대통령직속 국가인공지능전략위원회 | 보도자료

보도시점 2026.2.25.(수) 10:00 배포 2026.2.24.(화) 18:00

국가인공지능전략위원회, 제2차 전체회의 개최

- AI 3강 도약의 구체적 청사진, '대한민국 인공지능행동계획' 확정
- ▲국가정보 관리 시스템 혁신으로 안전하고 복원력 있는 AI정부 인프라 구축 방향 제시 ▲화이트해커를 활용한 보안 취약점 신고 제도 도입 추진 ▲AI시대 과학기술 경쟁력 대도약을 위한 'K-문샷' 본격 추진 등 주요 정책 의결
- AI전략위 내 'AI민주주의 분과' 및 '보안'·'지역' 특별위원회 신설

국가인공지능전략위원회(위원장 이재명 대통령, 이하 '위원회')는 2월 25일(수) 10시, 위원회가 위치한 서울스퀘어(16층)에서 **제2차 전체회의**를 개최했다고 밝혔다. 회의는 **임문영 상근 부위원장**이 **주재**하였으며, **정부·민간 위원** 및 **관계 부처** 등 50여 명이 참석한 가운데, **'대한민국 인공지능행동계획(인공지능 기본계획)'**을 포함한 총 **5개**의 **안건**을 **심의·의결**하였다.

< 국가인공지능전략위원회 제2차 전체회의 개요 >

■ **(일시/장소)** 2월 25일(수), 10:00~11:00 / 서울스퀘어 16F

■ **(참석)** 민간임문영 상근 부위원장**(주재)** 및 위원, 정부경제부총리 겸 재정경제부 장관(부위원장), 과기부총리 겸 과기정통부 장관(부위원장) 및 정부위원(대참 포함) 등 50여명

■ **(안건)** ❶ 대한민국 인공지능행동계획(인공지능 기본계획(2026~2028)) (주관: 위원회·과기정통부)
❷ AI정부 인프라 거버넌스·혁신 추진방향 (주관: 위원회)
❸ 보안 취약점 신고·조치·공개 제도 도입 로드맵 (주관: 위원회)
❹ AI시대 과학기술 경쟁력 대도약을 위한 K-문샷 추진전략(안) (주관: 과기정통부)
❺ 국가인공지능전략위원회 운영세칙 일부개정안 (주관: 위원회)

◇ 안건 1. 대한민국 인공지능행동계획

먼저, 제1호 안건으로 **「대한민국 인공지능행동계획(인공지능 기본계획(2026~2028))」**을 **심의·의결**하였다. '대한민국 인공지능행동계획'은 지난 2월 10일 **국무회의**에 **보고**된 바 있으며, 이번 회의에서 **세부 내용**을 **최종 확정**하여 「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법(이하 'AI기본법')」 제6조에 따른 **법정계획**인 **'인공지능 기본계획'**으로 **의결**되었다.

위원회는 **제1차 전체회의**('25.9.8.)에서 의결한 **대한민국 인공지능행동계획(이하 '인공지능행동계획') 추진방향***을 토대로 100일간 **초안**을 마련하였다. 이후 대국민 공개 의견 수렴, 330개 주요 기관·단체 설명회 및 현장 간담회 등 **폭넓은 의견 청취**로 내용을 보완하였고, **총 99개 실행과제**와 **326개 정책 권고**로 구성된 **최종안**을 **확정**하였다.

* 'AI 3대 강국 도약' 비전 달성을 위한 ❶AI혁신 생태계 조성 ❷범국가 AI기반 대전환 ❸글로벌 AI기본사회 기여라는 3대 정책축과, 이를 뒷받침하는 12대 전략분야

인공지능행동계획은 대한민국의 **혁신 성장**과 **국민 삶의 질 향상**을 위해 인공지능을 국가·사회 전반에 효과적으로 내재화하기 위한 **종합 실행 전략**으로, **범정부 차원**의 **제도** 및 **거버넌스 개선**을 아우르고 있다. 주요 과제로는 ▲**창작자 권리**를 **보호**하면서 **저작물 AI활용**을 **촉진**하는 **법·제도 개선 방안** 마련, ▲**화이트해커**와 **협력**해 **보안 취약점**을 **선제적·상시적**으로 **발굴·제거**하는 제도 도입, ▲**민간·공공 AI·데이터 정책** 간 연계·협업을 위한 **거버넌스** 정립 방향 마련, ▲국민이 **신청하지 않아도** AI·데이터를 활용해 **복지혜택**을 받을 수 있도록 관련 법 개정, ▲**사회적 숙의**를 기반으로 한 **AI기본사회 추진계획** 마련 등을 담고 있다.

이날 의결된 **인공지능행동계획**은 향후 **범정부 인공지능 정책 추진**의 **기준**이 된다. 위원회는 부처별 **이행 상황**을 체계적으로 **점검**해 나갈 계획이며, 부처와 긴밀한 협력을 통해 **국민**이 **체감**할 수 있는 **성과**를 **창출**할 수 있도록 **노력**해 나갈 것이다.

◇ 안건 2. AI정부 인프라 거버넌스 · 혁신 추진방향

이어서, 제2호 안건으로 **대통령 지시**('25.9.28, 중대본 회의)에 따라 **국가정보 관리 시스템**을 **근본적으로 재설계**하기 위한 「**AI정부 인프라 거버넌스·혁신 추진방향**」을 **심의·의결**하였다.

※ 국가AI전략위원회 산하 AI정부 인프라 거버넌스·혁신 TF 구성·운영('25.9.30~)
- 공동리더 : AI미래기획수석(정부), 아토리서치 대표(민간)

정부는 **정부·공공 부문 데이터센터 안전기준**을 **민간 수준 이상**으로 강화('26.2.11 시행)하고, 재해 대응 능력과 수용 용량의 한계에 도달한 **국가정보자원관리원**(국정자원) **대전센터**를 **2030년까지 폐쇄**할 계획이다.

또한, 국민 생활 영향도를 고려한 **시스템 유형별 복구목표기준***을 마련하는 등 **재해복구체계(DR) 구축 방향**을 정립하고, 데이터 중요도에 따라 **기밀**(Classified) 데이터는 **정부·공공 데이터센터**, **민감**(Sensitive)·**공개**(Open) 데이터는 **민간 클라우드**로 이관하는 방향으로 추진한다.

* 시스템 유형별 복구목표시간(안) : ▲국가 핵심 시스템(실시간~1시간 이내), ▲대국민 필수 시스템(3~12시간 이내), ▲행정 중요 시스템(1~5일 이내)

올해에는 **국정자원 대전센터** 시스템(693개) 등을 대상으로 **DR 시스템 134개**를 **우선 구축**하고, 이 중 **3개 핵심 시스템**(디브레인, 우편정보시스템, 안전디딤돌) 중심으로 **민간 클라우드 기반 DR 구축 선도 프로젝트**를 추진한다. 또한, 시스템 분류 등을 고려한 **국정자원**의 **공공 정보시스템**을 **재배치**하는 **로드맵**도 수립할 계획이다.

과학기술부총리 산하에 관계부처 합동으로 **AI정부 인프라 총괄 전담조직**(가칭AI정부 인프라 거버넌스·혁신 추진단)을 신설하여, **공공 정보시스템 구축·운영**의 **적정성**을 **검토**하고, 영국 정부디지털청(GDS) 등 해외사례를 참고한 **중장기 거버넌스 재설계** 방안도 마련할 예정이다.

◇ 안건 3. 보안 취약점 신고 · 조치 · 공개 제도 도입 로드맵

제3호 안건으로는 "기존 **사후 대응 중심**의 국내 정보보안 패러다임을 **사전 예방**으로 전환"하기 위해 "**화이트해커**가 **기업·기관의 보안 취약점을 상시적**으로 찾아 신고하고, **피신고 기관**은 신고된 취약점을 **조치**하며 그 이후 투명하게 공개함으로써 해킹 등 보안사고를 사전에 예방"하는 **'보안 취약점 신고·조치·공개 제도 도입 로드맵'**을 **심의·의결**하였다.

현재 국내 **보안 제도**는 1회성·체크리스트 중심 점검에 절차 평가 위주로 **실시간으로** 이루어지고 **상시적으로 고도화되는 해킹 등에 대응**하기에 어려움*이 있다.

* **[예]** △ (**인증**) ISMS, ISMS-P → **年 1회 체크리스트 점검,** △ (**점검**) 보안적합성 검증, 개인정보 영향평가 → **도입시 검증**, △ (**평가**) 개인정보 수준평가, 사이버보안실태 평가 → **절차평가 중심**

관련 미국·유럽은 **보안 취약점 신고·조치·공개 제도**(이하 'CVD/VDP*)**를 이미 운영** 중이며 그 **배경**에는 '10년~'20년대 **세계적인 보안 대란사태****가 있었다. **위원회는 유사한 시대적 상황**에서 **AI**를 활용한 **신종 위협**이 더욱 **확산***** 되는 지금, 미국·유럽이 도입한 해당 제도를 벤치마킹, **공공·민간 전반에 단계적으로 도입**해 현재의 **국가적 보안 사태를 극복한다는 방침**이다.

* Coordinated Vulnerability Disclosure : 조정된 취약점 공개 / Vulnerability Disclosure Policy : 취약점 공개 정책

** (워너크라이, '17) 美국가안보국이 발견했으나 미공개한 윈도우 취약점이 150개국 해킹 활용 / (솔라윈즈, '20) 취약점 SW업데이트 파일이 美연방기관 연쇄 해킹

*** 해커들, AI 이용 5주만에 전 세계 방화벽 600대 침해('26.2. 아마존)

이를 위한 **구체적인 도입 방안과 추진 로드맵**은 아래와 같다.

[도입 방안]

△ **(대상)** 초기에는 **참여 기업·기관 모집**을 통해 시행하되 궁극적으로는 **공공**은 **의무화**하고 **민간**은 공공조달 연계 등 **전면적 참여를 유도**한다.

△ **(참여 유인) 공공**의 경우 **기관 평가**와 연계, **민간**의 경우 보안인증 가점, 공공조달, **개인정보보호법**에 따른 **사고시 과징금 감경 요소**에 반영, **화이트해커**는 **신고포상제 활성화**로 초기 참여를 유도한다.

△ **(보호)** 초기에는 **참여기업·기관-화이트해커 상호 협의**하에 제한적으로 운영하되, 궁극적으로는 **화이트해커**가 **민·형사 처벌 걱정 없이 상시적으로 기업·기관**이 정한 정책 범위(해킹범위, 신고방식 등) 내에서 **선의적 목적의 해킹**을 할수 있게 관계 법령을 정비한다. 참고로 현재는 **화이트해커의 망 접근이 불법**으로 제품만을 대상으로 한 취약점 신고 포상제만 운영되고 있으며 이마저도 **신고된 취약점에 대한 조치 강제력** 없이 **연중 상시가 아닌 주기적**(분기별 1회 등) **이벤트성**으로 운영되고 있다.

[추진 로드맵]

△ **(1단계 : 시범사업)** '26년에는 **과기정통부·국정원** 주도로 민간·공공분야 **시범 사업**을 운영하여 국내 제도 도입 효과를 사전에 검증한다.

△ **(2단계 : 참여 확대)** **'27년**에는 **시범사업 결과 바탕**으로 **민간**(과기정통부)·**공공**(국정원)**분야 제도설계 및 관련 가이드라인을 마련·배포**하며, **이외 부처**들은 **민간·공공**의 **참여 유인**(과징금, 조달 연계 등)**을 제도화**한다.

△ **(3단계 : 법제화)** 2단계 이후 최대한 조속히 **관계 법령**(정보통신망법 등) **개정을 완료**해 공공 의무화·민간 전면 참여 촉진과 상시적 제도운영을 뒷받침할 **법·제도적 기반을 완성**한다.

※ (정비검토 대상) ▲정보통신망법(과기정통부/법무부), ▲개인정보보호법(개보위), ▲국가정보보안 기본지침(국정원), ▲저작권법 지침(문체부), ▲기타 민·형사 리스크방지 지원(법무부)

◇ 안건 4. AI시대 과학기술 경쟁력 대도약을 위한 K-문샷 추진전략(안)

제4호 안건으로는 **AI 기반 과학 패러다임으로의 전환**을 **우리나라가 글로벌 과학기술 선도 국가로 대도약하는 기회로 활용**하기 위한 「**AI시대 과학기술 경쟁력 대도약을 위한 K-문샷 추진전략(안)**」을 심의·의결하였다.

동 전략은 ❶**AI를 활용해 국가 과학기술혁신을 가속화**하고, ❷이를 통해 **국가적 미션을 해결**하는 **두 가지 전략으로 구성**된다. 전략 ❶은 (가칭)**국가과학AI연구센터**를 중심으로 **연구데이터, GPU, AI모델, 자율실험실 등 과학기술 AI 핵심 자원을 통합**하고, **산학연 삼각협력체계를 구축하는 것을 주요 내용으로 한다.**

전략 ❷는 **산학연이 공동으로 직면한 8대분야* 12대 국가적 미션**을 **'35년까지 과학기술×AI로 해결**하는 것을 목표로 한다. 이를 위해 미션별로 **책임과 권한이 있는 PD**(Program Director)를 임명하고, **행정력, 예산 등 자원을 집중 지원**하는 **PD 중심 책임운영체계를 구축**하여 **'35년까지 가시적 성과를 창출**할 계획이다.

* 첨단바이오, 미래에너지, 피지컬AI, 우주, 소재, AI과학자, 반도체, 양자

◇ 안건 5. 국가인공지능전략위원회 운영세칙 일부개정안

제5호 안건으로는 AI기본법 시행('26.1.22)에 따라 법정 위원회로 전환된 **위원회**가 **강화된 역할**을 **효율적**으로 **수행**하기 위해 **분과/TF** 등 **내부 조직**을 **개편**하는 내용 등을 담은 **'국가인공지능전략위원회 운영세칙 일부개정안'**을

의결하였다.

위원회는 **AI 민주주의 아젠다 확대**에 **대응**하여 AI시대 거버넌스 발전, 국민 통합 등에 관한 사항을 심층 논의하는 **'AI 민주주의 분과'**를 **신설**한다. 또한, 기존 과학·인재 분과에서 **인재** 부분을 **교육TF**와 **통합**하여 **'교육·인재 분과'**를 **신설**한다. **지역, 보안** 등 정부 기관 간 지속 협력이 필요한 **중장기 이슈**의 경우에는 기존의 **한시 TF**를 **특별위원회**로 **전환**해 운영토록 하며, **AI 관련 현안**에 **유연**하게 **대응**하기 위한 **한시전담팀(TF)**의 **설치·운영 근거** 또한 **마련**한다.

아울러, 보다 **많은 정부 부처**가 **위원회 논의**에 **참여**할 수 있는 **근거**를 **마련**한다. 위원회는 그 취지에 따라 이번 전체회의에 AI기본법상의 정부위원(16개 부처)뿐 아니라, 성평등부, 공정위, 국가데이터처가 참석하여 의견을 개진할 수 있도록 하였다.

앞으로도 위원회는 **국가 인공지능 정책의 컨트롤타워**이자 **부처 간 정책 조정·협력 플랫폼**으로서의 **기능**을 보다 **효율적**으로 **수행**하기 위해 **노력**해 나갈 방침이다. 아울러, 위원회는 **범정부 차원**의 **체계적·일관적**인 **입법 방향**을 **제시**하기 위해 법률 전문가 등으로 구성된 **법률TF**를 **발족**할 계획이다.

구윤철 경제부총리 겸 재정경제부 장관은 "**인공지능행동계획**의 진정한 성과는 **실행 과정**의 **디테일**에 있다고 하면서 **현장 중심**으로 정책추진상황을 **상시 점검**하고 **국민 체감**이 큰 사업의 **선택과 집중**을 통해 **성공 사례**를 **조기에 창출**해야 한다"고 강조했다. 아울러 "AI는 **성장, 고용, 산업 구조, 소득 분배**까지 영향을 미치는 **핵심 경제 변수**인 만큼, **AI 사회**로의 전환 과정에서 **부담**과 **성과**가 **공정**하게 **분배**될 수 있도록 **일자리 구조 변화**와 **산업·지역 간 격차**에 대한 **대응**도 지금부터 치열하게 준비해야 한다"고 강조했다.

배경훈 과기부총리 겸 과학기술정보통신부 장관은 "정부 출범 이후 **국가AI전략위를 중심**으로 민관이 함께 총력을 다한 결과 **우리나라도 AI 3강의 토대를 만들었다**"며, "이제는 **국민이 체감할 수 있는 과제를 구체화하고, 속도감 있게 이행**해야 하는 시기인 만큼 **모든 부처**가 **본격적인 성과 창출**을 위해 **협력하는 것이 중요**하다"고 강조했다.

임문영 위원회 상근 부위원장은 "오늘 **「대한민국 인공지능행동계획」**을

비롯한 **주요 정책**들의 **의결**을 통해, 앞으로 **우리 정부**가 **추진**해 나갈 **방향**이 보다 **구체적**으로 **설계**되었다"며, "**각 부처**는 최종 확정된 인공지능행동계획을 **책임 있게 이행**해 주길 바라며, **위원회**는 이에 필요한 **정책적 조율**과 **지원**을 아끼지 않을 것"임을 밝혔다. 아울러, "**현장**의 **작은 과제** 하나하나가 **모여 국가경쟁력**을 **좌우**한다는 인식 아래, **위원회**는 **정책 현장**을 **직접 점검**하며 **실질적인 성과**로 이어질 수 있도록 **면밀히** 챙겨나가겠다"고 강조했다.

붙임 1. 회의 개요
2-1~5. 안건별 주요 내용

별첨. 안건 1~4

담당 부서 <총괄&안건1>	국가인공지능전략위원회 지원단 총괄전략팀	책임자 담당자 담당자	팀 장 사무관 사무관	김보경 (02-2224-4121) 이상민 (02-2224-4122) 조은형 (02-2224-4123)
담당 부서 <안건2>	국가인공지능전략위원회 지원단 총괄전략팀	책임자 담당자	팀 장 사무관	김보경 (02-2224-4121) 이상민 (02-2224-4122)
담당 부서 <안건3>	국가인공지능전략위원회 지원단 AI데이터·규제혁신팀 국가인공지능전략위원회 지원단 대외협력팀	책임자 담당자	팀 장 전문관	유경태 (02-2224-4131) 이승호 (02-2224-4145)
담당 부서 <안건4>	과기정통부 연구개발정책실 미래전략기술정책과	책임자 담당자	과 장 사무관	이우진 (044-202-4620) 여동재 (044-202-4632)
담당 부서 <안건5>	국가인공지능전략위원회 지원단 총괄전략팀	책임자 담당자	팀 장 사무관	김보경 (02-2224-4121) 이상민 (02-2224-4122)

붙임1 회의 개요

□ 개 요

○ 일 시 : ‘26. 2. 25.(수) 10:00 ~ 11:00 (총 60분)

○ 장 소 : 국가인공지능전략위원회 지원단 회의실 (서울스퀘어 16층)

○ 안 건 : 총 5건

① 대한민국 인공지능행동계획(인공지능 기본계획(2026~2028))(위원회·과기정통부, 공개)

② AI정부 인프라 거버넌스·혁신 추진방향(위원회, 공개)

③ 보안 취약점 신고·조치·공개 제도 도입 로드맵(위원회, 공개)

④ AI시대 과학기술 경쟁력 대도약을 위한 K-문샷 추진전략(안) (과기정통부, 공개)

⑤ 국가인공지능전략위원회 운영세칙 일부개정안(위원회, 비공개)

□ 세부 일정(안)

시 간	행사 내용
10:00~10:05	▪ 모두 말씀
10:05~10:58	▪ 안건 설명 및 심의·의결
10:58~11:00	▪ 회의 마무리

붙임2-1 「대한민국 인공지능행동계획(인공지능 기본계획)」 주요 내용

Ⅰ 추진 배경

□ **경제 성장 궤도 재진입**과 **도약**이 결정되는 **중대한 기로**에서 **AI**는 대한민국의 새로운 **혁신 성장**과 **국민 삶의 질 향상**을 견인할 **핵심 수단**

☞ **국가AI전략위를 중심**으로 **민·관 역량**을 **총결집**한 **대응전략 마련** 추진

※ (美) AI리더십 강화를 위한 조치사항 설정 및 연방정부에 지시('25.7월, 'AI 실행계획')
(中) 글로벌 기술 표준 및 다자협력 주도 방침 천명('25.7월, 'AI 글로벌 거버넌스 행동계획)

Ⅱ 추진 경과

□ **'25.9.8.**(국가AI전략위 출범식) **대한민국 인공지능행동계획 추진방향** 수립

○ **'AI 3대 강국 도약' 비전 달성**을 위한 **❶AI혁신 생태계 조성 ❷범국가 AI기반 대전환 ❸글로벌 AI기본사회 기여**라는 **3대 정책축·12대 전략분야***를 제시

* [1]AI고속도로 구축 [2]차세대 AI기술 선점 [3]AI핵심인재 확보 [4]AI모델 확보 [5]AI규제혁신 [6]산업AX [7]공공AX [8]지역AX [9]AI기반 문화강국 [10]AI기반 국방강국 [11]AI기본사회 [12]글로벌 AI이니셔티브

□ **위원회 출범 후 3개월간 100여차례 회의**(8개 분과, 6개 TF 등), **1박 2일 끝장토론, 국가CAIO협의회*** **논의** 등을 거쳐 **초안**을 마련('25.11월)

* **(국가CAIO협의회)** AI미래기획수석 주재, 부처별 CAIO(차관급) 참여

□ 위원회 **출범 100일 기자간담회**(12.15.), **주요 기관·단체**(330개) **설명회**(12.30.), **공개 의견 접수** 등 **폭넓은 소통**을 통해 **총 99개 실행과제**와 **326개 정책권고**를 담은 **「대한민국 인공지능 행동계획」 최종안** 마련

○ 행동계획에는 각 부처가 이행해야 하는 **정책권고** 및 **추진기한**을 제시

* **(주관부처)** 과기(121), 교육(32), 산업(31), 행안(25), 국방(23), 복지(17), 중기(12), 국토(11), 국정원(10), AI전략위(9) 등
(추진기한) '26.1분기 81개(24.8%), '26.2~4분기 185개(56.7%), '27년 이후 60개(18.4%)

Ⅲ 주요 내용

정책축 1 AI 혁신생태계 조성

1 **(AI고속도로 구축) 누구나** 충분한 **AI컴퓨팅·데이터 자원** 등을 **안전**하게 **활용**해 **AI 혁신서비스·기술**을 마음껏 창출하는 **'AI고속도로' 구축**

○ 첨단 GPU와 국산 AI반도체를 토대로 **대규모·강소형 데이터센터**를 **균형 있게 확충**하고, AI대전환을 뒷받침할 **AI·데이터 거버넌스** 정립

* 정부내 AI행정과 AX전략 수립(Chief AI Officer), 이를 뒷받침할 데이터 개방·관리 활용(Chief Data Officer), 기술자문(Chief Technical Officer) 담당 최고책임자의 책임·역할, 협력체계 정립

○ **민간**의 **화이트해커**를 활용한 **선제적·상시 보안점검체계** 도입 등 **보안 패러다임**을 **사후 대처**에서 **사전 예방** 중심으로 전환

2 **(차세대 AI기술 선점) 피지컬AI 1위 달성**('30)을 목표로 핵심기술·데이터를 확보하고, **AI**가 **과학적 발견**을 **가속화***하는 **선순환체계** 구축

* **(美 제네시스 전략('25.11월))** 연방정부·국립연구소의 슈퍼컴퓨팅, 데이터셋 등을 AI플랫폼으로 연계·활용, 에너지·신소재 등 핵심전략 분야의 AI기반 연구혁신을 가속하는 국가 주도 전략

○ 연구 全 과정을 지원하는 도구인 **AI연구동료**를 개발·활용하고, **국가과학AI연구소**를 설립해 **전략기술 과학데이터·AI 허브**로 육성

3 **(AI 핵심인재 확보) 초·중·고 연속적**인 **AI 필수 교육체계**를 **구축**하고, **AI/AX 인재 양성**을 **촉진***하는 한편, **세계 최고 인재**를 **전략적**으로 **유치**

* SW중심대학('25년 58개)를 **AI중심대학**으로 전환·확대, **계약학과** 등 산업수요 기반 인재 양성 확대 등

○ 여러 부처에 걸친 **AI 인재양성 사업**의 **상호 연계** 및 **효율화 방안** 마련

4 **(AI모델 확보) 세계 수준**의 **독자 범용 AI모델** 확보로 **모두의 AI 기반 마련**

○ **의료·바이오** 등 **주요 산업 분야별 특화 모델** 개발로 **신성장동력 창출**

5 **(AI규제혁신)** AI학습에 필요한 **원본 개인정보**와 **저작물 활용***이 **권리 침해**나 이용자의 **법적 불확실성** 없이 **안전**하고 **자유**롭게 이루어지도록 **관련 법제 정비**

* **(거래시장 有)** 거래 활성화 지원, **(거래시장 無)** AI학습 거부권 행사 지원, 거부 표시 없는 경우에만 선사용후보상 원칙 적용

정책축 2 범국가 AI 기반 대전환

6 **(산업 AX)** 글로벌 제조업 1위('30)를 위한 **「제조 AI 2030 전략」** 수립 및 강점 있는 제조·문화·의료분야 AX 통한 **한국형 AI풀스택 수출 전략** 마련

7 **(공공 AX)** 공무원 AI 활용 등을 지원해 **칸막이 행정**을 **해소**하고, **AI기반 통합민원플랫폼**을 **구축** 및 **민간**과 **연계**하여 국민 **편의성** 제고

○ **민간 역량**을 활용해 **공공시스템**을 **효율적**이고 **복원력** 있게 **재설계***하고, 이를 운영할 **통합적**이며 **전문성**을 갖춘 **거버넌스 구축 방안**을 마련

* **국가정보자원관리원 화재**(9.26.)에 **즉각 대응, 대통령 지시**("거버넌스 포함 근본적 개선")에 따라 **AI정부 인프라 거버넌스·혁신 TF**를 **구성**(9.30.) 및 **운영**해 **개선방안** 마련

8 **(지역 AX)** **5극 3특 권역별 성장엔진**에 기반한 초광역 **AX 혁신벨트** 및 K-AI 특화 **시범도시** 조성으로 국가 **균형발전** 견인

9 **(AI기반 문화강국)** **AI기반 콘텐츠 창·제작 지원**체계 구축 및 **K-문화 콘텐츠 산업AX** 발전전략 수립으로 **K-컬처의 지속가능한 성장** 촉진

10 **(AI기반 국방강국)** 국방CAIO·관리체계 수립 등 **국방 AI거버넌스**를 **혁신**하고, **획득체계 개편***으로 국방 AI **도입 지연 해소**

* AI 발전 주기(3~6개월)을 고려, 국방 AI 도입을 전통적 무기 획득(10년 이상) 대비 획기적으로 단축 추진

정책축 3 글로벌 AI 기본사회 기여

11 **(AI기본사회)** **노동, 복지, 교육 등**을 포함한 **국민 일상 전반**을 **AI로 보장**하는 '**AI기본사회 추진계획**' 수립

○ **복지 신청주의**를 **탈피***한 **AI기반 복지 모델** 수립, 응급·원격의료 혁신으로 **AI기본의료**를 구현하고, **인간-AI**가 **협업**하는 **고용생태계** 구축

* 「사회보장기본법」, 「사회보장급여법」, 「아동수당법」, 「저출산고령사회기본법」, 「에너지법」 등 관련법 개정 추진

12 **(글로벌 AI이니셔티브)** **APEC AI 이니셔티브**를 필두로 UN, AI서밋 등에서 **기술·규범 연대를 주도**하는 **K-AI 이니셔티브 의제** 적극 확산

○ (가칭)**아태지역 AI허브 특화지구** 조성 등 **전략적 글로벌 AI협력체계** 구축

붙임2-2 「AI정부 인프라 거버넌스·혁신 추진방향」 주요 내용

1. 배 경

□ 이번 국정자원 화재('25.9.26~9.27)는 **정부**가 **직접 구축·관리**하는 폐쇄적 **공공 정보화 시스템**의 **구조적 취약성**을 드러낸 사고

⇨ 대통령 지시('25.9.28)에 따라 **공공 정보화 관리 시스템**의 **근본적 재설계** 추진

○ 예산·조직의 **양적 확대** 등 **미봉책**을 넘어, 정부가 직접 운영하는 **폐쇄적 패러다임 한계**를 극복하고 **AI 네이티브 공공 서비스**로 개편

※ 국가AI전략위 산하 AI정부 인프라 거버넌스·혁신 TF 구성·운영('25.9.30~)
- 공동리더 : AI미래기획수석(정부), 아토리서치 대표(민간)

2. 문제점 진단

○ **(안전조치 소홀) 배터리-서버 未분리** 등 데이터센터 안전이 **민간 수준**에 비해 미흡하고, **국정자원 대전센터**(KT연구소 건물 임대 중) **한계 도달**

※ 행정·공공기관 1·2등급 시스템 운영시설의 69.5%가 배터리실 미분리('25.6월)

○ **(재해복구체계 미비) 국정자원 내 Active-Active DR** 구축이 **全無**하고, 기관은 배정된 예산 범위 내에 **일관된 기준 없이 DR** 구축

○ **(비전문적·혼재된 거버넌스)** 민간에 비해 **전문성**이 **부족**한 **공무원** 및 **원청·하청 인력**에 개발·운영을 의존하고, **총괄적 위기관리 체계 부재**

3. 중점 추진방향

(1) AI정부 인프라 안전조치 강화

□ **정부·공공 부문 데이터센터 안전 관리체계 강화**

○ **민간 수준 이상**으로 **배터리 안전기준 강화**를 위해 공공 정보시스템 **운영시설 안정성 기준**(전자정부법 하위 고시) **개정**('26.2.11 개정 고시 시행)

○ **전체 행정·공공 시스템 운영시설**(1,474개) **특별조사**(~'26.1분기) 및 **1·2등급 시스템 운영시설** 중심 배터리·서버 분리 여부 **현장점검**(~'26.2분기)

○ **국정자원 대전센터**는 **'30년까지 폐쇄** 및 시스템 단계적 이전 추진

□ **재난 대비 모의훈련 강화**

○ DR 구축 기관에 대한 **실전형 재해복구훈련** 실시(年 1회 이상) **의무화**

(2) AI정부 인프라 혁신

□ 재해복구체계(DR) 및 민간 클라우드 활용 방향 정립

○ 국민 생활 영향도 등 고려하여, **시스템 유형별 복구 목표 기준** 및 **DR 구현 방식**(Active-Active, Active-Standby, 스토리지 DR 등) 마련·고도화

< 시스템 유형별 복구 목표 시간 및 DR 구현방식(안) >

구분	복구 목표 시간	DR 구현방식
국가핵심 시스템(A1)	**실시간~1시간 이내**	Active-Active DR
대국민 필수 시스템(A2)	**3~12시간 이내**	Active-Standby DR
행정 중요 시스템(A3)	**1~5일 이내**	스토리지 DR

※ A1·A2·A3등급 外 국민·행정 일반 시스템(A4등급)은 "소산 백업" 구현
※ 복구 목표 시간을 범위로 설정하더라도, 각 기관은 구축환경에 맞게 최대한 단축 노력

○ 데이터 중요도에 따라 **C등급**(기밀) 데이터는 **정부·공공 데이터센터**, **S**(민감)·**O등급**(공개) 데이터는 **민간 클라우드**로 이관하는 방향으로 추진

□ 국정자원 재해복구체계(DR) 구축 및 시스템 재배치

○ '26년에는 **국정자원 대전센터** 시스템(693개) 등을 대상으로 **134개 DR** 우선 구축(Active-Active DR 13개, 스토리지 DR 121개)

- Active-Active DR 중, **3개 시스템(디브레인, 우편정보시스템, 안전디딤돌)** 중심으로 **민간 클라우드 전환 및 DR 구축 선도 프로젝트** 추진

○ 시스템 등급 분류 등 고려하여, **국정자원 內 시스템 재배치 로드맵** 마련

- 국정자원 대전센터 시스템 중, 별도 ISP 없이 **'26년에 민간 클라우드 이전 시스템**(50개 예상) 선정 및 **우선 이전** 추진

(3) AI정부 인프라 거버넌스 개편

□ AI정부 인프라 총괄 전담조직 신설

○ **과학기술부총리** 산하에, 관계부처(과기·행안부, 기획처 등) 합동 가칭 **AI정부 인프라 거버넌스·혁신 추진단** 신설

- **중앙행정·공공기관** 시스템 구축·운영의 **적정성 검토** 및 **위기관리 방안 수립·점검**을 수행하고, 과학기술관계장관회의에서 심의·조정

- **英 정부디지털청(GDS)** 등 해외 사례 고려, 기술·혁신 기능과 디지털정부 기능을 통합하는 방향의 **중장기 거버넌스 재설계 방안** 마련

붙임2-3 「보안 취약점 신고·조치·공개 제도 도입 로드맵」 주요 내용

Ⅰ 추진 배경

□ **초연결 디지털 의존사회·AI시대**, 전통적 **정보보안 체계의 무력化 시작**

○ **AI·클라우드** 기반 초고속 **대규모 사이버 공격 등장과 함께** 파일리스(Fileless) 공격, 공급망 침투 등 기존 **방어우회 신종 위협 확산**

□ 지난 **2025년**은 이러한 **잠재적 위협**이 **현실화** 된 해

○ 침해 사고의 양적 증가뿐 아니라 **대형·중대사고도** 연쇄 발생, **국가행정망**까지 뚫리며 **사이버 위협**의 **안전지대가 '소멸 위기'**에 **직면**

※ (침해사고) '24년 1,887건 → '25년 2,383건(약 26.3% 증가) (KISA) / (대형·중대사고) '25.4 SKT, '25.9 KT, '25.11 쿠팡, / (행정망 해킹) '25.10월 행안부 인정

☞ 기존 정보보안 **체계로는 더 이상 한계, 근본적인 패러다임 변화 필요**

※ (VIP, '25.12.2 국무회의) "**초연결 디지털 사회를 맞이해 민간·공공을 아우르는 '패러다임 시프트' 수준의 새로운 디지털 보안제도** 마련 필요"

Ⅱ 국내 정보보안 제도와 해외 현황

□ **(국내)** 국내 **정보보안 체계는 1회성, 정적점검 위주로 근원적 한계 내재**

○ 정보보안 **인증·점검·평가 등 제도는 年 1회 또는 제품 도입시**에만 실시, **절차점검 위주로** 실시간 **진화**하는 **사이버 위협** 대응에 역부족

※ **(인증)** ISMS, ISMS-P → 年 1회 체크리스트 점검, **(점검)** 보안적합성 검증, 개인정보 영향평가 → 도입시 검증, **(평가)** 개인정보 수준평가, 사이버보안실태 평가 → 절차평가 중심

○ **정보보호 책임자 지정과 관련 공시** 등 제도는 보안 **인력과 투자**의 양을 늘리는 데에는 **기여**하나 **'방어의 질'**은 **보장**하지는 못하는 실정

※ **SKT, KT, LGU+, 쿠팡은 모두 ISMS 인증 획득 및 정보보호 공시·책임자 지정에도 불구 사고 발생**

< 국내 정보보안 제도 현황 >

구분		과기정통부	개인정보위	국정원
보호 관할		민간 정보통신망 보호	민간·공공 개인정보 보호	국가·공공기관 사이버 보안
운영제도	사전 예방	정보보호공시, 정보보호책임자 지정	개인정보보호책임자 지정, 개인정보영향평가(시스템 도입시)	보안성 검토, 보안적합성 검증(장비 도입시)
	주기적 대응	정보보호인증(年1회), 취약점 신고포상제(年중)	개인정보보호인증(年1회), 개인정보 보호수준 평가(年1회)	사이버보안관리실태평가(年1회), 사이버보안훈련(年1회)
	사고시 제재	2년 이하 징역 또는 2천만원 이하 벌금	전체 매출의 3% 이내 과징금 / 5년 이하 징역 또는 5천만원 이하 벌금	원인분석, 결과통보, 유출 자료 국가안보 영향 평가 등
한계		**실시간** 이루어지고, **상시적으로 고도화**되는 **해킹**에 대한 **방어능력 검증, 대응능력 향상과 동떨어진 상황**		

□ **(해외)** 美·EU는 우리나라와 달리 민간(화이트해커)과 협력, **상시적·선제적**으로 보안 **취약점을 신고·조치**하고 **공개**(CVD/VDP*)하는 **정책** 운영

* **C**oordinated **V**ulnerability **D**isclosure : 조정된 취약점 공개 / **V**ulnerability **D**isclosure **P**olicy : 취약점 공개 정책

[참고] 취약점 신고·조치·공개제도(CVD/VDP) 개요 및 국내 관련 현황

■ **(개요) 기업·기관**이 **자사 정보통신망·제품** 등에 대해 **화이트해커가 취약점을 상시 발굴**할 수 있게 관련 정책을 공개(해킹범위·신고절차 등)하고(=VDP), **화이트해커**는 해당 정책을 준수, **취약점**을 **발굴·신고**하며 기관은 **신고된 취약점을 조치**하고 공개(=CVD)

■ **(국내)** 화이트해커의 **정보통신망 침입 행위**가 선의의 목적이어도 **불법**으로 **간주**(정보통신망법 위반)되어 **제도 미운영** ⇨ **정보통신망이 아닌 제품**(SW) 만을 대상, 취약점을 신고하면 포상하는 **'신고 포상제'***만 운영(신고 취약점에 대한 **조치 강제력 부재)**

* 과기정통부·KISA 운영 / 분기별 1회 총 1천만원 수준 포상금(기업이 아닌 정부가 지급)

○ **해당 제도** 운영을 **美는 공공 의무화, 민간**은 공공조달 필수요건 연계 등 **참여** 유인, **EU는 공공 의무화**에 **민간도 상당부문** 의무화*(또는 추진 중)

* [대상] 에너지, 은행, 택배 등 국민 생활 필수·중요 분야 서비스(완료) + 제품 전체(추진 중)

○ **제도도입 배경**에는 **'10~'20년대 세계적 대란 수준**의 보안사고 존재

※ (워너크라이, '17) 美국가안보국이 발견했으나 미공개한 윈도우 취약점이 150개국 해킹 활용 / (솔라윈즈, '20) 취약점 SW업데이트 파일이 美연방기관 연쇄 해킹

- 해당 사태를 계기로 정보보안에 대한 **인식**이 **기존 내부인력 위주 폐쇄적 대응·사후 조치**에서 **개방형 협력·사전 대응**으로 변화

※"우리가 의존하는 기술의 안전보장을 정부 혼자서 해낼 수 없다. 취약점을 식별/수정하기 위해 민간 화이트 해커의 도움이 필요하다."(美 사이버인프라보안국 국장, '21)

☞ 이러한 시대적 상황은 바로 **우리나라가 지난해** 겪은 **보안사태**와 유사

Ⅲ 고려 사항 및 제도 도입 방안

[참고] 국가AI전략위원회 전문가, 관계부처 논의 경과

- **(전문가 논의) 해커원**('25.12.24) ※ 전 세계 최대 화이트해커(240만명 가입) 플랫폼
- **(관계부처 협의) 과기정통부, 국정원, 개인정보위, 법무부, 조달청** 등 ※ 총 5차례
- **(시민단체 의견수렴) 민변·시민사회·장애인** 인권단체 소속 사회분과 위원('25.12.30)

1 주요 고려 사항

❶ **(인식·평판)** 해당 제도로 취약점이 **공개될** 시 보안 실패로 간주되어 **기업·기관 이미지 실추 우려**, 해커에 대한 부정적 시각도 여전

☞ 참여기업·화이트해커가 **보안향상 우수 기업·기여자**라는 **인식 형성**과 함께 **기업·해커들**에 대한 보호 제도 동반 필요

❷ **(책임 소지)** 정보통신망 침입 이외에도, **취약점 탐색 과정**에서 의도치 않은 **개인정보 확인**, 정보통신망 저해 등 다양한 **책임 소지** 존재

☞ **기업·화이트해커가 책임**질 수 있는 **부문**과 **그렇지 않은 부문**을 명확히 하고, 책임질 수 있는 부문에 대한 **법·제도적 보호장치** 필요

※ (예 : 美 국방부 요구사항) 취약점 탐색 관련 △어떠한 경우에도 데이터 유출 금지, △상업적·재정적 이익 고의침해 방지, △접근권한 없는 정보노출 시 영구삭제 및 국방부 보고

❸ **(역량)** 제도 운영이 **기업·기관의 업무 마비**를 일으킬 **가능성**(전담 인력·예산 부족), 충분한 화이트해커 확보와 관련 역량도 필요

☞ **기관 역량**을 고려해 **단계적**으로 **확대**하고, 제3기관을 활용한 **제도 도입·운영 지원**과 함께 국내 화이트해커 등 **보안 인력 육성 필요**

2 도입 방안

○ **(대상)** 초기에는 **참여 기업·기관 모집**을 통해 시행하되 궁극적으로는 美와 유사하게 **공공**은 **의무화**, **민간**은 **전면적인 참여 유도** 목표

○ **(운영 방식)** 美·EU와 동일하게 대상 기관, 기업이 정한 **정책 범위 내** 화이트 해커에게 **모든 정보통신망·서비스**에 대한 **취약점 탐지** 허용

- **피신고 기업·기관**은 **취약점**을 **조치**하고 조치한 이후, 화이트해커와의 협의를 통해 일정시일 내 **기업·기관명/취약점** 등 공개

- 다만, **기업·기관·화이트해커 실명**은 본인 의사를 고려해 **익명 공개** 허용

- **영세 기업·기관**에 대해서는 KISA 등을 통해 1차 취약점 신고 접수와 선별, 기관 전달 등을 수행하고, **취약점 조치 지원**도 병행*

* AI취약점 자동 분석·검증 플랫폼 구축, API 보급 등 지원 병행

○ **(참여 유인) 공공**은 **기관 평가** 연계, **민간**은 보안인증 가점·**공공조달 우대, 화이트 해커는 신고 포상제 활성화로** 초기 참여 유도

- 특히 **개보법**에 따른 **사고시 과징금**에 해당제도 운영 노력을 **감경**요소로 반영

○ **(보호 장치)** 초기에는 **참여기업·기관-화이트해커 상호 협의**하에 운영하되, 궁극적으로는 관계 **법률 개정**을 통해 **민·형사 처벌 면제 명확화**

○ **(인식 개선)** 화이트 해커와 제도 참여 기업·기관, 정부간 **협력 네트워크** 구축 및 홍보 캠페인, **정부표창 수여 등 인식개선** 추진

Ⅳ 추진 로드맵

□ **(1단계 : 시범사업(~'26)) 민간 분야는 과기정통부, 공공 분야는 국정원** 주도로 **시범 사업**을 운영, 국내 제도 도입 가능성과 효과를 사전 검증

※ (예) 5~10개 선도기관(기업/공공기관)과 KISA, 화이트해커 등 참여, 해당 제도 실효성을 현실 환경에서 검증, 규제샌드박스 제도 연계로 최대한 美·EU와 유사한 환경 조성

□ **(2단계 : 참여 확대(~'27)) 시범사업 바탕 민간**(과기정통부)·**공공**(국정원) **분야 제도 설계 및 관련 가이드라인 마련·배포, 관계부처 참여유인 제공**

□ **(3단계 : 법제화(2단계 상황 고려, 최대한 조속히 추진)) 관계 법령 개정 완료**

※ (정비검토 대상) 정보통신망법(과기정통부/법무부), 개인정보보호법(개보위), 국가정보보안 기본지침(국정원), 저작권법 지침(문체부), 기타 민·형사 리스크방지 지원(법무부)

Ⅴ 향후 계획

□ **민간(과기정통부)·공공(국정원) CVD/VDP 시범 사업 시행** : '26.하반기

붙임2-4 「AI 시대 과학기술 경쟁력 대도약을 위한 K-문샷 추진전략」 주요 내용

□ 개 요

○ 최근 과학 연구는 **AI가 가설 생성, 실험 설계, 데이터 수집·분석 등 전 과정에서 혁신을 창출**하는, 이른바 **'제5차 패러다임'** 돌입

☞ **AI 시대 과학기술 경쟁력 대도약**을 위해 **산학연이 결집, 파급력이 큰 국가적 미션을 AI로 해결**하는 **범국가 프로젝트 'K-문샷' 추진**

□ 주요 내용

○ **(전략 1) 국가 과학기술 AI 자원·역량 총결집**

- **(과학기술 AI 연구 자원)** 국가 연구데이터 수집·활용 기반, GPU(8천장 이상), 분야별 파운데이션·특화 AI 모델, 자율실험실 등 **핵심 자원 결집**
- **(자율형 AI 과학자)** 가설 수립, 실험, 결과 분석 등 **과학적 탐구 전 과정을 AI가 스스로 반복, 난제 해결에 기여**하는 시스템 구축
- **(산학연 삼각협력체계 구축)** 바이오, 소재, 휴머노이드 등 **임무별 산학연 역량을 총결집**하여 **과학기술 AI 성과 창출 가속**

○ **(전략 2) 과학기술×AI를 활용한 국가적 미션 해결**

- **(미션 구체화)** 대국민 공모, 전문가 기획 등으로 **발굴한 미션 후보**에 대해 **적절성 평가 및 범부처·전문가 의견수렴**을 거쳐 최종 선정
- **(PD 책임운영체계 구축)** 미션 달성을 위한 **책임과 권한이 있는 PD**(Program Director)를 지정, **행정, 예산 등 가용 자원 지원**
- **(대국민 보고)** 부총리 겸 과기정통부 장관을 단장으로 **'K-문샷 추진단'**을 구성, 마일스톤 기반의 **주기적 진도 점검, 주요 성과는 대국민 공개**

□ 향후 계획

○ 핵심 미션 확정 및 전담지원기관·PD 지정('26.3월, 제5차 과기관계장관회의)

○ K-문샷 지원단 구성('26.3월 말) 및 신규 사업 기획('26.4월)

붙임2-5 「국가인공지능전략위원회 운영세칙 일부개정안」 주요 내용

□ 개요

○ 「인공지능기본법」 시행에 따라 **법률상 기관**으로 전환되는 **위원회**의 **강화된 역할**을 **효율적**으로 **수행**하기 위한 분과 등 **위원회 조직 개편**

□ 주요 내용

○ 위원회 설치·운영의 근거가 대통령령에서 법률로 전환됨에 따라, 운영세칙에서 인용하는 상위법령 변경 사항을 반영

○ **위원회 회의**에 정부위원 외에도 **안건 관련 중앙행정기관**이 **참석**할 수 있는 **근거**를 **마련**

○ 기존 8개 분과를 **10개 분과**로 **확대 개편**

- **AI 민주주의 분과**를 **신설**하고, 기존 과학 및 인재 분과를 분리하며, 인재 부분은 기존 교육 TF와 통합해 **교육·인재 분과 신설**

현행	개정안
1. 기술혁신 및 인프라 분과 2. 과학 및 인재 분과 3. 산업 AX 및 생태계 분과 4. 공공 AX 분과 5. 데이터 분과 6. 사회 분과 7. 국방 및 안보 분과 8. 글로벌 협력 분과	1. (현행과 같음) **2. 과학 분과** 3. (현행과 같음) 4. (현행과 같음) 5. (현행과 같음) 6. (현행과 같음) 7. (현행과 같음) 8. (현행과 같음) **9. AI 민주주의 분과 (신설)** **10. 교육·인재 분과 (신설)**

○ 분과 내에 소분과를 구성·운영할 수 있는 근거를 마련하고, 회의 기록 공개 원칙과 위원의 제척·회피 사항 등을 규정

○ **지역특별위원회**와 **보안특별위원회**를 **신설**

○ AI 관련 **현안 대응**을 위한 **한시전담팀(TF)**의 설치·운영 근거 마련