Information Systems Review
Vol. 22, No. 4 November 2020 http://dx.doi.org/10.14329/isr.2020.22.4.185

스마트팩토리의 주요 보안요인 연구: AHP를 활용한 우선순위 분석을 중심으로

Investigating Key Security Factors in Smart Factory: Focusing on Priority Analysis Using AHP Method

허 진 (Jin Hoh) 유로서비스(주) 대표
이 애 리 (Ae Ri Lee) 상명대학교 경영학부 조교수, 교신저자

요 약

4차 산업혁명과 함께 ICT(정보통신기술)와 제조업이 융합된 스마트 제조업 시대로 변화하고 있다. 과거의 제조업은 생산효율 증진을 위한 단순 목적으로 공업적인 기술 혁신을 추구했다면, 스마트 제조업에서는 ICT와 융합된 스마트팩토리 구축을 통해 제조 공정과 서비스 형태가 융·복합 플랫폼 형태로 변모하고 있다. 스마트팩토리 구현 기업들은 ICT의 장점을 활용한 이점과 함께, 개방화/융합화/정보화에 따라 발생하게 되는 보안 이슈를 동시에 접하게 된다. 스마트팩토리에서는 ICT를 기반으로 모든 기계와 설비 등이 연결되어 기존에 생각하지 못했던 융·복합적 보안 위협요인에 노출되고 상시적으로 다양한 사이버 위협이 발생할 수 있음으로 보안이 더욱 강화되어야 한다. 보안사고의 위험을 줄이고 스마트팩토리를 성공적으로 도입하기 위해서는, ICT 기술들이 적용되고 있는 스마트팩토리 산업 현장의 특성을 감안하여 우선적으로 적용되어야 할 주요 보안요인들을 도출할 필요가 있다.

본 연구에서는 스마트팩토리 구축 시 적용해야 할 보안요인들의 중요도를 파악하기 위해 단말/네트워크/플랫폼·서비스 범주를 포괄한 '스마트팩토리 보안요인의 계층적 분류 모델'을 제시하고, 스마트팩토리 및 보안 관련 전문가 그룹(기술위원, 사업전문가, 보안전문가)을 대상으로 중요도 평가 분석을 수행하였다. 본 연구에서는 AHP 기법을 활용하여 다양한 보안 위협으로부터 안전한 스마트팩토리 구현에 필요한 보안요인들의 상대적 중요도를 도출하고 이를 기반으로 스마트팩토리 보안요인 간의 우선순위를 제시하였다. 본 연구 결과를 통해, 앞으로 더욱 확산될 스마트팩토리가 보다 안전하게 구축·운용될 수 있도록 스마트 제조업 시대에 필요한 정보보안 확보에 기여할 수 있을 것이다.

키워드 : 스마트팩토리, 스마트공장, 스마트 제조업, 사물인터넷, 정보보안, 계층화 분석법

Ⅰ. 서 론

진화된 ICT(Information and Communication Technology, 정보통신기술)를 기반으로 한 4차 산업혁명은 우리 사회와 산업에 새로운 변화를 가져오고 있다. 이러한 변화의 영향으로 기존의 폐쇄적 구성

을 기반으로 한 전통적인 제조환경이 ICBM(IoT, Cloud, Big Data, Mobile)을 구성요소로 한 개방적인 형태의 새로운 제조환경으로 변화하고 있다(진상기, 박영원, 2017). 제조업에서의 변화는 생산현장에서 새로운 제조환경을 기반으로 생산성 향상을 추구하고, ICT를 기반으로 프로세스와 서비스 등이 유기적으로 연동되는 융합 비즈니스 환경으로 기업 혁신을 요구하고 있다(이무순, 손달호, 2017; 최영환, 최상현, 2018). 이러한 변화는 세계적 규모의 공장을 가진 대기업 뿐만 아니라 중소규모의 제조기업에도 기업 전반에 걸친 경영혁신을 촉진하고 있다(유창현, 2017; 정선양 등, 2016). 독일, 미국, 중국, 일본, 한국 등 세계 각국에서는 4차 산업혁명의 일부분으로 스마트팩토리(Smart Factory)를 추진하고 있으며 제조현장에 속속 도입되고 있다. 독일은 인더스트리 4.0 정책으로 스마트팩토리 구현을 적극적으로 추진하고 있으며, 미국은 AMP(Advanced Manufacturing Partnership, 첨단 제조업 파트너십) 정책의 일환으로 제조업 혁신과 IIoT(Industrial Internet of Things, 산업인터넷)를 추진하고 있다(진상기, 박영원, 2017). 국내에서도 제조업 3.0 정책의 일환으로 2020년까지 1만개의 스마트팩토리를 구축하는 정책이 추진되고 있다(장경석, 2017).

한편, 이러한 스마트팩토리 확산 정책과 함께 스마트팩토리에서의 보안의 중요성이 더욱 커지고 있다. 스마트팩토리 구현 기업들은 ICT를 활용한 이점과 함께, 개방화/융합화/정보화에 따라 발생하게 되는 보안 이슈를 동시에 접하게 된다(Lee *et al.*, 2020). 기존 제조환경에서의 보안관리는 개별 기업의 공장 내에 한정되어 운영되었던 ICS (Industry Control System, 산업제어시스템)를 기반으로 한 폐쇄적 연결을 전제로 하고 있고, 개별 기업이나 협력 기업의 임직원 및 외부 방문객에 의한 인적사고를 주로 방지하는 관리적 보안이 중심이었다면, 새롭게 변화되는 스마트팩토리에서는 융합 연동 시스템 구조에 맞는 보안관리가 필요하다(나재훈, 나중찬, 2016). 과거와 달리, 스마트팩토리 환경에서는 개별적인 기계와 설비, 시스템들이 IoT로 연결·확장되고, 새로운 시스템과 기존 시스템 간의 연결로 인해 다양한 측면의 보안 문제를 대면하게 된다(김다빈 등, 2015). 즉, 스마트 제조 환경에서는 ICT를 기반으로 모든 기계와 설비 등이 연결되어 기존에 생각하지 못했던 융·복합적 보안 위협요인에 노출되고 상시적으로 다양한 사이버 위협이 발생할 수 있음으로 이러한 스마트팩토리의 특성을 고려한 새로운 측면의 기술적 보안이 더욱 강화되어야 한다(Lee *et al.*, 2020). 최근 스마트팩토리 도입이 제조업의 경쟁력 향상은 물론이고 제조업의 서비스화(Product Servitization) 및 휴먼팩토리(Human Factory) 개념을 기존의 공장에 도입하는 것으로 인식 되면서, 스마트팩토리로 전환하거나 ICT 기반의 시스템으로 고도화 하는 공장이 급격히 증가하고 있다는 것을 고려하면 스마트팩토리에서의 보안은 매우 중요하게 다루어야 하는 현안 과제이다.

기업보안 및 산업보안에 대한 기존 연구들은 산업보안 정책 설계 및 사이버보안 거버넌스 구축 방안 연구 등 보안의 관리적 측면을 주로 다루거나, 융합 환경에서의 산업보안 평가 모형 및 IT 보안서비스 품질 측정 방법 연구 등 보안에 대한 측정 및 평가에 대해서 다뤄왔다(경지훈, 김종수, 2015; 김동희, 2016; 임창묵 등, 2013). 또한 최근의 IoT 및 스마트팩토리 보안에 대한 일부 연구에서 기업의 경쟁력 제고를 위해 스마트팩토리의 안정적 운영을 위한 보안관리에 대해 다루고는 있으나(정선양 등, 2016), 이들 보안요인들 중 어떤 것을 우선적으로 고려해야 하는지에 대한 명확한 제시가 부족하다. 보안사고의 위험을 줄이고 스마트팩토리를 성공적으로 도입하기 위해서는, 기존의 ICS 보안 및 IoT 보안 등에서 확인된 보안요인들을 검토하고, 새로운 ICT 기술들이 적용되고 있는 산업현장 환경과 스마트팩토리의 특성을 감안하여 우선적으로 적용되어야 할 주요 보안요인들이 무엇인지 분석할 필요가 있다.

이에, 본 연구에서는 스마트팩토리 구축 시 적용해야 할 보안요인들의 중요도를 도출하기 위해

계층화 모형을 제시하고, 스마트팩토리 및 보안 전문가를 대상으로 한 실증 분석을 하고자 한다. 본 연구는 AHP(Analytic Hierarchy Process) 기법을 활용하여 다양한 보안 위협으로부터 안전한 스마트팩토리 구현에 필요한 보안요인들의 상대적 중요도를 분석하고 이를 기반으로 스마트팩토리 보안요인 간의 우선순위를 도출하는 것을 목적으로 한다. 본 연구를 통해 스마트팩토리 환경에서 가장 중요하게 다뤄져야 하는 보안요소가 무엇인지 파악할 수 있고, 보다 안전하고 보안성이 뛰어난 스마트팩토리 구축에 기여할 수 있을 것이다.

Ⅱ. 이론적 배경

2.1 산업환경 변화와 스마트 제조업 시대

최근 산업환경은 다양한 기술의 융합화로 기업 간의 개별 경쟁에서 생태계 간 경쟁으로 시장의 경쟁구도가 변화하고 있다. 이른바 4차 산업혁명이라 일컫는 산업환경 변화는 디지털 혁명에 기반하여 디지털, 물리적, 생물학적 공간 영역의 경계가 희석되는 기술과 산업의 융합시대로의 변화를 말한다(김은 등, 2017). 제조업 선진국들은 4차 산업혁명을 적극 활용하여 자국의 제조업 부활을 본격적으로 추진하고 있으며, 이러한 4차 산업혁명은 ICT와 제조업이 융합된 스마트 제조업 시대로의 변화를 촉진하고 있다(유창현, 2017). 과거의 제조업은 생산효율 증진을 위한 단순 목적으로 공업적인 기술 혁신을 추구했다면, 스마트 제조업은 ICT와 융합하면서 제조 공정과 서비스의 형태를 변경하고 혁신의 가치를 증폭시키는 융・복합적인 플랫폼 형태로 변화하고 있다(전자신문, 2016). 4차 산업혁명 시대에는 제조업 기업들이 기존의 제조방식과 경영방식으로는 살아남기 어렵고 다양한 수요 구조를 반영하여 글로벌 경쟁력을 가질 수 있는 기술혁신 역량을 강화해야 한다(이무순, 손달호, 2017).

이렇듯 4차 산업혁명 시대를 맞아 제조업 혁신을 이루기 위해서 제조/생산 공장 시스템 및 기술을 새롭게 변화하도록 하는 스마트팩토리에 대한 관심이 증가하고 있다(Pagnon, 2017). 스마트팩토리를 통한 제조업 혁신을 위해, 우리나라를 비롯하여 선진 국가들과 주요 기업에서는 스마트 제조업으로의 변화를 위한 제조업 혁신 전략과 비전을 수립하고 있다. 스마트 제조업의 비전은 제조 공장이 공급망과 긴밀히 인터넷으로 연결되어 고객의 반응에 즉각적으로 대응하고, 제조 공정이 디지털화되어 데이터 자산을 ICT와 융합하여 지능화하며, 자원을 친환경・효율적으로 활용하고 생산된 제품이나 생산 시설이 사람에게 위해하지 않은 지속 가능성을 지원하는 제조업이 되도록 하는 것이다(이순열, 2016; 한국표준협회, 2018).

2.2 스마트팩토리 정의 및 특성

2.2.1 정의

스마트팩토리(또는 스마트공장)는 전통 제조업에 IoT와 같은 새로운 ICT를 결합하고 적용해서 모든 생산과정을 최적화하는 것으로서, 이를 통해 제조 경영 전반을 ICT 융합 공장 중심으로 혁신하는 것이다(Zuehlke, 2010; 강선준 등, 2019). 스마트팩토리의 구체적인 프로세스를 살펴보면, IIoT 기반의 기술을 적용해서 기계, 공정, 설비 등 공장 내부에 있는 모든 사물을 연결・감시하고, 발생되는 제조공정 상의 데이터를 관리・분석한 후, 실시간 동기화를 통해 현장 상황에 맞는 모델을 수립하고 활용하여 공장 운영의 최적화 모델을 구현하는 것이다(노상도, 2016). 기술 측면에서 스마트팩토리는 CPS(Cyber Physical System, 사이버물리시스템), IoT, AI(Artificial Intelligence, 인공지능), 스마트센서 등 다양한 ICT 신기술들이 핵심 구성요소로 제공되며 서로 융합・연결되는 혁신적인 플랫폼이다(강선준 등, 2019). 스마트팩토리의 CPS는 제품, 공정, 생산설비와 공장에 대한 물리적 공간과 사이버 공간의 통합 시스템으로, CPS는 제조공정에서 발생되는 데이터가 ICT를 통해 동기화

되고, 효율적인 공장 운영을 위해 생산계획 변경과 공정 상의 문제 및 개별 설비 장애 등의 상황을 스마트센서를 통해 인지하고 대응할 수 있도록 하는 시스템이다(노상도, 2016). 독일의 인더스트리 4.0과 미국의 IIoT 정책에서는 ICT 발전을 기반으로 한 CPS를 중심으로 IoT, Cloud, Big Data, Mobile, 즉, ICBM이 활용되는 것을 스마트팩토리의 핵심 개념으로 설명하고 있다(진상기, 박영원, 2017). 스마트팩토리는 ICT 융합기술을 생산 현장에 적용하여 기획부터 설계, 제품 상용화에 이르기까지 혁신을 통한 제조업의 경쟁력을 확보하도록 한다(김현 등, 2014; 이무순, 손달호, 2017). 한국의 민관합동 조직인 스마트공장추진단에서는 스마트팩토리를 “설비와 물류자동화를 기반으로 하여 공정 자동화, 공장에너지관리, 제품개발수명주기관리(PLM), 공급사슬관리(SCM), 전사적자원관리(ERP) 등의 시스템이 ICT를 이용하여 구현된 공장”이라고 정의하고 있다(산업통상자원부, 2015a; 서창성 등, 2018).

2.2.2 특성

스마트팩토리를 위해서는 IoT, Big Data, AI, CPS, Cloud Computing 등의 융합 기술을 기반으로 제조업의 혁신을 이끄는 스마트 제조라는 새로운 패러다임으로 변화해야 한다. 제조업에 ICT를 융합한 구조의 스마트팩토리는 시시각각 변화하는 4M1E(Man, Machine, Material, Method, Energy)의 생산자원에 대한 정보를 현장에서 실시간으로 취합하여 경영자의 의사결정을 위한 실시간 정보를 제공하고, 고객에게는 주문된 제품에 대한 정보를 제공하며, 공장 관리자에게는 공정 현장의 정보를 실시간으로 제공한다는 특성을 가진다(강정석, 조근태, 2018; 이현정 등, 2017; 차석근 등, 2015). 스마트팩토리의 실현을 위해서는 기계와 설비를 포함하는 모든 사물이 서로 네트워크로 연결되어 정보를 교환하고(IoT), 물리공간과 사이버공간이 유기적으로 융합되어 소통하며(CPS), 사물이 스스로 상황을 인지하고 판단할 수 있으면서(AI) 자율적으로 운영되고 상황에 적응하는 공장 시스템이 구축되어야 한다(산업통상자원부, 한국생산성본부, 2016).

스마트팩토리에서는 언제 어디서나 어떤 사물과도 연결되어 데이터를 주고받을 수 있는 네트워크 구성이 필수적이다. 즉, 제품이 생산되는 제조공정에 있는 수많은 기계와 공정라인 그리고 작업자 등이 ICT로 연결되어 정보를 교환하며 생산에 필요한 활동을 지원한다. 이러한 활동이 가능하기 위해서는 다양한 종류의 유무선 네트워크 기술을 이용하여 데이터를 효과적으로 송수신하고 원활하게 처리할 수 있는 네트워크 인프라가 구축되어야 한다(서창성 등, 2018). 과거에는 네트워크 인프라를 데이터를 송수신하는 유무선 형태의 라우터와 게이트웨이, 기지국 등의 장비만으로 인식하였으나, 최근에는 기술의 융합 및 장비 간 역할의 경계가 명확하지 않게 되면서 네트워크를 통한 데이터의 수집과 처리 그리고 저장을 위한 데이터센터까지 포괄하는 개념으로 확장되고 있다(김용운 등, 2016; 전승우, 2014). 공장 내·외부 네트워킹을 제공하는 유무선 네트워크는 모든 산업의 핵심으로 떠오른 IoT를 더욱 발전시키고 경쟁력을 향상시키기 위해 필수적이다(차석근, 2015). 스마트팩토리의 기술적 특징 중 하나는 이러한 네트워크를 구성하는데 있어, 공장에서 요구되는 수준의 가용성을 지원할 수 있도록 디바이스와 플랫폼·서비스 구성요소 간 연결성과 상호연동성이 보장되어야 한다는 것이다.

KEIT(한국산업기술평가관리원)에서 제시한 스마트팩토리 주요 전략기술의 특성을 살펴보면, 애플리케이션 측면에서는 스마트팩토리 혁신을 위한 지능화·네트워크화 된 제조현장의 시스템 요소와 실시간 연계하여 전 공장과 가치사슬의 최적 운영을 지원하는 고도화된 ICT 활용 및 응용 기술이 요구된다(이규택, 이건재, 2015). 또한, 플랫폼 측면에서는 제조 기계·자원·데이터 관리를 위한 공장 내·외부 플랫폼을 연동하는 운영·제어 플랫폼의 개발로 하위 스마트 디바이스와 상위 어

플리케이션에서 이를 활용하여 제품의 설계 및 가상 생산이 실공장 라인에서 연결되게 하는 기술이 요구된다(이규택, 이건재, 2015). 디바이스와 네트워크 측면에서는 제조환경을 고려한 다기능 센서 및 제어기 그리고 유무선 통신기술과 능동적 제조관리를 위한 특화된 디바이스 모듈 및 운용 기술이 필요하다. 또한, 상호 운용성과 보안 강화를 위해 스마트팩토리 주요 구성요소들의 데이터와 서비스 간의 운용 보장을 위한 통신・인터페이스의 규격 및 구성요소의 안정성, 가용성, 신뢰성 그리고 보안성 제공을 위한 기술 등이 필요하다(이규택, 이건재, 2015).

한편, IoT나 CPS 등의 새로운 기술은 네트워크로 연결을 확장해 주는 것과 동시에 스마트 팩토리에서의 보안에 대한 위협 또한 증가시킨다(Park *et al.*, 2020). 특히 스마트팩토리를 구성하고 있는 센서와 장비 그리고 설비는 대체로 컴퓨팅 성능이 단순하고 보안성도 취약한 경우가 많고 네트워크로 연결되어 있기에 공장 외부로부터의 해킹 등 보안 위험에 노출될 수 있다. 스마트팩토리 시대를 맞이하여 ICT 분야와 제조 분야 간 융복합화가 이루어지면서 융합보안 측면의 문제가 확산될 것으로 예상되므로, 스마트팩토리에서의 보안 강화는 필수적으로 다뤄야 할 과제이다(서혁준, 2016).

2.3 스마트팩토리 보안

스마트팩토리 추진을 통해 제조업 경쟁력을 강화할 수 있지만, 기반기술인 IoT를 활용함에 있어 가장 이슈가 되는 것은 보안이다. 스마트팩토리에서는 ICS에 첨단 ICT가 접목됨에 따라 다양한 종류의 사이버 공격에 의해 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)의 3가지 정보보안 목표가 위협받는 사례가 증가할 수 있다. 특히 제조업에서는 허가된 사용자가 시스템 자원을 필요로 할 때 큰 지체 없이 객체・자원에 접근하여 사용할 수 있는 가용성이 보장되어야 하는데, IoT를 통한 네트워크 연결 구조 시스템에서 어떻게 정보보안의 기밀성과 무결성을 유지하면서 동시에 제조업의 특성을 감안한 가용성을 보장할지는 스마트팩토리 보안에 있어서 어려운 문제이다.

공장시스템 보안에 대한 통계자료에 의하면, 스마트팩토리 도입 이전에도 이미 SCADA(Supervisory Control And Data Acquisition, 원격 감시제어 및 데이터 수집) 시스템의 네트워크 설정과 방화벽의 중요한 설정에 상당한 오류가 발견되었고, PLC(Programmable Logic Controller, 프로그래머블 로직 컨트롤러)와 같은 제어시스템의 32%가 DoS 및 DDoS 공격에 취약하다고 보고되었다(서혁준, 2016). 특히 현재 구축되고 있는 스마트팩토리는 새롭게 건설되는 공장들만을 대상으로 하는 것이 아니고 기존의 SCADA 시스템 등 ICS로 운영되던 공장도 대상으로 하고 있으므로, 기존 기계 설비들에 대한 보안요구 수준이 더욱 높아져야 한다.

스마트팩토리의 핵심기술인 IoT는 수많은 디바이스, 서비스, 사용자가 연계되어 유동적으로 생성하는 네트워크로 통합된 플랫폼에서 관리되므로, IoT 환경의 스마트팩토리에 대한 공격 형태는 기존보다 더욱 다양할 수 있다(최종석 등, 2017). 예를 들어, IoT를 통해 공장 내 시스템을 원격 제어하거나 원격 모니터링 하는 경우에 무선통신 등 취약점을 악용한 중요 정보 유출에 대한 위협이 증가할 수 있고, 만약 공장의 업무 네트워크나 ICS 네트워크에 악성코드가 감염되면 타 시스템으로의 감염 확산과 그로 인한 피해가 기하급수적으로 커질 수 있으므로 보안에 대한 위험관리가 보다 강화되어야 한다(한국인터넷진흥원, 2017).

최근 스마트팩토리 구축에 있어 클라우드 컴퓨팅이 도입되기 시작했는데, 클라우드 환경에서는 가상화 플랫폼의 하이퍼바이저를 통해 가상 서버가 상호 연결된 구조적 특성으로 인해 접근통제 분야의 보안대책이 더욱 필요하다(서창성 등, 2018; 손지연 등, 2015; 차영태, 2012). 스마트팩토리 접근통제 보안요소는 물리적, 관리적 그리고 기술적

보안 측면이 있는데, 스마트팩토리의 기기들이 대체로 컴퓨터 성능이 단순하고 보안성이 약하며 외부공격에 취약한 상태임을 감안할 때 기술적 보안이 IT 관리자 입장에서는 가장 중요한 보안요소라고 할 수 있다. 기술적 보안에는 서버 보안, PC 보안, 네트워크 보안, 통합 보안, 애플리케이션 보안 등이 있으며, 접근보안 소프트웨어, 암호화, 인증, 안티바이러스, 방화벽, IPS(침입방지시스템) 등의 기술적 보안 솔루션이 있다(이병권 등, 2016; 차영태, 2012).

스마트팩토리는 공장의 장비, 설비, 센서가 통신으로 연결되어 외부 해킹 등의 보안위협이 필연적으로 발생할 수 있으므로, 특히 외부 공격 및 해킹을 차단하기 위한 사이버보안 강화가 새로운 과제로 부상하고 있다(산업통상자원부, 2015a, 2015b; 한국인터넷진흥원, 2017). 스마트 제조업 시대의 도래로 ICT 분야와 제조업 분야의 활발한 융·복합화가 전개됨에 따라 기존 사이버공간의 보안 피해가 더 넓은 물리적·사이버 공간으로 확대되는 융합보안의 문제가 확산될 것으로 예상된다. 그러므로 센서와 IoT 기기, ICS 등이 공장 내·외부 생태계에 연결되는 스마트팩토리의 특성을 반영하여, 스마트팩토리에서 더욱 중요한 보안요인이 무엇인지 파악하고 그에 따른 보안대책 실현이 필요하다.

스마트팩토리의 주축을 이루는 솔루션과 관련한 중요 보안요인을 정리해 보면 다음과 같다. 첫째, 공장자동화 솔루션을 중심으로 한 스마트팩토리 구축이 있다. 공장에서의 자동화는 컴퓨터 설비 및 전자기술을 이용하여 기계화된 생산 공정을 조작하고 운영하는 것이다. 공장자동화 중심의 스마트팩토리에서는 자동조립기기, 수치제어 공작기계, 산업용 로봇 등을 이용하여 자동화 기기 및 미리 작성된 프로그램에 의하여 제품을 생산하는 무인화에 가까운 생산 공정 시스템 구축이 핵심이다(강정석, 조근태, 2018). 이러한 생산 장비 자동화 중심의 스마트팩토리 구축에 있어서 보안 측면에서 특히 유의해야 하는 것은 장비/기기 단의 보안이다. 컴퓨터 프로그램에 의해서 동작하는 자동화 기기에서 보안의 취약점을 틈탄 공격 방지 및 장비 가동중지 등의 문제가 발생하지 않도록 기기 사용에 대한 사용자 인증 강화, 암호화, 비상전원 강화, 필수장비 이중화 등이 중요할 것이다(이병권 등, 2016; 이승환 등, 2019).

둘째, 원격자동제어 시스템 강화 측면에서의 스마트팩토리 구축이 있다. 최근, 제조업의 기존 자동제어 시스템에 스마트 센서, IoT, CPS, 클라우드 컴퓨팅 등 정보기술을 적용하여 기존 대비 한 단계 상승한 원격제어 시스템 구축 솔루션이 적용되고 있다(강정석, 조근태, 2018). 특히 ICS의 효율적 관리를 위해 외부기기를 통한 접속이 증가하고 폐쇄적인 망구성 형태에서 개방적인 망구성 형태로 변경되는 경우도 많아지고 있다(배춘석, 고승철, 2019; 진상기, 박영원, 2017). 이 경우, 공장의 생산자동화제어시스템이 외부 네트워크와 연결됨에 따라, 현재 인터넷망 연결 환경에서 빈번하게 발생하고 있는 보안 사고의 문제점이 나타날 수 있다(손경호, 2014; 오준형 등, 2017). 일례로, 호주에서는 퇴사 직원이 무선 네트워크를 이용하여 폐수처리공장 제어시스템을 불법적으로 해킹하여 오작동을 유발시킨 사례가 있었다(이승환 등, 2019). 이러한 경우, 보안측면에서 특히 유의해야 하는 것은 네트워크 보안이다(Lee *et al.*, 2020; 강선준 등, 2019; 이승환 등, 2019). 즉, 인터넷 및 외부 네트워크를 통한 보안 위협을 막기 위하여, 보안 프로토콜 사용, 네트워크 경계 보호, 방화벽 및 라우터 설치 강화, 보안관제 네트워크 로그 체크 강화 등이 중요할 것이다(강선준 등, 2019). 또한, 기기/장비에 대한 원격접근 통제 및 서비스에 대한 접근권한 통제 강화 등이 필요할 것이다(이병권 등, 2016).

셋째, 공급가치사슬 통합관리 체계 구축을 위한 스마트팩토리 솔루션을 도입할 수 있다. 제조기업들은 스마트팩토리 구축을 통해 공급가치사슬 전체가 마치 하나의 공장처럼 실시간 연동되고 통합되는 생산체계를 갖추고자 한다(강정석, 조

근태, 2018) 스마트팩토리 표준화 로드맵에서는 제품의 기획 및 설계, 제조 공정, 유통 판매 등의 전체 공급사슬 과정을 ICT로 통합/연계되는 생산체제를 갖춤으로써, 시장 변화에 대한 적기 대응 생산과 맞춤형 제조가 가능하도록 지향하고 있다(차석근, 2016). 이를 위해서는 공급가치사슬 상 연계되는 협력 기업들의 설비 및 시스템들이 유기적으로 서로 연결되고 상호 소통되며 지능적으로 운영되는 협력 플랫폼을 갖춰야 한다(강선준 등, 2019; 강정석, 조근태, 2018; 김은영, 박문수, 2018; 이규택, 이건재, 2015). 그런데, 이 경우 한 회사에서의 악성코드 감염과 해커 침입으로 인한 피해 여파가 통합적으로 연계된 다른 회사로 전파될 수 있는 위험이 커질 수 있으므로, 특히 통합/연계된 플랫폼 및 서비스 단의 보안이 중요하게 된다. 이를 위해서는 플랫폼 및 서비스에 대한 사용자 관리와 패스워드 관리, 접근권한 통제 등이 이뤄져야 하며, 안전한 플랫폼 운영을 위한 악성코드 관리, 서비스 사용 모니터링 및 로그 기록과 보존 관리 등이 필요하다(이승환 등, 2019).

넷째, 실시간 데이터 수집/분석 강화를 통한 의사결정 지원 측면의 스마트팩토리 구축을 추진할 수 있다. 스마트팩토리 구축에 있어서, 4M1E 현장의 각종 데이터를 스스로 수집하고 실시간으로 분석하는 솔루션을 적용함으로써 효과적인 의사결정을 지원할 수 있다(Park *et al.*, 2020; 강정석, 조근태, 2018). 이를 위해 제조/생산과 관련된 정보 및 현장 디바이스로부터 데이터를 수집/분석하여 판단할 수 있는 시스템을 구성하고, 분석 및 판단 결과가 다시 제조현장에 반영할 수 있도록 하는 효율적인 데이터 채널 네트워크 및 플랫폼이 구축되어야 한다(강정석, 조근태, 2018; 차석근, 2016). 이 경우, 디바이스, 네트워크, 플랫폼 단의 보안이 모두 고려되어야 한다.

이와 같이 스마트팩토리 구축을 위한 여러 솔루션이 있으며, 회사 규모 및 스마트팩토리 구축 전략에 따라 이들 솔루션을 단계적・점진적으로 적용하거나 종합적으로 적용할 수 있다. 상기에서 살펴본 것과 같이, 스마트팩토리에서의 보안을 전반적으로 강화하기 위해서는 디바이스, 네트워크, 플랫폼 및 서비스 측면의 보안요인들이 고루 검토되어야 한다.

Ⅲ. 연구방법론

3.1 연구 모델 개발-스마트팩토리 보안요인의 계층화된 분류 모델

본 연구에서는 스마트팩토리에서 필요한 보안요인 도출을 위해, 제Ⅱ장에서 분석한 기존문헌 조사와 함께 IoT 및 산업보안 관련 보안 가이드라인 및 표준 문서(<표 1> 참조)를 조사 분석하였다. 이러한 조사를 바탕으로 해외 사례들과 비교하여 국내 실정에 맞게 스마트팩토리 구축・운용 시 필요한 주요 보안요인들을 도출하도록 하였다.

〈표 1〉 보안 가이드라인 및 표준 관련 문서

보안 가이드라인/ 표준 문서	주요 내용
IEC 62443	산업망 네트워크 및 시스템 보안
ISA 99	제조 및 제어 시스템 보안
NAMUR BNA115	산업자동망 시스템 IT 보안
ISO/IEC 15408	IT 보안의 평가 척도
ISO 27000	정보보호 관리시스템 국제표준체계
VDI/VDE 2182	산업자동화를 위한 정보보안
NISTSP 800-82	산업제조시스템 보안 가이드
NISTIR 7628	스마트 그리드 사이버 보안 가이드라인

출처: 산업통상자원부(2015a).

도출한 보안요인들을 크게 3가지 범주인 '디바이스 보안', '네트워크 보안', '플랫폼 및 서비스 보안'으로 계층 1을 분류하고, 범주별 하위요소(계층 2 요인)들을 파악하였다. 기존문헌 및 보안 관련 표준과 가이드라인을 토대로 연구자가 도출한 스마트팩토리에서의 보안요인 구성의 타당성

을 확인하기 위해, 정보시스템 및 보안 전공 교수 3명과 스마트팩토리 및 보안 분야 전문가 3명을 대상으로 한 인터뷰를 통해 3가지 영역과 그 하위 계층의 보안요인이 적절한지 검증하였다. 이를 기반으로 본 연구에서는 '스마트팩토리 보안요인들의 중요도 및 우선순위 평가를 위한 계층화된 분류 모델'을 <표 2>와 같이 구성하였다.

3.2 연구방법론 및 데이터 수집

본 연구에서는 AHP(Analytic Hierarchy Process) 기법을 사용하여 스마트팩토리에서 중요하게 다뤄야 할 보안요인들의 중요도 및 우선순위를 분석하였다. AHP는 계층적 분석 방법으로서 평가요소가 여러 개 있을 때 다기준(multi-criteria) 하에서의 우선순위를 선정하는 기법이며, 정보시스템 연구에서 광범위하게 사용되고 있다(Ngai, 2003). 이러한 AHP 기법을 통해 계층별 평가요소들을 쌍대비교해서 상대적 가중치(중요도)를 구할 수 있고 계층별 종합 중요도 평가치를 계산할 수 있어, 이를 통해 우선순위를 도출할 수 있다(경태원, 김상국, 2007; 김근형, 2019). 본 연구의 목적이 스마트팩토리에서의 보안요인을 확인하고 보안요인들 간의 중요도 기반 우선순위를 도출하는 것이므로, AHP 기법은 본 연구에 적합한 방법론이다.

본 연구에서는 AHP를 통해 중요도 및 우선순위를 도출했던 기존문헌(경태원, 김상국, 2007; 김대진, 홍일유, 2014)의 분석과정을 참조하여, AHP를 통한 분석을 4단계 과정으로 수행하였다. 첫째, 중요도 의사결정 대상 요인들의 위계적 계층구조를 구성하였다. 둘째, 요인들 간에 9점 척도의 쌍대비교를 통하여 정량적 판단 자료를 수집하였다. 즉, 평가 대상 보인요인들을 쌍으로 묶어 1:1 쌍대비교 평가를 진행토록 하였다. 비교 평가 시, 두 요인 중 상대적으로 '더 중요한 요소'에 대해 '더 중요한 정도'를 9점 척도(극히 많이>대단히 많이>아주 많이>매우 많이>많이>상당히>약간>조금>동등)로 측정하였다. 셋째, 요인들 간의 상대적 중요도를 구하였다. 이 과정에서 설문자의 일관성 지수를 평가하여 설문 데이터의 신뢰성을 확인하였다. 일반적으로, 일관성 비율(Consistency Rate, CR)이 10% 이하이면 적합한 것으로 판단한다(김대진, 홍일유, 2014). 넷째, 평가대상이 되는 여러 요인들에 대한 종합 순위(종합 평가치)를 얻기 위하여 요인들의 상대적 중요도를 종합하였다.

〈표 2〉 스마트팩토리 보안요인의 계층적 분류 모델

계층 1	계층 2
디바이스 (기기/장비) 보안	암호화
	사용자 인증 식별
	비상전원 강화
	필수장비 이중화
	디바이스 운용의 환경통제 강화
	원격접근 통제
네트워크 보안	화이트리스트 정책
	방화벽 및 라우터 설치
	DMZ(DeMilitarized Zone) 사용
	정적주소 사용
	보안 프로토콜 사용
	네트워크 경계 보호 강화
	적절한 보안관제 네트워크 로그 사용
플랫폼 및 서비스 보안	바이러스 백신 사용
	패스워드 관리 강화
	접근권한 통제
	사용자 관리
	서비스 로그 관리
	침입 탐지 소프트웨어 설치 관리
	서비스 암호화

또한, 본 연구에서는 스마트팩토리에서의 보안요인 중요도를 아래와 같은 절차로 분석하였다.

1) 계층 1 요인들의 중요도 분석
2) 계층 1별 하위 계층 2 요인들의 중요도 분석
   • 디바이스 보안(계층 1)의 하위 계층(계층 2) 보안요인들에 대한 중요도 분석

- 네트워크 보안(계층 1)의 하위 계층(계층 2) 보안요인들에 대한 중요도 분석
- 플랫폼 및 서비스 보안(계층 1)의 하위 계층(계층 2) 보안요인들에 대한 중요도 분석

3) 최하위계층(계층 2) 기준의 통합 중요도 분석

본 연구에서는 중요도를 객관적으로 평가해 줄 수 있는 스마트팩토리 및 보안 분야 전문가를 대상으로 중요도 평가 설문조사를 실시하여 스마트팩토리 보안요인 중요도를 실증적으로 분석하도록 하였다. 구체적으로 본 연구의 대상자는, (1) 민관합동 스마트공장추진단(스마트제조혁신추진단)에 소속·위촉된 기술위원, (2) 스마트공장추진단에 파견되었거나 스마트팩토리 보급·확산을 위해 수요기업의 사업 점검 및 자문을 수행하는 경력 10년 이상의 사업전문가, (3) ISMS(Information Security Management System, 정보보호관리체계) 인증심사원 등의 보안 관련 자격 및 박사학위가 있는 보안전문가를 대상으로 하였다. 특히, 본 연구에서는 중요도 평가 시 전문가 그룹별 차이점 유무를 검토하기 위하여, 전문가의 소속 및 역할 분야 그룹(기술위원, 사업전문가, 보안전문가)별 스마트팩토리 보안요인 중요도를 비교 분석하여 집단별 차이점이 있는지 파악하도록 하였다.

본 연구에서는 26명의 전문가를 대상으로 중요도 평가에 대한 설문조사를 실시하였는데, 이 중 설문조사 응답을 완료하지 않은 2개의 데이터를 제외한 후 24개의 전문가 응답 데이터를 최종 분석 데이터로 설정하였다. 본 연구의 응답자 분포는 <표 3>과 같다.

〈표 3〉 응답자 분포

전문가 그룹 구분	응답 수 (명)
기술위원	12
사업전문가	6
보안전문가	6
합계	24

Ⅳ. 분석 결과

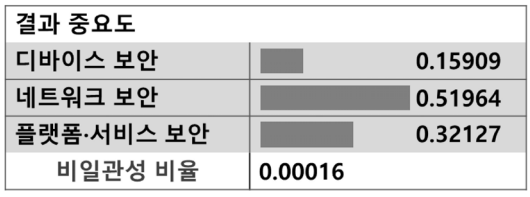
본 연구에서는 AHP 솔루션인 '아이메이크잇(I Make It)' 소프트웨어를 이용하여 데이터를 수집하고 분석하였다. '아이메이크잇(I Make It)'은 기존에 많이 사용되어 온 '엑스퍼트 초이스(Expert Choice)'를 대체하여 온라인 환경에서 사용할 수 있도록 지원하는 AHP 소프트웨어이다. 아이메이크잇(I Make It) 시스템은 설문에 참여한 응답자의 일관성 비율(CR) 값을 확인할 수 있도록 지원한다. 본 연구에서의 일관성 비율(CR) 확인 결과, 모든 일관성 비율(CR)이 임계치인 0.1(10%)을 초과하지 않아, 설문 대상자의 응답에 대한 신뢰성이 확보되었다.

4.1 스마트팩토리 보안요인 중요도 및 우선순위 분석 결과

본 연구에서 제안한 <표 2>의 계층적 모형의 요인들을 쌍대 비교하여 요인의 중요도를 계산하고 우선순위를 분석한 결과는 다음과 같다.

4.1.1 계층 1 요인들의 상대적 중요도 분석 결과

계층 1 요인들의 상대적 중요도를 분석한 결과(<그림 1> 참조), 네트워크 보안 > 플랫폼 및 서비스 보안 > 디바이스 보안 순으로 중요도가 평가되었다. 즉, 네트워크 보안이 가장 중요한 것으로 분석되었다.



〈그림 1〉 계층 1 요인 중요도 분석 결과

4.1.2 계층 1별 하위 계층 2 요인들의 중요도 분석 결과

계층 1(디바이스 보안, 네트워크 보안, 플랫폼 및 서비스)별 계층 2 보안요인들에 대한 상대적 중요도 평가 결과는 아래 <그림 2>와 같다.

디바이스 보안 측면(계층 1)의 하위 계층(계층 2) 보안요인들에 대한 중요도 분석 결과, 사용자인증 식별 > 원격접근 통제 > 암호화 > 필수장비 이중화 > 환경통제 강화 > 비상전원 강화 순으로 중요도가 평가되었다.

네트워크 보안 측면(계층 1)의 하위 계층(계층 2) 보안요인들에 대한 중요도 분석 결과, 방화벽 및 라우터 설치 > 네트워크 경계 보호 강화 > 보안 프로토콜 사용 > 적절한 네트워크 로그 사용 > DMZ 사용 > 정적주소 사용 > 화이트리스트 정책 순으로 중요도가 평가되었다.

플랫폼 및 서비스 보안 측면(계층 1)의 하위 계층(계층 2) 보안요인들에 대한 중요도 분석 결과, 접근권한 통제 > 패스워드 관리 강화 > 침입 탐지 소프트웨어 설치 관리 > 사용자 관리 > 서비스 암호화 > 서비스 로그 관리 > 바이러스 백신 사용 순으로 중요도가 평가되었다.

4.1.3 최하위 계층(계층 2) 기준의 통합 중요도 분석 결과

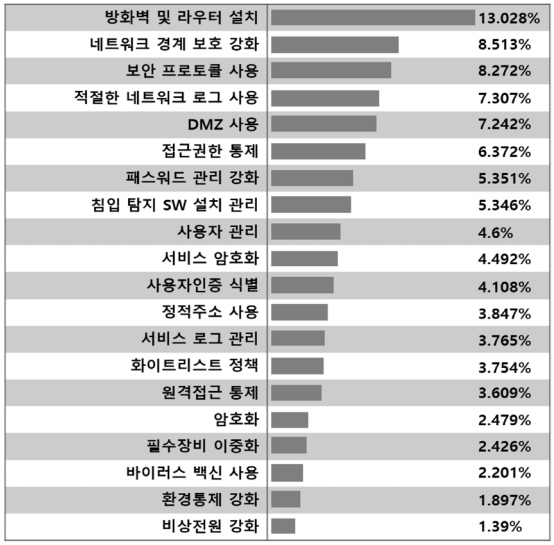
계층 2 모든 요인들에 대한 통합 중요도 분석 결과는 <그림 3>과 같다. 중요도 평가 결과, 방화벽 및 라우터 설치 > 네트워크 경계 보호 강화 >

디바이스 보안	
결과중요도	
암호화	0.15583
사용자인증 식별	0.25822
비상전원 강화	0.08738
필수장비 이중화	0.15247
환경통제 강화	0.11925
원격접근 통제	0.22686
비일관성 비율	0.00234

네트워크 보안	
결과중요도	
화이트리스트 정책	0.07225
방화벽 및 라우터 설치	0.25071
DMZ 사용	0.13936
정적주소 사용	0.07404
보안 프로토콜 사용	0.15919
네트워크 경계 보호 강화	0.16383
적절한 네트워크 로그 사용	0.14062
비일관성 비율	0.00596

플랫폼·서비스 보안	
결과중요도	
바이러스 백신 사용	0.0685
패스워드 관리 강화	0.16657
접근권한 통제	0.19833
사용자 관리	0.14319
서비스 로그 관리	0.11719
침입 탐지 SW 설치 관리	0.16641
서비스 암호화	0.13982
비일관성 비율	0.00699

〈그림 2〉 계층 1별 하위 계층 2의 보안요인 중요도 분석 결과



〈그림 3〉 계층 2 전체 요인들의 중요도 분석 결과

보안 프로토콜 사용 > 적절한 네트워크 로그 사용 > DMZ 사용 > 접근권한 통제 > 패스워드 관리 강화 > 침입 탐지 소프트웨어 설치 관리 > 사용자 관리 > 서비스 암호화 > 사용자인증 식별 > 정적주소 사용 > 서비스 로그 관리 > 화이트리스트 정책 > 원격접근 통제 > 암호화 > 필수장비 이중화 > 바이러스 백신 사용 > 환경통제 강화 > 비상전원 강화 순으로 중요도가 나타났다.

4.2 전문가 그룹별 중요도 비교 분석 결과

3개의 전문가 그룹(기술위원, 사업전문가, 보안전문가)별 차이점이 있는지 파악하기 위하여, 그룹별 보안요인 중요도를 분석하였다. 분석 결과, 기술위원 그룹과 사업전문가 그룹은 대체로 유사한 결과를 보였으나 보안전문가 그룹은 다른 결과를 보이는 것이 있었다.

4.2.1 그룹별 계층 1 요인의 중요도 분석 결과

전문가 그룹별 계층 1의 평가요인별 상대적 중요도와 우선순위를 살펴보면, 먼저 기술위원 그룹에서는 네트워크 보안 > 플랫폼 및 서비스 보안 > 디바이스 보안 순으로 나타나 네트워크 보안의 중요도가 가장 높게 평가되었다.

사업전문가 그룹의 중요도 평가 결과도 네트워크 보안 > 플랫폼 및 서비스 보안 > 디바이스 보안 순으로 나타났다. 사업전문가 그룹의 결과는 기술위원 그룹과 요인별 중요도 값은 차이가 나지만, 중요도의 우선순위는 동일하였고 네트워크 보안의 중요도가 가장 높았다.

보안전문가 그룹의 중요도 순위 평가 결과는 앞의 두 그룹과 다르게 나타났는데, 플랫폼 및 서비스 보안 > 네트워크 보안 > 디바이스 보안 순으로 나타났다. 즉, 보안전문가 그룹에서는 플랫폼 및 서비스 보안의 중요도가 가장 높게 평가되었다.

이러한 3개 그룹의 계층 1 요인에 대한 중요도 우선순위 분석 결과를 비교 정리하면 <표 4>와 같다.

4.2.2 그룹별 계층 1의 하위 계층 2 요인들의 중요도 분석 결과

그룹별 계층 1의 하위 계층 2 요인들의 중요도와 우선순위를 분석한 결과, 먼저 디바이스 보안의 하위요인에 대한 평가 결과는 <표 5>와 같이 나타났다. 분석 결과, 기술위원 그룹에서는 사용자인증 식별이 우선순위가 가장 높은 보안요인으로 평가되었고 비상전원 강화가 가장 낮게 나타났다. 사업전문가 그룹에서는 암호화가 가장 우선하는 보안요인이었고 비상전원 강화가 가장 낮았으며, 보안전문가 그룹에서는 원격접근 통제가 가장 우선시되는 보안요인이었고 비상전원 강화가 가장 낮은 순위를 보였다.

다음으로, 그룹별 네트워크 보안요인의 하위요인에 대한 중요도 평가 결과를 비교 분석하였다. <표 6>의 결과를 살펴보면, 모든 그룹에서 공통적으로 방화벽 및 라우터 설치가 가장 중요한 요인으로 평가된 것을 알 수 있다. 반면, 가장 낮은 순위의 요인으로 분석된 것은, 기술위원 그룹에서는 화이트리스트 정책이었고, 사업전문가와 보안전문가 그룹에서는 정적주소 사용이 가장 낮게 나타났다.

〈표 4〉 그룹별 계층 1 요인의 중요도 분석 결과

계층 1 보안요인	기술위원		사업전문가		보안전문가	
	중요도	우선순위	중요도	우선순위	중요도	우선순위
디바이스 보안	0.154	3	0.10279	3	0.21446	3
네트워크 보안	0.51978	**1**	0.72806	**1**	0.30255	2
플랫폼 및 서비스 보안	0.32622	2	0.16916	2	0.48299	**1**

〈표 5〉 그룹별 디바이스 보안요인 중요도 분석 결과

디바이스 보안요인	기술위원		사업전문가		보안전문가	
	중요도	우선순위	중요도	우선순위	중요도	우선순위
암호화	0.14765	4	0.25649	**1**	0.09564	4
사용자인증 식별	0.23217	**1**	0.24961	2	0.29338	2
비상전원 강화	0.1052	6	0.06819	6	0.06789	6
필수장비 이중화	0.17509	3	0.11206	5	0.14695	3
환경통제 강화	0.14206	5	0.12569	4	0.07462	5
원격접근 통제	0.19782	2	0.18796	3	0.32152	**1**

〈표 6〉 그룹별 네트워크 보안요인 중요도 분석 결과

네트워크 보안요인	기술위원		사업전문가		보안전문가	
	중요도	우선순위	중요도	우선순위	중요도	우선순위
화이트리스트 정책	0.05369	7	0.06969	6	0.13452	4
방화벽/라우터 설치	0.21066	**1**	0.36987	**1**	0.23762	**1**
DMZ 사용	0.15926	4	0.11147	5	0.12073	6
정적주소 사용	0.0812	6	0.06936	7	0.05758	7
보안 프로토콜 사용	0.17924	2	0.14779	2	0.12518	5
네트워크 경계 보호 강화	0.17238	3	0.11745	3	0.17818	2
적절한 네트워크 로그사용	0.14358	5	0.11436	4	0.14619	3

〈표 7〉 그룹별 플랫폼 및 서비스 보안요인 중요도 분석 결과

플랫폼 및 서비스 보안요인	기술위원		사업전문가		보안전문가	
	중요도	우선순위	중요도	우선순위	중요도	우선순위
바이러스 백신 사용	0.06971	7	0.06583	7	0.06468	7
패스워드 관리 강화	0.17183	2	0.18674	2	0.12711	3
접근권한 통제	0.16252	3	0.20668	**1**	0.27538	**1**
사용자 관리	0.13907	5	0.1667	3	0.11986	4
서비스 로그 관리	0.13541	6	0.10498	6	0.08923	6
침입 탐지 SW 설치관리	0.14828	4	0.14398	4	0.23095	2
서비스 암호화	0.17317	**1**	0.12509	5	0.0928	5

끝으로, 그룹별 플랫폼 및 서비스 보안요인의 하위요인에 대한 중요도 평가 결과를 비교 분석하였다. <표 7>에 정리된 평가결과를 보면, 기술위원 그룹에서는 서비스 암호화가 가장 우선순위가 높은 보안요인으로 나타났고, 사업전문가와 보안전문가 그룹에서는 접근권한 통제가 가장 우선순위가 높았다. 또한, 모든 그룹에서 공통적으로 바이러스 백신 사용이 가장 낮은 순위의 보안요인으로 나타났다.

V. 결 론

본 연구는 스마트팩토리에서의 중요한 보안요인이 무엇인지 파악하기 위하여, 단말/네트워크/플랫폼・서비스 범주별 세부 보안요인들을 분류하고 이들의 중요도를 분석하였다. 연구 결과, 3가지 계층 1 요인 중, 네트워크 보안이 가장 중요하게 평가되었으며, 다음으로 플랫폼 및 서비스 보안, 디바이스 보안 순이었다. 결과를 종합해 보면, 스마트팩토리 운영을 위해서 필요한 보안요인 중 가장 우선적으로 고려할 사항은 계층 1에서는 네트워크 보안요인이고, 네트워크 보안 하위 계층 2 요인에서는 공통적으로 방화벽 및 라우터 설치의 요인이 가장 중요하게 다뤄져야 할 요인으로 파악되었으며, 네트워크 경계 보호 강화 및 보안 프로토콜 사용도 중요한 보안요인임을 알 수 있었다. 플랫폼 및 서비스 보안요인에서는 접근권한 통제가 가장 우선시 되는 보안요인이며, 패스워드 관리 강화 및 침입 탐지 소프트웨어 설치 관리 또한 상당히 중요한 요인으로 파악되었다. 또한, 서비스 암호화 측면은 기술위원 전문가 집단에서 1순위의 보안요인으로 평가된 만큼, 이 또한 주의할 보안요소이다. 디바이스 보안에서는 사용자인증 식별이 가장 중요하게 다뤄질 보안요인으로 파악되었고, 원격접근 통제 및 암호화 또한 상대적으로 중요한 요인으로 분석되었다.

단, 이러한 중요도 평가는 전문가 그룹별로 다소 상이한 결과를 보인 부분도 있었다. 특히 보안전문가 그룹은 기술위원 및 사업전문가 그룹과 달리, 계층 1 범주에서 플랫폼 및 서비스 보안 측면을 가장 중요하게 평가하였다. 계층 2 보안요인 중요도 평가에서도 그룹 간 차이 나는 부분이 존재했다. 하지만, 이들 세부 요인들에 대한 중요도 평가 시, 랭킹 3~4위 안에 드는 상위권 요인들은 대체로 일치하였다. 이와 같이 전문가 그룹별 차이점이 다소 있음에도 전반적인 평가에서 우선 시되는 공통 요인이 파악되었으므로 이들을 우선으로 보안을 점검하도록 해야 할 것이다. 또한, 기업/조직 시스템에 대한 보안 인증 및 점검을 위주로 활동하는 보안전문가 그룹의 계층 1 요인 평가 결과가 달랐다는 점은, 향후 스마트팩토리의 보안에 대한 인증/점검에 있어 우선 검토될 체크리스트 설정 시 관련 전문가들의 종합적인 의견을 반영할 필요가 있음을 시사한다.

본 연구를 통한 학문적・실무적 공헌과 기대효과는 다음과 같다.

본 연구 결과를 토대로, 4차 산업혁명과 스마트제조업 시대를 맞아 제조업의 경쟁력을 높일 수 있는 정책으로 추진하고 있는 스마트팩토리 구현에 있어 가장 중요한 과제 중 하나인 보안 측면에서 중요하게 검토해야 할 요소들을 정의할 수 있다. 스마트팩토리는 ICS에 첨단 ICT가 접목된 형태로 구축되고 있어 신기술의 다양한 장점을 활용할 수 있는 반면, ICT 기술들이 융・복합되어 통신 프로토콜을 사용하는 기계들로 구성된 공정과 개방적 네트워킹 시스템에서 운용되는 점을 제대로 고려하지 않으면 정보보안 문제가 발생할 가능성이 높다. 최근 들어 기업의 정보를 대상으로 시스템 감염 및 비인가 접근 등 다양한 정보보안 공격들이 증가하고 있는데, 이러한 공격 시도를 미리 차단하기 위해서는 단순하게 개별 디바이스에 대한 보안만이 아니라 네트워크와 플랫폼・서비스에 대한 보안이 필요하다. 본 연구는 기존의 폐쇄적 공장 시스템과 다른 스마트팩토리의 특성을 고려하여, 디바이스 보안, 네트워크 보안, 플랫폼・서비스 보안의 3가지 측면에서 스마트팩토리에서 특히 중요한 보안요인이 무엇인지 구조화할 수 있도록 하였다.

본 연구에서는 보안요인들을 계층화하고 AHP 기법을 활용하여 객관적인 전문가 그룹을 대상으로 요인 간 중요도를 파악하였으며, 기술위원, 사업전문가, 보안전문가 그룹별로 중요도의 차이점을 비교 분석하였다. 이를 통해, 특히 보안시스템 인증/점검을 위주로 하는 보안전문가 그룹의 평가결과가 사업전문가 및 기술위원과 다른 점이 있음을 알 수 있었고, 이로써 다양한 전문가 그룹의

의견을 고루 반영한 종합적인 스마트팩토리 보안 인증·점검 지침 수립이 필요함을 거증하였다.

또한, 정성적 보안요인들을 보다 객관적으로 평가하고 우선순위화하여 제시함으로써, 보안 에 대한 전문인력이 상대적으로 부족한 중소·중견 기업에서도 스마트팩토리 보안의 필수적인 핵심 준수사항이 무엇인지 참조할 수 있도록 하였다.

스마트팩토리는 제조산업 혁신을 위해서 앞으로 더욱 확대될 분야이며, 특히 중소제조기업의 경쟁력 강화 측면에서 더욱 필요하다. 스마트팩토리 구축에 따른 중소기업 경쟁력 변화에 대한 조사 자료에 의하면, 중소제조기업에서 스마트팩토리를 구축함으로써 생산성 개선, 불량률 감소, 납기 단축 등 실제 경쟁력이 향상된 것으로 나타났다(최영환, 최상현, 2018). 그러나 경쟁력을 높이기 위한 스마트팩토리 구축에 있어 보안이 제대로 검토되지 않고 적용·확산된다면, 해당 기업뿐만 아니라 공급가치사슬 연계 기업 및 산업 전체적으로 큰 손실이 발생할 수 있다. 이와 같이 스마트팩토리의 보안이 중요함에도 불구하고, 특히 중소제조기업에서는 공장에서의 보안의 필요성에 대한 인식이 아직 부족하고 보안에 대한 투자 여력 또한 한계가 있다. 특히 대기업 주도형 성장 중심의 국내 산업구조 특성으로 인해 스마트팩토리와 보안 체계 구축에 있어 중소기업의 어려움이 존재하고 이에 대한 지원이 필요하다. '4차 산업혁명 시대의 제조업의 귀환'(김은 등, 2017)이라는 문구와 같은 제2의 제조업 붐이 다시 이뤄지기 위해서는 대기업과 중소기업이 모두 상생할 수 있는 스마트팩토리 구축이 추진되어야 하며, 이는 정부 및 지자체 차원에서도 중요한 과제일 것이다. 최근 정부 및 지자체에서는 ICT 결합을 통한 제조혁신을 위해 생산 시스템의 개방화로 전환될 수 있도록 특히 지역 제조기업 및 중소기업들의 스마트팩토리 구축을 지원하고 있다(최영환, 최상현, 2018). 단, 이를 위해서는 보안체계 구축 지원이 함께 수반되어야 하고, 본 연구결과에서 검증된 것과 같이 우선순위가 높은 보안요인들이 필수적으로 보강되어야 한다. 그러므로 스마트팩토리 추진 및 지원 사업에 있어서 필수적인 보안체계가 갖춰진 스마트팩토리가 구축될 수 있도록 실효성 있는 추진방안이 필요하다. 예를 들어, 중소기업 같이 보안 시스템에 대한 검토 여력이 부족한 경우, 본격적인 스마트팩토리 구축 전 보안체계 정립을 위한 사전 컨설팅 및 교육 서비스를 시행함으로써 공장에서의 보안의 중요성에 대한 이해도를 높이고 필요 시 관련 솔루션을 소개해 주는 연속적인 서비스를 제공할 수 있을 것이다. 특히 아직까지 제조기업에서는 자사 단위 공장에 스마트팩토리 솔루션을 적용하는 경우가 많고, 공급가치사슬이 연결된 기업 간 협력 플랫폼을 고려한 보안체계 구축이 미흡하므로 이에 대한 새로운 보안 컨설팅 서비스가 필요할 것이다. 또한 스마트팩토리에서의 단말/네트워크/플랫폼 단의 보안 위협과 공격이 날로 진화하고 있기에 이에 대응한 특화된 스마트팩토리형 ICT 보안 솔루션 개발 및 창업을 촉진하는 정책을 추진할 수 있을 것이다.

본 연구는 몇 가지 한계점이 있다. 첫째, 본 연구에서는 단말/네트워크/플랫폼·서비스 범주를 중심으로 보안요인들의 중요도 및 우선순위를 제시하였다. 한편, 이러한 우선순위는 스마트팩토리를 구축하려는 기업의 규모(대/중견/중소 기업) 및 스마트팩토리 구현 수준(기초, 중간, 고도화)에 따라 달라질 수도 있을 것이다. 즉, 스마트팩토리를 구축하려는 기업의 시스템 형태나 구성에 따라 필요한 보안요인이 달라질 수 있으므로, 향후 연구에서는 이를 감안한 우선순위화를 검토해 볼 수 있을 것이다. 둘째, 본 연구는 AHP를 통해 스마트팩토리 보안요인의 우선순위를 도출한 탐색적 연구로서, 인과적 연구에서와 같이 보다 정밀한 분석 타당성 검증 측면의 보완이 필요하다. 향후 연구에서는 중요도가 높게 나타난 주요한 요인들이 어떻게 결과 변인에 영향을 미치는지 보다 정밀한 연구 모델을 설정하여 분석해 볼 필요가 있다. 셋째, 최근 디지털 트윈, 증강 분석, 지능형 사물, 엣지 컴퓨팅, 분산 클라우드, AI 보안 등 새롭게 진화

된 기술들이 등장하면서 스마트팩토리 구축에 활용될 수 있는 ICT 기술 또한 진화되고 있다. 따라서 앞으로의 연구에서는 새롭게 도입될 신기술을 대상으로 관련 보안요인들을 지속적으로 추가 검토할 필요가 있다.

결론적으로, 본 연구는 스마트팩토리 구축에 있어 현실적으로 발생할 수 있는 보안의 위협요인을 파악하고 이에 대비한 주요 보안요인이 무엇인지 제시하였다. 본 연구 결과는, 앞으로 더욱 확산될 스마트팩토리가 보다 안전하게 구축・운용될 수 있도록 스마트 제조업 시대에 필요한 정보보안 확보에 기여할 수 있을 것이다.

참 고 문 헌

[1] 강선준, 오정미, 오승연, "ICT융합보안 시대의 스마트 팩토리 보안", *한국기술혁신학회 학술대회논문집*, 2019, pp. 625-643.

[2] 강정석, 조근태, "자동화 및 스마트 공장 구축에 대한 정부 지원사업의 효과 분석", *기술혁신학회지*, 제21권, 제2호, 2018, pp. 738-766.

[3] 경지훈, 김종수, "IT 보안 서비스 품질의 측정 방법에 관한 연구: 정량 지표의 사용 가능성", *산업경영시스템학회지*, 제38권, 제4호, 2015, pp. 30-38.

[4] 경태원, 김상국, "AHP 기법을 이용한 IT 프로젝트 관리 우선순위 수립에 대한 연구", *Information Systems Review*, 제9권, 제3호, 2007, pp. 157-181.

[5] 김근형, "스마트관광을 위한 IT 서비스 개발의 우선순위 도출을 위한 AHP 분석모델", *정보시스템연구*, 제28권, 제4호, 2019, pp. 49-64.

[6] 김다빈, 김경모, 조진성, "IoT 보안 요구사항에 대한 고찰", *한국정보과학회 학술발표논문집*, 2015, pp. 1072-1074.

[7] 김대진, 홍일유, "AHP 분석방법을 통한 정보제공 웹사이트 평가속성 가중치산정에 관한 연구: 외식정보 제공 웹사이트 중심으로", *Information Systems Review*, 제16권, 제3호, 2014, pp. 1-23.

[8] 김동희, *융합시대의 사이버보안 거버넌스 구축방안에 관한 연구* (박사학위논문), 고려대학교, 2016.

[9] 김용운, 임정일, 이수형, 정지석, "스마트공장의 진화 모델", *월간계장기술*, 2월호, 2016, pp. 102-113.

[10] 김은, 김미정, 김범수, 김영훈, 이애리, 이태진, 정대영, 조호정, 최동석, 하희탁, 한순홍, 현용탁, *4차 산업혁명과 제조업의 귀환: 독일 전문가들이 들려주는 인더스트리 4.0의 모든 것*, 클라우드나인, 2017.

[11] 김은영, 박문수, "4차 산업혁명시대 지역 중소기업의 제조혁신 한계와 스마트공장 정책 방향성 연구", *과학기술학연구*, 제18권, 제2호, 2018, pp. 269-306.

[12] 김현, 박준희, 김근영, 박윤규, "ICT 기반 스마트공장", *Electronics and Telecommunications Trends*, 제29권, 제5호, 2014, pp. 62-71.

[13] 나재훈, 나중찬, "산업제어시스템 보안 표준화 동향", *정보보호학회지*, 제26권, 제4호, 2016, pp. 28-35.

[14] 노상도, "스마트공장 사이버물리시스템(CPS) 기술 동향 및 이슈", *전자공학회지*, 제43권, 제6호, 2016, pp. 47-50.

[15] 배춘석, 고승철, "스마트팩토리 도입 기업의 보안강화 사례 연구", *정보보호학회논문지*, 제29권, 제3호, 2019, 675-684.

[16] 산업통상자원부, *스마트공장 발전 전략 수립 및 고도화 방안 연구*, 산업통상자원부, 2015a.

[17] 산업통상자원부, *스마트공장 보급・확산을 위한 업종별 참조모델*, 산업통상자원부, 2015b.

[18] 산업통상자원부, 한국생산성본부, *미래 스마트공장 방향 제시 및 스마트제조산업 발전 방안 연구*, 산업통상자원부 & 한국생산성본부, 2016.

[19] 서창성, 정신진, 김석찬, "기업의 생산성 향상

을 위한 스마트 팩토리 구축", *한국통신학회지(정보와통신)*, 제35권, 제6호, 2018, pp. 43-49.
[20] 서혁준, "스마트공장 보안 대응 방안", *월간계장기술*, 2016 기획특집, 2016, pp. 88-91.
[21] 손경호, "산업제어시스템 보안성 평가·인증 동향 분석", *정보보호학회지*, 제24권, 제5호, 2014, pp. 15-25,
[22] 손지연, 강현철, 배희철, 이은서, 한효녕, 박준희, 김현, "개인맞춤생산을 위한 IoT기반 개방형 제조서비스 플랫폼", *한국통신학회지(정보와통신)*, 제33권, 제1호, 2015, pp. 42-47.
[23] 오준형, 유영인, 이경호, "기반시설 침해사고 및 제어시스템 표준 동향", *정보보호학회지*, 제27권, 제2호, 2017, pp. 5-11.
[24] 유창현, ***R&D** 투자기업의 사업화 실현 성공요인에 관한 연구: 혁신형 중소기업을 중심으로* (박사학위논문), 경기대학교, 2017.
[25] 이규택, 이건재, "스마트공장 R&D 로드맵 소개", *KEIT PD ISSUE REPORT*, 제15권, 제11호, 2015.
[26] 이무순, 손달호, "ICT 기업 융합성과의 결정요인에 관한 연구", *정보시스템연구*, 제26권, 제3호, 2017, pp. 1-23.
[27] 이병권, 김동원, 노봉남, "안전한 스마트공장 구축을 위한 위험우선순위(SFRPN) 기반 최소 보안요구사항에 관한 연구", *정보보호학회논문지*, 제26권, 제5호, 2016, pp. 1323-1333.
[28] 이순열, "스마트공장을 위한 사물인터넷 기술 동향", *전자공학회지*, 제43권, 제6호, 2016, pp. 25-30.
[29] 이승환, 강진혁, 민병서, "중소기업 스마트공장을 위한 정보보호관리체계에 대한 연구", *정보 및 제어 논문집*, 2019, pp. 46-47.
[30] 이현정, 유상근, 김용운, "스마트공장 기술 및 표준화 동향", *Electronics and Telecommunications Trends*, 제32권, 제3호, 2017, pp. 78-88.
[31] 임창묵, 박형준, 김동현, "효과적인 산업보안 규제정책 방향과 정책수단", *국정관리연구*, 제8권, 제2호, 2013, pp. 123-151.
[32] 장경석, "국내외 스마트 팩토리 동향", ***KB**금융지주경영연구소 **KB**지식비타민*, 제17권, 제27호, 2017.
[33] 전승우, "사물 인터넷 시대 앞두고 네트워크가 진화하고 있다", *LG Business Insight*, 제29호, 2014.
[34] 전자신문, "스마트 팩토리로 제조업을 혁신하라", [소프트웨이브 서밋 2016], *전자신문*, 2016.
[35] 정선양, 전중양, 황정재, "중소기업의 글로벌 경쟁력 제고를 위한 스마트공장 표준화 전략", *기술혁신학회지*, 제19권, 제3호, 2016, pp. 545-571.
[36] 진상기, 박영원, "제4차 산업혁명 대비 미래대응체계 및 개선방향에 관한 탐색적 연구", *지역정책연구*, 제28권, 제1호, 2017, pp. 107-135.
[37] 차석근, "스마트공장 표준화 동향과 시스템 구조", *전자공학회지 특집*, 제43권, 제6호, 2016, pp. 465-471.
[38] 차석근, "IoT/M2M를 적용한 스마트팩토리 표준화 동향과 시스템 구조", *한국통신학회지(정보와통신)*, 제32권 제5호, 2015, pp. 36-41.
[39] 차석근, 윤재영, 홍정기, 강현구, 조현찬, "스마트공장을 위한 IT 융합 표준화 동향 분석과 시스템 구조", *한국정밀공학회지*, 제32권, 제1호, 2015, pp. 17-24.
[40] 차영태, "클라우드 컴퓨팅 보안 기술동향과 산업전망", *KEIT PD ISSUE REPORT*, 제12권, 제6호, 2012.
[41] 최영환, 최상현, "스마트공장 시스템 구축이 중소기업 경쟁력에 미치는 요인에 관한 연구", *Information Systems Review*, 제19권, 제2호, 2018, pp. 95-113.
[42] 최종석, 박종규, 김호원, "인공지능과 사물인터넷 융합 보안 기술 연구방안", *한국통신학회지(정보와통신)*, 제34권, 제3호, 2017, pp. 65-73.

[43] 한국인터넷진흥원, *스마트공장 중요정보 유출방지 가이드*, 한국인터넷진흥원, 2017.

[44] 한국표준협회, “SyC SM(Smart Manufacturing, 스마트 제조)”, *KSA Policy Study*, 27 Issue paper, 2018-1호, 2018.

[45] Lee, S. J., A. Azween, and N. Z. Jhanjhi, “A review on honeypot-based botnet detection models for smart factory”, *International Journal of Advanced Computer Science and Applications*, Vol.11, No.6, 2020, pp. 418-435.

[46] Ngai, E. W. T., “Selection of web sites for online advertising using the AHP”, *Information & Management*, Vol.40, No.4, 2003, pp. 233-242.

[47] Pagnon. W., “The 4th industrial revolution: A smart factory implementation guide”, *International Journal of Advanced Robotics and Automation*, Vol.2, No.2, 2017, pp. 1-5.

[48] Park, S. T., G. Li, and J. C. Hong, “A study on smart factory-based ambient intelligence context-aware intrusion detection system using machine learning”, *Journal of Ambient Intelligence and Humanized Computing*, Vol.11, No.4, 2020, pp. 1405-1412.

[49] Zuehlke, D., “Smart factory-towards a factory-of-things”, *Annual Reviews in Control*, Vol.34, No.1, 2010, pp. 129-138.

Information Systems Review
Volume 22 Number 4
November 2020

Investigating Key Security Factors in Smart Factory: Focusing on Priority Analysis Using AHP Method

Jin Hoh* · Ae Ri Lee**

Abstract

With the advent of 4th industrial revolution, the manufacturing industry is converging with ICT and changing into the era of smart manufacturing. In the smart factory, all machines and facilities are connected based on ICT, and thus security should be further strengthened as it is exposed to complex security threats that were not previously recognized. To reduce the risk of security incidents and successfully implement smart factories, it is necessary to identify key security factors to be applied, taking into account the characteristics of the industrial environment of smart factories utilizing ICT.

In this study, we propose a 'hierarchical classification model of security factors in smart factory' that includes terminal, network, platform/service categories and analyze the importance of security factors to be applied when developing smart factories. We conducted an assessment of importance of security factors to the groups of smart factories and security experts. In this study, the relative importance of security factors of smart factory was derived by using AHP technique, and the priority among the security factors is presented. Based on the results of this research, it contributes to building the smart factory more securely and establishing information security required in the era of smart manufacturing.

Keywords: Smart Factory, Smart Manufacturing, IoT, Information Security, Analytic Hierarchy Process

* CEO, Euroservice Corp.
** Corresponding Author, Assistant Professor, Department of Business Administration, Sangmyung University

◐ 저 자 소 개 ◑

허　　진 (i6366@naver.com)

상명대학교에서 정보시스템·보안 전공으로 경영학 박사 학위를 취득하였다. 유로서비스(주)에 근무하면서 스마트 경영과 제조 기획업무를 수행하고 있다. 주요 연구 관심분야는 Digital Transformation, Smart Factory, Business Analytics 등이다.

이 애 리 (sharon@smu.ac.kr)

KAIST에서 테크노 경영 전공으로 석사학위를 취득하고, 연세대학교에서 정보시스템학 박사학위를 취득하였다. KT에 근무하면서 경영전략과 신사업 연구개발 업무를 수행하였고, 연세대학교 바른ICT연구소 연구교수로 재직한 바 있다. 현재 상명대학교 경영학부 (MIS 전공) 조교수로 재직 중이다. Information & Management, Computers in Human Behavior, Internet Research, Behaviour & Information Technology, Journal of Global Information Management 등의 학술지에 논문을 발표하였다. 주요 연구 관심분야는 Digital Transformation, Information Security & Privacy, Virtual Community, Social Media, Business Intelligence, Big Data Analytics 등이다.

논문접수일 : 2020년 08월 05일　　**게재확정일 : 2020년 10월 26일**
1차 수정일 : 2020년 09월 03일