https://doi.org/10.33778/kcsa.2019.19.4.173

4차 산업혁명의 보안 인프라 구축을 위한 융합보안산업 지식 맵 개발★

이 대 성*

요 약

Cyber Physical System으로 상징되는 제4차 산업혁명(Industry 4.0)이 전 세계적으로 확산되어 감에 따라 향후 구현될 다양한 사이버 시스템들의 기술적 안정·신뢰성을 확보하기 위해서는 융합보안 인프라 구축이 필수적이다. 본 연구에서는 4차 산업혁명의 확산과 관련하여 생활안전의 개념을 포함하는 광의의 융합보안산업 및 기술의 현상을 파악하고, 관련된 지식간의 연계 가능성을 분석하여 보안의 융합화에 필요한 산학협력을 촉진할 수 있는 인력양성, 기술개발, 정책개선 등에 관한 종합적인 발전 정책을 제안하고자 한다.

Development of Convergence Security Industry Knowledge Map for the 4th Industrial Revolution Security Infrastructure

Daesung Lee*

ABSTRACT

As the 4th Industrial Revolution(Industry 4.0), symbolized as CPS(Cyber Physical System), spreads around the world, it is essential to establish a converged security infrastructure to secure technical stability and reliability of various cyber systems to be implemented in the future. In this study, we will investigate the phenomenon of broad convergence security industry and technology including the concept of life safety in relation to the spread of the 4th industrial revolution, and analyze the possibility of linkage between related knowledge to promote academic-industrial cooperation necessary for the convergence of security. we would like to propose a comprehensive development policy on human resource development, technology development and policy improvement.

Key words : The 4th Industrial Revolution, Convergence Security Industry, Knowledge Map, Convergence Security Infrastructure

접수일(2019년 10월 16일), 게재확정일(2019년 10월 28일)

* 부산가톨릭대학교/컴퓨터공학과

★ 본 논문은 2017년도 부산가톨릭대학교 교내연구비에 의하여 이루어진 연구로서, 관계부처에 감사드립니다.

1. 서 론

4차 산업혁명이 지향하는 방향은 기존 산업사회의 CPS(Cyber Physical System)화 및 산업간 융복합화를 통해 새로운 산업을 창출하는 것이며, 대표적 사례로는 제조업 생산시스템의 스마트 혁신, O2O(Online to Offline) 플랫폼을 이용한 서비스 산업 혁신, 스마트시티에 의한 미래도시 건설 및 라이프 스타일 혁신 등을 들 수 있다[1, 2, 3, 4].

기술혁신 측면에서는 Schwab의 주장[5]과 같이 3차 산업혁명의 기반을 토대로 하여 기존 기술의 경계영역을 융합하는 기술혁명으로 인터넷, 센싱, 인공지능을 중심으로 4차 산업혁명의 핵심기술들이 모든 사물, 인간, 공간이 연결되어 커뮤니케이션하는 초연결사회로 나타난다. 산업혁신 측면에서는 독일의 '인더스트리 4.0'으로 대표되는 제조업 혁신을 들 수 있으며, 시스템 혁신 측면에서는 1, 2차 산업혁명이 오프라인, 3차 산업혁명이 온라인 중심이었다면, 4차 산업혁명은 온라인과 오프라인의 융합(O2O)으로 나타난다.

이처럼 다양한 측면에서 4차 산업혁명이 진행되고 있으며, 기술간 융합에 따른 보안 문제점과 산업간 융합에 따른 보안 문제점이 지속적으로 새롭게 등장하고 있다. 이러한 융합보안 이슈에 대해 융합보안산업과 융합보안기술 및 서비스 관점에서 관련된 지식간의 연계 가능성을 분석하고 보안의 융합화에 필요한 산학협력을 촉진할 수 있는 인력양성, 기술개발, 정책개선 등 종합적인 발전정책을 고려할 시점이다.

본 연구에서는 ICT를 중심으로 하는 3차 산업혁명을 대신하여 앞으로의 인류사회를 견인할 4차 산업혁명의 등장과 이에 따른 융합보안산업 및 융합보안서비스를 창출하기 위한 산학연 기술맵을 개발하고자 한다.

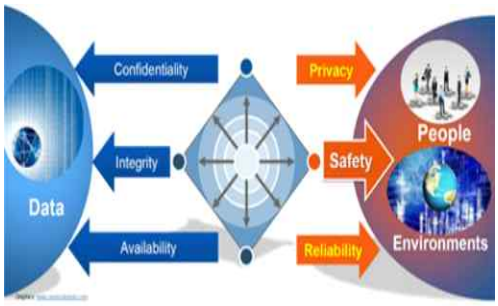
본 논문의 구성은 다음과 같다. 2장에서는 융합보안 관련 국내 및 국외 연구사례를 알아보고, 3장에서는 융합보안산업 동향에 대해 산업적 관점과 기술적 관점으로 살펴본다. 4장에서는 융합보안 플랫폼을 소개하며, 5장에서 융합보안산업 지식맵을 소개하고, 6장에서 결론을 맺도록 한다.

2. 관련 연구

2.1 국외 융합보안 연구사례

미국 국립표준원(NIST: National Institute of Standards and Technology)은 2016년 4월 지난 20년간 ICT 기술의 발전으로 데이터와 영상정보를 생활안전에 활용할 수 있게 되었고, 모바일 기술이 추가적으로 접목 가능해 짐으로써 기술적 활용 범위가 더욱 증가했다고 분석하면서 융합보안 인프라 구축에 필요한 요소기술들에 대한 발전 로드맵을 분석하였다.

미국 시장 조사회사인 가트너는 사이버 보안과 물리적 안전을 확보하기 위하여 데이터에 대한 기밀성, 무결성, 가용성을 확보하고, 사람들의 프라이버시와 안전, 모든 시설/경비에 대한 안전·신뢰성을 동시에 확보할 수 있는 융합보안의 필요성을 강조하였다[그림 1].



(그림 1) 융합보안 비즈니스 Value Chain

미국 시장 조사회사인 MarketsandMarkets는 [그림 2]와 같이 융합보안산업이 발전하기 위해서는 그동안 독자적으로 사업이 이루어져 왔던 정보보안, 지휘통제, 중요정보통신망 보호, 감시시스템, 재난관리, 백업/복구시스템, 바이오인증/객체식별 등의 분야간 기술/사업 융합이 이루어져야 하며, 이를 위해 융합설계 및 컨설팅, 융합 SI 및 유지보수가 가능한 융합보안 서비스산업 육성의 필요성을 지적하였다[6, 7, 8].

(그림 2) 미래 신성장 산업으로서의 융합보안산업 Value Chain

2.2 국내 융합보안 연구사례

국내에서 이루어진 융합보안의 정의에 관한 연구는 그다지 많지 않으며, 여러 자료를 정리해 볼 때, 한국전자통신연구원(ETRI)이 가장 광의로 해석한다고 볼 수 있다. ETRI는 자동차, 조선 등 산업간 융합에 따른 보안기술의 내재화에 중점을 두고 있으며, 물리보안과 정보보안의 융합을 하위의 개념으로 본다.

KIET(2014)[9]는 IT 융합과 사물인터넷 확산에 따라 정보보안과 물리보안 간의 융합, 혹은 보안 기술이 IT 융합산업에 적용되어 창출되는 제품 및 서비스라고 지칭하고, 산업별 환경을 고려한 최적화된 융합보안 솔루션을 개발하여 제품의 신뢰성을 확보하고, 산업의 생산성을 향상시킬 수 있다고 정의한다.

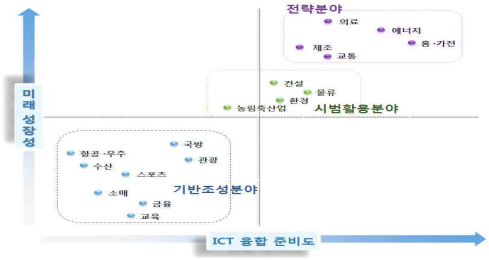
삼성 SDS(2010)[10]는 융합보안관제의 현실적 수요와 기술적 동향 분석을 통해 융합보안관제의 핵심 기술로 유연한 인터페이스 구조를 통한 관제 대상 영역의 통합, 표준화된 분석데이터를 기반으로 한 효율적인 데이터 저장 및 검색, Rule에 기반한 상황 인식 및 대처를 들었고, 각 관제대상에서 발생하는 이벤트의 상관관계를 효율적으로 분석하고 체계적인 관리 정책을 수립할 수 있는 관제 모델 수립이 융합 보안 관제의 성패를 좌우하는 핵심요소라고 강조하였다.

김정덕(2009)[11]은 융합보안의 개념을 정리하기 위해 국외에서 연구되고 있는 융합보안의 개념을 기반으로 융합보안을 통합보안과 복합보안 측면에서 분석함으로써 국내에서 혼용되고 있는 융합보안의 개념에 접근하였다. 그는 효과적으로 융합보안을 구현하기 위해서는 하향식 접근법을 사용해야 한다고 주장하였는데, 이는 기업의 자산을 책임지고 있는 최고 경영층이 통합의 정도를 결정하고, 올바르게 역할과 책임을 할당한 후, 개선 여부를 파악하여 조직의 목표달성에 기여한다고 보았다.

하경수(2015)[12]은 융합보안산업을 안전산업의 관점에서 접근하면서, “안전(Safety & Security) 수요를 민간시장이 수용하여 재화 생산과 서비스 제공을 동반하는 산업”이라 정의하였으며, 제조와 서비스가 결합한 구조를 지닌다고 설명하였다.

현장 실태조사를 통한 실증연구에서는 넥스트I&I가 2016년 7월 국내 최초로 N 전력회사의 융합보안 마스터 플랜을 수립하였는데, 국내외 사례를 분석한 결과, 융합보안에 필요한 새로운 거버넌스체계 구축, 다양한 출입통제 경로의 효율화를 위한 첨단인증 방식 도입, 물리보안과 정보보안 정보의 통합 활용, 드론 등 ICT 신기술을 도입한 차세대 관제체계 구축을 보안발전 방향의 시사점으로 제시하였다[13].

한편, 정부차원에서도 ICT 산업과 타 산업간의 융합이 가시화됨에 따라 부처 공동으로 안심사회 구현을 위한 「K-ICT 융합보안 발전전략」을 마련하여 ICT 융합산업의 보안성 강화, 융합보안 기업 경쟁력 강화, 융합보안 활성화 기반 조성을 발표하고, 산업 지원 영역을 전략분야, 시범활용분야, 기반조성 분야로 구분하여 육성할 예정이다. 중소기업벤처부도 물리보안과 정보보안을 기술적으로 결합하여 재난 발생과 관련된 위기대응체계를 통합적으로 구축하여 국민의 생명과 재산을 보호하고, 민간의 생활안전 관련 산업을 새로운 유망성장산업으로 육성하기 위한 안전기술 로드맵을 제시하였다.



(그림 3) 정부의 융합보안산업 분야별 발전전략

3. 융합보안산업 동향

3.1 산업 동향

국내외적으로 융합보안산업은 초기 성장단계에 있는데, 첫째 서비스 관점에서 정보보안과 물리보안이 융합되고 있으며, 둘째 공공영역에 가까운 재난관리에 정보보안과 물리보안 기술이 접목되어 생활안전산업의 모습을 갖추고 있으며, 셋째, 자동차, 조선, 에너지 등 타산업과 ICT 융합의 기반기술로서 미래 신산업으로서의 전체 모습을 갖추기 시작했다.

먼저, 융합보안산업을 구성하는 정보보안, 물리보안, 재난관리, 시설경비 4대 산업구조는 1980년대 이후 아날로그 기술에 기반한 노동집약적 구조하에서 형성된 것으로, 디지털 기술의 발전에도 불구하고 정부부처별 소관법령에 준거하여 고착화된 영역에서 주어진 보안사업의 업무 내용과 범위에 따라 임무를 수행하고 있으며, [표 1]과 같이 총 종사자수는 5만 5천여명으로 추정되고 있다.

(표 1) 국내 4대 보안사업 현황 비교

	주요 업무	종사자수	사업 주체
정보 보안	. 시스템 보안 . 네트워크보안 . 데이터 보안	10,720명/ 311사	민간 주도
물리 보안	. 출입 통제 . 영상 감시 . 침입 대응	29,210명/ 553사	민간 주도
재난 관리	. 사회재난(화재, 폭발 등) . 자연재해(풍수해, 진진 등) . 특수재난(유해물질, 원자력 등)	40,410명 (2014)	관 주도
시설 경비	. 시설 경비 . 요인 경호	500,000명/ 4,500사	민관 혼합

※ 출처: 한국정보보호산업협회, 한국방재협회, 한국경비협회, 국민안전처 등 각 통계자료에서 발췌

한편, 세계 융합보안보안 산업동향을 보면, IoT와 클라우드 컴퓨팅을 기술기반으로 하여 정보보안 기업인 시만텍(Symantec), 인텔(Intel/McAfee), IBM, 트렌드마이크로(Trend Micro), EMC 등이 기존 시장을 확대하면서, 시만텍의 블루코트(Blue Coat) 인수, 시스코(Cisco)의 클라우드락(CloudLock) 인수, IBM Security의 Resilient Systems 인수 등과 같이 빅데이터와 클라우드 등 융합보안을 둘러싼 기업간 인수합병이 빠르게 확산되고 있다.

물리보안 기업으로는 미국의 Honeywell Security, ADT Security Services, Tyco International 등이 시장 성장을 주도하고 있으며, ESRI(Environmental Systems Research Institute)는 전세계 GIS 시장의 80%를 점유하고 있다.

3.2 기술 동향

융합보안 기술의 분류체계는 국가별, 기관별로 다양하게 존재하는데, 본 연구에서는 사이버 생활의 안전을 위한 네트워크, 시스템, 데이터 보안 등 정보보안 기술, 국민의 일상생활 안전을 위한 영상감시, 출입통제, 침입대응 등 물리보안기술 및 보안사업의 양대 분야를 융합하는 IoT, 클라우드 컴퓨팅, AI 기반의 빅데이터 분석, LBS (Location-Based Service)에 필요한 5G 모바일/위성 기술 등으로 구성하는데, 이를 그림으로 표현하면 [그림 4]와 같다.

(그림 4) 융합보안기술의 분류 체계

융합화기술은 기존의 정보보안기술과 물리보안기술의 융합을 촉진하면서 새로운 보안기술의 융합화를 촉진하는 기술로써, IoT 보안기술, 클라우드 보안기술, 빅데이터 분석 및 보안기술, 5G 모바일 보안기술로 구성된다. IoT 보안기술은 융합보안의 핵심기술로써, IoT 기기들의 상호 운용성을 위해서는 국제표준이 필요하지만 아직까지 IoT 기술을 주도하는 국제표준이 없기 때문에 다양한 표준화 기구들이 각자의 특장점을 바탕으로 연구개발을 진행하고 있다. 클라우드 보안기술은 네트워크 장비에서

HW와 SW를 분리하는 보안기능의 가상화 기술과 이를 기반으로 하는 고성능 보안 가상화 플랫폼 기술이 중점적으로 개발되고 있다. 특히, SDsec 및 NFV 환경에서 보안기능의 동적 재구성, 고성능 제어, 가시성을 확보하기 위해 네트워크 하이퍼바이저, 컴퓨팅과 네트워킹이 결합된 서버-스위치 등 고성능 클라우드 보안 플랫폼 기술개발이 진행 중이다.

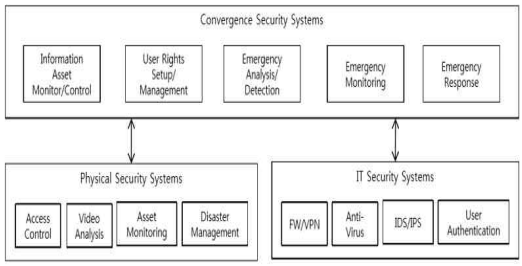
빅데이터 보안기술은 빅데이터를 구성하는 파일 및 데이터를 서버 등에 저장하는 과정에서 분산 데이터의 위·변조 방지, 휴대용 기기나 장치를 통해 입력되는 데이터 유효성에 대한 실시간 관리, 대량 데이터 생산시 사용자의 비의도적 행동으로 인해 발생되는 바이러스 차단, end-to-end에서 필요한 부분을 선별적인 암호화로 인한 데이터 보안 위협 차단 등이 중점적으로 개발되고 있다.

5G 모바일 보안기술에서는 국제기구를 중심으로 DDoS 공격 대응과 LTE 내의 공격 없는 라디오 접근망으로부터 5G 내 다중 통신망 레벨의 취약점이 존재함에 따라 5G 보안 구조, 접근 제어, 프라이버시 보호, 보안 모니터링 및 관리, Slicing/Virtualization 및 강력한 분리, 보안 표준화 등이 연구되고 있다.

4. 융합보안 플랫폼

융합보안 플랫폼은 [그림 5]와 같이 물리적 보안 모듈과 사이버 보안 모듈이 독립적 기능을 하되, 통합관제가 가능하도록 구성되어야 한다. 통합관제의 기능은 각종 인적·물적 자산의 흐름 통제, 사용자의 인증 및 인가, 로그 분석 기반의 비정상 행위 탐지, 비상시의 관제 및 대응으로 구성된다. 이를 위해, 소프트웨어/애플리케이션 단에서는 외부로부터 수집되는 다양한 데이터 소스들이 통합되어야 하며, 급증하는 데이터를 처리할 수 있도록 대규모의 컴퓨터 저장용량을 확보해야 한다. 네트워크 단에서는 DDoS 공격 등 융합보안플랫폼과 연결된 네트워크의 장애를 차단하기 위해 자가조직 네트워크(SON)를 구성하고[1], 네트워크를 최대한 분산시켜야 한다.

또한, 플랫폼의 전방에서 정보를 수집하는 IoT 등에서 전송되는 데이터의 작성, 수집, 저장, 처리, 전송에 대한 보안 효율화와 사용자 및 플랫폼 운용자의 통신 인프라로서의 단말기능도 최적화해야 한다.



(그림 5) 물리보안과 정보보안 플랫폼의 융합

5. 융합보안산업 지식맵

5.1 기업 설문조사

1) 개요

o 조사대상 기업 선정
- 선정 방법: 유관협회로부터의 주요 기업 추천 및 전자공시시스템을 이용한 기업 현황 및 신뢰도 평가
- 8개 기술분야, 총 80개 기업 경영 현황/분석 및 선정

o 설문항목: 11개 항목으로 구성

o 설문조사 기간: 2017. 11. 14. ~ 2017. 12. 13(30일간)

o 설문 응답: 응답율 31.2% / 25개 기업[2]

2) 설문결과 분석

o 응답자의 50% 이상이 IT 솔루션을 개발하는 기업이었으며, 정보보안, 물리보안, 재난관리 기업 순으로 응답에 참여하였다.

o 응답기업의 핵심기술 역량을 묻는 항목에 대하여는

1) 통신 장애가 발생하였을 때 스스로 치유하여 고품질의 통신이 이루어지도록 하는 기술로서, 망의 특성에 따라 자가 설정(Self Configuration), 자가 최적화(Self Optimization) 그리고 자가 치유(Self Healing)로 구분된다.

2) SPTek, 뉴젠, 미래기술에이원, 비유비즈, 비전테크, 세이브더칠드런, 아이오코드, 엔시정보기술, 에스딘, 유비시스, 자인컴, 제오스페이스, 지피모바일, 큐브바이트, 타이어비즈, 타임텍, 포에버정보, 한국클라우드협회, 넷코아테크, 대신정보, 시큐아이, 이니텍, 케이사인, 하이트론시스템즈

단일기술이 31.8%, 복수기술이 68.2%로 응답하였으며, 복수기술의 경우에는 IoT, 클라우드 컴퓨팅, 빅데이터인 것으로 조사되었다.

o 융합보안사업에 진출하고자 할 경우에 필요한 기술역량 확보 전략을 묻는 항목에서는 사업영역 확대와 자체 개발이 68.7%로, 콘소시엄 형태의 기술협력 32.1%를 크게 상회하였다.

o 연구소 조직의 유무와 규모를 묻는 항목에서는 18.2%가 없는 것으로 응답하였으나, 대부분 연구소를 설치할 계획을 갖고 있다고 응답하였다.

o 산업시장, 기술정보의 수집 소스를 묻는 질문에는 55.0%가 정부나 공공기관이 제공하는 웹사이트에 의존한다고 응답하였으며, 35.0%는 전문정보사업체를 이용하고 있다고 응답하였다.

o 기업이 가장 중시해야할 경쟁력에서는 기술품질이 58.6%를 차지하였으며, 영업 및 마케팅 29.6%, 기업인지도 14.8%로 응답하여, 기술품질 중심의 영업 및 마케팅 능력의 융합이 필요한 것으로 나타났다.

o 기업이 겪고 있는 애로 사항으로서는 전문인력의 부족이 50.0%로 절반을 차지하였고, 기술개발비 34.6%, 사업자금 15.4%의 순으로 응답하여, 대부분의 기업이 전문인력과 기술개발비 확보에 어려움을 갖고 있는 것으로 조사되었다.

5.2 융합보안 시스템기술 맵

융합보안 시스템기술 맵은 정보보안 기술, 물리보안 기술, 융합화 기술의 3가지 기술영역으로 구분하여 요소기술과 세부기술을 조사하였으며, 요소기술 및 요소교과의 진화를 고려하여 구성하였다.

특히 세부기술에 관하여는 매년 새로이 추가되는 첨단기술을 지속적으로 추가하기 위해 코드관리할 예정이다.

[그림 4]에서 언급한 융합보안 기술 중에서 정보보안 기술과 물리보안 기술은 지면 관계상 생략하고, 4차 산업의 기반기술인 IoT, 클라우드, 빅데이터, 모바일 분야를 중심으로 융합화 기술의 세부 내용을 살펴보면 [표 2]와 같다.

(표 2) 융합화 기술 맵

구분	요소 기술	세부 기술
I. IoT	I.1 IoT 응용기술	I.1.1 안전사고 대비 네트워크시스템 I.1.2 GPS 기반 안전사고 예측맵 I.1.3 안전사고 대비 스토리텔링시스템 I.1.4 로봇제어 기반의 원격표준시스템
	I.2 IoT 보안 운영체계	I.2.1 IoT 노드간 인증기술 I.2.2 원격 보안관제 기술
	I.3 공유 및 시험평가인증	I.3.1 취약점 자동수집/공유 프레임워크 I.3.2 도메인 보안성 자동화 시험기술
J. 클라우드	J.1 가상머신 시스템 제어	J.1.1 시스템 제어기술 J.1.2 가상머신 구축 기술
	J.2 클라우드 클라이언트 서비스기술	J.2.1 중소규모 클라우드 서비스 기술 J.2.2 대규모 클라우드 서비스기술
	J.3 관리 자동화 기술	J.3.1 데이터 병합기술 J.3.2 관리 자동화 기술
	J.4 컴플라이언스 지원	J.4.1 백업 및 복구기술 J.4.2 서버/플랫폼/스토리지용 보안감시기술 J.4.3 외부 정보유출 통제기술
	J.5 보안 연계	J.5.1 SLA 보안연계 기술 J.5.2 자원간 보안연계 기술 J.5.3 통합보안 연계기술
K. 빅데이터	K.1 빅데이터 수집/저장	K.1.1 실시간 데이터 수집 K.1.2 데이터 연계 및 통합기술 K.1.3 대용량 트랜잭션 데이터 저장기술 K.1.4 인메모리 저장기술
	K.2 빅데이터 분석/처리	K.2.1 실시간 처리분석 기술 K.2.2 네트워크 분석기술
	K.3 시각화	K.3.1 데이터 시각화 기술 K.3.2 서비스 시각화 기술
L. 5G 모바일	L.1 서비스/플랫폼 기술	L.1.1 지역 보안요구사항 분석 및 표준화 L.1.2 프로토타입 정립
	L.2 액세스 시스템	L.2.1 초고속 데이터 전송기술 L.2.2 Small Cell 네트워크 용량 증대 기술 L.2.3 비직교 다중접속기술(NOMA) 기술
	L.3 단말 및 부품	L.3.1 5G 빔포밍기술 L.3.2 대용량 다중 안테나 기술

5.3 융합보안 교과 맵

융합보안 신산업에 필요한 기술인재를 육성하기 위해서는 보안(Security), 안전(Safety), 신뢰성(Reliability), 프라이버시(Privacy)를 종합적으로 이해하고 연구하는 인력양성 교육 훈련과정이 필수적이다. 이에 필요한 학문 분야는 컴퓨터/SW계, 정보보안계, 전자통신계의 학문융합이 전제가 되어야 하며, 정보수집, 전송, 저장, 분석, 이용, 공격방어 및 공통 등 7개 구간으로 나누어 정리하면 [표 3]과 같다.

(표 3) 융합보안 교과 맵

	A. 컴퓨터/SW공학계	B. 정보보안계	C. 전자통신계
1. 공통	A.1.1 SW 공학 A.1.2 SW 아키텍처	B.1 암호기술과 응용 B.2 융합보안관리체계	
2. 정보수집구간			C.2.1 IoT 플랫폼 C.2.2 무선임베디드 IoT시스템
3. 정보전송구간	A.3 인터넷 프로토콜	B.3 네트워크보안	C.3.1 무선이동통신 C.3.2 멀티미디어통신 C.3.3 센서 네트워크
4. 정보저장구간	A4 클라우드 컴퓨팅	B.4 시스템 및 DB보안	C.4 차세대 스토리지
5. 정보분석구간	A5.1 인공지능 A5.2 지능형SW A.5.3 빅데이터 분석		C.5 영상공학
6. 사용자정보구간		B.6 모바일 보안	
7. 공격방어구간		B.7.1 악성코드분석 B.7.2 디지털포렌식 B.7.3 정보보호 평가인증 B.7.4 개인정보보호	C.7 C4ISR 체계 공학

6. 결 론

융합보안이라는 새로운 산업시스템을 이해하고 향후의 발전방향을 전망하기 위해서는 기존의 다양한 보안사업에 대한 기술적·제도적 이해는 물론 4차 산업혁명을 이끄는 IoT, 빅데이터, 클라우드 컴퓨팅, 5G 모바일 등 사고나 재난 발생을 사전에 예측하고, 물적·인적 피해에 대한 선제적, 능동적인 대응을 할 수 있는 첨단 기술에 대한 복합적인 이해가 필수적이다. 이제 융합보안은 기존의 4대 보안사업(정보보안, 물리보안, 시설경비, 재난관리)이 기술적으로 통합 통제가 가능해졌지만, 오랜기간 각기 다른 조직문화와 시스템 운용지식이 서로 다른 상태에서 성장해 왔기 때문에, 현재의 인력과 제도로는 정부부처간, 민관간, 산업간 연계라는 수평적 융복합 액티비티는 물론 통합적인 하나의 신산업으로 발전하기에는 여전히 한계를 보이고 있다.

따라서 4차 산업혁명시대에 핵심 공통기반산업인 융합보안산업을 조기에 육성하고 글로벌 경쟁력을 갖추기 위해서는 첫째, 대학의 융합보안 인력양성을 위한 교육체계가 혁신되어야 한다. 융합보안산업의 발전이 지연되고 있는 가장 큰 요인은 인력수요가 증가하고 있음에도 불구하고 융합보안 인력이 절대 부족하기 때문이며, 이는 인력양성체계가 미흡하고 수요 맞춤형 인력공급이 부족하기 때문이다.

둘째, 빠르게 변화하고 있는 융합보안 환경에 대응하여 기업들이 지속적으로 성장하기 위해서는 벤처기업의 육성지원이 필요하다. 이번 연구에서는 융합보안산업을 구성하는 정보보안기업, 물리보안기업, 재난관리 기업, IoT 기업, 클라우드 기업, 빅데이터 기업, 모바일/인터넷 기업, 기타 기업(CCTV, 바이오 등) 등 8개 기업군으로 나누어 조사하였으나, 자금 뿐 아니라 기술력에서도 대기업에 비해 크게 뒤떨어졌다.[3] 4차 산업혁명과 같이 새로운 패러다임을 요구하는 혁신의 시기에 대기업만으로는 시장 환경에 유연하게 대응할 수 없기 때문에, 융합보안 벤처기업 육성전략은 과거와는 달리 대기업과 벤처기업이 창업시부터 기술제휴하여 시장에 적시에 진입하는 것이 중요하다.

셋째, 융합보안산업의 발전을 위해서는 기관별로 산재되어 있는 융합보안 관련 정보들을 효율적으로 공유할 수 있는 환경이 구축되고 공유되어야 한다. 융합보안의 3대 보호대상인 자연재난, 사회재난, 사이버재난에 대한 방대한 정보의 대부분은 정부나 공공기관이 보유하고 있다. 최근 정부 3.0에 따라 많은 정보가 공개되고는 있으나, 융합보안과 관련된 재난 정보는 특정용도에 제한할 수 밖에 없는 상황이다. 따라서 재난 분석예측과 관련된 벤처기업들에 대한 등록제 도입과 함께 외부에서 악용될 위험이 있는 재난정보나 시스템 취약점, 설정 상황 등에 대한 정보를 제공함으로써, 정보수집구간에서의 사회적 비용을 줄이고, 벤처기업차원에서 특정분야에 대한 정보 분석·예측 기술역량을 갖추도록 지원하는 것이 매우 중요하다.

이 밖에 기업애로요인으로 소규모의 벤처기업들은 기술정보나 시장정보를 전문 정보조사기업보다는 정부나 공공기관의 자료에 의존하기 때문에, 중소 벤처기업의 기술기획 및 사업기획 역량을 강화시킬 수 있도록, 이들 기관이 발간하는 최첨단 정보의 품질을 제공할 수 있도록 노력해야 한다.

3) 국내 보안 기업 현황을 보면 100인 미만 기업이 83.7%, 자본금 50억 미만이 87.9%를 차지하는 등 영세성을 면치 못하고 있음.

참고문헌

[1] Babiceanu, R. F. & Seker, R., "Big Data and virualization for manufacturing cyber-physical systems: A survey of the current status and future outlook.", Computers in Industry, 81: 128-137, 2016

[2] Anis, A., Schafer, W. & Niggemann, O., "A comparison of modeling approaches for planning in cyber physical production systems", In Emerging Technology and Factory Automation(ETFA), 2014 IEEE, 1-8, 2014

[3] Aguiar, S., Pinto, R., Reis J. & Concalves, G. M., "A Marketplace for Cyber-Physical Production Systems: Architecture and Key Enablers", In INTELLI 2017, The Sixth International Conference on Intelligent Systems and Applications. 2017

[4] 김대근, 박만곤, "인더스트리 4.0 기반 사이버물리시스템과 생산관리시스템간의 미들웨어 구축을 통한 수평적 통합", 멀티미디어학회논문지, 17(12): 1484-1493, 2014

[5] Klaus Schwab, "The Fourth Industrial Revolution", World Economic Forum Book, 2016

[6] MarketsandMarkets, "Physical Security Market", 2017.3

[7] MarketsandMarkets, "Publick Safety and Security Market", 2016.11

[8] MarketsandMarkets, "Disaster Recovery as a Service Market", 2016

[9] KIET, "사물인터넷 시대 안전망, 융합보안산업", 2014.4

[10] 삼성SDS, "융합보안시장 동향 보고", 2010.9

[11] 김정덕, 김건우, 이용덕, "융합보안의 개념 정립과 접근방법", 정보보호학회지 제19권 제6호, 68-74, 2009.12

[12] 하경수, 조철규, 김평수, "시스템경비 관제시설의 구축과 보안 및 경영대책", 한국컴퓨터정보학회논문지, 제20권 제5호, 113-121, 2015.5

[13] 한국남동발전, "스마트 융합보안 마스터 플랜 고도화 최종보고서", 2016.10

〔저자소개〕

이 대 성 (Daesung Lee)
1999년 2월 인하대학교 전자계산공학과 학사
2001년 2월 인하대학교 전자계산공학과 석사
2008년 2월 인하대학교 정보공학과 박사
2012년 3월 ~ 현재 부산가톨릭대학교 부교수
email : dslee@cup.ac.kr