http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.24, No.4, November 2019, pp.31-48
https://doi.org/10.7838/jsebs.2019.24.4.031

AHP 기법을 이용한 금융회사 『개인정보의 안전성 확보조치 기준』 우선순위에 관한 연구: 금융회사 위·수탁자 간 인식 차이를 중심으로

A Study on the Priority of 『Personal Information Safety Measure』 Using AHP Method: Focus on the Defferences between Financial Company and Consignee

김세영(Seyoung KIM)*, 김인석(Inseok KIM)**

초 록

4차 산업혁명시대 흐름 속에서 살아남기 위해 기업들은 빅데이터, 인공지능, 사물인터넷 등 최신 기술을 활용한 개인화 서비스에 많은 관심과 노력을 기울이는 한편, 업무 효율성 및 전문성, 비용 절감 등의 이유로 개인정보 처리를 제3자에게 위탁하고 있다. 이러한 환경에서 위탁자는 수탁자에 대한 개인정보 안전성 확보를 위해 보다 효과적이고 합리적인 기준으로 수탁자를 점검할 필요가 있다. 본 연구는 금융회사와 수탁자를 대상으로 AHP 기법을 이용하여 「개인정보 안전성 확보조치 기준」 항목별 중요도와 우선순위를 도출하고, 금융회사와 수탁자 간의 중요도에 대한 인식 차이를 객관적으로 비교 분석하였다. 이를 바탕으로 금융회사 자체 점검과 수탁자 점검의 차이를 인식하고 목적에 맞는 가중치를 반영한 차별화된 점검기준을 적용할 수 있는 정책적 근거와 시사점을 제시한다.

ABSTRACT

To survive in the trend of the fourth industrial revolution, companies are putting a lot of attention and effort into personalization services using the latest technologies such as big data, artificial intelligence and the Internet of Things, while entrusting third parties to handle personal information on the grounds of work efficiency, expertise and cost reduction. In such an environment, consignors need to check trustees on a more effective and reasonable basis to ensure personal information safety for trustees. This study used AHP techniques to derive the importance and priority of each item of "Personal Information Safety Assurance Measures" for financial companies and trustees, and objectively compared and analyzed differences in perceptions of importance between financial institutions and trustees. Based on this, the company recognizes the difference between self-inspection of financial institutions and inspection of trustees and presents policy grounds and implications for applying differentiated inspection standards that reflect the weights appropriate for the purpose.

키워드 : 개인정보보호 정책, 개인정보 안전성 확보조치 기준, 계층분석기법
Personal Information Security Policy, Personal Information Safety Measure, AHP

* First Author, Graduate School of Information Security, Korea University(seyoung@nonghyup.com)
** Corresponding Author, Graduate School of Information Security, Korea University(iskim11@korea.ac.kr)
Received: 2019-08-07, Review completed: 2019-08-26, Accepted: 2019-09-02

1. 서 론

1.1 연구배경 및 목적

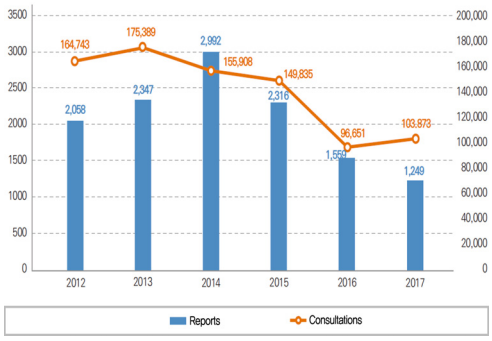
개인정보 보호는 '개인의 삶의 질'과 '기업의 생존'을 위한 핵심 분야로 인식될 만큼 중요성이 날로 증대되고 있으며, 4차 산업혁명시대 사회 안전의 기본이자 국가 성장의 지속 가능성을 뒷받침하는 중요한 가치로 여겨지고 있다. 많은 기업들은 4차 산업혁명시대 흐름 속에서 살아남기 위해 빅데이터, 인공지능, 사물인터넷, 핀테크 등 최신 기술을 활용한 개인화 서비스에 많은 관심과 노력을 기울이고 있다. 이렇듯 개인정보의 가치는 나날이 중요해지고 있으나 한편으로는 업무 효율성 및 전문성, 비용 절감 등의 이유로 개인정보 처리를 위탁하는 것이 현실이다.

정부에서는 이로 인한 개인정보의 무분별한 사용과 오남용을 막기 위해 법령 및 가이드 등 관련 제도를 지속적으로 강화하고 실태점검에 나서는 등 개인정보 보호를 위해 높은 수준의 규제를 적용해 오고 있다. 특히 개인정보 위탁자에게는 수탁자의 교육 및 점검 등을 포함한 관리 감독 역할을 부여하고, 수탁자의 과실로 발생한 개인정보 유출에 대해서도 위탁자가 책임지도록 하고 있다[10].

개인정보 보호에 대한 정책과 제도는 그동안 수많은 이슈와 사건들을 겪으면서 개선과 보완을 통해 오늘에 이르렀다. 그 사이에 개인정보의 활용과 보호에 대한 사회적인 인식 변화와 개인정보의 안전한 사용을 위한 제도적 측면은 어느 정도 성숙되었다고 볼 수 있으나, 실효성 측면에서는 아직도 보완해야 할 부분이 남아 있다.

행정안전부 자료에 따르면 개인정보 침해 신고 건수는 2014년 이후 다소 감소하였으나 여전히 1년에 1천 건 이상을 기록하고 있고[8], 개인정보처리자에 대한 신뢰성은 금융부문 36.2%, 의료부문 33.1%, 행정부문 26.5%, 교육부문 24.5%, 생활(쇼핑)부문 11.5%로 기대에 미치지 못하고 있다[7].

2010년 이후 개인정보 유출사고 유형에 있어 중요한 사실은 개인정보사고의 주요 발생 원인이 외부의 해킹으로 발생한 사고 보다 내부의 인력 또는 아웃소싱에서 발생한 유출사고가 급격히 늘어났다는 것이며, 이러한 유출사고의 피해가 외부 해킹의 사례보다 더욱 심각한 피해를 낳고 있다는 것이다[6].



〈Figure 1〉 Number of Personal Information Breach Reports and Consultations〔7〕

본 연구는 개인정보 유출시 파급력이 가장 크고 개인정보 위탁 처리가 많은 금융산업 분야를 대상으로 AHP 기법을 이용하여 위탁자와 수탁자 측면의 개인정보의 안전성 확보조치 기준에 대한 우선순위와 인식을 비교 분석 하였다. 특히, 최근 중요도가 높아지고 있는 파기 관련 항목을 반영하여 기존 연구와 차이점을 비교하고, 위탁자와 수탁자 그룹을 구분하여

위탁자와 수탁자 관점의 중요도를 객관적으로 분석하고 서로의 차이점을 과학적으로 도출하였다. 이를 바탕으로 금융회사가 개인정보 처리를 위탁함에 있어 객관적으로 수탁자의 인식을 이해하고, 보다 효과적이고 합리적으로 수탁자 점검에 활용할 수 있는 정책적 근거와 시사점을 제시하고자 한다.

1.2 연구의 범위 및 방법

본 연구는 금융회사의 종사자 A그룹과 금융회사로부터 개인정보 처리를 위탁받은 수탁회사의 종사자 B그룹을 대상으로 선정하여 개인정보의 안전성 확보조치 기준에 대한 설문 조사를 실시하였다. 개인정보의 안전성 확보조치 기준 항목별 상대적 중요도와 시급성을 측정하여 우선순위를 도출하였다.

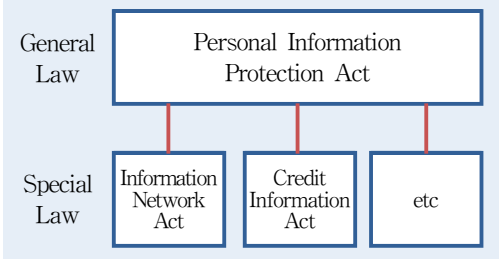
A그룹은 은행, 보험, 카드 등 12개 금융회사의 정보보호 및 IT, 보안 업무 종사자 59명으로 구성하였다. B그룹은 금융회사의 개인정보 처리를 위탁받은 감정평가 및 채권관리, DM발송, IT서비스 등 18개 수탁업체의 개인정보 관련 업무 종사자 30명으로 구성하여 금융산업 분야의 개인정보의 안전성 확보조치와 관련 전문성이 확보된 실무자 총 89명을 대상으로 하였다. 설문 조사는 2017년 개정된 '개인정보의 안전성 확보조치 기준(행정안전부 고시 제2017-1호)'을 대상으로 항목별 가중치 산정을 위한 쌍대비교(Pair-wise Comparison)를 실시하였고, 결과 분석은 다기준 의사결정(MCDM; Multiple Criteria Decision Making)에 가장 광범위하게 활용되는 AHP(Analytic Hierarchy Process; 계층적 의사결정 기법)를 이용하여 의사결정의 합리성과 논리성을 높였다.

2. 이론적 배경

2.1 개인정보보호 관련 법률

한국은 1989년 12월에 최초의 개인정보보호법 시안을 마련하고, 이후 공공부문에 적용하는 "공공기관의 개인정보보호에 관한 법률", 민간부분에 적용하는 "신용정보의 이용 및 보호에 관한 법률(이하 신용정보법)", "정보통신망이용촉진및정보보호등에관한법률(이하 정보통신망법)" 등 특별법을 각각 제정·시행하였다[13].

2011년 3월에 제정한 "개인정보보호법"은 일반법으로서 개인정보의 수집·유출·오용·남용으로부터 사생활의 비밀 등을 보호함으로써 국민의 권리와 이익을 증진하고, 나아가 개인의 존엄과 가치를 구현하기 위하여 개인정보 처리에 관한 사항을 규정함을 목적으로 제정되었다. 이는 특별법인 "정보통신망법"과 "신용정보법"에서 규정하지 않는 개인정보 보호에 대한 일반적인 사항을 적용하고 있다.



〈Figure 2〉 Personal Information Protection Act

2.2 개인정보의 안전성 확보조치 기준

개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등 개인정보처리자는 "개인정보보호

법” 제23조, 제24조 및 제29조에 따라 개인정보가 분실・도난・유출・위조・변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적・관리적 및 물리적 안전조치에 관한 기준을 따라야 한다. 이에 따라 행정안전부는 “개인정보보호법”의 하위 행정규칙인 ‘개인정보의 안전성 확보조치 기준’을 제정하고, 개인정보처리자 유형 및 개인정보 보유량에 따른 기술적, 관리적, 물리적인 안전조치 기준을 준수하도록 하고 있다.

〈Table 1〉 Personal Information Safety Measure

CRITERIA	DATE		
	2011.09	2014.12	2016.09
1.1 Establishing and implementing an internal management plan	○	○	○
1.2 Internal management plan changes and history management	○	○	○
1.3 Checking the implementation status of the internal management plan			○
2.1 Provide minimum access differential	○	○	○
2.2 Changing or deleting access rights when changing users	○	○	○
2.3 Recording and storing access rights	○	○	○
2.4 Do not share user accounts	○	○	○
2.5 Establishing and applying password-writing rules	○	○	○
2.6 Access restriction in case of password scheduling error			○
3.1 Unauthorized IP Access Control and Detection	○	○	○
3.2 Secure authentication means applied when accessing the external connection.	○	○	○
3.3 Access control measures to prevent external exposure	○	○	○
3.4 Check and take actions for vulnerabilities		○	○
3.5 Block access if not in use for a certain period of time.			○
3.6 Protection measures such as setting a password for a terminal		○	○
3.7 Installing and operating security programs such as vaccines	○	○	○
4.1 Encrypts when sending unique identification information outside of the country	○	○	○
4.2 Encrypts when storing the unique identification information system	○	○	○
4.3 Encrypting the Internet section of unique identification information	○	○	○
4.4 Encrypts when storing a unique identification information PC	○	○	○
4.5 Applying safe encryption algorithms	○	○	○
4.6 Establishing and implementing safety management procedures for encryption keys			○
5.1 Archive and manage access records	○	○	○
5.2 Check access records half-yearly		○	○
5.3 Prevent forgery and loss of access records	○	○	○
6.1 Establishing and operating access control procedures	○	○	○
6.2 Paper, storage media safe location	○	○	○
6.3 Control the entry and exit of auxiliary storage media		○	○
6.4 Limiting the use of non-accredited terminals for administrative purposes			○
7.1 Establishing and inspecting the crisis response manual			○
7.2 Planning for backup and recovery			○
8.1 Destruction after Retention Period		○	○

* [행정자치부고시 제2016-35호, 2016.9.1., 전부개정]
[행정자치부고시 제2014-7호, 2014.12.30., 일부개정]
[행정안전부고시 제2011-43호, 2011.9.30., 제정]

주요 내용은 내부관리 계획의 수립 및 시행, 접근 권한의 관리, 접근 통제, 개인정보 암호화, 접속기록의 보관 및 점검, 악성 프로그램 등 방지, 관리용 단말기의 안전조치, 물리적 안전조치, 재해・재난 대비 안전조치, 개인정보 파기 등으로 구성되어 있다[9].

2.3 금융회사의 개인정보 위탁 현황

개인정보처리자가 개인정보의 처리 업무를 위탁하는 경우에는 “개인정보보호법” 제26조, “신용정보법” 제17조, “정보통신망법” 제25조 등에 따라 위탁하는 업무의 내용과 수탁자를 정보주체가 언제든지 쉽게 확인할 수 있도록 공개해야 하고, 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실・도난・유출・위조・변조 또는 훼손되지 않도록 수탁자를 교육하고 감독하여야 한다. 특히, 수탁자가 위탁받은 업무와 관련하여 유출 등 피해를 입힌 경우 위탁자는 수탁자와 연대하여 손해배상 책임을 진다[3].

개인정보 위탁과 유사한 개념으로 ‘제3자 제공’이 있으나, 제3자 제공은 개인정보를 제공받는 자의 목적과 이익을 위해 개인정보가 이전되는 경우로서 제3자 스스로 관리・감독 책임을 갖는다는 점에서 위탁과 구분된다.

한편, 금융회사가 홈페이지에 공개한 개인정보처리위탁 현황을 살펴보면 A사는 80개, B사는 96개, C사는 74개의 수탁자를 두고 있는 것으로 나타났다. 주요 업무는 DM발송, 콜센터, 채권추심, 감정평가, 이벤트 등이며 금융업무와 연관된 다양한 부수업무 처리를 위해 각 분야의 전문 업체에게 개인정보 처리를 위탁하여 운영하고 있다. 이는 금융업무의 특수성에 따른 복잡한 업무형태로 인해 비롯된 부득이한 상황으로 인식하고 있으나, 수탁자의 증가는 위탁자의 개인정보 관리・감독의 질을 저하시키고 리스크를 증가시키는 중요한 요소 중 하나임에 틀림없다.

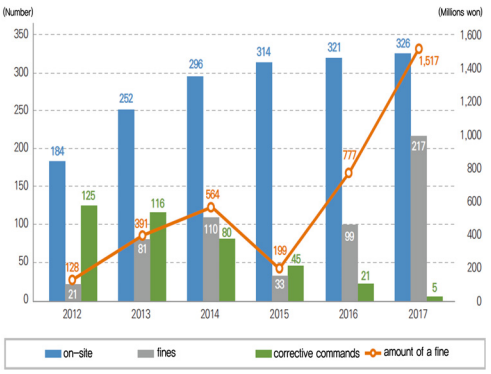
〈Table 2〉 Consignment Service of Financial Companies〔6〕

BANK	INSURANCE	CARD
ATM operation	Insurance contract recruitment	Issuing cards Operation of CD device
Providing financial transaction information	Health examination	Franchise recruitment
Loan / Credit Real Estate Services	Accident investigation	Settlement Service
	For Sale	Point Service Poll

2.4 개인정보보호법 위반 사례

“개인정보보호법” 제24조제4항 및 제63조, 동법 시행령 제21조에 따라 행정안전부는 개인정보처리자가 안전성 확보에 필요한 조치를 하였는지 정기적으로 조사하고, 5만 명 이상의 고유식별정보를 처리하는 기관은 2년마다 고유식별정보 안전성 확보조치 이행현황에 대한 자체점검을 실시하고 그 결과를 행정안전부에 제출하여야 한다.

행정안전부에서 발표한 개인정보 실태점검 및 행정처분 사례를 보면 2017년 기준 326개 기관을 점검하여 217개 기관에 대해 총 15억 원의 과태료를 부과하였으며, 위반 건수 및 금액은 매년 증가하는 추세이다[8].



〈Figure 3〉 Fines Levied and Corrective Orders[8]

2018년 이후 개인정보보호법 위반 행정처분 결과 공표를 분석해 보면, 29개 기업에 대해 61건의 위반사항으로 약 3억 5천7백만 원의 과태료를 부과하였다. 그 중 수집동의 고지 위반, 유출통지 위반 등 행정절차 사항이 21%(13건)이고, 파기 미이행, 암호화 미적용, 접근권한 미조치 등 안전성 확보조치 사항이 79%(48건)에 해당한다[1].

〈Table 3〉 An Analysis of the Administrative Disposal Cases for Violation of the Personal Information Protection Act

CRITERIA	RATE	CNT	SUM (Unit 1,000 won)
Administrative violation	21%	13	66,000
· violation of notice	15%	9	50,000
· etc	7%	4	16,000
safety violation	79%	48	291,000
· breach of destruction	21%	13	75,000
· No encryption	18%	11	72,000
· etc	39%	24	144,000
TOTAL	100%	61	357,000

2.5 선행연구

Lee[6]는 금융회사 수탁사 관리·감독 개선 방안 연구를 통해 다수의 수탁자 관리에 대한 문제점과 대안을 제시하였다. 개인정보 위탁 관련 '금융회사의 개인신용정보가 적정하게 관리되고 있는가?'에 대해 응답자의 50%가 미흡하다고 답변하였다. 이는 '다수의 수탁자로 인한 관리감독 인력과 예산부족'이 41.7%, '수탁자의 관리·감독 방법론 부재'가 25%로 조사되었다. '금융회사의 적정한 수탁자의 수'에 대해서는 응답자의 85% 이상이 20개 이하로 답변하여 실제 금융회사의 수탁자 수와 큰 차이를 보였다. 이에 따른 대안으로는 수탁자 관리조직 수립, 전문 평가기관에 점검 위탁, 수탁자 선정 시 사전에 위험분석을 선행하여 리스크를 예방하는 방안을 제시하였다[6].

임동성은 수탁자 점검 활동이 정보보안 성과에 미치는 영향 연구를 통해 수탁자 점검을 위한 측정항목을 AHP 기법을 이용하여 도출하고 관리적, 물리적, 기술적 관리 수준과 영향도에 대한 연구 가설을 통해 수탁사 점검 요인이 정보보안 성과에 미치는 영향 및 상관 관계를 회귀분석으로 검증하였다[3].

김영희는 개인정보의 안전성 확보조치 기준별 우선순위 연구를 통해 개인정보의 안전성 확보를 위한 평가 항목 및 계층구조를 수립하고 AHP 기법을 이용한 가중치 분석을 통해 기업 및 공공기관의 개인정보 보호를 위한 우선순위 기준 모델을 제시하였다[5].

기존연구는 기업들이 안전한 개인정보 보호를 위해 수탁자를 효과적으로 관리·감독해야 할 필요성과 수탁자 점검활동으로 정보보안 성과를 향상시키는 방안을 도출하였다. '개인정보의

안전성 확보조치 기준'에 대해 AHP 기법을 이용한 점검 항목의 가중치 및 우선순위 등을 제시하였다. 그러나, 점검항목을 수립함에 있어 최근 중요성이 높아져 2014년 12월 이후 추가된 '내부 관리계획 이행실태 점검', '관리용 단말기에 비인가자 사용 제한', '보존기간 경과 후 파기' 등이 포함되지 않았으며, 개인정보가 수탁자에게 이전되어 있음에도 위탁자의 관점에서만 안전성 확보를 위한 방안을 연구하였다. 본 연구에서는 최근 중요성이 높아진 항목들을 포함하여 점검 항목을 현행화하여 우선순위를 도출하고, 개인정보 관리 주체인 위탁자와 수탁자 각각의 관점에서의 중요도를 구분하여 비교·분석 하였다는데 선행연구와 차별성이 있다.

3. 연구 설계 및 방법

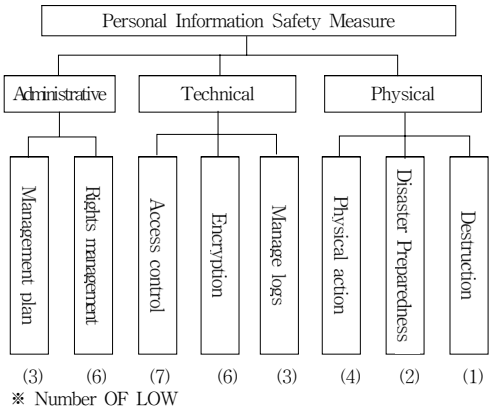
3.1 AHP 기법

AHP(Analytic Hierachy Process) 기법은 1970년대 초반 Thomas L. Saaty가 합리적 의사결정을 지원하기 위해 제안한 모형으로 의사결정이 필요한 여러 속성들의 중요도를 파악함으로써 최적의 대안을 찾는 의사결정모델이다. 여러 대안에 대해 상대적 중요도와 시급도를 고려하여 쌍대 비교로 가중치를 계산하고 우선순위를 도출한다. 객관성을 확보하기 위해 정량적 기준을 함께 사용한다. 평가지표와 비교대안이 많은 경우 복잡한 수치 계산이 요구되는데, 평가의 용이성과 정확성을 위해 전산프로그램이 활용되기도 한다. AHP 응용분야는 전략계획 수립, 성과측정지표 가중치 산정, 입지선정, 자원할당, 사업 및 공공정책의 수립, 프로그램 선정 등 우선순위 선정과 관련된 모든 활동에 활용된다[11, 12, 14].

AHP 기법을 이용하여 유효한 결과를 획득하기 위해서는 평가기준 도출 및 계층구조 생성, 쌍대비교를 통한 속성별 가중치 계산 및 일관성 검증, 속성별 선호도 합산을 통한 중요도 및 우선순위 선정 순으로 단계별 과정을 거쳐야 한다.

3.2 연구 모형

본 연구에서는 평가항목을 도출하기 위해 "개인정보보호법" 및 동법 시행령의 하위 행정규칙인 '개인정보의 안전성 확보조치 기준'을 사용하였다.



〈Figure 4〉 Hierarchy

'개인정보의 안전성 확보조치 기준'은 개인정보 보호를 위해 개인정보처리자가 준수해야 할 중요사항이 모두 포함되어 있으며, 시대에 따라 필요성이 높아진 사항은 추가하는 등 개선과 보완을 통해 완성도를 높여왔다. 특히, 정부가 실시하는 공공기관 및 기업의 개인정보 실태점검시 위반사항 평가 및 과태료 부과 기

준으로 활용하고 있으며 다수의 선행연구에서도 위탁자가 수탁자를 점검하기 위한 기준으로 제시하고 있어서 개인정보 보호를 위한 평가항목으로 가장 적합하다고 할 수 있다.

‘개인정보의 안전성 확보조치 기준’은 내부관리계획 수립 및 시행, 접근권한의 관리, 접근통제, 개인정보의 암호화, 접속기록의 보관 및 점검, 악성 프로그램 등 방지, 관리용 단말기의 안전조치, 물리적 안전조치, 재난재해 대비 안전조치, 개인정보의 파기 등 10개 조항으로 구분되어 있으며, 준수해야 할 세부항목은 총 32개로 구성되어 있다.

〈Table 4〉 Evaluation Criteria

TOP	MID	LOW
admin-istrative	Management Plan	1.1 Establishing and implementing an internal management plan
		1.2 Internal management plan changes and history management
		1.3 Checking the implementation status of the internal management plan
	Rights Management	2.1 Provide minimum access differential
		2.2 Changing or deleting access rights when changing users
		2.3 Recording and storing access rights
		2.4 Do not share user accounts
		2.5 Establishing and applying password-writing rules
		2.6 Access restriction in case of password scheduling error
Technical	Access Control	3.1 Unauthorized IP Access Control and Detection
		3.2 Secure authentication means applied when accessing the external connection.
		3.3 Access control measures to prevent external exposure
		3.4 Check and take actions for vulnerabilities
		3.5 Block access if not in use for a certain period of time.
		3.6 Protection measures such as setting a password for a terminal
		3.7 Installing and operating security programs such as vaccines
	Encryption	4.1 Encrypts when sending unique identification information outside of the country
		4.2 Encrypts when storing the unique identification information system
		4.3 Encrypting the Internet section of unique identification information
		4.4 Encrypts when storing a unique identification information PC
		4.5 Applying safe encryption algorithms
		4.6 Establishing and implementing safety management procedures for encryption keys
	Manage Logs	5.1 Archive and manage access records
		5.2 Check access records half-yearly
		5.3 Prevent forgery and loss of access records
Physical	Physical Action	6.1 Establishing and operating access control procedures
		6.2 Paper, storage media safe location
		6.3 Control the entry and exit of auxiliary storage media
		6.4 Limiting the use of non-accredited terminals for administrative purposes
	Disaster Preparedness	7.1 Establishing and inspecting the crisis response manual
		7.2 Planning for backup and recovery
	Destruction	8.1 Destruction after Retention Period

'개인정보의 안전성 확보조치 기준'을 기본으로 생성한 계층구조는 <Figure 4>와 같다. 최종 평가기준은 <Table 4>와 같다. 세부항목이 1개인 '악성프로그램 등 방지'와 '관리용단말기 안전조치' 조항은 성격이 동일한 조항인 접근통제, 물리적 안전조치의 세부항목으로 각각 조정하여 정제하였다.

3.3 연구 분석 방법

본 연구의 주된 목표는 금융회사가 개인정보를 안전하게 보호하기 위한 사항들에 대해 중요도를 선정하고, 수탁자에게 이전된 개인정보가 안전하게 보호될 수 있도록 관리·감독 및 점검 시 활용할 수 있는 효과적이고 합리적인 정책적 근거를 제시하기 위한 것이다. 이를 위해, '개인정보의 안전성 확보조치 기준'을 바탕으로 관리적, 기술적, 물리적 조치로 상위조치를 구성하고 종속 구조를 취하는 중위지표와 하위지표를 구성하였으며, 중요도 분석을 위해 항목별 쌍대비교를 조사하는 AHP 설문지를 작성하였다.

설문조사는 2019년 3월 18일부터 4월 15일까지 약 1개월간 금융회사 종사자인 A그룹과 금융회사의 개인정보 처리를 담당하는 수탁회사의 종사자인 B그룹으로 구분하여 실시하였다. A그룹은 은행, 보험, 카드 등 12개 금융회사의 정보보호 및 IT, 보안 업무를 담당하는 실무자 및 관리자 59명을 대상으로 하고, B그룹은 감정평가, 채권관리, DM발송, IT서비스 등 금융회사의 개인정보 처리를 위탁받아 운영하는 18개 수탁자의 실무자 및 개인정보보호 담당자 30명을 대상으로 하였다.

설문결과는 쌍대 비교행렬을 구성하고 기하평균(Geometry mean)을 이용하여 중요도를 산출하였고, 일관성 검증은 일관성지수 CI(Consistency Index)를 임의지수 RI(Random Index)로 나누어 계산한 일관성비율 CR(Consistency Ratio)을 이용하였다. CR은 CI로만 일관성을 판별하기 부족한 단점을 보완코자 도입한 것으로, 완전한 일관성을 유지하면서 쌍대비교를 하였다면 CI = 0, CR = 0이 된다. 일반적으로 CR 값이 0.1 미만이면 충분히 일관성이 있는 것으로 판단한다[2, 11, 12].

$$G = \sqrt[n]{a_1 a_2 \cdots a_n}$$

$$CI = \frac{\lambda_{\max} - n}{n-1}, \quad CR = \frac{CI}{RI}$$

본 연구에서는 AHP 가중치 평가를 위해 "DRESS Ver 1.7 for Windows" 프로그램을 사용하였으며, 총 89건의 설문지 중 Saaty가 논리적 일관성을 갖는다고 판단한 CR = 0.1 미만인 83건의 설문지만 평가 대상에 포함하였다.

4. 분석결과 및 시사점

4.1 가중치 분석 및 결과

본 연구에서 분석한 '개인정보의 안전성 확보조치 기준'에 대한 상위지표 및 중위지표의 가중치 분석 결과는 <Table 5>, <Table 6>과 같고, 하위지표의 가중치 분석 결과는 <Table 7>과 같다.

〈Table 5〉 Results of TOP

TOP	Weight	Rank	CR
administrative	0.367	1	0.02
Technical	0.362	2	
Physical	0.272	3	

상위지표는 관리적 조치(0.367)가 가장 중요한 것으로 나타났으며, 기술적 조치(0.361), 물리적 조치(0.272) 순서로 나타났다. 이는 수많은 전산사고 및 개인정보 유출 사건 등으로 인해 그동안 기술적 및 물리적 조치에 대한 투자가 크게 이루어지고 안전성 또한 한층 강화되어 왔기 때문에, 상대적으로 관리적 조치의 중요도가 높게 나타난 것으로 보인다. 또한, 2010년 이후 개인정보 유출사고의 주요 발생 원인이 외부의 해킹 보다는 내부의 인력 또는 아웃소싱에서 발생한 유출사고가 급격이 늘어났고, 이러한 유출사고의 피해가 외부 해킹의 사례보다 더욱 심각한 피해를 낳고 있다는 선행연구[14] 내용에 대한 인식이 반영된 결과로 판단된다.

〈Table 6〉 Results of TOP and MID

TOP	MID	Weight	Rank	CR
admin-istrative	Management Plan	0.177	2	0.02
	Rights Management	0.190	1	
Technical	Access Control	0.147	3	
	Encryption	0.147	4	
	Manage Logs	0.068	7	
Physical	Physical Action	0.109	5	
	Disaster Preparedness	0.060	8	
	Destruction	0.103	6	

중위지표는 관리적 조치에 해당하는 접근권한관리(0.189)와 내부권한관리(0.177)의 중요도가 가장 높게 나타났으며, 그 다음 접근통제(0.147), 개인정보암호화(0.147), 물리적안전조치(0.109), 개인정보파기(0.103) 접속기록관리(0.068), 재난재해조치(0.060) 순으로 나타났다. 이는 상위지표의 중요도가 중위지표에 그대로 나타났음을 알 수 있다.

하위지표는 항목수가 많아 항목간 중요도 차이가 크지 않다는 특이점이 있으나, 중위지표와 마찬가지로 관리적 조치에 해당하는 항목들이 가중치가 높았다. 중요도가 가장 높게 나타난 항목은 내부 관리계획 이행실태 점검(0.085)이며, 그 뒤로 내부 관리계획 수립 및 시행(0.056), 사용자 변경시 접근권한 변경 및 말소(0.043), 사용자계정 공유 금지(0.041), 최소한의 접근권한 변경 및 말소(0.043) 순으로 나타났다. 반면, 중요도가 낮은 항목은 일정시간 미사용시 접속차단(0.014), 접속기록 등을 반기별로 점검(0.017), 서류 및 저장매체의 안전한 장소 보관(0.017), 단말기의 비밀번호 설정 등 보호조치(0.018), 안전한 암호화 키 관리절차 수립 및 시행(0.020) 순으로 나타났다.

중요도가 가장 높은 내부 관리계획 이행실태 점검은 개인정보의 안전성 확보조치와 관련한 내부 관리계획의 적정성과 실효성을 보장하기 위한 조치사항으로 2016년 9월에 새롭게 추가된 항목이다. 이 외에도 2014년 12월 이후 추가된 항목 중 물리적 조치 항목인 관리용 단말기에 비인가자 사용 제한(0.035), 보존기간 경과 후 파기(0.035), 보조저장매체의 반출입 통제(0.030) 3개가 10위권 안에 포함되어 있는 것으로 나타났다. 이는 '개인정보의 안전성 확보조치 기준'에 있어서, 정부의 정책 방향과 현장에서 인식하는 중요성이 일정 부분 부합한다는 하나의 방증이 될 수 있을 것이다.

4.2 위탁자와 수탁자의 가중치 분석 결과

위탁자와 수탁자 관점의 중요도는 종합결과와 비슷하면서도 다소 차이가 있는 것으로 나타났다. 위탁자 관점에서는 내부 관리계획 이행실태 점

〈Table 7〉 Results of LOW

TOP	MID	Result		LOW	Result		Enforced since 2014.12
		Weight	Rank		Weight	Rank	
admin-istrative	Manage ment Plan	0.177	2	1.1 Establishing and implementing an internal management plan	0.056	2	
				1.2 Internal management plan changes and history management	0.036	6	
				1.3 Checking the implementation status of the internal management plan	0.085	1	○
	Rights Manage ment	0.189	1	2.1 Provide minimum access differential	0.038	5	
				2.2 Changing or deleting access rights when changing users	0.043	3	
				2.3 Recording and storing access rights	0.021	23	
				2.4 Do not share user accounts	0.041	4	
				2.5 Establishing and applying password-writing rules	0.022	22	
				2.6 Access restriction in case of password scheduling error	0.024	18	○
Technica l	Access Control	0.147	3	3.1 Unauthorized IP Access Control and Detection	0.027	12	
				3.2 Secure authentication means applied when accessing the external connection.	0.020	24	
				3.3 Access control measures to prevent external exposure	0.024	19	
				3.4 Check and take actions for vulnerabilities	0.020	24	○
				3.5 Block access if not in use for a certain period of time.	0.014	32	○
				3.6 Protection measures such as setting a password for a terminal	0.018	29	○
				3.7 Installing and operating security programs such as vaccines	0.025	16	
	Encrypti on	0.147	4	4.1 Encrypts when sending unique identification information outside of the country	0.027	11	
				4.2 Encrypts when storing the unique identification information system	0.026	14	
				4.3 Encrypting the Internet section of unique identification information	0.027	10	
				4.4 Encrypts when storing a unique identification information PC	0.023	21	
				4.5 Applying safe encryption algorithms	0.024	20	
				4.6 Establishing and implementing safety management procedures for encryption keys	0.020	28	○
	Manage Logs	0.068	7	5.1 Archive and manage access records	0.024	17	
				5.2 Check access records half-yearly	0.017	30	
				5.3 Prevent forgery and loss of access records	0.026	15	
Physical	Physical Action	0.109	5	6.1 Establishing and operating access control procedures	0.026	13	
				6.2 Paper, storage media safe location	0.017	30	
				6.3 Control the entry and exit of auxiliary storage media	0.030	9	○
				6.4 Limiting the use of non-accredited terminals for administrative purposes	0.035	7	○
	Disaster Prepar-edness	0.060	8	7.1 Establishing and inspecting the crisis response manual	0.020	26	○
				7.2 Planning for backup and recovery	0.020	26	○
	Destruc-tion	0.103	6	8.1 Destruction after Retention Period	0.035	8	○

〈Table 8〉 Results of Trustee and Consigno

TOP	MID	Result		LOW	trustee		consigno	
		Weight	Rank		Weight	Rank	Weight	Rank
admin-istrative	Management Plan	0.177	2	1.1 Establishing and implementing an internal management plan	0.061	2	0.045	3
				1.2 Internal management plan changes and history management	0.037	6	0.032	8
				1.3 Checking the implementation status of the internal management plan	0.091	1	0.072	1
	Rights Management	0.189	1	2.1 Provide minimum access differential	0.046	4	0.028	13
				2.2 Changing or deleting access rights when changing users	0.047	3	0.036	6
				2.3 Recording and storing access rights	0.023	17	0.017	30
				2.4 Do not share user accounts	0.040	5	0.045	4
				2.5 Establishing and applying password-writing rules	0.021	22	0.024	19
				2.6 Access restriction in case of password scheduling error	0.024	16	0.025	17
Technical	Access Control	0.147	3	3.1 Unauthorized IP Access Control and Detection	0.028	10	0.024	18
				3.2 Secure authentication means applied when accessing the external connection.	0.021	25	0.020	24
				3.3 Access control measures to prevent external exposure	0.024	15	0.023	22
				3.4 Check and take actions for vulnerabilities	0.021	23	0.019	26
				3.5 Block access if not in use for a certain period of time.	0.013	32	0.015	32
				3.6 Protection measures such as setting a password for a terminal	0.017	30	0.019	27
				3.7 Installing and operating security programs such as vaccines	0.022	18	0.030	9
	Encryption	0.147	4	4.1 Encrypts when sending unique identification information outside of the country	0.027	12	0.026	16
				4.2 Encrypts when storing the unique identification information system	0.025	13	0.028	11
				4.3 Encrypting the Internet section of unique identification information	0.028	11	0.027	14
				4.4 Encrypts when storing a unique identification information PC	0.021	21	0.027	15
				4.5 Applying safe encryption algorithms	0.022	20	0.028	12
				4.6 Establishing and implementing safety management procedures for encryption keys	0.018	28	0.023	21
	Manage Logs	0.068	7	5.1 Archive and manage access records	0.025	14	0.023	20
				5.2 Check access records half-yearly	0.017	29	0.017	30
				5.3 Prevent forgery and loss of access records	0.022	19	0.034	7
Physical	Physical Action	0.109	5	6.1 Establishing and operating access control procedures	0.029	9	0.021	23
				6.2 Paper, storage media safe location	0.016	31	0.019	25
				6.3 Control the entry and exit of auxiliary storage media	0.030	8	0.028	10
				6.4 Limiting the use of non-accredited terminals for administrative purposes	0.031	7	0.043	5
	Disaster Preparedness	0.060	8	7.1 Establishing and inspecting the crisis response manual	0.021	24	0.018	29
				7.2 Planning for backup and recovery	0.021	26	0.018	28
	Dest-ruction	0.103	6	8.1 Destruction after Retention Period	0.019	27	0.047	2

검(0.091)이 종합결과와 동일하게 가장 높았고, 그 다음이 내부 관리계획 수립 및 시행(0.061), 사용자 변경시 접근권한 변경 및 말소(0.047), 최소한의 접근권한 차등 부여(0.046), 사용자계정 공유 금지(0.040) 순으로 나타났다. 이는 종합결과와 마찬가지로 위탁자 관점에서도 안전한 개인정보 보호를 위해 관리적 조치를 가장 중요하게 생각하는 것을 알 수 있다.

한편, 수탁자 관점에서는 내부 관리계획 이행실태 점검(0.072)이 위탁자와 동일하게 중요도가 제일 높았고, 내부 관리계획 수립 및 시행(0.045)이 세 번째, 사용자계정 공유 금지(0.045)가 네 번째로 높아 위탁자 관점과 유사하게 나타났다. 그러나, 위탁자 관점에서 중요도가 낮게 나타난 보존기간 경과 후 파기(0.047)가 수탁자 관점에서는 두 번째로 높았으며 관리용 단말기에 비인가자 사용 제한(0.043)이 다섯 번째로 높아 위탁자와 큰 차이를 보였다. 또한, 위탁자 관점에서는 중요도가 네 번째로 높았던 최소한의 접근권한 차등 부여가 수탁자 관점에서는 열세 번째로 다소 낮게 나타났다. 이런 차이는 수탁자가 개인정보를 직접 수집하지 않고 위탁자의 요청에 따라 개인정보를 처리하고 장기간 보관하지 않고 즉시 파기해야 하는 업무 특성에 따른 것으로 추측된다. 즉, 개인정보 라이프사이클[4]에 따라 체계적으로 고객정보를 관리하는 위탁자와 단순 데이터를 제한적으로 처리하는 수탁자의 업무 특성이 그대로 나타난 결과임을 알 수 있다.

4.3 위탁자와 수탁자간 인식차이 검증 결과

본 연구에서는 위탁자와 수탁자의 인식 차이를 검증하기 위하여 t-test를 실행하였다. 이를 위해 상위지표, 중위지표에 해당되는 하위지표의 평균을 구하고, 평균값으로 t-test를 실행하였으며 분석결과는 <Table 9>, <Table 10>과 같다.

〈Table 9〉 T-Test Results of TOP

TOP	AVE		
	trustee	consigno	significance level
administrative	8.366	9.267	0.024*
Technical	8.507	9.141	0.034*
Physical	9.281	10.027	0.150

*p < .05.

〈Table 10〉 T-Test Results of TOP and MID

TOP	MID	AVE		
		trustee	consigno	signi-ficance level
admin-istrative	Management Plan	9.770	9.880	0.847
	Rights Management	8.000	9.079	0.015*
Tech-nical	Access Control	8.550	9.057	0.250
	Encryption	8.522	8.765	0.540
	Manage Logs	8.650	9.670	0.044*
Physical	Physical Action	9.479	10.391	0.089
	Disaster Preparedness	9.010	9.290	0.746
	Destruction	8.620	9.390	0.421

*p < .05.

상위지표별 위탁자와 수탁자의 평균분석결과 상위지표인 관리적 조치와 기술적 조치 두 지표에서 위탁자와 수탁자가 통계적으로 유의미한 차이를 확인하였다.

중위지표별 위탁자와 수탁자 인식차이 분석결과는 다음과 같다. 첫째, 검증결과 관리적

조치의 접근권한관리에서 위탁자(8.00)와 수탁자(9.079) 간 차이가 통계적으로 유의한 것으로 나타났다. 즉 사용자계정 공유 금지항목과 비밀번호 작성규칙 수립 및 적용을 위탁자에 비해 수탁자가 더 중요하게 생각하는 것으로 나타났다. 이에 비해 접근권한관리 항목 중 접근권한 차등부여, 사용자 변경시 접근권한 변경 및 말소, 접근권한 기록 및 보관, 비밀번호 일정 횟수 오류시 접근 제한 등의 항목은 위탁자가 수탁자보다 상대적으로 더 중요하게 생각한 것으로 나타났다.

이는 위탁자가 수탁자에 비해 규모가 크고 업무가 세분화 되어 있으며, 사용자별 권한을 중요시하는 금융회사의 특성이 나타난 것으로 추측된다.

둘째, 기술적 조치 내 접속기록관리에서 위탁자(8.650)와 수탁자(9.670)간 유의미한 차이를 확인하였다. 구체적으로 접속기록의 위변조 및 분실방지에 대해 수탁자가 더 중요하게 인식하였다. 이에 반해 접속기록 보관 및 관리, 점검 등에 대해서는 위탁자가 상대적으로 수탁자보다 더 중요하게 생각한 것으로 나타났다. 이는 업무처리를 위해 데이터를 장기간 보관하고 다수의 사용자가 수시로 접속하는 금융회사와 짧은 기간 동안 데이터를 전달받아 처리하고 파기하는 수탁자의 데이터 보관주기 차이가 접속기록 관리 항목의 순위에 반영된 것으로 추측된다.

위 두 중위지표 외의 항목은 통계적으로 유의미한 차이를 보이지 않는 것으로 나타났다.

4.4 분석결과 종합 및 시사점

금융산업 분야의 위탁자와 수탁자를 대상으로 '개인정보의 안전성 확보조치 기준' 항목별 우선순위에 대해 비교・분석해 보았다.

Kim[5]은 2014년 정보보호컨설팅 전문가와 기업의 개인정보보호실무자를 대상으로 분석한 개인정보의 안전성 확보 조치를 위한 최종 우선순위는 안전한 비밀번호 설정(1위), 관리계획 수립 및 시행(2위), 보안프로그램 운영(3위), 개인정보의 암호화 저장(4위), 최소한의 접근권한 차등 부여(5위) 순으로 제안하였다[5].

그러나, 금융산업 분야의 위탁자와 수탁자의 정보보호 관리자 및 실무자를 대상으로 조사한 본 연구에서는 내부 관리계획 이행실태 점검(1위), 내부 관리계획 수립 및 시행(2위), 사용자 변경시 접근권한 변경 및 말소(3위), 최소한의 접근권한 차등 부여(4위), 사용자계정 공유 금지(5위) 순으로 나타났다. 선행연구 이후에 '개인정보의 안전성 확보조치 기준'에 추가된 내부 관리계획 이행실태 점검이 새롭게 1위로 나타났고, 2위는 기존과 동일하게 내부 관리계획의 수립 및 시행으로 나타났으며 최소한의 접근권한 차등 부여는 5위에서 4위로 한 단계 높아졌다. 또한, 선행연구에서는 관리적 조치와 기술적 조치가 고르게 상위권에 분포되었다면, 본 연구에서는 관리적 조치가 상위권을 차지하고 있다는 차이점이 있다.

위탁자와 수탁자 관점에서는 내부 관리계획 이행실태 점검, 내부 관리계획 수립 및 시행, 사용자계정 공유 금지, 사용자 변경시 접근권한 변경 및 말소 등이 상위권으로 비슷하게 나타났으나, 보존기간 경과 후 파기 항목에 대해서는 통계적 유의미 범위에는 들어가지 않았지만 위탁자는 27위, 수탁자는 2위로 차이가 크게 나타났다. 이는 위탁자와 수탁자 모두 최근 개인정보의 안전성 확보조치 기준에 대해 동일한

인식을 보여주는 한편, 고객정보를 장기간 보관 및 관리해야 하는 위탁자와 개인정보 처리 후 보관할 필요가 없는 수탁자의 인식 차이를 보여주는 중요한 요소로 볼 수 있다.

특히, 상위지표인 관리적 조치와 기술적 조치에서 위탁자와 수탁자 간 통계적 유의미한 차이를 확인 하였다. 그리고 중위지표별 위탁자와 수탁자 간 인식을 비교한 결과 관리적 조치의 중위지표인 접근권한관리, 기술적조치의 중위지표 접속 기록 관리에서 위탁자와 수탁자 간 통계적으로 유의미한 인식의 차가 있음을 확인하였다.

종합적으로 결과를 비교・분석해 보면 관리적 조치가 가장 중요하고 그중에서도 내부 관리계획 이행실태 점검이 1위로 나타난 것은 그동안 기술적 물리적 조치에 대한 투자가 크게 이루어지고 안전성 또한 한층 강화되어 왔기 때문에, 관리적 조치인 내부 관리계획 수립 및 시행, 점검을 통해 관리적, 기술적, 물리적 조치를 철저히 확인하여 안전성을 확보하고 부족한 부분은 보완하는 방향으로 인식이 변화하고 있음을 알 수 있다. 수탁자 점검에 있어서도 물리적으로 모든 것을 완벽히 점검한다는 것은 현실적으로 어려운 일이므로 수탁자가 내부 관리계획의 수립 및 점검 활동을 제대로 하고 있는지를 점검하는 것이 중요한 포인트가 될 수 있다. 또한 수탁자에게 제공된 개인정보는 목적 달성 후 반드시 파기하도록 하여 사용자 고의 또는 외부 침해 발생 시에도 개인정보 유출이 최소화 될 수 있도록 하여야 할 것이다.

이를 위해 기업은 자체 점검과 수탁자 점검에 대해 차이를 인식하고 목적에 맞는 각각의 점검계획을 수립해야 할 필요가 있다. 자체 점검의 경우 내부 관리계획의 이행실태 점검 항목 위주로, 수탁사 점검인 경우 내부 관리계획의 이행실태 점검 및 보존기간 경과 후 파기 항목 위주로 가중치를 부여하는 등 실제 중요도를 반영하고, 목적과 항목별 중요도에 따른 차별화된 점검기준을 적용한다면 보다 효과적이고 객관적인 평가가 가능할 것이다.

5. 결 론

본 연구에서는 대량의 개인정보를 수집 및 이용하고 수탁사에 개인정보 처리 위탁이 많은 금융산업 분야를 대상으로 '개인정보의 안전성 확보조치 기준' 우선순위를 조사하였다. 또한, 위탁자와 수탁자 측면의 인식 차이를 비교 분석하여 금융회사가 개인정보 처리를 위탁함에 있어 객관적으로 수탁자의 인식을 이해하고 보다 효과적이고 합리적으로 수탁자 점검에 활용할 수 있는 정책적 근거와 시사점을 제시하였다.

금융회사는 이를 바탕으로 「개인정보 안전성 확보조치 기준」에 대한 자체 점검과 수탁사 점검의 차이를 인식하고 목적에 맞는 가중치를 반영한 차별화된 점검기준을 적용할 수 있을 것이다. 예를 들면, 금융회사 자체점검 기준에는 내부 관리계획 이행실태 점검, 내부 관리계획 수립 및 시행, 사용자 변경시 접근권한 변경 및 말소 등 위탁자 측면의 중요도가 높은 항목에 가중치를 반영하고, 수탁자 점검 기준에는 내부 관리계획 이행실태 점검과 보존기간 경과 후 파기 등 수탁자 측면의 중요도가 높은 항목에 가중치를 반영하여 각각의 목적에 맞는 점검계획을 수립하여 점검 및 평가를 할 수 있다. 점검결과 미흡한 항목에 대해서도 중요도에 따라 단순 조치 또는 주의로 경미하게 대하거나

계약 해지로 엄격하게 대하는 등점검결과에 대한 평가기준을 수립하는데 객관적이고 효과적인 자료로 활용할 수 있을 것이다.

이런 정책적 함의에도 불구하고, 본 연구는 몇 가지 한계가 있다. 본 연구에서는 금융회사와 금융회사의 수탁자를 대상으로 조사하였다. 수탁자의 규모는 중소기업 수준에서 영세기업까지 폭이 넓었고 업종은 매우 다양하였다. 단순히 개인정보 처리 후 파기로 업무가 종료되는 곳이 있는가 하면 대량의 개인정보를 정기적으로 수탁 처리하는 곳, 고객에게 비대면 서비스를 제공하는 곳 등 업무형태도 큰 차이를 보였다. '개인정보의 안전성 확보조치 기준'은 기업의 규모와 개인정보 보유 건수에 따라 적용하는 기준을 다르게 정하였으나, 본 연구에서는 금융회사의 개인정보 보호를 목적으로 하여 영세한 수탁자에게도 동일한 기준을 제시하였다. 이런 한계를 보완하여 향후 연구에서는 기업의 규모, 기업별 개인정보처리 현황, 개인정보처리에 관한 다양한 특성별 평가 가중치 기준을 반영하여 좀더 정교한 가중치 도출과 특화된 적정한 평가가 이루어져야 할 것이다.

또한, 시대의 변화와 기술의 발전에 따라 모든 가치와 중요성은 변화하기 마련이다. 개인정보의 안전성 확보조치 또한 사회적 흐름에 따라 개선과 보완을 통해 변화하고 있다. 본 연구 결과가 선행연구와 차이점을 보였듯이 앞으로 발생할 이슈와 개인정보 유출 사고 유형 등에 따라 새로운 기준이 추가될 수도 있고 중요성 및 우선순위가 변경될 수도 있다.

따라서 '개인정보의 안전성 확보조치 기준' 우선순위는 필요한 환경에 맞는 조사 및 연구가 필요하고, 새로운 중요성이 인식되는 시기마다 우선순위 분석 연구가 지속적으로 이루어진다면 많은 기업들이 개인정보를 보호하는 데 큰 도움이 될 것으로 보인다.

References

[1] Announcement of administrative disposition result of breach of personal information protection law(5th~8th), https://www.mois.go.kr/frt/bbs/type013/commonSelectBoardList.do?bbsId=BBSMSTR_000000000006.

[2] Choi, J. W., "A study on the improvement of management outcomes in the start-up companies using AHP and DEA: focusing on the tenant companies of business incubator center," Kyung Hee University, 2011

[3] Im, D. S., "An Empirical Study on the Impact of Management Level Diagnosis of Consignee's Personal Information Protection on Information Security Performance," Chonnam National University, 2018.

[4] Jang, Y. R., "A study on the protection of personal information Life Cycle phased in personal information Act," Konkuk University, 2012

[5] Kim, Y. H., "A Study on the Relative Importance of the Administrative and Technical Measures for the Personal Information Protection," The Journal of

Society for e-Business Studies, Vol, 19, No. 4, pp. 135-150, 2014.

[6] Lee, Y. J., "A Study on the Improvement and Supervisory Status for Personal Fiduciary Services in Financial Institutions," Korea University, 2014.

[7] Ministry of the Interior and Safety, "2018 Personal Information Protection Status Survey," pp. 154-155, 2019.

[8] Ministry of the Interior and Safety, "Case of personal information inspection and administrative disposal," https://www.privacy.go.kr, pp. 8-9, 2018.

[9] Ministry of the Interior and Safety, "Manual of Personal Information Safety Measure," Ministry of Government Legislation, 2017.

[10] Ministry of the Interior and Safety, "Personal Information Protection Act," Ministry of Government Legislation, 2017.

[11] Saaty, T. L., "Decision Makingwith Dependence and Feedback: The Analytic Hierachy Process," Int. j. ServesSciences. Vol. 1. No. 1, pp. 83-98, 2008.

[12] Saaty, T. L., "The Analytic Hierachy Process," New York McGraw-Hill. International, 1980.

[13] Song, K. J., " A Study on Determination of Weight Coefficients of checklists for Privacy Impact Assessment(PIA) by means of the AHP," Dongguk University, 2010.

[14] Yoo, J. K., "A Six-sigma Handbook," Korea Productivity Center, 2009.

저 자 소 개

김세영 (E-mail : seyoung@nonghyup.com)
2016년~2018년 고려대학교 정보보호대학원 금융보안학과 석사과정
2012년~2016년 농협은행 IT본부
2017년~현재 농협중앙회 정보보호부
관심분야 개인정보보호, 정보보호정책, 전자금융법규

김인석 (E-mail: iskim11@korea.ac.kr)
2008년 고려대학교 정보경영공학대학원 박사
2009년~현재 고려대학교 정보보호대학원 교수
FDS산업포럼 회장, 한국정보보호학회 운영위원
관심분야 전자금융보안, 금융 IT 컴라이언스, 핀테크