「한국지방행정학보」 제4권 제1호(2007. 8): 127-146

공공기관의 개인정보관리에 관한 연구

- 개인정보보호를 위한 생애주기별 관리 실태를 중심으로-

A Study on Management of Private Information in Pubic Sector

- Focused on Management Status with Life Cycle for Privacy-

신 영 진 (행정자치부 전자정부본부 전문위원)

According to embodiment e-government, the citizen's needs for information have increased and spreaded to information sharing for public convenience. Especially, the government made various plans to improve efficiency and convenience of administrative system to support citizen's services as G4C system and public information sharing system, and so on. To increase amount of private information, it is need to construct safe management system. But the plan how we protect and manage private information in pubic agency is not enough, so we are urgent to make protection policy from outflow of information with online and offline.

Therefore, this study tried to suggest development plans as 'how public agencies do manage shared private information?'. The study compared management systems for private information among public agencies(central government, local government, public agency, educational agencies) with life cycle(collection, utilization, management, abolition). As the results, the study analyzed to support budget and manpower as well as to maintain legal system for privacy. And the study suggested safe management system with physical and technical methods. The study is need to raise recognition of their president and to improve education and management for private information in public sector. This study has means to construct rom now, how we do manage private information of public agencies is important issue to construct country based on citizen's relives.

키워드 : 공공기관, 개인정보보호, 정보관리, 실태분석

Key Words : public agency, privacy protection, information management, status analysis

I. 서 론

우리나라는 정보통신기술을 이용하여 행정기관의 사무를 전자화함으로써 행정기관 상호간 또는 국민에 대한 행정업무를 효율적으로 수행하고자 전자정부를 추진하고 있다(전자정부법 개정, 2006). 이러한 과정은 1960년대 처음 컴퓨터가 도입되면서, 1980년대 행정전산망 사업, 1990년대 행정정보화사업, 2000년대 전자정부 중점 11대 과제와 전자정부 31대 과제 등이 추진되면서 고도화된 행정정보화를 가져오게 되었다. 그러나 이러한 정보화환경의 구현은 정보의 대량성, 유동성 등으로 인해 노출되기 용이해졌으며, 특히 정부에서 보유하고 있는 개인정보에 대한 노출, 악용, 침해 등 개인정보를 둘러싼 문제제기가 증가되고 있다. 지난 2005년 G4C 민원발급 서비스의 위·변조 사건은 공공기관에서의 개인정보보호에 대한 대책의 필요성을 제기하였다(행정자치부, 2005). 또한 지난 이명박(대통령 후보)의 주민정보 유출사건을 비롯하여 앞으로 행정정보의 공동이용이 확산됨에 따라 발생할 문제에 적극적으로 대처하는 개인정보보호 정책이 필요하다.

우리나라는 '공공기관의 개인정보보호에 관한 법률(개인정보보호법)'을 살펴보면, 지난 행정전산화에 따라 1986년 '전산망 보급 확장 및 이용 촉진에 관한 법률'을 제정하였으며[1], 1994년 '공공기관의 개인정보보호에 관한 법률'을 제정하였다. 또한 1999년과 2007년에 거쳐 관련 법률이 개정되면서, 신기술의 도입 및 행정환경의 변화를 포함한 접근방안을 포괄하고 있다.[2] 또한 2000년부터 공공기관을 대상으로 개인정보관리에 관한 실태조사를 실시하였으며, 이를 통해 공공기관이 개인정보를 철저히 관리하도록 권고하고 있다. 또한 공공기관의 개인정보보호 담당자들을 대상으로 정기적인 교육을 실시하고 있으며, 방문교육 및 위탁교육 등 맞춤형 교육과정을 마련하고 있다. 이외에도 2005년부터 공공기관이 보유하고 있는 홈페이지에서의 개인정보 노출에 대한 모니터링을 실시하여 시정·조치하도록 하였으며, 홈페이지 상에서의 개인정보 노출을 방지하도록 하고 있다.

그러나 지금까지 공공기관의 개인정보보호를 위한 관리방안들은 수동적인 측면에서 논의되어 왔다. 더욱이 다른 업무와 겸직하고 있는 개인정보보호 담당자들에게 적극적인 대응과 업무의 집중적 관리를 의무화하기에는 현실적인 한계가 있다. 이에 대

---

1) 개인정보보호관련 조문(1994)으로는 제25조(누구든지 전산망에 의하여 처리, 보관, 전송되는 타인의 비밀을 침해하거나 누설하여서는 아니 된다)와 제6호 3항(다른 국가기관 등이 보유하고 있는 정보를 이용하는 국가기관 등은 정보의 누설방지 등을 위하여 노력하여야 한다)에 근거를 두었다.

2) '개인정보보호법'외에 행정목적별 개인정보보호에 관한 법률을 살펴보면, 정보·통신분야(정보통신부)에는 '정보통신망 이용 촉진 및 정보보호 등에 관한 법률', 금융·신용분야(재정경제부, 공정거래위원회)에는 '신용정보의 이용 및 보호에 관한 법률', 의료분야(보건복지부)에는 '보건의료기본법', '의료법' 등이 있다.

해 앞으로 미래사회의 변화에 대해 대응할 수 있는 적극적인 개인정보관리가 이루어질 수 있도록 실질적인 대책들이 마련되어야 한다. 이에 본 연구에서는 공공기관에서의 개인정보가 보다 효율적이고 예방적인 차원에서 관리되어지도록 방안을 제시해 보고자 한다. 이에 현재 추진되고 있는 관리실태를 비교하고, 그에 따라 공공기관의 특성을 파악하여 어떤 정책이 우선적으로 추진되어야 할지를 제시하는 데 본 연구의 의의가 있다.

II. 개인정보관리에 관한 논의

1. 개인정보의 개념

정보통신기술의 발달로 인하여 종이문서가 전자문서로 대체되면서, 개인정보에 대한 인식도 변화하고 있다.

<표 1> 공공기관의 개인정보유형

대분류	소분류	세부항목
인적정보	일반정보	이름, 주민번호, 운전면허, 주소, 전화번호, 성별
	가족정보	가족의 성명, 주민번호, 직업, 출생지 등
	의료정보	병력기록, 정신질환 및 신체장소 등
	신체정보	DNA 정보, 지문, 홍채 등
	부동산정보	주택, 토지, 자동차 소유현황
	동산정보	현금, 저축액, 주식, 채권 등 소유현황
경제정보	소득정보	봉급액, 이자소득, 사업소득 등
	신용정보	대출금, 신용카드사용액, 신용상태 등
	수익정보	보험가입 현황, 투자 또는 퇴직, 연금 등
사회정보	병역정보	군번, 계급, 근무부대 및 주특기 등
	법적정보	전과, 교통위반기록, 구속 납세 등
	고용정보	회사, 고용주, 직무평가, 훈련, 상벌기록 등
	교육 및 훈련정보	학력, 성적, 출석상황, 훈련프로그램 등
기타	습관 및 취미정보	흡연 및 음주, 스포츠 및 오락 등
	통신정보	전자우편 및 전화통화 내용, 인터넷 접속 등 로그파일 등
	위치정보	GPS 등을 통해 확인가능한 개인의 위치정보

자료: 성윤모(2004).

일반적으로 개인정보는 개인의 건강상태, 신체적 특징, 사상이나 신념과 같은 정신세계, 학력·경력·재산 상태, 사회적·경제적 지위 등 개인에 관한 사실·판단·평가를 나타내는 모든 정보를 의미한다. 여기에는 생존하고 있는 자연인에 관한 정보뿐만 아니라 법인정보, 사자(死者)의 정보도 모두 포함한다. 이러한 개인정보는 '개인정보보호법'에 근거하여 규정하고 있으며, '정보통신망 이용 촉진 및 정보보호 등에 관한 법률(정보보호법)'에 근거하여 기술적·관리적 보호기준을 수립하고 있다

2. 정보이용과 정보관리

우리나라가 본격적으로 전자정부를 구현하면서, 전자정부 11대 중점 과제와 전자정부 로드맵 31대 과제를 추진하게 되었다. 이러한 과정에서 전자정부에서의 정보유통을 활성화시키는 대표적인 2가지 과제를 들면, G4C 민원발급시스템과 행정정보 공동이용 시스템을 들 수 있다. 정보시스템 및 인터넷을 이용한 개인정보공유 및 대민서비스는 '민원사무처리에 관한 법률 시행령(제33조의2) 및 행정자치부고시(제2003-21호)에 따라 전자문서화되었다. 먼저, G4C 시스템은 2003년부터 서비스를 제공하기 시작하였는데, 무인민원발급기(KIOSK), 인터넷 등을 통한 민원서비스의 범위가 확대되고 있다.

<표 2> 인터넷 민원서비스 범위의 확대

구분	2004년	2005년	2006년	2007년
인터넷 신청	400여종	500여종	600여종	1,000여종
인터넷 발급	8종	20여종	30여종	50여종

자료 : 행정자치부(2005).

더욱이 지난 2005년 G4C 민원발급 시스템과 연계한 민원서류의 위·변조 사건을 비롯한 전자문서의 위·변조 발생으로, 거래상대방의 신원확인 및 전송내용의 비밀 유지 등이 어려지고 있다. 이로 인해 공공기관에서 보유하는 개인정보가 노출되는 사고를 해결하기 위한 방안들이 마련되고 있다. 그 중에서 행정정보 공동이용은[3] 지난 2005년부터 공공기관간의 문서감축 및 공동이용을 위한 시스템 개발과 법제 정비를 추진하고 있다.

행정자치부는 공공기관을 대상으로 '개인정보보호법'에 근거하여 보유하고 있는 개인정보파일을 수집하여 관보에 게재하도록 규정하고 있다. 그에 따르면, 현재 중앙행정기관, 지방자치단체, 공공기관, 각급 학교 등 총 22,000여개 공공기관에서 보유하고

3) 개인정보의 공동이용형태는 행정기관의 정보화의 유형에 따라 ① 내부 업무 처리를 위한 정보 공동이용, ② 정책 결정 지원을 위한 정보 공동이용, ③ 민원 서비스를 위한 정보 공동이용, ④ 열린 정부를 위한 정보 공동이용으로 구분할 수 있다(김동욱, 1996; 박홍윤 외, 1999).

있는 개인정보가 증가하고 있음을 알 수 있다.

<표 3> 보유기관별 개인정보파일 현황[4)]

보유기관	개인정보 파일수	
	2006년	2007년
합계	1,144	1,345
중앙행정기관(소속기관 포함)	277	294
지방자치단체(시도, 시군구)	397	510
교육기관(교육청 및 각급 학교)	67	102
공공기관(정부투자기관 및 기타)	403	439

자료: 행정자치부(2007).

그러나 공공기관에서 보유하고 있는 정보접근방식으로 국민의 인터넷 민원서비스와 공공기관의 행정정보 공동이용 서비스가 확대되고 있다. 그러나 현재의 개인정보 보호와 보안수준에 대한 미흡한 점을 인정하고 관리대책을 마련해야 한다. 일례로 지난 2007년 4월에 '국회 디지털포럼'주관으로 정부기관을 대상으로 한 모의해킹을 실시한 결과, 대상기관의 85%가 해킹에 취약하다고 나타났다. 또한 행정자치부에서 '홈페이지 개인정보 노출 모니터링'을 실시(2005~2007)하였는데, 개인정보가 노출된 경우가 13만 건이며, 보안이 취약한 경우도 318건이었다(행정자치부, 2007).

<표 4> 공공기관의홈페이지개인정보노출현황

구 분	2005		2006				2007	
			상반기		하반기			
	노출 사이트	노출건수	노출 사이트	노출건수	노출 사이트	노출건수	노출 사이트	노출건수
중앙행정기관	1	1	10	1,060	25	8,177	7	510
지방자치단체	77	16,707	21	2,279	163	31,300	43	6,365
기타(소속・산하기관)	3	706	42	8,634	240	33,450	10	34
합계	11	6,729	73	11,973	428	72,927	265	18,519

자료 : 행정자치부(2007).

4) 개인정보파일의 예로는 행정자치부(비위면직자 파일, 지적 파일 등), 건설교통부(토지종합전산파일, 토지거래 파일 등), 국세청(소득세 과세표준 및 세액신고서, 근로소득 원천징수 영수증 등), 서울특별시(사업용 차량 파일, 불법주정차과태료관리, 위생업소관리 등), 부산광역시(택시운전자격관리, 정화조관리, 환경개선부담금 등)등이 소유하고 있는 정보가 해당된다.

따라서 개인정보의 이용범위가 확대되어 짐에 따라 이를 보호할 효율적인 대책이 마련되어야 한다. 즉 하드웨어인 측면뿐만 아니라 소프트웨어적인 측면을 고려하여 전화번호부, 주소록, 스케줄, 상담내용, 메모리 등 개인적으로 필요한 모든 정보를 관리하는 개인정보관리(Personal Information Management)가 이루어져야 한다.

3. 선행 연구 동향

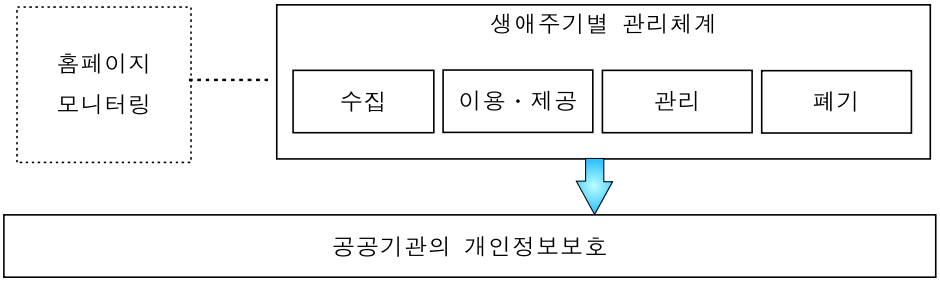
지금까지 개인정보에 관한 보호 또는 관리에 관한 연구가 지속적으로 이루어져 왔는데, 권헌영(2005), 홍석한(2005)은 전자정부 구현에 따른 개인정보보호의 중요성을 주장하였다. 유비쿼터스 사회가 도래함에 따라 발생하는 문제를 해결하고 개인정보보호를 강화하도록 오태원(2006), 임영덕(2005) 등이 새로운 환경에서의 개인정보보호를 강조하였다. 이러한 흐름 속에서 김재정(2007), 김지현(2007), 심영선(2006), 조승만(2006), 길준규(2004), 권건보(2004), 등은 공공기관의 정보관리에 따른 문제해결을 위한 법적 규정의 중요성을 제기하였으며, 임종인(2006), 신영진(2006)은 공공기관의 정보보호현황을 파악하고 그에 따른 정책적 과제를 제시하였다. 또한 윤취영(2003)은 공공기관의 개인정보보호를 위한 방안으로 개인정보의 관리 및 평가체계의 중요성을 제기한 바 있다.

그러나 행정정보 공동이용이 증가하고 있는 현 시점에서, 권건보(2006), 염동훈(2005), 김대성(2004), 박홍윤(2002), 박홍윤·윤견수(1999) 등은 개인정보를 공동이용하는 측면에서 공공기관 간의 개인정보를 이용하는 과정에서의 프라이버시 보호방안을 제시하였다. 또한 공공기관에서의 개인정보가 노출됨에 따라 김민기(2004), 문신용·윤기찬(2004)은 개인정보의 침해사례를 통해 개인정보보호에 대한 정책적 방향을 제시하였다. 이와 같이 교육정보(NEIS), 의료정보 등 대표적인 개인정보를 이용하여 개별적인 관리대책을 마련하고자 노력하였다.

이외에도 개인정보보호를 위한 기술적인 방안이 지속적으로 이루어져 왔으며, 공공기관의 개인정보보호에 관한 표준화된 체계와 합리적인 관리방안이 필요하다. 여기서 제기된 선행연구들의 관점을 종합하면, 공공기관의 개인정보보호를 위해서는 신기술의 변화에 따른 지속적인 관리체계가 필요하다는 것이다. 이를 해결하기 위한 제도적 뒷받침이 필요한데, 각 개별 사례를 바탕으로 한 문제해결방안들이 절실하다는 것이 연구자들의 주장이다. 이에 본 연구에서는 기존의 연구체계를 바탕으로 우리나라에서의 개인정보 관리실태를 비교하고, 그에 따라 중앙행정기관, 지방자치단체, 공공기관, 교육기관 등을 대상으로 우선적으로 추진되어야 할 정책들을 제시하고자 한다.

4. 연구의 분석 틀과 방법

본 연구에서는 공공기관에서 추진하고 있는 개인정보의 보호 및 관리 실태를 생애주기를 중심으로 조사하고자 한다. 이를 위해서 각급 25개 공공기관[5]을 선정하여 2007년 6월에 설문조사와 면접조사를 실시하고자 한다.



<그림 1> 분석의 틀

먼저, 행정자치부에서 공공기관을 대상으로 실시하고 있는 홈페이지 모니터링의 결과를 바탕으로, 조사대상기관을 선정하였다.[6] 이들 기관을 대상으로 생애주기별 관리체계에 관해 다시 개인정보의 수집, 이용·제공, 관리, 폐기로 구분하여 설문조사와 면접조사를 2단계로 구분하여 실시하도록 한다.

둘째, 공공기관을 구분하여 기관유형에 따른 개인정보 관리현황을 파악하고, 각 기관간의 실태비교를 하여 각 기관의 특징을 도출한다.

셋째, 본 연구과정에서의 문제점 및 한계를 통해 앞으로 공공기관의 개인정보보호를 강화할 수 있는 정책을 제시한다.

---

5) 25개 대상기관은 5개 중앙행정기관(국민고충처리위원회, 국가보훈처, 환경부, 중소기업청, 병무청), 3개 시도(충남, 전남, 경남), 8개 시군구(경기 김포시, 서울시 종로구, 경기 화성시, 대전 유성구, 전남 목포시, 제주 제주시, 경북 구미시, 부산시 진구), 4개 공공기관(대한주택공사, 교통안전공단, 한국전력공사, 부산항만공사), 5개 교육기관(서울교육대학교, 한밭대학교, 제주대학교, 전남대학교, 부산대학교)으로 구성하였다.

6) 행정자치부에서는 공공기관을 대상으로 홈페이지상의 개인정보 노출현황을 조사하였다.

구 분	2005		2006				2007	
			상반기		하반기			
	노출사이트	노출건수	노출사이트	노출건수	노출사이트	노출건수	노출사이트	노출건수
중앙행정기관	1	1	10	1,060	25	8,177	7	510
지방자치단체	77	16,707	21	2,279	163	31,300	43	6,365
기타(소속・산하기관)	3	706	42	8,634	240	33,450	10	34
합계	11	6,729	73	11,973	428	72,927	265	18,519

※ 2005년, 2006년 상반기는 정보보호진흥원, 자치정보화조합에 의해 비정기적으로 점검하여 상대적 노출건수가 적음

III. 분석 결과 및 한계

1. 생애주기별 관리 실태

1) 개인정보의 수집단계

공공기관에서 보유하고 있는 개인정보를 일반정보, 경제상황, 사회경력, 의료정보, 민감정보 등으로 구분하여[7] 인터넷, 전화, 서면 등의 방법으로 수집하고 있는 현황을 조사하였다. 지방자치단체가 보유하고 있는 개인정보가 48%로 가장 많았으며, 그 중에 기초자치단체가 개인정보를 많이 보유하고 있음을 알 수 있었다.

<표 5> 공공기관의 개인정보 보유 현황

기관 / 비율	중앙행정기관	지방자치단체		공공기관	교육기관
		광역자치단체	기초자치단체		
기관별 현황	24(%)	7(%)	39(%)	11(%)	19(%)

전체 조사된 공공기관이 개인정보를 수집하는 방법으로는 인터넷 59.48%, 전화 7.52%, 서면 61.76%, 기타 10.78% 등으로 나타났다. 개인정보의 양이 많은 기초자치단체는 인터넷을 통해 수집되는 개인정보가 49%, 서면으로 수집되는 개인정보가 26%를 차지하여 다른 기관에 비해 인터넷을 통한 개인정보의 수집이 더 많다는 것을 알 수 있다 이렇게 개인정보를 수집하는 과정에서 개인정보의 주체에게 그 사실을 공지하고, 홈페이지를 통해 개인정보보호 지침 및 정책을 게시하였다. 그러나 일부기관에서는 개인정보의 보유기간, 외부위탁사실, 삭제요청, 파기사항 등에 대해 공지하고 있지 않아 개인정보주체의 권익을 침해할 우려가 있다.[8] 또한 대부분의 기관이 개인정보를 수집함에 있어, 주민등록번호를 따로 수집하지 않고, 정부의 통합 ID, 신용정보회사의 실명확인 등을 활용하고 있다.

---

7) 일반정보(성명, 주민등록번호, 생년월일, 주소, 본적, 가족관계, 전화번호(유선/무선), 주소(자택/직장), e-mail), 경제상황(소득, 동산 및 부동산, 은행계좌, 신용카드번호), 사회경력(학력, 직업, 직장명, 범죄경력), 의료정보(신장, 체중, 혈액형, 병력, 신체장애, 생체정보), 민감정보(사상, 신조, 종교, 가치관), 기타(전화통화내역, IP주소, CCTV 화상정보)

8) 공공기관의 개인정보보호를 위한 기본지침에 근거하여 개인정보관련 부서/책임자(담당자) 안내, 개인정보 수집 및 이용 목적, 타 기관과의 개인정보 공유가능, 정보주체의 개인정보 수정·열람, 개인정보의 보유·이용 기간, 개인정보보호를 위한 각종 기술적 조치, 개인정보 삭제요청, 개인정보 외부위탁 사실, 개인정보 파기사항 등에 대해 공지하여야 한다.

<표 6> 공공기관의 개인정보 수집경로

구분		수집경로			
		인터넷	전화	서면	기타
중앙행정기관		11.44	0.33	11.76	4.25
지방자치단체	광역	6.86	0.00	8.17	0.98
	기초	18.95	0.98	25.82	4.58
공공기관		11.44	0.00	0.00	0.00
교육기관		10.78	0.00	0.98	0.00
전체(계)		59.48	1.31	46.73	9.80

2) 개인정보의 이용 및 제공 단계

공공기관에서 외부기관에게 개인정보의 수집, 이용 및 제공, 관리 등에 관한 상황을 위탁하고 있는 지를 조사하였는데, 비교대상 공공기관 중에서 지방자치단체가 외부기관에의 위탁관계를 가장 많이 형성하고 있었다. 그 중에서 기초자치단체가 34%로 외부에 위탁을 가장 많이 하고 있었으며, 그 다음으로 중앙행정기관과 공공기관이 각각 22%로 위탁을 수행하고 있었다.

<표 7> 공공기관 특성별 개인정보 위탁현황

기관 / 비율	중앙행정기관	지방자치단체		공공기관	교육기관
		광역자치단체	기초자치단체		
기관별 현황	22(%)	11(%)	34(%)	22(%)	11(%)

그러나 대부분의 위탁사항을 살펴보면, 개인정보저장시스템의 유지보수 및 기술적 관리를 위해서 외부업체에 위탁하고 있었으며(28%), 고객 등의 불만접수처리 등을 위해 위탁을 하고 있었다(8%).

<표 8> 공공기관의 개인정보 위탁관련 세부사항

위탁관련 세부사항	현황(%)
개인정보 저장 시스템의 유지 보수 및 기술적 관리	28
개인정보의 수집	4
고객 불만 처리(고객상담센터 등)	8
고객 정보 CRM 등 정보의 생성·처리	0
기타	4

<표 8>와 같이, 공공기관에서의 개인정보저장시스템의 유지보수 및 기술적 관리를 위한 위탁사항을 보면, 기초자치단체(12%), 중앙행정기관(8%) 등 순으로 위탁하고 있었다. 이처럼 공공기관이 외부에 위탁계약시 명시하고 있는 준수사항을 보면, 개인정보에 관한 비밀유지(28%)가 가장 많으며, 위탁처리 범위·기간 등 명기(24%), 제3자 제공의 금지(20%), 사고시의 책임부담(20%), 처리 종료 후의 개인 정보의 반환/파기 등 규정(8%)을 명시하고 있다. 그 중에서 가장 중요한 개인정보에 관한 비밀유지를 담고 있는 위탁사항의 경우, 중앙행정기관(8%), 기초자치단체(8%), 공공기관(8%)에서 준수사항으로 지정하고 있다.

3) 개인정보의 관리단계

(1) 제도적 관리단계

공공기관에서 운영하고 있는 개인정보보호를 위한 제도적 관리가 이루어지고 있는지 조사한 결과를 살펴보면 다음과 같다. 즉, 공공기관이 개인정보를 보호 및 관리하기 위해서는 공공기관에 의해 제정된 자체규정이 수립되어야 한다.

<표 9> 공공기관의 개인정보보호 자체규정 현황

기관 / 비율	중앙행정기관	지방자치단체		공공기관	교육기관
		광역자치단체	기초자치단체		
기관별 현황	39(%)	8(%)	15(%)	15(%)	23(%)

이에 대해 조사대상 공공기관들 중의 52%가 자체규정을 수립하여 개인정보보호에 적극적으로 대처하고 있다. 그중에서 중앙행정기관이 개인정보보호에 관한 자체 규정 및 자체적인 개인정보보호계획을 수립하여 추진하고 있었다. 공공기관이 자체적으로 규정하고 있는 내용들을 살펴보면, 개인정보보호의 책임관 지정(48%), 개인정보DB에 대한 접근권한 부여기준(44%), 개인정보DB에 대한 접근 권한의 변경 및 말소(36%), 개인정보DB에 대한 접근권한의 변동에 따른 로그정보의 기록(36%), 침입차단 시스템의 설치·운영(36%) 등을 규정하고 있다. 이 중에서 공공기관별로 담고 있는 규정의 우선순위를 보면, 로그정보를 기록하는데 중앙행정기관(20%), 책임관을 지정하는 데 공공기관(9%)과 교육기관(12%), 기초지방자치단체(7%), 광역지방자치단체(5%) 순으로 규정을 두고 있다. 공공기관에서 개인정보보호를 위해 두고 있는 자체 규정의 내용을 보면 <표 10>과 같다.

<표 10> 공공기관의 개인정보보호 자체규정 내용

개인정보보호에 관한 자체규정 내용	현황(%)
개인정보관리책임자의 지정에 관한 사항	48
개인정보보호 조직의 구성·운영에 관한 사항	10
개인정보 취급자의 교육에 관한 사항	28
개인정보DB에 대한 접근 권한 부여 기준에 관한 사항	44
개인정보DB 접근 권한 변경 및 말소에 관한 사항	36
개인정보DB 접근 권한 부여, 변경, 말소에 대한 로그정보 기록에 관한 사항	36
침입차단시스템 설치·운영에 관한 사항	36
개인정보 취급자의 개인정보DB 접근 권한 패스워드 작성 규칙에 관한 사항	24
개인정보처리시스템 및 개인정보 취급자의 PC 설정 및 보안에 관한 사항	32
개인정보처리시스템에서의 개인정보 출력(인쇄, 화면표시, 파일 생성 등)의 용도 특정에 관한 사항	32
개인정보취급자가 개인정보를 종이로 인쇄하거나, 이동저장매체에 복사하는 경우의 내역 기록에 관한 사항	20
개인정보취급자가 개인정보를 종이로 인쇄하거나, 이동저장매체에 복사하는 경우의 승인 절차에 관한 사항	16
기타	12

개인정보보호에 관한 조직체계를 구성하고 있는 지에 대해 모든 기관이 법률에 의거하여 책임관을 두고 있었으나, 별도의 조직체계를 운영하고 있는 기관은 전체 조사대상 기관의 28%가 해당되었다. 또한 대부분의 공공기관이 개인정보보호책임관, 분야별 책임관, 담당자를 선정하고 있으나, 개인정보보호외의 다른 업무도 수행하고 있었는데, 담당자로 다른 업무를 겸직한 1인 담당자를 두는 경우가 52%이고, 다른 업무를 겸직한 2인 이상의 담당자를 두고 별도의 시스템을 운영하는 경우가 28%로 개인정보보호에 관한 업무비중이 그다지 높지 못한 것을 알 수 있었다.

<표 11> 공공기관의 개인정보보호 조직체계[9)]

구분	조직체계 구성정도(%)				
	조직 구성	독립한 담당자		겸직한 담당자	
		1인	2인 이상	1인	2인 이상
중앙행정기관	4			8	8
광역자치단체	4			8	8
기초자치단체	4			24	0
공공기관	12			0	4
교육기관	4			12	8
전체(계)	28			52	28

9) 개인정보보호 조직체계는 개인정보보호책임관, 개인정보보호관리자, 개인정보보호담당자로 구성된다.

(2) 물리적・기술적 관리단계

공공기관에서는 기관내의 개인정보를 보호하고 안전한 관리체계를 구현하기 위해 비밀번호(P/W), 백신프로그램, 침입차단/탐지 시스템, 취약성 진단시스템, 접근로그(LOG) 보관 등의 물리적인 대책을 마련하고 있다. 이에 대해 가장 많이 도입되고 있는 보안방법이 비밀번호를 이용하거나(25%) 백신 프로그램을 활용하고 있는 것으로 나타났다(25%).

<표 12> 공공기관의 개인정보보호 장치 및 대책

개인정보보호 장치 및 대책	도입현황(%)
비밀번호(패스워드)를 이용한 보안장치	25
백신 프로그램을 이용한 컴퓨터 바이러스 방지장치	25
침입차단시스템을 이용한 보안장치	24
시스템 취약성진단 시스템을 이용한 정기 점검	11
침입탐지시스템을 이용한 보안장치	20
접근기록(LOG) 보관	23
기타 기술적 장치	8

이와 관련하여 홈페이지에서의 개인정보에 대한 노출방지대책을 수립하여 추진하고 있는데, 담당자가 직접 모니터링을 하고 있는 경우가 가장 높았으며(22%), 필터링 프로그램을 도입하거나(14%), 웹 방화벽을 설치하였다고 하였다(10%). 그 외에도 웹 암호화, 개인정보 진단 프로그램, 키보드보안 등을 운영하고 있었다. 그러나 홈페이지 모니터링을 비롯한 개인정보보호를 위한 예산이 부족하여, 추가적인 프로그램 구매나, 보안패키지를 설치하지 못하고 있어 이에 대한 정부차원에서의 지원을 요구하고 있다.

<표 13> 홈페이지상의 개인정보 노출방지 추진 현황

홈페이지상의 개인정보 노출방지대책	도입현황(%)
필터링 프로그램 등 관련 솔루션 도입・운영	14
홈페이지 취약점 진단・제거 솔루션 도입・운영	6
검색엔진을 통한 개인정보 수집 방지 대책 시행	16
담당자를 통한 홈페이지 개인정보 노출 여부 수동 모니터링	22
웹방화벽의 도입・운영	10
기타	6

또한 일선기관을 비롯한 대민서비스를 제공하는 공공기관에서는 개인정보를 취급하는 담당자들에게 DB 접근권한을 부여하고 있었다. 이는 대부분 정보시스템 상에서의

접근통제를 실시하고 있으나, 사내 규정이나 별도의 문서승인절차를 거쳐 접근제한을 두고 있다. 이에 따라 개인정보를 안전하게 구현하기 위해서는 DB 등의 정보시스템에 대한 접근통제를 강화하여, 무분별한 정보유통을 최소화하여야 할 것이다. 이에 따라 정보시스템에 대한 접근권한을 통제하여 인사 이동시 신속히 변경하도록 하며, 관리자로 하여금 DB접근권한에 대해 정기적으로 갱신하도록 하였다.

(4) 개인정보의 파기단계

공공기관에서 보유하고 있는 개인정보는 행정목적을 위해 수집・이용・처리・폐기되어진다. 이러한 과정에서 홈페이지의 경우 회원이 탈퇴 또는 서비스기간이 종료될 때, 개인정보를 즉시 삭제하여야 한다. 이에 대한 조사결과를 보면, 대부분 조사대상기관이 개인정보를 즉시 파기하고 있었으나, 일부 교육기관에서는 학적관련 정보를 영구보존하고 있어 그에 따른 예외규정이나 관리가 필요하다. 이처럼 개인정보를 파기하지 않고 보유하는 경우 세법, 상법, 국세기본법 등과 같은 법률, 기관 내부규정, 관련 법령, 방침 등에 의해 근거를 두고 보유할 수 있다. 그 외에 개인정보가 유출될 수 있으므로, 그에 대한 관리규정을 마련해야 한다. <표 14>에서와 같이, 개인정보의 파기현황을 보면, 지방자치단체가 잘 준행하고 있으며, 기초자치단체가 그중에서 가장 개인정보의 사후관리를 철저히 하고 있음을 알 수 있다.

<표 14> 공공기관의 개인정보 파기 현황

기관 / 비율	중앙행정기관	지방자치단체		공공기관	교육기관
		광역자치단체	기초자치단체		
기관별 현황	19(%)	10(%)	38(%)	19(%)	14(%)

2. 분석의 한계

지금까지 공공기관의 개인정보관리 현황을 살펴보면, 대부분의 공공기관이 개인정보보호에 관한 중요성을 인식하고 있었으며, 이를 위한 교육, 지침, 매뉴얼 등을 제공하고 있다, 기술적 보안을 위해서는 개인정보처리 및 관리 시스템에 대한 취약점 진단, 방화벽 설치, 암호화 등을 통해 안전성을 확보하였다. 이외에 개인정보보호의 인식제고를 위한 방안으로 공공기관의 자체교육, 사이버 교육, 방문교육 등을 실시하고 있다. 그러나 개인정보보호를 강화하기 위한 인력과 예산이 부족한 실정이므로, 이에 대한 지속적인 대책이 마련되어야 한다. 앞서 살펴보았던 생애주기별로 공공기관간의 개인정보 관리실태를 살펴보았는데, 그 과정에서의 몇 가지 미흡한 점들이 발생

하였다.

먼저 본 연구의 과정에서 공공기관마다 구현하고 있는 개인정보의 관리체계가 '개인정보보호법'에 근거하여 규정하고 있으나, 기관마다 상이한 체계를 구현하고 있어 서로 비교하여 결과를 도출하기에는 한계가 있다. 일례로 중앙행정기관, 지방자치단체, 공공기관, 교육기관마다 수집하고 있는 개인정보가 다르므로, 개인정보의 중요도에 따른 관리체계를 구현할 수 있는 방안을 제시할 필요가 있다. 개인정보의 수집과정에서도 인터넷, 서면, 전화 등을 채택하고 있으나, 이외에 어떤 방식을 채택하고 있는 지 파악하지 못하고 있어 개인정보의 수집경로를 파악하는 데는 한계가 있다.

둘째, 본 연구에서는 개인정보의 이용 및 제공과정에서 개인정보를 위탁하고 있었는데, 개인정보가 저장된 시스템의 유지보수 또는 기술적 관리를 위해 가장 많이 위탁계약을 맺고 있었다. 그러나 본 연구에서 이용과 제공이 외부기관과의 교류를 포괄하여 담고 있지 못한 데 한계가 있다.

셋째, 본 연구에서는 개인정보가 제도적인 측면에서 관리되고 있는지에 대해 중점을 두었다. 이러한 과정에서 개인정보보호를 위한 규정, 인력 및 전담조직에 초점을 두었는데, 이외에도 개인정보보호를 위한 예산과 교육에 대한 현황을 포괄하지 못하였다. 개인정보보호를 위해서 정부는 공공기관의 개인정보를 규정하는 법제가 필요하며, 이를 처리하기 위한 조직체계가 마련되어야 한다. 그러나 현실적으로 공공기관에서 개인정보보호 업무책임자가 다른 업무와 겸직하고 있었으며, 제대로 교육을 받지 못한 경우가 많아 그에 대한 적극적인 대책이 필요한 상황이다.

넷째, 공공기관의 개인정보를 보호하기 위한 물리적·기술적 관리에서는 비밀번호(P/W), 백신프로그램, 침입차단/침입탐지 시스템, 취약성 진단시스템, 접근로그(LOG) 보관 등을 하고 있는지에 대해 파악하였다. 신기술의 발달됨에 따라 개인정보관리시스템에 대한 침입방지를 위한 다양한 대책이 구현되고 있다. 따라서 이에 대해 표준화된 기술적 대책을 마련하지 않으면, 본 연구에서 제시한 항목으로는 기술적인 대책이 이루어졌다고 볼 수 없다.

다섯째, 개인정보의 파기에 관해 대부분이 기관이 즉시 파기하고 있었으나, 교육기관 등을 비롯하여 일부기관에서는 개인정보를 영구보존해야 할 경우가 있다. 그러나 본 연구에서 보았던 법률상 즉시파기 사항만으로 개인정보의 사후처리가 잘되었다고 볼 수 없으므로, 개인정보를 파기하지 않을 경우에 대한 근거규정을 파악하여 현황을 관리할 필요가 있다.

본 연구는 공공기관의 개인정보를 생애주기별로 어떻게 관리하는 지에 대해 초점을 두어 연구하였다. 이런 과정에서 25개 기관으로 개인정보를 처리하는 모든 기관의 특성을 포함하였다고 보기는 어렵다. 또한 개인정보관리가 단순히 생애주기별로 이루어지는

것이 아니므로, 개인정보의 수집에서 폐기까지 전 과정을 안전하게 운영하기 위한 관리 체계가 구현되어야 한다.

IV. 정책적 시사점 : 개선방안

정보기술의 발달로 인하여 개인정보보호에 대한 중요성이 강조되고 있는데, 역기능적 기술의 발달로 인한 침해를 방지하기에는 공공기관의 보안대책이 매우 미흡한 실정이다. 이에 대해 공공기관의 개인정보보호를 위한 관리현황을 생애주기별로 구분하여 살펴보았다. 먼저, 개인정보의 수집단계에서는 '개인정보보호법'에 근거한 개인정보의 정의와 범위가 기관마다 적용하기에는 모든 공공기관의 개인정보를 포괄하지 못한 실정이다. 이처럼 공공기관에서 보유하고 있는 개인정보를 모두 포괄하지 못하기 때문에, 개인정보에 대한 명확한 분류체계가 필요하다. 또한 다양한 방법을 통해 개인정보를 수집하고 있는데, 이러한 과정에서 개인정보의 유통경로를 파악할 수 있는 방안이 마련되어야 할 것이다. 현재 개인정보의 전송에 따른 LOG기록을 두고 있으나, 이외에 수집된 개인정보의 범주를 관리한다면, 필요한 정보를 안전하고 쉽게 제공받을 수 있을 것이다.

둘째, 개인정보의 이용 및 제공단계에서는 개인정보가 다른 기관으로부터 수집되거나 다른 기관에게 제공하는 경우가 앞으로 행정정보공동이용시스템으로 대체되기 때문에 상당부분 정보의 전환이 발생할 것이다. 그러나 각 기관에서 보유하고 있는 개인정보가 업무처리의 편리를 도모하기 위해서는 외부기관에게 위탁하는 경우가 증가할 것이므로 이에 대한 철저한 위탁관리가 필요하다. 현재 외부기관과의 위탁계약시 개인정보처리에 대한 책임 및 관리에 대해 강력한 법적 규정을 적용하지 못하고 있으며, 개인정보에 대한 모든 관리에 대해 철저한 모니터링도 이루어지고 있지 못하다. 따라서 외부기관과의 위탁체결에 대한 아웃소싱 가이드라인을 제공하고, 위탁기관에서의 개인정보 관리가 철저히 이루어지도록 아웃소싱 표준화 모델을 지원하여 위탁업무의 효과를 거둘 수 있도록 해야 한다.

셋째, 개인정보의 관리단계에서 제도적 관리는 개인정보보호에 관한 자체 규정을 마련하도록 하고, 그에 따른 개인정보보호 전담부서, 개인정보보호 담당자 등을 지정하여 운영하도록 규정하고 있다. 그러나 현재의 개인정보보호 전담부서 및 담당자가 개인정보보호를 위한 관리대책을 수립하지 못하고 있어 이에 대한 관리대책을 지원해 주어야 한다. 즉, 현재 명확치 않은 개인정보보호예산의 정기예산편성에 편성하여 기관별 개인정보보호예산을 마련해야 한다. 또한 개인정보보호 전담부서 및 담당자의 업무체계를 구축하고, 국가차원에서의 개인정보보호대책에 반영하여 실질적인 관리정책을 제공하도록 활용해야 한다. 이외에도 개인정보보호 담당자들에 대한 교육이수과정을 두어 매년 일정기간의 교육을 제공하

고, 개인정보처리과정에서의 업무지식을 배양하도록 지원해야 한다. 이에 대해 전문교육 프로그램, CD 및 동영상을 통한 실시간교육, 기관별 수준평가에 따른 맞춤형교육 등이 마련되어야 한다.

다음은 개인정보의 기술적·물리적 관리로는 개인정보관리를 위한 통합정보관리시스템을 구축하여 개별적으로 개인정보를 저장하지 않고 실시간 접근 가능한 관리프로세스를 구축하도록 한다. 물론, 개인정보에 관한 모니터링제도가 운영되고 있으나, 인프라적인 측면에서의 개인정보관리를 모두 포괄하지 못하고 있다. 따라서 하드웨어적인 보호체계는 범정부적으로 구현하고, 홈페이지 모니터링을 제도화하여 온라인과 오프라인 상에서의 보호체계가 구현되도록 한다.

이외에도 공공기관의 개인정보 보호를 위한 방안이 지속적으로 마련되고 있으며, 개인정보보호에 대한 관심도 증가하고 있다. 최근 개인정보관련 문제가 이슈가 되면서, 행정자치부, 정보통신부, 국가정보원 등이 이를 해결하기 위한 협력관계가 형성되고 있다. 이처럼 정보보호 담당부처들 간의 통합네트워크를 형성하여 개인정보보호를 위한 기본대책을 마련한다면, 보다 효과적인 정책집행과 성과를 가져올 것이다.

V. 결 론

우리나라는 전자정부를 구현하는 과정에서 발생하는 문제를 해결하기 위해 다각적인 정책들을 추진하고 있다. 즉, 우리나라가 사이버인프라를 구축하여 활성화하는 과정에서, 개인정보의 침해 및 노출이 발생하고 있는데, 이를 해결하기 위한 대책이 시급한 실정이다. 더욱이, 대국민서비스의 질적 향상을 가져오기 위한 G4C 민원발급서비스, 행정정보공동이용서비스 등이 보편화되어가고 있는 현 시점에서, 개인정보의 유통은 점차 증가할 것이다. 그러나 지난 민원서류 위·변조 사건을 계기로 개인정보보호에 대한 중요성이 제기되고 있다. 또한 유비쿼터스 사회의 구현에 따른 편리한 생활환경과 더불어, 개인정보의 노출을 막기 위한 대책들이 마련되어야 한다.

이에 행정자치부에서는 '개인정보보호법'에 근거하여 개인정보보호정책을 추진하였으며, 전 공공기관을 대상으로 개인정보 관리방안을 제시하고 있다. 그 대표적인 것이 2000년부터 추진하여 온 공공기관의 개인정보보호 실태조사와 2005년부터 실시한 홈페이지 개인정보 노출 모니터링이다. 본 연구에서는 이를 활용하여 공공기관의 개인정보보호를 위한 관리실태를 생애주기별로 진단해 보았다. 즉, 개인정보를 수집, 이용·제공, 관리, 폐기하는 단계로 구분하여 분석하였는데, 먼저, 개인정보의 수집단계에서는 개인정보의 수집방법이 다양해지고 있으며, 수집된 개인정보의 양도 증가하고 있다. 따

라서 개인정보의 수집과정에서 개인정보의 유통경로를 파악하고, 수집된 개인정보의 분류체계를 명확히 할 필요가 있다.

둘째, 개인정보의 이용 및 제공단계에서는 개인정보에 대한 외부위탁과정을 살펴보았는데, 현재 외부기관에 위탁하고 있는 공공기관 중에서 대부분이 기존의 시스템을 유지 보수하기 위해서 위탁한 상태이다. 그러나 외부기관과의 위탁계약을 체결하여 운영하고 있음에도 위탁계약의 준수정도를 파악하지 못하고 있다. 따라서 통합전산망센터 등을 이용하여 외부기관에 대한 위탁을 최소화하고, 개인정보를 위탁하는 전과정에 대해 표준화된 지핌과 모델을 제시해 줄 필요가 있다.

셋째, 개인정보의 관리단계에서는 개인정보보호에 관한 제도적 관리측면에서는 관련 규정을 자체적으로 제정하도록 하였다. 또한 공공기관의 개인정보보호 책임관, 관리자, 담당자를 구성하여 개인정보보호업무를 처리하도록 하였으며, 이외에 다른 업무와의 겸직에 대한 인력확보가 필요하다. 또한 개인정보의 안전성을 보장하기 위해 개인정보보호예산을 확충하고 개인정보보호에 관한 교육을 실시하여 개인정보관련 처리능력을 높이도록 해야 한다. 개인정보의 물리적·기술적 관리단계에서는 개인정보보호를 위한 비밀번호, 백신프로그램, 침입차단/탐지 시스템, 취약성 진단시스템 등이 추진되어 왔다. 이에 개인정보처리과정에 대한 실시간 관리체계를 구축하고, 웹사이트를 통한 안전한 대책마련이 시급한 실정이다.

넷째, 개인정보의 파기단계에서는 법률에 근거하여 즉시파기 하도록 규정하고 있으나, 보유상황에 따라 발생하는 차이에 대해 언제까지 보관할 수 있는지에 대해 명확한 기준이 부족하다. 따라서 이에 대한 개별 규정을 마련하여 기관의 특성에 따른 보존가능성을 포괄해야 한다.

이처럼 본 연구에서는 생애주기별 개인정보 관리체계를 분석해 보았으며, 그에 따른 개인정보보호방안을 제시하였다. 지금까지 우리나라는 적극적인 전자정부 구현과정을 거쳐 성공적인 성과를 거두어왔으며, 앞으로도 세계최고의 전자정부를 구현할 것이다. 그러나 정보인프라를 기반으로 하는 전자정부가 안전한 관리체계가 구현되는 것은 당연한 일이다. 그럼에도 불구하고 공공기관을 대상으로 하는 개인정보 보호정책은 개인정보관리체계에 대한 전반적인 구도를 그리기가 쉽지 않다. 더욱이 공공기관별로 추진하고 있는 정책들이 명확히 들어나지 않아, 그 성과를 평가하는데 한계가 있다. 따라서 앞으로 공공기관의 개인정보보호를 위한 범정부적인 차원에서의 추진체계를 구축하고, 좀더 강력한 권한을 부여하여 개인정보보호가 정착되고 발전될 수 있도록 지원해 주어야 할 것이다. 이러한 과정에서 본 연구가 지속 발전가능한 개인정보 보호정책을 추진하는데 있어서 안정화된 관리체계를 지원하는 연구가 되기를 기대한다.

<참 고 문 헌>

강동식. (2005). “개인정보판매허가제 도입.” 디지털타임스: 9.25.

권헌영. (2004). “전자정부시대 개인정보보호제도의 쟁점”. 사이버커뮤니케이션학회.

_____. (2004). “전자정부시대의 개인정보보호법제의 쟁점”.「정보화정책」 11(3). pp.55-78.

권건보. (2006). “행정정보 공동이용과 개인정보보호”.「전자정부법제연구」. 행정자치부.

_____. (2004).「자기정보통제권에 관한 연구: 공공부문에서의 개인정보보호를 중심으로」. 서울대 대학원.

길준규. (2004).「개인정보의 보호에 관한 연구」. 한양대학교.

김대성. (2004).「행정정보의 공동이용에 따른 법적과제에 관한 연구 : 개인정보보호를 중심으로」. 한양대학교.

김민기. (2004). 초등학교 홈페이지에서의 불건전 정보유통 및 개인정보노출 실태분석. 「한국정보교육학회보」, 8(4): 489~501.

김유경. (2005. 9. 23). 온라인 주민번호 대체수단. 전자신문: etnews.co.kr

김재정. (2007).「유비쿼터스환경에서의 개인정보보호 발전방안에 관한 연구」. 한양대학교.

김지현. (2007).「RFID기술에서의 개인정보보호 방안에 관한연구」. 건국대학교.

김태현.(2003).「개인정보보호제도에 관한 헌법적 고찰」. 경희대학교.

구은회. (2005. 2. 16) 공공기관 홈페이지서 개인정보 줄줄. 매일노동뉴스: labortoday.co.kr

문신용·윤기찬. (2004). 공공기관의 개인정보침해사례 분석의 함의 및 과제.「한국행정연구」. 한국행정연구원. 13(4): 210-251.

박성원. (1996).「행정정보의 관리전략 - 프라이버시보호를 중심으로 -」. 강원대학교 지역개발연구소.

박홍윤. (2002). 공공기관에서 개인정보의 이용과 통제-컴퓨터 프로필링 기법을 중심으로-.「한국사회와 행정연구」. 서울행정학회. 13(2).:89-:113

박홍윤, 윤견수. (1999). 공공부문에 있어서 개인정보의 공동이용에 따른 문제점과 해결방안.「정보화정책」. 6(3)

손호영. (2007).「개인정보의 사법상 보호에 관한 연구」. 중앙대 대학원

송귀종. (2005).「전자정부하에서의 개인정보보호에 관한 연구 : 공공부문을 중심으로」. 경희대 대학원.

심영선. (2006).「유비쿼터스 환경에서 개인정보보호법제의 개선과 확립에 관한 연구」. 이화여대.

정보통신정책연구원(2001). 일본 전자정부의 개인정보 보호. 연구원 자료. 정보통신정책연구원.

정부혁신지방분권위원회(2004. 4. 3) 전자적 민원처리 촉진 관련 법령정비 추진경과 보고. 내부보고자료.

강연두. (2005. 9. 24). 인터넷통한 개인정보유출 급증.「연합뉴스」.

오태원. (2006. 5). RFID에 관한 법정책적 연구.「인터넷법률」. 통권 제35호: 96-126.

염동훈. (2005).「공공기관의 행정정보 공동이용에 따른 개인정보보호 문제에 관한 연구」. 건국대학교.

윤동춘. (2000).「국가기관의 개인정보관리에 관한 헌법적 연구」.

윤취영. (2003).「개인정보화수준 및 성숙도 진단을 위한 통합평가시스템 개발에 관한 연구」. 연세대학교.

이경호·김소정·임종인. (2003) 전자정부와 프라이버시. 한국정보보호학회.

이동훈. (2004). 전자정부와 개인정보보호.「Information Security Review」. 1(2).

임영덕. (2005).「유비쿼터스 컴퓨팅에서의 개인정보보호」. 성균관대 대학원

임종인. (2006). 행정기관 정보보호 현황 및 과제: 정보보호.「지역정보화」. 자치정보화조합정보통신부. (2005).「안전한 u-Korea 구현을 위한 정보보호 중장기 로드맵」

정보통신정책연구원. (2004). 개인정보침해신고 유형 및 통계현황(2003.2-10). IT의 사회, 문화적 영향 연구: 21세기 한국메가트렌드 시리즈, 47: www.kisdi.re.kr/

정준현. (2005. 9). RFID/USN시대의 사생활보호의 법적 문제..「정보처리학회지」. 한국정보처리학회. 12(.5): 93-98

조승만. (2006).「유비쿼터스 컴퓨팅 환경에서의 RFID 사용에 따른 개인정보보호에 관한 연구」. 충남대학교.

한국전산원. (2005. 9. 30). 전자정부동향, 6. from http://www.nca.or.kr/nca_news/trend03_0913.htm

한국전자통신연구원. (2005).「인터넷 ID 관리 서비스」. 2005년 기술백서.

한국정보보호진흥원. (2005).「정보보호백서」.

행정자치부. (2005).「인터넷 민원서류 위・변조 방지대책 자료집」.

행정자치부. (2005. 9. 30). 행정자치부, 인터넷 민원 위·변조 피해사례접수. 뉴스와이어

행정자치부. (2007).「2007년 상반기 개인정보처리실태조사결과」.

홍석한. (2005).「전자정부구현에 따른 개인정보보호에 관한 연구」. 경희대 대학원

황인호. (2001).「개인정보보호제도에서의 규제에 관한 연구」. 건국대학교.

Adams, James. (1994). *The New Spies: Exploring the Frontiers of Espionage* London: Hutchinson.

Arquila, John. (1998). 'The Great Cyberwar of 2002,' Wired 6 (2). Feb.

Banks. S, (1990). "Security Policy", Computer & Security 9(7).

Brian, D. Loader. (1997). *The Governance of Cyberspace Politics, Technology and Global Restructuring*,

Cynthia E. Irvine. (2000). Security Issues for Automated Information Systems. G. David Garson, *Handbook of Public Information Systems*, Marcel Dekker.

Crabb, M. D. (1999). *Building A Successful Security Infrastructure.*

Earl, M. J. (1996). Integrating IS and the Organisation: A Framework of Organisational Fit. In M.J.Ear(ed). *Information Management: The Organisational Dimension,* Oxford: Oxford University Press, ch. 24. 485-502.

Elgamal,Taher. (2001.9). *Policy-Based Security.* OECD Information Security Workshop in Tokyo, Japan.

Fredrick, B. Cohen. (1994). *A Short Course on Computer Viruses.* John Willey & Sons.

Galliers, R. D. (1987). Information Systems Planning in the UK and Australia: a Comparison of Current Practice,. Zorkorczy, P.I.(ed.), Oxford Surveys in IT, Oxford: Oxford University Press. ch.4: 223-55.

Kay, J. (1993). Foundations of Corporate Sucess: How Business Strategies Add Value, Oxford: Oxford University Press.

Mark D. Rasch. (1996). Criminal Law and The Internet, in The Internet and Business: A Lawyer's Guide to the Emerging Legal Issues. www.cl.a.org/RuhBook/chp11.htm

McKersie, R. B. and Walton R.E.(1991) Organisational Change, in The Corporation of the 1990s: Information Technology and Organisational Transformation, Scott-Morton, M.S.(ed). USA: Oxford University Press.

OMB. (2002). OMB Guidance for Implementing the Privacy Provision of the E-Government Act of 2002. from http://www.whitehouse.gov/omb/memoranda/m03-22.html

Simon, D. Leslie. (2000). *NetPolicy. Com.* Woodrow Wilson Center Press.

West, Darrell M. (2003), *Global E-Government*, Rhode Island, U.S.A., Center for Public Policy, Brown University.

http://www.kisa.or.kr/Information_Security_Policy/data/m_03/vol.002_04.PDF

www.fcw.com 2005. 9. 6

http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.html

http://icic.sppo.go.kr

http://jura.pe.kr/info/critical-ifra.htm

http://members.tripod.com/steganography/stego.html

http://mips.mindef.gov.sg/doc/Dataprot.doc

http://www.ahnlab.com