사이버보안 클러스터 구축 연구

박대우*

*호서대학교 벤처대학원

Research on the Cyber Security Cluster

Dea-woo Park*

*Hoseo Graduate School of Venture

E-mail : prof_pdw@naver.com

요 약

국내 정보보호 산업 성장률(7.1%)은 이전 3년 성장률(15%)에 비해 하락하였다. 정부는 K-ICT 시큐리티 2020을 발표했다. 정보보호산업의 경쟁력 강화와 창업활성화, 일자리 창출을 추진한다는 정책에 맞춰, ICT 산업과 연계된 사이버보안 클러스터 조성이 필요하다. 본 논문에서는 사이버보안 클러스터 구축을 위한 연구를 한다. 해외의 성공적인 사이버 클러스트를 조사하고 분석한다. 또한 국내에 있는 기존의 클러스트를 분석하고 문제점을 파악한다. 결론적으로 사이버 클러스트를 구축하고 운영하기 위한 방안에 대한 연구와 사이버 클러스트의 기대효과를 연구한다.

ABSTRACT

Korea Information Security Industry growth rate (7.1%) declined compared to the previous three years growth (15%). The government has announced a 2020 K-ICT security. According to the policy of promoting the competitiveness of industry consolidation and data protection enable entrepreneurship, job creation, there is a need for the ICT industry in conjunction with cyber security cluster composition. In this paper, I research for cybersecurity cluster. Investigate a successful cyber clusters of foreign and analyzed. In addition, I analysis of existing cluster in the domestic and identify the problem. Consequently, building a cyber-research cluster and the expected effects of cyber-research and on how to operate the cluster.

키워드

사이버보안, 클러스트, 연구 분석, 기대효과

Ⅰ. 서 론

미래창조과학부는 2016년 6월 9일 열린 제8차 경제관계장관회의에서 제1차 정보보호산업 진흥 계획인 ‘K-ICT 시큐리티 2020’을 발표했다. 창업활성화와 해외 진출을 중심으로 정보보호산업의 경쟁력 강화와 일자리 창출을 추진할 계획이다. 이번 계획을 통해 2020년까지 정보보호 창업기업 100개, 글로벌 강소기업 10개를 육성하려고 한다. 현재 1조6000억원 규모의 정보보호 수출규모를 4조5000억원으로 확대하고, 1만9000여개 일자리 창출을 기대하고 있다. 지능정보기술을 활용한 정보보호 원천기술 확보로 선진국과의 기술격차를 현재 1.5년에서 0.2년으로 단축하겠다는 의지도 내보였다.

한국 정부는 융합이 진전된 ▲의료 ▲에너지 ▲교통 ▲홈・가전 ▲제조 5대 분야에서 우선 정보통신기술(ICT) 융합보안 정책을 펴기로 했다. K-ICT 융합보안 발전전략은 ICT 융합 안심사회를 구현하기 위한 정책이다. ICT와 교통・의료・에너지 등 산업간 융합이 확산되면서 해킹 등 사이버 보안위협이 산업은 물론이고 일상생활로 확대될 위험이 커지는 데 따른 대응책이다.

미래창조과학부는 5대 ICT 융합 제품 및 서비스 개발 때 설계 단계부터 보안기능을 적용하도록 추진한다. 지능형 CCTV와 바이오인식, 스마트카드, 빅데이터 기반 영상분석 등 4대 미래유망 물리보안산업의 육성도 지원한다. 예를 들어 스마트의료 분야에선 체내 약물주입 펌프를 해킹해 주입량을 조작할 수 있다는 위험이 발견되면서, 지난해 미국에서 사용이 금지됐다. 스마트 교통 분야에선 원격으로 시동이나 브레이크 조작이 가능성이 꾸준히 제기되고 있다.

미래창조과학부는 창업활성화 전략으로 침해

대응 시설·인력 양성기관 등을 집적한 정보보호 클러스터 조성을 추진하고, 글로벌 펀드 및 엑셀러레이터와 연계해 유망 스타트업의 발굴에서 사업화까지 전 단계에 지원을 한다고 밝혔다.

국내 정보보호 기업은 매출액 300억원 미만의 영세 중소기업이 대부분(92%)이고, 내수시장(80%)에 의존하고 있다. 또한 2014년 국내 정보보호산업 성장률(7.1%)은 이전 3년 성장률(15%)에 비해 큰 폭으로 하락, 세계 시장 성장률(8.5%)보다 낮은 성장정체현상이 뚜렷하다.

따라서 정부의 정책에 발 맞춰서 정보보호산업이 독자적인 기능으로 존재하기보다 다른 ICT분야의 필수기능으로 포함되면서, ICT 산업과 연계된 집적화된 사이버보안 클러스터 조성이 필요하다.

본 논문에서는 사이버보안 클러스터 구축을 위한 연구를 한다. 해외의 성공적인 사이버 클러스트를 조사하고 분석한다. 또한 국내에 있는 기존의 클러스트를 분석하여 문제점을 파악한다. 결론적으로 사이버 클러스트를 구축하고 운영하기 위한 방안에 대한 연구와 사이버 클러스트의 기대효과를 연구한다.

Ⅱ. 해외 클러스터 사례 및 효과 분석

2.1 사이버 시큐리티 스파크(Cyber Security Spark)

이스라엘(Israel) 텔아비브에서 남쪽으로 100㎞ 떨어진 곳에 베르셰바(Beer Sheva) 지역이 있다. 이스라엘 정부는 보안산업을 키우기 위해 유닛 8200과 같은 군부대와 민간의 협력을 강화하는 '사이버 스파크' 프로젝트를 추진했다.

이스라엘의 베르셰바 77 Ha'Energia Street, Advanced Technologies Park에 20만㎡(약 6만평) 규모의 부지를 조성해 그림 1처럼 이스라엘방위군(IDF)과 대학, 글로벌 보안회사의 R&D센터를 한곳에 모으는 작업을 하고 있다. IBM 록히드마틴 EMC 등 해외 기업들도 이곳에 R&D센터를 세웠다. 네게브 사막 한복판에 위치한 도시다. 사막 한편에 완공된 6층짜리 빌딩이 있다.

이곳에는 세계 적인 소프트웨어 업체 '오라클', 독일 최대 통신사 '도이치텔레콤', 미국 군수업체 '록히드마틴' 등 13개 다국적 기업 직원 1,000여명이 근무하고 있다.

이스라엘 군의 시설을 사막 한곳에 모아 놓은 세계 최초의 '사이버 보안 도시'가 될 것"이라며 "이스라엘의 기술력과 인력을 활용해 연구·개발의 시너지를 높이려는 글로벌 기업들이 유치 대상"이라고 말했다.

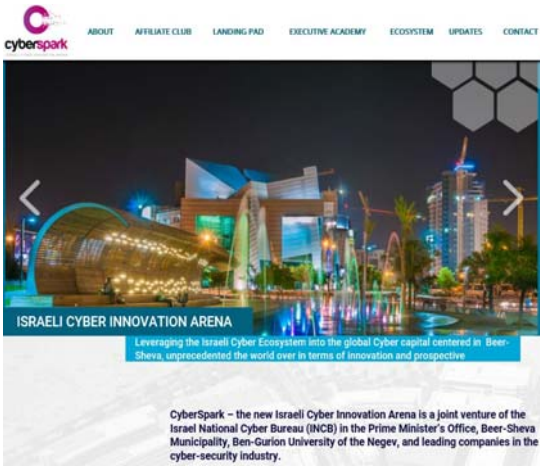

Fig. 1 CyberSpark Home page

베르셰바 벤구리온 대학만 해도 컴퓨터 엔지니어링을 전공하는 기술 인력 8,000여명이 재학 중이라는 것이다. 여기에 이스라엘 정부는 사막 지대의 접근성을 위해 베르셰바를 기점으로 지중해와 홍해를 잇는 철도 건설 계획도 추진하고 있다.

전(全) 국토의 50% 이상이 사막인 이스라엘은 안보 위협 속에서도 전 세계에서 글로벌 금융 위기를 가장 잘 극복한 나라로 꼽힌다. 과감한 양적 완화 조치와 함께 '창업 국가(Start-up Nation)'라는 별명대로 끊임없이 신생 스타 기업을 탄생시키며 성장을 이끌고 있다.

이스라엘 최고 정보수집부대인 '유닛8200'은 최정예 사이버보안 전문가를 배출하는 곳으로 유명하다. 이스라엘 대표 보안회사이자 나스닥 상장사인 체크포인트의 길 슈웨드 창업자도 이 부대 출신이다.

에비아타 마타냐 이스라엘국가사이버국(INCB) 국장은 "베르셰바단지는 5,000여명의 사이버 전문가가 모이는 대규모 단지로 조성될 것"이라며 "정부는 민간기업이 활발히 비즈니스를 펼칠 수 있도록 '마중물' 역할을 할 것"이라고 말했다.

200여개의 이스라엘 사이버보안 관련 회사들은 세계를 무대로 비즈니스를 하고 있다. 체크포인트를 비롯해 지난해 나스닥에 상장한 사이버아크 등이 대표적인 이스라엘 업체다.

이스라엘 정부에 따르면 이들 보안업체가 연간 수출하는 금액만 30억달러(약 3조3100억원)에 이른다. 이는 글로벌 사이버보안 시장의 5% 규모다. 첸 비탄 사이버아크 총괄매니저는 "정부 관계자와 다양한 회의를 하면서 보안산업 생태계를 함께 조성하고 있다"고 설명했다.

Ⅲ. 사이버보안 클러스터 구축 방안

3.1 사이버보안 클러스터 구축 준비

국내 클러스터는 상대적으로 역사가 일천하고 제반 환경이 취약한 상태이기 때문에 인내심과

장기적인 안목의 지속적인 투자가 필요하다.

국내의 대표적 클러스터인 대덕연구단지의 경우 혁신 주체 간 네트워킹이 미약한 실정이다. 따라서 사이버보안 클러스트 구축을 위한 사업화 체제도 이제 시작 단계로 향후 내실을 기하기 위한 지속적 노력과 전략이 필요하다.

또한, 대덕연구단지의 분원 형태로 이뤄진 기타 지방 클러스터의 경우(예, 대구 테크노폴리스)는 대부분 지역 유치형으로 건물 등의 인프라와 같은 외견적 형태만 구축되어 있을 뿐 실질적 클러스터의 시너지 기능은 현재 단계에서는 기대하기 힘든 구축 초기 단계이므로 정부가 저극적으로 주도하여 추진하는 준비단계가 필요하다.

클러스터는 장기간 투자의 산물로서 클러스터가 완벽한 생태계를 갖추기 까지 보통으로 20년 이상의 시간이 소요된다. 실리콘 밸리와 할리우드, 도요타 클러스터는 60년 이상, 시스타 사이언스파크는 35년, 울루는 30년의 기간에 걸쳐 현재에 이르고 있다. 이들 클러스터는 성장과정을 거치면서 VP, SO, SS의 역할이 정립되고 긴밀한 네트워크가 형성되므로 장기간의 사업준비 기간과 인내심이 요구된다.

3.2 사이버보안 클러스터 구축 방안

◮ 정부 주도의 클러스터 운영 정책개발 필요

- 국가경쟁력을 높이기 위한 장기적인 전략으로, 동종기업들 간의 협업을 장려할 수 있는 정부 주도 플랫폼이 필요하다.

◮ 중소기업 지원책으로써의 클러스터 정책 시행 가능

3.3 전문기관의 비식별 조치 지원 강화 및 데이터 브로커 양성

전문기관이 벤처기업 등 소규모 회사의 비식별 조치를 지원하기 위해 개인정보보호법 등 관련 법률로부터 개인정보를 제공받아 처리할 수 있는 권한을 받아야 비식별 조치가 원활이 이뤄질 수 있다. 이러한 경우 전문기관에서 개인정보보호법 위반 사례가 발생해 프라이버시 침해가 될 수 있다. 하지만, 이러한 침해 가능성에 대한 대책도 법률에 명시하고 정부에서 정기적으로 점검을 한다면 충분히 해결될 수 있을 것으로 판단된다.

또한, 이러한 전문기관의 적극적인 지원은 향후 데이터 활용 선진국과 같이 데이터 브로커의 밑거름이 될 수 있다. 엑시엄사(Acxiom)와 같은 데이터 브로커는 데이터 활용의 기반시설이라고 할 수 있다. 이러한 데이터 브로커 없이 데이터 융합을 성공한 사례는 현재까지 국내외에 거의 없다.

그러므로 현재의 공공기관들로 구성된 전문기관에게 적극적인 비식별 조치 지원 권한을 우선 부여하고 일정 기간 동안 빅데이터 활성화 효과 및 개인의 프라이버시 침해요소를 모니터링 한 후 민간 전문기관에게도 비식별 조치 지원 권한을 부여해 국내 빅데이터 산업을 활성화 하여야 할 것이다.

3.4 입주 기업에 대한 인센티브를 제공

시큐리티 스파크가 ICT 정보보호 산업 클러스터 기능을 충실히 하기 위해서는 무엇보다 국내 산업단지 분포와 기존 영업망과의 연계성을 고려한 위치를 선정하는 것이 중요하다. 그리고 일정 수준 이상의 기업이 입주하여 산업단지 효과를 내야한다. 정책당국은 시큐리티 스파크 입주 기업에 대한 인센티브를 제공할 수 있어야 한다.

3.5 사이버 시큐리티 클러스터 기대 효과 분석

입주한 기업들은 ICT 정보보호 제품개발 지원 및 교육 시설 이용, 공동브랜드 사업 및 공동 마케팅, 공동 제품개발을 위한 컨설팅 혜택 등이 가능하다. 국가 연구시설장비 공동 활용 서비스와 특허 및 인증 지원시설 등의 도움도 받을 수 있다. 스타트업이 입주하면 사업장 임대와 세제혜택 등이 절실하기 때문이다.

이와 함께 ICT 시큐리티 스파크를 통해 연구개발(R&D) 역량을 강화해 한국 기업들이 글로벌 제품을 능가하는 기술력을 확보할 수 있다면 큰 도움이 될 것이다.

Ⅳ. 결 론

현재 중소 및 벤처기업의 경우 연간 연구개발(R&D) 투자비중이 매출 대비 10% 전후다. 이러한 낮은 비중이 ICT 정보보호산업 경쟁력 저하의 원인이 된다.

국내 사이버 클러스트 구축은 ICT 정보보호 업계 간 정보를 공유하고 상생협력 강화를 이끌기에 필수적인 셈이다. 이를 통해 정부가 ICT 정책 방향을 정할 때 기업과 현장의 상황을 쉽게 파악할 수 있기 때문이다.

사이버 클러스트 구축을 위한 해외 시큐리티 스파크 등의 성공요인을 분석하고, 국내 환경에 맞게 제안한다. 또한 구축 준비와 기대효과에 대한 연구를 통해 국내 사이버보안 시장을 활성화를 기대한다.

참고문헌

[1] KISA, 해외 현지 조사 · 분석을 통한 ICT 융합보안클러스터 조성방안 연구용역, Aug. 2016.

[2] 박대우, “해외 현지 조사 · 분석을 통한 ICT 융합보안클러스터 조성방안 연구용역 제안서”, Aug. 2016.