Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.3, Jun. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.3.745

구문분석을 통한 PIMS와 PIPL의 중복성 평가*

김 소 라,[1†] 김 태 성[2‡]
[1](주)싸이버원, [2]충북대학교

Redundancy assessment of PIMS and PIPL by parsing*

So-Ra Kim,[1†] Tae-Sung Kim[2‡]
[1]Cyberone.Co.Ltd, [2]Chungbuk National University

요 약

개인정보 침해사고가 잇따르고 그 피해규모가 심각함에 따라 정부에서는 개인정보의 보호를 위하여 다수의 개인정보보호 관련 인증제도를 도입하였다. 그중에서도 PIMS와 PIPL은 서로 유사한 점이 많아 중복규제라는 문제점이 제기되어 왔다. 본 연구에서는 그동안 논란이 되어 온 PIMS와 PIPL 간의 중복성을 규명하기 위하여 두 인증제도 심사기준의 중복성을 구문분석을 통해 평가한다.

ABSTRACT

As infringement accidents of personal information have often occurred and estimates of damages are too large, the government introduces many certifications related with personal information management system for protecting personal information. Among them, PIMS and PIPL share many points in common, so many complaints about duplicate regulation have been suggested. This study evaluates the duplication of two certifications in order to examine redundancy between PIMS and PIPL both of which have been controversial.

Keywords: IMS, PIPL, redundancy assessment, parsing

I. 서 론

정보사회의 고도화와 개인정보의 경제적 가치 증대로 사회 모든 영역에 걸쳐 개인정보의 수집과 이용이 보편화되고 있으나, 이에 따른 개인정보 침해 사례가 지속적으로 발생하여 국민들의 프라이버시 침해와 정신적·금전적 피해를 초래함에 따라 2011년 「개인정보보호법」이 제정되었다.

그러나 「개인정보보호법」이 시행된 이후에도 2012년 통신회사 개인정보 유출 사고, 2013년 6.25 사이버 공격, 2014년 카드 3사 개인정보 유출 사고 등 개인정보 유출 사고는 꾸준하게 발생하고 있으며, 이러한 대규모 개인정보 유출사고는 기관 및 기업의 이미지 손상, 자산손실 뿐 아니라 집단소송 등으로 이어져 조직의 생존에 중대한 위협요인으로 작용하고 있다[1]. 이에 정부에서는 개인정보보호와 관련된 다수의 인증제도를 양산하게 되었다.

그중에서도 특히 개인정보보호 관리체계 인증제도는 기관 및 기업의 자율적인 개인정보보호 활동에 대해 객관적이고 공신력 있는 검증을 통해 개인정보보호에 대한 적합성을 증빙할 수 있도록 한다. 이러한 국내 개인정보보호 관리체계 인증제도로는 2011년부터 시행된 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 정보통신망법)」 상의 개인정보보호 관리체계 인증(Personal Information Management System, 이하 PIMS)이 있으며, 2013년에

Received(01. 28. 2016), Modified(05. 11. 2016), Accepted(05. 18. 2016)
* 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단 기초연구사업의 지원을 받아 수행된 연구임(NRF-2011-0025512).
† 주저자, kimsr_@naver.com
‡ 교신저자, kimts@cbnu.ac.kr(Corresponding author)

는 「개인정보보호법」 상의 개인정보보호 인증(Personal Information Protection Level, 이하 PIPL)이 도입되었다.

그러나 PIPL은 도입 초기부터 기존에 시행되고 있던 PIMS와의 중복에 대한 우려가 제기되었다. PIMS와 PIPL은 모두 조직이 개인정보보호 관리체계를 잘 수립하여 운영하고 있는지에 대해 평가하여 인증을 부여하는 인증제도로서, 그 목적과 방법이 매우 유사한 제도라고 할 수 있다. 유사제도의 중복은 인증을 받으려는 기관 및 기업에 혼란을 야기하고 여러 인증을 취득해야 하는 기관 및 기업은 비용 등의 부담이 커질 수밖에 없다. 또한 기관 및 기업의 인증 획득 의지를 약화시켜 인증제도의 실효성마저 약화될 수 있다.

이러한 유사 및 중복되는 인증제도로 인한 부작용 때문에 정보보호 관련 유사 인증제도 간의 상호인정 및 통합에 대하여도 활발하게 논의가 이루어져왔으며, 개인정보보호 관리체계 인증제도인 PIMS와 PIPL을 우선 통합하기로 관계부처 간 합의가 이루어지기에 이르렀다[2].

그러나 PIMS와 PIPL 두 인증제도가 어떻게 얼마만큼 중복이 되는지 실증적이고 구체적으로 그 중복성을 평가한 연구는 찾아보기 힘들다. 따라서 본 연구에서는 PIMS와 PIPL 두 인증제도간의 중복성을 평가하고 두 인증제도간의 중복성을 규명하고자 한다.

II. 이론적 배경 및 선행연구

2.1 개인정보보호 관련 인증제도

2.1.1 개인정보보호 관리체계 인증(PIMS)

PIMS는 기업이 개인정보보호 활동을 체계적·지속적으로 수행하기 위해 필요한 보호조치 체계를 구축하였는지 점검하여 일정 수준 이상의 기업에 인증을 부여하는 제도이다[3]. PIMS는 방송통신위원회 심의·의결 '개인정보보호 관리체계 인증제 도입에 관한 건' 제2010-66-273호에 근거하여 2011년부터 인증을 실시해 왔다. 이후 2012년 2월 17일 개정된 「정보통신망법」 제47조의3에 의해 법적 근거가 마련되었으며, 방송통신위원회 고시 제2013-17호 '개인정보보호 관리체계 인증 등에 관한 고시'에 의해 운영되고 있다.

Table 1. Screening criteria of PIMS

Control area	Control content	Number of control objecti-ves	Number of control items
Management process	Establishing policy and scope	1	3
	Management's responsibility and organization	1	2
	Risk management	1	3
	Implementation	1	2
	Maintenance	1	3
	Subtotal	5	13
Protection measures	Personal information policy	3	6
	Personal information protection organization	2	6
	Personal information asset classification	2	2
	Education for personal information protection	2	4
	Personnel security	1	4
	Managing incidents	3	7
	Technical protection measures	8	42
	Physical protection measures	3	8
	Subtotal	24	79
Life cycle	Collection of personal information	3	10
	Use and provision of personal information	5	16
	Management and destruction of personal information	1	6
	Subtotal	9	32
Total		38	124

「정보통신망법」 제47조의3 제1항에서 '방송통신위원회는 정보통신망에서 개인정보보호 활동을 체계적이고 지속적으로 수행하기 위하여 필요한 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하고 있는 자에 대하여 제2항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다.'고 정하고 있어 정보통신망에서 개인정보보호 관리체계를 수립하여 운영하고 있는 기업은 자율적으로 심사를 신청

하여 인증을 받을 수 있다.

PIMS 인증을 받기 위해서는 다음의 세 가지 요구사항을 만족시켜야 한다. 첫째, 5단계 개인정보보호 관리과정에 따라 개인정보보호 관리체계를 수립하고 운영해야 한다. 둘째, 개인정보보호 유관 법적 요구사항 및 전사적으로 다양한 관리적·기술적 요구사항을 만족할 수 있는 보호대책을 수립하고 운영하여야 한다. 셋째, 개인정보의 생명주기와 관련된 법적 요구사항을 만족할 수 있도록 생명주기준거 요구사항을 만족하여야 한다.

PIMS의 심사 기준은 KISA-ISMS, ISO/IEC 27001, BS10012 등 국내외의 표준과 「정보통신망법」에 명시된 개인정보보호조치를 고려하여 국내 환경에 적합하도록 보완하여 개발되었다. 인증심사 기준은 개인정보 관리과정, 보호대책, 생명주기 3개 분야의 124개 통제항목, 310개의 세부점검 사항으로 구성되어 있다.

PIMS는 인증제도의 객관성 및 신뢰성 확보를 위해 인정기관, 인증위원회, 인증기관을 분리하여 운영하고 있다. 인정기관은 인증제도를 관리·감독하는 기관으로, 방송통신위원회가 수행하며, 산업계, 학계, 정부의 전문가로 구성된 인증위원회가 인증결과를 심의한다. 인증기관은 한국인터넷진흥원으로 지정하여 심사의 객관성을 확보한다.

PIMS는 크게 4단계로 진행된다. 첫째, 인증신청 및 계약을 준비하는 준비단계, 심사팀이 문서심사 및 기술심사를 한 후 그 결과 발견된 결함사항을 신청기관(기업)이 보완조치하는 심사단계, 인증위원회가 인증심사결과를 심의하여 인증서를 교부하는 인증단계, 인증취득 후의 사후관리단계로 구분된다.

2.1.2 개인정보보호 인증(PIPL)

PIPL은 개인정보처리자의 개인정보보호 관리체계 구축 및 개인정보보호조치 사항을 이행하고 일정한 보호수준을 갖춘 경우 인증마크를 부여하는 제도이다. PIPL은 「개인정보보호법」 제13조에 근거하고 있으며 2013년 10월 28일 제정된 안전행정부고시 「개인정보보호 인증제 운영에 관한 규정」이 제정되어 2013년부터 시행되고 있다.

개인정보보호 인증과정을 통해 개인정보보호 관련 법령에서 요구하는 기준을 기관 내부에서 준수하는지 여부를 점검하고, 조직내부 구성원에게 개인정보보호에 대한 중요성을 전파하고, 인식 및 역량을 제고할 수 있다. 지속적이고 체계적인 개인정보보호 활동을 수행함에 따라 개인정보취급자의 부주의, 안전성 확보조치 미흡 등으로 발생할 수 있는 개인정보 침해 가능성을 최소화할 수 있다[3].

Table 2. Screening criteria of PIPL

Screening area	Screening content	Number of screening items	Number of screening items by types		
			Public/Large	Medium	Small
Protection management system	Establishing protection management system	5	5	3	-
	Execution and operation	6	6	3	-
	Review and monitoring	2	2	-	-
	Correction and improvement	2	2	2	-
	Total	15	15	8	-
Protection measures	Handling personal information	14	14	13	12
	Guarantee of right of information subject	3	3	3	3
	Managerial measures for ensuring safety	10	10	10	8
	Technical measures for ensuring safety	16	16	13	7
	Physical measures for ensuring safety	7	7	5	3
	Sub total	50	50	44	33
Total		65	65	52	33

PIPL은 「개인정보보호법」의 적용을 받는 모든 개인정보처리자(공공기관, 민간기업, 법인, 단체 및 개인)가 신청할 수 있다. 인증을 취득하고자 하는 개인정보처리자는 공공기관, 대기업, 중소기업, 소상공인 중 해당되는 유형으로 인증심사를 신청한다.

인증심사 기준은 크게 개인정보보호 관리체계 분야와 개인정보보호대책 분야로 구성되어 있다. 개인

정보보호 관리체계 분야는 PDCA(Plan - Do - Check - Act)의 관점에서 보호 관리체계의 수립(Plan), 실행 및 운영(Do), 검토 및 모니터링(Check) 그리고 교정 및 개선(Act)으로 심사영역이 구성되어 있다. 개인정보보호대책 분야는 관리적·기술적·물리적 안전성 확보조치 등과 같은 보호조치뿐만 아니라 법적으로 요구되는 개인정보의 처리, 정보주체 권리보장 등에 대한 항목을 포함하여 심사영역이 구성되어 있다.

인증심사기준은 최대 65개 심사항목을 신청기관 유형별(공공기관, 대기업, 중소기업, 소상공인)로 차등 적용한다. 신청기관 유형별로 심사항목 자체에 차이가 있는 것은 아니며, 심사항목의 적용 유무로 구분되어 있다.

PIPL의 인증 절차는 인증심사 준비단계, 심사단계, 인증단계로 구성되며, 인증유지관리를 위한 유지관리단계가 있다. 준비단계는 인증심사를 위해 사전에 준비를 하는 단계로, 신청기관은 인증심사 준비를 완료하여 인증기관에 인증신청을 하고, 인증기관은 신청기관의 인증준비 상태를 사전에 점검하여 인증심사 준비여부를 확인한 후에 계약을 체결한다. 인증심사 단계에는 인증심사팀 구성 및 심사계획 통보, 인증심사 수행, 보완조치 요청 등이 포함된다. 마지막으로 유지관리 단계에서는 인증취득기관은 인증서를 취득한 이후 연간 1회 이상 정기적으로 유지관리심사를 받아야 하고 인증 유효기간 만료 90일 전까지 인증기관에 인증의 갱신을 신청해야 한다.

2.2 중복규제의 문제점

2.2.1 중복의 개념 및 문제점

중복(重複)은 사전적으로 '거듭하거나 겹침'의 의미를 지닌다[4]. 영어로는 overlap(겹침), duplication(이중), repetition(반복), redundancy(중복) 등으로 표기될 수 있다. 중복성은 사전적으로 정의되지 않았으나 '유사'의 사전적 의미는 '서로 비슷함'이며, '유사성'은 '서로 비슷한 성질'이라고 정의되는 것으로 보아 중복성이란 거듭하거나 겹치는 성질이라고 이해할 수 있을 것이다.

관리적 시각에서의 중복은 효율성을 저해한다는 부정적인 시각과 가외성을 통해 위험을 해소하는 긍정적인 시각의 두 가지 측면에서 논의되어 왔다[5]. 중복규제란 하나의 피규제자 또는 하나의 행위에 대하여 다수의 규제권자가 존재하는 현상을 말한다. 즉, 하나의 기관과 한 가지 사안에 대하여 여러 부처가 규제하는 것을 의미한다[6].

중복규제는 부처별로 관할권이 중복되어 유사한 업무를 여러 부처가 담당하기 때문에 발생한다. 즉, 정부기능의 중복이 규제의 중복을 가져오는 가장 큰 이유가 된다. 유사한 업무를 여러 부처가 담당하게 되는 이유는 기술의 융합, 경제의 복잡화와 상호 긴밀한 관련성 등으로 관할이 모호해지는 데 따른 불가피한 측면도 있지만, 규제권한이 커지면 커질수록 부처의 예산과 위상이 커지는 속성으로 인해 경쟁적으로 규제의 관할영역을 넓히려는 부처 간 경쟁에 주로 기인한다. 여기에 정부, 지자체의 규제와 관할권의 근거인 법률, 조례의 정의나 서술방식이 추상적이고 정밀하지 않은 점도 중복의 문제를 초래하는 또 하나의 원인이라 할 수 있다[7].

중복규제는 다음과 같은 문제점을 가져온다.

첫째, 사업자등에게 규제비용을 이중으로 부담하게 하여 기업의 경영활동에 지장을 초래한다. 동일한 사안에 대해 복수의 규제기관이 중복적으로 규제를 함으로써 사업자등은 막대한 자원이 낭비되고 사업활동이 위축된다[7]. 둘째, 유사한 업무를 여러 부처와 기관에서 담당함으로써 정부시책이 분산되고 부처 간 갈등 및 경쟁으로 인한 낭비와 비효율이 증가하게 된다[6]. 셋째, 중복규제에 따른 정부 정책의 일관성 결여는 피규제자들의 규제순응도와 준법의식을 약화시킨다. 규제와 관련하여 이해관계를 가진 자들이 어떤 내용의 법률과 규제가 누구에 의해 어떤 방식으로 집행, 운영되는지를 명확히 알 수 없게 만들어 이해당사자들의 혼란을 가중시키며, 이는 피규제자들로 하여금 규제에 따라야 한다는 의무감과 준법의식을 약화시키는 원인이 되는 것이다[7].

2.2.2 (개인)정보보호 관련 중복규제의 문제점

이와 같은 문제는 개인정보보호 관련 인증제도에서도 나타난다. 개인정보보호 관리체계 인증제도인 PIMS, PIPL은 기업의 개인정보보호 수준을 측정한다는 공통점이 있다. 그러나 두 인증제도의 운영주체는 서로 다르다. PIMS의 인정기관은 방송통신위원회이며, 인증기관은 한국인터넷진흥원이고, PIPL의 인정기관은 행정자치부이며, 인증기관은 한국정보화진흥원으로 지정되어 있다. 이처럼 개인정보보호 관리체계와 관련한 유사한 두 인증제도에 대하여 각

기 다른 담당 부처가 관련 업무를 수행하고 있다.

또한 (개인)정보보호 관련 인증제도는 ISMS, PIMS, PIPL, e-Privacy, PIA 등이 있으며 (개인)정보보호라는 동일한 목적에 대하여 중복되는 규제가 너무 많아 여러 인증의 대상이 되는 기관 및 기업의 규제준수 의지를 약화시키는 결과가 나타난다[8]. 또한 두 인증제도의 통제항목이 큰 차이가 없다는 문제도 제기되어 왔다.

이러한 상황에서 국내 기업들은 법정의무인증인 ISMS 인증 획득에만 집중하게 되고 최근 1년여간(2014년 1월~2015년 9월) 발급된 인증서 수는 ISMS는 202건에 달하나, PIMS는 15건, PIPL은 13건에 그치고 있어 개인정보보호 관리체계 인증제도는 ISMS에 비해 활성화되지 못하고 있는 상황이다.

2.3 관련 선행연구

PIMS와 PIPL에 관한 국내 연구는 타 정보보호 관련 인증제도와의 비교 및 개선방향을 제시한 연구[9-11], 효과적인 개인정보 관리체계의 도입 방안에 대한 연구[12], 개인정보보호 관리체계의 구축 사례 연구[13]가 있다. 또한 개인정보보호 환경의 다변화 및 신기술의 등장으로 인한 PIMS의 변화에 관한 연구[14]와 특정 분야에 적합하도록 특화시킨 개인정보보호 관리체계 인증제도 개발에 관한 연구들[15-18]이 있다.

해외에서는 BS 7799, ISO/IEC 17799 등 정보보안표준을 비교한 연구들[19, 20]이 주를 이루고 있으며 이 연구들은 정보보안표준들은 한 두 단락으로 이루어진 항목만을 제시하고 있기 때문에 세부통제항목에 대한 설명이 필요함을 역설하고 있다.

국내외 정보보호 및 개인정보보호 관련 인증제도에 관한 연구들은 기존에 있던 인증제도들을 서로 비교하거나 인증제도의 지표 개발에 관한 연구가 많았으며, PIMS와 PIPL에 대하여 내용적 측면인 심사기준에 대하여 중복의 정도를 평가한 연구는 부재한 상황이다.

유사제도간의 중복성에 관한 연구는 여러 분야에서 이루어져 왔다. 김운수 외[21]는 서울시 도시관리계획 환경성검토 제도에 대해 유사 제도와의 비교검토를 수행하고 서울시 환경성검토 제도의 운영 실태를 분석하여 제도의 실효성을 향상시킬 수 있는 방안을 제안하면서 법적근거, 운영주체, 평가목적 및 대상, 평가항목, 평가방법 및 내용을 비교하였다. 김정해[6]는 산업안전분야의 중복규제 문제의 실태를 분야별 규제법령과 담당기관의 중복현황과 중복규제 유형화에 따른 영역별 현황을 조사하여 부처간에 중복되어 있는 규제의 실태를 밝히고 일원화할 수 있는 방안을 제시하였다. 한국소프트웨어진흥원[22]의 연구 보고서에서는 디지털콘텐츠 거래인증제도와의 유사제도를 비교하여 유사제도 간의 연계방안으로 식별표지를 통일하고, 인증항목을 통합하는 방법을 제시하였다. 개인정보보호 관련 인증제도의 중복성에 관한 연구를 수행한 심미나[9]는 PIMS와 기존 정보보호 인증제도간의 중복성을 제도적 관점과 방법론적 관점으로 접근하여 인증제도간의 중복성을 평가하고 심사항목의 모듈화 방안을 제안하였다.

III. PIMS와 PIPL 간의 중복성 평가 방법론

개인정보보호 관리체계 인증제도인 PIMS와 PIPL간의 중복성을 판단함에 있어 내용적인 측면의 중복성 평가는 매우 중요하다. 만약 개인정보보호를 위한 제도화의 논리가 다르더라도 실제 인증심사에 있어서 '내용'이 되는 심사기준이 중복된다면 별개의 제도라 할지라도 실질적으로는 내용상 중복된다고 할 수 있다.

PIMS는 「정보통신망법」에 근거하고 있으며, PIPL은 「개인정보보호법」에 근거하고 있어 제도화의 논리는 다르다고 할 수 있다. 그런데 두 인증의 적용대상을 보면, PIMS는 정보통신망에서 개인정보보호 관리체계를 수립하여 운영하고 있는 기업을 대상으로 하고 있고, PIPL은 「개인정보보호법」의 적용을 받는 모든 개인정보처리자가 신청할 수 있다. 「개인정보보호법」은 개인정보보호에 관하여 일반법의 지위를 가지며, 개인정보를 처리하는 공공기관, 법인, 단체 및 개인에 대하여 적용된다. 따라서 PIMS와 PIPL의 적용을 모두 받는 기업이 발생하게 된다.

별개의 인증제도라는 이유로 동일한 대상에 대하여 유사한 심사기준에 의한 인증심사를 거듭하는 것은 인증제도의 효율성 및 제도의 활성화를 저해하는 요인이 될 수 있다. 따라서 본 연구에서는 PIMS와 PIPL의 심사기준에 대하여 중복성 평가를 실시한다.

3.1 중복성 평가 요소

중복여부는 PIMS의 통제항목과 PIPL의 심사항목 각각에 대한 상세내용을 비교하여 평가하게 된다.

하나의 통제항목(심사항목)이 갖는 목표는 항목의 개발자 혹은 평가자에 따라 얼마든지 세분화할 수 있어 목표수준에 대한 이해가 다를 수 있다. 당연히 목표에 대한 이해도가 다를 경우 중복여부의 평가가 달라질 수밖에 없다[9].

이러한 주관적 요인을 제거하기 위해서는 하나의 통제항목(심사항목) 상세내용을 특정 규칙으로 일관되게 표현해야 한다. 이때 특정 규칙은 각 통제항목(심사항목) 상세내용을 이루는 요소들로 구성한다. 통제항목(심사항목)의 상세내용은 인증을 신청한 기관이 개인정보보호를 위한 활동 즉, 행위를 어떤 대상에 대하여 수행해야 하는지를 정의한 것이다. 따라서 두 인증제도의 중복성 평가는 결국 통제항목(심사항목) 상세내용의 이행행위와 이행대상이 서로 얼마나 중복되는지를 판단하는 것이다.

본 연구에서는 중복성 평가를 위해 구문분석을 실시한다. 구문분석은 통사적인 성격을 가지는 품사 범주나 형태 범주가 이루는 통사적 구조와 유형을 체계화하여 실제 문장의 구조를 분석해 내는 과정으로 정의될 수 있다[23]. 즉, 구문분석은 문장을 분석하여 객관화함으로써 문장의 각 요소를 비교분석할 수 있는 방법을 제공해준다. 구문분석을 통해 통제항목(심사항목)의 상세내용을 구성하는 요소를 이행대상과 이행행위로 나누고 각각에 대하여 중복성 평가를 한 후, 두 요소의 평가를 종합하여 최종 평가를 하게 된다.

3.2 중복성 평가 기준

심사기준에 대한 중복성을 평가하기 위해서는 논리적인 중복성 평가 방법을 필요로 한다. 심사기준에 대해 중복성을 평가하는 평가기준의 중복여부가 심사기준의 중복을 판단하는 가장 중요한 부분이므로 객관적으로 두 인증제도의 통제항목(심사항목)과 각 항목의 상세설명에 대한 중복성을 판단할 수 있는 기준을 세우는 것이 필요하다.

심사기준의 통제항목(심사항목)은 정성적 평가를 통해 이루어질 수밖에 없으나, 중복성 평가를 위한 기준을 보다 세분화하여 명확하게 함으로써 계량적 접근을 시도한다. 계량적 평가를 가능하도록 하는 평가기준이 되는 중복 판단 기준은 중복성의 개념에 따라 완전하게 동일하거나 겹치는 정도의 '완전중복', 완전하게 상이하거나 일부 유사한 부분이 있으나 의미가 전혀 다른 정도의 '완전상이', 극히 일부이거나 거의 대부분이 유사한 정도의 '일부중복' 혹은 '일부상이' 등으로 구분할 수 있다[9]. 또한 소프트웨어 개발 요구사항에 대한 최진재와 황선영[24]의 연구에서 사용한 '완전중복, 포함중복, 부분중복, 비중복'으로도 중복관계를 표현할 수 있다.

본 연구에서는 통제항목(심사항목)의 상세내용을 구성하는 요소에 대하여 완전하게 일치하는 경우에는 '완전중복', 일부 유사 또는 겹치는 부분이 있거나 부분으로 포함되는 경우에는 '부분중복', 의미가 전혀 다르거나 겹치는 부분이 없는 경우에는 '비중복'으로 판단한다.

IV. PIMS와 PIPL 간의 중복성 평가

4.1 구조적 비교

본격적으로 PIMS와 PIPL 간의 중복성을 평가하기 전에 두 인증제도의 구조적 비교를 실시하였다. PIMS와 PIPL은 모두 PDCA 사이클을 토대로 구성되었다. PIMS는 개인정보 관리과정, 보호대책, 생명주기의 3개 영역으로 구성되어 있고 PIPL은 개인정보보호 관리체계와 보호대책의 2개 영역으로 구성되어 있어 그 체계를 달리하는 것처럼 보일 수 있으나, 두 인증제도는 구조적으로 표 3과 같이 대응된다.

표 3과 같이 PIPL의 심사영역이 PIMS의 여러 통제분야에 걸쳐 대응되는 특징을 보인다. 따라서 PIMS이 PIPL에 비해 더 세부적으로 통제분야를 나누어 구성하고 있음을 알 수 있다.

4.2 통제항목과 심사항목 간 비교

PIMS와 PIPL은 심사기준에 대한 구조 비교에서와 같이 상이한 구조를 갖고 있다. 또한 심사기준의 구조를 지칭하는 명칭도 다르게 사용하고 있다. PIMS는 통제분야, 통제목적, 통제항목으로 구분하고 PIPL은 심사영역, 심사목적, 심사항목으로 구분하고 있다. 후자일수록 하위항목이며, 상위항목보다 더 세분화된다. 두 인증제도의 구조는 통제분야-심사목적, 통제목적-심사목적, 통제항목-심사항목으로 대응된다.

이처럼 PIMS의 통제항목과 PIPL의 심사항목의 차이로 인해 심사항목 각각에 대한 상세내용의 요소를 곧바로 대응시켜 비교하는 데 어려움이 있다. 따

Table 3. Structure comparison of PIMS and PIPL

PIMS		PIPL	
Control area	Control content	Screening area	Screening content
Management process	Establishing policy and scope	Protection management system	Establishing protection management system
	Management's responsibility and organization		
	Risk management		Execution and operation
	Implementation		
	Maintenance		Correction and improvement
Protection measures	Personal information policy	Protection measures	Establishing protection management system
	Personal information protection organization		
	Personal information asset classification		Execution and operation
	Education for personal information protection		Managerial measures for ensuring safety
	Personnel security		
	Managing incidents		
	Technical protection measures		Technical measures for ensuring safety
	Physical protection measures		Physical measures for ensuring safety
Life cycle	Collection of personal information		Handling personal information
	Use and provision of personal information		Guarantee of right of information subject
			Managerial measures for ensuring safety
			Technical measures for ensuring safety
	Management and destruction of personal information		Handling personal information

라서 통제항목(심사항목)의 상세내용을 구성하는 요소 간의 중복성 평가를 수행하기에 앞서 통제목적(심사목적)을 고려하여 통제항목(심사항목)을 기준으로 비교한 후 대응시키는 과정을 선행한다.

PIMS의 124개 통제항목에 대하여 PIPL의 공공기관 기준에 해당하는 65개 심사항목 전체를 비교하여 대응시킨다. 표의 왼쪽에는 PIMS의 심사기준을 두고 이를 기준으로 하여 표의 오른쪽에 PIPL의 심사기준이 대응되도록 하였으며, 표 4의 예시와 같다.

4.3 통제항목(심사항목)의 상세내용에 대한 중복성 평가

선행된 PIMS의 통제항목과 PIPL의 심사항목 간에 대응된 결과를 바탕으로 상세내용의 구성요소에 대하여 중복성을 평가한다. 이를 위해 통제항목과 심사항목의 상세내용을 이행대상과 이행행위의 두 요소로 구분하고 구문분석을 실시하여 서로 비교하되, 기계적인 분석이 아닌 각 요소의 의미를 파악하여 완전하게 일치하는 경우에는 '완전중복', 일부 유사 또는 겹치는 부분이 있거나 부분으로 포함되는 경우에는 '부분중복', 의미가 전혀 다르거나 겹치는 부분이 없는 경우에는 '비중복'으로 판단한다. 그리고 이행대상과 이행행위 각각의 중복성을 판단하고 이를 종합하여 해당 통제항목과 심사항목 상세내용의 중복성에 대한 최종 평가를 수행한다. 이와 같은 중복성 평가 기준에 의해 동일한 이행대상에 대하여 동일한 이행행위를 요구하는 경우에는 중복성이 있다고 평가하게 된다.

이러한 중복성 평가 요소와 기준에 의해 통제항목과 심사항목 상세내용을 비교하여 중복성을 평가하며, 그 예시는 표 5와 같다.

PIMS 통제항목의 상세내용에서 드물게 이행행위를 수행하는 주체를 명시한 경우가 있는데, 이러한

Table 4. Comparison of control and screening items (partial)

PIMS				PIPL			
Control content	Control objective	Control item		Screening content	Screening objective	Screening item	
1. Measures for collection of personal informa-tion	1.1 Collection of minimum information	1.1.1	Collection of minimum information to provide services	5. Handling of personal informa-tion	5.1 Protection measures for collection of personal information	5.1.1	Limitation of collection of personal information
		1.1.2	Limitation of collection of important personal information			5.1.4	Limitation of collection of sensitive and unique identification information
		1.1.3	Measures for indirect collection			5.1.5	Protection measures for indirect collection
		1.1.4	Limitation of collection and use of resident registration number			5.1.4	Limitation of collection of sensitive and unique identification information
		1.1.5	Alternatives of resident registration number			5.1.6	Provision of alternative for joining

이행주체에 해당하는 부분은 밑줄로 표시하였고, 이행행위와 이행대상 두 요소에 해당되지 않는 부분은 괄호로 묶어 표시하였다. 이행행위는 굵은 글씨로 나타내었고, 이행대상은 기울임체로 표시하였다.

표 5에서 통제항목과 심사항목 상세내용의 이행행위는 각각 '저장'과 '보관, 보호조치에 의한 관리'이며 이는 모두 '개인정보처리시스템의 접속기록'에 대하여 수행하도록 하고 있기 때문에 '개인정보처리시스템의 접속기록'이 이행대상이 된다. 이행대상은 완전히 일치하기 때문에 '완전중복' 평가를 하였다. 이행행위는 PIPL에서는 '보관'과 '보호조치에 의한 관리'라고 명시하고 있는 반면, PIMS에서는 '저장'만 명시하고

Table 5. Redundancy assessment of detailed contents (partial)

PIMS				PIPL				
Control content	Control objective	Control item	Detailed content	Screening item	Detailed content	Target	Action	Assess-ment
7. Technical protection measures	7.6 Access history manage-ment and monitor-ing	Access history storage for personal informa-tion process-ing system	*Access history* (identifier, date and hour of access and reading, modification, deletion, output of personal information) for personal information handler *of personal information processing system* (such as application, DB) must **be stored**.	Access history manage ment for personal informa-tion system	*Access history of personal information processing system* must **be kept and managed** by protection measures.	Fully overlap	Partial overlap	Partial overlap

있어 두 인증제도에서 요구하는 행위가 다르다는 것을 알 수 있다. 그러나 '보관'과 '저장'은 표기는 다르지만 의미는 유사하기 때문에 이행행위는 부분적으로만 겹치는 것으로 판단하여 '부분중복' 평가를 하였다. 마지막으로 이행대상과 이행행위의 중복성 평가 결과는 각각 '완전중복'과 '부분중복'으로, 동일한 대상에 대하여 부분적으로만 겹치는 행위를 요구하기 때문에 최종적으로 '부분중복' 평가를 하였다.

4.4 통제항목(심사항목)의 상세내용에 대한 중복성 평가 결과

PIMS의 124개 통제항목과 PIPL의 65개 심사항목의 상세내용에 대하여 중복성을 평가한 결과는 다음과 같다.

중복성 평가 결과 PIMS의 124개 통제항목은 PIPL의 심사항목에 대하여 완전중복 10개(8.07%), 부분중복 73개(58.87%), 비중복 41개(33.06%)로 나타났으며, 중복되는 항목의 비율은 66.94%로 절반 이상의 항목이 PIPL의 항목과 중복되어 높은 중복성을 보이는 것으로 나타났다.

PIPL의 65개 심사항목은 PIMS의 통제항목에 대하여 완전중복 10개(15.38%), 부분중복 54개(83.08%), 비중복 1개(1.54%)로 나타났으며, 중복되는 항목의 비율은 98.46%에 달하는 것으로 분석되어 매우 높은 중복성을 보인다. 따라서 두 인증제도 간에는 중복성이 있음이 규명되었다.

PIMS와 PIPL의 중복 비율이 차이를 보이는 이유에 대하여는 PIMS의 통제항목이 이행대상에 대해 보다 더 세세하게 정의하고 있기 때문인 것으로 생각된다. 본 연구에서는 통제항목(심사항목)의 상세설명에 대하여 이행대상과 이행행위의 요소로 나누어

Table 6. Result of redundancy assessment (based on PIPL)

Redundancy criteria		Number of pertinent items (ratio)
Over-lap	Fully overlap	10 (15.38%)
	Partial overlap	54 (83.08%)
	Sub total	64 (98.46%)
Non-overlap		1 (1.54%)
Total		65 (100%)

Table 7. Result of redundancy assessment (based on PIMS)

Redundancy criteria		Number of pertinent items (ratio)
Over-lap	fully overlap	10 (8.07%)
	Partial overlap	73 (58.87%)
	Sub total	83 (66.94%)
Non-overlap		41 (33.06%)
Total		124 (100%)

중복성을 평가하였다. 이때, 동일한 이행행위라 할지라도 이행대상이 다르면 그 항목은 중복되지 않는다고 본다. 예를 들어 '보호대책 수립'이라는 동일한 이행행위가 각각 '서버'와 '네트워크'라는 서로 다른 이행대상에 대하여 수행하도록 정의되었다면 중복되지 않는 항목이라고 평가하게 된다.

그밖에 중복성을 평가하는 과정에서 개인정보보호 관리체계 인증제도 심사기준의 통합 시에 반영할만한 몇 가지 개선사항들을 발견하였다. 이에 대한 개선방법은 다음과 같다.

첫째, 한 항목에 하나의 이행대상을 정의한다. 하나의 심사항목에서 두 개의 이행대상을 정의하고 있는 경우가 있는데 통제항목(심사항목)은 개인정보의 보호를 위한 이행행위를 어떤 대상에 대해 수행해야 하는지를 정의한 것이다. 따라서 이를 명확하게 드러내기 위해서는 한 항목에는 하나의 이행대상을 정의하는 것이 바람직하다. 둘째, 용어를 통일한다. PIMS와 PIPL에서 사용하는 용어가 다른 경우가 있다. 예를 들면, PIMS에서는 개인정보보호정책, 개인정보관리책임자, 이용자와 같은 용어를 사용하고 있으나, PIPL에서는 개인정보 관리계획, 개인정보보호책임자, 정보주체라는 용어를 사용하고 있다. 개인정보보호 관리체계 인증제도의 통합 시에는 두 인증제도에서 다르게 사용하고 있는 용어를 통일하는 것이 필요하며, 법령에서 사용되고 있는 용어의 경우에는 그를 따르도록 한다. 셋째, 이행주체의 명시여부에 대해 일관성을 갖도록 한다. PIPL에서는 일관성 없이 '개인정보처리자'를 이행주체로 명시하고 있다. 그러나 개인정보처리자는 인증 신청기관인 개인정보보호 관리체계를 운용하는 조직 자체를 지칭하므로 특별한 의미를 갖지 못한다. 이행행위를 수행하는 이행주체가 의미를 갖는 경우에는 그대로 유지하지

만, '개인정보처리자'와 같이 특별한 의미 없이 명시된 경우에는 항목의 일관성을 위해 이행주체를 삭제한다. 넷째, 지나치게 세부적인 사항을 명시하지 않는다. 통제항목(심사항목)의 상세내용에 지나치게 세부적인 사항을 제시하는 경우가 있다. 이는 PIMS에서 많이 보이며, 이행대상의 예시를 나열하는 경우가 많다. 지나치게 많은 수식어를 사용하거나 예시를 일일이 열거하는 것은 이행대상과 행위를 명확하게 드러내는 데 방해요소가 되므로 지양하고, 세부적인 사항은 세부점검항목이나 인증 가이드 등에 정의하도록 한다.

V. 결 론

본 연구에서는 중복성과 중복규제의 원인과 문제점을 고찰하고, 개인정보보호 관리체계 인증제도간의 중복성을 평가하기 위한 방법론을 제시하였으며, 이를 바탕으로 중복성 평가를 수행하였다. 그 결과, 두 인증제도 간에는 상당한 수준의 중복성이 있음이 규명되었다.

본 연구는 PIMS와 PIPL 두 인증제도에 대하여 그 동안 논란이 되어 왔던 중복성을 구문분석을 통해 실증적으로 규명하였다는 점에서 의의가 있다. 또한 본 논문은 2014년 8월 결정된 개인정보보호 관리체계 인증제도 통합의 타당성을 뒷받침 한다.

향후에는 통합에 따른 개인정보보호 관리체계 인증제도의 효율적인 운영과 제도의 안정화를 도모하기 위한 바람직한 제도 운영 방안 등의 후속 연구가 필요하다.

References

[1] Korea Local Information Research & Development Institute, "Countermeasure of public institution of introduction of PIPL," 2014 Local Information Issue, Vol. 2, 2014.

[2] Boannews, "Visualization of integration of information security certification... What is priority?," 2014.8.11.

[3] Korea Internet & Security Agency, Outline of PIMS, Retrieved Oct. 21, 2015, from http://pims.kisa.or.kr/kor/intro/pimsIntro01.jsp.

[4] Korean Standard Dictionary, Retrieved Nov. 2, 2015, from http://stdweb2.korean.go.kr.

[5] M. Landau, "Redundancy, rationality, and the problem of duplication and overlap," Public Administration Review, Vol. 29, pp. 346-358, 1969.

[6] Jung-hai Kim, "A Study on the Reform of the overlapping regulation in the industrial safety sector," Korean Society and Public Administration, 15(1), pp. 211-233, 2004.

[7] Korea Ministry of Government Legislation, A study on Status and Improvement of duplicate regulation, 2008.

[8] Datanet, "ISMS, maintaining certification is more important than certification." 2013.10.7.

[9] Mi-na Sim, "(A) study on the implementation methodology of the efficient PIMS certification system," Ph.D. Thesis, Korea University, 2010.

[10] Heung-youl Youm, "The necessity of international standardization of personal information management system," Review of The Korea Institute of information Security & Cryptology, 23(4), pp. 65-72, 2013.

[11] Dong-hee Bang, "A study on the improvement of the personal information protection certification in the personal information protection legal system: Focusing on the current status, the problem, and the remedial alternative of certificate system," Public Law Journal, 15(1), pp. 263-300, 2014.

[12] Geon-sang Cha, Ho-hyeon Han, and Yong-tae Shin, "An effective Personal information management system to ensure self-imposed control on personal information protection act," Journal of Korean Institute of Information Scientists and Engineers: Information

networking, 39(3), pp. 276-281, 2012.
〔13〕 Eun-yeop Park, Jin-won Choi, and Tae-hee Cho, "A case study on building personal information management System Certification," Review of The Korea Institute of information Security & Cryptology, 21(5), pp. 27-36, 2011.
〔14〕 Jin-hwan Jeon and Kang-rae Cho, "The main changes in personal information management system certification by revised notification," Review of The Korea Institute of information Security & Cryptology, 23(5), pp. 20-23, 2013.
〔15〕 Dae-ha Park and Keun-hee Han, "A Study on PIMS Controls for PII outsourcing management under the cloud service environment," Jonornal of The Korea Institute of information Security & Cryptology, 23(6), pp. 1267-1276, 2013.
〔16〕 Jeong-woo Chae and Jin-hong Jeong, "Study on building security controls framework for the industrial security management system," Korean Academy of Public Safety and Criminal Justice, 22(1), pp. 300-341, 2013.
〔17〕 Jin-young Han and Su-jin Lee, "Privacy assessment model in healthcare: The case of specialty hospital," Journal of Internet Electronic Commerce Research, 14(6), pp. 27-44, 2014.
〔18〕 Dae-ha Park, Sang-nyeong Yoo, and Heung-youl Youm, "Development of information system operational audit checklist for personal information protection in public organizations," Journal of Security Engineering, 12(1), pp. 47-64, 2015.
〔19〕 K. Höne and J.H.P. Eloff, "Information security policy - what do international information security standards say?," Computers & Security, Vol. 21, No. 5, pp. 402-409, 2002.
〔20〕 M. Siponen and R. Willison, "Information security management standards: Problems and solutions," Information & Management, Vol. 46, No. 5, pp. 267-270, 2009.
〔21〕 Woon-soo Kim, Sook-young Jeong, Young-hyeon Cho, and Kyung-bae Kim, "A Study on improving scheme of environmental review aspects in urban management planning in Seoul," Seoul Studies, 8(1), pp. 107-125, 2007.
〔22〕 Korea IT Industry Promotion Agency, Report on Hw to Link a Similar Procedure for the Expansion of Digital Content Transaction Certification, 2008.
〔23〕 Hong-bin Im et al., Parsing Methodology of Korean, Hankookmunhwasa, 2002.
〔24〕 Jin-jae Choi and Sun-young Hwang, "Requirements redundancy and inconsistency analysis for use case modeling," Journal of KIISE: Software and Applications, 3(7), pp. 869-882, 2004.

〈저자소개〉

김 소 라 (So-Ra Kim) 정회원
2013년 2월: 충북대학교 법학부 졸업
2016년 2월: 충북대학교 정보보호경영학과 석사
2016년 3월~현재: (주)싸이버원 컨설턴트
〈관심분야〉 (개인)정보보호관리체계 인증, 정보보호 정책

김 태 성 (Tae-Sung Kim) 종신회원
1997년 2월: KAIST 산업경영학과 박사
1997년 2월~2000년 8월: 한국전자통신연구원 정보통신기술경영연구소 선임연구원
2005년 1월~2006년 2월: Univ. of North Carolina at Charlotte 방문교수
2010년 7월~2012년 7월: Arizona State University 방문연구원
2000년 9월~현재: 충북대학교 경영정보학과 교수/학과장, 보안컨설팅연계전공 주임교수, 일반대학원 정보보호경영전공 주임교수, 국가정보원 보안관리실태평가 자문 및 평가위원, 금융보안원 금융보안컴플라이언스 자문위원, 전자정부 민관협력포럼 자문위원
〈관심분야〉 정보통신과 정보보호 분야의 경영 및 정책 의사결정