情報保護學會論文誌
第 22 卷 第 2 號, 2012. 4

공공분야 개인정보보호 정책 집행과제의 우선순위 분석: 개인정보보호 수준진단 지표의 선정 및 중요도를 중심으로*

신 영 진,[1†] 정 형 철[2‡] 강 원 영[3]
[1]행정안전부, [2]수원대학교, [3]한국인터넷진흥원

A Study of Priority for Policy Implement of Personal Information Security in Public Sector: Focused on Personal Information Security Index*

Young-Jin Shin,[1†] Hyeong-Chul Jeong,[2‡] Won-Young Kang[3]
[1]Ministry of Public Administration and Security, [2]University of Suwon,
[3]Korea Internet & Security Agency

요 약

본 연구는 2008년부터 2011년까지 행정안전부에서 시행하고 있는 공공기관의 개인정보보호 수준진단 지표의 정책적 의미를 고찰하고, 각 지표의 중요도 선정에 따른 개인정보보호의 정책적 문제를 다루었다. 우선, 개인정보보호 수준진단 지표를 선정하기 위해 개인정보보호에 대한 정책 방향을 개인정보보호의 정책 및 기술적 측면, 개인정보의 관리적 측면, 개인정보 침해 대응적 측면인 세 분야로 구분하였다. 그리고, 각 정책방향에 따라 선정된 지표의 세부사항에 대해 학자, 전문가, 실무자를 대상으로 AHP 조사를 실시하여 우선적으로 추진해야 할 정책을 정하도록 하였다. AHP를 통해 개인정보보호 수준 진단 지표의 중요도를 도출하였으며, 개인정보보호정책의 일반적인 체계를 갖추기 위해 필요한 정책과제를 도출하였다. 결과적으로 공공기관의 개인정보보호의 제도적 기반 확충을 위해서는 웹사이트 상의 개인정보관리, 개인정보보호를 위한 전담 조직 및 인력, 그리고 개인정보보호시스템 도입 등이 우선 시 된다. 본 연구의 정책과제를 기초로 공공기관의 개인정보보호 수준진단 체계가 지속된다면 개인정보를 취급하는 공공기관에 대한 국민의 신뢰가 높아지고, 개인정보의 안전한 유통 및 가치가 향상되리라 기대한다.

ABSTRACT

This study is to consider political implication of indicators to measure personal information security in public sector studied by Ministry of Public Adminstration and Security from 2008 to 2011. The study analyzed the priority of personal information security policy dividing into personal information security infrastructure, personal information management with life cycle, correspondence of information infringement by scholars, experts, and chargers. As the results, to progress personal information security policy is important to management of personal identification information on web site; specially institutional infrastructure as responsible organization, exclusive manpower, and security budget; personal information security infrastructure. As like the results, it would be reflected in the progress of personal information security policy and tried to provide systematic management program with improving safe information distribution and usefulness.

Keywords: Personal information security index, Public sector, Priority of personal information security policy, AHP

접수일(2012년 2월 29일), 게재확정일(2012년 4월 20일)
* 본 연구의 교신저자 정형철은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 기초연구사업을 수행하였음(2011-0004945).
† 주저자, jinsyj@mopas.go.kr
‡ 교신저자, jhc@suwon.ac.kr

I. 서 론

정보사회가 고도화됨에 따라 정보화 순기능에 반하는 정보화 역기능 문제가 대두되고 있다. 정보화 역기능 중 해킹, 바이러스 위협 등 네트워크 및 시스템 보안 역시 주요 관심사이지만, 정보화 역기능 중 개개인의 국민이 직접적으로 접하게 되는 문제의 대부분은 개인정보 유출로 인한 직·간접적 피해이기에, 개인정보보호 문제가 현시점에서 심각하게 논의되고 다루어져야 한다. 한편, 행정업무에서 다양한 대국민 전자민원서비스가 제공됨에 따라, 민간 영역이 아닌 공공기관에서도 일반 국민의 개인정보가 다량으로 수집·이용 및 유통되고 있어, 과거와 달리 공공기관의 개인정보 유출 사고가 발생할 여지가 다분히 증가하고 있다. 그런데, 국민의 신뢰를 바탕으로 국가정책을 추진하는 공공기관의 개인정보 침해사고는 심각한 사회적 문제를 유발 할 수 있다. 이에 따라 공공기관을 대상으로 개인정보보호에 대한 정책이 강화될 필요가 있으며, 정부차원에서 개인정보보호를 위한 가이드라인, 지침 등을 마련할 필요가 있다. 이를 위해 정부차원의 공공기관 대상 개인정보보호 종합대책을 수립 및 추진함에 있어, 행정안전부는 2007년에 '공공기관 개인정보보호 수준진단' 지표를 개발하여 2008년부터 현장진단에서 해당 지표를 활용하고 있다. 공공기관의 개인정보보호 수준 진단 시 18대 진단 항목별로 100점 만점의 점수를 산출 한 후 지표에 부여된 중요도를 곱하여 최종 점수를 산출한다는 점에서 각 진단지표의 중요도는 매우 중요한 의미를 가지고 있다. 즉, 중요도에 따라 진단점수가 다르게 나타나지만, 가장 중요한 점은 개인정보보호에 대한 정책의 중요성이 어디에 있는가가 나타나기 때문이다. 이에, 본 연구에서는 2008년과 2009년 실시된 AHP 결과를 비교 분석함으로 공공기관에서 개인정보보호에 관한 기본적인 정책 방향을 수립할 때, 우선적으로 고려해야 할 정책과제의 중요도가 무엇인가를 검토하고자 한다.

본 연구에서는 개인정보보호 수준진단 지표에 대해 살펴보고, 중요도 결정을 위한 AHP 방법을 활용한 연구모형과 연구방법을 설명하였다. 또한 공공분야의 개인정보보호에 관한 정책중요도를 AHP 결과에 기초하여 도출한 후, 개인정보보호 수준진단지표의 중요도에 관한 변화 및 정책과제의 우선순위를 제시하고자 한다.

II. 개인정보보호 수준진단 지표의 범주화

2.1. 연구 동향 및 정책 방향

우리나라 개인정보보호 수준을 판단하고 최근 제시된 공공기관의 개인정보보호에 관한 법률을 비롯한 관계 법률(2010), 개인정보보호지침(2008), 공공기관의 CCTV설치 및 운영에 관한 지침(2008), 개인정보보호를 위한 기술적·물리적 보호조치(2009), 개인정보보호업무매뉴얼(2008), 그리고 개인정보보호관련 규정, 개인정보보호에 관한 평가체계 등의 검토를 위해서는 이를 가늠할 수 있는 진단지표가 필요하다[18][19][23][24][25]. 이러한 진단지표는 기존의 개인정보보호를 위해 연구된 내용을 기반으로 개인정보보호 수준 진단을 위한 정책과제의 이론적 범주화의 틀을 마련할 수 있다고 생각하기에 기존의 연구 내용을 살펴보기로 한다.

먼저, 권헌영[1]은 정보사회에서의 개인정보보호의 중요성을 제기하면서 개인정보보호에 관한 정책설계의 필요성을 제기하였다. 이에 개인정보보호의 제도 및 정책을 중심으로 변미리[6]는 보안관리의 문제, 통합기구의 부재 등을 지적하였으며, 개인정보보호에 관한 기관별 세부대책이 수립되어야 한다고 보았다. 임종인 등[15]은 개인정보보호를 위한 정책방향 제시함에 있어서 정보보호의 안전기준과 의무사항을 강화하여야 하며, 정보보호를 위한 개인정보보호 조직체계의 강화, 안전진단의 의무화, 사이버 범죄에 대한 처벌 강화 등을 주장하였다. 장태수[17]는 정보보호를 위한 통합기구의 분산적 보안이 유기적으로 통합되어야 하며, 개인정보보호에 관한 인식제고를 위해 교육을 제공하고 정보공개를 통한 관리방안을 주장하였다. 특히, 개인정보보호를 위한 안전한 관리방안에 관하여는, 신영진[9][10]은 개인정보관리의 효율성을 높이기 위해 개인정보보호예산과 인력을 적절히 확보하여야 하며, 정보보호를 위한 보안시스템의 구축 등이 필요하다고 주장하였다. 개인정보의 수집 및 관리에 대해서는 김민호[3]는 적법하고 정당한 개인정보의 수집부터 폐기까지 의 관리를 강화하고, 개인정보의 수집을 제한하고 개인정보 보유파일을 안전하게 관리하여야 하며, 침해사고가 발생할 경우 대응절차 등을 마련하여 효율적으로 운영하여야 한다고 보았다. 송유진 등[7]도 개인정보의 수집, 저장·관리, 이용·제공, 파기 등 일련의 과정에서 개인정보를 안전하게 관리하고 보호하는 방안을 제시하였다. 박홍윤[5]은 개인정보

〔표 1〕 개인정보보호를 위한 세부정책 분류

상위지표	중위지표	하위지표	내적 일치도
정책적·기술적 측면	정책기반	1. 개인정보보호 조직 및 인력 확충	0.706
		2. 개인정보보호예산 확보	-
		3. 개인정보보호 교육 제공	0.685
		4. 개인정보보호방침 마련	0.815
	기술기반	5. 개인정보보호시스템의 도입	0.547
		6. 개인정보처리시스템의 접근통제	0.650
		7. 개인정보 저장·전송 시 암호화	0.551
처리단계의 관리적 측면	수집 및 보유	8. 개인정보수집절차 마련	0.896
		9. 개인정보파일대장의 관리	0.847
		10. CCTV 관리규정 마련	0.823
		11. 개인정보 저장·출력 매체 관리	0.516
	이용 및 제공	12. 개인정보처리시스템의 접근·이용기록 관리	0.660
		13. 처리정보의 이용 및 제공시 관리	0.791
	파기	14. 개인정보의 파기절차 마련	0.761
		15. 저장매체 파기 관리	0.796
침해대응적 측면	웹사이트 개인정보의 노출방지	16. 웹사이트 개인정보 노출 관리	0.738
	개인정보의 유출방지	17. 개인정보침해사고 대응절차 마련	0.378
	개인정보의 침해구제	18. 개인정보침해 구제절차 마련	0.798

의 이용과 통제에 관한 정보시스템통제의 중요성을 제기하였으며, 시스템의 개발을 통해 개인정보의 안전한 관리를 지원하여야 한다고 보았다.

또한, 개인정보의 침해사고를 분석하여 정보보호를 위한 제도와 대책을 마련함에 있어서, 김민기〔2〕는 공공기관의 홈페이지를 대상으로 불건전한 방법으로 개인정보가 유통되거나 노출되는 실태를 분석하여 인터넷상의 안전성을 확보하여야 한다고 주장하였으며, 문신용 등〔4〕은 개인정보침해사고를 분석하여 대책을 마련하여야 한다고 주장하였다. 이외에도 오태원〔11〕, 임영덕〔14〕 등은 유비쿼터스 사회가 도래됨에 따라 발생할 수 있는 개인정보의 침해사고를 예방하고 안전한 정보화환경을 구현하기 위해서 개인정보보호에 관한 정책이 강화되어야 한다고 보았다. 임종인〔16〕, 윤취영〔12〕 등은 앞으로 개인정보보호를 위한 공공기관의 노력을 평가하고 안전한 관리체계가 필요하다고 보았다.

이와 같은 개인정보보호에 관한 다양한 법률, 규정, 지침, 가이드라인 및 업무매뉴얼을 비롯하여 개인정보보호에 관해 공공기관이 수행해야 할 법적 준수사항이나 정책과제들을 정책적 측면, 기술적 측면, 관리적 측면, 그리고 개인정보 침해사고에 대한 대응적 측면 등으로 세분화 할 수 있다. 특히, 앞서 논의한 연구와 법적 규정을 바탕으로 전반적인 정책과 기술에 관해서는 정책·기술적 측면으로 통합할 수 있으며, 개인정보의 생애주기(수집·이용·제공·파기 등)에 따른 개인정보 관리, 그리고 개인정보의 침해 및 역기능으로부터의 대응하기 위한 개인정보 침해사고 대응절차로 구분하여 크게 정책, 관리, 대응이라는 세부분으로 정책과제를 범주화할 수 있다.

2.2. 지표의 범주화

한국지역정보개발원 등〔22〕은 국내 정보보호수준 향상을 위해 개인정보보호 지표들을 도출하였는데, 이는 정책·기술적 보호기반, 생애주기별 정보관리, 정보침해 대응대책 등 크게 3개 상위지표와 18개 하위지표로 분리된다. 그런데, 이는 기존의 연구동향과 정책방향을 기초로 한 것이며, 각 세부정책의 특성에 따라 상위정책 및 매우 다양한 세부과제로 세분화 할 수 있다. 초기 개발된 지표는 3개 상위지표, 8개 중위지표, 18개 하위지표, 85개 진단항목으로 범주화 되었다〔21〕. 이들 측정 지표의 특성을 살펴보기로 하자.

먼저, 제 1 상위지표는 정책·기술적 측면으로 구성되며, 이는 다시 공공기관에서 개인정보보호를 수행하기 위해 필요한 조직·예산·교육 등의 정책기반과 개인정보보호를 위해 필요한 시스템의 도입과 운영·관리를 위한 기술적 기반으로 양분된다. 여기서, 중위지표인 (1) 정책기반은 개인정보보호에 관한 조직 및 인력의 확충, 개인정보보호예산의 확보, 개인정보보호에 관한 교육 제공 및 개인정보보호방침 마련 등의 하위지표들이 구성된다. 또한, (2) 기술기반은 개인정보보

호시스템의 도입 및 개인정보처리시스템의 접근통제, 개인정보의 저장·전송 시 암호화 등으로 구성된다. 물론, 이들 각 하위지표 별 수행 및 진단하여야 할 구체적 진단항목이 할당되어 있다[1].

제 2 상위지표인 처리단계의 관리적 측면에서는 개인정보의 수집·보유, 이용·제공, 파기 등 생명주기(life-cycle)별 단계에 따라 절차기준이 설정되는 특징을 지닌다. 구체적으로 (1) 개인정보의 수집 및 보유정책에서는 개인정보수집절차를 마련하고 준수하고, 개인정보파일대장과 CCTV를 적절히 관리하고, 개인정보 저장·출력매체를 안전하게 관리하는 방법의 하위지표로 구성되어 있다. (2) 개인정보의 이용 및 제공정책은 개인정보처리시스템의 접근·이용에 관한 기록 관리, 처리정보의 이용 및 제공시 적절한 관리 등으로 구성되어 있다. (3) 개인정보의 파기정책은 개인정보의 파기절차를 수립하며, 저장매체를 파기할 때도 그에 따른 계획을 수립하여 안전하게 파기하도록 준수사항으로 구성된다.

제 3 상위지표인 침해대응적 측면은 개인정보의 침해사고를 해결하기 위해 사전·사후적 보호조치로 설명할 수 있는데, (1) 웹사이트 개인정보 노출방지를 위한 웹 모니터링 등과 같은 침해방지방안, (2) 개인정보 유출방지를 위한 대응절차를 수립, (3) 개인정보 침해발생시 구제절차를 운영의 하위지표 등으로 구분된다.

한편, 〔표 1〕의 오른편에 해당 지표들의 내적일치도인 크론바흐 알파값을 볼 수 있다. 본 내적일치도는 2010년 자율진단에 참여한 1,023 개 기관의 자료를 기초로 계산한 결과이다. 내적일치도 값이 높으면, 해당 문항들은 서로 유사한 개념을 측정하고 있다고 볼 수 있다. 위의 예에서 개인정보 침해사고 대응절차의 세부과제들의 내적일치도 0.378 이외에 모든 세부정책의 내적일치도가 높음을 볼 수 있다. 개인정보보호 지표들 간에 음의 내적일치도가 발견되지 않고 대부분 높은 일치도가 나타났으므로, 계층적 구조로 개발한 본 정보보호 지표들의 진단항목들은 내부적으로 동일한 정책 목표를 수행하도록 설계되었다고 할 수 있다.

1) 85개 진단항목에 대해서 일례를 들면, 정책·기술적 측면의 하위지표 중 '개인정보보호에 관한 조직 및 인력 확충'은 (1) 개인정보보호 업무를 담당하는 부서 및 협의체 구성 여부, (2) 개인정보관리책임관(CPO) 지정 여부, (3) 개인정보보호 담당자 지정 여부, (4) 분야별 책임관 및 개인정보취급자 지정 여부 등의 진단항목으로 구성되어 있다.

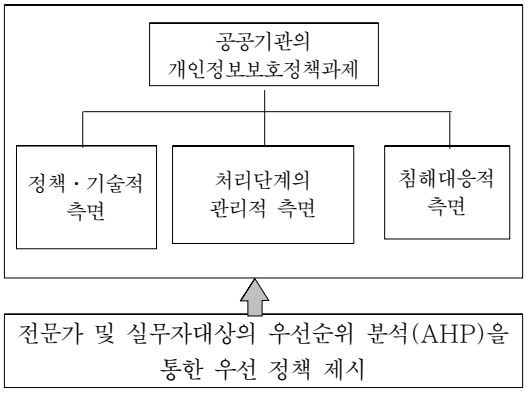
III. 중요도 분석 연구방법

본 연구의 주된 목표는 공공기관이 개인정보보호를 추진하는 정책과제들을 중요도를 선정하고 이들 중요도에 기초하여 공공기관 개인정보보호의 정책방향이 어떠한가를 밝히는 것이다. 이를 위해서 첫째, 개인정보보호의 정책적·기술적 측면, 처리단계의 관리적 측면, 개인정보 침해대응적 측면으로 구성된 상위 정책에 종속 구조를 취하는 하위 18대 정책의 중요도성을 밝히기 위해 AHP 설문지를 우선 작성하였다〔8〕〔21〕.

둘째, 하위 18대 정책의 중요도를 밝히고자, 하위정책에 대한 구체적 진단항목이 자세히 기술된 설문지를 기초로 2008년 6월 5일에서 6월 25일, 2009년 5월 1일에서 5월 11일까지 2차례 설문조사를 실시하였다. 설문조사의 대상은 개인정보보호관련 법률·기술·정책을 전공하거나 연구하고 있는 학자 및 연구자로 구성된 전문가집단과 중앙부처 및 지방자치단체의 개인정보보호업무를 담당하는 실무자집단이었다.

셋째, 공공기관의 개인정보보호정책을 추진하기 위한 우선정책과제를 선정하고자 AHP 방법으로 중요도를 산출하였다. 본 연구에서는 단일 순위행렬을 기하평균으로 형성한 후 고유치분해방법으로 집단중요도를 산출하였다. 특히, 개인 일관성 지수가 0.2이상인 응답자는 응답일관성이 결여된 설문으로 고려하여 제거하였다.

계층적 구조이므로, 응답자의 일관성을 측정하기 위해, 계층 전체에 대한 계층일관성 지수(HCI) 및 계층무작위 지수(HRI)를 사용하여, 계층일관성 비율(consistency ratio of an entire hierarchy: CRH)을 계산하였다. 본 연구에서 다루는 지표는 모두 3개의 층이므로 HCI, HRI, CRH는 다음과 같이



〔그림 1〕 분석의 틀

계산된다.

$$HCI = CI^{(1)} + \sum_{i}^{s^{(1)}} w_i^{(1)} CI_i^{(2)} + \sum_{i}^{s^{(1)}} \sum_{j}^{s_{(i)}^{(2)}} w_{i(j)}^{(2)} CI_{i(j)}^{(3)}$$

$$HRI = RI_1^{(1)} + \sum_{i}^{s^{(1)}} w_i^{(1)} RI_i^{(2)} + \sum_{i}^{s^{(1)}} \sum_{j}^{s_{(i)}^{(2)}} w_{i(j)}^{(2)} RI_{i(j)}^{(3)}$$

$$CRH = HCI / HRI$$

여기서, $w_i^{(k)}$는 k번째 층에서 i번째 지표에 대한 AHP 중요도로 $k=1,2,3$이다. 그리고 $w_{i(j)}^{(k)}$는 k번째 층에서 상위 i지표에 대응되는 하위 j지표의 AHP 중요도다. 또한, $CI_{i(j)}^{(k)}$와 $RI_{i(j)}^{(k)}$는 k번째 층에서 i번째 상위지표에 대응되는 지표 j의 일관성지수와 무작위지수를 의미한다. 그리고, $s^{(1)}$은 1번째 층에 대응되는 지표의 개수로 여기서는 $s^{(1)}=3$이며, $s_{(i)}^{(2)}$는 2번째 층에서 상위 i번째 지표에 속한 하위지표들의 개수로 $s_1^{(2)}=2, s_2^{(2)}=3, s_3^{(2)}=3$이다〔20〕. 유도된 중요도를 기초로 공공기관이 개인정보보호 정책을 수립함에 있어 효율적인 방향을 다음 제시하고자 한다. 또한, 이들 중요도가 향후 어떤 방향으로 개선되어 2011년까지 적용되어 왔는가를 살펴보기로 한다.

IV. 분석 결과

4.1. 지표개발 전개과정

행정안전부가 주관하는 '공공기관 개인정보보호 수준진단' 지표는 2007년 개발되었으며, 2008년에는 40여개 중앙부처를 대상으로 현장진단이 실시되었다. 2009년에는 중앙부처, 자치단체, 공사공단, 교육기관으로 그 대상이 확대되어 70여 기관에 대한 현장진단이 실시되었다. 그리고 2010년에는 100여개 기관에 대한 현장진단이 실시되었고 자율진단의 규모를 대폭 확대한 바 있으며, 2011년에는 현장진단의 규모를 2010년에 비해 100% 이상 증가한 220개 기관으로 하여 해당 사업을 지속적으로 확대 추진하면서 공공기관의 개인정보보호 수준 향상을 도모하여 왔다. 비록, 개인정보보호 수준진단지표가 2008년의 85개 지표에서 2009년 75개, 2010년 70개, 2011년 48개 지표로 변화하였으나, 진단항목의 변화만 있을 뿐, 3대 상위지표, 8대 중위지표 및 18대 하위지표는 변화없이 그대로 유지되어 왔다.

한편, 가장 최근인 2011년 진단에서는, 2010년 결과에 기초하되, 진단대상 기관을 가군, 나군, 다군으로 분류하여 차등적 지표가중치를 부여한 바 있다. 여기서 가군은 개인정보보호 수준이 다소 높거나 높이 요구되는 기관, 나군은 보통 수준 기관, 다군은 개인정보보호를 홍보하고 발전시켜야할 기관으로, 기관별 특성에 따라 집중해야할 정책의 방향성이 다소 다른 기관들을 의미한다. 또한, 2010년에는 개인정보보호 예산은 공공기관이 자체적으로 결정할 수 없는 사안일 수 있다는 의견에 따라 참고지표로만 활용하게 되는 가중치 변화가 있었다. 그런데, 지표전개과정의 많은 변화에도 불구하고, 현 진단지표의 중요도는 2008년과 2009년의 AHP 결과, 그 중 특히 2009년 결과에 그 근원을 두고 있다. 이에, 본 연구에서는 2008년과 2009년 실시된 AHP 결과를 비교분석함으로 공공기관에서 개인정보보호에 관한 기본적인 정책 방향을 수립할 때, 우선적으로 고려해야 할 정책과제를 살펴보기로 한다. 또한, 지표의 중요도 변화를 통해 공공기관의 개인정보보호에 대한 정책의 고도화 방향을 아울러 살펴보겠다.

〔표 2〕는 2008년 응답자와 2009년 응답자의 기관과 연구 분야의 분포를 보여준다. 2008년에는 학계와 공공기관 실무자의 조사율이 거의 동일하였으나 신뢰성 있는 응답을 한 비율은 학계에 있는 사람이 다소

〔표 2〕 설문조사의 응답 결과 및 비율

변수	항목	2008				2009			
		응답자 98명		응답자 61명		응답자 346명		응답자 242명	
		빈도	비율(%)	빈도	비율(%)	빈도	비율(%)	빈도	비율(%)
기관유형	학자・전문가	47	47.95	32	52.46	18	5.20	15	6.20
	실무자	48	48.97	29	47.54	303	87.57	211	87.19
	기타	3	3.06	0	0	25	7.23	16	6.61
연구분야	법률	21	21.43	16	26.23	3	0.87	2	0.83
	정책	33	33.67	20	32.79	49	14.16	37	15.29
	기술	25	25.51	13	21.31	96	27.75	66	27.27
	기타	19	19.38	12	19.67	198	57.23	137	56.61

높았음을 볼 수 있다. 2009년에도 신뢰성 있는 응답을 한 비율은 2008년과 유사하다. 한편, 2008년에는 연구 분야가 법학인 사람의 신뢰성 있는 응답비율이 정책 담당자보다 다소 높은 반면, 2009년에는 연구 분야 간 신뢰성 있는 응답자의 비율 변화는 거의 차이가 없음을 볼 수 있다[2].

4.2. 중요도 결과 비교

집단의사결정에서 최종 진단지표의 중요도 w를 계산하는 방법으로, 계층일관성이 높은 자료에 대해, 집단 전체의 기하평균 행렬을 사용하는 기하평균 산출방법과 각 개인별 중요도를 산출한 후 이를 다시 산술평균 하는 방법을 생각할 수 있다[13]. 본 연구에서는 두 방법의 CRH를 비교하여 CRH가 낮은 기하평균 방법으로 각 진단 지표의 중요도(중요도)를 계산하였다. 이제, 중요도 결과를 비교분석하기로 하자.

첫째, 개인정보보호정책의 3개 상위지표에 대한 중요성을 비교한 결과, 정책·기술적 측면(0.4856, 0.5034)이 가장 높게 나타나, 개인정보보호환경을 조성하기 위한 기반 확충이 가장 우선시 되어야 함을 알 수 있다. 그 다음 순위로 2008년에는 처리단계의 관리적 측면(0.3191), 2009년에는 침해대응적 측면(0.2582)이 중요하다고 보았다([표 3] 참고). 2008년도와 2009년도의 차이가 발생한 것은, 2008년에 인터넷상의 해킹사고 및 개인정보의 웹사이트 상 노출이 증가하여 정부에서도 본격적인 웹사이트 모니터링 사업을 추진하였는데, 이러한 계기로 개인정보보호 담당 실무자의 의견이 2009년에 반영된 것으로 고려된다. 한편, 이와 같은 결과에 따라 공공기관 개인정보보호 우선 순위는 정책 및 기술 기반 → 침해 대응 → 관리의 순으로 결정되었다.

[표 3] 3개 상위지표 정책의 중요도

상위지표	2008		2009	
	중요도	순위	중요도	순위
정책·기술적 측면	0.4856	1	0.5034	1
처리단계의 관리적 측면	0.3191	2	0.2384	3
침해대응적 측면	0.1954	3	0.2582	2

둘째, 중위지표 중에서 중요도를 선정한 결과, 2008년과 2009년의 응답결과가 유사하게 나타났는데, 먼저, 정책·기술적 측면의 정책기반과 기술기반에서는 정책기반(0.6230, 0.5971)이 기술기반(0.3770, 0.4029)보다 중요한 것으로 나타났다([표 4] 참고). 정책·기술적 측면의 정책기반과 기술기반이 다른 상위정책들보다 상대적으로 중요도가 높게 나타나는데 이는 개인정보보호환경을 조성함에 있어 인프라의 중요성을 강조되고 있음을 의미한다고 하겠다. 그런데, [표 4]에서 보면, 정책기관과 기술기반의 중위지표가 다른 중위지표에 비해 2개에 불과하기 때문에 기술기반의 중요도를 다른 상위지표에 포함된 중위지표와 단순 비교하기는 다소 무리한 면이 있다. 하지만, 정책·기술적 측면의 상위지표가 다른 상대지표에 비해 매우 높은 수준이기에 기술기반의 중위 중요도 역시 다른 중위지표의 중요도에 비해 높은 수준이라고 언급할 수 있다. 이에 따라, 제도적 기반에서는 개인정보보호에 관한 조직 및 인력을 확충하고, 개인정보보호에 관한 예산과 교육과정을 마련하고, 개인정보보호에 관한 규정을 강화하는 일이 무엇보다도 중요하며, 기술적 기반에서는 개인정보처리과정을 안전하게 운영할 수 있는 개인정보보호시스템을 구축하고 개인정보처리시스템의 안전한 접근통제가 제도적 기반 다음으로 이루어져야 하는 방향으로 정책이 유도되어야 한다고 할 수 있다.

다음의 처리단계의 관리적 측면에서는 개인정보의 수집 및 보유(0.440, 0.4210), 이용 및 제공(0.3682, 0.3677), 파기(0.1878, 0.2113) 순으로 정책과제가 강화되어야 함으로 나타났다. 이처럼 개인정보의 수집 및 보유를 위한 정책과제가 이용 및 제공에 따른 정책과제와 파기과정에서의 정책과제보다 중요하다고 전문가들은 보았다. 이러한 결과를 기초로, 파기 과정보다는 수집 및 이용되는 과정에서 개인정보가 침해될 우려가 높기 때문에 이에 대한 안전한 관리대책 수립이 필요함을 발견할 수 있다.

침해대응적 측면에서는 웹사이트 개인정보의 노출방지(0.4213, 0.6333), 개인정보의 유출방지(0.3067, 0.1885), 개인정보침해구제(0.2720, 0.1782) 순으로

2) 2008년과 2009년 응답자의 가장 큰 변화는 실무자인 사람의 비율이 대폭 확대하였는 점인데, 2008년 초기에는 학자와 법률 분야 전문가들이 해당 지표에 좀 더 관심을 두고 검토하였으며, 이들의 의견이 다소 높게 반영되었다. 하지만, 2008년 1차 진단을 마치고, 지표를 발전시키는 과정에서 정책 담당자인 실무자의 의견이 강화되어야 한다는 의견이 높게 개진되었다. 이러한 관계로 2009년에 실무자를 많이 조사하게 되었으며, 결국 실무자의 의견이 향후 중요도 개선에 많은 영향을 끼치게 될 것임을 응답자 비율에서 미리 짐작할 수 있다.

〔표 4〕 중위지표의 중요도 결과

상위지표	중위지표	2008		20009	
		중요도	내부순위	중요도	내부순위
정책·기술적 측면	정책기반	0.6230	1	0.5971	1
	기술기반	0.3770	2	0.4029	2
처리단계의 관리적 측면	수집 및 보유	0.4440	1	0.4210	1
	이용 및 제공	0.3682	2	0.3677	2
	파기	0.1878	3	0.2113	3
침해대응적 측면	웹사이트 개인정보의 노출방지	0.4213	1	0.6333	1
	개인정보의 유출방지	0.3067	2	0.1885	2
	개인정보의 침해구제	0.2720	3	0.1782	3

〔표 5〕 년도 별 하위지표에 부여된 중요도

상위지표	하위지표	2008		2009		2010		2011		
		중요도	순위	중요도	순위	중요도	순위	가군	나군	다군
정책및 기술적 측면	1. 개인정보보호 조직 및 인력 확충	10.70	1	13.73	2	13	2	8	13	14
	2. 개인정보보호예산 확보	7.88	3	7.94	4	0	0	0	0	0
	3. 개인정보보호 교육 제공	6.08	8	7.36	5	8	4	6	8	10
	4. 개인정보보호방침 마련	5.59	10	5.12	8	6	5	4	6	7
	5. 개인정보보호시스템의 도입	6.70	6	11.43	3	12	3	14	12	10
	6. 개인정보처리시스템의 접근통제	6.48	7	5.69	7	6	5	8	6	4
	7. 개인정보 저장·전송 시 암호화	5.13	12	5.92	6	6	5	8	6	4
처리 단계의 관리적 측면	8. 개인정보수집절차 마련	4.96	13	2.83	13	3	13	2	3	4
	9. 개인정보파일대장의 관리	1.28	17	1.35	18	1	17	1	1	3
	10. CCTV 관리규정 마련	1.11	18	1.91	17	2	15	1	2	2
	11. 개인정보 저장·출력 매체 관리	6.81	5	2.43	14	5	9	7	5	3
	12. 개인정보처리시스템의 접근·이용기록 관리	7.04	4	3.93	11	6	5	8	6	4
	13. 처리정보의 이용 및 제공시 관리	4.71	14	3.52	12	4	11	3	4	5
	14. 개인정보의 파기절차 마련	3.96	15	2.33	15	3	13	2	3	5
	15. 저장매체 파기 관리	2.03	16	1.95	16	2	15	2	2	4
침해 대응적 측면	16. 웹사이트 개인정보 노출 관리	8.23	2	14.3	1	14	1	16	14	12
	17. 개인정보침해사고 대응절차 마련	5.99	9	4.26	9	5	9	7	5	5
	18. 개인정보침해 구제절차 마련	5.31	11	4.02	10	4	11	3	4	4
총점		100		100		100		100		

중요도가 나타났다. 즉, 개인정보의 노출 및 유출사고가 발생하지 않도록 보호조치를 강화하고, 안전한 정보화환경을 구현하도록 침해사고발생시 구제 및 대응대책이 마련되어야 한다. 더욱이, 웹사이트를 통해 정보제공 기능이 보편화됨에 따라 각 기관에서의 웹사이트 운영상 기술적·관리적 측면에서의 보호가 더욱 요구되고 있다. 흥미로운 점은 2008년과 2009년 모두 3단계 별 각각의 상위정책의 순위는 변화가 없다는 점이다. 이에 따라 단계별 상위정책의 중요성을 가늠할 수 있다.

셋째, 2008년과 2009년 100점 만점으로 환산한 하위지표의 중요도는 〔표 5〕에 주어져 있다. 여기서, 공공기관의 개인정보보호를 위한 제도적 기반을 갖추기 위해 개인정보보호를 위한 조직 및 인력이 확충되어야 하며(0.1070, 0.1373), 웹사이트 개인정보의 노출방지를 위한 대책(0.0823, 0.1430), 개인정보보호에 관한 예산을 확보하는 것이(0.0788, 0.0794) 다른 과제에 비해 중요하게 나타났음을 볼 수 있다. 흥미로운 점은 2008년과 2009년의 세부정책의 1, 2 순위에 변화가 있다는 점이다. 즉, 개인정보보호 조직 및 인력확충이 2008년에는 가장 중요한 요소였으나, 2009년 실무자 위주의 결과에서는 웹사이트 개인정보 노출 관리가 가장 중요한 요소로 등장한다는 점이다. 즉, 공공기관의 실질적 평가 및 진단에서 실무담당자

입장에서는 조직과 인력 문제보다 개인정보 노출 관리의 중요도가 더 절실하다는 점이다. 이를 통해 향후 정보보호 수준 진단에서 실무자의 의견이 더 강조되는 방향으로 정책의 변화가 있어야 함을 알 수 있다.

〔표 5〕는 2011년까지 공공기관 개인정보보호 수준 진단 시 적용된 년도별 중요도의 변화를 아울러 보여준다. 2008년과 2009년에는 앞의 AHP에 의한 조사 결과가 그대로 반영되어 개인정보보호 수준이 진단되었으며, 2010년에는 개인정보보호 예산에 대한 중요도를 부여하지 않고 참고 지표로 고려해야 하는 의견 때문에 예산 부분에는 중요도가 부여되지 않고, 그 값이 다른 영역에 재 할당되어 새로운 중요도가 산출되었다. 그런데, 2010년의 중요도는 2009년의 값을 정수로 변경하되, 예산부분의 중요도는 2008년에 비해 2009년 낮게 계산된 개인정보 관리 부분인 개인정보 저장·출력 매체 관리와 개인정보처리 시스템의 접근·이용 기록 관리에 주로 할당되었음을 볼 수 있다. 한편, 2011년에는 공공기관의 전반적인 보호수준 제고를 위해 대상 기관을 확대하여 추진하는 과정에서, 기관별 특성을 고려하여 지표를 개선할 필요가 대두되었다. 이에 따라 개인정보보호 수준이 다소 높고 어느 정도 고도화된 기관은 가군, 보통 수준인 기관을 나군, 개인정보보호 수준의 아직 초기단계라고 고려된 기관을 다군으로 분류한 차등 중요도지표가 개발되었다. 여기서, 가군은 중앙부처가 주로 해당되며, 나군은 기초자치단체, 다군은 공사공단이나 대학 등이 주로 해당되었다. 결국, 2011년의 각 가중치는 2010년 결과에 기초하여 정보보호 수준이 높은 기관들이 평균적으로 높은 수준에 도달한 지표에는 가중치를 낮게 부여하고 그렇지 않은 영역에는 가중치를 상대적으로 높게 주는 방법으로 개편되었다. 여기서 2011년의 나군의 중요도는 2010년과 동일함으로 개인정보보호 진단항목의 일반적 중요도를 보여준다.

결론적으로 2011년 각 기관의 가중치를 기초로 공공기관 개인정보보호 수준 진단이 어느 단계로 발전해야 하는가의 정책 변화를 가늠할 수 있다. 즉, 초기에는 개인정보보호 조직 및 인력확충이 중요하며, 담당자의 교육이 우선시 되는 등 기반적 측면이 무엇보다도 강조되었다는 점이다. 그리고, 개인정보보호 수준이 어느 정도 안정화 단계에 들어서면, 개인정보보호 시스템 도입, 접근 통제, 로그파일 관리 및 분석, 웹사이트 상 개인정보 노출 사전 필터링 등 기술적 측면과 관리에 대한 중요도가 강조되고 있음을 볼 수 있다. 이와 같이 개인정보보호 수준 향상은 초기의 일반적 기반 확충 단계에서 기술적 관리가 강조되는 방향으로 고도화 됨을 발견할 수 있다. 즉, 개인정보보호 정책은 개인정보보호에 대한 공공기관 전반의 인식의 확대에서 점차적으로 기술 및 시스템 도입으로 전환되어 침해대응정책을 강화하는 방향으로 발전한다.

4.3. 응답자특성별 결과비교

개인정보보호정책과제의 응답자는 개인정보보호에 관한 제도(법률, 정책 등), 기술, 기타 분야에서 이론적·실무적 경험을 갖추고 있는 사람으로, 크게 학자·연구자로 구성된 전문가집단과 개인정보보호업무를 담당하는 실무자집단으로 구분할 수 있다. 본 절에서는 이들 전문가집단과 실무자집단의 차이를 비교하기로 한다.

두 집단 모두 2008년 조사에서는 정책·기술적 측면(0.4227, 0.5545)이 가장 중요하다고 보았으며, 처리단계의 관리적 측면(0.3732, 0.2631), 개인정보 침해대응적 측면(0.2041, 0.1824) 등의 순으로 정책이 중요하다고 보았다(〔표 6〕 참고). 그 중에서 실무자집단은 정책·기술적 측면이 개인정보보호정책에 더 큰 비중을 차지한다고 보았으며, 처리단계의 관리적 측면 및 개인정보 침해대응적 측면에서는 전문가집단이 실무자집단에 비해 중요하다고 보았다. 그런데, 2009년 조사에서는 전문가집단의 견해는 큰 변화가 없으나, 실무자집단에서는 많은 변화가 있음을 볼 수

〔표 6〕 전문가 및 실무자의 정책중요도 비교

구분		전문가(CRH = 0.1434)		실무자(CRH = 0.04417)	
		중요도	순위	중요도	순위
정책·기술적 측면	2008	0.4227	1	0.5545	1
	2009	0.4454	1	0.5860	1
처리단계의 관리적 측면	2008	0.3732	2	0.2631	2
	2009	0.2810	2	0.1936	3
침해대응적 측면	2008	0.2041	3	0.1824	3
	2009	0.2737	3	0.2205	2

〔표 7〕 전문가 및 실무자의 중위지표 중요도 비교

상위지표	중위지표		전문가(CRH=0.1434)		실무자(CRH=0.04417)	
			중요도	내부순위	중요도	내부순위
정책 및 기술적 측면	정책기반	2008	0.6495	1	0.5929	1
		2009	0.5448	1	0.6008	1
	기술기반	2008	0.3505	2	0.4071	2
		2009	0.4552	2	0.3992	2
처리단계의 관리적 측면	수집 및 보유	2008	0.3991	1	0.4939	1
		2009	0.4664	1	0.4211	1
	이용 및 제공	2008	0.3833	2	0.3483	2
		2009	0.3544	2	0.3639	2
	파기	2008	0.2176	3	0.1578	3
		2009	0.1792	3	0.2150	3
침해대응적 측면	웹사이트 개인정보 노출방지	2008	0.3480	2	0.4359	1
		2009	0.5257	1	0.6408	1
	개인정보 유출방지	2008	0.1249	3	0.3410	2
		2009	0.2649	2	0.1867	2
	개인정보 침해구제	2008	0.5271	1	0.2232	3
		2009	0.2095	3	0.1725	3

있다. 즉, 정책·기술적 측면의 중요도가 실무자 집단에서 2009년에 더 비중이 높아진 반면, 이에 비례하여 처리단계의 관리적 측면의 비중은 크게 감소하였다는 점이다. 결국, 2009년 실무자 집단의 의견은 2008년과 비교하여 그 우선순위가 관리적 측면보다 개인정보의 침해 대응적 측면을 강조해야 하는 것으로 바뀌었음을 보게 된다.

한편, 전문가 집단에서 2008년과 2009년 개인정보의 침해대응적 측면의 중위지표 3가지의 순위가 모두 바뀐 점을 제외하면, 중위지표의 다른 영역에서는 전문가 집단이나 실무자 집단 모두 그 변화가 크지 않다(〔표 7〕 참고). 〔표 7〕의 중요도는 3대 분야별 각각의 상위정책의 중요도 합이 1이 되도록 계산한 것이다.

〔표 7〕에서 주목할 점은 2008년에서는 전문가 집단에서 개인정보의 침해 대응적 측면에서 '개인정보 침해 구제' 방안이 매우 중요하였으나, 2009년에는 그 중요도가 가장 낮아졌다는 점이다. 즉, 1 년의 기간 동안, 개인정보 침해 대응이라는 관점에서는 사후적 침해 구제보다 이와 같은 일이 발생하지 않도록 미리 사전에 방지하는 것이 침해대응 측면에서 더 중요하다고 보는 변화가 있었다. 2009년 기준으로 전문가집단은 정책·기술적 측면에서 제도적 기반을 마련하고(0.5448), 처리단계의 관리적 측면에서 개인정보의 수집 및 보유(0.4664)시 안전한 관리방안 등이 확립되어야 한다고 보았다. 또한, 개인정보침해대응에서 웹사이트 개인정보 노출방지(0.5257) 등 사전적 대응의 중요성이 매우 강조되었음을 볼 수 있다.

〔표 7〕에서 실무자집단의 견해를 비교를 살펴보면, 정책·기술적 측면에서의 제도적인 정책 기반이 가장 우선되어야 할 정책으로 보았으며 그 중요도는 2009년에 더욱 증가하였다. 그 외에 처리단계의 관리적 측면에서 개인정보의 수집 및 보유시 안전한 개인정보보호환경이 구현되어야 하며, 개인정보 침해대응적 측면에서는 웹사이트 상에서의 개인정보가 노출되지 않도록 방지하여야 한다고 하였다. 종합적으로 실무자의 의견은 2008년과 2009년에 큰 차이는 없었다.

이상으로 중위지표에 대한 중요도 의견들을 종합하여 보면, 가장 큰 차이는 개인정보보호의 침해대응적 측면에 있다. 즉, 학자 등 전문가 집단은 '개인정보침해 구제의 중요성'을 실무자 집단은 '웹사이트 개인정보 노출 방지'를 중요한 정책 방향으로 본다는 점이다. 물론, 2009년에 전문가의 의견 역시 실무자 의견과 비슷하게 변화가 있었지만, 중요도 간에 약간의 간극은 계속 존재한다. 결론적으로 이러한 전문가들의 의견은 각 공공기관에서 개인정보보호에 관한 정책을 수립하는 단계에서 기틀을 마련하는 데 있어 중요한 고려사항이라고 볼 수 있으며, 앞으로 개인정보보호에 관한 인식을 높이는 데 중요한 기본적인 정책들이 되리라 본다. 즉, 별도의 독립된 개인정보보호 부서에서 개인정보를 처리하여야 하며, 개인정보를 수집할 때 정보주체에게 개인정보의 수집 목적, 근거, 용도 등에 관한 명확한 지침을 마련되어야 하며, 무엇보다도 웹사이트 상에서 개인정보가 노출되지 않도록 철저한 관리하는 방안이 수립되어야 할 것이다.

V. 결론 및 시사점

본 연구에서는 공공분야에서 개인정보가 안전하게 관리되고 보호받을 수 있는 방안을 마련하기 위해 우선적으로 추진되어야 할 정책과제를 다루었다. 이를 위하여 개인정보를 크게 개인정보보호의 정책적·기술적 측면, 처리단계별 개인정보 관리, 개인정보 침해대응적 측면으로 3개 상위지표를 구성하였으며, 각 정책분야의 상위정책 범주에 따라 세부정책들을 구분하여 AHP 방법으로 정책의 중요도 순위를 정하였다. 2009년 AHP 결과, 개인정보보호의 정책·기술적 측면, 개인정보 침해대응적 측면, 처리단계의 관리적 측면 순으로 중요하다고 응답하였다.

개인정보보호 정책의 우선순위를 AHP 방법을 사용할 때 각 정책 간 엄밀한 독립성이 있어야 하나, 사실 중복되는 진단항목이 발생하기도 한다. 예를 들어, 개인정보의 파기절차를 마련하기 위해 계획을 수립할 경우, 이는 개인정보의 관리적 측면에 포함되지만, 이러한 계획 수립은 개인정보보호의 정책 기반에도 포함되어 이중으로 중복 평가된다. 즉, 하나의 정책이 여러 부분에서 세부적인 중첩이 발생하고 있어, 하위지표의 추진방안들이 명확히 적용되지 않으면 정책의 일관성을 확보하지 못하게 된다. 그러므로 세부적인 실행단계를 추진함에 있어서 세부 추진과정의 중복지표를 배제하는 연구 및 해당 정책 개발이 보다 면밀하게 다루어져야 한다. 그런데, 본 연구에서는 하위단의 여러 정책과제를 서로 비교하지 못하였는데 이러한 점은 본 연구의 한계점이라 하겠다.

또한, 개인정보보호에 관한 정책분야를 구분함에 있어 제시한 개인정보보호의 정책적·기술적 측면, 처리단계의 관리적 측면, 개인정보의 침해대응적 측면을 동등한 범주로 비교한 것은 문제가 있을 수 있다. 사실 이들은 동등한 범주이기 보다는 프로세스 과정으로 이해될 수 있기 때문이다. 즉, 어느 하나의 단계가 완성되면 자동적으로 다음 단계가 동반 상승할 수 있는 여지가 있다. 그러므로 정책들 간의 연계성을 고려하는 문제를 고찰하여야 한다. 사실, 이와 같은 이유로 2011년 중요도는 대산 집단을 가군, 나군, 다군으로 구분하여 정책의 우선순위에 변화를 두었는데 이는 정책들의 연계성을 고려하기 위함이다. 끝으로 본 연구가 AHP기법을 사용하여 개인정보보호정책을 비교함에 있어, 그동안 제기되었던 모든 가능한 정책을 범주화하여 비교하지 못한 한계가 있다. 향후, 지속적인 정보통신기술의 변화에 따라 대응되는 정책요소들은 앞으로도 보완되어야 할 필요가 있을 것이다.

결론적으로 본 연구는 개인정보보호를 위한 정책을 추진하기 위하여 어떤 정책을 우선적으로 추구하는 것이 바람직한가를 다룬 것으로, 정책분야를 임의로 나누어 중복되거나 대표성이 부족하다는 한계에도 불구하고 개인정보보호를 강화하기 위한 종합적인 시각에서 접근하였다는 점에 연구 의의를 두고자 한다. 사실 공공기관에서 개인정보를 이용한 정부업무의 추진과정이 불가피한 수단으로 인식되고 있으므로, 개인정보보호를 위한 정책적인 방향이 공공기관에 반드시 제시되어야 할 것이다. 즉, '공공기관의 개인정보보호 수준진단'은 공공기관이 개인정보의 관리방안을 마련하고 안전한 개인정보보호의 기틀을 만드는 기반이 되리라 생각한다. 이러한 개인정보보호 수준진단을 통해 각 기관의 개인정보보호 수준이 향상될 것이며, 궁극적으로는 개인정보보호의 보호주체인 국민의 신뢰를 받을 수 있을 것이다.

참고문헌

〔1〕 권헌영, "전자정부시대의 개인정보보호법제의 쟁점", 정보화정책, 11(3), pp.55-78, 2004년 9월.

〔2〕 김민기, "초등학교 홈페이지에서의 불건전 정보 유통 및 개인정보 노출 실태 분석", 한국정보교육학회 논문지, 8(4), pp.489-500, 2004년 12월.

〔3〕 김민호, "공공부문 개인정보보호법제의 현황과 과제", 토지공법연구, 37(1), pp. 207-223, 2007년 8월.

〔4〕 문신용, 윤기찬, "공공기관의 개인정보침해사례 분석의 함의 및 과제", 한국행정연구, 2004년 12월.

〔5〕 박홍윤, "공공기관에서 개인정보의 이용과 통제-컴퓨터 프로필링 기법을 중심으로-", 한국사회와 행정연구, 13(2), pp. 89-113, 2002년 8월.

〔6〕 변미리, "서울시 전자정부의 개인정보보호에 관한 연구", 서울: 서울시정개발연구원, 2004년 7월.

〔7〕 송유진 외, "개인정보 라이프사이클에 따른 프라이버시 보호 프레임워크", 정보보호학회지, 2006년.

〔8〕 성도경, 장철영, "AHP 기법을 이용한 전자정부 구현전략의 우선순위 결정에 관한 연구", 한국행정논집, 14(2), pp. 353-372, 2002년 6월.

〔9〕 신영진, "공공기관의 개인정보보호에 관한 효율성 분석", 한국지방자치학회보, 18(1), pp. 87-106, 2006년 3월.

〔10〕 신영진, "우리나라 개인정보보호수준의 개선방안

에 관한 연구", 정보화정책, 16(1), pp. 41-53, 2009년 3월.
〔11〕 오태원, "RFID에 관한 법정책적 연구", 인터넷법률, 제35호, pp. 96-126, 2006년 5월.
〔12〕 윤취영, "개인정보화수준 및 성숙도 진단을 위한 통합평가시스템 개발에 관한 연구", 연세대학교, 2003년 8월.
〔13〕 이종찬, "AHP의 통계적 성질에 관한 연구", 박사학위논문, 고려대학교, 2012년 2월.
〔14〕 임영덕, "유비쿼터스 컴퓨팅에서의 개인정보보호", 성균관대 대학원, 2005년 8월.
〔15〕 임종인 외, "개인정보보호를 위한 기술개발 및 기술정책에 관한 연구", 한국전산원, 2004년 9월.
〔16〕 임종인, "행정기관 정보보호 현황 및 과제: 정보보호, 지역정보화", 지역정보화지, 2006년 9월.
〔17〕 장태수, "국가·공공기관 전자적 침해사고 대응현황", 제8회 개인정보보호심포지엄 SIS 2003 발표집, 서울: 한국정보보호진흥원. 2003년 7월.
〔18〕 정보통신부, "안전한 u-Korea 구현을 위한 정보보호 중장기 로드맵", 2005년 4월.
〔19〕 정보통신부, "개인정보보호지침", 2005년 10월.
〔20〕 정형철, "개인정보보호 수준진단 지표의 중요도에 대한 AHP 및 비모수 검정 연구", Journal of the Korean Data Analysis Society, 12(3), pp.1499-1510, 2010년 6월.
〔21〕 행정안전부, 한국정보보호진흥원, "공공기관 개인정보보호 수준진단 프로그램 적용 및 확산", 2008년 12월.
〔22〕 행정자치부, 한국지역정보개발원, "개인정보보호 수준측정 지표개발최종보고서", 2007년 12월.
〔23〕 행정안전부, "공공기관 개인정보관리업무매뉴얼", 서울 : 행정안전부, 2008년 4월.
〔24〕 행정안전부, "공공기관의 CCTV설치 및 운영에 관한 지침", 2006년 8월; "공공기관 CCTV관리가이드라인", 2009년 9월; "표준 개인정보보호지침", 2011년 9월.
〔25〕 행정안전부, "개인정보보호를 위한 기술적 · 물리적 보호조치", 2009년 11월; "개인정보의 안전성 확보조치 기준 고시 및 해설서", 2011년 9월.

〈著者紹介〉

신 영 진 (Young-Jin Shin) 정회원
2004년 2월: 성균관대학교 행정학과 행정학박사
2004년 10월~현재: 행정안전부 전문위원
〈관심분야〉 전자정부, 정보보호, 개인정보보호, 미래예측

정 형 철 (Hyeong-Chul Jeong) 정회원
1989년 2월: 고려대학교 통계학과 졸업
1991년 2월: 고려대학교 통계학과 이학석사
1997년 8월: 고려대학교 통계학과 이학박사
2005년 3월~현재: 수원대학교 통계정보학과 부교수
〈관심분야〉 데이터마이닝, AHP, 개인정보보호, 정보보호 위험도 예측

강 원 영 (Won-Young Kang) 정회원
2000년 8월: 고려대학교 행정학과 행정학석사
2000년 9월~현재: 한국인터넷진흥원 책임연구원
〈관심분야〉 개인정보보호, 인터넷, 정보보호 정책