정 보 보 호 학 회 지
제25권 제4호, 2015. 8

정보보안경영 전문가 자격요건

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 개시하였다.

9월까지 2차 WD가 개발될 예정인 본 표준은 2년간의 연구기간을 거치면서 표준의 범위에 관해 이미 많은 논란을 거쳤으며, 현재는 정보보안경영 전문가가 보유해야 할 비즈니스 관련 전문성에 대한 논쟁이 진행되고 있다.

본 논문에서는 이 표준이 개시되기까지의 배경과 진행 현황, 주요 현안들을 살펴본다. 본 표준은 국제 정보보안 인력 및 교육 시장에 상당한 영향을 미칠 것으로 예상되며, 이에 대한 해외의 대응을 살펴보고 활용 방안을 제시한다. 또한 국내 보안 전문가 및 인력 양성 기관들의 관심과 참여를 촉구한다.

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. 기존 국제 표준은 ISMS 감사인에 대한 자격 요건은 제공하였으나 실무자에 대한 자격 요건을 제시한 표준은 아직 없다.

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 27021로 정식 표준화 과제를 시작하였으며, 현재 2차 WD를 개발 중에 있다.

본 논문에서는 이 국제 표준이 개시되기까지의 과정과 표준이 다루고 있는 내용 및 주된 현안을 소개하고 향후 대응 방안을 언급하고자 한다.

Ⅱ. 국제 전문가 자격 인증 관련 현황

2.1. 정보보안 전문가 자격 제도 현황

현재 전세계적으로 많은 정보보안전문가 자격제도가 존재하고 있다. 국내는 국가기술자격으로서 정보보안기사, 정보보안산업기사를 두고 있으며, 가까운 일본에는 정보보안기술사 제도가 있다. 스웨덴의 경우 27000 시리즈에 특화된 전문가 인증제도(Accredited personal certification scheme for professionals working with the 27000-series)를 수립하였다. 유럽의 EC-Council에서도 보안 전문가 자격을 운영하고 있다(EC-Council certified security specialist, ECSS)

민간에서 운영하는 국제적인 보안자격으로는 다음 표에서 다양한 자격 제도의 일부를 보여주고 있다.

2.2. 전문가 자격 인증 관련 표준 현황

ISO/IEC에서 만들어진 사람에 대한 인증에 관련된 표준의 가장 기초가 되는 것이 ISO/IEC 17024 :2012 Conformity assessment - General requirements for bodies operating certification of persons[1]이다. 제목에서 나타나듯 이 표준은 사람에 대한 인증을 운영하는 기관에 대한 일반적인 요구사항을 다루고 있다.

이 표준에서는 자격 인증기관의 일반 요건, 구조적 요건, 자원, 기록, 인증 프로세스, 인증기관의 경영체계 등에 대한 요건과 함께 인증 스킴을 다루고 있으며, 8장의 인증 스킴에서 인증의 범위, 자격 요건, 능력, 학력

* TCA 서비스 대표 (khoh@tcaservices.kr)

〔표 1〕 민간 국제 보안자격제도 현황

자격 명칭	인증유형	인증기관
CISA	IT auditor	ISCA
CISM	IS manager	
SSCP	Systems security	ISC2
CAP	authorizing and maintaining information systems	
CSSLP	Secure Software Lifecycle	
CISSP,	Information Systems Security	
CISSP concentrations	Architecture	
	Engineering	
	Management	
Security+	Security incidents	CompTIA
CASP	Advanced Security Practitioner	
CCSP	Cisco Network security engineer	Cisco
CCNA security		
GSEC, GCIH, GCIA, etc.	Security Administration	GIAC (SANS)
GCFA, GREM	Forensics	
GSLC	Management	
GSNA	Audit	
GSSP-Java, -Net, GWEB	Software security	
GLEG	Legal	
GSE	Incident handling Expert	
CPP	Consulting security management	ASIS
PCI	Investigator	
PSP	Physical security professional	

및 경력 등에 대한 요건을 명시하도록 하고 있다.

ISACA, ISC2, GIAC 등 많은 민간 국제 보안전문가 자격제도가 이 ISO/IEC 17024에 따라 인증을 받고 있다. 어떤 자격 인증제도가 ISO 인정을 받았다고 할 때는 이 표준을 따라 인정을 받았다는 뜻이다. 이 때 인정(accreditation)이란 인증 또는 평가 기관이 특정 인증 또는 평가를 하기 위한 요건을 만족함을 공식적으로 인정한다는 의미로 사용된다.

이 표준은 분야에 관계 없이 사람에 관한 인증에는 모두 적용되기 때문에 소프트웨어 공학, 환경 안전 등의 각종의 자격 인증기관들이 이를 따라 고 있다. 예를 들어 ISO/IEC 24773 Software engineering – Certification of software engineering professionals – Comparison framework[2]은 이 ISO/IEC 17024에 따라 소프트웨어 공학 전문가에 대한 자격 인증 스킴을 비교하기 위한 프레임워크를 제시하고 있으며, 소프트웨어 공학 전문가에 대한 인증 요구사항의 집합인 인증 스킴이 포함해야 할 사항을 정의하고 있다. 또한 그 인증 스킴 요구사항의 하나로 소프트웨어 공학 전문가가 보유해야 할 지식 및 수준과 스킬 및 수행 수준을 제시하고 있다.

한편 ISMS 인증 심사를 수행하는 심사원에 대한 자격 요건 및 평가는 ISO/IEC 27007:2011[3]에서 규정하고 있다. ISO/IEC 27007의 경우 ISO/IEC 17024를 참조하지 않고, 모든 분야에 적용되는 경영체계의 심사에 관한 지침인 ISO 19011 Guidelines for auditing management systems[4]의 구조를 따르고 있다.

ISO 19011은 7장에서 감사인의 자격과 평가를 다루고 있으며, ISO/IEC 27007은 ISO 19011의 일반적인 요구사항을 기본으로 하고 정보보안 경영체계의 심사원에게 필요한 요건들을 추가하여 명시하고 있다.

이러한 현황에서 보듯이 일반 전문가에 대한 자격 인증기관에 대한 국제 표준(ISO/IEC 17024)은 존재하고 있다. 그러나 일반 경영체계 심사원에 대한 지침(ISO 19011)에 따라 정보보안경영체계 심사원에 대한 자격 요건을 규정한 표준(ISO/IEC 27007)이 존재하듯이, ISO/IEC 17024에 따라 정보보안경영체계 전문가에 대한 자격 요건을 구체적으로 규정한 국제 표준은 개발되지 않은 상태였다. 따라서, ISO/IEC 24773이 ISO/IEC 17024에 기초하여 소프트웨어 공학 분야의 전문가에 필요한 지식과 스킬을 추가적으로 규정하였듯이, 정보보안 경영체계를 수립, 운영하는 전문가에게 필요한 지식과 스킬을 추가적으로 규정하고자 하는 것이 새로 시작된 ISO/IEC 27021 표준의 배경이자 목적이었다.

Ⅲ. 정보보안경영 전문가 자격 요건 표준

3.1. 진행 과정

2012년 스웨덴 국가 대표인 Fredrik Björck가 스웨덴의 정보보호관리 전문가에 대한 인증제도 수립을 발표하고, 이에 여러 국가에서 관심을 표명함으로써 정보보안경영 전문가 국제인증(International Certification

of Information Security Management Specialists)에 관한 study period가 개시되었다. 이 연구기간에는 스웨덴의 Fredrik Björck, 한국의 오 경희, 일본의 Yonoske Harada가 공동 라포처로 참여하였다.

이 SP는 1년간 진행되어 정보보호 전문가에 대한 기존의 국제 자격제도 및 표준 현황을 조사하고 ISO/IEC 27000 시리즈에 기초하여 정보보호관리체계를 구축, 운영하기 위한 전문가 자격제도의 필요성을 조사하였다. 종료 회의에서 정보보호관리 전문가에 대한 인증 표준의 개발 필요성에 대한 현장 투표를 수행한 결과 회의 참가 20개국의 전원 찬성 투표로 ISO/IEC 27021 표준 번호가 할당되었다.

그러나 ISO/IEC JTC 1 결의 단계에서 IEC가 인력에 대한 신규 인증 스킴의 소유권 문제를 제기함으로써 1년간 SP가 연장되었다. 제안된 표준은 ISO/IEC 27006과 같은, 정보보호 전문가를 인증하기 위한 요구사항을 개발하는 것이었다. 그러나 이러한 요구사항이 실현되기 위해서는 인증기관 및 인증기관을 인정하기 위한 인정기관의 체계가 필요하며, IEC에서는 이러한 인증 스킴에 관한 문서는 본질적으로 인증기관 또는 인정기관이 개발/참조해야 하는 문서임을 주장하였다.

ISO의 적합성 평가 위원회인 CASCO 가 2012년 발행한 Directive[5] 문서에서는 표준 개발자는 “중립 원칙”에 따라 제1자(제조자 또는 공급자), 제2자(사용자 또는 구매자), 제3자(인증기관과 같은 독립 기관) 모두에게 적용될 수 있는 문서를 개발하도록 하고 있다. 이에 따르면 제3자 기관이 주로 참조하기 위한 인증스킴에 관한 문서는 SC의 개발 범위를 넘어서는 것이었다.

이에 따라 연장된 SP 과정에서는 ISO와 IEC 각각에서 인증제도를 담당하는 기구인 CASCO (Committee on conformity assessment)와 CAB(Conformity assessment body)이 참여하여, 이러한 신규 인증 제도가 만들어진다면 어떤 기구가 소유권을 가지고 인증 제도를 운영할 것인지, ISO/IEC JTC 1 SC 27/WG 1의 가능한 역할은 무엇인지에 관한 심도있는 토론이 이루어졌다.

IEC CAB은 또한 인증 스킴에는 이를 운영하기 위한 소유자가 필요한데, 이 역할을 누가 맡을 것인지를 정의해야 한다고 주장하였다. IEC는 기존 보안에 관련된 인력에 대한 표준 및 인증 스킴을 보유하고 있다고 주장하며 신규 인증 스킴에 대한 소유권에 관심을 보였다. 그러나 IEC가 소유권을 갖는 인력에 대한 인증 스킴은 “폭발성 환경에서의 인력 적합성 인증(IECEx Certification of Personnel Competence for Explosive Atmospheres)”에 관한 것으로서 정보보안 인력과는 일부 차이가 있다. 한편, CASCO는 이미 ISMS 심사원에 대한 인증 표준을 보유하고 있지만 직접적으로 인증체계를 운영하고 있지는 않다.

연장된 SP에서는 인증 스킴에 대한 문제는 ISO/CASCO와 IEC/CAB, 또는 각 국의 인증체계의 결정사항으로 남겨 두고, 표준을 개발하는 SC 27에서는 제1자, 2자, 3자가 모두 활용할 수 있는 정보보안관리 인력에 대한 자격 요건을 국제 표준화하는 것이 적절하다고 합의되었다.

이에 따라 최종 신규작업항목 제안은 “정보보안경영 전문가 자격 요구사항 Conformity requirements for information security management professional”이라는 제목으로 이루어졌으며, 국가 투표를 통과하여 2014년 10월부터 정식 표준 프로젝트로 개시되었다. 이 표준은 2016년 발표를 예정으로 하고 있으며 2015년 9월 2차 WD가 개발될 예정이다.

ISO/CASCO와 IEC/CAB은 이 표준이 발행되고 나면 관련 업계의 반응에 기초하여 스킴 개발을 결정하기로 합의했다. 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.

한편 IEC/CAB은 6월 운영회의에서 신속한 적합성 수요 대응을 위한 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 결의하였다.

3.2. ISO/IEC 27021의 내용

이 표준은 정보보안경영 전문가의 자격 요구사항을 명세하고 있다. 이 표준은 제1자인 전문가 및 전문가 양성 교육기관에서도, 제2자인 정부기관, 보안전문회사, 보안직원을 채용하고자 하는 수요기관 등에서도, 그리고 전문가를 인증하기 위한 인증기관과 그 인증기관을 인정하는 인정기관에서 모두 활용할 수 있다.

1차 회의에서는 브레인스토밍을 통해 지식 및 스킬의 항목들을 선정하였다. 1차 WD에서는 일본 측의 노

〔표 2〕 정보보안경영 전문가 지식 및 스킬

대분류	소분류
거버넌스	
일반적 스킬	분석 스킬 분석적 사고 - 문제 해결을 위한 분석적 접근 방법 포함
	소통(communications)
경영 자격 (management competence)	리더쉽 - 전략 - 인적자원
	모든 역할을 다 할 수 있는 팀 (Cross functional teams)
	비즈니스 스킬 사업 효익과 ISMS의 통합 지식
	재무 및 예산 - 재무 원칙에 대한 이해 - ISMS 예산 수립 능력 - ISMS 구현 비용 (인적 자원, 통제 비용, 기술적 인프라 및 통제 운영 비용, 프로세스 비용 포함)
	비즈니스 메트릭 - 균형성과표(BSC) - 핵심 효과 지표 - 보안 KPI
	경영 규율(management disciplines) - 프로젝트 관리 - 포트폴리오 관리 - 변경 관리
	법 - 계약관리 - 법 규제 이해 - 컴플라이언스 부서와의 상호작용
정보보안 자격	정보의 가치 평가
	정보보안 위험관리 - 위협 평가 - 취약성 평가
	보안 통제에 대한 지식
	IS 감사 스킬
	상황적 인식 - "큰그림"을 평가하기 위한 능력
	IS 보안 아키텍처 개발
	IS 정책 개발, 구현 및 강제
통제 운영에 관한 지식	모니터링
	보고
	정보보안 사고 관리 CERT 팀 등

력으로 ISMS 전문가에 대한 개요로서 전문가의 조직 내 역할, 기능 및 지식 구조에 대한 설명이 포함되었으나, 2015년 4월 쿠칭에서의 2차 회의 토론을 통해 조직에 따라 달라질 수 있는 ISMS 전문가의 역할 등은 부록으로 보내고, 본문의 내용은 순수하게 지식과 스킬의 명세에 집중하기로 결의하였다.

2015년 7월 현재 정보보안경영 전문가가 보유해야 할 지식 및 스킬로서 edior 그룹이 내용 기고를 요청한 내용은 [표 2]와 같다.[6]

3.3. ISO/IEC 27021 관련 주요 현안

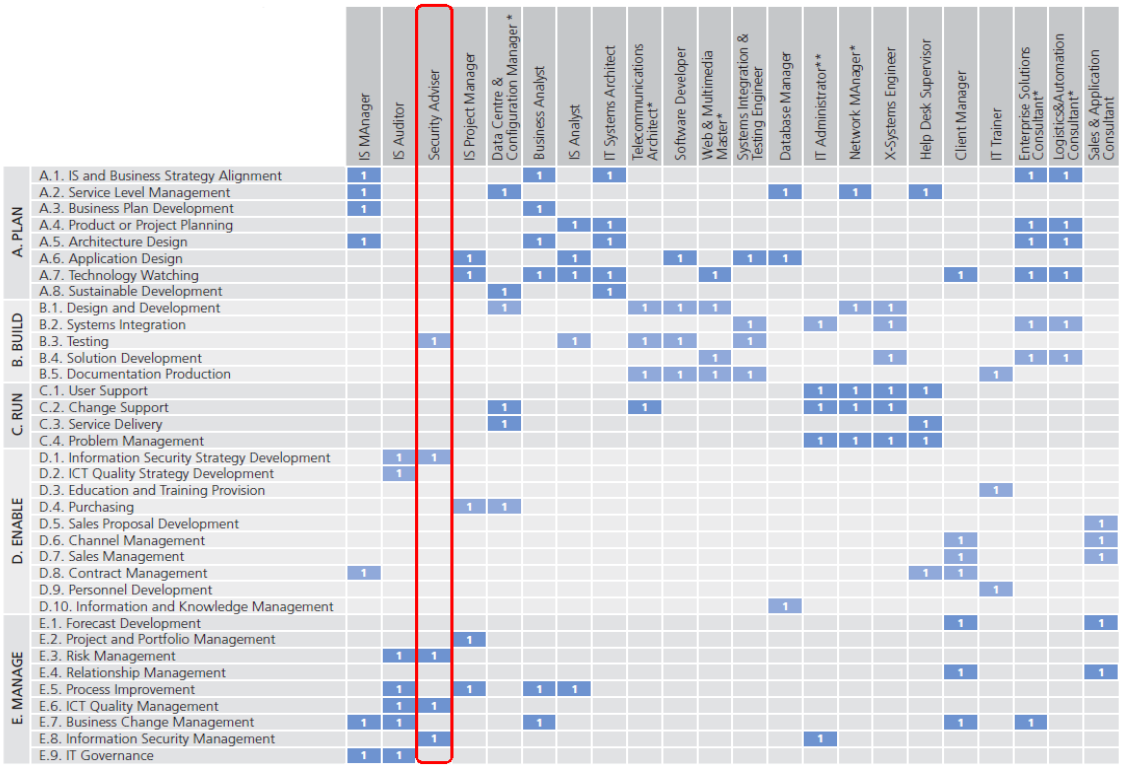
지난 회의에서의 가장 큰 쟁점은 ISMS 전문가의 자격 요건에 정보보안 외의 일반적인 경영지식을 포함할 것인가 하는 점이다. 유럽의 e-Competence Framework (e-CF) 3.0[7]에 익숙해져 있는 유럽과 미국 지역의 일부 전문가들은 일반적인 거버넌스, 비즈니스 분석 스킬, 경영관련 능력 등은 평가하기 어려움을 주장하며 ISMS 전문가의 지식과 스킬을 정보보안 분야에 국한시킬 것을 주장하고 있다.

그러나 대다수의 전문가들은 자신들의 경험에 기초하여 정보보안경영 전문가들의 가장 큰 현안은 경영진을 설득하는 것이며 이를 위해 비즈니스 경영진의 관점에서 정보보안의 효익을 제시하고 지속적으로 보안에 투자할 수 있도록 이끄는 것이라고 보고 있다. 이를 위해서는 일반적인 비즈니스에 대한 이해와 지식, 의사소통 스킬이 필요하다고 보는 입장이다. 이러한 논의를 반영하여 [표 2]와 같은 항목들이 제시되었다.

유럽 연합은 e-CF를 통해 ICT 관련 자격을 정리하였다. 이에는 직무 정의, 훈련과정, 학습과정, 자격(qualification), 진로(career path), 인증 등이 포함된다. 또한 각 자격에 필요한 지식 및 기술 뿐만 아니라 능숙도 등급을 5단계로 나누어 제시하고 있다. 이 e-CF는 상당히 체계적인 구조이지만 이 프레임워크에 따르면 보안 전문가는 ICT의 이행 5단계(계획 Plan, 구성 Build, 실행 Run, 개시 Enable, 관리 Manage) 중 관리 단계 이전의 4단계에서는 테스트와 정보보안 전략 개발의 자격을 보유하는 것으로 되어 있다. 또한 Manage 단계에서도 위험관리, 품질 관리, 정보보안 관리의 자격 보유를 요구 받고 있다.

물론 보안 전문가가 이러한 자격을 보유해야 하는 것은 당연한 것이다. 그러나 예를 들어 [표 3]의 A.1의 사업전략과 IS 전략의 연계의 경우, 정보보안경영 전문가가 이에 관한 완전한 자격을 갖출 필요는 없더라도, 정보보안 전략을 사업 전략에 연계할 책임은 있는 것이며, 이에 따른 전문성을 보유하는 것은 좋은 보안 전문가가 되기 위해 필요한 요소라고 보인다.

〔표 3〕 e-CF 자격 구조에서 EUCIP 프로파일에 따른 보안 전문가의 자격 요소



두 번째 쟁점은 전문가의 윤리 강령과 행위 기준을 어느 정도나 포함할 것인가 하는 부분이다. ISO/IEC 17024에서는 전문가의 지식과 스킬에 더불어 각 인증기관이 인증 스킴에서 제시해야 하는 내용의 하나로 전문가 윤리 강령과 행위 기준을 들고 있다. 그러나 지난 회의에서는 이의 내용을 채우는 것은 각 인증기관의 일이며 윤리는 가치의 문제이기 때문에 표준을 제시하는 것이 적절하지 않다는 주장이 제시되어, 항목은 남기되 전문가는 윤리 강령을 따라야 한다는 선언적인 내용만 남긴 상태이다.

기타 자격(competence)의 정의, 표준이 포함해야 할 내용에 대한 세부사항 등이 주로 논의되었다. 자격은 기존의 다른 ISO 표준의 정의를 따라 '지식과 스킬 knowledge and skills'로 정의되었으며, 자격의 등급은 본 표준에 포함하지 않고, 정보보안경영 전문가가 수행할 수 있는 다양한 기능이나 직무는 조직에 따라 달라질 수 있으므로 필요한 경우 부록으로 제시하는 것으로 정리되었다.

Ⅳ. 결 론

지금까지 정보보안경영 전문가 자격 요건 표준이 개발 개시되기까지의 배경과 진행 현황, 주요 현안들을 살펴보았다.

정보보안경영 전문가 자격 요건 표준은 정보보안 인력 시장에 큰 영향을 미칠 것으로 예상된다. 전술한 바대로 이미 IEC의 CAB가 주도적으로 대응하고 있으며, SC 27/WG 1에 참여하는 자격 인증 및 교육 분야의 각국의 전문가들의 많은 관심을 끌고 있다.

가장 중요하고, 또 앞으로도 논의가 지속될 것으로 예상되는 업무 관련 전문성의 필요성에 대한 공감대는 넓게 퍼져 있지만 그에 대한 문장으로 된 설명은 아직 충분히 제시되지 않아 많은 참여가 필요한 상황이다.

일본에서는 기 보유하고 있는 정보보안 기술사를 이 표준에 따라 국제 인증을 받는 것을 목표로 참여를 시작하였다. 일본의 자격 제도는 현재의 국제적인 인력에 대한 자격 기준이 요구하고 있는 재인증 등의 요구사항을 포함하고 있지 않아서 현재의 제도로는 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. 일본은 부록으로라도 자국의 국가 자격 제도의 지식체계 구성 등을 포함시키기 위해 끈질기게 노력하고 있다.

우리나라의 경우에도 기존의 SIS에서 발전된 정보보안 기사/산업 기사 자격이 존재하며, 미래창조부의 2013년 정보보호 산업발전 종합대책에 따르면 2016년 정보보호기술사제도를 시행할 예정으로 있다. 우리나라의 자격제도 역시 일본과 유사하게 재인증을 요구하지 않고 있으므로 ISO/IEC 17024에 따른 국제인증은 불가능하다.

그러나 본 표준이 인증기관을 위한 표준이 아니라 단순히 정보보안경영 전문가의 자격 요건이 되면서, 한국과 일본의 국내 기술자격이라 하더라도 ISO/IEC 27021 표준에 부합한다고 주장할 수는 있을 것이다. 그러나 국내의 기술 자격이 대부분 비즈니스 관련 지식 및 스킬 보다는 기술적 지식의 검증에 치중되어 있어 기존의 정보보안 기사/산업 기사 자격이 본 표준을 따른다고 하기에는 무리가 있다. 신규로 개발되는 정보보안 기술사 자격이 이러한 국제 표준 동향을 참조하고, 가능하다면 부합할 수 있는 방안을 고민 하는 것이 필요할 것이다. 이를 위해서는 국내의 제도 운영 관계자가 국제 표준화에 능동적으로 참여하여 신규 제도 신설 및 운영에 반영할 필요가 있다.

2014년부터 적용되고 있는 새로운 ISO 규칙에 따르면 위원회 표준(CD)은 국가별 1표로 투표가 이루어지지만 작업반 표준(WD)의 단계에서는 회의에서의 결정사항은 국가 별로 1표가 아니라 참석한 전문가 별 1표로 산정된다. CD 단계에서도 많은 전문가들이 참여하여 여러 측면으로 지원 발언을 하게 되면 더 그 국가의 주장에 힘이 실리는 경향이 있다. 특히 원어민이 아닌 국가의 경우 언어문제를 극복하고 국가 이익을 관철하기 위해서는 다수의 전문가들의 상호 지원이 필수적이지만, 현재 WG 1의 참여 인원으로는 불가능한 상황이다.

전세계 보안인력 시장에 영향을 미칠 수 있는 현안이 되는 본 표준에 대해 직간접적 이해당사자들의 의견을 수렴할 수 있는 저변 확대와 국내 관련 담당 기관의 직접 참여가 절실하다.

참 고 문 헌

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

[2] ISO/IEC 24773:2008 Software engineering − Certification of software engineering professionals − Comparison framework, ISO, Sept. 2008.

[3] ISO/IEC 27007:2011 Information technology -- Security techniques -- Guidelines for information security management systems auditing, ISO, Aug. 2014.

[4] ISO 19011:2011 Guidelines for auditing management systems, ISO, Nov. 2011.

[5] ISO/CASCO, Conformity assessment for standards writers : Do’s and dont’s, ISO, 2012.

[6] N0116 Call for contributions on the revised document structure for ISO/IEC 27021 Competence requirements for information security management systems professionals, ISO, July 2015.

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

〈저 자 소 개〉

오 경 희 (Kyeong Hee Oh)

1988년 8월 : 서강대학교 전산과 졸업
1992년 2월 : KAIST 전산과 석사
2012년~현재 : TCA서비스 대표, 고려사이버대학 겸임교수
2013년~현재 : vITU-T SG17 Q3 Associate rapporteur
2010년~현재 : 산업표준심의회 정보보안기술(ISO/SC27) 전문위원
2015년~현재 : 한국정보시스템감사통제협회 부회장
관심분야 : 정보보안경영, 아키텍처, IT 감사, 거버넌스, 통제