http://www.calsec.or.kr/jsebs
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.20, No.1, Feb. 2015, pp.201-215
http://dx.doi.org/10.7838/jsebs.2015.20.1.201

미래 융합환경 기반의 정보보호 직업군 설계

A Design on Information Security Occupational Classification for Future Convergence Environment

이윤수(Yunsoo Lee)*, 신용태(Yongtae Shin)**

초 록

정보화 시대를 넘어 융합의 시대로 나아감에 따라 고도화된 보안위협이 발생하고, 그에 따라 정보보호에 대한 필요성 및 중요성은 더욱 커져가고 있다. 그러나 그간의 국내 연구들은 정보보호 기술 직업군 위주의 단편적인 분류를 수행하고 있으며 미래 융합환경에 대한 고려가 부족한 실정이다. 따라서, 본 논문에서는 미래 융합환경에 대비한 정보보호 직업분류체계 및 필요역량을 설계하기 위해서 기존 정보보호 직업군 분류체계 및 직업군별 필요역량에 대한 선행연구 분석을 통해 정보보호 인력의 정의를 내린 후 직업군 분류를 실시하고 직업군별 필요역량을 도출하였다. 세부적으로 미래 융합환경에 대해 고려하여 정보보호 직업분류체계를 구성한 미국의 NICE(National Initiative for Cybersecurity Education)를 기반으로 하여 국내 실정에 적합한 형태로 직업군 및 직업군별 필요역량을 재분류하고 타당성을 검증하였다. 본 연구결과는 미래 융합환경에 적합한 정보보호 인력의 수급차 해소 및 처우개선을 위한 기초 자료로서 활용할 수 있을 것이다. 또한 향후 연구를 통해 정보보호 직업군별 필요역량을 이용하여 해당 직업군에 필요한 융합적인 직무역량을 습득할 수 있는 표준화된 교육 훈련 방법을 마련하는데 활용할 수 있을 것으로 기대된다.

ABSTRACT

Recently advanced security threats have increasingly occurred, and the necessity and importance of Information Security has been growing with the advent of the era of convergence beyond information-oriented age. Most domestic studies in the field of occupational classification of Information Security have only focused on technology-oriented occupations. Relatively little research has been carried out on the occupational classification in the view of convergence environment. Therefore, in this paper we gave a definition of Information Security occupations, classified them and draw required capabilities by occupations in order to design the occupational classification system of Information Security and the required capabilities for future convergence environment by analyzing the previous studies.

We also reclassified the occupational classification and required capabilities by occupations, and verified the validity of them based on National Initiative for Cybersecurity Education's the occupational classification system of Information Security considering the future convert-gence environment. It is expected that the results of this study will be employed as base data for manpower demand and supply and improvement of working conditions in the future convergence environments. In the future study we will build standardized instruction methods which provide occupational capabilities by using the required capabilities by occupations.

키워드 : 정보보호 직업, 정보보호 직업 분류체계, 정보보호 직업 역량, 융합환경
Information Security Occupation, Information Security Occupational Classification, Information Security Occupation Capability, Convergence Environment

* First Author, Korea Internet & Security Agency(myvipman@gmail.com)
** Corresponding Author, School of Computing, College of Information Science, Soongsil University (shin@ssu.ac.kr)
Received: 2015-01-30, Review completed: 2015-02-13, Accepted: 2015-02-19

1. 연구배경 및 필요성

정보화 시대에 들어서 인터넷 등 정보통신망의 급격한 발전에 따라 해킹이나 바이러스, 사이버 범죄 등의 각종 보안위협 역시 끊임없이 발전하고 있어 정보보호에 대한 필요성 및 중요성은 점점 커져가고 있으며 이에 따라 정보보호 인력에 대한 분류도 세분화되어 가고 있다[1~3]. 또한 최근에는 정보화 시대를 넘어 융합의 시대로 나아감에 따라 정보보호 인력 역시 미래 융합환경에 맞게 세분화 및 재분류되며 융합적인 직무역량을 필요로 하고 있다[4, 5].

그리고 이러한 미래융합 시대의 고도화된 보안위협이 발생함에 따라 정보보호와 관련된 각종 사건들이 사회적 이슈로 부각됨에 따라 정보보호 인력에 관한 사회적 관심이 급증하고 있다[10]. 그 중에서도 정보보호 인력은 양적 수급 차와 더불어 질적 수급 차가 보다 중요한 해결과제로 등장하고 있으며, 동시에 정보보호 인력의 처우개선을 위한 다양한 요구가 나타나고 있다. 현재 국내 정보보호 산업은 빠르게 발전하고 있지만 인력에 대한 정의, 직업분류 등 정보보호 인력의 처우개선에 관한 기준이 부재한 실정이다. 또한 정보보호 인력의 직업분류에 따른 필요역량 역시 구체화되어 있지 않아 정보보호 인력양성 시 직업군별로 효율적이며 차별화된 교육훈련에 어려움을 겪고 있다. 그러나 그간의 국내 연구들은 정보보호 기술 직업군 직무 위주의 단편적인 분류를 수행하고 있으며 미래 융합환경에 대한 고려가 부족한 실정이다.

따라서, 본 논문에서는 미래 융합환경에 대비한 정보보호 인력의 수급차 해소 및 처우개선을 위한 기초자료로 적합한 정보보호 직업분류체계 및 필요역량을 도출하고자 한다. 미래 융합환경에 대비한 정보보호 직업분류체계 및 필요역량을 설계하기 위해서 기존 정보보호 직업군 분류체계 및 직업군별 필요역량에 대한 선행연구 분석을 통해 정보보호 인력의 정의를 도출 및 직업군 분류를 실시하고 직업군별 필요역량을 도출하였다. 도출한 내용을 미래 융합환경에 대해 고려하여 정보보호 직무분류체계를 구성한 미국의 NICE(National Initiative for Cybersecurity Education)[11]를 기반으로 하여 국내 실정에 적합한 형태로 직업군 및 직업군별 필요역량을 재분류하고 타당성을 확보하기 위한 연구를 실시하였다.

2. 선행 연구

기존의 정보보호 직업분류체계 및 직업군별 필요 역량에 대한 내용을 분석하기 위해 선행연구조사를 실시하였으며, 먼저 기존에 국내의 정보보호 직업분류체계 및 직업군별 필요역량 연구는 어떻게 이루어져있는지에 대해 조사하였다.

Kim et al.[7]은 한국고용정보원에서 발표한 한국고용직업분류표[9]를 참고하여 정보보호의 관리적, 기술적, 물리적 직무와 관련된 직업을 도출하였으며 크게 ‘정보보호 관리자’, ‘정보보호 컨설턴트’, ‘정보보호 엔지니어’의 3가지로 정보보호 직무를 나누었다. ‘정보보호 관리자’ 직업군은 다시 ‘최고 정보보안 관리자’, ‘정보보안 관리자’, ‘IT보안 감시자/위험 관리자’로 세분화 되고, ‘정보보호 컨설턴트’ 직업

군은 'IT 보안 전문가', '개인정보보호 전문가'로 세분화 되었다. 마지막으로 '정보보호 엔지니어' 직업군은 '디지털 포렌식 전문가', 'IT 보안 기술자', 'IT 시스템 운영 및 유지전문가'로 세분화하여 총 8가지의 직업군으로 분류하였다. 또한 구분된 정보보호 직무에 따라 정보보호 관련 자격증 및 미국 IT 보안 필수 요구지식을 참고하여 직업군 별로 '정보시스템 전략경영', '정보보호관리/개인정보관리 기법', '운영체제 일반 및 보안' 등의 총 13가지의 필수요구지식을 도출하였다.

산업인력공단[6]에서는 정보보안 전문인력의 수요처인 기업과 공공분야에서 이루어지는 정보보안 직무분석을 수행하고, 해당 직무를 수행하기 위해 필요한 정보보안 이론과 실무지식을 도출하여 '개발자', '컴퓨터시스템 설계 및 분석가', '네트워크 시스템 개발자', '보안엔지니어', '보안 연구자', '암호알고리즘 연구원', '보안 아키텍트', '응용소프트웨어 개발자', '시스템 소프트웨어 개발자', '정보보안 프로그래머' 등 총 21가지의 정보보호 직업군으로 분류하고 해당 직무를 수행하기 위한 필요 지식 및 역량을 도출하였다.

다음으로, 기존 해외의 정보보호 직업군 분류체계 및 직업군별 필요역량 연구를 알아보기 위해서 두 가지의 선행연구조사를 실시하였다. Information Technology(IT) Security Essential Body of Knowledge(EBK)[12]에서는 정보보호 직업군을 'Chief Information Officer (CIO), 'Chief Risk Officer(CRO)', 'Certified Computer Examiner', 'Digital Forensics Analyst', 'Digital Forensics Engineer', 'Digital Forensics Practitioner', 'Digital Forensics Professional', 'Cyber Security Officer', 'Chief Information Security Officer(CISO)', 'Enterprise Security Officer' 등 총 51개의 직업군으로 분류하였고 다양한 측면의 전문가 양성 및 보안 인력의 선발 훈련 유지를 위한 표준 가이드라인으로 보안 실무자가 반드시 알고 시행해야 할 필수 지식 및 기술을 IT 보안 역량 분야 14개, IT 보안 역할 10개로 구성하여 IT 보안 필수요구지식 기준에 대한 프레임워크를 수립하였다.

National Initiative for Cybersecurity Education(NICE)[13]에서는 21세기 혁신적인 사이버 보안 교육, 훈련, 인식을 통해 경제적 번영과 안전한 국가 보안능력을 갖추고 미국 내 사이버 보안을 향상하는 것을 목적으로 'Security Provision', 'Protect and Defend, Investigate', 'Collect and Operate', 'Analyze', 'Operate and Maintain', 'Oversight and Development'의 7가지로 정보보호 직업군을 분류하였으며, 각 직업군별로 세분화하여 총 215개의 직업을 분류하였다. 또한 7가지 직업군별로 필요한 역량을 지식(Knowledge), 기술(Skill), 능력(Ability)의 3가지 역량으로 구분하여 제시하였다. 'Security Provision' 직업군에서 필요한 지식은 '접근 인증방법 관련 지식', '고객 조직에 적용되는 비즈니스 프로세스 및 운영에 관한 지식', '애플리케이션 취약점 관련 지식' 등으로 세분화되어있었으며, 필요한 기술은 '기밀성, 무결성, 가용성의 원칙을 적용하는 기술', '소프트웨어 디버깅 수행 기술', '식별된 보안 위험에 대한 대책을 설계하는 기술', 필요능력은 '클라이언트/서버 모델 관련 네트워크 프로그래밍 활용능력', '취약점 및 구성(형상) 데이터 분석 기반의 보안 문제 식별 능력', '고객의 요구 사항을 사이버 운영 현황으로 해석하고 변환 할 수 있는 능력'등

으로 세분화되어 있었다. 이러한 형식으로 총 7가지 직업군에 대하여 지식, 기술, 능력을 세분화하여 직업군별로 평균 130개 정도의 필요역량을 제시하였다.

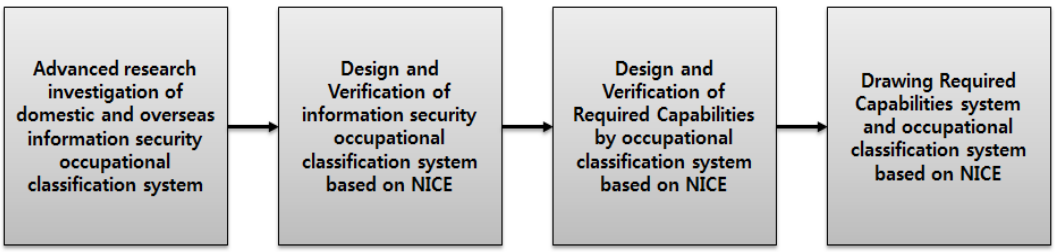
3. 융합 환경기반 정보보호 직업분류체계 및 필요역량 설계

3.1 정보보호 직업분류체계 및 필요역량 도출방법론

NICE를 기반으로 한 정보보호 직업군 설계 및 필요역량 도출 방법론은 다음과 같다. 먼저, 국내·외의 정보보호 직업분류체계 선행연구조사를 통해 기존의 직업군 분류와 각 직업군별 필요역량을 조사 및 분석한다. 다음으로 분석한 선행연구 데이터를 이용하여 정보보호 직업군을 정의하고 도출된 정보보호 직업군을 다시 NICE 기반 정보보호 직업분류체계에 맞게 재분류한 뒤 전문가 회의를 통해 타당성을 검증한다. 정보보호 직업분류체계별 필요역량 설계 과정도 정보보호 직업분류체계 설계 과정과 마찬가지로, 선행연구 데이터를 이용하여 각 직업분류체계별로 제시한 필요 역량을 도출하고 NICE 기반 직업분류체계에 맞도록 재분류 한다. 또한 도출한 직업분류체계별 필요역량을 전문가 회의를 거쳐 국내 실정에 맞도록 필요한 내용을 선택하고 타당성을 검증한다. 마지막으로, 이러한 방법론을 통해 도출된 정보보호 직업분류체계 및 직업분류체계별 필요역량을 종합하여 최종 도출한다.

3.2 정보보호 직업분류체계 설계 및 검증

먼저 정보보호 직업군을 설계하기 위해 4단계의 정보보호 직업군 설계 방법론을 거쳐 정보보호 직업군을 도출하였다. 첫 번째 단계로, 선행연구 데이터를 선행연구 데이터를 기반으로 동일한 직무를 수행하는 직업을 서로 다른 직업명으로 표기한 경우, 1개의 직업명으로 통합하여 정리하였다. 예를 들어, <Table 1>과 같이 동일한 직무를 수행하는 유사 직업군임에도 불구하고 정보보호 전문인력 양성을 위한 필수 요구지식 및 교육인증 프로그램 연구[7]에서는 '최고 정보보안 관리자', 정보보안 기사, 정보보안 산업기사 국가기술자격 종목개발 연구[6]에서는 '최고 정보보안 정책가', Information Technology(IT) Security Essentail Body



〈Figure 1〉 A Methodology of Information Security Occupational Classification System and Required Capabilities

〈Table 1〉 Design of Information Security Occupational Classification(Step 1)

Kim and Bakc[7]	Human Resource Development Service of Korea[6]	Homeland Security[12]	NIST[11]	Mapping
Chief information SeCurity Manager	Chief Information Security policy officer	Chief Information Officer(CIO)	Chief Information Security Officer	O
Information Security Manager	Information Security Director	Security Program Director	Information Security Policy Manager	O
			Information Systems Security Manager	
IT Security Observer/ Risk Manager	Information system Auditor	Auditor	Certification Agent	O
		Certified Computer Examiner	Information Assurance Manager	
Personal Information Security Expert.	Developer	Chief Risk Officer(CRO)	Cyber Security Officer	X
IT System Operation and Maintenance Expert.	Security Researcher	Digital Forensics Analyst	Information Security Program Manager	X
IT Security Expert	Computer System Design and analysis Expert	Digital Forensics Engineer	Security Training Coodinator	X
Digital Forensic Expert.	Network System Developer	Cyber Security Officer	Incident Analyst	X
IT Security Technician	Security Engineer	Enterprise Security Officer	Incident Handler	X

of Knowledge(EBK)[8]에서는 'Chief Information Officer(CIO)', National Initiative for Cybersecurity Education(NICE)[13]에서는 'Chief Information Security Officer'로 각 연구마다 상이한 명칭을 '최고 보안 관리자(보안전략전문가)'로 통일시켜 정리하는 등 직업명을 통합하여 정리하였다.

두 번째 단계로, 각 선행연구 데이터를 통해 세부 직업들을 포함할 수 있는 직업군을 도출하였다. 크게 정보보호 핵심 직업군과 정보보호 연관(주변) 직업군으로 분류하였으며, 정보보호 핵심 직업군은 일반 직업군과 특화 직업군으로 분류하였다. 그 결과, '보안장비 개발' 직업군과 '보안프로그램 개발' 직업군을 모두 포함하는 '보안시스템 개발'이라는 직업군을 도출하고, '보안 관제', '보안 수사' 직업군을 모두 포함하는 '침해사고 대응' 직업군을 도출하는 등의 기준 직업군을 도출하여 일반 직업군으로 분류하였고, '개인정보보호', '금융정보보호', '의료정보보호' 등의 직업군은 특수 직업군으로 분류하였다. 마지막으로, '위험관리 경영', '재난/재해 방지'같은 직업군들은 정보보호 연관(주변)직업군으로 따로 분류하였다.

〈Table 2〉 Design of Information Security Occupational Classification(Step 2)

Group		Standard Occupational Classification		
Information Security Occupational Classification	Normal	Security System Development	Security Product Development	Research
				Design
				Realization
				Installation
			Security Program Development	Research
				Design
				Realization
				Installation
		Security product/Service sale		
		Security product/Service operation		
		Emergency Response	Security Control	
			Security Investigation	
		Security Consulting (Examination)	Security Technology Consulting	Vulnerability Analysis
				Penetration Testing
			Security Management Consulting	
		Security Education	Security Technology Education	
			Security Management Education	
		Security Product(Technology) Certification Evaluation	Information System Security Inspection	
			Security Management Certification Evaluation	
		Security Management Certification Evaluation	Security Management Certification Evaluation	
		Security Management	Security Manager	
			Security Worker	
	Specialization	Personal Information Protection		
		Financial Information Protection		
		Medical Information Protection		
		Industrial Information Protection		
Occupational Classification Related with Information Security		Risk Management(including finance)		
		Prevention of Disaster		
		System Operation/Maintenance		
		Information System Supervision		
		Security Guard		

세 번째 단계에서는 2단계에서 도출한 정보보호 직업군 설계 案을 바탕으로 전문가 심층인터뷰, 자문위원회를 실시하여 검증을 실시하였다. 이를 통해 누락된 직업군은 단계별로 추가 및 검증을 통해 포함하였고 유사 직업군이 있는 경우, 기준 직업군에 유사 직업군을 추가하여 직업명 통일 근거를 뒷받침하였다. 또한, 정보보호 핵심 직업군 중 일반 직업군을 생태계 기반의 수요와 공급(제품/서비스)으로 분류하였다.

마지막으로 네 번째 단계에서는, 최종 검증이 완료된 직업군 설계 案을 바탕으로 선행연구를 정리하였다. 최종 완성된 직업(군) 설계를 위한 데이터를 기준 직업군~유사 직업군~선행연구 직업 순으로 정렬하였다.

〈Table 3〉 Design of Information Security Occupational Classification(Step 4)

Standard Occupational Classification			Similar Occupational Classification	Previous Research			
				[7]	[6]	[12]	[11]
Cryptography							
Security System development	Security Device Development	Research		IT Security Technician			R&D Research
		Design			Developer Computer System Designer and Analyst	Enterprise Security Architect Security Architect Requirements Analyst Security Analyst	Information Security Architect Security Architect Security Solutions Architect
		Realization			Developer Network System Developer		Developer
		verification (Test)					Application Security Tester Security Quality Engineer Security Quality Assurance Engineer Testing and Evaluation Specialist
		Installization			Security Engineer		Security System Engineer

이렇게 4단계로 정보보호 직업군 설계를 진행하고 전문가 회의를 거쳐 총 35개의 정보보호 직업군이 도출되었으며 국내외 참고문헌 선행연구 및 단계별 설계·검증을 통해 각 직업군별 정의를 도출하였다. 도출한 정보보호 직업군과 그 정의는 다음과 같다. '보안제품 개발자' 직업군은 암호/인증, 시스템/네트워크 등의 분야에서 정보보호 시스템 연구/설계/개발 업무를 수행하며, 'SW 분석/설계 전문가' 직업군은 SW 분석 전문가 직업군과 SW 설계 전문가 직업군을 합쳐놓은 직업군으로, 시스템 개발을 위한 요구사항 분석 및 이를 해결하기 위한 계획과정을 수행한다. 'SW 개발자' 직업군은 시스템 구현과 함께 이와 연관된 프로젝트 관리업무를 수행하며, '보안제품 기술자' 직업군은 개발된 정보보호 시스템에 대한

품질보증과 함께 고객 맞춤화(설치)를 위한 기술(운영)지원 업무를 수행한다. ‘SW 테스트 기술자(품질 관리자)’ 직업군은 개발된 시스템에 대한 품질보증과 함께 고객 맞춤화를 위한 기술(운영)지원 업무를 수행하며, ‘보안제품 기술영업’ 직업군은 정보보호 시장분석을 통해 잠재적인 시장(고객)을 발굴하고, 고객 요구사항 분석을 통해 최적의 정보보호 시스템 구축방안을 제시하는 업무를 수행한다.

‘사이버 보안 관제사(보안관제요원)’ 직업군은 정보자산(HW/SW/NW) 위협요소를 실시간으로 탐지하여, 시스템 취약점을 분석하고, 해킹/웜/바이러스 발생시 대응팀과 협조하여 빠르게 보안위협에 대응하는 업무를 수행하며, ‘취약성 분석 전문가’ 직업군은 정보자산(HW/SW/NW)에 피해를 끼칠 수 있는 보안위협을 확인하고, 정보자산 취약성에 따라 발생할 수 있는 위험정도와 피해규모를 평가하고, 이를 감소시킬 수 있는 통제방법을 도출하는 업무를 수행한다. ‘모의 해킹 전문가’ 직업군은 정보자산(HW/SW/NW)에 대해 다양한 해킹도구/기법을 활용하여 시스템 침투가능성을 진단을 수행하며, ‘침해사고 대응 전문가’ 직업군은 보안사고 발생에 따른 피해규모 최소화를 위해 체계적인 대응행위(보안사고 보고/시스템 복구/예방전략 수립)를 수행한다.

‘사이버 범죄 수사관’ 직업군은 사이버범죄에 대한 증적자료 확보를 통해 법적인 수사업무를 집행하는 업무를 수행하며, ‘디지털 포렌식 전문가’직업군은 보안사고와 연관된 위협요인에 대한 증거 수집/복구/추적 활동을 수행한다. ‘암호/해독 전문가’ 직업군은 중요정보에 대한 높은 수준(고강도)의 암호화 또는 높은 수준으로 암호화된 정보에 대해 해석하는 업무를 수행하며, ‘악성코드 분석 전문가’ 직업군은 정보자산을 위협하는 악성코드를 분석하여 세부적인 동작원리와 함께 대응방법을 설계하는 업무를 수행한다.

‘정보시스템 감리사’ 직업군은 사전에 설계된 객관적인 기준에 따라 시스템에 대한 효과성/효율성/안전성 등을 평가하는 업무를 수행하며, ‘정보시스템 보안감사’ 직업군은 시스템 보안 상태를 사전에 정의된 보안 요구사항과 비교하여 객관적인 충족여부를 검증하는 업무를 수행한다. ‘보안제품 인증 전문가’ 직업군은 보안시장에 출시된(출시예정인) 보안제품에 대해 사전에 정의된 보안 적합성(보안 프로파일) 충족여부를 평가하는 업무를 수행하며, ‘보안관리 인증 전문가’ 직업군은 조직 수준의 정보보호 관리체계 통제항목 충족여부를 평가하는 업무를 수행한다. ‘보안기술 컨설턴트’ 직업군은 정보자산(HW/SW/NW)과 비즈니스 프로세스 대상의 위협/취약점에 대응되는 보안 수준(보안 대응책)을 비교하여 기술적인 보안 해결책을 제시(설계)하는 업무를 수행하며, ‘보안관리 컨설턴트’ 직업군은 정보자산(HW/SW/NW)과 비즈니스 프로세스 대상의 위협/취약점에 대응되는 보안 수준(보안 대응책)을 비교하여 관리적인 보안 해결책을 설계하는 업무를 수행한다. ‘보안 컨설턴트(보안진단 전문가)’직업군은 정보자산(HW/SW/NW)과 비즈니스 프로세스 대상의 위협/취약점에 대응되는 보안 수준(보안대응책)을 비교하여, 고객의 요구 수준에 따른 통합적인 보안 해결책을 설계하는 업무를 수행한다.

‘지식 관리자’ 직업군은 조직의 비즈니스 프로세스 흐름 속에서 발생되는 정보생성/정보활용(유통)/정보폐기 등에 관한 통합적인 정보생애주기 관리업무를 수행한다. ‘DB 보안 관리자’ 직업군은 조직의 비즈니스 프로세스

흐름 속에서 발생된 모든 정보를 대상으로 통합적인(중앙 집중의) 보안통제(접근통제) 업무를 수행하며, '정보시스템(네트워크) 관리자' 직업군은 시스템/네트워크 운영/관리 업무를 체계적으로 진행하는 업무를 수행한다. '보안시스템 관리자' 직업군은 정보자산(HW/SW/NW) 보호 목적의 보안시스템을 고장 없이 안정적으로 구축/운영/유지 보수하는 업무를 수행하며, '개인정보보호 관리자' 직업군은 개인정보(사생활) 보호를 위한 정책개발/법제도준수/보안관리 활동을 수행/책임하는 업무를 수행한다. '보안관리자' 직업군은 조직관점의 보안목적을 달성하기 위하여 보안정책/보안 관리체계/보안시스템 구축/운영(관리)업무를 실제적으로 수행하며, '보안관리 기획자' 직업군은 조직 경영목표에 부합된 보안정책을 수립하고, 이를 실제적으로 구현하기 위한 단계적 추진전략을 수립하는 업무를 수행한다. '준법감시자' 직업군은 책임 있는 비즈니스 업무수행을 위해 지켜야 할 관련법규 준수활동을 설계/운영/평가하는 업무를 수행하고, '보안 교육 전문가(변화관리 전문가)' 직업군은 정보보호 인식제고/지식/역량 향상을 위해 사용자/전문가 대상의 교육 프로그램을 설계/운영하는 업무를 수행한다.

'보안전문 검사/변호사' 직업군은 보안 분야(사이버 범죄 등)에 특화된 법률적 지식을 보유한 법조인 직업군이며, '개인정보보호 전문가' 직업군은 특정 조직의 개인정보보호 수준을 진단(평가), 이에 부합되는 보안 대책 구축 방안을 제시하는 업무를 수행한다. '최고 보안관리자(보안전략 전문가)' 직업군은 조직경영관점의 보안전략(보안전술)을 총괄적으로(통합적으로) 수립/운영(관리)/조정하는 업무를 수행하며, '보안전문 교수/기자' 직업군은 보안 분야(법/기술/관리)에 특화된 학문적 지식과 역량을 보유하며 보안 분야(법/기술/관리)에 특화된 기사를 조사/보도하는 업무를 수행한다. 마지막으로 '국제 보안 전문가' 직업군은 국제적 수준의 상호 운영성이 확보될 수 있는 보안기술/보안 관리체계 표준화 업무를 수행한다.

위와 같이 도출한 35개의 정보보호 직업군을 NICE에서 제시한 정보보호 직업분류체계에 따라 7개 직업군(Security Provision, Protect and Defend, Investigate, Collect and Operate, Analyze, Operate and Maintain, Oversight and Development)으로 재분류하였다. 재분류한 결과는 다음과 같다. 첫 번째, 'Security Provision(개발)' 직업군에는 '보안제품 개발자', 'SW 분석/설계 전문가', 'SW 개발자', '보안제품 기술자', 'SW 테스트 기술자(품질 관리자)', '보안제품 기술영업'의 6가지 직업군이 분류되었다. 두 번째, 'Protect and Defend(사전 침투/방어)' 직업군에는 '사이버 보안 관제사(보안관제요원)', '취약성 분석 전문가', '모의 해킹 전문가', '침해사고 대응 전문가'의 4가지 직업군이 분류되었다. 세 번째, 'Investigate(사후 조사)' 직업군에는 '사이버 범죄 수사관', '디지털 포렌식 전문가'의 2가지 직업군이 분류되었다. 네 번째, 'Collect and Operate(수집/해독)' 직업군에는 '암호/해독 전문가', '악성코드 분석 전문가'의 2가지 직업군이 분류되었다. 다섯 번째, 'Analyze(진단/평가)'직업군에는 '정보시스템 감리사', '정보시스템 보안감사', '보안제품 인증 전문가', '보안관리 인증 전문가', '보안기술 컨설턴트', '보안관리 컨설턴트', '사이버 보안 관제사(보안 관제요원)'의 7가지 직업군이 분류되었다. 여섯 번째, 'Operate and Maintain(관리)' 직업군에는 '지식 관리자', 'DB 보안 관리자', '정보시스템(네트워

크 관리자)', '보안시스템 관리자', '개인정보보호 관리자', '보안관리자'의 6가지 직업군이 분류되었다. 마지막으로 일곱 번째, 'Oversight and Development(감독/총괄)' 직업군에는 '보안관리 기획자', '준법 감시자', '보안 교육 전문가(변화관리전문가)', '보안전문 검사/변호사', '개인정보보호 전문가', '최고 보안 관리자(보안전략전문가)', '보안전문 교수/기자', '국제 보안 전문가'의 8가지 직업군이 분류되었다.

3.3 정보보호 직업분류체계별 필요역량 설계 및 검증

정보보호 직업분류체계별 필요역량을 설계하기 위해 먼저 선행연구조사를 분석한 결과와 NICE 기반 7가지 정보보호 직업분류체계를 매핑하여 가장 중요하다고 여겨지는 필요역량을 도출하였다. 그 결과, 'Security Provision(개발)' 직업군은 '현재 또는 향후 발생 가능할 보안위협에 대한 인식', '특정 응용 프로그램이나 환경에 대한 적절한 지식 저장소 기술과 맞출 수 있는 능력', '개발된 보안시스템을 고객 환경에 적용할 수 있는 능력'이 주요 역량으로 나타났고, 'Protect and Defend(사전 침투/방어)' 직업군은 '시스템/네트워크 보안위협(취약점) 식별/도출(인지/분류) 능력)', '모의 침투 원칙/도구/기술에 대한 지식', '책임 할당 영역에서 일반적인 공격자 전술, 기술, 절차에 대한 지식(역사적 국가별 전술, 기술 및 절차, 새로운 기능 등)'이 주요 역량으로 나타났다. 그 외에도 각 직업군별로 필요 역량을 나열한 결과를 요약하면 아래 <Table 4>와 같다.

〈Table 4〉 Analysis Results of Previous Research

Occupational Classification	Required Capabilities
Security Provision	• Awareness of possible security threat in present or future. • Appropriate knowledge repository skill and suitable ability about specific application program or environment. • Ability which is applicable to developed security system in customer environment.
Protect and Defend	• Identification/derivation(recognition/classfication) of System/Network security threat(vulnerability) • Knowledge about penetration testing rule/device/skill • Knowledge about general offensive tactics, skill, process in responsible allocation. (historical nation tactics, Skill and process, New function etc.)
Investigate	• Skill which can identify and derive from medicolegal interest data in various media. • Device structure of digital forensic/Utilization ability of supporting program • Identification ability about abnormal behavior according to information type.
Collect and Operate	• Collection/Integration/Interpretation ability of related information utilizing various security (event) device. • Cognitive technologies/Utilization ability of reverse engineering/obfuscation • Encoding algorithm knowledge(IPSEC, AES, GRE, IKE, MD5, SHA, 3DES)
Analyze	• Standard knowledge(procedure) related with security system reliability/performance • Knowledge about requirement of internal expert system for safety, performance and reliability. • Performance competency of risk management(assessment) related with business procedure.
Operate and Maintain (Management)	• Knowledge about basic system and operational system solution related with problem. • Knowledge about risk threshold/management procedure(methods)(utilization ability of analysis equipment for Vulnerability Identification) • Skill which deign the measure about identified security risk
Oversight and Development	• Knowledge about new information technology/security technology(risk/system) • Knowledge about access control of policy-based and risky acceptance • Construction/Role/Responsibility of the response system of Organizational security accident.

〈Table 5〉 The Derived Results of Required Capabilities by the Information Security Occupations

No	occupational groups	Required Capability
1	Security Provision	• Awareness of possible security threat in present or future. • Management of life cycle for obtaining security system Availability/reliability • Competency about security system design/skill/development • Framework of security system quality verification(performance measure/revision) • Ability which is applicable to developed security system in customer environment. • Collection of network traffic/Competency of filtering analysis
2	Protect and Defend	• Knowledge about method/procedure/skill of collecting information/generation/report/share • Knowledge about Various cyber attack(tactics/skill/procedure)(Passive, Active, Insider, Close-In, Distribution) • Identification/derivation(recognition/classfication) of System/Network security threat(vulnerability) • Knowledge about penetration testing rule/device/skill • Establishment of system/network emergency plans/recovery ability of security accident (disaster).
3	Investigate	• Information theory/knowledge about extracting information • Identification ability about abnormal behavior following information type. • Extract/analysis/utilizing ability of memory dump(debugger result) for extracting information • Tool structure of digital forensic/utilization ability of supporting program • Skill which can identify and derive from medicolegal interest data in various media. • Ability of electronic evidence collection/packing/transportation/storage for protecting information change/loss and physical damage/destruction etc.
4	Collect and Operate	• Collection/integration/interpretation ability of related information utilizing various security (event) device. • Ability of decoding/analysis/interpretation about electronic signature/malignant code/ volatility data etc. • Ability of Cryptography/encoding algorithm knowledge/realization • Cognitive technologies/utilization ability of reverse engineering/obfuscation • Knowledge about hacking method in various operation system • Technique tracking and analyzing legal/technical trend which can affect cyber activities
5	Analyze	• Standard knowledge(procedure) related with security system reliability/performance • Competency which can assess security system suitability/ruggedness/integrity • Awareness of recent industrial trend about security system detection/supply etc. • Standard knowledge(procedure) related with Security management Procedure/system • performance competency of risk management(assessment) related with business procedure.
6	Operate and Maintain	• Control method of risk acceptance based on security policy • Knowledge about risk threshold/management procedure(methods)(utilization ability of analysis equipment for Vulnerability Identification) • performance ability of response procedure according to security accident • Security system construction/operation(utilization) • Knowledge about security system construction rule and response method • Knowledge about operational information assurance principle and security requirement • Ability which design policy reflected in operational security purpose.
7	Oversight and Development	• Knowledge about new information technology/security technology(risk/system) • Knowledge about legal governance related with business • Knowledge about external organization(academic institutions) dealing with cyber security problems. • Construction/Role/Responsibility of the response system of Organizational security accident. • Awareness of international cyber information security trend

다음으로, 도출된 직업분류체계별 필요역량을 전문가 회의를 통해 국내 정보보호산업 실정 적합하도록 필수역량만을 선택하고 기존 연구에는 없지만 새롭게 추가해야할 필수역량을 도출하여 종합하였다. 그 결과, 7가지 직업군별로 평균 6개의 필요역량을 도출하여 <Table 5>와 같은 NICE 기반 정보보호 직업군별 필요역량을 도출하였다.

4. 결 론

제 3장에서 도출한 NICE 기반의 정보보호 직업분류체계 및 직업군별 필요역량을 종합하여 최종적으로 정보보호 직업분류체계 및 직업군별 필요역량을 도출하였다. 그 결과 'Security Provision(개발)' 직업군에 포함되는 직업은 '보안제품 개발자', 'SW 분석/설계 전문가', 'SW 개발자', '보안제품 기술자', 'SW 테스트 기술자(품질 관리자)', '보안제품 기술영업'의 직업들이 포함되며 필요한 주요 역량으로는 '현재 또는 향후 발생 가능할 보안위협에 대한 인식', '보안시스템 가용성/신뢰성 확보를 위한 생명주기 관리', '보안시스템 설계/기술/개발에 대한 역량', '보안시스템 품질검증(성능측정/보정) 방법론', '개발된 보안시스템을 고객환경에 적용할 수 있는 능력', '네트워크 트래픽 수집/필터링 분석 역량'이 필요한 것으로 나타났다. 'Security Provision' 직업군을 포함한 나머지 6개 직업군에 대하여 포함되는 직업과 필요역량을 보기 쉽게 표로 요약하면 <Table 6>과 같다.

이러한 연구결과는 미래 융합환경에 적합한 정보보호 인력의 수급차 해소 및 처우개선을 위한 기초자료로 사용하고, 향후 정보보호 직업군에 대한 명확한 직업분류체계와 직업군별 필요역량을 이용하여 해당 직업군에 필요한 융합적인 역량을 집중적으로 습득할 수 있는 표준화된 교육 훈련방법을 마련하는데 활용하여 미래 융합환경에 적합한 정보보호 인력양성에도 긍정적인 효과를 나타낼 수 있을 것으로 기대된다.

〈Table 6〉 The derived Results of the Occupational Classifications and Required Capabilities by the Information Security Occupations Based on NICE

No	Occupational Groups	Occupation	Necessary capability
1	Security Provision	Security Product Developer	• Awareness of possible security threat in present or future. • Management of life cycle for obtaining security system Availability/reliability • Competency about security system design/skill/development • Framework of security system quality verification (performance measure/revision) • Ability which is applicable to developed security system in customer environment. • Collection of network traffic/Competency of filtering analysis
		SW Analysis/Design Expert	
		SW Developer	
		Security Product Engineer	
		SW Test Engineer(Quality Manager)	
		Security Product Sales Engineer	
2	Protect and Defend	Cyber Security Controller (Security Controller)	• Knowledge about method/procedure/skill of collecting information/generation/report/share • Knowledge about Various cyber attack(tactics/skill/procedure) (Passive, Active, Insider, Close-In, Distribution) • Identification/derivation(recognition/classfication) of System/Network security threat(vulnerability) • Knowledge about penetration testing rule/device/skill • Establishment of system/network emergency plans/recovery ability of security accident(disaster).
		Vulnerability Analyst	
		Simulation Hacking Expert	
		CERT Expert	

3	Investigate	Cyber Crime Investigator	• Information theory/knowledge about extracting information • Identification ability about abnormal behavior following information type. • Extract/analysis/utilizing ability of memory dump(debugger result) for extracting information • Tool structure of digital forensic/utilization ability of supporting program • Skill which can identify and derive from medicolegal interest data in various media. • Ability of electronic evidence collection/packing/transportation/ storage for protecting information change/loss and physical damage/destruction etc.
		Digital Forensic Expert	
4	Collect and Operate	Cryptography Expert	• Collection/integration/interpretation ability of related information utilizing various security(event) device. • Ability of decoding/analysis/interpretation about electronic signature/malignant code/ volatility data etc. • Ability of Cryptography/encoding algorithm knowledge/realization • Cognitive technologies/utilization ability of reverse engineering/ obfuscation • Knowledge about hacking method in various operation system • Technique tracking and analyzing legal/technical trend which can affect cyber activities
		Malware Analyst	
5	Analyze	Information System Supervisor	• Standard knowledge(process) related with security system reliability/performance • Competency which can assess security system suitability/ruggedness/integrity • Awareness of recent industrial trend about security system detection/supply etc. • Standard knowledge(procedure) related with Security management process/system • performance competency of risk management(assessment) related with business process.
		Information System Security Inspector	
		Security Product Certification Expert	
		Security Management Certification Expert	
		Security Technology Consultant	
		Security Management Consultant	
		Cyber Security Controller(Security Controller)	
6	Operate and Maintain	Knowledge Manager	• Control method of risk acceptance based on security policy • Knowledge about risk threshold/management procedure(methods)(utilization ability of analysis equipment for Vulnerability Identification) • performance ability of response procedure according to security accident • Security system construction/operation(utilization) • Knowledge about security system construction rule and response method • Knowledge about operational information assurance principle and security requirement • Ability which design policy reflected in operational security purpose.
		DB Security Manager	
		Information System(Network) Manager.	
		Security System Manager.	
		Personal Information Security Manager	
		Security Manager.	
7	Oversight and Development	Security Management Director	• Knowledge about new information technology/security technology(risk/system) • Knowledge about legal governance related with business • Knowledge about external organization(academic institutions) dealing with cyber security problems. • Construction/Role/Responsibility of the response system of Organizational security accident. • Awareness of international cyber information security trend
		law-abiding monitor	
		Security Education Expert (Change management Expert)	
		Security Prosecutor/Lawyer	
		Personal Information Security Manager	
		Chief Security Manager (Security Strategic Expert)	
		Security Professor/Reporter	
		International Security Expert	

References

[1] Bae, Y. S. and Chang, H. B., "A Qualitative Research on ICT Policy Design for Small and Medium Business," The Journal of Society for e-Business Studies, Vol. 18, No. 1, pp. 57-70, 2013.

[2] Bailey, J. and Stefaniak, G., "Preparing the information technology workforce for the new millennium," ACM SIGCPR Computer Personnel, Vol. 20, No. 4, pp. 4-15, 1999.

[3] Carey, A., "2006 Global Information Security Workforce Study," IDC, 2006.

[4] Chai, S. M. and Kim, M. K., "A Road To Retain Cybersecurity Professionals : An Examination of Career Decisions Among Cybersecurity Scholars," Journal of The Korea Institute of Information Security and Cryptology, Vol. 22, No. 2, pp. 295-316, 2012.

[5] Chai, S. M., Bagchi, S., Goel, R., Raghav, H., and Upadhyaya, S., "A Framework for Understanding Minority Students' Cybersecurity Career Interests," Procedings of the Twelfth Americas conference on Information systems, pp. 3426-3432, 2006.

[6] Human Resources Development Service of Korea, "A Study on National Technical Qualifications, Engineer Information Security and Industrial Engineer Information Security," 2010.

[7] Kim, J. D. and Baek, T. S., "A Study on Essential Body of Knowledge and Education Certification Program for Information Security Professional Development," Journal of Digital Convergence, Vol. 9, No. 5, pp. 113-121, 2011.

[8] Kim, K. G., "Cybersecurity Career Roadmap," The Magazine of the IEIE, Vol. 41, No. 4, pp. 50-59, 2014.

[9] Korea Employment Information Service, "KECO," 2009.

[10] Lee, J. T., Kim, Y. H., Na, Y. S., and Chang, H. B., "A Study on IT Based Risk Management System Development for Business Continuity Management : Centering on Cases at Automobile Manufacturing Industry," The Journal of Society for e-Business Studies, Vol. 18, No. 2, pp. 69-79, 2013.

[11] NIST, "National Initiative for Cybersecurity Education(NICE)," 2011.

[12] United States Department of Homeland Security, "Information Technology(IT) Security Essential Body of Knowledge (EBK)" : A Competency and Functional Framework for IT Security Workforce Development," 2008.

[13] Yoo, H. W. and Kim, T. S., "Information Security Professionals' Turnover Intention and Its Causes," Journal of the Korea Institute of Information Security and Cryptology, Vol. 20, No. 1, pp. 95-104, 2010.

저 자 소 개

이윤수 (E-mail : myvipman@gmail.com)
1987년 한국외국어대학교 경영정보대학원 (경영학 석사)
현재 한국인터넷진흥원 수석연구원
관심분야 사이버보안 인적역량 강화 정책 및 교육훈련, 기업경영정보 시스템 컨설팅, 인터넷 및 정보보안, ICT 국제협력 등

신용태 (E-mail : shin@ssu.ac.kr)
1985년 한양대 산업공학 (석사)
1990년 University of Iowa 전산학 (석사)
1994년 University of Iowa 전산학 (박사)
2015년 (사)개방형컴퓨터통신연구회(OSIA) 회장 역임 중
현재 숭실대학교 컴퓨터학부 교수
관심분야 컴퓨터 네트워킹, 컴퓨터 활용, 인터넷과 정보보안, 인터넷 활용 등