석사학위논문

스마트공장 구축시 중소기업의 보안수준 향상을 위한 우선순위 도출에 관한 연구

-구축수준 Level2 이하 중소제조기업을 중심으로-

2022년

한성대학교 지식서비스&컨설팅대학원

스마트융합컨설팅학과

스마트융합컨설팅전공

박 상 복

석 사 학 위 논 문
지도교수 원종혁

스마트공장 구축시 중소기업의 보안수준 향상을 위한 우선순위 도출에 관한 연구

-구축수준 Level2 이하 중소제조기업을 중심으로-

A Study on the Priority of the Smart Factory for the Improvement of Security Level of Small and Medium Enterprises
-Focusing on Small and Medium Manufacturing Businesses with Level 2 or Low Level of Construction-

2021년 12월 일

한성대학교 지식서비스&컨설팅대학원

스마트융합컨설팅학과

스마트융합컨설팅전공

박 상 복

석 사 학 위 논 문
지도교수 원종혁

스마트공장 구축시 중소기업의 보안수준 향상을 위한 우선순위 도출에 관한 연구

-구축수준 Level2 이하 중소제조기업을 중심으로-

A Study on the Priority of the Smart Factory for the Improvement of Security Level of Small and Medium Enterprises
-Focusing on Small and Medium Manufacturing Businesses with Level 2 or Low Level of Construction-

위 논문을 컨설팅학 석사학위 논문으로 제출함

2021년 12월 일

한성대학교 지식서비스&컨설팅대학원

스마트융합컨설팅학과

스마트융합컨설팅전공

박 상 복

박상복의 컨설팅학 석사학위 논문을 인준함

2021년 12월 일

심사위원장 홍 정완 (인)

심 사 위 원 박 인채 (인)

심 사 위 원 원 종혁 (인)

국 문 초 록

스마트공장 구축시 중소기업의 보안수준 향상을 위한 우선순위 도출에 관한 연구 -구축수준 Level2 이하 중소제조기업을 중심으로-

한성대학교 지식서비스&컨설팅대학원
스 마 트 융 합 컨 설 팅 학 과
스 마 트 융 합 컨 설 팅 전 공
박 상 복

전 세계적으로 다양한 기술의 발전이 가져오는 삶의 변화는 굉장히 편리하며 효율적이고 다양한 형태로 다가오고 있다. 그중에서도 전통적인 제조업 분야에 있어서 자동화 및 디지털 기술의 발전과 함께 ICT와의 융합이 활발히 이루어지고 있는 스마트공장에 대한 추진이 활발해 지고 있다. 특히, 학문 간의 전통적 경계가 허물어지고 기술 융합이 경제체제와 사회구조를 급격히 변화시키는 4차 산업혁명 시대가 더욱 가속화되고 있다. 스마트제조(smart manufacturing)는 이러한 4차 산업혁명 시대에서 인간, 기술, 정보의 융합을 통해 제조업의 전략적 혁신을 도모하고자 하는 패러다임의 변화로서 ICT와 제조기술을 융합하여 더욱 혁신적인 생산성 향상을 추구하고자 하는 기술이다. 또한 스마트공장(smart factory)은 이러한 기술 융합을 통하여 제조업 현장에서 운영중인 설비, 장비와 공정이 보다 지능화되고 네트워크로 연결되는 구조를 기준으로 한다. 그리고 각 설비 및 장비에서 발생하는 생산데이터와 정보가 실시간으로 공유되고 활용되어 최적화된 생산운영이 가능한 공장을

만들고자 하는 개념으로 정의할 수 있다. 또한, 공장 간의 협업적인 운영이 지속되는 지능형 ICT융합 제조시스템을 지칭하기도 한다.

하지만, 이러한 시스템의 발전에는 긍정적인 효과와 부정적인 효과가 같이 존재하게 되는데, 스마트공장에 있어서도 긍정적인 효과로는 ICT융합을 통한 시스템이 지능화되는 효과가 있지만, 부정적으로는 사이버위협이 증가하면서 실제 피해사례도 지속적으로 발생하고 있다는 점을 들 수 있다. 따라서 과거와는 달리 개별적인 기계와 설비 그리고 시스템들이 네트워크 기반으로 연결되면서 확장되고 있었다. 이에 따라 새로운 시스템과 기존 시스템 간의 연결시 보안문제에 대한 대응방안이 요구되었다.

본 연구는 기존의 연구들에 있어서 스마트공장 구축시 발생할 수 있는 보안문제에 대하여 폭 넓은 시각으로 접근하기 위해 다음과 같은 방법론을 적용하였다. 기존의 연구에 대한 면밀한 분석과 도출방법의 문제점, 해결방안 제시의 적절성, 실증 대상의 전문가 설문 등을 실증하였다. 실증대상의 기준은 스마트공장의 구축 규모 중 Level2 이하인 중소제조기업을 중심으로 구축 시 우선적으로 고려해야할 보안요소 항목을 규정하는 연구로서 명확한 연구의 배경 및 목적을 제시하고 있다.

그리고 스마트공장 구축수준 Level2이하 중소제조기업의 현황을 분석하여 해당 기업이 스마트공장을 구축함에 있어 보다 현실적으로 고려할 수 있는 보안에 대한 우선순위 항목을 제시하였다. 해당 우선순위 항목 중 각 기업의 역량에 맞는 보안 요소를 선정할 수 있도록 함으로써 좀 더 효율적이고 효과적인 시스템 운영방법을 제시했다는데 연구자로서 의의를 가질 수 있었다.

또한, 연구방법으로는 조사통계학적 증명을 통해 진행하였으며 그 과정에서 스마트공장에 대한 전문가들의 설문과 실제 운영중인 기업에 대한 스마트공장 수준확인 보고서에 대한 실증분석을 검토하여 최종적인 결과를 도출하고 반영하였다.

우선순위 보안항목에 대한 결론을 통해 스마트공장 Level2이하 중소기업 기준으로 스마트공장을 구축하는데 있어 보안에 대한 실질적인 적용 및 운영 효과성을 부여하고자 한다. 현실적으로 적용이 가능한 우선순위

를 도출하고 전문가 실증을 통해 결론을 제안하여 심리적 안정성을 부여하고자 한다.

그리고 도출된 결론의 제언을 통해 현재 다소 정채되고 있는 중소제조기업의 스마트공장 신규 구축에 있어서 발전방향의 새로운 기준이 되어질 만한 기준을 제언하고자 한다.

【주요어】 스마트공장 구축시 보안, 우선순위 보안 항목, 스마트공장 보안 고려사항, ICT 융합 스마트공장 보안

목 차

I. 서 론 ····· 1

1.1 연구의 필요성 ····· 1
1.2 연구의 범위 ····· 3
1.3 연구의 구성 ····· 5

II. 이론적 배경과 선행연구 ····· 7

2.1 스마트공장에 대한 이해 ····· 7
2.1.1 스마트공장의 정의 ····· 7
2.1.2 스마트공장의 특성 ····· 10
2.1.3 국내의 스마트공장 추진현황 ····· 12
2.2 스마트공장에서의 보안요소 검토 ····· 16
2.3 선행연구 검토 ····· 19
2.4 본 연구에 있어서의 차별성 ····· 23

III. 중소기업의 보안수준 향상을 위한 우선순위 항목 도출 ····· 25

3.1 중소기업의 보안수준 향상을 위한 우선순위 항목 도출방법 ····· 25
3.2 연구대상 및 자료수집 방법 ····· 29

IV. 중소기업의 보안수준 향상을 위한 우선순위 항목 도출 검토 ····· 33

4.1 실증분석을 통한 중소기업의 보안수준 향상을 위한 우선순위 항목에 대한 타당성 검증 ····· 33

4.1.1 검증 절차 ····· 33
4.1.2 조사 결과 ····· 39
4.2 실증분석을 통한 중소기업의 보안수준 향상을 위한 우선순위 항목 도출 ····· 50
4.2.1 최종 보안 우선순위 항목 분석 및 도출 ····· 50

V. 결 론 ····· 54

참 고 문 헌 ····· 56

ABSTRACT ····· 59

표 차례

[표 2-1] 산업혁명의 단계별 비교 ····· 9
[표 2-2] 스마트공장 수준별 단계 ····· 11
[표 2-3] 환경별 상대적인 우선순위가 다른 보안 목표 ····· 12
[표 2-4] 연도별 스마트공장 보급목표 ····· 13
[표 2-5] 스마트공장 지원유형별 보급현황 ····· 13
[표 2-6] 우리나라의 중소기업 기준 ····· 15
[표 2-7] 스마트공장 수준 총괄도 ····· 16
[표 2-8] 스마트공장 운영을 위한 보안요인 선행연구 ····· 19
[표 2-9] 스마트팩토리 보안관리 항목 우선순위 선행연구 ····· 19
[표 2-10] 스마트공장의 최소보안요구사항 우선순위 선행연구 ····· 21
[표 2-11] 5G 스마트공장의 보안요구사항 선행연구 ····· 22
[표 3-1] 선행연구에서 추출한 스마트공장 보안관리 항목 ····· 26
[표 3-2] 연구대상 및 자료수집 방법 ····· 32
[표 4-1] 설문조사 응답자 특성 - 근무분야 ····· 34
[표 4-2] 설문조사 응답자 특성 - 경력년수 ····· 35
[표 4-3] 설문조사 응답자 특성 - 학력 ····· 35
[표 4-4] 설문조사 응답자 특성 - 스마트공장 직접 업무 경력유무 ···· 36
[표 4-5] 스마트공장 수준확인 심사보고서 특성 - 종업원수 ····· 37
[표 4-6] 스마트공장 수준확인 심사보고서 특성 - 매출액 ····· 37
[표 4-7] 스마트공장 수준확인 심사보고서 특성 - 업종 ····· 38
[표 4-8] 스마트공장 도입 및 구축에 따른 중소기업 보안수준 현황 ·· 40
[표 4-9] 스마트공장 도입 및 구축시 보안 검토 사항 중요도 ····· 42
[표 4-10] 스마트공장 도입 및 구축시 보안 영역별 필요성 수준 ···· 43
[표 4-11] 스마트공장 도입 및 구축시 보안 우선순위 적용 검토 항목 · 44
[표 4-12] 스마트공장에 대한 경영진 인식 수준 (보안분야) ····· 46
[표 4-13] 스마트공장과 관련한 보안교육 실시 및 수준 ····· 46
[표 4-14] 스마트공장 보안 업무 담당자 지정 여부 ····· 47

[표 4-15] 스마트공장 도입 및 구축기업 도입 혹은 검토 프로그램 ·· 48
[표 4-16] 스마트공장 도입 및 구축기업 보안 운영 세부 분야 ·····49
[표 4-17] 기업 규모별 보안 가이드라인에 대한 실증분석 자료 비교 ·· 50
[표 4-18] 스마트공장 구축에 있어서 기업 규모별 보안 가이드라인 ·· 53

그림 차례

[그림 1-1] 연구의 순서와 구성 ····· 6
[그림 2-1] 스마트공장의 개념 ····· 8
[그림 2-2] 스마트 제조업 개념도 ····· 10
[그림 2-3] 스마트공장 추진현황 ····· 14
[그림 2-4] 스마트공장 지역별 도입현황 ····· 15
[그림 2-5] 스마트공장 표준지도 ····· 17
[그림 2-6] 스마트공장 영역별 보안위협 ····· 18
[그림 4-1] 스마트공장 도입 및 구축시 보안 영역별 필요성 수준 도표 ··· 43

Ⅰ. 서 론

1.1 연구의 필요성

전 세계적으로 ICT의 발전과 함께 스마트공장 운영분야에서는 유례없는 자동화 및 디지털화가 가속화 되고 있다. 더욱이 최근에는 스마트제조라는 주창과 함께 4차 산업혁명의 물결에 휩싸이게 되었다. 이러한 4차 산업혁명의 물결은 우리나라 경제에 있어서도 기존보다 빠른 발전을 요구하고 있으며 산업분야 전반에 걸쳐서 지속적인 요구사항을 발생시키고 있다. 그 중에서 스마트공장은 4차 산업혁명을 주도적으로 이끌어갈 제조업의 기반이 될것으로 전망되어 지며 세계 경제에 상당한 부가가치를 창출할 것으로 예상되어 진다.

이러한 변화의 물결 영향으로 기존에 폐쇄적인 구조의 환경을 보유하고 있던 제조 현장에서도 IoT, Cloud, Big Data, Mobile 등을 기반으로 한 개방적인 구조의 시스템들이 등장하게 되었다. 실제로 제조 현장에 이러한 시스템들이 다양한 방식으로 접목됨과 동시에 새로운 제조환경의 기반으로 자리매김함으로써 생산성 향상을 포함한 다양한 성과 창출에 기여할 수 있게 되었다.

이와 같은 변화의 물결은 새로운 제조환경을 구축하고 기존의 제조방식에서 가지고 있던 한계성을 개선함으로써 보다 효과적이고 효율적인 생산환경을 구축하고자 하는 변화를 만들어냈으며, 이것이 전 세계적으로 도입과 추진을 시작하게 된 스마트공장의 배경이 된 것이다. 독일에서 추진된 '인더스트리 4.0(Industry 4.0)[1)]'과 함께 미국에서 추진된 '첨단제조파트너십(AMP 2.0)[2)]', 중국에서 추진된 'Made in China 2025[3)]' 전략 등이 모두 이러한 내용을 담고 스마트공장 구축을 통한 제조환경의 변화를 만들어내기 위한 노력으로 정의 할 수 있다.

---

1) ICT와 제조업 융합, 국가 간 표준화를 통한 스마트공장 추진을 위한 독일의 정책

2) 첨단제조혁신을 통한 국가 경쟁력 강화, 일자리 창출, 경제 활성화를 위한 미국의 스마트화 정책

3) 30년 후 제조업 선도국가 지위 확립을 위한 중국의 스마트화 추진 정책

하지만, 단순히 ICT와의 융합을 통한 제조 현장의 발전이 긍정적인 효과만을 가져오는 것은 아니다. 스마트공장 구축 등을 추진하는 각 기업들이 이러한 새로운 기술들을 활용하여 생산성 향상 등과 같은 목표 달성의 성과를 만들어내고 있지만 반대로 이러한 시스템들을 통해 만들어지는 정보들에 대한 관리, 즉 보안의 관리에 있어서는 역량이 부족하거나 다양한 이슈와 문제들이 야기되고 있는 것이 현실이다. 그리고, 이러한 보안관리에 있어서는 작은 문제가 실제로는 상당히 심각한 수준으로 발전하여 기업의 경영에 막대한 손실을 끼칠 수 있다는 것이 더 큰 문제일 수 있다.

또한, 최근에는 산업안전 분야, 환경보호 분야, 생명 존중 분야 등 사회적인 요구를 수용하여 서비스를 제공하는 분야에 있어서 융합 기반의 비즈니스 모델이 많이 발생하고 있으며 이러한 비즈니스 모델에 있어서 정보에 대한 중요성이 날로 증가하고 있는 것이 현재 상황이다. 하지만 중소기업에 있어서의 보안 및 관리에 대한 투자와 관심은 높은 편이지만 실제 구현을 하는 기업은 매우 제한적으로 실현되고 있다. 최근 큰 규모의 금전적 피해를 발생시키는 보안 침해사고가 급증하게 되면서 사이버보안에 대한 사회적인 공감대와 보안 인식이 높아지게 되었다. 그러나 아직도 중소기업에서는 보안에 대한 관리와 대응에 있어서는 미온적이라 할 수 있다. 현실적으로는 별도의 보안절차의 운영에 따른 불편함과 비용부담 등으로 인하여 관리와 관심이 부족해진 것으로 판단되고 있다.

최근 기업이 도입하여 구축하고 있는 스마트공장에 있어서도 예전과 달리 기계, 설비와 시스템들이 IoT(Internet of Things) 혹은 IoE(Internet of Everything)와 같은 개념으로 연결되어 확장되고 있으며, 4차 산업혁명이라는 변화의 물결 속에서 상상 이상으로 발전하고 있다. 그리고 이러한 기술발전은 AI와 같은 기술이 활용되는 다양한 융합 환경을 실현하고 있기에 더이상 보안에 대한 인식과 관리를 등한시할 수 없게 되었다.

따라서 이제는 스마트공장의 도입에 있어서 보안적인 요소를 고려하여야 함은 물론이고 어떤 문제점에 대해서 어떠한 해결방안을 적용시켜야 하는지 면밀한 검토가 필요하게 되었다. 제조업의 경쟁력 향상 뿐만아니

라 제조업의 서비스화, 휴먼 팩토리의 구현 등을 위하여 스마트공장으로 바뀌거나 ICT와 연계한 기술 기반의 시스템을 고도화하기 위한 스마트공장의 구축 등이 다방면에서 이루어지고 있기에 이러한 보안의 요소를 시급하게 다루어야 하는 것이 현안이 된 것이다. 하지만 기존의 연구들은 스마트공장 구축에 있어서 우선적으로 고려해야 하는 보안의 요소가 무엇인지를 제시하는 선행연구도 다수 있었다. 하지만 보안의 문제에 따른 고려사항이 무엇인지에 대한 일반적으로 제시하는 차원에서 순위 정도만 거론하고 있으며 중소기업의 규모나 구축수준에 따른 좀 더 구체적이고 현실적인 보안 우선순위 항목에 대한 제시는 부족하다고 판단되어 진다. 특히 관련전문가 및 실무자의 의견반영을 통해 대응방안을 제시한 사례도 많지 않았다.

이에 따라 본 연구에서는 선행연구를 비교 분석한 후 도출된 보안요소들과 보안의 우선적 고려사항을 중심으로 도출방안을 제시하기 위한 연구를 진행하였다. 그리고 중소기업 중 스마트공장 구축수준이 Level2 이하인 기업들을 대상으로 스마트공장 구축 시 적용해야 하는 보안 우선순위 항목에 대한 고려사항을 제언하고자 하였다. 이러한 제언을 위해 스마트공장 구축시 우선적인 고려가 필요한 보안의 요소들에 대해서 전문가 의견과 구축 현장에서 활동하고 있는 실무자들이 느끼는 보안의 우선 요소에 대한 의견을 파악하고 분석하였다. 또한 스마트공장 구축 기업을 대상으로 실시된 'A' 기관의 스마트공장 수준확인 결과와의 비교분석을 통해 전문가 의견에 대한 타당성 분석 및 실증분석도 병행하여 진행하였다.

이러한 전문가 설문 및 'A'기관의 스마트공장 수준확인 결과의 실증분석을 통해 결론적으로 스마트공장 도입 및 구축을 예정하고 있거나 진행중인 Level2 이하의 중소기업에서 기업의 운영수준에 맞는 우선순위 보안항목을 검토하고 적용할 수 있도록 제언하였다.

1.2 연구의 범위

스마트공장과 관련하여 독일의 인더스트리 4.0 정책과 AMP(Advanced

Manufacturing Partnership) 정책[4]의 일환으로 IIoT를 진행하고 있는 미국을 포함한 다양한 선진 산업국들의 정책을 분석하였다. 국내에서는 제조업 3.0 정책[5]을 통해 2022년까지 3만개의 스마트공장을 구축할 수 있도록 지원하고 있으며 제조업 중심으로 스마트공장 도입이 추진되어지고 있다. 이에 기존에 공장 내에서만 한계적으로 운영되던 산업제어시스템 기반시스템들이 ICT 기술과 접목되면서 사이버위협의 불안감이 증가하게 되었다. ICT를 기반으로 한 모든 기계와 설비에서부터 이와 연계된 시스템들로 사이버 위협의 범위가 이동하고 있기 때문에 스마트공장 시스템 영역을 고려한 새로운 보안관리의 패러다임 전환이 필요하게 되었다.

현재의 보안관리 체계는 기업과 부서 단위에서의 보안관리를 중점으로 하고 있으며, 일반적인 보안의 영역을 구분하여 어떠한 활동을 해야 할지에 대한 활동 정의는 수립되어 있다. 하지만 세부적으로 각 기업의 규모나 수준에 따른 구체적인 보안가이드라인 제시는 이루어지지 못하고 있는 실정이다. 또한 보안관리에 필요한 표준이나 규정의 제정에는 일정한 기간과 비용이 소요되기 때문에 중소기업의 입장에서는 보안활동에 대한 우선순위가 고려된 보안항목의 검토와 제시가 현실적으로 필요한 실정이다. 이에 본 논문은 기존의 연구를 바탕으로 중소기업이 스마트공장 구축시 고려할 보안 우선순위 항목을 도출하고자 전문가 및 실무자 의견수렴과 분석하였다. 그리고 스마트공장 도입 기업을 대상으로 실시된 스마트공장 수준확인 결과 내 중소기업의 보안수준 분석 자료에 대한 비교를 통해 전문가 의견에 대한 타당성 검증을 위한 실증연구를 진행하고자 한다.

본 논문은 다음과 같이 구성되어 있다. I장에서는 해당 연구의 필요성, 연구의 범위, 연구의 구성에 대해 작성한다. II장에서는 이론적 배경과 선행연구 조사를 통해 스마트공장에 대한 이해를 위해 스마트공장의 정의 및 특성에 대해 알아보고 국내 스마트공장의 추진현황도 조사한다. 또한, 본 연구의 목표인 스마트공장 구축에 있어서 중소기업이 고려할 보안 우선순위 항목 제시를 위해 정보보안과 관련된 내용 또는 설계를 위한 방법론과 스마트공장 수준확

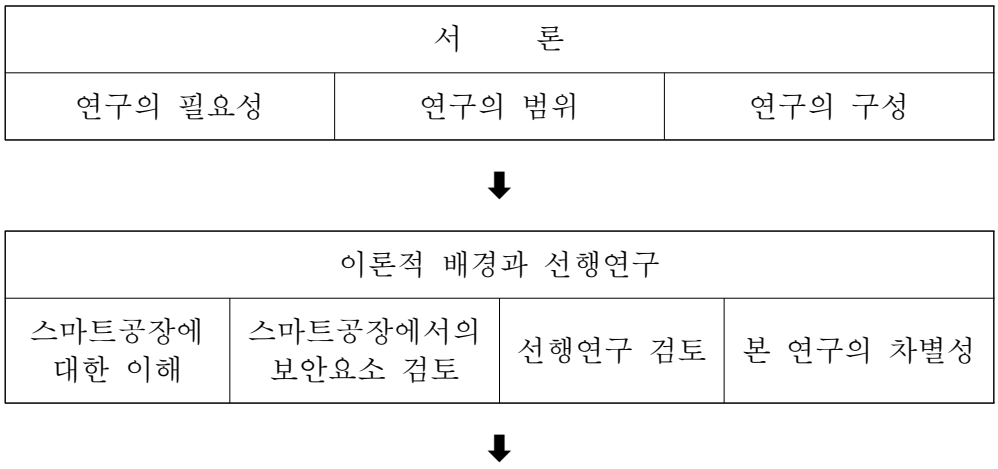
4) 미국의 4차 산업혁명 관련 벤처 육성 정책

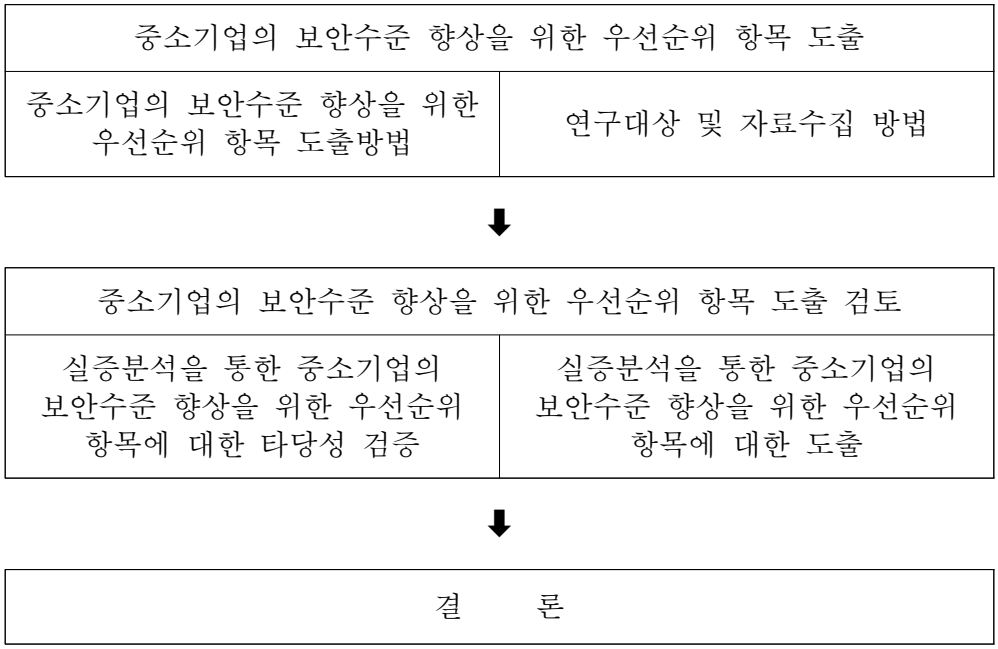
5) 산업통상자원부에서 발표한 융합형 신 제조업 창출 등 스마트공장 추진 정책

인 제도를 분석하고 기존에 연구되어진 스마트공장에 대한 보안 관련 연구들을 조사한다. III장에서는 실제적으로 스마트공장 구축에 있어서 중소기업이 고려할 보안 우선순위 항목에 대한 제언을 위해 II장에서 조사한 선행연구들을 세부 내용별로 분류하고 현실적으로 Level2이하 중소기업 환경에서 필요한 보안관리 항목을 도출한다. IV장에서는 III장에서 확인한 보안 관련 항목과 연계하여 Level2이하 중소기업이 스마트공장 구축에 있어서 고려해야하는 보안 우선순위 항목에 대한 전문가 및 실무자 설문, 기존에 실시된 스마트공장 수준확인 기업들의 수준확인 자료를 분석하여 1차적으로 보안 필요 항목에 대한 도출을 실시하였다. 그리고 해당 전문가 의견자료와 스마트공장 수준확인 보고서 상의 중소기업의 보안 수준 내용을 비교분석함으로써 전문가 의견에 대한 타당성을 검증함과 동시에 최종적인 보안 우선순위를 도출 및 선정하여 제시한 뒤, 끝으로 V장에서 결론을 맺는다.

1.3 연구의 구성

본 연구는 아래의 [그림 1-1]과 같은 순서대로 진행하고 해당 구성의 내용으로 진행하고자 한다.





[그림 1-1] 연구의 순서와 구성

II. 이론적 배경과 선행연구

II장에서는 기업 규모별 스마트공장 보안가이드라인을 도출하기 위해 스마트공장의 정의 및 특성, 국내 스마트공장의 추진현황을 살펴보고 스마트공장의 보안요소를 다룬 선행연구들을 검토한다. 그리고, 선행연구를 바탕으로 본 연구의 차별성을 제시토록 한다.

2.1 스마트공장에 대한 이해

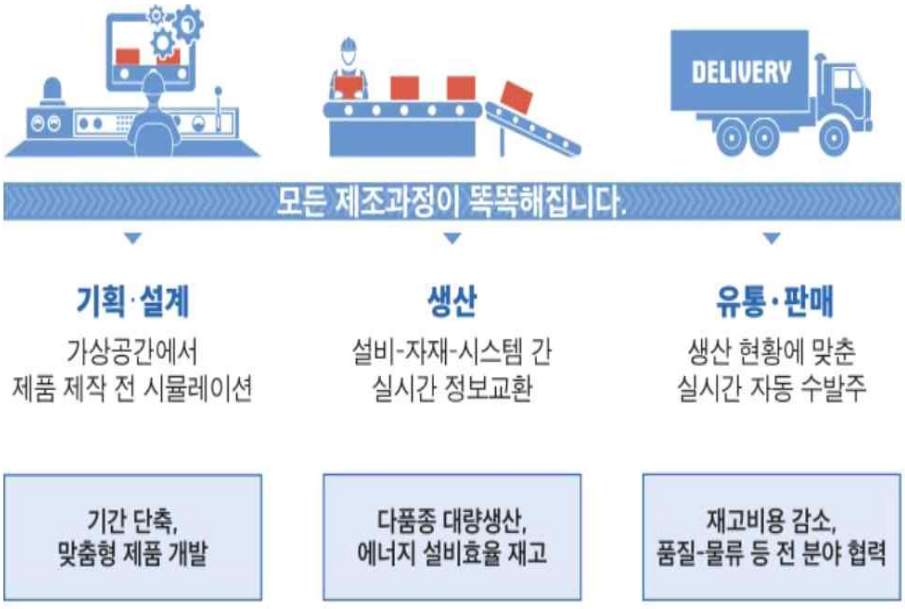
2.1.1 스마트공장의 정의

제조업 부문에 있어서 선진국들은 그동안 여러 차례의 산업혁명을 통하여 증기기관 기반의 기계화 혁명을 시작으로 전기에너지 기반의 대량생산 혁명, 그리고 컴퓨터와 인터넷 기반의 지식정보 혁명까지 꾸준한 혁신을 통한 새로운 환경을 등장시켰다. 그리고 이러한 새로운 환경을 통해 제조업 부문의 선진국들은 지속적인 산업발전과 더불어 각 기업별 경쟁력을 강화하여 꾸준한 생산성 향상을 가져오게 되었다. 다만, 최근에는 저렴한 인건비나 다양한 혜택 지원 등 제조원가를 중심으로 한 경쟁력을 바탕으로 빠르게 성장하고 있는 개발도상국을 포함한 다양한 국가의 도전을 받고 있는 현실이다.

개발도상국을 포함한 다양한 국가들의 인건비를 중심으로 한 경쟁력 검토는 제조업 부문의 선진국들에게 각 기업들 개별로 이루어진 산업군 내 전체적인 경쟁력 약화라는 문제를 가져왔으며 이에 각 기업들은 지속적인 경영에 있어서 가장 중요한 요소로 제조 가격의 경쟁력을 확보하기 위해서 인건비가 저렴하거나 다양한 혜택을 부여하는 중국, 인도, 베트남 등지로 공장을 이전하게 될 수 밖에 없었다. 하지만, 최근에는 이러한 개발도상국을 포함한 다양한 국가들이 단순히 인건비로만 가격경쟁력을 구

축하려 하는 것이 아니라 R&D(Research and Development)와 R&BD(Research and Business Development) 수행을 통해 기술적 진보도 함께 추진하면서 더욱 선진국들을 위협하고 있다.

이러한 다양한 변화들은 결국 다양한 기술을 융합하는 변화에 대한 확대로 기업 개별의 경쟁관계에서 생태계 자체의 경쟁으로 시장 경쟁구도를 변화시키게 되었다. 이러한 경쟁의 모습을 가진 환경의 변화는 지속적으로 기술개발과 역량의 재고를 요청하게 되었으며 이를 통해서 경쟁력을 강화하고 나아가서는 타 기업과 차별화된 경쟁력을 갖추어야 하는 원인이 된 것이다. 이 차별화된 경쟁력을 갖추기 위해 최근에 등장한 것이 4차 산업혁명 기반의 스마트공장이라고 할 수 있으며, 이러한 스마트공장은 ICT와의 융합을 통해 기존의 전통적인 제조업 방식을 프레임을 완전히 다른 개념으로 바꾸게 만든 것이다.



[그림 2-1] 스마트공장 정의 (스마트제조혁신추진단, 2019)

과거에는 생산 효율성을 향상시키기 위해 단순한 목적으로 공장의 자동화 등을 추진했지만 지금은 제조업이 ICT와 융합하면서 서비스의 형태를 탈바꿈

하고 혁신의 가치를 증대시키는 융·복합적인 플랫폼 형태로 바뀌고 있다는 것을 [그림2-1]에서 확인할 수 있다. 4차 산업혁명 시대에는 기존의 방식으로는 경쟁력을 확보할 수 없으며 고객의 다양한 요구수준에 맞추기도 어렵기 때문에 보다 지능화되고 첨단화된 스마트공장 구축을 고려하지 않을 수 없는 것이다.

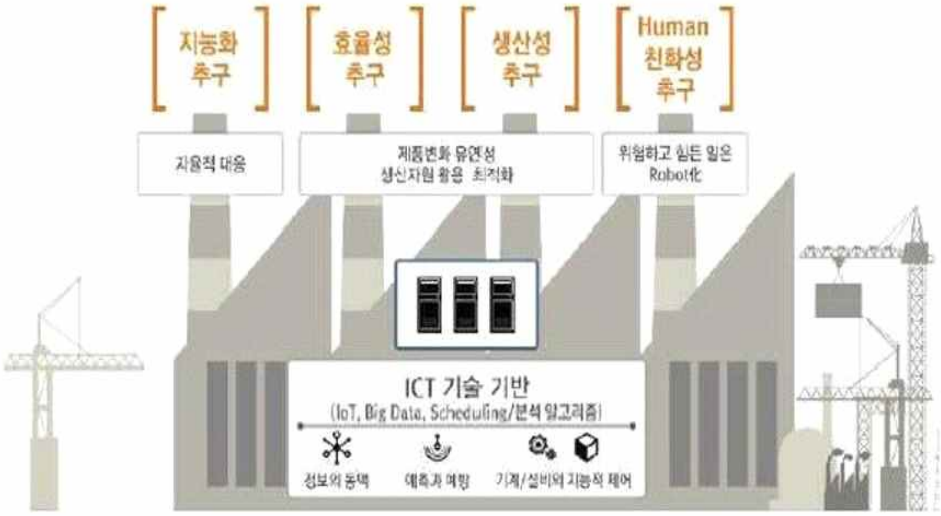
스마트공장과 관련한 기술혁신의 등장과 중요성에 대한 부각 등 새로운 패러다임의 등장과 전환은 2016년 1월 20일 스위스에서 개최된 '세계경제포럼'에서 3차 산업혁명을 바탕으로 한 디지털, 바이오, 물리학 등과 여러분야의 경계를 융합하는 기술혁신이 4차 산업혁명이라는 이름으로 변화하면서 더욱 부각되었다. 국내에서도 아래 [표2-1]에서 설명된바와 같이 제조업 선진국들이 추진한 혁신을 바탕으로 4차 산업혁명을 본격적으로 검토하여 다양한 지원정책을 추진하고 있다.

[표 2-1] 산업혁명의 단계별 비교 (스마트제조혁신추진단, 2019)

구분	1차	2차	3차	4차
시기	18세기 후반	20세기 초반	1970년 이후	2020년 이후
혁신 부문	증기의 동력화	전력, 노동, 분업	전자기기, ICT 혁명	ICT와 제조업 융합
커뮤니케이션 방식	신문, 책 등	TV, 전화기 등	SNS, 인터넷 등	IoT
생산방식	기계	대량생산	부분 자동화	시뮬레이션을 바탕으로 한 자동생산
생산통제주체	사람	사람	사람	자율화 기계

이러한 개념을 바탕으로 아래의 [그림2-2]과 같이 제조업에서는 스마트공장을 통해 지능화 추구, 효율성 추구, 생산성 추구, Human 친화성 추

구 등과 같은 연계된 성과를 달성할 수 있는 시스템이 스마트공장의 대표적인 모델이라고 표현되고 있다.



[그림 2-2] 스마트 제조업 개념도 (전자신문, 2021)

스마트공장에 대하여 종합적으로 정의한다면 제품 생산에서 판매에 이르기까지의 전 과정이 IoT, AI 등 다양한 정보통신기술과의 연계를 통하여 구현되어야 한다. 그리고 고객이 요구하는 제품의 수준을 최적화된 공정내에서 자동화된 설비로 생산할 수 있어야 한다. 이를 통해 실시간으로 수요에 대응함과 동시에 관련 데이터의 활용과 관리를 통제하는 사람 중심의 최첨단 공장시스템을 구현하는 것이라고 할 수 있다.

2.1.2 스마트공장의 특성

제조업 분야에 있어서 기존의 공장 자동화 시스템은 컴퓨터 또는 로봇과 같은 설비를 활용해 무인시스템 및 일부 생산라인에 있어서의 자동화시스템을 만들고, 설계 설비 또는 제조 설비 등의 생산 관련 시스템을 유기적으로 연결시키는 시스템 구조를 가지고 있었다. 하지만, 스마트공장 시스템은 기획에서 생산, 유통에 이르기까지의 전 과정을 ICT(정보통신) 기술과 접목하

여 각 단위 공정별로 구성요소를 체계화하였다는 특징이 있다. 그리고 통합적인 생산관리 시스템을 접목시킴으로써 보다 효율성 높은 효과적인 시스템 구조를 가지고 있다고 할 수 있다.

따라서, 이러한 구조에 대해 아래 [표2-2]와 같은 수준별 단계를 정의할 수 있다. 각 수준별 보안에 있어서의 고려사항이나 우선순위 보안요소, 보안에 대한 검토 및 도입 역량에 따라 다소의 차이가 나타날 수 있다.

[표 2-2] 스마트공장 수준별 단계 (스마트제조혁신추진단, 2019)

구분	세부 운영수준	시스템 구축 결과
고도화	· 설비, 자재, 시스템 유무선 네트워크로 연결(IoT/CPS) · 스스로 판단하는 지능형 설비, 시스템을 통한 자율적 공장 운영, 전 제조 과정의 통합 운영	사물/서비스/비즈니스 모듈 간 실시간 대화체제 구축, 사이버 공간상에서 비즈니스 실현
중간수준2	· 관리 시스템을 통한 설비 자동 제어 → 실시간 생산 최적화 · 분야별 관리 시스템간 실시간 연동 (개발 ↔ 생산자원관리 ↔ 자원관리)	협력사와 공급사슬 및 엔지니어링 정보공유, 제어자동화 기반 공정운영 최적화, 실시간 의사결정
중간수준1	· 설비 정보 자동집계 → 실시간 공장 운영 모니터링, 품질분석 · 분야별 관리 시스템간 부분적 연계 ex) 기준정보 · 엔지니어링 정보 생성, 수주정보 → 생산계획	다양한 ICT를 활용한 설비 정보 자동 획득, 협력사와 고신뢰성 정보를 공유하여 기업운영 자동화 지향
기초수준	· 생산실적 정보 자동집계 → 자재 흐름 실시간 파악, Lot-tracking · 부분적 관리 시스템 운영 (설계, 영업, 재고, 회계 등)	기초적 ICT를 활용한 정보 수집 및 이를 활용한 생산관리 구현
ICT 미적용	· Excel 정도 활용, 시스템을 갖추고 있지 못한 상태	해당사항 없음

이러한 스마트공장의 구성 환경은 결과적으로 기존의 환경과는 다른 환경의 영역을 구축하고 있으며 보안의 적용과 관리에 있어서도 다루고 있는 목표나 요소가 다를 수 있으므로 보안에서 중요시 하고 있는 3가지

영역의 우선순위 역시 달리하고 있다(LG CNS, 2018). 이 환경별 보안의 상대적 우선순위를 정리해보면 아래 [표2-3]와 같다.

[표 2-3] 환경별 상대적인 우선순위가 다른 보안 목표 (LG CNS, 2018)

우선순위	기존 ICT 환경	스마트공장 환경
1	기밀성	가용성
2	무결성	무결성
3	가용성	기밀성

결론적으로 스마트공장의 가장 대표적인 특징으로는 먼저 IoT와 같이 각종 기기에 통신과 센서기능을 장착함으로써 스스로 데이터를 주고 받을 수 있고 이를 통해 처리정보를 교환하는 형태가 있다. 그리고 CPS와 같이 다양한 물리적, 화학적 및 기계공학적 시스템들을 컴퓨터와 네트워크로 연결하여 자율적이고 지능적인 제어를 통한 내외부 의사소통 형태가 있다. 또한 도출된 데이터의 활용과 판단(AI)을 할 수 있도록 하드웨어, 소프트웨어, 네트워크 등 ICT 기술로 연결된 시스템을 통해 생산과 연계된 활동을 지원하는 구축시스템 등이 있다.

2.1.3 국내의 스마트공장 추진현황

국내의 제조업은 금융위기 이전까지는 저부가가치 산업으로 인식되는 경향이 많아 생산시설의 해외이전 및 인력과 부품의 아웃소싱 등을 강화하는 모습을 보였으나, 금융위기 이후 선진국들을 중심으로 빠른 경제 회복과 함께 제조업에 대한 기존의 패러다임에 변화가 생기면서 제조업이 주요 산업으로 재부각하게 되었다. 따라서, 이러한 추세에 발맞추어 국내에서도 2014년 7월에 제조업 혁신 3.0 정책의 수립을 통해 6대 과제의 일환으로 스마트공장 구축사업이 추진되게 되었으며, 이 정책을 통해 기존의 제조업에 경쟁력을 배가시킬 수 있는 ICT를 융합하여 경쟁력 향상과

생산 효율 달성, 3D 업종으로 인식되던 제조현장의 인력난 문제 해결까지 중소기업에 대한 적극적인 지원이 이루어지고 있다.

[표 2-4] 연도별 스마트공장 보급목표 (중소벤쳐기업부, 2019)

목표	누계 (2014년~2022년)	2019년	2020년	2021년	2022년
기존	20,000개	3,000개	3,000개	3,000개	3,200개
확대	30,000개	4,000개	6,000개	6,000개	6,200개

위 [표 2-4]에서 보는 바와 같이 2019년 중소벤처기업부 보도자료에 의하면 2020년까지 기존 3,000개 보급목표에서 6,000개 보급을 목표로 상향시킬 정도로 관심 높은 추진계획이라고 할 수 있다.

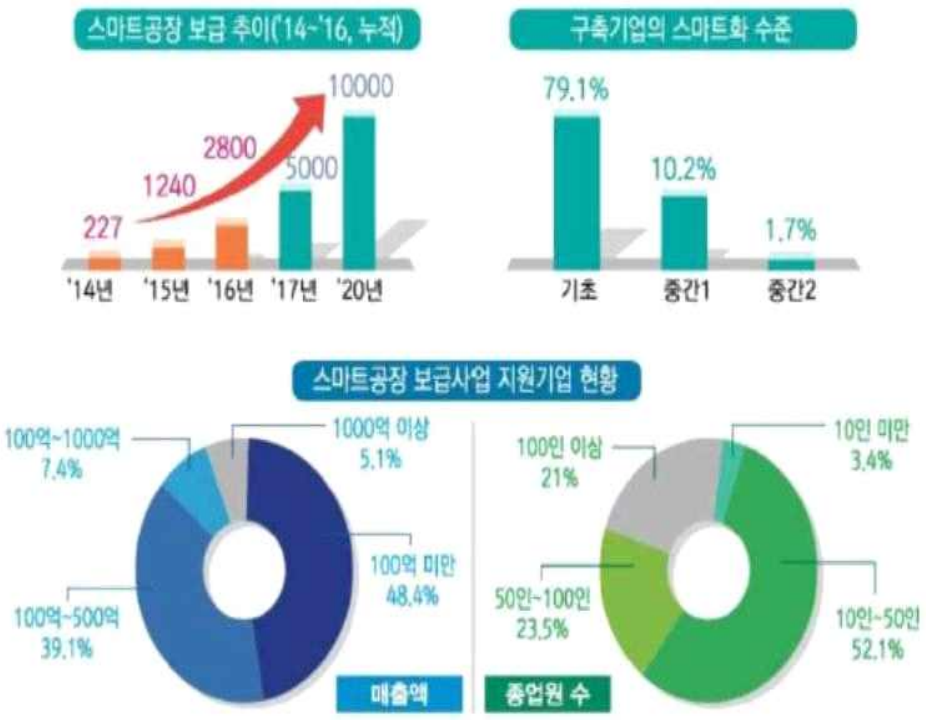
[표 2-5] 스마트공장 지원유형별 보급현황 (중소벤처기업부, 2021)

구분		2017년	2018년	2019년	2020년	합계
정부지원형		3,495개	2,221개	2,820개	4,730개	13,266개
민간 중심 보급	대중소 상생형	1,508개	679개	1,023개	1,000개	4,210개
	수준확인	-	-	914개	1,409개	2,323개
	소계	1,508개	679개	1,937개	2,409개	6,533개
합계		5,003개	2,900개	4,757개	7,139개	19,799개

실제로 위 [표2-5]에서와 같이 스마트공장 구축 성과는 지원유형별

보급현황은 2020년 기준으로 7,139개에 이는다는 것을 통해 적극적인 지원을 시행되고 있음을 알 수 있다.

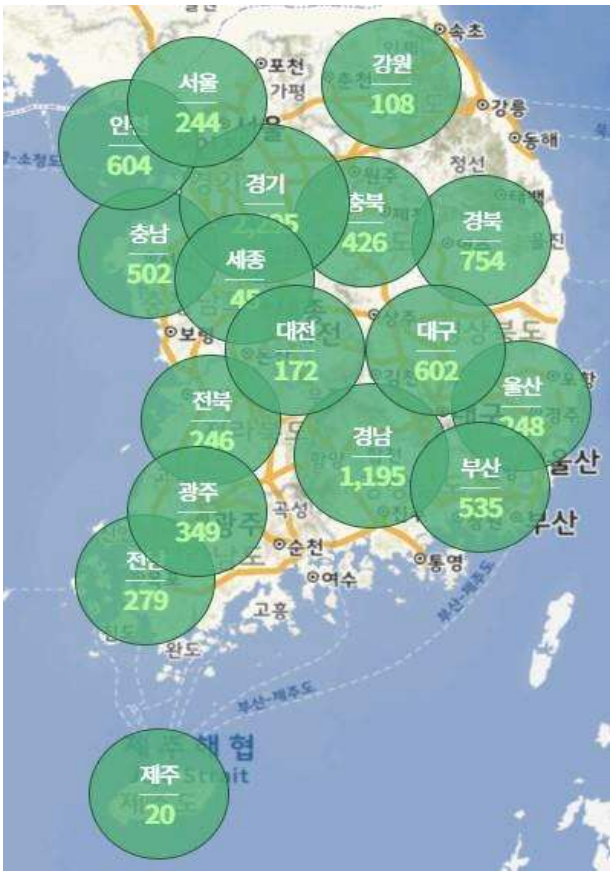
또한, [그림2-3]의 산업통상부 보도자료에는 2014년 최초 지원사업을 시작으로 2020년까지 1만개사까지 스마트공장 구축을 지원할 계획이었으며, 정부에서도 2022년까지 3만개사까지 스마트공장 구축을 지원할 계획을 9개 부처와 협의하여 추진하여 왔었음을 확인할 수 있다.



[그림 2-3] 스마트공장 추진현황 (산업통상자원부, 2017)

또한, 정부에서는 스마트공장의 원활한 추진과 전문성 있는 수행기관의 운영을 위해 2019년 7월 스마트제조혁신추진단을 출범시켰으며, 2021년 11월 현재까지 제조업을 포함한 산업 전반에 있어서 스마트공장 도입과 추진을 위한 다양한 지원사업을 진행하고 있다. 아래 [그림2-4]과 같이 2021년 현재 서울, 경기, 인천 등 수도권을 포함하여 전국적으로 많은 중

소기업이 스마트공장을 도입하여 운영하고 있으며 지속적인 고도화 등 시스템 개선을 추진하고 있다는 것을 알 수 있다.



[그림 2-4] 스마트공장 지역별 도입현황 (스마트제조혁신추진단, 2021)

이러한 스마트공장 지원을 신청하기 위한 중소기업의 범위는 아래 [표 2-6]과 같은 기준을 적용하고 있다.

[표2-6] 우리나라의 중소기업 기준 (중소벤처기업부, 2019)

규모	매출액
중기업	120억 ~ 1,500억
소기업	10억 ~ 120억

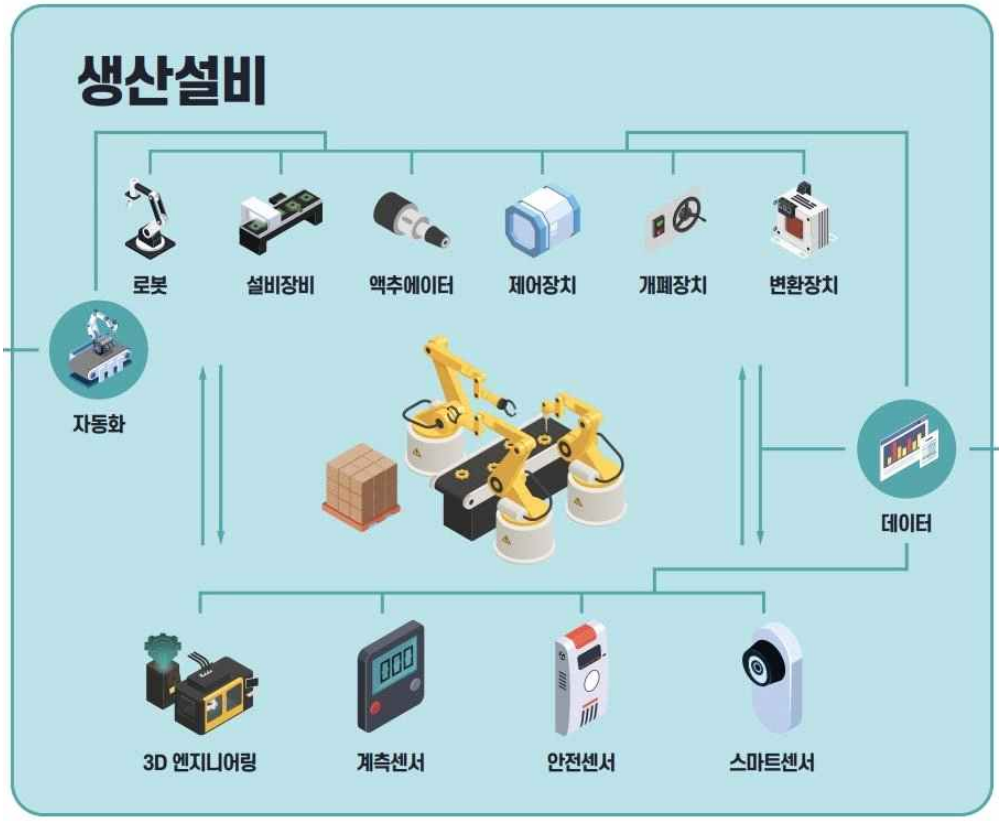
2.2 스마트공장에서의 보안요소 검토

위에서 살펴 본 바와 같이, 스마트공장은 기존의 제조업 생산 환경에 있어서의 자동화 시스템과는 기술적인 차이가 있는 특성을 가지고 있다. 해당 업무의 영역에서 별도로 고려되어야 하는 보안의 요소가 발생할 수 밖에 없는 것이다. 이러한 보안의 요소와 관련하여 현재 스마트제조혁신 추진단에서는 스마트공장을 구축할 때, 스마트공장의 수준별 구축의 범위를 제시하고 있으며 아래 [표2-7]의 내용과 같이 현장자동화 분야, 공장운영 분야, 기업자원관리 분야, 제품개발 분야, 공급사슬관리 분야 등에 대하여 ICT 미적용, 기초, 중간1, 중간2, 그리고 고도화의 수준으로 분류하고 있다. 이러한 분류 수준의 업무 영역별 스마트공장 구축시에 보안의 요소가 검토된다면 보다 효과적일 수 있다고 할 수 있다.

[표 2-7] 스마트공장 수준 총괄도 (스마트제조혁신추진단, 2021)

<table>
<tr><th>구분</th><th>현장자동화</th><th>공장운영</th><th>기업자원
관리</th><th>제품개발</th><th>공급사슬
관리</th></tr>
<tr><td rowspan="2">고도</td><td colspan="4">IoT / IoS 기반의 CPS화</td><td rowspan="2">인터넷
공간 상의
비즈니스
CPS
네트워크
협업</td></tr>
<tr><td>IoT / IoS화</td><td colspan="3">IoT / IoS(모듈)화
빅데이터 기반의 진단 및 운영</td></tr>
<tr><td>중간2</td><td>설비제어
자동화</td><td>실시간
공장제어</td><td>공장운영
통합</td><td>시뮬레이션과
일괄
프로세스
자동화</td><td>다품종 개발
협업</td></tr>
<tr><td>중간1</td><td>설비데이터
자동집계</td><td>실시간
의사결정</td><td>기능 간
통합</td><td>기술 정보
생성
자동화와
협업</td><td>다품종 생산
협업</td></tr>
<tr><td>기초</td><td>실적집계
자동화</td><td>공정물류
관리(POP)</td><td>관리 기능
중심 기능
개별 운용</td><td>서버를
통한
기술/납기
관리</td><td>단일 모기업
의존</td></tr>
<tr><td>ICT
미적용</td><td>수작업</td><td>수작업</td><td>수작업</td><td>수작업</td><td>전화와
이메일 협업</td></tr>
</table>

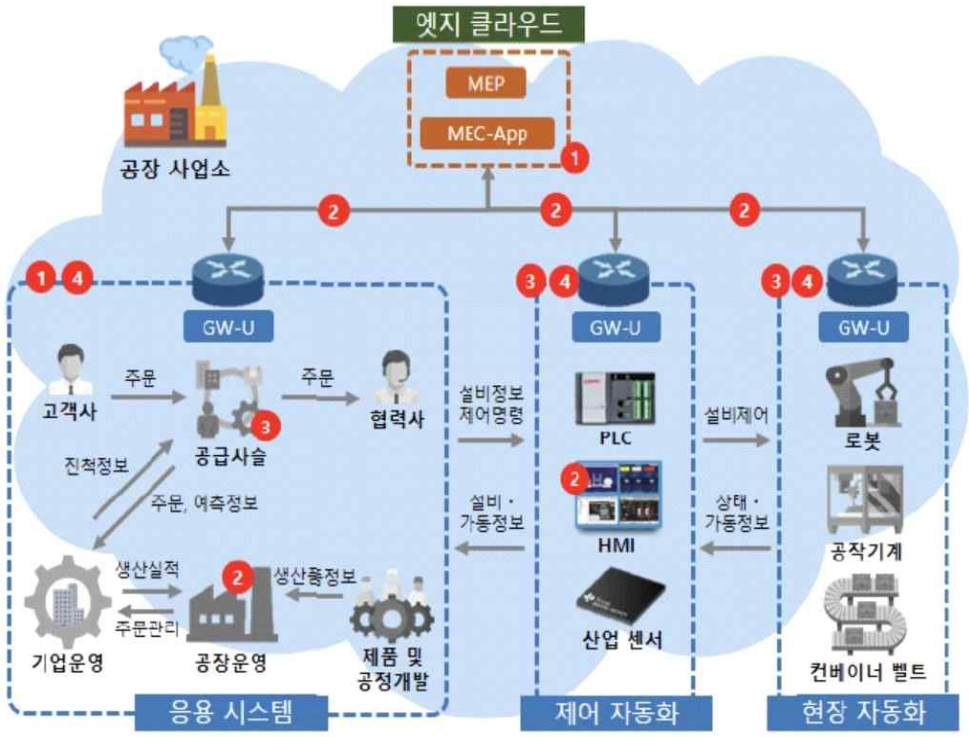
추가적으로 최근에 스마트공장 구축 영역별 고려사항에 대한 전반적인 안내를 위해 스마트제조혁신추진단에서는 아래 [그림2-5]와 같이 스마트공장 표준지도를 만들어서 제공하고 있다. 표준지도를 통해 각 영역별 스마트공장 연계 구축분야에 대한 안내와 함께 해당 영역에서의 고려사항 등을 별도로 정리하여 제공하고 있으며 스마트공장을 도입하여 구축코자 하는 중소기업에게 시스템 고려사항을 이해할 수 있도록 제공하고 있다.



[그림 2-5] 스마트공장 표준지도 (스마트제조혁신추진단, 2021)

한편 아래 [그림2-6]과 같이 한국통신학회에서 정의한 사례들을 통해 최근의 스마트공장에서의 보안요소는 일부분만 해당되는 것이 아니라 시스템의 구축과 관리, 하드웨어 및 소프트웨어 운영, 현장설비 등의 물리적 시스템 전반에 걸친 보안요소를 검토해야 한다. 첫 번째는 시스템 구축과

관리에 있어서의 기술적 보안요소가 있다. 두 번째는 공장운영 관리 및 관련 데이터의 관리를 위한 인원에 대한 보안요소가 있다. 세 번째는 데이터 수집 및 보관 등을 위한 하드웨어 운영에 있어서의 보안요소가 있다. 네 번째는 내외부 의사소통 및 데이터의 전송 등 운영에 있어서의 네트워크 보안요소가 있다. 다섯 번째는 전체적인 현장 및 설비의 접근에 대한 관리에 있어서의 물리환경적 보안요소가 있다고 정의할 수 있다. 이러한 내용을 바탕으로 선행연구의 검토를 진행하였다.



[그림 2-6] 스마트공장 영역별 보안위협 (한국통신학회, 2020)

2.3 선행연구 검토

허진(2018)은 'AHP 기법을 적용한 스마트공장 보안요인 우선순위에 관한 연구'에서 도출된 보안요인들을 대상으로 스마트공장 구축 시 적용해야 하는 우선순위를 도출하기 위해 계층화 모형을 구성하고, 스마트공장 구축에 종사하고 있는 민관합동 조직인 스마트공장추진단 기술위원 등 전문가를 대상으로 한 실증분석을 진행하였다. 실증분석은 AHP를 활용하였으며 이를 통해서 다양한 보안 위협으로부터 안전한 스마트공장 구현에 필요한 보안요인들의 상대적 중요도를 도출하고 이를 바탕으로 스마트공장 보안요인간의 우선순위를 제시하였다. 제시한 내용을 살펴보면 아래 [표2-8]과 같다.

[표 2-8] 스마트공장 운영을 위한 보안요인 선행연구 (허진, 2018)

세부분야	스마트공장 운영을 위한 보안요인
네트워크 보안 분야	방화벽 및 라우터 설치
플랫폼 · 서비스 보안 분야	서비스 암호화, 접근권한 통제
디바이스 보안 분야	사용자인증 식벼, 암호화

한석호(2019)는 '스마트 팩토리 보안관리 항목 연구'에서 스마트 팩토리 환경에 적합한 보안관리 항목의 도출 및 검증을 통해 기존 정보보호관리체계의 통제항목이 스마트 팩토리 환경을 완전하게 포함하지 못하는 것을 확인하였다. 그리고 통제항목간의 비교를 통해 보안관리 항목 중 기술적, 물리적 보안보다 관리적 보안 항목이 비중이 크게 증가한다는 것을 제시하였다. 제시한 내용을 살펴보면 아래 [표2-9]와 같다.

[표 2-9] 스마트팩토리 보안관리 항목 우선순위 선행연구 (한석호, 2019)

우선순위	항목
1	경영진 차원의 사고 관리

2	네트워크 이중화
3	긴급상황 복구절차 마련 및 주기 검증
4	경영진 인식 강화
5	코드변경 보안 절차
6	정밀한 R&R
7	가동중단 방지대체 설비
8	외부서비스 보안 방안 강화
9	별도의 교육체계
10	산업스파이 및 내부유출자 관리 강화
11	시스템 취약점 점검 및 정기보안감사
12	별도의 정책
13	스마트기기 반출입 엄격관리
14	권한분리 및 최소화
15	시스템 등급화 및 모듈화
16	시스템 설계부터 보안대책 구현
17	침입차단시스템
18	시스템 변경 기록관리
19	QWASP 준수 및 테스트
20	데이터접근 통제 강화
21	외부자 관리 강화
22	제어시스템 네트워크 분리
23	통신망 유출방지
24	데이터 CIA 보장방안
25	외주개발 보안관리
26	클라우드 보안관리 방안
27	별도의 테스트 환경 구성
28	무선 네트워크 보안 강화
29	경영마케팅 정보보안 강화
30	접근인가 엄격제한
31	스마트태그 통한 위협대응 방안
32	시스템(서비스) 가용성 보장 성능/용량유지

배순석,고승철(2019)은 ‘스마트팩토리 도입 기업의 보안강화 사례 연구’에서 안전한 스마트팩토리의 도입 및 운영을 위해 실제 스마트팩토리

보안 적용 사례를 제시하였다. 그리고 국내 · 외 표준과의 부합성을 비교 분석하여 타 연구의 이론적인 취약성 중심의 연구에서 한 단계 더 나아가 스마트팩토리 현장에서의 보안 강화 효과를 제시하였다.

신재훈(2018)은 '스마트 팩토리 보안요인에 대한 연구동향 분석 : 국내(RISS)와 해외(SCOPUS) 데이터 중심으로'에서 국내외 스마트팩토리와 관련된 연구들과 해외의 Industry 4.0와 관련된 연구를 조사하여 연구 내에서 보안에 대한 언급이 되어 있는지 파악해보고 각 연구별로 언급된 보안 관련 항목들을 취합하였다. 현재 스마트 팩토리 보안에 대해 어느 분야가 강조되어 있으며 강조되지 않고 있는지에 대해서도 파악하였다. 그리고 스마트 공장 추진단 기술위원이 선행한 연구에서의 보안사항과 스마트 팩토리 보안 관련 연구에서 언급하고 있는 보안사항들을 비교하여 스마트 팩토리에 필요한 보안요인들을 좀 더 명확하게 제시하였다.

이병권,김동원,노봉남(2016)은 '안전한 스마트공장 구축을 위한 위험우선순위(SFRPN) 기반 최소보안요구사항에 관한 연구'에서 국내 스마트공장에 적용 가능한 최소한의 정보보호 요구사항을 제시함으로써 효율적인 보안대책마련을 위한 기반이 될 수 있도록 제시하였다. 제시한 내용을 살펴보면, 아래 [표2-10]과 같다.

[표 2-10] 스마트공장의 최소보안요구사항 우선순위 선행연구 (이병권 外, 2016)

우선순위	항목
1	네트워크 접근 통제
2	암호화 정책
3	개인보관 정보 암호화
4	공개 서버 보안
5	영상정보처리기기 운영
6	중요정보 암호화 및 전송 시 암호화
7	패스워드 관리
8	원격 접근 통제
9	무선 네트워크 보안
10	회사 대표의 정보보호 인식

허진,정철용(2017)은 '융합 기반 스마트공장 보안의 위협과 대응 동향'에서 개별적으로 운영되던 산업현장에 ICT 환경의 변화에 따라 IoT, 클라우드, 빅데이터 그리고 모바일 등의 기술이 적용되면서 융합 환경으로 구성되어 최근 도입이 활발히 이루어지고 있는 스마트공장 모델의 성공적 추진을 위해 스마트공장과 융합보안에 대한 개념 등을 제시한 후, 동 분야에서 융합에 따라 발생하고 있는 보안 분야의 위협과 대응 동향을 제시하였다. 권순현,김지윤,임재덕,유일선(2020)은 '5G 기반의 스마트공장 보안 동향 분석'에서 예상되는 스마트공장의 보안 위협 및 보안 요구사항에 대하여 살펴보고, 이에 대처하기 위한 스마트공장 보안 표준 등을 분석하여 제시하였다. 제시한 내용을 살펴보면, 아래 [표2-11]과 같다.

[표 2-11] 5G 스마트공장의 보안요구사항 선행연구 (권순현 外, 2020)

순번	세부 항목
1	5G 기반 스마트공장 제조 장비의 전 주기 보안 위협을 통합 관제
2	5G 엣지 컴퓨팅 보안을 위한 네트워크 슬라이스 보안
3	스마트공장 가용성 보장을 위한 MEC 기반 위협 / 침입 감내
4	OT/IT의 안전한 연계를 위한 경계 보안

박은주(2017)는 'STRIDE 위협 모델링에 기반한 스마트팩토리 보안 요구사항에 관한 연구'에서 기술적인 관점으로 접근하여 시스템의 프로세스별 데이터의 흐름을 분석하고 스마트 팩토리의 시스템에 존재하는 취약점들을 수집한 뒤 마이크로소프트에서 개발한 위협 모델링 방법론인 STRIDE 모델을 사용하여 공격 시나리오를 도출하고 나서, 31가지 항목의 보안 요구사항을 체크리스트 방식으로 제시하였다.

위와 같은 선행연구들을 조사하여 분석한 결과, 기존의 선행연구들은 대부분 스마트공장 구축에 있어서 기술적인 분야에 있어서의 보안 영역을 강조하고 있었다. 세부적인 우선순위 보안항목의 제시에 있어서도 구축수

준 Level2이하 중소기업이 즉시 검토하고 도입 적용하기에는 어려움이 있는 분야의 내용도 존재한다는 것을 알 수 있었다. 다만, 스마트공장 구축에 있어서 검토가 필요할 수 있는 우선순위 보안항목에 대한 기본적인 방향성의 설정에 있어서 관리적 분야 및 물리적 분야의 보안요소에 대한 연구가 필요하다는 것을 판단할 수 있었다.

2.4 본 연구에 있어서의 차별성

위에서 살펴본 바와 같이 기존 연구는 스마트공장 구축에 있어서 일반적인 보안요소 중 우선적으로 고려해야하는 보안항목을 파악하는 정도 이거나 기술적인 부분에 있어서 검토되어야 하는 보안요소의 항목을 제시하는 내용이 대부분을 차지하고 있다. 그리고 이론적인 취약성 중심의 보안요소를 파악하여 해당 보안의 취약성이나 위험을 감소시킬 수 있는 보편화된 내용의 방향으로 개선방안을 제시하고 있다. 또한 기술적인 분야에서 최우선적으로 검토되어질 필요가 있는 보안요구사항에 대하여 제시하고 있음을 알 수 있다. 그리고 일부 연구에 있어서는 스마트공장 구축 기업 중 보안 강화 사례에 대한 제시를 통해 해당 기업이 고려해야 할 보안요소를 구체적으로 제시하고 있는 경우도 있었다. 하지만 이 연구에 있어서도 실질적으로 구축 기업의 규모나 운영 역량을 고려한 개선방안의 제시가 이루어지지 못했다는 부분은 한계성을 지니고 있었다.

그러나 스마트공장을 도입 및 구축하기 위하여 고려해야 하는 보안요소에 대하여 중소기업들이 실질적이고 현실적인 해당사항을 검토하기 위해서는 부족한 면이 있었다. 기존에 기업들이 가지고 있는 내부 역량과 ICT와 연계된 시스템 적용의 범위 등 현재 산업현장의 환경을 감안하고 스마트공장의 특성을 감안하여 적용할 수 있는 방안의 제시가 좀 더 필요하다고 판단되었다.

따라서, 본 연구는 선행연구를 통해 구체적으로 제시되지 못한 우선순위 보안항목에 대하여 중소기업 기준의 적용 가능한 도출을 목표로 하고 있다. 우리나라에서 일반적으로 중소기업의 기준으로 분류되고 있는 중기

업 (120억 ~ 1,500억) 및 소기업 (10억 ~ 120억)의 영역에서 현재 스마트공장을 구축하고자 하는 중소기업을 대상으로 현실적으로 적용이 가능하거나 구축시 우선적인 고려가 가능한 보안 우선순위 항목에 대한 도출 연구를 진행하였다. 검증을 위해서 스마트공장 구축수준 평가 결과에 있어서 스마트공장 구축수준 Level2 이하 중소기업의 현황을 가장 잘 파악하고 있는 전문가 및 실무자 집단에 대해 설문조사를 실시하였으며 우선순위 항목에 대하여 분석 및 검증하였다.

이와 함께 'A' 수행기관을 통해 실시된 스마트공장 구축수준 Level2 이하 중소기업의 스마트공장 수준확인 평가 결과 자료의 분석도 함께 진행하였다. 해당 자료의 분석결과가 실질적으로 전문가들이 제시한 중소기업이 고려할 보안 우선순위 항목과 일치되는 부분이 있는지 실증 분석하고 검증해 볼수 있었다. 이를 통해 스마트공장을 구축하고자 하는 중소기업이 현장에서 실제로 검토하여 적용 가능한 우선순위 보안항목의 타당성 있는 자료화를 도출할 수 있었다. 이를 통해 결론적으로 스마트공장 Level2이하 중소기업이 스마트공장을 구축함에 있어서 보안에 대한 실질적인 운영효과를 향상 시킴으로 최종적으로 심리적 안정성을 부여하고자 한다.

향후에 스마트공장을 구축함에 있어서 구축수준 Level2 이하 중소기업이 고려할 보안 우선순위 항목에 대한 방향성을 제시함으로써 새로운 기준을 제언하고자 한다.

III. 중소기업의 보안수준 향상을 위한 우선순위 항목 도출

III장에서는 본 연구에 있어서 중소기업의 보안수준 향상을 위해 고려할 스마트공장 보안 우선순위 항목 도출방법, 연구대상 및 자료수집 방법에 대하여 제시하고자 한다.

3.1 중소기업의 보안수준 향상을 위한 우선순위 항목 도출방법

본 연구에서는 II장에서 조사한 선행연구 결과를 바탕으로 스마트공장 보안관리 항목 중 방향성 설정에 참고할만한 보안 항목에 대하여 우선적으로 파악하고, 해당 보안관리 항목 중 실질적으로 스마트공장 구축수준 Level2 이하의 중소기업이 고려할 수 있는 항목을 8가지로 정리하여 설문문항을 구성하였다. 또한, 정리한 설문문항을 근거로 해당 문항에 대한 전문가 설문을 진행하여 본 연구에서 검토하고 실증코자 한 스마트공장 구축수준 Level2 이하의 중소기업이 고려할 스마트공장 보안 우선순위 항목을 도출하였고, 추가적으로 해당 항목에 대하여 'A' 수행기관에서 2020년 ~ 2021년 2년간 심사한 스마트공장 수준확인 심사보고서와 비교분석을 통해 전문가 의견에 대한 타당성 검증을 실시하였다. 그리고, 이러한 실증결과를 토대로 기존의 선행연구에서는 제시되지 못한 보안 우선순위 항목을 제시함으로써 보다 차별성있고 현실적으로 적용가능한 스마트공장 구축수준 Level2 이하의 중소기업이 중소기업의 보안수준 향상을 위해 고려할 스마트공장 보안 우선순위 항목을 제시하고자 하였다.

선행연구를 통해 스마트공장 구축시 고려해야 할 보안 항목들은 아래 [표3-1]과 같이 각 영역별로 도출하여 정리할 수 있었다.

[표 3-1] 선행연구에서 추출한 스마트공장 보안관리 항목
(연구자 재구성, 2021)

영역		내용	고려사항
1	보안정책	스마트공장 보안을 위한 정책, 표준지침, 가이드라인 제정 (ISO27001 A.5항 정보보안정책)	정책 수립 및 적용
		스마트공장 보안을 위한 정책의 주기적 검토 (ISO27001 A.5항 정보보안정책)	주기적 정책검토
2	보안조직	스마트공장 보안 역할 부여 (ISO27001 A.6항 정보보안 조직)	담당자 지정
		스마트공장 보안에 대한 책임과 권한 부여 (ISO27001 A.6항 정보보안 조직)	책임과 권한 부여
		스마트공장 보안을 위한 외부자 보안 관리 (ISO27001 A.7항 인적자원 보안)	외부자 보안관리
3	인적보안	중요정보 유출 방지를 위한 인적보안 관리 (ISO27001 A.7항 인적자원 보안)	인적보안
		협력업체 외부 인원에 대한 인적보안 관리 (ISO27001 A.15항 공급자 관계)	협력업체 보안
		스마트공장 보안에 대한 교육훈련의 계획 및 시행 (ISO27001 A.7항 인적자원 보안)	교육계획 및 시행
		경영진의 정보보안 인식여부 (ISO27001 A.7항 인적자원 보안)	경영진 보안 인식
4	자산관리	정보자산 식별 및 등급화 필요 (ISO27001 A.8항 자산관리)	자산 관리

영역		내용	고려사항
5	암호화	중요 정보 암호화 정책 수립 및 적용 (ISO27001 A.10항 암호화)	암호화 정책
		데이터에 대한 암호화 및 관리 (ISO27001 A.10항 암호화)	암호화된 데이터 관리
6	접근통제	시스템 접근통제 기능 설정 및 적용 (ISO27001 A.9항 접근통제)	시스템 접근통제
		중요정보에 대한 보관정책 수립 및 적용 (ISO27001 A.9항 접근통제)	중요정보 보관정책
		사용자별 역할, 접근권한의 설정 및 적용 (ISO27001 A.9.2항 사용자 접근관리)	사용자 접근통제
		로그인 및 패스워드 정책 수립 및 적용 (ISO27001 A.9.4항 시스템 접근통제)	패스워드 정책
7	물리/ 환경적 보안	제조시설 등 보호구역의 지정 및 운영 (ISO27001 A.11항 물리적 및 환경적 보안)	보호구역 지정
		시설 내 보안관리를 위한 모니터링 방안 적용 (ISO27001 A.11항 물리적 및 환경적 보안)	모니터링 방안
		보안장애 대비 설비 운영 적용 (ISO27001 A.11항 물리적 및 환경적 보안)	장애 대응 설비

영역		내용	고려사항
8	운영보안	시스템 취약점 점검 및 주기적 보완 검토 (ISO27001 A.12.6항 기술적 취약점 관리)	시스템 무결성 점검
		시스템 가용성 확보를 위한 모니터링 및 절차 적용 (ISO27001 A.12항 운영보안)	시스템 가용성 모니터링
		정보시스템 감사 계획 수립 및 시행, 모니터링 실시 (ISO27001 A.12.7항 정보시스템 감사 고려)	정보시스템 정기 감사
9	통신보안	시스템 네트워크 운영 지원 (ISO27001 A.13.1항 네트워크 보안 관리)	시스템별 네트워크
		외부로의 시스템 정보 전송에 대한 안전성 확보 (ISO27001 A.13.2항 정보전송)	안전한 정보 전송
10	준거성	개인정보 등에 대한 안전한 관리 및 법규 준수 (ISO27001 A.18.1항 법적 요구사항 준수)	개인정보보호
		해킹 등 위협 대비를 위한 방안 적용 (ISO27001 A.18.2항 정보보호 검토)	산업보안

3.2 연구대상 및 자료수집 방법

선행연구를 분석하여 위와 같이 추출한 스마트공장 보안관리 항목 중 실제로 스마트공장 구축수준 Level2 이하 중소기업이 보안수준 향상을 위해 고려할 보안 우선순위 항목을 도출하고 검증하기 위하여 현재 스마트공장과 관련한 전문가 (학계 / 스마트공장 관련 평가위원 / 스마트공장 수준확인 심사원 / SI 개발업체 대표자 / 스마트공장 관련 컨설턴트 / 스마트공장 업무 실무자)를 대상으로 설문조사를 실시하였다. 설문문항의 구성은 위에서도 언급한 바와 같이 선행연구를 통해 각 영역별로 도출한 보안 항목 중 ISO27001 요구사항 및 법적 요구사항 등과이 비교를 통해 공통된 8가지 항목의 문항으로 분류하여 재구성 하였다. 이 설문지를 이메일 등과 같이 온라인 방식을 통해 전달 및 회신을 받았으며 자기기입식 조사를 통해 진행하였다. 설문 답변 중 스마트공장 관련 보안위협이 크지 않다고 답변하였거나 스마트공장 구축시 보안요인이 고려되지 않아도 된다고 답변한 설문을 제외하였으며 실제 유효하게 파악된 설문 80개를 대상으로 실증분석을 통한 타당성 검증을 실시하였다.

그리고, 아래와 같이 스마트공장 관련 평가위원 및 수준확인 심사원은 해당 기관과 협회에서 적법한 선발과정을 거쳐 전문가로써의 자격을 부여받았기 때문에 본 연구의 검증과정에 적합한 전문가들이라고 할 수 있다.

스마트공장 평가위원 자격요건 (스마트제조혁신추진단)
□ 평가위원 자격요건 1. 산업계 가. 관련분야 박사학위 소지자로서 해당분야 3년 이상의 경력을 가진 자 나. 관련분야 석사(학사)학위 소지자로서 해당분야 5년(7년) 이상 경력자 다. 관련분야 부장급 또는 이에 상당한 직급 이상인 자 2. 학계 : 대학의 관련분야 전임강사 이상인 자 3. 연구(공공기관 등)계 가. 관련분야 박사학위 소지자로서 해당분야 3년 이상의 경력을 가진 자 나. 관련분야 석사(학사)학위 소지자로서 해당분야 5년(7년) 이상 경력을 가진 자 4. 엔지니어링산업진흥법 시행령에 따른 관련분야 특급기술자 이상

스마트공장 수준확인 심사원 자격요건 (중소벤처기업부)
□ 심사원 자격요건 • 기술사를 취득한 자로 관련분야에서 3년 이상 근무경력이 있는 자 • 관련분야 박사학위를 취득한 자로 해당분야에서 3년 이상 근무경력이 있는 자 • 관련분야 석사학위를 취득한 자로 해당분야에서 5년 이상 근무경력이 있는 자 • 관련분야 학사학위를 취득한 자로 해당분야에서 7년 이상 근무경력이 있는 자 • 관련분야에서 10년 이상 근무경력이 있는 자

- 전문가 대상수 : 스마트공장 관련 업무를 진행한 전문가 그룹
(총 90명 - 설문 제외 전문가 10명 포함)

[* 스마트공장 구축 및 운영, 고도화 업무 관련 전문가 선정 기준

- 스마트공장 관련 평가위원 : 평가위원 경력 3년 이상 및 평가횟수 3회 이상자
- 스마트공장 수준확인 심사원 : 심사위원 경력 3년 이상 및 심사횟수 3회 이상자
- 스마트공장 관련 컨설턴트 : 컨설팅 경력 3년 이상 및 컨설팅 횟수 3회 이상자
- 스마트공장 업무 실무자 : 스마트공장 관련업무 3년 이상자]

또한, 'A' 수행기관에서 2020년 및 2021년 2년간 심사한 스마트공장 수준확인 심사보고서를 아래와 같이 실증분석하여, 전문가 설문을 통해 파악한 내용과 실제 스마트공장 구축 수준 Level2 이하 중소기업의 현황과의 비교분석을 통해 보다 현실적이고 적용 가능한 기업 규모별 보안 가이드라인을 도출 및 제시하고자 한다.

다만, 스마트공장 수준확인 심사보고서 내 평가문항과 스마트공장 전문가들의 설문문항에 있어서 일부 문항이 정확하게 일치하고 있지는 않지만, 문항의 비교분석을 통해 비슷한 내용을 포함하고 있는 문항은 최종 보안 우선순위 항목을 도출하는데 있어서 1개의 문항으로 통합하여 우선순위 항목을 도출하도록 정리하였다.

- 심사년도별 대상업체수 : 2020년 - 60개업체 / 2021년 - 50개업체 (총 110개 업체)

[* 세부 보고서 업체 분류

- 종업원수 : 10명 이하, 11명 ~ 30명, 31명 ~ 50명, 51명 ~ 100명, 101명 이상의 5개 인원수 항목으로 분류
- 매출액 : 30억 이하, 31억 ~ 50억, 51억 ~ 100억, 101억 이상의 4개 매출액 항목으로 분류
- 업종군 : 18개 제조업, 비제조업으로 분류]

[* 세부 보고서 분석 항목

– 분석항목 : 경영진 인식, 보안교육, 담당자 여부, 도입 프로그램, 물리환경적 보안, 기타
(각 항목별 수준을 확인하기 위한 자료화)]

결과적으로 연구대상 및 자료수집 방법을 정리한다면, 조사대상, 조사분석, 결과도출 등의 항목에 대하여 위에서 정리한 전문가 설문과 스마트공장 수준확인 심사보고서를 분석하여 결과를 도출한 아래 [표3-2]와 같다.

[표 3-2] 연구대상 및 자료수집 방법

구분	조사대상	조사분석	결과 도출
	순서1	순서2	
내용	전문가 대상 설문조사서 (8개 문항 등)	스마트공장 수준확인 심사보고서	보안가이드라인 제시를 위한 항목 도출
방법	1) 이메일을 통한 자기기입식 조사 2) 관련 설문조사 항목별 전문가 의견 분석	1) 110개 업체 대상 현황 분석 2) 종업원수 / 매출액 / 업종 등 3) 분석항목에 대한 기업 수준 현황 도출	기업 규모별 보안가이드라인에 대한 우선순위 항목 도출 및 제시

※ 최종 보안 우선순위 항목 도출을 위해, 전문가 설문을 통해 확인된 보안 우선순위 항목과 스마트공장 수준확인 심사보고서를 통해 확인된 중소기업의 보안 적용 현황 수준을 비교분석하여, 최종적으로 중요도 빈도를 차지하고 있는 수준을 10점 점수로 환산을 통해 배점도가 높은 항목을 우선순위 보안 항목으로 도출하여 제시하였다.

IV. 중소기업의 보안수준 향상을 위한 우선순위 항목 도출 검토

4.1 실증분석을 통한 중소기업의 보안수준 향상을 위한 우선순위 항목 타당성 검증

4.1.1 검증 절차

연구 결과 작성된 중소기업의 보안수준 향상을 위해 고려할 스마트공장 보안 우선순위 항목 도출에 대한 타당성 검증을 진행하기 위해 전문가 설문조사와 'A' 수행기관에서 진행한 스마트공장 수준확인 심사보고서의 현황에 대한 비교분석을 통해 실증분석하였다.

설문조사의 조사대상은 현재 스마트공장과 관련한 전문가 (학계 / 스마트공장 관련 평가위원 / 스마트공장 수준확인 심사원 / 스마트공장 프로그램 개발업체 대표자 / 스마트공장 지도 컨설턴트 / 스마트공장 업무 실무자)로 조사협조 이메일을 발송한 후 자기기입식 응답방식으로 메일에 대한 회신을 받았다. 총 90명이 설문서 조사에 응답하였으나 그 중 스마트공장 관련 보안위협이 크지 않다고 답변하였거나 스마트공장 구축시 보안요인이 고려되지 않아도 된다고 답변한 설문을 제외하고 80개 설문에 대한 데이터를 최종적으로 확보하여 실증분석을 진행하였다. 연구 결과 도출된 항목에 대해서는 전문가 의견에 대한 항목별 빈도분석(비율)을 통해 기존에 제시된 일반적인 보안항목들 중 현실적으로 구축시 고려할 보안 우선순위 항목에 대해 분석 및 검증을 진행하였다. 관련한 보안 우선순위 항목을 최종적으로 도출하고 정리하였으며 현실적으로 적용가능하고 신뢰성있는 보안 우선순위 항목을 제시하고자 하였다.

이와 더불어, 'A' 수행기관에서 실제로 스마트공장과 관련한 기업의 수준확인 심사가 진행된 스마트공장 수준확인 심사보고서를 실증 분석하였

다. 중소기업 기준 스마트공장 구축수준 Level2 이하의 공장들이 보안에 대해 가지고 있는 역량이나 수준을 확인하였다. 전문가 설문에서 제시된 의견과의 비교 분석을 통해 보다 현실적으로 중소기업이 고려할 보안 우선순위 항목에 대한 도출과 적용 우선순위 제시를 진행코자 하였다. 설문에 응답한 전문가 80명의 특성을 정리하면 다음과 같다.

[표 4-1] 설문조사 응답자 특성 - 근무분야

소속	학계 전문가	스마트공장 평가위원 및 수준확인 심사원	스마트공장 프로그램 개발업체 대표자	스마트공장 지도 컨설턴트 및 업무 실무자
사례수(명)	6	27	9	38
비중(%)	7.5	33.8	11.3	47.4

[표 4-1]과 같이 설문 응답자의 근무분야에 있어서는 스마트공장 지도 컨설턴트 및 업무 실무자가 전체 중 47.4%를 차지하고 있어 가장 많은 응답을 해주었으며, 스마트공장 평가위원 및 수준확인 심사원 33.8%, 스마트공장 프로그램 개발업체 대표자 11/3%, 학계 전문가가 7.5% 수준의 응답비율을 차지하였다.

전체적인 응답자 비율을 분석한 결과, 스마트공장에 대한 충분한 이해도가 있으며, 스마트공장과 연계한 내용에 대한 의견에 대하여 신뢰성을 가질 수 있는 근무분야의 전문가들이 답변해주었다는 내용을 확인할 수 있었다.

[표 4-2] 설문조사 응답자 특성 - 경력년수

경력년수	3년 ~ 5년	6년 ~ 10년	11년 ~ 15년	16년 이상
사례수(명)	2	18	12	48
비중(%)	2.5	22.5	15	60

[표 4-2]와 같이 각 분야별 전문가들의 경력년수를 분석한 결과, 6년 이상 업무 경력을 가지고 있는 전문가 비율이 전체인원 중 98%를 차지할 정도로 설문 응답자들의 전문성은 해당기간 스마트공장과 관련한 의견을 확인하는데 있어서 충분히 신뢰할 만한 수준이라는 것을 확인할 수 있었다.

[표 4-3] 설문조사 응답자 특성 - 학력

학력	학사	석사	박사
사례수(명)	44	27	9
비중(%)	55	33.7	11.3

[표 4-3]과 같이 전문가들의 학력에 있어서도 단순히 학사만 존재하는 것이 아닌 석사 및 박사의 차지비율 역시 45% 정도를 보이고 있었으며, 석사 및 박사의 전공분야를 확인한 결과, 석사 및 박사 응답자 총 36명의 전공분야가 산업공학분야 7명, 기계공학분야 8명, 품질 및 시스템 관련분야 10명, 컨설팅 분야가 11명으로 보다 전문가적인 시각과 의견제시

가 가능한 수준이라고 파악되었다. 또한, 학력이 학사인 전문가들 역시 관련업에 6년 이상 종사한 전문가들이 대부분으로 충분한 전문성을 가진 전문가들임을 확인할 수 있었다. 이러한 결과를 종합해볼 때, 전문가들의 스마트공장 보안과 관련한 답변에 대해서도 신뢰성을 부여할 수 있는 수준이라고 확인되었다.

[표 4-4] 설문조사 응답자 특성 - 스마트공장 직접 업무 경력유무

항목	유	무
사례수(명)	69	11
비중(%)	86.3	13.7

[표 4-4]와 같이 보다 구체적으로 스마트공장과 관련한 직접적인 업무 경력을 확인하기 위해 스마트공장 직접 업무 경력유무를 확인한 결과, 전체 전문가 중 직접 업무를 진행한 경력이 있는 전문가가 86.3% 수준이었으며, 직접적인 업무 진행한 경력이 없다고 답변한 전문가가 13.7%의 수준을 보였다. 다만, 직접적인 업무 경력이 없다고 답변한 전문가 11명의 답변을 분석한 결과, 해당 답변을 한 전문가 분포는 스마트공장 수준확인 심사원 11명으로 확인되었으며, 관련 전문가 11명 모두 최근 2년내 스마트공장 관련 프로젝트 수행 경험이 없어 관련 답변을 한 것으로 분석되었다. 따라서, 전체 설문 응답 전문가 모두 실질적으로는 스마트공장과 관련한 업무 경력은 직접적인 업무 경력이 아니더라도 유사 경력이 있다는 것을 확인할 수 있었으며, 충분히 전문가적인 시각을 보유하고 있다는 내용이 확인되었다.

다음으로, 'A' 수행기관에서 2020년 및 2021년 진행한 110개 중소기업의 스마트공장 수준확인 심사보고서에 대한 특성을 정리하면 다음과 같다고 할 수 있다.

[표 4-5] 스마트공장 수준확인 심사보고서 특성 - 종업원수

	10명 이하	11명 ~ 30명	31명 ~ 50명	51명 ~ 100명	101명 이상
2020년	21	20	6	9	4
2021년	24	12	4	10	0
합 계	**45**	**32**	**10**	**19**	**4**
비중(%)	**40.9**	**29.1**	**9.1**	**17.3**	**3.6**

[표 4-5]와 같이 'A' 수행기관에서 진행한 스마트공장 수준확인 심사보고서 분석을 통해 확인할 결과, 스마트공장 구축수준 Level1 및 Level2 중소기업 중 70% 정도가 30명 미만의 종업원수를 보유하고 있었으며, 기업의 규모가 크지 않다는 것을 확인할 수 있었다.

[표 4-6] 스마트공장 수준확인 심사보고서 특성 - 매출액

	30억 이하	31억 ~ 50억	51억 ~ 100억	101억 이상
2020년	31	7	7	15
2021년	24	4	10	12
합 계	**55**	**11**	**17**	**27**
비중(%)	**50**	**10**	**15.5**	**24.5**

또한, [표 4-6]과 같이 해당 기업별 매출액 수준을 분석한 결과, 50억

이하 기업이 60%, 51억 ~ 100억 이하 기업이 15.5%, 101억 이상 기업이 24.5%로 대부분의 기업이 50억 이하의 매출액 수준을 보이고 있었다.

[표 4-7] 스마트공장 수준확인 심사보고서 특성 - 업종

	기계/자동차	전기/전자	의료/화학	농식품/음식료	비제조업
2020년	23	8	19	8	2
2021년	30	8	10	2	0
합 계	**53**	**16**	**29**	**10**	**2**
비중(%)	**48.2**	**14.5**	**26.4**	**9.1**	**1.8**

[표 4-7]과 같이 스마트공장 수준확인 심사보고서 해당 기업별 업종을 분석한 결과, 제조업의 비중이 98.2%에 해당하였으며 대부분 스마트공장을 도입 및 구축하는 기업들은 제조업에 해당된다는 것을 확인할 수 있었다. 다만, 제조업에 해당하는 기업들의 세부 업종에 있어서는 110개 기업을 대상으로 스마트공장 수준확인 심사보고서를 분석하였기 때문에 업종의 한계성은 일부 있을 수 있었다.

그러나, 110개 업종에 대한 세부 분류에 있어서는 기계/자동차 업종이 48.2%, 의료/화학 업종이 26.4%로 제품을 가공하거나 근로자보다 생산성 확보가 가능한 분야에 있어서 스마트공장을 도입 및 구축하고 있다는 내용은 확인할 수 있었다.

위와 같이, 실증분석을 통한 기업 규모별 스마트공장 보안가이드라인 타당성을 검증하기 위한 검증절차를 적용하여 다음의 조사 결과를 도출하게 되었다.

4.1.2 조사 결과

조사 결과에 있어서는 우선적으로 전문가 설문을 통해 전문가들이 본 관점에서 스마트공장 구축수준 Level2 이하의 중소기업에 대한 현재의 중소기업 보안수준 현황 확인과 함께 스마트공장 도입 및 구축시 보안 검토 필요항목에 대하여 빈도 분석을 통해 결과 도출을 실시하였다.

그리고, 해당 내용을 바탕으로 전문가들의 시각으로 스마트공장 구축수준 Level2 이하의 중소기업에 있어서 필요한 각 영역별 보안내용에 대해 5점 척도로 필요수준의 빈도 분석을 통해 세부적인 보안 검토 영역을 도출하였다.

또한, 최종적으로 이러한 세부적인 보안의 영역 중 전문가들이 생각하는 스마트공장 구축수준 Level2 이하의 중소기업에 있어서의 보안 우선순위 적용항목에 대한 빈도 분석을 통해 최종적으로 중소기업의 보안 현황 수준, 전문가들이 필요하다고 생각하는 보안의 영역별 내용, 해당 중소기업이 보안 적용시 우선순위 적용항목을 도출하여 타당성 검증의 대상자료로 활용코자 하였다.

이와 함께, 'A' 수행기관에서 2020년 및 2021년 실시한 스마트공장 수준확인 심사보고서의 분석을 통해 실제로 스마트공장 구축수준 Level2 이하 중소기업의 보안 인식수준, 인력운영 현황, 보안시스템 및 프로그램 운영내용 등을 확인하였다. 그리고 전문가들이 제시한 보안의 우선순위 적용항목이 현실적으로 해당 중소기업의 보안운영 전반에 걸쳐 우선순위 항목이 될 수 있는지에 대하여 전문가 설문조사 결과 내용과의 비교를 통해 타당성 검증을 진행코자 하였다.

다만, 중소기업의 보안수준 향상을 위해 고려할 보안 우선순위 항목을 도출하는 과정에서 8가지의 보안항목에 대하여 전문가들이 보안에 대한 필요 항목들을 답변한 결과가 조사되었으나, 조사 후 스마트공장 구축수준 Level2 이하 중소기업의 보안운영 현황과의 비교분석 과정에서 실제로 항목 내용의 표기는 다르지만 보안 우선순위 항목에 있어서는 같은 분야의 내용으로 분류될 수 있는 항목들이 존재한다는 것이 확인되었다. 따라

서 최종적인 중소기업이 고려할 보안 우선순위 항목의 도출은 비슷한 내용과 관련한 분야가 같은 항목을 재정리하여 5가지 항목의 우선순위로 결론을 도출하게 되었다. 이러한 실증분석 결과의 전반적인 내용을 가지고 최종적으로 4.2.1항에서 중소기업의 보안수준 향상을 위해 고려할 보안 우선순위 항목의 도출을 통해 스마트공장 구축에 있어서 중소기업의 보안 수준 향상을 위해 고려할 보안 우선순위 항목을 기존이 연구들보다 현실성 있게 제시코자 하였다.

[표 4-8] 스마트공장 도입 및 구축에 따른 중소기업 보안수준 현황

구 분	매우 낮음	낮음	높음	매우 높음
1. 스마트공장 보안 필요성	0 (0%)	10 (12.5%)	**39 (48.8%)**	31 (38.7%)
2. 경영진 및 실무자의 보안 인식 여부	21 (26.2%)	**30 (37.5%)**	**25 (31.3%)**	4 (5%)
3. 스마트공장 도입 및 구축시 보안 영역 검토 여부	21 (26.2%)	**33 (41.2%)**	25 (31.3%)	1 (1.3%)
4. 스마트공장 도입 및 구축시 보안 투자 검토 여부	21 (26.2%)	**48 (60%)**	10 (12.5%)	1 (1.3%)
5. 스마트공장 담당자 지정 여부 (겸임포함)	21 (26.2%)	**48 (60%)**	10 (12.5%)	1 (1.3%)
6. 보안관련 설비 및 시스템 검토 여부	21 (26.2%)	**45 (56.2%)**	13 (16.3%)	1 (1.3%)
7. 보안관련 프로세스 검토 여부	9 (11.3%)	**49 (61.1%)**	19 (23.8%)	3 (3.8%)
8. 보안관련 인증 검토 여부	27 (33.8%)	**40 (49.9%)**	13 (16.3%)	0 (0%)

스마트공장 관련분야 전문가들의 스마트공장 구축수준 Level2 이하의 중소기업에 있어서 현재 보안수준 현황을 확인해 본 결과, 1항의 보안 필요성에 있어서 87.5%가 필요성에 대해 높음 이상으로 답변하여 실제로 보안이 필요하다고 할 수 있었다. 2항의 경영진 및 실무자의 보안 인식 여부에 있어서는 낮음으로 답변한 전문가가 37.5%, 높음으로 답변한 전문가가 31.3%로 인식하고 있는 기업과 그렇지 못한 기업이 비슷한 수준을 보였다. 3항에서 보안영역에 대한 기업의 검토 여부에 있어서도 낮음으로 답변한 전문가가 41.2%, 높음으로 답변한 전문가가 31.3%로 검토하고 있는 기업과 그렇지 못한 기업이 비슷한 수준을 보였다. 4항의 보안 투자 검토 여부에 있어서는 86.2%의 기업이 검토하지 않고 있다는 답변이 나왔으며 그만큼 비용소요에 있어서 해당 기업들이 소극적인 모습을 보이고 있다고 할 수 있었다. 5항의 스마트공장 담당자 지정 여부에 있어서도 86.2%의 기업이 지정하고 있지 않다고 답변하였으며, 6항의 보안관련 설비 및 시스템 검토 여부에 있어서도 82.4%의 기업이 검토하지 않고 있다고 답변되는 등 인건비, 설비 및 시스템 도입에 따른 비용적인 부담을 해당 기업들이 느낀다고 할 수 있었다. 7항의 보안관련 프로세스 검토 여부에 있어서도 61.1% 정도의 기업이 검토하고 있지 않다고 답변하였으며, 8항의 보안관련 인증 검토 여부에 있어서도 83.7%정도의 기업이 검토하고 있지 않다고 답변하는 등 전반적인 프로세스 및 관리체계에 있어서도 해당 기업들이 미흡한 모습을 보이고 있다고 할 수 있었다.

다음으로, 스마트공장 도입 및 구축시 보안 검토 사항에 대한 중요도를 전문가 설문결과에서 정리해보면, 아래와 같다.

[표 4-9] 스마트공장 도입 및 구축시 보안 검토 사항 중요도

구 분	중요하지 않음	보통	중요	매우 중요
1. 스마트공장 보안 검토 (프로세스 구축 포함)	0 (0%)	5 (6.5%)	**35 (43.8%)**	**40 (49.7%)**
2. 경영진 및 실무자의 보안 교육	0 (0%)	3 (3.9%)	**42 (52.3%)**	35 (43.8%)
3. 스마트공장 담당자 지정 운영 (겸임포함)	0 (0%)	2 (2.6%)	**48 (59.9%)**	30 (37.5%)
4. 보안에 대한 투자	0 (0%)	1 (1.3%)	**47 (58.7%)**	32 (40%)
5. 설비 및 시스템 구축	0 (0%)	1 (1.3%)	**45 (56.2%)**	34 (42.5%)

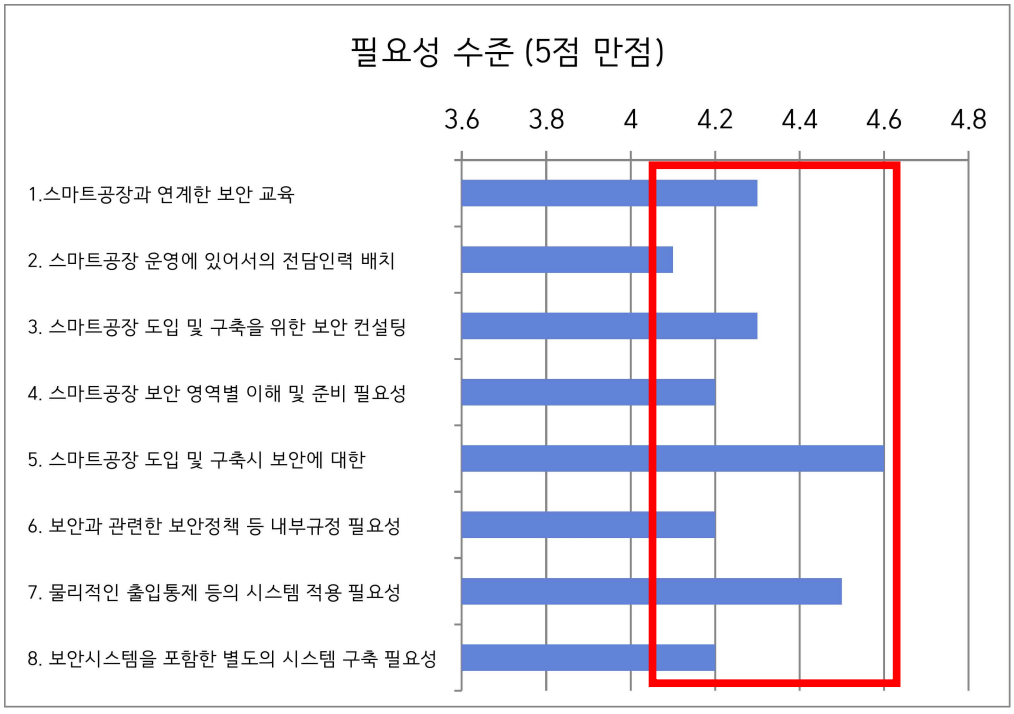
[표 4-9]와 같이 스마트공장 도입 및 구축에 있어서 보안 검토 (프로세스 구축 포함)가 중요하다는 의견이 93.5% 수준으로 응답되었으며, 경영진 및 실무자의 보안 교육 역시 중요하다는 의견이 96.1% 수준으로 응답되었다. 스마트공장 도입 및 구축에 따른 담당자 지정 (겸직 포함) 운영이 필요하다는 항목에 있어서도 중요하다는 의견이 97.4% 수준으로 응답되었고, 보안에 대한 투자도 중요하다는 의견이 98.7% 수준으로 응답되었다. 마지막으로, 스마트공장 도입 및 구축에 있어서 설비 및 시스템 구축이 중요하다는 의견도 98.7% 수준으로 응답될 정도로 전반적인 보안 검토사항에 대하여 전문가들은 모두 중요하다고 생각하고 있었다.

이러한 답변을 바탕으로, 단순히 스마트공장 도입 및 구축시 보안에 대한 검토 필요성이 중요하다는 것만 확인하는 것이 아니라, 실제로 전문가들이 생각하는 보안 검토사항 중 세부 영역별 필요성 수준은 어느정도인지에 대해서도 5점 척도 기준으로 좀 더 구체적으로 설문 분석하였으며, 해당 결과는 아래와 같았다.

[표 4-10] 스마트공장 도입 및 구축시 보안 영역별 필요성 수준

세부 보안영역	필요성 수준 (5점 만점)
1. 스마트공장과 연계한 보안 교육	4.3
2. 스마트공장 운영에 있어서의 전담인력 배치	4.1
3. 스마트공장 도입 및 구축을 위한 보안 컨설팅	4.3
4. 스마트공장 보안 영역별 이해 및 준비 필요성	4.2
5. 스마트공장 도입 및 구축시 보안에 대한 지원의 필수적 필요성	4.6
6. 보안과 관련한 보안정책 등 내부규정 필요성	4.2
7. 물리적인 출입통제 등의 시스템 적용 필요성	4.5
8. 보안시스템을 포함한 별도의 시스템 구축 필요성	4.2

위 결과에 대한 각 항목별 필요성 수준을 도표화하면, 아래 [그림 4-1]과 같고 각 영역별 수준을 한눈에 확인할 수 있다.



[그림 4-1] 스마트공장 도입 및 구축시 보안 영역별 필요성 수준 도표

위 [표 4-10]과 같이 전체 전문가 응답자 80명에 대한 각 설문 문항별 1점 ~ 5점 척도에 대한 필요성 수준의 답변 결과를 총합하고 평균하여 각 문항별 배점 점수로 환산하여 결과치를 산출한 결과, 1항 ~ 8항까지 스마트공장 도입 및 구축시 보안 영역별 필요성에 대한 답변이 전 문항에 있어서 배점 척도 '4'점 이상의 수준으로 전문가 모두 필요성이 높다라는 결과치가 나왔다. 특히, 해당 영역 중 스마트공장 도입 및 구축시 보안에 대한 지원의 필수적 필요성 항목은 5점 만점에 4.6점으로 전체 항목 중 전문가들이 가장 필요하다고 느끼는 항목으로 확인되었다. 이와 같은 결론에 비추어 본다면, 전문가들이 생각하는 스마트공장 구축수준 Level2 이하의 중소기업에 있어서는 각 영역별 보안이 중요하게 고려되고 필요하다고 말할 수 있었다.

마지막으로, 전문가들이 보안에 대하여 필요하다고 말한 항목 중 실제로 전문가들이 생각하는 우선순위 적용 검토 항목은 무엇인지에 대하여 최종적으로 확인하였다. 이 확인 결과는 아래와 같이 나타나게 되었다.

[표 4-11] 스마트공장 도입 및 구축시 보안 우선순위 적용 검토 항목

구 분	1순위	2순위	3순위	4순위	5순위
1. 스마트공장 운영을 위한 보안정책 및 프로세스 수립/운영 분야	**45 (54.5%)**	12 (15.6%)	13 (16.9%)	8 (10..4%)	2 (2.6%)
2. 스마트공장 운영을 위한 보안조직 운영 분야	2 (2.6%)	20 (26%)	13 (16.9%)	18 (23.4%)	**27 (31.1%)**
3. 스마트공장 운영을 위한 인적자원 보안 분야 (협력사 보안관리 포함)	5 (6.5%)	16 (20.8%)	15 (19.5%)	**26 (29.8%)**	18 (23.4%)
4. 스마트공장 운영을 위한 물리/환경적 보안 분야	10 (13%)	2 (2.6%)	**36 (52.8%)**	20 (26%)	12 (15.6%)
5. 스마트공장 운영을 위한 시스템 운영 및 네트워크 보안 분야	18 (23.4%)	**30 (35.6%)**	3 (3.9%)	8 (10.4%)	21 (26.7%)

위 [표 4-11]과 같이 전문가들의 설문조사 항목 중 최종적으로 스마트공장 도입 및 구축시 보안 우선순위 적용 검토 항목을 1순위 ~ 5순위까지 빈도분석을 실시한 결과, 1순위 - 스마트공장 운영을 위한 보안정책 및 프로세스 수립/운영 분야, 2순위 - 스마트공장 운영을 위한 시스템 운영 및 네트워크 보안 분야, 3순위 - 스마트공장 운영을 위한 물리/환경적 보안 분야, 4순위 - 스마트공장 운영을 위한 인적자원 보안 분야 (협력사 보안관리 포함), 5순위 - 스마트공장 운영을 위한 보안조직 운영 분야로 확인되었다. 이 결과를 통해 확인할 수 있는 부분은, 전문가들이 생각하는 스마트공장 구축수준 Level2 이하의 중소기업에 있어서는 보안정책 및 프로세스 수립/운영을 통해 기본적인 업무 프레임을 구축하는 것이 가장 우선적으로 고려되어야 하는 사항으로 확인된 것이다.

다만, 앞에서 전문가들이 의견제시한 스마트공장 도입 및 구축시 보안 영역별 필요성 수준은 총 8개의 항목으로 구성되었으나, 해당항목 중 스마트공장 도입 및 구축을 위한 컨설팅과 보안과 관련한 보안 정책 등 내부 규정 필요성은 보안 프로세스 구축분야와 관계된 영역이기에 1개의 영역으로 통일해도 가능하다고 판단되었고, 스마트공장과 연계한 보안교육과 보안 영역별 이해 및 준비에 대한 부분 역시 인적보안분야 내 교육분야와 관계된 영역으로 이 역시 1개 영역으로 통일해도 가능하다고 판단되어 최종적인 보안 우선순위 항목의 도출은 5개의 영역으로 분류하여 진행하게 되었다.

그리고, 이러한 전문가 설문조사 결과가 실제로 스마트공장 구축수준 Level2 이하의 중소기업의 보안수준 향상을 위해 고려할 보안 우선순위 항목으로 제시될 수 있을지에 대한 타당성 검증을 위해 추가적으로 'A' 수행기관에서 2020년 및 2021년 진행한 스마트공장 수준확인 110개 심사업체에 대한 보고서를 실증분석하여 전문가 의견과 매칭해보았다.

[표 4-12] 스마트공장에 대한 경영진 인식 수준 (보안분야)

경영진 인식 수준 (보안분야)					
구 분	매우 높다	높다	보통	낮다	매우 낮다
2020년	7	43	8	2	0
2021년	2	42	6	0	0
합계	**9**	**85**	**14**	**2**	**0**
비중(%)	**8.2**	**77.3**	**12.7**	**1.8**	**0**

[표 4-12]와 같이 스마트공장 수준확인 110개 심사 업체에 대한 보고서 중 보안분야에 대한 경영진 인식 수준을 확인할 결과, 보안에 대한 경영진 인식수준은 85.5%로 높은 수준을 보였으며, 전문가 의견과는 약간 상이하게 실질적으로 경영진의 인식수준은 높다는 것을 확인할 수 있었다. 년도별 수준을 각 년도별로 확인해보더라도 보안분야에 대한 경영진 인식 수준은 높다는 것을 알 수 있었다.

[표 4-13] 스마트공장과 관련한 보안교육 실시 및 수준

보안교육 실시 및 수준					
구 분	매우 높다	높다	보통	낮다	매우 낮다
2020년	1	3	3	40	13
2021년	2	2	8	28	10
합계	**3**	**5**	**11**	**68**	**23**
비중(%)	**2.7**	**4.5**	**10**	**61.8**	**20.9**

[표 4-13]과 같이 스마트공장과 관련한 보안교육 실시 및 수준을 확인해 본 결과, 보안교육 실시 및 수준은 82.7% 정도가 낮은 수준을 보였음. 이 부분은 전문가들의 의견과 동일하게 스마트공장을 도입 및 구축하는 중소기업에 있어서 실질적인 보안 관련 교육이 필요하다는 것을 확인할 수 있었다. 또한, 년도별 보안교육 실시 및 수준을 확인해보더라도 2020년에 비해 2021년 보안교육 실시 및 수준이 조금 향상된 부분은 있으나, 전반적으로는 아직까지 보안교육이 부족하다는 것을 알 수 있었다.

[표 4-14] 스마트공장 보안 업무 담당자 지정 여부

보안업무 담당자 지정 여부				
구 분	별도 지정	겸직	지정 검토	검토 안함
2020년	4	4	39	13
2021년	2	6	26	16
합계	**6**	**10**	**65**	**29**
비중(%)	**5.5**	**9.1**	**59.1**	**26.4**

[표4-14]와 같이 스마트공장 보안 업무 담당자 지정 여부를 확인해본 결과, 해당 중소기업에서는 실제로 스마트공장 보안 업무 담당자 (겸직 포함)를 별도로 지정하여 운영하기 어려운 현실이라는 것을 확인하였고, 추후 검토하고자 하는 비율이 59.1%, 검토조차도 하고 있지 않은 비율이 26.4%가 될 정도로 가장 어려움을 겪는 부분이라는 것을 확인하였다. 전문가 의견에 있어서도 필요성에 있어서는 스마트공장 보안 업무 담당자가 필요하다는 의견이 대부분이었으나, 보안 우선순위 항목에 있어서는 5순위로 답변할 정도로 전문가들 역시 현실적으로 중소기업에서 보안 업무 담당자를 전담 혹은 겸임으로 임명하여 운영하기 어렵다는 부분의 의견은 일치하는 모습을 보였다.

[표 4-15] 스마트공장 도입 및 구축기업 도입 혹은 검토 프로그램

도입 혹은 검토 프로그램					
구 분	ERP	MES	SCM	PLM	없음
2020년	35	6	7	0	12
2021년	36	4	4	2	4
합계	**71**	**10**	**11**	**2**	**16**
비중(%)	**64.5**	**9.1**	**10**	**1.8**	**14.5**

[표 4-15]와 같이 스마트공장 도입 및 구축기업에 있어서 실제로 도입 혹은 검토하고 있는 프로그램을 확인해 본 결과, 64.5% 기업이 ERP를 도입 혹은 검토하고 있었다. 다만, 실제 ERP를 도입 혹은 검토하고 있는 세부내용에 대해 확인해 본 결과, 스마트공장과 직접 연계된 전사 자원관리시스템으로써의 ERP가 아닌 재무회계의 간단한 솔루션 개념의 ERP를 사용하고 있는 기업이 대부분이었다. 그러나, 프로그램 운영에 따른 기본적인 보안시스템 또는 보안 네트워크 등에 대한 고려는 필요하다고 판단되었다. 전문가들 역시 실제 ERP에 대한 활용이 전사 자원관리시스템으로써의 활용이 아니더라도 해당 프로그램 내 기업의 중요한 DB 등이 존재함에 따라 보안시스템 및 네트워크 보안에 대한 부분의 필요성을 강조한 것으로 일부 의견과 실제 중소기업의 운영현황에 있어서의 중요성이 일치되었다.

[표 4-16] 스마트공장 도입 및 구축기업 보안 운영 세부 분야

보안 운영 세부 분야				
구 분	2020년	2021년	합계	비중(%)
서버운영	6	4	**10**	**9.1**
보안시스템 운영	0	3	**3**	**2.7**
보안설비 운영	8	6	**14**	**12.7**
그룹웨어	6	4	**10**	**5.5**
출입통제	15	16	**31**	**28.2**
CCTV	13	8	**21**	**19.1**
보안정책 등	6	4	**10**	**9.1**
없음	8	7	**15**	**13.6**

[표 4-16]과 같이 스마트공장 도입 및 구축기업에서 실제로 보안 운영 세부 분야를 확인해 본 결과, 가장 많은 비중을 차지한 부분이 출입통제로 전체에서 28.2%를 차지하고 있었으며, 세부 내용으로는 외부자 출입통제 시스템, 주요 시설 및 설비에 있어서의 접근통제 시스템이 해당되는 내용이었다. 다음으로는 CCTV 운영으로 전체에서 19.1%를 차지하였다. 결과적으로는 최소한 해당 기업들이 물리환경적 보안에 있어서는 어느정도 적용하고 있는 부분이 있다는 것을 확인할 수 있었으며, 그 이외에 보안 설비 및 시스템, 보안정책 등 프로세스 수립 및 운영분야에 있어서는 미흡한 부분을 보이고 있다는 것을 알게 되었다. 이 역시 전문가 설문조사와 연계해서 파악해본다면, 전문가들이 보안 우선순위 항목에서 1순위 및 2순위로 제시한 중소기업이 고려할 보안 항목의 내용과 일치하는 모습을 보였다.

4.2 실증분석을 통한 중소기업의 보안수준 향상을 위한 우선순위 항목 도출

4.2.1 최종 중소기업의 보안수준 향상을 위한 우선순위 항목 분석 및 도출

앞에서 전문가 설문과 'A' 수행기관에서 2020년 및 2021년 진행한 스마트공장 수준확인 심사보고서의 실증분석을 통해 최종 중소기업의 보안수준 향상을 위해 고려할 보안 우선순위 항목을 분석하고 도출한 결과, 아래와 같은 결과를 가져오게 되었다. 특히, 전반적인 전문가 의견과 'A' 수행기관의 스마트공장 수준확인 심사를 통해 확인된 스마트공장 구축수준 Level2 이하의 중소기업의 보안 운영 현황이 대부분 일치하였으나, 일부 항목에 있어서는 전문가 의견과 실질적인 중소기업의 현황에 있어서 차이가 발생하거나 해당 보안 항목을 중소기업이 현실성있게 반영할 수 없는 부분도 존재한다는 것을 추가로 확인할 수 있었다. 따라서, 이러한 자료를 보다 구체적으로 비교 분석하여 최종적인 스마트공장 구축에 있어서 중소기업의 보안수준 향상을 위해 고려할 보안 우선순위 항목을 제시한다면 다음과 같다고 할 수 있다.

[표 4-17] 중소기업이 고려할 보안 우선순위에 대한 실증분석 자료 비교

구 분	전문가 의견	중소기업 현황
1. 스마트공장 운영을 위한 보안정책 및 프로세스 수립/운영 분야	1순위 **(5점)**	수립 및 운영 미흡 (낮음) **(4점)**
2. 스마트공장 운영을 위한 보안조직 운영 분야	5순위 **(1점)**	담당자 지정 미흡 (검토 혹은 미고려) **(4점)**

구 분	전문가 의견	중소기업 현황
3. 스마트공장 운영을 위한 인적자원 보안 분야 (협력사 보안관리 포함)	4순위 **(2점)**	경영자 인식 높음 / 보안교육 일부 실시 **(2.5점)**
4. 스마트공장 운영을 위한 물리/환경적 보안 분야	3순위 **(3점)**	출입통제 등 일부 영역 도입 및 고려됨 **(1점)**
5. 스마트공장 운영을 위한 시스템 운영 및 네트워크 보안 분야	2순위 **(4점)**	프로그램 운영 대비 시스템 도입 미흡 **(4점)**

결과적으로, 위 [표 4-17]에서 비교 분석한 내용을 확인해본다면 전문가 설문에 있어서 전문가들이 필요로하는 중소기업이 고려할 보안 우선순위 항목과 중소기업 현황에 대한 자료의 실증분석 내용에서 스마트공장 운영을 위한 보안정책 및 프로세스 수립/운영분야는 전문가들이 1순위로 가장 고려가 필요한 항목이라고 의견제시한 것과 같이 현실적으로 중소기업에서도 가장 적용이 미흡한 부분이라고 평가되었다. 또한, 스마트공장 운영을 위한 시스템 운영 및 네트워크 보안 분야 역시 전문가들이 2순위로 필요하다고 의견제시한 것과 같이 중소기업에 있어서도 실제로 재무회계 분야의 ERP 등 프로그램을 사용하고 있음에도 불구하고 보안시스템 및 설비의 운영에 있어서는 미흡한 수준을 보이고 있었다. 다만, 전문가들이 3순위 ~ 5순위로 제시한 보안 우선순위 항목은 오히려 중소기업 현황에 있어서 많은 부분 적용이 되고 있는 부분도 있고, 적용이 필요하지만 기업의 시스템 역량이나 재무적 지원 부족으로 인하여 적용하기에 어려운 부분이 있다는 것을 파악하게 되었다. 따라서, 3순위 ~ 5순위의 전문가들이 의견제시한 보안 우선순위 항목은 중소기업의 입장에서 보다 접근하기 쉽고 스마트공장 도입 및 구축에 어려움을 겪지 않을 내용부터 우선적으

로 검토하여 우선순위가 제시되는 것이 보다 현실적이라는 결론을 도출하게 되었다. 특히, 재무적 지원이 필요한 부분은 앞으로 스마트공장 도입 및 구축과 연계된 정부 지원사업이 단순히 설비와 연동된 시스템 혹은 프로그램의 지원이 아닌 보다 중소기업 현실과 스마트공장 도입 및 구축의 운영 성과가 나타날 수 있는 방향으로의 지원으로 개선이 필요하다는 내용도 확인할 수 있는 계기가 되었다.

그리고, 이러한 비교분석을 통해 최종적으로 중소기업이 고려할 보안 우선순위 항목을 도출하는 방법으로는, 전문가 의견에서 선정된 1순위 ~ 5순위에 대한 보안 우선순위 항목과 중소기업 운영 현황 수준에 대해서도 각 항목별 수준에 대하여 5점 점수 척도로 환산하고, 두 항목에서 결과로 나온 항목별 점수를 합산하여 합산 점수가 높은 항목순으로 최종적인 중소기업이 고려할 보안 우선순위 항목을 도출하는 방식을 적용하였다.

- 전문가 의견 : 1순위 → 5점 / 2순위 → 4점 / 3순위 → 3점
  4순위 → 2점 / 5순위 → 1점
  (우선순위가 높을수록 필요하다고 평가되기에 점수배점이 높음)

- 중소기업 현황 : 매우 높음 또는 우수, 고려됨 → 1점 /
  높음 또는 양호 → 2점 / 보통, 일부 실시 → 3점
  낮음 또는 미흡 → 4점 / 매우 낮음 → 5점
  (높음이나 우수보다 낮음이나 미흡한 현황 개선이 시급하기에 점수배점이 높음)

따라서, 최종적인 스마트공장 구축에 있어서 중소기업이 고려할 보안 우선순위 항목을 전문가들의 의견과 중소기업의 운영 현황 수준에 대한 결과를 5점 척도의 수준 지표를 반영하여 최종적인 합계 점수로 환산하였으며 이러한 환산점수에 의해 높은 점수순의 최종적인 보안 우선순위 항목을 제시한다면 다음 [표 4-18]과 같다고 결론지을 수 있다.

[표 4-18] 스마트공장 구축에 있어서 고려할 보안 우선순위 항목

우선순위	보안 우선순위 항목 세부 내용	총점
1순위	**스마트공장 운영을 위한 보안정책 및 프로세스 수립/운영**	**9점**
2순위	**스마트공장 운영을 위한 시스템 운영 및 네트워크 보안**	**8점**
3순위	**스마트공장 운영을 위한 보안조직 운영 (담당자 지정 포함)**	**5점**
4순위	**스마트공장 운영을 위한 인적자원 보안 (협력사 보안관리 포함)**	**4.5점**
5순위	**스마트공장 운영을 위한 물리/환경적 보안**	**4점**

추가적으로, 이러한 내용과 연계하여 기존의 선행사례 연구에서 제시된 일반적인 각 영역별 보안의 구체적인 운영내용과의 연계를 통해 스마트공장 구축수준 Level2 이하의 중소기업도 조금 더 전문성에 대한 검토가 필요한 내용에 대하여 확인하고 검토할 수 있는 방향으로의 스마트공장 도입 및 추진이 이루어지면 좋겠다고 생각되었다.

그리고, 스마트공장 관련 전문가 의견 중 보안위협이 크지 않다고 답변하였거나 보안요인이 고려되지 않아도 된다는 사유로 답변한 스마트공장 수준확인 심사원 자격의 전문가 10인의 답변 사유도 확인한 결과, 1) 중소기업의 규모나 재정도, 자립도 등을 확인하였을 때 실질적인 보안운영이 쉽지 않다는 의견과, 2) 중소기업 대부분이 실무자가 멀티플레이 관점으로 다양한 업무를 복합적으로 수행하고 있기에 보안에 대한 업무의 책임과 권한을 추가로 부여하기 현실적으로 어렵다는 의견으로 답변한 것으로 파악되었다. 이 부분 역시 위에서 언급한 내용과 같이 스마트공장에 대한 지원이 단순한 프로그램이나 시스템 구축이 아닌 중소기업이 부족한 부분의 역량을 향상시켜주거나 재정적인 부분을 포함하여 자립도를 높여줄 수 있는 방향으로의 제도 지원이 절실하다는 것을 대변해주고 있다는 것을 알 수 있다.

V. 결 론

스마트공장의 가장 큰 특징으로 언급된 기획에서 생산, 유통에 이르기까지의 전 과정을 ICT(정보통신) 기술과 접목하여 각 단위 공정별로 구성요소를 체계화하고, 통합적인 생산관리 시스템을 접목시킴으로써 보다 효율성 있고 효과적인 시스템 구조를 갖추고자 함을 목표로 연구하였다.

최근에는 사이버침해 위협이 높아짐에 따라 스마트공장 구축시 보안에 대해 고려할 요소들이 증가하게 되었다. 이러한 보안의 위협요인을 낮추기 위해서는 다양한 고려요소를 반영해야만 하며 이를 위해서는 운영 능력이 비교적 높은 중소기업 이상의 규모의 기업이어야 한다. 하지만 스마트공장 구축수준 Level2 이하의 중소기업에서는 보안이슈에 대한 위험 인지의 이해도가 낮은 편이며 위협을 해결할 만한 시스템이나 설비의 구축에도 예산 등의 어려움이 있다는 것을 알 수 있었다.

이에 따라, 스마트공장 업무와 연관성이 있는 전문가 80명의 설문조사와 'A' 수행기관에서 2020년 및 2021년 진행한 스마트공장 수준확인 110개 심사업체의 보고서 내용 중 보안과 관련된 내용의 수준을 실증 분석한 결과를 비교 분석하였다. 이러한 분석을 통한 자료를 바탕으로 전문가 의견에 대한 타당성 검증을 통해 좀 더 현실성 있는 보안 우선순위 항목의 제시를 함으로서 스마트공장 구축수준 Level2 이하의 중소기업도 보안의 위험성을 줄일 수 있을 것이다. 해당 중소기업의 구축가능한 재정적 범위 내에서 순차적으로 고려할 수 있는 보안 우선순위 항목에 대한 제언을 통해 발생할 수 있는 보안의 이슈와 문제에 대한 대응방안을 제시코자 하는 연구로써 본 연구의 의의가 있다고 하겠다.

본 연구의 한계점으로는 심사 전문가와 같은 설문 대상에 대한 범위의 한계, 스마트공장 수준확인이 완료된 다수의 수행기관을 모두 대상으로 하여 결론을 도출하지 못하였다는 점을 들 수 있다. 그리고 기존에 제시된 보안 우선순위 항목의 타당성이 부족하다고 판단하였기 때문에 본 연구의 결과물과의 비교분석을 통한 신뢰성 높은 보안 우선순위 항목을 도출하지

못했다는 것도 한계점이라 할 수 있다. ICT 기술의 접목이 지속적으로 활발해지고 있는 스마트공장 구축에 있어서 구체적인 분석과 실증 검증을 실시하지 못했다는 것은 본 연구의 한계성이 있을 수 있다.

따라서, 추후에는 보다 다양한 계층과 기관의 자료 분석과 전문적인 통계분석, 기존 보안 우선순위 항목과의 구체적인 연관성 비교 분석 등을 통해 좀 더 세부적인 내용의 보안 우선순위 항목 검토와 제시를 하는 것이 필요할 것이다. 그리고 해당 보안 우선순위 항목의 영역에 중소기업 자체적으로 해결하기 어려운 부분에 대한 정부기관으로써의 역할과 지원사항에 대한 제시도 병행하여 이루어진다면 더 좋은 연구가 진행될 수 있을 것으로 기대한다.

참 고 문 헌

1. 국내문헌

고재진, 이규택. (2015). 『스마트공장 현황 및 시사점』. 한국산업기술평가관리원.

권순현, 김지윤, 임재덕, 유일순. (2020). 5G 기반의 스마트공장 보안 동향 분석. 『정보보호학회지』 30권 6호.

국가기술표준원. https://www.kats.go.kr/

김광석, 최연경, 김기범, 박문구. (2018). 『4차 산업혁명과 제조혁신: 스마트 팩토리 도입과 제조업 패러다음 변화』. 삼정KPMG 경제연구원.

김현진, 김진영, 백주련. (2018). 스마트 팩토리 보안 사고 유형 분석 및 대안 프레임 제시. 『한국컴퓨터정보학회 학술발표논문집』 26(2), 161-164.

나재훈, 나중찬. (2016). 산업제어시스템 보안 표준화 동향. 『정보보호학회지』 26권 4호, pp 28-35.

박종만. (2015). 중소제조업 스마트공장 기술 동향과 이슈. 『한국통신학회』 Vol.40, No.12, pp.2491-2502.

박형욱. (2015). 스마트 팩토리와 연관된 생산제조기술 동향. 『한국통신학회지(정보와통신)』 33(1), 24-29.

배춘석, 고승철. (2019). 스마트팩토리 도입 기업의 보안강화 사례 연구. 『한국정보보호학회지』 29권 3호.

배병환. (2019). 주요국 스마트공장 보안 동향 분석 및 시사점. 『정보통신기술진흥센터 주간기술동향』.

서창성. (2016) “스마트 팩토리 구축을 통한 중소기업 생산성 향상에 대한 연구,”. 국내석사학위논문 부산대학교 대학원.

서혁준. (2016). 『스마트공장 보안 대응 방안』. 계장기술 9월호, 기획특집, pp 88-91.

스마트제조혁신추진단. https://www.smart-factory.kr/
신재훈. (2018) “스마트 팩토리 보안요인에 대한 연구동향 분석, 국내(RISS)와 해외(SCOPUS) 데이터 중심으로”. 국내석사학위논문 충북대학교 대학원.
이무순. (2017) “ICT 기업 융합 성과의 결정요인에 관한 연구”. 국내박사학위논문. 계명대학교 대학원.
이병권, 김동원, 노봉남. (2016). 안전한 스마트공장 구축을 위한 위험우선순위(SFRPN) 기반 최소보안요구사항에 관한 연구. 『정보보호학회논문지』 26(5), 1323-1333.
이상동. (2016) 『4차 산업혁명을 이끄는 융복합 기술의 표준화 연계 전략』. KSA한국표준협회.
이인재. (2018). 『제조업 혁신을 위한 미래 스마트팩토리 추진 방향』. 정보통신기술진흥센터.
이정철, 박진우. (2016). 스마트공장 관련 산업 분류체계 추진방향. 『대한산업공학회』 pp.1493-1515.
이현정, 유상근, 김용운. (2017). 스마트공장 기술 및 표준화 동향. 『전자통신동향분석』 32권 3호, pp 78-88.
임명성. (2016). 제조업과 정보통신기술의 융합 : 스마트 팩토리 4.0에 기반한 한국 제조업 3.0 성공 전략. 『한국디지털정책학회』 Vol.14, No.3, pp.219-226.
임재현. (2015).『다시 시작하는 인더스트리 4.0』. 포스코경영연구원 동향분석센터.
장경석. (2017). 『국내·외 스마트 팩토리 동향』. KB 지식 비타민, 17-37호, KB금융지주경영연구소.
조윤정. (2015). 『국내 제조업 고도화 방안으로서 스마트공장의 가능성』. KDB산업은행.
조혜지, 김용균. (2018). 『스마트 팩토리 기술 및 산업 동향』. 정보통신기술진흥센터.
중소기업정보기술진흥원. (2019). 『2019년 중소기업 정보화 수준조사』

한근희. (2019). 스마트공장 보안과 표준. 『한국통신학회지(정보와통신)』 36(6), pp. 41-46.
한국생산성본부. (2016). 『미래 스마트공장 방향 제시 및 스마트제조산업 발전방안 연구』. 산업부.
한석호. (2019). "스마트 팩토리 보안관리 항목 연구". 국내석사학위논문 중앙대학교 대학원.
한양대학교. (2015). 『스마트공장 발전 전략 수립 및 고도화 방안 연구』 산업부.
한국인터넷진흥원. (2017). 『스마트공장 중요정보 유출방지 가이드』
한국전자통신연구원. (2018). 『스마트 제조 기술 및 표준』
허 진. (2018). "AHP 기법을 적용한 스마트공장 보안요인 우선순위에 관한 연구". 국내박사학위논문 상명대학교 대학원.

2. 국외문헌

Baum, F., & Bulthuis, W. (2014). *Managing security, safety and privacy in Smart Factories.* Smart Factory Innovation Forum.
Fourth Industrial Revolution (2017). Retrieved from https://en.wikipedia.org/wiki/Fourth_Industrial_Revolution
Jesus, M. H., & Diego, M. H. (2016). *Research of Cybersecurity at Oil and Gas Industry.* F17, Cyber security and new technology risks.
NIST, S. (2015). 800-82 Rev 2. *Guide on industrial control systems security.* Draft.
Sherisse Pham (2018). *Computer virus cripples top Apple supplier TSMC.* Retrieved from https://money.cnn.com/2018/08/06/technology/tsmc-chip-supplier-virus/index.html

ABSTRACT

A Study on the Priority of the Smart Factory for the Improvement of Security Level of Small and Medium Enterprises -Focusing on Small and Medium Manufacturing Businesses with Level 2 or Low Level of Construction-

Park, Sang Bok

Major in Smart Convergence Consulting

Dept. of Smart Convergence Consulting

Graduate School of Knowledge Service & Consulting

Hansung University

The changes in life brought about by the development of various technologies around the world are coming in very convenient, efficient and diverse forms.,Among them, the development of automation and digital technology in the traditional manufacturing sector and the promotion of smart factories, which are actively engaged in convergence with ICT, are becoming active.,In particular, the era of the Fourth Industrial Revolution, in which the traditional boundaries between academic disciplines are broken down and technology convergence drastically changes the economic system and social structure, is

accelerating.,Smart manufacturing is a paradigm shift in the era of the Fourth Industrial Revolution that aims to promote strategic innovation of manufacturing through the convergence of human, technology and information. It is a technology that aims to improve productivity more innovatively by integrating ICT and manufacturing technology.,In addition, smart factories are based on the structure in which facilities, equipment and processes operated in manufacturing sites are more intelligent and connected to networks through the convergence of technologies.,And it can be defined as a concept to create a factory that can be optimized for production operation by sharing and utilizing production data and information generated from each facility and equipment in real time.,It also refers to an intelligent ICT convergence manufacturing system that continues to operate collaboratively between factories.

However, there are positive and negative effects on the development of such systems. In the smart factory, the system through ICT convergence is intelligent as a positive effect, but negatively, cyber threats are increasing and actual damage cases are continuously occurring.,Therefore, unlike the past, individual machines, equipment and systems were being expanded as they were connected to the network.,Accordingly, it is required to respond to security problems when connecting new systems and existing systems.

In this study, the following methodology was applied to approach security problems that may arise when building a smart factory from a wide perspective.,The study demonstrated the problems of the existing research and the method of deriving, the appropriateness of the solution, and the expert questionnaires of the empirical subjects.,The criteria for the empirical study are the research that defines the security factor items to be considered first when building small and medium-sized manufacturing companies with level 2 or less

among the scale of building smart factories.

And by analyzing the current status of small and medium-sized manufacturing companies under Level 2 of Smart Factory Construction, the priority items for security that can be considered more realistically in building smart factories were presented.,It was meaningful as a researcher that it suggested a more efficient and effective system operation method by allowing the selection of security elements suitable for each company's competence among the priority items.

In addition, the research method was conducted through the survey statistical proof. In the process, the survey of experts on smart factories and the empirical analysis of the report on the level of smart factories for companies actually operated were reviewed and the final results were derived and reflected.

Through the conclusion of priority security items, we will give practical application and operational effectiveness to security in building smart factories based on SMEs under level 2.,The purpose of this study is to derive the practical priorities and to provide psychological stability by suggesting the conclusions through expert demonstration.

And through the suggestion of the conclusion drawn, I would like to suggest a standard that will be a new standard for the development direction in the construction of a smart factory of small and medium-sized manufacturing companies that are currently somewhat flat.

【key words】 Security, priority security items, smart factory security considerations, ICT convergence smart factory security