論文

방위산업체의 관리적 보안모델 개선에 관한 연구

나복엽1*, 장 현2**, 류연승3***

A Study on the Improvement of Administrative Security Model of Defense Industry

Bok-Yeop Na1*, Hyun Jang2** and Yeon-Seung Ryu3***

ABSTRACT

Defense companies are special fields that produce high-tech weapons connected directly with national security, and specialized security is essential. Especially, defense companies have military secret and defense technology, so they are operated in a closed manner. However, important information is still being leaked due to advanced and specialized hacking. This security vulnerability is due to the fact that the basic security flaws are not resolved because the appropriate standards for administrative security such as security organization, personnel and budget are not set. Therefore, in this study, we set appropriate standards for large defense companies. As a result, it is desirable that the security organization organize the IT security together with the unified business performance system and direct it to the CEO, and the security personnel and the budget should set the proper standards considering the domestic and overseas security trends and increase gradually.

초 록

방위산업체는 국가안보와 직결된 첨단무기를 생산하는 특수 분야로서, 특화된 보안이 필수적이다. 특히 방위산업체는 군사비밀 및 방위산업기술을 보유하고 있어 폐쇄적으로 운영되고 있지만, 고도화 · 전문화된 해킹으로 인해 여전히 중요정보가 유출되고 있는 실정이다.

이러한 보안 취약성은 보안조직과 인력 및 예산 등 관리적 보안에 대한 적정 기준이 설정되지 않아, 근본적인 문제가 해소되지 않기 때문이다. 따라서 본 연구에서는 방위산업체의 보안 강화를 위해 대기업 방위산업체를 대상으로 조직, 인력 및 예산 측면에서 적정 기준을 설정하였다. 그 결과, 보안조직은 IT보안을 통합하여 일원화된 업무수행 체제를 갖추어 CEO 직속으로 편성하고, 보안인력과 예산은 국내외 보안동향을 고려하여 적정한 기준을 설정한 후 단계적으로 늘려 나가는 것이 바람직한 것으로 분석되었다.

Key Words : Defense companies(방위산업체), Security model(보안모델), Organization(조직), Personnel(인력), Budget(예산)

논문접수: 2018년 6월 12일 논문확정:
*나복엽, 한화지상방산 보안팀 부장
**장 현, 강원지방경찰청 항공대 경감
***류연승, 명지대 컴퓨터공학과 교수
(교신저자 E-mail: ysryu@mju.ac.kr)
http://journal.kadis.or.kr/
ISSN 1738-6144

Ⅰ. 서 론

방위산업은 국가의 안전을 보장하고 국민의 생명과 재산을 보호하기 위한 무기를 생산하는 산업이다. 이러한 방위산업은 민수산업과 달리 주요한 군사비밀과 방위산업기술을 다루는 방위산업체의 특수 분야로서, 국가안보와 관련된 첨단무기를 생산하기 때문에 그 어느 산업보다 특화된 보안이 중요하다. 그러한 보안의 궁극적인 목표는 예산을 투자하여 보안시스템을 구축하고, 보안조직과 인력을 활용하여 정보 보호와 리스크를 관리하는 것이다. 그러므로 보안은 조직, 인력, 예산의 3요소가 잘 들어맞아야 한다.

2016년 군용함정을 제작하는 방위산업체인 한진중공업이 해킹을 당해 군 당국이 군사기밀 유출 여부에 대한 보안사고 조사를 진행했다. 그 결과 북한이 한진중공업을 해킹해 해군 잠수함의 공중점화 기술을 절취한 것으로 드러났다. 최근 북한 신포급 잠수함의 잠수함발사탄도미사일(SLBM) 기술이 급속히 진전한 것을 감안하면, 우리 해군 기술을 도용했을 가능성이 제기된다.(1) 이렇게 방위산업체를 노린 해킹 건수는 2014년-2016년까지 3년간 1천억 건에 달하는 것으로 군은 파악하고 있으며, 한 시간에 4백만 건 꼴이다.(2) 그야말로 국내 방위산업체가 해커의 먹잇감이 되고 있으며, 그 피해는 국가안보를 위협하는 수준에 이른다.

이러한 방위산업체 보안의 근본적인 문제는 보안조직 편성, 인력확보 및 예산투자에 대한 기준 미흡과 CEO의 보안관심 부족에 기인한다는 의견이 꾸준히 제기되었다. 기존 연구에서는 이러한 보안조직, 인력 및 예산을 종합적으로 분석한 자료를 찾아보기 힘들었으며, 특히 방위산업체와 관련된 연구는 거의 없었다. 반면에 일반기업을 대상으로 한 보안전담조직 편성모델(3), 정보보호 인력의 산정 및 양성(4), 정보보호 인력 및 예산의 적정성(5), 기타 보안관리(6)에 대한 각 분야 별 연구 활동은 활발히 진행되고 있었다.

따라서 본 연구에서는 국내외 통계정보, 외국 자료, 기타 문헌조사와 함께 주요 대기업의 방위산업체 보안실장(9명)을 대상으로 심층 인터뷰를 통해 보안조직, 인력 및 예산의 3가지 측면에서 방위산업체의 실상을 진단하고 개선된 보안모델을 제시하고자 한다. 이러한 방위산업체 보안의 문제와 근본 원인을 밝히고 보안조직 편성, 인력 확보 및 예산편성 기준을 제시한다면, 방위산업체의 보안수준을 높이는 동시에 경영 리스크를 감소시키는데 기여할 것으로 예상된다.

Ⅱ. 이론적 근거 및 관련 연구

조직은 어떤 일들을 진행시키거나 특정한 목적을 위해 존재하며, 그 조직을 구성하는 요소는 사람이다.(7) 그러한 목적 달성을 위해 조직은 예산을 투자하여 제품과 서비스를 생산한다. 기업의 경영전략과 비즈니스 지원을 위한 보안조직은 적절한 인력 구성과 예산 투자가

(1) 『경향신문』, "해군 잠수함 미사일 콜드런치, 북에 해킹 당해", 2017. 9. 26.

(2) 『TV조선』, "방위산업체 전산망 북 해커에 뚫렸다", 2016. 9. 23.

(3) 강현식 · 김정덕. "정보보호 전담조직 편성 모델에 관한 연구", 『한국전자거래학회』 20(2), 2015. 5.; 이주형. "항공보안조직 개선에 관한 연구", 『한국 항공경영학회』, 2017.

(4) 박재영. "금융기관 정보보호 업무의 적정 인력 산정에 대한 연구", 『고려대학교 정보보호대학원 석사학위 논문』, 2017. 5.; 방하경. " 공기업의 정보보안 인력의 적정성에 관한 연구", 『고려대학교 정보보호대학원 석사학위 논문』, 2011. 6.; 서경진 외. "정보보안 인력 양성을 위한 탐색적 연구", 『한국정보시스템학회』, 2015. 6.; 우광제. "융합보안전문가의 핵심과업 및 직무역량 요구 분석", 『중앙대학교 박사학위 논문』, 2015. 2.

(5) 임정환 · 김인석. "협동조합형 금융회사의 중앙회를 위한 정보보호 인력 및 예산의 적정성에 관한 연구", 『인터넷방송통신학회』, 2016.

(6) 최광복. "사이버전 대응을 위한 국방 정보보호 환경 분석과 보안관리 모델 연구방향 고찰", 『정보보호학회』 제21권 제6호, 2011. 10.

(7) Royston Greenwood and Danny Miller. "Tackling Design Anew: Getting Back to the Heart of Organizational Theory", *Academy of Management Perspectives*, November 2010, p.78

필수적 요건이다. 이 장에서는 보안조직을 기반으로 보안 인력 및 예산 편성 기준에 대한 근거와 관련 연구를 알아보고자 한다.

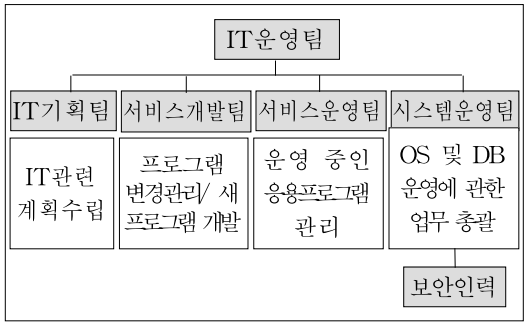
2.1 보안조직 편성의 기준

일반적으로 보안조직을 분류하는 3가지 구성 형태를 알아보고, 방위산업보안업무훈령에 명시된 편성 기준과 상황변수를 기준으로 한 보안조직 편성 모델을 비교해 보고자 한다.

2.1.1 보안조직 구성 형태

보안조직 편성은 크게 3가지로 대별할 수 있다. ① 보안조직이 별도로 존재하지 않고 IT 운영팀에 귀속되어 있는 Type 1, ② 경영스태프 또는 내부통제 조직에 소속되어 있는 Type 2와 ③ CEO(Chief Execution Officer) 직속의 별도 조직으로 편성하여 운영하는 Type 3이다. 보안조직을 구성할 때에는 회사의 규모와 시스템 환경, IT예산, 기업의 관리구조, 관리해야 할 정보자산 등을 고려해야 한다.

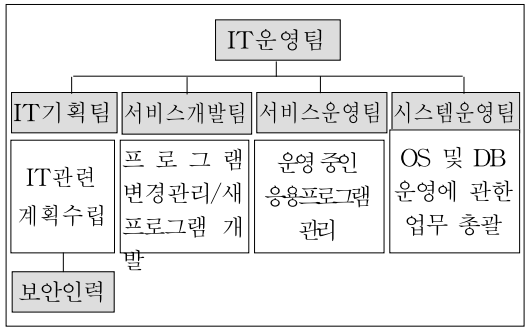
1) Type 1: IT운영팀에 귀속



<그림 1> 보안인력이 시스템운영팀에 귀속된 경우
출처: 양대일, 『정보보호개론』, 2016

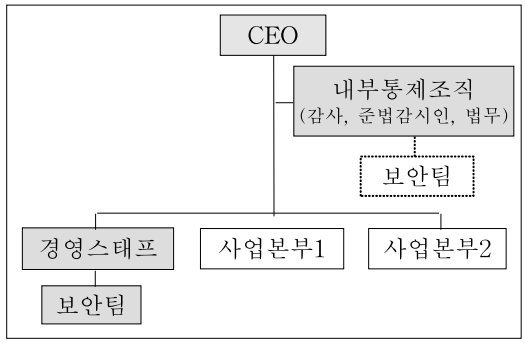
<그림 1>과 같은 회사는 보안인력이 존재하기는 하지만, 가장 보안에 소극적인 형태이다. 즉 보안인력은 방화벽 운영이나 시스템에 대한 보안 패치, PC 보안에 한정된 업무만을 수행한다. 이러한 형태의 보안조직은 관리적인 측면에서 보안을 고려할 수 없을 뿐만 아니라, IT 운영팀 내부에서도 직급이나 영향력이 낮은 경우가 많아 보안정책을 조직 전반에 걸쳐 운영할 만한 힘이 없다.

<그림 2>는 상위 조직만 시스템 운영팀에서 IT 기획팀으로 바뀌었다. 그런데 IT 기획팀은 일반적으로 다른 팀과 커뮤니케이션이 활발하고 IT 운영팀이 전체 사업에 대한 관점을 유지하고 있으므로, 보안인력이 시스템 운영팀의 하위조직에 속한 경우보다는 더 많은 통제력을 갖출 수 있다. 하지만 역시 바람직한 인력구성은 아니다. 왜냐하면 보안인력이 IT 운영팀의 하위조직으로 존재하는 한, 보안 프레임워크를 적용하는 것은 불가능하기 때문이다.(8) 보안인력이 시스템 운영팀이나 IT기획팀에 소속된 Type 1은 종업원 수가 적고 시스템이 많지 않은 중소기업에 적합한 구조이다.



<그림 2> 보안인력이 IT운영팀(IT기획팀)에 귀속된 경우
출처: 양대일, 『정보보호개론』, 2016

2) Type 2: 경영스태프 또는 내부통제 조직에 소속



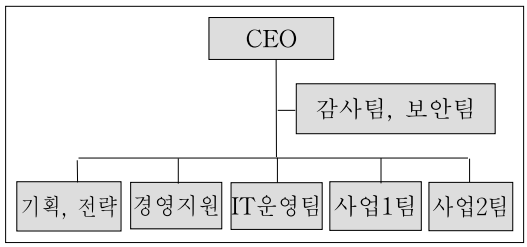
<그림 3> 경영스태프 또는 내부통제조직 산하인 경우
참고: 강은성, 『CxO가 알아야 할 정보보안』, 2015

이 Type은 CFO(Chief Financial Officer)와 같은 경영 스태프나 감사와 같은 내부통제 조직 산하에 정보보호 조직이 있는 구조로서,

(8) 양대일,『정보보안 개론』, 한빛아카데미, 2016. pp.525-526.

도식화하면 <그림 3>과 같다. CFO나 HR(Human Relations)과 같은 경영 스태프는 예산, 회계, 인사 등을 통해 내부관리 임무를 수행하고 감사, 준법감시인, 법무조직은 내부통제 역할을 한다. 이러한 구조의 장점은 전사적으로 힘이 있고, CEO와 일상적으로 소통하는 고위임원이 정보보호 조직을 담당하기 때문에 CEO 직속일 때보다는 못하지만 정보보호 조직에 힘이 실린다는 점이다. 반면에 이러한 조직구조는 IT조직과 정보보호 조직 사이의 협업을 약화시킬 수 있다는 단점이 있다. 아예 처음에 역할과 책임(R&R)을 정할 때부터 이슈가 발생하기도 한다. 이러한 충돌을 정리해야 할 CEO가 소극적으로 대응하면 문제가 악화되고, 협업을 통해 막아야 할 보안위협을 차단하지 못함으로써 회사의 보안위험은 커질 수 있다.(9) 대부분의 대기업 방위산업체는 이러한 조직구조를 유지하고 있다.

3) Type 3: 경영진 직속

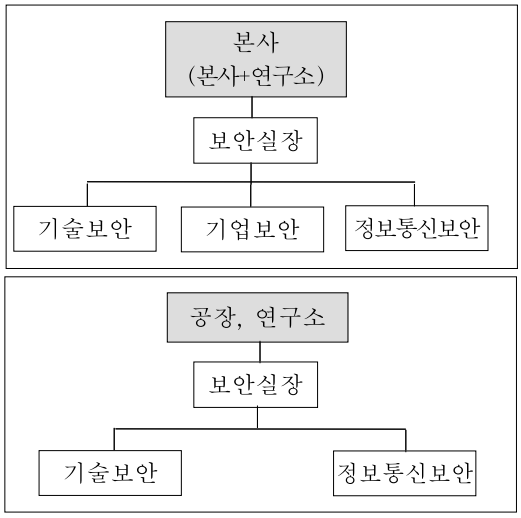


<그림 4> 보안인력이 경영진 직속인 경우
출처: 양대일,『정보보호 개론』, 2016

<그림 4>와 같이 보안팀을 CEO 또는 CSO(Chief Security Officer) 직속의 별도 조직으로 운영하는 것이 가장 바람직하다. 조직에서 이러한 보안팀의 위치는 감사팀과 유사한데, 모든 부서의 보안 사항에 대한 감사가 가능해야 하고, 통제 정책과 운영보안에 적합하게 변경할 수 있도록 회사의 모든 팀과 커뮤니케이션할 수 있어야 한다.(10) 경영진 직속으로 운영하는 Type 3은 CEO의 힘이 실려 보안업무를 수행하기 용이하므로 가장 바람직한 구조이다. 하지만 CEO 입장에서는 보안사고가 발생하면 직접적인 보안책임을 져야 하는 부담이 있다.

(9) 강은성.『 CxO가 알아야 할 정보보안』, 한빛미디어, 2015. pp.46-47.
(10) 양대일,『정보보안 개론』, 한빛아카데미, 2016. pp.526-527

2.1.2 방위산업보안업무훈령 상 보안조직 편성 기준



<그림 5> 최상의 보안수준 요구업체의 보안조직도
출처: 국방부,『방위산업보안업무훈령』, 2017. 2

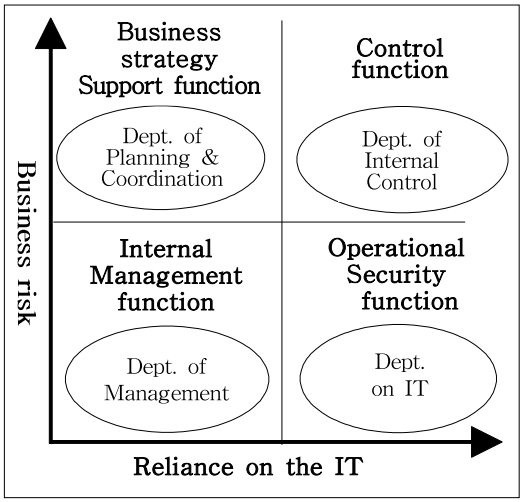
방위산업체는 업체의 규모 및 무기생산 유형에 따라 보안수준 요구가 달라진다. 방위산업보안업무훈령에 명시된 '방위산업체 보안수준 분류기준' 에 따르면, '최상의 보안수준 요구업체' 는 주요 무기를 생산하는 300명 이상의 종업원을 가진 대기업이 여기에 해당된다. 따라서 대기업은 '보안인력 운영 표준모델' 중 <그림 5>의 '최상의 보안수준 요구업체의 보안조직도' 를 기준으로 편성하는 것을 원칙으로 한다. 즉, 본사 또는 본사와 연구소가 같이 있는 경우 보안실장과 보안실무자 3명 등 총 4명으로 구성하고, 공장 또는 연구소는 보안팀장을 포함하여 3명의 보안인력으로 편성한다고 규정되어 있다.(11)

2.1.3 상황변수를 기준으로 한 보안조직 편성 모델

Gartner의 설문조사 결과에 의하면, 실제 정보보호 전담조직은 기업이 설정한 정보보호 전략 방향에 따라 기획 · 조정 부서, 경영지원 부

(11) 국방부, "방위산업보안업무훈령", 국방부훈령 제 2132호, 2018. 2. 13. p.142.

서, 내부통제 부서, IT 부서 등에 편성되어 있는 것으로 분석되었다.(12)



<Figure 6> Informational Security Departmentalization Model
출처: 강현식,『한국전자거래학회지』, 2015

강현식 · 김정덕(13)에 따르면, 정보보호 전담조직 편성은 <그림 6>과 같이 비즈니스 위험도와 IT 의존도로 구성된 상황변수를 기준으로 4가지 모델을 제시하고 있다. ① 비즈니스 위험도가 높고 IT 의존도가 낮은 경우, 비즈니스 전략지원 기능을 우선할 수 있기 때문에 기획 · 조정부서 산하에 편성되는 것이 효율적이다. ② 비즈니스 위험도와 IT 의존도가 모두 높을 때에는 통제기능을 우선할 수 있다. IT와 관련된 사고는 비즈니스에 큰 위협으로 작용되며, 내부통제의 관점에서 다루어져야 한다. 내부통제 부서에는 감사부서, 위험관리부서 및 준법준수 부서 등이 포함된다.(14) ③ 비즈니스 위험도가 낮고 IT 의존도가 높을 경우, IT 운영 지원 기능을 우선할 수 있다. 이러한 경우, 정보보호 전담조직은 IT 부서 산하에 편성될 수 있다. ④ 비즈니스 위험도와 IT 의존도 모두가 낮을 때에는 정보보호의 내부관리 지원 기능이 우선될 수 있다. 이러한 경우, 정보보호 전담조직은 인사, 총무 등 경영지원 부서 산하에 편성될 수 있다.(15)

조직구조는 상황변수에 의해 영향을 받으며 상황변수와 조직구조가 적합할 때 최종적으로 조직의 효율성이 높아질 수 있다.(16) 그러므로 조직을 제대로 평가하기 위해서는 상황변수와 조직구조를 동시에 고려해야 한다. 이러한 상황변수에 기반한 보안조직 편성 모델을 일반화하여 적용하기에는 다소 어려움이 있다.

2.2 보안인력 운영의 기준

방위산업체 보안인력의 편성 기준과 업무수행 역량은 방위산업보안업무훈령에 별도로 명시하고 있다. 여기에서는 국방부의 방위산업보안업무훈령과 금융권의 전자금융감독규정에 명시된 보안인력의 편성기준을 살펴보기로 한다.

2.1.1 방위산업체의 보안인력 편성 기준

1) 방위산업보안업무훈령 상 보안인력 편성 기준

<표 1> 최상의 보안수준 요구업체의 보안인력 모델

구 분	인 원	직 책
본 사	4명	보안실장 기술보안 정보통신 보안 기업보안
공장, 연구소	3명	보안팀장 정보통신 보안 기업보안

출처: 국방부, 『방위산업보안업무훈령』, 2017.2

<표 1>의 보안인력 모델에서와 같이, 방위산업체 본사의 경우 보안업무를 총괄하는 보안실장과 각 분야별 보안실무자인 기술보안, 기업보안 및 정보통신 보안 담당자로 구성되어 있

(12) Gartner. *Determining Whether the CISO Should Report Outside of IT*, 2014.
(13) 강현식 · 김정덕. "정보보호 전담조직 편성 모델에 관한 연구",『한국전자거래학회』 20(2), 2015. 5. pp.167-174.
(14) COSO, *Enterprise Risk Management-Integrated Framework: Executive Summery,* 2004.
(15) 강현식 · 김정덕. "정보보호 전담조직 편성 모델에 관한 연구",『한국전자거래학회』 20(2), 2015. 5. pp170-171.
(16) Forrester. *Security Organization 2.0: Building a Robust Security Organization*, 2010.

다. 공장 또는 연구소는 보안팀장과 실무업무를 담당하고 있는 정보통신보안과 기업보안 담당자로 구성되어 있다.(17) 전술한 <그림 5>에서 보면, 정보통신 보안 담당자는 IT부서에 분임보안담당자로 편성하지 않고, 보안실장(보안팀장) 직속으로 두고 IT보안 업무를 조정 · 통제하도록 명시되어 있다. 이는 IT보안의 중요성과 전문성을 고려한 인력구성이다.

<그림 5> 또는 <표 1>에 언급된 기술보안, 기업보안의 개념은 통상적으로 보안업계에서 사용하는 용어와 다소 상이하다. 이 훈령의 취지는 본사는 '보안실장을 중심으로 실무자 3명이 보안업무를 수행하고, 공장 또는 연구소는 보안팀장을 포함하여 실무자 2명이 각각 수행 한다' 는 것이므로, <그림 5> 또는 <표 1>에 명시된 직책보다는 '사람 수' 에 초점을 맞추어 보안인력을 편성해도 무방하다.

2) 방위산업보안업무훈령 상 보안인력의 업무 수행 역량 기준

방위산업보안업무훈령(제 64조)의 '보안담당관 임명 요건' 에 "군 보안 분야에 2년 이상 근무한 경력이 있거나, 방위산업보안 관련 분야에서 2년 이상 근무한 경력이 있는 자" 로 명시되어 있다. 단순히 군 보안 분야나 방위산업보안 관련 분야에 근무한 경력만을 제시할 뿐, 보안분야의 전문지식이나 실무경력 또는 공인자격증 보유에 관한 언급이 없다.

2.1.2 금융회사의 '전자금융감독규정' 상 보안인력 편성의 기준

금융위원회 고시 전자금융감독규정(18) 제 8조(인력, 조직 및 예산) 2항에 따르면, 금융회사 또는 전자금융업자는 정보기술부문 인력은 총 임직원 수의 100분의 5 이상, 정보보호인력은 정보기술부문 인력의 100분의 5 이상이 되도록 할 것을 명시하고 있다.

이 규정에서 총 임직원 수를 산정하는 기준은 금융회사 등의 상시 종업원으로 하되, 1년 이상 장기 휴직자와 외주(outsourcing) 인력은 제외하고 있다. 또한 정보기술 인력 산정은 "금융회사의 총 임직원 중 내부규정에 따라 IT 기획 · 개발 · 운영 · 정보보호 등 정보기술부문의 업무를 처리하는 사람" 과 "IT업무를 담당하는 상시 종업원 중 해당 금융회사의 IT업무를 적법한 절차에 의해 수행하는 사람으로서, 이 규정 제60조(외부주문 등에 대한 기준) 제1항 제13호에 의한 업무수행인력 관리방안에 따라 관리되고 있는 사람" 으로 정하고 있다.

그리고 정보보호 인력은 "금융회사의 총 임직원 중 내부규정에 따라 정보보호 업무를 처리하는 사람" 과 "정보보호 업무를 담당하는 상시 종업원 중 해당 금융회사의 정보보호 업무를 적법한 절차에 의해 수행하는 사람으로서, 전자금융감독규정 제60조 제1항 제13호에 의한 업무수행인력 관리방안에 따라 관리되고 있는 사람" 이다.

2.3 보안예산 투자 비율의 기준

방위산업체의 보안예산 편성 비율에 대한 명시적 기준은 없다. 이는 업체의 규모, 방위산업물자의 성격, 매출액 및 IT 인프라 등에 따라 투자해야 할 보안예산이 달라 적정한 투자금액을 규정하기는 현실적으로 어려움이 있기 때문이다. 현 보안업무규정(대통령령 제28211호), 방위산업보안업무훈령(국방부 훈령 제2132호) 및 ISMS(정보보호 관리체계)의 104개 통제항목(19)에도 보안예산에 대해 별도로 언급된 내용은 없다. 다만, 전자금융거래법의 하위규정인 전자금융감독규정 제 8조(인력, 조직 및 예산) 2항에 의하면, 금융회사 또는 전자금융업자는 정보보호 예산을 정보기술부문 예산의 100분의 7 이상이 되도록 규정하고 있다.

한편, Gartner의 최근 'IT 주요항목 자료(IT Key Metrics Data)' (20)에 따르면, 기업은 IT보안과 위험관리를 위해서 전체 IT예산 중 평균 5.6%를 투자하고 있다. Gartner의 관점은 기업이 IT보안을 위해 IT예산의 4-7%

(17) 국방부, "방위산업보안업무훈령", 국방부훈령 제 2132호, 2018. 2. 13. p.142.
(18) 금융위원회, "전자금융감독규정", 시행 2016. 10. 5. 금융위원회 고시 제2016-37호.
(19) 한국정보보호심사협의회, 『ISMS 실무가이드』, 인포더북스, 2015. 8. 20. p.434.
(20) Gartner, *IT Key Metrics Data 2015: Key IT Security Measure: Multiyear*, 15 December 2014.

를 집행해야 한다는 입장이다.(21) 이는 우리나라 금융회사의 정보보호 예산비율보다 다소 낮은 편이다.

Ⅲ. 방위산업체 보안의 실상 분석

이번 장에서는 방위산업과 방위산업보안의 특성을 고려하여 보안 조직, 인력 및 예산의 3가지 측면에서 방위산업체의 실상을 분석하고, 관리적 보안에 내재된 근본적인 문제요인을 진단하고자 한다.

3.1 방위산업과 방위산업보안의 특성

국가가 존속하려면 튼튼한 국방력을 갖추는 것이 절대적으로 필요하다. 이를 위해서는 우수한 첨단무기를 생산하는 방위산업의 육성은 필수적 요건이다. 그만큼 방위산업은 국가안보와 밀접한 관계에 있다.(22) 이러한 방위산업을 보호하기 위한 보안은 다른 산업과 달리 다음과 같은 세 가지 특성을 가지고 있다.

3.1.1 국가안보와 직결되는 치명적 리스크 발생

방위산업 무기체계에 사용되는 첨단과학기술은 거의 대부분 C4I(전술지휘자동화체계), 위성통신 및 유무선 통신 등의 네트워크와 연결되어 있어서 해킹공격에 취약하다. 만일 방위산업체가 해킹으로 군사비밀 및 방위산업기술이 경쟁국 또는 적대세력에 유출된다면, 전쟁을 하기 이전에 무력화되는 치명적 리스크가 발생하게 된다. 그만큼 방위산업보안은 국가안보와 직결되어 있기 때문에 보안감사기관에서 매년 정기 감사를 실시하며, 방위산업시설은 국가중요시설로 지정하여 관리하고 있다.

2011년 이후 세계적으로 방위산업체에 대한 해킹공격은 더욱 고도화되고 있다. 방위산업체는 국가안보와도 밀접하게 연관되어 있기 때문에 앞으로도 경쟁국, 적대국의 공격자들이 방위산업체에 대한 공격을 더욱 확대할 것으로 보인다. 국내 방위산업체에 대한 공격은 단순히 산업기밀 유출을 넘어 국가안보에 대한 위험이 야기되는 만큼 더욱 강력한 보안대책과 관리를 통한 예방이 필수적이다.(23)

3.1.2 해킹 방지를 위한 망 분리 의무화

방위사업청에서는 해킹으로 방위산업기술이 유출되자 '방위산업물자 및 방위산업체 지정 규정'을 개정(2016. 12. 30)하고, 방위산업체에게 인터넷 망과 업무 망을 분리하여 해킹을 방지하는 보안대책을 구비하도록 요청하였다. 이에 따라 금년부터 각 방위산업체는 자체적으로 수억 원-수십억 원을 투자하여 물리적 망 분리를 시행하고 있다.

방위사업은 일정한 시설기준과 보안요건을 갖춘 뒤 산업통상자원부 장관으로부터 방위산업체 지정을 받아야만 사업을 영위할 수 있다.(24) 이러한 보안요건은 방위산업체 지정의 근거 사유가 되므로, 미 충족 시에는 방위산업체 지정도 취소될 수밖에 없다(25) 방위사업청의 보안요건을 충족시키기 위해 방위산업체는 물리적 망 분리 이후 망간자료전송 등 새로운 보안시스템 구축 및 개인 별 인터넷 PC를 설치함으로써 보안지원 공수가 종전보다 배로 증가하였다.

3.1.3 방위산업기술보호법 시행에 따른 컴플라이언스 강화

우리나라의 방위산업 수출 증가 및 국내 기술수준의 향상, 방위산업체에 대한 지속적인 해킹 등으로 방위산업기술의 유출 가능성이 급격하게 증가함에 따라 국가의 안전보장 및 국내 방위산업기술 보호를 위하여 방위산업기술보호법(26)을 제정 시행(2016. 6. 30)하고 있다. 이에 따라 <그림 7>과 같이, 방위산업체는 방위산업기술보호법 제2조(정의) 및 제13조(방위산업기술보호체계의 구축운영 등)에 의거

(21) Susan Moore. "Gartner Says Many Organizations Falsely IT Security Spending with Maturity", *Press Release*, December 9, 2016.
(22) 한국방위산업진흥회, "100대 국정과제 속 방위산업을 말하다", 2017. 8. 3.
(23) 안랩 시큐리티대응센터 분석팀, "국내 방위산업체 공격 동향 보고서", 2017. 7. 3. p.38.
(24) 법제처, "방위사업법", 법률 제15051호(제 35조) 국가법령정보센터, 2017. 11. 28.
(25) 대법원, "방위산업물자 지정처분 취소", 2009두12853 판결, 2009.12.29. 선고.
(26) 법제처, "방위산업기술보호법" 법률 제1363호, 국가법령정보센터, 2015, 12. 29.

①보호대상 기술의 식별 및 관리 체계, ②인원통제 및 시설보호체계, ③정보보호 체계를 구축 · 운영하여야 한다. 만약 이러한 보호체계의 구축 · 운영이 부실할 경우, 대상기관장에게 개선 권고, 시정명령을 할 수 있으며(동 법 제13조), 방위산업기술의 유출 및 침해 또는 비밀누설 시 징역형과 벌금을 병과할 수 있다.(동 법 제21조) 그리고 위반자 외에 그 법인에게도 벌금형을 과하는 양벌규정이 있다.(동 법 제23조) 올해부터 방위사업청에서는 모든 방위산업체를 대상으로 방위산업기술 보호체계의 구축 및 운영에 대한 실태조사 후 개선권고 및 시정명령을 할 예정이어서 방위산업체 보안업무 수요는 전례 없이 급증하고 있다.

구 분	보호체계 구축 내용
보호대상 기술의 식별 및 관리체계	- 방위산업기술을 분류 · 식별하는 체계 - 기술 관련 정보를 체계적으로 축적· 관리하는 인적 · 물적 체계
인원통제 및 시설보호 체계	- 기술보호 책임자 임명, 보호구역 설정 및 출입제한을 통한 인원통제 체계 - 보호구역에 대한 불법적 접근 탐지 체계
정보보호 체계	- 암호화 기술을 이용한 보안체계 - 안티 바이러스 소프트웨어 설치 - 방화벽 및 보안관제시스템 설치 - 시스템 · 컴퓨터 등에 대한 외부망 차단 체계

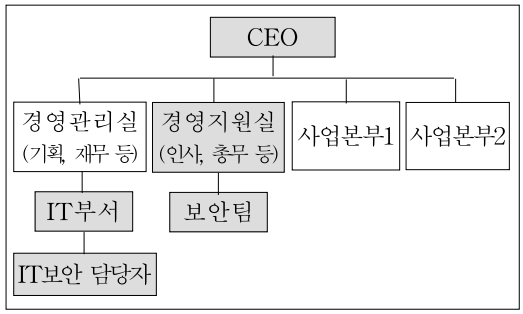
<그림 7> 방위산업 기술보호 체계
출처: 방위산업기술보호법

3.2 방위산업체 보안조직의 편성 현황 및 분석

3.2.1 보안조직의 편성 현황

대기업 방위산업체의 보안조직은 경영스태프 또는 내부통제 조직에 소속된 Type 2가 대부분이지만, 중소기업은 보안팀이 IT 운영팀에 귀속된 Type 1이 주를 이룬다. Type 1은 주로 규모가 작은 중소기업에 적합한 편성이며, 중소기업은 IT부서 내부에 보안 부서를 편성하는 것이 경제적이다.

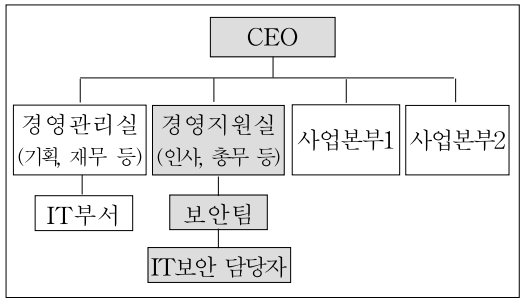
한편, 대기업 방위산업체 중에서도 4개 업체만 IT부서와의 독립적인 보안조직을 유지하고 있을 뿐, 아직도 대부분 업체가 기술보안 부문을 IT부서에 분임하여 임무를 수행하고 있다. 이를 도식화하면 <그림 8>과 같다.



<그림 8> IT보안은 IT부서에, 보안팀은 경영지원실에 귀속

다시 말해서, 보안팀은 인사 · 총무 · 안전환경 등을 관장하는 경영지원조직 소속으로 두고, IT보안은 기획 · 재무 · 회계업무를 수행하는 경영관리조직 산하의 IT부서에 1명의 IT보안담당자를 두어 협업으로 보안업무를 수행하고 있다. 이렇게 보안팀이 IT부서의 협업이 필요한 이원화체제는 기술보안 업무를 수행하기 어렵다.

이를 해결하기 위해서는 <그림 9>와 같이 보안팀에 IT보안담당자를 보직시켜 실질적인 관리 · 물리 · 기술 보안을 통합 운영하도록 개선이 필요하다. 그러나 방위산업체는 수십 년 동안 <그림 8>의 형태로 보안조직을 운영하고 있는 실정이다.



<그림 9> 보안팀에서 관리 · 물리 · 기술보안을 통합

3.2.2 방위산업체 보안조직 분석

기업정보는 정보시스템 등 IT 자산을 기반으로 저장 및 송 · 수신하였기 때문에 전통적으로 정보보호 전담조직은 IT부서 산하에 편성하여 IT 운영지원을 중점으로 정보보호 활동

을 수행하였다. 하지만 정보보호의 중요성이 증대됨에 따라 정보보호 전담조직이 수행해야 할 책임의 범위가 넓어지게 되었다.(27) 그리하여 방위산업 보안업무의 중요성을 자각한 L업체, K업체, H1업체 및 H2업체는 <그림 9>와 같이 보안팀이 관리 · 물리 · 기술보안을 통합 운영하는 형태의 조직 구조를 유지하고 있다. 이 중 L업체와 K업체는 수년 전부터 IT보안 담당자를 보안팀에 편성 운영해 왔으며, H1 · H2업체는 작년에 보안팀이 IT보안까지 통합 수행하도록 조직을 개편하였다. 그 결과 이들 업체는 우수한 보안수준을 유지하고 있으며, L업체와 H업체가 작년도 방위산업 보안감사에서 전국 방위산업체 중 최우수업체로 평가를 받았다.

위 4개 업체를 제외하고 대다수 방위산업체는 보안팀이 관리보안과 물리 보안만을 전담하고, IT부서가 기술보안을 분임 수행하고 있는 실정이다. 외형적으로는 보안팀이 통합된 보안 업무를 수행하고 있는 것처럼 보이나, 실제로는 기술보안이 분리된 '반쪽 보안'을 하고 있다. 이렇게 이원화된 보안업무 수행 체계로는 고도로 전문화된 해킹기술을 방어하기가 어렵다. 한편, 보안실장 9명을 대상으로 <그림 9>의 통합된 보안조직 편성에 관하여 심층 인터뷰를 실시한 결과, 모두 적절하다고 동의하면서 전술한 <그림 5>와 같이 CEO 직속으로 편성해야 한다는 의견을 제시하였다.

십여 년 동안 CEO 직속으로 보안 조직을 운영하던 L업체가 근래 CEO가 교체된 이후 경영스태프 산하 조직으로 개편 되었다. 이는 해킹 리스크가 큰 보안조직을 CEO가 직접 관장하는 것에 대한 책임부담이 크게 작용한 것으로 판단된다. 또한 CEO에 따라 기술보안 분야의 난해한 보안용어로 인하여 소통의 어려움을 느끼고, CSO(Chief Security Officer) 책임 하에 보안조직을 운영 하도록 하는 경우도 많다. 보안의 승패는 CEO의 보안관심에 달려있는 만큼, 리스크가 큰 방위산업체는 CEO 직속으로 편성하는 것이 효율적이다.

3.3 보안인력 구성 현황 및 분석

(27) Forrester. *Security Organization 2.0: Building a Robust Security Organization*, 2010.

보안조직을 효과적으로 구성하기 위해서는 전담 인력을 확보하는 것이 필요하다. 그 규모는 회사의 정보자산, 비즈니스 형태 및 보안이슈에 따라 달라진다. 여기에서는 방위산업체의 보안인력 구성 현황을 토대로 양적 · 질적 측면에서 분석해 보고자 한다.

3.3.1 방위산업체 보안인력 구성 현황

1) 보안인력의 양적 구성 현황

현재 대기업의 보안인력 수는 전술한 '최상의 보안수준 요구업체의 보안인력 모델'인 <표 1>에 미치지 못하는 수준이다. 방위산업 보안업무훈령에는 본사(연구소 포함) 4명, 공장 또는 연구소는 3명으로 편성하도록 명시하고 있다.

<표 2> 대기업 방위산업체의 보안인력 현황

구 분		상위부서	보안인력
A사	**본사**	경영관리본부	**7명**
	연구소	본사 보안팀	2명
	공장	생산본부	4명
B사	**본사+공장**	경영지원 총괄 산하 총무지원실	**6명**
C사	**본사+연구소**	방산사업본부	**4명**
	공장	공장장	5명
D사	본사	인사지원실	3명
	연구소(2개)	본사 보안팀	3-4명
	공장	본사 보안팀	4명
E 사	**본사+공장**	사업기획부	**4명**
	연구소	본사 보안팀	2명
F 사	본사	경영지원실	3명
	연구소	연구소장	4명
	공장	공장장	3명
G 사	본사+연구소 +공장	경영지원실	2명
	연락사무소	인사지원팀	2명
H사	본사+공장	경영지원실	2명
	연구소	안전환경팀	2명
I사	본사	영업본부	2명
	연구소	운영지원팀	2명
	공장	운영지원실	2명

<표 2>는 우리나라의 대표적인 9개 대기업 방위산업체에 대한 보안조직의 상위부서 및 인력 구성을 나타낸 현황이다. <표 2>에서 보듯이 A, B, C 및 E사를 제외한 대다수 방위산업체는 본사(연구소 또는 공장 포함)가 3명 이하로 편성되어 있어서 방위산업보안업무훈령에 명시한 보안모델의 수준에 미치지 못하는 실정이다. 이렇게 보안인력이 부족한 상태에서 전문화된 보안업무를 수행하기는 어렵다. 또한 연구소 또는 공장의 경우, 2명으로 편성된 업체도 있어 CEO의 관심도 및 보안수준을 가늠할 수 있다. 상대적으로 방위산업체 본사 중 가장 많은 7명의 보안인력을 편성한 A사는 전문화된 보안인력이 각 분야 별 임무를 분담하여 수준 높은 보안업무를 수행하고 있다는 평가를 받고 있다.

2) 보안인력의 질적 구성 현황

보안인력의 숫자도 중요하지만, 전문성 있는 보안인력을 확보하는 것이야말로 수준 높은 보안업무를 수행하는데 필수적인 요건이다. 하지만 현재 방위산업체의 보안인력은 질적 측면에서 전문성이 부족한 것으로 파악된다. 보안업무를 총괄하는 보안실장의 경우, IT보안에 대한 전반적인 전문지식을 갖추고 있어야만 관리 · 물리보안과 기술보안의 통합된 업무수행이 가능하다. 최고의 보안수준이 요구되는 방위산업체' 인 대기업의 보안실장들은 거의 대부분 군 정보수사기관에서 장기간 근무한 보안 경력자들이다. 이들 중에는 수십 년 동안 보안 및 정보수사업무 경험이 많아 물리보안 분야의 전문성을 인정받고 있다. 그러나 IT보안 분야의 실무경험이나 전문지식 또는 공인된 자격증을 갖춘 사람은 전무하다. 다만 C사의 보안실장 1명만 정보보호 관련 학위를 갖고 있는 것으로 확인되었다.

3.3.2 국내 금융회사의 정보보호 인력 현황

한국은행의 2016년 금융정보화 추진 현황에 따르면, 국내 156개 금융회사를 대상으로 조사한 결과 <표 3>과 같이 금융기관의 IT인력이 총 임직원 수에서 차지하는 비중은 3.9%로 전년과 같은 수준이었으며, 정보보호 인력이 IT인력에서 차지하는 비중은 9.1%(총 임직원 수 기준 0.4%)를 기록하였다.(28) 이는 '전자금융감독규정' 에 명시된 IT인력 비율(총 임직원 수의 5% 이상)에는 미치지 못하는 3.9% 수준이지만, 규정된 정보보호 인력비율(IT인력의 5% 이상)보다 2배에 가까운 9.1%의 높은 수준을 나타내고 있다. 그만큼 고도화된 해킹의 빈도가 증가되었고, 현실적으로 전자금융감독규정에 명시된 기준보다 훨씬 더 많은 정보보호 인력이 절실히 필요하다는 것을 입증하고 있음을 알 수 있다.

<표 3> 금융기관의 총 임직원 수, IT인력 수, 정보보호 인력 수

연 도	총 임직원	IT인력	정보보호 인력
2012년	240,191명	8,202명 (3.4%)	447명 [5.4%]
2013년	242,545명	8,356명 (3.4%)	574명 [6.9%]
2014년	239,496명	9,152명 (3.8%)	769명 [8.4%]
2015년	235,471명	9,191명 (3.9%)	807명 [8.8%]
2016년	**232,621명**	**9,182명 (3.9%)**	**831명 [9.1%]**

주: ( )내는 총 임직원 수에서 차지하는 비중, [ ]내는 IT인력에서 차지하는 비중
출처: 금융정보화추진협의회

3.3.3 해외 정보보호 인력 현황

2014년 Gartner 자료에 따르면, <그림 10>과 같이 IT 정규직(Full-Time Equivalent) 근무자를 기준으로 IT 인프라 및 애플리케이션 보안과 일반적인 IT 리스크 관리, IT 컴플라이언스, IT 사내 보안 등을 담당하는 인력은 전체 IT 인력 중 7.7%에 해당한다고 보았다.(29) 이러한 정보보호 인력 비중은 전술한 <표 3>의 같은 해 2014년 국내 금융회사의 정보보호 인력 비율(8.4%)보다 낮은 편이다. 하지만 2012년 이후 4.1%, 2013년 5.2%,

(28) 임정환 · 김인석, "협동조합형 금융회사의 중앙회를 위한 정보보호 인력 및 예산의 적정성에 관한 연구" , 『인터넷방송통신학회』, 2016. 3. 5. p.32.
(29) 임정환 외, 2016, P.33

2017년 7.7%로 매년 빠르게 상향곡선을 나타내고 있다.

<그림 10> 전체 IT인력 중 정보보호 인력 비중, 2010-2014
출처: 임정환 외, 인터넷방송통신학회, 2014

3.3.4 보안인력 운영 분석

보안인력의 양적 측면에서 보면, 대다수 방위산업체들이 방위산업보안업무훈령에 명시된 본사 4명, 공장 또는 연구소 3명의 요구수준을 충족하지 못하고 있어 절대적으로 보안인력이 부족한 실정이다. 그나마 대다수 업체의 IT보안 인력은 보안팀이 아닌 IT부서에 소속된 이원화 보안업무 수행체제를 유지하고 있어, 기술보안 분야에 대한 관심이 부족한 편이다. 질적 측면에서도 보안업무에 대한 전문성이 부족한 것으로 나타나는 등 다음과 같이 양적, 질적 측면에서 개선이 필요한 것으로 분석되었다.

1) 보안 인력의 절대 부족

국내 금융회사의 정보보호 인력은 IT인력에서 차지하는 비중(2016년 기준)이 9.1%로서, 전자금융감독규정' 에 명시된 정보보호 인력 비율(IT인력의 7% 이상)을 상회하는 수준이다. 반면에 해외의 정보보호 인력 비중은 7.7%(2014년 기준)로서, 같은 해 국내 금융회사의 정보보호 인력 비율(8.4%)보다 낮은 편이다. 따라서 방위산업보안의 특성을 고려하여 방위산업체 보안인력은 최소한 금융회사 수준에 맞추어서 세부적인 가이드라인을 설정할 필요가 있다. 단순히 본사 4명, 공장 또는 연구소 3명으로 명시할 것이 아니라, 방위산업에 종사하는 총 임직원 수와 정보시스템 운영환경 등을 고려하여 IT인력과 정보보호 인력을 비율로 설정하는 것이 합리적이다. 그러므로 국내외 정보보호 수준 측면에서 볼 때, IT인력 대비 보안인력은 최소한 9% 이상을 확보 하도록 강제적 규정이 필요하다. 만약 이를 준수하지 못할 경우에는 정기 보안감사 때 그 사유와 장기적 보안인력 확보 방안, 보안에 미치는 영향 등에 대한 분석 자료를 제출하도록 의무화해야 한다.

2) 보안업무 수행체제의 이원화

이원화 체제의 보안조직은 불완전한 보안업무를 수행하게 되고, 보안팀이 IT부서장의 협조가 없다면 IT보안에 대한 감사 및 통제가 실제로 제약을 받게 된다. 그 결과 일관된 보안업무 수행이 곤란하다는 것이 큰 단점이다. 보안팀이 IT보안 정책을 수립하거나 IT보안에 대한 자체감사를 할 때에도 일일이 IT부서장의 협조를 받아야 하는 어려움이 있다. IT부서는 회사 전체의 정보보안 시스템을 운영하는 조직이다. 그러므로 IT부서의 팀장은 IT운영을 총괄하며, 반면에 보안팀은 기업의 정보보안을 책임진다.(30) 아직도 이원화 체제로 보안업무를 수행하는 방위산업체는 IT보안 인력을 보안팀에 흡수하여 통합된 보안업무를 수행할 수 있도록 CEO 및 보안관계자의 관심이 요구된다.

3) 보안 인력의 전문성 부족

보안인력의 수를 늘리는 것보다 보안 인력의 질적 전문성을 높이는 일이 더 중요하다. IT기술 분야의 발전 속도는 하루가 다르게 변하고 있어 불과 1년 전의 경험과 지식은 쓸모가 없을 정도 이다. 끊임없이 발전해 가는 보안환경 변화를 따라잡기 위해서 전문지식을 습득하지 않으면 퇴보의 수준에 머물게 된다. 방위산업체 보안실장 중 정보보호 관련 학위를 가진 1명을 제외하고 CISSP, CISA 등 공인 자격증이나 IT 실무경력이 있는 사람이 전무한 것을 볼 때, 방위산업체가 보안 전문 인력 확보 및 양성에 얼마나 무관심했는지를 잘 알 수 있다.

아울러 방위산업체 보안감사 시 보안 담당자 개개인의 전문성 및 업무수행역량 평가에

(30) 김세헌. "기업의 정보보안을 위한 최고 경영자의 역할", CONCERT FORECAST 2013, KAIST, 2013. 3. 20.

더 비중을 두어야 한다. 최초 보안인력을 선발할 때부터 기본적인 자격요건을 강화할 수 있도록 방위산업보안업무훈령의 '보안인력의 자격 기준' 을 보다 더 구체적으로 명시할 필요가 있다. 단순히 '군 보안 분야 또는 방위산업 보안 분야에 2년 이상 근무한 경력자' 를 기준으로 한정할 것이 아니라, 최소한 "정보보안 관련 학위, 일정 기간 (3-5년)의 IT 실무 경력 또는 국내외 정보보호 관련 전문자격증 취득자를 우선 선발 한다" 는 등의 자격요건을 명시하여 전문 인력을 확보해야 한다. 아울러 현업의 보안담당자들도 전문성 제고를 위해 공인 자격증이나 보안 관련 학위를 취득하도록 독려하고, 방위산업 보안감사 때 이를 확인함으로써 적극적인 동기를 유발시켜야 한다.

3.4 보안예산 투자의 실상

3.4.1 방위산업체 보안예산 투자 현황

방위산업체의 보안예산 투자에 대한 통계와 관련된 연구 보고서는 찾아보기 어렵다. 방위산업체가 이러한 투자 현황을 외부로 공개하기를 꺼려하고 있으며, 방위산업 보안 감사기관에서도 보안예산과 관련된 내용은 감사항목에서 제외되어 있어 이에 대한 분석 통계는 없다. 그리하여 정부, 국내 기업 및 금융회사 등 국내 정보보호 동향과 해외의 동향을 참고하여 방위산업체 보안예산의 적정 기준을 분석하고자 한다.

3.4.2 국내 정보보호 예산 현황

1) 정부의 정보보호 예산 현황

<표 4> 연도별 국가 정보보호 예산

연도	정보화 예산	정보보호 예산	정보보호 예산비율
2009	3조1,378억 원	1,757억 원	5.6%
2010	3조2,867억 원	2,695억 원	8.2%
2011	3조2,897억 원	2,035억 원	6.2%
2012	3조2,668억 원	2,633억 원	8.1%
2013	3조3,000억 원	2,400억 원	7.3%
2014	**3조2,500억 원**	**2,600억 원**	**8%**

출처: 기획재정부

<표 4>는 2009년부터 2014년까지 6년간 정부가 정보보호를 위해 투자한 예산 현황이다. 2009년의 정보보호 예산비율은 5.6%였지만, 2014년에는 8%로 증가하였음을 알 수 있다. 또한 2014년의 정보화 예산(3조 2,500억 원)은 전년도(2013년)에 비해 500억 원이 줄어들었음에도 불구하고, 정보보호 예산은 2013년 2,400억 원에서 2014년에는 2,600억 원으로 소폭 증가하였다.

반면 정보보호 예산이 전년도(2013년) 대비 200억 원(8%)이 늘어난 2,600억 원으로 편성된 것은 전년도에 두 차례 발생한 대형 사이버 공격의 영향 때문이다. 정부의 이러한 예산편성 동향을 분석해 보면, 2009년 7.7 디도스 해킹 사고가 발생하자 정보보호 예산을 1,757억 원에서 다음해 2010년에는 2,695억 원으로 대폭 인상하였다. 그러나 2011년에는 정보보호 예산을 2,035억으로 줄였다가 그 해 3.4 디도스 공격과 농협 전산망 해킹사고가 발생하자 2012년에는 2,633억 원으로 상향조정하는 등 임시방편으로 정보보호 예산을 편성하고 있는 실정이다.

2) 국내 기업의 정보보호 예산 현황

2013년 한국인터넷진흥원의 자료에 의하면, 2012년 IT예산 중 정보보호 투자 비중이 5%가 넘는 기업은 영국, 미국이 각각 50%, 41%인 것과 비교해 우리나라는 3%에 불과한 것으로 확인됐다.(31) 반면에 미국의 경우 정보 보호 예산이 IT예산의 9-10% 비율 이지만, 우리나라의 경우에는 1-3% 정도 이다. 게다가 5% 이상 투자한 사업체는 3.1%에 불과하다.(32)

과학기술정보통신부의 '2017년 정보보호 실태조사 결과' 발표에 따르면, 기업과 일반 국민의 정보보호 예방 및 대응활동이 전반적으로 향상되고 정보 보호에 대한 투자도 점진적으로 증가하는 것으로 나타났다. 기업부문 조사 결과에 따르면, <그림 11>과 같이 정보보호 예산

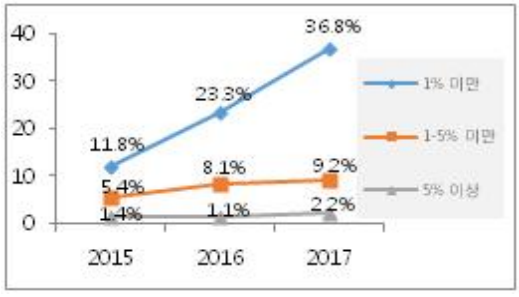
(31) 손경호. "기업 IT예산, 보안비중 여전히 낮다", 『ZDNet Korea』, 2013. 10. 25.

(32) 김세헌. "기업의 정보보안을 위한 최고 경영자의 역할", CONCERT FORECAST 2013, KAIST, 2013. 3. 20.

을 편성한 기업이 전체의 48.1%를 상회하여 전년(2016년) 대비 15.6%p 증가하였다. 이는 2015년 18.6%, 2016년 32.5%, 2017년 48.1%로서 큰 폭으로 증가하고 있음을 알 수 있다.

<그림 11> 정보보호 예산을 편성한 기업 비율(%)
출처: 과학기술정보통신부, 2017

또한 <그림 12>와 같이 IT예산 중 정보보호 예산을 5% 이상 편성한 기업도 전년(1.1%) 대비 2배로 늘어난 2.2%로서, 정보보호 투자는 점차 증가하는 것으로 나타났다.(33)



<그림 12> IT예산 중 정보보호 예산비율(%)
출처: 과학기술정보통신부, 2017

그러나 아직도 IT예산 대비 정보보호 예산의 비율을 5% 이상 편성한 기업이 불과 2.2%의 미미한 수준이고, 5% 미만인 업체도 46%에 달하고 있다.

3) 국내 금융회사의 정보보호 현황

<표 5>는 국내 금융회사가 2012년부터 2016년 간 총 예산 중 IT예산 및 정보보호를 위해 투자한 예산 현황을 나타난 것이다. <표 5>와 같이, 2016년 금융회사의 총 예산은 68조 30억 원이며, 그 중 IT예산은 5조 6,919억 원으로 나타났다. 한편 금융회사의 정보보호 예산은 6,246억 원으로 IT예산 중 11.0%의 비중을 차지하여 금융당국이 제시한 예산 비중(IT예산 대비 정보보호 예산 7% 이상 편성)을 크게 상회하는 것으로 나타났다.(34)

<표 5> 국내 금융회사의 총 예산, 정보보호 예산

연도	총 예산	IT예산	정보보호 예산
2012	63조9,250억 원	5조2,290억 원 (8.2%)	-
2013	58조7,780억 원	4조8,330억 원 (8.2%)	4,430억 원 [9.2%]
2014	63조8,700억 원	5조4,990억 원 (8.6%)	5,997억 원 [10.9%]
2015	66조6,810억 원	5조4,924억 원 (8.2%)	6,146억 원 [11.2%]
2016	**68조 30억 원**	**5조6,919억 원 (8.4%)**	**6,246억 원 [11.0%]**

주: ( )내는 총 예산에서 차지하는 비중,
[ ]내는 IT예산에서 차지하는 비중
출처: 금융정보화추진협의회, 2017

2016년 IT예산은 2012년도의 5조2,290억 원보다 4,629억 원이 증가한 5조6,919억 원을 투자하여 0.2% 소폭 증가하였지만, 상대적으로 정보보호 예산은 2013년 4,430억 원(9.2%)에서 2016년에는 6,246억 원(11.0%)으로 1.8% 늘어났다. 이러한 정보보호 예산은 IT예산의 증가 비율(0.2%)보다 무려 9배나 늘어난 수치이다. 금융회사에서는 금융당국이 제시하는 '전자금융감독규정' 보다 훨씬 높은 수준의 정보보호 예산을 투자하고 있다는 것을 알 수 있다.

3.4.3 해외 정보보호 예산 현황

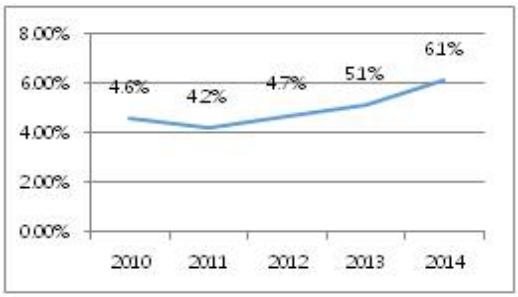
2014년 Gartner 자료에 따르면, <그림 13>에서와 같이 해외에서는 전체 IT투자액 중 정보보호에 대한 투자액은 2011년 이후 계속 증가하는 추세로, 2014년은 전체 IT투자액의 6.1%로 조사되었다.(35)

(33) 과학기술정보통신부, "2017년 정보보호 실태조사 결과", 보도자료, 2018. 1. 9. p.2.

(34) 금융정보화추진협의회, "2016년도 금융 정보화 추진현황", 한국은행, 2017. 7. 10. p.1.

(35) 임정환 외. 2016, P33.

이는 전년도 대비 1% 증가된 수치로서, 정보보호 예산이 빠른 속도로 상승하고 있다는 것을 나타낸다. 그러나 이는 같은 해(2014년) 국내 금융회사의 정보보호 예산 비율인 11%에는 미치지 못하고 있다.



<그림 13> 연도별 전체 IT예산 중 정보보호 예산 비율, 2010 - 2014

출처: 임정환 외, 인터넷방송통신학회, 2016

3.4.4 보안예산 투자 분석

방위산업체의 경우, IT예산 및 정보보호 예산 투자에 대한 기준도 없을 뿐만 아니라 선행연구 사례가 없어 보안예산의 적정 기준을 판단하기가 어려웠다. 다만 국내 정보보호 예산 현황을 볼 때, 국내기업 중 2017년 IT예산 대비 정보보호 예산 비율이 5% 이상인 기업이 2.2%에 불과한 반면, 국내 금융회사는 2016년 정보보호 예산 비율이 11.0%에 이르고 있다. 이는 금융회사가 대형 해킹사고가 발생한 이후 금융당국이 '금융기관 정보보호 예산 가이드라인' 을 제정하여 정보보호 예산 비중을 7% 이상 유지하도록 하는 등 꾸준히 보안대책을 강구한 결과이다. 한편, 해외에서는 보안투자 비율이 2014년 6.1%에 달하고 있어 국내기업(5% 이상 2.2%)보다는 월등히 높지만, 같은 해인 2014년 국내 금융회사 투자비율(11%)보다는 상대적으로 낮은 것으로 나타났다.

한편, 대기업 방위산업체 보안실장들과의 심층 인터뷰에서 각 업체의 정보보호 예산 투자 비율을 확인한 결과 2-3% 수준에 불과하였고, 인터뷰에 응한 모두가 대폭적인 예산투자와 CEO의 관심이 절실히 필요하다는 의견을 제시하였다. 결국 CEO의 보안 관심은 예산의 투자로 나타난다. 이제 보안은 해킹사고가 나면 임시방편으로 정보보호 예산을 증액하는 등 뒷북치기 식 편성을 할 것이 아니라, 방위산업체의 리스크를 감소시키는 '투자' 로 인식해야 한다.

따라서 방위산업체의 보안은 국가안보와 직결되어 리스크가 큰 만큼, 최소한 국내 금융회사의 정보보호 예산 수준에 맞출 수 있도록 IT예산 대비 10% 이상으로 투자 비율을 높여야 한다. 왜냐하면 금융회사는 고객의 재산과 개인정보를 보호하는 차원이지만, 방위산업체는 국가 안보를 위태롭게 할 수 있는 방위산업물자를 생산하므로 보안 사고에 따른 피해는 금융회사보다 훨씬 더 크기 때문이다.

Ⅳ. 방위산업체의 개선된 관리적 보안 모델

이번 장에서는 3장에서 분석한 내용을 토대로 방위산업체가 보안업무를 효율적으로 수행하기 위하여 필요한 보안조직, 인력 및 예산의 3가지 측면에서 관리적 보안모델을 제시하고자 한다.

4.1 조직 측면

보안조직이 어떤 유형이냐에 따라 경영진의 힘을 받는 정도가 달라진다. 보안팀이 CEO 직속으로 편성되면, 아무래도 CEO의 직접 지침을 받아 보안정책 수립이 용이하다. 그러나 2단계 하위조직으로 편성되거나 IT보안을 위임한 이원화 체제의 조직은 상대적으로 그 위상이 약화된다. 무엇보다도 CEO가 보안에 대한 직접적인 관심을 가질 수 있도록 전술한 <그림 4>와 같이 CEO 직속으로 편성해야 한다.

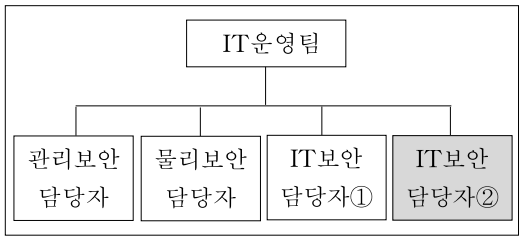
Gartner에 따르면, 보안이 단순히 IT 운영 이슈가 아니라, 비즈니스 리스크 문제로 관리되어야 한다는 업체의 인식이 점차 높아지고 있다.(36) 보안사고가 발생 하면 감사기관으로부터 보안사고 조사를 받는 등 회사에 엄청난 피해가 발생하고, 방위산업 수주에도 직접적인 영향을 미치게 된다. 심지어 방위산업기술보호

(36) Warwick Ashford, Information Security governance maturing, says Gartner", *Computer Weekly*, 21 Jul 2015.

법의 강화로 방위산업체 지정이 취소될 수도 있는 최악의 상황을 맞을 수 있다. 따라서 경영 리스크 관리 차원에서 CEO 직속으로 보안조직을 편성하는 것이 바람직하다.

4.2 인력 측면

방위산업보안업무훈령의 '방위산업체 보안수준별 보안조직 및 인력구성 지침' 에 "방위산업체 대표는 이러한 보안조직 구성 및 인력을 운영하여 보안요건 충족 및 보안수준을 유지하여야 한다." 는 조항이 있으나, 예시에 불과하여 각 업체가 이를 준수하지 않아도 별다른 제재가 없다. 그로 인하여 방위산업체의 보안인력은 절대적으로 부족하여 실제로 보안업무를 수행하기가 어려운 실정이지만, CEO나 CSO는 보안인력 확보 및 양성에 관심이 부족하다. 따라서 최우선적으로 IT보안 담당자를 2명으로 늘리고, 단계적으로 IT 인력 대비 보안인력의 비중을 9% 이상으로 확보해야 한다.



<그림 14> 보안인력의 전문성 제고 및 IT보안 강화

<그림 14>에 도식한 바와 같이, 관리 · 물리보안 담당자는 현재와 같이 각각 1명씩 편성하되, 기존의 1명이 수행해 왔던 IT보안 담당자를 2명으로 늘려야 한다. 기존의 서버, 네트워크, DB 및 애플리케이션 운영을 비롯하여 망 분리 이후 추가 구축된 시스템의 운영보안 업무에 부가하여, 새로 제정 시행하고 있는 방위산업기술보호법의 기술보호체계 업무를 전문성 있게 수행하려면 적어도 2명의 IT보안 담당자가 필요하기 때문이다.

IT보안담당자 ①은 PC, 노트북, 저장장치 등 End Point(최종사용자 단) 보안을 주 임무로 수행하고, 망 분리 관련 운영보안과 각종 로그분석, 모니터링 및 침해사고 발생 시 즉각 대응하는 업무를 수행한다. IT보안담당자 ②는 서버, 네트워크 장비, DB 등 IT 인프라 보안을 주 임무로 하되, 방위산업기술을 보호하기 위한 정보보호체계 보안업무를 수행한다. 작년에 방위산업보안 감사기관에서 IT보안의 중요성을 고려하여 IT보안 배점을 40%에서 60%로 상향 조정한 것도 바로 그런 현실을 반영한 것이다.

아울러 단순히 보안인력의 숫자 확보에 치중할 것이 아니라, 전문성을 강화하는 것이 급선무이다. 특히 보안실장들은 기술보안 분야에 대한 전문지식을 갖출 수 있도록 정보보호 관련 학위를 취득 하거나 <표 6>과 같은 공인자격증을 획득하도록 동기를 부여하고, 통합된 보안업무 수행 역량을 높여야 한다.

<표 6> 국내외 정보보호 관련 자격증 현황

구분	자격증 명칭	주관기관
국내	정보보안기사	KISA(한국정보보호진흥원)
	정보보안 산업기사	
	ISMS(정보보호관리체계) 인증 심사원	
	산업보안 관리사	산업기술보호협회
	디지털 포렌식 전문가	한국포렌식학회
	CPPG(개인정보관리사)	한국CPO포럼
해외	**CISSP**(Certified Information Systems Security Professional)	**(ISC)²**; International Information System Security Certification Consortium
	CCFP(Certified Cyber Forensics Professional)	
	SSCP(System Security Certified Practitioner)	
	CISA(Certified Information Systems Auditor)	**ISACA**; Information Systems Audit and Control Association
	CISM(Certified Information Security Manager)	
	CGEIT(Certified in the Governance of Enterprise IT)	
	CRISC(Certified in Risk and Information Systems Control)	
	EnCE(EnCase Certified Examiner)	

출처: 소프트캠프

국내에서는 KISA(한국정보보호진흥원), 산

업기술보호학회 등에서 시행하는 정보보안 관련 자격증이 있으며, 해외에서는 국제정보시스템 보안자격증 협회인 (ISC)² 와 ISACA(정보시스템감사 통제협회)에서 시행하는 국제공인 자격증이 있다. 이 (ISC)² 는 세계에서 가장 큰 IT보안 조직이며, 여기에서 발행하는 자격증 중에서 CISSP(국제공인 정보시스템 보안전문가)는 전 세계적으로 가장 널리 알려진 자격증이다.

ISACA는 정보 거버넌스, 보안 및 감사 분야에 대한 서비스를 제공하기 위해 설립된 협회이다. ISACA에서 발행하는 CISA(국제공인 정보시스템 감사사)는 세계적으로 인정받는 보안감사 관련 전문자격증이며, CISM(국제공인 정보보안 관리자)은 정보보호 관리자들을 위한 유일한 자격증이다. 이들 국제공인 자격증 중 CISSP, CISA 및 CISM은 국내 금융회사에서 보안인력을 선발할 때 우선적으로 고려하는 매우 유용한 국제공인 자격증이다.

특히 CISSP, CISA, CISM 등 국제공인 자격증은 자격증을 취득한 이후에도 일정한 시간 이상의 CPE(Continual Professional Education; 지속적 전문교육)를 이수하지 않으면 자격증이 취소된다. 이러한 CPE는 보안업무를 수행하는데 필요한 최신 지식과 실력을 유지하기 위한 목적이다. 이는 공인 자격증을 보유하고 있더라도 전문성을 향상을 위해 끊임없이 노력하도록 동기를 유발하는데 도움이 된다.

4.3 예산 측면

방위산업체의 보안예산 편성에 대한 명시적 기준은 없으며, 방위산업체 보안감사 시 감사기관에서 보안예산에 대한 평가를 별도로 하지 않는다. 이와는 달리 금융회사는 전자금융감독규정의 정보보호 예산 편성 기준(IT예산의 7% 이상)을 따르고 있으며, 2016년 현재 11.0%를 상회하고 있다. 해외의 정보보호 예산도 전체 IT 투자액의 6.1%(2014년 기준)에 달하고 있으며, 매년 빠르게 상승하고 있는 것으로 분석되었다.

따라서 방위산업체의 정보보호 예산은 방위산보안의 특성과 해킹 건수의 증가 및 국가안보에 미치는 영향 등을 고려하여 증액하여야 한다. 보안예산의 뒷받침 없이 보안조직을 운영하는 것은 '말 뿐인 보안' 에 불과하다. 방위산업체가 현재 수준의 보안예산을 급격하게 증액하는 것은 현실적으로 어렵다. 따라서 우선 금융당국의 7%를 기준으로 예산편성 가이드라인을 제정하고 난 다음, 향후 방위산업체의 매출액과 보안환경 변화에 맞추어 단계적으로 늘려나가야 한다.

Ⅴ. 결론

5.1 연구 결론

지금까지 살펴본 바와 같이, 금융회사의 '전자금융감독규정' 상 정보보호 인력 편성의 기준은 IT부문 인력의 5% 이상이 되도록 할 것을 명시하고 있다. 하지만 2016년의 경우, 금융회사는 정보보호 인력을 IT인력 대비 9.1%로 유지하고 있어서 실제로 전자금융감독규정의 기준을 훨씬 상회하고 있다. 반면에 방위산업보안업무훈령에는 대기업의 보안인력은 본사 4명, 공장 또는 연구소 3명으로 편성하도록 규정하고 있다. 해외에서는 보안인력의 비중이 2014년 기준으로 IT인력 대비 7.7%로, 국내(8.4%)에 비해 낮다.

한편 보안예산에 대해서는 방위산업보안업무훈령 및 ISMS에도 별도의 언급은 없고, 금융회사의 전자금융감독규정에는 정보보호 예산을 IT부문 예산의 7% 이상을 투자하도록 규정하고 있다. 해외에서는 2014년 IT예산 투자액이 6.1%인데 비해, 국내 금융회사의 2016년도 정보보호 예산 비율(11%)은 이보다 훨씬 낮은 수준이다.

그러므로 방위산업체의 보안인력 및 예산의 기준은 국내 금융회사에 버금가는 수준을 유지해야 한다. 제일 먼저 방위산업체의 보안조직은 IT보안을 통합하여 일원화된 보안업무 수행체제를 갖추어야 한다. 둘째, 보안인력은 IT인력 대비 9% 이상을 유지하도록 방위산업보안업무훈령을 개정 보완하고, 만약 이를 준수하지 못하면 보안감사 때 그 사유를 해명하는 자료를 제출하도록 의무화해야 한다. 셋째, 정보보호 예산은 IT예산의 7% 이상으로 기준을 설정하고, 보안환경 변화에 따라 매년 단계적으로 늘려서 10% 이상으로 유지하도록 하는

것이 바람직한 것으로 분석되었다.

지금까지 방위산업체가 군사비밀 및 방위산업기술을 보유하고 있다는 이유로 보안업무를 폐쇄적으로 운영함에 따라 방위산업체 스스로 보안 수준을 개선하려는 노력이 부족했다는 사실을 부인하기 어렵다. 국가안보와 직결된 기밀을 다루는 방위산업체의 보안은 금융회사보다 훨씬 리스크가 크다. 오히려 리스크가 크면 클수록 예산을 투자하여 보안 경영을 하는 것이 거시적 안목에서 볼 때 훨씬 비용 효과적이다.

보안은 더 이상 조직운영에 소모되는 '비용' 이 아니라 회사의 정보자산 보호와 리스크 감소를 위한 '투자' 라는 인식의 변화가 필요하다. 그동안 보안에 투자하는 것은 '비용' 이라는 인식 때문에 적절한 예산 투자 및 전문화된 보안인력 확충에 인색했던 것도 사실이다. 이제 방위산업기술보호법이 시행된 이후 해킹사고가 발생한 업체는 강력한 제재를 받게 되므로, 보안예산을 투자하지 않을 수 없는 상황이다. 보안사고가 터지고 나서 리스크를 수용할 것인가, 아니면 사전에 리스크를 예방할 것인가의 문제는 오직 CEO의 몫이다. CEO의 보안인식이 변화되지 않으면 방위산업체의 보안수준 향상은 요원하다는 것을 시사하고 있다.

따라서 방위산업체의 현 보안수준을 획기적으로 개선하기 위해서는 정부 당국이 정책적 차원에서 조직, 인력 및 예산 측면의 명확한 기준을 제시하고, 방위산업체 CEO는 보안경영 차원에서 기획관리(조직편성), 경영지원(인력관리) 및 재무관리(예산투자)의 3요소를 조화롭게 운용하는 지혜를 발휘해야 한다. 그것이 방위산업체의 안정된 방위산업무기의 생산을 보장하며, 국가안보에 위험을 초래할 수 있는 군사기밀 및 방위산업기술을 보호하는 현명한 해법이 될 것이다.

5.2 연구의 한계점

본 연구에서는 방위산업보안업무훈령에서 요구하는 '최고의 보안수준 요구업체' 인 대기업을 중심으로 개선된 보안모델을 제시하긴 했지만, 향후에는 재정적으로 열악한 중소기업 보안모델에 대한 지속적인 연구가 필요하다. 또한 방위산업체의 보안모델을 연구함에 있어서 방위산업보안의 특수성과 보안 상 문제로 구체적인 통계 데이터를 구하기 어려웠고, 선행연구 자료들이 많지 않아 보안모델을 검증하는데 한계가 있었다. 아울러 각 방위산업체들의 구체적인 조직 운영 및 보안 취약점들을 공개할 수 없는 제한 사항이 있었음을 밝혀둔다.

참고문헌

1) 강은성. 『CxO가 알아야 할 정보보안』, 한빛미디어, 2015.
2) 강현식 · 김정덕. "정보보호 전담조직 편성 모델에 관한 연구", 『한국전자거래학회』 20(2), 2015. 5
3) 『경향신문』, "해군 잠수함 미사일 콜드런치, 북에 해킹 당해", 2017. 9. 26.
4) 과학기술정보통신부, "2017년 정보보호 실태조사 결과", 2018. 1. 9.
5) 국방부, "방위산업보안업무훈령", 국방부훈령 제2132호, 2018. 2. 13.
6) 금융위원회, "전자금융감독규정", 시행 2016. 10. 5, 금융위원회 고시 제2016-37호.
7) 금융정보화추진협의회, "2016년도 금융 정보화 추진현황", 한국은행, 2017. 7. 10.
8) 김세헌. "기업의 정보보안을 위한 최고 경영자의 역할", CONCERT FORECAST 2013. KAIST, 2013. 3. 20.
9) 박재영. "금융기관 정보보호 업무의 적정인력 산정에 대한 연구", 『고려대학교 정보보호 대학원 석사학위논문』, 2017. 5.
10) 방하경. "공기업의 정보보안 인력의 적정성에 관한 연구", 『고려대학교 정보보호 대학원 석사학위논문』, 2011. 6.
11) 법제처, "방위산업기술보호법" 법률 제1363호, 국가법령정보센터, 2015. 12. 29.
12) 대법원, "방위산업물자 지정 처분취소", 2009두12853 판결, 2009.12.29. 선고.
13) 법제처, "방위사업법", 법률 제15051호, 국가법령정보센터, 2017. 11. 28.
14) 서경진 · 최지은 · 김희웅. "정보보안 인력 양성을 위한 탐색적 연구", 『한국정보시스템학회』, 2015. 6.
15) 소프트캠프(http://blog.softcamp.co.kr), 보안 관련 자격증 소개", (검색일 : 2018, 5, 2.)
16) 손경호. "기업 IT예산, 보안비중 여전히 낮다", 『ZDNet Korea』, 2013.
17) 안랩 시큐리티대응센터 분석팀, "국내 방위

산업체 공격 동향 보고서", 2017.
18) 양대일.『정보보안 개론』, 한빛아카데미, 2016.
19) 우광제. "융합보안전문가의 핵심과업 및 직무 역량 요구 분석",『중앙대학교 박사학위 논문』, 2015. 2.
20) 이주형. "항공보안조직 개선에 관한 연구",『한국항공경영학회』, 2017.
21) 임정환 · 김인석. "협동조합형 금융회사의 중앙회를 위한 정보보호 인력 및 예산의 적정성에 관한 연구",『인터넷방송통신학회』, 2016. 3. 5.
22) 최광복. "사이버전 대응을 위한 국방 정보보호 환경 분석과 보안관리 모델 연구방향 고찰",『정보보호학회』 제21권 제6호, 2011. 10.
23) 한국방위산업진흥회, "100대 국정과제 속 방위산업을 말하다", 2017.
24) 한국정보보호심사협의회,『ISMS 실무가이드』, 인포더북스, 2015. 8. 20.
25)『TV조선』, "방위산업체 전산망 북 해커에 뚫렸다", 2016. 9. 23.
26) COSO, *Enterprise Risk Management – Integrated Framework: Executive Summery,* 2004.
27) Forrester. *Security Organization 2.0: Building a Robust Security Organization*, 2010.
28) Gartner. *Determining Whether the CISO Should Report Outside of IT*, 2014
29) Gartner. *IT Key Metrics Data 2015: Key IT Security Measure: Multiyear*, 15 December 2014.
30) Royston Greenwood and Danny Miller. "Tackling Design Anew: Getting Back to the Heart of Organizational Theory", *Academy of Management Perspectives,* November 2016.
31) Susan Moore. "Gartner Says Many Organizations Falsely IT Security Spending with Maturity", *Press Release*, December 9, 2016.
32) Warwick Ashford. "Information Security governance maturing, says Gartner", *Computer Weekly*, 21 Jul 2015.