



제 428회 국회 (임시회)
제2차 과학기술정보방송통신위원회

국가연구개발혁신법 일부개정법률안

검 토 보 고

〈 국가연구개발과제 보안체계 정비 등 〉

■ 최수진의원 대표발의(의안번호 제2208216호)

2025. 8.

과학기술정보방송통신위원회

전문위원 임 명 현

목 차

I. 제안경위	1
II. 제안이유	1
III. 주요내용	2
IV. 검토의견	3
1. 범부처 보안지침 수립 및 보안등급 세분화(안 제21조제2항·제3항·제5항 신설 등)	3
2. 보안관리 조치 체계화(안 제21조제6항·제7항 신설 및 제31조제1항 등)	10
3. 연구보안 전담기관 지정(안 제21조의2 신설)	18
4. 부 칙	22

[참고자료]

1. 국가연구개발사업 보안대책	24
2. 연구보안 실태 및 인식조사 주요 결과	29

I. 제안경위

가. 발 의 자 : 최수진의원 등 12인

나. 발 의 일 : 2025. 2. 17.

다. 회 부 일 : 2025. 2. 18.

II. 제안이유

국가 간 기술주도권 확보 경쟁이 심화됨에 따라 국내·외에서 연구자산 등의 유출 사례 및 탈취 위협이 증가하고 있음. 미국 등 주요국들은 자국의 연구자산 보호를 위한 관련 정책 마련과 제도 도입을 통해 우위를 확보하는 한편, 연구보안 체계가 미비한 국가와는 연구 협력을 지양하는 상황임. 글로벌 기술 선도국과 연구 협력 강화를 통해 국가 과학기술 경쟁력 확보에 힘써야 하는 우리나라 입장에서 연구보안 체계 정비가 조속히 이루어져야 할 필요성이 있음.

현행법은 국가연구개발과제 중 일반과제와 구분하여 국가안보 등을 위해 보안이 필요한 과제(이하 “보안과제”라 한다)의 분류 근거와 보안과제 수행기관의 보안대책 마련 의무를 규정하고 있으나, 이러한 대응만으로는 전략적 가치가 있는 잠재적 중요기술에 대한 관리가 제한적임. 또한, 연구성과의 소유권 이전에 관한 사항, 보안점검 조치 명령의 시정 기한 등이 규정되어 있지 않고, 연구현장에서 연구보안 업무를 효율적으로 지원하기 위한 전담 조직의 근거 부재 등 연구자산 보호·관리 체계가 미흡한 한계가 존재함.

이에 국가연구개발과제의 현행 보안등급을 세분화하여 중간등급의 보안

과제(이하 “민감과제”라 한다)를 신설하여 보안관리를 강화하고, 일부 제도적 미비점을 개선·보완하는 근거를 마련하여 국가연구개발 현장의 연구보안 체계를 정비하고 국제공동연구 활성화에 기여하고자 함.

Ⅲ. 주요내용

- 가. 과학기술정보통신부장관이 범부처 보안지침을 수립하되 필요시 중앙행정기관의 장이 추가로 별도 보안지침을 수립할 수 있으며, 이에 따라 연구개발기관의 장이 보안대책을 마련하도록 체계를 정비함(안 제21조제1항 및 제2항·제3항 신설).
- 나. 잠재적 중요기술의 선제적 보호를 위해 보안과제와 일반과제의 중간 보안등급을 신설함(안 제21조제4항 및 제5항 신설).
- 다. 보안과제의 성과 소유권 이전시 의무와 연구개발기관의 보안관리 조치 의무를 상향입법하는 등 연구보안 관리를 체계화 함(안 제21조제6항·제7항 신설 및 제8항부터 제10항까지).
- 라. 연구현장의 보안 업무 부담 완화 및 관련 정책의 체계적 추진을 위해 연구보안 정책 이행을 지원할 전담 집행조직 근거를 마련함(안 제21조의2 신설).
- 마. 단순 보안대책 위반이 바로 부정행위로 간주되지 않도록 시정명령 미이행을 부정행위로 규정하고, 연구보안 부정행위의 범위를 보안과제의 보안사항 누설·유출에서 보안과제·민감과제의 성과 누설·유출로 확대함(안 제31조제1항).

IV. 검토의견

1. 범부처 보안지침 수립 및 보안등급 세분화(안 제21조제2항·제3항·제5항 신설 등)

가. 개정안의 내용

개정안은 국가연구개발사업 및 연구개발과제와 관련하여 과학기술정보통신부장관 및 중앙행정기관의 장이 연구개발 수행 과정에서 요구되는 보안사항 준수를 위한 보안지침을 수립하도록 하고, 보안과제가 아닌 연구개발과제 중 유출 시 국가에 영향을 미칠 수 있는 과제를 ‘민감과제’로 분류하여 국가연구개발과제의 보안등급을 세분화하려는 것임.

현행	개정안
제21조(국가연구개발사업 등의 보안) ① <u>관계 중앙행정기관의 장 및 연구개발기관의 장은 소관 국가연구개발사업 및 연구개발과제와 관련하여 연구개발성과 등 대통령령으로 정하는 중요 정보가 유출되지 아니하도록 보안대책을 수립·시행하여야 한다.</u> <u><신설></u>	제21조(국가연구개발사업 등의 보안) ① <u>과학기술정보통신부장관은 연구개발 수행 과정에서 요구되는 보안사항 준수를 위한 보안지침을 수립하여야 한다. 이 경우 보안사항에 관하여 필요한 사항은 국가정보원장과 협의하여 정한다.</u> ② <u>중앙행정기관의 장은 제1항에 따른 보안지침에 추가적으로 정할 필요가 있는 사항에 대해 과학기술정보통신부장관과 협의하여 별도로 보안지침을 수립할 수 있다.</u> ③ <u>국가연구개발사업을 직접 수행하</u>
<u><신설></u>	

현행	개정안
② 중앙행정기관의 장은 외부로 유출될 경우 기술적·재산적 가치에 상당한 손실이 예상되거나 국가안보를 위하여 <u>보안이 필요한</u> 연구개발과제를 보안과제로 분류할 수 있다. <u><신 설></u> ③ ~ ⑥ (생략)	는 중앙행정기관의 장 및 대통령령으로 정하는 연구개발기관의 장은 제1항 또는 제2항의 보안지침에 따라 보안대책을 마련·시행하여야 한다. ④ ----- ----- ----- -----<u>별도의 관리가 필요하다고 인정하는</u>----- -----. ⑤ 중앙행정기관의 장은 제4항의 보안과제로 분류하지 않았으나 유출시 국가에 미치는 영향을 고려하여 추가적인 관리가 필요하다고 인정하는 연구개발과제를 민감과제로 분류할 수 있다. ⑥ ~ ⑪ (생략)

나. 검토의견

현행법 제21조제2항에 따라 중앙행정기관의 장은 외부로 유출될 경우 기술적·재산적 가치에 상당한 손실이 예상되거나 국가안보를 위하여 보안이 필요한 연구개발과제를 보안과제로 분류하고 있으며,

관계 중앙행정기관의 장 및 연구개발기관의 장은 같은 조 제1항에 따라 보안과제의 연구개발성과나 산업기술과 관련된 비공개 연구개발 성과 정보가 유출되지 않도록 보안관리 실태 점검, 보안사고의 예방·대응·조사·재발방지 방안 등 보안대책을 수립하여야 함.¹⁾

개정안은 과학기술정보통신부장관이 보안대책의 수립에 앞서 범부처 보안지침을 수립하고 필요에 따라 중앙행정기관의 장이 별도의 보안지침을 수립할 수 있도록 함으로써 연구보안 관리 정책의 일관성을 확보하며,

보안과제의 분류체계를 '일반과제-민감과제-보안과제'의 3단계 분류 체계로 개편하여 보안등급에 따라 강화된 맞춤형 보안조치 및 관리를 적용함으로써 민감과제에 대해서는 일반과제보다 강화된 보안조치를 요구하면서도 보안과제에 부과되는 보안조치 사항에 대한 연구현장의 부담을 완화하고 완충지대를 마련하려는 취지로 보임.

1) 「국가연구개발혁신법」

제21조(국가연구개발사업 등의 보안) ① 관계 중앙행정기관의 장 및 연구개발기관의 장은 소관 국가연구개발사업 및 연구개발과제와 관련하여 연구개발성과 등 대통령령으로 정하는 중요 정보가 유출되지 아니하도록 보안대책을 수립·시행하여야 한다.

② 중앙행정기관의 장은 외부로 유출될 경우 기술적·재산적 가치에 상당한 손실이 예상되거나 국가안보를 위하여 보안이 필요한 연구개발과제를 보안과제로 분류할 수 있다. (후 략)

개정안과 관련하여 다음 사항에 대한 검토가 필요한 것으로 보임.

첫째, 국가연구개발사업의 과제에 대한 체계적인 보안관리를 위하여 국가연구개발사업의 총괄부처인 과학기술정보통신부 차원에서 범부처 보안지침을 확립하도록 하는 것은 타당한 것으로 보임.

현행법 시행령은 다음과 같이 보안대책에 포함되어야 하는 내용을 세부적으로 규정하고 있으며, 이에 따라 중앙행정기관의 장과 연구개발기관의 장이 별도로 보안대책을 수립하여 운영할 수 있음.

< 「국가연구개발혁신법 시행령」에 따른 보안대책 주요 내용 >

수립 주체	주요 내용
중앙행정기관의 장	- 연구개발성과의 수집·분석·가공·배포 방안 - 보안관리 실태 점검의 구체적 방안 - 보안사고의 예방·대응·조사·재발방지 방안 - 외국에 소재한 기관·단체 또는 외국인과 공동으로 연구를 수행하는 경우의 보안관리 방안 - 보안대책 총괄 담당자 지정 방안 - 보안교육 실시 방안 - 국가정보원과의 보안 관련 협력 방안
연구개발기관의 장	- 소속 연구자가 준수해야하는 보안 관련 의무사항 - 연구시설 및 연구관리시스템에 대한 보안조치 사항 - 보안사고의 예방·대응·조사·재발방지 방안 - 외국에 소재한 기관·단체 또는 외국인과 공동으로 연구를 수행하는 경우의 보안관리 방안 - 보안대책 총괄 담당자 지정 방안 - 보안교육 실시 방안 - 보안관리규정 제정·운영 방안

과학기술정보통신부는 교육부, 환경부, 농림축산식품부 등 9개 부처와 공동고시로서 「국가연구개발사업 보안대책」을 제정하여 운영 중이며([참고 1]),

보건복지부²⁾, 해양수산부³⁾ 등 소관 부처별로도 예규, 훈령 또는 고시 형식으로서 보안관리규칙을 개별적으로 두고 있으나, 보안과제의 가장 큰 비중을 차지하는 방위사업청과 국방부는 별도로 연구개발사업 보안대책을 두고 있지 않은 것으로 확인됨.

따라서 법률에 근거한 범부처 보안지침에 따라 연구보안 관리 체계를 일원화함으로써 연구보안 정책의 일관성·통일성을 확보하고, R&D 총괄부처인 과학기술정보통신부가 부처별로 산재된 보안대책 준수 여부를 관리함으로써 보안대책의 실효성을 제고할 수 있다는 점에서 타당한 취지로 보임.

둘째, 현행 보안과제-일반과제의 이분법적 체계에서 벗어나 분류체계를 세분화할 경우 명확한 분류 기준 및 가이드라인 마련이 필요할 것으로 보임.

과학기술정보통신부에 따르면 2023년 기준⁴⁾으로 국가연구개발과제 중 보안과제 건수는 733건(전체 국가연구개발과제 71,804건의 1.0%)이며, 예산은 2조 9,035억원(전체 국가연구개발과제 예산 30조 5,731억원의 9.5%) 수준인데, 여전히 보안과제 분류 기준이 추상적이며 경제적 중요성보다는 국방기술 등 국가안보를 주요 기준으로 하여 분류가 이루어지고 있음.⁵⁾

2) 「보건복지부 소관 연구개발사업 보안관리규칙」(보건복지부예규)

3) 「해양수산 연구개발사업 보안관리지침」(해양수산부훈령)

4) 2024년 기준 보안과제 현황은 2025년 8월 현재 조사가 진행 중임

5) 과기부 등 9개 부처 공동고시 제10조에 따른 보안등급 구분 기준은 다음과 같음

I급	유출될 경우 대한민국과 외교관계가 단절되고 전쟁을 일으키며, 국가의 방위계획·정보
----	---

< 분류 기준별 보안과제 수 (2023년 기준) >

보안과제 분류 기준	보안과제 수	비율
방위력개선사업 관련 과제	671건	91.5%
미래핵심기술	25건	3.4%
국산화 추진기술	1건	0.1%
국가핵심기술	21건	2.9%
수출허가제한 필요기술	5건	0.7%
개별 중앙행정기관 인정 과제	10건	1.4%
합계	733건	100%

자료: 과학기술정보통신부 제공 자료를 바탕으로 작성

따라서 보안과제, 민감과제 및 일반과제의 명확한 경계 설정을 위하여 기술적·재산적 가치 손실 등 경제적 중요성과 영향을 포함한 보안등급 분류 기준과 가이드라인을 마련할 필요가 있음.

특히, 「국가연구개발사업 보안대책」 제3조에 따르면 중앙행정기관의 장은 보안과제 지정·해제 등 분류가 필요할 때마다 ‘보안과제분류위원회’를 설치하여 검토를 진행하고 있는데,⁶⁾

	활동 및 국가방위에 반드시 필요한 과학과 기술의 개발을 위태롭게 하는 등의 우려가 있는 보안과제의 핵심적인 정보
Ⅱ급	유출될 경우 국가안전보장 및 국가경쟁력 확보에 막대한 지장을 끼칠 우려가 있는 보안과제의 핵심적인 정보로 문서나 전자매체 유출이 과제 중요사항의 직접적 유출로 이어질 수 있는 경우
Ⅲ급	유출될 경우 국가안전보장 및 국가 경쟁력 확보에 해를 끼칠 우려가 있는 보안과제의 핵심적인 정보로 문서나 전자매체 유출이 과제 중요사항의 직접적 또는 간접적인 유출로 이어질 수 있는 경우

6) 「국가연구개발사업 보안 대책」

제3조(연구개발사업과제 보안과제 분류) ① 중앙행정기관의 장은 법 제21조제2항에 따라 소관 연구개발과제를 보안과제로 지정·해제하는 등 분류가 필요할 때에는 검토를 위하여 해당 연구개발 분야 및 보안업무 전문가 등으로 구성된 보안과제분류위원회를 설치하여 운영하여야 한다. 단, 다음 각 호에 해당하는 경우 보안과제분류위원회의 검토를 생략한다.

1. 연구개발과제 발굴을 위한 사전 기획을 통해 보안과제로 분류될 수 있는 경우
2. 자유공모 과제에 대하여 연구개발과제평가단을 통해 보안과제로 분류될 수 있는 경우
3. 다른 법령에 의한 절차를 통해 보안과제로 분류될 수 있는 경우

각 기관별로 보안과제를 분류할 때마다 한시적으로 위원회 조직을 구성하여 운영할 경우, 보안과제 분류의 일관성이 확보되기 어려울 것이므로 안 제21조의2에 따라 지정되는 연구보안 전담기관으로 하여금 모든 부처에 공통적으로 적용될 분류 기준을 마련하도록 하는 방안을 고려해볼 수 있을 것임.

가. 개정안의 내용

현행	개정안
제21조(국가연구개발사업 등의 보안) ① ~ ② (생략) <u><신설></u>	제21조(국가연구개발사업 등의 보안) ① ~ ⑤ (생략) ⑥ 제4항에 따른 보안과제의 연구개발성과성과소유기관 또는 연구개발성과소유 연구자는 특별한 사정이 없는 한 그 성과의 소유권을 이전하지 않는 것을 원칙으로 한다.
<u><신설></u>	⑦ 제6항에도 불구하고 연구개발성과의 소유권을 외국으로 이전하는 경우 중앙행정기관의 장에게 사전승인을 얻어야 한다.
③ 제2항에 따라 보안과제로 분류된 연구개발과제를 수행하는 연구개발기관은 <u>보안교육 실시, 보안책임자 지정 등 대통령령으로 정하는</u> 보안관리 조치를 하여야 한다.	⑧ 제4항의 보안과제 또는 제5항의 민감과제----- -----다음 각 호의----- ----- -----.
<u><신설></u>	1. 보안책임자 지정
<u><신설></u>	2. 수행 연구자에 대한 보안교육 실

현행	개정안
<u><신 설></u> <u><신 설></u> <u><신 설></u> ④ 중앙행정기관의 장은 제1항에 따른 보안대책의 수립·시행 실태 및 제3항에 따른 보안관리 실태를 점검하고, 그 결과에 따라 관련 기관에 필요한 조치를 하도록 명할 수 있다. ⑤ 중앙행정기관의 장은 제1항부터 제4항까지의 업무를 국가정보원장에게 위탁할 수 있다. ⑥ 제1항에 따른 보안대책의 내용, 제2항에 따른 보안과제의 분류 기준, 제3항에 따른 보안관리 실태 점검 및 조치 사항은 대통령령으로 정한다. 제31조(국가연구개발사업 관련 부정행위의 금지) ① 올바른 연구윤리 확보를 위하여 연구자 및 연구개발기	시 3. 수행 연구자의 외국 접촉 및 외국인 연구자의 연구수행 등에 대하여 과학기술정보통신부장관이 고시하여 정하는 조치 4. 수행 연구자가 외국 정부·기관·단체 등으로부터 제공받은 행정적·재정적 지원에 관한 정보의 관리조치 5. 그 밖에 대통령령으로 정하는 보안관리 조치 ⑨ 중앙행정기관의 장은 제3항에 따른 보안대책의 마련·시행 실태 및 제8항에 따른 보안관리 실태를 점검하고, 그 결과에 따라 해당 기관에 필요한 조치를 하도록 기한을 정하여 시정을 명할 수 있다. ⑩ -----제9항에 따른 업무를 국가정보원장과 합동으로 수행하거나----- ⑪ 제4항 및 제5항에 따른 보안과제·민감과제-----제9항-----조치 등에 관하여 필요한----- 제31조(국가연구개발사업 관련 부정행위의 금지) ① -----

현행	개정안
관은 국가연구개발활동을 수행하는 경우 다음 각 호의 국가연구개발사업 관련 부정행위(이하 “부정행위”라 한다)를 하여서는 아니 된다. 1. ~ 3. (생략) <u><신설></u> 4. 제21조제1항에 따른 보안대책을 위반하거나 제21조제2항에 따라 보안과제로 분류된 연구개발과제의 보안사항을 누설하거나 유출하는 행위 5.·6. (생략) ② ~ ⑤ (생략)	----- ----- ----- -----. 1. ~ 3. (현행과 같음) 4. 특별한 사유 없이 제21조제9항에 따른 시정명령을 이행하지 아니한 행위 5. 제21조제4항-----분류되거나 제21조제5항에 따라 민감과제로 분류된 연구개발과제의 성과를----- 6.·7. (현행 제5호 및 제6호와 같음) ② ~ ⑤ (현행과 같음)

나. 검토의견

현행법 제16조에 따라 연구개발성과는 해당 연구개발과제를 수행한 연구개발기관이 해당 연구자로부터 권리를 승계하여 소유하는 것이 원칙이나, 예외적으로 연구자가 소유하거나 여러 연구개발기관이 공동으로 소유할 수 있음. 연구개발성과를 소유한 기관이나 연구자는 이를 공동활용하거나 정보를 공개하는 등의 조치를 할 수 있으며 성과의 소유권을 이전하는 등 권리를 행사할 수도 있음.

개정안은 보안과제에 대해서는 성과 소유기관이나 성과 소유 연구자라 할지라도 원칙적으로는 소유권을 이전하지 아니하도록 하되, 예외적으로 이전하더라도 그 행선지가 외국인 경우에는 중앙행정기관의 장에게 사전 승인을 받도록 함으로써 보안과제 관련 성과의 소유권의 무분별한 이전 및 유출을 사전에 방지하려는 것으로 보이며,

민감과제에 대하여도 보안관리 조치 의무를 부여하고, 과제 수행 연구자의 외국 접촉, 외국 정부·기관·단체 등으로부터 받는 지원 관련 정보를 관리하는 등 보안관리 조치의 종류를 구체화하려는 취지로 보임.

국가정보원에 따르면 2023~2024년 동안 국가 산업기술 유출 사례는 총 46건으로 나타났으며, 최근 한 대학교수가 자율주행차 기술 70여건을 외국에 유출하여 유죄 판결을 받은 바,⁷⁾

7) 황윤기, “‘중국에 자율주행차 기술유출’ KAIST 교수 징역 2년 확정”, 연합뉴스, 2024.5.30,

국가 간 기술주도권 확보 경쟁 심화로 인한 연구자산 유출 위험이 증가하고 있다는 점에서 국가안보에 영향을 미칠 중요 연구자산 유출을 최소화하기 위하여 보안과제 성과의 소유권 이전을 제한하고 보안과제 조치 체계를 정비하는 것은 국내 연구자산 보호 측면에서 타당한 입법으로 보임.

개정안과 관련하여 다음 사항에 대한 검토가 필요한 것으로 보임.

첫째, 해외 주요국은 대체로 해외자금 수혜 정보 신고를 의무화하고 있으며, 국내에는 최근 국외 수혜 정보 보고 제도가 마련되었으나 연구기관 자체 관리체계가 미흡하다는 점을 고려할 필요가 있음([참고 2]).

< 주요국의 연구보안 관련 외국 수혜 현황 신고 정책 동향 >

국가	주요 정책
 미국	- 정부연구비 신청 시 물질적·비물질적 외국 수혜 현황 신고 의무화 - 국가 안보·경쟁력 관련성과 외국기관과의 협력 보고 강조
 일본	- 국외 포함 타 연구자금 수혜 현황 신고 의무화 및 관련 시스템 개편 - 연구자의 연구절차 상 위험판단 및 적극적 상담·보고 강조
 영국	- 외국기관과의 관계 등 포함 개인적·영리적 이해관계 신고 의무화 - 적대국으로부터의 보안위협 예방 및 지적재산 보호 강조
 호주	- 외국 인재프로그램, 외국연구지원 등 외국영향 관련 정보공개 강조 - 대학의 외국파트너 확인(로비스트·제재목록 등재) 및 보고 강조

자료: 국가과학기술자문회의 제공 자료를 바탕으로 재작성

우리나라는 외국 정부, 기관 등의 보안과제 참여(국제공동연구)에 대한 사전승인과 외국인 연구원의 보안과제 참여 제한을 원칙으로 하

고 있으나 기관별로 보안관리 체계가 상이하므로 공통 기준을 마련함으로써 외국인 연구원의 스파이 행위로 인한 잠재적 보안 위협에 대응할 필요가 있음.

또한, 연구자가 명성, 경제적·금전적 이득 등을 추구함에 따라 이해충돌로 인해 연구 진실성(Research Integrity)이 저해될 수 있으므로 보안과제를 수행하는 연구자가 외국 정부·기관과 접촉 시 신고 또는 외국 정부·기관·단체 등으로부터의 수혜 내역을 주기적으로 등록하도록 하고 연구개발기관이 그 정보를 체계적으로 관리함으로써 연구자의 사적 이익 추구를 사전에 방지하고 연구에 대한 공적 신뢰를 보장할 수 있다는 의의도 있을 것으로 보임.

둘째, 개정안은 현재 부처별로 훈령·예규·고시의 형식으로 규정되어 있는 보안대책 및 제재의 근거를 법률에 상향하여 규정함으로써 보안대책 위반에 대한 제재의 법적 타당성 및 구속력을 확보할 수 있다는 점에서 타당한 것으로 보임.

보안과제로 분류된 연구개발과제를 수행하는 연구개발기관은 「국가연구개발혁신법」 및 시행령에 따라 보안교육, 보안책임자 지정 등 보안관리 조치 의무를 지고 있으며, 중앙행정기관의 장은 보안대책과 보안관리 실태를 점검하여 관련 기관에 필요한 조치를 하도록 명할 수 있으나⁸⁾ 조치 불이행 시 제재처분의 근거가 부재하였음.

8) 「국가연구개발혁신법」

제21조(국가연구개발사업 등의 보안) ①·② (생략)

③ 제2항에 따라 보안과제로 분류된 연구개발과제를 수행하는 연구개발기관은 보안교육 실시, 보안책임자 지정 등 대통령령으로 정하는 보안관리 조치를 하여야 한다.

개정안에 따라 중앙행정기관의 장이 보안대책과 보안관리 실태를 점검하고 시정명령을 할 수 있도록 하고, 시정명령을 이행하지 아니하는 것을 안 제31조제1항에 따라 부정행위로 간주할 경우 현행법 제32조9)에 따른 제재처분을 할 근거가 마련되므로 관리조치 위반을 사전

④ 중앙행정기관의 장은 제1항에 따른 보안대책의 수립·시행 실태 및 제3항에 따른 보안관리 실태를 점검하고, 그 결과에 따라 관련 기관에 필요한 조치를 하도록 명할 수 있다. (후 략)

「국가연구개발혁신법 시행령」

제46조(보안관리 조치) 법 제21조제3항에서 “보안교육 실시, 보안책임자 지정 등 대통령령으로 정하는 보안관리 조치”란 다음 각 호의 조치를 말한다.

1. 보안과제를 수행하는 연구실에 대한 보호구역 설정
2. 보안과제를 수행하는 연구자의 연구실 출입권한 차등 부여 및 출입 현황 관리
3. 보안과제를 수행하는 연구자에 대한 보안교육 실시 및 보안서약서 제출 요청
4. 보안과제를 수행하는 외국인 연구자의 연구 수행에 대한 연구개발기관의 장의 승인 및 중앙행정기관의 장에 대한 보고
5. 연구개발기관이 운영하는 연구관리시스템에 대한 보안관리 조치
6. 연구개발정보 처리 과정 및 그 결과에 대한 보안관리 조치
7. 보안책임자 지정

제47조(보안관리 실태 점검 및 관련 조치) ① 중앙행정기관의 장은 법 제21조제4항에 따라 보안관리 실태를 점검하려면 그 시기·내용 및 방법 등이 포함된 점검계획을 실태 점검을 하려는 날부터 10일 전까지 점검 대상 연구개발기관의 장에게 통보해야 한다.

② 법 제21조제4항에 따라 조치를 하도록 명령을 받은 연구개발기관의 장은 해당 조치에 따른 결과를 조치명령을 받은 날부터 6개월 이내에 중앙행정기관의 장에게 제출해야 한다.

제48조(보안사고에 대한 조치) ① 연구개발기관의 장은 다음 각 호의 어느 하나에 해당하는 사고(이하 “보안사고”라 한다)가 발생한 경우에는 그 사고를 알게 된 즉시 필요한 조치를 하고, 중앙행정기관의 장에게 보고해야 한다.

1. 제44조제1항 각 호에 해당하는 연구개발성과의 침해·유출·누설·분실·훼손·도난
2. 제44조제1항 각 호에 해당하는 연구개발성과를 유통·관리·보존하는 시스템의 유출·파손·파괴

② 연구개발기관의 장은 제1항에 따른 보고를 한 후 다음 각 호의 사항을 파악하여 지체 없이 중앙행정기관의 장에게 보고해야 한다.

1. 보안사고의 일시·장소
2. 보안사고를 낸 사람의 인적사항
3. 보안사고의 세부 내용

③ 중앙행정기관의 장은 보안사고를 알게 되거나 제1항에 따른 보고를 받은 경우에는 그 경위를 조사할 수 있다. 이 경우 해당 연구개발기관과 연구책임자는 조사에 성실히 협조해야 한다.

9) 「국가연구개발혁신법」

제32조(부정행위 등에 대한 제재처분) ① 중앙행정기관의 장은 다음 각 호의 어느 하나에 해당하는 경우에는 해당 연구개발기관, 연구책임자, 연구자, 연구지원인력 또는 연구개발기관 소속 임직원에게 대하여 10년 이내의 범위에서 국가연구개발활동(연구지원은 제외한다)에 대한 참여를 제한하거나 이미 지급한 정부 연구개발비의 5배의 범위에서 제재부가금을 부과할 수 있다.

1. 2. (생 략)
3. 연구자 또는 연구개발기관이 제31조제1항 각 호의 어느 하나에 해당하는 부정행위를 한 경우
4. ~ 6. (생 략)

② 제1항에 따른 참여제한 처분이나 제재부가금 부과처분은 병과할 수 있다.

③ 중앙행정기관의 장은 제1항 및 제2항에 따른 제재처분과 별도로 이미 지급한 정부 연구개발비 중 제재사유와 관련된 연구개발비를 환수할 수 있다.

에 방지하고 이에 대한 제재의 일관성과 공정성이 제고되는 효과가 있을 것으로 보임.

④ 중앙행정기관의 장은 제재처분을 하거나 연구개발비를 환수하는 때에는 제재사유의 중대성, 위반행위의 고의 유무, 위반 횟수, 연구개발과제의 수행 단계 및 진행 정도 등을 고려하여야 한다.

⑤ 제1항에 따른 제재처분은 그 제재사유가 발생한 연구개발과제의 종료일 또는 그 제재사유가 발생한 국가연구개발활동의 종료일로부터 10년이 지나면 할 수 없다.

⑥ 제1항에 따른 제재사유별 참여제한의 기준 및 제재부가금의 부과기준, 제3항에 따른 연구개발비 환수의 기준 및 범위는 대통령령으로 정한다.

3. 연구보안 전담기관 지정(안 제21조의2 신설)

가. 개정안의 내용

개정안은 국가연구개발사업의 보안 업무를 효율적으로 추진하기 위하여 연구보안 전담기관을 지정하여 보안지침·보안대책의 수립 및 시행과 보안과제·민감과제의 분류 등의 업무를 지원하도록 하고 있음.

현행	개정안
<신설>	제21조의2(연구보안 전담기관의 지정 등) ① 과학기술정보통신부장관은 국가연구개발사업의 보안 업무를 효율적으로 추진하기 위하여 필요한 전문인력과 시설을 갖춘 기관 또는 단체를 연구보안 전담기관으로 지정할 수 있다. ② 제1항에 따른 연구보안 전담기관은 다음 각 호의 업무를 수행한다. 1. 제21조제1항부터 제8항까지 업무에 대한 지원 2. 국가연구개발사업의 보안과 관련된 상담·홍보·교육·실태조사 3. 국가연구개발사업의 보안과 관련된 기반 조성 4. 국가연구개발사업의 보안과 관련된 국제협력 5. 그 밖에 국가연구개발사업의 보안을 지원하기 위하여 과학기술정보

현행	개정안
	<u>통신부장관이 필요하다고 인정하는 업무</u> ③ <u>과학기술정보통신부장관은 예산의 범위에서 제2항에 따른 연구보안 전담기관의 운영 및 사업 수행에 필요한 비용의 일부 또는 전부를 출연하거나 보조할 수 있다.</u> ④ <u>과학기술정보통신부장관은 연구보안 전담기관으로 지정된 기관 또는 단체가 다음 각 호의 어느 하나에 해당하는 경우 그 지정을 취소하거나 6개월 이내의 기간을 정하여 업무의 전부 또는 일부를 정지할 수 있다. 다만, 제1호에 해당하는 경우에는 지정을 취소하여야 한다.</u> <u>1. 거짓이나 그 밖의 부정한 방법으로 지정을 받은 경우</u> <u>2. 제5항에 따른 지정 기준에 적합하지 아니하게 된 경우</u> <u>3. 이 법이나 다른 법령을 위반하여 연구보안 전담기관으로서의 업무를 수행하는 것이 부적절하다고 인정되는 경우</u> ⑤ <u>그 밖에 전담기관의 지정 및 지정취소의 요건·절차 등에 관하여 필요한 사항은 대통령령으로 정한다.</u>

나. 검토의견

현행법 제22조10)에 따라 중앙행정기관의 장은 연구보안 관련 업무의 전부 또는 일부를 대행하는 기관을 지정할 수 있으며, 현재는 한국연구재단, 한국산업기술기획평가원, 한국보건산업진흥원 등이 전문기관으로 지정되어 연구보안 관련 업무를 대행하고 있음.

개정안은 보안지침의 수립, 보안과제와 민감과제의 보안등급 분류, 보안관리 조치 등에 대한 지원과 연구보안 관련 기반 조성, 국제협력 등의 업무를 수행하는 ‘연구보안 전담기관’을 지정하여 운영하기 위한 근거를 마련하려는 것임.

과학기술정보통신부장관이 국가적 수준의 연구보안 전담기관을 지정하여 창구를 단일화함으로써 부처별로 산재된 연구보안 전문기관의 중복으로 인한 비효율을 완화하고, 보안과제 성과의 이전과 유출 방지 업무를 효율적으로 처리할 수 있을 것이라는 점에서 타당한 입법 취지로 보임.

또한, 기술주권 확보를 위해 연구보안 관련 전문인력을 양성하고 국

10) 「국가연구개발혁신법」

제22조(전문기관의 지정 등) ① 중앙행정기관의 장은 소관 국가연구개발사업의 효율적인 추진을 위하여 제9조부터 제19조까지, 제21조, 제31조제3항, 제33조제1항, 제34조제2항에 따른 업무의 전부 또는 일부를 대행하는 기관을 전문기관으로 지정할 수 있다.

② 전문기관은 다음 각 호의 어느 하나에 해당하는 기관 중에서 지정한다.

1. 다른 법률에 따라 설립된 기관 중 국가연구개발사업의 기획·관리·평가 등을 지원하는 기관으로서 대통령령으로 정하는 기관
2. 「공공기관의 운영에 관한 법률」에 따른 공공기관
3. 그 밖에 「민법」 등 다른 법률에 따라 설립된 비영리법인 중 대통령령으로 정하는 기준에 부합하는 기관

③ 중앙행정기관의 장은 전문기관에 대하여 업무 대행에 사용되는 비용의 전부 또는 일부를 예산의 범위에서 출연 또는 보조할 수 있다. (후략)

제협력 기능 등을 수행하기 위한 전담 지원체계를 구축함으로써 연구 현장에 집중된 보안 업무부담을 완화하고, 국제공동연구를 촉진 중인 주요 과학기술협력국과의 연구보안 정책 협력을 강화할 수 있다는 측면에서도 입법 필요성이 있다고 보임.

4. 부칙

가. 개정안의 내용

개정안 부칙은 이 법의 시행일을 공포 후 6개월이 경과한 날로 정하고 있음.

개 정 안
부 칙
이 법은 공포 후 6개월이 경과한 날부터 시행한다.

나. 검토의견

개정안은 보안지침, 보안대책 및 민감과제 분류 기준 수립, 보안관리 실태 점검 및 시정명령의 기준 등의 마련과 이에 필요한 시행령 개정¹¹⁾에 따라 소요될 기간을 고려하여 부칙으로 6개월의 시행 유예기간을 두고 있음.

다만, 「국가전략기술 육성에 관한 특별법」 제27조¹¹⁾에서는 전략연구

11) 「국가전략기술 육성에 관한 특별법」

제27조(국가전략기술 정보보호 및 보안) ①·②(생략)

③ 중앙행정기관의 장은 소관 전략연구과제를 「국가연구개발혁신법」 제21조제2항에 따른 보안과제로 분류할 수 있으며, 효율적이고 신속한 연구개발 추진을 위하여 필요한 경우 같은 조 제3항에도 불구하고 보안과제로 분류한 전략연구과제의 기술적 특성 등을 반영한 보안관리 조치 사항을 별도로 지정·운영할 수 있다.

④ 중앙행정기관의 장은 제3항에 따른 보안관리 조치의 실행에 필요한 예산의 전부 또는 일부를 지원할 수 있다.

⑤ 중앙행정기관의 장은 국가정보원장과 합동으로 소관 전략연구사업의 연구과제를 수행하는 기술육성주체에 대하여 「국가연구개발혁신법」 제21조에 따른 보안관리 실태점검을 할 수 있다.

⑥ 제2항에 따른 통보의 대상이 되는 정보의 범위, 통보의 방법 및 절차, 제3항에 따른 전략연구과제 보안관리 조치 사항의 지정·운영 등에 필요한 사항은 대통령령으로 정한다.

과제를 보안과제로 분류하고 보안관리 조치 등을 할 수 있는 근거를 두고 있으므로,

개정안에 따라 보안과제 분류체계를 보안과제 및 민감과제로 세분화할 경우 「국가전략기술 육성에 관한 특별법」을 함께 개정하기 위하여 부칙에 “다른 법률의 개정”을 규정하는 조를 신설하는 것을 검토할 필요가 있음.

문 의 처
02)6788-5227

참고 1

국가연구개발사업 보안대책 [과학기술정보통신부·국가유산청·산림청·교육부·환경부·기상청·경찰청·농촌진흥청·농림축산식품부고시]

제1조(목적) 이 지침은 「국가연구개발혁신법」(이하 "법"이라 한다) 제21조제1항 및 같은 법 시행령(이하 "령"이라 한다) 제44조에 따른 중앙행정기관의 장이 수립하는 소관 국가연구개발사업 및 연구개발과제(이하 "연구개발과제등"이라 한다)와 관련한 보안대책으로서 법 제21조제1항에 따른 중요 정보가 유출되지 아니하도록 방지함을 목적으로 한다.

제2조(적용범위) 이 지침은 중앙행정기관 소관 국가연구개발사업에 적용한다. 다만, 중앙행정기관의 장이 해당 국가연구개발사업에 대하여 그 특성에 따라 별도의 보안규정을 마련하였을 경우 해당지침을 우선하여 적용할 수 있다.

제3조(연구개발과제 보안과제 분류) ① 중앙행정기관의 장은 법 제21조제2항에 따라 소관 연구개발과제를 보안과제로 지정·해제하는 등 분류가 필요할 때에는 검토를 위하여 해당 연구개발 분야 및 보안업무 전문가 등으로 구성된 보안과제분류위원회를 설치하여 운영하여야 한다. 단, 다음 각 호에 해당하는 경우 보안과제분류위원회의 검토를 생략한다.

1. 연구개발과제 발굴을 위한 사전 기획을 통해 보안과제로 분류될 수 있는 경우
2. 자유공모 과제에 대하여 연구개발과제평가단을 통해 보안과제로 분류될 수 있는 경우
3. 다른 법령에 의한 절차를 통해 보안과제로 분류될 수 있는 경우

② 연구개발기관의 장은 수행 예정이거나 수행하고 있는 보안과제에 대하여 재분류가 필요하다고 판단하는 경우에는 보안과제분류위원회에 보안과제 여부를 재분류해 줄 것을 요청할 수 있다.

③ 연구개발기관의 장은 수행 예정이거나 수행하고 있는 연구개발과제에 대하여 보안과제로 분류가 필요하다고 판단되는 경우에 보안과제분류위원회에 보안과제로 분류해 줄 것을 요청할 수 있다

④ 중앙행정기관의 장은 소관 연구개발과제를 보안과제로 분류하거나 해제한 경우에 다음 각 호의 사항을 포함하는 관련 정보를 국가정보원장에게 7일 이내에 통보한다.

1. 보안과제명
2. 보안과제 수행 연구개발기관 및 연구책임자
3. 보안과제 분류 또는 해제 사유

제4조(연구개발기관의 보안대책 수립 등) 연구개발기관의 장은 법 제21조제1항 및 영 제44조에 따른 보안대책(이하 "연구기관보안대책"이라 한다.)으로써 별표1에 따른 사항을 포함하는 자체규정을 마련하여야 한다. 다만, 공동연구개발기관이 자체 보안대책을 마련하기 어려운 경우 또는 주관연구기관과 공동연구개발기관의 보안대책을 통일성 있게 운영할 필요가 있는 경우에는 주관연구개발기관의 보안대책에 공동연구개발기관이 따르도록 한다.

제5조(보안대책 총괄담당자 지정 등) ① 연구개발기관의 장은 소속 임직원 중에서 제4조에 따른 연구기관보안대책에 따른 업무를 총괄하는 보안대책 총괄담당자를 지정하여야 한다.

② 그 밖에 보안대책 총괄담당자의 지정절차·업무 등에 관한 사항은 제4조에 따른 연구기관보안대책으로 정한다.

제6조(연구보안심의회의 구성 및 운영) ① 연구개발기관의 장은 다음 각 호의 사항을 심의하기 위하여 연구개발기관 내에 연구보안심의회를 구성·운영하여야 한다.

1. 연구기관보안대책의 수립·변경(연구보안에 관한 자체규정의 제·개정을 말한다)에 관한 사항
2. 법 제21조제3항에 따른 보안관리 조치를 위한 계획에 관한 사항
3. 법 제21조제3항에 따른 보안관리 조치에 관한 자체점검 결과 및 자체점검 결과에 따른 조치방안에 관한 사항
4. 제8조에 따른 외국 정부 등과의 접촉 관리에 관한 사항
5. 제9조에 따른 외국 연구자 등의 참여에 관한 사항
6. 보안사고에 대한 조치계획 및 재발방지 대책에 관한 사항
7. 연구기관보안대책을 위반한 연구자에 대한 징계에 관한 사항
8. 보안과제 참여 연구자에 대한 보안수당 지급에 관한 사항
9. 그 밖에 연구개발기관의 장이 보안과 관련하여 심의가 필요하다고 인정하는 사항

② 그 밖에 연구보안심의회의 구성·운영에 관한 사항은 연구기관보안대책으로 정한다.

제7조(보안교육 및 보안서약) ① 연구개발기관의 장은 보안과제를 수행할 예정이거나 수행하고 있는 연구자에 대하여 다음 각 호의 사항을 포함하는 보안교육을 실시하여야 한다.

1. 이 지침에 따른 연구자의 의무 사항
2. 연구기관보안대책에 따른 연구자의 의무 사항
3. 보안과제 수행에 따른 우대조치에 관한 사항
4. 의무사항을 위반할 경우에 법, 「산업기술의 유출방지 및 보호에 관한 법률」, 「대외무역법」에 따라 받을 수 있는 불이익에 관한 사항
5. 그 밖에 보안사고의 예방을 위해 필요한 사항

② 제1항에 따른 교육을 받은 연구자는 연구개발기관의 장에게 보안서약서를 제출하여야 한다.

③ 제2항에 따른 보안서약서의 서식은 별지 제1호 서식을 따르며, 필요한 경우 연구개발기관의 장이 그 내용을 준용하여 정할 수 있다.

④ 연구개발기관의 장은 필요한 경우 보안과제를 수행하지 않는 소속 연구자와 기타 소속 직원에 대해서도 보안교육을 실시할 수 있으며, 특별히 보안상 필요한 경우 서약서를 제출하도록 할 수 있다.

제8조(외국 정부 등과의 접촉 관리 등) ① 보안과제를 수행하고 있거나 수행한지 3

년이 지나지 아니한 연구자가 외국에 소재한 정부·기관·단체 또는 외국인 등(본사와 지사의 소재가 다를 때에는 본사 위치를 기준으로 하는 것을 원칙으로 한다)과 보안과제와 관련하여 접촉(연구자가 상호작용하는 경우 또는 특정하여 유의미한 정도로 접촉이 반복되는 경우를 말한다.) 하는 경우에는 해당 접촉일로부터 10일 이내에 접촉 일시·장소·방법·내용 등에 관한 사항을 현재 소속된 연구개발기관의 장(퇴직으로 소속기관이 없거나 법 제2조제3호에 따른 연구개발기관이 아닌 기관으로 이직하는 경우에는 마지막으로 소속되었던 연구개발기관의 장)에게 보고하여야 한다.

② 보안과제를 수행하고 있거나 수행한지 3년이 지나지 아니한 연구자가 외국 정부·기관·단체 등의 지원을 받아 연구개발을 수행하는 경우 사전에 연구보안심의회의 심의를 거쳐 현재 연구자가 소속된 연구개발기관의 장(퇴직으로 소속기관이 없거나 법 제2조제3호에 따른 연구개발기관이 아닌 기관으로 이직하는 경우에는 마지막으로 소속되었던 연구개발기관의 장)의 사전 승인을 받아야 한다.

③ 연구개발기관의 장은 제1항에 따라 보고받은 사항, 제2항에 따라 사전 승인한 사항을 보고 및 승인 후 1월 이내에 중앙행정기관의 장에 보고하고 국가정보원장에 통보한다.

제9조(외국 연구자 등의 보안과제 참여 등) ① 보안과제에의 대한민국 국적을 가지지 아니한 외국인의 참여는 내국인을 통한 목적달성이 어려울 경우 보충적으로 인정하는 것을 원칙으로 한다.

② 연구개발기관의 장은 보안과제에 관하여 외국 정부·기관·단체 등과 공동연구를 수행하려거나 이들에게 연구의 일부를 수행하게 하려는 경우 중앙행정기관의 장의 사전 승인을 얻어야 한다.

③ 연구개발기관의 장은 보안과제에 대한 외국인의 참여를 승인하려할 경우 제6조에 따른 연구보안심의회의 심의를 거쳐야 한다. 이 때 연구보안심의회는 외국인의 보안과제에의 기여 가능성, 기술격차 등을 고려할 때 향후 외국에의 기술 유출 가능성 등을 종합적으로 검토하여야 한다.

④ 연구개발기관의 장은 제2항에 따라 중앙행정기관의 장의 사전승인을 얻었거나 제3항에 따라 보안과제에 외국인을 참여시킨 경우 해당 사항이 발생하고 1월 이내에 해당 보안과제에서 외국 연구개발기관 등과 공동연구 등을 위한 협약사항 또는 이에 준하는 사항, 또한 참여 외국인의 신상 및 과제 참여 범위, 과제 관련 정보 접근 권한의 범위 등의 정보를 중앙행정기관의 장에 보고하고 국가정보원장에게 통보하여야 한다.

제10조(보안등급 표기) ① 연구개발기관의 장은 보안과제 수행과정에서 산출되는 문서와 다양한 형식의 자료 및 데이터에 대하여 추가적인 보안이 필요한지 여부를 판단하고, 추가적인 보안이 필요한 경우 보안등급을 구분하여 표기하여야 한다.

② 연구개발기관의 장은 연구기관보안대책에 따라 보안등급의 구분을 자율적으로 정할 수 있다. 다만, 보안등급을 정하기 어려울 경우 다음 각 호와 같은 구분을 준

용할 수 있다.

1. I 급 : 유출될 경우 대한민국과 외교관계가 단절되고 전쟁을 일으키며, 국가의 방위계획·정보활동 및 국가방위에 반드시 필요한 과학과 기술의 개발을 위태롭게 하는 등의 우려가 있는 보안과제의 핵심적인 정보
2. II 급 : 유출될 경우 국가안전보장 및 국가경쟁력 확보에 막대한 지장을 끼칠 우려가 있는 보안과제의 핵심적인 정보로 문서나 전자매체 유출이 과제 중요사항의 직접적 유출로 이어질 수 있는 경우
3. III 급: 유출될 경우 국가안전보장 및 국가 경쟁력 확보에 해를 끼칠 우려가 있는 보안과제의 핵심적인 정보로 문서나 전자매체 유출이 과제 중요사항의 직접적 또는 간접적인 유출로 이어질 수 있는 경우

③ 제1항에 따라 보호가 필요한 문서의 종류와 보안등급에 관한 사항은 연구기관보안대책으로 정한다.

제11조(보안과제 수행에 따른 우대조치) 연구개발기관의 장은 보안과제를 수행하는 연구자에 대하여 보안수당 지급 등 우대조치를 할 수 있다.

제12조(보안관리 실태 점검) ① 영 제47조제1항에 따라 중앙행정기관의 장이 수립하는 보안관리 실태 점검계획에 포함되어야 하는 사항은 다음 각 호와 같다.

1. 연구기관보안대책의 수립·시행 실태 점검에 관한 사항
2. 이 지침에 따른 의무사항의 이행 실태 점검에 관한 사항
3. 연구기관보안대책에 따른 의무사항의 이행 실태 점검에 관한 사항
4. 보안관리 실태 점검의 시기·방법에 관한 사항

② 중앙행정기관의 장은 법 제21조제4항 및 영 제47조 따른 보안관리 실태 점검을 실시할 때에 국가정보원장과 합동으로 실시한다.

제13조(보안사고에 대한 조치) ① 연구개발기관의 장은 영 제48조제1항 및 제2항에 따라 중앙행정기관의 장에게 보안사고에 관한 사항을 보고하고 국가정보원장에 통보한다.

② 중앙행정기관의 장은 영 제48조제3항에 따른 보안사고 경위 조사를 국가정보원과 합동으로 실시한다. 이 경우 조사를 실시하기 전에 다음 각 호의 사항을 국가정보원장과 협의한다.

1. 조사방식(서면 또는 현장) 및 조사시기
2. 조사범위 및 조사방법
3. 조사반 구성
4. 그 밖에 조사에 필요한 사항

제14조(연구개발결과에 따른 보안과제 분류) ① 중앙행정기관의 장은 연구개발결과에 따라 보안 과제 여부가 달라질 수 있는 경우 법 제12조제2항에 따른 최종평가를 할 때에 연구개발과제평가단으로 하여금 연구개발결과를 고려한 보안과제 분류의 적정성을 검토하게 할 수 있다.

② 제1항에 따라 연구개발결과를 고려했을 때 보안과제로의 분류가 부적정한 것으

로 판단된 경우, 해당 보안과제는 보안과제분류위원회의 검토 없이 보안과제에서 해제된 것으로 보며, 제3조제4항에 따라 보고 및 통보한다.

③ 제1항에 따라 연구개발결과를 고려했을 때 보안과제로의 분류가 필요하다고 판단된 경우, 해당 연구개발과제는 보안과제분류위원회의 검토 없이 보안과제로 분류된 것으로 보며, 제3조제4항에 따라 보고 및 통보한다.

제15조(보안과제 연구개발성과의 귀속 및 실시) ① 보안과제를 통해 창출된 연구개발성과를 협약에 따라 소유하고 있는 기관은 그 성과의 소유권을 특별한 사정이 없는 한 이전하지 않는 것을 원칙으로 한다.

② 제1항에도 불구하고 보안과제로부터 창출된 연구개발성과의 소유권을 국내의 다른 기관으로 이전할 필요성이 있을 때에는 이전받는 기관이 제3조부터 제15조까지를 적용받도록 계약을 체결하여야 하며, 이 때 제3조부터 제15조의 ‘연구개발기관’은 성과를 이전받는 기관으로 본다. 다만 외국으로의 소유권 이전이 불가피할 경우에는 이에 대하여 중앙행정기관의 장의 사전 승인을 얻어야 한다.

③ 보안과제의 연구개발성과에 대하여 다른 기관과 실시계약을 체결하려는 경우 ‘제3자 기술 실시(사용)권 금지협약’을 체결하여야 하며, 외국기업 또는 외국으로 수출하고자 할 경우에는 중앙행정기관의 장의 사전 승인을 얻어야 한다.

제16조(비공개 연구개발성과에의 준용) 이 대책은 영 제44조제1항제1호의 「산업기술의 유출방지 및 보호에 관한 법률」 제2조제1호에 따른 산업기술과 관련된 비공개 연구성과에 대해서도 준용하여 적용한다. 단, 제3조 및 제11조는 적용하지 않으며, 연구개발기관의 장은 중앙행정기관의 장에 비공개를 요청할 때 과제의 특성에 따라 제8조와 제9조, 제13조, 제15조의 적용을 완화하거나 제외하도록 요청할 수 있다.

제17조 (권한의 대행) ① 중앙행정기관의 장은 보안과제의 관리가 통합적으로 이루어질 수 있도록 전문기관의 부재 또는 전문기관에 관련 보안 취급이 불가능한 경우 등 특별한 사유가 없는 한 제3조, 제8조 및 제9조, 제14조의 사무를 보안관리의 전문성을 높일 수 있도록 당해 과제의 전문기관이 대행하도록 하며, 제12조, 제13조, 제15조까지의 사무는 필요시 전문기관이 대행하도록 할 수 있다.

② 법 제4조에 해당하는 사업의 경우 특별한 사정이 없는 한 해당 연구개발기관이 전문기관으로서 제3조의 사무를 대행하는 것으로 본다.

③ 중앙행정기관의 장은 제1항에 따라 전문기관이 대행하는 업무의 수행에 대하여 평가를 실시할 수 있다.

④ 제1항과 제2항에 따라 보안과제의 관리를 전문기관이 대행하고 있는 경우 보안과제분류위원회는 전문기관에 두어 운영한다.

제18조 (재검토기한) 중앙행정기관의 장은 이 고시에 대하여 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 2022년 1월 1일 기준으로 매 3년이 되는 시점(매 3년째의 12월 31일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

참고 2 연구보안 실태 및 인식조사 주요 결과

1. (전담조직) 연구기관 47.2%(43/91)가 전담조직 존재

① 대학 : 36.1%(13/36) ② 공공연 : 38.7%(12/31) ③ 기업 : 75%(18/24)

2. (국외 수혜정보 관리) 연구기관 66.6%(34/51)가 국외 수혜정보 관리규정 존재

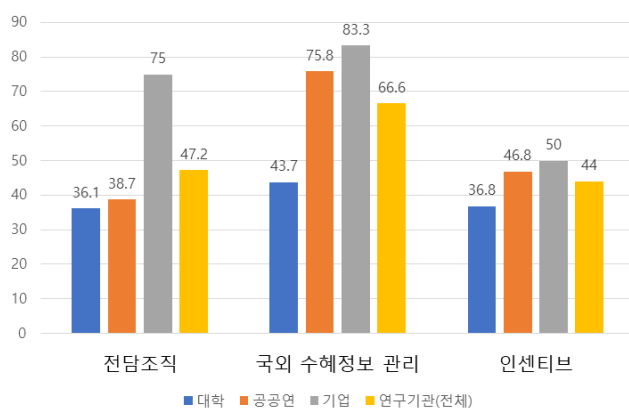
① 대학 : 43.7%(7/16) ② 공공연 : 75.8%(22/29) ③ 기업 : 83.3%(5/6)

3. (인센티브) 연구기관 44%(26/59)가 보안과제 관련 우대조치 규정 존재

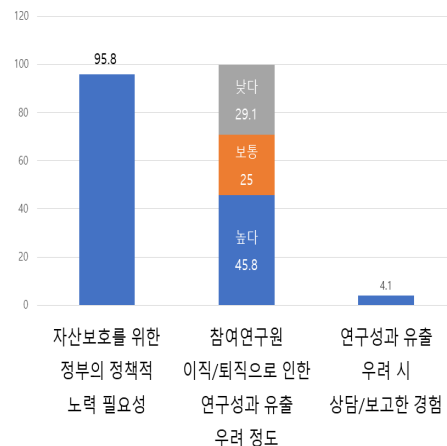
① 대학 : 36.8%(7/19) ② 공공연 : 46.8%(15/32) ③ 기업 : 50%(4/8)

4. (보안인식) 연구자는 국가R&D 자산 보호를 위한 정책적인 노력이 필요하다 (95.8%, 69/72)고 생각하나, 성과유출 우려 시 상담·보고한 경험은 미미

- 연구원의 이직 및 퇴직 등으로 인한 연구성과 유출 우려 : (매우)높다 45.8% (33/72)
- 연구성과 유출 우려시 소속기관에 상담·보고한 경험 : 4.1%(3/72)



< 연구기관 대상 >



< 연구자 대상 >

< 연구보안 실태 및 인식조사 개요 >

○ (조사시기·방법) '23.4~6월/ 심층인터뷰 및 설문조사

○ 조사대상

- (심층인터뷰) 전문기관(4), KAIST, KIST, 생기연, 항우연, 보안과제 수행기업 등 11곳
- (설문조사) 전문기관(15), 대학 산단*(50), 공공연(36), 기업(40), 대학 연구자**(100)

*정부지원 연구비 규모가 250억원 이상 **전략기술 분야 전문가 또는 정부연구비 규모가 소속대학 내에서 상 또는 중인 연구자

○ 주요 조사항목

- (전문기관) 연구보안 전담조직 유무, 보안과제 분류 시기 및 절차, 실태점검 시기
- (연구기관) 연구보안 전담조직 유무, 국외수혜정보 관리규정, 보안과제 우대조치
- (연구자) 연구성과 유출을 우려한 정도, 연구성과 유출 우려 시 소속기관 상담·보고한 경험

자료: 연구보안 체계 내실화 방안(안), 국가과학기술자문회의 제5회 심의회의(2023. 9. 26.)