개인정보의 안전성 확보조치 기준에서의 우선순위 정립에 관한 연구

김영희* · 국광호**

요 약

정보화 및 인터넷의 급속한 발전에 따라 개인정보를 취급하는 기업에서 개인정보의 안전한 취급·관리를 위한 조치를 취하지 않아 개인정보가 유출되고 오·남용되는 사례가 빈번히 발생하고 있다. 이에 국내에서는 개인정보주체의 프라이버시 보호와 피해를 줄이기 위해 개인정보보호 관련 법제를 강화하고 관련 법제를 바탕으로 개인정보처리자가 개인정보를 보호하기 위한 안전성 확보조치 기준을 마련하고 따르도록 하고 있다. 그러나 개인정보의 안전성 확보조치 기준항목의 경우 각 개인정보 처리 기업의 특성 및 항목별 중요도에 따른 우선 적용 기준 등이 고려되지 않아 이행에 어려움이 따르고 있다. 따라서 본 연구에서는 개인정보의 안전성 확보조치 기준들의 세부적인 사항들을 기존 문헌 연구와 관련 법률을 통해 평가 기준을 도출하고, 평가 기준의 정량화 및 계층화를 위해 KJ (Kawakita Jiro) 기법을 이용하여 유사기준 항목의 통합 및 그룹화를 하여 계층구조를 생성한다. 이렇게 생성된 계층 구조를 AHP (Analytical Hierarchy Process) 기법을 이용해 전문가 대상으로 가중치 산정하여 기업에서 보다 합리적이고 효율적인 개인정보보호를 위한 우선순위 제안을 목적으로 한다.

A Study on Priority Rankings of Actions Providing Personal Information Security

Young Hee Kim* · Kwang Ho Kook**

ABSTRACT

With the rapid development of the Internet and information technology, a company that deals with personal information does not have proper action to protect personal privacy and not take measures for the safe handling and management of personal information. It generates the case to abuse of personal information occurring frequently. In order to focus the effort to reduce damage and protect the privacy of personal information entity and enhance privacy laws based on the connection method and the processing of personal information, Korea encourages a company to follow regulation by providing certain criteria. However, in the case of items of measures standard of safety of personal information such as priority applicable criteria in accordance with the importance of itemized characteristics and the company of each individual information processing is not taken into account, and there are some difficulties to execute. Therefore, we derive criteria by law and reviewing existing literature related, the details of the measures standard of safety of personal information in this study and generate a hierarchical structure by using the KJ method for layering and quantification of the evaluation in integration of the reference item similar and the grouping. Accordingly, the weights calculated experts subject using the AHP method hierarchical structures generated in this manner, it is an object of the proposed priority for privacy and efficient more rational enterprise.

Key words : Personal Information Protection, KJ, AHP, Information Security

접수일(2014년 5월 20일), 수정일(1차: 2014년 6월 18일), 게재확정일(2014년 6월 24일)

* 서울과학기술대학교 IT정책전문대학원 산업정보시스템공학전공

** 서울과학기술대학교 기술경영융합대학 글로벌융합산업공학과 (교신저자)

1. 서 론

정보화 및 인터넷의 급속한 발전에 따라 사이버 위협과 해킹, 정보의 무분별한 유통 등의 정보보호의 역기능을 초래하게 되었다. 이로 인해 기업의 개인정보 유출 및 업무연속성 침해에 따른 금전적 손실이 증가되고 있다[1]. 이에 개인정보취급 기업에서는 개인정보보호를 위한 관리적·기술적 보호조치 기준을 갖추기 위해「개인정보보호법」제24조 제3항 및 제29조와 같은 법 시행령 제21조 및 제30조 따른 개인정보의 안전성 확보조치 기준고시를 활용하고 있다. 개인정보의 안전성 확보조치 기준고시의 주요 목적은 법에서 명시한 것처럼 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·변조·훼손되지 아니하도록 안전성을 확보하기 위하여 취하여야 하는 세부적인 기준을 정하는 것으로 개인정보 처리 기업 및 처리자가 개인정보를 취급함에 있어 명확하게 지켜야 할 기술적·관리적 세부 기준을 구체적이고 명확하게 제시하고 준수하도록 하고 있다[2]. 그러나 기존의 개인정보를 처리하고 관리하기 위한 법률 및 시행령에 따른 개인정보의 안전성 확보에 필요한 최소한의 기술적·관리적 보호조치 기준을 개인정보처리 기업에서 적용하기에는 각 기준별 시급성, 중요성 및 대상 기업의 환경에 따른 방안이 고려되지 않아 이행에 어려움이 따르고 있다. 이는 각 기준 별 일치된 개념이 존재하기 않고 각 기준에 대해 계량적으로 수치화하여 우선순위를 가리기 어렵기 때문이다.

따라서 이번 연구에서는 개인정보의 안전성 확보조치 기준고시 중 개인정보의 안전한 보호에 필요한 기술적·관리적 조치 기준인 3조에서 10조를 활용하여 관련 조와 각 세부 항에 대해, 개인정보보호전문가를 통한 개인정보의 안전성 확보조치 기준별 가중치를 측정해 상대적으로 중요한 항목을 도출하고, 이를 통해 기업에서 우선 적용되어야 하는 기준을 산정, 정량화 하고자 한다.

2. 관련 연구

개인정보를 취급하는 기업에서 개인정보의 안전한 취급관리를 위한 관리적·기술적 조치를 취하지 않아 개인정보가 유출되고 오·남용되는 사례가 자주 발생하고 있으며, 사회적으로 심각한 문제로 대두되고 있다[3]. 이와 함께 e비즈니스 환경에서 경제주체의 활동이 개인정보를 매개로 하여 유지·운영되고 있어 개인정보가 기업의 자산 및 상업적 가치를 지니게 되었다. 이로 인해 개인정보를 취급하는 공공기관 및 기업에서 개인정보의 관리적·기술적·물리적 보호조치에 많은 노력을 취하고 있으며, 개인정보보호 조치 강화를 위한 보다 강력한 법률 및 제도도 함께 연구되고 등장하고 있다[4].

2.1 개인정보보호 관련 법 규정

개인정보보호 법률 및 규정은 개인정보의 유출·남용으로부터 개인의 인격주체성을 보호함으로써 개인의 존엄성과 가치를 보호 하고 더 나아가 국민의 권리와 이익 증진을 위함에 있다[5]. 이에 따라 개인정보를 취급하는 기업에서는 개인정보의 생명주기 영역 등에 대한 보호 범위의 수립, 고유식별정보 처리의 제한, 개인정보 수집·이용 제공 기준 확립 및 안전한 처리를 위한 조치 및 관리·감독 등을 준수 하여야 한다.

선진 각국은 1970년대부터 정보통신망에서 처리되는 개인정보의 보호를 위하여 개인정보 주체자의 사생활 보호에 관한 입법조치 등 각국의 실정에 맞는 법·규정을 제정하고 개인정보의 보호 및 문제를 해결하고 있다. 하지만 1980년 이후 정보통신망의 발전에 따른 국가 간의 정보가 유통되고, 국제정보은행이 출현함에 따라 각국은 상이한 법률 간의 조화유지의 필요성과 개인정보보호 및 정보의 자유유통 및 안전한 이용에 관한 균형의 필요성이 대두 되었다. 이러한 흐름에 따라 각국은 개인정보보호 정책에 대한 각 국가 간의 편차에 따른 프라이버시가 침해되고 소홀히 관리되지 않도록 국제적 통일된 기준을 마련하거나 국제협력을 강화하려는 노력이 이뤄지고 있다[6][7].

우리나라의 개인정보보호 관련 법제는 대상의 형태에 따라 민간부분과 공공부분의 형태로 이원화된 구조였다. 민간부분은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 과 「신용정보의 이용 및 보호에 관한 법률, 공공부문은 「공공기관의 개인정보보호에 관한 법률」에 의해 관할되었으며 타 주요사업자에 대한

법률도 따로 존재하고 있어 개인정보를 통합적으로 관리하고 적용하는데 한계를 드러냈다.

이러한 상황에 개인정보 침해사고 및 대규모 개인정보 유출 사고의 증가로 개인의 주체성 침해와 불안감이 급증하고 있어 전체를 통합하고 관할 할 수 있는 법률에 대한 필요성 및 법 적용의 사각지대 해소의 요구가 증대되었다. 이에 2011년 3월 29일 일반법 형태의「개인정보보호법」이 제정되고, 동법 시행령과 시행규칙이 2011년 9월 29일 제정되어 2011년 9월 30일자로 전면 시행되었다[8].

<표 1> 국내·외 개인정보보호에 관한 법률 [6][7]

국가	관련 법률
한국	• 개인정보보호법(2011.3.29. 법률 제11690호) • 공공기관의 개인정보보호에 관한 법률 (1994.1.7., 법률 제4734호) • 신용정보의 이용 및 보호에 관한 법률 (1995.1.5., 법률 제4866호) • 정보통신망이용촉진 및 정보보호에 관한 법률 (2001. 1. 16, 법률 제6360호) • 위치정보의 이용 및 보호 등에 관한 법률 (2005.1.27., 법률7372호)
미국	• 정보공개법(Freedom of Information Act, 1974) • 프라이버시보호법(Privacy Protection Act, 1980,미국) • 컴퓨터에 의한 정보조합과 프라이버시보호에 관한 법률(Computer Matching and Privacy Protection Act,1988,) • 전자정부법(E-Government Act, 2002) • 금융프라이버시권에 관한 법률 (Right to Fianancial Privacy Act, 1978) • 금융현대화법(The Financial Services Modernization Act, 1999)
유럽	• 정보보호법(Data Protection Act,1998,영국) • 정보처리파일 및 자유에 관한법률(1978,프랑스) • 연방정보보호법(1974,독일) • 개인정보법(Personal Data Act,1998,스웨덴)
일본	• 개인정보보호에 관한 법률(2003,일본)

2.2. 개인정보의 안전성 확보 기준

국내에서는 개인정보주체의 프라이버시 보호와 피해를 줄이기 위해 개인정보보호 관련 법제를 강화하고 관련 법제를 바탕으로 개인정보를 보호하기 위한 안전성 확보조치 기준을 마련하고 강화하고 있다[14].

현재 시행되고 있는 개인정보보호의 안전성 확보조치 관련 사항은 「개인정보보호법」 및「정보통신망법」에서 세부적으로 정의 하고 있으며, 개인정보의 안전한 보호를 위해 준수해야 할 관리적·기술적 조치사항을 공공, 민간 부분 등 개인정보 취급자 대상으로 지켜야할 세부적인 법률적 요건을 상세하게 정의 하고 있다.

관련 법률에서는 개인정보보호 내용은 개인정보 대량 유출사고의 방지 및 2차 피해 예방을 위해 개인정보처리 기업의 개인정보 보호체계 강화 및 이용자 자신의 개인정보 주체 강화를 목적으로 하며 개인의 존엄과 가치를 구현하기 위하여 개인정보 처리에 관한 사항을 규정함을 목적으로 한다.

<표 2>개인정보의 안전성 확보 주요 내용

구분	주요내용
근거	▶「개인정보보호법」 및 시행령
세부 규정	▶개인정보의 처리 (법 제15조 에서 제22조) ▶민감정보 및 고유식별정보의 범위 제한 및 보호범위(법 제23조 제24조) ▶개인정보의 안전성 확보조치(법 제29조) • 이용자 개인정보의 안전한 취급을 위한 내부관리 계획의 수립·시행의 보호 조치 • 이용자 개인정보에 대한 불법적인 접근을 차단하기 위한 접근통제 규칙, 침입차단시스템 및 침입탐지시스템 설치·운영 등 보호조치 • 개인정보취급자의 개인정보취급시스템에 대한 접속기록의 위조·변조 방지를 위한 보호조치 • 이용자의 개인정보가 안전하게 저장. 전송될 수 있도록 보호조치 • 악성 프로그램의 침투 여부를 항시 점검. 치료할 수 있는 백신소프트웨어의 설치. 운영 등 보안 조치 • 개인정보 유출 시 신고 및 통지(법 제34조)
성격	반드시 준수해야 하는 최소한의 기준
강제 여부	▶3~5천만 원 이하의 과태료 ▶2년 이하의 징역 또는 1천만 원 이하의 벌금

3. 우선순위 체계 제안

본 연구에서는 개인정보보호의 안전성 확보조치 기준별 가중치 산정을 위한 항목 도출을 위하여 「개인

정보보호법」 및 동법 시행령에 따른 개인정보의 안전성 확보조치 기준을 조사하였으며 관련 기준을 토대로 전문가 집단을 통한 기준별 평가항목을 도출하고, APH 기법을 통해 개인정보의 안전성 확보조치 기준에 대한 가중치를 산정하여 평가한다.

먼저 기준별 평가항목 설정을 위해 개인정보의 안전성 확보조치 시행에 관한 법률·규제·규정에서 정의한 평가항목을 도출하였으며, 평가항목을 대상으로 개인정보보호 컨설팅 전문가 및 실무 보안 전문가 집단을 대상으로 KJ(Kawakita Jiro) 기법을 통해 평가항목을 정제화 하고 계층화·구조화 하였다. 마지막으로 AHP(Analytical Hierarchy Process) 기법을 통해 개인정보의 안전성 확보조치 기준 평가항목별 가중치를 산출한다.

3.1 평가 기준

개인정보의 안전성 확보조치 시행에 관한 법률·규제·규정에서 정의한 평가항목 도출을 위해 「개인정보보호법」에서 정의한 개인정보처리자가 개인정보의 안전성 확보를 위해 이행해야 할 기술적·관리적·물리적 보호조치 세부기준 제시를 위해 「개인정보보호법 제24조 제3항 및 제29조와 같은 법 시행령 제21조 및 제30조」에 따라 개인정보처리자가 개인정보를 처리함에 있어서 개인정보의 분실·도난·유출·변조·훼손되지 아니하도록 안전성을 확보하기 위하여 취하여야 하는 세부적인 기준인 개인정보의 안전성 확보조치 기준 고시 3조에서 10조를 활용해 평가 기준을 정한다[2].

<표 3> 개인정보의 안전성 확보 기준

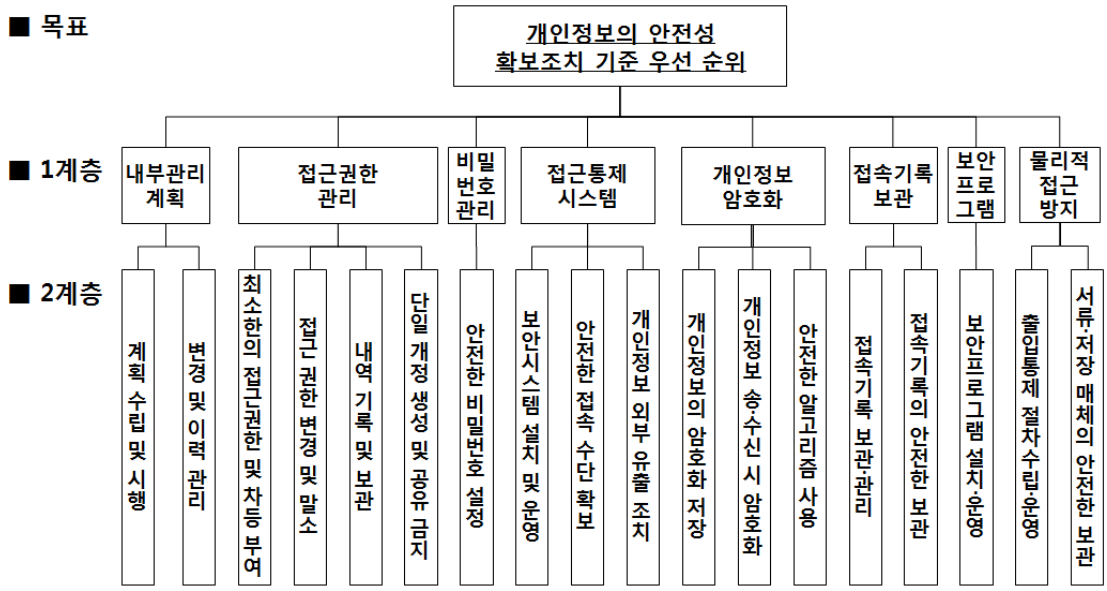
항목(1계층)	세부항목(2계층)
내부관리 계획의 수립·시행	계획 수립 및 시행
	소상공인 계획 수립 관련 예외 사항
	변경 및 이력 관리
접근권한 관리	최소한의 접근권한 및 차등 부여
	접근권한 변경 및 말소
	내역 기록 및 보관
	단일 계정 생성 및 공유 금지
비밀번호 관리	안전한 비밀번호 설정
접근통제 시스템 설치 및 운영	보안시스템 설치 및 운영
	안전한 접속 수단 확보
	개인정보의 외부 유출 조치
	운영체제 및 보안프로그램 접근 통제
개인정보의 암호화	개인정보의 암호화 저장
	개인정보 송·수신 시 암호화
	일방향 암호화
	고유식별정보의 인터넷구간·DMZ 저장 시 암호화
	고유식별정보의 내부망·업무용컴퓨터 저장 시 암호화
	안전한 알고리즘 사용
	인터넷구간·DMZ 저장 시 암호화
	안전한 알고리즘 사용
접속기록의 보관 및 위·변조 방지	접속기록의 보관 및 관리
	접속 기록의 안전한 보관
보안프로그램 설치 및 운영	보안프로그램 운영
물리적 접근 방지	출입통제 절차 수립·운영
	서류·저장 매체의 안전한 보관

3.2 계층 구조

본 연구에서는 평가항목을 정제화 하고 계층 모형을 만들기 위해 <표 3>에서 도출한 1계층 8개, 2계층 25개의 주요 평가 기준을 대상으로 관련 전문가 집단을 대상으로, KJ 기법을 이용해 개인정보의 안전성 확보조치 기준 평가항목 중 표준 평가항목으로 사용가능한지 여부와 그룹화 등을 결정하였다. 이를 위해 개인정보보호 전문가 7명을 대상으로 KJ 기법을 활용하여 아이디어(평가항목)를 그룹화 하고 제목을 작성 하였다.

KJ 기법은 평가 요소를 수집하고 전문가 집단을 통해 복잡한 현상을 그룹화하고 이해하는데 복잡한 통계방법을 사용하지 않고도 간단히 객관적으로 평가요소들을 요약 할 수 있는 수단으로서 이용할 수 있어 개인정보의 안전성 확보를 위한 평가항목의 정제화 및 계층화를 통한 구조화에 적합한 기법이라고 할 수 있다.[15].

KJ 기법을 이용하여 정제된 개인정보의 안전성 확보조치 기준별 우선순위를 위한 계층구조를 살펴보면 크게 다음과 같이 3개의 계층으로 구성하였다. 먼저 AHP 의사 결정을 위한 목표(Goal)로 개인정보의 안전성 확보조치 기준으로 설정되었고 주 기준으로 개인정보보호 안전성 확보조치 기준에서 정의하는 필수 의무사항 및 대표성을 띄면서 중복성이 존재하지 않는 8개 항목에 대해서 항목명을 간소화하여 내부관리



(그림 1) 계층 구조

계획, 접근권한 관리, 비밀번호 관리, 접근통제 시스템 설치 및 운영, 개인정보의 암호화, 접속기록의 보관 및 위·변조방지, 보안프로그램 설치 및 운영, 물리적 접근 방지 항목과 각 주 기준에 대한 세부 항목으로 정제되어 정의 하였다.

4. 가중치 분석

본 연구는 KJ 기법을 통해 정량화 되고 계층화된 계층도에 대해 AHP 평가 설문을 통해 평가항목에 대한 가중치와 우선순위를 도출 하였다.

AHP 기법의 계층적 분해를 통해 의사결정 요소들 간의 논리적이고 유기적 관계를 계층적으로 모델화 하고 파악함으로 써 수많은 평가 요소들의 다양하고 복잡한 문제에 대해서도 체계적 분석이 가능하다[9].

이는 의사결정이 필요한 복잡한 문제를 동일 그룹으로 분류하고 세분화한 계층 구조를 생성하고 평가요소들 간의 쌍대비교(Pair-wise Comparison)를 통해 각 요소들 간의 가중치를 산출하고 일관성을 검증을 통해 논리적인 오류를 찾아 집단적인 의사 결정을 가능하게 한다[10][11].

4.1 우선순위 기준 가중치 분석

가중치 분석을 위해 먼저 쌍대비교를 위한 평가 기준은 그림 1 에서 도출한 평가기준 항목의 중요도에 대해 9점 척도를 사용하여 평가 하였다.

요소 및 대안들을 쌍대 비교하는 방법은 A와 B중에 중요도를 가리는 질문하게 되는데 이때 사용되는 척도는 9점 척도를 기본형으로 이용하였다.

<표 4> 쌍대비교의 선호도 측정치 값

값	설명
1	대안 A가 대안 B의 선호도가 동일함
3	대안 A가 B보다 약간 중요함
5	대안 A가 B보다 중요함
7	대안 A가 B보다 매우 중요함
9	대안 A가 B보다 절대적으로 중요함
2,4,6,8	1,3,5,7,9의 중간 값
위 척도의 역수	대안 B가 대안 A보다 중요할 경우 사용

AHP 쌍대비교 기준 수치에 따라 쌍대비교 값을 집계하고, 중요도 척도에 의해 i안이 5점을 받았다면 반대편의 쌍대비교 값 j안은 1/5값으로 표현하면 된다. 이렇게 행렬 값이 구해지면, 열 합계를 구한다. 이후 표준화(Normalize)행렬을 구하면 되는데, 앞서 구했던

행렬 값을 각각 열 합계로 나누어 구한 뒤 행 합계를 구한다. 다시 행렬 값과 행 합계로 행렬계산을 하게 되면 가중치 곱을 구할 수 있게 된다[12].

AHP 계층 모형을 토대로 전문가 평가를 위한 간격척도 방식의 설문지를 작성 하여, 의견 취합 후 기하평균을 이용하여 여러 전문가가 집단으로 참여하여 의사결정한 개인적인 의견을 종합 하였다.

본 연구에서는 개인정보보호전문가를 대상으로 30명 미만을 대상으로 설문을 실행하였다. 또한 AHP 설문에서 중요한 부분인 쌍대비교를 통해 도출된 가중치가 논리적인 오류가 없고 일관성이 있는지 확인하기 위해 일관성 비율 (CR. Consistency Ratio)을 계산하였다. 의사결정자의 판단이 논리적으로 일관성을 유지하고 있는지에 대한 여부를 확인하게 되는데, 이를 위해 T.L Satty 가 제안한 고유벡터를 이용하여 가중치의 추정한다. 계층 내 평가 요소간의 상대적인 중요도는 합이 1인 가중치로 일반적으로 나타내다. 이처럼 요소가 n개 가 있는 경우 아래와 같은 벡터 형태로 표현 한다.

$$W^T = (w_1, w_2, \cdots w_n), w_i \geq 0 \qquad (1)$$

$$\sum_{j=1}^{n} w_j = 1$$

그리고 가중치 벡터 W 는 다음과 같이 고유치 문제를 풀어 도출해 낼 수 있다. λ_{max}는 고유치 중 가장 큰 수치로 이에 대응되는 고유벡터가 가중치 벡터 W가 된다, 이때 A는 쌍대행렬이다.

$$A\,W = \lambda_{max}\,W \qquad (2)$$

일관성 지수(ConsistencyIndex:CI)와 일관성 비율(ConsistencyRatio:CR)은 아래 식을 통하여 구할 수 있으며, max는 항상 n보다 같거나 크기 때문에 계산된 max 가 n에 가까울수록 쌍태비교 행렬 A의 수치들이 논리적으로 오류가 없이 일관성을 가진다고 할 수 있다.

일관성 지수 = $$CI = \frac{\lambda_{max-n}}{n-1} \qquad (3)$$

일관성 비율 = $$CR = \frac{CI}{RI} \times 100 \qquad (4)$$

다시 말해 CI는 일관성 지수를 나타내며 값이 0에 가까울수록 일관성이 크다고 말할 수 있다. RI (Random Index)는 CI들의 평균값을 말하여 1에서 9사이의 난수를 이용하여 구성한 비교행렬을 나타낸다.

일관성 지수의 경우 0.1 이상의 경우 의사결정자의 판단에 논리적 오유가 존재하고 일관성이 결여 되었다고 판단하므로 실제 AHP 기법을 활용하기 위해서는 일관성 지수가 0.1 이하가 되어야 한다.

산정된 일관성 비율이 0.1 미만인 설문은 논리적이고 합리적으로 평가되었다고 판단하여 분석 대상으로 선정하였고 일관성 비율이 0.1 이상인 경우는 논리적인 오류가 존재하는 비합리적이라 설문이라 판단하고 분석 대상에서 제외하였다.

AHP 기법은 평가가 필요한 문제에 있어서 전문적 경험과 관련 지식이 풍부한 집단이 선발된 경우에는 그 평가 집단이 성향과 특성이 동질적이면 그 규모는 10명에서 15명이면 설문을 평가하는데 충분하다 라고 말하고 있다[13].

이에 따라 최종적으로 논리적인 오류가 없다고 판단되고 일관성 비율이 0.1 이하인 10개의 설문에 대해 가중치를 도출하고 평가 하였다

<표 5> 쌍대비교의 선호도 측정치 값

평가자	일관성 지수 CI	일관성 비율 CR
1	0.137	0.097
2	0.131	0.093
3	0.017	0.012
4	0.118	0.084
5	0.032	0.023
6	0.135	0.096
7	0.14	0.1
8	0.012	0.009
9	0.056	0.04
10	0.119	0.085

4.2 우선순위 기준 가중치 평가 결과

개인정보의 안전성 확보조치 기준 영역 내 1계층의 평가항목 8개 영역에 대해 10명의 전문가 응답한 설문을 쌍대비교한 결과를 이용하여 개인정보 안전성 확보조치 기준항목에 대한 각각의 가중치를 산정하였으며,

다수의 전문가 판단을 취합하는 방법은 Satty의 연구에서 제시한 것처럼 동의를 구하여 단일의 중요도를 산출하는 방법과 개별적으로 중요도를 평가한 후 통합하는 하는 2가지 방법 중 본 연구에서는 다수의 전문가 판단을 통합하기 위해 행렬의 역수성 유지에 적합한 기하평균(geometric mean)을 활용하여 10명의 전문가 집단의 가중치를 산정하였다[10].

<표 6> 최종 평가항목 가중치

항목	가중치	하위평가기준	가중치
내부관리계획	0.145	계획 수립 및 시행	0.658
		변경 및 이력 관리	0.342
접근권한관리	0.174	최소한의 접근권한 및 차등 부여	0.356
		접근권한 변경 및 말소	0.307
		내역 기록 및 보관	0.106
		단일 개정 생성 및 공유 금지	0.232
비밀번호관리	0.126	안전한 비밀번호설정	1.000
접근통제시스템설치및운영	0.122	보안시스템 설치 및 운영	0.320
		안전한 접속 수단 확보	0.299
		개인정보의 외부 유출 조치	0.381
개인정보의암호화	0.181	개인정보의 암호화 저장	0.402
		개인정보 송·수신 시 암호화	0.296
		안전한 알고리즘 사용	0.302
접속기록의보관및위조변조방지	0.066	접속기록의 보관 및 관리	0.525
		접속 기록의 안전한 보관	0.475
보안프로그램설치운영	0.090	보안프로그램 운영	1.000
물리적접근방지	0.097	출입통제 절차 수립·운영	0.490
		서류·저장 매체의 안전한 보관	0.510

개인정보의 안전한 보호를 위한 기준별 우선순위를 비교 분석해 보았다. 먼저 1계층을 비교해 본 결과 개인정보의 암호화(0.181) 기준항목이 접속기록의 보관 및 위·변조방지(0.066) 기준항목 보다 훨씬 더 우선순위가 높고 중요한 항목이라고 전문가들은 판단하고 있다. 다시 말해, 개인정보보호를 위한 관리적 기술적 조치 사항들 중 개인정보처리시스템에서의 고유식별 정보를 포함한 개인정보의 외부 유출에 대한 보안 조치 항목인 개인정보의 암호화에 대한 기준항목이 기록에 대한 로깅 및 관리에 관한 기준항목 보다는 개인정보보호를 위해 선 조치되어야 할 중요한 기준항목이라고 전문가들은 판단하고 하고 있으며 이를 바탕으로 각각의 기준항목들 중에서도 시급하게 적용되어야 되는 기준 항목이 존재하는 것으로 판단된다.

2계층에서는 각 항목별 가중치를 평가하여 우선순위 항목을 최종 평가 하였다.

종합하면 개인정보의 안전성 확보조치 기준별 상위 항목의 우선순위는 개인정보의 암호화(1위 0.181), 접근권한 관리(2위 0.174), 내부관리 계획(3위 0.145), 비밀번호 관리(4위 0.126), 접근통제시스템 설치 및 운영(5위 0.122), 보안프로그램 설치 및 운영(6위 0.090), 물리적 접근 방지(7위 0.097), 접속기록 보관 및 변조방지(8위 0.066)순으로 개인정보의 안전성 확보를 위해 기술적·관리적 조치 사항 별 우선순위가 제안 되었다.

5. 결 론

본 연구에서는 기존에 동일하게 요구되는 개인정보의 안전성 확보조치 기준에 대해 전문가를 대상으로 실제 개인정보 처리 기업에서 개인정보보호를 위해 보다 시급하고 중점적으로 적용하고 관리되어야 할 조치 기준을 확인하고 도출하였다. 즉 개인정보를 보호하고 관리하기 위한 법률 및 시행령에서 제시한 개인정보의 안전성 확보에 필요한 관리적·기술적 보호기준의 경우 개인정보 처리 기업의 특성 및 중요도에 따른 우선 적용 기준이 고려되지 않아 조치기준 이행에 어려움이 따르고 있다. 이에 따라 「개인정보보호법」에서 제시한 개인정보의 안전한 보호를 위한 관리적 기술적 조치 기준에 대해서 전문가를 대상으로 AHP 기법을 이용하여 가중치를 산정하고 우선순위를 과학적으로 제시 하였다.

먼저 개인정보의 안전성 확보조치 기준들의 세부적인 사항들을 기존 문헌 연구와 법률을 통해 평가 기준을 도출 하였고, 평가 기준의 정제화 및 계층화를 위해 브레인스토밍 기법 중의 하나인 KJ 기법을 이용하여 전문가의 창의성을 바탕으로 복잡한 현상을 객관적으로 분석하여 평가 기준들의 유사항목을 통합하고 그룹화 하여 계층구조를 생성하였다. 이와 함께 AHP 기법을 이용해 계층화된 평가 기준을 전문가를 통해 객관적이고 공정한 평가를 수행하여 가중치를 산정하고 우선순위를 도출하였다. 그 결과 개인정보의 암호화 항목이 접속기록의 보관 및 위·변조방지 항목 보다 개인정보보호를 위해 세배 더 중요하고 우선순위가 높은 항목이라고 전문가들은 판단하고 있다. 이처럼 전체 평가 기준에 대한 우선순위 도출을 통해 기업에서 개인정보의 안전성 확보조치 기준 적용을 위한 보다 합리적이고 효율적인 수단으로 활용 가능 할 것이다.

본 연구의 의의는 일괄적으로 요구하고 있는 개인정보처리 기업 및 공공기관의 개인정보의 안전성 확보를 위한 조치 기준항목의 가중치를 평가하고 우선순위에 따라 선 조치되어야 될 최적의 모형을 제공하고 있다고 할 수 있다.

이에 따라 개인정보보호 활동에 대한 충분한 투자가 어려운 중소기업 및 개인정보보호 전문 인력을 갖추고 있지 않는 기업에서 개인정보의 보호를 위한 조치사항을 이행하는데 어려운 점이 존재하는데, 본 연구에서 제시한 계층구조 및 평가항목에 따른 가중치별 우선순위는 개인정보의 보호를 위한 우선 적용기준 및 모범 사례로 활용되는 계기가 될 것이다.

하지만 향후 연구에는 법률에서 요구한 개인정보의 안전성 확보조치 기준 이외 평가항목 산정을 위한 다양한 전문가의 참여와 각 전문가의 전문도에 따른 가중치를 부여하고 결과를 반영하여 좀 더 정교한 가중치 도출과 개인정보보호를 위한 추가 기준 도출을 하고, 이 연구의 결과를 바탕으로 기업에 적용하여 그 효용성과 적정성 평가를 통한 실효성 검증과 개인정보를 취급하는 공공, 민간, 통신 등 다양한 기관별 특화된 우선순위 산정 방안이 필요할 것으로 보인다.

참고문헌

[1] 김영섭, “개인정보보호 수준 평가지표 개발에 관한 연구”, 석사학위논문, 전남대학교, 2008

[2] 행정안전부, “개인정보의 안전성 확보조치 기준”, 행정안전부고시 제43호, pp. 1-48, 2011

[3] 방송통신위원회, 한국정보보호진흥원. “개인정보의 기술적 관리적 보호조치 기준 해설서”, 한국정보보호진흥원, 2009

[4] 이동녁, “개인정보보호를 위한 정보시스템 보안감사 방법에 관한 연구”, 석사학위논문, 명지대학교, 2010

[5] 김정덕, “개인정보보호 거버넌스의 목표와 프로세스에 관한 연구”, 한국정보보호학회지, 제21권 제5호, pp. 7-11. 2011

[6] 정태명, “사업자 개인정보보호수준 향상방안 연구”, 한국CPO포럼, pp. 3-6, 2008

[7] Domingo R. Tan, Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United Stats and European Union, 21 Loy. L.A. Int'l & Comp. L. Rev. 661, 1999

[8] 행정안전부, “개인정보보호법”법률 제 11690호, 2011

[9] Saaty T.L, "Decision making for leaders (AHP series, Vol.2)", RWS, 1995

[10] Saaty,T.L, “The Analytic Hierarchy Process”, New York : McGraw - Hill. International, 1980

[11] Saaty,T.L,“Decision Makingwith Dependenceand Feedback:The Analytic Network Process”, Int. J. ServicesSciences, Vol. 1, No.1, pp.83-98, 2008

[12] 이정현, “개인정보보호 강화를 위한 인터넷 개인인증 프레임 워크 개선모델 연구”, 박사학위논문, 고려대학교, 서울, 2012

[13] 이창효, “집단의 의사결정론”, 세종출판사, 2000

[14] 행정안전부, “2012년 국가정보화백서”, 한국정보화진흥원, pp. 407~408, 2012

[15] Service Design Platform, http://www.servicedesignplatform.com/

[저 자 소 개]

김 영 희 (Young-hee Kim)

2001년 컴퓨터공학사
2001년~2012년 인젠, 인터파크
2012년~현재 한화S&C
2013년 산업정보시스템공학석사
2013년~현재 서울과학기술대학교
IT정책전문대학원
산업정보시스템공학 박사과정

email : sorak75@naver.com

국 광 호 (Kwang Ho Kook)

1979년 서울대학교 산업공학사
1981년 서울대학교 대학원 산업공학 석사
1989년 美조지아 공과대학교 대학원 산업공학박사
1989년~1993년 한국전자통신연구원 선임연구원
1993년~현재 서울과학기술대학교 기술경영융합대학 글로벌융합산업공학과 교수

email : khkook@seoultech.ac.kr