JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 31 No. 11, pp. 319-326, November 2026
https://doi.org/10.9708/jksci.2026.31.11.319

A Method of Automated Security Control Mapping for Heterogeneous Security Guidelines using BGE-M3 and GraphDB

Yun Gyu Eo*, Sun Woo Shin**, Hyeon Jun Son*, Su Man Nam***

*Student, Dept. of Digital Security, Cheongju University, Cheongju, Korea
**M.S. Student, Dept. of Information Security, Korea University, Seoul, Korea
***Professor, Dept. of Digital Security, Cheongju University, Cheongju, Korea

[Abstract]

The Cloud Security Assurance Program (CSAP), the Information Security and Personal Information Management System (ISMS-P), and ISO/IEC 27001 differ in control classification and terminology, making it difficult for organizations to interpret and manage security requirements in an integrated manner. This paper proposes an automated security control mapping method using BGE-M3 and a graph database, organizing 248 controls extracted from these heterogeneous frameworks into 16 domains and 67 categories with profiles constructed from representative keywords. It normalizes and combines semantic relevance scores between controls and category profiles from BGE-M3's Dense, Sparse, and ColBERT components, assigns each control to the category with the highest final score, and represents mappings as relationships between graph database nodes. Comparing the automated mapping results for all 248 controls with manually annotated ground truth showed a Top-1 mapping accuracy of 90.32% and a Top-3 accuracy of 96.77%.

▸ **Key words**: Automated Security Control Mapping, BGE-M3, Graph Database, CSAP, ISMS-P, ISO/IEC 27001

[요 약]

클라우드 보안인증제(CSAP), 정보보호 및 개인정보보호 관리체계(ISMS-P), ISO/IEC 27001은 통제 항목의 분류 체계와 용어가 달라 기업과 기관이 보안 요구사항을 통합적으로 해석하고 관리하기 어렵다. 본 논문은 GraphDB를 활용한 BGE-M3 기반 보안 컨트롤 자동 매핑 기법을 제안하며, 이종 보안 가이드라인에서 추출한 248개 컨트롤을 16개 도메인과 67개 카테고리로 구성하고 대표 키워드로 카테고리 프로파일을 구축한다. BGE-M3의 Dense, Sparse, ColBERT로 산출한 컨트롤과 프로파일 간 관련도 점수를 정규화하고 결합해 각 컨트롤을 최종 점수가 가장 높은 카테고리에 할당하고, 결과를 GraphDB의 노드 간 관계로 표현한다. 전체 248개 컨트롤의 자동 매핑 결과를 수작업 정답지와 비교한 결과, 최상위 후보 일치율은 90.32%, 상위 3개 후보 내 정답 포함률은 96.77%로 나타났다.

▸ **주제어**: 보안 컨트롤 자동 매핑, BGE-M3, 그래프 DB, CSAP, ISMS-P, ISO/IEC 27001

• First Author: Yun Gyu Eo, Sun Woo Shin, Corresponding Author: Su Man Nam
*Yun Gyu Eo (henry4787@cju.ac.kr), Dept. of Digital Security, Cheongju University
**Sun Woo Shin (swshin@cloud-air.kr), Dept. of Information Security, Korea University
*Hyeon Jun Son (shj13918957@cju.ac.kr), Dept. of Digital Security, Cheongju University
***Su Man Nam (smnam@cju.ac.kr), Dept. of Digital Security, Cheongju University
• Received: 2026. 09. 18, Revised: 2026. 10. 16, Accepted: 2026. 11. 02.

Copyright © 2026 The Korea Society of Computer and Information
http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945
www.kci.go.kr

I. Introduction

최근 클라우드 전환으로 국내외 기업과 공공기관이 준수해야 할 정보보호 및 개인정보보호 규제가 복잡해졌다. 이들은 서비스의 신뢰성을 확보하기 위해 클라우드 보안 인증제(CSAP), 정보보호 및 개인정보보호 관리체계(ISMS-P), 글로벌 표준인 ISO/IEC 27001 등 이종 간 보안 관리 가이드라인을 모두 충족해야만 한다[1, 2]. 그러나, 각 보안 가이드라인은 목적에 따라 항목, 이름 규칙, 기술 수준 등이 다르게 정의되어 있다[3, 4]. 그리하여 기업과 기관에서는 적은 자원으로 이들을 직접 연결하는 데 어려움을 겪고 있다[5].

이러한 문제를 해결하기 위해, 본 논문에서는 이종 보안 가이드라인에서 GraphDB를 활용한 BGE-M3 기반 보안 컨트롤 자동 매핑 기법을 제안한다. 제안 기법은 CSAP, ISMS-P, ISO/IEC 27001로부터 추출한 248개의 컨트롤을 대상으로 16개 도메인, 67개 카테고리를 생성한다. 생성된 분류 체계는 대표 키워드를 통해 카테고리 프로파일을 만든다. 이후 BGE-M3의 Dense, Sparse, ColBERT 알고리즘들을 활용하여 평가 함수를 통해 유사도 점수를 계산한다. 제안 기법에서 산출된 점수는 GraphDB에서 자동으로 노드(컨트롤)-노드(카테고리) 관계로 만들게 된다.

본 논문의 본문 구성은 다음과 같다. 2장에서는 관련 연구 및 GraphDB의 배경 이론을 살펴보고, 3장에서는 제안하는 자동 매핑 기법의 상세 절차를 소개한다. 4장에서는 전문가 수작업 정답지와의 비교를 통한 실험 결과를 제시하며, 5장에서는 본 연구의 결론 및 향후 연구 과제를 제시한다.

II. Background and Related Work

1. Security Compliance Frameworks

CSAP는 공공기관에 안전성 및 신뢰성이 검증된 민간 클라우드 서비스를 공급하기 위해 KISA가 주관하는 클라우드 서비스 보안 인증 제도이다[1]. 이 제도는 클라우드 서비스의 높은 수준의 정보보안을 통해 사용자들이 안심하고 사용할 수 있도록 안전한 클라우드를 지향한다. 인증 대상은 IaaS(인프라), PaaS(개발환경), SaaS(응용소프트웨어) 등 공공에 클라우드 서비스를 제공하려는 사업자이다. 인증 기준은 데이터 중요도(상, 중, 하)와 서비스 유형(IaaS, PaaS, SaaS)에 따라 약 110~117개의 통제 항목으로 구성된다. CSAP는 공공 클라우드 보안 검증은 국정원 중심의 단일 검증체계로 개편 예정이며(2027년 7월 시행 예정), ISMS 체계와 연계 예정이다[6].

ISMS-P는 기업이나 조직이 주요정보 자산과 고객의 개인정보를 안전하게 보호하기 위해 종합적인 관리 체계가 기준에 적합한지 인증하는 제도이다[2]. 이 제도는 일반 정보보안 영역뿐만 아니라 개인정보 처리 단계별(수집, 이용, 제공, 파기 등) 법적 요구사항까지 함께 심사한다. 인증 기준은 관리체계 수립 및 운영 16개, 보호대책 요구사항 64개, 개인정보 처리단계별 요구사항 21개 항목으로 총 101개로 구성된다[2].

ISO 27001:2022 Annex A는 기업이 정보 자산을 보호하고 보안 위험을 줄이기 위해 도입하는 정보보안 수칙이다. ISO 27001(본문 일부)이 정보보안 관리체계(ISMS)의 운영 프로세스 구축을 다룬다면, 이 보안 수칙은 실제 업무 환경에 적용해야 하는 실질적인 보안 기술과 가이드라인을 제공한다. 이 가이드라인은 조직적 통제 37개, 개인적 통제 8개, 물리적 통제 14개, 기술적 통제 34개의 항목으로 구성된다.

Table 1. Comparison of CSAP, ISMS-P, and ISO/IEC 27001

Type	CSAP	ISMS-P	ISO 27001
Supervising Authority	KISA, MSIT*	KISA, MSIT, PIPC**	ISO/IEC
Scope	Public Cloud	Domestic Companies	Global / Exporting Enterprises
Categories	Administrative, Physical, Technical & Cloud-specific	Management System, Security Measures, Personal Information	Organizational, People, Physical, Technological
Number of Controls	110~117 (Varies by type)	101	93
* MSIT : Ministry of Science and ICT ** PIPC: Personal Information Protection Commission			

Table 1은 국내외 대표 보안 관리체계인 CSAP, ISMS-P, ISO 27001:2022 Annex A를 비교한 내용이다. 상기 세 제도는 접근 통제, 암호화, 인적 보안 등 핵심 보안 요구사항에서 공통된 통제 목표를 구성함에도 불구하고, 분류 체계와 용어 및 문서 구조의 상이함으로 인해 상호 연계성이 부재하다[3, 7]. 이에 따라 다중 인증을 준비하는 조직은 개별 대응에 따른 불필요한 리소스 낭비와 해석 오류에 따른 실무적 부담을 겪고 있다[4, 5, 8].

기존 연구에서는 보안 온톨로지를 통한 표준 간 매핑[4]과 Transformer 기반 계층적 분류를 통한 매핑 후보 추

www.kci.go.kr

천[5]이 제안되었다. 본 연구는 키워드 기반 공통 카테고리 프로파일에 BGE-M3의 세 관련도 점수를 결합하여 컨트롤을 자동 분류하고, 그 결과를 GraphDB의 관계로 연결한다는 점에서 차별성을 갖는다.

2. Semantic Textual Similarity

SBERT(Sentence-BERT)는 샴 네트워크(Siamese Network)와 풀링(Pooling)을 결합해 문장을 고정 차원 벡터로 변환하고 실시간 유사도를 계산하는 모델이다[9]. 샴 네트워크는 가중치를 공유하는 두 개 이상의 쌍둥이 인코더 서브 네트워크를 병렬로 배치하는 구조이다. 풀링은 BERT가 출력한 가변길이의 단어별 벡터들을 압축하여 문장 전체를 대표하는 하나의 고정 크기 벡터로 압축하는 연산이다[10]. 이들은 아래 수식(1)과 같이 Cosine Similarity의 수식을 통해 유사도 계산을 한다.

$$\text{Cosine Similarity}(u,v) = \frac{u \cdot v}{\|u\|_2\|v\|_2} = \frac{\sum_{i=1}^{d} u_i v_i}{\sqrt{\sum_{i=1}^{d} u_i^2}\sqrt{\sum_{i=1}^{d} v_i^2}} \quad (1)$$

예를 들어, '문장1'은 "소프트웨어 취약점을 점검한다", '문장2'는 "보안 결함을 분석한다"가 있다고 가정한다. '문장1'의 벡터는 $u = [1.0, 2.0, 3.0]$이며, $v = [2.0, 3.0, 4.0]$이다. $u \cdot v$의 계산 방법은 수식(2)와 같다.

$$u \cdot v = (1.0 \times 2.0) + (2.0 \times 3.0) + (3.0 \times 4.0) = 2.0 + 6.0 + 12.0 = 20.0 \quad (2)$$

$\|u\|_2\|v\|_2$의 계산 방법은 수식(3), (4)와 같다.

$$\|u\|_2 = \sqrt{1.0^2 + 2.0^2 + 3.0^2} = \sqrt{1+4+9} = \sqrt{14} \approx 3.742 \quad (3)$$

$$\|v\|_2 = \sqrt{2.0^2 + 3.0^2 + 4.0^2} = \sqrt{4+9+16} = \sqrt{29} \approx 5.385 \quad (4)$$

최종 코사인 유사도 결과는 수식 (5)와 같이 약 0.99로, 매우 유사한 의미를 지녔다고 볼 수 있다.

$$\text{Cosine Similarity}(u,v) = \frac{20.0}{3.742 \times 5.385} = \frac{20.0}{20.151} \approx 0.9925 \quad (5)$$

3. Graph Databases

GraphDB[11, 12]는 기존 RDBMS의 테이블 형태가 아닌, 노드 간의 관계를 나타내는 간선(Edge, Relationship)으로 직접 연결하여 관리하는 데이터베이스이다. GraphDB에서 노드는 데이터의 개체(Entity)이며, 간선은 개체 간의 연결, 방향성, 관계 유형을 갖는다(Fig. 1 참고). 노드와 간선 모두에 키-값(Key-Value) 형태로 메타데이터를 저장할 수 있다[11]. 반면 RDBMS(Relational Database Management System)는 외래키와 JOIN을 이용해 개체 간 연관성을 조회하며, GraphDB에서는 이를 노드와 관계로 표현하고 관계 패턴으로 조회할 수 있다[15]. RDBMS는 기존 SQL과 테이블 구조를 활용할 수 있다는 장점이 있으며, GraphDB는 개체 간 연결을 명시적으로 표현하고 관계 중심으로 탐색할 수 있다는 장점이 있다. 다만, Neo4j 도입에는 그래프 모델링과 Cypher에 대한 추가 학습 및 운영 환경 구성이 필요하다. 본 연구에서는 공통 카테고리에 연결된 이종 가이드라인의 컨트롤을 관계 중심으로 표현하고, 해당 카테고리를 통해 컨트롤 간 연관성을 탐색 및 관리하기 위해 GraphDB를 채택하였다.

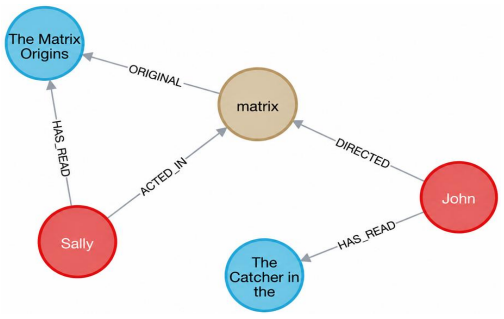


Fig. 1. Example of a Graph Database Representation

GraphDB에는 Neo4j, AllegroGraph, ArangoDB 등이 있다[13]. 이 중 Neo4j는 노드 간 관계를 직접 참조할 수 있는 구조로 저장한다. 또한, '(해커)-[:공격]->(취약점)-[:영향]->(서버)'처럼 직관적인 Cypher 쿼리 언어를 사용할 수 있다[14].

www.kci.go.kr

III. Proposed Method

1. Overview

본 논문은 3개의 가이드라인으로부터 추출된 정보로부터 BGE-M3를 활용하여 GraphDB에서 컨트롤과 카테고리 간 자동 연결 기법을 제안한다. 제안 기법은 각 컨트롤과 67개의 카테고리 프로파일의 관련도를 산출하고, 정규화된 점수를 합산하여 가장 높은 카테고리와 연결한다. Fig. 2는 제안 기법의 절차를 보여준다.

(1) 컨트롤(Control) 정의 : CSAP, ISMS-P 및 ISO/IEC 27001에서 총 248개의 보안 컨트롤 정의
(2) 카테고리(Category) 프로파일 구축 : 16개 도메인과 67개 카테고리를 정의하고, 도메인 이름, 카테고리 이름, 대표 키워드 활용 카테고리 프로파일 구축
(3) 의미 관련도 산출 : 각 컨트롤을 67개의 카테고리 프로파일과 비교하여 BGE-M3의 Dense, Sparse 및 ColBERT를 통해 각각 점수 산출
(4) 다중 점수 정규화 및 통합 : 세 점수를 각각 0과 1 사이로 정규화하고 설정된 가중치에 따라 $HybridScore$로 계산
(5) 후보 순위화 및 범주화 할당 : 67개의 카테고리를 $HybridScore$를 기준으로 Top-1의 카테고리를 해당 컨트롤과 연결

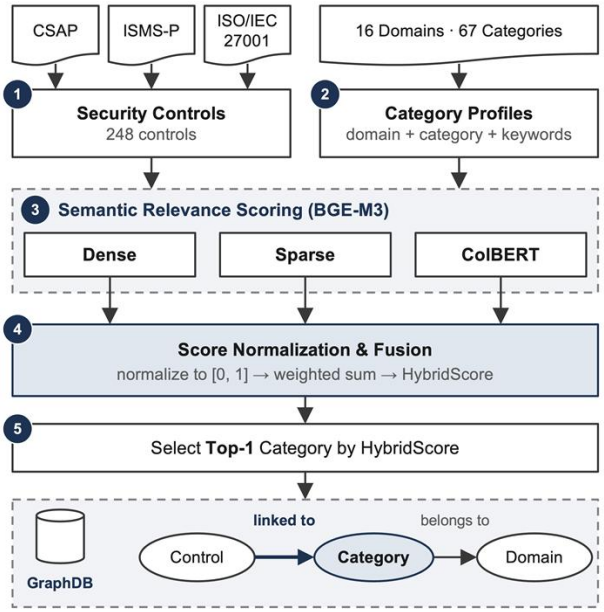


Fig. 2. Architecture of the Proposed Method

2. Detailed Procedure

본 장은 제안 기법의 5단계 절차를 상세하게 소개한다.

2.1 Control Extraction

제안 기법의 컨트롤 정의 단계는 GraphDB의 노드를 결정하는 것이다. 제안 기법은 GPT-5-Codex를 활용하여 GraphDB의 컨트롤을 CSAP, ISMS-P, ISO/IEC 27001:2022 Annex A로부터 추출한다. CSAP는 의미가 유사하거나 중복되는 세부 요구사항을 통합하여 14개 상위 분야와 27개 세부 주제로 구분하였다. 각 주제에서 핵심 통제 목적을 나타내는 대표 컨트롤을 2개씩 정의하여 연구용 컨트롤 54개로 재구성하였다. 이를 ISMS-P 101개, ISO/IEC 27001 93개와 합하여 Table 2와 같이 총 248개 컨트롤로 구성하였다.

Table 2. Number of Security Controls Extracted from Each Framework

Security Management Guidelines	Number of Controls
CSAP	54
ISMS-P	101
ISO 27001	93
Total	**248**

각 컨트롤에는 컨트롤 ID, Framework, 제목, 세부 요구사항 등의 정보도 포함되어 있다. Table 3은 컨트롤의 세부 정보의 예시를 보여준다.

Table 3. Examples of Extracted Security Control Attributes

Type	CSAP	ISMS-P	ISO 27001
Control	Least privilege principle and control of privileged account use	Network access control	Privileged access rights
Control ID	CSAP-033	ISMSP-041	A.8.2
Framework	CSAP	ISMS-P	ISO 27001
Control Domain	Access control and account management	Section 2: Protective Measure Requirements	Technological controls (A.8)
Control Item	9.2 Access privilege control and session management	2.6 Access Control	N/A
Detailed Requirement	Least privilege principle and control of privileged account use	Network access control	Privileged access rights

www.kci.go.kr

2.2 Category Profile Construction

다음은 프로파일 구축 단계로서, 각 컨트롤은 카테고리들과 연결하기 위해 프로파일을 구축한다. 한 개의 카테고리는 id, name, domain_id, description을 갖는다. 예를 들어, GOV-01 카테고리는 name이 '정책·지침', domain_id가 “GOV”, description이 “정책, 조직, 책임, 경영진, 감사 및 준수”이 된다. 본 분류체계는 CSAP, ISMS-P, ISO/IEC 27001의 통제항목을 유사한 보안 목적에 따라 공통 개념으로 묶고, 이를 상위 보안 영역과 세부 통제 개념의 두 단계로 구분한 것이다. 상위 영역은 16개 도메인으로, 각 영역의 세부 개념은 전체 67개 카테고리로 구성하며, 개별 가이드라인의 고유 요구사항도 해당 영역에 포함한다.

도출된 카테고리에서는 접근권한 제한, 필요한 권한만 허용, 권한 회수 등과 같이 최소 권한을 요구하지만, 카테고리 이름만으로 인지하기 어렵다. 이를 보완하기 위해 연구자가 카테고리 정의와 연결된 통제항목을 검토하여, 카테고리의 핵심 의미를 나타내고 인접 카테고리와 구별되는 대표 키워드를 카테고리당 4~7개씩 수동 선정하였다. 각 카테고리의 프로파일은 도메인 이름, 카테고리 이름 및 대표 키워드로 구성한다. Table 4는 Category IAM-03의 프로파일 예이다.

Table 4. Example of Category Profile IAM-03

Domain: Account & Access Control └── Category: IAM-03 Privilege & Least Privilege └── Keywords: least privilege, access rights, privilege granting, …

Table 4와 같은 방법으로 67개의 카테고리 모두 프로파일을 구축한다. 구축된 프로파일은 Table 5와 같이 전처리하여 BGE-M3에 입력한다.

Table 5. Preprocessed Category Profile Given as Input to BGE-M3

Account & Access Control | Privilege & Least Privilege least privilege | access rights | privilege granting privilege modification | privilege revocation privilege review | need-to-know

2.3 Semantic Relevance Scoring

의미 관련도 산출 단계는 컨트롤 문장과 카테고리 프로파일을 BGE-M3에 입력하여 관련도를 출력한다. BGE-M3에서는 두 문장의 관련성을 Dense, Sparse, ColBERT의 알고리즘을 각각 사용한다.

먼저, Dense는 컨트롤 문장과 카테고리 프로파일을 각각 고정 차원 벡터로 변환하고, L2 정규화된 두 벡터의 내적으로 코사인 유사도를 계산한다[16, 17]. 예를 들어, 컨트롤은 “최소 권한 부여 원칙 및 특권 계정 사용 통제”이고, 카테고리는 “계정·접근통제 권한·최소권한”이라고 가정하자. 두 문장은 전체적으로 권한 관리와 최소권한에 관한 내용이므로 약 0.83이 된다(값이 높을수록 유사도 높음).

Sparse는 컨트롤 문장과 카테고리 프로파일에 공통으로 포함된 토큰에 대해, BGE-M3가 산출한 양쪽 토큰 가중치를 곱한 뒤 합산하여 관련도 점수를 계산한다[16, 18]. 컨트롤과 카테고리의 중요 토큰은 “최소, 권한, 부여”가 된다. 이때 Sparse는 약 0.13이 된다(값이 높을수록 유사도 높음).

ColBERT는 L2 정규화된 토큰 벡터의 내적을 이용하여, 컨트롤의 각 토큰과 카테고리 프로파일의 모든 토큰 간 유사도를 계산한다. 이후 컨트롤 토큰별로 가장 높은 유사도를 선택하고, 이를 평균하여 관련도 점수를 산출한다[16, 19]. Table 6은 ColBERT의 토큰 매핑 결과이다. 컨트롤과 카테고리 프로파일의 결과는 약 0.78이 된다.

Table 6. Example of Token-Level Matching Using ColBERT

Control expression		Category profile expression
required privilege	↔	least privilege
privilege permission	↔	privilege granting
privilege verification	↔	privilege review

2.4 Score Normalization and Fusion

의미 관련도 산출 단계에서 계산된 Dense, Sparse, ColBERT 점수는 서로 다른 범위를 가질 수 있다[20]. 본 단계에서는 각 컨트롤과 67개 카테고리 사이에서 계산한 Dense, Sparse, ColBERT 점수를 종류별로 나누어 Min-Max 정규화한다. 각 점수에서 같은 종류의 최솟값을 빼고 최댓값과 최솟값의 차이로 나누어 0~1 범위로 변환하며, 67개 점수가 모두 같으면 정규화 결과를 모두 0으로 설정한다. 다음은 제안 기법의 최종 유사도 결과를 보여주는 $HybridScore$의 수식이다.

$$HybridScore = (\mathrm{Dense} \times w_D) + (\mathrm{Sparse} \times w_S) + (\mathrm{ColBERT} \times w_C) \quad (6)$$

수식 (6)에서, w_D, w_S, w_C는 모두 가중치이다. 가중치는 합이 1이 되도록 0.1 간격으로 설정하고, 최소 두 종류

www.kci.go.kr

의 점수를 사용하는 63개 조합을 비교하였다. 이 중 Top-1 정확도가 가장 높은 Dense 0.1, Sparse 0.2, ColBERT 0.7을 최종 가중치로 선정하였다.

2.5 Candidate Ranking and Category Assignment

이 단계는 이전 단계에서 계산된 각 카테고리의 프로파일의 $HybridScore$를 통해 후보를 순위화 및 범주화를 할당하는 단계이다. Table 7은 컨트롤 CSAP-033의 측정한 다중 점수 결과의 예이다.

Table 7. Hybrid Scores and Ranking of Candidate Categories for CSAP-033

Category	HybridScore
IAM-03 Privilege & Least Privilege	1.0000
IAM-04 Privileged & Special Rights	0.8778
IAM-01 Account & Identity Management	0.6475
…	…
Remaining 64 categories	-

67개 카테고리 중 가장 높은 순위 3개는 IAM-03 권한·최소권한(1.0000), IAM-04 특권·특수권한(0.8778), IAM-01 계정·식별관리(0.6475)이다. 이들은 CSAP-033과 연관성이 높은 후보들이 된다. 이때 컨트롤 CSAP-033의 '최소 권한 부여 원칙 및 특권 계정 사용 통제'는 IAM-03의 '권한·최소권한'이 주요 카테고리(Top-1)로 설정한다. GraphDB에서 Table 8과 같이 연결성을 정의한다.

Table 8. Example of Control-Category Mapping in a Graph Database

(CSAP-033)-BELONGS_TO->(IAM-03)

나머지 순위 2개는 직접 연결되지 않고 전문가가 확인할 수 있는 추천 후보로 사용한다.

IV. Experimental Results

본 장은 제안 기법의 효율성을 측정하기 위해 사전에 구축한 수작업 정답지와 비교하여 성능을 측정한다. 실험 환경 및 소프트웨어 구성은 Table 9와 같다.

Table 9. Experimental Environment and Software Configuration

Type	Specification or Version
Operating System	macOS 26.6.2
Processor	Apple M4 10-Core
Memory	16GB
Python	3.9.6
BGE-M3	BAAI/bge-m3
FlagEmbedding	1.4.2
PyTorch	2.8.0
Transformers	4.57.6
Sentence-Transformers	5.1.2
Neo4j Python Driver	5.28.4

수작업 정답지는 산학 보안 전문가들의 협업을 통해 구축하였으며, 초기 매핑 결과가 불일치한 항목은 재검토하여 최종 합의를 이루었다. 또한, 구축된 정답지 데이터는 직관적인 확인과 탐색이 가능하도록 그래프 형태로 웹을 통해 접근이 가능하며, 이의 소스 파일은 깃허브[21]에 공개하고 있다.

제안 기법과 정답지 카테고리가 서로 일치하면 성공으로 처리한다. Fig. 3은 컨트롤 CSAP-033의 비교 결과 화면이다.

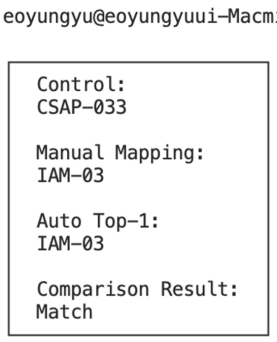


Fig. 3. Comparison of Manual and Automated Mapping Results for CSAP-033

이 과정은 3장 2.1절에서 추출한 컨트롤 248개 전체를 대상으로 한다. Table 10은 수작업 정답지와 비교하여 제안 기법의 일치율을 보여준다.

Table 10. Top-k Mapping Accuracy against the Manually Annotated Ground Truth

Metric	Top-1	Top-2	Top-3
Match (count)	224	238	240
Mismatch (count)	24	10	8
Accuracy (%)	90.32	95.97	96.77

www.kci.go.kr

제안 기법에서 Top-1 이내 불일치 개수는 24개이다. 이는 의미가 유사한 Category의 중복, 여러 통제 목적이 포함된 문장, 문맥이 부족한 짧은 문장 등에서 주로 발생하였다. 이 중 16개는 수동 Category가 Top-3에 포함되어 있었으나 유사한 다른 Category가 더 높은 점수를 받은 경우이며, 나머지 8개는 Top-3에도 포함되지 않았다. 이러한 불일치는, 제안 기법은 문장 자체를 중심으로 판단하는 반면, 수작업 정답지는 상위 통제 분야와 관리 목적까지 고려하므로 차이가 발생한다.

Table 11은 동일한 실험 조건에서 Dense, Sparse, ColBERT의 단독 사용과 결합 사용에 따른 매핑 정확도를 비교한 결과이다. 결합 방식은 단독 방식 중 가장 높은 정확도를 보인 ColBERT 대비 Top-1과 Top-3 정확도가 각각 2.01%p 높아, 세 점수 결합에 따른 성능 향상을 확인하였다.

Table 12는 주요 가중치 조합의 매핑 정확도를 비교한 결과이다. Top-3 정확도는 (0.5, 0.3, 0.2)에서 가장 높았으며, 본 연구는 최종 할당되는 카테고리의 정확도를 우선하여 Top-1 정확도가 가장 높은 (0.1, 0.2, 0.7)을 선정하였다.

Table 11. Comparison of Mapping Accuracy by Scoring Method

Scoring Method	Top-1 Accuracy (%)	Top-3 Accuracy (%)
Dense	85.48	93.55
Sparse	58.06	77.02
ColBERT	88.31	94.76
Dense + Sparse + ColBERT	90.32	96.77

Table 12. Mapping Accuracy for Selected Weight Combinations

w_D	w_S	w_C	Top-1 Accuracy (%)	Top-3 Accuracy (%)
0.1	0.2	0.7	90.32	96.77
0.1	0.1	0.8	89.92	95.16
0.4	0.2	0.4	89.11	97.98
0.5	0.3	0.2	87.50	98.39

V. Conclusions

제안 기법은 이종 보안 가이드라인의 통제 항목을 체계적으로 통합 및 관리하기 위해, GraphDB와 BGE-M3를 활용하여 컨트롤과 카테고리를 자동으로 연결한다. 제안 기법은 3개의 보안 관리 가이드라인(CSAP, ISMS-P, ISO/IEC 27001)로부터 248개 컨트롤과 16개 도메인, 67개 카테고리를 만든다. 이를 기반으로 대표 키워드가 반영된 카테고리 프로파일을 구축한 뒤, BGE-M3의 Dense, Sparse, ColBERT 다중 점수를 정규화하고 평가 함수를 통해 점수를 산출한다. 산출된 점수는 GraphDB에서 높은 점수를 대상으로 각 컨트롤에 적합한 카테고리를 자동으로 연결한다.

제안 기법은 사전에 구축된 수작업 정답지와 비교할 때, Top-1 카테고리 이내에서 전체 248개 컨트롤 중 224개(90.32%)가 일치하였다. 뿐만 아니라, Top-3 추천 범위 내 일치율은 96.77%(240개)이다.

향후 연구에서는 복합적인 목적을 포함하거나 문맥이 짧아 오분류된 통제 항목의 매핑 정확도를 개선하기 위해, 도메인 특화 유사도 산출 알고리즘을 고도화하고 다양한 임베딩 모델과의 비교 검증을 거쳐 매핑 성능을 개선할 것이다.

ACKNOWLEDGEMENT

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (RS-2026-25588760, Contribution Rate: 70%).

This work was supported by the Korea Evaluation Institute of Industrial Technology (KEIT) and the Ministry of Trade, Industry & Energy (MOTIE) of the Republic of Korea (No. RS-2022-00142509, Contribution Rate: 30%).

REFERENCES

[1] Korea Internet & Security Agency, "Cloud Service Security Certification (CSAP)," KISA, https://www.kisa.or.kr/1050603, accessed September 14, 2026.

[2] Personal Information Protection Commission, "ISMS-P Certification Criteria," Privacy Portal, https://www.privacy.go.kr/front/contents/cntntsView.do?contsNo=59, accessed September 14, 2026.

[3] K. Scarfone, M. Souppaya, and M. Fagan, "Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines," NIST IR 8477, February 2024. DOI: 10.6028/NIST.IR.8477.

[4] S. Ramanauskaitė, D. Olifer, N. Goranin, and A. Čenys, "Security Ontology for Adaptive Mapping of Security Standards," IJCCC, Vol. 8, No. 6, pp. 878-890, December 2013. DOI: 10.15837/ijccc.2013.6.764.

[5] V. Agarwal, R. Bar-Haim, L. Eden, N. Gupta, Y. Kantor, and

www.kci.go.kr

A. Kumar, "AI-Assisted Security Controls Mapping for Clouds Built for Regulated Workloads," Proc. IEEE CLOUD, pp. 136-146, September 2021. DOI: 10.1109/CLOUD53861.2021.00027.

[6] SK Shieldus, "CSAP Reform: What Will Change from 2027?," SK Shieldus Security Insights, https://www.skshieldus.com/security-insights/trends/csap-2027-saas-csp-strategy, accessed September 14, 2026.

[7] S. Fenz, S. Plieschnegger, and H. Hobel, "Mapping Information Security Standard ISO 27002 to an Ontological Structure," Information & Computer Security, Vol. 24, No. 5, pp. 452-473, November 2016. DOI: 10.1108/ICS-07-2015-0030.

[8] K. P. Joshi, L. Elluri, and A. Nagar, "An Integrated Knowledge Graph to Automate Cloud Data Compliance," IEEE Access, Vol. 8, pp. 148541-148555, November 2020. DOI: 10.1109/ACCESS.2020.3008964.

[9] N. Reimers and I. Gurevych, "Sentence-BERT: Sentence Embeddings Using Siamese BERT-Networks," Proc. EMNLP-IJCNLP, pp. 3982-3992, November 2019. DOI: 10.18653/v1/D19-1410.

[10] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "BERT: Pre-Training of Deep Bidirectional Transformers for Language Understanding," Proc. NAACL-HLT, pp. 4171-4186, June 2019. DOI: 10.18653/v1/N19-1423.

[11] R. Angles and C. Gutierrez, "Survey of Graph Database Models," ACM Computing Surveys, Vol. 40, No. 1, pp. 1-39, February 2008. DOI: 10.1145/1322432.1322433.

[12] J. Guia, V. G. Soares, and J. Bernardino, "Graph Databases: Neo4j Analysis," Proc. ICEIS, Vol. 1, pp. 351-356, April 2017. DOI: 10.5220/0006356003510356.

[13] D. Fernandes and J. Bernardino, "Graph Databases Comparison: AllegroGraph, ArangoDB, InfiniteGraph, Neo4J, and OrientDB," Proc. DATA, Vol. 1, pp. 373-380, July 2018. DOI: 10.5220/0006910203730380.

[14] N. Francis et al., "Cypher: An Evolving Query Language for Property Graphs," Proc. ACM SIGMOD, pp. 1433-1445, June 2018. DOI: 10.1145/3183713.3190657.

[15] Neo4j, “Comparing relational to graph database,” Neo4j Documentation, https://neo4j.com/docs/getting-started/appendix/graphdb-concepts/graphdb-vs-rdbms/, accessed October 19, 2026.

[16] J. Chen, S. Xiao, P. Zhang, K. Luo, D. Lian, and Z. Liu, "M3-Embedding: Multi-Linguality, Multi-Functionality, Multi-Granularity Text Embeddings Through Self-Knowledge Distillation," Findings of ACL 2024, pp. 2318-2335, August 2024. DOI: 10.18653/v1/2024.findings-acl.137.

[17] V. Karpukhin et al., "Dense Passage Retrieval for Open-Domain Question Answering," Proc. EMNLP, pp. 6769-6781, November 2020. DOI: 10.18653/v1/2020.emnlp-main.550.

[18] S. Robertson and H. Zaragoza, "The Probabilistic Relevance Framework: BM25 and Beyond," Foundations and Trends in Information Retrieval, Vol. 3, No. 4, pp. 333-389, April 2009. DOI: 10.1561/1500000019.

[19] O. Khattab and M. Zaharia, "ColBERT: Efficient and Effective Passage Search via Contextualized Late Interaction over BERT," Proc. ACM SIGIR, pp. 39-48, July 2020. DOI: 10.1145/3397271.3401075.

[20] M. Montague and J. A. Aslam, "Relevance Score Normalization for Metasearch," Proc. ACM CIKM, pp. 427-433, November 2001. DOI: 10.1145/502585.502657.

[21] SW-SecurePolicy, "Security Knowledge Graph Neo4j," GitHub, https://github.com/SW-SecurePolicy/security-knowledge-graph-neo4j

Authors



Yun Gyu Eo is currently pursuing a B.S. degree in Digital Security at Cheongju University, Cheongju, Republic of Korea. His research interests include supply chain security and AI-based anomaly detection.



Sun Woo Shin received his B.S. degree in Information and Communication Engineering from Myongji University, Korea. He is currently pursuing the M.S. degree in Information Security at Korea University, Seoul, Republic of Korea. Since 2022, he has been the CEO of SetSecurity, and since 2025, the CEO of Cloud Air Inc. His research interests include cloud security, security policy automation, cyber ranges, AI factories, and zero trust.



Hyeon Jun Son is currently pursuing a B.S. degree in Digital Security at Cheongju University, Cheongju, Republic of Korea. His research interests include penetration testing.



Su Man Nam received his M.S. and Ph.D. degrees in Electrical and Computer Engineering from Sungkyunkwan University, Korea, in 2013 and 2017, respectively. In 2018, he joined the Department of Biomedical Informatics at Ajou University, Korea, as a researcher. He previously served as the head of the research institutes at DuDu Information Technologies, Inc. and Team Solution Co., Ltd. Since 2024, he has been a professor in the Department of Digital Security at Cheongju University, Korea. His research interests include Internet of Things (IoT) security, modeling and simulation, digital twins, and wireless sensor networks (WSNs).

www.kci.go.kr