ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

위탁자의 개인정보보호 관리역량 제고에 관한 연구

A Study on the Management Capabilities Enhancement of Consignor's Personal Information Protection

정 환 석[1] 박 억 남[1] 이 상 준[2*]
Hwan-Suk Cheong Euk-Nam Park Sang-Joon Lee

요 약

주민번호를 포함한 개인정보의 처리업무는 상당한 전문지식과 많은 비용이 소요되어 IT 전문 업체에 위탁 처리하는 경우가 보편화 되었다. 개인정보 관련 사고는 점차 증가하고 있으며, 사고 유형의 대부분은 수탁자에 의한 누출 혹은 유출에 의해 발생하고 있다. 개인정보보호 실태점검과 관리수준 진단 결과 공공기관에서의 수탁자에 대한 개인정보 사고 예방노력과 개인정보보호 관리체계 구축 노력이 시급한 상황이다. 본 논문에서는 개인정보 보호의 효율적 제고 방안에 대하여 연구하였다. 개인정보 처리 업무위탁에 대한 법률사항을 분석하고, 관리체계 구축을 위한 법률 기준 지표를 선택하여, 수탁자에 대한 개인정보보호 관리수준 분석 방안과 수탁자 개인정보보호 관리체계 강화 방안을 제시하였다. 개인정보보호 관리체계 강화 방안으로 수탁자 개인정보보호 관리체계를 제시하였고, 세 가지 법률 강화방안을 제시하였다. 본 논문에서는 개인정보보호 관리체계 강화 방안을 구성하기 위하여 공공기관의 대표적 개인정보 처리 위탁업무 중 IT유지보수, 고지서인쇄, 콜센터와 관련된 30개 수탁자들을 대상으로 설문조사를 통해 조사하였고, 강화방안에 대한 문헌 근거를 제시하였으며, 개인정보 위탁자와 수탁자에 대한 FGI를 통해 강화방안에 대한 검증을 실시하였다.

☞ 주제어 : 개인정보, 개인정보보호법, 개인정보보호 관리체계, 위탁자

ABSTRACT

Personal information processing works, including resident registration number is common to be consigned by IT specialized company due to high level expertise and tremendous cost. The accident related to personal information is increasing and most of accidents are caused by the consignee's leaking information. According to the Inspection of personal information protection and the management level diagnosis of personal information protection, public Institutions need to build the consignee's accident prevention and personal information management system as soon as possible. In this paper, the efficient enhancement ways for the personal information protection is studied. We analyze the law of business consignment and select basic management items related with personal information protection, and propose a analysis scheme for management level of personal information protection and a enhancement scheme for management system of personal information protection. This paper suggests consignee's management system of personal information protection for the enhancement way and the three Strengthening ways in law. To compose the a enhancement scheme for management system of personal information protection, we conduct questionnaire survey to 30 consignees(IT maintenance, notice printing, call center, welfare center) related to typical tasks of public organizations, present reference for this scheme, and execute verification of this scheme by focus group interview of consignor and consignee.

☞ keyword : Personal Information, Personal Information Protection Act, Personal Information Protection Management System, Consignor

1. 서 론

IT기술의 급속한 발전으로 인해 우리의 생활 전반을 포함한 모든 업무가 IT와 관련을 가지게 되었다. 이러한 IT 의존도가 높아질수록 그에 따른 서비스의 질은 높아지겠지만, 정보보호 관련 사고의 피해규모는 날로 커지고 있고 다양해지고 있다. 전 세계가 네트워크로 연결된 현대사회에서는 개인, 기업, 국가의 침해사고는 연쇄적이면서 빠르게 그 피해를 전파하게 되며, 피해의 확산 방지를 위해서는 개인과 기업, 국가의 적극적인 정보보호 활동을 필요하게 된다.

이를 위해 국내에서는 여러 법이 제정 되었고, 그 중 개인정보보호법의 제정('11.3월), 시행('11.9월)은 법률적

[1] Graduate School of Information Security, Chonnam National University, Gwangju, 61186, Korea.
[2] Graduate School of Business Administration, Chonnam National University, Gwangju, 61186, Korea.
* Corresponding author (s-lee@jnu.ac.kr)
[Received 8 January 2016, Reviewed 26 January 2016(R2 4 May 2016), Accepted 13 June 2016]

개인정보보호 관리의 기준을 제시하고 있다. 하지만, 이런 일련의 노력에도 불구하고 개인정보 누출/유출사고는 지속적으로 발생되고 있다. 특히, 우리나라는 발전된 IT인프라와 함께 주민번호 중심의 개인식별체계가 운영되고 있어 정보유출에 따른 피해가 더욱 큰 상황이다. 2014년 7월 관계부처 합동으로 발표한 '개인정보보호 정상화대책'에 따르면 개인정보 관련 사고 발생 시, 가장 대표적인 유출정보는 주민번호이다[1].

주민번호를 포함한 '개인정보의 처리업무'는 상당한 전문지식과 많은 비용이 소요되어 IT 전문업체(수탁자)에 위탁 처리하는 비율이 84%에 이르고 있다[2]. 하지만, 개인정보보호법 제정이후 2012년 한 해 전체 사업체 중 0.6%가 개인정보 누출 또는 유출사고를 겪은 적이 있는 것으로 나타났고, 법 제정 원년 대비 0.1%P 증가한 것으로 나타났다[3]. 개인정보 누출·유출사고가 있었던 사업체의 73.8%가 '수탁자에 의한 누출·유출'인 것으로 나타나 개인정보 보호와 관련하여 수탁자들의 역할이 매우 큰 것으로 분석되었다.

공공기관에서의 개인정보 처리 업무위탁의 중요성에 대하여는 '2014년 범정부TF 개인정보보호 실태점검 결과'와 '2014년 공공기관 개인정보보호 관리수준 진단 결과'에서도 확인 할 수 있다. 2014년 초 범정부TF팀은 공공기관 및 민간기업체를 대상으로 13개 분야 64개 항목에 대한 개인정보보호 실태점검을 실시하였다. 그 결과 공공기관과 민간기업 모두 '업무 위탁 시 준수사항 위반(15.7%)', '수집·이용 동의 위반(10.1%)', '안전조치 의무 위반(8.1%)', '파기절차 미 준수(8.1%)', '개인정보취급자에 대한 관리감독 미흡(7.5%)' 등의 순으로 위반비율이 높은 것으로 나타났다. 특히, 업무 위탁 및 파기와 관련해서는 대량 유출사건의 원인이 되므로 더욱 많은 관심과 활동이 필요한 상황이다[4].

이와 더불어 행정자치부와 한국인터넷진흥원(KISA)은 2012년부터 '공공기관 개인정보보호 관리수준 진단'을 실시하고 있다. 2012년 189개 기관 3개분야 12개지표 21개 항목으로 시작하여, 2015년에는 738개 기관 3개분야 12개지표 24개항목으로 확대 실시하였다. 이는 개인정보보호법 시행 이후 각 공공기관들이 스스로 개인정보를 안전하게 관리하고, 침해예방 및 보호활동을 수행하도록 유도·지원하기 위함이다. 2015년 관리수준진단 결과에 의하면 '접근권한 관리', '수탁업체 관리/감독'등 관리체계 구축 및 시행부분은 개선이 시급한 항목으로 나타났다[5]. 실태점검과 관리수준진단 결과 공공기관에서의 수탁자에 대한 개인정보 사고 예방노력과 개인정보보호 관리체계 구축 노력이 시급한 상황이다.

위탁자와 수탁자의 연관관계를 살펴보면, 위탁자는 개인정보 처리 업무들에 대하여 각각 하나의 수탁자에게 업무를 위탁하고 있는 반면 하나의 수탁자는 다수의 위탁자를 대상으로 개인정보 처리 업무를 위탁받아 처리하고 있다. 따라서, 한 수탁자를 대상으로 관리체계를 구축 및 강화한다면, 그 수탁자에게 업무를 위탁한 여러 다른 위탁자들의 개인정보들은 강화된 관리체계에 의하여 자연스럽게 관리 및 처리 될 수 있다.

더욱이 법률에서는 위탁자의 수탁자에 대한 개인정보보호 관리·감독 의무사항을 규정하고 있다. 하지만, 수탁자에 대한 관리체계 강화방법이나 관리 · 감독 방법에 있어 구체적이지 않고 위탁자 스스로 판단하고 준비하여 관리/감독토록 하고 있어 위탁자 입장에서도 애로사항이 많은 상황이다. 또한 수탁자 입장에서는 별도의 비용과 시간을 투자하여 이에 대비하여야 한다. 정보보호를 위한 투자가 가능한 대기업이나 중견기업에서도 이에 대한 준비와 활동에는 적지 않은 예산과 자원이 투입된다. 하지만 대다수 IT관련 수탁자들의 경우는 그에 따른 준비나 활동보다는 위탁받은 업무를 처리하기에 급급한 경우가 많아 IT기업에서 유독 사건/사고가 많이 발생하고 있으며, 수탁자 표준 관리체계 및 관리방안 수립이 절실한 상황이다.

따라서, 본 연구에서는 개인정보 처리 업무위탁에 대한 법률사항 분석을 통하여 관리체계 구축을 위한 법률 기준 지표를 수립하고, 수탁자에 대한 개인정보보호 관리수준 분석 후 미흡사항을 도출하고, 이를 교육 및 컨설팅 수행을 통해 수탁자가 직접 보완 및 관리체계를 수립/이행할 수 있도록 하여 위탁자와 수탁자 모두 개인정보처리에 대한 효율적인 관리가 되도록 하는 개인정보 보호의 효율적 제고 방안에 대하여 제안하고자 한다.

2. 관련 연구

2.1 위탁에 대한 정의 및 관련 법률

2.1.1 개인정보 처리 업무 위탁

개인정보처리자는 정보주체로부터 동의나 법령근거 등을 통하여 수집한 개인정보를 수집 목적에 근거하여 처리하여야 한다. 하지만 비용절감, 업무효율화, 서비스 개선 등 다양한 목적으로 민간기업은 물론 공공기관들 조차 각종 업무를 외부 기업이나 개인에게 위탁하는 사례가 증가하고 있다. 업무 위탁은 현대사회의 분업화에 따라 나타난 자연스런 경영방식의 하나이나 대부분 고객의 개인정보도

함께 이전하게 되어 개인정보가 유통되거나 남용될 위험이 크므로 이에 대한 대책이 필요하다. 업무위탁으로 인한 개인정보 침해유형은 크게 네가지로 구분할 수 있다. 이들 침해유형으로는 다른 회사의 상품·서비스를 동시 취급하면서 개인정보를 공유, 고객 개인정보를 이용하여 부가서비스 등 다른 서비스에 무단가입, 서비스가입신청서 등 개인정보의 분실·유출, 고객 DB를 빼내어 판매, 정보시스템 안전조치 미비로 인한 개인정보 유출 등이다.

업무위탁의 유형은 표 1과 같이 개인정보의 수집·관리 업무 그 자체를 위탁하는 개인정보처리업무 위탁과 개인정보의 이용·제공이 수반되는 일반업무를 위탁하는 개인정보취급업무 위탁으로 구분될 수 있다. 또한 개인정보취급업무 위탁은 다시 홍보·판매권유 등 마케팅업무의 위탁과 상품배달·애프터서비스 등 계약이행업무의 위탁으로 구분할 수 있다.

(표 1) 업무위탁과 제3자 제공의 비교
(Table 1) Business Consignment compared with Third Parties

구분	업무위탁	제3자 제공
관련조항	개인정보보호법 제26조	법 제17조
예시	배송업무, TM위탁등	사업제휴 등
이전목적	위탁자의 이익	제3자의 이익
예측가능성	정보주체 사전예측 가능	정보주체 사전예측 곤란
이전방법	원칙 : 위탁사실 공개 예외 : 위탁사실 고지	원칙 : 제공목적등 고지후 정보주체의 동의 획득
관리감독책임	위탁자 책임	제공받는자 책임
손해배상책임	위탁자 부담	제공받는자 부담

개인정보를 다른 사람에게 이전하거나 다른 사람과 공동으로 이용하게 된다는 측면에서 업무위탁은 개인정보의 제3자 제공과 동일하다. 하지만, 개인정보 이전 목적이 전혀 다르고 이전된 개인정보에 대한 관리/감독 등 법률적 관계도 전혀 다르다. 업무 위탁의 경우에는 개인정보처리자의 업무처리 범위 내에서 개인정보 처리가 행해지고 위탁자인 개인정보처리자의 관리/감독을 받지만, 제3자 제공은 제3자의 이익을 위해서 개인정보 처리가 행해지고 제3자의 책임하에 개인정보를 처리하게 된다. 즉, 업무위탁은 개인정보처리자(위탁자)의 사업목적 달성을 위하여 수탁자에게 개인정보를 제공하는 것을 의미하며, 개인정보의 수집・관리, 이용・제공, 가공, 복구 등이 수반되는 업무를 위탁하는 경우를 말한다. 홈페이지・시스템・CCTV 운영 및 유지보수, 각종 시설물 회원관리, 기관 홍보물·소식지 배송 등을 위탁하는 경우가 이에 해당한다. 단순한 시스템 유지보수 등 직접적으로 개인정보를 처리하지 않더라도 수탁자가 관리자 권한 등을 통해 개인정보에 접근할 수 있는 업무도 개인정보 위탁업무로 보고 있다[9].

제3자 제공은 정보주체나 개인정보처리자가 아닌 제3자의 사업목적 달성을 위해 제3자에게 개인정보를 제공하는 것을 의미하며, 정보주체에게 제3자 제공에 대하여 고지 및 동의를 받아야 하고, 개인정보의 제3자 제공에 따른 관리/감독의 책임은 '제공받는 자'에게 있으며, 개인정보의 누출·유출등의 사고 시 손해배상 책임 또한 '제공받는 자'가 부담하여야 한다. 따라서 업무위탁의 경우에는 수탁자에게 개인정보가 이전되더라도 개인정보에 대한 개인정보처리자의 관리/감독권이 미치지만, 제3자 제공의 경우에는 일단 개인정보가 제3자에게 제공되고 나면 개인정보처리자의 관리·감독권이 미치지 못한다.

2.1.2 개인정보 처리 업무 위·수탁 관련 법령 및 지침

개인정보처리자가 정보주체로부터 받은 정보들은 개인정보 라이프싸이클(수집, 저장, 이용 및 제공, 파기)에 의하여 처리하여야 한다. 개인정보처리자가 직접 처리하기 힘든 경우 위탁을 주게 되며, 이 경우 위탁자는 표 2와 같은 개인정보보호법 제26조와 시행령 제28조를 준수하여 처리하여야 한다.

위탁 계약에 따라 개인정보를 처리하는 경우, 아래와 같이 법 의무사항을 문서화하여야 한다.

① 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
② 개인정보의 기술적・관리적 보호조치에 관한 사항
③ 위탁업무의 목적 및 범위
④ 재위탁 제한에 관한 사항
⑤ 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
⑥ 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
⑦ 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등에 관한 사항

문서화 방법은 위·수탁 계약서, 협약서, 특약서 등 위・수탁자의 인감・서명날인 등이 포함된 자료만 인정되며 보안각서나 서약서 등은 인정되지 않으므로 유의하여야 한다.

개인정보 처리 업무를 위탁 시 개인정보처리자는 운영하는 홈페이지에 위탁업무 내용과 수탁자를 지속적으로 게재하여야 하며, 홈페이지에 게재할 수 없는 경우에는 위탁자의 사업장등 보기 쉬운 장소에 게시하거나 관보, 신문, 소식지등에 지속적으로 공개하여야 한다. 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 '서면등의 방법'으로 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다.

(표 2) 개인정보 처리 위탁관련 법령(개인정보보호법)
(Table 2) Privacy Laws Related Business Consignment

구분	법조항	내용
법률	제26조	①업무위탁 시 문서화 ②업무위탁 사실 공개 ③홍보업무등 위탁시 정보주체에 고지 ④위탁자의 수탁자 교육 및 감독 ⑤위탁범위 초과 이용 또는 제공 금지 ⑥손해배상발생시 수탁자는 위탁자 소속직원 처리 ⑦수탁자 관련 법규정 준용사항
시행령	제28조	①법제26조제1항제3호에서 "대통령령으로정한사항" ②법제26조제2항에서 "대통령령으로정하는방법" ③홈페이지 게재 불가시 공개방법 ④법제26조제3항 전단에서 "대통령령으로정하는방법" ⑤위탁사실 게시방법 ⑥위탁자의 수탁자 감독

위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 정기적으로 수탁자를 교육하고, 수탁자의 개인정보 처리현황 및 실태, 목적외 이용·제공 여부, 재위탁 여부, 안전성 확보조치 여부 등을 정기적으로 관리·감독하여야 한다.

개인정보 처리 업무위탁 시 수탁자가 준수하여야 되는 사항들에 대해 개인정보보호법에서는 아래 표 3과 같이 규정하고 있다. 수탁자가 직접 개인정보를 수집/이용하는 경우에는 위탁자와 똑같은 수준의 법령 준수를 요구하고 있으며, 더욱이 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법' 혹은 '망법'이라 한다)에서는 개인정보 취급 위탁에 관하여 정보주체의 동의를 얻도록 하고 있으나, 개인정보보호법은 마케팅 등 업무 위탁이 아닌 일반적인 위탁의 경우 위탁사실을 공개하도록 하고 있다. 따라서 정보통신 서비스 제공자가 정보통신서비스 이용자의 개인정보 관련 사무를 위탁할 때에는 정보통신망법에 따른 동의를 얻어야 한다. 정보통신서비스 이용자 이외의 개인정보 처리 위탁에 관하여는 개인정보보호법이 적용된다.

(표 3) 개인정보 처리 업무위탁 시 수탁자 준수 법조항
(Table 3) The Trustee Complies with Legal Provisions

구 분	조 항
개인정보보호법 제3장 개인정보의 처리	
제1절 개인정보의 수집, 이용, 제공 등	제15조 ~ 제22조
제2절 개인정보의 처리 제한	제23조, 제24조, 제24조의2, 제25조, 제27조, 제28조
제4장 개인정보의 안전한 관리	제29조 ~ 제31조, 제33조, 제34조, 제34조의2
제5장 정보주체의 권리 보장	제35조 ~ 제38조
부 칙	제59조(금지행위)
개인정보의 안전성확보조치 기준 (개정 2014.12.30)	제3조 ~ 제10조
표준 개인정보 보호지침	제18조 ~ 제21조

수탁자는 개인정보를 보호하기 위하여 '개인정보 안전성 확보조치 기준'에서 정하고 있는 기술적/물리적/관리적 조치를 하여야 한다. 특히, 고유식별번호와 비밀번호 등에 대하여는 반드시 암호화하여 보관해야 개인정보 누출·유출사고에 대비 할 수 있으며, 위·수탁 계약의 종료 등 개인정보 처리 업무위탁에 대한 목적달성이나 회원탈퇴 등의 경우에는 반드시 해당 개인정보를 복구할 수 없는 방법으로 파기하여야 하며, 해당 사실에 대하여 위탁자에게 알려야 한다.

2.2 문헌연구

이용진은「금융회사 개인신용정보 수탁사에 대한 관리감독 현황 및 개선방향에 관한 연구」에서 국내·외 정보보호 관리·감독 사례를 살펴보고, 금융회사의 업무 수탁자들에 대한 개인신용정보보호 현황 분석을 통해 문제점을 도출하였고, 개인신용정보 수탁자 점검을 30회 이상 수행한 보안전문가를 대상으로 설문을 실시하여 개선방

향을 도출·제시하였다. 특히, 금융기관의 업종을 고려한 수탁자 개인신용정보보호수준을 파악하기 위한 점검항목을 도출하여 정보보호 수준을 파악하였다[6].

강태훈은「개인정보보호 수탁사 관리체계 강화 방안 연구」에서 개인정보보호법과 정보통신망법을 적용받는 위탁자가 수탁자의 관리·감독을 위해 수탁자 보안수준을 점검하고 이를 보완하기 위하여 내부관리계획 수립, 수탁자의 주기적인 교육, 실태점검 프로세스 수립, 관리/감독 및 통제 기준 마련, 전담조직 구성 필요성에 대하여 제언하였고, 특히, 법의 실효성을 높이기 위하여 년 1회 이상 수탁사 관리체계 정기점검 의무화 추가에 대한 법률 개선 방안을 제시하였다. 즉, 위탁자가 수탁자에 대한 관리/감독 기능을 강화함으로써 수탁자의 보안수준을 강화할 수 있다고 하였다[7].

고영대는「개인정보보호 강화를 위한 위탁 업무 보안 관리 프레임웍 제안」에서 위탁자가 개인정보 처리 업무의 위탁 시 관리단계를 3단계(업체 선정 및 계약단계, 업무진행 및 이행단계, 계약해지 및 종료단계 등)로 나누고 각 단계별 고려사항 및 개인정보 보호 요건들에 대하여 제시하였다. 이는 기존의 연구들이 수탁자에 대한 관리·감독에 초점이 맞추어 진행된데 반해, 위탁업무 절차별 관리방법에 초점을 맞춰 연구하였다[8].

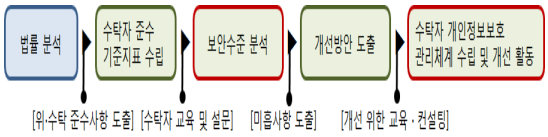
앞서 살펴본 연구들은 금융기관과 정보통신서비스제공자 등 위탁자에 대한 수탁자 관리/감독 방법에 대한 연구들이었다. 특히, 강태훈의 연구에서는 위탁자의 관리/감독 기능이 강화 될수록 수탁자의 보안수준이 높아진다고 하였다. 하지만, 이는 위탁자의 관리/감독 기준설정에 따라 수탁자의 보안수준에 대한 신뢰성이 낮을 수도 있다. 즉, 위탁업무 특성 대비 위탁자의 기준지표가 법령기준 혹은 수탁자가 수행 할 수 있는 능력보다 현저히 낮거나 높게 책정된다면, 원래의 수탁 업무를 제대로 수행하지 못하거나 형식적인 점검 행위로 이어져 오히려 법령기준에 못 미칠 수도 있다. 또한, 선행 연구들은 각각의 연구 대상 수탁자가 금융기관 및 온/오프라인 판매를 포함하는 일반기업에 해당하는 것으로써 각기 해당 특별법 하에서의 개인정보 처리 방안에 대해 연구하였다.

이에 본 논문에서는 공공기관의 대표적 개인정보 처리 위탁업무 중 IT유지보수, 고지서인쇄, 콜센터, 복지관등 30개 수탁자들에 대하여 보안수준을 살펴보고, 수탁자 입장에서의 개인정보 보호를 위한 관리체계 개발과 이를 통한 위탁자의 개인정보보호 관리수준을 제고하는 방향에 대하여 연구하고자 한다.

3. 수탁자 개인정보보호 관리수준 분석

3.1 프로세스 및 방법

개인정보 처리 업무를 위탁 받아 처리하고 있는 수탁자들의 개인정보보호 관리수준 개선을 위하여 (그림 1)의 흐름으로 분석 및 개선하였다.



(그림 1) 수탁자 개인정보보호 관리수준 분석 및 개선 프로세스
(Figure 1) Management-Level Analysis and Improvement Processes

우선, 개인정보보호법령과 지침 및 가이드라인등을 분석하여 수탁자가 준수하여야하는 모든 사항들에 대하여 분석하였다. 이를 토대로 수탁자의 보안수준을 분석할 수 있는 지표를 개발하였고, 이를 기초로한 설문항목을 만들었다. 설문에 앞서 관련 수탁자에게 해당 법령과 진단지표 및 개선 프로세스에 대하여 설명하고 점검이 목적이 아닌 수탁자 보안수준 제고를 위한 사항이라고 설명하고 진행하였다. 사전 설명 없이 진행할 경우 수탁자에 어떤 피해를 가 할 수 있다는 오해를 야기할 수 있어, 자기의 미흡한 점을 숨기기보다는 이번 기회에 개선하여 유출가능성을 최소화하자는 취지를 충분히 공감케 한 후 수행하였다. 이를 통해 수탁자 관리체계 개선의 필요성과 이해도를 높이고, 수탁자가 작성하는 설문지의 신뢰성을 높일 수 있었다. 이후, 설문결과에 대하여 분석 작업을 통해 해당 수탁자들의 준거성에 대하여 분석하고 문제점에 대하여 도출 및 개선방안을 연구하였다. 마지막으로 수탁자별 개선사항에 대하여 자료제공 및 관리방안에 대한 교육 및 컨설팅을 통하여 관리수준을 제고하도록 하는 순으로 진행하였다.

수탁자들의 관리실태 점검은 자기기입식 설문조사 방식을 채택하였고, 점검지표는 표 3의 개인정보보호 법령을 기준으로 법적 준거성 확보에 중점을 두어 구성하였으며, 표 4와 같이 4개 평가영역, 12개 점검지표, 30개 점검항목으로 구성하였다.

(표 4) 수탁자 개인정보보호 관리체계 점검내용
(Table 4) Depositary Privacy Management System Checks

평가영역	점검분야	법적근거
I.수탁자 개인정보보호 관리체계		
1.내부관리 체계수립	개인정보 처리 업무수탁의 문서화	(법)제26조 (영)제28조
	내부관리계획의 수립	(법)제29조 (안)제3조
	개인정보보호책임자의 지정	(법)제31조
	개인정보처리방침의수립및공개	(법)제30조
2.개인정보 취급자관리	개인정보취급자의 보안서약서작성	(표)제18조③
	개인정보취급자에 대한 교육실시	(법)제28조②
3.개인정보 유출통지 등 관리절차	개인정보 유출 등 사고 대응 절차서 수립	(법)제34조
4.정보주체의 권리 보장	개인정보의 열람/삭제등 요구대응절차수립	(법)제35조 ~제38조
II. 개인정보 처리 단계별 보호		
5.개인정보 수집	개인정보 수집/이용 동의	(법)제15조
	필요 최소한의 개인정보 수집	제16조
	민감정보및고유식별정보 처리제한 준수	제23, 24조
	주민번호 수집 시 법령 준수	제24조의2
	만 14세 미만 아동의 개인정보 수집	제22조⑤
6.개인정보 이용/제공	개인정보의 이용/제공 제한	제17, 18조
	개인정보의 재 위탁	제19조
	개인정보의 목적외이용 및 제3자제공	제19조
7.개인정보 파기	개인정보 처리목적 달성 시 파기	제21조
	파기 사실에 대한 위탁자 통보	제26조④
8.개인정보 저장 및 관리	비밀번호 작성규칙 수립	(안)제5조
	개인정보의 암호화	(법)제24조 ③ (안)제7조
	물리적 접근 방지	(안)제10조
III. 개인정보 안전성 확보 조치		
9.개인정보 처리시스템 관리	접근권한의 최소범위로 차등부여	(안)제4조①
	접근권한의 변경 또는 말소	(안)제4조②
	접근권한 이력의 기록 및 보관	(안)제4조③
	접속계정의 1인 1계정 발급	(안)제4조④
	접속기록의 보관 및 관리	(안)제8조
10.접근통제	접근통제시스템 설치 및 운영	(안)제6조① ②④
	비인가된 P2P, 공유설정에 대한 차단	(안)제6조③
11.보안 프로그램 운영	보안프로그램(백신등) 설치/운영	(안)제9조
IV. 특정 IT 기술 활용 시 개인정보보호		
12.CCTV 활용 시 의무사항 준수	CCTV 설치/운영 기준 준수	(법)제25조 (영)제22조 ~제26조

수탁자 관리실태 설문에 대한 보안수준 평가방법은 각 점검 항목에 대한 중요도를 표 5과 같이 법률에 명시되어 있으며 징역(5년이하) 혹은 벌금/과태료(5천만원이하)가 부과되는 항목은 H-High(5점), 법률에 명시되어 있으며 징역(3년이하) 혹은 벌금/과태료(3천만원이하)가 부과되는 항목은 H-Mid(4점), 법률에 명시되어 있으며 징역(2년이하) 혹은 벌금/과태료(1천만원이하)가 부과되는 항목은 H-Low(3점), 단순 법률 명시 항목은 M(2점), 법률에 명시되어 있지 않으며 벌금/과태료도 없는 항목은 L(1점)으로 구분하였다.

(표 5) 중요도 평가 기준 및 점수
(Table 5) Priority Evaluation Criteria And Scores

중요도	점수	중요도 기준		
		법률명시	징역	벌금/과태료
H-High	5	O	5년이하	5천만원이하
H-Mid	4	O	3년이하	3천만원이하
H-Low	3	O	2년이하	1천만원이하
M	2	O	-	-
L	1	기타 항목		

강태훈은 논문을 통해 정보통신망법과 개인정보보호법을 기준으로 위·수탁자가 준수해야 할 공통적 법조항을 비교하여 보여주고 있다. 이를 토대로 수탁자 보안수준 점검지표를 제작하였으며, 법률명시 여부에 따라 중요도를 3단계로 구분하여 보안수준 점수를 산정 하였다[7]. 본 연구에서는 좀 더 상세한 보안수준 점수를 측정해보고자 법률명시여부에 더하여 징역 혹은 벌금·과태료 부과 기준에 따라 5단계로 나누어 해당기관의 보안수준 점수를 산정하였다.

(표 6) 점검결과에 따른 기준점수
(Table 6) Basic Scores According To Inspection Results

구분	설명		점수(B)
인지여부 실시여부	매우 잘 지킨다	Y	1
	잘 지킨다		
	보통이다		
	잘 지키지 않는다	N	0
	전혀 지키지 않는다		
	해당없음	N/A	0
적용여부	예 | 그렇다		1
	기타(합당한이유등) | 부분완료		0.5
	아니오 | 그렇지않다 | 해당없음		0

점검결과에 따른 기준점수는 표 6과 같이 '인지여부' 혹은 '실시여부'에 따라서 '예'인 경우(매우잘지킨다, 잘지킨다, 보통이다)는 '1점'을, '아니오'인 경우(잘지키지않는다, 전혀지키지않는다) 또는 '해당없음'인 경우는 '0점'을 부과하여 평가하였으며, 각 점검항목별 평가결과, 도메인별 전체점수, 전체 보안수준으로 산출하였다. 보안수준 산출식은 표 7과 같으며 강태훈 논문과의 비교를 위해 동일한 산출식을 적용하였다.

(표 7) 보안수준 산출식
(Table 7) Security Level Equation

구 분	산출식
중요도	High-High=5점, High-Mid=4점, High-Low=3점, Middle=2점, Low=1점
점검결과에 따른 기준점수	예=1점, 아니오=해당없음=0점, 기타=0.5점
지표별 중요도 기준점수	기준답변수 = 30개(답변 기관의 수)
점검결과	지표별 선택개수 * 기준점수
각 지표별 평가결과	중요도 * 점검결과
도메인별 전체점수	항목별 만점
도메인별 평가점수	각 지표별 평가결과의 합
도메인별 보안수준(%)	도메인별평가점수/도메인별전체점수
총평가 점수	도메인별 평가점수의 합
총 보안수준	총평가점수/도메인별전체점수의 합

3.2 수탁자 개인정보보호 관리수준 조사

공공기관 개인정보 처리 위탁업무 중 특성에 따라 6개 그룹 30개 수탁자 (IT유지보수(10), 고지서인쇄(3), 콜센터(1), 단체보험(1), 아파트관리사무소(6), 복지관(9)) 개인정보보호 담당자를 대상으로 2014년 12월부터 2015년 3월까지 자가 설문응답 및 증빙자료 확인 형식으로 관리수준 점검을 실시하였다. 설문 및 점검 결과 도메인별 평균 보안수준은 표 8과 같으며, 연구대상 수탁자와 지표의 차이가 있지만 강태훈 논문의 연구결과(45.5%)와 같이 수탁자의 보안수준(45%)은 여전히 낮은 수준으로 조사되었다[7]. 이는 '2015년 개인정보보호 관리수준 진단' 항목 중 '위탁업무에 따른 개인정보보호 활동' 지표 점수(전체기관 평균 점수 86.75점)와 비교할 때 관리감독 활동은 잘 하고 있으나, 실질적인 수탁자 관리감독 방법이나 관리지표상에 문제가 있음을 알 수 있다[5].

(표 8) 수탁자 개인정보보호 관리수준 분석결과
(Table 8) Consignee Privacy Management Level Analysis

도 메 인	보안수준(%)
평 균	45.0
1. 내부관리체계 수립	55.5
2. 개인정보 취급자관리	53.3
3. 개인정보 유출 통지등 관리절차	20.0
4. 정보주체의 권리 보장	13.3
5. 개인정보 수집	61.0
6. 개인정보 이용 / 제공	18.9
7. 개인정보 파기	46.7
8. 개인정보 저장 및 관리	39.2
9. 개인정보처리시스템 관리	52.0
10. 접근통제	51.7
11. 보안프로그램 운영	86.7
12. CCTV 활용 시 의무사항 준수	41.7

각 도메인별로 살펴보면, 보안프로그램운영부분은 86.7%로 높은 보안수준을 나타냈지만, 개인정보 유출 통지등 관리절차, 개인정보의 이용 및 제공, 파기, 저장 및 관리 등 전반적으로 50%이하로 낮은 보안수준을 나타내고 있어 이에 대한 대책마련이 시급하다.

즉, 보안프로그램의 구입 후 운영이라는 가장 단순한 사항은 쉽게 지킬 수 있겠지만, 지침이나 절차 등 관리체계의 수립 및 시행에 대하여는 수탁자 입장에서는 시간과 비용, 인력 등을 투입하여야 하기 때문에 쉽지 않음을 알 수 있다.

따라서, 수탁자의 개인정보 처리를 위한 관리체계 수립 및 이행으로 개인정보의 보호와 관리가 시급히 필요하다.

3.3 수탁자 개인정보보호 관리수준 세부 분석 결과

3.3.1 수탁자 개인정보보호 관리체계

1) 내부관리체계 수립

수탁자의 내부관리체계 수립에 대한 보안수준(준수율)은 표 9와 같이 55.5%로 조사되었다. 개인정보 처리 업무 수탁의 문서화 여부는 76.7%(23건)로 높은 비율을 나타내고 있으나, 필수사항인 만큼 23.3%(7건)에 대한 즉시 개선이 필요하였다. 내부관리계획의 수립여부는 46.7%(14건)만이 준수하고 있었으며, 53.3%(16건)는 아직 계획 수립 없이 개인정보를 관리하고 있었다. 개인정보보호책임자

의 지정여부에서는 63.3%(19건)이 지정하고 있으나 36.7%(11건)는 개인정보보호책임자를 지정하지 않고 있었다. 개인정보처리방침의 수립 및 공개여부는 36.7%(11건)만이 수립 및 공개하고 있었고, 60%(18건)는 수립하지 않았거나 홈페이지가 없다는 이유로 게시하지 않고 있었다(홈페이지 외의 다른 방법으로 알려야 함). 그 이유 중 43.3%(13건)은 '의무사항인지 몰라서' 이었고, 16.7%(5건)은 '작성방법을 몰라서', 3.3%(1건)은 '번거로워서'라고 답했다.

(표 9) '내부관리체계 수립' 관련 보안수준
(Table 9) Security Level in Establishing an Internal Management System

점검 항목	중요도	Y (빈도율)	N (빈도율)	N/A (빈도율)	기타 (빈도율)
1-1	HL	23 (76.7%)	7 (23.3%)	0	0
1-2	HM	14 (46.7%)	16 (53.3%)	0	0
1-3	HL	19 (63.3%)	11 (36.7%)	0	0
1-4	HL	11 (36.7%)	18 (60.0%)	0	1 (3.3%)
전체점수		390			
평가점수		216.5			
보안수준		55.5%			

2) 개인정보 취급자 관리

표 10과 같이 개인정보취급자관리에 대한 보안수준(준수율)은 53.5%로 조사되었다. 개인정보취급자의 보안서약서 작성 여부는 53.3%(16건), 미작성은 46.7%(14건)으로 나타났다.

(표 10) '개인정보 취급자 관리' 관련 보안수준
(Table 10) Security Level in Personal Information Management Operator

점검항목	중요도	Y	N	N/A	기타
2-1	L	16 (53.3%)	14 (46.7%)	0	0
2-2	M	48 (53.3%)	42 (46.7%)	0	0
전체점수		210			
평가점수		112			
보안수준		53.3%			

개인정보취급자에 대한 교육여부에 대하여 53.3%(48건)가 준수하고 있으며, 세부 교육대상자로 보면 책임자 교육이 46.7%(14건), 취급자 교육이 66.7%(20건), 임직원 교육이 46.7%(14건)로 나타나 아직까지 수탁자의 책임자급 교육은 많이 부족한 것으로 나타났다. 교육방법에 대하여 조사한 결과 표 11과 같이 75%(18건)가 자체교육을 한 것으로 나타났으며, www.privacy.go.kr의 교육자료 수강 등 무료제공하는 교육자료를 활용하여 교육한 것으로 나타났다. 즉, 취급자들에 대한 교육은 실시하고 있으나 자체교육이나 온라인학습을 통하므로 취급 개인정보에 대한 유의사항등 취급업무에 맞는 내용의 구성은 확인 할 수 없어 교육수준은 아직 많이 부족했다

(표 11) 개인정보보호 관련 교육 방법 및 횟수 분석
(Table 11) Training Methods in Privacy Education

교육방법	횟수	비율
① 정부/지자체/공공기관 위탁	2	8.3%
② 민간컨설팅 회사 위탁	0	0.0%
③ 사업자단체(협회,협의회등) 위탁	1	4.2%
④ 개인정보보호 관련 민간단체 위탁	2	8.3%
⑤ 기타 기관 위탁	1	4.2%
⑥ 자체 교육	18	75%

3) 개인정보 유출 통지 등 관리절차

표 12와 같이 개인정보 유출 등 관리절차에 대하여 보안수준은 20%로 나타났다. 이 부분은 초창기 개인정보보호법 시행 부분에 있어 여러 기관과 업체에서 많은 고민을 필요로 했던 부분이었다. 역시나 수탁자들은 자체 대응절차서를 20% 정도만이 구비하고 있었으며, 나머지 80%는 위탁자의 대응절차를 따라가거나 상황 발생 시에 대응하겠다는 것이었다. 이에 표준 대응절차서 제공의 필요성 질문에 99%가 필요하다고 응답했다.

(표 12) '개인정보 유출통지등 관리절차 ' 관련 보안수준
(Table 12) Security Level in Leakage Notice Management Procedures

점검항목	중요도	Y	N	N/A	기타
3-1	HM	6 (20.0%)	24 (80.0%)	0	0
전체점수		120			
평가점수		24			
보안수준		20.0%			

4) 정보주체의 권리보장

표 13과 같이 정보주체의 권리보장에 대한 보안수준은 13.3%로 나타났으며, 개인정보의 열람/정정/삭제/정지 요구 시 대응절차서 수립에 대하여 76.7%(23건)는 인지하고

있었지만, 13.3%(4건)만이 대응절차서를 수립하고 있다고 응답했다. 그 중 위탁자가 직접 운영 중인 개인정보처리시스템의 유지보수 등을 수행하는 수탁자들은 위탁자의 대응절차를 따르는 것으로 나타났다.(26.7%) 표준 절차서에 대한 자료제공 요청은 93.3%(28건)이었다. 필요하다고 인식은 하고 있으나 절차서를 만드는 방법이나, 노하우등이 없으므로, 이에 필요한 표준절차서를 제공함이 필요하다.

(표 13) '정보주체의 권리보장' 관련 보안수준
(Table 13) Security level in Personal Rights Guaranteed

점검항목	중요도	인지여부		실시여부		
		Y	N	Y	N	N/A
4-1	HM	23	7	4 (13%)	18 (60%)	8 (26%)
전체점수	120					
평가점수	16					
보안수준	13.3%					

3.3.2 개인정보 처리 단계별 보호

1) 개인정보 수집 여부

수탁자가 개인정보를 수집하는 것은 내부직원 채용 시에 개인정보 수집과 위탁자에게 개인정보 수집 및 처리를 직접 위탁받는 경우로 나눌 수 있다. 수탁자가 내부 직원들의 개인정보를 수집하는 경우는 전체 수탁자에 속하며, 위탁받아 직접 수집하는 경우는 63%(19건)으로 위탁업무의 특성에 따라 다르게 나타났다.

수탁자의 개인정보 수집목적을 중복 선택으로 조사한 결과, 법적의무이행(40%), 고객관리 및 서비스제공(32%), 계약의 체결 및 이행(24%), 홍보 또는 마케팅 목적(4%) 등이 있다. 개인정보 수집 방법으로는 홈페이지 회원가입(5%), 민원/계약 등 각종 서식(70%), 이메일로 수집(5%), 경품/할인권 행사(2.5%), 제3자 제공(12.5%), 위탁(5%) 등이었다.

수탁자들이 보유하고 있는 개인정보의 규모는 1천명미만이 56.7%, 5천명미만은 33.3%, 1만명미만은 3.3%, 일백만명 미만은 3.3%, 일천만명 미만이 3.3%였다. 개인정보를 직접 수집하는 수탁자에서 대체로 많은 수의 개인정보를 보유하고 있었다.

개인정보 수집의 근거로는 정보주체의 동의(32.7%), 법령의 근거(36.7%), 계약의 체결 및 이행을 위해 필수적인 정보의 수집(30.6%)등 이었다. 동의를 받아 개인정보를 수집하는 경우 수집/이용 목적, 수집항목, 보유/이용 기간, 동의 거부권리 등 4가지 사항들을 정보주체에게 고지하여야 한다. 이에 대한 인지여부를 조사하였더니 86.6%(26건)가 인지하고 있다고 대답하였으나, 아직 13.4%(4건)정도는 인지하지 못하고 있다고 답하였다. 또한, 수집 동의를 받고 있는 경우는 15.8%(16.3건), 동의 받지 않는 경우는 15.8%(5건), 개인정보 수집과 관계없는 경우는 30%(9건)이었다. 예외적 경우를 제외하고 개인정보 수집 시 동의를 받지 않는 경우는 법령 위반사항이라 즉시 개선해야 할 사항이다.

개인정보의 필요 최소한의 수집과 관련하여는 다분히 주관적인 답변이겠지만 73.3%가 기관에서 필요로 하는 최소한의 수집을 하고 있다고 답하였다. 하지만, 설문기간 중 다시 한 번 확인한 결과 불필요한 항목이 발견된 기관은 3.3%였다.

민감정보와 고유식별번호 수집기관에 대하여는 수집근거에 대하여 조사결과 법령의근거 47.1%, 다른정보와 함께 일괄적으로 수집동의 5.9%, 다른 정보의 수집에 대한 동의와는 별도로 동의 받는 기관이 20.6%, 근거 없이 수집하는 기관은 11.8%등이었다.

고유식별번호 중 주민번호 수집기관은 54.8%가 법령의 근거에 의하여 수집하였고, 16.1%가 다른 정보와 함께 일괄 수집동의를 받고 있었으며, 다른 정보의 수집 동의와 별도로 동의를 받고 있는 기관은 6.5%, 근거없이 수집하고 있는 기관은 12.9%에 해당하였다. 개인정보 수집과 관련한 전체 보안수준을 정리한 결과 표 14와 같이 61%임을 알 수 있었다.

(표 14) '개인정보 수집' 관련 보안수준
(Table 14) Security Level in Personal Information Collection

점검항목	중요도	인지여부		실시여부		
		Y	N	Y	N	N/A
5-1	HM	26	4	16.3 (54.2%)	5 (15.8%)	9 (30%)
5-2	M	-	-	22 (73.3%)	1 (3.3%)	7 (23.3%)
5-3	HH	-	-	25 (73.5%)	4 (11.8%)	5 (14.7%)
5-4	HM	-	-	24 (77.4%)	4 (12.9%)	3 (9.7%)
5-5	HH	-	-	11 (36.7%)	1 (3.3%)	18 (60%)
전체점수	990					
평가점수	604					
보안수준	61.0%					

2) 개인정보 이용・제공

수탁자는 개인정보 처리 위탁업무 시 제공받거나 수집/이용을 허용받아 수집하는 경우에는 해당 목적범위 내에서 처리하여야 한다. 개인정보 제3자 제공과 관련하여 제3자 제공 시 고지 및 동의를 받아 처리하는 부분에 대하여 80%는 인지하고 있었으나 20%는 인지하지 못하고 있었다. 하지만, 고지 및 동의를 실시하고 있느냐는 부분에서는 대부분(93.3%)의 수탁자들이 해당없음을 표시하였고, 6.7%만이 고지 및 동의를 받고 있다고 하였다. 하지만, 제3자 제공사례가 있느냐에 대한 질문에서는 40.6%가 정보주체의 동의, 법률근거 또는 수집목적 범위 내에서 제공하고 있다고 하였고, 별도 근거 없이 제공한 사례는 없었으며, 59.4% 는 해당사항이 없다고 응답하였다.

개인정보를 수집 또는 제공받은 목적 외의 용도로 이용하는 경우 고지 및 동의를 받아야 된다. 이에 대하여 80%가 인지하고 있었으며, 20%는 인지하지 못하고 있었다. 또한 6.7%만이 정보주체에게 고지 및 동의를 받고 있었으며, 나머지 93.3%는 해당없음으로 답하였다. 법률 및 동의 등에 근거하여 개인정보를 목적외로 이용 또는 제공한 경우가 있느냐에 대한 질문에는 15.6%가 제공사례가 있었고, 위반한 사례는 없었으며, 84.4%는 해당사항이 없다고 답하였다. 수탁자는 위탁자와의 협의를 통해 재위탁 또는 직접 수집한 개인정보를 개인정보처리시스템을 통해 처리하고 이를 유지보수 위탁 할 경우 이를 공개하여야 한다. 이에 대하여 실시하고 있는 기관은 3.3%에 불과하였고, 16.7%는 공개하지 않는다고 하였다. 나머지80%는 해당없음으로 답하였다. 개인정보처리 위탁사실에 대한 문서화에 대하여는 위탁자와의 계약을 통하여 실시한 경험이 있어서인지 80%가 인지하고 있었으며, 20%는 아니라고 답하였다. 문서화 실시여부에 대하여는 36.7%가 실시하고 있다고 하였고, 16.7%는 실시하지 않았으며, 46.7%는 해당없음으로 답하였다. (처리 위탁에 대한 공개여부에 해당없음이 80%라는 것은 재 위탁을 하지 않는다는 표시이나, 문서화와 관련하여는 11%가 실시하고 있다고 하였다. 아직 위・수탁에 대한 이해가 확실히 되어 있지 않음을 보여주는 수치이다.)

따라서, 표 15와 같이 개인정보 이용 및 제공과 관련하여 600점 만점 중 106점으로 보안수준은 18.9%로 확인되어 심각한 상태임을 확인하였다.

(표 15) '개인정보 이용・제공' 관련 보안수준
(Table 15) Security Level in Using or Providing Personal Informations

점검항목	중요도	인지여부		실시여부		
		Y	N	Y	N	N/A
6-1	HL	24 (80%)	6 (20%)	2 (6.7%)	0	28 (93.3%)
6-2	HL	-	-	13 (40.6%)	0	19 (59.4%)
6-3	HH	24 (80%)	6 (20%)	2 (6.7%)	6 (20.0%)	22 (73.3%)
6-4	HL	-	-	5 (15.6%)	0 (0.0%)	27 (84.4%)
6-5	HL	-	-	1 (3.3%)	5 (16.7%)	24 (80%)
6-6	HL	24 (80%)	6 (20%)	11 (36.7%)	5 (16.7%)	14 (46.7%)
전체점수	600					
평가점수	106					
보안수준	18.9%					

3) 개인정보 파기

개인정보 파일은 처리 목적 달성 시 지체없이 파기하거나 분리보관하는 등 적법하게 처리하여야 한다. 표 16과 같이 파기와 관련하여 53.3%가 적법하게 처리하고 있었고, 46.7%는 아니라고 답하였다. 개인정보 파기 시 파기사실의 위탁자 통보에 대하여 76.7%가 인지하고 있었으며, 23.3%는 인지하지 못하고 있었다. 또한 40%는 위탁자에게 해당 사실을 통보하고 있었고, 30%는 통지하지 않고 있었으며, 30%는 해당사실이 없다고 답하였다. 따라서 개인정보 파기에 대하여 180점 만점 중 92점으로 보안수준은 46.7%로 확인되었다.

(표 16) '개인정보 파기' 관련 보안수준
(Table 16) Security Level in Destroying Personal Information

점검항목	중요도	인지여부		실시여부		
		Y	N	Y	N	N/A
7-1	HM	-	-	16 (53.3%)	14 (46.7%)	0
7-2	L	23 (76.7%)	7 (23.3%)	12 (40.0%)	9 (30.0%)	9 (30%)
전체점수	180					
평가점수	92					
보안수준	46.7%					

4) 개인정보 저장 및 관리

수탁자가 개인정보를 저장 및 관리하는 방법에 대하여 조사한 결과 업무용PC에서 엑셀이나 한글등 응용프로그램을 이용하여 관리하고 있는 경우는 41.5%였고, 고객관리프로그램이나 개인정보처리시스템을 이용하여 관리하는 경우는 46.3%였고, 종이문서등으로 보관하는 경우는 7.3%이고, 저장 및 관리를 하지 않는 경우는 4.9%였다.

(표 17) 개인정보 암호화 현황
(Table 17) Personal Information Encryption Status

암호화 대상 정보	보유여부		암호화 현황		
	Y	N	전부	일부	미실시
주민등록번호	23(77%)	7(23%)	3(13%)	9(39%)	11(47%)
비밀번호	10(33%)	20(67%)	6(20%)	1(10%)	3(30%)
바이오정보	1(3%)	29(97%)	1(100%)	-	-
여권번호	0	30(100%)	0(100%)		
운전면허번호	6(20%)	24(80%)	1(16%)	1(16%)	4(68%)
외국인등록번호	2(6%)	28(93%)	0	1(50%)	1(50%)

고유식별번호 보관 시 암호화 여부와 관련한 조사 결과는 표 17과 같다. 주민등록번호는 76.7%가 보유하고 있으며, 이중 13%는 전부 암호화하여 보관하고 있다고 하였고, 39.1%는 일부 암호화를, 나머지 47.8%는 암호화를 하지 않는다고 답하였다.

비밀번호는 33.3%가 보유하고 있다하였고, 이중 20%는 전부암호화를, 10%는 일부암호화를 30%는 암호화를 미실시하고 있다고 답하였다. 바이오정보는 3.3%만이 보유하고 있다고 답하였고, 전부 암호화하여 보관하고 있다고 답하였다. 여권번호는 수탁자 모두가 보유 또는 이용하지 않고 있다고 답하였다. 운전면허번호는 20%가 보유하고 있다고 답하였고, 그 중 16.7%는 전부암호화를, 16.7%는 일부암호화를, 66.7%는 암호화를 미실시하고 있다고 답하였다. 외국인등록번호의 경우 6.7%가 보유하고 있다하였고, 그 중 일부암호화 또는 암호화를 미실시하는 곳이 각각 50%를 차지하였다.

수탁자는 비밀번호 작성 규칙을 수립하여 운영하여야 한다. 조사결과 46.7%가 이를 실시하고 있었고, 46.7%는 실시하지 않고 있었다. 개인정보가 포함된 서류의 경우 잠금장치가 있는 보관함을 이용하여야 한다. 70%는 잘 이행하고 있다고 답하였고, 23.3%는 이행하지 않는다고 답하였다. 전산실 등 출입통제가 이루어지는 곳은 출입통제 절차를 수립/운영하여야 한다. 40%는 이행하고 있었고, 36.7%는 이행하고 있지 않았다. 시스템 유지보수 업체의 경우 위탁자 건물 내에 상주토록 하는 경우가 많다. 이때 개인정보가 포함된 파일이나 대장등을 관리하는 경우가 있다. 이때는 위탁자가 제공하는 문서함에 보관하게 되며, 문서함은 잠금장치가 있어야 되고, 사용하지 않을 경우 꼭 해당 문서함에 보관하여야 한다. 이의 수행여부에 대하여 8개 업체가 잘 수행한다고 답하였다.

따라서, 표 18과 같이 개인정보의 저장 및 관리와 관련하여 1,200점 만점 중 312점으로 보안수준은 39.2%로 확인 되었다.

(표 18) '개인정보 저장 및 관리' 관련 보안수준
(Table 18) Security Level in Personal Information Storage and Management

점검항목	중요도	보유여부		실시여부		
		Y	N	Y	N	N/A
8-2	HM	42 (23%)	138 (77%)	23 (12.8%)	19 (10.6%)	138 (76.7%)
8-3	HM	-	-	14 (46.7%)	14 (46.7%)	2 (6.7%)
8-4	HM	-	-	21 (70.0%)	7 (23.3%)	2 (6.7%)
8-5	HM	-	-	12 (40.0%)	11 (36.7%)	7 (23.3%)
8-6	HM	-	-	8 (26.7%)	0 (0%)	22 (73.3%)
전체점수	1,200					
평가점수	312					
보안수준	39.2%					

5) 개인정보처리시스템 관리

개인정보처리시스템에 대한 접근권한은 최소범위로 차등 부여하여야 한다. 이에 대하여 83.3%가 인지하고 있었으며, 73.3%는 차등부여하고 있다고 답하였고, 10%는 실시하지 않고 있다고 답하였다. 수탁자는 퇴직 등 인사이동에 의하여 부득이 개인정보취급자(시스템 유지관리자, 업무취급 담당자등)가 변경되었을 경우 지체 없이 개인정보처리시스템(또는 업무용PC)의 접근(사용)권한을 변경 또는 말소하여야 한다. 이에 대하여 86.7%가 인식하고 있었으며, 66.7%는 실시하고 있다고 답하였고, 6.7%는 실시하지 않고 있다고 답하였다. 위·수탁자는 개인정보처리시스템 접근권한 이력을 기록 및 최소 3년 이상 보관하여야 한다. 이에 대하여 73.3%가 인지하고 있었으며, 26.7%는 인지하지 못하고 있었다. 또한 36.7%는 이를 시행하고 있었으며, 40%는 시행하지 않고 있다고 답하였다. 위·수

탁자는 개인정보처리시스템에 접속 할 수 있는 사용자 계정을 발급하는 경우, 개인정보취급자 별로 한 개의 사용자 계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다. 이에 대하여 83.3%가 인지하고 있었으며, 56.7%는 이를 시행하고 있다고 답하였고, 26.7%는 시행하고 있지 않다고 답하였다. 위·수탁자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 6개월 이상 위/변조 및 도난, 분실되지 않도록 안전하게 보관 및 관리하여야 한다(업무용 PC의 경우 해당없음). 이에 대하여 80%가 인지하고 있다고 답하였고, 26.7%는 시행하고 있고, 26.7%는 시행하고 있지 않다고 답하였다. 개인정보처리시스템 관리에 대하여 전체 600점 만점 중 312점의 평가점수를 받아 보안수준은 52%이었다. 표 19에 이들 결과를 정리하였다.

(표 19) '개인정보처리시스템 관리' 관련 보안수준
(Table 19) Security Level in System Management

점검항목	중요도	인지여부		실시여부		
		Y	N	Y	N	N/A
9-1	HM	25 (83%)	5 (17%)	22 (73.3%)	3 (10.0%)	5 (16.7%)
9-2	HM	26 (87%)	4 (13%)	20 (66.7%)	2 (6.7%)	8 (26.7%)
9-3	HM	22 (73%)	8 (27%)	11 (36.7%)	12 (40.0%)	7 (25.0%)
9-4	HM	25 (83%)	5 (17%)	17 (56.7%)	8 (26.7%)	5 (16.7%)
9-5.	HM	24 (80%)	6 (20%)	8 (26.7%)	8 (26.7%)	14 (46.7%)
전체점수	600					
평가점수	312					
보안수준	52%					

6) 접근통제

위·수탁자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위하여 접근제한시스템(침입 차단/탐지 시스템 등), 개인정보유출방지시스템, VPN, 전용선 등 안전한 접속수단 등을 이용하여야 한다. 또한, 위탁자에게 제공 받거나 직접 수집하는 개인정보의 처리를 위하여, 개인정보처리시스템 없이 업무용 PC에 개인정보를 저장 후 처리하고 있는 수탁자는 업무용 컴퓨터의 운영체제나 보안 프로그램 등에서 제공하는 접근통제 기능을 이용하여 접근 통제하여야 한다. 이에 대하여 83.3%는 인지하고 있었고, 16.7%는 인지하고 있지 않다고 답하였다. 또한, 46.7%는 그렇게 실시하고 있었고, 23.3%는 실시하지 않는다고 답하였다.

수탁자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 또는 업무용PC에 필요한 조치를 취하여야 된다. 이에 대하여 83.3%는 인지하고 있었고, 16.7%는 인지하지 못하고 있다고 답하였다. 또한, 56.7%는 이를 시행하고 있고, 16.7%는 시행하고 있지 않다고 답하였다. 접근통제에 대한 보안수준을 표 20에 정리하였다. 전체 240점 만점 중 124점의 평가점수를 받아 보안수준은 51.7% 이었다.

(표 20) '접근통제' 관련 보안수준
(Table 20) Security Level in Access Control

점검항목	중요도	인지여부		실시여부		
		Y	N	Y	N	N/A
10-1	HM	25 (83%)	5 (17%)	14 (46.7%)	7 (23.3%)	9 (30.0%)
10-2	HM	25 (83%)	5 (17%)	17 (56.7%)	5 (16.7%)	8 (26.7%)
전체점수	240					
평가점수	124					
보안수준	51.7%					

7) 보안프로그램 운영

수탁자는 업무용 PC에 대해 악성프로그램을 방지·치료 할 수 있는 백신 소프트웨어 등 보안 프로그램을 설치/운영하여야 하며, 자동 업데이트 기능사용 등 최신성을 유지하여야 한다. 이에 대하여 90%가 인지하고 있었으며, 86.7%는 이를 실시하고 있었고, 3.3%는 실시하지 않고 있다고 답하였다. 표 21과 같이 보안프로그램 운영에 대하여 전체 120점 만점 중 104점의 평가점수를 받아 보안수준은 86.7% 이었다.

(표 21) '보안프로그램 운영' 관련 보안수준
(Table 21) Security Level in Security programs

점검항목	중요도	인지여부		실시여부		
		Y	N	Y	N	N/A
11-1	HM	27 (90%)	3 (10%)	26 (86.7%)	1 (3.3%)	3 (10.0%)
전체점수	120					
평가점수	104					
보안수준	86.7%					

8) CCTV 활용 시 의무사항 준수

영상정보처리기기는 법령에서 구체적으로 허용하는 경우(법제25조1항) 등을 제외하고는 공개된 장소에 설치·운영하여서는 안된다. 위·수탁자는 CCTV 설치·운영 시 아래의 사항을 준수하여야 한다.

가. 사생활을 현저히 침해하는 장소에 설치 금지
나. 설치 전 이해관계자들의 의견 수렴(공공기관)
다. 안내판 설치
라. 영상정보처리기기의 임의조작 및 녹음기능 사용 금지
마. 법제29조에 따른 안전성 확보 조치 실시
바. 영상정보처리기기 운영/관리방침의 마련 및 공개등
사. 위·수탁 시 문서화하고, 취급자교육 및 관리/감독 실시

이에 대하여 90%가 인지하고 있다고 답하였고, 50%는 이에 따라 실시하고 있다고 하였으며, 6.7%만이 실시하지 않고 있다고 답하였다.

수탁자는 영상정보처리기기 운영·관리방침을 마련하여야 하고 이에 따라 관리하여야 한다. 이에 대하여 33.3%가 잘 이행하고 있다고 답하였고, 23.3%는 그렇지 않고 있다고 답하였다. 표 22와 같이 CCTV 활용 시 의무사항 준수에 대하여 전체 240점 만점 중 100점의 평가점수를 받아 보안수준은 41.7% 이었다.

(표 22) 'CCTV 활용 의무사항 준수' 관련 보안수준
(Table 22) Security Level in CCTV

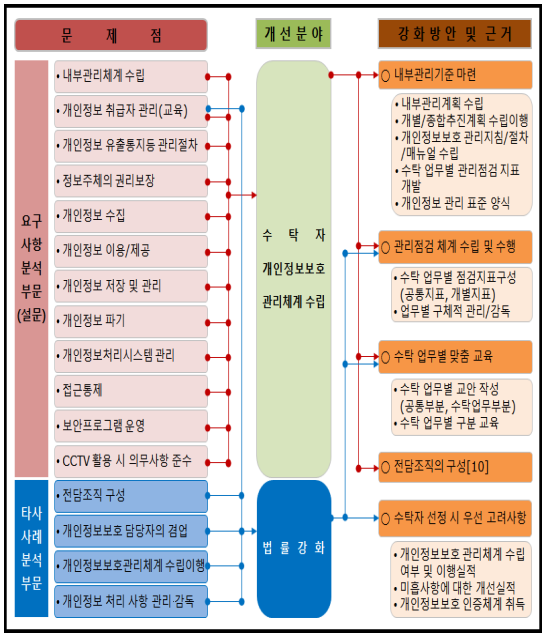
점검항목	중요도	인지여부		실시여부		
		Y	N	Y	N	N/A
12-1	HM	27 (90%)	3 (10%)	15 (50.0%)	2 (6.7%)	13 (43.3%)
12-4	HM	-	-	10 (33.3%)	7 (23.3%)	13 (43.3%)
전체점수	240					
평가점수	100					
보안수준	41.7%					

4. 수탁자 개인정보보호 관리체계 강화 방안

지금까지 개인정보 처리 위탁 시 수탁자가 지켜야 할 사항들에 대한 준수율(보안수준)에 대하여 확인 해 보았다. 이는 안전성 확보조치 차원의 관리감독 사항으로 개인정보 처리 위탁에 있어 업체 선정 시에 정보보안 수준을 측정하여 적정 수준에 미달인 업체와는 계약하지 않도록 하는 수탁자 보안수준 등급제에 대한 방안도 연구되고 있다. '정보보호관리체계 수준평가 방법론 및 등급기준 연구'에서는 정보보호 수준평가를 통해 수탁자에 대한 정보보호 등급을 적용하여 계약가능 수준인 업체와 미달인 업체를 구분토록 하는 방안을 제시하였고, 미국의 Shared-Assessment Program에서는 전문평가기관에 의한 정보보호 수준 평가인증을 통하여 적정 수준의 수탁자를 선택하는 방안을 제시하고 있다[10][11]. 본 연구에서는 이와 함께 개인정보보호 강화방안을 제시코자 한다.

4.1 강화 방안 도출

지금까지 분석한 자료를 토대로 개선분야와 강화방안을 도출하였다. 개선분야는 '수탁자 개인정보보호 관리체계 수립'부분과 '법률강화'부분으로 구분하였으며, 강화방안으로는 '내부관리기준 마련', '관리점검체계 수립 및 이행', '수탁 업무별 맞춤 교육', '전담조직의 구성', '수탁자 선정 시 우선 고려사항'등 5가지 항목으로 분석하였다. 수탁자 개인정보보호 개선 분야 및 강화방안은 그림 2와 같다.



(그림 2) 수탁자 개인정보보호 강화 방안 도출
(Figure 2)The Enhancement Way of Consignee's PIMS

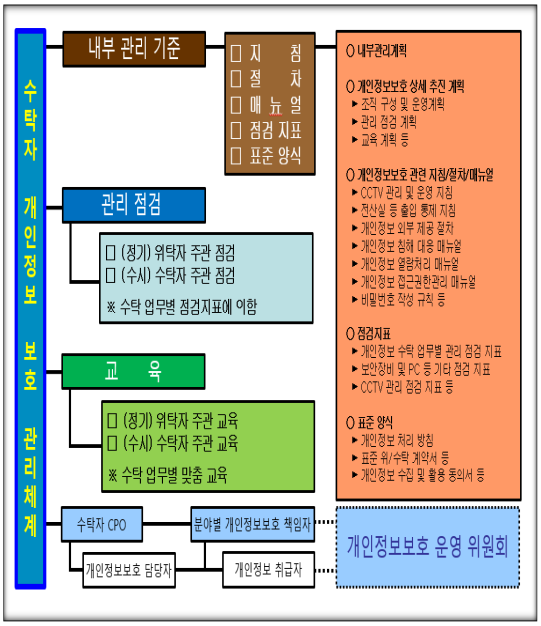
4.2 개선분야 및 방안

4.2.1 수탁자 개인정보보호 관리체계 수립

개인정보 처리 업무 위탁에 대한 수탁자의 개인정보보호 보안수준은 45%로 매우 낮은 수준임이 파악되었다. 보안수준을 향상하기 위한 방안으로 수탁자 개인정보보호 관리체계 수립을 통한 체계적인 관리방안을 제시하고자 한다.

개인정보 처리 위 · 수탁자를 불문하고, 내부 관리기준에 의하여 모든 관리체계가 이루어 져야한다. 이를 통한 기준이 정립된 다음 세부적인 관리가 진행되어야 할 것이다.

위탁자나 수탁자 모두 관리체계 수립의 기준은 개인정보보호법령 상 동일하게 적용된다. 하지만 위탁자에 비하여 수탁자의 모든 상황이 열악할 수 있기에 해당 수탁업무 처리를 위하여 모든 관리체계를 수립하고 수행하기엔 역부족일 수 있다. 예를들어 내부관리기준은 종이문서로서만 존재하고, 관리점검과 교육, 조직체계 등도 위탁자의 관리/감독을 대비하여 형식적으로만 존재할 수 있기 때문이다. 따라서, 개인정보 처리 위 · 수탁 업무를 위해 그림 3과 같은 최소한의 관리체계를 수립하여 이행하도록 할 필요가 있다.



(그림 3) 수탁 업무에 대한 수탁자 개인정보보호 관리 체계도
(Figure 3) Consignee Privacy Management System Diagram

1) 내부관리기준 마련

내부관리기준은 지침, 절차, 매뉴얼, 점검지표, 표준양식등으로 세분화 할 수 있다.

○ 내부관리계획 수립

내부관리계획(혹은 내부관리지침)은 행정자치부에서 예시한 표준양식을 해당 수탁자에 맞게 수정하여 수립하면 된다. 이는 위 · 수탁자 모두의 개인정보 보호를 위한 기준이 되는 매우 중요한 근거가 되며, 조직의 구성 및 역할, 관리감독, 교육, 침해대응방안 등으로 구성된다. 하지만, 조사결과 수탁자의 46.7%(16개)만이 내부관리계획을 수립하고 있어 이에 대한 보완이 필요하다.

○ 개별 혹은 종합 추진계획 수립 및 시행

내부관리계획을 근거로한 종합적인 추진계획을 수립하여 시행하여야 한다. 여기에는 CPO 지정을 포함한 세부적인 조직구성 및 운영계획, 관리점검계획, 교육계획 등의 내용 및 상세일정을 포함한다.

○ 개인정보보호 관련 지침/절차/매뉴얼 수립

개인정보 보호의 세부 운영을 위한 관련 지침/절차/매뉴얼을 수립하여 취급자에게 인지시켜야 한다. 여기에는 CCTV 관리 및 운영지침, 전산실등 출입통제지침, 개인정보의 외부제공절차, 개인정보 침해 대응 매뉴얼, 비밀번호 작성 규칙 등이 있으며, 수탁업무 특성을 고려하여 선택적으로 작성하여 수립하면 되며, 수탁자 개인정보 취급자에게 교육하여 숙지토록 하여야 한다.

○ 개인정보 처리 수탁 업무별 관리점검 지표 개발

개인정보 처리 수탁 업무별 관리점검 지표를 개발하여야 한다. 수탁 업무별 관리점검 지표에는, 개인정보의 수집/ 이용/ 제공/ 저장/ 파기 등에 따른 점검지표, 보안장비 및 PC 유지관리 점검지표, CCTV 점검지표, 개인정보 종이문서 관리 점검지표 등 수탁업무 특성에 맞게 개발하여야 한다. 이는 위탁자가 개발하여 제공 할 수도 있고, 수탁자 스스로 준비 할 수도 있다.

○ 개인정보 관리 표준 양식

개인정보처리방침과 표준 위·수탁 계약서, 개인정보 수집 및 활용 동의서 등 제공된 표준양식들을 토대로 수탁자 현황을 감안하여 알맞게 수정하여 활용하여야 한다. 수탁자 보안수준 제고를 위하여 수탁업무 수행을 위해 꼭 필

요한 기준들과 표준 양식들을 제공하고 교육함으로써 수탁자 스스로 효율적으로 관리할 수 있도록 하여야 한다.

2) 관리점검 체계 수립 및 시행

개인정보 처리 위·수탁 업무에 대하여 업무별 관리점검 지표를 개발하여 이를 시행하여야 한다. 개인정보의 처리 업무별로 법령준수를 위한 다양한 점검항목이 존재한다. 따라서, 이러한 업무의 성격을 반영한 수탁업무별 점검지표를 개발하여 수시 혹은 정기적으로 점검하여야 한다. 일반적으로 위탁자는 내부관리계획에 의하여 정기적으로 위탁업무에 대하여 점검하게 되고, 이에 수탁자는 점검에 응하게 된다. 이때, 위탁자는 위탁업무에 맞는 점검지표(공통지표+개별지표)를 개발하여 수탁자를 점검하면 더욱 효과적인 점검이 될 것이다. 또한, 수탁자 스스로 해당 수탁 업무들에 대하여 표 23과 같은 개별 점검지표를 개발하여 수시로 점검을 실시하여야 한다. 이를 통한 보완활동과 개선보고를 통하여 위탁자의 개인정보를 계약완료 시까지 안전하게 관리할 수 있다.

(표 23) 개인정보 공통 · 개별 점검지표의 예시
(Table 23) Example of Common or Partial Check List

구분	점검 지표 및 내용
공통 지표	개인정보보호 법령 준수 부분 - 법령 항목 별 관리 사항 점검 등
	개인정보의 기술적, 관리적 안전조치 점검 부분 - 개인정보 기술적 관리조치 사항 점검 - 개인정보 관리적 관리조치 사항 점검 등
	개인정보보호 내부관리지침 준수 부분 - CPO 지정 및 역할 수행 사항 - 취급자 관리감독 및 교육 사항 - 개인정보 침해사고 대응 사항 등
개별 지표	개인정보의 처리 단계별 준수사항 이행 부분 - 개인정보 수집/이용 기준 준수 사항 - 개인정보의 보관 기준 준수 사항 - 개인정보의 파기 기준 준수 사항 - 개인정보의 제3자 제공 기준 준수 사항 등
	CCTV 관리 이행사항 점검 부분 - 개인영상정보 파일 관리 준수 사항 - 개인영상정보 제3자 제공방법 준수 사항 등
	IT 유지 관리 부분 - 보안장비, PC, 서버 등 관리 준수 사항 - 접근권한 및 이력관리 등 관리 준수 사항 등
	출입통제 부분 - 관리지역 출입통제 사항 등

3) 수탁 업무별 맞춤 교육

수탁자의 개인정보보호에 대한 교육은 '위탁자 주관 교육'과 '수탁자 주관 교육'이 있다. 법령에서는 개인정보 취급자에 대하여 정기적으로 필요한 교육을 실시토록 하고 있어 위탁자는 수탁자에 대하여 내부관리계획에 의해 정기적으로 교육을 실시하고 있다.

하지만, 교육 내용에 대하여 구체적으로 제시하지 않아 수탁자에 대하여는 법령소개 및 위반사례등 간단한 내용으로 구성하거나, 온라인 무료교육(www.privacy.go.kr) 수강을 인정하고 있어, 위탁 업무별 차별화된 내용으로 구성되어 있지는 않아 전문성이 떨어진다.

이는 교육해야 할 분야가 다양하고, 내용의 깊이 또한 다양하기 때문에 개별 위 · 수탁 업무에 대하여 상세히 알 수 없는 개인정보보호 강사의 강의 범위를 초과할 수 있고 교육이 진행되더라도 짧게 진행 되는 것이 대부분일 것이기 때문이다. 따라서 위탁 업무에 따른 개별 및 전문화 교육이 필요하다.

수탁자 주관 교육도 마찬가지로 해당 업무 수행에 있어 꼭 필요한 부분을 개별점검 지표를 참고하여 교육함이 필요할 것이다. 위탁 업무를 가장 잘 이해하고, 적절하게 취급할 수 있어야 하는 수탁자 취급자들에 대하여는 수탁업무의 수행 시 법령 사항과 취급 유의사항, 사고발생에 따른 대처방법, 위탁자 업무 협조 및 당부사항 등 상세한 내용으로 구성되어야 할 것이다. 아래 표 24와 같이 공통사항과 개별사항으로 구분하여 취급자별로 교육 및 교육확인 하여야 할 것이다.

(표 24) 개인정보 보호 관련 수탁자 교육 예시
(Table 24) Example of Trustee Education

구분	교육내용
공통	개인정보 위·수탁 시 법령 등 준수사항 및 사례 (업무적용 및 위반사례 포함)
	위탁자의 개인정보보호 지침 및 관리체계 등
	개인정보 위·수탁 시 관리 절차(계약,교육,감독)등
수탁 업무별	개인정보 위·수탁 업무의 성격, 정의, 개념 등
	개인정보 취급자(책임자, 담당자 포함) 준수사항등
	IT 관리 위·수탁 시 준수사항 및 사례
	개인정보처리시스템 유지보수 및 개발 시 절차와 유의사항
	CCTV 관리 위·수탁 시 준수사항 및 사례
	개인정보의 처리 시 준수사항 및 사례
	개인정보 유출 및 침해사고 시 대응절차 소개
	개인정보 수탁 업무별 점검지표 소개 등

4) 전담 조직의 구성

위 세 가지 사항들을 수행할 수 있는 조직의 구성이 필요하다. 위탁자의 입장에서는 많은 수탁자를 관리하기 위한 체계적인 조직 구성원이 필요할 것이고, 수탁자의 경우도 수탁업무의 수에 따라 조직의 구성 규모가 달라 질 것이다. 하지만, 위·수탁자 모두 업무처리를 위한 조직 구성은 필요하며, 이에 대한 담당자 지정과 역할 구분도 필요하다. 따라서, 개인정보보호 책임자, 업무 분야별 개인정보보호책임자와 취급자, 개인정보보호 담당자를 지정하고 관리체계에 의하여 각자 해당 역할을 충실히 수행할 수 있도록 하여야 할 것이다.

최동근의 연구논문에서 알 수 있듯이 정보보안부서 내 정보보안 업무 전담자의 역량은 조직의 정보보안 수준을 일반부서 내 업무 담당자와 비교하여 2배 이상 높일 수 있다고 하였다. 따라서, 정보보호 전담 조직의 구성을 통해 기업의 개인정보보호 수준을 높여야 한다는 것이다[12].

4.2.2 수탁자 개인정보보호 관리체계 수립을 위한 법률 강화

앞서 2.1.2 절에서 언급하였듯이, 개인정보보호법 제26조에는 개인정보처리자가 해당 개인정보의 처리를 제3자에게 위탁할 경우 처리제한 사항에 대하여 정의하고 있고, 시행령 제28조에는 개인정보의 처리 업무 위탁 시 조치사항에 대하여 정의하고 있다. 수탁자의 행위에 대하여는 법 제26조 7항에 위탁자와 같은 법규정 사항을 준용토록하고 있다. 하지만, 3.2절에서 살펴보았듯이 수탁자의 개인정보보호 보안수준은 매우 낮은 수준이었다. 따라서, 위탁자는 수탁자에게 개인정보 처리를 위탁하기에 앞서 수탁자의 관리수준 정도를 파악하여 일정수준 이상이 되지 않으면 위탁하지 않아야 한다. 즉, 표준 개인정보보호지침 제19조(수탁자의 선정 시 고려사항)에 인력과 물적시설, 재정부담능력, 기술 보유의 정도, 책임능력등을 종합고려하여 선정토록 하고 있고, 고영대는 수탁자 선정단계에서 외형적 규모-인력, 물적 시설, 재정 부담능력, 기술보유정도, 책임 능력-와 개인정보보호 요소-사고여부, 전담인력/조직, 대외 인증현황-등을 고려하도록 제안하고 있다[8].

여기에 더하여 '개인정보보호 관리체계의 수립여부 및 이행 실적'을 고려하여 선정하여야 할 것이다. 이 검증단계를 통해 개인정보 관리체계가 수립·이행되고 있는 수탁자에 한하여 업무처리를 위탁하고, 안정적으로 관리되고 처리되도록 관리·감독하여야 할 것이다.

또한, 개인정보보호법 제26조, 시행령 제28조(개인정보의 처리 업무 위탁 시 조치)에 기술적/관리적 보호조치, 안전성 확보조치, 관리현황점검 등 감독에 관한 사항을 규정하고 있다. 이는 수탁자에 대한 위탁자의 관리/감독의 기준을 제시한 것이나 구체적이지 않아 자의적 해석에 따른 형식적인 관리/ 감독으로 끝나는 경우가 있을 수 있어 위탁한 개인정보의 유출에 대한 위협은 높다고 할 수 있다. 이는 3장의 보안수준 점검결과에서도 확인 할 수 있다. 강태훈은 정보통신망법과 개인정보보호법내에서 수탁자 관리 점검사항에 대하여는 명시하고 있으나 기술적/관리적 보호조치에 국한되고, 개인정보 라이프싸이클 전반에 대한 수탁자 점검항목과 년 1회 이상의 정기점검 의무화를 추가시킬 필요성에 대하여 언급하고 있다[7].

따라서, 법의 실효성을 높이고 수탁자의 개인정보보호 관리체계를 강화하기 위하여 아래와 같이 보다 명확한 제시가 필요하다.

- ○ 위탁 업무 특성에 맞는 점검지표 구성
  및 이에 따른 구체적인 관리 감독 실시
- ○ 점검 횟수는 업무특성에 맞게 시행토록 내부관리계획에 구체적으로 추가 시행
- ○ 수탁자 개인정보보호 교육의 차별화 실시
  → 위탁 업무별, 취급자별 맞춤형 교육 실시
  (위탁업무에 맞는 구체적이고, 사례 중심적 교육내용 개발 및 교육 실시)

4.3 강화방안에 대한 검증

본 논문에서 제시한 수탁자 개인정보보호 관리체계 수립 및 법령강화 방안에 대한 적합성 여부 및 실현가능성을 검증하고자, 위탁자로서 실제 1년 이상 업무를 담당하고 있는 개인정보보호 담당자 10명(이번 연구 참여자 3명 포함)과 이번 연구에 참여한 30개 수탁사의 개인정보보호 담당자(30명) 전원, 객관적이고 전문적인 검증을 위해 현재 개인정보보호 종합포털(www.privacy.go.kr)에 등록되고 공공기관 임직원 및 수탁자 대상 개인정보보호 강의 경험과 수탁자 관리·감독 관련하여 지식이 풍부한 행자부 개인정보보호 전문강사와 PIMS·PIPL 인증심사원자격을 소지하고 심사원으로 활동 중인 전문가(20명)들에게 Focus Group Interview를 실시하였다. 인터뷰 그룹은 연구 참여 수탁자(30개)를 기준으로 중복 위탁 가능한 지역 공공기관 위탁자(7개)를 포함하여 10개의 위탁자로 구성하였고 연구대상 위·수탁자의 절반수준인 20명의 전문가를 추가하여 강화방안에 대한 현실적이고 객관적인 결론을 얻고자 하였다.

강화방안에 대한 검증결과는 표 25와 같이 도출되었다. 검증은 해당 내용에 대하여 설명하고 그에 대한 필요성과 실현가능성에 대하여 FGI 방식으로 진행하였다. 표 25와 같이 수탁자 내부관리기준 마련의 필요성(100%) 및 실현가능성(100%), 관리점검체계의 수립 및 강화의 필요성(95%) 및 실현가능성(88.3%), 수탁 업무별 맞춤 교육의 필요성(96.7%) 및 실현가능성(81.7%), 전담조직의 구성의 필요성(100%) 및 실현가능성(73.3%), 수탁자 선정 시 고려사항의 필요성(91.7%) 및 실현가능성(81.7%)로 도출되었다.

(표 25) 강화방안 검증 결과
(Table 25) The result of the Enhancement Way

검증항목	구분	위탁자 (10)	수탁자 (30)	전문가 (20)	소개
내부관리기준 마련	(실)	10	30	20	60(100%)
	(필)	10	30	20	60(100%)
관리점검체계 수립 및 강화	(실)	10	24	19	53(88.3%)
	(필)	10	27	20	57(95%)
수탁 업무별 맞춤 교육	**(실)**	**9**	**22**	**18**	**49(81.7%)**
	(필)	10	28	20	58(96.7%)
전담조직의 구성	**(실)**	**8**	**21**	**15**	**44(73.3%)**
	(필)	10	30	20	60(100%)
수탁자 선정 시 고려사항	**(실)**	**9**	**20**	**20**	**49(81.7%)**

※ (실) : 실현가능성, (필) : 필요성

전반적으로 위탁자는 5개 부분 모두에 대하여 긍정적인 응답인데 반하여, 수탁자는 전담조직의 구성에 대하여 필요성은 공감하나 실현가능성에 대하여는 현실적으로 어렵다는 응답이 많았다. 또한 수탁업무별 맞춤 교육에 대하여도 필요성은 인정하나 실현을 위해서는 시간과 금전적인 투자가 별도로 투자되어야하는 부담감이 많다고 응답하였다. 수탁자 선정 시 고려사항에 대하여도 실현을 위하여 비용이 투자되어야 되는 부분에 대하여 부담을 가진다고 응답하였다.

전문가들의 의견 또한 수탁업무별 맞춤교육 및 관리점검체계 수립에 대하여 필요성은 인정하지만, 경험상 교안구성과 개별점검지표수립에 많은 시간과 노력이 투자되어야 되는 어려움을 지적하였다. 전담조직의 구성부분에 대하여도 위/수탁자 모두 필요는 하나 현실적으로 전담자를 배치할 수 있는 여건에 애로가 많다는 의견이었다. 이는 위탁자 또한 같은 의견이었다.

5. 결 론

본 논문에서는 개인정보의 위·수탁 업무에 대한 법률적 검토와 수탁자들에 대한 개인정보보호 실태를 분석하고 문제점을 도출하였다. 또한 이러한 분석을 토대로 개인정보 처리 위탁자가 보다 효율적인 방법으로 수탁자를 선택하고, 수탁자에 대한 일관된 감사 형태의 관리/감독과 교육시행이 아닌 수탁자 스스로 수탁된 업무별 개인정보를 관리하고 교육 할 수 있는 방안으로 '수탁자 개인정보보호 관리체계' 수립 방안에 대하여 제시하였다.

이를 위해서 첫째, '수탁자 내부관리기준 수립'이 필요하다. 이를 위하여 수탁자에게 필요한 양식을 제공하고 컨설팅과 교육을 통하여 시행할 수 있도록 하였다. 둘째, '관리점검체계 수립과 시행' 부분에서는 수탁업무별 점검지표 개발 및 제공을 통하여 체계적인 점검을 권고하였다. 지금까지 위탁자 위주의 일관된 감사형태의 감독은 지양하고, 위탁자와 수탁자 상호 협력에 따른 체계적이면서 수탁업무 특성에 맞는 점검지표를 개발하여 정기 혹은 수시 관리감독이 필요한 점을 제시하였다.

셋째, '수탁업무별 맞춤교육' 부분에서는 위 관리점검 부분에서 언급하였듯이 수탁업무별 특성에 맞는 교육이 이루어져야됨을 제시하였다. 일관된 교육을 통하여 수탁자 스스로 해석하여 수행하는 것이 아닌 수탁업무별 특성을 잘 파악하여 업무처리 시 법적 유의사항이나 처리절차, 유출사고 대응방안 등 공통교육부분과 수탁업무 분야에 대해 구분 교육하여야 함을 제시하였다.

넷째, '전담조직의 구성'부분으로는 위탁자의 조직구성과 맞추어 수탁자 또한 취급자 위주의 구성보다는 이를 총괄하는 CPO와 담당자를 구성하여 체계적인 관리가 이루어 져야함을 제시하였다.

이러한 관리체계의 수립에 따른 수탁자의 보안수준은 최초 설문 및 점검 시 45%였던 것을 내부관리기준 제시, 관리점검과 교육방법 및 조직구성안 제시 등으로 모든 보안점검지표를 만족시킬 수 있을 것이다. 또한, 관리체계가 제대로 갖추어지지 않은 수탁자는 위탁자의 사업을 받아 처리할 수 없으므로, 관리체계 수립 및 시행을 통하여 계약 및 위탁자의 개인정보를 보다 안전하게 처리할 수 있음을 나타낸다. 따라서, 위·수탁자 모두 개인정보 보호 관리체계의 안정적이고 체계적인 운영을 통해 보안수준을 높이고 개인정보의 유출 가능성을 현저히 낮출 수 있다는 결과를 도출하였다.

본 논문에서 제안하는 '수탁자 개인정보보호 관리체계 수립 방안'은 개인정보보호 활동의 법적 준거성을 만족시

키고 있으나, 경영 현장에서 개인정보 처리 위탁 시 발생할 수 있는 유출사고 위험성을 최소화하여 고객의 소중한 개인정보를 잘 보호 할 수 있음을 실증적으로 증명하는 추가적인 연구를 추진할 계획이다.

참 고 문 헌 (Reference)

[1] Joint Interagency, Personal Information Protection Normalization measures, 2014, p.8. http://www.pmo.go.kr/pmo/news/news01.jsp?mode=view&article_no=49241

[2] Press Release by Ministry of Government Administration and Home Affairs, Privacy breaches greatly enhanced prevention activities, 2014. http://www.moi.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000008&nttId=44682

[3] Ministry of Future Creation and Science, KISA, 2013 Information Security Survey(Business Sector), 2013, p.137-139. http://isis.kisa.or.kr/board/?pageId=060200&bbsId=15&itemId=43&pageIndex=2

[4] Joint Interagency, Personal Information Protection Normalization measures, 2014, p.3. http://www.pmo.go.kr/pmo/news/news01.jsp?mode=view&article_no=49241

[5] Ministry of Government Administration and Home Affairs, 2015 Public Institution Personal Information Protection Management Level Diagnostic Result, 2015, pp.4. http://www.privacy.go.kr/nns/ntc/selectBoardArticle.do?nttId=5925&bbsId=BBSMSTR_000000000001

[6] Y. J. Lee, A Study on the Improvement and supervisory Status for Personal Fiduciary Services in Financial Institutions, Journal of Security Engineering, Vol.11, No.3, 2014, pp.233-250. http://dx.doi.org/10.14257/jse.2014.06.02

[7] T. H. Kang, Study on Measures to Strengthen Personal Information Protection Consignee Management System, Journal of the Korea Institute of Information Security and Cryptology, Vol.23, No.4, 2013, pp.781-797. http://dx.doi.org/10.13089/JKIISC.2013.23.4.781

[8] Y. D. Go, A Proposal of Enhanced Personal Information Security Management Framework of Consigning of Personal Information, Journal of the Korea Institute of Information Security and Cryptology, Vol.25, No.2, 2015, pp.383-393. http://dx.doi.org/10.13089/JKIISC.2015.25.2.383

[9] Ministry of Government Administration and Home Affairs, 2014 Public Institution Personal Information Protection Management Level Diagnostic Results, 2014, pp.2. http://www.privacy.go.kr/nns/ntc/selectBoardArticle.do?nttId=5925&bbsId=BBSMSTR_000000000001

[10] http://sharedassessments.org/about/,Jan(2012)

[11] KISA, A Reasearch on ISMS Maturity Level and Evaluation Methodology, Sep(2010), pp.18-26. http://www.kisa.or.kr/jsp/common/libraryDown.jsp?folder=017271

[12] D. K. Choi, Study the role of information security personnel have on an organization's information security level, Journal of the Korea Institute of Information Security and Cryptology, Vol.25, No.1, 2015, pp.197-209. http://dx.doi.org/10.13089/JKIISC.2015.25.1.197

[13] B. Y. Min, Study on Personal Information Management Plan for Consignment Work, A Master's Thesis ofr Graduate School of Information and Communication. Sungkyunkwan University 2014.

[14] D. K. Jeong, Comparative study of the privacy information protection policy(Privacy information basic laws and dedicated organization), Journal of the Korea Institute of Information Security and Cryptology, Vol.22, No.4, 2012, pp.923-939.

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

[16] ISO/IEC 27014, Information technology - Security techniques – Governance of information security.

[17] BS 10012:2009, Data protection – Specification for a personal information management system, BSI, 2009.

[18] JIS Q 15001:2006, Personal information protection management systems – Requirements. Japanese Standards Association Japan Institute for Promotion of Digital Economy and Community, 2006.

[19] ISO/IEC FDIS 27014, Information technology – Security techniques – Governance of information security.

[20] ISO/IEC 29100(2011), Information technology - Security techniques – Privacy framework.

[21] H. Y. Youm, The International Standard Necessary of PIMS, Review of the Korea Institute of Information Security and Cryptology, Vol.23, No.4, 2013, pp.66-72.

◐ 저 자 소 개 ◑

정 환 석 (Hwan-Suk Cheong)
1999년 경일대학교 컴퓨터공학과(공학사)
2014년 경북대학교 산업대학원 컴퓨터공학과(공학석사)
2014년 ~ 현재 전남대학교 일반대학원 정보보호협동과정(박사과정)
관심분야 : 개인정보보호, 정보보호, 정보보호인증
E-mail : xpertstone@hanmail.net

박 억 남 (Euk-Nam Park)
2008년 세종대학교 정보보호학과(공학사)
2011년 광운대학교 경영대학원 도시계획부동산학과(경영학석사)
2015년 전남대학교 일반대학원 정보보호협동과정 (박사수료)
관심분야 : 국제 정보보호 표준, 국제 개인정보보호 표준, 개인정보보호 법률
E-mail : mssinnovator@naver.com

이 상 준 (Sang-Joon Lee)
1991년 전남대학교 전산통계학과(이학사)
1993년 전남대학교 전산통계학과(이학석사)
1999년 전남대학교 전산통계학과(이학박사)
1995~2005 서남대학교 경영전산정보학과 조교수
2005~2007 신경대학교 인터넷정보통신학과 조교수
2007~현재 전남대학교 경영학과 교수
관심분야 : 경영정보시스템, 스마트컴퓨팅, 소프트웨어공학, 정보보호
E-mail : s-lee@chonnam.ac.kr