박사학위청구논문
2023학년도

IPA 방법을 활용한 방산업체 보안전문가 직무영향분석 연구

(중요도, 난이도, 수행빈도를 중심으로)

A Study on the Job Impact Analysis of Security Experts in Defense Industry Using IPA Method

(Focusing on Importance, Difficulty, and Performance Frequency)

광운대학교 대학원

방위사업학과

이 승 목

IPA 방법을 활용한
방산업체 보안전문가 직무영향분석 연구

(중요도, 난이도, 수행빈도를 중심으로)

A Study on the Job Impact Analysis of Security Experts in Defense Industry Using IPA Method

(Focusing on Importance, Difficulty, and Performance Frequency)

광 운 대 학 교 대 학 원

방 위 사 업 학 과

이 승 목

IPA 방법을 활용한
방산업체 보안전문가 직무영향분석 연구

(중요도, 난이도, 수행빈도를 중심으로)

지 도 교 수　　정　석　재

이 논문을 공학 박사학위 청구논문으로 제출함.

2023년 12월

광 운 대 학 교　대 학 원

방 위 사 업 학 과

이　승　목

이승목의 공학 박사학위논문을 인준함

심사 위원장 손 채 봉 인

심 사 위 원 정 석 재 인

심 사 위 원 김 장 엽 인

심 사 위 원 김 홍 빈 인

심 사 위 원 우 한 철 인

광 운 대 학 교 대 학 원

2023년 12월

감사의 글

30여 년의 군 생활을 하는 동안 많은 날을 지새우고 보고서와 씨름하였는데, 박사학위 논문을 시작하며 과거의 그 어느 때보다 고뇌하고 힘든 시간을 보냈지만, 인생의 새로운 목표를 향해 도전하게 하신 하나님께 우선 감사드립니다.

많은 분들의 아낌없는 조언과 도움이 없었다면 오늘 이 박사 논문을 마무리하지 못했을 것입니다. 특히, 지혜로운 지도와 격려로 이 자리까지 이끌어 주신 정석재 지도교수님께 깊은 감사의 인사를 드리며, 교수님 덕분에 힘든 여정과 어려운 순간을 극복하며 여기까지 올 수 있었습니다.

또한, 바쁘신 중에도 심사 위원장으로서 정성스럽게 지도해 주시고 따뜻한 마음으로 배려해 주신 손채봉 교수님, 논문의 완성도를 위해 조언해주신 김홍빈 교수님, 우한철 박사님, 그리고 연구의 기본 틀이 되는 통계분석과 문맥의 구조까지 지속적인 관심과 적절한 조언을 해 주신 김장엽 교수님께 마음 깊이 감사의 말씀을 드립니다. 아울러, 다양한 분야에서의 전문 경험을 바탕으로 도움을 주신 선·후배 부대원, 정성 어린 설문 조사에 응해주고 응원해 주신 방산 업체 보안관계자분들께도 진심을 담아 감사의 말씀을 전합니다.

제가 학문의 길로 들어서도록 항상 지지해 주고 힘이 되어 준 아내 곽미경, 사랑하는 아들 주환, 정환에게도 고마움을 전합니다. 남편으로서, 아빠로서 많이 부족하고 소홀함에도 항상 곁에서 응원하며 지켜봐 준 덕분에 논문을 잘 마무리할 수 있었습니다. 더 좋은 남편, 더 좋은 아빠가 되기 위해 노력할게요!

지난 3년 동안 박사학위 과정을 통해 무기체계의 획득절차와 방위산업 전반에 걸친 다양한 지식을 배워나갔으며 이러한 깊이 있는 학업을 통해 '국방사업관리사' 자격증도 취득할 수 있었습니다. 많은 견문을 넓혀 주신 학과 교수님과 관계자분들, 더불어 현재 함께 근무하고 있는 국방과학연구소 해양기술연구원 동료 소원분들의 격려로 오늘의 영광스러운 졸업을 맞이하게 되었습니다.

모든 분들께 다시 한번 감사드리며, 학문의 깊이를 더해 갈수록 더 배워야 할 분야가 많음을 깨달았는데, 앞으로도 더욱 겸손하고 적극적인 배움의 자세로 정진해 나아가겠습니다. 감사합니다. 그리고 사랑합니다.

국문 요약

IPA 방법을 활용한 방산업체 보안전문가 직무영향분석 연구 : 중요도, 난이도, 수행빈도를 중심으로

K-방산의 관심과 확대가 지속되는 가운데, 국내 방산업체와 국방 연구기관을 겨냥한 자료 탈취 등의 목적으로 한 해킹 등이 발생하고 있다. 반면, 국내 일부 방산업체의 경우 전문 보안 인력 및 예산 부족 등의 이유로 보안의 기본적인 시스템 유지 조치 어려워 보안 위협에 노출되고 적대국 및 해커의 주요 공격대상이 되고 있는 실정이다. 국가정보원이 23년 3월 발표한 것에 의하면 최근 5년 동안 적발된 산업기술 해외유출 사건은 93건이며, 이 중 국민경제와 국가안보에 심대한 영향을 미치는 국가의 핵심기술은 33건이나 되는 것으로 밝혀졌다. 방산업체 안팎에서는 보안에 대한 중요성을 인식하고 지금보다 강화된 보안 시스템과 대응체계를 갖춰야 한다는 목소리가 높아지고 있다. 따라서 방산업체 보안전문가들의 직무를 명확히 분석하여 업체 경영진에게 보안업무의 필요성을 제시하고, 교육시스템과 방산업체 평가 및 감사에 대한 과학적인 기초자료를 제시하여 방산업체의 '사이버 레질리언스'[1] 를 강화하는 데 목적이 있다.

본 연구에서는 방위산업보안업무훈령과 방위산업기술 보호지침, 해당 분야 논문을 기초로 '예비직무'를 산출하고, '예비직무'를 근거로 방산보안 분야 전문가 11명을 대상으로 델파이 기법을 통해 '예비직무'에 대한 합의점을 찾아 설문에 필요한 직무를 확정 후 방산보안 분야 전문가 40여 명 대상으로 중요도, 난이도, 수행빈도에 관한 설문을 실시하여 설문결과를 근거로 IPA 방법을 활용, 방산업체 보안전문가의 직무를 분석· 평가하였다.

1) 사이버 복원력은 시스템을 보호할 뿐만 아니라 직면한 위협이나 공격에 관계없이 시스템을 계속 실행하는 능력

본 연구는 방산업체 보안전문가 직무를 중요도-수행빈도, 중요도 - 난이도, 중요도/난이도의 평균-수행빈도로 구분하여 분석・평가하였고 크게 4가지 정책적 개선 요소가 도출되었다. 첫째, 방산업체 경영진 차원에서 비밀관리, 정보통신보안 분야 등 14개 세부 직무에 인력을 충원해야 하며, IT 발전속도에 뒤처지지 않도록 첨단화된 보안시스템 구축이 필요하다. 둘째, 교육기관에서는 방산업체 보안전문가들이 중요하면서도 어렵게 인식하고 있는 정보통신보안을 포함한 중·장기 보안계획 수립 등 20개 세부 직무를 교육내용에 포함 등 '교육 커리큘럼'을 일부 개선해야 한다. 셋째, 통합실태조사 평가에 대한 명확한 기준점 마련과 평가 시 정보통신보안과 비밀관리 직무에 대한 가중치 부여가 필요하다. 넷째, 방위산업보안업무훈령과 방위산업기술보호법의 일원화를 통한 '방위산업보안기본법(가칭)'의 제정이 필요하다.

결론적으로 본 연구는 방산업체 경영진에게는 인력충원의 필요성, 교육기관에는 전문교육의 개선 소요, 감사 및 평가기관에는 가중치 항목 식별 등 과학적 직무 값을 제시하였는바, 향후 관계기관에서 유용한 자료로 활용할 것으로 기대해 본다.

주제어: 직무분석, 중요도, 난이도, 수행빈도, IPA 분석

Abstract

A Study on the Job Impact Analysis of Security Experts in Defense Industry Using IPA Method : Focusing on Importance, Difficulty, and Performance Frequency

As interest and expansion in the K-defense industry continues, hacking aimed at domestic defense companies and defense research institutes for the purpose of stealing data is occurring. On the other hand, some domestic defense companies are exposed to security threats due to difficulties in maintaining basic security systems due to lack of professional security personnel and budget, and are becoming major targets of attacks by hostile countries and hackers. According to the National Intelligence Service announced in March 2023, there have been 93 cases of industrial technology being leaked overseas over the past five years, of which 33 cases were national core technologies that have a significant impact on the national economy and national security. lost. Voices are growing both inside and outside the defense industry to recognize the importance of security and to have a more strengthened security system and response system. Therefore, we clearly analyze the duties of defense industry security experts and present the necessity of security work to company management, and present scientific basic data on the education system and defense industry evaluation and audit to strengthen the 'cyber resilience' of defense industry companies. The purpose is to do this.

In this study, 'preliminary jobs' were calculated based on the Defense Industry Security Work Directive, the Defense Industry Technology Protection Guidelines, and papers in the field, and based on the 'preliminary jobs', 11 experts in the defense industry security field were selected through the Delphi technique. After finding a consensus on 'preliminary duties' and confirming the duties required for the survey, we conducted a survey on the importance, difficulty, and frequency of performance to about 40 experts in the defense industry security field, and used the IPA method based on the survey results to identify defense industry security experts. The job of was analyzed and evaluated.

This study analyzed and evaluated the jobs of defense industry security experts by dividing them into importance-performance frequency, importance-difficulty, and average importance/difficulty-performance frequency, and four major policy improvement factors were derived. First, at the level of defense industry management, manpower must be added to 14 detailed positions, including secret management and information and communication security, and an advanced security system must be established to keep up with the pace of IT development. Second, educational institutions must improve the 'educational curriculum' by including 20 detailed jobs in the training content, such as establishing mid- to long-term security plans, including information and communication security, which defense industry security experts recognize as important but difficult. Third, it is necessary to establish a clear standard for evaluating the integrated survey and to give weight to information and communication security and

secret management duties during the evaluation. Fourth, it is necessary to enact the 'Framework Act on Defense Industry Security (tentative name)' through unification of the Defense Industry Security Work Directive and the Defense Industry Technology Protection Act.

In conclusion, this study presented scientific job values, such as the need for manpower recruitment for defense industry executives, the need for improvement of professional education for educational institutions, and the identification of weighted items for audit and evaluation organizations, and is expected to be used as useful data by related organizations in the future. see.

Key words: Job analysis, importance, difficulty, frequency of performance, IPA analysis

차 례

그림 차례

표 차례

제1장 서 론

제1절 연구배경 및 목적

1. 연구의 배경

윤석열 대통령은 지난 3월 국군방첩사령부(이하 방첩사)를 방문('23. 3.22.)하여 "우리 군이 과학기술 강군으로 도약하기 위해서는 확고한 군사보안태세를 정립하고, 방산업체의 핵심기술이 외부로 유출되지 않도록 방산기술 보호활동을 적극 시행해야 한다."라고 강조했다. 그러나 방산업체 현장에서는 정부의 노력과는 다르게 직원들의 해이한 보안의식, 이메일 피싱·해킹사고 피해, 기술 해외유출 등으로 보안교육 강조와 보안전문가 활용이 절실해 보인다. 국내 방산 업체는 약 500여 개사(대기업 : 약 10개사, 중견기업: 약 100개사, 중소기업: 약 400개사)[2]가 있으나, 일부 방산업체의 경우 전문 보안인력 및 예산 부족 등의 이유로 기본적인 보안 체제 유지가 어려워 보안 위협에 노출되어 있으며 해커의 주요 공격 대상이 되고 있다. 최근 천안에 소재한 중견 방산업체의 경우 대표 이사와 임원들이 보안 인가를 받지 않은 상태에서 보안 시설을 무단으로 출입하는가 하면 보안도면 등을 개인 PC로 옮기는 등의 보안사항을 위반하였다가 적발되기도 하였다.[3] 000주요 방산업체 또한 21년 16억 원 규모의 이메일 '피싱 사기'를 당한 사실이 알려졌다.[4] 국가정보원이 23년 3월에 발표한 것에 따르면 최근 5년 동안 적발한 산업기술 해외유출 사건은 93건으로 이 중 국가안보와 국민경제에 심대한 영향을 미치는 국가 핵심기술은 33건이나 되는 것으로 밝혀졌다.[5] 'K-방산'에 대한 관심이 집중되고 있는 가운데 국내 방산업체와 방위사업청을 겨냥한 자료 탈취 등을 목적으로 한 해킹 등이 발생 되고 있으며 방사청에 대한 해킹 시도도 연간

2) "방산업체, 제로트로스트 사이버 보안 현대화 해야", 데이터넷, 2021. 9. 20.
3) "방산업체 A사, '방위사업법'·'보안 규정' 위반...철저한 수사 절실", 이뉴스투데이, 2023. 3.31.
4) "KAI, 이메일 '피싱사기' 당했다… '16억원 규모 피해'". 조선일보, 2021. 6.18.
5) "기술 유출 범죄 대응 강화…여야, 첨단전략산업법 추진". 매일경제, 2023. 6. 4.

3,000건에 이르고, 방산업체를 포함하면 연평균 121만 건의 해킹 공격이 있었던 것으로 나타났다.[6)]

국내 방산업체들은 상기와 같이 외부 해킹 위협에 노출되어 있어 사이버 보안에 주의를 기울여야 한다. 최근 들어 방산업체를 상대로 해킹 등 사이버 공격이 늘어나고 있는 실정인데, 방산업체 안팎에서는 보안에 대한 중요성을 인식하고 지금보다 강화된 보안시스템과 대응체계를 갖춰야 한다는 목소리가 높아지고 있다. 사이버 공격이 점점 강력해지고 정교화되고 있어 대응체계를 더욱 강화해야 하며, 보안전문가들의 능력향상과 더불어 체계화된 교육시스템 마련이 시급한 실정이다. 따라서 본 논문에서 방산업체 보안전문가들의 직무에 대한 중요도, 난이도, 수행빈도를 측정하고 IPA 분석을 통해 업체 경영진에 보안업무의 필요성을 제시하고, 교육시스템과 방산업체 통합실태조사(보안감사)의 체계화를 위한 기초자료를 제시하고자 한다.

2. 연구의 목적

본 논문에서는 방위산업보안업무훈령, 방위산업기술 보호지침, 산업 및 방산보안 직무와 관련된 각종 논문의 선행연구를 통해 방산업체 보안전문가의 직무를 산출한 후 현장 설문을 통해 각 직무별 중요도, 난이도, 수행빈도를 분석하여 방산업체 경영진, 방산보안 교육담당 기관, 통합실태조사 관계기관(방위사업청, 국정원, 방첩사)에 방산보안 업무에 대한 과학적이고 정량화된 자료를 제시하는데 목적이 있다.

첫째, 방산업체 경영진에 대한 방산보안의 중요성과 인력충원 등 방향을 제시하고 자 한다. K-방산에 대한 확산분위기 속에서 적대국의 해킹 시도가 급증하고 있으나, 업체에서는 경영의 어려움, 중요성의 인지도 부족 등 관심이 부족한 실정

6) “방위사업청 겨냥한 해킹… 2019년 2575건→ 2021년 4316건, 2년 만에 '따블'”, 뉴스데일리, 2022.2. 5.

이다. 따라서 과학적 방법에 의한 보안전문가 직무분석을 통해 업체 경영진에게 필요한 데이터를 제시할 필요가 있다.

둘째, 교육주관 기관에 방산업체 보안전문가 직무분석 결과를 제시함으로써 체계화된 교육시스템을 마련하고 자 한다. 00학교에서는 매년 방산업체 보안실무자 대상으로 방산보안 교육을 실시하고 있다. 물론, 업체 보안실무자 대상 교육 후 설문조사와 사후 강평 등을 통해 향후 교육 개선책이 마련되고 교육계획이 수립되고 있다. 그러나, 방산업체 보안전문가의 직무에 대한 충분한 분석자료 없이 교육계획이 작성되고 있는 실정이다.

셋째, 통합실태조사 등 방산업체 감사기관에 정량화된 방산업체 보안직무를 제시하고자 한다. 방위사업청에서는 방산업체의 중복 수검에 대한 부담을 경감시키고자 2020년 3월부터 통합실태조사를 실시하고 있다. 방위산업기술 보호지침에 명시된 자가진단표와 실태조사 핵심항목을 기준으로 실태조사를 실시하고 있는데 평가 기준에 대한 모호성, 가중치에 대한 비공개(감사 내부적으로 평가) 등으로 방산업체에서 볼멘소리가 나오고 있는 실정이다. 따라서, 방산업체 보안직무의 중요도, 난이도, 수행빈도를 근거로 한 과학적 자료를 제공한다면 통합실태조사(감사)에 대한 객관적 평가에 일부 도움이 될 것으로 기대한다.

제2절 연구범위 및 방법

방위산업보안업무훈령, 방위산업기술 보호지침과 각종 논문에서 제시한 보안업무의 직무를 비교・확인하여 방산업체 보안전문가의 예비직무를 산출한 후 보안분야 전문가 의견을 수렴하는 델파이 기법을 통해 직무를 확정하고, 현장 전문가 대상 설문을 통해 각 직무별 중요도, 난이도, 수행빈도를 구한 후 도출된 결과를 근거로 IPA 분석을 활용하여 인력충원 소요, 교육 우선순위, 통합실태조사 가중치 등을 제시하고자 한다.

이에 따라 본 연구에서는 그림 1과 같이 ① 1차적으로 방위산업보안업무훈령과 방위산업기술 보호지침, 해당 분야 논문을 기초로 예비직무를 산출하고, ② 산출한 예비직무를 근거로 방산보안 분야 전문가 10여 명을 대상으로 델파이 기법을 통해 예비직무에 대한 합의점을 찾아 설문에 필요한 직무를 최종 확정한다. 이후 ③ 상기 확정된 직무를 근거로 방산보안 분야 전문가 40여 명 대상으로 중요도, 난이도, 수행빈도에 관한 설문을 실시하고, ④ 설문결과를 근거로 IPA 방법을 활용하여 방산업체 보안전문가의 직무를 세부적으로 분석·평가한다.

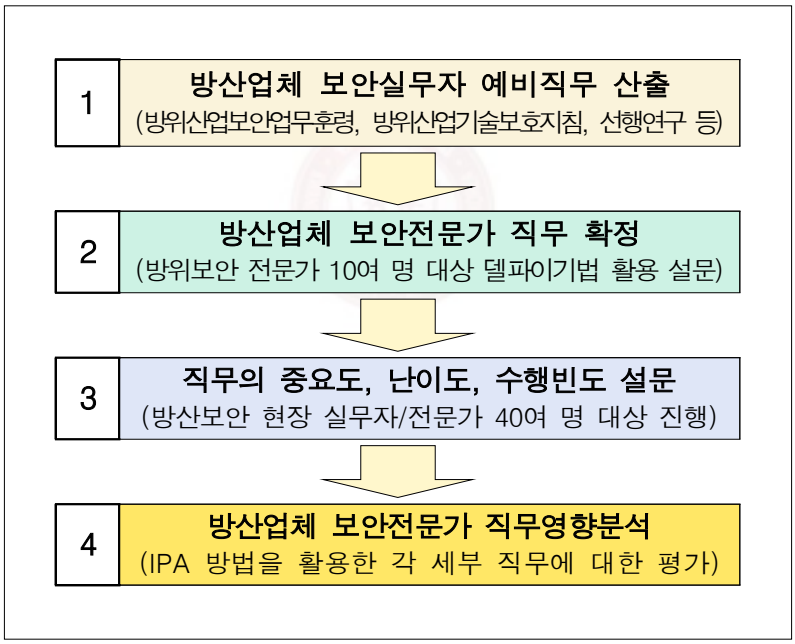


그림 1. 연구수행 절차
Figure 1. Research Performance Procedures

제3절 논문의 구성

1장 서론은 연구를 수행하게 된 배경 및 목적, 이를 달성하기 위한 연구범위 및 방법을 제시한다.

2장 이론적 고찰 및 선행연구에서는 방위산업의 특징과 방위산업과 방산보안의 변천 흐름, 방산보안의 환경과 기술유출 사례, 방산업체의 보안환경을 제시 후 방산보안 관련 선행 논문을 연구하였고, 직무분석의 정의와 특징, 직무분석의 방법, 직무분석의 목적에 대하여 파악하고, 직무분석 방법과 관련된 선행 연구 활동을 분석하여 향후 방산업체 보안전문가의 직무를 분석·평가하는 기초를 마련한다.

3장은 방위산업보안업무훈령과 방위산업기술 보호지침, 산업보안관리사 직무, 각종 논문에서 제시하고 있는 방산업체(산업체) 보안전문가의 직무를 수집하고, 방산업체 보안업무와 관련된 선행 연구활동을 분석하여 예비직무 산출을 위한 기초자료를 수집한다.

4장은 연구대상 및 연구 수행절차를 설명하고, 델파이 기법과 IPA 분석방법에 대한 개념을 설명 후 훈령 및 지침, 선행 연구 논문을 근거로 방산업체 보안전문가의 예비직무를 산출하고, 델파이 기법으로 직무를 확정 후 설문을 통해 직무에 대한 중요도, 난이도, 수행빈도의 평균값을 도출하여 연구분석을 위한 준비를 한다.

5장 앞에서 제시한 방산업체 보안전문가의 직무에 대한 중요도, 난이도, 수행빈도의 평균값을 근거로 중요도-수행빈도, 중요도-난이도, 중요도/난이도 평균-수행빈도를 IPA 기법을 통해 직무영향을 분석한다.

6장에서는 결과물로 산출한 직무영향 분석을 기초로 방산업체 보안전문가 직무의 중요도, 난이도, 수행빈도에 대한 종합적인 결론과 이를 토대로 향후 연구 방향을 포함한 정책적인 제언을 한다.

제2장 이론적 고찰 및 선행연구

제1절 방위산업과 방산보안

1. 방위산업의 정의

방위산업은 사전적으로 국가 방위를 위하여 군사적으로 소요되는 물자의 생산과 개발에 기여하는 산업으로 정의하고 있으며, 방위산업 발전 및 지원에 관한 법률에서는 방위산업을 방위산업물자 등의 연구개발 또는 생산(제조·수리·가공·조립·시험·정비·재생·개량 또는 개조)과 관련된 산업으로 정의하고 있다. 넓은 뜻으로는 무기·탄약 등 직접적인 전투기구뿐만 아니라 피복·군량 등 비전투용 일반 군수물자까지도 포함하여 해석한다. 그러나 일반적으로는 국방력 형성에 중요한 요소가 되는 총·포·탄약·함정·항공기·전자기기·미사일 등 무기장비의 생산과 개발을 담당하는 산업의 총칭으로 그 범위를 한정하고 있다. 제2차 세계대전 전까지는 군수산업으로 해석되었으나, 전쟁 개념이 방위전 개념으로 발전하면서 방위산업이라는 용어로 사용하고 있다.[7)]

2. 방위산업기술의 특징

산업기술은 제품 또는 용역의 개발·생산·보급 및 사용에 필요한 제반 방법 내지 기술상의 정보 중에서 행정기관의 장(위탁 또는 위임받은 법인이나 기관·단체의 장)이 산업경쟁력 제고나 유출방지 등을 위하여 지정·고시·공고·인증하는 기술을 말하며, 국가 핵심기술과 산업발전법 등 다양한 법률에서 지정된 기술을 '산업기술'이라고 정의한다.[8)] 이 중 국가 핵심기술은 해외로 기술 유출 시 국가안전보장과 국민의 경제발전에 심대한 악영향을 줄 우려가 있는 기술을 의미하는 것이다.

---

7) 한국민족문화대백과사전, 한국학중앙연구원, http://encykorea.aks.ac.kr/
8) 산업기술의 유출방지 및 보호에 관한 법률(약칭: 산업기술보호법) 제 2조 정의

국방 과학기술은 국방에 필요한 무기체계와 자동화 체계에 관한 기술적 조사·연구개발 및 시험 등을 하는 엔지니어링 기술로 정의[9]되어 있으며, 방위산업기술보호법에서 보호대상으로 정의하고 있는 방위산업기술은 방위산업과 관련한 국방과학기술 중에서 국가안보 등을 위하여 보호되어야 하는 기술로서 방위사업청장이 지정·고시한다.[10] 각 기술 간의 관계는 그림 2와 같다.

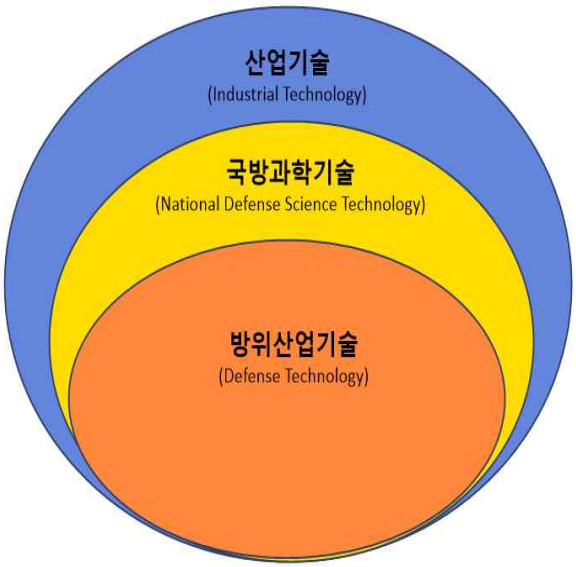


그림 2. 방위산업기술의 범주
Figure 2. Category of Defense Industry Technology
자료출처 : 박흥순 학술논문(2019) 인용

이 중 방위산업기술은 다음과 같은 특징이 있다. 첫째, 방위산업기술은 첨단기술과 무기체계의 발달과 더불어 함께 발전한다는 것이다. 둘째, 방위산업기술은

9) 국방기술품질원, 국방과학기술용어사전, 2017
10) 방위산업기술 보호법(약칭: 방산기술보호법) 제 2조 정의

다른 기술개발과 달리 장기간 연구가 이루어 진다는 것이다. 셋째, 적에게 방위산업기술이 유출시 국가안보에 상당한 영향을 준다는 것이다. 넷째, 방위산업은 다양한 산업활동을 통해 고용창출이 가능하고 파급효과가 크다는 것이다.(박홍순; 김세용; 김용환, 2019)

3. 방산보안의 역사

방위산업 초창기의 방위산업 보안은 군이 필요로 하는 각종 장비뿐 아니라 장병들의 의식주에 필요로 하는 물품을 생산하는 업체가 파업이나 화재 등 각종 사고 시 군에 직접적 피해를 줄 수 있어 이를 예방하기 위한 목적으로 시작되었으며, 방위산업 보안은 적으로부터 군에서 필요로 하는 방위산업 물자를 생산하고 공급하는 방산업체의 기밀을 보호하며, 업체가 물자를 적절한 시기에 생산 및 공급할 수 있도록 보장하기 위한 모든 활동이다. 1965년 국방부에서는 군사보안업무훈령에 의거 군수업체에 대한 보안업무를 수행하기 시작하였고 1966년 군납업체 및 군수 공장을 상대로 '보안측정'을 하여 그 결과를 계약 체결 시 반영하였으며, 1977년 국방부에서 '방위산업보안업무훈령'을 제정하면서 군수업체에 대한 방위산업보안업무를 지원하는 체제가 마련하였다. 방산업체는 대통령령으로 정하는 '보안요건'을 갖추어야 한다. 보안요건은 방위사업법 시행령에 규정되어 있으며 방위산업보안업무훈령으로 세부적으로 제시하고 있다. 방산업체의 '보안요건'은 표 1과 같이 방위사업법 시행령 제44조에 규정되어 있다. 이런 보안요건은 군사기밀을 취급하는 방산업체의 기밀유출을 방지하기 위한 보안체계 요건을 일컫는 것이라 할 것이다.(류연승, 2018)

표 1. 방위사업법 시행령 제44조 보안요건

Table 1. Security Requirements in Article 44 of the Enforcement Decree of the Defense Acquisition Program Act

자료출처 : 방위사업법 시행령 제44조

방산업체 보안요건
1. 방산시설이 충분히 보호될 수 있는 지역 및 시설에 관한 보안대책
2. 방산업체에 종사하는 인원에 관한 보안대책
3. 비밀문서의 취급 및 보관·관리에 관한 보안대책
4. 방산물자 및 원자재에 관한 보호대책
5. 장비 및 설비의 보호대책
6. 통신시설 및 통신수단에 대한 보안대책
7. 각종 자료의 정보처리과정 및 정보처리 결과자료의 보호대책
8. 보안사고에 대비한 관계정보기관과의 유기적인 통신수단
9. 그 밖에 보안유지를 위하여 방위사업청장이 필요하다고 인정하는 보안대책

국방부는 방산업체의 보안업무 지원을 위해 '방위산업보안업무훈령'을 제정하였고, 방위산업보안업무훈령의 주요 내용은 ①계획보안, ②문서보안, ③기업보안, ④인원보안, ⑤시설보안, ⑥정보통신보안 등으로 구성되어 있으며, 방산업체는 이 훈령에 따라 방위사업법에 규정된 보안요건의 대책을 강구해야 하며, 매년 보안감사를 통해 방산업체의 보안대책을 점검하였다. 2006년 개청한 방위사업청은 2012년 '방산기술통제관실'을 신설하였고 방산기술통제관실은 '15년 12월 방위산업기술보호법을 제정하여 국가안보를 위해 보호할 필요성이 있는 기술을 '방위산업기술'로 지정하고 방산업체 등 관련 대상기관의 방위산업기술 보호체계 구축을 지원해 나가고 있다. 이후 방산기술통제관실은 2018년 핵심기술 기획·개발 조직을 포함하여 '국방기술보호국'으로 개편하였다.(류연승, 2018)

방위사업청에서는 방산업체가 방산물자 또는 국방과학기술을 수출할 때는 승인을 받도록 통제하고 보호하기 위하여 2015년 방위산업기술보호법을 제정하였고 이 중 방위산업기술은 2016년 12월에 처음으로 지정 고시되었으며, 현재 고시(방위사업청 고시 제2020-1호)에 따라 8대 분야 45개 분류로 총 123개 기술이 있다. 이로써 방위산업기술 보호법을 통해 국방과학기술을 보호하는 체계를 구축하게 되었다.

4. 방산보안의 환경 및 기술 유출

과거 방위산업은 대다수가 해외에서 직구매를 우선 하였으나, 최근에는 자체 연구개발을 통해 국내 방위산업기술 확보에 심혈을 기울이고 있어 기술을 유출하기 위한 시도가 증가하자 앞에서도 설명했듯이 방위사업청에서는 방산기술보호법을 제정하여 방산기술에 대한 보호체계 구축을 지원하고 있다. 방산기술보호법이 시행되면서 기존 방산보안에서의 '군사기밀보호' 위주의 보안정책에서 '방위산업기술' 유출을 방지하기 위한 정책이 포함되었고, 대상기관도 방산업체 뿐만 아니라 방위산업기술을 다루는 연구소・일반업체 등 관련된 제반 기관으로 보안정책의 확장이 되기 시작했다. (PARK, Heungsoon; GO, Heejae; HWANG, Jonghyeon., 2018)

방위산업기술 유출은 외부침입에 의한 유출과 전・현직 종사자에 의한 내부 기술유출이 있으며 최근에는 해킹에 의한 기술유출 등 사이버위협을 통한 방위산업 관련 업체 대상으로 증가하고 있다. 최근 국정원에 따르면 2018~2022년 국정원이 적발한 국내 산업기술 유출 사건은 93건으로 피해예방액은 25조 원(연구개발비와 예상 매출액을 반영해 추산)에 달하고 이 가운데 국가안보와 국민경제에 중대한 영향을 미치는 국가 핵심기술은 33건으로 1/3에 이른다고 밝혔다.[11] 이와 같이 해킹, 내부 기술유출 등이 심각한 수준이며, 방산기술 유출과 관련된 피해 사례는 다음과 같다.

11) "기술유출땐 피해 막대… 국회·정부 검토과정 협력해야", 디지털타임스, 2023. 8. 3.

가. □□청을 사칭한 이메일을 통한 해킹시도

2016년 5월 △△진흥회와 □□청을 사칭한 해킹 이메일이 국내 방위산업분야 업체 약 700여 곳에 발송되었고, '국내 방산전시회 참가 지원에 대한 설문조사'라는 제목으로 붙임 자료를 열람시 악성코드에 감염시켜 자료 유출을 시도하였으나 신속한 신고로 차단(해럴드경제, 2016. 5.13.)

나. 협력업체 퇴사자를 통한 방산기술 유출

○○항공의 협력업체에서 1년 이하 단기 직원으로 근무하였던 ○○○은 '22년 5월부터 약 한 달에 걸쳐 국산 헬리콥터 '○○○' 계기판 도면 등 영업비밀 12건을 반출한 뒤 퇴사한 혐의를 받고 불구속 송치(한국일보, 2023. 6. 7.)

다. 하도급업체 무선공유기를 통한 방산기술 유출

'13.11. 무인항공기 부품을 생산하는 방산관련 업체 임직원 □□□이 회사 방침을 준수하지 않고 개인 무선공유기를 무단반입한 후 무선 인터넷 공유기능을 이용, 개발 중인 UAV 설계도 수백 장을 아무런 통제 없이 외부로 유출(장경준, 2018 학술논문 인용)

라. 북한 정찰국 소행으로 추정되는 해킹

북한 정찰총국 소속으로 추정되는 해커들은 해군 수송함을 건조하는 OOO 중공업 대상으로 해군 함정 건조 설계도 등 각종 기밀자료가 들어있는 업무망 PC를 해킹하여 탈취(뉴데일리, 2020.12. 6.)

마. 외국 지사를 이용한 자료 유출

'13.10. OOO 방산업체의 중국지사에서 근무하고 있는 □□□가 북한에 포섭되어

해당 직원의 권한과 계정으로 VPN을 통해 1년간 200여 차례에 걸쳐 본사 전산망에 침투, 다량의 정보를 유출(장경준, 2018 학술논문 인용)

5. 방산업체의 보안환경

방위산업 업체는 무기체계를 통합하는 체계종합업체와 구성품을 생산하는 다수의 협력업체로 이루어져 있는데, 70%에 이르는 대부분의 업체는 중소기업이 차지하고 있다. 반면, 기술보호 역량은 상대적으로 취약하다. 대다수의 중소 방산업체는 열악한 환경과 예산 부족 등의 이유로 보안에 대한 투자를 꺼리고 있고 이로 인해 방산기술 보호 역량점수는 대기업에 비해 극도로 낮은 수준이다. 최근 중소벤처기업부에서 실시한 중소기업과 대기업간 기술보호 역량수준을 평가한 결과, 그림 3과 같이 대기업에 비해 약 56-70% 정도 수준을 유지하고 있다.[12)]

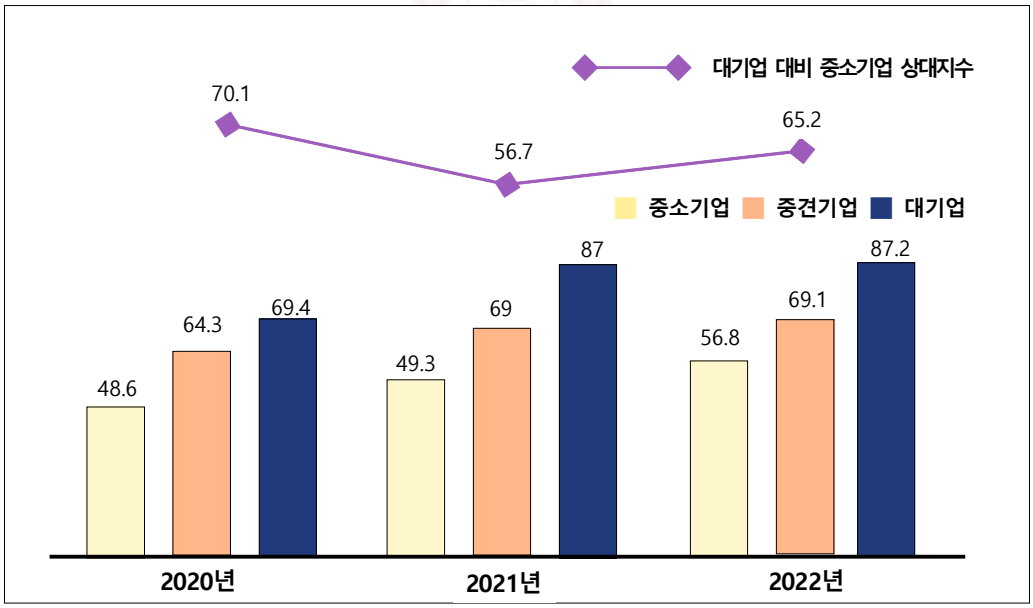


그림 3. 기업규모에 따른 기술보호 역량 수준
Figure 3. Level of technical protection capability by enterprise size
자료출처 : 중소기업 기술보호울타리 통계자료, 2023.

12) 중소벤처기업부 중소기업 기술보호울타리 기술보호수준 실태조사 현황, 2023

또한, 대부분의 업체 경영진에서는 보안에 대한 관심도 부족한 실정이다. 예산 부족도 있지만 단순히 지키는 업무라고 생각하는 인식이 만연되어 있다. AESRM에서는 2005년의 보고서에 이어 2007년에도 'The Convergence of Physical and Information Security In The Context Enterprise Risk Management'를 발표하였는데, 이 연구에서 기업의 경영진들은 보안을 기술적 기능으로만 여기고 상위 수준의 경영 프로세스나 의사결정에 필요한 기능으로는 여기지 않는다는 사실을 확인할 수 있었다.(Deloitte, 2007, 우광제, 2015 재인용.) 대부분의 경영진들은 보안을 자료와 자원을 보호하는 기술적 기능만으로 인식하는 실정이다. 기업의 70% 이상이 기술보안을 비생산적인 요소로 인식하고 있다.(김성훈, 2002, 연희모, 2013 재인용.)

앞에서도 설명했듯이 방위산업체는 방산물자의 안정적 생산을 위해서 일정한 수준의 시설기준뿐 아니라 보안요건을 갖추어야 한다. 방위산업체의 보안에 대한 최종 책임은 업체의 대표에게 있으며, 업체의 대표는 보안업무를 총괄하는 보안전담부서를 설치하거나 보안담담관을 임명하여 운용해야 한다. 주요방위산업체들은 상기 법령에 따라 대다수가 보안전담 부서를 두고 있으며 일반방위산업체는 인사나 총무부서에 전임보안담당관을 임명하고 있다. 주요방위산업체에 편성된 보안전담부서에는 보안실장, 기업보안담당, 정보통신보안담당으로 구분되어 진다. 보안실장은 업체에서의 보안업무를 총괄하며 기업보안담당과 정보통신보안담당을 통제한다. 기업보안담당은 보안실장을 도와서 인원보안・문서보안・시설보안・기업보안 등의 실무를 담당한다. 정보통신보안담당은 정보보호시스템 운용, 네트워크 보안관리 등 정보보호 업무를 수행한다. 일반방위산업체에서는 전담 보안담당관이 보안과 관련된 모든 업무를 담당하고 있다. 방위산업체별 보안전담 부서 편성과 보안실무자 운영 표준 모델은 그림 4와 같다.(우광제, 2014)

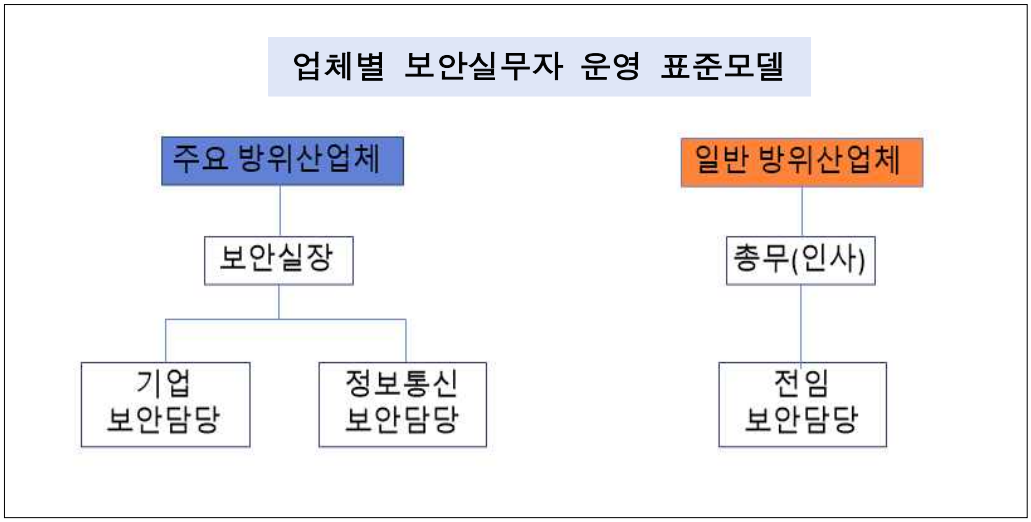


그림 4. 보안실무자 운영 표준모델
Figure 4. Security Practitioner Operational Standard Mode
자료출처 : 방위산업보안업무훈령, 우광제 학술논문(2014) 재인용.

최근 방위산업보안업무훈령에는 방산업체별 보안수준 분류 기준을 세부적으로 분류하고 있다. ○○○ 보안수준 요구업체, □□□ 보안수준 요구 업체, ◇◇◇◇ 보안수준 요구업체로 구분한다.[13] 세부내용은 비공개로 되어 있어 자세히는 밝힐 수 없으나, 대부분 업체는 상기 그림 4와 같이 운용되고 있고 일부 ○○○ 보안수준 업체에서는 △△보안 담당인원을 추가 채용하고 있다.

제2절 방산보안 관련 선행연구

국방부에서 1977년「방위산업보안업무시행규칙」을 제정한 이후 46년이라는 긴 역사를 가지나, 이러한 긴 역사에도 불구하고 보안상의 이유로 폐쇄적으로 운영되었기 때문에 학문적 연구가 거의 이루어지지 않았다.(류연승, 2018)

특히, 국방부・방첩사령부에서「방위산업보안업무훈령」을 외부로 공개하지 않다 보니 더더욱 학문적 연구가 제한이 되고 있고 세미나 참석도 특정인에 한정하여

13) 방위산업보안업무훈령 국방부훈령 제2422호

실시하다 보니 제도적, 물리적인 제한이 되는 실정이다.

반면, 2012년 이후부터 방산물자의 수출이 증가와 더불어 방산기술의 수준이 높아지면서 방위산업기술 보호에 대한 관심이 증가했고 방사청 방산기술통제관실이 신설되기도 했다. 2015년도에는 국군기무사령부(現 방첩사) 부설기관으로 국방보안연구소 조직에 '방산보안연구실'이 신설되면서 방위산업보안 분야에 대한 연구가 본격적으로 시작되었다. 한편, '방위산업기술 보호법'이 제정되면서 한국산업보안연구학회에 '방산보안연구회', 정보보호학회 산하에 '방위산업기술보호연구회'가 발족하는 등 학계뿐 아니라 다방면에서 관심이 증가하기 시작했다.(정보보호학회, 2020, 고희재, 2021 재인용.)

네이버 학술정보에서 키워드('방산보안') 검색을 하여 최근 10년간 학위·학술논문을 확인한 결과 표 2와 같이 총 184건이 수집되었다. 반면, 18년의 비교적 짧은 역사를 가지고 있는 산업보안 관련 연구는 학술논문 3,700여 건, 학위논문 2,400여 건의 검색되었다. 이와 같이 방위산업보안 분야에 대한 학계의 연구는 많이 부족한 실정이다.

표 2. 방위산업보안 관련 연구논문(14-23년)
Table 2. Research papers on defense industry security (14-23)
자료출처 : 네이버 학술정보검색, '23. 11. 1. 기준

구분	계	14년	15년	16년	17년	18년	19년	20년	21년	22년	23년
계	184	10	15	13	12	17	20	14	33	32	18
학위	35	3	5	1	1	1	7	3	3	6	5
학술	148	7	10	11	11	16	13	11	30	26	13

표 3은 방위산업보안 관련 주요 연구 논문으로 ① 보안환경의 변화 연구, ② 보안의식에 대한 제고, ③ 방위산업기술보호의 체계구축, ④ 방산보안관계자의 보안직무 등으로 분류하였다.

다수 논문들이 방위산업보안환경과 방위산업 기술보호체계에 대한 논문이며, 방산업체 보안전문가에 대한 직무연구는 융합보안 전문가, 정보통신 보안실무자 직무분석 외 확인된 것은 없었다.

표 3. 방위산업보안 관련 주요 연구논문 요약
Table 3. Summary of major research papers related to defense industry security
자료출처 : 고희재 학위 논문(2021) 참고

분야	저 자	연 구 내 용
보안 환경 변화	류연승(2018)	방산기술보호법이 제정된 이후를 '방산보안 2.0' 시대로 규정하면서 시대별 특징 비교 및 향후 발전 방향을 고찰
	고희재 등(2019)	방산기술보호법 제정으로 보안 영역 확장 등 환경의 변화에 따라 방위산업보안 개념 재정립
인식 제고	이형진(2016)	방산업체 대상 방산기술보호 교육 인식 제고를 위해 정부의 역할과 중소기업의 인식변화가 필요
	손창근(2018)	대상기관 중 하나인 각 군의 관련자를 대상으로 방산기술보호의 중요성 인식 제고를 위한 교육 발전 방안을 제시
보호 체계 구축	박흥순 등(2019)	방산기술보호지침의 자가진단 항목을 대상으로 한 우선 순위 분석 및 효율적 진단과 보호체계의 체계적인 구축방안 제시
	허아라(2018)	우리나라와 미국의 국가정보 분류체계를 비교·설명하면서, 방산기술정보 분류체계를 연구
	이승훈(2018)	대상기관에서 방위산업술 보호체계를 자율적으로 구축할 수 있도록 내규를 작성하고 자가진단 등의 시행 방안을 연구
	장경준(2018)	방산업체 망 분리 시스템의 문제점 분석 및 방산기술 유출 취약점과 유출 방지 대책 연구
	고희재(2021)	방위산업보안과 방위산업기술보호를 통합한 보안수준 평가 지표를 개발하고 평가 항목별 가중치와 우선순위 도출
보안 직무	우광제(2014)	데이컴 기법을 이용한 방위산업체 정보통신 보안실무자 직무분석을 통해 교육과정 개발 기초자료 제공
	우광제(2016)	융합보안 전문가인 방위산업체 보안전문가들의 직무를 규명하고, 직무수행에 필요한 핵심과업과 교육적 요구 분석

제3절 직무분석의 이해

1. 직무분석의 정의

국가공무원법 직무분석규정에서는 “해당 직위의 성과책임 규명, 직무평가 및 직무수행요건 규명 등 각종 직무정보를 체계적으로 수집·분석하는 모든 활동”이라고 정의하고 있다.[14]. 직무분석은 어떤 일을 어떤 목적으로 어떤 방법에 의해 어떤 장소에서 수행하는지를 알아내고, 직무를 수행하는 데 요구되는 지식, 능력, 기술, 경험, 책임 등이 무엇인지를 과학적이고 합리적으로 알아내는 것이라고 정의하고 있고 직무분석은 직무에서 수행하는 과제와 도구, 장비, 작업 요건과 같은 작업이 수행되는 상황, 그리고 작업 수행에 요구되는 인적 요건들에 관한 정보를 제공하고 이와 같은 자료들을 통해 많은 인사 결정에 필요한 기본적 정보를 제공하기 때문에 조직 내의 인적자원 관리의 가장 핵심적인 기능이며, 또한 출발점이라고 할 수 있다.[15]

2. 직무분석의 목적

직무분석을 위한 직무정보는 기업, 정부, 개인 및 조합 등에서 범위와 내용이 매우 광범위하고 다양하기 때문에 필요성에 따라 그 형태와 접근 방법이 다를 수밖에 없지만 궁극적인 목적에 관계없이 그 자료는 정확하고 모든 것을 포함해야 하며 연구 및 용도에 알맞은 형태로 소개되어야 한다. 이러한 정보를 획득하고 소개하는 기술이 곧 직무분석이다.(진기정, 2014)

직무분석은 직무특성에 관련된 여러 가지 수집된 중요한 정보를 각 직무에 관한 목적에 맞게 일치시키는 기술이다. 그리고 각 직무에서 요구하고 있는 지식, 기술, 특징, 자격요건 등 다른 직무와 구별되는 요소를 분명하게 하여 수행하는

14) 직무분석규정 대통령령 제2811호(2017)
15) 심리학용어사전, 한국심리학회, 2014. http://www.koreanpsychology.or.kr

일에 대해 상세하게 정보를 얻는 과정인 것이다.(McCormick, 1976 등 다수, 김수연, 2010 재인용.)

따라서, 직무분석의 목적은 실질적으로 직무 기술서(job description)나 작업자 명세서(worker specification)를 만들어 이로부터 얻어낸 정보를 여러모로 활용하는 것이다. 직무 기술서는 분석하려는 직무가 어떠한 활동이나 과제가 이루어지고 작업 조건이 무엇인지를 찾아내는 기술을 의미하며, 작업자 명세서는 직무를 수행하는 사람이 필요로 하는 지식이나 기술, 능력과 같은 인간적인 요건이 무엇인지를 명확히 기록하는 것으로 직무 기술서는 과제 중심 직무분석을 통해 작성되는 것이며, 작업자 명세서는 작업자 중심의 직무분석을 통해 작성되는 것이다. 직무 기술서는 직무 자체와 작업 환경에 관한 정보를 알려주는 것이기 때문에 직무의 파악에 활용이 되고, 작업자 명세서는 작업자에게 요구되는 인간적 요건을 알려주기 때문에 선발이나 교육과 같은 인적자원의 관리에 활용이 된다. 직무를 분석할 때는 직무 기술서와 작업자 명세서를 모두 작성하는 것이 일반적인 것이라 할 것이다.(심리학용어사전, 2014)

3. 직무분석 방법

직무 분석에서 직무에 대한 정보를 제공하는 가장 중요한 자원은 현업 전문가이다. 현업 전문가의 자격 요건은 명확하게 정해진 것은 없지만, 최소한 수행되는 직무에 대한 모든 과제를 이해하고 잘 알고 있을 정도의 충분한 오랜 경험을 갖고 최근에 종사한 사람이라고 되어 있다.(Thompson & Thompson, 1982) 따라서 직무를 분석할 때 가장 적절한 정보를 제공할 수 있는 사람은 현재 직무와 관련된 일을 하고 있는 현업 전문가이여야 하며, 특히 현재 직무에 종사하고 있는 현직자이다. 현직자는 자신들의 직무에 관해 가장 상세하게 알고 있기 때문이다. 하지만 모든 현직자들이 자신의 직무를 잘 표현할 수 있는 것은 아니므로

직무분석을 위해 정보를 잘 전달할 만한 사람을 선택해야 한다. 이와 같이 가장 적절한 것을 찾는 과정이 직무분석 방법이다. 직무분석 방법은 일반적으로 최초분석법, 비교확인법, 그룹 토의기법(데이컴법) 등이 있다. 참고할 자료가 풍부한 경우에는 비교확인법이 효율적이며 그룹토의 기법(데이컴법)은 직무분석 대상 직종에 관련된 전문가 집단이 모여서 일정 기간동안 발표, 토의, 정리를 거쳐 브레인스토밍을 통한 직무를 분석하는 방법이다.(강경종 등, 2001, 김수연, 2010, 문인수, 2022) 앞에서 언급한 최초분석법, 비교확인법, 데이컴법에 대해 자세히 알아보겠다.[16)]

가. 최초분석법은 조사할 직무 대상에 관한 참고문헌이나 자료가 없거나, 그 분야에 경험과 지식을 갖춘 사람이 적을 때 직접 작업현장을 방문하여 분석을 실시하는 것으로써 관찰법, 면접법, 체험법, 설문지법, 작업 일지법, 중요사건기록법(결정적 사건법) 등이 있다.

1) 관찰법은 분석자가 직접 직무정보를 수집하는 것으로 다른 사람에게 불편을 주지 않고 분석이 가능하며, 작업현장을 직접 확인하면서 실질적인 내용을 파악하기 때문에 정확한 결과물을 얻을 수 있으나, 직무의 시작에서 종료까지 많은 시간이 소요되는 직무에는 적용이 어렵고, 지적이거나 정신적, 감각적인 작업을 주로 하는 직무파악에는 제한이 된다. 특히, 분석자의 주관 개입의 가능성이 있을 수 있다.

2) 면접법은 직무에 관한 정확한 지식 확보가 가능하고, 다양한 직무들에 광범위하게 적용이 가능하나, 자료의 수집에 많은 시간과 노력이 필요하고, 수량화된 정보를 얻기는 제한된다.

16) 네이버블로그, https://blog.naver.com/zazayo90/222900003322

3) 체험법은 직무분석자의 직접적인 체험을 통해 현장의 생생한 직무분석 자료 획득이 가능하며, 직무활동에서의 의식의 흐름과 감각적인 내용 및 피로의 상태 등 내부 구조까지 분석이 가능한 면도 있으나, 분석자가 그 직무에 종사하고 있는 담당자의 심리상태에 도달하기가 어렵고, 분석자가 분석을 위해서는 많은 시간이 소요된다.

4) 설문지법은 양적인 정보를 얻을 수 있으며, 많은 사람들로부터 짧은 시간 내에 정보를 얻을 수 있는 장점이 있는 반면, 질문지 설계 및 작성이 어렵고 완전한 사실 파악이 제한되며, 응답자가 성실성이 부족시 회수율이 낮다.

5) 작업일지법은 일상적인 수행에 관한 정보를 수집하므로 해당 직무에 대한 포괄적인 정보 취득이 가능하고, 직무당사자의 전반적인 업무 흐름 파악이 되나, 작업자들의 문장력에 있어 개인차가 있기 때문에 사용이 어렵고 작업자가 의도적으로 왜곡되게 일지가 작성될 가능성도 있다.

6) 중요사건기록법(결정적 사건법)은 직무 행동과 직무성과 간의 관계를 직접적으로 파악할 수 있고 직무수행과 관련된 중요한 지식, 기술, 능력 등을 파악할 수 있으나, 응답자들이 과거에 일어났던 결정적 사건들을 회상할 때 그 사건을 왜곡할 가능성이 있고 일상적인 수행과 관련된 지식, 기술, 능력을 배제할 수 있어 정확한 조사를 위해 특별히 훈련받은 사람을 필요로 한다.

나. 비교확인법은 분석된 자료를 참고로 하여 현재의 직무 상태를 비교하여 확인하는 방법으로 기존 자료 분석시기와 현재 분석시기 간의 차이점을 발견하여 보완하고, 대상 직무에 대한 참고문헌과 자료가 충분한 경우에 널리 사용되는 직무분석법이다. 따라서, 직무의 폭이 상당히 넓어 단시간 내에 관찰을 통한 파악이 어려운 경우에 비교적 효과적이나, 비교확인법만으로는 안전한 분석이 어려워 다른 방법과 상호보완하는 것이 유효하다.(김수연, 2010)

다. 데이컴법(DACUM)은 교과과정을 새롭게 개발하는 데 활용되며, 교육훈련을 목적으로 교육목표와 교육내용을 비교적 단시간에 추출하는 데 효과적인 직무분석 방법으로써 주로 소집단의 브레인스토밍 기법을 활용한다.

제4절 직무분석 관련 선행연구

네이버 학술정보에서 검색한 결과 '직무분석'과 관련된 논문은 매년 50-80여편 이상이 작성되었으며, 다양한 분야와 직종에서 활발한 연구가 이루어지고 있었다. 다수의 논문에서는 DACUM 기법을 활용하여 직무분석을 하였고, 델파이 및 AHP기법을 활용한 방법, 중요도・난이도・수행도 분석, 빅데이터를 활용한 직무분석 등의 논문이 확인되었다. 직무분석과 관련된 주요 논문은 표 4와 같다.

표 4. 직무분석 관련 주요 연구논문 요약
Table 4. Summary of key research papers related to job analysis

분야	저 자	논 문 제 목 주 요 내 용
데이컴 기법	우광제(2014)	DACUM 기법을 이용한 방위산업체 정보통신보안실무자 직무분석
		DACUM을 활용, 정보통신보안실무자들의 책무와 과업을 도출하고, 설문조사를 통해서 도출된 과업에 대한 타당도와 신뢰도 검증
	우광제(2015)	융합보안전문가의 핵심과업 및 직무역량 요구분석
		DACUM 직무분석을 통해 융합보안전문가의 직무와 핵심과업을 도출 후, 설문조사를 실시하여 과업의 검증 및 핵심과업과 직무 역량에 대한 교육적 요구를 분석
	나재관(2022)	평생교육 관점에서 방과후학교 담당자의 직무분석 및 핵심역량 개발
		DACUM 직무분석을 통해 방과 후 학교 담당자에 대한 직무를 분석, 델파이 기법을 통해 책임과업과 핵심역량 도출 및 타당성 검증
델파이 / AHP	이민형 등(2015)	델파이 기법을 활용한 해양경비안전본부 직무분석
		전문가를 선정하여 예비조사를 실시, 직무를 식별하고, 델파이 조사를 통해 선정된 직무를 중심으로 적합성을 평가한 후 제2차 및 제3차 델파이 조사로 내용타당도 검증

	김선녀(2021)	델파이 기법과 계층적 의사결정방법(AHP)의 적용을 통한 병원 간호부서별 직무역량 평가지표 개발
		국가직무능력표준(NCS)의 직업기초능력 분류기준을 적용하여 병원 간호부서 직무역량의 개념 틀을 구성하고 델파이 기법으로 내용 타당도 검증 후 AHP 기법을 통해 가중치를 부여, 병원 간호 부서별 직무역량 평가지표와 간호부서별 직무역량 평가점수표 개발
중요도 난이도 수행도	정연희 등(2016)	DACUM기법을 이용한 한방간호사의 직무분석
		DACUM기법을 통해 한방간호사의 직무를 도출한 후 한방간호사 대상 설문을 통해 타당성을 검증 후 재차 한방간호사 대상 중요도, 난이도, 수행빈도 설문을 통해 수행작업표를 완성
	최정화 등(2019)	DACUM 기법을 이용한 영양사의 직무분석(중요도, 수행도, 난이도 분석)
		DACUM을 통해 영영사들의 직무를 도출한 후 설문을 통해 타당성 검증과 중요도, 난이도, 수행빈도를 분석하여 교육 과정 기초자료 활용
기타	박상호(2019)	빅데이터를 활용한 산업보안 전문인력 요구직무 분석
		문헌연구나 기존 방법과는 달리 빅데이터 기반의 텍스트마이닝 기법을 활용하여 대량의 산업보안 채용공고 내용을 분석하여 산업보안 전문인력에 대한 직무분석

2011년 발표한 '국내 직무분석에 관한 연구논문 분석: 2000년 이후 국내 학술지 발표 논문을 중심으로' 논문에서는 주로 DACUM과 설문조사 등 2가지 이상의 방법을 혼용한 연구가 대다수를 차지하였고, 직무분석 결과로 직무분석표, 직무명세서, 작업명세서의 순으로 나타났으며, 직무개편, 선발, 교육, 평가 등 다양한 분야에서 활용이 되고 있었으며 교육 프로그램 개발 및 개선을 제안한 연구가 상대적으로 높은 편이라고 기술하고 있다(조대연 등, 2011)

2019년 발표한 '국내 직무분석에 관한 체계적 문헌고찰: 2010년 이후 국내 학술지 발표 논문 중심으로' 논문에서도 직무분석 시 가장 많이 활용된 기법으로는 DACUM 기법이었으며, 대상은 공공교육 분야, 직무교육 분야, 의료분야로 구성되어 있었고 주요분석 내용은 직무 정의, 책무와 과업, 중요도 등이며 직무분석 연구 결과는 교육과정 개발 및 개선에 활용되고 있다고 언급하고 있다.(박현경; 양지희, 2019)

제3장 방산업체 보안전문가 직무 수집

제1절 지침 및 규정에 명시된 보안전문가 직무

방위산업보안업무훈령, 방위산업기술 보호지침, 산업보안관리사의 직무, 관련 선행 연구논문 등을 통해 확인된 직무는 아래와 같다.

1. 방위산업보안업무훈령에 명시된 직무

방위산업보안업무훈령에 명시된 보안전문가 직무는 보안실장(팀장), 기업보안 담당, 정보통신담당으로 구분되어 있으나, 비공개되어 있어 세부내용을 기술하기는 제한된다. 따라서, 기존 공개된 자료를 활용하여 방산업체 보안전문가들의 직무를 수집하였다. 즉, 기존 논문을 통해 확인된 자료 표 5는 방위산업보안업무훈령 체계이며, 표 6은 방산업체 보안측정 자가진단 요소로 상기 자료를 통해 방산업체 보안전문가의 직무를 유추해 나가겠다.

표 5. 방위산업보안업무훈령 체계
Table 5. Defense Industry Security Instruction System
자료출처 : 방위산업보안업무훈령, 고희재 학위 논문(2021) 재인용.

제 1장 총 칙	임무 및 보안책임
제 2장 문서보안	비밀생산, 비밀관리, 비밀파기
제 3장 인원보안	비밀취급인가, 신원조사, 보안관계관 운용
제 4장 시설보안	시설물보안, 출입/사진촬영
제 5장 정보통신보안	정보통신보안대책, 통신망이용 보안송수신, 정보시스템 보안관리, 네트워크 보안관리, 인터넷 보안관리, PC/주변장치 보안관리, 정보보호시스템 보안관리, 보안시스템 관리/운용
제 6장 기업보안	하도급보안, 기술개발보안, 외국인 보안관리, 수출, 수입/합작, 수송, 방산관련 보험
제 7장 보안조사	보안측정, 보안감사, 보안사고조사
제 8장 기타보안	비밀 제공/설명, 일반자료 관리, 회의시 보안, 보안교육, 보안행정, 보칙

표 6. 방산업체 보안측정 자가진단 요소
Table 6. Self-diagnosis factor for security measurement of defense industry
자료출처 : 방위산업보안업무훈령, 고희재 학위 논문(2021) 재인용.

분 야	평 가 항 목
문서보안	보안내규 작성
인원보안	신원조사
	보안관계관 운용
	퇴직자 및 외국인 고용 보안관리
시설보안	보호구역 설정 및 보호대책
	출입통제
	시설 보안대책
	방화 대책
정보통신보안	무선 LAN 관리
	디지털 복합기 관리
	네트워크 관리
	망 관련 보안대책
	전산자료 관리
	개인/휴대형 컴퓨터 관리
	보조기억매체 관리
	정보보호시스템 관리
기업보안	기술인력 보안대책
	하도급 보안대책
	보안사고 대응

2. 방위산업기술 보호지침에 명시된 직무

방위산업기술 보호지침에는 방산업체 보안실무자가 수행할 자가진단 및 실태조사 핵심 평가항목으로 표 7은 방위산업기술보호 자가진단표로 34개 항목으로 구성되어 있고, 통합실태조사 핵심 평가항목으로 총 63개 항목으로 구성되어 있다. 이 중 방산업체 보안전문가의 직무분석 시에는 실제 직무 수행자가 행동화 할 수 있는 요소인 자가진단표를 활용할 예정이다. 통합실태조사 핵심 평가항목은 보안전문가의 직무라기보다는 감사를 수행하는데 필요한 항목으로 볼 수 있기 때문이다.

표 7. 방위산업 기술보호 자가진단표 요약
Table 7. Defense Industry Technology Protection Self-Diagnosis Table Summary
자료출처 : 방위산업기술보호지침

구 분	점 검 항 목	
기술의 식별·관리 (10)	① 연간 시행계획의 수립·시행	② 내규 작성
	③ 기술보호책임자 임명	④ 기술보호교육 실시
	⑤ 심의회의 구성 및 운영	⑥ 기술 유출 및 침해 대응 준비
	⑦ 자가진단	⑧ 기술의 식별 및 등재
	⑨ 관리대상기술 취급·관리	⑩ 관리대상기술 공개 및 제공
인원통제 (6)	① 신원조사	② 방산기술취급인가자 보호대책
	③ 외부인 관리	④ 외국인 관리
	⑤ 외부인이나 외국인 관리	⑥ 해외 출장 시 보호대책
시설보호 (4)	① 기술보호구역의 설정·운영	② 기술보호구역 통제
	③ 정보통신장비 사용 통제	④ 외부인·외국인통제
정보보호 (9)	① 정보보호시스템 설치·운용	② 정보통신망 외부망과 차단
	③ 인터넷 관제	④ 사이버 침해사고 예방·복구
	⑤ 정보통신망 원격 관리	⑥ 정보통신 및 저장매체 관리
	⑦ 관리대상기술 접근 제한	⑧ 전산자료 반출 관리
	⑨ 자료유출 관리 및 대응	
연구개발 기술보호 (5)	① 개발성과물 보호 관리	② 연구개발사업 보호 활동
	③ 수출 및 국내이전시 보호	④ 합작·기술제휴 기술보호
	⑤ 방산협력업체 기술보호	

3. 산업보안관리사의 직무

산업보안관리사는 산업현장에서 기술유출을 방지하기 위한 산업보안 활동의 일환으로, 현장에서의 보호 가치대상(인력·관리, 설비·구역, 정보·문서 등)을 내·외부 위해요소로부터 침해받지 않도록 예방·관리 및 대응하는 역할을 수행하는 전문가로서 국가공인 산업보안관리사 자격검정시험은 첨단산업기술의 유출방지 및 보호를 위해 산업현장에서 필요로 하는 산업보안 전문인력의 역량 검증을 위한 자격제도이다. 산업보안관리사의 직무는 총 5단계로 이루어지며, 1단계는 보안 요구사항 분석 및 보안관리 체계화를 통한 보안정책 수립단계, 2단계는 영역별 보안 실무 계획작성 단계, 3단계는 보안 취약점 점검으로 보안 위협 요소 등의 취약사항 모니터링 및 인지하는 단계, 4단계는 보안 취약점 등의 위기 대응 및 업무지속성 관리 단계, 5단계는 보안 관련 정보 및 상담 교육 등의 서비스를 제공하는 단계로 이루어 진다.

산업보안관리사 시험은 관리적보안, 물리적보안, 기술적보안, 보안사고 대응, 보안지식경영으로 이뤄지고 있다. 따라서 산업보안관리사는 표 8에서와 같은 직무를 수행하고 있다고 유추할 수 있다.[17]

표 8. 산업보안관리사 직무
Table 8. Job of Industrial security manager
자료출처 : 산업보안관리사 공식 홈페이지

산업보안관리사 직무	
정책수립	보안요구사항 분석
	보안정책 수립
보안실무계획	보안실무계획 작성
	보안행정업무
보안취약점 점검	취약점 모니터링
	취약지 점검
보안사고대응	위기 대응(백업시스템 유지)
	업무지속성 관리
보안서비스	보안교육/상담
	제반 보안업무 지원

17) 산업보안관리사 홈페이지, https://license.kaits.or.kr/certificate/introduce.do

제2절 선행 연구에서 수집한 방산업체 보안전문가 직무

2014년 발표한 'DACUM 기법을 이용한 방위산업체 정보통신보안실무자 직무분석'(우광제, 2014)에서 정보통신보안실무자의 직무를 확인한 결과 7개의 책무와 73개의 과업을 제시하였다. 이는 방산업체 보안전문가에 대한 직무라기 보다는 정보통신보안실무자의 직무이다. 세부직무는 표 9와 같다.

표 9. 정보통신보안실무자 직무분석 요약
Table 9. Information and Communication Security Operators Job Analysis Summary
자료출처 : 우광제 박사학위 논문(2014)

책 무	과 업	책 무	과 업
정보통신 보안대책 (계획) 수립	정보통신 보안대책 검토 등 10개 과업	정보통신 보안시스템 (보안솔루션) 관리	보안시스템 도입 소요 판단 등 15개 과업
정보시스템 (네트워크) 보안관리	사용자 계정 관리하기 등 10개 과업	핵심기술 및 저장매체 관리	보호대상 핵심기술(도면) 선정 등 10개 과업
상용정보 통신망 (인터넷) 보안관리	상용정보통신망 보안측정 등 10개 과업	개인용 컴퓨터(PC) 보안관리	필수 보안프로그램 배포/설치 등 10개 과업
휴대 / 사무형 정보통신장비 보안관리	정보통신장비 등록 관리 등 8개 과업		

이 중 방산업체 보안전문가의 직무는 책무부분이 해당되며, 과업은 실무자인 정보통신보안담당자가 수행하는 직무로 보면 된다. 따라서, 향후 방산업체 보안전문가 직무는 ① 정보통신보안대책(계획) 수립, ② 정보통신 보안시스템(보안솔루션) 관리, ③ 정보시스템(네트워크) 보안관리, ④ 핵심기술(도면) 전사자료 및 저장매체 관리, ⑤ 상용정보통신망(인터넷) 보안관리, ⑥ 개인용 컴퓨터(PC) 보안관리, ⑦ 휴대/사무형 정보통신장비 보안관리를 포함시킬 예정이다.

2016년 발표한 ‘융합보안전문가의 핵심과업 요구분석’(우광제, 2016) 에서는 DACUM 기법을 활용하여 방산업체 보안실무자들을 융합보안 측면에서 해당 직무를 분석하였다. 융합보안 측면에서 7개의 책무와 49개의 과업으로 분류하였고 주요 책무는 ① 보안행정, ② 비밀관리, ③ 인원보안, ④ 시설/장비보안, ⑤ 정보통신보안, ⑥ 보안교육, ⑦ 보안감사/조사로 구분하였고, 세부 과업은 표 10과 같다.

표 10. 융합보안전문가의 직무분석 요약
Table 10. Summary of job analysis by convergence security professionals
자료출처 : 우광제 학술논문(2016)

책 무	과 업	책 무	과 업
보안행정 (8)	중장기 보안계획 수립 연간 보안업무계획 수립 보안내규 작성(개정) 보안일일결산 감독 보안수준 평가 회의시 보안조치 하도급 보안관리 수출입 보안조치	비밀관리 (7)	보호대상 비밀 지정 비밀 생산 보안조치 비밀소유조사/재분류 비밀 보관/관리실태 확인 대외발송자료 보안성 검토 비밀 저장매체 관리 비밀 안전조치
인원보안 (8)	보안관계관 운용 직원 신원조사업무 처리 보안서약서 집행/관리 비밀취급인가업무 처리 개인정보보호업무 처리 핵심기술인력 보호 외국인(직원) 보안관리 퇴직자 보안조치	시설/장비 보안 (9)	보호구역(시설) 설정 시설/장비 보호대책 구축 출입통제시스템 운용 출입증 관리 사진촬영(녹음) 통제 비인가자 접근/출입 통제 외래인 출입시 보안조치 장비 수송시 보안조치 유사시 안전조치
정보통신 보안 (8)	주전산기(서버) 보안관리 네트워크 보안관제 정보보호시스템 보안관제 정보통신 저장매체 관리 개인용컴퓨터 보안관리 사무장비 보안관리 협력업체 시스템 보안관리 보안관제결과(해킹) 조치	보안교육 (4)	보안교육계획 수립하기 주제/대상별 교안 작성 보안교육 실시 교육성과 분석
		보안감사 /조사 (5)	보안측정 의뢰/결과 조치 부서/계열사 보안감사 정기/수시 보안점검 보안사고 조사/조치 중앙보안감사 수검

제4장 연구방법 설계 및 설문조사

제1절 연구방법 수행절차

1. 연구 대상

연구대상은 500여 개 방산업체 중 표 11에서와 같이 한국방위산업진흥회에서 현황을 유지하고 있는 83개 방산업체에서 근무하고 있는 보안전문가의 직무에 대해 중요도·난이도·수행빈도의 평균값을 구한 후 IPA 분석기법을 활용하여 과학적 기초자료를 제공할 계획이다.

표 11. 방위산업체 분야별 현황
Table 11. State of Defense Industry by Sector
자료출처 : 한국방위산업진흥회 통계자료(2023.10.16.기준)

분 야	계	화력	탄약	기동	항공유도	함정	통신전자	화생방	기타
주 요 방산업체	65	7	7	12	13	7	10	3	6
일 반 방산업체	18	1	2	2	3	1	6	0	3
총 계	83	8	9	14	16	8	16	3	9

2. 연구수행 절차

연구수행 절차는 표 12와 같이 예비직무 → 1차 설문조사 → 2차 설문조사 → 3차 설문조사 → 분석(종합적 결론) 순으로 진행한다. 예비직무 단계에서는 방위산업보안업무훈령, 방위산업기술 보호지침, 산업보안관리사 직무, 선행 연구한 논문을 참고문헌으로 활용하여 상호 자료를 비교확인하는 방법(직무분석 중 비교확인법)으로 방산업체 보안전문가의 예비직무를 산출한다.

1차 설문조사 단계에서는 산출한 예비직무를 설문지로 구성하여 방산분야 보안전문가 11에게 제공, 델파이 기법을 통해 동의여부를 수렴한다.

표12. 연구방법 수행절차

Table 12. Procedures for carrying out research methods

연구수행 절차		연구수행 방법
연구 방법	예비직무	• 직무분석 중 비교확인법을 활용, 보안전문가 예비직무 산출 • 방산보안업무 훈령 등 지침 + 선행연구논문을 기초로 검증
	1차 설문조사	예비직무에 대한 동의여부 설문 • 산출한 예비직무를 사전 제공하고 동의여부를 문의 • 방산분야 보안전문가(11명)를 섭외, 델파이기법으로 시행
	2차 설문조사	1차 설문 결과 합의를 위한 설문 • 1차 설문결과를 방산보안 전문가(11명)에게 제공, 직무 확정 • 삭제, 통합, 추가된 직무와 합의율을 제공하여 동의여부 확인
	3차 설문조사	확정 직무에 대한 본 설문 • 확정된 각 직무에 대해 중요도, 난이도, 수행빈도 평가(5점 척도) • 방산보안 현장실무·전문가 등 40여 명 대상 설문 조사
종합적 결론		• 중요도, 난이도, 수행빈도 평균값 도출, IPA방법 분석 • 향후 연구 방향을 포함한 정책적 제언

2차 설문조사 단계에서는 1차 설문결과를 종합하여 삭제, 통합, 추가 직무에 대한 항목을 만들고, 방산분야 보안전문가 11명에게 재발송하여 1차 설문결과에 대한 합의(동의)를 실시한다. 동의가 이루어지지 않을 경우 다시 환류하여 합의 과정을 반복하고 최종 방산업체 보안전문가의 직무를 확정한다.

3차 설문조사 단계에서는 확정된 각 직무에 대해 방산보안 현장실무·전문가 40여 명 대상으로 중요도·난이도·수행빈도를 5점 리커트 척도 설문조사를 실시하여 평가하고, 설문조사 시 방산보안분야 애로·건의사항을 병행 수집한다.

분석(종합적 결론) 단계에서는 설문조사를 통해 수집된 중요도・난이도・수행빈도의 평균 값을 엑셀(EXEL)로 구한 후 IBM SPSS 통계프로그램을 활용, IPA 방법을 통해 분석을 한다.

제2절 측정방법 및 분석도구

1. 델파이 기법

전문가 집단토의의 경우 발생하는 약점을 극복하기 위해서 개발된 전문가들의 의견을 종합하는 기법으로 '전문가 합의법'이라고도 한다. 델파이라는 용어는 아폴론 신전이 있던 고대 그리스의 도시 델포이(Delphoe)의 아폴론 신전에서 예언가들이 모여 미래를 점치던 것에서 유래했다고 전해진다.[18)]

집단의 의견들을 조정 및 통합하거나 개선시키기 위한 방법으로 1948년 미국의 랜드연구소에서 개발되었고, IT・교육・군사・연구개발 분야 등에서 주로 활용되고 있다. 델파이는 응답자의 익명성을 보장하고 그림 5와 같이 반복적인 환류작업을 통하여 전문가들의 합의를 통하여 새로운 아이디어를 만들어 내고, 이러한 반복적인 피드백을 통하여 하향식 의견 도출을 통해 문제를 해결하는 방식이다. (최용석; 백승철; 권혁인, 2018, 나무위키)

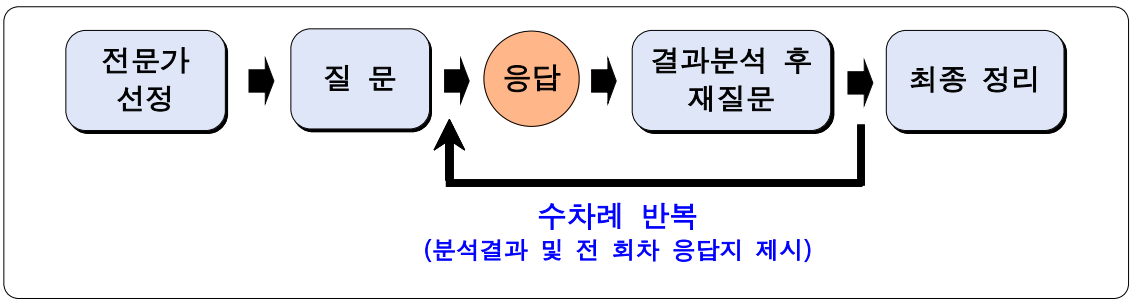


그림 5. 델파이 기법 수행 절차
Figure 5. Procedures for performing Delphi techniques
자료출처 : 델파이 기법 절차(나무위키)

18) 교육학용어사전, 서울대학교 교육연구소, 1995. / 나무위키

2. IPA 분석

IPA(Importance-Performance Analysis)는 기업 혹은 고객이 제품과 서비스의 각 속성에 대한 상대적 중요도와 수행도(만족도)를 메트릭스로 상호 우선순위를 비교・분석하여 최종 결정하는 평가방법이다.(Martilla,J.& James,J.C, 1977) IPA 분석은 중요도와 수행도를 측정한 후 개선 방향성과 우선순위 등을 결정할 수 있는 기법으로 Martilla와 James(1977)에 의해서 처음으로 구현되었다. IPA 분석은 적용되는 분야에 따라 수행도(performance)를 대신하여 만족도(satisfaction)로 활용되기도 한다.(임성근; 소순창; 이창섭, 2017)

IPA 분석은 주로 마케팅 분야에서 특정 제품에 대한 고객의 만족도를 파악하기 위하여 폭넓게 활용되었으며, 그 외 사회복지, 교육학, 정책학, 그리고 행정학 등에서 제도 및 정책에 대한 만족도를 측정하기 위하여 활용되기고 한다. IPA 분석은 그림 6과 같이 각 요소별 수집한 설문지의 각 요소별 중요도 및 수행도의 평균을 산출하고, IPA 매트릭스를 시각화한 후 각 사분멸 우선순위 해석의 절차를 거친다.[19]

IPA 매트릭스는 평가요소인 중요도와 수행도를 통하여 2차원 도면상에서 표기하고, 그 위치에 따라서 새롭게 의미를 부여하는 것으로 중심점을 기준으로 나누어진 4사분면에 대해 '유지', '집중', '저순위', '과잉'으로 표시하여 실무자들이 쉽게 결과를 파악할 수 있게 하는 분석기법인 것이다. IPA 메트릭스의 형태는 다음 그림 7과 같다.(이을지, 2016, 임성근; 소순창; 이창섭, 2017, 문인수, 2022)

19) 네이버블로그, https://blog.naver.com/accept119/223064198001, 중요도-수행도 분석

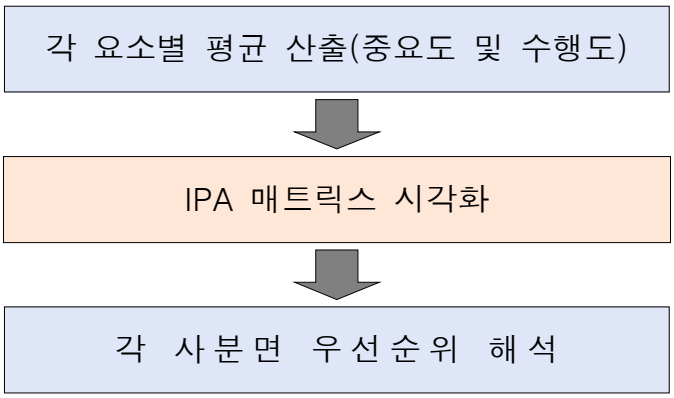


그림 6. IPA 분석 절차
Figure 6. IPA Analysis Procedure

중요도 ↑ 높음	제 2사분면 (concentrate here)	제 1사분면 (keep up the good work)
	집중 영역 (높은 중요도 - 낮은 만족도)	유지 영역 (높은 중요도 - 높은 만족도)
	제 3사분면 (low priority)	제 4사분면 (possible overkill)
낮음 ↓	저순위 영역 (낮은 중요도 - 낮은 만족도)	과잉 영역 (낮은 중요도 - 높은 만족도)

← 낮 음 만 족 도 높 음 →

그림 7. 각 사분면 IPA 매트릭스 분석
Figure 7. Analysis of each quadrant IPA matrix
자료출처 : Martilla,J.& James(1977), 이을지(2016), 문인수(2022) 재인용.

다음 표 13은 Martilla,J.& James(1977)의 IPA 분석 기법을 방산업체 보안전문가의 직무분석에 활용하고자 연구자가 수정하여 정리하였다.(이을지, 2016 참고하여 수정)

표 13. 연구자가 수정한 각 사분면 IPA 매트릭스 분석
Table 13. Analysis of each quadrant IPA matrix modified by the researcher

중요도-수행빈도 IPA 분석	↑ 높음 중요도 낮음 ↓ 제 2사분면: (현상 유지) 제 1사분면: (지속 개발) 인력 충원 제 3사분면: (낮은 우선순위) 인원 재판단 제 4사분면: (과잉노력 지양) 선택적 인력 충원 ← 낮 음 수 행 빈 도 높 음 →
중요도-난이도 IPA 분석	↑ 높음 중요도 낮음 ↓ 제 2사분면: (현상 유지) 제 1사분면: (역량개발 집중) 전문교육/시간증편 제 3사분면: (낮은 우선순위) 자체교육 <전문교육 불필요> 제 4사분면: (선택적 역량개발) 선택적 교육 ← 낮 음 난 이 도 높 음 →
(중요도+난이도)/2-수행빈도 IPA 분석	↑높음 (중요도+난이도)/2 낮음 ↓ 제 2사분면: (현상 유지) 제 1사분면: (지속 개발) 평가시 가중치 상향 제 3사분면: (낮은 우선순위) 평가시 가중치 하향 제 4사분면: (현상유지) ← 낮 음 수 행 빈 도 높 음 →

3. 분석 도구

방산업체 보안전문가 직무의 각 요소별 중요도·난이도·수행빈도의 평균값과 분산에 대해서는 엑셀(EXEL) 프로그램을, 각 요소에 대한 Cronbach'α 값(신뢰도), IPA 분석 및 4사분면 도표 작성에는 IBM SPSS statistics 23 통계 프로그램 도구를 활용하여 구현하겠다.

제3절 방산업체 보안전문가 예비직무 산출

방산업체 보안전문가의 예비직무는 그림 8과 같이 방위산업보안업무훈령, 방위산업기술 보호지침, 산업보안관리사 직무, 선행연구 논문을 비교확인법을 통해 산출하였다.

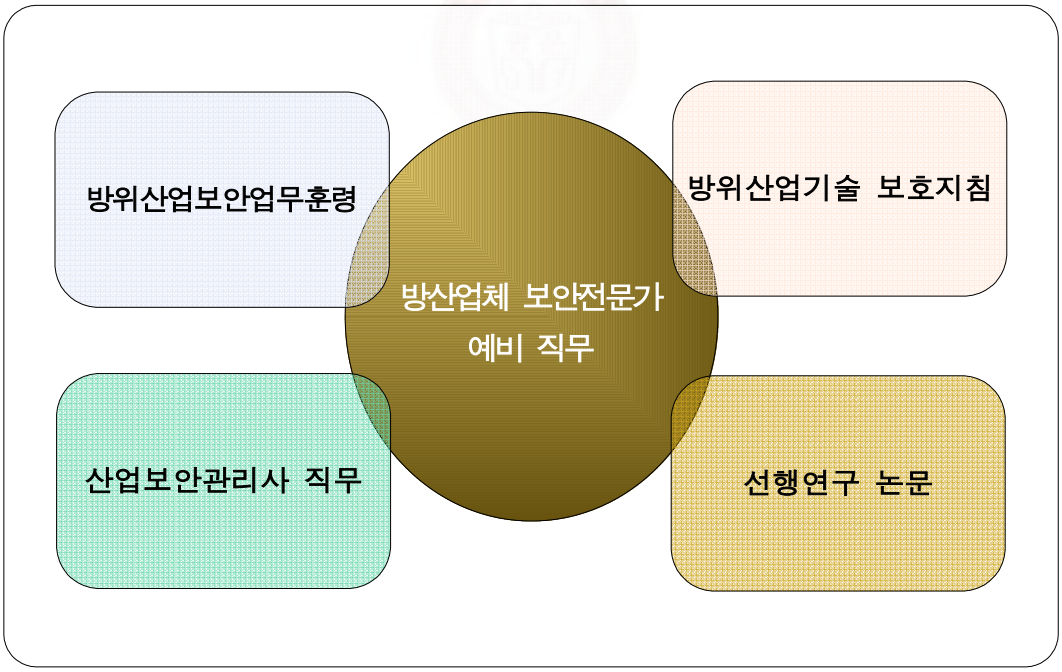
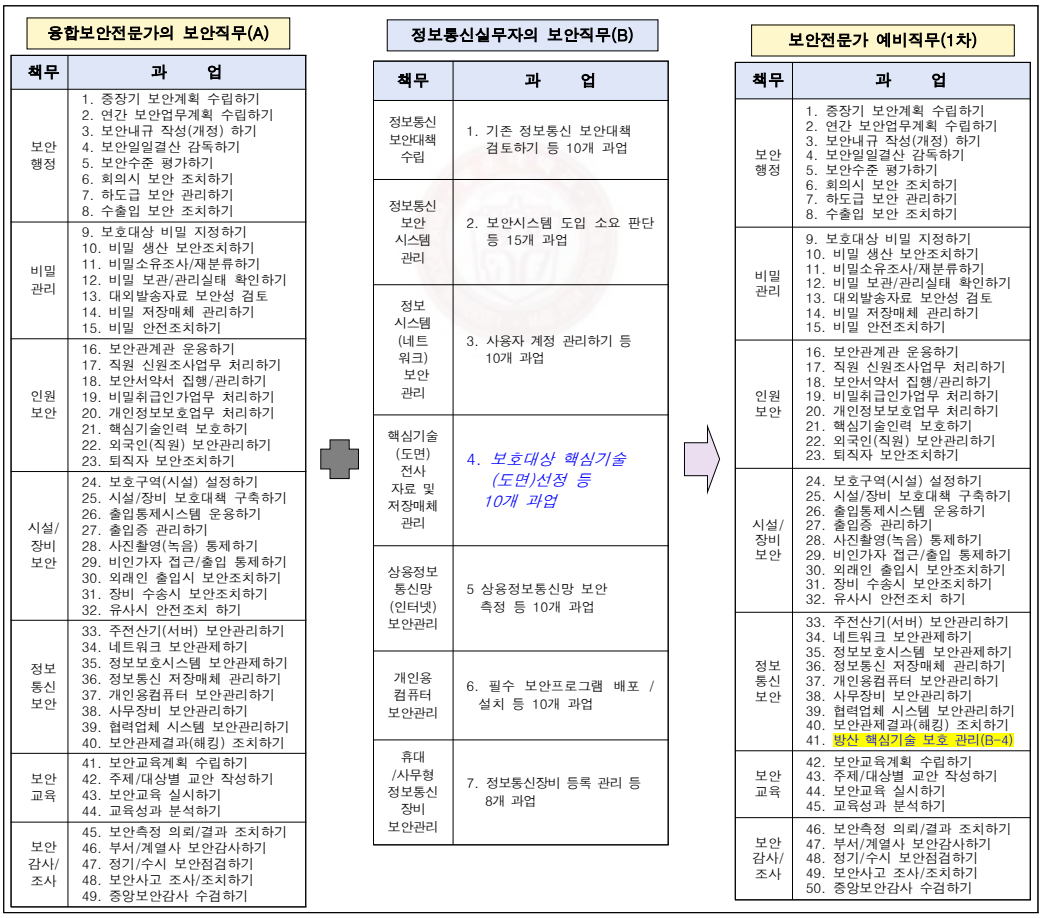


그림 8. 방산업체 보안전문가 예비직무 산출 모델
Figure 8. Model of preliminary job calculation for security experts in defense industry

우선, 연구자의 방산업체 보안전문가의 직무와 가장 근접한 우광제(2016) 논문의 ‘융합보안전문가’의 직무를 기준으로 ① 동 연구자가 제시한 정보통신보안실무자의 직무, ② 방산업무보안업무훈령에 명시한 직무, ③ 방위산업기술 보호지침에 명시한 자가진단표, ④ 산업보안관리사 직무 순으로 비교확인법에 의거 예비직무를 산출하겠다. 그림 9는 융합보안전문가(A)와 정보통신실무자의 직무(B)를 비교한 자료이다. 정보통신실무자 직무 대부분이 융합전문가의 정보통신보안 직무에 포함되고 있어 ‘방산 핵심기술 보호관리(B-4)’ 직무만을 추가하였다.



융합보안전문가의 보안직무(A)

책무	과 업
보안 행정	1. 중장기 보안계획 수립하기 2. 연간 보안업무계획 수립하기 3. 보안내규 작성(개정) 하기 4. 보안일일결산 감독하기 5. 보안수준 평가하기 6. 회의시 보안 조치하기 7. 하도급 보안 관리하기 8. 수출입 보안 조치하기
비밀 관리	9. 보호대상 비밀 지정하기 10. 비밀 생산 보안조치하기 11. 비밀소유조사/재분류하기 12. 비밀 보관/관리실태 확인하기 13. 대외발송자료 보안성 검토 14. 비밀 저장매체 관리하기 15. 비밀 안전조치하기
인원 보안	16. 보안관계관 운용하기 17. 직원 신원조사업무 처리하기 18. 보안서약서 집행/관리하기 19. 비밀취급인가업무 처리하기 20. 개인정보보호업무 처리하기 21. 핵심기술인력 보호하기 22. 외국인(직원) 보안관리하기 23. 퇴직자 보안조치하기
시설/ 장비 보안	24. 보호구역(시설) 설정하기 25. 시설/장비 보호대책 구축하기 26. 출입통제시스템 운용하기 27. 출입증 관리하기 28. 사진촬영(녹음) 통제하기 29. 비인가자 접근/출입 통제하기 30. 외래인 출입시 보안조치하기 31. 장비 수송시 보안조치하기 32. 유사시 안전조치 하기
정보 통신 보안	33. 주전산기(서버) 보안관리하기 34. 네트워크 보안관제하기 35. 정보보호시스템 보안관제하기 36. 정보통신 저장매체 관리하기 37. 개인용컴퓨터 보안관리하기 38. 사무장비 보안관리하기 39. 협력업체 시스템 보안관리하기 40. 보안관제결과(해킹) 조치하기
보안 교육	41. 보안교육계획 수립하기 42. 주제/대상별 교안 작성하기 43. 보안교육 실시하기 44. 교육성과 분석하기
보안 감사/ 조사	45. 보안측정 의뢰/결과 조치하기 46. 부서/계열사 보안감사하기 47. 정기/수시 보안점검하기 48. 보안사고 조사/조치하기 49. 중앙보안감사 수검하기

정보통신실무자의 보안직무(B)

책무	과 업
정보통신 보안대책 수립	1. 기존 정보통신 보안대책 검토하기 등 10개 과업
정보통신 보안 시스템 관리	2. 보안시스템 도입 소요 판단 등 15개 과업
정보 시스템 (네트워크) 보안 관리	3. 사용자 계정 관리하기 등 10개 과업
핵심기술 (도면) 전사 자료 및 저장매체 관리	*4. 보호대상 핵심기술 (도면)선정 등 10개 과업*
상용정보 통신망 (인터넷) 보안관리	5 상용정보통신망 보안 측정 등 10개 과업
개인용 컴퓨터 보안관리	6. 필수 보안프로그램 배포 / 설치 등 10개 과업
휴대 /사무형 정보통신 장비 보안관리	7. 정보통신장비 등록 관리 등 8개 과업

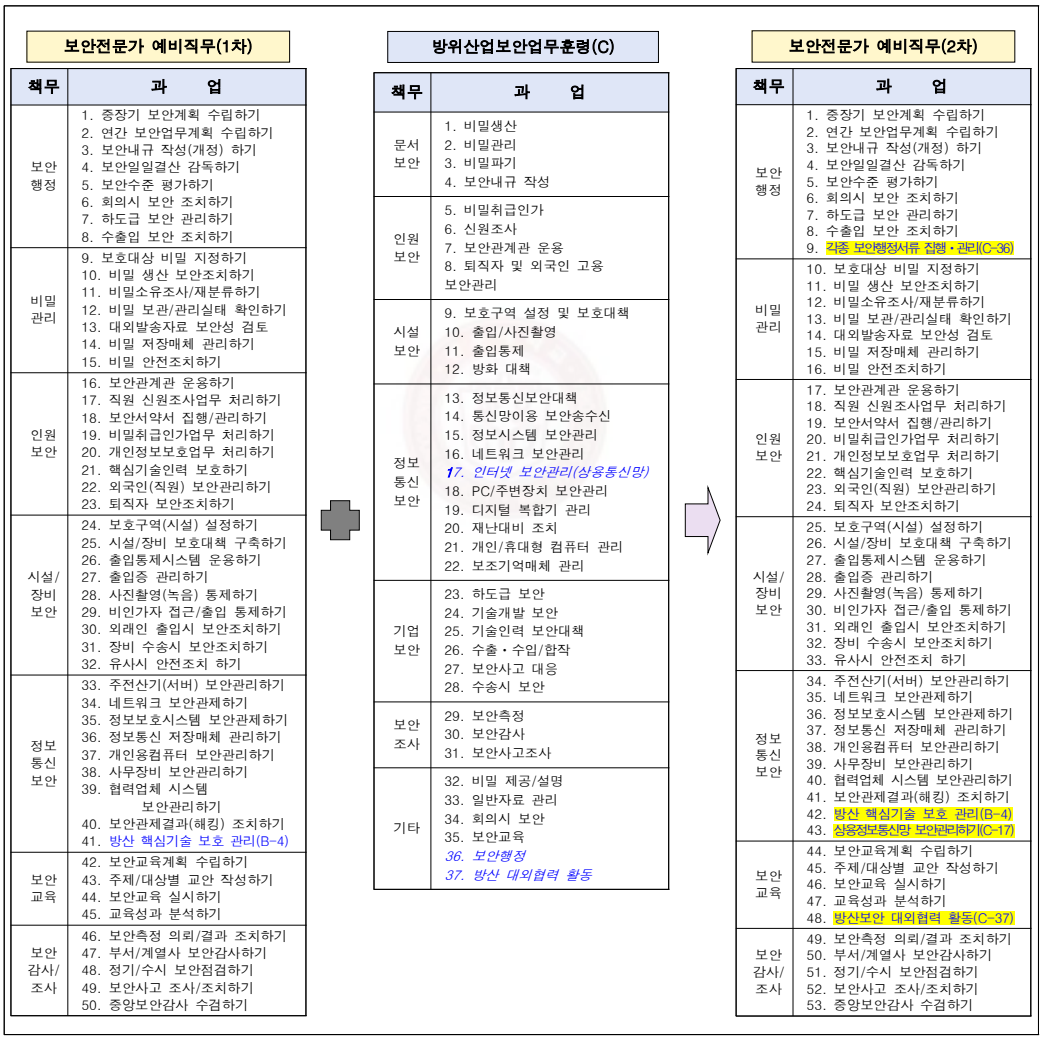
보안전문가 예비직무(1차)

책무	과 업
보안 행정	1. 중장기 보안계획 수립하기 2. 연간 보안업무계획 수립하기 3. 보안내규 작성(개정) 하기 4. 보안일일결산 감독하기 5. 보안수준 평가하기 6. 회의시 보안 조치하기 7. 하도급 보안 관리하기 8. 수출입 보안 조치하기
비밀 관리	9. 보호대상 비밀 지정하기 10. 비밀 생산 보안조치하기 11. 비밀소유조사/재분류하기 12. 비밀 보관/관리실태 확인하기 13. 대외발송자료 보안성 검토 14. 비밀 저장매체 관리하기 15. 비밀 안전조치하기
인원 보안	16. 보안관계관 운용하기 17. 직원 신원조사업무 처리하기 18. 보안서약서 집행/관리하기 19. 비밀취급인가업무 처리하기 20. 개인정보보호업무 처리하기 21. 핵심기술인력 보호하기 22. 외국인(직원) 보안관리하기 23. 퇴직자 보안조치하기
시설/ 장비 보안	24. 보호구역(시설) 설정하기 25. 시설/장비 보호대책 구축하기 26. 출입통제시스템 운용하기 27. 출입증 관리하기 28. 사진촬영(녹음) 통제하기 29. 비인가자 접근/출입 통제하기 30. 외래인 출입시 보안조치하기 31. 장비 수송시 보안조치하기 32. 유사시 안전조치 하기
정보 통신 보안	33. 주전산기(서버) 보안관리하기 34. 네트워크 보안관제하기 35. 정보보호시스템 보안관제하기 36. 정보통신 저장매체 관리하기 37. 개인용컴퓨터 보안관리하기 38. 사무장비 보안관리하기 39. 협력업체 시스템 보안관리하기 40. 보안관제결과(해킹) 조치하기 41. 방산 핵심기술 보호 관리(B-4)
보안 교육	42. 보안교육계획 수립하기 43. 주제/대상별 교안 작성하기 44. 보안교육 실시하기 45. 교육성과 분석하기
보안 감사/ 조사	46. 보안측정 의뢰/결과 조치하기 47. 부서/계열사 보안감사하기 48. 정기/수시 보안점검하기 49. 보안사고 조사/조치하기 50. 중앙보안감사 수검하기

그림 9. 보안전문가 예비직무 1차 종합

Figure 9. 1st round of preliminary jobs for security experts

1차 종합한 예비직무를 토대로 방위산업보안업무훈령(C)에 명시된 주요 보안업무를 비교하여 2차 보안 예비직무를 그림 10과 같이 도출하였다. 방산보안업무훈령에 명시된 '상용정보통신망 보안관리(C-17)', '각종 보안행정서류 집행・관리(C-36)', '방산보안 대외협력활동(C-37)'을 추가하였다.



보안전문가 예비직무(1차)

책무	과 업
보안 행정	1. 중장기 보안계획 수립하기 2. 연간 보안업무계획 수립하기 3. 보안내규 작성(개정) 하기 4. 보안일일결산 감독하기 5. 보안수준 평가하기 6. 회의시 보안 조치하기 7. 하도급 보안 관리하기 8. 수출입 보안 조치하기
비밀 관리	9. 보호대상 비밀 지정하기 10. 비밀 생산 보안조치하기 11. 비밀소유조사/재분류하기 12. 비밀 보관/관리실태 확인하기 13. 대외발송자료 보안성 검토 14. 비밀 저장매체 관리하기 15. 비밀 안전조치하기
인원 보안	16. 보안관계관 운용하기 17. 직원 신원조사업무 처리하기 18. 보안서약서 집행/관리하기 19. 비밀취급인가업무 처리하기 20. 개인정보보호업무 처리하기 21. 핵심기술인력 보호하기 22. 외국인(직원) 보안관리하기 23. 퇴직자 보안조치하기
시설/ 장비 보안	24. 보호구역(시설) 설정하기 25. 시설/장비 보호대책 구축하기 26. 출입통제시스템 운용하기 27. 출입증 관리하기 28. 사진촬영(녹음) 통제하기 29. 비인가자 접근/출입 통제하기 30. 외래인 출입시 보안조치하기 31. 장비 수송시 보안조치하기 32. 유사시 안전조치 하기
정보 통신 보안	33. 주전산기(서버) 보안관리하기 34. 네트워크 보안관제하기 35. 정보보호시스템 보안관제하기 36. 정보통신 저장매체 관리하기 37. 개인용컴퓨터 보안관리하기 38. 사무장비 보안관리하기 39. 협력업체 시스템 보안관리하기 40. 보안관제결과(해킹) 조치하기 41. 방산 핵심기술 보호 관리(B-4)
보안 교육	42. 보안교육계획 수립하기 43. 주제/대상별 교안 작성하기 44. 보안교육 실시하기 45. 교육성과 분석하기
보안 감사/ 조사	46. 보안측정 의뢰/결과 조치하기 47. 부서/계열사 보안감사하기 48. 정기/수시 보안점검하기 49. 보안사고 조사/조치하기 50. 중앙보안감사 수검하기

방위산업보안업무훈령(C)

책무	과 업
문서 보안	1. 비밀생산 2. 비밀관리 3. 비밀파기 4. 보안내규 작성
인원 보안	5. 비밀취급인가 6. 신원조사 7. 보안관계관 운용 8. 퇴직자 및 외국인 고용 보안관리
시설 보안	9. 보호구역 설정 및 보호대책 10. 출입/사진촬영 11. 출입통제 12. 방화 대책
정보 통신 보안	13. 정보통신보안대책 14. 통신망이용 보안송수신 15. 정보시스템 보안관리 16. 네트워크 보안관리 *17. 인터넷 보안관리(상용통신망)* 18. PC/주변장치 보안관리 19. 디지털 복합기 관리 20. 재난대비 조치 21. 개인/휴대형 컴퓨터 관리 22. 보조기억매체 관리
기업 보안	23. 하도급 보안 24. 기술개발 보안 25. 기술인력 보안대책 26. 수출・수입/합작 27. 보안사고 대응 28. 수송시 보안
보안 조사	29. 보안측정 30. 보안감사 31. 보안사고조사
기타	32. 비밀 제공/설명 33. 일반자료 관리 34. 회의시 보안 35. 보안교육 *36. 보안행정* *37. 방산 대외협력 활동*

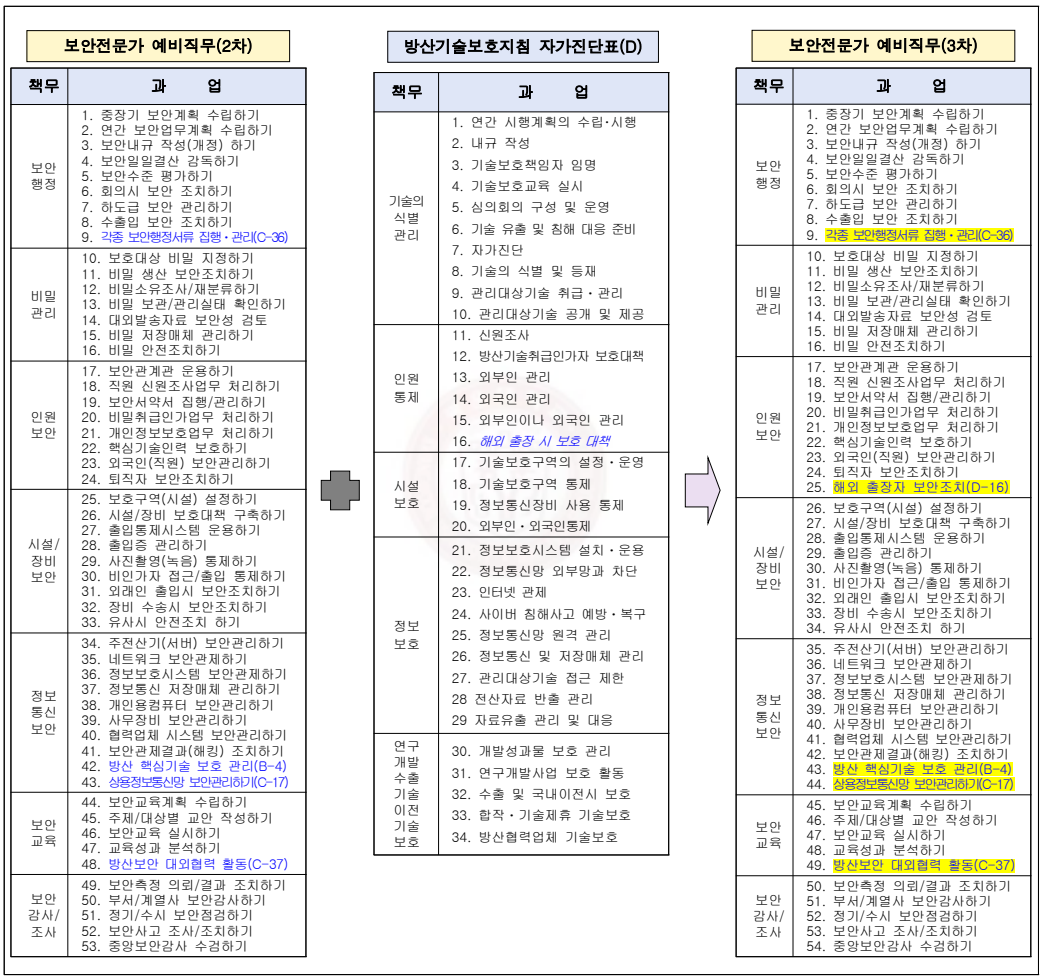
보안전문가 예비직무(2차)

책무	과 업
보안 행정	1. 중장기 보안계획 수립하기 2. 연간 보안업무계획 수립하기 3. 보안내규 작성(개정) 하기 4. 보안일일결산 감독하기 5. 보안수준 평가하기 6. 회의시 보안 조치하기 7. 하도급 보안 관리하기 8. 수출입 보안 조치하기 9. 각종 보안행정서류 집행・관리(C-36)
비밀 관리	10. 보호대상 비밀 지정하기 11. 비밀 생산 보안조치하기 12. 비밀소유조사/재분류하기 13. 비밀 보관/관리실태 확인하기 14. 대외발송자료 보안성 검토 15. 비밀 저장매체 관리하기 16. 비밀 안전조치하기
인원 보안	17. 보안관계관 운용하기 18. 직원 신원조사업무 처리하기 19. 보안서약서 집행/관리하기 20. 비밀취급인가업무 처리하기 21. 개인정보보호업무 처리하기 22. 핵심기술인력 보호하기 23. 외국인(직원) 보안관리하기 24. 퇴직자 보안조치하기
시설/ 장비 보안	25. 보호구역(시설) 설정하기 26. 시설/장비 보호대책 구축하기 27. 출입통제시스템 운용하기 28. 출입증 관리하기 29. 사진촬영(녹음) 통제하기 30. 비인가자 접근/출입 통제하기 31. 외래인 출입시 보안조치하기 32. 장비 수송시 보안조치하기 33. 유사시 안전조치 하기
정보 통신 보안	34. 주전산기(서버) 보안관리하기 35. 네트워크 보안관제하기 36. 정보보호시스템 보안관제하기 37. 정보통신 저장매체 관리하기 38. 개인용컴퓨터 보안관리하기 39. 사무장비 보안관리하기 40. 협력업체 시스템 보안관리하기 41. 보안관제결과(해킹) 조치하기 42. 방산 핵심기술 보호 관리(B-4) 43. 상용정보통신망 보안관리하기(C-17)
보안 교육	44. 보안교육계획 수립하기 45. 주제/대상별 교안 작성하기 46. 보안교육 실시하기 47. 교육성과 분석하기 48. 방산보안 대외협력 활동(C-37)
보안 감사/ 조사	49. 보안측정 의뢰/결과 조치하기 50. 부서/계열사 보안감사하기 51. 정기/수시 보안점검하기 52. 보안사고 조사/조치하기 53. 중앙보안감사 수검하기

그림 10. 보안전문가 예비직무 2차 종합

Figure 10. 2nd round of preliminary jobs for security experts

2차 종합한 예비직무를 토대로 방위산업기술 보호지침(D)에 명시된 자가진단표를 비교하여 3차 보안 예비직무를 그림 11과 같이 도출하였다. 비교확인한 결과, '해외 출장자 보안조치(D-16)'를 추가하였다.



보안전문가 예비직무(2차)

책무	과 업
보안 행정	1. 중장기 보안계획 수립하기 2. 연간 보안업무계획 수립하기 3. 보안내규 작성(개정) 하기 4. 보안일일결산 감독하기 5. 보안수준 평가하기 6. 회의시 보안 조치하기 7. 하도급 보안 관리하기 8. 수출입 보안 조치하기 9. 각종 보안행정서류 집행·관리(C-36)
비밀 관리	10. 보호대상 비밀 지정하기 11. 비밀 생산 보안조치하기 12. 비밀소유조사/재분류하기 13. 비밀 보관/관리실태 확인하기 14. 대외발송자료 보안성 검토 15. 비밀 저장매체 관리하기 16. 비밀 안전조치하기
인원 보안	17. 보안관계관 운용하기 18. 직원 신원조사업무 처리하기 19. 보안서약서 집행/관리하기 20. 비밀취급인가업무 처리하기 21. 개인정보보호업무 처리하기 22. 핵심기술인력 보호하기 23. 외국인(직원) 보안관리하기 24. 퇴직자 보안조치하기
시설/ 장비 보안	25. 보호구역(시설) 설정하기 26. 시설/장비 보호대책 구축하기 27. 출입통제시스템 운용하기 28. 출입증 관리하기 29. 사진촬영(녹음) 통제하기 30. 비인가자 접근/출입 통제하기 31. 외래인 출입시 보안조치하기 32. 장비 수송시 보안조치하기 33. 유사시 안전조치 하기
정보 통신 보안	34. 주전산기(서버) 보안관리하기 35. 네트워크 보안관제하기 36. 정보보호시스템 보안관제하기 37. 정보통신 저장매체 관리하기 38. 개인용컴퓨터 보안관리하기 39. 사무장비 보안관리하기 40. 협력업체 시스템 보안관리하기 41. 보안관제결과(해킹) 조치하기 42. 방산 핵심기술 보호 관리(B-4) 43. 상용정보통신망 보안관리하기(C-17)
보안 교육	44. 보안교육계획 수립하기 45. 주제/대상별 교안 작성하기 46. 보안교육 실시하기 47. 교육성과 분석하기 48. 방산보안 대외협력 활동(C-37)
보안 감사/ 조사	49. 보안측정 의뢰/결과 조치하기 50. 부서/계열사 보안감사하기 51. 정기/수시 보안점검하기 52. 보안사고 조사/조치하기 53. 중앙보안감사 수검하기

방산기술보호지침 자가진단표(D)

책무	과 업
기술의 식별 관리	1. 연간 시행계획의 수립·시행 2. 내규 작성 3. 기술보호책임자 임명 4. 기술보호교육 실시 5. 심의회의 구성 및 운영 6. 기술 유출 및 침해 대응 준비 7. 자가진단 8. 기술의 식별 및 등재 9. 관리대상기술 취급·관리 10. 관리대상기술 공개 및 제공
인원 통제	11. 신원조사 12. 방산기술취급인가자 보호대책 13. 외부인 관리 14. 외국인 관리 15. 외부인이나 외국인 관리 16. *해외 출장 시 보호 대책*
시설 보호	17. 기술보호구역의 설정·운영 18. 기술보호구역 통제 19. 정보통신장비 사용 통제 20. 외부인·외국인통제
정보 보호	21. 정보보호시스템 설치·운용 22. 정보통신망 외부망과 차단 23. 인터넷 관제 24. 사이버 침해사고 예방·복구 25. 정보통신망 원격 관리 26. 정보통신 및 저장매체 관리 27. 관리대상기술 접근 제한 28 전산자료 반출 관리 29 자료유출 관리 및 대응
연구개발 수출 기술 이전 기술 보호	30. 개발성과물 보호 관리 31. 연구개발사업 보호 활동 32. 수출 및 국내이전시 보호 33. 합작·기술제휴 기술보호 34. 방산협력업체 기술보호

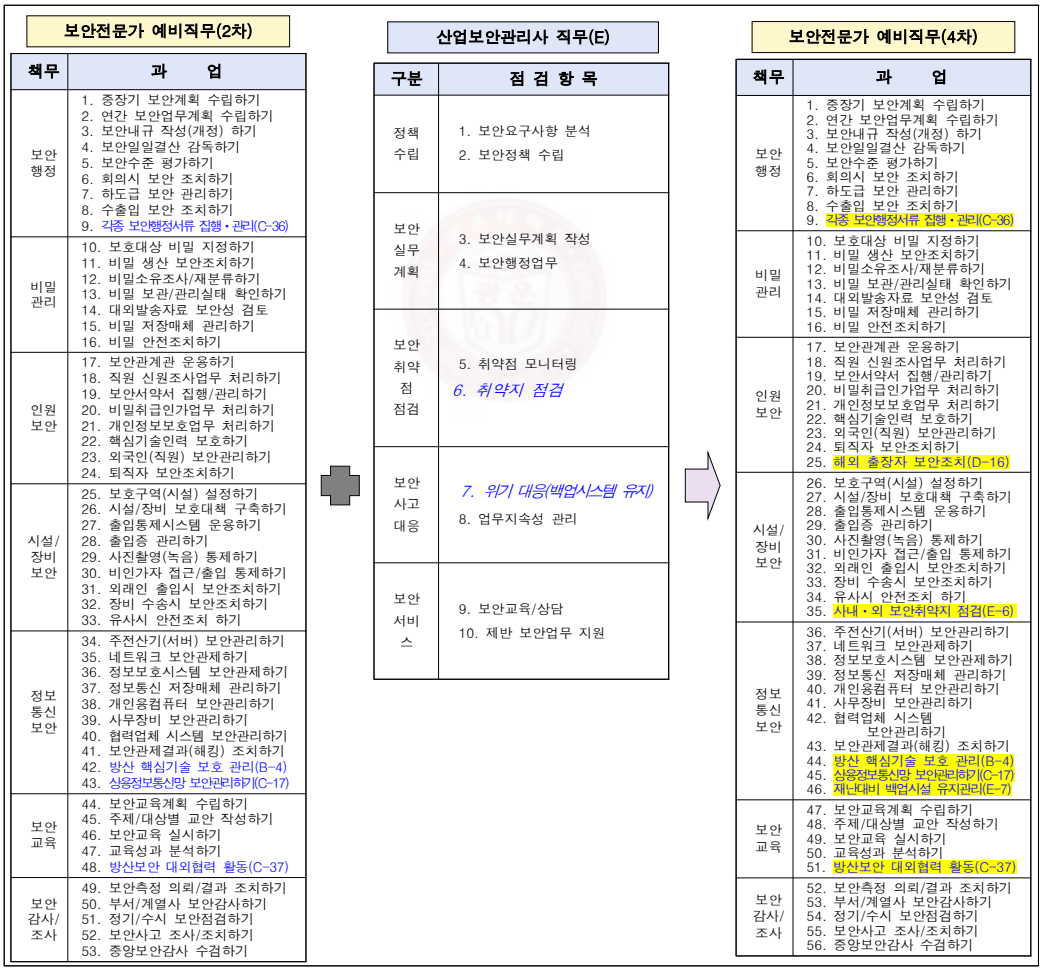
보안전문가 예비직무(3차)

책무	과 업
보안 행정	1. 중장기 보안계획 수립하기 2. 연간 보안업무계획 수립하기 3. 보안내규 작성(개정) 하기 4. 보안일일결산 감독하기 5. 보안수준 평가하기 6. 회의시 보안 조치하기 7. 하도급 보안 관리하기 8. 수출입 보안 조치하기 9. 각종 보안행정서류 집행·관리(C-36)
비밀 관리	10. 보호대상 비밀 지정하기 11. 비밀 생산 보안조치하기 12. 비밀소유조사/재분류하기 13. 비밀 보관/관리실태 확인하기 14. 대외발송자료 보안성 검토 15. 비밀 저장매체 관리하기 16. 비밀 안전조치하기
인원 보안	17. 보안관계관 운용하기 18. 직원 신원조사업무 처리하기 19. 보안서약서 집행/관리하기 20. 비밀취급인가업무 처리하기 21. 개인정보보호업무 처리하기 22. 핵심기술인력 보호하기 23. 외국인(직원) 보안관리하기 24. 퇴직자 보안조치하기 25. 해외 출장자 보안조치(D-16)
시설/ 장비 보안	26. 보호구역(시설) 설정하기 27. 시설/장비 보호대책 구축하기 28. 출입통제시스템 운용하기 29. 출입증 관리하기 30. 사진촬영(녹음) 통제하기 31. 비인가자 접근/출입 통제하기 32. 외래인 출입시 보안조치하기 33. 장비 수송시 보안조치하기 34. 유사시 안전조치 하기
정보 통신 보안	35. 주전산기(서버) 보안관리하기 36. 네트워크 보안관제하기 37. 정보보호시스템 보안관제하기 38. 정보통신 저장매체 관리하기 39. 개인용컴퓨터 보안관리하기 40. 사무장비 보안관리하기 41. 협력업체 시스템 보안관리하기 42. 보안관제결과(해킹) 조치하기 43. 방산 핵심기술 보호 관리(B-4) 44. 상용정보통신망 보안관리하기(C-17)
보안 교육	45. 보안교육계획 수립하기 46. 주제/대상별 교안 작성하기 47. 보안교육 실시하기 48. 교육성과 분석하기 49. 방산보안 대외협력 활동(C-37)
보안 감사/ 조사	50. 보안측정 의뢰/결과 조치하기 51. 부서/계열사 보안감사하기 52. 정기/수시 보안점검하기 53. 보안사고 조사/조치하기 54. 중앙보안감사 수검하기

그림 11. 보안전문가 예비직무 3차 종합
Figure 11. 3rd round of preliminary jobs for security experts

다음은 3차 종합한 예비직무를 토대로 산업보안관리사 직무(E)를 비교하여 그림 12와 같이 4차 보안 예비직무를 도출하였다. 산업보안관리사 직무 중 취약지 점검, 위기 대응(백업시스템 유지) 직무를 추가하여 '사내·외 보안취약지 점검

(E-6)', '재난대비 백업시스템 유지(E-7)'로 직무명칭을 수정하여 포함시켰다. 이로써 최초 융합보안전문가 직무 49개에서 ①'방산 핵심기술 보호관리(B-4)', ②'상용정보통신망 보안관리(C-17)', ③'각종 보안행정서류 집행·관리(C-36)', ④'방산보안 대외협력활동(C-37)', ⑤'해외 출장자 보안조치(D-16)', ⑥'사내·외 보안취약지 점검(E-6)', ⑦'재난대비 백업시스템 유지(E-7)' 등 7개 직무를 포함하여 56개로 예비직무를 산출하였다.



보안전문가 예비직무(2차)

책무	과 업
보안 행정	1. 중장기 보안계획 수립하기 2. 연간 보안업무계획 수립하기 3. 보안내규 작성(개정) 하기 4. 보안일일결산 감독하기 5. 보안수준 평가하기 6. 회의시 보안 조치하기 7. 하도급 보안 관리하기 8. 수출입 보안 조치하기 9. 각종 보안행정서류 집행·관리(C-36)
비밀 관리	10. 보호대상 비밀 지정하기 11. 비밀 생산 보안조치하기 12. 비밀소유조사/재분류하기 13. 비밀 보관/관리실태 확인하기 14. 대외발송자료 보안성 검토 15. 비밀 저장매체 관리하기 16. 비밀 안전조치하기
인원 보안	17. 보안관계관 운용하기 18. 직원 신원조사업무 처리하기 19. 보안서약서 집행/관리하기 20. 비밀취급인가업무 처리하기 21. 개인정보보호업무 처리하기 22. 핵심기술인력 보호하기 23. 외국인(직원) 보안관리하기 24. 퇴직자 보안조치하기
시설/ 장비 보안	25. 보호구역(시설) 설정하기 26. 시설/장비 보호대책 구축하기 27. 출입통제시스템 운용하기 28. 출입증 관리하기 29. 사진촬영(녹음) 통제하기 30. 비인가자 접근/출입 통제하기 31. 외래인 출입시 보안조치하기 32. 장비 수송시 보안조치하기 33. 유사시 안전조치 하기
정보 통신 보안	34. 주전산기(서버) 보안관리하기 35. 네트워크 보안관제하기 36. 정보보호시스템 보안관제하기 37. 정보통신 저장매체 관리하기 38. 개인용컴퓨터 보안관리하기 39. 사무장비 보안관리하기 40. 협력업체 시스템 보안관리하기 41. 보안관제결과(해킹) 조치하기 42. 방산 핵심기술 보호 관리(B-4) 43. 상용정보통신망 보안관리하기(C-17)
보안 교육	44. 보안교육계획 수립하기 45. 주제/대상별 교안 작성하기 46. 보안교육 실시하기 47. 교육성과 분석하기 48. 방산보안 대외협력 활동(C-37)
보안 감사/ 조사	49. 보안측정 의뢰/결과 조치하기 50. 부서/계열사 보안감사하기 51. 정기/수시 보안점검하기 52. 보안사고 조사/조치하기 53. 중앙보안감사 수검하기

산업보안관리사 직무(E)

구분	점 검 항 목
정책 수립	1. 보안요구사항 분석 2. 보안정책 수립
보안 실무 계획	3. 보안실무계획 작성 4. 보안행정업무
보안 취약 점 점검	5. 취약점 모니터링 *6. 취약지 점검*
보안 사고 대응	*7. 위기 대응(백업시스템 유지)* 8. 업무지속성 관리
보안 서비 스	9. 보안교육/상담 10. 제반 보안업무 지원

보안전문가 예비직무(4차)

책무	과 업
보안 행정	1. 중장기 보안계획 수립하기 2. 연간 보안업무계획 수립하기 3. 보안내규 작성(개정) 하기 4. 보안일일결산 감독하기 5. 보안수준 평가하기 6. 회의시 보안 조치하기 7. 하도급 보안 관리하기 8. 수출입 보안 조치하기 9. 각종 보안행정서류 집행·관리(C-36)
비밀 관리	10. 보호대상 비밀 지정하기 11. 비밀 생산 보안조치하기 12. 비밀소유조사/재분류하기 13. 비밀 보관/관리실태 확인하기 14. 대외발송자료 보안성 검토 15. 비밀 저장매체 관리하기 16. 비밀 안전조치하기
인원 보안	17. 보안관계관 운용하기 18. 직원 신원조사업무 처리하기 19. 보안서약서 집행/관리하기 20. 비밀취급인가업무 처리하기 21. 개인정보보호업무 처리하기 22. 핵심기술인력 보호하기 23. 외국인(직원) 보안관리하기 24. 퇴직자 보안조치하기 25. 해외 출장자 보안조치(D-16)
시설/ 장비 보안	26. 보호구역(시설) 설정하기 27. 시설/장비 보호대책 구축하기 28. 출입통제시스템 운용하기 29. 출입증 관리하기 30. 사진촬영(녹음) 통제하기 31. 비인가자 접근/출입 통제하기 32. 외래인 출입시 보안조치하기 33. 장비 수송시 보안조치하기 34. 유사시 안전조치 하기 35. 사내·외 보안취약지 점검(E-6)
정보 통신 보안	36. 주전산기(서버) 보안관리하기 37. 네트워크 보안관제하기 38. 정보보호시스템 보안관제하기 39. 정보통신 저장매체 관리하기 40. 개인용컴퓨터 보안관리하기 41. 사무장비 보안관리하기 42. 협력업체 시스템 보안관리하기 43. 보안관제결과(해킹) 조치하기 44. 방산 핵심기술 보호 관리(B-4) 45. 상용정보통신망 보안관리하기(C-17) 46. 재난대비 백업시설 유지관리(E-7)
보안 교육	47. 보안교육계획 수립하기 48. 주제/대상별 교안 작성하기 49. 보안교육 실시하기 50. 교육성과 분석하기 51. 방산보안 대외협력 활동(C-37)
보안 감사/ 조사	52. 보안측정 의뢰/결과 조치하기 53. 부서/계열사 보안감사하기 54. 정기/수시 보안점검하기 55. 보안사고 조사/조치하기 56. 중앙보안감사 수검하기

그림 12. 보안전문가 예비직무 4차 종합
Figure 12. 4th round of preliminary jobs for security experts

산출한 56개의 직무 중 6번 세부 직무인 ‘회의시 보안조치’는 보안전문가의 직무라기 보다는 회의 주관자 및 주관부서의 직무로써 제외하였고, 56번 직무인 ‘중앙보안감사 수검’은 방위사업청에서 방산업체의 중복 수검에 대한 부담을 경감시키기 위해 ’20년 3월부터 ‘통합실태조사’[20]로 통합되어 직무 명칭을 변경하였다. 최종 확정된 예비직무는 55개로 표 14와 같다.

표 14. 비교확인법을 통해 최종 확정된 예비직무

Table 14. Preliminary jobs finalized through the comparative verification method

책무	과 업
보안 행정	1. 중장기 보안계획 수립하기 2. 연간 보안업무계획 수립하기 3. 보안내규 작성(개정) 하기 4. 보안일일결산 감독하기 5. 보안수준 평가하기 6. 회의시 보안 조치하기(삭제) 7. 하도급 보안 관리하기 8. 수출입 보안 조치하기 9. 각종 보안행정서류 집행・관리(C-36)
비밀 관리	10. 보호대상 비밀 지정하기 11. 비밀 생산 보안조치하기 12. 비밀소유조사/재분류하기 13. 비밀 보관/관리실태 확인하기 14. 대외발송자료 보안성 검토 15. 비밀 저장매체 관리하기 16. 비밀 안전조치하기
인원 보안	17. 보안관계관 운용하기 18. 직원 신원조사업무 처리하기 19. 보안서약서 집행/관리하기 20. 비밀취급인가업무 처리하기 21. 개인정보보호업무 처리하기 22. 핵심기술인력 보호하기 23. 외국인(직원) 보안관리하기 24. 퇴직자 보안조치하기 25. 해외 출장자 보안조치(D-16)
시설 / 장비 보안	26. 보호구역(시설) 설정하기 27. 시설/장비 보호대책 구축하기 28. 출입통제시스템 운용하기 29. 출입증 관리하기 30. 사진촬영(녹음) 통제하기 31. 비인가자 접근/출입 통제하기 32. 외래인 출입시 보안조치하기 33. 장비 수송시 보안조치하기 34. 유사시 안전조치 하기 35. 사내・외 보안취약지 점검(E-6)
정보 통신 보안	36. 주전산기(서버) 보안관리하기 37. 네트워크 보안관제하기 38. 정보보호시스템 보안관제하기 39. 정보통신 저장매체 관리하기 40. 개인용컴퓨터 보안관리하기 41. 사무장비 보안관리하기 42. 협력업체 시스템 보안관리하기 43. 보안관제결과(해킹) 조치하기 44. 방산 핵심기술 보호 관리(B-4) 45. 상용정보통신망 보안관리하기(C-17) 46. 재난대비 백업시설 유지관리(E-7)
보안 교육 / 기타	47. 보안교육계획 수립하기 48. 주제/대상별 교안 작성하기 49. 보안교육 실시하기 50. 교육성과 분석하기 51. 방산보안 대외협력 활동(C-37)
보안 감사 / 조사	52. 보안측정 의뢰/결과 조치하기 53. 부서/계열사 보안감사하기 54. 정기/수시 보안점검하기 55. 보안사고 조사/조치하기 56. 중앙보안감사 수검하기(수정)

책무	과 업
보안 행정	1. 중장기 보안계획 수립 2. 연간 보안업무계획 수립 3. 보안내규 작성(개정) 4. 보안일일결산 감독 5. 보안수준 평가 6. 하도급 보안 관리 7. 수출입 보안 조치 8. 각종 보안행정서류 집행・관리
비밀 관리	9. 보호대상 비밀 지정 10. 비밀 생산 보안조치 11. 비밀소유조사/재분류 12. 비밀 보관/관리실태 확인 13. 대외발송자료 보안성 검토 14. 비밀 저장매체 관리 15. 비밀 안전조치
인원 보안	16. 보안관계관 운용 17. 직원 신원조사업무 처리 18. 보안서약서 집행/관리 19. 비밀취급인가업무 처리 20. 개인정보보호업무 처리 21. 핵심기술인력 보호 22. 외국인(직원) 보안관리 23. 퇴직자 보안조치 24. 해외 출장자 보안조치
시설 / 장비 보안	25. 보호구역(시설) 설정 26. 시설/장비 보호대책 구축 27. 출입통제시스템 운용 28. 출입증 관리 29. 사진촬영(녹음) 통제 30. 비인가자 접근/출입 통제 31. 외래인 출입시 보안조치 32. 장비 수송시 보안조치 33. 유사시 안전조치 34. 사내・외 보안취약지 점검
정보 통신 보안	35. 주전산기(서버) 보안관리 36. 네트워크 보안관제 37. 정보보호시스템 보안관제 38. 정보통신 저장매체 관리 39. 개인용컴퓨터 보안관리 40. 사무장비 보안관리 41. 협력업체 시스템 보안관리 42. 보안관제결과(해킹) 조치 43. 방산 핵심기술 보호 관리 44. 재난대비 백업시설 유지관리 45. 상용정보통신망 보안관리
보안 교육 / 기타	46. 보안교육계획 수립 47. 주제/대상별 교안 작성 48. 보안교육 실시 49. 교육성과 분석 50. 방산보안 대외협력 활동
보안 감사 / 조사	51. 보안측정 의뢰/결과 조치 52. 부서/계열사 보안감사 53. 정기/수시 보안점검 54. 보안사고 조사/조치 55. 통합실태조사 수검

20) 기존의 ‘방위산업기술보호 실태조사’와 ‘보안감사’를 통합하여 실시

제4절 방산업체 보안전문가 직무 확정

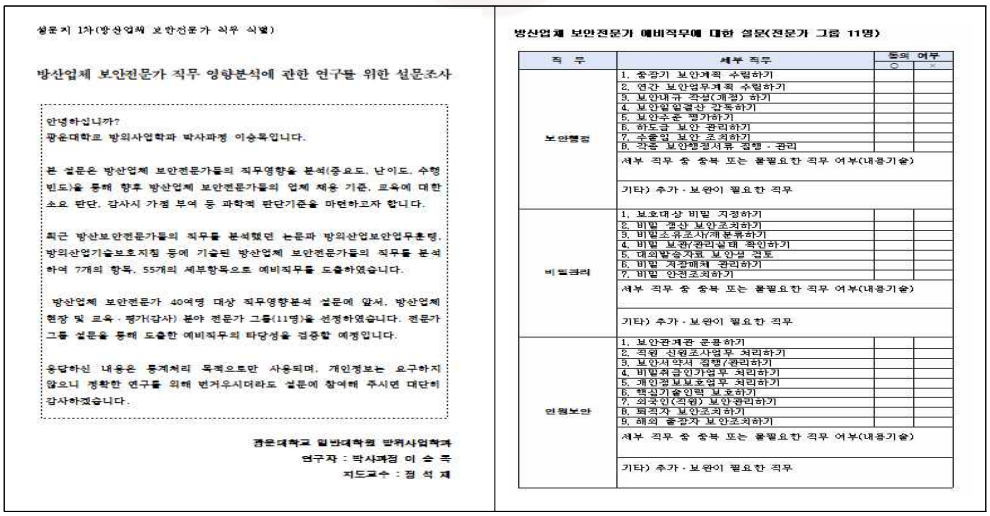
1. 1차 설문조사

산출한 예비직무를 기초로 표 15와 같이 20년 이상 경력을 보유한 방산분야 보안전문가 11명을 섭외하였고, 설문에 의한 델파이기법을 통해 예비직무에 대한 동의여부를 묻는 1차 설문을 '23. 9.11. - 20.간 실시하였다. 설문지 구성(부록 ①)의 예문은 그림 13과 같다. 직무분석 방법 중 데이컴법[21]을 시행하려 하였으나, 전국 각지에서 근무하고 있는 전문가를 섭외하기가 제한되어 델파이 기법을 활용하여 설문 형식으로 진행하였다.

표 15. 방산분야 보안전문가 편성

Table 15. Organization of security experts in the defense industry

소 속	대 상	비 고(%)
군 및 정부기관	4명	36.3%
방 산 업 체	7명	63.7%


설문지 1차(방산업체 보안전문가 직무 식별)

방산업체 보안전문가 직무 영향분석에 관한 연구를 위한 설문조사

안녕하십니까?
광운대학교 방위사업학과 박사과정 이승목입니다.

본 설문은 방산업체 보안전문가들의 직무영향을 분석(중요도, 난이도, 수행빈도)을 통해 향후 방산업체 보안전문가들의 업체 채용 기준, 교육에 대한 소요 판단, 감사시 가점 부여 등 과학적 판단기준을 마련하고자 합니다.

최근 방산보안전문가들의 직무를 분석했던 논문과 방위산업보안업무훈령, 방위산업기술보호지침 등에 기술된 방산업체 보안전문가들의 직무를 분석하여 7개의 항목, 55개의 세부항목으로 예비직무를 도출하였습니다.

방산업체 보안전문가 40여명 대상 직무영향분석 설문에 앞서, 방산업체 현장 및 교육·평가(감사) 분야 전문가 그룹(11명)을 선정하였습니다. 전문가 그룹 설문을 통해 도출한 예비직무의 타당성을 검증할 예정입니다.

응답하신 내용은 통계처리 목적으로만 사용되며, 개인정보는 요구하지 않으니 정확한 연구를 위해 번거로시더라도 설문에 참여해 주시면 대단히 감사하겠습니다.

광운대학교 일반대학원 방위사업학과
연구자 : 박사과정 이 승 목
지도교수 : 정 석 재

방산업체 보안전문가 예비직무에 대한 설문(전문가 그룹 11명)

직 무	세부 직무	동의 ○	여부 ×
보안행정	1. 중장기 보안계획 수립하기		
	2. 연간 보안업무계획 수립하기		
	3. 보안내규 작성(개정) 하기		
	4. 보안할당량산 강독하기		
	5. 보안조준 평가하기		
	6. 하도급 보안 관리하기		
	7. 소출입 보안 조치하기		
	8. 각종 보안행정자료 검토 · 관리		
	세부 직무 중 중복 또는 불필요한 직무 여부(내용기술)		
	기타) 추가 · 보완이 필요한 직무		
비밀관리	1. 보호대상 비밀 지정하기		
	2. 비밀 생산 보안조치하기		
	3. 비밀소유조사/계 분류하기		
	4. 비밀 보관/관리실태 확인하기		
	5. 대외발송자료 보안검 검토		
	6. 비밀 저장매체 관리하기		
	7. 비밀 안전조치하기		
	세부 직무 중 중복 또는 불필요한 직무 여부(내용기술)		
	기타) 추가 · 보완이 필요한 직무		
인원보안	1. 보안관계관 운용하기		
	2. 직원 신원조사업무 처리하기		
	3. 보안서약서 집행/관리하기		
	4. 비밀취급인가업무 처리하기		
	5. 개인정보보호업무 처리하기		
	6. 핵심기술인력 보호하기		
	7. 외국인(직원) 보안관리하기		
	8. 퇴직자 보안조치하기		
	9. 해외 출장자 보안조치하기		
	세부 직무 중 중복 또는 불필요한 직무 여부(내용기술)		
	기타) 추가 · 보완이 필요한 직무		

그림 13. 보안전문가 예비직무 1차 설문지 구성(예)

Figure 13. Security experts Preliminary Job 1st Questionnaire Organization(Example)

21) 8-12명의 구성된 데이컴위원회의 소집단이 브레인스토밍 기법을 활용하여 현장에서 토의

설문결과, 1개 직무 삭제(보호대상 비밀 지정하기, **합의율 63.6%**), 1개 직무는 통합(사무장비 보안관리), 2개 세부 직무(비밀 반입 및 반출 통제, 비밀 서류철 작성 관리 감독)는 추가, 24개 직무는 행동화할 수 있는 형식으로 명칭을 변경하였다.

각 직무별 세부 합의내용을 알아보겠다. 첫째, 보안행정에 대한 합의율와 합의내용은 표 16과 같다. 보안행정 직무의 8개 세부직무는 모두 80% 이상의 합의율을 보였고, 4개의 세부직무에 대해서는 직무내용을 순화하거나 행동화하는 명칭으로 변경하였다.

표 16. 보안행정 직무 설문결과

Table 16. Security Administration Job Survey Results

직 무	세부 직무	합의율(%)	비고
보안행정	1. 중장기 보안계획 수립	100	
	2. 연간 보안업무계획 수립	100	
	3. *보안내규 작성(개정) 하기* **→ 보안내규 제·개정**	100	명칭 변경
	4. *보안일일결산 감독하기* **→ 보안일일결산 감독·통제**	81.8	명칭 변경
	5. *보안수준 평가하기* **→ 보안수준평가 감독·통제**	90.9	명칭 변경
	6. *하도급 보안 관리하기* **→ 하도급 보안특약조건 검토 및 감독**	90.9	명칭 변경
	7. 수출입 보안 조치	81.8	
	8. 각종 보안행정서류 집행·관리	100	
	설문시 전문가 특이 의견 1. 하도급 보안관리 직무가 오히려 업체 입장에서 발목을 잡히는 행위가 될 수 있어 직무내용 순화 필요 2. 보안내규, 보안일일결산, 보안수준평가 직무에 대해서는 실제 행동화하는 명칭으로 변경		

둘째, 비밀관리 직무의 7개 세부직무에 대해서는 표 17과 같이 1개 세부직무는 삭제하였고, 3개 세부직무는 명칭변경, 2개 세부직무를 추가하였다. 삭제한 '보호대상 비밀지정하기'는 63.6%의 합의율과 비밀지정은 보안전문가의 직무가 아닌

지정권자의 임무라는 의견이 제시되었다. 명칭이 변경된 비밀 안전조치 등 3개 세부직무는 모호한 명칭이라는 의견이 있어 구체적인 명칭으로 변경되었다. 그 외 비밀 반입 및 반출 통제와 비밀 서류철 작성 관리 감독의 세부직무가 보안전문가 직무에 포함되어야 한다는 의견이 있어 추가하였다.

표 17. 비밀관리 직무 설문결과

Table 17. Secret Management Job Survey Results

직 무	세부 직무	합의율(%)	비고
비밀관리	1. *보호대상 비밀 지정하기*	63.6	삭제
	2. *비밀 생산 보안조치하기* → **비밀 생산(접수) 보안관리**	81.8	명칭 변경
	3. 비밀소유조사 / 재분류	90.9	
	4. *비밀 보관 / 관리실태 확인* → **비밀 보관/관리실태 확인・감독**	100	명칭 변경
	5. 대외발송자료 보안성 검토	100	
	6. 비밀 저장매체 관리	100	
	7. *비밀 안전조치* → **비밀 보호조치(지정/분류, 안전지출 등 포함)**	81.8	명칭 변경
	8. **비밀 반입 및 반출 통제**		추가
	9. **비밀 서류철 작성 관리 감독**		추가
	설문시 전문가 특이 의견 1. 비밀 반입 및 반출 통제에 대한 의견과 비밀 서류철 작성에 대한 관리 감독의 직무 추가 필요 2. 비밀 안전조치는 직무가 명확하지 않아 명칭변경 필요 3. 비밀 지정은 보안전문가 직무보다는 지정권자 임무		

셋째, 인원보안 직무는 9개의 세부직무로 구성되어 있는데, 표 18과 같이 9개 세부직무 모두 80% 이상의 합의를 얻어 삭제되는 세부직무는 없으며, 3개의 세부직무에 대해서 직무 명칭을 변경하였다. 직원 신원조사업무는 협력사를 포함해야 한다는 의견이 있어 명칭을 변경하였고, 핵심기술인력 보호는 보안전문가의

직무보다는 타 기관의 직무라는 의견이 있어 핵심기술인력 보안조치로 변경되었다. 해외 출장자 보안조치는 해당 부서의 임무로 보안부서의 직무는 해외 출장자에 대한 보안교육이 필요하다는 의견이 있어 변경하였다.

표 18. 인원보안 직무 설문결과

Table 18. Personnel Security Job Survey Results

직 무	세부 직무	합의율(%)	비고
인원보안	1. 보안관계관 운용	100	
	2. *직원 신원조사업무 처리* **→ 직원(협력사 등) 신원조사업무 처리**	100	명칭 변경
	3. 보안서약서 집행 / 관리	100	
	4. 비밀취급인가업무 처리	100	
	5. 개인정보보호업무 처리	90.9	
	6. *핵심기술인력 보호* **→ 핵심기술인력 보안조치**	81.8	명칭 변경
	7. 외국인(직원) 보안관리	100	
	8. 퇴직자 보안조치	100	
	9. *해외 출장자 보안조치* **→ 해외 출장자 보안교육**	90.9	명칭 변경
	설문시 전문가 특이 의견 1. 신원조사는 직원 및 협력사 포함 필요 1. 핵심기술인력에 대한 보호는 보안업무보다는 타 기관업무에 더 큰 비중 차지, 보안조치로 직무변경 필요 2. 해외 출장 보안조치는 해 부서의 조치이고 보안부서에서는 보안교육의 직무가 타당		

넷째, 시설/장비보안 직무는 10개의 세부직무로 구성되어 있으며, 표 19와 같이 80% 이상의 합의를 얻어 모든 세부 직무를 수용하였고, 유사시 안전조치는 명칭의 모호성으로 유사시 시설/장비 보안조치로 변경하였고, 사내·외 보안취약지 점검은 사내로 한정하는 것으로 변경하였다.

표 19. 시설/장비보안 직무 설문결과

Table 19. Facility and equipment security job survey results

직 무	세부 직무	합의율(%)	비고
시설/장비보안	1. 보호구역(시설) 설정	100	
	2. 시설/장비 보호대책 구축	100	
	3. 출입통제시스템 운용	81.8	
	4. 출입증 관리	81.8	
	5. 사진촬영(녹음) 통제	100	
	6. 비인가자 접근 / 출입 통제	100	
	7. 외래인 출입시 보안조치	100	
	8. 장비 수송시 보안조치	90.9	
	9. *유사시 안전조치(명칭모호)* **→ 유사시 시설/장비 보안조치**	81.8	명칭 변경
	10. *사내·외 보안취약지 점검* **→ 사내 보안취약지 점검**	100	명칭 변경
	설문시 전문가 특이 의견 1. 유사시 안전조치 직무는 용어가 불명확하여 혼선 초래, 유사시 시설 및 장비에 대한 보안조치로 변경 2. 사외 보안취약지 점검은 미해당(사내로 제한)		

다섯째, 정보통신보안 직무는 11개 세부직무로 구성되어 있는데, 표 20과 같이 모두 80% 이상 합의가 되어 추가되거나 삭제되는 세부 직무는 없다. 단, 세부 직무 중 정보통신실무자가 수행해야 할 주전산기(서버) 보안관리 등 8개 세부 직무는 감독 및 통제하는 것으로 명칭이 변경되었고 추가 의견으로 제시한 업체 망분리 정책과 시스템 유지관리는 3번 세부 직무인 네트워크 보안관제에 포함하여 명칭을 변경하였다. 사무장비 보안관리는 정보통신 저장매체 관리에 통합하여 '정보통신 장비 및 저장매체 관리'로 명칭을 변경하였다.

표 20. 정보통신보안 직무 설문결과

Table 20. Information and Communication Security Job Survey Results

직 무	세부 직무	합의율(%)	비고
정보통신 보안	1. *주전산기(서버) 보안관리* → **주전산기(서버) 보안관리 감독**	100	명칭 변경
	2. *네트워크 보안관제* → **네트워크(망분리 포함) 보안 관제 감독**	90.9	명칭 변경
	3. *정보보호시스템 보안관제* → **정보보호시스템 보안관제 감독**	90.9	명칭 변경
	4. *정보통신 저장매체 관리(6번과 통합)* → **정보통신 장비 및 저장매체 관리**	100	명칭 변경
	5. 개인용컴퓨터 보안관리	100	
	6. *사무장비 보안관리(4번과 통합, 삭제)*	100	통합
	7. *협력업체 시스템 보안관리* → **협력업체 시스템 보안관리 감독**	90.9	명칭 변경
	8. *보안관제결과(해킹) 조치* → **보안관제결과(해킹) 조치 관리 감독**	100	명칭 변경
	9. 방산 핵심기술 보호 관리	90.9	
	10. *재난대비 백업시설 유지관리* → **재난대비 백업시설 유지관리 통제**	90.9	명칭 변경
	11. *상용정보통신망 보안관리* → **상용정보통신망 보안관리 통제**	100	명칭 변경
	설문시 전문가 특이 의견 1. 정보통신보안 분야는 대부분 정보통신실무자의 임무로 보안전문가는 해당 업무에 대한 통제와 감독임무 수행 2. 업체 망분리 정책과 시스템 유지관리에 대한 직무 필요 → 네트워크(망분리 포함) 보안관제 감독 직무에 통합 3. 사무장비 보안관리는 정보통신 저장매체 관리와 통합 필요		

여섯째, 보안교육/기타 직무는 총 5개로 구성되었는데, 표 21과 같이 90% 이상의 합의를 얻었으며, 보안교육 실시는 대·내외 보안교육 실시로, 교육성과 분석은 보안교육 성과분석으로 명칭을 구체화 하였다.

표 21. 보안교육/기타 직무 설문결과

Table 21. Security training and other job survey results

직 무	세부 직무	합의율(%)	비고
보안교육/기타	1. 보안교육계획 수립	100	
	2. 주제/대상별 교안 작성	100	
	3. *보안교육 실시* **→ 대내·외 보안교육 실시**	100	명칭 변경
	4. *교육성과 분석* **→ 보안교육 성과분석**	90.9	명칭 변경
	5. 방산보안 대외협력 활동	100	
	설문시 전문가 특이 의견 1. 대외 직무교육 수강 등 인적계발 노력이 필요하다는 의견 → 보안교육내용에 포함		

일곱째, 표 22와 같이 모두 100% 합의를 이루었으며, 부서/계열사 보안감사는 오해유발 가능성이 있어 부서/계열사 보안점검으로, 보안사고 조사/조치는 보안사고 시 초동조치/관계기관 신고로 행동화하는 명칭으로 변경하였다.

표 22. 보안점검/조사 직무 설문결과

Table 22. Security inspection and investigation job survey results

직 무	세부 직무	합의율(%)	비고
보안점검/조사	1. 보안측정 의뢰/결과 조치	100	
	2. *부서/계열사 보안감사* **→ 부서/계열사 보안점검**	100	명칭 변경
	3. 정기/수시 보안점검	100	
	4. *보안사고 조사/조치* **→ 보안사고시 초동조치 및 관계기관 신고**	100	명칭 변경
	5. 통합실태조사 수검	100	
	설문시 전문가 특이 의견 1. 부서/계열사에 대한 보안감사라는 직무 명칭은 오해 유발 가능, 감사보다는 보안점검 직무가 타당 2. 보안사고 조사/조치보다는 보안사고시 초동조치 및 관계기관 신고라는 행동화 직무로 변경 필요		

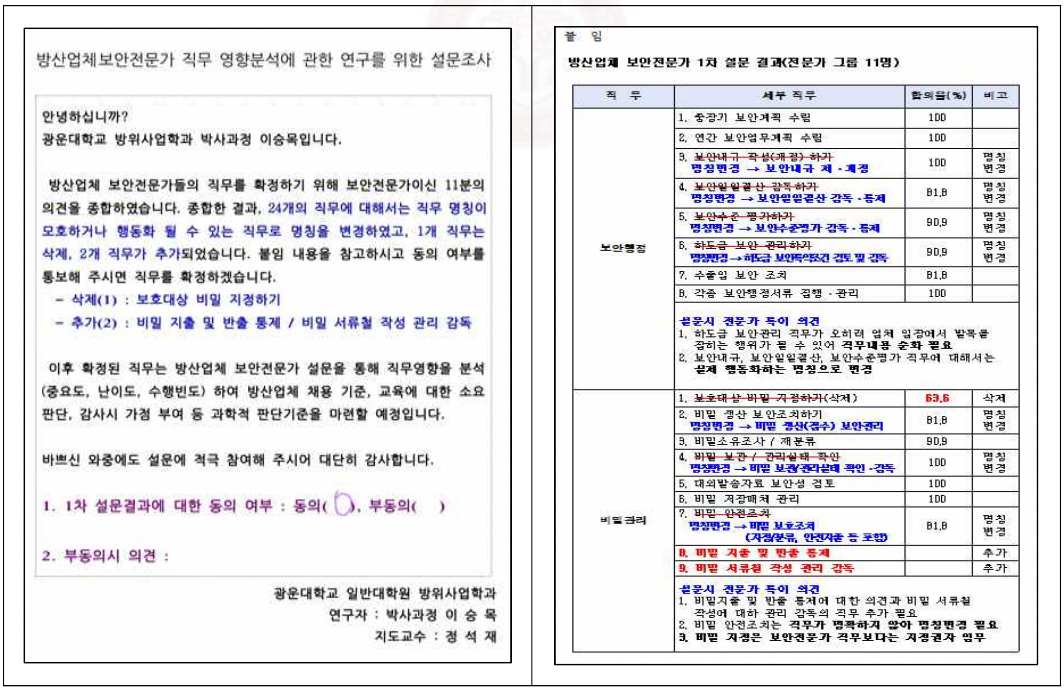
2차 설문조사

종합한 1차 설문조사 결과를 '23. 9.21. - 9.25.간 설문에 응해준 11명에게 재발송하여 합의여부를 문의하였고, 표 23과 같이 11명 모두 특이사항 없이 동의하였다. 그림 14는 동의 여부(SNS, 1:1 전화를 통해 입수)에 대한 답변 결과의 일부 예이다.

표 23. 합의 응답 수단 및 동의 결과

Table 23. Consensus Response Means and Consent Results

합의 응답 수단	대 상	동의수(11명, 100%)
SNS・메일	5명	5명(45.4%)
1:1 전화통화	6명	6명(54.6%)



방산업체보안전문가 직무 영향분석에 관한 연구를 위한 설문조사

안녕하십니까?
광운대학교 방위사업학과 박사과정 이승목입니다.

방산업체 보안전문가들의 직무를 확정하기 위해 보안전문가이신 11분의 의견을 종합하였습니다. 종합한 결과, 24개의 직무에 대해서는 직무 명칭이 모호하거나 행동화 될 수 있는 직무로 명칭을 변경하였고, 1개 직무는 삭제, 2개 직무가 추가되었습니다. 붙임 내용을 참고하시고 동의 여부를 통보해 주시면 직무를 확정하겠습니다.

- 삭제(1) : 보호대상 비밀 지정하기
- 추가(2) : 비밀 지출 및 반출 통제 / 비밀 서류철 작성 관리 감독

이후 확정된 직무는 방산업체 보안전문가 설문을 통해 직무영향을 분석(중요도, 난이도, 수행빈도) 하여 방산업체 채용 기준, 교육에 대한 소요 판단, 감사시 가점 부여 등 과학적 판단기준을 마련할 예정입니다.

바쁘신 와중에도 설문에 적극 참여해 주시어 대단히 감사합니다.

1. 1차 설문결과에 대한 동의 여부 : 동의( ), 부동의( )

2. 부동의시 의견 :

광운대학교 일반대학원 방위사업학과
연구자 : 박사과정 이 승 목
지도교수 : 정 석 재

붙 임

방산업체 보안전문가 1차 설문 결과(전문가 그룹 11명)

직 무	세부 직무	합의율(%)	비고
보안행정	1. 중장기 보안계획 수립	100	
	2. 연간 보안업무계획 수립	100	
	3. ~~보안내규 작성(개정) 하기~~ 명칭변경 → 보안내규 제・개정	100	명칭 변경
	4. ~~보안일일결산 감독하기~~ 명칭변경 → 보안일일결산 감독・등재	81,8	명칭 변경
	5. ~~보안수준 평가하기~~ 명칭변경 → 보안수준평가 감독・등재	90,9	명칭 변경
	6. ~~하드급 보안 관리하기~~ 명칭변경 → 하드급 보안특약조건 검토 및 감독	90,9	명칭 변경
	7. 수출입 보안 조치	81,8	
	8. 각종 보안행정서류 집행・관리	100	
	설문시 전문가 특이 의견 1. 하드급 보안관리 직무가 오히려 업체 입장에서 발목을 잡히는 행위가 될 수 있어 **격무내용 순화 필요** 2. 보안내규, 보안일일결산, 보안수준평가 직무에 대해서는 **실제 행동화하는 명칭으로 변경**		
비도큐리	1. ~~보호대상 비밀 지정하기~~(삭제)	63,6	삭제
	2. 비밀 생산 보안조치하기 명칭변경 → 비밀 생산(증수) 보안관리	81,8	명칭 변경
	3. 비밀소유조사 / 재분류	90,9	
	4. ~~비밀 보관 / 관리실태 확인~~ 명칭변경 → 비밀 보관/관리실태 확인・감독	100	명칭 변경
	5. 대외발송자료 보안성 검토	100	
	6. 비밀 저장매체 관리	100	
	7. ~~비밀 안전조치~~ 명칭변경 → 비밀 보호조치 (자정/분류, 안전자준 등 포함)	81,8	명칭 변경
	8. 비밀 지출 및 반출 통제		추가
	9. 비밀 서류철 작성 관리 감독		추가
	설문시 전문가 특이 의견 1. 비밀지출 및 반출 통제에 대한 의견과 비밀 서류철 작성에 대한 관리 감독의 직무 추가 필요 2. 비밀 안전조치는 **격무가 명확하지 않아 명칭변경 필요** 3. **비밀 지정은 보안전문가 직무보다는 지정권자 업무**		

그림 14. 동의 여부에 대한 답변(예)

Figure 14. Answer to consent(example)

2차 설문조사에 설문자 모두 동의를 하여 더 이상의 추가 설문은 진행하지 않았다. 합의한 결과, 표 24와 같이 방산업체 보안전문가의 직무가 최종 확정되었다. 예비직무 산출 시 충분한 비교확인·검증으로 직무에 대한 설문이 조기에 종료된 것으로 예측된다. 최종 확정된 직무를 바탕으로 방산보안 현장 실문자 및 전문가 40여 명 대상으로 3차 설문을 진행할 예정이다.

표 24. 최종 확정된 방산업체 보안전문가 직무

Table 24. Finalized duties of defense industry security experts

직 무	세 부 직 무	직 무	세 부 직 무
보안행정 (8)	1. 중장기 보안계획 수립 2. 연간 보안업무계획 수립 3. 보안내규 제·개정 4. 보안일일결산 감독·통제 5. 보안수준평가 감독·통제 6. 하도급 보안특약조건 검토 및 감독 7. 수출입 보안 조치 8. 각종 보안행정서류 집행·관리	비밀관리 (8)	9. 비밀 생산(접수) 보안관리 10. 비밀소유조사 / 재분류 11. 비밀 보관/관리실태 확인·감독 12. 대외발송자료 보안성 검토 13. 비밀 저장매체 관리 14. 비밀 보호조치(지정, 안전지출 등) 15. 비밀 반입 및 반출 통제 16. 비밀 서류철 작성 관리 감독
인원보안 (9)	17. 보안관계관 운용 18. 직원(협력사 등) 신원조사 업무 19. 보안서약서 집행 / 관리 20. 비밀취급인가업무 처리 21. 개인정보보호업무 처리 22. 핵심기술인력 보안조치 23. 외국인(직원) 보안관리 24. 퇴직자 보안조치 25. 해외 출장자 보안교육	시설/장비보안 (10)	26. 보호구역(시설) 설정 27. 시설/장비 보호대책 구축 28. 출입통제시스템 운용 29. 출입증 관리 30. 사진촬영(녹음) 통제 31. 비인가자 접근 / 출입 통제 32. 외래인 출입시 보안조치 33. 장비 수송시 보안조치 34. 유사시 시설/장비 보안조치 35. 사내 보안취약지 점검
정보통신 보안 (10)	36. 전산기(서버) 보안관리 감독 37. 네트워크(망분리 포함) 보안 관제 감독 38. 정보보호시스템 보안관제 감독 39. 정보통신 장비 및 저장매체 관리 40. 개인용컴퓨터 보안관리 41. 협력업체 시스템 보안관리 감독 42. 보안관제결과(해킹) 조치 관리 감독 43. 방산 핵심기술 보호 관리 44. 재난대비 백업시설 유지관리 통제 45. 상용정보통신망 보안관리 통제	보안교육/기타 (5)	46. 보안교육계획 수립 47. 주제/대상별 교안 작성 48. 대내·외 보안교육 실시 49. 보안교육 성과분석 50. 방산보안 대외협력 활동
		보안점검/조사 (5)	51. 보안측정 의뢰/결과 조치 52. 부서/계열사 보안점검 53. 정기/수시 보안점검 54. 보안사고시 초동조치 및 관계기관 신고 55. 통합실태조사 수검

3. 3차 설문조사(중요도, 난이도, 수행빈도 측정)

3차 설문조사는 앞에서 확정한 방산업체 보안전문가의 직무(55개)에 대해 40명의 방산보안 현장 실무자 및 전문가 대상으로 '23. 10. 5. - 14.까지 실시하였다. 이 중 방산업체 설문대상자는 향후 방산업체의 인적구성의 분포를 확인하기 위해 사전 선정 없이 무작위 선발하였다. 표 25는 본 설문의 개요와 기본 인적사항 설문 양식이다.

표 25. 설문 개요 및 기본 인적사항 설문 양식

Table 25. Survey Overview and Basic Personal Information Survey Form

설 문 개 요	
설문 기간	'23. 10. 5. - 14.(10일간)
설문 대상	방산보안 현장 실무자 및 전문가 40명
평가 요소	중요도・난이도・수행빈도
응답 척도	각 요소별 5점 리커트 척도
기본 인적사항 설문 양식	
직 업	□ 군/정부기관 □ 교육기관 □ 방산업체 보안관계자 □ 기 타
연 령	□ 20대 □ 30대 □ 40대 □ 50대 □ 60대 이상
최종학력	□ 학사 □ 석사 수료 □ 석사 □ 박사 수료 □ 박사
보안경력	□ 5년이하 □ 5-10년 □ 10-15년 □ 15-20년 □ 20년이상

설문지가 발송된 40명 중 응답한 인원은 총 38명(설문 응답률 95.0%)으로서 매우 성실히 응답해 주었다. 특히, 일부 설문자는 전화를 하여 설문 응답에 대한 추가 질문을 하는 등 적극적으로 답변해 주었다.

각 세부 직무별 중요도, 난이도, 수행빈도의 세부측정은 5점 리커트 척도[22]로 시행하였고, 설문자들의 주관적 판단 제거 및 오류를 최소화하기 위해 표 26과 같이 각 요소별 명확한 기준점을 제시하였다.

표 26. 각 요소별 측정을 위한 기준점

Table 26. Reference points for measurement by each element

구 분	5점 척도 평가 기준
중요도	5점 : 방산업체 운영에 심각한 영향을 미치는 직무
	4점 : 방산업체 운영에 크게 영향이 있는 직무
	3점 : 방산업체 운영에 상대적 영향을 미치는 직무
	2점 : 방산업체 운영에 일부 영향을 미치는 직무
	1점 : 방산업체 운영에 영향이 미미한 직무
난이도	5점 : 수행업무가 고도의 전문성을 요구하는 직무
	4점 : 수행업무가 일부 전문성을 요구하는 직무
	3점 : 수행업무가 일정교육 이수시 가능한 직무
	2점 : 수행업무가 대리수행자가 가능한 직무
	1점 : 수행업무가 누구나 할 수 있는 직무
수행빈도	5점 : 수시 또는 일일단위 수행하는 직무
	4점 : 일일 ~ 주단위 수행하는 직무
	3점 : 주간 ~ 월간단위 수행하는 직무
	2점 : 월간 ~ 분기단위 수행하는 직무
	1점 : 분기 이상 단위 수행하는 직무

22) 리커트 척도(Likert scale)는 설문 조사 등에 사용되는 심리 검사 응답 척도의 하나로, 각종 조사에서 널리 사용되고 있다. 리커트 척도에서는 응답자가 제시된 문장에 대해 얼마나 동의하는지를 답변하도록 한다. 리커트 척도라는 명칭은 이 척도 사용에 대한 보고서를 발간한 렌시스 리커트(Rensis Likert)의 이름에서 따온 것이다(Likert, 1932). 라이커트 척도라고도 한다.

제5장 방산업체 보안전문가 직무영향 분석

제1절 설문자 기본 인적사항 분석 결과

1. 설문 대상자 인적구성 분석

설문 기본 인적사항 구성 현황은 표 27과 같다. 설문에 참여한 38명을 분석한 결과, 대부분의 설문자는 방산업체 보안관계자(32명, 84.2%)이며, 연령은 40대 이상(34명, 89.5%), 학력은 1명을 제외하고 학사 이상 인원이고, 보안경력은 5년에서 20년 이상 인원으로 고루 분포하였다.

표 27. 설문대상자 기본 인적 현황

Table 27. Basic human resources status of survey subjects

항 목	세부항목	인원수	분포율(%)
소 속	군/정부기관	5	13.2
	방산업체	32	84.2
	기타	1	2.6
연 령	30대	4	10.5
	40대	13	34.2
	50대	21	55.3
학 력	고졸	1	2.6
	학사	22	57.9
	석사 수료	2	5.3
	석사	9	23.7
	박사 수료	3	7.9
	박사	1	2.6
보안 경력	5년 이하	10	26.3
	5-10년	11	28.9
	10-15년	4	10.5
	15-20년	3	7.9
	20년 이상	10	26.3

2. 방산업체 보안부서 인적구성 분석

설문에 참여한 방산업체 보안관계자는 총 32명으로 이들에 대한 연령, 학력, 보안경력에 대한 구성 분포율은 표 28과 같다.

표 28. 방산업체 보안전문가 인적 구성 분포율

Table 28. Distribution rate of personnel composition of security experts

항 목	세부항목	인원수	분포율(%)
연 령	30대	4	12.5
	40대	8	25.0
	50대	20	62.5
학 력	고졸	1	2.6
	학사	19	59.4
	석사 수료	1	3.1
	석사	8	25.0
	박사 수료	2	6.3
	박사	1	3.1
보안 경력	5년 이하	9	28.1
	5-10년	9	28.1
	10-15년	3	9.4
	15-20년	2	6.3
	20년 이상	9	28.1

표 28에서 보는 바와 같이 방산업체 보안전문가들의 연령이 40대 이상으로 87.0%(50대 이상 62.5%)를 차지하고 있으며, 학력은 20명이 학사 이하로 확인되었다. 설문 대상자를 무작위로 선발했다는 사실로 비추어 볼 때 대부분 방산업체 보안부서의 인적구성은 유사할 것으로 예측된다. 방산업체 보안부서의 인적구성이 고연령과 학사이하 인원이 60% 이상이라는 결과에 대해서는 업체 경영진 입장에서 관심이 필요한 사안으로 판단된다.

제2절 각 요소별 설문 결과 분석

1. 중요도 분석 결과

방산업체 보안전문가 직무에 대한 분석결과 '방산 핵심기술 보호관리'가 가장 중요한 직무이며, 중요한 10개의 직무 중 5개의 직무가 정보통신보안과 관련된 직무로 확인되었다. 특히, '통합실태조사 수검'에 대한 직무가 2번째로 중요한 업무로 분석되었는데 이는 통합실태조사의 수검결과가 업체의 향후 사업획득에 큰 영향을 미치는 것으로 예상된다. 또한, 보안업무의 중·장기 계획으로 볼 수 있는 연간 보안업무 계획 수립 및 보안내규 제·개정 업무가 중요한 것으로 평가되었는데 이는 보안업무의 현재와 미래를 계획할 수 있는 업무로 업체와 보안전문가 입장에서 중요한 업무로 여겨진다.

보안일일결산 감독·통제 등 10개의 직무는 대부분 누구나 할 수 있는 단순한 직무로써 수시 또는 일상적으로 진행되는 행정위주 업무로 확인되었다. 중요도 상위 10개 직무와 중요도 하위 10개 직무는 표 29와 같다.

표 29. 중요도 상위 및 하위 10개 직무

Table 29. Top and bottom 10 jobs of importance

구 분	세부 직무	
중요도 상위 10개 직무	43. 방산 핵심기술 보호 관리	55. 통합실태조사 수검
	37. 네트워크(망분리 포함) 보안 관제 감독	3. 보안내규 제·개정
	2. 연간 보안업무계획 수립	38. 정보보호시스템 보안관제 감독
	54. 보안사고시 초동조치 및 관계기관 신고	42. 보안관제결과(해킹) 조치 관리 감독
	36. 전산기(서버) 보안관리 감독	9. 비밀 생산(접수) 보안관리
중요도 하위 10개 직무	4. 보안일일결산 감독·통제	8. 각종 보안행정서류 집행·관리
	50. 방산보안 대외협력 활동	35. 사내 보안취약지 점검
	49. 보안교육 성과분석	19. 보안서약서 집행 / 관리
	5. 보안수준평가 감독·통제	25. 해외 출장자 보안교육
	29. 출입증 관리	6./47. 하도급 보안특약조건 등 2개

표 30. 보안 직무의 중요도 측정 결과

Table 30. Security Job Importance Measurement Results

직무	세부 직무	중요도(평균)	분산	순위
보안 행정	1. 중장기 보안계획 수립	3.974	0.783	
	2. 연간 보안업무계획 수립	4.316	0.654	5★
	3. 보안내규 제·개정	4.342	0.772	4★
	4. 보안일일결산 감독·통제	2.711	1.076	55
	5. 보안수준평가 감독·통제	3.263	0.956	49
	6. 하도급 보안특약조건 검토 및 감독	3.316	0.978	45
	7. 수출입 보안 조치	3.737	1.010	
	8. 각종 보안행정서류 집행·관리	2.947	1.078	54
비밀 관리	9. 비밀 생산(접수) 보안관리	4.000	1.081	10★
	10. 비밀소유조사 / 재분류	3.605	0.894	
	11. 비밀 보관/관리실태 확인·감독	3.658	0.988	
	12. 대외발송자료 보안성 검토	3.816	0.803	
	13. 비밀 저장매체 관리	3.921	0.886	
	14. 비밀 보호조치(지정, 안전지출 등)	3.526	1.121	
	15. 비밀 반입 및 반출 통제	3.789	0.982	
	16. 비밀 서류철 작성 관리 감독	3.342	0.880	
인원 보안	17. 보안관계관 운용	3.711	0.968	
	18. 직원(협력사 등) 신원조사업무	3.605	0.678	
	19. 보안서약서 집행 / 관리	3.237	0.942	50
	20. 비밀취급인가업무 처리	3.553	0.849	
	21. 개인정보보호업무 처리	3.474	0.689	
	22. 핵심기술인력 보안조치	3.868	0.820	
	23. 외국인(직원) 보안관리	3.553	0.903	
	24. 퇴직자 보안조치	3.868	0.982	
	25. 해외 출장자 보안교육	3.263	0.686	48
시설/ 장비 보안	26. 보호구역(시설) 설정	3.868	0.766	
	27. 시설/장비 보호대책 구축	3.737	0.415	
	28. 출입통제시스템 운용	3.737	0.740	
	29. 출입증 관리	3.289	0.752	47
	30. 사진촬영(녹음) 통제	3.553	0.632	
	31. 비인가자 접근 / 출입 통제	3.737	0.686	
	32. 외래인 출입시 보안조치	3.658	0.664	
	33. 장비 수송시 보안조치	3.421	0.899	
	34. 유사시 시설/장비 보안조치	3.500	0.635	
	35. 사내 보안취약지 점검	3.158	0.731	52
정보 통신 보안	36. 전산기(서버) 보안관리 감독	4.237	0.510	9★
	37. 네트워크(망분리 포함) 보안 관제 감독	4.368	0.671	3★
	38. 정보보호시스템 보안관제 감독	4.289	0.590	6★

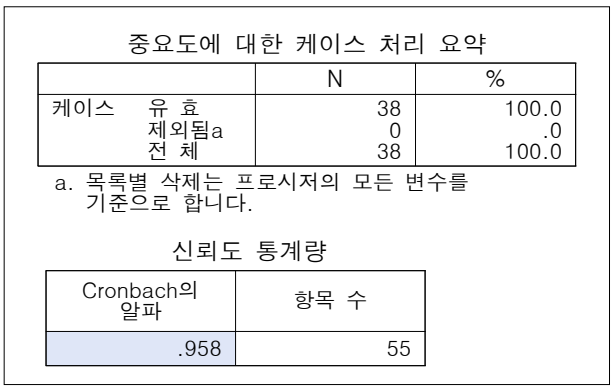
	39. 정보통신 장비 및 저장매체 관리	3.921	0.723	
	40. 개인용컴퓨터 보안관리	3.684	0.708	
	41. 협력업체 시스템 보안관리 감독	3.632	0.942	
	42. 보안관제결과(해킹) 조치 관리 감독	4.237	0.672	8★
	43. 방산 핵심기술 보호 관리	4.579	0.521	1★
	44. 재난대비 백업시설 유지관리 통제	3.737	0.632	
	45. 상용정보통신망 보안관리 통제	3.763	0.888	
보안교육/기타	46. 보안교육계획 수립	3.553	0.903	
	47. 주제/대상별 교안 작성	3.316	0.817	45
	48. 대내·외 보안교육 실시	3.395	0.516	
	49. 보안교육 성과분석	3.184	1.073	51
	50. 방산보안 대외협력 활동	3.132	0.982	53
보안점검/조사	51. 보안측정 의뢰/결과 조치	3.684	0.871	
	52. 부서/계열사 보안점검	3.447	0.849	
	53. 정기/수시 보안점검	3.684	0.871	
	54. 보안사고시 초동조치 및 관계기관 신고	4.237	0.834	7★
	55. 통합실태조사 수검	4.474	0.851	2★
평 균 값		3.684		

표 30에서 보는 바와 같이 중요도의 평균 값은 3.684로 높게 측정되었는데, 이는 방산업체 보안전문가들은 스스로 자신의 직무가 중요하다고 인식하고 있으며, 직무가 소홀할 경우 업체 운영에 상대적으로 또는 크게 영향을 미치는 것으로 분석되었다.(업체 상대적 영향: 3, 업체 크게 영향: 4)

다음은 분산 값에 대해 알아보겠다. 분산 값이 1을 초과하는 값은 표 30에서와 같이 보안일일결산 감독·통제 등 6개로 확인되었다. 보안일일결산, 각종 행정서류 집행, 비밀생산(접수) 보안관리, 비밀 보호조치(지정, 안전지출 등)는 업체에서 보안업무를 수행하는 보안전문가의 강조 여부 및 이행 정도에 따라 다르게 나타나는 것으로 볼 수 있다. 특히, 각종 행정서류 집행 외 4개 세부 직무의 경우 소홀히 했을 경우 보안사고로 이어지는 경향이 강하다. 따라서, 형식적이냐 실질적이냐에 따라 중요도의 수준 차이를 보이게 된다. 수출입 보안조치는 업체의 규모와 수출입 관련 업무를 수행하느냐에 따라 중요도에 차이가 나타나게 된 것이다.

따라서, 설문자의 업체의 임무에 따라 다르게 평가한 것으로 분석되었다.

그림 15와 같이 설문대상자 38명의 중요도 55개 항목에 대한 Cronbach'α 값[23]이 0.958로 나와 설문자들의 설문 답변에 대한 신뢰도는 매우 높은 것으로 확인되었다.



중요도에 대한 케이스 처리 요약

		N	%
케이스	유 효	38	100.0
	제외됨a	0	.0
	전 체	38	100.0

a. 목록별 삭제는 프로시저의 모든 변수를 기준으로 합니다.

신뢰도 통계량

Cronbach의 알파	항목 수
.958	55

그림 15. 중요도 측정에 대한 Cronbach'α 값(55개 항목)
Figure 15. Cronbach'α value for measuring importance (55 items)

2. 난이도 분석 결과

방산업체 보안전문가 직무에 대한 분석결과 '통합실태조사 수검'이 가장 난이도가 높은 세부 직무로 확인되었으며, 난이도 10개의 직무 중 5개의 세부직무가 정보통신보안과 관련된 직무로 확인되었다. 특히, 정보통신보안과 관련된 직무 중 전산기(서버) 보안관리 감독 등 5개 세부 직무는 고도의 전문성과 교육이 필요한 직무로 분석되었다. 또한, 중·장기 보안계획 수립, 보안내규 제·개정, 보안사고시 초동조치 및 관계기관 신고, 수출입 보안관리에 대한 업무를 어려워하는 것으로 확인되었다.

23) 크롬바하 알파 값이 0.60을 넘으면 신뢰도가 만족할 만한 수준으로 판단, 1에 가까울수록 높은 신뢰도(조철호, SPSS/AMOS 활용 구조방정식모형 논문통계분석, 도서출판 청람, 2014.)

보안서약서 집행/관리, 보안일일결산 감독·통제, 출입증 관리, 각종 보안행정서류 집행·관리, 외래인 출입시 보안조치, 사진촬영(녹음) 통제, 장비 수송시 보안조치, 사내 보안취약지 점검은 반복되는 일상적인 업무이며, 비밀취급인가 업무처리와 직원(협력사) 신원조사업무는 신청 및 종합 후 관계기관에 제출하는 단순 종합업무로 확인되었다. 난이도 상위 10개 직무와 난이도 하위 10개 세부 직무는 표 31과 같다.

표 31. 난이도 상위 및 하위 10개 직무

Table 31. Top and bottom 10 jobs in difficulty

구 분	세부 직무	
난이도 상위 10개 직무	55. 통합실태조사 수검	36. 전산기(서버) 보안관리 감독
	38. 정보보호시스템 보안관제 감독	37. 네트워크(망분리 포함) 보안 관제 감독
	43. 방산 핵심기술 보호 관리	1. 중장기 보안계획 수립
	42. 보안관제결과(해킹) 조치 관리 감독	3. 보안내규 제·개정
	54. 보안사고시 초동조치 및 관계기관 신고	7. 수출입 보안 조치
난이도 하위 10개 직무	19. 보안서약서 집행 / 관리	4. 보안일일결산 감독·통제
	29. 출입증 관리	8. 각종 보안행정서류 집행·관리
	32. 외래인 출입시 보안조치	20. 비밀취급인가업무 처리
	30. 사진촬영(녹음) 통제	33. 장비 수송시 보안조치
	18. 직원(협력사 등) 신원조사업무	35. 사내 보안취약지 점검

표 32. 보안 직무의 난이도 측정 결과

Table 32. Security Job Difficulty Measurement Results

직무	세부 직무	난이도(평균)	분산	순위
보안 행정	1. 중장기 보안계획 수립	3.947	0.754	6★
	2. 연간 보안업무계획 수립	3.763	0.402	
	3. 보안내규 제·개정	3.895	1.016	8★
	4. 보안일일결산 감독·통제	2.184	1.073	54
	5. 보안수준평가 감독·통제	3.263	1.118	
	6. 하도급 보안특약조건 검토 및 감독	3.158	1.110	
	7. 수출입 보안 조치	3.763	0.888	10★
	8. 각종 보안행정서류 집행·관리	2.368	0.996	52

비밀 관리	9. 비밀 생산(접수) 보안관리	3.263	0.902	
	10. 비밀소유조사 / 재분류	3.079	1.264	
	11. 비밀 보관/관리실태 확인・감독	3.105	0.908	
	12. 대외발송자료 보안성 검토	3.474	0.688	
	13. 비밀 저장매체 관리	3.053	0.754	
	14. 비밀 보호조치(지정, 안전지출 등)	2.868	0.820	
	15. 비밀 반입 및 반출 통제	3.026	0.621	
	16. 비밀 서류철 작성 관리 감독	2.842	0.893	
인원 보안	17. 보안관계관 운용	3.158	1.164	
	18. 직원(협력사 등) 신원조사업무	2.632	0.780	47
	19. 보안서약서 집행 / 관리	2.132	0.658	55
	20. 비밀취급인가업무 처리	2.500	0.581	50
	21. 개인정보보호업무 처리	2.684	0.979	
	22. 핵심기술인력 보안조치	3.342	0.988	
	23. 외국인(직원) 보안관리	2.974	0.999	
	24. 퇴직자 보안조치	3.000	0.865	
	25. 해외 출장자 보안교육	2.789	0.711	
	26. 보호구역(시설) 설정	3.237	0.780	
시설/ 장비 보안	27. 시설/장비 보호대책 구축	3.289	1.022	
	28. 출입통제시스템 운용	2.921	0.994	
	29. 출입증 관리	2.289	0.914	53
	30. 사진촬영(녹음) 통제	2.553	1.065	49
	31. 비인가자 접근 / 출입 통제	2.658	0.880	
	32. 외래인 출입시 보안조치	2.474	0.797	51
	33. 장비 수송시 보안조치	2.553	0.686	48
	34. 유사시 시설/장비 보안조치	2.763	0.726	
	35. 사내 보안취약지 점검	2.632	1.104	46
정보 통신 보안	36. 전산기(서버) 보안관리 감독	4.263	0.794	2★
	37. 네트워크(망분리 포함) 보안 관제 감독	4.237	0.996	4★
	38. 정보보호시스템 보안관제 감독	4.237	0.888	3★
	39. 정보통신 장비 및 저장매체 관리	3.605	1.056	
	40. 개인용컴퓨터 보안관리	3.184	0.965	
	41. 협력업체 시스템 보안관리 감독	3.368	1.104	
	42. 보안관제결과(해킹) 조치 관리 감독	3.921	1.048	7★
	43. 방산 핵심기술 보호 관리	4.079	0.777	5★
	44. 재난대비 백업시설 유지관리 통제	3.632	0.780	
	45. 상용정보통신망 보안관리 통제	3.632	0.834	
보안 교육 / 기타	46. 보안교육계획 수립	3.342	0.772	
	47. 주제/대상별 교안 작성	3.474	0.797	
	48. 대내・외 보안교육 실시	3.211	0.657	
	49. 보안교육 성과분석	3.421	1.061	
	50. 방산보안 대외협력 활동	2.947	1.349	

보안 점검 / 조사	51. 보안측정 의뢰/결과 조치	3.553	0.849	
	52. 부서/계열사 보안점검	3.342	0.826	
	53. 정기/수시 보안점검	3.342	0.772	
	54. 보안사고시 초동조치 및 관계기관 신고	3.789	0.927	9★
	55. 통합실태조사 수검	4.342	0.718	1★
평 균 값		3.210		

표 32에서 보는 바와 같이 난이도의 평균값은 3.210로 기준치(3.0)보다 다소 높게 평가되었는데, 이는 방산업체 보안전문가가 업무를 수행하는데 있어 정보통신보안 등 일부 전문성을 요구하는 직무에 어려움이 있음을 예측할 수 있다.

다음은 분산 값에 대해 알아보겠다. 분산 값이 1을 초과하는 값은 표 32와 같이 보안내규 제·개정, 보안일일결산 감독·통제, 보안수준평가 감독·통제, 하도급 보안특약조건 검토 및 감독, 비밀소유조사/재분류, 시설/장비 보호대책 구축, 사진촬영(녹음) 통제, 사내 보안취약지 점검, 보안교육 성과분석 등 9개 세부 직무로 직무의 경력·경험에 따라 난이도가 차이가 생기는 것으로 판단되며, 정보통신보안 직무 중 정보통신 장비 및 저장매체 관리, 협력업체 시스템 보안관리 감독, 보안관제결과(해킹) 조치 관리 감독 등 3개 세부직무는 전산분야 전문성 여부에 따라 난이도가 차이가 발생함을 보여주고 있다. 또한, 보안관계관 운용과 관련 난이도의 차이를 보이는 것은 해당 업체의 보안 관계관 선정의 협조 여부에 따라 난이도가 생기는 것으로 보이며, 방산보안 대외협력활동에 차이가 보이는 것은 방산업체 보안전문가들의 대내·외적 활동과 개인적인 성향에 따라 차이가 나타난 것으로 판단하였다

그림 16과 같이 설문대상자 38명의 난이도 55개 항목에 대한 Cronbach'α 값이 0.965로 나와 설문자들의 난이도 설문 답변에 대한 신뢰도는 매우 높은 것으로 분석되었다.

난이도에 대한 케이스 처리 요약

		N	%
케이스	유 효	38	100.0
	제외됨a	0	.0
	전 체	38	100.0

a. 목록별 삭제는 프로시저의 모든 변수를 기준으로 합니다.

신뢰도 통계량

Cronbach의 알파	항목 수
.965	55

그림 16. 난이도 측정에 대한 Cronbach'α 값(55개 항목)
Figure 16. Cronbach'α value for difficulty measurement (55 items)

3. 수행빈도 분석 결과

방산업체 보안전문가 직무에 대한 분석결과 '보안일일결산 감독・통제'가 가장 수행빈도가 높은 세부 직무로 확인되었으며, 난이도 10개의 직무 중 출입증 관리, 출입통제시스템 운용, 외래인 출입시 보안조치, 사진촬영(녹음) 통제, 비인가자 접근/출입 통제 등 5개의 세부 직무가 시설/장비 보안과 관련된 직무로 확인되었고, 정보통신보안과 관련된 직무 중 정보보호시스템 보안관제 감독, 정보통신장비 및 저장매체 관리, 개인용컴퓨터 보안관리 등 3개 세부 직무가 수행빈도가 높았다.

중・장기 보안계획 수립 등 계획분야와 관련된 직무와 보안교육 성과분석 등 교육과 관련된 직무 및 매년 1회 실시하는 통합실태조사 업무가 수행빈도가 낮은 직무로 분석되었다. 수행빈도 상위 10개 직무와 수행빈도 하위 10개 세부직무는 표 33과 같다.

표 33. 수행빈도 상위 및 하위 10개 직무

Table 33. Top and bottom 10 jobs in frequency of performance

구 분	세부 직무	
수행빈도 상위 10개 직무	4. 보안일일결산 감독・통제	29. 출입증 관리
	32. 외래인 출입시 보안조치	28. 출입통제시스템 운용
	31. 비인가자 접근/출입 통제	40. 개인용컴퓨터 보안관리
	8. 각종 보안행정서류 집행・관리	38. 정보보호시스템 보안관제 감독
	30. 사진촬영(녹음) 통제	39. 정보통신 장비 및 저장매체 관리
수행빈도 하위 10개 직무	1. 중장기 보안계획 수립	55. 통합실태조사 수검
	2. 연간 보안업무계획 수립	3. 보안내규 제・개정
	10. 비밀소유조사 / 재분류	49. 보안교육 성과분석
	54. 보안사고시 초동조치 및 관계기관 신고	46. 보안교육계획 수립
	27. 시설/장비 보호대책 구축	6. 하도급 보안특약조건 검토 및 감독

표 34. 보안 직무의 수행빈도 측정 결과

Table 34. Performance frequency measurement result of security job

직무	세부 직무	수행빈도(평균)	분산	순위
보안 행정	1. 중장기 보안계획 수립	1.079	0.075	55
	2. 연간 보안업무계획 수립	1.184	0.208	53
	3. 보안내규 제・개정	1.316	0.384	52
	4. 보안일일결산 감독・통제	4.789	0.225	1★
	5. 보안수준평가 감독・통제	2.263	1.280	
	6. 하도급 보안특약조건 검토 및 감독	2.105	0.908	46
	7. 수출입 보안 조치	2.105	1.070	
	8. 각종 보안행정서류 집행・관리	3.842	1.704	7★
비밀 관리	9. 비밀 생산(접수) 보안관리	2.632	1.536	
	10. 비밀소유조사 / 재분류	1.737	0.632	51
	11. 비밀 보관/관리실태 확인・감독	2.553	1.335	
	12. 대외발송자료 보안성 검토	3.684	1.195	
	13. 비밀 저장매체 관리	3.132	1.469	
	14. 비밀 보호조치(지정, 안전지출 등)	2.500	1.446	
	15. 비밀 반입 및 반출 통제	3.026	1.486	
	16. 비밀 서류철 작성 관리 감독	2.842	1.164	
인원 보안	17. 보안관계관 운용	2.632	1.590	
	18. 직원(협력사 등) 신원조사업무	3.447	1.389	
	19. 보안서약서 집행 / 관리	3.711	1.292	

	20. 비밀취급인가업무 처리	2.947	1.294	
	21. 개인정보보호업무 처리	2.974	1.540	
	22. 핵심기술인력 보안조치	2.816	1.452	
	23. 외국인(직원) 보안관리	2.632	1.698	
	24. 퇴직자 보안조치	3.211	1.144	
	25. 해외 출장자 보안교육	3.158	1.218	
	26. 보호구역(시설) 설정	1.842	0.947	
시설/장비 보안	27. 시설/장비 보호대책 구축	2.079	0.885	47
	28. 출입통제시스템 운용	4.026	1.432	4★
	29. 출입증 관리	4.053	1.132	2★
	30. 사진촬영(녹음) 통제	3.842	1.110	9★
	31. 비인가자 접근 / 출입 통제	3.974	1.053	5★
	32. 외래인 출입시 보안조치	4.026	1.107	3★
	33. 장비 수송시 보안조치	3.000	1.459	
	34. 유사시 시설/장비 보안조치	2.211	1.144	
	35. 사내 보안취약지 점검	2.737	1.226	
정보통신 보안	36. 전산기(서버) 보안관리 감독	3.500	1.392	
	37. 네트워크(망분리 포함) 보안 관제 감독	3.632	1.374	
	38. 정보보호시스템 보안관제 감독	3.842	1.164	8★
	39. 정보통신 장비 및 저장매체 관리	3.816	0.911	10★
	40. 개인용컴퓨터 보안관리	3.868	1.144	6★
	41. 협력업체 시스템 보안관리 감독	2.632	0.725	
	42. 보안관제결과(해킹) 조치 관리 감독	3.368	1.698	
	43. 방산 핵심기술 보호 관리	3.368	1.266	
	44. 재난대비 백업시설 유지관리 통제	2.632	1.428	
	45. 상용정보통신망 보안관리 통제	3.316	1.573	
보안교육/기타	46. 보안교육계획 수립	1.921	0.885	48
	47. 주제/대상별 교안 작성	2.237	0.672	
	48. 대내·외 보안교육 실시	2.526	0.743	
	49. 보안교육 성과분석	1.816	0.857	50
	50. 방산보안 대외협력 활동	2.500	0.959	
보안점검/조사	51. 보안측정 의뢰/결과 조치	2.158	1.001	
	52. 부서/계열사 보안점검	2.237	0.888	
	53. 정기/수시 보안점검	2.474	1.175	
	54. 보안사고시 초동조치 및 관계기관 신고	1.895	2.097	49
	55. 통합실태조사 수검	1.158	0.137	54
평 균 값		2.818		

표 34에서 보는 바와 같이 수행빈도 평균값은 2.818로 평가되었는데, 이는 방산업체 보안 업무가 일일단위 기본적으로 수행하는 직무 외 대부분 주간 및 월간

단위 직무로 수행되고 있다는 것을 보여주고 있다.(3:주간-월간)

다음은 분산 값에 대해 알아보겠다. 분산 값이 1을 초과하는 값은 표 34와 같이 55개의 세부 직무 중 38개에서 확인되었는데, 약 69%의 업무가 업체의 특징과 업체 마다의 근무 여건에 따라 수시로 차이가 발생하고 있음을 보여주고 있다. 특히, 보안사고시 초동조치 및 관계기관 신고는 2.097의 큰 분산값을 보여주고 있는데, 이는 업체의 보안사고 발생 여부에 따라 수행빈도의 차이가 발생하는 것으로 판단하였다.

그림 17과 같이 설문대상자 38명의 수행빈도 55개 항목에 대한 Cronbach'α 값이 0.885로 나와 설문자들의 수행빈도 설문 답변에 대한 신뢰도는 높은 것으로 분석되었다.

수행빈도에 대한 케이스 처리 요약

		N	%
케이스	유 효	38	100.0
	제외됨a	0	.0
	전 체	38	100.0

a. 목록별 삭제는 프로시저의 모든 변수를 기준으로 합니다.

신뢰도 통계량

Cronbach의 알파	항목 수
.885	55

그림 17. 수행빈도 측정에 대한 Cronbach'α 값(55개 항목)
Figure 17. Cronbach'α value for performance frequency measurement (55 items)

4. 방산업체 보안전문가 직무 평균 값

표 35는 방산업체 보안전문가의 세부직무에 대한 중요도・난이도・수행빈도의 직무 평균값을 나타낸 도표이다. 다음 직무영향 분석 단계에서는 상기 도표를 기초로 IPA 분석을 진행하겠다.

표 35. 방산업체 보안전문가 세부직무 평균 값

Table 35. Average value of detailed jobs for security experts in defense industry

직무	세부 직무	중요도	난이도	수행빈도
보안 행정	1. 중장기 보안계획 수립	3.974	3.947	1.079
	2. 연간 보안업무계획 수립	4.316	3.763	1.184
	3. 보안내규 제·개정	4.342	3.895	1.316
	4. 보안일일결산 감독·통제	2.711	2.184	4.789
	5. 보안수준평가 감독·통제	3.263	3.263	2.263
	6. 하도급 보안특약조건 검토 및 감독	3.316	3.158	2.105
	7. 수출입 보안 조치	3.737	3.763	2.105
	8. 각종 보안행정서류 집행·관리	2.947	2.368	3.842
비밀 관리	9. 비밀 생산(접수) 보안관리	4.000	3.263	2.632
	10. 비밀소유조사 / 재분류	3.605	3.079	1.737
	11. 비밀 보관/관리실태 확인·감독	3.658	3.105	2.553
	12. 대외발송자료 보안성 검토	3.816	3.474	3.684
	13. 비밀 저장매체 관리	3.921	3.053	3.132
	14. 비밀 보호조치(지정, 안전지출 등)	3.526	2.868	2.500
	15. 비밀 반입 및 반출 통제	3.789	3.026	3.026
	16. 비밀 서류철 작성 관리 감독	3.342	2.842	2.842
인원 보안	17. 보안관계관 운용	3.711	3.158	2.632
	18. 직원(협력사 등) 신원조사업무	3.605	2.632	3.447
	19. 보안서약서 집행 / 관리	3.237	2.132	3.711
	20. 비밀취급인가업무 처리	3.553	2.500	2.947
	21. 개인정보보호업무 처리	3.474	2.684	2.974
	22. 핵심기술인력 보안조치	3.868	3.342	2.816
	23. 외국인(직원) 보안관리	3.553	2.974	2.632
	24. 퇴직자 보안조치	3.868	3.000	3.211
	25. 해외 출장자 보안교육	3.263	2.789	3.158
시설 / 장비 보안	26. 보호구역(시설) 설정	3.868	3.237	1.842
	27. 시설/장비 보호대책 구축	3.737	3.289	2.079
	28. 출입통제시스템 운용	3.737	2.921	4.026
	29. 출입증 관리	3.289	2.289	4.053
	30. 사진촬영(녹음) 통제	3.553	2.553	3.842
	31. 비인가자 접근 / 출입 통제	3.737	2.658	3.974
	32. 외래인 출입시 보안조치	3.658	2.474	4.026
	33. 장비 수송시 보안조치	3.421	2.553	3.000
	34. 유사시 시설/장비 보안조치	3.500	2.763	2.211
	35. 사내 보안취약지 점검	3.158	2.632	2.737
정보 통신 보안	36. 전산기(서버) 보안관리 감독	4.237	4.263	3.500
	37. 네트워크(망분리 포함) 보안 관제 감독	4.368	4.237	3.632
	38. 정보보호시스템 보안관제 감독	4.289	4.237	3.842
	39. 정보통신 장비 및 저장매체 관리	3.921	3.605	3.816
	40. 개인용컴퓨터 보안관리	3.684	3.184	3.868
	41. 협력업체 시스템 보안관리 감독	3.632	3.368	2.632
	42. 보안관제결과(해킹) 조치 관리 감독	4.237	3.921	3.368
	43. 방산 핵심기술 보호 관리	4.579	4.079	3.368
	44. 재난대비 백업시설 유지관리 통제	3.737	3.632	2.632
	45. 상용정보통신망 보안관리 통제	3.763	3.632	3.316
보안 교육 / 기타	46. 보안교육계획 수립	3.553	3.342	1.921
	47. 주제/대상별 교안 작성	3.316	3.474	2.237
	48. 대내·외 보안교육 실시	3.395	3.211	2.526
	49. 보안교육 성과분석	3.184	3.421	1.816
	50. 방산보안 대외협력 활동	3.132	2.947	2.500
보안 점검 / 조사	51. 보안측정 의뢰/결과 조치	3.684	3.553	2.158
	52. 부서/계열사 보안점검	3.447	3.342	2.237
	53. 정기/수시 보안점검	3.684	3.342	2.474
	54. 보안사고시 초동조치 및 관계기관 신고	4.237	3.789	1.895
	55. 통합실태조사 수검	4.474	4.342	1.158
각 요소별 평균 값		**3.684**	**3.210**	**2.818**
Cronbach'α 값		**0.958**	**0.965**	**0.885**

제3절 방산업체 보안전문가 직무영향 분석

1. 중요도-수행빈도 IPA 분석

그림 18에서와 같이 중요도-수행빈도에 대한 각 사분면별 방산업체 보안전문가의 세부직무를 표현해 보았다. 표 13(연구자가 수정한 각 사분면 IPA 매트릭스 분석, p34)에서 제시한 것과 같이 1사분면은 지속개발 구간으로 인력 충원이 요구되며, 2사분면은 현상유지 구간, 3사분면은 낮은 우선순위 구간으로 인원 재판단(또는 현 보직자에 대한 추가 임무 부여)이 요구되고, 4사분면은 선택적 인력 재편(필요한 직무분석을 통한 선택적 인원 충원)이 필요한 구간으로 판단하였으며 각 직무별 IPA 분석결과를 세부적으로 알아보겠다.

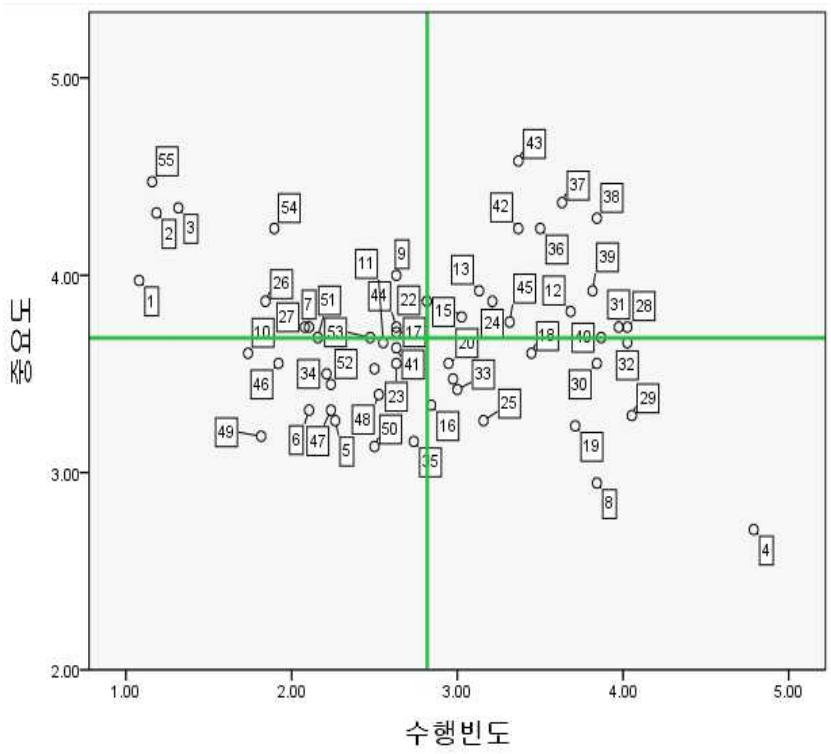


그림 18. 중요도-수행빈도 IPA 분석 종합
Figure 18. Importance - performance frequency IPA Analysis Synthesis

첫째, 표 36을 기초로 '보안행정' 직무에 대한 중요도-수행빈도 IPA 분석결과는 다음과 같다.

표 36. 중요도-수행빈도 직무 값(보안행정)
Table 36. Importance - Performance Frequency Job Value(Security Administration)

직무	세부 직무	중요도	수행빈도
보안행정	1. 중장기 보안계획 수립	3.974	1.079
	2. 연간 보안업무계획 수립	4.316	1.184
	3. 보안내규 제·개정	4.342	1.316
	4. 보안일일결산 감독·통제	2.711	4.789
	5. 보안수준평가 감독·통제	3.263	2.263
	6. 하도급 보안특약조건 검토 및 감독	3.316	2.105
	7. 수출입 보안 조치	3.737	2.105
	8. 각종 보안행정서류 집행·관리	2.947	3.842

그림 19에서 보는 바와 같이 1사분면(지속개발)에 해당하는 직무는 없으며, 현상유지 구간인 2사분면에는 1. 중장기 보안계획 수립, 2. 연간 보안업무계획 수립, 3.보안내규 제·개정, 7. 수출입 보안조치로 현상유지가 필요한 직무이다. 3사분면(낮은 우선순위)에 해당되는 직무는 5. 보안수준평가 감독·통제, 6. 하도급 보안특약조건 검토 및 감독으로 중요성과 수행빈도가 전부 낮은 직무로써 인원 재판단이 요구되는 구간이다. 과잉노력을 지양하는 4사분면에는 4. 보안일일결산 감독·통제, 8. 각종 행정서류 집행·관리 직무로 단순인력으로 조정하거나, 선택적 인력으로 재편성이 필요한 구간이다.

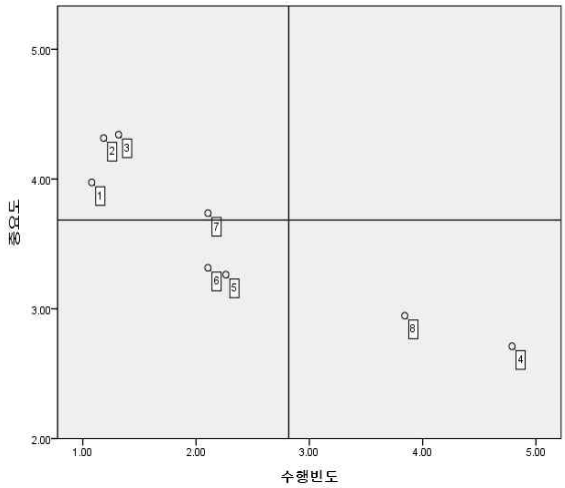


그림 19. 중요도-수행빈도 IPA 분석 도표(보안행정)
Figure 19. Importance - performance frequency IPA analysis chart (security administration)

둘째, 표 37을 기초로 '비밀관리' 직무에 대한 중요도-수행빈도 IPA 분석결과는 다음과 같다.

표 37. 중요도-수행빈도 직무 값(비밀관리)
Table 37. Importance - Performance Frequency Job Value(Secret management)

직무	세부 직무	중요도	수행빈도
비밀 관리	9. 비밀 생산(접수) 보안관리	4.000	2.632
	10. 비밀소유조사/재분류	3.605	1.737
	11. 비밀 보관/관리실태 확인・감독	3.658	2.553
	12. 대외발송자료 보안성 검토	3.816	3.684
	13. 비밀 저장매체 관리	3.921	3.132
	14. 비밀 보호조치(지정, 안전지출 등)	3.526	2.500
	15. 비밀 반입 및 반출 통제	3.789	3.026
	16. 비밀 서류철 작성 관리 감독	3.342	2.842

그림 20에서 보는 바와 같이 1사분면(지속개발)은 12. 대외발송자료 보안성검토, 13. 비밀 저장매체 관리, 15. 비밀 반입 및 반출 통제이며, 2사분면(현상유지)은 9. 비밀 생산(접수) 보안관리이며, 3사분면(낮은 우선순위)은 10. 비밀 소유조사/재분류, 11. 비밀 보관/관리 실태 확인·감독, 14. 비밀 보호조치(지정, 안전지출 등)이며, 4사분면(과잉노력 지양)은 16. 비밀 서류철 작성 관리 감독이다.

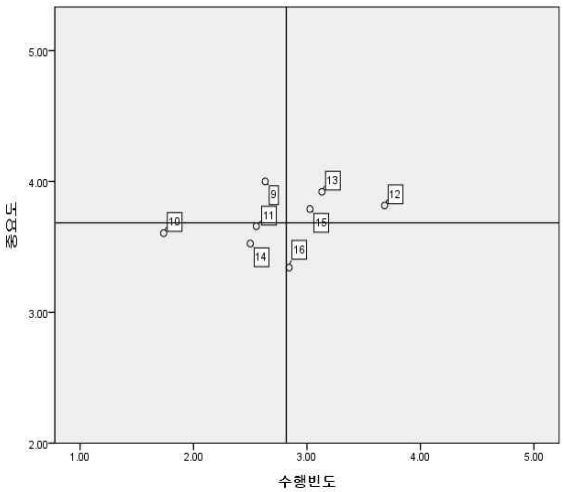


그림 20. 중요도-수행빈도 IPA 분석 도표(비밀관리)
Figure 20. Importance - performance frequency IPA analysis chart (Secret management)

셋째, 표 38을 기초로 '인원보안' 직무에 대한 중요도-수행빈도 IPA 분석결과는 다음과 같다.

표 38. 중요도-수행빈도 직무 값(인원보안)
Table 38. Importance - Performance Frequency Job Value(Personnel security)

직무	세부 직무	중요도	수행빈도
인원 보안	17. 보안관계관 운용	3.711	2.632
	18. 직원(협력사 등) 신원조사업무	3.605	3.447
	19. 보안서약서 집행 / 관리	3.237	3.711

	20. 비밀취급인가업무 처리	3.553	2.947
	21. 개인정보보호업무 처리	3.474	2.974
	22. 핵심기술인력 보안조치	3.868	2.816
	23. 외국인(직원) 보안관리	3.553	2.632
	24. 퇴직자 보안조치	3.868	3.211
	25. 해외 출장자 보안교육	3.263	3.158

그림 21에서 보는 바와 같이 1사분면(지속개발)은 24. 퇴직자 보안조치이며, 2사분면(현상유지)은 17. 보안관계관 운용, 22. 핵심기술인력 보안조치이며, 3사분면(낮은 우선순위)은 23. 외국인(직원) 보안관리이며, 4사분면(과잉노력 지양)은 18. 직원(협력사) 신원조사 업무, 19. 보안서약서 집행관리, 20. 비밀취급인가 업무 처리, 21. 개인정보보호업무 처리, 25. 해외 출장자 보안교육이다.

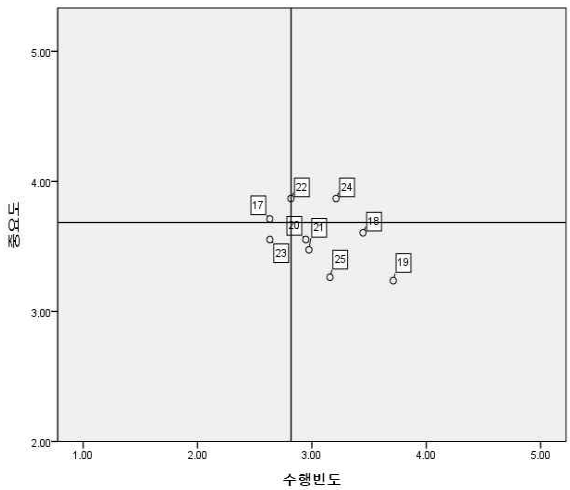


그림 21. 중요도-수행빈도 IPA 분석 도표(인원보안)
Figure 21. Importance - performance frequency IPA analysis chart (Personnel security)

네째, 표 39을 기초로 '시설/장비보안' 직무에 대한 중요도-수행빈도 IPA 분석 결과는 다음과 같다.

표 39. 중요도-수행빈도 직무 값(시설/장비보안)
Table 39. Importance - Performance Frequency Job Value(Facility & Equipment Security)

직무	세부 직무	중요도	수행빈도
시설/장비보안	26. 보호구역(시설) 설정	3.868	1.842
	27. 시설/장비 보호대책 구축	3.737	2.079
	28. 출입통제시스템 운용	3.737	4.026
	29. 출입증 관리	3.289	4.053
	30. 사진촬영(녹음) 통제	3.553	3.842
	31. 비인가자 접근/출입 통제	3.737	3.974
	32. 외래인 출입시 보안조치	3.658	4.026
	33. 장비 수송시 보안조치	3.421	3.000
	34. 유사시 시설/장비 보안조치	3.500	2.211
	35. 사내 보안취약지 점검	3.158	2.737

그림 22에서 보는 바와 같이 1사분면(지속개발)은 28. 출입통제시스템 운용, 31. 비인가자 접근/출입 통제 이며, 2사분면(현상유지)은 26. 보호구역(시설) 설정, 27. 시설/장비 보호대책 구축 이며, 3사분면(낮은 우선순위)은 34. 유사시 시설/장비 보호조치, 35. 사내 보안취약지 점검이며, 4사분면(과잉노력 지양)은 29. 출입증 관리, 30. 사진촬영(녹음) 통제, 32. 외래인 출입시 보안조치, 33. 장비 수송시 보안조치이다.

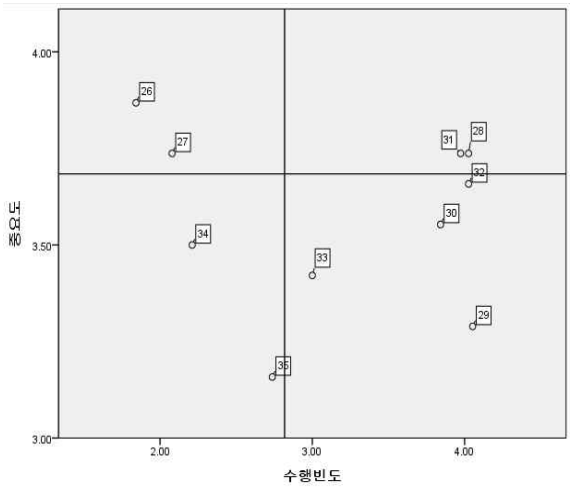


그림 22. 중요도-수행빈도 IPA 분석 도표(시설/장비보안)
Figure 22. Importance - performance frequency IPA analysis chart (Facility & Equipment Security)

다섯째, 표 40을 기초로 '정보통신보안' 직무에 대한 중요도-수행빈도 IPA 분석 결과는 다음과 같다.

표 40. 중요도-수행빈도 직무 값(정보통신보안)
Table 40. Importance - Performance Frequency Job Value(Information& communication security)

직무	세부 직무	중요도	수행빈도
정보 통신 보안	36. 전산기(서버) 보안관리 감독	4.237	3.500
	37. 네트워크(망분리 포함) 보안 관제 감독	4.368	3.632
	38. 정보보호시스템 보안관제 감독	4.289	3.842
	39. 정보통신 장비 및 저장매체 관리	3.921	3.816
	40. 개인용컴퓨터 보안관리	3.684	3.868
	41. 협력업체 시스템 보안관리 감독	3.632	2.632
	42. 보안관제결과(해킹) 조치 관리 감독	4.237	3.368
	43. 방산 핵심기술 보호 관리	4.579	3.368

	44. 재난대비 백업시설 유지관리 통제	3.737	2.632
	45. 상용정보통신망 보안관리 통제	3.763	3.316

그림 23에서 보는 바와 같이 1사분면(지속개발)은 36. 전산기(서버) 보안관리 감독, 37. 네트워크(망분리 포함) 보안 관제 감독, 38. 정보보호시스템 보안관제 감독, 39. 정보통신 장비 및 저장매체 관리, 40. 개인용컴퓨터 보안관리, 42. 보안관제결과(해킹) 조치 관리 감독, 43. 방산 핵심기술 보호 관리, 45. 상용정보통신망 보안관리 통제이며, 2사분면(현상유지)은 44. 재난대비 백업시설 유지관리 통제이며, 3사분면(낮은 우선순위)은 41. 협력업체 시스템 보안관리 감독이며, 4사분면은 없다. 이와 같이 정보통신보안업무는 대부분 지속개발하고 인원충원이 필요한 직무로 확인되었다.

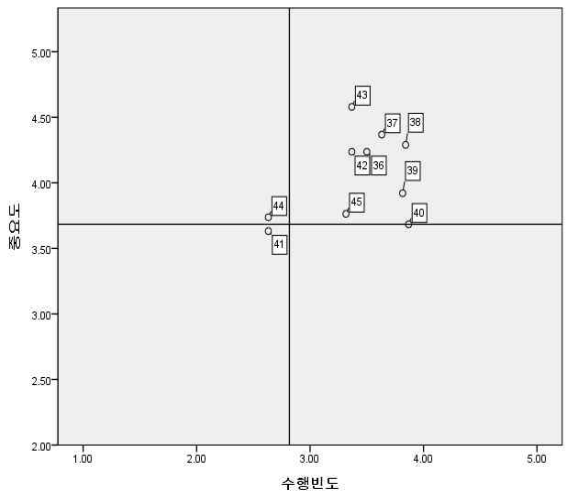


그림 23. 중요도-수행빈도 IPA 분석 도표(정보통신보안)
Figure 23. Importance - performance frequency IPA analysis chart (Information& communication security)

여섯째, 표 41을 기초로 '보안교육/기타' 직무에 대한 중요도-수행빈도 IPA 분석결과는 다음과 같다.

표 41. 중요도-수행빈도 직무 값(보안교육/기타)
Table 41. Importance - Performance Frequency Job Value(Security training/other)

직무	세부 직무	중요도	수행빈도
보안교육/기타	46. 보안교육계획 수립	3.553	1.921
	47. 주제/대상별 교안 작성	3.316	2.237
	48. 대내·외 보안교육 실시	3.395	2.526
	49. 보안교육 성과분석	3.184	1.816
	50. 방산보안 대외협력 활동	3.132	2.500

그림 24에서 보는 바와 같이 보안교육/기타 직무는 전체가 3사분면(낮은 우선순위)에 해당되는 것으로 확인되었다.

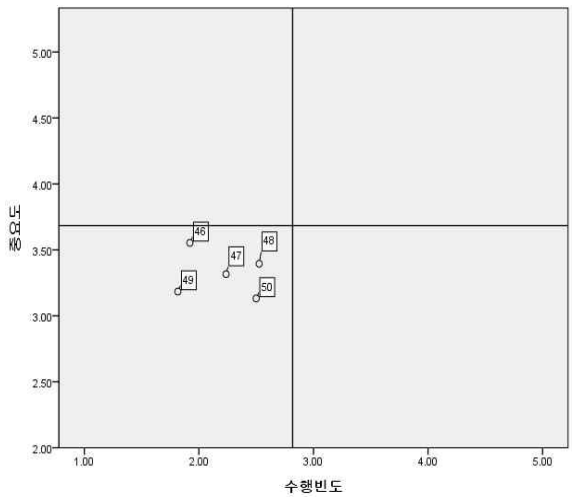


그림 24. 중요도-수행빈도 IPA 분석 도표(보안교육/기타)
Figure 24. Importance - performance frequency IPA analysis chart (Security training/other)

일곱째, 표 42을 기초로 '보안점검/조사' 직무에 대한 중요도-수행빈도 IPA 분석결과는 다음과 같다.

표 42. 중요도-수행빈도 직무 값(보안점검/조사)
Table 42. Importance - Performance Frequency Job Value(Security inspection/investigation)

직무	세부 직무	중요도	수행빈도
보안점검/조사	51. 보안측정 의뢰/결과 조치	3.684	2.158
	52. 부서/계열사 보안점검	3.447	2.237
	53. 정기/수시 보안점검	3.684	2.474
	54. 보안사고시 초동조치 및 관계기관 신고	4.237	1.895
	55. 통합실태조사 수검	4.474	1.158

그림 25에서 보는 바와 같이 보안점검/조사 직무는 1사분면은 없으며, 2사분면은 51. 보안측정 의뢰/결과 조치, 53. 정기/수시 보안점검, 54. 보안사고시 초동조치 및 관계기관 신고, 55. 통합실태조사 수검이며, 3사분면(낮은 우선순위)은 52. 부서/계열사 보안점검으로 확인되었다. 이처럼 보안점검/조사 직무는 부서/계열사 보안점검 외 대체로 중요한 직무이나, 수행빈도는 낮은 직무로 확인되었다.

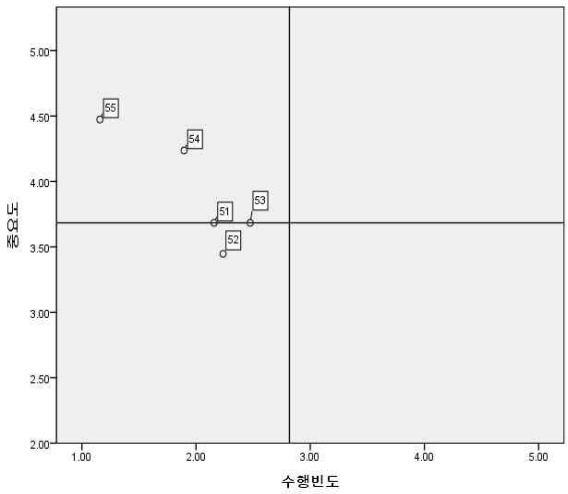


그림 25. 중요도-수행빈도 IPA 분석 도표(보안점검/조사)
Figure 25. Importance - performance frequency IPA analysis chart (Security inspection/investigation)

2. 중요도-수행빈도 IPA 분석 종합

앞에서 분석한 내용을 기초로 표 43과 같이 정리하였다. 1사분면에 포함된 대외발송자료 보안성 검토 등 14개의 세부 직무는 인원 충원 등 보안직무의 '지속개발'이 필요한 구간으로 업체 경영진과 보안부서에서 인원 충원에 대한 관심이 요구되는 영역이다. 따라서, 인원 충원이 필요한 직무는 비밀관리(3개), 인원보안(1개), 시설/장비보안(2개), 정보통신보안(8개)으로 확인되었다.

3사분면에 포함된 보안수준평가 감독·통제 등 15개 세부 직무는 낮은 우선순위로 인원을 감원하거나 보직된 인원에게 추가 임무를 부여할 영역이다.

표 43. 각 사분면 중요도-수행빈도 세부직무
Table 43. Quadrant Importance - Performance Frequency Detailed Job

2사분면(14개) (현상유지)	1사분면(14개) (지속개발, 인력 충원)
1. 중장기 보안계획 수립	12. 대외발송자료 보안성 검토
2. 연간 보안업무계획 수립	13. 비밀 저장매체 관리
3. 보안내규 제·개정	15. 비밀 반입 및 반출 통제
7. 수출입 보안 조치	24. 퇴직자 보안조치
9. 비밀 생산(접수) 보안관리	28. 출입통제시스템 운용
17. 보안관계관 운용	31. 비인가자 접근/출입 통제
22. 핵심기술인력 보안조치	36. 전산기(서버) 보안관리 감독
26. 보호구역(시설) 설정	37. 네트워크(망분리 포함) 보안 관제 감독
27. 시설/장비 보호대책 구축	38. 정보보호시스템 보안관제 감독
44. 재난대비 백업시설 유지관리 통제	39. 정보통신 장비 및 저장매체 관리
51. 보안측정 의뢰/결과 조치	40. 개인용컴퓨터 보안관리
53. 정기/수시 보안점검	42. 보안관제결과(해킹) 조치 관리 감독
54. 보안사고시 초동조치 및 관계기관 신고	43. 방산 핵심기술 보호 관리
55. 통합실태조사 수검	45. 상용정보통신망 보안관리 통제
3사분면(15개) (낮은 우선순위, 인원 재판단)	**4사분면(12개) (과잉노력 지양, 선택적 인력 충원)**
5. 보안수준평가 감독·통제	4. 보안일일결산 감독·통제
6. 하도급 보안특약조건 검토 및 감독	8. 각종 보안행정서류 집행·관리
10. 비밀소유조사/재분류	16. 비밀 서류철 작성 관리 감독
11. 비밀 보관/관리실태 확인·감독	18. 직원(협력사 등) 신원조사업무
14. 비밀 보호조치(지정, 안전지출 등)	19. 보안서약서 집행 / 관리
23. 외국인(직원) 보안관리	20. 비밀취급인가업무 처리
34. 유사시 시설/장비 보안조치	21. 개인정보보호업무 처리
35. 사내 보안취약지 점검	25. 해외 출장자 보안교육
41. 협력업체 시스템 보안관리 감독	29. 출입증 관리
46. 보안교육계획 수립	30. 사진촬영(녹음) 통제
47. 주제/대상별 교안 작성	32. 외래인 출입시 보안조치
48. 대내·외 보안교육 실시	33. 장비 수송시 보안조치
49. 보안교육 성과분석	
50. 방산보안 대외협력 활동	
52. 부서/계열사 보안점검	

다음은 1사분면(지속개발)에 해당되는 인력 충원이 필요한 직무에 대해 세부적으로 알아보겠다. 세부 직무 비율은 표 44와 같다.

표 44. 인력 충원이 필요한 세부 직무 비율
Table 44. Percentage of detailed jobs requiring staffing

직무	세부 직무	중요도 (I)	수행빈도 (P)	I×P	세부비율 (I×P/∑)×100	비율 (%)
비밀 관리	12. 대외발송자료 보안성 검토	3.816	3.684	14.058	7.076	19.028
	13. 비밀 저장매체 관리	3.921	3.132	12.281	6.181	
	15. 비밀 반입 및 반출 통제	3.789	3.026	11.466	5.771	
인원	24. 퇴직자 보안조치	3.868	3.211	12.420	6.251	6.251
시설 장비	28. 출입통제시스템 운용	3.737	4.026	15.045	7.573	15.048
	31. 비인가자 접근/출입 통제	3.737	3.974	14.851	7.475	
정보 통신	36. 전산기(서버) 보안관리 감독	4.237	3.500	14.830	7.464	59.673
	37. 네트워크(망분리 포함) 보안 관제 감독	4.368	3.632	15.865	7.985	
	38. 정보보호시스템 보안관제 감독	4.289	3.842	16.478	8.294	
	39. 정보통신 장비 및 저장매체 관리	3.921	3.816	14.963	7.531	
	40. 개인용컴퓨터 보안관리	3.684	3.868	14.250	7.172	
	42. 보안관제결과(해킹) 조치 관리 감독	4.237	3.368	14.270	7.183	
	43. 방산 핵심기술 보호 관리	4.579	3.368	15.422	7.762	
	45. 상용정보통신망 보안관리 통제	3.763	3.316	12.478	6.281	
	∑(I×P)			198.675	100	100

비밀관리 직무는 19.0%, 인원보안은 6.3%, 시설/장비보안은 15.0%, 정보통신보안은 59.7%의 비율로 인력 충원이 필요하다는 것을 확인할 수 있었다. 특히, 정보통신보안 직무의 경우 IT분야의 첨단화가 필요한 세부 직무로서 인력 충원뿐 아니라 첨단시스템을 갖추기 위한 노력도 병행되어야 함을 판단할 수 있다. 그림 26은 인력 충원이 필요한 직무에 대해 세부적으로 도식화한 자료이다.

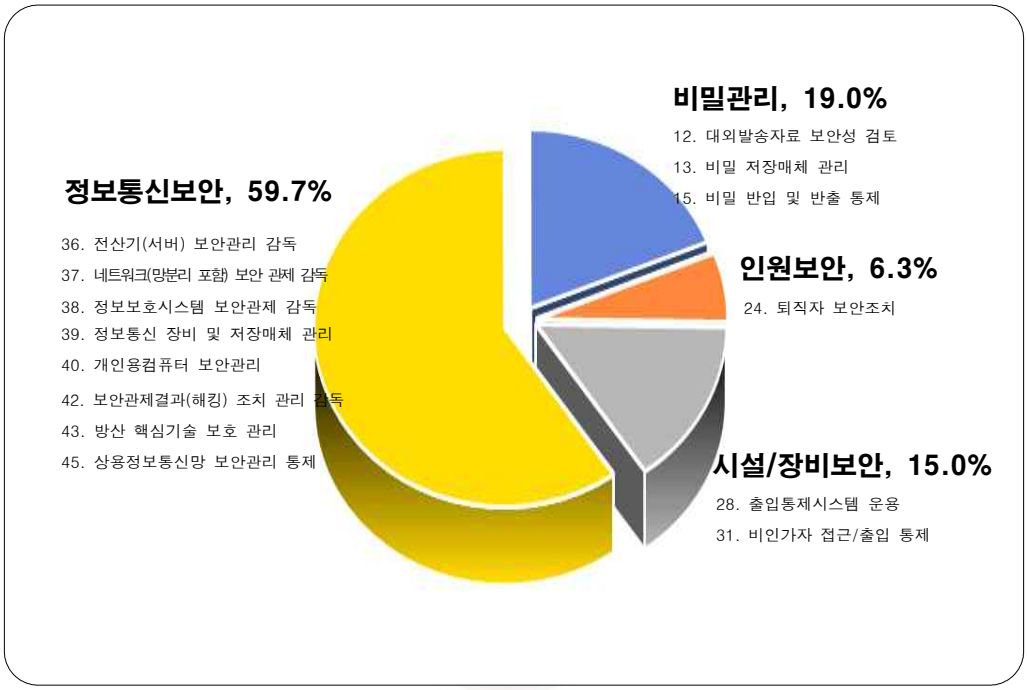


그림 26. 인력 충원이 필요한 직무(도표)
Figure 26. Jobs that require additional manpower(diagram)

3. 중요도-난이도 IPA 분석

그림 27에서와 같이 중요도-난이도에 대한 각 사분면별 방산업체 보안전문가의 세부 직무를 표현해 보았다. 표 13(연구자가 수정한 각 사분면 IPA 매트릭스 분석, p34)에서 제시한 것과 같이 1사분면은 역량개발 집중 구간으로 전문화 교육 및 시간 증편이 요구되며, 2사분면은 현상유지 구간, 3사분면은 낮은 우선순위 구간으로 전문교육은 불필요하며 내부 자체교육만으로도 충분히 업무수행이 가능한 직무이다. 4사분면은 선택적 전문교육(필요한 직무에 따라 선택적 전문교육 실시)이 필요한 구간으로 판단하였으며, 각 직무별 IPA 분석결과를 세부적으로 알아보겠다.

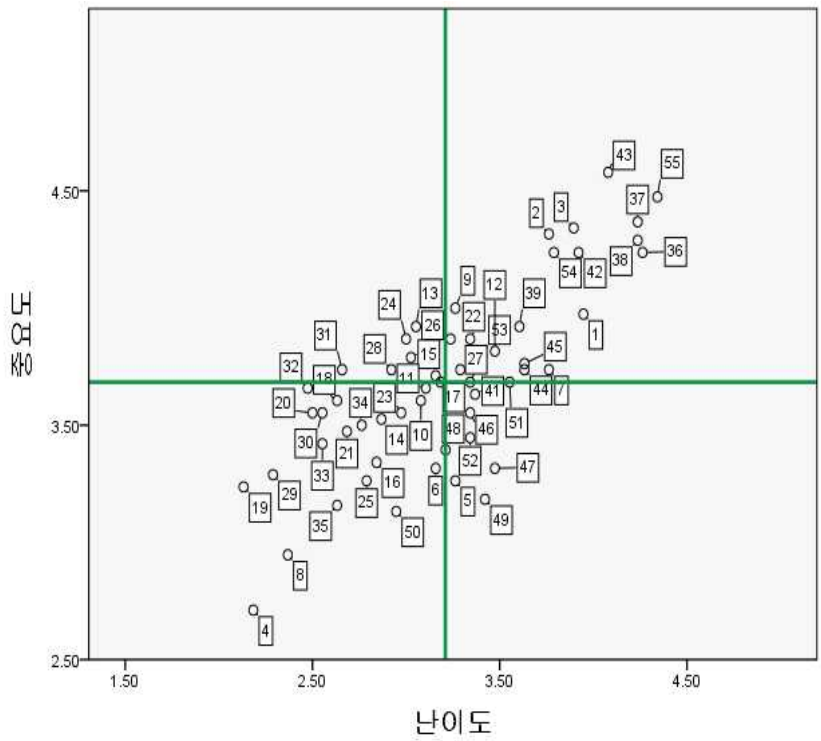


그림 27. 중요도-난이도 IPA 분석 종합
Figure 27. Importance - difficulty IPA Analysis Synthesis

첫째, 표 45를 기초로 '보안행정' 직무에 대한 중요도-난이도 IPA 분석결과는 다음과 같다.

표 45. 중요도-난이도 직무 값(보안행정)
Table 45. Importance-difficulty job value(security administration)

직무	세부 직무	중요도	난이도
보안 행정	1. 중장기 보안계획 수립	3.974	3.947
	2. 연간 보안업무계획 수립	4.316	3.763

	3. 보안내규 제·개정	4.342	3.895
	4. 보안일일결산 감독·통제	2.711	2.184
	5. 보안수준평가 감독·통제	3.263	3.263
	6. 하도급 보안특약조건 검토 및 감독	3.316	3.158
	7. 수출입 보안 조치	3.737	3.763
	8. 각종 보안행정서류 집행·관리	2.947	2.368

그림 28에서 보는 바와 같이 1사분면은 역량개발을 집중하는 구간으로 1. 중장기 보안계획 수립, 2. 연간 보안업무계획 수립, 3. 보안내규 제·개정, 7. 수출입 보안 조치이며, 2사분면은 현상유지 구간으로 해당하는 세부직무는 없다. 3사분면은 낮은 우선순위로 전문교육은 불필요한 구간으로 4. 보안일일결산 감독·통제, 6. 하도급 보안특약조건 검토 및 감독, 8. 각종 보안행정서류 집행·관리이며, 과잉노력을 지양하는 4사분면에는 5. 보안수준평가 감독·통제가 이 구간에 해당된다.

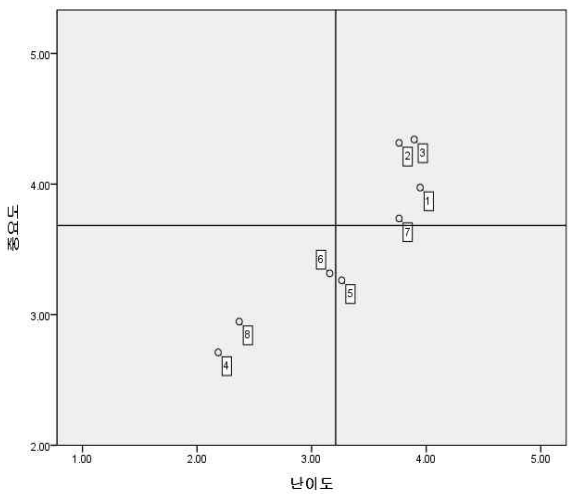


그림 28. 중요도-난이도 IPA 분석 도표(보안행정)
Figure 28. Importance-difficulty IPA analysis chart(Security administration)

둘째, 표 46을 기초로 '비밀관리' 직무에 대한 중요도-난이도 IPA 분석결과는 다음과 같다.

표 46. 중요도-난이도 직무 값(비밀관리)
Table 46. Importance-difficulty job value(Secret management)

직무	세부 직무	중요도	난이도
비밀 관리	9. 비밀 생산(접수) 보안관리	4.000	3.263
	10. 비밀소유조사 / 재분류	3.605	3.079
	11. 비밀 보관/관리실태 확인・감독	3.658	3.105
	12. 대외발송자료 보안성 검토	3.816	3.474
	13. 비밀 저장매체 관리	3.921	3.053
	14. 비밀 보호조치(지정, 안전지출 등)	3.526	2.868
	15. 비밀 반입 및 반출 통제	3.789	3.026
	16. 비밀 서류철 작성 관리 감독	3.342	2.842

그림 29에서 보는 바와 같이 1사분면(지속개발)은 9. 비밀 생산(접수) 보안관리, 12. 대외발송자료 보안성검토이며, 2사분면(현상유지)은 13. 비밀 저장매체 관리, 15. 비밀 반출 및 반입 통제이며, 3사분면(낮은 우선순위)은 10. 비밀 소유조사/재분류, 11. 비밀 보관/관리 실태 확인・감독, 14. 비밀 보호조치(지정, 안전지출 등), 16. 비밀 서류철 작성 관리 감독이며, 4사분면(선택적 역량개발)은 없다.

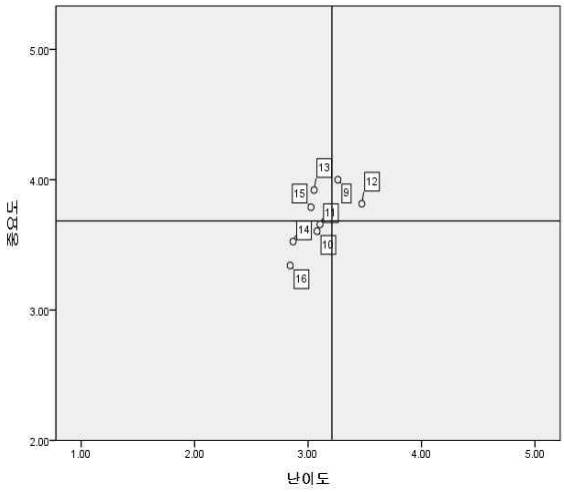


그림 29. 중요도-난이도 IPA 분석 도표(비밀관리)
Figure 29. Importance-difficulty IPA analysis chart(Secret management)

셋째, 표 47을 기초로 '인원보안' 직무에 대한 중요도-난이도 IPA 분석결과는 다음과 같다.

표 47. 중요도-난이도 직무 값(인원보안)
Table 47. Importance-difficulty job value(Personnel security)

직무	세부 직무	중요도	난이도
인원 보안	17. 보안관계관 운용	3.711	3.158
	18. 직원(협력사 등) 신원조사업무	3.605	2.632
	19. 보안서약서 집행/관리	3.237	2.132
	20. 비밀취급인가업무 처리	3.553	2.500
	21. 개인정보보호업무 처리	3.474	2.684
	22. 핵심기술인력 보안조치	3.868	3.342
	23. 외국인(직원) 보안관리	3.553	2.974
	24. 퇴직자 보안조치	3.868	3.000
	25. 해외 출장자 보안교육	3.263	2.789

그림 30에서 보는 바와 같이 1사분면(역량개발 집중)은 17. 보안관계관 운용, 22. 핵심기술인력 보안조치이며, 2사분면(현상유지)은 24. 퇴직자 보안조치이며, 3사분면(낮은 우선순위)은 18. 직원(협력사 등) 신원조사업무, 19. 보안서약서 집행/관리, 20. 비밀취급인가업무 처리, 21. 개인정보보호업무 처리, 25. 해외 출장자 보안교육이며, 4사분면(선택적 역량개발)은 없다.

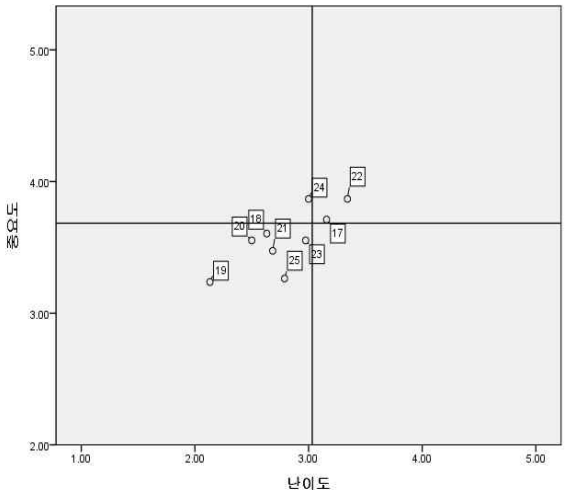


그림 30. 중요도-난이도 IPA 분석 도표(인원보안)
Figure 30. Importance-difficulty IPA analysis chart(Personnel security)

넷째, 표 48을 기초로 '시설/장비보안' 직무에 대한 중요도-난이도 IPA 분석 결과는 다음과 같다.

표 48. 중요도-난이도 직무 값(시설/장비보안)
Table 48. Importance-difficulty job value(Facility & Equipment Security)

직무	세부 직무	중요도	난이도
시설/장비보안	26. 보호구역(시설) 설정	3.868	3.237
	27. 시설/장비 보호대책 구축	3.737	3.289
	28. 출입통제시스템 운용	3.737	2.921

	29. 출입증 관리	3.289	2.289
	30. 사진촬영(녹음) 통제	3.553	2.553
	31. 비인가자 접근 / 출입 통제	3.737	2.658
	32. 외래인 출입시 보안조치	3.658	2.474
	33. 장비 수송시 보안조치	3.421	2.553
	34. 유사시 시설/장비 보안조치	3.500	2.763
	35. 사내 보안취약지 점검	3.158	2.632

그림 31에서 보는 바와 같이 1사분면(역량개발 집중)은 26. 보호구역(시설) 설정, 27. 시설/장비 보호대책 구축이며, 2사분면(현상유지)은 28. 출입통제시스템 운용, 31. 비인가자 접근/출입 통제 이며, 3사분면(낮은 우선순위)은 29. 출입증 관리, 30. 사진촬영(녹음) 통제, 32. 외래인 출입시 보안조치, 33. 장비 수송시 보안조치, 34. 유사시 시설/장비 보호조치, 35. 사내 보안취약지 점검이며, 4사분면(선택적 역량개발)은 없다.

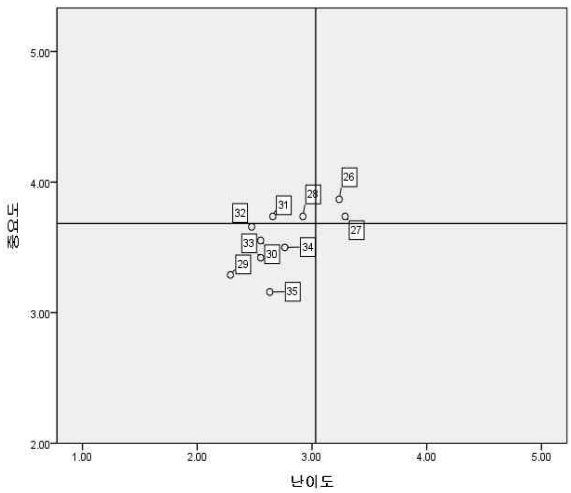


그림 31. 중요도-난이도 IPA 분석 도표(시설/장비보안)
Figure 31. Importance-difficulty IPA analysis chart(Facility & Equipment Security)

다섯째, 표 49를 기초로 '정보통신보안' 직무에 대한 중요도-난이도 IPA 분석 결과는 다음과 같다.

표 49. 중요도-난이도 직무 값(정보통신보안)
Table 49. Importance-difficulty job value(Information & communication security)

직무	세부 직무	중요도	수행빈도
정보통신보안	36. 전산기(서버) 보안관리 감독	4.237	4.263
	37. 네트워크(망분리 포함) 보안 관제 감독	4.368	4.237
	38. 정보보호시스템 보안관제 감독	4.289	4.237
	39. 정보통신 장비 및 저장매체 관리	3.921	3.605
	40. 개인용컴퓨터 보안관리	3.684	3.184
	41. 협력업체 시스템 보안관리 감독	3.632	3.368
	42. 보안관제결과(해킹) 조치 관리 감독	4.237	3.921
	43. 방산 핵심기술 보호 관리	4.579	4.079
	44. 재난대비 백업시설 유지관리 통제	3.737	3.632
	45. 상용정보통신망 보안관리 통제	3.763	3.632

그림 32에서 보는 바와 같이 2사분면(현상유지)의 40. 개인용컴퓨터 보안관리와 3사분면(낮은 우선순위)의 41. 협력업체 시스템 보안관리 감독 외 전체의 항목이 1사분면(역량개발 집중)에 해당된다.

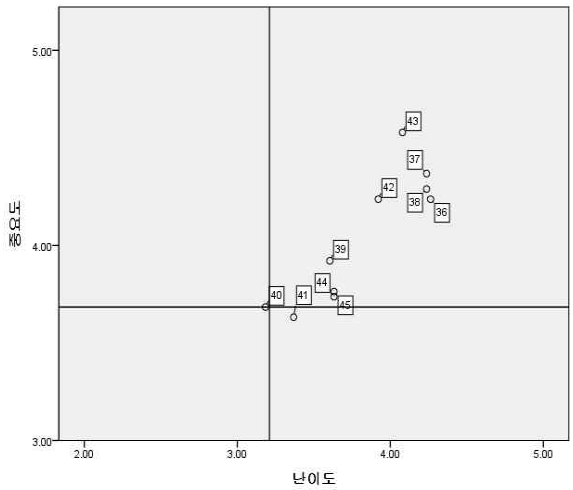


그림 32. 중요도-난이도 IPA 분석 도표(정보통신보안)
Figure 32. Importance-difficulty IPA analysis chart(Information & communication security)

여섯째, 표 50을 기초로 '보안교육/기타' 직무에 대한 중요도-난이도 IPA 분석 결과는 다음과 같다.

표 50. 중요도-난이도 직무 값(보안교육/기타)
Table 50. Importance-difficulty job value(Security training/other)

직무	세부 직무	중요도	난이도
보안교육/기타	46. 보안교육계획 수립	3.553	3.342
	47. 주제/대상별 교안 작성	3.316	3.474
	48. 대내·외 보안교육 실시	3.395	3.211
	49. 보안교육 성과분석	3.184	3.421
	50. 방산보안 대외협력 활동	3.132	2.947

그림 33에서 보는 바와 같이 1사분면(역량개발 집중)과 2사분면(현상유지)의 영역에는 없으며, 3사분면(낮은 우선순위)의 50. 방산보안 대외협력 활동 외 전체가 4사분면(선택적 역량개발)의 영역에 해당된다.

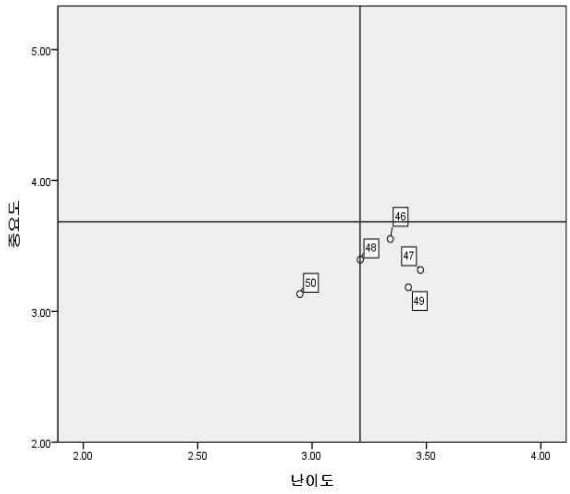


그림 33. 중요도-난이도 IPA 분석 도표(보안교육/기타)
Figure 33. Importance-difficulty IPA analysis chart(Security training/other)

일곱째, 표 51을 기초로 '보안점검/조사' 직무에 대한 중요도-난이도 IPA 분석 결과는 다음과 같다.

표 51. 중요도-난이도 직무 값(보안점검/조사)
Table 51. Importance-difficulty job value(Security inspection/investigation)

직무	세부 직무	중요도	난이도
보안 점검 / 조사	51. 보안측정 의뢰/결과 조치	3.684	3.553
	52. 부서/계열사 보안점검	3.447	3.342
	53. 정기/수시 보안점검	3.684	3.342
	54. 보안사고시 초동조치 및 관계기관 신고	4.237	3.789
	55. 통합실태조사 수검	4.474	4.342

그림 34에서 보는 바와 같이 1사분면(역량개발 집중)은 54. 보안사고시 초동조치 및 관계기관 신고, 55. 통합실태조사 수검이며, 2사분면(현상유지)과 4사분면

(과잉노력 지양)은 없으며, 3사분면(낮은 우선순위)에는 51. 보안측정 의뢰/결과 조치, 52. 부서/계열사 보안점검, 53. 정기/수시 보안점검이 해당된다.

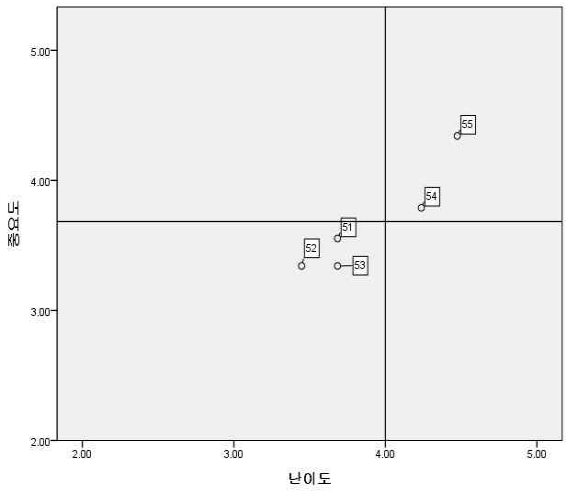


그림 34. 중요도-난이도 IPA 분석 도표(보안점검/조사)
Figure 34. Importance-difficulty IPA analysis chart(Security inspection/investigation)

4. 중요도-난이도 IPA 분석 종합

앞에서 분석한 내용을 기초로 표 52와 같이 정리하였다. 1사분면에 포함된 중장기 보안계획 수립 등 20개의 세부 직무는 역량개발을 집중하는 영역으로 전문교육 및 시간 증편이 필요한 보안직무에 해당된다. 세부적으로 살펴보면 보안행정(3개), 비밀관리(2개), 인원보안(2개), 시설/장비보안(2개), 정보통신보안(8개), 보안점검/조사(2개)로 확인되었다. 이 중 특이할 만한 사항으로 보안행정(3개), 비밀관리(2개), 인원보안(2개), 시설/장비보안(2개)에 대해서 평상시 수행하는 업무임에도 어렵게 느끼고 있으며, 정보통신보안 분야에 대해서는 예상과 같이 전반적으로 난이도가 높게 나타났고, 통합실태조사 수검에 대한 부담감과 어려움을 느끼고 있음을 알 수 있었다.

3사분면에 포함된 보안일일결산 감독·통제 등 24개 세부 직무는 낮은 우선순위로써 전문교육은 불필요하며 부서 내 자체교육으로도 임무수행이 가능한 영역이다.

표 52. 각 사분면 중요도-난이도 세부직무
Table 52. Quadrant Importance - difficulty Detailed Job

2사분면(6개) (현상유지)	1사분면(20개) (역량개발 집중, 전문교육/시간증편)
13. 비밀 저장매체 관리 15. 비밀 반입 및 반출 통제 24. 퇴직자 보안조치 28. 출입통제시스템 운용 31. 비인가자 접근/출입 통제 40. 개인용컴퓨터 보안관리	1. 중장기 보안계획 수립 2. 연간 보안업무계획 수립 3. 보안내규 제·개정 7. 수출입 보안 조치 9. 비밀 생산(접수) 보안관리 12. 대외발송자료 보안성 검토 17. 보안관계관 운용 22. 핵심기술인력 보안조치 26. 보호구역(시설) 설정 27. 시설/장비 보호대책 구축 36. 전산기(서버) 보안관리 감독 37. 네트워크(망분리 포함) 보안 관제 감독 38. 정보보호시스템 보안관제 감독 39. 정보통신 장비 및 저장매체 관리 42. 보안관제결과(해킹) 조치 관리 감독 43. 방산 핵심기술 보호 관리 44. 재난대비 백업시설 유지관리 통제 45. 상용정보통신망 보안관리 통제 54. 보안사고시 초동조치 및 관계기관 신고 55. 통합실태조사 수검
3사분면(24개) (낮은 우선순위, 자체교육)	4사분면(5개) (과잉노력 지양, 선택적 전문교육)
4. 보안일일결산 감독·통제 6. 하도급 보안특약조건 검토 및 감독 8. 각종 보안행정서류 집행·관리 10. 비밀소유조사/재분류 11. 비밀 보관/관리실태 확인·감독 14. 비밀 보호조치(지정, 안전지출 등) 16. 비밀 서류철 작성 관리 감독 18. 직원(협력사 등) 신원조사업무	5. 보안수준평가 감독·통제 46. 보안교육 계획 수립 47. 주제/대상별 교안 작성 48. 대내·외 보안교육 실시 49. 보안교육 성과분석

19. 보안서약서 집행 / 관리	
20. 비밀취급인가업무 처리	
21. 개인정보보호업무 처리	
23. 외국인(직원) 보안관리	
25. 해외 출장자 보안교육	
29. 출입증 관리	
30. 사진촬영(녹음) 통제	
32. 외래인 출입시 보안조치	
33. 장비 수송시 보안조치	
34. 유사시 시설/장비 보안조치	
35. 사내 보안취약지 점검	
41. 협력업체 시스템 보안관리 감독	
50. 방산보안 대외협력 활동	
51. 보안측정 의뢰/결과 조치	
52. 부서/계열사 보안점검	
53. 정기/수시 보안점검	

다음은 1사분면(역량개발 집중)에 해당되는 전문교육 및 시간 증편이 필요한 직무에 대해 세부적으로 알아보겠다. 세부 직무 비율은 표 53과 같다.

표 53. 전문교육이 필요한 세부 직무 비율
Table 53. Percentage of detailed jobs requiring specialized training

직무	세부 직무	중요도 (I)	난이도 (D)	I×D	세부비율 (I×D/∑)×100	비율 (%)
보안 행정	1. 중장기 보안계획 수립	3.974	3.947	15.685	5.156	20.675
	2. 연간 보안업무계획 수립	4.316	3.763	16.241	5.338	
	3. 보안내규 제·개정	4.342	3.895	16.912	5.559	
	7. 수출입 보안 조치	3.737	3.763	14.062	4.622	
비밀 관리	9. 비밀 생산(접수) 보안관리	4.000	3.263	13.052	4.290	8.647
	12. 대외발송자료 보안성 검토	3.816	3.474	13.257	4.357	
인원 보안	17. 보안관계관 운용	3.711	3.158	11.719	3.852	7.668
	22. 핵심기술인력 보안조치	3.474	3.342	11.610	3.816	
시설 장비	26. 보호구역(시설) 설정	3.868	3.237	12.521	4.115	8.155
	27. 시설/장비 보호대책 구축	3.737	3.289	12.291	4.040	

정보통신	36. 전산기(서버) 보안관리 감독	4.237	4.263	18.062	5.937	43.192
	37. 네트워크(망분리 포함) 보안 관제 감독	4.368	4.237	18.507	6.083	
	38. 정보보호시스템 보안관제 감독	4.289	4.237	18.172	5.973	
	39. 정보통신 장비 및 저장매체 관리	3.921	3.605	14.135	4.646	
	42. 보안관제결과(해킹) 조치 관리 감독	4.237	3.921	16.613	5.461	
	43. 방산 핵심기술 보호 관리	4.579	4.079	18.678	6.139	
	44. 재난대비 백업시설 유지관리 통제	3.737	3.632	13.573	4.461	
	45. 상용정보통신망 보안관리 통제	3.763	3.632	13.667	4.492	
보안점검	54. 보안사고시 초동조치 및 관계기관 신고	4.237	3.789	16.054	5.277	11.662
	55. 통합실태조사 수검	4.474	4.342	19.426	6.385	
	∑(I×D)			304.239	100	100

보안행정 직무는 20.7%, 인원보안은 7.7%, 비밀관리는 8.6%, 시설/장비보안은 8.1%, 정보통신보안은 43.2%, 보안점검/조사는 11.7%의 비율로 전문교육이 필요하다는 것을 확인할 수 있었으며 보안행정, 인원보안, 비밀관리, 시설/장비보안 직무는 평상시 수행하는 직무임에도 어렵다고 인식하고 있었다. 정보통신보안은 예상했던 것과 같이 난이도가 높은 직무를 나타났고, 보안사고조치, 통합실태조사 수검도 전문교육이 필요함을 확인하였다. 그림 35는 전문교육이 필요한 직무에 대해 세부적으로 도식화한 자료이다.

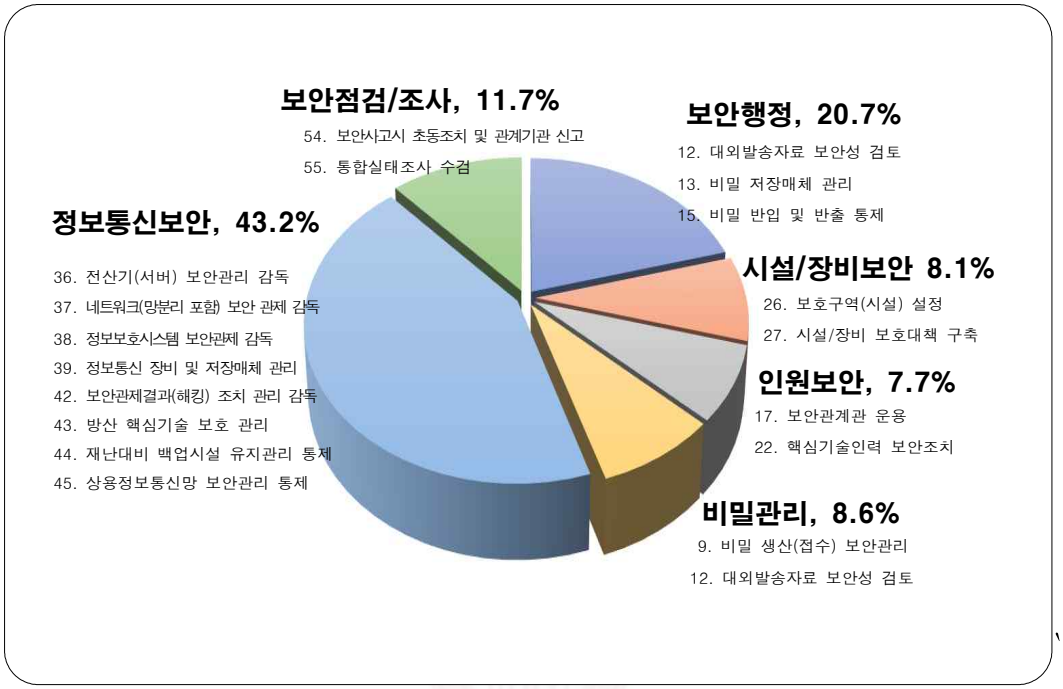


그림 35. 전문교육이 필요한 직무(도표)
Figure 35. Job requiring professional training(diagram)

5. 중요도/난이도 평균-수행빈도 IPA 분석

그림 36에서와 같이 중요도/난이도 평균(이하 I/D 평균)-수행빈도에 대한 각 사분면별 방산업체 보안전문가의 세부 직무를 표현해 보았다. 표 13(연구자가 수정한 각 사분면 IPA 매트릭스 분석, p34)에서 제시한 것과 같이 1사분면은 지속개발 구간으로 감사 및 평가시 가중치를 상향하는 영역이며, 2사분면과 4사분면은 감사 및 평가시 가중치에 변화가 없는 현상유지 영역이며, 3사분면은 낮은 우선순위 구간으로 감사 및 평가시 가중치를 하향하는 영역으로 판단하였으며, 각 직무별 IPA 분석결과를 세부적으로 알아보겠다.

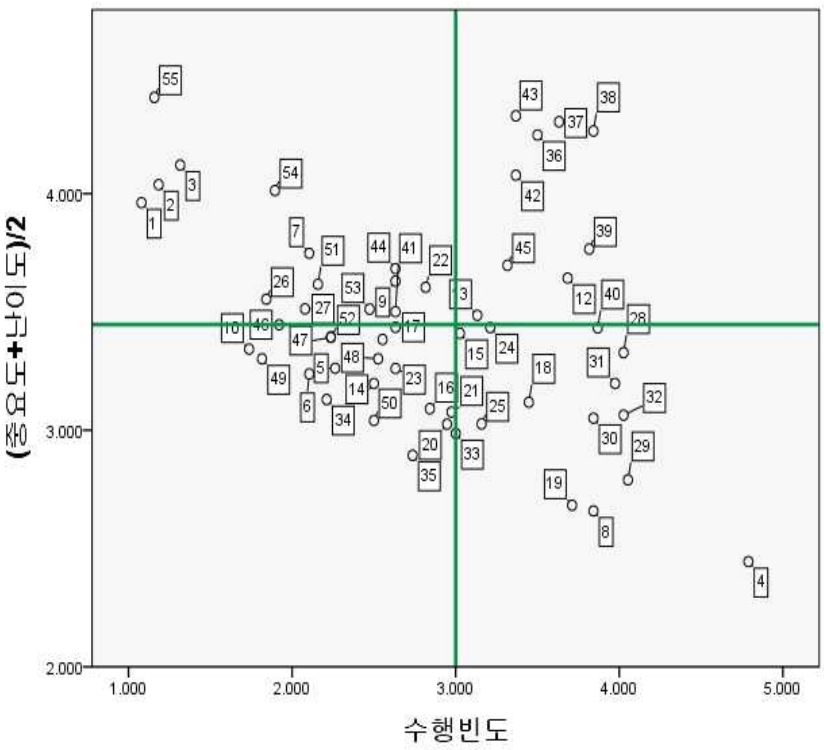


그림 36. I/D 평균-수행빈도 IPA 분석 종합
Figure 36. I/D Mean - performance frequency IPA Analysis Synthesis

첫째, 표 54를 기초로 '보안행정' 직무에 대한 I/D 평균-수행빈도 IPA 분석결과는 다음과 같다.

표 54. I/D 평균-수행빈도 직무 값(보안행정)
Table 54. I/D Mean - Performance Frequency Job Value(Security Administration)

직무	세부 직무	I/D평균	수행빈도
보안 행정	1. 중장기 보안계획 수립	3.962	1.079
	2. 연간 보안업무계획 수립	4.038	1.184
	3. 보안내규 제·개정	4.121	1.316

	4. 보안일일결산 감독・통제	2.445	4.789
	5. 보안수준평가 감독・통제	3.262	2.263
	6. 하도급 보안특약조건 검토 및 감독	3.238	2.105
	7. 수출입 보안 조치	3.748	2.105
	8. 각종 보안행정서류 집행・관리	2.659	3.842

그림 37에서 보는 바와 같이 1사분면(지속개발)에 해당하는 세부직무가 없으며, 2사분면(현상유지)에는 1. 중장기 보안계획 수립, 2. 연간 보안업무계획 수립, 3.보안내규 제・개정, 7. 수출입 보안조치가 포함되며, 3사분면(낮은 우선순위)에는 5. 보안수준평가 감독・통제, 6. 하도급 보안특약조건 검토 및 감독이며, 4사분면(현상유지)에는 4. 보안일일결산 감독・통제, 8. 각종 행정서류 집행・관리가 해당된다.

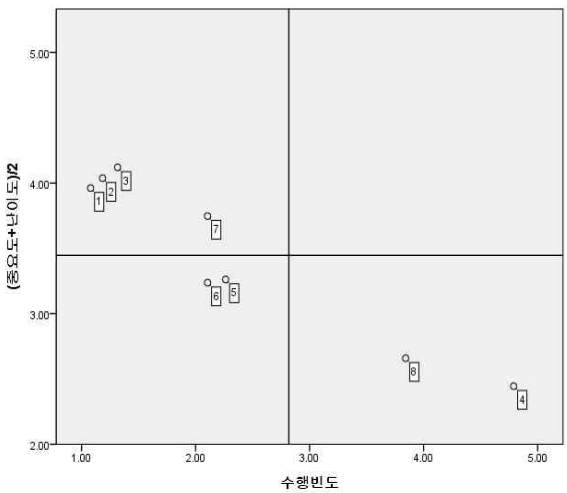


그림 37. I/D 평균-수행빈도 IPA 분석 도표(보안행정)
Figure 37. I/D Mean - Performance Frequency IPA analysis chart (security administration)

둘째, 표 55를 기초로 '비밀관리' 직무에 대한 I/D 평균-수행빈도 IPA 분석결과는 다음과 같다.

표 55. I/D 평균-수행빈도 직무 값(비밀관리)
Table 55. I/D Mean - Performance Frequency Job Value(Secret management)

직무	세부 직무	I/D평균	수행빈도
비밀 관리	9. 비밀 생산(접수) 보안관리	3.630	2.632
	10. 비밀소유조사/재분류	3.343	1.737
	11. 비밀 보관/관리실태 확인・감독	3.384	2.553
	12. 대외발송자료 보안성 검토	3.643	3.684
	13. 비밀 저장매체 관리	3.486	3.132
	14. 비밀 보호조치(지정, 안전지출 등)	3.198	2.500
	15. 비밀 반입 및 반출 통제	3.410	3.026
	16. 비밀 서류철 작성 관리 감독	3.091	2.842

그림 38에서 보는 바와 같이 1사분면(지속 개발)은 12. 대외발송자료 보안성 검토, 13. 비밀 저장매체 관리이며, 2사분면(현상유지)은 9. 비밀 생산(접수) 보안 관리이며, 3사분면(낮은 우선순위)은 10. 비밀 소유조사/재분류, 11. 비밀 보관/관리 실태 확인・감독, 14. 비밀 보호조치(지정, 안전지출 등)이며, 4사분면(현상유지)은 15. 비밀 반입 및 반출 통제, 16. 비밀 서류철 작성 관리 감독이다.

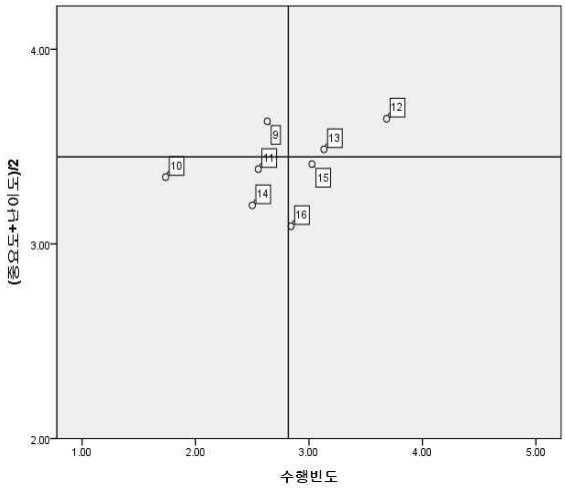


그림 38. I/D 평균-수행빈도 IPA 분석 도표(비밀관리)
Figure 38. I/D Mean - performance frequency IPA analysis chart (Secret management)

셋째, 표 56을 기초로 '인원보안' 직무에 대한 I/D 평균-수행빈도 IPA 분석결과는 다음과 같다.

표 56. I/D 평균-수행빈도 직무 값(인원보안)
Table 56. I/D Mean - Performance Frequency Job Value(Personnel security)

직무	세부 직무	I/D평균	수행빈도
인원 보안	17. 보안관계관 운용	3.435	2.632
	18. 직원(협력사 등) 신원조사업무	3.118	3.447
	19. 보안서약서 집행 / 관리	2.683	3.711
	20. 비밀취급인가업무 처리	3.026	2.947
	21. 개인정보보호업무 처리	3.077	2.974
	22. 핵심기술인력 보안조치	3.604	2.816
	23. 외국인(직원) 보안관리	3.261	2.632
	24. 퇴직자 보안조치	3.434	3.211
	25. 해외 출장자 보안교육	3.027	3.158

그림 39에서 보는 바와 같이 1사분면(지속개발)은 없으며, 24. 퇴직자 보안조치이며, 2사분면(현상유지)은 22. 핵심기술인력 보안조치이며, 3사분면(낮은 우선순위)은 17. 보안관계관 운용, 23. 외국인(직원) 보안관리이며, 4사분면(현상유지)은 18. 직원(협력사) 신원조사 업무, 19. 보안서약서 집행관리, 20. 비밀취급인가 업무 처리, 21. 개인정보보호업무 처리, 25. 해외 출장자 보안교육이다.

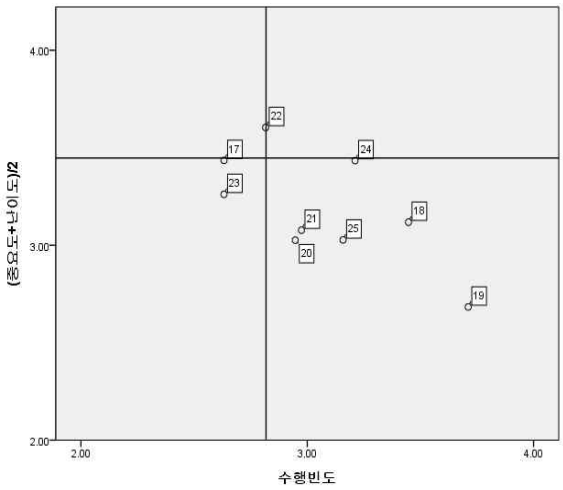


그림 39. I/D 평균-수행빈도 IPA 분석 도표(인원보안)
Figure 39. I/D Mean - performance frequency IPA analysis chart (Personnel security)

네째, 표 57을 기초로 '시설/장비보안' 직무에 대한 I/D 평균-수행빈도 IPA 분석결과는 다음과 같다.

표 57. I/D 평균-수행빈도 직무 값(시설/장비보안)
Table 57. I/D Mean - Performance Frequency Job Value(Facility & Equipment Security)

직무	세부 직무	I/D평균	수행빈도
	26. 보호구역(시설) 설정	3.554	1.842
	27. 시설/장비 보호대책 구축	3.513	2.079

시설 / 장비 보안	28. 출입통제시스템 운용	3.328	4.026
	29. 출입증 관리	2.790	4.053
	30. 사진촬영(녹음) 통제	3.051	3.842
	31. 비인가자 접근/출입 통제	3.198	3.974
	32. 외래인 출입시 보안조치	3.064	4.026
	33. 장비 수송시 보안조치	2.986	3.000
	34. 유사시 시설/장비 보안조치	3.130	2.211
	35. 사내 보안취약지 점검	2.894	2.737

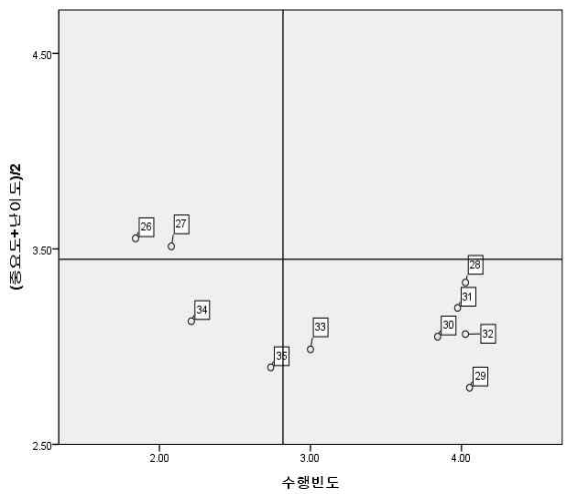


그림 40. I/D 평균-수행빈도 IPA 분석 도표(시설/장비보안)
Figure 40. I/D Mean - performance frequency IPA analysis chart (Facility & Equipment Security)

그림 40에서 보는 바와 같이 1사분면(지속개발)은 해당사항이 없으며, 2사분면(현상유지)은 26. 보호구역(시설) 설정, 27. 시설/장비 보호대책 구축이며, 3사분면(낮은 우선순위)은 34. 유사시 시설/장비 보호조치, 35. 사내 보안취약지 점검이며,

4사분면(현상유지)은 28. 출입통제시스템 운용, 29. 출입증 관리, 30. 사진촬영(녹음) 통제, 31. 비인가자 접근/출입 통제, 32. 외래인 출입시 보안조치, 33. 장비 수송시 보안조치이다.

다섯째, 표 58을 기초로 '정보통신보안' 직무에 대한 I/D 평균-수행빈도 IPA 분석결과는 다음과 같다

표 58. I/D 평균-수행빈도 직무 값(정보통신보안)
Table 58 I/D Mean - Performance Frequency Job Value(Information& communication security)

직무	세부 직무	I/D평균	수행빈도
정보통신보안	36. 전산기(서버) 보안관리 감독	4.248	3.500
	37. 네트워크(망분리 포함) 보안 관제 감독	4.304	3.632
	38. 정보보호시스템 보안관제 감독	4.265	3.842
	39. 정보통신 장비 및 저장매체 관리	3.766	3.816
	40. 개인용컴퓨터 보안관리	3.432	3.868
	41. 협력업체 시스템 보안관리 감독	3.501	2.632
	42. 보안관제결과(해킹) 조치 관리 감독	4.078	3.368
	43. 방산 핵심기술 보호 관리	4.329	3.368
	44. 재난대비 백업시설 유지관리 통제	3.683	2.632
	45. 상용정보통신망 보안관리 통제	3.697	3.316

그림 41에서 보는 바와 같이 1사분면(지속개발)은 36. 전산기(서버) 보안관리 감독, 37. 네트워크(망분리 포함) 보안 관제 감독, 38. 정보보호시스템 보안관제 감독, 39. 정보통신 장비 및 저장매체 관리, 42. 보안관제결과(해킹) 조치 관리 감독, 43. 방산 핵심기술 보호 관리, 45. 상용정보통신망 보안관리 통제이며,

2사분면(현상유지)은 41. 협력업체 시스템 보안관리 감독, 44. 재난대비 백업시설 유지관리 통제이며, 3사분면(낮은 우선순위)은 41. 협력업체 시스템 보안관리 감독이며, 4사분면은 40. 개인용컴퓨터 보안관리이다.

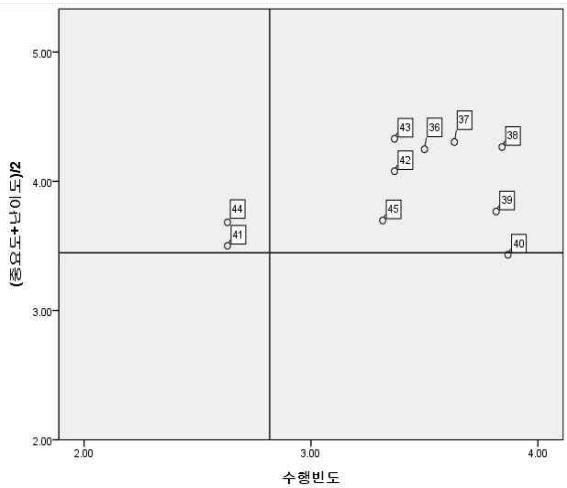


그림 41. I/D 평균-수행빈도 IPA 분석 도표(정보통신보안)
Figure 41. I/D Mean - performance frequency IPA analysis chart (Information& communication security)

여섯째, 표 59를 기초로 '보안교육/기타' 직무에 대한 I/D 평균-수행빈도 IPA 분석결과는 다음과 같다.

표 59. I/D 평균-수행빈도 직무 값(보안교육/기타)
Table 59. I/D Mean - Performance Frequency Job Value(Security training/other)

직무	세부 직무	I/D평균	수행빈도
보안교육/기타	46. 보안교육계획 수립	3.446	1.921
	47. 주제/대상별 교안 작성	3.393	2.237
	48. 대내·외 보안교육 실시	3.302	2.526
	49. 보안교육 성과분석	3.302	1.816
	50. 방산보안 대외협력 활동	3.041	2.500

그림 42에서 보는 바와 같이 보안교육/기타 직무는 전체가 3사분면(낮은 우선순위)에 해당되는 것으로 확인되었다.

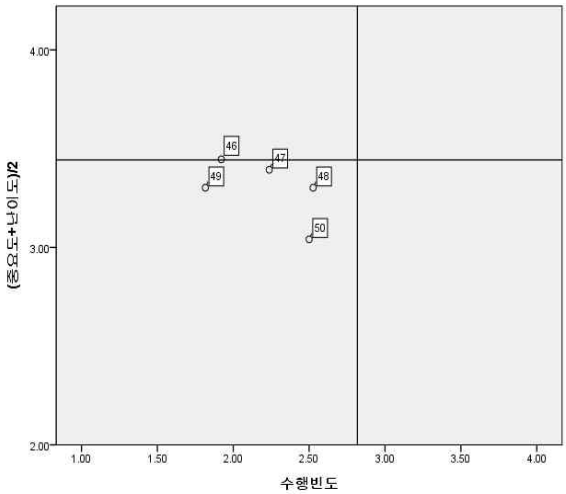


그림 42. I/D 평균-수행빈도 IPA 분석 도표(보안교육/기타)
Figure 42. I/D Mean - performance frequency IPA analysis chart (Security training/other)

일곱째, 표 60을 기초로 '보안점검/조사' 직무에 대한 I/D 평균-수행빈도 IPA 분석결과는 다음과 같다.

표 60. I/D 평균-수행빈도 직무 값(보안점검/조사)
Table 60. I/D Mean - Performance Frequency Job Value(Security inspection/investigation)

직무	세부 직무	I/D평균	수행빈도
보안 점검 / 조사	51. 보안측정 의뢰/결과 조치	3.617	2.158
	52. 부서/계열사 보안점검	3.394	2.237
	53. 정기/수시 보안점검	3.512	2.474
	54. 보안사고시 초동조치 및 관계기관 신고	4.013	1.895
	55. 통합실태조사 수검	4.407	1.158

그림 43에서 보는 바와 같이 보안점검/조사 직무는 1사분면과 4사분면은 없으며, 2사분면은 51. 보안측정 의뢰/결과 조치, 53. 정기/수시 보안점검, 54. 보안사고 시 초동조치 및 관계기관 신고, 55. 통합실태조사 수검이며, 3사분면(낮은 우선순위)은 52. 부서/계열사 보안점검으로 확인되었다.

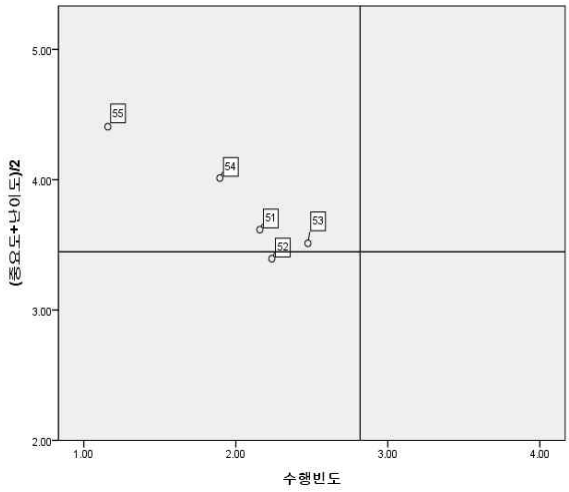


그림 43. I/D 평균-수행빈도 IPA 분석 도표(보안점검/조사)
Figure 43. I/D Mean - performance frequency IPA analysis chart (Security inspection/investigation)

6. 중요도/난이도 평균-수행빈도 IPA 분석 종합

앞에서 분석한 내용을 기초로 표 61과 같이 정리하였다. 1사분면에 포함된 대외발송자료 보안성 검토 등 9개의 세부 직무는 많은 역량과 노력, 상당한 시간을 요구하는 직무로써 감시 및 평가시 가중치의 상향이 필요한 영역이다.

3사분면에 포함된 보안수준평가 감독·통제 등 15개 세부 직무는 단순하면서도 수행빈도가 낮은 직무로써 감시 및 평가시 가중치를 하향할 필요가 있다.

표 61. 각 사분면 I/D 평균-수행빈도 세부직무
Table 61. Quadrant I/D Mean - Performance Frequency Detailed Job

2사분면(14개) (현상유지, 가중치 유지)	1사분면(9개) (지속개발, 가중치 상향)
1. 중장기 보안계획 수립 2. 연간 보안업무계획 수립 3. 보안내규 제·개정 7. 수출입 보안 조치 9. 비밀 생산(접수) 보안관리 22. 핵심기술인력 보안조치 26. 보호구역(시설) 설정 27. 시설/장비 보호대책 구축 41. 협력업체 시스템 보안관리 감독 44. 재난대비 백업시설 유지관리 통제 51. 보안측정 의뢰/결과 조치 53. 정기/수시 보안점검 54. 보안사고시 초동조치 및 관계기관 신고 55. 통합실태조사 수검	12. 대외발송자료 보안성 검토 13. 비밀 저장매체 관리 36. 전산기(서버) 보안관리 감독 37. 네트워크(망분리 포함) 보안 관제 감독 38. 정보보호시스템 보안관제 감독 39. 정보통신 장비 및 저장매체 관리 42. 보안관제결과(해킹) 조치 관리 감독 43. 방산 핵심기술 보호 관리 45. 상용정보통신망 보안관리 통제
3사분면(15개) (낮은 우선순위, 가중치 하향)	**4사분면(17개) (현상유지, 가중치 유지)**
5. 보안수준평가 감독·통제 6. 하도급 보안특약조건 검토 및 감독 10. 비밀소유조사/재분류 11. 비밀 보관/관리실태 확인·감독 14. 비밀 보호조치(지정, 안전지출 등) 17. 보안관계관 운용 23. 외국인(직원) 보안관리 34. 유사시 시설/장비 보안조치 35. 사내 보안취약지 점검 46. 보안교육계획 수립 47. 주제/대상별 교안 작성 48. 대내·외 보안교육 실시 49. 보안교육 성과분석 50. 방산보안 대외협력 활동 52. 부서/계열사 보안점검	4. 보안일일결산 감독·통제 8. 각종 보안행정서류 집행·관리 15. 비밀 반입 및 반출 통제 16. 비밀 서류철 작성 관리 감독 18. 직원(협력사 등) 신원조사업무 19. 보안서약서 집행 / 관리 20. 비밀취급인가업무 처리 21. 개인정보보호업무 처리 24. 퇴직자 보안조치 25. 해외 출장자 보안교육 28. 출입통제시스템 운용 29. 출입증 관리 30. 사진촬영(녹음) 통제 31. 비인가자 접근/출입 통제 32. 외래인 출입시 보안조치 33. 장비 수송시 보안조치 40. 개인용컴퓨터 보안관리

다음은 1사분면(지속개발)에 해당되는 감사 및 평가시 가중치 부여가 필요한 직무에 대해 세부적으로 알아보겠다. 세부 직무 비율은 표 62와 같다.

표 62. 가중치가 필요한 세부 직무 비율
Table 62 Percentage of detailed jobs requiring weights

직무	세부 직무	I/D평균 (A)	수행빈도 (P)	A×P	세부비율 (A×P/∑)×100	비율 (%)
비밀 관리	12. 대외발송자료 보안성 검토	3.643	3.684	13.421	10.637	19.291
	13. 비밀 저장매체 관리	3.486	3.132	10.918	8.654	
정보 통신	36. 전산기(서버) 보안관리 감독	4.248	3.500	14.868	11.784	80.709
	37. 네트워크(망분리 포함) 보안 관제 감독	4.304	3.632	15.632	12.390	
	38. 정보보호시스템 보안관제 감독	4.265	3.842	16.386	12.987	
	39. 정보통신 장비 및 저장매체 관리	3.766	3.816	14.371	11.390	
	42. 보안관제결과(해킹) 조치 관리 감독	4.078	3.368	13.735	10.886	
	43. 방산 핵심기술 보호 관리	4.329	3.368	14.580	11.556	
	45. 상용정보통신망 보안관리 통제	3.697	3.316	12.259	9.716	
	∑(A×P)			126.170	100	100

비밀관리 직무는 19.3%, 정보통신보안은 80.7%의 비율로 감사 및 평가 시 가중치가 필요하다는 것을 확인할 수 있었다. 따라서 감사 및 평가시 비밀관리 직무와 정보통신보안 직무에 대해 비중을 높여야 함을 확인하였다. 현재 방산업체에서 수검을 받고 있는 통합실태조사의 경우 통합이전의 보안감사 분야(비밀관리)에 대한 평가 비중을 일부 상향시킬 필요가 있음을 보여주고 있다. 예를 들어 통합실태조사시 비밀관리를 포함한 보안감사 분야의 평가 비중을 일부 상향해야 함을 의미한다. 그림 44는 감사 및 평가 시 가중치가 필요한 직무에 대해 세부적으로 도식화한 자료이다.

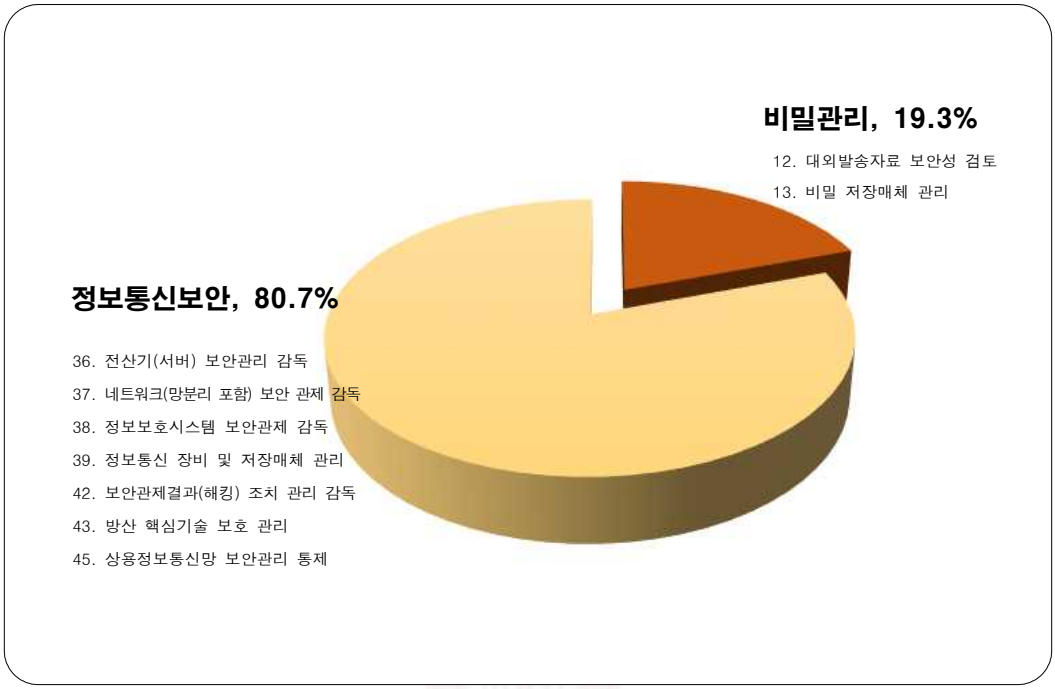


그림 44. 가중치가 필요한 직무(도표)
Figure 44. Jobs requiring weighting(diagram)

7. 설문시 제기된 추가 의견

설문에 응해준 38명 중 32건의 추가 의견이 제시되었다. 설문자들은 ① 현재 방위산업보안업무훈령과 방위산업기술보호법이 혼재하다 보니 방산보안업무에 혼선을 초래한다는 의견을 6명이 제기하였다. ② '20년 3월부터 시행중인 통합실태조사 시 관계기관의 과도한 자료요구와 업체의 실정을 미고려한 조사라는 볼멘소리를 낸 설문자도 6명이나 되었다. ③ 방산보안에 대한 업체 경영진의 관심부족(5명), ④ 정보통신보안에 대한 전문인력 확충(3명)과 IT·융합보안 필요(3명)의 순으로 제시하였다. 세부 제기된 내용은 표 63과 같다.

표 63. 설문시 제기된 추가 의견(애로 및 건의사항)
Table 63. Additional comments made during the survey (distress and suggestions)

설문 추가 의견(애로・건의사항) - 32건
1. 방위산업보안업무훈령과 방위산업기술보호법의 혼선 초래, 개정・통합 필요(6)
2. 통합실태조사 과도한 자료요구, 업체 실정 미고려, 조사관에 대한 불신 등(6)
3. 방산업체 경영진 보안 관심 부족, 첨단화된 정보시스템 투자 미흡(5)
4. 정보통신분야 기하급수적으로 발전 반면, IT・융합보안 대책 미흡(3)
5. 정보통신보안 전문성 필요, IT발전에 맞도록 전문인력 확충(3)
6. 보안 의무교육에 대한 명확한 상벌 부여 / 실무자 전문교육 확대(2)
7. 체계업체의 협력업체에 대한 기술보호 지원책임 한계 불명확(2)
8. 현실성 있는 방산보안업무 필요 / 행정간소화 시급(2)
9. 보안업무의 조직 및 인력구성 불충분(2)
10. 보안관계자와 기술보호책임에 대한 책임 한계 모호(1)

제7장 결 론

제1절 연구결과 요약

범정부 차원의 방산 수출 지원체계 마련과 K-방산의 세일즈 외교 등의 노력으로 매년 사상 최대 규모의 흑자를 기록하고 있다. 반면, K-방산의 확산과 달리 국내 방산기술을 노리는 적대국 또는 해커들의 공격도 증가하고 있는 추세이다. 국내 방산기술을 보호하기 위해서는 방산보안과 방산기술보호에 더 큰 관심과 노력이 절실한 시점이다.

따라서, 금번 연구에서는 방산보안의 중심에 있는 보안전문가의 직무를 진단하여 궁극적으로 '사이버 레질리언스'의 강화와 K-방산의 확산세를 측면지원하는 계기가 될 것이며 과학적 방법인 델파이 기법과 IPA 방법을 통한 직무영향 분석 결과가 향후 방산업체의 경영진, 관계 교육기관 및 평가기관에 유의미한 데이터를 제시하게 될 것으로 기대한다.

방산업체 보안전문가의 직무분석 결과를 정리해 보겠다. **첫째, 인력충원이 요구되는 세부 직무는 총 14개로 다음과 같다.**

인력충원이 요구되는 세부직무(14개, 경영층 관심 분야)	비율(%)
• 비밀관리 – 대외발송자료 보안성 검토 • 비밀관리 – 비밀 저장매체 관리 • 비밀관리 – 비밀 반입 및 반출 통제	19.0
• 인원보안 – 퇴직자 보안조치	6.3
• 시설/장비보안 – 출입통제시스템 운용 • 시설/장비보안 – 비인가자 접근/출입 통제	15.0
• 정보통신보안 – 전산기(서버) 보안관리 감독 • 정보통신보안 – 네트워크(망분리 포함) 보안 관제 감독 • 정보통신보안 – 정보보호시스템 보안관제 감독 • 정보통신보안 – 정보통신 장비 및 저장매체 관리 • 정보통신보안 – 개인용컴퓨터 보안관리 • 정보통신보안 – 보안관제결과(해킹) 조치 관리 감독 • 정보통신보안 – 방산 핵심기술 보호 관리 • 정보통신보안 – 상용정보통신망 보안관리 통제	59.7

정보통신보안(8개) 직무는 IT분야 고경력과 전문성을 갖춘 인력이 필요하며 특히, 비밀관리(3개), 퇴직자 보안조치, 시설/장비보안(2개) 직무는 경영층의 관심 부족과 인력 부족시 큰 사고로 확대될 가능성이 높은 직무로 분석된 수준의 비율만큼 인력충원 또는 임무 재분배가 요구되다.

둘째, 전문교육이 요구되는 세부 직무는 총 20개로 다음과 같다.

전문교육이 요구되는 세부 직무(20개, 교육기관 관심 분야)	비율(%)
• 보안행정 – 중장기 보안계획 수립 • 보안행정 – 연간 보안업무계획 수립 • 보안행정 – 보안내규 제·개정 • 보안행정 – 수출입 보안 조치	20.7
• 비밀관리 – 비밀 생산(접수) 보안관리 • 비밀관리 – 대외발송자료 보안성 검토	8.6
• 인원보안 – 보안관계관 운용 • 인원보안 – 핵심기술인력 보안조치	7.7
• 시설/장비보안 – 보호구역(시설) 설정 • 시설/장비보안 – 시설/장비 보호대책 구축	8.1
• 정보통신보안 – 전산기(서버) 보안관리 감독 • 정보통신보안 – 네트워크(망분리 포함) 보안 관제 감독 • 정보통신보안 – 정보보호시스템 보안관제 감독 • 정보통신보안 – 정보통신 장비 및 저장매체 관리 • 정보통신보안 – 보안관제결과(해킹) 조치 관리 감독 • 정보통신보안 – 방산 핵심기술 보호 관리 • 정보통신보안 – 재난대비 백업시설 유지관리 통제 • 정보통신보안 – 상용정보통신망 보안관리 통제	43.2
• 보안점검/조사 – 보안사고시 초동조치 및 관계기관 신고 • 보안점검/조사 – 통합실태조사 수검	11.7

중·장기 보안계획 수립 등 보안행정 직무(4개), 비밀생산(접수) 보안관리 등 비밀관리(2개), 보안관계관 운용 등 인원보안(2개) 직무, 보호구역(시설) 설정 등 시설/장비보안(2개) 직무, 전산기(서버) 보안관리 감독 등 정보통신보안(8개) 직무를 어렵다고 느끼고 있다. 특히, 보안행정, 비밀관리, 인원보안, 시설/장비보안의 경우 대다수 보안전문가들이 평상시 기본적으로 수행하는 업무임에도 어려움을 느끼고 있다는 것이 특이한 점이라 할 것이다.

셋째, 평가시 가중치가 요구되는 세부 직무는 총 9개로 다음과 같다.

평가시 가중치가 요구되는 세부직무(9개, 평가기관 관심 분야)	비율(%)
• 비밀관리 – 대외발송자료 보안성 검토 • 비밀관리 – 비밀 저장매체 관리	19.3
• 정보통신보안 – 전산기(서버) 보안관리 감독 • 정보통신보안 – 네트워크(망분리 포함) 보안 관제 감독 • 정보통신보안 – 정보보호시스템 보안관제 감독 • 정보통신보안 – 정보통신 장비 및 저장매체 관리 • 정보통신보안 – 보안관제결과(해킹) 조치 관리 감독 • 정보통신보안 – 방산 핵심기술 보호 관리 • 정보통신보안 – 상용정보통신망 보안관리 통제	80.7

대외발송자료 보안성 검토 등 비밀관리(2개) 직무, 전산기(서버) 보안관리 감독 등 정보통신보안(7개) 직무는 많은 시간 소요, 지속성과 전문성이 필요하면서도 중요도가 높은 영역으로 평가 시 가중치를 상향할 필요성이 있다.

제2절 정책적 제언

앞에서 언급한 연구결과를 바탕으로 방산업체 보안전문가의 직무역량을 강화하기 위한 정책적 제언사항은 다음과 같다.

첫째, 방산업체 경영진 차원에서 비밀관리(19%), 인원보안(6.3%), 시설/장비 보안(15%), 정보통신보안(59.7%) 분야에 전문성을 갖춘 인력을 충원해야 하며 특히, 정보통신보안의 비중이 상당히 높게 나타난 점을 볼 때 **IT 분야 발전 속도에 뒤처지지 않도록 보안시스템 구축**도 관심을 가져야 한다. 앞에서도 설명했듯이 현재 방산업체 보안부서에 근무하는 대다수가 4·50대 이상이며 학사 이하가 60%를 차지하고 있다. 업체의 입장에서 볼 때 IT분야 전문인력을 보안부서가 아닌 연구부서에 보직시키는 것도 이해가 되는 바이나, 연구부서 못지 않게 보안부서도 중요하다는 경영진의 인식전환이 필요하다. 더불어 전문성을 갖춘 보안부서 근무자 확보를 위해 기존 보직자들에 대한 교육여건 보장과 중

・장기적인 전문인력 확보 노력도 필요하고, 기하급수적으로 발전하고 있는 IT 분야에 걸맞은 '첨단 및 융합 보안시스템' 구축에 업체의 적극적인 투자와 지원이 절실하다 할 것이다.

둘째, 방산기술보호와 방산보안 교육기관에서 업체 보안전문가에 대한 교육 프로그램을 일부 개편할 필요가 있다. 현재는 대부분 '방산기술보호'와 '정보통신 보안'에 대한 교육이 집중되고 있다. 앞에서 분석한 것 같이 중・장기 보안계획 수립 등 '보안행정' 직무를 어렵다고 인식하고 있고 방산업체 보안전문가라면 당연히 잘 알고 있을 것으로 생각했던 '비밀관리' 직무에 대해서도 어렵다고 인식하고 있었다. 한편, '정보통신보안' 직무는 예상했던 것 같이 중요하면서도 어렵다는 인식을 재확인할 수 있었다. 설문을 통해 확인된 20개 세부 직무가 전부일 수는 없다. 단, 관계 교육기관에서는 상기 설문결과를 참고하여 교육 전반에 대한 커리큘럼 조정 등 고객(방산업체 보안전문가)의 니즈(Needs)와 입장을 충분히 고려한 교육계획 수립이 필요하다 할 것이다.

셋째, 통합실태조사 평가에 대한 명확한 기준점 마련이 요구되며, 과도한 자료요구 등 감사에 대한 경감 노력이 필요하다. 2020년 3월부터 방산업체 대상 방위산업기술보호의 '실태조사'와 기존의 '보안감사'의 이중부담에 대한 경감 차원에서 실시하고 있으나, 다수의 방산업체에서는 통합실태조사에 대한 볼멘소리가 여전하다. 설문결과에서 확인했듯이 과도한 자료요구, 업체의 환경과 실정 미고려, 조사관에 대한 불신 등 다수의 방산업체 보안전문가들이 통합실태조사에 대한 어려움을 호소하고 있다. 방위산업기술 보호지침의 부록 '실태조사 핵심 점검항목'에는 항목별 점검내용은 제시하고 있으나 배점은 명문화되어있지 않다. 물론, 실태조사 기관 내부적으로 명확한 평가기준이 마련되어 있을 것이다. 통합실태조사 제도의 발전과 개선을 위해서라도 실태조사 항목별 명확한 평가 채점(기준)표가 공개되어야 할 것이다.

또한, 통합실태조사가 당연히 방위산업기술보호에 중점을 둔다는 것에는 이견이 없다. 그러나 IPA 분석결과에서 보았듯이 감사 및 평가 시 '정보통신보안'과 '비밀관리'에 대한 가중치가 필요하다는 것을 알 수 있었다. 특히, 통합실태조사가 보안감사와 통합하여 시행한다는 본래 취지로 비추어 볼 때 '비밀관리'(舊 보안감사분야) 직무의 감사 및 평가 점수를 일정 부분 상향할 필요가 있다고 본다.

더불어, 통합실태조사에 대한 과도한 자료요구에 대해서도 개선이 필요하다. 최근 대다수 감사의 경우 수검받는 기관(업체)에 부담을 최소화하기 위해 자료요구를 지양하고 가급적 현장위주로 감사를 시행하는 분위기이다. 따라서, 통합실태조사의 경우도 업체에 감사준비를 위한 불필요한 행정 소요 등 부담을 경감시키기 위한 개선책 마련이 필요하다 할 것이다.

넷째,「방위산업보안업무훈령」과「방위산업기술보호법」의 통합이 필요하다. 방산업체에서는 유사한 두 개의 보안정책을 적용받고 있어서 보안 행정소요의 증가 및 예산 낭비 등 보안 업무의 효율성이 저하되는 문제가 나타나고 있고 설문에서도 동일한 의견이 식별되고 있다. 그래도 다행인 것은 현재 방첩사에서 관련 연구가 시작되고 있다는 것이다.[24] 모두가 공감하고 현실성 있는 방산보안 업무로 탈바꿈할 수 있도록 관계기관들의 숙의를 통해 일원화된 '방위산업보안기본법(가칭)'의 제정이 필요하다 할 것이다.

금번 연구는 방산업체 보안전문가 직무의 중요도·난이도·수행빈도 등 직무영향을 구체적으로 분석한 최초의 논문이며, 방산업체 보안전문가의 직무를 구체화시키기 위해 비교확인법(직무분석방법), 델파이 기법, IPA 분석 활용 등 '분석의 다변화'를 꾀한 연구물이라 할 것이다. 특히, 동 연구를 통해 방산업체 경영진에게는 인력충원 필요성, 교육기관에는 전문교육의 소요, 감사 및 평가기관에는 가중치 항목을 제시했다는 데 의의가 있다.

---

24) "'K방산' 보안 강화한다… 방첩사 '방산보안기본법' 제정 검토", new1뉴스, 2023. 7. 7.

제3절 연구의 한계

본 연구는 학문적·정책적으로 방위산업보안과 방산업체 보안전문가의 직무를 발전시켰다는 기대에도 불구하고 일부 한계를 가지고 있다. 첫째, 방산보안 전문가(11명)와 방산보안 현장 실무자(40명) 등 일부 인원으로 국한된 설문으로 연구 결과물의 일반화가 되지 못했다. 둘째, 방산업체의 규모, 특성 등이 다름에도 차별화한 연구결과를 구분하지 못했다. 따라서, 본 연구에서 한계점을 보완하기 위해서는 향후 방산업체 및 군/정부기관에 근무 중인 다양한 직책의 보안 실무자를 대상으로 설문자의 수와 범위를 확대하고, 방위산업의 규모와 특성을 고려한 방산업체별 보안전문가의 직무연구를 세분화할 필요가 있다.

참 고 문 헌

[1] 강경종, 김종우. 전문대학 교육과정 모형개발과 운영방안, 서울:한국직업능력개발원. 2001.

[2] 고희재. 방위산업 보안수준 평가 지표 개발 연구. 국내박사학위논문 중앙대학교 대학원, 2021. 서울

[3] 고희재; 이창무. 델파이 및 AHP 를 활용한 방산업체 보안 평가 지표 개발. 한국경호경비학회지, 2021, 67: 1-26.

[4] 김선녀. 델파이 기법과 계층적 의사결정방법(AHP)의 적용을 통한 병원 간호부서별 직무역량 평가지표 개발. 국내박사학위논문 고신대학교 일반대학원, 2021. 부산

[5] 김성훈. 한국기업의 핵심인력 육성 및 인재관리 능력. 한국경영자총협회, 통권 제 288호. 2002, 30-34

[6] 김영태, et al. 언어재활사의 직무 중요도, 난이도, 빈도에 대한 인식. Communication Sciences & Disorders, 2015, 20.1: 97-105.

[7] 김은영; 조혜주. 유치원과 어린이집 교사의 직무에 대한 인식: 수행빈도, 중요도, 난이도를 중심으로. 2013.

[8] 나재관. 평생교육 관점에서 방과후학교 담당자의 직무분석 및 핵심역량 개발. 국내박사학위논문 동의대학교 대학원, 2022. 부산

[9] 박홍순; 김세용; 김용환. 체계적인 방위산업기술 보호를 위한 보호체계 우선순위 분석 연구. 융합보안논문지, 2019, 19.4: 4-5.

[10] 류연승. 방산보안 2.0. 정보보호학회지, 2018, 28.6: 6-12.

[11] 문인수. 학교전담경찰관의 직무분석과 개선방안. 국내박사학위논문 동국대학교 일반대학원, 2022. 서울

[12] 박상호. 빅데이터를 활용한 산업보안 전문인력 요구직무 분석. 국내박사 학위논문 중앙대학교 대학원, 2019. 서울

[13] 박현경; 양지희. 국내 직무분석에 관한 체계적 문헌고찰: 2010 년 이후 국내 학술지 발표논문 중심으로. 교육컨설팅코칭연구, 2019, 3.2: 45-64.

[14] 박홍순; 김세용; 김용환. 체계적인 방위산업기술 보호를 위한 보호체계 우선순위 분석 연구. 융합보안논문지, 2019, 19.4: 4-5.

[15] 손창근; 류연승. 각 軍의 방위산업기술보호 인식 및 역량 제고를 위한 교육 방안. 정보보호학회지, 2018, 28.6: 63-69.

[16] 송화선. 영상편집 직무의 수행 빈도, 중요도, 난이도 인식에 관한 연구. 디지털콘텐츠학회논문지, 2007, 8.4: 531-539.

[17] 염상원; 김장엽; 한재현. IPA 방법론을 통한 연구개발 업체선정 평가모형 개선 연구. 한국방위산업학회지, 2018, 25.4: 41-60.

[18] 우광제; 송해덕. DACUM 기법을 이용한 방위산업체 정보통신보안실무자 직무분석. 융합보안논문지, 2014, 14.4: 73-84.

[19] 우광제. 융합보안 관점에서 방위산업보안 개념 정립과 연구동향 분석. 융합보안논문지, 2015, 15.6: 69-78.

[20] 우광제, 송해덕. 융합보안전문가의 핵심과업 요구분석 - 방위산업체 보안 전문가를 중심으로. 융합보안 논문지 16.3_2 (2016): 87-98.

[21] 연희모. 내부자에 의한 산업기밀 유출방지 방안. 국내석사학위논문 성균관 대학교 국가전략대학원, 2013. 서울

[22] 이민형; 박주상. 델파이 기법을 활용한 해양경비안전본부 직무분석-해양 경찰안전국을 중심으로. 한국경찰연구, 2015, 14.3: 135-152.

[23] 이승훈. 자율적 방위산업기술보호를 위한 보호체계 구축 방안. Review of KIISC, 2018, 28.6: 20-24.

[24] 이여진, et al. 외래간호사의 직무에 대한 중요도, 난이도, 빈도 분석. 기본간호학회지, 2009, 16.2: 232-241.

[25] 이을지. 교육청 소속 기록연구사 직무 분석에 관한 연구. 국내석사학위논문 한성대학교 대학원, 2016. 서울

[26] 이을지; 이호신. 교육청 소속 기록연구사의 직무 분석에 관한 연구. 한국기록관리학회지, 2016, 16.3: 131-156.

[27] 이형진. 방위산업기술보호법 제정의 의미와 방위산업기술보호 중요성 인식 제고 방안. 한국산업보안연구, 2016, 6.2: 57-80.

[28] 임성근; 소순창; 이창섭. IPA 분석을 활용한 정부 3.0 서비스 정부에 대한 공급자와 수요자 간 인식차이 분석. 서울대학교 한국행정연구소, 2017, 55.2: 137-167.

[29] 장경준. 방위산업기술 자료의 외부 반출 시 보호 방안. Review of KIISC, 2018, 28.6: 50-55.

[30] 정연희, et al. DACUM 기법을 이용한 한방간호사의 직무분석. 동서간호학연구지, 2017, 23.1: 63-74.

[31] 조대연, et al. 국내 직무분석에 관한 연구논문 분석: 2000 년 이후 국내 학술지 발표 논문을 중심으로. 역량개발학습연구, 2011, 6.4: 1-19.

[32] 진기정. 직무분석을 통한 자연환경복원 엔지니어링 표준품셈 합리화 방안 연구. 2014.

[33] 최용석; 백승철; 권혁인. 델파이기법을 이용한 U-city 사업의 핵심성공요인 도출. 인터넷전자상거래연구, 2008, 8.3: 183-209.

[34] 최정화,이경은. DACUM 기법을 이용한 영양사의 직무분석 - 중요도, 수행도 및 난이도 분석 -. 한국식품영양학회지 32.5 (2019): 536-552.

[35] 허아라; 류연승. 국방과학기술 정보의 분류체계 고찰. 정보보호학회지, 2018, 28.6: 25-32.

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

[37] Martilla,J.& James,J.C(1977).Importance-permance analysis, Journal of Marketing, 41(1):13-17.

[38] McCormick, E. 1976. Job and task analysis. in; M. Dunnette, (ed.,) Handbook of industrial and organizational psychology. p. 651-696. Rand McNalley, Chicago.

[39] PARK, Heungsoon; GO, Heejae; HWANG, Jonghyeon. Conceptualization of defense industrial security in relation to protecting defense technologies. In: International Conference on Computational Science and Its Applications. Cham: Springer International Publishing, 2018. p. 158-169.

[40] THOMPSON, Duane E.; THOMPSON, Toni A. Court standards for job analysis in test validation. Personnel Psychology, 1982, 35.4: 865-874

[41] 교육학용어사전, 서울대학교 교육연구소, 1995.

[42] 국방기술품질원, 국방과학기술용어사전, 2017.

[43] 방위산업기술 보호법

[44] 방위산업기술 보호지침 별표 3・별표12

[45] 방위사업법 시행령 제44조 '보안요건'

[46] 방위산업보안업무훈령 국방부훈령 제2422호

[47] 중소벤처기업부 중소기업 기술보호울타리 기술보호수준 실태조사현황, 2023.

[48] 직무분석규정 대통령령 제2811호(2017)

[49] 산업기술의 유출방지 및 보호에 관한 법률

< 인터넷 사이트 >

[50] 네이버블로그, https://blog.naver.com/zazayo90/222900003322

[51] 네이버블로그, https://blog.naver.com/accept119/223064198001

[52] 산업보안관리사 홈페이지, https://license.kaits.or.kr/certificate/introduce.do

[53] 심리학용어사전, 한국심리학회, 2014. http://www.koreanpsychology.or.kr

< 부　록 >

① 설문지 1차(방산업체 보안전문가 직무 식별)

② 설문지 2차(방산업체 보안전문가 직무 식별)

③ 설문지 3차(방산업체 보안전문가 직무영향분석)

설문지 1차(방산업체 보안전문가 직무 식별)

방산업체 보안전문가 직무 영향분석에 관한 연구를 위한 설문조사

안녕하십니까?
광운대학교 방위사업학과 박사과정 이승목입니다.

본 설문은 방산업체 보안전문가들의 직무영향을 분석(중요도, 난이도, 수행빈도)을 통해 향후 방산업체 보안전문가들의 업체 채용 기준, 교육에 대한 소요 판단, 감사시 가점 부여 등 과학적 판단기준을 마련하고자 합니다.

최근 방산보안전문가들의 직무를 분석했던 논문과 방위산업보안업무훈령, 방위산업기술 보호지침 등에 기술된 방산업체 보안전문가들의 직무를 분석하여 7개의 항목, 55개의 세부항목으로 예비직무를 도출하였습니다.

방산업체 보안전문가 40여명 대상 직무영향분석 설문에 앞서, 방산업체 현장 및 교육·평가(감사) 분야 전문가 그룹(11명)을 선정하였습니다. 전문가 그룹 설문을 통해 도출한 예비직무의 타당성을 검증할 예정입니다.

응답하신 내용은 통계목적으로만 사용될 것임을 약속드리며, 정확한 연구를 위해 힘드시더라도 설문에 적극 참여해 주시길 당부드립니다.

광운대학교 일반대학원 방위사업학과
연구자 : 박사과정 이 승 목
지도교수 : 정 석 재

방산업체 보안전문가 예비직무에 대한 설문(전문가 그룹 11명)

직 무	세부 직무	동의 여부	
		○	×
보안행정	1. 중장기 보안계획 수립하기		
	2. 연간 보안업무계획 수립하기		
	3. 보안내규 작성(개정) 하기		
	4. 보안일일결산 감독하기		
	5. 보안수준 평가하기		
	6. 하도급 보안 관리하기		
	7. 수출입 보안 조치하기		
	8. 각종 보안행정서류 집행・관리		
	세부 직무 중 중복 또는 불필요한 직무 여부(내용기술)		
	기타) 추가・보완이 필요한 직무		
비밀관리	1. 보호대상 비밀 지정하기		
	2. 비밀 생산 보안조치하기		
	3. 비밀소유조사/재분류하기		
	4. 비밀 보관/관리실태 확인하기		
	5. 대외발송자료 보안성 검토		
	6. 비밀 저장매체 관리하기		
	7. 비밀 안전조치하기		
	세부 직무 중 중복 또는 불필요한 직무 여부(내용기술)		
	기타) 추가・보완이 필요한 직무		

인원보안	1. 보안관계관 운용하기		
	2. 직원 신원조사업무 처리하기		
	3. 보안서약서 집행/관리하기		
	4. 비밀취급인가업무 처리하기		
	5. 개인정보보호업무 처리하기		
	6. 핵심기술인력 보호하기		
	7. 외국인(직원) 보안관리하기		
	8. 퇴직자 보안조치하기		
	9. 해외 출장자 보안조치하기		
	세부 직무 중 중복 또는 불필요한 직무 여부(내용기술)		
	기타) 추가·보완이 필요한 직무		
시설/장비보안	1. 보호구역(시설) 설정하기		
	2. 시설/장비 보호대책 구축하기		
	3. 출입통제시스템 운용하기		
	4. 출입증 관리하기		
	5. 사진촬영(녹음) 통제하기		
	6. 비인가자 접근/출입 통제하기		
	7. 외래인 출입시 보안조치하기		
	8. 장비 수송시 보안조치하기		
	9. 유사시 안전조치 하기		
	10. 사내·외 보안취약지 점검		
	세부 직무 중 중복 또는 불필요한 직무 여부(내용기술)		
	기타) 추가·보완이 필요한 직무		

정보통신보안	1. 주전산기(서버) 보안관리하기		
	2. 네트워크 보안관제하기		
	3. 정보보호시스템 보안관제하기		
	4. 정보통신 저장매체 관리하기		
	5. 개인용컴퓨터 보안관리하기		
	6. 사무장비 보안관리하기		
	7. 협력업체 시스템 보안관리하기		
	8. 보안관제결과(해킹) 조치하기		
	9. 방산 핵심기술 보호 관리		
	10. 재난대비 백업시설 유지관리		
	11. 상용정보통신망 보안관리하기		
	세부 직무 중 중복 또는 불필요한 직무 여부(내용기술)		
	기타) 추가·보완이 필요한 직무		
보안교육/기타	1. 보안교육계획 수립하기		
	2. 주제/대상별 교안 작성하기		
	3. 보안교육 실시하기		
	4. 교육성과 분석하기		
	5. 방산보안 대외협력 활동		
	세부 직무 중 중복 또는 불필요한 직무 여부(내용기술)		
	기타) 추가·보완이 필요한 직무		

보안감사/조사	1. 보안측정 의뢰/결과 조치하기		
	2. 부서/계열사 보안감사하기		
	3. 정기/수시 보안점검하기		
	4. 보안사고 조사/조치하기		
	5. 통합실태조사 수검하기		
	세부 직무 중 중복 또는 불필요한 직무 여부(내용기술)		
	기타) 추가·보완이 필요한 직무		

설문에 참여해 주셔서 진심으로 감사드립니다.

설문지 2차(방산업체 보안전문가 직무 식별)

방산업체 보안전문가 직무 영향분석에 관한 연구를 위한 설문조사

안녕하십니까?
광운대학교 방위사업학과 박사과정 이승목입니다.

방산업체 보안전문가들의 직무를 확정하기 위해 보안전문가이신 11분의 의견을 종합하였습니다. 종합한 결과, 24개의 직무에 대해서는 직무 명칭이 모호하거나 행동화 될 수 있는 직무로 명칭을 변경하였고, 1개 직무는 삭제, 2개 직무가 추가되었습니다. 붙임 내용을 참고하시고 동의 여부를 통보해 주시면 직무를 확정하겠습니다.

- 삭제(1) : 보호대상 비밀 지정하기
- 추가(2) : 비밀 지출 및 반출 통제 / 비밀 서류철 작성 관리 감독

이후 확정된 직무는 방산업체 보안전문가 설문을 통해 직무영향을 분석(중요도, 난이도, 수행빈도)하여 방산업체 채용 기준, 교육에 대한 소요 판단, 감사시 가점 부여 등 과학적 판단기준을 마련할 예정입니다.

바쁘신 와중에도 설문에 적극 참여해 주시어 대단히 감사합니다.

1. 1차 설문결과에 대한 동의 여부 : 동의( ), 부동의( )

2. 부동의시 의견 :

광운대학교 일반대학원 방위사업학과
연구자 : 박사과정 이 승 목
지도교수 : 정 석 재

붙임 : 방산업체 보안전문가 1차 설문 결과(전문가 그룹 11명)

직 무	세부 직무	합의율(%)	비고
보안행정	1. 중장기 보안계획 수립	100	
	2. 연간 보안업무계획 수립	100	
	3. ~~보안내규 작성(개정) 하기~~ 명칭변경 → 보안내규 제·개정	100	명칭 변경
	4. ~~보안일일결산 감독하기~~ 명칭변경 → 보안일일결산 감독·통제	81.8	명칭 변경
	5. ~~보안수준 평가하기~~ 명칭변경 → 보안수준평가 감독·통제	90.9	명칭 변경
	6. ~~하도급 보안 관리하기~~ 명칭변경→하도급 보안특약조건 검토 및 감독	90.9	명칭 변경
	7. 수출입 보안 조치	81.8	
	8. 각종 보안행정서류 집행·관리	100	
	설문시 전문가 특이 의견 1. 하도급 보안관리 직무가 오히려 업체 입장에서 발목을 잡히는 행위가 될 수 있어 직무내용 순화 필요 2. 보안내규, 보안일일결산, 보안수준평가 직무에 대해서는 실제 행동화하는 명칭으로 변경		
비밀관리	1. ~~보호대상 비밀 지정하기~~(삭제)	63.6	삭제
	2. 비밀 생산 보안조치하기 명칭변경 → 비밀 생산(접수) 보안관리	81.8	명칭 변경
	3. 비밀소유조사 / 재분류	90.9	
	4. ~~비밀 보관 / 관리실태 확인~~ 명칭변경 → 비밀 보관/관리실태 확인·감독	100	명칭 변경
	5. 대외발송자료 보안성 검토	100	
	6. 비밀 저장매체 관리	100	
	7. ~~비밀 안전조치~~ 명칭변경 → 비밀 보호조치 (지정/분류, 안전지출 등 포함)	81.8	명칭 변경

	8. 비밀 반입 및 반출 통제		추가
	9. 비밀 서류철 작성 관리 감독		추가
	설문시 전문가 특이 의견 1. 비밀 반입 및 반출 통제에 대한 의견과 비밀 서류철 작성에 대한 관리 감독의 직무 추가 필요 2. 비밀 안전조치는 직무가 명확하지 않아 명칭변경 필요 3. 비밀 지정은 보안전문가 직무보다는 지정권자 임무		
인원보안	1. 보안관계관 운용	100	
	2. ~~직원 신원조사업무 처리~~ 명칭변경 → 직원(협력사 등) 신원조사업무 처리	100	명칭 변경
	3. 보안서약서 집행 / 관리	100	
	4. 비밀취급인가업무 처리	100	
	5. 개인정보보호업무 처리	90.9	
	6. ~~핵심기술인력 보호~~ 명칭변경 → 핵심기술인력 보안조치	81.8	명칭 변경
	7. 외국인(직원) 보안관리	100	
	8. 퇴직자 보안조치	100	
	9. ~~해외 출장자 보안조치~~ 명칭변경 → 해외 출장자 보안교육	90.9	명칭 변경
	설문시 전문가 특이 의견 1. 핵심기술인력에 대한 보호는 보안업무보다는 타 기관업무에 더 큰 비중 차지, 보안조치로 직무변경 필요 2. 해외 출장 보안조치는 해 부서의 조치이고 보안부서 에서는 보안교육의 직무가 타당		
시설/장비 보안	1. 보호구역(시설) 설정	100	
	2. 시설/장비 보호대책 구축	100	
	3. 출입통제시스템 운용	81.8	
	4. 출입증 관리	81.8	
	5. 사진촬영(녹음) 통제	100	
	6. 비인가자 접근 / 출입 통제	100	

	7. 외래인 출입시 보안조치	100	
	8. 장비 수송시 보안조치	90.9	
	9. ~~유사시 안전조치~~(명칭모호) 명칭변경 → 유사시 시설/장비 보안조치	81.8	명칭 변경
	10. ~~사내·외 보안취약지 점검~~ 명칭변경 → 사내 보안취약지 점검	100	명칭 변경
	설문시 전문가 특이 의견 1. 유사시 안전조치 직무는 용어가 불명확하여 혼선 초래, 유사시 시설 및 장비에 대한 보안조치로 변경 2. 사외 보안취약지 점검은 미해당(사내로 제한)		
정보통신보안	1. ~~주전산기(서버) 보안관리~~ 명칭변경 → 주전산기(서버) 보안관리 감독	100	명칭 변경
	2. ~~네트워크 보안관제~~ 명칭변경 → 네트워크(망분리 포함) 보안 관제 감독	90.9	명칭 변경
	3. ~~정보보호시스템 보안관제~~ 명칭변경 → 정보보호시스템 보안관제 감독	90.9	명칭 변경
	4. ~~정보통신 저장매체 관리~~(6번과 통합) 명칭변경 → 정보통신 장비 및 저장매체 관리	100	명칭 변경
	5. 개인용컴퓨터 보안관리	100	
	6. ~~사무장비 보안관리~~(4번과 통합, 삭제)	100	통합
	7. ~~협력업체 시스템 보안관리~~ 명칭변경 → 협력업체 시스템 보안관리 감독	90.9	명칭 변경
	8. ~~보안관제결과(해킹) 조치~~ 명칭변경 → 보안관제결과(해킹) 조치 관리 감독	100	명칭 변경
	9. 방산 핵심기술 보호 관리	90.9	
	10. ~~재난대비 백업시설 유지관리~~ 명칭변경 → 재난대비 백업시설 유지관리 통제	90.9	명칭 변경
	11. ~~상용정보통신망 보안관리~~ 명칭변경 → 상용정보통신망 보안관리 통제	100	명칭 변경

	설문시 전문가 특이 의견 1. 정보통신보안 분야는 대부분 정보통신실무자의 임무로 보안전문가는 해당 업무에 대한 통제와 감독임무 수행 2. 업체 망분리 정책과 시스템 유지관리에 대한 직무 필요 → 네트워크(망분리 포함) 보안관제 감독 직무에 통합		
보안교육 / 기타	1. 보안교육계획 수립	100	
	2. 주제/대상별 교안 작성	100	
	3. ~~보안교육 실시~~ 명칭변경 → 대내·외 보안교육 실시	100	명칭 변경
	4. ~~교육성과 분석~~ 명칭변경 → 보안교육 성과분석	90.9	명칭 변경
	5. 방산보안 대외협력 활동	100	
	설문시 전문가 특이 의견 1. 대외 직무교육 수강 등 인적계발 노력이 필요하다는 의견 → 보안교육내용에 포함		
보안점검 / 조사	1. 보안측정 의뢰/결과 조치	100	
	2. ~~부서/계열사 보안감사~~ 명칭변경 → 부서/계열사 보안점검	100	명칭 변경
	3. 정기/수시 보안점검	100	
	4. ~~보안사고 조사/조치~~ 명칭변경 → 보안사고시 초동조치 및 관계기관 신고	100	명칭 변경
	5. 통합실태조사 수검	100	
	설문시 전문가 특이 의견 1. 부서/계열사에 대한 보안감사라는 직무 명칭은 오해 유발 가능, 감사보다는 보안점검 직무가 타당 2. 보안사고 조사/조치보다는 보안사고시 초동조치 및 관계기관 신고라는 행동화 직무로 변경 필요		

설문에 참여해 주셔서 진심으로 감사드립니다.

설문지 3차(방산업체 보안전문가 직무영향분석)

방산업체 보안전문가 직무 영향분석에 관한 연구를 위한 설문조사

안녕하십니까?
광운대학교 방위사업학과 박사과정 이승목입니다.

지난 9.11. ~ 9.25. 간 보안전문가이신 11명 대상으로 설문을 진행하였고 SNS를 통해 다양한 추가의견을 종합, 방산업체 보안전문가들의 7개 직무와 55개 세부 직무를 확정하였습니다.

확정된 직무는 방산분야 보안전문가 40여 명 대상으로 직무영향분석(중요도, 난이도, 수행빈도) 설문을 진행하여 방산업체 채용 기준, 교육에 대한 소요 판단, 감사시 가점 부여 등 과학적 판단기준을 마련할 예정입니다.

전문가님들의 소중한 의견이 적극 활용될 수 있도록 성심껏 응답해 주시길 당부드리며, 설문조사는 익명으로 실시하고 응답하신 자료는 통계법 등에 의거하여 학술적인 목적으로만 사용될 것임을 약속드립니다.

< 설문 방법 예시 >

직 무	세부 직무	중요도					난이도					수행빈도				
보안행정	1. 중장기 보안계획 수립	1	**2**	3	4	5	1	2	3	**4**	5	**1**	2	3	4	5
	2. 연간 보안업무계획 수립	1	2	3	**4**	5	1	2	**3**	4	5	**1**	2	3	4	5
	3. 보안예규 제·개정	1	**2**	3	4	5	1	2	3	**4**	5	1	**2**	3	4	5

중요도, 난이도, 수행빈도에 대한 세부 기준점은 본 설문지에서 제시

광운대학교 일반대학원 방위사업학과
연구자 : 박사과정 이 승 목
지도교수 : 정 석 재

방산분야 보안전문가 3차 설문 조사

1. 설문대상자 기본사항으로 해당사항에 (√) 해 주십시오.

직 업	□ 군/정부기관 □ 교육기관 □ 방산업체 보안관계자 □ 기 타
연 령	□ 20대 □ 30대□ 40대 □ 50대 □ 60대 이상
최종학력	□ 학사 □ 석사 수료 □ 석사 □ 박사 수료 □ 박사
보안경력	□ 5년이하 □ 5~10년 □ 10~15년 □ 15~20년 □ 20년이상

2. 설문대상자 연락처

연락처	010 - -

* 연락처는 설문에 활용하지 않고, 향후 답례품 제공목적으로만 활용됩니다. 원하시지 않을 경우 답변을 안해 주셔도 됩니다.

3. 방산업체 보안전문가 직무의 중요도, 난이도, 수행빈도에 대한 설문으로 해당사항에 (√) 해 주십시오.

구 분	5점 척도 평가 기준
중요도	5점 : 방산업체 운영에 심각한 영향을 미치는 직무
	4점 : 방산업체 운영에 크게 영향이 있는 직무
	3점 : 방산업체 운영에 상대적 영향을 미치는 직무
	2점 : 방산업체 운영에 일부 영향을 미치는 직무
	1점 : 방산업체 운영에 영향이 미미한 직무
난이도	5점 : 수행업무가 고도의 전문성을 요구하는 직무
	4점 : 수행업무가 일부 전문성을 요구하는 직무
	3점 : 수행업무가 일정교육 이수시 가능한 직무
	2점 : 수행업무가 대리수행자가 가능한 직무
	1점 : 수행업무가 누구나 할 수 있는 직무
수행빈도	5점 : 수시 또는 일일단위 수행하는 직무
	4점 : 일일 ~ 주단위 수행하는 직무
	3점 : 주간 ~ 월간단위 수행하는 직무
	2점 : 월간 ~ 분기단위 수행하는 직무
	1점 : 분기 이상 단위 수행하는 직무

직 무	세부 직무	중요도					난이도					수행빈도				
보안행정	1. 중장기 보안계획 수립	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	2. 연간 보안업무계획 수립	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	3. 보안내규 제·개정	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	4. 보안일일결산 감독·통제	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	5. 보안수준평가 감독·통제	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	6. 하도급 보안특약조건 검토 및 감독	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	7. 수출입 보안 조치	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	8. 각종 보안행정서류 집행·관리	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
비밀관리	1. 비밀 생산(접수) 보안관리	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	2. 비밀소유조사 / 재분류	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	3. 비밀 보관/관리실태 확인·감독	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	4. 대외발송자료 보안성 검토	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	5. 비밀 저장매체 관리	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	6. 비밀 보호조치(지정, 안전지출 등)	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	7. 비밀 반입 및 반출 통제	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	8. 비밀 서류철 작성 관리 감독	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
인원보안	1. 보안관계관 운용	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	2. 직원(협력사 등) 신원조사업무	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	3. 보안서약서 집행 / 관리	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	4. 비밀취급인가업무 처리	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	5. 개인정보보호업무 처리	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	6. 핵심기술인력 보안조치	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	7. 외국인(직원) 보안관리	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	8. 퇴직자 보안조치	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	9. 해외 출장자 보안교육	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
시설 / 장비보안	1. 보호구역(시설) 설정	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	2. 시설/장비 보호대책 구축	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	3. 출입통제시스템 운용	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	4. 출입증 관리	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	5. 사진촬영(녹음) 통제	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	6. 비인가자 접근 / 출입 통제	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	7. 외래인 출입시 보안조치	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	8. 장비 수송시 보안조치	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	9. 유사시 시설/장비 보안조치	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	10. 사내 보안취약지 점검	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤

정보통신보안	1.전산기(서버) 보안관리 감독	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	2.네트워크(망분리 포함) 보안 관제 감독	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	3. 정보보호시스템 보안관제 감독	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	4. 정보통신 장비 및 저장매체 관리	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	5. 개인용컴퓨터 보안관리	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	6. 협력업체 시스템 보안관리 감독	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	7. 보안관제결과(해킹) 조치 관리 감독	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	8. 방산 핵심기술 보호 관리	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	9. 재난대비 백업시설 유지관리 통제	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	10. 상용정보통신망 보안관리 통제	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
보안교육 / 기타	1. 보안교육계획 수립	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	2. 주제/대상별 교안 작성	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	3. 대내·외 보안교육 실시	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	4. 보안교육 성과분석	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	5. 방산보안 대외협력 활동	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
보안점검 / 조사	1. 보안측정 의뢰/결과 조치	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	2. 부서/계열사 보안점검	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	3. 정기/수시 보안점검	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	4. 보안사고시 초동조치 및 관계기관 신고	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
	5. 통합실태조사 수검	①	②	③	④	⑤	①	②	③	④	⑤	①	②	③	④	⑤
기 타	방산업체 보안전문가 직무수행간 애로·건의사항															

설문에 참여해 주셔서 진심으로 감사드립니다.