

# 개인정보의 관리적 · 기술적 보호조치 기준의 상대적 중요도에 관한 연구

## A Study on the Relative Importance of the Administrative and Technical Measures for the Personal Information Protection

김영희(Young Hee Kim)\*, 국광호(Kwang Ho Kook)\*\*

### 초 록

정보화 환경에서 개인정보의 수집 · 활용이 증가됨에 따라 개인의 프라이버시를 침해하는 개인정보 유출 및 오 · 남용되는 사고가 계속적으로 증가하고 있다. 이에 국가차원에서 개인정보 대량 유출사고 재발 방지 및 2차 피해 예방을 위해 관련 법률 · 규정 강화와 관련 법제를 바탕으로 개인정보취급기관에서 지켜야할 개인정보에 관한 안전성 확보에 필요한 보호조치 기준을 마련하였다. 이와 함께 관련 기준 항목별 중요도에 따른 우선순위 및 정량화에 대한 개선 연구도 함께 진행되었다. 그러나 법률에서 밝힌 안전성 확보조치 기준 및 개선연구의 경우 기준 항목에 대한 전문가 집단의 업무영역, 전문도등의 특성에 따른 분류와 차이점을 반영하지 않아 개인정보 처리기관에서 기준적용에 대한 합리적인 의사결정에 어려움이 존재한다. 따라서 이번 연구에서는 법률에서 요구한 개인정보의 안전성 확보조치 기준 평가를 위해 다양한 전문가의 참여와 각 전문가별 업무특성, 경험에 따른 가중치를 부여하고, 비모수적 검정을 통해 각 전문가 집단별 의견이 통계적으로 차이가 있는지 검정하여 좀 더 신뢰성 있는 기준별 가중치를 선별하여 개인정보 취급기관에서 우선 적용 가능한 합리적인 기준 제안을 목적으로 한다.

### ABSTRACT

As the collection and use of personal information increases, the accidents that abuse and leak personal information are continuously increasing. The nation has established new laws and strengthened related laws for the prevention of the mass leakage of personal information and the secondary damage due to the leaked personal information. The nation also established the guidelines that need to be implemented by the institutions handling personal information for the safety of the personal information. For the efficient implementation of guidelines under the limited time and resources, it is necessary to establish the priorities between guidelines. This paper compares the relative importance of the guidelines by AHP (Analytic Hierarchy Process) technique. We performed the analysis on two expert groups, the group of consultants working in information security consulting company and the group of information security staffs handling personal information directly in the company. We compared the differences between groups and recommended the relative importances of the guidelines.

**키워드** : 개인정보보호, 비모수 검정, 계층분석과정, 정보보안

Personal Information Protection, Mann-Whitney, AHP, Information Security

\* Department of Industrial and Information Systems Graduate School of Public Policy and Information Technology, Seoul National University of Science and Technology(sorak75@naver.com)

\*\* Corresponding Author, Department of Industrial and Information Systems Engineering, Seoul National University of Science and Technology(khkook@seoultech.ac.kr)

2014년 10월 23일 접수, 2014년 11월 10일 심사완료 후 2014년 11월 17일 게재확정.

## 1. 서 론

정보사회 진입과 고도화에 따른 정보화 역기능으로 사이버 위협과 해킹 및 다양한 형태의 침해 사례가 증가되고 이와 함께 개인 인격 주체성에 심각한 침해를 입히는 개인정보 유출 문제가 사회적 문제로 대두되고 있다[22]. 이에 국가 차원에서 개인 정보주체의 인격 주체성 보호와 자기결정권 강화를 위해 관련 법제를 강화하고 개인정보처리가 개인정보를 취급함에 있어 관리적·기술적으로 취해야 할 최소한의 안전성 확보 조치 기준을 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」과 「신용정보의 이용 및 보호에 관한 법률」, 공공부문의 「공공기관의 개인정보보호에 관한 법률」 등의 대표 법률과 이를 통합하는 일반법 형태의 「개인정보보호법」을 통해 고시하고 따르도록 하고 있다[15]. 해당 법률에서 밝힌 개인정보에 관한 관리적·기술적 보호조치를 위한 기준 고시의 주요 목적은 개인정보를 보호함에 있어 최소한의 지켜야 할 기준을 제시하고 이를 통해 개인정보 취급기관에서 개인정보의 수집·유출·관리 및 오·남용으로부터 안전한 보호를 위해 필수적으로 관리하고 지켜야 할 기준을 규정하고 강제화하는데 목적을 둔다[14]. 이와 함께 기준 고시를 바탕으로 일괄적으로 요구하고 있는 개인정보의 안전성 확보조치 기준 개선을 위해 기준항목별 상대적 중요한 항목을 도출하여 우선 적용해야 될 기준을 산정, 정량화하고 선 조치되어야 할 모델 도출에 관한 개선 연구도 진행되었다[9]. 하지만 법률에서 밝힌 안전성 확보조치 기준 및 개선 연구의 경우 기준 항목을 평가한 전문가 집단의 업무 영역, 전문도 등의 특성에 대

한 분류가 되지 않고 동일한 관점에서 평가되어, 개인정보 취급기관에서 기준 적용을 위한 의사결정 방향에 대한 신뢰성을 주지 못하였다. 따라서 이번 연구에서는 법률에서 요구한 개인정보의 안전성 확보조치 기준의 우선순위 평가를 위해 다양한 전문가의 참여와 각 전문가별 업무 특성, 전문도 등에 따른 가중치를 부여하고, 비모수적 검정 통해 전문가 집단 간 통계적으로 차이가 있는지 검정하고 좀 더 신뢰성 있는 기준별 가중치 도출을 통해 개인정보 취급기관에서 좀 더 합리적인 의사결정이 가능한 기준 모델 제안을 목적으로 한다.

## 2. 이론적 고찰

개인정보유출 및 도용, 침해에 따른 피해 구제, 상담 건수가 계속적으로 증가하고 있으며, 국내의 IT 인프라 성장 추세와 더불어 e-비즈니스 환경에서 개인정보의 비즈니스 측면의 가치와 자산으로써의 중요성이 되어 개인정보 침해 사례가 계속적으로 증가 하고 있다. 이처럼 개인정보의 보유와 활용이 기업의 비즈니스 연속성에 중대한 영향을 주는 핵심 관리 대상으로 인식되고 있으며, 개인정보 취급기관에서 또한 개인정보의 보호조치를 위한 투자와 노력을 기울이고 있다. 이와 함께 국가 차원에서도 개인정보보호 관련 법률을 강화하고 취급자가 따라야 할 기준을 마련하고 있다[12].

### 2.1 개인정보 정의와 보호의 필요성

국·내외 법률 및 규범에서 정의한 개인정보의 개념을 종합해 보면 생존하는 개인의 사

상, 신상, 재산, 신체, 사회적 지위 등에 관해 손해를 끼칠 수 있는 식별되거나 파악 가능한 정보로 개인의 의사에 반하거나 동의 없이 이용될 경우 개인의 안녕과 이해관계에 손해와 피해를 끼칠 수 있는 정보 총체를 일컫는 것으로 정의할 수 있다[16]. 다시 말해 개인정보를 보호하고 관리하는 목적은 개인의 인격 주체성을 보호하고 이를 통해 개인정보의 오·남용으로부터 개인의 자기결정 강화함으로써 개인의 존엄성 보호와 가치를 높이고 최종적으로 각 개인의 권리와 이익을 지키기 위함이다. 이처럼 개인정보보호의 중요성이 대두됨에 따라 개인정보 취급기관은 개인정보관리를 위한 내부 계획 수립·이행, 보호범위 지정과 함께 개인정보에 대한 수집, 이용 및 폐기에 이르는 전 과정에 대한 관리적·기술적 보호조치 취하고, 개인정보의 안전한 처리와 관리를 위한 감독·점검 및 개인정보침해에 대한 대응·구제 사항을 마련해야 한다[24]. 이와 같이 개인정보 취급기관에서 수집·이용·제공·파기 되고 있는 개인정보의 주요 특성을 살펴보면, 첫째 관리범위의 광의적인 특수성이 존재한다. 개인정보 오·남용에 대한 책임이 개인정보를 취급하는 해당 조직·부서의 책임으로 국한되지 않기 때문에 전사 차원의 개인정보 관리와 보호조치에 최선을 다해야 한다. 둘째 개인정보를 취급함에 있어 다수의 이해관계자가 존재한다. 개인정보를 보호하기 위해 전통적인 정보보안 형태와는 다르게, 개인정보 주체자 및 개인정보를 제공 받아 활용하는 취급자, 이를 다시 위탁·제공 받는 제 3자 등 여러 이해관계자가 존재하므로 일반적인 정보보호 영역보다 넓은 관점에서 관리해야 한다[6]. 셋째 개인정보 취급기관은 개인정보보호에 대한 법

률적 준거성에 대한 책임과 유출에 대한 기업의 유무형의 피해가 존재한다. 개인정보 유출 시 개인정보 이해관계자 및 취급기관에 미치는 악영향 및 파급효과가 일반적인 정보보안 관점과 비교되지 않게 크며 개인정보 유출 기업에 유·무형적으로 나쁜 영향을 미치고, 그 처벌 또한 높기 때문에 관련 법령 및 규정에 대한 준거성 보장이 필요하다[4, 7]. 넷째 해킹 및 침해 사고에 대한 패러다임이 변화되고 있다. 과거 일반적인 과시와 불특정 다수 대상으로 한 해킹 공격에서 현재 의도된 금전적인 이익을 추구하기 위한 개인정보 유출에 초점이 맞춰지고, 공격 기법 또한 지능화되고 고도화 되고 있어 피해 양상과 파급효과가 크게 나타난다[10]. 다섯째 개인정보주체자의 인식 변화에 따른 대응 형태의 변화와 함께 국가 차원에서의 규제 및 처벌이 강화 되고 있다. 과거 침해 사고에 대한 개인정보주체자의 소극적 대응에서 개인정보에 대한 권리와 가치에 대한 중요성을 인식하고 있어 손해배상 청구 및 소송을 통해 보다 적극적으로 대응하고, 국가적으로도 개인정보 유출에 대한 처벌 수위와 규제를 강화하고 기업의 개인정보보호에 대한 투자와 관심을 유도하고 있다. 이에 따라 개인정보 취급기관 또한 개인정보 관리 및 오·남용 방지를 위해 대응책 마련에 노력을 기울이고 있다[5]. 이처럼 개인정보의 다양한 특징에 기인하여 개인정보의 보호와 관리가 선택이 아닌 필수적으로 보호하고 관리해야 되는 중요한 사안인지 알 수 있다.

## 2.2 국내외 개인정보보호 법률 및 현황

정보기술의 발달 및 전산화된 데이터의 국

가적 이동에 따른 개인정보의 중요성이 대두되면서 경제협력개발기구(OECD : Organization for Economic Cooperation and Development)는 1980년대 개인에 대한 사생활 보호와 국가 간 개인정보의 이동에 관한 국제정책에 대한 지침으로 “프라이버시 보호와 개인 데이터의 국제 유통에 관한 가이드라인에 대한 이사회의 권고”가 채택되었다[18]. 이에 각국은 관련 지침을 바탕으로 국가 간 개인정보보호 정책의 상이함에 따른 개인의 사생활이 침해되지 않도록 관련 법제를 마련하고 강화하는데 노력하고 있다[3]. 우리나라의 개인정보보호 관련 법률은 1994년 1월 입법화된 「공공 기관 등의 개인정보보호에 관한 법률」과 2001년 제정된 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 1995년 제정된 「신용정보의 이용 및 보호에 관한 법률」 등을 통해 공공 및 민간부분으로 나뉘어 관리되었으며 내용면에서도 「OECD의 기본 원칙」을 대부분 수용하여 해외 법률과 큰 차이가 없었다[23]. 하지만 대규모 개인정보 유출 사고의 증가로 인한 개인정보주체자의 사생활 및 주체성 침해가 급증하고, 국내 IT 및 환경에 적합하고 공공기관과 민간기관으로 이원화되어 있는 구조를 통합할 수 있는 법률에 대한 요구 사항이 증대되어, 2011년 3월 29일 일반법 형태의 「개인정보보호법」이 제정되고 시행되었다. 해당 법률은 「OECD 기본 8원칙」과 국제적 규범·기준, 국내 타 법령과의 형평성 및 근거를 종합적으로 고려하고 공공, 민간, 온·오프라인, 기업·개인을 아우르는 포괄적인 형태의 일반법으로, 동법의 제정에 따라 개인정보주체자의 기본권 보호와 국민 편의 증대와 환경을 고려한 개인정보의 안전한 이

용을 위한 근거 마련과 함께 개인정보의 안전성 확보에 필요한 기준과 의무를 마련하고 강화한데 중요한 의의가 있다[8]. 이와 함께 개인정보에 대한 최소한의 관리적·기술적 조치 기준을 「개인정보보호법」 및 「정보통신망법」 등에 상세하게 제시하고 있으며, 핵심 내용은 개인정보를 처리함에 있어서 개인정보 처리자가 개인정보의 분실·도난·유출·변조·훼손되지 않도록 취하여야 하는 기준을 정하고 있다.

## 2.3 보호조치 기준 및 기존 연구의 한계

「개인정보보호법」 및 「정보통신망법」 등에서는 개인정보처리자가 개인정보를 사용하고 처리함에 있어 조치하여야 할 관리적·기술적·물리적 조치 사항에 필요한 최소한의 기준 제시하고 있다. 관련 주요 세부 기준은 첫째 내부관리 계획의 수립·시행 관한 항목으로 개인정보보호와 관리를 위한 체계적이고 전사를 통합할 수 있는 계획 수립·이행에 관한 세부기준을 두고 있다. 둘째 접근 권한 관리 항목으로 개인정보처리시스템에 관한 접근관리와 비인가 접근 차단을 통해 개인정보의 오·남용 및 훼손 방지에 관한 세부기준을 두고 있다. 셋째 비밀번호 관리 항목으로 개인정보취급자 및 정보주체자에 대한 안전한 비밀번호 작성규칙 수립에 관한 세부기준을 두고 있다. 넷째 접근통제 시스템 설치 및 운영에 관한 항목으로 정보통신망을 통한 비인가자의 불법적 접근 및 침해 시도 차단을 위한 보안시스템 설치·운영에 관한 세부기준을 두고 있다. 다섯째 개인정보의 암호화에 관한 항목으로 고유 식별 정보, 비밀번호 등과 같은 주요 개인정보

에 대한 불법적인 노출 및 위·변조 방지를 위한 암호에 관한 세부기준을 두고 있다. 여섯째 접속기록의 보관 및 위·변조 방지 항목으로 개인정보취급시스템에 저장된 개인정보의 입·출력, 담당자별 접근내역 보관에 관한 세부기준을 두고 있다. 일곱째 보안 프로그램 설치 및 운영 항목으로 악성 프로그램에 대한 예방 및 치료 목적의 보안 프로그램 설치 및 운영에 관한 세부기준을 두고 있다. 여덟째 물리적 접근 방지 항목의 경우 대량의 개인정보를 보관하고 있는 장소에 대한 출입통제 절차 수립·운영 관한 세부 기준을 두고 있다[14]. 이와 함께 김영희, 국광호[9]는 개인정보보호를 위한 관리적·기술적 조치 기준항목의 시급성, 중요성 등이 고려되지 않고 일괄적으로 요구하고 있는 문제점 해결을 위해 기준항목을 전문가 대상으로 가중치를 평가하고 우선순위를 도출하여 개인정보 취급기업에서 선 조치되어야 될 모델을 제공하고 있다. 하지만 개선 연구 또한 평가자의 전문도, 업무영역 등 경험에 대한 분류가 되지 않아 우선순위 도출에 대한 신뢰성을 주지 못하는 한계점을 가지고 있다. 따라서 이번 연구에서 우선순위 평가를 위해 각 전문가별 업무 특성, 전문도를 고려한 직무 영역별 두 집단으로 나눠 가중치를 부여하고, 비모수적 검정 통해 전문가 집단 간 의견에 대한 통계적으로 차이가 있는지 검정하여 좀 더 신뢰성 있는 우선순위 모델을 제안한다.

### 3. 연구 방법론

본 연구에서는 개인정보보호 전문가별 개인정보보호의 안전성 확보조치 기준 우선순

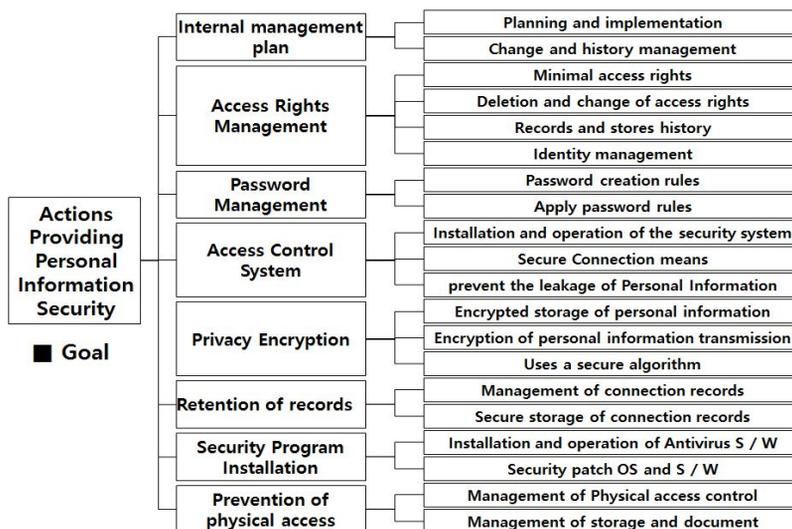
위 제안과 각 전문가별 평가 결과에 대한 차이성 검정을 통해 유의미한 결과 도출을 연구 범위로 한다. 이를 위해 다음의 절차를 거친다. 첫째 평가 기준 도출을 위하여 관련 법령, 기존 문헌을 분석하여 안전성 확보 조치 기준을 도출하고 추가하여 계층화·구조화 한다. 둘째 각 기준별 우선순위 평가를 위해 전문가 집단을 선정하며 그 대상은 지식정보보안컨설팅 전문 업체에서 개인정보보호 관련 컨설팅 수행 경험이 있는 개인정보보호 전문가 집단과 개인정보 취급기관에서 개인정보 보호업무를 담당하는 실무자 집단으로 한다. 이와 함께 각 전문가 집단 별 설문을 진행하고, AHP(Analytical Hierarchy Process) 기법을 통해 개인정보의 안전성 확보조치 기준의 가중치를 도출하였다. 마지막으로 각 전문가 집단에서 평가한 가중치 결과가 통계적으로 차이와 유의성이 존재하는지 확인을 위해 비모수 검정 기법 중의 하나인 Mann-Whitney test를 활용하여 검정을 실시한다.

#### 3.1 우선순위 평가 기준 및 계층화

본 연구에서는 개인정보보호를 위한 기술적·관리적 보호조치 기준의 우선순위 평가 기준 도출을 위해 「개인정보보호법」에서 제시한 개인정보의 안전 확보조치 기준고시 중 개인정보의 안전한 보호에 필요한 기술적·관리적 조치 기준인 3조에서 10조를 활용해 관련 조와 각 세부 항을 선행 연구하고, 이와 함께 평가 기준에 대한 계층 모형을 체계적으로 구조화한 기존 연구의 개인정보의 안전성 확보를 위한 표준 평가 항목을 활용하여 법률적 재해석을 통해 추가 기준 항목을 도출하여

계층화한다. 개인정보의 안전성 확보 조치 기준 계층 구조를 살펴보면 우선순위 제안과 의사결정을 위한 1계층 영역은 내부관리 계획, 접근 권한 관리, 비밀번호 관리, 접근통제 시스템 설치 및 운영, 개인정보의 암호화, 접속 기록의 보관 및 위·변조 방지, 보안 프로그램 설치 및 운영, 물리적 접근 방지 항목이며, 2계층 영역의 경우 1계층 영역별 관리적·기술적으로 개인정보 보호에 필요한 세부 항목으로 구성된다[9]. 이와 함께 개인정보의 안전성 확보조치 기준고시의 추가 해석을 통해 2계층 평가 기준을 분리하고 재 정의하여 전문가집단을 대상으로 검정하였다. 추가된 세부사항으로 1계층 영역의 ‘비밀번호 관리 영역’과 ‘보안 프로그램 설치 및 운영’ 항목을 세분화하였다. 종합하면 각 상위 평가기준에 대한 하위 평가기준 형태로 구성되며 세부사항은 첫째 내부관리 계획은 ①계획수립 및 시행 ②변경 및 이력 관리에 관한 하위 평가항목, 둘째 접근권한 관리는 ①최소한의 접근권한 및

차등 부여 ②접근권한 변경 및 말소 ③내역 기록 및 보관 ④단일 계정 생성 및 공유 금지에 관한 하위 평가항목, 셋째 비밀번호 관리는 ①비밀번호 작성 규칙 수립 ②비밀번호 규칙 시스템구현에 관한 하위 평가항목, 넷째 접근통제 시스템 설치 및 운영 ①보안시스템 설치 및 운영 ②안전한 접속 수단 확보 ③개인정보의 외부 유출 조치에 관한 하위 평가항목, 다섯째 개인정보의 암호화는 ①개인정보의 암호화 저장 ②개인정보 송·수신 시 암호화 ③안전한 알고리즘 사용에 관한 하위 평가항목, 여섯째 접속기록의 보관 및 위·변조방지는 ①접속기록의 보관 및 관리 ②접속 기록의 안전한 보관에 관한 하위 평가항목, 일곱째 보안프로그램 설치 및 운영은 ①백신 S/W 설치·운영 ②OS, S/W보안패치에 관한 하위 평가항목, 여덟째 물리적 접근 방지는 ①출입 통제 절차 수립·운영, ②서류·저장 매체의 안전한 보관에 관한 하위 항목으로 정제화 되어, 다음 <Figure 1> 형태로 도식화 하였다.



<Figure 1> Hierarchy

### 3.2 AHP 분석

본 연구에서는 개인정보의 안전성 확보조치 기준에 대한 우선순위를 평가하기 위해 AHP 기법을 이용해 기준 항목 간의 쌍대 비교(Pair-wise Comparison)를 통해 가중치를 산정하고 우선순위를 도출한다.

AHP 기법은 의사결정이 필요한 문제들의 여러 속성을 계층적으로 분류하고 각 속성의 상대적 중요도를 파악함으로써 최적대안을 찾는 기법으로 1970년대 초 Thomas L. Saaty에 의해 연구되었다. 최적 대안의 선정과 평가를 위해서는 해당 전문가들의 경험적 판단을 정량적인 절차를 거쳐야 되는데, AHP 기법의 경우 평가 기준에 대한 통합적이고 객관적인 검증이 가능하므로 해당 연구의 가중치 판단에 적합하다 할 수 있다[19, 21]. AHP 기법을 통한 의사결정과 관련된 문제를 해결하는 핵심 원리는 첫째 전문가 대상으로 의사결정사항에 대한 문제를 설정하고 여러 요소들 간의 관계를 계층화(hierarchy)한다. 의사결정에 필요한 문제를 주 요인과 세부 요인으로 계층을 구분하여 시각화한다. 둘째 단계는 목표 달성에 필요한 상위계층의 직계 하위계층에 속하는 요소들 간의 쌍대 비교 통해 행렬을 작성한다. 이는 여러 대안에 대한 전문가 평가에 대한 오류 방지와 판단의 용이성을 높이기 위해 구조화한 것이다. 셋째 단계로 각 전문가 집단의 평가요소 간 상대적 가중치 산정과 일관성 검증 단계이다. 이를 위해 Thomas L. Saaty가 개발한 고유벡터를 활용, 평가요소 간 상대적인 중요도에 대한 가중치를 추정하며, 아래와 같은 행태로 표현된다.

$$Aw = nw \text{ 단, } w' = (w_1, w_2, \dots, w_n) \quad (1)$$

그리고 평가자가 벡터  $w$ 을 정확하게 모르고 쌍대 비교를 통해 정확한 가중치 평가할 수 없는 것을 가정하므로 고유근 분해로 벡터  $w$ 을 추정한다.

$$A'w' = \lambda_{\max} W', \lambda_{\max} \text{는 가장 큰 고유치} \quad (2)$$

이와 함께  $\lambda_{\max}$ 는  $n$ 보다 항상 같거나 크기 때문에  $\lambda_{\max}$ 가  $n$ 에 가까울수록 쌍대 비교에 관한 행렬  $A$ 가 오류가 없고 일관성이 있다고 판단할 수 있다.

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

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

마지막으로 의사결정에 필요한 대안을 최종 도출하기 위해 각 계층에서의 가중치를 종합하여 중요도 벡터를 도출한다[20]. 이와 같이 AHP 기법을 활용해 평가요소들 간의 정성적, 정량적 의견을 논리적이고 체계적으로 분석 가능하므로 합리적인 의사결정을 가능하게 한다.

### 3.3 비모수 검정

본 연구에서는 전문가 집단 간의 평가항목 가중치간 의견 차이가 있는지 검정하기 위해 비모수적 검정을 활용해 두 집단의 유의성을 분석한다. 일반적으로 비모수(Nonparametric) 검정은 모수적(Parametric) 검정에 비해 결과

해석과 정보가 제한적이며 정규분포의 가정을 충족시키지 못하지만, 비모수 검정을 활용한 가설검정 시에는 모집단에 대한 가정이 불필요하므로 가정 수립에 대한 오류를 없앨 수 있고, AHP 기법과 같이 전문가 평가에 대한 표본 수가 적고 정규분포를 따르지 않을 시 적용 가능하고 계산이 복잡하지 않는 장점이 존재한다[1, 2, 13]. 이에 비모수 검정을 위해서는 첫째 모집단 Data에 대한 독립변수, 종속변수인지 파악하고 쌍을 이루는지 검토 후 정규성 검정을 한다. 정규성을 만족하면 T-검정을 수행하고 정규성을 충족시키지 못할 경우에는 비모수 검정을 수행한다. 둘째, 두 모집단이 동일하다는 귀무가설  $H_0$ 을 세우고,  $n = n_A + n_B$ 개의 관측 값의 표본을 크기순으로 순서를 부여하고 A 표본의 순위 합  $W_A$ 을 검정한다. 셋째, 귀무가설에 대한 기각역을 검정한다. 귀무가설  $H_0$ , 대립가설  $H_1$ 로 표현한다. A 집단의 평균  $\mu_A$ , B 집단의 평균  $\mu_B$ 을 의미한다. 여기서 귀무가설은 기존에 있는 검정된 가설이며, 대립가설은 새롭게 주장하고자 하는 가설이다.

$$\text{귀무가설 } H_0: \mu_A = \mu_B \quad (5)$$

$$\text{대립가설 } H_1: \mu_A \neq \mu_B \quad (6)$$

넷째, 최종 검정 후 도출된 P값의 결과를 통해 귀무가설 또는 대립가설이 채택될지 결정한다, 다시 말해 귀무가설이 옳다는 가정하에 도출된 결과보다 실제 도출될 유의 확률과 검정 이전에 설정한 유의수준 간의 비교를 통한 유의성을 판단하고 가설을 선택한다. 이에 본 연구에서는 개인정보의 안정성 확보

조치 기준별 우선순위 평가를 위한 개인정보 보호 컨설팅전문가 집단과 개인정보 취급기관의 개인정보보호실무자 집단 간 상대적 중요도 평가 가중치가 통계적으로 유의한 특성이 존재하는지 분석하기 위해 비모수 검정(Mann-Whitney)을 수행하였으며 유의수준은  $P = 0.05$ 로 적용하였다.

#### 4. 중요도 분석 모델

본 장에서는 중요도 분석 모델에 따라 법률·규제에 및 기존 선행연구 분석을 통해 개선된 계층모형을 수립하고, 두 집단의 전문가 대상으로 AHP 기법 기반의 설문을 통해, 개인정보의 안전성 확보조치 기준에 대한 가중치를 산정하고, 각 전문가 집단의 평가 결과에 대해 유의성 분석을 위하여 비모수 검정 기법 중의 하나인 Mann-Whitney test를 활용한다.

##### 4.1 가중치 분석 및 결과

본 연구는 선행연구에서 밝힌 표준 평가 항목을 통해 개선 및 정량화된 계층도에 대해 AHP 설문을 통해 평가항목에 대한 가중치와 우선순위를 도출하였다. 이때, 쌍대 비교를 위한 평가 기준은 <Figure 1>에서 도출한 평가 기준 항목의 중요도에 대해 9점 척도를 사용하여 평가 하였으며, 설문대상은 먼저 개인정보보호 전문가 집단은 지식 정보보안 컨설팅전문 업체에서 기업의 개인정보보호 수준 진단 및 평가에 대한 방법론 및 체계를 포함한 정보보호컨설팅 경험

이 있는 인력을 대상으로 하며, 개인정보보호 실무자 집단은 IT기업 및 공공기관에서 개인정보 관리체계 수립 및 이행과 함께 관리적·기술적 보호조치 실무를 수행하는 인력으로 두 집단 모두 개인정보 관련 지식과 경험이 풍부한 5년 이상의 경력을 보유한 인력으로, 평가기준에 대한 쌍대비교가 가능한 전문지식을 갖췄다고 판단된다. 이와 함께 각 전문가 집단에서 도출된 가중치가 논리적인 오류가 없는지 판단하기 위해 일관성 비율(CR, Consistency Ratio)을 계산하였다. 이렇게 산정된 값 중 일관성 비율이 0.1 미만인 설문은 논리에 오류가 없고 전문가의 평가가 합리적이라고 판단하고, 0.1 이상인 설문은 논리적 오류가 존재하는 설문이라고 판단하여 우선순위 분석에서 제외하였다. 이에 최종적으로 일관성에 오류가 없다고 판단되는, 개인정보보호 컨설팅전문가 집단 설문 11개, 개인정보실무자 집단 10개의 설문에 대해 가중치를 도출하고 평가 하였다. AHP 기법에서는 의사결정에 필요한 전문적 지식과 경험 등 연구 목적에 맞는 전문가의 의견 수렴이 중요하고, 해당 기준에서 집단의 특성이 유의하면 가중치 평가를 위한 규모는 10명 내·외면 충분하고 밝히고 있다[5]. 이와 함께 각 전문가 집단 내 다수의 의견을 통합하기 위해 기하평균을 통한 각 전문가 집단의 가중치를 산정하였다[11]. 개인정보의 관리적·기술적 보호조치 기준에 대한 전문가별 우선순위를 분석결과는 <Table 1>과 같다. 세부사항은 먼저, 개인정보보호 전문가 집단의 경우 1계층에서는 내부관리 계획(0.170) 기준 항목이 가장 높고, 근소하게 개인정보

의 암호화(0.164) 기준 항목, 접근 권한 관리(0.156) 기준 항목 순으로 우선순위가 높고 중요한 항목으로 판단하고 있으며, 1계층과 2계층의 가중치를 반영한 종합 가중치의 경우 내부관리 계획 수립 및 시행 평가 기준(0.106)이 가장 높고 접근 권한에 대한 내역 기록 및 보관(0.016) 기준 항목이 가장 낮은 것으로 판단하고 있다. 둘째, 개인정보보호 실무자 대상의 경우 개인정보의 암호화(0.194) 기준 항목, 접근 권한의 관리(0.188) 기준 항목, 접근통제시스템 설치 및 운영(0.126) 기준 항목 순으로 중요도가 높게 나왔으며, 종합 가중치의 경우 개인정보의 암호화 저장(0.078) 기준 항목이 가장 우선순위가 높고 접근 권한에 대한 내역 기록 및 보관(0.026) 기준 항목이 가장 낮다고 판단하고 있다. 이와 함께 기존 연구[9]에서 밝힌 우선순위의 경우 개인정보의 암호화 기준항목, 접근권한 관리 기준항목이 가장 높고, 물리적 접근 방지 기준항목, 접속기록 보관 및 변조방지 기준항목 순으로 중요도 낮다고 평가하고 있다. 이는 이번 연구에서 우선순위를 평가한 전문가 집단 중 개인정보보호 실무자 집단과 유사한 가중치를 부여하고 있다. 이는 기존 연구에서 평가를 진행한 집단의 특성이 개인정보 실무자 중심으로 치우쳐져 제안된 것으로 판단된다. 이에 따라 본 연구에서는 다양한 전문가별 업무 특성, 전문도를 고려한 가중치 분석을 통해 좀 더 신뢰성 있는 우선순위 도출을 통해 개인정보 취급자가 개인정보를 보호를 위한 관리적 기술적으로 취해야 할 조치 항목들 중 보다 시급하게 적용되어야 할 기준이 제안 되었다.

〈Table 1〉 Weights of Evaluation Items Final

upper level criteria	Lower level criteria	Expert groups			Working Groups				
		Upper Weight	Lower Weight	Total Weight	Rank	Upper Weight	Lower Weight	Total Weight	Rank
Internal management plan	Planning and implementation	0.170	0.622	0.106	1	0.100	0.670	0.067	3
	Change and history management		0.378	0.064	4		0.330	0.033	19
Access Rights Management	Minimal access rights	0.156	0.372	0.058	5	0.188	0.332	0.062	4
	Deletion and change of access rights		0.363	0.057	7		0.263	0.049	12
	Records and stores history		0.101	0.016	20		0.137	0.026	20
	Identity management		0.164	0.026	18		0.268	0.050	10
Password Management	Password creation rules	0.136	0.592	0.081	2	0.120	0.432	0.052	7
	Apply password rules		0.408	0.055	8		0.568	0.068	2
Access Control System	Installation and operation of the security system	0.118	0.318	0.038	15	0.126	0.306	0.039	17
	Secure Connection means		0.302	0.036	16		0.288	0.036	18
	prevent the leakage of Personal Information		0.380	0.045	13		0.406	0.051	8
Privacy Encryption	Encrypted storage of personal information	0.164	0.404	0.066	3	0.194	0.400	0.078	1
	Encryption of personal information transmission		0.301	0.049	10		0.287	0.056	6
	Uses a secure algorithm		0.295	0.048	11		0.313	0.061	5
Retention of records	Management of connection records	0.052	0.539	0.028	17	0.008	0.547	0.048	13
	Secure storage of connection records		0.461	0.024	19		0.453	0.040	16
Security Program Installation	Installation and operation of Antivirus S/W	0.092	0.521	0.048	12	0.094	0.542	0.051	9
	Security patch OS and S/W		0.479	0.044	14		0.458	0.043	14
Prevention of physical access	Management of Physical access control	0.112	0.510	0.057	6	0.090	0.450	0.041	15
	Management of storage and document		0.490	0.055	9		0.550	0.050	11

### 4.2 전문가 집단별 가중치 비교

본 연구에서는 서로 다른 전문분야의 전문가들의 가중치 평가 결과가 집단의 종류에 따라 영향을 받는지 비교 분석하기 위하여 2개의 모집단에 대한 비모수 검정 기법 중의 하나인 Mann-Whitney test를 활용한다. AHP 기법의 경우처럼 제한된 수의 전문가 평가를 통해 표본을 도출하므로 샘플 수가 작고 그 결과 또한 정규분포를 따르지 않아 비모수 검정을 사용한다[1]. 이와 함께 가설 검정을 위해 두 전문가 집단의 집단 간 중앙값(Median)이 차이가 없다는 귀무가설을 설정하고 그에 대한 대립가설로 두 모집단의 중앙값이 차이가 있다는 것을 가정하고 양측 검정을 실행한다. 즉 귀무가설  $H_0$ 는 “두 집단 간 가중치 차이가 없다”, 대립가설  $H_1$ 는 “두 집단 간 가중치 차이가 있다.”라고 가정한다. 그 결과 각 전문가 집단 간 개인정보의 안전성 확보조치 기준 항목 간 유의 확률은 <Table 2>와 같다. 검정 시 유의수준이 0.05 이하일 경우 두 집단 간의 중앙값이 차이가 없다는 귀무가설이 기각되므로 본 연구 또한 유의수준을 0.05로 정의한다.

세부적인 내용은 내부관리 계획, 비밀번호 관리, 개인정보의 암호화 항목은 근사 유의 확률(양측)이 유의수준 0.05보다 작게 나왔으며 이는 통계적으로 두 전문가 집단 간 의견의 차이가 있는 것을 나타낸다.

평가항목 각 전문가별 가중치에 의하면 내부관리 계획 항목과 비밀번호 관리 항목은 개인정보보호 전문가 집단에서 더 높게 나타났으며 개인정보의 암호화 항목은 개인정보보호 실무자 집단의 가중치가 높게 나타났다. 이는 개인정보보호 전문가 집단이 개인정보보호실무자에 비해 개인정보의 관리적·기술적 보호를 위하여 내부관리 계획 및 비밀번호 관리가 상대적으로 더 중요하고, 개인정보보호실무자의 경우 개인정보의 암호화 항목이 개인정보보호 전문가 집단보다 더 중요하게 생각한다고 할 수 있다. 이처럼 각 전문가 집단사이의 가중치 차이가 나는 크게 나는 이유는 이 평가 항목이 개인정보보호를 위한 정책 확립 관점과 유출에 대한 피해 최소화 관점에 따라 나뉘진다고 볼 수 있다. 내부관리 계획 항목의 경우 개인정보 취급기관에서 개인정보 보호활동에 필요한 체계적이고 전사적인 규정 및 정책을 수립 하고 관리 및 이

<Table 2> Significant Probability

	Mann-Whitney	Wilcoxon	Z	p value
Internal management plan	18.00	84.00	-2.605	0.009
Access Rights Management	33.00	88.00	-1.549	0.121
Password Management	27.00	93.00	-1.972	0.049
Access Control System	48.00	114.00	-0.493	0.622
Privacy Encryption	21.00	87.00	-2.394	0.017
Retention of records	51.00	117.00	-0.282	0.778
Security program installation	39.00	94.00	-1.127	0.260
Prevention of physical access	48.000	114.00	-0.493	0.654

행을 목적으로 하는 정책적 항목으로 개인정보 보호보호를 위한 관리적 보안 강화에 초점을 둔 항목이며, 비밀번호 관리 항목의 경우도 이와 유사하게 규칙을 수립하는 정책적인 보안 항목이다, 이와 반대로 개인정보보호 실무자 측면에서 가중치를 높게 준 개인정보암호화 항목의 경우 불가피하게 발생 할 수 있는 내·외부자에 의한 개인정보 위·변조 및 유출·노출 시 피해를 최소화하기 위한 개인정보의 암호화 저장 및 전송에 대한 안전한 보호를 위한 항목으로 개인정보 침해에 대한 피해 최소화를 위한 실무 관점의 평가 기준이다. 즉 개인정보보호 전문가 집단은 개인정보보호를 위해 내부관리 계획, 비밀번호 관리 등 정책 및 관리적 보안을 좀 더 중요하게 생각한다면, 개인정보보호 실무자 집단은 개인정보의 암호화 부분 등 정보 유출 측면의 기술적 보안을 좀 더 중요 시 한다는 것을 확인할 수 있다. 이는 각 전문가 집단의 직무 특성이 반영된 것을 확인할 수 있으며, 개인정보보호 전문가 집단을 대표하는 컨설팅 직무는 개인정보 취급기관에 개인정보보호 컨설팅을 통해 지켜야 할 거버넌스 측면의 기준과 정책 수립·이행 관점으로, 개인정보보호 실무자 집단은 각 기업에서 보안 실무를 함에 있어 개인정보 위·변조 및 유출·노출 등 위협에 대한 최선의 방어적 입장에서 유출에 대한 피해를 최소화 하는 관점에서 중요도를 판단하였다. 이에 개인정보의 안전성 확보를 위해서는 각 전문가 집단의 서로 중요하다고 생각하는 평가항목에 대한 보완과 이해를 통해 개인정보보호의 안전한 관리를 위한 상호 보완적인 노력이 필요할 것으로 보인다. 이번 연구에서는 법률에서 요구한 개

인정보의 안전성 확보조치 기준 평가를 위해 다양한 전문가의 참여와 각 전문가별 업무 특성, 전문도 등에 따른 가중치를 부여하고, 비모수 검정 통해 전문가 집단에 의견에 대한 통계적으로 차이가 있는지 검정하여 좀 더 신뢰성 있는 기준별 가중치를 선별하여 개인정보 취급기관에 적용 가능한 합리적인 기준을 제안하였다.

## 5. 결 론

개인정보의 오·남용 및 유출 방지를 위해 개인정보의 관리적·기술적 안전성 확보 방안을 법령에서 마련을 하고, 효과적으로 기업에 적용하기 위한 기준별 중요도에 따른 우선순위 및 정량화에 대한 개선 연구가 진행되고 있다. 하지만 법률에서 밝힌 안전성 확보조치 기준 및 개선연구의 경우 기준 항목에 대한 전문가 집단의 업무 영역, 전문도 등의 특성에 따른 분류와 차이점을 반영하지 않아 개인정보처리기관에서 우선순위 적용에 대한 합리적인 의사결정에 어려움이 존재한다. 이에 본 연구에서는 먼저 기존 연구에서 밝힌 개인정보의 안전성 확보조치 평가 기준을 바탕으로 관련 문헌과 법률적 해석을 통해 법률에서 명확하게 요구하고 있는 평가 기준을 추가 후 계층화하고, 기존 연구에서 문제점으로 제기한 각 전문직군별 집단을 분리하고 추가 설문을 통해 집단별 경험 및 역량에 따른 가중치를 부여를 통한 우선순위를 도출하였다. 이와 함께 각 개인정보보호 전문가 집단 간 평가 가중치가 통계적으로 유의한 의견의 차이가 존재하는지 검정하기 위해

맨-휘트니(Mann-Whitney)의 U 검정을 통해 의견 차이를 검정하였다. 그 결과 내부관리 계획, 비밀번호 관리, 개인정보의 암호화 항목에 유의수준이 0.05 이하로 차이가 나므로 나타났으며, 유의하다고 검정된 항목의 가중치 결과 보면 개인정보보호 전문가 집단은 내부관리 계획 항목과 비밀번호 관리 항목이, 개인정보보호실무자의 경우 개인정보의 암호화 항목이 상대적으로 더 중요하고 개인정보 취급기관에서 개인정보를 안전하게 관리하기 위해 먼저 선 조치되어야 할 중요한 항목이라 평가하고 있다.

본 연구의 의의는 개인정보 취급기관에서 지켜야 할 개인정보의 안전성 확보 조치 기준에 대한 의견을 다양한 전문가들 대상으로 충분히 수렴하여 좀 더 객관적이며 신뢰성 높은 가중치를 도출하였고, 각 전문가 집단 간 개인정보보호에 대한 시각 차이를 비교 분석하여 개인정보 취급기관에 개인정보를 위한 우선순위별 적용 가능한 합리적인 기준 제안을 목적으로 한다. 이를 바탕으로 개인정보 취급기관에서 개인정보보호를 위한 조치 사항을 이행함에 있어 외부 전문가 집단의 권고 사항과 취급기관 내 실무자 관점에서 의견 차이를 이해하고 두 집단 간의 통합 가중치를 바탕으로 개인정보보호를 위한 우선 조치에 필요한 기준으로 효율적이고 합리적이고 수단으로 활용 가능할 것이다. 하지만 본 연구에서는 몇 가지 한계점이 존재한다. 먼저 평가항목으로 사용된 안정성 확보조치 기준들 간의 법률적 경중에 대한 가중치 및 타 개인정보보호 조치 조항들 간의 상관관계에 대한 종합적인 내용이 반영된 평가 기준을 제시하지 못하였고, AHP 기법 적용을 위

해 설문한 전문가들의 개인적 평가 능력을 동등하게 설정하여 전문가별 능력이 다를 때 평가결과에 대한 신뢰도가 감소할 수 있는 한계점이 존재한다. 이에 따라 향후 연구에서는 전문가의 평가능력에 대한 가중치 반영을 위해 실무경험, 실무지식을 고려한 전문도를 차등 반영 하여 결과의 신뢰성 확보와 함께 개인정보의 안전성 확보 조치기준 이외 개인정보보호를 위해 필요한 다양한 법률적 요구 사항, 타 법률 등을 아우를 수 있는 정량화된 평가 기준이 필요할 것으로 보인다.

---

## References

---

- [1] Choi, S. U., "Implementation of Nonparametric Statistics in the Non-Normal Process," *Journal of the Korea Safety Management and Science*, pp. 573-577, 2012.
- [2] Gibbons, J. D. and Chakraborti, S., *Non-parametric Statistical Inference*, 5 Edition, Chapman and Hall/CRC, 2010.
- [3] Implement the OECD 'Privacy Guidelines' in the Electronic Environment : Focus the internet 1998, <<http://www.oecd.org>>.
- [4] Kim, B. S., "The Legal Justice of Conferring Criminal Negligence on Chief Privacy Officers," *Journal of the Korea Society of IT Services*, Vol. 10, No. 4, pp. 21-32, 2011.
- [5] Kim, D. K. and Kim, O. K., "A Study

- on the Development of Criteria and Priority Orders for Selecting Third Party Logistics Companies,” Journal of the Korean Operations Research and Management Science Society, Vol. 20, No. 2, pp. 161-163, 2003.
- [6] Kim, J. D. and Hwang, S. H., “A Study on Critical Success Factors for Implementing Governance of Personal Information Protection,” Journal of the Korea Institute of Information Security and Cryptology, Vol. 21, No. 5, pp. 97-203, 2011.
- [7] Kim, J. Y., “Analyzing Effects on Firms’ Market Value of Personal Information Security Breaches,” The Journal of Society for e-Business Studies, Vol, 18, No. 1, pp. 1-12, 2013.
- [8] Kim, S. G., “Analysis on Domestic and Foreign Privacy Information Acts to Suggest Directions for Developing Korean Privacy Information Protection Act,” Journal of the Korea Institute of Information Security and Cryptology, Vol. 22. No. 5. pp. 1091-1102, 2012.
- [9] Kim, Y. H. and Kook, K. H., “A Study on Priority Ranking of Actions Providing Personal Information Security,” Convergence Security Journal, Vol, 14. No. 4, pp. 9-17, 2014.
- [10] Korea Communications Commission, National Information Society Agency, “15th hacking prevention workshop,” National Information Society Agency, 2011.
- [11] LEE, C. H., “group decision making,” sejongbooks, 2000.
- [12] Lee, P. J., “System of Personal Information Protection Act and The Related Laws,” Journal of the Korean Review of Crisis and Emergency Management, Vol. 10, No. 1, pp. 81-103, 2014.
- [13] Mann, H. and Whitney, D., “On a Test of whether One of Two Random Variables Is Stochastically Larger than the Other,” Ann. Math. Statist, Vol. 18, pp. 50-60, 1949.
- [14] Ministry of Security and Public Administration, “Actions Providing Personal Information Security,” Ministry of Security and Public Administration Notice No. 43, pp. 1-48, 2011.
- [15] Ministry of Security and Public Administration, “National Informatization Whith Paper,” National Information Society Agency pp. 407-408, 2012.
- [16] Ministry of Security and Public Administration, “The terms of the Personal Information Protection Act personal information and infringement,” Ministry of Security and Public Administration, pp. 18-53, 2010.
- [17] National IT Industry Promotion Agency, Korea Internet Security Center, “IT industry 10 grand challenge,” National IT Industry Promotion Agency, 2012.
- [18] Organization for Economic Cooperation and Development guidelines, Annex to the recommendation of the Council of Vol. 23, 1980, “Guidelines governing the

- protection of privacy and transborder flows of personal data.”
- [19] Saaty, T. L., “The Analytic Hierarchy Process,” New York : McGraw-Hill. International, 1980.
- [20] Saaty, T. L., “Decision Making with Dependence and Feedback : The Analytic Network Process,” Int. J. Services Sciences, Vol. 1, No. 1, pp. 83-98, 2008.
- [21] Saaty, T. L., “Decision making for leaders (AHP series, Vol. 2),” RWS, 1995.
- [22] Shin, Y. J., Jeong, H. C., and Kang, W. Y., “A Study of Priority for Policy Implementation of Personal Information Security in Public Sector,” Journal of the Korea Institute of Information Security and Cryptology, Vol. 22, No. 2, pp. 379-390, 2012.
- [23] So, W. Y., “A Study on the Operating Status of the Protection Organizations in Developed Countries,” Korea Information Security Agency, 1998.
- [24] Wacks, R., Personal Information : Privacy and the Law, Oxford : Clarendon Place, 1989.

## 저 자 소 개



김영희 (E-mail : sorak75@naver.com)  
2001년 컴퓨터공학사  
2001년~2012년 인젠, 인터파크  
2012년~현재 한화S&C  
2013년 산업정보시스템 (공학석사)  
2013년~현재 서울과학기술대학교  
IT정책전문대학원  
산업정보시스템공학 (박사과정)  
관심분야 정보보호, 개인정보보호



국광호 (E-mail : khkook@seoultech.ac.kr)  
1979년 서울대학교 산업공학사  
1981년 서울대학교 대학원 산업공학 (석사)  
1989년 美조지아 공과대학교 대학원 (산업공학박사)  
1989년~1993년 한국전자통신연구원 선임연구원  
1993년~현재 서울과학기술대학교 기술경영융합대학  
글로벌융합산업공학과 교수  
관심분야 정보보호, 정보통신

〈Table 1〉 Weights of Evaluation Items Final

upper level criteria	Lower level criteria	Expert groups			Working Groups				
		Upper Weight	Lower Weight	Total Weight	Rank	Upper Weight	Lower Weight	Total Weight	Rank
Internal management plan	Planning and implementation	0.170	0.622	0.106	1	0.100	0.670	0.067	3
	Change and history management		0.378	0.064	4		0.330	0.033	19
Access Rights Management	Minimal access rights	0.156	0.372	0.058	5	0.188	0.332	0.062	4
	Deletion and change of access rights		0.363	0.057	7		0.263	0.049	12
	Records and stores history		0.101	0.016	20		0.137	0.026	20
	Identity management		0.164	0.026	18		0.268	0.050	10
Password Management	Password creation rules	0.136	0.592	0.081	2	0.120	0.432	0.052	7
	Apply password rules		0.408	0.055	8		0.568	0.068	2
Access Control System	Installation and operation of the security system	0.118	0.318	0.038	15	0.126	0.306	0.039	17
	Secure Connection means		0.302	0.036	16		0.288	0.036	18
	prevent the leakage of Personal Information		0.380	0.045	13		0.406	0.051	8
Privacy Encryption	Encrypted storage of personal information	0.164	0.404	0.066	3	0.194	0.400	0.078	1
	Encryption of personal information transmission		0.301	0.049	10		0.287	0.056	6
	Uses a secure algorithm		0.295	0.048	11		0.313	0.061	5
Retention of records	Management of connection records	0.052	0.539	0.028	17	0.008	0.547	0.048	13
	Secure storage of connection records		0.461	0.024	19		0.453	0.040	16
Security Program Installation	Installation and operation of Antivirus S/W	0.092	0.521	0.048	12	0.094	0.542	0.051	9
	Security patch OS and S/W		0.479	0.044	14		0.458	0.043	14
Prevention of physical access	Management of Physical access control	0.112	0.510	0.057	6	0.090	0.450	0.041	15
	Management of storage and document		0.490	0.055	9		0.550	0.050	11