https://doi.org/10.33778/kcsa.2020.20.3.079

개인정보 수탁사의 보안관리 대상 식별 방안 연구 : 개인정보처리방침 및 정보보호인증 데이터 이용★

최 원 녕* , 국 광 호**

요 약

인터넷 기업의 영업 이익과 업무 효율성을 높이기 위해 개인정보를 이용한 업무 위탁행위가 증가되고 있다. 개인정보를 위탁받은 업체들에서 개인정보 노출 사고가 발생하는 경우 업무를 위탁한 기업들이 고스란히 피해를 입게 된다. 본 연구는 개인정보를 위탁받은 업체들의 업무 속성들을 분석하고 개인정보의 중요도에 따른 가중치를 적용하여 개인정보 노출 위험성이 높은 업체를 식별할 수 있는 모델을 제시하는데 목적이 있다. 이를 위해 개인정보 위탁관계, 개인정보 위탁서비스, 개인정보 이용항목들을 분석하고 사회연결망 분석과 군집분석을 활용하여 네트워크 중심성이 높은 업체 중 정보보호인증 획득이 필요한 업체를 식별하였다. 본 연구 결과는 개인정보를 이용하는 기업들을 관리하는 민간기업이나 공공기업의 정보보호 전략 수립에 활용될 수 있을 것이다.

An Evaluation of the Necessity of Security Management of Personal Information Consignees : using Privacy Policy and ISMS data

Won-Nyeong Choi*, Kwang-Ho Kook**

ABSTRACT

Business consignment using personal information is increasing for the operating profit and work efficiency of Internet companies. If the personal information leakage accident occurs at the consignee, the consigner who provided personal information will be damaged greatly. The purpose of this study is to analyze the business attributes of consignee using consigned personal information and present a model that can be used to select companies with high risk of personal information leakage by considering the importance of the involved personal information. For this, personal information consignment relations, consignment services, and personal information items used were analyzed. Social network analysis and cluster analysis were applied to select companies with high network centrality that are advisable to obtain information security certification. The results of this study could be used to establish information protection strategies for private or public enterprises that manage companies using personal information.

Key words : Privacy, Consignee, Privacy Policy, ISMS, SNA, Cluster Analysis

접수일(2020년 07월 04일), 수정일(2020년 09월 22일), 게재확정일(2020년 09월 28일)

★ 이 연구는 서울과학기술대학교 교내연구비의 지원으로 수행되었음.

* 서울과학기술대학교 IT정책전문대학원 산업정보시스템 (주저자)

** 서울과학기술대학교 글로벌융합산업공학과(교신저자)

1. 서 론

기업의 영업 이익과 업무 효율성을 높이기 위해 개인정보를 이용하는 업무 위탁 행위가 증가되고 있으며 개인정보를 활용하는 취급자도 확대되고 있다. 또한 개인정보 오남용과 취급 위험이 증가함으로 인해 개인정보 취급 위탁에 관한 규정도 강화되고 있다[1]. 그러나 개인정보 이용 업무를 위탁받아 처리하는 과정에서 개인정보 처리시스템을 개발하고 운영하는 수탁사의 과실로 인해 개인정보 유출사고나 위반 사례가 발생되고 있다[2]. 일례로 2014년 카드사의 시스템 개발을 위탁받은 업체 직원이 개인정보를 유출한 사고를 들 수 있다[3]. 개인정보 위수탁 문서에 법적 의무 사항을 포함하지 않은 경우나 개인정보 이용 위탁 업무와 수탁자를 공개하지 않는 경우, 교육을 실시하지 않은 사례도 발생되고 있어 개인정보 수탁사의 관리감독의 필요성이 높아지고 있다[4].

민간기업과 공공기관들은 업무 효율성을 위해 특정 업무들에 대해서 자사에서 처리하지 않고 수탁사에게 업무를 위탁하고 있다. 특히 시스템 유지보수, 본인확인, 결제 등의 업무처리가 필요한 경우 수탁사들에게 업무를 위탁하여 업무처리를 하고 있으며 본인확인, 결제 등 특정 서비스들은 한정된 업체에 업무를 위탁하고 있다. 이러한 업무위탁에 대한 정보들은 개인정보처리방침에 공시하도록 되어 있으며, 기관/업체 서비스 홈페이지에서 확인이 가능하다[5].

그동안 국내 개인정보 수탁사에 관한 연구로서 개인정보 수탁사의 정보보호관리감독 방안에 대한 연구와 관리수준 점검 항목에 대한 연구가 진행되었다. 이들 연구에서는 수탁사 점검 기준을 수립하고 설문조사 방식으로 수탁사들의 보안수준을 점수화하였다[6][7]. 설문조사 방식이 아닌 공개데이터를 활용한 연구로서 개인정보처리방침 데이터를 이용한 위탁과 수탁관계에 대한 유통구조를 분석한 연구가 진행되었다[8]. 이 연구에서는 위수탁자의 연결관계 데이터를 활용하여 개인정보 수탁사중 집중처리자를 선별하고 이들의 관리 중요성을 강조하였다. 하지만 이 연구는 위수탁사의 단순한 연결관계만을 고려하여 집중처리 수탁사를 선별하였다. 위수탁사의 단순한 연결관계뿐만 아니라 위탁서비스에 사용되는 개인정보들의 중요성을 고려한 가중치를 적용한다면 중요한 위치의 수탁사를 보다 효율적으로 찾을 수 있을 것이다.

이에 본 연구는 공개 데이터를 활용하여 개인정보 수탁사의 업무속성을 분석하고 가중치를 적용하여 관리감독이 필요한 수탁사를 선별할 수 있는 모델을 제시하고자 한다. 이를 위해 개인정보 이용 위탁업무를 분석하고 개인정보 항목의 가중치와 정보보호인증 획득여부를 조사한 결과에 사회연결망 분석방법과 데이터 마이닝 분석기법인 군집분석방법을 적용하여 구한 결과를 결합하여 보안감독이 필요한 수탁사를 식별하는 방법을 제시한다.

2. 문헌 연구

본 장에서는 개인정보 위수탁사에 관한 선행연구들 중 개인정보 수탁사를 관리감독하기 위한 방안에 대해 분석한 연구와 개인정보 수탁사의 식별에 관한 연구, 개인정보 가중치를 적용한 연구를 살펴본다.

2.1 개인정보 수탁사 관리감독 방안연구

개인정보 수탁사를 관리감독하기 위한 연구로 이용진 등[10][11]은 금융업종 별 10개의 금융회사를 무작위 선발하고 각 회사 홈페이지의 개인정보처리방침을 조사하여 금융업종별 위탁업무를 분석하였다. 즉 은행(15개), 신용카드(15개), 증권(14개), 보험(15개), 저축은행(8개), 선물(10개)과 같이 업종별 위탁 업무의 종류를 분석하였다. 이들 업무중 대량의 개인신용정보가 이용되는 'DM발송'과 다수의 금융회사에게 제공되어 금융거래정보가 대량으로 처리되는 'CD/ATM 서비스' 업무를 선정하고 전문가 그룹을 대상으로 설문조사를 통하여 이들 업무를 수행하는 'DM발송 수탁사'와 'CD/ATM 수탁사'에 대한 관리감독의 문제점을 개선하는 방법을 제시하였다. 즉, 금융회사 위탁 업무에 대한 위험도 평가, 수탁사 업종에 대한 정보보호평가 기준 정립, 위탁 계약의 보안요구사항 관리, 전문평가기관의 수탁사 보안인증 등의 방안을 제시하였다. 강태훈 등[12]은 개인정보관련 법률과 정책분석을 통해 개인정보 수탁사들을 효과적으로 관리 감독할 수 있는 방안을 제시하였다. 이를 위해 통신사, 쇼핑몰 등 4개 기업에서 개인정보 처리 업무를 위탁받은 65개 수탁사

의 위탁업무 특성에 따라 총 9개 위탁 업무군으로 분류하고 이들을 대상으로 설문 및 증빙자료 수집을 통해 이들의 개인정보 보안수준을 분석하였다. 개인정보 수탁사들의 효율적인 관리 감독을 위한 방안으로 수탁사의 내부관리계획 표준양식 마련, 수탁사의 개인정보 담당자를 대상으로 한 정보보호 교육, 수탁사의 개인정보보호 점검절차 수립 등의 개선 방안을 제시하였다.

2.2 개인정보 수탁사 식별에 관한 연구

이재근 등[8]은 개인정보처리자가 인터넷 홈페이지에 공개하는 개인정보처리방침 데이터에 네트워크 이론을 접목하여 개인정보의 유통구조를 분석하는 방법을 제안하였으며 개인정보를 많이 수탁하는 업종 및 개인정보 집중처리자를 식별할 수 있음을 보였다. 이를 통해 개인정보가 집중되는 업종들과 개인정보 집중처리자들의 개인정보보호에 보다 많은 자원을 투입하여 성과를 높일 수 있음을 밝혔다. 또한 이재근[9]은 개인정보처리자의 규모, 처리방침 공시수준, 개인정보 민감도를 이용하여 개인정보보호 성과수준을 예측하는 회귀모형을 수립하고 이를 이용하여 개인정보처리자의 개인정보보호 수준을 추정할 수 있음을 보였다. 이를 통해 개인정보처리방침 데이터를 활용하여 개인정보보호 성과 예측 모델과 개인정보의 위탁 정보를 결합하면, 개인정보 수탁사중 개인정보보호 성과가 낮은 개인정보처리자를 분석하는 것이 가능함을 보였다.

2.3 개인정보 가중치(자산가치)에 관한 연구

개인정보파일을 구축 및 운영하는 공공기관은 개인정보보호법 제33조에 의해 개인정보 영향평가를 수행하고 있다. 이와는 다르게 민간기업은 자율적으로 수행할 수 있다. 개인정보 영향평가는 개인정보가 처리되는 사업 추진시 개인정보 영향분석을 통해 개선방안을 수립하여 적용함으로써 개인정보 침해사고를 사전에 예방하는것에 목적이 있다. 행정안전부장관은 개인정보 영향평가에 필요한 세부기준을 구체화한 영향평가 수행안내서를 마련하여 제공하고 있으며, 한국인터넷진흥원에서 발행한 개인정보 영향평가 수행안내서에서는 개인정보 영향도의 산정을 위해 개인정보 등급별 자산가치 점수를 적용하도록 안내하고 있다. 특히 개인정보의 자산가치는 영향평가 기관의 평가 방법에 따라 달라질 수 있음을 함께 명시하고 있다[13].

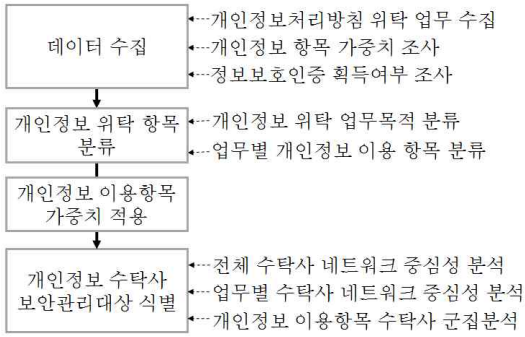
개인정보 자산가치를 활용한 개인정보 영향평가 관련 연구들은 다양하게 진행되었다. 이기성 등[14]은 위험수준 산정 모델을 제시하는데 활용하였으며, 천명호 등[15]은 SNS에서 개인정보 사용형태를 고려하여 개인정보 자산가치를 측정하는데 활용하였다. 전동진 등[16][17]의 연구에서는 개인정보 위험평가에 자산가치 수치를 활용하였고 다른 연구에서는 K병원의 개인정보 영향평가 분석 사례 연구에 활용되었다. 또한 정해산[18]은 실제 사례를 통해 개인정보 영향평가 제도 운영 실태를 분석하고 제도의 문제점에 대한 개선방안을 제시하였으며, 김형건[19]은 개인정보의 영향도 평가 기준을 사용하여 형태소 분석을 통해 개인정보보호 영향도 평가 시스템을 제안하는데 활용하였다. 선행 연구들에서는 개인정보 영향평가 수행안내서의 절차 및 방법론을 활용하였고 이 중 최근 연구에서는 2018년 발행한 개인정보 영향평가 수행안내서에 명시된 개인정보 영향도 1등급 자산가치 5점, 2등급 자산가치 3점, 3등급 자산가치 1점을 적용하였다[18][19].

3. 연구 방법

본 장에서는 연구 절차와 연구범위에 대해 설명한다. 그리고 본 연구에서 제안하는 개인정보 항목별 가중치를 적용하기 위한 방법을 설명한다.

3.1 연구 절차

본 연구에서는 (그림 1)과 같이 수집된 데이터를 활용하여 개인정보 위탁사에 대한 위탁업무목적을 분류하고 개인정보 위탁업무별 개인정보 이용항목을 분석한다. 다음 단계로 개인정보 항목별 중요도를 판단하여 개인정보 등급에 따른 가중치를 산정하며, 마지막 단계로 사회연결망 분석을 적용하여 정보보호관리가 필요한 수탁사를 식별하는 방안에 대해 서술한다.



(그림 1) 연구 절차

3.2 개인정보 데이터 수집 및 위탁업무조사

설문조사 방식은 쉽게 행해질 수 있고 지리적인 한계점 극복 및 많은 응답을 빠른 시간에 얻을 수 있기 때문에 데이터 수집에 많이 활용되고 있다. 그러나 설문답변자에게 설문에 대한 부담감을 줄 수 있으며, 불성실한 답변, 설문답변자가 설문문항을 정확히 이해하지 못함에 의한 데이터의 신뢰성 문제가 발생할 수 있고, 설문 비응답자들에 의한 편차(bias)가 발생할 수 있다. 따라서 본 연구에서는 설문조사 방식이 아닌 공개데이터만을 활용하여 개인정보 위수탁자간의 업무속성을 조사하고 위탁업무를 분류하였으며 분류된 위탁업무에 따라 수탁사에서 사용하는 개인정보 이용항목들을 조사하였다.

본 논문은 인터넷 대표기업 10개사의 개인정보 위수탁업무에 대해 분석하였다. 2018년 매출기준 상위 포털4사, 쇼핑몰3사, 게임3사를 선정하였으며, 2018년 11월부터 2019년1월 사이 공시된 대표 홈페이지의 개인정보처리방침 데이터를 수집하였다. 수집된 데이터 중 위탁업무내용(수탁업체)을 분석하여 수탁업체 131곳을 선정하였다.

131곳의 위탁업무를 분류한 결과 <표 1>과 같이 결제서비스(카드결제, 편의점결제, 계좌이체, 상품권결제, 휴대폰결제, 간편결제, 무통장입금, 가상계좌결제), 본인확인/인증서비스(본인확인, 계좌인증, 신용카드인증, 전화번호인증), 배송서비스(배송, 픽업), 고객상담서비스(상담, ARS), 그 외에 현금영수증발행, 제세공과금처리, 문자발송, 안심번호서비스, 이벤트대행 등으로 분류되었다.

<표 1> 위탁업무분류에 따른 개인정보 이용항목

위탁업무분류		개인정보 이용항목
결제서비스	카드	이름,성별,생년월일,연락처, 아이핀번호,CI,카드번호, 카드유효기간,CVC번호
	편의점	카드번호,승인번호
	계좌이체	은행명,계좌번호
	상품권	상품권번호
	휴대폰	성별,생년월일,연락처,통신사
	간편	연락처,상품명
	무통장입금	이름,은행명
	가상계좌	이름,은행명,이메일,연락처 (현금영수증)
본인확인/인증서비스	본인확인	이름,성별,생년월일,내외국인여부, 연락처,이동통신사,CI,DI
	계좌인증	이름,성별,생년월일,계좌번호
	신용카드	이름,성별,생년월일,내외국인여부, 카드번호,카드유효기간,비밀번호앞2자리
	전화번호	연락처
배송서비스	배송	이름,연락처,주소
	픽업	이름,연락처
고객상담서비스	상담	이름,생년월일,연락처,주소
	ARS	연락처
기타서비스	현금영수증발행	연락처
	제세공과금처리	이름,연락처,주민등록번호
	문자발송	연락처
	안심번호서비스	연락처
	이벤트대행	이름,연락처

분류된 위탁업무에 따라 수탁사에서 위탁사가 수집한 개인정보항목 중 어떤 항목들을 사용하는지 조사하였다. 이를 위해 웹사이트의 개인정보처리방침 내용에 위탁업체의 개인정보 이용항목이 명시되어 있는 카드사 4곳, A편의점, B-point, C-pay 등을 조사하였으며, 실제 위탁업무를 수행하는 기업인 PG(Payment Gateway)사 2곳의 서비스 소개자료 등을 확인하여 <표 1>의 위탁업무분류에 따른 개인정보 이용항목을 조사하였다. 조사한 내용 중 개발/유지보수 위탁업무에 사용되는 개인정보항목은 특정 지을 수 없어 대상에서 제외하였다.

3.3 개인정보 이용항목별 가중치 조사

최근 선행연구에서 활용하였던 2018년 행정안전부와 한국인터넷진흥원(KISA)에서 발간한 개인정보 영향평가 수행안내서를 활용하여 <표 2>와 같이 본 논문에서 사용할 개인정보 이용 항목별 개인정보 가중치를 적용하였다. <표 1>에서 분류한 개인정보 이용항목과 <표 2>의 개인정보 자산가치 항목을 살펴 본 결과 3등급의 정보는 이용되지 않아 1등급, 2등급의 개인정보만을 고려하였다. 가중치 적용방법은 선행연구에서와 동일하게 위탁업무별 개인정보 이용항목이 1등급으로 분류된 항목을 하나라도 포함하면 해당 업무의 개인정보의 가중치를 5점으로 평가하였고 그 외는 2등급인 3점으로 가중치를 평가하였다[13][18][19].

<표 2> 개인정보 가중치[13]

등급	자산 가치	설명	분류	개인정보
1 등급	5	개인의 식별이 가능	고유식별정보	주민등록번호
		민감한 개인정보	인증정보	비밀번호
		법령에 따른 제한 정보	신용/금융정보	카드번호, 계좌정보
2 등급	3	조합이 되면 개인의 식별이 가능	개인식별정보	이름, 성별, 생년월일, 연락처, 주소, 이메일 등
3 등급	1	개인식별 정보와 조합된 간접 개인정보	자동생성정보	IP정보, MAC주소, 쿠키 등

3.4 개인정보 수탁사 정보보호인증획득 조사

정보보호 인증획득여부는 기업이 정보보호에 대한 조치와 활동이 적합함을 증명하는 제도이며, 정보보호 활동의 효율성을 평가할 수 있는 항목 중 하나이다[20]. 인증획득 업체를 조사하기 위해 한국인터넷진흥원 홈페이지에 2002년부터 2019년 6월까지 공시된 정보보호관리체계 인증 및 개인정보보호관리체계 인증을 획득한 796개의 업체 정보를 수집하였다. 이 정보들을 개인정보 수탁사명과 비교하여 인증획득 유무를 1차 확인하였고 영문/국문회사명, 회사명칭 변경부분까지 2차 확인하였으며 각 수탁사들의 대표홈페이지에 방문하여 인증획득 유무를 3차 확인하였다. 인증을 획득한 수탁사들 대부분은 대표 홈페이지 첫페이지에 인증마크를 공시하거나 회사소개 메뉴와 언론기사를 통해 인증획득여부를 공표하고 있었다. 연구대상의 131개 수탁사 중 52개사가 정보보호 인증을 획득한 기업으로 최종 확인되었다[5][21].

3.5 개인정보 위수탁 네트워크

개인정보를 위탁하고 수탁하는 기업들 사이의 관계는 사회연결망 분석을 통해 분석될 수 있다. 개인정보 위수탁 네트워크는 개인정보처리자(노드), 위탁관계(에지), 위탁업무흐름(링크방향)으로 표현될 수 있다. 개인정보 위수탁 관계에 의한 개인정보 업무의 흐름은 위탁사에서 수탁사로 단방향으로 전달되며 1개의 위탁사는 다수의 수탁사에게 개인정보 업무를 위탁하고 있다. 수탁사의 입장에서는 다수의 위탁사들이 한 수탁사에 개인정보업무를 위탁할 수 있으므로 업무 집중처리 수탁사가 존재한다. 본 논문에서는 내향 연결 정도 중심성(In-Degree Centrality)을 이용하여 개인정보 수탁사의 가중치를 평가한다. 이때 <표 2>의 개인정보 가중치를 이용하여 위탁사에서 수탁사로 전달되는 개인정보 항목들의 자산가치에 의해 위탁사에서 수탁사로의 해당 에지의 가중치로 적용한다.

4. 연구 결과

본 장에서는 보안관리가 필요한 수탁사를 선별하기 위해 가중치를 적용하여 수탁사의 중심성을 분석한다. 이를 위해서 사회연결망분석툴인 UCINET 6.6을 이용하였다. 또한 유사 서비스 및 업종별로 개인정보 이용정도의 비교 분석을 위해서 SPSS 21.0 분석툴을 사용하여 군집분석을 진행하였다.

4.1 가중치를 적용한 수탁사 식별

개인정보의 가중치를 고려하지 않은 경우와 본 연구에서 제안하는 가중치를 고려하는 방법을 통해 네트

워크 중심성을 비교분석한 결과는 <표 3>과 같다. 상위 10개 업체 중 'B사' 는 제안한 연구방법으로 분석하였을 경우 선행연구에서와 같이 가중치를 고려하지 않은 경우보다 내향 연결 정도 중심성이 낮아져 수탁사 순위가 5단계 하락하고 'L사, M사'는 'H사'보다 높아 순위가 상승하는 결과를 확인하였다. 이러한 변화는 보다 더 중요한 개인정보를 이용하는 수탁사의 가중치가 높아짐에 따라 선행 연구방법에서 단순한 위수탁의 연결관계만을 고려한 결과와 다른 결과를 보여준다.

<표 3> 가중치 적용/비적용시 상위 10개 수탁사 분석 결과

가중치 비 적용시		가중치 적용시	
수탁사	In-Degree	수탁사	In-Degree
A사	0.05760	A사	0.21583
B사	0.04317	C사	0.17986
C사	0.03597	D사	0.17986
D사	0.03597	E사	0.17986
E사	0.03597	F사	0.16547
F사	0.03597	G사	0.16547
G사	0.03597	B사	0.12950
H사	0.02878	L사	0.11511
I사	0.02878	M사	0.10791
J사	0.02878	H사	0.08633

4.2 정보보호인증이 필요한 수탁사 식별

개인정보의 가중치를 고려하여 네트워크 분석을 통해 얻어진 상위 40개 수탁사들의 정보보호인증 획득여부를 조사한 결과는 <표 4>와 같다. <표 4>로부터 중심성이 높은 것으로 평가되는 In-Degree Centrality가 0.08633 인 'I사'가 정보보호인증을 획득하지 못한 것으로 나타났다. 해당 기업은 4개의 위탁사에서 본인확인 업무를 위탁받은 수탁사로 보안관리가 필요한 개인정보 수탁사로 판단된다. 또한 'V사, W사, X사, Y사, Z사'도 In-Degree Centrality가 비교적 상위에 있는 데 정보보호인증을 획득하지 못한 것으로 나타났다. In-Degree Centrality가 0.05755 미만인 수탁사들 중에서는 절반정도가 정보보호인증을 획득한 것으로 나타났다.

<표 4> 제안 연구 수탁사 상위 40개 분석 결과

수탁사	In-Degree	인증획득	수탁사	In-Degree	인증획득
A사	0.21583	획득	V사	0.05755	미획득
C사	0.17986	획득	W사	0.05755	미획득
D사	0.17986	획득	X사	0.05755	미획득
E사	0.17986	획득	Y사	0.05755	미획득
F사	0.16547	획득	Z사	0.05755	미획득
G사	0.16547	획득	AA사	0.05755	획득
B사	0.12950	획득	AB사	0.05755	획득
L사	0.11511	획득	AC사	0.04317	획득
M사	0.10791	획득	AD사	0.04317	미획득
H사	0.08633	획득	AE사	0.04317	미획득
I사	0.08633	미획득	AF사	0.04317	획득
J사	0.08633	획득	AG사	0.04317	미획득
N사	0.08633	획득	AH사	0.04317	획득
O사	0.07194	획득	AI사	0.04317	획득
P사	0.07194	획득	AJ사	0.04317	미획득
Q사	0.07194	획득	AK사	0.03597	획득
R사	0.06475	획득	AL사	0.03597	획득
S사	0.06475	획득	AM사	0.03597	미획득
T사	0.06475	획득	AN사	0.03597	미획득
U사	0.06475	획득	AO사	0.03597	미획득

위탁업무별로 개인정보 이용정도가 다르므로 위탁업무별 수탁사들의 정보보호인증 획득 여부를 분석한 결과 <표 5>와 같이 결제업무는 25곳 중 22곳이, 안심서비스업무는 5곳 중 4곳이 정보보호인증을 획득하였음을 볼 수 있다.

<표 5> 위탁업무별 정보보호인증 획득 분석 결과

위탁업무별	획득	미획득	총합계
결제	22	3	25
안심서비스	4	1	5
간편결제	2	-	2
문자발송	5	6	11
배송	5	25	30
본인확인	5	4	9
상담	6	12	18
이벤트 대행	1	9	10
제세공과금 처리	1	13	14
휴대폰 결제	1	-	1
신용카드 인증	-	1	1
전화번호 인증	-	2	2
픽업	-	1	1
현금영수증 발행	-	1	1
ARS	-	1	1
총합계	52	79	131

이중 정보보호인증 획득업체 비율이 높은 결제업무에 대해 중심성이 높은순으로 정렬하였을때 <표 6>과 같이 중심성이 비교적 높은 In-Degree Centrality가 0.05755 인 3곳 중 정보보호인증을 획득하지 못한 'W사' 는 개인정보이용에 대한 보안관리감독이 필요한 수탁사로 확인되었다.

<표 6> 결제 업무 수탁사 중심성 분석 결과

결제 업무 수탁사	In-Degree	인증획득
A사	0.215827	획득
E사	0.179856	획득
D사	0.179856	획득
C사	0.179856	획득
G사	0.165468	획득
F사	0.165468	획득
L사	0.115108	획득
M사	0.107914	획득
Q사	0.071942	획득
P사	0.071942	획득
O사	0.071942	획득
AA사	0.057554	획득
AB사	0.057554	획득
W사	0.057554	미획득
BA사	0.035971	획득
BB사	0.035971	획득
BC사	0.035971	획득
BD사	0.035971	획득
BE사	0.035971	획득
BF사	0.035971	획득
BG사	0.035971	획득
AL사	0.035971	획득
AK사	0.035971	획득
BH사	0.035971	미획득
AN사	0.035971	미획득

<표 5>에서 정보보호인증 획득업체 비율이 높은 안심서비스 업무에 대한 수탁사 중심성 분석 결과는 <표 7>과 같다. <표 7>에서 In-Degree Centrality가 0.021583인 'AR사' 는 정보보호인증을 획득하지 못하였는데 동일한 중심성을 가진 업체들이 정보보호인증을 받은 점을 고려할 때 보안관리감독이 필요한 수탁사로 확인되었다.

<표 7> 안심서비스 업무 수탁사 중심성 분석 결과

안심서비스 업무 수탁사	In-Degree	인증획득
AH사	0.043165	획득
AF사	0.043165	획득
AP사	0.021583	획득
AQ사	0.021583	획득
AR사	0.021583	미획득

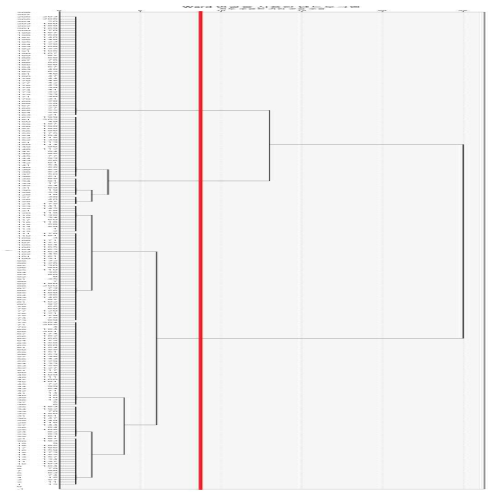
4.3 군집분석을 활용한 수탁사 식별 분석

수탁사들의 유사성은 앞절에서와 같이 위탁업무에 따라 분류할 수도 있지만 데이터 분석 기법인 군집분석을 통해 분류될 수도 있다. 수탁사들의 유사성을 개인정보 이용항목들의 유사성에 따라 분류하기 위해 <표 8>과 같이 수탁사들의 개인정보 이용항목들을 매트릭스 형태로 정렬하였다. 매트릭스의 각행은 수탁업체를 나타내며 각열은 <표 1>의 위탁업무에서 분석된 사용하는 개인정보 항목들을 나타낸다. i번째 행의 수탁업체가 j번째 열의 개인정보항목을 이용하는 경우에는 (i, j)번째 원소가 1로 표현되며 이용하지 않는 경우에는 0으로 표현된다.

<표 8> 수탁사별 개인정보 이용항목 매트릭스

수탁사명	개인정보 이용항목				
	이름	성별	생년월일	…	…
A사	1	1	0	1	1
B사	1	0	1	1	0
…	0	1	1	1	1

데이터들을 명목척도로 설정한 후 유클리디안 거리(Euclidean Distance)를 이용하여 수탁사별 거리를 산정하였다. Ward 연결법을 사용하여 계층적 군집분석을 수행하고 덴드로그램을 확인하여 (그림 2)와 같이 군집간의 거리가 비교적 먼 3개의 군집을 최종적으로 선정하였다. 첫 번째 군집은 '편의점결제, 계좌이체, 상품권결제, 간편결제, 무통장입금, 가상계좌결제, 전화번호인증, 배송, 픽업, 상담, ARS, 현금영수증발행, 제세공과금처리, 문자발송, 안심번호서비스, 이벤트대행' 수탁사들로, 두 번째 군집은 '신용카드결제, 신용카드인증' 수탁사들, 세 번째 군집은 '휴대폰결제, 본인확인, 계좌인증' 수탁사들로 군집이 나눠짐을 볼 수 있다.



(그림 2) 수탁사별 덴드로그램

이중 첫 번째 군집에서 In-Degree 중심성을 높은 순으로 정렬 후에 인증여부를 확인한 결과 정보보호인증을 획득하지 못한 In-Degree Centrality가 0.057554인 'V사, W사, Y사, Z사'들이 개인정보관리가 필요한 수탁사들로 확인되었으며, 두 번째 군집에서는 In-Degree Centrality가 0.057554인 'X사'가 개인정보관리가 필요한 수탁사로 확인되었다.

<표 9> 세 번째 군집의 수탁사 중심성 및 인증여부 분석 결과

세 번째 군집 수탁사	In-Degree	인증여부
A사	0.215827	획득
D사	0.179856	획득
F사	0.165468	획득
G사	0.165468	획득
B사	0.129496	획득
H사	0.086331	획득
J사	0.086331	획득
I사	0.086331	미획득
S사	0.064748	획득
AB사	0.057554	획득
X사	0.057554	미획득
AS사	0.021583	획득
AT사	0.021583	획득
AU사	0.021583	미획득
AV사	0.021583	미획득

세 번째 군집에서는 <표 9>와 같이 In-Degree Centrality가 0.086331인 'I사'가 개인정보관리가 필요한 개인정보 수탁사로 확인되었다. 'I사'는 법적으로 정보보호인증을 획득해야 하는 회사는 아니지만 중심성도 높고 위탁사의 본인확인관련 정보를 처리하는 수탁사이므로 관리감독이 필요한 회사로 판단된다. 또한 군집 분석을 통해 'I사, V사, W사, X사, Y사, Z사'들이 개인정보관리가 필요한 수탁사로 확인되었는데 이는 <표 4>에서 살펴본 In-Degree Centrality가 높은 수탁사들중 인증을 획득하지 못한 회사들과 일치하는 결과를 얻을 수 있음을 알 수 있다.

5. 결 론

본 연구는 공개데이터인 개인정보처리방침 데이터의 개인정보 위탁업무내용을 수집하고 수탁사의 업무속성 및 개인정보 가중치를 조사하였다. 이를 토대로 가중치를 고려하는 사회연결망 분석방법과 군집 분석방법을 적용하여 개인정보 관리감독이 필요한 개인정보 수탁사를 식별할 수 있는 모델을 제시하였다. 가중치를 고려하면 가중치를 고려하지 않는 경우와 중심성이 변화함을 볼 수 있다. 이는 중요한 정보를 이용하는 수탁사에 가중치를 부여함으로써 개인정보의 중요성을 고려하여 네트워크 중심성이 높은 수탁사를 식별하는 것을 가능하게 한다. 이와 함께 제안한 연구방법에 정보보호인증획득 결과를 결합함으로써 중심성이 높은 수탁사 중 정보보호인증을 획득하지 못한 수탁사를 식별할 수 있었다.

본 연구의 의의는 다음과 같다. 첫째, 공개 데이터를 이용하여 단순한 개인정보 위수탁관계만이 아닌 개인정보의 중요도에 따른 가중치를 적용하여 개인정보를 활용하고 있는 중요 수탁사를 식별할 수 있는 방법론을 제시하였다. 둘째, 수탁사들의 네트워크 중심성과 정보보호인증획득 정보를 결합하여 정보보호인증획득이 필요한 수탁사를 평가할 수 있는 방법을 제시하였다. 제안된 방법론은 공공기관에서 수탁사 점검시에 우선적으로 보안점검이 필요한 수탁사를 식별하는 데 사용 될 수 있다. 또한 동종업계 위탁사들이 수탁업체를 공동관리하기 위한 보안관리 전략을 수립하는데 도움을 줄 수 있다.

본 연구의 한계점은 다음과 같다. 첫째, 개인정보취급방침의 자동화 수집부분이 어려워 IT전체업종을 연구대상으로 모두 고려하지 못하였다. 둘째, 위수탁업무를 분류하는 과정에서 위탁사의 개인정보업무 서비스 형태에 따라 업무 분류 및 개인정보 이용형태, 가중치 선정 방법도 다양할 수 있어 일반화 하는데 어려움이 있다. 한계점으로 파악된 부분들은 향후 위탁사 범위와 특정 업무서비스 형태의 기준이 명확하게 정해진다면 해결이 가능할 것이다.

향후에는 문헌연구와 전문가들의 추가분석을 통한 가중치 선정방법에 대한 연구를 진행하여 개인정보 관리감독이 필요한 수탁사를 식별하는 모델을 강화하는 연구가 필요할 것이다.

참고문헌

[1] 행정안전부, 한국정보보호진흥원, '민간기업 개인정보 매뉴얼', pp. 10, 2008.

[2] 행정자치부 보도자료, "6천여 IT수탁사에 대한 대대적인 개인정보관리실태 점검실시", 2015.4.3.

[3] 금융위원회, "신용카드업자 고객정보 유출 관련 현황 및 대응방안", 2014.1.8.

[4] 보안뉴스 홈페이지, <https://www.boannews.com/media/view.asp?idx=69505>, 2018.5.18.

[5] 행정안전부, '개인정보보호법', 법률 제14839호, 2017.7.26.

[6] 강태훈, "개인정보보호 수탁사 관리체계 강화 방안 연구", 高麗大學校 情報經營工學專門大學院, 2014.

[7] 임동성, 이상준, "수탁사 개인정보 관리 수준 점검 항목의 상대적 중요도 분석", 예술인문사회융합멀티미디어논문지, 제8권, pp. 1-11, 2018.

[8] 이재근, 김현진, 강상욱, 염흥열, "네트워크 이론을 적용한 개인정보 유통구조 분석", 정보화정책, 제21권, 제1호, pp. 17-34. 2014.

[9] 이재근, "개인정보보호 정책 공시 데이터를 이용한 개인정보보호 성과 수준 예측모델에 관한 연구", 순천향대학교 대학원, 2014.

[10] 이용진, "금융회사 개인신용정보 수탁사에 대한 관리·감독 현황 및 개선방향에 관한 연구", 高麗大學校 情報保護大學院, 2014.

[11] 이용진, 임종인, "금융회사 개인신용정보 수탁사에 대한 관리·감독 현황 및 개선 방향에 대한 연구", 보안공학연구논문지, 제11권, 제3호, pp. 233-250, 2014.

[12] 강태훈, 임종인, "개인정보보호 수탁사 관리체계 강화 방안 연구", 정보보호학회논문지, 제23권, 제4호, pp. 781-797, 2013.

[13] 행정안전부, 한국인터넷진흥원, '개인정보 영향평가 수행안내서', 201804.

[14] 이기성, 안효범, 이수연, "개인정보 노출을 예방하는 방법에 관한 연구", 융합보안 논문지, 제12권, 제1호, pp. 71 - 77, 2012.

[15] 천명호, 최종석, 신용태, "SNS에서 개인정보유출방지를 위한 개인정보 유출위험도 측정 방법", 정보보호학회논문지. 제23권, 제6호, pp. 1199 - 1206, 2013.

[16] 전동진, 정진홍, "C쇼핑몰 개인정보 영향평가 사례연구", 한국산업정보학회논문지, 제17권, 제6호, pp. 73 - 82, 2012a.

[17] 전동진, 정진홍, "개인정보 영향평가 사례 연구", 디지털융복합연구, 제10권, 제8호, pp. 149 - 157, 2012b.

[18] 정해산, "공공기관 개인정보영향평가제도의 실효성 확보방안 연구", 고려대학교 정보보호대학원, 2018.

[19] 김형건, 최석환, 윤광욱, 최윤호, "회원가입 약관 정보 자동 수집을 통한 웹기반 개인정보보호 영향도 평가 시스템", 정보과학회 컴퓨팅의 실제 논문지, 제25권, 제9호, pp. 425 - 435, 2019.

[20] 최원녕, 김우제, 국광호, "기업의 정보보호활동의 효율성 평가", 융합보안논문지, 제18권, 제5호, pp. 25-32, 2018.

[21] 한국인터넷진흥원 홈페이지, <https://isms.kisa.or.kr/main/isms/issue/>, 2019.7.

〔저자소개〕

최 원 녕 (Won-Nyeong Choi)
2020년 서울과학기술대학교
IT정책전문대학원
산업정보시스템전공 박사과정
email : dsu94@daum.net

국 광 호 (Kwang-Ho Kook)
1979년 서울대학교 산업공학사
1981년 서울대학교 대학원 산업공학 석사
1989년 미조지아 공과대학교 대학원 산업공학박사
1989년 ~ 1993년 한국전자통신연구원 선임연구원
1993년 ~ 현재 서울과학기술대학교 글로벌융합산업공학과 교수
email : khkook@seoultech.ac.kr