情報保護學會論文誌
第 23 卷 第 1 號, 2013. 2

개인정보영향평가 자격기준의 문제분석과 개선방안 연구 - 유사자격과 개인정보영향평가 자격체계와의 유사성 분석을 중심으로*

김 이 랑,† 심 미 나,‡ 임 종 인
고려대학교 정보보호대학원

A Study in the Improvement and Analysis Problem of Privacy Impact Assessment Qualification Criteria: focus on Similarity Analysis between Similar Certificates and Certification System of Privacy Impact Assessment*

Erang Kim,† Mina Shim,‡ Jong In Lim
Graduate School of Information Security, Korea University

요 약

2011년 9월 개인정보보호법의 발효로 공공기관의 개인정보영향평가가 의무화됨에 따라 영향평가 전문인력의 수요가 증가할 것으로 예상된다. 하지만 국내에는 이에 특화된 전문자격이 존재하지 않아 현 시점에서는 불가피하게 유사자격 등의 기준으로 영향평가 전문인력을 인정하고 있는 상황이나, 향후 중장기적으로 볼 때 이는 영향평가 시장의 걸림돌로 작용할 것으로 예상된다. 이에 본 논문에서는 유사자격과 영향평가 자격체계와의 비교를 통해 개인정보영향평가 자격요건에 대한 유사자격의 충족 여부를 분석하여 유사자격 인정의 타당성 여부를 확인한다. 비교 결과 유사자격의 타당성이 낮다고 판단됨에 따라 새로운 전문자격 수립, 유사자격에 추가 시험 또는 교육 운영, 전문자격의 모듈화 운영 등의 자격기준 개선방안을 제시하였으며, 세 가지 개선방안은 개인정보영향평가 시장의 품질 향상에 기여할 것으로 기대한다.

ABSTRACT

Since Personal Information Protection Act came into effect on September 2011, PIA(Privacy Impact Assessment) of public institutions has become obliged. Therefore, an increasing demand for PIA professionals is being expected. In domestic, however, no specialized certificates exist and therefore similar certificates have become a requirement for PIA professionals. Henceforth, however, the system based on these similar certificates is to be an obstacle to advancing PIA. Therefore, this study analyzes the sufficiency of current similar certificates compared with the PIA qualification requirements. And then, analyzes the validity of allowance as similar certificates by using this outcome of the validity. As this comparison draws a clear gap between PIA qualification and similar certificates, this paper suggest three suggestions to improve current qualification. Three suggestions are expected to contribute a qualitative improvement of the PIA industry.

Keywords: Privacy, Privacy Imoact Assessment, Qualification Criteria

접수일(2012년 12월 07일), 게재확정일(2012년 12월 14일)
* 이 논문의 저자 및 일부는 이 단계 BK21 사업에 지원을 받아 수행하였습니다.

† 주저자, kim0730@korea.ac.kr
‡ 교신저자, mnshim@korea.ac.kr

I. 서 론

최근 몇 년 간 수많은 개인정보 유출사고로 스팸메일, 스팸전화, 명의도용, 사생활 침해 등 크고 작은 피해가 발생하였으나, 개인정보를 보호하기 위한 법규가 미비하여 이를 예방하기가 사실상 어려운 실정이었다. 2011년 9월 30일 개인정보보호법의 발효로 국민들의 개인정보보호를 위한 기본적인 체계가 정비되었고, 이 법을 통해 공공기관에 대한 개인정보영향평가(PIA: Privacy Impact Assessment)가 의무화되었다. 900개 이상의 공공기관에서 개인정보영향평가(이하 영향평가) 수요가 발생할 것으로 예상됨에 따라 영향평가 전문인력 양성의 필요성이 대두되고 있다[1]. 하지만 현재 국내에는 PIA만을 위한 전문자격이 존재하지 않아, 개인정보보호법 시행령에서는 정보보호전문가(이하 SIS), 정보시스템감리사(이하 ISA), 기사 및 기술사, 공인정보시스템감사사(이하 CISA), 공인정보시스템보호전문가(이하 CISSP), 개인정보관리사(이하 CPPG) 등의 유사자격을 제시하고 있다.[1] 그러나 위의 자격들은 애초 다른 목적의 자격으로 PIA 수행인력의 전문성과 평가결과의 품질을 보장하기에는 한계가 존재한다.

영향평가 수급분석 결과, 향후 5년간 연평균 200여 건의 수요가 예상되었고, 평가기관들의 실질적 영향평가 실적은 약 6%, 전문성을 보장할 수 있는 영향평가 경험 보유 인력은 약 7% 정도에 불과하였다[2]. 지금은 시급한 제도수행으로 기존의 유사자격을 인정해주고 있지만, 지속적으로 검증받지 않은 유사자격 인력을 활용하는 것은 영향평가의 효과성을 유지하고, 지속적인 발전을 보장하는데 장애가 될 것이다. 이런 상황에도 유사자격 활용의 한계와 이러한 한계를 극복하기 위한 대안에 대해 구체적으로 논의되지 못하고 있다.

따라서 본 논문에서는 "개인정보영향평가 자격제도 수립방안 연구"를 기준으로 유사자격인 CPPG와 ISA를 비교함으로써, 실제 유사자격이 영향평가를 수행하는데 적합한 자격요건을 지닌 것인지 영향평가 수행인력 자격기준의 적절성에 대해 연구 할 것이다. 이를 위해 Ⅱ장에서는 영향평가 개요 및 전문인력 자격기준의 현황과 문제점에 대해 살펴보고, Ⅲ장에서는 연구의 목표 및 본 논문에서 사용되는 방법론을 살펴본다. Ⅳ장에서는 영향평가 자격체계와 유사자격인 CPPG, ISA가 영향평가 대체자격으로서의 조건을 어느 정도 갖추고 있는지 비교하고, Ⅴ장에서는 Ⅳ장에서 비교한 내용을 통해 각 자격이 대체자격으로서 이미 갖추고 있는 부분과 부족한 부분들을 구체적으로 살펴본다. Ⅵ장에서는 비교 결과에 따른 부족한 부분을 보충하여 영향평가 자격기준의 개선방안을 제시하고 마지막 Ⅶ장에서는 본 논문의 결론을 도출하고 향후 과제 및 기대효과에 대해 살펴본다.

1) 개인정보보호법 시행령 제37조 제1항 제2호

II. 개인정보영향평가 개요 및 전문인력 자격기준

2.1 개인정보영향평가 개요

2.1.1 개인정보영향평가 개념과 의의

개인정보영향평가란 개인정보를 활용하는 정보시스템의 구축·변경 시 위험요인의 분석하고 개선사항을 도출하는 절차를 뜻한다. 일정규모 이상[2]의 개인정보파일을 운영하는 경우 개인정보보호법 제33조 및 개인정보보호법 시행령 제35조에 근거하여 영향평가 수행이 의무화됨에 따라 도입되었으며, 개인정보 침해요인의 사전분석 및 개선방안 수립을 목적으로 한다. 보통 정보시스템을 구축하기 전 또는 분석·설계하는 단계에서 이루어지며, 개인정보의 수집·이용 및 관리상에 중대한 침해위험의 발생이 우려되는 경우 대상시스템의 개발 또는 구축하는 과정에서도 수행할 수 있다[3].

2.1.2 개인정보영향평가 수행주체

영향평가 수행을 위해서는 개인정보보호 관련 법규·지침, 시스템 개발·분석 등에 대한 전문지식이 필요하기 때문에 통상적으로 평가 대상 사업에 대한 이해도가 높은 사업주관부서가 기관 내 개인정보보호 전담 조직, 정보보안 조직 등의 도움을 받아 별도의 영향평가팀을 구성하여 수행할 것이 권고된다. 한편 개인정보보호법 제33조 제1항에서는 영향평가를 행정안전부장관이 지정하는 평가기관에 의뢰하여 실시하도록 명시하고 있다. 이는 소규모 개인사업자의 경우 자

2) 개인정보 보호법 시행령 제35조에 따라 ①민감정보 또는 고유식별정보가 포함된 5만명 이상의 개인정보파일 ②다른 개인정보파일과 연계하는 50만명 이상의 개인정보파일 ③100만명 이상의 정보주체에 관한 개인정보파일 ④개인정보파일의 운용체계를 변경하려는 경우 개인정보영향평가 의무수행 대상으로 함

체적으로 영향평가팀을 구성하여 운영하는 것이 현실적으로 어렵고, 공공기관의 경우에도 보유하고 있는 개인정보의 양이 방대하며, 침해에 따른 피해의 파장이 크기 때문에 영향평가의 신뢰성과 객관성을 확보하기 위함이다[4].

2.2 개인정보영향평가 전문인력 자격기준

2.2.1 법률상의 전문인력 자격기준

개인정보보호법 시행령 제37조에서는 영향평가의 신뢰성과 객관성을 보장하고 결과물의 품질을 확보하기 위해 영향평가기관 지정조건으로 영향평가 전문인력을 10명 이상 상시 보유할 것을 요구하고 있다. 여기서 영향평가 전문인력이란 영향평가에 대한 "전문성을 갖춘 인력"을 의미한다. 개인정보보호법 시행령 제37조 제1항 제2조와 개인정보영향평가에 관한 고시 및 해설서 제5조에서는 자격기준으로 〔표 1〕의 조건을 요구하고 있다.

2.2.2 전문인력 자격기준 구성요소

자격기준은 크게 학력, 경력, 보유자격으로 구성된다. 학력은 고급 전문인력에서만 요구되는 요소이므로 경력과 보유자격이 일반, 고급 전반에 거쳐 중요한 비교요소가 된다. 하지만 경력은 전문성에 대한 객관적 비교가 어렵고, 자격취득 이후의 숙련도 평가를 위한 요소이므로 본 논문에서는 세 개 요소 중 보유자격을 중심으로 살펴보기로 한다.

III. 연구 목표 및 방법론

3.1 연구 목표

본 논문의 목표는 다음과 같다.

〔표 1〕 개인정보영향평가 전문인력의 자격기준

	자격기준
일반 수행 인력	1. SIS, ISA, 정보통신 직무분야의 국가기술자격, CISA, CISSP, 그 밖의 개인정보보호 관련 자격 + 1년 이상 관련 경력 2. CPPG + 1년 이상 관련 경력
고급 수행 인력	1. 일반수행인력 자격 + 5년 이상 관련 경력 2. 관련 분야 박사학위 + 3년 이상 관련 경력 3. 정보통신 직무분야의 국가기술자격 + 3년 이상 관련 경력

① 유사자격이 영향평가 전문인력이 갖추어야 할 자격요건을 얼마나 만족하는지 유사성 확인 및 검증

② 유사자격에서 부족한 부분을 보완한 영향평가 자격기준 개선방안 제안

본 논문에서는 정량적 유사도를 기준으로 특정 자격 유사도의 낮고 높음을 판단하는 이분법적 접근보다는, 부족한 부분과 유사한 부분을 파악하여 부족한 부분을 보완할 수 있는 방안을 모색하는 것이 품질을 유지하면서도 초기의 영향평가 수요를 충족시키는 비용 효율적인 방법이라고 판단되어 정성적 비교분석을 한다.

3.2 자격 유사성 비교방법론

영향평가 자격체계와 유사자격들을 비교하기 위해 먼저 유사성의 성격에 따라 개념을 정의하고, 유사성의 비교기준, 비교대상, 비교항목을 설정한다.

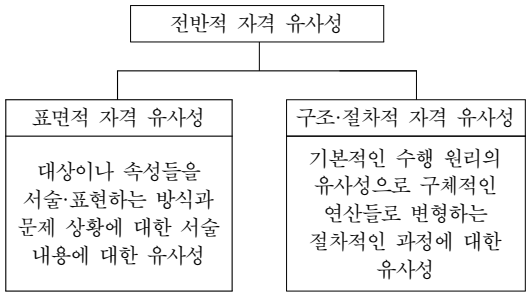
3.2.1 유사성과 자격유사성의 정의

유사성 비교는 영향평가 직무 관점에서 특정 자격의 약점과 부족한 부분을 명확히 파악하여 효과적인 대응을 할 수 있게 해준다.

유사성은 그 성격에 따라 표면 유사성, 구조적 유사성, 절차적 유사성으로 나뉜다. 표면 유사성은 문제에서 서술된 눈에 띄는 구체적인 단어나 문구 등의 서술적 정보의 유사성을 뜻하며, 구조 유사성은 공유하는 해법법칙이나 주요 구성 요인들 사이의 인과적인 관계의 유사성을 뜻한다[5][6]. 절차적 유사성은 문제의 절차적인 세부 사항이 표적 문제의 해결법과 일치하는 유사성을 의미한다[7]. 이러한 표면과 구조, 절차에 대한 유사성을 모두 언급하는 것을 전반적 유사성이라 한다[8].

유사성 개념을 기반으로 자격 유사성을 정의하면 다음과 같다. 표면적 자격 유사성은 업무의 내용을 구성하는 다양한 대상, 대상의 속성, 대상이나 속성을 서술하거나 표현하는 방식과 업무에 대한 서술 내용에 대한 유사성을 뜻하고, 구조·절차적 자격 유사성은 업무수행을 위한 구체적인 절차나 과정으로 전개하는데 필요한 기본적인 수행 원리의 유사성으로 해당 직무수행과 관련된 아이디어를 구체적인 연산들로 변형하는 절차적인 과정에 대한 유사성을 뜻한다. 이러한 표

〔표 2〕 자격 유사성에서의 유사성 정의



면 유사성과 구조·절차적 유사성 두 가지를 모두 갖추었을 때 전반적 자격 유사성을 가진다고 한다. 자격 유사성에서의 유사성에 대한 정의는 〔표 2〕와 같다.

3.2.2 유사성 비교기준

아직까지 객관적인 영향평가 전문자격체계가 마련된 바가 없고, 영향평가 자격에 요구되는 기준이 제시된 바가 없다. 하지만 2012년 5월, 행정안전부와 한국정보화진흥원에서는 "개인정보영향평가 자격제도 수립방안 연구"를 통해 데이컴 기법[3]을 이용한 직무분석과 관련분야 전문가 자문을 거쳐 새로운 영향평가 자격체계를 제시한 바 있다. 따라서 본 논문에서는 위의 연구에서 도출된 영향평가 자격체계를 활용하여 유사성 비교기준으로 제시하도록 한다.

3.2.3 유사성 비교대상

유사성 비교대상에 적합한 유사자격은 CPPG[4]와 ISA[5]이다. CPPG는 유사자격 중 영향평가와 표면적 자격 유사성이 가장 높고 기본지식 부분이 가장 유사하고, ISA는 구조·절차적 자격 유사성이 가장 높고 직무상 기본적인 작업 유형이 가장 유사할 것으로 예상되기 때문이다. CISA와 CISSP과 같은 해외 자격의 경우 효과적이고 실질적인 대안을 마련할 수 있는 가능성이 낮기 때문에 본 논문의 비교 유사자격 비교대상에서 제외하도록 한다.

3.2.4 유사성 비교항목

본 논문에서는 국가자격의 자격요소와 데이컴 기법을 통해 도출한 직무분석 결과물 등을 기반으로 ①운영목적 및 대상 ②작업, ③지식, ④기능, ⑤평가기준, ⑥검정과목을 유사성 비교항목으로 도출하였다.

국내 국가자격의 자격요소는 크게 자격체계, 검정체계, 관리운영체계로 구분된다〔9〕. 본 논문에서는 자격검정체계 전반이 아닌 자격의 전문성 부분을 비교하므로 국가자격의 자격요소 중 자격체계 부분만 이용하도록 한다. 국가자격의 자격체계는 운영목적 및 자격의 활용도를 포함하는 자격의 필요성과 검정기준(지식·기능의 내용 및 수준), 검정방법, 검정과목, 응시자격을 포함하는 자격체계의 적합성으로 구성되며, 이 가운데 본 논문에서는 국가자격의 자격체계의 운영목적, 검정기준, 검정과목을 기준으로 '운영목적 및 대상', '지식', '기능', '검정과목'의 비교항목을 도출하였다.

또한 같은 이름을 가진 지식, 기능이다 하더라도 해당되는 작업에 따라 다른 의미를 가질 수 있기 때문에. 직무분석 결과 도출된 작업 부분을 고려하여 '작업'을 유사성 비교항목에 추가하였다.

그리고 영향평가와 감리, 관리 등의 평가 작업들이 바르게 이루어지기 위해서는 평가항목에 대한 제대로 된 이해가 필수적으로 요구되며, 평가항목에 대한 올바른 이해가 선행되지 못한다면 좋은 평가 품질은 기대할 수 없다. 따라서 평가항목의 목적과 의미에 대한 명확한 이해에 대한 고려를 위해 '평가기준'을 비교항목에 추가하였다.

IV. 영향평가 자격체계와 유사자격 비교

목적 및 대상, 작업, 지식, 기능, 평가기준, 검정과목 관점에서 CPPG와 ISA를 각각 비교하고, 각 자격이 영향평가 자격으로 인정받기 위해 필요한 요소를 도출하였다[6]〔10〕〔11〕〔12〕〔13〕.

비교기준과 대상이 된 CPIA[7]와 CPPG, ISA는

3) 데이컴(DACUM) 기법은 'Developing A Curriculum'의 줄임말로 적은 비용으로 빠른 시간에 결과를 분석하고, 접근방법이 체계적이며, 적용이 용이하여 자격 개발과 교과과정 개발에 많이 사용됨

4) CPPG는 한국CPO포럼에서 개인정보보호 정책 및 대처 방법론에 대한 지식 및 능력을 평가하여 개인정보관리사 자격을 인증하기 위한 목적으로 2009년부터 운영됨

5) ISA는 한국정보화진흥원에서 국가 정보화사업에 대한 감리체계 확립과 실제 정보시스템 분야의 감리 전문 인력 확보를 위해 2000년부터 국가공인민간자격으로 운영됨

6) CPPG에 관련된 내용은 CPPG 공식 웹사이트에서 제공하는 내용을 분석하였고, ISA에 관련된 내용은 한국직업능력개발원의 "정보시스템감리사 직무분석"과 한국정보화진흥원의 "정보화사업 감리 수행 가이드"에서 제공하는 내용을 분석함

모두 데이컴 기법을 사용하여 만들어졌지만, 업무를 나누거나 지식, 기능, 검정과목을 뽑은 수준이 각기 다르다. 따라서 관련 자료들을 기반으로 직무분석 결과물의 수준을 맞추는 정규화 작업을 선행하였다. 정규화 과정에서 불가피하게 세부적인 내용이 삭제되거나 특정 부분이 확대되는 오류가 발생하였을 가능성이 존재하지만 각각의 자격 개발 및 운영 관련 자료들을 토대로 오류 발생 가능성을 최소화하였다.

4.1 비교기준 1 : 목적과 대상

일반적으로 유사자격들은 자격취득의 목적과 대상이 유사하기 때문에 일부 차이가 존재 하지만 대체자격이 될 가능성이 높다고 할 수 있다.

4.1.1 목적 비교

CPIA, CPPG, ISA간 구체적인 목적 비교는 〔표 3〕와 같다.

CPPG와 CPIA는 개인정보보호 분야의 인력양성을 목적으로 하고 있지만, CPIA가 영향평가라는 전문적인 업무와 관련된 지식을 갖춘 전문가 양성을 목적으로 하는데 반해, CPPG는 좀 더 범용적인 개인정보관리 인력을 요구한다는 차이가 존재한다.

ISA의 경우 정보시스템감리업무를 담당할 전문가를 양성하는 것을 목적으로 하지만 CPIA와 ISA는 정보시스템의 체계를 확립하여 활성화를 유도하며, 시스템의 문제점을 사전에 파악하여 개선 방안을 도출한다는 측면에서 목적이 일치하는 부분이 존재한다. 하지만 CPIA는 목적의 대상이 개인정보를 활용하는 정보시스템에 관련되어 있다는 점에서 차이점을 보인다.

4.1.2 대상 비교

CPIA는 영향평가, CPPG는 개인정보관리, ISA는 정보시스템 감리 직무를 대상으로 한다. CPIA, CPPG, ISA 간 구체적인 대상 비교는 〔표 4〕와 같다.

개인정보관리업무는 개인정보위험분석을 포함한 개인정보 정책수립부터 시스템 구축, 감사 및 사고대응

〔표 3〕 자격 간 목적 비교

자격명	목적
CPIA	• 개인정보보호 및 영향평가 전문가와 품질관리 전문가의 체계적 양성 • 영향평가 체계 확립 지원 및 활성화 • 개인정보보호 및 영향평가 업무 능력 평가에 대한 객관적 지표 마련
CPPG	• 개인정보보호가 요구되는 산업계 전문가 배출 • 개인정보보호 업무 능력 평가에 대한 객관적인 지표 마련
ISA	• 정보시스템 감리 담당 전문가 양성 • 감리체계의 확립 지원 및 감리의 활성화 유도

등의 업무를 포괄하며, 이는 개인정보를 관리기관이 고용한 개인정보 관리자의 업무이다. 반면, 개인정보처리시스템 도입 시에 전문기관에 의해 수행되는 영향평가의 경우 일반적으로 기업의 개인정보관리활동에는 직접적으로 포함되지 않는다. 개인정보보호 감사활동이 포함되기는 하지만 사전적 성격의 영향평가와는 달리 수립된 개인정보보호정책과 시스템들, 관리 활동들이 제대로 수행되고 있는지 사후적으로 평가하는 것으로 영향평가와는 성격이 다르다.

정보시스템감리는 주로 기술적 측면에서 프로젝트가 기본계획대로 되었으며, 효율성, 신뢰성, 품질보증 등 기술적 요건이 보장되고 있는가를 감독·지도·평가하는 활동을 말한다. 감리 활동은 성과의 극대화를 위한 관리적, 기술적 성격이 강하며 사후적이기 보다 진행 중인 사업을 성공적으로 완수시키는 것을 목적으로 한다.

4.1 비교기준 2 : 업무

직무기반 자격을 비교하는데 있어 중요한 것은 특정 직무를 수행할 수 있는 여부에 대한 것이므로 업무는 기본적인 비교대상이 된다. 업무가 유사하다면 해당 업무를 수행하기 위해 필요한 지식과 기능, 해당 지식과 기능을 평가하기 위한 검정 도메인도 유사하다고 할 수 있기 때문에 업무는 가장 중요한 비교대상이라고도 할 수 있다.

CPIA의 업무는 크게 평가계획의 수립, 영향평가의 실시, 평가결과의 정리로 구분되면 자세한 내용은 〔표 5〕와 같고, CPPG는 크게 기획, 전략수립 및 구현, 개인정보 관리, 감사 및 대응으로 구분되며 자세한 내용은 〔표 6〕과 같다. CPPG의 직무 자체는 관리 업무

7) Ⅳ장과 Ⅴ장에서는 "개인정보영향평가 자격제도 수립방안 연구"에서 도출한 영향평가 자격체계를 자격 비교상의 편의를 위해 'Certified Privacy Impact Assessor'를 의미하는 CPIA라 칭함

〔표 4〕 자격 간 대상 비교

자격명	대상
CPIA	• 개인정보영향평가: 개인정보를 활용하는 새로운 정보시스템의 도입이나 기존 시스템의 중대한 변경 시 동 시스템의 구축, 운영, 변경 등이 개인정보에 미치는 영향을 사전에 조사, 예측, 검토하여 개선 방안을 도출하는 체계적인 절차
CPPG	• 개인정보관리: 개인정보보호 정책 및 대처 방법론에 대한 지식 및 능력을 바탕으로 개인정보 취급자 관리, 개인정보보호와 관련된 보안정책 수립, 관련법규에 대한 지식 적용
ISA	• 정보시스템감리: 독립된 객관적 입장에서 정보시스템 분야에 대하여 안전성, 효율성, 효과성, 준거성, 무결성, 신뢰성 등의 시스템 전반 사항을 점검, 분석, 평가 한 후 문제점 등을 찾아내어 개선사항을 컨설팅하는 일련의 행위

이지만, 단순한 관리업무나 침해사고 대응 업무만이 아닌 요구사항분석과 위험분석업무, 정보보호감사업무 등을 포괄한다는 점에서 CPIA의 세부 업무와 일치되는 부분이 상당 부분 존재한다. 예를 들어 CPPG 입장에서 보면 CPIA 업무 중 개인정보흐름분석을 위한 업무 일부와 개인정보침해요인분석을 위한 위험분석과 감사, 개선계획 수립을 위한 보호정책 수립의 경우 유사한 부분이 존재한다. 반면, 평가계획 수립과 관련된 부분과 실제 영향평가 실시하는 부분의 평가자료 수집과 개인정보 취급업무흐름도, 개인정보흐름표, 개인정보흐름도, 정보시스템구조도 작성 등의 구체적인 실제 업무는 포함하고 있지 못하며, 실제 영향평가 영역과 평가항목을 구성하는 업무와 구체적인 영향평가서 작성하는 내용도 빠져있다.

ISA의 업무는 감리계획, 감리수행, 감리보고, 사후관리로 구분되면 자세한 내용은 〔표 7〕과 같다. 감리계획에서 감리수행, 감리보고, 사후관리에 이르는 기본적인 업무 절차와 성격은 CPIA의 영향평가 업무와 유사한 것으로 보인다. 하지만 감리업무의 수행 대상이 일치하지는 않기 때문에, ISA의 감리업무 수행 인증이나 경험이 형식적인 평가수행능력에 도움을 줄 수는 있어도, 구체적인 영향평가 업무와는 완전히 일치하지 않으므로 구조적 유사성으로 업무수행 가능성을 완전히 보장할 수는 없다. 특히 ISA에서는 영향평가 실시 업무에서 개인정보 취급현황 분석, 업무흐름도, 개인정보흐름표, 흐름도 작성과 같은 업무에 대한 내용은 빠져있으며, 개인정보침해요인분석 업무의 영향평가 영역 및 평가항목 구성, 개인정보보호조치 현황, 침해요인 도출, 개인정보 위험도 산정과 같은 업무에

〔표 5〕 CPIA 업무

책무	작업
A 평가계획의 수립	A1 영향평가 필요성 검토
	A2 영향평가 수행주체 선정
	A3 영향평가 수행계획 수립
B 영향평가의 실시	B1 평가자료 수집
	B2 개인정보 흐름분석
	B3 개인정보 침해요인 분석
C 평가결과의 정리	C1 개선계획의 수립
	C2 보고서 작성

〔표 6〕 CPPG 업무

책무	작업
A 기획	A1 요구사항 조사하기
	A2 위험 분석하기
	A3 보호정책 수립하기
B 전략수립 및 구현	B1 총괄전략 수립하기
	B2 보호정책 구현하기
C 개인정보 관리	C1 개인정보 흐름별 관리하기
	C2 교육 및 훈련하기
D 감사 및 대응	D1 보호현황 감사하기
	D2 침해사고 대응하기

대한 내용도 포함하고 있지 않다.

4.2 비교기준 3 : 지식

CPPG는 개인정보 관련 지식 부분에서 많은 부분이 CPIA와 유사하다. 개인정보관리체계 부분에 영향평가와 관련된 내용이 일부 포함되지만, 이는 영향평가의 목적과 기본개념, 절차, 체계, 영향평가팀의 주요역할 등 개요적인 내용으로 영향평가 대상 선정 방법, 현장 조사 기법, 보고서 작성 방법 등 구체적인 영향평가 수행방법에 관한 내용은 배제되어 있다. 위험관리에 관한 내용도 공통적으로 포함하고 있지만, CPPG에서는 위험을 분석하기 위한 절차 정도의 지식을 요구하고 CPIA에서는 방법론은 물론 CCTV, RFID 등 구체적인 정보기술에 대한 위험분석을 할 수 있는 수준의 지식을 요구한다. 이 밖에 전반적인 정보기술에 관한 지식, 현장조사방법, 품질보증방법 등과 같은 프로젝트 수행 시 필요한 지식이 포함되어 있지 않다.

ISA는 감리방법론, 즉 문제를 분석·평가하는 방법이나 프로젝트 수행 방법론에 관한 지식, 데이터베이

〔표 7〕 ISA 업무

책무	작업
A 감리계획	A1 감리 대상 선정하기
	A2 예비 조사하기
	A3 도구와 기법 확보하기
	A4 감리 일정과 인력 계획하기
	A5 감리 프로그램 개발하기
	A6 감리 계획서 작성하기
B 감리수행	B1 착수 회의와 현황 파악하기
	B2 감리 프로그램 수정하기
	B3 증거 수집하기
	B4 증거 평가하기
	B5 결론 도출하기
C 감리보고	C1 감리 보고서 초안 작성하기
	C2 감리 보고서 초안 확인하기
	C3 감리 보고서 최종안 작성하기
	C4 감리 종료 회의하기
	C5 감리 보고서 제출하기
D 사후관리	D1 시정 조치 계획 검토하기
	D2 시정 조치 결과 확인하기
	D3 감리 품질 평가하기

스, 시스템 구조 등 일반적인 정보기술과 관련된 지식, 정보시스템의 품질이나 보안 관련 측면에서의 영향평가와 유사한 지식을 요구한다. ISA는 영향평가 수행을 위한 일반적인 방법론과 노하우와 같은 지식은 충분히 제공하는 한편, 영향평가 수행을 위해 필수적

〔표 8〕 자격 간 지식비교

자격명	지식
CPIA	• 영향평가의 개요와 이해 • 프로젝트 수행 방법론 개요와 이해 • 조직체계와 비즈니스의 이해 • 정보기술 및 정보시스템 개요와 이해 • 개인정보보호 관련 컴플라이언스 개념과 이해 • 해킹대응기술의 개요와 이해 • 개인정보파일 운영체계 이해 • 2차적 정보생성 개념 이해 • 특정IT기술 이해(CCTV, RFID 등) • 품질보증방법 및 품질관리전략에 대한 지식 • 정보수집 및 보존 기법 이해 • 개인정보보호 및 정보보호관련 법제 이해 • 개선방안 및 개선계획 수립 방법 • 개인정보 흐름분석 이해 • 위험관리 개요와 이해 • 정보보안체계 이해 • 현장조사방법 이해 • 개인정보처리 이해
CPPG	• 개인정보의 개요 개인정보의 중요성 • 개인정보보호 관련 법률체계 • 개인정보보호 원칙과 의무 • 개인정보 관리체계 개요 • 주요 개인정보 관리체계 • 개인정보 보호조치의 개요 • 개인정보의 기술적 관리적 보호조치 기준 • 개인정보 수집·이용 원칙 • 개인정보 저장·관리 원칙 • 개인정보 처리 시 유의사항 • 기업의 사회적 책임 • 정보주체의 권리 • 개인정보 위탁 원칙 • 분쟁해결절차 • 기업의 사회적 책임 • 위험관리의 이해
ISA	• 감리목적과 기본 개념 • 계약처리 규칙 • 감리계획 수립방법 • 감리수행 절차 • 조사·시험방법 • 분석과 평가방법 • 계약처리 규칙 • 감리의 절차와 기술 • 정보기술 • 프로젝트 관리 • 정보시스템 품질 • 정보시스템 보안 • 감리기준·지침 체계와 내용 • 감리 프로그램 작성방법 • 감리보고서 작성방법 • 감리대상 업무별 감리 접근방법

으로 요구되는 개인정보 관리, 보호와 관련된 기본적인 지식과 개인정보위험분석과 관련된 부분, 구체적인 영향평가방법에 대한 지식은 전혀 제공하지 못한다.

4.3 비교기준 4 : 기능

CPPG의 경우 개인정보시스템 분석, 관리체계 수립, 개인정보 흐름분석 등 개인정보 관련 능력의 일부분은 포함하고 있지만, 개인정보 영향 분석을 수행할 수 있는 기능은 포함하고 있지 않다. 또 위험 파악능력이나 IT 환경분석 능력, 위험통제 비용이나 통제수준 및 허용수준 등을 추정하는 등 영향평가를 수행하는데 있어 필요한 핵심적인 능력은 부족하다. 또한 평가업무와 결과의 품질을 유지하기 위한 기능과 평가 및 감리업무에서 필수적으로 요구되는 능력인 대인관계기술과 소통능력도 요구하지 않는다.

ISA의 경우 IT 환경분석 능력, 위험파악 능력, 프로젝트 수행 시 협상기술, 회의주관 능력, 대인관계기술 등의 CPIA에서 요구하는 필수적인 기능과 능력들을 포함하고 있다. 하지만 개인정보영향분석 능력 등 개인정보 관련 기능은 요구하고 있지 않다.

〔표 9〕 자격제도 간 기능비교

자격명	기능
CPIA	• 문서작성능력 • 도구 활용능력 • 대인관계 기술 • 의사소통 및 경청능력 • 이해력 • 자기개발능력 • 발표력 • 컴퓨터 활용능력 • 회의 주관 능력 • 논리적 추론 능력 • 자원관리 능력 • 위험 파악 능력 • 프로젝트 관리 능력 • 의사결정능력 • 업무분해 기술 • 보호대책 수립 • 영향평가 가능성에 대한 판단 능력 • 개인정보 영향 분석 능력 • 자료 수집, 분류, 관리, 분석 능력 • 문제점 파악 및 분석 능력 • 영향평가 계획수립 능력 • 내·외부 IT 환경분석 능력 • 법제 요구사항 분석 능력 • 평가항목 이해 및 개발 능력
CPPG	• 법제도 분석 능력 • 조직구성 능력 • 자료 문서화 능력 • 보고서 작성 능력 • 자료 수집 및 조사 능력 • 자료 분류 및 평가 능력 • 분석관련 소프트웨어 사용능력 • 개인정보보호에 대한 비용효과 분석 능력 • 개인정보시스템 분석 능력 • 보호대책 수립 혹은 통제 능력 • 자원 할당법 및 일정계획 능력 • 비상계획 및 업무 지속성 관리 능력 • 개인정보보호시스템 운영 능력 • 네트워크 트래픽 분석 능력 • 시스템 로그 분석 능력 • 교육자료 작성 및 교육방법론 • 개인정보관리체계 수립 및 조사능력 • 개인정보 침해 현황 조사 및 분석 • 경찰, 검찰, 국정원 등 수사 협조 능력
ISA	• 협상기술 • 대인관계기술 • 계획수립 능력 • 의사소통능력 • 문제점 파악 능력 • 논리적 추론능력 • 정보검색능력 • 평정·계산능력 • 이해력 • 위험 파악 능력 • 문서작성능력 • 보호대책 수립 • 회의주관 능력 • 법제도 분석 능력 • 발표력 • IT 환경분석 능력 • 프로젝트 관리 능력 • 감리가능성에 대한 판단 능력 • 자료 수집과 분류·분석 능력

4.4 비교기준 5 : 평가기준

영향평가와 감사, 감리 등의 평가 작업들이 제대로 이루어지기 위해서는 평가항목의 목적과 의미 등, 평가항목에 대한 제대로 된 이해가 필수적으로 요구된다.

〔표 10〕 CPIA 평가기준

평가영역	평가분야
1. 대상기관 개인정보보호 관리체계	• 대상기관 개인정보 보호조직 • 개인정보 보호계획 • 개인정보 처리방침 • 개인정보 파일관리 • 개인정보 위탁 및 제공시 안전 조치 • 개인정보 침해대응 • 정보주체 권익보호 • 개인정보 처리구역 보호
2. 대상시스템의 개인정보보호 관리 체계	• 대상 시스템의 개인정보 관리 • 개인정보 취급내용 공개
3. 개인정보 처리 단계별 보호	• 수집단계 • 파기단계 • 저장 및 보유단계 • 이용 및 연계·제공 단계
4. 특정 IT 기술 활용 시 개인정보보호	• CCTV 활용 • 바이오 정보 활용 • RFID 활용 • 위치정보 활용

평가항목의 경우, 직무분석에서 분석된 내용이 아니기 때문에 CPIA는 행정안전부의 "개인정보 영향평가 수행 안내서" 부록의 개인정보영향평가 항목을, ISA는 한국정보화진흥원의 "정보화사업 감리 수행 가이드"에서 정보화사업 유형별 표준 점검항목을 참고하였다. CPPG는 별도의 평가항목을 가지고 있지 않으므로, 가장 유사한 평가항목체계인 개인정보관리체계(이하 PIMS)[8]의 평가항목들을 이용하였다.

CPIA의 평가기준은 크게 대상기관 개인정보보호관리체계, 대상시스템의 개인정보보호관리체계, 개인정보 처리 단계별 보호, 특정 IT 기술 활용 시 개인정보보호로 구분되며 〔표 10〕과 같다. CPPG의 평가기준으로 사용되는 PIMS의 평가기준은 크게 개인정보보호 관리과정 요구사항, 개인정보 보호대책 요구사항, 생명주기 요구사항으로 구분되며 〔표 11〕과 같다. PIMS의 개인정보보호 관리과정 요구사항과 개인정보보호대책 요구사항의 경우 대상기관 및 대상시스템의 개인정보보호관리체계를 수립하고 있다. PIMS의 평가기준들은 CPIA의 대상기관 및 대상시스템의 개인정보보호관리체계 부분을 모두 만족시킨다. 이는 CPPG의 주요 내용에 해당되는 사항이기도 하다. 또

8) PIMS는 한국인터넷진흥원에서 기업이 개인정보보호 활동을 체계적·지속적으로 수행하기 위해 필요한 보호조치 체계를 구축하였는지 점검하여 일정 수준 이상의 기업에 인증을 부여하는 제도임

한 PIMS의 생명주기 요구사항의 개인정보 수집, 이용, 제공, 파기에 따른 조치사항도 CPIA의 개인정보 처리단계별 보호를 반영하고 있다. 하지만, PIMS나 CPPG는 특정 IT 기술 활용시의 개인정보보호 요구사항, 즉 CCTV, RFID, 바이오정보, 위치정보 활용시의 조치사항들을 제대로 이행하고 있는지에 대한 내용은 포함하고 있지 않다.

〔표 11〕 PIMS 평가기준

평가영역	평가분야
1. 개인정보보호 관리과정 요구사항	• 개인정보 정책수립 • 관리체계 범위설정 • 구현 • 위험관리 • 사후관리
2. 개인정보 보호대책 요구사항	• 개인정보 보호정책 • 개인정보 보호조직 • 침해사고 처리 및 대응절차 • 개인정보 분류 • 기술적 보호조치 • 교육 및 훈련 • 물리적 보호조치 • 인적보안 • 내부검토 및 감사
3. 생명주기 요구사항	• 개인정보 수집에 따른 조치 • 개인정보 이용 및 제공에 따른 조치 • 개인정보 관리 및 파기에 따른 조치

〔표 12〕 ISA 평가기준

평가영역	평가분야
1. 정보기술 아키텍처 구축 사업	• 기반정립 • 관리체계 • 이행계획 수립 • 현행 아키텍처 구축 • 기반정립 및 현행 아키텍처 구축 시 품질보증 활동 • 목표 아키텍처 구축 • 목표 아키텍처 구축 및 이행계획 수립 시 품질보증 활동
2. 정보화전략 계획수립 사업	• 업무 • 기술 • 현황분석 및 전략수립 시 품질보증 활동 • 정보화 계획 • 개선모델 및 실행계획 수립 시 품질보증 활동
3. 시스템 개발 사업	• 시스템 구조 • 품질보증활동 • 응용시스템 • 시험활동 • 데이터베이스 • 운영준비
4. 데이터베이스 구축사업	• 데이터 수집 및 시범구축 • 데이터 구축 • 품질검사
5. 시스템 운영 사업	• 서비스 제공 • 서비스 지원
6. 유지보수 사업	• 유지보수
7. 사업관리	• 착수/계획 시 사업관리 • 실행/통제 시 사업관리 • 종료 시 사업관리

ISA의 평가기준은 크게 정보기술 아키텍처 구축 사업, 정보화전략 계획수립 사업, 시스템 개발사업, 데이터베이스 구축사업, 시스템 운영사업, 유지보수 사업, 사업관리로 구분되며 〔표 12〕와 같다. ISA의 경우 주요 기준항목들이 성능, 효율성, 보안성 등 다양한 영역으로 평가하는데 비해, CPIA는 개인정보보호의 관점에서만 평가하므로 평가기준 항목에서는 유사한 부분을 찾기가 어렵다. 개인정보보호를 위한 평가기준으로 활용될 수 있는 각 감리대상 별 보안성 관련 기준들의 경우만 유사하다고 할 수 있다. 이처럼 사용자 보안부분에 대한 요구조건과 관련해서 일부 중복되지만 개인정보 관련 내용이 없으며 그 외의 경우에는 공통분모가 존재하지 않는다.

4.5 비교기준 6: 검정과목

검정과목들은 직무분석 결과 도출된 지식과 기능을 반영한 것이므로 결과가 업무, 지식, 기능과 유사하게 나올 것으로 예상되지만 이러한 지식과 기능을 제대로 반영하고 있는지 다른 부가적인 지식과 기능을 포함하고 있는지 각각의 지식과 기능이 어느 정도 구체적인지는 또 다른 문제이다. 그러므로 최종적인 결과물로서의 검정과목은 다른 비교기준들과는 차별화된 독자적 비교대상이 될 수 있다.

CPIA의 검정과목은 〔표 13〕과 같이 (개인)정보처리 기술 및 환경, 개인정보보호 법률 및 정책, 개인정보 보호 기술 및 관리, 개인정보영향평가 이론, 개인정보 영향평가 실무, 프로젝트 품질관리로 구성된다. CPPG의 검정과목은 〔표 14〕와 같이 개인정보 보호의 이해, 개인정보 보호제도, 개인정보 라이프사이클 관리, 개인정보의 보호조치, 개인정보 관리체계로 구성된다.

〔표 13〕 CPIA 검정과목

검정과목	일반	고급
(개인)정보처리 기술 및 환경	○	○
개인정보보호 법률 및 정책	○	○
개인정보보호 기술 및 관리	○	○
개인정보영향평가 이론	○	○
개인정보영향평가 실무	×	○

〔표 14〕 CPPG 검정과목

과목명	과목내용
1 개인정보 보호의 이해	1-1 개인정보의 개요 1-2 개인정보보호의 중요성 1-3 기업의 사회적 책임
2 개인정보 보호제도	2-1 개인정보보호 관련 법률체계 2-2 개인정보보호 원칙과 의무 2-3 정보주체의 권리 2-4 분쟁 해결절차
3 개인정보 라이프사이클 관리	3-1 개인정보 수집, 이용 3-2 개인정보 저장, 관리 3-3 개인정보 제공
4 개인정보의 보호조치	4-1 개요 4-2 개인정보의 기술적·관리적 보호 조치 기준
5 개인정보 관리체계	5-1 개인정보관리체계 개요 5-2 주요 개인정보 관리체계

CPPG의 모든 도메인은 개인정보관리 및 보호에 필요한 기초적인 일반적인 내용들을 포괄하고 있으므로, 영향평가 수행에 필요한 기본적인 내용들을 포괄하고 있다고 보인다. 특히 영향평가자격의 교육 도메인인 개인정보보호법률 및 정책, 개인정보보호기술 및 관리 등과 많은 부분 유사하다. 문제는 영향평가 수행에 필요한 개인정보처리기술 및 환경에 대해서는 포함하고 있지 않고 영향평가의 내용이 개인정보관리체계 도메인에 아주 적은 비중으로 간단하게 소개되고 있다. 또한 영향평가 실무 도매인에 대해 매우 단순한 소개 정도에 그치고 있고 프로젝트 품질관리와 관련된 내용이나 영향평가 단계별 품질 관리 요건 및 방법에 대한 내용도 포함하고 있지 않다.

ISA의 검정과목은 〔표 15〕와 같이 감리 및 사업관리, 소프트웨어 공학, 데이터베이스, 시스템 구조, 보안으로 구성된다. ISA의 데이터베이스 도메인과 시스템 구조 도메인은 CPIA의 개인정보 처리기술 및 환경 부분의 내용을 포괄하고 있다. CPIA의 경우 정보시스템 중 구체적으로 개인정보처리기술과 관련된 기술들을 위한 기반 기술들에 대한 충분한 내용을 제공하는 것으로 보여진다. 또 보안 도메인은 CPIA의 개인정보보호기술 및 관리 도메인의 정보보안 개요 및 취약성, 위협 등의 침해위험과 개인정보 침해위험 분석 및 대응기술, 개인정보 기술적, 관리적 보호조치 부분에 포함되는 기본적인 보안취약점과 기술적, 관리적 보안대책의 내용을 포괄하고 있다. 또한 ISA 경우 감리 및 사업관리 도메인의 감리지침 및 관련 기술, 조직관리론, 프로젝트 관리의 경우 영향평가 이론과 실무 도메인을 이해하고 수행하는데 필요한 일반적인 경영적 지식들을 제공한다는 점에서 유용하다.

〔표 15〕 ISA 검정과목

과목명	과목내용
1 감리 및 사업관리	1-1 공통 기술 1-2 정보화·감리 관련 법·제도 1-3 감리지침 및 관련기술 1-4 조직 관리론 1-5 프로젝트관리
2 소프트웨어 공학	2-1 객체지향 및 컴포넌트 기술 2-2 디자인 패턴 2-3 프로세스 품질 2-4 비용 산정 2-5 정보화 관련 표준 2-6 개발 방법론 2-7 프로그래밍 언어 2-8 시스템 테스트 2-9 사용자 인터페이스 2-10 유지보수 2-11 SW 분석설계
3 데이터베이스	3-1 자료 구조론 3-2 데이터마이닝 3-3 데이터베이스 개념 3-4 관계형 DB 지식 3-5 객체지향 DB 지식 3-6 DB관련 기술 3-7 상용 DBMS 지식 3-8 인터넷 정보처리 3-9 경영 기반기술
4 시스템 구조	4-1 아키텍처 설계 4-2 응용 기술 4-3 시스템 성능·용량산정 4-4 컴퓨터 시스템 4-5 통신 시스템 4-6 네트워크 4-7 기타 신기술
5 보안	5-1 보안기술 5-2 보안관리

V. 영향평가 자격체계와 유사자격 비교결과

5.1 비교 결과 분석

5.1.1 CPIA와 CPPG 유사성 분석결과

①목적과 대상 기준에서는 CPPG는 CPIA와 개인정보보호 인력 양성이라는 목적이 유사해 보이지만, 그 목적의 대상이 근본적으로 일치하지 않는다. ②업무 기준에서는 CPPG의 직무 자체의 성격이 관리이

지만 단순한 관리업무나 침해사고 대응 업무만이 아닌 요구사항 분석과 위험분석업무, 정보보호 감사업무 등을 포괄한다는 점에서 CPIA의 세부 업무와 일치하는 부분이 상당 부분 존재한다고 볼 수 있다. 하지만 평가계획 수립과 관련된 부분, 실제 영향평가 실시 시 구체적인 실제 업무, 영향평가서 작성하는 내용은 포함하고 있지 못하다. ③지식 기준에서는 개인정보 관련 지식 부분이나 영향평가 수행에 필요한 개인정보 관련 지식은 충분히 제공하고 또 개인정보관리체계 부분에 영향평가 개요 수준의 내용을 포함하고 있다. 하지만 구체적인 영향평가 수행방법에 관한 내용은 배제되어 있고, 프로젝트 수행 시 필요한 지식이 포함되어 있지 않다. ④기능 기준에서는 개인정보 관련 능력의 일부분만을 포함하고 개인정보 영향 분석을 수행할 수 있는 기능, 영향평가 수행 시 필요한 핵심적인 능력, 평가업무와 대인관계기술과 소통능력에 대해서도 중점을 두고 있지 않다. ⑤평가기준 기준에서는 특정 IT 기술 활용 시의 개인정보보호 요구사항 평가영역을 제외한 나머지 평가기준 항목은 매우 유사하다고 판단된다. ⑥검정과목 기준에서는 CPPG의 모든 도메인은 개인정보관리 및 보호에 필요한 기초적인 일반적인 내용들을 포괄하고 있으므로, 영향평가 수행에 필요한 기본적인 내용들을 포괄하고 있다고 볼 수 있다. 하지만 CPPG는 영향평가와 같은 특정 관리체계, 개인정보처리기술 및 환경, 프로젝트 품질관리에 대한 내용은 포함하고 있지 않으며, 영향평가 관련 내용은 아주 적은 비용으로 간단하게 소개되고 있는 정도에 머물러 있다.

CPPG는 영향평가 수행에 필요한 개인정보관리 및 보호와 관련된 일반적인 지식을 갖출 수 있도록 보장해주고, 영향평가 기준들에 대한 이해를 제공하는데 반해, 이러한 지식을 가지고 실질적으로 영향평가를 수행할 수 있도록 하기 위한 절차적 지식, 일반 관리적 지식, 품질보증 및 관리와 관련된 지식과 기능, 평가기준 및 검정과목은 존재하지 않고, 영향평가 업무 숙련도를 평가할 수 있는 항목이 없다는 한계가 존재한다. 또한 구체적으로 개인정보영향분석을 수행해야 할 개인정보처리시스템과 CCTV, RFID와 같은 환경에 대한 지식 또한 제공하고 있지 못하다.

CPPG와 CPIA는 자격간의 큰 차이가 존재 한다고 하기 보다는 포함관계에 있다고 표현 할 수 있다. CPPG의 내용 대부분이 CPIA의 일부분에 포함되므로 CPPG 보유만으로는 다양한 환경에서의 영향평가를 수행하고 전 과정을 관리할 수 있는 프로젝트 관리자급 영향평가 전문인력으로 인정해주기는 어렵다. CPPG가 영향평가 대체자격이 되기위해서는 특수한 개인정보처리시스템, 영향평가 절차 및 기준, 프로젝트 관리, 품질관리, 평가기법 등에 관해 추가적인 검

〔표 16〕 CPIA와 CPPG 유사성 비교 결과

기준	유사한 부분	부족한 부분
목적과 대상	• 개인정보보호 분야의 인력양성	• 대상의 차이 CPIA: 영향평가 CPPG: 개인정보관리 • 영향평가 업무
업무	• 요구사항 분석과 위험분석업무, 정보보호감사 업무 등	• 평가계획 수립 관련 부분과 평가항목을 구성하는 업무 • 실제 영향평가 실시 부분의 구체적 업무와 영향평가서 작성 내용
지식	• 개인정보 관련 지식 • 영향평가 관련 개요적인 내용 • 영향평가 수행에 필요한 개인정보관리 및 개인정보보호와 관련된 기본 지식	• 구체적인 영향평가 수행방법 • 프로젝트 수행 시 필요한 지식 • 구체적인 영향평가 수행방법에 대한 지식
기능	• 개인정보 관련 능력	• 개인정보 영향 분석 수행 능력 • 영향평가 수행에 필요한 핵심적인 능력 • 평가업무와 결과의 품질 유지 능력 • 대인관계기술과 소통능력
평가기준	• 대상기관의 개인정보보호관리체계 • 대상시스템의 개인정보보호관리체계 • 개인정보처리단계별 보호	• 특정 IT 기술 활용시의 개인정보보호 요구사항
검정과목	• 개인정보에 대한 법적·기술적 내용 • 개인정보보호의 이해, 개인정보보호의 중요성, 개인정보라이프사이클관리, 개인정보보호조치, 개인정보관리체계 등 • 개인정보보호법률 및 정책, 개인정보보호 기술 및 관리 등	• 특정 관리체계에 대한 이론과 실무 내용 • 프라이버시 위험 작성 방법과 영향평가 수행보고서 작성 방법 • 개인정보처리기술 및 환경에 대한 내용 • 영향평가 수행에 필요한 구조, 절차적, 방법론적 지식 • 프로젝트 품질관리와 관련된 내용이나 영향평가 단계별 품질 관리에 대한 내용

증이 요구된다. 즉, CPPG는 CPIA와 구조·절차적 유사성 보다는 표면 유사성이 높으므로 이에 따라 표면적으로 포괄하지 못한 지식들과 함께 구조·절차적 부분에 대한 보강이 필요하다.

5.1.2 CPIA와 ISA 유사성 분석 결과

①목적과 대상 기준에서는 시스템의 문제점을 사전에 파악하여 개선 방안을 도출하고 정보시스템 체계 확립 및 활성화 측면에서 목적이 일치하지만, CPIA는 목적의 대상이 개인정보를 활용하는 정보시스템으로 한정되어 있어 유사하다고 보기는 어렵다. ②업무 기준에서는 계획, 수행, 사후관리에 이르는 기본적인 업무 절차가 유사해 구조·절차적 유사성이 높아 보이지만, 업무수행 대상이 일치하지 않아 ISA는 CPIA에서 포함하는 영향평가 업무에 관한 내용이나 개인정보침해요인분석 업무를 포함하고 있지 못하다. ③지식 기준에서는 프로젝트 수행 방법론에 관한 지식, 일반적인 정보기술과 관련된 지식, 정보시스템의 품질이나 보안과 관련된 측면에서의 지식은 상당수 유사한 지식을 요구한다. 하지만 영향평가 수행을 위해 필수적으로 요구되는 개인정보 관리·보호와 관련된 지식은 물론, 개인정보위험분석과 관련된 부분, 구체적인 영향평가 방법에 대한 지식은 전혀 제공되지 못하고 있다. ④기능 기준에서는 ISA는 CPIA에서 요구하는 필수적인 기능과 능력들을 대부분 포함하고 있다. 하지만 개인정보영향분석 능력 등 개인정보 관련 기능은 요구하고 있지 않다. 따라서 구조적인 기능은 유사하더라도 실제 구체적으로 개인정보관리 환경에서 적용하여 잘 작동할 수 있을지는 보장하기가 어렵다. ⑤평가기준 기준에서는 각 대상 별 보안성 관련 기준의 경우와 사용자 보안부분에 대한 요구조건과 관련해서는 일부 유사한 부분이 존재한다. 하지만 정보시스템 감리의 경우 성능, 효율성, 보안성 등 다양한 영역으로 평가하는데 비해, CPIA는 개인정보보호의 관점에서만 평가하므로 유사한 부분을 찾기가 어렵다. ⑥검정과목 기준에서는 정보시스템에 대한 지식, 일반적인 방법론, 프로젝트 수행 시 필요한 지식들을 공통적으로 포함하고 있다. 하지만 이러한 지식들이 일반적인 지식에 머물러 있을 뿐 ISA에서는 구체적인 개인정보처리 시스템과 이 시스템과 네트워크에 대한 위험성들에 대해서는 다루고 있지는 않는다. 또 CPIA의 경우 ISA와는 달리 정보시스템 중 구체적으로 개인정보처리기술과 관련된 기술들만을 다루고 있다는 차이점이 존재한다.

〔표 17〕 CPIA와 ISA의 유사성 비교 결과

기준	유사한 부분	부족한 부분
목적과 대상	• 정보시스템 체계 확립 및 활성화 유도, • 시스템의 문제점을 사전에 파악하여 개선 방안 도출	• 대상의 차이 CPIA: 개인정보를 활용하는 정보시스템 ISA: 정보시스템
업무	• 기본적인 업무 절차와 업무의 성격	• 구체적인 영향평가 업무 • 개인정보침해요인분석 업무
지식	• 감리방법, 프로젝트 수행 방법론에 관한 지식 • 일반적인 정보기술 관련 지식 • 정보시스템 품질이나 보안 관련 지식 • 영향평가 수행을 위한 일반적인 방법론과 노하우와 같은 지식	• 영향평가 수행을 위해 필수적으로 요구되는 기본적인 지식 • 개인정보위험분석과 관련된 부분, 구체적인 영향평가방법에 대한 지식
기능	• IT 환경분석 능력, 위험파악 능력, 프로젝트 수행 시 협상기술, 회의주관 능력, 대인관계 기술 등	• 개인정보영향분석 능력 등의 개인정보 관련 기능
평가기준	• 대상 별 보안성 관련 기준 • 사용자 보안부분에 대한 요구조건	• 개인정보 관점의 평가기준
검정과목	• 기본적인 일반 방법론 • 시스템, 네트워크, 데이터베이스에 대한 기본적인 지식 • 정보시스템에 대한 보안 요구사항 및 기술과 관리 등의 지식 • 영향평가 수행에 필요한 검정 내용 • 감리지침 및 관련 기술, 조직관리론, 프로젝트 관리	• 구체적인 개인정보처리시스템과 이 시스템과 네트워크에 대한 위험성 • 개인정보 및 개인정보보호, 개인정보보호 법률에 대한 기본지식 • 구체적인 영향평가 방법 및 절차에 대한 지식

ISA는 시스템 기반의 감리 혹은 영향평가 업무를 수행하기 위한 기본적인 지식과 방법론을 포함한다. ISA의 개별 평가와 감리의 방법론에 대한 이해, 즉 예비조사, 증거확보, 계획 수립, 인력확보, 증거확보, 결론도출, 보고서 작성, 시정조치, 품질평가와 관련한 일련의 평가 업무와 관련된 절차와 지식은 개인정보영향에 대한 평가를 수행하기 위한 절차적 방법론과

많은 부분이 일치한다. 하지만 구체적으로 영향평가를 수행하기 위한 세부적인 절차와 방법, 대상으로서의 개인정보에 대한 지식과 영향평가 기준 등을 포함하지 않는다.

CPIA와 ISA는 프로젝트 수행에 관련해서는 유사한 부분을 많이 보였지만, 대상에 관한 내용에서는 상당한 차이를 보임을 알 수 있었다. CPIA와 ISA는 표면유사성이 낮고 구조·절차적 유사성이 높다고 할 수 있다. ISA 보유자는 영향평가를 수행할 수 있는 잠재적인 능력은 갖추었다고 판단되나 실제 영향평가의 수행 목적과 대상으로서의 개인정보와 개인정보처리시스템, 개인정보 라이프사이클 등을 숙지하고 있는지는 보장할 수 없다. 이에 ISA가 영향평가 대체자격으로 인정받기 위해서는 추가적으로 개인정보 및 개인정보보호 개요, 개인정보보호 라이프사이클, 영향평가 절차 및 기준 등에 대한 지식과 대한 지식과 기능을 보강하여야 한다.

5.2 소결

다양한 기준을 통해 CPIA와 유사자격들을 비교·분석해본 결과, 유사자격이 온전히 영향평가 전문자격으로 대체되기에는 부족한 부분이 존재함을 도출하였다. CPPG는 대상과 대상의 속성에 대한 유사성이 존재하므로 표면유사성이 높은 반면, ISA는 해결법칙이나 절차적 과정이 유사하므로 구조·절차적 유사성이 높다고 할 수 있다. 반면 다른 면에 대해서는 부족한 부분들이 존재하기 때문에 전반적 유사성은 갖추고 있다고 보기 어렵고, 각 자격 자체만으로는 영향평가를 수행하기 위한 지식과 기능, 업무수행 능력을 갖추고 있다고 볼 수 없다. 하지만, 두 자격 모두 일정 부분에 대해서는 영향평가 수행에 필요한 지식과 기능을 갖추고 있으므로 부족한 부분만 보완된다면 충분히 영향평가 대체자격으로 활용될 수 있는 가능성이 있다.

따라서 유사자격들은 각각 부족한 부분들을 보완할 수 있는 내용을 추가하여 표면유사성과 구조·절차적 유사성을 보강함으로써 영향평가 전문자격의 대체자격으로 개선할 수 있는 방안을 모색하여야 한다. 다음 장에서는 구체적으로 영향평가 전문인력 자격기준의 개선방안을 제시한다.

VI. 개인정보영향평가 자격기준 개선방안

본 장에서는 수요에 대응하는 한편, 기존 유사자격을 활용하면서 영향평가의 품질과 전문성 향상과 저비용 방안을 마련하기 위한 세 가지 개선 방안을 제안한다.

6.1 대안 1: 개인정보영향평가 전문자격 수립

비교대상 유사자격 중에서 영향평가 자격체계와 전반적인 유사성을 갖는 자격은 존재하지 않았다. 따라서 가장 확실한 대안은 표면적인 부분과 구조·절차적인 부분, 영향평가 수행을 위해 필요한 모든 지식과 기능을 포괄하는 개인정보 영향평가만을 위한 새로운 자격을 개발하는 것이다. 이 경우, 개인정보 영향평가만을 위해 특화된 전문인력을 확보할 수 있고, 보장된 영향평가 결과물을 얻을 수 있다는 장점이 있다. 이미 기존연구[9]에서 영향평가 전문인력이 갖추어야 할 자격요건을 포함한 영향평가 자격체계를 개발하였으므로, 이를 활용하거나 발전시키는 방안도 고려할 수 있다.

하지만 문제는 영향평가 전문자격만을 전문자격으로 인정할 경우, 영향평가 초기 수요를 감당할 수 있는 전문가들을 확보하기가 어렵다는 점이다. 물론 전문성이 부족한 인력들이 영향평가를 수행하는 것은 잘못된 영향평가 결과물을 얻게 되어 중장기적으로 더 큰 손해를 낳게 되지만, 초기에는 진입장벽을 낮춰 어느 정도의 수요를 확보한 후 수행인력들에 대한 교육이나 또 다른 방법을 통해 확보한 수행인력의 능력을 향상시키는 방법도 고려하여야 한다. 또한 초기의 수요를 맞추기 위해 영향평가 전문자격의 합격률을 적정 수준보다 높게 잡거나, 시험문제의 수준을 낮추는 것은 장기적으로 봤을 때 옳은 방법이 아니다.

따라서 이미 유사자격을 취득한 사람들에게 부족한 부분들을 보완하게 함으로써 필요인력의 공급 및 수준을 보충해야 한다. 이에 영향평가 전문자격 개발 및 운영과 동시에 기존의 유사자격을 활용할 수 있는 방안을 마련할 필요가 있다. 이를 위해 다음 대안에서 기존 유사자격 소지자들을 적은 비용과 낮은 진입장벽으로 영향평가 수행인력으로 양성·활용하는 한편, 영향평가 수행품질도 유지하기 위한 방안을 제시한다.

6.2 대안 2: 유사자격에 관련 모듈 의무교육 혹은 시험트랙 추가 운영

비교대상 유사자격 중 영향평가 자격체계와 전반적

9) 한국정보화진흥원의 "개인정보 영향평가 자격제도 수립방안 연구"

인 유사성을 갖고 있지 않으나 표면적 유사성 또는 구조·절차적 유사성만으로 유사자격으로 인정받고 있는 자격이 존재함을 알 수 있었다. 영향평가 대체자격으로 인정하기 위해서는 자격 차원에서 부족하다고 판단되는 유사성 부분에 대한 시험트랙을 추가적으로 응시하게 하거나, 관련 모듈에 대한 교육과정을 이수하도록 하는 등의 추가 절차가 필요하다.

추가 시험트랙의 경우, 해당 자격을 운영하는 기관의 도움을 받아 이미 자격을 취득한 사람이 개인정보 영향평가 전문인력의 자격요건으로 해당자격을 사용할 경우 추가 시험트랙을 응시하도록 하여야 한다. 이미 세분화된 자격 트랙들을 운영하고 있는 미국 프라이버시전문가(이하 CIPP)[10]의 경우를 참고하여 유사한 방식으로 영향평가 트랙을 만들어 사용할 수 있다. 하지만 해외 자격의 경우 국내에서 별도의 트랙을 만들어 시행하기가 현실적으로 어렵기 때문에 불가피하게 부족한 부분에 대한 추가 교육과정을 이수하게 하면 될 것이다. 교육과정의 경우 현재 한국정보화진흥원에서 공무원과 민간전문가를 대상으로 매년 총 4회씩 운영하고 있는 영향평가 교육과정을 유사자격 소유자들에게 확대 실시하여 영향평가 전문인력 자격을 부여받기 위해서는 이를 필수적으로 추가 이수해야 하는 방향을 고려하여 볼 수 있다.

이와 같은 대안은 각 유사자격들의 부족한 부분에 대한 전체 교육과정의 재이수나 재 검정에 따른 비용과 시간에 따른 개인적, 사회적 낭비를 최소화할 수 있는 방안이 될 것으로 기대된다. 하지만 유사자격을 운영하는 기관이 새롭게 시험트랙을 만들어야 한다는 부담을 가질 수 있고, 운영기관들의 협조 없이는 불가능한 방안이라는 한계가 존재한다.

6.3 대안 3 : 개인정보영향평가 전문자격의 모듈화 운영

마지막 대안은 영향평가 전문자격을 운영하는 기관에서 유사자격 보유자를 위한 별도의 시험 모듈을 제공하는 것이다. 영향평가 전문자격 도메인 자체를 모듈화 하여 유사자격이 없는 경우와 유사자격이 있는 경우를 구분하여 다른 모듈을 검정하도록 한다. 예를 들어 유사자격이 없는 경우에는 모든 모듈을 검정하여야 할 것이고, 유사자격이 있는 경우는 각 자격별로 부족하다고 판단되어지는 영역의 모듈만을 검정하면 된다. 구체적으로 ISA 소지자들의 경우 개인정보관리 및 보호 모듈을 검정해야 할 것이고, CPPG 소지자들의 경우 영향평가 절차 및 방법과 프로젝트 관리 모듈 등을 검정하면 될 것이다.

이러한 자격의 모듈화 운영은 최근 자격 운영 방안 중 하나로 논의되고 있다. 특히 IT기술의 급속한 발전으로 인해 대부분의 직종에서 IT활용이 일반화됨에 따라 기초사무 IT분야 국가기술자격은 최근 타 유사자격과의 경쟁에서 우위를 차지할 수 있는 새로운 대안으로 모듈식 자격에 관심을 가지고 있다. 이에 기초사무 IT분야 국가기술자격을 '기초사무 IT능력별 모듈 자격화', '기초사무 IT능력 간 연계성을 고려한 모듈 자격화', '단일 종목 내 능력별 시험과목 모듈화', '능력별 모듈 자격화와 종합자격 신설' 등과 같은 4가지 방법의 모듈화 방식을 제안하고 있다[21][22]. 개인정보 영향평가 전문자격을 모듈화 할 때에도 위와 같은 방법의 모듈화 방법을 참고 할 수 있다

위의 방안은 ISA나 CPPG를 운영하는 기관의 별도의 도움 없이 영향평가 전문자격을 운영하는 기관의 모듈화를 통해 달성할 수 있다는 점에서 좀 더 편리하고 현실적인 대안이 될 것으로 판단된다. 또 변화에 따라 자격 종목을 쉽게 변경·신설·폐지할 수 있고, 특정 능력에 대한 불필요한 중복 검정이 이뤄지는 것을 막을 수 있다는 장점이 존재한다. 하지만 하나의 자격에서 시험과목을 선택하고, 해당 과목의 과락에 따라 자격을 부여하기 때문에 자격증에 해당 과목의 합격여부를 별도로 표기해야 한다는 제한이 있다.

VII. 결론 및 기대효과

본 논문에서는 "개인정보 영향평가 자격제도 수립 방안 연구"에서 도출한 영향평가 자격체계와 관련법에서 제시하고 있는 유사자격인 CPPG와 ISA를 비교함으로써 유사자격이 영향평가 전문인력이 갖추어야 할 자격조건들을 얼마나 만족시키고 있는지 확인하였다. 그 결과 CPPG는 개인정보에 관련된 일반적인 지식이나 영향평가 수행에 필요한 기본지식은 포함하고 있지만 실질적으로 영향평가를 수행할 때 필요한 지식은 요구하지 않고, ISA는 영향평가 업무를 수행하기 위한 기본적인 지식은 보유한 반면, 개인정보 및 영향

10) CIPP는 각 국가 법제의 특수성을 반영하여 미국(US), 캐나다(C), 유럽(E)등으로 구분되어 있고, 정부와 공공영역(G)에 특수화되거나, 정보시스템전문가(IT)들을 위해 별도로 구분되어 있다. 미국은 법률적·정책적 내용들을 중심으로 하는 CIPP/US와 기술적인 부분에 초점을 맞추고 있는 CIPP/IT를 별도로 운영함

평가에 관한 기본지식 부분이 부족함을 알 수 있었다. 비교 결과 명확하게 부족한 부분이 도출되었으므로 유사자격들을 그대로 영향평가 대체자격으로 사용하기에는 무리가 있다고 판단되었다. 이에 본 논문에서는 새로운 영향평가 전문자격 개발, 유사자격에 시험트랙 및 의무교육 추가 운영, 영향평가 전문자격의 모듈화 운영 등의 세 가지 개선방안을 제시하였다.

또한, 영향평가 유사자격 중 표면적 유사도가 높다고 판단되는 CPPG와 구조·절차적 유사도가 높다고 판단되는 ISA에 대해서만 비교해보았다. 하지만, 향후에는 그 외의 유사자격인 CISA, CISSP, SIS 등에 대해서도 같은 기준을 적용하여 비교함으로써 각 자격의 부족한 부분을 도출하여야 한다. 하지만 예상하건데, 본 논문에서 비교했던 두 자격이 다른 유사자격보다 유사성이 높다고 판단되므로 그 외의 유사자격에 대한 비교에서도 영향평가 수행에 필요한 지식 및 스킬 중 공백이 상당부분 존재할 것으로 예상된다. 따라서 이 자격들에 대해서도 부족한 부분이 도출되면 이를 보완할 수 있는 인증모듈이나 교육프로그램의 개발이 필요할 것이다.

제시한 개인정보 영향평가 전문인력 자격기준의 개선방안을 이용하여 얻을 수 있는 기대효과는 다음과 같다. 첫째, 개인정보 영향평가 전문자격 수립 시, 기존의 유사자격 등의 기준보다 좀 더 명확하게 영향평가 수행을 위해 필요한 자격을 갖춘 전문인력을 검증할 수 있다. 둘째, 유사자격에 관련 모듈 의무교육 혹은 시험트랙 추가 운영 시에는 전체 교육과정의 재이수나 재 검정에 따른 비용과 시간에 따른 개인적, 사회적 낭비를 최소화할 수 있을 것으로 기대된다. 마지막으로 개인정보 영향평가 전문자격의 모듈화 운영의 대안의 경우 ISA나 CPPG 운영기관의 별도의 도움 없이 영향평가 전문자격 운영기관의 모듈화를 통해 달성할 수 있다는 점에서 좀 더 편리하고 현실적인 대안이 될 것이다. 위의 세 가지 대안을 통한 기대효과를 종합해 보았을 때, 사회적으로나 개인적으로 적은 비용으로 영향평가 시행 초기의 수요를 충족시키는 한편, 영향평가의 수행 품질 또한 유지할 수 있을 것으로 기대된다.

참고문헌

〔1〕 이유지, "개인정보 영향평가기관 더 늘어난다," 디지털데일리, 2012년 1월 13일.

〔2〕 한국정보화진흥원, "개인정보 영향평가 자격제도 수립방안 연구," 2012년 9월.

〔3〕 행정안전부, "개인정보 영향평가 수행 안내서," 2011년 12월.

〔4〕 장호익, "개인정보 영향평가에 관한 법제연구," 박사학위논문, 숭실대학교, 2011년 1월.

〔5〕 M.L. Gick, and K.J. Holyoak, "Schema induction and analogical transfer," Cognitive Psychology vol. 15, no. 1, pp.1-38, Jan, 1983.

〔6〕 D. Gentner, "The mechanisms of analogical learning," Dept. of Computer Science, University of Illinois at Urbana-Champaign (Urbana, Ill.), Oct. 1987.

〔7〕 Z. Chen, "Analogical problem solving: A hierarchical analysis of procedural similarity," Journal of Experimental Psychology: Learning, Memory, and Cognition, vol. 28, no. 1, pp.81-98, Jan. 2002.

〔8〕 D. Gentner, and B. Markman, "Structure mapping in analogy and similarity," American Psychologist, Vol. 52, no. 1, pp.45-56, Jan. 1997.

〔9〕 한국직업능력개발원, "민간자격 국가공인 신청 편람," 2012년도 공인신청자용.

〔10〕 개인정보관리사(CPPG) 공식 웹사이트, http://www.cpptest.or.kr (검색일시: 2012년 10월 15일)

〔11〕 한국인터넷진흥원, "개인정보보호관리체계 인증 준비 안내서(사업자용)," 2010년 12월.

〔12〕 한국직업능력개발원, "정보시스템감리사 직무분석," 2000년 12월.

〔13〕 한국정보화진흥원, "정보화사업 감리 수행 가이드," 2011년 7월.

〈著者紹介〉

김 이 랑 (Erang Kim) 학생회원
2010년 8월: 경희대학교 전자공학과 졸업
2011년 2월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 개인정보영향평가, 개인정보보호, 금융보안, 정보보호정책, 정보보호컨설팅 등

심 미 나 (Mina Shim) 종신회원
1996년 2월: 성신여자대학교 전산학과 졸업
2006년 2월: 고려대학교 정보보호대학원 공학석사
2010년 2월: 고려대학교 정보보호대학원 공학박사
2008년 3월~현재: 고려대학교 정보보호대학원, 세종사이버대/대학원,
서울디지털대 정보보호/개인정보보호정책 강의
2010년 9월~현재: 고려대학교 정보보호대학원 연구교수
〈관심분야〉 정보보호정책, 프라이버시, 개인정보보호, 개인정보영향평가, 위험분석, 정보법학 등

임 종 인 (Jong In Lim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
現 고려대학교 정보보호대학원 원장, 고려대학교 사이버국방학과 교수, 개인정보보호위원회 위원, 대검찰청 디지털수사자문위원회 위원장, 금융보안 연구원 보안전문기술위원회 위원장, 행정안전부 정책자문위원회 위원, 국방부 정보화책임관 자문위원, 한국저작권위원회 위원 등
〈관심분야〉 사이버국방, 정보법학, 디지털포렌식, 개인정보보호, 융합기술보안 등