Journal of KIIT. Vol. 24, No. 6, pp. 19-32, Jun. 30, 2026. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2026.24.6.19

ISMS-P 기반 인공지능 활용 통합 산업기술보호 관리체계 제안

최익서*, 최은선**, 박남제***

Proposal for an Integrated Industrial Technology Protection Management System Utilizing AI based on ISMS-P

Ikseo Choi*, Eunsun Choi**, and Namje Park***

이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(RS-2026-25498234)

요 약

본 논문은 산업기술의 보호를 위한 산업보안 관리체계의 실효성 제고를 목적으로, 최신 인공지능 기술인 RAG와 S-BERT를 활용하여 ISMS-P 기반의 통합 산업보안 관리체계 구축 방안을 제안한다. 최근에 산업기술 유출 위험은 점점 커지고 이로 인해 산업보안 관리체계의 필요성은 더욱 증가하고 있음에도 불구하고, 산업통상자원부에서 2011년 개발한 산업보안관리체계가 현장에서 적용 한계나 실용성 약화로 인해 2015년 일부 기업체 인증을 마지막으로 지금은 사용되지 않고 있다. 그래서 본 논문은 2025년 기준 산업기술보호법을 근거로 기존 산업보안 관리체계를 현행화하고, 이를 ISMS-P의 세부항목과 매핑하였다. 이 과정에서 RAG와 S-BERT를 활용하여 항목 간 연관성과 중복·누락 여부를 객관적으로 평가하였으며, 최종적으로 4개 영역, 26개 분야, 111개 항목, 363개 세부항목으로 구성된 통합 산업기술보호 관리체계를 도출하였다.

Abstract

This paper proposes a plan to build an integrated industrial security management system based on ISMS-P by utilizing the latest artificial intelligence technologies, RAG and S-BERT, with the aim of enhancing the effectiveness of the industrial security management system for protecting industrial technology. Recently, the risk of industrial technology leakage has been increasing, and the need for an industrial security management system has increased accordingly. However, the industrial security management system developed by the Ministry of Trade, Industry and Energy in 2011 is no longer in use after receiving certification from some companies in 2015 due to limitations in application and weakened practicality in the field. Therefore, this paper updated the existing industrial security management system based on the Industrial Technology Protection Act as of 2025 and mapped it to the detailed items of ISMS-P. In this process, RAG and S-BERT were utilized to objectively evaluate the inter-item correlation and duplication/omission, and ultimately an integrated industrial technology protection management system consisting of 4 areas, 26 fields, 111 items, and 363 sub-items was derived.

Keywords

industrial technology protection, industrial security, retrieval augmentation generation, RAG, ISMS-P, S-BERT

* 제주대학교 사이버보안인재교육원 특별연구원
- ORCID: https://orcid.org/0000-0002-0870-7575
** 광주교육대학교 컴퓨터교육학과 교수
- ORCID: https://orcid.org/0000-0001-6384-5324
*** 제주대학교 초등컴퓨터교육전공 교수(교신저자)
- ORCID: https://orcid.org/0000-0003-4434-8933

· Received: Sep. 26, 2025, Revised: Jun. 10, 2026, Accepted: Jun. 13, 2026
· Corresponding Author: Namje Park
Dept. of Computer Education, Teachers College, Jeju National University, 61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 63294, Korea
Tel.: +82-64-754-4914, Email: namjepark@jejunu.ac.kr

Ⅰ. 서 론

현대 산업환경은 4차 산업혁명과 디지털 전환의 가속화로 인해 산업기술 유출 위험이 크게 증가하고 있다[1]. 클라우드 컴퓨팅, 사물인터넷, 인공지능 등 신기술의 도입은 기업 경쟁력 향상과 동시에 보안 위협도 증가시키고 있는 것이다. 이에 따라 산업기술보호법 등 관련 법령과 실무 관리체계 간 괴리가 더욱 커지고 있음에도 불구하고, 기업들은 실질적인 보안 지침 없이 개별 대응에 의존하고 있다[2]. 또한 산업통상자원부에서 한국산업기술보호협회 등과 협업을 통해 2011년 개발한 산업보안관리체계가 현장에서 적용 한계나 실용성 약화로 인해 2015년 일부 기업체 인증을 마지막으로 지금은 운용되지 않고 있다[3]. 그래서 정보보호 관리체계(ISMS, Information Security Management System)와 개인정보보호 관리체계(PIMS, Personal Information Management System)로 구분된 관리체계를 통합한 정보보호 및 개인정보보호 관리체계(ISMS-P, Information Security Management System & Personal Information) 인증제도[4]가 성공적으로 정착됨에 따라 산업기술 보호 분야에서도 이와 유사한 통합 관리체계의 필요성이 대두되고 있다. 본 논문은 검색증강생성(RAG, Retrieval Augmented Generation)[5]과 S-BERT(Sentence-Bidirectional Encoder Representations from Transformers)[6]를 활용하여 현장에서 적용의 한계 등 사유로 현재 사용되지 않고 있는 기존 산업보안 관리체계를 현행화하고, 이를 ISMS-P 기반으로 재구성하는 것을 목적으로 한다.

Ⅱ. 관련 연구

2.1 ISMS-P와 산업기술보호 관리체계 비교

ISMS-P는 조직의 정보자산 보호를 위한 정책, 위험관리, 보안대책, 모니터링 등 종합적이고 지속적인 관리체계로, 국제표준(ISO/IEC 27001)에 기반하여 정보보호와 개인정보보호를 통합적으로 평가·인증하는 제도이다[7]. 반면 산업기술보호 관리체계는 산업기술 유출 방지와 법적 규제에 초점을 두고 있으나, 실질적인 보호수준 평가나 자율적 관리체계는 미흡하다[8]. 두 체계 모두 자산 유출 방지와 통제체계 확립이라는 목적에서 구조적 유사성이 크며, ISMS-P의 항목 상당수가 산업기술 보호에도 적용 가능하다. 본 논문은 RAG와 S-BERT를 활용해 ISMS-P와 산업기술보호 관리체계의 항목을 의미적으로 매핑하고, 정량적 유사도 분석을 통해 통합 관리체계 모델을 제안한다. 이를 통해 산업기술 보호체계의 실무적 신뢰성과 평가 가능성을 높이고, 향후 ISMS-P 인증과 산업기술 보호인증의 통합 연계도 기대할 수 있다.

2.2 RAG

RAG는 대규모 언어모델(LLM, Large-scale Language Model)의 생성 능력과 외부 지식 검색 시스템을 결합한 인공지능(AI, Artificial Intelligence) 기술로, 쿼리와 문서 간 의미 유사성을 바탕으로 관련 정보를 검색한 뒤 이를 활용해 보다 정확하고 최신의 결과를 생성한다[9]. 산업보안 관리체계 현행화 및 ISMS-P 통합 과정에서 RAG는 방대한 문서의 효율적 처리, 최신 법령 반영, 일관된 해석 및 적용을 가능하게 한다. 산업기술보호법과 ISMS-P 문서를 임베딩해 벡터 데이터베이스에 저장하고, 쿼리 기반 검색과 의미 기반 매핑을 수행함으로써 정확성을 높인다. RAG 기반 접근은 기존 분석 대비 시간 효율성과 의미론적 정합성이 뛰어나며, 산업보안 분야 분석 및 관리체계 통합의 혁신적 패러다임을 제시한다.

2.3 S-BERT

S-BERT(Sentence-BERT)는 문장 수준의 의미론적 유사성을 측정하기 위해 개발된 트랜스포머 기반 언어 모델로, 네트워크 구조를 활용해 각 문장을 고정된 벡터로 효율적으로 임베딩한다. 기존 BERT(Bidirectional Encoder Representations from Transformers) 대비 대규모 문장 비교 시 계산 효율성이 높으며, 문장 간 의미적 유사성을 정량화할 수 있다[10]. S-BERT는 의미론적 유사성 검색, 문서 클러스터링, 텍스트 분류 등에서 뛰어난 성능을 보이며, 본 연구에서는 산업보안과 ISMS-P 항목 간 의

미 기반 매핑 및 정량적 평가에 활용된다. 임베딩 결과는 유지, 개선, 신설 등 객관적 기준 설정에 기초 자료로 제공된다.

III. 기존 산업기술보호 관리체계 실태

3.1 산업기술보호 정책 현황

2006년 제정된 산업기술보호법은 국가핵심기술 지정, 유출 금지, 형사처벌 등 산업기술 보호의 법적 기반을 제공해왔다. 그러나 이 법은 보호 대상과 행위 규제에 집중되어 있어, 사전 예방 또는 자율적인 보호 관리체계와 실무적 평가체계가 부족하다. ISMS-P나 ISO27001과 같은 정보보호 인증제도와 달리, 산업기술보호법은 보호수준 평가나 기업 보호 역량 진단 기준이 없다. 산업기술보호지침 등도 현장 적용률이 낮고, 인증·점검 체계와 연계되지 않아 실효성이 떨어진다. 결과적으로 현행 제도는 보호대상 기술은 규정하지만, 보호수단과 보호역량을 정량화하거나 비교할 수 있는 공식적 장치는 마련되어 있지 않다. 이러한 한계로 인해 산업기술 보호 정책은 사후 규제 중심에 머물러 있으며, 실질적 보호의 사각지대가 존재한다[11]. 본 연구는 이를 극복하기 위해 ISMS-P의 요소를 산업기술 보호모델에 적용하는 평가체계 재설계를 제안한다.

3.2 산업기술보호 관리체계 실태

3.2.1 우리나라 산업기술보호 관리체계 실태

우리나라의 산업기술보호 관리체계는 2000년대 중반 이후 산업기술 해외 유출 증가에 대응해 2006년 산업기술보호법 제정과 함께 발전해 왔다. 표 1과 같이 2011~2015년 산업보안 관리체계가 국가 주도로 설계·운영되었으나, 법적 강제력과 인센티브 부족, 기존 정보보호 인증과의 중복, 정책 연속성 부족 등으로 2015년 일부 기업체 인증을 마지막으로 지금은 운용되지 않고 있다. 또한 현행 산업기술보호지침은 실무적 가이드로 존재하지만 법적 구속력과 평가·인증 체계가 없어 현장 적용성이 낮다[8]. 반면 ISMS-P는 항목 기반의 체계적 평가와 인증, 자율점검, 등급화, 사후관리까지 갖춘 인증제도[12]로 산업기술보호 관리체계와 구조적으로 큰 차이를 보인다. 현재 산업기술 보호는 법령 중심의 사후 규제에 머물러 있고, 실질적 보호수준 진단 및 비교가 어렵다. 따라서 항목 기반 평가와 인증체계 도입이 시급하며, ISMS-P와 같은 정보보호 인증체계의 요소를 산업기술 보호모델에 적용하는 것이 필요하다.

표 1. 기존 산업보안 관리체계[3,8]
Table 1. Existing industrial security management system

Area	Field	Item	Detail items
Administrative	Operation and management of the industrial security management system	3	11
	Document and records management	4	18
	Management responsibility	5	15
	Asset management	4	16
	Human asset management	6	24
	Design and development related security	7	16
	Purchase information security	3	7
	Security related to product realization	9	25
Physical	Physical security	5	16
Technical	Access control	7	27
	Technical security	6	37
Security incident response	Security incident management	3	11
	Measurement, analysis, and continuous improvement	8	31
Security knowledge management	Business continuity management	5	15
	Industrial security performance management	1	4
	Technology value assessment	1	5
	Technology transfer and introduction contract management	1	4
Total	17	78	282

3.2.2 해외·국제표준 산업기술보호 관리체계 실태

해외 및 국제표준 산업기술보호 관리체계는 ISO/IEC 27001 등 정보보호 국제표준을 기반으로 하여, 산업기술 보호와 정보보호를 통합적으로 관리하는 추세이다[13]. 주요 선진국은 표 2와 같이 산업기술 유출 방지를 위해 법령과 기술적·관리적 보

호조치를 강화하고 있으며, 미국, 유럽, 일본 등은 국가핵심기술 지정, 수출통제, 내부자 관리 등 다양한 정책을 운영하고 있다.

표 2. 주요 국가 산업기술보호 관리체계
Table 2. Major national industrial technology protection management systems

country name	Industrial technology protection management system
USA [14]-[16]	The United States has established a multi-layered legal and policy framework for industrial technology protection, characterized by strong federal support and regulation [14]. The U.S. industrial technology protection system can be broadly categorized into legal frameworks, government-led initiatives, standards and frameworks, and information-sharing mechanisms.
European Union [17][18]	It takes a balanced approach, providing a unified regulatory framework across member states while allowing for flexible application tailored to each country's unique characteristics and industrial structure [15].
Japan [19]	We are strengthening the prevention of industrial technology leakage through laws such as the unfair competition prevention act and the economic security promotion act [16], and are strengthening security capabilities through public-private cooperation and international cooperation [17].
China [20]	A comprehensive legal system is being established through the national security act, cyber security act, etc., and technology protection is being strengthened through state-led initiatives [18], closely linking national security and industrial technology protection.

산업기술보호 관리체계에 관한 국제표준은 표 3과 같이 정보보호 관리체계의 일관성과 실효성을 강조하며, 각국은 이를 자국 산업특성에 맞게 보완 적용하고 있다. 최근에는 인공지능, 클라우드 등 신기술 환경에 대응한 자동화 및 지속적 업데이트 체계 도입이 확대되고 있다. 특히, IEC 62443은 산업 자동화 및 제어시스템의 사이버보안에 특화된 국제표준으로서, 정책, 시스템, 절차 등 다양한 수준에서의 보안 요구사항에 대해서 정의를 하고 있으며, OT와 IT의 융합적인 환경에서 보안 과제 해결에 초점을 맞추고 있다.

표 3. 관리체계 국제표준[19-21]
Table 3. International standards for management systems[21]

International standard	Management system
ISO/IEC 27001 [22]	An international standard for Information Security Management Systems (ISMS), it covers the entire life cycle of establishing, operating, monitoring, and improving a management system to systematically protect an organization's information assets.
ISO/IEC 27701	This standard expands ISO/IEC 27001 to include requirements for a Personal Information Management System (PIMS). It provides a framework that meets global privacy regulations like the GDPR while also integrating with existing information security management systems, making it ideal for protecting personal information-related industrial technologies.
IEC 62443 [23]	This is an international standard specializing in cybersecurity for industrial automation and control systems. It provides specific guidelines for managing security risks in operational technology environments across various industries, including manufacturing, energy, chemicals, and transportation.

3.2.3 중단된 산업보안관리체계의 현행화 방향

산업기술보호법 및 그 시행령과 시행규칙의 2025년 개정 내용을 반영하여, 기존 산업보안 관리체계를 현행화한다. ISMS-P 기반의 통합 관리체계로 점검항목을 연계 및 통합하여 중소기업의 부담을 최소화한다. 산업기술보호법의 목적과 주요 조항(국가핵심기술 지정, 유출방지 등)을 관리체계에 반영한다. 시행령·시행규칙의 절차와 세부사항(신고, 실태조사 등)을 관리체계에 포함한다. RAG 기반 데이터 전처리 등 최신 기술을 활용해 관리체계의 실효성을 높인다. 또한 본 논문에서는 산업보안 관리체계와 산업기술 보호 관리체계를 동일 개념으로 혼용하여 적용한다.

Ⅳ. ISMS-P 기반 통합 산업기술보호 관리체계 제안

4.1 ISMS-P 기반 통합 산업보안관리체계 개요

ISMS-P 기반 통합 산업보안 관리체계는 ISMS-P와 산업기술보호법을 통합해 기업이 다양한 보안 요구를 단일 프레임워크로 관리할 수 있도록 설계되었다. 실효성, 확장성, 일관성을 핵심 원칙으로 하며, RAG와 S-BERT라는 선행 기술을 활용해 항목 현행화, 매핑, 최종 결과표를 자동화·객관화하였다. 데이터 전처리 과정에서 두 관리체계의 항목을 표준화·정규화하고, 의미적 연관성을 강화해 일관된 통합체계를 구축하였다. 이 모델은 기업의 관리 부담을 줄이고, 산업기술 보호와 국가 경쟁력 강화에 기여하는 효율적 프레임워크를 제공한다.

4.2 설계 환경

본 논문에서는 AI 기반 네트워크 보안 분석을 위한 실험 환경으로 소형 폼팩터 기반의 가상화 테스트베드를 구축하였다. 표 4는 하드웨어 사양, 가상화 플랫폼 구성, 컨테이너 기반 서비스 환경을 구체적으로 나타낸 것이다. 여기에서, 컨테이너 기반 서비스 환경은 연구 목적에 따라 LXC 컨테이너 4개를 운영하며, AI 및 벡터 데이터베이스 기반 분석 환경을 구성하였고, 이 중 Ollama는 성능이 부족하여 OpenAI Gpt 모델(Gpt-4o mini, Gpt-4o)을 사용하고, Milvus2는 백업용으로 사용하였다. 가상화 성능은 16GB 메모리와 4코어 CPU를 통해 동시에 3개의 AI/데이터베이스 컨테이너를 안정적으로 운영하며, 각 컨테이너당 2-4GB 메모리와 2-4개 CPU 코어를 할당했는데, 이러한 테스트베드 환경은 네트워크 보안 분석을 위한 그래프 기반 AI 모델 연구에 최적화되어 있으며, Milvus 벡터 데이터베이스와 Langflow 자동화 도구를 통한 실시간 위협 탐지 실험을 수행할 수 있다.

그림 1은 이러한 테스트 환경을 실제로 캡처하여 나타낸 것이다.

표 4. 테스트 베드 환경
Table 4. Test bed environment

Hardware	- Processor: Intel N100 (4 cores/4 threads, base clock 0.8GHz, Turbo Boost up to 3.4GHz, 6MB L3 cache) - Memory: 16GB DDR4 3200MHz (single SODIMM slot) - Storage: 512GB NVMe SSD - Power Consumption: TDP 6W (low-power, fanless design)
Virtualization platform	- Host OS: Proxmox VE 8.3.0 Debian GNU/Linux - Kernel: Linux 6.8.12-4-pve (x86_64 architecture) - Host node name: bluesxxx - Virtualization technology: KVM/QEMU, LXC container technology
Container-based service environment	1. Running containers 1) langflow (VMID: 210) - 2 CPU cores, 4 GB memory, 62.44 GB storage allocated - Disk usage: 22.32 GB - AI workflow management and automation tool 2) milvus (VMID: 211) - 2 CPU cores, 4 GB memory, 124.93 GB storage allocated - Disk usage: 8.70 GB - Vector database service 2. network configuration 1) Physical Network Interfaces - 'enp3s0': Primary Ethernet Adapter (MAC: e0:51:d8:18:34:22) 2) Virtual Network Configuration - 'vmbr0': Virtual Bridge (IP: 172.16.76.140/24) - Per-Container Virtual Ethernet Interfaces (veth210i0, veth211i0, veth212i0)
Testbed performance	Processing performance: Intel N100 delivers approximately 5,500 points in PassMark, with single-thread performance up 40% compared to the previous generation

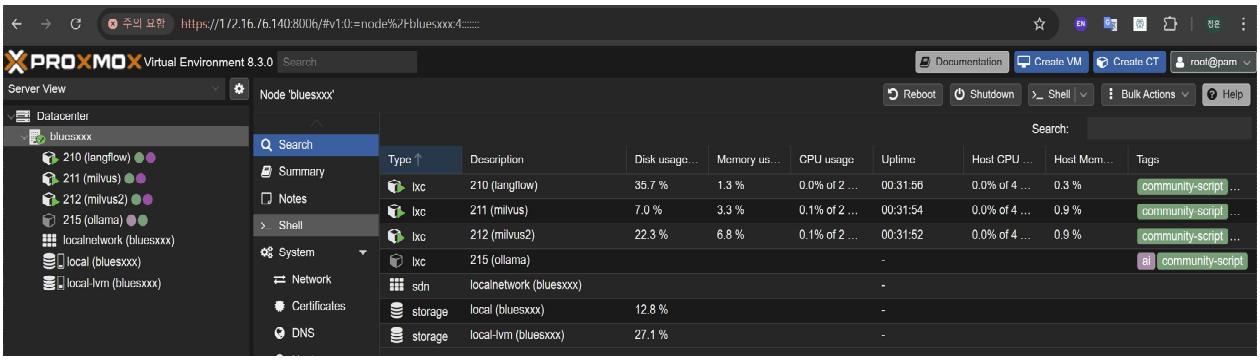

그림 1. 테스트 환경
Fig. 1. Test environment

4.3 ISMS-P 기반 통합 관리체계 설계

본 논문은 RAG를 이용하여 ISMS-P 기반의 산업기술보호 관리체계를 체계적으로 개발하는 일련의 단계로 구성되는데, 그림 2와 같이 설계한다.

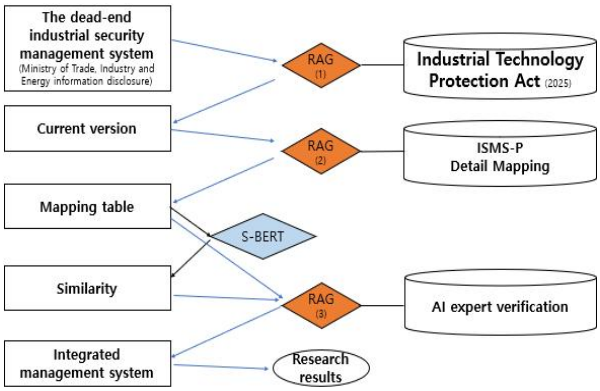

그림 2. 통합 관리체계 설계도
Fig. 2. Integrated management system design diagram

그림 2는 전체적인 통합 관리체계 설계를 한눈에 알 수 있도록 표시하였고, 표 5를 통해 프로세스는 현행화, 매핑과 유사도 분석, 최종 산업기술 보호를 위한 통합시스템 도출이라는 세 단계로 구성되며, 각 단계는 이전 단계의 결과물을 기반으로 계속 진행됨을 알 수 있다. 즉, 1단계는 산업기술보호법(2025년 기준)에 따라 기존 산업보안 관리체계를 현행화하고, 2단계는 현행화된 관리체계와 ISMS-P 세부항목 간 매핑 및 유사도 분석을 수행한다. 추가로 RAG를 이용한 매핑을 위해 데이터 전처리 작업과 텍스트 정규화 작업을 진행하였다. 데이터 전처리 작업은, ISMS-P는 3개 영역, 21개 분야, 101개 항목, 328개 주요확인 사항으로 분류되지만 기존 산업보안 관리체계는 2013년 기준으로 5개 분야, 17개 원칙, 78개 기준, 282개 세부기준으로 분류되는 것을 영역, 분야, 항목, 세부항목으로 4단계의 분류 명칭을 표준화하였다. 3단계에서는 매핑 결과와 전문가 Multi-Agent 검증을 바탕으로 ISMS-P 구조에 산업기술 보호 요소를 통합한 최종 관리체계를 도출한다. 이러한 통합적 접근방법은 기업의 다양한 보안요구 사항을 단일한 프레임워크 내에서 효율적으로 관리할 수 있게 해주며, 실무적 적용성과 법적 준수성을 전부 확보할 수 있다.

표 5. 프로세스 3단계
Table 5. 3-step process

Step 1	Step 2	Step 3
Current module design	Mapping module design	Integrated system module design
Confirm the revised Industrial Technology Protection Act of 2025 - The Ministry of Trade, Industry and Energy's management system was updated to comply with the Industrial Technology Protection Act of 2025 and a current table was created	- Create a mapping table by analyzing the correlation between the current management system and ISMS-P details. - Identifying duplicates, omissions, and inconsistencies between the two systems S-BERT similarity analysis	Based on the S-BERT analysis results, the ISMS-P structure was verified through expert multi-agents and a result table was derived. Developing an integrated management system that includes items necessary for industrial technology protection while maintaining the structure of ISMS-P

4.4 산업기술보호법 기반 관리체계 현행화 모듈

RAG를 이용한 현행화 모듈을 활용해, 기존 산업보안 관리체계의 282개 세부항목을 2025년 개정된 최신 산업기술보호법(및 시행령·시행규칙)에 맞게 자동으로 현행화하는 방법을 제시한다. RAG 모델은 표 6과 같이 산업기술보호법 전문을 벡터 임베딩해 지식베이스로 구축하고, 기존 관리체계 항목별로 관련 법조항을 검색·매핑하여 최신 법적 요구사항에 맞게 항목을 분류한다. 이 과정은 Langflow 기반 AI 파이프라인으로 자동화되어, 법령 개정에 신속하게 대응할 수 있으며, 현행화표를 통해 각 항목의 법적 근거와 변경 이력을 명확히 추적할 수 있다. 결과적으로, 본 현행화 모듈은 산업보안 관리체계의 법적 준수성과 실무 적용성을 높이고, 이후 ISMS-P와의 통합 매핑의 기초 자료로 활용된다.

표 6. 현행화 모듈 설계 절차
Table 6. Current module design procedure

Building a knowledge base	Enter management system items	Legal article search	Create current content
Constructed by vector embedding the text of the 2025 industrial technology protection act	Enter items from the existing ministry of health and welfare management system into the RAG model	Search the knowledge base for legal provisions related to each management system item	Create updated content for management system items based on searched legal provisions

4.5 ISMS-P 기반 산업기술보호 관리체계 매핑 모듈

ISMS-P 기반 산업기술보호 관리체계 매핑 모듈은 현행화 모듈에서 도출된 현행화된 산업보안 관리체계 세부항목과 ISMS-P 세부항목 간의 매핑을 수행하는데, 표 7과 같은 절차를 통해 진행된다.

표 7. 매핑 모듈 설계 절차
Table 7. Mapping module design procedure

Building a knowledge base	Enter current items	Related ISMS-P Search Items	Generate mapping results
Build a knowledge base for the RAG model by vector embedding the entire ISMS-P certification criteria	Enter each detailed item of the current industrial security management system into the RAG model	For each industrial security management system item, search for similar ISMS-P details	Generate mapping results by selecting the most relevant items

여기에서는 우선 ISMS-P 인증기준을 전처리하고, 전처리된 텍스트는 의미 단위로 분할되어 벡터 임베딩되고, 이는 RAG 모델의 지식 베이스가 된다. 다음에는 현행화 모듈로 도출된 산업기술보호 관리체계 세부항목을 각각 RAG 모델에 입력한다. 이후 검색된 ISMS-P 세부항목 중에서 다수가 매핑이 되는 경우 가장 관련성이 높은 세부항목을 하나만을 선택하여 매핑결과를 생성한다. 다만, 본 논문에서와 같이 RAG를 이용한 연구에서 유사한 문서들의 벡터 표현이 비슷해져서 서로 구분이 안되는 오버스무딩(Over-smoothing) 현상이 발생한다는 다수의 연구가 존재한다[8]. 따라서 이러한 문제점을 해결하기 위해 S-BERT 기반 임베딩 기술을 이용하여 유사도 검사를 실시하여 정량화하였다. S-BERT [24][25]는 문장 수준의 의미론적 유사성을 포착하는데 특화된 모델로서 한국어에 최적화되어 있어 각 항목을 벡터로 변환한다. 이때 항목의 전체 내용뿐만 아니라 제목, 목적, 요구사항 등 각 부분을 개별적으로 임베딩하고 이를 결합하는 방식을 적용하며, 의미적으로 유사한 문장은 벡터 공간에 가깝게 배치하고 다른 문장은 멀리 배치하도록 학습되어 있어 유사하지만 구분되어야 하는 항목들의 매핑에 적합하다. 이처럼 생성된 매핑 결과를 통해 표 8과 같이 유사도 기준(0.7 이상 유지, 0.5-0.7 개선, 0.5 미만 신설)으로 매핑 유형을 분류한다. 동일한 문장의 유사도 값이 1.0이고, 유사도가 0.7 이상이면 두 매핑 세부항목 간 목적과 내용면에서 거의 동일하

여 상호 대체 적용이 가능한 경우이고, 유사도가 0.5 이상에서 0.7 미만인 경우는 한 쪽이 다른 쪽의 일부 내용만을 커버하거나 양쪽 항목의 범위가 부분적으로 겹치는 경우이고, 유사도가 0.5 미만이면 목적과 내용면에서 다르거나 유사한 항목이 없어 산업보안 관리체계 고유한 항목일 가능성이 높은 경우이다[26,27]-[30].

표 8. 매핑 유형
Table 8. Mapping types

Mapping category	Similarity criteria	Number	Definition and description
Maintain	0.7% or more	49	If they are almost identical and can be applied interchangeably
Improvement	Less than 0.5~0.7%	198	If the ranges of both items only partially overlap
Creation	less than 0.5%	35	If there are no similar ISMS-P items or items that are different in purpose and content

매핑 결과, 유지 항목은 49개, 개선 항목은 198개, 산업보안 고유 요구사항(35개)은 신설이 필요함을 확인하였다. 정책·운영·기술적 조치 등으로 인해 두 체계의 공통점과 차이점이 도출되었으며, 이 매핑표는 통합 관리체계 개발의 핵심자료로 활용된다.

4.6 ISMS-P 기반 산업기술보호 관리체계 통합 모듈

4.6.1 Multi-Agent Collaborative RAG 설계

본 논문에서 제안하는 Multi-Agent Collaborative RAG 시스템은 ISMS-P와 산업보안 관리체계의 효과적 통합 분석을 위해 설계된 혁신적인 접근 방법이다. 기존의 단일 RAG 시스템이 갖는 편향성 및 제한된 관점의 한계를 극복하기 위해, 다중 전문가 에이전트가 협업하여 포괄적이고 균형잡힌 분석 결과를 도출하는 구조로 설계되었다. 표 9는 기존 RAG 시스템과 제안하는 Multi-Agent Collaborative RAG 시스템의 핵심 차이점을 보여주고 있다[31]-[36].

표 9. RAG 시스템 비교
Table 9. RAG system comparison

Aspect	Traditional RAG	Multi-agent RAG
Processing	Single agent	Multiple experts
Analysis	Limited view	Multi-perspective
Structure	Sequential	Parallel processing
Expertise	Basic retrieval	Domain knowledge
Output	Simple Q-A model	Consensus synthesis
Objectivity	Bias potential	Independent analysis

그림 3. 다중 에이전트 RAG 시스템 구조
Fig. 3. Multi-agent RAG system architecture

제안된 시스템은 계층적 구조로 설계되어 있으며, 각 계층은 특정 기능을 담당한다. 전체 시스템은 그림 3과 같이 5개의 주요 계층으로 구성된다.

1계층인 입력 계층(Input layer)은 사용자가 ISMS-P 기준과 산업보안 요구사항을 동시에 입력할 수 있는 ChatInput 인터페이스를 제공한다. 이 계층은 복합적 질의를 받아들이고 후속 처리를 위해 데이터를 전달하는 역할을 수행한다. 2계층인 데이터 전처리 계층(Data preprocessing layer)은 data separator 컴포넌트가 입력된 혼재된 요구사항을 체계적으로 분리하고 구조화한다. 이 과정에서 ISMS-P 관련 요구사항과 산업보안 항목들을 식별하고 분류한다. 3계층인 이슈 분석 계층(Issue analysis layer)은 OpenAI 언어모델을 활용한 issue analysis model이 구조화된 데이터를 표준화된 이슈 형태로 변환한다. 이렇게 변환된 구조화된 이슈는 모든 전문가 에이전트가 공통으로 분석할 수 있는 표준 형식으로 제공된다. 4계층인 다중 전문가 분석 계층(Multi-Expert analysis layer)은 4개의 독립적인 전문가 에이전트가 병렬적으로 동일한 구조화된 이슈를 각자의 전문 관점에서 분석한다. 각 에이전트는 서로 다른 분석 철학과 접근 방식을 갖추고 있어 다양한 관점의 의견을 제시한다. 5계층인 통합 분석 계층(Synthesis layer)은 discussion synthesis prompt가 4개의 전문가 에이전트의 독립적 분석 결과를 종합하여 최종 통합 분석 보고서를 생성한다. 이렇게 Multi-Agent Collaborative RAG 시스템을 설계하고 그림 4와 같이 실제로 구현하였다.

표 10은 전문가 에이전트별 역할을 정의한 것으로, 4개의 전문가 에이전트는 각각의 역할을 통해 매핑 및 유사도 검사를 마친 분석 결과를 바탕으로 검증을 하여 결과표를 도출한다. ISMS-P Guardian Agent는 기존 ISMS-P 체계의 안정성과 일관성을 최우선으로 보호하는 보수적 관점의 분석을 담당하며, 프롬프트는 “ISMS-P 전문가로서 기존 체계의 안정성과 일관성을 최우선으로 고려...”로 설계되었다.

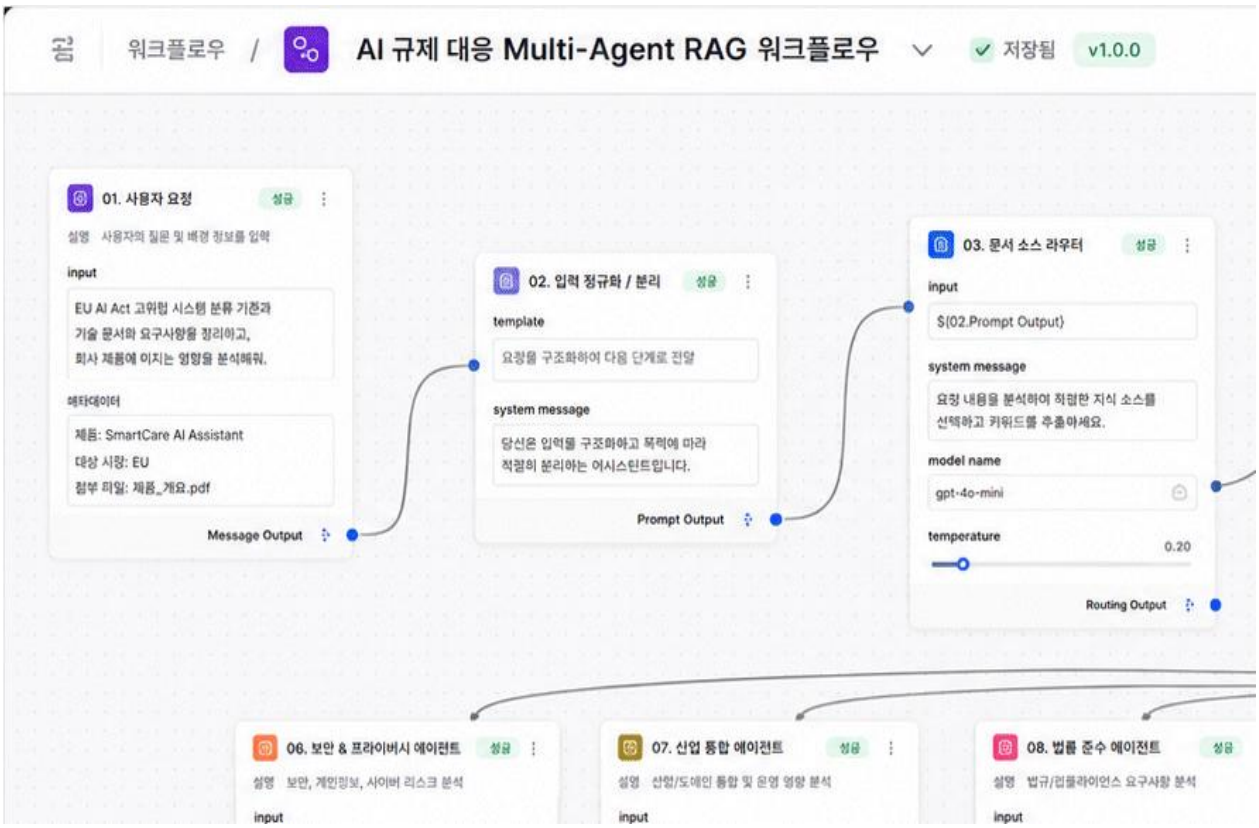

그림 4. Multi-Agent Collaborative RAG 구현
Fig. 4. Implementation of Multi-Agent Collaborative RAG

Industrial integration Agent는 산업보호 요구사항의 효과적 통합을 위한 혁신적이고 진보적인 접근 방안을 제시하며, 프롬프트는 “산업보호 통합 전문가로서 효과적이고 혁신적인 통합 방안...”으로 설계되었다. Legal compliance agent는 법적 컴플라이언스와 규제 준수 관점에서 통합 방안의 법적 타당성을 검토하며, 프롬프트는 “법적 컴플라이언스 전문가로서 규제 준수와 법적 리스크...”로 설계되었다. Implementation agent는 실제 조직 환경에서의 구현 가능성과 운영 효율성을 중심으로 실무적 분석을 수행하며, 프롬프트는 “실무 구현 전문가로서 실제 조직 환경에서의 적용 가능성...”으로 설계되었다. 여기에서 4개의 전문가 에이전트의 병렬 처리를 통해 전체 분석 시간을 최적화한다. 각 에이전트는 동일한 구조화된 이슈를 독립적으로 처리하며, 서로의 분석 과정에 영향을 주지 않도록 설계하였다.

표 10. 전문가 에이전트별 역할
Table 10. Roles of expert agents

Agent name	Specialization	Main features
ISMS-P guardian	Information protection management system	Protecting existing systems and maintaining consistency
Industrial integration	Industrial protection integration	Presenting a new integrated methodology
Legal compliance	Legal compliance	Measures to minimize legal risks
Implementation	practical implementation	Organization-level feasibility review

4.6.2 통합 산업기술보호 관리체계

표 11와 같이 ISMS-P와 통합 관리체계의 세부항목을 비교하였더니, ISMS-P 고유영역이 81개, 산업보안 특화 영역으로 35개 신설항목이 있음을 알 수 있다. 또한 최종 비교표를 나타내는 표 12를 보면, 4개 영역, 26개 분야, 111개 항목, 363개 세부항목의 통합 관리체계를 도출하였다. 이는 Multi-Agent RAG 시스템을 활용해 ISMS-P, 산업기술, 법률, 실무 전문가의 의견을 병렬적으로 반영하여, 법적·실무적·기술적 요구를 모두 충족하는 구조로 설계되었다. 최종 통합 관리체계는 기업의 정보보호와 산업기술 보호를 동시에 실현할 수 있는 실용적 프레임워크로, 관리 효율성 및 보안 수준을 크게 높일 수 있다.

표 11. ISMS-P와 통합 관리체계 세부항목 비교
Table 11. Comparison of ISMS-P and integrated management system details

Division	Details item	Maintain	Improve-ment	Inherence	Creation
ISMS-P	328	49	198	81	-
Integrated management system	363	49	198	-	35

표 12. 최종 비교표
Table 12. Final comparison table

Division	Area	Field	Item	Details item
ISMS-P	3	21	101	328
Existing industrial security management system	5	17	78	282
Integrated management system	4	26	111	363

V. 결 론

본 논문은 2011년 산업보안 관리체계가 산자부와 한국산업기술보호협회 등이 협업을 통해 설계·운영하였으나 법적 강제력과 인센티브 부족, 기존 정보보호 인증과의 중복 등의 이유로 2015년 기업체 인증을 마지막으로 지금은 운용되지 않고 있는 산업보안 관리체계를 최신 산업기술보호법에 맞게 1단계에서 RAG를 이용하여 현행화하고, 2단계에서는 현행화된 관리체계와 ISMS-P 기반으로 인증체계와 통합하는 방안을 RAG와 S-BERT 인공지능 기술을 활용해 매핑 및 유사도 검사를 실시하여 정량화 하고 이를 다중 에이전트 RAG를 이용하여 검증 후 표 13과 같이 전체를 비교하는 표를 제시하였다. 기존 ISMS-P에 산업보안 영역을 신설하고 35개 신규 항목을 추가하는 등 통합 관리체계를 도출하였으며, 이는 산업계·공공·인증기관 모두에 중복 인증 부담 감소, 효율적 보안 관리, 정책 실효성 강화, 인증 신뢰성 제고 등 다양한 이점을 제공한다.

표 13. ISMS-P 기반 통합 관리체계 전체 비교
Table 13. Comparison of the ISMS-P-based integrated management system

Authentication realm	Certification criteria		ISMS-P			Industrial technology protection			
			Item	Detailed items		Detailed items			
				Common-ness	Inherence	Total	Maintain	Improve-ment	Creation
1. Establishment and operation of management system (16/42)	1.1	Establishment of management system foundation	6	17	-16	33	7	26	-
	1.2	Risk management	4	13	-19	32	5	27	-
	1.3	Management system operation	3	6	1	5	1	4	-
	1.4	Management system inspection and improvement	3	6	-24	30	5	25	-
2. Protective measures requirements (64/195)	2.1	Policy, organization, and asset management	3	9	3	6	1	5	-
	2.2	Human security	6	19	-1	20	1	19	-
	2.3	Outsider security	4	10	3	7	0	7	-
	2.4	Physical security	7	17	-4	21	3	18	-
	2.5	Authentication and authority management	6	15	7	8	4	4	-
	2.6	Access control	7	25	7	18	6	12	-
	2.7	Apply encryption	2	4	3	1	0	1	-
	2.8	Information system introduction and development security	6	17	12	5	0	5	-
	2.9	System and service operation management	7	23	2	21	5	16	-
	2.10	System and service security management	9	36	20	16	5	11	-
	2.11	Accident prevention and response	5	15	-5	20	6	14	-
	2.12	disaster recovery	2	5	3	2	0	2	-
3. Personal information requirements by processing stage (21/91)	3.1	Protective measures when collecting personal information	7	36	36	0	0	0	-
	3.2	Protective measures taken when retaining and using personal information	5	20	20	0	0	0	-
	3.3	Protective measures when providing personal information	4	16	16	0	0	0	-
	3.4	Protective measures when personal information is destroyed	2	8	6	2	0	2	-
	3.5	Protection of information subject rights	3	11	11	0	0	0	-
subtotal			101	328	81	247	49	198	-
4. Industrial security requirements (10/35)	4.1	Industrial technology identification and classification	1	1		1	-	-	1
	4.2	Prevention of technology leaks	3	13		13	-	-	13
	4.3	Research and development security	3	16		16	-	-	16
	4.4	Intellectual property rights protection	1	2		2	-	-	2
	4.5	Industrial security incident response	2	3		3	-	-	3
subtotal			10	35		35	-	-	35
Total			111	363		35	49	198	35

또한, 통합 관리체계는 국제표준과의 정합성을 높여 글로벌 공급망 보안 요구에도 효과적으로 대응할 수 있다. 정책적으로는 중소기업을 위한 간편 인증 도입, 산업통상자원부의 ISMS-P 인증위원회 참여, 관련 법령 개정 등 통합 거버넌스와 법적 근거 마련이 필요함을 제안한다. 한계점으로는 최신 산업현장 요구 반영의 한계, 실질적인 각계 현장 전문가에 의한 검증 미실시, 실증 연구 미흡, 지속적 갱신 방안 미비 등이 있으며, 향후 부처 협업, 국가 비밀 관리에 관한 통합 법안 제정, 실증 연구, 전문

가 검증, 국제표준 연계, 자동화·지능화, 보안 문화 확산 등에 대한 추가 연구가 필요함을 제언한다. 결론적으로, ISMS-P 기반 통합 산업보안 관리체계는 산업기술 보호와 국가 경쟁력 강화를 위한 체계적이고 실질적 대안이며, 기업들 입장에서도 중복 인증 등의 부담을 피할 수 있어 환영받을 수 있는 현실적인 대안임을 다시 한번 강조한다.

References

[1] G. H. Kim and K. S. Ha, "The Research on Security Cognition and Management Status of Technology Outflow about Small-medium Companies in New IT Environment", The Society of Digital Policy & Management, Vol. 11, No. 11, pp. 305-311, Nov. 2013.

[2] S. B. Kwon, H. G. Kim, S. Y. Choi, and H. S. Lee, "The Improvement Method of Digital Forensic for Responding to Technology Leakage of SMEs", The Korean Career·Entrepreneurship & Business Association, Vol. 7, No. 1, pp. 85-101, Jan. 2023. https://doi.org/10.48206/kceba.2023.7.1.85.

[3] Ministry of Trade, Industry and Energy, "Industrial Security Management System Certification Audit Form", Information disclosure, https://www.motie.go.kr/kor/contents/53. [accessed: May 20, 2025]

[4] Korea Internet & Security Agency Certification Examiner, "ISMS-P", https://isms.kisa.or.kr/main/ispims/intro/. [accessed: May 20, 2025]

[5] E. B. Lee and H. Bae, "A Survey on the Latest Research Trends in Retrieval-Augmented Generation", The Transactions of the Korea Information Processing Society (KTSDE), Vol. 13, No. 9, pp. 429-436, Sep. 2024. https://doi.org/10.3745/TKIPS.2024.13.9.429.

[6] D. R. Ko, J. Y. Lee, D. H. Lee, and J. E. Kim, "SBERT-PRO: Predicate Oriented Sentence Embedding Model for Intent and Event Detection", Journal of KIISE (JOK), Vol. 51, No. 2, pp. 165-172, Feb. 2024. https://doi.org/10.5626/JOK.2024.51.2.165.

[7] S. W. Hong and J. P. Park, "Effective Management of Personal Information & Information Security Management System(ISMS-P) Authentication systems", The Korea Academia-Industrial cooperation Society, Vol. 21, No. 1, pp. 634-640, Jan. 2020. https://doi.org/10.5762/KAIS.2020.21.1.634.

[8] I. S. Choi, "Research on Industrial Security Management System Based on ISMS-P Utilizing RAG", Jeju National University, Ph.D. Aug. 2025.

[9] C. B. Yang and Y. S. Kim, "Implementation of Retrieval Augmented Generation (RAG) Model Using LLM: A RapidMiner-Based Approach", Korean Institute of Smart Media, Vol. 14, No. 2, pp. 34-42, Feb. 2025. https://doi.org/10.30693/SMJ.2025.14.2.34.

[10] G. S. Park and J. T. Kim, "Legal search method using S-BERT", The Korean Society Of Computer And Information, Vol. 27, No. 11, pp. 57-66, Nov. 2022. https://doi.org/10.9708/jksci.2022.27.11.057.

[11] D. S. Song and Y. W. Choi, "Redefining the Scope of Industrial Technology in the Act on Prevention of Divulgence and Protection of Industrial Technology", The Institute for Legal Studies Dong-A University, No. 95, pp. 229-261, May 2022. https://doi.org/10.31839/DALR.2022.05.95.229.

[12] W. Kim, Y. Y. Cho, and S. C, Kang, "A Study on the Expansionon Certification of Information Security and Personal Information Security Management System", International Next-generation technology Convergence Association, Vol. 6, No. 8, pp. 1353-1364, Aug. 2022. https://doi.org/10.33097/JNCTA.2022.06.08.1353.

[13] K. I. Song and J. S. Jang, "Characteristics and Implementation of ISO/IEC 27001 : 2013 Information Security Management System", Vol. 14, No. 2, pp. 108-113, Jun. 2014.

[14] E. K. Park and S. H. Wang, "Implications of the Export Control Reform Act of 2018", Korea Legislation Research Institute, No. 61, pp.

299-321, Dec. 2021. https://doi.org/10.22851/kjlr.2021..61.009.

[15] J. B. Kim, "Economic Espionage Act in USA", Journal of Law (Journal of Law), Vol. 12, No. 1, pp. 183-203, Dec. 2001.

[16] S. S. Hong, "A Study on The Background and Implications of The DTSA(Defend Trade Secrets Act of 2016) of the United States", Gachon Law Review (Gachon Law Review), Vol. 12, No. 4, pp. 43-78, Dec. 2019. https://doi.org/10.15335/GLR.2019.12.4.002.

[17] M. Tu and J. J. Kim, "A Comparative Study of EU Directive 95/46 and General Data Protection Regulation - Its Implications for China's Legislation", The Korea-China Society of Law, Vol. 30, pp. 49-71, May 2017. https://doi.org/10.22415/clr.2017.30..003.

[18] J. W. Kim, "Analysis of Issues and Prospects with the Right to Explanations as a Control Measure for Algorithm-Based Automated Decision-Making in EU-GDPR", Democratic Legal Studies, No. 69, pp. 277-298, Mar. 2019. https://doi.org/10.15756/dls.2019..69.277.

[19] J. S. Jung, "Comparative legal study of the punishable provision to prevent outflow and conserve Industrial Technologies : focus on the US, Japan, and China", Korean National Security and Public Safety Association, No. 4, pp. 8-32, Jun. 2017.

[20] M. J. Lee, "China Manufacturing 2025 and Sino-American Technology Hegemony Competition", The Journal of Modern China Studies, Vol. 20, No. 4, pp. 1-40, Jun. 2019. https://doi.org/10.35820/JMCS.20.4.1.

[21] Korean Standards Association, ISO certification, https://www.ksa.or.kr/ksa_kr/index.do. [accessed: May 20, 2025]

[22] J. Y. Choi, E. J. Choi, and M. J. Kim, "A Comparison Study between Cloud Service Assessment Programs and ISO/IEC 27001:2013", Journal of Digital Convergence, Vol. 12, No. 1, pp. 405-414, Dec. 2014. https://doi.org/10.14400/JDPM.2014.12.1.405.

[23] J. H. Jin, S. S. Park, J. T. Kim, and K. H. Han, "A Study on Application Methodology of SPDL Based on IEC 62443 Applicable to SME Environment", KIPS Transactions on Computer and Communication Systems (KTCCS), Vol. 11, No. 6, pp. 193-204, Jun. 2022.

[24] Y. W. Kim, D. Y. Kim, H. H. Seo, and Y. M. Kim, "Content-based Korean journal recommendation system using Sentence BERT", Vol. 29, No. 3, pp. 37-55, Sep. 2023. https://doi.org/10.13088/jiis.2023.29.3.037.

[25] G. S. Park and J. T. Kim, "Legal search method using S-BERT", Journal of The Korea Society of Computer and Information (JKSCI), Vol. 27, No. 11, pp. 57-66, Nov. 2022. https://doi.org/10.9708/jksci.2022.27.11.057.

[26] J. M. Park, "An Evaluation of ChatGPT's Understand of Korean Grammar Concepts -Exploring Its Educational Potential through Semantic Similarity Analysis-", Journal of CheongRam Korean Language Education, No. 103, pp. 309-336, Jan. 2025. https://doi.org/10.26589/jockle..103.202501.309.

[27] J. Kim and N. Park, "Development of a board game-based gamification learning model for training on the principles of artificial intelligence learning in elementary courses", Journal of The Korean Association of Information Education, Vol. 23, No. 3, pp. 229-235, Jun. 2019. https://doi.org/10.14352/jkaie.2019.23.3.229.

[28] J. Kim and N. Park, "Role Based Access Control based File Access Control Mechanism with Smart Contract", Journal of KIIT, Vol. 17, No. 9, pp. 113-121. Sep. 2019. http://dx.doi.org/10.14801/jkiit.2019.17.9.113.

[29] M. Kim, J. Moon, D.o Won, and N. Park, "Revisit of Password-Authenticated Key Exchange Protocol for Healthcare Support Wireless Communication", Electronics, Vol. 9, No. 5, Art

No. 733, Apr. 2020. https://doi.org/10.3390/electronics9050733.

[30] J. Kim and N. Park, "Dynamic/Static Object Segmentation and Visual Encryption Mechanism for Storage Space Management of Image Information", Journal of KMS, Vol. 22, No. 10, pp. 1199-1207, Oct. 2019.

[31] P. W. Khan, Y.-C. Byun, and N. Park, "IoT-Blockchain Enabled Optimized Provenance System for Food Industry 4.0 Using Advanced Deep Learning", Sensors, Vol. 20, No. 10, Art No. 2990, May 2020. https://doi.org/10.3390/s20102990.

[32] D. Lee and N. Park, "A Study on COP-Transformation Based Metadata Security Scheme for Privacy Protection in Intelligent Video Surveillance", Journal of KIISC, Vol. 28, No. 2, pp. 417-428, Apr. 2018.

[33] N. Park, Y. Sung, Y. Jeong, S.-B. Shin, and C. Kim, "The Analysis of the Appropriateness of Information Education Curriculum Standard Model for Elementary School in Korea", International Conference on Computer and Information Science, Springer, pp. 1-15, Jun. 2018. https://doi.org/10.1007/978-3-319-98693-7_1.

[34] J. Kim and N. Park, "BlockChain Technology Core Principle Education of Elementary School Student Using Gamification", Journal of The Korean Association of Information Education, Vol. 23, No. 2, pp. 141- 148, Apr. 2019.

[35] D. Lee and N. Park, "Technology and Policy Post-Security Management Framework for IoT Electrical Safety Management", The Transactions of The Korean Institute of Electrical Engineers, Vol. 66, No. 12, pp. 1879-1888, Dec. 2017.

저자소개

최 익 서 (Ikseo Choi)

1998년 6월 ~ 2024년 2월 : 제주경찰청 산업기술보호수사팀장
2023년 3월 ~ 2025년 8월 : 제주대학교 융합정보보안학협동과정(박사)
2024년 7월 ~ 현재 : 제주대학교 사이버보안인재교육원 특별연구원
관심분야 : 산업기술보호, 산업보안, 개인정보, 인공지능, 블록체인, 디지털포렌식, IoT

최 은 선 (Eunsun Choi)

2022년 8월 : 제주대학교 컴퓨터교육전공(교육학박사)
2020년 3월 ~ 2023년 12월 : 제주대학교 사이버보안인재교육원 연구원
2024년 1월 ~ 2024년 9월 : 요크대학교 물리학, 공학 및 기술학부 박사후연구원
2024년 9월 ~ 현재 : 광주교육대학교 컴퓨터교육과 교수
관심분야 : 인공지능교육, 정보교육, 인공지능 인문학

박 남 제 (Namje Park)

2008년 2월 : 성균관대학교 컴퓨터공학과(공학박사)
2003년 4월 ~ 2008년 12월 : 한국전자통신연구원 정보보호연구단 선임연구원
2009년 1월 ~ 2009년 12월 : 미국 UCLA대학교 공과대학 Post-Doc, WINMEC 연구센터 Staff Researcher
2010년 1월 ~ 2010년 8월 : 미국 아리조나 주립대학교 컴퓨터공학과 연구원
2010년 9월 ~ 현재 : 제주대학교 초등컴퓨터교육전공, 대학원 융합정보보안학과 교수
2011년 9월 ~ 현재 : 창의교육거점센터장, 정보영재 주임교수, 사이버보안인재교육원장
관심분야 : 융합기술보안, 컴퓨터교육, 해사클라우드