colspan="2">• 사람들의 행동에 영향을 미칠 수 있는 잠재의식적이거나, 의도적 조작 또는 기만적인 기술을 통해 정보에 입각한 의사결정능력을 현저하게 손상시킴으로써 다른 방법으로는 하지 않았을 행동을 하거나 결정을 내리게 하는 행위
– (현저한 장애) 합법적인 설득을 넘어서는 정도의 강압, 조작 또는 기만 등을 수반
– (정보에 입각한 결정) 사용가능한 옵션, 각 선택의 위험과 혜택, AI 시스템이 사용자의 행동에 미칠 수 있는 영향, 적절한 경우 의사 결정이나 사용자의 행동에 중요한 기타 상황 정보를 포함한 관련 정보에 대한 이해와 지식</td></tr>
<tr><td rowspan="4">중대한 피해를 야기할 경우
(상당한 가능성 포함)</td><td>피해 유형</td><td>내용</td></tr>
<tr><td>심리적 피해</td><td>• 개인의 정신 건강 및 인지적, 정서적 취약점을 악용하는 조작 기술을 배포하는 AI 시스템으로서, 즉각적으로 드러나지 않을 수 있으나 지속적이고 심각한 결과 초래가 우려 (다만, 이를 측정하는 것은 어렵기 때문에 사례별 관련 상황을 종합적으로 고려 하여 그 심각성을 판단하는 것이 필요)
* (예시) 인간의 말 패턴, 행동 및 감정을 모방하도록 설계된 AI 애플리케이션은 의인화된 특징과 감정을 통해 사용자가 서비스에 정서적으로 의존하게 함으로써 자살 행동 및 타인에게 해를 끼칠 위험 등 심각한 피해를 야기할 가능성 있음</td></tr>
<tr><td>재정적 및 경제적 피해</td><td>• 재정적 손실, 재정적 배제, 경제적 불안정 등 다양한 악영향을 포함
*(예시) 심각한 금전적 피해를 유발하는 사기성 상품을 제공하는 챗봇</td></tr>
<tr><td>피해의 심각성에 대한 임계값</td><td>• 잠재적, 조작적, 기만적 기법으로 인한 피해가 '중대한' 경우에만 적용
– 피해의 심각성은 중대한 피해에 대해 객관적이고 관찰 가능한 효과가 있는 AI 시스템 사용으로 인해 발생했거나 발생할 가능성이 있는 피해의 정도를 의미
– (중대성 고려 요건) ▲AI 시스템의 상호의존성, 다양한 유형의 피해 조합, 개인 또는 집단에 대한 악영향, ▲구체적 상황 및 누적 효과, ▲피해 규모 및 강도▲영향을 받는 사람의 취약성, ▲지속 기간 및 가역성</td></tr>
<tr><td>인과관계 및 '합리적인 피해 가능성' 임계값</td><td>• '합리적으로 발생할 가능성이 있는 경우'에도 금지 조항을 적용하며, 이는 객관적 기준과 보편적인 인정 기준(ex. 기술 및 과학)에 따라 합리성을 판단하는 것을 의미
• 한편, 금지 가능성 있는 AI 시스템을 제공하거나 사용하지 않기 위해 조작 또는 기만적 기술을 배포하는 AI 시스템의 제공자와 배포자는 ▲투명성 및 개인의 자율성, ▲관련 법률 준수, ▲최신 관행 및 업계 표준을 준수하는 것을 권고</td></tr>
</table>

• **(취약점의 유해한 악용)** 1) 연령, 장애 또는 사회경제적 상황으로 인한 취약점을 악용해야 하며, 2) AI 시스템에 의한 착취는 개인 또는 집단의 행동을 실질적으로 왜곡하는 목적 또는 효과, 3) 왜곡된 행동은 해당 개인, 다른 사람 또는 집단에게 심각한 피해를 입히거나 그럴 가능성이 높아야 함

– '취약성'의 개념을 별도 정의하고 있지 않으나, 이는 개인 또는 집단이 정보에 입각한 결정을 내리거나 행동에 영향을 미칠 수 있는 인지적, 정서적, 신체적 및 기타 형태의 취약성 등 광범위한 범주를 포괄

* 연령, 장애 또는 특정 사회경제적 상황으로 정의된 취약 집단 외의 경우는 AI법 제5조1(b)항의 범위를 벗어남

〈 '취약점의 유해한 악용(법 제5조(1)(b)항)'의 구체적 기준 〉

구분	주요내용
나이	• 연령은 주요 취약성 범주에 포함되는 것으로, 어린이(18세 미만)나 노인 모두를 포함
장애	• 신체적, 정신적, 지적, 감각적 장애를 포괄
특정 사회·경제적 상황	• '특정'은 개인의 고유한 특성이 아닌, 특정 취약한 사회 또는 경제적 집단에 대한 법적 지위나 구성원으로 해석되어야 함 – 다만, 이 범주는 원칙적으로 비교적 안정적이고 장기적인 특성을 다루는 것을 목표로 하지만 일시적인 실업, 과도한 부채나 이주 상태 등 일시적 상황도 특정 사회경제적 상황으로 포함될 수 있음 ※ 누구나 겪을 수 있는 고충이나 외로움 등의 상황은 사회경제적 관점에서 구체적이지 않으므로 적용대상 제외 * (예시) 이주민, 난민 등 특수한 사회적 상황의 사람들은 법적 지위와 사회경제적 안정성이 부족한 경우가 많으며 특히 AI 시스템에 의한 착취에 취약할 수 있음
행동을 심각하게 왜곡하는 목적 또는 효과를 가진 경우	• 취약점 악용은 ▲'목적'이 있거나, ▲'집단의 행동을 실질적으로 왜곡하는 효과'를 가져야 함 – 이때, 사소한 영향이 아닌 실질적인 영향을 의미하나, 반드시 고의성이 필요하지 않음
중대한 피해를 야기할 경우 (상당한 가능성 포함)	• 취약한 사람 또는 집단의 행동 왜곡이 해당 사람 또는 다른 사람에게 심각한 피해를 입히거나 그럴 가능성이 합리적으로 높아야 함 – 위 법 제5조1항(a)호와 동일한 개념을 사용하므로 동일한 판단기준 적용
조작적이고 기만적이며 악용적인 AI 시스템	• 법 제5조1(a)항 및 (b)항의 금지조항 적용 시 필수요건은 'AI를 이용한 취약점 조작 및 악용이 중대한 피해를 야기하거나 야기할 가능성이 합리적'이어야 함 * (예시) AI 동반자 시스템, 치료 챗봇, 온라인 음악 플랫폼, 피싱 시도를 모방한 보안 교육 및 기타 학습 시뮬레이션에 사용되는 AI 기반 조작 및 기만 기법

• **(소셜 스코어링)** 1) AI 시스템은 특정 기간에 걸쳐 자연인 또는 자연인 그룹을 평가하거나 분류하기 위한 목적(사회적 행동, 개인 특성 등)으로 사용하거나 이를 기반으로 사용해야 하며, 2) AI 시스템의 도움으로 생성된 소셜 스코어링은 ▲데이터가 원래 생성되거나 수집된 것과 관련이 없는 사회적 맥락에서, 그리고/또는 ▲사회적 행동이나 그 심각성에 비해 불균형적인 대우를 받는 경우 등 개인이나 그룹에 불합리한 대우를 야기할 수 있는 것

〈'소셜 스코어링(법 제5조(1)(c)항)'의 구체적 기준 〉

구분	주요내용
특정기간 동안의 사회적 행동이나 개인적 또는 성격적 특성을 기반으로 한 평가 또는 분류	• (자연인 또는 자연인 집단의 평가 또는 분류) 공공 및 민간 부문의 평가 및 분류 관행을 모두 포괄하는 광범위한 범위를 포괄 (단, 원칙적으로 법인은 제외) * '평가'는 '데이터보호법'상 '프로파일링' 개념과 연관 있으며, 이는 특정 형태의 평가를 구성 * (예시) AI 시스템이 자연인 또는 집단을 평가하거나 분류하기 위한 목적으로서, 이들의 사회적 행동 또는 개인적·성격적 특성에 따라 점수를 부여하는 경우
	• (특정기간 동안) 평가 또는 '특정기간'에 걸친 데이터를 기반으로 해야 함 – 특정한 개별 상황의 데이터 또는 행동에 대한 일회성 또는 일괄적인 평가나 등급으로 제한되어서는 안되며, 해당 사건의 모든 상황을 고려하여 평가하는 것이 중요
	• (사회적 행동 또는 알려진, 추론되거나 예측된 개인적 또는 성격적 특성) ▲개인 또는 집단의 사회적 행동, ▲알려진, 추론되거나 예측된 개인 및 성격적 특성(또는 둘 다와 관련된) 인공지능 기반 데이터 처리로서, 데이터는 당사자가 직접 제공하거나 감시를 통해 간접적으로 수집한 정보, 제3자로부터 얻은 정보 또는 다른 정보로부터 추론하여 수집한 정보 등을 뜻함

구분	주요내용
소셜 스코어링으로 불리한 대우를 받거나, 사회적 행동의 심각성에 비해 정당하지 않거나, 불균형적인 대우를 받아야 함	• (소셜 스코어링과 평가 사이의 인과적 연관성) AI 시스템에 의한 또는 그 도움을 통해 생성된 소셜 스코어링의 평가 또는 집단에 대해 불리하거나 불리한 대우로 이어져야 함 • (관련 없는 사회적 맥락에서 해롭거나 불리한 대우 및/또는 정당하지 않거나 불균형한 대우) 소셜 스코어링에 따라 불이익 또는 불리한 대우가 발생하거나 발생할 수 있어야 함 *▲데이터가 원래 생성되거나 수집된 맥락과 관련 없는 사회적 맥락에서, 또는 ▲사회적 행동이나 그 심각성에 비해 정당하지 않거나 불균형적인 경우
공공 또는 개인이 제공하거나 사용 여부와 무관	• 공공 또는 민간에 의해 제공되거나 사용되는지 여부에 관계없이 허용되지 않는 AI를 이용한 소셜 스코어링 관행을 금지함 – (관할 시장 감시 당국의 점검) AI 관행이 합법적이고 정당한 것임을 입증해야 할 책임 ※ (예외) AI 시스템 제공자와 배포자는 각자의 책임에 따라, ▲AI 시스템 기능의 투명성, 데이터 유형 및 출처에 대한 정보 제공 등 해당 데이터가 합법적으로 수집되었는지, ▲AI 시스템이 의도대로 작동하는지, ▲그로인한 불리한 대우가 정당하고 사회적 행동에 비례하는지 등 관련 법률을 준수하고, 합법적이고 유익한 목적(예: 절차의 효율성, 서비스 품질, 안전 등)으로 사람을 평가하거나 분류하기 위해 AI 시스템을 사용할 수 있음 – 다만, 금지된 AI 시스템의 소셜 스코어링에 해당하지 않도록 제공자와 배포자는 고위험 AI 시스템(예: 필수 공공 서비스 및 혜택, 신용도 평가 등)에 대한 요건 준수로서, 위험 관리, 투명성, 데이터 거버넌스, 기본권 영향 평가, 인적 감독, 모니터링 등에 대한 지침을 제공

• **(개별 범죄 위험 평가 및 예측)** AI 시스템은 1) 자연인이 범죄를 저지를 위험을 평가하거나 예측하는 위험 평가를 수행해야 하며, 2) ▲자연인의 프로파일링, ▲자연인의 성격 특성 평가 등의 위험을 평가하거나 예측하는 것을 기반으로 해야 함

※ 다만, 범죄 예측 및 위험 평가 활동 자체를 금지하는 것은 아님을 유의할 필요 있음

* (예외) 위치 기반 또는 지리 공간 예측 또는 장소 기반 범죄 예측, 범죄 행위와 관련된 객관적이고 검증 가능한 사실에 기반하여 사람의 평가를 지원하는 AI 시스템, 법인 관련 범죄 예측 및 평가에 사용되는 AI 시스템

〈 '개별 범죄 위험 평가 및 예측(법 제5조(1)(d)항)'의 구체적 기준 〉

구분	주요내용
범죄를 저지른 사람의 위험 평가 또는 가능성 예측	• '범죄 예측'은 일반적으로 범죄학 이론과 결합하여 다양한 첨단 AI 기술과 분석 방법을 통해 대량의 과거 데이터(사회-경제 데이터 및 경찰 기록 등)에 적용하여 범죄를 통제하고 예방하기 위한 경찰 및 법 집행 전략과 조치를 알리는 근거로서 활용 • '범죄 예측 AI 시스템'은 과거 데이터 내에서 패턴을 식별하여 지표를 범죄 발생 가능성과 연관시킨 후, 예측 결과물로 위험 점수를 생성 *(예시) 자원이 부족한 법 집행 당국이 범죄를 탐지, 저지 및 예측하기 위한 사전 예방적 접근을 가능하게 하나, 타인의 미래 행동을 예측하기 위해 범죄에 대한 과거 데이터를 사용하면 편견을 지속하거나 강화할 우려 – 범죄의 예방 및 적발 단계뿐만 아니라 수사, 기소 및 형사 처벌의 집행 단계 등 법 집행 활동의 모든 단계에서 이루어질 수 있음
자연인의 프로파일링 또는 성격 특성의 평가 기반	• AI 시스템이 자연인 또는 그룹의 성격 특성을 동시에 프로파일링하거나 평가 여부와 관계없이 적용 – 특정 그룹(예: 테러리스트, 갱스터 등)에 대한 프로필을 구성하고 적용하는 것으로서, 이전에 다른 사람이 저지른 범죄에 대한 과거 데이터를 바탕으로 범죄 가해자 범주를 구성하는 경우를 의미

구분	주요내용
	• (자연인 프로파일링) '특정 개인적 측면 평가'를 포함하는 것으로, 범죄를 저지른 사람의 위험을 평가하거나 예측하기 위한 목적으로 수행 • (성격 및 특성 평가) 범죄를 저지른 사람의 위험을 평가하거나 예측하기 위한 위험 평가가 그 사람의 성격적 특성을 평가하는 경우에도 적용 • (전적으로) 개인의 프로파일링 또는 성격 특성에 대한 평가를 '전적으로' 하는 경우에만 금지 규정이 적용되며, 이때 '전적으로'(법 제42조)는 프로파일링 또는 성격 특성 평가에 모두 적용 ※ (예외) 범죄 행위와 직접적으로 연관된 객관적이고 검증 가능한 사실에 기반한 인간의 평가를 지원하는 AI 시스템은 제외 (고위험 AI 시스템으로 분류되는 경우, 법 집행 당국(또는 위탁받은 경우)은 인적 감독을 포함한 요건과 안전장치 적용

• **(무차별 스크래핑을 통한 얼굴 인식 데이터베이스)** 1) 얼굴 인식 데이터베이스를 구축하거나 확장하기 위한 목적으로, 2) 데이터베이스 구축·확장 시 무차별 스크래핑을 위하여 AI도구를 사용하되, 3) 이 때, 이미지의 출처는 인터넷 또는 CCTV영상을 그 요건으로 함

* (예외) 얼굴 이미지 이외의 생체 데이터(예: 음성 샘플), 스크래핑에 AI 시스템이 관여하지 않는 경우, AI 모델 학습 또는 테스트 목적으로 사용되는 얼굴 이미지 데이터 베이스 등 개인 식별을 위해 사용되지 않는 경우는 예외에 해당

〈 '무차별 스크래핑을 통한 얼굴 인식 데이터베이스((법 제5조(1)(e)항'의 구체적 기준 〉

구분	주요내용
얼굴 인식 데이터베이스	• '데이터베이스'는 컴퓨터의 신속한 검색 및 검색을 위해 특별히 조직된 데이터 또는 정보의 집합 – 데이터베이스의 목적이 반드시 얼굴 인식에 사용될 것을 요구하지 않음
무차별 스크래핑을 통해 얼굴 이미지 획득	• '스크래핑'은 일반적으로 웹 크롤러, 봇 또는 기타 수단을 사용하여 CCTV, 웹사이트, 소셜 미디어 등 다양한 소스에서 데이터 또는 콘텐츠를 자동으로 추출하는 것을 뜻함 – 데이터베이스를 탐지하여 정보를 추출하고, 해당 정보를 다른 목적으로 사용하도록 프로그래밍된 소프트웨어('프로그램')를 도구로서 활용 • '무차별'은 대상을 구체적·개별적으로 지정하지 않고, '진공청소기'처럼 가능한 많은 데이터와 정보를 흡수하는 기법을 뜻함 ※ (예외) 스크래핑 도구에 특정 개인이나 미리 지정된 그룹의 사람 얼굴만 포함된 이미지나 동영상을 수집하도록 지시하는 경우 또는, 특정 범죄자를 찾거나 피해자 그룹을 식별하는 등의 목적으로 스크래핑되는 경우에는 본 법 적용대상에서 제외 – 이에, 시스템에서 이미지 또는 동영상에 대한 타겟 검색과 비타겟(무차별) 검색을 결합하는 경우, 비타겟 스크래핑은 금지 ※ (예외) 인터넷에서 대량의 얼굴 이미지를 수집하여 가상 인물에 대한 새로운 이미지를 생성하는 AI 시스템(단, 이 경우 AI법 제50조의 투명성 요건에 해당할 수 있음)
인터넷 및 CCTV 영상	• 얼굴 이미지의 출처가 인터넷 또는 CCTV 영상을 요건으로 하고 있음 – 다만, 인터넷의 경우 개인이 소셜 미디어 플랫폼에 자신의 얼굴 이미지를 게시했다고 해서 해당 이미지가 얼굴 인식 데이터베이스에 포함되는 데 동의했다고 볼 수 없음 – 한편, CCTV 영상에서 얼굴 이미지를 스크랩하는 예시 (공항, 거리, 공원 등의 장소에서 운영되는 감시 카메라로 촬영한 이미지) – 이 때, AI 시스템이 사람의 사진을 받아 인터넷에서 일치하는 얼굴을 검색하는 경우, 즉 '이미지 검색 엔진을 리버스 엔지니어링'하는 경우 이는 표적 스크래핑으로 간주

• **(감정 인식)** 1) 직장 및 교육 기관의 영역에서 2) 자연인의 감정을 추론하는 AI 시스템 금지(의료 또는 안전상의 이유로 시스템을 사용하는 경우는 제외)

※ 금지 대상에 해당하지 않는 감정 인식 시스템은 부속서 III (1)(c)항에 따라 고위험 AI 시스템으로 간주되며, 투명성 요건을 준수해야 함

〈 '감정 인식(법 제5조(1)(f)항) '의 구체적 기준 〉

구분	주요내용
감정을 추론하는 AI 시스템	• (감정을 추론하는 AI 시스템) '자연인의 감정을 식별하거나 추론하는 AI 시스템을 의미 – '감정 인식 시스템(법 제3조제39항)'은 '생체 인식 데이터를 기반으로 자연인의 감정이나 의도를 식별하고 추론하는 것을 목적으로 하는 AI 시스템'으로 정의 · '생체 인식 데이터 기반'은 개인의 신체적 또는 행동적 속성으로서, 입력 방법은 한 가지 방식(예: 얼굴 이미지) 또는 여러 방식(예: 얼굴 정보와 뇌파(EEG)를 결합한 방식)과 관련될 수 있는 바, 감정 인식, 생체 분류 또는 기타 목적으로 사용되는 모든 생체 데이터를 포함 – '추론'은 일반적으로 식별을 전제 조건으로 하므로, 금지 규정은 감정이나 의도를 식별하거나 추론하는 AI 시스템을 모두 포함하는 것으로 이해해야 함 – 즉, 법 제5조 제1항(f)의 금지 규정은 다른 감정 인식 시스템에 적용되는 규정(부속서 III, 제1항(c) 및 AI법 제50조)과 유사한 범위를 갖는 것으로 해석하고 개인의 생체 데이터를 기반으로 한 추론으로 제한할 필요가 있음 *(예시) 키 입력(타이핑 방식), 얼굴 표정, 신체 자세 또는 움직임에서 감정을 추론하는 AI 시스템은 생체 인식 데이터를 기반으로 하므로 금지 범위에 해당하나, 특정 글의 스타일이나 어조를 정의하기 위해 작성된 텍스트(내용/감정 분석)에서 감정을 추론하는 AI 시스템은 생체 데이터를 기반으로 하지 않으므로 금지 범위에 포함되지 않음
	• 감정 또는 의도 식별 및 추론 – '식별'은 자연인의 생체 데이터(예: 음성 또는 표정)를 처리하여 감정 인식 시스템에서 이전에 프로그래밍된 감정과 직접 비교하고 식별할 수 있는 경우 발생 – '추론'은 시스템 자체에서 분석 및 기타 프로세스를 통해 생성된 정보를 추론하는 방식으로 이뤄짐. 이 경우 감정에 대한 정보는 자연인에 대해 수집된 데이터에만 기반하지 않고, 데이터로부터 감정을 감지하는 방법을 학습하는 머신러닝 접근 방식을 포함하여 다른 데이터로부터 추론
	• (감정) 명백한 표정이나 제스처가 감정이나 의도를 식별하거나 유추하는 데 사용되는 경우 에는 금지 대상에 포함 – AI법 제5조1(f)항의 목적상 감정 또는 의도의 개념은 넓은 의미로 이해되어야 함 *(예시) 몸짓, 찡그린 표정, 미소 없는 얼굴 등을 통해 직원이 고객에게 불행하거나 슬프거나 화가 났다고 추론하는 AI 시스템, 음성이나 몸짓을 통해 학생이 화가 나서 폭력적인 행동을 하려고 한다는 것을 추론하는 AI 시스템
직장 및 교육 기관에 대한 금지 조치의 제한	• (직장) 직원, 계약자, 연수생, 자원봉사자 등의 지위와 무관하며, '사업장' 개념은 고용, 근로자 관리 및 자기 고용의 영역에서 AI 시스템의 시장 출시, 서비스 투입 또는 사용을 다루는 AI법의 다른 조항과 일관되게 선발 및 채용 과정에서 후보자를 대상으로 적용되는 것으로 이해되어야 함 • ('교육 기관) 공립 및 사립 교육 기관을 모두 포함하는 것으로 이해해야 하며, 학생의 유형이나 연령 또는 특정 환경(온/오프라인 등)에 대한 제한은 없음 *(예시) 교육 기관에서 학생이 해당 애플리케이션을 사용하도록 요구하는 경우 이러한 감정 인식 시스템의 사용은 금지되나, 교육 기관 외부에서 온라인 언어 학습을 위해 감정 인식을 사용하는 AI 기반 애플리케이션은 금지된 AI 시스템에 해당하지 않음
의료 및 안전상의 이유로 인한 예외	• 치료용 시스템과 같이 의료 또는 안전상의 이유(생명 및 건강 보호와 관련)로 직장 및 교육 기관의 영역에서 사용되는 감정 인식 시스템은 명시적 예외대상에 해당 – 특히, 치료적 용도는 CE 마크가 부착된 의료기기 사용을 의미하며, 웰빙의 일반적인 측면을 감지하기 위한 감정 인식 시스템의 사용은 포함하지 않음을 유의해야 함 ※ 직장에서의 일반적인 스트레스 수준 모니터링은 건강 또는 안전 측면에서 허용되지 않으므로, (예시) 직장이나 교육 기관에서 번아웃이나 우울증을 감지하기 위한 AI 시스템은 금지

• **(특정 '민감한' 특성에 대한 생체 인식 분류)** 1) 생체 인식 데이터를 기반으로 2) 자연인을 개별적으로 분류하여 3) 인종, 정치적 의견, 노동조합 가입 여부, 종교적 또는 철학적 신념, 성생활 또는 성적 취향을 추론하거나 유추하는 4) 생체 인식 분류 시스템

※ 다만, EU 또는 국내법에 따라 법 집행 목적으로 획득한 생체 데이터 셋의 라벨링, 필터링 또는 분류에는 미적용(예: 법 집행 기관에서 아동 성적 학대 자료가 포함된 것으로 의심되는 데이터 세트에 라벨을 지정하고 필터링할 수 있는 AI 시스템, 용의자를 식별하는 데 도움이 되는 손가락 길이나 구별되는 표시 또는 문신과 같은 특정 특성에 따라 가해자의 손을 필터링하고 라벨을 붙이는 행위)

〈 특정 '민감한' 특성에 대한 생체 인식 분류(법 제5조(1)(g)항) 의 구체적 기준 〉

구분	주요내용
생체 인식 분류 시스템	• 생체 인식 데이터는 생체 특징을 기반으로 하는 행동 특성을 포함한 것으로, 생체 인식 분류의 범위에는 스카프나 십자가 등 옷이나 액세서리, 소셜 미디어 활동에 따른 분류는 제외 • 생체 인식 분류는 특정 범주에 사람을 할당하는 신체적 특징(예: 얼굴 특징 및 형태, 피부색)을 기준으로 할 수 있으나, 일부는 인종과 같이 EU 차별금지법에 따라 보호되는 특수한 '민감한' 특성 또는 특성일 수 있음 – 다만, AI법상 생체정보 분류의 정의 범위를 벗어나기 위해서는 '다른 상업적 서비스에 부수적일 것, 객관적인 기술적 이유로 반드시 필요할 것' 등 두 가지 조건을 모두 충족해야 함
개인은 생체 인식 데이터에 따라 개별적으로 분류	• 자연인을 '개별적으로' 분류해야 하지만, 생체 인식 분류의 목적이나 결과가 아닌 경우(예: 개인이 아닌 전체 그룹을 분류하는 경우) 금지 규정이 적용되지 않음 *(예시) 특정 특징(예: 오른쪽 눈 밑의 흉터)이나 오른손에 문신이 있다는 이유로 개인을 분류하고 선별할 수 있는 AI 시스템은 '개별 생체 인식 분류'에 해당하나, 금지된 AI 시스템에 적용되기 위한 경우 다른 요건도 모두 충족해야 함
인종, 정치적 의견, 노동조합 가입 여부, 종교적 또는 철학적 신념, 성생활 또는 성적 취향을 추론하거나 유추하는 행위	• 인종, 정치적 견해, 노동조합 가입 여부, 종교 또는 철학적 신념, 성생활 또는 성적 지향 등 제한된 수의 민감한 특성을 추론하거나 유추하는 것을 목적으로 하는 생체 인식 분류 시스템은 금지대상에 해당 *(예시) 문신이나 얼굴에서 개인의 종교적 성향을 추론할 수 있다고 주장하는 생체 인식 분류 시스템 ※ (예외) 피부색이나 눈 색깔에 따라 범죄 피해자의 DNA를 분석하는 시스템, 또는 범죄 피해자의 출신을 고려하여 범죄 피해자의 DNA를 분석하는 시스템은 예외적 경우에 해당

• **(실시간 원격 생체 인식 시스템(RBI))** 1) 법 집행 목적으로 2) 공공장소에서 3) 실시간(Real-Time) 원격 생체 인식 시스템(Remote Biometric Identification)의 사용 금지

– 해당 시스템의 배포자만 해당 조항의 적용을 받으며, 법 제5조1(h)항(i)~(iii)호의 경우 예외적으로 허용

※ (예외적 허용) (i)납치, 인신매매 또는 성적 착취의 특정 피해자에 대한 표적 수색과 실종자 수색, (ii)자연인의 생명 또는 신체적 안전에 대한 구체적이고 실질적이며 임박한 위협 또는 테러, (iii)공격의 실질적이거나 예측 가능한 위협을 방지하기 위한 목적인 경우에 한하여 허용

* (예시) 용의자가 어느 방향으로 도주하는지 확인하는 등 자연인을 추적하는 데 사용되는 AI 시스템도 생체 인식의 정의에 포함될 수 있으나, 범죄 용의자의 위치 파악을 허용(법 제5조(1)(h)(iii))

– 예외적 허용(법 제5조1(h)항(i)~(iii)호)을 위하여 법 집행 목적으로 공개적으로 접근 가능한 공간에서 실시간 RBI 시스템의 사용을 승인하는 경우, 고위험 AI 시스템에 대한 규칙도 해당 사용에도 적용

※ 원격 생체 인식 시스템은 고위험 AI 시스템(법 제6조 2항에 따른 부속서 III)으로서, 실시간 원격 생체 인식 시스템과 구별

〈 '실시간 원격 생체 인식(RBI) 시스템(법 제5조(1)(h)항)'의 구체적 기준 〉

구분	주요내용
실시간	• '실시간'은 시스템이 생체 데이터를 '즉각적으로, 또는 어떠한 경우에도 상당한 지연 없이' 캡처하고 추가 처리하는 것을 의미 – '상당한 지연 없이'란, AI 법에 별도 정의하고 있지 않으므로 사례별로 평가해야 함 * (예시) 법 집행 기관이 모바일 기기를 통해 몰래 사람의 사진을 촬영하여 즉각적인 검색을 목적으로 데이터베이스에 제출하는 경우, 상황에 따라 금지 사항에 해당할 수 있음
원격 생체 인식	• (본인 확인 목적으로만 사용되는 '생체 인식') '생체 인식'은 데이터베이스에 저장된 개인의 생체 인식 데이터와 해당 개인의 생체 인식 데이터를 비교하여 자연인의 신원 확인을 목적으로 신체적, 생리적, 행동적 또는 심리적 인간의 특징을 자동으로 인식하는 것 ※ (예외) '생체 인증'은 센서에 제시된 데이터를 스마트폰, 여권 또는 신분증 등 기기에 저장된 이전에 기록된 다른 데이터 세트와 비교하는 것으로 구성되며, 생체 인증의 목적은 특정 사람이 자신이 주장하는 사람인지 확인하는 경우 금지된 AI 시스템에 해당하지 않음 • (원격성) 일반적으로 개인의 생체 인식 데이터와 참조 데이터베이스에 포함된 생체 인식 데이터를 비교하여 원거리에서 개인의 적극적인 개입 없이 생체 인식 시스템이 개인을 식별할 수 있는 능력 ※ (예외) 서비스에 대한 액세스, 기기 잠금 해제, 구내 보안 액세스 등의 목적으로만 자연인의 신원을 확인하기 위해 생체 인식 시스템을 사용하는 것은 '원격'의 개념에서 제외 * (예시) – 감시 목적으로 지하철 역의 벽이나 천장에 설치된 카메라에 사용되는 RBI 시스템 (○) – 생체인식 지하철 티켓 등 사람이 적극적으로 개입하고 의식적으로 생체인식 센서에 접근하여 접근 권한을 얻는 데 사용되는 시스템 (X) • (참조 데이터베이스) 비교 목적의 생체 인식 데이터가 포함된 참조 데이터베이스가 없으면 신원 확인이 불가능하므로, 신원 확인을 위한 비교 수행을 위하여 참조 데이터베이스의 존재 필수 * (예시) 쉥겐 정보 시스템(Schengen Information System) 데이터베이스를 얼굴 인식 목적의 참조 데이터베이스로 사용하는 경우
공개적으로 액세스 가능한 공간에서	• '공개적으로 액세스 가능한 공간(법 제3조제44항)'은 특정 액세스 조건의 적용 여부와 잠재적인 수용 인원 제한에 관계없이 불특정 다수의 자연인이 접근할 수 있는 공공 또는 개인 소유의 모든 물리적 공간 ※ (예외) 온라인 공간 또는, 공장, 회사, 작업장 등 제한된 인원만 출입할 수 있는 특정 공간 혹은, 교도소 및 국경 통제소 등 일반인이 접근할 수 없는 공간 ※ 일반인이 접근할 수 있는 공간인지 여부는 사례별 분석을 기반으로 해야 함
법 집행 목적	• 법 집행은 법 제3조제46항에서 '공공 안전에 대한 위협으로부터 보호하고 예방하는 것을 포함하여 범죄의 예방, 수사, 적발, 기소 또는 형사 처벌 집행을 위해 법 집행 기관(또는 이들을 대신하여) 수행하는 활동'으로 정의 – 공공 안전 위협에 대한 보호 및 예방을 포함하여 형사 범죄의 예방, 수사, 적발, 기소 또는 형사 처벌의 집행을 담당하는 모든 공공기관 * (예시) 법 집행 업무를 수행하는 경찰 당국 및 형사 사법 당국(ex. 검찰) 포함 – 회원국 법률에 따라 공안 위협에 대한 보호 및 예방을 포함하여 범죄의 예방, 수사, 적발, 기소 또는 형사 처벌의 집행을 목적으로 공권력 및 공적 권한을 행사하도록 위임받은 기타 모든 기관 또는 단체

• **(제5조(1)(h)항 적용 시 공통 요건)** 법 집행 목적으로 공공장소에서 '실시간' RBI시스템을 사용하는 것은 기본권 침해에 해당하므로, AI법 제5조(5)는 회원국의 국내법에 따라 예외적으로 시스템 사용에 대한 법적 근거 마련이 필요

– 배포자로부터 법 집행 목적으로 공개적으로 접근 가능한 공간에서 실시간 RBI 시스템의 사용 통보를 받은 회원국의 국가 시장 감시 당국 및 국가 데이터 보호 당국은 위원회에 연례 보고서를 제출해야 함

※ 위원회는 집계된 데이터를 바탕으로 연례 보고서를 발행해야 함

– **(제5조(1)(h)항(i)호 적용 시 조건)** 1) 표적대상의 개인 식별 및 보호조치, 2) 사전 승인 필요, 3) 법 집행을 위해 공개적으로 접근 가능한 공간에서 '실시간' 원격 생체 인식 시스템을 사용할 때마다 당국에 통지

* AI법 제5조(1)(h)항의 금지 규정이 적용되지 않는 기타 모든 RBI 시스템 사용은 '고위험 인공지능 시스템(법 제6조)'의 범주에 해당(부속서 III)

〈 예외적 허용을 위한 안전장치 및 조건(법 제5조제2항) 〉

구분	주요내용
· (제5조(1)(h)항(i)호 적용 시 조건) 납치, 인신매매, 성적 착취의 특정 피해자에 대한 표적 수색 및 실종자 수색을 위해 실시간 표적 시스템의 사용을 위하여 ▲표적 개인 및 보호조치, ▲사전 승인, ▲당국에 통지 요건을 준수해야 함	
표적 개인 및 보호조치	• 납치, 인신매매, 성적 착취의 특정 피해자에 대한 표적 수색 및 실종자 수색(제5조(1)(h)항(i)호)을 위해 실시간 표적 시스템의 사용행위에는 법 제5조(2)~(7)항의 안전장치 및 조건 적용 – '특정인의 신원 확인'을 위하여 법 집행 목적으로 공개적으로 접근 가능한 공간에서 실시간 표적 시스템의 사용을 허용 – 시스템 사용 전, 시스템을 사용할 수 있는 상황의 특성(특히 시스템을 사용하지 않을 경우 발생할 수 있는 자연인, 사회 및 법 집행 목적에 대한 피해의 심각성, 가능성 및 규모를 시스템 사용 시 관련자의 권리와 자유에 미치는 결과 등과 비교하여 평가해야 함) – 실시간 RBI의 사용은 지리적 범위, 기간, 대상자 측면에서 명확하게 제한되어야 함 – 실시간 RBI 시스템의 배포 전, 배포하는 법 집행 기관은 기본권 영향 평가를 실시하고 해당 시스템을 EU데이터베이스에 등록해야 함(정당한 사유가 있는 경우 제외)
사전 승인 필요	• 실시간 표적 시스템의 개별 사용은 사전 승인 필요 (다만, 이러한 시스템의 결과물에 따라서만 법적 효력을 발생시키는 자동화된 의사결정은 경우 금지) – 기본권 영향평가 및 관할 국가 당국이 사용을 승인한 경우에만 사용 가능
당국에 통지	• 제5조(1)(h)항(i)호에 열거된 사항 중, 법 집행을 위해 공개적으로 액세스 가능한 공간에서 '실시간' 원격 생체 인식 시스템을 사용할 경우, 관련 시장 감시 당국 및 국가 데이터 보호 당국에 통지해야 함

Reference

▪과학기술정보통신부, '인공지능 기본법을 위한 '하위법령 정비단' 본격 출범' 보도자료 (2025.1.16.)

▪제22대 국회 제418회(정기회) 제3차 과학기술정보방송통신위원회(정보통신방송법안심사소위원회) 회의록 (2024.11.21.)

▪https://artificialintelligenceact.eu/implementation-timeline/

▪https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act

▪https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application

▪https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/

▪https://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g21709029.htm

▪https://news.kbs.co.kr/news/pc/view/view.do?ncd=8152063

▪https://biz.newdaily.co.kr/site/data/html/2025/01/14/2025011400239.html

▪https://www.etnews.com/20250311000267

▪https://www.yna.co.kr/view/AKR20250301028700073

▪https://www.economidaily.com/view/20250311174838807

▪https://www.newstheai.com/news/articleView.html?idxno=7371

PART Ⅱ

「디지털의료제품법」 시행 및 디지털제품 보안

1. 디지털 시대의 도래 및 「디지털의료제품법」 제정

• **(제정 배경)** 디지털 시대의 도래로 의료기기 분야에서도 인공지능 등 디지털 기술의 적용이 확대되고 있으며, 디지털의료제품의 등장은 환자의 치료 기회 확대 및 일상적인 질병의 예방·관리 실현에 기여할 것으로 예상

- 다만, 이들 제품은 디지털 기술의 특성상 기술개발의 속도가 빠르고 영역 간 융복합이 활발하게 이루어지며 사이버보안 등 문제가 발생할 수 있어 하드웨어 및 전통적인 의약품에 적합한 기존 규제체계로는 대응에 한계

- 이에 **디지털의료제품의 특성**을 **반영**한 **관리체계**를 **별도로 구축**하여 디지털의료제품의 안전성 및 유효성을 확보하기 위한 **「디지털의료제품법」 제정·시행**('24.1.23. 제정, '25.1.24. 시행)*

* 한편, 디지털의료·건강지원 기기는 '26.1.24. 시행 예정이며, 「디지털의료제품법 시행령」('25.1.24) 및 「디지털의료제품법 시행규칙」('25.2.28) 제정·시행에 이어 '25.3월 현재 고시 제정 추진 중(고시 1건 제정 완료)[26]

• **(구성 및 체계)** 「디지털의료제품법」은 총 9장(章), 61조(條)로 구성

〈 「디지털의료제품법」 구성 〉

구분	주요내용
제1장 총칙	- 목적, **정의(디지털의료기기, 디지털융합의약품, 디지털의료·건강지원기기 등), 제품의 분류 및 등급 지정,** 다른 법률과의 관계 등
제2장 안전관리종합계획의 수립 등	- 디지털의료제품 안전관리종합계획 수립·시행, 디지털의료제품에 대한 자문
제3장 디지털의료기기	- **디지털의료기기 제조·수입 허가,** 임상시험계획 승인, **디지털의료기기제조업자등 준수사항, 전자적 침해행위 보호 조치, 실사용 평가, 우수 관리체계 인증 등** - 디지털의료기기소프트웨어 품질관리기준 적합판정, 판매 특례 등
제4장 디지털융합의약품	- 디지털융합의약품 제조·수입 허가 등
제5장 디지털의료·건강지원기기	- 디지털의료·건강지원기기 제조·수입 신고, 성능인증, 유통관리
제6장 디지털의료제품 발전을 위한 기반 마련	- 디지털의료제품 영향평가, **허가·신고 등 사전 검토, 구성요소 성능평가,** 인력양성, 연구개발 및 표준화 지원, 디지털의료제품 규제지원센터, 인증업무대행기관 지정 등
제7장 관리·감독 등	- 보고와 검사, 업무 정지 등
제8장 보칙, 제9장 벌칙	- 심사 결과의 공개, 수수료, 권한의 위임·위탁, 벌칙 및 과태료 등

26) 「디지털의료제품 분류 및 등급 지정 등에 관한 규정」, 「 디지털의료제품 허가·인증·신고·심사 및 평가 등에 관한 규정」, 「디지털의료기기 제조 및 품질관리 기준」, 「디지털의료기기 임상시험계획 승인 및 실시·관리에 관한 규정」, 「 디지털의료기기 전자적 침해행위 보안지침」, 「우수관리체계 인증 기준에 관한 규정,」 「디지털융합의약품 허가 등에 관한 수수료 규정」, 「디지털의료제품법에 따른 기관 지정 등에 관한 규정」(해당 규정은 3.6. 제정 완료) 해당

2. 디지털의료제품법 주요내용 – 디지털의료제품의 안전성 확보 관련 내용을 중심으로

○ 적용 대상 : 디지털의료제품

• **(범위)** 「디지털의료제품법」은 디지털의료제품의 범위를 ▲디지털의료기기, ▲디지털융합의약품, ▲디지털의료·건강지원기기로 정의(법 제2조제2호)

– **(디지털의료기기)** 지능정보기술, 로봇기술, 정보통신기술, 가상융합기술 등 첨단 디지털 기술*이 적용된 의료기기 또는 이 의료기기와 디지털 의료·건강지원 기기가 조합된 제품

* 디지털기술의 세부 범위는 동법 시행규칙 및 「디지털의료제품 분류 및 등급 지정 등에 관한 규정」(안)에서 규정하고 있으며, '독립형 소프트웨어 기술', ' 인공지능기술', '지능형로봇기술', '초고성능컴퓨팅 기술', '가상융합기술'로 명시

– **(디지털융합의약품)** 디지털의료기기 또는 디지털의료·건강지원기기와 조합된 의약품

– **(디지털의료·건강지원기기)** 의료의 지원 및 건강의 유지·향상을 목적으로 사용되는 디지털 기술이 적용된 제품으로 디지털의료기기를 제외한 제품

• **(분류 및 등급 지정)** 식품의약품안전처장(이하, 식약처장)은 디지털의료제품의 사용목적, 기능 및 사용 시 인체에 미치는 잠재적 위해성 등에 따른 체계적·합리적 안전관리를 위해 디지털의료제품 분류 및 등급 지정(법 제3조)

– 이에 따라 디지털의료기기의 경우 사용목적, 사용 시 인체에 미치는 잠재적 위해성, 기기에 적용되는 기술 유형, 기기의 형태를 고려하여 제품 또는 제품군별로 분류하고, 안전관리의 수준*이 높은 순서에 따라 4등급부터 1등급까지 구분하여 제품 또는 제품군별로 지정(시행규칙 제3조)

* 이 경우 디지털의료기기의 소프트웨어적 특성도 고려되도록 ▲해당 소프트웨어가 사용되는 의료적 상황 또는 환자의 상태, ▲소프트웨어가 의료에 미치는 영향, ▲소프트웨어의 성능저하, ▲오작동으로부터 발생 가능한 직접적·간접적 피해 정도, ▲소프트웨어의 기능적 특성을 판단기준으로 명시(시행규칙 [별표1])

– 다만, 안전관리의 수준이 아직 정해지지 않은 기기의 경우 등급을 지정하지 않거나 임시지정이 가능하며(시행규칙 제3조제2항 단서), 이는 신기술이 적용된 디지털의료기기의 경우 일률적으로 위해성을 심사하기 어렵고 분류 및 등급체계를 미리 정할 수 없는 경우가 존재하는 점을 고려한 것임

○ 디지털의료제품의 제조·수입 등

• **(디지털의료기기 제조·수입 등)** 디지털의료기기 제조업·수입업을 하려는 자는 식약처장의 허가를 받아야 하며, 디지털의료기기 제조업자·수입업자(이하, 디지털의료기기제조업자등)는 제조·수입하려는 디지털의료기기 제품 또는 제품군별로 제조·수입 신고·인증·허가를 받아야 함(법 제8조, 제11조)

– 이 경우 허가 등 신청 시 ▲사용목적 및 작용원리 ▲소프트웨어 검증 및 유효성 ▲전자적 침해행위로부터 보호조치 ▲사용적합성 등 관련 자료를 제출하도록 하여(시행규칙 [별표2]), 허가 등 심사 과정에서 디지털의료기기의 특성이 고려될 수 있도록 함

– 한편, 디지털의료기기제조업자등은 신고·인증·허가 받은 사항 중 디지털의료기기의 안전성·유효성에 영향을 미치는 중요한 사항이 변경된 경우 변경 신고·인증·허가 의무(법 제11조, 제12조)

※ 중요한 사항에 해당하지 않는 사항의 변경 시는 변경된 사항에 대한 기록 작성·보관 및 식약처장 보고 의무만 부담(법 제11조 제2항)

• **(디지털융합의약품 제조 등)** 의약품과 디지털의료기기, 디지털의료·건강지원기기가 조합된 디지털융합 의약품의 특수성을 고려한 통합적인 평가체계 마련

– 즉, 기존 「약사법」 등에 따르면 주된 기능이 의약품인 경우 이와 조합된 디지털의료기기나 디지털 의료·건강지원기기 부분에 대해서는 평가가 이루어지기 어려웠으나,

– 「디지털의료제품법」은 디지털융합의약품 제조업·수입업 허가와 디지털융합의약품 제조 판매 또는 수입 허가(품목별)를 규정하면서(법 제29조제1항), 디지털융합의약품의 부분을 구성하는 디지털의료기기 또는 디지털의료·건강지원기기의 평가와 관련된 사항*을 규정(동조 제2항)

* 디지털융합의약품 제조 허가 신청 시 디지털의료기기가 조합된 경우 디지털의료기기 제조·수입 신고·인증·허가에 필요한 자료(법 제8조 참고), 디지털의료·건강지원기기와 조합된 경우 디지털의료·건강지원기기 성능인증 자료(법 제34조 참고) 제출 요구

– 또한, 이미 신고·인증·허가를 받은 디지털의료기기와 조합된 경우에는 그 신고서·인증서·허가서 제출로 디지털융합의약품 관련 허가 신청 시 필요한 자료 일부를 갈음할 수 있도록 함(동조 제2항 단서)

• **(디지털의료·건강지원기기 제조 등)** 의료기기·의약품과 공산품의 중간영역에 있어 법령상 별도 규정·관리되고 있지 않던 개인용 건강관리(웰니스) 제품 등 디지털의료·건강지원기기에 대한 관리체계 마련

– 이에 따라 디지털의료·건강지원기기를 제조·수입·판매하려는 자는 식약처장에게 신고할 수 있으며, 식약처장은 신고 또는 성능인증 받은 기기를 관리목록에 등재 및 공개할 수 있음(법 제33조)

※ 디지털의료·건강지원기기는 원칙적으로 신고를 하지 않아도 제조 등이 가능하나, 신고한 기기의 경우 식약처장의 성능인증을 받을 수 있으며, 포장·용기 및 홍보물 등에 성능인증 표지 사용 가능(법 제34조)

• 한편, 「디지털의료제품법」은 빠르게 발전하고 융합하는 디지털 기술의 특성에 맞춰 디지털의료제품의 **인·허가** 절차를 **간소화**하고 **전주기 안전성 확보**를 위한 **다양한 허가·평가 체계** 규정

〈 디지털의료제품의 다양한 허가·평가 체계 세부내용 〉

관련 제도	제도 주요내용	효과(절차 간소화/안전성 확보)
실사용 평가 (제15조)	시판 후 디지털의료기기제조업자등이 해당 기기를 실제 사용하는 과정에서 수집·생성된 정보를 바탕으로 해당 기기의 안전성·유효성 평가	· **(간소화)** 실사용 평가 결과를 변경 신고·인증·허가 등에 활용 · **(안전성 확보)** 기기 성능 및 안전성 정보의 변경 등을 신속하게 반영 가능
우수 관리체계 인증 (법 제16조)	식약처장은 디지털의료기기 안전성 확보 및 품질 유지를 위해 디지털의료기기제조업자등 대상으로 우수 관리체계 인증 가능	· **(간소화)** 인증을 받은 경우 허가 등에 필요한 자료 일부 면제 · **(안전성 확보)** 또한 필요한 자료의 제출 시기·방법을 달리 정할 수도 있어 자료 제출 범위가 시판 후까지 확대
구성요소 성능평가 (법 제40조)	센서, 인공지능 알고리즘 등 디지털의료제품 구성요소에 대해 미리 그 성능을 평가	· **(간소화)** 동일한 구성요소 사용 제품의 경우* 허가 등에 필요한 자료 일부 면제 * 허가 등 신청 시 성능평가 결과 제출 제품
인공지능 적용 기기 허가 시 변경관리 계획 제출 (규칙 제7조제2항 등)	인공지능기술이 적용된 디지털의료기기는 제조 허가·인증 시 변경관리계획서 추가 제출 가능	· **(간소화)** 변경관리 계획의 범위에서 경미한 변경으로 처리(변경 허가·인증 不要) · **(안전성 확보)** 빠르게 변화하는 인공지능기술 변경 등을 신속하게 반영 가능

* 식약처 보도자료('24.7.31.) 및 국회 보건복지위원회 『디지털의료제품법안 디지털의료제품에 관한 법률안 검토보고』('23.4월) 내용 재구성

○ 전자적 침해행위로부터 보호 등

• **(준수사항)** 디지털의료기기제조업자등은 **디지털의료기기의 결함이나 오류, 전자적 침해행위*** **등**으로부터 디지털의료기기의 **안전 관리 및 소비자 보호**를 위한 사항 **준수 의무**(법 제13조, 시행규칙 제29조)

* 해킹, 컴퓨터 바이러스, 논리 · 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 디지털의료기기의 안전성과 유효성, 성능 등에 영향을 미치는 행위

〈 준수사항 세부내용 〉

- 디지털의료기기의 오작동, 기능의 미비 등 제품의 결함이나 오류로 인하여 발생하는 문제를 지속적으로 수집 · 관리, 개선
- 전자적 침해행위로부터의 취약점에 대한 지속적인 보완
- 제품의 결함이나 오류 또는 전자적 침해행위로 발생하는 문제를 개선 또는 보완한 경우에는 디지털의료기기가 공급 · 설치된 장소 또는 사용자에게 알리고, 그 조치 정보를 기록 · 보관
- 디지털의료기기의 입출고 정보를 확인하고 기록 · 보관
- 결함이나 오류 등으로 인체에 위해를 끼치거나 끼칠 위험이 있는 디지털의료기기로 의심되는 경우 식약처장이 정하는 바에 따라 보고하고 필요한 안전조치를 실시
- 의료기기, 의약품 또는 디지털의료 · 건강지원기기에서 생성, 수집 · 가공된 데이터를 사용하여 작동하는 디지털의료기기를 제조 · 수입하려는 경우 「개인정보 보호법」, 「의료법」 등 관련 법령에 따라 적법하게 수집 · 가공된 데이터를 사용
- 그 밖에 식품의약품안전처장이 정하여 고시하는 안전관리 및 소비자 보호를 위한 기준 준수

• **(전자적 침해행위로부터 보호)** 디지털의료기기제조업자, 디지털의료기기 융합의약품 제조업자 등은 전자적 침해행위로부터 안전한 보호를 위해 디지털 의료기기 취약점의 지속적 감시 및 물리적·기술적 관리체계 구축에 대한 **보안지침 준수 의무**(법 제14조)

– '24.12.16. 행정예고된 **「디지털의료기기 전자적 침해행위 보안지침」(안)**은 **레거시 디지털의료기기*** 에 대한 **보안**체계, **SBoM 관리체계**를 따르도록 하고, 전자적 침해행위 발생 시 대응요령 등 규정

* 레거시 디지털의료기기 : 제품에 대한 업데이트 지원 등이 종료된 디지털의료기기

– 또한, 인공지능기술이 적용된 디지털의료기기의 경우 인공지능에 대한 학습데이터 중독, 변형, 조작 등 데이터에 대한 공격, 인공지능 모델 추출 및 회피 공격 등 **인공지능 침해**에 대한 **보안 방안** 별도 규정

〈 보안지침(안) 주요내용 〉

대상	디지털의료기기 제조업자 등 (제조업자+수입업자+소프트웨어의 유지 관리업무를 위탁받은 자) **디지털의료기기 융합의약품 제조업자 등**					
내용	**보안활동 문서화**	**물리적 보안체계**	**기술적 보안체계**	**위험관리**	**전자적 침해행위 대응**	**취약점 감시 및 대응**
	· 보안업무 수행 문서화	· 장비 등 물리적 보안 · 운영 기기의 보안 통신	· 데이터 보안 · 인공지능 보안	· 위험 관리 활동과 개발 및 검증 활동	· 침해사고 신고, 침해사고 조치 방안	· 취약점 감시 · 취약점 공개 · 취약점 조치 방안

* 식약처 보도자료('24.12.17.) 참고

• **(위반 시 제재)** 디지털의료기기제조업자 등이 준수사항(법 제13조) 및 보안지침(법 제14조)을 위반한 경우 허가 등 취소, 업무 전부·일부 정지 명령(법 제50조) 및 500만원 이하 과태료 부과(제61조제1항) 가능

3. 디지털 연결 기기 안전성 확보 관련 해외 동향

1) 미국, 「연방 식품·의약품·화장품법」(FD&C법)

• 미국은 **네트워크**를 **활용**하는 **의료기기**에 대한 **사이버보안 강화**를 위해 **「연방 식품·의약품·화장품법」**(이하, FD&C법) **개정**('22.12월)

- 연방식품의약품청(이하, FDA)는 의료기기의 사이버보안 강화를 위해 '14년부터 「시판 전 사이버보안 지침」을 마련·적용해 오고 있었으며, 이번 개정은 FDA에 의료기기 사이버보안 관련 권한을 명시적 부여

※ 현재 FDA는 개정 내용에 대한 가이던스 초안을 공표('24.10월)한 상태이며, 초안이 확정되면 기존 「시판 전 사이버보안 지침」에 해당 내용 추가 반영(Section Ⅷ)

• **(적용 대상) 사이버 기기**(cyber device) 해당하는 의료기기

- 사이버 기기는 ▲제조사가 검증, 설치 또는 승인한 소프트웨어를 포함하고 ▲인터넷 연결 능력이 있으며 ▲사이버보안 위협에 취약할 가능성이 있는 제조사가 검증, 설치 또는 승인한 기술적 특성을 포함하고 있는 기기를 의미(제524B조 (c))

• **(사이버보안 요구사항 준수의무)** 사이버 기기의 **시판 전 허가**를 **신청**하는 자는 해당 기기의 **사이버보안 요구사항**을 **준수**하여야 하며, 요구사항 준수를 확인하기 위해 보건복지부 장관이 요구하는 정보를 포함하여야 함(제524B조(a), (b))

〈 사이버보안 요구사항(제524B조 (b) (1)~(4)) 〉

- **조정된 취약점 공개**(coordinated vulnerability disclosure, CVD) 및 관련 절차를 포함하여 **시판 후 사이버보안 취약점 및 악용**을 **모니터링, 식별** 및 **해결**하기 위한 **계획**을 장관에게 제출
- 기기 및 관련 시스템의 **사이버보안 확보(cybersecure)**에 대한 **합리적**인 **보증 제공**을 위한 **프로세스 및 절차**를 설계, 개발 및 유지하고, 기기 및 관련 시스템에 대한 **시판 후 업데이트 및 패치 제공**
- 상용, 오픈소스 및 기성 소프트웨어(off-the-shelf software) 구성요소를 포함한 **소프트웨어 자재 명세서(SBoM)**를 장관에게 제출
- 장치 및 관련 시스템의 사이버보안 확보(cybersecure)에 대한 합리적인 보증을 입증하기 위해 장관이 규정을 통해 요구할 수 있는 기타 요건 준수

• **(금지행위) 사이버보안 요구사항 미준수** 시 동법상 **금지행위**에 **해당**하여 1년 이하의 징역 또는/및 1,000달러 이하 벌금 부과(제331조(q), 제333조(a))

2) EU

○ EU「의료기기 규정」및「체외 진단 의료기기 규정」

• EU는 의료기기 및 체외 진단 의료기기의 안전성 및 유효성을 확보하기 위하여 각각「의료기기 규정」[27] 및「체외 진단 의료기기 규정」[28]을 제정·시행 중

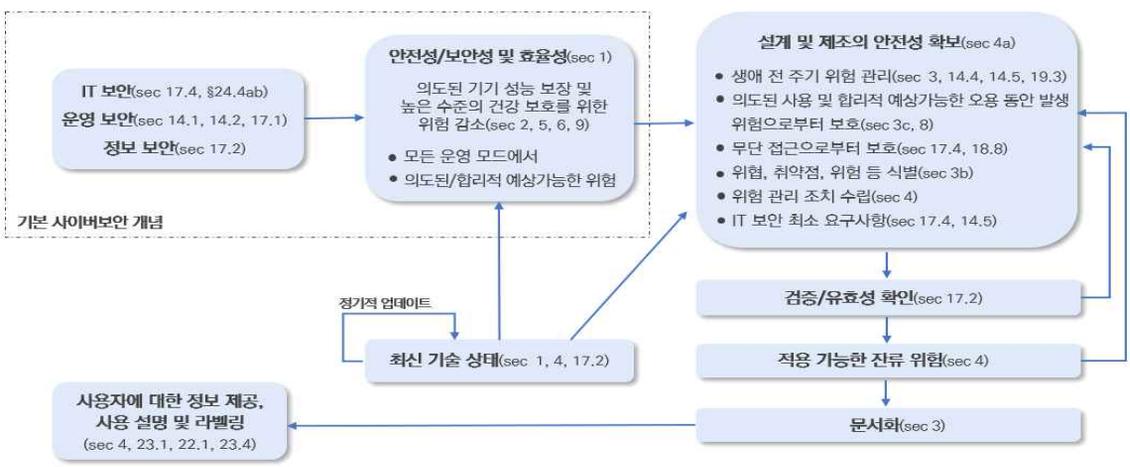
- 이에 따라 의료기기 또는 체외 진단 의료기기는 출시 및 서비스 투입을 위하여 **일반 안전 및 성능 요구사항(부속서 I)**을 **준수**하여야 하며, 동 요구사항에는 온라인 연결 의료기기 증가로 인한 사이버보안 확보의 중요성을 반영하여 **사이버보안 관련 요구사항**(시판 전/후 측면 모두 포함)*이 **포함** **

* 구체적으로, 프로그램 가능한 전자 시스템을 포함하는 기기 및 그 자체로 기기인 소프트웨어 안전·성능 관련 요구사항 해당

** EU 의료기기 조정 그룹[29] 제정「의료기기 사이버보안 가이던스」는 부속서 I 중 사이버보안 관련 요구사항 준수 지침 제시

- 한편, 의료기기 등 제조업자는 부속서 I 의 요구사항 충족 입증을 위한 **적합성 평가 실시** 및 **적합성 선언서 작성, CE마크 부착** 의무 규정(의료기기 규정 제5조, 제10조, 체외진단의료기기 규정 제5조, 제10조)

〈 일반 안전 및 성능 요구사항(부속서 I) 중 사이버보안 관련 요구사항 〉



* Medical Device Coordination Group, MDCG 2019-16 Guidance on Cybersecurity for medical device(2019.12월), 5면 참고

○「사이버복원력법」(Cyber Resilience Act)[30]

• EU 내 디지털 요소가 있는 제품의 보안성 향상과 사이버위협 대응을 위하여 **제품의 전체 생애주기**에 걸친 **사이버보안 규제 프레임워크** 마련을 위한 **「사이버복원력법」**[31] **제정**('24.12.10. 발효, '27.12.11 전부 시행 예정)

27) Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC

28) Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU

29) 의료기기 조정 그룹(Medical Device Coordination Group)은「의료기기 규정」제103조에 근거하여 설립되었으며, 동 규정 제105조 및「체외 진단 의료기기 규정」제99조에 따라 적합성 평가기관의 평가 기여, 동 규정의 조화로운 이행 보장을 위한 지침 개발 기여, 기술 진행 상황의 지속적 모니터링 및 일반 안전 및 성능 요구사항의 수정 필요성 식별 기여, 유럽 시장 감시 프로그램 개발 및 유지 관리 지원 등 업무 수행

30)「의료기기 규정」및「체외 진단 의료기기 규정」의 적용을 받는 의료기기는 동법 적용대상에서 제외되나, 동법은 디지털제품 사이버보안 확보를 위한 별도 규제체계를 마련했다는 점에서 우리나라의「디지털의료제품법」과 일맥상통하는 점이 있는 점을 고려하여 이하에서 동법 주요 내용을 간략하게 소개함

31) Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) NO 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828

- **(적용 대상) 디지털 요소가 있는 제품**으로서 제품의 목적이나 사용 범위에 **기기·네트워크에 대한 직·간접적, 논리적·물리적 데이터 연결**을 **포함**하고 **EU 시장**에 유통·이용될 수 있도록 **공급**된 경우 해당
  - 여기서 디지털 요소가 있는 제품(Product with digital elements)이란 SW·HW 제품과 그 원격 데이터 처리 솔루션을 의미하며, 시장에 별도 출시된 SW·HW 구성요소를 포함
  - **오픈소스 소프트웨어**의 경우 **상업적 활동 과정**에서 배포·이용을 위해 EU 시장에 **공급** 시 **적용 대상 포함**
- **(필수 사이버보안 요구사항)** 디지털 요소가 있는 제품은 **필수 사이버보안 요구사항(부속서 Ⅰ)**을 **충족**한 경우만 **EU 시장 공급** 가능하며(제6조), 제조업자는 제품 출시 전 필수 요구사항 준수 입증을 위한 적합성 평가를 실시하고, 적합성 선언서 작성 및 CE마크 부착 의무(제13조)

〈 필수 사이버보안 요구사항 (부속서 Ⅰ) 〉

구분	주요내용
Part 1. 제품 속성 관련 보안 요구사항	• 적절한 수준의 **사이버보안을 보장**하는 방식으로 **제품 설계·개발·생산** • 악용 가능한 취약점이 없는 상태로 제품 납품 • Secure by default 설정을 갖춘 상태로 시장에 제품 공급 • 보안 업데이트를 통한 취약점 해결 • 인증, 신원확인, 접속 관리 시스템 등 무단 접속으로부터 보호 • 저장, 전송 또는 처리된 데이터의 기밀성 보호 • 승인되지 않은 조작, 수정으로부터 데이터, 프로그램, 구성의 무결성 보호 • 데이터 활용과 관련해 적절하고 관련성이 있는 것으로 제한하여 처리 • 서비스 거부 공격에 대한 복원력, 완화 조치 등 필수 기능의 가용성 보호 • 다른 장치나 네트워크가 제공하는 서비스 가용성에 대한 부정적인 영향 최소화 • 외부 인터페이스를 포함한 공격 표면을 제한하도록 설계·개발·생산 • 악용 완화 매커니즘·기술을 활용해 사고의 영향을 줄이는 설계·개발·생산 • 데이터, 서비스, 기능에 대한 접근 또는 수정을 포함하여 관련 내부 활동을 기록·모니터링하여 보안 관련 정보 제공 • 사용자가 모든 데이터와 설정을 영구적으로 안전하고 쉽게 삭제할 수 있는 기능 제공
Part 2 제조업체의 취약점 관리 관련 요구사항	• 제품의 최상위 종속성을 포함하여 기계로 읽을 수 있는 형식의 **소프트웨어 자재 명세서(SBoM) 작성** 등 제품에 포함된 취약성 및 구성요소 식별, 문서화 • **보안 업데이트**를 제공하는 등 지체없이 취약점을 해결 및 수정 • 제품의 보안에 대한 효과적이고 정기적인 시험과 검토 • 보안 업데이트 시 취약점 설명, 영향받는 제품 정보, 취약점의 영향, 심각도, 취약점 개선에 도움이 되는 정보를 포함해 교정된 취약점에 대한 정보 공개 • **조정된 취약점 공개(CVD)에 대한 정책** 수립 및 시행 • 제품 취약점을 보고하기 위한 연락처 제공 등 제품 및 제3자 구성요소의 잠재적 취약점에 대한 정보를 쉽게 공유하기 위한 조치 • 취약점이 적시에 수정, 완화되도록 보장하기 위해 제품에 대한 업데이트를 안전하게 배포하는 매커니즘 제공 • 보안 문제 해결을 위해 보안 업데이트를 하는 경우 사용자가 취할 수 있는 조치 등 관련 정보를 제공하는 메시지와 함께, 지체없이 무료 배포되도록 보장

- **(제재)** 「사이버복원력법」은 동법 위반 사업자*에 대한 제재 규정(제64조)

※ 필수 요구사항(부속서 Ⅰ) 위반의 경우 1,500만 유로 또는 전 세계 연간 매출액 2.5% 중 높은 금액 부과 가능

4. 시사점

○ 디지털 연결 제품에 대한 사이버보안 확보

- 디지털 전환의 가속화 및 초연결 환경의 도래로 어느 한 제품에 대한 사이버공격은 해당 제품 관련 공급망 및 국가·사회 전체에 광범위한 영향을 미칠 수 있음
  - 이에 미국, EU 등 해외 주요국은 디지털 연결 기능이 있는 제품의 사이버보안 확보를 위해 관련 규제를 강화하고 있으며, '24.12월 발효된 EU 「사이버복원력법」은 '모든' 연결 제품에 대한 사이버보안 기준을 제시하기에 이르렀음
- 「디지털의료제품법」 제정 또한 연결 제품 제조자 등의 사이버보안 의무를 규정하고 있다는 점에서 위의 주요국 동향의 연장선상에 있는 것으로 볼 수 있으며,
  - 특히, 제조자 등에 대한 사이버보안 의무화(위반 시 제재)의 경우 디지털 연결 제품 보안을 대체로 사업자 자율에 맡기고 있는 국내 법체계* 전체로 확대 적용하는 방향을 검토할 필요성이 있음

* 대표적으로, 민간 분야 정보보호 일반법이라고 할 수 있는 정보통신망법은 디지털 연결 기기 보안을 위하여 안전성 확보조치(제45조), 정보통신망연결기기등에 관한 인증(제48조의6)을 규정하고 있으나 권고적 효력을 가지는데 불과함

○ 디지털 기술의 특성을 반영한 전 주기 보안 관리 체계 구축

- 빠르게 변화하는 디지털 기술의 특성을 반영하여 제품 출시 전 사이버보안 요구사항 충족뿐만 아니라 출시 후 지속적인 취약점 관리, 사고 대응 등을 통한 전 주기적 보안 관리 체계 구축 필요
  - 이와 관련하여 「디지털의료제품법」, 미국 「FD&C법」 및 EU 「사이버복원력법」은 SBoM 작성, 출시(시판) 후 보안 업데이트 제공, 조정된 취약점 공개(CVD) 정책 수립 등 지속적 취약점 관리에 관한 사항을 공통적 규정
  - 한편, 「디지털의료제품법」과 같이 제품의 안전 관리를 위한 인·허가 제도를 운영하는 경우 기술 변화가 제품 안전성 변경 등이 제품 출시(인·허가) 후에도 신속하게 반영될 수 있도록 다양한 허가·평가 체계 도입 검토

○ 특별법 제정에 따른 중복 규제 문제에 대비 법률 간 조화 방안 모색

- 「디지털의료제품법」은 디지털 기술과 의료기기가 결합된 특수성을 반영하기 위해 특별법 제정 방식을 선택함에 따라 기존 법률 또는 동일한 디지털 기술을 적용 대상으로 하는 다른 특별법과 중복 규제 문제 발생 가능

※ **(기존 법률과 중복 예)** 동법 하위 지침인 「디지털의료기기 전자적 침해행위 보안지침」(안)의 내용은 정보통신망법상 침해사고 신고·대응 관련 규정(제48조의3~제48조의5)과 중복 가능

※ **(다른 특별법과 중복 예)** 인공지능기술이 적용 의료기기 제조업자등의 경우 동법의 전자적 침해행위 보호 관련 준수사항 등(제13조, 제14조)과 인공지능기본법상 안전성 확보 의무(제32조), 고영향 인공지능사업자 책무(제34조) 등과 중복 가능

- 이를 위해 특별법에 중복 소지가 있는 타 법 내용을 모두 포함하여 규정하는 방안도 있으나 ICT 융합의 확산으로 이와 같은 특별법 제정은 증가할 것으로 예상되는 만큼 관계부처 간 협력체계 구축, 유사 제도 간 적용관계 정립 등 법률 간 조화를 위한 중·장기적인 방안 모색 필요

Reference

▪국회 보건복지위원회, 『디지털의료제품법안 디지털의료제품에 관한 법률안 검토 보고』, 2023.4월

▪식품의약품안전처 보도자료, 디지털의료제품법 국회 본회의 통과, 2023.12.20

▪식품의약품안전처 보도자료, 식약처, 세계 첫 「디지털의료제품법」 본격 시행을 위한 하위 규정 입법예고, 2024.7.31

▪식품의약품안전처 보도자료, 식약처, AI(인공지능)·소프트웨어에 특화된 디지털의료제품 규정 행정예고, 2024.12.17

▪방지호, “의료기기 SBOM 동향”, 제11회 2024 의료기관 정보보호 컨퍼런스 발표자료, 2024. 5. 21

▪한국의료기기안전정보원, 『유럽(CE) 의료기기 MDR 제도 이해 및 대응 전략 보고서』, 2022

▪한국인터넷진흥원, 『2024 해외 사이버보안 입법동향』, 2024.12월

▪한국인터넷진흥원, 『인터넷·정보보호 법제동향』 제175호, 2022.4월

▪Medical Device Coordination Group, 『MDCG 2019-16 Guidance on Cybersecurity for medical device』, 2019.12월

PART Ⅲ

호주, 2024 사이버보안 입법패키지 하위규칙 제정

1. 개요

○ 호주는 2024 사이버보안 입법패키지 통과에 따른 후속조치로 총 6개의 하위규칙 제정

• 호주는 '2023-2030 호주 사이버보안 전략'을 수립('23.11.)하고, 그 일환으로 국제 모범사례에 부합하는 법체계 구축 및 사이버보안 분야 글로벌 리더십 강화를 위한 법제 개선 추진

- 이에, 2024 사이버보안 입법패키지로 불리는 「2024 사이버보안법」, 「2024 주요기반보안 및 기타 법률 개정(대응 강화 및 예방)에 관한 법률」, 「2024 정보서비스 및 기타 법률의 개정(사이버보안)에 관한 법률」 등 3종의 입법*을 추진하여, 최종 승인을 받음('24.11.29.)

* ▲Cyber Security Act 2024 ▲Security of Critical Infrastructure and Other Legislation Amendment(Enhanced Response and Prevention) Act 2024, ▲Intelligence Services and Other Legislation Amendment (Cyber Security) Act 2024

- 이후 입법 후속조치로 법률의 내용을 구체화하는 하위규칙 초안을 공개, 의견수렴('24.12.16 ~ '25.2.14.)을 거쳐 제정 추진

〈 2024 사이버보안법 입법패키지 하위규칙 제정 추진현황 〉

법률	하위규칙	시행일
2024 사이버보안법	• 2025 스마트 기기 보안표준 규칙	제정일 ('25. 2. 27.)로부터 12개월 후
	• 2025 랜섬웨어 보고 규칙 • 2025 사이버사고 검토위원회 규칙	제정일 ('25. 2. 27.)로부터 6개월 후
2024 주요기반보안 및 기타 법률 개정 (대응 강화 및 예방)에 관한 법률	• 2025 주요기반보안(통신 보안 및 위험 관리 프로그램) 규칙 • 2025 주요기반보안(데이터 저장 시스템) 규칙 • 2025 주요기반보안(주요 통신자산)에 관한 규칙	제정일 ('25. 3. 1.)로부터 12개월 후

2. 「2024 사이버보안법」 하위규칙 주요내용

2025 스마트 기기 보안표준 규칙

- 「2024 사이버보안법」은 호주 정부가 인터넷에 직·간접적으로 연결 가능한 스마트 기기의 보안표준을 수립하고, 제조·공급업체로 하여금 보안표준을 준수한 스마트 기기를 제조·공급하도록 의무를 부과함
  - 또한, 제조업체·공급업체는 컴플라이언스 설명서와 함께 제품을 제조·공급해야 하고, 컴플라이언스 설명서 사본을 보관해야 함
- 본 규칙은 제조·공급업체가 준수해야 할 스마트 기기 보안표준 및 컴플라이언스 설명서의 구체적인 내용을 정함
- **(정의)** 본 규칙은 스마트 기기 보안표준에 사용되는 용어를 다음과 같이 정의함

〈 스마트 기기 보안표준 규칙 정의 조항 〉

구분	주요내용
소비자	• 상품 및 서비스를 취득한 것으로 간주되는 경우(반대의사가 있는 경우는 제외) 소비자로 분류
소비자용 스마트 기기	• 개인, 가정, 소비용으로 사용하거나 사용할 가능성이 있는 관련연결가능제품을 소비자용 스마트 기기로 분류 ※ 단, 데스크톱, 노트북, 태블릿, 스마트폰, 치료용품, 자동차·자동차 부품은 제품에서 제외
API* 키 * Application Prgramming Interface Key	• 특정 사용자, 제품 또는 애플리케이션을 식별하고 인증하여 애플리케이션 프로그래밍 인터페이스에 접근하는 경우 사용되는 문자열
암호화 키	• 데이터를 암호화하고 해독하는 데 사용되는 데이터
비밀 키	• 데이터를 암호화하거나 승인 받은 사람 또는 권한을 받은 사람만 알도록 의도된 암호화 키
키 해싱 알고리즘	• 데이터 입력과 비밀 키를 사용하여 데이터와 비밀 키에 대한 지식이 없으면 추측·재현할 수 없는 값을 생성하는 알고리즘
보안 업데이트	• 제품의 보안을 보호하거나 강화하는 소프트웨어 업데이트를 말하는 것으로, 제조업체에서 발견하거나 보안문제점 보고를 받아 알게 된 보안문제점을 해결하기 위한 소프트웨어를 포함

- **(소비자용 스마트 기기 보안표준)** 본 규칙은 제조업체가 준수해야 하는 소비자용 스마트 기기 보안표준으로 ▲비밀번호, ▲보안문제점 보고방법, ▲보안 업데이트 지원기간에 관한 사항을 규정함
  - **(비밀번호)** 제조업체는 스마트 기기의 보안을 위해 사용자가 직접 비밀번호를 입력하여 제품마다 각기 다르도록 해야 하고, 공개적으로 사용가능한 정보 또는 고유 제품번호 등을 비밀번호로 사용하지 못하도록 설정해야 함
    ※ 암호화 키, API키, 또는 통신 프로토콜 페어링에 사용되는 개인 식별번호는 비밀번호에 미포함
  - **(보안문제점 보고방법)** 제조업체는 제품의 하드웨어·소프트웨어 등의 보안문제점을 다음과 같은 방법으로 보고받아 처리해야 함
    ※ ▲한 곳 이상의 보고 창구 마련 ▲보고 한 자에 대해 접수 확인서 제공 ▲보안문제점 업데이트 시 정보 게시 ▲게시된 업데이트 정보가 접근 가능하고 명확·투명하며 누구나 이용할 수 있도록 명시

- **(보안 업데이트 지원기간)** 제조업체는 보안 업데이트가 가능한 대상*의 지원기간을 명시하고 기간을 단축해서는 안되며, 기간을 연장하는 경우에는 가능한 한 빠르게 업데이트를 해야 함

  * ▲제품 하드웨어 ▲사전 설치된 소프트웨어 ▲제조업체가 개발하거나 제조업체를 대신하여 개발된 소프트웨어

• **(컴플라이언스 설명서)** 법률에서 스마트 기기 제조·공급업체가 제품과 컴플라이언스 설명서를 함께 제공하고 설명서를 보관하도록 규정함에 따라, 제조·공급업체는 설명서에 다음 사항을 포함하여야 함

〈컴플라이언스 설명서에 포함해야 할 사항〉

• 제품 유형 및 식별자 • 제품 제조업체의 공표문 – 제조업체가 직접 설명서 작성 – 제품의 보안표준 요구사항을 준수	• 제품 제조업체의 이름 및 주소 ※ 제조업체의 대리인으로 대체 가능 • 제조업체 서명자의 서명, 이름, 역할 • 컴플라이언스 설명서의 발행 장소 및 날짜

2025 랜섬웨어 보고 규칙

• 「2024 사이버보안법」은 랜섬웨어 공격을 받아 그 대금을 직접 지불한 사업체 등 보고 의무 대상에게 72시간 이내 지정된 연방기관에 랜섬웨어 대금 지불 보고서를 제출하도록 의무를 부과함

• 본 규칙은 법률상 보고 의무가 있는 대상을 구체화하고, 해당 사업체가 랜섬웨어 대금 지불 보고서를 제출하는 경우, 포함해야 할 보고 내용을 명시함

– **(보고 의무 대상)** ①랜섬웨어 대금을 직접 지불한 사업체, ②매출액이 300만 달러를 초과한 사업체, ③주요기반운영자, 및 ④다른 사업체가 지불한 사실을 인지한 사업체

– **(보고서 내용)** 보고 의무 대상은 랜섬웨어 대금 지불 보고서에 다음 사항을 포함하여 보고해야 함

〈 랜섬웨어 대금 지불 보고서 포함 내용 〉

구분	주요내용
사업체 정보	• 보고 대상 사업체의 연락처 및 사업 세부 정보(사업자번호 및 주소 포함) • 다른 사업체 연락처 및 사업 세부 정보(사업자번호 및 주소 포함)
사이버보안 사고의 내용과 미치는 영향	• 사고의 발생 시점 또는 발생한 것으로 추정되는 시점 • 보고 대상 사업체가 사고를 인지한 시점 • 보고 대상 사업체의 고객/기반시설에 미치는 영향 • 랜섬웨어 또는 기타 멀웨어의 변종(있는 경우) 정보 • 보고 대상 사업체의 시스템 악용된 취약점 정보 • 연방 기관 또는 국가 기관에 도움이 될 수 있는 사이버보안 사고에 대응·완화 또는 해결에 관한 정보
협박 주체	• 협박 주체가 요구한 금액 및 방법 • 협박 주체와 커뮤니케이션한 내용 – 협박 주체와 해당 사업체 간 소통수단 및 시기 – 해당 소통수단에 대한 요약 – 지불 또는 요구와 관련된 수행된 선지불 협상에 대한 요약
대금 지불	• 랜섬웨어 대금 지불 금액 및 방법

2025 사이버사고 검토위원회 규칙

- 「2024 사이버보안법」은 사이버보안 사고의 체계적 검토를 통해 향후 유사한 사고를 예방·탐지·대응하는 등 개선사항을 도출하기 위하여, 독립적 지위를 가지는 사이버사고 검토위원회를 설립하도록 함
  - 사이버사고 검토위원회는 위원장 및 상임위원(2~6인)으로 구성
  - 사회·경제적 안정성, 국방, 국가안보에 심각한 위해가 있거나 새로운 수법·기술이 포함되는 사이버보안 사고 등을 검토하고 예방·대응 방안을 마련하는 기능을 수행하며, 이에 관한 완전한 재량권을 보유
- 본 규칙은 사이버사고 검토위원회(이하 '위원회')의 원활한 운영을 위하여, 사고 검토의 수행 방법·절차, 상임위원 및 전문가 패널의 임명·폐지에 관한 사항을 규정함
- **(위원회의 사고 검토)** 위원회는 사이버사고 발생 또는, 내무부 장관 및 국가사이버보안조정관 등 법률에서 정하는 자로부터 서면의뢰를 받는 경우, 사고 검토 수행여부를 결정하고 가능한 빠른 시간 내에 이를 공고하여야 함
  - 사고 검토 여부를 결정할 때에는 해당 사고의 심각성 및 영향의 규모를 고려하여 우선순위를 정하여야 함
  - 또한, 위원회가 사고 검토를 상임위원 및 전문가 패널에 위임할 수 있으며, 이 경우 위임사항에는 ▲검토를 수행하는 상임위원의 수, ▲전문가 패널의 수/자격요건, ▲검토 수행에 필요최소한의 보안 허가 수준을 명시하도록 함
    ※ 위원회는 내무부 장관의 승인을 받아 사고 검토 위임사항을 변경할 수 있음

〈 사고 검토 공고에 포함해야 할 사항 〉

• 사고 검토를 수행할 상임위원의 수	• 해당 사고가 위원회의 사고 검토 대상에 해당하는지 여부
• 사고 검토를 돕기 위해 임명될 전문가 패널의 수	• 사고 검토 수행을 위해 제안된 기간
• 사고 검토의 대상이 되는 사이버보안 사고의 세부정보	• 위원회가 공고하기에 적절하다고 판단하는 기타 정보

- **(상임위원)** 동 규칙은 법률에서 내무부 장관이 서면으로 임명하도록 규정하는 '상임위원'에 관한 임명 자격요건과 해지 사유를 명시하여 규정함

〈 상임위원 임명·해지에 관한 요건 〉

구분	주요내용
임명 자격	• 호주/연방정부에서 기밀 정보에 접근할 수 있는 보안등급 허가를 받은 자 • 사이버보안/정보보호/법학 분야의 학사 학위를 받거나 유사 수준의 학력, 또는 해당 분야의 상당 경력 보유자 • 연방, 또는 주 정부에서 고위직 직원으로 근무하는 자 • 감사, 검토 절차, 행정, 재무, 등의 상당한 경력 보유자 • 사고 관리 및 위기 대응 관련 상당한 경험자 • 주요기반에 관한 상당한 경험자 • 관련 분야에서 상당한 학력 및 지식의 소유자
임명 해지	• 위원이 잘못된 행동을 하는 경우 • 위원이 신체적·정신적 능력 상실로 인해 직무를 수행할 수 없는 경우 • 위원이 파산한 경우 • 위원이 회의에 연속 3회 불참하는 경우 • 위원이 적절한 직무 수행과 상충되거나 그러할 가능성이 있는 업무를 하는 경우 • 장관이 위원 임명 자격요건에 해당하지 않는다고 판단하는 경우

• **(전문가 패널)** 위원장은 동 법에서 사고 검토를 지원하는 역할을 수행하는 '전문가 패널'을 파트타임의 형태로 위촉할 수 있으며, 위촉 기간은 4년을 초과할 수 없음

- 또한, 위원장은 전문가 패널 중에서 사고 검토를 위한 패널을 임명할 수 있음
- 패널로 위촉 전에는 이해관계 및 보유자산이 직무 수행과 충돌 및 우려가 있는 경우 서면으로 통지하고, 위촉 시에는 위원회에서 심의·예정중인 사안의 이해관계를 공개하도록 함

※ 전문가 패널의 위촉·해지 요건은 상임위원의 임명·해지 요건과 유사함

3. 「2024 주요기반보안 및 기타 법률의 개정(대응 강화 및 예방)에 관한 법률」 하위규칙 주요내용

2025 주요기반보안(통신보안 및 위험 관리 프로그램) 규칙

• 「2024 주요기반보안 및 기타 법률의 개정(대응 강화 및 예방)에 관한 법률」은 「2018 주요기반보안법[32]」과 「1997 통신법[33]」을 개정하여 주요기반에 중대한 위험이 있는 경우, 주요기반 자산에 대한 책임 조직이 주요기반 위험 관리 프로그램을 강화하도록 문서화된 지침을 제공

• 본 규칙은 법률 개정의 후속조치로써 주요 통신자산 보호에 관한 보안 규정을 한층 강화하고, 위험을 식별하고 세분화하는 등 강화된 위험 관리를 위한 의무사항 및 중대한 위험 요건 등을 규정하고 있음

• **(정의)** 동 규칙에서는 위험 식별·세분화를 위한 용어를 다음과 같이 정의함

〈 주요기반보안 위험 관리 프로그램에 관한 용어 정의 〉

구분	주요내용
관련 통신 서비스 제공업체 자산	• 20,000건 이상 활성화된 광대역, 유선 전화, 음성 서비스 및 공공 모바일 통신서비스의 자산 및 연방에 공급되는 통신서비스 자산
주요 통신자산	• 관련 통신서비스 제공업체가 소유, 운영 및 제공하는 통신 시설 또는 네트워크
주요 공급업체	• 제품 또는 서비스 제공이 책임 조직의 주요 통신자산 보안에 중대한 영향을 미치는 공급업체
주요기반 자산 (Critical Infrastructure Asset)	• 법률에서는 주요기반 자산을 통신분야, 금융분야, 에너지분야 등으로 분류하고 있으나, 본 규칙은 통신분야의 주요 통신자산, 관련 통신 서비스 제공업체 자산 및 일정 기준이상의 데이터 저장 시스템으로 정의
책임 조직	• 하나 또는 이상의 주요기반 자산(이하 CI 자산)에 대한 책임이 있는 조직
사이버 및 정보보안 위험	• CI 자산 및 컴퓨터·정보 시스템에 부적절하게 접근하거나 오용하는 경우, 컴퓨터 시스템을 사용하여 관련 무단 접근 권한을 획득 하는 경우
직원 위험	• 핵심 근로자가 CI 자산의 적절한 기능을 손상시키거나 심각한 손상을 입히는 경우
핵심 근로자	• 책임 조직의 직원 및 하청업체, 또는 CI 자산의 기능을 방해하거나 손상을 초래하는 자
물리적 보안 위험	• CI 자산에 무단 제어 및 접근을 통해 기능을 손상시키거나 자산에 해를 입히는 경우
자연 재해	• 화재, 홍수, 폭풍, 지진, 쓰나미, 우주 기상 문제 또는 생물학적 위험(전염병 포함)의 경우

32) Security of Critical Infrastructure Act 2018(SoCI Act)
33) Telecommunication Act 1997

• **(주요기반보안 위험 관리 프로그램)** 본 규칙은 법률에서 명시하는 주요기반보안 위험 관리 프로그램(이하 프로그램)의 강화를 위하여 책임 조직의 의무사항 및 위험에 관한 내용을 규정하고 있음

- 본 규칙은 모든 위험 관리를 위해 책임 조직이 법률에 따라 프로그램을 적용하고, CI 자산에 관한 운영 현황 식별, 중대한 위험 식별 및 최소화·제거 등을 위한 프로그램을 수립·유지·최신화하도록 함

〈 주요기반보안에 관한 중대한 위험 요건 〉

• 해당 CI자산 기능에 대한 필수 운영 또는 정보통신기술의 방해	• 관리할 수 없는 기간 동안 CI 자산의 기능이 느려지거나 중단된 경우
• 주요 공급업체, 작업자, 또는 관리형 서비스 제공업체의 CI자산의 보안 및 기능을 손상시키는 행위(Ex.백도어 파일 등)	• 사회·경제적 안정성 또는 국가 안보 침해로 CI자산의 기능 손상
• 기업의 중요데이터를 보관하는 저장 시스템의 가용성, 무결성, 신뢰성 또는 기밀성에 영향을 미치는 경우	• 통신의 손상, 도난, 또는 조작
	• CI 자산의 운영 제어 또는 모니터링 시스템의 원격 접근
	• CI 자산의 중요 구성요소의 접근권한 상실 또는 고의적 조작

• **(사이버 및 정보보안 위험 관리)** 본 규칙은 책임 조직이 사이버 및 정보보안 위험을 최소화·제거하도록 하고, CI 자산에 대한 사이버 및 정보보안 위험의 영향을 완화하도록 함

- 모든 책임 조직은 사이버보안 성숙도 프레임 워크 1단계를 충족해야 하며, 주요 통신자산 및 관련 통신서비스 제공업체의 자산의 책임 조직은 프레임 워크 2단계를 충족해야 함

※ 사이버보안 성숙도 프레임워크 1단계: 단순 접근통제 수준 / 2단계: 통제 우회 및 탐지 회피 예의 주시

• **(직원 위험 관리)** 책임 조직이 핵심 근로자를 식별하고, 핵심 근로자에 부여하는 접근권한의 적절성 판단 및 중대한 위험을 최소화·제거하기 위해 프로그램을 수립·유지하도록 함

- 법률에서 핵심 근로자에 대한 신원조회를 허용하는 경우, 범죄 경력 그리고, 전자 및 대면방식의 신원확인을 포함한 신원조회를 통해 핵심 근로자의 접근권한에 대한 적절성을 판단해야 함

• **(공급망 위험 관리)** 책임 조직이 공급망에 대한 중대한 위험을 최소화·제거 및 공급망 위험으로 CI 자산에 미치는 영향을 완화하기 위해 프로그램을 수립·유지하도록 함

- 공급망 위험은 ▲공급망의 무단 접근 및 악용, ▲공급망 제공자의 권한 오용 ▲공급망 문제로 인한 자산 손실 ▲공급망 내 장비, 서비스 등의 위협 ▲주요 공급업체에서 발생하는 위험 등으로 분류

• **(자연 재해 및 물리적 보안 위험 관리)** 책임 조직이 자연재해 및 물리적 보안 위험 관리를 위하여 다음과 같은 내용을 포함하여 프로그램을 수립·유지하도록 함

- ▲CI 자산의 물리적 구성요소 식별, ▲중요한 물리적 구성요소의 무단 접근에 대응방안 ▲중대한 물리적 보안 위험 및 자연재해의 최소화·제거 ▲동반자를 동행한 방문자 또는 핵심 근로자에게만 접근 제한

2025 주요기반보안(데이터 저장 시스템) 규칙

• 「2024 주요기반보안 및 기타 법률의 개정(대응 강화 및 예방)에 관한 법률」에서는 기업의 핵심 데이터를 저장하거나 처리하는 '데이터 저장 시스템'의 기준을 제시하고, 이를 충족한 경우 주요기반 자산으로 간주

• **(데이터 저장 시스템)** 본 규칙은 법률에서 정하는 요건에 해당하는 데이터 저장 시스템을 주요기반 자산으로 분류하여 이에 대한 책임이 있는 조직이 위험 관리 프로그램을 수립·유지하도록 함

〈 데이터 저장 시스템 요건 〉

구분	정의
데이터 저장 시스템 (Data storage systems)	• 주요기반 자산(assets)인 경우, 다음의 요건을 모두 충족할 시 데이터 저장 시스템에 해당 – 주요기반 자산의 책임 조직이 소유하고 있는 경우 또는 직접 시스템을 운영하는 경우 – 데이터 저장 시스템이 주요기반 자산과 연결되어 사용되거나 사용될 예정인 경우 – 비즈니스 핵심(critical)데이터가 데이터 저장 시스템에 의해 저장, 처리되는 경우 – 데이터 저장 시스템에 영향을 미칠 수 있는 위험 발생이 중대한 위험으로 이어질 수 있는 경우 – 주요기반 자산에 관련 영향을 줄 수 있는 위험 발생이 중대한 위험으로 이어질 수 있는 경우

2025 주요기반보안(주요 통신자산) 규칙

• 「2024 주요기반보안 및 기타 법률의 개정(대응 강화 및 예방)에 관한 법률」은 주요 통신자산의 책임 조직으로 하여금 합리적으로 실행 가능한 범위 내에서 해당 자산을 보호하도록 규정하고 있음

– 통신서비스 또는 통신 시스템에 대한 변경 또는 변경의 제안이 책임 조직의 역량에 중대한 악영향을 미칠 가능성이 있는 경우, 책임 조직은 내무부 장관에게 해당 서비스·시스템 변경 등 관련 사항을 통지하도록 규정함

• **(주요 통신자산의 보호)** 본 규칙은 법률에서 주요 통신자산이 주요기반 자산과 같다고 명시함에 따라, 주요 통신자산에 대한 책임 조직에게도 주요기반 위험 관리 프로그램 규칙 상 동일한 의무를 준수하도록 함

〈 주요 통신자산에 관한 정의 〉

구분	정의
주요 통신자산	• 이동 통신사가 소유 또는 운영하는 주요 통신자산 또는, 통신서비스 제공업체의 자산
통신서비스 제공업체 자산	• 20,000건 이상 활성화된 광대역, 유선 전화, 음성 서비스 및 공공 통신서비스의 자산과 연방에 공급되는 통신서비스 자산
주요기반 자산	• 이동 통신사가 소유 또는 운영하는 주요 통신자산 또는, 통신서비스 제공업체의 자산, 일정 기준에 해당하는 데이터 저장 시스템

4. 전망 및 시사점

○ 호주는 2024 사이버보안 입법패키지와 그 후속 하위규칙(6종) 정비를 통해, 사이버보안 분야에서 글로벌 리더가 되기 위한 법제도적 기반 마련

• 호주는 최근 몇 년간 정부와 민간 주요 네트워크에 대한 사이버공격으로 정보유출 등 피해가 증가함에 따라, 국제 모범사례에 비추어 자국의 사이버보안 입법을 재검토하고 체계적 개선·정비를 추진

- 최근 중요하게 부각되고 있는 ▲스마트기기 보안 강화, ▲랜섬웨어 지불 및 사고의 보고·검토 체계 확립, ▲공급망 보안을 비롯한 주요기반의 위험관리 강화 등 최근 글로벌 사이버보안 입법·정책과 흐름을 같이하는 사이버보안 법제를 마련한 것에 의의가 있음

  ※ EU 「사이버복원력법」(CRA) 및 「NIS2 지침」, 영국 「제품 보안 및 통신인프라법」(PSTI), 미국 「주요기반 사이버사고 보고법」(CIRCIA), 싱가포르 「개정 사이버보안법 2024」 등[34]

• 호주 정부는 이번 법령 정비를 통해, 정부와 기업 간에 사이버 공격 대응에 필요한 정보공유가 원활하고 시의적절하게 이루어질 것이며, 주요기반에 대한 위험관리 강화로 보안 수준을 한층 더 높일 것으로 전망함

- 반면, 호주정보산업협회(AIIA[35])는 주요기반 자산에 영향을 미치는 모든 사고에 정부 개입을 확대하는 것에 우려를 표했으며, 이해관계자의 충분한 의견수렴 없이 조급하게 입법을 추진한다는 비판도 있었음

○ 스마트 기기의 보안취약점 개선, 정부의 사이버사고 등 정보의 수집·검토 역량 제고, 주요 인프라의 공급망 보안 위험관리에 관한 사항은 국내 정보보호 법제에도 시사하는 바가 큼

• 우리나라는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'), 「정보통신기반 보호법」(이하 '기반보호법') 등을 통해 ▲정보통신망연결기기등 보안, ▲침해사고 신고 및 대응, ▲주요기반 보호 등을 규율하고 있으며, 호주를 비롯한 최근의 글로벌 입법 대응방향을 참고하여 향후 개선점을 모색해 볼 필요가 있음

- **(스마트기기 보안)** '정보통신망연결기기등'의 정보보호에 관한 인증제도(정보통신망법)를 통해 기업의 자율적인 보안을 촉진·유도하고 있으나, 기기의 보안취약점을 찾아내서 지속적으로 개선할 수 있는 프로세스(취약점 신고 접수창구 운영, 신고받은 취약점의 개선조치 및 업데이트 제공 등) 시행, 소비자에게 보안에 관한 정보 제공을 확대하는 방안(인증 라벨제 등) 등 고려 필요

- **(사고 신고 및 검토)** 정보통신망법과 기반보호법 등에서 전자적 침해행위로 인한 사고를 신고·통지받아 정부가 사고 분석·대응을 지원하는 체계를 갖추고 있으나, 랜섬웨어나 중요 사이버사고에 대한 정보를 수집·분석하고 체계적 검토를 통해 향후 유사한 사고 예방·탐지 및 대응을 위한 정부의 조치 역량을 강화할 수 있는 제도적 방안도 보완 필요

- **(주요기반보안)** 호주의 주요기반 위험관리 프로그램과 같이 주요정보통신기반시설의 보호계획, 보호지침, 보호대책 및 이행여부 확인, 취약점 분석·평가 등의 제도를 반영·강화하여 공급망 보안의 위험관리를 개선하는 방안 검토 필요

34) 자세한 내용은 '2024 해외 사이버보안 입법동향' (한국인터넷진흥원, 2024.12.) 참고
35) Australia Information Industry Association, 호주의 기술산업을 대표하는 협회

Reference

▪https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/cyber-security-act

▪https://www.cisc.gov.au/legislation-regulation-and-compliance/cyber-security-legislative-reforms

▪https://www.arnnet.com.au/article/3612357/cyber-security-act-passes-parliament_html

▪https://www.csoonline.com/article/3612378/australias-first-cyber-security-act-passes-both-house.html

Ⅳ PART 일본「사이버 대응역량 강화법안」주요내용 및 시사점

1. 개요

○ 일본은 사이버안보 역량을 미국, 유럽 등 주요국 수준 이상으로 강화하기 위한 법제도 정비 추진

- 일본 정부는 **「국가안전보장전략」**('22.12.16 각의결정)을 통해 자국의 **사이버안보 역량을 미국, 유럽 등 주요국 수준 이상으로 강화시키기 위한 4가지 목표**를 설정 ('22.12.16.)
  - ① 사이버공격에 대한 민관협력 강화, ② 통신정보를 활용한 사이버위협 탐지, ③ 공격자의 서버침입 무해화, ④ 사이버안전보장 분야의 일원화된 정책 종합·조정을 위한 조직 신설

〈 국가안전보장전략 中 일부내용〉

사이버공간의 안전하고 안정적인 이용, 특히 국가 및 중요 인프라 등의 안전 등을 확보하기 위하여, **사이버안전보장 분야의 대응능력을 미국, 유럽 등 주요국 이상으로 강화**시킨다.

…(중략)…

무력 공격은 아니지만 국가 및 중요 인프라 등에 대한 안보상 우려를 야기하는 중대한 사이버공격이 예상되는 경우 이를 사전에 제거하고, 이러한 사이버공격이 발생할 시 피해 확산을 방지하기 위해 능동적 사이버 방어를 도입한다. 이를 위해 사이버안전보장 분야의 정보수집·분석 능력을 강화하는 한편, 능동적 사이버 방어를 실시하기 위한 체제를 정비하고, 다음 (가)부터 (다)까지를 포함하여 필요한 조치의 실현을 위한 검토를 추진한다.

(가) 중요 인프라 분야를 포함하여 민간사업자 등이 사이버공격을 받았을 경우 **정부에 대한 정보공유와 민간사업자 등에 대한 대응, 지원 등의 노력**을 추진한다.
(나) 국내 통신서비스사업자가 제공하는 통신정보를 활용하여 **공격자의 악용이 의심되는 서버 등을 탐지**하기 위해 **필요한 조치**를 추진한다.
(다) 국가, 중요 인프라 등에 대한 안보상 우려를 야기하는 중대한 사이버공격에 대해 가능한 **공격자의 서버 등에 대한 침입을 사전에 차단하고 무해화할 수 있도록 정부에 필요한 권한**이 부여되도록 한다.

능동적 사이버 방어를 포함한 이러한 노력을 실현하고 촉진하기 위해 내각 사이버보안센터(NISC)를 발전적으로 개편하고, **사이버안전보장 분야의 정책을 일원적으로 종합 조정하는 새로운 조직을 설치**한다. 그리고 이러한 사이버안전보장 분야에서의 새로운 노력을 실현하기 위해 법제도 정비, 운용을 강화한다.

- 상기 목표를 실현하기 위하여, 내각산하 신설기구인('23.3.31.) '사이버안전보장 체제정비 준비실(サイバー安全保障体制整備準備室)'은 전문가 자문단을 통해 법제도 정비 검토 및 의견수렴 진행 ('24.11.29.)
  - 전문가 자문단은 ▲민관 양방향 정보공유 촉진, ▲사이버공격 대응을 위한 통신정보 활용 검토, ▲경찰 및 자위대의 접근 무해화 조치 권한 구축, ▲조직 개편 등을 제언

• 내각은 자문단의 제언을 바탕으로 **「중요 전자계산기 부정행위로 인한 피해방지 법안(신법)*」** 및 **「동법 시행에 따른 관계법령 정비법안(정비법)**」을 마련**하고 의회(중의원) 제출 ('25.2.7.)

* 重要電子計算機に対する不正な行為による被害の防止に関する法律(신법)

** 重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律(정비법)

• **신법**은 주요기반 사업자와 정부 간 민관협력 강화, 사이버공격 실태파악을 위한 통신정보 이용에 관하여 규정하고 **정비법**은 경찰 및 자위대의 사이버공격 무해화 조치, 사이버안보 거버넌스 정비 등을 규정

〈 법률안 개요 〉

신법 (「중요 전자계산기 부정행위로 인한 피해방지 법안」)

①민관협력 강화

- 특별 사회기반사업자의 특정 전자계산기 도입신고(제2장)
- 특별 사회기반사업자의 특정 침해사건 등 보고 (제2장)
- 정보공유 및 대책 논의를 위한 협의회 설치(제9장)
- 특정 중요 전자계산기의 취약점 대응강화(제42조)
- 벌칙 등(제12장)

②통신정보 이용

- 특별 사회기반사업자의 동의에 따른 통신정보 취득(제3장)
- 동의없는 통신정보 취득 (제4장·제6장)
- 자동화된 기계적 정보 선별 (제5장·제7장)
- 취득한 통신정보의 엄격한 취급(제23조)
- 독립기관의 사전승인 및 지속적 검사(제10장)

↳ **분석·취약점 정보 등의 제공**(제8장) ↲

정비법 (「동법 시행에 따른 관계법령 정비법안」)

③접근 무해화 조치

- **「경찰관직무집행법」 개정**
  - 심각한 피해를 방지하기 위한 경찰의 무해화 조치
  - 독립기관 및 경찰청장 등의 사전승인
- **「자위대법」 개정**
  - 내각총리대신 명령에 의한 자위대의 통신보호조치
  - 주일미군이 사용하는 컨트롤 타워 전자계산기 등의 보호

④조직 및 체제정비

- **「사이버보안기본법」 개정**
  - 사이버보안전략본부 개편·기능강화
- **「내각법」 개정**
  - 내각 사이버보안 담당관 신설
- **「내각부 설치법」 개정**
  - 내각부 소관사무에 통신정보 이용 등 추가

2. 「중요 전자계산기 부정행위로 인한 피해방지 법안」 주요내용

• 「중요 전자계산기 부정행위로 인한 피해방지 법안(신법)」은 **총 12장(章) 86조(條)로 구성**

〈 법률안의 구성 〉

구분	주요내용
제1장	• 총칙 (제1조~제3조)
제2장	• 특별 사회기반사업자의 특정 침해사고 등의 보고 등 (제4조~제10조)
제3장	• 당사자 협약 (제11조~제16조)
제4장	• 외외(外外) 통신목적 전송조치 (제17조~제20조)
제5장	• 당사자 협약 또는 외외(外外) 통신목적 전송조치를 통해 취득한 통신정보의 취급 (제21조~제31조)
제6장	• 특정 외내(外內) 통신목적 전송조치 및 특정 내외(內外) 통신목적 전송조치 (제32조, 제33조)
제7장	• 특정 외내(外內) 및 특정 내외(內外) 통신목적 전송조치를 통해 취득한 통신정보의 취급 (제34조~제36조)
제8장	• 종합정리 분석정보 등의 제공 (제37조)
제9장	• 협의회 (제45조)
제10장	• 제1절 사이버통신정보감리위원회 설치 등 (제46조) • 제2절 검사 등 (제63조)
제11장	• 기타 (제71조~제78조)
제12장	• 벌칙 (제79조~제86조)

특별 사회기반사업자에게 특정 중요 전자계산기의 도입·변경 시 신고 및 침해사건 보고 의무 부과

• **(특정 중요 전자계산기 도입·변경 신고)** 「경제안전보장추진법」에 따른 **특별 사회기반사업자**는 **특정 중요 전자계산기**를 **도입·변경**하는 경우 **제품명·제조업체명 등**을 해당 사업의 소관대신에게 **신고**하여야 하며, 소관대신은 이를 지체없이 내각총리대신에 통지하여야 함

용어	정의
특별 사회기반사업자	• 「경제안전보장추진법」에 따른 특정 사회기반사업자* 중 특정 중요 전자계산기를 사용하는 자 ※ 전기, 가스, 석유, 수도, 철도, 화물자동차 운송, 외항운송, 항공, 공항, 통신, 방송, 우편, 금융, 신용카드, 항만의 215개 사업자
특정 중요 전자계산기	• 「경제안전보장추진법」(2022)에 따른 **특정 사회기반사업자**가 사용하는 전자계산기 중 **사이버보안 피해를 입을 경우** 같은 법 제1항에서 규정한 **특정 중요설비의 기능이 정지 또는 저하될 우려가 있는 것**으로서 정령으로 정하는 것 (해당 특정 중요설비의 일부를 구성하는 경우 포함)

• **(특정 침해사건 등의 보고) 특별 사회기반사업자**는 중요 전자계산기에 대한 **특정 부정행위***로 사이버보안 **피해를 입은 사건(특정 침해사건)** 또는 그 **원인**이 될 수 있는 **사건을 인지한 경우**, 사고 정보 및 원인 정보에 관한 사항을 소관대신 및 내각총리대신에 **보고**하여야 함

* **특정 부정행위** : 다음 각 호의 어느 하나에 해당하는 행위
- 형법 제168조의2(부정명령전자기록 작성 등) 제2항의 죄에 해당하는 행위
- 부정액세스행위 금지법 제2조제4항에 따른 부정액세스행위
- 형법 제2편 제35장의 죄에 해당하는 행위로서 전자계산기의 사이버보안을 해치는 행위로 인해 발생하는 행위(전자계산기에 연결된 전기통신회선의 기능 장애를 가하여 발생하는 행위 포함)

• **(신고·보고의무 이행을 위한 정부의 조치)** 소관대신은 특별 사회기반사업자의 의무 이행을 위해 ▲보고 또는 자료제출 요구, ▲이행·시정 명령, ▲지도·자문 가능

※ 소관대신의 명령 위반(200만엔 이하 벌금), 보고 또는 자료제출 요구 불응 등(30만엔 이하 벌금)

• **(신고·보고받은 정보의 안전관리)** 소관대신, 내각총리대신은 신고·보고받은 정보의 누설, 멸실, 훼손 방지 및 안전관리를 위한 조치를 해야 함

※ 해당 정보의 취급사무 종사자는 알게 된 정보에 관한 비밀 누설·도용 금지 → 위반 시 형사처벌(2년 이하의 구금형 또는 100만엔 이하의 벌금)

특정 중요 전자계산기의 취약점 개선을 위한 조치 강화

• **(취약점 정보의 제공 및 대응)** 전자계산기등 공급사업의 소관대신은 특정 중요 전자계산기의 보안취약점을 알게 된 경우, 해당 전자계산기의 공급자에게 취약점 정보 및 대응방법 등을 공표 등의 방법으로 알리고, 필요한 조치를 요청하거나 보고 또는 자료제출 요구 가능 (위반시 제재규정 없음)

※ 내각총리대신 또는 특별 사회기반사업 소관대신도 공급자에게 조치 요청을 하거나, 전자계산기 공급사업 소관대신에게 의견을 개진할 수 있음

○ 사이버공격 피해방지를 위한 '정보공유 및 대책 협의회' 설립

- 내각총리대신은 사이버공격으로 인한 피해방지를 위하여 관계행정기관장 등으로 구성된 '정보공유 및 대책 협의회'를 설치

  ※ (구성) 내각총리대신, 관계행정기관장으로 구성되고 내각총리대신이 필요하다고 인정하는 경우 동의를 얻어 중요 전자계산기 사용자, 전자계산기 공급자 등을 구성원으로 추가 가능

- 협의회는 비밀유지 의무가 적용되는 피해방지정보*를 공유하고, 이를 통해 피해방지 대책, 피해방지정보의 적정한 관리조치 등 협의

  * 피해방지정보 : 제공용 종합정리분석정보** 및 기타 정보(선별후통신정보***를 포함한 것은 제외)

  ** 제공용 종합정리분석정보 : 종합정리분석정보로서 선별 후 통신정보를 포함하지 않는 것

  *** 선별 후 통신정보 : 내각총리대신이 취득한 통신정보 중에서 기계적 정보만을 선별하여 기록하는 조치(자동선별) 이후의 통신정보

○ 정부가 사이버공격 실태를 파악하기 위하여 통신정보를 수집·분석, 활용 및 유관기관에 제공할 수 있는 법적 기반 마련

- **(통신정보의 취득)** 내각총리대신은 **특별 사회기반사업자 또는 전기통신역무 이용자와의 협약에 따라**, 동의에 기반하여 전기통신역무 이용자가 주고받은 통신정보를 제공받을 수 있음

  ※ 외-내(外-內) 통신정보를 분석, 분석결과를 해당 사업자·이용자에게 제공

  - 다만, 동의가 없더라도 사이버공격에 관한 통신이 **의심되는 충분한 근거**가 있는 경우, **사이버통신정보감리위원회 사전승인**을 받아 통신정보를 취득할 수 있음

  ※ 외-외(外-外), 외-내(外-內), 내-외(內-外) 통신분석을 위한 정보 취득 가능

〈 '통신정보 취득 및 이용' 개요 〉

동의에 따른 통신정보 취득

- 내각총리대신은 특별 사회기반사업자와의 협약에 따라 통신정보 취득가능(제3장)
- 외-내 통신정보를 분석하여 필요한 결과를 해당 사업자에게 제공

동의없는 통신정보 취득

외-외(外-外) 통신 분석	외-내(外-內), 내-외(內-外) 통신분석
• 내각총리대신은 **해외 사이버공격**을 파악하기 위하여 **독립기관의 승인**을 받아 통신정보 취득가능(제4장)	• 내각총리대신은 **국내 사이버공격**을 파악하기 위하여 특정 외국 설비와의 통신 등 분석이 필요할 경우 **독립기관의 승인**을 받아 통신정보 취득가능(제6장)

※ **외-외(外-外) 통신** : 국내 네트워크를 통해 해외에서 해외로 전송되는 통신
외-내(外-內) 통신 : 해외에서 국내로 전송되는 통신
내-외(內-外) 통신 : 국내에서 해외로 전송되는 통신

↑ 독립기관의 사전승인 필요 ↑

독립기관(제10장)

↓ 승인 후 지속적인 조사·검사

자동화된 방법으로 기계적 정보 선별

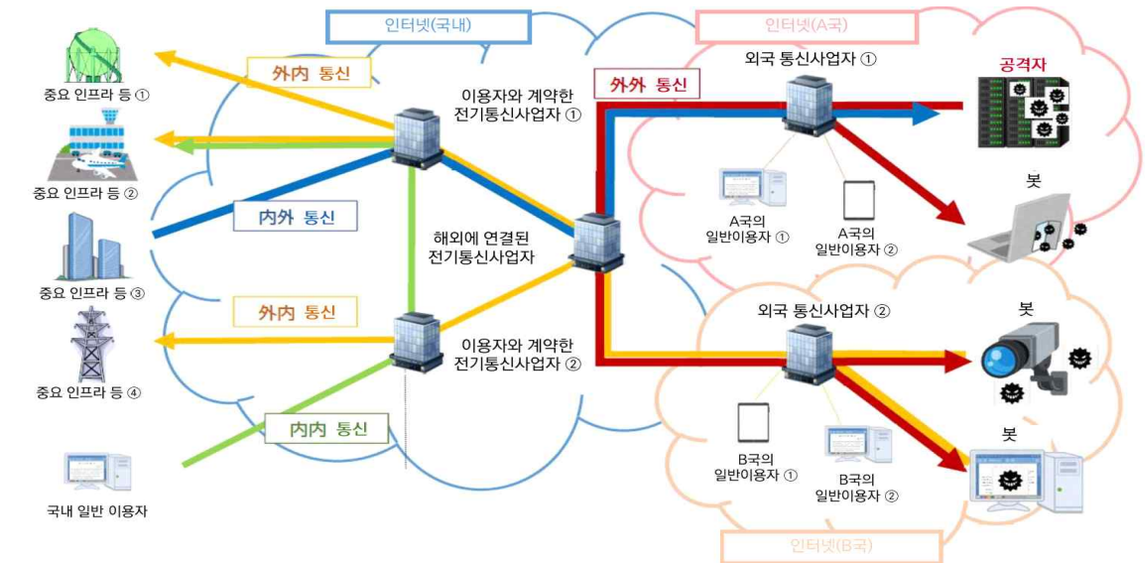
- 내각총리대신은 취득한 통신정보 중에서 **조사해야 할 사이버공격과 관련이 있다고 판단되는 기계적 정보**를 사람이 알지 못하는 자동화된 방법으로 선별해야 하고 그 외 정보는 즉시 삭제해야 함(제2조 제8항, 제5장, 제7장)

※ **기계적 정보** : IP 주소, 통신일시, 명령어 등 통신에 본질적 내용이 아닌 정보

↓

의회 보고

〈 통신정보 취득 대상이 되는 외국 관계통신 〉



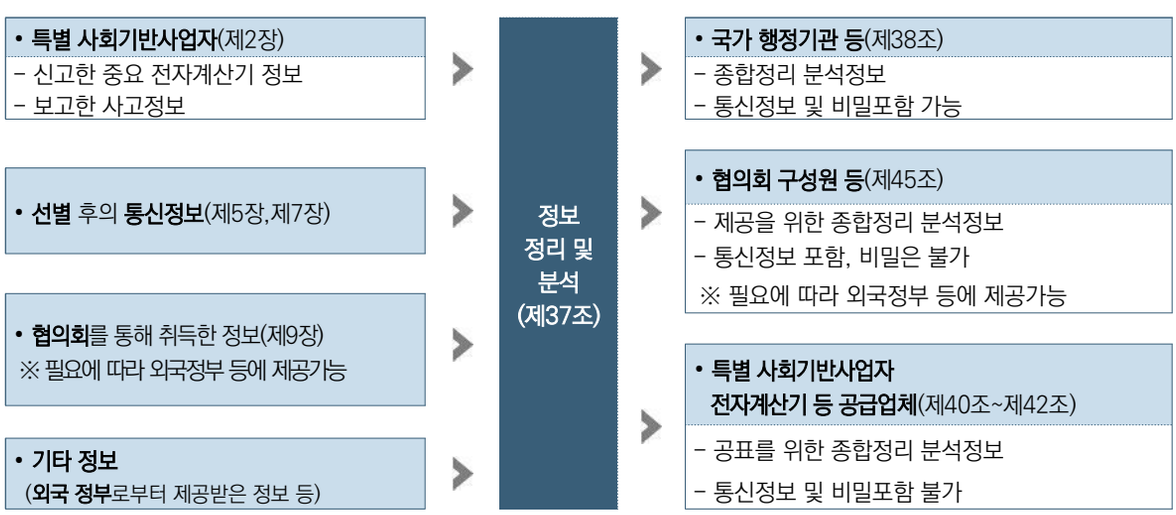
• **(자동화된 정보선별)** 내각총리대신은 취득한 통신정보 중 조사해야 할 사이버공격과 관련있다고 판단되는 **기계적 정보*를 자동화된 방법으로 선별**하고, 그 외 정보는 즉시 삭제

– 내각총리대신은 자동 선별 후 통신정보의 분석이 필요하다고 판단하는 경우 방위대신 등 관계 행정기관의 장에게 협조요청 가능

* **기계적 정보 :** 통신일시, IP 주소, 통신량, 포트번호, 명령어, 프로토콜 등 **통신에 본질적인 내용**(이메일 본문 및 제목, 첨부파일 내용 및 명칭, IP전화 통화내용, 웹사이트에 게재된 글·이미지)**이 아닌 정보**

• **(분석·취약점 정보 등의 제공)** 내각총리대신은 사고 보고 정보, 통신정보 등을 종합 정리·분석하여 관계 행정기관 등에 제공

〈 '종합정리 분석정보 제공' 개요 〉



○ 독립기관인 '사이버통신정보감리위원회'의 심사·승인, 검사 등 통제장치 마련

- 통신정보 이용의 적정성 확보를 위해 내각부 산하에 독립기관인 '사이버통신정보감리위원회' 설립하여 동의없는 통신정보 취득에 대한 신속한 심사·승인, 통신정보 취급에 관한 지속적 검사, 무해화 조치에 대한 심사·승인 등의 기능을 수행하도록 함

  ※ 내각총리대신은 국회(양원) 동의를 얻어 전문지식을 가진 위원장과 4명의 위원을 임명

○ 통신의 비밀 보호를 위한 통신정보의 엄격한 취급 및 비밀 누설·도용 금지의무 부과

- **(통신정보의 엄격한 취급)** 내각총리대신은 취득한 통신정보의 자동 선별을 제외하고, 선별하기 전의 통신정보 이용·제공 불가

  ※ 통신정보 기록 DB 제3자 제공시 형사처벌(4년 이하의 구금형 또는 200만엔 이하 벌금)

- **(비밀 누설·도용 금지)** 통신정보, 종합정리분석정보 등 취급사무 종사자(행정기관 공무원, 위원회, 협의회 사무 종사자 등)에게 비밀 유지의무 부과

  ※ 위반시 최대 3년 이하 구금형 또는 150만엔 이하 벌금

○ 정보처리추진기구(IPA) 등 전문기관에 대한 사무의 위탁 근거 마련

- 내각총리대신 등은 다음과 같은 사무를 독립행정법인 정보처리추진기구(IPA) 및 정령으로 정하는 특정 법인 등에 위탁 가능

〈 위탁사무의 내용〉

위탁사무		수탁기관
내각총리대신	• **내각총리대신의 보고 등 정보정리 및 분석사무** (제37조에 규정된 사무) ※ 선별 후 통신정보를 취급하는 사무를 제외 • **중요 전자계산기를 사용하는 자 등에 대한 주지** (제41조에 규정된 사무의 일부)	▶ • **정보처리추진기구** 및 그 밖의 해당 사무에 대하여 **충분한 기술적 능력 및 전문적 지식경험**을 갖추고 해당 사무를 확실하게 수행할 수 있는 **법인**으로서 정령으로 정하는 법인
내각총리대신 또는 **소관대신**	• **전자계산기 공급자 관련 정보제공 등**(제42조제1항에 규정된 사무의 일부)	

- 내각총리대신 또는 소관대신은 정보처리추진기구 등 수탁기관이 요청할 경우, 위탁사무를 수행하기 위해 필요한 제공용 종합정리분석정보 및 선별 후 통신정보를 제외한 기타 정보를 제공할 수 있음
- 수탁기관의 임직원 등은 정당한 사유없이 해당 사무에 관하여 알게 된 비밀을 누설·도용하여서는 안 되며 벌칙 등 형법 적용에 있어 법령에 따라 공무에 종사하는 직원으로 간주됨

○ 동 법안은 공포일로부터 1년 6개월을 초과하지 않는 범위 내에서 정령으로 정하는 날부터 시행

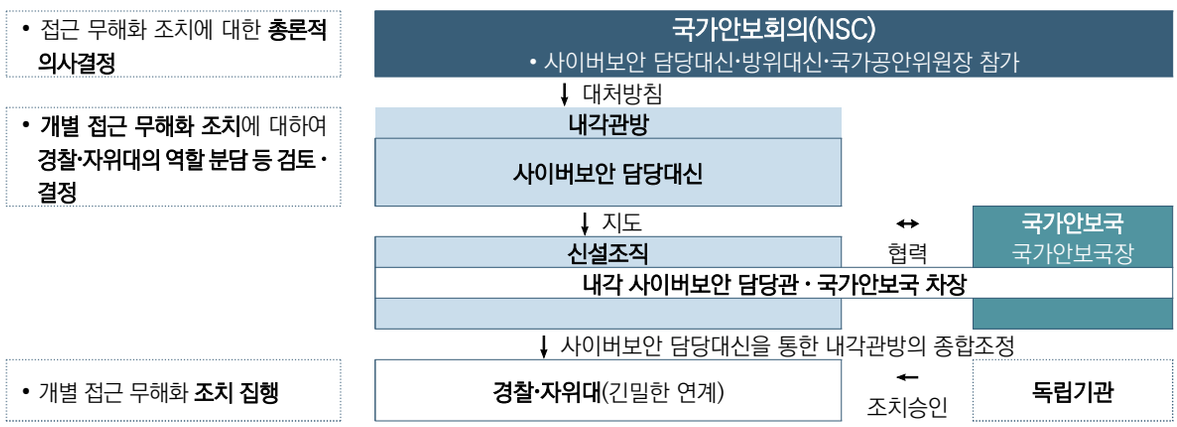
- 사이버통신정보감리위원회 설치는 1년을 초과하지 않는 범위에서, 통신정보의 이용은 일부를 제외하고 2년 6개월을 초과하지 않는 범위 내에서 정령으로 정하는 날로부터 시행

3.「동법 시행에 따른 관계법령 정비법안」 주요내용

○ 사이버공격에 대한 심각한 피해를 방지하기 위해 경찰 및 자위대에 서버 등 사이버공격에 대한 '접근 확인 및 무해화 조치' 권한 부여

- **(접근 확인 및 무해화 조치의 의미)** 사이버공격으로 의심되는 접근을 확인* →해당 서버 등이 공격에 이용되지 않도록 ① **설치된 공격용 프로그램 중지·제거**, ② 공격자가 해당 서버 등에 **접근할 수 없도록 설정 변경하는 조치**
  * 공격에 사용되는 서버 등의 취약점을 이용하는 등 원격 로그인을 통해 설치·작동 중인 공격용 프로그램 등을 확인
  - 해외 서버 등에 대한 조치의 경우, 주권 침해에 해당하더라도 '긴급상황' 등 국제법상 법리를 원용하는 등 국제법적으로 허용되는 범위 내에서 실시

〈 접근 무해화 조치의 거버넌스 구조 〉



○「경찰관직무집행법」과「자위대법」의 개정을 통해 경찰·자위대가 '접근 확인 및 무해화 조치'를 실시할 수 있는 요건과 절차를 구체화하고 역할을 분배함

〈 접근 무해화 조치의 요건·절차 개요 〉

경찰(경찰관 직무집행법 제6조 제2항)		자위대(자위대법 제81조의3, 제91조의3, 제95조의 4)
• **경찰청장이 지정하는 경찰관** (사이버피해 방지조치 집행관)	↔	• **내각총리대신은** 다음과 같은 경우 **통신보호 조치를 명령**하고 **자위대 등이 해당 조치 실시 가능** - ① 특정 중요 전자계산기에 대한 사이버공격 발생 - ② 외국정부가 배후에 있는 행위자에 의한 정교한 공격으로 판단되는 경우 - ③ 자위대가 처리해야 하는 특별한 필요*가 있는 경우 * 자위대가 보유한 특수 기술이나 정보가 필요한 경우
• **조치의 시행요건** - ① 사이버공격에 이용되는 전기통신을 인지하는 경우 - ② 방치할 경우 심각한 위해가 발생할 우려가 있어 긴급한 조치가 필요한 경우	내각관방의 조정을 통한 협력	• 주일미군이 사용하는 전자계산기를 사이버공격으로부터 보호하는 자위대 요원은 긴급한 필요가 있을 경우 무해화 조치 실시가능
• **조치의 내용** - ① 공격관련 서버 등의 관리자 등에 대한 조치명령 - ② 공격관련 서버 등에 대한 조치*를 자체 실시 * 공격용 프로그램 중지 및 삭제 등		• **조치 시행요건 및 내용은 경찰과 유사**
↓ 요청 ↑ 승인		↓ 요청 ↑ 승인

독립기관 등

• 독립기관의 승인과 경찰청장·방위대신의 지시가 필요
※ 승인을 받을 수 없다고 인정되는 특별한 사유가 있을 시 사후통보 가능

〈 경찰의 정보기술 이용 부정행위 피해방지 조치 〉

- 사이버피해 방지조치 집행관(경찰청장이 지정하는 경찰관)은 ① 공격받은 전자계산기 등의 **관리자에게 피해방지 조치를 명령**하거나, ② **자체적으로 조치** 실시 가능

  ※ 해외 서버 등에 대한 조치 시 사전에 경찰청장을 통해 외무대신과 협의

  - **(요건)** 정보기술 이용 부정행위가 의심되는 통신 등을 그대로 방치할 경우 **생명·신체, 재산상에 중대한 위해가 발생할 우려**가 있어 **긴급한 조치가 필요**한 경우
  - **(절차)** 경찰은 해당 조치를 실시하기 위해서 **사이버통신정보감리위원회 및 경찰청장의 사전 승인**을 받아야 함

    ※ **(사전 승인의 예외)** 기능에 중대한 장애를 발생시키거나 발생시킬 우려가 있는 전기통신이 현재 전송되고 있는 경우, 기타 위해방지를 위해 인정되는 특별한 사유가 있는 경우, 해당 조치 이후 위원회에 사후 통지해야 함
  - **(내용)** 해당 전자계산기의 접속 차단, 전자기적 기록의 삭제, 기타 피해방지 조치명령 또는 조치

〈 자위대의 중요 전자계산기에 대한 통신방호 조치 〉

- 내각총리대신은 자위대에 **중요 전자계산기*의 통신방호조치**를 명할 수 있고, 명령을 받은 부대 등은 경찰과 공동으로 조치 실시

  * **중요 전자계산기** : 국가행정조직, 지방공공단체, 독립행정법인, 지방독립행정법인, 법률에 의해 직접 설립되거나 특별법에 따른 특별설립행위로 설립된 법인 등이 사용하는 전자계산기 등

  - **(요건)** 중요 전자계산기에 대한 특정 부정행위가 ①외국정부 배후 행위자에 의한 고도로 조직적·계획적인 행위로 판단되는 경우로서, ② 자위대가 대처할 특별한 필요성이 인정되는 경우(다음의 어느 하나에 해당하는 경우를 말함)*

    * **▲해당 특정 부정행위로 인해 중요 전자계산기에 특정 중대한 지장**(기능이 정지·저하되어 사무·사업의 안정적 수행에 회복하기 어려운 지장을 초래하여 국가와 국민 안전을 현저히 훼손하는 사태를 초래하는 것)**이 발생할 우려가 큰 경우, ▲자위대가 보유한 특수한 기술·정보가 필수적인 경우 ▲ 국가공안위원회의 요청 또는 동의가 있는 경우**
  - **(절차)** 자위대는 통신방호조치를 실시하기 위해 방위대신 및 사이버통신정보감리위원회의 사전 승인 필요
  - **(기타)** 직무상 주일미군이 사용하는 특정 전자계산기를 사이버공격으로부터 보호하는 자위대 요원의 경우도 경찰의 권한을 준용

○ 능동적 사이버 방어체계 구축을 위한 사이버보안 조직 및 체제 정비

〈 '조직 및 체제정비' 개요 〉

사이버보안전략본부 강화 (사이버보안기본법 제26조, 제28조, 제30조, 제30조의2)	내각 사이버보안 담당관 신설 (내각법 제192조의2 및 제16조)	내각부 소관사무 추가 (내각부설치법 제4조 제9조)
• 사이버보안전략본부 개편 • 사이버보안전략본부 기능강화	• 사이버보안 확보에 관한 종합조정 등 사무를 수행하는 내각 사이버보안 담당관을 내각관방에 신설	• 내각부 소관사무에 민관협력 및 통신정보 이용에 관한 사무추가 • 상기 사무를 관장하는 내각부 특명 담당대신 설치 가능

• **(사이버보안전략본부 강화)** 「사이버보안 기본법」에 따라 설치된 '사이버보안전략본부'의 본부장을 기존 내각관방장관에서 내각총리대신으로 개편하고, 모든 내각각료를 구성원으로 포함함

※ 전략본부 내에 '사이버보안추진 전문가 협의회' 구축

– 또한 ① 중요 사회기반사업자 등의 사이버보안 확보에 관한 기준 마련, ② 국가 행정기관 등의 사이버보안 확보 현황 평가업무 등의 기능을 추가함

• **(내각 사이버보안 담당관 신설)** 내각관방에 사이버보안 확보에 관한 사무를 주관하는 내각 사이버보안 담당관(차관급 특별직 공무원) 신설

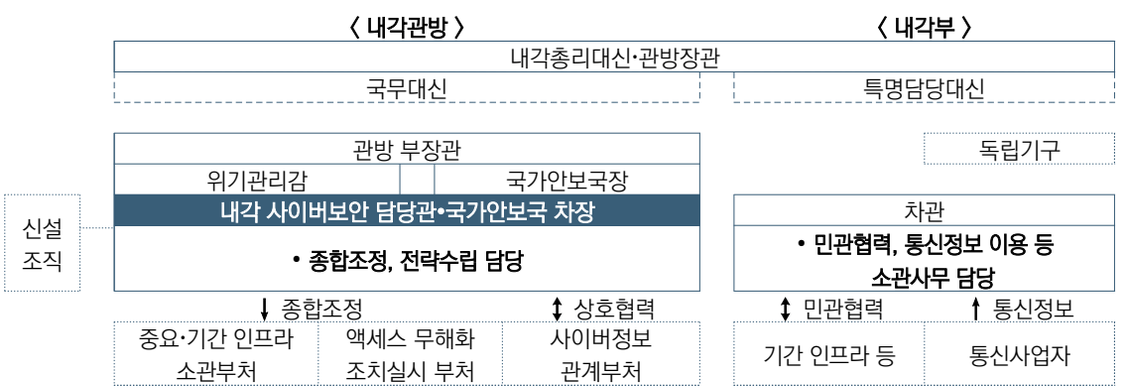
※ 국가안보국 차장을 3명으로 늘리고, 내각 사이버보안 담당관을 해당 직책에 임명

※ 내각 사이버보안센터(NISC) 개편은 정령 개정으로 추진할 예정

• **(내각부의 소관사무 추가)** 민관협력 강화 및 통신정보 이용에 관한 사무를 추가하고, 내각부 산하에 사이버 통신정보감리위원회를 설치

※ 상기 사무를 관장하는 내각부 특명담당대신을 임명

〈 능동적 사이버방어 거버넌스 체계 〉



○ 동 법안의 시행은 「중요 전자계산기 부정행위로 인한 피해방지 법안」 시행일과 동일

• 단, ▲사이버보안전략본부 개편, ▲내각 사이버보안 담당관 설치 등은 6개월을 넘지 않는 범위 내에서 정령으로 정하는 날로부터 시행

4. 시사점

• 동 법안은 '국가안전보장전략'('22.12.)에 따라 능동적 사이버 방어 실시체제를 정비하여 사이버안전보장 분야 대응능력을 강화하려는 일본의 적극적 의지를 반영한 것으로 볼 수 있음

- 전략에서 제시하는 ▲ 사이버공격에 대한 민관협력, ▲ 통신정보를 활용한 사이버공격 탐지, ▲ 공격자의 서버침입 무해화 등 조치 실현을 뒷받침하기 위한 법제 정비를 추진

• '능동적 사이버 방어'는 사이버공격에 의한 피해가 발생하기 전에 또는 그 피해가 확대되기 전에 대응하는 것을 말하며, 최근의 고도화·전문화된 사이버공격과 그 피해·영향 등을 고려할 때 기존의 사고 발생 이후 대응으로는 피해를 막는데 한계가 있다는 인식에서 적극 논의되고 있음

- 우리나라도 '국가사이버안보전략'('24.2.)에서 '공세적 사이버 방어활동 강화'를 전략과제로 제시하면서, 국가안보·국익을 위협하는 악의적 사이버활동에 대한 억지력을 확보하고 위협행위자의 사이버공격에 대한 선제적 방어역량을 강화하겠다고 밝힘
- 또한, 「국가사이버안보 기본법」 제정안(정부안 입법예고, '22.11)에서도 정부로 하여금 사이버안보 위해자 추적 등 사이버위협 무력화를 위한 활동 방안과 억지력 확보를 위한 사법·경제·외교적 제재 등 공세적 대응조치 방안을 마련하도록 규정함(안 제7조제5항)

• 다만, 능동적 사이버 방어조치 또는 공세적 대응조치가 무엇을 뜻하는지, 어떤 방식으로 구현될 것인지가 불분명하여 통신비밀 침해 또는 권한없는 정보통신망 침입·접근 등의 법적 논란이 제기[36]되기도 함

• 이번 일본 법안은 이러한 법적 논란을 최소화하기 위해 ▲ 정부의 통신정보 취득·활용 및 제공을 위한 법적 근거와 기준을 명확히 하면서 오·남용 방지대책 및 제3자에 의한 통제 장치를 마련하는 한편, ▲ 무해화 조치의 실시 기관, 대상 및 요건을 구체적으로 적시하고 있는 것으로 보임

※ **(통신정보 취득·제공 관련)** 통신의 본질적 내용을 제외한 기계적 정보의 범위 명확화, 취급자의 오·남용 방지대책 마련, 제3의 감독기구에 의한 정기 검사 등

※ **(무해화 조치 관련)** 범죄수사, 국방 등 권한을 가진 경찰, 자위대가 조치 수행, 별도 감독기구 승인 등

• 그러나 일각에서는 통신의 비밀에 대한 침해 가능성, 독립기관의 사후 승인 등 통제절차 형식화, 사이버공간에서 수집된 광범위한 정보의 중앙집중화에 따른 관료주의적 통제 강화 등 다양한 문제점을 제기[37]하기도 함

- 중의원 본회의 심의과정(본회의 회부, 3.18.)에서, 제1야당(입헌민주당)은 동 법안과 관련하여 ▲ 광범위한 통신정보 수집과 인권침해, ▲ 해외서버 등 무해화 조치에 따른 외교관계 악화, ▲ 모호한 독립기관 통제 예외사유 등을 지적하고 있어 추후 입법 추진경과를 살펴볼 필요성

• 한편, 일본 내각에서 추진한 동 법안에서 ▲ 중요 인프라에 도입·변경되는 중요 전자계산기 취약점 개선 등 조치 근거를 마련하고, ▲ 사고정보, 통신정보, 취약점 정보 등을 종합적으로 취득·분석하여 사이버공격 탐지 및 유관기관 공유체계를 구축한 점은 국내 주요기반시설 보호 및 침해사고 예방·대응체계 강화에도 참고가 될 수 있음

36) 攻撃元にアクセスし無害化「能動的サイバー防御」法案閣議決定 (NHK, 2025. 2. 7.) https://www3.nhk.or.jp/news/html/20250207/k10014715361000.html
37) 【衆院本会議】サイバー対処能力強化法案審議入り「国民生活と経済活動を守るため、サイバー防御の強化は待ったなし」山岸議員 (2025. 3. 18.)) https://cdp-japan.jp/news/20250318_8969

Reference

▪内閣官房, 説明資料(サイバー対処能力強化法案及び同整備法案について) (2025. 2. 7.)

▪内閣官房, サイバー安全保障分野での対応能力の向上に向けた提言(有識者会議) (2024. 11. 29.)

▪https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/index.html

▪https://www.sangiin.go.jp/japanese/joho1/kousei/gian/217/gian.htm

▪https://internet.watch.impress.co.jp/docs/news/1661550.html

▪https://xtech.nikkei.com/atcl/nxt/keyword/18/00002/120200271/?P=2

▪https://rocket-boys.co.jp/security-measures-lab/what-active-cyber-defense/#index-5

▪https://www3.nhk.or.jp/news/html/20250207/k10014715361000.html

▪https://cdp-japan.jp/news/20250318_8969

부록

국내 인터넷·정보보호 입법동향 목록

○ 입법예고된 법령

법령명	입법예고 기간	주요내용
「위치정보의 보호 및 이용 등에 관한 법률 시행령」 일부개정령안	2025. 2. 19. ~ 2025. 3. 31.	• **(소관부처)** 방송통신위원회 • **(개정이유)** 방송통신위원회 권한의 일부를 그 소속기관인 방송통신사무소에 위임하는 「위치정보의 보호 및 이용 등에 관한 법률」 제38조에 따라 구체적인 위임업무를 동법 시행령에 신설 • **(주요내용)** – 위치정보사업자 등의 신고 업무 방송통신사무소 권한 위임근거 신설
「자동차 및 자동차부품의 성능과 기준에 관한 규칙」 (「자동차관리법」 시행규칙) 일부개정령안	2025. 2. 27. ~ 2025. 4. 8.	• **(소관부처)** 국토교통부 • **(개정이유)** 자동차 사이버보안 관리체계 인증제도를 도입하고 자동차 소프트웨어 업데이트 준수사항을 신설하는 내용으로 「자동차관리법」이 개정됨에 따라, 위임사항 등을 정하기 위함 • **(주요내용)** – 무선 업데이트를 '케이블 등의 연결없이 무선으로 데이터를 전송하는 방법으로 자동차 소프트웨어를 변경하는 것'으로 정의 – 자동차 사이버보안 관리체계 인증내용에 따라, 자동차 부품 및 시스템 관련 사이버공격·위협이 식별되는 등 관련 의무를 준수하여 제작되도록 함 – 자동차의 소프트웨어는 버전을 확인할 수 있어야 하며, 무선 업데이트를 실시할 경우 특정 기준에 적합해야 함

○ 공포된 법령

법령명	공포일	주요내용
「정보통신기반보호법 시행령」 일부개정령	2025. 1. 14.	• **(소관부처)** 과학기술정보통신부 • **(개정이유)** 「정보통신기반 보호법」이 개정(법률 제20068호, 2024. 1. 23. 공포, 2025. 1. 24. 시행)됨에 따라, 위임사항 등을 정하기 위함 • **(주요내용)** – 주요정보통신기반시설 보호에 관한 업무를 총괄하는 정보보호책임자의 업무에 주요정보통신기반시설 보호지침 준수명령의 이행업무 추가 – 주요정보통신기반시설의 침해사고 발생 시 관계 중앙행정기관장 등의 복구 및 보호 조치명령을 이행하지 않는 경우의 과태료 금액 명시
「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」 제정	2025. 1. 21.	• **(소관부처)** 과학기술정보통신부 • **(개정이유)** AI의 건전한 발전을 지원하고 AI 사회의 신뢰 기반 조성에 필요한 기본적인 사항을 규정하기 위함 • **(주요내용)** – AI 사업자는 고영향 AI 및 생성형 AI를 통해 제품·서비스를 제공할 때 AI가 사용된다는 사실을 사전고지 해야 함 – 고영향 AI 사업자는 위험관리 방안 및 이용자 보호방안 수립·운영 등의 안전성·신뢰성 확보조치를 이행해야 함

법령명	공포일	주요내용
「디지털포용법」 제정	2025. 1. 21.	• **(소관부처)** 과학기술정보통신부 • **(제정이유)** 디지털포용 증진 관련 사업 육성에 관한 사업을 규정함으로써 사회구성원의 삶의 질 향상과 사회통합에 이바지하기 위함 • **(주요내용)** – 국가·지자체는 모든 구성원이 지능정보서비스·제품에 원활하게 이용할 수 있도록 시책을 마련하고, 집행과정에서 의견수렴 방안을 마련 – 디지털역량센터의 지정 · 지원, 디지털역량 함양 종합정보시스템 구축 · 운영의 근거를 마련 – 무인정보단말기를 설치 · 운영하는 자 및 제조 · 임대하는 자에게 디지털 취약계층의 정보접근 등을 증진하기 위한 조치를 취할 의무부과 – 정부가 디지털포용을 위한 기술 및 서비스의 연구 · 개발 및 확산을 위한 사업을 전문기관 등에 위탁할 수 있는 근거를 마련
「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 일부개정	2025. 1. 31.	• **(소관부처)** 과학기술정보통신부 • **(제정이유)** 전문인력 양성을 위한 과기정통부 장관의 교육기관 지정과 관련하여, 환경 · 외부적 요인 등을 고려하지 아니한 획일적인 지정취소 사유를 개선하기 위함 • **(주요내용)** – 과기정통부장관이 클라우드컴퓨팅 관련 교육훈련 실시기관의 지정일부터 1년 이상 교육실적이 없다는 사유로 해당 교육기관의 지정을 취소하려는 경우, 해당 교육실적이 없는 '정당한 사유'를 고려해야 함
「전자금융감독규정」 일부개정 (「전자금융거래법」 고시)	2025. 2. 5.	• **(소관부처)** 금융위원회 • **(개정이유)** 금융회사 등이 보안위험에 유연하게 적응할 수 있도록 「전자금융감독규정」을 '규칙' 중심에서 '원칙' 중심으로 합리화하여 금융회사 등의 자율보안 역량강화를 뒷받침 • **(주요내용)** – CISO는 정보보호위원회 주요 심의·의결 사항 등을 이사회에 보고 – 기존 은행 등이 부담하던 재해복구센터 구축 의무가 일정 규모 이상의 여신전문금융회사 등으로 확대 – 금융회사 등이 준수해야 하는 건물, 설비, 전산실 등 시설부문 관련 세부 내용을 대부분 삭제하고 원칙 중심으로 합리화 – 타 규정과 중복되는 내용 및 지나치게 구체적인 규정을 삭제 및 통합 – 전자금융업무 지연·중단 사고보고 범위를 일부 축소
「개인정보 보호법」 시행령 일부개정령	2025. 2. 25.	• **(소관부처)** 개인정보보호위원회 • **(개정이유)** 「개인정보 보호법」이 개정(법률 제19234호, 2023. 3. 14. 공포, 2025. 3. 13. 시행)됨에 따라, 제도 운영상 나타난 일부 미비점을 개선·보완하기 위함 • **(주요내용)** – 정보주체의 개인정보를 전송받을 수 있는 자가 갖추어야 하는 시설 및 기술 기준을 마련하고 정보주체의 요구에 따라 개인정보를 전송해야 하는 개인정보처리자의 범위를 규정 – 전송요구의 대상이 되는 개인정보 범위를 규정 – 가명정보의 결합을 수행하는 전문기관의 지정 기준 및 재지정 기준 정비 – 개인정보관리 전문기관의 지정절차 및 금지행위를 규정

법령명	공포일	주요내용
「전기통신사업법」 일부개정	2025. 3. 18.	• **(소관부처)** 과학기술정보통신부 및 방송통신위원회 • **(개정이유)** 불법 스팸으로 인한 개인정보 유출 및 금융사기 등 민생범죄를 방지하기 위하여, 대량문자전송사업자의 등록요건 준수여부 정기점검 및 전송자격 인증제도의 근거를 마련 • **(주요내용)** – 과기정통부장관 또는 방송통신위원회는 대량문자전송사업자의 등록요건 준수 여부를 연 1회 주기적으로 점검 – 대량문자전송사업자에 대한 전송자격 인증제의 법적근거를 마련하고, 부가통신사업을 등록하는 경우 전송자격 인증여부를 확인
「전기통신사업법」 시행령 일부개정령	2025. 3. 28.	• **(소관부처)** 과학기술정보통신부 • **(개정이유)** 현행 전기통신사업법령은 부가통신서비스 중단 시 이용자 고지 의무가 유료 서비스에 한정되어 이용자의 혼란과 피해를 예방하기에 미흡한 점이 있다는 지적 제기 • **(주요내용)** – 무료 서비스의 경우에도 부가통신역무의 제공이 중단된 사실 및 그 원인, 대응조치 현황 등을 이용자에게 알리도록 고지 의무대상 확대 – 부가통신역무 제공이 4시간 이내로 중단된 경우에 고지의무를 면제하였던 기존의 조항을 2시간 이상 중단된 경우에도 고지하도록 의무 대상 확대 – 전기통신서비스 중단 시 고지 수단으로 기존의 문자, 전자우편, 회사 홈페이지 공지 외에도 SNS 등을 이용할 수 있도록 고지수단 추가

○ 발의된 법률안

법안명	제안일	주요내용
「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안 (고동진의원 대표발의)	2025. 1. 16.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 최근 사회적으로 카카오톡 등에 대한 검열 논란이 야기되고 있으나, '표현의 자유'는 헌법적 가치이기 때문에, 법률적으로 확실히 보장되어야 한다는 지적이 제기 • **(주요내용)** – 누구든지 카카오톡 등 정보통신서비스의 이용자가 해당 정보통신서비스를 이용할 때에 다른 법률에서 특별히 규정된 경우 외 그 이용과 관련된 정보를 검열하거나 감시, 조사 및 감청하여서는 아니되도록 규정 – 위반 시 7년 이하의 징역 또는 7천만원 이하의 벌금
「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안 (고동진의원 대표발의)	2025. 1. 23.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 최근 일각에서는 국민들의 '표현의 자유'를 침해하려는 행태가 나타나고 있어, 자유민주주의의 핵심이 되는 자유권적인 기본권이 무너질 수 있다는 우려가 제기 • **(주요내용)** – 누구든지 국민의 정보통신서비스 이용에 대한 '표현의 자유'를 침해하지 않도록 규정하고 해당 '표현의 자유'는 모욕죄, 명예훼손죄 등 다른 법률에서 특별히 제한하는 경우 외에는 반드시 보장되도록 규정

법안명	제안일	주요내용
「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안 (조인철의원 대표발의)	2025. 1. 24.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 알고리즘정보추천서비스의 경우 이용자의 선호에 부합하는 정보만을 제공하여 이용자가 해당 서비스의 이용 여부를 선택할 수 있도록 조치가 필요하다는 의견이 제기 • **(주요내용)** – 알고리즘정보추천서비스 제공 사업자는 해당 서비스의 이용 여부를 선택할 수 있다는 사실과 그 선택절차 등을 약관에 명시적으로 규정 – 해당 서비스의 지속적 이용의사가 있는지 여부를 묻는 선택항목을 주기적으로 제공하는 등 이용자의 선택권을 보장하기 위한 필요한 조치를 마련
「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안 (이헌승의원 대표발의)	2025. 3. 21.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 불법스팸 전송에 따른 벌금이나 과태료에 비하여 전송으로 얻는 이익이 더 크다는 지적 제기 • **(주요내용)** – 불법스팸을 전송한 정보통신서비스 제공자 등에게 과징금을 부과하고 불법스팸 전송 행위를 몰수·추징 대상으로 규정할 수 있는 근거 마련 – 불법스팸 전송 관련 민관 상설 협의체 구성·운영 근거 규정
「위치정보의 보호 및 이용 등에 관한 법률」 전부개정법률안 (신성범의원 대표발의)	2025. 1. 22.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 위치정보법을 전부 개정하여 사업자가 위치정보 산업에 활발히 진출할 수 있는 기반과 이용자 권리 침해 보호 방안을 마련하기 위함 • **(주요내용)** – 위치정보산업에 진흥을 법의 목적에 추가하고 위치정보산업을 새롭게 정의함과 동시에 위치정보산업 진흥사업의 실시 근거를 마련 – 개인위치정보와 사물위치정보의 구분을 폐지하고 위치정보로 일원화 – 위치정보의 수집 · 이용 · 제공에 따라 위치정보사업자와 위치기반서비스 사업자로 구분하고 있는 현행 체계를 위치정보사업의 개념으로 통합 – 위치정보사업자등이 위치정보를 제3자에게 제공시 표시 · 통지로 규제 완화
「의료법」 일부개정법률안 (전진숙의원 대표발의)	2025. 2. 11.	• **(소관위원회)** 보건복지위원회 • **(제안이유)** 의료기관에서 운영하고 있는 영상정보·검사정보시스템 등에 대한 전자적 침해가 환자 및 의료기관의 정보침해로 이어질 수 있어, 현행 법상 전자의무기록에 대한 침해사고 범위를 확대할 필요성 제기 • **(주요내용)** – 전자의무기록 외에 의료기관에서 운용하는 전산시스템에 대한 전자적 침해행위로 정보가 유출된 경우에도 진료정보 침해사고로 관리
「인공지능 발전과 신뢰기반 조성 등에 관한 기본법」 일부개정법률안 (정철민의원 대표발의)	2025. 2. 21.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 양질의 AI 서비스·제품들은 대부분 유료라 경제적 이유로 저소득층의 AI 서비스 접근성이 떨어지면 소득격차가 고착화될 우려 • **(주요내용)** – 과기정통부 장관은 AI 기본계획을 수립할 시 AI 서비스에 대한 접근성 확보에 관한 사항을 포함해야 함 – 국가 및 지자체는 AI 제품 및 서비스를 이용하는 저소득층·청소년 등에 대하여 그 비용의 전부 또는 일부를 예산 범위에서 지원해야 함

법안명	제안일	주요내용
「개인정보 보호법」 일부개정법률안 (이수진의원 대표발의)	2025. 1. 16.	• **(소관위원회)** 정무위원회 • **(제안이유)** 공연 또는 운동경기 입장권 구입 시 생체정보를 의무적으로 제공하도록 하는 입장권 판매업체의 계획에 대한 관리의 필요성 제기 • **(주요내용)** – 현행법에 민감정보의 유형으로 지문·얼굴·홍채 및 손바닥 정맥 등 개인식별 생체정보를 추가하여 법적근거를 명확하게 함 – 개인정보처리자가 민감정보를 처리하지 아니하고 재화 또는 서비스를 제공할 수 있는 경우에 정보주체에게 그 사실을 알리도록 함
「개인정보 보호법」 일부개정법률안 (강민국의원 대표발의)	2025. 1. 31.	• **(소관위원회)** 정무위원회 • **(제안이유)** 최근 알리·테무 등 해외사업자의 형식적인 국내 대리인 제도 운영으로 국내 이용자의 권리가 제대로 보호되지 않는다는 문제제기 • **(주요내용)** – 개인정보처리자에게 국내대리인 관리·감독 의무를 부과 – 개인정보처리자가 국내 법인을 설립·운영 중에 국내대리인 관리·감독이 소홀하거나 국내대리인 전화번호를 미공개하는 경우 등에 과태료 부과
「개인정보 보호법」 일부개정법률안 (민병덕의원 대표발의)	2025. 1. 31.	• **(소관위원회)** 정무위원회 • **(제안이유)** AI기술 개발이 시급한 분야에서 개인정보가 포함된 데이터 활용 및 개인정보 처리과정의 투명성 강화에 대한 필요성 증대 • **(주요내용)** – AI 기술을 개발하거나 성능을 개선하기 위해 필요한 경우 강화된 안전조치 및 정보주체의 권리보장 방안 등을 마련하여 개인정보보호위원회의 심의·의결을 거친 때에 적법하게 수집한 개인정보를 활용할 수 있도록 규정 – 사전에 개인정보 처리방침을 통해 처리 현황을 투명하게 공개하고, 일정 규모 이상의 민감정보·고유식별정보 등이 포함된 경우 위험요인 등을 평가하도록 규정
「개인정보 보호법」 일부개정법률안 (김태선의원 대표발의)	2025. 2. 11.	• **(소관위원회)** 정무위원회 • **(제안이유)** AI가 공개된 개인정보를 학습하는 과정에서 정보주체의 동의를 받아야 하는지 여부가 불명확하다는 문제제기 • **(주요내용)** – 정보주체가 스스로 사회관계망서비스 등에 직접 또는 제3자를 통하여 공개한 개인정보에 대해서 정보주체의 동의 없이 수집할 수 있도록 함 ※ 수집 범위는 해당 정보주체의 동의가 있었다고 객관적으로 인정되는 범위 내로 한정
「개인정보 보호법」 일부개정법률안 (고동진의원 대표발의)	2025. 3. 13.	• **(소관위원회)** 정무위원회 • **(제안이유)** AI기술 개발 시 개인정보가 포함된 데이터 활용에 대한 요구 및 개인정보 처리과정의 투명성 강화에 대한 필요성 증대 • **(주요내용)** – AI 기술을 개발하거나 성능을 개선하기 위해 필요한 경우 강화된 안전조치 및 정보주체의 권리보장 방안 등을 마련하여 적법하게 수집한 개인정보를 활용할 수 있도록 규정 – AI 기술을 개발하거나 성능을 개선하기 위해 필요한 경우 강화된 안전조치 및 정보주체의 권리보장 방안 등을 마련하여 개인정보보호위원회의 심의·의결을 거친 때에 적법하게 수집한 개인정보를 활용할 수 있도록 규정 – 개인정보보호위원회의 동일·유사한 심의·의결이 있었던 경우 심의·의결 절차를 간소화할 수 있도록 하고 심의·의결한 주요내용을 인터넷에 공개

부록

해외 인터넷·정보보호 입법동향 목록

○ ’25년 1월

국가	입법동향
튀르키예	• 사이버보안기구 설립을 위한 대통령령 공포 ('25.1.8.)
영국	• 랜섬웨어 법안 추진을 위한 의견수렴 (’25.1.14.)
미국	• 연방통신위원회(FCC), 국가통신시스템의 사이버보안 강화를 위한 잠정규정예고문 발표 (’25.1.16.)

○ ’25년 2월

국가	입법동향
미국	• 미시시피 주 하원, 「사이버보안 표준준수 조직의 면책법(안)」 발의 (’25.1.20.)
미국	• 상원, 「사이버보안 보험법(안)」 발의 (’25.1.24.)
미국	• 상원, 「라우터법(안)」 발의 (’25.1.27.)
EU	• 개정 「사이버보안법」 및 「사이버연대법」 발효 (’25.2.4.)
일본	• 일본, 「사이버 대응역량 강화법(안)」 국회제출 (’25.2.7.)

○ ’25년 3월

국가	입법동향
호주	• 「스캠 방지 프레임워크법」 제정 (’25.2.20.)
스페인	• 「사이버보안 조정 및 거버넌스에 관한 법률」 초안 의견수렴 (’25.2.10.)
EU	• 집행위원회, 「사이버복원력법」 이행규정 초안 발표 (’25.3.14.)

※ 해외 인터넷·정보보호 입법동향 목록은 한국인터넷진흥원의 공식 홈페이지(지식플랫폼)에 수시로 게재되는 「인터넷·정보보호 법제동향」 목록임을 안내드립니다.

2025년 1분기

인터넷·정보보호 법제동향

『인터넷·정보보호 법제동향』은 디지털·정보보호 관련 입법동향 및 주요 이슈를 분석하여 정책 자료로 활용하기 위해 한국인터넷진흥원에서 기획, 발간하는 분석보고서입니다.

한국인터넷진흥원(KISA) 정책연구실 법제연구팀

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY