The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 17, No. 4, pp.209-218, Aug. 31, 2017. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2017.17.4.209
JIIBC 2017-4-27

금융보안 전문 자격제도 도입 필요성에 관한 연구

A Study on the Necessity of the Introduction of Professional Certification System for Financial Security

정희형*, 권헌영**

Hee-Hyoung Jung*, Hun-Yeong Kwon**

요 약 날로 고도화 지능화 되는 금융보안 위협에 효율적이고 선제적으로 대응하고, 금융 이용자가 안전하게 금융서비스를 제공받을 수 있도록 금융권의 전문적인 정보 보안인력이 필요한 실정이다. 하지만 2015년 기준 금융IT 보안인력은 금융IT인력 중 4.9%로 전년대비 다소 증가하였으나, 여전히 낮은 수준이다. 이에 본 연구에서는 점차 금융 보안 전문 인력들의 증가가 예상되는 가운데 금융 보안 전문 인력들의 최소한의 업무수행능력 검증과 보안의식 제고를 위하고 기존 보안자격제도의 과목과 금융보안원 및 금융감독원에서 제시한 교육커리큘럼 및 검사기법들을 비교분석하여 금융 분야에 특화된 정보보안 전문자격 도입 필요성에 대하여 연구하고자 한다.

Abstract In order to efficiently and preemptively respond to financial security threats that are becoming more sophisticated and intelligent, and to enable financial users to receive financial services safely, financial information security professionals are needed. However, as of 2015, the number of financial IT security personnel was 4.9%, which is slightly lower than the previous year, but still low. In this study, it is expected that the number of experts in financial security will increase gradually. In order to verify the minimum performance of financial security professionals and enhance the security consciousness, the subjects of the existing security qualification system, Curriculum and inspection techniques to analyze the necessity of introducing information security specialization specialized in financial sector.

Key Words : Financial Security, Security Specialist, Certificate

Ⅰ. 서 론

IT기술이 발전하고 모바일 기기의 활용 추세가 가속화되면서 기존 금융 산업의 환경도 점차적으로 변화되고 있다. 우선 금융서비스의 중심이 기존 오프라인에서 편의성이 뛰어난 인터넷 및 모바일 중심으로 재편되고 있는 추세이다. 인터넷과 IT기술이 발전하고 모바일 기기가 진화하면서 비대면 채널 및 모바일 기기를 활용하는 금융서비스가 활성화되고 있다.

은행이 제공하는 인터넷뱅킹(모바일뱅킹 포함) 서비스의 가입자 수(은행간 중복포함)는 2015년말 1억 1,685만명에 이르렀으며, 서비스 규모는 2015년중 일평균 40조 2,869억원, 7,802만건을 기록하였다. 특히 2015년말 기준으로 스마트폰 기반 모바일뱅킹(이하 스마트폰뱅킹)의 등록 고객수는 6,479만명에 이르러 연간 34.4%의 높은 증가율을 기록하였다[1].

날로 고도화·지능화 되는 금융보안 위협에 효율적·선제적으로 대응하고, 금융 이용자가 안전하게 금융서비스

*정회원, 고려대학교 정보보호대학원 금융보안학과
**정회원, 고려대학교 정보보호대학원 금융보안학과
접수일자: 2017년 5월 1일, 수정완료: 2017년 6월 25일
게재확정일자: 2017년 8월 11일

Received: 1 May, 2017 / Revised: 25 June, 2017 /
Accepted: 11 August, 2017
*Corresponding Author: goygud@gmail.com
Dept. of Information Security, Korea University, Korea

를 제공받을 수 있도록 금융권의 전문적인 정보 보안인력이 필요한 실정이다. 2015년 말 국내 154개 금융기관의 금융IT인력은 총 9,288명으로 전년 말 대비 1.5% 증가한 것으로 나타났다. 이 가운데 정보보호관리 인력은 4.9% 증가하는데 그쳐 전년수준(34.0%)보다 크게 낮아졌다[2]. 또한 2011년 금융보안 문제점과 대책을 모색하기 위한 금융보안정책토론회 당시 '보안 쪽에는 인력과 질 부분에서 수준과 전문성이 결여되어 전문성을 갖춘 보안인력을 육성하기 위해선 금융보안 전문가 자격제도가 필요하고 자격제도를 시행하여 보안 전문가의 위상을 자리 잡아야 하며, 조직적 뒷받침이 약한 보안을 보다 체계적으로 강화해야 할 수 있도록 감사 부문과 결합해 책임자를 두고 업무를 강화할 수 있도록 해야 한다'라고 금융보안 수준 제고 방안을 제시 하였다[3].

본 연구에서는 정부주도의 사전규제에서 민간중심의 자율규제로 전환됨에 따라 금융기관에서는 정보보안 인력의 업무수행능력 검증과 보안의식 제고를 높여야 하고 전자금융 감독규정 시행세칙에 따라 금융감독원의 전자금융 업무 보고서(IT019) 중 "CISO(정보보호최고책임자)지정현황" 작성요령에 CISO/CIO의 유관자격증은 '감리원','CISA','CISSP','SIS','정보보호관리체계 인증 심사원' 이렇게 5개 자격증에 대해서만 유관자격증으로 인정하고 있지만 금융보안에 특화된 자격은 없음에 따라 유관자격증과 금융보안원 및 금융감독원에서 제시한 교육커리큘럼 및 검사기법들을 비교분의 금융 분야에 특화된 정보보안 전문자격 도입 필요성에 대하여 연구하고자 한다.

또한 금융보안 전문가의 수요를 예측하고, 금융보안 전문가의 직무를 분석하여 자격·검정체계를 도출한다. 도출된 자격·검정체계를 활용하여 공인자격제도 등록을 위한 기틀과 국가차원에서 금융보안 전문가를 체계적으로 양성할 수 있는 기반을 마련하고 금융기관에서 정보보안 분야의 중요성과 필수성을 인식시키는데 그 목적이 있다.

II. 금융보안 전문인력의 현황과 양성체계

1. 금융보안 개념 및 의의

기술 서비스 채널 간의 여러가지 융복합 현상이 발생한다. 금융IT와 비금융IT, 모바일 기술 그리고 온라인과 오프라인 간의 융복합이 일어나므로 접점이 증가하고 대응 수단을 복잡하게 할 뿐 아니라 기존에는 없었던 새로운 취약점을 발생시키게 한다[4].

정보보안(information security)의 사전적 의미는 정보를 안전하게 유지하는 것이다. 정보를 안전하게 유지한다는 것의 의미는 내가 가지고 있는 정보가 나의 의도와는 다르게 다른 사람들에게 노출되어지는 것으로부터 안전하게 지킨다는 특성이 강하다. 즉 내가 원하는 상대방에게는 정보를 제공하고 내가 원하지 않는 상대방에게는 정보를 제공하지 않는 것을 말한다[5].

금융보안의 중요성은 금융기관 자원의 방대함과 금융기관을 이용하는 고객의 자산 및 정보, 사용자수를 감안한다면 그 보안의 범위는 상당히 광범위 하고 중요하다고 설명할 수 있다. 또한 금융기관의 전산시스템 복잡성과 규모, 결제 대금의 규모와 금융기관의 사용빈도, 다국적 금융기관과의 업무 등을 고려한다면 금융 보안은 국방 보안의 중요성에 버금간다고 말할 수 있을 것이다.

직접 대면하지 않는 방식의 전자금융거래 이용수단의 발달로 금융소비자들의 이용 편의성은 높아진 만큼 그에 따른 각종 보안위협도 함께 증가하였으며, 전자금융 이용자의 컴퓨터와 모바일 기기 등에 악성코드를 감염시켜 금융정보를 취득하고 부당거래를 통해 불법적으로 자금을 취하고자 하는 등의 위협은 지속적으로 증가하고 있다[6].

DDos 공격・해킹 등 사이버 공격을 통해 금융 전산시스템을 마비시키거나 고객정보를 부당하게 취득하여 금융서비스 이용자의 불편 및 피해를 초래하고 있는 위협이 지속적으로 증가하고 있으며, 최근의 사이버공격은 여러 금융회사에 지능형지속위협(APT)공격 등을 통해 동시 다발적으로 전산자료를 파괴(삭제)하여 금융시스템을 일시에 대량으로 마비시키는 양상으로 날로 대형화・지능화되는 사이버공격으로 인해 기존 대응체계가 무력화되는 상황에서 금융보안에 새로운 전환점을 마련해야 할 시점이라고 할 수 있겠다[7].

또한 금융보안원 허창원 원장은 금융보안에 대해서 '금융보안은 금융에 대한 전반적인 이해를 기반으로 IT와 보안 기술, 법률 지식 등이 종합적으로 요구되는 특수분야다.'라고 정의하였다[8].

2. 금융보안 전문 인력의 역할

연이어 발생하는 해킹사고로 기업에서 정보보안을 위

한 기술적 대책과 법률대응까지 책임지는 정보보호 최고책임자(CISO)의 중요성이 날로 높아지고 있음에 따라 최근 발의된 정보통신망 이용촉진 및 정보보호 등에 관한 법률의 일부개정안에 따르면 중소 사업자를 제외한 대규모 사업자의 임원급 CISO 선임, 정보보호 업무 외 겸직 금지와 정보보호최고책임자의 자격요건을 법령으로 정하도록 발의함에 따라서 발의가 통과된다면 CISO의 자격요건에 대해서 더욱 강화되고 특히 금융보안의 자격요건은 더욱 더 강화될 것이다.

현재 정보통신망법(제45조3제3항)에 따르면 정보보호 최고책임자가 다음 업무를 총괄한다고 되어 있다.

표 1. 정보통신망법에 나타난 정보보호최고책임자의 총괄 업무
Table 1. General supervision of the chief information security officer in the Information and Communication Network Act

제45조의3 제3항
정보보호관리 체계의 수립 및 관리·운영
정보보호 취약점 분석·평가 및 개선
침해사고의 예방 및 대응
사전 정보보호 대책 마련 및 보안조치 설계·구현 등
정보보호 사전 보안성 검토
중요 정보의 암호화 및 보안서버 적합성 검토
그 밖에 법/법령에 따라 정보보호를 위하여 조치이행

CISO는 정보보호 관리 체계의 수립·운영, 보안 취약점 분석과 정보보호 대책 수립·이행, 사고 대응의 업무를 총괄한다고 볼 수 있다.

전자금융거래법과 그 시행령(제21조의2제3항, 시행령 제11조의3제2항)을 종합하면 정보보호최고책임자는 다음과 같은 업무를 수행한다.

표 2. 전자금융거래법과 그 시행령에 나타난 정보보호최고책임자의 업무
Table 2. The tasks of the chief information security officer in the Electronic Financial Transactions Act and the Enforcement Decree

제21조의2 제4항과 시행령 제11조의3 제2항
전자금융거래의 안정성 확보 및 이용자 보호를 위한 전략 수립
정보기술 부문의 보호 및 관리
정보기술 부문의 보안에 필요한 인력관리 및 예산편성
전자금융거래의 사고 예방 및 조치
전자금융업무 정보기술 부문 보안을 위한 심의에 관한 사항
정보보호 대책 수립·이행

크게 보면 전자금융거래와 정보기술 부문을 포함하여 정보보호 거버넌스 수립, 정보보호 관리 체계의 수립·운영, 정보보호 대책의 수립·이행, 사고 대응을 주요 업무로 분류할 수 있다. 전자금융거래 부문에 관한 사항은 금융위원회 고시인 전자금융감독규정 제3장 '전자금융거래의 안전성확보 및 이용자 보호'와 연결된다.

정보통신기반보호법과 그 시행령(제5조제5항, 시행령 제9조제2항)을 종합하면 정보보호책임자의 업무는 다음과 같다.

표 3. 정보통신기반보호법과 그 시행령에 나타난 정보보호책임자의 업무
Table 3. The work of the information protection officer who appeared in the information communication infra protection law and enforcement decree

제5조 제5항과 시행령 제9조 제2항
주요 정보통신기반시설을 보호하기 위한 관리대책의 수립·시행
주요 정보통신기반시설보호대책의 수립, 예방/복구에 기술적 지원 요청
주요 정보통신기반시설의 취약점 분석·평가 및 이를 수행하는 전담반 구성
주요 정보통신기반시설의 보호에 필요한 조치 명령 또는 권고의 이행
주요 정보통신기반시설이 교란·마비를 인지한 때에 관계기관에 통지
침해사고가 발생한 주요 정보통신기반시설의 복구 및 보호에 필요한 조치
기타 다른 법령에 규정된 주요 정보통신기반시설의 보호업무에 관한 사항

금융위원회에서 발표한 금융회사 정보기술부문 보호업무 이행지침에 따르면 '정보기술부문의 주요 업무 예시' 중 '4.IT 정보보호'에 대한 아래 13가지 항목을 정하였다.

표 4. 정보기술부문의 주요 업무 예시 中 IT 정보보호
Table 4. Information technology department's main business example IT information protection

분류
취약점 분석・평가 및 그 이행 계획 수립 및 시행
내부 정보보호 정책 수립 및 정보보호 관련 규정・지침 제・개정
정보보호 아키텍처 유지관리
정보보호 교육 계획 수립 및 교육 실시
전자금융 및 정보기술부문 관련 보안성 검토
전자금융 관련 정보보호 대책 수립 및 시행
모의해킹, 디도스대응훈련 등 비상대응훈련 계획 수립 및 실시
IT 내부 통제(법규준수 포함) 관리
침해시도에 대한 실시간 보안 관제 및 통합보안관제시스템 운영
외부 직원 출입 통제 및 노트북, USB 등 반출・입 통제
침해방지・대응시스템 구축・운영
시스템 접근 통제, 권한 관리 및 사용자 인증 관련시스템 구축・운영
고객 정보 보호 및 정보 유출 방지 시스템 구축・운영 등

이렇게 정보통신망법, 전자금융거래법, 정보통신기반보호법, 금융회사 정보기술부문 보호업무 이행지침 등에 의거하여 금융보안 전문 인력의 최소한의 업무역할을 정의할 수 있다.

3. 금융보안 전문가 인력수급 현황 및 전망

2015년 한국금융연구원에서 조사한 바에 따르면, 2015년 조사대상 금융회사의 금융보안 인력은 전체 금융 인력의 0.6%를 차지한다고 한다[9].

금융권이 구조조정을 통한 인력 감축 상황에서도 서버 관리 등을 담당하는 금융IT 및 정보보안 인력을 추가로 영입한 것으로 나타났다. 특히 지난해 하반기 시중은행 6곳에서만 140명가량의 신입 IT 인력을 채용했다. 지난해 한국은행이 국내 155개 금융기관을 대상으로 조사한 결과를 보면 2014년 말 총 임직원 수는 23만9539명으로 전년 대비 1.2% 감소했지만 금융정보화 및 정보보안을 담당하는 IT 인력은 9136명으로 9.3% 증가했고, 금융IT 인력 가운데 정보 보호 관리 인력은 770명으로 전년 대비 34.1% 증가한 것으로 나타났다[10].

가. 금융기관 서베이를 통한 수요전망

국내에서 영업 중인 주요 7개 금융업권 1,339개의 금융회사를 대상으로 향후 1년 이내(2015년 9월 기준) 추가 채용 예상 규모에 대한 조사를 실시한 결과, 조사대상 금융회사 중 324개의 회사에서 향후 1년 이내 추가채용이 예정되어 있는 것으로 조사되었다.

아래의 예상대로 채용시 전체인력의 평균 5%이상을 채용해야 하는 금융보안 인력의 비중이 213.2명이 되게 된다.

표 5. 업권별 추가채용 예상규모
Table 5. Estimated additional employment by sector

구분	전체	은행	보험	증권	신탁	저축	여신	신협
예정	4,264	615	545	876	190	1,137	533	368
비중	100	14.4	12.8	20.5	4.5	26.7	12.5	8.6

나. 산업인력 현황 분석 보고서를 통한 수요전망

2011-2015년간 생명보험과 자산운용 산업의 순수익은 성장세를 유지하였으며, 저축은행도 구조조정 이후 회복추세를 보이고 있으며 2015년 10월 기준 우리나라 금융업 취업자 수는 79.3만명으로 추정한다.

2005-2010년간 금융·보험산업의 순이익은 연평균 7.5% 성장하였으며, 자산운용, 캐피탈, 생명보험, 카드산업의 성장률은 연평균 20.5%, 14.6%, 14.1%, 9.0%으로 상대적으로 높은 성장세를 보였으며 한국금융연구원은 향후 5년간의 금융인력 수요는 매년 최대 6,058명씩 증가할 것으로 추정하였으며, 증가율은 0.7- 0.8%에 달할 것으로 전망하고 있다.

표 6. 금융인력 수요전망
Table 6. Financial manpower demand forecast

구분	2016	2017	2018	2019	2020	평균
증가인원	5,526	6,380	6,278	6,076	6,030	6,058
비중	0.70	0.80	0.78	0.75	0.74	0.75

4. 금융보안 전문인력 양성체계

가. 국내 교육 현황

다른 산업분야와는 달리 보안 산업은 기술변화가 너무 빨라 자격제도만으로는 국내외의 기술 수준에 부합하는 인력의 양성이 쉽지는 않다. 자격증을 보유한 전문가의 수준을 적절히 평가할 수 있는 방법도 도출하기 쉽지 않고 지속적으로 발전하는 보안 기술에 대해 자격증 소지자들이 재교육 등을 통해 지식과 기술을 업데이트 하고 있는지 평가하기도 쉽지 않기 때문이다. 이런 한계에도 불구하고 금융보안 자격제도는 보안 관련학과의 커리큘럼을 보다 체계적으로 구조화하고 새로운 기술개발의 결과를 가장 효율적으로 교육과정에 반영할 수 있는 도구가 될수 있다[11].

2015년에 대학 및 대학원의 정보보호 관련 학과를 조사한 결과에 따르면, 전문대학 9개, 대학교 38개, 대학원 36개 학과 등 총 83개 학과가 운영되고 있어, 2014년에 비해 10% 증가하였다. 최근 정보보호의 중요성에 대한 인식이 높아짐에 따라 정규교육기관의 정보보호 관련 학과의 개설도 꾸준히 증가하고 있다.

2015년에 전문대학 이상 정규교육기관의 재적학생 수는 8,312명으로 2014년에 비해 약 800여 명(10.7%)이 증가하였다. 또한, 2015년에 정규교육기관이 배출한 정보보호 인력은 총 1,132명으로, 전문대학 108명, 대학 613명, 대학원 411명이다. 대학의 경우는 41% 증가하고, 대학원의 경우는 46% 증가하며 높은 증가율을 기록하였다.

금융보안원은 주요업무로 통합보안관제, 침해사고 대응, 취약점 분석평가, 보안성 검토, 금융보안적합성 시험,

핀테크 보안, ISMS인증, 개인정보 비식별 조치 지원, 정책 및 기술연구, 금융보안 표준화, 금융보안교육 업무를 수행하며 금융보안 교육에 증진하고 있다.

나. 국내 금융보안 대학원 교육현황

고려대학교 정보보호대학원은 금융보안 리스크관리 전문가, 금융사고 조사전문가, 금융 개인정보보호 전문가, 금융보안 시스템관리 전문가 육성을 위해 금융보안학과를 개설하였다.

연세대학교 정보대학원은 융합형 금융보안 전문가로써 전사적 관점에서 통합된 금융 IT 보호 전략 및 관리정책을 수립할 수 있는 능력 배양을 하며 금융보안 조직을 운영하며 금융 IT 보호 기술·관리 전문가 양성하기 위해 정보보호학과를 개설하였다.

국민대학교 일반대학원은 금융정보보안 관련 문제를 연구하고 이를 학문적·실무적으로 응용 및 확장할 수 있는 전문성과 국제 경쟁력을 겸비한 금융정보보안 전문인력을 양성하고, 변화하는 정보보안의 취약점을 극복하며, 창의 금융 서비스를 선도하는 핵심 인력 양성을 목표로 하고, 금융과 지식정보보안 관련 지식을 결합하여 금융기업에서의 미래 정보기술 환경에 능동적으로 대처할 수 있는 금융정보보안 전문가를 목표로 금융정보보학학과를 개설하였다.

건국대학교 정보통신대학원은 금융과 IT가 접목되면서 생기는 다양한 연구주제를 다루고, 그 방법론과 모형개발 그리고 실무에 제시하는데 목적을 두었으며, 또한 최근의 개인정보 유출과 금융사고에 따라, 금융과 정보기술(IT)을 두루 아는 금융IT 융합전문가 육성을 위하여 금융IT학과를 개설하였다.

5. 금융보안 전문인력 양성 및 활용의 문제점

금융보안 인력 양성은 단기 전문교육을 통한 양적 확대에 치중하고 있으며 특히 각 교육기관에서는 금융보안에 대한 학과 및 커리큘럼이 매우 부족한 상황이다. 이러한 상황에서 앞서 설명한 금융보안 전문가 수요현황 및 수요전망과 각 대학 및 교육기관 등을 통하여 배출되는 신규 및 경력 채용인력들에 대한 객관적 검증체계가 없어 금융과 보안에 대한 전문지식의 낮은 수준으로 인한 여러가지 피해가 발생 시킬 수 있다.

또한 정보보호 전문인력 공급의 지역적 불균형이 존재한다. 독립적인 정보보호 학과의 대부분은 지방 대학에 개설되어 있는 반면, 수도권 대학에서는 정보보호 학과는 소수인 것을 알 수 있다. 이는 수도권의 우수한 정보보호 전문인력 양성에 구조적 제약으로 작용 할 수 있다[12].

Ⅲ. 국내외 유사 전문자격의 비교분석

1. 국내외 자격현황

국가자격(정보보안기사, 정보관리기술사, 정보처리기사, 정보통신기사 등), 국가공인민간자격(SIS, ISA), 민간자격(CPPG), 국제공인자격(CISA, CISSP)에 대한 시행횟수, 합격인원 등 자격 운영현황을 살펴볼 때, 상당히 많은 자격 보유자가 배출되고 있으며 금융보안 관점에서 잠재적 수행인력이 될 수 있는 대상임을 생각할 수 있다.

2. 자격제도 사례 분석

가. 국가자격

정보보안 분야의 국내 국가자격의 경우 한국인터넷진흥원(KISA)에서 시행한 정보보안기사가 유일하다. 2001년부터 정보보호전문가(SIS)라는 명칭으로 국가민간자격으로 시행되었으나 2013년 10월부터 국가공인자격으로 승격되었다.

정보보안 기사, 산업기사 국가기술자격은 IT 및 정보통신 기술에 대한 이론 및 실무지식을 바탕으로 정보보안 시스템 및 솔루션 개발, 주요 운영체제 및 네트워크 장비, 정보보안 장비에 대한 운영 및 관리 직무를 담당하며 정보보안 기사는 추가로 조직의 정보보안정책의 수립과 대책수립 및 관리, 정보보호 관련 법규 적용 등을 수행한다.

나. 국가민간자격

한국정보화진흥원(NIA)에서 시행하고 있는 국가민간자격인 정보시스템감리사는 급증하고 있는 감리 수요의 충족과 민간 부문의 감리 활성화를 위하여 1997년부터 정보시스템 감리인 양성교육을 하였고, 2001년부터 자격검정을 하고 있으며, 매회 1회 검정 시험이 진행되고 있다. 정보시스템 감리를 수행할 전문 인력의 확보와 민간부문 정보시스템 감리의 활성화 및 정보시스템의 부실방지와 품질향상을 위해 정보시스템의 모든 제반 절차 및 산출물을 전체적으로 점검후 평가하여 관계자들에게 개선사항을 권고하는 목적을 두고 시행된 자격제도이다.

다. 국제공인자격

공인정보시스템감사사(CISA)는 ISACA에 의하여 1969년부터 운영된 자격증으로 정보시스템감사통제협회(ISACA)에서 운영해오고 있다. 전 세계적으로 118,000여 명이 보유하고 있다. 컴퓨터 시스템의 유효성과 효율, 신뢰성, 안전성을 확보하기 위해 독립적인 입장에서 일정한 시스템 감사 기준에 의거하여 시스템을 종합적으로 점검 ·평가하고, 관계자에게 조언 및 권고하는 목적으로 자격제도를 운영하고 있다.

공인정보시스템보호전문가(CISSP)는 ISC2에서 주관하는 자격증이다. 1989년 ISC2가 설립됨에 따라 시행되었으며, 2004년 ISO/IEC 17024 인증을 획득하여 국제 표준 자격증으로 운영되고 있다. ISC2의 2011년 연간보고서에 따르면 2011년까지 전 세계의 CISSP 보유자는 20,000명에 달하는 것으로 나타나 있으며, 2010년 말 현재 우리나라에는 약 2500명이 CISSP 자격증을 보유하고 있는 것으로 집계되고 있다. 보안과 위험관리, 자산보안, 보안엔지니어링, 통신과 네트워크 보안, 신원과 접근관리, 보안평가와 검사, 운영보안, 소프트웨어 개발보안이 주요과목이다.

3. 시사점

가. 운영목적 관점

금융보안 전문자격의 경우, 자격운영의 주된 목적은 금융보안 전문가의 체계적 양성이 주된 목적이 될 것인데, 전문가가 되기 위해 갖추어야 할 지식과 기술 등을 단계별로 갖추도록 자격제도가 운영되어야 할 것이다. 또한 현재 우리나라의 정보보안기사 자격제도는 일본의 정보보안기술사와 유사하게 재인증을 요구하지 않고 있으므로 ISO/IEC 17024에 따른 국제인증은 불가능하다[13]. 이에 따라 추후 국제인증 및 보수교육 등을 통하여 시대의 흐름에 뒤처지지 않는 인증이 필요하다.

나. 자격의 활용도 관점

신뢰성 유지를 위해서 국가 인증의 자격증 제도가 필요한데 보안산업의 경쟁력 회복을 위해서 초급과 고급을 이어주는 경력 경로를 만들어 주고 이들에 대한 적정한 처우개선을 통해 금융 보안인력이 안정적으로 직무에 충실할 수 있는 기반을 조성해줄 필요도 대두되고 있다[11].

금융보안 전문자격의 경우, 업무 수행을 위한 금융업과 IT기술 및 보안 처리전반의 이해가 요구되는 기사수준의 자격이면서도 CISO 및 관리자의 자격을 검증할수 있는 전반의 관리와 판단, 자문과 지도가 필요한 만큼 기술사 수준에 맞는 자격체계가 되어야 한다.

다. 검정기준 관점

금융보안 전문자격의 경우, 이와 같이 동일한 유사자격의 지식과 스킬을 토대로 하면서 금융보안업무에서 요구하는 지식을 작업 단위별로 도출하는 방식으로 지식과 스킬을 개발할 수 있는데, 정보관리기술사나 정보시스템 감리사와 같이 기술사 수준의 작업 업무들은 금융보안 쪽에서도 기술사 수준으로 요구하는 지식이나 스킬로 연결되는 경우가 많았고, 그 외 지식들은 작업단위로 도출해야 하는 지식이나 스킬로 도출됨을 알 수 있다.

라. 검정방법 관점

금융보안 전문자격의 경우, 실무진과 CISO등의 직급별 체계로 인한 기존 자격제도인 기사와 기술사 수준을 요구하지만 국가자격의 검정방법과 같이 필기와 더불어 실기 혹은 논문형 실기가 필요한 것인지, 면접 또한 필요한 것인지를 보다 복합적인 관점을 통해 고려해 보아야 할 것이다.

마. 검정과목 관점

금융보안 전문자격의 경우, 전산관리에 요구되는 지식과 스킬뿐만 아니라 금융업의 전반을 다루는 기본지식과 보안업무를 실무로 처리할 수 있는 지식과 스킬을 요구하므로 이에 맞는 과목구성이 필요하다. 특히 금융보안 자격이 정해진 양식에 따라 질문답 형식으로 허술하게 수행되어 그 결과에 대해서도 신뢰가 떨어지지 않도록 하기 위해서 IT전반의 기초지식을 검정하는 과목 구성 또한 고려할 필요가 있다.

검정과목에 대해서는 앞서 설명한 금융보안원의 교육 커리큘럼의 내용과 금융감독원의 IT검사 매뉴얼 중 평가항목 및 점검사항의 내용을 참고하여 과목선정에 설계를 한다면 검정과목 선정에 있어 선제적인 도움이 될 수 있다.

바. 응시자격 관점

금융보안 전문자격의 경우, 기사와 기술사 수준의 자격제도로 운영될 것을 고려하거나 국가자격 형태로 발전할 것을 감안한다면 이와 유사한 응시자격 규정이 되어

야 할 것이다. 기술사 수준의 검정 경력을 과도하게 길게 책정한다면 고급인력 양성에 걸림돌이 될 수 있어 이를 감안해야 한다. 또한, 검정과목과 방법에 따라 단계별 응시절차를 둘 것인지를 고려해야 할 것이다.

미국에서는 국가안보국과 국토안보부가 중심이 되어 학제간 성격을 갖는 정보보안 교육 프로그램을 개발하고 이를 인증함으로써 인력 양성을 위한 기반구조를 구축하고 있으며, 이러한 인증프로그램에 가입된 140여개의 대학 및 대학원 재학생과 졸업생에게 공공기관 우선 채용 등 많은 인센티브를 제공하고 있다[14].

사. 인력 관점

다른 자격증제도와 마찬가지로 금융보안 전문인력의 경력관리, 프로젝트 계획시 인건비 추정, 내부 인적자원 관리에의 활용, 직무수준의 평가 등 다양한 목적으로 활용될 수 있다[15].

높은 이직률/퇴사율, 그리고 기업 측 이슈와 중복되는 보안 인력의 과도한 업무량이 이슈로 부각되었으며, 이에 대한 대안으로는 개인들의 장기적 관점에서의 자기개발 및 커리어 구축이 필요하다는 점이 도출되었다[16].

Ⅳ. 직무분석

1. 직무분석 단계

금융보안자격의 직무분석은 직무 분석준비, 직무모형의 두 단계로 수행하였다. 각 단계의 직무분석 방법은 금융보안 자격/검정 체계 설계를 목적으로 수행하였으며, 목적 달성을 위한 유의미한 결과 도출을 위하여 구체적인 기준과 방법을 적용하였다.

2. 직무분야 및 직무정의

금융보안이란, 「기존 IT보안의 범위에서 조금 더 특화된 환경인 금융권에서의 해킹 등 사이버공격에 대비하고 IT에 대한 지식 뿐만 아니라 컴플라이언스와 금융서비스 전반에 대한 높은 이해를 요구하는 융합보안」을 말한다. 현재 금융보안을 전담할 수 있는 자격종목이 개설되어 있지 않기 때문에 정보기술, 정보통신, 정보보호 또는 소프트웨어 보안 취약점 진단원 자격 소지자들이 대신 업무를 수행하도록 제도적 인정기준을 마련하고 있어 전문성 또는 신뢰성 측면의 여러 가지 문제점이 제기되고 있다. 그러므로 금융보안 전문 인력 양성을 위한 금융보안 전문자격 종목의 개발은 매우 중요하다.

금융보안 전문가는 금융권의 보안전략을 수립하고 금융권의 관련 제도,법 등의 고도의 전문지식을 가지고 IT 기반의 취약점 진단 및 보완등을 수행하여 종합적으로 컨설팅을 하는 등의 업무를 수행하는 인력을 말한다.

3. 직무모형

직무분석을 통해 나타난 직무모형은 다음과 같이 제시하였다. 금융보안 전문가의 책무는 4가지로 구성된다. 첫째는 금융권의 물리적 안전 및 보안관리, 둘째는 자산관리 및 신탁조직의 보안운영, 셋째는 자금세탁, 사기위험 탐지 및 모니터링 등 금융범죄 예방 및 조치 운영, 넷째는 신용거래/예금/은행운영/금융범죄/개인정보등의 컴플라이언스 관리운영, 이때 책무의 특성과 내용을 고려하여 총 22개의 작업영역이 결정되었다.

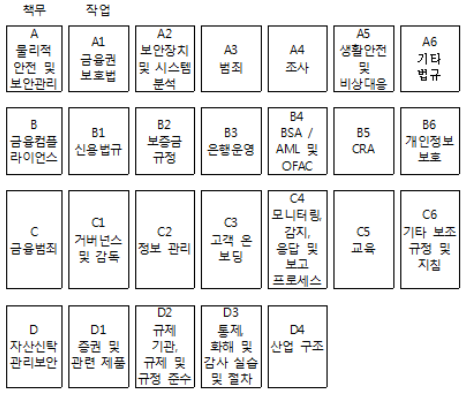

그림 1. 직무모형
Fig. 1. Job model

Ⅴ. 금융보안 전문자격제도의 설계와 쟁점

보안 대책의 필요성과 중요성을 감안할 때 정보보호 분야의 인력을 집중 양성하는 것은 국가적으로 올바른 정책이라고 볼 수 있다[17]. 비전문적인 금융보안 인력은 국민 편의와 공익을 심각하게 저해한다는 측면과 금융보안 전문가 저변확대 측면을 고려하였을 경우 국가자격으로의 추진을 지향한다. 그리고 금융기관의 보안 관리를 도모할 수 있는 자체 전문인력 양성과 금융기관과 협력

중인 협력사 직원 및 신규직원의 다양한 인력을 양성한다는 측면에서 민간자격을 추진할 수 있을 것이다.

1. 국가자격

국가자격은 국가(전문)자격과 국가(기술)자격으로 나뉘며 국가(전문)자격은 개별법에 의하여 시행되는 자격으로 해당 소관부처 및 산하 소속기관에서 주관한다. 또한 국가(기술)자격은 국가기술자격법에 의하여 운영되는 자격으로 기술・기능분야(기술사・기능장・기사・산업기사・기능사)와 서비스분야(1급・2급・3급・단일종목)로 구성되어 있다.

국가자격은 모두 법에 근거하여 시행되는 자격증이므로 금융보안 전문자격증을 국가자격으로 추진하기 위해서는 법률 제정이 우선시 되어야 한다.

국가가 직·간접적으로 금융보안 자격에 대해 관리·통제를 하는 이유는 다음과 같이 몇 가지로 요약해 볼 수 있다.

첫째, 자격증 제도 도입은 일반 소비자와 사용자들을 보호한다는 산업안전의 측면이 있다. 구조나 토목, 교량 등의 분야에는 고급자격증의 참여가 절대적이다. 같은 맥락에서 의료, 통신, 선박, 항공 등 다양한 분야에서 대중과 사용자의 안전에 관계되는 소프트웨어를 장착해야 하는 경우 엄격한 품질유지가 요망되는데 이런 경우 금융보안 자격제도는 최소한의 안전도 제고에 기여할 수 있다.

둘째, 금융보안 자격제도는 보안 관련학과의 커리큘럼을 보다 체계적으로 구조화하고 새로운 기술개발의 결과를 가장 효율적으로 교육과정에 반영할 수 있는 도구이다. 일반적으로 자격증을 받기 위해서는 대학이나 인증받은 전문교육기관에서 소정의 교육과정을 이수하고 해당분야의 경험을 쌓은 후 , 시험을 거쳐 관련 협회나 인증기관의 추천을 받는 형식을 취한다. 자격증 제도는 전문가로서의 표준을 유지하며 또한 전문가로서의 행동윤리를 준수한다는 표시이다.

셋째, 정부가 공식적으로 인정하는 보건 위생이나 복지, 안전 분야에서의 법적 결과물인 면허와는 달리 인증은 금융보안 전문가들을 대상으로 치루는 특정 분야의 기본적인 지식과 기술을 검증하는 과정의 결과물이다. 금융보안 전문가가 인증을 받고자 하는 이유는 전문가로서의 지식과 식견 그리고 실천적인 기술을 보유하고 있다는 객관적인 증거가 될 수 있기 때문이다. 특히 대학이나 전문기관에서 공식적인 교육을 받지 못한 경우 이런 인증시험을 거쳐 전문가로서의 대우를 받을 수 있다.

마지막으로, 자격증별로 사용자 또는 소비자 그룹에게 일정 수준의 안전을 보장할 수 있는 금융보안을 제공하는데 일반적으로 달성가능한 수준의 실행능력을 정의함으로써 이런 목적을 달성할 수 있다는 것이다.

2. 민간자격

민간자격이란 국가 외 개인・법인・단체가 신설하여 관리・운영하는 자격을 말한다. 금융보안 전문자격을 민간자격으로 관리・운영 할 경우 비교적 간단한 등록절차로 인하여, 자격제도 활성화를 통한 직업 능력개발 촉진 및 사회경제적 지위향상을 도모할 수 있다.

3. 민간자격 국가공인자격

민간자격 국가공인자격제도는 정부가 민간자격에 대한 신뢰를 확보하고 사회적 통용성을 높이기 위하여 1년 이상, 3회 이상 검정실적이 있고, 법인이 관리・운영하며, 민간자격 등록관리 기관에 등록한 자격 중 우수한 자격을 자격정책심의회의 심의를 거쳐 공인하는 제도이다. 해당 자격제도는 국가공인 기준 과 같은 기준들을 만족해야 공인받을 수 있기 때문에 민간자격에 비해 자격에 대한 신뢰도가 높지만, 추가적인 심의를 통해 등록되므로 민간자격보다 많은 시간이 걸리는 단점이 있다. 금융보안 전문자격증을 민간자격으로 등록하여 국가공인 기준과 같은 기준들을 만족하여 개발 보안의 수요를 충족하고 이후에는 해당 자격을 소지한 전문가들의 전문성・신뢰성을 높이기 위한 민간자격 국가공인자격으로의 추진이 필요시 된다.

Ⅵ. 결 론 및 정책제언

금융 산업은 고객과의 신뢰를 기반으로 지속가능한 고객관계를 유지해야만 영속기업의 본질을 유지할 수 있다[18]. 2011년 잇따른 금융사고에 따른 금융위원회 회의에서 “금융 부문 자율보안체계 확립 방안 종합대책 마련”의 일환으로 국가의 금융보안 부분에 인력양성 등 금융업계의 산업경쟁력 및 보안의 원천으로 글로벌 수준의 금융보안 육성을 위한 노력이 강화되고 있다.

이러한 시점에서, 금융보안 산업을 이끌어나가기 위한

인력의 양성은 매우 시급하고, 금융상품의 복잡성과 정보보호의 중요성이 대두된 현 상황에서[19] 이에 대한 전문성 있는 기술력의 보유 여부가 산업의 경쟁력에 중요한 역할을 한다고 볼 수 있다. 우수한 보안 인력을 확보하기 위한 경쟁이 국내외적으로 심화되고 있고, 시장에서 요구되는 능력을 갖춘 보안인력에 대한 필요성이 증대되고 있어, 산업현장에서 요구되는 개인의 지식과 기술을 반영하고 이를 평가함으로써 개인의 능력 수준을 보장할 수 있는 자격제도의 신설 및 개선이 절실하다.

금융보안원에서는 기존 수행 업무인 보안관제, 침해대응, 취약점 분석・평가, 금융보안 정책・기술 연구, 금융보안 교육, 금융IT・보안 인증평가 등 보안서비스 제공 외에 금융보안 전문가 양성 및 평가를 위한 전문자격제도 도입을 제언해본다.

References

[1] Jung-hwan Lim, In-Seok Kim, “A study on Information Protection Manpower and Budget Adequacy for Cooperative-Type Financial Company's Federation”, The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 16, No. 3, pp. 29-38, Jun. 30. 2016.
DOI: http://dx.doi.org/10.7236/JIIBC.2016.16.3.29

[2] Financial settlement bureau, Bank of Korea, “Financial Information System in 2015”, Jun. 2016

[3] Digital Daily, “Strengthen financial security Strengthen internal control and secure professional manpower”, May. 2011

[4] Financial Security Institute, “Electronic payment service trends and implications report", Oct. 2014

[5] Kyung-in Kang, “Introduction to information security”, Seoul Oh Sung Media, 2012

[6] Dong-geun Lee, “Comparative Study of IT Security among Financial Institutions in Korea and Japan for Financial Security”, Dongguk University, May. 2014

[7] Knowledge Insight and Frontier, “Comprehensive Measures to Enhance Financial Data Security for Enhancing Electronic Financial Security”, Jul. 2013

[8] Seoul Economy, “Financial reform and training of security personnel”, Jul. 2016

[9] Knowledge Insight and Frontier, “Basic statistics of financial personnel and supply and demand forecast”, Financial Services Commission, Dec. 2015

[10] Wn-dong Sin, "Financial market, improvement of treatment of professional manpower to secure IT manpower", Korea Human Resources Strategy Institute, Jun. 2016

[11] Moon-Ju Kwon, Lin Choi, Yeon-Moon Na, Jung-Sun Kim, Yun-Seok Shin, "A Study on improvement of software qualification system", Korea Software Promotion Agency, 2008

[12] Jung-Deok Kim, Tae-Suk Bae, "Required knowledge and training certification program for training information security professionals", Journal of Digital Convergence, Oct. 2011

[13] Kyung-hee Oh, "Information Security Management Professional Qualifications", Korea Institute Of Information Security & Cryptology, Aug. 2015

[14] Jung-Deok Kim, “A Study on National Information Security Issues and Policy Measures”, The Society of Digital Policy & Management, Feb. 2012

[15] Moon-Ju Kwon, Min-Ha Kim, "An Exploratory Demand Analysis on the Establishment of National Technology and Certified Private Qualifications in Software Field", Korea Society of IT Services , Sep. 2009

[16] Kyoung-Jin Seo, Ji-Eun Choi, Hee-Woong Kim, "An Exploratory Study for Training Information Security Manpower", Korea Assocaition of Information Systems, Jun. 2015

[17] Kyu-Sung Noh, Tae-Hyun Ha, “An Exploratory Study on the Introduction of Electronic Commerce Security Professional Qualification System”, Korea Society Of Industrial Information Systems, Nov. 2000

[18] Eun-sun Choi, Kyung-Ho Lee,, "A Study on the Improvement of Efficiency by Improving Rule of Detection of Abnormal Signs in Electronic Financial Transactions", Korea Institute Of Information Security & Cryptology, June. 2015
[19] Chang-Rae Choi, Jang-Ho Yoon, Kyung-Ho Lee, "Research on IT contracting policy based on financial security risk", Korea Institute Of Information Security & Cryptology, Aug. 2014

저자 소개

정 희 형(정회원)

- 2007년 : 단국대학교 컴퓨터과학/경영정보학 학사
- 2017년 : 고려대학교 정보보호대학원 금융보안정책 석사

권 헌 영(정회원)

- 1999년 ~ 2005년 : 연세대학교 법학 박사
- 2002년 ~ 2006년 : 대통령자문 전자정부특별위원회 전문위원
- 2013년 ~ : 금융감독원 금융IT 전문가협의회
- 2014년 ~ : 행정자치부 정책자문위원회
- 2015년 ~ : 고려대학교 정보보호대학원 교수