정 보 보 호 학 회 지
제27권 제5호, 2017. 10

정보보안경영 전문가 자격요건 국제 표준화

오 경 희*

요 약

적절한 능력을 보유한 정보보안경영 전문가를 확보하는 것은 전세계적으로 많은 조직의 관심사가 되고 있다. 정보보안경영체계 관련 표준을 다루는 ISO/IEC JTC 1 SC 27/WG 1에서는 이러한 요구를 다루기 위하여 2014년 10월 ISO/IEC 27021 정보보안경영 전문가 자격 요건에 대한 국제표준을 개시하였으며 3년에 걸친 노력 끝에 FDIS 투표가 성공적으로 완료되어 국제 표준 발표를 앞두고 있다.

정보보안경영 전문가 자격 요건은 크게 업무 경영 자격과 정보보안 자격의 2개의 범주 나누어지며 각각의 범주에 12개의 자격(능력)을 포함하고 있다. 본 논문에서는 이 24개의 자격(능력)의 내용을 소개하고 그 함의와 향후의 전망을 논한다.

Ⅰ. 서 론

전세계적으로 보안사고가 급증하고 이에 의한 피해 규모가 증가함에 따라, 조직의 정보보안 경영체계를 수립, 운영하고 정보보안 사고에 적절히 대응하기 위한 능력 있는 정보보안경영 전문가를 확보하는 것이 많은 조직의 관심사가 되고 있다. 정보보안경영체계(ISMS) 관련 요구사항, 방법, 절차 등의 표준화를 수행하고 있는 ISO/IEC JTC 1 SC 27 WG 1에서는 이러한 시장의 요구를 다루기 위하여 2012년부터 연구를 시작하였으며 2014년 10월 멕시코 회의에서 ISO/IEC 27021 ISMS 전문가 자격 요구사항(Competence requirements for information security management systems professionals)[1]로 정식 표준화 과제를 시작하였으며, 현재 FDIS 투표를 끝내고 IS 발표를 앞두고 있다.

본 표준이 개시되기 전의 상황은 기존 국제 표준 중에서 ISO/IEC 27006 정보보안경영시스템의 감사 및 인증을 제공하는 기관에 대한 요구사항(Requirements for bodies providing audit and certification of information security management systems)[2]이 ISMS 감사인에 대한 자격 요건을 제공하고 있었다. 한편 시장에서는 CISSP(Certified Information Systems Security Professional), CISM(Certified Information Security Manager), 유럽의 e-CF Security Adviser[3] 등 여러 정보보안 자격증이 존재하고 있었다. 이에 따라 과연 정보보안 전문가에 대한 표준이 필요한지에 대한 연구기간(study period)이 진행되었다.

연구기간 중 대다수의 전문가들은 자신들의 경험에 기초하여 “정보보안경영 전문가들의 가장 큰 현안은 경영진을 설득하는 것이며 비즈니스 경영진의 관점에서 정보보안의 효익을 제시하고 지속적으로 보안에 투자할 수 있도록 이끄는 것”이라고 답했다.

기존의 ISMS 감사인 자격은 결과를 평가하는 지식과 기량은 포함하지만 이를 만들어 내기 위한 지식과 기량은 포함하지 않고 있다. 또한 시장에 존재하는 기존의 자격 검증은 정보보안의 기술적인 측면에 치중하고 있었다. 이에 따라 실제 컨설턴트 또는 정보보안 관리 담당자/책임자를 고용하는 고객 기관에서 자격증을 획득한 인력을 고용하더라도 이들이 고객 기관의 업무 측면을 이해하지 못하거나 의사소통에 한계가 나타나는 경향이 있었다. 이러한 문제를 해결하기 위해서는 일반적인 업무에 대한 이해와 지식, 의사소통 기량이 필요하다고 보는 입장이 대다수를 점함으로써 신규 표준의 필요성이 정당화되었다.

특히 ISO/IEC 27001에 따른 정보보안경영시스템을 수립, 구축, 운영, 개선하기 위해서는 좀 더 경영시스템의 수립 및 운영에 관한 조직적, 인적, 업무적 측면에 대한 이해가 강조되어야 한다는 요구가 높았다. ISO/IEC

이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(정보보안경영전문가 자격기준 국제표준화)

* TCA 서비스 대표 (khoh@tcaservices.kr)

27021은 이러한 요구를 만족시키기 위하여 개발되었다.

본 논문에서는 이 신규 국제 표준이 다루고 있는 내용을 소개하고 이 표준이 가지고 있는 의미와 향후 대응 방안을 언급하고자 한다.

Ⅱ. ISO/IEC 27021의 내용

2.1. 개요

ISO/IEC 27021은 ISMS 전문가에 대한 자격 요구사항을 제시한다.

Management라는 단어는 일반적으로 '경영'이라고 번역되나 정보보안 분야에서는 '관리'라고 번역되기도 한다. ISMS의 경우 국내에서는 '정보보호관리체계'라고 일반적으로 사용되지만 ISO/IEC 27001의 부합화 표준의 제목에서는 환경, 품질 등에서 사용되는 용어에 따라 '정보보안경영시스템'이라는 용어를 사용하고 있다. 본 논문에서는 사용되는 용례에 따라 '경영'으로 번역하기도 하고 '관리'로 번역하기도 하였다. Competence 역시 표준 용어에서는 '자격'으로 번역되지만 세부항목에서는 '능력'으로 번역하는 것이 한국어 문장에서는 더 자연스럽기 때문에 세부 항목에서는 '능력'이라는 용어를 사용하였다.

4장에서는 ISMS 자격에 대한 개념과 본 표준의 구조를 설명하고 있다.

ISMS 전문가가 보유해야 할 자격은 모든 경영 시스템에 공통적으로 필요한 업무 경영 관련 자격(business management competence)과 정보보안 분야의 업무 수행을 위한 자격(information security competence)으로 나누어 볼 수 있다. 본 표준에서는 5장에서 업무 관리 자격을 설명하고 있으며, 6장에서는 정보보안 자격을 설명하고 있다.

부록에서는 ISMS 지식 체계(body of knowledge) 개발의 일환으로써 지식 키워드를 제공하고 있다.

2.2. ISMS Competence의 개념

자격(competence)은 본 표준의 3.1에서 "의도한 결과를 성취하기 위해 지식과 기량(skill)을 적용하는 능력"이라고 정의하고 있다.

이 정의는 ISO/IEC 17024 적합성 요구사항 - 사람의 인증을 운영하는 기관에 대한 일반 요구사항(Conformity assessment - General requirements for bodies operating certification of persons)[4]에서 정의된 것으로 ISO 19011 감사관리 시스템을 위한 지침(Guidelines for auditing management systems)[4]에서도 감사인에 대한 자격을 언급하기 위하여 이 정의를 따르고 있다.

이에 따라 본 표준에서는 세부적인 자격을 정의하기 위하여 의도한 결과, 필요한 지식, 필요한 기량의 측면에서 자격을 서술하는 구조를 갖는다. 또한 이 자격은 ISMS를 수립, 구축, 운영, 개선하는 전문가를 위한 것이기 때문에, 각 자격마다 ISO/IEC 27001 세부 조항과의 연결성을 명시하고 있다.

ISO는 다양한 경영시스템 표준을 개발하고 있다. 정보보안 뿐만 아니라 품질관리, 시설 관리(facility management), 서비스 관리, 환경관리 등 다양한 경영시스템이 존재하며, 이들은 한 조직 내에서 운영될 수 있다. 이러한 원칙에 따라 2015년 이후 ISO에서 개발되는 경영시스템 표준들은 공통의 구조와 공통 요구사항을 가지고, 각 절 하에서 분야별 요구사항을 추가하는 형태로 개발되고 있다.

이러한 원칙에 따라 ISMS 전문가의 자격 역시 크게 경영시스템에 공통된 측면과 정보보안 특유의 측면 2개의 범주로 나누어 질 수 있다. 다른 분야의 전문가 자격을 구성한다면, 이들 각각은 경영 시스템에 관련된 자격을 공유하면서 해당 분야 특유의 자격으로 구성된다. [그림 1]에서 이러한 관계를 그림으로 도시하였다.

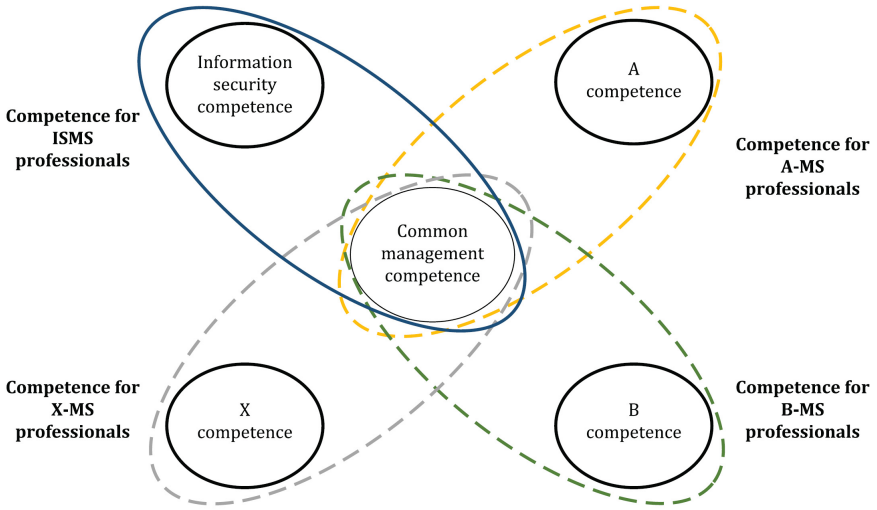
2.3 업무 경영 자격

본 표준에서는 경영시스템에 관련된 공통 자격을 업무 경영 자격(Business management competence)라고 부르고 있다. 이 범주에는 12개의 능력이 포함된다.

2.3.1. 리더십

리더십 능력을 통해 달성하고자 하는 결과는 정보보안을 제공하기 위해 전 조직에 걸쳐 직원들을 지시, 동기부여 및 격려하는 것이다.

관련 지식으로는 리더십 이론, 협상 기법이 필요하며, 약속을 준수하고 조직의 다양한 수준에서 책임과 권한을 효율적으로 배정하는 등의 기량이 요구된다.



〔그림 1〕 ISMS 자격과 공통 및 분야별 자격의 관계

2.3.2. 의사소통

의사소통 능력을 통해 달성하고자 하는 결과는 정확한 정보를 간결한 방식으로 관련 당사자와 공유하고 정보보안에 관해 조직의 경영진과 가장 생산적인 상호작용을 가능하게 하는 것이다.

관련 지식으로는 소통 이론, 이해당사자 분석 기법, 소통 기법 등이 필요하며, ISMS 관련 내외부 소통 필요성을 결정하고 소통 프로세스와 채널 설계, 최고 경영진과 업무 전문가들과 관계 수립, 적절한 언어와 매체를 사용하여 다양한 청중과 소통하는 기량이 요구된다.

2.3.3. 사업전략과 ISMS

이 능력을 통해 달성하고자 하는 결과는 업무 전략이 구성되는 방법을 이해하고 정보보안 및 ISMS 전략을 전반적인 업무 전략에 맞추는 방법을 이해하는 것이다.

관련 지식으로는 업무 전략 및 전략 수립 프로세스, 전략 수립 기법 등이 필요하며, 업무 및 그 전략의 맥락에서 정보보안 목표를 수립하고 전략적 방향을 제시하고 자원 할당을 지원하는 등의 기량이 요구된다.

2.3.4. 조직 설계, 문화, 행동, 및 이해관계자 관리

이 능력을 통해 달성하고자 하는 결과는 ISMS 구현이 조직의 구조 및 문화와 일치하도록 하는 것이다.

관련 지식으로는 조직 설계 이론, 조직 문화 이론, 조직 행위 접근방법, 방법론 및 프레임워크, 갈등관리 이론 등이 필요하며, 조직 설계, 조직 행동을 이해하고 조직의 문화를 분석 및 평가하고 이해관계자들의 다양한 요구를 조정하는 등의 기량이 요구된다.

2.3.5. 프로세스 설계 및 조직 변화 관리

이 능력을 통해 달성하고자 하는 결과는 정보보안 관련 일상 활동의 성과를 만들어 내는 것이다.

관련 지식으로는 프로세스 설계 방법론 및 프레임워크, 조직의 상황, 변경관리 방법론 및 프레임워크 등이 필요하며, 정보보안 목표를 달성하기 위한 계획을 감독하고 조직 및 외주 프로세스를 지휘 관리하며 변화관리와 기록 관리 등의 기량이 요구된다.

2.3.6. 인적 자원, 팀 및 개인 관리

이 능력을 통해 달성하고자 하는 결과는 개인, 팀 및 전체 인력의 개발 필요를 다루기 위해 선행 활동을 수행하고 조직의 프로세스를 개발하는 것이다.

관련 지식으로는 능력 및 기량의 필요성 분석, 평가 시스템 및 프로세스에 대한 방법, 학습 및 개발 지원 방법, 관련 자격증 지식 등이 필요하며, 조직 및 개인의 목적, 목표 및 세부목표를 수립하고 연계, 권한 이양 등의 전략을 이해하고 활용하는 등의 기량이 요구된다.

2.3.7. 위험관리

이 능력을 통해 달성하고자 하는 결과는 위험 관리 방법론, 프레임워크 및 결과를 이해하는 것이다.

관련 지식으로는 업무 위험관리 방법론 및 프레임워크, 위험 평가 및 처리, 조직이 운영되는 법규 환경 지식 등이 필요하며, 위험의 정의와 실제 시나리오에서의 구성요소에 대한 이해, 다양한 분석 및 처리 방법, 결과를 설명하기 위한 기량 등이 요구된다.

2.3.8. 자원 관리

이 능력을 통해 달성하고자 하는 결과는 적절한 재무적 자원에 대한 요구가 실행되고 정보보안 목표와 연계되도록 보장하는 것이다.

관련 지식으로는 재무보고 및 측정, 예산 수립 및 관리 기법, 비용 관리 및 감소 기법 등이 필요하며, 구현 및 운영 비용을 모두 포함하는 예산 수립, 현금 흐름 및 이익과 손실을 포함하는 재무 보고의 이해, 비즈니스 케이스 및 투자 케이스 작성 등의 기량이 요구된다.

2.3.9. 정보시스템 아키텍처

이 능력을 통해 달성하고자 하는 결과는 조직의 정보의 생성, 저장, 처리, 전송 및 폐기에 적용가능한 정보시스템 아키텍처를 이해하는 것이다.

관련 지식으로는 정보시스템 아키텍처 요구사항, ICT 응용과 업무 프로세스의 통합 및 의존성, 시스템 개발 방법론 등이 필요하며, 업무 목표와 정보시스템에 영향을 미치는 동인을 이해하고 보안과 정보시스템 아키텍처와의 상호작용 이해 등의 기량이 요구된다.

2.3.10. 프로젝트 및 포트폴리오 관리

이 능력을 통해 달성하고자 하는 결과는 다양한 ISMS 관련 프로젝트와 활동들을 관리하여 적시에 예산 및 품질을 만족하는 결과를 산출하는 것이다.

관련 지식으로는 프로젝트 및 포트폴리오 관리 방법론 및 프레임워크, 활동계획 수립 도구 지식 등이 필요하며, 업무부서와 협력하여 ISMS 관련 투자 프로젝트의 포트폴리오를 관리하고 여러 부서에 걸친 팀 내에서 작업할 수 있는 등의 기량이 요구된다.

2.3.11. 공급자 관리

이 능력을 통해 달성하고자 하는 결과는 조직 내에서 공급자 및 공급 사슬의 역할 및 정보보안의 영향을 이해하는 것이다.

관련 지식으로는 공급자 및 공급 사슬의 활용, 평가 및 정보보안에 미치는 영향 평가, 공급자 관리, 공급자 관계의 수립, 평가, 선정, 관리 및 종료에 관한 정보보안 지침을 제공하는 등의 기량이 요구된다.

2.3.12. 문제 관리

이 능력을 통해 달성하고자 하는 결과는 ISMS에 영향을 미치는 문제를 적시에 식별하고 해결하는 것이다.

관련 지식으로는 문제 해결 및 분석 방법론 및 프레임워크에 관한 지식이 필요하며, 정보 및 데이터의 분석과 종합, 경영 문제를 분석적으로 기술, 분석적 접근 방법의 적용 및 문제 해결방안 제안, 이를 관련 이해당사자에게 제시하고 설명하는 등의 기량이 요구된다.

2.4 정보보안 관련 자격

정보보안 관련 자격 역시 12개의 능력으로 이루어져 있으나 이들은 6개의 하위 영역으로 나누어진다. 1) 정보보안, 2) 정보보안 계획, 3) 정보보안 운영, 4) 정보보안 지원, 5) 정보보안 성과 평가, 6) 정보보안 개선이 그것이다. 각 영역은 1 ~ 3개의 세부 능력을 포함한다.

2.4.1. 정보보안

정보보안 영역에는 정보보안 거버넌스와 조직의 상황 2개 능력이 포함된다.

1) 정보보안 거버넌스를 통해 달성하고자 하는 결과는 ISMS에 대한 상위수준의 방향을 제시하는 것이다.

관련 지식으로는 업무 및 기업 거버넌스, 정보보안 거버넌스 프레임워크, 관련 표준 및 법 규제 현안에 관한 지식이 필요하며, 업무 거버넌스를 지원하고 연계되는 정보보안 거버넌스 프레임워크를 설계, 구현, 유지, 역할 및 책임 정의 등의 기량이 요구된다.

2) 조직의 상황 관련 능력을 통해 달성하고자 하는 결과는 ISMS에 영향을 미칠 수 있는 내외부 현안을 식별하는 것이다.

관련 지식으로는 분석 방법론 및 프레임워크, 조직 문화, ISMS가 구현될 조직의 상황 등이 필요하며, 이해관계자를 결정하고 이들의 요구사항을 식별, ISMS의 범위, 경계 및 적용성, ISMS의 목적, 효익, 결과를 이해관계자들과 소통하는 등의 기량이 요구된다.

2.4.2. 정보보안 계획

정보보안 계획 영역에는 ISMS 범위와 정보보안 위험 평가 및 처리 2개 능력이 포함된다.

1) ISMS 범위 능력을 통해 달성하고자 하는 결과는 계획에서 구현에 이르기까지 정보보안의 공통 목표를 위한 전략적 방향을 제시하는 것이다.

관련 지식으로는 정보보안 목표, 정보보안 거버넌스 및 정책, 계획 수립 등이 필요하며, ISMS 범위 정의, 모든 관련 기능 및 모든 수준에서 정보보안 정책과 일관성 있는 정보보안 목표 수립 등의 기량이 요구된다.

2) 정보보안 위험 평가 및 처리 능력을 통해 달성하고자 하는 결과는 정보보안 경영시스템 범위 내에서 효과적으로 정보보안 위험을 관리하는 것이다.

관련 지식으로는 정보보안 위험평가/처리 방법론 및 프레임워크, ISO 31000 및 27005와 같은 관련 국제 표준에 대한 지식 등이 필요하며, 정보보안 위험을 평가하고 위험 관련 활동을 ISMS 프로세스에 통합하고 구현하는 등의 기량이 요구된다.

2.4.3. 정보보안 운영

정보보안 운영 영역에는 정보보안 운영 능력 하나만이 포함된다. 이 능력을 통해 달성하고자 하는 결과는 정보보안 관련 프로세스를 효과적이고 효율적으로 운영하여 성과를 만들어 내는 것이다.

관련 지식으로는 정보보안 관련 통제의 관리 방법, ISO 27002 표준 등에 관한 지식이 필요하며, 외주 포함 정보보안 프로세스/운영을 측정, 기타 업무 프로세스/운영 내에서의 정보보안 측정 등의 기량이 요구된다.

2.4.4. 정보보안 지원

정보보안 지원 영역에는 정보보안 인식, 교육 및 훈련과 문서화의 2개 능력이 포함된다.

1) 정보보안 인식, 교육 및 훈련 능력을 통해 달성하고자 하는 결과는 ISMS 범위 내의 업무 수행자들에게 정보보안 문화를 보급하는 것이다.

관련 지식으로는 정보보안 인식, 교육 및 훈련 접근 방법 및 기법 등이 필요하며, 교육 및 인식 프로그램을 수립하고 민감한 정보시스템의 보안 상태에 대한 인식을 유지, 정보보안 문화를 지원하기 위한 집행 메커니즘을 평가하고 제안하는 등의 기량이 요구된다.

2) 문서화 능력을 통해 달성하고자 하는 결과는 ISMS 문서의 생명주기를 통제하는 것이다.

관련 지식으로는 ISMS에 필요한 문서, 문서의 생성, 편집, 배포 도구, 분서 버전관리 도구 및 기법 지식 등이 필요하며, ISMS를 위한 문서 인벤토리의 생성 및 변경, 문서 변경관리 및 버전 통제 등의 기량이 요구된다.

2.4.5. 정보보안 성과 평가

정보보안 성과 평가 영역에는 ISMS 모니터링, 측정, 분석 및 평가와 ISMS 감사, 경영진 검토의 3개 능력이 포함된다.

1) ISMS 모니터링, 측정, 분석 및 평가 능력을 통해 달성하고자 하는 결과는 정보보안의 성과와 ISMS의 효과성을 평가하는 것이다.

관련 지식으로는 모니터링 및 측정 특성, 정성적 및 정량적 데이터를 집약하고 제시, 추세분석 지식 등이 필요하며, 평가 기준 및 프로세스를 수립하고 조직의 프로세스가 정보보안 정책에 따라 구현되었는지 모니터, 측정, 평가하는 등의 기량이 요구된다.

2) ISMS 감사 능력을 통해 달성하고자 하는 결과는 내외부 관련 규정에 따라 정기적으로 ISMS 준수 수준을 평가하는 것이다.

관련 지식으로는 정보보안 감사 방법론 및 프레임워크, 내외부 감사 프로세스 및 절차, 정보보안 평가 지식 등이 필요하며, 내부 ISMS 감사 관리, 감사 발견사항, 권고사항 및 요점을 처리하기 위해 필요한 자원을 포함하여 개선 계획을 제안하는 등의 기량이 요구된다.

3) 경영진 검토 능력을 통해 달성하고자 하는 결과는 ISMS의 지속적 개선, 적절성 및 효과성을 보장하는 것

이다.

관련 지식으로는 재무보고 및 측정, 예산관리기법, 비용 관리 기법 등이 필요하며, 검토 주기 결정, ISMS 목표, 예산, 사업 척도를 검토하고 적절한 조치를 확인, 경영진 검토 회의를 효과적으로 주도하고 적절한 이해 관계자와 소통하는 등의 기량이 필요하다.

2.4.6. 정보보안 개선

정보보안 개선 영역에는 지속적 개선과 기술 추세 및 개발의 2개 능력이 포함된다.

1) 지속적 개선 능력을 통해 달성하고자 하는 결과는 ISMS의 모든 핵심 측면을 적시에 지속적으로 개선하는 프로세스를 수립하는 것이다.

관련 지식으로는 지속적 개선 방법론 및 프레임워크가 필요하며, 현재의 ISMS를 유지할 것인지를 판단, 교정활동 제안, 교정 활동의 효익과 비용 및 업무 중단의 균형 유지, ISMS 적정성, 적절성 및 효과성 개선 메커니즘 제안 등의 기량이 필요하다.

2) 기술 추세 및 개발 능력을 통해 달성하고자 하는 결과는 ISMS를 가장 최신의 기술적 혁신과 연계하는 것이다.

관련 지식으로는 최신 혁신 기술 및 그 응용과 그들이 완화시키거나 도입할 수 있는 구체적인 정보보안 위험에 대한 지식이 필요하며, 인공 지능 등 혁신적 기술을 이해하고 ISMS가 지속적인 적정성 및 효과성을 유지하도록 하는 기량이 필요하다.

Ⅲ. 전문가 자격 기준 표준화의 함의

3.1. 현재 27021 표준의 문제점

ISO/IEC 27021은 2년의 연구기간을 거치면서 총 5년의 시간을 거쳤으나 실제로 개발이 진행된 것은 3년이며, 초반 사업 경영 자격의 포함 여부 및 구체화 정도의 논의에 많은 시간을 빼앗겨 후반의 검토가 미흡한 측면이 있다. 개발 기간은 1년 연장이 가능하였으나, 후반에 변경된 에디터들이 표준의 개발 배경 및 절차에 대한 이해 부족으로 논의를 서둘러 마무리함으로써 표준의 완성도가 일부 미흡한 측면이 있다.

본 표준의 개시를 촉발한 스웨덴의 경우 표준이 전문가의 인증에 필요한 수준의 구체성을 갖추지 못했으며, 모든 자격을 전문가 1인이 만족하는 것은 매우 어렵다는 취지에서 반대 투표를 하였다.[5] 한국의 경우에도 여러 개선점을 지적하였으나 FDIS 단계에서는 편집상의 오류만이 수용되어 발표 후 수정안을 제출할 예정이다. 프로젝트에 초기부터 가장 적극적으로 참여한 3개 국 중 2개 국이 만족하기 어려운 결과를 낳았다는 점에서 에디터십의 중요성이 다시 한 번 확인되었다.

일부 미진한 사항이 존재함에도 불구하고 국제표준의 발표는 확정된 사항이므로, 수정 제안을 진행하는 동시에 이 표준의 활용 방안을 고려할 필요가 있다.

3.2. 27021 활용에 고려해야 할 배경 지식

3.2.1. ISO/IEC 17024

ISO/IEC에서 만들어진 인증 표준 중, 사람을 대상으로 하는 인증의 기초가 되는 표준은 ISO/IEC 17024 :2012 적합성 평가 - 사람에 대한 인증을 운영하는 기관에 대한 일반 요구사항 (Conformity assessment - General requirements for bodies operating certification of persons이다. 기존 시장에 존재하는 정보보안 자격증 중에는 ISO의 인증을 받은 자격증들이 많은데 이들은 이 ISO/IEC 17024의 일반 요구사항에 따라 인증을 받은 것이다.

이 표준에서는 4장에서 10장에 걸쳐 자격 인증기관의 일반 요구사항, 구조적 요구사항, 자원 요구사항, 기록 및 정보 요구사항, 인증 스킴, 인증 프로세스 요구사항, 인증기관의 경영시스템 요구사항을 다루고 있다. 또한 부록 A에서는 사람에 대한 인증과 인증 활동을 위한 원칙을 제공한다.

인증 스킴을 다루는 이 표준의 8장에서는 인증의 범위, 자격 요구사항, 능력, 학력 및 경력 등에 대한 요구사항을 명시하도록 하고 있다. 기존의 정보보안 자격 인증을 제공하는 인증기관들은 이 인증 스킴의 내용을 자체적으로 규정하여 인증을 제공하고 있다. ISO/IEC 27021은 이들 요구사항 중 정보보안경영시스템 전문가의 자격 요건을 명세한 표준이다.

3.2.2. 다른 인증표준 체계와의 비교

이 구조는 ISO/IEC 17021-1 및 ISO/IEC 27006과 대비 된다. ISO/IEC 17021-1 적합성 평가 – 경영시스템의 감사 및 인증을 제공하는 기관에 대한 요구사항 (Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 1 : Requirements)[6]는 정보보안을 포함한 다양한 경영시스템의 인증기관에 대한 일반적인 요구사항을 제공한다. ISO/IEC 27006 정보보안경영시스템의 감사 및 인증을 제공하는 기관에 대한 요구사항 (Requirements for bodies providing audit and certification of information security management systems) 표준은 이 ISO/IEC 17021-1 문서에 기초하여 동일한 구조에 정보보안 측면의 추가 요구사항을 포함하여 만들어졌다.

한편 ISO 19011 경영시스템 감사에 대한 지침 (Guidelines for auditing management systems)[7]은 모든 경영시스템에 대한 일반적인 감사 지침이며, ISO/IEC 27007 정보보안 경영시스템 감사에 대한 지침(Guidelines for information security management systems auditing)[8]은 19011의 구조에 정보보안 경영시스템 감사에 특유한 추가 요구사항을 포함한다.

이 두 개의 표준 내용에도 감사인의 자격 요건이 포함되어 있기 때문에 ISMS 인증기관들은 이 3개의 표준 즉 ISO/IEC 17024, ISO/IEC 27006 및 27007에 근거하여 감사인을 인증하고 있다.

3.2.3. ISO/IEC 27021 개발 과정의 논의

ISO/IEC 27021 개발의 초기 의도는 ISO/IEC 17024에 기초하여 ISMS 전문가를 위한 인증 요구사항을 개발하는 것이었다. 그러나, 이렇게 만들어 지는 표준은 적합성 평가에 관한 표준이고 ISO/IEC JTC 1/SC 27의 업무 범위를 넘어가는 것이었다. 적합성 인증은 ISO 쪽에서는 CASCO(Committee on conformity assessment)의 업무 범위이며 IEC의 경우에는 CAB(Conformity assessment board)가 된다. IEC의 CAB은 이 표준의 승인 단계에서 이러한 업무 범위의 문제를 제기하는 한편, 표준의 진행 중 신속한 적합성 수요 대응을 위하여 CAB 체계를 전면 개편하고, 사이버 보안 분야 적합성 평가 대응을 위한 작업그룹(WG 17)을 신설하였다. 특히 이 신규 제안 관련 적합성 평가 수요에 대해서도 WG 17에서 병행 검토하기로 결의한 바 있다.

추가적인 1년에에 걸친 연구기간(Study period) 동안 ISO/ CASCO와 IEC/CAB과의 협의를 진행하면서, SC 27에서는 ISMS 전문가를 위한 자격 요건을 개발하는 것은 가능하다는 합의에 도달하였다. 이에 따라 ISO/IEC 27021 표준은 제목과 범위가 수정되어 재투표를 거쳐 개시되게 되었다.

3.3. 27021 활용 방안 및 향후의 과제

3.3.1. ISO 인증기관에 대한 인정 체계

현재 ISO/IEC 27021이 국제표준으로 발표되더라도 이에 기초한 ISMS 전문가 인증을 바로 시작하기에는 어려움이 있다. 이 표준은 정보보안 전문가의 자격 요구사항에 대한 표준일 뿐으로, 어떤 인증기관이 이에 기초한 전문가 인증을 수행한다고 하더라도 이를 확인하고 인정해주는 체계가 수립되어 있지 않다.

ISO/IEC 17024에 대한 부합성을 평가하여 인증해주는 ISO 인정(accreditation) 체계는 국제적으로 운영되고 있다. 이에 따른 인정을 받은 기관이 ISO/IEC 27021 표준을 따르고자 할 경우, ISO/IEC 17024 내에 자격 요구사항을 제시하고 준수하도록 하는 요구사항이 포함되어 있으므로, 이 두 표준에 대한 부합성을 기존의 인정 체계에 따라 인정 받을 수 있다. 하지만 ISO/IEC 17024를 따르지 않은 상태에서 ISO/IEC 27021 표준의 부합성을 검증하는 체계는 존재하지 않는다.

즉, 어떤 인증기관이 ISO/IEC 27021에 따라 ISMS 전문가 인증을 수행하고 이를 객관적으로 인정받고자 한다면 ISO/IEC 17024에 따른 인정을 받아야 한다. 이 인증기관은 그 과정에서 ISO/IEC 17024의 8장에서 요구하는 인증 스킴을 개발해야 한다. 이때 8장의 인증스킴 요구사항인 자격 요구사항에 대해 ISO/IEC 27021의 요구사항을 만족하도록 개발하여야 한다.

이미 ISO/IEC 17024 인증을 받은 국제 자격증들은 ISO/IEC 27021이 요구하는 정보보안 자격은 일반적으로 포함하고 있으며, 사업 경영 자격에 포함된 요구사항들을 자신들의 지식 체계에 새롭게 포함시키거나 또는

기존의 내용에 매핑하는 작업이 필요할 것이다.

한편 ISO/CASCO와 IEC/CAB은 이 표준이 발행된 후 관련 업계의 반응에 기초하여 스킴 개발을 결정하기로 합의한 바 있다. 이런 방식으로 인증 스킴이 개발된다면, 다양한 인증기관이 운영하는 단일 국제 인증 체계가 만들어 질 것이며, 그렇지 않은 경우 각각의 인증기관이 자신의 인증 스킴을 운영할 수도 있다.

3.3.2. 국내 자격 제도와 ISO 표준 인정의 차이

우리나라의 경우 정보보안 기사/산업 기사 자격이 존재하며, 정보보호기술사제도를 시행하려는 노력이 있었으나 시장 규모의 문제로 중단된 바 있다.[9] 우리나라의 자격제도는 현재의 국제적인 인력에 대한 자격기준이 요구하고 있는 재인증 등의 요구사항을 포함하고 있지 않아서 현재의 제도로는 ISO/IEC 17024에 따른 국제인증은 불가능하다. 또한 기존의 정보보안 기사/산업 기사 자격은 ISO/IEC 27021 표준의 업무경영 자격을 모두 만족시키지는 못한다.

한편 우리나라는 본 과제의 수립 및 진행과정에 적극적으로 참여하면서 2016년 초 발표된 '정보보호관리·운영' 국가직무능력표준[10]의 내용을 포함하도록 기고하였으며 대부분이 받아들여졌다. 그러나 그렇다고 해서 국가직무능력표준이 ISO/IEC 27021 표준을 모두 포함하는 것은 아니다.

일본에서는 기 보유하고 있는 정보보안 기술사를 이 표준에 따라 국제 인증을 받는 것을 목표로 참여를 시작하였다. 일본의 자격 제도 역시 우리나라와 마찬가지로 재인증을 요구하지 않고 있으므로 ISO/IEC 17024에 따른 국제 인증을 받을 수 없다.

이에 대응하기 위하여 일본은 연구기간 동안 재인증을 포함하지 않는 "qualification" 개념을 신규 자격 표준에 도입하기 위하여 노력하였으나, 여타 국가의 반대로 무산되었다. 이에 따라 일본은 부록 A를 포함시켜 ISO/IEC 27021을 만족하는 지식 체계에 포함되어야 할 키워드를 제시하고자 하였다.

본 표준을 국내에서 적극적으로 활용하기 위해서는 2가지 방안이 가능하다. 기존 국내 자격의 요구사항을 ISO/IEC 27021 요구사항과 매핑하여 만족여부를 확인하고 필요한 경우 국내 자격 요구사항을 확장함으로써 이에 대한 부합성을 주장할 수 있다. 그러나 이에 대하여 ISO로부터 객관적인 인정을 받을 수는 없다. 또는 ISO/IEC 27021 및 17024의 요구사항을 포함하는 새로운 자격제도를 만들고 ISO의 인증을 받을 수도 있을 것이다.

이 두 방안은 각각 장단점이 있으므로 이해당사자들의 논의와 고려가 진행되어야 한다. 특히, 국내에서의 진행은 앞 절에서 설명한 ISO/CASCO와 IEC/CAB의 인증스킴 개발에 관한 국제 동향을 검토하고 반영하면서 이루어져야 할 것이다.

Ⅳ. 결 론

지금까지 FDIS 투표를 마친 ISO/IEC 27021의 주요 내용을 살펴보고 그 활용방안과 문제점에 대해 검토하였다.

정보보안경영 전문가 자격 요건 표준은 국제 정보보안 인력 시장에 상당한 영향을 미칠 것으로 예상된다. 전술한 대로 이미 IEC의 CAB가 주도적으로 대응하고 있다. 꾸준히 참여한 일본은 물론이고, 주도적으로 참여하지 않았지만 본 표준의 국제 표준화에 찬성 투표를 한 30여개국 모두 자격 인증 및 교육 분야에서 이 표준의 활용을 원하고 있다고 해석할 수 있다.

국제 표준에 따른 인정을 원하는 정보보안 전문가들과 정보보안 전문가를 고용하고자 하는 수요기관 뿐만 아니라 자격 인증기관, 교육기관 등에 관련된 이해당사자들의 많은 논의가 있기를 바란다.

참 고 문 헌

[1] ISO/IEC 27021 FIDS, Competence requirements for information security management systems professionals, ISO, Oct. 2017

[2] ISO/IEC 27006:2015 Requirements for bodies providing audit and certification of information security management systems, ISO, Oct. 2015.

[3] European e-Competence Framework 홈페이지, http://www.ecompetences.eu/

[4] ISO/IEC 17024:2012 Conformity assessment -- General requirements for bodies operating certification of persons, ISO, Dec. 2012.

[5] ISO/IEC N17234, SoV FDIS 27021, ISO, Sept, 27017.

[6] ISO/IEC 17021-1:2015, Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 1 : Requirements, ISO, June, 2015.
[7] ISO 19011:2011 Guidelines for auditing management systems, ISO, Nov. 2011.
[8] ISO/IEC 27007:2011 Information technology -- Security techniques -- Guidelines for information security management systems auditing, ISO, Nov. 2011.
[9] 디지털타임스, 2016, “정보보안기술사 자격증 연내 도입 ‘불투명’”, 2016. 11. 02
[10] 한국산업인력공단, 국가직무능력표준 직무명: 정보보호관리·운영, 2016. 02

〈저자소개〉

오 경 희 (Kyeong Hee Oh)
1988년 8월 : 서강대학교 전산과 졸업
1992년 2월 : KAIST 전산과 석사
2012년~현재 : TCA서비스 대표
2013년~2017년 : ITU-T SG 17 Q3 Associate rapporteur
2017년~현재 : ITU-T SG 17 Q14 Corapporteur
2010년~현재 : 산업표준심의회 정보보안기술(ISO/SC27) 전문위원
2017년~현재 : 산업표준심의회 블록체인(ISO/TC 307) 전문위원
관심분야 : 정보보안경영, 아키텍처, IT 감사, 거버넌스, 통제, 블록체인