

발간등록번호

00-0000000-000000-00

ISBN 000-00-0000-000-0 0000

지식재산 보호기술 개발을 위한 선행연구

2026. 07



제 출 문

지식재산처장 귀하

본 보고서를 “지식재산 보호기술 개발을 위한 선행연구” 과제의 최종 보고서로 제출합니다.

2026년 7월 3일

- 주관연구기관명 : 한국특허전략개발원
- 연구기간 : 2026년 5월 11일 ~ 2026년 7월 3일
- 주관연구책임자 : 권병기 (한국특허전략개발원 연구위원)
- 참여연구원
 - 연구원 : 전상규 (한국특허전략개발원 전문위원)
 - 연구원 : 최진영 (한국특허전략개발원 책임연구원)
 - 연구원 : 황지훈 (한국특허전략개발원 주임연구원)

목 차

제1장 서론	1
제1절 연구의 필요성	1
제2절 연구의 내용 및 방법	7
제2장 환경분석	8
제1절 대내외 정책·제도 동향	8
제2절 시장 동향	23
제3절 기술동향	28
제4절 시사점 및 대응방향	32
제3장 R&D 추진전략	35
제1절 추진 방향 도출	35
제2절 비전 및 목표	47
제3절 핵심 추진과제	48
제4절 추진전략	57
제4장 기대효과	60
제1절 기술적 효과	60
제2절 경제적 효과	61
제3절 사회적 효과	62
제 5장 결론	64

표 목차

표 1. 국내 산업별 유출 비중 및 주요 내용	1
표 2. 지식재산처의 기술유출 대응체계 강화 현황	6
표 3. 부처별 역할	6
표 4. AI 위험관리 프레임워크 개요	9
표 5. 글로벌 주요국 vs 국내 지식재산 보호 정책·제도 비교 분석	33
표 6. SWOT 분석	39
표 7. 현황 및 문제점과 핵심 이행 과제	41
표 8. 위조방지 분야 고도화 가능성	43
표 9. 위조방지 사업의 차별성	45
표 10. 위조방지 원천기술 구분	48
표 11. 위조방지·정품식별 분야 기술분야 후보 및 도출 근거	50
표 12. 집중 투자 분야 선정	51
표 13. 산업스파이 방지기술 기술개발	51
표 14. 부처 기술유출 대응 사업과의 차별성	53
표 15. 12대 국가전략기술 중 한국 특허 출원 비중 비교	54
표 16. 산업스파이 방지 분야 4대 핵심 기술분야 및 도출 근거	55
표 17. 특허분석 기반 산업스파이 방지기술 유망 후보과제(안)	55
표 18. 위조방지·산업보안 공통 구조	57
표 19. Two-Track 추진체계	58
표 20. 성과확산 메커니즘 3단계 설계	58



그림 목차



그림 1. NIST가 인정한 3가지 PQC알고리즘	8
그림 2. 유럽 공통 데이터 공간	12
그림 3. NIS2 시행에 따른 주요사항	13
그림 4. DPP에 수록되는 공급단계별 정보	13
그림 5. 일본 경제안보추진법안 주요내용	15
그림 6. AI대응 로드맵	16
그림 7. K-브랜드 위조상품 민관 공동대응 협의회	20
그림 8. AI기반 국내 온라인 위조상품 모니터링 사업개요	20
그림 9. 제5차 산업기술 유출방지 및 보호 종합계획 비전 및 추진과제	21
그림 10. 글로벌 위조시장	24
그림 11. 글로벌 위조방지 패키징 기술시장 규모 전망	25
그림 12. 사이버보안 방지 기술 시장	26
그림 13. 25년도 K-브랜드 위조물품 통관단계 적발 현황	27
그림 14. 산업기술 유출건수 및 규모, 사례	28
그림 15. 적외선 기반 위변조 방지 멀티스펙트럼	29
그림 16. 농식품 정보의 위·변조를 막을 수 있는 메타 라벨링 기술	29
그림 17. UEBA 운영체계	31
그림 18. Zero trust 아키텍처	32
그림 19. 특사경 기술유출 적발 사례	45
그림 20. 비전 및 목표	47

요 약 문

첨단 산업기술의 해외 유출과 K-브랜드 위조상품 유통이 산업화·조직화되면서 국가 성장동력 훼손과 국민 건강·안전 위협이 심화되고 있다. 최근 5년('20~'24년)간 적발된 산업기술 해외 유출은 105건, 피해 추산액은 약 25조 원에 달하며, 전 세계에 유통되는 한국 기업의 위조상품 규모는 약 97억 달러로 우리나라 전체 수출액의 1.5%에 이른다. 그러나 기존의 사후 적발·처벌 중심 대응만으로는 지능화되는 기술유출과 고도화되는 위조상품 유통을 효과적으로 방어하는 데 한계가 있으므로, 지식재산 보호정책의 무게중심을 선제 예방형 체계로 전환하기 위한 혁신기술 기반 R&D 추진이 시급하다.

지식재산 보호기술은 국가 경제안보와 산업경쟁력 확보 측면에서 전략적 중요성이 높으나, 초기 시장의 불확실성과 낮은 수익성으로 인해 민간의 자발적 투자가 제한적이다. 특히 국내 물리보안·위조방지 업계는 자본금 50억 원 미만 영세기업 비중이 94.9%에 달해 고도화된 R&D 투자가 구조적으로 어렵다. 반면 EU 디지털제품여권(DPP), 미국 SBOM 등 글로벌 공급망 규제는 제품 진위 검증, 이력 추적, 디지털 무결성 확보를 요구하고 있어, 국내 기업의 수출경쟁력 확보를 위해 정부 주도의 선제적 마중물 투자가 요구된다.

본 연구는 국내외 정책·제도, 시장 및 기술 동향을 종합적으로 조사·분석하여 지식재산 보호기술 R&D의 추진 여건과 환경을 진단하고, 이를 토대로 사업 추진전략, 핵심 추진과제 및 기대효과를 도출하였다. 환경분석 결과, 미국·EU·중국·일본 등 주요국은 지식재산 보호와 산업기술 보호를 국가안보 및 공급망 전략의 핵심 의제로 격상하고 있으며, 기술 표준, 인증체계, 사이버보안, 위조방지 인프라를 연계한 보호체계를 강화하고 있는 것으로 나타났다. 반면 국내는 관련 법·제도 정비에도 불구하고 지능화된 기술유출을 사전에 탐지·차단 하거나 고도화된 위조를 실시간 식별할 기술적 실행 수단과 통합 대응 인프라가 미흡한 것으로 분석되었다.

환경분석과 SWOT 분석을 토대로 본 연구는 사업 비전을 'K-Tech & K-Brand 수호를 통한 지식재산 보호 강국 도약'으로 설정하고, 목표를 '혁신기술 활용을 통한 지식재산 보호 강화'로 제시하였다. 사업 추진 방향은 위조상품 원천 차단을 위한 위조방지·식별 기술 자립화, 첨단 산업기술 유출의 선제적 예방·탐지·추적을 위한 능동형 방어기술 확보, 보안 표준·인증 패스트트랙 구축 및 수요 기반 지식재산 보호 문화 확산으로 설정하였다.

추진전략은 위조방지·식별기술과 산업스파이 방지기술을 Two-track 구조로 구분하되, AI 판별, 블록체인, 디지털 워터마킹 등 공통 기반기술을 활용하여 통합 보호 생태계를 구축하는 방향으로 설계하였다. 또한 기술 특성에 따라 자유공모와 정책지정 방식을 병행하고, 수요 연계형 실증, 성능 인증 패스트트랙, 독점적 통상실시권 도입을 연계함으로써 기술개발-실증-인증-현장 적용-사업화로 이어지는 전주기 성과확산 체계를 강화하고자 하였다.

핵심 추진과제는 특허 빅데이터 분석, 한국 산업 특성, AI 활용 가능성을 종합하여 도출하였다. 내역1인 위조방지 및 식별기술은 물리적 복제가 원천적으로 어려운 '코드·정보 기반 기술'과 물리·디지털 인증을 결합한 '고도화·복합인증 기술'을 중점 투자 분야로 설정하였다. 이를 통해 데드카피 수준의 정교한 위조에 대응하고, 현장 수요 기반 자유공모와 PM 주도 통합 실증 체계를 통해 산업 현장 적용성을 높이는 방향으로 기획하였다.

내역2인 산업스파이 방지기술은 산업기술 유출 대응을 예방·탐지·추적-통합보호의 전주기 구조로 재설계 하였다. 이에 따라 데이터 통제 및 권한 지능화, 지능형 이상행위 탐지, 유출 추적 및 디지털 증거 확보, 물리·사이버 융합 보안 등 4대 핵심 기술분야를 도출하였다. 또한 보안기술의 기밀성과 공공성을 고려하여 정책지정 방식으로 추진하고, 실증과 적용까지 연계되는 PM 중심의 전주기 관리체계를 마련하였다.

본 연구가 도출한 사업은 기술적으로 해외 의존도가 높은 위조방지 원천기술의 국산화와 지능형 산업스파이 방지기술의 독자 확보를 통해 기술 자립화와 선제적 대응 역량을 강화할 것으로 기대된다. 경제적으로는

위조상품 유통 및 산업기술 유출 피해를 경감하고, 수출기업 보호, 국가 성장동력 유지, 지식재산 보호기술 산업의 신성장동력 창출에 기여할 수 있다. 사회적으로는 유해 위조상품 차단을 통한 국민 건강·안전 보호, 공정경쟁 시장 질서 확립, 사후 대응에서 선제 예방으로의 정책 패러다임 전환을 촉진할 것으로 기대된다.

결과적으로 본 연구는 지식재산 보호기술 R&D 추진의 객관적 타당성과 세부 실행과제를 체계적으로 도출함으로써, 기존 사후 적발·처벌 중심 대응에서 AI 기반 실시간 탐지·차단 등 선제 예방형 보호체계로 전환하기 위한 정책적·기술적 기반을 제시하였다. 제안된 사업이 추진될 경우, 지식재산 보호기술이 국가 경제안보의 핵심 R&D로 자리매김하고, K-Tech와 K-Brand의 가치를 기술로 수호하는 지식재산 보호 강국 실현에 기여할 것으로 기대된다.

S U M M A R Y

As the overseas leakage of advanced industrial technologies and the distribution of counterfeit K-brand products become increasingly industrialized and organized, damage to national growth engines and threats to public health and safety are intensifying. Over the past five years from 2020 to 2024, 105 cases of overseas industrial technology leakage were detected, with estimated damages amounting to approximately KRW 25 trillion. In addition, the global circulation of counterfeit products involving Korean companies is estimated at approximately USD 9.7 billion, equivalent to 1.5% of Korea's total exports. However, conventional responses centered on post-incident detection and punishment have clear limitations in effectively defending against increasingly sophisticated technology leakage and advanced counterfeit distribution. Accordingly, it is urgent to promote innovation-technology-based R&D to shift the focus of intellectual property protection policy toward a proactive prevention-oriented system.

Intellectual property protection technologies are strategically important for ensuring national economic security and industrial competitiveness. However, voluntary private-sector investment remains limited due to uncertainty in the early-stage market and low profitability. In particular, 94.9% of companies in Korea's physical security and anti-counterfeiting industry are small enterprises with capital of less than KRW 5 billion, making advanced R&D investment structurally difficult. Meanwhile, global supply chain regulations such as the EU Digital Product Passport and the U.S. Software Bill of Materials are requiring product authenticity verification, history tracking, and digital integrity assurance. Therefore, government-led proactive investment is needed as a catalyst to secure the export competitiveness of Korean companies.

This study comprehensively investigated and analyzed domestic and international policy, institutional, market, and technology trends to diagnose the conditions and environment for promoting R&D in intellectual property protection technologies. Based on this analysis, the study derived business promotion strategies, core implementation tasks, and expected effects. The environmental analysis found that major countries, including the United States, the European Union, China, and Japan, are elevating intellectual property protection and industrial technology protection to key national security and supply chain strategy agendas. They are also strengthening protection systems that integrate technical standards, certification systems, cybersecurity, and anti-counterfeiting infrastructure. In contrast, although Korea has improved related laws and institutions, it still lacks sufficient technical implementation tools and integrated response infrastructure to proactively detect and block intelligent technology leakage or identify advanced counterfeiting in real time.

Based on the environmental and SWOT analyses, this study established the business vision as "leaping forward as a leading nation in intellectual property protection by safeguarding K-Tech and K-Brand." The goal was defined as "strengthening intellectual property protection through the use of innovative technologies." The promotion directions were set as follows: achieving technological self-reliance in anti-counterfeiting and identification technologies to fundamentally block counterfeit products; securing active defense technologies for the proactive prevention, detection, and tracking of advanced industrial technology leakage; establishing a fast-track system for security standards and certification; and expanding a demand-driven culture of intellectual property protection.

The promotion strategy was designed as a two-track structure consisting of anti-counterfeiting and identification technologies and anti-industrial espionage technologies. At the same time, it aims to build an integrated protection ecosystem by utilizing common enabling technologies such as AI-based identification, blockchain, and digital watermarking. In addition, the initiative was designed to combine open competition and policy-designated approaches according to technology characteristics, while linking demand-driven demonstration, performance certification fast-tracks, and the introduction of exclusive non-exclusive licenses. Through this structure, the initiative seeks to strengthen an end-to-end performance diffusion system that connects technology development, demonstration, certification, field application, and commercialization.

The core implementation tasks were derived by comprehensively considering patent big data analysis, the characteristics of Korean industries, and the potential for AI application. For Category 1, anti-counterfeiting and identification technologies, “code- and information-based technologies,” which make physical replication fundamentally difficult, and “advanced and hybrid authentication technologies,” which combine physical and digital authentication, were selected as priority investment areas. Through these technologies, the initiative aims to respond to highly sophisticated counterfeiting at the level of dead copies and enhance industrial applicability through field-demand-based open competition and a PM-led integrated demonstration system.

For Category 2, anti-industrial espionage technologies, the response system for industrial technology leakage was redesigned as a full-cycle structure covering prevention, detection, tracking, and integrated protection. Accordingly, four core technology areas were identified: data control and intelligent authority management; intelligent abnormal behavior detection; leakage tracking and digital evidence acquisition; and physical-cyber convergence security. In addition, considering the confidentiality and public nature of security technologies, this category was designed to be promoted through a policy-designated approach, with a PM-centered full-cycle management system that links technology development to demonstration and application.

The initiative derived from this study is expected to strengthen technological self-reliance and proactive response capabilities by localizing core anti-counterfeiting technologies, which currently have a high level of dependence on foreign technologies, and independently securing intelligent anti-industrial espionage technologies. Economically, it can contribute to reducing damages from counterfeit product distribution and industrial technology leakage, protecting export companies, maintaining national growth engines, and creating new growth drivers in the intellectual property protection technology industry. Socially, it is expected to protect public health and safety by blocking harmful counterfeit products, establish a fair and competitive market order, and accelerate the policy paradigm shift from post-incident response to proactive prevention.

In conclusion, this study systematically derived the objective feasibility and detailed implementation tasks for promoting R&D in intellectual property protection technologies. In doing so, it presented the policy and technological foundation for transitioning from a conventional response system centered on post-incident detection and punishment to a proactive prevention-oriented protection system based on AI-enabled real-time detection and blocking. If the proposed initiative is implemented, intellectual property protection technologies are expected to become a core area of R&D for national economic security and contribute to realizing a leading nation in intellectual property protection that safeguards the value of K-Tech and K-Brand through technology.

제1장 서론

제1절 연구의 필요성

◇ 국내 첨단기술의 해외 유출과 위조상품 불법 유통이 심화되면서, 강력한 지식 재산 보호 체계 구축이 국가 경제안보의 필수 과제로 부상

□ 산업스파이의 지능화·첨단화에 따른 국가 경제안보 위협

- 첨단 산업기술 유출*은 국내 기업 피해뿐만 아니라 국가 성장동력 훼손과 안보 위협으로 직결됨에 따라, 기술보호 정책은 사후 적발 중심 대응에서 선제 예방형 대응으로 전환 필요
- 최근 5년('20~'24년)간 적발된 산업기술 해외 유출은 총 105건, 피해 추산액은 약 25조 원에 달하는 등 국가 경제에 치명적 타격
- * 특히 반도체(39%), 디스플레이(20%) 등 국가 경제를 지탱하는 핵심 산업 분야의 비중이 높아, 이러한 기술 유출은 단순한 개별 기업의 손실을 넘어 국가 경제의 성장 잠재력을 훼손하고 안보를 위협하는 중대한 사안 (출처: 국가정보원)

표 1. 국내 산업별 유출 비중 및 주요 내용

산업 분야	유출 건수(최근 5년)	비중(%)	핵심 내용
반도체	41건	39%	메모리 및 미세 공정 노하우 탈취 집중
디스플레이	21건	20%	OLED 등 차세대 패널 기술 경쟁 심화
자동차	9건	8.5%	자율주행 및 전기차 관련 핵심 설계 기술
기타	34건	32.5%	이차전지, 조선, 바이오 등 전방위 확산

출처: 국가정보원(NIS)

- 미국, 독일 등 주요 선진국도 기술 탈취를 국가적 위기로 인식
- * (미국) 위조·불법복제·영업비밀(사이버 포함) 탈취로 인한 미국 경제 손실이 연 2,250억~6,000억 달러 (미 GDP 1~3%) 규모로 평가(출처: IP Commission)
- * (독일) 사이버범죄·사보타주 피해가 연간 약 2,670억 유로(약 3,000억 달러) 수준으로 추정, 응답 기업의 81%가 데이터 절도(고객정보·접근정보·지식재산/특허 등)를 경험했다고 보고 (출처: Bitkom)
- 생성형 AI, 클라우드 등 신기술이 유출 도구로 악용되며, 민간의 기존 물리적 보안 체계를 무력화
- (AI·클라우드 악용) 챗GPT 등 생성형 AI에 핵심 코드를 입력하거나, 클라우드 협업 툴을 통한 비정상 접근 등 유출 경로가 디지털·지능형으로 진화
- (대응 한계) 개별 기업 차원에서는 고도화된 사이버·내부자 공모 위협을 방어하는 데 기술 및 재정적 한계에 봉착하여 국가 차원의 방패(Anti- Espionage) 기술의 개발이 시급

□ 국내 위조상품 유통의 산업화·조직화

- (역기능 확대) K-브랜드, 한류 확산과 온라인 유통 증가로 국내 제품의 위조상품 유통이 산업화·조직화
 - (경제적 손실) 위조 유통은 국내기업의 매출 감소 및 국가 브랜드 가치, 일자리 등 사회경제에 직접 타격
 - * 전 세계 유통되는 한국 기업의 위조상품 규모는 약 97억 달러(약 11조 원)에 이르며, 이는 한국 전체 수출액의 1.5%에 해당하는 막대한 규모. 위조상품 유통으로 인한 한국의 제조업 일자리 상실은 약 1만 3천여 개, 세수 손실은 약 15억 7천만 달러로 추산
(출처: Illicit Trade and the Korean Economy(OECD, 2024))
 - (국민 안전 위협) 화장품, 의약품, 유아용품 등 유해 물질이 함유된 가품 유통으로 국민의 건강과 생명을 직접적으로 위협
 - * 온라인 주문·소포 기반 위조 유통 품목에 의류·신발뿐 아니라 전기장비·장난감·화장품 등이 포함됨을 제시하며, 소비자 안전과 직결될 수 있음을 시사함
- (유통 경로의 다변화) 국경 간 전자상거래 및 소포 중심의 쪼개기 유통으로 기존 단속 체계 무력화
 - 쪼개기 유통 구조는 단속 회피와 소비자 점점 확대를 동시에 유발해 피해 확산 속도를 높임
 - * 전자상거래 활동 지표가 높을수록 위조품 수입이 증가하며, 특히 소포(small parcels) 기반 위조 반입과의 상관성이 더 강하게 나타난다고 분석, 온라인 주문 위조품 적발의 90% 이상이 우편(post) 경로로 운송되었다고 나타남 (출처: Illicit Trade and the Korean Economy(OECD, 2024))
 - (기술적 대응 필요) 육안 식별이 불가능한 데드카피(Dead-copy) 수준의 위조 기술에 대응하기 위해, 위변조가 원천 차단되는 고신뢰 식별 기술(블록체인, DNA 잉크 등) 개발 및 보급 절실

□ 지식재산 침해 방지라는 단일 정책목표 아래, 위조상품 근절과 산업기술 유출 대응 정책의 통합적 추진 필요

- 위조상품 유통과 산업스파이 범죄는 우리 기업의 핵심 가치(기술, 브랜드 등)를 훼손하고 국가 수출경쟁력을 저해하는 공통 위협 요인

◇ (위조방지) 기술 양극화 해소 및 글로벌 표준 선도를 위한 정부의 마중물 역할 필요

□ 글로벌 위조방지 시장의 급성장과 기술 고도화로 인한 시장진입 장벽 상승

- (시장 성장) 지식재산 보호기술 시장은 규제 강화, 기술 진화, 사이버 위협 및 침해 지능화에 따라 급격한 성장세
 - * 글로벌 위조방지 시장은 2025년 2,040.8억 달러 → 2033년 4,282.8억 달러 확대 전망
(출처: Grand View Research, 2025)
- (기술 진입장벽 상승) 기술 고도화에 따라 복제저항성 확보, 디지털 인증, 글로벌 표준 대응 등 요구 수준이 급격히 상승하며, 기술 개발 및 적용에 필요한 비용과 복잡성이 크게 증가
 - 위조방지 기술은 홀로그램·보안스티커 중심에서 나노마킹·블록체인·AI 판독을 결합한 복합 인증 기술 중심으로 전환 중이며, 소재·알고리즘·플랫폼의 복합 설계 역량을 보유한 기업만이 시장에 참여 가능
 - 초기 투자비용과 개발 리스크가 높고 단기간 수익창출이 어려운 구조로, 정부의 선제적 기술개발

지원 없이 국내기업의 기술격차는 회복 불가능한 수준으로 확대될 위험

□ 고비용·저효율의 기술적 딜레마로 인한 민간투자의 구조적 한계

- **(산업 기반의 영세성)** 국내 물리보안 및 위조방지 업체는 자본금 50억 미만의 영세 기업이 압도적 다수(94.9%)를 차지하여, 고도화된 R&D 투자가 원천적으로 불가능한 투자 교착 상태
 - * 물리보안 기업 중 자본금 50억 원 미만 기업 비중 94.9%, 정보보안 기업 중 88.0%가 50억 미만으로 조사됨(출처: '23 정보보호산업 실태조사(KISIA, 2024))
- **(기술의 진부화)** 자금력 부족으로 인해 RFID, 블록체인 등 첨단 기술 대신, 복제가 쉬운 홀로그램 등 진입장벽이 낮은 범용 기술(Low-end) 위주로 시장이 고착화됨
 - 데드카피(Dead-copy)를 원천 차단하기 위해선 나노 마킹, 복합 인증 등 차세대 기술이 필요하나, 초기 투자 비용 대비 수익 불확실성(High Risk)이 커 정부의 마중물 역할 필수
 - * 전자·디지털 태그(RFID 등)나 IT 융합(블록체인·NFT) 등 고보안 기술은 단가가 높거나 시스템 구축이 복잡하여, 자금력이 부족한 수출 중소기업이 자발적으로 도입하기에는 한계가 명확

□ 글로벌 규제 강화 및 국내 표준기술 부재로 인한 수출 차단의 현실적 위험

- **(EU 디지털 제품 여권의 즉각적 위협)** EU는 2027년 배터리를 시작으로 산업 제품에 디지털 제품 여권(Digital Product Passport, DPP)을 단계적으로 의무화하기로 확정하여, 위조방지 기술 미보유 기업은 대EU 수출 자체가 차단되는 상황에 직면
 - DPP 규제는 2027년 배터리를 시작으로 섬유·철강·전자·타이어 등 전 산업군으로 확대 적용될 예정이며, 제품의 정품 인증·이력 추적·진위 검증을 위한 위조방지 기술 내재화를 사실상 강제
 - 블록체인 기반 정품 인증·디지털 마킹 등 위조방지 기반 기술 없이는 DPP 대응이 불가능하며, 정부 지원이 없으면 중소 수출기업은 단독으로 이 체계를 구축할 수 없어 EU 시장 퇴출로 이어질 우려
- **(표준 공백의 이중 위협)** KS A ISO 22382·22383 등 위조방지 관련 국내 표준은 채택되어 있으나, 표준 요건을 실질적으로 충족하는 국산 위조방지 기술의 개발·실증이 미흡하여 기술 종속과 무역 장벽이라는 이중 위협에 노출
 - 국내 기업이 우수한 기술을 보유하더라도 글로벌 시장에서 표준 부합성을 공인받지 못해 수출 경쟁력 저하로 귀결
 - EU 등 주요국이 위조 식별 가이드라인을 강화하는 추세에서, 독자적 기술 규격 없이는 해외 원천 기술에 대한 종속과 이에 따른 로열티 부담·기술 협상력 상실이 불가피

□ 개별 기업 단독 대응의 실효성 한계

- 현재 위조 피해 대응은 개별 기업이 자체 비용으로 감당하는 구조이나, 위조품 유통의 규모·속도·경로가 어느 한 기업의 대응 역량을 근본적으로 초과
 - 위조상품 적발·소송·모니터링 비용은 중소 수출기업에 과중한 부담이며, 현지 소송의 손해배상액이 낮아 비용 대비 실효성이 미흡하여 개별 법적 대응의 한계가 명확
 - 글로벌 e-커머스 플랫폼(알리바바·아마존 등)을 통한 위조품 유통은 24시간·다국가 동시 진행으로, 어느 한 기업이 단속·차단할 수 있는 범위를 초과
 - 근본적 해법은 사후 단속이 아닌 사전 기술 차단, 즉 위조가 물리적·기술적으로 불가능하도록 제품에

고신뢰 인증 기술을 내재화하는 것이며, 이는 정부 주도 기술 개발로만 실현 가능

◇ (산업보안) 지능형 위협에 대응하는 ‘공공재’로서의 보안 기술 확보

□ 산업보안 기술의 패러다임 전환

- (기술 전환) 산업보안 기술은 기존 DLP*·DRM** 중심의 사후 통제 방식에서 UEBA***, AI 기반 이상탐지, 포렌식 워터마킹, 제로트러스트 기반 통합보안 체계로 전환되는 추세
 - * DLP(데이터 유출 방지) : 사내 정보의 외부 전송 통제·차단
 - ** DRM(디지털 저작권 관리) : 문서 암호화를 통한 권한자 외 접근(열람·수정) 통제
 - *** UEBA(사용자·단말 행위 분석) : 평소 행동 패턴 분석을 통한 내부 이상행위 탐지
- 생성형 AI, 클라우드, 재택근무 확산 등으로 기술 유출 경로가 다변화·지능화되며, 사전 탐지 및 실시간 대응 중심의 보안 기술 수요가 급격히 증가
- (기술 진입장벽 상승) 이러한 기술 전환에 따라 데이터 분석, AI 모델링, 보안 아키텍처 설계 등 고도화된 기술 역량과 대규모 투자, 전문 인력 확보가 필수적 요구
 - 차세대 산업보안 기술은 단일 솔루션이 아닌 플랫폼 기반 통합보안 구조로 발전하면서, 초기 구축 비용과 운영 복잡성이 크게 증가

□ 개별 기업의 보안 역량을 초과하는 비대칭적 기술 유출 위협

- (주요 타겟) 대기업 대비 보안 역량이 절대적으로 부족한 중소기업이 산업스파이의 주요 타겟으로 지목되며 피해가 집중됨
 - 최근 5년(‘20~’24)간 적발된 기술유출 사건의 86.5%가 중소기업에 집중되는 등 대기업 대비 보안 역량이 절대적으로 부족한 중소기업이 산업스파이의 주 타겟이 되고 있음
 - * 최근 5년(‘20~’24)간 전체 기술유출 668건 중 중소기업 피해가 578건(86.5%)으로 압도적 비중 차지 (출처: 경찰청 산업기술유출 수사 통계(2025))
- (대응 역량) 포렌식 워터마킹(유출 경로 추적)이나 AI 기반 이상징후 탐지 기술은 막대한 구축 비용과 전문 인력이 요구되어, 중소·중견기업은 사실상 ‘보안 무방비’ 상태에 노출
 - * 최근 5년간(‘20~’24) 적발된 산업기술 해외 유출 건수는 105건으로 이를 통한 피해 규모는 약 25조 원으로 추산(출처: 국가정보원(NIS))

□ AI·클라우드 등 환경 변화에 따른 국가 안보 차원의 대응 필수

- (지능형 공세) 생성형 AI를 활용한 코드 탈취, 클라우드 협업 툴을 통한 우회 공격 등 유출 수법은 고도화되는 반면, 기업의 방어 체계는 과거 머물러 있어 창과 방패의 격차 심화
 - 특히 재택근무·클라우드 확산으로 인한 문서 권한 관리(DRM)의 허점과 초소형 카메라를 이용한 불법 촬영 등은 개별 기업의 보안 통제 범위를 벗어난 위협임
- (공공재적 확산) 기술 보호는 단순 사익 보호를 넘어 국가 경쟁력(GDP, 일자리)과 직결되는 공공재 성격을 가짐
 - * 경제적 파급효과 : 국내 정보보호산업 매출은 약 16.8조 원(’23년) 규모로 성장 중이나, 중소기업의

◇ (정책제도) 지식재산처 출범에 따른 위조상품·기술유출 대응 컨트롤타워 구축 필요

□ BH·국회·재계의 지식재산처 중심 기술보호 체계 강화에 대한 국가적 요구

- 지식재산처 승격('25.10.) 이후 BH·국회·재계를 중심으로 기술유출 대응 체계의 총괄 주체로서 지식재산처의 역할 강화 요구가 지속 제기
 - * 국민권정부 정부조직개편에 따라 특허청은 국무총리 소속 지식재산처로 승격('25.10.)
- (VIP 지시) 제2·3회 국무회의(각 '26.1.20, 1.27) 및 재계간담회('25.10.)에서 "기술유출 대응 체계 구축 및 특사경 인력증원 방안 수립", "기술유출 범죄에 대한 처벌 강화 필요" 등 지재처 중심의 대응체계 강화 지시
- (국회 의결) 국회 정보위원회('25.10.)는 "지식재산처 중심의 기술안보 컨트롤타워 구축이 시급"하다고 결의하며, 지재처가 지식재산 정책·보호·분쟁대응의 전주기 정책을 종합 집행할 수 있는 유일한 중앙행정기관임을 명시
- (재계 요구) 산업계는 영업비밀·특허 등 지식재산 중심의 기술보호 체계 고도화와 처벌 실효성 강화를 지재처에 지속 요청

□ 위조방지와 기술유출 대응 모두의 핵심은 지식재산 보호이며, 지식재산처는 이를 위한 제도적·법적 기반을 보유

- 위조상품 피해는 상표권·디자인권 등 산업재산권 침해가 핵심이므로, 지식재산 보호 체계를 총괄하는 지식재산처가 위조방지 기술 개발의 정책 주체로서 고유한 적격성을 보유
- 위조상품으로 인한 피해는 결국 수출 기업의 상표·브랜드·디자인 등 산업재산권이 침해당하는 것이며, 이에 대한 제도·법적 대응 권한은 지식재산처가 독점적으로 보유
- 지식재산처는 K-브랜드 정부인증제도('26년 하반기 시행) 및 추경 95억 원을 확보하는 등 위조방지 정책 추진 기반을 실질적으로 구축 중이나, 인증제도의 실효성은 기술적 위조방지 수단(나노마킹·AI 판독·블록체인 추적 등)이 병행될 때 비로소 담보됨
- 따라서 제도와 기술의 연계·통합이 가능한 지식재산처가 위조방지 기술 개발 R&D를 직접 추진하는 것이 정책 일관성 측면에서 필수적
- 기업의 핵심 기술·경영정보는 영업비밀·특허 등 지식재산으로 보호되므로, 기술보호의 핵심이 곧 지식재산 보호로 귀결
- '25년 경찰 송치 기술유출 사건의 약 66%가 영업비밀 침해(부정경쟁방지법 위반)이며, 이는 산업 기술보호법 위반(13%), 형법상 업무상 배임(22%) 등을 크게 상회
 - * 경찰청 기술유출 범죄 단속 통계('25년 송치 기준): 부경법 118건(66%), 산기법 22건(13%), 형법 등 39건(22%), 총 179건 (출처: 경찰청)
- R&D 수행 기업의 76.1%가 영업비밀을 가장 중요한 지식재산으로 인식(美 국립과학재단 NSF, 2021) 하여, 기술보호 수단 중 영업비밀·특허의 중요성이 글로벌하게 확인됨
- 지식재산처는 기술유출 선제적 대응을 위한 법적 근거와 예산·조직 기반을 순차적으로 완비

표 2. 지식재산처의 기술유출 대응체계 강화 현황

시기	내용	비고
'18.7월	■ 부정경쟁방지법 개정으로 행정조사 대상에 '아이디어 탈취' 포함	사후조치 (법제)
'19.3월	■ 사법경찰직무법 개정으로 특허·영업비밀·디자인 수사팀 출범	사후조치 (법제)
'21.7월	■ 기술디자인특사경과, 부정경쟁조사팀 신설	사후조치 (직제)
'24.1월	■ 사법경찰직무법 개정으로 영업비밀 침해 전반으로 수사범위 확대	사후조치 (법제)
'24.8월	■ 산업재산정보법 제정·시행으로 기술유출 방지 목적 미공개 특허 분석 및 제공 가능	사전조치 (법제)
'26.5월	■ 산업스파이 신고포상금제도 도입	사전조치 (법제)

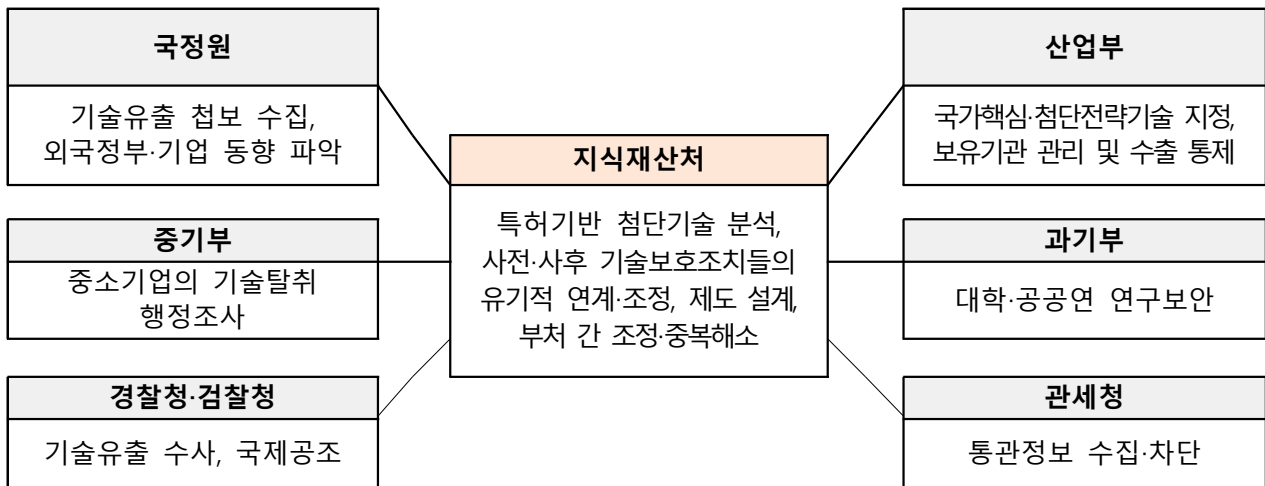
- 특허 산업재산정보법('24.8)은 지식재산처장이 출원 중인 미공개 특허정보를 기술유출 방지 목적으로 분석·이용할 수 있는 근거를 마련한 유일한 법률로, 지식재산처만 수행 가능한 고유 업무영역을 확립

* 산업재산정보법 §15① - 지식재산처장은 국가의 안전보장 또는 국가의 중대한 이익과 관련된 기술 등의 유출 방지 및 보호를 위하여 필요한 경우 출원 중인 산업재산 정보를 이용하거나 관계 국가행정 기관에 제공할 수 있다.

□ 범부처 기술유출 대응에서 지식재산처의 총괄조정 역할 및 특허기반 선제탐지 필요

○ 기술유출 대응은 다수 부처에 기능이 분절되어 있어 유기적 연계·조정과 보호 공백 발굴·제도 반영이 시급하며, 이를 총괄할 컨트롤타워 역할은 지식재산 전주기 정책을 집행할 수 있는 지식재산처의 고유 영역

표 3. 부처별 역할



○ 특허 기반 기술 유출 패턴 분석을 통해 기술유출 위험신호를 선제적·과학적으로 실시간 탐지하는 역량은 지식재산처만 보유

- '26년 특허빅데이터 조사 사업 25억 원을 확보하는 등 특허 빅데이터를 활용한 기술유출 선제 대응 역량을 제도화

- 또한, 특허 대상으로 국가핵심기술, 국가첨단전략기술 등 국가 기술안보에 중요한 기술과 관련된 특허들을 선제적으로 선별 및 관계기관에 공유 중

○ 따라서 본 사업은 범부처 기술유출 대응 체계에서 타 부처 사업과 중복되지 않는 지식재산처 고유의 특허·영업비밀 기반 기술유출 방지 기술개발 영역을 담당하며, 이를 통해 기술보호의 핵심 영역인 지식

제2절 연구의 내용 및 방법

□ 지식재산 보호기술 분야 환경 분석

- 국내외 정책·제도, 시장 및 기술 동향, 관련 연구개발 사업 현황 등을 종합적으로 조사·분석하여 지식재산 보호기술 R&D 분야의 추진 여건 및 환경을 진단
- 지식재산 보호기술 연구개발 관련 국내외 우수사례와 지원체계를 분석하여 사업 추진의 시사점과 성공요인을 도출

□ 지식재산 보호기술 추진전략 수립

- 국내외 정책·시장·기술 환경 분석 결과를 토대로 사업 추진의 기본방향과 전략목표를 설정하고, 중장기 관점의 사업 추진전략을 수립
- 지식재산 보호기술 사회문제 해결 수요와 사업화 가능성을 고려하여 핵심 지원 분야 및 중점 투자영역을 도출하고 분야별 추진전략을 마련

□ 지식재산 보호기술 기대효과 도출

- 지식재산 보호기술 R&D를 통해 창출 가능한 중점 연구개발 과제 및 핵심기술을 도출하고, 분야별 전략적 투자 필요성을 제시
- 연구개발 성과의 기술적 우수성 및 사회·경제적 파급효과를 분석하여 국민 체감 성과 창출 및 국가 경쟁력 제고 측면의 기대효과를 도출

제2장 환경분석

제1절 대내외 정책·제도 동향

1 해외정책 동향

□ (미국) 미국의 기술패권 유지를 위한 지식재산 보호 및 사이버보안 전략 강화 추진

- 차세대 암호 체계인 양자내성암호로의 전환을 국가 안보 차원의 필수 과제로 격상하여 범정부 차원의 이행 로드맵 이행
- 미국 국립표준기술원(NIST)을 중심으로 글로벌 양자내성암호 표준 알고리즘 최종 확정 및 연방기관의 기술 도입 의무화
- 2024년 ML-KEM, ML-DSA, SLH-DSA 등 3종의 알고리즘을 세계 최초 표준으로 승인하며 글로벌 암호 체계 전환의 기준점 형성



그림 1. NIST가 인정한 3가지 PQC알고리즘

- 2030년까지 연방 정부 시스템의 전면적인 양자내성암호 전환을 목표로 하는 ‘양자 컴퓨팅 사이버 보안 대비법’에 근거하여 단계별 이행 강제
 - * 특히 현재 데이터를 탈취해 두었다가 향후 양자컴퓨터로 해독하려는 ‘Harvest Now, Decrypt Later’ 위협에 대응하기 위해 선제적 전환을 가속화
- 기존 암호 체계와 양자내성 암호를 혼합하여 사용하는 하이브리드 암호 방식을 과도기적 표준으로 설정하여 보안 공백 최소화
- 구글 및 클라우드플레어 등 글로벌 빅테크 기업들과 협력하여 실제 네트워크 트래픽에 하이브리드 TLS를 선제적 도입
- 암호 알고리즘 교체 시 발생 가능한 시스템 병목 현상 해결을 위한 하드웨어 가속기 개발 및 최적화 가이드라인 보급
- 인공지능 확산에 따른 신규 보안 위협에 대응하기 위하여 AI 위험관리 프레임워크 수립 및 규범 주도권 확보
 - AI 모델 자체에 대한 공격방어와 AI를 활용한 보안 운영고도화를 포괄하는 종합 대책 마련
- AI 학습 데이터의 오염이나 모델 회피 공격 등 새로운 형태의 위협으로부터 핵심 기술 자산을 보호하는 기술 가이드라인 제시

- 사이버보안 특화 거대언어모델(LLM)을 활용하여 위협 탐지 및 대응 의사결정을 자동화하는 지능형 보안 체계 구축 지원

표 4. AI 위험관리 프레임워크 개요

(추진근거) '20년에 제정된 '국가인공지능 이니셔티브법(National Artificial Intelligence Initiative Act of 2020 (P.L. 116-283))'*에 따른 미 의회의 지시로 AI RMF를 수립

- * 공공 및 민간 영역에서 신뢰할 수 있는 AI 시스템 개발 등을 위해 국가 AI 이니셔티브를 수립·이행하는 내용을 포함
- (목적) 모든 분야·규모의 기업·조직이 AI 위험을 해결할 수 있도록 유연하고 체계적이며 측정 가능한 프로세스를 제공하여 AI 기술의 이점을 극대화 하고 동시에 개인·그룹·조직·사회에 부정적인 영향을 미칠 가능성을 줄이기 위해 수립
- (주체 및 절차) NIST 주관으로 정부 기관·민간기업·학계·비영리단체·시민·AI 실무자 등 민관협력으로 정보제공요청(RFI)*, 3번의 워크숍, 2개의 초안 문서에 대한 공개 의견 수렴, 공개 포럼 등을 통해 수립
- * 정보제공요청(RFI, Request for information) : 정책·전략·프로젝트 기획 단계에서 전문가와 대중을 대상으로 필요한 정보를 공개적으로 요청하는 과정
- (내용) AI RMF는 조직의 크기와 형태에 상관없이 조직의 전체적인 위험관리 정책에 포함되어 AI 시스템의 전 주기에서 신뢰할 수 있는 AI 시스템 구현을 위한 핵심 기능의 위험관리 프로파일을 제시
- (적용대상) 모든 분야·규모의 기업·조직의 'AI 시스템'
- (적용주체 및 방식) 'AI 행위자'*가 제시된 항목에 따라 자발적으로 참고 및 점검
 - * 설계자·개발자·배포자·사용자, 고위 경영진이나 관리자 등
- (적용시점) AI 시스템의 설계, 개발, 활용, 테스트, 평가 등 모든 단계
- (핵심내용) 안전성, 책임·투명성 등 신뢰할 수 있는 AI 시스템의 7가지 특성을 제시하고, 이를 위한 조직의 핵심 기능을 4가지 영역(거버넌스, 매핑(위험 식별), 측정, 관리)에서 제시

- 생성형 AI와 저작권 보호 사이의 균형 마련을 위한 법적 근거 구체화 및 저작권자 권익 보호 정책 수립
- AI 학습 데이터의 '공정이용' 적용 범위와 창작자 보상 체계에 대한 미국 저작권청(USCO)의 공식 견해 정립
 - * 미국 저작권청은 생성형 AI가 원저작물의 스타일을 모방하여 창작자의 시장 가치를 훼손하는 '시장 희석화' 우려를 포함
- AI 생성 콘텐츠의 투명성 확보를 위한 디지털 워터마킹 기술 표준화 및 위·변조 방지를 위한 메타데이터 관리 체계 도입
- 데이터 활용 과정에서 민감 정보 유출을 막기 위해 동형암호 등 프라이버시 강화 기술 도입 및 표준화 추진
- 글로벌 공급망의 신뢰성 확보를 위하여 SBOM(소프트웨어 자재명세서) 제출 의무화 등 디지털 공급망 보안 체계 고도화
- 연방 정부 조달용 소프트웨어에 대해 SBOM 제출을 의무화하는 행정명령(EO 14028)을 시행하여 소프트웨어 투명성 제고

- NIST와 CISA(사이버보안 및 인프라 보안국) 주도로 SP 800-218 기반 소프트웨어 공급망 보안 프레임워크를 제정하여 국제 표준화 선도
- 오픈소스 소프트웨어의 취약점을 실시간으로 파악하고 관리하기 위한 자동화 플랫폼 구축 및 민간 산업계 확산 유도
- 공급망 전반의 제로 트러스트 아키텍처 적용을 통한 외부 침입 방어 및 내부 기술 유출 차단 고도화
- 네트워크 침해 시 자동으로 우회 경로를 생성하고 복구하는 자가 치유 네트워크 기술을 도입하여 회복탄력성 강화
- 개별 제품 단위를 넘어 연결된 모든 디지털 자산의 무결성을 상시 검증하는 인증 체계 및 세분화된 접근 제어 기술 도입
- 주요 기술 기업 주도의 취약점 관리 자동화 표준을 연합 보안 기준과 연계하여 디지털 생태계 전체의 보안 수준 향상
- 개별 제품 보안을 넘어 연결된 ‘소프트웨어 체인’ 전체의 무결성을 검증하는 플랫폼 기반의 보안 환경 조성 독려
- IBM, 마이크로소프트 등 자국 내 빅테크 기업들이 주도하는 SBOM 기반 취약점 관리 및 대응 자동화 기술의 시장 표준화 지원
- 민관공조 기반 단속체계 고도화와 해외 유통망 단절에 집중
 - 지식재산권 집행조정관(IPEC) 주도로 부처 간 공동 전략을 수립하고 국정 차원의 대응체계를 운영
 - 백악관은 지재권 보호 공동전략(Joint Strategic Plan)을 수립하여 연방기관의 역할과 목표를 일원화
 - 전략에는 위조상품 근절, 온라인 플랫폼 책임 강화, 공급망 내 정품추적 시스템 도입 등의 과제가 포함
 - 국토안보부 산하 IPR 조정센터를 중심으로 위조상품 단속을 통합적으로 추진하며 국경 단속을 강화
 - 미 세관(CBP)은 연간 13억 개 이상의 국제 우편물에 대해 검사를 시행하고 위조품 유통을 차단
 - 단속 대상에는 명품, 의약품, 산업재, 부품 등 고부가가치 제품군이 포함되며, 위험도 기반 선별검사를 운영
 - 해외 정책 파트너십을 기반으로 지재권 보호를 위한 다자간 협력을 강화하며 제3국 대응체계 수립 지원
 - 우선협상국과의 MOU 체결 및 현지 정부·세관 교육훈련을 통해 위조단속 역량 전파
 - 국제 민간기업과 협력해 블록체인, 디지털 인증 등 첨단기술 기반 위조방지 플랫폼을 공동 개발
- 지식재산의 경제적 가치를 극대화하고 핵심기술의 해외 유출을 방지하기 위한 법의 집행 및 제도적 지원 대폭 강화
 - 글로벌 지식재산 보호 규범 선도와 공정한 시장 경쟁 환경 조성을 위한 제도적 장치 및 국제 공조 체계 마련
 - 미국 상공회의소(GIPC) 주도의 국제 지식재산 지수 평가를 통해 자국 중심 IP보호 환경 우위를 유지하고 통상 압력 강화
 - 연방거래위원회(FTC)는 제약사가 ‘오렌지 북(FDA 특허 목록)’에 부적절한 특허를 등재하여 제네릭 진입을 지연시키는 행위에 대해 이의제기 및 규제 강화

- 2025년 기준 미국은 지식재산 지수 종합 1위를 유지하며 특허권, 영업비밀 보호 등 전 분야에서 압도적인 글로벌 우위 지속
- 영업비밀 및 핵심 산업기술 유출에 대하여 ‘간첩죄’ 적용을 검토하는 등 위반 행위에 대한 처벌 수위 상향으로 기술 주권 수호
- 경제스파이법(EEA)을 통해 국가 핵심기술 유출 시 최대 15년 징역 및 500만 달러 벌금을 부과하는 등 간첩죄 수준의 강력한 법적 억제력 확보
- 연방거래위원회는 제약 분야 등 주요 산업에서 특허권의 부당한 행사를 견제하고 시장 경쟁 환경을 조성하기 위한 이의제기 절차 강화
- 반도체, 이차전지 등 국가 핵심 산업 분야의 영업비밀 보호를 위해 FBI와 법무부 간의 전담 합동 수사 체계 고도화
- 국가방첩전략에 기술보호 항목이 포함되며, 민간과 협력한 산업보안 가이드라인이 전국적 확산 체계를 구축
- 국가방첩·보안센터(NCSC)는 핵심기술 보호 수칙, 내부자 위협 대응 매뉴얼 등 산업별 대응자료를 배포
- 기업은 이를 바탕으로 자율 보안체계를 수립하며, 연방계약기업에는 보안 인증(CMMC) 의무가 확대 적용
- 영업비밀보호법(DTSA)을 통해 민간기업이 연방법원에 직접 손해배상 소송을 제기할 수 있는 경로가 확보됨
- 2016년 제정된 DTSA는 민사소송 제기 절차를 명확히 하여 피해 기업의 실질적 구제 가능성을 높임
- 법원은 가처분, 손해배상, 반환명령 등 다양한 민사구제 수단을 통해 기술피해 회복을 지원

□ (EU) EU 디지털주권 확보 및 지식재산 보호체계 고도화를 위한 통합규제 거버넌스전략 추진

- 세계최초 인공지능법 시행 및 데이터가치 보호를 위한 지식재산 규제체계 확립
- 인공지능 기술의 위험성 기반 분류와 지식재산권 보호 간의 균형적 규제 프레임워크 마련
- 생성형 AI 모델의 훈련데이터 출처 공개를 의무화하여 저작권자의 권익 보호 및 알고리즘 투명성 제고
- AI 생성물의 권리 귀속 주체에 관한 법적 논의와 더불어 지재권 침해 방지를 위한 기술적 보호조치 구체화
- 고위험 AI 시스템에 대한 엄격한 준수 의무 부과를 통해 기술 오남용 방지 및 유럽형 AI 신뢰생태계 조성
- 데이터법 및 데이터 거버넌스법을 통한 산업데이터의 안전한 공유와 영업비밀 방어체계 고도화
- 보건, 에너지, 제조 등 10대 전략 분야의 데이터를 통합하는 ‘유럽 공통 데이터 공간(Common European Data Spaces)’을 구축하여 단일 데이터 시장 실현 가속화

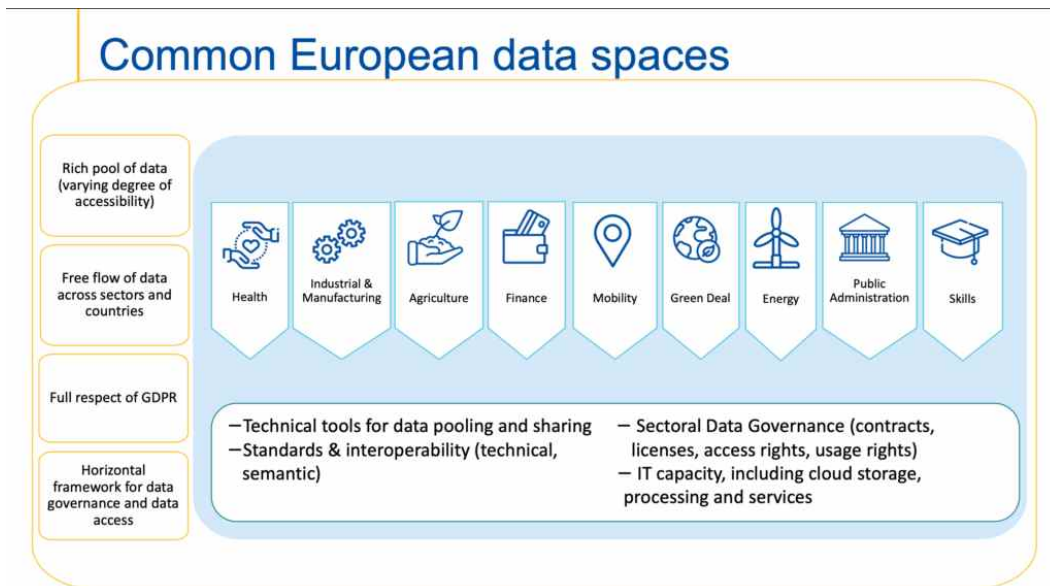


그림 2. 유럽 공통 데이터 공간

- 데이터 이동권 보장 과정에서 기업의 핵심기술 및 영업비밀이 부당하게 노출되지 않도록 하는 기술적·법적 방어권 보장 근거 마련
- 공정한 데이터시장 형성을 위해 데이터공유 계약 내 지식재산권 보호 독소 조항 배제 및 표준 가이드라인 보급
- 비개인 데이터의 역외 무단이전을 제한하여 유럽 내 생성데이터의 경제적 가치를 보호하고 디지털 주권 수호 기반 강화
- 사이버복원력법 및 EU-CyCLONe(EU사이버위기 연락기구) 중심의 디지털제품 보안성 강화 및 범국가 위기 대응체계 가동
 - 디지털제품의 설계 단계부터 보안성 확보를 의무화하여 역내 유통제품의 사이버보안 요건 상향
- EU 시장내 하드웨어 및 소프트웨어 제품에 대한 사이버보안 인증 및 CE마크 부착 의무화로 보안 수준 상향 평준화 유도
- 보안 취약점 발견 시 제조사의 보고의무 및 신속한 보안패치 배포를 통한 디지털 공급망 전체의 위협대응력 제고
- 제품 수명주기 전 과정에 걸친 보안 업데이트 제공 기간의 명시를 통해 소비자 보호 및 장기적 시스템 안정성 확보
- 중요 정보인프라 보호를 위한 NIS2(네트워크 및 정보보안에 관한 지침)의 본격 이행 및 핵심산업 분야에 대한 보안 통제력 확충
- 에너지, 교통, 금융 등 핵심 서비스 제공기관에 대한 보안 거버넌스 강화 및 강력한 감독체계 가동을 통한 복원력 확보
- 공급망 보안 강화를 위해 핵심 파트너사에 대한 정기적 보안 실태 점검 실시 및 위협 정보 공유 플랫폼 운영 활성화
- 국가간 대규모 사이버 위기 대응을 위한 'EU-CyCLONe'를 가동하여 범유럽 차원의 공동 대응역량 강화

	NIS2 20, 21조에서 명시한 주요 기업의 준수사항	IEC 62443 표준을 활용한 현재 대응방안
거버넌스와 프로세스	- 리스크 분석과 정보시스템 보안 정책 - 사이버 리스크 관리의 효과성 평가 - 비즈니스 연속성 확보	- 정책과 절차 수립 - 리스크 관리 체계 도입과 개선 - 재난 복구 대비와 비즈니스 연속성 확보 - 보안 요구사항 이해 - 국제표준 기준 네트워크 아키텍처
조직과 인력	- 사이버 리스크 관리 방법에 대한 최고 경영진의 승인과 감독 - 컴퓨터 바이러스 예방 및 사이버 보안 교육 - 공급망 보안	- 역할과 책임 상세 정의 - 보안 인식 개선과 교육 진행 - 협력업체 보안
기술과 보안역량	- 사고처리 - 암호학과 암호화 - 취약점 처리와 투명한 공개 - 자산 관리와 접근 통제 정책 - 안전한 통신 시스템과 다중 인증 사용	- 자산 식별과 정보 최신화 - 네트워크 분할과 분리 - 업데이트 및 취약점 관리 - 원격 접근 보안

그림 3. NIS2 시행에 따른 주요사항

- 디지털제품여권(DPP) 도입 및 에코디자인 규정 기반의 글로벌 공급망 투명성 규제 확대
 - 지속 가능한 제품을 위한 에코 디자인 규정(ESPR) 이행을 통한 제품 전 생애주기 데이터 투명성 확보
 - 제품의 내구성, 수리가능성, 재활용률 및 탄소발자국 정보를 담은 디지털제품여권(DPP) 도입을 통해 글로벌 공급망 이력 관리 강제
 - 2027년 배터리 분야 의무화를 시작으로 섬유, 철강, 알루미늄 등 주요 산업군에 순차적으로 DPP 적용을 확대하여 역외 기업의 규제준수 요구

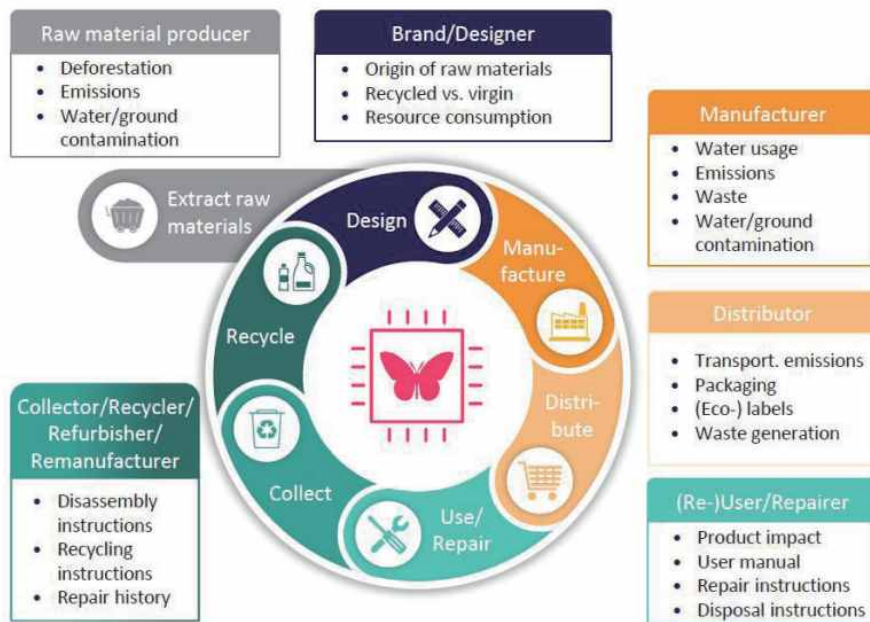


그림 4. DPP에 수록되는 공급단계별 정보

- 공급망 실사 지침을 통한 기업의 사회적 책임 및 지식재산권 보호 의무 통합 관리 체계 구축
 - 글로벌 가치사슬 전 과정에서의 인권·환경 침해 여부 모니터링 시 데이터 위변조 방지를 위한 블록체인 기반의 데이터 무결성 검증 기술 도입 지원
 - 역내 유통제품의 원재료 수급처부터 폐기단계까지의 정보를 디지털화하여 투명하게 공개함으로써 모조품 유입 차단 및 정품 인증 효과 극대화

- 법령·기구·행동계획 중심의 범유럽 통합 체계 구축을 통한 위조방지 대응 추진
 - EU 집행위는 지재권 보호·집행 행동계획을 수립하고 예방·집행·협력·교육 등 4대 전략 축을 기반으로 추진
 - ‘IP Action Plan’을 통해 지식재산권 침해 대응체계 일원화 및 단속 인프라 강화
 - 위조 상품 유통 차단, 지재권 수호 인식 제고, 국제 공급망 상 보호조치 이행이 주요 추진 방향
 - EUIPO 산하 위조 및 해적행위 관측소(OEIPR)를 통해 데이터 기반 정책 수립과 민관 협력체계 구축
 - OEIPR는 EU 내 위조·해적 제품 통계를 집계 및 분석, 기술별 대응 우선순위를 제시
 - 민간 기업, 세관, 경찰 등과 협력하여 위조 대응 기술 가이드라인(예: Anti-Counterfeiting Technology Guide) 제공
 - 형사사법 협력을 기반으로 회원국 간 단속·처벌 수단의 균형화 및 법적 조화를 유도
 - 2014/62/EU 지침에 따라 화폐·상품 위조 행위에 대한 형사처벌 기준 마련
 - 위조방지 관련 형사적 책임 범위를 통일시켜 역내 범집행 격차를 최소화
 - 제3국과의 IP 공조 사업(AfrIPI, ARISE+, IP Key 등)을 통해 위조 근절 역량 전파 및 국제공조 네트워크를 운영
 - 개발도상국의 지식재산 제도 개선과 위조방지 기술 보급을 지원
 - 공적개발원조(ODA)와 연계하여 글로벌 위조 유통 경로 단절 목적의 협력 강화
- 통합특허제도 안착 및 지식재산권 보호를 위한 실질적 집행력 강화
 - 유럽 통합특허 및 통합 특허법원(UPC) 시스템 운용을 통한 지재권 보호 효율성 및 사법적 일관성 극대화
 - 단일출원으로 EU 가입국 전역에서 특허 효력을 일괄 보장하여 행정비용 절감 및 역내 혁신기업 지재권확보 동력 지원
 - 통합 특허법원의 전문성 강화를 통해 국경을 넘는 특허분쟁에 대한 신속 판결 체계를 확립하여 사법 리스크 획기적 감소 도모
 - 제도 시행 초기(7년) 동안 기존 유럽 특허(EP)에 대해 통합법원 관할을 배제할 수 있는 ‘옵트아웃(Opt-out)’ 제도를 운영하여 기업의 선택권 및 사법적 적응 기간 보장
 - 소송절차의 디지털화 및 표준화를 통해 중소기업의 사법 접근성을 개선하고 유럽 내 특허분쟁 해결의 중심지 역할수행
 - 지식재산권 침해 대응을 위한 IP Toolbox(IP관리 및 보호를 위한 디지털 데이터베이스) 운용 및 위조상품 유통차단을 위한 민관협력체계 고도화
 - 온라인 마켓플레이스 내 지재권 침해 적발 및 차단 절차 간소화를 위한 민관협력 프레임워크 구축 및 시장 질서 확립
 - 중소기업의 글로벌 지재권 분쟁대응력 제고를 위한 맞춤형 법률컨설팅 및 SME Fund 운영 범위 확대
 - EUIPO의 ‘위조 방지 기술 가이드(Technology Guide)’를 정기 발간하여 지재권 침해위험을 경고하고 역외 유입 제품에 대한 통관감시 강화

- 전략 기술 분야를 중심으로 산업기밀 보호를 ‘유럽 전략 자율성’의 요소로 간주하고, 관련 규제·지원 연계를 강화
- 반도체, 배터리, AI 등 핵심 기술에 대해 IP 보호와 병행하여 EU 산업기반의 자율성과 독립성 확보 목표
- 국가 안보 목적의 기술 유출 규제 강화 움직임과도 연결되며, 대외 투자심사와 수출통제 제도와의 연계 강화

□ (일본) 경제 안보 강화 및 첨단기술 유출 방지를 위한 지식재산·사이버보안 전략 추진

- 경제안전보장추진법(ESPA) 기반의 특정 중요기술 보호 및 공급망 안정성 확보체계 가동
- 특정 중요기술에 대한 연구개발 지원과 특허출원 비공개 제도를 통한 핵심기술 역외 유출 방지 장치 마련
- 국가안보에 중대한 영향을 미치는 첨단기술 특허의 경우 공개를 유예하고 비밀유지의무를 부과하여 기술주권 수호 기반 확립
- 부정경쟁방지법 개정을 통해 영업비밀 국외 유출 시 법인에 최대 10억 엔의 벌금을 부과하는 등 처벌 수위를 대폭 상향하여 억지력 확보
- 반도체, 축전지, 중요 광물 등 특정 주요 물자의 안정적 수급을 위한 공급망 강인화 정책 추진 및 기업 대상 보안감사 실효성 제고
- 비공개 대상으로 지정된 기술 보유기업에 대해 공개 유예에 따른 기술료 손실 보상금 지급 기준을 마련하고 내부 보안시설 구축 비용을 지원하여 민간의 정책 수용성 제고

1	공급망 강인화	반도체, 자동차용 축전지 등 전략물자의 국내 생산 지원. 지원받은 공장에서 생산한 제품은 국내 공급 우선
2	기간 인프라의 안전확보	사이버 공격에 대비해 통신, 에너지, 금융 등 기간 인프라 설비 도입할 때 정부가 사전 심사
3	첨단기술의 개발지원	인공지능, 양자컴퓨터 기술 등 ‘게임체인저’가 될 수 있는 첨단기술을 개발하는 기업이나 대학에 자금 지원. 대신 정보 관리를 철저히 하고 해외 반출을 금지
4	특허의 공개제한	군사 목적 전용 가능한 기술은 일정 기간 후에도 공개하지 않도록 하고 대신 정부가 자금 지원

그림 5. 일본 경제안전보장추진법안 주요내용

- 기밀 정보 취급 권한을 제한하는 보안 클리어런스 제도 도입을 통한 인적 보안관리 및 국제 협력 신뢰성 고도화
- 민간 전문가 및 공무원이 국가 기밀 정보에 접근 시 신원조사를 의무화하여 기술 스파이 활동 차단 및 국제 공동연구 참여 자격 확보
- 첨단분야 인력 이동 시 발생 가능한 영업비밀 침해 사례를 사전 모니터링하고 기업의 자율적 내부 통제 시스템 구축 가이드라인 배포

- 경제안전 보장 기금을 통한 특정 중요 기술 육성 및 연구 성과 보안관리 체계의 실무적 집행력 강화
- AI, 양자, 우주 및 ‘Quantum Secure Japan 이니셔티브’를 통한 양자내성암호(PQC) 전환 등 국가 전략적 가치가 높은 기술분야를 선정하여 민관협력 연구기관 중심의 대규모 R&D 자금을 투입하고 연구 전과정의 기술유출방지 가이드라인 적용
- 반도체, 이차전지 등 11대 특정 중요물자의 안정적 수급을 위해 기업별 공급망 상세 조사 및 설비 투자 지원 시 보안 솔루션 도입을 의무화하는 기술보호 연계 강화
- 제조업 강점을 살려 공장 및 산업 제어 시스템(OT)과 가상 공간을 연계한 ‘산업·가상융합(CPS) 보안’ 기술개발에 집중”
- AI 및 디지털전환 가속화에 대응한 지식재산권 보호 규범 정비 및 글로벌 표준화 주도
- 생성형 AI 관련 저작권 침해판단 기준 구체화 및 데이터 활용 활성화를 위한 제도적 유연성 확보
- ‘지식재산 전략 프로그램 2024/2025’를 통해 AI 기술 발전과 창작자 보호 간의 균형을 맞춘 유연한 저작권 해석 및 규범 정립
- AI 학습 단계에서의 저작물 이용에 관한 허용범위와 영리 목적의 대량 크롤링에 대한 권리자 보호 방안을 담은 지침 정비 추진
- AI 생성물의 특허권 인정 여부에 대한 국제 논의에 적극 참여하고 일본 특허청(JPO) 중심의 고품질 심사 및 AI 대응 로드맵 실행

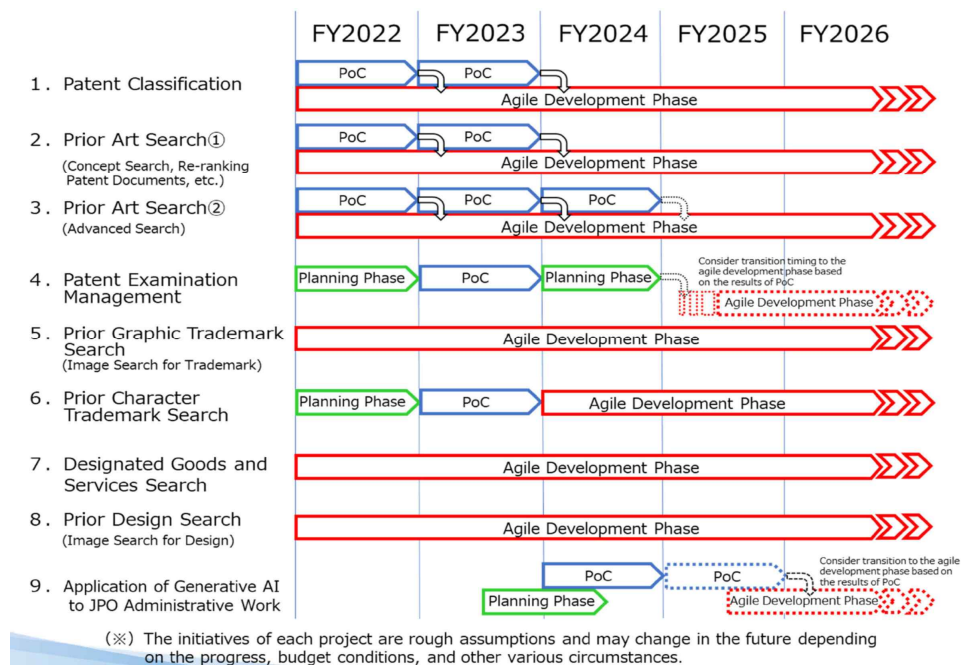


그림 6. AI대응 로드맵

- 클라우드 보안 인증 제도(ISMAP) 고도화 및 공공 부문 디지털 인프라의 사이버 복원력 강화
- 침해사고 발생 전 공격자 서버에 침투하여 위협요인을 사전에 탐지하고 무력화하는 선제적 사이버 방어 법제화를 통해 핵심기술 탈취 시도에 대한 방어역량 확보
- 정부 조달 시 클라우드 서비스의 보안성을 사전에 검증하는 ISMAP 대상 확대 및 민간 금융·의료 분야로의 자율적 확산 유도

- 사이버보안 전략본부 주도의 중요 인프라 방호지침 개정 및 랜섬웨어 공격 대비 백업시스템 의무화 등 실전적 대응 역량 확충
- 전력, 금융 등 14대 핵심사회기반시설 운영기관이 업무시스템을 조달할 때 보안성이 검증된 장비만 사용하도록 강제하는 공급망 보안관리 지침적용
- 중소기업 해외진출 지원 및 위조상품 대응을 위한 지식재산 활용·집행 시스템 고도화
 - 성장지원형 지식재산 선순환 목표 아래 스타트업 및 중소기업의 글로벌 지재권 전략수립 컨설팅 확대
 - 해외 특허출원 비용 지원 및 현지 지재권 분쟁 해결을 위한 국가별 보호가이드북 보급을 통해 수출기업의 기술경쟁력 강화지원
 - 영업비밀 보호를 위한 비밀정보 관리핸드북 개정 및 기술유출 피해기업에 대한 원스톱 상담서비스 체계의 전국적 확산
 - AI 기반 위조상품 적발 시스템 도입 및 국경조치 강화를 통한 역외 침해물품 유입차단 실효성 제고
 - 디지털 거래 플랫폼 내 위조품 유통 차단을 위한 제도적 환경을 정비하고, 재무성 관세국과 특허청 간 협력을 통해 AI 이미지 분석기술을 활용한 위조품 실시간 판별 및 디지털 단속성과 극대화
 - 세관, 경찰, 특허청이 공조하여 해외에서 유입되는 위조품을 국경 단계에서 차단하고, 정품 인증을 위한 독자적인 홀로그램 및 IoT 추적 시스템 보급
 - 디지털 거래 플랫폼에서의 위조품 유통을 막기 위해 상표법 및 부정경쟁방지법을 개정하여 플랫폼 사업자의 책임 강화 및 외국 사업자 단속 근거 마련
 - 주요 교역국과의 지재권 보호 협의체 운영을 통해 위조상품 제조 거점에 대한 합동단속 및 사범공조 체계의 실효성 확보
 - * 한·미·일 특허청장 회의(2024.12) 신설 등을 통해 3국 간 첨단 기술 특허 심사 협력 및 지식재산 보호 공조 체계 격상

□ (중국) 지식재산 강국건설 및 국가 안보 중심의 첨단기술 보호 거버넌스 강화전략 추진

- 2026년 신규 지식재산 규제 시행을 통한 특허·상표 행정의 양적팽창에서 질적 고도화로의 패러다임 전환
 - 특허 심사지침 전면 개편 및 XML 기반 전자출원 의무화를 통한 심사 속도와 정확성의 획기적 개선 도모
 - 2026년부터 모든 특허출원서의 XML 형식제출을 강제하여 데이터 활용도를 높이고 심사 주기를 15개월 이내로 단축하는 고효율 행정 체계 구축
 - 전세계 특허출원량 1위의 양적성장을 넘어 인공지능 및 빅데이터 기반의 고품질 심사시스템을 도입하여 원천기술 보호의 실효성 확보
 - AI, 빅데이터, 바이오 등 신산업 분야의 고품질 특허 확보를 위해 심사 기준이 대폭 수정
 - 기존 알고리즘 관련 기준을 ‘인공지능 등과 관련된 특허 출원 심사 관련 규정’으로 변경하여 AI 관련 발명에 대한 심사 기준을 명확히 제시
 - 인공지능과 관련된 특허 출원 심사 기준에 ‘필요한 경우 명세서(說明書)의 내용을 심사해야 한다’는 표현을 추가하여 심사의 정확성을 높임
 - 법규 위반 및 사회 도덕 위반 심사 사례에 ‘빅데이터 기반의 쇼핑몰 내 매트릭스 판매 보조 시스템’, ‘무인 자율주행 차량의 긴급 의사결정 모델 구축 방법’을 추가하여 AI 기술의 윤리적 측면까지 고려한

심사 기준 제시

- 상표 행정의 무게추를 등록 중심에서 사용 중심으로 이동시켜 부정한 목적의 상표출원 및 매복 행위 근절 강화
 - 상표 등록 후 실질적 사용 여부에 대한 감사를 강화하고 미사용 상표에 대한 직권취소 절차를 간소화하여 시장 질서의 선진화 도모
 - 악의적 상표선점 행위에 대한 처벌 수위를 상향하고 지식재산권 침해에 대한 징벌적 손해배상 제도를 실무적으로 엄격히 적용
 - * 공안부 주도의 ‘쿤룬(Kunlun) 2024’ 특별 행동을 통해 지재산 침해 범죄를 집중 단속하고, 약 4만 4천 건의 행정 위법 사건을 처리하는 등 집행력 과시
 - 데이터 안보법 및 반간첩법 기반의 핵심기술 역외 유출 방지와 국가 주도의 기술 보안 통제력 극대화
 - 국가 비밀지정 범위를 첨단 AI 및 핵심 전략기술로 확대하여 국외 유출 시 형사 처벌을 강화하는 기술 봉쇄 전략실행
 - 딥시크 등 독자적 AI 알고리즘 및 핵심 아키텍처를 국가 비밀로 지정하여 해외 협력이나 인력 이동 시 사전 승인 절차를 엄격히 통제
 - * 기업이 기술을 수출하거나 민감 데이터를 해외로 이전할 때 정부의 ‘기술 보안 평가’를 의무적으로 받도록 하여 핵심 기술의 역외 유출을 원천 차단
 - 국가 핵심기술 보유 기관에 대한 보안 실태 점검을 정례화하고 기술 유출 사고 발생 시 기업 책임자의 연대책임을 강화하는 법적 근거 마련
 - * 간첩 행위의 정의를 ‘국가 안보 및 이익에 관련된 문건·데이터·자료’의 취득으로 대폭 확대하여 기술 유출 처벌 기반 강화
 - 국가 비밀로 분류되지 않더라도 유출 시 부정적 영향을 미칠 수 있는 정보를 ‘업무 비밀’로 관리하여 규제
 - 데이터 안보법 기반의 중요 데이터 역외 이전 안전 평가 제도 고도화 및 데이터 주권 수호를 위한 규제 장벽 강화
 - 산업별 중요데이터의 분류 기준을 세분화하여 해외서버로의 전송 시 국가인터넷정보판공실(CAC)의 사전안전성 평가통과 의무화
 - 알고리즘 추천 서비스에 대한 등록제를 강화하여 플랫폼 기업의 데이터 운용 투명성을 확보하고 서방 국가의 데이터접근에 대한 기술적 방어선 구축
- 수출통제 및 블랙리스트 제도를 활용한 글로벌 공급망 내의 기술패권 대응 및 대외 보복 수단 확보
 - 수출 통제법과 신뢰할 수 없는 기업 리스트 연계를 통한 전략물자 및 첨단기술의 국외 반출 통제강화
 - 희토류 등 자원 무기화와 연계하여 핵심 소재의 가공 기술 및 관련 설비의 수출금지 목록을 최신화하고 위반기업에 대한 제재 조치 단행
 - 미국의 수출규제에 대응하여 자국기업 보호를 위한 반외국제재법 활용도를 높이고 글로벌 공급망 내에서의 중국산 기술점유율 수호정책 추진
 - 지식재산권 보호를 명분으로 한 표준특허(SEP) 전략 및 국제표준화 기구 내의 영향력 확대를 통한 기술굴기 완성

- 5G·6G 및 자율주행 등 차세대 통신 분야에서 자국 기업 보유 표준특허 비중을 높이고 국제표준 제정과정에서 중국제안 기술채택 유도
- 표준특허 허용 과정에서 공정 거절 행위에 대한 규제 가이드라인을 수립하여 글로벌 특허분쟁 시 자국 기업에 유리한 사법적 판단 근거 마련
- 전 세계 위조상품의 주요 생산지라는 국제적 비판에 대응하기 위해 전자상거래법을 통해 알리바바, 징둥 등 플랫폼 사업자의 모니터링 및 삭제 의무를 법제화
- 주요 플랫폼 기업들은 블록체인 기반의 추적 시스템과 스마트 패키징 기술을 도입하여 유통 과정에서 위조품 혼입을 차단하고 소비자 신뢰 회복 시도

2 국내정책 동향

□ 국가첨단전략산업의 기술주권 수호 및 K-브랜드 가치보호를 위한 범부처 협력체계 강화

- 반도체·이차전지 등 국가첨단전략산업의 혁신생태계 조성 및 기술역량 강화를 위한 범부처 통합지원
 - 국가첨단전략산업 특별법에 근거하여 첨단 전략기술의 지정 범위를 81개 이상으로 확대하고 기술지정 수요조사와 연계한 적기 보호 체계 가동
 - 산업통상자원부 주관으로 관계중앙행정기관과 협의하여 해외인수합병(M&A) 심사절차를 강화함으로써 외국인에 의한 전략기술 무단 반출 사전 차단
 - * 산업부 장관 소속 산업기술보호전문위원회 산하에 ‘M&A 전문위원회’를 설치하여, 국가핵심기술 보유 기업의 해외 M&A 시 기술 유출 가능성과 안보 영향을 더욱 정밀하게 심의
 - * 기업의 신청이 없더라도 산업부 장관이 직접 특정 기술이 국가핵심기술에 해당하는지 판정하고, 관련 기업에 해외 M&A 절차를 밟도록 통지할 수 있는 권한이 강화
 - 2026년 시행되는 신규 연구개발 지원정책과 연계하여 소기업 및 중기업의 연구전담요원 확보기준을 정비하고 첨단기술 연구시설 확충을 위한 재정지원 확대
 - 전략산업 특화단지 지정 및 전문인력 양성·보호 정책을 통해 기술개발부터 산업화까지 이어지는 전주기적 보호장벽 구축
 - 안보상 우려가 있는 외국인 연구자에 대한 비자 심사 강화 및 핵심인력의 해외 이직 방지를 위한 이직관리계약 실효성 제고 방안 마련
 - * 산업통상자원부와 법무부는 국가 핵심기술 분야 연구소·대학에 진학하거나 취업하려는 외국인에 대해 비자 발급 전 안보 심사를 강화
 - 국가 첨단전략기술 보유기관의 수출심사 부담 완화를 위한 제도 정비와 병행하여 사각지대 해소를 위한 상시 기술심의 체계 고도화
- K-브랜드 및 핵심수출 품목의 글로벌 브랜드 가치 수호를 위한 범부처·민관합동 위조상품 대응 협력
 - 특허청(現지재처), 산업부, 중기부, 농림부, 해수부, 외교부 등이 참여하는 ‘위조화장품 대응 관계기관 협의회’ 가동을 통한 범부처 원팀 대응
 - K-브랜드 관련 11개 업종별 협·단체가 참여하는 ‘K-브랜드 민관협의회’를 통해 해외 온라인 플랫폼 내 유통되는 K-브랜드 위조상품 실태를 실시간 모니터링하고 단속정보 공유

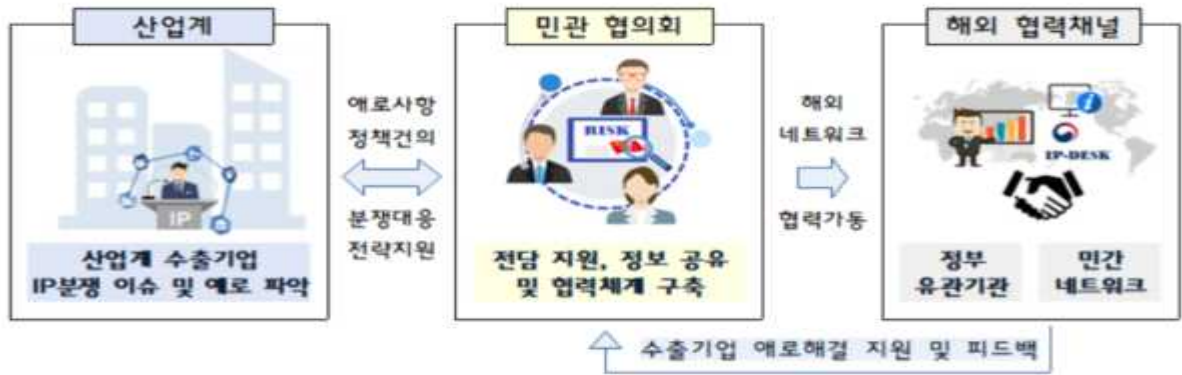


그림 7. K-브랜드 위조상품 민관 공동대응 협의회

- 24시간 실시간 AI 모니터링 시스템 기반의 위조상품 유통차단 및 K-브랜드 보호포털(한국지식재산보호원)을 통한 전방위적 피해구제 지원
- 해외 주요 전자상거래 플랫폼 및 SNS 내 K-브랜드 위조상품 게시물을 자동 탐지·차단하는 지원사업의 지원범위와 예산규모 확대
- 정품과 위조상품의 식별 및 유통 이력 추적을 위한 위조방지 기술 도입 지원을 강화하여 우리 기업의 브랜드 신뢰도와 글로벌 시장경쟁력 확보

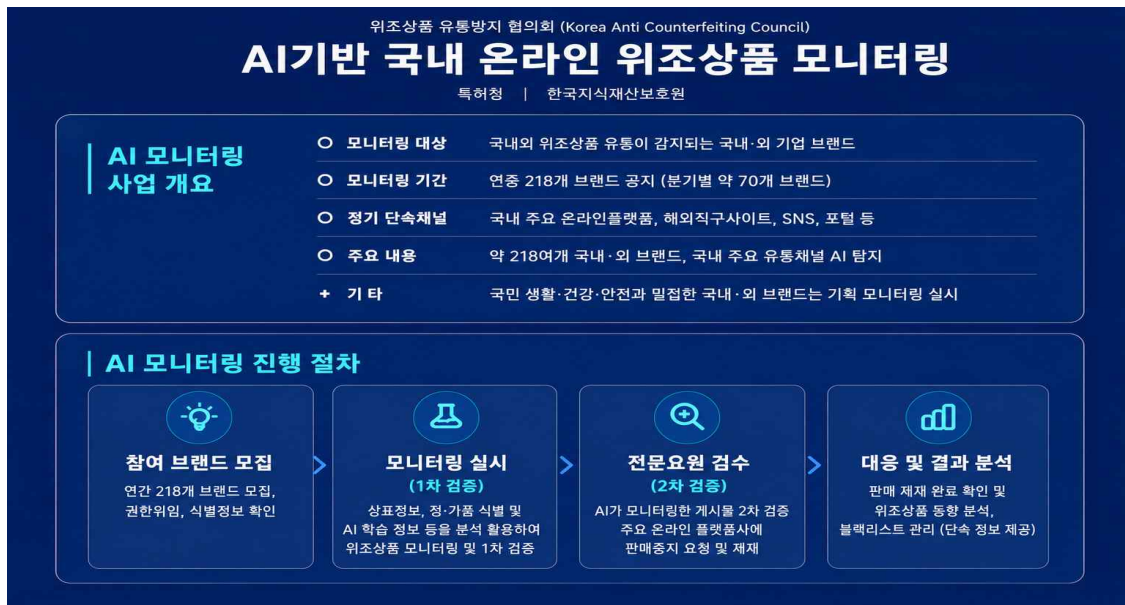


그림 8. AI기반 국내 온라인 위조상품 모니터링 사업개요

□ 산업기술 유출방지 및 제도적 실효성 제고를 통한 국가 기술안보 확립

- 국가핵심기술 보호를 위한 ‘산업기술보호법’ 및 ‘부정경쟁방지법’의 처벌규정 대폭 강화
 - 기술 유출 범죄에 대한 대법원의 양형 기준을 상향하고, 징벌적 손해배상 제도를 확대하여 범죄 억지력을 실질적으로 확보
 - (양형기준 상향) 국가핵심기술의 국외 유출 시 최대 징역 18년(기존 9년 → 15년, 가중 시 18년)까지 선고가 가능하도록 양형 기준을 대폭 강화
 - (징벌적 배상) 고의적인 영업비밀 및 특허권 침해, 아이디어 탈취 행위에 대한 징벌적 손해배상 한도를

손해액의 3배에서 5배로 상향하여 피해 구제 실효성 제고

- (브로커 처벌) 침해행위를 알선하거나 중개하는 ‘기술 유출 브로커’에 대한 형사처벌 규정을 신설하고, 법인에 대한 벌금형 상한을 행위자 벌금의 3배 강화

○ 제5차 산업기술 유출방지 및 보호 종합계획(2025-2027) 이행을 통한 예방 및 신속대응 체계 구축

- 국가핵심기술 유출 시 최대 18년형 선고 및 초범 감경조항 삭제를 골자로 하는 강화된 대법원 양형 기준의 엄격한 적용
- 산업기술보호법 개정을 통해 기술유출 행위에 대한 징벌적 손해배상 한도를 상향하고 영업비밀 유출 시 형사처벌 수위를 간첩죄 수준으로 격상
- 반도체·바이오·조선 등 국가핵심기술 보유기관에 대한 보안실태 점검을 정례화하고 기술 유출 사고 발생 시 기업 책임자의 관리 책임 명문화

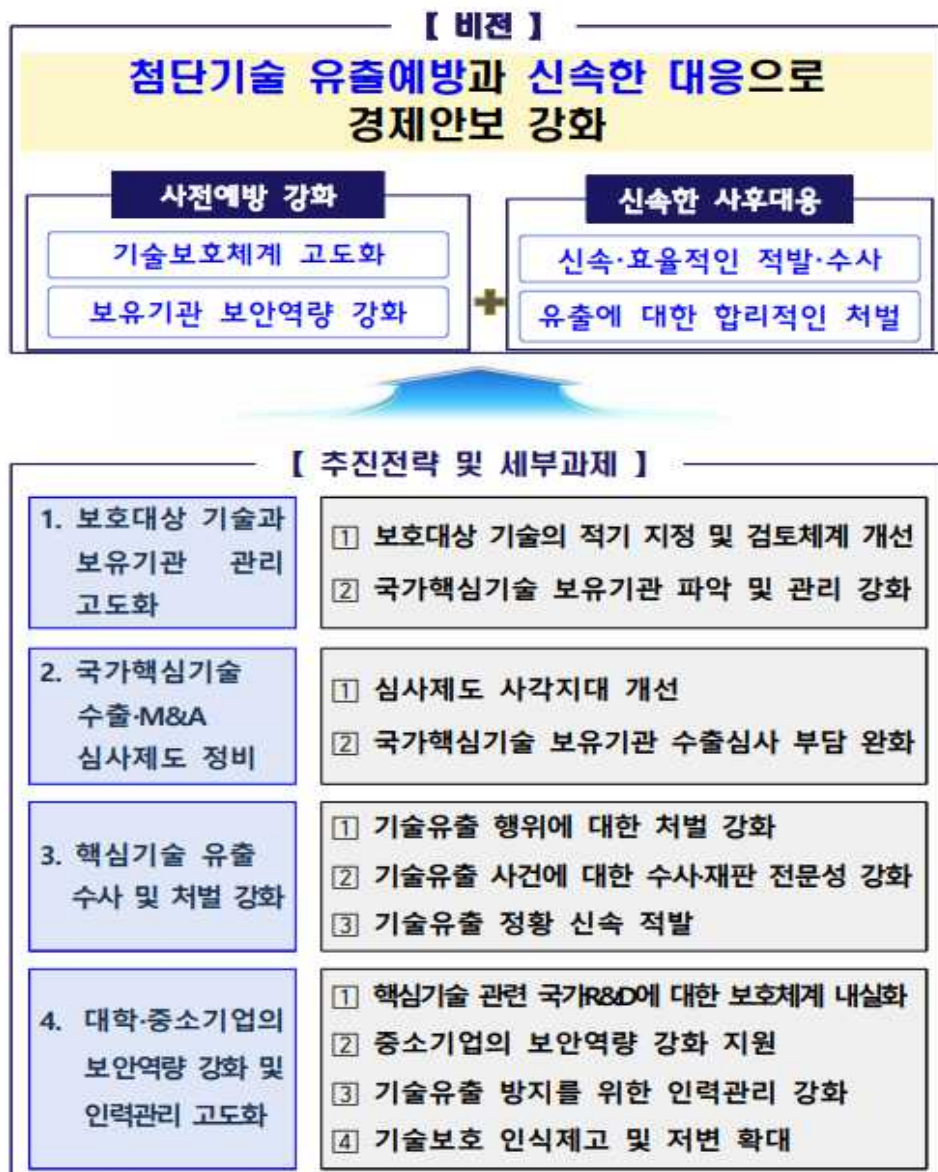


그림 9. 제5차 산업기술 유출방지 및 보호 종합계획 비전 및 추진과제

- 특허청이 국가정보원, 국방부 등과 함께 방첩기관으로 공식 지정(2024.4)되었으며, 산업 스파이 정보

수집 및 분석 역량을 강화하고 기술 유출 수사의 전문성 확보

- 특허청 산하 기술디자인특별사법경찰과 디지털 포렌식 지원 조직을 확충하여, 고도의 기술적 이해가 필요한 첨단기술 유출 사건에 대한 전담 수사 체계 고도화
 - 범정부 기술유출 합동대응단을 통한 수사기관 간 정보공유 플랫폼 고도화 및 디지털 증거분석 기반의 수사역량 결집
 - 2023년 발표된 ‘산업기술유출 방지 종합대책’에 따라 첨단산업 인수합병 심사 강화, 해외인재 채용 통제, 보안이행 점검 체계 구축
 - 국가정보원 산업기밀보호센터와 검·경 전담수사팀 간의 유기적 협력을 통해 기술스파이 징후를 선제적으로 포착하고 신속한 초동수사 전개
 - 국가 R&D 과제 수행기업에 대해서는 연구성과 유출 방지를 위한 성과물 등록·열람 통제·비인가 반출 차단 등 기준 신설
 - 국정원-산업부-법무부-과기부 등 합동 전담팀을 운영하여 해외투자, 기술이전 계약, 인수합병 시 기술위험 사전 검토 시행
 - 국가핵심기술 보유기관의 클라우드 서비스 이용 가이드라인 마련 및 공공·민간 영역의 데이터 보안 거버넌스 통합 관리 체계 정착
- 중소기업 및 대학의 보안 역량 강화를 위한 상생형 보안 인프라 구축 및 인력 관리 고도화
- 중기부 주도의 상생형 기술유출방지 시스템 구축 사업을 통해 대기업의 보안 노하우를 협력사에 전수하는 민관협력 모델 확산
 - 보안 인프라가 취약한 중소기업을 대상으로 물리적·기술적 보안 시스템 구축 비용을 지원하고, 핵심 기술의 선제적 방어를 유도
 - 문서중앙화, 내부정보유출방지(DLP), 보안 방화벽 등 핵심 보안 솔루션 도입 비용의 최대 80%를 정부와 대기업 기금으로 지원
 - 기술 임치제도 활용기업에 대한 우대점수 부여 및 기술 자료 보관기관의 보안성 강화를 통해 중소기업 핵심기술의 입증 및 보호 기반 확충
 - 대학 및 연구기관 대상의 국가 R&D 보호체계 내실화 및 산업보안관리사 자격제도 개편을 통한 전문인력 저변확대
 - 연구개발 전 과정의 보안관리 실태점검 가이드라인 보급 및 연구 성과의 무단 유출 방지를 위한 학계 맞춤형 보안교육 프로그램 운영
 - 산업보안관리사 자격의 국가기술자격 전환 추진 및 과정평가형 제도 도입을 통해 실무 중심의 기술보호 전문인력 양성체계 고도화

□ 차세대 보안 인프라 및 지능형 사이버방어 체계 구축을 통한 디지털 복원력 강화

- 양자컴퓨팅 위협 대응을 위한 양자내성암호(PQC) 전환 및 국가 암호체계 현대화
- 2026년 국가 행정망 및 중요정보 인프라 대상 양자내성암호 전면 도입을 위한 단계별 이행 로드맵 가속화
 - 국가 암호모듈 검증기준(KCMVP)에 PQC 알고리즘을 반영하고 하이브리드 암호방식을 통한 과도기적

보안 공백 최소화 및 표준화 선도

- 현재 데이터를 탈취한 후 미래에 해독하려는 보안 위협에 대비하여 공공·금융 등 민감정보 취급기관의 데이터 암호화 수준 향상
- 제로트러스트(Zero Trust) 보안모델의 범정부 확산 및 지능형 사이버방어(Active Cyber Defense) 역량 확보
- ‘제로 트러스트(Zero Trust)’ 보안 모델 도입을 가속화하고, AI 모델의 오염 및 유출을 방지하는 ‘AI 특화 사이버보안 기술’ 개발 추진
- 단일 경계보안의 한계를 극복하기 위해 모든 접근에 대한 상시 검증 및 권한제어 체계를 구축하여 내부자에 의한 정보유출 사전 차단
- 인공지능 기반의 지능형 보안관제 시스템을 고도화하여 신종 사이버위협에 대한 실시간 탐지 및 자가치유 네트워크 기술 확보

□ 지식재산 행정 혁신 및 글로벌 규범 선도를 통한 지식재산 강국 입지 강화

- 2025년 국제지식재산지수 세계 10위 안착을 위한 글로벌 IP 리더십 강화 및 행정 고도화
- 글로벌 IP5(한·미·일·중·유럽) 청장회의 주도를 통한 AI 발명자성 인정 및 국제 양도제도 도입 등 글로벌 지재권 질서 재편 기여
- 2025년 9월 한-아세안 청장회의를 통한 지식재산 교육협력 확대 및 한국형 지재권 행정시스템의 글로벌 표준화 추진
- 생성형 AI 학습데이터의 정당한 이용규범 마련을 위해 저작물 활용 시 보상 체계와 투명성 확보를 위한 가이드라인 수립 완료
- 지식재산 가치평가 기반의 IP 금융 활성화 및 중소기업의 글로벌 지재권 분쟁대응을 위한 전방위 지원
- IP 담보대출 회수지원기구 예산 확대를 통한 금융 생태계 활성화 및 해외지재권보호센터(IP-DESK)의 맞춤형 법률컨설팅 강화
- 온라인 마켓플레이스 내 위조상품 단속을 위한 AI 기술 적용 확대 및 K-브랜드 가치수호를 위한 범부처 통합단속 체계 정착

제2절 시장 동향

□ 글로벌 규제강화와 지능화 되고 있는 위조 상품 시장의 확대에 의해 위조방지 기술 시장은 급격한 성장세를 보이고 있음

- 위조상품유통은 개별기업의 문제를 넘어 국가경쟁력의 위협요인으로 대두
- 세계 무역액의 약 2.3%에 달하는 위조 및 불법복제 상품의 확산은 합법적 기업의 혁신 의지를 저해하고 국가 세수를 감소시키는 경제적 침해 범죄로 정의
- * '21년 기준 위조 및 불법 복제물 무역은 전 세계 무역량의 최대 2.3%(Mapping Global Trade in Fakes 2025(OECD/EUIPO(2025)))
- 경제협력개발기구(OECD) 분석에 의하면 위조 상품은 소비자 안전 위협을 넘어 글로벌 공급망의

신뢰 구조를 근본적으로 훼손하는 고도화된 위협으로 진화

- 유럽연합(EU)의 경우 수입액의 최대 4.7%*가 위조 상품으로 추산되며 이는 지식재산 보호 패러다임이 사후 대응에서 사전 예방으로 전환되는 결정적 계기

* '21년 기준 유럽연합(EU) 내 위조품의 비중은 전체 수입액의 최대 4.7%(Mapping Global Trade in Fakes 2025(OECD/EUIPO(2025)))

- 가짜 의약품이나 불량 부품의 유통은 단순한 경제적 손실을 초과하여 공공의 안전과 생명을 직접적으로 위협하는 심각한 사회적 비용을 발생
- 디지털 전환 가속화와 글로벌 인력 유동성 증가는 전통적 보안 체계의 한계를 노출하며 실시간 모니터링 기반의 신규 보호 전략 수립을 요구



그림 10. 글로벌 위조시장

- 글로벌 위조방지 및 산업보안 시장은 규제 강화, 기술 진화, 사이버 위협 증가에 따라 급격한 성장세를 보이고 있음

- 글로벌 위조방지 패키징 시장은 2025년 2,040.8*억 달러 규모에서 2033년 4,282.8억 달러로 확대되며 연평균 9.4%의 견고한 성장세를 기록

* Anti-counterfeit Packaging Market(2026-2033), Grand View Research

- 의약품, 식품, 사치품 등 소비자 안전과 직결되거나 브랜드 가치가 높은 산업군을 중심으로 정품 인증 기술 수요 급격한 증대
- 제약 및 소비재 분야의 브랜드 보호 솔루션 수요 급증이 시장 확대를 견인하며 특히 북미 지역이 세계 시장의 43.21%를 점유하며 기술 주도권 확보
- 이커머스 시장의 폭발적 성장은 온라인 플랫폼을 통한 위조품 유통 경로를 다변화시켜 스마트폰 기반의 고도화된 인증 기술 도입을 촉발

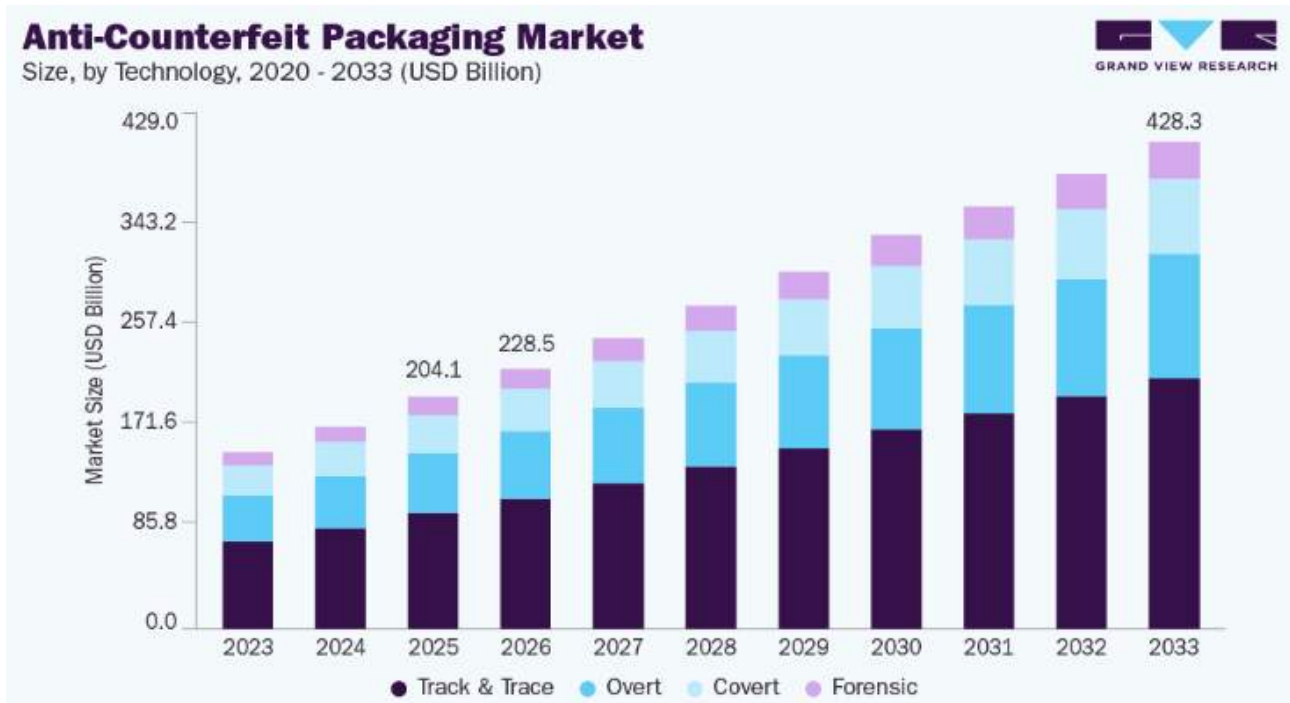


그림 11. 글로벌 위조방지 패키징 기술시장 규모 전망

- 인공지능(AI)과 블록체인 기반의 이력 관리 기술이 유통 전 과정의 투명성을 확보하며 위조품 유통을 원천적으로 차단하는 실시간 단속 기술로 진화
- 2035년에는 관련 시장 규모가 약 7,176억 달러로 전망됨에 따라 나노기술과 스마트 라벨링이 결합된 고정밀 위조방지 솔루션 도입 가속화

□ 산업기술 보호 및 제로트러스트 보안 시장의 필수 비즈니스화에 따른 시장 확대

- 글로벌 사이버보안 및 기술유출 방지 시장은 2025년 이후 연평균 10% 내외의 지속적인 성장세를 유지하며 제로트러스트 모델이 핵심 트렌드로 부상
 - 모든 접근을 상시 검증하는 제로트러스트(Zero Trust) 보안 아키텍처가 선택이 아닌 필수 요구사항으로 자리 잡으며 관련 솔루션 도입 폭증
 - 내부자 위협 분석(UEBA) 및 계정·접근관리(IAM) 기술을 중심으로 하는 지능형 산업보안 시장의 기술 고도화 및 시장 세분화
- 글로벌 사이버보안 시장은 연평균 13.8%의 고성장률을 기록하며 2024년 2,096억 달러에서 2029년 3,921억 달러 규모로 확대 전망
 - Markets and Markets(2024)에 따르면, 글로벌 보안 수요는 산업 전반에 걸쳐 확산이 되며 전체 보안산업을 견인
 - 보안 사각지대 해소, 클라우드 환경 보안성 강화, OT/IT 융합보안 수요가 성장세를 지지
 - 제조·금융·헬스케어·정부 분야에서의 데이터 보호 수요가 핵심 동력으로 작용
 - 공급망 보안 시장은 SBOM(소프트웨어 구성요소 명세) 등 하드웨어-소프트웨어 간 보안 통합 필요성 증대로 연평균 15.54% 성장 전망
 - Mordor Intelligence 분석에 따르면, 사이버공격 대상이 소프트웨어뿐 아니라 IoT, 펌웨어로 확산됨에

따라 보안 대응 영역이 확대

- 글로벌 공급망을 활용하는 제조기업들이 제품 보안 인증과 부품 단위 보안 점검을 강화하는 추세
- AI 기반 보안 시장은 2024년 24.5억 달러에서 2029년 77.5억 달러로 약 3.2배 성장 예상되며, 연평균 성장률은 약 25%에 달함
- Statista에 따르면, AI는 이상행위 탐지, 행위 기반 접근제어, 사용자 위협 모델링 등에서 핵심 기술로 부상
- 전통적 규칙기반 보안의 한계를 보완하며, 실시간 판단과 선제적 대응이 가능한 고도화 솔루션 수요를 창출

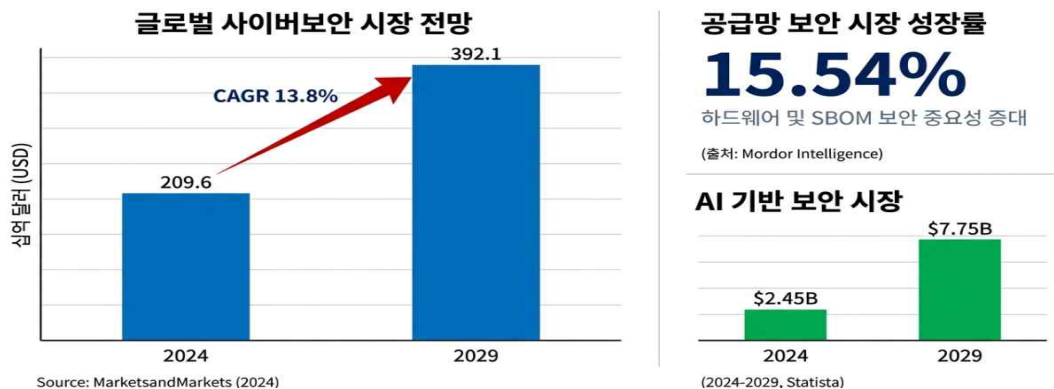


그림 12. 사이버보안 방지 기술 시장

□ 국내 수출 기업의 위조상품 피해액 및 기술유출 피해 규모 추이 분석

- K-브랜드 인지도 상승에 따른 글로벌 위조 피해 규모의 심화 및 경제적 손실 증대
- 국내 수출 기업의 브랜드 훼손에 따른 연간 경제적 피해 규모는 수조 원대에 달하며 온라인 플랫폼을 통한 위조품 유통이 주된 원인으로 지목
- * 2025년 통관 과정에서 적발된 케이(K)-브랜드 위조물품은 모두 11만 7,005점('26, 관세청)
- * 상표권 침해 사범 388명을 형사 입건, 정품 가액 기준 약 4,326억 원 상당의 위조상품을 압수('26, 지식재산처)
- 위조상품 유통으로 인한 정품 매출 감소 및 브랜드 신뢰도 하락이 국내 기업의 글로벌 시장 점유율 확보에 중대한 장애 요인으로 작용

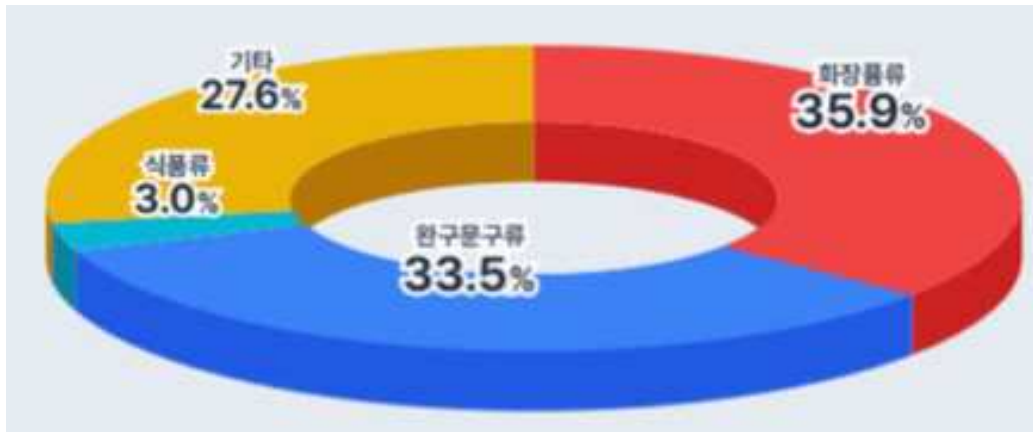


그림 13. 25년도 K-브랜드 위조물품 통관단계 적발 현황

- 국가핵심기술 및 산업기술 유출 사고의 대형화에 따른 국가적 경제 피해 누적
 - 최근 7년간(2017~2023) 국내 핵심기술의 해외 유출로 인한 예상 피해액은 약 33조원 규모에 달하며 반도체·이차전지 등 주력 산업에 피해가 집중('25, 지식재산처)
 - 최근 5년간(2019~2023) 적발된 국가핵심기술 및 산업기술 해외유출 시도는 총 96건으로 집계되며 매년 지속적인 위협 노출('24, 이재관 의원실)
 - 2023년 산업기술 유출 적발 건수는 23건으로 최근 5년 내 최고치를 기록하는 등 기술 탈취 수법의 지능화와 시도의 빈번함이 심화('24, 산업부)
- 기술 유출 수법이 네트워크 공격, 인적 경로, 클라우드 우회 등 다변화됨에 따라 단순 경계 보안을 넘어서는 전방위적 보호 체계의 부재가 피해 확산의 주요 원인
 - 중소·벤처기업뿐만 아니라 국가 핵심기술 보유 기관을 대상으로 한 조직적 산업스파이 활동이 증가하면서 국가 안보 및 경제적 근간을 위협



피해 성격: 전·현직 임직원에 의한 내부 유출이 대다수, 지능적/계획적 범죄.

반도체 (전직 연구원 유출) 삼성전자 전 연구원이 20나노 D램 공정 기술(볼츠만)을 중국 경쟁사로 유출. 공정 단계 700여 개 유출.	자율주행 (학계 유출) KAIST 교수가 자율주행 핵심 라이다(LiDAR) 기술을 중국 '천인계획' 지원을 받고 유출.	조선/방산 (설계도면 유출) 잠수함 설계 도면이 컨설팅 이직 과정에서 경쟁사 및 해외로 유출 의혹.
---	---	--

그림 14. 산업기술 유출건수 및 규모, 사례

제3절 기술동향

□ 위조방지 기술은 아날로그 보안 요소에서 디지털 식별 체계를 거쳐 물리·디지털 융합인 퍼지털 (Phygital) 보안 패러다임으로 진화

- 홀로그램 및 미세문자 등 육안 식별 위주의 전통적 아날로그 보안 기술에서 나노 광학 소재와 메타 물질을 적용한 물리적 복제 방지 기술로 고도화
 - 홀로그램, 색변환 잉크, 마이크로 텍스트 등 육안 기반 위조 방지 요소가 전통적 식별 방식의 주류를 형성
 - 사용자는 눈으로 정품 확인이 가능하며, 감정사는 특정 장비를 활용하여 판별 정밀도를 확보
 - 다만 복제 기술의 발달로 육안 기반 보안 요소는 위조 내성(Anti-counterfeiting resilience)이 점차 약화되는 한계를 드러냄
- 기존 아날로그 방식의 한계를 극복하기 위해 빛을 특정 각도에서만 굴절시켜 문양을 나타내는 렌티큘러 렌즈 기반의 나노기술을 도입하여 고도의 위·변조 방지 기능 구현
 - 가시광선뿐만 아니라 자외선 및 적외선 스펙트럼에서도 정품 여부를 판별할 수 있는 특수 보안 소재를 적용
 - 일반적인 복제 수단으로는 재현이 불가능한 강력한 물리적 장벽 구축

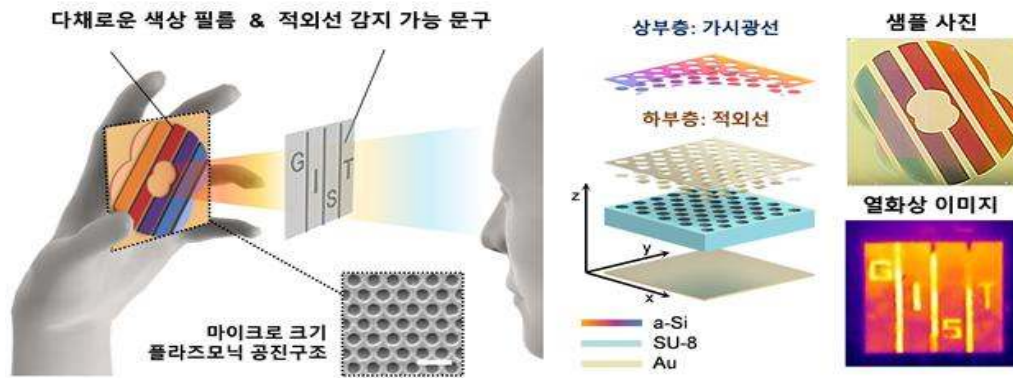


그림 15. 적외선 기반 위변조 방지 멀티스펙트럼

- 제품 표면에 육안으로 보이지 않는 미세 패턴이나 메타 물질을 삽입하여 정밀 분석 기기로만 확인이 가능한 은닉형 보안 요소를 강화함으로써 브랜드 보호의 실효성 극대화
- 위조품 제조 기술의 정교화에 대응하여 복제 시 패턴의 무결성이 파괴되도록 설계된 고난도 물리 보안 기술을 도입하여 원천적인 위조 시도 차단

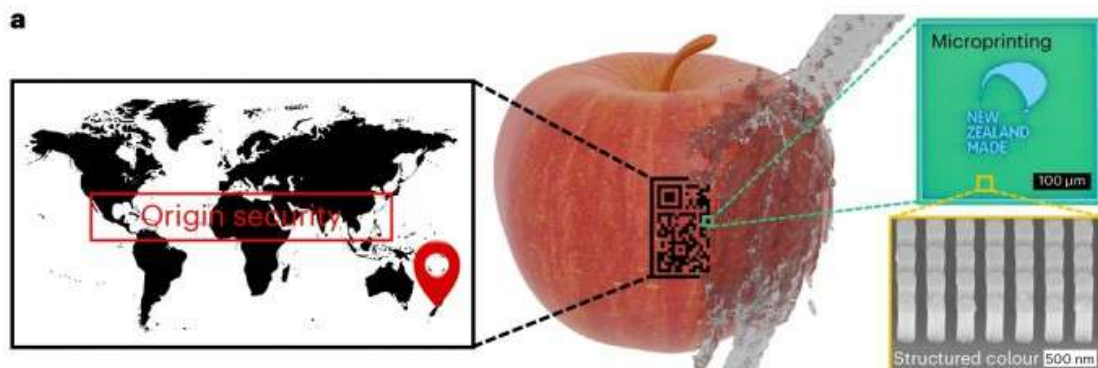


그림 16. 농식품 정보의 위·변조를 막을 수 있는 메타 라벨링 기술

- 개별 제품 단위에 고유 식별 정보를 부여하고 실시간 추적을 가능케 하는 디지털 QR 및 RFID 기반의 지능형 유통 이력 관리 체계 정착
- QR 코드, RFID/NFC 태그 등 디지털 고유식별자가 도입되며 실시간 인증과 공급망 추적이 가능해짐
- 제품마다 고유한 디지털 코드를 부여하고 QR 코드나 RFID 태그를 활용하여 생산부터 최종 소비 단계까지의 전 과정을 실시간으로 모니터링하는 추적 시스템 확산
- 제품별 ID를 부여하고 정품 여부를 온라인 DB 또는 클라우드에서 자동 검증하는 구조로 전환
- 소비자와 유통사가 스마트폰 등으로 직접 확인 가능한 사용자 친화적 인증 방식이 확산됨
- 스마트폰 전용 앱과 연계하여 소비자가 현장에서 즉시 진품 여부를 확인하고 제조사는 제품의 유통 경로를 파악하여 병행 수입 및 불법 유통을 방지하는 디지털 가시성 확보
- 플랫폼 사업자는 DB를 통해 가품 유통 여부를 조기 감지하고 유통경로를 차단할 수 있음
- 데이터의 위·변조가 불가능한 블록체인 기술을 유통 이력 관리 시스템에 접목하여 개별 제품의 디지털 기록에 대한 무결성과 대외적 신뢰성 보장

- 블록체인으로 제품 생산·유통·소비 전 주기의 인증 이력과 검증 로그를 위변조 없이 기록
- 글로벌 유통망 내에서 각 주체의 입력 정보를 실시간 공유하고 검증함으로써 불법 복제품의 시장 진입을 원천적으로 봉쇄하는 지능형 공급망 보안 구현
- ‘비가시 식별자(숨은 암호코드)’ 기술이 제품 디자인 내에 삽입되어 별도 라벨 없이도 진위 확인이 가능
- 고유 난수 기반 암호 코드를 포장 인쇄물에 삽입하고, 스마트폰 스캔 시 서버 대조로 정품 여부를 판별
 - 위조업자는 보안요소의 존재 자체를 인지하기 어렵고, 복제 성공률이 극히 낮음
- 물리적 보안 요소와 디지털 인증 데이터가 유기적으로 결합된 피지털(Phygital) 융복합 보안 기술로의 본격적인 진화 및 관련 생태계 조성
 - 제품 고유의 미세한 물리적 특성인 피지컬 핑거프린트(Physical Fingerprint)를 추출하여 디지털 코드와 일대일로 매칭하는 차세대 융합 보안 기술 고도화
- 나노 입자의 무작위 배열 등 가공 과정에서 자연적으로 발생하는 고유 패턴을 데이터베이스화하여 물리적 실체와 디지털 기록이 일치해야만 진품으로 승인하는 다중 인증 체계 확립
- 머신러닝 알고리즘은 정품과 가품 이미지·패턴 간 차이를 학습하고 오차율 1% 미만 수준으로 구분 가능
- 정품 라벨의 폰트, 인쇄 위치, 윤곽 차이 등을 미세 단위까지 자동 탐지하여 가품 여부를 판단
- 온라인 쇼핑몰, SNS 등에서는 상품 이미지와 설명 간 불일치를 분석해 위조 의심 게시물 선별
- AI 이미지 분석 기술을 활용하여 특수 장비 없이 스마트폰 카메라만으로도 미세한 위조 패턴이나 워터마크를 정밀 감별하는 지능형 단속 환경 조성
- 딥러닝 알고리즘이 수만 건의 정품 및 위조품 데이터를 학습하여 일반인이 식별하기 어려운 고난도 위조품까지 높은 정확도로 즉각 판별하고 실시간 신고 시스템과 연계
- 위조 Hotspot을 자동 탐지하고, 단속 기관과 민간 유통사 간의 정보 공유 체계를 연동
- 유럽연합(EU)의 디지털 제품 여권(DPP) 도입 및 ISO 22380 등 국제 표준 부합성 확보를 통한 글로벌 공급망 투명성 규제 대응 강화
- 제품 사기 방지 일반 원칙(ISO 22380)과 진품 인증 성능 기준(ISO 22383)을 준수하는 추적 시스템을 도입하여 위조 위험을 체계적으로 관리

□ 산업 기술 유출 방지의 사후 적발에서 지능형 선제 예방으로의 패러다임 전환을 위한 첨단 산업 보안 기술 고도화 추진

- 기존 산업 보안 체계는 사후 감사 위주의 제한적 대응에서 벗어나지 못했던 구조적 한계를 가짐
 - 로그 기반 대응은 사건 발생 후 조사에 초점을 두며, 정보 유출을 사전에 차단하는 데는 한계
 - 유출 시점 파악, 외부 반출 경로 확인, 유출자 특정 등에 상당한 시간과 인력이 소요
 - 내부자 또는 협력사에 의한 유출은 흔히 장기간 탐지되지 않고 누적 피해 초래
 - DLP, DRM 등 전통적 기술은 파일 반출·복사·출력 차단 기능에 초점을 두었으나, 이상행위 탐지 능력은 낮음
 - 사전에 정의된 규칙 기반 탐지는 예외적 상황에 대한 유연한 대응이 어렵고 오탐률이 높음

- 사후 로그 분석 중심의 수동적 대응 체계를 탈피하여 인공지능 기반의 이상행위 탐지 및 내부자 위협 분석(UEBA) 중심으로 보안 체계 진화
 - UEBA 기반 보안은 사용자 행위 단위의 위험 수준 점수를 산정하고 누적 위험도 기반 조치를 취함
 - 단일 이벤트가 아니라, 복수의 행위 조합에 따라 잠재 위험을 판단하는 고도화된 보안 체계로 진화
 - UEBA시스템을 통해 임직원의 평소 업무 패턴을 학습하여 비정상적인 데이터 접근이나 기밀 자료의 무단 반출 징후를 실시간으로 간파하는 지능형 모니터링
 - 인공지능이 대량의 사용자 행위 데이터를 분석하여 기술 유출의 전조 증상을 포착하고 사고 발생 전 즉각적인 경고 및 접근 차단 프로세스 가동
 - * 예외적 파일 접근, 대용량 복사, 비정상 시간대 접속, 인가되지 않은 클라우드 업로드 등을 실시간 인식
 - 보안 특화 거대언어모델(LLM)을 활용하여 침해 사고의 위협 의도를 신속히 파악하고 대응 시나리오를 자율적 생성하는 지능형 보안 운영(SOC) 환경 구현
 - 이상징후 발생 시 관리자 경고, 자동 차단, 사전 지정 경로 폐쇄 등 대응 수단 연계

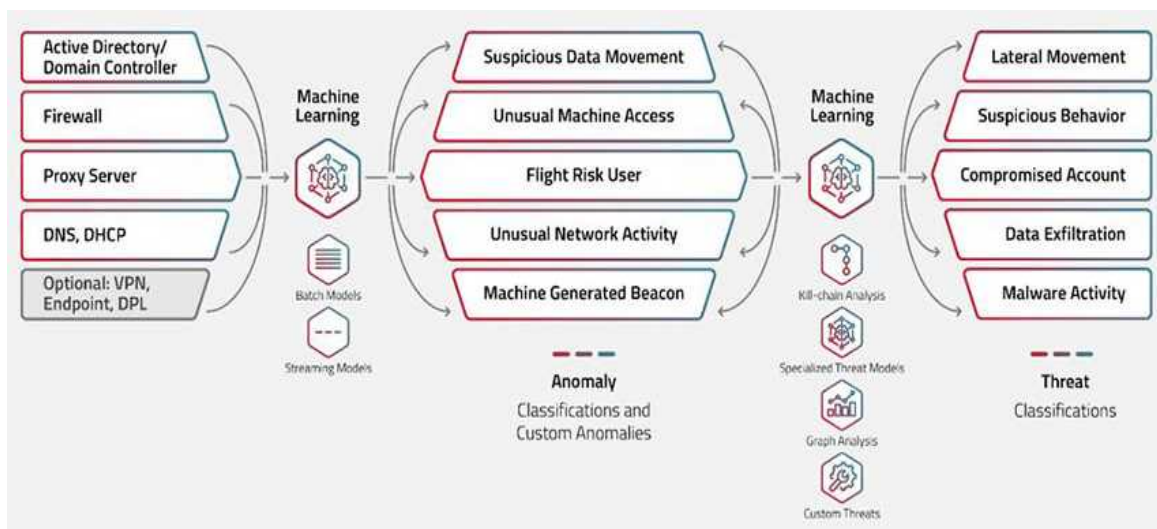


그림 17. UEBA 운영체제

- 네트워크 경계 보안의 한계를 극복하기 위해 모든 접근 시도를 상시 검증하고 권한을 최소화하는 제로 트러스트(Zero Trust) 보안 아키텍처의 전면적 확산
 - 2025년 보안 트렌드에 따라 제로 트러스트를 필수 비즈니스 요구사항으로 설정하고 계정 및 접근 관리(IAM)와 다중요소인증(MFA)을 결합한 신원 기반 접근 통제 실시
 - ZTNA(Zero Trust Network Access) 기반 보안은 어떤 사용자도 기본 신뢰하지 않으며, 매 요청마다 인증·검증을 수행
 - 문서 파일 단위의 권한 제어(IRM) 및 실시간 워터마크 기술을 적용하여 정보가 외부로 노출되더라도 누설자 추적과 캡처 방지 등 데이터 주권 보호

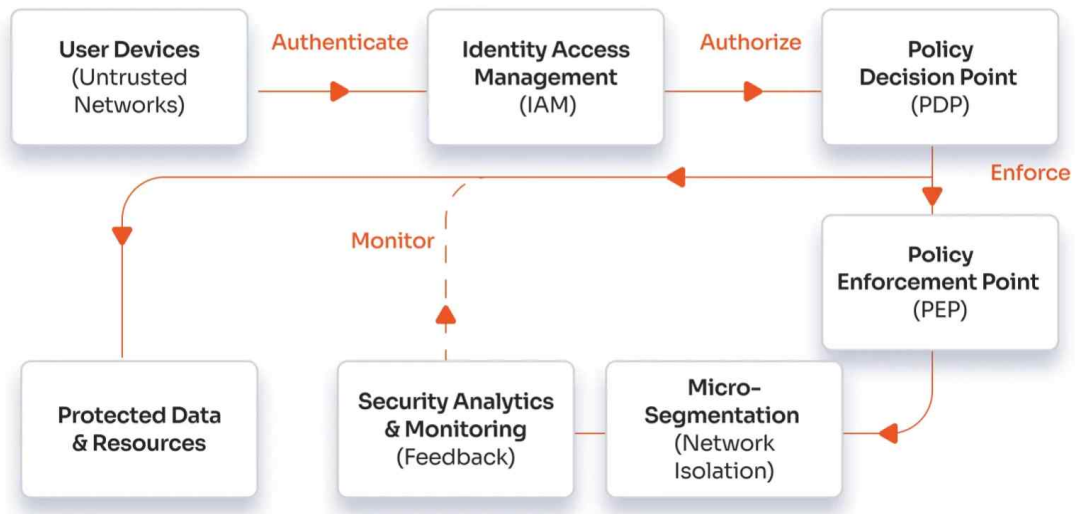


그림 18. Zero trust 아키텍처

- 생성형 AI 확산에 따라 기밀정보 유출 대응을 위한 프라이빗 AI 도입이 증가
 - 사내 서버 기반 챗봇, 입력 정보 암호화, 외부 AI 차단 시스템 도입 등이 표준화되고 있음
 - AI가 생성한 허위 문서 및 위조 정보 식별 기술 등도 산업 보안 분야의 신기술로 부상
- 물리적 보호와 디지털 보안이 융합된 다층 방어 인프라 강화 및 자율 복구 등 미래형 원천 기술을 통한 보안 복원력 확보
- 핵심기술 개발 부서 대상으로 물리적 망분리와 정보 유출방지(DLP) 솔루션이 연계된 고신뢰 안심존 (Secure Zone) 환경의 조성
 - 핵심 개발 부서 PC의 USB 포트 차단 및 인터넷 망분리를 시행하고 별도 인가된 안전 장소에서만 기밀 자료의 열람과 토론이 가능하도록 물리적 보안 강화
 - 기술 유출 수법의 다변화에 대응하기 위해 반도체나 조선 산업 등 업종별 특화된 보안 기술 분류 체계 및 솔루션 보급

제4절 시사점 및 대응방향

1 시사점

□ (해외) 기술 안보 중심의 배타적 보호장벽 강화 및 공급망 통제 심화

- (패러다임 전환) 주요국(美·EU·中)은 지식재산 보호를 통상 이슈를 넘어 국가 존망과 직결된 안보 의제로 격상하고, 자국 첨단 기술 유출 방지를 위한 법적·제도적 장벽을 최고 수준으로 높이고 있음
 - * (美) ‘혁신경쟁법’, ‘칩스법’ 등을 통해 기술 유출을 간접 혐의로 강력 처벌 / (EU) ‘공급망 실사 지침’ 등을 통해 위조품 및 지적권 침해 물품의 역내 반입 원천 봉쇄
- (표준 선점 경쟁) 자국의 보호 기술 및 인증 체계를 글로벌 표준으로 만들기 위한 표준 전쟁 가속화
 - 단속 지원 기술 중심이 아니라 기술 유출 예방, 위조 증거 확보 등 기술 중심으로 R&D 무게중심 이동

□ (국내) 법·제도는 마련되었으나, 기술적 수단과 인프라 미흡

- (법·제도 한계) 「산업기술보호법」, 「부정경쟁방지법」 등 법적 근거는 강화되고 있으나, 실제 현장에서 지능화된 유출(AI, 클라우드 등)을 탐지하거나 고도화된 위조를 식별할 기술적 실행 수단은 미흡
- (지원 파편화) 부처별, 산업별로 보호 지원이 산발적으로 이루어져, 국가 차원의 통합된 기술 보호 R&D 로드맵과 표준화된 대응 플랫폼이 부재한 상황
- 국내는 K-브랜드 위조 및 첨단산업 기술유출이 경제·안보 리스크로 격상, 범정부 대응체계가 단속·수사 중심에서 기술 기반까지 확대
- * OECD 추산 '24년 기준 한국 기업 위조 피해 약 97억 달러(약 11조 원) 규모, 2025년 통관 단계 적발 11만 7,005점(정품가액 약 4,326억 원) 압수
- * 최근 5년('20~'24) 산업기술 해외유출 105건(피해 약 25조 원) 추산, 피해의 86.5%가 중소기업 집중(수사 통계) 등 구조적 취약성 고착화

표 5. 글로벌 주요국 vs 국내 지식재산 보호 정책·제도 비교 분석

구분	글로벌 주요국 (미국, EU, 중국 등)	국내 현황	격차 및 한계 (Gap Analysis)
정책 기초	[경제안보] · 기술 유출을 간접 행위로 간주 · 국가 존망과 직결된 안보 이슈화	[산업보호] · 개별 기업의 재산권 보호 중심 · 경제적 손실 방지 차원 접근	· 안보 의식 부재국가 차원의 전략적 통제력 약화 및 컨트롤타워 기능 미흡
대응 방식	[선제적·예방적] · (美) 기획수사팀(Disruptive Tech Strike Force) 운영 · (EU) 공급망 실사 의무화로 사전 차단	[사후적·처벌적] · 유출/위조 발생 후 고소·고발 의존 · 피해 발생 시점엔 이미 회복 불가능	· 골든타임 실기사건 발생 전 탐지·차단 기술 부족으로 피해 확산 방지
기술 수단	[디지털·지능형] · 블록체인, 디지털 워터마킹 의무화 · 사이버·물리 융합 보안(CPS) 표준 적용	[아날로그·물리형] · 홀로그램, CCTV, 출입 통제 위주 · 디지털 증거 능력 확보 미흡	· 기술적 지체로 지능화된 범죄(AI, 해킹)를 막을 첨단 방어 기술(R&D) 부재
지원 체계	[생태계 주도] · (EU) 중소기업 IP 바우처 및 통합 플랫폼 · 민관 합동 정보 공유(ISAC) 활성화	[개별 지원 (Siloed)] · 부처별, 사업별 단발성 지원 산재 · 영세 기업은 보안 사각지대 방치	· 인프라 파편화 · 국가 표준 플랫폼 부재로 기업 간 보안 격차(양극화) 심화

2 대응 방향

□ [R&D 전략] 능동형 탐지 기술로 패러다임 전환

- 인력 중심의 사후 수사 한계를 극복하기 위해, AI 기반의 이상징후 탐지 및 유출 경로 추적 기술 개발에 정부 R&D 예산 투입이 시급함

- 국내는 「산업기술보호법」 등에 의해 처벌 수위는 강화되었으나 실제 유출 범죄의 기소율은 50% 미만, 범죄 실행 단계에서 이를 포착할 기술적 감시 자산이 없기 때문에 유출된 기술의 회수는 사실상 불가능함
- * (미국) 법무부와 상무부가 주도하여 혁신기술 타격대를 결성('23), AI 기술을 활용하여 기술 탈취 시도를 사전에 탐지하고 공급망을 역추적하는 선제적 방어 체계 가동
- * (EU) 사이버 복원력법을 통해 디지털 제품의 설계 단계부터 보안 기능 탑재를 의무화하여 위협을 원천 차단

□ [기술 고도화] 디지털 증거 능력 확보 및 차세대 식별 기술

- 글로벌 기술 규제(디지털 여권 등)에 대응하고 국내 기업의 수출 경쟁력을 지키기 위해, 복제 불가능한 차세대 식별 소재 및 블록체인 융합 기술 확보 필수
- 국내 위조방지 기술은 육안 식별(QR, 홀로그램)에 의존하여, 스마트폰 스캔 조작 복제하는 '가짜 사이트 연결' 수법에 속수무책임
- * (민간) LVMH, 까르띠에 등 글로벌 명품 기업들은 아우라(Aura) 블록체인 컨소시엄을 통해, 제품의 생산부터 유통까지 전 과정을 디지털로 추적하여 위조품 혼입을 원천 봉쇄
- 또한 디지털 기술 유출 시 법적 효력을 갖는 디지털 포렌식 증거기술 표준이 미비함
- * (미국) 바이든 행정부 'AI 행정명령'('23.10)을 통해 AI 생성물에 대한 워터마킹(Watermarking) 및 디지털 인증 기술 표준 개발을 국책 과제로 천명

□ [생태계 조성] 중소기업 전용 국가 표준 보안망 구축

- 중소기업의 투자 여력을 보완하기 위해 정부가 표준 보안 모델을 개발·보급하고, 클라우드 기반의 공공 보안 서비스를 지원해야 함
- 국내 기술 유출 피해의 86.5%가 중소기업이나, 이들은 보안 솔루션 도입 비용 부담으로 무방비 상태에 노출
- * (EU) SME Fund를 조성하여 중소기업의 IP 보호 활동을 직접 지원하고, 범유럽 위조품 감시 플랫폼을 통해 국경 간 단속 정보를 실시간 공유
- * (일본) '부정경쟁방지법' 개정('23)을 통해, 중소기업의 데이터나 영업비밀이 클라우드 상에서 침해될 경우에도 보호받을 수 있도록 기술적·제도적 안전장치 마련

제3장 R&D 추진전략

제1절 추진 방향 도출

1 SWOT 분석

□ (Strengths) 공공 인프라, 기술기반, 정책의지 결합에 따른 제도-기술-현장 연계 추진 가능

- 세계적 수준의 ICT 인프라 및 디지털 데이터 기반 기술 축적을 통해 정품인증·산업보안 기술 상용화 기반이 구축되어 있음
 - 5G, AI, 블록체인 등 기반 기술 인프라가 안정적으로 마련되어 위조방지 플랫폼 및 자율보안 기술 전환에 유리한 여건 보유
 - 국내 스마트폰 보급률, 초고속 통신 인프라 수준은 세계 상위권이며, QR·NFC 기반 인증 환경 활용성도 높음
 - 2025년 국제지식재산지수(GIPC) 세계 10위 달성 등 글로벌 최상위권의 IP 행정 경쟁력 및 사법 시스템 확보
- 정부의 강력한 지식재산 보호 정책 의지와 범부처 협력 체계 기반의 제도 추진력 확보
 - 산업기술보호법, 국가첨단전략산업법, 상표법 등 다층 법제 기반 정비
 - 지식재산처 방첩기능 부여, AI 위조탐지 확대 등 실행 기반 강화
 - 일부 위조방지 요소 기술(DRM, 보안소재 등)은 국제 경쟁력을 보유하며 조폐공사·보안인쇄기업 등 특허기관 중심의 기술자립 기반 확보
 - 정부의 강력한 기술보호 및 국가 핵심기술 수호 의지 기반의 범부처 합동대응 거버넌스 가동
- 2025년 국제지식재산지수(GIPC) 세계 10위, 지식재산권 분야 세계 2위 달성 등 글로벌 최상위권의 제도적 인프라 입증
 - 2024년 종합 16위에서 2025년 10위로 7단계 수직 상승하며 역대 최고 순위 기록하는 등 국가 지식재산 보호 환경의 비약적 개선 증명
 - 영업비밀 및 기밀정보 보호 분야에서 세계 9위를 기록하며 부정경쟁방지법 강화에 따른 실무적 보호 실효성을 대외적으로 인정
 - 행정 효율성 및 사법적 구제 절차의 선진화를 통해 글로벌 선도 국가로서의 IP 규범 확보

□ (Weaknesses) 원천기술 자립도 미흡 및 민간의 보안투자 비용부담에 따른 현장 도입 지연

- 핵심 보안 소재 및 원천기술의 높은 대외 의존도로 인한 기술적 공급망 리스크 상존
 - 위조방지용 특수필름(편광판 등), 보안잉크 등 핵심 소재 분야 기술 자립도가 일본·미국 등 선도국 대비 취약하여 대외 의존도 심화
 - 특허 출원량 등 양적 지표는 세계 상위권이나, 실질적 기술 가치를 나타내는 특허영향력지수(PII)가 0.68~0.78 수준으로 미국(2.1~2.6) 대비 현저히 낮음
 - 원천·핵심 기술보다는 기존 기술을 개선한 개량기술 위주의 출원이 집중되어 글로벌 표준 선점 및 로열티 수익 창출 역량 한계
- 산업보안 기술은 AI 기반 이상행위 탐지 등 신기술 도입 초기 단계이며, 중소기업의 기술 수용성 및

비용 부담이 구조적 제약으로 작용

- DRM, DLP 등 전통기술은 일정 수준 고도화되었으나, UEBA, ZTNA 등 자율보안 기술은 데이터셋 부족 및 실증 사례 부족으로 실효성 저조
- 중소기업의 보안 인프라 도입률은 50% 미만으로, 초기 구축 및 유지비용이 기술 도입의 가장 큰 저해요인
- 민간 클라우드, 모바일 환경에서 통합 보안이 가능한 범용 솔루션 부족
- 보안기술 개발은 부처별 분산형 R&D 구조로 인해 현장 수요와 연계된 실증 기반 확보에 한계
- 위조방지, 인증, 이상행위 탐지 등 R&D는 기술성 중심의 소재개발에 편중되어 실수요 기반 서비스 기획 부족
- 소비자, 유통사, 브랜드사의 사용자 경험(UX), 신뢰성, 유지관리 요구가 기술 개발단계에 반영되지 못하고 있음
- 기술 이전 및 확산이 제한되어 중소·중견기업으로의 기술 스푼오버(Spillover)가 구조적으로 미흡
- 표준에 부합하는 해당 표준을 선도할 수 있는 원천기술 개발이 뒷받침되지 않아 국산 보안 기술의 해외 시장 진출 시 객관적 기술 차별성 확보에 난항
- 복제저항성, 판별 민감도, 인증 실패율 등 성능 정량평가 지표에서 KS A ISO 22383 표준 요건을 상회하는 기술 수준을 입증할 수 있는 국산 원천기술이 부재하여, 국가공인 수준의 기술 경쟁력 확보가 미정립
- 조폐공사 등 일부 기관의 자체 시험 수준에 그쳐, KS A ISO 표준을 선도하는 기술력을 민간에 확산하고 해외 진출로 연결하는 데 제약
- 해외 조달·유통망에서 요구되는 표준 연계 인증은 기술 보유 자체가 전제되어야 하나, KS A ISO 22383 표준 수준을 선도하는 국산 기술이 부재하여 기술 수출 시 장벽으로 작용
- 중소·중견기업의 첨단 보안 솔루션 도입 비용 부담 및 전문 보안인력 확보의 어려움
- 제로트러스트(Zero Trust), 내부자 위협 분석(UEBA) 등 차세대 지능형 보안 시스템 구축을 위한 초기 투자비 및 유지보수 비용이 민간 영역의 보안 수준 상향 평준화 저해
- 중소기업의 보안 솔루션 정착률이 대기업 대비 50% 미만 수준으로 낮으며, 보안 진단 인력 부재로 인한 시스템 운용 및 침해 사고 대응력 취약

□ (Opportunities) K-브랜드 확산, 비대면 전환, 국제 규범 강화 등 대외 환경 변화가 기술 확산 및 시장 진입의 전략적 계기 제공

- 글로벌 시장 내 K-브랜드 인지도 및 가치 상승으로 인한 보호 명분 및 국제적 수요 존재
- K-뷰티, 푸드, 가전 등 주요 수출 품목의 글로벌 점유율 확대로 인해 정품 인증 및 브랜드 보호 솔루션의 동반 수출 기회 창출
- 위조 피해 실태가 정량화되며 K-브랜드 보존을 위한 공공 개입 정당성 확보
- 해외지식재산센터 및 관세청 합동 단속 등을 통해 역외 위조상품 유통에 대한 능동적 대응 및 국제 공조 기반 확보
- 우리 기업의 브랜드 가치 수호가 곧 국가 경제 안보와 직결된다는 사회적 공감대 형성을 통해 민관 합동 대응 에너지 결집

- 팬데믹 이후 비대면·온라인 중심의 유통 구조로 급속히 전환되며 디지털 인증 및 보안 기술의 필수 인프라화 추세가 본격화됨
- 이커머스, D2C(Direct to Consumer) 채널에서 정품 여부의 식별이 기업 신뢰도와 직결되며, 디지털 인증 시스템의 보편적 수요 확대
- SNS 기반 유통과 크로스보더 쇼핑 확산은 클라우드 기반의 실시간 인증 플랫폼 수요를 견인
- 온라인 거래의 고도화로 소비자 대상 직접 인증 솔루션의 상용화 환경 조성
- 생성형 AI, 디지털 제품 여권(DPP) 등 국제적 기술규범이 확대되며 위조방지·산업보안 기술의 법제화 및 의무화 흐름 가속화
- EU 디지털제품여권(DPP), 미국 SBOM 등 글로벌 공급망 규범은 정품 인증·무결성 보장을 핵심 요건으로 설정하며 관련 기술의 도입이 필수화
- ISO 22380, 22383, 23234 등 국제표준은 국내 기술의 호환성과 수출 가능성을 확대할 수 있는 기반으로 작용
- 글로벌 기업과의 공동 인증체계 구축, 기술 공동개발, 상호 인정 협약을 통한 진입장벽 완화 가능
- 정책적 기조 변화와 공공사업 연계 확대에 따라 기술의 공공 수요와 조달 연계 가능성 상승
- 국가첨단전략산업법, 산업기술보호법 및 지식재산전략 기본계획 등과 연계되어 위조방지 및 보안 기술의 공공 적용 범위 확대
- 교육·의료·물류·에너지 등 비제조 분야로의 기술 확산 가능성이 열리며 다분야 수요 기반 확보
- 정부 주도의 실증사업 확대, 지자체 기반 위조 단속 체계와의 기술 연계 등으로 공공-민간 협력 확산 기반 마련
- K-방산, K-의료 등 국가 핵심 수출 품목 보호를 위한 정품 인증, 기술보호 요구 증가에 따라 국산 기술의 우선 채택 가능성 부상
- 위조 방지 기술을 핵심 품목 수출 지원 사업과 연계하여 국가 브랜드 신뢰도 확보에 기여
- 한류 확산에 따른 저작권, 상표권 침해 증가로 K콘텐츠 분야의 디지털 IP 보호 기술 수요가 동반 확대

□ (Threats) 위조·유출 수법의 지능화, 글로벌 규범 경쟁 심화, 기술 의존도 등 외부 환경 변화가 국내 기술의 확산과 자립성에 구조적 위협 요인으로 작용

- 생성형 AI·딥페이크 등 신기술을 활용한 위조·모방 기술이 고도화되며 전통적인 위조방지 수단의 대응 한계가 뚜렷해짐
- AI 기반 정교한 이미지·라벨 복제가 가능해짐에 따라 홀로그램, 잉크 등 육안 기반 요소만으로는 진위 판별이 어려움
- 디지털 인증 정보에 대한 위·변조 기법도 진화하면서, 단일 보안 요소의 방어력은 점차 약화
- 온라인 플랫폼 내 AI 자동 생성 콘텐츠 확산으로 인해 위조 탐지·판별의 정확도 저하 및 실시간 대응의 한계 발생
- 위조방지 및 산업보안 분야의 국제 기술표준 선점 경쟁 심화로 인해 국내 기술의 글로벌 시장 진입 장벽이 지속 상승
- ISO, IEC, NIST 등 국제표준기구 주도권을 미국, EU, 일본 등이 선점하며 기술 사양의 글로벌 기준화를 주도

- 기술의 성능과 무관하게 국제표준과 부합되지 않을 시 수출 및 조달 시장 진입이 제한되는 구조가 정착
- 국내 개발 기술이 기술적으로 경쟁력이 있음에도 불구하고 인증 체계 부재로 인해 신뢰 확보가 어려운 상황 발생 가능
- 산업스파이, 내부자 유출, 클라우드 기반 침투 등 유출 경로가 복합·다변화되며 보안 체계의 설계 난이도가 급격히 상승
 - 단순 매체 복사 위주에서 탈피하여 내부자 포섭, 해외 우회 법인을 통한 세탁, 지능형 사이버 공격 등 고도화된 산업스파이 활동빈번
 - 최근 7년간 약 33조 원 규모의 누적 예상피해 발생 등 반도체·이차전지 등 국가 첨단산업의 경쟁력을 근본적으로 위협하는 구조적 유출위험 상존
 - 주요국 간 기술 민족주의 강화 및 수출통제 확대로 인해 우리 기업의 해외 현지법인 보안관리 및 공급망 내의 기술수호 부담가중
 - AI, IoT, 모바일 기반 스마트 제조 환경으로 전환되며 기존 보안 인프라의 적용 한계가 표면화
- 핵심 소재·플랫폼 기술의 해외 의존도가 높아, 공급망·정책 환경 변화 시 국내 기술 자립성에 구조적 취약성 노출
 - 위조방지 소재(나노필름, 렌티큘러 등)는 일본, 유럽 등에서의 기술력 우위로 인해 원천소재 수입 의존
 - 인증 플랫폼의 경우 미국, 중국 등의 대형 클라우드 기업 중심으로 기술·특허·API 경쟁력이 집중
 - 소프트웨어 자재명세서(SBOM), 디지털 제품 여권(DPP) 등 글로벌 디지털 인증 규범 확산 시 국내 기술의 대응 속도 지연 우려
- 기술이 고도화될수록 보안 비용과 유지 관리 리스크도 함께 상승하며, 민간 기업의 도입 지속성이 위협받을 가능성 상존
 - 위조방지 및 산업보안 솔루션은 설치·운영·갱신 비용이 복합적으로 발생하며, 중소기업의 경제적 수용성 제약
 - 인증 실패·오인식 등으로 인한 소비자 불만과 브랜드의 이미지 훼손 등 위험도 병존
 - 보안 기술의 고도화는 해커의 우회 전략을 동시에 고도화 시키는 결과를 초래하며 지속적 투자와 리스크 관리 필요

표 6. SWOT 분석

		강점(S)	약점(W)
		내부 역량 ○ 세계 수준의 ICT 인프라(5G, AI) 및 디지털 데이터 기반 보유 ○ 범부처 협력 기반의 강력한 기술보호 정책 의지 및 법제 정비 ○ GIPC 세계 10위권의 글로벌 최상위 IP 행정/사법 시스템 입증	○ 핵심 보안 원천소재(나노필름, 잉크 등)의 높은 해외 의존도 ○ 중소기업의 첨단 보안 솔루션 도입 비용 부담 및 전문 인력 부족 ○ 표준 부합한 국내 선도 기술의 부족 ○ 부처별 분산형 R&D로 인한 현장 수요 중심 실증 기반 약화
외부 환경		[SO 전략]	[WO 전략]
		기회(O) ○ 글로벌 K-브랜드 확산에 따른 정품 인증 시장 팽창 ○ 비대면 유통 가속화에 따른 실시간 디지털 인증 수요 증대 ○ EU DPP, 미국 SBOM 등 글로벌 공급망 보안 규범 강화	- (WO1) AI 기반 이상행위 탐지 및 피지털 보안 시스템 고도화로 위협대응 능력 확보 - (WO2) 표준에 부합한 인증기술 동시 개발을 통해 국제 기술 장벽 선제적 대응 - (WO3) 기업수요 기반 연구개발을 통해 기술의 시장 적합성 및 신뢰성 확보
		[ST 전략]	[WT 전략]
		위협(T) ○ 생성형 AI 기반 '슈퍼페이크' 위조 및 유출 수법 고도화 ○ 클라우드, 인력 매수 등 기술유출 경로의 지능적 다변화 ○ 국제 표준(ISO, NIST) 선점 경쟁 및 기술 장벽 강화	- (WT1) 핵심 원천기술을 확보를 위한 집중적인 혁신기술 확보 추진 - (WT2) 신규기술의 법적 리스크를 줄이기 위한 법적 리스크 관리 - (WT3) 개발된 기술의 시장 진입 장벽 해소를 위한 표준/인증 연계

SWOT 시사점	전략	추진 전략
○ 기존 위조방지 기술은 물리 기반에 편중되어 있으며, AI·블록체인 등 디지털 융합 기술과의 연계가 미흡함 ○ K-브랜드 위조피해가 확산되고 있음에도 정품 인증 기술이 수출품에 적용되지 않아 시장 신뢰 확보에 한계 존재 ○ DPP, SBOM 등 국제 기술보호 규범 강화에 비해 국내 인증 기준과 법제 기반이 미비하여 글로벌 시장 대응이 어려움	- (SO1) ICT 및 디지털 데이터를 기반으로 한 융복합형 기술개발 추진 - (SO2) K-브랜드 확산을 기회로 활용하여 위조방지·산업보안 기술을 수출품 연계 필수 항목으로 추진 - (SO3) 글로벌 공급망 규범에 부합한 기술보호 정책 및 법제 정비	
○ 핵심 보안 원천소재(나노필름, 잉크 등)의 높은 해외 의존도 및 실증 기반 부족으로 기술 신뢰성 확보에 어려움 존재 ○ 개발 기술의 상용화 단계에서 법적 근거 미비로 시장 진입 지연 및 법적 불확실성 존재 ○ ISO 등 국제 인증체계 미충족 시 기술 성과와 무관하게 글로벌 유통망 진입이 제한되는 구조적 한계 존재	- (ST1) 소재·인증·실증 격차 해소를 위한 수요기업 기반 R&D로 기술 신뢰도 확보 - (ST2) R&D 성과물의 시장 활성화를 위한 법리적 근거 즉시 연계 - (ST3) 인증 표준과 연계된 디지털 기반 정품 인증 플랫폼 조성	기술개발과 동시에 표준에 부합한 인증 체계를 마련하여 시장 진입 장벽 해소
○ 생성형 AI 기반의 위조·유출 수법이 고도화됨에 따라 기존 보안 체계로는 실시간 대응에 한계 존재 ○ 국내 인증 기준/성능 평가에 부합한 선도 기술이 부재하여 기술 신뢰도 확보 및 수출에 제약 발생 ○ 부처별 분산형 R&D 구조로 인해 현장 수요와 연계된 실증 기반 및 사용자 관점의 기술 적합성 확보에 한계 존재	- (WO1) AI 기반 이상행위 탐지 및 피지털 보안 시스템 고도화로 위협대응 능력 확보 - (WO2) 표준에 부합한 인증기술 동시 개발을 통해 국제 기술 장벽 선제적 대응 - (WO3) 기업수요 기반 연구개발을 통해 기술의 시장적합성 및 신뢰성 확보	수요기업 참여형 현장 실증 체계 구축을 통한 기술의 시장 적합성 및 신뢰성 확보
○ 위조방지 및 산업보안 핵심기술의 해외 기술 의존도가 높아 공급망 리스크 및 정책환경 변화 시 자립성 위협 노출 ○ 생성형 AI, 개인 정보 등 기술 고도화에 따른 법적·윤리적 리스크가 발생하고 있으나 사전 평가 및 대응 미흡 ○ 공인 성능 인증체계 부재로 민간 시장에서의 기술 채택 저조 및 수출 시 신뢰 확보 어려움 발생	- (WO1) AI 기반 이상행위 탐지 및 피지털 보안 시스템 고도화로 위협대응 능력 확보 - (WO2) 표준·인증 동시 개발을 통해 국제 기술 장벽 선제적 대응 - (WO3) 기업수요 기반 연구개발을 통해 기술의 시장적합성 및 신뢰성 확보	

2 전략적 추진 방향

□ SWOT 분석을 통한 핵심 이슈 및 시사점

- 국내 지식재산 보호 환경의 내부 역량과 외부 환경을 종합한 SWOT 분석 결과, 과거의 단편적·공급자 중심 R&D에서 벗어나 시장 수요 기반의 패키지형 보호 생태계로 전환 필요
 - (강점) 세계 최고 수준의 ICT·제조 인프라 및 정부의 강력한 디지털 혁신(DX) 의지
 - (약점) 보안업계의 영세성(94.9%가 자본금 50억 미만), 요소기술 중심의 파편화된 R&D, 공인된 성능평가·표준에 부합한 기술개발이 부재
 - (기회) K-브랜드 가치 급상승, 글로벌 기술안보 시장 급성장, AI·블록체인 등 신기술의 보안 적용성 증대
 - (위협) 생성형 AI 등 신기술을 악용한 산업스파이 공격 고도화, 테드카피(완벽 복제) 범람, 주요국의 보호 규제 장벽 강화
- (시장실패 보완) 민간의 영세성을 극복하기 위해 정부 R&D가 투입되어야 하나, 과거처럼 파편화된 기술 (예: 단일 RFID, 미세패턴 등) 지원은 지양하고 통합 플랫폼 기반으로 나아가야 함
- (초격차 위협 대응) K-브랜드와 국가 핵심기술을 노리는 지능형 위협에 대응하기 위해, 기술 수요자의 직접 참여로 실제 현장의 시나리오를 반영한 실증형 R&D가 필수적임

표 7. 현황 및 문제점과 핵심 이행 과제

구분	현황 및 문제점 (As-Is)	개선 방향 (To-Be)	핵심 이행 과제
[전략 1] 능동형 방어 기술	· 사후 적발·처벌 중심 · 아날로그 식별(육안) · 물리적 경계 보안 의존	· 사전 탐지·예방 중심 · 디지털 융합 식별(AI) · Zero-Trust 기반 보안	① AI 기반 유출 징후 탐지 기술 개발 ② 위변조 원천 차단 소재/부품 개발 ③ 디지털 포렌식 증거 확보 기술 고도화
[전략 2] 글로벌 표준 선점	· 표준선도 기술의 부재 · 기업별 자체 기준 난립 · 해외 인증/규제 종속	· K-Security 표준 정립 · 국제 표준(ISO) 주도 · 상호운용성 확보	① 위조방지 기술 성능평가 체계 구축 ② 보안 기술 가이드라인 보급 ③ 글로벌 인증 상호인정 추진
[전략 3] 보호 생태계 확산	· 대/중소기업 보안 격차 · 고비용으로 도입 저조 · 공급망 보안 취약	· 전주기 보호 안전망 · 서비스형보안(SECaaS) · 공급망 전체 보안 강화	① 중소기업 맞춤형 보안 패키지 보급 ② 실증 센터(Test-bed) 구축 및 운영

3 사업 추진 방향

□ [내역 1. 위조방지] 코드·정보, 고도화·복합인증 2개 분야에 R&D 집중 투자

- (기술 성숙도) 시각·물리 및 전자·디지털은 민간 주도 성숙 기술로 공공 R&D 효과 제한
 - 홀로그램 등 시각·물리 기술은 Uflex·HP·DNP Group 등 글로벌 기업이 시장을 선점한 성숙 영역으로, 신규 공공 투자를 통한 기술 차별성 확보가 어려운 구조

- 아울러 위조품의 30~35%에 이미 모방 홀로그램이 적용되어, 소재 기반 물리적 위조 억제 효과의 실효성 자체가 감소 추세
- PUF 칩·파괴형 안테나 등 전자·디지털 기술은 반도체·RFID 전문 민간기업의 핵심 IP 집중 구간으로, 국내 범용 조달이 가능한 수준
- (한국 시장 특성) K-뷰티·패션·식품의 위조 피해 구조상 코드·정보, 고도화·복합인증이 직접 해법
 - K-브랜드 위조 피해는 오프라인 소재 복제가 아닌 전자상거래 플랫폼을 통한 디지털 무한 유통이 핵심 경로: 해외 온라인 위조 적발 건수 2023년 16,774건 → 2025년 36,116건으로 2년 새 2배 이상 급증
 - K-뷰티·패션·식품 위조 피해 추정액 2024년 기준 1조 5,000억 원으로, 스캔 한 번으로 진위를 즉시 판별하는 코드·정보(히든코드 알고리즘) 기술이 가장 직접적인 대응 수단
 - 화장품·식품은 성분·유통기한 등 공급망 이력 검증 수요가 높고, 패션은 동일 상품 재활용·환류 차단이 핵심과제로, 고도화·복합(AI 판독·블록체인 이력 관리) 기술과 산업 수요가 부합
- (AI 활용 고도화 가능성) 코드·정보 및 고도화·복합은 AI 접목을 통한 고도화 가능
 - (코드·정보 분야) 기존 QR 등 단순 코드는 복제에 취약하나, 딥러닝 기반 위·변조 판별 알고리즘을 결합할 경우 복제 시 발생하는 미세 텍스처 변화를 자동 감지하는 고난도 인증으로 고도화 가능
 - (고도화·복합인증 분야) 글로벌 AI 식품 이력추적 시장(2025년 42.5억 달러 → 2026년 49.2억 달러)에서 AI·블록체인·IoT의 결합이 식품·화장품 공급망 위변조 차단의 핵심 기술 방향으로 자리잡고 있으며, 글로벌 기업의 51%가 디지털 인증에, 46%가 블록체인에 집중 투자 중
 - 두 분야 모두 AI 기술을 접목함으로써 기존 단순 인증 수준을 넘어서는 원천기술 공백 해소와 초격차 확보가 가능한 구간
- 기술성숙도, 한국 산업 특성 및 AI 활용 고도화 가능성을 종합적으로 고려했을 때, 시각·물리 및 전자·디지털 분야는 글로벌 민간기업의 기술 선점과 높은 완성도로 인해 공공 R&D 투자 효과가 제한적인 반면, 코드·정보 및 고도화·복합인증 분야는 원천기술 공백이 존재하고 AI 접목을 통한 초격차 확보가 가능

표 8. 위조방지 분야 고도화 가능성

구분	핵심 개념	기술 성숙도	한국 산업 특성	AI 활용 고도화 가능성	R&D 투자 대상
시각·물리	물리적 보안요소로 위조 억제 및 식별	홀로그램 등 글로벌 기업 선점 성숙 영역으로 공공 투자 차별화 여지 제한	위조 주 경로의 온라인 전환으로 물리적 소재 억제 효과 감소	소재 물성 개선이 핵심으로 AI 접목 고도화 여지 제한적	제외
코드·정보	고유정보 기반 정품 여부 확인	히든코드 등 일부 기술 공백 존재, 공공 R&D를 통한 원천기술 확보 가능	K-뷰티·패션·식품 등 온라인 유통 산업 구조상 스캔 기반 즉시 진위 판별 수요 높음	딥러닝 히든코드 알고리즘으로 복제 불가 고난도 인증 고도화 가능	집중 투자
전자·디지털	유통이력 추적 및 이상유통 탐지	반도체·RFID 민간 핵심 IP 집중, 국내 범용 조달 대응 가능	오프라인·온라인 이력 관리 수요 있으나 민간 솔루션으로 대응 가능한 수준	민간 기술 완성도 높아 공공 R&D AI 접목 추가 차별화 효과 미미	제외
고도화·복 합인증	첨단기술 융합 고신뢰 보호 체계	AI·블록체인·IoT 융합 분야로 기술 표준 미확립, 선도적 공공 R&D 투자 효과 높음	화장품·식품 공급망 이력 검증, 패션 재활용 차단 등 한국 주력 소비재 보호 수요에 직결	AI·블록체인·IoT 결합으로 스마트폰 연동 통합 인증 구현 및 글로벌 시장 선도 기회	집중 투자

□ [내역 2. 산업스파이 방지] 산업스파이 전주기 대응 기술로의 전환

- 최근 기술 유출은 내부자, 협력사, 클라우드 협업 환경 등 다중 경로를 통해 발생하고 있으며, 단순 사후 통제(DLP 중심) 방식으로는 선제적 대응에 한계 존재
- 생성형 AI, 원격근무, SaaS 협업툴 확산으로 데이터 이동 경로가 복잡화되면서 행위 기반 이상 탐지(UEBA), 제로트러스트 접근통제(ZTNA) 등 선제 탐지 기술의 필요성이 급증
 - 실제 글로벌 보안시장에서는 행위 기반 탐지와 제로트러스트 아키텍처가 표준 보안모델로 전환 중이며, 국내 기업은 고도화 기술 확보 측면에서 상대적으로 취약
 - 포렌식 워터마킹 등 디지털 추적 기술은 기술유출 발생 시 입증 가능성과 역지력 확보를 위한 핵심 수단으로, 단순 보안 기능을 넘어 법적 대응 기반 기술로 자리매김 중
- 이에 따라 산업스파이 방지 기술은 예방 - 탐지 - 추적 - 통합보호의 전주기 구조로 재설계할 필요가 있으며, 고난도 신기술에 대한 선제적 R&D 투자 타당성 확보

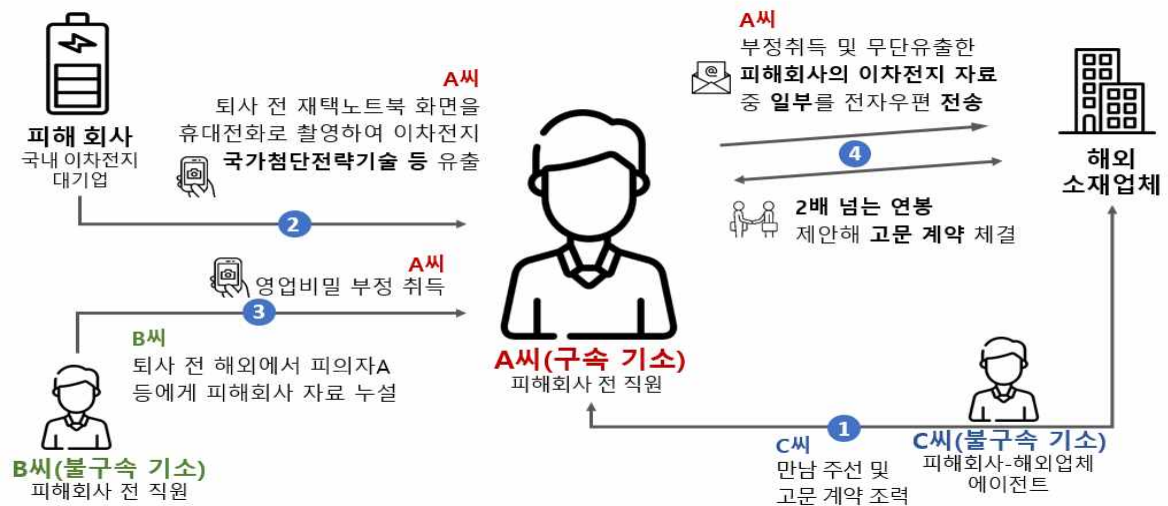
□ (지식재산처 추진의 당위성) 본 사업은 지식재산 보호 관점의 식별·인증 기술 개발

- (지식재산 법률 체계상 지재처 고유 관할) 위조방지·정품식별은 지식재산권 법률 집행의 물리적 전제 조건으로서 지재처가 담당하는 고유 업무영역
 - 상표법 제108조(침해행위), 디자인보호법 제113조, 부정경쟁방지법 제2조(부정경쟁행위) 등 지재권 보호 법률은 위조상품의 "식별 가능성"을 법 집행의 전제로 함
 - 식별 기술이 없으면 지재권 침해 사실의 물리적 입증이 불가능하여 법 집행 자체가 저해되며, 위조상품 단속·행정처분·통관 차단 등 지재권 보호 행정도 식별 기술 없이는 실효성 확보 불가
 - 따라서 위조방지·식별기술 개발은 타 부처 소관 기술이 아닌 지식재산 보호 법률·행정의 집행 기반을 구축하는 지재처 고유 사업

- **(기술유출 R&D 수행 부처 중 유일한 방첩기관)** 지식재산처는 기술안보 등 국가안보를 위한 방첩기관인 동시에 R&D 지원 사업을 수행할 수 있는 부처로서, 기술보호 분야 R&D 지원의 당위성과 실효성을 겸비한 유일한 기관
 - 지식재산처는 국정원, 법무부, 관세청, 경찰청, 해양경찰청, 국군방첩사령부에 이어 7번째 방첩기관으로 지정('23.12)되었으며, 방첩기관 중 가장 기술유출 방지에 특화된 전문성을 바탕으로 방첩기관 역할을 수행하고 있음.
 - 산업부 등 기존 R&D 부처는 방첩기관 지위를 보유하고 있지 않아 기술보호 R&D 지원의 실효성 확보에 한계를 가지는 것과 달리, 지식재산처는 기술침해·첨단기술 유출 방지 등 기술안보를 주요 목적으로 활동하는 방첩기관으로서, 기술유출 대응 과정에서 도출되는 현장 수요를 기술개발 지원 과제에 직접 반영할 수 있어 타 부처의 일반 R&D 지원과는 본질적으로 차별화
 - 이차전지·반도체 등 국가핵심기술을 겨냥한 해외 산업스파이 위협이 고도화되는 상황에서, 방첩 권한과 R&D 지원 기능을 겸비한 지재처만이 실제 수사 현장 수요에 부합하는 기술보호 R&D 과제를 기획·지원할 수 있는 적합한 주체
- **(특별사법경찰 현장 노하우의 기술개발 연계)** 지재처 소속 특별사법경찰(특사경)의 위조상품 단속 및 기술유출 수사 실무 경험을 기술개발에 직접 반영함으로써 현장 적합성 높은 차별화된 기술 개발 가능
 - (위조방지) 특사경은 위조상품 단속 현장에서 정품·위조품 식별의 실패 유형, 위변조 수법의 진화 패턴, 증거 확보의 법적 요건 등 실전 노하우를 축적하고 있으며, 이는 타 부처가 보유할 수 없는 지재처만의 고유 자산
 - 단속 현장에서 실제 식별이 곤란했던 위변조 사례와 기술적 한계를 R&D 요구사항으로 직접 전환함으로써, 실험실 중심의 일반 기술개발과 달리 현장 수요에 정확히 부합하는 식별·인증 기술 도출 가능
 - (산업스파이 방지) 특사경은 반도체·이차전지 등 국가핵심기술을 겨냥한 산업스파이 수사를 전담하며, 기술·영업비밀 유출의 수법 유형, 내부자 행위 패턴, 디지털 증거 확보의 법적 요건 등 수사 실무 노하우를 축적하고 있으며, 이는 타 부처가 보유할 수 없는 지재처만의 고유 자산
 - 실제 기술유출 수사에서 탐지가 곤란했던 이상행위 패턴과 증거 확보의 기술적 한계를 R&D 요구사항으로 직접 전환함으로써, 현장 법집행 수요에 정확히 부합하는 유출 탐지·추적 기술 도출 가능
 - 개발된 기술의 수사 현장 적용성 검증 및 피드백 환류 체계도 특사경 조직을 통해 내부적으로 구축 가능하여, 기술개발-수사운용-성능개선의 선순환 구조 실현

◆ 특사경 기술유출 적발 사례 - 이차전지 국가첨단전략기술 해외유출 적발

- (사건 개요) 지식재산처 특사경은 이차전지 국가첨단전략기술을 해외로 유출하려 한 국내 대기업 전직 팀장 A씨 등 3명 적발·기소('25.7)
- (범행 수법) 재택 노트북 화면 촬영으로 셀 설계·중장기 전략 등 핵심자료 3,000여 장 무단 반출 후 해외업체에 기술고문으로 취업, 이메일로 자료 전송
- (단속 성과) 특사경이 국정원 첩보 입수 즉시 수사 착수, 압수수색으로 증거 확보 및 관련자 3명 전원 검거해 침수조 원대 피해 사전 차단
- (처벌 결과) 주범 A씨 구속, B·C씨 불구속 기소 / 국가첨단산업법·부정경쟁방지법·업무상배임 등 적용



- ①② 피해기업의 국가첨단전략기술, 국가핵심기술 및 영업비밀 무단 유출
- ③ 피해기업의 영업비밀 부정취득 및 국외누설
- ④ 피해기업의 영업비밀 국외 부정사용

그림 19. 특사경 기술유출 적발 사례

- (타 부처 R&D와의 본질적 차별) 본 사업은 일반 연구개발과 다음과 같은 본질적 차별점을 보유하여 지재처 고유 사업 영역에 해당

표 9. 위조방지 사업의 차별성

구분	일반 소재 R&D (산업부·과기부)	본 위조방지 사업 (지식재산처)
연구 목적	소재의 기능적 성능 향상	지식재산권 침해 판별·식별
핵심 성능 지표	경도·내열성·전도성 등 소재 물성	복제저항성·판별 민감도·법정 증거력
기술 기준	재료 규격(KS M 등), 산업 표준	ISO 22383 등 위조방지 성능기준
법적 연계	산업기술 보호, 수출통제	상표·디자인·특허 등 지재권 보호
주요 수요처	제조 공정·부품 업체	브랜드 기업·관세청·단속기관·소비자
사업 결과물	소재·부품의 규격화 제품	지재권 침해 판별 가능한 인증 솔루션

□ 기술 특성에 따른 차별화된 R&D 추진체계 설계

- **(위조방지)** 기술 유형별 위험 구조와 확산 메커니즘을 반영한 차별화된 R&D 구조 설계
 - 위조방지 기술은 단일 기술요소가 아니라 물리·디지털·알고리즘이 결합된 복합 인증 구조로 설계되어야 하며, 개별 기술 간 인터페이스와 성능기준의 일관성이 확보되지 않으면 시장 신뢰 확보가 어려운 구조
 - 위조방지 분야는 PM 중심으로 사전 시나리오를 설계하고, PM이 직접 세부과제 간의 기술적 정합성을 조율하고 연계하는 통합적 역할을 수행하도록 설계
- **(산업스파이 방지)** 산업스파이 방지 기술은 국가 정책, 기밀 관리 등 정보 보안 영역의 특성과 고위험·고불확실성 구조에 대응하여 정책 지정형 R&D 체계 적용
 - 기술 유출 수법은 내부자 위협, 협력사 경유 유출, 클라우드·AI 기반 경로 등으로 빠르게 진화하고 있어 기술 성공 가능성과 시장 적합성의 불확실성이 높은 영역
 - 산업스파이 분야는 PM과 주관기관 책임자가 초기 단계에서 다수의 기술 아이디어를 병렬 탐색하고, PoC 기반 성능 검증 및 현장 적용
- **(표준화 개발)** 표준화에 부합한 기술 설계(Co-Design)를 통한 시장 신뢰 기반 확보
 - 위조방지 기술은 기술적 우수성만으로는 확산이 어려우며, 공공조달·수출입 검증 과정에서 공인 성능 기준이 확보되지 않으면 시장 채택이 제한되는 구조
 - 4대 기술유형별 성능요건(복제저항성, 판별 민감도, 내구성 등)을 구조화하고, R&D 기획 단계부터 국내·외 표준(ISO 22383)과의 정합성을 확보하여 인증·조달과 연계 가능한 체계를 사전 설계
 - 기술개발 완료 이후 표준화를 추진하는 방식이 아니라, 개발과 동시에 표준에 부합한 성능 기준을 내재화하여 시장 진입 지연 리스크를 최소화하기 위한 전략적 선택
- **(수요기반)** 수요기업 참여 및 전주기 실증 기반 확산 구조 구축
 - 기술 공급자 중심 R&D는 실제 현장 적용성과 괴리가 발생할 가능성이 높으므로, 기술이 실제로 적용될 공급망 전반이 참여하는 사용자 중심 개발 구조로 전환
 - 위조방지 분야는 사용자 시나리오 도출 → 기술 고도화 → 현장 적용으로 이어지는 실증 중심 평가 체계를 적용하여 실효성을 확보
 - 산업스파이 분야는 PoC 단계에서 실제 기업 환경 로그 및 운용 조건을 반영하여 성능을 검증함으로써 실환경 적합성을 조기에 확보
 - 중소기업의 도입 장벽을 고려하여 산업스파이 기술은 클라우드 기반 구독형(SaaS) 모델 등 보급형 구조로 확산을 유도하여 기술 접근성을 제고

□ 규제 공백 해소 및 신기술의 시장 안착을 위한 법·제도 및 확산체계 설계 병행

- 첨단 위조방지 및 산업보안 기술은 개발이 완료되더라도, 공공조달 기준 부재, 성능인증 체계 미정립 등 제도적 공백으로 인해 유통망 및 공공시장 진입에 제약 존재
 - 현행 기술유출 관련 처벌 수준 및 양형 기준은 고도화된 기술탈취 범죄의 경제적 피해 규모에 비해 억지력이 낮다는 지적 지속 제기
 - 포렌식 워터마킹 등 디지털 기반 증거 기술은 개발이 진행되고 있으나, 법정에서 무결성 및 원본 동일성 인정 기준이 명확하지 않아 기술 활용에 제도적 한계 존재
- 따라서 기술개발과 병행하여 규제요인 발굴, 법령 개선안 마련, 국가 단위 성능인증 가이드라인 설계를 추진하는 것이 필수적이며, 이는 R&D 성과의 시장 확산과 직결되는 정책적 전제조건

제2절 비전 및 목표

□ 사업비전

- 대내외 환경분석 및 SWOT 분석 결과, 지식재산 보호기술 R&D는 혁신기술 활용을 통한 선제 예방형 보호체계로의 전환이 필요한 것으로 도출
- 이에 위조방지 및 식별기술 혁신, 산업스파이 방지 기술 고도화를 핵심 축으로 사업의 비전 및 목표를 제시
- 본 사업의 비전은 ‘K-Tech & K-Brand 수호를 통한 지식재산 보호 강국 도약’이며, 목표는 ‘혁신기술 활용을 통한 지식재산 보호 강화’임

비전

K-Tech & K-Brand 수호를 통한 지식재산 보호 강국 도약

목표

혁신기술 활용을 통한 지식재산 보호 강화

사업 목표

① 위조상품
원천 차단을 위한
위조방지·식별
기술 자립화

+

② 첨단 산업기술
유출의 선제적
예방·탐지·추적을 위한
능동형 방어 기술 확보

+

③ 보안 표준·인증
패스트트랙 구축 및
수요 기반 지식재산
보호 문화 확산

추진 방향 및 핵심 추진 과제

[위조방지]

위조방지 및 식별기술 혁신

- 2대 핵심 위조방지 원천기술 개발
 - 코드·정보 기반 기술
 - 고도화·복합인증 기술

+

[산업보안]

**산업스파이 방지 기술
고도화**

- 산업스파이 전주기 방어 기술 확보
 - 사전 예방 (지능형 접근제어)
 - 실시간 탐지 (멀티모달 유출 인지)
 - 사후 추적 (디지털 마커 및 포렌식)
 - 통합 보호 (물라사이버 융합 보안 인프라)

그림 20. 비전 및 목표

제3절 핵심 추진 과제

1 위조방지 및 식별기술 연구개발

□ 2대 핵심 위조방지 원천기술 개발

- 기존 육안 식별 위주의 아날로그 보안(일반 홀로그램, QR 등)은 스마트폰 스캔조차 위조하는 가짜 사이트 연결 및 데드카피(Dead-copy) 수법 앞에서는 한계가 명확함
- 이를 극복하기 위해 물리적 복제가 원천적으로 불가능한 핵심 기술 중심으로 기술개발 및 고도화 추진
 - * 글로벌 위조상품 경제 규모는 1.7조 달러 이상으로 급증, LVMH, 까르띠에 등 글로벌 명품 기업들은 아우라(Aura) 블록체인을 통해 제품의 생산부터 유통까지 전 과정을 디지털로 추적하여 위조품 혼입을 원천 봉쇄 중임

표 10. 위조방지 원천기술 구분

구분	추진방향	기술개발 내용(예시)
코드·정보 기반 기술	무단 복제 및 악의적 유포를 막기 위해, 스캔 시 위·변조를 실시간으로 판별하는 지능형 알고리즘 및 히든 코드 적용	• 비가시 식별자(Hidden Code) 내재화 : 포장재나 제품 디자인 내에 육안으로 식별이 불가능한 '숨은 암호코드'를 삽입하는 기술 • 실시간 교차 검증 알고리즘 : 고유 난수 기반 암호 코드를 스마트폰으로 스캔 시 서버와 실시간으로 대조하여 정품 여부와 복제 여부를 즉각 판별하는 시스템 • 가짜 사이트 우회 차단 : 단순 QR코드 복사를 통한 피싱(가짜 인증 사이트 연결)을 막기 위한 동적(Dynamic) 코드 생성 및 URL 인증 기술
고도화·복합 인증 기술	물리적 보안 요소와 디지털 인증 데이터가 유기적으로 결합된 '피지털(Phygital)' 융복합 보안 기술로 발전시켜 스마트폰 등 보편적 기기로 판독 가능하도록 구현	• 물리-디지털 1:1 매칭(Physical Fingerprint) : 제품 가공 과정에서 자연 발생하는 무작위 고유 패턴을 추출해 디지털 코드와 일대일로 연동하는 다중 인증 체계 구축 • AI 기반 모바일 정밀 감별 : 특수 장비 없이 스마트폰 카메라만으로 라벨의 폰트, 인쇄 윤곽, 미세 워터마크 등을 오차율 1% 미만 수준으로 정밀 판독하는 딥러닝 영상 인식 기술 • 블록체인 기반 공급망 무결성 연동 : 제품의 생산-유통-소비 순주기의 검증 로그를 위·변조가 불가능한 블록체인에 기록하여 실시간 추적을 지원하는 플랫폼 기술

□ 자유공모를 통한 현장 수요 기반 위조방지 기술개발 및 실증 체계 구축

- 국내 위조방지 기술개발은 특정 보안 소재나 라벨 등 요소기술 중심의 R&D에 머물러 실제 산업현장이나 소비자 인증 환경과 단절되는 실증 공백 현상이 발생하고 있음
 - * 2025년 기준 관세청 통관 단계에서 적발된 K-브랜드 위조물품은 총 11만 7,005점(정품 가액 약 4,326억 원)에 달하며, 중소기업 중심의 단편적 솔루션 도입만으로는 쪼개기 유통 등 고도화된 공급망 침투를 방어하기 어려움
- (자유공모 방식의 현장 수요 발굴) 산업현장의 다양한 위조방지 기술 수요를 자유공모 방식으로 광범위하게 수렴하여, 기술적 완성도와 현장 적용 가능성을 종합적으로 평가·선별함으로써 수요 지향형 R&D

과제를 발굴

- **(PM 주도형 기술개발)** 각 기술분야별로 PM(Project Manager)을 지정하여 PM이 직접 세부과제 간의 기술적 정합성을 조율하고 연계하는 통합적 역할을 수행
- **(공급망 전주기 실증)** 최종 수요기업의 컨소시엄 참여를 의무화하고, 현장 실증 중심의 R&D를 추진하여 상용화 가능성을 극대화함

□ **(수행방식) 자유공모를 통한 현장 수요 기반 기술개발 및 PM 주도 통합 관리**

- 위조방지 기술은 공급자 참여 저변이 충분히 확보되어 있어 자유공모 방식으로 다양한 주체의 창의적 기술 아이디어를 수렴하고, PM이 선별된 과제 간 기술적 정합성 조율 및 통합 실증을 관리하는 방식으로 추진
- PM(Project Manager)이 2대 기술유형별 세부과제의 구성·조율·통합 관리를 주도하며, 기술 간 인터페이스와 통합 실증을 관리
- 2026년 하반기 전문가위원회를 집중 운영하여 자유공모 과제 심사 기준 및 분야별 평가 방향을 수립하고, PM 운영체계 구축을 완료할 예정

□ **(2대 기술분야 도출 근거) 특허 빅데이터 분석 기반 핵심기술 후보 도출 → 한국 산업 특성 및 AI 활용 고도화 가능성 기반 2대 집중 투자 분야 도출**

- 본 사업의 2대 핵심 기술분야는 지식재산처의 고유 역량인 특허 빅데이터를 분석하여 객관적·과학적으로 도출되었으며, 최신 기술 동향과 국내 기술 수준을 종합 반영
- * 특허 분석은 산업재산정보법('24.8 시행)에 따라 지식재산처장에게 부여된 고유 업무영역으로, 특허 기반 기술 도출은 타 부처가 수행할 수 없는 차별적 기획 역량

□ **(특허분석 4단계 프로세스) 본 사업은 최근 특허 데이터 분석을 기반으로 핵심 기술분야 후보를 도출하였으며, 그 과정은 다음과 같음**

- **(1단계)** 특허 SNA 분석 : 위조방지·식별 분야 관련 IPC/CPC 특허분류코드 기반 전 세계 특허 데이터를 수집하여 키워드·인용·공동출원 네트워크 분석을 통해 기술 군집 및 핵심 기술영역을 시각화
- **(2단계)** LDA 및 워드클라우드 분석 : 수집된 특허의 청구항·요약·기술 설명 텍스트에 대해 토픽 모델링 (LDA) 및 워드클라우드 분석을 수행하여 주요 기술 토픽과 신흥 키워드를 도출
- **(3단계)** 핵심특허 분석 및 전문가 활용 : 도출된 기술영역별 핵심특허 및 주요 출원인을 분석하고, 산·학·연 전문가 협의체를 통한 기술 영향력·파급력 검증 수행
- **(4단계)** 주요 테마 후보 도출 - 분석 결과를 종합하여 시장 수요·기술 파급력·국내 기술역량을 고려한 기술분야(테마) 후보 도출

□ **(위조방지 분야 특허분석 특화 방향) 한국 주력 소비재 타게팅 및 차세대 원천기술 중심**

- 한국 산업의 특성을 반영하여 K-브랜드 주력 소비재(화장품·패션·식품·의약품 등) 위조 대응 기술 영역을 집중 분석
- 글로벌 위조상품 경제 규모가 1.7조 달러 이상으로 급증하는 가운데, 한국 기업의 위조상품 피해 규모는 약 11조 원에 달하며 화장품·패션·식품·전자제품 등 소비재 분야 피해가 집중
- 유럽(명품), 미국(의약품·전자) 등 국가별 주력 산업과 위조 대응 기술 개발 방향이 상이한 점을 반영하여, 한국은 K-콘텐츠·K-뷰티·K-푸드 등 한류 소비재 산업의 위조 대응에 특화
- 홀로그램·RFID 등 기존 상용화 기술을 뛰어넘는 차세대 원천기술 확보를 목표로 특허분석 범위 설정

- 기존 상용 기술(일반 홀로그램, QR코드, 기본 RFID)은 이미 위조업자의 데드카피(Dead-copy) 및 가짜 사이트 연결 수법에 무력화됨에 따라, 물리적 복제 자체가 원천 불가능한 기술군을 중심으로 분석
- 나노 광학 소재, 메타물질, PUF(물리적 복제방지) 칩, AI 기반 정밀 감별, 블록체인 기반 공급망 추적 등 차세대 기술영역에 특허분석 범위 집중
- 수요실증형 R&D 구조로 설계하여 한국 주력 소비재 산업의 실제 위조 피해 상황에 기반한 시나리오 도출
 - 수요기업(화장품·패션·식품·제약 등) 컨소시엄 참여를 필수화하고, 실제 유통 환경에서의 현장 실증을 기술개발의 핵심 단계로 포함
 - 관세청 통관·플랫폼사업자·유통사 등 위조 차단 현장 기관을 실증 파트너로 포함하여 통관-유통-소비 전주기의 실효성 확보
- 특허분석 결과를 수요조사 결과와 교차검증하여 공급자·수요자 관점이 모두 반영된 시장 수요 부합 기술 후보군 도출

□ (기술분야 후보) 시각·물리 / 코드·정보 / 전자·디지털 / 고도화·복합

표 11. 위조방지·정품식별 분야 기술분야 후보 및 도출 근거

기술분야 후보	핵심 방향성	특허분석 기반 도출 근거
시각·물리 기반	나노 광학 소재·메타물질 기반 물리적 복제불가 기술	광학·메타물질·보안잉크 등 소재 기반 특허 집적도 높음, 선도국 대비 원천기술 확보 필요
코드·정보 기반	동적 코드·공급망 추적 등 디지털 정보 기반 인증	블록체인·공급망 추적·SBOM/HBOM 등 디지털 인증 특허 급증
전자·디지털 태그	PUF 칩·고신뢰 하드웨어 인증 기술	PUF·반도체 칩 보안·하드웨어 트로이 탐지 등 하드웨어 보안 특허 집중도 뚜렷
고도화·복합 인증	AI·블록체인·피지컬 융합 인증	생성형 AI·멀티모달·블록체인 기반 복합 인증 특허 증가, 수요기업 선호도 최상위

- (2개 기술분야 선정) 한국 산업의 특성과 AI 활용 고도화 가능성을 고려하여 2개 집중 투자 분야 분야(코드·정보, 고도화·복합인증) 선정
- 기술성숙도, 한국 산업 특성 및 AI 활용 고도화 가능성을 종합적으로 고려했을 때, 시각·물리 및 전자·디지털 분야는 글로벌 민간기업의 기술 선점과 높은 완성도로 인해 공공 R&D 투자 효과가 제한적인 반면, 코드·정보 및 고도화·복합인증 분야는 원천기술 공백이 존재하고 AI 접목을 통한 초격차 확보가 가능

표 12. 집중 투자 분야 선정

구분	핵심 개념	기술 성숙도	한국 산업 특성	AI 활용 고도화 가능성	R&D 투자 대상
시각·물리	물리적 보안요소로 위조 억제 및 식별	홀로그램 등 글로벌 기업 선점 성숙 영역으로 공공 투자 차별화 여지 제한	위조 주 경로의 온라인 전환으로 물리적 소재 억제 효과 감소	소재 물성 개선이 핵심으로 AI 접목 고도화 여지 제한적	제외
코드·정보	고유정보 기반 정품 여부 확인	히든코드 등 일부 기술 공백 존재, 공공 R&D를 통한 원천기술 확보 가능	K-뷰티·패션·식품 등 온라인 유통 산업 구조상 스캔 기반 즉시 진위 판별 수요 높음	딥러닝 히든코드 알고리즘으로 복제 불가 고난도 인증 고도화 가능	집중 투자
전자·디지털	유통이력 추적 및 이상유통 탐지	반도체·RFID 민간 핵심 IP 집중, 국내 범용 조달 대응 가능	오프라인·온라인 이력 관리 수요 있으나 민간 솔루션으로 대응 가능한 수준	민간 기술 완성도 높아 공공 R&D AI 접목 추가 차별화 효과 미미	제외
고도화·복합인증	첨단기술 융합 고신뢰 보호 체계	AI·블록체인·IoT 융합 분야로 기술 표준 미확립, 선도적 공공 R&D 투자 효과 높음	화장품·식품 공급망 이력 검증, 패션 재활용 차단 등 한국 주력 소비재 보호 수요에 직결	AI·블록체인·IoT 결합으로 스마트폰 연동 통합 인증 구현 및 글로벌 시장 선도 기회	집중 투자

2 산업스파이 방지기술 연구개발

□ 산업스파이 전주기(예방·탐지·추적) 방어 기술 확보

- 기존의 사후 적발 위주의 보안시스템이나 단순 네트워크 접근 통제만으로는 첨단 산업기술 유출 시도를 원천 차단하는 데 한계가 명확함
- * 최근 5년간(2020~2024) 적발된 산업기술 해외 유출 시도는 총 111건이며, 이 중 ‘내부자에 의한 유출’이 70% 이상을 차지함. USB 반출 등 물리적 수단을 넘어 캡처, 화면 촬영, 소스코드 분할 반출 등 우회 기법이 고도화되어 선제적 방어 기술이 시급함
- 이를 위해 △제로 트러스트 기반 사전 예방, △멀티모달 실시간 탐지, △디지털 마커 기반 사후 추적 및 △통합 보호를 아우르는 지능형 보안 핵심기술 확보

표 13. 산업스파이 방지기술 기술개발

구분	추진방향	기술개발 내용(예시)
사전 예방 (지능형 접근제어)	신뢰 기반 통제를 벗어나, 사용자의 행위 맥락을 실시간으로 분석하는 제로 트러스트(Zero-Trust) 아키텍처 도입	• AI 기반 동적 접근 제어 : 평소 업무 패턴과 다른 이상 접근(심야 시간대 핵심 도면 대량 열람 등)을 AI가 인지하여 즉각적으로 열람 권한을 차단·축소하는 능동형 제어 기술 • 생체인증 우회 방어(Liveness Detection : 딥페이크나 위조 생체정보를 활용한 비인가자의 시스템 접근을 차단하기 위한 고도화된 안면·음성 복합 위변조 탐지 기술
실시간 탐지	망분리 환경을 우회하는 물리적·소프트웨어적 유출	• Vision AI 융합 화면 촬영 방지 : 스마트폰 카메라 렌즈의 반사광이나 촬영 모션을 시각 지능(Vision AI)으로 즉각 인식하여,

(멀티모달 유출 인지)	행위를 실시간으로 인지·차단하는 엔드포인트 단말 보안 고도화	PC 화면을 자동으로 블라인드 처리하는 물리적 유출 차단 기술 • 멀티모달 이상 행위 탐지 : 비인가 원격 프로그램 실행, 클립보드 복사, 캡처 등 복합적인(Multi-modal) 소프트웨어적 이상 행위를 프로세스 단위에서 실시간 탐지 및 차단하는 알고리즘
사후 추적 (디지털 마커 및 포렌식)	유출된 데이터의 출처와 유출자를 정확히 역추적하고, 법적 증거력을 확보할 수 있는 무결성 검증 체계 구축	• 비가시성 디지털 워터마크(Invisible Watermark) : CAD 도면, 반도체 설계도, 핵심 소스코드 내부에 육안이나 일반 소프트웨어로는 식별이 불가능한 고유 마커를 삽입하여, 유출 후 파일이 분할·변형되더라도 원본 출처를 추적하는 기술 • 블록체인 기반 보안 로그 포렌식: 데이터 열람, 복사, 반출 등의 모든 이력을 위·변조가 불가능한 블록체인에 기록하여 산업스파이 수사 시 법적 증거 능력을 확보하는 추적 플랫폼
통합 보호 (물리·사이버 융합 보안 인프라)	사전 예방·실시간 탐지·사후 추적 기술을 단일 플랫폼으로 통합하여, 기술유출 전주기 대응이 가능한 지능형 통합보안 인프라 구현	• 전주기 통합 보안 플랫폼 : 제로트러스트 접근제어(예방) + Vision AI 탐지(탐지) + 디지털 워터마크(추적)를 단일 관제 체계로 연동하여 유출 시도를 탐지부터 증거확보까지 자동화하는 통합 플랫폼 기술 • 자율형 융합 방어 및 접근 통제: 드론로봇 기반 시설 보안 감시로 침입을 자동 탐지하고, 침입 발생 시 제로트러스트 기반의 데이터 접근 차단과 위치기반 스마트 단말 기능 통제를 즉각 실행하여 물리적 침입이 데이터 유출로 이어지는 것을 원천 차단하는 기술

□ 전략적 상세 기획 및 PM 주도형 전주기 실증 체계 확립

- 기존 보안 기술 R&D는 개발 완료 시점에 이미 기술이 구식화되거나, 수요기업의 실제 내부망 인프라와 호환되지 않아 상용화율이 저조한 '실증 갭(Gap)' 문제가 지속 발생
- 산업보안 분야는 해킹 및 유출 기법의 진화 속도가 매우 빨라, 실제 산업현장의 요구사항과 최신 위협에 민첩하게 대응하기 어려움

□ (과제 구성안 도출) 기획위원회 등을 통해 4대 기술 테마 및 과제 구성안 도출하고, 보안 기술의 기밀성 유지를 위해 별도 공모 없이 지식재산처가 역량 검증된 수행기관을 직접 지정하는 '정책지정' 방식으로 추진

* [사전 기획 운영] 2026년 하반기 전문가위원회를 집중 운영하여 4대 기술 유형별 실효성 있는 R&D 시나리오 도출 및 상세 과제 기획을 완료할 예정임

- **(PM 주도형 기술개발)** 각 기술 테마별로 PM(Project Manager)을 지정하여 PM이 직접 세부과제 간의 기술적 정합성을 조율하고 연계하는 통합적 역할을 수행
- **(공급망 전주기 실증)** 최종 수요기업의 컨소시엄 참여를 의무화하고, 현장 실증 중심의 R&D를 추진하여 상용화 가능성을 극대화함

□ (추진 당위성 및 타 부처 사업과의 차별성) 지식재산처 고유 영역인 특허·영업비밀 중심의 기술유출 방지 기술개발

- 기술유출의 66%가 영업비밀 침해(부경법 위반)인 구조에서 기술보호의 본류는 지식재산 보호이며, 본 사업은 특허·영업비밀 침해 대응 기술에 특정된 지식재산처 고유 영역 중심으로 추진
- * '25년 경찰 송치 기술유출 사건 최종 구성: 부경법 위반 118건(66%), 산업기술보호법 22건(13%), 형법 등 39건(22%), 총 179건 (출처: 경찰청)

- 기술 유출의 대다수를 차지하는 영업비밀 특허 아이디어 탈취 등의 기술유출 유형은 지재처 소관이며, 산업기술보호법 중심의 국가핵심기술(본질적으로는 지식재산권에 해당) 유출은 전체 기술유출의 13%에 불과
- 본 사업은 지식재산권 침해를 구체적 보호대상으로 특정하여 "특허 도용·영업비밀 유출 방지" 기술 개발을 중심으로 추진되며, 이는 타 부처 사업과의 본질적 차별점
- 산업재산정보법('24.8 시행)에 따라 지식재산처장만이 출원 중인 미공개 특허정보를 기술유출 방지 목적으로 분석·이용할 수 있는 법적 권한을 보유하여, 특허기반 기술유출 방지 기술개발은 지재처 고유 업무영역

표 14. 부처 기술유출 대응 사업과의 차별성

부처	담당 영역	본 사업과의 관계
산업통상자원부	국가핵심기술(NCT) 지정·관리, 보유기관 수출통제	NCT 지정/관리는 산업부, 지재권 침해 방지 기술개발은 지재처
과학기술정보통신부	대학·공공연 연구보안 체계 구축	연구현장 보안관리는 과기부, 지재권 기반 기술유출 방지 기술개발은 지재처
중소벤처기업부	중소기업 기술탈취 행정조사·구제	피해 구제는 중기부, 예방·탐지 기술개발은 지재처
국가정보원	기술유출 첩보 수집·수사	수사 첩보는 국정원, 이를 뒷받침할 특허·영업비밀 기반 분석기술 확보는 지재처
경찰청·검찰청	기술유출 수사, 국제공조	수사는 경·검, 수사에 필요한 디지털 증거 확보·포렌식 기술개발은 지재처

□ (수행방식) 정책지정형 추진

- 수요조사 결과 공급-수요 비대칭 구조로 인하여 역량 있는 수행기관의 자발적 참여를 유인하기 어려우며, 수요 대응이 구조적으로 지연될 가능성
 - 참여기업 대상 산업스파이 방지 분야 참여의향 긍정응답 40.0%로 위조방지 분야(60.0%) 대비 현저히 낮음
 - 수혜기업의 산업스파이 방지 성과물 도입의향 긍정응답은 88.9%로 위조방지 분야(69.5%)를 크게 상회
- 한국 사이버보안 분야는 글로벌 수준에 못 미치므로 원천기술 확보를 위한 정책주도의 기술개발 추진 필요
 - 12대 국가전략기술 중 한국의 특허 출원(KR/IP5) 비중은 사이버보안 분야가 평균 7.7%로 차세대통신·반도체(15% 이상) 등 대비 현저히 낮은 수준
 - 세부적으로 디지털 취약점 분석·대응(공급망 보안) 분야는 한국 점유율 5.8%에 불과, 글로벌 경쟁에서 원천기술 확보가 시급

표 15. 12대 국가전략기술 중 한국 특허 출원 비중 비교

순위	기술분야	KR 비중	순위	기술분야	KR 비중
1	차세대원자력	17.8%	7	수소	10.4%
2	첨단로봇·제조	17.0%	8	첨단모빌리티	10.1%
3	반도체·디스플레이	15.6%	9	인공지능	9.5%
4	이차전지	13.7%	10	사이버보안	7.7%
5	차세대통신	12.3%	11	양자	7.2%
6	첨단바이오	9.1%	12	우주항공·해양	4.9%

* 출처 : '03~'22년 국가전략기술 중점기술별 출원 통계
(KR IP-R&D 출원 / IP5 IP-R&D 전체 출원 비중)

- 보안 특성에 따른 전략적 역량 결집 필요로 인한 개발 과정 및 성과물의 고도 보안 관리 요구
 - 산업스파이 방지 기술은 개발 과정 및 성과물이 고도의 보안 관리 대상으로, 공개 공모 방식은 보안 리스크 유발 가능
 - 정책지정형을 통해 역량 검증된 수행기관(출연연·대학·기업)을 선별 지정함으로써 사업 목표 달성과 보안성 양립 실현

□ (4대 기술분야 도출 프로세스) 특허 빅데이터 분석 기반 객관적·과학적 도출

- 본 사업의 4대 핵심 기술분야는 지식재산처의 고유 역량인 특허 빅데이터 분석을 통해 도출되었으며, 내역1(위조방지)과 동일한 4단계 프로세스 적용

□ (산업스파이 분야 특허분석 특화 방향) 기 상용화 기술 고도화 및 지식재산 보호 관점 특화

- DLP·DRM 등 이미 상용화된 기술에 대해 국내외 최근 5년 특허 출원 동향을 정밀 분석하여 기존 상용 솔루션이 포착하지 못하는 고도화 포인트(Zero Trust, UEBA, PQC, Adaptive Deception 등) 도출
 - 기존 상용 DLP·DRM은 파일·문서 단위의 정적 통제에 중점을 두어, 특허 출원 전 핵심 기술정보의 암묵지적 유출, 영업비밀의 부분적 변형 유출, 핵심 연구인력 이동을 통한 간접 유출 등에 대한 대응 한계
 - 본 사업은 특허·영업비밀 등 지식재산의 법적 보호요건과 부합하는 방향으로 기술을 재설계하여, 지식재산 침해의 입증·추적·예방에 최적화된 기술 고도화 추진
- 보호대상을 지식재산권 침해(특허 도용·영업비밀 유출)로 특정하여 타 부처 사업과의 본질적 차별성 확보
 - (데이터 통제·권한 지능화) 영업비밀 해당 정보 식별·분류 지능화 및 특허 출원 전 기술정보의 단계적 접근통제 기술
 - (지능형 이상행위 탐지) 특허·영업비밀 관련 대량 열람·반출 등 지식재산 침해 전조 행위에 특화된 UEBA 모델 개발
 - (유출 추적·디지털 증거 확보) 부정경쟁방지법상 영업비밀 침해죄 입증에 법정 증거능력을 갖춘 포렌식 워터마킹 및 산업재산 침해 디지털 증거 체인 기술
 - (물리·사이버 융합 보안) 특허 출원 전 연구개발 현장(R&D 실험실·설계 부서 등) 특화 보안구역 통합관리 기술

□ (도출된 4대 기술분야) 데이터 통제·권한 지능화 / 지능형 이상행위 탐지 / 유출 추적·디지털 증거 / 물리·사이버 융합 보안

표 16. 산업스파이 방지 분야 4대 핵심 기술분야 및 도출 근거

4대 분야	핵심 방향성 (대응 단계)	특허분석 기반 도출 근거
데이터 통제·권한 지능화	Zero Trust 기반 동적 접근통제 (사전 예방)	DLP·DRM 고도화, 동적 권한부여 관련 특허 급증
지능형 이상행위 탐지	UEBA·AI 기반 위험예측 (실시간 탐지)	UEBA, 생성형 AI 대응 관련 핵심특허 집중
유출 추적·디지털 증거 확보	포렌식 워터마킹·법정 증거력 (사후 대응)	포렌식 워터마킹, 블록체인 증거체인 특허 확대
물리·사이버 융합 보안 인프라	CPS 보안·촬영 탐지 (통합 보호)	OT/ICS 보안, 물리·사이버 통합 인프라 특허 증가

□ (특허분석 기반 40개 유망 후보과제) 4대 기술분야별 상세 리스트

- 특허 빅데이터 분석을 통해 도출된 40개 후보과제를 4대 기술분야별로 배분한 결과는 아래와 같으며, 2026년 하반기 PM을 통해 분야별 3개 컨소시엄에 해당하는 세부 RFP를 상세 도출 예정

표 17. 특허분석 기반 산업스파이 방지기술 유망 후보과제(안)

구분	과제명
1. 데이터 유출방지 기술 (DLP)	생성형 AI(LLM) 환경에서의 데이터 거버넌스 및 민감정보 보호·활용 통합 플랫폼
	하이브리드·멀티클라우드 환경에서의 데이터 이동 경로 가시화 및 제어 기술
	SBERT 기반 비정형 국가핵심기술 문서 자동 분류 및 동적 레이블링 기술
	SaaS 및 협업 도구 환경에서의 데이터 전주기 보안 관리 및 접근권한 통제 기술
	글로벌 공급망 협업 환경에서의 기술 데이터 안전 공유를 위한 가상 샌드박스 기술
	암호화 트래픽 환경에서의 행위 기반 데이터 유출 탐지 및 가시성 확보 기술
	양자내성암호(PQC) 기반 데이터 저장·전송 구간 무결성 보장 기술
	데이터 중심 제로트러스트 기반 접근 통제 및 실시간 권한 회수 기술
	모바일 및 BYOD 환경에서의 기업 핵심 데이터 격리 및 유출 방지 기술
	데이터 사용권 추적 및 정책 기반 자동 폐기 제어 기술
2. 지능형 이상행위 탐지 기술 (UEBA)	행위 및 업무 컨텍스트 기반 내부자 위협 사전 탐지 기술
	그래프 신경망(GNN) 기반 조직 내 정보유출 공모 행위 탐지 기술
	적응형 기만(Adaptive Deception) 기반 내부 위협 유도 및 공격자 행위 분석 기술
	비대면 근무 환경에서의 행위 기반 생체 인증 기술
	클라우드 네이티브 환경에서의 비정상 접근 및 권한 오남용 탐지 기술
	이상행위 발생 시 보안 정책 자동 대응 및 유출 경로 차단 기술
	비식별 보안 로그 기반 프라이버시 보존형 행위 분석 및 위험도 평가 기술
	지능형 위협 대응을 위한 행위 기반 분석 및 자동 대응 기술
	고권한 사용자 대상 비정상 데이터 접근·조작 탐지 기술
	엔드포인트 환경에서의 경량 이상행위 탐지 기술

구분	과제명
3. 유출 추적·디지털 증거 확보 기술	화면 촬영 유출 대응을 위한 디지털 포렌식 워터마킹 기술
	생성형 AI 기반 디지털 증거 위변조 탐지 및 무결성 검증 기술
	블록체인 기반 국가핵심기술 유통 이력 추적 플랫폼
	클라우드 환경에서의 휘발성 데이터 수집 및 분석 자동화 기술
	소스코드 유출 대응을 위한 코드 지문 분석 및 역추적 기술
	다크웹 및 비가시 네트워크 기반 유출 정보 탐지 및 유통 경로 분석 기술
	멀티미디어 파일 기반 비가시 워터마킹 및 유출 추적 기술
	유출 사고 대응을 위한 디지털 포렌식 데이터 자동 수집 및 분석 기술
	분산 환경에서의 디지털 증거 신뢰성 보장 및 원격 포렌식 관리 기술
	모바일 기기 대상 비파괴 데이터 복구 및 포렌식 분석 기술
4. 물리·사이버 융합 보안 인프라 기술	위치기반 보안구역 내 스마트 단말 기능 통제 기술
	생체정보 기반 다중 인증 및 출입통제 기술
	AI 기반 RF 스펙트럼 분석을 활용한 불법 무선장치 탐지 기술
	드론 및 로봇 기반 시설 보안 감시 및 침입 탐지 기술
	멀티모달 영상 분석 기반 이상행동 및 침입 탐지 기술
	OT/ICS 환경에서의 물리·사이버 데이터 무결성 검증 기술
	물리·사이버 보안 로그 통합 상관분석 플랫폼
	침입 발생 시 데이터 접근 차단 자동화 기술
	망분리 및 VDI 환경에서의 정보 유출 방지 기술
	제로트러스트 기반 물리·사이버 통합 보안 체계

제4절 추진전략

□ (전략1) 위조방지·산업보안 통합 보호 생태계 구축

- **(단절된 보호 체계의 한계)** 위조상품 유통과 산업기술 유출은 그동안 각각 별도로 분절 대응되어 왔으나, 두 침해 유형은 우리 기업의 핵심 가치(브랜드, 기술 등)를 동시에 훼손하고 수출 경쟁력을 저해하는 공통 구조를 가짐
 - 위조상품 대응은 단속·컨설팅 위주의 사후 행정 중심, 산업기술 보호는 물리보안 중심의 제도적 대응에 머물러, 기술 기반의 선제 예방 체계가 공통적으로 부재한 상황
 - * '20~'24년 기술유출 피해 약25조 원, 위조상품 피해 약11조 원 등 합산 37조 원의 연간 피해가 발생하고 있으나, 이를 기술적으로 예방하는 R&D 투자는 전무함
- **(통합 대응의 필요성)** 위조상품과 산업스파이는 침해 대상은 다르나, 「K-브랜드·K-Tech 핵심 가치 훼손」이라는 단일 위협 구조로 수렴되며 다음과 같은 공통 기술 기반을 공유함
 - 블록체인 기반 무결성 검증, AI 기반 이상 판별, 디지털 포렌식 워터마킹 등 핵심 기반기술이 위조방지와 산업보안 양 분야에 공통 활용되어, 단일 사업 프레임 하에서 시너지 창출이 가능

표 18. 위조방지·산업보안 공통 구조

구분	위조방지(내역1)	산업보안(내역2)
침해 대상	브랜드·제품	핵심기술·영업비밀
기술 방향	식별·차단	예방·탐지·추적
공통 기반	AI 판별, 블록체인, 워터마킹	AI 탐지, 블록체인, 워터마킹·포렌식

□ (전략2) 기술 특성에 따른 Two-Track 추진체계 설계

- **(단일 방식 적용의 한계)** 위조방지 기술과 산업보안 기술은 수요 구조, 기술 완결성 요건, 위협 변화 속도가 본질적으로 상이하여, 동일한 공모 방식 및 R&D 구조를 획일 적용하면 각 분야의 목표 달성이 구조적으로 불가능함
 - 위조방지 기술은 2대 유형(코드·정보, 고도화·복합인증)이 유기적으로 결합되어야 위조 차단 실효성이 확보되는 시스템적 완결성 필요
 - * 완전 분산형 자유공모 시 기술 간 정합성을 담보할 조율 주체가 없어 성과 파편화가 우려되므로 2대 기술로 최소한의 범주화 필요
 - 산업보안 기술은 생성형 AI 악용, 클라우드 우회, 딥페이크 인증 탈취 등 위협이 하루가 다르게 진화하는 분야로, 정부가 사전에 기술개발이 필요한 테마를 지정하고, 기술 검증과 실증을 연속으로 진행함으로써, 사업화 성공 가능성을 제고할 필요
- **(Two-Track 추진체계)** 두 내역사업의 기술 특성에 맞는 이원화된 추진체계를 설계하여 각 분야의 목표 달성 가능성을 극대화함
 - **(내역1)** 다양한 주체의 창의적 기술 아이디어를 자유공모 방식으로 수렴하고, PM이 과제 선별·조정 및 세부기술 간 통합 실증을 관리하여 위조방지 기술의 현장 적용성과 시스템 완결성을 동시에 확보
 - **(내역2)** 대응 단계(예방-탐지-추적)별 기술 테마 및 과제 구성안을 사전 설계하고, 보안 기술의 기밀성

유지를 위해 별도 공모 없이 지식재산처가 역량 검증된 수행기관을 직접 지정하는 ‘정책지정’ 방식으로 추진

표 19. Two-Track 추진체계

구분	내역 1 (위조방지 및 식별)	내역 2 (산업스파이 방지)
공모 방식	자유공모	정책지정
선택 이유	현장 수요 기반 다양한 기술 아이디어 발굴 및 PM 주도 통합 실증 조율 필요	기밀성 확보 및 역량 기관 전략적 결집 필요
R&D 구조	자유공모 과제 선별PM 조정 기반 과제 구성	기술 테마 기반 수행기관 직접 지정
선정 기준	기술 혁신성·현장 적용 가능성·수요기업 연계	보안 역량·현장 실증 적합성
수요 연계	수요기업 참여 의무화	산업현장 실증 중심

□ (전략3) 연구성과의 현장 안착을 위한 성과확산 메커니즘 구축

- (기술개발-현장 적용 단절 문제) 정부 R&D 성과가 개별 과제 수준에 머물러 실제 기업 현장에 적용 및 확산되지 못하는 구조적 문제는 보안 및 위조방지 분야에서 더욱 심각하게 나타남
 - 수요기업은 검증되지 않은 기술의 보안 인프라 도입을 기피하는 경향이 있어, 공신력 있는 성능 인증 체계 없이는 시장 자연 확산을 기대하기 어려운 구조
 - 기존 비독점 통상실시 중심의 성과 이전 방식은 수요기업의 기술 도입 투자 유인을 약화시켜 자발적 상용화를 저해
- (성과확산 메커니즘 3단계 설계) 「기술개발 → 인증 → 현장 적용」의 전주기 확산 체계를 사업 기획 단계부터 설계하여 내재화함

표 20. 성과확산 메커니즘 3단계 설계

단계	추진 내용	핵심 목표
1단계 수요 연계형 실증	수요기업 컨소시엄 참여 의무화, 착수 시점부터 현장 수요 반영, 기술 적용 시나리오 공동 개발	R&D-현장 단절 방지
2단계 성능 인증 패스트트랙	국가 공인 성능 평가 가이드라인 및 인증 체계를 R&D와 병행 구축, 개발 완료 즉시 인증 취득 가능 구조 마련	시장 진입 장벽 해소
3단계 독점적 통상실시권 도입 추진	R&D 협약 시 실증 기여 수요기업에 한시적 독점 통상실시권 부여 추진 (법령 정비 선행 필요)	조기 상용화 유인 강화

- (독점적 통상실시권) 비독점 통상실시 중심의 현행 성과이전 방식은 수요기업의 상용화 투자 유인을 구조적으로 약화시켜, 우수한 기술이 개발되더라도 시장 확산으로 이어지지 못하는 근본 원인으로 작용함
 - 동일 기술을 복수의 기업이 동시에 활용할 수 있는 비독점 구조에서는, 기술 도입 초기의 경쟁 우위 확보가 불가능하여 막대한 현장 도입 비용을 부담할 유인이 약화됨
 - 위조방지 기술과 산업보안 기술은 기업 내부의 보안 인프라와 긴밀하게 통합되어야 효과를 발휘하는 특성상, 수요기업의 자발적 투자와 깊은 기술 수용이 상용화의 핵심 요건
- * (미국 Bayh-Dole Act(1980)의 시사점) 미국은 정부 R&D 성과의 상용화 부진 문제를 해결하기 위해 Bayh-Dole Act를 제정하여 연구기관이 연방 지원 특허를 보유하고 민간에 독점 실시권을 부여할 수 있도록 허용
- 국가연구개발혁신법 제18조 제1항은 「연구개발성과 소유기관은 실시하려는 자와 실시권의 내용 및

범위에 관한 계약을 체결하고 실시를 허락할 수 있다」고 규정함

- 동 조항은 실시권의 '내용 및 범위'를 협약으로 정할 수 있다고 규정하여, 독점 실시를 명시적으로 금지하고 있지 않음
- 산업기술혁신사업 공통운영요령 제37조의2에서는 참여기업에 대한 '우선실시권'을 이미 인정하고 있어, 독점적 통상실시는 이를 한 단계 강화한 개념으로 제도적 연속성이 존재함
- * 다만 독점 실시를 명시적으로 허용하는 조항이 없어 법적 해석 확인 필요

제4장 기대효과

제1절 기술적 효과

해외 위조방지 원천기술의 국산화 및 지능형
산업스파이 방지기술의 독자 확보로 기술 자립화를 실현하고
고도화되는 침해 수법에 대한 선제적 대응 역량을 강화

- (위조방지 원천기술 자립화) 해외 의존도가 높은 핵심 위조 방지 기술의 국내 독자적 기술 확보 가능
 - (나노·광학 소재 원천기술 확보) 기존 홀로그램 중심의 저수준 방어에서 벗어나, 나노마킹, DNA 잉크, 광학 PUF 등 물리적 복제가 원천 불가능한 차세대 인증 소재 기술을 국내 자체 개발
 - 데드카피(Dead-copy) 수준의 정교한 위조에 대응 가능한 고신뢰 물리 인증 원천기술 확보로 해외 기술 의존도 탈피
 - 소재-디바이스-알고리즘-플랫폼으로 연결되는 위조방지 기술 밸류체인의 국내 완성으로 기술 주권 확립
 - (AI 기반 위조 판별 기술 고도화) 딥러닝·컴퓨터 비전 기반 위조품 자동 판별 알고리즘을 개발하여, 기존 인력 중심 단속의 정확도, 속도 한계를 기술적으로 극복
 - 온라인 유통 플랫폼에서의 실시간 위조상품 모니터링 및 자동 차단 시스템의 핵심 엔진으로 활용
 - 블록체인 연계 유통이력 추적 기술과 결합하여 위조품 유통 전주기 추적이 가능한 통합 플랫폼 기술 확보
 - (글로벌 기술 표준 선도) 국내 위조방지 기술의 성능 평가 기준 및 국제 표준(ISO) 대응 체계를 구축하여, 국내 기업의 글로벌 시장 공신력 확보 기반 마련
 - 자체 기술규격 확보를 통해 EU 등 주요국의 위조 식별 가이드라인 강화에 선제적 대응이 가능하며, 해외 기술 종속 및 무역 장벽 위험 해소
- (지능형 산업스파이 방지 기술의 국내 자립화) 고도화되는 침해 수법에 대한 선제적 대응 역량 확보
 - (AI 기반 이상행위 탐지 시스템 개발) UEBA 기술과 거대언어모델(LLM) 기반 보안 분석을 결합한 차세대 이상행위 탐지 시스템을 국내 자체 개발하여, 해외 보안 솔루션 의존도 해소
 - 생성형 AI를 활용한 코드 탈취, 클라우드 협업 툴을 통한 우회 공격 등 신규 유출 수법에 대한 실시간 탐지 및 차단 기술 확보
 - 내부자의 위협, 내부자와 공모, 유출과 초소형 촬영 등 기존 보안 체계로 탐지 불가능한 위협에 대한 다층 방어 기술 확보
 - (포렌식 워터마킹 및 유출 경로 역추적 기술 확보) 디지털 문서, 설계도면, 소스코드 등에 비가시적 워터마크를 삽입하여 유출 경로를 정밀 추적하는 한국형 디지털 포렌식 도구 개발
 - 기술경찰, 검·경 수사기관의 범죄 입증 능력을 획기적으로 향상시키는 수사 지원 도구로 활용 가능
 - 유출 사고 발생 시 증거 확보 시간을 대폭 단축하고, 책임 소재의 명확한 규명이 가능한 법과학적 기술 기반 마련

- **(중소기업 맞춤형 보안 기술 보급)** SaaS 기반의 클라우드형 저비용 보안 서비스를 개발하여, 보안 역량이 절대적으로 부족한 중소·중견기업의 기술 보호 수준을 획기적으로 향상
- 기존 대기업 중심의 고가 보안 솔루션을 중소기업이 부담 없이 이용할 수 있는 구독형 모델로 전환하여 기술보호 사각지대 해소

□ **(융합기술 파급효과) 타 산업 분야로의 기술 확산 및 응용 가능성**

- 위조방지 나노·광학 소재 기술은 의약품 인증, 식품 안전, 전자부품 진위 확인 등 다양한 산업 분야로 확산 적용 가능
- AI 이상행위 탐지 기술은 금융 사기 탐지, 사이버 침해 대응, 내부 감사 등 보안, 컴플라이언스 (Compliance) 전반에 활용이 가능한 범용 플랫폼 기술로 발전 가능
- 블록체인 기반 유통이력 추적 기술은 탄소배출 인증, ESG 공급망 관리, 의약품 유통 투명성 확보 등 글로벌 규제 대응 분야로 확장 가능

제2절 경제적 효과

위조방지 기술 보급을 통해 수출기업의 경제적 피해를 경감하고 핵심 산업기술 유출 방지를 통해 국가 성장 동력을 보호하여 첨단기술 분야 투자 유치 및 산업 생태계 활성화에 기여

□ **(위조상품 유통 피해 경감) 위조방지 기술 보급을 통한 직접적 경제적 피해 저감**

- **(수출손실 경감)** 전 세계에서 유통되는 한국 기업의 위조상품 규모는 약 97억 달러(약 11조 원)에 이르며, 이는 한국 전체 수출액의 1.5%에 해당하는 막대한 규모로, 본 사업의 위조방지 기술 보급을 통해 수출기업의 직접적 매출 손실을 완화
- 위조상품 유통으로 인한 한국의 제조업 일자리 상실은 약 1만3천여 개, 세수 손실은 약 15억7천만 달러에 달하며, 기술적 대응을 통해 이러한 사회경제적 손실을 체계적으로 경감
- K-브랜드의 글로벌 신뢰도 제고로 프리미엄 가격 유지 및 수출 경쟁력 강화 효과 기대
- * OECD 분석('24)에 따르면 한국은 위조 상품 피해 규모 세계 8위로, 기술적 대응 없이는 피해가 지속 확대될 것으로 전망

□ **(핵심 산업기술 유출 억제를 통한 경쟁력 강화) 산업스파이 방지 기술의 현장 적용으로 국가 핵심기술 보호**

- **(유출 피해 저감)** 최근 5년간 적발된 산업기술의 해외 유출 피해 추산액 약 25조 원의 실질적 경감 효과 기대
- 반도체(39%), 디스플레이(20%), 자동차(8.5%) 등 국가 경제를 지탱하는 핵심 산업 분야의 기술 유출을 선제적으로 차단하여 국가 성장동력 보호
- 기술유출 사건의 86.5%가 집중되는 중소기업에 SaaS형 보안 서비스를 보급함으로써, 보안 취약 기업 대상 현장 적용 확산을 통한 산업 전반의 보안 수준 향상
- **(기업 투자 환경 개선)** 기술보호 인프라 강화로 국내외 기업의 R&D 투자 안전성이 제고되어, 첨단기술

분야 투자 유치 및 산업 생태계 활성화에 기여

- 핵심기술 보유 기업의 기업가치 방어 효과와 함께, 기술 신뢰성에 기반한 글로벌 파트너십 확대에 기여

□ (지식재산 보호기술 산업의 신성장동력 창출) 관련 산업 생태계 확대 및 일자리 창출

- (시장 창출) 글로벌 위조방지 시장('25년 2,040.8억 달러→ '33년 4,282.8억 달러 전망)에서 국내 기업의 기술 경쟁력을 확보하여 글로벌 시장 진출 기반 마련
 - 원천기술 확보를 기반으로 국내 위조방지 및 보안 기업의 기술 수준을 글로벌 수준으로 격상시켜, 그동안 진입이 어려웠던 고부가가치 시장으로의 확장 지원
- (산업 연관효과) 나노소재, AI·빅데이터, 블록체인, 보안 솔루션, 정보서비스 등 연관 산업의 동반 성장 유발
 - 본 사업에서 개발된 핵심기술의 민간 이전·사업화를 통해 스타트업 창업, 기존 기업의 신사업 진출 등 산업 생태계 확대 효과 기대
- (수입대체 효과) 현재 해외 솔루션에 의존하고 있는 고급 보안 제품·서비스의 국산화를 통해 연간 수백억 원 규모의 수입대체 효과 기대
- 동 사업의 R&D 투자를 통한 생산 유발, 부가가치 유발, 고용 유발 등 국가 경제 전반에 긍정적 파급효과 발생 전망
 - 위조방지 관련 소재·장비 제조업, 보안 SW 개발업, 정보서비스업 등 다양한 산업 부문에 걸쳐 파급 효과가 분산되어 경제 전반의 성장에 기여

제3절 사회적 효과

위조방지 기술 보급을 통한 공정경쟁 시장 조성 및
국민안전 보호와 사회안전망 강화를 통해 선제 예방형
체제로의 신뢰사회 구현에 기여

□ (공정 경쟁 질서 확립) 위조방지 기술 보급을 통한 건전한 시장 환경 조성

- (소비자 신뢰 제고) 위조 불가능한 고신뢰 인증 기술의 대중화를 통해, 소비자가 정품과 가품을 명확히 구분할 수 있는 환경을 조성하여 정품 사용 문화 확산에 기여
- 스마트폰 앱 기반 간편 정품 인증 서비스 등 소비자 친화적 기술을 개발·보급하여, 일반 국민의 위조 상품 피해를 자기 방어적으로 예방
- 온라인 유통 플랫폼에서의 자동 위조품 모니터링 기술 도입으로 전자상거래 생태계의 신뢰성을 강화하고, 정당한 기업 활동을 보호하는 공정경쟁 환경 구축
- (국가 브랜드 가치 제고) K-브랜드의 글로벌 정품 신뢰도를 기술로 보장함으로써, 한류 확산에 따른 국가 브랜드 가치의 지속적 상승을 뒷받침
 - 위조상품으로 인한 국가 이미지 훼손을 방지하고, '메이드 인 코리아' 제품에 대한 글로벌 소비자의 신뢰를 기술적 수단으로 보장

□ (국민안전 보호) 유해 위조상품 유통 차단을 통한 국민 건강·안전 확보

- (안전 위협 차단) 화장품, 의약품, 유아용품, 전기장비 등 국민 안전과 직결되는 품목의 위조상품 유통을 기술적으로 차단하여 국민의 건강과 생명을 보호
 - 유해 물질이 함유된 가품의 시장 유입을 원천 봉쇄하는 고도화된 식별 기술 보급으로, 위조상품으로 인한 건강 피해 사고를 사전에 예방
 - 자동차 부품, 의료기기 등 안전 관련 산업재의 위조품 유통을 차단하여, 제품 결함으로 인한 대형 사고 위험을 기술적으로 경감
- (소비자 피해 구제 강화) 위조상품 유통 이력의 블록체인 기반 추적 기술을 통해, 피해 발생 시 유통 경로의 신속한 파악과 책임 소재 규명이 가능하여 소비자의 실질적 권리 보호에 기여

□ (사회안전망 강화) 국가 핵심기술 보호로 경제안보 확립

- (선제적 예방 체계 구축) 기존의 사후 적발·처벌 중심의 대응 체계에서, AI 기반 이상행위 실시간 탐지 및 자동 차단 기술 도입을 통한 선제 예방형 체계로의 패러다임 전환
 - 기술유출 시도를 사전에 감지하고 차단함으로써, 기술유출 사건 발생 자체를 억제하는 구조적 예방 효과 창출
 - 기술 유출 피해가 집중되는 중소기업의 보안 역량을 국가 차원에서 지원함으로써, 산업 전반의 보안 수준을 상향 평준화
- (정책 패러다임 전환 촉진) 본 사업을 통해 확보된 기술 성과는 지식재산 보호 정책의 「사후 대응→선제 예방」 패러다임 전환을 기술적으로 실현하는 핵심 인프라로 기능
 - 과학적 증거 기반의 기술 유출 수사 지원 도구(디지털 포렌식) 개발로, 법 집행의 실효성을 제고하고 기술 침해에 대한 억지력 강화
 - 범부처 지식재산 보호 거버넌스(지식재산처, 산업부, 중기부, 경찰청 등)의 기술적 기반을 마련하여, 정책 간 연계 시너지 극대화

□ (지식재산 보호 인식 제고) 기술 기반 보호 체계의 사회적 확산

- (인식 전환) 지식재산 보호가 '규제와 단속'이 아닌 '기술과 혁신'으로 실현될 수 있다는 인식을 사회 전반에 확산시키는 계기로 작용
 - 기업, 소비자, 정부 모두가 참여하는 지식재산 보호 생태계를 기술적으로 구현함으로써, 자율적 보호 문화의 정착에 기여
 - 청년 창업가 및 중소기업 대표의 기술보호 인식 제고를 통해, R&D 투자의 선순환 구조를 형성하고 혁신 생태계의 지속가능성 확보
- (국제 협력 강화) 한국형 지식재산 보호 기술의 글로벌 확산을 통해, 국제 지식재산 보호 협력의 기술 허브로서의 위상 확보
 - 개발도상국 대상 위조방지·보안 기술 이전 협력 등 국제 기여를 통해 글로벌 IP 보호 질서 강화에 기여

제 5장 결론

□ 첨단 산업기술 유출 심화에 따른 기술보호 정책의 선제 예방형 대응체계 전환 필요

- 최근 5년('20~'24년)간 적발된 산업기술 해외 유출은 총 105건, 피해 추산액은 약 25조 원에 달하는 등 국가 경제에 중대한 피해가 지속적으로 발생하고 있으며, 이는 개별 기업의 손실을 넘어 국가 경제의 성장잠재력 훼손 및 안보 위협으로 직결
- 생성형 AI, 클라우드 등 신기술이 기술 유출 수단으로 활용되면서 기존 물리적 중심의 보안체계를 우회·무력화하는 등 유출 방식이 고도화
- 개별 기업 단위의 대응만으로는 고도화된 사이버 공격 및 내부자 공모형 위협 대응에 한계가 존재하므로, 국가 차원의 방어체계(Anti-Espionage 기술) 구축 및 선제 예방 중심의 기술보호 정책 전환 필요

□ 국내 위조상품 유통의 산업화·조직화 심화

- K-브랜드 확산 및 한류 영향력 확대, 온라인 유통 구조 확산에 따라 국내 제품에 대한 위조상품 유통이 산업화·조직화되는 양상이 심화되고 있으며, 이는 기업 매출 감소뿐 아니라 국가 브랜드 가치 저하 및 고용 기반 약화 등 사회·경제 전반에 부정적
- 육안 식별이 불가능한 데드카피(Dead-copy) 수준의 위조 기술에 대응하기 위해, 위변조가 원천 차단되는 고신뢰 식별 기술(블록체인, DNA 잉크 등) 개발 및 보급 절실

□ 기술 양극화 해소 및 글로벌 표준 선도를 위한 공공의 마중물 역할 강화 필요

- 기술 고도화에 따라 복제저항성 확보, 디지털 인증 체계 구축, 글로벌 표준 대응 등 요구 수준이 급격히 상승하고 있으나, 민간 단독 대응에는 기술·비용적 한계 존재
- 자금력 부족으로 인해 RFID, 블록체인 등 첨단 기술 대신, 진입장벽이 낮은 범용 기술(Low-end) 위주로 시장이 고착화되는 현상이 나타남에 따라 마중물형 연구개발 지원 확대 및 고신뢰 보안기술 중심의 시장 전환 지원 필요

□ 글로벌 규제 강화 및 국내 표준기술 부재에 따른 수출 경쟁력 약화 우려

- 국내 기업의 경우 글로벌 시장에서 요구되는 표준 부합성 및 인증체계에 대응할 수 있는 기술 및 인증체계가 부족함에 따라 수출 경쟁력 저하로 이어질 가능성이 높으며, 독자 기술 기반의 표준 대응체계 구축 및 글로벌 규제 대응 역량 강화 필요