박사학위논문

개인정보보호 강화를 위한 개인정보 관리역량 성숙도 모델 및 평가지표 개발

Development of Personal Information Management Competency Maturity Model and Evaluation Indicators to Strengthen Privacy

제주대학교 대학원

융합정보보안학협동과정

오 상 익

2023년 2월

개인정보보호 강화를 위한 개인정보 관리역량 성숙도 모델 및 평가지표 개발

지도교수 박 남 제

오 상 익

이 논문을 융합정보보안학협동과정 박사학위 논문으로 제출함

2022년 11월

오상익의 융합정보보안학협동과정 박사학위 논문을 인준함

심사위원장 변 영 철 ㊞

위 원 조 정 원 ㊞

위 원 강 구 홍 ㊞

위 원 박 명 환 ㊞

위 원 박 남 제 ㊞

제주대학교 대학원

2022년 11월

Development of Personal Information Management Competency Maturity Model and Evaluation Indicators to Strengthen Privacy

Sangik Oh
(Supervised by professor Namje Park)

A thesis submitted in partial fulfillment of the requirement for the degree of Doctor of Philosophy in Convergence Information Security

2022. 11.

This thesis has been examined and approved.

Yung-cheol Byun .....

Thesis director, Namje Park, Prof. of Elementary Computer Education

Jungwon Cho .....

Koohong Kang .....

Myunghwan Park .....

Namje Park .....

2022. 11. 28.

Department of Convergence Information Security
GRADUATE SCHOOL
JEJU NATIONAL UNIVERSITY

목 차

표 목 차

<표 Ⅱ-23> AHP 연구의 Random Index (Saaty, 1982)
<표 Ⅲ-1> 연구 절차
<표 Ⅲ-2> 5개 상위 평가구조별 개인정보 관리역량성숙도 평가항목 선별 결과
<표 Ⅲ-3> 개인정보보호 역량 및 윤리 평가항목의 분류
<표 Ⅲ-4> 도출된 개인정보 관리역량성숙도 평가항목
<표 Ⅲ-5> 델파이 조사 방법과 내용
<표 Ⅲ-6> 델파이 선행연구의 전문가패널 수
<표 Ⅲ-7> 1차 델파이 조사 전문가 풀 구성
<표 Ⅲ-8> 델파이 조사 환류 회의 참가자
<표 Ⅲ-9> 2차 델파이 조사 전문가 풀 구성
<표 Ⅲ-10> AHP 조사 방법 및 활동 내용
<표 Ⅲ-11> AHP 조사를 위한 전문가 풀 구성
<표 Ⅲ-12> 델파이 조사 전문가패널의 일반적 특성
<표 Ⅲ-13> 용어 수정이 필요한 요인
<표 Ⅲ-14> 1차 델파이 설문조사 결과
<표 Ⅲ-15> 2차 델파이 조사 분석 결과
<표 Ⅲ-16> 델파이 조사 도출 평가항목 수
<표 Ⅲ-17> 최종 도출된 측정 문항
<표 Ⅲ-18> AHP 조사 전문가패널의 일반적 특성
<표 Ⅲ-19> 상위개념의 상대적 중요도 및 순위
<표 Ⅲ-20> 하위개념 우선순위 및 상위개념 내 상대적 중요도
<표 Ⅲ-21> 사전 계획 및 설계단계의 하위개념 우선순위 및 상대적 중요도
<표 Ⅲ-22> 개인정보 생애주기 보호 단계의 하위개념 우선순위 및 상대적 중요도
<표 Ⅲ-23> 안전성 확보 조치단계의 하위개념 우선순위 및 상대적 중요도
<표 Ⅲ-24> 개인정보 관리 수준 점검 및 개선단계의 하위개념 우선순위 및 상대적 중요도
<표 Ⅲ-25> 권리보장 및 윤리역량단계의 하위개념 우선순위 및 상대적 중요도
<표 Ⅲ-26> 하위개념 우선순위 및 전체 대비 상대적 중요도
<표 Ⅲ-27> 사전 계획 및 설계단계 세부 지표의 상대적 중요도 및 순위
<표 Ⅲ-28> 개인정보 생애주기 보호 단계 세부 지표의 상대적 중요도 및 순위
<표 Ⅲ-29> 안전성 확보 조치단계 세부 지표의 상대적 중요도 및 순위
<표 Ⅲ-30> 개인정보 관리 수준 점검 및 개선단계 세부 지표의 상대적 중요도 및 순위

<표 Ⅲ-31> 권리보장 및 윤리역량단계 세부 지표의 상대적 중요도 및 순위
<표 Ⅲ-32> 세부 지표 전체 대비 우선순위 및 상대적 중요도
<표 Ⅲ-33> 최종 평가지표 점수 환산표
<표 Ⅲ-34> BCMM 기반의 제안된 개인정보 관리역량 성숙도 모델(PCM2)
<표 Ⅲ-35> 최종 도출된 개인정보 관리역량 성숙도 모델 및 평가지표
<표 Ⅳ-1> 대상자의 인구통계학적 특성
<표 Ⅳ-2> 세부 지표의 평균과 표준편차
<표 Ⅳ-3> Cronbach's α 값 산출 결과
<표 Ⅳ-4> 세부 지표의 신뢰도 분석 결과
<표 Ⅳ-5> 참여 대상자의 인구통계학적 특성
<표 Ⅳ-6> PIA의 성숙도 측정모델
<표 Ⅳ-7> CMMI의 성숙도 측정모델
<표 Ⅳ-8> 제안된 개인정보 관리역량 성숙도 모델(PCM2)
<표 Ⅳ-9> PIA-CMMI-PCM2 성숙도 측정 결과 비교
<표 Ⅳ-10> PIA의 개인정보 영향평가 측정 결과
<표 Ⅳ-11> 신규 제안한 평가지표의 측정 결과
<표 Ⅳ-12> 개인정보 관리역량에 대한 집단 간 평균 비교 결과
<표 Ⅳ-13> 하위개념에 대한 집단 간 평균 비교 결과
<표 Ⅳ-14> 전체-지방자치단체-공공기관-민간기업 성숙도 수준 결과
<표 Ⅳ-15> 개인정보 관리역량성숙도 자가 진단 결과(최종)
<표 Ⅳ-16> 지방자치단체-공공기관-민간기업의 성숙도 자가 진단 결과 비교
<표 Ⅳ-17> 신규 개발 지표의 집단 간 성숙도 자가 진단 결과 비교

그 림 목 차

요 약

본 연구는 개인정보 취급자가 스스로 개인정보 관리역량성숙도를 측정 함에 있어 더욱 객관적으로 관리역량 수준을 확인하고 그 결과에 따라 개인정보 관리 현상에 대한 개선 또는 관리를 할 수 있는 평가지표를 개발하는 데 그 목적이 있다.

본 연구의 목적을 달성하기 위하여 선행연구 및 문헌을 고찰하여 연구에 필요한 개념을 설계하였다. 이를 토대로 현행 개인정보보호 및 정보보안 성숙도 모델의 문제점을 파악하였다. 기존의 ISMS-P, PIA, 공공기관 개인정보 관리 수준 진단, ISO27702 모델에서 75개 평가지표를 선정하였고, 개인정보 취급자의 역량과 윤리의식 측정을 위한 14개 항목을 신규 제안하여 총 89개의 평가지표를 도출하였다. 전문가패널을 대상으로 2차례에 걸쳐 델파이 조사하였고, 평가지표 간 상대적 중요도를 파악하기 위해 AHP 조사기법을 통해 가중치를 평가하였다. 그 결과 최종 평가지표는 5개의 상위개념, 17개의 하위개념, 89개의 세부 지표로 확정되었다. 평가지표를 측정할 성숙도 모델은 기존의 업무 연속성 성숙도 모델(BCMM)을 기반으로 하여 7단계(Very High, High, Very Medium, Medium, Low, Very Low, None)의 성숙도 수준으로 된 개인정보 관리역량 성숙도 모델(PCM2 : Privacy Competency Maturity Model)을 제안하였다.

본 연구에서 개발한 개인정보 관리역량 성숙도 모델과 평가지표에 대한 사용자의 신뢰도 검증 결과, Cronbach's α 값이 0.9 이상으로 매우 높은 것으로 분석되었다. 또한, 공공과 민간기관 종사자를 대상으로 개인정보 관리역량 자가 진단 테스트 결과, 공공이 민간보다 개인정보 관리역량 수준이 높은 것으로 나타났다. 기존 성숙도 측정모델인 PIA, CMMI와 제안한 성숙도 측정모델인 PCM2를 비교분석한 결과, PIA와 CMMI는 개인정보처리자 평가에 적합하고, PCM2는 개인정보 취급자 평가에 적합한 것으로 나타났다.

지금까지의 개인정보보호 관련 역량 모델 평가에 관한 연구를 보면 정보보호 위주의 연구가 대부분이다. 기관 내에서 강력한 보호 대책 및 기준에도 불구하고 내부자에 의한 개인정보 침해사고가 꾸준히 발생하는 원인은 통제하는 주체와 통제받는 주체가 인간이다. 이러한 인간의 특성을 고려하여 개인정보 취급자의 관리역량과 윤리의식을 평가하기에는 기존의 성숙도 모델로는 한계점이 있다. 이들의 평가 모델은 개인정보처리자인 기관의 개인정보보호 관리체계와 자산을 평가하기에는 적합하지만, 개인정보 취급자를 식별하고 평가하기에는 한계가 있다.

그렇기에 본 연구에서는 개인정보 취급자를 관점으로 기존의 모델을 한 단계 개선하고 인간의 내면을 고려한 개인의 관리역량과 윤리의식을 높일 수 있는 지표를 신규로 개발하여 개인정보 관리역량 성숙도 모델 및 평가지표를 개발하였다는 데 큰 의의가 있다. 개발된 모델은 개인정보처리자가 아닌 개인정보 취급자를 평가 대상으로 한다는 점, 개인정보 관리역량성숙도 평가에 유용한 정보를 제공한다는 점, 그리고 평가의 실제적인 활용성을 위해서 개발하였다고 할 수 있다.

본 연구를 통해서 개발된 평가지표를 활용하여 개인정보 취급자가 스스로 업무를 수행하는데 세부적인 관리지침으로 활용할 수 있도록 하였으며, 개인정보 관리역량 수준을 진단하여 이를 기반으로 객관적이고 신뢰할 수 있는 개인정보 보호 관리가 이루어질 수 있도록 할 뿐만 아니라 더욱 체계화된 개인정보 관리 체계 정립에 기여될 것으로 기대한다.

주제어 : 개인정보보호, 개인정보취급자, PCM2, AHP, 성숙도

Ⅰ. 서 론

1.1 연구 배경

디지털 정보 기술이 발전하면서 세계 경제의 패러다임은 지식자산인 데이터를 기반으로 한 새로운 부(富)와 가치 창출되는 데이터 기반의 경제로 급속히 전환되고 있다. Big Data, AI, UAM 등 모든 산업 분야에서 사용되는 자원은 바로 데이터다. 데이터 없는 혁신은 불가능하다. 특히, 개인정보는 경제발전과 사회성장을 위한 핵심적인 데이터다. 신산업 육성을 위해서는 데이터가 Big Data, AI, IoT 등 신기술의 핵심이 됨에 따라, 데이터의 안전한 이용과 보호를 위한 사회적 규범 확립이 시급한 상황이라는 점에 공감대가 형성되고 있다. 하지만, 사이버 침해사고로 인한 개인정보 유출 사고의 규모 및 건수는 증가하고 있으며, 개인정보의 경제적, 사회적 가치가 증가함에 따라 개인정보 주체인 개인이 자신의 정보에 관하여 과거와 달리 적극적으로 관리, 통제하는 추세다. 개인정보 유출 사고로 인한 개인정보의 유출 또는 훼손이 발생하는 경우 해당 기관은 법 위반으로 인한 재정적 손해뿐만 아니라, 개인정보보호에 대한 관리 감독 소홀로 인한 경영진 입건 등 형사적 책임과 회사 이미지 하락으로 인한 이미지 손실, 매출 하락 등의 악영향을 미친다.

특히, 공공부문은 2021년 기준 개인정보 669억 건을 처리하고 있으며, 공공기관의 16.4%는 100만 명 이상의 개인정보를 보유하고 있는 만큼 개인정보보호를 최우선으로 하여야 한다[1]. 하지만, 개인정보보호위원회가 2022년 2월 발표한 중앙행정기관, 지방자치단체, 공공기관 등 총 795개 공공기관 대상으로 한 '2021년 개인정보 관리 수준 진단' 결과는 <표 Ⅰ-1>과 같으며, 공공기관 절반가량이 개인정보 관리 평가에서 '보통 이하'로 판정받았다[2]. 특히, 226개 기초지방자치단은 양호등급이 47%로 개인정보 관리 수준이 상대적으로 미흡한 것으로 나타났다.

<표 Ⅰ-1> 2021년 공공기관 개인정보 관리 수준 진단 평가 결과(기관별)[2]

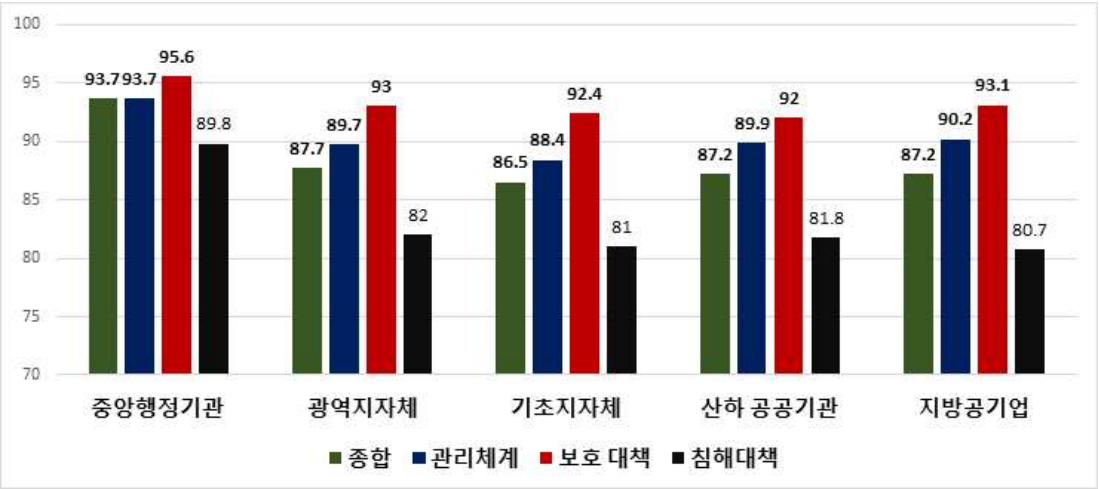
구 분		평균 (795개)	중앙행정 기관	지방자치단체		산하 공공기관	지방 공기업
				광역	기초		
결과(점)		87.4	93.2	87.7	86.5	87.2	87.2
등급별	양호	452 (57%)	35 (71%)	12 (47%)	106 (47%)	208 (60%)	91 (59%)
	보통	274 (34%)	13 (18%)	3 (44%)	100 (44%)	112 (32%)	46 (30%)
	미흡	69 (9%)	0 (11%)	2 (9%)	20 (9%)	30 (8%)	17 (11%)

<표Ⅰ-2>의 유형별로 보면, 정보 주체의 권리행사 절차와 개인정보 처리 방침 마련 등 보호 대책 분야는 양호한 것으로 나타났으나, 침해사고 예방 관련 안전성 확보 조치 등 침해대책 분야는 다소 미흡한 것으로 나타났다[2].

<표 Ⅰ-2> 2021년 공공기관 개인정보 관리 수준 진단 평가 결과(유형별)

구분	종합	관리체계	보호 대책	침해대책
중앙행정기관	93.7	93.7	95.6	89.8
광역지자체	87.7	89.7	93	82
기초지자체	86.5	88.4	92.4	81
산하 공공기관	87.2	89.9	92	81.8
지방공기업	87.2	90.2	93.1	80.7

특히, 개인정보의 침해대책 분야 중 개인정보 처리시스템의 접근권한 관리 및 접속기록 점검이 가장 미흡한 것으로 나타나, 해당 항목은 개인정보 유출 사고의 주요 원인이 되기 때문에 이를 최소화하는 방안이 필요하다.



[그림 Ⅰ-1] 2021년 공공기관 개인정보 관리 수준 진단 평가 결과(유형별)

최근 발생한 신변 보호 중인 전 여자친구의 모친을 살해하고 그 동생을 중태로 빠뜨린 혐의를 받는 이석준 사건으로 인해 공무원의 개인정보 무단 열람과 유출이 심각한 사회적 문제가 되고 있음을 다시 한번 일깨워 주고 있다. 이 사건을 통해 공무원이 개인정보 처리시스템에 접근 후 개인정보를 무단으로 유출하고 흥신소에 개인정보를 판매한 사실이 드러나 충격을 주기도 했다.

공무원은 업무 특성상 개인정보를 취급되는 경우가 많다. 2022년 2월 개인정보보호위원회에 따르면 공공기관에서의 개인정보 무단 열람 또는 유출 사례는 매년 수만 건씩 발생하고 있는 것으로 나타났다[1]. 2013~2017년간 공무원이 보건복지부 사회보장 정보시스템을 이용해 타인의 개인정보를 무단열람하다가 적발된 건수가 2,061건이나 되는 것으로 나타났다. 2021년 상반기에만 공공기관의 개인정보 유출 건수가 144,000건으로 나타났으며, 이 중 업무 과실에 의한 유출이 80,000건에 달한다[1]. 이 때문에 접근권한 자격을 가진 자만 개인정보에 접근할 수 있도록 하고 있으며, 무단 열람하거나 유출하는 경우 처벌과 징계가 뒤따르게 하고 있다. 하지만, 개인정보에 무단 접근하는 것을 적발하기 쉽지 않고, 적발되더라도 낮은 처벌 수위가 많아 이 들의 경각심이 크지 않다는 지적이 나왔다. 개인정보보호위원회에 따르면, 2017~2019년 중앙행정기관과 지방자치단체에서 개인정보 유출로 인한 징계받은 건수는 총 153건, 이 중 형사 고발한 사건은 2건에 불과하다고 나타났다. 일탈 행위가 적발되더라도 대부분 기관 내부 징계로 그치기 때문에 징계나 처벌 규정이 정상적으로 작동될 수 있도록 제도 정비와 개인정보 취급자들이 스스로 역량을 강화할 방안을 마련할 필요가 있다[1].

따라서 본 연구는 개인정보처리자와 개인정보 취급자가 스스로 개인정보보호를 위한 법·규정의 준수와 개인정보의 생애주기별 수행 능력, 윤리지수를 측정하여 관리역량을 강화하기 위한 기준으로 활용할 수 있도록 평가지표를 개발하고 활용하여 지방자치단체의 개인정보 취급자가 스스로 업무를 수행하는데 세부적인 관리지침과 가이드라인으로 적용될 수 있도록 하여 법·규정의 준수와 개인정보보호에 대한 인식 제고와 사고 예방에 기여하고자 하였다.

또한, 개인의 개인정보보호 역량과 윤리지수 수준을 평가하여 이를 기반으로 객관적이고 신뢰적인 개인정보보호 관리가 이루어지도록 하는 것이다.

1.2 논문의 구성

본 연구는 공공기관의 개인정보 관리역량 향상방안을 제안하기 위해 크게 5개의 장으로 구성된다.

첫 장, 서론에서는 연구의 배경이 되는 개인정보에 따른 변화를 알아보고 문제와 연구의 목적 및 범위를 설정한다.

2장 관련 연구에서는 본 연구를 수행하는 데 개인정보의 정의, 개인정보의 유출 사례, 필요한 제도나 규제, 개인정보보호 관리체계를 살펴보고, 개인정보보호 역량 모델 방식을 구분하고 장단점을 분석한다. 효과성 실증연구를 위해 요구되는 요소들을 정리한다.

3장에서는 개인정보 취급자의 개인정보 관리역량 강화를 위하여 개인정보 관리역량 모델 및 평가지표 설계를 위하여, 전문가 집단의 의견을 수렴하여 최종 요인을 도출하는 델파이 조사기법에서 도출된 평가지표를 바탕으로 한 계층 분석을 통해 지표 간의 상대적 중요도와 우선순위를 검증할 수 있는 AHP 분석기법을 이용하여 연구를 진행한 후 개인정보 관리역량 모델 및 평가지표를 개발한다.

4장에서는 개발된 개인정보 관리역량 모델과 평가지표에 대한 신뢰도 검증, 기존 성숙도 모델과 제안 모델 비교 분석, 집단 간 자가 진단 테스트 검증 등 실증하여 모델의 유의성을 증명한다.

5장에서는 본 연구를 요약하고 결과를 분석하고 고찰하여, 연구 결과가 가지는 가치를 평가하며, 개선사항을 분석하고, 향후 연구 방향과 과제에 대해 제시한다.

[그림 Ⅰ-2] 논문의 구성

1.3 연구의 범위와 방법

본 연구의 목표를 달성하기 위해, 기존 연구 자료들을 활용하였으며, 인터넷을 통한 자료 검색과 국가기관의 각종 지침을 참조하였다.

또한, 개인정보 관리체계 모델 적용 사례를 분석하여, 개인정보 역량 강화 모델의 개선점을 찾아 방향성을 찾아보았다.

1) 본 연구는 개인정보 취급자의 개인정보보호 수준 향상에 관한 내용을 분석하고, 관리역량성숙도 향상을 이끌 방안을 찾기 위해서 개인정보 관리역량 성숙도 모델을 설계, 구현, 분석의 과정을 수행한다.

2) 개인정보 관리역량 성숙도 모델을 개인정보 취급자를 대상으로 적용하여 제안된 모델이 개인정보 취급자의 개인정보보호 활동에 영향을 미치는지 실증 검증을 한다.

Ⅱ. 이론적 배경

2.1 개인정보보호의 개요

2.1.1 개인정보의 개념과 가치

가. 개인정보의 개념

개인정보의 개념에 대해서는 다양한 정의가 존재한다. Wacks(1989)는 개인정보를 '개인의 건강 상태, 신체적 특징, 신념이나 사상과 같은 정신세계, 사회적·경제적 지위, 경력・학력・재산 상태 등 개인에 대한 사실·판단·평가에 관한 모든 정보'라고 정의하였으며[3], OECD(1980) 권고안은 개인정보를 '알아볼 수 있는 또는 알아본 개인에 관한 모든 정보'라고 정의하였다[4].

한편, 우리나라의 개인정보 보호법에 규정된 개인정보의 정의는 '살아 있는 개인에 관한 정보'로서 이름, 주소 등으로 개인을 특정할 수 있는 정보, 해당 정보만으로는 특정인을 식별할 수 없어도 타 정보와 결합하여 식별이 가능한 정보, 가명 처리한 정보를 말한다[5].

<표 Ⅱ-1>과 같이 성명, 생년월일, 주소 등 개인에 관한 모든 정보는 개인정보이며, 해당 정보만으로 정보 주체가 누구인지 알 수 없더라도 정보를 결합하였을 때 누구인지 식별할 수 있으면 개인정보에 해당하는 것이다. 하지만, 법인·단체에 관한 정보, 사망한 자는 개인정보로 보지 않는다.

<표 Ⅱ-1> 개인정보의 종류[6](출처 : 개인정보보호위원회의 개인정보보호 포털)

구분		개인정보 종류
인적 사항	일반정보	이름, 주소, 연락처, 생년월일, 성별, 출생지, 주민등록번호 등
	가족 정보	가족관계, 가족 구성원의 정보
신체적 정보	신체정보	지문, 얼굴, 유전자 정보, 음성, 홍채, 몸무게, 키 등
	의료·건강 정보	건강 상태, 진료기록, 장애등급, 신체장애, 혈액형, IQ, 병력, 약물 테스트 등 신체검사 정보
정신적 정보	기호・성향 정보	도서 대여 기록, 잡지 구독 정보, 물품구매 기록, 웹사이트 접속기록
	내면의 비밀 정보	정당・노조 가입 여부 및 활동, 종교, 가치관, 사상, 신조 등
사회적 정보	교육정보	학력, 출석상황, 성적, 기술 자격증(전문 면허증) 보유, 상벌 기록, 생활기록부, 건강기록부 등
	병역정보	병역 여부, 군번, 계급, 제대유형, 부대, 주특기 등
	근로 정보	직장, 근무처, 고용주, 근로 경력, 직무 평가 기록, 상벌 기록 등
	법적 정보	재판 기록, 과태료 납부내역, 전과・범죄 기록 등
재산적 정보	소득정보	사업소득, 이자소득, 급여, 수수료 및 보너스 등
	신용정보	대출 및 담보 설정내역, 계좌번호, 신용카드번호, 신용평가 정보 등
	부동산 정보	자동차, 소유주택, 토지, 기타 소유 차량, 상가/건물 등
	기타 수익 정보	보험 가입현황, 병가, 휴가 등
기타 정보	통신정보	E-Mail, 통화기록, Log file, 쿠키 등
	위치정보	개인의 위치정보
	습관 및 취미 정보	음주량, 흡연여부, 선호 스포츠, 레포츠, 도박, 여가 등

고유 식별정보는 개인정보 보호법 제24조 제1호에 '개인을 특정하기 위하여 고유하게 부여된 식별정보로서 대통령령으로 정하는 정보'로 규정하고 있으며, 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호가 이에 해당한다. 이는 우리나라의 경우, 고유 식별정보가 각종 실명확인제도, 금융실명제, 개인 신용평가 등과 결합하여 모든 경제·사회 활동에서 광범위하게 활용되므로 특별히 규율할 필요가 있기 때문이다[7].

개인정보 중에서도 특히 사생활 침해의 우려가 더 큰 정보를 민감정보로 개인정보 보호법 제23조 제1호에 별도 규정하고 있다. 민감정보[7]는 '건강, 성생활 등에 관한 정보, 정치적 견해, 노동조합·정당의 가입·탈퇴, 사상·신념, 그 밖에 정보 주체의 사생활을 현저하게 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보'를 말한다. 여기에서 말하는 대통령으로 정하는 '정보'의 의미는 인종이나 민족에 관한 정보, 유전자 검사로 얻어진 유전정보, 범죄경력, 개인의 신체·행동·생리적 특징에 관한 정보로서 특정 개인을 식별할 목적으로 일정한 기술을 통해 생성한 정보 등이 민감정보에 해당한다.

개인정보 보호법은 가명 정보의 정의를 개인정보를 가명 처리하여 특정 개인을 알아볼 수 없는 정보라고 한다. 즉, 가명 정보란 등으로 개인을 특정할 수 있는 정보 또는 해당 정보만으로는 특정 개인을 식별할 수 없더라도 다른 정보와 쉽게 결합하여 특정할 수 있는 정보를 가명 처리하여 특정 개인을 알아볼 수 없는 정보라고 한다. 여기에서 말하는 가명 처리란 개인정보 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 식별할 수 없도록 처리하는 것을 말한다[8].

개인정보를 영향도에 따라 등급을 분류하면 <표 Ⅱ-2>와 같으며, 1등급은 "그 자체로 개인의 식별이 가능하거나 매우 민감한 개인정보 또는 관련 법령에 따라 처리가 엄격하게 제한된 개인정보", 2등급은 "조합되면 명확히 개인의 식별이 가능한 개인정보", 3등급은 "개인식별정보와 조합되면 부가적인 정보를 제공하는 간접정보"로 분류한다[9].

<표 Ⅱ-2> 영향도별 개인정보 분류[9]

(※ 개인정보보호위원회. "개인정보 영향평가 수행 안내서" 내용 인용 및 재구성)

등급	조합설명	위험성	분류	개인정보 종류	근거
1	그 자체로 개인의 식별이 가능하거나 매우 민감한 개인정보 또는 관련 법령에 따라 처리가 엄격하게 제한된 개인정보	- 정보 주체의 경제적/사회적 손실 야기 또는 사생활을 현저하게 침해 - 범죄에 직접적으로 악용 가능 - 유출 시 민·형사상 법적책임 부여 가능 및 대외 신뢰도 저하	고유 식별 정보	· 주민등록번호 · 여권번호 · 운전면허번호 · 외국인등록번호	· 개인정보 보호법 제24조 · 같은 법 시행령 제19조
			민감 정보	· 사상·신념 · 노동조합·정당의 가입·탈퇴 · 정치적 견해 · 병력(病歷) · 신체적·정신적 장애 · 성적(性的) 취향 · 유전자 검사정보 · 범죄경력정보 · 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보 · 인종이나 민족에 관한 정보	· 개인정보 보호법 제23조 · 같은 법 시행령 제18조
			인증 정보	· 비밀번호 · 바이오 정보(지문, 홍채, 정맥 등)	· 개인정보의 안전성 확보 조치 기준 고시 제2조
			신용 정보/ 금융 정보	· 신용카드번호 · 계좌번호 등	· 신용정보의 이용 및 보호에 관한 법률 제2조, 제1호 가목, 제1의2호, 제2호
			의료 정보	· 건강 상태 · 진료기록 등	· 의료법 제22조, 제23조 · 같은 법 시행규칙 제14조 등
			위치 정보	· 개인 위치정보 등	· 위치정보의 보호 및 이용 등에 관한 법률 제2조, 제16조 등

등급	조합설명	위험성	분류	개인정보 종류	근거
2	조합되면 명확히 개인의 식별이 가능한 개인정보	- 정보 주체의 신분과 신상정보 확인 또는 추정 가능 - 광범위한 분야에서 불법적인 이용 가능	개인 식별 정보	· 이름 · 주소 · 전화번호 · 이메일주소 · 생년월일 · 성별 등	
			개인 관련 정보	· 학력 · 직업 · 키 · 몸무게 · 혼인 여부 · 가족 상황 · 취미 등	
			기타 개인 정보	· 해당 사업의 특성에 따라 별도 정의	
3	개인 식별정보와 조합되면 부가적인 정보를 제공하는 간접정보	- 정보 주체의 활동 성향 등에 대한 추정 가능 - 제한적인 분야에서 불법적인 이용 가능	자동 생성 정보	· IP 정보 · MAC 주소 · 사이트 방문 기록 · 쿠키 등	
			가공 정보	· 통계 정보 등	
			제한적 본인 식별 정보	· 회원 번호 · 사 번 · 내부용 개인 식별정보 등	

나. 개인정보의 가치와 중요성

개인정보는 개인에 관한 정보로서 가족, 건강에 관한 정보와 같이 사적인 정보는 물론 직장정보와 같은 사회적·경제적 정보도 포함된다. 또한, 객관적인 정보 이외에도 정보 주체에 대한 의견이나 평가와 같은 주관적 평가도 포함된다.

따라서 개인정보는 개인의 인격적 표상의 성격이 강하며, 해당 정보 주체와 불가분의 관계에 있다. 개인정보 중에서도 민감정보는 특히 인격적 성격이 강하다고 한다. 이러한 정보는 특히 사회적 차별을 야기 또는 현저히 인권을 침해할 우려가 있다.

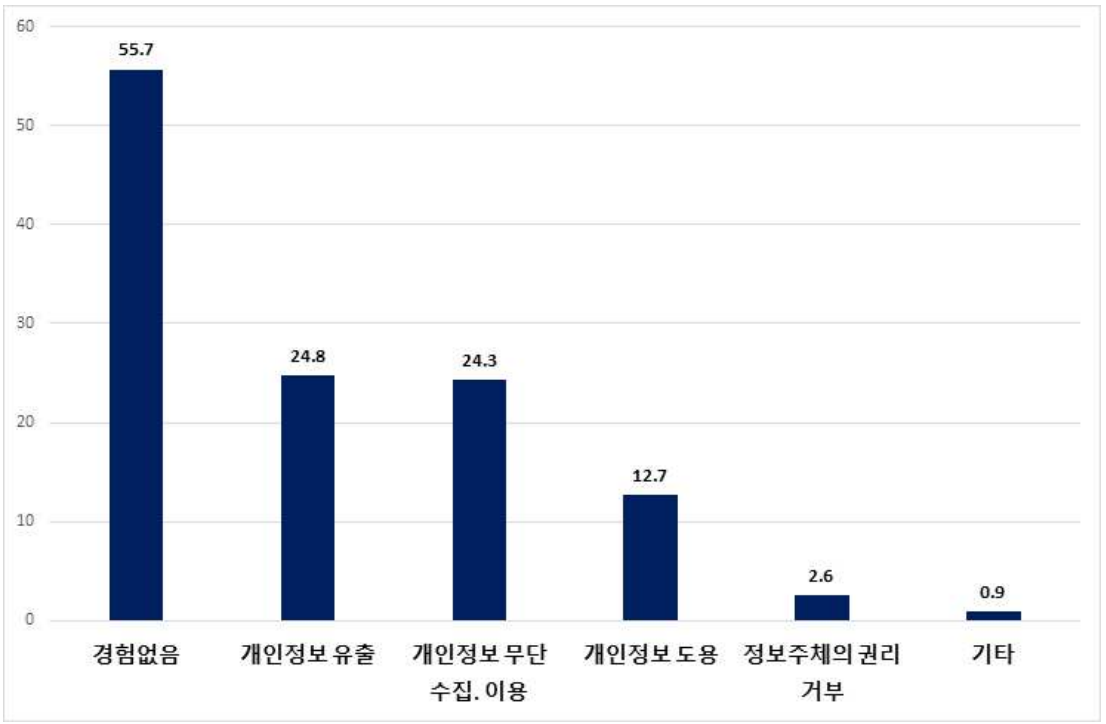
개인정보는 그 자체로 특정인의 인격을 나타내므로 정보 주체와 완전히 분리하여 파악하기에는 부자연스러운 측면이 있으며, 개인정보는 정보 주체와 불가분의 관계에 있다고 한다.

개인정보를 포함한 데이터가 핵심인 4차 산업혁명 시대의 핵심 자원으로 부상

하면서 개인정보가 경제적·재산적 가치를 가지게 되었다. 모든 처리에 있어 모든 개인정보가 항상 경제적·재산적 가치를 가지는 것은 아니지만 개인정보의 활용을 통한 다양한 가치 창출이 가능해짐에 따라 공공과 민간을 불문하고 개인정보가 경제적 가치를 가지게 되었다.

한편, 정부도 개인정보 보호법 개정을 통해 정보 주체의 동의 없이 통계작성, 과학적 연구, 공익적 기록보존 등으로 가명 정보를 사용할 수 있는 근거를 마련하였다. 이는 정부에서도 개인정보의 재산적 가치를 인정한다는 사실을 보여주는 대표적인 사례라 한다. 이처럼 개인정보는 그 자체로 인격적 가치와 재산적 가치를 모두 가진다고 볼 수 있다.

개인정보는 재산적 성격으로 인해 양도성을 가진다[10]. 개인정보보호위원회가 발표한 "2021 개인정보보호 실태조사 보고서"에 따르면, 정보 주체의 44.3%가 지난 1년간 개인정보 침해 경험을 한 것으로 [그림 Ⅱ-1]과 같이 나타났다.



[그림 Ⅱ-1] 2021년 개인정보 침해 경험(1년간)
(출처 : 개인정보보호위원회, "2021년 개인정보보호 실태조사 보고서" 인용)

개인정보 침해 경험 유형은 개인정보의 유출 24.8%, 개인정보의 무단 수집·이용 24.3%, 개인정보의 도용 12.7% 순으로 나타났다.

개인정보 침해를 경험한 이들 중 29.7%는 개인정보 침해 사실을 통지받았음에도 피해 구제를 위해 아무런 대응도 하지 않은 것으로 나타났다. 반면 70.3%는 침해사고에 대응했다. 또한, 침해사고를 경험한 이들 중 52.4%는 회원 탈퇴, 비밀번호 변경, 보안 설정 추가 등 개인적인 보안 조치한 것으로 나타났다[11]. 개인정보가 누군가에 의해 악의적인 목적으로 유출되는 경우 개인의 사생활 침해, 개인 안전과 재산 피해가 발생할 수 있다. 또 유출된 개인정보는 개인에게 원치 않는 대량의 광고성 스팸메일 발송을 위한 도용, 보이스피싱 등 범죄행위에 악용될 우려가 있다. 뿐만아니라 한번 유출된 개인정보는 회수가 사실상 불가능하기 때문에 더욱 심각하다고 할 수 있어 개인정보보호의 필요성과 중요성은 매우 높다고 한다. 개인정보가 중요한 이유는 개인정보를 통해 정보 주체가 누구인지 식별해 낼 수 있고, 그러면 정보 주체의 프라이버시와 같은 인간의 기본권 영역에 접근하는 것이 가능해져 인권에 대한 침해가 발생할 수 있기 때문이다[12]. 정보처리 기술의 발전으로 개인정보의 수집 및 이용, 저장이 용이하고 데이터에 대한 정확성이 높아져 다수의 기업이 경영전략 상 개인정보를 주요 자산으로서의 가치를 높게 평가하고 있기 때문에[13], 제대로 관리하지 못할 경우 신뢰성 하락으로 기업의 이미지가 크게 될 수 있다[14].

다. 개인정보보호의 목적과 필요성

개인정보를 보호하고 관리하는 목적은 개인정보의 오·남용, 유출 사고로부터 개인의 자기 결정권을 강화함으로써 개인정보의 인격적 주체성과 존엄성을 보호하고 가치를 높여서 정보 주체의 권리와 이익을 지키기 위함이다.

이에 따라 개인정보를 취급하는 기관에서는 개인정보의 생애주기별 보호 범위 및 기준 확립, 개인정보의 안전성 확보 조치, 정보 주체의 권리보장, 영상정보처리기기 규제에 대한 사항을 준수하여야 한다.

이를 위해서는 개인정보를 취급하는 기관과 기업에서는 개인정보보호와 관리를 위한 개인정보 처리 방침 및 내부 관리계획 수립·시행, 개인정보보호 책임자

지정 및 역할 부여, 개인정보에 대한 수집・이용・제공・보관・파기 등 생애주기 전 과정에 대한 관리적・기술적 보호 조치를 취해야 한다. 또한, 개인정보의 안전한 관리와 보호를 위한 안전성 확보 조치, 정보 주체의 권리보장, 개인정보 침해에 대한 대응 및 구제방안을 마련해야 한다.

개인정보를 취급하고 있는 기관에서 개인정보의 생애주기별 특성을 살펴보면, 첫 번째, 개인정보의 생애주기 전 단계에서 발생할 수 있는 개인정보 오・남용, 유출 사고에 대한 책임이 개인정보 취급 해당 조직으로 국한되는 것이 아니기 때문에 전사적 관리체계를 수립・시행해야 한다[15][16]. 두 번째, 개인정보를 취급하는 경우 해당 조직뿐만 아니라 개인정보 취급자, 위・수탁자 등 다수의 이해관계자가 존재하기 때문에 광의적인 관점에서 관리해야 한다[15][17]. 세 번째, 개인정보 취급기관은 개인정보보호에 대한 법률적 준거성이 존재한다. 개인정보 침해 시 취급기관과 이해관계자에 미치는 부정적인 영향 및 파급효과가 보안사고보다 크고, 그에 따른 처벌 수위도 높기 때문에 법률적 준거성 보장이 필요하다[15][17]. 네 번째, 정보 주체의 인식 변화에 따른 대응 형태 변화와 함께 국가 차원에서의 규제와 처벌이 강화되고 있다. 침해사고에 대한 대응에서는 과거에는 소극적인 대응이었지만, 현재는 개인정보에 대한 권리와 가치에 대한 중요성을 인식하고 정보 주체자 스스로 자기 결정권 보장을 받기 위해 소송과 손해 배상 청구를 통해 적극적으로 대응하고 있다. 국가 차원에서도 개인정보 침해사고에 대한 규제와 처벌 수위를 강화함으로써 기관의 개인정보보호에 대한 투자와 역량을 높이고자 유도하고 있다.

이처럼 개인정보의 다양한 특징과 트렌드 변화에 기인하여 개인정보 취급기관에서는 변화에 신속하게 대응하기 위한 개인정보보호와 관리 정책을 수립하고 시행하여야 한다.

2.1.2 개인정보의 생애주기

개인정보에 대한 생애주기 분류는 연구자별로 다양하다. 한국인터넷진흥원에서 개발한 CUPD 모델[18]은 수집, 이용, 제공, 파기 등 4단계로 분류하였다. 수집 단계는 수집 시 동의, 개인정보 수집 제한 등으로 구성되었다. 이용 단계는 개인정보 관리책임자의 지정, 목적 외 이용 금지, 개인정보의 보호조치로 구성되어 있다. 제공 단계는 개인정보 처리 위·수탁 규정, 동의 없이는 제3자 제공 금지 등으로 구성되어 있다. 파기 단계는 개인정보의 수집・이용・제공 목적이 달성된 때 즉시 파기 등으로 구성되어 있다[18]. 한국전산원[19]은 개인정보의 침해 유형을 정보의 '수집'과 '이용 및 제공', '저장 및 관리', '파기'의 4가지로 구분하였다. 수집 단계에서는 과도한 개인정보 수집 또는 동의를 얻지 않고 Log를 이용한 수집, 이용 및 제공 단계에서는 개인정보의 매매, 누출·누설, 사용자 동의 없는 광고·스팸, 저장 및 관리단계에서는 개인정보의 불완전한 저장, 정보의 미인증행위, 파기 단계에서는 정보 주체의 동의·철회·열람·정정 요구에 불응하는 행위를 예로 들었으며 이러한 침해 유형은 유비쿼터스 환경에서 더욱 다양화될 수 있다고 제언하였다[19]. 우리나라의 개인정보 보호법에는 개인정보의 수집·보유, 이용・제공, 파기 등 3단계로 분류되었다. 수집은 정보 주체에 관한 모든 형태의 개인정보를 취득하는 것뿐만아니라 정보 주체로부터 직접 개인정보를 제공받는 것을 말한다. 첫째, 개인정보를 수집하는 경우 서비스 제공을 위하여 필요한 최소한의 정보를 정당하고 적법하게 수집해야 하며, 필수정보 이외의 정보를 수집하는 경우 선택항목으로 구분하여 해당 정보의 제공 동의를 하지 않는다는 이유로 서비스 제공을 거부하지 않아야 한다[21]. 만 14세 미만의 아동 개인정보를 수집하려는 경우에는 법정 대리인의 동의를 받아야 하며, 법정 대리인이 동의를 거부하거나, 법정 대리인의 동의 의사가 확인되지 않을 시 수집일로부터 5일 이내에 파기해야 한다[3][20]. 주민등록번호는 법률・대통령령・국회규칙・대법원규칙・헌법재판소 규칙・중앙선거관리위원회규칙・감사원규칙 등 법적 근거가 있는 경우에만 수집・이용 등 처리한다. 각급 행정기관의 훈령・예규・고시, 지방자치단체의 조례・규칙 등으로 주민등록번호를 수집・이용 등 처리할 수 있는 근거가 될 수

없으며, 인터넷 홈페이지 등에서는 스마트폰 인증, 아이핀 등 주민등록번호 대체 수단을 제공하여야 한다. 민감정보나 주민등록번호를 제외한 고유 식별정보 처리 시 법령에 구체적으로 처리 허용하는 경우를 제외하고는 정보 주체에게 별도의 동의를 받아야 한다. 두 번째, 각 기관에서 보유하고 있는 개인정보에 대한 항목, 보유량, 처리목적 및 방법, 보유기간, 이용 처리시스템, 개인정보 취급자 등 현황을 주기적으로 관리하여야 하며, 공공기관은 개인정보 보호법 제32조에 따라 해당 관계기관의 장에게 등록하여야 한다. 보유하는 개인정보를 조회하거나 출력하는 경우 용도를 특정하고 항목의 최소화, 개인정보의 표시 제한, 출력물의 보호조치 등을 수행해야 한다[21]. 세 번째, 개인정보를 제3자에게 제공하는 경우 법적 근거이거나 정보 주체에게 관련 내용을 명확하게 고지하고 동의받아야 하며, 제3자에게 개인정보를 제공하는 과정에서 개인정보를 안전하게 보호하기 위한 보호 대책을 마련하여 이행하여야 한다. 네 번째, 개인정보 처리 업무를 제3자에게 위탁하는 경우 위탁 사실과 수탁자 정보 등을 정보 주체에게 알려야 하며, 필요한 경우 동의받아야 한다. 다섯 번째, 보유하는 개인정보에 대한 보유기간 설정 및 파기정책을 수립하고 보유기간이 경과되거나 목적 달성된 경우 지체 없이 개인정보를 파기하여야 한다. 개인정보처리자가 개인정보의 생애주기별로 처리 시에는 수집의 제한, 처리의 제한, 정확성・완전성 및 최신성, 안전한 관리, 공개, 생활 침해의 소화, 익명・가명화, 책임 및 의무 준수 등 1980년 OECD의 권고지침을 바탕으로 규정된 8가지 개인정보 처리의 원칙을 준수해야 한다는 내용으로 이루어져 있다.

본 연구에서 개발하고자 하는 개인정보 관리역량 성숙도 모델 중심으로 내용을 정리하면 <표 Ⅱ-3>과 같다.

<표 Ⅱ-3> 개인정보의 생애주기 주요 내용

생애주기	주요 내용	
수집	· 개인정보 수집의 적절성 · 개인정보 수집·이용 동의 방법의 적절성	
보유	· 저장기간 산정	
이용·제공	· 목적 외 이용·제공 제한 · 제공 시 안전성 확보 조치	· 위탁 계약 및 위탁 사실 공개 · 수탁자 대상 교육・관리 감독
파기	· 파기 계획 수립·시행 · 분리 저장 계획 수립·수행	· 파기 관리대장 기록 관리

2.1.3 개인정보의 안전성 확보 조치

개인정보의 안전성 확보 조치 기준은 개인정보 보호법 제29조, 개인정보 보호법 시행령 제30조를 근거로 개인정보처리자가 개인정보를 처리 함에 있어 개인정보가 위조·변조·분실·도난·유출 또는 훼손되지 않도록 기술·관리·물리적 안전 조치에 관한 기준을 정하여 2011년에 제정되었다. 2019년에는 개인정보 침해사고의 사전 예방과 사후 추적 관리를 강화하고자, 접속기록 항목을 육하원칙에 따라 구체적으로 명시하여 규정하고, 접속기록 보관 기간을 6월 이상 보관에서 모든 개인정보 처리시스템은 1년 이상, 5만 명 이상 개인정보의 처리 또는 민감정보, 고유 식별정보를 처리하는 시스템은 2년 이상 보관 등의 내용으로 개정되었다[23][24].

적용 대상으로는 개인정보처리자, 개인정보 취급자, 개인정보 처리 위·수탁자 등 개인정보 이해관계자가 준용하게 되어 있으며, 적용대상자는 개인정보를 처리할 때 기준에 명시한 내용은 반드시 준수해야 하는 최소한의 기준으로 마련되어 있다[23][24]. 개인정보의 안전성 확보 조치 기준의 주요 내용으로는 내부 관리계획의 수립·시행, 접근권한 관리, 접근통제, 개인정보의 암호화, 접속기록의 보관·점검, 악성 프로그램 방지, 관리용 단말기의 안전 조치, 물리적 안전 조치, 재해재난 대비 안전 조치, 개인정보의 파기 등이며[23][24], 본 연구에서 개발하고자 하는 개인정보 관리역량 성숙도 모델 중심으로 내용을 정리하면 <표 Ⅱ-4>와 같다.

<표 Ⅱ-4> 개인정보의 안전성 확보 조치 기준 주요 내용 정리

구 분	주요 내용	개인정보의 안전성 확보 조치 기준 조항
내부 관리계획의 수립·시행	· 개인정보 내부 관리계획 수립 · 내부 관리계획의 이행실태 연 1회 이상 점검 관리	제4조
접근권한 관리	· 업무담당자별 접근권한 차등 부여 · 접근권한 부여·변경·말소내역 기록 및 3년 이상 보관 · 계정·비밀번호의 일정 횟수 오류 시 접근제한 조치	제5조

구 분	주요 내용	개인정보의 안전성 확보 조치 기준 조항
접근통제	· 개인정보 취급자별 계정 발급 · 비밀번호 작성 규칙 수립·적용 · 불법적인 접근 및 침해사고 방지 대책 · 안전한 접속 수단·인증 수단 적용 · 개인정보 처리시스템의 접근통제 조치	제6조
개인정보의 암호화	· 개인정보 내부 관리계획 수립 · 내부 관리계획의 이행실태 연 1회 이상 점검·관리 · 고유 식별정보 저장 시 안전한 암호알고리즘 적용 · 비밀번호 저장 시 안전한 일방향 암호알고리즘 적용	제7조
접속기록의 보관 및 점검	· 개인정보 처리시스템의 접속기록 1년(또는 2년) 이상 보관·관리 · 접속기록 월 1회 이상 정기 점검 및 후속 조치 · 개인정보 다운로드 사유 확인 및 후속 조치 · 접속기록의 안전한 보관	제8조
악성 프로그램 방지	· 고유 식별정보 및 비밀번호 등 반출 시 안전한 알고리즘 적용 · 응용프로그램 또는 운영체제 SW의 수시 업데이트	제9조
관리용 단말기의 안전 조치	· 관리용 단말기에 대한 필수 안전 조치	제10조
물리적 안전 조치	· 개인정보 보관장소에 대한 물리적 출입 통제 · 보조 저장매체의 반출·입 통제	제11조
재해·재난 대비 안전 조치	· 개인정보 처리시스템의 보호 위한 위기 대응 매뉴얼 마련 및 점검 · 개인정보 처리시스템 백업 및 복구	제12조
개인정보의 파기	· 파기 계획 대비 개인정보의 안전한 파기	제13조

2.2 개인정보보호 법률과 제도

2.2.1 개인정보 보호법

가. 개인정보 보호법

개인정보 보호법은 2004년부터 논의가 이어졌는데, <표 Ⅱ-5>와 같이 2008년 이후 통신사와 포털, 유통사 등에서 대규모 개인정보 유출 사고의 발생으로 개인정보보호에 관한 일반법 제정 필요에 대한 사회적 공감대가 본격적으로 형성되면서 2011년 3월 29일, 공공과 민간을 모두 아우르는 개인정보보호에 관한 일반법이 제정됐다[26].

<표 Ⅱ-5> 개인정보 유출 관련 주요 사고 현황[27]
(출처 : 감사원, "2021 개인정보보호 추진실태 감사보고서" 인용)

업체	발생 연월	원인	피해 규모	유출정보
옥션	2008.1.	해킹	1,081만 명	성명, 주민등록번호, 주소 등
현대캐피탈	2011.4.	해킹	175만 명	성명, 주민등록번호, 연락처 등
SK커뮤니케이션즈	2011.7.	해킹	3,500만 명	성명, 주민등록번호, 연락처 등
넥슨	2011.11.	해킹	1,320만 명	아이디, 비밀번호(암호화) 등

2020년 2월 개정된 국내 개인정보 보호법은 총 10개 장과 76개 조로 <표 Ⅱ-6>과 같이 구성되어 있다.

<표 Ⅱ-6> 개인정보 보호법 주요 내용

원칙	법률 조항 및 주요 내용	8대 원칙	처벌규정
총칙	제2조(정의)	적용 대상	
개인정보 처리원칙	제3조(개인정보보호 원칙)	합법성 정당성 필요성 정보 주체의 동의	
	제16조(개인정보의 수집 제한)	수집 제한의 원칙	제75조
	제18조(개인정보의 목적 외 이용·제공 제한)	활용 및 제공 목적의 제한	제71조
	제19조(개인정보를 제공받은 자의 이용·제공 제한)		

원칙	법률 조항 및 주요 내용	8대 원칙	처벌규정
정보 주체의 권리	제4조(정보 주체의 권리) 제35조(개인정보의 열람) 제36조(개인정보의 정정·삭제) 제37조(개인정보의 처리정지) 제38조(권리행사의 방법 및 절차)	정보를 제공받을 권리 열람권 삭제권 정정권 처리 제한권 침해에 의한 구제권	제73조, 제75조
개인정보처리자의 의무	제15조(개인정보의 수집·이용)	정보 주체의 동의 정보를 제공받을 권리	제75조
	제17조(개인정보의 제공)		제71조
	제20조(정보 주체 이외로부터 수집한 개인정보의 수집 출처 등 고지)	정보를 제공받을 권리	
	제21조(개인정보의 파기)	처리 활동의 기록 및 유지	제73조
	제22조(동의를 얻는 방법)		제75조
	제23조(민감정보의 처리 제한)		제71조, 제73조
	제24조(고유 식별정보의 처리 제한)		
	제25조(영상정보처리기기의 설치·운영 제한)		제72조, 제75조
	제26조(업무위탁에 따른 개인정보의 처리 제한)		제75조
	제27조(영업양도 등에 따른		
	개인정보의 이전 제한)		
	제28조(개인정보 취급자에 대한 감독)		
	제28조의2 - 제28조의7(가명 정보의 처리)		제71조
	제29조(안전조치 의무)	기술적·관리적 및 물리적 조치	
	제30조(개인정보 처리 방침의 수립 및 공개)		제75조
	제31조(개인정보보호 책임자의 지정)	책임자 지정 의무	
	제32조(개인정보 파일의 등록 및 공개)		
	제32조의2(개인정보보호 인증)		
	제33조(개인정보 영향평가)		
	제34조(개인정보 유출 통지 등)	통지 및 신고 의무	
	제63조(자료 제출 요구 및 검사)	처리 활동의 기록 및 유지	

제1장은 총칙으로서 법률의 제정 목적 및 정의, 개인정보보호 원칙과 정보 주체의 권리를 규정하고 있으며, 제2장에서는 개인정보보호 정책의 수립으로써 정책 수립 및 관리·감독을 수행하는 독립기구로서의 개인정보보호위원회의 직무,

심의·의결사항 등 역할을 규정하고 있다[26].

제3장은 제15조부터 제34조까지 개인정보의 수집・이용, 제공, 위탁, 파기 등 각 개인정보의 처리단계별로 개인정보처리자의 의무를 규정하고 있다[26]. 각 의무에 대한 구체적인 절차와 적용 범위는 개인정보 보호법 시행령에서 정한다. 특히 제29조에서는 개인정보처리자가 “개인정보가 위조・변조・도난・분실・유출 또는 훼손되지 않도록 접속기록 보관, 내부 관리계획 수립 등 안전성 확보에 필요한 기술・관리・물리적 보호조치를 해야 한다.”라고 안전 조치 의무를 규정하고 있다[26]. 제31조는 개인정보보호 책임자의 지정 의무와 책임자가 수행하여야 할 업무를 규정하고 있다. 개인정보보호 책임자는 기관 내에서 개인정보보호 계획을 수립하고 이를 총괄적으로 시행하는 역할을 담당한다[26].

제32조는 공공기관의 개인정보 기록 운영 및 보관과 관련하여 처리 방법을 규정하고 개인정보보호위원회에 보고하도록 하였다.

제32조의2에서는 개인정보보호 인증제도를 개인정보보호위원회가 운영하고, 위원회가 지정한 전문기관이 인증업무를 수행하도록 하고 있다. 제33조는 개인정보 영향평가 관련 내용이 규정되고, 공공기관을 대상으로 영향평가를 의무화하였으며, 영향평가 결과를 개인정보보호위원회에 제출하도록 하였다.

제34조는 개인정보 유출 시 신고 및 통지 의무를 규정하였다. 개인정보유출 사실을 인지한 경우, 개인정보처리자는 그 사실을 해당 정보 주체에게 즉시 통지하여야 한다. 또한, 시행령 제39조 제1항에 의하여 1천 명 이상 개인정보가 유출될 경우, 개인정보처리자는 해당 사실을 지정된 전문기관에 신고하여야 한다.

제4장에서는 개인정보처리자에 대하여 정보처리의 전 단계별로 구체적인 의무를 부과하고 있으며, 제5장은 앞서 제4조에서 규정한 정보 주체의 권리를 보장하기 위한 구체적인 내용을 규정하였다. 이번 개정안에서 신설된 제6장은 대부분 기존 정보통신망법에서 이번 데이터 3법 개정을 통해 개인정보 보호법과 중복된 내용을 삭제하고 개인정보 보호법으로 이관된 것으로써, 정보통신 서비스 제공자에 대한 개인정보 처리 등의 특례를 규정하고 있다.

제7장은 개인정보 분쟁조정, 제8장은 단체소송에 관한 내용으로, 정보 주체가 피해받은 경우의 구제 절차를 포함하고 있다.

정보 주체의 권리는 개인정보 보호법 제4조에 규정되어 있으며, 정보를 제공받

을 권리, 개인정보 수집 시 처리 동의 여부 및 동의 범위 등을 결정할 권리, 정보 주체의 개인정보에 대한 열람권, 삭제 및 정정권, 침해 발생 시 구제를 요청할 권리로 구성되어 있다.

<표 Ⅱ-7> 개인정보 보호법상 정보 주체의 권리보장 내용

구 분	주요 내용
정보를 제공받을 권리	개인정보의 처리에 관한 정보를 제공받을 권리
열람권	개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람을 요구할 권리
처리 제한권	개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리
삭제권・정정권	개인정보의 처리정지, 정정・삭제 및 파기를 요구할 권리
침해에 의한 구제권리	개인정보 처리로 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리

EU의 GDPR은 정보 주체의 권리를 보장해야 할 의무를 자세하게 다루고 있는데, 합법성, 공정성 및 투명성, 목적 제한, 데이터 최소화, 정확성, 동의, 계약, 통보받을 권리, 액세스 권한, 수정 권리, 처리 제한 권리, 반대할 권리 등 기존 개인정보 보호법에서 다루어지고 있던 영역들도 있지만, 잊힐 권리, 데이터 이동권리, 프로파일링을 포함한 자동화된 의사결정과 관련된 권리와 같은 새로운 개념들이 도입되었다.

첫 번째, 정보를 제공받을 권리는 정보 주체가 제공한 정보가 어디서 어떻게 처리되는지를 적법성, 투명성, 공정성에 따라 알기 쉽게 제공받을 수 있는 권리를 의미한다.

개인정보 보호법에서는 정보 제공의 방법에 대해 정보 주체가 알기 쉽게 글자 크기 및 굵기, 색상 등을 통해 다른 정보와 구분하여 식별할 수 있도록 하고 있으며, GDPR에서는 “간결하고 투명하며 명확하고 이해하기 쉬운 언어를 사용”하도록 하고 있다. 아동에게 정보를 제공할 때 아동이 이해할 수 있는 수준으로 그림, 표현 등을 통해 제공하도록 GDPR에서는 규정하고 있다.

두 번째, 정보 주체의 열람권은 정보 주체가 개인정보가 어떻게 처리되고 있는

지 접근하여 열람할 수 있는 권리를 의미한다[25].

세 번째, 처리 제한권은 정보 주체의 요청이 있는 경우, 개인정보처리자는 정보를 보유만 할 수 있으며 추가적인 처리를 제한해야 하는 권리를 의미한다. 개인정보 보호법에서는 개인정보 처리 동의 여부, 동의 범위 등을 선택하고 결정할 권리로 의미하고 있으며, GDPR에서는 정보 주체가 정보 주체의 정보를 처리 제한 요청 시 개인정보 보유 상태를 유지할 수 있으며, 이 외에는 처리하지 못하도록 하고 있다.

네 번째, 삭제·정정권은 개인정보의 삭제 및 파기, 처리정지, 정정을 요구할 권리를 의미한다. GDPR에서는 아동 수준에 맞는 삭제 권리의 행사 방법을 제공하고 있으며, 국내에서도 아동이 아닌 나이가 도래할 시 정보 주체와 보호자에게 권리에 대해 사전 고지 방식으로 개선을 제안한 연구가 있다[25].

마지막으로 침해에 의한 구제권리는 개인정보의 처리로 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리를 의미한다[25].

2.2.2 국외의 개인정보보호 관련 법률 및 제도 현황

각국의 개인정보보호제도는 해당 국가의 법체계와 문화적 특성에 따라 상이하지만, 대다수 국가의 개인정보보호제도는 1980년 경제협력개발기구(OECD)에서 발표한 '프라이버시 보호와 국가 간 이동에 대한 가이드라인'에 기초하고 있다[28]. 이 가이드라인은 전 세계가 개인정보 보호법을 마련하게 되는 기틀이 되었으며, 특히 여기에서 규정한 개인정보보호의 8가지 원칙은 현재까지도 대부분 국가의 법령에서 널리 활용되고 있다[29].

OECD는 개인정보보호의 원칙을 수집의 제한, 정보의 정확성, 목적의 명확성, 이용의 제한, 안전성의 보호, 정보 공개, 개인 참여, 책임성의 8가지로 정하고, 회원국들이 이러한 원칙에 근거하여 개인정보보호제도를 마련할 것을 권고하였다. 이는 국내 개인정보 보호법에도 반영되었으며, 개인정보보호 원칙을 규정한 제3조에서는 OECD 권고안[28]에 기초하여 <표 Ⅱ-8>과 같이 수집 제한의 원칙, 이용의 제한 등 8가지의 개인정보보호 원칙을 규정하고 있다.

<표 Ⅱ-8> OECD 개인정보보호의 8원칙[28](출처 : The OECD Privacy Framework(2013))

원칙	상세내용
수집 제한의 원칙	개인정보의 수집은 제한되어야 하며, 수집하는 경우 합법적이고 공정한 절차에 따라 정보 주체에게 알리거나 동의받아야 함
정보 정확성의 원칙	개인정보는 그 이용 목적에 부합하는 것만 수집하고, 목적에 필요한 범위 내에서 정확하고 완전하며 최신의 상태를 유지해야 함
목적 명확성의 원칙	개인정보 수집 목적은 수집하기 이전 또는 당시에 명시되어야 하고, 명시된 목적으로만 이용해야 함
이용 제한의 원칙	개인정보는 수집된 목적으로만 이용해야 하며, 목적 이 외로는 이용할 수 없음(단, 정보 주체에게 별도 동의받거나 법률에 따라 허가된 경우는 제외)
안전성 보호의 원칙	개인정보의 분실, 불법적인 접근・훼손・사용・변조・공개 등의 위험에 대비하여 합리적인 보호조치를 마련해야 함
공개의 원칙	개인정보 관리자의 주소 등을 비롯하여 개인정보의 이용목적, 관련된 정책 등의 내용이 포함된 공개방침이 있어야 함
개인 참여의 원칙	정보 주체는 본인의 개인정보 확인, 열람 요구, 이의제기 및 정정, 삭제, 보완 청구권을 가짐
책임의 원칙	개인정보 관리자는 위에서 제시한 원칙들이 지켜지도록 필요한 제반 조치

가. EU

유럽연합은 회원국 간의 개인정보보호 법체계를 조화롭게 통일하기 위하여 1995년「개인정보보호에 관한 유럽연합과 각료회의 지침(95/46/EC)」을 제정하였다. 이를 'Directive 95'라 부르기도 한다. 이후 정보통신 분야에 대하여 1997년「신부문의 개인정보 처리 및 프라이버시 보호에 관한 유럽의회와 이사회 지침」을 제정하였고, 2002년에는 스팸과 위치정보와 관련된 내용을 추가하여「전자통신 부문에서의 개인정보 처리 및 프라이버시 보호에 관한 유럽의회와 이사회 지침」을 제정하였다.

EU의 개인정보보호 지침은 강제력을 지니지는 않지만, EU 회원국에게 개인정보보호에 대한 통일된 입법기준을 제시하는 것에서 의미를 찾을 수 있다. 특히 해당 지침에 부합하는 보호 체계를 갖추지 않은 나라에 대해 개인정보의 국외 이전을 엄격히 제한하고 있다는 점도 특징으로 들 수 있다. 'Directive 95'는 개인정보처리자의 의무, 정보 주체의 권리, 개인정보의 국외 이전, 개인정보 전담 기

구 설치 등을 규정하고 있다.

한편, EU는 2016년 4월 'Directive 95'를 새롭게 개정한 「개인정보보호에 관한 유럽연합과 각료이사회의 규정」을 채택하였다. 'General Data Protection Regulation(GDPR)'이라고 부르는 이 규정은 2018년부터 시행하였다. 'Directive 95'와 달리 강제력이 있는 GDPR는 개인정보를 국외로 이전하는 경우 규정 위반에 대한 처벌과 정보 주체의 권리를 한층 강화하는 등 개인정보보호에 관해 더욱 엄격한 규정을 EU 전역에 일관성 있게 적용하고 있다.

<표 Ⅱ-9> GDPR 주요 내용

원칙	법률 조항 및 주요 내용	8대 원칙	처벌 규정
총칙	제2조(정의)	적용 대상	
General Provisions	제1조(주제 및 목적)		
	제2조(물적 범위)	적용 범위	
	제3조(지리적 범위)		
	제4조(정의)		
Principles	제5조(개인정보 처리 관련 원칙)		제83조 제5항
	제6조(처리의 적법성)	적법성	
	제7조(동의의 조건)	수집 시 정보 주체의 동의	
	제8조(아동의 동의에 적용되는 조건)		제83조 제4항
	제9조(민감정보 처리)	민감정보	제83조 제5항
	제10조(범죄경력 및 범죄행위에 관한 개인정보의 처리)	범죄 개인정보	
	제11조(신원확인이 필요 없는 개인정보의 처리)		제83조 제4항
Rights of the Data Subject	제12조(개인정보 주체 권리행사를 위한 투명한 정보 통지, 형식)	정보를 제공받을 권리	제83조 제5항
	제13조(개인정보가 정보 주체로부터 수집되는 경우 제공되는 정보)		
	제14조(개인정보가 정보 주체로부터 수집되지 않는 경우 제공되는 정보)		
	제15조(정보 주체 열람권)	열람권	
	제16조(정정권)	정정권	
	제17조(삭제권)	삭제권	
	제18조(처리의 제한권)	처리 제한권	

원칙	법률 조항 및 주요 내용	8대 원칙	처벌 규정
	제19조(정정, 삭제, 처리 제한 고지)	고지의무	
	제20조(개인정보 이전권)	이전권	
	제21조(반대할 권리)	반대권	
	제22조(프로파일링 등 자동화된 개별 의사결정)	프로파일링권	
	제23조(제한)		
Controller and Processor	제24조(컨트롤러의 책임)	행정적·기술적·물리적 조치	제83조 제4항
	제25조(설계, 기본 설정에 의한 개인정보 보호)		
	제26조(공동 컨트롤러)		
	제27조(컨트롤러, 프로세서의 대리인)	책임자 지정 의무	
	제28조(프로세서)		
	제29조(컨트롤러 또는 프로세서의 책임하에 처리)	책임자 지정 의무	
	제30조(정보처리 활동의 기록)	처리 활동의 기록 및 유지	
	제31조(감독기구와의 협력)		
	제32조(정보처리의 안전)	기술적 · 조직적 조치	
	제33조(감독기관에의 개인정보 유출 통지)	통지 의무	
	제34조(이용자에의 개인정보 유출 통지)		
	제35조(정보보호 영향평가)		
	제36조(사전 자문)		
	제37조(DPO의 지정)	책임자 지정 의무	
	제38조(DPO의 지휘)		
	제39조(DPO의 업무)		
	제40조(행동강령)		
	제41조(승인된 행동강령의 모니터링)		
	제42조(인증)		
	제43조(인증기관)		

나. 미국

미국은 공공부문에 대해서만 1974년 제정된 「프라이버시법(Privacy Act of 1974 of the United States)」을 두고 있으며, 민간부문에 대해서는 별도로 법률을 두고 있지 않다. 민간부문에 대해서는 자유로운 정보유통과 국제무역을 확보하고자 개인정보보호 자율규제 방식을 취하고 있다. 금융기관이나 온라인거래상 등 특별히 개인정보의 보호가 필요한 분야에 대해서는 영역별로 개별법을 제정하여 개인정보를 보호하고 있는데, 이와 같은 자율규제 방식은 구체적으로 보호가 필요한 부분에만 한정하여 규제함으로써 최대한 정보유통의 진입장벽을 낮추고자 하는 데 목적이 있다.

그러나 미국의 개별법 체제는 1995년 EU 지침이 제정되면서 영향을 받게 되었다. EU 지침 제25조에 따라 적정성 평가를 통과하지 못한 국가는 EU와의 자유로운 개인정보 이전이 불가능한데, 미국은 민간부문을 포괄하는 호법이 제정되어 있지 않기 때문에 개인정보 유통에 제한이 생기게 되었다. 이에 미국은 EU 지침에 따른 적정성 수준을 보장하는 새로운 개인정보보호조치로 '세이프 하버 원칙'을 해결방안으로 제시하였고, EU는 미국의 세이프 하버 원칙이 EU의 적정성 기준에 부합한다고 판단하였다.

이로써 미국은 EU 회원국의 개인정보를 EU 수준으로 보호해주면서 EU와의 무역마찰을 피하고, EU 이외의 국가들과는 본래대로 자유로운 무역과 개인정보 유통을 유지할 수 있게 되었다.

그러나 2015년 10월, 유럽최고재판소(CJEU)는 양측의 정보공유 협약인 '세이프 하버' 조약을 무효화해 페이스북과 구글 등 미국 정보기술(IT) 기업이 본사 내 서버에 정보를 저장하는 것이 금지됐다. 이에 EU와 미국은 2016년부터'EU·미국 기밀 보호(EU-US Privacy Shield)' 협약을 새롭게 체결하기 위해 준비 중이다. 새 협약에는 EU 이용자들이 제기한 불만이 제대로 처리되지 않으면 미국의 옴부즈맨이 적극적으로 협조하게 하고 있으며, 미국의 기업들이 EU 내 정보보호 기준과 유사한 기준을 적용하고 있는지에 대한 정기 검열도 받도록 하는 내용이 포함되어 있다.

다. 일본

일본은 공공분야의 개인정보에 대해 「행정기관이 보유하는 개인정보의 보호에 관한 법률」, 「개인정보보호에 관한 법률」, 「독립행정법인 등이 보유하는 개인정보의 보호에 관한 법률」, 「각 지방자치단체가 보유하는 개인정보에 관한 조례」, 「마이넘버법」 등이 존재한다. 또한, 일본의 각 정부 부처는 소관 사업 분야별로 사업자들이 준수해야 할 개인정보보호 가이드라인을 제정하여 배포한다.

일본의 「개인정보보호에 관한 법률」은 2003년 5월에 제정되었으며, 정보통신사회의 발전에 따라 개인정보의 이용이 확대되고 있는 것에 비추어 개인정보의 유용성을 배려하면서 개인의 권리·이익을 보호하기 위함을 목적으로 하고 있다. 이 법에서는 개인정보보호에 관한 정책의 기본이 되는 사항을 정하고 국가와 지방공공단체의 책무 등을 명확화하는 동시에 개인정보 취급사업자의 준수 의무 등을 정하고 있다. 일본의 개인정보보호 관련 법률들은 'OECD 프라이버시 8원칙'을 수용하여 해당 원칙들을 구현하는 것에 중점을 두고 있다.

한편, 정보기술(IT) 발달에 따른 환경 변화에 대응하기 위하여 2015년 9월 「개인정보보호에 관한 법률」이 개정되었다. 이번 개정에는 개인정보의 정의 조항에 개인식별부호, 민감정보 등을 포함시켜 개인정보의 개념을 더욱 구체화하였다. 또한, 개인정보를 특정 개인이 식별되지 않는 형태로 가공한 '익명가공 정보'조항을 도입하여 빅 데이터 산업 등에 활용 가능성을 높였다. 아울러 개인정보 제3자 제공 기록을 의무화하여 개인정보의 보호 수준을 제고하였다. 개인정보보호위원회를 신설하고 권한을 강화하여 보다 일원화된 개인정보보호 시스템을 구축하였다. 그 외에도 개인정보의 국외 이전에 관한 규정을 정비하고 소규모개인정보처리자에 대해서도 법 적용을 확대하는 등 변화가 있었다.

2.3 개인정보보호 역량성숙도 모델

2.3.1 성숙도 모델

성숙도 모델은 조직의 경영시스템에 대한 현재 수준을 진단하고, 개선의 방향성을 제시하여 주는 평가도구라고 한다. 성숙도 모델의 목표는 프로세스의 효율적 관리와 이를 통한 업무성과 향상이고, 궁극적으로 업무 프로세스에 대한 조직의 관리능력을 높이는 데 있다. 본 모델을 통한 성숙도의 측정과 개선 활동은 업무에 대한 통합적 수행 능력과 개선 능력을 확보하게 함으로써 이러한 목표 달성을 가능하게 한다.

가. ISM3 & CMMI

ISM3(Information Security Management Maturity Model)은 2004년 ISECOM(Institute for Security and Open Methodology)의 Vicente Aceituno Canal가 발표하였으며, 정보보호의 일반적인 프로세스에 초점을 맞춘 것으로 정보보호 관리체계에 관한 이론과 실무 간의 갭을 줄이고, 성숙도 모델과 보안관리를 연결하고자 하였다. ISM3은 일종의 품질시스템으로서 정보보호를 품질 이슈로 보고, 프로세스에 대한 문서화가 필수로 요구한다. 이러한 품질 접근방법은 정보보호와 관련된 공격이나, 사고, 오류 등이 발생하는데도 불구하고 신뢰감을 줄 수 있다. 또한, ISM3은 위험평가를 요구하지 않는 대신에 위험 관리를 수행함으로써 지속적인 프로세스 개선이 가능하다. ISM3은 정보보호를 프로세스의 결과로 간주하고 관리 프로세스의 역량을 측정할 수 있는 8가지의 척도를 제시한다. 그리고 5등급의 정보보호 프로세스 역량성숙도를 기반으로 조직의 특성을 고려한 5등급의 조직 성숙도 수준을 제시한다[30].

CMMI(Capability Maturity Model Integration)는 기존부터 소프트웨어의 품질보증 기준으로 널리 이용되고 있는 업무 능력 및 성숙도 평가 모델인 CMM의 후속 모델이다. CMMI는 미국국방부의 지원 아래 카네기 멜론 대학 소프트웨어

공학 연구소가 공동으로 SW-CMM과 SE-CMM 등의 요소를 통합 개발한 것이다. CMMI의 목적은 SW 제품 또는 서비스의 개발, 획득, 유지관리를 위한 조직의 공정 및 관리능력 향상을 위한 가이드를 제공하는 데 있다.

ISM3은 CMMI나 COBIT 등과 같이 프로세스 기반의 접근법을 사용하는 모델로써 총 46개의 프로세스를 일반적(Generic), 전략적(Strategic), 전술적(Tactical), 운영적(Operational) 등 4가지 영역으로 분류하고 있다[30].

첫 번째는 전략적(지시 및 제공) 요소로 정보보호나 물리적 보안 등에 대한 리더십과 서로 간의 조화를 제공하고, 정보보호 관리체계에 대한 검토 및 개선 등을 수행한다. 두 번째는 전술적(구현 및 최적화) 요소로 운영관리를 위한 환경을 정의하고, 보안 목표를 정의하며, 이를 달성하기 위한 적절한 프로세스 선택을 수행한다. 세 번째는 운영적(실행 및 보고) 요소로 자산을 식별 및 보호하고, 생명주기 통해 정보시스템을 보호 및 개선하여 효율적이고 효과적으로 자원을 할당한다. 또한, ISM3은 <표 Ⅱ-10>과 같은 문서화, 활동, 범위, 비 가용성, 효과성, 자원 사용 비율, 합목적성, 효율성의 8가지 척도(Metrics)를 사용하여 정보보호 프로세스를 관리함으로써 관리자는 결과를 손쉽게 살펴볼 수 있으며, 결과가 조직에 가져오는 이익을 파악하고, 프로세스의 변경이 해당 프로세스를 얼마나 개선하게 되는지 점검할 수 있다.

<표 Ⅱ-10> ISM3의 성숙도 수준

수준	역량 수준	요구되는 척도
1	기초	문서화
2	정의	기초 수준 + 활동, 범위, 비 가용성, 효과성
3	관리	정의 수준 + 자원 사용 비율
4	통제	관리 수준 + 품질(합목적성)
5	최적화	통제 수준 + 효율성

다음의 <표 Ⅱ-11>은 앞서 일반적, 전략적, 전술적, 운영적 등 4가지 영역으로 분류되어 제시된 46개의 프로세스에 대해 조직 성숙도 달성을 위해 요구되는 프로세스 역량성숙도 수준을 나타낸 것으로 최소한 관리 수준을 요구하고 있다. ISM3에서는 5단계의 정보보호 성숙도를 측정하도록 성과 측정 항목으로는 경영진 보고, 자원할당, 개발 보안, 인적 보안, 접근통제, 포렌식, 첩보 등 7개의 측정 항목을 제시하고 있다.

<표 Ⅱ-11> 조직별 정보보호 프로세스 역량성숙도

측정 항목	Basic Level	SME Level	eCommerce Level	Enterprise Level
전략적 관리자에게 보고	관리	관리	관리	관리
정보보호를 위한 자원할당	관리	관리	관리	관리
시스템개발 생명주기 통제	-	-	관리	관리
인적 보안	-	-	-	관리
접근통제	-	관리	관리	관리
포렌식	-	-	-	관리
첩보	-	-	-	-

나. 업무 연속성 성숙도 모델(BCMM)

업무 연속성 성숙도 모델(Business Continuity Maturity Model)은 1997년에 조직의 업무 연속성을 위한 역량성숙도 모델의 필요성을 느껴 5년여에 걸친 연구 및 조사를 통해 개발된 것으로 2001년 미국 Virtual Corporation의 Scott Ream에 의해 Contingency Planning & Management Conference에서 처음으로 발표됐다.

BCMM은 총 6등급의 성숙도 수준과 각 성숙도 수준의 특징을 구분하는 공통적인 속성인 8개의 조직 역량(Corporate Competencies)으로 아래의 <표 Ⅱ-12>와 같이 총 6등급의 성숙도 수준을 사용하고 있다. 특히 BCMM에서는 1~3등급의 성숙도 수준을 '프로그램 기초(Program Basic)' 단계라 하여 전사적 차원의 업무 연속성 프로그램이 적절히 수립되어 있지 않은 조직을 나타내고, 4~6등급의 성숙도 수준을 '프로그램 개발(Program Development)' 단계로 전사적 차원의 업무 연속성 프로그램을 수립하고 자체적인 개선 능력을 갖춘 조직을 나타낸다[31].

<표 Ⅱ-12> BCMM의 업무 연속성 성숙도 모델

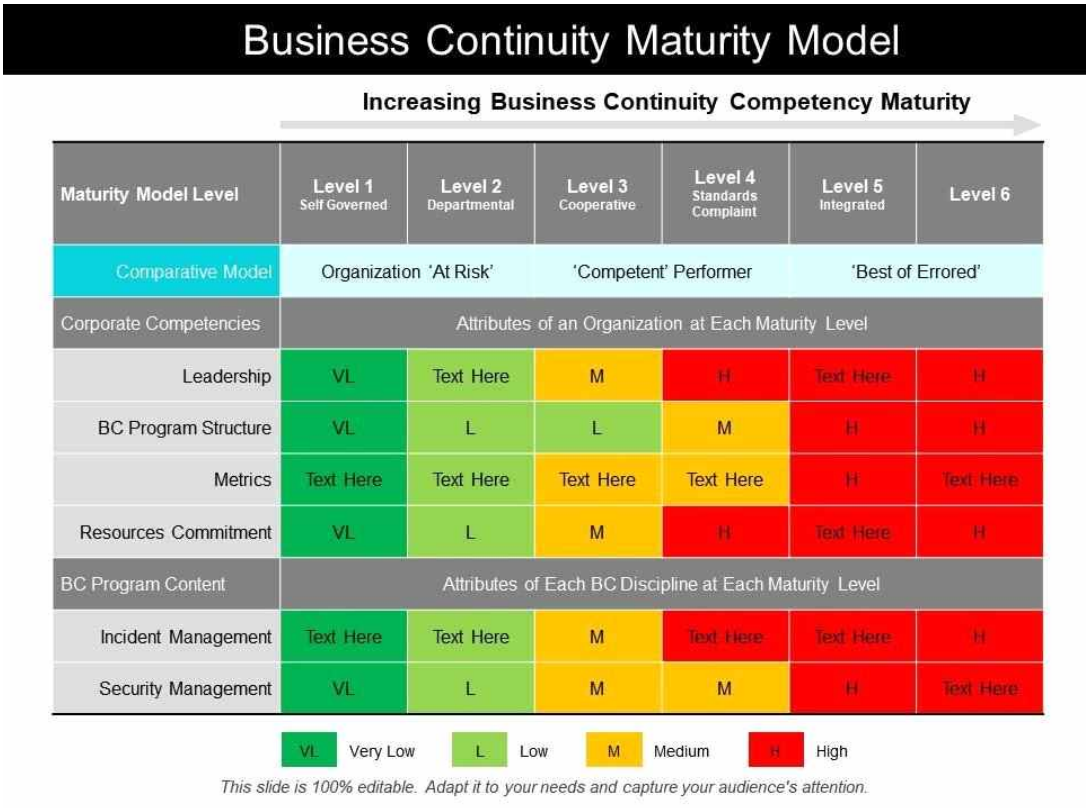
BCMM 성숙도 수준	Program Basics			Program Development		
	경영자 지원	전문가 지원	관리	모든 담당자 참여	통합 계획	Cross-Punctional
1등급(Self Governed)	×	×	×	×	×	×
2등급(Departmental)	Marginal	Partial	×	×	×	×
3등급(Cooperative)	Partial	○	Partial	×	×	×
4등급(Standards Complaint)	○	○	○	○	×	×
5등급(Integrated)	○	○	○	○	○	×
6등급	○	○	○	○	○	○
업무 연속성 능력 성숙도 증가 →						

BCMM은 다음의 <표 Ⅱ-13>에서 보는 바와 같이, 6등급의 성숙도 수준과 함께 총 8가지의 조직역량과 관련된 속성을 정의하고 4점 척도(High, Medium, Low, Very Low)로 점수를 부여하였다[31].

<표 Ⅱ-13> BCMM 성숙도 모델

측정 항목	1등급	2등급	3등급	4등급	5등급	6등급
리더십	VL	L	M	H	H	H
임직원 인식 수준	VL	L	L	M	H	H
BCM 프로그램 구조	VL	L	L	M	H	H
프로그램 보급도	VL	L	L	L	M	H
척도	VL	L	M	M	H	H
자원 지원	VL	L	M	H	H	H
외부 협력체계	VL	L	L	M	H	H
BCM 프로그램 콘텐츠	VL	L	M	H	H	H
업무 연속성 능력 성숙도 증가 →						

BCMM은 조직의 업무 연속성을 위해 개발된 성숙도 모델이지만 업무 연속성 계획이나 재난복구계획 모두 정보보호 계획의 일부분으로 볼 수 있으므로 정보보호 계획 수립 시 적용이 가능하다.



[그림 Ⅱ-2] BCMM의 예시[76]

BCMM은 6단계의 성숙도 수준과 각 성숙도 수준의 특징을 구분하는 공통적인 속성인 8개의 조직 역량(리더십, 임직원 인식 수준, BC 프로그램 구조, 프로그램 보급도, 척도, 자원 지원, 외부 협력체계, BC 프로그램 콘텐츠)을 제공함으로써 조직의 현재 성숙도 수준의 평가 및 목표 수준 설정을 쉽게 한다.

2.3.2 프라이버시 중심 설계(PbD : Privacy by Design)

프라이버시 중심 디자인(PbD : Privacy by Design)은 기존에 건축 분야에서 사용되었으며, 1990년대 중반에 캐나다 온타리오주 정보 프라이버시 위원회의 Ann Cavoukian 박사가 주장한 개념으로서 개인정보를 취급하는 모든 측면에 있어 개인정보보호가 적절하게 이루어지는 환경을 '사전적'으로 조성하는 것을 의미한다[32].

Ann Cavoukian 박사는 Privacy by Design을 '개인정보보호를 고려한 설계'로 개인정보 침해사고 발생 이후에 조치하는 것이 아니라 사전에 개인정보 침해 위협을 예측하거나 가능성을 대비하여 서비스 기획·설계 단계 등 사전 예방하는 개념이라고 설명하였다[32][33].

가. Privacy by Design 7대 기본원칙

프라이버시 중심 디자인의 목적은 프라이버시를 확보하는 것과 자기 정보 결정권을 가지는 것, 조직을 위해 지속 가능한 경쟁적 이점을 갖는 것, 그리고 이것은 <표 Ⅱ-14>와 같이 7대 기본원칙에 의해 달성될 수 있다. 이 원칙은 모든 종류의 개인정보에 적용된다.

<표 Ⅱ-14> PbD의 7대 기본원칙[34]
(출처 : 개인정보보호위원회, "자동 처리되는 개인정보보호 가이드라인" 인용)

구분	원칙	내용
1	사후 조치가 아닌 사전 예방	프라이버시 침해사고 발생 후 조치하는 것이 아닌 침해사고를 예측하고 사전 예방하는 것
2	초기설정부터 프라이버시 보호조치	정보시스템 또는 사업 진행 과정에서 개인정보 보호를 위한 설정을 기본으로 하여 자동으로 프라이버시가 최대한 보장되도록 하는 것
3	프라이버시 보호를 내재한 설계	설계에 프라이버시 보호를 내재화함으로써 프라이버시를 정보시스템 또는 개인정보의 처리와 통합 및 적용하도록 하는 것
4	프라이버시 보호와 사업기능의 균형	서비스 제공을 위한 가용성, 기밀성, 무결성 중 어느 하나도 포기하지 않고 프라이버시의 안전한 보호와 사업의 기능성 두 가지 모두 확보하기 위해 노력하는 것
5	개인정보 생애주기 전체에 대한 보호	개인정보의 생애주기 전 단계에 걸쳐 보호될 수 있도록 안전 조치를 적용하는 것
6	개인정보 처리 과정에 대한 가시성 및 투명성 유지	개인정보의 처리 과정에 대해 정보 주체가 완전하고 명확하게 이해하도록 하여 신뢰성을 제고시키는 것
7	이용자 프라이버시 존중	프로세스, 프로그램 등에 명시적인 보호 체계가 없더라도 이용자의 프라이버시를 보장하기 위한 활동을 수행하는 것

첫 번째 원칙은 "사후적이 아닌 사전적, 구제책이 아닌 예방적인 것"이어야 한

다. 프라이버시 중심 디자인은 수동적인 것이 아니라 선견적으로 대응하는 것이 특징이다. 프라이버시 침해가 발생하기 전에 그 침해를 예상하고 예방하는 것을 목적으로 한다. 이 때문에 사후가 아닌 사전에 작용하는 것이다.

두 번째 원칙은 “프라이버시 보호는 초기설정에서 유효화되는 것”이다. 프라이버시 보호의 구조는 시스템에 최초부터 설계된다. 개인 데이터는 개인이 아무것도 하지 않아도 그대로 보호된다. 개별적 조치는 불필요하다.

세 번째 원칙은 “프라이버시 보호의 구조가 시스템의 구조에 포함되는 것”이다. 프라이버시 보호의 구조는 IT시스템 및 비즈니스 관행의 디자인 및 구조에 포함된다. 사후적으로 부가 기능을 추가하는 것이 아니다. 즉, 프라이버시 보호의 구조는 IT시스템 및 비즈니스 관행에 불가결한 중심적 기능이 된다.

네 번째 원칙은 “전 기능적인 것과 제로섬(Zero-sum)이 아닌 포지티브섬(Positive-sum)”이다. 프라이버시 중심 디자인에서는 프라이버시 보호의 구조를 설계하는 것으로 편리함을 방해하는 등의 관계를 만드는 제로섬의 접근이 아닌, 모두 정당한 이익 및 목표를 거두는 포지티브섬 접근을 지향한다.

다섯 번째 원칙은 “데이터는 라이프사이클 전반에 걸쳐 보장될 것”이다. 프라이버시 정보는 생성되는 단계부터 폐기되는 단계까지 보안이 철저하게 지켜져야 한다. 모든 데이터는 데이터 라이프 사이클 관리하에 안전하게 보유되고 그 과정의 종료 시에는 확실하게 폐기된다.

여섯 번째 원칙은 “프라이버시 보호의 구조와 운용은 가시화되어 투명성이 확보될 것”이다. 어떠한 비즈니스 관행 또는 기술이 관계되고 프라이버시 보호의 구조가 제대로 기능하는 것을 모든 관계자에 의해 보증한다. 이때, 시스템의 구성 및 기능은 이용자, 제공자에게 항상 가시화되고 검증 가능해야 한다.

마지막 원칙은 “이용자의 프라이버시를 최대한 존중하는 것”이다. 설계자, 관리자에 대해 프라이버시 보호를 실현하기 위한 강력하고 표준적인 수단과 적절한 통지 및 권한 부여를 간단하게 실현할 수 있도록 옵션 수단을 제공하고, 이용자 개인의 이익을 최대한 유지한다.

다. EU GDPR의 PbD 원칙 적용 사례

EU는 AI, IoT, 빅 데이터 등 신기술로 인한 개인정보의 위협에 대응하기 위해 가장 적합한 프라이버시 보호 방안으로 'Privacy by Design' 적용을 GDPR 제25조에 규정하였는데, 주요 내용은 <표 Ⅱ-15>와 같다.

<표 Ⅱ-15> PbD 적용한 GDPR 제25조 주요 내용[34]
(출처 : 개인정보보호위원회, "자동 처리되는 개인정보보호 가이드라인" 인용)

구분		내 용	비고
1	①	개인정보 처리의 성격과 범위, 상황, 목적, 최신 기술과 비용 등을 포함하여 처리로 인해 개인의 권리와 자유에 대해 발생 가능한 위험성을 고려	권리와 자유 침해 방지
	②	컨트롤러는 처리 수단을 결정한 시점 및 처리 당시 시점에서 데이터 처리 최소화 등 개인정보보호 원칙을 효과적인 방식으로 이행하고 GDPR의 요건을 충족하여야 함	처리 최소화
	③	정보 주체의 권리를 보호하기 위한 적절한 기술 및 관리 조치를 이행하여야 함	정보 주체 권리보호 및 안전조치
2	①	컨트롤러는 기본 설정을 통해, 개별적인 특정 목적에 따라 필요한 정도에 한하여 개인정보가 처리될 수 있도록 보장하기 위한 적절한 기술 및 관리 조치를 이행하여야 함	기본 설정에 의한 개인정보 보호
	②	Data Protection by Default는 수집되는 개인정보의 양, 해당 처리의 범위, 개인정보의 보관 기간 및 접근 가능 기간을 설정하는 시점에 적용하여야 함	적용 부분 및 시점
	③	개인정보가 정보 주체의 개입 없이 불특정 다수에게 열람되지 않도록 기본 설정을 통해 보장	접근제한

라. EU ENISA의 'Privacy by Design 적용을 위한 8가지 핵심 전략'

EU ENISA는 개인정보보호를 위한 다양한 접근방법, 전략, 기술적 요소 등을 검토하는 것을 목적으로 Privacy by Design을 적용하려는 사업자를 위해 8가지 핵심 전략을 <표 Ⅱ-16>과 같이 제시하였다.

<표 Ⅱ-16> PbD 적용을 위한 8가지 핵심 전략[34]
(출처 : 개인정보보호위원회, "자동 처리되는 개인정보보호 가이드라인" 인용)

구분	원칙	내용
①	최소화	프라이버시 침해 가능성을 최소화하기 위해 개인정보의 명확한 활용목적에 따라 처리되는 개인정보의 양을 최소화하여야 함
②	숨기기	개인정보가 처리되는 과정에서 평문 전송 등으로 인해 외부에서 해당 내용을 볼 수 없도록 조치하여야 함
③	분리	개인에 대한 다양한 정보들을 가능한 한 분리해서 저장하여 하나의 DB에서 한 사람이 식별되지 못하도록 하여야 함
④	총계화	많은 양의 개인정보를 처리할 경우, 가능한 한 개인이 식별되지 않도록 식별자를 최소화하고, 처리 결과는 범주화 등을 통해 개인 식별 불가능하여야 함
⑤	정보제공	어떤 정보가 어떤 목적으로 어떻게 사용되는지 등 개인정보 처리 과정 전반에 대해 정보 주체가 투명하게 알 수 있도록 제공하여야 함
⑥	통제	'⑤정보제공' 전략 적용을 기반으로 정보 주체가 개인정보 처리 과정 전반에 대해 명확하게 이해하여 자기 개인정보의 잘못된 활용이나 보안 수준에 대해 권리 행사가 가능하여야 함
⑦	집행	내부 개인정보보호 정책은 법·제도 의무사항을 모두 반영하여야 하며, 강제적으로 시행되어야 함
⑧	입증	컨트롤러는 내부 개인정보보호 정책이 효과적으로 운영되고 있고, 데이터 유출 사고에 즉시 대응 가능 등 법적 의무사항을 준수하고 있다는 입증할 수 있어야 한다.

2.3.3 ISO/IEC27701

ISO/IEC 27701:2019는 ISO(International Organization for Standardization: 국제 표준화 기구)에서 2019년 8월 발표한 국제 표준으로 정보보호 관리체계(ISMS)의 요구사항을 규정한 국제 표준인 ISO/IEC27001과 이를 기반으로 경영 시스템을 구현하고 유지하기 위한 지침인 ISO/IEC 27002의 확장판이다[8]. ISO/IEC 27001에서 요구하는 ISMS를 유지하고 있는 조직에서 개인정보에 관련된 별도의 시스템 구축하는 것이 아니라 부문별로 강화된 사항들에 대해 분석·적용하여 기존의 틀을 유지하면서 개인정보에 관련된 사항들을 강화한다. 또한, ISO/IEC 27701에서는 거의 모든 조직이 개인식별정보(PII : Personally Identifiable Information)를 처리한다고 하고 있고, 이에 따라 PII의 종류나 수는 이전과 비교할 수 없을 정도로 증가하고 있다[35].

ISO/IEC 27701에서는 PII와 관련하여 PII 컨트롤러에 대한 ISO/IEC 27002 추가지침, PII 프로세서에 대한 ISO/IEC 27002 추가지침을 추가하여 GDPR에서 요구 프로세서와 컨트롤러의 보안 사항에 대해서도 대비하고 있다. ISO/IEC 27701은 ISO/IEC 27001, ISO/IEC 27002의 확장판인 만큼 해당 인증을 받기 위해서는 ISO/IEC 27001에 대한 인증이 필수적으로 선행되어야 하며 ISO/IEC 27701 만 별도로 인증을 받을 수는 없다[36].

ISO/IEC 27701의 구성은 <표 Ⅱ-17>과 같이 1장 범위, 2장 참고문헌, 3장 용어, 정의 및 약어로 ISO/IEC 27001과 같은 구성이며, 4장 일반규정부터는 ISO/IEC 27701에 대한 일반규정들로 기존 ISO/IEC 27001과는 차이점을 가진다. 5장은 ISO/IEC 27001 관련 PIMS 요구사항, 6장은 ISO/IEC 27002 관련 PIMS 지침, 7장은 PII 컨트롤러에 대한 ISO/IEC 27002 추가지침, 8장은 PII 프로세서에 대한 ISO/IEC 27002 추가지침으로 구성된다. 이때 공통으로 적용된 변경 사항은 ISO/IEC 27001, ISO/IEC 27002에서 언급되는 “정보보안”의 요건들이 “정보보안 및 개인정보보호”로 확대된다는 사항이다.

<표 Ⅱ-17> ISO/IEC27701 구성

1장 범위		
2장 참고자료		
3장 용어, 정의 및 약어		
4장 일반 규정		
	4.1 표준의 구조 4.2 ISO/IEC 27001 요구사항 적용	4.3 ISO/IEC 27002 지침 적용 4.4 고객
5장 ISO/IEC 27001 관련 PIMS 요구사항		
	5.1 일반규정 5.2 조직 환경 5.3 리더십 5.4 계획	5.5 지원 5.6 운영 5.7 성능 평가 5.8 개선
6장 ISO/IEC 27002 관련 PIMS 지침		
	6.1 일반규정 6.2 정보보호 정책 6.3 정보보호 조직 6.4 인적자원 보안 6.5 자산 관리 6.6 접근 제어 6.7 암호화 6.8 물리적, 환경적 보안	6.9 운영 보안 6.10 통신 보안 6.11 시스템 도입, 개발, 유지보수 6.12 공급자 관계 6.13 정보보호 사고 관리 6.14 업무 연속성 관리의 정보보호 측면 6.15 준거성
7장 PII 컨트롤러에 대한 추가지침		
8장 PII 프로세서에 대한 추가지침		

2.3.4 ISMS-P

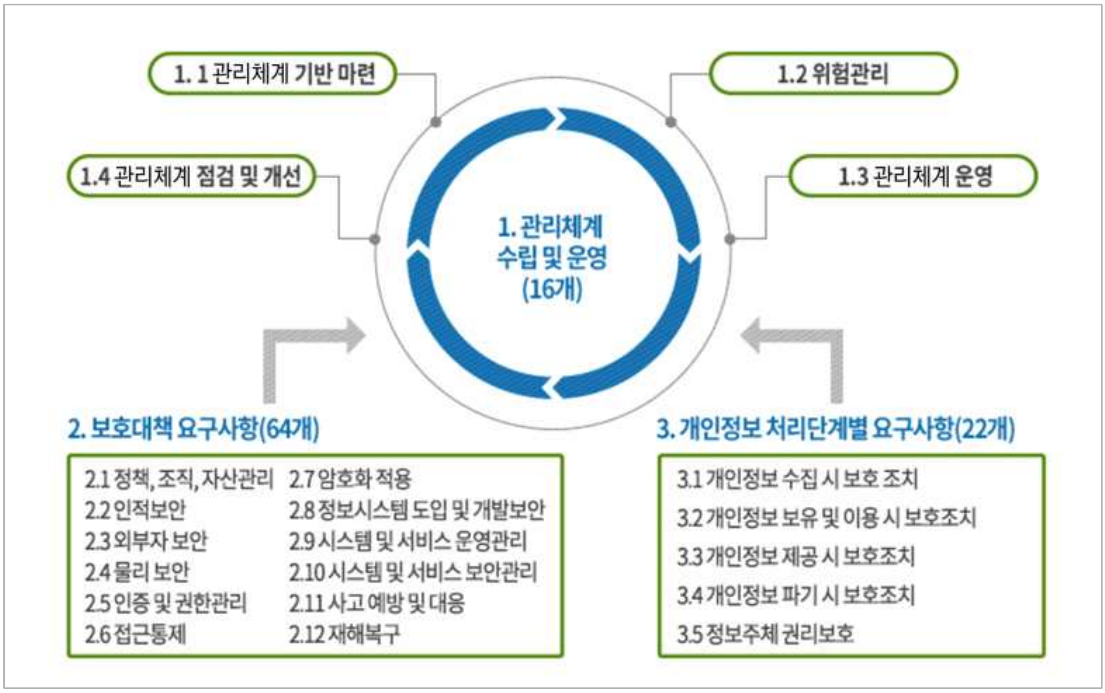
"정보보호 및 개인정보보호 관리체계 인증"이란 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조 제3항 및 제4항, 개인정보 보호법제32조의 2에 따라 인증 신청인의 개인정보보호 및 정보보호를 위한 일련의 활동과 조치가 인증기준에 적합함을 한국인터넷진흥원 또는 국가 공인 인증기관이 증명하는 것을 말한다. 정보보호를 위한 ISMS 인증과 정보보호 및 개인정보보호를 위한 ISMS-P 인증으로 구분한다. ISMS-P 인증심사의 종류는 '최초 심사', '사후 심사', '갱신심사'가 있

다. ‘최초 심사’는 ISMS-P 인증을 처음으로 취득하고자 할 때 수행하는 심사이며, 인증범위에 중요한 변경이 있어 재인증 신청 시에도 같은 심사를 받아야 한다. 최초 심사를 통해 인증을 취득하면 3년의 유효기간이 부여된다. ‘갱신심사’는 ISMS-P 인증의 유효기간 갱신을 위해 받는 심사를 말한다[37].

가. ISMS-P 인증기준

ISMS-P 인증기준은 [그림 Ⅱ-3]과 같이 관리체계 수립 및 운영, 보호 대책 요구사항, 개인정보 처리단계별 요구사항으로 되어 있다.

‘관리체계 수립 및 운영’은 관리체계 기반 마련, 위험관리, 관리체계 운영, 관리체계 점검 및 개선으로 구성되어 있다. ‘보호 대책 요구사항’은 정책, 조직, 자산, 교육, 인적, 접근통제, 암호화 적용, 운영·보안 관리, 사고 예방 및 대응, 재해복구 등 총 12개의 인증기준으로 되어 있다. ‘개인정보 처리 단계별 요구사항’은 개인정보 생명주기 보호 조치사항, 정보 주체의 권리보장으로 구성되어 있다.



[그림 Ⅱ-3] ISMS-P 인증기준[40]

(출처 : 한국인터넷진흥원, "정보보호 및 개인정보보호 관리체계 인증제도 안내서" 인용)

ISMS-P 인증기준의 구성은 <표 Ⅱ-18>과 같이 ISMS, ISMS-P 인증유형에 따라 구분된다.

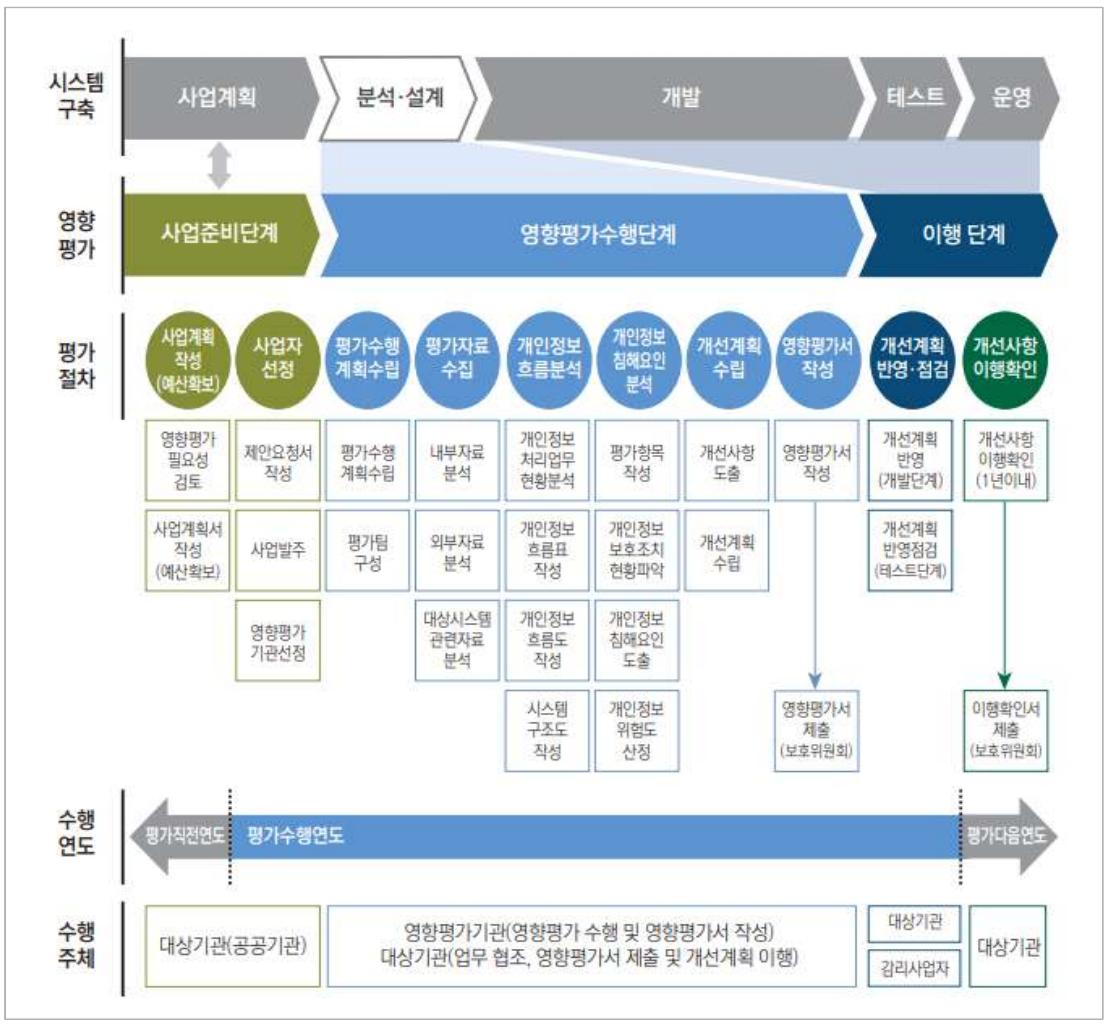
<표 Ⅱ-18> 인증유형별 ISMS-P 인증기준

(출처 : 한국인터넷진흥원, "정보보호 및 개인정보보호 관리체계 인증제도 안내서" 인용)

인증영역	인준기준	항목수	적용여부	
			ISMS	ISMS-P
1. 관리체계 수립 및 운영(16개)	1.1 관리체계 기반 마련	6	○	○
	1.2 위험 관리	4	○	○
	1.3 관리체계 운영	3	○	○
	1.4 관리체계 점검 및 개선	3	○	○
2. 보호 대책 요구사항 (64개)	2.1 정책, 조직, 자산 관리	3	○	○
	2.2 인적 보안	6	○	○
	2.3 외부자 보안	4	○	○
	2.4 물리 보안	7	○	○
	2.5 인증 및 권한 관리	6	○	○
	2.6 접근통제	7	○	○
	2.7 암호화 적용	2	○	○
	2.8 정보시스템 도입 및 개발 보안	6	○	○
	2.9 시스템 및 서비스 운영관리	7	○	○
	2.10 시스템 및 서비스 보안관리	9	○	○
	2.11 사고 예방 및 대응	5	○	○
	2.12 재해복구	2	○	○
3. 개인정보 처리단계별 요구사항(22개)	3.1 개인정보 수집 시 보호조치	7	-	○
	3.2 개인정보 보유 및 이용 시 보호조치	5	-	○
	3.3 개인정보 제공 시 보호조치	4	-	○
	3.4 개인정보 파기 시 보호조치	3	-	○
	3.5 정보 주체 권리보호	3	-	○
계		102	80	102

2.3.5 개인정보 영향평가(PIA)

개인정보 영향평가(Privacy Impact Assessment)는 개인정보의 처리가 수반되는 사업을 추진하거나 신규 시스템의 도입, 기존 개인정보 처리시스템의 중대한 변경하는 경우 개인정보에 미치는 영향을 사전에 분석하고 이에 대한 개선 방안을 수립하여 개인정보의 침해사고를 사전 예방하기 위하여 실시하는 절차이다[9]. 개인정보 영향평가의 시기와 절차는 [그림 Ⅱ-4]와 같다.



[그림 Ⅱ-4] 개인정보 영향평가 시기

(출처 : 한국인터넷진흥원, "개인정보 영향평가 수행 안내서" 인용)

개인정보 영향평가 대상[9]은 일정 규모 이상의 개인정보를 전자적으로 처리하는 개인정보 파일을 구축·운영·변경하려는 공공기관은 개인정보 보호법 제33조 및 시행령 제35조에 근거하여 영향평가를 수행한다. 대상은 5만 명 이상의 정보 주체의 민감정보 또는 고유 식별정보의 처리가 수반되는 개인정보 파일, 해당 공공기관의 내·외부의 다른 개인정보 파일과 연계하려는 경우로, 연계 결과 정보 주체의 수가 50만 명 이상인 개인정보 파일, 100만 명 이상의 정보 주체 수를 포함하고 있는 개인정보 파일 등이 포함된 시스템을 구축하는 경우이다[9]. 또한, 민감정보나 대량의 개인정보를 수집·이용하는 기관은 개인정보 침해로 인한 사회적 피해를 막기 위해 영향평가 수행이 가능하다[9]. 첫 번째, 시스템을 신규 구축 또는 기존 시스템 변경하는 경우 사업계획 단계에서 영향평가의 의무대상 여부를 파악하고 예산 확보 후, 대상 시스템의 구축 계획부터 설계 완료 전에 영향평가를 수행하여야 한다[9]. 또한 시스템 설계·개발·구현 시 영향평가 결과를 반영해야 한다. 두 번째, 개인정보 처리시스템을 기구축·운영 중인 경우, 수집·이용·관리상 중대한 침해위험의 발생 우려되는 경우나 전반적인 개인정보보호 체계를 점검하여 개선하기 위한 경우에도 수행할 수 있으며, 공공기관은 개인정보보호위원회가 지정한 영향평가기관에 평가를 의뢰하여 수행한다[9]. 개인정보 영향평가는 <표 Ⅱ-19>와 같이 5개 평가영역, 25개 평가 분야에 대하여 총 85개의 지표로 구성되어 있다.

<표 Ⅱ-19> PIA 인증기준

(출처 : 한국인터넷진흥원, "정보보호 및 개인정보보호 관리체계 인증제도 안내서" 인용)

평가영역	평가 분야	세부 분야
1. 대상 기관 개인정보보호 관리체계	1.1 개인정보보호 조직	개인정보보호 책임자의 지정
		개인정보보호 책임자 역할수행
	1.2 개인정보보호 계획	내부 관리계획 수립
		개인정보보호 연간계획 수립
	1.3 개인정보 침해 대응	침해사고 신고 방법안내
		유출 사고 대응
	1.4 정보 주체 권리보장	정보 주체 권리보장 절차 수립
		정보 주체 권리보장 방법안내
2. 대상시스템의 개인정보보호 관리체계	2.1 개인정보 취급자 관리	개인정보 취급자 지정
		개인정보 취급자 관리·감독
	2.2 개인정보 파일 관리	개인정보 파일 대장 관리
		개인정보 파일 등록
	2.3 개인정보 처리 방침	개인정보 처리 방침의 공개
		개인정보 처리 방침의 작성

평가영역	평가 분야	세부 분야
3. 개인정보 처리단계별 보호조치	3.1 수집	개인정보 수집의 적합성
		동의받는 방법의 적절성
	3.2 보유	보유기간 산정
	3.3 이용·제공	개인정보 제공의 적합성
		목적 외 이용·제공 제한
		제공 시 안전성 확보
	3.4 위탁	위탁 사실 공개
		위탁 계약
		수탁사 관리·감독
	3.5 파기	파기 계획 수립
		분리보관 계획 수립
		파기 대장 작성
4. 대상시스템의 기술적 보호조치	4.1 접근권한 관리	계정 관리
		인증 관리
		권한 관리
	4.2 접근통제	접근통제 조치
		인터넷 홈페이지 보호조치
		업무용 모바일기기 보호조치
	4.3 개인정보의 암호화	저장 시 암호화
		전송 시 암호화
	4.4 접속기록의 보관 및 점검	접속기록 보관
		접속기록 점검
		접속기록 보관 및 백업
	4.5 악성프로그램 방지 등	백신 설치 및 운영
		보안업데이트 적용
	4.6 물리적 접근 방지	출입 통제 절차 수립
		반출·입 통제 절차 수립
	4.7 개인정보의 파기	안전한 파기
	4.8 기타 기술적 보호조치	개발환경 통제
		개인정보 처리화면 보안
		출력 시 보호조치
	4.9 개인정보 처리 구역 보호	보호구역 지정
5. 특정 IT 기술 활용 시 개인정보보호	5.1 CCTV	CCTV 설치 시 의견수렴
		CCTV 설치 안내
		CCTV 사용 제한
		CCTV 설치·관리에 대한 위탁
	5.2 RFID	RFID 이용자 안내
		RFID 태그 부착 및 제거
	5.3 바이오 정보	원본 정보 보관 시 보호조치
	5.4 위치정보	개인위치정보 수집 동의
		개인위치정보 제공 시 안내 사항

평가항목은 대상 기관 및 사업의 특성, 침해사고 사례, 법 제도의 변화 등에 따라 추가・변경・삭제 등 탄력적으로 구성하여 이용할 필요가 있으며, 개인정보보호 관련 법령·고시가 개정된 경우, 해당 사항에 대해서는 반드시 평가항목에 반영하여 점검하여야 한다.

2.4 개인정보보호 역량 및 윤리지수

2.4.1 개인정보보호 인식과 역량

정보보안 인식(Information security awareness)은 정보보안에 대한 자각 및 정보보안 활동의 관심 정도이다[42].

Layton, T는 정보보호에 대한 인식은 조직구성원의 정보보호 행동을 이끄는 중요한 요인으로 보았으며 정보보호 인식은 정보보호 태도, 특성, 동기부여, 믿음, 윤리 등의 영향이 서로 밀접한 관련이 있는 것으로 가정하였다[43].

임채호는 정보보호 인식 제고를 정보보호를 추진하는 모든 조직과 주체가 당연히 기본적으로 해야 하는 ISMS 상에 있어야만 하는 매우 중요한 요소로 보았으며 정보보호 인식 제고를 사람들이 자신의 직무 수행에 있어서 정보보안의 함축된 상황을 잘 이해할 수 있도록 하는 프로세스로 정의하고 정보보호의 중요성 인식, 보안사고 발생 시 대응 방안과 보호 체계 등이 포함된다고 하였다[44].

장명희와 강다연은 정보를 다루는 조직구성원의 윤리의식 문제를 심각하게 고려해야 할 필요성이 있다고 주장하며 기업의 정보보안 인식을 조직 내 직무 수행에 있어 개인이 정보보안 중요성을 알고 있는 정도라고 하였다[45].

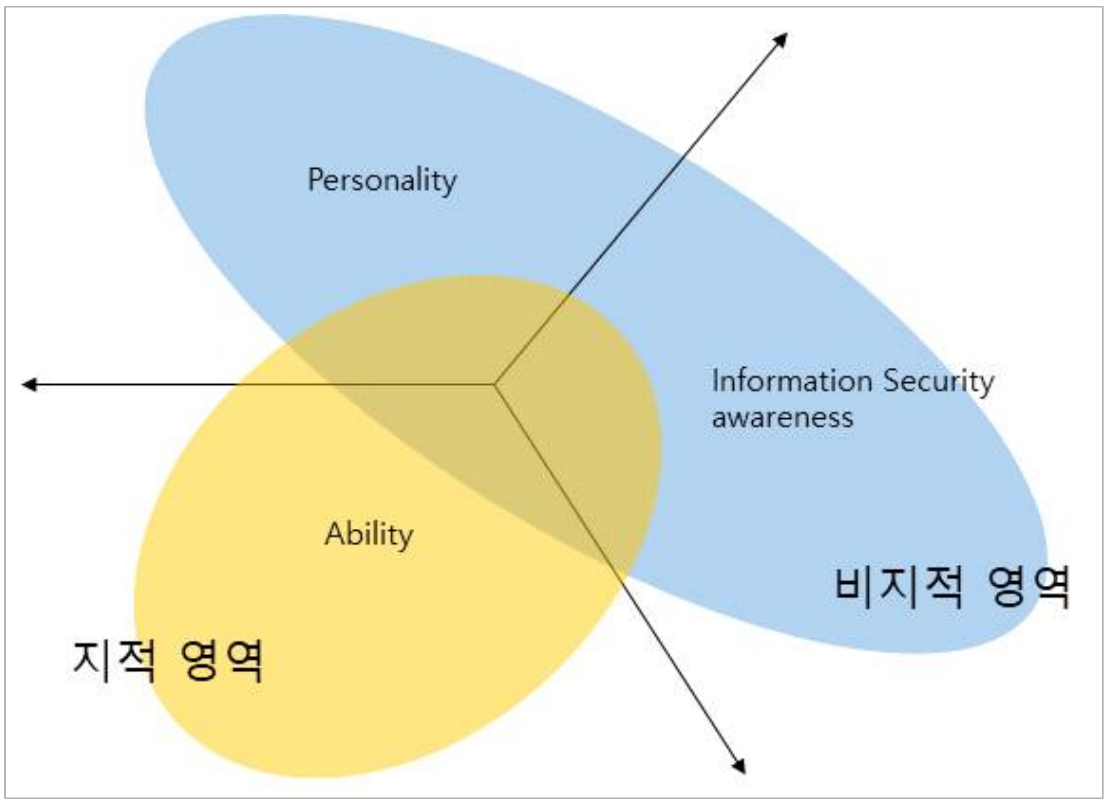
김주연은 개인정보의 수집과 이용이 지속적인 증가추세에서, 개인정보를 보호하기 위한 법적 근거 마련, 각종 정책·제도 시행 등이 이루어지고 있지만, 실제 개인정보보호를 위한 노력이나 인지 수준은 매우 낮은 것으로 분석하였다. 정기적이고 지속적인 개인정보보호 교육의 필요성을 강조하였다[46].

정은영은 보건 행정 전공대학생들의 환자 개인정보보호인지를 높이기 위해서는 올바른 윤리적 가치관 확립이 필요하고, 이를 위한 체계적이고 지속적인 교육운영을 강조하였다[47].

많은 연구가 개인정보 담당자와 보안담당자뿐만 아니라 조직 전체의 개인정보보호 인식 수준 향상의 중요성을 강조하고 있다.

2.4.2 개인정보보호 윤리

보안윤리를 조직구성원의 보안 활동에 필요한 적성 위에서 언급한 대로 크게 비지적 영역과 지적 영역으로 나누었다. 비지적인 영역을 개인 성향(personality)과 정보보안 인식(Information security awareness)으로, 지적인 영역을 능력(ability)으로 분류하였다[48].



[그림 Ⅱ-5] 보안윤리 적성의 분류
(출처 : 조유나.(2018). "조직 내 구성원의 보안윤리 적성검사 도구 개발에 관한 연구" 인용)

가. 정보보안 윤리 적성의 분류에 대한 정의

정보보안 윤리 적성에 대한 분류를 <표 Ⅱ-20>과 같이 정의하였다.

<표 Ⅱ-20> 정보보안 윤리 적성 분류
(출처 : 조유나.(2018). "조직 내 구성원의 보안윤리 적성검사 도구 개발에 관한 연구" 인용)

분류	정의 및 설명	연구자
개인 성향	▸ 개인의 가치관, 삶의 목적이나 태도, 직장이 나 직업에 대한 개인의 고유한 가치관 ▸ 개인이 조직에서 갖게 되는 성향	▸ 유지찬(2010) ▸ 김석영(2016)
정보보안 인식	▸ 정보보안에 대한 자각 및 정보보안 활동의 관심 정도 ▸ 정보 보안과 관련하여 조직에서 정의한 규정 및 권장하는 절차에 대해 조직원이 인식하는 정도	▸ 백민정(2010) ▸ ChoiN,D 외(2008) ▸ 한진영, 유현선 (2016)
능력	▸ 조직의 정보보안 정책에 대해 이해하고 해결할 수 있으며, 정보보안 기술을 적용할 수 있는 능력의 정도 ▸ 정보보안과 관련 문제를 이해하고, 문제해결을 위한 아이디어를 제시 및 실행계획을 수립하는 능력	▸ 강다연, 장명희 (2012) ▸ 한진영, 유현선 (2016)

첫 번째, 개인 성향(personality)은 개인의 가치관, 삶의 목적이나 태도, 개인이 조직에서 갖게 되는 성향을 의미한다[49][50].

두 번째, 정보보안 인식(Information security awareness)은 정보보안에 대한 자각 및 정보보안 활동의 관심 정도, 정보 보안과 관련하여 조직에서 정의한 규정 및 권장하는 절차에 대해 조직원이 인식하는 정도 등으로 정의한다[42][51][53].

세 번째, 능력(ability)은 조직의 정보보안 사항에 대해 이해하며 해결할 수 있고 정보보안 기술을 적용할 수 있는 능력의 정도, 정보보안과 관련 문제를 이해하고, 문제해결을 위한 아이디어를 제시 및 실행계획을 수립하는 능력으로 정의한다[52][53].

나. 정보보안 윤리 적성 항목 개발

정보보안 윤리의 적성 항목에 따른 분류는 <표 Ⅱ-21>과 같으며, 첫 번째, 개인 성향에는 정보윤리 기본원칙을 참고하여 항목으로 도덕성, 사명감, 자기통제, 사회성으로 구성한다. 두 번째, 정보보안 인식에는 정보보안 규범, 정보보안 교육, 자기효능감, 정보보안 행동 등으로 구성한다. 세 번째, 능력은 피해 인지력, 기술사용 방법, 기술 활용도, 문제해결 능력 등으로 구성한다[48].

<표 Ⅱ-21> 정보보안 윤리 적성 항목의 분류

(출처 : 조유나.(2018). "조직 내 구성원의 보안윤리 적성검사 도구 개발에 관한 연구" 인용)

구분		항목	정의 및 설명	연구자
비지적)	개인 성향	도덕성	▸ 인간의 본성을 존중하고, 사회적 질서를 준수하는 태도	▸조주연(2003) ▸추병완(2011)
		사명감	▸ 조직구성원으로서 사명감과 직업의식 ▸ 맡은 일에 대한 투철한 책임 의식	
		자기통제	▸ 자신에 의한 자신에 대한 통제 ▸ 자신이 하고 싶은 대로 하고자 하는 충동이 일어날 때 충동을 극복하고자 하는 개인의 노력	
		사회성	▸ 일반적으로 사회가 요구하는 규범과 역할에 적응해가는 능력 ▸ 타인의 감정을 이해하고 설득할 수 있는 능력	
	정보보안 인식	정보보안 규범	▸ 조직 내 정보보안을 위해 규정된 정보보안 규범을 조직구성원이 정보보안에 긍정적이라 생각하는 정도	▸강다연, 장명희 (2012) ▸최종근, 최명신 (2016)
		정보보안 교육	▸ 조직의 정보보안 교육에 대한 조직구성원들의 인지된 효용성	
		자기효능감	▸ 정보보안을 위해 주어진 정책에 대해 성공적으로 수행할 수 있다는 개인의 기대감 정도 (보안정책 인지, 습득, 적용, 적응 정도)	
		정보보안 행동	▸ 조직의 정보보안을 실행하기 위한 조직구성원들의 실천적인 행동 사항 정도	
지적	능력	피해 인지력	▸ 정보보안에 관련한 피해를 판단할 수 있는 정도	▸강다연, 장명희 (2012)
		기술 사용 방법	▸ 정보기술 관련 보안 능력, 정보기술 연계 능력 등 전략적으로 조직 보안을 위한 기술의 사용 방법	
		기술 활용도	▸ 위와 같은 정보보안 기술 사용 방법을 알고 충분히 잘 이용할 수 있는가에 대한 정도	
		문제해결 능력	▸ 정보보안과 관련 문제를 이해하고, 문제해결을 위한 아이디어를 제시 및 실행계획을 수립하는 능력	

2.5 선행연구의 시사점

개인정보보호 인증체계를 분석한 결과 ISMS-P는 개인정보 수집·제공 시 보호조치, 개인정보 보유·이용 시 보호조치, 개인정보 파기 시 보호조치, 정보 주체 권리보호, ISMS 보호 대책으로 구분되어 있으며, 인증받고자 하는 기관에서 범위를 정하고, 현재 운영 중인 시스템과 서비스를 대상으로 한다[40]. 개인정보보호 영향평가는 개인정보 수집, 이용, 제공, 파기, 안전성 확보 조치 등으로 구분되어 있으며, 대량의 개인정보를 보유하거나 위험성이 높다고 예상되는 시스템과 서비스 구축을 계획하는 경우에만 사전방식으로 진행되고 있다[41]. 김영희(2018)는 AHP 기법을 이용하여 25개의 안전성 확보 조치 기준항목에 대하여 우선순위를 제안하였으며, 측정 대상은 샘플링 방식으로, 시기는 사후 방식으로 하였다[71]. 강민수(2016)는 핀테크 서비스 분야에서 활용할 수 있는 개인정보보호 자가 평가항목을 42개로 구성하였으며, 사후 방식으로 진행할 수 있게 하였다[72]. 오유리(2019)는 공공기관을 대상으로 한 개인정보 관리 수준 진단과 정보보안 관리실태 평가항목을 활용하여 공직자 대상으로 활용도 조사를 하였다[73]. 선행연구를 바탕으로 반영된 개인정보 관리역량 측정 항목 도출 매핑 매트리스는 <표 Ⅱ-22>와 같다.

<표 Ⅱ-22> 개인정보보호 역량성숙도 측정 항목 매핑 매트리스

연구자	통제항목수	연구내용	측정주체	측정주기	측정대상	개인정보보호 역량 측정 항목											
						업무처리흐름분석	개인정보흐름분석	위험도 및 침해요인분석	개인정보영향평가	수집	이용 및 제공	보관 및 파기	내부관리계획	접근관리	접근통제	접속기록관리	개인정보의 암호화	정보주체의 권리보장
김영희(2018)[71]	25	AHP 기법 이용 안전성 확보 조치 기준의 우선순위 제안	개인정보처리자	사후	샘플링								○	○	○	○	○	
강민수(2016)[72]	42	핀테크 서비스의 개인정보보호 자가평가항목 개발	개인정보처리자	사후	샘플링					○	○	○	○	○	○	○	○	

연구자	통제항목수	연구내용	측정주체	측정주기	측정대상	개인정보보호 역량 측정 항목												
						업무처리흐름분석	개인정보흐름분석	위험도 및 침해요인분석	개인정보영향평가	수집	이용 및 제공	보관 및 파기	내부관리계획	접근관리	접근통제	접속기록관리	개인정보의 암호화	정보주체의 권리보장
오유리 (2019) [73]	26	개인정보보호 분야 26개 통제항목 활용 조사	개인정보처리자	사후	샘플링					○	○	○	○	○	○	○	○	○
ISMS-P [40]	102	기관의 개인정보 관리수준 측정	개인정보처리자	사후	샘플링	○				○	○	○	○	○	○	○	○	○
PIA [41]	85	대량의 개인정보 포함 시스템 개발 시 측정	개인정보처리자	사전	구축 시스템	○	○	○		○	○	○	○	○	○	○	○	
공공기관 개인정보 관리수준 진단	13	공공기관의 개인정보 관리수준 평가	개인정보처리자	사후	샘플링					○	○	○	○	○	○	○	○	○

하지만, 선행연구자의 연구와 ISMS-P, PIA, 공공기관 개인정보 관리 수준 진단 등은 개인정보처리자를 대상으로 평가하고 있으며, PIA만 사전 평가이며, 나머지는 사후평가로 진행되었다. 측정 대상 선정은 샘플링 방식으로 진행되어 있다. 개인정보 침해사고는 대부분 개인정보 취급자를 대상으로 발생하고 있음에도 이를 평가하는 모델은 존재하지 않는다. 게다가 개인정보처리자의 문제해결 자체를 지나치게 강조하여 단기적인 성과에 머무르는 수준에 그치고 있었으며, 개인정보 취급자를 위한 개인정보 윤리의식 측정과 공정한 평가, 포상 또한 적절하게 제공되지 않아 일시적인 활동에 그치는 문제점이 있었다.

본 연구에서는 이와 같은 문제점과 함께 기존 성숙도 모델의 근본적인 한계를 극복하면서도 개인정보 취급자 모두가 지속적인 개인정보 관리역량 강화와 개인정보 윤리의식 향상을 위한 개인정보 관리역량 성숙도 모델 및 평가지표를 개발하고, 실제 적용을 통해 검증한 방법론을 제안하고자 한다.

2.6 개인정보보호 적용방법론

2.6.1 델파이 기법

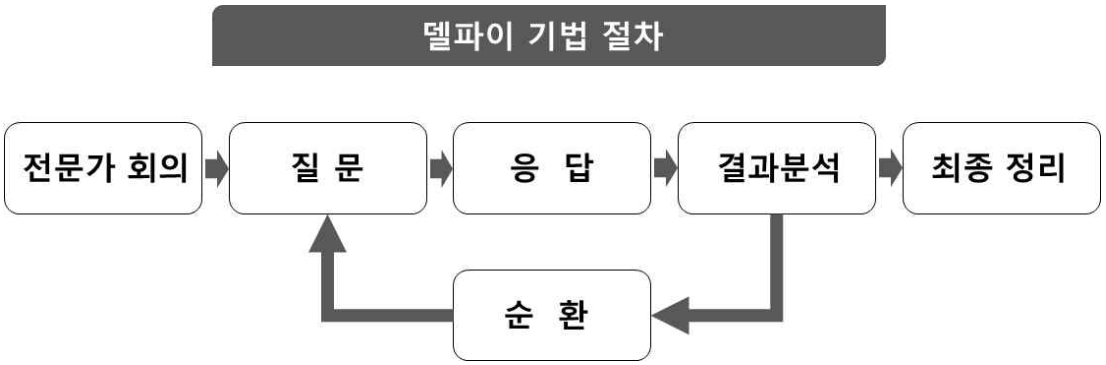
가. 델파이 기법의 개념

델파이 기법은 전문가의 경험과 지식을 통한 문제해결 또는 미래 예측을 위한 기법이며, 1964년 미국의 Rand 연구소에서 개발되어 IT, 교육, 군사, 연구 분야에서 활용되고 있다. 이 기법은 정확한 지식이 없는 특정 이슈에 대하여 다수의 의견을 종합하고자 할 때 이용한다. 델파이 기법은 개인보다는 그룹의 의견이 더 우월하다는 전제에서 시작된 것으로 전문가 집단의 견해를 통하여 불확실한 문제의 해결방안 제시, 미래 예측 등을 도출해내는 방법으로서 발전하였다[54]. 특히, 특정 이슈에 대한 지식이 불완전하거나 동의가 부족하다고 생각될 때 수행된다[55][56][57][58]. 델파이 기법은 전문가패널이 동일 문제에 대하여 2회 이상의 반복적인 과정을 걸쳐 견해를 제시해야 하며, 이 과정에서 그들은 다른 전문가들의 견해 정보를 피드백(Feedback)을 받고, 문제에 대한 견해를 제시할 기회를 얻게 된다. 이러한 일련의 과정에 참여한 전문가는 익명성을 보장받음으로 권위자 발언의 영향, 다수의 횡포, 사전 조율에 의한 집단 역학의 약점, 한 번 행한 입장의 고수 등의 문제점을 제거한 일종의 패널 방식의 연구조사 방법이다[59]. 델파이 기법은 통계 모델이나 절차를 기초로 한 연구를 하는 방법은 아니지만, 인간의 판단에 근거하여 미래 예측이나 해결방안을 도출하려는 목적으로 활용된다[55].

델파이 기법의 특징[58]을 보면, 첫 번째, 익명의 반응이다. 즉, 델파이 조사 패널 참여 전문가들은 대면하지 않고 설문지로만 의견을 제시할 수 있다. 두 번째, 통제된 피드백과 반복이다. 설문 과정을 여러 번의 반복 함에 있어 통제된 피드백만으로 상호작용을 할 수 있도록 한다. 세 번째, 통계적 집단 반응이다.

나. 델파이 기법의 절차

델파이 기법은 미래의 사건에 관해 학식 있는 의견을 개발하고 교환하는 과정을 통해 합의된 결과를 획득하는 직관적 예측 절차로 전체적인 과정은 대체로 비슷하며, 일반적인 절차는 전문가패널의 선정과 구성, 전문가 회의, 2회 이상의 설문조사를 통한 질문 및 응답, 도출된 의견 결과분석, 순환을 통한 의견 합의 단계로 이루어진다[59][60][61].



[그림 Ⅱ-6] 델파이 기법의 절차[61]
(출처: 홍석훈 외, 2015년 통일예측 시계(서울: 통일연구원, 2015) p. 12 인용)

1) 전문가 집단 구성

델파이 조사를 위해서는 연구주제와 관련된 분야 전문가들로 참가자를 구성하는데, 현재 전문가를 선정하는 표준 기준이 규정되어 있지 않아서 델파이 기법에 있어 전문가패널을 선정하는 것은 델파이 시행과정에서 매우 중요한 일이다[54][59][60]. 델파이 기법에서의 전문가 선정과 구성은 델파이 조사가 전문가의 다양한 경험을 기반으로 한 직관을 수치화된 데이터로 표현하는 방법이라고 할 때 조사 참여 전문가의 자질은 매우 중요한 요소이기 때문에 조사 대상은 관련 연구 분야의 전문가를 선정하여 구성한다. 조사 대상은 참여자의 전문성, 대표성, 적절성, 성실성, 참가자의 수 등을 신중히 고려해야 한다[59]. 전문가패널이 반드시 대표성을 가질 필요는 없으나, 해당 연구 문제에 대한 의견 제시 능력을 보유하고 있는지 대해서는 우선 고려해야 한다[56]. 델파이 기법에서의 참여 전문가 패널의 수에 대한 규칙은 정해져 있지 않지만, Anderson은 전문가패널 수가 1

0~15명일 때 유용한 결과를 도출할 수 있음을 규명했다[57]. Dalkey는 패널 수의 상관관계에서 평균 그룹에 대한 오차의 최소화와 신뢰성의 최대화를 위해 10명 이상의 패널이 필요하다고 하였다[58]. 대부분 델파이 조사 연구는 10~35명의 전문가를 패널로 활용하고 있으며, 이 연구에서는 응답률을 고려하여 15명을 전문가패널로 선정하여 진행하였다.

2) 1차 델파이 설문조사

1차 조사 설문은 대부분 비구조화된 응답 양식을 이용한다. 1차 조사는 탐색단계로, 비구조화된 설문지는 참가 전문가들의 확산적 지각을 고찰한 후 의견을 수렴하고자 할 때 적합하다[54][62]. 처음부터 구조화된 설문지를 활용하는 수정 델파이 기법과 같이 1차 설문지가 지나치게 세분화되거나 구조화되면 응답자의 반응범위와 의견의 범위가 줄어들 수 있는 우려가 있어 본 연구에서는 개인정보 관리역량 성숙도 평가 시 고려할 지표에 대해 영역별로 개방형 설문을 통해 전문가들의 다면적인 의견을 수집·수렴할 수 있도록 하였다.

3) 2차 델파이 설문조사

2차 델파이 설문지는 1차 분석이 완료되면 구조화된 설문지를 작성한다. 2차 조사는 합의 도출의 시작 단계이며 2차 설문을 참여 전문가패널에 제시하면서 그들의 반응과 의견을 재평가하도록 한다[59]. 2차 설문지에는 지표에 대한 중요도나 우선순위를 평가하기 위해 리커트(Likert) 5점 척도(또는 7점 척도)를 이용하며, 응답 결과를 평균, 표준편차, 중앙값을 이용한다. 조사 대상 전문가의 합의 수준을 확인하기 위하여 수렴도, 사분위수, 합의도를 산출하고 항목의 내용 타당성을 위해 내용 타당도 등을 구하여 결과를 도출한다[61][62]. 본 연구에서는 2차 델파이 조사분석을 위해 1차 델파이 분석을 통해 도출된 개인정보 관리역량 수준을 평가하기 위한 지표에 대해 중요도를 표시하도록 하였으며, 기타란에 항목 이외의 의견이나 부가 설명 등을 기재할 수 있도록 질문지를 구성하여 질적 분석 자료로 이용하였다.

다. 델파이 기법의 신뢰도와 타당도

신뢰도(Reliability)란 측정 도구로 측정된 값이 얼마나 일정하게 도출되었는지에 대한 개념을 의미한다. 델파이 기법 연구에서 신뢰도 확보를 위해서는 각 설문에 참여 대상 전문가의 기준을 명확하게 설명하고 조사 결과에 대한 통계적인 근거와 엄격한 코딩에 의한 설문지를 구성하여야 한다. 델파이 기법 설문의 신뢰도는 Cronbach's α 계수를 이용하고 있다[59].

타당도(Validity)란 측정하고자 하는 것을 정확하게 측정하였는가에 대한 개념이다. 델파이 기법에서의 타당도는 Lawshe[78]에 의해 제안된 CVR(Content Validity Ratio)을 이용해 검증하며, 응답 수 중 리커트 5점 척도에서 4와 5를 선택한 수를 합산한 결과가 내용타당도 비율(CVR)이 타당하다고 응답한 패널의 수다. 내용타당도 비율(CVR)은 패널 수에 따라 최솟값을 제시하고 있으며, 최솟값 이상이 되었을 때 항목의 내용타당도가 있다고 판단된다.

$$CVR = \frac{n_e - (\frac{N}{2})}{\frac{N}{2}} \quad \cdots\cdots\cdots\cdots \ (가)$$

CVR 값은 (가) 식과 같이 구하며, 척도는 4와 5를 응답한 패널의 수, N은 전체 응답자의 빈도수, n_e은 '필수'항목을 나타내는 패널 수를 의미한다.

2.5.2 AHP 기법

가. AHP의 개요

AHP(Analytic Hierarchy Process) 기법은 Thomas L. Saaty 박사가 1970년대에 창안한 다기준 의사결정 방법론이다[63][64]. AHP는 다수의 대안에 다방면의 평가 기준과 다수의 주체에 의하여 의사결정이 필요한 상황을 위해 설계된 정략적 평가 방법이다[64]. 평가자의 비합리적 또는 합리적 판단을 직관적으로 동시에 고려하며 포괄적 문제해결의 틀을 제공한다. AHP는 의사결정 계층구조를 구성하는 요소 간의 쌍대비교에 의한 판단을 통해 평가자들의 지식과 경험, 직관을 반영하여 의사결정에 이용되는 방법론이며, AHP의 이론 자체에 관한 연구도 활발히 이루어지고 있다[65][66]. 다속성 의사결정의 문제는 상충되는 다수의 기준에서 최적의 대안을 선택하는 문제로 AHP 기법은 이러한 의사결정을 위한 분석 프레임워크를 제공한다[67]. 계층구조를 구성하는 요소들을 쌍대 비교를 통하여 상위계층의 요소부터 하위계층 요소의 가중치 측정 후 각 단계별 가중치들을 종합적으로 도출하여 최하위 대안들에 대한 상대적 우선순위를 표현한다[68].

이러한 AHP는 의사결정자의 오랜 직관이나 경험 등이 평가의 밑바탕이 되므로 수치화할 수 있는 양적 평가 기준을 포함해 보통 의사결정 문제 중 취급하기 어렵지만, 반드시 고려되어야 할 질적 평가 기준들도 쉽게 적용할 수 있으며, 분석과정도 쉽고 직관적인 장점이 있다[66][67].

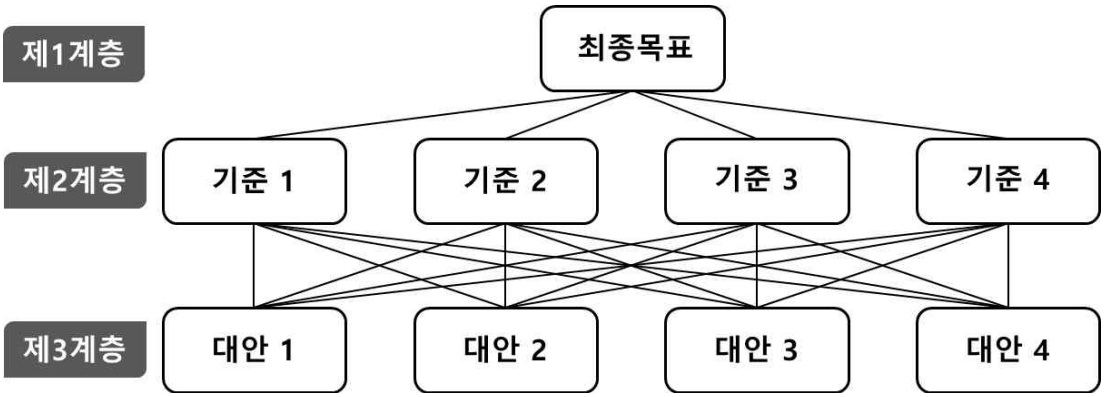
나. AHP의 절차

AHP 분석기법은 일반적으로 4단계를 거치며, 계층의 구성, 구성된 단계의 요인별 쌍대 비교, 쌍대 비교의 분석을 통한 요인별 가중치 도출, AHP 연구의 일관성 평가 및 검증하는 단계로 이루어진다[65].

1) 계층의 구성

계층분석기법은 주어진 의사결정 문제를 상호 관련된 요소들로 계층화하여 문제를 분리하는 과정을 의미한다. 계층이란 상-하위 관계를 기반으로 범주 컬럼을 배열하는 것을 의미하며, 최상층 레벨에는 가장 포괄적인 의사결정의 목적이 설

정되고, 그다음의 계층 레벨들은 의사결정 목적에 영향을 미치는 다양한 속성들로 구성된다. 이들의 속성은 상호 관련된 의사결정 요인들의 계층으로 분류하여 [그림 Ⅱ-7]과 같이 의사결정에 대한 구조화를 설정하며, 계층이 낮을수록 구조화를 구체화할 수 있게 된다.



[그림 Ⅱ-7] AHP의 일반적 구조체계

2) 평가 기준의 쌍대 비교

다속성 의사결정을 하는 경우 각 속성별 상대적 중요도를 모두 고려하여 가중치를 정하기는 쉽지 않다. 따라서 AHP 기법에서는 속성들을 2개씩 쌍대 비교한다. 하나의 계층에 포함된 요인들에 대한 상대적 중요도 평가를 위해 평가 대상 기준들의 쌍대 비교를 하고, 그 결과를 행렬로 도출하는 과정이다. 쌍대 비교의 과정에는 평가 기준에 대한 의사결정권자의 선호도를 먼저 나타내며 이를 계량화 과정에 포함한다. 이를 위해 신뢰성 있는 평가 척도가 필요하고, AHP 기법에서는 Saaty 박사가 제안한 9점 척도가 가장 많이 사용되고 있다[69][70].

일반적인 쌍대 비교의 상대적 중요성 척도는 5단계 척도로 구성되어 이용되며, 이는 계층 간의 구조를 안정화하는데 일반적 척도로 평가된다[70]. 본 연구에서도 이러한 상대적 중요성에 대한 척도 값을 적용하였다.

3) 가중치 도출

AHP 분석기법은 각 요소에 대하여 가중치를 도출하고, 가중치 도출을 위해 선형 대수론의 고유치 방법을 이용한다. n개의 요인과 그 가중치를 N, 그리고 일대 비교 중요도는 아래 식의 (가)와 같이 구한다.

$$a_{ij} = \frac{N_i}{N_j} \ (i, j = 1,2,3,4 \cdots, n) \ \cdots\cdots\cdots \ (가)$$

따라서, 일대 비교행렬 A = [N_{ij}] 는 아래 식 (나)와 같으며, 중요도는 고유벡터 법을 이용하여 구한다.

$$A = \begin{bmatrix} \frac{N_1}{N_1} & \frac{N_1}{N_2} \cdots & \frac{N_1}{N_n} \\ \frac{N_2}{N_1} & \frac{N_2}{N_2} \cdots & \frac{N_2}{N_n} \\ \cdots & \cdots & \cdots \\ \frac{N_n}{N_1} & \frac{N_n}{N_2} \cdots & \frac{N_n}{N_n} \end{bmatrix} \cdots\cdots\cdots \ (나)$$

위의 (나) 식에서 N1/N1은 A1을 비교한 것이며 값은 1이다. N1/N2는 A2에 비교한 A1의 심각 정도를 나타내는 값이며, N1/Nn은 An에 비교한 A1의 쌍대비교 값이다. 하지만 실제적으로는 평가자가 정확한 N을 알지 못하며, 쌍대 비교에 의한 정확한 평가가 불가능하다고 가정하므로 다음과 같은 식 (다) 식에서 N을 추정한다.

$$AN = \lambda max \, N \ \cdots\cdots\cdots \ (다)$$

다. AHP의 일관성

AHP에서는 응답자나 의사결정권자의 판단이 일관성을 유지하고 있는지를 판단해야 하며, 이를 위해서는 일관성 지수(CI : Consistency index)를 계산하여 논리적 일관성 여부를 확인할 수 있다. 이때 일관성 비율(CR : Consistency ratio)을 이용해 일관성 상실 여부를 판단하며, 일관성 지수는 아래의 (라) 식과 같다.

$$CI = (\lambda max - n)(n-1) \cdots\cdots \text{(라)}$$

$\lambda \max \geq n$(단, n = 행렬의 차원)
λmax = 비교행렬의 최대 고유값
n = 비교행렬의 차수

비일관성 비율(CR)은 위의 (라) 식을 통해 도출한다. RI(Random Index)는 난수 지수로 1부터 9까지 수치를 임의 설정하여 역수 행렬을 작성한 후 평균 일관성 지수를 산출한 결과이며, 일관성의 허용 한도를 보인다. RI는 비교행렬 크기(n)에 따라 다르며 <표 Ⅱ-23>과 같다.

<표 Ⅱ-23> AHP 연구의 Random Index (Saaty, 1982)

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
R1	0.00	0.00	0.58	0.90	1.12	1.12	1.32	1.41	1.45	1.49	1.52	1.54	1.56	1.58	1.59

일반적으로 쌍대비교가 CR 값이 0.1 이하이면 일관성을 갖고 있다고 판단하며 만약, 특정 판단행렬의 일관성 비율이 0.1을 초과하였다면 판단행렬을 수정하거나[69], 재평가를 통해 판단행렬의 일관성을 개선하도록 권장하였다[70]. 일관성 비율이 0.1 이내.이면 응답 결과를 합리적인 수용이 가능하며, 0.2 이내이면 납득할 수 있는 수준이지만 0.2 이상이면 일관성이 부족한 것으로 판단한다고 하였다[70].

Ⅲ. 개인정보 관리역량 성숙도 모델 및 평가지표의 개발

3.1 연구설계

3.1.1 연구설계 및 대상

이 연구는 개인정보 취급자가 스스로 개인정보 관리역량성숙도를 향상할 수 있도록 역량 평가지표를 개발하기 위하여 AHP와 델파이 기법을 활용하여 개인정보보호 분야 5년 이상의 전문가 및 개인정보 업무담당자를 대상으로 연구를 진행하였으며 이 연구의 전체적인 연구설계의 순서와 대상은 다음과 같다.

가. 연구의 설계

이 연구는 개인정보 관리역량성숙도 평가지표를 개발을 위하여 위해 ISMS-P, 개인정보보호 영향평가, 공공기관 개인정보 관리 수준 진단, Privacy by design 등 역량 모델의 분석을 통해 상위개념을 분류하고 분류된 상위개념에 따라 실질적인 하위개념과 세부 평가지표들을 도출하여 도출된 항목들을 바탕으로 개인정보 관리역량성숙도 평가지표 개발 시 가장 우선시되는 요인 간의 상대적 중요도를 파악하여 가중치가 부여된 평가지표를 개발하는 것에 연구의 목적이 있다. 즉, 개인정보 관리역량성숙도를 측정 함에 있어 더욱 객관적으로 관리역량 수준을 확인하고 그 결과에 따라 개인정보 관리 현상에 대한 개선 또는 관리를 할 수 있는 평가지표를 개발하고자 하는 연구라 한다. 구체적인 연구 절차는 <표 Ⅲ-1>과 같다.

<표 Ⅲ-1> 연구 절차

단계		방법	내용
1단계	개념 및 세부 지표 개발	문헌연구와 선행연구 검토	선행연구를 통한 평가지표 개발 (5개 분야, 89개 세부 지표)
2단계	개념 및 세부 지표 선정 (델파이 조사)	1차 개방형 질문지	역량성숙도 측정 항목 범주화(15명)
		2차 폐쇄형 질문지	설문 문항에 대한 전문가패널 델파이 조사 분석(13명)
3단계	개념 및 세부 지표 가중치 및 우선순위 선정(AHP 분석)	AHP 질문지	설문 문항에 대한 전문가패널 AHP 조사 분석(10명)

첫 번째 단계에서는 개인정보 관리역량성숙도 측정에 대한 문헌연구와 선행연구 분석을 통해 관련 내용을 확인하고 연구 절차 및 연구 방법을 도출하였다.

두 번째 단계에서는 개인정보 관리역량 성숙도 모델을 측정하는 하위요소와 세부 지표를 도출하기 위하여 전문가패널을 활용한 델파이 조사기법을 사용하였다. 1차, 2차의 조사를 통해 각 하위요소의 개념을 정리하고 구성하는 항목들의 내용타당도를 확인하여 세부 지표를 도출하였다.

세 번째 단계에서는 1차, 2차의 델파이 조사를 통해 개발된 하위개념과 세부 지표를 바탕으로 AHP 기법을 이용하였다. 델파이 조사 기법을 활용해 최종 도출된 구조화된 평가지표를 기초로 AHP를 실행 후 최종 도출된 항목의 상대적 중요도 및 우선순위를 검증, 가중치를 부여한 지표를 개발하였다.

나. 하위개념 및 세부 지표의 개발

1) 개인정보 관리역량성숙도 평가항목 도출

개인정보 관리역량 성숙도 모델 및 평가지표를 개발하는데 델파이 조사에서 상위개념의 평가구조에 대해 제시하고 응답의 이해도와 타당도의 향상을 위해 현재의 개인정보보호 분야에서 주로 활용되고 있는 성숙도 모델에 대해 분석하였다. 분석된 결과를 토대로 예비 평가항목에 대한 상위개념의 평가구조와 개별 평가항목들을 선별하였다.

선행연구를 바탕으로 서로 유사한 통제항목들은 통합시키고, PbD(Privacy by design) 8대 원칙을 적용하여 계획.설계단계 PbD 적용, 권리보장 및 윤리역량을

추가하여 반영하였다. 따라서 김영희(2018), 강민수(2016), 오유리(2019)와 ISMS-P의 개인정보 수집, 이용, 제공, 파기, 안전성 확보 조치와 개인정보 영향평가의 개인정보 흐름 분석을 재구성하여 계획·설계단계 PbD 적용, 개인정보 생애주기의 보호, 안전성 확보 조치, 개인정보 관리 수준 점검 및 개선, 권리보장 및 윤리역량으로 총 5개로 상위개념 평가구조를 <표 Ⅲ-2>와 같이 도출하였다.

<표 Ⅲ-2> 5개 상위 평가구조별 개인정보 관리역량성숙도 평가항목 선별 결과

도출된 상위개념 평가항목		평가항목 적용					측정 대상		측정 범위		측정 주기			
상위개념	하위개념	김영희	강민수	오유리	ISMS-P	PIA	기관	개인	샘플링	전수	P	D	C	A
계획·설계 단계의 PbD 적용	업무처리 흐름 분석					○	○	○		○	○	○	○	○
	개인정보 흐름 분석					○	○	○		○	○	○	○	○
	개인정보 안전성 분석					○	○	○		○	○	○	○	○
	관리체계 수립							○		○	○	○	○	○
개인정보 생애주기의 보호	수집		○	○	○	○	○	○		○	○	○	○	○
	이용 및 제공		○	○	○	○	○	○		○	○	○	○	○
	보관 및 파기		○	○	○	○	○	○		○	○	○	○	○
안전성 확보 조치	내부 관리계획	○	○	○	○	○	○			○	○	○	○	○
	접근관리	○	○	○	○	○	○	○		○	○	○	○	○
	접근통제	○	○	○	○	○	○	○		○	○	○	○	○
	접속기록 관리	○	○	○	○	○	○	○		○	○	○	○	○
	개인정보의 암호화	○	○	○	○	○	○	○		○	○	○	○	○
개인정보 관리 수준 점검 및 개선	관리/기술적 보호			○	○	○	○	○		○	○	○	○	○
	대응훈련 능력			○	○	○	○	○		○	○	○	○	○
권리보장 및 윤리역량	정보 주체의 권리보장		○		○	○	○	○		○	○	○	○	○
	조직의 역량			○			○			○	○	○	○	○
	개인의 역량 및 윤리의식							○		○	○	○	○	○

개인의 개인정보보호 역량 및 윤리 평가항목은 조직 내 구성원의 보안윤리 적성검사 도구를 12개 항목으로 분류한 선행연구[48]를 활용하여 <표 Ⅲ-3>과 같이 개인정보보호에 대한 도덕성과 자기통제, 개인정보 처리 업무의 사명감, 개인정보보호 법률 및 제도 이해력과 행동, 개인정보보호 교육 이수 및 자기 계발,

개인정보보호에 대한 자기효능감, 개인정보보호 기술 능력과 활용도, 개인정보 침해에 대한 피해 인지력과 문제해결 능력 등 7개 항목으로 재구성하였다.

<표 Ⅲ-3> 개인정보보호 역량 및 윤리 평가항목의 분류

구분		항목	정의 및 설명		채택항목
비지적	개인성향	도덕성	인간의 본성을 존중하고, 사회적 질서를 준수하는 태도		개인정보보호에 대한 도덕성과 자기통제
		사명감	조직구성원으로서 사명감과 직업의식을 가짐, 맡은 일에 대한 투철한 책임 의식		
		자기통제	자신에 의한 자신에 대한 통제 자신이 하고 싶은 대로 하고자 하는 충동이 일어날 때 충동을 극복하고자 하는 개인의 노력	→	개인정보 처리 업무의 사명감
		사회성	일반적으로 사회가 요구하는 규범과 역할에 적응해가는 능력 타인의 감정을 이해하고 설득할 수 있는 능력		
	정보보안인식	정보보안규범	조직 내 정보보안을 위해 규정된 정보보안규범을 조직구성원이 정보보안에 긍정적이라 생각하는 정도		개인정보보호 법률 및 제도 이해력과 행동
		정보보안교육	조직의 정보보안교육에 대한 조직구성원들의 인지된 효용성		개인정보보호 교육 이수 및 자기 계발
		자기효능감	정보보안을 위해 주어진 정책에 대해 성공적으로 수행할 수 있다는 개인의 기대감 정도(보안정책 인지, 습득, 적용, 적응 정도)	→	
		정보보안행동	조직의 정보보안을 실행하기 위한 조직구성원들의 실천적인 행동사항 정도		개인정보보호에 대한 자기효능감
지적	능력	피해인지력	정보보안에 관련한 피해를 판단할 수 있는 정도		개인정보보호 기술 능력과 활용도
		기술사용방법	정보기술 관련 보안 능력, 정보기술 연계 능력 등 전략적으로 조직 보안을 위한 기술의 사용 방법		
		기술활용도	위와 같은 정보보안기술 사용방법을 알고 충분히 잘 이용할 수 있는가에 대한 정도	→	피해 인지력과 문제해결 능력
		문제해결능력	정보보안과 관련 문제를 이해하고, 문제해결을 위한 아이디어를 제시 및 실행 계획을 수립하는 능력		

2) 평가항목 분류

델파이 조사 시 응답의 이해와 타당성을 높이기 위해 질문지에 예시를 현재 ISMS-P, PIA, 공공기관 개인정보 관리 수준 진단, ISO27702, 개인정보보호 중심설계(PbD)의 통제항목에서 개별 평가항목들을 선별하여 표현하였다. 선별된 평가항목 중 서로 유사한 통제항목을 통합하였고, 상위개념으로 도출된 계획·설계단계 PbD 적용, 개인정보 생애주기의 보호, 안전성 확보 조치, 개인정보 관리 수준 점검 및 개선, 권리보장 및 윤리역량의 상위개념에 따라 평가항목을 재분류하였다. 도출된 개인정보 관리역량 성숙도 모델의 세부 평가항목들에 대한 분류는 <표 Ⅲ-4>와 같다.

<표 Ⅲ-4> 도출된 개인정보 관리역량성숙도 평가항목

상위개념	하위개념	도출된 세부 지표	기존 모델 적용 현황			
			ISMS-P	PIA	개인정보 관리 수준 진단	ISO27702
계획·설계단계 PbD 적용	업무처리 흐름 분석	개인정보 처리 업무처리 흐름도·흐름표 작성	V	V		
		업무처리 흐름도·흐름표 개정관리	V	V		
	개인정보 흐름 분석	개인정보 수집, 이용, 보유기간 적절성 검토		V		
		주민등록번호, 민감정보, 고유 식별정보 처리 적절성 검토		V		
		개인정보 수집 항목 구분 적절성 검토		V		
		만 14세 미만의 아동 정보 수집 적절성 검토		V		
		제3자 제공, 위·수탁 적절성 검토		V		
		개인정보의 타 시스템 연계 적절성 검토				
		개인정보 안전성 확보 조치 적절성 검토				
		개인정보 처리 흐름도 작성 및 이력 관리	V	V		
		개인정보 처리 흐름표 작성 및 이력 관리	V	V		

상위개념	하위개념	도출된 세부 지표	기존 모델 적용 현황			
			ISMS-P	PIA	개인정보 관리 수준 진단	ISO27702
	개인정보 안전성 분석	개인정보 처리 위험도 및 침해요인 분석		V		
		개인정보 위험평가 분석				
		개인정보의 보호 대책 선정				
		개인정보의 보호 대책 구현				
	관리체계 수립	개인정보보호 정책 수립 적절성 검토	V			
		법적 요구사항 준수 적절성 검토	V			
		관리체계 점검 및 개선 계획 수립 적절성 검토	V			
개인정보 생애주기 보호	수집	개인정보 수집 필수사항 안내 및 동의	V	V	V	V
		목적별 최소한의 필수정보 수집	V	V	V	V
		개인정보 수집 항목의 필수와 선택정보 구분	V	V	V	V
		민감정보 처리 별도 동의	V	V	V	V
		고유 식별정보 별도 동의	V	V	V	V
		만 14세 미만의 아동의 정보 수집 시 법정 대리인 동의	V	V	V	V
		주민등록번호 수집 제한 법적 준수	V	V	V	V
		선택정보 동의 거부 시 서비스 제공	V	V	V	V
		개인정보의 국외 이전 안내 및 동의	V	V		V
	이용 및 제공	개인정보 처리 위탁 계약서 작성 및 체결	V	V	V	V
		위탁업무의 정보 공개	V	V	V	V
		수탁자 대상 교육 및 관리 감독	V	V	V	V
		목적 내 제3자 이용·제공 시 필수사항 고지 및 동의	V	V	V	V
		목적 외 제3자 이용·제공 시 필수사항 고지 및 동의	V	V	V	V
		목적 외 제3자 이용·제공 사항 공고	V	V	V	V
		개인정보 이용 및 제3자 제공 대장 기록 관리	V	V	V	V

상위개념	하위개념	도출된 세부 지표	기존 모델 적용 현황			
			ISMS-P	PIA	개인정보 관리 수준 진단	ISO27702
	보관 및 파기	개인정보 자료 보관실의 잠금장치 및 출입 통제	V	V	V	V
		개인정보 저장 장비의 잠금장치 및 출입 통제	V	V	V	V
		개인정보 파기 기간 준수	V	V	V	V
		개인정보 파일 파기 절차 준수	V	V	V	V
		개인정보 파기 방법 적절성	V	V	V	V
		개인정보 파일 파기 관리 대장 기록 관리	V	V	V	V
안전성 확보 조치	내부 관리계획	내부 관리계획 수립 및 이력 관리	V	V	V	V
		내부 관리계획 이행점검 및 개선	V	V	V	V
	접근관리	접근권한 절차 수립 및 이력 관리	V	V	V	V
		접근권한 차등 부여	V	V	V	V
		접근권한 변경내역 기록 및 관리	V	V	V	V
	접근통제	안전한 비밀번호 작성 규칙 적용	V	V	V	V
		계정 오류 입력 접근제한 설정	V	V	V	V
		부재 시 시스템 접속 차단 설정	V	V	V	V
		비업무용 사이트 접속 차단 설정	V	V	V	V
		비인가자 접근 차단	V	V	V	V
		안전한 접속(또는 인증) 수단 적용	V	V	V	V
		관리용 단말기 접근통제	V	V	V	V
	접속기록 관리	개인정보 취급자의 접속 기록 보관 기간 설정	V	V	V	V
		접속기록 필수정보 적용	V	V	V	V
		접속기록의 안전한 보관	V	V	V	V
		접속기록 점검 관리	V	V	V	V
	개인정보의 암호화	개인정보의 암호화	V	V	V	V
		비밀번호의 암호화	V	V	V	V

상위개념	하위개념	도출된 세부 지표	기존 모델 적용 현황			
			ISMS-P	PIA	개인정보 관리 수준 진단	ISO27702
개인정보 관리 수준 점검 및 개선	관리/기술적 보호	개인정보 관리 정책의 점검 및 검토	V		V	V
		개인정보 관리 정책의 개선	V		V	V
		개인정보 관리 점검 및 검토	V		V	V
		개인정보 관리 점검결과 확인된 사항 조치	V		V	V
		보안취약점 점검 및 위험평가 검토	V		V	V
		보안취약점 개선 조치	V		V	V
		개인정보 노출 여부 모니터링 및 검토				
		개인정보 노출 모니터링 결과 확인된 사항 조치				
	대응훈련 능력	개인정보 침해사고 대응훈련	V			V
		개인정보 침해사고 대응훈련 통한 확인된 사항 조치	V			V
		개인정보 재해복구 훈련	V			V
		개인정보 재해복구 훈련을 통한 확인된 사항 조치	V			V
권리보장 및 윤리역량	정보 주체의 권리보장	정보 주체 중심의 개인정보 처리 방침 공개	V	V	V	V
		정보 주체 중심의 개인정보 수집 이용동의서 제공	V	V	V	V
		개인정보의 열람·정정·삭제·처리정지의 처리	V	V	V	V
		법적 대리인의 동의권 보장	V	V	V	V
		개인정보 유출 신고 안내	V	V	V	V

상위개념	하위개념	도출된 세부 지표	기존 모델 적용 현황			
			ISMS-P	PIA	개인정보 관리 수준 진단	ISO27702
	조직의 역량	조직의 개인정보보호 관련 규정 준수	V	V	V	V
		조직의 개인정보 침해사고 지침 준수	V	V	V	V
		개인정보보호 전담 조직 및 인력 구성	V	V	V	V
		개인정보보호 전용 예산 편성	V	V	V	V
		개인정보보호 교육과정 운영 및 평가	V	V	V	V
		성과관리(또는 인센티브제도) 운용				
		위반자 제재 및 처벌				
	개인의 역량과 윤리의식	개인정보보호에 대한 도덕성과 자기통제				
		개인정보 처리 업무의 사명감				
		개인정보보호 법률 및 제도 이해력과 행동				
		개인정보보호 교육 이수 및 자기 계발				
		개인정보보호에 대한 자기효능감				
		개인정보보호 기술 능력과 활용도				
		피해 인지력과 문제해결 능력				

세부 통제항목에 대한 분류는 연구자가 처음에는 주관적으로 분류했으나 델파이 조사와 전문가의 순환 환류 회의를 통해 세부 항목별 검증과 재구성이 이루어졌다.

첫 번째, 계획.설계단계 PbD 적용 단계에서는 업무처리 흐름 분석, 개인정보 흐름 분석, 개인정보 안전성 분석, 관리체계 수립 등 4개의 하위개념과 18개의 세부 지표로 구성하였다. 18개의 세부 지표에는 기존의 ISMS-P, PIA, 공공기관 개인정보 관리 수준 진단, ISO27702 모델에서 14개의 항목을 도출하였고, 개인정보 안전성 확보 조치 적절성 검토, 개인정보 위험평가 분석, 개인정보의 보호 대책 선정, 개인정보의 보호 대책 구현 등 4개 항목을 제안하였다.

두 번째, 개인정보 생애주기 보호 단계에서는 수집, 이용 및 제공, 보관 및 파기 등 3개의 하위개념과 기존의 ISMS-P, PIA, 공공기관 개인정보 관리 수준 진단, ISO27702 모델에서 22개의 세부 지표를 도출하였다.

세 번째, 안전성 확보 조치단계에서는 내부 관리계획, 접근관리, 접근통제, 접속기록 관리, 개인정보의 암호화 등 5개의 하위개념과 기존의 ISMS-P, PIA, 공공기관 개인정보 관리 수준 진단, ISO27702 모델에서 18개의 세부 지표를 도출하였다. 네 번째, 개인정보 관리 수준 점검 및 개선단계에서는 관리/기술적 보호, 대응능력 향상 등 2개의 하위개념과 12개의 세부 지표로 구성하였다. 다섯 번째, 권리보장 및 윤리역량단계에서는 조직의 역량, 개인의 역량과 윤리의식 등 2개의 하위개념과 14개의 세부 지표로 구성하였다. 14개의 세부 지표에는 기존의 ISMS-P, PIA, 공공기관 개인정보 관리 수준 진단, ISO27702 모델에서 6개의 항목을 도출하였고, 조직의 역량에 성과관리(또는 인센티브제도) 운용 1개 지표를, 개인의 역량과 윤리의식에 개인정보보호에 대한 도덕성과 자기통제, 개인정보 처리 업무의 사명감, 개인정보보호 법률 및 제도 이해력과 행동, 개인정보보호 교육이수 및 자기 계발, 개인정보보호에 대한 자기효능감, 개인정보보호 기술 능력과 활용도, 피해 인지력과 문제해결 능력 등 7개의 지표를 제안하였다.

3.2 델파이 조사

본 연구에서는 개인정보 관리역량 수준에 대한 평가항목을 개발하기 위하여 전문가패널을 구성한 후 델파이 조사를 <표 Ⅲ-5>와 같이 실시하였다.

<표 Ⅲ-5> 델파이 조사 방법과 내용

단계	내용
-	전문가패널 구성(15명)
1차	1차 개방형 질문지 작성, 배포, 회수, 결과분석
전문가 회의	1차 결과 검토 및 의견 제시
2차	2차 폐쇄형 질문지 작성, 배포, 회수, 결과분석

3.2.1 1차 델파이 조사

가. 전문가패널 구성

델파이 조사는 연구주제와 적합한 전문가패널의 의견을 수렴하여 예측 또는 의사결정을 하는 연구 방법이기 때문에, 전문가패널의 구성과 선정은 매우 중요하다. 성공적인 델파이 연구를 위해서는 관련분야에 이해도 또는 공헌도가 높거나 문제에 대한 합리적인 의견을 제시할 수 있는 전문가들로 선정해야 한다.

델파이 전문가패널의 선정은 연구주제와 밀접하게 관련된 관련 전문가를 패널로서 선택할 수도 있으며, 관련 전문가가 다수일 경우 전문가 내에서 무작위 추출이 가능하다[54].

<표 Ⅲ-6>과 같이 보안 분야의 델파이 및 AHP 연구에서는 64명을 패널로 선정하였다. 평가지표 개발 관련 연구에서는 13~27명을 패널로 선정하였다.

<표 Ⅲ-6> 델파이 선행연구의 전문가패널 수

구분	논문 제목	패널수(명)	저자
보안분야	AHP 방법 이용한 경찰의 산업기술보호 분야 역량 강화 방안	64명	최익서(2020) [79]
평가모형	전문가 델파이 기법을 통한 쌀 교육 프로그램 개발 및 교육효과 평가	27명	김지현(2013) [80]
	이해당사자 기반 평생교육 실습 프로그램 평가 척도 개발	13명	구경희(2017) [81]

본 연구에서는 개인정보 관리역량 성숙도 모델을 개발하기 위하여 전문가패널을 구성하여 델파이 조사하였다. 전문가패널은 사전에 전화를 통하여 협의하였으며 이메일을 통해 자료를 송부하고 회수하였다. 패널은 개인정보보호 및 정보보안 분야 전문가이면서 변호사, 박사, 관련 전문 자격보유자, 10년 이상의 경력 보유 전문가로 총 15명을 <표 Ⅲ-7>과 같이 구성하였다.

<표 Ⅲ-7> 1차 델파이 조사 전문가 풀 구성

구분	분야	경력
1	변호사	10년
2	변호사	10년
3	박사	25년
4	개인정보보호 분야 전문가	20년
5	개인정보보호 분야 전문가	18년
6	개인정보보호 분야 전문가	12년
7	개인정보보호 분야 전문가	14년
8	개인정보보호 실무자	14년
9	개인정보보호 실무자	10년
10	개인정보보호 실무자	10년
11	개인정보보호 실무자	10년
12	개인정보보호 실무자	10년
13	개인정보보호 실무자	10년
14	개인정보보호 실무자	10년
15	개인정보보호 실무자	10년

나. 조사 절차 및 방법

본 연구자가 문헌 연구와 선행연구를 바탕으로 “개인정보 관리역량 성숙도 모델” 평가지표로서 계획·설계단계 PbD 적용, 개인정보 생애주기의 보호, 안전성 확보 조치, 개인정보 관리 수준 점검 및 개선, 권리보장 및 윤리역량의 5개 분류와 하위 요인의 세부 지표로 89개를 선정하고 이에 속하지 않는 개인정보 역량 평가항목을 기재할 수 있도록 기타를 추가하여 1차 델파이 조사지를 작성하였다.

1차 델파이 조사는 2022년 1월 13일부터 1월 18일까지 6일 동안 진행되었으며, 1차 델파이 조사지는 전문가 패널에게 E-mail을 통하여 발송하였고, 조사지에는 질문지의 질문 의도와 이해도를 높이기 위해 평가항목에 대한 예시를 기재하였다.

다. 자료처리

1차 델파이 조사는 개방형 설문 방식으로 진행하였고, 자료는 Microsoft Excel 2018을 이용하여 데이터를 입력하고 전문가 회의를 통해 평가항목을 분석하였다.

3.2.2 전문가 회의

가. 전문가 구성

델파이 조사 분석과정에서 발생할 수 있는 오류를 사전에 방지하고 도출된 항목 선정과 구조화를 위하여 <표 Ⅲ-8>과 같이 3명의 전문가를 선정하여 순환회의 및 연구에 참여하였다.

<표 Ⅲ-8> 델파이 조사 환류 회의 참가자

구분	분야	경력	참여내용
1	변호사	10년	1~2차 델파이 조사 후 적합성 검증
2	개인정보보호 분야 전문가	12년	
3	개인정보보호 실무자	10년	

나. 조사 절차 및 방법

1차 델파이 조사 결과를 바탕으로 3명의 전문가 회의를 통해 유사하거나 같은 개념의 통합과 질문의 의도에 적합하지 않은 항목들을 삭제하여 2차 델파이 조사를 통하여 최종적인 평가항목을 도출할 수 있도록 하였다. 전문가 회의는 2022년 1월 20일 대면으로 진행하였다.

3.2.3 2차 델파이 조사

가. 전문가패널 구성

본 연구에서는 도출된 개인정보 관리역량 성숙도 모델의 하위개념, 세부 지표에 대한 1차 델파이 조사 결과를 분석·반영 후 2차 델파이 조사를 하였다. 2차 델파이 조사를 위한 전문가패널은 개인정보보호에 대한 지식 및 경험 보유 등을 판단하여 <표 Ⅲ-9>와 같이 구성하였다.

<표 Ⅲ-9> 2차 델파이 조사 전문가 풀 구성

구분	분야	경력
1	변호사	10년
2	박사	25년
3	개인정보보호 분야 전문가	20년
4	개인정보보호 분야 전문가	18년
5	개인정보보호 분야 전문가	12년
6	개인정보보호 분야 전문가	14년
7	개인정보보호 실무자	14년
8	개인정보보호 실무자	10년
9	개인정보보호 실무자	10년
10	개인정보보호 실무자	10년
11	개인정보보호 실무자	10년
12	개인정보보호 실무자	10년
13	개인정보보호 실무자	10년

나. 조사 절차 및 방법

2차 델파이 조사지는 1차 델파이 조사에 대한 분석 결과를 바탕으로 세부 지표를 수정하였다. 1차 델파이 조사와 전문가 회의를 거쳐 '사전 계획 및 설계의 PbD 적용' 명칭을 '사전 계획 및 설계단계'로 수정하여 89개의 세부 지표로 2차 델파이 조사지를 개발하였다.

2차 델파이 조사는 2022년 1월 20일부터 1월 25일까지 6일 동안 진행되었으며, 1차 델파이 조사에 참여했던 전문가 중에서 개별 인터뷰가 가능한 전문가 13명에게 E-mail을 통해 발송하였고 개별 인터뷰로 진행하였다.

본 연구에서는 델파이 조사에 대한 타당도 검정에 있어 평가항목들의 중요도 평가에서는 평균값이 3.00 미만인 평가항목들을 제거하고자 하였고, 평가항목에 대한 중요도를 파악하기 위하여 CVR 지수의 최솟값에 대하여 Lawshe (1975)가 제시한 기준인 패널 수 1명일 경우의 0.54 이상이면 타당한 개념으로 보았고, Cronbach's α 값은 0.60 이상을 신뢰도가 있는 것으로 보았다[78].

다. 자료처리

2차의 설문자료 데이터는 입력과 범주화 과정을 Microsoft Excel 2018에서 실시하여 항목 간의 일치 수준을 판단하기 위해 Cronbach's α 값을 분석하였다.

3.3 AHP 조사

본 연구에서는 개인정보 관리역량 수준에 대한 평가항목을 개발하기 위하여 전문가패널을 구성한 후 AHP 조사를 <표 Ⅲ-10>과 같이 실시하였다.

<표 Ⅲ-10> AHP 조사 방법 및 활동 내용

단계	내용
-	전문가패널 구성(10명)
AHP 조사	AHP 질문지 작성, 배포, 회수, 결과분석

3.3.1 전문가패널 구성

본 연구에서는 두 차례의 델파이 질문을 통해 나온 전문가들의 의견을 범주화하고 2차 델파이 응답 결과에 따라 5개의 상위 분류와 17개의 하위개념, 89개의 세부 지표에 대해 쌍대 비교 방식의 AHP 조사를 하였다. AHP 조사를 위한 전문가패널은 개인정보보호에 대한 지식 및 경험 보유 등을 판단하여 <표 Ⅲ-11>과 같이 10명으로 구성하였다.

<표 Ⅲ-11> AHP 조사를 위한 전문가 풀 구성

구분	분야	경력
1	변호사	10년
2	박사	25년
3	개인정보보호 분야 전문가	12년
4	개인정보보호 분야 전문가	14년
5	개인정보보호 실무자	10년
6	개인정보보호 실무자	10년
7	개인정보보호 실무자	10년
8	개인정보보호 실무자	10년
9	개인정보보호 실무자	10년
10	개인정보보호 실무자	10년

3.3.2 조사 방법 및 자료처리

가. 조사 절차 및 방법

3차 조사에서 사용된 AHP 설문지는 2차례의 델파이 질문을 통해서 나온 전문가들의 의견을 범주화하고 2차 델파이 응답 결과에 따라 5개의 상위 분류, 16개의 하위개념, 89개의 세부 지표에 대해 쌍대 비교 방식의 AHP 질문지를 구성하였다. 상위개념과 하위개념, 평가지표의 혼동을 막기 위해 별지의 용어에 대한 설명을 통하여 응답의 오류를 최소화하고자 하였다. AHP 조사는 2022년 2월 14일부터 2월 16일까지 3일 동안 진행되었으며, 1차 델파이 조사에 참여했던 전문가 중에서 개별 인터뷰가 가능한 전문가 10명에게 E-mail을 통해 발송하였고 개별 인터뷰로 진행하였다.

이 연구에서는 Saaty (1982)의 AHP 연구 방법을 적용하여 연구를 진행 함에 있어 일반적으로 쌍대 비교의 측정값에 대한 신뢰도를 나타내는 일관성 비율(CR : Consistency Ratio)은 0.1 이하일 때 가장 합리적으로 판단하였다[63][64].

수거한 응답지를 분석한 결과를 통해 각 구성 요소별 중요도를 도출하였다. 상대적 중요도를 도출하기 위해 일관성 비율이 적절한 응답지를 코딩된 자료에서 각 평가 요인들의 기하평균을 구한 값을 최종적으로 활용하였다.

나. 자료처리

3차 설문인 AHP를 통해 도출된 자료는 Microsoft Excel 2018과 Export Choice 11을 통하여 일관성 비율(C.R)을 검토하고 중요도와 우선순위, 가중치를 도출하였다.

3.4 델파이/AHP 조사분석 결과

3.4.1 델파이 조사 분석 결과

가. 델파이 조사 전문가패널의 일반적 특성

본 연구에서 선정한 전문가패널의 일반적 특성은 다음과 같다. 1차 델파이 조사 시의 패널은 총 15명으로 개인정보 보호법 관련 변호사 2명, 박사 1명, 개인정보보호 및 정보보호 관리체계(ISMS-P) 분야 전문가 4명, 관련 경력 10년 이상 8명으로 선정되었다. 2차 델파이 조사 시의 패널은 총 13명으로 개인정보 보호법 관련 변호사 1명, 박사 1명, 개인정보보호 및 정보보호 분야 전문가 4명, 관련 경력 10년 이상 7명으로 다음의 <표 Ⅲ-12>와 같이 선정되었다.

<표 Ⅲ-12> 델파이 조사 전문가패널의 일반적 특성

구분		응답 인원(명)	
		1차	2차
전문 분야	변호사	2	1
	전문가	4	4
학력	박사	1	1
경력	10년 이상	8	7
계		15	13

나. 1차 델파이 조사 분석 결과

전문가 집단을 대상으로 한 1차 델파이 조사의 결과는 사전 연구를 통해 설정된 획·설계단계 PbD 적용, 개인정보 생애주기의 보호, 안전성 확보 조치, 개인정보 관리 수준 점검 및 개선, 권리보장 및 윤리역량 등 5개의 상위개념에 따라 전문가 개개인이 평가항목으로 필요하다고 판단되는 요소들을 자유스럽게 기술하는 개방형 설문조사 방법을 통하여 자료를 수집하고 분석하였다.

조사 결과 15명의 전문가가 연구에 참여하였으며, 5개의 평가항목에 필요한 평

가 요인들은 총 89개의 세부 지표가 나열되었다. 1차 조사에서 파악된 총 89개의 개념을 정리하여 3명의 전문가와 같이 전문가 회의를 하였다.

전문가 회의를 통해 89개의 세부 지표 중 제거할 필요가 있는 세부 지표는 없는 것으로 확인되었고, 용어 수정이 필요한 요인에 대한 의견은 <표 Ⅲ-13>과 같다.

<표 Ⅲ-13> 용어 수정이 필요한 요인

구분	총 항목수	용어 수정이 필요한 요인
개인정보 관리역량 성숙도 상위개념	1	* 계획·설계 단계 PbD 적용 → 사전 계획 및 설계단계

1차 델파이 조사 분석 결과와 전문가 회의에서 반영한 각 평가 요인별 의미가 유사하거나 동일하다고 판단되는 개념들을 통합하거나 제거한 결과는 <표 Ⅲ-14>와 같으며, 최종적으로 89개의 세부 지표를 도출하였다.

<표 Ⅲ-14> 1차 델파이 설문조사 결과

상위 개념	하위 개념	세부 지표		측정 항목
사전 계획 및 설계 단계	업무처리 흐름 분석	1	개인정보 처리 업무 처리 흐름도·흐름표 작성	처리하려는 업무 흐름도 및 흐름표를 작성하였는지 확인하고 처리한다.
		2	업무처리 흐름도·흐름표 개정관리	업무 흐름도 및 흐름표는 최신 상태로 유지되고 있는지 확인하고 처리한다.
	개인정보 흐름 분석	3	개인정보 수집, 이용, 보유기간 적절성 검토	개인정보를 수집하는 경우 목적에 필요한 최소한의 범위에서만 수집하도록 계획하고, 개인정보 보유기간을 명확한 근거에 의하여 정하고 있는지 확인하고 처리한다.
		4	주민등록번호, 민감정보, 고유 식별정보 처리 적절성 검토	주민등록번호 수집 시 법령에 근거하고 있으며, 인터넷 홈페이지는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있도록 계획하고, 민감정보, 고유 식별정보를 처리하는 경우 다른 개인정보의 처리에 대한 동의와 별도로 구분하여 동의받도록 계획하고 있는지 확인하고 처리한다.

상위 개념	하위 개념	세부 지표		측정 항목
		5	개인정보 수집 항목 구분 적절성 검토	개인정보를 수집하는 경우 필수항목과 선택항목을 분리하고 선택적으로 동의할 수 있는 사항에 동의하지 아니하여도 서비스 이용이 가능하도록 계획하고 있는지 확인하고 처리한다.
		6	만 14세 미만의 아동 정보수집 적절성 검토	만 14세 미만의 아동 개인정보 수집 시, 법정 대리인에게 동의받도록 계획하고 있는지 확인하고 처리한다.
		7	제3자 제공, 위·수탁 적절성 검토	제3자 제공에 관한 사항을 정보 주체에게 알리고 받도록 계획하고, 위수탁 업무인지 여부를 확인하고 처리한다.
		8	개인정보의 타 시스템 연계 적절성 검토	개인정보 처리 업무가 타 시스템과 연계되는지 검토하고 적절하게 연계되도록 계획하고 있는지 확인하고 처리한다.
		9	개인정보 안전성 확보 조치 적절성 검토	개인정보의 안전성 확보 조치 계획을 명확한 근거에 의하여 수립하고 있는지 확인하고 처리한다.
		10	개인정보 처리 흐름도 작성 및 이력 관리	개인정보 처리 흐름도 작성 및 이력 관리하고 있는지 확인하고 처리한다.
		11	개인정보 처리 흐름표 작성 및 이력 관리	개인정보 처리 흐름표 작성 및 이력 관리하고 있는지 확인하고 처리한다.
	개인정보 안전성 분석	12	개인정보 처리 위험도 및 침해요인 분석	개인정보 처리에 따른 위험도 및 침해요인을 분석하고 처리한다.
		13	개인정보 위험평가 분석	개인정보 처리에 따른 위험도 및 침해요인 결과에 따라 위험평가를 분석하고 처리한다.
		14	개인정보의 보호 대책 선정	개인정보의 개인정보 위험평가 분석 결과를 바탕으로 보호 대책을 수립하고 처리한다.
		15	개인정보의 보호 대책 구현	개인정보의 보호 대책 수립 결과를 바탕으로 보호 이행 대책을 구현하고 처리한다.

상위 개념	하위 개념	세부 지표		측정 항목
	관리체계 수립	16	개인정보보호 정책 수립 적절성 검토	개인정보보호 정책, 조직, 예산이 적절하게 수립하고 있는지를 확인하고 처리한다.
		17	법적 요구사항 준수 적절성 검토	개인정보 처리 업무 관련 법적 요구사항을 검토하고 준수 절차를 수립하여 처리한다.
		18	관리체계 점검 및 개선 계획 수립 적절성 검토	관리체계 수립 결과를 바탕으로 보호조치 개선방안이 계획되어 있는지 확인하고 처리한다.
개인정보 생애주기 보호	수집	19	개인정보 수집 필수사항 안내 및 동의	개인정보 수집 시 4가지 필수사항(수집 목적, 수집 항목, 보유 및 이용 기간, 동의 거부권 및 거부 시 불이익)을 안내하고 동의받고 있는지 확인하고 처리한다.
		20	목적별 최소한의 필수정보 수집	목적별 최소한의 필수정보만 수집하고 있는지 확인하고 처리한다.
		21	개인정보 수집 항목의 필수와 선택정보 구분	개인정보 수집 항목을 필수정보와 선택정보를 구분하여 동의받고 있는지 확인하고 처리한다.
		22	민감정보 처리 별도 동의	민감정보 처리를 위해 별도 동의받고 있는지 확인하고 처리한다.
		23	고유 식별정보 별도 동의	고유 식별정보(여권번호, 운전면허번호, 외국인등록번호) 수집할 때 별도의 동의를 받고 있는지 확인하고 처리한다.
		24	만 14세 미만의 아동의 정보수집 시 법정 대리인 동의	만 14세 미만의 아동 개인정보 수집 시, 법정 대리인에게 동의받고 있는지 확인하고 처리한다.
		25	주민등록번호 수집 제한 법적 준수	법률에서 구체적으로 처리를 요구하거나 허용하는 경우를 제외하고 주민등록번호를 처리하지 않고 있는지 확인하고 처리한다.
		26	선택정보 동의 거부 시 서비스 제공	뉴스레터, 마케팅, 홍보를 위한 개인정보 수집에 동의하지 않더라도 기본적인 서비스를 제공하고 있는지 확인하고 처리한다.
		27	개인정보의 국외 이전 안내 및 동의	개인정보의 국외 이전 시, 정보 주체에게 알리고 동의받고 있는지 확인하고 처리한다.

상위 개념	하위 개념	세부 지표		측정 항목
	이용 및 제공	28	개인정보 처리 위탁 계약서 작성 및 체결	개인정보의 처리 업무를 위탁하는 경우, 개인정보 위탁계약서를 작성하고 있는지 확인하고 처리한다.
		29	위탁업무의 정보 공개	위탁업무의 내용과 수탁자(위탁받아 처리하는 자)를 공개하고 있는지 확인하고 처리한다.
		30	수탁자 대상 교육 및 관리 감독	수탁자에 대한 관리·감독을 수행하고 있는지 확인하고 처리한다.
		31	목적 내 제3자 이용·제공 시 필수사항 고지 및 동의	수집하는 개인정보를 목적 내 제3자에게 제공 시 필수 고지항목(제공받는 자, 이용목적, 개인정보 항목, 보유 및 이용 기간, 동의 거부권 및 거부 시 불이익 내용)을 안내하고 동의받고 있는지 확인하고 처리한다.
		32	목적 외 제3자 이용·제공 시 필수사항 고지 및 동의	목적 외 제3자 이용·제공 시 필수 고지항목(제공받는 자, 이용목적, 개인정보 항목, 보유 및 이용 기간, 동의 거부권 및 거부 시 불이익 내용)을 안내하고 동의받고 있는지 확인하고 처리한다.
		33	목적 외 제3자 이용·제공 사항 공고	공공기관은 개인정보의 목적 외 이용 또는 제3자 제공에 관한 사항에 관한 공고를 하고 있는지 확인하고 처리한다.
		34	개인정보 이용 및 제3자 제공 대장 기록 관리	목적 외 제3자 이용·제공 사항을 관리대장에 기록 관리하고 있는지 확인하고 처리한다.
	보관 및 파기	35	개인정보 자료 보관실의 잠금장치 및 출입 통제	개인정보 자료를 잠금장치가 된 캐비닛 등 안전한 장소에 보관하고 있는지 확인하고 처리한다.
		36	개인정보 저장 장비의 잠금장치 및 출입 통제	개인정보를 저장하고 있는 전산장비는 잠금장치 및 출입 통제가 되어 있는지 확인하고 처리한다.
		37	개인정보 파기 기간 준수	보유기간이 경과 되거나 처리목적 달성된 개인정보는 보유 및 이용 기간 종료 후 5일 이내에 즉시 파기하고 있는지 확인하고 처리한다.
		38	개인정보 파일 파기 절차 준수	개인정보 파일 파기 시 개인정보보호 책임자의 승인 절차를 준수하는지 확인하고 처리한다.
		39	개인정보 파기 방법 적절성	개인정보 파기 시 복원·재생할 수 없는 형태로 완전하게 파기하는지 확인하고 처리한다.
		40	개인정보 파일 파기 관리대장 기록 관리	개인정보 파기에 관한 사항을 기록하고 관리하고 있는지 확인하고 처리한다.

상위 개념	하위 개념	세부 지표		측정 항목
안전성 확보 조치	내부 관리계획	41	내부 관리계획 수립 및 이력 관리	개인정보의 안전한 처리를 위한 내부 관리계획을 수립하고 이력 관리하고 있는지 확인하고 처리한다.
		42	내부 관리계획 이행 점검 및 개선	안전한 처리를 위한 내부 관리계획에 대한 이행 점검을 반기 1회 이상 하고 있는지 확인하고 처리한다.
	접근관리	43	접근권한 절차 수립 및 이력 관리	개인정보 처리시스템의 중요도(민감도) 및 업무 연관성 등을 고려하여 담당자별 차등 접근권한 절차를 마련하고 이력 관리하고 있는지 확인하고 처리한다.
		44	접근권한 차등 부여	개인정보 처리시스템에 대한 접속 권한을 업무 수행 개인정보 취급자에게만 개인별(ID)별로 부여하였는지 확인하고 처리한다.
		45	접근권한 변경내역 기록 및 관리	개인정보 처리시스템 접근권한의 부여·변경·말소 내역을 기록하고, 최소 3년간 이를 보관하고 있는지 확인하고 처리한다.
	접근통제	46	안전한 비밀번호 작성 규칙 적용	개인정보 처리시스템 접속 시 안전한 비밀번호 작성 규칙을 적용하고 있는지 확인하고 처리한다.
		47	계정 오류 입력 접근제한 설정	계정정보(ID) 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 접근을 제한하고 있는지 확인하고 처리한다.
		48	부재 시 시스템 접속 차단 설정	일정 시간 이상 업무처리하지 않는 경우 시스템 접속을 차단하고 있는지 확인하고 처리한다.
		49	비업무용 사이트 접속 차단 설정	파일 공유용 P2P, 웹하드, 도박 등 유해 사이트 접속을 차단하고 있는지 확인하고 처리한다.
		50	비인가자 접근 차단	비인자자가 관리용 기기에 접근하여 임의 조작 못하도록 조치하고 있는지 확인하고 처리한다.
		51	안전한 접속(또는 인증) 수단 적용	개인정보 처리시스템에 접속 시 안전한 접속 수단이나 안전한 인증수단을 적용하고 있는지 확인하고 처리한다.
		52	관리용 단말기 접근통제	관리용 단말기가 본래 목적 외로 사용되지 않도록 조치하고 있는지 확인하고 처리한다.

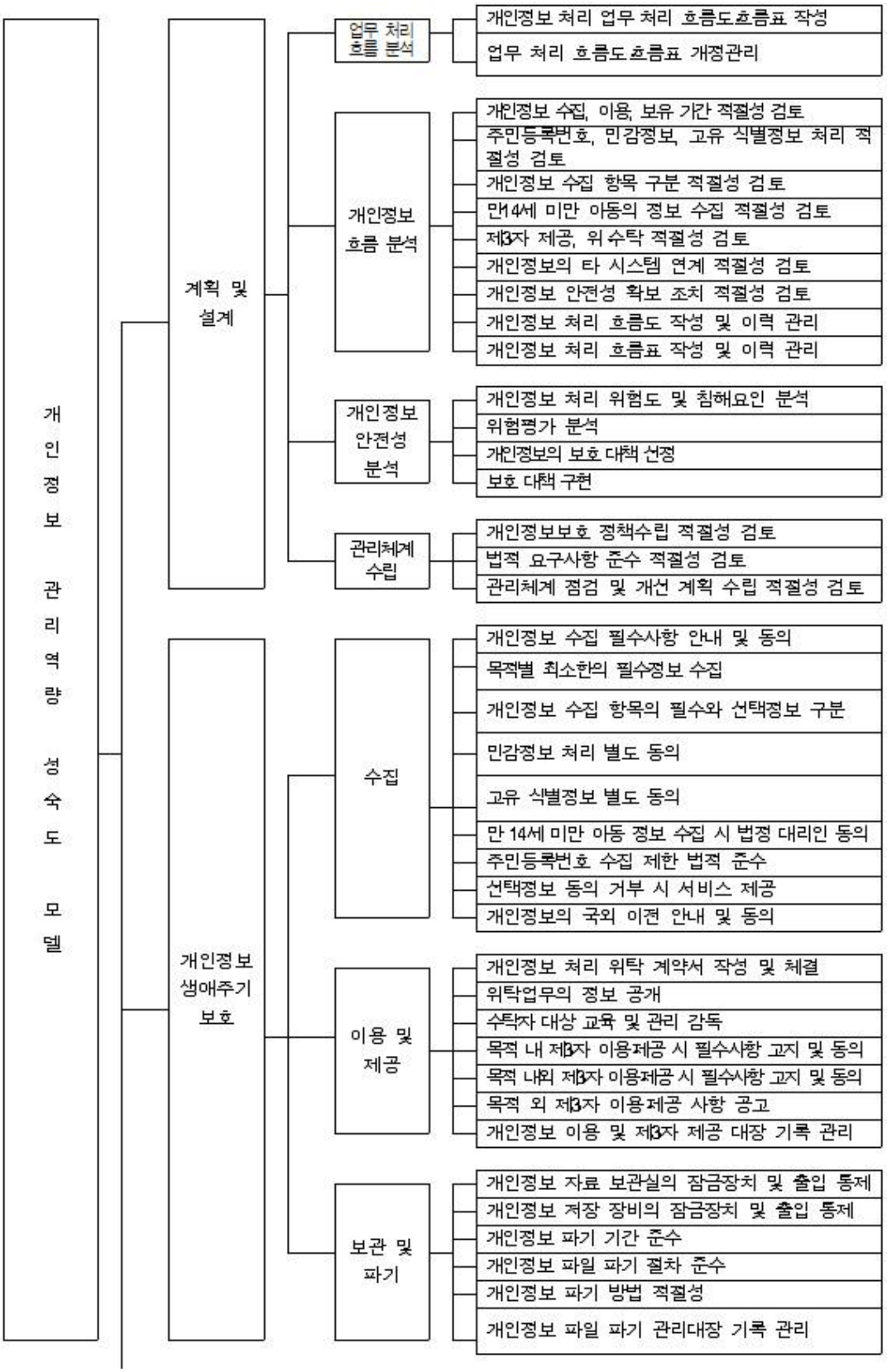
상위 개념	하위 개념	세부 지표		측정 항목
	접속기록 관리	53	개인정보 취급자의 접속기록 보관 기간 설정	개인정보 취급 업무담당자의 접속기록을 최소 1년 이상(5만 명 이상의 개인정보를 처리하거나, 고유 식별정보 또는 민감정보를 처리하는 경우는 2년 이상) 보관하고 있는지 확인하고 처리한다.
		54	접속기록 필수정보 적용	개인정보 취급자 및 처리 업무를 확인할 수 있도록 개인정보 취급자의 계정, 접속일시, 접속지 정보, 처리한 정보 주체 정보, 수행업무(조회, 다운로드 등) 등을 확인할 수 있도록 하였는지 확인하고 처리한다.
		55	접속기록의 안전한 보관	개인정보 처리시스템 접속기록이 위·변조 및 도난, 분실되지 않도록 안전하게 보관하고 있는지 확인하고 처리한다.
		56	접속기록 점검 관리	개인정보의 오남용, 분실·유출·도난·변조 또는 훼손 등을 대응을 위해 접속기록을 월 1회 이상 점검 및 후속 조치를 하고 있는지 확인하고 처리한다.
	개인정보의 암호화	57	개인정보의 암호화	고유 식별정보(주민등록번호, 여권번호 등), 비밀번호, 바이오 정보(지문, 얼굴 등)가 암호화되어 있는지 확인하고 처리한다.
		58	비밀번호의 암호화	비밀번호는 일방향 암호화를 적용하여 저장되는지 확인하고 처리한다.
개인정보 관리 수준 점검 및 개선	관리/기술적 보호	59	개인정보 관리 정책의 점검 및 검토	개인정보 처리 방침, 관련 계획 및 지침, 가이드, 매뉴얼 등 관련 정책서가 법적 준거성과 현실에 맞게 수립되어 있는지를 연 1회 이상 점검하고 보완 조치계획을 하고 있는지 확인하고 처리한다.
		60	개인정보 관리 정책의 개선	개인정보 처리 방침, 관련 계획 및 지침, 가이드, 매뉴얼 등 관련 정책서가 법적 준거성과 현실에 맞게 수립하였는지 점검한 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.
		61	개인정보 관리 점검 및 검토	개인정보 생애주기, 안전성 확보 조치 등 개인정보 관리실태를 연 1회 이상 점검하고 보완 조치계획을 하고 있는지 확인하고 처리한다.

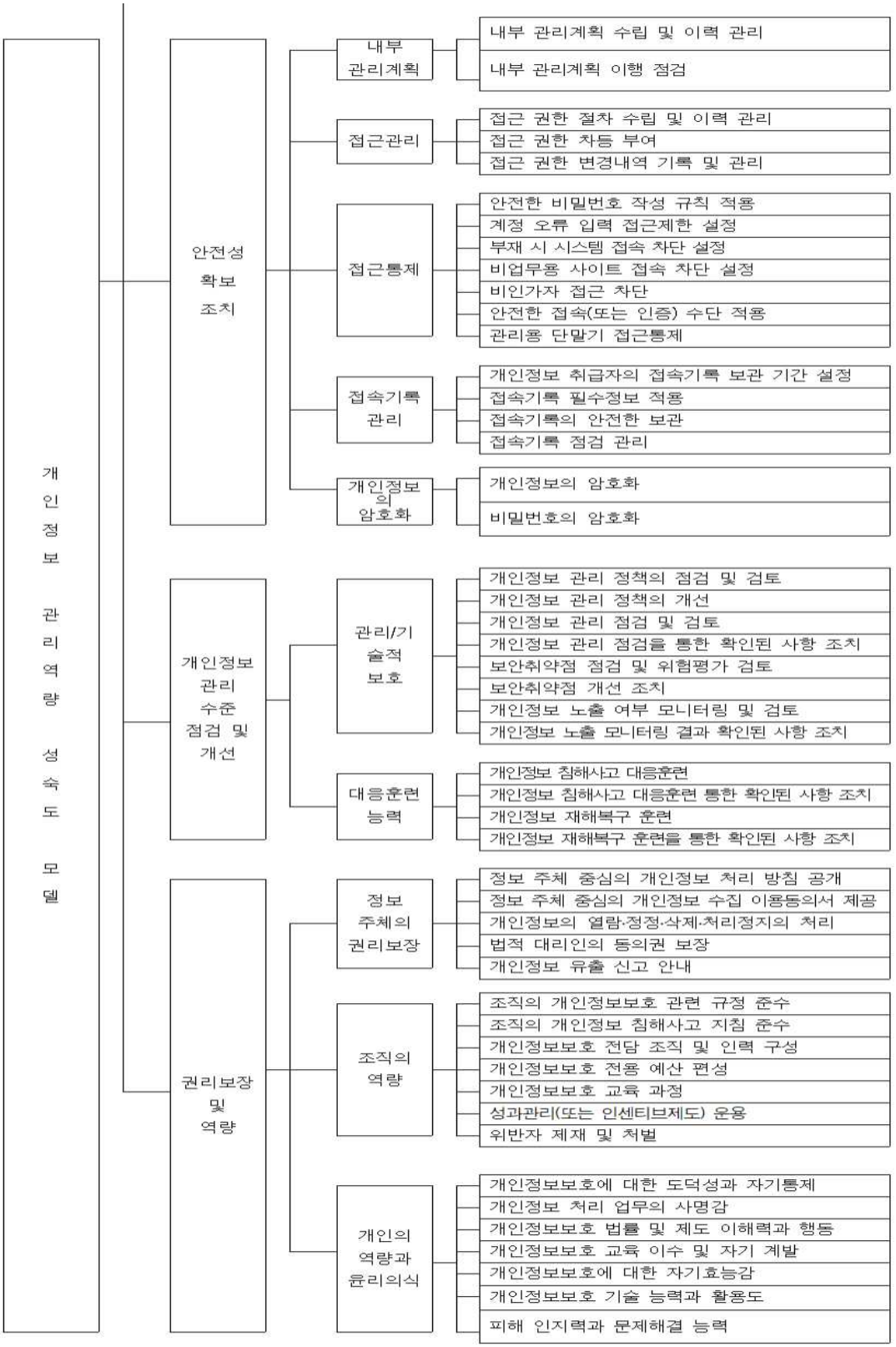
상위 개념	하위 개념	세부 지표		측정 항목
		62	개인정보 관리 점검 결과 확인된 사항 조치	개인정보 생애주기, 안전성 확보 조치 등 개인정보 관리실태 점검 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.
		63	보안취약점 점검 및 위험평가 검토	개인정보 처리시스템 또는 홈페이지를 통해 해킹 사고가 발생하지 않도록 연 1회 이상 취약점 점검을 수행하고 위험 분석 평가, 보완 조치계획을 하고 있는지 확인하고 처리한다.
		64	보안취약점 개선 조치	개인정보 처리시스템 또는 홈페이지 보안취약점 점검 점검한 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.
		65	개인정보 노출 여부 모니터링 및 검토	홈페이지, 개인정보 처리시스템을 통해 개인정보 노출 여부를 월 1회 이상 모니터링하고 보완 조치계획을 하고 있는지 확인하고 처리한다.
		66	개인정보 노출 모니터링 결과 확인된 사항 조치	개인정보 노출 여부 모니터링 점검한 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.
	대응훈련 능력	67	개인정보 침해사고 대응훈련	개인정보 유출 사고 발생 시 개인정보 유출 사고 대응계획에 따라 신속히 대응하여 그 피해를 최소화하기 위해 개인정보 침해사고 대응 훈련을 실시하고, 결과에 따른 보완 조치계획을 하고 있는지 확인하고 처리한다.
		68	개인정보 침해사고 대응훈련 통한 확인된 사항 조치	개인정보 침해사고 대응훈련 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.
		69	개인정보 재해복구 훈련	재해재난 발생 시 개인정보 처리시스템 보호를 위해 수립된 위기 대응 매뉴얼에 따라 모의훈련을 실시하고 보완 조치계획을 하고 있는지 확인하고 처리한다.
		70	개인정보 재해복구 훈련을 통한 확인된 사항 조치	개인정보 처리시스템 재해복구 훈련 결과에 따른 필요한 보완 조치를 하였는지 확인하고 처리한다.

상위 개념	하위 개념	세부 지표		측정 항목
권리 보장 및 윤리 역량	정보 주체의 권리보장	71	정보 주체 중심의 개인정보 처리 방침 공개	개인정보 처리 방침을 정보 주체가 알기 쉽게 필수사항을 모두 투명·명확하게 포함하여 수립하고, 홈페이지 등 정보 주체가 쉽게 확인할 수 있도록 주기적으로 공개하고 있는지 확인하고 처리한다.
		72	정보 주체 중심의 개인정보 수집 이용 동의서 제공	개인정보 수집 이용동의서는 정보 주체가 알기 쉽게 구성하고, 민감정보 등 중요한 부분은 글씨 크기, 굵기, 색상, 밑줄 등을 처리하였는지 확인하고 처리한다.
		73	개인정보의 열람·정정·삭제·처리정지의 처리	개인정보의 열람·정정·삭제 및 처리정지에 관한 사항을 안내하고, 절차에 따라 적법·명확하게 처리하고 있는지 확인하고 처리한다.
		74	법적 대리인의 동의권 보장	만14세 미만의 아동의 개인정보를 처리하는 경우, 해당 아동의 법정 대리인 동의를 받고, 그 과정에서 법정 대리인이 동의를 거부하거나 동의 의사가 확인되지 않는 경우에는 해당 법정 대리인의 개인정보를 5일 이내 파기하고 있는지 확인하고 처리한다.
		75	개인정보 유출 신고 안내	개인정보 침해 사실을 신고할 수 있는 방법을 정보 주체에게 안내하고 있는지 확인하고 처리한다.
	조직의 역량	76	조직의 개인정보보호 관련 규정 준수	우리 조직의 개인정보보호 관련 규정을 마련되어 있는지 확인하고 처리한다.
		77	조직의 개인정보 침해사고 지침 준수	우리 조직의 개인정보 침해사고에 대한 지침이 마련되어 있는지 확인하고 처리한다.
		78	개인정보보호 전담 조직 및 인력 구성	조직 내 개인정보보호 전담 조직 및 인력이 구성되어 있는지 확인하고 처리한다.
		79	개인정보보호 전용 예산 편성	개인정보보호 전용 예산을 편성하고, 개선을 위한 예산 증액 노력을 하고 있는지 확인하고 처리한다.
		80	개인정보보호 교육 과정 운영 및 평가	임직원 및 수탁자 등 맞춤형 개인정보보호 교육 프로그램을 운영하고 있는지 확인하고 처리한다.

상위 개념	하위 개념	세부 지표		측정 항목
		81	성과관리(또는 인센티브제도) 운용	조직구성원의 개인정보 관리역량을 높일 수 있도록 성과관리 또는 인센티브 제도를 운영하고 있는지 확인하고 처리한다.
		82	위반자 제재 및 처벌	우리 조직은 개인정보 오남용, 유출 위반자에 대해서 규정에 따라 투명하고 공정하게 제재와 처벌을 하고 있는지 확인하고 처리한다.
	개인의 역량과 윤리의식	83	개인정보보호에 대한 도덕성과 자기통제	우리 조직의 개인정보보호 관련 규정과 처벌 규정을 잘 알고 있고, 자신이 하고 싶은 대로 하고자 하는 충동이 일어날 때 충동을 극복하고자 하는 개인의 노력을 하고 있는지 확인하고 처리한다.
		84	개인정보 처리 업무의 사명감	조직구성원으로서 사명감과 직업의식을 가지고 맡은 일에 대한 투철한 책임 의식이 있는지 확인하고 처리한다.
		85	개인정보보호 법률 및 제도 이해력과 행동	조직 내 개인정보보호를 위해 규정된 규범을 조직구성원이 개인정보보호에 긍정적이고, 이를 성공적으로 수행할 수 있도록 하고 있는지 확인하고 처리한다.
		86	개인정보보호 교육이수 및 자기 계발	개인정보보호 교육에 어느 정도 관심이 있고, 연 몇 회를 이수하고 있는지 확인하고 자기계발을 통해 관리능력을 향상시키는 노력을 한다.
		87	개인정보보호에 대한 자기효능감	개인정보보호 업무를 위해 주어진 정책에 대해 성공적으로 수행할 수 있다는 개인의 기대감 정도(보안정책 인지, 습득, 적용, 적응 정도)를 확인하고 노력한다.
		88	개인정보보호 기술능력과 활용도	개인정보 처리시스템 또는 업무용 단말기의 안전조치 방법을 어느 정도 알고 있고, 이를 수행하고 있는지 확인하고 처리한다.
		89	피해 인지력과 문제해결 능력	개인정보 침해사고 대응 절차를 잘 이해하고 있고, 개인정보 침해사고 대응훈련에 적극 참여하여 대응능력을 키우고자 노력하고, 침해사고가 발생하면 즉시 문제를 해결할 수 있다.

전문가 회의를 통해 1차 델파이 조사를 통해 도출된 89개의 세부 지표를 유사 항목으로 분류하여 하위개념을 설정하여 구조화하였으며 전문가 회의 참여자 전원의 합의된 구조는 [그림 Ⅲ-1]과 같다.





[그림 Ⅲ-1] 델파이 조사를 통해 도출된 평가지표의 구조

다. 2차 델파이 조사 분석 결과

2차 델파이 조사에서는 “개인정보 관리역량 성숙도 모델” 평가지표의 항목에 대한 검증과 이후 3차 조사인 상대적 중요도의 평가를 위해 1차 델파이 조사 분석 결과를 반영한 89개의 세부 지표로 구성된 2차 설문지를 13명의 전문가 패널에게 배부, 회수를 통해 분석하였다. 2차 델파이 조사를 통한 평가항목들의 중요도 평가에서는 평균값이 3.00 미만인 평가항목을 제거하고자 하였고, 평가항목에 대한 중요도를 파악하기 위하여 CVR 값이 0.54 이상이면 타당한 개념으로, Cronbach′s α 값은 0.60 이상이면 신뢰도가 있는 것으로 보았다.

2차 델파이 조사 분석 결과는 <표 Ⅲ-15>와 같다. 89개의 세부 지표 전체의 CVR 값은 0.54~1.00으로, Cronbach′s α 값의 평균은 0.85로 타당도와 신뢰도가 적절하다고 나타났다.

<표 Ⅲ-15> 2차 델파이 조사 분석 결과

하위개념	세부 지표	M	SD	CVR	Cronbach's α
업무처리 흐름 분석	개인정보 처리 업무처리 흐름도·흐름표 작성	4.38	0.62	0.85	0.90
	업무처리 흐름도·흐름표 개정관리	4.15	0.66	0.69	
개인정보 흐름 분석	개인정보 수집, 이용, 보유기간 적절성 검토	4.31	0.72	0.85	0.96
	주민등록번호, 민감정보, 고유 식별정보 처리 적절성 검토	4.46	0.63	0.69	
	개인정보 수집 항목 구분 적절성 검토	4.31	0.72	0.85	
	만 14세 미만의 아동 정보수집 적절성 검토	4.46	0.63	0.69	
	제3자 제공, 위·수탁 적절성 검토	4.38	0.74	0.85	
	개인정보의 타 시스템 연계 적절성 검토	4.46	0.63	0.69	
	개인정보 안전성 확보 조치 적절성 검토	4.31	0.72	0.85	
	개인정보 처리 흐름도 작성 및 이력 관리	4.46	0.63	0.69	
	개인정보 처리 흐름표 작성 및 이력 관리	4.38	0.74	0.85	
개인정보 안전성 분석	개인정보 처리 위험도 및 침해요인 분석	4.31	0.72	0.69	0.79
	개인정보 위험평가 분석	4.54	0.50	1.00	
	개인정보의 보호 대책 선정	4.62	0.62	0.85	
	개인정보의 보호 대책 구현	4.38	0.62	0.85	

하위개념	세부 지표	M	SD	CVR	Cronbach's α
관리체계 수립	개인정보보호 정책 수립 적절성 검토	4.31	0.72	0.69	0.81
	법적 요구사항 준수 적절성 검토	4.46	0.63	0.85	
	관리체계 점검 및 개선 계획 수립 적절성 검토	4.38	0.74	0.69	
수집	개인정보 수집 필수사항 안내 및 동의	4.31	0.72	0.69	0.92
	목적별 최소한의 필수정보 수집	4.38	0.74	0.69	
	개인정보 수집 항목의 필수와 선택정보 구분	4.23	0.80	0.54	
	민감정보 처리 별도 동의	4.31	0.82	0.54	
	고유 식별정보 별도 동의	4.38	0.74	0.69	
	만 14세 미만의 아동의 정보수집 시 법정 대리인 동의	4.46	0.63	0.85	
	주민등록번호 수집 제한 법적 준수	4.23	0.80	0.54	
	선택정보 동의 거부 시 서비스 제공	4.46	0.63	0.85	
	개인정보의 국외 이전 안내 및 동의	4.15	0.66	0.69	
이용 및 제공	개인정보 처리 위탁 계약서 작성 및 체결	4.62	0.74	0.69	0.71
	위탁업무의 정보 공개	4.38	0.74	0.69	
	수탁자 대상 교육 및 관리 감독	4.77	0.58	0.85	
	목적 내 제3자 이용·제공 시 필수사항 고지 및 동의	4.38	0.74	0.69	
	목적 외 제3자 이용·제공 시 필수사항 고지 및 동의	4.31	0.72	0.69	
	목적 외 제3자 이용·제공 사항 공고	4.38	0.62	0.85	
	개인정보 이용 및 제3자 제공 대장 기록 관리	4.46	0.63	0.85	
보관 및 파기	개인정보 자료 보관실의 잠금장치 및 출입 통제	4.46	0.75	0.69	0.72
	개인정보 저장 장비의 잠금장치 및 출입 통제	4.38	0.74	0.69	
	개인정보 파기 기간 준수	4.69	0.61	0.85	
	개인정보 파일 파기 절차 준수	4.46	0.63	0.85	
	개인정보 파기 방법 적절성	4.31	0.46	1.00	
	개인정보 파일 파기 관리대장 기록 관리	4.46	0.63	0.85	
내부 관리계획	내부 관리계획 수립 및 이력 관리	4.46	0.50	1.00	0.92
	내부 관리계획 이행점검 및 개선	4.54	0.50	1.00	
접근관리	접근권한 절차 수립 및 이력 관리	4.60	0.49	1.00	0.82
	접근권한 차등 부여	4.60	0.49	1.00	
	접근권한 변경내역 기록 및 관리	4.20	0.60	0.80	

하위개념	세부 지표	M	SD	CVR	Cronbach's α
접근통제	안전한 비밀번호 작성 규칙 적용	4.46	0.75	0.69	0.78
	계정 오류 입력 접근제한 설정	4.38	0.74	0.69	
	부재 시 시스템 접속 차단 설정	4.69	0.61	0.85	
	비업무용 사이트 접속 차단 설정	4.46	0.63	0.85	
	비인가자 접근 차단	4.46	0.63	0.85	
	안전한 접속(또는 인증) 수단 적용	4.31	0.46	1.00	
	관리용 단말기 접근통제	4.46	0.63	0.85	
접속기록 관리	개인정보 취급자의 접속기록 보관 기간 설정	4.38	0.74	0.69	0.82
	접속기록 필수정보 적용	4.31	0.72	0.69	
	접속기록의 안전한 보관	4.46	0.63	0.85	
	접속기록 점검 관리	4.54	0.63	0.85	
개인정보의 암호화	개인정보의 암호화	4.62	0.49	1.00	0.92
	비밀번호의 암호화	4.69	0.46	1.00	
관리/기술적 보호	개인정보 관리 정책의 점검 및 검토	4.54	0.50	1.00	0.96
	개인정보 관리 정책의 개선	4.31	0.72	0.69	
	개인정보 관리 점검 및 검토	4.62	0.49	1.00	
	개인정보 관리 점검결과 확인된 사항 조치	4.38	0.62	0.85	
	보안취약점 점검 및 위험평가 검토	4.62	0.49	1.00	
	보안취약점 개선 조치	4.38	0.62	0.85	
	개인정보 노출 여부 모니터링 및 검토	4.54	0.63	0.85	
	개인정보 노출 모니터링 결과 확인된 사항 조치	4.46	0.50	1.00	
대응훈련 능력	개인정보 침해사고 대응훈련	4.54	0.50	1.00	0.91
	개인정보 침해사고 대응훈련 통한 확인된 사항 조치	4.31	0.72	0.69	
	개인정보 재해복구 훈련	4.62	0.49	1.00	
	개인정보 재해복구 훈련을 통한 확인된 사항 조치	4.38	0.62	0.85	

하위개념	세부 지표	M	SD	CVR	Cronbach's α
정보 주체의 권리보장	정보 주체 중심의 개인정보 처리 방침 공개	4.46	0.50	1.00	0.87
	정보 주체 중심의 개인정보 수집 이용동의서 제공	4.62	0.49	1.00	
	개인정보의 열람·정정·삭제·처리정지의 처리	4.31	0.72	0.69	
	법적 대리인의 동의권 보장	4.46	0.63	0.85	
	개인정보 유출 신고 안내	4.54	0.50	1.00	
조직의 역량	조직의 개인정보보호 관련 규정 준수	4.46	0.50	1.00	0.85
	조직의 개인정보 침해사고 지침 준수	4.69	0.46	1.00	
	개인정보보호 전담 조직 및 인력 구성	4.31	0.72	0.69	
	개인정보보호 전용 예산 편성	4.54	0.63	0.85	
	개인정보보호 교육과정 운영 및 평가	4.23	0.70	0.69	
	성과관리(또는 인센티브제도) 운용	4.54	0.50	1.00	
	위반자 제재 및 처벌	4.62	0.49	1.00	
개인의 역량과 윤리의식	개인정보보호에 대한 도덕성과 자기통제	4.31	0.61	0.85	0.86
	개인정보 처리 업무의 사명감	4.54	0.63	0.85	
	개인정보보호 법률 및 제도 이해력과 행동	4.31	0.46	1.00	
	개인정보보호 교육 이수 및 자기 계발	4.38	0.74	0.69	
	개인정보보호에 대한 자기효능감	4.77	0.58	0.85	
	개인정보보호 기술 능력과 활용도	4.69	0.72	0.69	
	피해 인지력과 문제해결 능력	4.62	0.49	1.00	

2차에 걸쳐 실시한 델파이 조사를 통해 도출된 평가항목의 수는 <표 Ⅲ-16>과 같으며 최종적으로 사전 계획 및 설계에서 18개의 항목, 개인정보 생애주기 보호에서 22개의 항목, 안전성 확보 조치에서 18개 항목, 개인정보 관리 수준 진단 점검 및 개선에서 12개, 권리보장 및 윤리역량에서 19개의 항목으로 총 89개의 항목이 최종 도출되었다.

<표 Ⅲ-16> 델파이 조사 도출 평가항목 수

구분	상위개념	도출된 평가항목 수	
		1차	2차
1	사전 계획 및 설계	18	18
2	개인정보 생애주기 보호	22	22
3	안전성 확보 조치	18	18
4	개인정보 관리 수준 진단 점검 및 개선	12	12
5	권리보장 및 윤리역량	19	19
계		89	89

최종 도출된 세부 지표에 대한 측정 문항을 정리하면 다음 <표 Ⅲ-17>과 같다.

<표 Ⅲ-17> 최종 도출된 측정 문항

상위 개념	하위 개념	세부 지표		측정 문항
사전 계획 및 설계 단계	업무처리 흐름 분석	1	개인정보 처리 업무 처리 흐름도·흐름표 작성	처리하려는 업무 흐름도 및 흐름표를 작성하였는지 확인하고 처리한다.
		2	업무처리 흐름도·흐름표 개정관리	업무 흐름도 및 흐름표는 최신 상태로 유지되고 있는지 확인하고 처리한다.
	개인정보 흐름 분석	3	개인정보 수집, 이용, 보유기간 적절성 검토	개인정보를 수집하는 경우 목적에 필요한 최소한의 범위에서만 수집하도록 계획하고, 개인정보 보유기간을 명확한 근거에 의하여 정하고 있는지 확인하고 처리한다.
		4	주민등록번호, 민감정보, 고유 식별정보 처리 적절성 검토	주민등록번호 수집 시 법령에 근거하고 있으며, 인터넷 홈페이지는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있도록 계획하고, 민감정보, 고유 식별정보를 처리하는 경우 다른 개인정보의 처리에 대한 동의와 별도로 구분하여 동의받도록 계획하고 있는지 확인하고 처리한다.

상위 개념	하위 개념	세부 지표		측정 문항
		5	개인정보 수집 항목 구분 적절성 검토	개인정보를 수집하는 경우 필수항목과 선택항목을 분리하고 선택적으로 동의할 수 있는 사항에 동의하지 아니하여도 서비스 이용이 가능하도록 계획하고 있는지 확인하고 처리한다.
		6	만 14세 미만의 아동 정보수집 적절성 검토	만 14세 미만의 아동 개인정보 수집 시, 법정 대리인에게 동의받도록 계획하고 있는지 확인하고 처리한다.
		7	제3자 제공, 위·수탁 적절성 검토	제3자 제공에 관한 사항을 정보 주체에게 알리고 받도록 계획하고, 위수탁 업무인지 여부를 확인하고 처리한다.
		8	개인정보의 타 시스템 연계 적절성 검토	개인정보 처리 업무가 타 시스템과 연계되는지 검토하고 적절하게 연계되도록 계획하고 있는지 확인하고 처리한다.
		9	개인정보 안전성 확보 조치 적절성 검토	개인정보의 안전성 확보 조치계획을 명확한 근거에 의하여 수립하고 있는지 확인하고 처리한다.
		10	개인정보 처리 흐름도 작성 및 이력 관리	개인정보 처리 흐름도 작성 및 이력 관리하고 있는지 확인하고 처리한다.
		11	개인정보 처리 흐름표 작성 및 이력 관리	개인정보 처리 흐름표 작성 및 이력 관리하고 있는지 확인하고 처리한다.
	개인정보 안전성 분석	12	개인정보 처리 위험도 및 침해요인 분석	개인정보 처리에 따른 위험도 및 침해요인을 분석하고 처리한다.
		13	개인정보 위험평가 분석	개인정보 처리에 따른 위험도 및 침해요인 결과에 따라 위험평가를 분석하고 처리한다.
		14	개인정보의 보호 대책 선정	개인정보의 개인정보 위험평가 분석 결과를 바탕으로 보호 대책을 수립하고 처리한다.
		15	개인정보의 보호 대책 구현	개인정보의 보호 대책 수립 결과를 바탕으로 보호 이행 대책을 구현하고 처리한다.

상위 개념	하위 개념	세부 지표		측정 문항
	관리체계 수립	16	개인정보보호 정책 수립 적절성 검토	개인정보보호 정책, 조직, 예산이 적절하게 수립하고 있는지를 확인하고 처리한다.
		17	법적 요구사항 준수 적절성 검토	개인정보 처리 업무 관련 법적 요구사항을 검토하고 준수 절차를 수립하여 처리한다.
		18	관리체계 점검 및 개선 계획 수립 적절성 검토	관리체계 수립 결과를 바탕으로 보호조치 개선방안이 계획되어 있는지 확인하고 처리한다.
개인정보 생애주기 보호	수집	19	개인정보 수집 필수사항 안내 및 동의	개인정보 수집 시 4가지 필수사항(수집 목적, 수집 항목, 보유 및 이용 기간, 동의 거부권 및 거부 시 불이익)을 안내하고 동의받고 있는지 확인하고 처리한다.
		20	목적별 최소한의 필수정보 수집	목적별 최소한의 필수정보만 수집하고 있는지 확인하고 처리한다.
		21	개인정보 수집 항목의 필수와 선택정보 구분	개인정보 수집 항목을 필수정보와 선택정보를 구분하여 동의받고 있는지 확인하고 처리한다.
		22	민감정보 처리 별도 동의	민감정보 처리를 위해 별도 동의받고 있는지 확인하고 처리한다.
		23	고유 식별정보 별도 동의	고유 식별정보(여권번호, 운전면허번호, 외국인등록번호) 수집할 때 별도의 동의를 받고 있는지 확인하고 처리한다.
		24	만 14세 미만의 아동의 정보수집 시 법정 대리인 동의	만 14세 미만의 아동 개인정보 수집 시, 법정 대리인에게 동의받고 있는지 확인하고 처리한다.
		25	주민등록번호 수집 제한 법적 준수	법률에서 구체적으로 처리를 요구하거나 허용하는 경우를 제외하고 주민등록번호를 처리하지 않고 있는지 확인하고 처리한다.
		26	선택정보 동의 거부 시 서비스 제공	뉴스레터, 마케팅, 홍보를 위한 개인정보 수집에 동의하지 않더라도 기본적인 서비스를 제공하고 있는지 확인하고 처리한다.
		27	개인정보의 국외 이전 안내 및 동의	개인정보의 국외 이전 시, 정보 주체에게 알리고 동의받고 있는지 확인하고 처리한다.

상위 개념	하위 개념	세부 지표		측정 문항
	이용 및 제공	28	개인정보 처리 위탁 계약서 작성 및 체결	개인정보의 처리 업무를 위탁하는 경우, 개인정보 위탁계약서를 작성하고 있는지 확인하고 처리한다.
		29	위탁업무의 정보 공개	위탁업무의 내용과 수탁자(위탁받아 처리하는 자)를 공개하고 있는지 확인하고 처리한다.
		30	수탁자 대상 교육 및 관리 감독	수탁자에 대한 관리·감독을 수행하고 있는지 확인하고 처리한다.
		31	목적 내 제3자 이용·제공 시 필수사항 고지 및 동의	수집하는 개인정보를 목적 내 제3자에게 제공 시 필수 고지항목(제공받는 자, 이용목적, 개인정보 항목, 보유 및 이용 기간, 동의 거부권 및 거부 시 불이익 내용)을 안내하고 동의받고 있는지 확인하고 처리한다.
		32	목적 외 제3자 이용·제공 시 필수사항 고지 및 동의	목적 외 제3자 이용·제공 시 필수 고지항목(제공받는 자, 이용목적, 개인정보 항목, 보유 및 이용 기간, 동의 거부권 및 거부 시 불이익 내용)을 안내하고 동의받고 있는지 확인하고 처리한다.
		33	목적 외 제3자 이용·제공 사항 공고	공공기관은 개인정보의 목적 외 이용 또는 제3자 제공에 관한 사항에 관한 공고를 하고 있는지 확인하고 처리한다.
		34	개인정보 이용 및 제3자 제공 대장 기록 관리	목적 외 제3자 이용·제공 사항을 관리대장에 기록 관리하고 있는지 확인하고 처리한다.
	보관 및 파기	35	개인정보 자료 보관실의 잠금장치 및 출입 통제	개인정보 자료를 잠금장치가 된 캐비닛 등 안전한 장소에 보관하고 있는지 확인하고 처리한다.
		36	개인정보 저장 장비의 잠금장치 및 출입 통제	개인정보를 저장하고 있는 전산장비는 잠금장치 및 출입 통제가 되어 있는지 확인하고 처리한다.
		37	개인정보 파기 기간 준수	보유기간이 경과 되거나 처리목적 달성된 개인정보는 보유 및 이용 기간 종료 후 5일 이내에 즉시 파기하고 있는지 확인하고 처리한다.
		38	개인정보 파일 파기 절차 준수	개인정보 파일 파기 시 개인정보보호 책임자의 승인 절차를 준수하는지 확인하고 처리한다.
		39	개인정보 파기 방법 적절성	개인정보 파기 시 복원·재생할 수 없는 형태로 완전하게 파기하는지 확인하고 처리한다.
		40	개인정보 파일 파기 관리대장 기록 관리	개인정보 파기에 관한 사항을 기록하고 관리하고 있는지 확인하고 처리한다.

상위 개념	하위 개념	세부 지표		측정 문항
안전성 확보 조치	내부 관리 계획	41	내부 관리계획 수립 및 이력 관리	개인정보의 안전한 처리를 위한 내부 관리계획을 수립하고 이력 관리하고 있는지 확인하고 처리한다.
		42	내부 관리계획 이행 점검 및 개선	안전한 처리를 위한 내부 관리계획에 대한 이행 점검을 반기 1회 이상 하고 있는지 확인하고 처리한다.
	접근 관리	43	접근권한 절차 수립 및 이력 관리	개인정보 처리시스템의 중요도(민감도) 및 업무 연관성 등을 고려하여 담당자별 차등 접근권한 절차를 마련하고 이력 관리하고 있는지 확인하고 처리한다.
		44	접근권한 차등 부여	개인정보 처리시스템에 대한 접속 권한을 업무 수행 개인정보 취급자에게만 개인별(ID)별로 부여하였는지 확인하고 처리한다.
		45	접근권한 변경내역 기록 및 관리	개인정보 처리시스템 접근권한의 부여·변경·말소 내역을 기록하고, 최소 3년간 이를 보관하고 있는지 확인하고 처리한다.
	접근 통제	46	안전한 비밀번호 작성 규칙 적용	개인정보 처리시스템 접속 시 안전한 비밀번호 작성 규칙을 적용하고 있는지 확인하고 처리한다.
		47	계정 오류 입력 접근제한 설정	계정정보(ID) 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 접근을 제한하고 있는지 확인하고 처리한다.
		48	부재 시 시스템 접속 차단 설정	일정 시간 이상 업무처리하지 않는 경우 시스템 접속을 차단하고 있는지 확인하고 처리한다.
		49	비업무용 사이트 접속 차단 설정	파일 공유용 P2P, 웹하드, 도박 등 유해 사이트 접속을 차단하고 있는지 확인하고 처리한다.
		50	비인가자 접근 차단	비인자자가 관리용 기기에 접근하여 임의 조작 못하도록 조치하고 있는지 확인하고 처리한다.
		51	안전한 접속(또는 인증) 수단 적용	개인정보 처리시스템에 접속 시 안전한 접속 수단이나 안전한 인증수단을 적용하고 있는지 확인하고 처리한다.
		52	관리용 단말기 접근 통제	관리용 단말기가 본래 목적 외로 사용되지 않도록 조치하고 있는지 확인하고 처리한다.

상위 개념	하위 개념	세부 지표		측정 문항
	접속 기록 관리	53	개인정보 취급자의 접속기록 보관 기간 설정	개인정보 취급 업무담당자의 접속기록을 최소 1년 이상(5만 명 이상의 개인정보를 처리하거나, 고유 식별정보 또는 민감정보를 처리하는 경우는 2년 이상) 보관하고 있는지 확인하고 처리한다.
		54	접속기록 필수정보 적용	개인정보 취급자 및 처리 업무를 확인할 수 있도록 개인정보 취급자의 계정, 접속일시, 접속지 정보, 처리한 정보 주체 정보, 수행업무(조회, 다운로드 등) 등을 확인할 수 있도록 하였는지 확인하고 처리한다.
		55	접속기록의 안전한 보관	개인정보 처리시스템 접속기록이 위·변조 및 도난, 분실되지 않도록 안전하게 보관하고 있는지 확인하고 처리한다.
		56	접속기록 점검 관리	개인정보의 오남용, 분실·유출·도난·변조 또는 훼손 등을 대응을 위해 접속기록을 월 1회 이상 점검 및 후속 조치를 하고 있는지 확인하고 처리한다.
	개인 정보의 암호화	57	개인정보의 암호화	고유 식별정보(주민등록번호, 여권번호 등), 비밀번호, 바이오 정보(지문, 얼굴 등)가 암호화되어 있는지 확인하고 처리한다.
		58	비밀번호의 암호화	비밀번호는 일방향 암호화를 적용하여 저장되는지 확인하고 처리한다.
개인 정보 관리 수 준 점검 및 개선	관리/ 기술적 보호	59	개인정보 관리 정책의 점검 및 검토	개인정보 처리 방침, 관련 계획 및 지침, 가이드, 매뉴얼 등 관련 정책서가 법적 준거성과 현실에 맞게 수립되어 있는지를 연 1회 이상 점검하고 보완 조치계획을 하고 있는지 확인하고 처리한다.
		60	개인정보 관리 정책의 개선	개인정보 처리 방침, 관련 계획 및 지침, 가이드, 매뉴얼 등 관련 정책서가 법적 준거성과 현실에 맞게 수립하였는지 점검한 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.
		61	개인정보 관리 점검 및 검토	개인정보 생애주기, 안전성 확보 조치 등 개인정보 관리실태를 연 1회 이상 점검하고 보완 조치계획을 하고 있는지 확인하고 처리한다.
		62	개인정보 관리 점검 결과 확인된 사항 조치	개인정보 생애주기, 안전성 확보 조치 등 개인정보 관리실태 점검 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.

상위 개념	하위 개념	세부 지표		측정 문항
		63	보안취약점 점검 및 위험평가 검토	개인정보 처리시스템 또는 홈페이지를 통해 해킹 사고가 발생하지 않도록 연 1회 이상 취약점 점검을 수행하고 위험 분석 평가, 보완 조치계획을 하고 있는지 확인하고 처리한다.
		64	보안취약점 개선 조치	개인정보 처리시스템 또는 홈페이지 보안취약점 점검 점검한 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.
		65	개인정보 노출 여부 모니터링 및 검토	홈페이지, 개인정보 처리시스템을 통해 개인정보 노출 여부를 월 1회 이상 모니터링하고 보완 조치계획을 하고 있는지 확인하고 처리한다.
		66	개인정보 노출 모니터링 결과 확인된 사항 조치	개인정보 노출 여부 모니터링 점검한 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.
	대응 훈련 능력	67	개인정보 침해사고 대응훈련	개인정보 유출 사고 발생 시 개인정보 유출 사고 대응계획에 따라 신속히 대응하여 그 피해를 최소화하기 위해 개인정보 침해사고 대응훈련을 하고, 결과에 따른 보완 조치계획을 하고 있는지 확인하고 처리한다.
		68	개인정보 침해사고 대응훈련 통한 확인된 사항 조치	개인정보 침해사고 대응훈련 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.
		69	개인정보 재해복구 훈련	재해재난 발생 시 개인정보 처리시스템 보호를 위해 수립된 위기 대응 매뉴얼에 따라 모의훈련을 실시하고 보완 조치계획을 하고 있는지 확인하고 처리한다.
		70	개인정보 재해복구 훈련을 통한 확인된 사항 조치	개인정보 처리시스템 재해복구 훈련 결과에 따른 필요한 보완 조치를 하였는지 확인하고 처리한다.

상위 개념	하위 개념	세부 지표		측정 문항
권리 보장 및 윤리 역량	정보 주체의 권리보장	71	정보 주체 중심의 개인정보 처리 방침 공개	개인정보 처리 방침을 정보 주체가 알기 쉽게 필수사항을 모두 투명.명확하게 포함하여 수립하고, 홈페이지 등 정보 주체가 쉽게 확인할 수 있도록 주기적으로 공개하고 있는지 확인하고 처리한다.
		72	정보 주체 중심의 개인정보 수집 이용 동의서 제공	개인정보 수집 이용동의서는 정보 주체가 알기 쉽게 구성하고, 민감정보 등 중요한 부분은 글씨 크기, 굵기, 색상, 밑줄 등을 처리하였는지 확인하고 처리한다.
		73	개인정보의 열람·정정·삭제·처리정지의 처리	개인정보의 열람·정정·삭제 및 처리정지에 관한 사항을 안내하고, 절차에 따라 적법·명확하게 처리하고 있는지 확인하고 처리한다.
		74	법적 대리인의 동의권 보장	만14세 미만의 아동의 개인정보를 처리하는 경우, 해당 아동의 법정 대리인 동의를 받고, 그 과정에서 법정 대리인이 동의를 거부하거나 동의 의사가 확인되지 않는 경우에는 해당 법정 대리인의 개인정보를 5일 이내 파기하고 있는지 확인하고 처리한다.
		75	개인정보 유출 신고 안내	개인정보 침해 사실을 신고할 수 있는 방법을 정보 주체에게 안내하고 있는지 확인하고 처리한다.
	조직의 역량	76	조직의 개인정보보호 관련 규정 준수	우리 조직의 개인정보보호 관련 규정을 마련되어 있는지 확인하고 처리한다.
		77	조직의 개인정보 침해사고 지침 준수	우리 조직의 개인정보 침해사고에 대한 지침이 마련되어 있는지 확인하고 처리한다.
		78	개인정보보호 전담 조직 및 인력 구성	조직 내 개인정보보호 전담 조직 및 인력이 구성되어 있는지 확인하고 처리한다.
		79	개인정보보호 전용 예산 편성	개인정보보호 전용 예산을 편성하고, 개선을 위한 예산 증액 노력을 하고 있는지 확인하고 처리한다.
		80	개인정보보호 교육 과정 운영 및 평가	임직원 및 수탁자 등 맞춤형 개인정보보호 교육 프로그램을 운영하고 있는지 확인하고 처리한다.
		81	성과관리(또는 인센티브제도) 운용	조직구성원의 개인정보 관리역량을 높일 수 있도록 성과관리 또는 인센티브제도를 운영하고 있는지 확인하고 처리한다.
		82	위반자 제재 및 처벌	우리 조직은 개인정보 오남용, 유출 위반자에 대해서 규정에 따라 투명하고 공정하게 제재와 처벌을 하고 있는지 확인하고 처리한다.

상위 개념	하위 개념	세부 지표		측정 문항
	개인의 역량 및 윤리 의식	83	개인정보보호에 대한 도덕성과 자기통제	우리 조직의 개인정보보호 관련 규정과 처벌 규정을 잘 알고 있고, 자신이 하고 싶은 대로 하고자 하는 충동이 일어날 때 충동을 극복하고자 하는 개인의 노력을 하고 있는지 확인하고 처리한다.
		84	개인정보 처리 업무의 사명감	조직구성원으로서 사명감과 직업의식을 가지고 맡은 일에 대한 투철한 책임 의식이 있는지 확인하고 처리한다.
		85	개인정보보호 법률 및 제도 이해력과 행동	조직 내 개인정보보호를 위해 규정된 규범을 조직구성원이 개인정보보호에 긍정적이고, 이를 성공적으로 수행할 수 있도록 하고 있는지 확인하고 처리한다.
		86	개인정보보호 교육 이수 및 자기 계발	개인정보보호 교육에 어느 정도 관심이 있고, 연 몇 회를 이수하고 있는지 확인하고 자기계발을 통해 관리능력을 향상시키는 노력을 한다.
		87	개인정보보호에 대한 자기효능감	개인정보보호 업무를 위해 주어진 정책에 대해 성공적으로 수행할 수 있다는 개인의 기대감 정도(보안정책 인지, 습득, 적용, 적응 정도)를 확인하고 노력한다.
		88	개인정보보호 기술 능력과 활용도	개인정보 처리시스템 또는 업무용 단말기의 안전조치 방법을 어느 정도 알고 있고, 이를 수행하고 있는지 확인하고 처리한다.
		89	피해 인지력과 문제 해결 능력	개인정보 침해사고 대응 절차를 잘 이해하고 있고, 개인정보 침해사고 대응훈련에 적극 참여하여 대응능력을 키우고자 노력하고, 침해사고가 발생하면 즉시 문제를 해결할 수 있다.

3.4.2 AHP 조사분석 결과

가. AHP 조사 전문가패널의 일반적 특성

본 연구에서 선정한 전문가패널의 일반적 특성은 다음과 같다. AHP 조사 시의 패널은 총 10명으로 개인정보 보호법 관련 변호사 1명, 박사 1명, 개인정보보호 및 정보보호 관리체계(ISMS-P) 분야 전문가 2명, 관련 경력 10년 이상 6명으로 다음의 <표 Ⅲ-18>과 같이 선정되었다.

<표 Ⅲ-18> AHP 조사 전문가패널의 일반적 특성

구분		응답 인원(명)
전문 분야	변호사	1
	전문가	1
학력	박사	2
경력	10년 이상	6
계		10

나. AHP 조사분석 결과

“개인정보 관리역량 성숙도 모델” 평가지표 개발을 위한 개념별 우선순위를 도출하고자 사전에 두 차례의 델파이 조사를 통해 도출된 총 89개의 평가지표에 대해 AHP 기법을 통해 상대적 중요도를 분석하였다.

델파이 조사를 통해 도출된 평가지표들의 상대적 중요도와 영향력에 대해 전문가들을 통하여 정량화 및 구조화하기 위해 계층화 분석인 AHP 연구가 적절하다고 판단하였다.

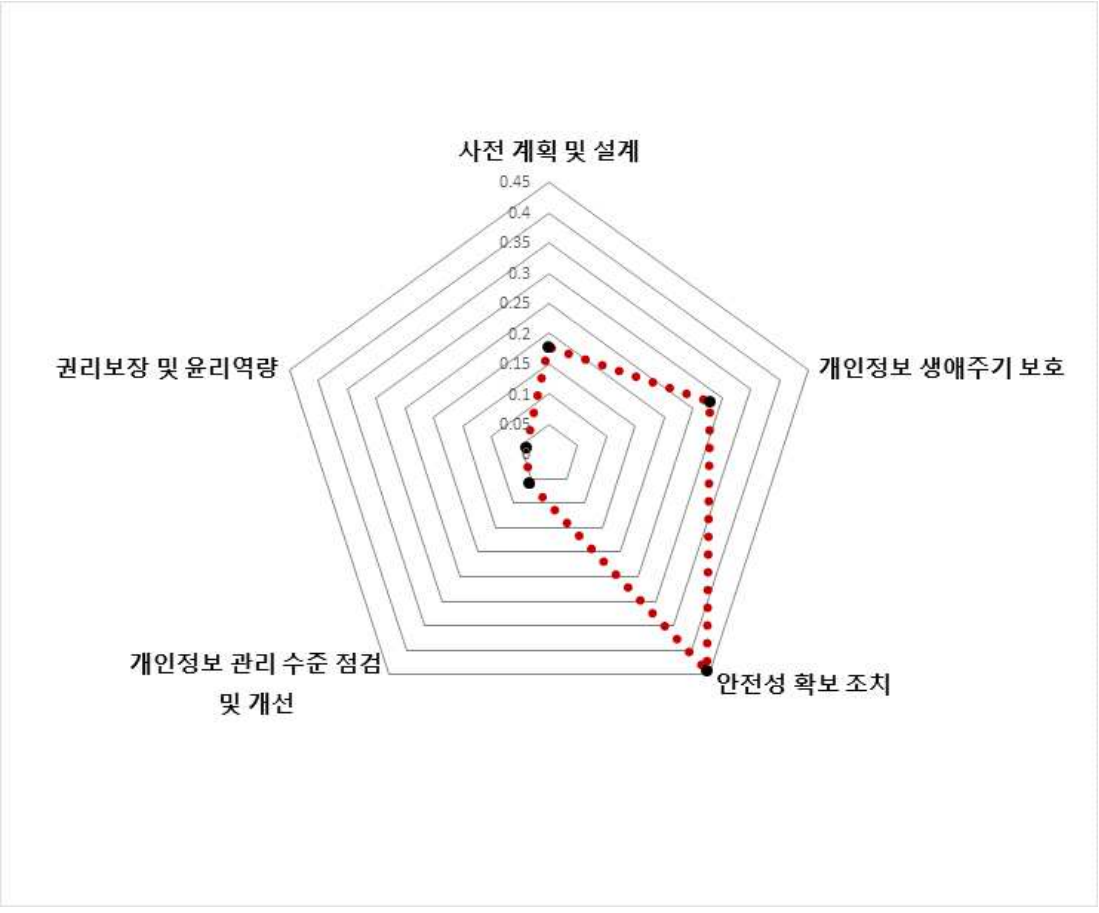
1) 상위개념의 가중치 결과

“개인정보 관리역량 성숙도 모델” 평가지표를 분석하기 위하여 먼저 상위개념에 대해 우선순위를 분석하였다. 분석 결과는 <표 Ⅲ-19>와 같다.

<표 Ⅲ-19> 상위개념의 상대적 중요도 및 순위

구분	상위개념	상대적 중요도	내부순위	CR
1	사전 계획 및 설계	0.179	3	0.028
2	개인정보 생애주기 보호	0.280	2	
3	안전성 확보 조치	0.443	1	
4	개인정보 관리 수준 점검 및 개선	0.057	4	
5	권리보장 및 윤리역량	0.041	5	

상대적 중요도 및 순위는 안전성 확보 조치(0.443), 개인정보 생애주기 보호(0.280), 사전 계획 및 설계(0.179), 개인정보 관리 수준 점검 및 개선(0.057), 권리보장 및 윤리역량(0.041) 순으로 나타났다. 이를 그래프로 표현하면 [그림 Ⅲ-2]와 같다.



[그림 Ⅲ-2] 상위개념의 상대적 중요도

상위요소의 일관성 비율(C.R)은 0.028로 일관성 비율이 0.1 이하인 경우 응답자가 논리적인 일관성을 가지고 응답하였다고 판단할 수 있으므로 일관성 비율이 적절하다고 판단된다.

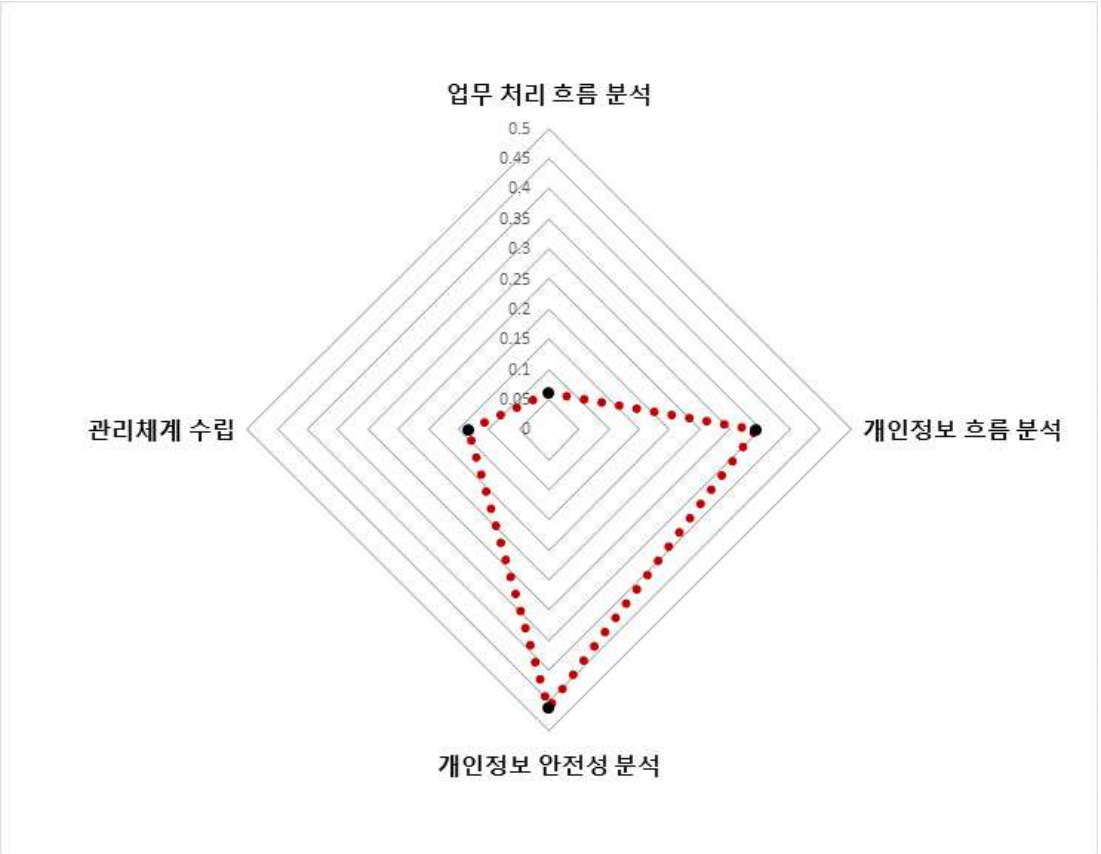
2) 하위개념에 대한 가중치 결과

상위개념에 대한 하위개념의 가중치와 상대적 중요도는 <표 Ⅲ-20>과 같다.

<표 Ⅲ-20> 하위개념 우선순위 및 상위개념 내 상대적 중요도

상위개념	하위개념	상대적 중요도	내부순위	CR
사전 계획 및 설계 (0.179)	업무처리 흐름 분석	0.061	4	0.05
	개인정보 흐름 분석	0.342	2	
	개인정보 안전성 분석	0.463	1	
	관리체계 수립	0.134	3	
개인정보 생애주기 보호 (0.280)	수집	0.387	2	0.019
	이용 및 제공	0.443	1	
	보관 및 파기	0.169	3	
안전성 확보 조치 (0.443)	내부 관리계획	0.224	2	0.064
	접근관리	0.354	1	
	접근통제	0.180	3	
	접속기록 관리	0.137	4	
	개인정보의 암호화	0.104	5	
개인정보 관리 수준 점검 및 개선 (0.057)	관리/기술적 보호	0.25	2	0.000
	대응훈련 능력	0.75	1	
권리보장 및 윤리역량 (0.041)	정보 주체의 권리보장	0.327	2	0.056
	조직의 역량	0.260	3	
	개인의 역량 및 윤리의식	0.413	1	

사전 계획 및 설계단계의 하위개념에 대한 일관성 비율(C.R)은 0.05(C.R<0.10)로 적절하게 나타났으며, 상대적 중요도 및 순위는 [그림 Ⅲ-3]과 같이 개인정보 안전성 분석(0.463), 개인정보 흐름 분석(0.342), 관리체계 수립(0.134), 업무처리 흐름 분석(0.061) 순으로 나타났다.

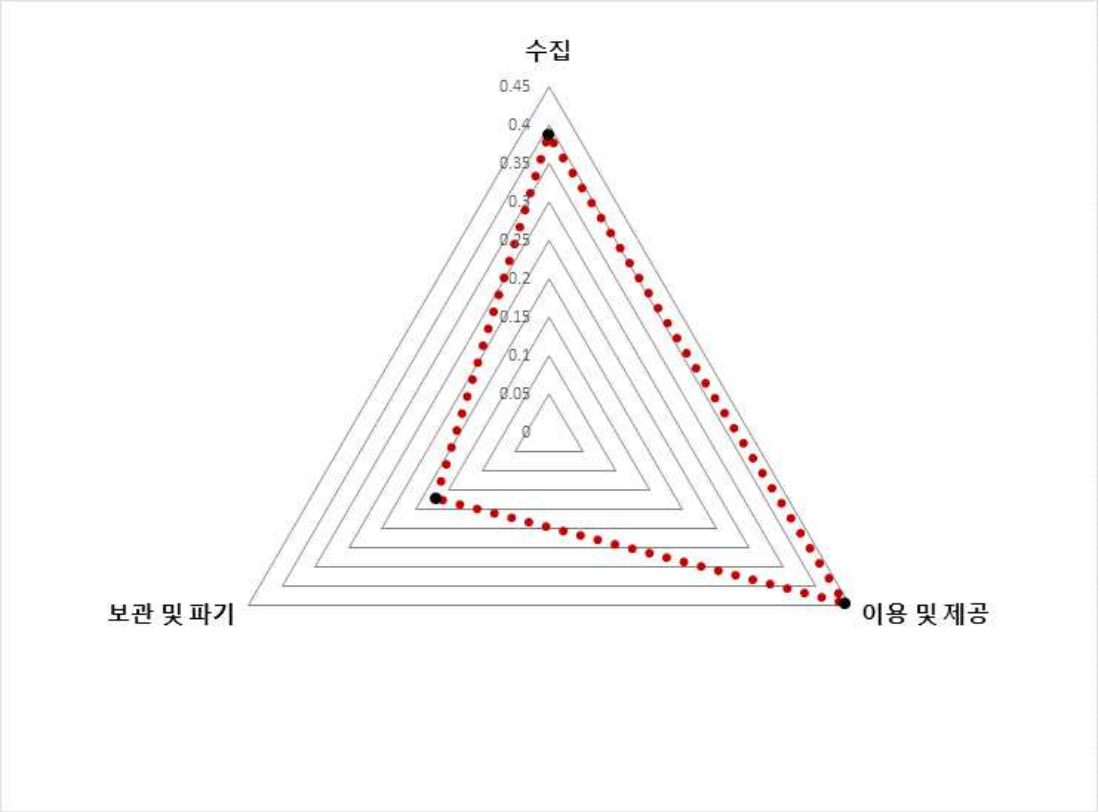


[그림 Ⅲ-3] 사전 계획 및 설계단계 하위개념의 상대적 중요도

<표 Ⅲ-21> 사전 계획 및 설계단계의 하위개념 우선순위 및 상대적 중요도

상위개념	하위개념	상대적 중요도	내부순위	CR
사전 계획 및 설계 (0.179)	업무처리 흐름 분석	0.061	4	0.05
	개인정보 흐름 분석	0.342	2	
	개인정보 안전성 분석	0.463	1	
	관리체계 수립	0.134	3	

개인정보 생애주기 보호 단계의 하위개념에 대한 일관성 비율(C.R)은 0.019(C.R<0.10)로 적절하게 나타났으며, 상대적 중요도 및 순위는 [그림 Ⅲ-4]와 같이 이용 및 제공(0.443), 수집(0.387), 보관 및 파기(0.169) 순으로 나타났다.

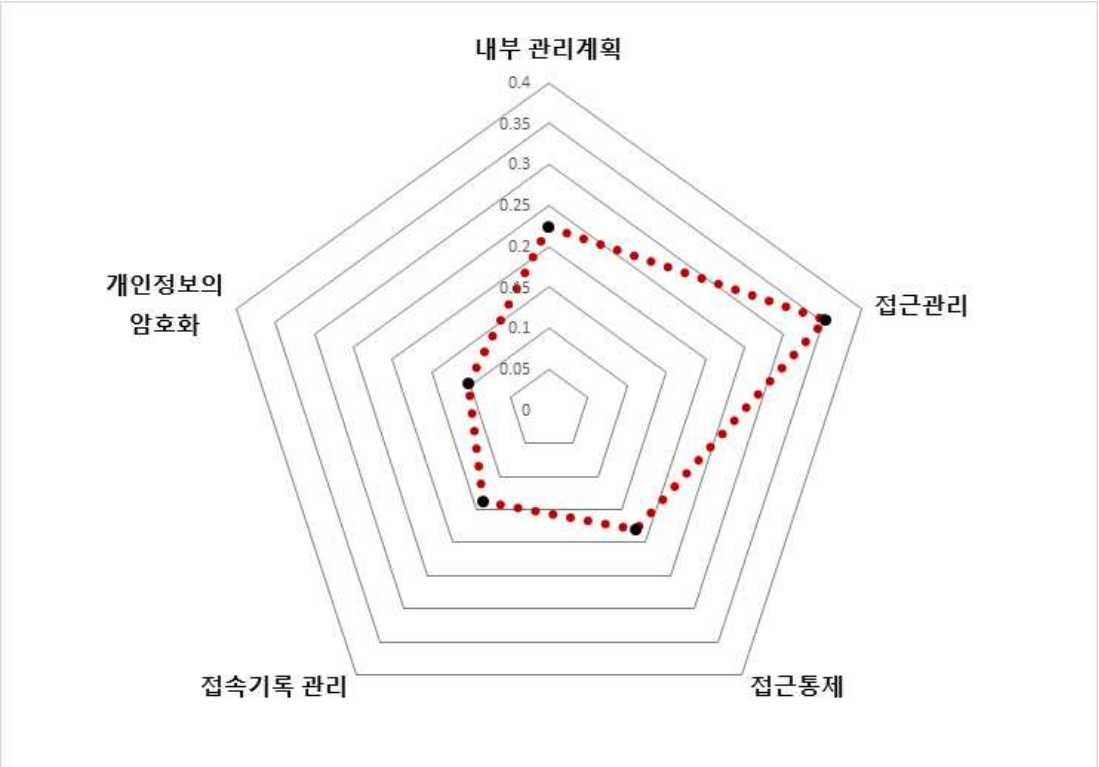


[그림 Ⅲ-4] 개인정보 생애주기 보호 단계 하위개념의 상대적 중요도

<표 Ⅲ-22> 개인정보 생애주기 보호 단계의 하위개념 우선순위 및 상대적 중요도

상위개념	하위개념	상대적 중요도	내부순위	CR
개인정보 생애주기 보호 (0.280)	수집	0.387	2	0.019
	이용 및 제공	0.443	1	
	보관 및 파기	0.169	3	

안전성 확보 조치단계의 하위개념에 대한 일관성 비율(C.R)은 0.095(C.R<0.10)로 양호하게 나타났으며 상대적 중요도 및 순위는 [그림 Ⅲ-5]와 같이 접근관리(0.354), 내부 관리계획(0.224), 접근통제(0.180), 접속기록 관리(0.137), 개인정보의 암호화(0.104) 순으로 나타났다.

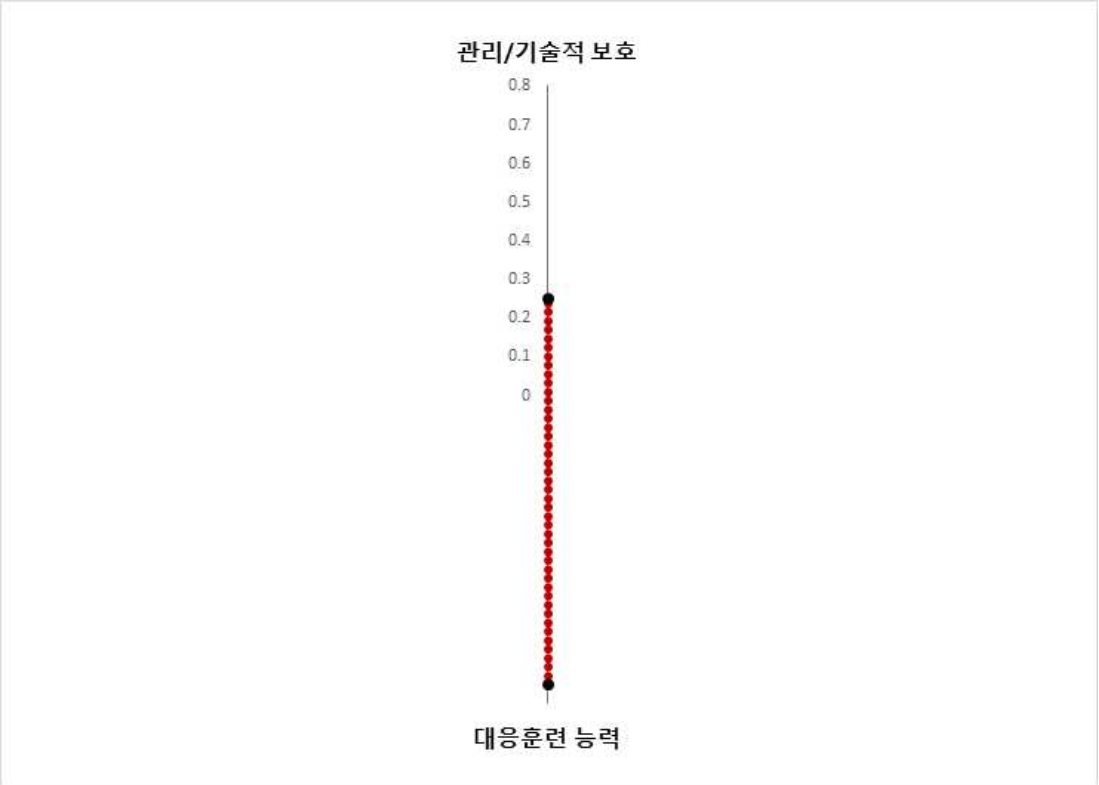


[그림 Ⅲ-5] 안전성 확보 조치단계 하위개념의 상대적 중요도

<표 Ⅲ-23> 안전성 확보 조치단계의 하위개념 우선순위 및 상대적 중요도

상위개념	하위개념	상대적 중요도	내부순위	CR
안전성 확보 조치 (0.443)	내부 관리계획	0.224	2	0.064
	접근관리	0.354	1	
	접근통제	0.180	3	
	접속기록 관리	0.137	4	
	개인정보의 암호화	0.104	5	

개인정보 관리 수준 점검 및 개선단계의 하위개념에 대한 일관성 비율(C.R)은 0.000(C.R<0.10)로 적절하게 나타났으며 상대적 중요도 및 순위는 [그림 Ⅲ-6]과 같이 대응훈련 능력(0.75), 관리/기술적 보호(0.25) 순으로 나타났다.

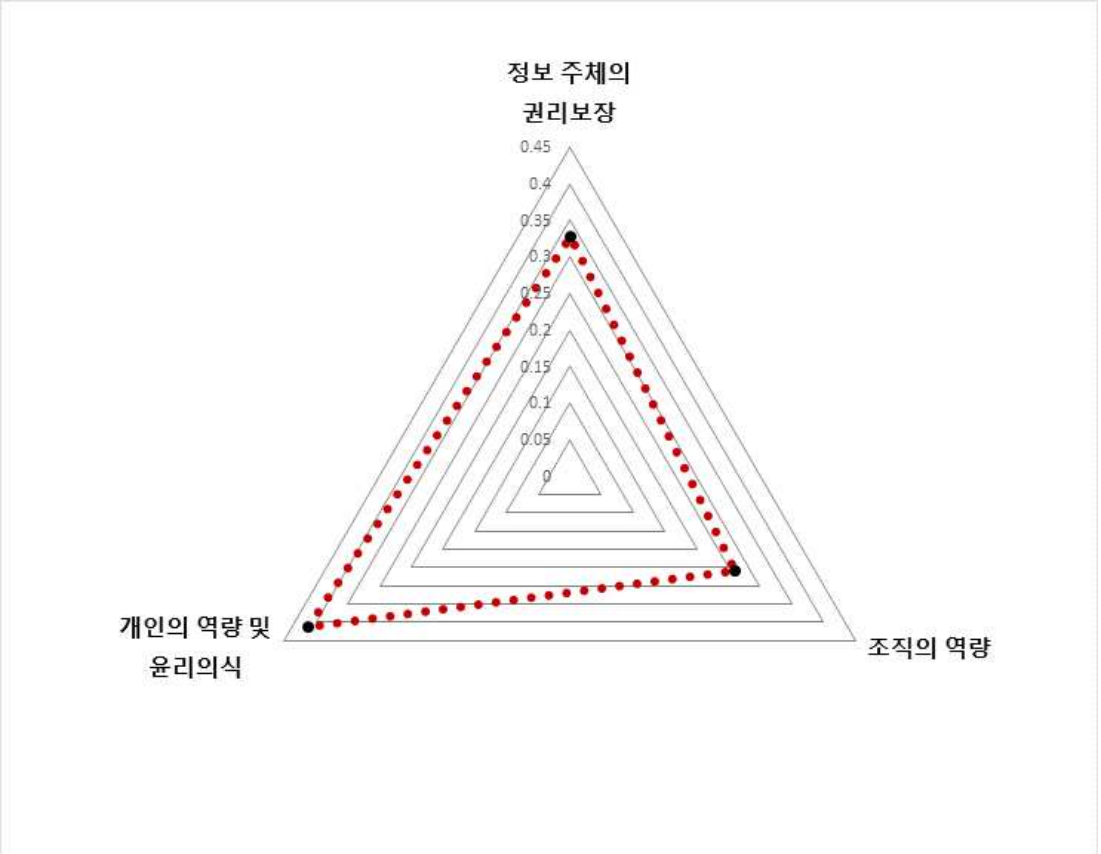


[그림 Ⅲ-6] 개인정보 관리 수준 점검 및 개선단계 하위개념의 상대적 중요도

<표 Ⅲ-24> 개인정보 관리 수준 점검 및 개선단계의 하위개념 우선순위 및 상대적 중요도

상위개념	하위개념	상대적 중요도	내부순위	CR
개인정보 관리 수준 점검 및 개선 (0.057)	관리/기술적 보호	0.25	2	0.000
	대응훈련 능력	0.75	1	

권리보장 및 윤리역량단계의 하위개념에 대한 일관성 비율(C.R)은 0.000(C.R<0.10)로 적절하게 나타났으며 상대적 중요도 및 순위는 [그림 Ⅲ-7]과 같이 개인의 역량 및 윤리(0.413), 정보 주체의 권리보장(0.327), 조직의 역량(0.260) 순으로 나타났다.



[그림 Ⅲ-7] 권리보장 및 윤리역량단계 하위개념의 상대적 중요도

<표 Ⅲ-25> 권리보장 및 윤리역량단계의 하위개념 우선순위 및 상대적 중요도

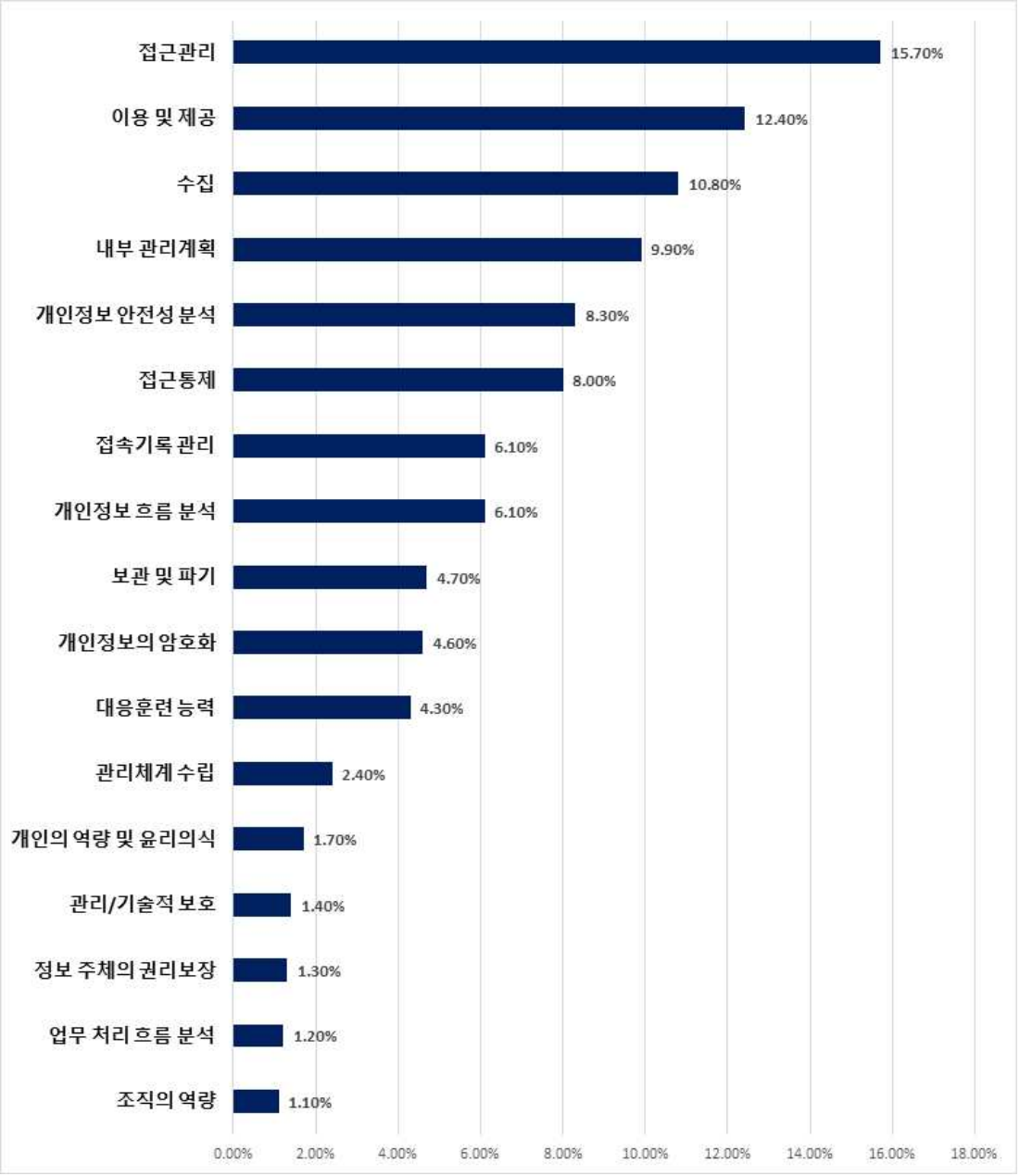
상위개념	하위개념	상대적 중요도	내부순위	CR
권리보장 및 윤리역량 (0.041)	정보 주체의 권리보장	0.327	2	0.056
	조직의 역량	0.260	3	
	개인의 역량 및 윤리의식	0.413	1	

하위개념을 전체 대비 상대적 중요도를 기준으로 순위를 나열하면 <표 Ⅲ-26>과 같이 나타낼 수 있다.

<표 Ⅲ-26> 하위개념 우선순위 및 전체 대비 상대적 중요도

순위	하위개념	전체대비 상대적 중요도	CR
1	접근관리	0.157	
2	이용 및 제공	0.124	
3	수집	0.108	
4	내부 관리계획	0.099	
5	개인정보 안전성 분석	0.083	
6	접근통제	0.080	
7	개인정보 흐름 분석	0.061	
8	접속기록 관리	0.061	
9	보관 및 파기	0.047	0.03
10	개인정보의 암호화	0.046	
11	대응훈련 능력	0.043	
12	관리체계 수립	0.024	
13	개인의 역량 및 윤리의식	0.017	
14	관리/기술적 보호	0.014	
15	정보 주체의 권리보장	0.013	
16	업무처리 흐름 분석	0.012	
17	조직의 역량	0.011	
계		1.000	

전체를 100%로 보았을 때 [그림 Ⅲ-8]과 같이 접근관리는 15.7%를 차지하여 상대적 중요도가 가장 높은 하위개념인 것으로 나타났다. 이용 및 제공은 12.4%, 수집은 10.8%로 나타나 각각 2, 3위로 나타났다. 반면, 상대적 중요도가 가장 낮은 하위개념은 조직의 역량(1.1%)으로 나타났다. 하위개념의 상대적 중요도에 대한 종합 비일관성 비율(overall CVR)은 0.03으로 일관성이 확보되었음을 알 수 있었다.



[그림 Ⅲ-8] 하위개념 우선순위 및 전체 대비 상대적 중요도

3) 세부 지표에 대한 상대적 중요도 및 우선순위

첫 번째, '사전 계획 및 설계단계'에 대한 세부 지표 우선순위 및 상대적 중요도를 살펴보면 <표 Ⅲ-27>과 같다.

<표 Ⅲ-27> 사전 계획 및 설계단계 세부 지표의 상대적 중요도 및 순위

상위 개념	하위 개념	세부 지표	상대적 중요도	내부 순위	CR
사전 계획 및 설계	업무처리 흐름 분석	업무처리 흐름도.흐름표 작성	0.667	1	0.000
		업무처리 흐름도.흐름표 개정 관리	0.333	2	
	개인정보 흐름 분석	개인정보 수집, 이용, 보유기간 적절성 검토	0.123	4	0.084
		주민등록번호, 민감정보, 고유 식별정보 처리 적절성 검토	0.164	3	
		개인정보 수집 항목 구분 적절성 검토	0.067	6	
		개인정보의 타 시스템 연계 적절성 검토	0.071	5	
		만 14세 미만의 아동 정보수집 적절성 검토	0.035	9	
		제3자 제공, 위·수탁 적절성 검토	0.038	8	
		개인정보 안전성 확보 조치 적절성 검토	0.059	7	
		개인정보 처리 흐름도 작성 및 이력 관리	0.229	1	
		개인정보 처리 흐름표 작성 및 이력 관리	0.214	2	
	개인정보 안전성 분석	개인정보 위험평가 분석	0.494	1	0.012
		개인정보 처리 위험도 및 침해요인 분석	0.308	2	
		개인정보의 보호 대책 선정	0.105	3	
		개인정보의 보호 대책 구현	0.093	4	
	관리체계 수립	관리체계 수립	0.126	3	0.010
		법적 요구사항 준수 적절성 검토	0.416	2	
		관리체계 점검 및 개선 계획 수립 적절성 검토	0.458	1	

개인정보 흐름 분석에서의 상대적 중요도 및 순위는 개인정보 처리 흐름도 작성 및 이력 관리(0.229), 개인정보 처리 흐름표 작성 및 이력 관리(0.214), 주민등록번호, 민감정보, 고유 식별정보 처리 적절성 검토(0.164), 개인정보 수집, 이용, 보유기간 적절성 검토(0.123), 개인정보의 타 시스템 연계 적절성 검토(0.071), 개인정보 수집 항목 구분 적절성 검토(0.067), 개인정보 안전성 확보 조치 적절성 검토(0.059), 제3자 제공, 위·수탁 적절성 검토(0.038), 만 14세 미만의 아동 정보 수집 적절성 검토(0.035) 순으로 나타났다. 개인정보 안전성 분석에서의 상대적 중요도 및 순위는 개인정보 위험평가 분석(0.494), 개인정보 처리 위험도 및 침해요인 분석(0.308), 개인정보의 보호 대책 선정(0.105), 개인정보의 보호 대책 구현(0.093) 순으로 나타났다. 관리체계 수립에서의 상대적 중요도 및 순위는 관리체계 점검 및 개선 계획 수립 적절성 검토(0.458), 법적 요구사항 준수 적절성 검토(0.416), 관리체계 수립(0.126) 순으로 나타났다.

모든 항목에 대한 일관성 비율인 C.R값은 0.1 이하로 업무처리 흐름 분석의 C.R값은 0.000, 개인정보 흐름 분석의 C.R값은 0.084, 개인정보 안전성 분석의 C.R값은 0.012, 개인정보 영향평가의 C.R값은 0.010으로 나타나 일관성 있는 것으로 판단된다.

두 번째, '개인정보 생애주기 보호 단계'에 대한 세부 지표 우선순위 및 상대적 중요도를 살펴보면 <표 Ⅲ-28>과 같다.

<표 Ⅲ-28> 개인정보 생애주기 보호 단계 세부 지표의 상대적 중요도 및 순위

상위 개념	하위 개념	세부 지표	상대적 중요도	내부 순위	CR
개인정보 생애주기 보호	수집	개인정보 수집 필수사항 안내 및 동의	0.227	1	0.071
		목적별 최소한의 필수정보 수집	0.155	2	
		개인정보 수집 항목의 필수와 선택정보 구분	0.092	5	
		민감정보 처리 별도 동의	0.071	6	
		고유 식별정보 별도 동의	0.122	4	
		만 14세 미만의 아동의 정보수집 시 법정 대리인 동의	0.066	7	
		주민등록번호 수집 제한 법적 준수	0.169	3	
		선택정보 동의 거부 시 서비스 제공	0.052	8	
		개인정보의 국외 이전 안내 및 동의	0.046	9	

상위 개념	하위 개념	세부 지표	상대적 중요도	내부 순위	CR
	이용 및 제공	개인정보 처리 위탁 계약서 작성 및 체결	0.289	1	0.083
		위탁업무의 정보 공개	0.158	3	
		수탁자 대상 교육 및 관리 감독	0.209	2	
		목적 내 제3자 이용·제공 시 필수사항 고지 및 동의	0.056	7	
		목적 외 제3자 이용·제공 시 필수사항 고지 및 동의	0.060	6	
		목적 외 제3자 이용·제공 사항 공고	0.110	5	
		개인정보 이용 및 제3자 제공 대장 기록 관리	0.119	4	
	보관 및 파기	개인정보 자료 보관실의 잠금장치 및 출입 통제	0.105	6	0.056
		개인정보 저장 장비의 잠금장치 및 출입 통제	0.211	1	
		개인정보 파기 기간 준수	0.191	3	
		개인정보 파일 파기 절차 준수	0.203	2	
		개인정보 파기 방법 적절성	0.162	4	
		개인정보 파일 파기 관리대장 기록 관리	0.129	5	

수집에서의 상대적 중요도 및 순위는 개인정보 수집 필수사항 안내 및 동의(0.227), 목적별 최소한의 필수정보 수집(0.155), 주민등록번호 수집 제한 법적 준수(0.169), 고유 식별정보 별도 동의(0.122), 개인정보 수집 항목의 필수와 선택정보 구분(0.092), 민감정보 처리 별도 동의(0.071), 만 14세 미만의 아동의 정보수집 시 법정 대리인 동의(0.066), 선택정보 동의 거부 시 서비스 제공(0.052), 개인정보의 국외 이전 안내 및 동의(0.046) 순으로 나타났다.

이용 및 제공에서의 상대적 중요도 및 순위는 개인정보 처리 위탁 계약서 작성 및 체결(0.289), 수탁자 대상 교육 및 관리 감독(0.209), 위탁업무의 정보 공개(0.158), 개인정보 이용 및 제3자 제공 대장 기록 관리(0.119), 목적 외 제3자 이용・제공 사항 공고(0.11), 목적 외 제3자 이용・제공 시 필수사항 고지 및 동의(0.06), 목적 내 제3자 이용・제공 시 필수사항 고지 및 동의(0.056) 순으로 나타났다.

보관 및 파기에서의 상대적 중요도 및 순위는 개인정보 저장 장비의 잠금장치 및 출입 통제(0.211), 개인정보 파일 파기 절차 준수(0.203), 개인정보 파기 기간 준수(0.191), 개인정보 파기 방법 적절성(0.162), 개인정보 파일 파기 관리대장 기록 관리(0.129), 개인정보 자료 보관실의 잠금장치 및 출입 통제(0.105) 순으로 나타났다. 모든 항목에 대한 일관성 비율인 C.R값은 0.1 이하로 수집의 C.R값은 0.071, 이용 및 제공의 C.R값은 0.083, 보관 및 파기의 C.R값은 0.056으로 나타나 일관성이 있다고 판단하였다.

세 번째, '안전성 확보 조치단계'에 대한 세부 지표 우선순위 및 상대적 중요도를 살펴보면 <표 Ⅲ-29>와 같다.

<표 Ⅲ-29> 안전성 확보 조치단계 세부 지표의 상대적 중요도 및 순위

상위 개념	하위 개념	세부 지표	상대적 중요도	내부 순위	CR
안전성 확보 조치	내부 관리 계획	내부 관리계획 수립 및 이력 관리	0.667	1	0.000
		내부 관리계획 이행점검 및 개선	0.333	2	
	접근 관리	접근권한 절차 수립 및 이력 관리	0.413	1	0.056
		접근권한 차등 부여	0.327	2	
		접근권한 변경내역 기록 및 관리	0.260	3	
	접근 통제	안전한 비밀번호 작성 규칙 적용	0.202	1	0.47
		계정 오류 입력 접근제한 설정	0.147	3	
		부재 시 시스템 접속 차단 설정	0.166	2	
		비업무용 사이트 접속 차단 설정	0.147	3	
		비인가자 접근 차단	0.114	6	
		안전한 접속(또는 인증) 수단 적용	0.136	5	
		관리용 단말기 접근통제	0.087	7	
	접속 기록 관리	개인정보 취급자의 접속기록 보관 기간 설정	0.288	2	0.068
		접속기록 필수정보 적용	0.207	3	
		접속기록의 안전한 보관	0.175	4	
		접속기록 점검 관리	0.330	1	
	개인정보의 암호화	개인정보의 암호화	0.667	1	0.000
		비밀번호의 암호화	0.333	2	

내부 관리계획에서의 상대적 중요도 및 순위는 내부 관리계획 수립 및 이력 관리(0.667), 내부 관리계획 이행점검 및 개선(0.333) 순으로 나타났다. 접근관리에서의 상대적 중요도 및 순위는 접근권한 절차 수립 및 이력 관리(0.413), 접근권한 차등 부여(0.327), 접근권한 변경내역 기록 및 관리(0.260) 순으로 나타났다. 접근통제에서의 상대적 중요도 및 순위는 안전한 비밀번호 작성 규칙 적용(0.202), 부재 시 시스템 접속 차단 설정(0.166), 계정 오류 입력 접근제한 설정(0.147), 비업무용 사이트 접속 차단 설정(0.147), 안전한 접속(또는 인증) 수단 적용(0.136), 비인가자 접근 차단(0.114), 관리용 단말기 접근통제(0.087) 순으로 나타났다. 접속기록 관리에서의 상대적 중요도 및 순위는 접속기록 점검 관리(0.33), 개인정보 취급자의 접속기록 보관 기간 설정(0.288), 접속기록 필수정보 적용(0.207), 접속기록의 안전한 보관(0.175) 순으로 나타났다.

개인정보의 암호화에서의 상대적 중요도 및 순위는 개인정보의 암호화(0.667), 비밀번호의 암호화(0.333) 순으로 나타났다.

모든 항목에 대한 일관성 비율인 C.R값은 0.1 이하로 내부 관리계획과 개인정보의 암호화의 C.R값은 0.000, 접근관리의 C.R값은 0.056, 접근통제의 C.R값은 0.047, 접속기록 관리의 C.R값은 0.068로 나타나 일관성이 있다고 판단하였다

네 번째, '개인정보 관리 수준 점검 및 개선단계'에 대한 세부 지표 우선순위 및 상대적 중요도를 살펴보면 <표 Ⅲ-30>과 같다.

<표 Ⅲ-30> 개인정보 관리 수준 점검 및 개선단계 세부 지표의 상대적 중요도 및 순위

상위 개념	하위 개념	세부 지표	상대적 중요도	내부 순위	CR
개인정보 관리 수준 점검 및 개선	관리/기술적 보호	개인정보 관리 정책의 점검 및 검토	0.207	1	0.092
		개인정보 관리 정책의 개선	0.185	2	
		개인정보 관리 점검 및 검토	0.097	6	
		개인정보 관리 점검결과 확인된 사항 조치	0.103	5	
		보안취약점 점검 및 위험평가 검토	0.108	4	
		보안취약점 개선 조치	0.094	7	
		개인정보 노출 여부 모니터링 및 검토	0.134	3	
		개인정보 노출 모니터링 결과 확인된 사항 조치	0.072	8	

상위 개념	하위 개념	세부 지표	상대적 중요도	내부 순위	CR
	대응훈련 능력	개인정보 침해사고 대응훈련	0.345	2	0.004
		개인정보 침해사고 대응훈련 통한 확인된 사항 조치	0.370	1	
		개인정보 재해복구 훈련	0.185	3	
		개인정보 재해복구 훈련을 통한 확인된 사항 조치	0.100	4	

관리/기술적 보호에서의 상대적 중요도 및 순위는 개인정보 관리 정책의 점검 및 검토(0.207), 개인정보 관리 정책의 개선(0.185), 개인정보 노출 여부 모니터링 및 검토(0.134), 보안취약점 점검 및 위험평가 검토(0.108), 개인정보 관리 점검결과 확인된 사항 조치(0.103), 개인정보 관리 점검 및 검토(0.097), 보안취약점 개선 조치(0.094), 개인정보 노출 모니터링 결과 확인된 사항 조치(0.072) 순으로 나타났다.

대응훈련 능력에서의 상대적 중요도 및 순위는 개인정보 침해사고 대응훈련을 통한 확인된 사항 조치(0.37), 개인정보 침해사고 대응훈련(0.345), 개인정보 재해복구 훈련(0.185), 개인정보 재해복구 훈련을 통한 확인된 사항 조치(0.1) 순으로 나타났다.

모든 항목에 대한 일관성 비율인 C.R값은 0.1 이하로 관리/기술적 보호조치의 C.R값은 0.092, 대응훈련 능력의 C.R값은 0.004로 나타나 일관성이 있다고 판단하였다.

다섯 번째, '권리보장 및 윤리역량단계'에 대한 세부 지표 우선순위 및 상대적 중요도를 살펴보면 <표 Ⅲ-31>과 같다.

<표 Ⅲ-31> 권리보장 및 윤리역량단계 세부 지표의 상대적 중요도 및 순위

상위 개념	하위 개념	세부 지표	상대적 중요도	내부 순위	CR
권리 보장 및 윤리 역량	정보 주체의 권리보장	정보 주체 중심의 개인정보 처리 방침 공개	0.259	1	0.021
		정보 주체 중심의 개인정보 수집 이용동의서 제공	0.225	2	
		개인정보의 열람·정정·삭제·처리정지의 처리	0.149	5	
		법적 대리인의 동의권 보장	0.171	4	
		개인정보 유출 신고 안내	0.196	3	
	조직의 역량	조직의 개인정보보호 관련 규정 준수	0.232	1	0.072
		조직의 개인정보 침해사고 지침 준수	0.145	4	
		개인정보보호 전담 조직 및 인력 구성	0.201	2	
		개인정보보호 전용 예산 편성	0.151	3	
		개인정보보호 교육과정 운영 및 평가	0.076	7	
		성과관리(또는 인센티브제도) 운용	0.105	5	
		위반자 제재 및 처벌	0.090	6	
	개인의 역량과 윤리의식	개인정보보호에 대한 도덕성과 자기통제	0.227	1	0.079
		개인정보 처리 업무의 사명감	0.167	3	
		개인정보보호 법률 및 제도 이해력과 행동	0.191	2	
		개인정보보호 교육 이수 및 자기 계발	0.138	4	
		개인정보보호에 대한 자기효능감	0.089	6	
		개인정보보호 기술 능력과 활용도	0.109	5	
		피해 인지력과 문제해결 능력	0.080	7	

정보 주체의 권리보장에서의 상대적 중요도 및 순위는 정보 주체 중심의 개인정보 처리 방침 공개(0.259), 정보 주체 중심의 개인정보 수집 이용동의서 제공(0.225), 개인정보 유출 신고 안내(0.196), 법적 대리인의 동의권 보장(0.171), 개인정보의 열람.정정.삭제.처리정지의 처리(0.149) 순으로 나타났다.

조직의 역량에서의 상대적 중요도 및 순위는 조직의 개인정보보호 관련 규정(0.232), 개인정보보호 전담 조직 및 인력 구성(0.201), 개인정보보호 전용 예산 편성(0.151), 조직의 개인정보 침해사고 지침(0.145), 성과관리(또는 인센티브제도) 운용(0.105), 위반자 제재 및 처벌(0.09), 개인정보보호 교육(0.076) 순으로 나타났다. 개인의 역량 및 윤리에서의 상대적 중요도 및 순위는 개인정보보호에 대한 도덕성과 자기통제(0.227), 개인정보보호 법률 및 제도 이해력과 행동(0.191), 개인정보 처리 업무의 사명감(0.167), 개인정보보호 교육 이수 및 자기 계발(0.138), 개인정보보호 기술 능력과 활용도(0.109), 개인정보보호에 대한 자기효능감(0.089), 피해 인지력과 문제해결 능력(0.08) 순으로 나타났다.

모든 항목에 대한 일관성 비율인 C.R값은 0.1 이하로 정보 주체의 권리보장에 대한 C.R값은 0.021, 조직의 역량의 C.R값은 0.072, 개인의 역량 및 윤리의 C.R값은 0.079로 나타나 일관성이 있다고 판단하였다.

마지막으로 세부 지표들의 전체 대비 우선순위 및 상대적 중요도는 <표 Ⅲ-32>와 같다.

<표 Ⅲ-32> 세부 지표 전체 대비 우선순위 및 상대적 중요도

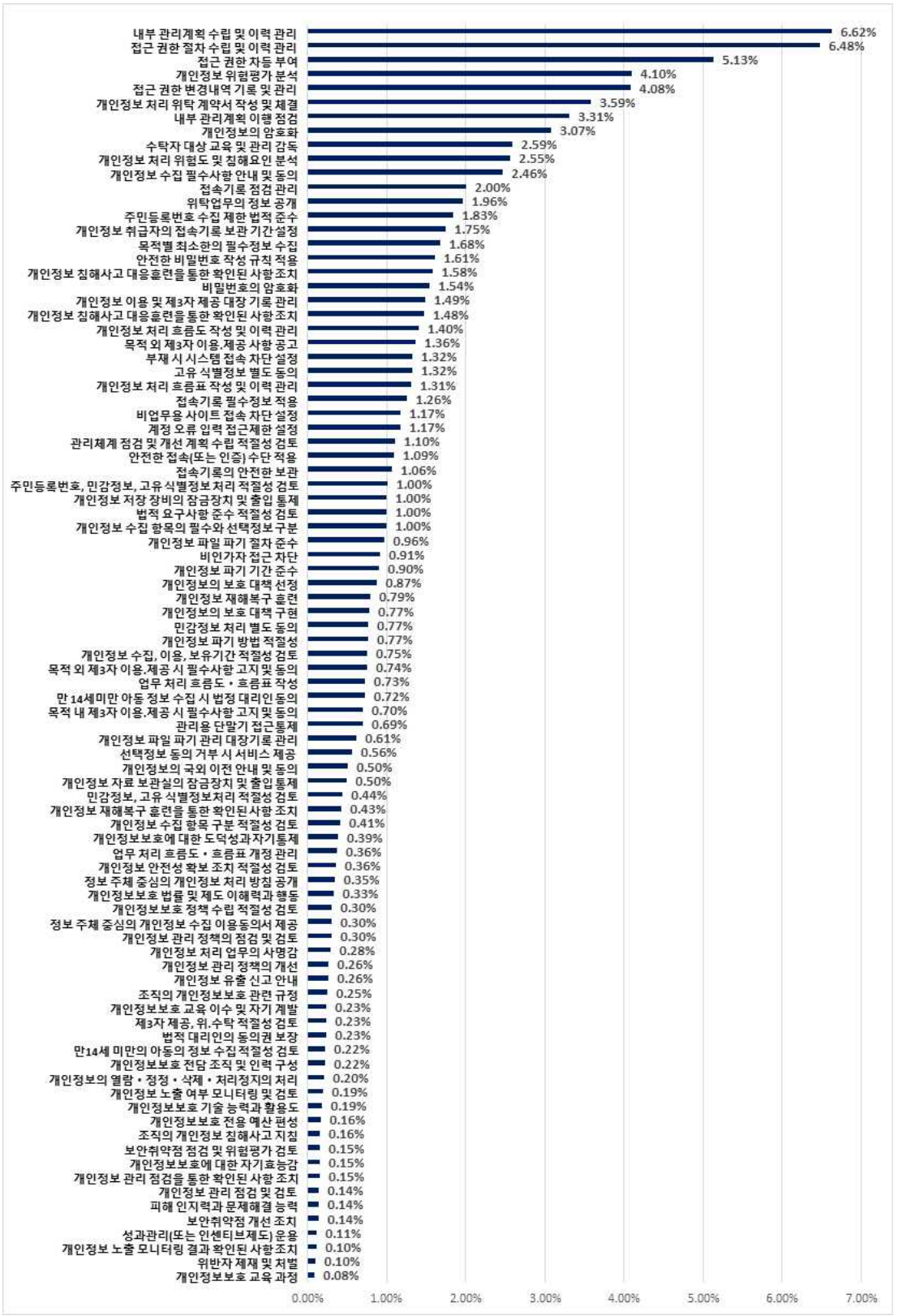
순위	하위개념	전체 대비 상대적 중요도	CR
1	내부 관리계획 수립 및 이력 관리	0.06621	0.07
2	접근권한 절차 수립 및 이력 관리	0.06482	
3	접근권한 차등 부여	0.05129	
4	개인정보 위험평가 분석	0.04096	
5	접근권한 변경내역 기록 및 관리	0.04079	
6	개인정보 처리 위탁 계약서 작성 및 체결	0.03585	
7	내부 관리계획 이행점검 및 개선	0.03305	
8	개인정보의 암호화	0.03073	

순위	하위개념	전체 대비 상대적 중요도	CR
9	수탁자 대상 교육 및 관리 감독	0.02593	
10	개인정보 처리 위험도 및 침해요인 분석	0.02553	
11	개인정보 수집 필수사항 안내 및 동의	0.02460	
12	접속기록 점검 관리	0.02003	
13	위탁업무의 정보 공개	0.01960	
14	주민등록번호 수집 제한 법적 준수	0.01832	
15	개인정보 취급자의 접속기록 보관 기간 설정	0.01748	
16	목적별 최소한의 필수정보 수집	0.01680	
17	안전한 비밀번호 작성 규칙 적용	0.01611	
18	개인정보 침해사고 대응훈련을 통한 확인된 사항 조치	0.01582	
19	비밀번호의 암호화	0.01540	
20	개인정보 이용 및 제3자 제공 대장 기록 관리	0.01490	
21	개인정보 침해사고 대응훈련을 통한 확인된 사항 조치	0.01475	
22	개인정보 처리 흐름도 작성 및 이력 관리	0.01402	
23	목적 외 제3자 이용·제공 사항 공고	0.01364	
24	부재 시 시스템 접속 차단 설정	0.01324	
25	고유 식별정보 별도 동의	0.01322	
26	개인정보 처리 흐름표 작성 및 이력 관리	0.01310	
27	접속기록 필수정보 적용	0.01256	
28	계정 오류 입력 접근제한 설정	0.01172	
29	비업무용 사이트 접속 차단 설정	0.01172	
30	관리체계 점검 및 개선 계획 수립 적절성 검토	0.01099	
31	안전한 접속(또는 인증) 수단 적용	0.01085	
32	접속기록의 안전한 보관	0.01062	
33	주민등록번호, 민감정보, 고유 식별정보 처리 적절성 검토	0.01004	
34	개인정보 저장 장비의 잠금장치 및 출입 통제	0.00999	
35	법적 요구사항 준수 적절성 검토	0.00998	
36	개인정보 수집 항목의 필수와 선택정보 구분	0.00997	
37	개인정보 파일 파기 절차 준수	0.00961	
38	비인가자 접근 차단	0.00909	

순위	하위개념	전체 대비 상대적 중요도	CR
39	개인정보 파기 기간 준수	0.00904	
40	개인정보의 보호 대책 선정	0.00870	
41	개인정보 재해복구 훈련	0.00791	
42	개인정보의 보호 대책 구현	0.00771	
43	민감정보 처리 별도 동의	0.00769	
44	개인정보 파기 방법 적절성	0.00767	
45	개인정보 수집, 이용, 보유기간 적절성 검토	0.00754	
46	목적 외 제3자 이용·제공 시 필수사항 고지 및 동의	0.00744	
47	업무처리 흐름도·흐름표 작성	0.00728	
48	만 14세미만 아동 정보 수집 시 법정 대리인 동의	0.00716	
49	목적 내 제3자 이용·제공 시 필수사항 고지 및 동의	0.00695	
50	관리용 단말기 접근통제	0.00694	
51	개인정보 파일 파기 관리 대장기록 관리	0.00610	
52	선택정보 동의 거부 시 서비스 제공	0.00564	
53	개인정보의 국외 이전 안내 및 동의	0.00499	
54	개인정보 자료 보관실의 잠금장치 및 출입 통제	0.00497	
55	민감정보, 고유 식별정보처리 적절성 검토	0.00435	
56	개인정보 재해복구 훈련을 통한 확인된 사항 조치	0.00428	
57	개인정보 수집 항목 구분 적절성 검토	0.00410	
58	개인정보보호에 대한 도덕성과 자기통제	0.00385	
59	업무처리 흐름도·흐름표 개정 관리	0.00364	
60	개인정보 안전성 확보 조치 적절성 검토	0.00361	
61	정보 주체 중심의 개인정보 처리 방침 공개	0.00348	
62	개인정보보호 법률 및 제도 이해력과 행동	0.00325	
63	개인정보보호 정책 수립 적절성 검토	0.00304	
64	정보 주체 중심의 개인정보 수집 이용동의서 제공	0.00302	
65	개인정보 관리 정책의 점검 및 검토	0.00295	
66	개인정보 처리 업무의 사명감	0.00283	
67	개인정보 관리 정책의 개선	0.00264	
68	개인정보 유출 신고 안내	0.00263	
69	조직의 개인정보보호 관련 규정	0.00248	
70	개인정보보호 교육 이수 및 자기 계발	0.00234	

순위	하위개념	전체 대비 상대적 중요도	CR
71	제3자 제공, 위·수탁 적절성 검토	0.00233	
72	법적 대리인의 동의권 보장	0.00230	
73	만 14세 미만의 아동 정보수집 적절성 검토	0.00216	
74	개인정보보호 전담 조직 및 인력 구성	0.00215	
75	개인정보의 열람·정정·삭제·처리정지의 처리	0.00200	
76	개인정보 노출 여부 모니터링 및 검토	0.00191	
77	개인정보보호 기술 능력과 활용도	0.00185	
78	개인정보보호 전용 예산 편성	0.00161	
79	조직의 개인정보 침해사고 지침	0.00155	
80	보안취약점 점검 및 위험평가 검토	0.00154	
81	개인정보보호에 대한 자기효능감	0.00151	
82	개인정보 관리 점검 결과 확인된 사항 조치	0.00148	
83	개인정보 관리 점검 및 검토	0.00138	
84	피해 인지력과 문제해결 능력	0.00137	
85	보안취약점 개선 조치	0.00135	
86	성과관리(또는 인센티브제도) 운용	0.00113	
87	개인정보 노출 모니터링 결과 확인된 사항 조치	0.00104	
88	위반자 제재 및 처벌	0.00097	
89	개인정보보호 교육과정 운영 및 평가	0.00082	
계		1.0000	

전체를 100%로 보았을 때 [그림 Ⅲ-9]와 같이 내부 관리계획 수립 및 이력 관리는 6.62%를 차지하여 상대적 중요도가 가장 높은 세부 지표인 것으로 나타났다. 접근권한 절차 수립 및 이력 관리는 6.48%, 접근권한 차등 부여는 5.12%로 나타나 각각 2, 3위로 나타났다. 반면, 상대적 중요도가 가장 낮은 세부 지표는 개인정보보호 교육과정 운영 및 평가(0.08%)로 나타났다. 하위개념의 상대적 중요도에 대한 종합 비일관성 비율(overall CVR)은 0.07로 일관성이 확보되었음을 알 수 있었다.



[그림 Ⅲ-9] 세부 지표 전체 대비 상대적 중요도(크기순)

3.5 최종 지표 및 가중치 도출 결과

앞서 도출된 상위개념, 하위개념, 세부 지표에 대한 가중치 및 상대적 중요도를 분석한 결과를 요약하면 <표 Ⅲ-33>과 같이 나타낼 수 있다. 전체 비일관성 비율(CR)은 0.06으로 일관성이 확보되었음을 알 수 있었다.

<표 Ⅲ-33> 최종 평가지표 점수 환산표

상위개념 (a)	하위개념 (b)	세부 지표		가중치 (c)	전체 대비 가중치(d) (a*b*c)	환산 점수 (e)
사전 계획 및 설계 (0.179)	업무처리 흐름 분석 (0.061)	1	업무처리 흐름도.흐름표 작성	0.667	0.00728	0.728
		2	업무처리 흐름도.흐름표 개정 관리	0.333	0.00364	0.364
	개인정보 흐름 분석 (0.342)	3	개인정보 수집, 이용, 보유기간 적절성 검토	0.123	0.00754	0.754
		4	주민등록번호, 민감정보, 고유식별정보 처리 적절성 검토	0.164	0.01004	1.004
		5	개인정보 수집 항목 구분 적절성 검토	0.067	0.0041	0.41
		6	개인정보의 타 시스템 연계 적절성 검토	0.071	0.00435	0.435
		7	만 14세 미만의 아동 정보수집 적절성 검토	0.035	0.00216	0.216
		8	제3자 제공, 위·수탁 적절성 검토	0.038	0.00233	0.233
		9	개인정보 안전성 확보 조치 적절성 검토	0.059	0.00361	0.361
		10	개인정보 처리 흐름도 작성 및 이력 관리	0.229	0.01402	1.402
		11	개인정보 처리 흐름표 작성 및 이력 관리	0.214	0.0131	1.31
	개인정보 안전성 분석 (0.463)	12	개인정보 위험평가 분석	0.494	0.04096	4.096
		13	개인정보 처리 위험도 및 침해요인 분석	0.308	0.02553	2.553
		14	개인정보의 보호 대책 선정	0.105	0.0087	0.87
		15	개인정보의 보호 대책 구현	0.093	0.00771	0.771

상위개념 (a)	하위개념 (b)	세부 지표		가중치 (c)	전체 대비 가중치(d) (a*b*c)	환산 점수 (e)
	관리체계 수립 (0.134)	16	개인정보보호 정책 수립 적절성 검토	0.126	0.00304	0.304
		17	법적 요구사항 준수 적절성 검토	0.416	0.00998	0.998
		18	관리체계 점검 및 개선 계획 수립 적절성 검토	0.458	0.01099	1.099
개인정보 생애주기 보호 (0.280)	수집 (0.387)	19	개인정보 수집 필수사항 안내 및 동의	0.227	0.0246	2.46
		20	목적별 최소한의 필수정보 수집	0.155	0.0168	1.68
		21	개인정보 수집 항목의 필수와 선택정보 구분	0.092	0.00997	0.997
		22	민감정보 처리 별도 동의	0.071	0.00769	0.769
		23	고유 식별정보 별도 동의	0.122	0.01322	1.322
		24	만 14세 미만의 아동의 정보 수집 시 법정 대리인 동의	0.066	0.00716	0.716
		25	주민등록번호 수집 제한 법적 준수	0.169	0.01832	1.832
		26	선택정보 동의 거부 시 서비스 제공	0.052	0.00564	0.564
		27	개인정보의 국외 이전 안내 및 동의	0.046	0.00499	0.499
	이용 및 제공 (0.443)	28	개인정보 처리 위탁 계약서 작성 및 체결	0.289	0.03585	3.585
		29	위탁업무의 정보 공개	0.158	0.0196	1.96
		30	수탁자 대상 교육 및 관리 감독	0.209	0.02593	2.593
		31	목적 내 제3자 이용·제공 시 필수사항 고지 및 동의	0.056	0.00695	0.695
		32	목적 외 제3자 이용·제공 시 필수사항 고지 및 동의	0.06	0.00744	0.744
		33	목적 외 제3자 이용·제공 사항 공고	0.11	0.01364	1.364
		34	개인정보 이용 및 제3자 제공 대장 기록 관리	0.119	0.0149	1.49

상위개념 (a)	하위개념 (b)	세부 지표		가중치 (c)	전체 대비 가중치(d) (a*b*c)	환산 점수 (e)
	보관 및 파기 (0.169)	35	개인정보 자료 보관실의 잠금장치 및 출입 통제	0.105	0.00497	0.497
		36	개인정보 저장 장비의 잠금장치 및 출입 통제	0.211	0.00999	0.999
		37	개인정보 파기 기간 준수	0.191	0.00904	0.904
		38	개인정보 파일 파기 절차 준수	0.203	0.00961	0.961
		39	개인정보 파기 방법 적절성	0.162	0.00767	0.767
		40	개인정보 파일 파기 관리대장 기록 관리	0.129	0.0061	0.61
안전성 확보 조치 (0.443)	내부 관리계획 (0.224)	41	내부 관리계획 수립 및 이력 관리	0.667	0.06621	6.621
		42	내부 관리계획 이행점검 및 개선	0.333	0.03305	3.305
	접근관리 (0.354)	43	접근권한 절차 수립 및 이력 관리	0.413	0.06482	6.482
		44	접근권한 차등 부여	0.327	0.05129	5.129
		45	접근권한 변경내역 기록 및 관리	0.26	0.04079	4.079
	접근통제 (0.180)	46	안전한 비밀번호 작성 규칙 적용	0.202	0.01611	1.611
		47	계정 오류 입력 접근제한 설정	0.147	0.01172	1.172
		48	부재 시 시스템 접속 차단 설정	0.166	0.01324	1.324
		49	비업무용 사이트 접속 차단 설정	0.147	0.01172	1.172
		50	비인가자 접근 차단	0.114	0.00909	0.909
		51	안전한 접속(또는 인증) 수단 적용	0.136	0.01085	1.085
		52	관리용 단말기 접근통제	0.087	0.00694	0.694

상위개념 (a)	하위개념 (b)	세부 지표		가중치 (c)	전체 대비 가중치(d) (a*b*c)	환산 점수 (e)
	접속기록 관리 (0.137)	53	개인정보 취급자의 접속기록 보관 기간 설정	0.288	0.01748	1.748
		54	접속기록 필수정보 적용	0.207	0.01256	1.256
		55	접속기록의 안전한 보관	0.175	0.01062	1.062
		56	접속기록 점검 관리	0.33	0.02003	2.003
	개인정보의 암호화 (0.104)	57	개인정보의 암호화	0.667	0.03073	3.073
		58	비밀번호의 암호화	0.333	0.0154	1.54
개인정보 관리 수준 점검 및 개선 (0.057)	관리/ 기술적 보호 (0.25)	59	개인정보 관리 정책의 점검 및 검토	0.207	0.00295	0.295
		60	개인정보 관리 정책의 개선	0.185	0.00264	0.264
		61	개인정보 관리 점검 및 검토	0.097	0.00138	0.138
		62	개인정보 관리 점검결과 확인된 사항 조치	0.103	0.00148	0.148
		63	보안취약점 점검 및 위험평가 검토	0.108	0.00154	0.154
		64	보안취약점 개선 조치	0.094	0.00135	0.135
		65	개인정보 노출 여부 모니터링 및 검토	0.134	0.00191	0.191
		66	개인정보 노출 모니터링 결과 확인된 사항 조치	0.072	0.00104	0.104
	대응훈련 능력 (0.75)	67	개인정보 침해사고 대응훈련	0.345	0.01475	1.475
		68	개인정보 침해사고 대응훈련을 통한 확인된 사항 조치	0.37	0.01582	1.582
		69	개인정보 재해복구 훈련	0.185	0.00791	0.791
		70	개인정보 재해복구 훈련을 통한 확인된 사항 조치	0.1	0.00428	0.428

상위개념 (a)	하위개념 (b)	세부 지표		가중치 (c)	전체 대비 가중치(d) (a*b*c)	환산 점수 (e)
권리보장 및 윤리역량 (0.041)	정보 주체의 권리보장 (0.327)	71	정보 주체 중심의 개인정보 처리 방침 공개	0.259	0.00348	0.348
		72	정보 주체 중심의 개인정보 수집 이용동의서 제공	0.225	0.00302	0.302
		73	개인정보의 열람.정정.삭제.처리정지의 처리	0.149	0.002	0.2
		74	법적 대리인의 동의권 보장	0.171	0.0023	0.23
		75	개인정보 유출 신고 안내	0.196	0.00263	0.263
	조직의 역량 (0.260)	76	조직의 개인정보보호 관련 규정	0.232	0.00248	0.248
		77	조직의 개인정보 침해사고 지침	0.145	0.00155	0.155
		78	개인정보보호 전담 조직 및 인력 구성	0.201	0.00215	0.215
		79	개인정보보호 전용 예산 편성	0.151	0.00161	0.161
		80	개인정보보호 교육과정 운영 및 평가	0.076	0.00082	0.082
		81	성과관리(또는 인센티브제도) 운용	0.105	0.00113	0.113
		82	위반자 제재 및 처벌	0.09	0.00097	0.097
	개인의 역량 및 윤리의식 (0.413)	83	개인정보보호에 대한 도덕성과 자기통제	0.227	0.00385	0.385
		84	개인정보 처리 업무의 사명감	0.167	0.00283	0.283
		85	개인정보보호 법률 및 제도 이해력과 행동	0.191	0.00325	0.325
		86	개인정보보호 교육 이수 및 자기 계발	0.138	0.00234	0.234
		87	개인정보보호에 대한 자기효능감	0.089	0.00151	0.151
		88	개인정보보호 기술 능력과 활용도	0.109	0.00185	0.185
		89	피해 인지력과 문제해결 능력	0.08	0.00137	0.137

항목별 복합 가중치를 적용하여 항목의 합이 100점이 되도록 항목에 대해 점수를 부여하였다. 세부 지표별 환산점수(e)는 상위개념(a), 하위개념(b), 세부 지표(c) 등 각 요소의 가중치를 모두 곱하여 전체 대비 가중치(d)를 도출한 후 100을 곱하였다.

3.6 개발된 개인정보 관리역량 성숙도 모델 및 평가지표

개인정보 관리역량 성숙도 측정모델은 앞장의 선행연구에서의 BCMM 모델을 확장하여 개인정보 관리역량 성숙도 모델(PCM2 : Privacy Competency Maturity Model)을 <표 Ⅲ-34>와 같이 제안한다.

<표 Ⅲ-34> BCMM 기반의 제안된 개인정보 관리역량 성숙도 모델(PCM2)

성숙도 단계		정의	배점	척도구간
역량 성숙도 증가 ↑	VH(Very High)	전사적으로 시행 및 성과 측정 계획이 수립되고 시행 후 결과에 따라 주기적으로 모니터링하고 결과에 따라 개선을 수행하는 단계	100	95% 초과
	H(High)	전사적으로 시행 및 성과 측정 계획이 수립되고 시행 후 주기적으로 모니터링하고 있는 단계	83.3	95% 이하
	VM(Very Medium)	전사적으로 시행계획과 성과 측정 계획이 수립되고 시행되고 있는 단계	66.7	85% 이하
	M(Medium)	전사적으로 시행계획이 수립되고 수행되고 있는 단계	50	65% 이하
	L(Low)	부분적으로 시행계획이 수립되고 수행되고 있는 단계	33.3	35% 이하
	VL(Very Low)	시행계획을 수립하지 않고 세부 평가항목을 부분적으로 수행하고 있는 단계	16.7	15% 이하
	N(None)	세부 평가항목으로 수행되지 않고 있는 단계	0	5% 미만

제안한 PCM2는 Very High, High, Very Medium, Medium, Low, Very Low, None 등 7등급의 성숙도 수준과 함께 개인정보보호 역량과 관련된 속성을 정의하였다. 제안된 PCM2 모델을 보면, 1단계인 N(None)은 세부 평가항목으로 수행되지 않고 있는 단계로 0점, 2단계인 VL(Very Low)은 시행계획을 수립하지 않고 세부 평가항목을 부분적으로 수행하고 있는 단계로 16.7점, 3단계인 L(Low)은 부분적으로 시행계획이 수립되고 수행되고 있는 단계로 33.3점, 4단계인 M(Medium)은 전사적으로 시행계획이 수립되고 수행되고 있는 단계로 50점, 5단계인 VM(Very Medium)은 전사적으로 시행계획과 성과 측정 계획이 수립되고 시행되고 있는 단계로 66.7점, 6단계인 H(High)는 전사적으로 시행 및 성과 측정 계획이 수립되고 시행 후 주기적으로 모니터링하고 있는 단계로 83.3점, 7단계인

VH(Very High)는 전사적으로 시행 및 성과 측정 계획이 수립되고 시행 후 결과에 따라 주기적으로 모니터링하고 결과에 따라 개선을 수행하는 단계로 100점으로 처리하여 역량 수준 평가에 대해 평가할 수 있도록 하였다.

제안한 개인정보 관리역량 성숙도 측정 모델(PCM2)과 AHP 기법을 통해 문항별 가중치를 부여한 최종 역량지표는 <표 Ⅲ-35>와 같이 도출되었다.

<표 Ⅲ-35> 최종 도출된 개인정보 관리역량 성숙도 모델 및 평가지표

상위 개념	하위 개념	세부 지표	평가지표	자가 진단표						
				N	VL	L	M	VM	H	VH
사전 계획 및 설계 단계	업무처리 흐름 분석	개인정보 처리 업무처리 흐름도·흐름표 작성	처리하려는 업무 흐름도 및 흐름표를 작성하였는지 확인하고 처리한다.							
		업무처리 흐름도·흐름표 개정 관리	업무 흐름도 및 흐름표는 최신 상태로 유지되고 있는지 확인하고 처리한다.							
	개인정보 흐름 분석	개인정보 수집, 이용, 보유기간 적절성 검토	개인정보를 수집하는 경우 목적에 필요한 최소한의 범위에서만 수집하도록 계획하고, 개인정보 보유기간을 명확한 근거에 의하여 정하고 있는지 확인하고 처리한다.							
		주민등록번호, 민감정보, 고유 식별정보 처리 적절성 검토	주민등록번호 수집 시 법령에 근거하고 있으며, 인터넷 홈페이지는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있도록 계획하고, 민감정보, 고유 식별정보를 처리하는 경우 다른 개인정보의 처리에 대한 동의와 별도로 구분하여 동의받도록 계획하고 있는지 확인하고 처리한다.							
		개인정보 수집 항목 구분 적절성 검토	개인정보를 수집하는 경우 필수항목과 선택항목을 분리하고 선택적으로 동의할 수 있는 사항에 동의하지 아니하여도 서비스 이용이 가능하도록 계획하고 있는지 확인하고 처리한다.							

상위 개념	하위 개념	세부 지표	평가지표	자가 진단표						
				N	VL	L	M	VM	H	VH
		만 14세 미만의 아동 정보수집 적절성 검토	만 14세 미만의 아동 개인정보 수집 시, 법정 대리인에게 동의받도록 계획하고 있는지 확인하고 처리한다.							
		제3자 제공, 위·수탁 적절성 검토	제3자 제공에 관한 사항을 정보 주체에게 알리고 받도록 계획하고, 위수탁 업무인지 여부를 확인하고 처리한다.							
		개인정보의 타 시스템 연계 적절성 검토	개인정보 처리 업무가 타 시스템과 연계되는지 검토하고 적절하게 연계되도록 계획하고 있는지 확인하고 처리한다.							
		개인정보 안전성 확보 조치 적절성 검토	개인정보의 안전성 확보 조치 계획을 명확한 근거에 의하여 수립하고 있는지 확인하고 처리한다.							
		개인정보 처리 흐름도 작성 및 이력 관리	개인정보 처리 흐름도 작성 및 이력 관리하고 있는지 확인하고 처리한다.							
		개인정보 처리 흐름표 작성 및 이력 관리	개인정보 처리 흐름표 작성 및 이력 관리하고 있는지 확인하고 처리한다.							
	개인정보 안전성 분석	개인정보 처리 위험도 및 침해요인 분석	개인정보 처리에 따른 위험도 및 침해요인을 분석하고 처리한다.							
		개인정보 위험 평가 분석	개인정보 처리에 따른 위험도 및 침해요인 결과에 따라 위험평가를 분석하고 처리한다.							
		개인정보의 보호 대책 선정	개인정보의 개인정보 위험 평가 분석 결과를 바탕으로 보호 대책을 수립하고 처리한다.							
		개인정보의 보호 대책 구현	개인정보의 보호 대책 수립 결과를 바탕으로 보호 이행 대책을 구현하고 처리한다.							

상위 개념	하위 개념	세부 지표	평가지표	자가 진단표						
				N	VL	L	M	VM	H	VH
	관리체계 수립	개인정보보호 정책 수립 적절성 검토	개인정보보호 정책, 조직, 예산이 적절하게 수립하고 있는지를 확인하고 처리한다.							
		법적 요구사항 준수 적절성 검토	개인정보 처리 업무 관련 법적 요구사항을 검토하고 준수 절차를 수립하여 처리한다.							
		관리체계 점검 및 개선 계획 수립 적절성 검토	관리체계 수립 결과를 바탕으로 보호조치 개선방안이 계획되어 있는지 확인하고 처리한다.							
개인정보 생애주기 보호	수집	개인정보 수집 필수사항 안내 및 동의	개인정보 수집 시 4가지 필수사항(수집 목적, 수집 항목, 보유 및 이용 기간, 동의 거부권 및 거부 시 불이익)을 안내하고 동의받고 있는지 확인하고 처리한다.							
		목적별 최소한의 필수정보 수집	목적별 최소한의 필수정보만 수집하고 있는지 확인하고 처리한다.							
		개인정보 수집 항목의 필수와 선택정보 구분	개인정보 수집 항목을 필수정보와 선택정보를 구분하여 동의받고 있는지 확인하고 처리한다.							
		민감정보 처리 별도 동의	민감정보 처리를 위해 별도 동의받고 있는지 확인하고 처리한다.							
		고유 식별정보 별도 동의	고유 식별정보(여권번호, 운전면허번호, 외국인등록번호) 수집할 때 별도의 동의를 받고 있는지 확인하고 처리한다.							
		만 14세 미만의 아동의 정보수집 시 법정 대리인 동의	만 14세 미만의 아동 개인정보 수집 시, 법정 대리인에게 동의받고 있는지 확인하고 처리한다.							
		주민등록번호 수집 제한 법적 준수	법률에서 구체적으로 처리를 요구하거나 허용하는 경우를 제외하고 주민등록번호를 처리하지 않고 있는지 확인하고 처리한다.							

상위 개념	하위 개념	세부 지표	평가지표	자가 진단표						
				N	VL	L	M	VM	H	VH
		선택정보 동의 거부 시 서비스 제공	뉴스레터, 마케팅, 홍보를 위한 개인정보 수집에 동의하지 않더라도 기본적인 서비스를 제공하고 있는지 확인하고 처리한다.							
		개인정보의 국외 이전 안내 및 동의	개인정보의 국외 이전 시, 정보 주체에게 알리고 동의받고 있는지 확인하고 처리한다.							
	이용 및 제공	개인정보 처리 위탁 계약서 작성 및 체결	개인정보의 처리 업무를 위탁하는 경우, 개인정보 위탁계약서를 작성하고 있는지 확인하고 처리한다.							
		위탁업무의 정보 공개	위탁업무의 내용과 수탁자(위탁받아 처리하는 자)를 공개하고 있는지 확인하고 처리한다.							
		수탁자 대상 교육 및 관리 감독	수탁자에 대한 관리·감독을 수행하고 있는지 확인하고 처리한다.							
		목적 내 제3자 이용·제공 시 필수사항 고지 및 동의	수집하는 개인정보를 목적 내 제3자에게 제공 시 필수 고지항목(제공받는 자, 이용목적, 개인정보 항목, 보유 및 이용 기간, 동의 거부권 및 거부 시 불이익 내용)을 안내하고 동의받고 있는지 확인하고 처리한다.							
		목적 외 제3자 이용·제공 시 필수사항 고지 및 동의	목적 외 제3자 이용·제공 시 필수 고지항목(제공받는 자, 이용목적, 개인정보 항목, 보유 및 이용 기간, 동의 거부권 및 거부 시 불이익 내용)을 안내하고 동의받고 있는지 확인하고 처리한다.							

상위 개념	하위 개념	세부 지표	평가지표	자가 진단표						
				N	VL	L	M	VM	H	VH
		목적 외 제3자 이용·제공 사항 공고	공공기관은 개인정보의 목적 외 이용 또는 제3자 제공에 관한 사항에 관한 공고를 하고 있는지 확인하고 처리한다.							
		개인정보 이용 및 제3자 제공 대장 기록 관리	목적 외 제3자 이용·제공 사항을 관리대장에 기록 관리하고 있는지 확인하고 처리한다.							
	보관 및 파기	개인정보 자료 보관실의 잠금장치 및 출입 통제	개인정보 자료를 잠금장치가 된 캐비닛 등 안전한 장소에 보관하고 있는지 확인하고 처리한다.							
		개인정보 저장 장비의 잠금장치 및 출입 통제	개인정보를 저장하고 있는 전산장비는 잠금장치 및 출입 통제가 되어 있는지 확인하고 처리한다.							
		개인정보 파기 기간 준수	보유기간이 경과 되거나 처리목적 달성된 개인정보는 보유 및 이용 기간 종료 후 5일 이내에 즉시 파기하고 있는지 확인하고 처리한다.							
		개인정보 파일 파기 절차 준수	개인정보 파일 파기 시 개인정보보호 책임자의 승인 절차를 준수하는지 확인하고 처리한다.							
		개인정보 파기 방법 적절성	개인정보 파기 시 복원·재생할 수 없는 형태로 완전하게 파기하는지 확인하고 처리한다.							
		개인정보 파일 파기 관리대장 기록 관리	개인정보 파기에 관한 사항을 기록하고 관리하고 있는지 확인하고 처리한다.							

상위 개념	하위 개념	세부 지표	평가지표	자가 진단표						
				N	VL	L	M	VM	H	VH
안 전 성 확 보 조치	내부 관리계획	내부 관리계획 수립 및 이력 관리	개인정보의 안전한 처리를 위한 내부 관리계획을 수립하고 이력 관리하고 있는지 확인하고 처리한다.							
		내부 관리계획 이행점검 및 개선	안전한 처리를 위한 내부 관리계획에 대한 이행 점검을 반기 1회 이상 하고 있는지 확인하고 처리한다.							
	접근관리	접근권한 절차 수립 및 이력 관리	개인정보 처리시스템의 중요도(민감도) 및 업무 연관성 등을 고려하여 담당자별 차등 접근권한 절차를 마련하고 이력 관리하고 있는지 확인하고 처리한다.							
		접근권한 차등 부여	개인정보 처리시스템에 대한 접속 권한을 업무 수행 개인정보 취급자에게만 개인별(ID)별로 부여하였는지 확인하고 처리한다.							
		접근권한 변경 내역 기록 및 관리	개인정보 처리시스템 접근권한의 부여·변경·말소 내역을 기록하고, 최소 3년간 이를 보관하고 있는지 확인하고 처리한다.							
	접근통제	안전한 비밀번호 작성 규칙 적용	개인정보 처리시스템 접속 시 안전한 비밀번호 작성 규칙을 적용하고 있는지 확인하고 처리한다.							
		계정 오류 입력 접근제한 설정	계정정보(ID) 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 접근을 제한하고 있는지 확인하고 처리한다.							
		부재 시 시스템 접속 차단 설정	일정 시간 이상 업무처리하지 않는 경우 시스템 접속을 차단하고 있는지 확인하고 처리한다.							
		비업무용 사이트 접속 차단 설정	파일 공유용 P2P, 웹하드, 도박 등 유해사이트 접속을 차단하고 있는지 확인하고 처리한다.							

상위 개념	하위 개념	세부 지표	평가지표	자가 진단표						
				N	VL	L	M	VM	H	VH
		비인가자 접근 차단	비인자자가 관리용 기기에 접근하여 임의 조작 못하도록 조치하고 있는지 확인하고 처리한다.							
		안전한 접속(또는 인증) 수단 적용	개인정보 처리시스템에 접속 시 안전한 접속 수단이나 안전한 인증수단을 적용하고 있는지 확인하고 처리한다.							
		관리용 단말기 접근통제	관리용 단말기가 본래 목적 외로 사용되지 않도록 조치하고 있는지 확인하고 처리한다.							
	접속기록 관리	개인정보 취급자의 접속기록 보관 기간 설정	개인정보 취급 업무담당자의 접속기록을 최소 1년 이상(5만 명 이상의 개인정보를 처리하거나, 고유 식별정보 또는 민감정보를 처리하는 경우는 2년 이상) 보관하고 있는지 확인하고 처리한다.							
		접속기록 필수 정보 적용	개인정보 취급자 및 처리 업무를 확인할 수 있도록 개인정보 취급자의 계정, 접속일시, 접속지 정보, 처리한 정보 주체 정보, 수행 업무(조회, 다운로드 등) 등을 확인할 수 있도록 하였는지 확인하고 처리한다.							
		접속기록의 안전한 보관	개인정보 처리시스템 접속기록이 위.변조 및 도난, 분실되지 않도록 안전하게 보관하고 있는지 확인하고 처리한다.							
		접속기록 점검 관리	개인정보의 오남용, 분실·유출·도난·변조 또는 훼손 등을 대응을 위해 접속기록을 월 1회 이상 점검 및 후속 조치를 하고 있는지 확인하고 처리한다.							
	개인정	개인정보의 암호화	고유 식별정보(주민등록번호, 여권번호 등), 비밀번							

상위 개념	하위 개념	세부 지표	평가지표	자가 진단표						
				N	VL	L	M	VM	H	VH
	보의 암호화		호, 바이오 정보(지문, 얼굴 등)가 암호화되어 있는지 확인하고 처리한다.							
		비밀번호의 암호화	비밀번호는 일방향 암호화를 적용하여 저장되는지 확인하고 처리한다.							
개인정보 관리 수준 점검 및 개선	관리/기술적 보호	개인정보 관리 정책의 점검 및 검토	개인정보 처리 방침, 관련 계획 및 지침, 가이드, 매뉴얼 등 관련 정책서가 법적 준거성과 현실에 맞게 수립되어 있는지를 연 1회 이상 점검하고 보완 조치 계획을 하고 있는지 확인하고 처리한다.							
		개인정보 관리 정책의 개선	개인정보 처리 방침, 관련 계획 및 지침, 가이드, 매뉴얼 등 관련 정책서가 법적 준거성과 현실에 맞게 수립하였는지 점검한 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.							
		개인정보 관리 점검 및 검토	개인정보 생애주기, 안전성 확보 조치 등 개인정보 관리실태를 연 1회 이상 점검하고 보완 조치계획을 하고 있는지 확인하고 처리한다.							
		개인정보 관리 점검결과 확인된 사항 조치	개인정보 생애주기, 안전성 확보 조치 등 개인정보 관리실태 점검 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.							
		보안취약점 점검 및 위험평가 검토	개인정보 처리시스템 또는 홈페이지를 통해 해킹 사고가 발생하지 않도록 연 1회 이상 취약점 점검을 수행하고 위험분석 평가, 보완 조치계획을 하고 있는지 확인하고 처리한다.							

상위 개념	하위 개념	세부 지표	평가지표	자가 진단표						
				N	VL	L	M	VM	H	VH
		보안취약점 개선 조치	개인정보 처리시스템 또는 홈페이지 보안취약점 점검 점검한 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.							
		개인정보 노출 여부 모니터링 및 검토	홈페이지, 개인정보 처리시스템을 통해 개인정보 노출 여부를 월 1회 이상 모니터링하고 보완 조치계획을 하고 있는지 확인하고 처리한다.							
		개인정보 노출 모니터링 결과 확인된 사항 조치	개인정보 노출 여부 모니터링 점검한 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.							
	대응훈련 능력	개인정보 침해사고 대응훈련	개인정보 유출 사고 발생 시 개인정보 유출 사고 대응계획에 따라 신속히 대응하여 그 피해를 최소화하기 위해 개인정보 침해사고 대응훈련을 하고, 결과에 따른 보완 조치계획을 하고 있는지 확인하고 처리한다.							
		개인정보 침해사고 대응훈련 통한 확인된 사항 조치	개인정보 침해사고 대응훈련 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.							
		개인정보 재해 복구 훈련	재해재난 발생 시 개인정보 처리시스템 보호를 위해 수립된 위기 대응 매뉴얼에 따라 모의훈련을 실시하고 보완 조치계획을 하고 있는지 확인하고 처리한다.							
		개인정보 재해 복구 훈련을 통한 확인된 사항 조치	개인정보 처리시스템 재해 복구 훈련 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.							

상위 개념	하위 개념	세부 지표	평가지표	자가 진단표						
				N	VL	L	M	VM	H	VH
권리 보장 및 윤리 역량	정보 주체의 권리보장	정보 주체 중심의 개인정보 처리 방침 공개	개인정보 처리 방침을 정보 주체가 알기 쉽게 필수 사항을 모두 투명·명확하게 포함하여 수립하고, 홈페이지 등 정보 주체가 쉽게 확인할 수 있도록 주기적으로 공개하고 있는지 확인하고 처리한다.							
		정보 주체 중심의 개인정보 수집 이용동의서 제공	개인정보 수집 이용동의서는 정보 주체가 알기 쉽게 구성하고, 민감정보 등 중요한 부분은 글씨 크기, 굵기, 색상, 밑줄 등을 처리하였는지 확인하고 처리한다.							
		개인정보의 열람·정정·삭제·처리정지의 처리	개인정보의 열람·정정·삭제 및 처리정지에 관한 사항을 안내하고, 절차에 따라 적법·명확하게 처리하고 있는지 확인하고 처리한다.							
		법적 대리인의 동의권 보장	만14세 미만의 아동의 개인정보를 처리하는 경우, 해당 아동의 법정 대리인 동의를 받고, 그 과정에서 법정 대리인이 동의를 거부하거나 동의 의사가 확인되지 않는 경우에는 해당 법정 대리인의 개인정보를 5일 이내 파기하고 있는지 확인하고 처리한다.							
		개인정보 유출 신고 안내	개인정보 침해 사실을 신고하는 방법을 정보 주체에게 안내하고 있는지 확인하고 처리한다.							
	조직의 역량	조직의 개인정보보호 관련 규정 준수	우리 조직의 개인정보보호 관련 규정을 마련되어 있는지 확인하고 처리한다.							
		조직의 개인정보 침해사고 지침 준수	우리 조직의 개인정보 침해사고에 대한 지침이 마련되어 있는지 확인하고 처리한다.							

상위 개념	하위 개념	세부 지표	평가지표	자가 진단표						
				N	VL	L	M	VM	H	VH
		개인정보보호 전담 조직 및 인력 구성	조직 내 개인정보보호 전담 조직 및 인력이 구성되어 있는지 확인하고 처리한다.							
		개인정보보호 전용 예산 편성	개인정보보호 전용 예산을 편성하고, 개선을 위한 예산 증액 노력을 하고 있는지 확인하고 처리한다.							
		개인정보보호 교육과정 운영 및 평가	임직원 및 수탁자 등 맞춤형 개인정보보호 교육 프로그램을 운영하고 있는지 확인하고 처리한다.							
		성과관리(또는 인센티브제도) 운용	조직구성원의 개인정보 관리역량을 높일 수 있도록 성과관리 또는 인센티브제도 운영하고 있는지 확인하고 처리한다.							
		위반자 제재 및 처벌	우리 조직은 개인정보 오남용, 유출 위반자에 대해서 규정에 따라 투명하고 공정하게 제재와 처벌을 하고 있는지 확인하고 처리한다.							
	개인의 역량과 윤리의식	개인정보보호에 대한 도덕성과 자기통제	우리 조직의 개인정보보호 관련 규정과 처벌 규정을 잘 알고 있고, 자신이 하고 싶은 대로 하고자 하는 충동이 일어날 때 충동을 극복하고자 하는 개인의 노력을 하고 있는지 확인하고 처리한다.							
		개인정보 처리 업무의 사명감	조직구성원으로서 사명감과 직업의식을 가지고 맡은 일에 대한 투철한 책임의식이 있는지 확인하고 처리한다.							

상위 개념	하위 개념	세부 지표	평가지표	자가 진단표						
				N	VL	L	M	VM	H	VH
		개인정보보호 법률 및 제도 이해력과 행동	조직 내 개인정보보호를 위해 규정된 규범을 조직 구성원이 개인정보보호에 긍정적이고, 이를 성공적으로 수행할 수 있도록 하고 있는지 확인하고 처리한다.							
		개인정보보호 교육 이수 및 자기 계발	개인정보보호 교육에 어느 정도 관심이 있고, 연 몇 회를 이수하고 있는지 확인하고 자기 계발을 통해 관리능력을 향상하는 노력을 한다.							
		개인정보보호에 대한 자기 효능감	개인정보보호 업무를 위해 주어진 정책에 대해 성공적으로 수행할 수 있다는 개인의 기대감 정도(보안정책 인지, 습득, 적용, 적응 정도)를 확인하고 노력한다.							
		개인정보보호 기술 능력과 활용도	개인정보 처리시스템 또는 업무용 단말기의 안전조치 방법을 어느 정도 알고 있고, 이를 수행하고 있는지 확인하고 처리한다.							
		피해 인지력과 문제해결 능력	개인정보 침해사고 대응 절차를 잘 이해하고 있고, 개인정보 침해사고 대응훈련에 적극 참여하여 대응 능력을 키우고자 노력하고, 침해사고가 발생하면 즉시 문제를 해결할 수 있다.							

Ⅳ. 개인정보 관리역량 성숙도 모델 및 평가지표의 실증

4.1 신뢰도 검증

4.1.1 자료수집 및 대상자의 일반적 특성

개발한 개인정보 관리역량 성숙도 모델 및 평가지표에 대한 신뢰성 검증을 위해 공공기관종사자와 이 기관을 대상으로 한 수탁업무를 수행하거나 수행한 경험이 있는 민간기관을 대상으로 2022년 11월 8일부터 11월 13일까지 조사를 진행하였다. 조사 방법은 설문지 방식으로, 측정 항목은 89개 세부 지표와 리커트 5점 척도로 구성되었다. 설문조사 대상은 총 115명이었으나 99부를 회수하였고, 배부된 설문지에 무응답한 경우와 불성실하고 신뢰성이 없다고 판단되는 설문지 11부를 제외하고, 설문에 적절하게 응답한 88명을 분석에 활용하였다. 대상자의 인구통계학적 특성은 <표 Ⅳ-1>과 같다.

<표 Ⅳ-1> 대상자의 인구통계학적 특성

구분		빈도(명)	백분율(%)
성별	남성	39	44.3
	여성	49	55.7
	계	88	100
연령	20대	26	29.5
	30대	30	34.1
	40대	19	21.6
	50대 이상	13	14.8
	계	88	100
기관유형	공공	48	54.5
	민간	40	45.5
	계	88	100

구분		빈도(명)	백분율(%)
업무유형	개인정보 취급	64	72.7
	일반업무	24	27.3
	계	88	100
경력	3년 미만	26	29.5
	3~6년	30	34.1
	7~10년	19	21.6
	11년 이상	13	14.8
	계	88	100

성별은 남성 44.3%(39명)와 여성 55.7%(49명)가 비슷한 비율인 것으로 나타났다. 연령별 분포는 30대가 34.1%(30명), 20대 29.5%(26명), 40대 21.6%(19명), 50대 이상 14.8%(13명) 순으로 나타났다. 기관 유형으로는 공공기관 54.5%(48명), 일반기업 45.5%(40명) 순으로 나타났다. 업무유형으로는 개인정보 취급 업무가 72.7%(64명), 일반업무 27.3%(24명) 순으로 나타났다. 개인정보 관련 업무경력으로는 3~6년 34.1%(30명), 3년 미만 29.5%(26명), 7~10년 21.6%(19명), 11년 이상 14.8%(13명) 순으로 나타났다.

4.1.2 자료 분석 방법

회수된 88부에 대한 통계분석은 IBM SPSS Statistics를 이용하여 조사대상자의 인구통계학적 특성, 평가지표의 신뢰도 검정 등을 실시하였다. 자료 분석과정은 다음과 같은 과정을 거쳐 조사자료에 대해 통계처리를 하였다.

첫 번째, 세부 지표별 평균과 표준편차를 분석하였다. 두 번째, 개발된 성숙도 모델의 신뢰도 검정을 위해 항목 간의 유사성과 일관성, 예측 가능성과 의존 가능성, 정확성, 안전성 등을 알아보는 신뢰성 분석은 크론바흐(Cronbach, 1951)의 알파계수(Cronbach's α)를 이용하여 신뢰성을 검증하였다. Cronbach's α 값이 0.7 이상이면 내적 일관성이 유의한 것으로 하였다.

4.1.3 신뢰도 검증 결과

가. 평가지표의 평균과 표준편차

개발한 개인정보 관리역량 성숙도 모델의 세부 지표에 대한 평균과 표준편차는 <표 Ⅳ-2>와 같다.

‘접속기록 점검 관리’는 평균값이 4.74로 상대적으로 높은 평균과 0.442로 낮은 표준편차로 다른 세부 지표들과 비교하여 일반적으로 가장 중요하게 생각하는 지표인 것으로 나타났다. ‘개인정보의 보호 대책 구현’ 지표도 평균이 4.72 이상이고 표준편차가 0.454 이하로 다른 지표들과 비교하여 실무자들이 중요하게 생각하는 지표인 것으로 나타났다.

한편, ‘보안취약점 개선 조치’, ‘제3자 제공, 위・수탁 적절성 검토’, ‘선택정보 동의 거부 시 서비스 제공’, ‘개인정보의 국외 이전 안내 및 동의’의 지표들의 평균은 3.95 이하이고 표준편차가 0.642 이상으로 다른 지표들과 비교하여 중요도가 상대적으로 낮고 중요도에 대한 실무자들의 인식에도 편차가 큰 것으로 나타났다.

<표 Ⅳ-2> 세부 지표의 평균과 표준편차

상위 개념	하위 개념	세부 지표	평균	표준 편차
사전 계획 및 설계 단계	업무처리 흐름 분석	개인정보 처리 업무처리 흐름도·흐름표 작성	4.08	0.698
		업무처리 흐름도·흐름표 개정관리	4.30	0.628
	개인정보 흐름 분석	개인정보 수집, 이용, 보유기간 적절성 검토	4.30	0.628
		주민등록번호, 민감정보, 고유 식별정보 처리 적절성 검토	4.58	0.673
		개인정보 수집 항목 구분 적절성 검토	4.36	0.647
		만 14세 미만의 아동 정보수집 적절성 검토	4.30	0.628
		제3자 제공, 위·수탁 적절성 검토	4.36	0.647
		개인정보의 타 시스템 연계 적절성 검토	4.30	0.628
		개인정보 안전성 확보 조치 적절성 검토	4.36	0.647
		개인정보 처리 흐름도 작성 및 이력 관리	4.30	0.628
		개인정보 처리 흐름표 작성 및 이력 관리	4.11	0.596

상위 개념	하위 개념	세부 지표	평균	표준 편차
	개인정보 안전성 분석	개인정보 처리 위험도 및 침해요인 분석	4.36	0.647
		개인정보 위험평가 분석	4.36	0.647
		개인정보의 보호 대책 선정	4.70	0.609
		개인정보의 보호 대책 구현	4.72	0.454
	관리체계 수립	개인정보보호 정책 수립 적절성 검토	3.02	0.371
		법적 요구사항 준수 적절성 검토	3.02	0.371
		관리체계 점검 및 개선 계획 수립 적절성 검토	3.02	0.371
개인정보 생애주기 보호	수집	개인정보 수집 필수사항 안내 및 동의	4.36	0.647
		목적별 최소한의 필수정보 수집	4.36	0.647
		개인정보 수집 항목의 필수와 선택정보 구분	4.36	0.647
		민감정보 처리 별도 동의	4.35	0.644
		고유 식별정보 별도 동의	4.36	0.647
		만 14세 미만의 아동의 정보수집 시 법정 대리인 동의	4.25	0.699
		주민등록번호 수집 제한 법적 준수	4.36	0.647
		선택정보 동의 거부 시 서비스 제공	3.39	0.668
		개인정보의 국외 이전 안내 및 동의	3.38	0.666
	이용 및 제공	개인정보 처리 위탁 계약서 작성 및 체결	4.35	0.644
		위탁업무의 정보 공개	4.35	0.644
		수탁자 대상 교육 및 관리 감독	4.35	0.644
		목적 내 제3자 이용·제공 시 필수사항 고지 및 동의	4.35	0.644
		목적 외 제3자 이용·제공 시 필수사항 고지 및 동의	4.35	0.644
		목적 외 제3자 이용·제공 사항 공고	4.35	0.644
		개인정보 이용 및 제3자 제공 대장 기록 관리	4.35	0.644
	보관 및 파기	개인정보 자료 보관실의 잠금장치 및 출입 통제	4.35	0.644
		개인정보 저장 장비의 잠금장치 및 출입 통제	4.65	0.626
		개인정보 파기 기간 준수	4.35	0.644
		개인정보 파일 파기 절차 준수	4.35	0.644
		개인정보 파기 방법 적절성	4.65	0.626
		개인정보 파일 파기 관리대장 기록 관리	4.35	0.644

상위 개념	하위 개념	세부 지표	평균	표준 편차
안전성 확보 조치	내부 관리계획	내부 관리계획 수립 및 이력 관리	4.35	0.644
		내부 관리계획 이행점검 및 개선	4.35	0.644
	접근관리	접근권한 절차 수립 및 이력 관리	4.65	0.626
		접근권한 차등 부여	4.35	0.644
		접근권한 변경내역 기록 및 관리	4.35	0.644
	접근통제	안전한 비밀번호 작성 규칙 적용	4.35	0.644
		계정 오류 입력 접근제한 설정	4.35	0.644
		부재 시 시스템 접속 차단 설정	4.65	0.626
		비업무용 사이트 접속 차단 설정	4.65	0.626
		비인가자 접근 차단	4.35	0.644
		안전한 접속(또는 인증) 수단 적용	4.35	0.644
		관리용 단말기 접근통제	4.65	0.626
	접속기록 관리	개인정보 취급자의 접속기록 보관 기간 설정	4.65	0.626
		접속기록 필수정보 적용	4.35	0.644
		접속기록의 안전한 보관	4.35	0.644
		접속기록 점검 관리	4.74	0.442
	개인정보의 암호화	개인정보의 암호화	4.35	0.644
		비밀번호의 암호화	4.35	0.644
개인정보 관리 수준 점검 및 개선	관리/기술적 보호	개인정보 관리 정책의 점검 및 검토	4.35	0.644
		개인정보 관리 정책의 개선	4.35	0.644
		개인정보 관리 점검 및 검토	4.65	0.626
		개인정보 관리 점검결과 확인된 사항 조치	4.65	0.626
		보안취약점 점검 및 위험평가 검토	4.06	0.684
		보안취약점 개선 조치	3.95	0.642
		개인정보 노출 여부 모니터링 및 검토	4.35	0.644
		개인정보 노출 모니터링 결과 확인된 사항 조치	4.35	0.644
	대응훈련 능력	개인정보 침해사고 대응훈련	4.35	0.644
		개인정보 침해사고 대응훈련 통한 확인된 사항 조치	4.35	0.644
		개인정보 재해복구 훈련	4.65	0.626
		개인정보 재해복구 훈련을 통한 확인된 사항 조치	4.35	0.644

상위 개념	하위 개념	세부 지표	평균	표준 편차
권리 보장 및 윤리 역량	정보 주체의 권리보장	정보 주체 중심의 개인정보 처리 방침 공개	4.35	0.644
		정보 주체 중심의 개인정보 수집 이용동의서 제공	4.35	0.644
		개인정보의 열람·정정·삭제·처리정지의 처리	4.65	0.626
		법적 대리인의 동의권 보장	4.65	0.626
		개인정보 유출 신고 안내	4.35	0.644
	조직의 역량	조직의 개인정보보호 관련 규정 준수	4.35	0.644
		조직의 개인정보 침해사고 지침 준수	4.65	0.626
		개인정보보호 전담 조직 및 인력 구성	4.34	0.741
		개인정보보호 전용 예산 편성	4.30	0.761
		개인정보보호 교육과정 운영 및 평가	4.35	0.644
		성과관리(또는 인센티브제도) 운용	4.35	0.644
		위반자 제재 및 처벌	4.35	0.644
	개인의 역량과 윤리의식	개인정보보호에 대한 도덕성과 자기통제	4.65	0.626
		개인정보 처리 업무의 사명감	4.35	0.644
		개인정보보호 법률 및 제도 이해력과 행동	4.35	0.644
		개인정보보호 교육 이수 및 자기 계발	4.65	0.626
		개인정보보호에 대한 자기효능감	4.33	0.738
		개인정보보호 기술 능력과 활용도	4.35	0.644
		피해 인지력과 문제해결 능력	4.35	0.644

나. 신뢰도 검증

신뢰성은 연구 대상에 대해 측정오류가 발생하지 않기 위해 모든 변수에 대하여 반복적으로 측정 시 결과에 대한 일관성 보장 여부를 판단하는 개념이다. 모든 변수에 대해 신뢰성 있게 측정되었는지를 검증이 필요하며, 본 연구에서도 Cronbach's α 계수를 활용하여 비슷한 개념에 대해 다수의 복수 항목으로 신뢰도를 측정하였다. Cronbach's α 계수는 0-1 사이의 값을 가지고 있고, 신뢰도 계수의 적정수준을 판정하는 절대적인 기준은 없지만, 일반적으로 Nunally (1979)가 제시한 0.7 이상이면 적정수준으로 판단하고 있다[77].

본 연구에서 개발한 개인정보 관리역량 성숙도 모델의 세부 지표에 대한 항목 간의 일치 수준을 판단하는 Cronbach′s α 값을 <표 Ⅳ-3>과 같이 산출한 결과, 0.992로 Cronbach′s α 값이 0.9 이상으로 신뢰도가 매우 높은 것으로 나타났다. 일반적으로 Cronbach′s α 값이 0.7 이상인 경우 신뢰할 수 있다고 볼 수 있다.

<표 Ⅳ-3> Cronbach's α 값 산출 결과

Cronbach's α	표준화된 항목의 Cronbach's α
0.992	0.992

다. 신뢰도 분석 결과

신뢰도 분석 결과 세부 지표 항목이 삭제된 경우의 Cronbach′s α 값이 <표 Ⅳ-4>에서 제시한 모든 항목이 포함되었을 때의 신뢰도 값인 표준화된 항목의 Cronbach′s α 값이 0.992보다 큰 값이 없기 때문에 모든 항목이 포함되었을 때의 신뢰도가 높다는 것을 의미한다.

<표 IV-4> 세부 지표의 신뢰도 분석 결과

상위 개념	하위 개념	세부 지표	평균	분산	상관 계수	Cronbach's α
사전 계획 및 설계 단계	업무처리 흐름 분석	개인정보 처리 업무처리 흐름도·흐름표 작성	4.53	0.286	0.318	0.992
		업무처리 흐름도·흐름표 개정관리	4.31	0.390	0.832	0.992
	개인정보 흐름 분석	개인정보 수집, 이용, 보유기간 적절성 검토	4.18	0.584	0.832	0.992
		주민등록번호, 민감정보, 고유 식별정보 처리 적절성 검토	4.25	0.624	0.790	0.992
		개인정보 수집 항목 구분 적절성 검토	4.33	0.431	0.853	0.992
		만 14세 미만의 아동 정보 수집 적절성 검토	4.56	0.457	0.832	0.992
		제3자 제공, 위·수탁 적절성 검토	4.00	0.278	0.853	0.992
		개인정보의 타 시스템 연계 적절성 검토	3.95	0.432	0.832	0.992
		개인정보 안전성 확보 조치 적절성 검토	3.97	0.190	0.853	0.992
		개인정보 처리 흐름도 작성 및 이력 관리	4.44	0.405	0.832	0.992
		개인정보 처리 흐름표 작성 및 이력 관리	4.09	0.191	0.539	0.992
	개인정보 안전성 분석	개인정보 처리 위험도 및 침해요인 분석	4.20	0.299	0.853	0.992
		개인정보 위험평가 분석	4.23	0.702	0.853	0.992
		개인정보의 보호 대책 선정	4.42	0.455	0.550	0.992
		개인정보의 보호 대책 구현	4.29	0.487	0.206	0.992
	관리체계 수립	개인정보보호 정책 수립 적절성 검토	4.48	0.321	0.299	0.992
		법적 요구사항 준수 적절성 검토	4.06	0.301	0.299	0.992
		관리체계 점검 및 개선 계획 수립 적절성 검토	4.30	0.560	0.299	0.992

상위 개념	하위 개념	세부 지표	평균	분산	상관 계수	Cronbach's α
개인정보 생애주기 보호	수집	개인정보 수집 필수사항 안내 및 동의	4.35	0.544	0.947	0.992
		목적별 최소한의 필수정보 수집	4.21	0.583	0.947	0.992
		개인정보 수집 항목의 필수와 선택정보 구분	4.39	0.500	0.947	0.992
		민감정보 처리 별도 동의	4.34	0.419	0.951	0.992
		고유 식별정보 별도 동의	4.32	0.497	0.947	0.992
		만 14세 미만의 아동의 정보수집 시 법정 대리인 동의	3.57	0.404	0.484	0.992
		주민등록번호 수집 제한 법적 준수	4.38	0.620	0.947	0.992
		선택정보 동의 거부 시 서비스 제공	3.85	0.648	0.347	0.992
		개인정보의 국외 이전 안내 및 동의	2.36	0.772	0.365	0.992
	이용 및 제공	개인정보 처리 위탁 계약서 작성 및 체결	4.38	0.464	0.951	0.992
		위탁업무의 정보 공개	4.31	0.546	0.951	0.992
		수탁자 대상 교육 및 관리 감독	4.41	0.452	0.951	0.992
		목적 내 제3자 이용·제공 시 필수사항 고지 및 동의	4.29	0.626	0.951	0.992
		목적 외 제3자 이용·제공 시 필수사항 고지 및 동의	4.28	0.619	0.951	0.992
		목적 외 제3자 이용·제공 사항 공고	4.27	0.632	0.951	0.992
		개인정보 이용 및 제3자 제공 대장 기록 관리	4.33	0.535	0.951	0.992
	보관 및 파기	개인정보 자료 보관실의 잠금장치 및 출입 통제	4.33	0.448	0.951	0.992
		개인정보 저장 장비의 잠금장치 및 출입 통제	4.30	0.595	0.496	0.992
		개인정보 파기 기간 준수	4.25	0.676	0.951	0.992
		개인정보 파일 파기 절차 준수	4.42	0.420	0.951	0.992
		개인정보 파기 방법 적절성	4.38	0.498	0.496	0.992
		개인정보 파일 파기 관리대장 기록 관리	4.38	0.411	0.951	0.992

상위 개념	하위 개념	세부 지표	평균	분산	상관 계수	Cronbach's α
안전성 확보 조치	내부 관리계획	내부 관리계획 수립 및 이력 관리	4.29	0.522	0.951	0.992
		내부 관리계획 이행점검 및 개선	4.27	0.528	0.951	0.992
	접근관리	접근권한 절차 수립 및 이력 관리	4.44	0.353	0.496	0.992
		접근권한 차등 부여	4.25	0.659	0.951	0.992
		접근권한 변경내역 기록 및 관리	4.27	0.615	0.951	0.992
	접근통제	안전한 비밀번호 작성 규칙 적용	4.28	0.601	0.951	0.992
		계정 오류 입력 접근제한 설정	4.06	0.683	0.951	0.992
		부재 시 시스템 접속 차단 설정	4.32	0.532	0.496	0.992
		비업무용 사이트 접속 차단 설정	4.34	0.434	0.496	0.992
		비인가자 접근 차단	4.37	0.322	0.951	0.992
		안전한 접속(또는 인증) 수단 적용	4.41	0.419	0.951	0.992
		관리용 단말기 접근통제	4.13	0.687	0.496	0.992
	접속기록 관리	개인정보 취급자의 접속기록 보관 기간 설정	4.27	0.476	0.496	0.992
		접속기록 필수정보 적용	4.37	0.305	0.951	0.992
		접속기록의 안전한 보관	4.45	0.528	0.951	0.992
		접속기록 점검 관리	4.30	0.578	0.065	0.992
	개인정보의 암호화	개인정보의 암호화	4.16	0.643	0.951	0.992
		비밀번호의 암호화	4.31	0.564	0.951	0.992

상위 개념	하위 개념	세부 지표	평균	분산	상관 계수	Cronbach's α
개인 정보 관리 수준 점검 및 개선	관리/기술적 보호	개인정보 관리 정책의 점검 및 검토	4.36	0.459	0.951	0.992
		개인정보 관리 정책의 개선	4.33	0.553	0.951	0.992
		개인정보 관리 점검 및 검토	4.25	0.589	0.496	0.992
		개인정보 관리 점검결과 확인된 사항 조치	4.28	0.571	0.496	0.992
		보안취약점 점검 및 위험평가 검토	4.31	0.564	0.347	0.992
		보안취약점 개선 조치	4.37	0.427	0.328	0.992
		개인정보 노출 여부 모니터링 및 검토	4.40	0.328	0.951	0.992
		개인정보 노출 모니터링 결과 확인된 사항 조치	4.38	0.568	0.951	0.992
	대응훈련 능력	개인정보 침해사고 대응훈련	4.32	0.445	0.951	0.992
		개인정보 침해사고 대응훈련 통한 확인된 사항 조치	4.21	0.583	0.951	0.992
		개인정보 재해복구 훈련	4.35	0.526	0.496	0.992
		개인정보 재해복구 훈련을 통한 확인된 사항 조치	4.28	0.619	0.951	0.992
권리 보장 및 윤리 역량	정보 주체의 권리보장	정보 주체 중심의 개인정보 처리 방침 공개	4.39	0.466	0.951	0.992
		정보 주체 중심의 개인정보 수집 이용동의서 제공	4.33	0.500	0.951	0.992
		개인정보의 열람·정정·삭제·처리정지의 처리	4.43	0.387	0.496	0.992
		법적 대리인의 동의권 보장	4.28	0.553	0.496	0.992
		개인정보 유출 신고 안내	4.30	0.560	0.951	0.992

상위 개념	하위 개념	세부 지표	평균	분산	상관 계수	Cronbach's α
	조직의 역량	조직의 개인정보보호 관련 규정 준수	4.36	0.476	0.951	0.992
		조직의 개인정보 침해사고 지침 준수	4.30	0.508	0.496	0.992
		개인정보보호 전담 조직 및 인력 구성	4.41	0.417	0.389	0.992
		개인정보보호 전용 예산 편성	4.24	0.602	0.368	0.992
		개인정보보호 교육과정 운영 및 평가	4.42	0.385	0.951	0.992
		성과관리(또는 인센티브제도) 운용	4.22	0.506	0.951	0.992
		위반자 제재 및 처벌	4.28	0.549	0.951	0.992
	개인의 역량과 윤리의식	개인정보보호에 대한 도덕성과 자기통제	4.20	0.717	0.496	0.992
		개인정보 처리 업무의 사명감	4.18	0.637	0.951	0.992
		개인정보보호 법률 및 제도 이해력과 행동	4.28	0.636	0.951	0.992
		개인정보보호 교육 이수 및 자기 계발	4.28	0.462	0.496	0.992
		개인정보보호에 대한 자기효능감	4.16	0.706	0.336	0.992
		개인정보보호 기술 능력과 활용도	4.21	0.566	0.951	0.992
		피해 인지력과 문제해결 능력	4.28	0.567	0.951	0.992

4.2 개인정보 관리역량 자가 진단 검증

4.2.1 자료수집 및 참여자의 일반적 특성

개발한 개인정보 관리역량 성숙도 모델의 측정 척도에 대한 검증을 위해 공공기관과 지방자치단체 개인정보 취급 업무담당자와 관련된 일반기업, IT업체 수탁자를 대상으로 2022년 11월 10일부터 11월 23일까지 조사를 진행하였다.

설문조사 대상은 총 92명이었으나 86부를 회수하였고, 배부된 설문지에 무응답한 경우와 불성실하고 신뢰성이 없다고 판단되는 설문지 4부를 제외하고, 설문에 적절하게 응답한 82명을 분석에 활용하였다. 대상자의 인구통계학적 특성은 <표 Ⅳ-5>와 같다.

<표 Ⅳ-5> 참여 대상자의 인구통계학적 특성

구분		빈도(명)	백분율(%)
성별 (n=38)	남성	44	53.7
	여성	38	46.3
		82	100
연령 (n=38)	20대	22	26.8
	30대	17	20.7
	40대	26	31.8
	50대 이상	17	20.7
	계	82	100
경력 (n=38)	3년 미만	30	36.6
	3~5년	13	15.9
	6~8년	24	29.3
	9년 이상	15	18.2
	계	82	100
기관 유형 (n=38)	민간기업	30	36.6
	공공기관	26	31.7
	지방자치단체	26	31.7
	계	82	100

성별은 남성 53.7%(44명), 여성 46.3%(38명)로 나타났다. 연령은 40대가 31.8%(26명), 20대 이하 26.8%(22명), 30대 20.7%(17명), 50대 이상 20.7%(17명) 순으로 나타났다. 개인정보 관련 업무경력 기간은 3년 미만 36.6%(30명), 6~8년 29.3%(24명), 9년 이상 18.2%(15명), 3~5년 15.9%(13명) 순으로 나타났다. 기관 유형으로는 민간기업 36.6%(30명), 지방자치단체 31.7%(26명), 공공기관 31.7%(26명) 순으로 나타났다.

4.2.2 PIA-CMMI-PCM2 비교 분석

본 연구에서는 기존 성숙도 측정모델과 개발한 성숙도 측정모델을 비교 분석하였다. 기존 성숙도 측정모델은 현재 국가 및 공공기관을 대상으로 실시되고 있는 공공기관 개인정보 관리 수준 진단[75]과 개인정보 영향 평가(PIA)[9]의 측정모델과 CMMI 모델을 이용하였고, PIA 성숙도 단계는 <표 Ⅳ-6>과 같다.

<표 Ⅳ-6> PIA의 성숙도 측정모델

성숙도 단계			정의	배점	척도구간
성숙도 증가 ↑	2	이행	전사적으로 시행계획이 수립되고 수행되고 있는 단계	100	80% 초과
	1	부분이행	부분적으로 시행계획이 수립되고 수행되고 있는 단계	50	80% 이하
	0	미이행	세부 평가항목으로 수행되지 않고 있는 단계	0	20% 미만

CMMI(Capability Maturity Model Integration) 모델은 Inital, Managed, Defined, Quantiatively managed, Optimizing 등 5단계로 성숙도 단계가 되어 있으며, [표 Ⅳ-7]과 같다.

<표 Ⅳ-7> CMMI의 성숙도 측정모델

성숙도 단계			정의	배점	척도구간
성숙도 증가 ↑	Level 5	Optimizing	혁신과 기술 향상을 통하여 지속적인 개선 및 관리 상태	100	90% 초과
	Level 4	Quantitatively Managed	통계 및 정량적 기술을 통한 평가 및 관리 상태	75	90% 이하
	Level 3	Defined	표준 및 절차, 도구 등에 의해 정의되고 적용되는 상태	50	70% 이하
	Level 2	Managed	문서화, 계획, 실행, 관찰 및 통제 적용 상태	25	30% 이하
	Level 1	Initial	예측이 불가하고 관리가 안 되는 상태	0	10% 미만

제안한 PCM2 모델은 <표 Ⅳ-8>과 같이 N, VL, L, M, VM, H, VH 등 7점 척도로 구성되어 있으며, 척도 구간과 배점을 이용하였다.

<표 Ⅳ-8> 제안된 개인정보 관리역량 성숙도 모델(PCM2)

성숙도 단계		정의	배점	척도구간
역량 성숙도 증가 ↑	**VH** (Very High)	전사적으로 시행 및 성과 측정 계획이 수립되고 시행 후 결과에 따라 주기적으로 모니터링하고 결과에 따라 개선을 수행하는 단계	100	95% 초과
	H (High)	전사적으로 시행 및 성과 측정 계획이 수립되고 시행 후 주기적으로 모니터링하고 있는 단계	83.3	95% 이하
	VM (Very Medium)	전사적으로 시행계획과 성과 측정 계획이 수립되고 시행되고 있는 단계	66.7	85% 이하
	M (Medium)	전사적으로 시행계획이 수립되고 수행되고 있는 단계	50	65% 이하
	L (Low)	부분적으로 시행계획이 수립되고 수행되고 있는 단계	33.3	35% 이하
	VL (Very Low)	시행계획을 수립하지 않고 세부 평가항목을 부분적으로 수행하고 있는 단계	16.7	15% 이하
	N (None)	세부 평가항목으로 수행되지 않고 있는 단계	0	5% 미만

자가 진단표 질문지 구성은 개발된 개인정보 관리역량 평가지표 89개 항목과 PIA 평가항목 중 개인정보 영향평가 3개 항목을 추가하여 총 92개 항목으로 구성하였고, 측정 척도를 ISMS-P, PIA 등 선행연구에서 분석한 이행, 부분 이행, 미이행 등 3점 척도와 CMMI 모델의 5점 척도, 본 연구에서 제안한 7점 척도의 PCM2 모델이 적용된 질문지를 각각 배부하여 진행하였다.

기존 성숙도 측정모델과 개발한 성숙도 측정모델을 비교 검증한 결과, <표 Ⅳ-9>와 같다.

<표 IV-9> PIA-CMMI-PCM2 성숙도 측정 결과 비교

상위 개념	하위 개념	세부 지표	PIA		CMMI		PCM2	
			산출 점수	백분율 (%)	산출 점수	백분율 (%)	산출 점수	백분율 (%)
사전 계획 및 설계 단계	업무처리 흐름 분석	개인정보 처리 업무처리 흐름도·흐름표 작성	23	60.53	24.5	64.47	23.00	60.53
		업무처리 흐름도·흐름표 개정관리	21	55.26	23.25	61.18	22.17	58.34
	개인정보 흐름 분석	개인정보 수집, 이용, 보유기간 적절성 검토	27.5	72.37	30.75	80.92	28.34	74.57
		주민등록번호, 민감정보, 고유 식별정보 처리 적절성 검토	27.5	72.37	30.75	80.92	28.34	74.57
		개인정보 수집 항목 구분 적절성 검토	27.5	72.37	30.75	80.92	28.34	74.57
		만 14세 미만의 아동 정보수집 적절성 검토	24.5	64.47	29.25	76.97	28.00	73.69
		제3자 제공, 위·수탁 적절성 검토	23.5	61.84	24	63.16	22.50	59.21
		개인정보의 타 시스템 연계 적절성 검토	21	55.26	23.75	62.50	22.67	59.65
		개인정보 안전성 확보 조치 적절성 검토	21.5	56.58	24	63.16	23.50	61.85
		개인정보 처리 흐름도 작성 및 이력 관리	20.5	53.95	22.75	59.87	22.50	59.22
		개인정보 처리 흐름표 작성 및 이력 관리	20.5	53.95	22.75	59.87	22.50	59.22

상위 개념	하위 개념	세부 지표	PIA		CMMI		PCM2	
			산출 점수	백분율 (%)	산출 점수	백분율 (%)	산출 점수	백분율 (%)
	개인정보 안전성 분석	개인정보 처리 위험도 및 침해요인 분석	19.5	51.32	21.5	56.58	20.17	53.07
		개인정보 위험평가 분석	19	50.00	20	52.63	19.17	50.44
		개인정보의 보호 대책 선정	19	50.00	20	52.63	19.17	50.44
		개인정보의 보호 대책 구현	19	50.00	20	52.63	19.17	50.44
	개인정보 영향평가	개인정보 영향평가 대상 검토	3	7.89	2.5	6.58	2.832	7.45
		관리체계 및 보호조치 계획 수립	3	7.89	2.5	6.58	2.832	7.45
		기술적 보호조치 방안 계획 수립	3	7.89	2.5	6.58	2.832	7.45
	관리체계 수립	개인정보보호 정책 수립 적절성 검토	22.5	59.21	25.25	66.45	22.67	59.66
		법적 요구사항 준수 적절성 검토	22.5	59.21	25.25	66.45	22.67	59.66
		관리체계 점검 및 개선 계획 수립 적절성 검토	22.5	59.21	24.5	64.47	22.50	59.22
개인정보 생애주기 보호	수집	개인정보 수집 필수사항 안내 및 동의	30.5	80.26	34	89.47	30.17	79.38
		목적별 최소한의 필수정보 수집	30.5	80.26	33.75	88.82	30.00	78.94
		개인정보 수집 항목의 필수와 선택정보 구분	30.5	80.26	34	89.47	30.17	79.38
		민감정보 처리 별도 동의	30.5	80.26	34	89.47	30.17	79.38
		고유 식별정보 별도 동의	31	81.58	34.25	90.13	30.33	79.82
		만 14세 미만의 아동의 정보수집 시 법정 대리인 동의	29.5	77.63	33	86.84	29.50	77.63
		주민등록번호 수집 제한 법적 준수	31	81.58	34.25	90.13	30.00	78.94
		선택정보 동의 거부 시 서비스 제공	20	52.63	20.5	53.95	19.33	50.88
		개인정보의 국외 이전 안내 및 동의	14	36.84	11.25	29.61	11.67	30.70

상위 개념	하위 개념	세부 지표	PIA		CMMI		PCM2	
			산출 점수	백분율 (%)	산출 점수	백분율 (%)	산출 점수	백분율 (%)
	이용 및 제공	개인정보 처리 위탁 계약서 작성 및 체결	19	50.00	20.25	53.29	19.17	50.44
		위탁업무의 정보 공개	18	47.37	19	50.00	16.83	44.30
		수탁자 대상 교육 및 관리 감독	17	44.74	18.25	48.03	17.50	46.06
		목적 내 제3자 이용·제공 시 필수사항 고지 및 동의	22	57.89	21.75	57.24	20.00	52.63
		목적 외 제3자 이용·제공 시 필수사항 고지 및 동의	22	57.89	21.75	57.24	20.00	52.63
		목적 외 제3자 이용·제공 사항 공고	23	60.53	22	57.89	18.16	47.80
		개인정보 이용 및 제3자 제공 대장 기록 관리	23	60.53	22	57.89	18.50	48.67
	보관 및 파기	개인정보 자료 보관실의 잠금장치 및 출입 통제	36	94.74	37	97.37	31.16	81.99
		개인정보 저장 장비의 잠금장치 및 출입 통제	36	94.74	37	97.37	31.16	81.99
		개인정보 파기 기간 준수	36	94.74	37	97.37	31.16	81.99
		개인정보 파일 파기 절차 준수	36	94.74	37	97.37	31.16	81.99
		개인정보 파기 방법 적절성	36	94.74	37	97.37	31.16	81.99
		개인정보 파일 파기 관리대장 기록 관리	33.5	88.16	35.75	94.08	30.33	79.81
안전성 확보 조치	내부 관리계획	내부 관리계획 수립 및 이력 관리	15.5	40.79	17	44.74	17.33	45.61
		내부 관리계획 이행점검 및 개선	15.5	40.79	17	44.74	17.33	45.61
	접근관리	접근권한 절차 수립 및 이력 관리	25.5	67.11	29	76.32	26.17	68.86
		접근권한 차등 부여	25.5	67.11	29	76.32	26.17	68.86
		접근권한 변경내역 기록 및 관리	25.5	67.11	29	76.32	26.17	68.86

상위 개념	하위 개념	세부 지표	PIA		CMMI		PCM2	
			산출 점수	백분율 (%)	산출 점수	백분율 (%)	산출 점수	백분율 (%)
	접근통제	안전한 비밀번호 작성 규칙 적용	25.5	67.11	31	81.58	27.50	72.38
		계정 오류 입력 접근제한 설정	24	63.16	29.25	76.97	26.34	69.31
		부재 시 시스템 접속 차단 설정	29	76.32	32.75	86.18	28.67	75.44
		비업무용 사이트 접속 차단 설정	29	76.32	31.25	82.24	27.66	72.80
		비인가자 접근 차단	29	76.32	32.75	86.18	28.67	75.44
		안전한 접속(또는 인증) 수단 적용	25.5	67.11	30.5	80.26	27.00	71.06
		관리용 단말기 접근통제	29	76.32	32.75	86.18	28.50	75.00
	접속기록 관리	개인정보 취급자의 접속기록 보관 기간 설정	23.5	61.84	25.25	66.45	23.33	61.40
		접속기록 필수정보 적용	25	65.79	25.5	67.11	23.50	61.83
		접속기록의 안전한 보관	24	63.16	25	65.79	23.17	60.96
		접속기록 점검 관리	22	57.89	22.5	59.21	21.50	56.58
	개인정보의 암호화	개인정보의 암호화	32	84.21	35	92.11	29.83	78.50
		비밀번호의 암호화	29	76.32	32.25	84.87	28.00	73.68
개인정보 관리 수준 점검 및 개선	관리/기술적 보호	개인정보 관리 정책의 점검 및 검토	24	63.16	27.25	71.71	24.50	64.48
		개인정보 관리 정책의 개선	24	63.16	27	71.05	24.33	64.04
		개인정보 관리 점검 및 검토	24.5	64.47	27.25	71.71	24.67	64.91
		개인정보 관리 점검결과 확인된 사항 조치	24.5	64.47	27	71.05	24.50	64.47
		보안취약점 점검 및 위험평가 검토	15	39.47	16.5	43.42	14.51	38.17
		보안취약점 개선 조치	15	39.47	16.5	43.42	14.51	38.17
		개인정보 노출 여부 모니터링 및 검토	15	39.47	17	44.74	15.17	39.92
		개인정보 노출 모니터링 결과 확인된 사항 조치	15	39.47	17	44.74	15.17	39.92

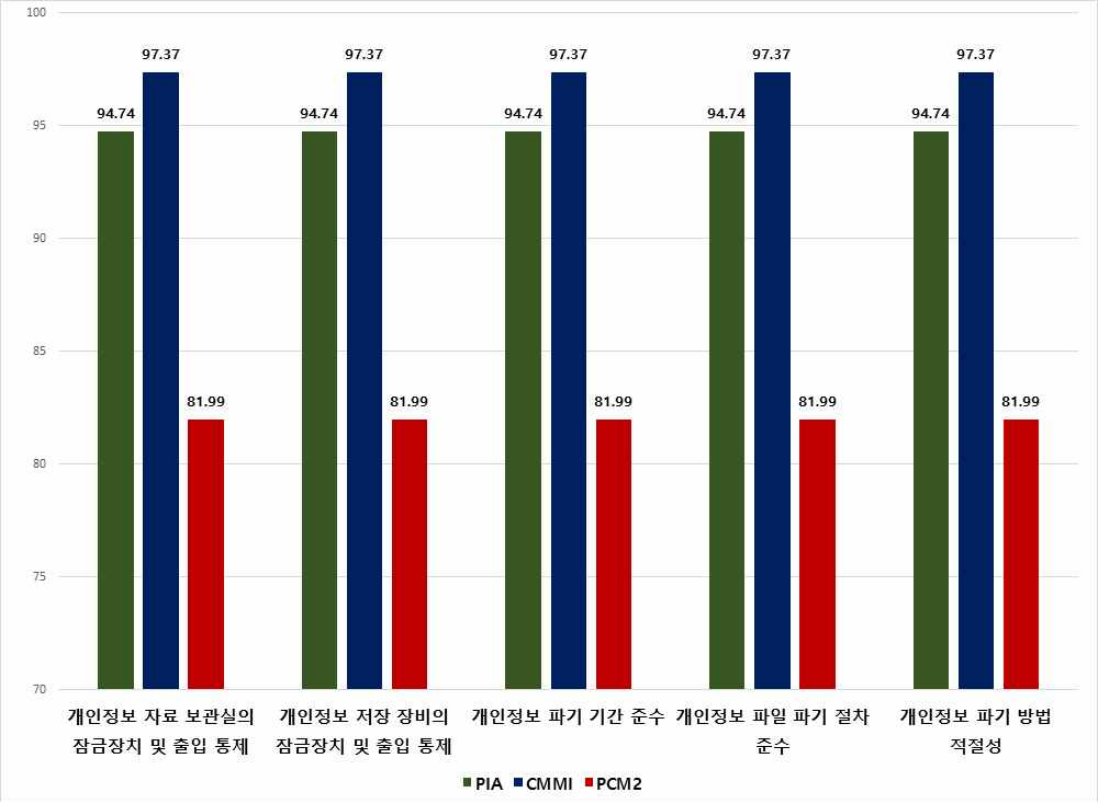
상위 개념	하위 개념	세부 지표	PIA		CMMI		PCM2	
			산출 점수	백분율 (%)	산출 점수	백분율 (%)	산출 점수	백분율 (%)
	대응훈련 능력	개인정보 침해사고 대응 훈련	14	36.84	14.75	38.82	13.67	35.97
		개인정보 침해사고 대응 훈련 통한 확인된 사항 조치	14	36.84	15	39.47	13.50	35.53
		개인정보 재해복구 훈련	13	34.21	12.75	33.55	11.84	31.14
		개인정보 재해복구 훈련을 통한 확인된 사항 조치	13	34.21	12.75	33.55	11.84	31.14
권리 보장 및 윤리 역량	정보 주체의 권리보장	정보 주체 중심의 개인정보 처리 방침 공개	23	60.53	27.25	71.71	24.50	64.48
		정보 주체 중심의 개인정보 수집 이용동의서 제공	23	60.53	27.25	71.71	24.50	64.48
		개인정보의 열람·정정·삭제·처리정지의 처리	23	60.53	27.25	71.71	24.50	64.48
		법적 대리인의 동의권 보장	23	60.53	28.25	74.34	25.17	66.24
		개인정보 유출 신고 안내	24.5	64.47	27.75	73.03	24.83	65.35
	조직의 역량	조직의 개인정보보호 관련 규정 준수	26.5	69.74	28.5	75.00	25.16	66.22
		조직의 개인정보 침해사고 지침 준수	24.5	64.47	26	68.42	22.33	58.77
		개인정보보호 전담 조직 및 인력 구성	15	39.47	15.5	40.79	13.67	35.97
		개인정보보호 전용 예산 편성	12.5	32.89	13	34.21	12.00	31.59
		개인정보보호 교육과정 운영 및 평가	28	73.68	29.5	77.63	26.00	68.41
		성과관리(또는 인센티브 제도) 운용	15	39.47	15	39.47	13.33	35.09
		위반자 제재 및 처벌	14	36.84	15.25	40.13	13.50	35.53

상위 개념	하위 개념	세부 지표	PIA		CMMI		PCM2	
			산출 점수	백분율 (%)	산출 점수	백분율 (%)	산출 점수	백분율 (%)
	개 인 의 역 량 과 윤리의식	개인정보보호에 대한 도덕성과 자기통제	30.5	80.26	33.75	88.82	30.33	79.82
		개인정보 처리 업무의 사명감	25	65.79	27.5	72.37	26.17	68.87
		개인정보보호 법률 및 제도 이해력과 행동	30.5	80.26	33.25	87.50	30.00	78.94
		개인정보보호 교육 이수 및 자기 계발	28.5	75.00	31.25	82.24	28.50	75.00
		개인정보보호에 대한 자기 효능감	27.5	72.37	30.25	79.61	28.17	74.13
		개인정보보호 기술 능력과 활용도	23.5	61.84	28	73.68	25.00	65.80
		피해 인지력과 문제해결 능력	23.5	61.84	27	71.05	24.34	64.04

가. PIA-CMMI-PCM2 측정 결과 비교

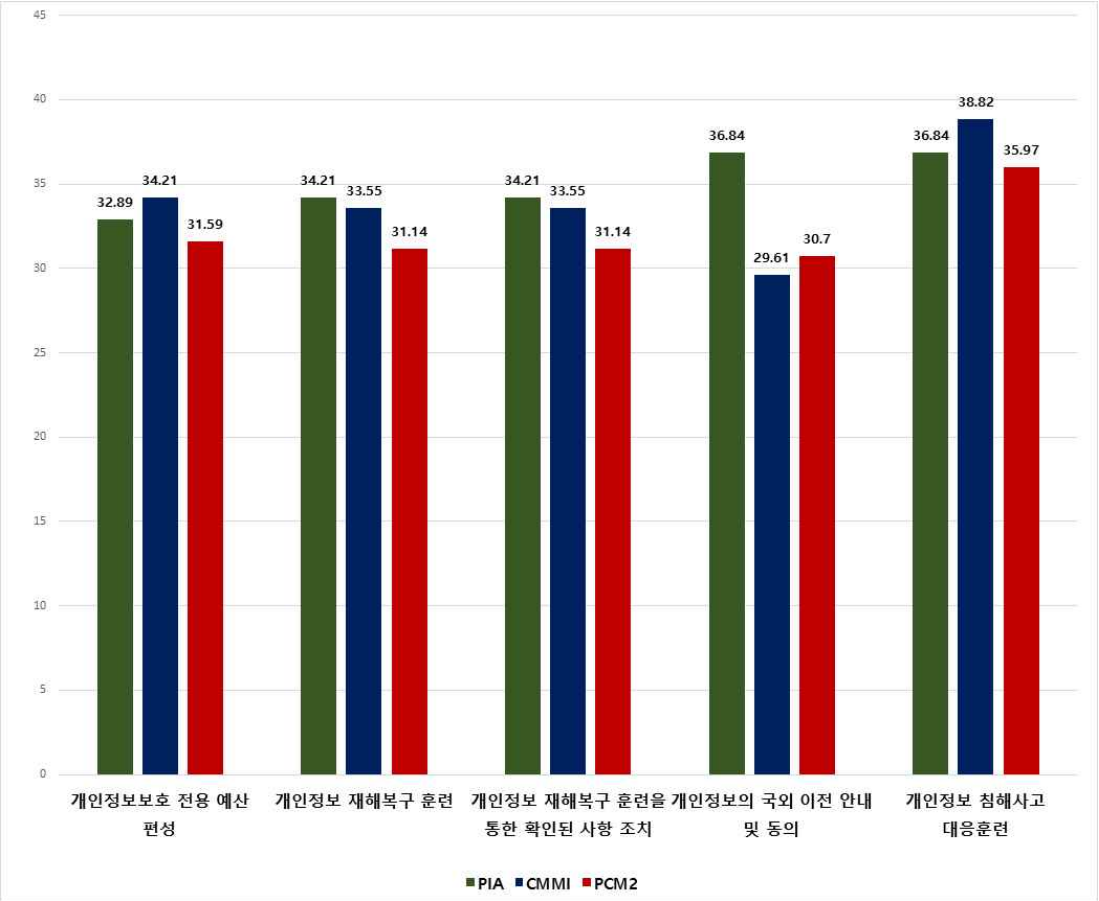
1) PIA-CMMI-PCM2 모델의 평가지표별 성숙도 순위 비교

성숙도가 가장 높은 지표는 [그림 Ⅳ-1]과 같이 개인정보 자료 보관실의 잠금장치 및 출입 통제, 개인정보 저장 장비의 잠금장치 및 출입 통제, 개인정보 파기 기간 준수, 개인정보 파일 파기 절차 준수, 개인정보 파기 방법 적절성 역량이 PIA 모델(94.74%)과 CMMI 모델(97.37%), PCM2 모델(81.99%) 모두 높게 나타났다.



[그림 Ⅳ-1] PIA-CMMI-PCM2 모델의 성숙도 상위 순위 결과

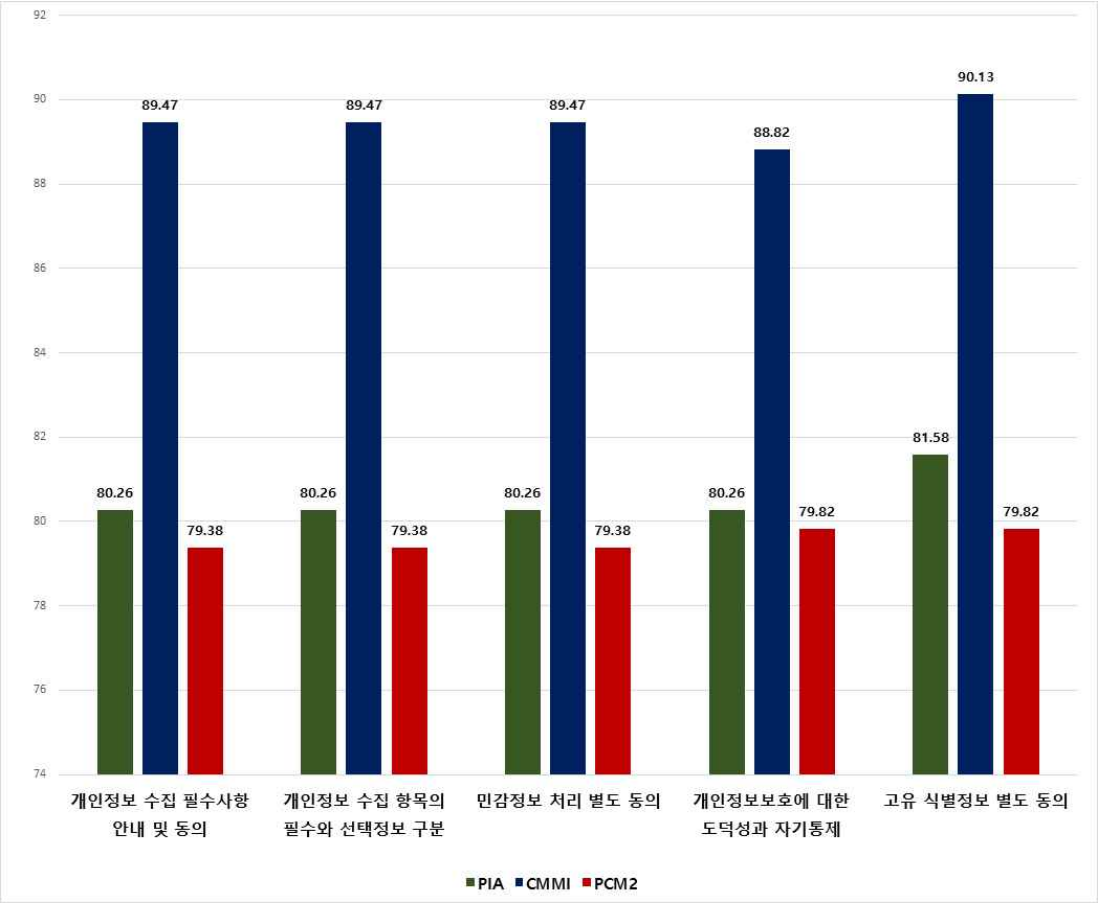
평가지표 중 개인정보보호 전용 예산 편성(PIA 32.89%, CMMI 34.21%, PCM2 31.59%), 개인정보 재해복구 훈련(PIA 34.21%, CMMI 33.55%, PCM2 31.14%), 개인정보 재해복구 훈련을 통한 확인된 사항 조치(PIA 34.21%, CMMI 33.55%, PCM2 31.14%), 개인정보의 국외 이전 안내 및 동의(PIA 36.84%, CMMI 29.61%, PCM2 30.7%), 개인정보 침해사고 대응훈련(PIA 36.84%, CMMI 38.82%, PCM2 35.97%)이 성숙도가 낮은 것으로 나타났으며, 결과는 [그림 Ⅳ-2]와 같다.



[그림 Ⅳ-2] PIA-CMMI-PCM2 모델의 성숙도 하위 순위 결과

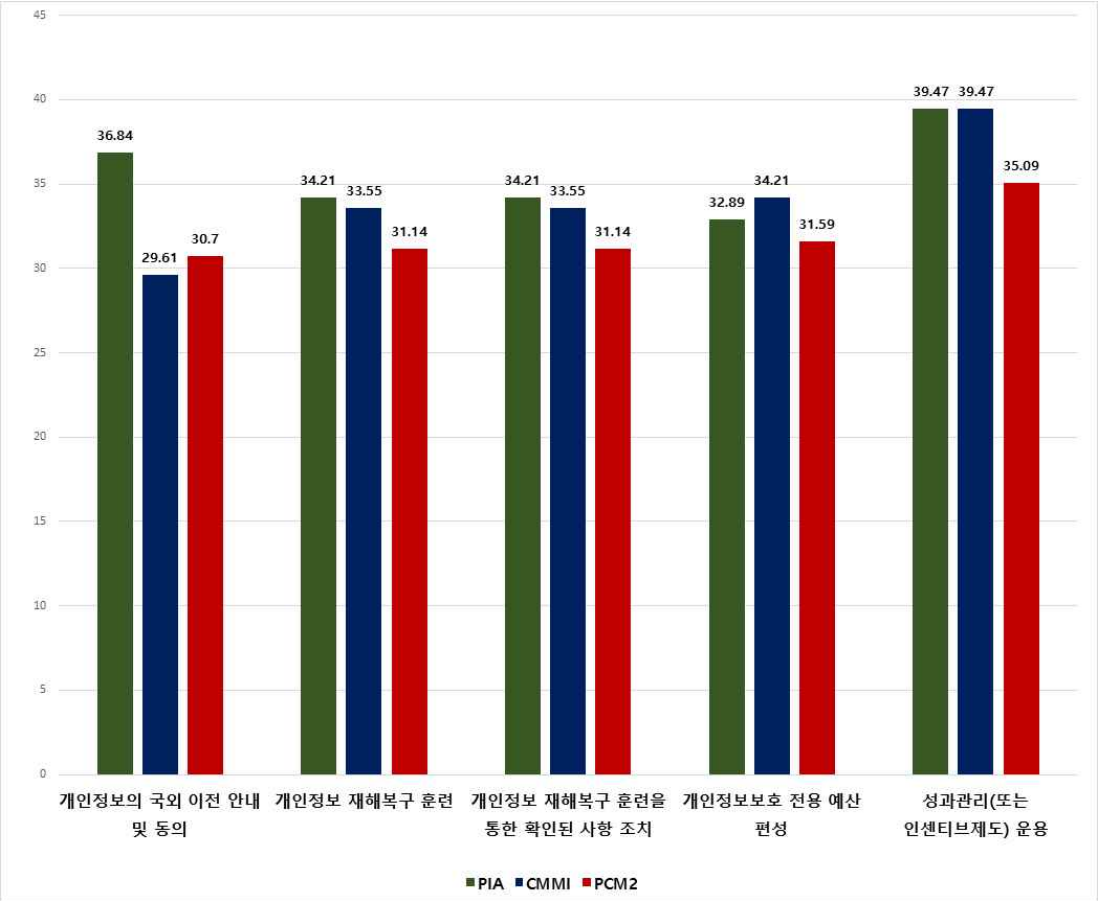
2) PIA-CMMI-PCM2 모델 간 편차 비교

PIA 모델과 CMMI 모델, PCM2 모델 간의 성숙도 편차가 가장 큰 지표는 [그림 Ⅳ-3]과 같으며, 개인정보 수집 필수사항 안내 및 동의(PIA 80.26%, CMMI 89.47%, PCM2 79.38%), 개인정보 수집 항목의 필수와 선택정보 구분(PIA 80.26%, CMMI 89.47%, PCM2 79.38%), 민감정보 처리 별도 동의(PIA 80.26%, CMMI 89.47%, PCM2 79.38%), 개인정보보호에 대한 도덕성과 자기통제(PIA 80.26%, CMMI 88.82%, PCM2 79.82%), 고유 식별정보 별도 동의(PIA 81.58%, CMMI 90.13%, PCM2 79.82%)로 실무자 인식의 편차가 가장 큰 것으로 나타났다.



[그림 Ⅳ-3] PIA-CMMI-PCM2 모델 성숙도 편차 비교(큰 순)

실무자 인식의 편차가 가장 작은 지표는 [그림 Ⅳ-4]와 같으며, 개인정보의 국외 이전 안내 및 동의(PIA 36.84%, CMMI 29.61%, PCM2 30.7%), 개인정보 재해복구 훈련(PIA 34.21%, CMMI 33.55%, PCM2 31.14%), 개인정보 재해복구 훈련을 통해 확인된 사항 조치(PIA 34.21%, CMMI 33.55%, PCM2 31.14%), 개인정보보호 전용 예산 편성(PIA 32.89%, CMMI 34.21%, PCM2 31.59%), 성과관리(또는 인센티브제도) 운용(PIA 39.47%, CMMI 39.47%, PCM2 35.09%) 순으로 나타났다.



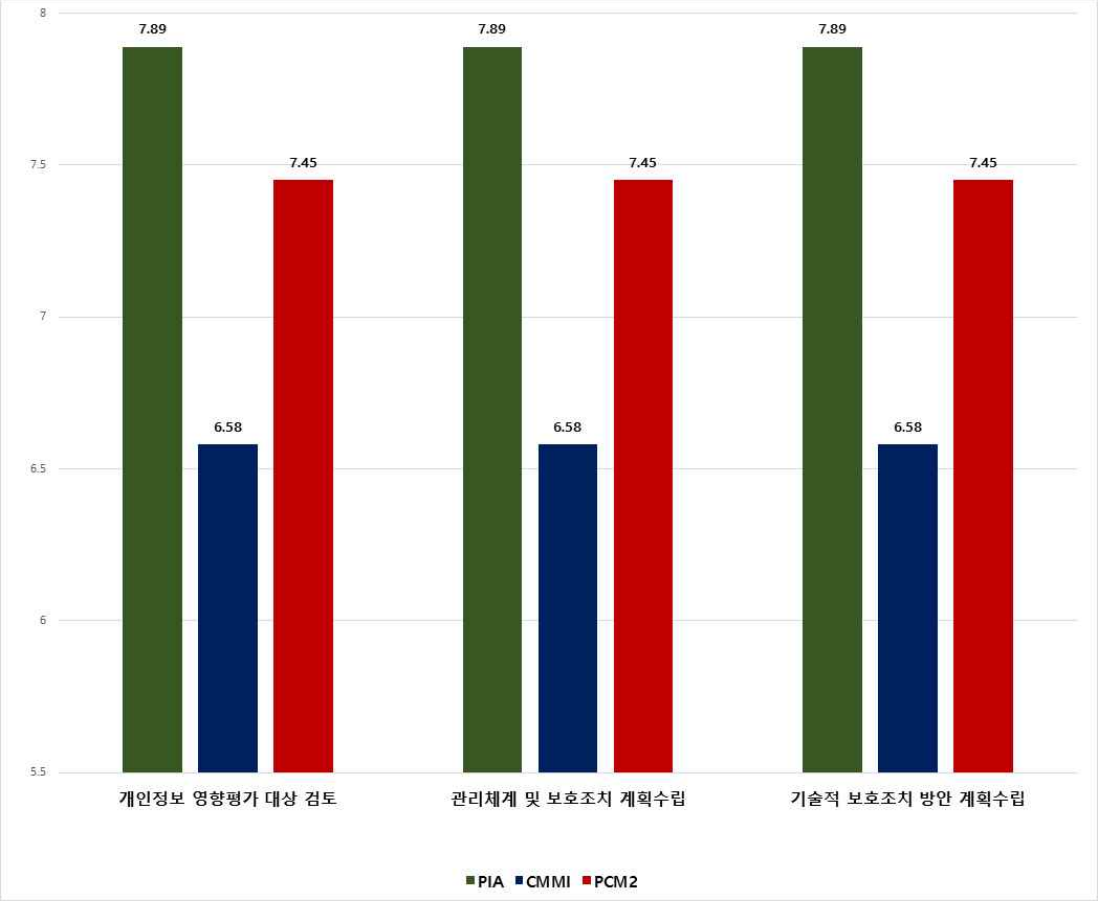
[그림 Ⅳ-4] PIA-CMMI-PCM2 모델 성숙도 편차 비교(작은 순)

나. PIA 모델의 개인정보 영향평가 적용 결과

PIA 모델의 평가지표 중 '개인정보 영향평가' 지표는 <표 Ⅳ-10>과 [그림 Ⅳ-5]와 같이 PIA 7.89%(3), CMMI 6.58%(2.5), PCM2 7.45%(2.832)로 성숙도가 가장 낮은 것으로 나타나, 개인정보 취급자의 평가에 적용하는 것은 다소 무리가 있는 것으로 나타났다.

<표 Ⅳ-10> PIA의 개인정보 영향평가 측정 결과

하위 개념	세부 지표	PIA		CMMI		PCM2	
		산출 점수	백분율 (%)	산출 점수	백분율 (%)	산출 점수	백분율 (%)
개인정보 영향평가	개인정보 영향평가 대상 검토	3	7.89	2.5	6.58	2.832	7.45
	관리체계 및 보호조치 계획 수립	3	7.89	2.5	6.58	2.832	7.45
	기술적 보호조치 방안 계획 수립	3	7.89	2.5	6.58	2.832	7.45



[그림 Ⅳ-5] PIA의 개인정보 영향평가 측정 결과

다. 신규 제안한 평가지표의 진단 결과

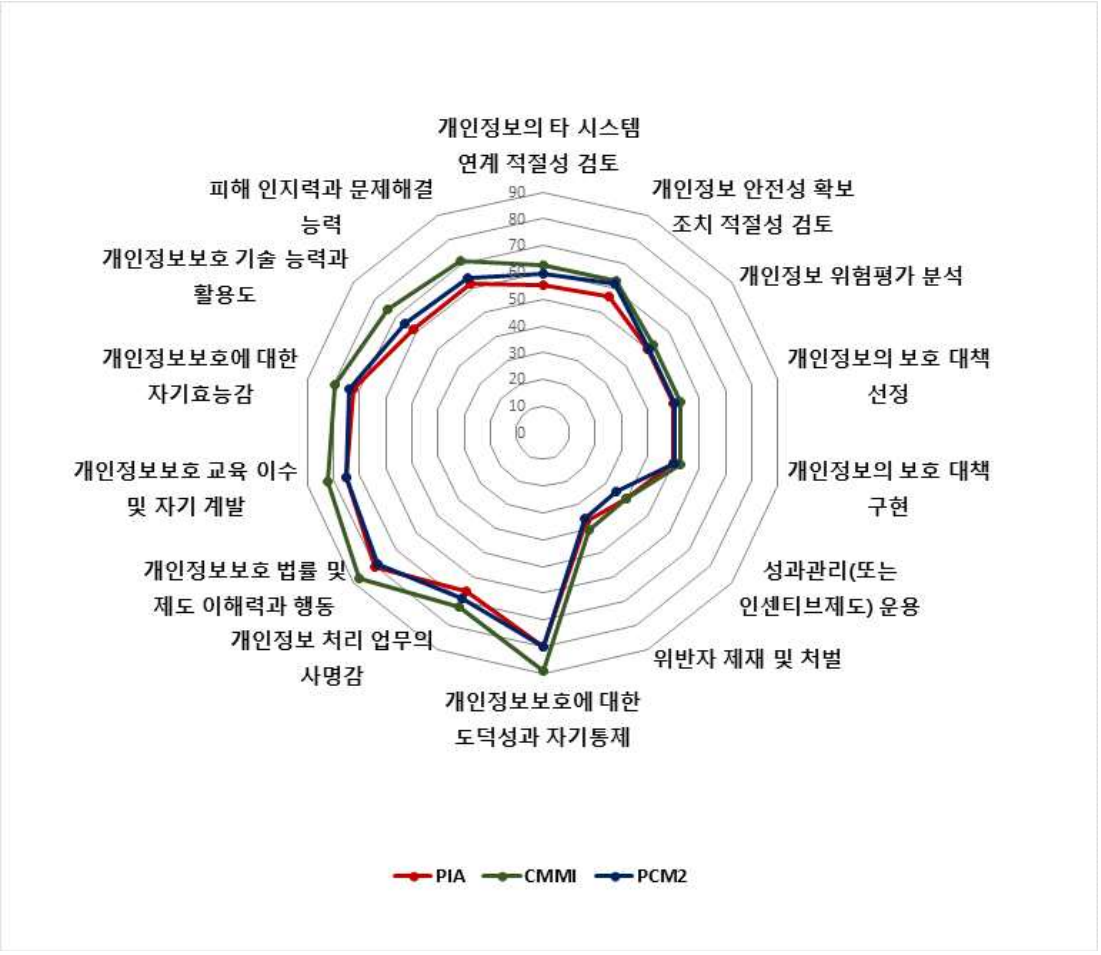
본 연구에서 신규로 제안된 14개의 평가지표를 PIA-CMMI-PCM2 모델에 적용하여 비교 분석한 결과는 <표 Ⅳ-11>과 같다.

<표 Ⅳ-11> 신규 제안한 평가지표의 측정 결과

하위 개념	세부 지표	PIA		CMMI		PCM2	
		산출 점수	백분율 (%)	산출 점수	백분율 (%)	산출 점수	백분율 (%)
개인정보 흐름 분석	개인정보의 타 시스템 연계 적절성 검토	21	55.26	23.75	62.50	22.67	59.65
	개인정보 안전성 확보 조치 적절성 검토	21.5	56.58	24	63.16	23.50	61.85
개인정보 안전성 분석	개인정보 위험평가 분석	19	50.00	20	52.63	19.17	50.44
	개인정보의 보호 대책 선정	19	50.00	20	52.63	19.17	50.44
	개인정보의 보호 대책 구현	19	50.00	20	52.63	19.17	50.44
조직의 역량	성과관리(또는 인센티브제도) 운용	15	39.47	15	39.47	13.33	35.09
	위반자 제재 및 처벌	14	36.84	15.25	40.13	13.50	35.53
개인의 역량과 윤리 의식	개인정보보호에 대한 도덕성과 자기통제	30.5	80.26	33.75	88.82	30.33	79.82
	개인정보 처리 업무의 사명감	25	65.79	27.5	72.37	26.17	68.87
	개인정보보호 법률 및 제도 이해력과 행동	30.5	80.26	33.25	87.50	30.00	78.94
	개인정보보호 교육 이수 및 자기 계발	28.5	75.00	31.25	82.24	28.50	75.00
	개인정보보호에 대한 자기효능감	27.5	72.37	30.25	79.61	28.17	74.13
	개인정보보호 기술 능력과 활용도	23.5	61.84	28	73.68	25.00	65.80
	피해 인지력과 문제해결 능력	23.5	61.84	27	71.05	24.34	64.04

첫 번째, 개인정보 흐름 분석단계에서 '개인정보 안전성 확보 조치 적절성 검토' 지표를 보면, PIA 모델은 55.26%(21), CMMI 모델 62.50%(23.75), PCM2 모델 59.65%(22.67)로 나타났다. '개인정보 안전성 확보 조치 적절성 검토' 지표는 PIA 56.58%(21.5), CMMI 63.16%(24), PCM2 61.85%(23.50)로 나타났다. 두 번째, 개인정보 안전성 분석단계에서는 PIA 지표 중 '개인정보 위험도 및 침해요인 분석' 결과를 바탕으로 한 '개인정보 위험평가 분석', '개인정보의 보호 대책 선정', '개인정보의 보호 대책 구현'은 PIA 50%(19), CMMI 52.63%(20), PCM2 50.44%(19.17)로 분석되었다. 세 번째, 조직의 역량에서 '성과관리(또는 인센티브제도) 운용' 지표는 PIA 39.47%(15), CMMI 39.47%(15), PCM2 35.09%(13.33)로 나타났고, '위반자 제재 및 처

벌’ 지표는 PIA 36.84%(14), CMMI 40.13%(15.25), PCM2 35.53%(13.50)로 나타났다. 네 번째, 개인의 역량과 윤리의식에서 ‘개인정보보호에 대한 도덕성과 자기통제’(PIA 80.26%, CMMI 88.82%, PCM2 79.82%), ‘개인정보 처리 업무의 사명감’(PIA 65.79%, CMMI 72.37%, PCM2 68.87%), ‘개인정보보호 법률 및 제도 이해력과 행동’(PIA 80.26%, CMMI 87.5%, PCM2 78.94%), ‘개인정보보호 교육 이수 및 자기 계발’(PIA 75%, CMMI 82.24%, PCM2 75%), ‘개인정보보호에 대한 자기효능감’(PIA 72.37%, CMMI 79.61%, PCM2 74.13%), ‘개인정보보호 기술 능력과 활용도’(PIA 61.84%, CMMI 73.68%, PCM2 65.80%), ‘피해 인지력과 문제해결 능력’(PIA 61.84%, CMMI 71.05%, PCM2 64.04%)으로 [그림 Ⅳ-6]과 같이 PIA 모델과 CMMI 모델, PCM2 모델 모두 근소한 편차를 보이는 것으로 나타나, 신규 개발된 평가지표가 PIA, CMMI, PCM2 모델 모두 적합하다고 판단된다.



[그림 Ⅳ-6] 신규 개발 지표 측정 결과(PIA-CMMI-PCM2 비교)

4.2.3 개인정보 관리역량 자가 진단 분석 결과

본 연구에서는 개인정보 취급자의 관리역량을 진단해 볼 수 있는 모델과 평가지표 개발에서만 그치지 않고, 실제로 진단을 통해 개인정보 관리역량이 어느 정도인지 알아보기 위하여 앞장에서 도출한 개인정보 관리역량성숙도 진단항목의 가중치를 반영하여 설계한 관리역량성숙도 자가 진단 테스트를 통해, 개인정보 취급자의 관리역량을 진단하였다.

분석 방법은 지방자치단체, 공공기관, 민간기업 등 세 집단 간 평균의 차이 검증을 위한 일원 배치 분산분석(One-way ANOVA)과 AHP 가중치 환산점수를 적용한 성숙도 수준 비교 분석하였다.

가. 집단 간 평균의 유의성 차이 검증

개인정보 관리역량과 하위개념에 대한 지방자치단체, 공공기관, 민간기업 등 세 집단 간 평균이 유의한 차이를 보이는지 검증하고자 일원 배치 분산분석(One-way ANOVA)을 실시하였다.

1) 개인정보 관리역량에 대한 세 집단 간 평균 비교

개인정보 관리역량에 대한 지방자치단체, 공공기관, 민간기업 등 세 집단 간 평균이 유의한 차이를 보이는지 검증한 결과는 <표 Ⅳ-12>와 같다. 그 결과 개인정보 관리역량(F=16.850, p<.001)은 유의한 차이를 보이는 것으로 나타났다.

유의한 차이를 보이는 변수에 대해서는 Duncan과 Scheffe의 사후분석(Duncan & Scheffe's post-hoc analysis)을 실시한 결과, 개인정보 관리역량은 민간기업 대비 지방자치단체와 공공기관이 더 높은 것으로 나타났다.

<표 Ⅳ-12> 개인정보 관리역량에 대한 집단 간 평균 비교 결과

종속 변수	집단	표본수	평균	표준 편차	F	p	Scheffe
개인정보 관리 역량	민간기업(a)	14	3.31	0.54	16.850***	.000	a<b,c
	공공기관(b)	12	5.28	0.77			
	지방자치단체(c)	12	5.24	0.75			

***p<.001

2) 하위개념에 대한 세 집단 간 평균 비교

하위개념에 대한 지방자치단체, 공공기관, 민간기업 등 세 집단 간 평균이 유의한 차이를 보이는지 검증한 결과는 <표 Ⅳ-13>과 같다.

<표 Ⅳ-13> 하위개념에 대한 집단 간 평균 비교 결과

종속변수	집단	표본수	평균	표준편차	*F*	*p*	Scheffe
업무처리 흐름 분석	민간기업(a)	14	3.07	1.64	8.902**	.001	a<b,c
	공공기관(b)	12	5.50	1.52			
	지방자치단체(c)	12	5.38	1.84			
개인정보 흐름 분석	민간기업(a)	14	3.84	1.20	9.754***	.000	a<b,c
	공공기관(b)	12	5.84	1.30			
	지방자치단체(c)	12	5.44	1.20			
개인정보 안전성 분석	민간기업(a)	14	2.93	1.49	9.452**	.001	a<b,c
	공공기관(b)	12	4.96	1.35			
	지방자치단체(c)	12	4.50	0.76			
관리체계 수립	민간기업(a)	14	3.21	1.75	7.993**	.001	a<b,c
	공공기관(b)	12	5.56	1.34			
	지방자치단체(c)	12	5.17	1.70			
수집	민간기업(a)	14	4.41	0.60	18.542***	.000	a<b,c
	공공기관(b)	12	5.78	0.66			
	지방자치단체(c)	12	5.65	0.65			
이용 및 제공	민간기업(a)	14	1.78	0.78	32.795***	.000	a<b,c
	공공기관(b)	12	5.49	1.57			
	지방자치단체(c)	12	4.90	1.39			
보관 및 파기	민간기업(a)	14	5.68	0.45	5.396**	.009	a<b,c
	공공기관(b)	12	6.07	0.30			
	지방자치단체(c)	12	5.99	0.05			
내부 관리계획	민간기업(a)	14	1.14	0.36	41.006***	.000	a<b,c
	공공기관(b)	12	4.75	1.60			
	지방자치단체(c)	12	5.75	1.82			
접근관리	민간기업(a)	14	4.21	0.43	24.351***	.000	a<b,c
	공공기관(b)	12	5.75	0.62			
	지방자치단체(c)	12	5.58	0.79			
접근통제	민간기업(a)	14	4.70	0.40	17.731***	.000	a<b,c
	공공기관(b)	12	5.79	0.57			
	지방자치단체(c)	12	5.77	0.64			
접속기록 관리	민간기업(a)	14	3.70	0.46	16.804***	.000	a<b,c
	공공기관(b)	12	5.29	0.96			
	지방자치단체(c)	12	5.00	0.79			
개인정보의 암호화	민간기업(a)	14	5.11	0.40	18.552***	.000	a<c<b
	공공기관(b)	12	6.04	0.33			
	지방자치단체(c)	12	5.63	0.43			
관리/기술적 보호	민간기업(a)	14	2.59	0.60	34.925***	.000	a<b,c
	공공기관(b)	12	5.09	1.06			
	지방자치단체(c)	12	4.89	0.88			

종속 변수	집단	표본수	평균	표준 편차	*F*	*p*	Scheffe
대응훈련 능력	민간기업(a)	14	1.18	0.46	44.437***	.000	a<b,c
	공공기관(b)	12	4.02	1.07			
	지방자치단체(c)	12	4.15	1.13			
정보 주체의 권리보장	민간기업(a)	14	4.19	0.36	33.877***	.000	a<b<c
	공공기관(b)	12	5.05	0.44			
	지방자치단체(c)	12	5.58	0.51			
조직의 역량	민간기업(a)	14	2.19	0.44	46.655***	.000	a<b,c
	공공기관(b)	12	4.54	0.78			
	지방자치단체(c)	12	5.07	1.13			
개인의 역량 및 윤리의식	민간기업(a)	14	4.62	0.49	18.698***	.000	a<b,c
	공공기관(b)	12	5.70	0.67			
	지방자치단체(c)	12	5.82	0.50			

*p<.05, **p<.01, ***p<.001

업무처리 흐름 분석(F=8.902, p<.01), 개인정보 흐름 분석(F=9.754, p<.001), 개인정보 안전성 분석(F=9.452, p<.01), 관리체계 수립(F=7.993, p<.01), 수집(F=18.542, p<.001), 이용 및 제공(F=32.795, p<.001), 보관 및 파기(F=5.396, p<.01), 내부 관리계획(F=41.006, p<.001), 접근관리(F=24.351, p<.001), 접근통제(F=17.731, p<.001), 접속기록 관리(F=16.804, p<.001), 개인정보의 암호화(F=18.552, p<.001), 관리/기술적 보호(F=34.925, p<.001), 대응훈련 능력(F=44.437, p<.001), 정보 주체의 권리보장(F=33.877, p<.001), 조직의 역량(F=46.655, p<.001), 개인의 역량과 윤리의식(F=18.698, p<.001) 모두에서 유의한 차이를 보이는 것으로 나타났다.

유의한 차이를 보이는 변수에 대해서는 Duncan과 Scheffe의 사후분석(Duncan & Scheffe's post-hoc analysis)을 실시한 결과, 업무처리 흐름 분석, 개인정보 흐름 분석, 개인정보 안전성 분석, 관리체계 수립, 수집, 이용 및 제공, 보관 및 파기, 내부 관리계획, 접근관리, 접근통제, 관리/기술적 보호, 대응훈련 능력, 조직의 역량, 개인의 역량과 윤리의식은 민간기업 대비 지방자치단체와 공공기관이 더 높은 것으로 나타났다. 개인의 암호화는 민간기업 대비 지방자치단체가, 지방자치단체 대비 공공기관이 더 높은 것으로 나타났고, 정보 주체의 권리보장은 민간기업 대비 공공기관이, 공공기관 대비 지방자치단체가 더 높은 것으로 나타났다.

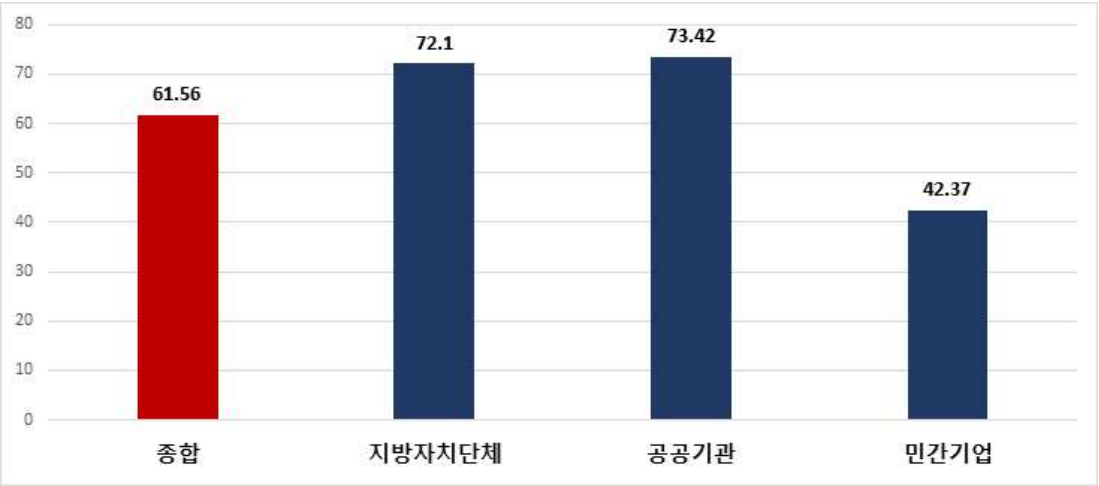
나. 가중치별 성숙도 자가 진단 검증

앞장에서 도출한 개인정보 관리역량성숙도 진단항목의 가중치를 반영하여 설계한 관리역량성숙도 자가 진단 테스트를 통해, 개인정보 취급자의 관리역량을 진단한 결과는 <표 Ⅳ-14>와 같다.

<표 Ⅳ-14> 전체-공공-민간 성숙도 수준 결과

구분	환산점수	백분율(%)	성숙도 수준(PCM2)
종합	0.693	61.56	M
지방자치단체	0.816	72.10	VM
공공기관	0.840	73.42	VM
민간기업	0.461	42.37	M

[그림 Ⅳ-7]과 같이 개인정보 관리역량성숙도의 자가 진단 테스트 참여자 82명의 평균은 61.56%(0.693)로 'M'의 성숙도 수준으로 보였으며, 지방자치단체는 72.10%(0.816)로 성숙도 수준은 'VM', 공공기관은 73.42%(0.840)로 성숙도 수준은 'VM', 민간기업은 42.37%(0.461)로 성숙도 수준이 'M'으로 나타났다. 공공기관이 개인정보 관리역량 수준이 가장 높은 것으로 나타났고, 지방자치단체, 민간기업 순으로 나타났다.



[그림 Ⅳ-7] 전체-지방자치단체-공공기관-민간기업 성숙도 수준 결과

1) 평가지표의 가중치별 성숙도 수준

<표 Ⅳ-15>는 세부 지표별 개인정보 관리역량성숙도 진단항목의 가중치를 반영하여 설계한 관리역량성숙도 자가 진단 분석한 결과이다. 가장 높은 성숙도의 등급은 'VM'으로 '개인정보 저장 장비의 잠금장치 및 출입 통제'(81.99%, 0.819), '개인정보 파일 파기 절차 준수'(81.99%, 0.788), '개인정보 파기 기간 준수'(81.99%, 0.741), '개인정보 파기 방법 적절성'(81.99%, 0.629), '개인정보 자료 보관실의 잠금장치 및 출입 통제'(81.99%, 0.407) 지표로 나타났다. 한편, '개인정보의 국외 이전 안내 및 동의'(30.7%, 0.153), '개인정보 재해복구 훈련'(31.14%, 0.246), '개인정보 재해복구 훈련을 통한 확인된 사항 조치'(31.14%, 0.133) 지표는 다른 지표보다 낮은 것으로 나타나, 조직에서는 구성원을 대상으로 한 재해복구 훈련을 통한 역량 수준 향상방안이 뒤따라야 할 것이며, 개인은 본인의 개인정보의 안전한 보관 및 백업 복구에 대한 지식을 높일 수 있도록 할 필요가 있다.

<표 Ⅳ-15> 개인정보 관리역량성숙도 자가 진단 결과(최종)

하위 개념	세부 지표	환산 점수	측정 결과 (총괄)		
			환산 점수	백분율 (%)	성숙도 단계
업무처리 흐름 분석	개인정보 처리 업무처리 흐름도·흐름표 작성	0.728	0.441	60.53	M
	업무처리 흐름도·흐름표 개정관리	0.364	0.212	58.34	M
개인정보 흐름 분석	개인정보 수집, 이용, 보유기간 적절성 검토	0.754	0.562	74.57	VM
	주민등록번호, 민감정보, 고유 식별정보 처리 적절성 검토	1.004	0.749	74.57	VM
	개인정보 수집 항목 구분 적절성 검토	0.41	0.306	74.57	VM
	만 14세 미만의 아동 정보수집 적절성 검토	0.435	0.321	73.69	VM
	제3자 제공, 위·수탁 적절성 검토	0.216	0.128	59.21	M
	개인정보의 타 시스템 연계 적절성 검토	0.233	0.139	59.65	M
	개인정보 안전성 확보 조치 적절성 검토	0.361	0.223	61.85	M
	개인정보 처리 흐름도 작성 및 이력 관리	1.402	0.830	59.22	M
	개인정보 처리 흐름표 작성 및 이력 관리	1.31	0.776	59.22	M

하위 개념	세부 지표	환산 점수	측정 결과 (총괄)		
			환산 점수	백분율 (%)	성숙도 단계
개인 정보 안전성 분석	개인정보 처리 위험도 및 침해요인 분석	4.096	2.174	53.07	M
	개인정보 위험평가 분석	2.553	1.288	50.44	M
	개인정보의 보호 대책 선정	0.87	0.439	50.44	M
	개인정보의 보호 대책 구현	0.771	0.389	50.44	M
관리 체계 수립	개인정보보호 정책 수립 적절성 검토	0.304	0.181	59.66	M
	법적 요구사항 준수 적절성 검토	0.998	0.595	59.66	M
	관리체계 점검 및 개선 계획 수립 적절성 검토	1.099	0.651	59.22	M
수집	개인정보 수집 필수사항 안내 및 동의	2.46	1.953	79.38	VM
	목적별 최소한의 필수정보 수집	1.68	1.326	78.94	VM
	개인정보 수집 항목의 필수와 선택정보 구분	0.997	0.791	79.38	VM
	민감정보 처리 별도 동의	0.769	0.610	79.38	VM
	고유 식별정보 별도 동의	1.322	1.055	79.82	VM
	만 14세 미만의 아동의 정보수집 시 법정 대리인 동의	0.716	0.556	77.63	VM
	주민등록번호 수집 제한 법적 준수	1.832	1.446	78.94	VM
	선택정보 동의 거부 시 서비스 제공	0.564	0.287	50.88	M
	개인정보의 국외 이전 안내 및 동의	0.499	0.153	30.7	L
이용 및 제공	개인정보 처리 위탁 계약서 작성 및 체결	3.585	1.808	50.44	M
	위탁업무의 정보 공개	1.96	0.868	44.3	M
	수탁자 대상 교육 및 관리 감독	2.593	1.194	46.06	M
	목적 내 제3자 이용·제공 시 필수사항 고지 및 동의	0.695	0.366	52.63	M
	목적 외 제3자 이용·제공 시 필수사항 고지 및 동의	0.744	0.392	52.63	M
	목적 외 제3자 이용·제공 사항 공고	1.364	0.652	47.8	M
	개인정보 이용 및 제3자 제공 대장 기록 관리	1.49	0.725	48.67	M

하위 개념	세부 지표	환산 점수	측정 결과 (총괄)		
			환산 점수	백분율 (%)	성숙도 단계
보관 및 파기	개인정보 자료 보관실의 잠금장치 및 출입 통제	0.497	0.407	81.99	VM
	개인정보 저장 장비의 잠금장치 및 출입 통제	0.999	0.819	81.99	VM
	개인정보 파기 기간 준수	0.904	0.741	81.99	VM
	개인정보 파일 파기 절차 준수	0.961	0.788	81.99	VM
	개인정보 파기 방법 적절성	0.767	0.629	81.99	VM
	개인정보 파일 파기 관리대장 기록 관리	0.61	0.487	79.81	VM
내부 관리 계획	내부 관리계획 수립 및 이력 관리	6.621	3.020	45.61	M
	내부 관리계획 이행점검 및 개선	3.305	1.507	45.61	M
접근 관리	접근권한 절차 수립 및 이력 관리	6.482	4.464	68.86	VM
	접근권한 차등 부여	5.129	3.532	68.86	VM
	접근권한 변경내역 기록 및 관리	4.079	2.809	68.86	VM
접근 통제	안전한 비밀번호 작성 규칙 적용	1.611	1.166	72.38	VM
	계정 오류 입력 접근제한 설정	1.172	0.812	69.31	VM
	부재 시 시스템 접속 차단 설정	1.324	0.999	75.44	VM
	비업무용 사이트 접속 차단 설정	1.172	0.853	72.8	VM
	비인가자 접근 차단	0.909	0.686	75.44	VM
	안전한 접속(또는 인증) 수단 적용	1.085	0.771	71.06	VM
	관리용 단말기 접근통제	0.694	0.521	75	VM
접속 기록 관리	개인정보 취급자의 접속기록 보관 기간 설정	1.748	1.073	61.4	M
	접속기록 필수정보 적용	1.256	0.777	61.83	M
	접속기록의 안전한 보관	1.062	0.647	60.96	M
	접속기록 점검 관리	2.003	1.133	56.58	M
개인 정보의 암호화	개인정보의 암호화	3.073	2.412	78.5	VM
	비밀번호의 암호화	1.54	1.135	73.68	VM

하위 개념	세부 지표	환산 점수	측정 결과 (총괄)		
			환산 점수	백분율 (%)	성숙도 단계
관리/ 기술적 보호	개인정보 관리 정책의 점검 및 검토	0.295	0.190	64.48	M
	개인정보 관리 정책의 개선	0.264	0.169	64.04	M
	개인정보 관리 점검 및 검토	0.138	0.090	64.91	M
	개인정보 관리 점검결과 확인된 사항 조치	0.148	0.095	64.47	M
	보안취약점 점검 및 위험평가 검토	0.154	0.059	38.17	M
	보안취약점 개선 조치	0.135	0.052	38.17	M
	개인정보 노출 여부 모니터링 및 검토	0.191	0.076	39.92	M
	개인정보 노출 모니터링 결과 확인된 사항 조치	0.104	0.042	39.92	M
대응 훈련 능력	개인정보 침해사고 대응훈련	1.475	0.531	35.97	M
	개인정보 침해사고 대응훈련 통한 확인된 사항 조치	1.582	0.562	35.53	M
	개인정보 재해복구 훈련	0.791	0.246	31.14	L
	개인정보 재해복구 훈련을 통한 확인된 사항 조치	0.428	0.133	31.14	L
정보 주체의 권리 보장	정보 주체 중심의 개인정보 처리 방침 공개	0.348	0.224	64.48	M
	정보 주체 중심의 개인정보 수집 이용 동의서 제공	0.302	0.195	64.48	M
	개인정보의 열람·정정·삭제·처리정지의 처리	0.2	0.129	64.48	M
	법적 대리인의 동의권 보장	0.23	0.152	66.24	VM
	개인정보 유출 신고 안내	0.263	0.172	65.35	VM
조직의 역량	조직의 개인정보보호 관련 규정 준수	0.248	0.164	66.22	VM
	조직의 개인정보 침해사고 지침 준수	0.155	0.091	58.77	M
	개인정보보호 전담 조직 및 인력 구성	0.215	0.077	35.97	M
	개인정보보호 전용 예산 편성	0.161	0.051	31.59	L
	개인정보보호 교육과정 운영 및 평가	0.082	0.056	68.41	VM
	성과관리(또는 인센티브제도) 운용	0.113	0.040	35.09	M
	위반자 제재 및 처벌	0.097	0.034	35.53	M
개인의 역량과 윤리 의식	개인정보보호에 대한 도덕성과 자기통제	0.385	0.307	79.82	VM
	개인정보 처리 업무의 사명감	0.283	0.195	68.87	VM
	개인정보보호 법률 및 제도 이해력과 행동	0.325	0.257	78.94	VM
	개인정보보호 교육 이수 및 자기 계발	0.234	0.176	75	VM
	개인정보보호에 대한 자기효능감	0.151	0.112	74.13	VM
	개인정보보호 기술 능력과 활용도	0.185	0.122	65.8	VM
	피해 인지력과 문제해결 능력	0.137	0.088	64.04	M

2) 평가지표의 가중치별 집단 간 성숙도 수준 비교

AHP 가중치에 의한 환산점수를 적용한 개인정보 관리역량 진단점수의 기관 유형별 차이 여부에 대한 검증을 한 결과는 <표 Ⅳ-16>과 같다.

<표 Ⅳ-16> 지방자치단체-공공기관-민간기업의 성숙도 자가 진단 결과 비교

하위 개념	세부 지표	환산 점수	역량성숙도 측정 결과								
			지방자치단체			공공기관			민간기업		
			환산 점수	백분율 (%)	성숙도 수 준	환산 점수	백분율 (%)	성숙도 수 준	환산 점수	백분율 (%)	성숙도 수 준
업무 처리 흐름 분석	개인정보 처리 업무처리 흐름도·흐름표 작성	0.728	0.546	75.01	VM	0.556	76.4	VM	0.251	34.53	L
	업무처리 흐름도·흐름표 개정 관리	0.364	0.258	70.85	VM	0.268	73.63	VM	0.126	34.53	L
개인 정보 흐름 분석	개인정보 수집, 이용, 보유기간 적절성 검토	0.754	0.607	80.56	VM	0.649	86.12	H	0.449	59.53	M
	주민등록번호, 민감정보, 고유식별정보 처리 적절성 검토	1.004	0.809	80.56	VM	0.865	86.12	H	0.598	59.53	M
	개인정보 수집 항목 구분 적절성 검토	0.41	0.330	80.56	VM	0.353	86.12	H	0.244	59.53	M
	만 14세 미만의 아동 정보수집 적절성 검토	0.435	0.344	79.18	VM	0.369	84.73	VM	0.259	59.53	M
	제3자 제공, 위수탁 적절성 검토	0.216	0.156	72.23	VM	0.171	79.18	VM	0.067	30.95	L
	개인정보의 타 시스템 연계 적절성 검토	0.233	0.155	66.68	VM	0.175	75	VM	0.094	40.48	M
	개인정보 안전성 확보 조치 적절성 검토	0.361	0.261	72.23	VM	0.276	76.39	VM	0.146	40.49	M
	개인정보 처리 흐름도 작성 및 이력 관리	1.402	0.935	66.67	VM	1.071	76.39	VM	0.534	38.11	M
	개인정보 처리 흐름표 작성 및 이력 관리	1.31	0.873	66.67	VM	1.001	76.39	VM	0.499	38.11	M

하위 개념	세부 지표	환산 점수	역량성숙도 측정 결과								
			지방자치단체			공공기관			민간기업		
			환산 점수	백분율 (%)	성숙도 수 준	환산 점수	백분율 (%)	성숙도 수 준	환산 점수	백분율 (%)	성숙도 수 준
개인정보 안전성 분석	개인정보 처리 위험도 및 침해요인 분석	4.096	2.561	62.52	M	2.787	68.05	VM	1.316	32.14	L
	개인정보 위험 평가 분석	2.553	1.454	56.96	M	1.666	65.27	VM	0.821	32.14	L
	개인정보의 보호 대책 선정	0.87	0.496	56.96	M	0.568	65.27	VM	0.280	32.14	L
	개인정보의 보호 대책 구현	0.771	0.439	56.96	M	0.503	65.27	VM	0.248	32.14	L
관리체계 수립	개인정보보호 정책 수립 적절성 검토	0.304	0.211	69.46	VM	0.228	75	VM	0.116	38.11	M
	법적 요구사항 준수 적절성 검토	0.998	0.693	69.46	VM	0.749	75	VM	0.380	38.11	M
	관리체계 점검 및 개선 계획 수립 적절성 검토	1.099	0.763	69.46	VM	0.855	77.78	VM	0.379	34.53	L
수집	개인정보 수집 필수사항 안내 및 동의	2.46	2.050	83.33	VM	2.152	87.48	H	1.699	69.06	VM
	목적별 최소한의 필수정보 수집	1.68	1.400	83.33	VM	1.470	87.48	H	1.140	67.87	VM
	개인정보 수집 항목의 필수와 선택정보 구분	0.997	0.831	83.33	VM	0.872	87.48	H	0.689	69.06	VM
	민감정보 처리 별도 동의	0.769	0.641	83.33	VM	0.673	87.48	H	0.531	69.06	VM
	고유 식별정보 별도 동의	1.322	1.102	83.33	VM	1.156	87.48	H	0.929	70.25	VM
	만 14세 미만의 아동의 정보수집 시 법정 대리인 동의	0.716	0.587	81.94	VM	0.616	86.1	H	0.477	66.68	VM
	주민등록번호 수집 제한 법적 준수	1.832	1.527	83.33	VM	1.552	84.7	VM	1.287	70.25	VM
	선택정보 동의 거부 시 서비스 제공	0.564	0.431	76.38	VM	0.353	62.53	M	0.107	19.04	L
	개인정보의 국외 이전 안내 및 동의	0.499	0.194	38.88	M	0.229	45.83	M	0.053	10.71	VL

하위 개념	세부 지표	환산 점수	역량성숙도 측정 결과								
			지방자치단체			공공기관			민간기업		
			환산 점수	백분율 (%)	성숙도 수 준	환산 점수	백분율 (%)	성숙도 수 준	환산 점수	백분율 (%)	성숙도 수 준
이용 및 제공	개인정보 처리 위탁 계약서 작성 및 체결	3.585	2.291	63.9	M	2.738	76.38	VM	0.597	16.66	L
	위탁업무의 정보 공개	1.96	1.252	63.9	M	1.443	73.61	VM	0.047	2.38	N
	수탁자 대상 교육 및 관리 감독	2.593	1.441	55.58	M	1.837	70.83	VM	0.432	16.66	L
	목적 내 제3자 이용·제공 시 필수사항 고지 및 동의	0.695	0.444	63.9	M	0.521	75	VM	0.165	23.79	L
	목적 외 제3자 이용·제공 시 필수사항 고지 및 동의	0.744	0.475	63.9	M	0.558	75	VM	0.177	23.79	L
	목적 외 제3자 이용·제공 사항 공고	1.364	0.985	72.2	VM	1.042	76.38	VM	0.033	2.39	N
	개인정보 이용 및 제3자 제공 대장기록 관리	1.49	1.076	72.2	VM	1.138	76.38	VM	0.071	4.76	N
보관 및 파기	개인정보 자료 보관실의 잠금장치 및 출입 통제	0.497	0.414	83.3	VM	0.421	84.69	VM	0.390	78.56	VM
	개인정보 저장 장비의 잠금장치 및 출입 통제	0.999	0.832	83.3	VM	0.846	84.69	VM	0.785	78.56	VM
	개인정보 파기 기간 준수	0.904	0.753	83.3	VM	0.766	84.69	VM	0.710	78.56	VM
	개인정보 파일 파기 절차 준수	0.961	0.801	83.3	VM	0.814	84.69	VM	0.755	78.56	VM
	개인정보 파기 방법 적절성	0.767	0.639	83.3	VM	0.650	84.69	VM	0.603	78.56	VM
	개인정보 파일 파기 관리대장 기록 관리	0.61	0.500	81.92	VM	0.508	83.31	VM	0.458	75	VM
내부 관리 계획	내부 관리계획 수립 및 이력 관리	6.621	5.241	79.16	VM	4.138	62.5	M	0.158	2.39	N
	내부 관리계획 이행점검 및 개선	3.305	2.616	79.16	VM	2.066	62.5	M	0.079	2.39	N

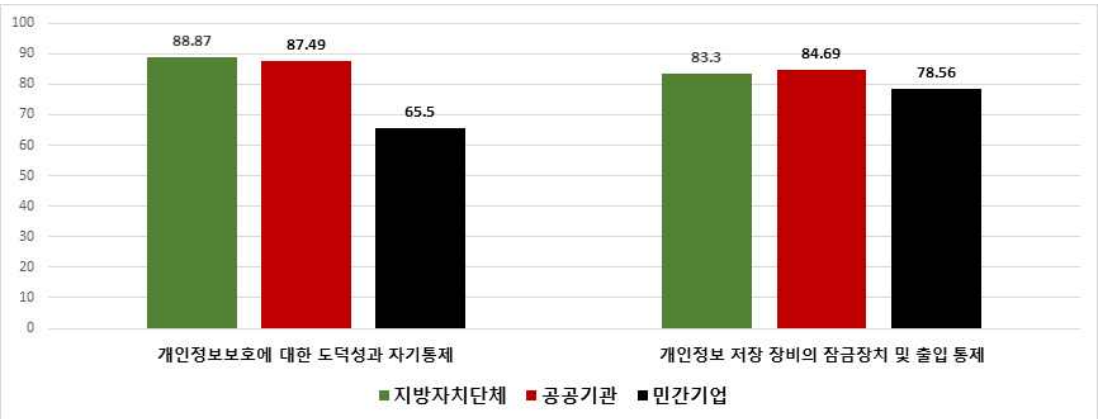
하위 개념	세부 지표	환산 점수	역량성숙도 측정 결과								
			지방자치단체			공공기관			민간기업		
			환산 점수	백분율 (%)	성숙도 수 준	환산 점수	백분율 (%)	성숙도 수 준	환산 점수	백분율 (%)	성숙도 수 준
접근 관리	접근권한 절차 수립 및 이력 관리	6.482	4.952	76.4	VM	5.131	79.16	VM	3.473	53.58	M
	접근권한 차등 부여	5.129	3.919	76.4	VM	4.060	79.16	VM	2.748	53.58	M
	접근권한 변경 내역 기록 및 관리	4.079	3.116	76.4	VM	3.229	79.16	VM	2.186	53.58	M
접근 통제	안전한 비밀번호 작성 규칙 적용	1.611	1.231	76.4	VM	1.275	79.16	VM	1.017	63.12	M
	계정 오류 입력 접근 제한 설정	1.172	0.895	76.4	VM	0.879	75.01	VM	0.684	58.35	M
	부재 시 시스템 접속 차단 설정	1.324	1.103	83.32	VM	1.085	81.93	VM	0.836	63.12	M
	비업무용 사이트 접속 차단 설정	1.172	0.960	81.93	VM	0.944	80.53	VM	0.684	58.35	M
	비인가자 접근 차단	0.909	0.757	83.32	VM	0.745	81.93	VM	0.574	63.12	M
	안전한 접속(또는 인증) 수단 적용	1.085	0.799	73.62	VM	0.844	77.77	VM	0.685	63.12	M
	관리용 단말기 접근통제	0.694	0.569	81.93	VM	0.569	81.93	VM	0.438	63.12	M
접속 기록 관리	개인정보 취급자의 접속기록 보관 기간 설정	1.748	1.214	69.45	VM	1.263	72.23	VM	0.791	45.23	M
	접속기록 필수 정보 적용	1.256	0.872	69.44	VM	0.924	73.6	VM	0.568	45.23	M
	접속기록의 안전한 보관	1.062	0.737	69.44	VM	0.752	70.83	VM	0.480	45.23	M
	접속기록 점검 관리	2.003	1.169	58.34	M	1.391	69.44	VM	0.882	44.04	M
개인정보의 암호화	개인정보의 암호화	3.073	2.390	77.77	VM	2.603	84.69	VM	2.268	73.81	VM
	비밀번호의 암호화	1.54	1.176	76.38	VM	1.283	83.31	VM	0.972	63.11	M

하위 개념	세부 지표	환산 점수	역량성숙도 측정 결과								
			지방자치단체			공공기관			민간기업		
			환산 점수	백분율 (%)	성숙도 수 준	환산 점수	백분율 (%)	성숙도 수 준	환산 점수	백분율 (%)	성숙도 수 준
관리/기술적 보호	개인정보 관리 정책의 점검 및 검토	0.295	0.213	72.23	VM	0.225	76.39	VM	0.140	47.62	M
	개인정보 관리 정책의 개선	0.264	0.187	70.83	VM	0.202	76.39	VM	0.126	47.62	M
	개인정보 관리 점검 및 검토	0.138	0.098	70.83	VM	0.105	76.39	VM	0.069	50	M
	개인정보 관리 점검결과 확인된 사항 조치	0.148	0.105	70.83	VM	0.111	75	VM	0.074	50	M
	보안취약점 점검 및 위험평가 검토	0.154	0.090	58.37	M	0.092	59.73	M	0.004	2.39	N
	보안취약점 개선 조치	0.135	0.079	58.37	M	0.081	59.73	M	0.003	2.39	N
	개인정보 노출 여부 모니터링 및 검토	0.191	0.111	58.37	M	0.117	61.11	M	0.011	5.95	VL
	개인정보 노출 모니터링 결과 확인된 사항 조치	0.104	0.061	58.37	M	0.064	61.11	M	0.006	5.95	VL
대응 훈련 능력	개인정보 침해 사고 대응훈련	1.475	0.779	52.79	M	0.799	54.18	M	0.088	5.95	VL
	개인정보 침해 사고 대응훈련 통한 확인된 사항 조치	1.582	0.857	54.18	M	0.813	51.4	M	0.094	5.95	VL
	개인정보 재해 복구 훈련	0.791	0.407	51.4	M	0.374	47.23	M	0.000	0	N
	개인정보 재해 복구 훈련을 통한 확인된 사항 조치	0.428	0.220	51.4	M	0.202	47.23	M	0.000	0	N

하위 개념	세부 지표	환산 점수	역량성숙도 측정 결과								
			지방자치단체			공공기관			민간기업		
			환산 점수	백분율 (%)	성숙도 수 준	환산 점수	백분율 (%)	성숙도 수 준	환산 점수	백분율 (%)	성숙도 수 준
정보 주체의 권리 보장	정보 주체 중심의 개인정보 처리 방침 공개	0.348	0.266	76.38	VM	0.232	66.69	VM	0.182	52.39	M
	정보 주체 중심의 개인정보 수집 이용동의서 제공	0.302	0.231	76.38	VM	0.201	66.69	VM	0.158	52.39	M
	개인정보의 열람·정정·삭제·처리정지의 처리	0.2	0.153	76.38	VM	0.133	66.69	VM	0.105	52.39	M
	법적 대리인의 동의권 보장	0.23	0.176	76.38	VM	0.153	66.69	VM	0.131	57.16	M
	개인정보 유출 신고 안내	0.263	0.201	76.38	VM	0.186	70.84	VM	0.135	51.19	M
조직의 역량	조직의 개인정보보호 관련 규정 준수	0.248	0.193	77.75	VM	0.179	72.22	VM	0.127	51.2	M
	조직의 개인정보 침해사고 지침 준수	0.155	0.105	68.05	VM	0.114	73.59	VM	0.059	38.11	M
	개인정보보호 전담 조직 및 인력 구성	0.215	0.143	66.67	VM	0.102	47.23	M	0.000	0	N
	개인정보보호 전용 예산 편성	0.161	0.089	55.58	M	0.072	44.45	M	0.000	0	N
	개인정보보호 교육과정 운영 및 평가	0.082	0.066	80.53	VM	0.064	77.77	VM	0.041	50	M
	성과관리(또는 인센티브제도) 운용	0.113	0.074	65.28	VM	0.052	45.84	M	0.000	0	N
	위반자 제재 및 처벌	0.097	0.059	61.12	M	0.050	51.41	M	0.000	0	N

하위 개념	세부 지표	환산 점수	역량성숙도 측정 결과								
			지방자치단체			공공기관			민간기업		
			환산 점수	백분율 (%)	성숙도 수 준	환산 점수	백분율 (%)	성숙도 수 준	환산 점수	백분율 (%)	성숙도 수 준
개인의 역량과 윤리의식	개인정보보호에 대한 도덕성과 자기통제	0.385	0.342	88.87	H	0.337	87.49	H	0.252	65.5	VM
	개인정보 처리 업무의 사명감	0.283	0.216	76.4	VM	0.228	80.56	VM	0.148	52.39	M
	개인정보보호 법률 및 제도 이해력과 행동	0.325	0.280	86.1	H	0.280	86.11	H	0.217	66.67	VM
	개인정보보호 교육 이수 및 자기 계발	0.234	0.192	81.94	VM	0.195	83.34	VM	0.145	61.9	M
	개인정보보호에 대한 자기 효능감	0.151	0.126	83.33	VM	0.126	83.33	VM	0.088	58.35	M
	개인정보보호 기술 능력과 활용도	0.185	0.129	69.46	VM	0.113	61.12	M	0.123	66.67	VM
	피해 인지력과 문제해결 능력	0.137	0.105	76.38	VM	0.091	66.68	VM	0.070	51.19	M

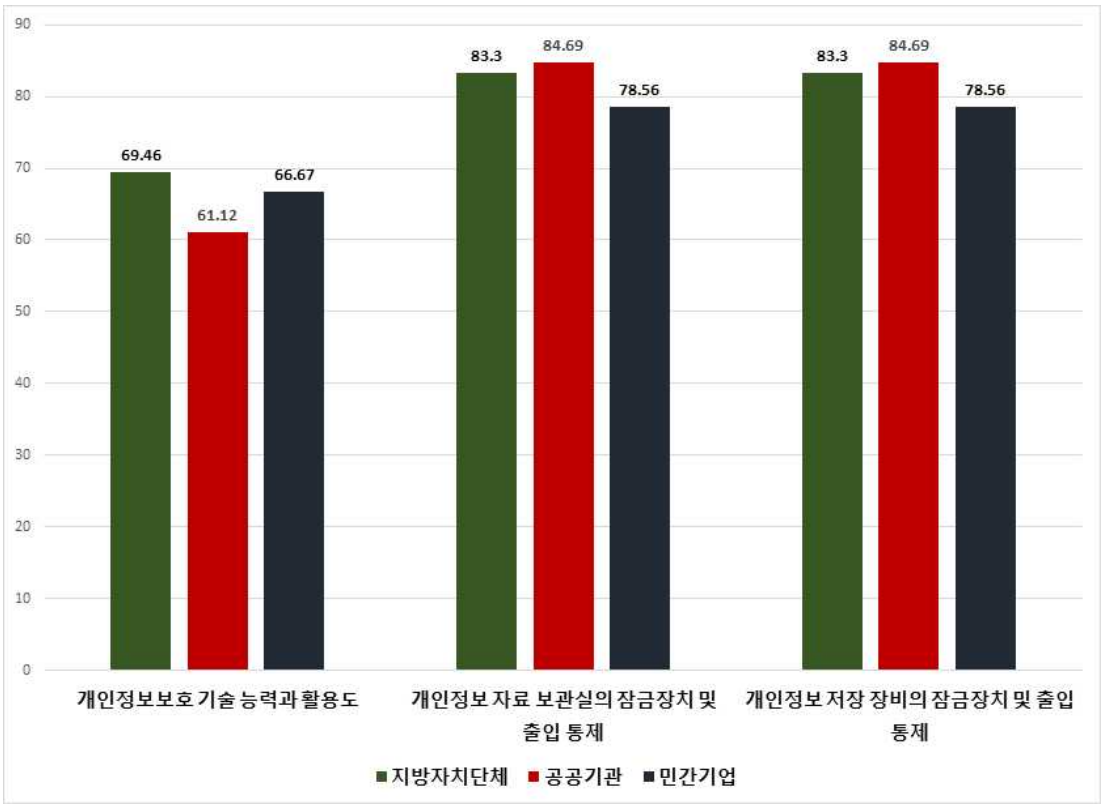
세 집단에서 가장 높은 수준의 성숙도 지표를 [그림 Ⅳ-8]과 같이 보면, 지방자치단체와 공공기관은 '개인정보보호에 대한 도덕성과 자기통제'(지방자치단체 88.87%(0.342), 공공기관 87.49%(0.337)로 'H' 등급의 성숙도 수준으로 나타났으며, 민간기업은 '개인정보 저장 장비의 잠금장치 및 출입 통제' 78.56%(0.785)로 'VM' 등급의 성숙도 수준으로 나타났다.



[그림 Ⅳ-8] 지방자치단체-공공기관-민간기업 상위 지표 순위

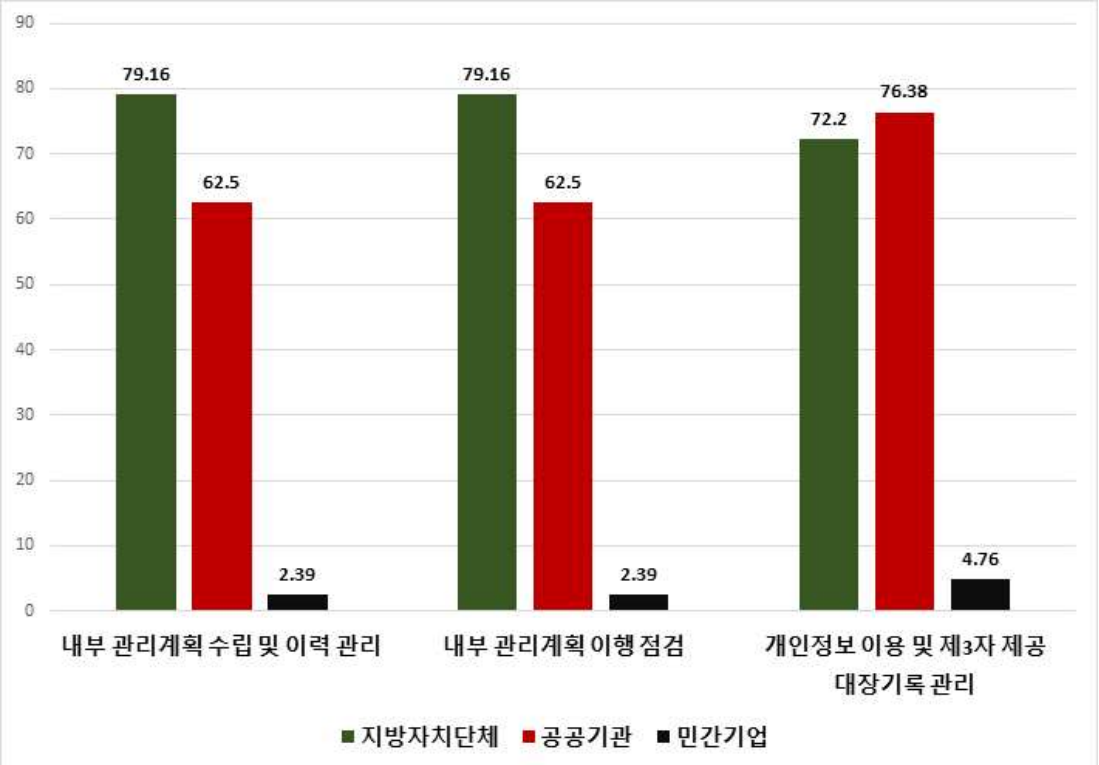
반면, 가장 낮은 성숙도 수준인 역량지표에는, 지방자치단체는 '개인정보의 국외 이전 안내 및 동의' 38.88%(0.194), 공공기관은 '개인정보보호 전용 예산 편성' 44.45%(0.072), 민간기업은 '개인정보보호 전담 조직 및 인력 구성', '성과관리(또는 인센티브제도) 운용', '위반자 제재 및 처벌', '개인정보 재해복구 훈련', '개인정보 재해복구 훈련을 통한 확인된 사항 조치', '개인정보보호 전용 예산 편성'으로 0%(0.0)로 나타났다. 이에 민간기업에서는 체계적인 개인정보보호 관리체계를 확립하기 위한 조직의 역량과 개인정보 취급자의 업무 사명감을 높일 방안이 뒤따라야 할 필요가 있다.

세 집단의 편차가 가장 낮은 지표는 [그림 Ⅳ-9]와 같이 '개인정보보호 기술 능력과 활용도', '개인정보 자료 보관실의 잠금장치 및 출입 통제, '개인정보 저장 장비의 잠금장치 및 출입 통제' 순으로 나타났다.



[그림 Ⅳ-9] 지방자치단체-공공기관-민간기업 간 편차 비교(작은 순)

세 집단의 편차가 가장 큰 지표는 [그림 Ⅳ-10]과 같이 '내부 관리계획 수립 및 이력 관리', '내부 관리계획 이행점검', '개인정보 이용 및 제3자 제공 대장기록 관리' 순으로 나타났다.



[그림 Ⅳ-10] 지방자치단체-공공기관-민간기업 간 편차 비교(큰 순)

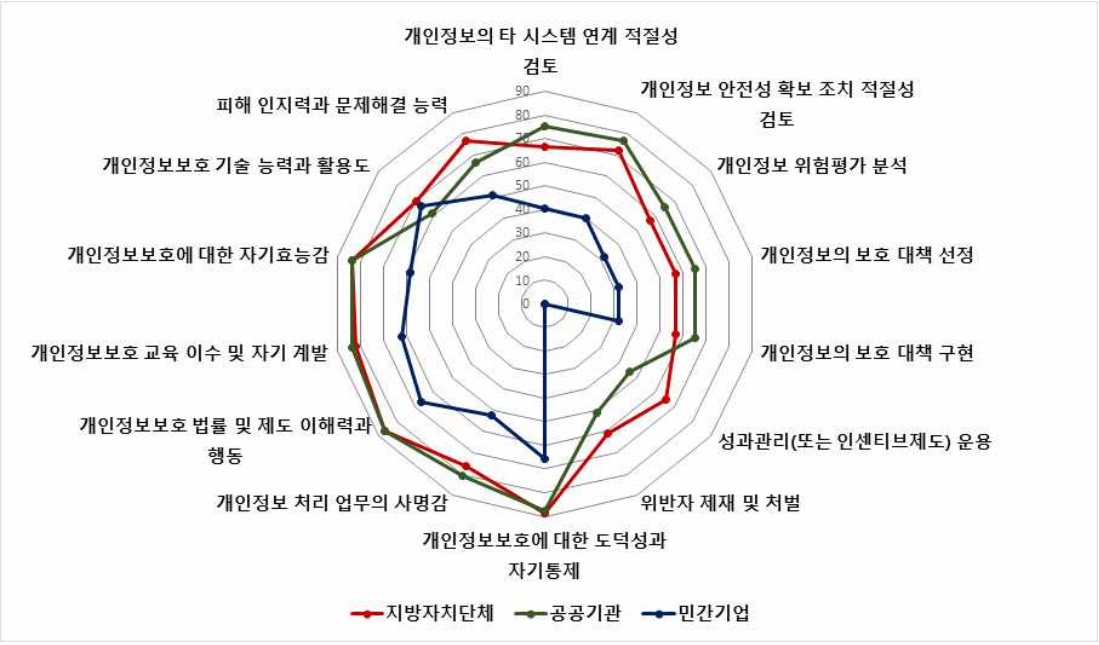
3) 신규 개발된 평가지표의 성숙도 수준 비교

본 연구에서 신규로 개발된 14개의 평가지표를 세 집단에 적용하여 실증 분석한 결과는 <표 Ⅳ-17>과 같다.

<표 Ⅳ-17> 신규 개발 지표의 집단 간 성숙도 자가 진단 결과 비교

하위 개념	세부 지표	환산 점수	역량성숙도 측정 결과								
			지방자치단체			공공기관			민간기업		
			환산 점수	백분율 (%)	성숙도 수 준	환산 점수	백분율 (%)	성숙도 수 준	환산 점수	백분율 (%)	성숙도 수 준
개인정보 흐름 분석	개인정보의 타 시스템 연계 적절성 검토	0.233	0.155	66.68	VM	0.175	75	VM	0.094	40.48	M
	개인정보 안전성 확보 조치 적절성 검토	0.361	0.261	72.23	VM	0.276	76.39	VM	0.146	40.49	M
개인정보 안전성 분석	개인정보 위험 평가 분석	2.553	1.454	56.96	M	1.666	65.27	VM	0.821	32.14	L
	개인정보의 보호 대책 선정	0.87	0.496	56.96	M	0.568	65.27	VM	0.280	32.14	L
	개인정보의 보호 대책 구현	0.771	0.439	56.96	M	0.503	65.27	VM	0.248	32.14	L
조직의 역량	성과관리(또는 인센티브제도) 운용	0.113	0.074	65.28	VM	0.052	45.84	M	0.000	0	N
	위반자 제재 및 처벌	0.097	0.059	61.12	M	0.050	51.41	M	0.000	0	N
개인의 역량과 윤리의식	개인정보보호에 대한 도덕성과 자기통제	0.385	0.342	88.87	H	0.337	87.49	H	0.252	65.5	VM
	개인정보 처리 업무의 사명감	0.283	0.216	76.4	VM	0.228	80.56	VM	0.148	52.39	M
	개인정보보호 법률 및 제도 이해력과 행동	0.325	0.280	86.1	H	0.280	86.11	H	0.217	66.67	VM
	개인정보보호 교육 이수 및 자기 계발	0.234	0.192	81.94	VM	0.195	83.34	VM	0.145	61.9	M
	개인정보보호에 대한 자기효능감	0.151	0.126	83.33	VM	0.126	83.33	VM	0.088	58.35	M
	개인정보보호 기술 능력과 활용도	0.185	0.129	69.46	VM	0.113	61.12	M	0.123	66.67	VM
	피해 인지력과 문제해결 능력	0.137	0.105	76.38	VM	0.091	66.68	VM	0.070	51.19	M

[그림 Ⅳ-11]과 같이 신규 개발된 지표별 집단 간 성숙도 수준 결과를 살펴보면, 개인정보 흐름 분석단계에서 '개인정보의 타 시스템 연계 적절성 검토' 지표를 보면, 지방자치단체 66.68%(0.155), 공공기관 75%(0.175), 민간기업 40.48%(0.094)로 나타났으며, '개인정보 안전성 확보 조치 적절성 검토'는 지방자치단체 72.23%(0.261), 공공기관 76.39%(0.276), 민간기업 40.49%(0.146)로 나타났다. 두 번째, 개인정보 안전성 분석단계에서 '개인정보 위험평가 분석', '개인정보의 보호 대책 선정', '개인정보의 보호 대책 구현'은 지방자치단체 56.96%, 공공기관 65.27%, 민간기업 32.14%로 나타났다. 세 번째, 조직의 역량에서 '성과관리(또는 인센티브제도) 운용' 지표는 지방자치단체 65.28%(0.0.074), 공공기관 45.84%(0.0.052)로 나타났으며, '위반자 제재 및 처벌' 지표는 지방자치단체 61.12%(0.059), 공공기관 51.41%(0.050)로 나타났다. 반면, 민간기업은 '성과관리(또는 인센티브제도) 운용', '위반자 제재 및 처벌' 지표 모두 0%로 나와 개인정보 취급자의 사명감과 책임을 강화하는 방안을 마련할 필요가 있다. 네 번째, 개인의 역량과 윤리의식 역량 7개 지표에서는 지방자치단체 평균 80.35%, 공공기관 78.38%로 성숙도 수준이 'VM'으로 높게 나타났으나, 민간기업은 60.38%로 공공분야보다 낮게 나타났다.



[그림 Ⅳ-11] 신규 개발 지표 측정 결과(집단 간 비교)

Ⅵ. 결론

6.1 연구 결과

본 연구는 개인정보 취급자가 스스로 개인정보 관리역량성숙도를 측정 함에 있어 더욱 객관적으로 관리역량 수준을 확인하고 그 결과에 따라 개인정보 관리 현상에 대한 개선 또는 관리를 할 수 있는 평가지표를 개발하는 데 목적이 있다.

이와 같은 연구의 목적을 달성하기 위해서 첫 번째, 선행연구 및 문헌을 고찰하여 연구에 필요한 개념을 설계하였다. 이를 토대로 현행 개인정보보호 및 정보보안 성숙도 모델의 문제점을 파악하였다. 기존의 ISMS-P, PIA, 공공기관 개인정보 관리 수준 진단, ISO27702 모델에서 총 5개의 상위개념과 17개 하위개념, 75개의 평가지표를 도출하였고, 개인정보 취급자의 역량과 윤리의식 측정을 위한 14개 항목을 신규 제안하여 총 89개의 세부 지표 초안을 도출하였다.

두 번째, 개발한 지표 초안은 전문가패널을 대상으로 2차에 걸쳐 델파이 조사를 한 결과, 세부 지표 전체의 CVR 값은 0.54~1.00으로, Cronbach's α 값의 평균은 0.85로 타당도와 신뢰도가 적절한 것으로 분석되었다. 그 결과 최종 89개의 평가지표와 3계층의 계층구조를 최종 도출되었다.

세 번째, 델파이 조사로 도출된 평가지표 간 상대적 중요도를 파악하기 위해 AHP 조사기법을 통해 가중치를 평가하였다. 요인을 AHP를 통해 3단계로 구분하여 각 기준에 따른 차원의 중요도를 산출하였고, 1단계 차원의 중요도는 안전성 확보 조치(0.443), 개인정보 생애주기 보호(0.280), 사전 계획 및 설계(0.179), 개인정보 관리 수준 점검 및 개선(0.057), 권리보장 및 윤리역량(0.041) 순으로 나타났다. 2단계 차원의 중요도는 접근관리(0.157), 이용 및 제공(0.124), 수집(0.108) 순으로 나타났다. 3단계 차원의 중요도는 내부 관리계획 수립 및 이력 관리(0.062), 접근권한 절차 수립 및 이력 관리(0.0648), 접근권한 차등 부여(0.0512) 순으로 나타났다.

네 번째, 평가지표를 측정할 성숙도 수준 모델은 선행연구에서의 업무 연속성

성숙도 모델(Business Continuity Maturity Model)을 활용하여 개인정보 관리역량 성숙도 모델(PCM2 : Privacy Competency Maturity Model)을 개발하였다.

본 연구에서 개발한 개인정보 관리역량 성숙도 모델과 평가지표에 대한 실증을 위해 평가지표의 신뢰도 검증, 자가 진단 테스트 등 2가지 방법으로 진행하였다. 첫 번째, 개인정보 관리역량 성숙도 모델 및 평가지표 안의 사용자 신뢰도를 알아보기 위해서 개인정보 관련 업무 종사자 88명을 대상으로 표본 설문조사를 시행하여 평가 모형안의 신뢰도(Cronbach's α값)는 0.9 이상으로 매우 높은 것으로 분석되었다.

두 번째, 기존 성숙도 측정모델인 PIA, CMMI와 제안한 성숙도 측정모델인 PCM2를 비교 분석하였는데, 실무자 인식의 편차가 가장 큰 지표는 개인정보 수집 필수사항 안내 및 동의, 개인정보보호에 대한 도덕성과 자기통제로 나타났으며, 개인정보의 국외 이전 안내 및 동의, 개인정보 재해복구 훈련이 편차가 가장 작은 것으로 나타났다.

세 번째, 개인정보 관리역량성숙도의 자가 진단 테스트 참여자 82명의 평균 점수는 61.56%로 'M'의 성숙도 수준으로 보였으며, 지방자치단체는 72.10%로 성숙도 수준은 'VM', 공공기관은 73.42%(0.840)로 성숙도 수준은 'VM', 민간기업은 42.37%(0.461)로 성숙도 수준이 'M'으로 나타났다. 공공기관이 개인정보 관리역량 수준이 가장 높은 것으로 나타났고, 지방자치단체, 민간기업 순으로 나타났다.

마지막으로 개인정보 관리역량 성숙도의 유의한 차이가 있는 검증을 위해 Duncan과 Scheffe의 사후분석을 실시한 결과, 업무처리 흐름 분석, 개인정보 흐름 분석, 개인정보 안전성 분석, 관리체계 수립, 수집, 이용 및 제공, 보관 및 파기, 내부 관리계획, 접근관리, 접근통제, 관리/기술적 보호, 대응훈련 능력, 조직의 역량, 개인의 역량과 윤리의식은 민간기업 대비 지방자치단체와 공공기관이 더 높은 것으로 나타났다. 개인의 암호화는 민간기업 대비 지방자치단체가, 지방자치단체 대비 공공기관이 더 높은 것으로 나타났고, 정보 주체의 권리보장은 민간기업 대비 공공기관이, 공공기관 대비 지방자치단체가 더 높은 것으로 나타났다.

6.2 연구의 시사점과 향후 연구 방향

지금까지의 개인정보보호 관련 역량 모델 평가에 관한 연구를 보면 정보보호 위주의 연구가 대부분이다. 기관 내에서 강력한 보호 대책 및 기준에도 불구하고 내부자에 의한 개인정보 침해사고가 꾸준히 발생하는 원인은 통제하는 주체와 통제받는 주체가 인간이기 때문이다. 아무리 기술적 보안이 체계적으로 되어 있어도 인간의 내면과 의식구조를 관리하는 인적 보안은 한계가 뒤따른다. 이러한 인간의 특성을 고려하여 개인정보 취급자의 관리역량과 윤리의식을 평가하기에는 ISMS-P, PIA, 공공기관 개인정보 관리 수준 진단, ISO27702, CMMI 등 기존의 성숙도 모델로는 한계점이 있다. 이 들의 평가 모델은 개인정보처리자인 기관의 개인정보보호 관리체계와 자산을 평가하기에는 적합하지만, 개인정보 취급자를 식별하고 평가하기에는 다소 무리가 있다.

그렇기에 본 연구에서는 개인정보 취급자를 관점으로 기존의 모델을 한 단계 개선하고 개인정보보호에 대한 도덕성과 자기통제, 개인정보 처리 업무의 사명감, 개인정보보호 법률 및 제도 이해력과 행동, 개인정보보호 교육 이수 및 자기 계발, 개인정보보호에 대한 자기효능감, 개인정보보호 기술 능력과 활용도, 피해 인지력과 문제해결 능력 등 개인의 관리역량과 윤리의식을 높일 수 있는 지표를 신규로 개발하여 개인정보 관리역량 성숙도 모델 및 평가방안을 연구하였다. 개발된 지표는 기관의 환경과 여건에 따라 평가에 대한 기준의 적용이 달라질 수 있지만 개인정보 관리역량 강화를 위해 평가지표별 관리 수준을 갖춰야 한다는 방향성을 제시할 수 있다는 점에서 큰 의의가 있다.

이 연구에서 개발된 개인정보 관리역량 평가지표의 활용방안은 다음과 같다.

첫 번째, 기관에서 평가지표를 통해 자체적인 평가도구로 활용하여 개인정보 관리 수준의 현상과 문제점을 객관적으로 파악한다. 두 번째, 여러 사업장을 관리하는 조직에서는 사업장별 관리 수준을 평가하여 비교평가 도구로 활용한다.

세 번째, 기관의 종사자가 개인정보 관리역량 평가를 통해 취약점을 개선하여 더욱 적절한 개인정보 관리 관리가 가능하며 관리의 피드백과 중장기적 관리 전

략을 수립하여 투자에 대한 근거로 활용한다.

이 연구에서 개발된 평가지표의 특징으로는 공공분야만의 개인정보 관리역량 수준만을 독립적으로 평가할 수 있는 지표로 활용할 수 있으며 평가항목별 가중치를 통한 환산점수가 부여되어 평가 수준을 점수화하여 확인할 수 있다는 장점이 있다.

개인정보를 취급하는 기관과 종사자들의 개인정보보호와 관리, 활용 능력이 향상되어 더욱 안전하게 업무를 수행하는 데에 중요한 일익을 담당하기를 바라면서 향후 연구 방향 제언을 하고자 한다.

첫째, 본 연구에서 개발된 개인정보 관리역량 성숙도 모델을 시간적인 제약으로 시스템 구축을 하지 못하였는데, 개인정보 취급기관과 개인정보 취급자들이 쉽게 활용할 수 있도록 개인정보 관리역량성숙도 진단 시스템을 구축할 필요가 있다.

둘째, 현재 개인정보 보호법에 명시되어 있는 개인정보처리자의 범위에 행정시·구를 포함하여 개인정보보호의 사각지대를 최소화할 필요가 있다.

마지막으로 본 연구에서 개발된 역량성숙도 모델의 활용성을 높이기 위해 부서 단위의 개인정보 관리 수준 진단 평가 시 평가항목으로 추가하고 이를 평가하여 인사고과 반영, 인센티브제도 제공하는 방안을 마련할 필요가 있다.

향후 산업 전반적으로 통용될 수 있도록 다른 연구 방법을 통해 개인정보 관리역량 평가지표의 개발 연구가 이루어질 수 있기를 제언하며, 이 연구의 평가지표가 자율적 개인정보 관리 수준 활동 관련 연구의 기초자료로 활용될 수 있기를 기대한다.

참 고 문 헌

[1] https://mobile.newsis.com/view.html?ar_id=NISX20220111_0001720921 (검색일자 : 2022.3.4.)

[2] https://www.boannews.com/media/view.asp?idx=94824&kind=2 (검색일자 : 2022.2.19.)

[3] Wacks, R. "Personal Information : Privacy and the Law." Oxford: Clarendon Place, 1989.

[4] OECD. "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." 1980.

[5] https://www.law.go.kr/lsSc.do?section=&menuId=1&subMenuId=15&tabMenuId=81&eventGubun=060101&query=%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%B2%95#undefined(검색일자 : 2022.1.21.)

[6] https://www.privacy.go.kr/nns/ntc/inf/personalInfo.do (검색일자 : 2022.1.21.)

[7] 임효진. "개인정보의 보호와 활용에 관한 정책변동 연구." 국내박사학위논문 성균관대학교 국정전문대학원, 2022. 서울

[8] 김민우. "개인정보의 개념과 그 보호에 관한 헌법적 연구." 국내박사학위논문 성균관대학교 일반대학원, 2021. 서울

[9] 개인정보보호위원회. "개인정보 영향평가 수행 안내서." 개인정보보호위원회, 2020.12.

[10] 주영선. “개인정보의 처리에 관한 동의제도.” 국내박사학위논문 전남대학교, 2022. 광주

[11] http://www.cctvnews.co.kr (검색일자 : 2022.1.21.)

[12] 이소은. “개인정보 보호법의 주요 개정 내용과 그에 대한 평가 - 개인정보 처리의 정당화 사유를 중심으로”, 이화여자대학교 법학논집, 24(3):249-28, 2020.

[13] 이동녘, 박정선.(2010). “개인정보보호를 위한 정보시스템 보안 감사 방법에 관한 연구”, 대한안전경영과학회지 12.4. pp.107～116

[14] 장진원. “개인정보 라이프사이클에 따른 개인정보보호 관리 실태 및 개선방안에 대한 연구”, 국내석사학위논문 동국대학교, 2014. 서울.

[15] 김영희. “개인정보의 안전성 확보를 위한 프레임워크 개발에 관한 연구.” 국내박사학위논문 서울과학기술대학교, 2018. 서울

[16] 행정안전부. “개인정보 침해사례 및 개인정보 보호법(안) 소개집” 행정안전부, 2020.

[17] 김정덕, 황수하. “개인정보보호 거버넌스의 목표와 프로세스에 관한 연구”, 한국정보보호학회 학회지, 제21권, 제5호, pp.7～11. 2011.

[18] 개인정보보호위원회. “개인정보의 범위에 관한 연구” 개인정보보호위원회, 2014.

[19] 한국전산원. “유비쿼터스 컴퓨팅 환경하의 개인정보 침해 유형 분석” 한국전산원, 2004.

[20] https://www.law.go.kr/admRulSc.do?menuId=5&subMenuId=41&tabMenuId=183&query=%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EC%9D%98%20%EA%B8%B0%EC%88%A0%EC%A0%81#liBgcolor0(검색일자 : 2022.1.21.)

[21] https://www.law.go.kr/lsSc.do?section=&menuId=1&subMenuId=15&tabMenuId=81&eventGubun=060101&query=%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%B2%95#liBgcolor0(검색일자 : 2022.1.21.)

[22]https://www.law.go.kr/admRulSc.do?menuId=5&subMenuId=41&tabMenuId=183&query=%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EC%9D%98%20%EA%B8%B0%EC%88%A0%EC%A0%81#liBgcolor0 (검색일자 : 2022.1.21.)

[23] 변동현. “기업 유형별 개인정보보호를 위한 보호조치에 관한 연구.” 국내석사학위논문 숭실대학교 대학원, 2021. 서울

[24] https://www.law.go.kr/admRulSc.do?menuId=5&subMenuId=41&tabMenuId=183&query=%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EC%9D%98%20%EC%95%88%EC%A0%84%EC%84%B1%20%ED%99%95%EB%B3%B4%EC%A1%B0%EC%B9%98#liBgcolor0(검색일자 : 2022.1.21.)

[25] 박홍민. “GDPR 기반의 정보 주체·아동 권리 강화 개선 연구.” 국내석사학위논문 숭실대학교 정보과학대학원, 2019. 서울

[26] https://www.boannews.com/media/view.asp?idx=101347(검색일자 : 2022.2.4.)

[27] 감사원. “2021 개인정보보호 추진실태 감사보고서” 감사원, 2022.

[28] OECD. “The OECD Privacy Framework” OECD, 2013.

[29] 유한나, 전문석. “국내 개인정보 보호법의 발전방향 제시를 위한 국외 개인정보 보호법 분석”. 정보보호학회논문지, 22(5), p.1091-1102. 2012.

[30] ISM3 v2.3, “*Information Security Management Maturity Model”,* 2009.

[31] The Complete Public Domain BCMM, Virtual Corporation, 2005.

[32] Ann Cavoukian, Privacy by Design-The 7 Foundational Principles (Information and Privacy Commissioner, Ontario, Canada, 2011), 1쪽

[33] 최혜선. “개인정보보호의 신경향 – 프라이버시 중심 디자인(Privacy by Design)을 중심으로–”, 일감법학 제24호, 2013.

[34] 개인정보보호위원회, “자동처리되는 개인정보보호 가이드라인”. 개인정보보호위원회, 2020.12.

[35] ISO/IEC. ISO/IEC 27701:2019(Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines). 2019, 08.

[36] 강민성. “EU-GDPR을 대비한 개인정보보호 인증제도의 개선방안.” 국내석사학위논문 숭실대학교 정보과학대학원, 2021. 서울

[37] https://isms-p.kisa.or.kr/main/ispims/notice/(검색일자 : 2022.5.2.)

[40] 한국인터넷진흥원. “정보보호 및 개인정보보호 관리체계 인증제도 안내서”, 한국인터넷진흥원, 2021.

[41] 한국인터넷진흥원. “개인정보 영향평가 수행 안내서”, 한국인터넷진흥원, 2020.

[42] Choi, N., Kim, D., Goo, J., & Whitmore, A. (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. Information Management and Computer Security, 16(5), 484-501.

[43] Layton, T. P.(2005). Information security awareness. Bloomington, Ind.: AuthorHouse.

[44] 임채호(2006). “효과적인 정보보호 인식 제고 방안.” 정보보호학회, 16(2), 30-36.

[45] 장명희, 강다연. “항만기업 종사자들의 정보보안 인식과 지각된 정보보안위험에 영향을 미치는 요인.” 한국항해항만학회지, 36(3), 261-271. 2012.

[46] Kim, Ju-yeon. “Improvement Method of Education for Personal Information Protection through Survey on Perception in College Students.” Journal of the Korea Institute of Information and Communication Engineering 23, no. 3 (March 31, 2019): 349 - 55. doi:10.6109/JKIICE.2019.23.3.349.

[47] Jung, Eun-Young. “The Effect of Ethical Values on the Patient's Personal Information Protection of College Students Majoring in Healthcare Administration.” Journal of Digital Convergence 18, no. 10 (October 28, 2020): 345 - 52. doi:10.14400/JDC.2020.18.10.345.

[48] 조유나. “조직 내 구성원의 보안윤리 적성검사도구 개발에 관한 연구.” 국내석사학위논문 상명대학교 경영대학원, 2018. 서울

[49] 유지찬. “위닝 프로페셔널.” 서울: 타임스퀘어. 2010.

[50] 김석영. “객실승무원의 개인 성향이 직무몰입에 미치는 영향” 국내석사학위논문, 2016.

[51] 백민정. “정보윤리활동이 정보보안성과에 미치는 영향에 관한 연구” 국내박사 학위논문. 2010.

[52] 강다연, & 장명희. “정보보안 정책 준수가 정보보안능력 및 행동에 미치는 영향 분석: 해운항만조직구성원을 대상으로.” 2014.

[53] 한진영, & 유현선. “경영진의 정보보안 지능이 조직원의 보안대책 인식에 미치는 영향.” Information Systems Review, 18(3), 137-153. 2016.

[54] Landeta, J.(2006). “Currentvalidity ofthe Delphimethod in socialsciences.” Technological Forecasting&Social Change, 73(5), 467-482

[55] Donohoe, Holly M.(2009) "Moving best practice forward: Delphi characteristics, advantages, potential problems, and solutions" The international journal of tourism research, 11(5): 415~437.

[56] Fink, A. & Kosecoff, J(1985). "How to conduct surveys: A step-by-step guide." London: Sage Publications.

[57] Anderson, D.(1997). "Strand of System, The Philosophy of C, Peirce", West Lafayette: Purdue University Press.

[58] Dalkey, N. C. (1969). "The Delphi methed; an exper mental study of group opinion", The Rand Corp.

[59] 이종성. "델파이 방법과 고등교육 연구." 연세교육연구, 1(2), 33-46. 1988.

[60] 이성웅. "Delphi기술 예측 기법의 유용성에 관한 연구." 전북대학교 대학원 박사학위논문. 1987.

[61] 박현, 고길곤, 유석현. "예비타당성조사 수행을 위한 다기준 분석 방안 연구(Ⅱ)", 2001년도 예비타당성 조사연구 보고서, 한국개발연구원 공공투자관리센터." (2001): 55-56.

[62] 최윤미(2002). "비즈니스 영어 평가내용 개발을 위한 델파이 연구." 이화여자대학교 대학원 석사학위논문

[63] Saaty,T.L, "The Analytic Hierarchy Process", New York : McGraw - Hill. International, 1980.

[64] Saaty,T.L,"Decision Makingwith Dependenceand Feedback:The Analytic Network Process", Int. J. ServicesSciences, Vol. 1, No.1, pp.83-98, 2000.

[65] 조근태, 저용곤, 강현수. "앞서가는 리더들의 계층 분석적 의사결정." 서울, 동현출판사. 2002.

[66] Vegas, L. G.(1990). “An overview of the analytic hierarchy process and its application”, European Journal Operational Research, 2-8.

[67] 박진규. “DEA AHP 모형을 이용한 국내 철강 유통업체 선정.” 국내석사학위논문 경북대학교 대학원, 2017. 대구

[68] 최윤정. “선용품 공급업체 선정 의사결정에 관한 연구.” 한국해양대학교 대학원 석사학위 논문. 2008.

[69] Triantaphyllou et al.,(1997). “Determining the most important criteria in maintenance decision making”. MCBUP Ltd.

[70] 송근원·이영. “AHP의 일관성 향상을 위한 척도 재구성 연구.” 한국 지방정부학회, 2011(12), 178-188.

[71] 김영희. “개인정보의 안전성 확보를 위한 프레임워크 개발에 관한 연구.” 국내박사학위논문 서울과학기술대학교, 2018. 서울

[72] Kang, Min Soo, et al. “A Study of Self-Checklist for Personal Information Protection of FinTech Service: For the Simple Payment Service.” The Journal of Society for E-Business Studies, vol. 20, no. 4, Society for e-Business Studies, 30 Nov. 2015, pp. 77 - 102. Crossref, doi:10.7838/jsebs.2015.20.4.077.

[73] 오유리. "정보보호 역량성숙도 모델 활용에 대한 연구." 국내석사학위논문 건국대학교, 2019. 서울

[74] https://intra.privacy.go.kr/pim/mng/new/personalInfoFileMyList.do(검색일자 : 2022.11.9.)

[75] https://www.pipc.go.kr/np/default/page.do?mCode=D050040000(검색일자 : 2022.11.9.)

[76] https://www.slideteam.net/business-continuity-maturity-model.html#images-(검색일자 : 2022.11.9.)

[77] 오상익. “지방자치단체의 정보보호서비스 대가 산정 모델 적용 성과 분석 및 개선 방안.” 국내석사학위논문 제주대학교, 2020.

[78] Ayre C and Scally AJ. “Critical values for Lawshe’s content validity ratio: revisiting the original methods of calculation.” Measurement and Evaluation in Counseling and Development. 47(1): 79-86. 2014.

[79] 최익서, 김진수, and 박남제. “AHP 방법 이용한 경찰의 산업기술보호 분야 역량 강화 방안.” 한국정보기술학회논문지 18.12 (2020): 103-112.

[80] 김지현. “전문가 델파이 기법을 통한 쌀 교육 프로그램 개발 및 교육효과 평가.” 국내석사학위논문 상명대학교 대학원, 2013. 서울

[81] 구경희. “이해당사자 기반 평생교육실습 프로그램 평가척도 개발.” 국내박사학위논문 동의대학교 대학원, 2017. 부산

ABSTRACT

Development of Personal Information Management Competency Maturity Model and Evaluation Indicators to Strengthen Privacy

Sangik Oh

Convergence Information Security
Graduate School, Jeju National University
Jeju, Korea

(Supervised by professor Namje Park)

The purpose of this study is to develop an evaluation index that allows personal information handlers to more objectively check the level of management capability and improve or manage personal information management according to the results.

In order to achieve the purpose of this study, the concepts necessary for research were designed by examining previous studies and literature. Based on this, the problems of the current personal information protection and information security maturity model were identified. A total of 89 evaluation indicators were derived by selecting 75 evaluation indicators from the existing ISMS-P, PIA, public institution personal information management level diagnosis, and ISO27702 model, and 14 new items for measuring personal information handler's competence and ethics. Delphi surveys were conducted twice on expert panels, and weights were evaluated through the AHP survey technique to understand the relative importance between evaluation indicators. As a result, the final evaluation index was confirmed as 5 higher concepts, 17 lower concepts, and 89 detailed indicators. The maturity model to measure the

evaluation index proposed a Privacy Competency Maturity Model (PCM2) based on the existing Business Continuity Maturity Model (BCMM) with seven levels of maturity (Very High, High, Very Medium, Medium, Very Low, None).

As a result of verifying the user's reliability of the personal information management competency maturity model and evaluation index developed in this study, it was analyzed that the Cronbach's α value was very high at 0.9 or more. In addition, as a result of the self-diagnosis test of personal information management capabilities for workers in public and private institutions, it was found that the public had a higher level of personal information management capabilities than the private sector. As a result of comparing and analyzing the existing maturity measurement models PIA and CMMI with the proposed maturity measurement model PCM2, PIA and CMMI are suitable for personal information controller evaluation, and PCM2 is suitable for personal information handler evaluation.

Most of the studies on the evaluation of competency models related to personal information protection so far have focused on information protection. Despite strong protection measures and standards within the institution, human beings are the controlling and controlled entities that constantly cause personal information infringement accidents by insiders. In consideration of these human characteristics, there are limitations in the existing maturity model to evaluate the management capabilities and ethical consciousness of personal information handlers. Their evaluation model is suitable for evaluating the personal information protection management system and assets of institutions that are personal information processors, but there is a limit to identifying and evaluating personal information handlers.

Therefore, this study is significant in that it developed a new indicator that can improve the existing model from the perspective of personal information handlers and increase individual management capabilities and ethical awareness

considering the human inner side. The developed model was developed for the evaluation of personal information handlers, not personal information processors, providing useful information for the evaluation of personal information management competency maturity, and practical use of the evaluation.

Using the evaluation index developed in this study, it is expected that personal information handlers can be applied as detailed management guidelines for performing their own tasks, and that personal information management capabilities can be evaluated to achieve objective and reliable personal information protection management.

Keywords: Privacy, Personal Information Handler, PCM2, AHP, Maturity Model

[부록 1] 개인정보 관리역량성숙도 자가 진단 질문지

개인정보 관리역량성숙도 자가 진단 질문지

안녕하십니까?

본 진단지는 '개인정보 관리 역량성숙도 측정'을 위하여 작성되었습니다. 귀하께서 응답하신 결과를 바탕으로 개인정보 관리 역량 진단 점수가 도출될 것이며, 다른 목적으로 이용되지 않습니다.

개인정보 관리 역량성숙도 모델 진단 점수란 개인정보 취급자의 역량을 자가 진단하기 위해 고안된 평가 모델입니다. 여기서 개인정보 관리 역량이란 개인정보 처리 업무 계획 단계에서부터 폐기 전반을 수행할 수 있는 업무 역량을 의미합니다.

본 진단모델은 개인정보 취급자의 역량을 사전 계획 및 설계, 개인정보의 생애주기, 안전성 확보 조치, 개인정보 관리 수준 점검 및 개선, 권리보장 및 윤리역량 5가지로 분류하고 있습니다. 세부항목별로 자신의 역량과 지식수준을 가장 잘 표현한다고 생각되는 수준을 선택해주시기 바랍니다.

[진단 응답 안내]

개인정보 관리 역량 지수 진단을 위한 측정 항목들이 나열되어 있습니다. 역량 및 지식에 대한 항목별 정의와 평가 문항을 읽고, 자신의 역량 및 지식수준을 자가 진단하여 가장 적절한 수준을 선택해주시기 바랍니다.

[개인정보 관리역량성숙도 수준단계]

성숙도 단계		정의
역량 성숙도 증가 ↑	VH (Very High)	전사적으로 시행 및 성과 측정 계획이 수립되고 시행 후 결과에 따라 주기적으로 모니터링 및 개선을 수행하는 단계
	H (High)	전사적으로 시행계획과 성과 측정 계획이 수립되고 시행되고 있는 단계
	M (Medium)	전사적으로 시행계획이 수립되고 수행되고 있는 단계
	L (Low)	부분적으로 시행계획이 수립되고 수행되고 있는 단계
	VL (Very Low)	세부 평가항목으로 수행되지 않고 있는 단계

□ **'사전 계획 및 설계단계'** 에 대한 개인정보 관리역량 자가 진단표입니다. 항목별 정의와 평가 문항을 읽고, 자신의 역량 및 지식수준을 자가 진단하여 가장 적절한 수준에 해당되는 항목에 'V' 또는 '○'로 표시해주세요.

하위 개념	세부 지표	평가지표	자가 진단표						
			N	VL	L	M	VM	H	VH
업무처리 흐름 분석	개인정보 처리 업무처리 흐름도·흐름표 작성	처리하려는 업무 흐름도 및 흐름표를 작성하였는지 확인하고 처리한다.							
	업무처리 흐름도·흐름표 개정 관리	업무 흐름도 및 흐름표는 최신 상태로 유지되고 있는지 확인하고 처리한다.							
개인정보 흐름 분석	개인정보 수집, 이용, 보유기간 적절성 검토	개인정보를 수집하는 경우 목적에 필요한 최소한의 범위에서만 수집하도록 계획하고, 개인정보 보유기간을 명확한 근거에 의하여 정하고 있는지 확인하고 처리한다.							
	주민등록번호, 민감정보, 고유 식별정보 처리 적절성 검토	주민등록번호 수집 시 법령에 근거하고 있으며, 인터넷 홈페이지는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있도록 계획하고, 민감정보, 고유 식별정보를 처리하는 경우 다른 개인정보의 처리에 대한 동의와 별도로 구분하여 동의받도록 계획하고 있는지 확인하고 처리한다.							
	개인정보 수집 항목 구분 적절성 검토	개인정보를 수집하는 경우 필수항목과 선택항목을 분리하고 선택적으로 동의할 수 있는 사항에 동의하지 아니하여도 서비스 이용이 가능하도록 계획하고 있는지 확인하고 처리한다.							
	만 14세 미만의 아동 정보 수집 적절성 검토	만 14세 미만의 아동 개인정보 수집 시, 법정 대리인에게 동의받도록 계획하고 있는지 확인하고 처리한다.							
	제3자 제공, 위·수탁 적절성 검토	제3자 제공에 관한 사항을 정보 주체에게 알리고 받도록 계획하고, 위수탁 업무인지 여부를 확인하고 처리한다.							

하위 개념	세부 지표	평가지표	자가 진단표						
			N	VL	L	M	VM	H	VH
	개인정보의 타 시스템 연계 적절성 검토	개인정보 처리 업무가 타 시스템과 연계되는지 검토하고 적절하게 연계되도록 계획하고 있는지 확인하고 처리한다.							
	개인정보 안전성 확보 조치 적절성 검토	개인정보의 안전성 확보 조치 계획을 명확한 근거에 의하여 수립하고 있는지 확인하고 처리한다.							
	개인정보 처리 흐름도 작성 및 이력 관리	개인정보 처리 흐름도 작성 및 이력 관리하고 있는지 확인하고 처리한다.							
	개인정보 처리 흐름표 작성 및 이력 관리	개인정보 처리 흐름표 작성 및 이력 관리하고 있는지 확인하고 처리한다.							
개인정보 안전성 분석	개인정보 처리 위험도 및 침해요인 분석	개인정보 처리에 따른 위험도 및 침해요인을 분석하고 처리한다.							
	개인정보 위험 평가 분석	개인정보 처리에 따른 위험도 및 침해요인 결과에 따라 위험 평가를 분석하고 처리한다.							
	개인정보의 보호 대책 선정	개인정보의 개인정보 위험평가 분석 결과를 바탕으로 보호 대책을 수립하고 처리한다.							
	개인정보의 보호 대책 구현	개인정보의 보호 대책 수립 결과를 바탕으로 보호 이행 대책을 구현하고 처리한다.							
관리체계 수립	개인정보보호 정책 수립 적절성 검토	개인정보보호 정책, 조직, 예산이 적절하게 수립하고 있는지를 확인하고 처리한다.							
	법적 요구사항 준수 적절성 검토	개인정보 처리 업무 관련 법적 요구사항을 검토하고 준수 절차를 수립하여 처리한다.							
	관리체계 점검 및 개선 계획 수립 적절성 검토	관리체계 수립 결과를 바탕으로 보호조치 개선방안이 계획되어 있는지 확인하고 처리한다.							

□ **'개인정보 생애주기 보호단계'** 에 대한 개인정보 관리역량 자가 진단표입니다. 항목별 정의와 평가 문항을 읽고, 자신의 역량 및 지식수준을 자가 진단하여 가장 적절한 수준에 해당되는 항목에 'V' 또는 '○'로 표시해주세요.

하위 개념	세부 지표	평가지표	자가 진단표						
			N	VL	L	M	VM	H	VH
수집	개인정보 수집 필수사항 안내 및 동의	개인정보 수집 시 4가지 필수사항(수집 목적, 수집 항목, 보유 및 이용 기간, 동의 거부권 및 거부 시 불이익)을 안내하고 동의받고 있는지 확인하고 처리한다.							
	목적별 최소한의 필수정보 수집	목적별 최소한의 필수정보만 수집하고 있는지 확인하고 처리한다.							
	개인정보 수집 항목의 필수와 선택정보 구분	개인정보 수집 항목을 필수정보와 선택정보를 구분하여 동의받고 있는지 확인하고 처리한다.							
	민감정보 처리 별도 동의	민감정보 처리를 위해 별도 동의받고 있는지 확인하고 처리한다.							
	고유 식별정보 별도 동의	고유 식별정보(여권번호, 운전면허번호, 외국인등록번호) 수집할 때 별도의 동의를 받고 있는지 확인하고 처리한다.							
	만 14세 미만의 아동의 정보수집 시 법정 대리인 동의	만 14세 미만의 아동 개인정보 수집 시, 법정 대리인에게 동의받고 있는지 확인하고 처리한다.							
	주민등록번호 수집 제한 법적 준수	법률에서 구체적으로 처리를 요구하거나 허용하는 경우를 제외하고 주민등록번호를 처리하지 않고 있는지 확인하고 처리한다.							
	선택정보 동의 거부 시 서비스 제공	뉴스레터, 마케팅, 홍보를 위한 개인정보 수집에 동의하지 않더라도 기본적인 서비스를 제공하고 있는지 확인하고 처리한다.							
	개인정보의 국외 이전 안내 및 동의	개인정보의 국외 이전 시, 정보주체에게 알리고 동의받고 있는지 확인하고 처리한다.							

하위 개념	세부 지표	평가지표	자가 진단표						
			N	VL	L	M	VM	H	VH
이용 및 제공	개인정보 처리 위탁 계약서 작성 및 체결	개인정보의 처리 업무를 위탁하는 경우, 개인정보 위탁계약서를 작성하고 있는지 확인하고 처리한다.							
	위탁업무의 정보 공개	위탁업무의 내용과 수탁자(위탁받아 처리하는 자)를 공개하고 있는지 확인하고 처리한다.							
	수탁자 대상 교육 및 관리 감독	수탁자에 대한 관리·감독을 수행하고 있는지 확인하고 처리한다.							
	목적 내 제3자 이용·제공 시 필수사항 고지 및 동의	수집하는 개인정보를 목적 내 제3자에게 제공 시 필수 고지항목(제공받는 자, 이용목적, 개인정보 항목, 보유 및 이용 기간, 동의 거부권 및 거부 시 불이익 내용)을 안내하고 동의받고 있는지 확인하고 처리한다.							
	목적 외 제3자 이용·제공 시 필수사항 고지 및 동의	목적 외 제3자 이용·제공 시 필수 고지항목(제공받는 자, 이용목적, 개인정보 항목, 보유 및 이용 기간, 동의 거부권 및 거부 시 불이익 내용)을 안내하고 동의받고 있는지 확인하고 처리한다.							
	목적 외 제3자 이용·제공 사항 공고	공공기관은 개인정보의 목적 외 이용 또는 제3자 제공에 관한 사항에 관한 공고를 하고 있는지 확인하고 처리한다.							
	개인정보 이용 및 제3자 제공 대장 기록 관리	목적 외 제3자 이용·제공 사항을 관리대장에 기록 관리하고 있는지 확인하고 처리한다.							

하위 개념	세부 지표	평가지표	자가 진단표						
			N	VL	L	M	VM	H	VH
보관 및 파기	개인정보 자료 보관실의 잠금장치 및 출입 통제	개인정보 자료를 잠금장치가 된 캐비닛 등 안전한 장소에 보관하고 있는지 확인하고 처리한다.							
	개인정보 저장장비의 잠금장치 및 출입 통제	개인정보를 저장하고 있는 전산장비는 잠금장치 및 출입 통제가 되어 있는지 확인하고 처리한다.							
	개인정보 파기 기간 준수	보유기간이 경과 되거나 처리목적 달성된 개인정보는 보유 및 이용 기간 종료 후 5일 이내에 즉시 파기하고 있는지 확인하고 처리한다.							
	개인정보 파일 파기 절차 준수	개인정보 파일 파기 시 개인정보보호 책임자의 승인 절차를 준수하는지 확인하고 처리한다.							
	개인정보 파기 방법 적절성	개인정보 파기 시 복원·재생할 수 없는 형태로 완전하게 파기하는지 확인하고 처리한다.							
	개인정보 파일 파기 관리대장 기록 관리	개인정보 파기에 관한 사항을 기록하고 관리하고 있는지 확인하고 처리한다.							

□ **'안전성 확보 조치'**에 대한 개인정보 관리역량 자가 진단표입니다. 항목별 정의와 평가 문항을 읽고, 자신의 역량 및 지식수준을 자가 진단하여 가장 적절한 수준에 해당되는 항목에 'V' 또는 '○'로 표시해주세요.

하위 개념	세부 지표	평가지표	자가 진단표						
			N	VL	L	M	VM	H	VH
내부 관리계획	내부 관리계획 수립 및 이력 관리	개인정보의 안전한 처리를 위한 내부 관리계획을 수립하고 이력 관리하고 있는지 확인하고 처리한다.							
	내부 관리계획 이행점검 및 개선	안전한 처리를 위한 내부 관리계획에 대한 이행 점검을 반기 1회 이상 하고 있는지 확인하고 처리한다.							

하위 개념	세부 지표	평가지표	자가 진단표						
			N	VL	L	M	VM	H	VH
접근관리	접근권한 절차 수립 및 이력 관리	개인정보 처리시스템의 중요도(민감도) 및 업무 연관성 등을 고려하여 담당자별 차등 접근권한 절차를 마련하고 이력 관리하고 있는지 확인하고 처리한다.							
	접근권한 차등 부여	개인정보 처리시스템에 대한 접속 권한을 업무 수행 개인정보 취급자에게만 개인별(ID)별로 부여하였는지 확인하고 처리한다.							
	접근권한 변경 내역 기록 및 관리	개인정보 처리시스템 접근권한의 부여·변경·말소 내역을 기록하고, 최소 3년간 이를 보관하고 있는지 확인하고 처리한다.							
접근통제	안전한 비밀번호 작성 규칙 적용	개인정보 처리시스템 접속 시 안전한 비밀번호 작성 규칙을 적용하고 있는지 확인하고 처리한다.							
	계정 오류 입력 접근제한 설정	계정정보(ID) 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 접근을 제한하고 있는지 확인하고 처리한다.							
	부재 시 시스템 접속 차단 설정	일정 시간 이상 업무처리하지 않는 경우 시스템 접속을 차단하고 있는지 확인하고 처리한다.							
	비업무용 사이트 접속 차단 설정	파일 공유용 P2P, 웹하드, 도박 등 유해사이트 접속을 차단하고 있는지 확인하고 처리한다.							
	비인가자 접근 차단	비인자자가 관리용 기기에 접근하여 임의 조작 못하도록 조치하고 있는지 확인하고 처리한다.							
	안전한 접속(또는 인증) 수단 적용	개인정보 처리시스템에 접속 시 안전한 접속 수단이나 안전한 인증수단을 적용하고 있는지 확인하고 처리한다.							
	관리용 단말기 접근통제	관리용 단말기가 본래 목적 외로 사용되지 않도록 조치하고 있는지 확인하고 처리한다.							
접속기	개인정보 취급	개인정보 취급 업무담당자의							

하위 개념	세부 지표	평가지표	자가 진단표						
			N	VL	L	M	VM	H	VH
록 관리	자의 접속기록 보관 기간 설정	접속기록을 최소 1년 이상(5만 명 이상의 개인정보를 처리하거나, 고유 식별정보 또는 민감정보를 처리하는 경우는 2년 이상) 보관하고 있는지 확인하고 처리한다.							
	접속기록 필수 정보 적용	개인정보 취급자 및 처리 업무를 확인할 수 있도록 개인정보 취급자의 계정, 접속일시, 접속지 정보, 처리한 정보 주체 정보, 수행업무(조회, 다운로드 등) 등을 확인할 수 있도록 하였는지 확인하고 처리한다.							
	접속기록의 안전한 보관	개인정보 처리시스템 접속기록이 위·변조 및 도난, 분실되지 않도록 안전하게 보관하고 있는지 확인하고 처리한다.							
	접속기록 점검 관리	개인정보의 오남용, 분실·유출·도난·변조 또는 훼손 등을 대응을 위해 접속기록을 월 1회 이상 점검 및 후속 조치를 하고 있는지 확인하고 처리한다.							
개인정보의 암호화	개인정보의 암호화	고유 식별정보(주민등록번호, 여권번호 등), 비밀번호, 바이오정보(지문, 얼굴 등)가 암호화되어 있는지 확인하고 처리한다.							
	비밀번호의 암호화	비밀번호는 일방향 암호화를 적용하여 저장되는지 확인하고 처리한다.							

□ **‘개인정보 관리 수준 점검 및 개선’**에 대한 개인정보 관리역량 자가 진단표입니다. 항목별 정의와 평가 문항을 읽고, 자신의 역량 및 지식수준을 자가 진단하여 가장 적절한 수준에 해당되는 항목에 ‘V’ 또는 ‘○’로 표시해주세요.

하위 개념	세부 지표	평가지표	자가 진단표						
			N	VL	L	M	VM	H	VH
관리/ 기술적 보호	개인정보 관리 정책의 점검 및 검토	개인정보 처리 방침, 관련 계획 및 지침, 가이드, 매뉴얼 등 관련 정책서가 법적 준거성과 현실에 맞게 수립되어 있는지를 연 1회 이상 점검하고 보완 조치계획을 하고 있는지 확인하고 처리한다.							
	개인정보 관리 정책의 개선	개인정보 처리 방침, 관련 계획 및 지침, 가이드, 매뉴얼 등 관련 정책서가 법적 준거성과 현실에 맞게 수립하였는지 점검한 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.							
	개인정보 관리 점검 및 검토	개인정보 생애주기, 안전성 확보 조치 등 개인정보 관리실태를 연 1회 이상 점검하고 보완 조치계획을 하고 있는지 확인하고 처리한다.							
	개인정보 관리 점검결과 확인된 사항 조치	개인정보 생애주기, 안전성 확보 조치 등 개인정보 관리실태 점검 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.							
	보안취약점 점검 및 위험평가 검토	개인정보 처리시스템 또는 홈페이지를 통해 해킹 사고가 발생하지 않도록 연 1회 이상 취약점 점검을 수행하고 위험분석 평가, 보완 조치계획을 하고 있는지 확인하고 처리한다.							
	보안취약점 개선 조치	개인정보 처리시스템 또는 홈페이지 보안취약점 점검 점검한 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.							
	개인정보 노출 여부 모니터링 및 검토	홈페이지, 개인정보 처리시스템을 통해 개인정보 노출 여부를 월 1회 이상 모니터링하고 보완 조치계획을 하고 있는지 확인하고 처리한다.							
	개인정보 노출 모니터링 결과 확인된 사항 조치	개인정보 노출 여부 모니터링 점검한 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.							

하위 개념	세부 지표	평가지표	자가 진단표						
			N	VL	L	M	VM	H	VH
대응훈련 능력	개인정보 침해사고 대응훈련	개인정보 유출 사고 발생 시 개인정보 유출 사고 대응계획에 따라 신속히 대응하여 그 피해를 최소화하기 위해 개인정보 침해사고 대응훈련을 하고, 결과에 따른 보완 조치계획을 하고 있는지 확인하고 처리한다.							
	개인정보 침해사고 대응훈련 통한 확인된 사항 조치	개인정보 침해사고 대응훈련 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.							
	개인정보 재해복구 훈련	재해재난 발생 시 개인정보 처리시스템 보호를 위해 수립된 위기 대응 매뉴얼에 따라 모의훈련을 실시하고 보완 조치계획을 하고 있는지 확인하고 처리한다.							
	개인정보 재해복구 훈련을 통한 확인된 사항 조치	개인정보 처리시스템 재해복구 훈련 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.							

□ **‘권리보장 및 윤리역량’**에 대한 개인정보 관리역량 자가 진단표입니다. 항목별 정의와 평가 문항을 읽고, 자신의 역량 및 지식수준을 자가 진단하여 가장 적절한 수준에 해당되는 항목에 ‘V’ 또는 ‘○’로 표시해주세요.

하위 개념	세부 지표	평가지표	자가 진단표						
			N	VL	L	M	VM	H	VH
정보주체의 권리보장	정보 주체 중심의 개인정보 처리 방침 공개	개인정보 처리 방침을 정보 주체가 알기 쉽게 필수사항을 모두 투명.명확하게 포함하여 수립하고, 홈페이지 등 정보 주체가 쉽게 확인할 수 있도록 주기적으로 공개하고 있는지 확인하고 처리한다.							

하위 개념	세부 지표	평가지표	자가 진단표						
			N	VL	L	M	VM	H	VH
	정보 주체 중심의 개인정보 수집 이용동의서 제공	개인정보 수집 이용동의서는 정보 주체가 알기 쉽게 구성하고, 민감정보 등 중요한 부분은 글씨 크기, 굵기, 색상, 밑줄 등을 처리하였는지 확인하고 처리한다.							
	개인정보의 열람·정정·삭제·처리정지의 처리	개인정보의 열람·정정·삭제 및 처리정지에 관한 사항을 안내하고, 절차에 따라 적법·명확하게 처리하고 있는지 확인하고 처리한다.							
	법적 대리인의 동의권 보장	만14세 미만의 아동의 개인정보를 처리하는 경우, 해당 아동의 법정 대리인 동의를 받고, 그 과정에서 법정 대리인이 동의를 거부하거나 동의 의사가 확인되지 않는 경우에는 해당 법정 대리인의 개인정보를 5일 이내 파기하고 있는지 확인하고 처리한다.							
	개인정보 유출 신고 안내	개인정보 침해 사실을 신고하는 방법을 정보 주체에게 안내하고 있는지 확인하고 처리한다.							
조직의 역량	조직의 개인정보보호 관련 규정 준수	우리 조직의 개인정보보호 관련 규정을 마련되어 있는지 확인하고 처리한다.							
	조직의 개인정보 침해사고 지침 준수	우리 조직의 개인정보 침해사고에 대한 지침이 마련되어 있는지 확인하고 처리한다.							
	개인정보보호 전담 조직 및 인력 구성	조직 내 개인정보보호 전담 조직 및 인력이 구성되어 있는지 확인하고 처리한다.							
	개인정보보호 전용 예산 편성	개인정보보호 전용 예산을 편성하고, 개선을 위한 예산 증액 노력을 하고 있는지 확인하고 처리한다.							
	개인정보보호 교육과정 운영 및 평가	임직원 및 수탁자 등 맞춤형 개인정보보호 교육 프로그램을 운영하고 있는지 확인하고 처리한다.							
	성과관리(또는 인센티브제도) 운용	조직구성원의 개인정보 관리역량을 높일 수 있도록 성과관리 또는 인센티브제도 운영하고							

하위 개념	세부 지표	평가지표	자가 진단표						
			N	VL	L	M	VM	H	VH
		있는지 확인하고 처리한다.							
	위반자 제재 및 처벌	우리 조직은 개인정보 오남용, 유출 위반자에 대해서 규정에 따라 투명하고 공정하게 제재와 처벌을 하고 있는지 확인하고 처리한다.							
개인의 역량과 윤리의 식	개인정보보호에 대한 도덕성과 자기통제	우리 조직의 개인정보보호 관련 규정과 처벌 규정을 잘 알고 있고, 자신이 하고 싶은 대로 하고자 하는 충동이 일어날 때 충동을 극복하고자 하는 개인의 노력을 하고 있는지 확인하고 처리한다.							
	개인정보 처리 업무의 사명감	조직구성원으로서 사명감과 직업의식을 가지고 맡은 일에 대한 투철한 책임 의식이 있는지 확인하고 처리한다.							
	개인정보보호 법률 및 제도 이해력과 행동	조직 내 개인정보보호를 위해 규정된 규범을 조직구성원이 개인정보보호에 긍정적이고, 이를 성공적으로 수행할 수 있도록 하고 있는지 확인하고 처리한다.							
	개인정보보호 교육 이수 및 자기 계발	개인정보보호 교육에 어느 정도 관심이 있고, 연 몇 회를 이수하고 있는지 확인하고 자기 계발을 통해 관리능력을 향상하는 노력을 한다.							
	개인정보보호에 대한 자기효능감	개인정보보호 업무를 위해 주어진 정책에 대해 성공적으로 수행할 수 있다는 개인의 기대감 정도(보안정책 인지, 습득, 적용, 적응 정도)를 확인하고 노력한다.							
	개인정보보호 기술 능력과 활용도	개인정보 처리시스템 또는 업무용 단말기의 안전조치 방법을 어느 정도 알고 있고, 이를 수행하고 있는지 확인하고 처리한다.							
	피해 인지력과 문제해결 능력	개인정보 침해사고 대응 절차를 잘 이해하고 있고, 개인정보 침해사고 대응훈련에 적극 참여하여 대응능력을 키우고자 노력하고, 침해사고가 발생하면 즉시 문제를 해결할 수 있다.							

[부록 2] AHP 설문지

설 문 지

NO.			

개인정보 관리 역량성숙도 모델 중요도 평가를 위한 AHP 설문지

안녕하십니까? 귀하와 귀하의 무궁한 발전을 기원합니다.

본 연구목적은 개인정보 취급자가 자기주도형으로 개인정보 관리 역량성숙도를 높이고자 지표를 AHP 기법을 활용하여, 항목별로 주요 요인을 도출하고 각 요인 간 전문가 집단의 평가를 통한 AHP를 이용 중요도를 파악 후 최종 결정요인을 분석하며 상대적 중요도가 높은 요인을 찾기 위한 설문입니다.

본 설문은 응답의 일관성이 낮은 경우 설문이 무효화가 되오니 신중하게 응답해 주시기 바랍니다.

본 조사에서 습득된 개인의 비밀은 통계법 제13조 및 제14조 규정에 의해 엄격히 보호되며 통계 목적 이외의 사용을 금지하고 있습니다.

바쁘신 와중에도 소중한 시간을 내어 주신 여러분께 감사드리고 항상 행복하시길 기원합니다.

감사합니다.

2022년 1월

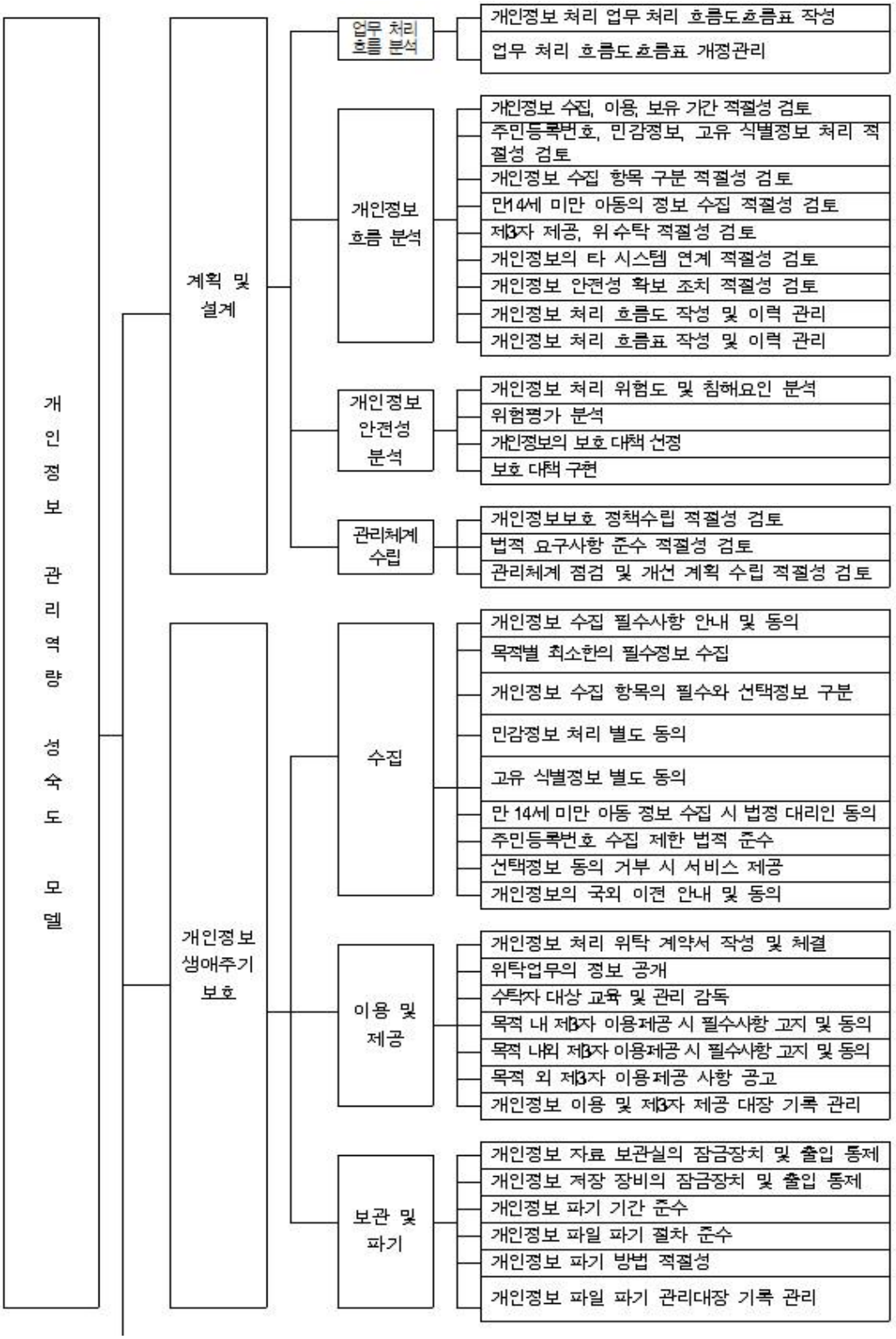
제주대학교 대학원 융합정보보안학협동과정

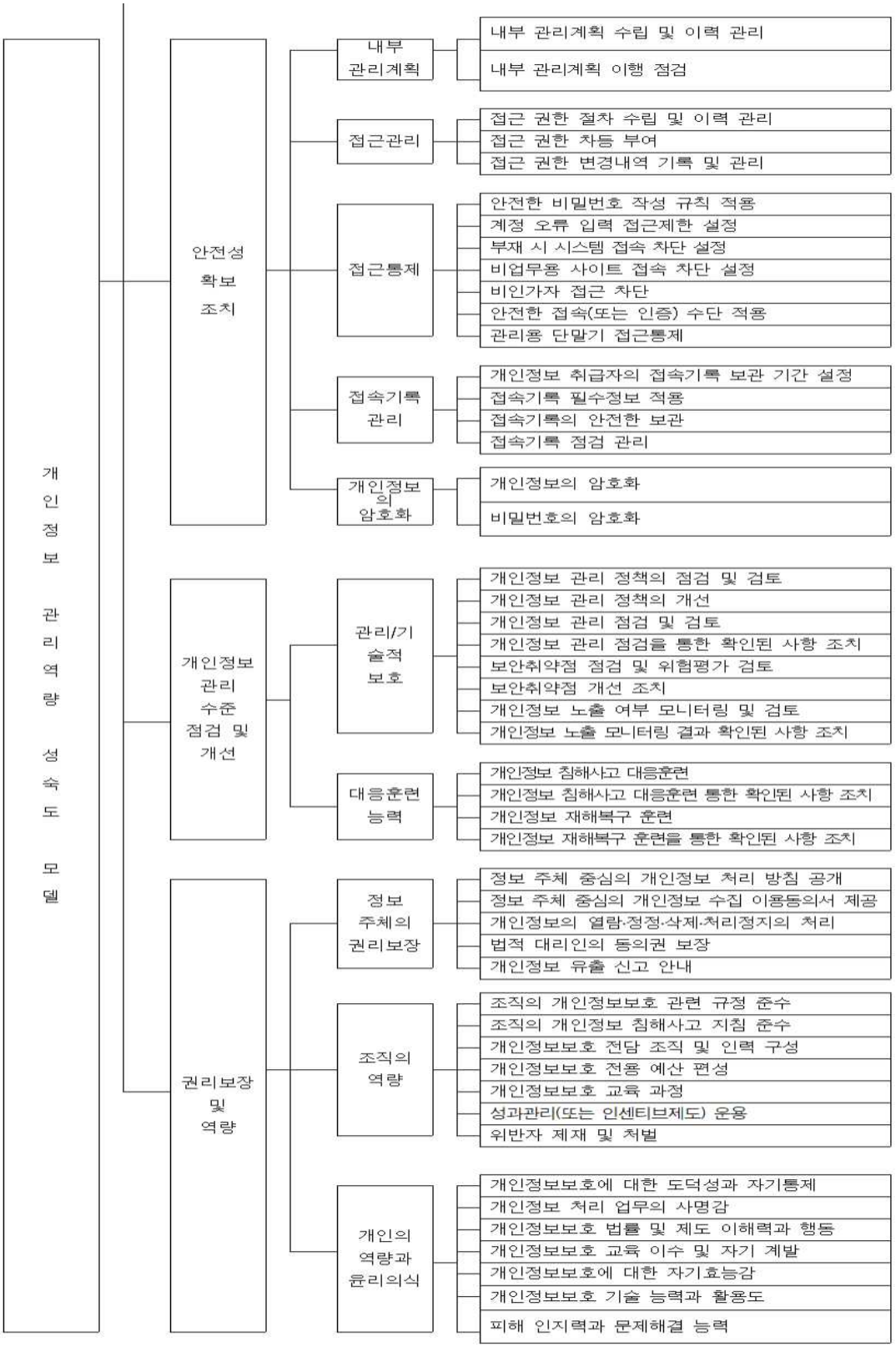
연 구 자 : 오 상 익
지도교수 : 박 남 제

응답대상 : 개인정보보호 전문가 및 경력자
문의사항 : 오 상 익(raitsu58@jejunu.ac.kr, 010- -)

※ 본 설문에 관한 문의사항이나, 응답결과의 송부는 위의 연락처로 주시기 바랍니다.

□ **‘개인정보 관리 역량성숙도 모델의 구조’** 입니다.





설 문 응 답 방 법

※ 귀하의 생각과 가장 일치하는 항목에 '○' 또는 '√'표를 해주시기 바랍니다.

예시)

평가항목(a)	중요도																	평가항목(b)
	절대중요		매우중요		중요		약간중요		같다		약간중요		중요		매우중요		절대중요	
	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
개인정보보호에 대한 도덕성과 자기통제														V				개인정보 처리 업무의 사명감
개인정보보호에 대한 도덕성과 자기통제													V					개인정보보호 법률 및 제도 이해력과 행동
개인정보보호에 대한 도덕성과 자기통제												V						개인정보보호 교육 이수 및 자기 계발

□ **'상위개념'**에 대한 중요도 평가입니다. 평가항목 중 가장 중요하다고 생각하는 항목에 'V' 또는 '○'로 표시해주세요.

평가항목(a)	중요도																	평가항목(b)
	절대중요		매우중요		중요		약간중요		같다		약간중요		중요		매우중요		절대중요	
	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
사전 계획 및 설계																		개인정보 생애주기의 보호
사전 계획 및 설계																		안전성 확보 조치
사전 계획 및 설계																		개인정보 관리 수준 점검 및 개선
사전 계획 및 설계																		권리보장 및 윤리역량
개인정보 생애주기의 보호																		안전성 확보 조치
개인정보 생애주기의 보호																		개인정보 관리 수준 점검 및 개선
개인정보 생애주기의 보호																		권리보장 및 윤리역량
안전성 확보 조치																		개인정보 관리 수준 점검 및 개선
안전성 확보 조치																		권리보장 및 윤리역량
개인정보 관리 수준 점검 및 개선																		권리보장 및 윤리역량

□ **'하위개념'**에 대한 중요도 평가입니다. 아래의 설명을 읽고, 평가항목 중 가장 중요하다고 생각하는 항목에 'V' 또는 '○'로 표시해주세요.

하위 개념	세부 지표	설명
업무처리 흐름 분석	개인정보 처리 업무처리 흐름도·흐름표 작성	처리하려는 업무 흐름도 및 흐름표를 작성하였는지 확인하고 처리한다.
	업무처리 흐름도·흐름표 개정관리	업무 흐름도 및 흐름표는 최신 상태로 유지되고 있는지 확인하고 처리한다.
개인정보 흐름 분석	개인정보 수집, 이용, 보유기간 적절성 검토	개인정보를 수집하는 경우 목적에 필요한 최소한의 범위에서만 수집하도록 계획하고, 개인정보 보유기간을 명확한 근거에 의하여 정하고 있는지 확인하고 처리한다.
	주민등록번호, 민감정보, 고유 식별정보 처리 적절성 검토	주민등록번호 수집 시 법령에 근거하고 있으며, 인터넷 홈페이지는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있도록 계획하고, 민감정보, 고유 식별정보를 처리하는 경우 다른 개인정보의 처리에 대한 동의와 별도로 구분하여 동의받도록 계획하고 있는지 확인하고 처리한다.
	개인정보 수집 항목 구분 적절성 검토	개인정보를 수집하는 경우 필수항목과 선택항목을 분리하고 선택적으로 동의할 수 있는 사항에 동의하지 아니하여도 서비스 이용이 가능하도록 계획하고 있는지 확인하고 처리한다.
	만 14세 미만의 아동 정보수집 적절성 검토	만 14세 미만의 아동 개인정보 수집 시, 법정대리인에게 동의받도록 계획하고 있는지 확인하고 처리한다.
	제3자 제공, 위·수탁 적절성 검토	제3자 제공에 관한 사항을 정보 주체에게 알리고 받도록 계획하고, 위수탁 업무인지 여부를 확인하고 처리한다.
	개인정보의 타 시스템 연계 적절성 검토	개인정보 처리 업무가 타 시스템과 연계되는지 검토하고 적절하게 연계되도록 계획하고 있는지 확인하고 처리한다.
	개인정보 안전성 확보 조치 적절성 검토	개인정보의 안전성 확보 조치 계획을 명확한 근거에 의하여 수립하고 있는지 확인하고 처리한다.
	개인정보 처리 흐름도 작성 및 이력 관리	개인정보 처리 흐름도 작성 및 이력 관리하고 있는지 확인하고 처리한다.
	개인정보 처리 흐름표 작성 및 이력 관리	개인정보 처리 흐름표 작성 및 이력 관리하고 있는지 확인하고 처리한다.

하위 개념	세부 지표	설명
개인정보 안전성 분석	개인정보 처리 위험도 및 침해요인 분석	개인정보 처리에 따른 위험도 및 침해요인을 분석하고 처리한다.
	개인정보 위험평가 분석	개인정보 처리에 따른 위험도 및 침해요인 결과에 따라 위험평가를 분석하고 처리한다.
	개인정보의 보호 대책 선정	개인정보의 개인정보 위험평가 분석 결과를 바탕으로 보호 대책을 수립하고 처리한다.
	개인정보의 보호 대책 구현	개인정보의 보호 대책 수립 결과를 바탕으로 보호 이행 대책을 구현하고 처리한다.
관리체계 수립	개인정보보호 정책 수립 적절성 검토	개인정보보호 정책, 조직, 예산이 적절하게 수립하고 있는지를 확인하고 처리한다.
	법적 요구사항 준수 적절성 검토	개인정보 처리 업무 관련 법적 요구사항을 검토하고 준수 절차를 수립하여 처리한다.
	관리체계 점검 및 개선 계획 수립 적절성 검토	관리체계 수립 결과를 바탕으로 보호조치 개선 방안이 계획되어 있는지 확인하고 처리한다.
수집	개인정보 수집 필수사항 안내 및 동의	개인정보 수집 시 4가지 필수사항(수집 목적, 수집 항목, 보유 및 이용 기간, 동의 거부권 및 거부 시 불이익)을 안내하고 동의받고 있는지 확인하고 처리한다.
	목적별 최소한의 필수정보 수집	목적별 최소한의 필수정보만 수집하고 있는지 확인하고 처리한다.
	개인정보 수집 항목의 필수와 선택정보 구분	개인정보 수집 항목을 필수정보와 선택정보를 구분하여 동의받고 있는지 확인하고 처리한다.
	민감정보 처리 별도 동의	민감정보 처리를 위해 별도 동의받고 있는지 확인하고 처리한다.
	고유 식별정보 별도 동의	고유 식별정보(여권번호, 운전면허번호, 외국인등록번호) 수집할 때 별도의 동의를 받고 있는지 확인하고 처리한다.
	만 14세 미만의 아동의 정보수집 시 법정 대리인 동의	만 14세 미만의 아동 개인정보 수집 시, 법정 대리인에게 동의받고 있는지 확인하고 처리한다.
	주민등록번호 수집 제한 법적 준수	법률에서 구체적으로 처리를 요구하거나 허용하는 경우를 제외하고 주민등록번호를 처리하지 않고 있는지 확인하고 처리한다.
	선택정보 동의 거부 시 서비스 제공	뉴스레터, 마케팅, 홍보를 위한 개인정보 수집에 동의하지 않더라도 기본적인 서비스를 제공하고 있는지 확인하고 처리한다.
	개인정보의 국외 이전 안내 및 동의	개인정보의 국외 이전 시, 정보 주체에게 알리고 동의받고 있는지 확인하고 처리한다.

하위 개념	세부 지표	설명
이용 및 제공	개인정보 처리 위탁 계약서 작성 및 체결	개인정보의 처리 업무를 위탁하는 경우, 개인정보 위탁계약서를 작성하고 있는지 확인하고 처리한다.
	위탁업무의 정보 공개	위탁업무의 내용과 수탁자(위탁받아 처리하는 자)를 공개하고 있는지 확인하고 처리한다.
	수탁자 대상 교육 및 관리 감독	수탁자에 대한 관리·감독을 수행하고 있는지 확인하고 처리한다.
	목적 내 제3자 이용·제공 시 필수사항 고지 및 동의	수집하는 개인정보를 목적 내 제3자에게 제공 시 필수 고지항목(제공받는 자, 이용목적, 개인정보 항목, 보유 및 이용 기간, 동의 거부권 및 거부 시 불이익 내용)을 안내하고 동의받고 있는지 확인하고 처리한다.
	목적 외 제3자 이용·제공 시 필수사항 고지 및 동의	목적 외 제3자 이용·제공 시 필수 고지항목(제공받는 자, 이용목적, 개인정보 항목, 보유 및 이용 기간, 동의 거부권 및 거부 시 불이익 내용)을 안내하고 동의받고 있는지 확인하고 처리한다.
	목적 외 제3자 이용·제공 사항 공고	공공기관은 개인정보의 목적 외 이용 또는 제3자 제공에 관한 사항에 관한 공고를 하고 있는지 확인하고 처리한다.
	개인정보 이용 및 제3자 제공 대장 기록 관리	목적 외 제3자 이용·제공 사항을 관리대장에 기록 관리하고 있는지 확인하고 처리한다.
보관 및 파기	개인정보 자료 보관실의 잠금장치 및 출입 통제	개인정보 자료를 잠금장치가 된 캐비닛 등 안전한 장소에 보관하고 있는지 확인하고 처리한다.
	개인정보 저장 장비의 잠금장치 및 출입 통제	개인정보를 저장하고 있는 전산장비는 잠금장치 및 출입 통제가 되어 있는지 확인하고 처리한다.
	개인정보 파기 기간 준수	보유기간이 경과 되거나 처리목적 달성된 개인정보는 보유 및 이용 기간 종료 후 5일 이내에 즉시 파기하고 있는지 확인하고 처리한다.
	개인정보 파일 파기 절차 준수	개인정보 파일 파기 시 개인정보보호 책임자의 승인 절차를 준수하는지 확인하고 처리한다.
	개인정보 파기 방법 적절성	개인정보 파기 시 복원·재생할 수 없는 형태로 완전하게 파기하는지 확인하고 처리한다.
	개인정보 파일 파기 관리대장 기록 관리	개인정보 파기에 관한 사항을 기록하고 관리하고 있는지 확인하고 처리한다.

하위 개념	세부 지표	설명
내부 관리계획	내부 관리계획 수립 및 이력 관리	개인정보의 안전한 처리를 위한 내부 관리계획을 수립하고 이력 관리하고 있는지 확인하고 처리한다.
	내부 관리계획 이행점검 및 개선	안전한 처리를 위한 내부 관리계획에 대한 이행점검을 반기 1회 이상 하고 있는지 확인하고 처리한다.
접근관리	접근권한 절차 수립 및 이력 관리	개인정보 처리시스템의 중요도(민감도) 및 업무연관성 등을 고려하여 담당자별 차등 접근권한 절차를 마련하고 이력 관리하고 있는지 확인하고 처리한다.
	접근권한 차등 부여	개인정보 처리시스템에 대한 접속 권한을 업무수행 개인정보 취급자에게만 개인별(ID)별로 부여하였는지 확인하고 처리한다.
	접근권한 변경내역 기록 및 관리	개인정보 처리시스템 접근권한의 부여·변경·말소 내역을 기록하고, 최소 3년간 이를 보관하고 있는지 확인하고 처리한다.
접근통제	안전한 비밀번호 작성 규칙 적용	개인정보 처리시스템 접속 시 안전한 비밀번호 작성 규칙을 적용하고 있는지 확인하고 처리한다.
	계정 오류 입력 접근제한 설정	계정정보(ID) 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 접근을 제한하고 있는지 확인하고 처리한다.
	부재 시 시스템 접속 차단 설정	일정 시간 이상 업무처리하지 않는 경우 시스템 접속을 차단하고 있는지 확인하고 처리한다.
	비업무용 사이트 접속 차단 설정	파일 공유용 P2P, 웹하드, 도박 등 유해사이트 접속을 차단하고 있는지 확인하고 처리한다.
	비인가자 접근 차단	비인자자가 관리용 기기에 접근하여 임의 조작 못하도록 조치하고 있는지 확인하고 처리한다.
	안전한 접속(또는 인증) 수단 적용	개인정보 처리시스템에 접속 시 안전한 접속 수단이나 안전한 인증수단을 적용하고 있는지 확인하고 처리한다.
	관리용 단말기 접근통제	관리용 단말기가 본래 목적 외로 사용되지 않도록 조치하고 있는지 확인하고 처리한다.

하위 개념	세부 지표	설명
접속기록 관리	개인정보 취급자의 접속기록 보관 기간 설정	개인정보 취급 업무담당자의 접속기록을 최소 1년 이상(5만 명 이상의 개인정보를 처리하거나, 고유 식별정보 또는 민감정보를 처리하는 경우는 2년 이상) 보관하고 있는지 확인하고 처리한다.
	접속기록 필수정보 적용	개인정보 취급자 및 처리 업무를 확인할 수 있도록 개인정보 취급자의 계정, 접속일시, 접속지 정보, 처리한 정보 주체 정보, 수행업무(조회, 다운로드 등) 등을 확인할 수 있도록 하였는지 확인하고 처리한다.
	접속기록의 안전한 보관	개인정보 처리시스템 접속기록이 위·변조 및 도난, 분실되지 않도록 안전하게 보관하고 있는지 확인하고 처리한다.
	접속기록 점검 관리	개인정보의 오남용, 분실·유출·도난·변조 또는 훼손 등을 대응을 위해 접속기록을 월 1회 이상 점검 및 후속 조치를 하고 있는지 확인하고 처리한다.
개인정보의 암호화	개인정보의 암호화	고유 식별정보(주민등록번호, 여권번호 등), 비밀번호, 바이오 정보(지문, 얼굴 등)가 암호화되어 있는지 확인하고 처리한다.
	비밀번호의 암호화	비밀번호는 일방향 암호화를 적용하여 저장되는지 확인하고 처리한다.
관리/기술적 보호	개인정보 관리 정책의 점검 및 검토	개인정보 처리 방침, 관련 계획 및 지침, 가이드, 매뉴얼 등 관련 정책서가 법적 준거성과 현실에 맞게 수립되어 있는지를 연 1회 이상 점검하고 보완 조치계획을 하고 있는지 확인하고 처리한다.
	개인정보 관리 정책의 개선	개인정보 처리 방침, 관련 계획 및 지침, 가이드, 매뉴얼 등 관련 정책서가 법적 준거성과 현실에 맞게 수립하였는지 점검한 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.
	개인정보 관리 점검 및 검토	개인정보 생애주기, 안전성 확보 조치 등 개인정보 관리실태를 연 1회 이상 점검하고 보완 조치계획을 하고 있는지 확인하고 처리한다.
	개인정보 관리 점검결과 확인된 사항 조치	개인정보 생애주기, 안전성 확보 조치 등 개인정보 관리실태 점검 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.
	보안취약점 점검 및 위험평가 검토	개인정보 처리시스템 또는 홈페이지를 통해 해킹 사고가 발생하지 않도록 연 1회 이상 취약점 점검을 수행하고 위험분석 평가, 보완 조치계획을 하고 있는지 확인하고 처리한다.

하위 개념	세부 지표	설명
	보안취약점 개선 조치	개인정보 처리시스템 또는 홈페이지 보안취약점 점검 점검한 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.
	개인정보 노출 여부 모니터링 및 검토	홈페이지, 개인정보 처리시스템을 통해 개인정보 노출 여부를 월 1회 이상 모니터링하고 보완 조치계획을 하고 있는지 확인하고 처리한다.
	개인정보 노출 모니터링 결과 확인된 사항 조치	개인정보 노출 여부 모니터링 점검한 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.
대응훈련 능력	개인정보 침해사고 대응훈련	개인정보 유출 사고 발생 시 개인정보 유출 사고 대응계획에 따라 신속히 대응하여 그 피해를 최소화하기 위해 개인정보 침해사고 대응 훈련을 실시하고, 결과에 따른 보완 조치계획을 하고 있는지 확인하고 처리한다.
	개인정보 침해사고 대응훈련 통한 확인된 사항 조치	개인정보 침해사고 대응훈련 결과에 따른 필요한 보완 조치하였는지 확인하고 처리한다.
	개인정보 재해복구 훈련	재해재난 발생 시 개인정보 처리시스템 보호를 위해 수립된 위기 대응 매뉴얼에 따라 모의훈련을 실시하고 보완 조치계획을 하고 있는지 확인하고 처리한다.
	개인정보 재해복구 훈련을 통한 확인된 사항 조치	개인정보 처리시스템 재해복구 훈련 결과에 따른 필요한 보완 조치를 하였는지 확인하고 처리한다.
정보 주체의 권리보장	정보 주체 중심의 개인정보 처리 방침 공개	개인정보 처리 방침을 정보 주체가 알기 쉽게 필수사항을 모두 투명·명확하게 포함하여 수립하고, 홈페이지 등 정보 주체가 쉽게 확인할 수 있도록 주기적으로 공개하고 있는지 확인하고 처리한다.
	정보 주체 중심의 개인정보 수집 이용동의서 제공	개인정보 수집 이용동의서는 정보 주체가 알기 쉽게 구성하고, 민감정보 등 중요한 부분은 글씨 크기, 굵기, 색상, 밑줄 등을 처리하였는지 확인하고 처리한다.
	개인정보의 열람·정정·삭제·처리정지의 처리	개인정보의 열람·정정·삭제 및 처리정지에 관한 사항을 안내하고, 절차에 따라 적법·명확하게 처리하고 있는지 확인하고 처리한다.
	법적 대리인의 동의권 보장	만14세 미만의 아동의 개인정보를 처리하는 경우, 해당 아동의 법정 대리인 동의를 받고, 그 과정에서 법정 대리인이 동의를 거부하거나 동의 의사가 확인되지 않는 경우에는 해당 법정 대리인의 개인정보를 5일 이내 파기하고 있는지 확인하고 처리한다.
	개인정보 유출 신고 안내	개인정보 침해 사실을 신고할 수 있는 방법을 정보 주체에게 안내하고 있는지 확인하고 처리한다.

하위 개념	세부 지표	설명
조직의 역량	조직의 개인정보보호 관련 규정 준수	우리 조직의 개인정보보호 관련 규정을 마련되어 있는지 확인하고 처리한다.
	조직의 개인정보 침해사고 지침 준수	우리 조직의 개인정보 침해사고에 대한 지침이 마련되어 있는지 확인하고 처리한다.
	개인정보보호 전담 조직 및 인력 구성	조직 내 개인정보보호 전담 조직 및 인력이 구성되어 있는지 확인하고 처리한다.
	개인정보보호 전용 예산 편성	개인정보보호 전용 예산을 편성하고, 개선을 위한 예산 증액 노력을 하고 있는지 확인하고 처리한다.
	개인정보보호 교육과정 운영 및 평가	임직원 및 수탁자 등 맞춤형 개인정보보호 교육 프로그램을 운영하고 있는지 확인하고 처리한다.
	성과관리(또는 인센티브 제도) 운용	조직구성원의 개인정보 관리역량을 높일 수 있도록 성과관리 또는 인센티브제도를 운영하고 있는지 확인하고 처리한다.
	위반자 제재 및 처벌	우리 조직은 개인정보 오남용, 유출 위반자에 대해서 규정에 따라 투명하고 공정하게 제재와 처벌을 하고 있는지 확인하고 처리한다.
개인의 역량과 윤리의식	개인정보보호에 대한 도덕성과 자기통제	우리 조직의 개인정보보호 관련 규정과 처벌 규정을 잘 알고 있고, 자신이 하고 싶은 대로 하고자 하는 충동이 일어날 때 충동을 극복하고자 하는 개인의 노력을 하고 있는지 확인하고 처리한다.
	개인정보 처리 업무의 사명감	조직구성원으로서 사명감과 직업의식을 가지고 맡은 일에 대한 투철한 책임 의식이 있는지 확인하고 처리한다.
	개인정보보호 법률 및 제도 이해력과 행동	조직 내 개인정보보호를 위해 규정된 규범을 조직구성원이 개인정보보호에 긍정적이고, 이를 성공적으로 수행할 수 있도록 하고 있는지 확인하고 처리한다.
	개인정보보호 교육 이수 및 자기 계발	개인정보보호 교육에 어느 정도 관심이 있고, 연 몇 회를 이수하고 있는지 확인하고 자기계발을 통해 관리능력을 향상시키는 노력을 한다.
	개인정보보호에 대한 자기효능감	개인정보보호 업무를 위해 주어진 정책에 대해 성공적으로 수행할 수 있다는 개인의 기대감 정도(보안정책 인지, 습득, 적용, 적응 정도)를 확인하고 노력한다.
	개인정보보호 기술 능력과 활용도	개인정보 처리시스템 또는 업무용 단말기의 안전조치 방법을 어느 정도 알고 있고, 이를 수행하고 있는지 확인하고 처리한다.
	피해 인지력과 문제해결 능력	개인정보 침해사고 대응 절차를 잘 이해하고 있고, 개인정보 침해사고 대응훈련에 적극 참여하여 대응능력을 키우고자 노력하고, 침해사고가 발생하면 즉시 문제를 해결할 수 있다.

가. **‘하위개념’**의 중요도 평가

하위 개념	평가항목	중요도																	평가항목
		절대중요		매우중요		중요		약간중요		같다		약간중요		중요		매우중요		절대중요	
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
사전 계획 및 설계단계	업무처리 흐름 분석																		개인정보 흐름 분석
	업무처리 흐름 분석																		개인정보 안전성 분석
	업무처리 흐름 분석																		개인정보 영향평가
	개인정보 흐름 분석																		개인정보 안전성 분석
	개인정보 흐름 분석																		개인정보 영향평가
	개인정보 안전성 분석																		개인정보 영향평가
개인정보 생애주기 보호	수집																		이용 및 제공
	수집																		보관 및 파기
	이용 및 제공																		보관 및 파기
안전성 확보 조치	내부 관리계획																		접근관리
	내부 관리계획																		접근통제
	내부 관리계획																		접속기록 관리
	내부 관리계획																		개인정보의 암호화
	접근관리																		접근통제
	접근관리																		접속기록 관리
	접근관리																		개인정보의 암호화
	접근통제																		접속기록 관리
	접근통제																		개인정보의 암호화
	접속기록 관리																		개인정보의 암호화
개인정보 관리 수준 점검 및 개선	관리/기술적 보호																		대응훈련 능력
권리보장 및 윤리역량	정보 주체의 권리보장																		조직의 역량
	정보 주체의 권리보장																		개인의 역량 및 윤리
	조직의 역량																		개인의 역량 및 윤리

□ **‘세부 지표’ 평가항목**의 중요도 평가

하위 개념	평가항목	중요도																	평가항목
		절대중요		매우중요		중요		약간중요		같다		약간중요		중요		매우중요		절대중요	
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
업무처리 흐름 분석	업무처리 흐름도.흐름표 작성																		업무처리 흐름도.흐름표 개정 관리
개인정보 흐름 분석	개인정보 수집, 이용, 보유기간 적절성 검토																		주민등록번호, 민감정보, 고유식별정보 처리 적절성 검토
	개인정보 수집, 이용, 보유기간 적절성 검토																		개인정보 수집 항목 구분 적절성 검토
	개인정보 수집, 이용, 보유기간 적절성 검토																		민감정보, 고유식별정보처리 적절성 검토
	개인정보 수집, 이용, 보유기간 적절성 검토																		만 14세 미만의 아동 정보수집 적절성 검토
	개인정보 수집, 이용, 보유기간 적절성 검토																		제3자 제공, 위·수탁 적절성 검토
	개인정보 수집, 이용, 보유기간 적절성 검토																		개인정보 안전성 확보 조치 적절성 검토
	개인정보 수집, 이용, 보유기간 적절성 검토																		개인정보 처리 흐름도 작성 및 이력 관리
	개인정보 수집, 이용, 보유기간 적절성 검토																		개인정보 처리 흐름표 작성 및 이력 관리
	주민등록번호, 민감정보, 고유식별정보 처리 적절성 검토																		민감정보, 고유식별정보처리 적절성 검토
	주민등록번호, 민감정보, 고유식별정보 처리 적절성 검토																		만 14세 미만의 아동 정보수집 적절성 검토
	주민등록번호, 민감정보, 고유식별정보 처리 적절성 검토																		제3자 제공, 위·수탁 적절성 검토

하위 개념	평가항목	중요도																	평가항목
		절대중요		매우중요		중요		약간중요		같다		약간중요		중요		매우중요		절대중요	
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
	주민등록번호, 민감정보, 고유식별정보 처리 적절성 검토																		개인정보 안전성 확보 조치 적절성 검토
	주민등록번호, 민감정보, 고유식별정보 처리 적절성 검토																		개인정보 처리 흐름도 작성 및 이력 관리
	주민등록번호, 민감정보, 고유식별정보 처리 적절성 검토																		개인정보 처리 흐름표 작성 및 이력 관리
	개인정보 수집 항목 구분 적절성 검토																		민감정보, 고유식별정보처리 적절성 검토
	개인정보 수집 항목 구분 적절성 검토																		만 14세 미만의 아동 정보수집 적절성 검토
	개인정보 수집 항목 구분 적절성 검토																		제3자 제공, 위·수탁 적절성 검토
	개인정보 수집 항목 구분 적절성 검토																		개인정보 안전성 확보 조치 적절성 검토
	개인정보 수집 항목 구분 적절성 검토																		개인정보 처리 흐름도 작성 및 이력 관리
	개인정보 수집 항목 구분 적절성 검토																		개인정보 처리 흐름표 작성 및 이력 관리
	민감정보, 고유식별정보처리 적절성 검토																		만 14세 미만의 아동 정보수집 적절성 검토
	민감정보, 고유식별정보처리 적절성 검토																		제3자 제공, 위·수탁 적절성 검토
	민감정보, 고유식별정보처리 적절성 검토																		개인정보 안전성 확보 조치 적절성 검토

하위 개념	평가항목	중요도																	평가항목
		절대중요		매우중요		중요		약간중요		같다		약간중요		중요		매우중요		절대중요	
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
	민감정보, 고유식별정보처리 적절성 검토																		개인정보 처리 흐름도 작성 및 이력 관리
	민감정보, 고유식별정보처리 적절성 검토																		개인정보 처리 흐름표 작성 및 이력 관리
	만 14세 미만의 아동 정보수집 적절성 검토																		제3자 제공, 위·수탁 적절성 검토
	만 14세 미만의 아동 정보수집 적절성 검토																		개인정보 안전성 확보 조치 적절성 검토
	만 14세 미만의 아동 정보수집 적절성 검토																		개인정보 처리 흐름도 작성 및 이력 관리
	만 14세 미만의 아동 정보수집 적절성 검토																		개인정보 처리 흐름표 작성 및 이력 관리
	제3자 제공, 위·수탁 적절성 검토																		개인정보 안전성 확보 조치 적절성 검토
	제3자 제공, 위·수탁 적절성 검토																		개인정보 처리 흐름도 작성 및 이력 관리
	제3자 제공, 위·수탁 적절성 검토																		개인정보 처리 흐름표 작성 및 이력 관리
	개인정보 안전성 확보 조치 적절성 검토																		개인정보 처리 흐름도 작성 및 이력 관리
	개인정보 안전성 확보 조치 적절성 검토																		개인정보 처리 흐름표 작성 및 이력 관리
	개인정보 처리 흐름도 작성 및 이력 관리																		개인정보 처리 흐름표 작성 및 이력 관리

하위 개념	평가항목	중요도																	평가항목
		절대중요		매우중요		중요		약간중요		같다		약간중요		중요		매우중요		절대중요	
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
개인정보 안전성 분석	개인정보 위험평가 분석																		개인정보 처리 위험도 및 침해요인 분석
	개인정보 위험평가 분석																		개인정보의 보호 대책 선정
	개인정보 위험평가 분석																		개인정보의 보호 대책 구현
	개인정보 처리 위험도 및 침해요인 분석																		개인정보의 보호 대책 선정
	개인정보 처리 위험도 및 침해요인 분석																		개인정보의 보호 대책 구현
	개인정보의 보호 대책 선정																		개인정보의 보호 대책 구현
개인정보 영향평가	개인정보 영향평가 대상여부 검토																		법적 요구사항 준수 적절성 검토
	개인정보 영향평가 대상여부 검토																		관리체계 점검 및 개선 계획 수립 적절성 검토
	법적 요구사항 준수 적절성 검토																		관리체계 점검 및 개선 계획 수립 적절성 검토

하위 개념	평가항목	중요도																	평가항목
		절대중요		매우중요		중요		약간중요		같다		약간중요		중요		매우중요		절대중요	
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
수집	개인정보 수집 필수사항 안내 및 동의																		목적별 최소한의 필수정보 수집
	개인정보 수집 필수사항 안내 및 동의																		개인정보 수집 항목의 필수와 선택정보 구분
	개인정보 수집 필수사항 안내 및 동의																		민감정보 처리 별도 동의
	개인정보 수집 필수사항 안내 및 동의																		고유 식별정보 별도 동의
	개인정보 수집 필수사항 안내 및 동의																		만 14세 미만의 아동의 정보수집 시 법정 대리인 동의
	개인정보 수집 필수사항 안내 및 동의																		주민등록번호 수집 제한 법적 준수
	개인정보 수집 필수사항 안내 및 동의																		선택정보 동의 거부 시서비스 제공
	개인정보 수집 필수사항 안내 및 동의																		개인정보의 국외 이전 안내 및 동의
	목적별 최소한의 필수정보 수집																		개인정보 수집 항목의 필수와 선택정보 구분
	목적별 최소한의 필수정보 수집																		민감정보 처리 별도 동의
	목적별 최소한의 필수정보 수집																		고유 식별정보 별도 동의
	목적별 최소한의 필수정보 수집																		만 14세 미만의 아동의 정보수집 시 법정 대리인 동의

하위 개념	평가항목	중요도																	평가항목
		절대중요		매우중요		중요		약간중요		같다		약간중요		중요		매우중요		절대중요	
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
	목적별 최소한의 필수정보 수집																		주민등록번호 수집 제한 법적 준수
	목적별 최소한의 필수정보 수집																		선택정보 동의 거부 시서비스 제공
	목적별 최소한의 필수정보 수집																		개인정보의 국외 이전 안내 및 동의
	개인정보 수집 항목의 필수와 선택정보 구분																		민감정보 처리 별도 동의
	개인정보 수집 항목의 필수와 선택정보 구분																		고유 식별정보 별도 동의
	개인정보 수집 항목의 필수와 선택정보 구분																		만 14세 미만의 아동의 정보수집 시 법정 대리인 동의
	개인정보 수집 항목의 필수와 선택정보 구분																		주민등록번호 수집 제한 법적 준수
	개인정보 수집 항목의 필수와 선택정보 구분																		선택정보 동의 거부 시서비스 제공
	개인정보 수집 항목의 필수와 선택정보 구분																		개인정보의 국외 이전 안내 및 동의
	민감정보 처리 별도 동의																		고유 식별정보 별도 동의
	민감정보 처리 별도 동의																		만 14세 미만의 아동의 정보수집 시 법정 대리인 동의
	민감정보 처리 별도 동의																		주민등록번호 수집 제한 법적 준수

하위 개념	평가항목	중요도																	평가항목
		절대중요		매우중요		중요		약간중요		같다		약간중요		중요		매우중요		절대중요	
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
	민감정보 처리 별도 동의																		선택정보 동의 거부 시서비스 제공
	민감정보 처리 별도 동의																		개인정보의 국외 이전 안내 및 동의
	고유 식별정보 별도 동의																		만 14세 미만의 아동의 정보수집 시 법정 대리인 동의
	고유 식별정보 별도 동의																		주민등록번호 수집 제한 법적 준수
	고유 식별정보 별도 동의																		선택정보 동의 거부 시서비스 제공
	고유 식별정보 별도 동의																		개인정보의 국외 이전 안내 및 동의
	만 14세 미만의 아동의 정보수집 시 법정 대리인 동의																		주민등록번호 수집 제한 법적 준수
	만 14세 미만의 아동의 정보수집 시 법정 대리인 동의																		선택정보 동의 거부 시서비스 제공
	만 14세 미만의 아동의 정보수집 시 법정 대리인 동의																		개인정보의 국외 이전 안내 및 동의
	주민등록번호 수집 제한 법적 준수																		선택정보 동의 거부 시서비스 제공
	주민등록번호 수집 제한 법적 준수																		개인정보의 국외 이전 안내 및 동의
	선택정보 동의 거부 시서비스 제공																		개인정보의 국외 이전 안내 및 동의

하위 개념	평가항목	중요도																	평가항목
		절대중요		매우중요		중요		약간중요		같다		약간중요		중요		매우중요		절대중요	
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
이용 및 제공	개인정보 처리 위탁 계약서 작성 및 체결																		위탁업무의 정보 공개
	개인정보 처리 위탁 계약서 작성 및 체결																		수탁자 대상 교육 및 관리 감독
	개인정보 처리 위탁 계약서 작성 및 체결																		목적 내 제3자 이용·제공 시 필수사항 고지 및 동의
	개인정보 처리 위탁 계약서 작성 및 체결																		목적 외 제3자 이용·제공 시 필수사항 고지 및 동의
	개인정보 처리 위탁 계약서 작성 및 체결																		목적 외 제3자 이용·제공 사항 공고
	개인정보 처리 위탁 계약서 작성 및 체결																		개인정보 이용 및 제3자 제공 대장 기록 관리
	위탁업무의 정보 공개																		수탁자 대상 교육 및 관리 감독
	위탁업무의 정보 공개																		목적 내 제3자 이용·제공 시 필수사항 고지 및 동의
	위탁업무의 정보 공개																		목적 외 제3자 이용·제공 시 필수사항 고지 및 동의
	위탁업무의 정보 공개																		목적 외 제3자 이용·제공 사항 공고
	위탁업무의 정보 공개																		개인정보 이용 및 제3자 제공 대장 기록 관리
	수탁자 대상 교육 및 관리 감독																		목적 내 제3자 이용·제공 시 필수사항 고지 및 동의

하위 개념	평가항목	중요도																	평가항목
		절대중요		매우중요		중요		약간중요		같다		약간중요		중요		매우중요		절대중요	
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
	수탁자 대상 교육 및 관리 감독																		목적 외 제3자 이용·제공 시 필수사항 고지 및 동의
	수탁자 대상 교육 및 관리 감독																		목적 외 제3자 이용·제공 사항 공고
	수탁자 대상 교육 및 관리 감독																		개인정보 이용 및 제3자 제공 대장 기록 관리
	목적 내 제3자 이용·제공 시 필수사항 고지 및 동의																		목적 외 제3자 이용·제공 시 필수사항 고지 및 동의
	목적 내 제3자 이용·제공 시 필수사항 고지 및 동의																		목적 외 제3자 이용·제공 사항 공고
	목적 내 제3자 이용·제공 시 필수사항 고지 및 동의																		개인정보 이용 및 제3자 제공 대장 기록 관리
	목적 외 제3자 이용·제공 시 필수사항 고지 및 동의																		목적 외 제3자 이용·제공 사항 공고
	목적 외 제3자 이용·제공 시 필수사항 고지 및 동의																		개인정보 이용 및 제3자 제공 대장 기록 관리
	목적 외 제3자 이용·제공 사항 공고																		개인정보 이용 및 제3자 제공 대장 기록 관리

하위 개념	평가항목	중요도																	평가항목
		절대중요		매우중요		중요		약간중요		같다		약간중요		중요		매우중요		절대중요	
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
보관 및 파기	개인정보 자료 보관실의 잠금장치 및 출입 통제																		개인정보 저장 장비의 잠금장치 및 출입 통제
	개인정보 자료 보관실의 잠금장치 및 출입 통제																		개인정보 파기 기간 준수
	개인정보 자료 보관실의 잠금장치 및 출입 통제																		개인정보 파일 파기 절차 준수
	개인정보 자료 보관실의 잠금장치 및 출입 통제																		개인정보 파기 방법 적절성
	개인정보 자료 보관실의 잠금장치 및 출입 통제																		개인정보 파일 파기 관리대장 기록 관리
	개인정보 저장 장비의 잠금장치 및 출입 통제																		개인정보 파기 기간 준수
	개인정보 저장 장비의 잠금장치 및 출입 통제																		개인정보 파일 파기 절차 준수
	개인정보 저장 장비의 잠금장치 및 출입 통제																		개인정보 파기 방법 적절성
	개인정보 저장 장비의 잠금장치 및 출입 통제																		개인정보 파일 파기 관리대장 기록 관리
	개인정보 파기 기간 준수																		개인정보 파일 파기 절차 준수
	개인정보 파기 기간 준수																		개인정보 파기 방법 적절성
	개인정보 파기 기간 준수																		개인정보 파일 파기 관리대장 기록 관리
	개인정보 파일 파기 절차 준수																		개인정보 파기 방법 적절성
	개인정보 파일 파기 절차 준수																		개인정보 파일 파기 관리대장 기록 관리
	개인정보 파기 방법 적절성																		개인정보 파일 파기 관리대장 기록 관리

하위 개념	평가항목	중요도																	평가항목
		절대중요		매우중요		중요		약간중요		같다		약간중요		중요		매우중요		절대중요	
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
내부관리 계획	내부 관리계획 수립 및 이력 관리																		내부 관리계획 이행점검 및 개선
접근관리	접근권한 절차 수립 및 이력 관리																		접근권한 차등 부여
	접근권한 절차 수립 및 이력 관리																		접근권한 변경내역 기록 및 관리
	접근권한 차등 부여																		접근권한 변경내역 기록 및 관리
접근통제	안전한 비밀번호 작성 규칙 적용																		계정 오류 입력 접근제한 설정
	안전한 비밀번호 작성 규칙 적용																		부재 시 시스템 접속 차단 설정
	안전한 비밀번호 작성 규칙 적용																		비업무용 사이트 접속 차단 설정
	안전한 비밀번호 작성 규칙 적용																		비인가자 접근 차단
	안전한 비밀번호 작성 규칙 적용																		안전한 접속(또는 인증) 수단 적용
	안전한 비밀번호 작성 규칙 적용																		관리용 단말기 접근통제
	계정 오류 입력 접근제한 설정																		부재 시 시스템 접속 차단 설정
	계정 오류 입력 접근제한 설정																		비업무용 사이트 접속 차단 설정
	계정 오류 입력 접근제한 설정																		비인가자 접근 차단
	계정 오류 입력 접근제한 설정																		안전한 접속(또는 인증) 수단 적용

하위 개념	평가항목	중요도																	평가항목
		절대중요		매우중요		중요		약간중요		같다		약간중요		중요		매우중요		절대중요	
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
	계정 오류 입력 접근제한 설정																		관리용 단말기 접근통제
	비업무용 사이트 접속 차단 설정																		비인가자 접근 차단
	비업무용 사이트 접속 차단 설정																		안전한 접속(또는 인증) 수단 적용
	비업무용 사이트 접속 차단 설정																		관리용 단말기 접근통제
	비인가자 접근 차단																		안전한 접속(또는 인증) 수단 적용
	비인가자 접근 차단																		관리용 단말기 접근통제
	안전한 접속(또는 인증) 수단 적용																		관리용 단말기 접근통제
접속기록 관리	개인정보 취급자의 접속기록 보관 기간 설정																		접속기록 필수정보 적용
	개인정보 취급자의 접속기록 보관 기간 설정																		접속기록의 안전한 보관
	개인정보 취급자의 접속기록 보관 기간 설정																		접속기록 점검 관리
	접속기록 필수정보 적용																		접속기록의 안전한 보관
	접속기록 필수정보 적용																		접속기록 점검 관리
	접속기록의 안전한 보관																		접속기록 점검 관리

하위 개념	평가항목	중요도																	평가항목
		절대중요		매우중요		중요		약간중요		같다		약간중요		중요		매우중요		절대중요	
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
개인정보의 암호화	개인정보의 암호화																		비밀번호의 암호화
관리/기술적 보호	개인정보 관리 정책의 점검 및 검토																		개인정보 관리 정책의 개선
	개인정보 관리 정책의 점검 및 검토																		개인정보 관리 점검 및 검토
	개인정보 관리 정책의 점검 및 검토																		개인정보 관리 점검결과 확인된 사항 조치
	개인정보 관리 정책의 점검 및 검토																		보안취약점 점검 및 위험평가 검토
	개인정보 관리 정책의 점검 및 검토																		보안취약점 개선 조치
	개인정보 관리 정책의 점검 및 검토																		개인정보 노출 여부 모니터링 및 검토
	개인정보 관리 정책의 점검 및 검토																		개인정보 노출 모니터링 결과 확인된 사항 조치
	개인정보 관리 정책의 개선																		개인정보 관리 점검 및 검토
	개인정보 관리 정책의 개선																		개인정보 관리 점검결과 확인된 사항 조치
	개인정보 관리 정책의 개선																		보안취약점 점검 및 위험평가 검토
	개인정보 관리 정책의 개선																		보안취약점 개선 조치
	개인정보 관리 정책의 개선																		개인정보 노출 여부 모니터링 및 검토
	개인정보 관리 정책의 개선																		개인정보 노출 모니터링 결과 확인된 사항 조치
	개인정보 관리 점검 및 검토																		개인정보 관리 점검결과 확인된 사항 조치

하위 개념	평가항목	중요도																	평가항목
		절대중요		매우중요		중요		약간중요		같다		약간중요		중요		매우중요		절대중요	
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
	개인정보 관리 점검 및 검토																		보안취약점 점검 및 위험평가 검토
	개인정보 관리 점검 및 검토																		보안취약점 개선 조치
	개인정보 관리 점검 및 검토																		개인정보 노출 여부 모니터링 및 검토
	개인정보 관리 점검 및 검토																		개인정보 노출 모니터링 결과 확인된 사항 조치
	개인정보 관리 점검결과 확인된 사항 조치																		보안취약점 점검 및 위험평가 검토
	개인정보 관리 점검결과 확인된 사항 조치																		보안취약점 개선 조치
	개인정보 관리 점검결과 확인된 사항 조치																		개인정보 노출 여부 모니터링 및 검토
	개인정보 관리 점검결과 확인된 사항 조치																		개인정보 노출 모니터링 결과 확인된 사항 조치
	보안취약점 점검 및 위험평가 검토																		보안취약점 개선 조치
	보안취약점 점검 및 위험평가 검토																		개인정보 노출 여부 모니터링 및 검토
	보안취약점 점검 및 위험평가 검토																		개인정보 노출 모니터링 결과 확인된 사항 조치
	보안취약점 개선 조치																		개인정보 노출 여부 모니터링 및 검토
	보안취약점 개선 조치																		개인정보 노출 모니터링 결과 확인된 사항 조치
	개인정보 노출 여부 모니터링 및 검토																		개인정보 노출 모니터링 결과 확인된 사항 조치

하위 개념	평가항목	중요도																	평가항목
		절대중요		매우중요		중요		약간중요		같다		약간중요		중요		매우중요		절대중요	
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
대응훈련 능력	개인정보 침해사고 대응훈련																		개인정보 침해사고 대응훈련을 통한 확인된 사항 조치
	개인정보 침해사고 대응훈련																		개인정보 재해복구 훈련
	개인정보 침해사고 대응훈련																		개인정보 재해복구 훈련을 통한 확인된 사항 조치
	개인정보 침해사고 대응훈련을 통한 확인된 사항 조치																		개인정보 재해복구 훈련
	개인정보 침해사고 대응훈련을 통한 확인된 사항 조치																		개인정보 재해복구 훈련을 통한 확인된 사항 조치
	개인정보 재해복구 훈련																		개인정보 재해복구 훈련을 통한 확인된 사항 조치
정보 주체의 권리보장	정보 주체 중심의 개인정보 처리 방침 공개																		정보 주체 중심의 개인정보 수집 이용동의서 제공
	정보 주체 중심의 개인정보 처리 방침 공개																		개인정보의 열람·정정·삭제·처리 정지의 처리
	정보 주체 중심의 개인정보 처리 방침 공개																		법적 대리인의 동의권 보장
	정보 주체 중심의 개인정보 처리 방침 공개																		개인정보 유출 신고 안내
	정보 주체 중심의 개인정보 수집 이용동의서 제공																		개인정보의 열람·정정·삭제·처리 정지의 처리
	정보 주체 중심의 개인정보 수집 이용동의서 제공																		법적 대리인의 동의권 보장
	정보 주체 중심의 개인정보 수집 이용동의서 제공																		개인정보 유출 신고 안내
	개인정보의 열람·정정·삭제·처리정지의 처리																		법적 대리인의 동의권 보장
	개인정보의 열람·정정·삭제·처리정지의 처리																		개인정보 유출 신고 안내
	법적 대리인의 동의권 보장																		개인정보 유출 신고 안내

하위 개념	평가항목	중요도																	평가항목
		절대중요		매우중요		중요		약간중요		같다		약간중요		중요		매우중요		절대중요	
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
조직의 역량	조직의 개인정보보호 관련 규정																		조직의 개인정보 침해사고 지침
	조직의 개인정보보호 관련 규정																		개인정보보호 전담 조직 및 인력 구성
	조직의 개인정보보호 관련 규정																		개인정보보호 전용 예산 편성
	조직의 개인정보보호 관련 규정																		개인정보보호 교육과정 운영 및 평가
	조직의 개인정보보호 관련 규정																		성과관리(또는 인센티브제도)운용
	조직의 개인정보보호 관련 규정																		위반자 제재 및 처벌
	조직의 개인정보 침해사고 지침																		개인정보보호 전담 조직 및 인력 구성
	조직의 개인정보 침해사고 지침																		개인정보보호 전용 예산 편성
	조직의 개인정보 침해사고 지침																		개인정보보호 교육과정 운영 및 평가
	조직의 개인정보 침해사고 지침																		성과관리(또는 인센티브제도)운용
	조직의 개인정보 침해사고 지침																		위반자 제재 및 처벌
	개인정보보호 전담 조직 및 인력 구성																		개인정보보호 전용 예산 편성
	개인정보보호 전담 조직 및 인력 구성																		개인정보보호 교육과정 운영 및 평가
	개인정보보호 전담 조직 및 인력 구성																		성과관리(또는 인센티브제도)운용

하위 개념	평가항목	중요도																	평가항목
		절대중요		매우중요		중요		약간중요		같다		약간중요		중요		매우중요		절대중요	
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
	개인정보보호 전담 조직 및 인력 구성																		위반자 제재 및 처벌
	개인정보보호 전용 예산 편성																		개인정보보호 교육과정 운영 및 평가
	개인정보보호 전용 예산 편성																		성과관리(또는 인센티브제도)운용
	개인정보보호 전용 예산 편성																		위반자 제재 및 처벌
	개인정보보호 교육과정 운영 및 평가																		성과관리(또는 인센티브제도)운용
	개인정보보호 교육과정 운영 및 평가																		위반자 제재 및 처벌
	성과관리(또는 인센티브제도)운용																		위반자 제재 및 처벌
개인의 역량 및 윤리의식	개인정보보호에 대한 도덕성과 자기통제																		개인정보 처리 업무의 사명감
	개인정보보호에 대한 도덕성과 자기통제																		개인정보보호 법률 및 제도 이해력과 행동
	개인정보보호에 대한 도덕성과 자기통제																		개인정보보호 교육 이수 및 자기 계발
	개인정보보호에 대한 도덕성과 자기통제																		개인정보보호에 대한 자기효능감
	개인정보보호에 대한 도덕성과 자기통제																		개인정보보호 기술 능력과 활용도
	개인정보보호에 대한 도덕성과 자기통제																		피해 인지력과 문제해결 능력
	개인정보 처리 업무의 사명감																		개인정보보호 법률 및 제도 이해력과 행동
	개인정보 처리 업무의 사명감																		개인정보보호 교육 이수 및 자기 계발

하위 개념	평가항목	중요도																	평가항목
		절대중요		매우중요		중요		약간중요		같다		약간중요		중요		매우중요		절대중요	
		9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
	개인정보 처리 업무의 사명감																		개인정보보호에 대한 자기효능감
	개인정보 처리 업무의 사명감																		개인정보보호 기술 능력과 활용도
	개인정보 처리 업무의 사명감																		피해 인지력과 문제해결 능력
	개인정보보호 법률 및 제도 이해력과 행동																		개인정보보호 교육 이수 및 자기 계발
	개인정보보호 법률 및 제도 이해력과 행동																		개인정보보호에 대한 자기효능감
	개인정보보호 법률 및 제도 이해력과 행동																		개인정보보호 기술 능력과 활용도
	개인정보보호 법률 및 제도 이해력과 행동																		피해 인지력과 문제해결 능력
	개인정보보호 교육 이수 및 자기 계발																		개인정보보호에 대한 자기효능감
	개인정보보호 교육 이수 및 자기 계발																		개인정보보호 기술 능력과 활용도
	개인정보보호 교육 이수 및 자기 계발																		피해 인지력과 문제해결 능력
	개인정보보호에 대한 자기효능감																		개인정보보호 기술 능력과 활용도
	개인정보보호에 대한 자기효능감																		피해 인지력과 문제해결 능력
	개인정보보호 기술 능력과 활용도																		피해 인지력과 문제해결 능력

귀하의 성실한 답변에 감사드립니다.

감사의 글

직장 생활하면서 새로운 도전을 위해 석사, 박사과정에 문을 두드렸을 때가 엊그제 같은데 어느새 5년이라는 시간이 지나고 이 논문이 나오기까지 많은 분의 도움을 받았습니다. 부족한 저를 이 자리까지 올 수 있게 도움을 주신 분들이 없었다면 논문이 나올 수 없었기에 이 자리를 빌려 감사의 마음을 전하고자 합니다.

먼저 부족한 저를 지금까지 아낌없는 믿음과 지도로 이끌어 주신 박남제 교수님께 진심으로 감사드립니다. 아직도 많이 부족하지만, 교수님의 가르침을 항상 마음속에 새기고 계속 발전하는 모습을 보이도록 노력하겠습니다. 또한, 논문심사 시 날카로운 지적과 따뜻한 조언을 해주신 변영철 교수님과 조정원 교수님, 강구홍 교수님, 박명환 교수님께 진심으로 감사드립니다. 박사과정 동안 함께 고민하고 많은 도움을 주면서 동고동락한 정원치 박사, 정유진 박사, 정성욱 박사 모두에게도 감사하다는 말을 전하고 싶습니다.

언제나 한결같이 믿어주시고 아낌없는 사랑을 베풀어주신 부모님 그리고 인자하시고 정이 많으신 장인어른과 장모님께도 감사의 마음을 전하며 기쁨을 함께 나누고자 합니다. 마지막으로 부족한 저에게 석사와 박사과정 동안 불평불만 없이 학비를 지원해주면서도 항상 곁에서 배려와 사랑으로 큰 힘이 되어준 이 세상에서 가장 사랑하는 아내, 건강하게 잘 큰 큰아들, 박사과정 동안 “아빠는 축구 같이 해준다고 해놓고 안 해주고, 잔소리만 한다.”고 불평하면서도 밝고 올곧게 잘 자라준 막내아들에게 지면으로나마 미안함과 감사의 마음을 전하며 그동안 노고에 조금이나마 보답하고자 하는 심정으로 이 논문을 바칩니다.

논문이 완성되기까지 주변에서 끝없는 격려와 도움을 주신 많은 분께 이 글을 통해 감사의 마음을 전하며, 앞으로 더욱 발전할 수 있도록 끊임없이 노력하겠습니다.

감사합니다.

2022년 11월

오 상 익