융합보안전문가의 핵심과업 요구분석★

- 방위산업체 보안전문가를 중심으로 -

우광제* · 송해덕**

요 약

지식 정보화 사회가 심화되면서 지능화, 첨단화, 복잡화 되어가는 기술 유출에 전략적으로 대응하기 위한 방안으로 융합보안이 대두되고 있다. 융합보안이 실효성을 기하기 위해서는 무엇보다도 융합보안 전문인력의 양성이 필수적이며 이를 위해서는이들 전문인력의 핵심직무에 대한 규명이 선행될 필요가 있다. 따라서 본 논문은 대표적인 융합보안 전문가인 방위산업체 보안전문가를 대상으로 그들의 직무를 규명하고, 직무 수행에 필요한 핵심과업과 교육적 요구를 분석하였다. 연구결과 7개의 책무와 49개의 과업이 도출되었고 핵심과업에 대한 교육적 요구 수준이 분석되었다. 이러한 연구결과는 융합보안전문가의 역량 개발과 학교기관 및 실무교육기관의 융합보안전문가 교육과정 개발에 기여할 것이다.

A need assessment on the key tasks of convergence security specialists

Kwang Jea Woo* · Hae-Deok Song**

ABSTRACT

As the informative society becomes intensified, the rise of the convergence security offers an alternative strategic correspondence to the technology leaks that are becoming more advanced, complex, and intelligent. In order to the convergence security to provide its efficacy, training convergence security specialists is essential. However, research on the subject has yet to be considered sufficient. Thus this research focuses on defense industry security specialists to define the duty and analze critical task as well as drawn and therefore the required academic level of the critical task was examined. These research work contributes to the competence development of convergence security specialists and further enhancement on convergence security training process of academic institutions and job training institutions.

Key words : 융합보안, 방위산업보안, 융합보안전문가, 직무분석, DACUM, 요구부석

접수일(2016년 5월 4일), 게재확정일(2016년 5월 18일)

★ 본 논문은 우광제의 2015년도 박사학위 논문에서 발췌 정리하였음.

* 중앙대학교 인적자원개발학과

** 중앙대학교 인적자원개발학과

1. 서 론

오늘날 기업들이 직면하고 있는 다양한 보안위협의 복잡성과 상호의존성은 조직 전체에서 보안 기능의 융합을 필요로 하고 있다[16]. 특히 지능화, 첨단화, 복잡화 되어가는 기술유출에 전략적으로 대응하기 위한 방안으로 최근 융합보안(Convergence Security)이 지속적으로 강조되고 있다. 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 융합보안 산업으로 변모되고 있다. 최근에는 이에 더해 보안기술이 다른 기술이나 산업과 융합하면서 새로운 보안제품과 서비스가 창출되면서[13] 융합보안의 산업구조는 '보안산업 내 보안영역 간의 통합'과 '다른 산업과의 융합'을 포함하는 두 가지 형태로 발전되고 있다.

이와 같이 융합보안 관련 환경변화에 따라 융합보안의 정의도 조직 내 모든 보안요소의 결합을 의미하는 '통합적 개념'과 보안기술이 다른 산업과 결합하여 새로운 산업을 창출하는 '복합적 개념'을 포함하는 것으로 발전하고 있다.[4]. 실제로 Contos, Hunt 와 Derodeff[20] 그리고 Latimer -Livingston[23]은 통합적 개념에서 융합보안을 IT기술과 도구들이 물리보안에 적용되고 물리보안의 요구에 대해 IT기술이 지원하는 것으로 정의하고 있으며, Tyson[28]은 융합보안을 단순한 물리보안과 정보보안의 통합 수준에서 벗어나 조직의 모든 보안자원을 전사적 차원에서 공식적, 협력적, 전략적으로 통합하는 것으로 정의하고 있다. 복합적 개념의 융합보안은 IT기술이 기존 산업기술과 융·복합되는 과정에서 발생하는 보안위협을 해결하기 위한 새로운 형태의 보안시스템을 의미한다[13].

방위산업 분야는 군사비밀, 산업기술, 방산물자, 핵심기술인력, 국가보안목표시설 등 국가안보와 관련된 다양한 보안요소를 보유하고 있기 때문에 다른 산업분야 보다 더 높은 수준의 보안이 요구된다. 이로 인해 방위산업체들은 보안 전담조직과 보안담당관을 임명하여 전사적 차원에서 제반 보안요소를 보호하기 위한 종합적인 보안대책을 강구하고 있다. 방위산업체의 보안전문가는 방위산업보안업무훈령[2]에 의거해서 방위산업체의 보안대책 수립으로부터 시행과 조정 및 감독까지 전반적인 보안업무를 수행하고 있다. 이러한 맥락에서 방위산업은 융합보안을 적용하고 있는 가장 대표적 산업분야라고 할 수 있다.

융합보안이 그 실효성을 기하기 위해서는 무엇보다도 융합보안 전문인력 양성이 중요하다. Tyson[28]은 기업이 융합보안의 도전에 직면하게 되면서 보안전문가들도 융합보안을 실천하는데 어려움을 겪게 되고, 융합보안 인적자원개발에 대한 요구를 간파하지 못한다면 결국 융합보안은 그 효과가 제대로 발휘되지 못하고 약화된다고 주장하였다. 국내에서도 최근 정부의 융합형 창의인재 육성과 융합보안 시장 활성화 정책이 추진되면서 융합보안 전문인력에 대한 관심이 높아지고 있다. 특히 한국인터넷진흥원의 조사에 따르면 정보보안인력과 물리보안인력을 포함한 지식정보보안인력의 신규 수요가 공급에 비해 2010년에는 1,455명이 부족하고 2018년까지 매년 평균 1,690명이 부족한 것으로 분석되었다[15].

이에 최근 융합보안 전문인력 양성을 위해 국내의 대학 및 대학원과 보안기관에서 융합보안학과를 신설하고 교육과정을 운영하고 있으나 융합보안 전문인력 양성에 대한 교육적 요구를 충분히 반영하지 못하는 실정이다. 융합보안의 교육적 요구를 반영하기 위해서는 무엇보다도 융합보안 전문인력의 직무에 대한 정확한 분석이 선행되어야 한다. 그러나 아직까지 융합보안 전문인력의 직무를 체계적으로 규명한 연구는 찾아보기 어렵다. 기존의 선행연구들은 정보보호 전문인력[3, 19]과 경호경비원[1]에 대한 직무분석 관련 연구들에 그치고 있을 뿐이다. 또한 융합보안 관련 전문인력의 교육적 요구를 보다 의미있게 파악하기 위해서는 경력에 따라 서로 다른 요구를 살펴볼 필요가 있다. 따라서 본 논문은 융합보안전문가의 직무와 핵심과업을 규명하고 이를 바탕으로 교육적 요구를 분석하는 것이다. 이를 위한 연구문제는 다음과 같다.

첫째, 융합보안전문가의 책무와 과업은 무엇인가?

둘째, 핵심과업에 대한 요구는 어떠한가?

셋째, 경력별 핵심과업 요구의 차이는 어떠한가?

2. 이론적 배경

2.1 융합보안과 융합보안전문가

과거의 전통적인 보안은 물리보안과 정보보안으로 구분되어 각각 발전되어 왔다. 그러나 보안환경의 변화와 보안산업의 발전추세에 따라 물리보안과 정보보안의 통합되는 융합보안이 대두되었다. 특히 최근의 융합보안은 물리보안과 정보보안의 단순한 결합보다는 전사적 차원에서 모든 보안요소를 통합하는 활동으로 정의된다. 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.[17]. CSO online에서도 융합보안을 비즈니스 연속성, 재난복구, 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[27].

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[9]. 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 성질을 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. 이러한 방위산업보안은 군사보안과 산업보안의 복합체이면서도 방위산업의 모든 보안요소를 통합하는 융합보안이라고 할 수 있고, 이러한 방위산업체의 보안을 담당하는 전문가는 대표적인 융합보안전문가이다.

2.2 융합보안전문가 인적자원개발

융합보안의 성공을 위해서는 융합보안전문가의 양성이 필수적이다. Tyson[28]이 융합보안 인적자원개발의 중요성을 주장 한 바와 같이 융합보안의 태동과 함께 융합보안 인적자원개발의 필요성이 함께 제기되었다. 최근 국내에서도 정부의 융합형 창의인재 육성과 융합보안 시장 활성화 정책이 추진되면서 융합보안전문가 양성에 대한 관심이 높아졌다.

융합보안의 인적자원개발 측면에서 가장 먼저 나타나고 있는 추세는 대학 및 대학원을 중심으로 한 융합보안 관련 학과들의 신설 또는 개편이다. 경기대학교, 성신여자대학교가 이미 융합보안학과를 개설하였고[5] 중앙대학교에서도 2015년부터 산업보안학과를 신설하여 융합보안을 주요 교과과정에 편성하고 있다[12]. 또한 일반대학원에도 융합보안학과를 신설하고 석·박사 산업공학전공과 정보보안전공으로 구분되는 교육과정을 마련하였다. 명지대학교는 2014년부터 산업대학원에 융합보안학과를 운영하고 있으며 일반대학원에도 보안경영공학과를 신설하여 보안과 경영을 융합하는 교육과정을 개설하였다[6]. 융합보안학과 외에도 여러 대학에 보안 관련 학과가 있으나 대부분 정보보안 관련 학과이고 금융과 같은 특정한 분야에 국한된 학과들이다.

정규 학교기관에서의 이러한 경향과 달리 실무적 보안 전문교육기관에서의 융합보안 인적자원개발 노력은 찾아보기 어렵다. 산업보안 전문교육기관인 한국산업기술보호협회는 산업보안 전문인력 양성 및 교육을 위해서 CSO(Chief Security Officer) 양성과정, 디지털포렌식, 물리보안, 관리보안, 핵심인원 관리, 개인

정보보호, 보안컨설팅, 산업보안내부강사 양성 등의 교육과정을 운영하면서 산업보안관리사 자격제도를 함께 시행하고 있다[14]. 방위산업체의 보안담당관과 보안실무자에 대한 교육은 국방부 산하기관에서 전담하고 있다. 국방부 산하기관에서는 보안실무자의 경력을 기준으로 신규교육과정과 보수교육과정으로 구분하여 보안교육을 시행하고 있다.

그러나 이와 같은 산업보안 측면의 양성 및 실무교육이나 자격제도 만으로는 융합보안전문가를 양성하고 그들의 전문성을 향상시키는데 한계가 있다. 이는 기업 보안환경의 변화와 융합보안 시장의 성장에도 불구하고 융합보안전문가에 대한 인적자원개발 연구와 노력이 부족한 탓이다. 융합보안전문가에 대한 인적자원개발을 위해서는 특히 이들 전문가를 양성하기 위한 체계적인 교육훈련이 요구된다.

2.3 융합보안전문가 직무분석

융합보안전문가의 양성을 위해서는 무엇보다도 변화하는 융합보안환경에서 융합보안전문가들의 핵심직무가 무엇인지를 명확히 분석할 필요가 있다. 그렇지만 융합보안전문가에 대한 국내・외 선행연구를 고찰해 본 결과 직무를 규명한 연구는 찾아보기 어렵다. 국내 연구에서 보안 관련 직무에 대한 연구는 정보보안전문인력[3, 19]의 직무분석 연구가 있었다. 한국직업능력개발원에서 진행된 직무분석에도 보안 관련 직종은 정보보호관리자[3]와 경호경비원[1] 등 2건에 불과하다.

정보보안 전문인력의 직무에 대한 연구 중에서 먼저 미국 오하이오 주립대학의 교육훈련센터(CETE, Center on Education and Trainning for Employment)에서 DACUM(Developing A CurriculUM) 방법을 활용해서 분석한 정보보호전문가의 직무는 16개의 책무와 156개의 과업으로 구성된다. 한편 김기윤과 나현미[3]는 DACUM 워크숍과 최초분석법을 활용해서 정보보호관리자의 직무를 분석하였다. 본 논문에서 정보보호관리자의 직무는 “정보시스템 관리 및 정보자산 관리, 물리적보안, 데이터보안, 소프트웨어보안, 통신보안 등에 대한 보안대책을 수립하고 시행 및 관리하는 것”으로 정의되고 4개의 책무와 13개의 과업이 도출되었다. 두 연구는 DACUM 직무분석을 연구방법으로 활용한 공통점은 있으나 연구대상의 직급이 다르고 직무의 정의가 다르다. 따라서 <표 1>과 같이 직무분석 결과인 책무와 과업이 서로 다르다.

<표 1> 정보보안전문가의 직무

연구자	CETE[19]	김기윤과 나현미[3]
대상	정보보호전문가	정보보호관리자
책무 (과업수)	1. 정보보호정책 시행(11) 2. 보안의식 교육(11) 3. 방화벽시스템 관리(13) 4. 침입탐지시스템 관리(16) 5. 네트워크시스템 관리(8) 6. 컴퓨터시스템 관리(5) 7. 백업시스템 관리(14) 8. 시스템로그 확인(8) 9. 신원확인관리 시행(7) 10. 재난복구계획 개발(10) 11. 물리적보안 시행(10) 12. 보안사고 대응(11) 13. 위기분석 수행(7) 14. 직원관리(5) 15. 관리적업무 수행(12) 16. 전문성 개발(5)	1. 보안정책 수립(2) 2. 위험관리(5) 3. 보안대책 수립(2) 4. 보안대책 관리(4)

한국직업능력개발원[1]에서는 DACUM 직무분석 방법을 활용하여 인원보안 전문인력인 경호경비원의 직무를 규명하였다. 직무분석 결과 경호경비원의 직무는 “고객의 요구를 바탕으로 경호경비 대상의 생명, 신체, 재산(시설 및 정보)을 보호하기 위해 사용 가능한 모든 수단과 방법을 동원하여 위해요인을 사전에 방지, 제거하기 위한 제반활동을 수행하는 것”으로 정의되었다. 경호경비원의 책무는 경호경비상담, 경호경비계획 경호경비실시, 평가 및 분석 등 4개가 도출되었고 책무에 따른 과업은 13개가 도출되었다

한편 방위산업체의 보안전문가 직무는 방위산업보안업무훈령[2]에 명시되어 있다. <표 2>는 보안전문가 직책 중에서 융합보안을 담당하고 있는 보안담당관(실장)과 기업보안담당의 임무이다. 방위산업보안업무훈령에 제시된 보안전문가들의 직책별 임무를 살펴보면 보안전문가가 해야 할 일의 범위나 중요도에 따른 구분이 없이 나열되어 있다. 대체로 보안담당관의 임무들은 통합적 업무가 많고 기업보안담당은 실행적이고 세부적인 업무요소가 대부분이다.

<표 2> 방위산업체 보안전문가 직책별 임무

보안담당관(실장)	기업보안담당
보안업무계획 수립	보안일일결산 확인감독
임직원 보안교육	비밀소유현황 조사
비밀보관소 운용	비밀생산시 보호실태 확인
비밀취급인가 업무	비밀 외주발간시 보안조치
보안감사 및 조치	비밀관련서류 관리실태 점검
보안성검토 조정/감독	폐휴지 처리절차 시행
자체 보안사고 조치	신원조사 대상자 선정/요청
비밀보유업무 총괄	비밀취급인가증 발급 신청
비밀취급인가업무 총괄	비밀취급인가 직위표 유지
비밀지출 및 파기	보안서약서 집행/관리
방산기술보호대책 강구	외래인 방문업무 처리
방산수출간 보안조치	언론취재 촬영업무 처리
방산보안 대외협력활동	항공사진 촬영협조 업무
하도급업체 보안지원	통제구역 보안대책 수립
핵심기술 보안대책 강구	출입증 발급 및 관리
	보안취약지 점검
	외국인 신원조사 업무
	협력업체 보안지도방문
	방산물자 호송간 보안조치

이들 직책별 임무는 방위산업체의 보안조직을 편성하고 보안업무를 정립하는데 활용되어진다. 그러나 임무의 개념과 범위가 직책별로 상이하고 책무와 과업이 명확히 구분되어 있지 않기 때문에 방위산업체의 융합보안전문가의 직무파악을 위해 활용하기에는 제한점이 있다. 따라서 방위산업체의 보안업무 정립을 위해서는 보안담당관의 직무분석을 통해 직책별로 명확한 책무와 과업을 도출할 필요가 있다. 이렇게 도출된 책무와 과업은 보안업무의 기준이 될 뿐만 아니라 보안전문가들의 교육훈련 요구를 분석하는데 자료로 활용될 수 있을 것이다.

2.4 DACUM 직무분석

직무를 분석하는 방법에는 최초분석법, 비교확인법, DACUM기법 등이 있다[7]. 최초분석법은 직무분석 대상과 관련된 자료가 부족하고 그 분야에 많은 지식과 경험을 갖춘 사람이 적을 때 직접 현장을 방문해서 분석을 하는 방법이고, 비교확인법은 기존의 분석된 자료를 토대로 현재의 직무 상태와 비교해 확인하는 방법이다[10]. 이에 비해 DACUM은 교육과정 개발을 의미하는 Developing A CurriculUM의 약자로, 직무를 정확하게 인지하고 있는 현업전문가들이 참여하는 워크숍을 통해 직무를 구성하는 요소와 이에 필요한 지식, 스킬 등을 결정하는 방법이다[25].

이처럼 직무분석에 다양한 방법이 적용 되고 있지만 융합보안 전문인력의 책무와 과업 중심의 교육과정 개발이라는 본 논문의 목적에 비추어 볼 때 DACUM 방법은 커리큘럼개발을 위한 사전 직무분석이라는 점에서 가장 타당한 직무분석 방법이라고 할 수 있다. 또한 국내 학술지 인용색인을 통해 선행연구를 분석한 결과 DACUM을 이용한 직무분석 방법은 현재 국가인적자원개발의 핵심과제로 추진중인 국가직무능력표준(National Competency Standard: NCS) 개발에도 활용되는 등 가장 많이 적용되고 있다[7]. 따라서 융합보안 전문인력 교육과정 개발을 위한 직무분석 방법으로는 DACUM 기법이 가장 적합하다고 볼 수 있다. 직무에 대한 정보를 도출하기 위한 DACUM 직무분석 절차는 요구분석, 직무분석, 과업검증, 훈련과업선정, 표준과업분석, 역량개발의 순으로 진행된다[25].

첫 번째 과정인 요구분석은 직무분석의 왜 필요한지를 파악하는 단계로 구성원들의 훈련을 위한 것인지, 경영관리 또는 생산과정의 변화를 위한 것인지, 기술향상을 위한 것인지, 또는 여러 가지 다양한 요구를 위한 것인지 등을 알아보는 과정이다[25]. 두 번째 과정인 직무분석은 워크숍을 통해서 직무를 구성하는 책무와 과업을 결정하고 같은 DACUM 차트를 개발하는 과정이다[25]. DACUM 워크숍은 직무분석을 체계적으로 진행하기 위해 현업전문가, 퍼실리테이터 등이 참여한 집단적 의사결정 방법이다. 세 번째 과업검증은 DACUM 차트의 일반성을 높이기 위해서 DACUM 워크숍을 통해 도출된 책무와 과업의 적절성을 확인하고 핵심과업이나 교육훈련에 필요한 과업을 선정하기 위해 각 과업에 대한 정보를 획득하는 단계이다[25]. 과업검증 과정을 통해 과업의 타당도, 중요도 및 필요수준, 난이도, 빈도, 현재 수행수준 등의 정보를 수집할 수 있으며 수집되는 정보의 종류는 직무분석의 목적에 따라 달라진다. 과업검증을 위한 자료수집 방법에는 설문조사, 패널 검증, 인터뷰 및 관찰 등이 있는데 이메일을 통한 설문조사가 가장 많이 사용되는 효율적인 방법이다[25].

네 번째는 훈련과업선정으로 과업검증의 결과 얻어진 정보를 바탕으로 훈련에 필요한 과업을 선정하는 과정이다[25]. 일반적으로 훈련과업은 과업의 중요도, 난이도, 빈도에 대한 정보나 필요수준과 현재 수행수준의 차이에 대한 정보를 바탕으로 분석된 과업의 우선순위에 의해서 결정된다. 다섯 번째 표준과업분석 단계에서는 직무분석을 통해서 선정된 과업들의 수행절차, 성과기준, 지식, 스킬, 도구, 안전 고려사항 등이 도출된다. 마지막으로 역량개발은 과업을 수행하는데 필요한 역량을 도출하는 단계이다. 역량개발은 교육과정 설계의 기초자료를 제공하기 위한 것으로 훈련과업과 표준과업분석의 내용을 바탕으로 직무역량을 도출하고 이를 정교화 및 계열화시키는 과정으로 이루어진다.

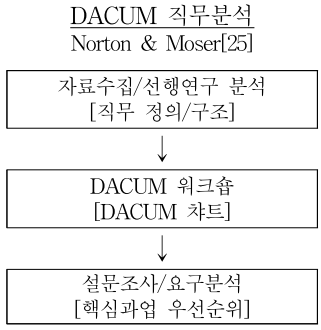
본 논문에서는 융합보안전문가의 핵심과업을 도출하고 교육적 요구수준을 분석하기 위해 세 번째 과정인 과업분석 단계까지 진행하였다.

3. 연구방법

3.1 연구절차

본 논문의 목적은 융합보안전문가의 직무를 체계적으로 분석하여 핵심과업을 식별하고 교육적 요구를 규명하는데 있다. 이러한 연구목적을 달성하기 위해 직무분석과 요구분석 과정을 복합적으로 진행하였다. 핵심과업을 식별하기 위한 직무분석 과정은 DACUM 직무분석 기법[25]을 활용했으며 핵심과업에 대한 요구분석은 설문조사를 통한 우선순위 결정방법[11]을 활용하였다. 이러한 연구절차에 따른 구체적인 연구 방법과 내용은 (그림 1)과 같다

핵심과업 식별을 위한 DACUM 직무분석 과정은 다음과 같다. 첫째, 자료수집과 선행연구 분석 단계로 2014년 3월 10일부터 4월 15일까지 DACUM을 포함한 직무분석 기법에 대한 사전 연구와 융합보안전문가의 직무와 관련된 자료가 수집되었다. 둘째, DACUM 워크숍을 2014년 5월 26일에 8시간 동안 실시하였다. 워크숍은 오리엔테이션을 시작으로 책무와 과업 도출, DACUM 차트 완성의 순으로 진행하였다. 셋째, 설문조사를 통해 과업의 타당도를 검증하고 Borich 요구도 공식과 The Locus For Focus 모델을 활용해서 핵심과업의 우선순위를 결정하였다.



(그림 1)

3.2 연구대상

연구의 대상은 한국방위산업진흥회 산하 92개 정회원사 방위산업체 소속 보안담당관 및 보안실무자들이다. 한국방위산업진흥회와 방위산업보안업무훈령의 방위산업체 보안수준별 보안인력 운용 표준모델[2]을 기초로 주요방위산업체 및 일반방위산업체의 보안업무 인력을 조사한 결과 약 270명의 보안담당관과 보안실무자가 종사하는 것으로 확인되었다. DACUM 직무분석의 과업검증을 위한 설문조사는 한국방위산업진흥회 산하 92개 업체에 종사하는 보안담당자 270명 중에서 보안업무만 전담하는 230명을 대상으로 진행되었다. 설문조사를 위한 샘플 크기는 Krejcie와 Morgan[22]이 제시한 연구대상 크기별 샘플 크기를 근거로 판단하였다.

연구목적을 달성하기 위해 융합보안전문가들의 직무분석과 요구분석이 함께 진행되었으며 이를 위해 DACUM 위원회가 구성되었다. DACUM 위원회는 현업전문가, 코디네이터, 퍼실리테이터를 포함하여 8명으로 구성하였다. 현업전문가는 2011년부터 2014년간 보안우수 방위산업체로 선정된 업체의 보안담당관 및 보안담당관 6명으로 참여하였다. 코디네이터는 방위산업체 보안업무를 지원하는 국방부 산하기관의 보안지원담당자가 수행하였고, 연구자는 퍼실리테이터로서 전반적인 워크숍 진행을 조력하였다.

3.3 조사도구 개발 및 구성

융합보안전문가의 직무에 대한 요구분석은 설문조사를 통한 우선순위 결정방법[11]이 활용되었다. 이를 위한 설문지는 DACUM 핸드북[25]에서 제안한 과업 검증 설문조사 양식을 준용하였다. 설문조사 항목에는 타당도, 중요도 및 필요수준, 현재 수행수준을 포함시켰다. 타당도 문항에 대한 답은 타당한지 아닌지를 'Y' 또는 'N'에 체크하도록 구성하였다. 중요도 및 필요수준과 현재 수행수준에 대한 답은 0점에서 5점까지 Likert식 6단계 척도로 구성하였다. 설문지는 설문의 배경과 취지를 담은 안내문과 함께 역량별 응답지를 포함하여 완성하였다.

설문지는 세 부분으로 구성하였다. 첫 번째 부분은 설문에 대한 안내문이고, 두 번째 부분은 DACUM 워크숍을 통해서 도출된 융합보안전문가의 책무별 과업에 대한 응답지이다. 마지막 부분은 설문대상의 일반적인 특성에 대한 설문지이다. 설문지 구성은 아래 <표 3>과 같다.

<표 3> 설문지 구성

구 분	내 용 및 문 항 수
1. 설문안내	설문 취지 / 용어의 정의 및 설명
2. 직무분석	A. 보안행정 : 9개 문항 B. 비밀관리 : 7개 문항 C. 인원보안 : 8개 문항 D. 시설/장비보안 : 9개 문항 E. 정보통신보안 : 8개 문항 F. 보안교육 : 4개 문항 G. 보안감사/조사 : 5개 문항
3. 일반적 특성	연령, 학력, 직책, 자격증, 경력 등

3.4 설문조사 및 요구분석

설문지는 한국방위산업진흥회를 통해서 2014년 9월 24일 배포되었다. 설문지는 212부가 회수 되었고 불성실하거나 응답내용이 누락된 9부를 제외한 203부가 최종적으로 과업검증에 사용되었다. 설문 응답자의 인구통계학적 특징을 분석해 보면 연령은 40-49세(87명, 42.9%)가 가장 많았고 학력은 학사(129명, 63.5%)가 주를 이루었다. 한편 융합보안전문가 중에서 보안 관련 전공자(20명, 9.9%)와 자격증보유자(72명, 35.5%)가 비전공자(183명, 90.1%)와 미보유자(131명, 64.5%)에 비해 적다는 것은 이들에 대한 교육의 필요성을 재차 확인시켜주었다. 경력별로는 10년 미만이 133명(65.5%), 10년 이상이 70명(34.5%)이었다.

설문조사에서 수집된 자료를 바탕으로 우선 과업의 타당도, 중요도 및 수행수준 등에 대한 설문조사 문항들이 얼마나 안정적으로 일관성 있게 측정되었는지를 확인하기 위해서 신뢰도 분석을 진행하였다. 신뢰도 분석은 문항내적일관성신뢰도 중에서 Cronbach's α에 의한 신뢰도를 산출하여 Nunnally[26], George와 Mallery[21]의 기준에 따라 신뢰도를 판단하였다.

직무분석 결과 도출된 과업들의 타당도를 검증하기 위해서 설문조사 결과를 기초로 내용타당도 비율(CVR: Content Validity Ratio)을 구해 분석하였다. 내용타당도 비율은 설문조사에 응답한 인원과 '타당하다'고 응답한 인원을 내용타당도 비율 공식에 대입해 산출하고 타당도 판단은 응답 인원에 따른 내용타당도 비율 최솟값을 기준으로 결정한다[24]. 본 논문에서는 Lawshe[24]가 제안한 내용타당도 비율 기준에 따라 응답 인원 203명에서의 내용타당도 비율 최솟값인 0.29를 기준으로 책무별 과업의 내용타당도를 판단하였다.

$$\text{내용타당도 비율}(CVR) = \frac{n_e - \frac{N}{2}}{\frac{N}{2}}$$

N : 응답한 인원수
n_e : '타당하다'고 답한 인원수

설문조사 결과 신뢰도와 타당도가 확인된 핵심과업에 대해서 조대연[11]의 우선순위결정 방법에 따라 요구분석을 실시하였다. 먼저 t-검정을 활용해서 필요수준과 현재의 수준의 평균 차이를 비교하여 유의미한 차이가 있는지를 확인하였다. 두 번째는 과업에 대한 우선순위를 확인하기 위해서 Borich 요구도 계산방법이 활용되었고, 마지막으로 The Locus for Focus 모델을 활용해서 핵심과업의 우선순위를 분석하였다.

4. 연구결과

4.1 융합보안전문가의 책무 및 핵심과업

DACUM 워크숍을 통해서 융합보안전문가의 직무

에 대한 정의가 도출되었고, 직무와 과업이 포함된 DACUM 차트가 완성되었다. DACUM 패널들에 의해 합의된 융합보안전문가 직무의 정의는 전사적 차원에서 보안위협을 분석하여 대책을 수립하는 것으로 비밀보안, 인원 보안, 물리 보안, 정보통신 보안 등 제반 보안대책을 통합적으로 실행하는 것이다.

패널들은 융합보안전문가 직무를 수행하기 위한 책무와 과업을 도출하였다. 최초 DACUM 챠트에는 7개의 책무와 50개의 과업이 포함되어 있었으나 설문조사를 통한 과업검증 결과 '보안행정' 책무 중 '보험/손해사정 보안지원하기'과업의 내용타당도비율이 기준치 이하인 0.01로 확인되어 최종 DACUM 챠트는 7개의 책무와 49개의 과업으로 결정되었다.

<표 4> 융합보안전문가 책무 및 과업

책 무	과 업	중요도	현수준
A. 보안행정	A-1. 중장기 보안계획 수립하기	3.85	2.70
	A-2. 연간 보안업무계획 수립하기	4.17	3.17
	A-3. 보안내규 작성(개정) 하기	4.11	3.14
	A-4. 보안일일결산 감독하기	3.32	3.10
	A-5. 보안수준 평가하기	3.44	2.96
	A-6. 회의시 보안조치하기	3.25	2.92
	A-7. 하도급 보안관리하기	3.51	2.84
	A-8. 수출입 보안조치하기	3.25	2.35
B. 비밀관리	B-1. 보호대상 비밀 지정하기	4.23	3.22
	B-2. 비밀 생산 보안조치하기	4.25	3.28
	B-3. 비밀 소유조사/재분류하기	3.81	3.27
	B-4. 비밀 보관/관리실태 확인하기	4.05	3.56
	B-5. 대외발송자료 보안성 검토하기	4.04	3.44
	B-6. 비밀 저장매체 관리하기	4.07	3.65
	B-7. 비밀 안전조치하기	3.93	3.56
C. 인원보안	C-1. 보안관계관 운용하기	3.86	3.28
	C-2. 직원 신원조사업무 처리하기	3.90	3.56
	C-3. 보안서약서 집행/관리하기	3.88	3.83
	C-4. 비밀취급인가업무 처리하기	3.94	3.63
	C-5. 개인정보보호업무 처리하기	3.86	3.45
	C-6. 핵심기술인력 보호하기	3.93	3.06
	C-7. 외국인(직원) 보안관리하기	3.67	2.92
	C-8. 퇴직자 보안조치하기	4.01	3.53
D. 시설/장비보안	D-1. 보호구역(시설) 설정하기	3.97	3.44
	D-2. 시설/장비 보호대책 구축하기	3.85	3.34
	D-3. 출입통제시스템 운용하기	4.18	3.68
	D-4. 출입증 관리하기	3.71	3.46
	D-5. 사진촬영(녹음) 통제하기	3.76	3.34
	D-6. 비인가자 접근/출입 통제하기	4.05	3.64
	D-7. 외래인 출입시 보안조치하기	4.02	3.57
	D-8. 장비 수송시 보안조치하기	3.55	3.05
	D-9. 유사시 안전조치 하기	3.58	3.10
E. 정보통신 보안	E-1. 주전산기(서버) 보안관리하기	4.33	3.20
	E-2. 네트워크 보안관제하기	4.28	3.14
	E-3. 정보보호시스템 보안관제하기	4.24	3.11
	E-4. 정보통신 저장매체 관리하기	4.22	3.57
	E-5. 개인용컴퓨터 보안관리하기	4.23	3.78
	E-6. 사무장비 보안관리하기	3.74	3.23
	E-7. 협력업체 시스템 보안관리하기	3.54	2.60
	E-8. 보안관제결과(해킹) 조치하기	4.11	2.97
F. 보안교육	F-1. 보안교육계획 수립하기	3.89	3.32
	F-2. 주제/대상별 교안 작성하기	3.54	2.94
	F-3. 보안교육 실시하기	3.94	3.38
	F-4. 교육성과 분석하기	3.31	2.77
G. 보안감사/조사	G-1. 보안측정 의뢰/결과 조치하기	3.96	3.38
	G-2. 부서/계열사 보안감사하기	3.71	3.04
	G-3. 정기/수시 보안점검하기	3.92	3.48
	G-4. 보안사고 조사/조치하기	4.14	3.39
	G-5. 중앙보안감사 수검하기	4.20	3.66

설문조사의 항목들이 안정적으로 일관성 있게 과업의 특징들을 측정하고 있는지를 확인하기 위해 Cronbach's α계수를 측정하였다. 과업의 중요도와 현재 수행수준을 측정하는 문항의 Cronbach's α계수가 각각 0.974와 0.978로 확인되었다. 따라서 중요도와 현재 수행수준을 기준으로 핵심과업을 도출하고 요구분석을 위한 신뢰도가 확보되었다.

핵심과업은 내용타당도가 검증된 49개 과업 중에서 중요도 수준이 4.0 이상인 과업을 기준으로 선정하였다. 핵심과업의 중요도 우순선위는 '정보통신보안' 책무의 '주전산기(서버) 보안관리하기' 과업의 중요도 평균값이 4.33으로 가장 높은 것으로 나타났다. 중요도 평균값이 4.0 이상인 핵심과업은 '네트워크 보안관제하기(4.28)', '비밀 생산시 보안조치하기(4.25)', '정보보호시스템 보안관제하기(4.24)', '보호대상 비밀 지정하기(4.23)', '개인용컴퓨터 보안관리하기(4.23)', '정보통신 저장매체 관리하기(4.22)' 등 19개 이다.

4.2 핵심과업 요구분석

융합보안전문가의 핵심과업에 대한 요구분석을 위해서 Borich 요구도 분석, The Locus for Focus 모델 분석결과는 <표 5>와 같다. 융합보안전문가의 핵심과

업에 대한 Borich 요구도 분석결과 가장 높은 요구도는 '네트워크 보안관제하기(4.86)' 과업이 선정 되었다. 핵심과업을 The Locus for Focus 모델을 활용하여 분석한 결과, 전체 핵심과업의 필요수준의 평균은 3.88이고 필요수준과 현재 수행수준의 차이 평균은 0.62이다. 따라서 The Locus for Focus 모델 분석 결과는 핵심과업별로 필요수준의 평균이 3.88보다 높고 수준의 차이 평균도 0.62보다 높으면 'HH'로 표기되었다. 같은 방식으로 필요수준의 평균이 3.88보다 낮고 수준의 차이 평균도 0.62보다 낮으면 'LL'로 표기되었다. 또한 필요수준의 평균이 3.88보다 높고 수준의 차이 평균이 0.62보다 낮으면 'HL'로, 필요수준의 평균이 3.88보다 낮고 수준의 차이 평균이 0.62보다 높으면 'LH'로 표기되었다.

<표 5> 핵심과업 우선순위 분석 결과

과 업	Borich		The Locus for Focus
	요구도	우선순위	
A-1. 중장기 보안계획 수립	4.43	5	LH
A-2. 연간 보안업무계획 수립	4.15	7	HH
A-3. 보안내규 작성(개정)	4.01	9	HH
A-4. 보안일일결산 감독	0.72	48	LL
A-5. 보안수준 평가	1.66	40	LL
A-6. 회의시 보안조치	1.06	46	LL
A-7. 하도급 보안관리	2.37	18	LH
A-8. 수출입 보안조치	2.93	13	LH
B-1. 보호대상 비밀 지정	4.27	6	HH
B-2. 비밀 생산 보안조치	4.15	8	HH
B-3. 비밀 소유조사/재분류	2.06	27	LL
B-4. 비밀 보관/관리실태 확인	2.00	28	HL
B-5. 대외발송자료 보안성검토	2.41	17	HL
B-6. 비밀 저장매체 관리	1.72	36	HL
B-7. 비밀 안전조치	1.45	43	HL
C-1. 보안관계관 운용	2.26	21	LL
C-2. 직원 신원조사업무 처리	1.31	44	HL
C-3. 보안서약서 집행/관리	0.21	49	HL
C-4. 비밀취급인가업무 처리	1.24	45	HL
C-5. 개인정보보호업무 처리	1.58	42	LL
C-6. 핵심기술인력 보호	3.43	10	HH
C-7. 외국인(직원) 보안관리	2.74	14	LH
C-8. 퇴직자 보안조치	1.94	30	HL
D-1. 보호구역(시설) 설정	2.09	26	HL
D-2. 시설/장비 보호대책 구축	1.97	29	LL
D-3. 출입통제시스템 운용	2.10	25	HL
D-4. 출입증 관리	0.93	47	LL
D-5. 사진촬영(녹음) 통제	1.59	41	LL
D-6. 비인가자 접근/출입 통제	1.70	38	HL
D-7. 외래인 출입시 보안조치	1.84	33	HL
D-8. 장비 수송시 보안조치	1.75	35	LL
D-9. 유사시 안전조치	1.69	39	LL
E-1. 주전산기(서버) 관리	4.86	2	HH
E-2. 네트워크 보안관제	4.87	1	HH
E-3. 정보보호시스템 보안관제	4.81	3	HH
E-4. 정보통신 저장매체 관리	2.74	15	HH
E-5. 개인용컴퓨터 보안관리	1.90	32	HL
E-6. 사무장비 보안관리	1.92	31	LL
E-7. 협력업체시스템 보안관리	3.35	11	LH
E-8. 보안관제결과(해킹) 조치	4.70	4	HH
F-1. 보안교육계획 수립	2.24	22	HL
F-2. 주제/대상별 교안 작성	2.15	24	LL
F-3. 보안교육 실시	2.21	23	HL
F-4. 교육성과 분석	1.76	34	LL
G-1. 보안측정 의뢰/결과 조치	2.28	19	HL
G-2. 부서/계열사 보안감사	2.51	16	LH
G-3. 정기/수시 보안점검	1.70	37	HL
G-4. 보안사고 조사/조치	3.12	12	HH
G-5. 중앙보안감사 수검	2.27	20	HL

차순위 핵심과업은 각각의 분석 결과에서만 우선순위가 높은 과업들로 선정된다. Borich 요구도에서만 우선순위가 높은 핵심과업은 '중장기 보안계획 수립하기', '협력업체 시스템 보안관리하기' 등 2개 과업이다. The Locus for Focus 모델에서만 우선순위가 높은 핵심과업은 '보안사고 조사/조치하기', '정보통신 저장매체 관리하기' 등 2개 과업이다. 이와 같이 각각의 분석에서만 우선순위가 높은 4개의 핵심과업은 앞에서 도출된 9개의 최우선순위 핵심과업에 이어 차순위 과업이라고 할 수 있다.

4.3 핵심과업 경력별 요구분석

융합보안전문가 전체를 대상으로 한 핵심과업 요구분석 결과와 경력 10년을 기준으로 경력별 핵심과업 요구분석을 비교한 결과는 <표 6>과 같다. 모든 경력의 융합보안전문가에게 요구되는 최우선순위 핵심과업은 '네트워크 보안관제하기', '주전산기(서버) 보안관리하기', '정보보호시스템 보안관제하기', '보안관제결과(해킹) 조치하기', '보호대상 비밀 지정하기', '연간

보안업무계획 수립하기', '비밀생산 보안조치하기', '보안내규 작성하기' 등 9개 과업이다.

<표 6> 핵심과업 우선순위 분석 결과

과 업	Borich 요구도 (순위) / The Locus for Focus		
	전체	10년 미만	10년 이상
E-2. 네트워크 보안관제	1/HH	1/HH	3/HH
E-1. 주전산기(서버) 보안관리	2/HH	2/HH	4/HH
E-3. 정보보호시스템 보안관제	3/HH	5/HH	1/HH
E-8. 보안관제결과(해킹) 조치	4/HH	3/HH	/HH5
A-1. 중장기 보안계획 수립	5/LH	4/LH	7/HH
B-1. 보호대상 비밀 지정	6/HH	7/HH	6/HH
A-2. 연간 보안업무계획 수립	7/HH	6/HH	9/HH
B-2. 비밀생산 보안조치	8/HH	9/HH	2/HH
A-3. 보안내규 작성	9/HH	8/HH	8/HH
C-6. 핵심기술인력 보호	10/HH	11/HH	10/HH
E-7. 협력업체시스템 관리	11/LH	10/LH	12/LH
G-4. 보안사고 조사/조치	12/HH	12/HH	14/HH
A-8. 수출입 보안조치	13/LH	14/LH	11/LH
C-7. 외국인(직원) 보안관리	14/LH	13/LH	20/LH
E-4. 정보통신 저장매체 관리	15/HH	17/HL	13/HH
G-2. 부서/계열사 보안감사	16/LH	15/LH	24/LL
B-5. 대외발송자료 보안성 검토	17/HL	20/HL	18/HH
A-7. 하도급 보안관리	18/LH	23/LH	15/LH
G-1. 보안측정 의뢰/결과 조치	19/HL	26/HL	17/HH
G-5. 중앙보안감사 수검	20/HL	28/HL	16/HL

5. 결론 및 제언

본 논문은 방위산업체 보안전문가를 대상으로 한 직무분석을 통해 융합보안전문가의 직무를 규명하고 핵심과업을 도출하였다. 또한 융합보안전문가의 핵심과업을 수행하기 위한 직무역량을 도출하고, 융합보안전문가의 경력에 따른 직무역량의 교육적 요구를 확인하여 융합보안전문가 양성을 위한 교육과정 개발에 기여하고자 하였다. 직무분석과 직무역량 모델 개발을 통해 밝혀진 연구결과를 바탕으로 연구의 의미를 정리하면 다음과 같다.

DACUM 워크숍과 설문조사를 통해 도출된 융합보안전문가의 직무들은 기존 연구와 방위산업보안업무훈령[2]에서 제시한 직무보다 직무의 특성을 반영하여 더 구체적이고 현장의 요구를 반영하였다는 점에서 의의가 있다. 방위산업보안업무훈령의 보안담당자 임무는 책무와 과업으로 구분되지 않고 임무목록으로만 나열되어 있었다. 보안실장과 기업보안담당의 직책 구분에 따른 책무와 과업도 상이하였다. 이것은 방위산업보안업무훈령상의 보안담당자 직책별 임무가 실제 방위산업체 현장의 보안전문가들의 직무와 일치하지 않는다는 것을 의미하는 것으로 향후 훈령에 명시된 보안담당관들의 임무에 대한 개정이 필요하다는 것을 시사한다.

융합보안전문가의 핵심과업에 대한 요구분석을 실시한 결과 정보통신보안 과업들에 대한 교육적 요구의 우선순위가 높은 것으로 확인되었다. 이것은 융합보안전문가의 과업에서 정보통신보안이 차지하는 비중이 높고 다른 과업들 보다 더 높은 전문성을 요구한다는 것을 의미한다. 또한 최근의 기업 활동이 대부분 정보통신시스템을 통해 이루어지고 있음을 고려할 때 정보통신보안시스템에 대한 보호가 가장 중요시 되고 있다는 것을 나타낸다.

핵심과업 중 최우선순위에 포함된 다른 과업들은 '보안행정'과 '비밀관리' 책무의 과업인 것으로 나타났다. 이는 전사적 차원에서 보안요소를 통합하고 운영 및 관리하는 융합보안전문가의 직무의 특성이 반영된 결과이다. 융합보안전문가는 기업의 보안대책의 수립에서부터 실행까지 책임을 지고 있기 때문에 '보안행정' 및 '비밀관리'와 관련된 과업들의 중요도 및 교육적 요구가 높다고 볼 수 있다.

핵심과업의 교육적 요구에 대한 경력별 우선순위를 비교한 결과 최우선순위 과업들은 경력에 구분 없이 대부분 일치하였고, 차순위 과업들은 전체 융합보안전문가와 10년 미만 경력자들의 과업이 일치하였다. 그러나 10년 이상 경력자에게만 요구되는 최우선 및 차순위 과업은 '수출입 보안조치', '정보통신 저장매체 관리하기', '대외비 발송 시 보안성 검토하기', '보안측정 의뢰/결과 조치하기'로 확인되었다. 이는 보안업무에 대한 경력여부에 관계없이 융합보안전문가는 다양한 분야에서 교육적 요구가 높다는 사실을 보여준다. 이러한 결과는 융합보안이 조직내 다양한 요소들을 통합하고 다른 영역들과 관계된다는 특성으로 인해 융합보

안전문가에게 외부환경과 조직의 변화를 고려하여 지속적인 교육훈련이 요구된다는 점을 시사한다. 경력과 함께 직급이 높아지고 업무 범위가 넓어지면서 더 전문적이고 높은 수준의 교육이 필요하다는 점에서 차이가 있다고 볼 수 있다.

결론적으로 본 논문을 통해 융합보안전문가의 직무가 규명되었고 핵심과업에 대한 요구분석을 통해 융합보안전문가의 교육적 요구가 확인되었다. 본 논문의 결과는 융합보안전문가를 양성하는 대학 및 대학교의 융합보안학과에서 교육과목을 보완하고, 융합보안 실무교육기관도 경력별 교육과정을 개발하는 기초자료로 활용될 수 있을 것이다. 또한 본 논문을 바탕으로 융합보안전문가의 역량을 도출하여 국가직무능력표준 개발과 역량기반 교육과정 개발까지 발전시킬 수 있을 것이다.

참고문헌

[1] 강경종, 김두현, 공배완, 연규일, 이민용, 백봉현. (2000). 경호경비원 직무분석. 서울: 한국직업능력개발원.

[2] 국방부. (2012). 방위산업보안업무훈령. 대한민국정부

[3] 김기윤, 나현미. (2000). 정보보호관리자에 대한 직무분석. 통신정보학회논문지, 10(3), 63-74.

[4] 김정덕, 김건우, 이용덕. (2009). 융합보안의 개념정립과 접근방법. 정보보안학회지, 19(6). 68-73.

[5] 대학알리미. (2014). http://www.academyinfo.go.kr/ 에서 2014년 5월 1일 검색.

[6] 명지대학교. 융합보안학과 http://www.gss.mju.ac.kr 에서 2014년 5월 1일 검색.

[7] 박용호, 조대연, 김벼리, 노유경, 왕몽, 정희정, 홍순현. (2011). DACUM법을 이용한 초등학교 방과후학교 강사 직무분석. HRD연구, 13(1), 163-186.

[8] 산업통산자원부. (2014). 산업융합촉진법. 대한민국정부.

[9] 우광제, 송해덕. (2014). DACUM기법을 이용한 방위산업체 정보통신보안실무자 직무분석. 융합보안논문지, 14(4), 73-84.

[10] 장수용. (2007). 직무분석 이렇게 한다. Job Analysis. 서울: SBC 전략기업컨설팅.

[11] 조대연. (2009). 설문조사를 통한 요구분석에서 우선순위결정 방안 탐색. 교육학연구. 교육문제연구, 35, 165-187.

[12] 중앙대학교. (2014). 산업보안학과. http://www.cau.ac.kr 에서 2014년 10월 8일 검색.

[13] 최진묵, 권정옥. (2010). 융합보안시장 동향 보고. 삼성SDS저널, 7(2). 13-29.

[14] 한국산업기술보호협회. (2014). 산업보안교육. http://www.kaits.or.kr 에서 2014년 10월 10일 검색.

[15] 한국정보보호학회. (2010). 지식정보보안 분야 인력현황 및 중장기 인력수급 정망 분석. 서울: 한국인터넷진흥원

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

[17] Booz, E. G., Allen, J. L., & Hamilton, C. L. (2005). Convergence of Enterprise Security Organization. Alexandria, VA: The Alliance for Enterprise Security Risk Management.

[18] Brannick, M. T., Levine, E. L., & Morgeson, F. P. (2007). Job and work analysis: Methods, research, and application for human resource management(2nd ed.). Thousand Oaks, CA: SAGE.

[19] CETE(Center on Education and Training for Employment). (2006). DACUM research chart for information security specialist. Columbus, OH: The Ohio State University.

[20] Contos, B. T., Hunt, S., & Derodeff, C. (2007). Physical and logical security convergence: Powered by enterprise security management. Maryland Heights, MO: Syngress Publishing.

[21] George, D., & Mallery, P. (2003). SPSS for Windows step by step: A simple guide and reference. 11.0 update (4th Ed.). Boston MA: Allyn & Bacon.

[22] Krejcie, R. V., & Morgan, D. W. (1970). Determing sample size for research activities. Education

al and Psychological Measurement, 30, 607-610.
[23] Latimer-Livingston, N. S. (2007). Let's get physical: What clients are asking about the integration of physical and logical(IT) security. Retrieved April 8, 2014 from http://www.gartner.com/analyst/14279.
[24] Lawshe, C. H. (1975). A quantitative approach to content validity. Personnel Psychology, 28(4), 563-575.
[25] Norton, R. E., & Moser, J. (2008). DACUM Handbook(3rd ed.). Columbus, OH: Center of Education and Training for Employment, The Ohio State University.
[26] Nunnally, J. C. (1978). Psychometric theory (2nd Ed.). New York, NY: McGraw-Hill.
[27] Slater, D. (2005). Security convergence, Defined. CSO online. Retrieved May 4, 2014 from http://www.csoonline.com/article/2118703/security-leadership/security-convergence--defined.html.
[28] Tyson, D. (2011). Security convergence: Managing enterprise security risk. Burlington, MA: Butterworth-Heinemann.

[저 자 소 개]

우 광 제 (Kwang Jea Woo)

1990년 육군사관학교 전산학과 학사
2002년 University of Nebraksa 경영정보학 석사
2015년 현재 중앙대학교 인적자원개발학과 박사
email : kwangjwoo@gmail.com

송 해 덕 (Hae-Deok Song)

1992년 서울교육대학교 교육학과 학사
1996년 서울대학교 교육공학 석사
2004년 Penn State University 교육공학 박사

email : hsong@cau.ac.kr