이일구 교수 지도

석사학위 청구논문

핵심 기술 인재 보호를 위한 특허 제도 방안 연구: 기술 보호와 개인정보 보호의 균형 전략을 중심으로

2025

성신여자대학교 대학원

미래융합기술공학과

송현채

핵심 기술 인재 보호를 위한 특허 제도 방안 연구: 기술 보호와 개인정보 보호의 균형 전략을 중심으로

이일구 교수 지도

이 논문을 석사학위논문으로 제출함

2025년 5월

성신여자대학교 대학원
미래융합기술공학과
송현채

인 준 서

송현채의 석사학위 논문으로 인준함

2025년 6월

심사위원장 김 성 민 (서명 또는 인)

심 사 위 원 임 연 섭 (서명 또는 인)

심 사 위 원 이 일 구 (서명 또는 인)

성신여자대학교 대학원

논문 개요

첨단 산업 기술의 급속한 발전과 글로벌 기술 패권 경쟁의 심화는 핵심 기술 인재 확보와 보호를 국가와 기업 차원에서 중요한 전략적 과제로 부각시키고 있다. 특히, 반도체, 인공지능(AI), 바이오헬스, 이차전지 등 국가 전략기술 분야에서의 경쟁은 단순한 기술 개발을 넘어서, 해당 기술을 창조하고 지속적으로 발전시킬 수 있는 핵심 인재를 선점하고 보호하는 역량에 따라 기술 패권이 결정되는 구조로 변화하고 있다. 이러한 흐름 속에서 인재 유출 문제는 보안과 산업 전략 측면에서 중요한 변수로 떠오르고 있다. 특히, 공개된 정보를 기반으로 핵심 인재를 식별하고 스카우트할 수 있어서, 가능성은 산업 보안 측면에서도 주요 변수로 떠오르고 있다.

그러나 특허 제도는 기술 정보의 공공성과 산업 재산권 보호를 목적으로 발명자의 이름뿐만 아니라 상세한 주소(건물명, 아파트의 동·호수 등 포함)까지 특허공보를 통해 전부 공개하고 있다. 과거에는 이 정보를 확인하기 위해 특허공보를 수작업으로 확인해야 했지만, 인공지능(AI)과 빅데이터 분석 기술의 발전으로 공개된 정보를 바탕으로 특정 인재를 식별하는 것이 기술적으로 가능해졌다. 실제로 일부 기업이나 투자자 및 해외 연구기관 등에서 이를 활용해 우수 인재를 선별하는 사례도 점차 증가하고 있다. 이는 특정 기업이나 국가가 오랜 기간 육성한 인재의 의지와 무관하게 외부에서 식별되고 접촉 대상이 될 수 있는 보안 취약성과 구조적 보안 위협을 의미한다.

본 연구는 이러한 구조적 취약성을 해결하기 위한 대안을 제안한다. 우선 한국 특허공보의 공개 정보 구조와 개인정보 기재 방식을 분석하고, 이를 바탕으로 미국, 유럽, 일본, 중국 등 주요국의 특허 제도와 비교함으로써 국제적 개인정보 보호 기준과의 차이점을 분석한다. 또한, 실제 공개된 특허

데이터를 기반으로 AI 및 데이터 분석이 인재 식별에 어떻게 활용될 수 있는지에 대한 사례를 분석하고, 인재 유출의 가능성을 구체적으로 도출하였다. 이 과정에서 기술 정보 공개의 공공성은 유지하되, 발명자의 개인정보 노출을 최소화할 수 있는 제도적 설계의 방향성을 모색한다.

특히 본 연구는 고유 연구자 번호(예: 국가 연구자 번호, ORCID 등)를 활용하여 발명자의 신원을 비식별화 하고, 연구 성과와 정보 열람은 연구자 본인의 선택적 정보 제공 동의하에 이루어지는 구조를 제안한다. 이 방법은 개인정보 보호와 기술 정보의 연계를 동시에 달성할 수 있는 실질적 대안으로 기능할 수 있으며, 연구자, 기업, 과제 관리자 등 다양한 이해관계자가 특허 정보를 효율적으로 활용할 수 있는 기반을 제공한다.

연구 방법론적으로는 국내외 특허 제도 비교 분석, 실제 공보 데이터 기반으로 한 실태 분석, 유출 사례 조사 그리고 이해관계자별 연구자 번호 활용 가능성 평가를 진행했다. 제안하는 대응 방안의 실현 가능성과 기대 효과를 정량적·정성적으로 검토하고 향후 제도적 설계 시 고려해야 할 기준을 제시하였다.

본 연구는 기술 정보의 공개를 전제로 한 특허 제도하에서도, 핵심 인재 보호와 개인정보 비공개를 동시에 실현할 수 있는 정보관리 체계를 제안한다. 단순히 제도를 비판하는 것에 그치지 않고, 기술 인재의 유출을 사전에 차단하고 첨단산업의 경쟁력을 장기적으로 확보하기 위한 인적자원 보안 전략을 수립하는데 기여할 수 있을 것이다.

목 차

표 차 례

그림 차례

제 Ⅰ 장 서론

1. 연구 배경 및 필요성

근래 인공지능(AI), 반도체, 바이오헬스, 항공우주 등 첨단산업 기술의 급진적인 성장은 국가와 기업 간 기술 경쟁을 더욱 치열하게 만들고 있다. 첨단 기술을 확보하고 고도화하는 것은 단순한 기술적 우위를 넘어 국가 경제력, 산업 주권, 나아가 국가 안보에까지 직결되는 중요한 요소로 자리잡았다. 이에 따라 특정 기술의 보유 여부뿐만 아니라 해당 기술을 창출하고 지속적으로 발전시킬 수 있는 핵심 인재의 확보와 보호가 국가적, 기업적 차원에서 중요한 전략적 과제로 부각되고 있다 [1].

이와 같은 산업 환경의 변화는 고급 기술 인재를 둘러싼 경쟁을 심화시키고 있다. 특히 산업통상자원부와 한국산업기술진흥원이 발표한 「2024년 산업기술 인력 수급 실태조사」에 따르면, 국내 핵심 산업에서 약 3만 8천여 명의 기술 인력이 부족한 것으로 나타났다. 이 중 소프트웨어 분야의 부족률은 3.9%로 가장 높았으며, 반도체(2.0%), 바이오헬스(1.9%) 등 전략 기술 분야 역시 지속적인 인재 부족 문제를 겪고 있다. 이와 같은 현상은 단편적인 인력 수급의 불균형으로만 보일 수도 있지만, 결국 미래 산업의 성장 기반을 위협하는 심각한 문제로 이어질 수 있다. 아래 그림으로 산업별 기술 인력 부족 인원과 부족률을 나타냈다.

[그림 1] 산업별 기술 인력 부족률

첨단산업 분야는 연구개발(R&D) 역량, 축적된 노하우, 창의적 사고를 지닌 사람에 의해 기술 혁신이 이루어진다는 점에서, 이러한 기술과 지식을 보유한 핵심 인재의 이탈은 인력 손실뿐 아니라 기업 및 국가 전체의 기술력 저하로 이어질 가능성이 크다. 따라서 핵심 인재의 유출을 방지하고 보호하는 것은 기술 혁신과 경쟁력 유지에 필수적인 요소로 자리잡고 있다.

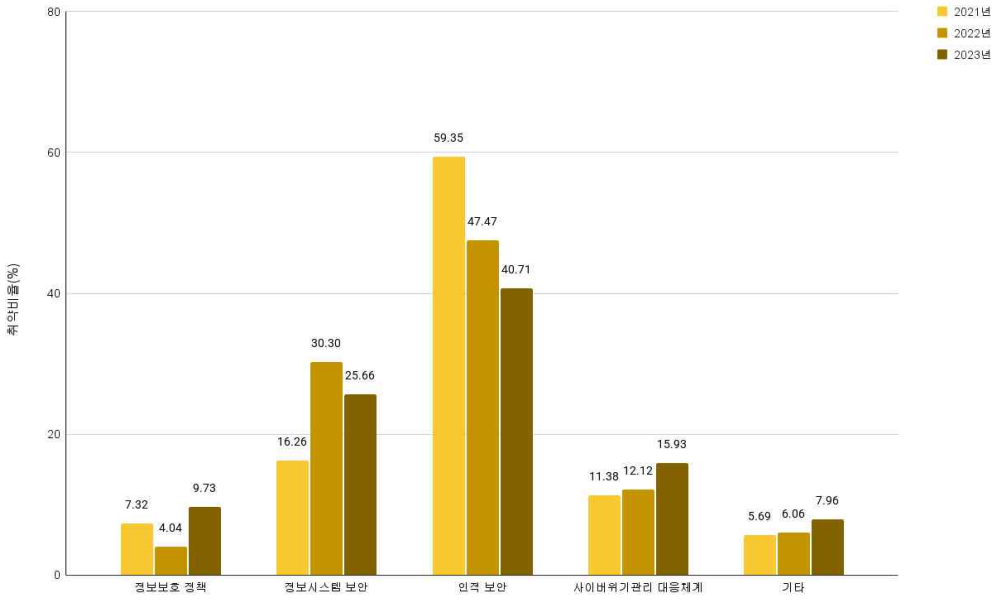
정보보호 및 개인정보보호 관리 체계(ISMS-P) 인증 기준은 인적 보안을 핵심 관리 항목으로 규정하고 있으며, 인력의 채용부터 퇴직까지 전 주기에 걸쳐 보안 리스크를 예방 및 관리할 수 있도록 다양한 보호 대책을 제시한다. 이에 따라 다수의 기업과 연구기관은 핵심 인재의 유출 방지 및 내부 위협 대응 역량을 강화하기 위해 관리적 보호 체계를 구축하고 있다. 주요 수단으로는 보안 서약서 작성, 보안 인식 제고 교육, 직무별 보안 책임 명시, 퇴직자 권한 회수 절차 구축 등이 포함된다 [2].

실무적으로는 이러한 조치를 바탕으로 비밀유지계약(NDA) 체계화, 직무

기반 이직 제한 협약의 활용, 보안사고 예방 중심의 퇴직 프로세스 설계 등이 병행되고 있으며, 이는 인적자원과 관련된 보안 관리 수준을 제도적으로 확보하는 기반이 된다. 그러나 현시점에서 인적자원 보안과 보호 체계는 주로 내부자에 의한 기술 유출 방지를 중점적으로 다루고 있고, 외부 정보 공개를 통해 발생할 수 있는 인재 식별이나 유출에 대한 대비는 상대적으로 취약하다.

특히, 특허 출원 과정에서 발명자의 개인정보(이름, 주소 등)가 세부적으로 공개되는 현행 제도를 살펴보면, 과거에는 비교적 제한된 정보만을 활용하도록 공개했지만, 최근 인공지능(AI) 및 빅데이터 분석 기술의 발전으로 심각한 보안 취약점이 되고 있다. 공개된 정보는 외부 공격자나 경쟁자가 쉽게 접근할 수 있는 자료가 되어, 핵심 인재의 식별 및 스카우트가 가능해지며, 첨단 산업의 보안을 위협하는 주요 요소로 떠오르고 있다.

국가정보원의 2024 국가정보보호백서에 따르면, 많은 기관이 기술적·물리적 보안 조치에 비해 인적 보안 영역에서 상대적으로 낮은 이행 수준과 취약한 대응 체계를 보이는 것으로 나타났다. 최근 3년간 정보보호 분야별 이행률 분석에 따르면, 인적 보안 분야의 취약 비율은 점진적으로 감소하고 있지만, 여전히 다른 보호 조치에 비해 가장 낮은 수준을 유지하고 있다. 특히, 보안 서약서 미작성, 정기 보안 교육의 미흡, 퇴직자 계정 미회수 등 기본적인 인적 보호 절차의 누락이 반복적으로 지적되고 있다 [3]. 이러한 미비점은 인적 요소를 통한 정보 유출 및 기술 침해의 가능성을 지속적으로 확대시키고 있다. 이와 같은 상황은 인적자원 보안이 기술적 보안 못지않게 독립적인 전략 수립과 체계적인 관리가 요구되는 핵심 영역임을 시사한다. 다음 그림은 2024 국가정보보호백서의 정보보호 분야별 취약률을 재구성한 것이다.



[그림 2] 정보보호 분야별 취약률

최근 인공지능(AI) 기반 분석 시스템은 특허공보, 논문, 산업 리포트, 소셜 네트워크 정보 등을 통합적으로 분석하여, 특정 기술 분야의 연구자, 발명자, 개발자를 식별하고 그들의 전문성, 경력 및 이력, 기술 기여도 등을 정밀하게 평가할 수 있다. 이러한 데이터 분석 결과는 인재 스카우트, 경쟁사 타게팅, 기술 정보 수집 등 다양한 방식으로 활용될 수 있으며, 핵심 인재를 보유한 기업에는 심각한 위협 요소로 작용할 수 있다 [4].

WIPO의 World Intellectual Property Indicators 2024 보고서에 따르면, 주요 국가들은 개인정보 보호를 위해 발명자 주소 공개를 제한하는 추세에 있다. 그러나 한국은 특허공보에 발명자의 이름뿐만 아니라 상세 주소(건물명, 아파트 동, 호수까지)까지 공개하는 관행을 유지하고 있어서 개인정보 노출 위험이 매우 큰 상황이다. 반면, 미국과 유럽 등 주요 국가들은 발명자의 상세 주소를 공개하지 않거나, 도시 수준의 정보만 제공하는 방식으로 개인정보 보호를 강화하고 있다.

첨단산업에서 핵심 인재는 기술 경쟁력의 핵심 동력이며, 산업의 혁신과 미래 성장을 이끄는 중요한 기반이다. 따라서 특허 제도의 기술 정보 공개 취지를 존중하면서도 인재 유출 위협을 예방하기 위한 정보보호 체계의 재설계가 필수적이다. 정보 공개와 보호, 데이터 활용의 균형을 적절하게 수립하는 것은 첨단산업 경쟁력을 지속 가능한 방향으로 발전하기 위해 반드시 해결해야 할 과제이다.

2. 연구 목적

본 연구는 첨단산업 기술 경쟁이 심화됨에 따른 핵심 인재 확보 및 보호의 중요성이 증대되고 있는 현실을 반영하여, 특허 공개 정보를 통한 인재 식별 및 유출 위험성을 체계적으로 분석하고, 이에 대응할 수 있는 구체적 방안을 제시하는 것을 목적으로 한다.

특허 제도는 기술에 대한 독점적인 권리를 보장하는 동시에, 일정 수준의 정보 공개를 통해 기술의 확산과 산업 발전을 도모하는 것을 목적으로 설계되어왔다. 이에 따라, 지식재산 권리관계를 명확하게 공시하기 위해 발명자의 이름과 상세 주소, 소속기관 등의 정보가 특허공보를 통해 누구나 열람 가능한 형태로 공개되는 구조를 갖추고 있다. 과거에는 정보 분석 기술의 한계와 접근성 제약으로 인해, 이러한 정보가 인재 유출이나 스카우트 전략에 실질적으로 활용되는 사례는 제한적이었다. 그러나 최근 인공지능 기반 분석 기술의 고도화와 정보 접근성의 비약적인 향상으로 인해, 특허 공개정보가 인재 식별 및 유출에 활용될 가능성이 현저히 증가하고 있다.

취지 구분	내용	기대 효과
기술의 사회적 공유 및 확산	발명의 내용을 공개하여 다른 이들이 기술을 학습/응용	- 기술의 누적적 발전 - 산업 전반의 혁신 촉진
기술 정보의 축적과 공공재 역할	공개 특허를 통해 기술 데이터베이스 구축	- R&D 전략 수립 - 기술 동향 분석 - 정책 참고 자료로 활용
중복 연구 방지	기존 기술을 공개하여 불필요한 중복 개발을 방지	- 연구 자원의 효율적 배분 - 신기술 개발
법적 안정성 및 권리 보호	기술 내용을 명시적으로 공시	- 제3자의 권리 침해 예방 - 법적 분쟁 대비 및 회피 가능성 제공

[표 1] 특허제도의 정보 공개 주요 취지

인공지능(AI) 기반의 데이터 분석 기술은 특허공보, 학술 논문, 산업 리포트, 연구자의 온라인 이력 및 소셜 미디어 정보 등을 통합적으로 수집·분석함으로써 특정 기술 분야에서의 핵심 인재를 정밀하게 식별할 수 있는 기반을 제공하고 있다. 이러한 분석은 발명자의 기술 기여도, 연구 성과, 소속 조직 및 경력 흐름을 가시화함으로써, 경쟁 기업이나 해외기관이 인재 확보 전략을 설계하는 데 매우 효과적인 도구로 작용할 수 있다. 특히, 이 과정에서 특허공보에 명시된 상세 주소 정보는 단순한 거주지를 넘어서 해당 인재의 사적 활동, 생활권, 조직 내부 배치 등의 간접적 정보로 확장되며 이는 개인의 프라이버시 침해와 더불어 기업 내 인재 구조의 외부 노출로 이어질 수 있다.

이와 같은 환경 변화에도 불구하고 현재의 인적자원 보안 체계는 여전히 내부 위협 관리에 집중되어 있으며, 외부 공개 정보를 기반으로 발생할 수 있는 유출 위험에 대해서는 체계적이고 실질적인 대응이 미비한 실정이다. 기존의 보안 체계는 주로 네트워크 통제, 문서 접근 제한, 비밀유지계약(NDA) 체결 등을 중심으로 설계되어 있고 공개 정보가 외부 분석 도구에 의해 재해석되고 유출 위험으로 전환되는 과정에 대해서는 근본적인 통제

수단이 부족하다. 더욱이 이러한 정보는 한 번 공개되면 회수나 수정이 어렵기 때문에 사후 대응보다는 사전 관리 체계의 정비가 시급하다.

본 연구의 주요 기여점은 다음과 같다.

첫째, 현행 특허 출원 및 공개 과정에서 발명자의 개인정보가 어떤 방식으로 노출되는지 분석하고, 이러한 정보 노출이 어떤 수준의 잠재적 위협으로 확장될 수 있는지 규명한다. 이를 위해 한국 특허 제도를 중심으로 미국, 유럽, 일본, 중국과 같은 주요국의 특허 정보 공개 방식과 개인정보 보호 수준을 비교 분석하고, 국내 제도의 기능적인 한계점과 개선 필요성을 진단한다.

둘째, 인공지능(AI) 및 데이터 분석 기술이 공개된 특허 정보에 포함된 개인정보를 활용하여 핵심 인재를 어떻게 식별하고 추적하는지 실증적으로 고찰한다. 다양한 공개 정보의 결합 분석을 통해 개인의 기술 이력과 조직적 위치를 시각화하는 기술은 인적자원 관리 측면에서 유용하게 활용될 수 있으나 경쟁사에 의해 활용되면 인재를 잠재적으로 유출하고 기업의 전략적 자산을 침해하여 기술 경쟁력을 약화하는 결과로 이어질 수 있다. 이와 같은 공개된 특허 정보를 활용하는 방식은 기존의 보안 통제 범위를 넘어서는 영역으로 새로운 형태의 위협으로 인식될 수 있다.

셋째, 공개 정보의 투명성과 공공성을 유지하면서도 발명자의 개인정보를 효과적으로 보호할 수 있는 실질적인 대안을 모색한다.

본 연구는 정보 공개가 필수적인 첨단산업 환경에서 기업의 핵심 인재를 효과적으로 보호하고 관리하기 위한 균형 잡힌 인적자원 보안 전략을 제안하고, 이를 통해 산업 경쟁력을 유지하면서 개인정보 보호의 원칙을 구현할 수 있는 정책적 시사점을 도출하고자 한다.

제 Ⅱ 장 이론적 배경

1. 인적자원 보안

1) 인적자원 보안

인적자원 보안(Human Resource Security)은 조직 내 인력의 고의적 혹은 비의도적 행위로 인한 보안 위협을 예방하고, 인력과 관련된 정보 자산의 보호를 통해 조직의 지속가능성과 기술 경쟁력을 확보하는 관리 체계를 의미한다 [5]. 전통적으로 보안은 기술적 조치(예: 방화벽, 접근통제 시스템 등)에 초점을 맞추어 발전해 왔지만, 실제 보안 사고의 상당수가 사람의 실수나 악의적 행위에서 비롯된다는 점에서 인적 요인을 중심으로 한 보안의 중요성이 지속적으로 강조 되어왔다.

특히 산업기술의 고도화, 글로벌 인재 유치 경쟁, 조직 구조의 유연화 등 변화하는 환경 속에서 인적자원 보안은 단순한 조직 내부의 통제를 넘어서 인재 유출, 기술 노하우의 외부 노출, 사이버 위협과의 연계 가능성 등 보다 복합적인 차원으로 확장되고 있다. 이에 따라 기존의 보안 정책에서 다루지 못했던 인력 중심의 리스크를 식별하고 이에 대한 대응체계를 구축하는 것이 인적자원 보안의 핵심 과제로 부상하게 되었다. Prato(2022)는 발명가의 국제 이동이 지식 확산과 생산성 성장에 미치는 영향을 분석하며, 글로벌 인재 경쟁의 심화를 강조하였다 [6].

2) 인적자원 보안 구성요소

인적자원 보안은 일반적으로 다음의 세 가지 주요 항목으로 구성된다.

- 사전 예방(pre-employment security): 채용 전 단계에서의 신원 확인, 배경 조사, 직무 적합성 평가 등을 통해 조직 내 보안 리스크를 최소화한다. 특히 국가 보안 기관이나 방산, 첨단 기술 기업에서는 이 단계가 더

욱 강조된다 [7].

- 재직 중 통제(in-employment control): 내부자 위협 탐지, 접근 권한 관리, 정보보안 교육, 보안 서약 체결 등을 통해 정보 유출 위험을 줄이고 직원의 보안 인식을 제고한다. 기술 중심 조직일수록 보안 문화 정착이 중요하게 작용한다 [8].
- 퇴직 후 조치(post-employment control): 퇴직자에 대한 보안 규정 유지, 퇴직 후 일정 기간 기술 정보 사용 제한(경업 금지) 조항, 퇴사자 로그 분석 등 조직 이탈 이후에도 정보 유출 가능성을 관리하는 단계이다 [9].

이러한 요소들은 개별적으로 작동하기보다 조직의 보안 전략 및 인사 전략과 유기적으로 통합되어야 한다. 특히 핵심 기술 인력이 많은 연구기관이나 기술 스타트업의 경우 인재 이탈이 곧 조직의 경쟁력 상실로 직결될 수 있으므로 인적자원 보안 체계의 전략적 운영이 필수적이다 [10].

3) 첨단산업 분야의 인적자원 보안

첨단산업 분야에서 인적자원 보안은 그동안 '내부자 위협(insider threat)' 대응을 중심으로 구축되었다. 특히 조직 내부 구성원이 접근할 수 있는 정보의 권한을 악용하거나 비고의적으로 민감한 정보가 유출되는 사례에 대한 주의가 강조되었다. 이에 따라 일부 기관과 기업은 비밀유지계약(NDA)의 체계적인 운영, 직무 기반 접근 제한 및 통제, 퇴직자 보안 프로토콜 적용 등 제도적 보안 도구들을 통해 인적 리스크를 관리하고 있다 [11].

그러나 최근 디지털 환경에서는 정보의 공개와 공유가 기본이 되면서 보안 위협이 단순히 내부 통제만으로는 대응하기 어려운 상황이 되었고 외부 요인에 의한 침해 가능성도 점점 커지고 있다. 예를 들어 특허공보나 학술논문, 연구 보고서 등에 포함된 발명자 및 연구자의 인적 정보는 인공지능(AI), 크롤링, 데이터 마이닝 기술과 결합되어 특정 인재의 경력, 소속, 기술 역량 등을 파악 및 분석하는데 활용되고 있다. 공개된 정보는 경쟁 기업이

나 해외기관이 인재를 스카우트하거나 기술 구조를 파악하는 데 활용될 수 있고 그 결과로 핵심 인재와 기술이 외부로 유출되는 보안 위협으로 이어질 가능성이 있다.

특히 첨단산업 분야는 고도의 전문성과 축적된 노하우를 보유한 소수 인재에 의해 기술 발전이 주도되는 구조를 갖는다. 반도체, AI, 바이오, 항공우주 등과 같은 분야에서는 기술 자체만큼이나 이를 운용하고 발전시키는 핵심 인재가 기업 경쟁력의 핵심 자산이다. 이들의 이탈은 단순한 인력 유출을 넘어 기업의 전략, 기술 노하우 등 무형 자산 전반이 외부로 유출되는 결과를 초래할 수 있다.

그러나 기존 인적자원 보안 정책은 조직 내부의 통제와 교육, 제도적 규정에만 집중되어 왔으며 공개 정보 기반의 인재 식별 가능성이나 외부 스카우트 위협에 대해서는 충분한 대응 체계를 갖추지 못하고 있다. 이에 따라 기업이나 연구기관은 핵심 인재를 외부의 정밀 분석 대상에 그대로 노출하고 있으며 정보 비대칭 상황에서의 일방적인 인재 유출 가능성을 내포하게 된다.

인재 유출은 단순히 조직 외부의 채용 경쟁이나 산업 이직으로만 발생하는 것이 아니라, 정보시스템 내에 노출된 민감 정보로부터 시작되기도 한다. 특히 인적 보안 체계가 기술적 보안에 비해 상대적으로 미흡한 경우, 내부 정보의 유출뿐만 아니라 외부에서의 인재 식별 및 접근이 쉬워져 유출 가능성이 구조적으로 확대된다.

국내 다수 기업과 연구기관이 내부자 위협에 대비한 보안 교육, 권한 통제 등 내부 보안 정책을 운영하고 있지만, 공개 정보에 의한 외부 식별 및 유출 위험에 대해서는 별도의 인적 보안 체계를 갖추지 못하고 있다 [12]. 이는 곧 정보공개 구조의 허점이 곧 인재 유출의 사각지대를 형성할 수 있다는 점을 시사하며, 정보보호와 인재보호를 통합적으로 접근하는 인적보안

개념의 확장이 요구된다.

궁극적으로 본 논문이 다룬 특허제도의 정보공개 문제는 단순한 개인정보 보호의 영역을 넘어, 인적보안과 인재유출이라는 보다 구조적이고 전략적인 문제로 확장될 수밖에 없다. 인적보안이 단지 내부자의 악의적 행위를 차단하는 소극적 수단이 아니라, 기술 역량의 외부 유출을 예방하는 적극적 전략으로 작동해야 한다는 인식 전환이 필요하다.

2. 특허 정보 공개 제도의 구조와 한계

1) 특허제도의 정보 공개 원칙

특허제도는 본질적으로 '정보의 독점'과 '정보의 공개'라는 상반된 두 요소를 동시에 내포한다. 특허권자는 일정 기간 동안 발명을 독점적으로 이용할 수 있는 권리를 부여받는 대신 해당 발명에 대한 기술적 내용을 공보로 공개하여 산업 전체 기술 발전에 기여 해야 한다. 이러한 제도의 기본 원리는 '공개를 통한 기술 발전'과 '보호를 통한 인센티브 제공'이라는 이중 구조에 기초하고 있으며 이는 주요 국가에서 공통적으로 유지되는 특허제도의 핵심 가치이다.

이 과정에서 발명자 및 출원인의 정보는 특허 출원 시점부터 공보를 통해 대외적으로 공개된다. 여기에는 발명자의 이름, 주소, 출원인 및 대리인의 정보 등이 포함되는데 한국 특허제도에서는 발명자의 상세 주소(건물명, 아파트의 동, 호수)까지 공보에 기재하는 것이 일반적인 관행으로 유지되고 있다. 개인정보 공개는 제도의 투명성과 공정성 확보에 기여했지만 최근에는 정보기술의 발전으로 민감한 개인정보가 노출되기 쉬워지면서 보안 및 프라이버시 침해 문제로 비판의 목소리가 커지고 있다.

특히 인공지능(AI) 기반의 데이터분석 기술이 고도화되면서 특허 정보에 포함된 발명자 정보가 타인의 기술 분야, 소속, 연구 경력 등을 식별하는 주요 실마리로 활용될 수 있다는 점이 문제로 지적된다. 이는 개인정보 보호

의 이슈이면서 동시에 첨단기술 인력 유출이라는 산업 보안 위협으로도 간주될 수 있다.

한국 특허공보는 특허청(KIPO)에서 발간하며 출원공개공보와 등록공보로 구분된다. 일반적으로 출원공개는 출원일로부터 18개월이 경과한 이후 진행되며 이후 심사를 통과한 발명은 특허 등록 공보를 통해 최종 등록 내용이 공개된다. 공보에는 발명의 명칭, 요약, 도면, 청구항 등 기술적 정보뿐 아니라 발명자의 이름과 주소, 출원인의 정보, 대리인 정보 등 다양한 인적 식별 정보가 포함된다.

문제는 이 중 특히 발명자의 주소 정보가 세부 단위(예: '서울시 강남구 역삼동 ○○아파트 ○○동 ○○호')까지 상세히 기재되어 있다는 점이다. 이러한 수준의 정보 공개는 다른 주요국에 비해 상당히 높은 개인정보 노출 수위를 보인다. 일반적으로 미국은 도시나 주(State) 단위까지만 공개하고 있으며, 유럽특허청(EPO)은 발명자의 이름만을 표기하거나 주소 공개를 최소화하고 있다.

한국에서의 상세 주소 공개는 과거에는 상대적으로 활용 가능성이 낮은 정보로 인식되었으나 최근 AI 기반 분석 기술, 공개데이터 수집 시스템, 조직 구조 분석 도구 등이 발달함에 따라 외부에서 특정 인재의 위치, 소속, 연구 활동을 역추적할 수 있는 주요 수단으로 작용하게 되었다. 실제로 특허공보에 나타난 주소 정보를 기반으로 발명자의 주거지 및 근무지까지 추적이 가능하며 이를 통해 특정 조직의 핵심 기술 인력을 식별하고 스카우트하는 행위가 가능하다는 점에서 산업 보안 관점에서의 대응 필요성이 제기되고 있다 [13].

2) 특허 주소 공개 방식 변경 제도

① 제도의 개요

이와 같은 문제 제기에 따라 한국 특허청은 개인정보 보호 요구를 반영해

‘주소 게재 방식 변경 제도’를 운영하고 있다. 이 제도는 일정 요건을 충족하면 발명자의 주소를 공보에 전면 게재하지 않고, 간략화된 형태(예: 시/도까지만 기재하거나 생략)로 변경할 수 있도록 허용한 것이다. 법적 근거는 「특허공보 게재·기재 생략 등에 관한 기준」(특허청 훈령)에 명시되어 있으며, 2021년 이후 관련 개정이 이루어졌다.

이 제도의 개요는 다음과 같다.

구분	내용
신청 대상	해당 발명의 발명자 본인 또는 그 대리인
신청 시점	출원공개 이전 또는 출원공개 이후에도 가능하나 공보 발행 시점에 따라 반영 여부가 달라짐
신청 방법	특허청 홈페이지를 통해 온라인 신청 가능
적용 범위	주소 전체를 생략하거나 동 단위 이하를 제외한 형태로 변경 가능
변경 대상 공보	(1) 변경 신청 접수일 이후 발간되는 공보 (2) 신청 이전 발간되었으나 온라인에서 제공 중인 공보

[표 2] 특허 주소 공개 방식 변경 제도 개요

이 제도는 개인정보 보호 강화를 위한 긍정적 시도라는 평가를 받지만, 자발적인 신청을 전제로 하고 있으며, 주소 공개가 기본값으로 유지된다는 점에서 구조적인 한계가 있다. 실제로 많은 발명자가 이 제도를 인지하지 못하거나 신청 방법을 몰라 활용하지 못하는 사례가 발생하고 있다.

② 제도의 실효성 문제 분석

특허 주소 공개 방식 변경 제도의 실효성을 평가하기 위해서는 신청률, 제도 인식 수준, 정보 노출 지속 사례 등을 복합적으로 검토해 볼 필요가 있다.

첫째, 실제 주소 공개 방식 변경 신청 비율은 매우 낮다. 특허청 내부 자료나 관련 보고서에 따르면 변경 신청 사례는 전체 출원 건수에 비해 상당히 일부에 해당하고 특허공보 대부분에는 상세 주소가 공개되고 있는 현실이다. 제도 이용 과정이 불편하고, 제도에 대한 정보가 부족하며, 신청을 유도할 유인이 부족하여 주소 공개 방식 변경 신청률이 매우 낮은 것으로 분

석된다.

둘째, 이미 발간된 공보의 정보는 지속적으로 공개되고 있다. 제도적으로는 과거 공보에 대해서도 변경 신청이 가능한 것으로 명시되어 있지만 실제로는 변경 반영이 지연되거나 일부 플랫폼에서는 이전 정보가 이전과 똑같이 노출되는 경우도 존재한다. 이는 개인정보의 통제가 사후적으로 완전하게 작동하지 않는다는 점을 시사한다.

셋째, 제도 인식 수준이 낮다. 다수의 연구자와 기업들은 해당 제도의 존재조차 알지 못하고 특허출원 시 주소 정보가 자동으로 공개된다는 사실에 대해서도 별다른 문제의식을 느끼지 못하고 있다. 심지어 일부 변리사나 출원 대리인조차도 신청 절차를 안내하지 않는 사례가 있어 정보 불균형이 제도 활용을 제한하는 구조적인 요인으로 작용한다.

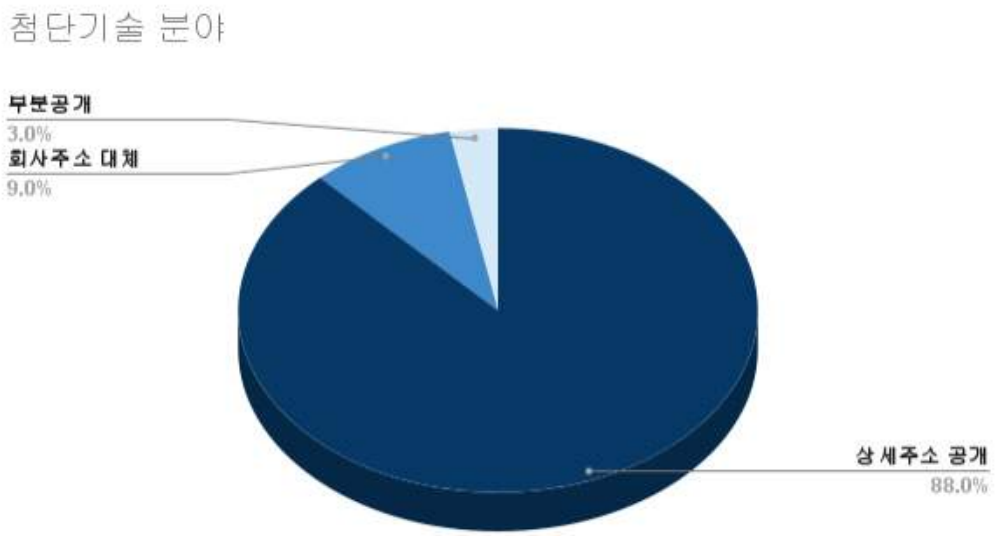
결과적으로 주소 게재 방식 변경 제도는 존재하지만, 실질적인 보호 장치로서 기능을 하지 못하고 있고 현재와 같은 신청 기반, 임의 적용 방식만으로는 공개 정보 기반의 개인정보 노출 문제를 해결하기 어렵다. 향후에는 개인정보 보호를 기본 전제로 하고 특별한 경우에만 예외적으로 전체 주소를 공개하는 '기본 비공개-예외 공개' 방식으로의 전환이 필요하다는 지적이 제기되고 있다 [14].

③ 특허 주소 공개 실태에 대한 실증 분석

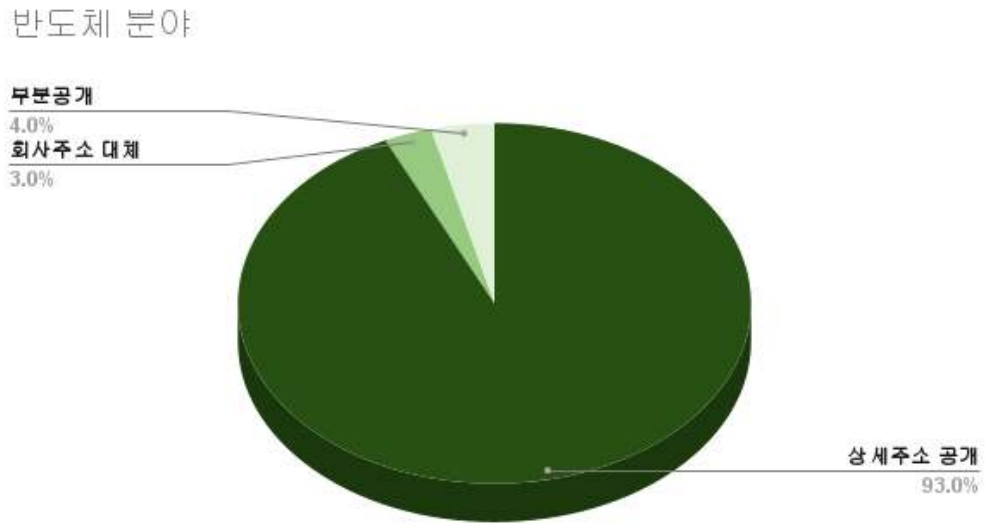
앞서 살펴본 바와 같이 국내 특허공보에 포함되는 발명자 주소 정보는 구조적으로 상세하게 공개되고 있으며 주소 공개 방식 변경 제도가 존재함에도 불구하고 신청 기반의 선택적 보호 체계로 인해 제도적 실효성에 한계가 있다는 지적이 있다. 이를 보완하기 위해 본 연구자는 실제 국내 특허정보 검색 서비스(KIPRIS)를 통해 '첨단기술'과 '반도체'를 키워드로 각각 100건씩의 공보를 표본 조사하고, 각 공보에서 기재된 주소의 공개 양상을 유형별로 분류하여 분석하였다.

분석 결과 ‘첨단기술’ 키워드로 검색한 공보 100건 중 상세 주소(동, 호수 등)까지 공개된 공보는 총 88건이었고, 기업 또는 기관 주소로 대체 기재된 사례는 9건, 일부 주소만 기재된 부분 공개 사례는 3건으로 나타났다. ‘반도체’ 키워드의 경우에는 상세 주소가 공개된 사례가 93건으로 더 높았으며 회사 주소 기재는 3건, 부분 공개는 4건이었다.

특히 주목할 점은 본 분석에서 확인한 공보들은 행정 상태 기준을 ‘전체’로 설정하여 검색된 것으로 등록 완료된 특허뿐 아니라 공개, 거절, 취하, 소멸 상태의 특허까지 포함되어 있다는 점이다. 그런데도 이러한 공보들 대부분에서 발명자의 상세 주소가 그대로 노출되고 있었으며 이는 주소 비공개 신청 제도가 존재하지만, 실제 신청이 이루어지지 않거나 제도에 대한 인지도가 낮아 공보 대부분에서 상세한 개인정보가 그대로 노출되고 있음을 시사한다. 아래 그림은 첨단기술 및 반도체 분야의 특허공보 주소 공개 유형별 분포를 나타낸 것이다.



[그림 3] 특허공보 주소 공개 유형별 비율 비교 (첨단 기술 분야)



[그림 4] 특허공보 주소 공개 유형별 비율 비교 (반도체 분야)

이러한 실태는 개인정보 노출의 심각성을 반증하는 한편, 주소 공개 방식 변경 제도가 서류 절차에 의존하고 있으며, 실효적 보호 장치로 기능하지 못하고 있음을 보여준다. 특히 반도체 분야처럼 민감도와 산업 보안 위험이 큰 영역에서조차도 고위험 수준의 개인정보가 구조적으로 공개되고 있다는 점은 인적자원 보호 정책 측면에서 시급한 개선 과제를 제기한다. 향후에는 공보 작성 단계에서 기본값을 '비공개'로 설정하거나 발명자 식별 정보를 고유 식별번호(예:연구자 번호) 기반으로 대체하는 등의 구조적 제도 개편이 필요할 것이다.

또한 본 연구에서는 주소 항목을 중심으로 실태를 분석하였지만, 개인정보 노출 위험은 주소 단독 항목에만 국한되지 않는다. 실제 특허공보에는 발명자의 실명, 상세 주소, 기술 분야 분류 코드(IPC), 출원인 소속, 출원일 등 다양한 정보가 병렬적으로 포함되며, 이러한 정보 조합은 AI 기반 분석 환경에서 개인 식별 가능성을 획기적으로 높이는 요인으로 작용한다. 즉, 이름이 없더라도 기술 키워드, 소속기관, 출원 시기 등이 결합하면 특정 인재를 식별하거나 그 이동 가능성을 추정하는 것이 충분히 가능해지는 것이다.

이는 주소 정보를 비공개 처리하더라도 나머지 항목들이 결합하여 인적 식별로 이어질 수 있는 구조적 한계를 보여준다. 따라서 개인정보 보호는 개별 항목의 비공개 처리보다는, 정보 결합 구조 전체를 재설계하는 방식으로 접근되어야 하며, 이는 향후 특허 정보 공개 제도 개편의 핵심 과제로 고려되어야 할 것이다.

제 Ⅲ 장 사례 분석

1. 국내외 특허제도 분석

1) 비교 기준 설정

국내외 특허제도를 비교하기 위해 본 연구는 다음의 세 가지 기준을 중심으로 분석한다.

기준	내용
정보 공개 원칙	특허제도가 지향하는 기술 정보의 공개 수준과 정책적 배경
개인정보 공개 범위	이름, 주소, 소속 등 개인정보 공개 수준
개인정보 보호 조치 유무	개인정보 보호 법제나 선택적 비공개 제도의 도입 여부

[표 3] 국내외 특허제도 분석 기준

이 비교를 통해 한국 특허제도의 개인정보 노출 정도가 국제 기준과 어떤 차이를 보이는지 평가하고 개선 방향을 도출하고자 한다.

2) 국내외 특허제도 비교

① 한국의 특허제도

한국은 출원공개 공보와 등록 공보를 통해 발명자의 이름과 상세 주소(동/호수까지 포함)를 기본적으로 공개하고 있으며 이는 개인정보 노출 수준이 상대적으로 높은 편에 해당한다. 주소 공개 방식 변경 제도가 마련되어 있으나 자발적인 신청을 해야 하고, 제도에 대한 인지도가 낮아 실질적인 효과가 미흡하다. 이러한 구조적인 한계는 앞서 제2장에서 다룬 바 있으므로 본 절에서는 이를 비교 기준으로 삼아 미국, 유럽, 일본의 제도와 개인정보 보호 수준을 중심으로 비교 분석하고자 한다.

② 미국의 특허제도

미국 특허청(USPTO)은 발명자의 이름은 공개하고 주소 정보는 도시 및

주(state) 수준으로만 표기한다. 예외적으로 주소 공개를 거부할 수 있는 절차도 마련되어 있다. (예: “John A. Smith, Seattle, WA”)

또한, P.O. Box(우편 사서함) 기재를 허용해 실제 주거지나 근무지 노출을 예방하고 있으며, 개인정보 보호의 관점에서 현실적이고 효과적인 수단으로 작용한다. 실제로 미국 내 특허공보를 대상으로 한 조사에서는 전체 공개 특허의 약 60% 이상이 우편 사서함 주소나 최소화된 주소를 사용하고 있는 것으로 나타났다. 미국 특허청은 개인정보 민원이 접수되면 해당 발명자 정보의 수정, 비공개 또는 삭제 요청을 처리할 수 있는 내부 행정절차를 운영하고 있다. 이는 정보 공개와 개인 프라이버시 보호 사이 균형을 확보 및 유지하려는 제도적인 노력의 일환으로 볼 수 있다.

미국은 출원서류 전반에 대해 [1]Freedom of Information Act(FOIA) 및 [2]Privacy Act의 적용을 받기 때문에, 행정기관이 수집한 개인정보의 관리, 수정, 비공개 등에 대해 엄격한 기준을 적용하고 있다 [15].

③ 유럽의 특허제도

유럽특허청(EPO)은 유럽연합 회원국과 비회원국 일부를 포함한 39개국에 대한 특허 절차를 통합 관리하며, 개인정보 보호 측면에서 가장 엄격한 기준을 유지하고 있다. EPO의 공보에는 발명자의 이름이 공개되나, 주소는 기본적으로 생략되며, 일부 국가의 요청에 따라 도시 수준까지만 표시된다 [16].

공식 검색 시스템인 Espacenet 또한 발명자 정보를 이름으로만 검색할 수 있게 제한되어 있고 주소나 소속기관을 기반으로 발명자를 역추적하거나 데이터 수집하는 것을 기술적으로 차단한다.

유럽은 [3]GDPR(General Data Protection Regulation)의 영향을 받아, 공개

1) Freedom of Information Act(FOIA)는 미국 연방정부의 정보 공개를 보장하는 법으로, 시민이 정부 문서를 요청할 수 있도록 규정한 1966년 제정 법률이다.
2) Privacy Act는 1974년 제정된 미국 연방법으로, 연방정부가 보유한 개인정보를 보호하고 정보 주체의 권리를 보장한다.

된 정보라 하더라도 발명자가 사적 정보로 판단될 경우 수정·삭제를 요청할 수 있는 권리가 보장된다.

또한, 국가별로 별도 개인정보 보호기관이 존재하며, 특허청을 상대로 직접 민원 제기를 통해 공보 정보 정정이 가능하다.

그 결과, 유럽에서는 공개의 투명성과 개인정보 보호 사이의 균형이 제도적·기술적으로 동시에 실현되고 있으며, 특히 발명자의 인적 정보 노출은 의도적·최소화된 설계하에 관리되고 있다 [17].

④ 일본의 특허제도

일본은 발명자의 이름은 공개하되, 주소 정보는 도도부현(都道府縣) 및 시·구 단위까지만 기재하며, 건물명, 호수 등 구체적 거주 정보는 포함하지 않는다. (예: “Tokyo-to, Shibuya-ku”)

일본은 별도의 주소 비공개 제도를 운용하지 않지만 기본 특허제도 자체가 주소의 불필요한 노출을 줄이는 방향으로 설계되어 있어 발명자 보호에 일정 부분 기여하고 있다.

또한 일본 특허청(JPO)은 출원 이후 개인정보에 대한 민원이 접수될 경우, 해당 정보의 수정이나 비공개 처리에 유연하게 대응할 수 있도록 내부적 기준을 마련해 두고 있다.

기술적인 측면에서도, 일본 특허청(JPO)이 운영하는 특허 정보 검색 시스템인 J-PlatPat은 개인정보 보호를 고려한 설계 방식으로 운영되고 있다. 해당 시스템은 기본적으로 소속기관명이나 발명자의 주소를 검색 조건으로 제공하지 않는다. 인명 기반 검색의 경우에도 발명자 이름 단독으로는 검색이 제한되고 문헌 번호, 출원 번호 등 추가적인 정보를 입력해야만 결과가 제공되는 방식이다 [18].

이러한 설계는 불특정 다수가 특정 개인의 기술 활동을 추적하거나 인재

3) GDPR(General Data Protection Regulation)은 EU의 개인정보 보호 규정으로 개인 데이터의 수집·처리·이전에 엄격한 기준을 적용한다.

를 식별하는 데 시스템을 악용하지 못하도록 하는 기술적/제도적 장치로 볼 수 있다.

⑤ 중국의 특허제도

중국은 국가지식산권국(CNIPA, China National Intellectual Property Administration)을 중심으로 특허제도를 운영하고 있으며, 최근 10년간 급격한 특허 출원 증가와 함께 개인정보 보호 측면에서도 일정 수준의 개선이 이루어지고 있다. 발명자의 이름은 기본적으로 공개되며 주소 정보는 원칙적으로 도시 및 성(省) 수준까지만 기재하는 것이 일반적이다. 예를 들어 “Beijing, Haidian District” 와 같이 구체적인 건물명이나 세부 주소는 기재하지 않는 경우가 많고 이러한 방침이 행정지침 수준에서 권고되고 있다 [19].

중국의 특허공보(CNIPA Gasette)는 특허 정보 외에도 심사 경과, 기술 분류, 출원인의 기업/기관명 등을 포함하지만 발명자 주소는 최소 단위로만 표기되고 개인 식별이 가능한 정보의 노출은 기술적으로 제한하는 방향으로 설계되고 있다. 개인정보 보호와 관련된 법적 체계는 비교적 최근에 구축되었는데, 2021년 11월 시행된『개인정보보호법(PIPL, Personal Information Protection Law)』을 통해 정부 기관과 기업의 개인정보 수집/처리/제공 등에 대한 엄격한 기준이 적용되기 시작했다. 이 법은 특허 정보 시스템에 직접 적용되지는 않더라도 공공 데이터 공개 시 개인정보 최소화를 지향해야 한다는 원칙을 형성하고 있다 [20].

또한, CNIPA는 개인정보가 과도하게 노출되었다고 판단될 경우 발명자 또는 대리인의 요청에 따라 정보 삭제나 수정 요청을 수용할 수 있는 행정적 절차를 운영하고 있다. 그러나 실질적으로 활용된 사례는 많지 않고 출원인의 제도 인지 수준이 낮아서 일본과 유사하게 제도적인 설계보다는 기본 표기 형식에서의 간접적인 보호 효과에 의존하고 있는 상황이다 [21].

중국의 특허 검색 시스템(CNIPA Search, SIPO 이전 시스템 포함)은 발명자 성명과 기술 키워드 중심으로 검색되며 주소를 기반으로 한 인명 역추적은 기능상 지원되지 않는다. 이는 검색 설계 단계에서의 기술적 비식별화 조치로 평가될 수 있다. 다만 중국은 기술 강국으로 부상하면서 특허 출원 건수가 세계 최대 수준으로 증가하고 있어 공개 정보의 누적 노출량이 상당한 만큼 향후 개인정보 보호에 대한 기술적/제도적 대응이 더욱 중요해질 것으로 보인다.

조항	조항 내용 요약	특허 시스템 적용 가능성
제6조	최소 수집 원칙	도시·성 수준의 주소만 공개, 세부 주소 생략
제16조	과도 수집 금지, 삭제, 수정 요청 가능	CNIPA에 정보 수정, 삭제 요청 가능(행정절차로 수용)
제17조	처리 목적 명확화 의무	특허공보 목적 외 정보 유출 시 문제 소지가 있음, 고지 필요
제24조	자동화된 의사결정 대응 및 정보 주체 권리 보장	시스템 설계 시 역추적 차단 가능성 존재 (검색 제한 등 기술적 장치 포함)

[표 4] 중국의 개인정보보호법(PIPL) 주요 조항과 특허공보 적용 가능성

3) 비교 분석 결과 및 시사점

한국은 발명자의 개인정보가 구조적으로 광범위하게 노출되는 유일한 국가에 해당하며, 개인정보 보호가 사후 신청 기반으로만 운영되고 있어 보호 실효성이 낮다.

반면 미국은 발명자 주소를 도시 및 주소 단위로 자율적으로 최소화하거나 P.O Box를 활용해 실주소 노출을 회피할 수 있으며 주소 비공개 신청 제도와 사후 정정 절차도 마련되어 있다.

유럽은 GDPR 기반의 강력한 법적 보호 체계와 검색 시스템 차원의 기술적 차단 기능을 병행하여 개인정보의 비의도적 노출을 근본적으로 차단하고 있으며, 발명자에게는 정정/삭제 권리가 법적으로 보장된다.

일본은 제도 설계 자체가 상세 주소 기재를 피하도록 구성되어 있고 기술적으로도 주소 기반 검색이 불가능하도록 설계되어 필요시 일부 정보의 비

공개 처리를 허용하는 유연한 대응도 가능하다.

중국은 개인정보보호법(PIPL) 제정 이후 공개 정보 최소화를 지향하는 구조적 전환을 시도하고 있으나 보호 방식은 여전히 기술적 제한 설계에 머무르고 있으며 행정적 보호 절차는 상대적으로 제한적이다.

항목/국가	한국	미국	유럽	일본	중국
성명 공개	공개	공개	공개	공개	공개
상세 주소 공개	동·호수 까지 기본 공개	도시·주 까지 (P.O. Box)	대부분 생략	시·구 까지 공개	도시·성 단위 까지만 기재
비공개 제도 유무	있음 (신청 필요)	최소 공개 (수정 가능)	GDPR 기반 수정 가능	없음 (공개 정보 자체 최소화)	행정적 수정 요청 가능(제한적)
검색 시스템의 비식별화 설계 여부	인명·주소 역추적 가능	수정·삭제 절차 있음	이름 검색 가능 (주소 기반 추적 불가)	주소·기관 기반 검색 제한, 인명 조건 검색만 가능	주소 기반 검색 기능 없음
연구자 번호 활용 여부	미활용	미활용	미활용	미활용	미활용

[표 5] 국내외 특허제도 비교표

이러한 비교는 한국이 공개 정보 기반의 인재 식별 및 유출 위험을 근본적으로 줄이기 위해 단순한 정보 비공개 신청 제도를 넘어서는 제도 설계 자체의 전면적인 개편이 필요함을 시사한다. 특히 다른 국가들이 개인정보 보호를 '기본값'으로 설정하고 있지만 한국은 여전히 '공개가 기본, 보호는 신청 기반'이라는 구조를 유지하고 있어 국제 흐름과 괴리를 보이고 있다.

정보 공개와 활용의 공공적 목적은 존중되어야 하지만 발명자의 개인정보는 원칙적으로 비공개로 전환하고 기술 흐름 및 실적 추적은 고유 연구자 번호(Researcher ID)를 기반으로 비식별 정보 연계를 통해 달성하는 이중 구조가 필요하다. 이러한 전환은 기술 경쟁과 인재 보호라는 두 목표 사이에서 균형을 달성하기 위한 핵심적인 조건이며 향후 디지털 특허 정보 환경

에서 필연적인 제도 진화 방향이 될 것이다.

특허공보에서 발명자의 주소가 포함된 개인정보가 공개되는 현행 제도는 정보공개법과 특허법의 원칙을 따른 결과이지만, 동시에 개인정보 보호법과 상충하는 측면이 존재한다. 정보 공개의 원칙은 기술 정보의 공익성과 기술 발전 촉진을 목표로 하나, 개인정보 보호법 제3조 및 제16조는 정보 주체의 권리를 우선하며, 개인정보는 목적 외 사용 및 최소 수집 원칙을 강조한다. 예를 들어 공공 데이터 제공 시에도 개인정보보호위원회는 비식별 조치를 권고하고 있으며, 최근 유럽의 GDPR 및 국내 법제 개정 흐름도 개인정보의 최소 공개와 자기 결정권 강화에 초점이 맞춰지고 있다. 따라서 향후 특허 정보 공개 제도 또한 이중 보호 원칙에 따라 기술 정보는 공개하되, 발명자 인적 정보는 별도 식별 체계(예: 연구자 번호)로 대체하는 등 법제 간 균형 있는 설계가 필요하다.

2. AI 및 데이터 분석 기반 인재 식별·유출 사례

디지털 기술의 발전으로 특정 산업 분야의 핵심 인재를 데이터 기반으로 식별하는 것이 점차 현실이 되어가고 있다. 특히 특허, 논문, 학술대회 발표, 산업보고서, 기업 IR 자료 등 다양한 공개 정보를 종합하여 분석하는 기술이 정교해지면서 특허공보에 포함된 발명자 정보는 기술 공시를 넘어 인재 분석의 실질적인 출발점으로 작용하고 있다.

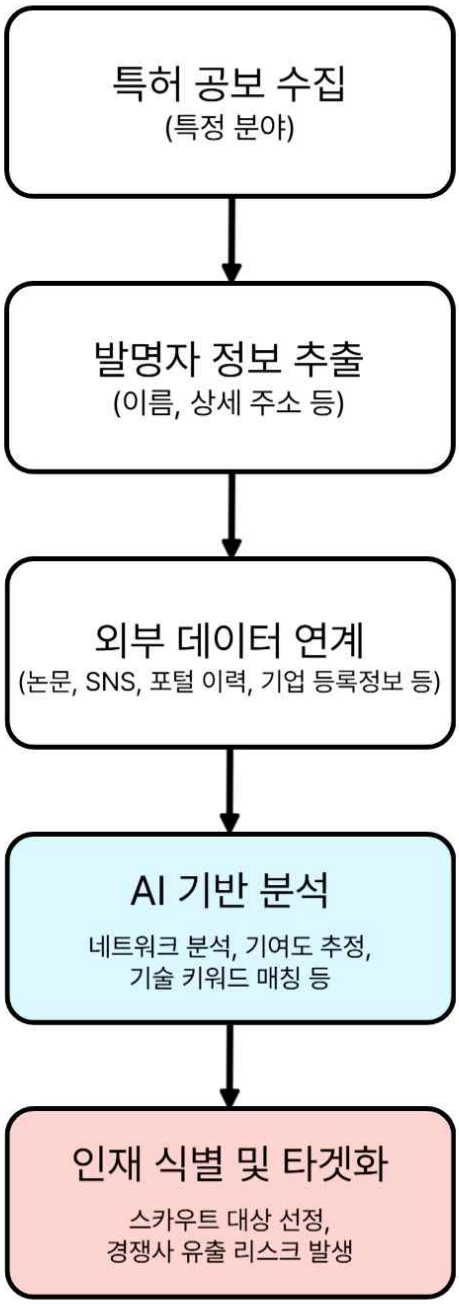
기존에는 특허공보에 공개된 이름과 주소, 소속기관 등의 정보가 수동적으로 해석되어 왔지만 최근에는 인공지능(AI) 기반 [4]자연어 처리(Natural Language Processing, NLP), [5]엔터티 연결 기술(entity linking), [6]지식 그래프 등 기술이 도입되면서 발명자의 전문 분야, 기술 기여도, 소속 이력,

4) 자연어 처리(NLP)는 컴퓨터가 인간 언어를 이해하고 처리할 수 있도록 하는 인공지능 기술이다.
5) 엔터티 연결 기술은 텍스트 내 개체를 외부 지식베이스의 고유 항목과 연결하는 자연어 처리 기술이다.
6) 지식 그래프는 개체와 개체 간 관계를 그래프 형태로 구조화한 지식 데이터베이스이다.

공동연구 네트워크 등이 데이터로 재구성되고 있다. 이와 같은 분석은 기업 간 기술 경쟁이나 국가 차원의 전략 수립 과정에서도 활용되고 있고 이로 인해 산업 보안 측면에서 인적자원이 외부에 노출되는 문제의 심각성이 부각되고 있다. 예를 들어, 해외의 글로벌 기업들은 인공지능(AI) 기반의 특허 분석 도구(PatSnap, Lens.org, Derwent Innovation 등)를 활용해서 경쟁사 주요 기술 흐름을 분석하고 동시에 기술의 핵심 기여자를 파악해 인재 영입 전략을 세운다. 이 과정에서 특허공보의 발명자 정보는 초기 식별의 단서로 활용되고 이후 링크드인(LinkedIn), 연구자 프로파일 시스템(ResearchGate, Google Scholar 등)과 결합되어 해당 인물의 상세 이력 정보, 소속의 변화, 기술 활동 내역 등을 상세히 파악할 수 있다.

문제는 이러한 분석이 비교적 저비용으로 자동화된 형태로 가능해졌다는 점이다. 과거에는 수작업으로 수개월 걸리던 작업이 이제는 클릭 한 번으로 수행될 수 있고 핵심 기술 인재의 노출과 유출을 새로운 방식으로 촉진 시키는 기제로 작동한다. AI 기반 분석이 단순한 기술 모니터링 수준을 넘어서 실제 인재 스카우트 및 기술 유출과 연결된 사례도 점차 보고되고 있다. 특히 고급 기술 인력을 겨냥한 경쟁사의 정밀 스카우트, 또는 국가 간 산업 기술 유출과 결합된 형태가 대표적이다.

국내 AI 연구기관의 경우 핵심 반도체 공정 기술의 발명을 주도한 연구원의 이름과 주소가 특허공보를 통해 외부에 공개되었고 해당 연구원이 해외 업체의 고액 연봉 제안을 받고 이직한 사건이 있었다 [22]. 이 과정에서 외국 기업은 특허 분석 도구와 온라인 이력 기반 정보를 결합해 해당 인재의 전문 기술 범위, 참여 프로젝트, 논문 수 등을 분석한 것으로 알려졌다. 이처럼 특허 정보와 외부 플랫폼이 결합하면 개별 인재에 대한 거의 완전한 프로파일링이 가능해진다.



[그림 5] AI 기반 인재 식별·유출 흐름

단계	목적	수단	위험 요소
① 특허공보 수집	정보 수집	키워드 검색, 자동 크롤링	기술 인재 노출
② 발명자 정보 추출	인물 식별	이름, 상세 주소, 소속 파악	실명·실주소 연결
③ 외부 데이터 결합	외부 정보 통합	논문, SNS, 포털 연계	프로필 구축 가능
④ AI 분석	역량 평가	키워드 분석, 영향도 계산	자동 타겟 지정
⑤ 타겟화	인재 확보	스카우트, 이직 유도	인재·기술 유출 위험

[표 6] AI 기반 인재 식별·유출 구조도 단계별 위험 요소

또한 국내 보안 기관이 발표한 산업기술 유출 사례 보고서에 따르면 일부 해외 기업은 특허 정보를 기반으로 국내 핵심 인력의 주소지를 파악하고 비공식 채널을 통해 이직 제안을 하는 등 전통적인 기술 유출 방식에서 벗어난 '인재 포섭형 유출'의 경향을 보여주고 있다. 특히 소재·부품·장비 및 바이오헬스 분야와 같이 특정 기술에 고도로 집중된 전문 인력이 있는 분야일수록 이러한 유출 경향은 더 두드러진다. 발명자 1명이 사실상 전체 기술 방향을 주도하거나 다수 특허의 중심에 위치하는 경우가 많으므로 해당 인재의 유출은 단순한 인력 손실을 넘어 기업 전체의 기술 자산이 외부로 이전되는 구조적 리스크로 이어진다.

한편, 국가 차원에서도 이러한 정보 기반 인재 식별의 위협을 인지하고 있다. 미국은 국가 안보 전략(National Security Strategy)에서 "민간 특허와 공개 기술 정보를 이용한 외국 정부의 인재 리크루팅 활동"을 주요 위협으로 지목한 바 있으며 일본과 독일 역시 특정 발명자 및 연구자의 활동 정보가 해외로 과도하게 노출되는 것을 막기 위해 정보 최소 공개 원칙을 강조하고 있다 [23].

현재 이러한 데이터 분석 기반 위협에 대해 국내외 제도는 여전히 충분한 대응 체계를 갖추지 못하고 있다. 한국의 경우, 공개 특허 정보에 대한 이용 제한이나 인적 정보 비식별화 조치는 매우 제한적이며, 정보 공개와 인재 보호 간의 균형을 위한 가이드라인이나 기술적 보완 장치가 거의 부재한 상태다.

주소 게재 방식 변경 제도가 존재하긴 하나 신청 기반이고, 제도 인지도도 낮으며, 이미 공개된 공보에 대한 사후 대응도 기술적으로 완전하지 않다. 더욱이, 한 번 공개된 특허공보는 특허 정보넷 키프리스(KIPRIS), 구글 특허, 해외 특허 포털 등 여러 경로로 확산되기 때문에, 공개 이후에는 정보의 회수가 실질적으로 불가능하다.

또한 데이터 분석 기업 및 플랫폼은 법적 책임 범위를 벗어나 있으며, 발명자에 대한 검색, 프로파일링, 스코어링 등의 결과를 제공하더라도 직접적으로 개인정보보호법의 적용을 받지 않는 경우가 많다. 기술적 도구가 법적 보호 체계를 우회해서 민감 정보를 분석할 수 있게 만드는 구조적인 공백을 의미한다.

이러한 위협은 향후 더 지능화될 가능성이 크다. 딥러닝 기반의 연구자 임팩트 예측 모델, 고유 식별자(ORCID, RID, Scopus Author ID 등) 기반의 경력 추적 시스템, 자동 이직 가능성 예측 알고리즘 등은 이미 상용화 초기 단계에 접어들고 있다. 이러한 기술들은 특허 발명자 정보를 디지털 신원으로 연결하는 중요한 매개체로 작용할 가능성이 크다.

제 Ⅳ 장 제안 대응 전략

1. 연구자 번호 기반 정보보호 방안

특허공보에는 발명자의 이름, 주소, 소속기관과 같은 인적 정보와 함께 기술 요약, 청구항 등 고도의 기술 정보가 통합되어 있다. 이러한 정보의 구성은 정보 공개의 취지에 부합하지만 인적 정보가 불필요하게 노출되어 개인정보 침해로 이어질 수 있다. 실제로 외국 특허청(EPO, USPTO 등)에서는 인적 정보의 표기를 제한하거나 기술 정보와의 연계를 최소화하여 제공하는 방식이 보편화되고 있다. 따라서 기술 정보에 대해서는 공개 원칙을 따르고 인적 정보는 고유 연구자 번호를 사용하거나 동의 절차를 통해 제한적으로 제공하는 방식의 이중 정보 관리 체계가 필요하다. 이러한 분리 구조는 기술 공개의 투명성과 인재 보호라는 상충 과제를 모두 해결할 수 있는 현실적인 대안이 될 수 있다.

기술 정보의 공개는 산업의 핵심적인 성장 동력이지만 여기에 포함된 인적 정보가 인공지능(AI) 기반 분석 등을 통해 인재 식별 및 기술 유출 가능성을 높이는 요인으로 작용할 수 있다. 따라서 기술 정보 공개의 취지를 유지하면서 인재 보호를 실질적으로 구현할 수 있는 제도적 보완이 절실한 상황이다.

이러한 문제를 해결하기 위한 실질적인 대안 중 하나로, 본 장에서는 연구자 식별번호(연구자 번호)를 활용하여 개인정보를 비식별화 한 특허 정보 표기 방식을 제안한다. 기존 발명자 이름과 주소를 공개하는 대신, 국가 단위 또는 기관 단위에서 관리되는 고유 연구자 식별번호를 이용하여 특허공보 상 인적 정보를 간접적으로 기재하도록 한다. 정보의 결합과 기술 흐름 분석적 특성은 유지하면서 개인정보 노출과 인재 식별 위험을 축소할 수 있

다. 이는 발명자의 개인정보 보호, 기술 유출 방지, 연구자 실적 관리 등 다양한 영역에 접목하는 통합적인 대응 전략이 될 수 있다.

최근 인공지능(AI) 및 데이터 분석 기술 발달로 공개 정보에 포함된 인적 정보를 단서로 특정 기술 인력을 식별하고, 나아가 핵심 인재 유출로 이어질 가능성을 현실화시키고 있다 [24]. 이에 따라 기술 정보의 공공성과 산업 보안 사이에서 균형 있는 대응이 요구되며, 개인정보를 직접적으로 노출하지 않으면서도 기술 흐름과 연구자의 기여도를 체계적으로 관리할 수 있는 대안으로 연구자 번호 기반의 정보 관리 체계가 주목받고 있다.

연구자번호란 개인 연구자에게 발급된 고유 식별번호로, 논문 발표, 특허 출원, 연구 실적 등 다양한 연구 활동을 통합적으로 연계하여 관리할 수 있도록 설계된 식별 체계이다. 대표적으로는 국내의 국가 연구자 번호(NRI; National Researcher Identifier)가 있고, 국제적으로는 ORCID(Open Researcher and Contributor ID), Scopus Author ID, ResearcherID(Web of Science) 등이 있다. 연구자 번호는 개인의 실명을 공개하지 않더라도 해당 연구자의 활동 내역을 일관성 있게 관리할 수 있다는 장점이 있다.

현재 특허공보에서는 발명자의 실명, 주소, 소속 등이 명시되어 있어 인재 식별 및 위치 추적이 용이하다는 점이 문제로 지적된다. 반면 연구자 번호를 특허공보 상에 기재하는 방식으로 전환할 경우, 실명이나 주소 등 개인정보의 노출을 줄이면서도 기술적 연계성과 추적 가능성은 유지할 수 있는 비식별 정보 제공이 가능하다. 즉, 발명자의 주소와 이름 대신 연구자 번호를 기재하고, 이 연구자 번호에 연결된 실적은 특허청이나 과학기술정보기관에서 별도로 관리함으로써 정보보호와 실적 관리의 균형을 꾀할 수 있다.

이러한 방안은 다음과 같은 장점을 갖는다.

첫째, 정보 공개의 공공성 유지 측면에서, 발명의 흐름과 기술의 진화는 지속적으로 추적할 수 있으며, 연구자의 활동을 실명 없이도 연결해 볼 수

있다.

둘째, 개인정보 보호 수준 향상이라는 측면에서, 연구자 개인의 실제 주소, 소속기관, 실명 등의 정보는 공개 정보에서 제외되므로 AI 기반 인재 식별 위험을 현저히 줄일 수 있다.

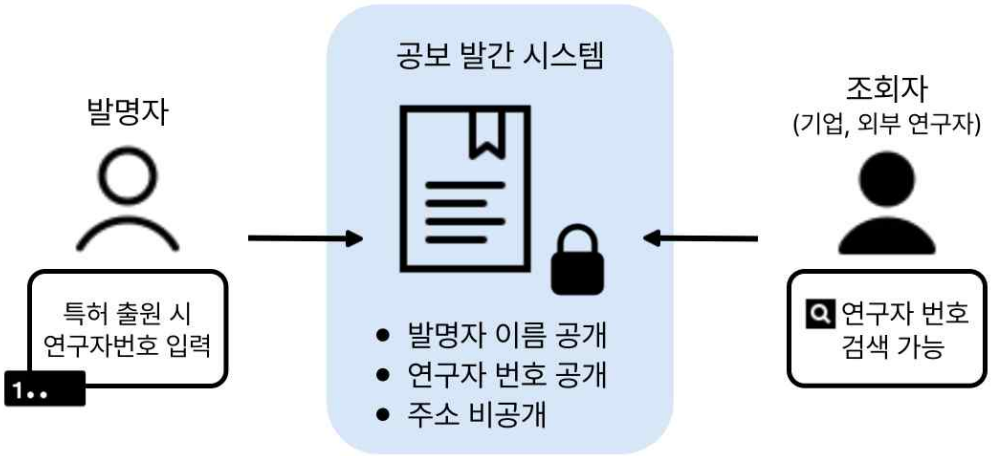
셋째, 정책 활용성 향상 측면에서, 연구자 번호를 기반으로 한 특허와 연구 실적 집계, R&D 성과 평가, 정부 지원 사업을 통합하여 효과적으로 관리할 수 있다.

해외에서도 비슷한 추세가 나타나고 있다. 유럽의 경우, GDPR(General Data Protection Regulation)을 바탕으로 특허 정보에 실명이 포함되더라도 공개된 이후 이의 제기가 가능하고, 향후 발명자 익명화와 대체 식별자 활용 방안에 대한 논의를 이어가고 있다. 미국의 경우, 일부 정부 기관은 발명자의 주소를 공보에 공개하지 않고 기관 내 연구자 식별번호나 팀 식별번호를 기반으로 성과를 관리하는 형태로 변화하고 있다. 이러한 흐름은 특허 시스템의 전반적인 개인정보 보호 중심 패러다임 전환을 상징적으로 보여준다.

우리나라 역시 현재의 '주소 공개 방식 변경 제도'만으로는 공개 정보 기반 인재 유출을 예방하기에 어려움이 있기에 이를 보완하는 일차적인 대응책으로서 연구자 번호 기반의 비식별 표기 방식의 도입과 적용이 긍정적으로 검토되어야 한다. 특히 이미 국가 연구자 번호(NRI)를 활용해 국가과학기술지식정보서비스(NTIS) 등에서 연구자의 이력과 실적을 통합적으로 관리하고 있다는 점에서 제도의 확대 및 적용은 기술적, 행정적 측면 모두에서 실현 가능성이 높다.

도입 초기에는 실명과 병행 표기하거나, 민감 정보를 원칙적으로 제외한 제한적 정보와 연구자 번호를 병기하는 방식도 고려해 볼 수 있다. 나아가, 해당 연구자 번호와 연동된 실적은 연구기관이나 정부 기관에서 관리·공개

하며, 외부에서 기술적 식별이 불가능하도록 시스템을 설계하는 방식이 바람직하다. 이는 실적의 신뢰성과 활용도는 유지하면서도, 정보 주체의 동의 없이 개인정보가 제3자에 의해 악용되는 것을 원천적으로 차단할 수 있는 구조이다.



[그림 6] 연구자 번호 기반 특허공보 개인정보 보호 구조

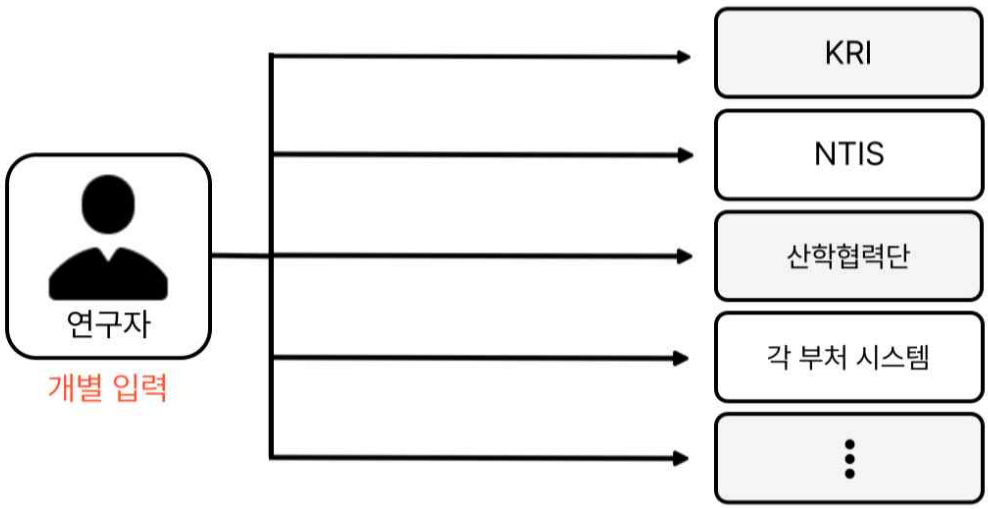
결론적으로, 연구자 번호를 활용한 특허 정보 관리 체계는 개인정보 보호와 기술 정보의 유통이라는 특허제도의 이중 목표를 조화롭게 달성할 수 있는 실질적인 대안이다. 향후 이를 위한 법제 정비와 정보시스템 개선이 병행된다면, 첨단산업 분야에서 핵심 인재의 정보 노출을 최소화하고, 기술 경쟁력의 보호를 위해 더 강력한 정책적 기반을 마련할 수 있을 것이다.

2. 연구자 번호 활용 확장

앞에서는 연구자 번호를 활용한 비식별 특허 정보 표기 방식이 개인정보 보호와 기술 정보 연계라는 두 목적 사이의 절충안을 마련할 수 있는 구조적 대응 전략으로 제시되었다. 그러나 연구자 번호의 활용 범위는 특허공보의 개인정보 대체 표기 수단에 그치지 않는다. 식별자 기반의 통일성 있는 정보 연계 구조는 연구자 개인의 성과관리부터 기업의 인재 평가 및 검증,

정부의 정책 평가까지 폭넓게 확장할 수 있고 연구생태계 전반의 정보 흐름을 유기적으로 연결할 수 있는 핵심 인프라로 작용할 수 있다.

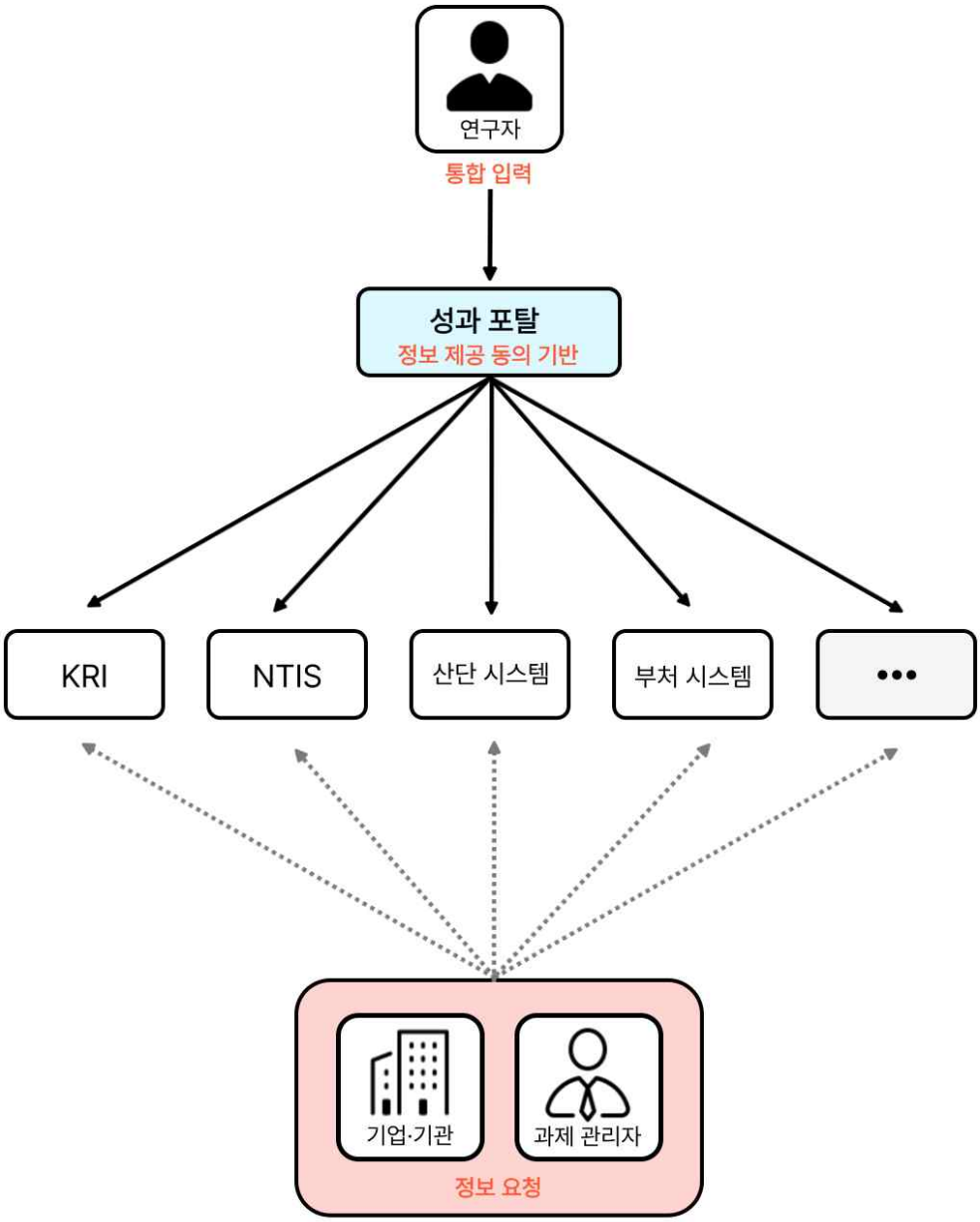
현재 국내에서는 한국연구재단(KRI)에서 발급하는 연구자 번호를 중심으로 다양한 연구 관리 시스템이 운영되고 있다. 대표적으로 국가과학기술지식정보서비스(NTIS), 한국과학기술정보연구원(KISTI), 대학 산학협력단, 정부 부처별 과제 관리 시스템 등이 존재하지만, 시스템 간 정보 연동은 미흡한 수준에 머물고 있다. 그 결과, 연구자 입장에서는 동일 정보를 여러 플랫폼에 반복적으로 입력해야 하고 시스템 간 실적 내용 불일치나 이력 누락, 자동 수집의 오류 등 문제들이 다양하게 발생하고 있다. 특히 동일 연구자가 다수의 플랫폼에 서로 다른 식별자로 등록된 경우 심사위원 선정, 과제 평가, 성과 집계의 과정에서 정보 신뢰성과 정확성이 대폭 저하된다. 이러한 분산적 구조는 연구자 번호의 본래 목적이었던 통합 식별과 효율적 관리의 기능을 약화시키고 제도적인 보완이 요구되는 지점이다.



[그림 7] 기존 연구자 성과 입력 방식

한계를 극복하기 위해서 연구자 번호를 중심으로 성과 및 실적과 이력 등이 자동으로 연계되도록 하는 “성과 통합 포탈 시스템(가제)”이 구축될 필

요가 있다. 연구자는 이 포탈을 통해 자신의 논문, 특허, 기술이전, 학술 활동, 과제 참여 이력 등과 같은 성과나 실적들을 연도별 그리고 유형별로 일괄 등록하여 관리할 수 있다. 등록된 정보는 연구자 번호를 키값으로 하여 통합적으로 축적된다. 이 포탈은 기존의 NTIS, IRIS 등과 같은 성과관리 시스템의 장점을 융합하고 연구자 주도 입력과 정부 주도 인증 체계가 병행되는 하이브리드 구조로 운영될 수 있다. 정부는 이 포탈 운영에 대한 표준화된 등록 지침 및 공개 범위 설정 기준을 마련해 정보의 신뢰성과 통일성을 높이고, 연구자의 자율성과 개인정보 통제권을 함께 보장해야 한다.



[그림 8] 제안 성과 포탈 활용 체계

이 체계를 통해 연구자 개인은 다양한 현실적인 장점을 얻을 수 있다. 반복적으로 작성해야 하는 보고서나 제안서에 필요한 기초 데이터를 자동으로 추출할 수 있고 개인 성과 현황을 연도별·주제별·유형별로 정리하여 포트폴리오를 편리하게 구성 및 제작할 수 있다. 이는 연구 경력의 연속성이 중요한 프리랜서 연구자, 기술이전 전문가, 창업가, 스타트업 CTO 등에게 특히 유용할 것이고, 중단 없는 커리어 관리가 가능해질 것이다. 또한 시스템 내에서 연구자의 기술 기여도와 활동 이력을 시각화할 수 있고, 논문 게재 수, 인용 횟수, 특허 등록 수, 수상 이력 등의 데이터를 분석해 향후 경력 설계에도 활용할 수 있다.

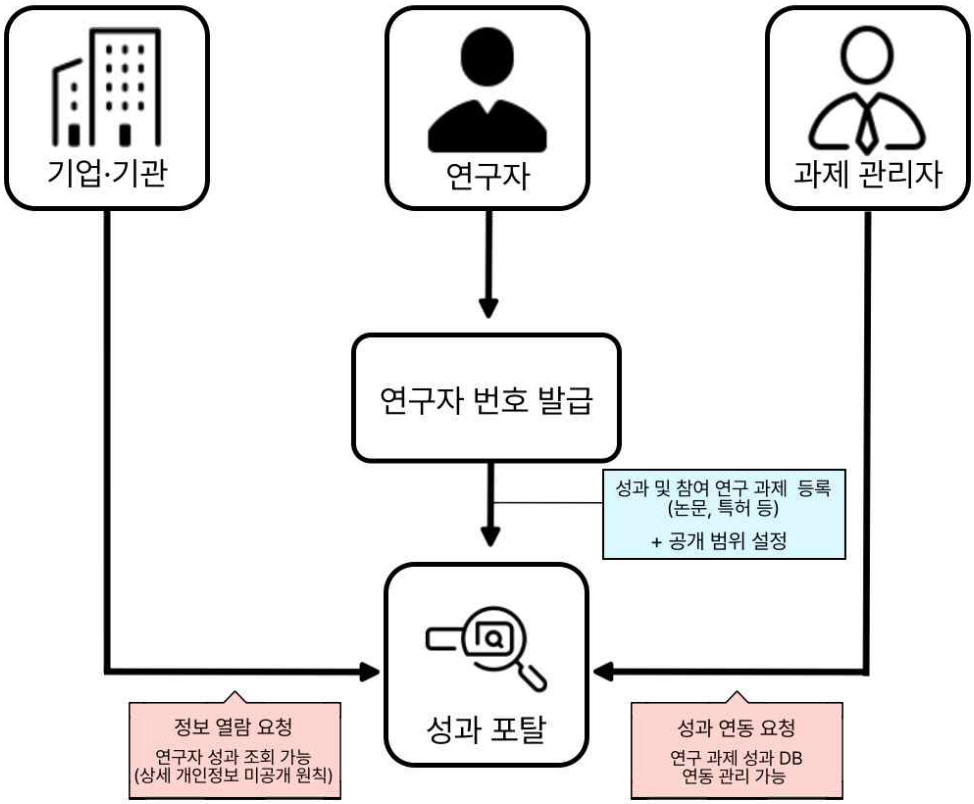
기업도 연구자 번호 기반의 성과 시스템은 인재 채용, 기술 검토, 공동연구 협업 등의 과정에서 높은 활용 가치를 가진다. 기업은 채용 절차의 지원서 접수 단계에서 지원자에게 연구자 번호를 제출받고, 지원자의 사전 동의에 따라 성과 포탈에서 해당 지원자의 연구 이력과 성과들을 직접 열람할 수 있다. 이를 통해 불필요한 서류 제출 과정은 줄이고 실적 검증의 신뢰도는 높일 수 있다. 과거 수행한 연구 주제나 특허 등록 내용, 논문 게재 실적 등은 해당 기업의 R&D 방향성과 연계하여 더 정밀한 평가 기준으로 작용될 수 있다. 특히 연구자(혹은 지원자)는 정보를 제공할 때 기업별로 공개 범위와 항목을 선택적으로 설정할 수 있도록 권한을 가질 수 있다. 예를 들어 학위, 논문, 특허 정보는 공개하고, 소속기관명이나 과거 수행 과제명은 비공개로 설정하는 방식으로 프라이버시 보호와 정보 제공의 균형을 보장할 수 있다.

또한 연구자 번호는 연구책임자, 산학협력단 실무자, 정부 부처의 사업 담당자 등과 같은 과제 관리 주체에게도 행정적 효율성을 높일 수 있는 유용한 도구로 활용될 수 있다. 현재는 과제별 참여자 정보를 수기로 정리하거나, 개별 연구자에게 실적 제출을 요청하는 방식으로 관리되고 있다. 연구자

번호와 연동된 성과 포탈 시스템을 활용한다면 과제명 또는 참여자의 연구자 번호만으로 자동 집계와 실적 추적이 가능하다. 이에 따라 연구개발 계획서 및 연구 보고서와 같은 서류의 작성이 간소화되고, 실적의 타당성과 투명성 확보가 가능해진다. 더불어 과제 참여 인원의 중복 등록, 허위 기재, 정보 누락 등을 방지할 수 있고 장기적으로는 연구자 간 협업 이력, 기술 접점, 공동연구 빈도 등의 데이터가 축적되어 정책적 분석 자료로도 활용될 수 있다. 예를 들어, 특정 기술 분야에서 연구자 간 연결 구조를 분석함으로써 연구 인프라의 밀도나 기술 축적 수준을 간접적으로 파악하거나, 중복 투자 방지를 위한 참고 자료로도 기능할 수 있다.

이와 같은 체계는 궁극적으로 개인정보 보호, 실적의 정합성 확보, 연구 행정의 효율성 제고라는 세 가지 축을 동시에 달성할 수 있는 구조로 자리 잡을 수 있다. 연구자 번호는 단순한 식별 수단을 넘어, 연구생태계 전반에서 정보의 신뢰도와 연결성을 높이고, 핵심 인재를 보호하며, 실증 기반의 정책 수립을 가능하게 하는 전략적 인프라로 기능할 수 있다.

아래 그림은 이러한 연구자 번호를 기반으로 한 성과 관리 체계의 전체 흐름과 각 이해관계자의 활용 방안을 시각적으로 정리한 것이다.



[그림 9] 연구자 번호 활용 성과 관리 체계

결론적으로 연구자 번호 기반 성과 관리 체계는 특허 정보에 대한 접근 제한이라는 단편적 조치를 넘어서, 연구자 주도의 정보 통제, 기업의 정보 수신 합리화, 행정기관의 사업성과 관리 간소화라는 세 주체의 이해관계를 동시 만족시킬 수 있는 고도화된 대응 전략이다. 향후에는 이를 기반으로 특허공보에 실명을 노출하지 않고도 연구자의 기여도를 식별하고, 평가할 수 있는 새로운 기술 기반 시스템(예: 인증 기반 디지털 프로필)으로 확장할 수 있다. 이를 위해서는 정보통신 인프라의 개선, 법제 정비, 기관 간 연동 체계 구축 등이 동반되어야 하며, 무엇보다도 연구자의 정보 자기 결정권과 인재 보호라는 철학적 기반 위에서 시스템이 설계되어야 한다.

이러한 구조를 기술적으로 보다 안전하고 확장성 있게 구현하기 위해 블록체인 기반의 분산 신원인증(DID: Decentralized Identifier) 기술을 적용할 수 있다. DID는 중앙 기관에 의존하지 않고 블록체인에 고유 식별자를 생성하여 해당 ID를 통해 개인의 신원을 증명하는 탈중앙화된 방식이다. 이를 연구자 번호에 적용하면 개인정보를 직접 저장하거나 유출 위험 없이 각 시스템 안에 연구자의 성과 정보를 신뢰성 있게 연계하고 검증할 수 있는 기반을 마련할 수 있다. 즉, 연구자 번호는 단순한 식별자에서 나아가 검증 가능한 전자 신원(Verifiable Credential, VC)을 포함한 디지털 신원 인프라의 핵심 구성요소로 확장될 수 있다 [25].

예를 들어 DID 기반의 연구자 번호를 가진 사용자는 NTIS, KISTI, NRI 등 각 기관의 시스템과 연동하여 본인이 동의한 범위 내에서 성과 정보를 공유할 수 있다. 기관은 연구자의 DID를 통해 블록체인에 등록된 VC를 검증함으로써 실적의 진위 여부를 별도의 행정절차 없이 확인할 수 있고, 연구자는 공개 범위를 사전에 세분화하여 정보 제공을 통제할 수 있다 [26].

VC는 발급 기관의 전자서명을 포함하고 있어서 위변조 불가능하며 연구자의 통제 하에 안전하게 관리될 수 있다. 이와 같은 DID 및 VC 기반의 체계는 개인정보를 포함하지 않는 비식별화 구조를 실현할 뿐 아니라 연구자의 신원 확인과 성과 검증을 보다 안전하고 효율적으로 수행할 수 있도록 한다.

구분	활용 방식	기대 효과
연구자	- 연구자 번호 연동 성과 포털에 논문, 특허, 기술이전, 참여 과제 등록 - 등록 정보 자동 포트폴리오 생성 - 연구 및 성과 유형별 정리 및 시각화	- 반복적 문서 작업의 효율화 (이력서, 제안서 등) - 기술 기여도, 성과 추세 파악 - 프리랜서, 전직 시에도 경력 연속성 확보
기업·기관	- 지원자가 제공한 연구자 번호로 성과 포털 열람(사전 동의 기반) - 열람 범위는 연구자가 선택 가능	- 이력 검증의 신뢰도 확보 - 포트폴리오 별도 요청 불필요 - 개인정보 통제권 유지 및 정보 전달의 효율화
과제 관리자	- 참여 연구자의 번호 기반 자동 성과 집계 가능 - 과제별 실적, 공동연구 이력 추적 가능 - 데이터 기반 정책 분석 활용	- 보고서, 실적 관리 자동화 - 오류, 중복, 누락의 최소화 - 협업 구조 및 중복 투자 분석 가능

[표 7] 이해관계자별 연구자 번호 기반 성과 정보 활용 방안 기대 효과

제 Ⅴ 장 결론

1. 결론

본 논문은 첨단산업 기술 경쟁의 심화와 함께, 특허 정보의 공개를 통한 핵심 인재 식별 및 유출 가능성이 새로운 보안 위협으로 부각되고 있는 현실을 문제의식으로 삼아 연구를 진행하였다. 특히, 특허공보에 포함된 발명자의 이름, 주소 등 인적 정보가 AI 기반 분석 기술에 의해 재구성되고, 이를 통해 특정 기술 분야의 핵심 기술을 보유한 인재가 외부에 의해 식별되고 인재 유출 대상이 될 수 있는 위험성을 분석하였다.

연구의 첫 번째 축은 특허 정보 공개 제도의 구조와 한계를 분석한 것이다. 국내 제도는 기본적으로 발명자의 상세 주소를 포함한 실명 정보를 공개하고 있어 개인정보가 외부로 노출될 가능성이 높다는 점을 지적하였다. 특히 미국, 유럽, 일본 등 주요 국가의 제도와 비교했을 때 한국은 정보 공개 범위가 상대적으로 넓고 개인정보 보호를 위한 제도적 장치의 실효성도 낮은 것으로 확인되었다.

두 번째 축은 인공지능(AI) 및 데이터 분석 기술이 공개 특허 정보를 비롯한 다양한 오픈 데이터를 통합하여 인재 식별에 활용되는 사례들을 분석한 것이다. 특허·논문·소셜미디어·학회 활동 이력 등 다양한 정보를 연계해 핵심기술 인재 프로파일링이 가능해지고 있고 실제로 경쟁사나 해외 기업이 이를 활용해 우수 인재를 스카우트하거나 기술 유출의 간접적인 수단으로 활용하는 사례도 점차 증가하고 있음을 확인할 수 있었다.

세 번째 축은 이러한 문제에 대응하기 위한 전략으로 연구자 번호를 활용한 비식별 정보 관리 체계와 성과관리 인프라의 확장 방안을 제안한 것이다. 이는 개인정보 공개 없이도 기술의 흐름과 연구자 실적을 파악할 수 있

도록 하고 동시에 기업, 과제 관리자, 연구자 사이의 정보 흐름을 통제할 수 있도록 설계해 인재 유출 위험을 줄이고 정보 활용의 효율성을 높일 수 있도록 한다.

기존의 기술 유출에 대한 논의가 내부자 위협이나 시스템 보안 측면에만 집중되었던 것과 달리 공개된 특허 정보가 새로운 유출 경로로 작동할 수 있다는 문제점을 인적자원 보안의 관점에서 분석했다는 점에서 학문적·정책적 의의가 있다. 또한, 개인정보 보호와 기술의 정보 공개라는 상충하는 정책적인 목표 사이의 균형을 도모하기 위해 실효성 있는 조정 메커니즘으로서 연구자 번호 기반 관리 체계를 제안하고 관리 체계의 확장 가능성을 다각도로 검토하였다는 점에서 구체적인 시사점을 제공한다. 특히 기존 제도와 기술 인프라를 활용한 현실적인 대안 제시는 향후 관련 정책 설계 과정에서 유의미한 참고 자료가 될 수 있을 것이다.

다만 본 연구는 다음과 같은 한계를 가진다. 첫째, 실제 인재 유출 사건에 대한 심층적 인터뷰나 정량적 통계 확보가 충분하지 않았다. 사례 중심의 분석은 가능했으나 데이터를 기반으로 인과관계를 명확하게 검증하는 것에는 한계가 있었다. 향후에는 유출 경로로서 특허 정보의 활용 빈도, 연구자 식별 기법의 정확도, 이직 사례와의 연관성 등을 정량적으로 분석할 필요가 있다.

둘째, 연구자 번호 기반 대응 전략이 실제 구현 가능한지에 대한 실증적 검토가 충분히 이루어지지 않았다. 시스템 통합, 개인정보 법제와의 정합성, 기관 간 연계 가능성 등은 실제 운영기관과의 협업을 통해 프로토타입 수준의 검증이 필요할 것이다.

셋째, 본 연구는 연구자 번호를 중심으로 한 하나의 해결책에 집중하였지만, 향후에는 블록체인 기반 성과 인증 시스템, 프라이버시 보호 설계(PbD), 연구자 정보 익명화 알고리즘 등 다양한 기술적 접근 방식과의 비교 연구도

병행할 필요가 있다.

본 연구에서 확인된 문제점을 바탕으로 향후 국내 제도의 개선을 위한 정책적 방향을 다음과 같이 제안할 수 있다. 우선, 발명자의 주소나 실명을 특허공보에 직접 기재하는 방식은 개인정보 침해와 인재 유출이라는 이중의 위험을 유발할 수 있으므로, 이러한 정보를 직접 노출하기보다는 연구자 번호와 같은 고유 식별자를 활용하는 방식으로 점차적인 전환이 필요하다.

또한, 연구자 번호를 기반으로 성과를 등록하고 관리할 수 있는 성과 포탈 시스템을 구축하고, 이 시스템을 통해 연구자 개인, 기업, 행정기관이 서로 다른 방식으로 정보를 활용할 수 있도록 유연하게 설계되어야 한다. 이를 위해 연구자는 자신의 성과 정보를 등록할 때 공개 범위와 항목을 설정할 수 있어야 하고 기업은 해당 정보를 사전에 동의받아 열람하는 방식으로 인재 채용이나 기술 검토에 활용할 수 있어야 한다. 과제 관리자는 이를 통해 참여 연구자의 실적을 통합적으로 집계하고 관리할 수 있어야 하며, 전체 국가 R&D 데이터의 신뢰성과 활용 가능성을 높이는 데 기여해야 한다.

이러한 제도가 안정적으로 운영되기 위해서 개인정보 보호법, 특허법, 국가 연구개발 관련 법령 간의 조화를 이룰 수 있도록 해야 하고, 고유 식별자 연계 방식이 법적으로도 명확히 허용되는 기반이 필요하다.

본 논문은 특허 정보 공개 제도의 구조적인 한계를 짚어보고 연구자 번호를 중심으로 한 관리 체계를 제안함으로써 기술 정보의 공공성과 인재 보호라는 두 가지 필요성이 충돌하지 않도록 하는 제도적 조정 가능성을 제시하였다.

연구자 번호 기반의 정보 비식별화 전략이 개인정보 보호와 기술 정보 연계라는 상충 과제를 균형 있게 해결할 수 있는 구조적 대응 모델임을 제시하였다. 특히 연구자 번호를 단순한 식별 대체 수단이 아닌, 성과관리와 정책 연계 기반으로까지 확장함으로써, 연구자 보호와 정보 활용이라는 두 축

의 통합 가능성을 검토하였다.

향후에는 다양한 기술과 법제, 산업계의 요구를 통합한 융합적 관점에서 이 문제를 지속적으로 논의하고 보완해 나가고, 이 제도의 실현 가능성과 정책 수용성에 대한 실증 연구가 필요하다. 예를 들어, 특허청 공보 시스템 내 연구자 번호 기입 항목을 시범 도입하고, 연구자 및 기업을 대상으로 정보 공개 방식에 대한 수용성과 우려 요인을 조사하는 방식의 파일럿 프로젝트가 효과적일 수 있다. 또한 정보 비공개 제도와 연구자 번호 연계 체계 간 통합 방안을 설계하면서, 기존 국가 인프라(예: NTIS, KRI, IRIS 등)와의 기술적 연계성, 데이터 통합 구조, 인증 절차 간소화 여부 등을 실무적으로 검토할 필요가 있다.

이와 같은 접근은 정책 설계 차원에서 제도 도입 가능성과 기대 효과를 정량화할 수 있으며, 나아가 산업별 민감도 차이, 연구자 직무 유형별 활용도, 제도 수용에 따른 보안 효과 등 후속 연구의 토대를 마련할 수 있다. 장기적으로는 연구자 간 협업 네트워크, 기술 기여 추적, 중복 과제 방지와 같은 정책적 활용까지 고려한 데이터 기반 연구 생태계 구축 전략으로 확장될 수 있을 것이다.

결국, 본 논문에서 다룬 모든 논의는 하나의 중심축으로 귀결된다. 바로, 특허 제도를 통한 권리 보호의 명확성과 기술·개인의 정보보호라는 사회적 가치 간의 균형이다. 기술 정보의 공개는 제도의 신뢰성과 권리 귀속의 정당성을 보장하기 위한 수단이지만, 그것이 불필요한 인적 정보 노출로 이어지는 순간, 보호의 수단이 오히려 위협의 통로로 전락할 수 있다.

따라서, 제도적 정비는 어느 한 편의 극단적 우위가 아니라, 정보 공개의 목적과 수단이 서로를 침해하지 않도록 조율하는 방향으로 나아가야 한다. 이는 단순한 개인정보 보호 차원을 넘어, 지식재산권 제도의 지속가능성과 기술 생태계의 신뢰를 확보하기 위한 필수 조건이다.

참고 문헌

[1] Ding, Jeffrey, and Allan Dafoe. *"The Logic of Strategic Assets: From Oil to Artificial Intelligence."* arXiv preprint arXiv:2001.03246. (2020). https://doi.org/10.48550/arXiv.2001.03246.

[2] 김동현, 이윤호. *"보안 7대 위협을 이용한 ISMS-P 인증효과에 관한 연구: 기업규모와 경력 중심으로."* 한국정보기술학회논문지, 18(4) (2020): 109-119. 10.14801/jkiit.2020.18.4.109.

[3] Hwang, I., Seo, R. & Hu, S. *"Boosting employee information security compliance: the contingent roles of task–technology and person–organization fits."* Humanit Soc Sci Commun 12, 563 (2025). https://doi.org/10.1057/s41599-025-04718-x.

[4] Haixing Gong, Hui Zou, Xingzhou Liang, Shiyuan Meng, Pinlong Cai, Xingcheng Xu, Jingjing Qu. *"DeepInnovation AI: A Global Dataset Mapping the AI Innovation and Technology Transfer from Academic Research to Industrial Patents."* arXiv preprint (2025). https://arxiv.org/abs/2503.09257.

[5] Zbigniew Ciekanowski, et al. *"Human Resources in Organizational Security Management."* European Research Studies Journal, Volume 26, Issue 4 (2023): 802 – 812. https://doi.org/10.35808/ersj/3328.

[6] Marta Prato. "The Global Race for Talent: Brain Drain, Knowledge Transfer, and Growth." *The Quarterly Journal of Economics*, Volume 140, Issue 1 (2025): 165 – 238. https://doi.org/10.1093/qje/qjae040.

[7] Jana Žuľová and Marek Švec. "*Legal Issues of Pre-employment Background Checks."* 1st edition. Hürth : Wolters Kluwer Deutschland (2

021).

[8] 박성환, 김범수, 박재영. *“정보보안문화와 경영진 리더십이 조직 구성원의 정보보안 행동에 미치는 영향.”* 정보보호학회논문지, 제32권 제2호 (2022): 355 - 370. https://doi.org/10.13089/JKIISC.2022.32.2.355.

[9] 최효식. *“기술 유출방지에 관한 정책방향 고찰: 기술보호 법령체계 정비와 영업비밀보호 강화 필요성을 중심으로.”* 국내석사학위논문, 동국대학교 일반대학원, (2024): 77. https://doi.org/10.23216/dgu.000000088671.11020.0000924.

[10] RuiQi Yang and Junjie Cai. “Intellectual Property Protection Strategy, Digital Governance, and the Upgrading of Corporate Human Capital Structure－A Quasi-Natural Experiment Based on the Construction of National Intellectual Property Model Cities.” Finance Research Letters (2025). https://doi.org/10.1016/j.frl.2025.107526.

[11] Frank L. Greitzer and Deborah A. Frincke. “Combining Traditional Cyber Security Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation.” Insider Threats in Cyber Security, Springer (2010): 85 - 113. https://doi.org/10.1007/978-1-4419-7133-3_5.

[12] 황인호. “내부자의 정보보안 준수를 위한 정보보안 환경 및 지원 체계 구축: 정보보안 공정성 분위기 강화 관점.” The Journal of the Korea Institute of Electronic Communication Sciences, Volume 17, Issue 5 (2022): 913 - 926. https://doi.org/10.13067/JKIECS.2022.17.5.913.

[13] Martin Sposato. “Opportunities and Risks of Artificial Intelligence in Recruitment and Selection.” Emerald Publishing (2021). https://www.researchgate.net/publication/352464056

[14] 현광남, 박남제. *“공공기관 데이터 개방 활성화를 위한 법령 분석 및 개인정보보호법 적용 방법 연구.”* KIIT 학술대회 논문집. (2023).

[15] 윤민우. *“미국의 정보자유법과 정보공개청구 제도.”* 가천법학, 제13권 제1호 (2020): 365 - 398. https://doi.org/10.15335/GLR.2020.13.1.012.

[16] 송홍석. *“새로운 유럽특허제도와 해외특허출원 전략.”* 전력전자학회지, 제28권 제2호 (2023): 48 - 57.

[17] 류지웅. *“치안공공데이터 이용 및 활용에 관한 법적 연구: EU의 공공데이터 이용 및 활용에 관한 주요 지침의 내용과 비교를 중심으로.”* 토지공법연구, 제91호 (2020): 267 - 299. http://dx.doi.org/10.30933/KPLLR.2020.91.267.

[18] 권지현. *“일본 특허출원비공개제도의 도입과 시사점.”* The Journal of Law & IP, 제12권 제2호 (2022): 1 - 42. https://doi.org/10.23190/lawnip.2022.12.2.001.

[19] 고천천. *“중국 개인정보보호법상 국가간 데이터이동제도에 관한 연구.”* 박사학위논문, 동아대학교, 2023. http://www.riss.kr/link?id=T16683136.

[20] 배덕현 *"중국의 개인정보보호 법제 구축에 대한 소고 -중화인민공화국 개인정보보호법(초안)을 중심으로-"* IT와 법연구 22 pp.247-300 (2021) : 247.

[21] 이상우 *"중국 개인정보 보호체계에 관한 연구 - 신(新)개인정보보호법의 주요내용 -"* 중국법연구 45 (2021) : 333.

[22] 전우정, 정유경. *"기술 영업비밀 해외유출 방지 대책에 관한 연구 - 양형기준 개선을 중심으로 -"* 법조 73.1 (2024) : 323-366.

[23] 정제용. *“미국의 산업기술유출 대응체계와 법제 분석.”* 범죄수사학연구, 제10권 제1호 (2024): 233 - 257. https://doi.org/10.46225/CIS.2024.04.10.1.233.

[24] 김소형, 오창성, 이상희. *“빅데이터 의미연결망 분석을 활용한 인공지능(AI) 인식 연구.”* 한국방송미디어공학회 학술발표대회 논문집. (2024).

[25] 김명길, 권민호, 이현희, 오시몬, 김요한. *“블록체인 기반 분산환경 상에서의 신원인증 기술동향.”* 정보보호학회지. 제34권 제1호 (2024): 45 - 52.

[26] 김태환, 조창희, 최형광 *“오픈소스 블록체인을 활용한 전자문서 위·변조 방지 시스템 설계 및 구현 연구 - 하이퍼레저를 중심으로”* 한국IT정책경영학회 논문지 13.1 (2021) : 2271-2279.

ABSTRACT

A Study on Talent Leakage and Response Strategies in Patent Information Disclosure

Song Hyunche
Department of Future Convergence Technology Engineering
Graduate School of
Sungshin Women's University

The rapid development of high-tech industries and the intensifying competition for global technology hegemony are highlighting the securing and protection of high-quality technology talents as important strategic tasks at the national and corporate level. Competition in national strategic technologies such as semiconductors, artificial intelligence (AI), bio-health, and secondary batteries is shifting beyond simple technology development to a structure in which success or failure depends on who preempts and protects key talents who can create and maintain the technology. As a result, the leakage of talent, especially the risk of identifying and scouting external information, is emerging as a key variable in security and industrial strategies.

However, the current patent system fully discloses not only the name

of the inventor but also the detailed address (including copper and lake) through public information for the purpose of publicizing technical information and protecting industrial property rights. In the past, such information could only be accessed in static documents, but today, the development of artificial intelligence (AI) and big data analysis technologies has made it technically possible to identify specific talents using public information, and in fact, companies, investors, and foreign research institutes are reported to use it to select high-quality talents. This refers to a structural security threat in which talents fostered for a long time by a specific company or country can be 'identified' and 'contacted' from the outside regardless of their will.

This study seeks to find policy alternatives to solve these structural vulnerabilities. First, the public information structure and personal information entry method of the Korean Patent Publication were precisely analyzed, and the difference from international personal information protection standards was examined by comparing it with patent systems in major countries such as the United States, Europe, Japan, and China. Furthermore, based on actual open patent data, how AI and data analysis can be used to identify talents was analyzed through cases, and the possibility of talent leakage was specifically derived. In this process, the direction of institutional design that can minimize the exposure of inventors' personal information while maintaining the publicity of technical information was sought.

In particular, this study proposes a structure in which the inventor's identity is marked in a non-identification manner using a unique

researcher number (e.g., national researcher number, ORCID, etc.), and performance and information reading are subject to the researcher's own selective consent. This plan can function as a practical alternative to achieving the two goals of personal information protection and technology information linkage in a balanced way, and provides a foundation for various stakeholders such as researchers, companies, and task managers to efficiently utilize information.

In terms of research methodology, the analysis of the domestic and foreign patent system, the analysis of actual public information data-based actual conditions, the review of leakage cases, and the possibility of using researcher numbers from a policy and technical perspective were conducted in parallel. In addition, the feasibility and expected effects of the proposed countermeasures were reviewed quantitatively and qualitatively, and criteria to be considered in future institutional design were presented.

In conclusion, this study shows the possibility of an information management system that can simultaneously protect key talents and disclose personal information even under a patent system that presupposes the disclosure of technical information. This is expected to be used as basic data for establishing human resource security strategies to prevent the leakage of technical talents in advance and secure competitiveness in high-tech industries in the long term.