



제 439회 국회 (정기회)
제1차 과학기술정보방송통신위원회

인공지능 발전과 신뢰 기반 조성 등에 관한 기본법 일부개정법률안

검 토 보 고

〈공공기관의 인공지능시스템 도입·활용 시 보안 조치 근거 마련〉
■ 채현일의원 대표발의(의안번호 제2220070호)

2026. 9.

과학기술정보방송통신위원회

수석전문위원 이지민

목 차

I . 제안경위	1
II . 제안이유 및 주요내용	1
III . 검토의견	2
1. 공공기관의 인공지능시스템 도입·활용 시 보안 조치 근거 마련	2

I. 제안경위

가. 발 의 자 : 채현일의원 등 12인

나. 발 의 일 : 2026. 7. 21.

다. 회 부 일 : 2026. 7. 22.

II. 제안이유 및 주요내용

최근 사용자의 컴퓨터에서 파일 열람, 명령 실행, 해외 서버 전송 등의 기능을 자율적으로 수행하는 방향으로 인공지능시스템이 개발되어 널리 활용되고 있음. 공공기관에서도 인공지능시스템을 활용하는 사례가 대폭 증가하였을 것으로 추정되나, 외부의 인공지능시스템이 공공기관이 보유·관리하는 공공·민간데이터에 접근함에 따라 발생할 수 있는 문제의 예방·대응에 관한 사항은 현재 훈령 또는 가이드라인 수준에서 규율되고 있음.

이에 공공기관에서 인공지능시스템을 도입·활용하는 경우 사전 보안 심사, 시스템 접근 권한의 통제, 데이터 외부전송의 차단 및 로깅 의무 부여 등 필요한 조치를 하도록 법률에 명시하려는 것임(안 제32조의2 신설).

Ⅲ. 검토의견

1. 공공기관의 인공지능시스템 도입·활용 시 보안 조치 근거 마련

가. 개정안의 내용

- 개정안은 공공기관에서 정책 수립 및 의사결정에 인공지능시스템을 도입·활용하기 위해서는 해당 인공지능시스템에 대한 보안조치를 하도록 하려는 것임(안 제32조의2 신설).

현 행	개 정 안
<u><신 설></u>	<u>제32조의2(공공기관의 인공지능시스템 보안) 공공기관의 장은 인공지능시스템을 정책 수립 및 의사결정에 도입·활용하려는 경우에는 다음 각 호의 조치를 하여야 한다.</u> <u>1. 해당 인공지능시스템의 이용에 따른 보안 위험의 분석·평가 및 대응</u> <u>2. 해당 공공기관의 데이터 보유·관리 등을 위한 정보체계에 대한 접근 권한의 관리·통제에 필요한 조치</u> <u>3. 해당 인공지능시스템에 의한 공공데이터 유출의 예방 및 차단에 필요한 조치</u> <u>4. 해당 인공지능시스템의 접속기</u>

현행	개정안
	록, 입·출력기록 등 대통령령으로 정하는 정보의 취득·보관에 필요한 조치 5. 그 밖에 인공지능시스템의 이용과 관련하여 공공기관이 보유·관리하고 있는 데이터의 보안 유지에 필요한 조치로서 대통령령으로 정하는 조치
부칙	
제1조(시행일) 이 법은 공포 후 6개월이 경과한 날부터 시행한다. 제2조(공공기관의 인공지능시스템 보안에 관한 적용례) 제32조의2의 개정규정은 이 법 시행 당시 공공기관이 인공지능시스템을 도입·활용하고 있는 경우에도 적용한다.	

나. 검토의견

- 인공지능기술이 빠르게 발달하면서 업무의 효율화를 위해 민간뿐만 아니라 공공부문에서도 인공지능시스템의 도입·활용이 활성화되는 추세임.
- 국가정보원이 2025년에 중앙행정기관·공공기관·지자체 등 300개 기관을 대상으로 조사한 결과에 따르면, 2023~2024년에 다수의 기관이 기관 내·외부 대용량 데이터 분석을 위하여 예측형 인공지능시스템을 도입하였고, 보고서 생성, 민원대응 등을 위하여 생성형 AI를 도입하는 기관의 비중이 2024년 34%에서 2025년 77%로 급증하였음.

○ 그런데, 공공기관은 전 국민에 대한 방대한 데이터를 보유하고 있고 여기에는 민감정보도 다수 포함되어 있어 보안 문제로 공공기관의 데이터가 유출될 경우 피해가 클 것으로 예상되고,

이와 더불어, 사이버보안 위협으로 공공서비스에 지연·장애가 발생할 수 있으며 이에 따른 국가적 피해 또한 심각할 것이라는 점을 고려할 때, 공공기관의 인공지능시스템 도입·활용 시 사전적으로 보안 조치를 취하도록 할 필요성이 있음.

○ 이와 관련하여, 현재 공공기관에서 인공지능시스템을 포함한 정보시스템을 도입·구축하는 경우, 이에 대한 보안 점검·관리에 대해서는 국가정보원이 업무를 수행하고 있음.

- 「국가정보원법」 제4조제1항제4호는 중앙행정기관 등에 대한 기관 대상 사이버공격 및 위협에 대한 예방 및 대응을 국가정보원이 수행하는 직무로 명시¹⁾하고 있고,

대통령령인 「사이버안보 업무규정」에 따라 국가정보원은 사이버보안 업무에 관한 기본지침을 수립하여야 하며, 중앙행정기관 등이 실시하는 정보화사업에 대한 보안성 검토를 실시하고 그 결과의 이행 여부를 확인²⁾할 수 있으며, 통합보안관제체계를 구축·운영하는 등 공공기관 사이버

1) 「국가정보원법」

제4조(직무) ① 국정원은 다음 각 호의 직무를 수행한다.

4. 다음 각 목의 기관 대상 사이버공격 및 위협에 대한 예방 및 대응

가. 중앙행정기관(대통령 소속기관과 국무총리 소속기관을 포함한다) 및 그 소속기관과 국가인권위원회, 고위공직자범죄수사처 및 「행정기관 소속 위원회의 설치·운영에 관한 법률」에 따른 위원회

나. 지방자치단체와 그 소속기관

다. 그 밖에 대통령령으로 정하는 공공기관

보안에 관한 업무를 수행함.

- 또한, 「국가 사이버보안 기본지침」에 따르면, 국가정보원이 실시하는 보안성검토의 대상이 되는 정보화사업에는 ‘인공지능을 활용하는 정보통신망 또는 정보시스템 구축’이 포함되어 있고, 각급기관의 장은 인공지능시스템을 구축·운용하고자 할 경우 보안대책을 수립·시행하여야 하며, 이 때 국가정보원장이 배포한 「AI 보안 가이드북」 등 AI 보안 관련 가이드라인을 활용하도록 노력하여야 함³⁾.

○ 한편, 현행법 제16조는 국가·지자체가 공공기관의 인공지능기술 도입 촉

2) 「사이버안보 업무규정」

제3조의2(사이버안보 업무의 기획·조정) ① 국가정보원장은 제3조제1호에 따른 사이버안보정보 업무(이하 “사이버안보정보 업무”라 한다) 및 같은 조 제2호에 따른 사이버보안 업무(이하 “사이버보안 업무”라 한다)에 관한 정책의 수립 등 기획업무를 수행하고, 사이버안보정보 업무 및 사이버보안 업무를 효율적·체계적으로 수행하기 위하여 다음 각 호의 지침 등을 수립·시행해야 한다.

1. 사이버안보정보 업무에 관한 기본지침
2. 사이버보안 업무에 관한 기본지침
3. 새로운 유형의 사이버공격·위협에 대응하기 위한 수시 보안대책

② 국가정보원장은 사이버안보정보 업무 및 사이버보안 업무에 대한 조정이 필요한 경우 국가안보에 중대한 영향을 미치는 긴급사안에 대해서는 직접 조정하고, 그 밖의 사안에 대해서는 제1항제1호 및 제2호에 따른 기본지침으로 정하는 바에 따라 조정한다.

제9조(사이버보안 예방 조치 등) ① 국가정보원장은 중앙행정기관등에 대한 사이버공격·위협을 예방하기 위하여 중앙행정기관등의 장이 시행하는 정보화사업(「지능정보화 기본법」 제11조제1항에 따른 지능정보화계획에 따른 사업을 포함한다)에 대하여 보안성 검토를 실시하고, 그 보안성 검토 결과의 이행 여부를 확인할 수 있다.

② 국가정보원장은 중앙행정기관등의 정보보호시스템, 암호장치, 암호모듈 및 보안기능이 있는 정보통신기기(이하 “정보보호시스템등”이라 한다)의 도입·운영 및 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제3호에 따른 클라우드컴퓨팅서비스(이하 이 조에서 “클라우드컴퓨팅서비스”라 한다)의 이용에 관한 보안대책을 수립할 수 있다.

③ 국가정보원장은 중앙행정기관등이 도입·운영하거나 이용하는 정보보호시스템등 및 클라우드컴퓨팅서비스가 제2항에 따른 보안대책에 적합한지 검증할 수 있다

3) 「국가 사이버보안 기본지침」

제15조(검토 기관) ① 국가정보원장은 각급기관의 장이 추진하는 다음 각 호에 해당하는 정보화사업에 대하여 보안성 검토를 실시한다. 다만, 국가정보원장은 정보화사업의 규모·중요도 등을 고려하여 상급기관의 장에게 보안성 검토를 위임할 수 있다.

23. 인공지능을 활용하는 정보통신망 또는 정보시스템 구축

제72조의2(인공지능시스템 보안) ① 각급기관의 장은 인공지능시스템을 구축·운용하고자 할 경우 보안대책을 수립·시행하여야 한다.

② 제1항에 따른 보안대책 수립·시행 시 국가정보원장이 배포한 「AI 보안 가이드북」 등 AI 보안 관련 가이드라인을 활용하도록 노력하여야 한다.

진 및 활용 확산을 위한 시책을 수립·시행하도록 하고 필요한 지원을 할 수 있도록 규정⁴⁾하여, 정부가 공공부문의 인공지능기술 도입·활용을 지원할 수 있는 근거를 마련하고 있으나,

공공부문 내 인공지능시스템 도입·활용 시 필요한 보안 조치나 위험 관리 등에 대해서는 명시하지 않고 있음.

○ 이에 개정안은 공공기관⁵⁾에서 정책 수립·의사결정에 인공지능시스템을 도입·활용할 때 공공기관의 장이 공공기관의 시스템과 보유 데이터를 보호하기 위하여 필요한 보안 조치를 취하도록 규정하려는 것으로,

현재 국가정보원의 지침, 가이드라인 등에 따라 수행하는 공공기관 인공지능시스템 보안 조치 의무를 법률에 명시하여 법적 근거를 강화하려는 취지로 보임.

- 국가정보원이 배포한 「AI 보안 가이드북」에서 제시된 AI시스템 보안대책 체크리스트에는 인공지능시스템 보안 위험 점검·검증, 데이터 접근 통제,

4) 「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」

제16조(인공지능기술 도입·활용 시책 등) ① 국가 및 지방자치단체는 기업 및 공공기관의 인공지능기술 도입 촉진 및 활용 확산을 위한 시책을 수립·시행하여야 한다.

② 국가 및 지방자치단체는 기업 및 공공기관의 인공지능기술 도입 촉진 및 활용 확산을 위하여 필요한 경우에는 다음 각 호의 지원을 할 수 있다.

1. 인공지능기술, 인공지능제품 또는 인공지능서비스의 개발 지원 및 연구·개발 성과의 확산
2. 인공지능기술을 도입·활용하고자 하는 기업 및 공공기관에 대한 컨설팅 지원
- 2의2. 공공기관이 보유·관리하고 있는 데이터를 학습용데이터로 생성·제공하고 적절한 품질 수준을 확보하기 위하여 필요한 지원
3. · 4. (생략)

5. 그 밖에 기업 및 공공기관의 인공지능기술 도입 및 활용을 촉진하기 위하여 대통령령으로 정하는 사항

5) 현행법 제6조제4항에서 ‘공공기관’을 「지능정보화 기본법」 제2조제16호에 따른 공공기관으로 규정하고 있는바, ① 「공공기관의 운영에 관한 법률」에 따른 공공기관, ② 「지방공기업법」에 따른 지방공사 및 지방공단, ③ 특별법에 따라 설립된 특수법인, ④ 「초·중등교육법」, 「고등교육법」 및 그 밖의 다른 법률에 따라 설치된 각급 학교, ⑤ 대통령령으로 정하는 법인·기관 및 단체임.

데이터 활용 기록 명세서 관리, 비상대응 체계 마련, 시스템 로그 기록·분석 등의 조치가 제시되어 있어, 안 제32조의2 각 호에 따른 보안 조치가 이미 국가정보원의 보안 관리에 포함되어 있는 것⁶⁾⁷⁾으로 보임.

○ 또한, 적용례를 통해 기존에 인공지능시스템을 이미 도입한 공공기관에 대해서도 보안 조치 의무가 적용됨을 명확히 하려는 것임.

○ 다만, 개정안은 다음과 같은 사항을 검토할 필요가 있음.

○ 첫째, 안 제32조의2에 따른 공공기관의 보안 조치가 현재 국가정보원이 지침·가이드라인 등에 따라 수행하고 있는 보안 관리 체계를 동일하게 법률에 명시하려는 것인지, 아니면 별도로 새로운 보안 조치 제도가 도입 되는 것인지 문언상 불명확하고,

현재 국가정보원이 수행하고 있는 보안 관리 체계와 별개로 새로운 보안 조치가 신설되는 것으로 해석될 여지가 있는바, 이에 대한 검토가 필요한 것으로 보임.

○ 둘째, 안 제32조의2에 따른 인공지능시스템 보안 조치 의무는 공공기관에만 적용되는데, 현재 국가정보원이 수행하는 사이버보안 업무의 대상에는 공공기관뿐만 아니라 중앙행정기관, 지방자치단체 등도 포함되어 있어, 개정안에 따른 보안 조치의 적용 범위가 현재 사이버보안 업무의 수행 체계와 부합하지 않는 문제가 있어 보임.

6) AI시스템 보안대책 체크리스트의 구체적인 내용은 [참고자료] 참조

7) 국가정보원은 「AI 보안 가이드북」에서 제시하는 AI시스템 보안대책 체크리스트에 안 제32조의2 각 호에 따른 보안 조치가 이미 모두 포함되어 있고, 각급기관의 장이 보안대책을 수립할 때 이를 따르고 있으며, 국가정보원의 보안성검토 시 적용되는 기준에도 AI시스템 보안대책 체크리스트의 사항이 모두 포함된다고 설명함.

- 국가정보원이 수행하는 사이버보안 업무의 대상은 「국가정보원법」 제4조제1항제4호에 따라 ① 중앙행정기관 및 그 소속기관과 국가인권위원회, 고위공직자범죄수사처 및 「행정기관 소속 위원회의 설치·운영에 관한 법률」에 따른 위원회, ② 지방자치단체와 그 소속기관, ③ 그 밖에 대통령령으로 정하는 공공기관⁸⁾임.
- 「사이버안보 업무규정」, 「국가 사이버보안 기본지침」은 국가정보원의 사이버보안 업무 대상을 중앙행정기관등 또는 각급기관으로 규정하여 공공기관뿐만 아니라 중앙행정기관, 지방자치단체 등도 적용 범위에 포함하고 있는 반면, 안 제32조의2에서는 이 중 공공기관에 대해서만 규정하고 있음.
- 이에 따라, 중앙행정기관이나 지방자치단체 등은 기존과 같이 관련 지침이나 가이드라인 등에 근거하여 인공지능시스템에 대한 보안 조치를 이행하는 반면, 공공기관에 대해서만 보안 조치 근거가 법률에 직접 명시되어, 공공부문 내 인공지능시스템 보안 조치의 법적 근거가 서로 달라지는 문제가 발생할 수 있음.

8) 「사이버안보 업무규정」

제7조(사이버보안 업무 대상 공공기관의 범위) 법 제4조제1항제4호다목에서 “대통령령으로 정하는 공공기관”이란 다음 각 호의 기관을 말한다.

1. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관
2. 「지방공기업법」에 따른 지방공사 및 지방공단
- 2의2. 「지방자치단체 출자·출연 기관의 운영에 관한 법률」 제2조제1항에 따른 출자·출연 기관 중 해당 지방자치단체의 조례로 정하는 기관
3. 특별법에 따라 설립된 법인. 다만, 「지방문화원진흥법」에 따른 지방문화원 및 특별법에 따라 설립된 조합·협회는 제외한다.
4. 「초·중등교육법」, 「고등교육법」 및 그 밖의 다른 법률에 따라 설치된 국립·공립 학교
5. 「정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조제1항 및 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조제1항에 따른 연구기관

다. 정부 및 관련 단체 의견

1) 과학기술정보통신부: 신중검토

- 공공기관에서 인공지능시스템을 도입할 때, 보안성을 강화하여 정보유출 사고 등을 예방하고자 하는 법안의 취지에는 공감함.
- 그러나, 공공기관에 도입되는 인공지능시스템은 정보시스템에 포함되므로 정보 보안과 관련된 개별 법령의 적용을 받아 취약점 분석·평가, 보안성 검토 등을 보안 관련 조치를 받고 있으며, 기관별 정보보안 업무에 관한 규정 내지 지침도 마련하여 정보시스템에 대한 접근 권한 및 관리 방법 등을 정하고 있음.
- 따라서, 인공지능기본법에 공공기관 인공지능시스템의 보안과 관련된 규정을 추가하는 것은 국정원·행안부 등 관계기관과 충분한 협의를 거치고 관련 규정·세칙 등과의 정합성을 고려하여 신중한 접근이 필요함.

2) 국가정보원: 신중검토

- 공공기관의 인공지능시스템 도입·활용 시 보안 조치 등에 관한 사항은 다른 개별 법령에서 엄격히 규율되고 있어 인공지능기본법에 관련 내용 신설 시 법적용·해석의 혼란을 초래할 수 있음.
- 또한, 인공지능기본법은 인공지능 관련 산업 활성화를 주된 목적으로 함에 따라 개정안과 같은 규제 조항 신설은 입법 취지에 맞지 않음.

문 의 처
02)6788-5230

※ 참고자료 : AI시스템 보안대책 체크리스트

순번	보안대책 체크리스트 항목	적용여부
1	신뢰할 수 있는 출처의 데이터 활용 - AI모델 학습·재학습에 신뢰할 수 있는 출처의 내·외부 데이터만 사용하였는가?	☐
2	신뢰할 수 있는 출처의 AI모델·라이브러리 활용 - 오픈소스 AI모델·라이브러리 등이 필요한 경우, 신뢰할 수 있는 출처에서 획득하여 사용하였는가?	☐
3	데이터 검사 - AI 학습 前 수집한 데이터에 악의적으로 변조 혹은 비인가 민감정보 등이 포함된 오염데이터가 있는지 검사하였는가?	☐
4	데이터 암호화 - 저장소에 보관된 원시·학습데이터의 외부 유출 및 오염 방지 등을 위하여 암호화하였는가?	☐
5	데이터 접근통제 - 데이터 저장소에 대한 사용자, 데이터, 접근경로별 권한을 부여하고 접근제어를 통해 통제하고 있는가?	☐
6	민감정보 사용 사전 승인 - AI시스템에 민감·비공개 정보를 포함시킬 경우 기관 내부 절차에 따라 사전 보고 및 승인을 받았는가?	☐
7	보안등급에 맞는 학습데이터 구성·활용 - AI시스템 활용 목적 및 등급에 맞게 기밀·민감·공개등급의 데이터를 분류하여 사용하였는가?	☐
8	데이터 로깅·모니터링 - 원시·학습데이터에 대한 접근·변경 등 발생행위에 대해 로그를 기록하고 정기적으로 분석하고 있는가?	☐
9	AI시스템 로깅·모니터링 - 사용자, 단말기 및 AI시스템 등에서 발생하는 AI 입·출력정보를 로그로 기록하고 정기적으로 분석하고 있는가?	☐
10	데이터 수집 명세서 관리 - 학습에 활용한 데이터의 출처, 일자, 수집경로, 해시값 등을 기록하여 이력을 관리하고 있는가?	☐
11	AI시스템 구성요소 명세서 관리 - AI시스템 구성요소에 대한 출처, 버전, 변경이력 등을 명세서로 작성하여 관리하고 있는가?	☐
12	AI시스템 구성요소 무결성 검증 - AI모델, 학습데이터, 라이브러리 등이 원본과 동일한지 여부를 정기적으로 확인하고 있는가?	☐
13	입·출력 필터링 - AI에 입력되는 프롬프트 및 출력되는 결과에 대해 민감정보 혹은 적대적 공격 문구의 포함여부를 확인하여 차단하고 있는가?	☐
14	입력 길이·형식 제한 - AI에 입력되는 프롬프트의 길이·형식·횟수 등을 제한하여 운영하고 있는가?	☐
15	가드레일 다중화 - AI시스템 오작동, 유해한 입·출력, 민감정보 유출 등을 방지하기 위한 보호장치를 계층적 혹은 병렬적으로 배치하여 운영 중인가?	☐

순번	보안대책 체크리스트 항목	적용여부
16	AI모델 구조·가중치 유출 방지 - AI모델의 구조·가중치 등이 외부로 유출되지 않도록 암호화하거나 접근 권한을 통제하고 있는가?	☐
17	AI시스템 경계보안 강화 - AI시스템과 타 시스템의 연계구간에 방화벽 등 정보보호제품을 활용하여 접근통제 하고 있는가?	☐
18	AI시스템 통신구간 보호 - 사용자와 AI시스템 혹은 AI시스템과 타 시스템 통신구간에 인증을 강화하고, 암호화 등 보호조치를 적용하였는가?	☐
19	과도한 권한 부여 제한 - AI시스템의 목적에 따라 접근 가능한 데이터 혹은 정보통신시스템을 통제하여 운영하고 있는가?	☐
20	민감 명령 승인 절차 마련 - 제어시스템 등 중요 시스템을 조작하는 등 민감한 작업에 대해 담당자의 명령 승인 절차를 마련하였는가?	☐
21	비상대응 체계 마련 - AI시스템이 잘못된 동작을 할 경우 즉시 작업을 중단시킬 수 있도록 비상정지 기능 등을 마련하였는가?	☐
22	설명 가능한 AI 구성 - AI의 추론·결정 과정 등을 담당자가 인지 가능한 형태로 표출하고 있는가?	☐
23	AI모델 대상 적대적 모의공격 수행 - AI모델의 보안성·안전성 확보를 위해 적대적 모의공격을 수행, 보호기능이 정상 동작하는지 분석하여 보완하였는가?	☐
24	AI모델에 적대적 공격유형 학습 - AI 탈옥 혹은 AI 오작동 유도 등 다양한 적대적 공격 유형을 지속적으로 학습시키고 있는가?	☐
25	AI시스템 구성요소 취약점 점검 및 보안업데이트 - AI시스템을 구성하는 소프트웨어, 라이브러리 등의 취약점을 정기 점검하고, 발견한 취약점에 대해 보안패치 등 업데이트를 실시하였는가?	☐
26	AI모델 복구 - AI모델에서 변조, 이상행위 발생 등이 의심될 경우 운영 중단 및 복원을 할 수 있도록 원본을 백업하고 관리하고 있는가?	☐
27	요청속도 제한 - 공격자가 AI시스템의 과부하 시도를 방지하기 위해 호출 횟수, 입력 길이, 동시 처리 요청수 등을 제한하고 있는가?	☐
28	AI시스템 구성요소 완전 삭제 - AI시스템 폐기 시 AI모델·학습데이터·벡터DB·로그 등 구성요소의 재사용이 불가능하도록 완전 삭제를 하였는가?	☐
29	용역업체 보안관리 - 용역업체를 활용 시, 업체 대상으로 보안관리 실태를 정기 점검하고 비인가 행위 여부를 확인하고 있는가?	☐
30	사용자 교육 및 보안정책 수립 - 기관 사용자가 AI시스템 활용 시 주의해야 할 보안수칙에 대해 정기적으로 안내·교육하고, 기관 내부 보안정책을 수립하였는가?	☐