J. Korea Saf. Manag. Sci. Vol. 16 No. 3 September 2014
http://dx.doi.org/10.12812/ksms.2014.16.3.433

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)

개인정보 위탁업무 보안성 강화방안 연구

손 태 현* · 박 정 선*
*명지대학교 산업경영공학과

A Study on the Enforced Security of Personal Information Outsourcing

Son Tae Hyun* · Park Jung Sun*
*Dept. of Industrial and Management Engineering, MyongJi University

Abstract

Increasing the outsourcing of personal information treatment, the safe management and director for fiduciary is very important. In this paper, under the personal information protection management systems the current situation of fiduciary management and direction was reviewed and the certification system was analysed in terms of availability of the controled items. Under the basis of legal compliance at the time of the Privacy Act, the characteristics of outsourcing type was also analyzed and derived new controled items.
As a result of the proposed research, new controled items for fiduciary could be used as a standard for the managing Director.

keywords : Privacy, Personal Information Protection, Security, Outsourcing Service

1. 서 론

개인정보를 활용하는 사업과 서비스가 다양해지면서 개인정보 유출과 사생활 침해 사고가 사회적 이슈로 등장하고 있다. 위탁자는 수탁자에 대한 관리 감독의 책임과 의무를 갖고 있으나 적정 수준에 미치지 못하는 것이 현실이다. 이러한 문제가 발생하는 가장 중요한 이유는 개인정보의 위탁이 업무수행에 따른 비용-효과성에 치중하여 위탁업무 및 제공되는 정보의 중요성, 수탁사의 자체 정보보호 능력에 대한 평가 기준 등이 제대로 반영되지 못하기 때문이며 수탁자에 대한 관리 감독이 적정한 수준으로 관리되지 못하고 있는 것이다. 따라서 본 논문에서는 위탁사의 수탁사 정보보호 관리 감독 방안과 이에 따른 통제사항을 제시하여 새로운 개선 방향을 모색해 보고자 한다.

국내에서도 개인정보보호 관련 법률에 대한 준거성과 체계적인 관리 활동을 평가하는 개인정보보호 인증제도가 등장하고 있고 그 범위 내에서 위탁업무에 대한 수준평가가 제한적으로 이루어지지만 위탁사무 특성을 고려한 맞춤형 관리·감독 기준은 제시되고 있지 않은 상황이다[1].

본 논문에서는 위탁사무의 유형과 특성, 통제영역에 대한 관계성 등을 검토하여 개인정보의 위탁자와 수탁자간에 위험을 줄이기 위한 개인정보보호 관리체계의 통제를 도출하고자 한다.

제 2장에서는 업무 위탁 분야에서 개인정보보호 현황을 검토하고 법적 규제사항과 인증제도의 통제 사항을 살펴보고 선행 연구 결과를 조사하였다. 제3장에서는 개인정보 취탁업무의 유형과 필수 통제사항을 제시하고 개인정보 수탁사 관리감독 모형을 제안하였다.

† Corresponding Author : Tae-Hyun Son, Industrial and Management Engineering, MyongJi University, M · P : 010-8809-1352, E-mail: sontaehyun@yahoo.com
Received August 4, 2014; Revision Received August 22, 2014; Accepted September 26, 2014.

개인정보보호법을 토대로 개인정보 위탁 시 법적인 준수사항을 도출하고 이를 통제영역으로 구분하였다. 그리고, 국내 개인정보보호 인증 제도인 개인정보보호 관리체계(PIMS)와 개인정보 보호수준 인증(PIPL), 정보보호관리체계(ISMS)의 위탁 관련 통제를 분석하여 법적 준수사항과 대응시켰다. 마지막으로 개인정보 위탁의 실무적용이 가능한 통제 모형을 제시하고, 개인정보 위탁을 위한 관리체계 통제를 제안하였다.

2. 업무위탁 개인정보보호 현황

2.1 위탁 관련 법적 규제 사항

개인정보보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)에 따르면 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에 위탁하는 개인정보처리자를 “위탁자(consignor)”로, 개인정보 처리 업무를 위탁받아 처리하는 자를 “수탁자(fiduciary)”로 정의하고 있다[2][3].

<Table 1>은 개인정보보호법 제26조를 구성하고 있는 제1항부터 제7항까지의 내용을 위탁자와 수탁자가 준수해야 할 사항으로 구분하고 있다. 제26조 제1항에 따라 제3자에게 개인정보의 처리를 위탁하는 경우에 위탁 업무 수행 목적 외 개인정보의 처리 금지, 개인정보의 기술적·관리적 보호조치에 관한 사항, 개인정보의 안전한 관리를 위한 사항이 제시되고 있으며 세부 준수사항을 도출하여 추후 통제와 연계하기 위하여 “표준 개인정보보호 지침” 제2절(개인정보 처리의 위탁)의 내용을 준수사항(①,②,⑦)에 기술하였다. 나머지 준수사항은 개인정보보호법 및 시행령에서 규정한 내용을 서술한 것이다[2].

정보시스템 위수탁 환경의 개인정보 수탁자는 제26조 제7항(⑦)이 요구하는 개인정보의 기술적·관리적 보호조치에 해당하는 동법 제29조(안전조치의무)와 이를 구체적으로 명시한 “개인정보의 안전성 확보조치 기준 고시”에 따라 이행되어야 한다.

개인정보 위탁자는 제26조 제2항(③)에 따라 위탁하는 업무의 내용과 수탁자를 정보주체가 언제든지 쉽게 확인할 수 있도록 공개해야 하며, 제26조 제6항(⑥)에서는 수탁자가 법을 위반하여 발생한 손해배상책임에 대해 위탁자가 책임을 질 수 있도록 규정하고 있어서 제26조 제4항(⑤)에 따라서 개인정보를 위탁한 자는 이를 수탁한 자의 교육과 보호조치의 이행을 감독할 의무를 갖는다.

<Table 1> Consignor and consignee's legal compliance (Privacy Act)

구분	준수사항	법조항
위탁자	① 수탁자를 선정할 때에는 인력과 물적 시설, 재정 부담능력, 기술 보유의 정도, 책임능력 등을 종합적으로 고려하여야 한다.	제26조 제1항
	② 수탁자의 처리 업무의 지연, 처리 업무와 관련 없는 불필요한 개인정보의 요구, 처리기준의 불공정 등의 문제점을 종합적으로 검토하여 이를 방지하기 위한필요한 조치를 마련하여야 한다.	제26조 제1항
	③ 위탁하는 업무의 내용과 수탁자를 정보주체가 언제든지 쉽게 확인할 수 있는 방법(예: 인터넷 홈페이지)으로 공개하여야 한다.	제26조 제2항
	④ 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우, 위탁하는 업무의 내용이나 수탁자가 변경된 경우에 해당 업무의 내용과 수탁자를 정보주체에게 알려야 한다.	제26조 제3항
	⑤ 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 않도록 수탁자를 교육하고, 처리현황 점검 등으로 개인정보를 안전하게 처리하는지 감독하여야 한다.	제26조 제4항
	⑥ 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여발생한 손해배상 책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 본다.	제26조 제6항
수탁자	⑦ 위탁받은 개인정보를 보호하기 위하여 “개인정보의 안전성 확보조치 기준 고시”에 따른 관리적·기술적·물리적 조치를 한다.	제26조 제1항
	⑧ 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다.	제26조 제5항
	⑨ 수탁자에 관하여는 제15조부터 제25조까지(수집·제공·이용·파기 등), 제27조부터 제31조까지(이전제한, 안전조치 등), 제33조부터 제38조까지(영향평가, 유출통지, 권리보장 등) 및 제59조(금지행위)를 준용한다.	제26조 제7항

2.2 국내 인증제도의 위탁 관련 통제

국내에서는 기업의 개인정보보호 활동을 체계적이고 지속적으로 수행하기 위해 필요한 보호조치 체계를 구축하였는지 점검하고 인증을 부여하는 PIMS 제도가 2011년부터 시행 중이다. 다만, PIMS에서는 일반적인 조직 내부의 개인정보보호 관리 활동에 중점을 두고 있어서 수탁사의 개인정보보호 위험을 적절하게 다루지 못하고 있다[4].

최근에는 개인정보보호법에 따른 준거성과 개인정보보호체계(관리체계) 및 개인정보 보호대책을 소상공인, 중소기업, 대기업 및 공공기관을 대상으로 인증을 부여하는 개인정보보호 인증제(PIPL)가 등장하였다[5]. PIPL은 인증 대상에 따라 평가할 통제사항이 다르지만 위탁 관련 통제사항은 법적 준거성을 기반으로 하므로 모든 대상(소상공인, 중소기업, 대기업, 공공기관)이 반드시 준수해야 하는 요구사항에 해당한다.

PIPL은 개인정보보호법을 근거로 수립된 제도이므로 위탁 관련 통제항목이 모두 법 준수사항에 대응이 되지만, PIMS는 정보통신망법의 준수사항도 포함하고 있어서 개인정보보호법 준수사항과 대응이 되지 않는 부분도 존재한다.

3. 업무위탁의 개인정보보호 방안

3.1 위탁업무의 유형별 분류

본 논문에서는 전체적인 위탁업무의 유형을 분류하고, 위탁업무 유형별 특성을 정의하였다. 위탁업무를 수탁사가 접근할 수 있는 IT 자원유형 및 사용권한, 자원에 대한 온라인 또는 오프라인을 통한 접근경로에 따라 <Table 2>와 같이 분류하였다.

수탁사가 접근할 수 있는 위탁사의 접근 정보 자원 유형은 기업 내부의 중요 데이터에 대한 접근인지 정보 시스템에 대한 접근인지에 따른 구분이며, 용역 수행원별로 자원의 갱신 가능여부에 따라 권한을 분리하여 읽기/쓰기 권한을 차등 부여하였다. 또한, 접근 경로를 온라인 또는 오프라인으로 구분하였는데 이것은 각각 네트워크 보안 및 물리적 보안을 좀 더 고려해야하는 특성을 갖는다.

(1) (유형 1)운영 위탁

기업 내의 정보 자원을 전담 운영하는 외주용역 유형으로서 기업내의 모든 정보 시스템 및 내부 데이터에 온라인으로 접근할 수 있다. IT 외주용역 중 가장 높은 권한을 부여받는 유형으로서 모든 정보 자원에 읽기 및 쓰기 권한으로 접근하여 업무를 수행할 수 있다. 이 유형에서 수탁사의 수행인력은 내부직원과 동일한 권한으로 온라인을 통하여 자원에 접근하기 때문에 용역수행원은 네트워크 접근권한 통제를 내부직원과 같은 수준으로 적용하여야 한다.

(2) (유형 2)유지보수

위탁 기업의 정보 자원에 대한 유지 보수 업무를 수행하는 유형으로서 유지보수 업무수행을 위해서는 유형 1과 같이 모든 정보 자원에 대한 접근이 가능하고, 모든 업무를 수행할 수 있는 권한이 필요하다. 그러나 유지보수 업무의 경우, 수탁사 내부에서 업무를 수행하거나 요청에 의해 단기간 동안만 작업을 할 수 있기 때문에 높은 권한을 부여할 수 없다.

<Table 2> Characteristic Classification for Outsourcing Type

위탁 업무 유형		특성				
		접근 정보 자원		자원 사용 권한		접근 경로
유형 1	운영 위탁	내부 데이터	○	읽기	○	온라인
		정보 시스템	○	쓰기	○	
유형 2	유지보수 위탁	내부 데이터	○	읽기 (내부자 동행)	✖ (○)	온라인
		정보 시스템	○	쓰기 (내부자 동행)	✖ (○)	
유형 3	개발(SI) 용역	내부 데이터	○	읽기	○	온라인
		정보 시스템	○	쓰기	✖	
유형 4	데이터 처리 위탁	내부 데이터	○	읽기	○	온라인
		정보 시스템	✖	쓰기	✖	
유형 5	오프라인 지원	내부 데이터	○	읽기	○	오프라인
		정보 시스템	✖	쓰기	✖	

따라서 용역 수행원은 정보 자원 사용에 대한 모든 권한을 부여 받지는 못하고, 업무수행 시에는 위탁사의 내부직원과 동행함으로써 필요한 권한을 획득하게 한다. 유형 2는 다른 유형과 달리, 외주용역 수행원의 물리적 위치에 따라 상주 및 비상주 유형으로 세분화될 수 있지만, 모두 온라인으로 자원에 접근하고, 내부직원에 의해 읽기 및 쓰기 권한을 획득할 수 있다는 공통된 특성을 갖는다.

(3) (유형 3)개발(SI) 용역

기업의 정보 시스템을 구축하는 업무를 수행하는 위탁 유형으로서 현재 기업의 IT 환경에 적합한 시스템을 구축하기 위해서는 모든 정보 자원에 접근할 수 있어야 한다. 그러나 개발 용역 수행 중, 내부 데이터를 수정 또는 삭제하는 등의 오류를 범하는 것을 예방하기 위하여 쓰기 권한을 부여하지 않는다. 대신, 개발 용역 수행원은 모든 정보 시스템 및 내부 데이터에 접근하여 읽기 권한을 통해 원하는 정보를 획득할 수 있기 때문에 내부 데이터의 복사본을 이용하여 개발된 시스템의 검증을 수행할 수 있다.

(4) (유형 4)데이터 처리 위탁

기업의 내부 데이터를 활용하여 업무를 수행하는 위탁 유형으로서 헬프데스크 또는 대리점이 이 유형에 속한다. 유형 1, 2, 3과 달리 정보 시스템에 대한 접근은 불가능하고, 온라인 접속을 통해 내부 데이터에 접근할 수 있다. 내부 데이터의 수정 및 삭제를 방지하기 위하여 “읽기 권한”만 부여받게 된다. 개인정보의 노출을 최소화하기 위하여 업무에 반드시 필요한 정보가 아닌 개인정보는 마스킹을 처리하여 위험을 제거할 수 있다. 위탁사의 정보 자원접근에 대한 로그를 유지하고, 관리하는 데이터보안 용역업체 또한 이 유형에 속한다.

(5) (유형 5)오프라인 지원

유형 4와 같이 위탁사의 내부 데이터를 활용하여 업무를 수행하지만 오프라인으로만 접근 가능하다는 특성을 갖는다. 따라서 오프라인으로 출력된 산출물을 관리하는 용역업체가 이 유형에 해당되고, 출력된 내부 데이터에 대해 “읽기 권한”을 부여받아 면담 및 상담을 통해 컨설팅을 수행하는 회계 또는 보안컨설팅 등도 이 유형에 속할 수 있다. 출력된 데이터가 업무 목적을 벗어나서 이용되지 않도록 관리 되어야 하며 사용이 완료된 정보에 대한 파기 확인이 중요한 통제사항이다[6].

3.2 수탁사 관리감독을 위한 통제사항

수탁사에게 위임한 개인정보를 안전하게 보호하는지 관리·감독하고 통제하기 위한 보안 방안으로 관리적 보안, 기술적 보안, 운영보안으로 나누어 [Table 3]과 같이 제안한다.

[Table 3] Outsourcing Control & Management Model

통제영역	항목수	통제분야	통제사항	통제 내용
관리적 보안	5	계약서	계약조건	계약 필수이행 사항 및 책임 규정
			보안서약서	외주 인력에 대한 준수 의무사항 서약
		인적 보안	정보보호 교육	참여인력 대상 정보보호교육
			직무 감독	주요 직무자 R&R 정의 및 직무분리
			위탁 종료	계약 종료 및 퇴직자 권한 회수
기술적 보안	5	계정 관리	인증 및 식별	역할기반의 접근권한 부여 및 검토
		접근 통제	패스워드 통제	안전한 패스워드 관리 및 작성규칙
			네트워크 통제	네트워크 분리 운영 및 원격접속 통제
			모바일 통제	모바일 사용 제한 및 허용기준
			인터넷 통제	업무목적 외 인터넷 접속 제한 및 모니터링
운영 보안	5	매체 보안	저장매체 관리	중요정보의 저장 매체 폐기 방법
			휴대용 매체 관리	휴대용 기기 매체 반입 제한 및 승인절차
		유출 차단	악성코드 차단	악성코드 침입 차단 대책
			출력보안	출력물 내용 유출 및 노출 최소화 방안
		모니터링	로그관리	정보시스템의 사용 내역 기록 및 보존
3개 분야	15	7개 통제목적 15개 통제사항		

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)

3.2.1 관리적 보안

(1) 개인정보의 처리 업무를 위탁하는 위탁자가 수탁자를 선정할 때에는 인력과 물적 시설, 재정 부담능력, 기술 보유의 정도, 책임능력 등을 종합적으로 고려한다. 개인정보의 처리 업무를 위탁하는 경우 계약서 등의 형식으로 수탁자가 준수해야 할 사항을 규정한다. 이 문서에 포함할 내용을 다음과 같이 제시한다.

(가) 위탁업무의 목적 및 범위
(나) 재위탁 제한에 관한 사항
(다) 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
(라) 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항
(마) 개인정보의 기술적·관리적 보호조치에 관한 사항

(2) 수탁사를 포함한 외주 용역업체 직원에게 제3자에게 개인정보 자산에 대한 접근권한을 부여할 경우 다음의 개인정보취급에 대한 준수사항과 책임을 명시하고 서명을 받는다.

(가) 재직/퇴직/계약해지 시 개인정보 유출/발설 금지 등의 개인정보보호 책임
(나) 조직 내 개인정보보호 규정 준수 의무
(다) 개인정보보호 의무에 미준수로 인한 사건 사고 발생 시 손해배상 책임

(3) 수탁사의 개인정보취급자를 대상으로 정기적인 개인정보보호교육을 실시한다. 교육의 시기, 기간, 대상, 내용, 방법 등을 포함한 연간 개인정보보호 교육 계획을 수립・이행한다. 교육대상에는 수탁사의 정규직원, 임시직원, 계약직원 등 모든 인력을 포함하고 교육 대상에 따라 수행업무의 성격에 따라 교육내용을 차별화한다. 교육 내용에 포함 할 사항은 다음과 같이 제시한다.

(가) 개인정보보호 관련 법률, 규정 및 업무 절차
(나) 개인정보 침해(누출)사고 사례 및 대응방안
(다) 개인정보보호 규정 위반 시 상벌규정, 책임 등

또한, 교육의 대상, 내용, 기간 등에 따라 효과적으로 교육을 수행할 수 있는 방법으로 온라인교육, 집합교육, 전달 교육 등을 선택한다. 업무 활동 중에 개인정보보호 인식제고 위하여 개인정보보호의 날 지정, 포스터 또는 뉴스레터 등을 제작한다. 교육의 효과와 적정성을 평가하기 위하여 설문 또는 테스트 등을 실시하고 차기 교육의 개선을 위하여 활용한다.

(4) 조직 내 중요 정보자산(정보, 시스템 등)을 취급하는 수탁사의 주요 직무자는 최소화하되 필요한 경우 별도로 지정하고 주기적으로 직무현황을 관리한다. 주요 직무로 분류할 수 있는 업무를 다음과 같이 제시한다.

(가) 중요정보(개인정보, 인사정보, 영업비밀, 산업기밀, 재무정보 등) 취급
(나) 주요 정보시스템(서버, DB, 응용 프로그램 등) 운영 및 개발
(다) 정보보호시스템 운영
(라) 정보보호 관리업무 수행

수탁자에게 위임한 직무의 권한 오남용을 예방하기 위하여 정보보호 관련 주요 직무 분리 기준을 수립하고 직무별 역할과 책임을 명확히 한다. 이를 위하여 정보보호 관련 주요 직무 분리 기준을 수립하고 직무별 역할과 책임을 명확하게 기술한다. 직무분리의 기준을 다음과 같이 제시한다.

(가) 개발과 운영 직무 분리 (필수)
(나) 정보시스템(서버, DB, 네트워크 등)간 운영직무 분리
(다) 정보보호 관리와 정보시스템 운영직무 분리

조직 규모가 작거나 인적 자원 부족 등의 사유로 인해 불가피하게 직무 분리가 어려운 경우, 직무자간의 상호 검토, 상위관리자의 주기적인 직무수행 모니터링 및 변경 사항 검토/승인, 직무자의 책임추적성 확보 등의 보완통제를 마련한다.

(5) 위탁사와 수탁사 간의 직무변경 및 수탁사 내부의 직무 변경 혹은 퇴직 발생 시 정보자산 반납, 접근권한의 조정·회수 등을 절차에 따라 이행하고 결과를 확인한다.

3.2.2 기술적 보안

(1) 개인정보처리시스템에 대한 접근을 필요 최소한으로 제한하고 접근 통제의 범위, 인가절차 등을 수립한다. 접근통제의 영역은 네트워크장비, 서버, 응용프로그램, DB 등으로 구분하고 영역별 사용자 등록·삭제, 접근권한 등록·변경·삭제에 대하여 공식작인 절차를 수립한다. 수탁사의 직원에 대한 직무별 또는 역할별 정보시스템 접근권한을 정의하고 정보시스템에 대한 접근권한은 업무 수행에 필요한 최소한으로 할당하며, 업무 담당자 직무에 따라 차등 부여한다.

또한 수탁사의 이직율을 고려하여 계정 등록·삭제 및 접근권한 등록·변경·삭제 권한을 한 사람에게 집중되지 않도록 하고 불가피한 경우, 접근권한 활동의 적정성을 주기적으로 검토한다.

(2) 사용자 패스워드는 법적요구사항, 외부 위협요인 등을 고려하여 패스워드 복잡도 기준, 초기 패스워드 변경, 변경주기 등 사용자 패스워드 관리절차를 수립한다. 특히 관리자 패스워드는 별도 보호대책을 수립하여 관리한다. 안전한 패스워드 사용 및 작성규칙을 다음과 같이 제안한다.

(가) 사전공격(Dictionary attack)에 취약하지 않도록 문자(영문 대소문자), 숫자, 특수문자 등을 일정 자리수 이상으로 조합하도록 패스워드 작성규칙을 수립하고 주기적으로 변경
(나) 연속 숫자, 생일, 전화번호, 아이디 등 추측하기 쉬운 개인 신상정보를 활용한 취약 패스워드사용 제한
(다) 정보시스템 도입 시 초기/임시 패스워드 로그인 시 지체 없이 변경
(라) 패스워드 처리(입력, 변경) 시 마스킹 처리
(마) 패스워드 자동 저장 금지
(바) 개인정보취급자의 경우, 패스워드 작성 규칙에 대해 법적 요구사항 반영

(3) 네트워크에 대한 비인가 접근을 통제하기 위해 필요한 네트워크 접근통제리스트, 네트워크 식별자 등에 대한 관리절차를 수립하고 서비스, 사용자 그룹, 정보자산의 중요도에 따라 내·외부 네트워크를 분리한다. 내부 네트워크 IP 주소는 사설 IP로 할당하고 내부망에서의 주소 체계는 사설 IP주소 체계를 사용하고 내부 주소체계가 외부에 유출되지 않도록 보안을 유지한다. 특히 수탁사가 사용하는 네트워크 영역을 물리적 또는 논리적으로 분리하여 인가되지 않은 접근을 통제한다.

(4) 수탁사가 모바일기기를 업내·외부 네트워크에 연결하여 활용하는 경우 중요정보 유출 및 침해사고 예방을 위해 기기 인증 및 승인, 접근 범위, 기기 보안설정, 오남용 모니터링 등의 접근통제 대책을 수립한다. 모바일 기기를 사용하는 경우 허용기준을 마련하고 모바일 기기정보(MAC, 시리얼 번호, 사용자 등)을 목록화하여 관리한다. 만일 모바일기기를 통한 업무를 허용할 경우 범위를 명확히 하고 기기이용에 대한 승인절차를 거쳐야 하며 접속시 기기인증을 수행하는 방안을 아래와 같이 마련하고 이행한다.

(가) 네트워크 장비를 통한 인증
(나) 전용장비(NAC 등)을 통한 인증
(다) AP 인증

(5) 수탁사가 인사정보, 영업비밀, 산업기밀, 개인정보 등 중요정보를 대량으로 취급·운영하는 주요직무자인 경우 인터넷 접속 또는 서비스(P2P, 웹메일, 웹하드, 메신저 등)를 제한하고 인터넷 접속은 침입차단시스템을 통해 통제한다.

3.2.3 운영 보안

(1) 수탁사가 운영하는 정보시스템 폐기 또는 재사용 시 위탁사의 중요정보를 담고 있는 하드디스크, 스토리지, 테잎 등의 저장매체 폐기 및 재사용 절차를 수립하고 매체에 기록된 중요정보는 복구 불가능하도록 완전히 삭제한다. 사용연한 경과, 고장 등의 사유로 정보시스템을 폐기 또는 재사용(양도, 내부판매, 재활용 등)할 경우 저장매체 처리에 관한 절차를 준수하여 저장매체에 저장된 중요정보 유출을 방지한다. 폐기하는 저장매체는 물리적으로 폐기하거나 디가우징을 하고 재사용할 저장매체는 낮은 수준의 완전포맷을 수차례 반복하여 내부 데이터가 복원되지 않도록 관리한다.

(2) 조직의 중요정보 유출을 예방하기 위해 수탁사가 사용하는 외장하드, USB, CD 등 휴대용 저장매체 취급, 보관, 폐기, 재사용에 대한 제한을 강화한다. 또한 매체를 통한 악성코드 감염 방지 대책을 마련한다. 수탁사 직원이 업무용으로 개인 휴대용 저장매체를 사용하는 것은 원칙적으로 금지하여야 하며 업무 목적상 외장하드, USB 메모리, CD 등 휴대용 저장매체를 사용하여야 하는 경우 허가된 저장매체만 사용할 수 있도록 다음과 같은 절차를 제안한다.

(가) 휴대용 저장매체 사용범위 : 통제구역, 제한구역 등
(나) 휴대용 저장매체 사용허가 및 등록절차
(다) 휴대용 저장매체 반출, 반입 절차
(라) 휴대용 저장매체 폐기, 재사용에 대한 절차

주요 정보시스템이 위치한 통제구역(전산실 등), 조직 내 중요정보에 접근이 가능한 제한구역(운영실, 관제실 등)에서는 수탁사의 휴대용 저장매체 사용 및 반입을 엄격하게 제한한다. 불가피하게 사용할 경우 책임자의 허가절차를 거친 후 적법한 절차에 따른 사용여부 확인을 위하여 지속적인 점검을 수행한다.

(3) 바이러스, 웜, 트로이목마 등의 악성코드로부터 정보시스템을 보호하기 위하여 다음의 보호대책을 제안한다.

(가) 위탁사 직원 PC 사용지침 (불분명한 이메일 및 파일 열람 금지, 허가받지 않은 프로그램 다운로드 및 설치 금지 등)
(나) 위탁사 직원 PC 백신프로그램 설치 범위 및 절차

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)

(4). 위탁받은 개인정보를 출력할 경우 용도를 특정하고 용도에 따라 출력 항목을 최소화한다. 또한, 개인정보 출력방법(테이프, 디스크, 인쇄, 휴대용 저장매체 등)에 따라 출력 일시, 방법 등 필요한 사항의 기록·관리 등 보호대책을 수립한다. 개인정보를 인쇄하거나, 파일로 출력할 경우에는 어떤 업무용인지 용도를 정하여 업무상 용도에 따라 필요하지 않은 항목을 출력하지 않도록 제한한다. 출력, 복사물의 생성, 이용, 전달, 파기 과정까지의 책임관계를 명확히 하여 사후 문서 유출 발생 시 출처를 확인할 수 있도록 한다.

또한, 수탁사가 업무를 목적으로 개인정보 조회, 출력 등을 수행할 경우, 마스킹 기술 등을 통해 개인정보 표시를 제한하여야 한다. 개인정보의 조회, 출력 등의 업무를 수행하는 과정에서 개인정보를 마스킹하여 업무상 과도한 개인정보가 노출되지 않도록 표시를 제한하기 위하여 다음의 방법을 고려할 수 있다.

(가) 성명 중 이름의 첫 번째 글자 이상
(나) 생년월일
(다) 전화번호, 휴대폰 전화의 국번
(라) 주소의 읍.면.동
(마) 인터넷 주소 등

(5) 수탁사가 운영하는 정보시스템, 응용프로그램, 보안시스템, 네트워크 장비 등 기록해야 할 로그유형을 정의하여 일정기간 보존하고 주기적으로 검토한다. 서비스 및 업무 중요도를 고려하여 로그 기록 및 보존이 필요한 주요 정보시스템(서버, 응용프로그램, 정보보호시스템, 네트워크 장비, DB 등)을 지정하고 각 시스템 및 장비별로 기록하여야 할 로그유형 및 보존기간을 정한다. 특히 로그유형 및 보존기간(최소 6개월 이상 권고)은 법적요건을 고려하여 정한다. 로그기록은 스토리지 등 별도 저장장치를 사용하여 백업하고 로그기록에 대한 접근권한부여는 최소화하여 수탁사의 비인가자에 의한 로그기록 위변조 및 삭제 등이 발생하지 않도록 대책을 세운다.

3.3 개인정보보호 수탁사 관리감독 모형

본 논문에서 제안하는 수탁사 관리감독을 위한 통제방안에 대하여 ISMS의 정보보호 관련 사항과 PIMS의 개인정보보호 관련 사항들을 분석하여 수탁사의 관리감독에 적합한 “개인정보 수탁사 관리감독 제안 모델”을 도출하였다. 본 논문에서는 ISMS의 18개 통제분야 104개 통제항목과 PIMS의 22개 관리과정 118개 통제항목을 분석·검토하였다.

제안모델은 “관리적 보안”, “기술적 보안”, “운영보안” 등 3개 통제영역에 대하여 7개 통제 분야, 15개 통제사항 및 내용으로 구성되었다. ISMS 및 PIMS의 대상분야 중 통제분야나 통제사항이 없는 항목은 신설하거나 보강하였다. 3개 통제영역 중 “관리적 보안” 영역에 “계약서”분야를 신설하고 2개 통제사항을 신설하였다. “인적보안”, “매체보안”, “유출차단” 분야에 대하여는 통제사항의 내용을 수탁자의 업무 특성에 맞춰 보완하였다.

3.3.1 수탁사 유형별 통제항목 제안

개인정보를 취급하는 취급자의 시스템 접근권한이나 개인정보취급 사항들을 시스템에서 체계적으로 관리할 수 있는 방안을 모색하였다. 그 방법으로 외주용역의 유형을 운영용역, 유지보수 영역, SI용역, 데이터 처리 용역, 오프라인 지원 등 5가지로 구분하여 본 논문에서 제안 한 통제사항들과 상관관계를 검토하여 유형별 보호대책을 제시하였다.

(1) 운영 위탁 유형은 위탁사의 역할을 동일한 수준으로 대행하는 역할이므로 내부자와 동일하거나 그 이상의 보안 통제가 필요한 상황이며 모든 통제사항의 적용이 필요하며 관리·감독의 수준이 가장 높은 유형이다.

(2) 유지보수 위탁 유형은 유지보수 형태에 따라 모든 정보 자산에 대한 접근과 권한이 필요한 경우와 제한적인 범위 내에서 한정적인 자산과 자원에 대하여 업무를 수행하는 경우로 구분할 수 있다.

(3) 개발 용역 유형은 운영 위탁과 거의 같은 수준의 보호 대책의 적용이 필요하며, 다만 운영환경 및 내부 업무망과 분리된 독립된 개발망에서 개발 사업이 수행된다면 중요 자산에 대한 접속로그 및 모니터링 통제는 선택적으로 적용할 수 있다.

(4) 데이터 처리 위탁 유형은 기업내의 헬프데스크 운영이나 위탁사 데이터를 활용한 대리점 운영과 같은 업무를 대행하는 것으로 내부 데이터의 수정 및 삭제 권한은 제공되지 않으며 위탁사가 제공한 데이터를 활용하는 권한만을 이용하므로, 네트워크 및 인터넷 사용 제한 등은 업무 처리 유형에 따라 필요한 경우 허용할 수 있다. 외부 인터넷의 접속이 필요한 경우라도 주요 직무자의 인터넷 서비스(P2P, 메신저, 웹메일, 웹하드 등) 기능은 제한하여야 한다.

(5) 오프라인 지원 유형은 주로 출력된 산출물을 활용하여 진행되는 컨설팅, 회계감사와 같은 위탁 유형으로 데이터 처리위탁의 용역 특성과 같이 정보시스템에 접근하지 않고 정보 자산 접근 권한이 불필요한 경우이다. 대부분의 기술적 보안과 운영보안의 통제를 적용하지 않으나 출력물 유출을 차단하는 통제가 필요하며 USB, CD, 외장하드와 같은 저장 매체가 이용되는 경우 별도의 보호조치가 선택적으로 적용되어야 한다.

3.3.2 제안모형의 특징

(1) 위탁계약서의 필수 포함사항 및 책임에 관한 규정
위탁업무의 목적과 범위, 권리와 책임을 명확하게 규정하고 개인정보보호에 관한 위험이 제거될 수 있도록 조치내용이 포함되어 있다. 특히 대외보안이 필요한 경우 보안의 범위 및 책임을 명확히 하기 위해 사업수행계약서와 별도로 비밀유지계약서를 작성할 수도 있다.

(2) 위탁계약의 종료에 따른 확인사항
계약의 종료에 따른 위탁사가 제공한 데이터의 회수 및 파기, 계정 및 사용권한의 회수, 계약 기간 중 취득한 정보 유출 금지에 관한 서약서 작성, 수탁업무에 사용한 정보시스템 및 저장 매체의 점검 등 필요한 조치가 이행되었는지를 실물위주로, 현장 확인하도록 하였다.

(3) 보안 교육과 직무 관리 감독
주기적으로 수탁 업무 현장을 점검하고 체크리스트를 작성하도록 요구함으로써 수탁사의 보안의식과 법 준수 수준을 향상시키도록 하였다.

(4) 사용자 인증 및 식별에 대한 통제 강화
사용자에게 1계정을 부여하고 계정이 공유되거나 노출되지 않도록 비밀번호를 강화하고 접근권한은 업무에 필요한 최소한의 범위로 한정하고 권한을 부여한 내역과 변경 이력을 일정기간 보관하도록 하였다.

(5) 정보기반 시설 및 장비들에 대한 접근 통제활동
위탁사가 사용하는 네트워크와 외주인력이 사용하는 네트워크를 물리적, 논리적으로 분리하도록 하였다.

(6) 저장매체의 사용제한 및 폐기절차
외주인력이 사용하는 저장매체는 엄격히 사용을 제한하도록 하였다. 사용이 허용된 저장매체에 대하여도 저장된 자료를 검사하여 허용 범위를 준수하고 있는지 감사하도록 하였다.

(7) 악성코드 및 출력에 의한 유출 차단 대책
업무용 컴퓨터에 악성코드를 감사하고 제거하는 백신 소프트웨어가 설치되고 실시간으로 감사하고 있도록 하였다. 중요정보가 인쇄된 출력물이 불법적으로 반출하는 것을 방지하기 위한 보호대책을 제시하도록 하였다.

(8) 정보 취급현황 관리 및 로그관리
평상시 수탁업무 활동의 로그기록이나 개인정보 접근형태, 업무처리 건수 등의 취급 현황 등을 검토하여 개인정보 유출 가능성을 최소화하거나 예방가능성을 높이도록 하였다.

3.3.3 제안모형의 장단점

(1) 장점
- (가) 위탁 사업에 필요한 보안 통제 영역을 정의하여 위탁사 정보보호 관리체계를 수립하였다.
- (나) 위탁 업무의 유형에 따라 적합한 보안 통제 항목을 적용할 수 있다.
- (다) 위탁 업무 유형별로 세부 용역 사항에 맞춰 통제항목을 선택적으로 적용하도록 구분하였다.
- (라) 위탁계약의 사전 검토부터 사업 종료 시점까지 전 과정을 관리할 수 있는 핵심 통제항목을 도출하였다.
- (마) 위탁사업의 특성상 취약한 관리항목을 모두 통제항목에 포함하였다.

(2) 단점
- (가) 제안 모델의 위탁업무 유형이 업종이나 업무형태에 따라 세분화되어 있지 못하다.
- (나) 통제 사항의 점검을 위한 체크리스트 도출이 위탁자마다 상이 할 수 있다.
- (다) 통제사항별로 수탁사가 준수하여야 할 가이드라인 수립이 필요하다.

4. 결 론

위탁사업에서 개인정보보호를 위한 실질적인 방안과 대책을 도출하기 위하여 개인정보보호에 관련된 관리적, 기술적 총제사항과 관련 법률 규정, 개인정보 유출 사례 등을 분석·검토하였다. 또한 수탁 업무의 유형과 특성을 분석하고 유형별 특성과의 관계를 상호 비교하였다. 이를 통하여 수탁사가 사업의 유형에 따라 해결해야 할 보안 통제 영역을 이해하고 적용해야 할 통제사항을 선정할 수 있도록 하였다. 또한 위탁사업에서

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)

필수적으로 적용해야 할 통제영역과 통제사항을 도출하여 사업 단계에 맞춰 분류하고 세부 항목을 제안하였다.

따라서 위탁사는 정보보호 관리체계를 운영하고 있거나 개인정보보호 관리체계를 운영하고 있는 경우, 자사의 기준에 맞는 수탁사 관리 감독 기준을 제시하고 정기적인 이행실태를 확인 할 수 있도록 수탁사용 개인정보보호 프레임으로 활용할 수 있을 것이다.

제안모델은 고객의 개인정보가 위탁업무 처리과정에 의해 유출되거나 오용될 가능성을 사전에 차단하고 예방할 수 있는 등 효과적으로 대응 할 수 있는 방안을 제시하였다. 따라서 통제사항에 맞춰 필요한 점검 체크리스트를 작성하여 주기적인 관리·감독을 함으로서 실질적인 효과를 얻을 수 있을 것이다. 제안 모델은 위탁사업의 유형을 분류하여 유형별 통제사항을 제시한 첫 번째 시도라는 면에서 의의를 찾을 수 있을 것이다.

본 논문에서는 사업 유형에 따라 통제사항을 적용하는 과정에서 세부 내용에 따라 선택할 수 있는 여지를 남겨 두었다. 이것은 위탁사업의 업무 유형이 좀 더 분화하지 못하고 큰 분류로 구분되고 있음을 보여 주는 것이다. 따라서 향후 연구를 통하여 선택사항이 발생하지 않을 수 있는 수준으로 사업 유형의 분류가 세분화 할 필요가 있을 것이다. 또한 통제사항을 현장에 적용하기 위한 점검도구인 체크리스트를 표준화하는 연구가 추가적으로 필요하다고 본다.

5. References

[1] Dae-Ha Park(Aug. 2013.), “Trends of information security and privacy international standardization” Review of KIISC, 23(4), 47-52,

[2] NIA(Nov. 2012), “Comparison of Personal Information Protection Act (PIPA), its enforceme nt ordinance, regulations and guideline” NIA

[3] MOSPA(Nov. 2011), “Criteria and manual for assuring security of personal information”, MOSPA

[4] KISA(Dec. 2010), “Introduction to Personal Information Management System certification” KISA

[5] NIA(Oct. 2013), “Textbook for training PIPL auditors” MOSPA

[6] Tae-hun Kang, Jong-in Lim((2013) “A Study on Consigned Party Management System Enhancement for Personal Information Protection”, Journal of The Korea Institute of Information Security & Cryptology(JKIISC). Vol. 23, No. 4, 781-797

저 자 소 개

손 태 현

연세대학교 수학과에서 이학사, 서울대학교 대학원 계산통계학과에서 이학석사 취득. 현재 명지대학교 대학원 산업경영공학과 박사과정 중.
관심분야 : 개인정보보호, 산업정보보안, 위험관리, 위험평가

주소 : 경기도 용인시 처인구 명지로 116 명지대학교 산업경영공학과

박 정 선

서울대학교에서 학사, 한국과학기술원에서 석사학위를 취득하였고, 미국 텍사스주립대학교 경영학박사를 취득하였으며, 현재는 명지대학교 산업경영공학과 교수로 재직중이다. 연구분야는 BSC-IT, Green IT, 정보 보안 등

주소 : 경기도 용인시 처인구 남동 명지대학교 공학관 507호