DACUM 기법을 이용한 방위산업체 정보통신보안실무자 직무분석

우광제* · 송해덕**

요 약

지식 정보화 사회가 심화되면서 정보보호에 대한 중요성이 날로 높아지고 있다. 최근 들어 개인정보와 핵심 산업기술 유출 사고가 늘어나면서 모든 산업분야는 보안대책을 강구하는데 안간힘을 쓰고 있다. 특히 방위산업은 국가 안전보장에 필요한 국방력을 구축하는 분야이므로 일반 산업분야보다 더 높은 수준의 보안대책이 요구된다. 방위산업체는 방위산업보안업무훈령에 따라 업체별 규모와 여건에 맞게 보안조직을 편성하고 보안실무자를 임명·운영하고 있다. 정보통신의 발달로 대부분의 핵심정보와 기술이 정보통신 시스템이나 저장매체에 기록·관리되고 있는 환경 속에서 정보통신보안실무자의 임무와 역할이 매우 중요하다. 그럼에도 방위산업체 정보통신보안실무자들의 직무에 대한 체계적인 분석과 그들의 전문성 향상을 위한 교육과정 개발이 부족한 실정이다. 이에 본 연구에서는 대표적인 직무분석 기법인 DACUM을 활용해서 정보통신보안실무자들의 책무와 과업을 도출하였고, 설문조사를 통해서 도출된 과업에 대한 타당도와 신뢰도를 검증하였다. 본 연구의 결과는 방위산업체 정보통신보안 업무의 발전에 기여하고 관련 규정의 개정 및 교육과정 개발을 위한 기초자료로 활용될 수 있을 것이다.

Job Analysis for IT Security Workers in Defense Industry through DACUM Process

Kwang Jea Woo* · Hae-Deok Song**

ABSTRACT

As the society turns into more of an information an technology centric society, the importance of information security is being increased these days. Recently, as the number of leaking accidents of personal information and valuable industrial technology is on the rise, every field of industry endeavors to come up with a security solution. In particular, since defense industry is a field where it establishes national defense power that is essential of national security, it requires higher standards of security solutions than any other ordinary fields of industry. According to Defense Industry Security Work Instructions, defense industry firms from security organizations and employ a security worker corresponding to the firm's scale and conditions. In an environment where essential information and technology are stored and managed in information and communication system or storing media, the duty and role of IT security workers are crucial. However, there is a shortage of systematic analysis on the work of IT security workers and development of curriculum to enhance their professionalism. Thus DACUM process, a job analysis technique, was used to identify IT Security workers' duties and responsibilities and verify the validity and credibility of the deducted results from the survey. The findings of this study will help in development of IT security duty in defense industry and can be used as baseline data for the development of curriculum and amendments of related regulations.

Key words : 방위산업, 정보통신보안, 융합보안, 직무분석, DACUM

접수일(2014년 5월 30일), 수정일(1차: 2014년 6월 15일), 게재확정일(2014년 6월 16일)

* 중앙대학교 인적자원개발학과
** 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 늘어나는 경제·금융 스파이가 현재를 특징지을 것이다."라고 예측한바 있다. 이러한 예측은 오늘날 산업분야에 있어서 보안의 중요성을 일깨우는 말이라 할 수 있으며 방위산업 분야에서도 다르지 않다[6]. 우리나라의 방위산업은 2006년 방위사업청 개청 당시 2억 5,320만 달러 수준이었던 수출액이 2013년에는 13.5배나 증가한 34억 1,580만 달러를 기록하고 있다[12]. 산업분야도 총기· 탄약으로 시작해 이제는 항공기와 함정 등 첨단 산업기술을 요하는 분야가 대부분을 차지하게 됐다. 방위산업 규모의 성장과 기술력의 발전은 핵심 산업기술 유출 위험의 증가로 이어지고 있다. 이러한 상황 속에서 국가의 안전보장과 직결되는 방위산업 분야에서는 일반산업보다 더 높은 수준의 보안대책이 요구된다.

핵심 산업기술을 보호하기 위한 기업들의 보안대책 강구에도 불구하고, 첨단기술을 해외로 불법 유출하다 적발된 건수가 지난해 49건을 포함해서 2009년부터 5년간 209건으로 집계됐다[1]. 그 중에서도 중소기업의 첨단기술 유출이 70% 이상을 차지했고 유출된 분야도 과거 전자·정보통신분야에서 방위산업, 전략물자 등으로 확대되고 있다. 기술 유출 주체는 전직 직원이 60.8%, 현직 직원이 19.6%로 전·현직 직원이 대부분이었지만, 협력업체도 9.6%로 비중이 높아졌다. 기술 유출의 원인은 대부분 금전적인 유혹과 개인 영리를 위한(80%) 것이었지만 인사와 처우에 대한 불만(15%) 때문인 경우도 있었다. 최근 주요 기술 유출 사례를 살펴보면 중국인 직원에 의한 국내 유기발광다이오드 기술의 중국 유출 기도, 수백억 원대 포탄 제조 설비·기술의 미얀마 불법 유출 기도 등이 있다[1].

정보통신기술의 발달은 기업의 성장에 핵심적 역할을 하고 있는 반면, 경쟁 국가 또는 기업의 정보유출 위협도 점점 증가하고 있다. 2011년 4월 현대캐피탈 정보 유출과 농협 전산망 마비 사건, 2013년 3월 정부기관 사이버테러, 그리고 올해 1월 신용카드사 개인정보 유출 등 정보통신과 관련된 보안사고는 국가시스템의 마비는 물론이고 기업에도 막대한 피해를 입게 했다. 국가 안보산업인 방위산업도 무기 생산부터 판매까지 모든 기업 활동이 정보통신 시설과 기술을 기반으로 이루어지고 있고 핵심기술과 비밀도 정보통신 매체에 보관된다. 따라서 방위산업의 핵심 산업기술 보호를 위해서는 정보통신 분야에 대한 보안대책이 강구되어야 하고, 정보통신 보안을 전담하는 부서 편성과 실무자의 전문성 확보가 필수적이다.

방위산업체는 방위산업보안업무훈령에 따라 정보통신보안실무자를 포함한 보안 전문인력을 운용하고 있고 일반기업체에서도 정보통신 보안의 중요성을 인식하고 정보보호 전문인력을 운용하고 있다. 체계적인 정보통신 보안업무 수행을 위해서는 업무실무자의 책무와 과업을 정립하고 이를 바탕으로 역량을 개발해 전문성을 확보하는 것이 중요하다. 방위산업체 정보통신보안실무자의 직무는 방위산업보안업무훈령에 명시되어 있고 전문성 확보를 위한 소집교육은 매년 시행되고 있다. 그러나 방위산업보안업무훈령에 명시된 직무는 책무와 과업의 구분이 모호하고 실제 방위산업체에서 이루어지고 있는 과업이 누락되어 있으며, 그 결과 보안실무자를 위한 체계적인 교육과정 개발도 이루어지지 않고 있다. 따라서 본 연구의 목적은 방위산업체 정보통신보안실무자의 직무를 체계적으로 분석하여 그들의 책무와 과업을 정립하는데 있다. 더 나아가 직무분석 결과는 방위산업보안업무훈령의 개정과 핵심 역량을 기반으로 하는 교육훈련 과정의 개발에 기초자료로 활용될 수 있을 것이다.

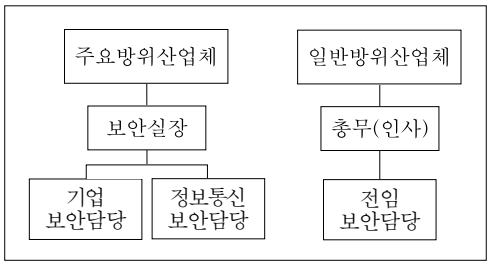
2. 이론적 배경

2.1 방위산업체 보안실무자

일반기업체와 달리 방위산업체는 방위사업법과 관련 법령에 의거해서 방산물자의 안정적인 생산을 위해 일정한 수준의 시설기준과 보안요건을 갖추어야 한다[2]. 방위산업체는 군의 핵심 전투장비를 생산하는 주요방위산업체와 그 외 방산물자를 생산하는 일반방위산업체로 구분되며 업체별로 생산하는 장비와 물자의 중요도, 생산규모 등에 따라 요구 되어지는 보안수준에 맞는 보안요건을 갖추어야 한다[3]. 방위산업체 보

안의 전반적인 책임은 업체 대표에게 있으며 업체 대표는 보안업무를 종합 관장하는 보안전담 부서를 설치하거나 보안담당관을 임명해야 한다[3]. 주요방위산업체들은 이러한 법령에 따라 대부분 보안전담 부서를 두고 있으며 일반방위산업체는 인사 또는 총무부서에 전임보안담당관을 임명해 운영하고 있다.

주요방위산업체 보안전담 부서에 편성되어 있는 보안담당관은 수행하는 임무에 따라 보안실장, 기업보안담당, 정보통신보안담당으로 구분되어 진다[3]. 보안실장은 업체의 보안업무를 총괄 관장하며 기업보안담당과 정보통신보안담당을 관리 감독한다. 기업보안담당은 보안실장을 보좌해 인원보안, 문서보안, 시설보안, 기업보안 등 실무를 담당한다. 정보통신보안담당은 정보보호시스템 운용, 네트워크 보안관리, 정보통신매체 보안성 검토 등 방위산업체의 정보보호와 관련된 업무를 수행한다. 보안전담 부서가 없는 일반방위산업체에서는 전담보안담당관이 업체의 보안관 관련된 모든 업무를 담당하고 있다. 방위산업체별 보안전담 부서 편성과 보안실무자 운영 표준 모델은 (그림 1)과 같다.



(그림 1) 보안실무자 운영 표준 모델[3]

방위산업보안업무훈령에는 방위산업체 보안실무자들의 직책별 임무가 제시되어 있다. 이 훈령에 제시된 직책별 임무를 살펴보면 보안실무자가 해야 할 책무와 과업이 구분되어 있지 않고 두 가지가 혼재되어 있다. 예를 들어 보안실장의 임무 중에서 첫 번째로 기술되어 있는 '보안내규, 보안활동계획 등 보안업무 수행에 관한 세부 계획 작성 및 시행에 대한 조정·감독' 항목은 책무와 과업이 함께 포함되어 있다. 특히 아래 <표 1> 에 명시된 정보통신보안담당의 임무 중에서도 '정보보호시스템 운용 및 보안관리' 또는 '정보시스템(네트워크) 보안대책' 등은 책무와 과업을 어느 정도 구분하여 명시하고 있지만, '저장매체 구입, 배포, 파기 및 PC 관리대장 유지' 등 나머지 임무는 과업의 조합으로 이루어져 있어 현업에 적용하기에는 한계가 있다. 방위산업체들도 방산보안업무훈령의 보안실무자 직책별 임무를 기초로 업체별 보안실무자의 직무기술서를 작성해 활용하고 있지만 직무분석을 통해 책무와 과업을 제대로 도출해서 직무기술서에 반영한 업체는 드물다. 따라서 방위산업체의 보안업무 발전을 위해서는 보안실무자 직무분석을 통해 직책별 명확한 책무와 과업을 도출해 방위산업보안업무훈령에 반영하고 업체들에 보안실무자 업무 기준을 마련해 주어야 한다.

<표 1> 훈령에 명시된 정보통신보안담당의 임무

정보통신보안담당의 임무
1. 정보통신 보안내규 작성 및 불시, 정기 보안점검 2. 저장매체 구입, 배포, 파기 및 PC 관리대장 유지 3. 재난 대비 백업시설 유지 관리 및 서버 이용자 계정 생성, 삭제 4. 정보보호시스템 운용 및 보안관리 - 방화벽, 침입탐지시스템 보안정책 최신화 - 보호시스템 로그 분석 등 모니터링 업무 - 정보보호시스템 비밀번호 주기적 변경 관리 - 정보보호시스템 자체 보안취약점 진단 5. 네트워크 보안대책 - 보약취약성 프로그램 사용여부 감시, 제거 - 서버 접속 로그확인, 비인가 접속 여부 감시 - 무선인터넷 및 백신프로그램 패치 등 관리 - 트로이목마 등 악성프로그램 유입여부 감시 6. PC정비, 교체간 보안성 검토 등 자료유출 방지 활동 7. 정보통신매체 반출입 시 통제 및 보안성 검토

방위산업체 보안실무자 중에서 정보통신보안실무자는 일반기업체의 정보보호관리자나 정보보호담당자 등과 같은 정보보호 전문인력의 역할을 수행한다고 볼 수 있다. 일반적으로 정보보호 전문인력은 정보보호에 대한 정규 및 비정규 교육기관을 통해 배출된 정보보호에 대한 지식을 가진 자로서 정보보호관리자, 정보시스템 개발자, 정보시스템 운영자, 정보보호 컨설턴트 등의 직업군에 종사하는 자로 정의된다[19]. 정보보호 전문인력의 직무 관련 주요 연구는 미국 오하이오 주립대학 교육훈련 센터(CETE: Center on Education and Training for Employment)에서 개발한 정보보호 전문가(Information Security Specialist) DACUM 차트[21]와 김기윤과 나현미의 연구[4] 등이 있다.

<표 2> 정보보호 전문인력의 책무

CETE의 연구[21]	김기윤과 나현미의 연구[4]
1. 정보보호 정책 시행 2. 보안의식 교육 3. 방화벽 시스템 관리 4. 침입탐지 시스템 관리 5. 네트워크 시스템 관리 6. 컴퓨터 시스템 관리 7. 백업 시스템 관리 8. 시스템 로그 확인 9. 신원확인 관리 시행 10. 재난복구계획 개발 11. 물리적 보안 시행 12. 보안사고 대응 13. 위기분석 수행 14. 직원 관리 15. 관리적 업무 수행 16. 전문성 개발	1. 보안정책 수립 2. 위험관리 3. 보안대책 수립 4. 보안대책 관리

오하이오 주립대 CETE에서 제안한 정보보호전문가의 DACUM 차트는 16개의 책무와 156개의 과업으로 구성되어 있다[21]. 김기윤과 나현미는 DACUM과 최초분석법을 병행 실시하고 한국직업능력개발원에서 2차에 걸친 워크숍을 통해 정보보호관리자 직무를 4개의 책무와 13개의 과업으로 제시했다[4]. <표 2>에서 보여지는 것처럼 두 연구 모두 DACUM 기법을 이용해서 정보보호 전문인력의 직무분석을 진행했으나, 분석결과는 책무의 수만 보더라도 서로 차이가 있다는 것을 알 수 있다. 한편 박상서와 최운호(2001)는 국방정보보호 인력이 해당 부서에서 수행해야 할 임무를 정책화, 정보보호 실무, 연구개발, 기술지원 등 네 가지로 제시했다.[9] 이렇듯 선행연구들의 연구 결과에 차이가 있는 것은 연구자와 참여자가 직무를 어떻게 정의하는지, 책무와 과업을 어떤 기준으로 이해하고 있는지, 어떤 분석방법을 사용하는지 등이 서로 다르기 때문이다. 최근 정보 환경의 변화에 따라 요구되는 방위산업체 정보통신보안실무자의 직무를 명확히 하기 위해서는 실증적인 직무분석을 통해서 그들이 현재 수행하고 있는 책무와 과업을 도출할 필요가 있다.

2.2 직무분석

직무분석은 여러 학자들에 의해 직무 그 자체 또는 직무수행자 관점, 과정 또는 내용적 관점 등 다양한 측면에서 정의 되어 왔다[17]. 직무 그 자체에 중점을 둔 학자들은 직무분석이란 직무를 정의하고 직무 수행에 필요한 행위들을 정의 하는 것[31] 또는 직무의 주요 구성요소를 찾기 위한 체계적인 방법[29]이라고 주장한다. 직무수행자 측면에서 직무분석의 정의를 살펴보면, 직무분석은 관찰 가능한 직무수행 행위를 수집하고 기술하는 것이며 직무수행 행위는 결과 성취를 위해서 사용한 기술과 근로자들이 상호작용하는 직무환경에 대한 것을 포함한다[28]. 과정적 관점에서의 직무분석은 직무의 특성을 발견해 가는 과정[24]이며, 어떤 목적에 의해 직무와 관련된 정보를 수집하고 분석하는 체계적인 절차[30]로 정의될 수 있다.

직무분석의 개념을 좀 더 확대해서 직무 뿐 만 아니라 과업분석이나 요구분석의 개념까지 포함해서 정의하는 학자들도 있다. 이러한 학자들에 의하면 직무분석은 과업, 책무 등을 포함하는 직무명세서를 개발하는 프로세스이며 직무수행자가 숙지해야 할 지식, 기술, 능력 등에 대한 직무 명확화이다[26]. 또한 직무분석은 직무를 구성하고 있는 일의 전체 및 그 직무를 완수하기 위해서 담당자에게 요구되는 경험, 기능, 지능, 능력, 책임과 그 직무가 타 직무와 구별되는 요인을 각각 명확하게 밝혀 기술하는 절차라고 할 수 있다[13]. 이와 같은 직무분석의 포괄적 접근은 전통적 직무분석의 한계를 벗어나 미래에 요구되는 직무에 대한 분석이 가능하다는 장점이 있지만 시간과 비용, 노력 등이 더 많이 투입되어야 하는 어려움도 있다. 따라서 직무분석을 과업분석과 혼용하거나 과업분석을 포함하는 개념으로 정의하게 되면, 직무분석 전문가가 아닌 현장의 실무자들이 직무분석을 실행하는데 현실적 어려움이 있고 부담이 될 수 있다[10].

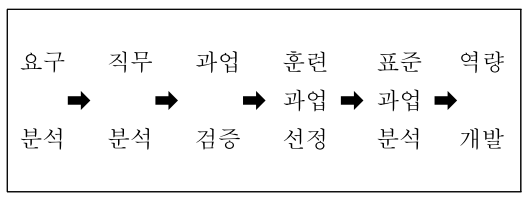
이와 같이 직무분석의 정의가 다양한 이유는 연구자들의 관점, 직무분석을 행하는 전문가들의 목적과 필요성이 다르기 때문이다. 직무분석은 일정 용도에 활용할 목적으로 직무의 실체를 밝히기 위해 적절한 수단을 써서 관련 자료를 수집, 정리, 기술하는 수단이다[15]. 직무분석은 주로 인적자원개발과 인사관리 분야에서 활용된다. 직무분석의 목적은 해당 직무에 종

사하는 자가 효과적으로 또는 성공적으로 업무를 수행하기 위해 요구되는 직무역량을 도출하는 것이다[18]. 직무분석 결과로 도출된 역량은 교육프로그램 개발의 기초자료로 유용하게 활용될 수 있다. 기업들은 이러한 직무분석을 통해 채용, 성과평가, 교육, 경력개발, 인력계획, 안전, 자격 요건 등과 같은 인사관리 시스템을 구축할 수 있다[23]. 본 연구에서는 방위산업체 정보통신보안실무자 책무와 과업의 표준을 제시하는 것이 연구의 목적이므로 직무분석을 '직무를 정의하고 직무내용과 직무수행 행위를 체계적으로 분석해 기술하는 것'이라고 정의하고자 한다.

직무분석에 대한 정의가 여러 가지 측면에서 해석되듯이 직무분석의 방법도 다양한 관점에서 구분된다. 직무와 직무수행자 측면에서 직무분석의 개념이 구분되듯이 직무분석 방법도 작업 중심 직무분석, 작업자 중심 직무분석, 혼합적 직무분석의 세 가지로 구분된다[21, 25]. 직무의 연관 관계를 파악하는 방법으로는 수직적 직무분석과 수평적 직무분석이 있다[13]. 수직적 분석이란 수직적 계층구조에 입각해 직무에 대한 정보를 체계적으로 분석하는 방법이고 수평적 분석은 개별 프로세스를 분석의 단위로 하여 각 프로세스에서 요구되는 다양한 직무를 시간의 흐름에 따라 체계적으로 분석하는 것을 말한다[13].

직무분석 방법을 인력의 개발과 관리를 위한 측면에서 구별하면 최초분석법, 비교확인법, DACUM 등으로 나눌 수 있다[10]. 최초분석법은 조사할 직무대상과 관련한 참고문헌이나 자료가 드물고 그 분야에 많은 지식과 경험을 갖춘 사람이 적을 때 직접 현장을 방문해 분석을 하는 방법이고 비교확인법은 기존의 분석된 자료를 토대로 현재의 직무 상태와 비교해 확인하는 방법이다[15]. DACUM은 교육과정 개발을 의미하는 Developing A CurriculUM의 약자로, 직무수행에 필요한 책무와 과업을 도출하고 일반적인 지식과 기술, 태도, 도구, 그리고 미래의 직무경향 등을 식별하는 직무분석 방법이다[27]. DACUM은 직무를 정확하게 인지하고 있는 현업 내용전문가들이 참여하는 워크숍을 통해 직무를 구성하는 요소와 이에 필요한 지식, 스킬 등을 결정함으로써 직무분석에 소요되는 기간을 단축할 수 있고 질 높은 직무분석 결과를 생성할 수 있는 장점이 있다[27]. 이처럼 직무분석에는 다양한 방법이 소개 및 실천되고 있지만 국내 학술지인용색인을 통해 선행연구를 분석한 결과 DACUM을 이용한 직무분석 방법이 가장 많이 활용되고 있다[10]. 특히 현재 국가인적자원개발의 핵심 과제로 추진 중인 국가직무능력표준 개발에도 DACUM이 주로 활용되고 있다. 본 연구에서는 방위산업체 정보통신보안실무자의 직무를 분석해서 궁극적으로는 국가직무능력표준 개발까지 발전시키는 것이 연구의 목적이기 때문에 방위산업체 정보통신보안실무자에 대한 직무분석 방법으로 DACUM을 활용하고자 한다.

DACUM은 교육과정 개발 방법 중 하나인 SCID (Systematic Curriculum & Instructional Development)의 첫 번째 프로세스인 분석단계(그림 2) 중에서 세 가지 주요 요소인 직무분석 워크숍, 과업검증, 과업분석 등에 활용된다[27]. 직무분석 단계는 워크숍을 통해서 직무를 구성하는 책무와 과업을 결정하고 DACUM 차트를 개발하는 과정이다[27]. 직무분석을 위해서 수집한 직무 전반에 대한 자료와 워크숍 과정에서 도출된 결과를 비교해 DACUM 차트의 책무와 과업을 결정한다. 과업검증은 DACUM 차트의 일반성을 높이기 위해서 책무와 과업의 적절성을 확인하고 개발된 과업 중에서 핵심과업이나 교육훈련에 필요한 과업을 선정하기 위해 각 과업에 대한 정보를 획득하는 단계이다. 과업분석 단계에서는 직무분석을 통해서 도출된 과업들의 수행절차, 성과기준, 지식, 스킬, 도구, 안전 고려사항 등이 도출된다. 본 연구에서는 방위산업체 정보통신보안실무자를 대상으로 책무와 과업의 표준을 제시하기 하는 것이 연구의 목적이므로, DACUM 분석 단계 중에서 직무분석 워크숍과 과업검증을 실시하여 핵심과업과 교육훈련에 필요한 과업을 선정하고자 한다.



(그림 2) SCID 분석단계[27]

국내 직무분석 연구 중에서 2011년까지 DACUM을 활용한 연구 26건을 조사한 결과 DACUM을 활용한

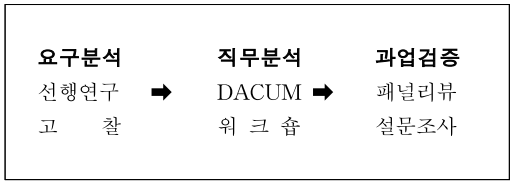
목적은 교과과정 개발이 17건(65.4%), 해당 직무의 수행업무 파악이 7건(26.9%), 출제기준 개발이 2건(7.7%) 순으로 나타났다[14]. DACUM 활용분야는 건축분야, 조선소 설비공 등과 같은 전통적인 기능 직종에서 소믈리에, 치매전문운동지도사 등과 같이 새로 생겨난 직종까지 다양하다[14]. 최근(2012년~ 2013년)에 발표된 논문 중에서도 부사관학과[5], 경찰경호학과[16], 레저관광경영학과[20] 등 교육과정 개발과 군 전문병 및 전문하사[11], 식물보호기사[8], 해외플랜트 프로젝트 비서[7] 등 점점 더 다양한 전문직업 종사자의 직무분석에까지 DACUM이 활용되고 있다. DACUM은 1990년대 국내에 도입된 이 후 가장 널리 활용되고 되는 방법 중의 하나인데, 이는 다른 직무분석 방법 보다 상대적으로 경제적이고 이른 시간 내에 정확한 분석 결과를 얻을 수 있기 때문이다[14]. 하지만 DACUM 품질기준을 토대로 주요 논문을 분석한 결과, 워크숍 시 현업 내용전문가 섭외가 어려워서 현장의 전문성 반영이 미흡하고, 책무 및 과업의 표현이 기준에 위배되며 과업검증을 하지 않아 직무분석 결과에 대한 타당성이 확보되지 못하는 등의 문제점이 발견됐다[14]. 본 연구는 이와 같은 문제점이 발생하지 않도록 DACUM 품질기준에 맞도록 절차와 내용을 정확하게 준용하려고 노력했다.

3. 연구방법

3.1 연구절차

본 연구는 방위산업체 정보통신보안실무자의 표준직무를 개발하기 위해서 DACUM의 주요 단계 중에서 직무분석 워크숍과 과업검증 단계를 진행했다. 직무분석은 원래 2~3일 간 현업 내용전문가들로 구성된 DACUM 워크숍을 진행해야 한다[27]. 그러나 방위산업체 정보통신보안실무자들이 연구를 위해서 2일 이상 워크숍에 참여하기가 현실적으로 어렵기 때문에, 간소화된 DACUM 워크숍을 진행했다. 간소화된 DACUM 워크숍을 활용 하고자 할 때 DACUM 퍼실리테이터는 분석대상 직무 관련 사전연구를 거쳐 분석대상 직무의 정의와 구조를 사전에 파악함으로써 DACUM 기간을 단축하는 효과를 거둘 수 있다[27].

DACUM을 위한 효과적인 워크숍 진행을 위해 직무분석 및 DACUM 선행연구 고찰, 방위사업법 및 방위산업보안업무훈령 등 관련 법규 검토, 방위산업체의 보안담당 부서 및 보안실무자 보직 현황 분석, 방위산업체 보안실무자 직무명세서 수집, 보안업무 우수 방위산업체 방문 등을 진행했다. 관련 법규와 직무명세서 등 각종 문헌자료 검토로 방위산업체 보안실무자 책무와 과업의 근거자료가 확보됐고 직무의 정의와 구조가 사전에 파악됐다. 특히 연구자가 2014년 3월 10일과 4월 15일 경기도에 있는 두 곳의 방위산업체를 방문해 현업 보안실무자와 함께 업무 현장을 체험하고 간단한 인터뷰를 진행해 업무 환경과 현장의 언어를 이해함으로써 내용전문가들과의 원활한 의사소통이 가능했다.



(그림 3) 연구절차

3.2 직무분석 (DACUM 워크숍)

직무분석을 위한 DACUM 워크숍은 2014년 4월 24일에 6시간 동안 진행했다. 워크숍에는 현업 내용전문가 6명, 퍼실리테이터, 코디네이터 등 총 8명이 DACUM 위원회 멤버로 참여했다. 현업 내용전문가는 2013년도 보안감사에서 우수한 평가를 받은 경기도 지역 방위산업체의 정보통신보안실무자들이다. 퍼실리테이터는 본 연구자가 담당했으며, 코디네이터는 방위산업체 보안업무를 지원하는 ○○기관 보안업무실무자가 수행했다.

워크숍은 오리엔테이션, 책무와 과업 도출, DACUM 차트 완성의 순으로 진행됐다. 퍼실리테이터 오리엔테이션에서는 워크숍 진행간 적극적인 참여 유도와 원활한 의사소통을 위해서 워크숍 위원회 멤버 소개 및 역할 안내, DACUM의 철학과 개념 설명, DACUM 차트 예시, 책무 및 과업에 대한 진술방법 설명 등을 진행했다. 이어서 현업 내용전문가들이 모두 참여해서 방위산업보안업무훈령에 명시된 정보통신보안실무자의 임

무와 업체에서 적용하고 있는 직무명세서를 기초로 명시된 책무 외에 추가로 수행하고 있는 임무까지 망라해 책무를 먼저 도출했다. 책무 도출은 비교적 수월하게 진행됐고 도출된 책무에 대한 합의도 별다른 이의나 문제 제기 없이 이루어졌다.

현업 내용전문가들은 도출된 책무별로 실제 수행하고 있거나 향후에 수행해야 할 과업의 브레인스토밍을 통해 과업을 계열화했다. 이렇게 도출된 책무와 과업을 바탕으로 퍼실리테이터는 DACUM 차트를 작성하고 전반적인 재검토 및 수정, 용어 정리 후 참여자들의 최종 합의로 방위산업체 정보통신보안실무자 DACUM 차트를 완성했다.

3.3 과업검증 (패널리뷰와 설문조사)

과업검증은 직무분석을 통해 도출된 책무와 과업의 타당성을 확인하고 핵심과업을 선정하기 위함이다. 과업검증에 참여하는 구성원들은 현업전문가 또는 그 직무를 수행해야 할 직접적인 책임이 있는 실무자의 직속상관들로 이루어진다[27]. DACUM 과업검증 방법은 설문조사, 패널리뷰, 인터뷰 또는 관찰 등이 있다[27]. 본 연구에서는 패널리뷰를 통해서 과업을 재검토하고 설문조사를 통해서 과업의 타당도와 신뢰도를 검증했다.

패널리뷰는 10~15명으로 구성된 현업전문가들이 모여 직무 관련 지식을 바탕으로 2시간 정도의 미팅으로 과업을 재검토 하는 과정으로 이루어진다[27]. 본 연구에서는 정보통신보안실무자 5명과 정보통신보안업무를 총괄하는 보안팀장급 5명으로 구성된 패널리뷰를 실시하였다. 패널들은 방위산업체 보안업무를 지원하는 ○○기관에서 진행하는 보안실무자 소집교육 입교자와 전문교관 중에서 선정됐으며 패널리뷰는 5월 22일 오후에 2시간 동안 진행됐다.

과업검증을 위한 설문조사를 준비할 때 퍼실리테이터는 '어떤 종류의 정보가 필요한지'를 신중하게 고려해야 한다[27]. 설문조사에는 과업수행 여부, 과업중요도, 학습난이도, 입직수준, 과업빈도 등과 관련한 질문이 포함될 수 있는데, 이 중에서 과업검증에 필요한 정보를 얻기 위한 최소한의 질문만 선택해 설문조사를 진행하는 것이 좋다[27]. 본 연구에서는 과업수행 타당도와 과업의 중요도 및 빈도 관련 질문을 통해서 DACUM 워크숍 결과 선정된 과업들이 실제로 현업에서 적용될 수 있는지의 타당도와 신뢰도를 검증하고 직무수행 특성을 분석했다. 설문지는 과업 항목별로 "정보통신보안실무자의 과업으로 타당한가?"(과업 타당도), "이 과업은 얼마나 중요한가?"(과업 중요도), "이 과업을 얼마나 자주 수행하는가?"(과업 빈도)의 질문으로 구성된다. 문항별 질문의 답은 Likert식 5단계 척도로 구성하고 설문의 배경과 취지를 담은 안내문을 포함해 설문지를 완성했다.

DACUM 과업검증을 위한 설문조사는 실무자 25명과 직속상관 25명을 대상으로 진행하되, 60% 이상의 응답률이면 양호한 것으로 고려된다[27]. 본 연구에서는 좀 더 정확한 과업 검증을 위해서 방위산업체 정보통신보안실무자와 보안팀장급 53명을 대상으로 팩스와 이메일로 설문조사를 진행했다. 설문지는 배포된 53부 중 39부가 회수 되어 응답률이 74%였다. 불성실한 응답을 한 3부를 제외한 36부가 최종적으로 과업검증에 사용됐다.

직무분석 결과 도출된 과업들의 타당도를 검증하기 위해서 설문조사 결과를 기초로 내용타당도 비율(CVR: Content Validity Ratio)을 구해 분석했다[22]. 내용타당도 비율은 설문조사에 응답한 인원과 '타당하다'고 응답한 인원을 아래의 내용타당도 비율 공식에 대입해 산출하고 타당도 판단은 응답 인원에 따른 내용타당도 비율 최솟값을 기준으로 결정한다[22]. 본 연구는 Lawshe(1975)가 제시한 내용타당도 비율 기준[22]에 따라 응답 인원 36명에서의 내용타당도 비율 최솟값인 0.31을 기준으로 책무별 과업의 내용타당도를 판단했다.

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

N : 응답한 인원 수
n_e : '타당하다'고 답한 인원 수

과업검증을 위한 설문조사의 문항이 얼마나 안정적으로 일관성 있게 측정했는지를 확인하기 위해서 신뢰도 분석을 진행했다. 신뢰도 분석은 문항내적일관성신뢰도 중에서 Cronbach's α에 의한 신뢰도를 산출했으며 0.60을 기준으로 설문조사 문항의 신뢰도를 판단했다.

4. 연구결과

4.1 정보통신보안실무자 책무와 과업 도출

방위산업체 정보통신보안실무자의 직무를 분석한 결과 7개의 책무와 73개의 과업이 도출됐다. 최초 DACUM 워크숍에서는 7개의 책무와 77개의 과업이 선정됐으나 과업검증 단계의 패널리뷰를 통해 유사한 과업이 통폐합되면서 결국 73개의 과업으로 구성된 방위산업체 정보통신보안실무자 DACUM 차트가 완성됐다. 책무와 과업 목록은 <표 3>과 같다.

<표 3> 정보통신보안실무자 책무와 과업

책 무	과 업
A. 정보통신 보안대책 (계획) 수립	A-1. 기존 정보통신 보안대책 검토하기 A-2. 대내외 보안환경·이슈 분석하기 A-3. 보안정책 및 관련규정 종합하기 A-4. 관련기관 및 관련부서와 협조하기 A-5. 보안대책(계획) 작성하기 A-6. 부서장 보고 및 승인 득하기 A-7. 보안대책(계획) 전파하기 A-8. 보안대책 정상시행 모니터링하기 A-9. 보안대책 실효성 평가하기 A-10. 보안대책 수정 및 보완하기
B. 정보통신 보안시스템 (보안솔루션) 관리	B-1. 보안시스템 도입 소요 판단하기 B-2. 보안시스템 도입 요청하기 B-3. 보안시스템 구축하기 B-4. 보안시스템 보안성 검토(요청)하기 B-5. 보안시스템 사용자 교육하기 B-6. 보안정책 최신화 유지하기 B-7. 시설 및 장비 보호대책 강구하기 B-8. 시스템 정상 운용 모니터링하기 B-9. 보안시스템 원격관리 통제하기 B-10. 보안시스템 취약점 진단하기 B-11. 보안시스템 유지 및 보수하기 B-12. 해킹 및 침해 여부 감시하기 B-13. 해킹 및 침해 사고시 대응 조치하기 B-14. 암호장비 및 프로그램 관리하기 B-15. 보안자재 관리하기
C. 정보시스템 (네트워크) 보안 관리	C-1. 사용자 계정 관리하기(IP, PW) C-2. 접근통제 관리하기(권한부여 등) C-3. 재난 대비 백업시스템 운용하기 C-4. 로그파일 관리하기 C-5. 바이러스 감염 예방하기 C-6. 보안 취약성 정기적 진단하기 C-7. 사내 인트라넷 보안 관리하기 C-8. 사내 이메일 관리하기 C-9. 무선 LAN 접근통제하기 C-10. 비밀 송수신 관리하기
D. 핵심기술 (도면) 전사자료 및 저장매체 관리	D-1. 보호대상 핵심기술(도면) 선정하기 D-2. 핵심기술 비밀등급 부여하기 D-3. 핵심기술 전산자료 생산 시 보안조치하기 D-4. 전산자료 보호대책 강구하기 D-5. 전산자료 작업 및 파기 시 보안조치하기 D-6. 전산자료 백업 및 복구대책 강구하기 D-7. 업무용 저장매체 등록 관리하기 D-8. 핵심기술 저장매체 보호대책 강구하기 D-9. 저장매체 반출입 및 파기 시 보안조치하기 D-10. 전산자료 및 저장매체 보유현황 관리하기
E. 상용정보 통신망 (인터넷) 보안관리	E-1. 상용정보통신망 보안측정하기 E-2. 보안측정 결과 취약점 보완하기 E-3. 사용자 IP 관리하기 E-4. 핵심기술(비밀) 작업 및 저장 통제하기 E-5. 이메일 보안관리하기 E-6. 회사 홈페이지(SNS) 보안관리하기 E-7. 공유프로그램 사용 통제하기 E-8. 인터넷 전화 관련 보안조치하기 E-9. 공개용 웹서버 보안조치하기 E-10. 비인가 사이트 접속 통제하기

책 무	과 업
F. 개인용 컴퓨터(PC) 보안관리	F-1. 필수 보안프로그램 배포/설치하기 (백신, 파일소거, 공유제거 등) F-2. PC 반입/반출 시 보안조치하기 F-3. PC 정비/교체 시 보안조치하기 F-4. PC내 핵심기술(비밀) 자료 저장 통제하기 F-5. 비인가 저장/주변장치 사용 통제하기 (USB메모리, MP3, 외장하드 등) F-6. 비인가 S/W 사용 통제하기 F-7. 개인별 PC 보호대책 강구 여부 확인하기 F-8. 퇴직자 PC 보안조치하기 F-9. 노트북(PDA) 보안대책 강구하기 F-10. PC 및 주변장치 현황 관리하기
G. 휴대/사무형 정보통신장비 (휴대폰, 카메라, FAX, 블랙박스) 보안관리	G-1. 정보통신장비 등록 관리하기 (인가, 보요현황 유지) G-2. 장비별 보안솔루션 배포/설치하기 G-3. 보안솔루션 오류/장애 처리하기 G-4. 보안솔루션 최신화 유지하기 G-5. 보안솔루션 보안취약점 개선하기 G-6. 장비 교체/폐기 시 보안조치하기 G-7. 핵심기술(비밀) 자료 송수신 통제하기 G-8. 일반자료 송수신 시 보안조치하기

DACUM 직무분석을 통해 도출된 7개의 책무와 71개의 과업들과 방위산업보안업무훈령에서 명시되어 있는 정보통신보안실무자의 임무들을 비교해 보면, 훈령에 명시된 7개의 임무 중에서 DACUM 직무분석 결과의 책무와 일치하는 것은 '정보보호시스템 운용 및 보안관리', '네트워크 보안관리' 등 2가지이다. 나머지 5개 임무는 책무보다는 과업에 해당되거나 정보통신 분야이기보다는 기업보안담당이나 보안팀장급의 업무에 해당되는 것으로 나타났다. 이것은 훈령에 명시된 임무들이 책무와 과업의 구분 없이 나열식으로 제시되어 있고 방위산업체에서 실제로 수행하고 있는 정보통신보안실무자의 책무와 과업이 많이 누락되어 있음을 나타낸다. 따라서 방위산업체 정보통신보안실무자의 임무를 재정립하고 이를 토대로 방위산업보안업무훈령을 개정할 필요성이 확인됐다.

4.2 정보통신보안실무자 과업검증 결과

방위산업체 정보통신보안실무자의 책무별 과업타당도를 검증해 본 결과 73개 과업 중에서 71개 과업은 내용타당도비율이 대부분 0.80 이상 이었다. 그러나 '핵심기술(도면) 전산자료 및 저장매체 관리' 책무 중에서 'D-1. 보호대상 핵심기술(도면) 선정하기'와 'D-2. 핵심기술 비밀등급 부여하기' 과업의 내용타당도비율은 각각 0.17과 0.11로, 설문 응답 인원 36명에 따른 내용타당도비율 최솟값 기준치인 0.31보다 낮았다. 따라서 이 두 가지 과업은 정보통신보안실무자의 과업에서 제외되어 최종적으로 7개의 책무와 71개의 과업으로 재선정됐다.

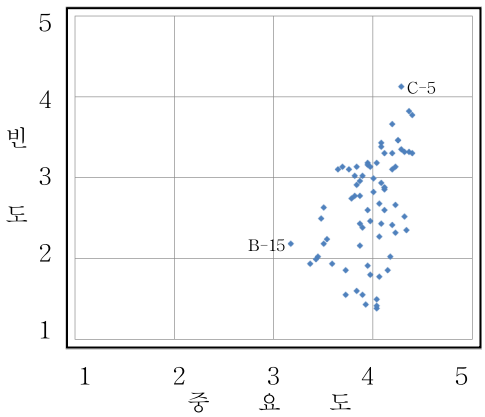
방위산업체 정보통신보안실무자의 과업타당도, 과업중요도, 과업빈도에 대한 신뢰도를 분석한 결과 각각의 Cronbach's α 계수 값이 0.95, 0.97, 0.97로 나타났다. 이 값들은 모두 0.60 이상이므로 과업검증을 위한 설문조사의 문항들이 안정적으로 일관성 있게 과업의 특징들을 측정했다는 것을 의미한다. 따라서 DACUM 직무분석과 설문조사 과업검증 결과에 따라 최종적으로 확정된 정보통신보안실무자의 책무와 과업들은 충분히 신뢰할 수 있는 수준이다.

정보통신보안실무자의 책무와 과업에 대한 중요도를 분석한 결과 7개 책무의 중요도 평균이 3.80 이상으로 모두 높은 수준의 중요도를 나타냈다.<표 4> 특히 '정보시스템(네트워크) 보안관리', '핵심기술(도면) 전산자료 및 저장매체 관리', '개인용컴퓨터(PC) 보안관리' 책무는 중요도 평균이 4.0 이상으로 정보통신보안실무자들이 중요하다고 인식하고 있는 핵심책무로 확인됐다.

<표 4> 책무별 중요도 평균

책 무	중 요 도
A. 정보통신 보안대책(계획) 수립	3.92
B. 정보통신 보안시스템(보안솔루션) 관리	3.92
C. 정보시스템(네트워크) 보안관리	4.04
D. 핵심기술 전산자료 및 저장매체 관리	4.12
E. 상용정보통신망(인터넷) 보안관리	3.85
F. 개인용컴퓨터(PC) 보안관리	4.17
G. 정보통신장비 보안관리	3.89

정보통신보안실무자의 핵심과업을 도출하기 위해서 중요도를 X축으로, 빈도를 Y축으로 해서 모든 과업을 2차원 산포도에 배치해 보았다.(그림 4)



(그림 4) 과업별 중요도 및 빈도 분포

모든 과업의 중요도 평균은 3점 이상으로 나타났으며 빈도는 과업의 특성에 따라 다양한 결과를 나타냈다. 특히 'C-5 정보시스템 바이러스 감염 예방하기' 과업은 중요도와 빈도가 모두 4점 이상으로 가장 핵심적인 과업인 것으로 확인되었다. 반면 'B-15 보안자재 관리하기' 과업은 가장 낮은 중요도와 빈도를 나타냈는데 이는 각 업체마다 보안자재 보유 유무와 관리 형태가 상이하기 때문인 것으로 확인됐다. 이상과 같이 과업별로 중요도와 빈도가 차이가 다소 있지만 71개 과업이 모두 정보통신보안실무자의 과업으로 타당한 것으로 확인됐다.

5. 결론 및 제언

본 연구는 방위산업체의 정보통신분야 보안업무 체계를 정립하고 핵심과업을 도출해 역량기반 교육훈련과정 개발의 기초를 마련하고자 했다. 이를 위해 DACUM 직무분석 기법을 이용해서 방위산업체 정보통신보안실무자의 책무와 과업을 도출하고 도출된 과업에 대한 검증을 진행했다. DACUM 직무분석 및 검증 결과는 다음과 같다.

첫째, 방위산업체 정보통신보안실무자의 직무는 7개의 책무와 71개의 과업으로 분석됐다. 7개의 책무와 책무별 과업은 정보통신 보안대책(계획) 수립 책무에 10개 과업, 정보통신 보안시스템(보안솔루션) 관리 책무에 15개 과업, 정보시스템(네트워크) 보안관리 책무에 10개 과업, 핵심기술(도면) 전산자료 및 저장매체 관리 책무에 8개 과업, 상용정보통신망(인터넷) 보안관리 책무에 10개 과업, 개인용컴퓨터(PC) 보안관리 책무에 10개 과업, 정보통신장비 보안관리 책무에 8개 과업 등이다.

둘째, 정보통신보안실무자 책무와 과업의 중요도는 모두 높은 수준을 나타냈으며 과업별 빈도는 업체별 보안업무 조직과 업무형태에 따라 다양한 분포를 보여주었다. 특히 중요도가 4.0 이상인 핵심 책무는 '정보시스템(네트워크) 보안관리', '핵심기술(도면) 전산자료 및 저장매체 관리', '개인용컴퓨터(PC) 보안관리' 등이고, 과업 중에서는 '정보시스템 바이러스 감염 예방하기'가 가장 핵심적인 과업인 것으로 확인됐다.

방위산업 관련 기관과 업체에서는 본 연구의 직무분석 결과를 다양하게 활용할 수 있을 것이다. 국방부 및 방사청 등에서는 방위사업법과 방위산업보안업무훈령의 정보통신보안 관련 내용을 개정하고, 교육기관에서는 정보통신보안실무자 교육과정을 개발할 수 있다. 또한 방위산업체는 정보통신 보안업무를 체계화하고 정보통신보안실무자의 업무수행 기준을 마련하는데 활용할 수 있다.

본 연구는 국가안보 산업으로서 보안을 가장 우선시 하는 방위산업체에서 실행되고 있는 정보통신보안실무자의 직무를 분석했다. 특히 정보통신보안실무자를 별도로 편성·운용하고 있는 주요방산업체를 대상으로 연구를 진행했기 때문에 기존의 정보보호 전문인력 직무 관련 연구들 보다 더 구체적이고 실증적인 연구결과를 얻을 수 있었다. 그러므로 방위산업체 정보통신보안실무자 책무와 과업은 방위산업체 뿐 만 아니라 일반기업체에서도 충분히 적용 가능할 것이다.

본 연구는 몇 가지 한계점이 있다. 첫째, 직무분석의 핵심인 DACUM 워크숍을 간소화하여 진행했다는 점이다. 방위산업체 특성상 현업전문가들을 2일 이상 워크숍에 참여시키기가 어려웠고 이러한 제한점을 극

복하기 위해서 사전연구와 자료 분석을 했음에도 불구하고 정보통신보안실무자 직무의 책무와 과업을 도출하기에 6시간은 다소 부족한 시간이었다.

둘째, 과업검증 과정에서 설문조사 인원이 36명으로 충분하지 못했다. DACUM 핸드북[27]에 따르면, 과업검증을 위한 설문조사는 25명의 실무자들과 25명의 직속상관들을 대상으로 실시하되, 60% 이상의 응답률이면 양호한 것으로 고려된다. 하지만 일반적인 통계분석에서 설문도구의 타당도와 신뢰도를 분석하기에는 사례 양이 충분하지 않다.

향후 DACUM 기법을 활용한 직무분석 연구자들은 본 연구의 한계점들을 보완해 완결성을 갖춘 연구가 되도록 DACUM 절차를 준수하되 과업의 타당도와 신뢰도 검증에 대한 더 많은 연구가 필요하다. 또한 방위산업체 보안업무 전반에 대한 직무 재정립을 위해서는 보안실장이나 기업보안담당 등 다른 보안실무자들에 대한 직무분석도 필요하다. 이러한 직무분석을 기초로 보안실무자에게 필요한 역량을 도출해 국가직무능력표준 개발과 역량기반 교육과정 개발의 기초를 제공할 수 있을 것이다.

참고문헌

[1] 국가정보원 산업기밀보호센터 (NISC: National Industrial Security Center), http://service12.nis.go.kr

[2] 국방부, '방위사업법', 2010.

[3] 국방부, '방위산업보안업무훈령(국방부 훈령 제1394호)', 2012.

[4] 김기윤, 나현미, "정보보호자에 대한 직무분석", 정보보호학회지, 제10권, 제3호, pp. 63-74, 2000.

[5] 김영종, "군 전문인력 양성학과 교육과정 개발 방안", 융합보안논문지, 제13권, 제2호, pp. 195-202, 2013.

[6] 김영수, "방위산업의 보안 관련 법률 검토", 산업보안연구, 제2권, 제2호, pp. 49-90, 2011.

[7] 김임정, 최애경, "해외플랜트 프로젝트비서 직무와 핵심작업에 관한 연구", 상업교육연구, 제26권, 제3호, pp. 45-70, 2012.

[8] 김정임, 김규섭, "DACUM을 이용한 식물보호기사의 직무분석 및 국가기술자격 시험의 출제기준 개발", 한국인간·식물·환경학회지, 제15권, 제3호, pp. 209-217, 2012.

[9] 박상서, 최운호, "국방 정보보호 인력 양성 방안", 융합보안논문지, 제1권, 제1호, pp. 69-81, 2001.

[10] 박용호, 조대연, 김벼리, 노유경, 황몽, 정희정, 홍순현, "DACUM법을 이용한 초등학교 방화후학교 강사 직무분석", HRD연구, 13권, 1호, pp. 163-186, 2011.

[11] 박효선, "군 특성화고 졸업 후 입대한 전문병 및 전문하사의 직무능력 향상방안", HRD연구, 제15권, 제1호, pp. 135-158, 2013.

[12] 산업연구원 편집부, 'KIET 방위산업 통계 및 경쟁력 백서', 산업연구원, 2014.

[13] 송상호, "프로세스를 중심으로 한 새로운 직무분석방법에 관한 연구", 인사관리연구, 제21집, 제1권, pp. 97-125, 1997.

[14] 윤동열, 조세형, 배을규, "국내 직무분석에서 DACUM 활용 현황과 비판", 교육문화연구, 제17권, 제3호, pp. 87-115, 2011.

[15] 장수용, '직무분석 조사기법', SBC전략기업컨설팅, 2011.

[16] 정일홍, "DACUM 분석을 통한 경찰경호학과 교육과정 개발 연구", 한국민간경비학회보, 제11권, 제4호, pp. 323-341, 2012.

[17] 조대연, 정은정, 홍순현, 강윤석, "국내 직무분석에 관한 연구논문 분석: 2000이후 국내 학술지 발표 논문을 중심으로", 한국HRD연구, 제6권, 제4호, pp. 1-19, 2011.

[18] 한국산업인력공단, '국가직무능력표준 개발 매뉴얼', 문원사, 2013.

[19] 한국정보보호진흥원, '정보보호 실태조사: 기업편', 2007.

[20] 황옥선, "DACUM Method에 의한 레저관광경영학 전공 교육과정 개발 연구", 상업교육연구, 제26권, 제3호, pp. 21-44, 2012.

[21] Center on Education and Training for Employment, 'DACUM Research Chart for Information Security Specialist', The Ohio State

University, 2006.
[22] C. H. Lawshe, "A quantitative approach to content validity", Personnel psychology, Vol 28, No. 4, pp. 563-575, 1975.
[23] F. P. Morgeson and M. A. Campion, "Social and cognitive sources of potential inaccuracy in job analysis", Journal of Applied Psychology, Vol. 82, No. 5, pp. 627-655, 1997.
[24] M. T. Brannick, E. L. Levine, and F. P. Morgeson, 'Job and Work Analysis: Methods, Research, and Applications for Human Resource Management.(2nd ed.)', Sage, 2007.
[25] O. F. Vosquijl, 'Job Analysis: Current and Future Perspectives. In A Ever, N. Anderson, & O. Smit · Voskuijl(Eds.). Handbook of Personnel Selection.', Blackwell Publishing, 2005.
[26] R. A. Noe, 'Employee training & development (5th ed.)', McGraw-Hill Companies, 2008.
[27] R. E. Norton and J. Moser, 'DACUM Handbook (3rd ed.)', Center on Education and Training for Employment, The Ohio State University, 2008.
[28] R. J. Harvey, "Job analysis, In M. Dunnette & L. Hough(Eds.)", Handbook of industrial and organizational psychology(2nd., Vol. II, pp. 71-163), Consulting Psychologists Press, 1991.
[29] R. L. DeSimone and D. M. Harris, 'Human resource development(2nd ed.)', The Dryden Press, 1998.
[30] S. Gibb, 'Human resource development: process, practices, and perspectives(2nd ed.)', Palgrave Macmillan, 2008.
[31] W. F. Cascio, 'Applied psychology in human resource management(5th ed.), Prentice-Hall, 1998.

[저 자 소 개]

우 광 제 (Kwang Jea Woo)

1990년 육군사관학교 전산학과 학사
2002년 University of Nebraksa 경영정보학 석사
2014년 현재 중앙대학교 인적자원 개발학과 박사과정

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