융합보안 관점에서 방위산업보안 개념 정립과 연구동향 분석★

우광제*

요 약

산업스파이에 의한 핵심기술 유출이 점차 지능화, 첨단화, 복잡화 되어가고 있으며 이로 인한 피해 또한 심각해지고 있다. 이러한 상황에 대응하는 방안으로 융합보안이 대두되었고 모든 산업분야에 점차 확대되고 있다. 특히 국가적 핵심기술과 인력 및 시설을 포함하고 있는 방위산업은 융합보안이 더 요구되는 산업분야이다. 방위산업은 국가의 안전보장에 필요한 방위산업물자를 연구, 개발, 생산하는 산업이다. 방위산업은 군사기밀, 산업비밀, 핵심기술인력, 방위산업물자, 국가중요시설, 정보통신체계 등 다양한 보안요소를 포함하고 있다. 방위산업보안은 군사보안과 산업보안의 복합체이며 방위산업의 모든 보안요소를 통합하는 융합보안이다. 따라서 방위산업보안은 융합보안의 대표적인 실천모델이라고 할 수 있다. 방위산업보안에 대한 연구는 일반적인 다른 산업분야에서의 보안과 관련된 연구에 비해 미흡한 실정이다. 방위산업의 핵심기술 유출을 방지하고 기술인력 및 시설을 보호하기 위해서, 방위산업보안을 융합보안의 개념에서 연구하고 실천하는 노력이 절실한 시점이다.

Resaerch Trend and Cocentualization of Defense Industry Security From Convergence Security Perspective

Woo, Kwang Jea*

ABSTRACT

Methods that industrial spies use to smuggle core technology out are becoming more intelligent, technological, and complex, thus resulting in more serious damages. In particular, defense industries in which involve national core technology as well as institutions including labor force are industries that are in a greater need of the convergence security. Defense Industry develops, experiments, and produces defense security supplies for national security protection. Defense industry involves a number of security elements such as military secret, industrial secret, core technology labor force, defense industry supply, critical national facility, and information communication system. Defense industry security is a complex of military security and industrial security which is convergence security that integrates all security elements of defense industry. Therefore, defense industry security is a typical ideal model for convergence security. Research on defense industry security is relatively insufficient compared to research of security in other industrial fields. In order to prevent core technology of denfese industry from leaking and to protect technical professionals and institutions, research and action on defense industry security from convergence security perspective are therefore essential at this point of time.

Key words : 방위산업보안, 융합보안, 방위산업

접수일(2015년 9월 25일), 게재확정일(2015년 10월 20일)

★ 본 논문은 우광제의 2015년도 박사학위 논문에서 발췌 정리하였음.

* 중앙대학교 인적자원개발학과

1. 서 론

미래학자 앨빈 토플러는 그의 저서 '권력이동'에서 권력은 무력에서 자본으로 그리고 미래에는 지식으로 이동할 것이며 21세기에는 산업스파이가 가장 큰 산업 중 하나가 되고 정보전쟁과 날로 늘어가는 경제·금융스파이가 현재를 특징지을 것이라고 예측한 바 있다[1]. 이러한 예측은 오늘날 현대사회에 그대로 반영되고 있으며 산업스파이에 의한 핵심기술 유출은 점차 지능화 및 첨단화, 다양화 및 복잡화되면서 산업 전반에 피해를 확산시키는 특징을 보이고 있다. 국가적 핵심기술을 보유하고 있는 방위산업 분야도 예외는 아니다. 특히 최근에는 정보통신의 발달로 인해 핵심기술 뿐만 아니라 개인정보를 유출하거나 정보통신시스템을 파괴하려는 위협도 점차 증가하고 있다.

산업기술보호센터에 따르면 핵심 산업기술을 해외로 유출하다가 적발된 건수가 지난 10년 동안 375건에 달하면서 매년 증가하고 있다[8]. 2010년 이후 발생한 주요 산업기술 유출 사례를 살펴보면 유기발광 다이오드 핵심기술의 중국 유출기도 사건, 세계 최대 용량 빌딩용 첨단에어컨 핵심기술 중국 유출기도 사건, 태양전지 생산 장비 제조기술 해외유출 사건, 차세대 디스플레이기술 해외유출 사건 등 국가적으로 중요한 핵심기술의 해외유출이 끊이지 않고 발생하고 있다. 한편 2014년 4월 현대캐피탈 정보유출과 농협 전산망 마비사건, 2013년 3월 정부기관 사이버 테러, 2014년 1월 신용카드사 개인정보 유출 등 정보통신과 관련된 보안 사고는 국가시스템의 마비는 물론 기업에도 막대한 피해를 입혔다. 또한 방위산업 분야에서도 국내 방위산업체 출신 기술자들이 공모하여 미얀마에 수백원대 규모의 포탄제조 설비 및 기술을 불법 유출 하다 적발되는 등 보안 사고는 모든 산업분야에서 발생하고 있으며 이에 따른 피해도 점차 증가하고 있다.

이러한 상황은 국가경쟁력의 확보와 기업의 생존을 위한 산업보안의 중요성을 일깨워 주고 있다. 특히 지능화, 첨단화, 복잡화 되어가는 기술유출에 전략적으로 대응하기 위한 방안으로 융합보안(Convergence Security)이 대두되고 있다. 오늘날 기업들이 직면하고 있는 다양한 보안위협의 복잡성과 상호의존성은 기업의 위기를 포괄적으로 평가하기 위한 조직 전체적인 보안 기능의 융합을 필요로 하게 되었다[22]. 일반적으로 산업에서의 '융합(Convergence)'이란 산업 간, 기술과 산업 간, 기술 간의 창의적인 결합과 복합화를 통하여 기존 산업을 혁신하거나 새로운 사회적·시장적 가치가 있는 산업을 창출하는 활동을 말한다[8]. 보안산업도 과거에는 정보보안과 물리보안으로 구분되어 성장해 왔으나, 현재는 정보보안과 물리보안이 통합되면서 고가치 융합보안 서비스 산업으로 부상하고 있다. 또한 최근에는 보안기술이 다른 기술이나 산업과 융합하면서 새로운 보안제품과 서비스가 창출되고 있다[18]. 이렇듯 융합보안의 산업구조는 '보안산업 내 보안영역 간의 통합'과 '다른 산업과의 융합' 이라는 두 가지 형태로 발전되고 있다.

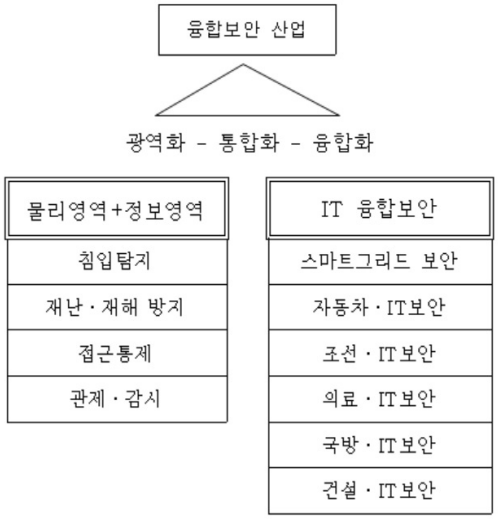
융합보안의 적용은 모든 산업분야로 점차 확대되고 있으며, 특히 방위산업 분야는 군사비밀, 산업기술, 방산물자, 핵심기술인력, 국가보안목표시설 등 다양한 보안요소를 보유하고 있기 때문에 융합보안이 보다 더 요구되는 분야라고 할 수 있다[11]. 이로 인해 방위산업체들은 보안 전담조직과 보안담당관을 임명하여 전사적 차원에서 제반 보안요소를 보호하기 위한 종합적인 보안대책을 강구하고 있다. 방위산업체의 보안전문가는 방위산업보안업무훈령에 의거해서 방위산업체의 보안대책 수립으로부터 시행과 조정 및 감독까지 전반적인 보안업무를 수행하고 있다[2]. 이러한 맥락에서 방위산업은 융합보안을 적용하고 있는 가장 대표적 산업분야라고 할 수 있다. 따라서 본 연구에서는 융합보안의 관점에서 방위산업보안의 개념을 정립하고 연구동향을 분석하였다.

2. 융합보안

2.1. 융합보안의 개념

일반적으로 산업에서의 융합(Convergence)이란 산업 간, 기술과 산업 간, 기술 간의 창의적인 결합과 복잡화를 통하여 기존 산업을 혁신하거나 새로운 사회적·시장적 가치가 있는 산업을 창출하는 활동을

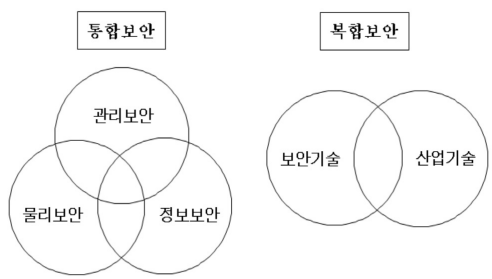
말한다[9]. 과거의 전통적 보안산업은 시설이나 장비를 보호하기 위한 물리보안(Physical Security)과 개인이나 기업의 정보를 보호하기 위한 정보보안(Information Security)으로 구분되어 각각 발전되어 왔다. 그러나 현재의 보안산업은 (그림 1)과 같이 출입통제, 주차시설 관리, CCTV, 영상보안 등 물리적 환경에서 이루어지는 전통적 보안산업이 컴퓨터, 네트워크상의 정보를 보호하는 정보보안 기술과의 접목을 통해 차세대 고부가가치 융합보안 서비스 산업으로 부상하고 있으며, 정보기술이 자동차, 조선, 의료, 건설, 국방, 전력 등 기존산업에 활용되면서 정보기술과 산업 간의 융합에서 발생하는 보안위협을 해결하기 위한 새로운 형태의 보안제품 및 서비스가 출연하고 있다[18]. 이러한 추세에 맞춰 미래창조과학부에서도 의료, 가전, 시설, 물류, 자동차 등의 분야에서 정보기술을 활용한 융합보안 서비스 사례를 제안하면서 '융합보안 시범사업'을 추진하고 있다[7]. 이렇듯 융합보안의 산업구조는 '보안산업 내 보안영역 간의 통합'과 '다른 산업과의 융합' 이라는 두 가지 형태로 발전하고 있다.



(그림 1) 융합보안 산업의 구성[18]

보안환경의 변화와 보안산업의 발전 추세에 따라 산업보안에 대한 연구도 기존에는 물리보안과 정보보안을 별개의 시스템으로 간주하였으나 최근에는 보안영역 간의 통합과 관련된 연구가 진행되고 있다. 또한 산업보안학은 법학, 범죄학, 경영학, 공학 등 여러 분야의 학문과 융합되어 독자적인 학문 영역을 확보하고 있다[15]. 산업보안 측면에서 보안의 정의는 단순히 산업기술이나 기밀의 유출 방지를 의미하는 협의적 개념과 각종 범죄로부터 모든 경제활동을 보호하는 일체의 노력을 의미하는 광의적 개념으로 구분될 수 있다[13]. 이러한 보안산업의 융합화와 학문적 융합 추세는 산업보안의 개념을 협의적 개념에서 광의적 개념으로 확장시키면서 산업보안이 융합보안(Convergence Security)으로 발전되는 계기가 되었다.

융합보안(Convergence Security)은 '융합'의 개념에 따라 다양하게 구분된다. 융합의 개념은 조직 내 보안요소들을 상호 연계하여 보안의 효과성을 높이고자하는 '통합적' 개념과 보안기술을 다른 산업기술들과 융화시켜 새로운 기술을 창출하는 '복합적' 개념으로 나눠 볼 수 있다[5]. 또한 '통합적' 개념의 융합보안은 물리보안과 정보보안의 통합과 전사적 차원에서 모든 보안요소의 통합으로 구분될 수 있다. 이와 같은 융합보안의 통합적 개념과 복합적 개념을 도식화하면 (그림 2)와 같이 나타낼 수 있다.



(그림 2) 융합보안의 통합적 개념과 복합적 개념[5]

융합보안의 가장 협의적 개념은 물리보안과 정보보안의 통합이다. 지식경제용어사전에 따르면 융합보안은 "물리보안과 정보보안을 융합한 보안개념으로, 각종 내·외부적 정보 침해에 따른 대응은 물론 물리적 보안장비 및 각종 재난·재해 상황에 대한 관제까지 포함하는 것"으로 정의되어 있다[16]. Contos, Hunt와 Derodeff는 융합을 IT기술과 도구들이 물리보안에 적용되는 것과 물리보안의 요구에 대해 IT기

술이 지원되는 것이라고 정의하였다[25]. 여기서 물리보안은 특정 자산을 보호하기 위한 유형적 요소들의 논리적인 구조[27]를 의미하며, 발생 가능한 각종 위해로부터 인원 및 자산 등 보호대상을 보호하기 위해 이루어지는 물리적인 조치[21]를 의미한다. 그리고 정보보안은 승인되지 않은 조직이나 사람들에게 정보가 노출되는 위험을 최소화하고 정보를 보호하는 것이다[35]. 따라서 물리보안과 정보보안의 융합은 주로 물리적 보안시장에서의 IT기술 채택과 같은 형태의 기술적 통합으로 이루어지고 있다.

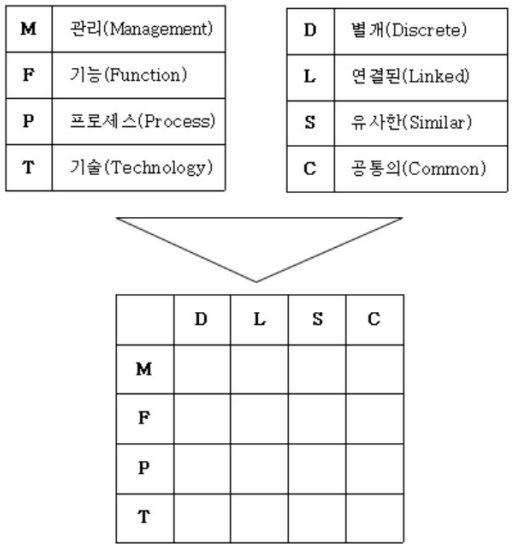
최근의 융합보안은 물리적보안과 IT보안의 단순한 결합의 개념 보다는 전사적 차원에서 모든 보안요소의 통합된 활동으로 정의된다. CSO online에서는 융합보안을 비즈니스 연속성, 재난 복구, 안전 위험관리에 있어서 논리보안, 정보보안, 물리보안, 인원보안의 통합으로 더 나은 보안, 전사적 차원의 위험관리, 비용 효율성을 달성하기 위해 분리되었던 운영적 관리 기능들을 통합하는 것으로 정의하였다[33].

ASIS(American Society for Information Science) International에서는 융합을 기업 내에 존재하는 비즈니스 기능과 프로세스 사이의 상호의존성 및 보안 위험을 식별하고, 이를 적절하게 관리할 수 있는 비즈니스 솔루션을 수립하는 것으로 정의하였다.[24]. Tyson은 위험 완화, 운영적 효과성 및 효율성 증가, 비용 절감 등을 통한 기업이익의 달성을 위해 조직의 축적된 보안 자원을 공식적, 협력적, 전략적으로 통합하는 것을 융합보안이라고 정의하였다[34].

한편 복합적 개념의 융합보안은 제품 및 서비스의 안전성과 신뢰성 향상을 위해 보안기술이 다른 산업에 융화되어 새로운 제품을 창출하고 산업의 부가가치를 높이는 것이라고 할 수 있다[5]. 이러한 복합적 융합보안은 주로 기술과 산업 또는 산업 간의 융합을 의미하는 것으로 보안산업 내에서의 융합을 의미하는 통합적 융합보안과는 다른 차원의 개념이다. 융합보안에 대한 연구도 연구의 목적과 대상에 따라 통합보안과 복합보안으로 구분되어 진행되고 있으나 최근 국·내외 연구들은 대부분 융합보안을 통합적 개념으로 이해하고 조직 내 보안요소들 간의 통합모델을 제시하고 있다[5, 10, 12, 19, 28, 30, 31, 33].

2.2. 융합보안의 모델

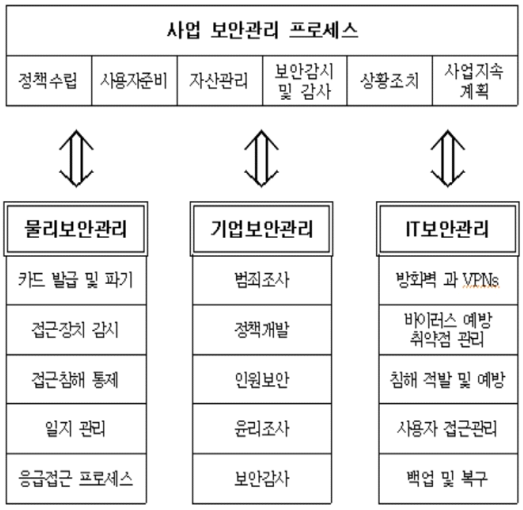
물리적, 기술적, 관리적 보안기능들이 서로 분리되어 운영된다면 조직은 보안에 대한 중복 투자와 보안 관리의 비효율성 등으로 인해 조직의 비용이 증가할 것이다. 이와 같은 문제점을 극복하기 위한 융합보안의 개념적 모델이 제시되었다. Gartner에서는 (그림 3)과 같은 융합보안 모델을 제시하였다. 이 모델은 각각의 영역의 기능, 프로세스, 기술이 서로 연계된 정도에 따라 세 가지 수준으로 융합되어 하나의 영역에 관리되어짐을 보여준다[5].



(그림 3) Gartner의 융합보안 모델[5]

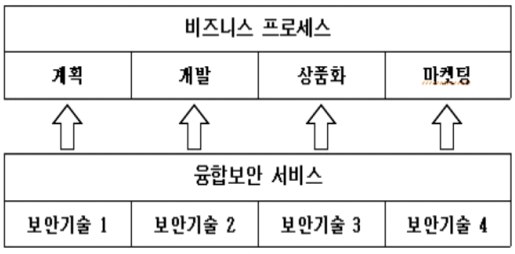
AESRM(The Alliance for Enterprise Security Risk Management)에서는 사업 보안관리 프로세스(Business Security Management Process)를 제시하였다[24]. 사업 보안관리 프로세스는 (그림 4)와 같이 기업의 취약점에 대한 대응계획을 작성하고 실시간 감시 및 대응을 위해서 기존의 물리보안과 정보보안 관리체계를 더 넓은 범위로 확장시킨다. 이러한 통합된 체계는 물리보안이나 정보보안에 국한된 문제에 대해서만 적용되었던 보안위협 평가에서 벗어나 전사적 차원에서 문제를 이해하고 해결할 수 있는 능력을 갖는다[24]. Gartner와 AESRM의 융합보안 모델은 융합의

방법에는 차이가 있으나, 개별적으로 수행되는 물리적, 기술적, 관리적 보안 기능 및 활동들을 상호 연계하여 통합적으로 관리한다는 공통점이 존재한다[5].



(그림 4) AESRM의 융합보안 모델[24]

Kang, Lee, Hwang, 그리고 Chang은 (그림 5)와 같이 제조산업에 있어서의 IT보안기술을 중심으로 한 융합보안 서비스모델을 제안하였다[29]. 융합보안 서비스모델에서 개별적인 보안방책은 비즈니스 프로세스에 적합화된 보안기능을 제공하기 위해서 통합되어진다. 이 모델에서 IT보안방책들은 각각의 제조산업체에 맞도록 적합화되어 융합되는 것이 중요하다. 융합보안 서비스모델이 제조산업체에 적용된 후에도 적용결과에 따라 변경된다.



(그림 5) 융합보안 서비스모델[29]

2.3. 융합보안의 연구동향

융합보안의 개념 정립에 있어서 가장 많은 노력은 2005년 1월에 구성된 AESRM(The Alliance for Enterprise Security Risk Management)에 의해서 이루어졌다[34]. AESRM은 국제적으로 보안에 대한 연구를 주도하고 있는 ASIS(American Society for Information Science) International, ISACA(Information Systems Aduit and Contral Association), ISSA(Information Systems Security Association)의 3개 기관이 모여 출범한 연합체이다. AESRM은 전통적 보안과 정보보안의 통합을 제안하고, 중요한 보안 이슈들에 대한 관심과 기업보안을 위한 포괄적인 접근의 필요성에 대한 최고위 경영진들의 관심을 이끌어 내기 위해서 구성되었다.

AESRM의 첫 번째 보고서인 'Convergence of Enterprise Security Organization'은 2005년 11월 미국의 경영컨설팅 회사인 Booz Allen Hamilton에 의해 작성되었다. Booz Allen Hamilton은 글로벌 기업에서 융합보안의 영향을 파악하기 위해 10억 달러에서 1천억 달러 규모의 수익을 기록하고 있는 36개 글로벌 기업의 CSO(Chief Security Officers), CISO(Chief Information Security Officers)를 포함한 보안전문가를 대상으로 인터뷰와 설문조사를 실시하였다. 연구결과는 융합보안이 모든 산업의 기업에 있어서 현저한 영향을 미치고 있는 것으로 나타났다. 보안관리자와 전문가에 대한 인터뷰 결과, 융합보안의 동인(動因) 또는 필요성은 첫째, 기업 생태계의 빠른 확장 둘째, 물리적 자산으로부터 정보기반 자산과 무형자산으로의 가치 이동 셋째, 기능적 경계를 불분명하게 하는 새로운 보호기술 넷째, 새로운 법과 규제 다섯째, 비용감소에 대한 지속적인 압력으로 확인되었다[24].

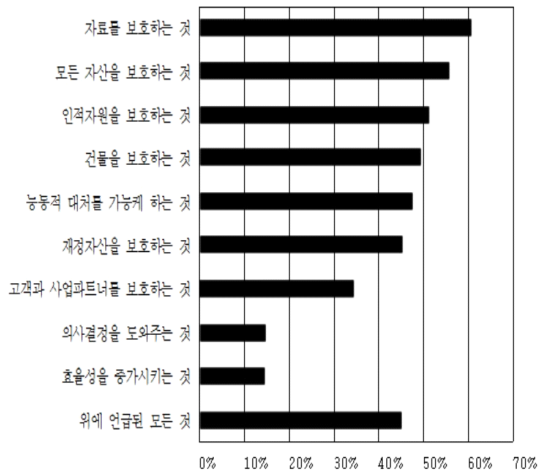
이러한 동인들은 기업의 전체 비즈니스 영역에 있어서 보안담당자들의 역할 변화와 함께 분야별 융합을 유발한다[24]. 예를 들어 기존의 보안과 위험에 대한 논의가 더 통합적이고 상호 기능적으로 바뀌면서, 물리보안과 정보보안 담당자들이 통합된 보안방안을 만들어 낼 것이라는 기대가 점 더 커진다는 것이다. 또한 이 보고서는 보안전문가들이 보안기능에만 중점을 두는 것이 아니고 전체 사업의 가치를 증진시키도록 보안을 통합하는 새로운 단계로 전환해야 한다는

것을 주장하였다[24].

AESRM에서는 2005년의 보고서에 이어 2007년에도 'The Convergence of Physical and Information Security In The Context Enterprise Risk Management'를 발표하였다[26]. 이 보고서는 미국의 전문가 서비스 네트워크인 Deloitte에 의뢰하여 작성되었으며 Deloitte의 회원사를 대상으로 한 설문조사를 통해 연구되었다. 이 연구의 목적은 첫째, 위기관리의 한 부분으로서 보안의 가치를 확인하는 것이고 둘째, 보안의 통합된 관점의 이익을 알아보는 것이다[26]. 보안에 대한 기업의 고위경영진들의 인식은 <표 1>과 같이 보안을 기술적 기능으로 만 여기고 상위 수준의 경영프로세스나 의사결정에 필요한 기능으로 여기지 않는다는 사실을 확인하였다.

Deloitte의 분석가들은 이러한 문제점을 지적하면서 조직이 중대한 위험을 이해하고 완화시킬 수 있도록 하는 '융합'의 중요성을 제기하였다. 또한 기업의 위기관리가 보안의 효율성 증대와 효과성 강화를 위한 기회에 중점을 두기 때문에, 향후 5년 동안 융합시장이 급격하게 성장 할 것이라고 예견하였다. 이 보고서는 기업에서 융합보안을 구축하기 위한 세 개의 방안으로 하나의 리더 아래 여러 기능들의 통합하는 방안, 각각의 기능을 분리해서 유지하되 공통관리자에게 보고하는 방안, 각각의 기능을 분리해서 유지하되 보안에 대한 이슈를 위기관리위원회에서 다루는 방안 등을 제안하였다[26].

<표 1> 보안에 대한 최고위 경영진의 인식[26]



국외에서 융합보안에 대한 연구는 주로 AESRM 보고서를 기초로 기업경영에 있어서 정보보안과 물리보안의 융합 필요성과 적용방안을 제안하였다[28, 30, 31, 33]. 반면 Schultz는 물리보안과 정보보안의 융합으로 인한 위험성을 제기하면서 물리보안과 정보보안의 섣부른 융합은 오히려 심각한 문제를 야기한다고 주장하였다[32]. 한편 융합보안을 위험관리 측면에서 해석한 Anderson은 기업의 보안의 핵심 프로세스는 위험평가, 정책개발, 투자기술, 재정적 지식 등에 중점을 두게 되면서, 보안담당자들은 다양한 자격증과 지식을 갖추도록 요구되어 질 것이라고 예측했다[23].

국내에서는 2008년 지식경제부의 '지식정보보안산업 진흥 종합계획'에서 지식정보보안산업의 분류 구분으로 정보보안 및 물리보안과 함께 융합보안의 용어가 처음으로 사용된 후부터 융합보안에 대한 연구가 활발해졌다. 김정덕 등은 융합보안의 개념 정립과 접근방법에 대한 연구에서 융합보안의 정의를 통합보안과 복합보안 측면에서 분석하고, 융합보안의 효과적 구현을 위해서는 하향식 접근법을 사용해야 한다고 주장하였다[5]. 이창훈과 하옥현도 산업기밀 보호체계에 있어서 물리보안과 정보보호로 구분된 기존 보안체계의 문제점을 지적하면서 이에 대한 효과적 해결방안으로 통합보안 측면에서 물리적·기술적·관리적 요소의 유기적 연동과 복합보안 측면에서 부가가치 창출요소에 대한 보호 필요성을 제안하였다[14].

통합보안 측면의 융합보안 연구는 주로 물리보안과 정보보안의 통합 위주로 이루어졌다. 하옥현은 산업기술의 유출이 융·복합적으로 이루어지는 상황 하에서 물리보안시스템과 정보보안시스템의 융합관제의 필요성을 제기하였다[19]. 그는 이러한 융합관제의 핵심기술로 상관관계 분석기술을 제안하면서 물리보안에 정보보안을 통합시킨 융합보안시스템의 설계 방안을 제안하였다. 안황권은 보안산업이 물리보안과 정보보안의 두 개의 축으로 발전해 오면서 서로 별개의 영역이라는 여겨졌으나, 보안위협이 복잡화, 변형화, 다양화되면서 융합보안이 등장하게 된 것이라고 주장하였다[10]. 그는 융합관제와 통합인증을 물리보안과 정보보안의 대표적 융합사례로 제시하였다.

복합보안 측면의 융합보안에 대한 연구는 보안기술이 다른 산업기술에 어떻게 접목될 수 있는지에 대

한 연구형태로 이루어졌다. 이근호는 정보통신기술의 발전에 따라 각종 장치간의 통신과 네트워크의 융합 기술이 점차 확대되고 있는 상황 속에서 Machine to Machine, 지능형 자동차, 스마트그리드, U-헬스케어에 대한 보안위협요소를 분석하고, 이에 대응하기 위한 방안으로 임베디드 시스템 보안, 포렌식 보안, 사용자 인증과 키관리 기법 등 정보보안기술의 융합을 제안하였다[12]. 안황권은 보안기술이 융·복합되어 적용되는 대표적 분야로 운송, 로봇, 금융, 의료, 건설, 국방에서의 융합보안 사례를 제시하면서 융합보안의 시대를 맞이하여 물리보안 사업자도 기존의 사업영역만을 고집하지 말고 보안환경의 변화 속에서 새로운 비즈니스 기회를 찾을 것을 제안하였다[10]. 한편 최경호 등은 각종 기상정보를 물리보안에 활용하는 융합모델을 제시하였다[17].

3. 방위산업보안

3.1. 방위산업보안의 개념

융합보안 개념과 모델의 적용은 모든 산업분야로 점차 확대되고 있으며 특히 방위산업 분야는 군사비밀, 산업기밀, 방산물자, 핵심기술인력, 국가보안목표시설 등 다양한 보안요소를 보유하고 있기 때문에 융합보안이 더 요구되는 분야라고 할 수 있다[11]. 산업보안이 '산업'과 '보안'의 합성어라면[13] 방위산업보안(Defense Industry Security)은 '방위산업' 분야에서의 '보안'을 의미한다. 그러므로 '방위산업'을 어떻게 정의하느냐에 따라 방위산업보안의 의미도 달라질 수 있다. 방위산업의 사전적 정의는 "국가를 방위하는데 필요한 무기, 장비, 기타 물자를 생산하는 산업"[6] 또는 "국가방위를 위하여 군사적으로 소요되는 물자의 생산과 개발에 기여하는 산업"이다[20]. Wikipedia에서는 방위산업을 "군사물자, 장비, 시설 등에 대한 연구, 개발, 생산, 서비스와 관련된 산업"이라고 정의하고 있다[36].

방위산업은 국가별·시대별 상황 또는 사용 목적에 따라 '군사산업(Military industry)', '무기산업(Arms industry)', '전쟁산업(War Industry)', '병기산업(Weapons Industry)', '군수산업(Munitions Industry)' 등으로 다양하게 사용되어져 왔다. 미국과 유럽에서는 군사무기를 중심으로 한 글로벌산업에 초점을 맞춰 '군사산업' 또는 '무기산업' 용어를 사용하고 있다. '군수산업'은 제2차 세계대전까지 사용되다가 전쟁개념이 방위전의 개념으로 발전되면서 '방위산업' 용어가 널리 사용되고 있다[20]. '전쟁산업'은 '평화산업'과 대칭되는 용어로 전쟁에 필요한 모든 물자를 생산하는 산업까지 포함하는 광의적 개념이고, '병기산업'은 적에게 직접 또는 간접으로 가해력을 발휘할 수 있는 기기를 제조 또는 개발하는 산업을 의미하는 협의적 개념이다.

방위사업법에서 방위산업의 정의는 "방위산업물자를 제고, 수리, 가공, 조립, 시험, 정비, 재생, 개량, 또는 개조하거나 연구 개발하는 업"을 의미한다. 여기서 '방위산업물자'는 군수품 중에서 방위사업청장이 산업통상자원부장관과 협의하여 지정한 방산물자를 의미하며, 물자의 특성에 따라 주요방산물자와 일반방산물자로 구분된다[3]. 한편 '군수품'은 국방부 및 그 직할부대·직할기관과 각 군에서 사용 및 관리하기 위해 획득하는 물품으로 전장에서 직접적으로 전투력을 발휘하는데 필요한 무기체계와 그 밖의 제반 지원요소를 통칭하는 비무기체계로 구분된다[3].

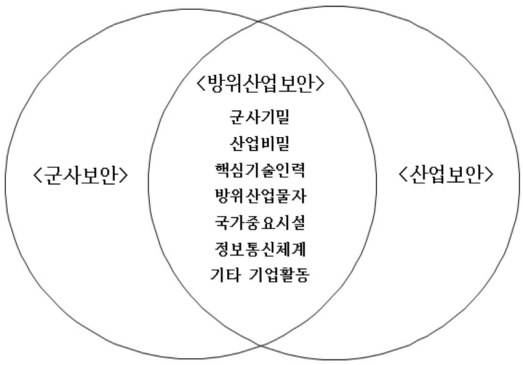
이상과 같이 방위산업은 방위 또는 방위산업물자에 대한 개념을 어떻게 정의하느냐에 따라 협의적 개념과 광의적 개념으로 구분할 수 있다. 방위산업의 협의적 개념은 국가방위에 직접적으로 필요한 무기 및 물자와 관련된 산업을 의미하고, 광의적 개념은 무기 및 물자 외에 간접적으로 필요한 물자까지 모두 포함된 산업을 의미한다. 이 연구는 방위사업법에서 규정한 방위산업체의 보안전문가들이 연구대상이기 때문에 방위산업의 정의도 동 법률에서 규정한 정의를 준용하여 "국가의 안전보장에 필요한 방위산업물자를 연구, 개발, 생산하는 산업"으로 정의하였다.

방위산업은 국가의 안전보장과 직결되는 산업이기 때문에 다른 일반산업보다 더 높은 수준의 보안이 요구된다. 일반산업에서는 산업기밀 보호 위주의 보안활동이 이루어지는 반면 방위산업은 일반산업보다 더 다양하고 복합적인 보안요소를 포함하고 있다. 방위산업체들은 군에서 필요한 기술과 물자를 연구개발하고 생산하는 과정에서 군사기밀을 보유하게 되며 이러한 군사기밀도 첨단 과학기술의 집합체인 산업기술의 성질

을 가지고 있다[4]. 이러한 측면에서 방위산업보안은 군사보안과 산업보안의 융합체로 이해할 수 있다.

방위산업체에 종사하는 직원들은 설계도면과 같은 군사기밀을 다루고 방위산업물자의 생산에 참여한다. 특히 방위산업 연구원들은 핵심 군사기밀과 산업기술을 보유하고 있기 때문에 이들에 의한 기밀유출 방지는 물론 외부세력의 위해로 부터의 보호가 필요하다. 한편 주요 방위산업체와 시설은 국가 안보에 직결되는 무기와 장비 및 시설을 보유하고 있기 때문에 통합방위지침(대통령훈령 제28호)에 따라 국가중요시설 지정되어 보호를 받는다. 일반 방위산업체들도 방위산업보안업무훈령에 따라 시설 및 장비에 대한 보안대책이 강구되어야 한다.

무기 계약 및 생산으로부터 판매에 이르기까지 방위산업체의 기업 활동은 정보통신 시설과 기술을 기반으로 이루어진다. 또한 방위산업물자의 연구개발 과정에서 생산된 핵심기술도 정보통신매체에 보관되고 있다. 따라서 방위산업체들은 방위산업보안업무훈령에 따라 정보보호시스템을 구축하고 네트워크와 인터넷망 등에 대한 보안대책을 강구하고 있다. 방위산업은 이외에도 방위산업물자의 수출입, 하도급, 수송 등 모든 분야에 있어서 보안대책의 강구가 요구되어 진다. 이상과 같이 방위산업은 군사기밀, 산업비밀, 핵심기술인력, 방위산업물자, 국가중요시설, 정보통신체계 등 다양한 보안요소를 포함하고 있다. 따라서 방위산업보안은 (그림 6)과 같이 군사보안과 산업보안의 복합체이면서도 방위산업의 모든 보안요소를 통합하는 융합보안이라고 할 수 있다.



(그림 6) 방위산업보안의 개념과 보안요소

3.2. 방위산업보안의 연구동향

방위산업보안에 대한 연구는 일반적인 다른 산업분야에서의 보안과 관련된 연구에 비해 찾아보기 어렵다. 이는 방위산업보안을 산업보안의 일부로 이해하여 산업보안의 개념을 방위산업보안에도 적용하려는 경향이 있고, 높은 수준의 보안이 유지되는 방위산업의 특성상 일반 연구자가 방위산업보안과 관련된 자료를 수집하기 어렵기 때문이다. 방위산업보안에 대한 일부 연구도 방위산업의 보안 관련 법률을 주제로 한 연구[4]에 국한된다.

김영수는 방위산업보안을 산업보안의 일부로 이해하면서 방위산업 관련 기밀이 유출된 경우 '군사기밀보호법' 보다는 '부정경쟁방지 및 영업비밀보호에 관한 법률'이나 '산업기술의 유출방지 및 보호에 관한 법률'을 적용해야 한다고 주장하였다[4]. 그의 연구는 방위산업의 다양한 보안요소들 중에서 군사기밀에 대한 분야를 중심으로 언급하고 있다. 그리고 방위산업체의 보안방안에 대한 연구가 아니고 오히려 방위산업체가 군으로부터 군사기밀을 불법적으로 수집한 경우의 법률적 검토에 대한 연구이다.

4. 결 론

이상에서 살펴 본 바와 같이 방위산업보안은 융합보안의 개념과 모델이 실천되고 있는 대표적인 분야이다. 또한 방위산업보안은 군사보안과 산업보안의 복합체이면서도 방위산업의 모든 보안요소를 통합하는 융합보안이라고 정의할 수 있다. 방위산업보안에 대한 연구는 방위산업의 중요성에 비해서 일부 한정된 분야에 국한되었다는 것을 확인 할 수 있었다.

융합보안의 관점에서 방위산업보안 개념을 정립함으로서 방위산업보안에 대한 연구가 통합적이고 복합적인 관점에서 이루어 질 수 있을 것이다. 이 연구에서 확인된 방위산업 보안요소들은 방위산업보안 실천전략 수립 과정에서 보안요소별 대응방안을 수립하는데 기여할 것이다. 또한 방위산업보안에 대한 연구동향 분석 결과는 융합보안의 개념과 연계된 방위산업보안 연구의 필요성을 제기하였다.

참고문헌

[1] 국가정보원, '첨단산업기술보호동향 제10호', 2009, http://www.service4.nis.go.kr 에서 2014년 3월 1일 검색

[2] 국방부, '방위산업보안업무훈령', 대한민국정부. 2012.

[3] 국방부, '방위사업법', 대한민국정부, 2014.

[4] 김영수, "방위산업의 보안 관련 법률 검토 - 형사처벌 법규를 중심으로", 산업보안연구학회지, 제2권, 제2호, pp. 49-90, 2011.

[5] 김정덕, 김건우, 이용덕, "융합보안의 개념 정립과 접근방법", 정보보안학회지, 제19권, 제6호, pp. 68-73, 2009.

[6] 두산백과사전, http://www.doopedia.co.kr 에서 2014년 5월 1일 검색.

[7] 미래창조과학부, "보도자료: 정보통신기술 융합보안 시장 활성화를 위하 첫걸음 내딛어 - 안전한 정보통신기술 융합 발전을 위한 융합보안 시범사업 착수", http://www.misp.go.kr 에서 2014년 5월 1일 검색.

[8] 산업기술보호센터, "소리없는 경제전쟁, 기술유출: 산업스파이 적발통계 인포그래픽", http://www.service4.nis.go.kr 에서 2014년 3월 1일 검색.

[9] 산업통상자원부, '산업융합촉진법', 대한민국정부, 2014.

[10] 안황권, "시큐리티 환경변화에 따른 융합보안의 대두와 물리보안업체의 대응", 정보·보안 논문지, 제11권, 제5호, pp. 31-40, 2011.

[11] 우광제, 송해덕, "DACUM기법을 이용한 방위산업체 정보통신보안실무자 직무분석", 융합보안논문지, 제14권, 제4호, pp. 73-84, 2014.

[12] 이근호, "IT 융합보안에서의 위협요소 분석", 한국융합학회논문지, 제1권, 제1호, pp. 49-55, 2010.

[13] 이창무, "산업보안의 개념적 정의에 관한 고찰". 산업보안연구학회논문지, 제2권, 제1호, pp. 73-90, 2011.

[14] 이창훈, 하옥현, "기밀유출방지를 위한 융합보안 관리체계", 정보·보안 논문지, 제10권, 제4호, pp. 61-67, 2010.

[15] 정병수, 류상일, 김화수, "산업보안의 연구경향 분석 - 학술연구정보서비스(2000년~2011년)를 중심으로", 한국치안행정논문, 제9권, 제2호, pp. 195-215, 2012.

[16] 지식경제용어사전, http://www.terms.naver.com 에서 2014년 5월 1일 검색.

[17] 최경호, 이동휘, 김민수, 김종민, 김귀남, "융합보안 서비스 사이언스를 위한 기상정보 활용모델 연구", 융합보안 논문지, 제13권, 제3호, pp. 79-84, 2013.

[18] 최진묵, 권정옥, "융합보안시장 동향 보고", 삼성SDS저널, 제7권, 제2호, pp. 13-29, 2010.

[19] 하옥현. "산업보안을 위한 융합보안관제시스템에 관한 연구", 정보·보안 논문지, 제9권, 제4호, pp. 1-6, 2009.

[20] 한국민족문화대백과사전, http://www.encykorea.aks.ac.kr 에서 2014년 5월 1일 검색.

[21] 한국산업보안연구학회, '산업보안학', 박영사, 2011.

[22] ASIS, 'Convergence of security risks', ASIS International, Retrieved May 4, 2014 from http://www.asis.org.uk/documents.

[23] K. E. Anderson, "Convergence: A holistic approach to risk management". Network Security, Vol. 2007, No. 5, pp. 4-7, 2007.

[24] E. G. Booz, J. L. Allen, and C. L. Hamilton, 'Convergence of Enterprise Security Organization', The Alliance for Enterprise Security Risk Management, 2005.

[25] B. T. Contos, S. Hunt, and C. Derodeff, 'Physical and logical security convergence: Powered by enterprise security management', Syngress Publishing, 2007.

[26] Deloitte. 'The convergence of physical and information security in the context of enterprise risk management', AERSM, 2007.

[27] J. Fay, 'Contemporary security management', Elsevier, 2010.

[28] A. Jones, "Convergence", Information Security Technical Report, Vol 12, pp. 69-73, 2007.

[29] J. Kang, J. Lee, C. Hwang, and H. Chang, “The study on a convergence security service for manufacturing industries”, Telecommunication Systems, Vol. 52, No. 2, pp. 1389-1397, 2013.
[30] S. Kim and C. S. Leem, “Enterprise security architecture in business convergence environments”, Industrial Management & Data Systems, Vol. 105, No. 7, pp. 919-936, 2005.
[31] S. M. Rahman and S. E. Donahue, “Convergence of corporate and information security”, International Journal of Computer Science and Information Security, Vol. 7, No. 1, pp. 63-68, 2010.
[32] E. E. Schultz, “Risks due to convergence of physical security systems and information technology environments”, Information Security Technical Report, Vol. 12, pp. 80-84, 2007.
[33] D. Slater, ‘Security convergence, Defined’, CSO online, 2005, Retrieved May 4, 2014 from http://www.csoonline.com/article/2118703/security-leadership/security-convergence--defined.html.
[34] D. Tyson, ‘Security convergence: Managing enterprise security risk’, Butterworth-Heinemann, 2007.
[35] H. S. Venter and J. H. P. Eloff, “A taxonomy for information security technology”, Computer & Security, Vol. 22, No. 4, pp. 299-307, 2003.
[36] Wikipedia, “Defense industry”, Retrieved May 4, 2014 from http://en.wikipedia.org/wiki/Defence_Industry.

[저 자 소 개]

우 광 제 (Woo, Kwang Jea)

1990년 육군사관학교 전산학과 학사
2002년 University of Nebraksa 경영학과 석사
2015년 중앙대학교 인적자원개발학과 박사

email : majwoo@yahoo.co.kr