韓國IT서비스學會誌
第18卷 第4號
2019年 10月, pp.55-66

Journal of Information Technology Services
https://doi.org/10.9716/KITS.2019.18.4.055

행정기관의 정보보호 담당인력을 어떻게 관리할 것인가?*

전효정** · 김태성*** · 박기태****

How Do We Manage the Information Security Workforce of the Administrative Agencies?*

Hyo-Jung Jun** · Tae-Sung Kim*** · Ki Tae Park****

■ Abstract ■

The career development of information security workforce affiliated in administrative department is very different from workforce affiliated in private companies. Their career development attempts are made not by voluntary motivation but by involuntary job movement by the principle of internal relocation. So they are not directly linked to monetary compensation or advancement. Due to the nature of the organization, their work attitude is very passive and there is little intention to turnover. They do not need professionalism, but they must be retrained according to the law. In this paper, we investigate and analyze the roles and responsibilities of information security workforce of each administrative department. And we do questionnaire survey to find out current roles and responsibilities of them will not affect the demand for retraining. Through these research, we would like to discuss how to manage information security workforce affiliated in administrative departments.

Keyword : Information Security Workforce, Administrative Agencies, R&R(Roles and Responsibilities), Skilled Level, Retraining Needs, MANOVA

Submitted : May 31, 2019 1st Revision : August 12, 2019 Accepted : October 9, 2019

* 이 논문은 2018년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임(NRF-2018S1A5A2A01039356).

** 충북대학교 경영정보학과 및 보안경제연구소

*** 충북대학교 경영정보학과 및 보안경제연구소, 교신저자

**** 국가보안기술연구소

1. 서 론

실리와 명분을 이유로 국가 간 물리적 군사전쟁의 가능성은 낮아지고 있지만, 국가 주요기반시설 및 행정업무는 물론 민간기업의 사업활동 대부분이 빠르게 네트워크화 되면서 사이버 전쟁에 대한 두려움은 커지고 있다. 일례로, 2017년 사이버 공격에 따른 우리나라 기업의 직간접 손실액은 약 77조원으로 GDP의 5%에 육박하는 것으로 추정되고 있으며, 기업들은 사이버 공격에 대한 공포로 디지털 트랜스포메이션 계획을 연기하는 등 사이버안전에 대한 우려가 ICT 新기술 확산의 걸림돌로 작용하고 있는 것으로 나타났다(MS News, 2019). 조직 내에 사건대응 전담팀을 별도로 구성하여 운영하는 것이 매년 증가세에 있는 데이터 유출로 인한 피해를 감소시키는 가장 효과적인 방법으로 제시되고 있으며 이로 인해 전문역량을 보유한 정보보호 인력을 확보하고 관리하는 것이 중요해지고 있다(Ponemon Institute, 2018).

우리나라는 전자정부 수출국이면서 지능정보기술을 기반으로 하는 첨단기술의 각축장임을 자부하는 정보통신 강국이다. 그러나 국가 안보상의 이유와 정보통신 역기능으로 인해 국가와 국민 모두가 일상적으로 사이버 위협에 노출되어 있다. 2013년 6월에는 어나니머스코리아가 청와대 공식 홈페이지를 해킹, 새누리당 당원, 청와대 인사, 군장병, 주한미군 등 신상정보가 담긴 링크주소를 게시한 바 있고(SBS 뉴스, 2013. 06. 26.), 2016년 12월에는 군이 운영하는 내부망이 해킹에 의해 뚫린 사실이 공개된 바 있다(IT World, 2016. 12. 07.). 정부를 대상으로 한 개인정보 유출 및 해킹사고가 빈번해지고 있는 현재 행정안전부는 사이버보안은 4차 산업혁명의 성장을 뒷받침하는 핵심 분야이며 사물인터넷, 빅데이터 등의 ICT 지능기술의 확산에 기인하여 지능화·대형화되고 있는 사이버보안 위협에 대해 행정기관이 먼저 적극 대응할 수 있어야 한다고 강조하고 있다(행정안전부, 2017. 11. 02.).

행정기관은 국민생활의 접점으로서 국가 주요기반시설과 전자정부서비스 대상 사이버 공격에 대응하기 위해 관계기관과 상호 긴밀히 공조하여 사전예방과 대응을 강화해 나가야 하는 의무가 있다. 그럼에도 불구하고 여러 한계로 인해 국가 정보화 및 정보보호 수준에 부응하지 못하고 있는 것으로 평가받고 있다. 원인은 다양하겠으나, 감사원(2016)은 국가 사이버안전 관리 실태 감사보고서를 통해 내부재배치로 정보보호 업무를 담당하게 된 인력의 68%가 정보보호 관련 이력이 없는 인력이라는 점을 들어 담당인력의 전문성이 낮아 적절한 대응 및 조치가 어려운 것을 지적한 바 있다.

민간 정보보호 전문업체에서 종사하는 정보보호 인력은 해당 업체의 정보보호 제품 및 서비스의 개발이나 판매와 관련된 업무를 수행한다. 정보보호 업무를 수행하지만 궁극적으로 정보보호 실현이 아니라 경영목표 달성을 목표로 한다. 금융·통신 등의 일반업체들은 자사의 정보보호 목표와 보유자산의 범주에 적합한 수준의 정보보호 대책을 수립하고 전담조직과 전담인력을 직접 채용하거나 아웃소싱하여 대응한다. 그러나 행정기관이나 중소기업은 일반업체에 비해 숙련도가 낮고 저임금을 불사하고 입사하는 인력에 의존해야 하는 형편이기에 인력관리에 근원적인 어려움을 겪게 된다. 더욱이 기술적인 정보보호를 대부분 아웃소싱하는 행정기관의 정보보호 담당인력은 민간업체 종사인력에 비해 기술 지식과 전문성은 상대적으로 낮아도 되지만 그만큼 재교육의 기회와 필요성도 적어 경력개발은 쉽지 않은 반면 법률과 각종 규정 준수와 국가의 정보보호 실현이라는 막강한 책무를 맡고 있어 연중 각종 감사 및 실태평가에 대응하기에도 여력이 없어 인력관리에 불균형이 발생하고 있다.

또한 행정기관은 정보보호 제품 및 서비스의 수요자의 입장이기 때문에 공급자인 정보보호 전문업체가 수행하는 정보보호 직무와 명칭은 같다고 하더라도 요구되는 전문성과 직무수준이 다르다. 산업현장에서 직무를 수행하기 위해 요구되는 지식·기술·태도 등의 내용을 국가가 체계화한 국가직무

능력표준(National Competency Standard, NCS)에서 정보보호 직무는 보안 엔지니어링, 정보보호 관리·운영, 정보보호 진단·분석, 보안사고 분석 대응, 정보보호 암호·인증, 지능형영상정보처리 6개이다(국가직무능력표준). 이 중 업무내용과 수준면에서 행정기관 정보보호 업무와 가장 유사한 직무는 정보보호 관리·운영 정도이다. 또한 정보보호 분야 직무를 전략 및 기획, 마케팅 및 영업, 연구개발 및 구현, 교육 및 훈련, 관리 및 운영, 사고 대응, 평가 및 인증 7개로 분류한 전효정 등(2009)의 연구와 비교해서도 전략 및 기획과 가장 유사하다. 행정기관 정보보호 업무에서의 사고대응, 관리 및 운영 등은 국가직무능력표준 및 정보보호 분야 직무체계와 직무군의 명칭은 유사하더라도 요구되는 직무수준과 직무내용이 확연히 다르다. 그 이유는 국가직무능력표준 및 정보보호 분야 직무체계는 기본적으로 정보보호 제품 및 서비스의 공급자 즉 민간업체의 입장에서 개발된 것이기 때문이다. 따라서 수요자의 입장인 행정기관의 직무내용과는 괴리가 발생할 수밖에 없다. 결과적으로 행정기관 정보보호 인력의 업무범위와 직무내용에 적합한 경력개발과 인력관리를 위한 기준은 사실상 없는 상황이다.

행정기관의 정보보호 수준을 높이기 위해서는 관리체계가 잘 수립되어 있어야 한다. 관리체계의 핵심 구성요소는 보안규정, 전담조직, 담당인력이다. 정보보호 업무가 명확히 정의될수록 관리체계의 수립은 수월해진다. 본 논문에서는 행정기관 정보보호 전담조직 및 담당인력에 할당된 업무분장내역을 조사·분석하여 행정기관 정보보호 업무를 3개로 분류하였다. 또한 국내 행정기관에서 정보보호 업무를 담당하고 있는 인력을 대상으로 설문조사를 실시하여, 종사하고 있는 기관이나 현재의 직급에 대한 정보가 아닌, 개인별 전문성을 판단할 수 있는 정보인 현재업무, 최종전공, 채용형태, 업무소요지식별 숙련된 정도와 재교육 필요정도 등을 조사·분석하여, 행정기관 정보보호 업무의 특징을 고려한 정보보호 전담인력 관리방안을 제시하고자 하였다.

2. 이론적 배경

행정기관의 정보보호 담당자들의 직무이동 및 경력개발이 민간업체 재직자들과 다른 가장 큰 특징 중 하나는 경력개발 시도가 자발적 동기에 의해서가 아니라 내부재배치에 의한 직무순환 원칙에 의한 비자발적 직무이동에 의해 이루어지는 경우가 많다는 것이다. 또한 조직특성으로 인해 행정기관 정보보호 역량이 낮은 주요인으로 정보보호 담당자들의 수동적인 업무태도가 꼽히고 있으며(노진우, 서진완, 2016), 공무원의 특성상 직장이동이 거의 없기 때문에 능력향상을 위한 내부적인 교육훈련이 매우 중요하다는 지적도 있다(조선일, 2006; 최무현, 김영우, 2010). 따라서 행정기관 정보보호 담당인력 관리는 민간업체와는 목적과 방안 자체가 달라져야 한다.

조선일(2006)은 직업공무원제로 인해 이직률이 낮아 공공 부문 종사자들의 능력개발이 매우 중요하다고 지적하면서, 문헌분석과 공무원 대상 인터뷰 등을 통해 업무수행에 필요한 능력요소들을 도출하였다. 또한 공무원 대상 설문조사를 통해 능력요소별로 상급자와 하급자 간의 현재 중요도와 교육 필요성 면에서의 인식차이를 분석하여 직종별·직급별로 필요한 능력요소와 필요 교과목을 제시하였다. 이미정, 이선중(2010)은 광역자치단체 종사자들을 대상으로 정보보호에 대한 인식과 행태의 차이를 분석하였다. 또한 조직문화로서의 정보보호와 관련된 선행연구를 분석하여 광역자치단체의 정보보호 수준을 평가하기 위한 프레임워크를 구성하였으며, 프레임워크를 기반으로 설문지를 개발하여 조사를 진행하였다. 프레임워크는 측정영역과 측정수준에 따라서 개인, 조직내부, 조직외부의 정보보호에 대한 인식을 평가하는 항목들로 설정되었다. 결론적으로 기술적·관리적·제도적 정보보호에 대한 조직원들의 이해도는 높았지만 실제 실행력은 낮은 것으로 분석되었고, 이의 해결을 위해서는 공무원 대상 교육프로그램의 개발 과정에서 정보보호 지식전달 뿐만 아니라 실제 실천까지 고려하여야 한다고 제안하였다. 최무현, 김영우(2010)은 공무원

의 특성상 인력이동이 거의 없기 때문에 공무원 개개인의 능력향상을 위한 교육훈련체계의 구축이 매우 중요하다고 하였으며, 지방공무원 교육훈련 및 관련 예산 현황을 조사하고 문제점을 도출하였다. 근본적인 원인 분석과 해결대안 도출을 위해 국장급 이상의 지방공무원을 대상으로 FGI(Focus Group Interview)를 실시하고 역량기반의 지방공무원 교육훈련 방안을 도출하였으며, 병행하여 일반 공무원을 대상으로도 설문조사를 실시하여 현재의 기본역량을 분석하고 적절한 교육훈련을 도출하였다. 박태형 등(2010)은 공공부문 성과관리를 위해서는 정보보호 업무를 수행하는 인력에 대한 교육의 효율성이 필요하다고 보고, 자료포락분석 기법을 이용하여 36개 공공부문 정보보호 담당부서의 정보보호 관련 교육업무의 효율성을 평가하였다. 이를 통해 공공부문 담당조직의 교육업무의 효율성 개선을 위해 내부직원들이 내부 또는 외부 직무교육에 자주 참여할 수 있는 기반이 마련되어야 한다고 하였다. 김동욱, 성욱준(2012)은 공공부문 정보보호 전문인력의 직군이탈에 영향을 주는 요인은 무엇인가라는 연구문제를 실증하기 위해 5개의 연구가설을 설정하고, 정보보호 담당 공무원과의 인터뷰 및 설문조사 등을 통해 직군이탈에 영향을 미치는 요인들을 도출하여 회귀분석 하였다. 결과적으로는 직무 스트레스와 정보보호 전담부서의 부재가 정보보호 전문인력의 직군이탈의도에 가장 많은 영향을 주는 것으로 나타났으며, 이를 해결함으로써 공공기관의 정보보호 수준을 높일 수 있을 것이라고 제안하였다. 이은주 등(2014)는 국내 교육기관 종사자들의 소속기관 유형, 근무지역, 담당직무별로 요구되는 정보보호 지식 및 기술에 차이가 있는지를 분석하기 위해 교육기관 정보보호 담당자들을 대상으로 설문조사를 실시하여 다차원척도법(MDS) 분석을 통해 정보보호 교육 프레임워크를 제시하였다. 강찬우, 박태형(2014)는 지방자치단체 정보보호 업무담당자들을 대상으로 설문조사를 통해 정보보호 직무분석을 수행하고, 지방자치단체의 정보보호 적정 인력을 산출하였으며 정보보호 직렬 신설 등의 전문인력 확보방안을 제시하였다. 박기관, 홍관웅(2014)는 강원도 인재개발원 교육이수자를 대상으로 설문조사를 통해 교육 프로그램과 교육효과 간의 관계를 분석하고 교육이수자들의 직렬, 직급, 담당여부 등의 특성을 반영한 차별화된 교육과정의 설계가 필요하며 강의식교육보다는 토론식교육이 적절하다고 제안하였다. 이홍재, 차용진(2015)는 최근 1년간 개인정보보호 교육에 참여한 경험이 있는 지방자치단체 공무원을 대상으로 설문조사를 통해 개인정보보호 교육운영의 개선방안을 도출하였다. CIPP(Context, Input, Process, Product) 모형을 기반으로 연구모형을 설정하고 연구가설을 도출하여 설문조사를 통해 실증하였으며, 개인정보보호 교육운영에 있어 기관장의 관심이 조절효과를 갖는다는 것을 검증하였다. 이홍재 등(2016)은 Kirkpatrick 모형을 통해 공무원 대상 개인정보보호 교육과정의 교육효과를 분석하였다. 모형의 기본구성을 Krikpatrick 분석 프로세스에 따라 구성하여 개인정보보호 교육효과 분석모형을 설정하였으며 구조방정식 형태로 설문지를 구성하여 조사하였다. 분석모형에 포함된 개인정보보호 교육효과 측정모형 및 지표의 검증을 위해 이홍재, 차용진(2015)의 설문조사 자료를 재활용하였다. 윤주범(2016)은 공공을 대상으로 하는 사이버위협에 대한 기술적인 대응도 중요하지만 담당인력에 대한 교육을 통한 보안의식 고취 및 보안 전문지식 향상을 통해 보안수준을 높이는 것이 중요하다고 하였다. 국내 국가·공공기관 정보보호 담당자 200명을 대상으로 설문조사를 실시하고 공공 분야 담당자들 대상의 보안효과 상승을 위한 커리큘럼을 제안하였다.

이처럼 행정기관 종사인력을 대상으로 교육 및 관리방안 수립을 위한 다수의 연구가 진행되어 왔다. 그러나 많은 연구가 다년간의 행정조치와 다부처 협력이 필요한 정보보호 담당인력의 관리방안 수립보다는 업무역량 향상을 위해 필요한 교육방안을 제시하는 데에 초점을 맞추고 있다. 또한 조사대상자를 행정기관이나 공공기관 종사인력으로 하면서 인력 자체에 초점을 맞추기 보다는 행정기관 및 공무원 조직이라는 조직적 특성에 주안점을 두고 분석하고 있다.

3. 조사 분석

3.1 업무분장내역 조사・분석

조사시점인 2017년 기준 국내 국가기관은 중앙행정기관 18부 5처 17청 등 40개(정부 24, 2017), 특별지방국가행정기관은 제외하고 지방행정기관(보통지방행정기관, 지방자치단체) 중 시・군・구 단위 260개(행정안전부, 2017), 공공기관 332개이다(기획재정부, 2017). 본 논문에서는 각 기관의 공식 홈페이지를 방문하여 조직도를 확인하고 공개된 정보화 및 정보보호 전담부서와 소속인력의 업무분장 내역을 수집・정리하였다. 중앙행정기관 중 국가 안보상 조직도 및 소속인력을 비공개로 하고 있는 몇 개 기관은 제외하였다. 지방행정기관 중 군・구 단위는 제외하였다. 공공기관은 대부분 공식 홈페이지에 조직도 및 업무분장 내역을 상세히 공개하고 있지 않아 조사는 진행하였으나 업무분장내역 분석에서는 제외하였다.

조직도와 업무분장내역을 기준으로 정보보호 담당인력에게 배정된 업무임에도 정보보호나 정보보안과 관련성이 낮은 업무는 일반 정보화 업무 및 보안과 관계없는 일상적인 행정업무로 취급하여 제외하였다. 대표적인 제외된 업무명은 일반서무, 영상회의시스템 운영・관리, 전화망 운영・관리, 문서수발, 나라e음 운영・관리, 국회업무 대응, 부서장이 아니면서 총괄로 단순 명시된 경우이다.

정보보호 및 정보보안 관련 업무의 범주는 관련 법률 및 규정을 참조하였다. 국가정보화 기본법(법률 15369) 기준 공공・행정기관 정보보호 담당자들의 주요 업무는 정보보호 시책 마련, 개인정보 보호 시책 마련, 건전한 정보통신윤리 확립이다. 정보통신기반 보호법(법률 15376) 기준 주요 업무는 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책 수립・시행, 주요정보통신기반시설의 보호 및 침해사고의 대응이다. 또한 국가사이버안전관리규정(대통령훈령 316)과 보안업무규정(대통령령 26140)에 의거하여 임명되어야 하는 정보보안담당관이 수행하여야 하는 정보보안 역할은 정보보안 정책 및 기본계획 수립・시행, 정보통신망 보호대책 수립・시행, 사이버공격 관련 정보 수집・분석 및 보안관제, 사이버침해사고 대응・복구, 정보보안 관련규정・지침 등 제・개정, 정보보안 감사・지도점검 실시, 정보보안 교육계획 수립・시행, 정보보안업무 심사분석 시행, 정보보안 예산 및 전문인력 확보, 정보보안 위규 적발 강화 및 사고조사 처리이다. 행정기관 정보보호 업무분장내역을 종합하여 정리하면 <표 1>과 같다.

〈표 1〉 행정기관 정보보호 담당부서 소속인력의 정보보호 관련 업무분장내역 분석 결과

구분		합계	중앙행정기관	지방행정기관
정보보안 관리 66.5%	개인정보보호	20.5%	22.9%	20.1%
	총 괄	3.0%	6.5%	2.4%
	정보보안	8.8%	19.0%	7.2%
	ISMS	0.2%	-	0.3%
	사이버보안 진단의 날	1.6%	-	1.9%
	전자서명 관리	4.7%	4.3%	4.8%
	정보보안 평가	4.0%	6.1%	3.7%
	정보보호 교육	3.3%	2.2%	3.5%
	정보보호 정책	1.6%	2.2%	1.5%
	용역업체 관리	0.5%	0.9%	0.4%
	CCTV	6.0%	-	7.0%
	USB보안	2.2%	1.3%	2.3%
	보안성 검토	4.4%	1.7%	4.8%
	보안자재	2.2%	1.3%	2.4%
	재난재해복구	1.6%	2.6%	1.5%
	출입통제	0.2%	-	0.3%
	국제협력	0.2%	1.3%	-
	기술개발	0.1%	0.4%	-
	기타	3.1%	2.7%	1.1%
네트워크 및 전산보안 18.3%	네트워크 보안	6.7%	2.6%	7.3%
	보안 취약점 관리	0.7%	0.9%	0.7%
	시스템 보안	7.1%	2.2%	7.9%
	전산보안	1.6%	1.3%	1.7%
	홈페이지 보안	2.2%	0.9%	2.4%
보호 및 대응 15.2%	PC보안	2.3%	0.4%	2.6%
	유해사이트 차단	0.5%	-	0.5%
	자료유출방지	0.3%	0.9%	0.2%
	기반시설보호	1.3%	1.3%	1.3%
	보안관제	4.7%	2.6%	5.1%
	사이버 침해 대응	6.0%	11.7%	5.2%

조사 과정에서 도출한 행정기관 정보보호 담당부서 소속인력의 정보보호 업무의 특징을 살펴보면 다음과 같다. 첫째, 일반 정보화 업무와 정보보호 업무를 완전히 분리하기 어렵다. 한 명의 인력에게 정보보호 업무 전체가 집중된 경우도 있으며 한 명이 정보화 업무와 정보보호 업무를 모두 수행하는 경우도 있다. 일례로 정보시스템 구축·관리를 위한 정보자원관리(HW, SW, 전산장비, 통신망, IP 등), 정보기술아키텍쳐 관리·운영 등의 업무가 정보보호 담당인력에게 보안업무와 함께 배정되어 있는 경우이다. 둘째, 전문적인 정보보호 지식 및 기술을 요하는 특징적인 보안업무의 비중이 적다. 즉 고도의 기술적 능력을 요하는 업무의 비중이 적다. 일례로 새올행정시스템, 통합정보자원관리시스템(지킴-e), 온-나라 및 문서유통시스템(중앙부처 및 자치단체 간 업무관리시스템), 공공데이터 공개 및 이용 등이 정보보호 업무로 자주 등장하는데 반해 취약점 분석, 사고대응, 보안관제 등은 거의 등장하지 않는다. 셋째, 지방은 CCTV를 이용한 통합도시관제 업무의 비중이 높은데 반해 중앙행정기관 정보보호 업무분장내역에 등장하지 않는다. 넷째, 업무분장내역이 총괄, 정보보안 담당, 정보보안, 정보보안 담당관 등으로 포괄적으로만 명시되어 있어 상세 업무내역을 알 수 없는 경우가 많다. 이는 중앙행정기관에서의 비율이 상대적으로 높은데, 보안상의 이유로 기관의 보안업무내역을 노출하지 않기 위한 보안정책 탓으로 돌리더라도 포괄적인 업무정의는 전문적인 업무 수행을 어렵게 할 수도 있다.

3.2 업무소요지식에 대한 숙련정도 및 재교육 수요

앞서 업무분장내역 조사·분석을 통해 행정기관 정보보호 담당자들의 업무를 정보보안 관리, 네트워크 및 전산보안, 보호 및 대응으로 분류하였다. 본 논문에서는 정보보호 담당자들의 현재업무를 3대 분류를 기준으로 묻고, 현재업무를 수행하는데 있어 주요 업무소요지식에 대한 숙련된 정도와 재교육 필요정도를 조사하였다. 응답의 편의성을 제공하기 위해 업무소요지식은 Jun and Kim(2018)에서 정의한 14개 정보보호 분야 업무소요지식을 제시하였다.

설문조사는 2017년 9월부터 11월까지 국내 행정기관 정보보호 담당자들을 대상으로 진행하였으며, 불성실 응답을 제외하고 191부를 정리하였다. 최종적으로 소속기관이 중앙 및 지방 행정기관인 109부만을 분석에 활용하였으며, 행정기관 중에서도 국가안보 관련 기관이나 통합보안관제센터 등은 포함되지 않았다.

응답자 기본사항은 <표 2>와 같다. 응답자의 성별은 남성 76.1%, 여성 23.9%이다. 나이는 40대 33.8%, 30대 31.2% 순이다. 최종전공은 전산계열 29.4%, 전기·전자·컴퓨터계열 25.7%, 정보보호·정보통신계열 20.2%, 기타 24.8%이다. 채용형태는 내부재배치에 의해 정보보호 업무를 담당하게 된 경우가 75.2%, 정보보호 전담으로 신규 채용된 경우가 34.8%이다. 현재업무는 정보보안 관리 56.9%, 네트워크 및 전산보안 22.9%, 보호 및 방어 20.2%이다.

〈표 2〉 응답자 기본사항

성별	남성	76.1%	여성	23.9%
나이	20세~29세	30세~39세	40세~49세	50세 이상
	5.5%	31.2%	33.0%	30.3%
최종전공	전산계열	전기·전자·컴퓨터계열	정보통신·정보보호계열	기타
	29.4%	25.7%	20.2%	24.8%
채용형태	신규 채용 (신입직)	신규 채용 (경력직)	내부 재배치	
	11.0%	13.8%	75.2%	
분장업무 (R&R)	정보보안 관리	네트워크 및 전산 보안	보호 및 방어	
	56.9%	22.9%	20.2%	

변수 간에 유의적인 관련성을 분석하기 위해 카이제곱 분석(Chi-Square Test)을 실시하였다. 그 결과 응답자의 현재업무와 최종전공 간에는 분포의 차이가 없는 것으로 밝혀졌다(유의확률 0.307). 반면 현재업무와 채용형태 간에는 분포의 차이가 있는 것으로 밝혀졌으며(유의확률 0.003($p < 0.05$)), 기대빈도 5보다 작은 셀은 하나도 없는 것으로 나타났으므로 이 결과는 신뢰할 수 있다(<표 3> 참조). 또한 최종전공과 채용형태 간에는 분포의 차이가 없는 것으로 밝혀졌다(유의확률 0.195). 직접적으로 최종전공, 채용형태, 현재업무 간의 영향 관계나 영향의 방향성을 확인하기 위해서는 보다 세분화된 추가 조사가 필요하겠으나, 이들 간에 유의한 관계가 있음은 확인할 수 있다.

현재 담당업무, 최종전공, 채용형태에 따라 업무소요지식에 대한 숙련된 정도와 재교육 필요 정도에 차이가 있는지 분석하기 위해 다변량검정(MANOVA, Multivariate Analysis of Variance)을 실시하였다. 종속변수가 2개이므로 각각 일변량분석(ANOVA, Analysis of Variance)을 실시하여 비교할 수도 있지만, MANOVA를 통해 종속변수간 상관관계가 높을 경우 ANOVA로는 밝힐 수 없는 결합된 차이를 밝혀낼 수 있으며 ANOVA를 여러 번 사용하면 1종오류(귀무가설이 참이지만 그 가설을 기각하게 되는 오류) 확률이 커질 수 있는데 이 확률도 줄일 수 있다(Keller, 2007; 송지준, 2013).

현재업무(그룹 3개)에 따라 업무소요지식에 대한 숙련된 정도가 다르다($p = 0.568$)와 재교육 필요 정도가 다르다($p = 0.912$), 최종전공(그룹 4개)에 따라 업무소요지식에 대한 숙련된 정도가 다르다($p = 210$)와 재교육 필요 정도가 다르다($p = 0.564$) 모두 유의한 차이가 확인되지 않았다. 채용형태(그룹 3개)에 따라 업무소요지식에 대한 숙련된 정도가 다르다($p = 0.016^{**} < 0.05$)에 대해서만 유의한 차이가 확인되었으며 역시 재교육 필요 정도가 다르다($p = 0.132$)는 유의한 차이가 확인되지 않았다(<표 4> 참조).

〈표 3〉 카이제곱검정

종속변수 \ 독립변수			채용형태		X^2/p
			신규 채용	내부 재배치	
분장업무 (R&R)	정보보안 관리	Count(%)	8(7.3%)	54(49.5%)	11.428/ 0.003**
		Expected Count	15.4	46.6	
	네트워크 및 전산 보안	Count(%)	9(8.3%)	16(14.7%)	
		Expected Count	6.2	18.8	
	보호 및 방어	Count(%)	10(9.2%)	12(11.0%)	
		Expected Count	5.4	16.6	
합 계			24.8%	75.2%	

0 cells (0.0%) have expected count less than 5. The minimum expected count is 5.45.
**$p < 0.01$.

〈표 4〉 MANOVA

		평균	표준편차	F/Sig.	사후검정
Skilled Level	신규 채용(신입직)	2.29	.66395	4.313/0.016*	a > b (Scheffe)
	신규 채용(경력직)	2.97	.52654		
	내부 재배치	2.59	.61235		
Retraining Needs	신규 채용(신입직)	3.20	.73037	2.066/0.132	-
	신규 채용(경력직)	2.88	.52792		
	내부 재배치	3.29	.73883		

*$p < 0.05$, **$p < 0.01$, ***$p < 0.001$.

3.3 분석 결과의 시사점

연구문제를 실증하기 위해 본 논문에서는 현재 행정기관 정보보호 전담부서에 할당된 정보보호 업무분장내역을 조사·분석하고, 행정기관 정보보호 업무를 정보보안 관리, 네트워크 및 전산보안, 보호 및 대응 3개로 분류하였다. 또한 실제 행정기관 정보보호 담당자들을 대상으로 설문조사를 실시하여 현재업무, 최종전공, 채용형태와 현재 담당업무 수행에 필요한 업무소요지식에 대한 숙련된 정도와 재교육 필요 정도에 대한 데이터를 수집·분석하였다.

업무분장내역 조사 결과, 행정기관 정보보호 업무는 일반 정보화 업무와 분리가 어렵고 상대적으로 기술 전문성을 요구하는 보안업무의 비중이 적으며 한명에게 정보보안 총괄로 업무가 일괄 분장되거나 정보화, 네트워크 관리, 서버 관리, 정보보호, 개인정보보호가 모두 분장되는 등의 경우가 많아 업무 전문성을 확보하기 어려운 상황임을 확인하였다. 또한 설문조사 분석 결과에서도 행정기관 정보보호 담당인력의 현재업무와 최종전공, 최종전공과 채용형태 간에는 분포의 차이가 없는 것으로 밝혀졌으며, 현재업무와 채용형태 간에만 분포의 차이가 있는 것으로 밝혀졌다. 현재업무를 담당하는 과정에서 신규 채용되는 인력과 내부 재배치되는 인력 간에 차이가 있을 수 있는 것으로 분석된다. 또한 업무소요지식에 대한 숙련된 정도와 재교육 필요 정도에 있어서도 현재업무와 최종전공을 기준으로는 그룹 간에 차이가 확인되지 않았고, 숙련된 정도에 있어서만 채용형태 그룹 간에 유의한 차이가 확인되었다. 즉 국내 행정기관 정보보호 전담인력의 경우 순환보직으로 맡은 업무에 대한 전문성을 키우기 어려운 조건에 있지만, 정보보호 전담으로 신규 채용되어 행정기관으로 진입하는 인력의 경우 업무전문성을 요구하는 보안업무 전담을 위해 채용된다는 점에서 보유한 업무소요지식에 대한 숙련 정도에 차이가 있다고 기대하는 것으로 분석된다. 따라서 현재업무 또는 최종전공이 무엇이냐에 따라서는 요구되는 또는 보유한 업무 전문성에 차이가 없을 수 있지만, 채용형태 즉 정보보호 업무전담으로 신규 채용되었는가와 내부 재배치되었는가에 따라서는 보유한 업무 전문성에 차이가 있을 수 있음을 시사한다.

감사원(2016)의 감사결과와 본 조사결과에서 행정기관의 정보보호 전담인력의 70% 이상이 내부 재배치로 업무를 맡게 되고 이탈율도 매우 낮은 것으로 확인됐다. 현재업무를 맡게 된 경로가 본인의 의지나 개인적인 경력개발 시도에 의해서가 아님을 시사한다. 이로 인해 채용형태가 정보보호 전담으로 신규 채용되었는가와 내부 재배치되었는가에 따라 업무 전문성에 차이가 있을 수 있는 것으로 보인다. 일반적으로 재직자들의 경력개발 활동은 직장이동이나 직무이동을 전제로 이루어지는데(Sicherman and Galor, 1990; Shelton, 2013), 여러 논문들에서 지적된 바와 같이 행정기관 종사 인력 즉 공무원들의 직장이동은 거의 없는데다가 현재업무에 대한 관심과 전문성이 낮으니, 경력개발 목표가 불명확하고 적극적인 활동도 하지 않는 상황이 반복되면 행정기관 정보보호 업무의 전문성은 지속적으로 낮아질 수밖에 없다.

그러나 채용형태에 따른 숙련된 정도에서 유의한 차이가 확인됨에 따라, 정보보호 전담으로 신규 채용된 인력과 내부 재배치된 인력 간에 보유한 업무전문성이 다르다는 점을 기반으로 행정기관 정보보호 인력관리 방안을 도출하고자 한다.

4. 인력관리 방안

정보보호 담당인력은 다른 업무와는 달리 전문적인 직무교육이 요구된다. 현재 기본적으로 국가정보원의 정보보안 관리실태 평가에서 요구하는 정보보안 담당자들의 정보보호 관련 의무 교육시수는 연간 40시간이다. 행정기관 정보보호 담당인력을 대상으로 많은 연구가 진행되어 왔지만, 대체적으로 직급 또는 관리자·실무자 등으로 교육대상을 분리하고 공무원이라는 특성을 고려한 교육

방안을 제시하는 데에 중점을 두고 있다. 그러나 정보보호 담당인력에 대한 교육 및 관리방안은 직급구분이나 조직특성에 의해서가 아니라 정보보호 업무 특징과 요구되는 업무 전문성을 반영할 수 있는 담당자들의 개인특성을 고려하여 수립되어야 한다.

조사·분석 결과와 현재 국내 행정기관 정보보호 관리 현황을 기반으로 정보보호 전담인력의 교육 및 관리방안을 제안하면 다음과 같다. 첫째, 국내 행정기관의 정보보호 인력들이 내부재배치로 업무를 맡게 되는 경우가 70% 이상임을 고려할 때, 모두에게 연 40시간이라는 공통적인 교육이수 조건을 제시하는 것으로 전체적인 업무 전문성의 향상을 기대하기는 어렵다. 정보보호 전담으로 신규 채용한 인력에 대해서는 별도로 다년간에 걸쳐 연계된 교육훈련을 받을 수 있도록 하여 업무전문성 강화를 도모하고, 내부 재배치된 인력은 업무에 대한 관심도와 전문성을 고려하여 단기 이론교육 위주로 받도록 하여 지식의 최신성과 지속성을 유지하는 방향으로 하여야 한다. 이를 위해서는 공무원인재개발원, 사이버보안인재센터, 사이버안전훈련센터, 정보보호교육센터 등의 정보보호 교육과정이 교육대상을 특정할 수 있도록 과정을 등급화(예: 일반, 심화, 전문)하고 최소 3년의 중기교육로드맵 형태로 제시되어야 한다. 현재 각 기관은 연 초에 해당 년도 교육과정 운영계획을 공개하고 있으며, 아직까지는 교육과정 간 선후관계를 명확하게 제시하거나 다년간에 걸쳐 연계하여 수강하여야 하는 교육과정은 없다. 현재의 교육과정 개설·운영은 각 기관별로 인적·물적 자원을 고려한 최선의 결과물이겠으나, 중장기적인 교육효과의 향상보다는 단기적인 수요대응에 치중하고 있는 것으로 보인다.

둘째, 정보보호 전담으로 채용된 신규인력을 포함하여 내부 재배치된 인력 중에서도 심화과정 이상의 재교육 과정을 이수한 정보보호 인력은 별도로 관리하고 타부서나 정보보호 이외의 업무에 배치되는 것을 최대한 배제하여 전문성을 키울 수 있도록 하여야 한다. 일례로 감사원(2016)은 2011년부터 2015년까지 22개 중앙 부처에서 충원한 정보보호 전담인력(정보보호 분야 자격증·학위 보유 또는 2년 이상 정보보호 분야 근무경력 보유) 중 34.1%가 순환보직제로 2015년 8월 말 현재 정보보안 담당부서가 아닌 부서에 근무하고 있거나 정보보안 업무와 다른 업무를 병행하여 수행하고 있다고 지적한 바 있다. 전문성 강화를 위해서는 별도의 정보보호 전담조직을 편성하여 운영하는 것도 중요하지만 전담인력이 군더더기 없이 정보보호 업무를 전담할 수 있도록 함으로써 전문성을 키울 수 있는 환경을 구축하는 것이 무엇보다도 절실하다. 다부처간 협의와 예산 마련이 우선이겠으나 정보보호 전담인력의 관리를 위해 행정안전부나 과학기술정보통신부 주관으로 행정기관 정보보호 전문인력등급제를 도입하여 별도로 관리할 수 있는 제도의 도입이 필요하다.

셋째, 행정기관이 갖는 지역별 정보보호 업무의 중요도와 관련 정보자원에는 많은 차이가 있기 때문에 전체 기관을 대상으로 일률적인 조치를 취하는 것은 어렵다. 정보보호 담당인력의 경우에도 규모가 작은 기관이나 지방 소도시 기관으로 갈수록 대체인력이 없어 직무교육으로 인한 공백을 메울 수 없는 경우가 빈번히 발생한다. 이를 위한 방안의 하나가 지역 소재의 행정기관, 공공기관, 일반업체 등의 정보보호 담당자 협력체인 지역정보보호협의체를 구성·운영하는 것이다. 전문적인 업무지식이나 교육경험을 공유할 수 있으며 나아가 취약점 정보까지 실시간으로 공유할 수 있어 정보소외에서도 벗어날 수도 있으므로, 당장 추가적인 인력충원이나 장시간의 직무교육을 받지 못하더라도 업무 전문성 향상을 기대해 볼 수 있다.

국민생활의 접점이자 수많은 사이버 위협의 직접적인 타겟이 되는 행정기관이 보안의 취약고리가 된다면 국가의 근간이 흔들릴 수도 있다. 본 논문은 현재 국내 행정기관은 고도로 숙련된 정보보호 전담인력의 확보와 유지에 어려움이 있고 이를 해결할 수 있는 방안은 다른 업무 인력과는 달라야 한다는 데에서 출발하였고, 이를 실증하기 위해

노력하였다는 데에 의의가 있다. 그러나 몇 가지 한계점을 지닌다. 첫째 행정기관 정보보호 담당인력의 관리방안을 논의하기 위해 행정기관의 정보보호 업무분장내역을 분석하였으나 각 기관별로 비표준형태이면서 공개된 정도도 다르고 최신화의 정도도 다른 가공되지 않은 업무분장내역을 평균적인 자료로 가정하고 활용하였다. 그럼에도 불구하고 업무분장내역은 현재 업무를 파악하는 데에 중요한 기준이 되며, 나아가 해당 기관의 정보보호 업무의 중요도까지 파악할 수 있는 중요한 근거자료가 된다는 데에 의의가 있다. 향후에는 공공·행정기관의 실제 업무내역과 담당자별 분장내역을 조사하는 연구가 필요하다. 이러한 연구가 진행된다면 민간업체와는 다른 인력관리의 핵심인 공공·행정기관만의 정보보호 직무체계 표준을 개발할 수 있으며 표준 직무체계를 기반으로 선후관계가 명확한 체계적인 교육과정의 개발이 가능하며, 교육과정 개발에 필요한 정보보호 지식 및 기술의 정의까지 다양한 연구가 가능하다. 둘째 설문조사를 진행하였으나 주요 변수 간에 상관관계나 영향정도를 분석하기에는 한계가 있어 심도 있는 시사점을 제시하지 못하였다. 조사대상의 특성상 개인정보보호와 공무상비밀누설 등을 고려하여 설문지를 최소한으로 구성하였고 세부적인 업무내역, 경력이동사항, 경력개발시도 등에 대해 묻지 못했기 때문이다. 셋째 행정 및 공공기관 대상 정보보호 전문 교육과정에 입과한 수강생들을 대상으로 설문조사를 진행하였기 때문에 현재 소속기관이 행정기관이 아닌 대략 40%의 설문결과가 분석에서 제외되었다. 향후, 행정기관과 공공기관 및 기타(주로 교육기관) 간의 차이를 분석해 보는 시도도 필요할 것으로 보인다.

참고문헌

감사원, 국가 사이버안전 관리 실태 감사보고서, 2016.

강찬우, 박태형, “직무분석을 통한 지방자치단체 정보보호 적정인력 산출에 관한 연구”, *한국지역정보화학회지*, 제17권, 제3호, 2014, 175-197.

국가사이버안전관리규정, www.law.go.kr.

국가정보화 기본법, www.law.go.kr.

국가직무능력표준, www.ncs.go.kr.

기획재정부, 2017년 공공기관 지정현황, 2017.

김동욱, 성욱준, “공공부문 정보보호전문인력의 직군이탈의도에 관한 연구”, *사회과학연구*, 제28권, 제2호, 2012, 55-78.

노진우, 서진완, “지방자치단체의 정보보호 현황 및 인식의 변화 분석”, *정보화정책*, 제23권, 제1호, 2016, 20-37.

박기관, 홍관웅, “교육프로그램과 교육효과성 관계에 관한 실증적 분석”, *한국지방자치학회보*, 제26권, 제4호, 2014, 173-192.

박태형, 임종인, 문신용, “공공부문 정보보호 담당 조직의 교육업무 효율성 평가”, *한국지역정보화학회지*, 제13권, 제4호, 2010, 1-24.

보안업무규정, www.law.go.kr.

송지준, SPSS/AMOS 통계분석방법(개정증보판), 21세기사, 2013.

IT World, 대한민국 군 내부망 해킹 사건 개요와 분석, 2016. 12. 07.

SBS 뉴스, 어나니머스 “청와대 해킹 北 소행 증거 발견”, 2013. 06. 26.

윤주범, “공공분야 정보보안 역량 강화를 위한 단기 교육과정 연구”, *정보보호학회논문지*, 제26권, 제3호, 2016, 769-776.

이미정, 이선중, “지방공무원의 정보보호 인식 및 행태에 관한 연구”, *한국사회와 행정연구*, 제20권, 제4호, 2010, 453-478.

이은주, 전효정, 김태성, 김연복, “정보보호 담당자를 위한 업무교육 프레임워크 개발”, *한국콘텐츠학회논문지*, 제14권, 제1호, 2014, 386-399.

이홍재, 권준이, 차용진, “Kirkpatrick 모형을 적용한 공무원 교육효과 측정에 관한 연구”, *한국지역정보화학회지*, 제19권, 제1호, 2016, 165-189.

이홍재, 차용진, “CIPP 모형을 활용한 개인정보보호 교육의 효과성 연구”, *지방정부연구*, 제19권,

제1호, 2015, 95-119.

전효정, 김태성, “정보보호 업무인력의 경력개발을 위한 재교육 방향”, *Journal of Information Technology Applications & Management*, 제25권, 제4호, 2018, 67-77.

전효정, 김태성, 유진호, 지상호, “정보보호 분야 직무체계 개발”, *정보보호학회논문지*, 제19권, 제3호, 2009, 143-152.

정부 24, 정부조직도, 2017.

정보통신기반 보호법, www.law.go.kr.

조선일, “지방공무원 능력개발을 위한 교육수요분석”, *한국사회와 행정연구*, 제16권, 제4호, 2006, 165-187.

최무현, 김영우, “지방공무원 역량강화에 관한 연구”, *지방정부연구*, 제13권, 제4호, 2010, 33-59.

행정안전부, 지방자치단체 행정구역 및 인구 현황, 2017.

행정안전부 보도자료, “4차 산업혁명시대, 지자체 사이버보안 대응방안 모색”, 2017. 11. 02.

ITU, Global Cybersecurity Index, 2018.

ITU, ICT Development Index, 2017.

Keller, G., Statistics for Management and Economics (7th ed.), Thomson, 2007.

MS News, 2019(https://news.microsoft.com/ko-kr/2018/06/18/cybersecurity-report/; 2019. 3. 22. last visited).

Ponemon Istitute, 2018 Cost of a Data Breach Study, Global Overview, 2018.

Shelton, M., “Impact of Perceived Organizational Support on Cyber Security Practitioners’ Turnover Intentions”, Doctoral dissertation : Walden University, 2013.

Sicherman, N. and O. Galor, “A theory of career mobility”, *Journal of Political Economy*, Vol. 98, No.1, 1990, 169-192.

UN, E-government Readiness Index, 2018.

About the Authors

전 효 정 (phdhyo@naver.com)

충북대학교 경영정보학과에서 학사, 석사, 박사 학위를 취득하였다. 석사 학위 후 한국전자통신연구원 사업기획팀에서 근무하였으며, 박사 학위 후 현재 충북대학교 경영정보학과 글로컬 보안컨설팅 전문인력 양성사업단 박사후연구원으로 근무하고 있다. 주요 관심분야는 정보보호 인력 및 정책이다.

김 태 성 (kimts@cbnu.ac.kr)

한국과학기술원 경영과학과에서 박사를 취득하고, 한국전자통신연구원 정보통신기술경영연구소에서 근무한 후, 현재 충북대학교 경영정보학과에서 정교수로 재직하고 있으며, 정보보호특성화대학사업의 주임교수를 맡고 있다. University of North Carolina at Charlotte과 Arizona State University에서 Visiting Professor와 Visiting Scholar로 각각 근무하였다. 국내외 경영과학, 정보통신, 정보보호 관련 학술지 및 학술대회에서 논문을 발표하였으며, 주요 관심분야는 정보통신과 정보보호 분야의 경영 및 정책 의사결정이다.

No Image

박 기 태 (parkkt@nsr.re.kr)

한양대학교 전자컴퓨터전기제어공학부(학사), 한양대학교 컴퓨터공학과(석사), 한양대학교 컴퓨터공학과(박사), 현재 ETRI 부설연구소 책임연구원으로 재직 중이다. 주요 연구분야는 정보보호, 기계학습, 사이버보안 교육을 포함한다.