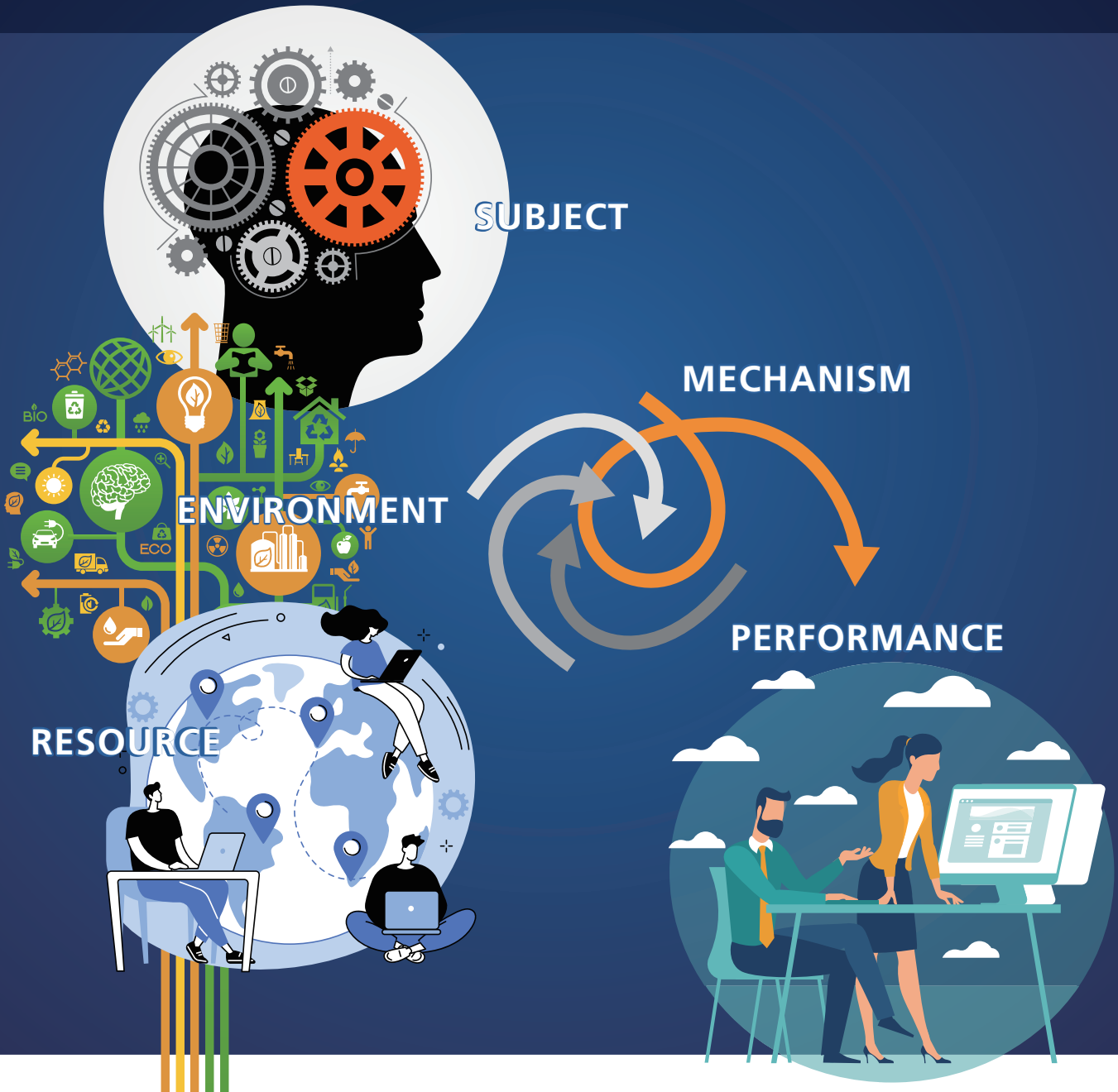
5권 1호

메커니즘 연구

Journal of MECHANISM MANAGEMENT



메커니즘경영학회
MECHANISM SOCIETY

5권 1호

메커니즘 연구

Journal of Mechanism Management

2025.05

메커니즘 경영학회
Mechanism Society

SER-M 모델을 활용한 자동차 산업 정보보안 메커니즘 연구

TISAX 인증 획득 성공 사례를 중심으로

A Study on Information Security Mechanism in the Automotive Industry Using the SER-M Model

Focusing on Successful Cases of TISAX Assessment

지신명*　　신호상**

목　　차

I. 서론
II.이론적 배경
1. TISAX 인증의 개념과 절차
2. SER-M 모델의 구성요소와 메커니즘
3. 정보보안과 경영성과 선행 연구 검토
III. 연구 설계 및 사례분석 방법
1. 연구 모델
2. 데이터 수집 및 분석 방법
IV. 사례 분석 및 논의
1. 주체 측면
2. 환경 측면
3. 자원 측면
4. 메커니즘 측면
5. 분석 결과
V. 결론

국 문 초 록

자동차 산업의 디지털 전환 가속화로 정보보안 위협이 증가함에 따라, 글로벌 공급망 내 TISAX(Trusted Information Security Assessment Exchange) 인증의 중요성이 강조되고 있다. 본 연구는 SER-M 모델을 활용하여 TISAX 인증이 기업의 정보보안 체계 구축 및 경영 성과에 미치는 영향을 구조적으로 분석하였다. 분석 결과, TISAX 인증 과정에서 주체(Subject), 환경(Environment), 자원(Resource)의 상호작용을 통해 다양한 전략적 메커니즘이 형성되며, 이는 기업의 정보보안 역량 강화와 경쟁력 확보에 핵심적으로 기여함을 확인하였다. 특히, 인증을 획득한 기업들은 고객 신뢰 증대, 글로벌 완성차 제조사와의 협력 기회 확대, 공급망 보안 요구 사항에 대한 선제 대응을 통해 전략적 우위를 확보하고 있었다.

사례 분석에 따르면, 대기업은 외부 환경 변화에 정보보안 전담 조직이 체계적으로 대응하고 내부 자원을 효과적으로 통합하는 '자원 혁신형(E-S-R)' 메커니즘을 나타낸 반면, 중소기업은 최고경영진의 리더십을 기반으로 자원을 선제적으로 확보하고, 이를 바탕으로 환경 변화에 유연하게 대응하는 '자원 창조형(S-R-E)' 전략을 구사하고 있었다. 또한 정보보안 전담 조직의 역량, 최고경영진의 리더십, 외부 환경에 대한 해석 역량이 인증 성과에 영향을 미치는 주요 요인임을 확인되었다. SER-M 모델을 기반으로 한 본 연구는 TISAX 인증 과정에서 형성되는 전략 메커니즘의 동태적 작용을 분석함으로써, 정보보안 전략 수립을 위한 실천 가능한 방향성과 구조적 기준을 제안하였다. 이로써, 정보보안 체계 구축은 자원의 배분을 넘어서, 주체, 환경, 자원의 유기적 상호작용에 기반한 전략적 메커니즘 설계 과정임을 시사하였다.

주제어: 정보보안 전략(Information Security Strategy), TISAX 인증(TISAX Assessment), 자동차 산업(Automotive Industry), SER-M모델(SER-M Model), 메커니즘(Mechanism)

I. 서론

자동차 산업은 글로벌 경제와 공급망의 중심에서 높은 품질과 안정성을 요구하는 현대 사회의 핵심 산업으로 자리매김하고 있다. 최근에는 스마트 모빌리티, 자율주행차, 커넥티드 자동차 등 정보통신 기술의 발달과 함께 디지털 전환이 급속히 진행되고 있으며, 이에 따라 사이버보안 위협 또한 빠르게 증가하고 있다. 실제로 2024년 전체 사이버 공격의 약 60%는 수천 개 이상의 자동차를 동시에 타격한 '초대형(massive)' 규모의 사건으로 분류되며, 이는 기존의 규제 중심의 보안 체계만으로는 실질적인 대응에 한계가 있음을 보여준다(Upstream Security Ltd., 2025).

이러한 보안 위협은 기존의 물리적 사고를 넘어 원격 해킹, 랜섬웨어 등 디지털 기반 공격으로 확산되고 있으며, 이는 자동차 제조업체뿐 아니라 부품 공급업체, 서비스 제공업체를 포함한 전체 공급망에 심각한 영향을 미치고 있다. 자동차 산업의 보안 사고는 그 빈도와 피해 규모가 지속적으로 증가하고 있으며, 공급망 전반의 운영 안정성과 신뢰성에 중대한 위협 요인으로 작용하고 있다(김동원 외, 2015). 이에 따라 자동차 제조업체와 협력업체들은 데이터 보호와 신뢰 확보를 위해 전략적 정보보안 체계의 도입이 필수적인 상황에 직면해 있다. 이러한 환경 속에서 독일자동차산업협회(VDA)와 유럽 자동차 제조·공급협회(ENX)는 자동차 산업에 특화된 정보보안 관리체계 및 인증 제도인 TISAX(Trusted Information Security Assessment Exchange) 표준을 개발하였다. TISAX는 공급망 내 데이터 보호를 위한 표준화된 접근법을 제공하며, 정보보안 수준을 강화하고 이를 통해 고객 신뢰와 경영 성과를 창출하는 데 기여하고 있다(지신명, 신호상, 2024). 최근 국내에서도 TISAX 인증의 필요성이 확산되면서, 인증을 준비하거나 획득한 기업들의 모범 사례가 점차 늘어나고 있다. 그러나 TISAX 인증 준비는 단순한 기술적 요건의 충족을 넘어, 자동차 산업 특유의 복잡한 공급 구조, 다양한 이해관계자, 고도화된 IT 인프라 등을 고려한 전략적 대응을 요구한다. 인증 과정에는 장기간의 준비와 상당한 자원 투입이 수반되며, 조직 내부의 역량뿐 아니라 외부 환경과의 정합성도 중요한 배경 요인으로 작용한다.

이러한 배경 속에서 본 연구는 TISAX 인증을 준비하고 추진하는 기업들이 어떠한 전략을 수립하고 실행하는지를 분석하고자 한다. 특히 인증 추진 과정에서 조직의 주체(Subject), 환경(Environment), 자원(Resource)이 상호작용하는 방식에 주목하고, 이로부터 기업별로 어떠한 메커니즘(Mechanism)이 형성되는지를 규명하고자 한다. 이를 위해 SER-M 모델을 분석틀로 적용하여, 자동차 산업내 기업들이 직면한 환경과 자원 조건, 그리고 그에 따른 전략적 선택이 TISAX 인증 성과와 어떤 관계를 형성하는지를 체계적으로 분석하고자 한다.

이를 위해 본 연구는 실제 인증을 수행한 사례를 중심으로 상이한 유형의 정보보안 메커니즘을 비교하고, 이들이 경영 성과 및 지속 가능성 확보에 미친 영향을 분석함으로써, 자동차 산업에서의 전략적 보안 접근이 기업 경쟁력에 어떻게 연결되는지를 설명하고자 한다. 나아가 이러한 분석을 통해, 유사한 인증 제도나 보안 체계를 도입하려는 타 산업군에도 적용 가능한 시사점을 제시하고자 한다.

논문접수일: 2025년 3월 4일, 게재확정일: 2025년 5월 23일
* 서울과학종합대학원대학교 경영학과 박사과정, denverchialex@gmail.com (제1저자)
** 서울과학종합대학원대학교 경영학과 전임교수, hsshin@assist.ac.kr (교신저자)

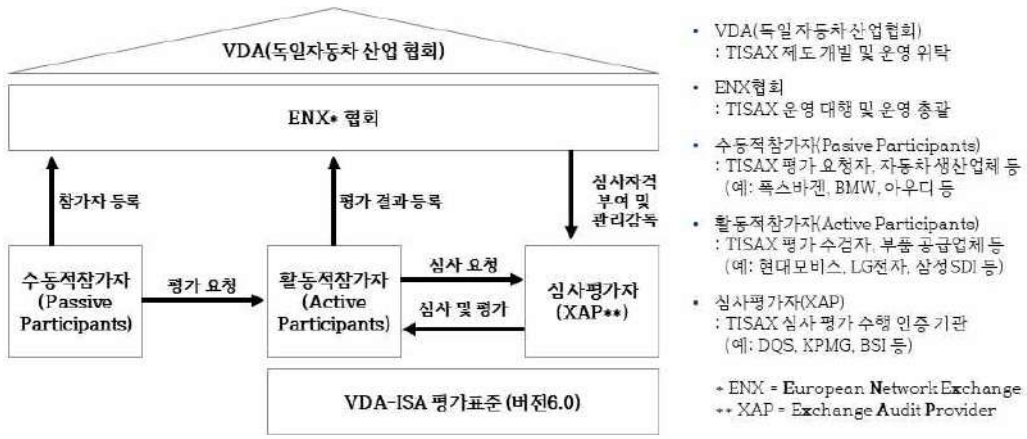
II. 이론적 배경

1. TISAX 인증의 개념과 절차

TISAX(Trusted Information Security Assessment Exchange)는 자동차 산업의 특수한 정보보안 요구를 반영하기 위해 개발된 평가 및 교환 절차로, 독일자동차산업협회(VDA)가 ISO/IEC 27001을 기반으로 자체 정보보안 평가 도구인 ISA(Information Security Assessment) 체크리스트를 개발하여 이를 체계화하였다. ENX 협회는 TISAX의 운영과 평가 절차의 감독, 그리고 감사 결과의 등록 및 공유를 담당한다. 기초가 된 ISO/IEC 27001은 다양한 산업 분야에서 정보보안 정책의 수립, 위험 평가 및 관리, 그리고 보안 통제 조치를 통해 정보보안을 체계적으로 구현하도록 설계된 국제 표준이다. 그러나 해당 표준은 범용적인 적용을 전제로 하고 있기 때문에, 복잡하고 고도로 통합된 공급망, 기술 집약적 설계 및 제조 공정, 그리고 지적재산 보호에 대한 산업 특유의 요구가 강한 자동차 산업의 보안 이슈를 충분히 반영하는 데 한계가 존재한다(지신명, 신호상, 2024).

이에 따라 TISAX는 ISO/IEC 27001의 핵심 원칙을 기반으로 하되, 자동차 산업이 직면한 고유의 보안 위협과 공급망 리스크를 반영한 보완적 체계로 발전하였다. 평가 절차에는 정보 제공 요청의 주체에 따라 활동적 참가자(Active Participants)와 수동적 참가자(Passive Participants)로 구분되며, 모든 평가 결과는 ENX 플랫폼을 통해 안전하게 상호 공유될 수 있다(ENX Association, 2024).

[그림 1] TISAX 참가자 그룹 구조



출처: ENX Association(2024) 제공 정보 재구성

[그림 1]에 나타난 바와 같이, TISAX 평가는 자동차 제조사(OEM)인 수동적 참가자가, 주로 부품 업체로 구성된 활동적 참가자에게 정보보안 관리 수준 입증을 요청하는 것에서 시작된다. 이후, 수동적 참가자의 정보보안 평가 요구 수준에 따라 활동적 참가자는 TISAX 평가 목표 및 수준을 등록하고, 공인된 심사 평가자에 의해 정보보안 역량 평가가 수행된다. 평가가 성공적으로 완료되고 인증을 획득하면 ENX 시스템에 등록되며, 이를 통해 관련된 모든 참가자 간에 평가 결과가 투명하고 신뢰성 있게 공유된다.

폭스바겐, BMW, 메르세데스-벤츠 등 주요 유럽 제조사들은 이미 TISAX를 공급망 참여의 필수 요건으

로 채택하고 있으며, 2024년 기준 전 세계 약 10,000개 기업이 인증을 획득하였다(ENX Association, 2024). 국내에서도 유럽 자동차 OEM과의 협력하는 기업들을 중심으로 관련 인증 도입이 확대되고 있으며, 약 250개 사업장이 인증을 완료한 상태다, 한국은 세계 5위의 자동차 생산국이지만, TISAX 인증 기업 수는 아직 글로벌 10위권에 미치지 못하고 있다. 그러나 글로벌 OEM 및 1차 협력사들과의 연계가 확대됨에 따라 국내 기업의 참여도는 점차 증가하고 있으며, 이에 따른 중요성 또한 부각되고 있다. 앞으로 참여 기업 수는 더욱 증가할 것으로 예상되며, 정보보안 평가 체계는 글로벌 자동차 산업 공급망의 보안성과 신뢰성 확보를 위한 핵심 수단으로 자리 잡아 가고 있음을 시사한다.

2. SER-M 모델의 구성요소와 메커니즘

SER-M 모델은 기업의 경영성과를 설명하기 위한 통합적 분석 틀로서 주체(Subject), 환경(Environment), 자원(Resource) 세 요소가 상호작용하여 메커니즘을 형성하고, 이를 통해 성과가 도출되는 과정을 설명한다. 기존의 요소 독립적 접근을 넘어서, 이들 간의 동태적 결합과 상호작용을 강조함으로써 기업의 지속 가능성과 경쟁력을 설명하는 데 효과적인 분석 도구로 작용한다(조동성, 2014; 조동성, 문휘창, 2022).

주체는 최고경영진 및 핵심 의사결정자로서 기업의 비전 수립, 전략 실행, 조직 구조 설계 등을 통해 전략의 중심축으로 작동하며 환경 및 자원을 고려한 판단과 실행을 통해 조직의 방향을 형성한다. 환경은 법적 규제, 경쟁구조, 시장 변화 등 외부 조건을 포함하며, 이에 대한 대응 전략은 기업 성과에 직접적 영향을 미친다. 자원은 내부의 인적, 물적, 기술적 기반으로, 전략 실행과 경쟁력 확보의 기반이다(구자원, 신철호, 이동환, 2009; 2012). 이들 요소는 각각 독립적 의미를 가지지만, SER-M 모델에서는 상호작용을 통해 성과를 창출한다는 점에서 중요한 통합적 의의를 지닌다(조동성, 2014).

메커니즘은 SER-M 모델의 핵심 개념으로, 주체, 환경, 자원이 상호작용하는 과정에서 형성되는 기업 경영의 원칙이다. 기업의 메커니즘은 그 기업만이 가지고 있는 고유한 특징을 반영하기 때문에, 경쟁 기업들이 쉽게 모방하기 어려운 지속적 경쟁우위의 원천이 될 수 있다(조동성, 2014).

조동성(2014)은 메커니즘을 창출하는 원리는 주체, 환경, 자원 간 다양한 상호작용 방식을 설명하기 위한 개념화이며, 이 세 요소가 상호작용하는 방식은 조합(Combination)과 순서(Permutation), 그리고 시간(Time)에 따라 설명할 수 있다고 하였다. 이는 곧 조직의 성과 역시 단순한 요소를 보유하는 데 그치지 않고, 그것들이 어떤 메커니즘에 따라 상호작용하느냐에 달려 있다는 점을 시사한다. 이러한 관점은 SER-M 모델이 자산 기반 논리를 넘어서, 메커니즘 중심의 전략적 사고로의 전환을 요구함을 보여준다.

이러한 관점은 특히 자동차 산업처럼 복잡한 공급망과 다양한 이해관계자가 얽혀 있는 산업 맥락에서 유의미하다. 정보보안이 전략적 경영 요소로 기능해야 한다는 점에서, SER-M 모델은 이를 체계적으로 해석할 수 있는 프레임워크를 제공한다. 예컨대 TISAX 인증과 같은 제도적 요건이 기업 성과에 어떤 방식으로 연결되는지를 메커니즘 관점에서 해석함으로써, SER-M 모델은 실무적으로도 높은 유용성을 지닌다고 할 수 있다.

3. 정보보안과 경영성과 선행 연구 검토

기존 정보보안 관련 연구는 보안 위협, 위험 관리, 보안 투자의 효과 등 개별 요인에 대한 분석에 주로 초점을 맞추어 왔다. 정보보안 인증이 경영성과에 미치는 영향을 다룬 정성적·정량적 연구도 일부 존재하나, 성과 창출의 내재적 작동 원리를 설명하는 메커니즘 기반 접근은 여전히 부족한 상황이다.

배영식(2012)은 정보보안 인증이 조직의 경영성과에 긍정적인 영향을 미친다고 주장하였으며, 박재영, 정우진(2019)은 보안 인증이 기업 주가에 긍정적으로 작용함을 보고하였다. 신현민, 김인재(2020)는 정보

보안 인증 기업이 비인증 기업보다 매출과 영업이익에서 유의미한 차이를 보이며, 기업 성과에 긍정적 영향을 줄 수 있음을 제시하였다. Alharbi and Gregg(2022)는 보안 투자가 단독으로는 제한적일 수 있으나, IT 투자와의 전략적 연계를 통해 재무 성과 개선에 기여할 수 있다는 점을 강조하였다. 그러나 이들 연구는 대부분 결과 중심의 분석에 머물며, 정보보안이 주체, 자원, 환경 등 투입 요소들과 어떠한 메커니즘을 통해 결합되어 성과로 이어지는지에 대한 설명은 상대적으로 부족하였다. 지신명, 신호상(2024)은 인과순환지도(CLD)를 통해 TISAX 인증이 정보보안 태세와 전략 결정에 영향을 미친다고 분석하였으나, 그 결과 역시 메커니즘의 구조와 작동 경로 자체를 직접적으로 다루지는 않았다.

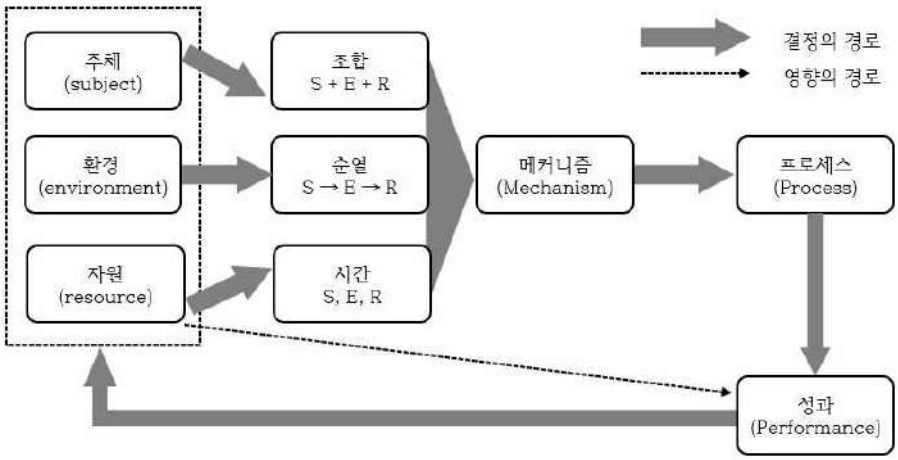
이러한 한계를 보완하는 대안적 분석틀로 SER-M 모델을 적용할 수 있다. 이는 메커니즘 기반의 전략적 사고틀로 다양한 산업의 사례 분석에 활용되어 왔다. 예를 들어, 김태종, 엄재근(2020)은 LG전자의 프리미엄 가전 시장을 대상으로 전략 메커니즘을 도출하였으며, 유정범 외(2021)는 종합 물류기업 메쉬코리아의 성장 사례를 통해 기술력과 외부 환경의 융합에 관한 메커니즘을 분석하였다. 이희수, 고영희(2022)는 직업훈련기관 사례를 통해 환경 대응 전략의 전개 과정을 고찰하였으며, 김지훈 외(2023)는 안전보건경영시스템 인증 메커니즘을 탐색하였다. 이용수, 임효숙(2024)은 전통 보험회사의 디지털 전환 사례를 통해 인슈어테크 기반 전략 메커니즘을 제시하였다. 따라서 본 연구는 SER-M 모델의 이론적 강점을 활용하여 TISAX 인증이 자동차 산업의 정보보안 역량 강화와 경영성과 창출에 기여하는 메커니즘을 심층적으로 분석하고자 한다. 기존 연구들이 다양한 산업군에 SER-M 모델을 적용해 온 것과 달리, 본 연구는 자동차 산업이라는 특수한 맥락에서 TISAX가 기업의 경쟁력과 지속 가능성에 미치는 영향을 조명한다. 특히, 인증 과정에서 주체, 환경, 자원이 상호작용하며 형성하는 메커니즘을 정리함으로써, 정보보안 전략 수립과 실행에 있어 실질적인 방향성을 제시하고자 한다.

III. 연구 설계 및 사례 분석 방법

1. 연구 모델

본 연구는 메커니즘 기반 관점을 적용하여 TISAX 인증 사례를 분석하였다. SER-M 모델은 주체, 환경, 자원이 상호작용하여 메커니즘을 형성하고, 이를 통해 기업 성과가 도출되는 과정을 설명하는 이론적 틀이다(조동성, 2014). [그림 2]에 제시된 내용으로서의 메커니즘 기반 관점(Mechanism-Based View)은 경영자가 의도하는 전략적 메커니즘을 구현하기 위해 주체, 환경, 자원의 각 요소들이 어떻게 조합(Combination)되고, 어떠한 순열(Permutation)로 배치되며, 활용 시점(Timing)이 어떻게 결정되는지가 전략 구성과 실행 방식에 결정적인 영향을 미친다고 본다. 이 관점은 주체, 환경, 자원을 효과적으로 결합하고 우선순위를 설정하는 전략적 사고와 행동 원칙(Logic of Thought and Principles of Behavior)을 설명하며, 기업의 경쟁우위는 개별 요소가 아닌 이들의 창조적 상호작용을 통해 형성된 메커니즘에서 비롯됨을 의미한다(조동성, 2014; 저우위보, 조동성, 2023).

[그림 2] 내용으로서의 메커니즘 기반 관점



출처: 조동성(2014, p.53), 메커니즘기반관점

SER-M 모델에서 조합은 메커니즘을 구성하는 각 요인의 결합을 지칭하며, 순열은 요인이 작동하는 순서에 따른 전략 형성의 흐름을 의미한다. 기업이 처한 상황과 대응 방식에 따라 <표 1>과 같은 메커니즘 유형으로 분류할 수 있다. 첫째, 창조형 메커니즘은 주체가 자원과 환경을 주도적으로 창출하는 방식이며, 둘째, 혁신형 메커니즘은 기존의 환경 혹은 자원에서 주체가 변화를 이끌어내는 형태이다. 셋째, 적응형 메커니즘은 주어진 환경이나 자원을 따라 주체가 수동적으로 대응하는 방식이다(조동성, 2014).

<표 1> 순열 기반의 메커니즘 유형

메커니즘	세부 유형	상세
창조형	환경 창조(SER)	주체가 강한 비전과 창의적 발상으로 새로운 환경을 적극 창조
	자원 창조(SRE)	주체가 강력한 비전을 가지고 조직 내부에 새로운 자원을 창출
혁신형	환경 혁신(RSE)	기존 자원을 주어진 조건으로 주체가 환경을 적극 혁신하는 유형
	자원 혁신(ESR)	기존 환경을 주어진 조건으로 주체가 자원을 적극적으로 혁신
적응형	환경 적응(ERS)	주어진 환경 하에 주체가 기존 자원을 소극적으로 유지하는 환경 적응
	자원 적응(RES)	기존 자원으로 주체가 소극적으로 환경을 활용하는 자원 적응

출처: 조동성(2014)

이러한 요소의 배치 순서와 기업의 대응 속도는 궁극적으로 TISAX 인증의 성공 여부와 정보보안 체계 강화에 있어 전략적 차별화를 가능하게 한다. 본 연구는 이러한 이론적 틀을 바탕으로, TISAX 인증 준비 과정에서 주체, 환경, 자원이 어떻게 상호작용하고, 각 요소가 어떤 방식으로 전략 형성에 영향을 미치는지를 분석하였다. 우선 주체가 중심이 되는 경우, 최고경영진의 리더십과 정보보안 담당자의 전략적 판단이 핵심 역할을 수행하며, 환경과 자원을 조정하는 방식으로 정보보안 체계가 설계된다. 반면, 환경이 우선시될 경우에는 글로벌 규제나 고객 요구에 기반한 전략 수립과 자원 확보가 이뤄지며, 자원이 중심이 될 경우에는 기존의 기술력과 인적 역량을 바탕으로 외부 요구를 조율하게 된다. 이러한 상호작용

은 요소의 배치 순서와 대응 속도에 따라 정보보안 체계의 유형을 달리하며, 결과적으로 차별적인 성과로 이어진다(조동성, 2014; 이형진, 하수경, 2024).

한편, 본 연구는 SER-M 모델의 전 범주를 포괄적으로 적용하기보다는, 분석 실효성을 높이기 위해 TISAX 인증을 획득한 두 대표 기업 사례에서 실제로 확인된 메커니즘 유형인 '자원 혁신형(E-S-R)'과 '자원 창조형(S-R-E)'에 초점을 맞추어 분석을 수행하였다. 이를 통해 SER-M 모델이 이론적 분류를 넘어서, 기업의 정보보안 전략이 제도적 요구에 어떻게 구조화되고 실행되는지를 설명할 수 있는 유효한 분석 프레임임을 실증적으로 제시하고자 한다.

2. 데이터 수집 및 분석 방법

본 연구는 TISAX 인증과 정보보안 경영성과 간의 관계를 분석하기 위해 문헌 자료, 사례 분석, 인터뷰 등 다양한 방법을 활용하였다. 연구의 신뢰성과 타당성을 확보하기 위해 학술 논문, 산업 보고서, 기업 공시 자료, 그리고 현장 실무자와 전문가 집단의 경험에 기반한 정성적 자료를 폭넓게 활용하였다. 문헌 자료는 정보보안 인증 관련 학술 연구, 자동차 산업 내 정보보안 정책과 실무 현황, ENX 보고서, 기존 TISAX 인증 사례 및 보안 규제에 대한 자료를 포함하며, TISAX를 주관하는 ENX와 실제 인증을 수행한 인증기관의 평가 자료를 참조하여 최신 동향과 업계 요구사항을 파악하였다.

사례 분석을 위한 정성적 자료는 본 연구에서 사례 분석 대상으로 선정된 현대모비스와 태림산업과의 실무 교류를 통해 심층적으로 확보하였다. 현대모비스는 과거부터 정보보안 실무진과의 협업 경험이 있어 TISAX 인증 추진 과정과 전략을 파악하였으며, 태림산업은 인증 수여식 전후로 경영진 및 실무 책임자와의 대면 미팅, 이메일 및 전화 커뮤니케이션을 통해 실제 대응 방식과 경영진의 인식을 파악하였다. 여기에 더해 인증기관 심사원 및 자동차 정보보안 컨설턴트의 의견도 반영하여 보다 균형 잡힌 시각을 확보하였다.

아울러, 정보보안 실무자 및 전문가 집단을 대상으로 설문조사를 수행하였으나, 해당 설문 결과에 대한 정량적 분석은 본 연구의 범위에서는 다루지 않고, 기존 문헌의 분석 결과를 인용하여 분석에 활용하였다. 정량적 근거는 기존 연구(지신명, 신호상, 2025)에서 수행된 AHP(Analytic Hierarchy Process) 결과를 인용하여 반영하였다. 해당 연구에서는 정보보안 전문가 18인을 대상으로, 기술적, 조직적, 환경적 요인 간의 상대적 중요도와 하위 요인을 분석하였다. 분석 결과, 조직적 요인이 가장 높은 가중치를 보였으며, 그 중에서도 정보보안 특히 전담부서와 경영진의 지원이 핵심 요인으로 도출되었다. 이러한 결과는 사례 분석에서 TISAX 인증 준비에 있어 SER-M 모델의 주체(S) 요소가 전략 형성과 실행에서 핵심적으로 작용함을 정략적으로 뒷받침하는 근거로 활용되었다.

IV. 사례 분석 및 논의

1. 주체 측면

주체는 기업의 정보보안 전략을 기획하고 실행하는 핵심 의사결정 주체로, 본 연구에서는 정보보안 담당자, 최고경영진, 관련 부서들이 이에 해당한다. 정보보안 전담 부서는 TISAX 인증 요구사항 분석, 정책 수립, 내부 절차 정비, 심사 대응 등 인증 준비와 유지 전반을 주도하며, 체계 유지를 위한 지속적인 개선에도 관여한다. 이러한 역할은 인증의 실질적 성공뿐 아니라 보안 체계의 지속 가능성 확보에 중요한 기여를 한다. 한편, 경영진은 정보보안을 기업 경영 전략의 중요한 축으로 인식하고, 이에 필요한 자원을 적극적으로 지원할 필요가 있다. 정보보안 투자가 비용으로만 인식되면 전략적 대응이 지연될 수 있으며, 조직적 지원이 부족할 경우 보안 정책의 적극적 실행도 어려워질 수 있다. 따라서 최고경영진의

전략적 리더십은 TISAX 인증 성공의 핵심요인으로 작용한다.

이러한 주체 요인의 중요성은 기존 정량적 연구에서도 확인된 바 있다. 지신명, 신호상(2025)의 연구에서는 AHP(Analytic Hierarchy Process)를 활용해 정보보안 전략 요인들의 상대적 중요도를 분석하였으며, 그 결과 조직적 요인이 기술적·환경적 요인보다 높은 중요도를 나타냈다. 특히 정보보안 전담 부서와 최고경영진의 리더십이 핵심 영향 요인으로 도출되었다.

본 연구는 이러한 정량적 결과를 사례 분석에 이론적 기반으로 활용하여, SER-M 모델의 주체 요소가 전략 수립과 실행 과정에서 어떻게 작용하는지를 해석하고자 한다. 아래 <표 2>는 해당 AHP 분석 결과를 재구성한 것으로, 조직적 요인(0.4550)이 가장 높은 비중을 차지하였으며, 정보보안 전담 부서(0.1472)와 경영진의 지원(0.1234)이 각각 1위와 2위를 기록하였다.

이 결과는 정보보안 전략 수립과 실행에서 주체 요인의 상대적 중요성을 정량적으로 보여주며, SER-M 모델의 주체 측면 분석에 이론적 정당성을 부여한다. 이후 사례 분석에서는 현대모비스와 태림산업이 이러한 주체 요인을 어떻게 전략적으로 활용했는지를 비교해 살펴보고자 한다.

<표 2> 정보보안 요인별 중요도 (AHP 분석 결과)

단계	주체	종합 중요도	중요도 순위
조직적 요인(0.4550)	**정보보안 전담부서**	**0.1472**	**1위**
	경영진의 지원	**0.1234**	**2위**
	내부 프로세스 정렬성	0.0949	4위
	직원 보안 인식 및 역량	0.0895	5위
기술적 요인(0.3123)	데이터 기밀성	0.1130	3위
	데이터 무결성	0.0801	6위
	데이터 가용성	0.0773	7위
	IT인프라 및 시스템 호환성	0.0420	11위
환경적 요인(0.2327)	법적 규제 및 정부 지원	0.0697	8위
	공급망 요구 및 신뢰성	0.0662	9위
	고객 요구 및 신뢰	0.0556	10위
	산업 경쟁 및 기술 트렌드	0.0412	12위

출처: 지신명, 신호상(2025) 논문 재구성

가. 정보보안 전담부서의 체계적 강화: 현대모비스 사례

현대모비스는 전문 정보보안 부서의 체계적인 운영이 TISAX 인증 성공에 어떻게 기여할 수 있는지를 보여주는 대표적인 사례이다. 2021년 TISAX 인증을 최초 획득한 이후, 인증 유지와 정보보안 역량 강화를 지속해왔으며, 2024년 기준 연간 매출 57조 원 중 절반 이상을 해외에서 달성할 만큼 글로벌 시장에서의 입지를 확고히 하고 있다(현대모비스, 2024)

현대모비스의 정보보안 전략은 정보보안 전담조직의 구조화된 운영 체계를 중심으로 구축되어 있다. 일반 정보보안팀 외에도 IT 운영팀과 사이버보안팀을 명확히 구분하여 정보보안의 세부 영역을 기능적으로 분화하였고, 본사는 글로벌 생산 및 R&D 법인의 보안을 총괄하며 강력한 정책과 솔루션을 일관되게 수

립하고 제공하고 있다. 이러한 구조는 ISO/IEC 27014에서 제시하는 정보보안 거버넌스의 핵심 요소인 '역할의 명확화'와 '중앙 통제 구조'를 잘 구현한 사례로 볼 수 있다.

특히, 2020년부터 사이버 전담 조직을 중심으로 자동차 사이버보안 업무 시스템(CSMS, Cyber Security Management System)을 고도화하고, 글로벌 보안 검점 간 정책 일관성과 실행 체계를 정비하였다. 이는 조직의 대응 역량이 TISAX 인증뿐 아니라 이후 정보보안 제도 대응 체계에도 기여했음을 보여준다. 또한, 정보보안 조직의 전문성과 지속적인 역량 강화는 Barney(1991)가 제시한 자원 기반 관점(Resource-Based View)에서 말하는 '내재된 조직역량'이 지속가능한 경쟁우위로 전환되는 과정을 잘 설명해준다. 즉, 현대모비스 사례는 대규모 조직에서 정보보안이 기술이나 정책을 넘어, 구조화된 조직 시스템과 전략적 자원 배분을 통해 성과로 연결될 수 있음을 시사한다.

나. 최고경영진의 리더십: 태림산업 사례

태림산업은 경남 창원에 위치한 자동차 부품 제조업체로, 글로벌 1차 협력사인 보쉬(Bosch), ZF 그룹 등 글로벌 1차 협력사에 납품하며, 생산품의 77% 이상을 수출하는 강소기업이다. 2024년, 경남 지역 중소기업 최초로 TISAX 인증을 성공적으로 획득하였으며 업계 최고 수준의 보안 시스템을 갖추게 되었다(인더스트리뉴스, 2024). 이러한 성과의 배경에는 최고경영진의 강력한 전략적 의지와 실행력이 자리잡고 있다. 태림산업의 최고경영진은 TISAX 인증을 글로벌 자동차 공급망 내 신뢰 확보와 장기적 경쟁력 유지의 전략적 수단으로 인식하고, 정보보안이 기업의 미래 성장과 직결된다는 점을 강조하며 전사적인 정보보안 체계 구축을 주도하였다. 이를 위해 정보보안 전담팀을 신설하고, 외부 컨설팅 업체와 협업하여 단계별 준비를 수행했으며, IT 인프라와 시스템을 개선하였다. 특히 정보보안 강화 없이는 글로벌 시장에서 경쟁력을 유지하기 어렵다는 위기의식을 공유하고 정보보안 강화를 주요 전략으로 확립하였다.

이와 같은 사례는 정보보안 전담 조직의 역량이 제한적인 중소기업에서도, 최고경영진의 전략적 판단과 실행이 TISAX 인증 성공의 핵심 요인이 될 수 있음을 보여준다. Calder and Watkins(2008)는 자원이 제한된 조직일수록 정보보안 전략이 경영진의 판단과 리더십에 크게 의존한다고 보았다. 실제로 태림산업은 정보보안을 디지털 전환의 일환으로 접근하였으며, 최고경영진은 이를 미래를 준비하는 위기 대응 수단으로 정보보안을 전략화하였다. 외부 컨설팅 업체와 내부 정보보안 전담팀 간 협업을 주도한 점 역시, 경쟁자와의 협업을 강조하는 최고경영진의 개방형 혁신 철학과 맞닿아 있다. 결과적으로 정보보안 목표를 경영 전략의 핵심 우선순위로 격상시키고, 조직 내외 자원을 효과적으로 조율함으로써 실질적 거버넌스를 구현하였다.

<표 3> 주체 측면 비교: 현대모비스와 태림산업

구분	현대모비스	태림산업
전략 주도	- 정보보안 전담조직 및 전문가 중심 전략 수립 - **AHP 종합중요도 1위 (0.1472)**	- 최고경영진(CEO) 주도 전략 수립 - **AHP 종합중요도 2위 (0.1234)**
조직 운영	- 글로벌 통합 보안 체계 구축 - 전문 보안 부서 간 협력 체계 운영	- 정보보안 전담팀 신설 - 외부 컨설팅 업체와의 전략적 협업
의사 결정	- 분화된 정보보안 조직 기반의 실행 체계	- 단일 의사결정 구조 - 최고경영진 직접 실행 주도
보안 문화 정착	- 전사적 CSMS 운영 - 규제 대응 체계 내재화	- 실무 교육 및 감사 체계를 통한 인식 제고
정보보안 거버넌스	- 역할의 명확화 및 중앙 통제 구조 구현 사례 (ISO/IEC 27104)	- 자원 제약 조직의 리더십 기반 전략 실행 사례 (Calder and Watkins, 2008)

<표 3>에서 보듯이, 현대모비스는 조직 기반의 구조화된 정보보안 전략을, 태림산업은 최고경영진 중심의 직접적 실행 전략을 각각 전개하였다. 이는 기업의 규모, 조직 구조, 의사결정 방식의 차이에 따른 것으로, 두 사례 모두 정보보안 전략 수립과 실행에서 주체 요인의 중요성이 핵심적으로 작용하였으며, 이는 이후 단계의 전략 전개와 성과에 결정적인 영향을 미쳤다.

2. 환경 측면

TISAX는 2017년 독일자동차산업협회(VDA)의 주도로 개발된 이후, 글로벌 자동차 공급망의 정보보안 표준으로 빠르게 확산되었다. 초기에는 Volkswagen을 중심으로 확산이 이루어졌으며, 2020년부터는 BMW, Mercedes-Benz, Bosch, ZF 등 독일 주요 완성차 및 부품 기업들이 하위 공급망 협력업체를 대상으로 TISAX 인증을 필수 요건으로 요구하면서 제도적 전환이 본격화되었다. 이후 2023년부터는 Stellantis, Renault 등의 OEM들도 이를 채택하며 글로벌 표준화가 가속되었다. ENX 보고서에 따르면 2024년 2분기 기준, 전 세계 10,000개 이상 기업이 TISAX 인증을 완료하였으며, 그 중 58%가 독일 외 지역에 위치하고 있다. TISAX는 단순한 보안 평가를 넘어, 글로벌 자동차 공급망 진입의 필수 조건으로 작용하고 있다(Raković, 2024). 이에 따라 자동차 부품 협력업체들은 기술적·조직적 대응을 넘어서, 외부 환경 변화에 대한 선제적, 전략적인 대응이 요구된다. 이러한 환경 변화는 정보보안 수준을 기업 생존과 직결되는 요소로 전환시키고 있으며, 이와 같은 상황 속에서 각기 다른 대응 전략을 전개한 대표적 사례로 현대모비스의 선제 대응 모델과 태림산업의 고객 수요 기반 적응 모델이 주목된다.

가. 글로벌 보안 규제 및 선제적 대응: 현대모비스 사례

현대모비스는 해외 매출 비중이 50%를 초과하는 사업 구조상, 유럽 OEM의 정보보안 요구사항을 조기에 인식하고 전략적 대응을 실행하였다. 2019년 이전부터 VDA 및 Volkswagen의 TISAX 인증 확산 움직임을 사전 모니터링하며, 2020년부터 인증 획득을 위한 내부 준비를 본격화하였다. 그 결과, 2021년에는 국내 자동차 부품업계 중 선도적으로 TISAX 인증을 획득하였다.

한편, 2022년 유엔 유럽경제위원회(UNECE) 산하 WP.29(World Forum for Harmonization of Vehicle Regulations)는 자동차 OEM을 대상으로 하는 사이버보안 국제 규정(UNR No. 155, CSMS)을 채택하였으며, 해당 규정은 2022년부터 유럽 시장 내 신차에 의무 적용되었다(최원석, 2020). 이는 완성차 제조사를 대상으로 한 규제로, 모듈·부품 공급사에 대한 직접 적용은 포함되지 않지만, 공급망 전반에 걸친 간접적 규제 대응이 요구되는 환경으로 전환되었다. 이에 현대모비스는 내부 대응 조직을 중심으로 CSMS(자동차 사이버보안 관리 시스템) 고도화 작업을 본격화하고, 글로벌 거점 간 보안 정책 통합 및 조직 정비를 추진하였다. 특히 2024년에는 유럽 자동차 제조·공급협회(ENX)로부터 아시아 부품업계 최초로 차량 사이버보안 인증인 VCS(Vehicle Cyber Security)를 획득하였다(연합뉴스, 2024). 이 인증은 법적 의무가 아닌 고객사 요구에 따른 자발적 대응이으로, 기존의 TISAX 인증 수준을 넘어서는 보안 역량이 요구된다. 따라서 현대모비스는 외부 규제 환경과 고객 요구에 대해 단기적 대응을 넘어 전략적 경쟁우위로 전환하려는 선도형 사례로 평가할 수 있다.

나. 공급망 내 고객사 요구 수용 및 전략화: 태림산업 사례

태림산업은 급변하는 외부 환경과 보안 요구의 강화 속에서도 전략적으로 대응한 중소기업의 대표적인 사례이다. 글로벌 공급망에서 정보보안 기준이 강화되면서, Bosch, ZF 그룹 등 독일계 1차 협력사는 공급망에 참여하는 국내 중소 부품 협력사들에게도 TISAX 인증을 요구하였다. 특히 ZF는 공식 서신을 통해 TISAX 인증을 향후 소싱의 필수 요건으로 명시하면서, 중소 부품기업에게 상당한 외부 압력과 환경

적 변화를 마주하게 되었다. 이와 같은 요구는 높은 진입 장벽으로 작용하였으며, 실제 다수 기업이 시간과 비용 부담을 이유로 대응을 유보하거나 회피하는 경향을 보였다. 기존 연구에서도 중소기업은 자금, 인력, 전문성 등의 제약뿐 아니라, 외부 환경 변화에 취약하다는 한계가 꾸준히 제기되어 왔다(문현정, 2009). 그러나 태림산업은 이와 같은 환경적 압력을 수동적으로 수용하지 않고, 전략적 전환의 계기로 인식하였다. 생산공정 전반에 디지털 전환 및 보안 고도화의 흐름을 접목시켜 기업 전략과 연계하고, 내부 개선과 외부 협업을 병행하며, 보안 수준을 단계적으로 높여 나갔다. 이러한 노력은 일회적인 인증 획득을 넘어, 외부 환경을 새로운 성장 기회로 전환하고자 한 실질적 적응 전략으로 해석된다.

이는 보안 역량과 기술 자산을 조직 내부에 내재화하는 구조적 토대가 되었고, 이러한 다각적 노력을 통해 2023년 말 TISAX 인증을 성공적으로 획득하였다. 이는 국내 중소기업이 보안이 취약하다는 이미지를 벗어나 환경의 변화에 적극적으로 핵심 역량을 내재화한 사례로 평가되며, 환경적 요인을 제약이 아닌 성장 기회로 전환하는 접근의 필요성을 시사한다.

<표 4> 환경 측면 비교: 현대모비스와 태림산업

구분	현대모비스	태림산업
주요 대응 동기	- EU 규제 및 글로벌 OEM 보안 요구 강화	- 1차 협력사 ZF그룹의 소싱 필수 요구
TISAX 인식 및 인증 시점	- 2019년, 독일 OEM 규제 사전 인지 - 2021년, 국내 기업중 선도적 대응 및 인증 획득	- 2020년, ZF그룹 공식 서신 수신 - 2023년, 경남지역 중소기업 중 최초 인증 획득
CSMS 인식 및 인증 시점	- 2020년, UN R155등 글로벌 규제 가시화에 따라 선제 대응 및 CSMS 조기 고도화 → 2024년 아시아 초 VCS인증 획득	- 미준비 (아직은 고객사 수요 없음)
환경 대응 전략	- 보안 규제를 성장 기회로 내재화	- 외부 압력을 전략 전환 계기로 활용

<표 4>는 두 기업이 동일한 외부 환경 변화에 대해 어떻게 상이한 전략을 선택했는지를 보여준다. 환경요인은 전략의 수립과 실행에서 구조적 차이를 발생시키며, 어떻게 인식하고 설계하느냐에 따라 대응 방향과 성과가 달라질 수 있다. 지신명, 신호상(2025)은 환경 요인이 기술적·조직적 요인에 비해 상대적 중요도는 낮게 평가될 수 있지만, 외부 요구와 자원의 연결을 유도하는 핵심 배경 변수로 작동할 수 있다고 분석하였다. 따라서 환경적 요구를 전략적으로 수용하고 이를 내부 체계에 반영하는 기업일수록, TISAX 인증 대응에서 보다 구조화된 경쟁우위를 확보할 가능성이 높은 것으로 해석된다.

3. 자원 측면

자원(Resource)은 기업이 보유한 정보보안 인프라, 기술력, 인적 역량 등을 포함하는 요소이다. 기존 연구에 따르면, 조직적 요인에 이어 자원 측면이라고 볼 수 있는 기술적 요인이 인증 성공에 높은 중요도를 가지며, 특히 데이터 보호체계, 보안 솔루션, 전문 인력의 확보와 같은 자원의 전략적 배분이 핵심 요건으로 작용한다(지신명, 신호상, 2025). 이는 SER-M 모델의 자원 요소가 인증 대응의 실행력을 뒷받침하는 주요 기반으로 작동함을 시사한다.

TISAX 인증 기준은 문서 요건을 넘어, 정보보안 시스템의 실질적 안정성과 기술 기반 역량을 요구한다. 특히 정보보안의 핵심 3요소인 데이터의 가용성(Availability), 기밀성(Confidentiality), 무결성(Integrity) 확보와 같은 핵심 기술 요소들이 충족되어야 한다(서형준, 2021). 정보보안 인프라가 미흡할 경우 보완 권고나 인증 지연으로 이어질 수 있고, 이는 공급망 신뢰도에 직접적인 영향을 미친다. 또한,

기술적 요건을 효과적으로 운영하고 감독할 수 있는 정보보안 인력과 교육 체계의 확보 역시 필수적이다. 기업의 자원 대응 전략은 조직의 규모와 내부 역량에 따라 상이한 양상을 보인다. 대기업은 다양한 조직 단위와 글로벌 인프라를 활용한 체계적 자원 통합 전략을 구사하는 반면, 중소기업은 제한된 자원을 외부 컨설팅 업체의 전문역량과 내부 자원의 탄력적 활용을 통해 극복하는 방식이 일반적이다.

가. 통합 인프라 기반의 전략적 운영: 현대모비스 사례

현대모비스는 정보보안 인프라 구축을 위해 구조화된 전사적 투자와 대응 전략을 수립하였다. 먼저 정보보안팀, IT 운영팀, 사이버보안팀 간의 역할을 명확히 분리하고 각 팀의 전문성을 강화함으로써, 기능 분화 기반의 자원 운영 체계를 구축하였다. 이러한 체계는 각 팀이 명확한 책임과 권한을 가지고 유기적으로 협력하여 보안 사고 대응의 신속성과 효율성을 높이는 데 기여하였다. 기술적 측면에서는 클라우드 기반 보안 솔루션, AI 기반 보안 모니터링 시스템, 침입 탐지 및 대응 시스템(IDPS) 등 첨단 기술을 통합적으로 도입하여 실질적 보안 역량을 확보하였다. 특히, AI 기반 시스템은 실시간으로 이상 징후를 탐지하고, 잠재적 위협을 사전에 차단하는 데 중요한 역할을 하였다. 이러한 기술적 투자는 단순히 현재의 보안 요구를 충족하는 데 그치지 않고, 미래 사이버 위협에 대한 확장성과 유연성을 제공하였다. 기술 자원 외에도 운영 차원에서의 통합이 특징적이다. 현대모비스는 본사와 해외 생산 법인 간 보안 정책, 기술, 인력을 연계하는 체계를 구축하였다. 이를 통해 자원의 일관된 배분과 관리가 가능해졌으며 단발적 인증 획득에 그치지 않고, 인증 이후에도 보안 수준을 지속적으로 고도화할 수 있는 기반으로 작용하였다. 그 결과, TISAX와 VCS 인증 이후에도 통합된 보안 자원 운영체계를 바탕으로 지속적인 역량 고도화를 추진하고 있으며, 글로벌 정보보안 역량을 선도하는 입지를 공고히 하고 있다.

나. 제한 자원 하의 유연한 활용 전략: 태림산업 사례

태림산업은 정보보안 전담 조직이 없던 초기 조건에서도 제한된 자원을 전략적으로 활용하여 TISAX 인증을 성공적으로 획득한 사례이다. 인증 준비 과정에서 정보보안 전담팀을 신설하고, 외부 컨설팅 업체를 선정하여 자문을 받았으며, IT 시스템을 단계적으로 점검하고 보완함으로써 필요한 자원을 시기별로 확보하고 구축해 나갔다. 대규모 보안 인프라를 구축하기 어려운 조건을 고려하여, 클라우드 보안 솔루션 도입과 핵심 인력 맞춤형 보안 교육을 통해 정보보안 역량 확보와 내부 보안 문화 정착을 동시에 추진하였다. 특히 주목할 만한 점은, 보안 역량 확보와 동시에 제조업의 디지털 전환 흐름을 선도하고자 본사 내에 MDCG(Manufacturing Data Community Ground)라는 개방형 혁신 플랫폼을 구축한 것이다. 기존 노후 공장을 업사이클링하여 스마트팩토리 공간으로 전환하고, 실증 기반 테스트베드로 활용함으로써 정보보안 관련 시스템을 실험·검증하고, 보안 요구사항을 실제 운영에 반영할 수 있는 기반을 마련하였다(이영주, 2023).

MDCG는 AI 기반 공정 모니터링, 디지털 트윈 기술, 스마트 물류 시스템 등 첨단 디지털 기술을 생산 현장에 접목·검증할 수 있는 실험 공간으로, 외부 기술 파트너와의 협업을 촉진하는 전략 거점으로 기능하였다. 이는 기술을 보유함과 동시에 제한된 자원을 외부 컨설팅 업체의 전문 역량과 연계하여 보안 역량으로 전환한 내재화된 실행 방식으로 해석할 수 있다. 이처럼 외부 역량을 내부 전략에 통합하는 방식은 자원 제약 속에서도 글로벌 보안 인증을 달성할 수 있는 중소기업의 실질적 전략 대안을 제시한다.

<표 5> 자원 측면 비교: 현대모비스 vs. 태림산업

구분	현대모비스	태림산업
자원 운영 구조	- 정보보안, IT운영, 사이버보안팀 팀분리 및 역할 기반 통합	- 정보보안팀 신설 및 외부 전문가 협업 기반 유연한 자원
기술 자원 활용	- 클라우드, AI기반, 보안 모니터링, IDPS등 첨단 시스템 전사적 적용	- 클라우드 기반 보안 솔루션, 단계적 시스템 점검
보안 인력 및 교육	- 정규 조직 내 전문 인력 확보 및 법규 기반 정기 교육	- 맞춤형 교육, 외부 컨설팅 업체와 협업을 통한 실무역량 확보
정책 실행력	- CSMS 기반 정책 일원화, 본사·법인 연계 강화	- MCDG 중심 디지털 기술 실증, 실행 모니터링
전략적 특징	- 전사 인프라 고도화를 통한 장기적 경쟁력 확보	- 외부 자원 연계 통한 내부 보안 전력 내재화

<표 5>은 두 기업의 자원 측면의 조건과 대응 전략을 비교한 것으로, 현대모비스는 체계적 인프라 구축과 전문 인력 운영을 통해 글로벌 수준의 정보보안 역량을 확보한 반면, 태림산업은 외부 전문성 활용과 내부 인력 조정 등 유연한 전략으로 제한된 자원을 극복하고 인증을 성공적으로 이행한 모범사례이다.

4. 메커니즘 측면

메커니즘은 주체, 환경, 자원이 상호작용하여 조직이 외부 변화에 대응하고 자원을 결합하여 전략적 목적을 달성하도록 유도하는 작동 원리이다. 이러한 메커니즘의 기능은 내용 차원의 조정(Coordinating), 과정 차원의 학습(Learning), 그리고 시간 차원인 선택(Selecting)의 세 가지로 구분할 수 있다.

주체가 환경에 대응하며 자원을 활용하는 과정에서 메커니즘이 형성되고, 이는 시간이 지남에 따라 경험과 지식에 의해 진화하며, 환경에 의해 선택된다. 이에 따라 동일한 출발점에 있는 기업이라 하더라도, 학습과 선택의 차이에 따라 시간이 지날수록 점차 차별화되는 양상을 보인다(조동성, 2014).

정보보안 체계 역시 이러한 메커니즘에 기반한 전략 형성 과정으로 해석될 수 있다. 정보보안은 기술 중심 대응을 넘어 주체, 환경, 자원이 상호작용하며 보안 역량 강화와 경영성과 창출로 이어지는 경로를 형성하지만 동일한 인증 목표를 향한 실행 과정에서도 세 요소가 작동 순서와 방식에 따라 정보보안 체계 구축의 방식과 메커니즘의 특성 및 전개 양상이 다르게 나타남을 확인하였다. 이러한 메커니즘적 접근은 정보보안 전략이 자원 배분이나 정책 이행을 넘어, 동태적 상호작용을 통해 구체화되는 전략 형성 과정임을 보여준다. 특히, 기업이 어떤 메커니즘을 중심으로 전략을 수립하느냐에 따라 정보보안 성과와 경쟁력 확보 여부가 결정된다.

<표 6> TISAX 인증 기업의 요인별 정보보안 메커니즘 분석

SER-M 요인	현대모비스 (대기업 모범사례)	태림산업 (중소기업 모범사례)
주체 요인	- 정보보안 전담 부서의 강력한 운영 - 전사적 보안 정책 추진	- 최고경영진의 강력한 리더십 - CEO의 직접적 정보보안 투자 결정
환경 요인	- EU 규제 및 글로벌 OEM 보안 요구 강화 - 글로벌 보안 규제에 선제 대응	- 1차 협력사 ZF그룹의 소싱 필수 요구 - TISAX인증 요구를 전략 전환의 기회로 해석
자원 요인	- 보안 전문 인력 운영 및 강력한 인프라 구축 - 본사 및 해외법인 간 정보보안 통합 운영	- 보안 전담팀 신설, 교육 통한 보안 역량 강화 - IT 시스템 개선, 외부 컨설팅 업체 적극 활용
조정	- 글로벌 보안 정책 일관된 적용	- 유연한 자원 배분과 현장 중심 실행

메커니즘	- 각 법인의 보안 정책 조정 및 통합	- 중소기업 내 자원 분배 최적화
학습 메커니즘	- 보안 기술 학습 및 정기 업데이트 - 유럽 보안 법규 반영 체계화	- 전사 교육, 내부 감사 정례화 - 보안 문화 내재화
선택 메커니즘	- 글로벌 정보보안 환경 요구를 전략 지표로 연계 - 전사적 보안 관리 체계 내제화	- 정보보안을 경영 전략적 성과 지표로 설정 - 인증 확보를 기업 신뢰 자산으로 인식
메커니즘 유형	E-S-R (자원혁신형)	S-R-E (자원창조형)

<표 6>은 두 사례 기업의 주체, 환경, 자원 요인과 함께 조정, 학습, 선택이라는 메커니즘 기능이 어떻게 작동하였는지를 비교한 것이다. 정보보안 체계구축은 이러한 기능을 통해 구체화되며, 이는 조직의 전략 방향, 실행 방식, 자원 활용 방식 전반에 영향을 미친다는 점을 확인할 수 있다.

현대모비스는 대기업으로서 강력한 정보보안 전담 조직과 통합된 글로벌 운영 체계를 기반으로, 유럽 OEM의 보안 요구에 선제적으로 대응하였다. 본사와 해외 법인 간 보안 정책을 일관되게 조정함으로써 글로벌 통합 운영 체계를 형성하였고(조정), 관련 법규와 기술에 대한 지속적인 교육과 업데이트를 통해 조직 전반에 내재화하였다(학습). 또한 정보보안을 경영 전략의 핵심 성과지표로 설정하고, 글로벌 고객 요구에 대응하는 체계적 전략을 선택적으로 실행하였다(선택). 반면 태림산업은 자원 제약 속에서도 최고경영진의 리더십을 중심으로 자원을 유연하게 배분하고 외부 컨설팅 업체와의 협업을 통해 실행 체계를 마련하였으며(조정), 실무 중심의 보안 교육 및 내부 감사 체계를 통해 보안 인식을 제고하고 이를 조직 문화로 정착시켰다(학습). 아울러 최고경영자의 판단에 따라 TISAX 인증을 신뢰 자산으로 전환하고, 이를 통해 중소기업으로서의 경쟁력을 강화하는 전략적 선택을 실행하였다(선택).

여기에 SER-M 모델의 순열에 의한 6가지 경영 메커니즘 유형 중 현대모비스와 태림산업에 해당되는 메커니즘을 검토하였다, 경영자가 주체, 환경, 자원이 이미 주어진 상황에서 선택할 수 있는 전략적 행동은 이들의 배열 방식, 즉 순열에 달려 있으며(조동성, 문휘창, 2022). 이는 동일한 요소를 가지고도 보안 전략이 전혀 다른 방향으로 전개될 수 있음을 보여준다.

현대모비스는 외부 환경(E)에 대한 전략적 인식을 통해 주체(S)가 조직적 실행을 하였고 기술 및 자원(R) 강화를 통하여 고도의 정보보안 체계를 확립하였다. 이는 새롭게 주어진 환경에 따라 주체가 적극적으로 자원을 혁신하는 자원 혁신형(E-S-R) 메커니즘으로 환경이 선도 역할을 한다는 점에서 주체가 수동적으로 보일 수 있지만 환경 범주 내 주체가 적극적으로 새로운 자원을 창출하는 혁신적 모델이다.

태림산업은 최고경영진의 리더십과 의사결정을 중심으로 정보보안 전략을 전개하였다. 최고경영진인 주체(S)의 판단에 따라 필요한 보안 자원(R)을 능동적으로 확보한 후, 외부 환경(E)에 적극적으로 대응하는 방식으로 발전하여 나감으로써 자원 창조(S-R-E)형 메커니즘을 적용하였다. 이처럼 두 기업은 동일한 TISAX 인증이라는 목표를 지향했음에도 불구하고, 전략 전개 순서와 중심축에서 명확한 차이를 차이를 보였으며, SER-M 모델은 이러한 차이를 구조적, 시간적 관점에서 설명하는 유효한 틀로 작용하였다. 이를 통해 기업의 정보보안 전략은 주체, 환경, 자원이 병렬적으로 존재하는 것이 아니라, 동태적으로 상호작용하고 순차적으로 구성되는 메커니즘 기반 전략적 전개 과정임이 실증적으로 입증되었다.

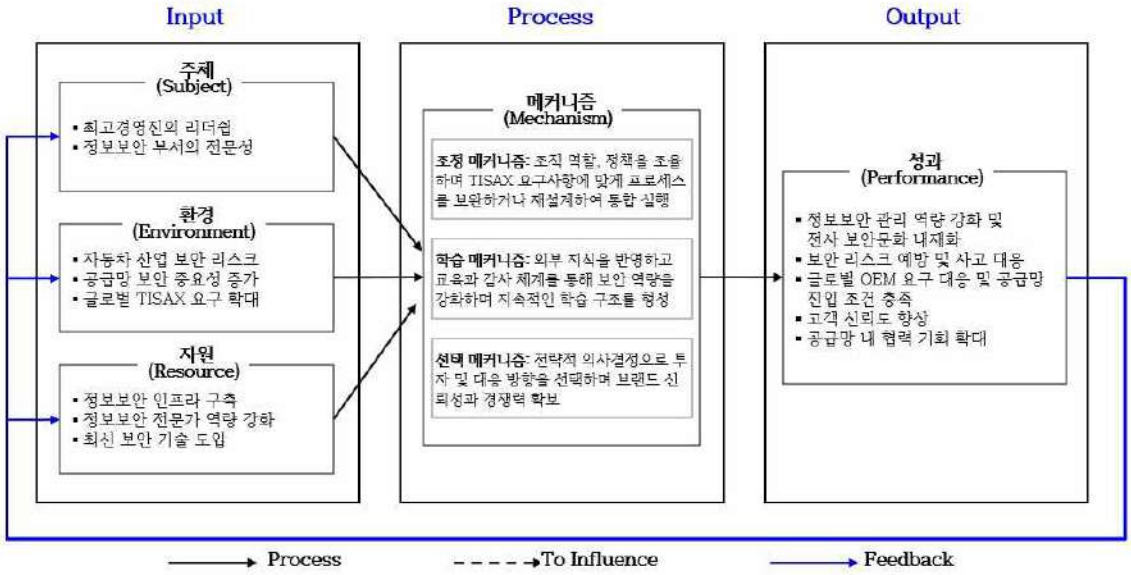
5. 분석 결과

앞선 분석 결과를 종합하면, SER-M 모델은 정보보안 전략을 해석하는 효과적인 분석 틀로 기능한다. TISAX 인증은 정보보안 요구사항을 충족하는 데 그치지 않고, 기업 내부의 주체, 환경, 자원이 상호작용하여 전략을 형성하고 실행하는 복합적 메커니즘 구축 과정으로 볼 수 있다. 이와 같은 복잡한 전략 전개 과정을 구조적으로 해석하는데 SER-M 모델은 매우 유용한 분석 도구가 된다. SER-M 모델은 주

체, 환경, 자원을 각각의 구성 요소로 나열하는 것이 아니라, 이들이 상호 작용을 통해 메커니즘을 형성하고, 전략 실행의 조정, 학습, 선택 과정을 통해 성과로 이어지는 Input-Process-Output의 논리로 설명할 수 있다.

[그림 3]은 이러한 논리를 시각화한 도식으로, 첫째, 좌측의 Input 단계에서는 전략 형성에 영향을 미치는 세 가지 구성요소를 포함한다. 주체는 최고경영진의 리더십과 정보보안 부서의 전문성을 의미하며, 환경은 자동차 산업의 보안 리스크, 글로벌 규제 및 고객 요구와 같은 외부 압력으로 구성된다. 자원은 정보보안 인프라, 전문 인력, 최신 보안 기술 등 조직 내부의 유·무형 자산을 포괄한다. 둘째, 가운데 Process 영역은 세 요인이 상호작용하며 형성하는 조정, 학습, 선택 메커니즘으로 구성된다. 여기서 조정 메커니즘은 정책과 실행의 일관성을 확보하는 과정, 학습 메커니즘은 외부 규제 및 기술 변화를 조직에 흡수하는 과정, 선택 메커니즘은 전략적 의사결정을 통해 보안 투자와 대응 방향을 설정하는 기능을 의미한다. 셋째, Output 단계는 이러한 메커니즘을 통해 도출되는 성과로, 정보보안 역량 강화, 외부 인증 대응력, 고객 신뢰 확보, 공급망 내 협력기회 확대 등을 포함한다. 특히 성과는 단발적인 결과에 그치지 않고, 다시 주체·자원·환경에 피드백되어 전략의 반복과 고도화로 이어지는 선순환 구조를 형성한다. 실제로 현대모비스는 TISAX 인증(2021년)과 VCS 인증(2024년)을 통해 글로벌 고객 신뢰도와 공급망 내 리더십을 확보하였으며, 태림산업은 중소기업으로서 TISAX 인증(2023년)을 획득하며 유럽 OEM과의 안정적 사업 기반을 마련하였다. 동일한 인증 목표를 갖더라도 주체, 환경, 자원의 해석과 배치 순서에 따라 전략 방식은 달라질 수 있으며, 이는 메커니즘의 조합 방식과 실행 결과에 직접적인 영향을 미친다.

[그림 3] SER-M 관점에서 본 TISAX 인증과 자동차 정보보안 경쟁력 강화



V. 결론

본 연구는 SER-M 모델을 적용하여 자동차 산업에서 TISAX 인증 사례를 중심으로 정보보안 전략이 어

떠한 메커니즘을 통해 형성되며, 이것이 기업의 경영성과와 어떻게 연계되는지를 분석하였다. SER-M 모델은 주체, 환경, 자원이라는 세 가지 요소의 상호작용을 통해 메커니즘이 형성되고, 이를 바탕으로 전략 실행 및 성과 창출이 이루어진다는 점에서 효과적인 이론적 틀로 가능함을 확인하였다.

사례 분석 결과, 현대모비스는 외부 환경(E)을 전략의 출발점으로 삼고, 이에 대응하는 조직의 주체(S)가 내부 자원(R)을 결합하여 혁신하는 자원 혁신형(E-S-R) 메커니즘을 따랐으며, 태림산업은 최고경영진의 리더십을 중심으로 필요한 자원(R)을 적시에 창출하고 환경(E)에 대응하는 자원 창조형(S-R-E) 메커니즘을 전개하였다. 이와 같은 차이는 조직 규모, 의사결정 구조, 리더십 형태 등 기업의 내부 특성에 따라 정보보안 전략의 구조와 실행 방식이 달라질 수 있음을 보여준다.

학문적 시사점으로는, 본 연구가 SER-M 모델을 정보보안 전략 분석에 적용함으로써, 기술적·정책적 대응에 국한되었던 기존 연구의 한계를 넘어 전략 메커니즘의 형성과 실행 과정을 동태적이고 구조적으로 설명할 수 있음을 실증적으로 제시하였다는 데 의의가 있다.

실무적 시사점으로는, 정보보안 전략의 효과적 실행을 위해 제도 도입을 넘어, 기업의 조직 구조와 외부 환경에 적합한 전략 메커니즘을 설계해야 한다는 점이 확인되었다. 대기업은 외부 환경 변화에 대한 보안 전담 조직을 통한 자원의 통합적 조정이 전략 실행력과 장기적 경쟁력 확보에 핵심 역할을 하며, 중소기업은 최고경영진의 리더십을 바탕으로 자원을 선제적으로 확보하고 이를 유연하게 실행하는 전략이 정보보안 강화를 위한 현실적인 해법임이 드러났다. SER-M 모델은 다양한 기업 특성에 따라 정보보안 전략이 어떻게 구분되고 구조화되는지를 설명할 수 있는 이론적 유용성을 지니며, 복합 산업 환경에서도 적용 가능한 분석 틀로서의 확장성을 보여주었다.

한계와 향후 과제로는, 본 연구가 사례 중심의 정성적 분석에 기반하였기 때문에 일반화에는 제약이 따른다는 점이 있다. 향후 연구에서는 금융, 의료, 에너지 등 다양한 산업 분야에서 정보보안 인증이 기업의 경영성과에 미치는 영향을 실증적으로 분석함으로써 SER-M 모델의 적용 가능성과 범용성을 더욱 확대할 필요가 있다. 또한, TISAX 인증 도입 전후의 재무성과, 고객 신뢰도, 공급망 안정성 등 구체적인 정량 지표를 포함한 후속 연구를 통해 분석의 정밀도를 높이는 것도 중요하다. 본 연구가 인증 과정의 메커니즘 형성에 초점을 맞추었다면, 향후 연구에서는 인증 이후 지속적인 정보보안 강화와 조직 학습이 장기적 성과에 미치는 영향을 심층적으로 탐구할 필요가 있다. SER-M 모델을 활용한 본 연구는 TISAX 인증이 단순한 규제 대응을 넘어, 자동차 산업 내 정보보안 경쟁력 강화와 경영성과 창출에 전략적으로 기여할 수 있음을 구조적으로 설명하였다. 이는 향후 정보보안 전략의 이론적 설계뿐만 아니라 실무적 실행 양 측면에서 모두 의미 있는 시사점을 제공할 수 있을 것으로 기대된다.

참고문헌

구자원, 신철호, 이동환. 2009.「기업 성장단계별 IT기업의 경영성과 결정요인에 관한 실증연구」.『상업경영연구』. 23(4): 413-438.

구자원, 신철호, 이동환. 2012.「메커니즘 요인 매개효과 검증을 위한 탐색적 연구」.『산업교육연구』. 26(4): 355-375.

김동원, 한근희, 전인석, 최진영. 2015.「자동차 공급망 위험관리(A-SCRM) 방안 연구」.『정보보호학회논문지』, 25(4), 793-805.

김지훈, 조규선, 엄재근. 2023.「ser-M 기반 안전보건경영시스템 메커니즘의 탐색적 연구 -안전보건경영시스템 구축 사례를 중심으로-」.『경영컨설팅연구』. 23(4): 207-216.

김태종, 엄재근. 2020.「ser-M 기반 프리미엄 가전 시장의 경영 전략 메커니즘에 관한 연구: LG 전자 사례를 중심으로」.『경영교육연구』. 35(6): 509-531.
문현정. 2009.「우리나라 중소기업의 정보 보호 역량 강화를 위한 교육 훈련 현황과 문제점」.『정보보호학회지』, 19(1): 2939. 한국정보보호학회.
박재영, 정우진. 2019.「기업의 정보보호 공시가 기업가치에 미치는 영향」.『지식경영연구』. 20(4): 39-55.
배영식. 2012.「정보보호 관리체계(ISMS) 인증이 조직 성과에 미치는 영향에 관한 연구」.『한국산학기술학회논문지』. 13(9): 4224-4233.
서형준. 2021.「공공부문 정보보안 행태에 미치는 영향요인: 정보보안의식의 매개효과를 중심으로」.『한국행정연구』, 30(2): 173207. 한국행정연구원.
신현민, 김인재. 2020.「정보보호 전문서비스 기업의 인증 및 상장 여부가 재무적 성과에 미치는 영향」.『지식경영연구』. 21(3): 197-213.
엄재근, 조규연, 탁진규. 2017.「ser-M 모형 분석을 이용한 기업가 정신에 관한 연구: 국내 9개 기업의 창업주 사례를 중심으로」.『한국경영교육학회』. 32(6): 431-451.
연합뉴스. 2024.「현대모비스, 유럽 車협회 사이버보안 인증 획득…아시아 최초」. https://www.yna.co.kr/view/AKR20240926065100003 (검색일: 2025년 4월 2일)
유정범, 박재홍, 이동근, 박기찬. 2021.「IT 기술력으로 대한민국을 연결하다: 메쉬코리아의 성공 메커니즘 분석」.『한국경영학회』. 25(신년 특별호): 139-154.
이영주. 2023.「디지털 전환시대 중소제조기업 경쟁력 강화를 위한 스마트팩토리 공간구성 연구: 전기 및 전자부품 제조업 태림산업(주)을 중심으로」.『한국공간디자인학회논문집』, 18(5): 299-310. 한국공간디자인학회.
이용수, 임효숙. 2024.「인슈어테크를 활용한 전통적 보험회사의 혁신 전략 : 라이나생명 사례를 중심으로」.『지능정보연구』. 30(2): 287-312.
이희수, 고영희. 2022.「직업훈련 전문기업 ㈜지아이티아카데미의 환경대응 전략 메커니즘에 관한 연구」.『한국경영학회』. 26(2): 23-59.
이형진, 하수경. 2024.「ser-M 모델 기반 글로벌 K-푸드 브랜드 확장 전략에 관한 연구:비비고 사례를 중심으로」.『브랜드디자인학연구』. 22(2): 19-28.
인더스트리뉴스. 2024.「태림산업, 경남 소재 중소기업 최초 'TISAX' 레이블 획득」. https://www.industrynews.co.kr/news/articleView.html?idxno=52552 (검색일: 2025년 2월 25일)
조동성. 2014. 메커니즘기반관점: 통합적 경영을 위한 새로운 전략 패러다임. 서울경제경영.
조동성, 문휘창. 2022. AI시대의 경영전략: 전략의 고수가 되는 비법. 서울경제경영.
저우위보, 조동성. 2023.「삼성 휴대폰의 중국시장 진출-성장-침체 사례를 통해 본 한국기업 중국 진출의 성공 방정식과 향후 재도약을 위한 제언: 메커니즘기반관점을 중심으로」.『한국경영학회 융합학술대회』. 61-104.
정지훈, 고영희. 2023.「국내 바이오제약 기업 성장 프로세스와 코로나-19 기회활용 전략: 셀트리온과 삼성바이오로직스 전략 메커니즘 비교분석」.『Korea Business Review』. 27(1): 27-52.
지신명, 신호상. 2024.「시스템 사고를 활용한 자동차 산업 정보보안 인증과 기업 성과 영향 분석: TISAX 인증을 중심으로」.『한국시스템다이내믹스 연구』. 25(3): 35-59.
지신명, 신호상. 2025.「AHP기법을 활용한 자동차 산업 정보보안 강화 요인 분석: TISAX 인증을 중심으로」.『정보보호학회논문지』. 35(2): 425-440.

현대모비스. 2024. 현대모비스 2024년 4분기 경영실적. https://www.mobis.com/kr/ir/irdisclosure.do#irdisclosure03 (검색일: 2025년 4월 20일)
최원석. 2020.「국제 학술대회를 중심으로 자동차 보안 기술 동향」.『정보보호학회지』, 30(6): 91~99. 한국정보보호학회
Alharbi, A., and D. Gregg. 2022, “The impact of IT investment and IT security intensity on firm performance.” In Proceedings of the 2022 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop, 1-21. Denver, Colorado, USA.
Barney, J. 1991, “Firm resources and sustained competitive advantage”. Journal of Management, 17(1): 99-120.
Calder, A. and S. Watkins. 2008, “IT Governance: A Manager's Guide to Data Security and ISO 27001/ISO 27002”. Kogan Page Ltd.
ENX Association. 2024. TISAX Participant Handbook: Version 2.7.2.
ISO/IEC. 2020. ISO/IEC 27014:2020, Information Security, Cybersecurity and Privacy Protection — Governance of Information Security. Edition 2.
Raković, R. M. 2024, “Information security in automotive industry: Mechanism TISAX”. Tehnika, 79(3): 361-367.
Upstream Security Ltd. 2025. Automotive & Smart Mobility Global Cybersecurity Report.

Abstract

A Study on Information Security Mechanism in the Automotive Industry Using the SER SER-M Model

Focusing on Successful Cases of TISAX Assessment

Shin Meung Chi Ho-Sang Shin

As the digital transformation of the automotive industry accelerates, information security threats are increasing, highlighting the growing importance of TISAX(Trusted Information Security Assessment Exchange) within the global supply chain. This study utilizes the SER-M model to analyze how TISAX assessments influence the development of corporate information security systems and overall business performance. The findings reveal that distinct strategic mechanisms emerge through the dynamic interaction of subjects, environments, and resources during the TISAX assessment process. These mechanisms play a critical role in enhancing firms' security capabilities while contributing to sustainable competitive advantage. In particular, companies that successfully completed the TISAX assessment secured strategic benefits such as stronger customer trust, expanded partnerships with global OEMs, and proactive alignment with supply chain security requirements.

Through comparative case analysis, this study identifies differentiated strategies across firm types. Large enterprises demonstrated a resource innovation-type (E-S-R) mechanism, where dedicated security teams systematically responded to external environmental changes and integrated internal resources. Conversely, small and medium-sized enterprises pursued a resource creation-type (S-R-E) strategy, led by top management leadership, focusing on preemptive resource acquisition and agile responses to external demands. Taken together, these results empirically demonstrate that the TISAX assessment functions not only as regulatory alignment but as a strategic driver that shapes organizational structures and decision-making logic. By applying the SER-M model, this study offers practical insights and structural guidance for designing information security strategies grounded in the dynamic interplay of subject, environment, and resources.

Keywords: Information Security Strategy, TISAX Assessement, Automotive Industry, SER-M Model, Mechanism

메커니즘 연구 5권 1호 (2025. 05.)

발　　행 : 메커니즘 경영학회
발 행 인 : 백권호
편집위원장 : 유재승
사　　무 : 서울특별시 서대문구 신촌로 203 7층(대현동, 핀란드타워)
전 화 번 호 : 02-360-0775
이 메 일 : jmm@ips.or.kr
2025년 05월 30일 발행

Journal of MECHANISM MANAGEMENT

Articles

Volume5, No.1
May 2025

A Study on Information Security Mechanism in the Automotive Industry Using the SER SER-M Model
Focusing on Successful Cases of TISAX Assessment
1 Shin Meung Chi, Ho-Sang Shin

GS Caltex: Analysis of Competitive Advantage and Growth Strategy
Focusing on the Mechanism-Based View Strategy
19 Tae Su Kim, Jae Seung You

Global Strategy Mechanisms of K-POP Entertainment Companies
A Comparative Case Study of HYBE, SM, JYP, and YG
49 Nak Hyun jung