

A Repeatedly Applicable Risk Prioritization Model for Increasingly Advanced AI Threats in the Financial Sector

Seungman Jin*, Deukjo Hong**

*Ph.D. course, Div. of Electronics and Information Eng. (Computer Eng.), Jeonbuk National Univ., Jeonju, Korea

**Professor, Dept. of Computer Science and Artificial Intelligence, Jeonbuk National Univ., Jeonju, Korea

[Abstract]

Financial institutions' rapid adoption of generative AI improves operational efficiency, but it also exposes them to autonomous AI threats that independently probe and attack external touchpoints, creating a problem in which threats evolve faster than security infrastructure and governance can be built. This study defines this speed gap as an independent research problem termed the Security Control Gap, and proposes a repeatedly recalculable risk-scoring model—based on likelihood, impact, detectability, and governance gap—that organizations can apply directly to security investment and phased response strategies. Applying this model to a Model Context Protocol (MCP)-based generative AI development environment, a Best-Worst Method (BWM) analysis identified unauthorized direct access to an external LLM (T1) as the top-priority threat; under an equal-weight baseline, T1 remained among the top two priorities together with T4 (Kendall's $\tau = 0.8$), indicating that the core conclusion is largely, though not fully, insensitive to the weighting scheme.

▶ **Key words:** Generative AI, Security Control Gap, Risk Management, Best-Worst Method (BWM)

[요약]

금융권의 급속한 AI 전환은 업무 효율성을 높이지만, 외부 접점을 통해 스스로 취약점을 탐색·공격하는 자율형 AI 위협에 노출시키며, 보안 인프라·거버넌스의 구축 속도보다 위협의 진화가 더 빠르다는 문제가 발생한다. 이에 본 연구는 이러한 진화 속도 차이를 Security Control Gap(탐지-통제 시차)라는 독립적인 연구문제로 정의하고, 발생가능성·영향도·탐지가능성·거버넌스 공백 네 요소로 위험 점수를 산정해 조직의 보안투자·단계별 대응전략에 반영 가능한 반복 재계산 모델을 제안한다. 이를 MCP 기반 생성형 AI 개발환경에 적용해 BWM(Best-Worst Method) 분석을 수행한 결과, 외부 LLM 무단 접속(T1)이 최우선 대응 위협으로 확인되었으며, 균등가중 기준에서도 T1은 T4와 함께 상위 순위를 유지하였으나(Kendall's $\tau=0.8$) T1·T4 순위가 뒤바뀌어, 핵심 결론에는 큰 영향이 없으나 가중치 방식에 완전히 불변하지는 않음을 확인하였다.

▶ **주제어:** 생성형 AI, Security Control Gap(탐지-통제 시차), 위험관리, BWM(Best-Worst Method)

• First Author: Seungman Jin, Corresponding Author: Deukjo Hong

*Seungman Jin (smjinking@naver.com), Div. of Electronics and Information Eng. (Computer Eng.), Jeonbuk National Univ.

**Deukjo Hong (deukjo.hong@jbnu.ac.kr), Dept. of Computer Science and Artificial Intelligence, Jeonbuk National Univ.

• Received: 2026. 07. 16, Revised: 2026. 08. 18, Accepted: 2026. 08. 20.

I. Introduction

AI 기술의 급격한 발전에 따라 Gartner는 생성형 AI 도입이 보안 조직의 최우선 위험관리 과제로 부상하고 있음을 지적한 바 있다[1]. 이러한 흐름 속에서 국내 금융당국 역시 기존 폐쇄망 중심 정책에서 벗어나 AI를 적극 활용할 수 있는 방향으로 정책 전환을 추진하고 있다. 금융위원회는 2024년 「금융분야 망분리 개선 로드맵」[2]과 2026년 「프런티어 AI 보안위협 금융분야 대응요령」[3]을, 금융보안원은 「생성형 AI 활용 가이드라인」[4]을, 금융감독원은 「생성형 AI 활용 지원방안 및 보완대책」[5]을 각각 발표·배포하여 금융회사의 AI 보안위협 대응을 제도적으로 뒷받침하고 있다. 이에 발맞춰 금융회사들은 생성형 AI를 업무에 직접 결합하는 개발환경을 구축하고 있으며, 특히 Anthropic 社가 제안한 MCP(Model Context Protocol)[6]을 이용한 개발환경의 구축은 이러한 흐름을 보여주는 대표적인 사례다.

문제는 이러한 개발환경이 필연적으로 외부 AI 모델·서비스와의 연결을 전제로 한다는 데 있다. 이 접점은 금융회사가 통제하는 보안 경계 바깥의 대상과 통신하는 지점이므로 그 자체로 새로운 공격 표면(Attack Surface)이 된다. 특히 최근에는 사람이 직접 취약점을 찾는 대신, 스스로 대상 시스템을 탐색하고 실제 공격까지 자율적으로 수행하는 자율형 공격 AI의 위협이 보고되고 있는데[7][8], 이러한 AI에게는 금융회사가 새로 연 외부 접점 하나하나가 자동으로 탐색 가능한 공격 대상이 된다. 금융회사가 업무 경쟁력을 위해 구축한 생성형 AI 접점이, 알려지지 않은 방식으로 그 접점 자체를 공격하는 또 다른 AI에게 노출되는 상황이 발생한다.

업무 경쟁력 확보를 위해 생성형 AI 활용이 필수가 된 이상 외부 연결을 차단하는 방식으로는 현실적인 대응이 어렵다. 특히 공격주체가 사람이 아닌 자율형 AI일 경우, 위협 탐색과 공격은 인간 보안 관리자가 전략을 수립하는 속도보다 훨씬 빠르게 진행된다. 더욱이 SSL Inspection, SWG, AI-DLP 등 새로운 보안 통제 인프라를 구축·운영하는 데에는 상당한 시간과 비용이 소요되므로, 결과적으로 통제 인프라가 완성되는 시점에는 이미 다음 세대의 위협이 그 경계를 넘어서는 악순환이 반복되는 상황이다.

본 연구에서는 이러한 구조적 문제를 탐지 가능 시점과 완전한 통제 가능 시점 사이에 존재하는 탐지-통제 시차(Security Control Gap)로 정의한다. 즉 위협을 인지한 이후에도 이를 충분히 통제할 수 있는 보안 체계가 완성되기까지 불가피하게 발생하는 시간적·관리적 공백을 의미하

며 Fig. 1과 같이, 시간이 흐를수록 AI 위협의 진화 수준과 보안 인프라 성숙 수준 간의 격차는 점차 확대되는 양상을 보인다. 이 시기에는 모든 위협에 동일한 수준의 보안 자원을 투입하기 어려우므로, 제한된 자원을 가장 위험도가 높은 위협에 먼저 배분할 수 있는 체계적인 위험 우선순위 결정 방법을 요구하게 된다.

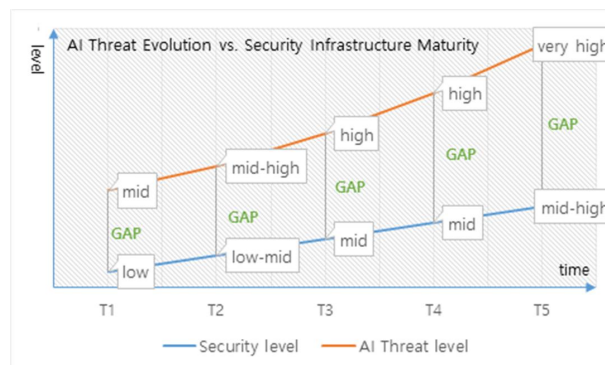


Fig. 1. Conceptual Diagram of Security Control Gap and Iterative Risk Assessment

본 연구가 다루는 연구문제는 다음과 같다. 빠르게 진화하는 자율형 공격 AI 등 신종 위협에 대해, 완전한 보안 통제 인프라가 갖추어지기를 기다리지 않고 알려진 취약점부터 최대한 신속하게 대응하기 위한 위험관리 방법이 필요하다는 것이다. 이를 위해 본 연구는 발생가능성(Likelihood), 영향도(Impact), 탐지가능성(Detectability), 거버넌스 공백(Governance Gap)의 네가지 요인을 기반으로 반복 적용 가능한 위험 우선순위 모델을 제안한다. 탐지가능성과 거버넌스 공백은 인프라 및 규제 수준에 따라 갱신되는 가변 요인으로 설계하여, 위협의 종류나 인프라 수준이 달라지더라도 동일한 절차로 다시 적용할 수 있도록 하였다. 각 요인의 상대적 가중치는 금융보안 전문가를 대상으로 한 BWM(Best-Worst Method) 조사를 통해 초기값으로 확보하며, 이를 바탕으로 완전한 보안 통제 인프라로 전환하는 과정에서 적용 가능한 단계적 대응 전략을 제시한다.

본 연구의 범위는 국내 금융권의 생성형 AI 개발환경이며, MCP는 이러한 환경을 보여주는 하나의 사례로 다룬다. 본 연구의 기여는 다음과 같다. 첫째, 생성형 AI 환경에서 위협 진화 속도와 보안 통제 성숙 속도 사이에 존재하는 탐지-통제 시차(Security Control Gap)를 독립적인 연구문제로 정의하였다. 둘째, 이 시차 환경에서 반복 적용 가능한 위험 우선순위 산정 모델을 제안하였다. 셋째, 금융보안 전문가 15인을 대상으로 한 BWM 기반 조사를 통해 초기 요인가중치와 위협별 요인점수를 확보하고, 이를 근거로 단계적 대응전략을 제시하였다.

현재까지 국내 금융권을 대상으로, 탐지-통제 시차라는 조건 자체를 연구 문제로 정식화하고 그 시차 동안 반복 적용 가능한 위험 우선순위 모델을 제시한 연구는 확인되지 않는다. 본 연구는 기존 연구의 한계를 극복하고자 한다.

II. Related Work

2.1 Shadow AI and the Rise of Autonomous Offensive AI

Shadow IT는 조직의 공식 승인 없이 임직원이 외부 IT 자원을 활용하는 현상이다[9]. 본 연구에서 Shadow AI란 정보보호 부서의 공식 승인 없이 임직원이 개인적으로 도입·연동하는 생성형 AI 도구 및 그 연동 인프라를 의미한다. 한편 OWASP의 Agentic AI 위협 문서[7]와 MITRE ATLAS[8]는 최근 자율 에이전트가 스스로 취약점을 탐색하고 공격 행위까지 수행할 수 있는 사례를 문서화하고 있다. 이는 기존 Shadow IT 논의가 전제하던 '수동적으로 오·남용되는 도구'라는 위협 모델을 넘어서는 것으로, 위협 자체가 방어 체계 구축 속도보다 빠르게 고도화될 수 있음을 시사한다.

2.2 MCP-Based Generative AI Development Environment (Case)

이러한 Shadow AI가 금융권에서 구체화되는 대표적 경로가 MCP 기반 AI 활용이다. 보안 부서의 통제 없이 개발자가 개인 노트북이나 로컬 환경에 MCP Server를 구축하고 외부 LLM API를 연동하는 행위 자체가, 공식 개발 표준인 MCP를 새로운 형태의 Shadow AI 연동 인프라로 전환시킨다. MCP[6]는 LLM과 데이터 소스, 개발도구 간 양방향 통신을 위한 개방형 프로토콜로, Client(IDE)-Server(로컬 자원)-Host(LLM)의 3자 토폴로지를 형성하며 외부 LLM과 내부 자원 간 자율적 연동을 허용한다. 본 연구는 MCP를 유일한 대상이 아니라, '외부 생성형 AI와의 접점이 내부 자원과 직접 연동되는 개발환경'이라는 더 넓은 범주를 대표하는 사례로 다룬다. 향후 유사한 접점을 형성하는 다른 프로토콜·도구가 등장하더라도 3장의 우선순위 모델은 동일하게 적용될 수 있다.

2.3 Limitations of Existing Research

OWASP Top 10 for LLM[10], MITRE ATLAS[8], NIST AI RMF[11]는 각각 위협 유형, 공격 전술, 조직 거버넌스 원칙을 제시하지만, 어떤 위협을 먼저 대응해야 하

는지 정하는 정량적 우선순위 산정 절차는 제공하지 않는다. Shadow IT 관련 선행연구[9] 역시 현상을 설명하는데 집중할 뿐, 자원이 제한된 상황에서 대응 순서를 어떻게 정할지는 논의하지 않는다. 무엇보다 이들 연구는 대체로 특정 시점의 위협 목록을 전제로 설계되어, 위협과 인프라 수준이 함께 변화하는 과도기적 상황에서 반복 재적용 가능한 절차까지는 반영하지 못한다. 이에 본 연구는 이러한 한계를 극복하고, 동적 환경 변화에 유연하게 대응할 수 있는 방법론적 대안을 제시하고자 한다.

III. Risk Prioritization Model

3.1 Derivation of Candidate Threats

본 장에서 제안하는 모델에 입력할 후보 위협을 도출하기 위해, MCP 기술 명세[6]를 분석하고 OWASP, MITRE 표준[10][7][8]을 매핑하였으며, 국내 금융 규제 교차 분석의 절차를 거쳐 5개 후보 위협을 정리하였다. 이 목록은 완결된 분류체계가 아니라 모델의 타당성을 검증하기 위한 입력 데이터라는 점에 유의할 필요가 있다. 향후, 새로운 위협이 관측되면 동일한 절차로 후보를 갱신하고, 모델에 다시 대입하면 된다.

Table 1. Candidate Threat List (Input for Model Validation)

Threat	Name	Definition
T1	Unauthorized Direct Access to External LLM	Directly entering internal information into an external generative AI web service
T2	Unapproved MCP Client Execution	Connecting to an external agent via a portable IDE/plugin
T3	Data Exfiltration via Local MCP Server	Transmitting assets through an encrypted tunnel via Tool Calls on a custom MCP Server
T4	Excessive Privilege Exercise by Autonomous Agent	Agent executing internal commands or modifying files with excessive privileges
T5'	Unverified Plugin Supply Chain Intrusion	Unauthorized installation /execution of unverified open-source plugins

3.2 Design Principles and Risk Scoring Formula

본 모델은 위협을 다시 분류하는 것이 아니라, 이미 식별된(또는 향후 새로 식별될) 후보 위협에 대해 '무엇을 먼저 대응할 것인가'라는 질문에 답하기 위해 설계되었다. 기존 위험평가 연구는 일반적으로 발생가능성(Likelihood)과 영향도(Impact)를 중심으로 위협을 평가하였다. 그러나 생성

형 AI 환경에서는 동일한 위협이라도 조직의 탐지 능력과 보안 인프라 수준에 따라 실제 위험도가 크게 달라질 수 있다. 또한 금융회사는 규제 환경 변화에 따라 동일한 기술이라도 통제 가능성이 지속적으로 변화하므로, 기존 위험평가 요소만으로는 실질적인 대응 우선순위를 산정하기 어렵다. 이에 본 연구에서는 기존 위험평가 요소에 탐지가능성(Detectability)과 거버넌스 공백(Governance Gap)을 추가하여 네 가지 평가요소로 위험 점수를 산정한다.

$$Risk_i = w1 \cdot Li + w2 \cdot Ii + w3 \cdot (1 - Di) + w4 \cdot Gi \quad (1)$$

여기서 각 요인은 다음과 같이 정의된다.

- L (Likelihood, 발생가능성): 해당 위협 행위가 실제 업무 환경에서 관측될 빈도. 전문가 정성 평가 및 관측 사례 빈도에 기반한다.
- I (Impact, 영향도): 위협이 실현되었을 때 예상되는 피해 규모(자산 유출 범위, 규제 위반 수준 등).
- D (Detectability, 탐지가능성): 현재 보안 인프라 수준에서 해당 위협을 식별할 수 있는 정도. 인프라가 고도화될수록 값이 커지는 가변 요인이다.
- G (Governance Gap, 거버넌스 공백): 관련 규제·내부통제 기준이 해당 위협의 적용 범위를 얼마나 불명확하게 남겨두는지의 정도. 규제가 정비될수록 값이 작아지는 가변 요인이다.

D와 G를 가변 요인으로 설계한 것은 본 모델의 핵심 설계 의도를 반영한다. 인프라가 SSL Inspection 등으로 고도화되면 D값이 상승하여 해당 위협의 위험 점수는 자연히 낮아지고, 반대로 새로운 위협이 등장하면 그 위협은 초기에는 D값이 낮아 높은 위험 점수를 받게 된다. 본 모델은 특정 시점의 위협 순위표가 아니라, 위협과 인프라 수준이 함께 변화하는 상황에서 반복적으로 재계산 가능한 절차이다.

네 요인을 단순 가중합으로 결합한 것은 다기준 의사결정에서 널리 쓰이는 단순가산가중법(Simple Additive Weighting, SAW)의 구조를 따른 것으로, 계산이 투명하고 요인별 기여도를 직관적으로 해석할 수 있다는 실무적 장점이 있다[12]. 다만 SAW 계열의 가중합은 본질적으로 보상적(compensatory) 결합 방식이어서, 한 요인의 낮은 값을 다른 요인의 높은 값이 상쇄할 수 있다는 한계를 갖는다. 예를 들어 영향도(I)가 극단적으로 높은 위협이라도 탐지가능성(D)이 충분히 높으면 종합 Risk 점수가 낮게 산정될 수 있다. 금융보안 맥락에서는 특정 요인이 임계 수준을 넘는 위협(예: 대규모 정보유출 가능성이 있는 위협)

에 대해 다른 요인 값과 무관하게 최소 대응 우선순위를 보장하는 비보상적(non-compensatory) 규칙, 예컨대 특정 요인이 'Very High'인 경우 최종 순위를 일정 수준 이하로 낮추지 않는 게이트(gate) 조건을 병행하는 방안이 안전할 수 있다. 본 연구는 이러한 비보상적 결합 방식(예: outranking 기법)을 향후 연구 과제로 남기고, 현재 모델에서는 위 한계를 명시적으로 인지한 상태에서 SAW 구조를 채택한다.

3.3 Weight Determination Method

본 절에서 산출하는 $w1-w4$ 는 관련 전문가 패널에서 L·I·D·G 네 요인 자체를 직접 비교하여 얻은 값이다. 조사는 두 부분으로 구성된다. 첫째, BWM 절차[13]에 따라 각 전문가는 네 요인 중 가장 중요한 요인(Best)과 가장 덜 중요한 요인(Worst)을 지정한 뒤, Best 요인이 나머지 각 요인보다 얼마나 중요한지(Best-to-Others, BO)와 나머지 각 요인이 Worst 요인보다 얼마나 중요한지(Others-to-Worst, OW)를 1~9 척도로 응답하였다. 둘째, 각 전문가는 5개 후보 위협(T1-T5') 각각에 대해 L·I·D·G 네 요인의 수준을 5점 리커트 척도(1=매우 낮음 ~ 5=매우 높음)로 직접 평가하였다. 이 두 응답을 결합함으로써, 위협별 Risk 점수는 '측정된 요인 점수 × 측정된 요인 가중치'의 곱으로 산출한다. 개인별 요인가중치는 다음 선형계획법(min-max 모델)로 산출한다[13]:

$$\begin{aligned} \min \xi \quad s.t. \quad & |w_B - a_{Bj} \cdot w_j| \leq \xi, \\ & |w_j - a_{jW} \cdot w_W| \leq \xi (j = L, I, D, G), \\ & \sum w_j = 1, \quad w_j \geq 0 \end{aligned} \quad (2)$$

여기서 ξ^* 는 해당 응답자의 비교값 불일치 정도를 나타내며, 일관성비율은 $CR^* = \xi^* / CI(a_BW)$ 로 계산한다. $CI(a_BW)$ 는 Best-Worst 직접비교값 a_BW (=BO 벡터 중 Worst 요인에 해당하는 값)에 대응하는 일관성지수로, [13]이 제시한 표($a_BW=1\sim9$ 에 대해 $CI=0.00\sim5.23$)를 사용한다. 본 연구는 $CR^* > 0.1$ 인 응답을 통상적인 임계값 [13][14]에 따라 유효 응답에서 제외하는 것을 분석 기준으로 사전에 채택하였으며, 이 기준은 특정 결과를 유도하기 위해 사후에 조정된 것이 아니라 BWM 문헌에서 통용되는 고정 임계값이다. 그룹 가중치는 개인별 가중치의 기하평균으로 집계한 뒤 합이 1이 되도록 재정규화한다. 4장에서 이 절차의 실제 산출 결과를 제시한다.

3.4 Iterative Recalculation Structure and Empirical Re-validation Procedure

본 모델의 핵심은 개별 위협의 순위를 한 번 산정하고 끝내는 것이 아니라, 인프라·규제 여건이 바뀔 때마다 (1) 식을 다시 계산하여 우선순위를 갱신하는 순환 구조에 있다. Fig. 2는 이 순환 구조를 나타낸 것이다. 여기서 추가된 '실증적 재검증(Empirical Re-Validation)' 단계가 반복하여 재계산할 때 신뢰성을 좌우한다. 다만 이 절에서 기술하는 레드팀 PoC 및 운영 로그·실사고 모니터링 기반의 '실증적 재검증' 단계는 본 연구에서 실제로 수행된 분석이 아니라, 향후 이 모델을 조직에 적용할 때 따라야 할 개념적 설계(conceptual design)로 제시하는 것이다.

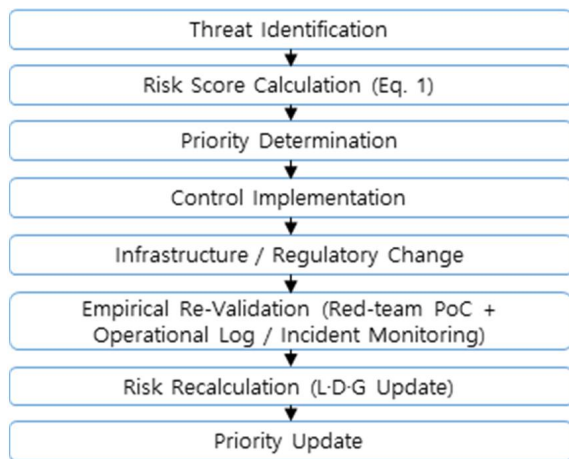


Fig. 2. Risk Priority Recalculation Cycle

이 단계는 두 가지 절차를 결합한다. 첫째는 레드팀 PoC로, 인프라 전환이나 신규 위협 후보 등장 시 통제된 테스트베드에서 해당 위협을 실제로 재현하여 구현 난이도와 탐지 여부를 직접 확인함으로써 L·D 값을 실측 근거로 갱신한다. 둘째는 운영 로그·실사고 모니터링으로, 실제 SIEM 이상탐지 빈도와 업계에 공개되는 실사고 사례를 정기적으로 수집하여 L·I 값을 보정하고 신규 위협 후보 유무를 점검한다. 이 두 절차를 거치지 않은 재계산은 값의 근거가 다시 전문가의 주관적 판단에 머무르게 되므로, 본 모델에서는 실증적 재검증을 재계산 주기마다 거쳐야 하는 필수 절차로 규정한다. 예를 들어 T3의 D값을 레드팀 PoC를 통해 측정하는 절차는 우선 격리된 테스트베드에 실제 MCP Client-Server-Host 구성을 재현하고, 로컬 MCP Server가 사내 소스코드, DB 조회결과를 JSON-RPC 응답에 담아 외부로 전송하도록 구성한다. 이 트래픽이 레거시 방화벽 세션 로그에 남기는 목적지IP, 포트, 전송량, 세션 지속시간을 기존 탐지 규칙과 대조하여,

규칙이 해당 트래픽을 실제로 탐지, 차단하는지를 성공, 실패로 기록한다. 동일 시나리오를 SSL-Inspection 적용 환경에서 반복하면 페이로드 수준 탐지 여부까지 확인할 수 있으며, 두 환경의 탐지 성공률 차이를 D값 갱신의 근거로 사용한다. Table 2는 이 순환이 실제로 순위를 어떻게 바꿀 수 있는지를 예시 수치로 보여준 것이다 - 아래 수치는 실측값이 아닌 illustrative 예시이며, 4장의 실제 BWM 조사 결과와는 무관하다.

Table 2. Example of Recalculation upon Infrastructure Transition (Illustrative weights $w_1=w_2=w_3=w_4=0.25$; illustrative values, not measured data)

Threat	Environment	L	I	D	G	Risk
T3	Legacy	0.5	0.9	0.2	0.6	0.70
T3	SSL Inspection Adopted	0.5	0.9	0.7	0.6	0.575
T3	New Attack Technique Emerges	0.5	0.9	0.3	0.6	0.675
T1	Legacy	0.8	0.7	0.4	0.5	0.65
T1	SSL Inspection Adopted	0.8	0.7	0.6	0.5	0.60

레거시 환경에서는 T3(0.70)의 위험 점수가 T1(0.65)보다 높아 T3가 최우선 순위를 차지한다. SSL Inspection 도입으로 T3의 탐지가능성(D)이 0.2에서 0.7로 상승하면 위험 점수는 0.575로 낮아지는 반면, T1은 D가 0.4에서 0.6으로 상대적으로 적게 상승하여 0.60을 유지함으로써 T1과 T3의 순위가 역전된다. 그러나 Table 2의 세 번째 행이 보여주듯, 기존 탐지 규칙을 우회하는 신규 공격기법이 등장하면 SSL Inspection을 도입한 상태에서도 T3의 D값은 다시 0.3으로 떨어지고 위험 점수는 0.675로 재상승한다. 결과적으로 인프라 고도화가 탐지-통제 시차를 영구히 없애는 것이 아니라, 새로운 위협이 등장할 때마다 그 시차가 다른 형태로 재발생한다는 것을 보여준다. 이 예시는 실제 조사 수치가 아니라 (1)식이 인프라·위협 변화에 따라 순위를 어떻게 재조정하는지를 보이기 위한 것이며, 실제 값은 아래 3.5절의 트리거가 발생할 때마다 위 실증적 재검증 절차를 거쳐 다시 산정해야 한다.

3.5 Recalculation Triggers

본 연구에서 제안하는 위험 우선순위 모델은 단일 시점의 평가를 목적으로 하지 않는다. 다음과 같은 변화가 발생할 경우 3.4절의 절차에 따라 위험 우선순위를 반복적으로 재산정하도록 설계하였다.

- 신규 생성형 AI 서비스 도입: 새로운 외부 LLM·에이전트 서비스가 조직 내 도입되는 경우
- MCP 구조 변경: MCP 프로토콜 명세 개정이나 유사 프로토콜로의 전환이 발생하는 경우
- 보안 인프라 고도화: SSL Inspection·SWG·AI-DLP 등 통제 인프라가 신규 도입·확장되는 경우
- 금융 규제 변경: 전자금융감독규정 등 관련 규제가 개정되어 거버넌스 공백(G)이 변화하는 경우
- 신규 공격사례 발생: 업계에 신규 공격기법이나 침해사고가 공개되어 기존 D-L 값의 근거가 무효화되는 경우
- 조직 보안정책 변경: 내부 승인 절차, 화이트리스트 정책 등 조직 자체 통제가 변경되는 경우

따라서 본 연구에서 제안하는 모델의 핵심은 특정 위협 목록 자체가 아니라, 새로운 생성형 AI 위협이 등장하더라도 동일한 절차를 반복 적용하여 대응 우선순위를 산정할 수 있다는 점에 있다.

IV. BWM-Based Initial Prioritization

본 장은 3장에서 설계한 모델에 대입할 초기 요인가중치와 위협별 요인점수를 확보하는 절차이며, 조사 자체는 검증 도구가 아니라 모델의 초기 입력값을 확보하는 절차로 자리매김한다. 조사는 시간차를 두고 두 단계로 진행되었다. 1차 조사는 델파이 기법[15]을 적용하여 후보 위협 목록을 확정하고 내용타당도를 검토하는 데 사용되었으며, 이는 4.1절에서 설명하는 바와 같이 초기값 설정에만 사용되고 매 재계산 시점마다 모델을 재검증하는 데 사용되지는 않는다. 이후 인프라·규제 변화에 따른 반복 재계산에는 매번 전문가 패널을 다시 소집하는 대신 3.4절의 실증적 재검증 절차(개념적 설계)를 사용하는 것을 목표로 한다.

4.1 Panel Composition and Survey Procedure

본 연구의 조사는 시간차를 두고 두 단계로 진행되었다. 1차 델파이 조사(후보 위협의 내용타당도 검토, CVR 산출)는 금융보안 실무자 9인, 학계 4인, 규제기관 담당자 2인 등 총 15인(평균 경력 12.4년)의 패널로 수행되었다. 이후 상당한 시간이 경과하면서 1차 패널 중 상당수가 교체되었고, 3.3절의 BWM-리커트 조사(2차 조사)는 동일한 소속 구성 비율(실무자 9인, 학계 4인, 규제기관 2인)을 유지하되 새로 구성된 15인 패널을 대상으로 실시하였다. 2차 패널의 소속은 은행권 실무자 9인, 학계 4인, 규제기관 담당자 2인이며, 경력은 평균 13.7년(범위 4~26년)으로 1차

패널과 다소 차이가 있다(그룹별 평균: 실무자 11.1년, 학계 16.3년, 규제기관 20.5년). 즉 본 연구의 1차 CVR 결과와 2차 BWM-리커트 결과는 동일 인물의 시계열 응답이 아니라, 동일한 소속 구성 프로필을 가진 별도 패널의 응답이라는 점을 명시한다.

전문가 선정 기준은 정보보호 관련 실무·연구 경력 최소 3년 이상인 자로 한정하였으며, 이 중 (i) 금융회사 정보보호 실무경험을 보유한 자를 15인 중 9인(다수)으로, (ii) 방법론 연구 및 정보보호 지식을 갖춘 정보보호 관련 학과 소속 연구자를 4인으로, (iii) 컴플라이언스 및 규제 분야 권위자를 2인으로 선정하였다. 모집은 목적표집(purposive sampling)과 쿼터표집(quota sampling)을 병행하였다: 저자가 참여하고 있는 국내 금융정보보호 관련 협의체 및 연구모임 등 정보보호 실무자 커뮤니티 네트워크를 통해 위 선정 기준에 부합하는 전문가를 파악한 뒤 개별적으로 참여를 요청(request)하고 승낙(consent)을 받았으며, 소속 그룹별 목표 인원(실무자 9인, 학계 4인, 규제기관 2인)을 사전에 설정하여 각 그룹에서 목표 인원 에 먼저 도달한 응답을 기준으로 마감하였다. 목표 인원을 초과하여 접수된 일부 응답은 도달 순서 기준으로 최종 분석에서 제외하였다. 이러한 모집 방식은 무작위 표집이 아니라는 점에서 특정 성향의 전문가가 과대표집되었을 가능성을 배제할 수 없다는 한계가 있으며, 이 한계는 결론에서 다시 논의한다.

2차 패널의 상당수는 1차 델파이 조사 당시 저자가 본 연구 주제(생성형 AI 환경의 위험 우선순위 모델링)를 이미 소개하고 의견을 구한 바 있는 동일 커뮤니티 소속 전문가로 구성되었다. 이 커뮤니티는 정기 오프라인 모임이 연 1~2회로 제한적인 대신 평소 온라인 메신저를 통한 소통이 활발하며, 연구 배경과 핵심 개념(L·I·D·G, Security Control Gap 등)에 대한 사전 이해도가 높아 별도의 상세한 사전 설명 없이도 신속한 응답이 가능하였다. 이에 따라 2차 조사(BWM-리커트)는 온라인 메신저를 통해 동일 일자에 배포·수집이 완료되었다.

1차 델파이 조사에서 산출한 CVR[16]의 경우, 전문가 15인 규모에서 [16]가 제시한 최소 임계값은 0.49이며, T1-T4는 CVR 0.60-1.00으로 이 임계값을 상회하여 채택되었으나, 최초 제시한 공급망 관련 위협은 CVR 0.47로 임계값에 미달하여 기각되었고 '검증되지 않은 오픈소스 플러그인의 무단 유입(T5)'으로 재정의한 후 2차 조사의 평가 대상 위협 목록에 포함하였다. 2차 조사에서는 3.3절에서 설명한 BWM 설문(요인 간 Best-Worst 비교, 1-9 척도)과 위협별 L·I·D·G 리커트 평가(1-5 척도)를 동일 응답

지에서 함께 수집하였다. 재정의된 T5' 항목에 대해서는 별도의 정량적 CVR 재평가를 수행하지 않았다.

다만 T5'는 2차 조사에서 15인 전문가 전원이 다른 4개 위협과 동일한 조건으로 L·I·D·G 리커트 평가를 수행하였다는 점에서, 항목 표현에 대한 암묵적 검토를 거쳤다고 볼 수 있다. 다만 이는 정식 내용타당도 검증 절차를 대체하지 못하므로, 본 연구는 이를 한계로 명시하고 (Conclusion 한계 목록에 추가), T5' 재정의 항목에 대한 별도 CVR 재평가를 후속 연구 과제로 남긴다.

4.2 BWM Weight Results

15인의 응답에 대해 3.3절의 선형계획법을 개별 적용하여 산출한 개인별 가중치와 CR*는 다음과 같다. 여기서 CR*는 개별 응답자 단위로 계산한 값이며(기하평균 집계 행렬에 대한 CR이 아님), 3인(CR* > 0.1)이 임계값을 초과하였다.

Table 3. Individual BWM Weights and Consistency Ratios (n=15) ★ CR* > 0.1 (exceeds conventional threshold [13])

Best/Worst	w _L	w _I	w _D	w _G	CR*
I/G	0.207	0.524	0.207	0.061	0.026
I/L	0.057	0.559	0.240	0.144	0.043
I/G	0.196	0.518	0.196	0.089	0.031
I/G	0.147	0.629	0.147	0.078	0.397 ★
L/G	0.466	0.172	0.259	0.103	0.032
L/G	0.500	0.214	0.214	0.071	0.062
D/G	0.119	0.153	0.651	0.077	0.420 ★
L/I	0.572	0.067	0.226	0.136	0.029
I/L	0.067	0.572	0.136	0.226	0.029
I/G	0.214	0.500	0.214	0.071	0.062
I/G	0.159	0.329	0.451	0.061	0.146 ★
D/G	0.202	0.202	0.543	0.053	0.012
I/G	0.150	0.350	0.450	0.050	0.044
D/G	0.232	0.139	0.578	0.051	0.022
I/D	0.243	0.601	0.053	0.104	0.024

CR* > 0.1인 3인(응답자 4, 7, 11)은 사전에 정한 임계값 기준에 따라 유효 응답에서 제외하였으며, 나머지 12인의 응답을 기하평균으로 집계하여 최종 그룹가중치를 산출하였다(w_L=0.252, w_I=0.365, w_D=0.280, w_G=0.104). 이 제외가 응답 편향을 초래했는지 확인하기 위해, 15인 전체 가중치와 12인 가중치를 비교한 결과 (Table 4) 요인 간 상대적 순서(w_I > w_D > w_L > w_G)는 동일하게 유지되었으며, 이를 바탕으로 산출한 위협 순위(4.4절) 역시 15인·12인 기준 모두에서 동일하였다. 따라서 3인의 제외가 결과의 방향을 바꾸는 방식으로 작용하지 않았다고 판단한다.

Table 4. Group Weight Comparison – Full Sample (n=15) vs. CR*-Filtered Sample (n=12)

Weight	Full Sample(15)	CR* Filtered(12)
w _L	0.232	0.252
w _I	0.366	0.365
w _D	0.303	0.280
w _G	0.100	0.104

4.3 Threat-Level Factor Scores (Measured, not Interpreted)

아래는 12인 응답 기준, 위협별 L·I·D·G 리커트 평균(1-5 척도)이다. 이 값은 위협 간 직접비교 결과를 해석·분해한 것이 아니라, 4.1절 조사에서 직접 측정된 값이다.

Table 5. Measured Mean Likert Scores per Threat (n=12)

Threat	L	I	D	G
T1	4.333	3.833	3.000	2.333
T2	3.000	2.833	3.167	3.083
T3	2.667	3.667	3.167	3.000
T4	2.667	4.000	2.500	3.917
T5'	3.333	4.000	3.000	3.000

4.4 Resulting Risk Prioritization

4.2절의 그룹가중치와 4.3절의 측정된 요인점수를 (1)식에 대입하여 산출한 Risk 점수는 다음과 같다(L·I·D·G는 5점 척도를 0-1로 정규화하여 사용)

Table 6. BWM-Based Risk Score and Priority (n=12)

Threat	Risk Score	Priority (Rank)
T1	0.659	1
T5'	0.634	3
T4	0.648	2
T3	0.567	4
T2	0.525	5

외부 LLM 무단 직접 접속(T1)이 최우선 대응 위협으로 확인되었다. 이는 T1의 발생가능성(L=4.33)이 다섯 후보 위협 중 가장 높고, 요인가중치 중 가장 큰 비중을 차지하는 영향도(w_I=0.365)에서도 상대적으로 높은 점수(I=3.83)를 받았기 때문이다.

4.5 Sensitivity Analysis

균등가중 기준선과 BWM 실측 가중치를 각각 적용하여 비교한 결과, BWM 기준으로는 T1(1위), T4(2위), T5'(3위), T3(4위), T2(5위)였으며 균등가중 기준으로는 T4(1위), T1(2위), T5'(3위), T3(4위), T2(5위)로 T1과 T4의 순위만 뒤바뀌었으며, Kendall의 순위상관계수는 $\tau=0.80$ 으로 나타나 대체로 높은 수준의 순위 일치를 보였다. 다만 완전한 일치($\tau=1.0$)는 아니므로, T1과 T4 두 위협 모두를

단기 대응 우선순위에 포함하는 방향으로 5.2절 대응전략을 조정할 필요가 있다. 또한, 위협 5개(n=5)의 소표본 비교라는 점에서 이 결과는 참고적 수준으로 해석해야 하며, 향후 후보 위협 수가 확대될 경우 재검증이 필요하다.

Table 7. Sensitivity Analysis – Equal-Weight Baseline vs. BWM-Derived Weights (n=12, Kendall's $\tau = 0.80$)

Threat	E-W score	E-W Rank	BWM score	BWM rank
T1	0.625	2	0.659	1
T5'	0.617	3	0.634	3
T4	0.654	1	0.648	2
T3	0.558	4	0.567	4
T2	0.537	5	0.525	5

V. Organizational Application

5.1 Reapplication of Priorities upon Infrastructure Transition

3.4절 Table 2의 예시처럼, 인프라가 SSL Inspection 등으로 고도화되면 D값 상승 폭이 큰 위협의 순위는 낮아지고 상승 폭이 작은 위협의 순위가 부상한다. Table 8은 현재(레거시) 우선순위와 SSL Inspection 도입 이후 예상되는 우선순위를 나란히 비교한 것이다. 이 표는 Table 2와 마찬가지로 실측 데이터가 아닌 illustrative 예시이며, 4장에서 제시한 실제 BWM 조사 결과(현재 순위: T1-T4-T5'-T3-T2)와는 독립적인 개념적 시나리오임을 밝힌다. 즉 이 표는 인프라 전환이 위협 순위를 어떻게 재조정할 수 있는지의 절차적 논리를 보이기 위한 것이지, 4장 결과에 대한 실제 전환 시뮬레이션이 아니다.

Table 8. Priority Comparison Before and After Infrastructure Transition (Illustrative Projection – not measured; independent of Section 4 results)

Threat	Current (Legacy) Rank	Expected Rank After SSL Inspection	Change
T3	1	2	▼ Falls due to sharp rise in D
T1	2	1	▲ Rises relatively as its D increase is smaller
T2	3	3	No change (expected)
T4	4	4	No change (expected)
T5'	5	5 (may rise if G is left unaddressed)	Depends on governance remediation

Table 8은 본 절의 대응 전략이 현재 시점의 결과를 고정된 답으로 제시하는 것이 아니라, 인프라 전환 단계마다 Table 2, Table 5, Table 6의 절차를 다시 밟아야 함을 보여준다. 즉 아래 단기·중기·장기 전략은 4.4절의 실측 결과를 기준으로 한 1회차 적용이며, SSL Inspection이 도입되는 시점에는 재계산된 순위를 기준으로 재수립해야 한다. 이러한 인프라 전환 전후의 순위 변화는, 향후 실제 재계산 데이터가 축적되면 Kendall의 순위상관계수[17]를 활용하여 순위 변동의 통계적 유의성을 검증하는 방식으로 확장할 수 있다.

5.2 Short, Mid, and Long-Term Response Strategy

현재 시점의 우선순위(T1-T4-T5'-T3-T2, 4.4절)를 기준으로 다음과 같은 단계적 전략을 제시한다. 단기(~6개월)에는 최우선 위협인 T1(외부 LLM 무단 직접 접속)과 2순위인 T4(자율 에이전트의 과도한 권한 행사)에 대응 자원을 집중한다. 외부 생성형 AI 웹서비스 접속에 대한 DLP·프록시 기반 통제와, 자율 에이전트의 권한 행사 범위를 제한하는 최소 권한 원칙을 우선 수립한다. 중기(~1년)에는 T5'(미검증 플러그인 공급망 침투)에 대응하는 승인되지 않은 오픈소스 플러그인 설치를 제한하는 화이트리스트 정책 적용과 병행하여, 전자금융감독규정 제15조에 따른 망분리 요건 중 연구·개발 목적에 대해 인정되는 대체 정보보호통제 적용 요건을 검토하여, 본 모델의 산정 결과 자체를 그 요건이 요구하는 자체 위험성평가 자료로 활용하고 MCP 개발환경에 적용 가능한 통제 방안을 수립한다. 장기(~2년)에는 T3(로컬 MCP 서버 경유 유출)와 T2(미승인 MCP 클라이언트 실행)에 대한 SSL Inspection 등 인프라 고도화를 완료하고, 감사 로그 기반 책임추적성 체계를 정비한다.

5.3 Internal Evaluation and Incentive Mechanisms

본 모델의 산출물은 외부 규제기관을 향한 제언보다, 조직 내부의 평가·의사결정 체계에 직접 반영할 때 더 큰 실효성을 갖는다.

- 내부 감사 가점 체계: 우선순위가 높은 위협(예: T1)에 대한 통제 조치를 우선 완료한 부서·팀에 내부 정보보호 감사 시 가점을 부여하여, 조직 전체의 대응 유인을 우선순위와 정렬시킨다.
- 경영진 보고 KPI화: 3.4절의 반복 재계산으로 갱신되는 Risk 점수 추이를 정기적인 경영진 보고 지표로 사용하여, 보안 투자·예산 배정의 근거 자료로 삼는다.
- 규제 대응 근거 자료화: 전자금융감독규정 제15조의

연구·개발 목적 망분리 예외가 요구하는 자체 위험성 평가 문서를 본 모델의 산정 결과와 실증적 재검증 이력으로 구성하여, 감독 대응 시 제시할 수 있는 상시 근거를 마련한다.

VI. Conclusion

본 연구의 핵심 기여는 '보안 인프라와 위협이 공존하는 탐지-통제 시차(Gap) 속에서, 한정된 자원으로 무엇을 가장 먼저 대응해야 하는가?'라는 실무적인 질문에 답을 제시한 것이다. 본 연구가 제시한 기여는 다음과 같다. 첫째, 탐지-통제 시차(Security Control Gap)의 정식화로, 위협이 탐지 가능해지는 시점과 완전히 통제 가능해지는 시점 사이의 구조적 간극을 금융권 생성형 AI 도입의 독립적인 연구문제로 정의하였다. 둘째, 반복 재계산 가능한 우선순위 절차로, 발생가능성·영향도·탐지가능성·거버넌스 공백 네 요인의 가중합으로 위협별 위험 점수를 산정하는 절차를 제안하였다. 이 절차의 반복 재계산 단계(레드팀 PoC, 운영로그 모니터링)는 본 연구에서 실제로 수행한 실증이 아니라 향후 적용을 위한 개념적 설계임을 분명히 한다. 셋째, BWM 기반 초기 우선순위 확보로, 금융보안 전문가 15인 중 일관성 기준을 충족한 12인의 BWM·리커트 응답을 통해 초기 요인가중치와 위협별 요인점수를 실측하였고, 외부 LLM 무단 직접 접속(T1)이 최우선 대응 위협으로 확인되었다. 균등가중 기준선과 비교한 결과 T1과 T4의 순위만 뒤바뀌었으며(Kendall's $\tau=0.80$), T1이 두 가중치 체계 모두에서 상위 1-2순위를 유지해 핵심 결론에는 큰 영향을 주지 않으나, 특정 가중치 산출 방식에 대한 민감도가 완전히 없다고는 볼 수 없음을 확인하였다.

본 연구의 한계는 다음과 같다. 첫째, 요인 간 가중합(SAW) 결합 방식은 본질적으로 보상적이어서, 특정 요인이 극단적으로 높은 위협이 다른 요인의 높은 값으로 상쇄될 수 있다는 한계가 있으며, 이에 대한 비보상적 대안(outranking 기법 등)은 후속 연구 과제로 남긴다. 둘째, 전문가 패널($n=15$, 유효응답 $n=12$)은 국내 금융권 전체를 대표하기에는 제한적이며, 선정 기준과 모집 절차를 4.1절에 명시하였으나 패널 규모 자체의 한계는 유지된다. 특히 패널은 저자의 정보보호 실무자 커뮤니티 네트워크를 통한 목적표집·쿼터표집으로 모집되었으므로, 무작위 표집 대비 특정 성향의 전문가가 과대표집되었을 가능성을 배제할 수 없다. 셋째, CR* 기준 초과 3인의 제외는 사전에 정한 통상적 임계값(0.1)에 따른 것이며 15인 전체와 12인

필터링 표본 간 결과가 일관됨을 확인하였으나, 소수 인원의 제외가 갖는 근본적 한계는 존재한다. 넷째, 1차 델파이 조사(위협 도출·CVR)와 2차 BWM·리커트 조사는 상당한 시간차를 두고 진행되었고 그 사이 패널 구성원 중 상당수가 교체되어, 동일한 소속 구성 비율은 유지되었으나 동일 인물의 시계열 응답은 아니다. 이는 1차 조사에서 확정된 후보 위협 목록(Table 1)이 서로 다른 두 패널에 걸쳐 사용되었다는 의미이며, 위협 도출 결과의 일관성에 영향을 줄 수 있는 요인으로 한계에 명시한다. 다섯째, 2차 패널의 상당수는 1차 델파이 조사 당시 저자로부터 본 연구 주제를 이미 소개받고 의견을 나눈 동일 커뮤니티 소속 전문가로 구성되어, 연구자의 가설이나 1차 AHP 결과(예: T3가 최우선순위였다는 점)를 사전에 인지한 상태에서 2차 BWM·리커트 응답을 했을 가능성을 배제할 수 없다. 이는 앵커링(anchoring) 또는 기대순응(demand characteristics) 편향의 소지가 있으며, 연구자와 사전 소통이 없는 독립적 패널을 사용한 재현 연구를 통해 검증할 필요가 있는 한계로 명시한다. 여섯째, 3.4절의 실증적 재검증 절차(레드팀 PoC·운영 로그 모니터링)는 개념적 설계로 제시된 것으로, 실제 레드팀 PoC·운영 로그를 통한 갱신 주기와 절차의 실행은 후속 연구가 필요하다. 일곱째, 후보 위협이 5개로 제한되어 있어 4.5절의 민감도 분석(Kendall's τ)은 소표본 결과로 해석에 주의가 필요하다. 여덟째, 재정의된 T5' 항목은 별도의 정량적 CVR 재평가를 거치지 않았으며, 2차 조사에서의 리커트 평가 참여만으로는 정식 내용타당도 검증을 완전히 대체하지 못한다는 한계가 있다. 이에 대한 독립적 CVR 재평가는 후속 연구 과제로 남긴다.

향후 연구에서는 이 절차를 자동화하여, 탐지 신호가 실시간으로 L·D값에 반영되고 인프라·위협 변화에 따라 Risk 점수가 즉시 재계산되는 통합 의사결정 파이프라인으로 발전시키고, 비보상적 결합 방식과의 비교, 그리고 확장된 후보 위협 목록에 대한 재검증을 진행하고자 한다. 본 연구는 단일 시점의 위험평가를 수행하는 기존 접근과 달리, 생성형 AI 기술과 보안 인프라가 함께 변화하는 환경을 고려하였다. 위협 우선순위는 고정된 값이 아니라, 보안 인프라의 성숙도와 규제 환경 변화에 따라 3.5절의 트리거가 발생할 때마다 반복적으로 재산정되어야 하는 동적(Dynamic) 의사결정 대상이다.

REFERENCES

- [1] Gartner, "Top Security and Risk Considerations for Generative AI," Gartner Research, 2024.
- [2] Financial Services Commission (Korea), "Roadmap for Improving Network Separation in the Financial Sector," FSC Press Release, 2024.
- [3] Financial Services Commission (Korea), "Response Guidelines for Frontier AI Security Threats in the Financial Sector," FSC Press Release, Jul. 1, 2026.
- [4] Financial Security Institute (Korea), "Guidelines for the Use of Generative AI in the Financial Sector," FSI Security Research Report, 2025.
- [5] Financial Supervisory Service (Korea), "Support Measures and Supplementary Countermeasures for the Use of Generative AI in the Financial Sector," FSS Guidebook, 2025.
- [6] Anthropic, "Model Context Protocol (MCP) Specification," Anthropic Technical Documentation, 2024.
- [7] OWASP Foundation, "Agentic AI — Threats and Mitigations," OWASP GenAI Security Project, 2025.
- [8] MITRE Corporation, "MITRE ATLAS (Adversarial Threat Landscape for AI Systems)," MITRE Knowledge Base, 2025.
- [9] A. Silic and A. Back, "Shadow IT — A View from Behind the Curtain," *Computers & Security*, vol. 45, pp. 274–283, 2014.
- [10] OWASP Foundation, "OWASP Top 10 for Large Language Model Applications 2025," OWASP Foundation Report, 2025.
- [11] NIST, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)," NIST AI 100-1, 2023.
- [12] A. Ishizaka and P. Nemery, "Multi-Criteria Decision Analysis: Methods and Software," Wiley, 2013.
- [13] J. Rezaei, "Best-worst multi-criteria decision-making method," *Omega*, vol. 53, pp. 49–57, 2015.
- [14] J. Rezaei, "Best-worst multi-criteria decision-making method: Some properties and a linear model," *Omega*, vol. 64, pp. 126–130, 2016.
- [15] H. A. Linstone and M. Turoff (Eds.), "The Delphi Method: Techniques and Applications," Addison-Wesley, 1975.
- [16] C. R. Lawshe, "A Quantitative Approach to Content Validity," *Personnel Psychology*, vol. 28, no. 4, pp. 563–575, 1975.
- [17] M. G. Kendall, "Rank Correlation Methods," Griffin, 1948.

Authors



Seungman Jin received the B.S. and M.S. degrees in Computer Engineering from Jeonbuk National University and Yonsei University, Korea, in 2002 and 2006, respectively, and completed the Ph.D.

coursework in Computer Engineering from Jeonbuk National University, Korea, in 2022. Mr. Jin performed information security duties at the Korea Internet & Security Agency (KISA) in 2002, Samsung Electronics in 2006, and FSEC in 2007. He joined Jeonbuk Bank in 2011, where he is currently serving as the Information Security Officer.



Deukjo Hong received the B.S. and M.S. degrees in Mathematics from Korea University in 1999 and 2002, respectively, and the Ph.D. degree in Information Security from Korea University in 2006.

Mr. Hong is currently a Professor in the Department of Computer Science & Artificial Intelligence at Jeonbuk National University. His research interests include cryptography and network security.