Journal of the Korea Academia-Industrial cooperation Society
Vol. 24, No. 12 pp. 125-136, 2023

https://doi.org/10.5762/KAIS.2023.24.12.125
ISSN 1975-4701 / eISSN 2288-4688

스마트팩토리 보안관리 지표 도출: 가전 분야 사례 연구

김지태[1], 권익현[2*]
[1]인제대학교 일반대학원 산업융합보안학과, [2]인제대학교 산업경영공학과

Deriving Security Management Indicators in Smart Factory: A Case Study in Home Appliance Industry

Jitae Kim[1], Ick-Hyun Kwon[2*]
[1]Department of Industrial Convergence Security, Graduate School, Inje University
[2]Department of Industrial and Management Engineering, Inje University

요 약 국내의 대기업은 물론 중소 제조기업의 경우에도 기업의 생산성 제고, 비용 절감 및 품질 향상 등을 위해 스마트팩토리 도입을 가속화하고 있다. 최근 들어서는 스마트팩토리 도입 및 고도화뿐만 아니라 스마트팩토리 운영에 따른 보안상의 이슈들을 확인·관리하기 위한 OT 보안 관련 전담 조직 신설 및 보안정책 수립 등 스마트팩토리 보안 활동에도 많은 관심과 노력을 기울이고 있다. 특히, 가전산업의 경우 모듈화된 부품과 제품의 연계로 인해 대기업과 중소기업 간의 경영상 긴밀한 협력관계 구축이 매우 중요한 경우가 많아 스마트팩토리 운영에 따른 보안상의 이슈 또한 더욱 중요시되고 있다. 따라서, 본 연구에서는 가전 분야 대기업과 중소기업의 협력관계 하에서 스마트팩토리 운영을 통한 지속 성장을 위해 성공적인 스마트팩토리 운영에 필요한 스마트팩토리 보안관리 지표를 도출하기 위한 사례 연구를 수행하였다. 나아가 AHP를 활용하여 가전 분야 대기업, 대기업과 상생형 협력관계에 있는 중소기업 및 스마트팩토리 보안 전문가를 대상으로 도출된 보안관리 지표별 중요도 인식 차이를 분석하였다.

Abstract In South Korea, both large corporations and small to medium-sized manufacturing companies are accelerating the adoption of smart factories to enhance company productivity, reduce costs, and improve product quality. Recently, there has been an increased focus on the introduction and advancement of smart factories and on addressing the security issues associated with smart factory operations. Therefore, dedicated organizations specializing in Operational Technology (OT) security have been established, and security policies have been formulated as part of smart factory security efforts. In particular, in the home appliance industry, where the interconnection of modular components and products is prevalent, establishing close collaborative relationships between large corporations and small to medium-sized enterprises (SMEs) has become crucial for efficient business operations. Consequently, security issues related to smart factory operations have gained even more prominence. Therefore, a case study was conducted to derive smart factory security management indicators necessary for successful smart factory operations, focusing on collaboration between large corporations and SMEs in the home appliance sector. Furthermore, the analytic hierarchy process was used to analyze the perceived importance of security management indicators by large corporations in the home appliance sector, SMEs engaged in collaborative relationships with major corporations, and experts in smart factory security.

Keywords : Security Management Indicators, Smart Factory, Home Appliance Industry, Operational Technology, Analytic Hierarchy Process

*Corresponding Author : Ick-Hyun Kwon(Inje Univ.)
email: ikwon@inje.ac.kr
Received September 4, 2023 Revised October 20, 2023
Accepted December 8, 2023 Published December 31, 2023

1. 서론

코로나19의 지속, 미-중 무역분쟁, 러시아-우크라이나 전쟁까지 국제 정세의 혼란으로 글로벌 공급망이 정상적으로 작동하지 않고 있다. 이러한 상황은 수출입 품목 제한, 물류비 인상 및 원자재 가격 폭등을 초래함으로써 제조기업들은 위기를 맞이하고 있다. 특히, 자국중심주의적 경제 권역화로 생산시설을 본국이나 권역 내 인접국으로 옮기도록 강제화하고 있고, 최근 미국이 인플레이션 방지법을 발의하는 등의 행보를 보임으로써 해외로 진출했던 제조기업이 국내로 복귀하는 이슈도 새롭게 부상하고 있다[1].

이러한 현안 이슈에 대응하기 위해 최근 대기업은 물론 중소기업의 경우에도 기업의 생산성 제고, 비용 절감 및 품질 향상 등을 위해 스마트팩토리 도입을 가속화하고 있다. 스마트 제조혁신 보고에 따르면, 2022년 12월까지 국내 스마트팩토리 보급·확산이 3만 개 시대를 열었고, 이제는 '고도화' 단계라고 발표였다. 정부는 2018년 12월 중소 제조업체 절반을 스마트공장으로 만들어 제조 강국을 실현하겠다는 비전과 함께 2022년 스마트공장 3만 개 보급, 스마트 산업단지 10곳을 만들겠다는 목표를 제시하였다. 정부는 연차별 목표를 초과 달성하며 2022년 스마트공장 3만 개 시대를 열었고, 스마트 제조혁신 정책을 크게 확대했다는 평가와 함께 성공적으로 1차 임무를 완료하였다[2].

특히 일부 대기업들은 '등대공장' 도입을 가속화하고 있다. 등대공장은 사물인터넷(IoT), 인공지능, 빅데이터 등 4차 산업혁명의 핵심기술을 적극적으로 도입해 세계 제조업의 미래를 혁신적으로 이끄는 공장을 말한다. 등대공장은 지속 가능한 등대(Sustainability Lighthouse)와 제조 등대(Manufacturing Lighthouse)로 구성되며, 밤하늘에 '등대'가 불을 비춰 길을 안내하듯 '등대공장'이 제조업의 미래를 밝힌다는 의미를 담고 있다. 2023년 5월 기준 세계경제포럼(World Economic Forum)이 선정한 전 세계 등대공장은 총 132개이며, Table 1과 같이 이 중 3개의 국내기업이 등재되어 있다.

대기업의 경우 스마트팩토리 도입 및 운영에 필요한 전담 조직을 구성해 가고 있음은 물론, 스마트팩토리 운영에 따른 보안상의 이슈들을 확인·관리하기 위한 OT(Operational Technology) 보안 관련 전담 조직 신설 및 정책 수립 등 스마트팩토리 못지않게 이와 관련한 보안 활동에도 상당한 노력을 기울이고 있다. 그러나, 대다수의 중소기업의 경우에는 스마트팩토리 운영만으로도

Table 1. List of Domestic Companies Selected as Lighthouses

Organization	Reason for Selection
POSCO (Pohang)	Driving productivity improvement and quality enhancement in the steel industry based on production AI
LS Electric (Cheongju)	In response to increased demand and cost-saving requirements, mass customization and cost improvement in production are achieved through IIoT-based automation and ML-based inspection/process control
LG Electronics (Changwon)	Product portfolio complexity, enhanced customer quality expectations, and workforce shortages are improved through AI and digital performance management

※ Source: World Economic Forum

기업의 많은 자원을 투입하고 있으며, 보안 전담 인력 또는 전문 인력이 부족한 이유 등으로 스마트팩토리 운영 관련 보안 이슈에 대해서는 어려움을 호소하고 있는 실정이다. 특히, 가전산업은 대기업과 중소기업간의 협력 관계에 있어 모듈화된 부품과 제품의 연계로 경영상의 협력이 매우 중요한 경우가 많아 스마트팩토리 운영에 따른 보안상의 이슈 또한 더욱 중요시 되고 있다. Yi and Jeong(2022)은 스마트팩토리 운영상 발생할 수 있는 보안상의 주요 이슈로 모바일 미디어를 이용한 민감한 정보 자산 유출, 악성 코드 감염을 통한 중요 정보 자산 유출, 원격 접근을 통한 중요 정보 자산 유출, 외주 회사 직원을 통한 중요 정보 자산 유출 등을 언급하였다[3].

본 연구에서는 정부의 성공적인 평가 이면으로 드러나지 않고 있는 스마트팩토리에 내재된 보안 문제를 해결하기 위하여 국내외 스마트팩토리 보안 관련 동향을 살펴보고, OT 보안 관련 국제 표준 및 국내 스마트팩토리 보안 가이드, 선행연구 분석 등을 토대로 '등대공장'을 추진하고 있는 여러 대기업과 'K-스마트 등대공장'을 추진하고 있는 중소·중견기업이 참고할 수 있는 보안관리 지표를 도출하고자 한다. 도출된 스마트팩토리 보안관리 지표에 대하여 대기업에 종사하고 있는 보안 전문가와 경상남도 테크노파크 스마트팩토리 추진 사업에 참여하고 있는 중소기업, 그리고 OT 보안 전문가를 대상으로 도출된 보안관리 지표에 대한 중요도 인식 차이를 분석하여, 현재 스마트팩토리를 운영 중인 기업에 우선시 되어야 할 보안관리 지표를 제시하는 것을 주요 연구 목적으로 한다.

본 논문은 총 5장으로 구성되며, 각 장의 내용은 다음

과 같다. 1장에서는 연구의 배경 및 필요성, 연구의 목표 및 내용에 관하여 기술하였다. 2장에서는 스마트팩토리 보안 관련 동향과 관련 연구 현황을 정리하였다. 3장에서는 본 연구의 핵심이 되는 보안관리 지표 도출을 위한 연구 방법과 연구모형을 제시하였다. 4장에서는 스마트팩토리를 운영하고 있는 대기업 및 중소기업, 그리고 OT 보안 전문가를 대상으로 실시한 설문조사 결과를 토대로 보안관리 지표의 우선순위를 도출하였다. 5장은 연구의 결과를 요약하였으며, 연구의 한계점과 향후 연구 방향에 관해 기술하였다.

2. 스마트팩토리 보안 동향 및 관련 연구

2.1 스마트팩토리 보안 이슈

스마트팩토리는 기획·설계·생산·유통·판매 등 전 생산 과정을 정보통신기술(ICT)로 통합해 최소의 비용과 시간으로 고객 맞춤형 제품을 생산하는 진화된 공장을 의미한다. 스마트팩토리는 사물인터넷(IoT), 인공지능, 빅데이터 등의 4차 산업혁명 핵심기술을 전 과정에서 활용하여 자동화와 디지털화를 구현하는 것으로 생산공정을 단편적으로 자동화하는 것이 아니라, 전체 공정이 네트워크로 연결되어 실시간으로 데이터를 수집하며 이렇게 수집된 데이터를 토대로 공장 내의 상황을 파악한 후, 최적의 효율을 달성하기 위해 각 기계 설비를 공장 스스로가 제어하는 수준에 도달할 수 있도록 지원한다. 스마트팩토리의 주요 특성으로는 생산설비와 정보기술이 결합한 고도로 자동화된 시스템으로써 생산 효율성, 유연성, 안전성 등의 장점이 있으며, 이러한 특성으로 인하여 생산성과 효율성을 높이고, 제품 품질 향상에도 기여한다[4].

한편 스마트팩토리의 가장 큰 단점은 역시 보안 문제이다. 스마트팩토리는 기획·설계·생산·유통·판매에 이르는 모든 공정이 유기적으로 연결되어 모든 과정에서 정보를 수집하고 분석한다는 큰 장점이 있지만, 이러한 유기적인 네트워크 연결로 인해 해킹, 악성코드와 같은 사이버 위험에 노출되고, 보안 취약점이 존재할 경우 생산라인 전체가 마비되는 심각한 문제를 초래할 수 있다. 이러한 이유로 인하여 스마트팩토리에서는 OT(Operational Technology) 시스템이 중요한 역할을 한다. OT 시스템은 제조공정, 제어시스템 등을 포함하여 생산 환경에서 사용되는 하드웨어, 소프트웨어, 네트워크 등을 의미한다. 이러한 OT 시스템에서는 다양한 취약점이 존재하며, 해커뿐만 아니라 내외부 비인가자로부터 공격 대상이 될 수 있다. 또한 OT 시스템이 해킹되면 제조공정이 마비되거나, 제품에 결함이 발생할 수 있어 막대한 손해를 초래할 수 있다[5].

이와 같은 이유로 인하여 스마트팩토리 운영과 관련된 OT 보안이 최근 들어 많은 관심을 받고 있다. OT 보안은 IT 보안과는 다르게, 제조공정을 포함한 생산 환경에서 발생할 수 있는 다양한 위협에 대응할 수 있어야 한다. 이처럼 OT 보안은 산업제어 시스템(Industrial Control System, ICS) 및 기타 실시간 제어 시스템 등과 같은 운영 기술(Operational Technology)에 대한 보안을 의미한다. OT 보안의 목적은 이러한 운영기술 시스템을 보호하여 제조업, 에너지 및 기타 다양한 산업 분야에서 발생할 수 있는 위협으로부터 시설 및 인력의 안전을 도모하고 생산성을 유지하는 것이며, 이를 위해 OT 보안은 물리적 보안, 네트워크보안, 데이터보호, 인적 보안 등 다양한 분야로 구성되어 있다[6]. 한국산업기술보호협회의 산업보안 안내서와 한국인터넷진흥원이 발행한 스마트공장 보안 모델(스마트공장 OT 영역별)[7]에 따르면 스마트팩토리에서 발생할 수 있는 보안사고 유형을 불법침입, 정보 유출, 서비스 거부 공격, 사회공학, 내부자 침해, 물리적 침해, 악성 행위, 데이터 변조, 악성코드, 비인가 접근 등 총 10가지로 분류하고 있다.

최근 스마트팩토리에 대한 취약점 및 관련 사고는 증가하고 있음에도 불구하고, 산업제어시스템 영역은 IT와 다른 프로토콜을 사용하고 있어 보안 사고위험을 실시간으로 탐지하기 어려운 환경이며, 생산공정의 OT 보안에 대한 역할 및 책임은 일반적인 정보보안과 같이 관리 영역이 아닌 경우가 대부분이기 때문에 보안 측면에서 빠른 해답을 찾지 못하고 있다. 또한, 스마트팩토리 운영에 있어 OT 보안 관련 전문지식을 가지고 있는 인력이 기업 내·외부에 부족하여 IT 전문가들이 이를 대신하는 경우가 많다. 이들은 연결성이 증대된 산업제어시스템을 IT 시스템으로 간주하고 그들의 전문지식을 적용하고 있으며 이는 향후 더 큰 위험을 초래할 수 있다[6].

최근 들어 스마트팩토리를 운영하는 기업들이 참고할 수 있는 보안 관련 표준 수립과 선행연구들이 진행되고 있지만, 현실적으로 많은 문제점과 제약이 존재한다[8]. 전문가들은 선행되어야 할 과제로 스마트팩토리 환경에 적합한 위험관리 및 정책 규정 개발, 이를 준수하기 위한 활동 등이 필요하다고 주장한다. 하지만 현재까지 스마트팩토리 관련 지침 및 규정 준수 수준은 여전히 낮은 편이며, IT의 요구사항과 겹치거나 모순되는 것들이 다수 존재한다[7]. 결론적으로 스마트팩토리는 일반 IT와는

환경적 요인이나 특성이 상이하여 기존 IT 보안 프레임워크를 통해 스마트팩토리의 보안성을 유지하는 것은 어려운 것이 현실이다.

2.2 스마트팩토리 보안 활동 및 표준화 동향

스마트팩토리 도입을 추진하고 있는 여러 국가에서는 해당 국가 차원에서 보안 취약점을 체계적으로 도출하고, 다양한 관점에서 보안 평가를 수행할 수 있도록 산업제어시스템 보안에 대한 정책을 수립하는 다양한 기관을 운영하고 있다. 국제적으로도 산업제어시스템 보안을 다루는 여러 기관이 존재한다[9].

국내의 경우 2017년 한국전자통신연구원의 부설 연구소인 국가보안기술연구소는 한국정보통신기술협회에 'ICS 보안 요구 사항' 표준을 등록하였으며, 산업제어시스템 보안에 대한 정책과 기술적인 지원을 담당하고 있다. 미국의 경우 산업제어시스템 보안을 다루는 기관인 사이버 보안 및 인프라 보안국(Cybersecurity and Infrastructure Security Agency, CISA)에서 보안 지식과 정보를 제공하고 그 지식을 공유하여 더 나은 위험관리를 가능하게 하고 있으며, 국가의 필수 자원을 보호하기 위해 산업제어시스템 보안에 관한 연구 및 보안 대응책 수립, 위기 대응 등의 업무도 담당하고 있다.

유럽연합(EU)의 경우 유럽 사이버안보기구(European Union Agency for Cybersecurity, ENISA)에서 산업제어시스템 보안과 관련한 정책 수립과 보안역량 강화를 위한 활동을 수행하고 있으며, 2019년부터 사이버 보안법(규정 2019/881)이 시행된 이후 제품, 프로세스 및 서비스의 전달을 지원하는 '유럽 사이버보안 인증 체계'를 준비하고 있다. 일본은 2017년 정보기술진흥원(Information Technology Promotion Agency, IPA) 예하에 산업 사이버보안센터(Industrial Cyber Security Center of Excellence, ICSCoE)를 출범시켰다. ICSCoE는 사이버 공격과 방어를 수행하는 해킹 방어 대회를 열어 인력을 양성하며, 최신 사이버 공격 관련 정보를 조사하고 분석하는 등 사이버 보안 위험에 대응하는 인재, 조직, 시스템 기술을 만들고 있다. 산업제어시스템의 안전성 및 신뢰성에 대한 위험평가를 수행하며, 모든 공격 가능성을 확인하고 필요한 대책을 수립하고 있다. 중국의 전자통신기술 사이버 보안 평가센터(China Electronics Technology Cyber Security Evaluation Center, CETC)는 중국의 전자 및 통신 장비 및 소프트웨어의 보안 평가 및 인증을 담당하는 기관 중 하나이며, CETC는 스마트팩토리 및 산업제어시스템 보안 평가와 관련된 서비스를 제공하고 있다.

국제적으로는 국제전기통신연합(International Telecommunication Union, ITU)에서 산업제어시스템 보안과 관련한 국제 표준화와 보안역량 강화를 위한 활동을 수행하고 있다. 또한, 산업제어시스템 보안 분야에서는 미국 국립표준 기술연구소(National Institute of Standards and Technology, NIST)에서 개발한 표준인 NIST SP 800-82를 기반으로 국제적으로 산업제어시스템 보안 표준화를 추진하고 있다[10].

2.3 스마트팩토리 보안 관련 선행 연구

Lee and Jung(2021)은 특허 검색을 통해 미국, 유럽, 일본 등 주요 국가 및 주체들의 스마트팩토리 보안 관련 기술의 연구개발 동향을 확인하고, 결과 분석을 통해 스마트팩토리 환경하에서 기업의 미래 보안 활동에 필요한 선제적인 가이드를 제공하고자 하였다[11].

Kim and Choi(2021)는 한정된 자원을 보유하고 있는 중소 제조기업의 효율적 투자 가이드를 제공하기 위해 스마트팩토리 구축 시 순차적으로 도입 가능한 보안기술에 대한 우선순위를 도출하는 연구를 수행하였다[12].

Kim(2022)은 국내외 스마트팩토리 보안관리 체계의 비교·분석을 통해 악의적인 활동, 도청, 물리적 공격, 사고, 고장/오작동, 정전, 재해 등 총 8개 분야 23개 항목에 대한 보안관리 진단 항목을 도출하였으며 해당 항목에 대한 적합성 검증을 수행하였다[13].

Kim(2021)의 연구에서는 스마트팩토리 보안관리에 필요한 지표 정책 및 조직관리(7개 문항), 인적 보안관리(8개 문항), 물리적 보안관리(7개 문항), 비밀정보관리(7개 문항), 시스템 및 서비스 보안관리 지표(8개 문항) 등 총 5가지 지표, 37개 문항에 대해 설문조사(리커드 5점 척도) 기반 적합성 검토를 수행하였다[14].

Han(2019)의 연구에서는 국내외 표준(ISO27001, IEC 62443) 및 한국인터넷진흥원의 기준가이드(스마트공장 중요정보 유출방지 가이드[15] 외) 및 국내외 관련 연구 조사 분석을 통해 스마트팩토리 보안관리 12개 영역, 65개 항목을 도출하였다[16].

Bae and Goh(2019)는 스마트팩토리 도입기업을 대상으로 보안관리 방안 도출을 위한 사례 연구를 수행하였다. 해당 연구에서는 최근 급증하고 있는 랜섬웨어 감염으로 인한 데이터 유실 사례를 바탕으로 외곽 관련(4개), 연구소 관련(5개), 인터넷망 관련(1개), 업무망 관련(1개), 생산망 관련(9개), 정책 및 교육훈련 관련(3개) 등 총 23개 보안 강화 과제를 도출 및 적용하였다[17].

Park(2017)의 연구에서는 기술적인 보안 관점에서 마이크로소프트에서 개발한 STRIDE 모델을 사용하여 네트워크(13개), 무선네트워크(5개), 애플리케이션(6개), 시스템(4개), 물리적(3개) 등 총 31개의 보안요구사항을 도출하였다[18].

이상의 스마트팩토리 보안 관련 선행 연구를 분석한 결과 그동안 다수의 연구가 수행되어 왔지만 대부분 범용적인 표준 형태의 스마트팩토리 대상 보안관리 지표에 관한 연구로 그 범위가 제한되었음을 알 수 있다. 본 논문은 가전산업과 같은 특정한 산업군을 대상으로 스마트팩토리 보안 관련 지표를 도출하고자 하는 연구로 기존 연구와 차별화된 특성을 나타낸다.

3. 가전 분야 OT 보안 관리지표 도출

가전산업의 일반적 특성은 제품개발의 각 단계마다 상이한 인적·기술적 자원을 필요로 한다는 것이다. 즉, 초기 기술개발 및 신제품 개발 단계에서는 고도의 두뇌 집적화, 연구개발 집중 등의 특성을 보인다. 부품과 소재 가공 단계에서는 기술 및 지능 집약적 특성을 나타내며, 최종 조립 단계에서는 노동집약적인 특성을 보인다. 따라서 타 산업과 비교해서 연구개발 비용이 많이 소요되고, 신속한 기술 혁신 및 대량생산체계를 필요로 한다. 특히, 가전산업은 대기업과 중소기업간의 긴밀한 협력관계를 기반으로 모듈화된 부품과 제품의 연계로 경영상의 협력이 매우 중요한 경우가 많으며, 이로 인한 보안상의 이슈 또한 중요하게 고려할 필요가 있다[19].

스마트팩토리는 같은 공장이라도 운영라인마다 PLC, HMI, SCADA, 생산 로봇 등의 다른 설비가 존재하고, 구성 방식이 다를 수 있다. 또한 이러한 설비들이 네트워크로 연결되어 있어 보안관리 지표를 스마트팩토리 운용기업에 범용적으로 적용하기 어려운 한계점이 존재한다. 이에 본 연구에서는 가전 분야 대기업 A사의 OT 보안 아키텍처 구성과 OT 보안 위협 사례를 바탕으로 국제 보안 요구사항에서 제시하는 보안관리 항목과 국내 스마트공장 기술보호 가이드에서 제시하는 기술보호 통제항목을 맵핑하였다. 대기업 A사의 OT 보안 관리지표 도출을 위해 해당 기업에 종사하는 OT 보안 담당자와 OT 보안 컨설턴트를 대상으로 하는 집단 심층 면접(Focus Group Interview, FGI)을 실시하였으며, 결과 분석을 통해 Table 2와 같은 대기업 관점의 보안관리 지표를 도출하였다.

본 연구에서 수행한 FGI에서는 제조산업 분야 스마트팩토리 운영기업의 OT 보안 담당자 7명(보안 경력 10년 이상 종사자)과 OT 보안 전문가(컨설턴트) 2명이 참여하였다. FGI의 신뢰성을 높이고 보다 객관적인 OT 보안 관리지표 도출을 위해서는 보다 다양한 전문가 그룹(예: 스마트팩토리 기술위원, 스마트팩토리 사업화 전문가 등)을 참여시키고 이들의 의견을 종합적으로 반영할 필요가 있다[20].

Table 2. Security Management Indicators Derived through FGI

Main Categories (8 Criteria)	Subcategories (57 Subcriteria)
Technology Protection Management	Asset Identification/Classification, Policy Development, Security Officer, Security Personnel, Security Agreement, Security Training, Security Policy Revision
Access Control	User Management, Password, Access Permissions, Least Privilege, Screensaver, Role Separation, Logon Attempts, Anomaly Detection, Security Authentication, Personal Data Management, External Specialist Agency
Data Protection	Data Encryption, Data Integrity, Encryption Key, Incident Notification and Response, Prevention of Activity Denial
Infrastructure Protection	Access Control, Log Management, Cloud, Time Synchronization, System Log Auditing, Audit Analysis Reporting, Anomaly Alerting
System Protection	Security Activities, Configuration/Change, Unauthorized Programs, Removable Storage Devices, Malware, Security Patch, Security Review, Penetration Testing
Network Security	Access Control, Connection Point, Wireless Devices, Mobile Devices, Network Segmentation, Unauthorized Access
Outsourcing	Technical Protection Requirements, Maintenance Contract, Access Permissions, Predictive Maintenance System
Emergency Response	Emergency Response Policy, Communication System. Incident Reporting, Backup Management, Business Function Resumption, Emergency Response Training, Emergency Recovery, Emergency Plan Testing, Emergency Service Provision

본 연구에서는 스마트팩토리를 운영하고 있는 대기업과 중소기업의 안정적인 스마트팩토리 구축을 위한 OT 보안관리 지표의 우선순위를 선정하고자 Table 2를 기준으로 대분류(상위개념 8개), 중분류(하위개념 57개) 항목에 대하여 설문조사를 통한 AHP(Analytic Hierarchy

Process, 계층화 분석법) 분석을 실시하였다.

AHP 분석은 1970년 초 Saaty(1990)가 고안한 기법으로 다수의 평가 기준에 대해 상대적인 중요도를 점수화하는 다기준 의사결정(Multi-criteria Decision Making) 기법이다[21]. AHP는 다양한 대안들에 대한 체계적인 평가를 지원하는 의사결정 지원 방법으로 평가지표 개발 연구에서 많이 활용되고 있다. AHP는 단계별로 분류한 평가 기준에 대한 계층 구조화, 계층별 비교를 위한 전문가 설문을 이용한 쌍대 비교(Pairwise Comparison)를 수행한다. 기하평균을 이용한 계층별 가중치 및 일관성 비율(Consistency Ratio, CR)을 산출하여 결과를 도출한다. CR 값이 0이면 설문이 완전히 일관되게 진행되었다고 판단할 수 있다[20].

AHP 분석에 필요한 설문조사를 위해 스마트팩토리를 운영하고 있는 가전 분야 대기업 A사에 종사하는 OT 보안 담당자와 책임자 20명, 그리고 A사와 상생형 협력기업으로 경상남도 테크노파크 스마트팩토리 추진 사업에 참여하고 있는 중소기업 OT 보안 담당자 또는 관리자 20명, A사에 OT 보안 솔루션 구축과 OT 보안 컨설팅을 수행한 OT 보안 전문가 20명 등 총 60명을 대상으로 e메일로 설문을 발송하였으며, 총 47명이 응답하였다. 응답자에 대한 세부 현황은 대기업 종사자 16명, 중소·중견기업 종사자 15명, OT 보안 전문가 16명 등이었다.

4. AHP 분석 결과

본 연구에서는 대기업 A사 및 중소기업 종사자 그리고 OT 보안 전문가로 응답 그룹을 나누었고, 스마트팩토리 운영을 위한 OT 보안관리 지표는 기술보호관리(7개), 접근통제(11개), 데이터보호(5개), 인프라보호(7개), 시스템보호(8개), 네트워크보안(6개), 외주용역관리(4개), 비상대응(9개) 등 총 8개 대분류 항목과 57개 중분류 항목으로 구성하였다.

AHP 분석에서는 일관성 비율(CR)이 0.1 이하일 경우 수용할 수 있으나 본 연구에서는 설문 응답자의 의견을 최대한 반영하기 위해 CR이 0.2 이하인 설문을 분석대상으로 수용하였다. CR 값이 0.1보다 작으면 설문 응답자들이 일관성 있게 쌍대 비교를 수행하여 응답한 것으로 일반적으로 판단하지만, CR 값들의 분포 등을 고려하여 본 연구에서는 최종적으로 0.2를 기준값으로 설정하였다[22].

AHP 조사는 대분류(상위개념) 8개 및 중분류(하위개념) 57개 항목을 9점(총 17점) 리커트 척도를 활용하여 쌍대 비교하는 방법으로 진행하였다. AHP 설문지 분석 결과를 토대로 대분류(상위개념)와 중분류(하위개념)의 항목별 가중치와 우선순위를 도출하고, 대기업, 중소기업, OT 보안 전문가 집단별 중요도 차이를 분석하였다.

4.1 대분류(상위개념) 요소의 우선순위 결과

스마트팩토리 OT 보안관리 지표 분석 결과 중에서 먼저 대분류(상위개념) 요소들에 대한 가중치와 우선순위를 분석한 결과는 Table 3과 같다. 그룹별 일관성 비율(CR)은 대기업 0.087, 중소기업 0.090, OT 보안 전문가 0.092로 세 그룹 모두 일관성 있게 응답한 것으로 평가되었다.

Table 3. Weights and Priorities for Criteria

Criteria	Large Corporation(①) Weight (Priority)	SMEs(②) Weight (Priority)	OT Experts(③) Weight (Priority)	Consistency Ratio
Technology Protection Management	0.211 (1)	0.104 (6)	0.117 (6)	
Access Control	0.150 (3)	0.125 (4)	0.174 (2)	
Data Protection	0.169 (2)	0.250 (1)	0.115 (7)	
Infrastructure Protection	0.133 (4)	0.106 (5)	0.123 (4)	① CR = 0.087 ② CR = 0.090 ③ CR = 0.092 CR < 0.2
System Protection	0.126 (5)	0.156 (2)	0.125 (3)	
Network Security	0.113 (6)	0.136 (3)	0.185 (1)	
Outsourcing	0.041 (8)	0.047 (8)	0.039 (8)	
Emergency Response	0.058 (7)	0.076 (7)	0.121 (5)	

응답 그룹별 대분류의 평가에 대한 세부적인 결과를 살펴보면, 대기업 종사자는 (1) 기술보호관리, (2) 데이터보호, (3) 접근통제, (4) 인프라보호, (5) 시스템보호, (6) 네트워크보안, (7) 비상대응, (8) 외주용역 순으로 평가한 반면, 중소기업 종사자는 (1) 데이터보호, (2) 시스템보호, (3) 네트워크보안, (4) 접근통제, (5) 인프라보호, (6) 기술보호관리, (7) 비상대응, (8) 외주용역 순으로 중요도를 평가하였다. 이와 같은 결과가 나타난 이유는 두 그룹(대기업과 중소기업 종사자) 간에 OT 보안에 대한 인식

과 스마트팩토리 환경이 서로 다르기 때문으로 추측된다. 그리고 OT 보안 전문가 그룹의 경우 (1) 네트워크보안, (2) 접근통제, (3) 시스템보호를 가장 높은 우선순위로 선정하였다. 이러한 결과는 스마트팩토리의 특성인 네트워크 구성과 접근통제를 중심으로 보안관리 지표의 중요성을 평가한 것으로 해석할 수 있다.

4.2 중분류(하위개념) 요소의 우선순위 결과

스마트팩토리 보안관리 지표의 중분류(하위개념) 요소들에 대한 가중치와 우선순위를 분석한 결과는 Table 4와 같다. 일관성 비율(CR)은 대기업 0.009~0.095, 중소기업 0.006~0.043, OT 보안 전문가 0.038~0.157로 세 그룹 모두 일관성 있게 응답하였다.

[기술보호관리] 지표 분석 결과 대기업 종사자는 (1) 정책제정, (2) 자산식별/분류를, 중소기업 종사자 및 OT 보안 전문가는 (1) 자산식별/분류, (2) 보안책임자 지정을 각각 중요하게 평가하였다.

[접근통제] 지표 분석 결과 대기업과 중소기업, OT 보안 전문가 그룹 모두 (1) 접근권한을 가장 중요한 항목으로 평가하였고, (11) 외부전담기관 지표를 세 그룹 모두 중요도가 가장 낮은 것으로 평가하였다.

[데이터보호] 지표 분석 결과 대기업, 중소기업, OT 보안전문가 모두 (1) 데이터무결성, (2) 데이터암호화, (3) 암호화키, (4) 사고알림/대응, (5) 활동부인방지 순으로 중요도를 평가하여 세 그룹의 인식이 동일함을 알 수 있었다.

[인프라보호] 지표 분석 결과 대기업은 (1) 출입통제, (2) 이상상황알림, (3) 로그관리 순으로 중요도를 평가한 반면, 중소기업은 (1) 로그관리, (2) 출입통제, (3) 시스템로그감사 순으로 평가하였다. OT 보안 전문가는 (1) 출입통제, (2) 로그관리, (3) 이상상황알람 순으로 평가하였다.

[시스템보호] 지표 분석 결과 대기업과 중소기업은 (1) 시스템보호활동, (2) 악성코드 순으로 유사한 평가를 하였지만, OT 보안 전문가는 (1) 이동식저장장치, (2) 시스템설정/변경 순으로 평가하여 보안관리 지표의 중요도에 대한 인식 차이가 존재하는 것으로 나타났다.

[네트워크보안] 지표 분석 결과 대기업은 (1) 접근통제, (2) 연결지점관리, (3) 망분리 순으로 평가하였으며, 중소기업은 (1) 접근통제, (2) 연결지점관리, (3) 무선기기 순으로 중요도를 평가하였다. OT 보안 전문가는 (1) 접근통제, (2) 망분리, (3) 연결지점관리 등의 순으로 중요도를 평가하였다. 세 그룹 모두 접근통제를 가장 중요한 지표로 평가한 것으로 나타났다.

[외주용역] 지표 분석 결과 대기업과 중소기업 모두 (1) 기술보호요구, (2) 접근권한, (3) 유지보수계약, (4) 예지보전시스템 순으로 동일한 평가결과를 보였으나 OT 보안 전문가와는 다소간의 인식 차이를 나타냈다.

[비상대응] 지표 분석 결과 세 그룹 모두 (1) 백업관리를 가장 중요한 보안관리 지표로 평가하였다. 특히 중분류(하위개념) 요소 중에서 [비상대응] 지표는 설문조사 집단 간 일관성 비율이 0.025~0.038로 차이가 매우 작아 가장 일관성 있는 항목으로 평가되었다.

4.3 최종 가중치 및 우선순위 분석 결과

앞서 도출한 스마트팩토리 보안관리 지표의 대분류(상위개념), 중분류(하위개념)에 대한 가중치와 우선순위 평가 결과를 바탕으로 대분류(상위개념)와 중분류(하위개념)에 대한 복합가중치를 산출하였다. 복합가중치는 대분류(상위개념)의 항목별 가중치(a)와 중분류(하위개념)의 항목별 가중치(b)를 곱하여 중요도를 산출하는 일반적인 방법을 사용하였다. 복합가중치(a×b) 계산 결과에 따른 중분류(하위개념) 항목별 복합가중치 및 우선순위는 Table 5와 같이 도출되었다.

복합가중치(a×b) 산출 결과를 토대로 그룹별로 우선순위가 높은 지표를 살펴보면, 대기업의 경우 (1) 데이터무결성, (2) 정책제정, (3) 자산식별/분류, (4) 암호화, (5) 책임자지정 순이었으며, 중소기업은 (1) 데이터무결성, (2) 데이터암호화, (3) 암호화키, (4) 접근통제, (5) 사고알림대응 순으로 높은 중요도를 나타내었다. OT 보안 전문가는 (1) 접근통제, (2) 망분리, (3) 연결지점, (4) 자산식별/분류, (5) 데이터무결성 순으로 중요도를 평가하였다. 한편 그룹별 우선순위가 낮은 항목을 살펴보면, 대기업의 경우 (53) 사고보고, (54) 비상서비스확보, (55) 비상대응훈련, (56) 비상계획테스트, (57) 외부전담기관 순으로, 중소기업은 (53) 연락체계, (54) 비상대응훈련, (55) 비상서비스확보, (56) 비상계획테스트, (57) 외부전담기관 순으로 각각 평가하였다. OT 보안 전문가의 경우 (53) 비상대응훈련, (54) 정책개정, (55) 개인정보관리, (56) 모의침투테스트, (57) 외부전담기관 등에 대해 낮은 평가를 하였다.

4.4 종합분석 결과

본 연구를 통해 대기업과 중소기업, 그리고 OT 보안 전문가의 설문 분석 결과, OT 보안관리 지표에 대한 중요도 인식 차이가 존재하는 것으로 평가되었다.

Table 4. Summary of Weights and Priorities for Subcriteria

Criteria	Subcriteria	Weight of Large Corporation (Priority)	Weight of SMEs (Priority)	Weight of OT Experts (Priority)	Consistency Ratio
Technology Protection Management	Asset Identification/Classification	0.231 (2)	0.211 (1)	0.308 (1)	① CR = 0.075 ② CR = 0.006 ③ CR = 0.147 CR 〈 0.2
	Policy Development	0.235 (1)	0.163 (3)	0.175 (3)	
	Security Officer	0.168 (3)	0.183 (2)	0.192 (2)	
	Security Personnel	0.147 (4)	0.157 (4)	0.142 (4)	
	Security Agreement	0.085 (5)	0.103 (5)	0.073 (5)	
	Security Training	0.075 (6)	0.110 (6)	0.063 (6)	
	Security Policy Revision	0.059 (7)	0.074 (7)	0.047 (7)	
Access Control	User Management	0.126 (2)	0.107 (3)	0.074 (6)	① CR = 0.058 ② CR = 0.025 ③ CR = 0.125 CR 〈 0.2
	Password	0.126 (3)	0.124 (2)	0.067 (7)	
	Access Permissions	0.148 (1)	0.189 (1)	0.163 (1)	
	Least Privilege	0.109 (6)	0.101 (4)	0.153 (2)	
	Screensaver	0.033 (10)	0.064 (9)	0.046 (9)	
	Role Separation	0.071 (7)	0.087 (5)	0.126 (4)	
	Logon Attempts	0.069 (8)	0.079 (7)	0.060 (8)	
	Anomaly Detection	0.125 (4)	0.085 (6)	0.122 (5)	
	Security Authentication	0.109 (5)	0.063 (10)	0.132 (3)	
	Personal Data Management	0.062 (9)	0.066 (8)	0.031 (10)	
	External Specialist Agency	0.023 (11)	0.036 (11)	0.025 (11)	
Data Protection	Data Encryption	0.282 (2)	0.235 (2)	0.252 (2)	① CR = 0.074 ② CR = 0.036 ③ CR = 0.043 CR 〈 0.2
	Data Integrity	0.298 (1)	0.302 (1)	0.283 (1)	
	Encryption Key	0.182 (3)	0.200 (3)	0.199 (3)	
	Incident Notification and Response	0.154 (4)	0.160 (4)	0.158 (4)	
	Prevention of Activity Denial	0.083 (5)	0.103 (5)	0.108 (5)	
Infrastructure Protection	Access Control	0.167 (1)	0.187 (2)	0.249 (1)	① CR = 0.024 ② CR = 0.010 ③ CR = 0.083 CR 〈 0.2
	Log Management	0.152 (3)	0.191 (1)	0.191 (2)	
	Cloud	0.145 (4)	0.137 (4)	0.128 (4)	
	Time Synchronization	0.103 (7)	0.101 (7)	0.106 (6)	
	System Log Auditing	0.117 (6)	0.139 (3)	0.107 (5)	
	Audit Analysis Reporting	0.142 (5)	0.116 (6)	0.081 (7)	
	Anomaly Alerting	0.174 (2)	0.130 (5)	0.137 (3)	
System Protection	Security Activities	0.190 (1)	0.189 (1)	0.135 (5)	① CR = 0.009 ② CR = 0.022 ③ CR = 0.144 CR 〈 0.2
	Configuration/Change	0.126 (4)	0.117 (5)	0.167 (2)	
	Unauthorized Programs	0.128 (3)	0.123 (4)	0.150 (4)	
	Removable Storage Devices	0.111 (5)	0.115 (6)	0.224 (1)	
	Malware	0.161 (2)	0.149 (2)	0.164 (3)	
	Security Patch	0.104 (6)	0.142 (3)	0.070 (6)	
	Security Review	0.089 (8)	0.107 (7)	0.053 (7)	
	Penetration Testing	0.093 (7)	0.057 (8)	0.037 (8)	
Network Security	Access Control	0.235 (1)	0.308 (1)	0.274 (1)	① CR = 0.007 ② CR = 0.029 ③ CR = 0.153 CR 〈 0.2
	Connection Point	0.196 (2)	0.151 (2)	0.210 (3)	
	Wireless Devices	0.149 (4)	0.142 (3)	0.095 (4)	
	Mobile Devices	0.120 (5)	0.136 (5)	0.089 (5)	
	Network Segmentation	0.180 (3)	0.137 (4)	0.262 (2)	
	Unauthorized Access	0.119 (6)	0.125 (6)	0.070 (6)	
Outsourcing	Technical Protection Requirements	0.366 (1)	0.347 (1)	0.210 (3)	① CR = 0.095 ② CR = 0.043 ③ CR = 0.157 CR 〈 0.2
	Maintenance Contract	0.180 (3)	0.218 (3)	0.176 (4)	
	Access Permissions	0.284 (2)	0.220 (2)	0.361 (1)	
	Predictive Maintenance System	0.170 (4)	0.215 (4)	0.253 (2)	

Emergency Response	Emergency Response Policy	0.146 (4)	0.116 (4)	0.147 (3)	① CR = 0.025 ② CR = 0.022 ③ CR = 0.038 CR 〈 0.2
	Communication System	0.102 (5)	0.096 (6)	0.109 (5)	
	Incident Reporting	0.079 (6)	0.099 (5)	0.106 (6)	
	Backup Management	0.169 (1)	0.195 (1)	0.165 (1)	
	Business Function Resumption	0.152 (2)	0.143 (3)	0.145 (4)	
	Emergency Response Training	0.070 (8)	0.077 (7)	0.053 (9)	
	Emergency Recovery	0.149 (3)	0.146 (2)	0.150 (2)	
	Emergency Plan Testing	0.060 (9)	0.062 (9)	0.053 (8)	
	Emergency Service Provision	0.072 (7)	0.066 (8)	0.073 (7)	

Table 5. Summary of Composite Weights and Priorities for Subcriteria

Weights (a) (①,②,③) for Criteria	Weights (b) (①,②,③) for Subcriteria	Composite Weight (a×b) of Large Corp. (Priority)	Composite Weight (a×b) of SMEs (Priority)	Composite Weight (a×b) of OT Experts (Priority)
Technology Protection Management (0.211, 0.104, 0.117)	Asset Identification/Classification (0.231, 0.211, 0.308)	0.049 (3)	0.022 (11)	0.036 (4)
	Policy Development (0.235, 0.163, 0.308)	0.050 (2)	0.017 (23)	0.175 (3)
	Security Officer (0.168, 0.183, 0.192)	0.035 (5)	0.019 (17)	0.022 (14)
	Security Personnel (0.147, 0.157, 0.142)	0.031 (6)	0.016 (25)	0.017 (29)
	Security Agreement (0.085, 0.103, 0.073)	0.018 (23)	0.011 (39)	0.009 (46)
	Security Training (0.075, 0.110, 0.063)	0.016 (29)	0.011 (35)	0.007 (49)
	Security Policy Revision (0.059, 0.074, 0.047)	0.012 (38)	0.008 (51)	0.006 (54)
Access Control (0.150, 0.125, 0.174)	User Management (0.126, 0.107, 0.074)	0.019 (19)	0.013 (32)	0.013 (37)
	Password (0.126, 0.124, 0.067)	0.019 (20)	0.015 (27)	0.012 (40)
	Access Permissions (0.148, 0.189, 0.163)	0.022 (12)	0.024 (8)	0.028 (8)
	Least Privilege (0.109, 0.101, 0.153)	0.016 (26)	0.013 (33)	0.027 (10)
	Screensaver (0.033, 0.064, 0.046)	0.005 (52)	0.008 (49)	0.008 (48)
	Role Separation (0.071, 0.087, 0.126)	0.011 (42)	0.011 (37)	0.022 (15)
	Logon Attempts (0.069, 0.079, 0.060)	0.010 (43)	0.010 (45)	0.010 (41)
	Anomaly Detection (0.125, 0.085, 0.122)	0.019 (21)	0.011 (41)	0.021 (16)
	Security Authentication (0.109, 0.063, 0.132)	0.016 (25)	0.008 (50)	0.023 (12)
	Personal Data Management (0.062, 0.066, 0.031)	0.009 (45)	0.008 (48)	0.005 (55)
	External Specialist Agency (0.023, 0.036, 0.025)	0.003 (57)	0.005 (57)	0.004 (57)
Data Protection (0.169, 0.250, 0.115)	Data Encryption (0.282, 0.235, 0.252)	0.048 (4)	0.059 (2)	0.029 (7)
	Data Integrity (0.298, 0.302, 0.283)	0.050 (1)	0.075 (1)	0.032 (5)
	Encryption Key (0.182, 0.200, 0.199)	0.031 (7)	0.050 (3)	0.023 (13)
	Incident Notification and Response (0.154, 0.160, 0.158)	0.026 (9)	0.040 (5)	0.018 (22)
	Prevention of Activity Denial (0.083, 0.103, 0.108)	0.014 (32)	0.026 (7)	0.012 (39)
Infrastructure Protection (0.133, 0.106, 0.123)	Access Control (0.167, 0.187, 0.249)	0.022 (13)	0.020 (14)	0.031 (6)
	Log Management (0.152, 0.191, 0.191)	0.020 (17)	0.020 (13)	0.024 (11)
	Cloud (0.145, 0.137, 0.128)	0.019 (18)	0.014 (30)	0.016 (31)
	Time Synchronization (0.103, 0.101, 0.106)	0.014 (34)	0.011 (40)	0.013 (35)
	System Log Auditing (0.117, 0.139, 0.107)	0.016 (30)	0.015 (29)	0.013 (34)
	Audit Analysis Reporting (0.142, 0.116, 0.081)	0.019 (22)	0.012 (34)	0.010 (42)
	Anomaly Alerting (0.174, 0.130, 0.137)	0.023 (11)	0.014 (31)	0.017 (27)

System Protection (0.126, 0.156, 0.125)	Security Activities (0.190, 0.189, 0.135)	0.024 (10)	0.030 (6)	0.017 (28)
	Configuration/Change (0.126, 0.117, 0.167)	0.016 (28)	0.018 (20)	0.021 (17)
	Unauthorized Programs (0.128, 0.123, 0.150)	0.016 (27)	0.019 (16)	0.019 (21)
	Removable Storage Devices (0.111, 0.115, 0.224)	0.014 (33)	0.018 (21)	0.028 (9)
	Malware (0.161, 0.149, 0.164)	0.161 (2)	0.149 (2)	0.164 (3)
	Security Patch (0.104, 0.142, 0.070)	0.013 (37)	0.022 (10)	0.009 (45)
	Security Review (0.089, 0.107, 0.053)	0.011 (41)	0.017 (24)	0.007 (51)
	Penetration Testing (0.093, 0.057, 0.037)	0.012 (39)	0.009 (46)	0.005 (56)
Network Security (0.113, 0.136, 0.185)	Access Control (0.235, 0.308, 0.274)	0.026 (8)	0.042 (4)	0.051 (1)
	Connection Point (0.196, 0.151, 0.210)	0.022 (14)	0.021 (12)	0.039 (3)
	Wireless Devices (0.149, 0.142, 0.095)	0.017 (24)	0.019 (15)	0.018 (25)
	Mobile Devices (0.120, 0.136, 0.089)	0.014 (35)	0.019 (19)	0.016 (30)
	Network Segmentation (0.180, 0.137, 0.262)	0.020 (15)	0.019 (18)	0.048 (2)
	Unauthorized Access (0.119, 0.125, 0.070)	0.013 (36)	0.017 (22)	0.013 (36)
Outsourcing (0.041, 0.047, 0.039)	Technical Protection Requirements (0.366, 0.347, 0.210)	0.015 (31)	0.016 (26)	0.008 (47)
	Maintenance Contract (0.180, 0.218, 0.176)	0.007 (49)	0.010 (43)	0.007 (50)
	Access Permissions (0.284, 0.220, 0.361)	0.012 (40)	0.010 (42)	0.014 (32)
	Predictive Maintenance System (0.170, 0.215, 0.253)	0.007 (50)	0.010 (44)	0.010 (43)
Emergency Response (0.058, 0.076, 0.121)	Emergency Response Policy (0.146, 0.116, 0.147)	0.008 (48)	0.009 (47)	0.018 (24)
	Communication System (0.102, 0.096, 0.109)	0.006 (51)	0.007 (53)	0.013 (33)
	Incident Reporting (0.079, 0.099, 0.106)	0.005 (53)	0.008 (52)	0.013 (38)
	Backup Management (0.169, 0.195, 0.165)	0.010 (44)	0.015 (28)	0.020 (20)
	Business Function Resumption (0.152, 0.143, 0.145)	0.009 (46)	0.011 (38)	0.018 (26)
	Emergency Response Training (0.070, 0.077, 0.053)	0.004 (55)	0.006 (54)	0.006 (53)
	Emergency Recovery (0.149, 0.146, 0.150)	0.009 (47)	0.011 (36)	0.018 (23)
	Emergency Plan Testing (0.060, 0.062, 0.053)	0.003 (56)	0.005 (56)	0.006 (52)
	Emergency Service Provision (0.072, 0.066, 0.073)	0.004 (54)	0.005 (55)	0.009 (44)

먼저 대기업 종사자의 종합평가 결과에 의하면, 대기업은 스마트팩토리를 운영하는 데 있어 보안관리 활동 전반을 담당하는 기술보호관리(대분류 0.211, 1순위) 지표를 중심으로 생산활동을 지속하기 위해 보호해야 할 자산을 식별하고 분류하기 위한 지표와 식별/분류된 자산을 보호하기 위한 데이터보호(대분류 0.169, 2순위) 활동을 중요한 지표로 평가하였다. 이와 같은 평가는 데이터 무결성(복합가중치 0.050, 종합 1순위)과 정책제정(복합가중치 0.050, 종합 2순위) 등과 같이 복합가중치 결과에서도 유사하게 평가된 것으로 분석되었다.

다음으로 중소기업의 종합평가 결과를 분석해 보면, 데이터 무결성(복합가중치 0.075, 종합 1순위), 데이터 암호화(복합가중치 0.059, 종합 2순위), 암호화키(복합가중치 0.050, 종합 3순위) 등 종합평가 상위 3개 항목 모두 데이터보호(대분류 0.250, 1순위) 항목에서 도출되었다. 반면, 대기업이 중요하게 평가한 정책제정(복합가중치 0.017, 종합 23순위)과 자산식별/분류(복합가중치 0.022, 종합 11순위)에 대해서는 상대적으로 낮은 평가를 하였다.

OT 보안 전문가 평가 결과 주목할 부분은 접근통제(복합가중치 0.051, 종합 1순위), 망분리(복합가중치 0.048, 종합 2순위), 연결지점관리(복합가중치 0.039, 종합 3순위) 등 종합평가 상위 3개 항목 모두가 네트워크 보안(대분류 0.185, 1순위)에서 도출된 점이다.

전술한 결과를 토대로 스마트팩토리의 보안관리 지표에 대한 중요도 평가 차이를 분석해 보면, 대기업은 보안정책을 중심으로 관리적인 보안을 중요하게 인식하고 있음을 알 수 있었다. 반면, 중소기업은 데이터보호와 시스템보호와 같은 물리적 보안을 가장 중요한 요소로 인식하고 있으며, OT 보안 전문가는 스마트팩토리가 가지는 특성인 네트워크를 기반으로 한 기술적인 보안을 가장 중요하게 인식하고 있는 것으로 평가되었다.

5. 결론

본 논문에서는 ICT를 기반으로 스마트팩토리를 지속적으로 확대해 가고 있는 가전 분야 대기업 A사를 중심으로 해당 대기업과 협력관계에 있으면서 스마트팩토리를 운영하고 있는 중소기업, 그리고 대기업에 OT 보안 컨설팅을 경험한 OT 보안 전문가를 대상으로 성공적인 스마트팩토리 운영에 필요한 스마트팩토리 보안관리 지표를 도출하기 위한 사례 연구를 수행하였다.

본 연구를 수행하게 된 배경과 본 연구가 지니는 의의, 시사점을 정리해 보면 다음과 같다.

먼저 본 연구는 제조 강국 실현을 위해서는 국내 대기업과 중소·중견 기업 대상 스마트팩토리 보급 확산과 스마트팩토리 수준 고도화뿐만 아니라 스마트팩토리 OT 보안관리의 중요성 또한 매우 중요하다는 문제 인식에 기반하여 시작하였다. 본 연구의 의의로는 여러 제조업 분야 가운데 하나인 가전 분야를 대상으로 가전 분야 대기업 A사의 실증 사례를 바탕으로 스마트팩토리 OT 보안관리 지표를 도출하였고, 이는 향후 스마트팩토리 도입을 추진하는 가전 분야 대기업과 중소·중견기업이 활용 가능한 보안관리 참고 모델로서 중요한 역할을 할 수 있을 것으로 기대한다. 또한 가전 분야 대기업과 중소기업을 사례로 보안관리 지표에 대한 중요도 인식 차이를 평가함과 동시에 OT 보안 전문가 그룹의 평가 결과를 함께 제시함으로써 가전 분야 대기업과 중소기업이 앞으로 스마트팩토리 수준을 더 높이고 안정적인 운영을 통해 제조 경쟁력을 갖추는 데 필요한 기반 연구가 되었다고 볼 수 있다.

한편, 본 연구가 지니는 한계점은 다음과 같다.

첫째, 기업마다 보안정책이 다른 상황에서 본 연구는 가전 분야 특정 대기업의 OT 시스템 구성과 보안 위협 유형을 바탕으로 보안관리 지표를 선정하고 평가하였기에, 자동차, 기계장비, 조선, 반도체, 화학 등 OT 시스템 구성과 보안 위협의 형태가 상이한 산업 분야에 본 연구의 스마트팩토리 보안지표를 활용하기에 어려운 한계가 있다.

둘째, 본 연구에 참여한 중소기업은 스마트팩토리 구축단계가 모두 기초 단계 수준이었으며, 응답자 대부분이 보안을 전담하지 않거나 보안 경력이 많지 않은 대상으로부터 설문조사가 진행되었다는 점이다.

다만 본 연구는 가전 분야에서 스마트팩토리를 운영중인 대기업과 협력 중소기업을 대상으로 실증 연구를 수행하였다는 점에서 관련 분야 연구의 초석이 될 수 있을 것이다. 향후 본 연구를 기반으로 가전분야에 표준화된 보안관리 지표 개발과 다양한 산업군에 대한 스마트팩토리 보안 관련 연구 등이 활발히 이루어지기를 기대해 본다. 한편 이러한 연구를 추진하기 위해서는 특정 산업군의 특성(예: 산업별 기술혁신 패턴)과 경영환경, 보안협력체계 등에 대한 면밀한 분석이 선행되어야 할 것이다[22].

References

[1] G. W. Kim, *A Study on the Cases of Smart Factories by SMEs and on Their Business Performance*, Master's Thesis, Hansung University, 2022.

[2] J. Y. Choi, "In the Era of 30,000 Smart Factories Dawning, Will 2023 Mark the Commencement of Advanced Smart Manufacturing Innovation?", *FA Journal*, 2022.

[3] K. J. Yi, Y. S. Jeong, "Smart Factory: Security Issues, Challenges, and Solutions", *Journal of Ambient Intelligence and Humanized Computing*, Vol.13, pp.4625-4638, 2022.
DOI: https://doi.org/10.1007/s12652-021-03457-6

[4] S. J. Kim, "Technology Research Trends of Smart Factory through the Keyword Network Analysis", *Journal of the Korea Academia-Industrial cooperation Society*, Vol.23, No.5, pp.17-23, 2022.
DOI: https://doi.org/10.5762/KAIS.2022.23.5.17

[5] J. H. Ryu, I. G. Lee, J. H. Moon, "OT Industrial Security Enhancement Focused on Security-by-Design", Korean Journal of Industry Security, Vol.13, pp.91-118, 2023
DOI: https://doi.org/10.33388/kais.2023.13.s.091

[6] J. W. Jung, *An Empirical Study on the Development of Security Requirements and Application to Improve the Security of Industrial Control Systems*, PhD Dissertation, Chung-Ang University, 2021.

[7] KISA, *Smart Factory Security Model*, 2021.

[8] J. M. Sohn, I. T. Lee, H. C. Lim, "Enhancement of Industrial Control Systems(ICS) Security for Service Company", *Journal of the Korea Service Management Society*, Vol.20, No.4, pp.183-200, 2019.
DOI: http://dx.doi.org/10.15706/jksms.2019.20.4.010

[9] K. H. Han, "Status of Smart Manufacturing Security Standardization", *TTA Journal*, Vol.178, pp.83-90, 2018.

[10] M. G. Kang, "Cybersecurity Status of Industrial Control Systems by Country", *Weekly ICT Trends*, Vol.1916, 2019.

[11] K. H. Lee, Y. H. Jung, "A Study on the Trends of Technology Development Related to Smart Factory Security: Based on Patent Analysis", *Korean Journal of*

Industry Security, Vol.11, No.3, pp.49-71, 2021.
DOI: https://doi.org/10.33388/kais.2021.11.3.049

[12] Y. H. Kim, Y. S. Choi, "Designing Smart Factory Security System on Spatial Strategy", *Journal of Information and Security*, Vol.21, No.5, pp.79-86, 2021.
DOI: https://doi.org/10.33778/kcsa.2021.21.5.079

[13] S. Y. Kim, *A Diagnostic Framework for Smart Factory Security Management*, Master's Thesis, Kyungil University, 2022.

[14] B. H. Kim, *A Study on Smart Factory Security Management System*, Master's Thesis, Ajou University, 2022.

[15] KISA, *Important Information Leakage Prevention in Smart Factory*, Jinhan M&B, 2020.

[16] S. H. Han, *A Study on Security Management Items for Smart Factory*, Master's Thesis, Chung-Ang University, 2019.

[17] C. S. Bae, S. C. Goh, "Case Study on Security Enhancement of Smart Factory", *Journal of the Korea Institute of Information Security and Cryptology*, Vol.29, No.3, pp.675-684, 2019.
DOI: https://doi.org/10.13089/JKIISC.2019.29.3.675

[18] E. J. Park, S. J. Kim, "Derivation of Security Requirements of Smart Factory Based on STRIDE Threat Modeling", *Journal of the Korea Institute of Information Security and Cryptology*, Vol.27, No.6, pp.1467-1482, 2017.
DOI: https://doi.org/10.13089/JKIISC.2017.27.6.1467

[19] T. J. Kim, J. G. Eom, "A Study on the Management Strategy Mechanism of the Premium Consumer Electronics Market based on Ser-M Framework: Focused on LG Electronics' Case", *Korean Business Education Review*, Vol.35, No.6, pp.509-531, 2020.
DOI: https://doi.org/10.23839/kabe.2020.35.6.509

[20] J. Hoh, A. R. Lee, "Investigating Key Security Factors in Smart Factory: Focusing on Priority Analysis Using AHP Method", *Information Systems Review*, Vol.22, No.4, pp.185-203, 2020.
DOI: http://dx.doi.org/10.14329/isr.2020.22.4.185

[21] T. L. Saaty, *The Analytic Hierarchy Process*, RWS Publication, Pittsburgh, 1990.

[22] J. H. Kim, H. J. Go, Y. H. Jung, "A Study on the Development of Security Certification Evaluation Index for the Improvement of Security Cooperation between Large and SMEs: Focusing on Cooperation in the Engineering Design Field of Shipbuilding Industry", *Korean Journal of Industry Security*, Vol.13, pp.73-90, 2023.
DOI: https://doi.org/10.33388/kais.2023.13.s.073

김 지 태(Jitae Kim) [정회원]

- 2023년 8월 : 인제대학교 일반대학원 산업융합보안학과 (보안경영학석사)
- 2003년 2월 ~ 현재 : LG전자 창원정보보안팀 책임

〈관심분야〉
산업보안, OT보안, 스마트팩토리

권 익 현(Ick-Hyun Kwon) [정회원]

- 2000년 2월 : 고려대학교 산업공학과 (공학석사)
- 2006년 2월 : 고려대학교 산업공학과 (공학박사)
- 2007년 1월 ~ 2008년 1월 : University of Illinois at Urbana-Champaign, 박사후연구원
- 2008년 3월 ~ 현재 : 인제대학교 산업경영공학과 교수

〈관심분야〉
산업보안, 스마트물류, 스마트제조