정책세미나 자료집

서울시 전자정부의 개인정보보호 방안

일시 : 2004년 7월 7일 (수) 14:00 ~ 17:00
장소 : 서울시정개발연구원 2층 대회의실

서울시정개발연구원
Seoul Development Institute

프로그램

□ 13시 30 ~ 14시 **등록**

□ 14시 ~ 14시 10분 **개회식**

개회사 : 백 용 호(서울시정개발연구원장)

□ 14시 10분 ~ 15시 **주제발표**

발표자 : 변미리(서울시정개발연구원 부연구위원)

□ 15시 ~ 16시 30분 **패널 토론**

사회자 : 장덕진(서울대학교 교수)

토론자 (가나다순)

김대성(서울시 정보통신담당관)

김현성(서울시립대 교수)

서진완(인천대 교수)

조주은(IT전략연구원 연구위원)

최 혁(서울시립대 교수)

홍영림(조선일보 전문기자)

□ 16시 30분 ~ 17시 **질의응답**

□ 17시 **폐회**

목 차

서울시 전자정부의 개인정보 보호 방안

변 미 리

(서울시정개발연구원 도시정보센터 부연구위원,

miree21@sdi.re.kr)

제1장 연구개요

1. 문제의 제기

정부 정보화의 최적화된 모습으로서의 전자정부에서는 정보기술을 조직에 적용하여 효율성을 최대화하기 위한 조직재구조화 프로젝트들이 진행 중이며, 이러한 조직재구조화의 결과로서 대시민 행정서비스의 외양과 품질이 사용자인 시민중심으로 변화하고 있다. 특히 전자정부는 정보기술의 발전에 따라 점차 심화된 발전단계로 나아가고 있는데, 전자정부라는 이름에서 시작된 정보화 정부는 모바일 정부, 유비쿼터스 정부라는 새로운 이름을 달면서 진화를 거듭하고 있다.

'도처에 연결된, 편재하는 정보기술과 인간'이라는 새로운 패러다임 하에서 정보화된 정부는 오프라인 공간에서 처리되던 행정서류들이 전자정부라는 온라인 공간에서 다뤄지기 시작하는 초보적 형태에서부터 궁극적으로 온라인 행정조직이 오프라인 조직을 점차 포괄하는 형태로 발전하고 있는데, 이 과정에서 모바일 커뮤니케이션 기기의 확대 보급과 초고속인터넷망의 보급이라는 인프라 환경의 성숙이 결정적인 역할을 하였다.

그런데 시민편의성을 최대화하기 위한 전자정부가 개인들의 일상생활에 장밋빛 미래를 보장할 것인가에 대해서는 논란이 분분하다. 언제 어디서나, 어느 곳에 있던지 시민들이 '온라인 on-line'화 되어 있다는 것, 언제 어디서든 '연결된 connected' 상태로 존재한다는 것은 편리성의 최대화라는 긍정적인 측면 이외에 사회공간의 다양한 영역에서 지금까지와는 전혀 새로운 문제들을 야기할 수 있다. '나는 언제어디서든 관찰되고 있다'는 것이다. 나에 관한 모든 정보는 정부의 데이터베이스에 축적되어 있으며, 정부에서는 원하다면 언제든지 나에 관해 시시콜콜한 정보, 개인의 사생활에 관한 정보 등을 열람할 수 있다. 심지어 정부 데이터베이스에 해커가 침입하여 나에 관한 정

보를 빼내간다면 어떻게 될 것인가?

사회현상은 항상 양면성을 갖고 있다. 정보화가 사회에 미치는 영향에 관한 초기 논쟁이 이러한 양면성을 단순하게 대별시킨 것에서도 알 수 있듯이 정보사회의 효율성과 개인의 정보통제와 모니터링이라는 두 가지 상반된 측면은 전자정부의 발전과정에서 반드시 드러날 수밖에 없는 기제이다.

본 연구는 이러한 배경에서 출발한다. 행정서비스 제공자로서의 공공영역에서 정보기술을 접목시키면서 행정효율성과 시민편의성을 최대화하기 위한 다양한 시도들이 진행되거나 현재 진행 중인데, 현재 전자정부 단계에서 정보화의 이면에 존재하는 부정적인 측면을 최소화시키기 위해서 어떤 조치들을 준비해야 하는지에 대한 문제의식이다. 최근 온라인 상에 유행하는 '블로그'(blog)[1]라는 개인 홈페이지로부터 야기되는 개인정보 공개와 침해, 개인사생활 침해 등의 문제는 정보의 공개, 공유가 주는 편리성 이면에 숨은 부정적 현상을 잘 보여준다.

지금까지 개인의 사생활(프라이버시)보호는 개인의 기본적인 권리에 관한 것으로 법에 명문화되어 있으며, 정보사회 이전까지는 개인사생활에 관한 법률적 보장이 주를 이루었다. 그런데 정보사회가 심화되면서 개인의 사생활 보호가 그리 단순한 문제가 아니며 지금까지의 법률적 규제에 벗어나는 현상이 많이 일어나기 시작했다. 다시 말하면 정보기술사회에서 프라이버시 보호는 기술적, 규제적, 윤리적 관점에서 새로운 방식으로 부각되고 있다. 즉, 개인에 관한 수많은 정보들이 네트워크화된 다양한 사회공간에서 유통되면서 초기 정보제공자 혹은 정보입력자로서 개인의 권한은 축소되고 자신에 관한 정보가 자기를 떠나 독립적으로 존재하면서 어떤 경우에는 개인을 통제하게

---

1) 블로그란 웹(web)의 b와 로그(log)의 합성어로 '인터넷 일기장'을 뜻하는 것으로 자신의 생활이나 사진 등을 인터넷에 올려 다른 사람들과 공유하는 것이다. 최근 디지털카메라, 휴대폰카메라의 보급이 확산되면서 급속하게 퍼지고 있다. 현재 국내에 개설된 블로그는 2300만개로 추산되며 10대와 20대의 경우 2-3개를 동시에 운영하는 경우도 있는데, 이는 자신을 적극적으로 표현하는 수단으로 블로그가 안성맞춤이기 때문이다. 싸이월드 사이트는 블로그로 유명해졌는데 여기에 등록된 블로그 개수는 800여만개에 이르고 있다. 블로그에서 자주 나타나는 대표적 개인정보 침해사례의 경우 다른 사람이 내 홈페이지를 만들어 내사진을 무단복사한다거나 음란사진에 내 얼굴을 합성하여 유포시키는 경우 등이다. 정보통신부 관계자에 따르면, "블로그를 운영하는 순간 자신의 정보를 타인에게 공개하는 것을 동의했다고 볼 수 있으며, 다만 자신의 개인정보가 타인에 의해 유용되지 않도록 하기 위해서는 블로그 접속자를 블로그 주인에게 공개하도록 하고 인터넷 회원 가입시 주민등록번호와 이름이 실제와 일치하는지 확인하는 절차를 도입하는 것을 검토중" 이라고 한다.

되는 주객이 전도된 상황이 전개되기도 한다. 오늘날 우리의 모바일 기기로 무수히 날아드는 광고전화, 혹은 이메일로 무한정 쌓이는 스팸메일을 생각하게 보면 이 상황이 결코 낯설지 않을 것이다.

네트워크화된 정보시스템을 통해 공간적, 시간적 제한을 받지 않고 유통되는 무한한 데이터들이 야기하는 정보보호의 문제는 두 가지 관점에서 접근할 수 있다. 먼저, 개인의 사생활보호라는 측면이다. 이는 주로 개인정보보호에 대한 제한, 유통되는 정보에 대한 통제권리, 정보공유와 정보집적의 문제 등 정보보호와 관련된 법적, 제도적 관점, 윤리적이고 규제적인 측면, 조직문화적 관점에서 접근할 수 있다. 둘째는 정보보호 측면이다. 이는 정보시스템의 보안문제, 해킹과 시스템의 하드웨어적 방어, 정보기기의 오작동, 컴퓨터 바이러스 등 정보기술적 관점, 정보시스템의 안전성 등의 문제로 접근할 수 있다.

변화하는 정보기술환경은 프라이버시에 대한 기회이자 위협이다. 전자정부의 구축은 시민의 편의성을 획기적으로 증대시키면서 동시에 개인에 관한 방대한 정보가 정부의 데이터베이스에 집적·유통된다는 의미이다. 다시 말하면 나에 관한 정보는 내가 마음대로 공개하거나 공개하지 않거나 하는 상황이 아닐 수도 있다는 것을 의미한다. 내가 어떤 사회복지 혜택을 받는지, 그리고 어떤 공간에서 누구와 살고 있는지, 나의 직업은 무엇이며, 무슨 차를 타고 다니며 세금을 얼마나 내는지에 대해 나 말고 또다른 누군가가 알수도 있으며, 이 정보는 또 다른 누군가에게 넘어갈 수도 있다. 전자정부는 네트워크의 효율성과 판옵티콘(panopticon)[2]의 경계에 서있다. 전자정부가 어떤 정책적 전망을 갖느냐에 따라 조지오웰적 의미의 빅브라더 정부의 가능성 여부가 결정된다고 할 수 있다. 어떤 방향으로든 기회구조는 열려있다. 어떤 정책적 방향으로 선회하느냐에 따라 조지오웰의 빅브라더로서의 전자정부가 될 기회구조가 훨씬 높아졌다는 것이다.

많은 경우 전자정부의 부정적 측면은 정보기술적 제한과 한계의 한축과 정보시스

2) 판옵티콘이란 제레미 벤담이 공개한 감옥의 설계도를 말하는데, 이 감옥의 특징은 한 가운데 위치한 감시탑을 원형으로 둘러싸고 있는 투명한 유리벽으로 된 방에 죄수를 가두는 형태이다. 이 감옥은 감시자만 죄수를 볼 수 있고 죄수는 감시자를 볼 수 없는 독특한 구조를 갖고 있다. 이후 푸코(Foucault)가 정보사회의 권력의 불균등현상을 원형감옥이라고 부르면서 널리 인용되기 시작했다. 결국 이는 정보권력이 일방에 집중되어 모든 사람이 통제되는 상황을 의미한다.

템을 운영하는 유지관리 측면, 사람들의 인식 측면 등에서 발생할 수 있다. 역설적이게도 기술적 한계는 오히려 제한적이라는 것이 지금까지의 연구에서 보여주기도 한다. 문제는 사람이다.

따라서 앞으로 정보기술환경의 변화에서 제도적, 정책적이고 조직관리적 차원에서 접근하는 정보보호의 문제가 핵심쟁점으로 떠오르게 될 것이다. 다시 말하면 정보기술의 확산과 시스템 통합에 따른 정보의 집적과 접근허용성의 증대는 프라이버시 침해의 가능성을 높이며, 따라서 정보보안과 개인정보보호 문제가 전자정부 추진에서의 주요 쟁점으로 등장하게 된다는 것이다. 최근 유비쿼터스 기술변화를 논하는 전문가들은 앞으로 개인정보보호를 포함해 프라이버시 보호가 가장 주요 쟁점이 될 것이라는데 의견을 모으고 있다. 전자정부의 개인정보보호와 정보보안의 문제는 전자정부 추진과정에서 나타날 수 있는 제도적(법·제도), 인식적(사회적 인식·윤리·문화), 기술적 문제의 복합체로 인식해야 한다.

본 연구는 이러한 정보화환경의 동태적 변화를 고려하여 서울시 전자정부에서 개인정보보호에 관한 관리정책 입안과 가이드라인 수립의 필요성에서 출발했다고 볼 수 있다. 이미 우리사회가 힘들게 경험한 것이지만 교육행정정보시스템 구축과 관련한 일련의 논쟁은 정보시스템의 효율성 측면과 개인정보보호와 정보보안에 관한 사회제도적 합의절차의 부재로 인한 대립이 얼마나 첨예할 수 있는가를 잘 보여주었다.

전자정부를 정체된 개념으로 파악하여 과거 경험에 비추어 특정 정책을 입안하고 이에 대한 사전적 보호조치만으로는 변화하는 환경이 야기할 다양한 문제들에 대해 적절한 해결책을 찾지 못할 것이다. 전자정부는 정체된 개념이 아닌 지속적으로 변화 발전하는 동태적 개념이다. 이를 고려하여 정보화에 따른 불확실성을 제거하고 공공부문과 시민영역간의 신뢰형성 구조로서 정보보안, 개인정보보호에 관한 정책방향이 수립되어야 한다.

2. 연구의 목적

본 연구는 서울시 전자정부의 변화하는 환경에 따라 새롭게 부각되고 있는 개인정보보호에 관한 논의와 사례연구를 통해 서울시 전자정부 추진과정에서 발생할 수 있는 문제를 최소화하기 위한 정책대안을 마련하는 데 목적이 있다. 전자정부의 추진과정은 조직효율성과 생산성을 높이기 위한 측면과 이 과정에서 불가피하게 발생할 수밖에 없는 개인정보 집적에 따른 사회적 위험요소의 증대라는 양가적 측면이 공존하는 과정이다. 이러한 상충되는 가치가 서울시 전자정부 추진이라는 공공영역에서 어떻게 조정되어야 하며, 개인정보보호의 범위와 한계는 어디까지인지를 밝히는 것이 본 연구의 주요 목적이다.

정보화 사회의 위험요소는 아날로그 사회로서의 산업사회보다 훨씬 첨예하고 사회적 파장범위가 넓을 수 있다. 오늘날 인터넷의 사회적 영향력을 고려해본다면 이에 대한 예측이 가능할 것이다. 한편으로 이러한 위험요소에도 불구하고 공공부문의 정보화라는 전자정부를 통해 시민들은 많은 다양한 서비스를 경험하며 삶의 질이 나아질 기회구조가 많아지는 것 또한 분명한 사실이다. 정보화사회에 필연적으로 나타날 수밖에 없는 이러한 상충되는 측면이 전자정부 발전단계에 따라 어떻게 조정되고 현재 서울시 전자정부에서는 어떤 정책방향으로 나아가야 할지 등 개인정보보호에 관한 정책방향 수립의 가이드라인이 마련될 때, 서울시 전자정부는 훨씬 더 시민에게 다가갈 수 있을 것이다.

3. 연구의 내용

- 정보사회의 발전과 개인정보보호에 관한 이론적 논쟁
  - 정보사회의 효율성과 통제의 문제
  - 개인정보보호에 관한 인식과 제도의 문제

- 정보보호에 관한 논의
  - 정보보호에 관한 유형별 접근
  - 전자정부의 개인정보보호 위상과 접근방법
- 전자정부에서의 개인정보보호 사례와 쟁점
- 서울시 전자정부의 개인정보 현황 분석
  - 서울시 전자정부의 개인정보 현황 분석
  - 서울시 전자정부의 개인정보보호 법과 제도
  - 서울시 전자정부의 정보보안 현황
- 서울시 전자정부의 개인정보보호 관련 인식(시민인식과 공무원 인식 조사)
- 외국 전자정부의 개인정보보호를 위한 제도적 기제 분석
- 서울시 전자정부의 개인정보보호 정책방향과 추진전략

4. 연구의 방법

1) 자료와 문헌연구

정보사회에서의 개인정보가 갖는 의미를 정보사회를 둘러싼 논쟁적인 관점을 대비시키면서 검토해보고, 이를 통해 전자정부에서의 개인정보보호가 갖는 의미와 한계 등을 도출한다. 또한 전자정부에서의 개인정보보호의 문제는 정태적이고 불변적인 개념이 아니라 지속적 변화하는 동태적 개념으로 접근할 때에만 정책적 함의를 도출할 수 있다는 전제 하에, 정보사회의 사회적 위험을 관리하는 차원에서 개인정보보호 문제에 접근한 이론적 논의들을 살펴본다. 이를 근거로 전자정부라는 공공영역에서 추진하는 정보화의 효율성과 개인의 정보보호 문제가 어떻게 보호되고 조정되어야 하는지를 도출할 것이다.

2) 질문지 조사법과 인터뷰

(1) 질문지 조사법 : 서울시민의 개인정보보호에 관한 인식 조사

전자정부에서의 개인정보보호의 문제는 기술적, 제도적, 인식적 문제를 모두 포괄하는 통합적 문제이다. 특히 인식적 문제는 개인정보보호 관련 정책 실행과 밀접한 관련성을 갖고 있다. 따라서 서울시민 500명을 대상으로 서울시민들이 느끼는 개인정보보호에 관한 정보허용범위, 보호되어야 할 정보유형, 공공부문에 대한 개인정보보호관련 신뢰정도 등에 관한 조사를 통해 전자정부 개인정보보호 관련 정책방향 도출의 기본자료로 이용한다.

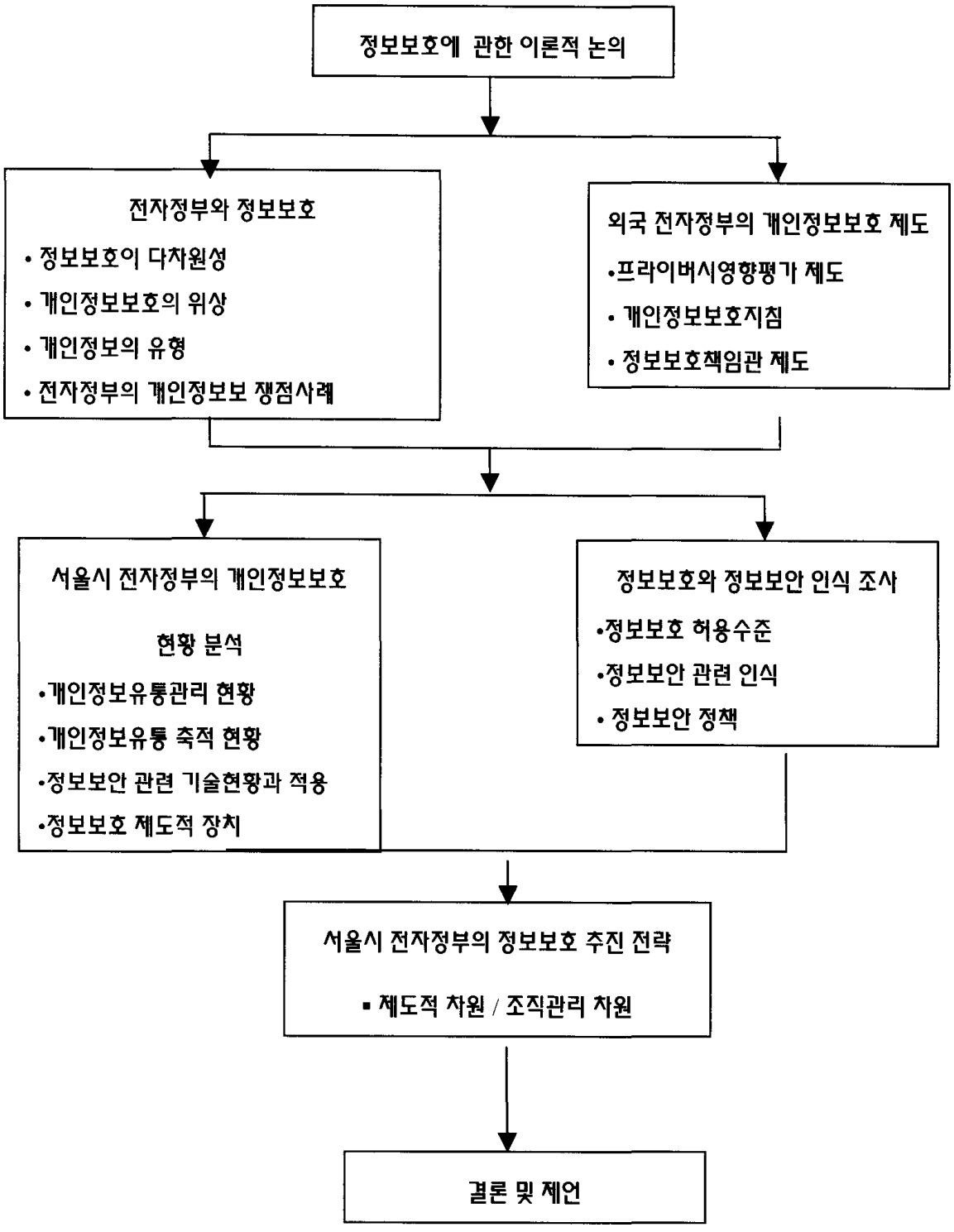
(2) 인터뷰(depth-interview) : 서울시 · 기초 자치단체 정보보호 담당자 대상

서울시 본청과 기초자치단체(구청)의 개인정보보호 담당자를 대상으로 정보보호 현황과 제도, 문제점과 애로점 등에 대한 인터뷰를 실시하여 전자정부의 개인정보보호를 위한 정책방안 도출의 기초자료를 확보하였다. 또한 현재 정보보호담당자들이 갖고 있는 개인정보보호에 대한 인식에 대해서는 조사를 실시하여 일반 시민이 느끼는 정보보호에 대한 인식과 비교해 보았다.

3) 서울시 개인정보 현황 조사

서울시 전자정부의 정보시스템에 포함되어 있는 개인정보 유형과 유통현황에 대한 조사를 시행하였으며, 이를 통해 개인에 대한 정보가 어디까지 유통되고 어디까지 보호되어야 할 것인지, 그리고 유통되는 정보라면 어떤 보호 기제를 동원해야 하는지에 대한 논의의 기초자료로 사용하였다.

5. 연구의 체계



<그림 1-1> 연구체계도

제2장 전자정부와 정보보호

1. 정보기술패러다임과 정보보호: 상충된 이해의 충돌

정보사회에 대한 많은 논의들은 정보기술이 가져온 편리성과 효율성의 증대, 그 결과 생산성의 향상으로 이어지는 일련의 과정들이 산업사회의 문제점을 해결하고 신경제 패러다임을 만들어 내면서 지식자본이 부가가치의 원천이 되는 사회구조적 변화에 강조점을 두고 있다. 이러한 맥락에서 정보기술의 긍정적인 역할이 강조되고, 산업사회의 생산력 향상의 원천으로서의 물적자본(phisical capital)이 정보사회에서는 지식자본(knowledge capital)으로 전화되는 정보적 생산양식으로의 변환(transformation)에 대한 논의로 이어지고 있다.

정보사회로의 이러한 변화는 일상생활을 전면적으로 바꾸고 있다. 인터넷으로 대별되는 일상생활의 혁명은 우리에게 유토피아적 이상사회를 꿈꾸게 한다. 최근 5년 사이에 일어난 변화를 그려보자. 네트워크 사회구조와 조직, 커뮤니케이션 방식의 변화, 닷컴기업의 출현과 엄청난 부의 증대 등은 정보사회의 유토피아적 담론이 얼마나 매혹적일 수 있는가를 증명하는 듯하다. 이러한 변화는 공공조직에서도 예외는 아닌바, 전자정부의 구현은 시민들의 일상생활의 편리성을 증대시키고 정부조직의 투명성을 제고하며 조직생산성을 증대로 나타났다.

그러나 우리가 이러한 정보화의 편리성 이면에는 여러 가지 위험이 도사리고 있다. 21세기의 시작을 알리는 2000년에 시작된 Y2K문제에서부터 이 모든 편리성을 한꺼번에 파괴할 수 있는 바이러스의 출현에 이르기까지 네트워크화된 세상은 우리가 상상하지 못할 정도의 위험을 도처에 파급시키고 있다.

사회변화는 언제나 일면적이며 선형적으로 일어나지 않는다. 모든 긍정적인 측면의 이면에는 그 긍정적인 측면을 상쇄할 만큼의 위험하고 부정적인 현상이 존재하고 있는 것이다. 이와 관련한 논쟁은 사실 정보사회의 출현 시기에서부터 계속되어 온 것이 사

실이다.

다니엘 벨(D Bell)에서 시작하는 후기자본주의 사회논쟁, 자본주의의 재구조화와 신경제론을 둘러싼 경제패러다임에 대한 논의들, 그리고 정보사회의 편익의 보편성과 제한성을 둘러싼 논쟁 등 정보사회로의 변화를 바라보는 사회과학자들의 상이한 관점의 이론적 논쟁은 정보사회 지지론자와 비판논자들을 중심으로 지속되었다. 이러한 정보사회를 둘러싼 논쟁에서 우리가 주목해야 할 점은 정보사회의 어떤 점이 긍정적으로 작용하며, 어떤 점이 부정적이며 위험을 야기할 요소인지를 파악하는 것이다. 울리히 벡(U Beck)의 위험사회론이나 기든스(A Giddens)의 현대성의 위험 등은 사회구조의 위험성에 대한 논의를 정보기술의 발전과 접목시켜 해석한 것으로 파악할 수 있다.

이와 같은 정보사회를 둘러싼 이론적 논쟁은 전자정부의 발전과정에도 동일하게 적용된다. 전자정부 관련 이론적 논의는 초기 단계의 전자정부의 오프라인 행정서비스의 온라인화를 목표로 정보시스템의 구축, 온라인 행정업무의 비율 증대 등 정보인프라 확충에 중점을 둔 단계를 거친 다음, 전자정부 발전단계를 보다 고도화하기 위한 전자정부의 활용성 제고에 대한 논의와 시민중심의 전자정부 서비스 방안에 대한 것으로 무게 중심이 이동한다. 이 과정은 정보접근성의 확장과 정보활용성의 증대로 요약할 수 있으며, 이러한 편익의 증대는 개인의 정보침해와 노출, 통제되지 않은 데이터베이스의 유통 등 정보보호와 관련된 광범위한 문제를 야기시킨다[3]. 전자정부의 정보서비스의 심화는 효율성의 증대임과 동시에 개인의 정보침해에 대한 위협요인이 될 수 있는 가능성을 확장시킨다.

전자정부의 공공적 특성은 개인에게 정부의 권리로서 강제할 수 있는 부분이 존재하기 때문이다[4]. 이러한 현황은 개인정보에 대한 위험이나 관리의 불확실성으로 파악할 수 있으며, 이는 경제학적 관점에서의 거래비용(transaction cost)의 증대를 의미한다. 즉, 전자정부의 편익을 누리기 위해 지불되어야 하는 비용으로서의 거래비용의 관점에서 접근한다면 정보보호에서의 위험관리차원의 정책적 관점이 필요하다. 다시 말하면 이는 정보사회에서 필연적으로 지불해야 할 사회적 비용이라는 것이다.

---

3) 기존 연구에 의하면 미국 연방정부와 주정부의 CIO를 대상으로 한 조사에 따르면, 전자정부의 진행과 함께 중요하게 대두할 정책분야로 전자상거래, 인터넷과 공공정보접근성, 정보시스템 보안 등이 지적되었다(한국정보보호센터, 2000).

4) 국세청의 정보는 개인의 동의여부와 상관없이 국가의 정보데이터베이스에 축적되어 있다.

개인정보보호나 정보보안에 대한 기술적 접근만으로는 오늘날 빈번하게 발생하는 문제에 완전히 대응하기에는 한계가 있다. 개인 정보의 오남용이나 정보보안시스템의 문제점은 기술적 취약성 뿐 아니라 정보를 관리하는 조직적 차원의 비기술적 요인에 의해 발생되는 경우가 많다는 점을 고려한다면, 개인정보보호에 대한 법제도적 차원과 조직관리 차원의 문제의 중요성이 더욱 강조된다고 하겠다. 따라서 전자정부의 개인정보보호를 포함한 정보보안의 문제는 하드웨어, 소프트웨어, 오르가웨어(orgaware)[5] 등의 세 차원을 동시에 고려하는 통합적 관점에서의 접근이 필요하다.

2. 정보보호의 다차원성과 개인정보 분류

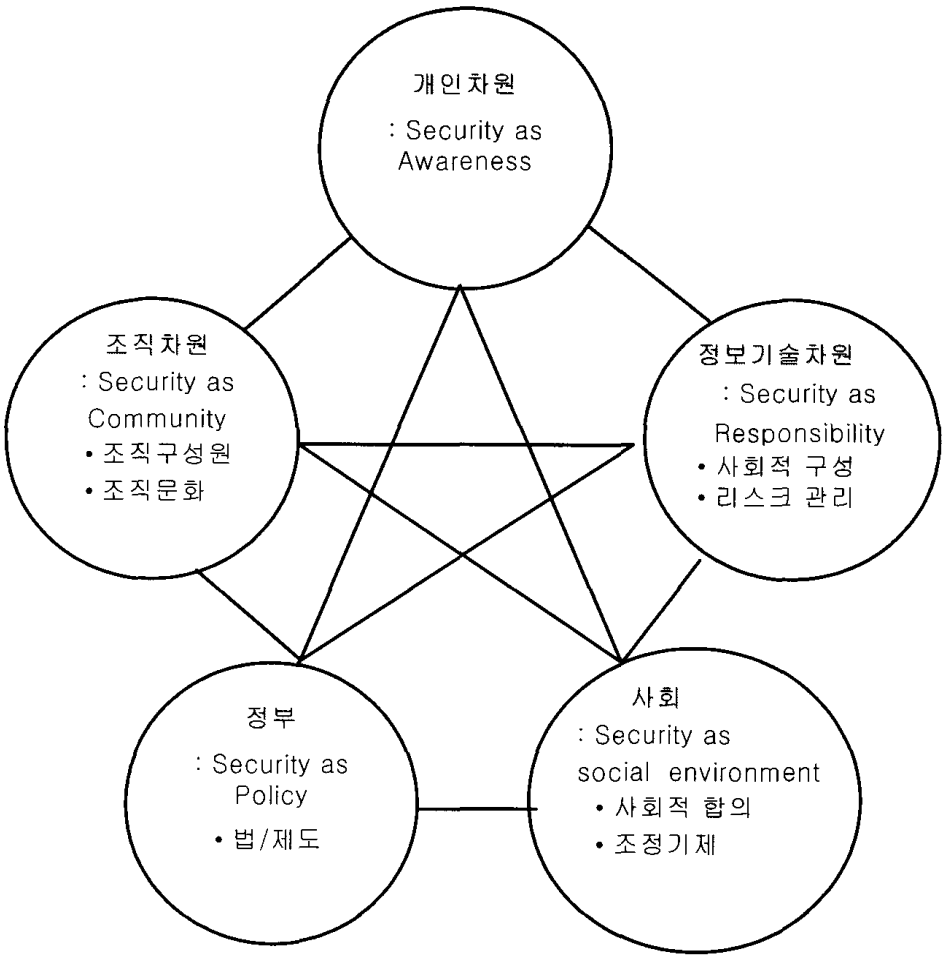
1) 정보보호의 다차원성

개인정보보호를 포함하여 정보보호에 관한 논의는 일면적이라기보다는 다면적으로 전개되는 것을 알 수 있다. 이미 앞에서 지적한 것처럼 정보보호에 관한 논의는 기술적 차원, 법제도적 차원, 조직 관리적 차원에서 접근할 수 있는데 여기서는 이러한 관점을 정보보호와 관련한 행위주체 차원에서 파악할 수 있음을 보여주고자 한다. 이러한 관점이 갖는 장점은 이후 서울시 전자정부의 개인정보보호 추진전략을 마련할 때 각 영역에서 어떤 역할을 담당할 지에 대한 그림을 그리는데 유용하다고 할 수 있다.

정보보호와 관련한 다차원성은 개인, 조직, 기술, 정책, 사회영역으로 나눠 파악할 수 있다(<그림 2-1> 참조).

---

5) 하드웨어와 소프트웨어의 상대적인 의미로 사용되는 개념으로 인간, 제도, 의사결정과정, 교육 등 조직의 정보시스템을 운영하고 관리하는데 필요한 인적·조직적 요소를 지칭하는 의미로 사용된다(Andersen, 1991)



<그림 2-1> 정보보안의 다차원성

개인차원의 영역은 주로 정보보호에 대한 인식의 문제로 접근가능한데, 한 사회에서의 정보보호나 정보허용 범위에 대한 것은 사회적 인식에 따른 합의의 문제이기 때문이다. 조직차원의 영역은 조직구성원이 갖고 있는 인식이나 조직이 형성하고 있는 조직문화를 의미한다. 이를 공공부문 조직에 적용시켜 본다면 정부조직에서 공무원이 갖는 정보보호 인식 정도와 조직 내부에서 정보보호의 중요성을 공유하는 문화 등이 정보보호 정책입안이나 정보유통이나 관리방식과 상관관계가 높다는 것이다. 다음으로 정보기술 차원은 말 그대로 정보보안 기술이 어떻게 사회적으로 구성되거나 적용되어

리스크 관리를 할 수 있는지 하는 차원에서 접근하는 것이다. 이 영역은 정보보호를 위한 출발점이자 핵심요소라고 할 수 있다. 다만 이 영역만이 모든 정보보호의 문제를 해결해준다는 기술중심적 접근은 한계가 있으며, 다른 영역에서의 접근과 함께 이뤄질 때 기술보안적 효과가 완전하게 나타날 것이다.

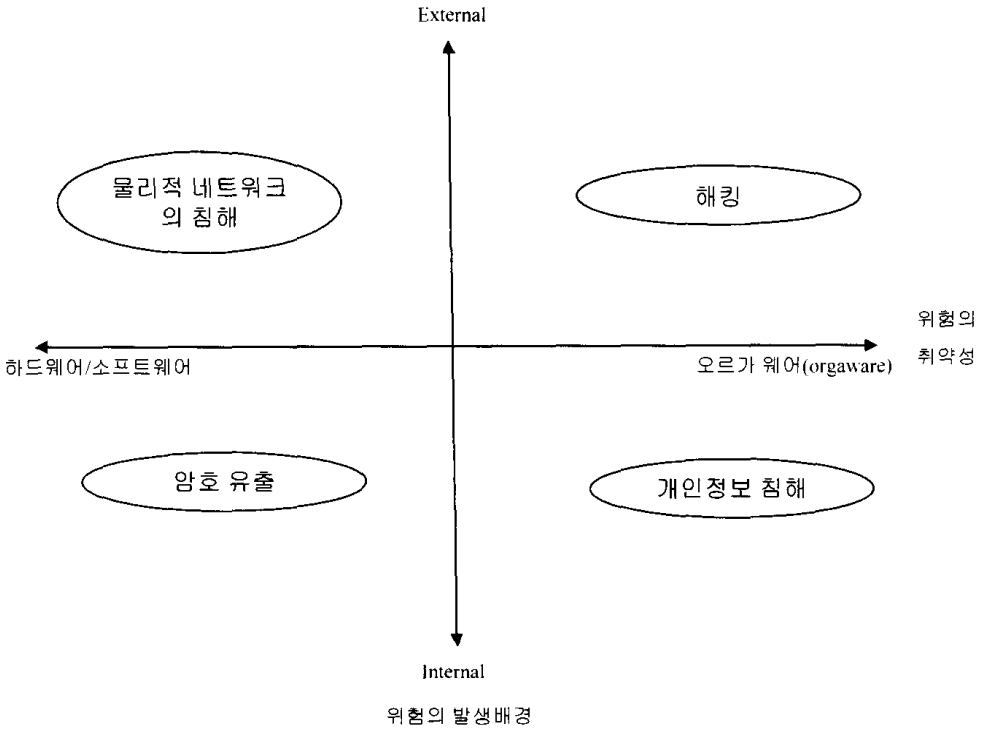
정부영역의 정보보안 접근은 주로 법제도 부문에서 나타날 수 있다. OECD(2003)가 전자정부의 장애요인으로 들고 있는 첫 번째 항목이 법·제도적 요인임을 고려한다면 특히 전자정부의 동태성을 고려한 법·제도적 측면의 정보보호에 대한 접근은 중요요소이다. 우리가 이후 논의할 것이지만 서울시 전자정부 역시 전자정부 발전단계에 조응하는 정보보호를 위한 법·제도적 대안의 제시 역시 이 측면을 고려한 것이다. 마지막으로 사회적 측면에서 정보보호 문제에 접근하는 것이다. 이는 일종의 사회적 합의에 도달하기 위한 조정기제를 의미하는 것인바, 오늘날 행정영역에서 논의되는 거버넌스 체제의 구축이라는 관점에서 접근하는 것이다. 거버넌스란 정부영역과 시민영역의 상호참여에 의한 민주적 조정기제를 의미한다. 따라서 정보보호를 개인의 인식, 조직문화 등이 반영된 사회적 구성물로 파악하는 관점은 정보보호를 위한 정책적 접근에서 중요한 측면이다.

이처럼 개인정보보호를 포괄하는 정보보호는 각 행위주체들의 관점을 포괄하는 전체적 관점에서 접근하여 각 영역에서 나타날 문제점을 파악할 때에만 현실적인 정책방향이 도출될 수 있다.

2) 정보보안 유형과 개인정보보호의 위상

우리는 앞에서 정보보호는 다차원적으로 접근해야 함을 설명하였다. 여기서는 이러한 정보보호를 위한 정보보안의 여러 유형들을 살펴보고 개인정보보호가 전체 정보보안에서 차지하는 위치에 대해 살펴보고자 한다. <그림 2-2>는 위험의 발생배경(Locus of Threat)이라는 한축과 위험의 취약점(Focus of Vulnerability)이라는 또 다른 축을 기준으로 정보보안 유형을 구분한 것이다. 가로축은 위험의 취액점이 하드웨어나 소프트웨어에서 나오는 것인지 아니면 오르가웨어(각주 5 참조) 쪽에서 나오는지를 기준으

로 구분한 것이며, 세로축은 위험의 발생배경이 외부적이냐 혹은 내부적이냐를 기준으로 구분한 것이다. 이러한 구분법에 의하면 개인정보보호 영역을 침해하는 정보보안의 경우는 오르가웨어와 내부적 요인이 결합되어 발생되는 경우가 빈번한 것으로 알려져 있다. 더욱이 하드웨어나 소프트웨어 측면에서 발생하는 위험의 취약점보다 오르가웨어 쪽에서 발생하는 위험의 취약성은 통제할 수 있는 정도가 어려운 것으로 알려져 있다



<그림 2-2> 정보보안에서의 개인정보보호의 위상

각 영역을 보면 하드웨어나 소프트웨어 측면의 외부적 요인에 의해 발생하는 대표적 경우가 물리적으로 네트워크에 침입하는 것으로 이에 대한 방어기제는 방화벽(firewall)의 구축 등이 해결책으로 제시되며, 하드웨어나 소프트웨어 측면이지만 내부적 배경에서 발생할 가능성이 큰 정보보안 유형은 암호유출 등으로 이는 PKI를 현실화한다던지 하는 해결책을 찾을 수 있다. 한편, 개인정보침해의 경우는 위험의 취약점은 오르가웨어 측면이며, 발생배경은 내부적이라는 점을 고려하면 개인의 인식이나 조

직원의 정보문화를 바꿔내는 것이 중요하다는 지적이다. 물론 각 영역에서 발생하는 정보보안의 문제가 이 기준만으로 설명하기에는 제한점을 가진다. 여기서 강조하는 것은 각 정보보안 유형별 위상의 차이가 있으므로 이를 고려한 보안대책이 필요하다는 점이다.

3) 개인정보의 유형분류

개인정보의 분류는 분류된 개인정보에 대한 취급과 연관되고 궁극적으로는 개인정보의 취급과 이를 다루는 제도의 내용에 큰 영향을 미치게 된다. 즉, 관리주체별 분류에 따라서 그 관리주체에 대한 의무부과 및 정보주체의 관리주체에 대한 권리부여 정도가 달라질 수 있으며 민감성의 정도에 따라서 절대 취급불가 개인정보 또는 상대적 취급 가능 개인정보 등 규제 대상이 달라질 수 있는 등 어느 분류에 의하는가에 따라 법적·제도적 성격이나 평가가 될 수 있다.

개인정보의 분류체계는 연구자에 따라 다양한 형태로 논의되고 있으며 아직 보편화된 체계는 정립되지 않은 상태이다. 다만 최근 개인정보보호에 관한 논의가 활발하개 이뤄지면서 관리주체별 분류, 성격별 분류 및 내용별 분류 등의 기준으로 체계화되기 시작한 것으로 보인다(황인호, 2001).

관리주체별 분류에서는 개인정보는 크게 공공개인정보와 민간개인정보로 나뉜다. 공공개인정보를 공공기록, 정보주체로부터 직접 수집한 기록과 정보주체 이외의 자로부터 수집한 기록 등으로 구분하기도 한다. 공공개인정보는 수집단계에서부터 각종 법적 근거에 의하여야 하는 정보인데 비해 민간개인정보는 원칙적으로 당사간의 계약에 의하여 수집, 취급, 활용되는 정보이다.

개인정보의 성격에 따라 민감한 정보와 그렇지 않은 정보를 분류하기도 하고 인격적 정보와 재산적 정보를 구분하여 다루기도 한다(황인호, 2001). 대체로 인격적 정보적 정보 중에서 차별적 처우의 기준이 되는 정보는 민감도가 높은 정보라고 할 수 있을 것이다. 서구의 경우처럼 다인종 및 다민족 국가에서는 인종이나 민족정보가 이러한 경우에 해당될 것이고 우리의 경우는 출신지역, 학력 등이 사례가 될 수 있을 것이다. 재산적 정보에서도 민감도가 높은 정보로는 신용불량기록이 이에 해당될 것이다.

이러한 내용들은 모두 개인에 대한 차별적 처우의 근거가 될 수 있을 것이므로 정당한 법적 근거에 의한 경우에만 개시될 수 있도록 하여야 하고 인격적 정보로서 민감도가 높은 정보는 원천적으로 수집이나 취급을 금지하도록 하는 규제도 가능할 것이다.

개인정보를 그 내용에 따라 분류하면서 구체화시킨 연구는 비교적 근간에 이루어진 일이다. Weible(1993)는 개인정보를 비교적 상세히 구분하면서 개인정보를 14개의 종류로 분류하고 그 상세한 내역을 예시로 밝히고 있다.

<표 2-1> Weible의 개인정보 분류표

분 류	예 시
일반정보	성명, 주민등록번호, 운전면허정보, 주소, 전화번호, 생년월일, 출생지, 본적지, 성별, 국적 등
가족정보	부모의 성명 및 직업, 배우자의 성명 및 직업, 부양가족의 성명, 가족구성원의 출생지 및 생년월일, 가족구성원의 주민등록번호 등
교육/훈련 정보	학생기록부, 학력, 학교성적, 기술자격증, 전문면허증, 서클활동, 상벌사항, 성격 및 행태 보고 등
병역정보	군번, 계급, 제대유형, 주특기, 근무부대 등
부동산정보	소유주택, 소유토지, 소유상점 및 건물 등
동산정보	자동차, 보유현금, 저축현황, 현금카드, 주식, 채권, 유가증권, 수집품, 고가의 예술품, 보석 등
소득정보	연봉, 이자소득, 임대소득, 기타 소득의 원천 등
기타 수익정보	보험가입현황, 보험 수익자, 회사의 판공비, 투자프로그램, 퇴직프로그램, 휴가, 병가 등
신용정보	대추상황, 저당권설정여부, 신용카드 연체 및 미납의 수담보설정여부 등
고용정보	고용형태, 고용주, 회사주소, 상관의 성명, 직무수행 평가기록, 훈련기록, 상벌기록 등
법적정보	전과기록, 교통위반기록, 파산 및 담보기록, 구속기록, 이혼기록, 납세기록 등
의료정보	본인 및 가족병력, 과거의 의료기록, 정신질환기록, 신체장애, 혈액형 등
조직정보	노조가입, 종교단체 가입, 정당가입, 클럽회원 등
습관취미 정보	흡연량, 음주량, 취미의 종류, 여가활동, 도박성향, 비디오 대여기록 등

한편, 행정자치부에서는 1998년 공공부문의 개인정보를 분류하면서 5개의 분류항목에 따라 정리한바 있다(행정자치부, 1998)[6].

6) 행정자치부로 통합되기 전의 총무처에서 분류함.

<표 2-2> 개인정보 분류표

분 류	예 시
내면의 비밀	사상, 신조, 종교, 가치관, 양심 등
심신의 상태	체력, 건강상태, 신체적 특징, 병력 등
사회경력	학력, 범죄경력, 직업, 자격, 소속정당 및 단체 등
경제관계	재산상황, 소득, 채권채무관계
생활·가정·신분 관계	성명, 주소, 본적, 가족관계, 출생지, 본관 등

한편 2002년 영국의 정보위원회 사무국[7]에서도 정보보호법(Data Protection Act of 1998)의 실행을 위하여 발간한 개인정보 안내지침서에서 개인정보를 14개의 분류항목으로 정리하였다.

<표 2-3> 영국 정보위원회의 개인정보 분류표

분 류	예 시
개인속성	성명, 주소, 연락처, 연령, 성별, 생일, 신체적 특징, 공공개인식별번호 등
가족, 사회 환경	혼인관계, 동거관계, 이혼경력, 가족속성, 세대원 정보, 취미, 주거환경, 여행 및 레저활동, 사회단체 봉사 및 기부활동 등
교육·훈련	학력, 자격, 기능, 직업훈련 기록, 전문성 강화 실습기록, 학생기록부 등
고용·근로	경력, 취업 상세정보, 근무평정기록, 보건기록, 직장내 훈련기록, 사회보장 기록 등
금융·신용	소득 및 수입, 자산 및 투자평가정보, 지출정보, 신용평가기록, 부채, 수익, 보험정보, 연금정보 등
계약활동	제공받는 재화 및 용역에 관한 정보, 법적 이용권 확보에 관한 정보, 계약상의 합의나 계약에 관한 정보 등
민감정보	인종 및 민족 정보, 정치적 견해, 종교정보, 노조가입정보, 신체·정신적 건강상태, 성생활 정보, 행정처분기록, 범죄·수사기록 등

2004년 정부혁신지방분권위원회에서는 개인정보관리 현황조사를 실시하면서 조사표에 의한 분류를 시도하였다. 이 위원회에서는 영국 정보위원회의 분류체계를 대체로 따르고 있으면서 한국의 실정에 맞게 분류체계를 보다 포괄적으로 묶었다(<표 204> 참조). 여기서는 속성정보를 기본정보로 하고, 활동정보와 민감정보로 개인정보를 분류

7) Information Commissioner's Office.

하고 있는데, 활동정보나 민감정보는 속성정보에 비해 개인의 사생활과 더욱 밀접한 관련이 있는 영역이다.

<표 2-4> 정부혁신지방분권위원회의 개인정보 분류표

분 류		예 시
속성정보		이름, 성별, 나이, 생년월일, 주민등록번호, 주소, 전화번호, 이메일주소, 혈액형, 신장, 체중, 사진, 지문, 장애, 기타 개인을 타인으로부터 식별하고 특성을 규정하는 정보
활동정보	가족·출신·생활환경	결혼·이혼 경력, 가족관계, 습관, 주거, 여행, 레저활동, 자선단체 가입 등
	학력·교육	학력, 출신학교, 성적, 학교생활, 기능, 자격 등
	고용·경력	취업, 사업경력, 구직·채용, 인사, 근무평정기록 등
	재산·신용·납세	수입, 임금, 투자, 지출, 채무, 보험, 연금, 납세사실 등
	사회보장·행정서비스	정부로부터의 급부, 급여, 면허·특허·인가, 행정계약 등
	기타	기타 개인의 일상생활과 관련된 정보
민감정보		인종·민족, 국적, 정치적 성향, 노조·사회단체활동, 보건·의료 기록, 성생활, 행정처분사실, 전과·수형사실, 병역사항, 기타 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보

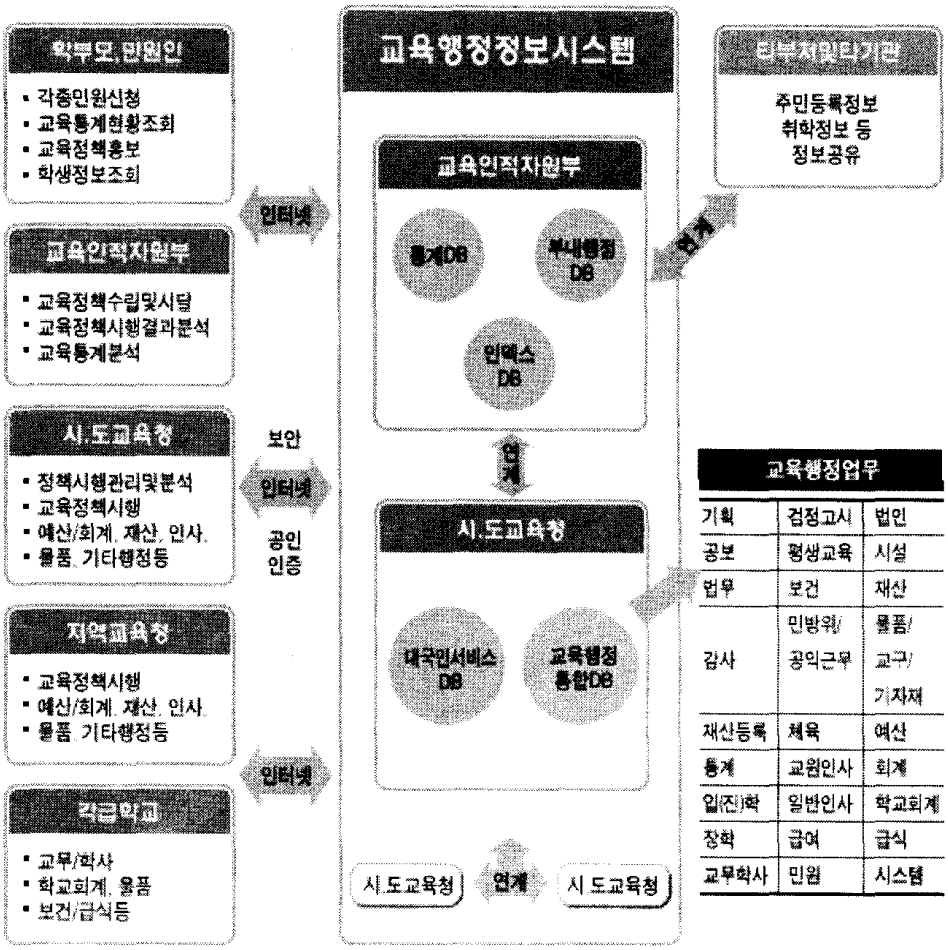
3. 전자정부와 개인정보보호 쟁점 사례

1) 교육행정정보시스템(NEIS) 사례

NEIS는 National Education Information System의 약자로, "교육행정정보시스템"을 지칭한다. 교육행정정보시스템(NEIS)은 기존에 학교 단위로 구축되어 있었던 정보시스템을 개편하여, 교육인적자원부, 교육청 등 모든 교육행정기관과 초·중등학교를 인터넷으로 연결하여 교육행정 업무를 전적으로 연계·처리할 수 있도록 구축한 시스템이다(김창환, 2002). NEIS의 추진배경은 기존 시스템을 개선할 필요성이 제기되었기 때문이다. 학교 안에 있는 서버를 관리하기 어려운 문제점과 이에 따른 해킹의 위험, 교사들의 과중한 업무부담, 업무 내용에 대한 표준화가 이루어지지 않음으로써 업무의 효율성이 떨어지는 문제점이 제기되었는데 정보통신기술의 발전으로 인하여 교육행정의 효율성을 높일 수 있는 방안 마련이 가능해짐에 따라 새로운 시스템의 구축이 요구되었다. 또한 초고속통신망설치와 인터넷 이용률의 세계 최고의 위치에 있고, IT산업은 급성장을 하고 있다. 이런 추세에서 교육행정의 생산성과 투명성을 높이기 위해서는 통합적이고 체계적인 교육정보시스템의 도입이 필요하다는 인식을 바탕으로, 2001년 초에 출범한 '전자정부 특별위원회'가 본 사업을 11대 중점 과제의 하나로 선정하여 2001년 5월 17일 본격 추진하게 되었다.

NEIS 사업의 목표는, 첫째, 교원의 업무경감 및 교육활동 전념을 통한 교육의 질 향상이다. 교원의 통계작성 등 단순 반복적인 행정업무를 전산처리하고, 복잡 다양한 업무를 표준화하여 일상적인 잡무를 줄이는 것이다. 둘째, 인터넷을 통한 학부모와의 정보공유로 가정과 학교의 만남의 활성화이다. 인증보안이 적용된 인터넷을 이용하여 자녀의 성장 관련 자료를 안방에서 온라인으로 열람할 수 있어, 자녀의 학교생활 문제점을 조기 발견, 상담을 통해 문제를 해결하는 것이다. 셋째, 서비스의 획기적 개선을 통한 대국민 만족도 제고이다. 연간 800만 건에 달하는 졸업증명서 등 제증명 발급 온라인 민원서비스를 전국 어디서나(우편, 근처의 학교, 교육청 등에서 발급) 신청하여 서비스를 받는 것이다. 넷째, 디지털 행정을 통한 교육행정의 생산성 향상이다. 온라인으로 정확한 자료를 기반으로 한 정책결정이 가능해지고, 인터넷을 통해 교육을 제공하는 것이다.

<그림 2-4> NEIS 관리체제



※ 출처: 정환규. 2003. "교육행정정보시스템(NEIS)의 쟁점과 과제," p. 5에서 재인용.

하지만 NEIS에서는 두 가지 문제점이 대두되었다. 첫째, 정보의 과다집중이다. 기존의 CS에서 집적되었던 학적관리, 학생생활기록부 등의 내용이 NEIS로 옮겨짐에 따라 교무수첩, 학생면담, 건강기록 등 개인의 신상과 관련한 많은 정보를 포괄하게 되었다. 둘째, 운영시스템의 적용성 제한이다. CS에서 메뉴의 사용범위를 학교차원에서 실정에 맞게 축소·운영하였으나 NEIS에서는 이러한 융통성이 제공되지 못한다고 느끼는데 있다.

<표 2-6> 교육행정정보시스템(NEIS) 27개 개발영역

단위업무	세 부 내 용
기획	주요 업무, 기관 평가
공보	보도자료 관리
법무	법률정보, 판례정보, 법령 질의 해석
감사	감사계획 및 결과, 감사현황 분석, 감사자료 공유, 사이버 감사
재산등록	재산등록 대상 및 내역관리, 재산신고
교육통계	학교 현황, 학생 현황, 교원 현황, 시설 현황, 주요 업무통계 등
입(진)학	초등학교 취학, 중학교 입학, 고등학교 입학 등
장학	교육과정, 연구학교, 장학정보, 학생행사관리, 연구대회 등
교무/학사	학교교육과정, **학적, 성적, 학생생활기록부, 학생생활, 교과용도서**
검정고시	원서접수, 성적처리, 고사장 관리, 합격처리 및 각종 통계 산출
평생교육	평생교육 시설 및 교육프로그램 관리, 학원 및 교습소 관리
보건	학교보건실 관리, 학교환경관리, **건강기록부 및 보건 통계**
체육	학교체육시설관리, 운동부 및 선수관리, 각종 현황 및 통계관리
교원인사	정·현원, 임용시험, 인사기록, 임용발령, 호봉, 전보, 평정, 승진, 연수, 상훈 및 징계, 복무, 기간제 교사, 전문직 임용, 자격검정관리
일반직 인사	정·현원, 임용시험, 인사기록, 임용발령, 호봉, 전보, 평정, 승진, 연수, 상훈 및 징계, 복무
급여	월급여, 연봉제, 명절휴가비, 연가보상비, 성과상여금, 연말정산, 기여금, 건강보험, 국민연금, 고용보험
민원	제증명, 유기한 민원, 진정/건의/질의, 정보공개, 현황통계 등
비상계획	민방위 편성, 민방위 해제, 민방위 교육훈련, 공익근무요원 편성, 공익근무요원 관리
법인	법인정보, 예·결산, 법인 대장
시설	시설사업관리, 학교시설승인, 학교시설사용승인, 시설유지관리, 시설현황, 수용계획
재산	공유재산관리계획, 재산대장관리, 사용허가. 대부관리, 폐교재산활용 관리
물품/교구/기자재	**취득/운용관리, 재물조사, 수급계획, 교구기준안 관리, 교구현황관리, 실험실습 재료관리, 기자재 기준안 관리, 기자재 현황관리, 기자재 통계**
예산	**예산편성, 예산배정, 예산이월, 예산운용, 예산통계**
회계	**세입, 세출, 세입·세출외 현금, 계약/압류, 결산, 자금**
학교회계	**예산, 세입, 세출, 결산, 세입·세출외 현금, 세무관리, 발전기금**
급식	학교급식통계, 급식관리, 급식 외 관리, 급식 분석
시스템	코드관리, 시스템연계, 보안, 사용자 인증 및 권한관리, 로그관리, 인터페이스관리, 배치작업 관리, 업무처리 승인 관리

※ 주: 굵은 글씨는 CS에서 처리되었던 업무를 표시한 것임.

※ 자료: 전자정부특별위원회, 『전자정부 백서』, 2003.

NEIS와 관련해 논쟁을 불러일으킨 주요 내용으로는 개인정보침해, 일방적인 추진 과정, 행정효율성 우선의 추진, 법적 근거 미비, 교원통제 문제, 교원잡무증가 등의 쟁점이 있었다. 여기에서 개인정보수집 내용에 대한 것을 중심으로 문제의 소지를 살펴보도록 하겠다.

미약한 개인정보보호와 법적 근거 미비

전교조 등 교육·시민단체가 2003년 2월 19일 국가인권위에 NEIS의 개인정보보호 문제에 대한 진정서를 제출하였다. 국가인권위에서는 학생지도 등에 필요한 학생 및 부모에 관한 정보를 16개 시도교육청 통합DB에 집적 관리하도록 함에 따른 기본권 제한의 발생여부, 그 발생시 헌법 상의 기본권 제한의 원칙에 따른 법적 근거 여부, 법적 근거가 있을 경우에라도 목적의 명확성, 피해의 최소성, 법익의 균형성, 수단의 적정성, 방법의 적절성 등 세 가지 관점에서 진정서를 검토하면서 사생활의 비밀과 자유 침해 여부에 대해 헌법 제10조, 제17조, 제37조제2항의 근거에 따라 개인정보의 수집은 적법한 권한이 있는 기관에서 하되 침해우려가 있는 경우 수집해서는 안된다는 의견을 제시하였다. 2003년 5월 인권위는 NEIS의 전반적인 개인정보침해를 제기하면서, 특히 학생의 사생활 비밀침해 등 인권침해 소지가 많은 교무/학사, 입(진)학 및 보건 영역은 NEIS 입력 대상에서의 제외할 것을 권고하는 결정을 내렸다.

NEIS에서 제외한 3개 영역은 종전의 CS방식으로 하되 개인정보의 누출로 인한 사생활 비밀침해 등 인권침해가 없도록 CS에 대한 보안체계 강화조치 강구를 권고한 것이다. 이에 교육부는 3개 항목의 세부 입력사항 358개 중 66%인 236개 항목을 삭제했다고 발표하였다. 이러한 인권위의 결정은 NEIS와 CS의 병행권고에 따라 NEIS와 CS의 장단점에 대한 때늦은 논란을 야기하였다.

<표 2-8> 양 시스템간의 반대 논리

CS 옹호측	NEIS 옹호측
NEIS 서비스 내용에 대한 홍보 미흡	CS의 보안성 취약
서비스 실시 이전 짧은 시범기간	NEIS로의 정보이관이 97% 이미 진행
NEIS 내에 너무 많은 개인 신상정보 등이 입력대상이 됨	CS체제에서는 정보담당교사에게만 업무가 과도하게 집중됨
16개 시도교육청 서버로 통합 운영하는데 따른 정보유출 우려 ⇒ 정보유출에 따른 인권 침해	각 학교 CS별로 방화벽을 설치하는데 막대한 재원 소요 ⇒ 정보집적에 따른 효율성

<표 2-9> NEIS와 CS의 보안성 비교

NEIS	보안항목	CS
공개키 기반 구조(PKI) 인증 솔루션	인증	ID와 비밀번호
통합인증권한관리(EAM)	권한관리	×
방화벽, IDS, 서버보안 솔루션	접근통제	방화벽
인증 및 데이터 암호	암호화	간단한 인증 암호화
보안 로그 관리 기능	감시/모니터링	×

NEIS 사례의 검토를 위해 전자정부 추진방식과 개인정보보호 차원에서 문제를 제기할 수 있다. 즉, 추진과정의 주요 의사결정단계에서는 이해관계자들의 의견을 다양하게 반영하고 참여할 수 있는 사회적 합의과정을 거쳐야 한다는 것이다. NEIS의 경우 교육현장의 교사, 교육행정전문가, 교원단체의 의견을 충분히 수렴하였다고 하지만 여러 가지 사항을 고려하여 사업이 추진되지 못하여 시민사회단체들의 반발에 부딪치는 등 나름대로 사업 후 일부난관을 겪게 되었다(전자정부 백서, 2003). 즉 제 교육주체의 합의를 통한 의사결정이 필요하다. 더 근본적인 문제는 NEIS에 입력되는 학생들의 정보가 헌법이 보장하는 기본인권을 침해한다는 것이 문제이다. 강화된 보안체계하에 학생정보가 수집된다고 하더라도 정부업무의 효율성을 위해서 개인정보가 정보주체의 동의 없이 수집·집적될 수 있느냐 하는 점에서 정보인권 문제로까지 확대되었다(김보

경, 2003).

우리는 NEIS사례를 통해 전자정부 서비스 심화와 개인정보 간에 서로 갈등적 요소가 제기될 수 밖에 없음을 확인할 수 있다. 1980년 OECD 개인정보보호원칙, 1990년 UN의 개인정보전산화 가이드라인에서는 개인정보를 수집·이용할 때 반드시 정부주체에게 동의를 받아야 하고 동의를 받을 때는 그 정확한 수집과 이용목적으로 명시해야 한다는 등의 '자기정보통제권'을 천명했다. 이러한 원칙들은 개인정보의 수집이나 이용에 대한 결정권이 국가나 기업 등 개인정보를 수집해 가는 쪽에 있는 것이 아니라 그 개인정보의 주체, 즉 국민에게 있음을 보여준다.

이러한 개인정보보호는 국가 행정작용과 상쇄관계(trade-off)에 있는 경우가 많다. 국가가 대국민 서비스를 하거나 국가의 고유업무를 수행하기 위해서는 일정정도의 개인정보가 필요하며, 국가·기업·개인이 정치·문화·사회 전반에 걸친 제도나 행위들을 결정함에 있어 DB화된 개인정보를 활용하는 비중도 크게 증가하는 추세이다. 원활한 국가의 행정작용을 위해 개인정보가 어느 수준까지 요구되어야 하는지, 공공부문에서는 개인정보 제공에 대한 선택권이 부여될 수 없는 것인지, 공공서비스를 받는 국민의 당연한 의무라면 어디까지 제공해야 하는지 검토가 요구되며, 이 과정은 사회적 합의와 조정과정을 전제로 해야 한다는 점을 확인할 수 있다.

정보화가 급속히 이루어지고 전자정부 서비스가 시작되면서 개인정보에 대한 활용이 보다 많아지고 있다. 앞에서 논의한 NEIS의 문제는 단순한 경제나 기술의 차원의 문제가 아니라는 것이다. NEIS에서 대해 제기된 가장 강력한 비판, 즉 현재 학생생활기록부와 건강기록부에 담겨진 250여 가지의 방대한 개인정보들은 정부기관인 교육청 단위로 수집될 수 없는 개인의 사생활에 속하는 정보이다.

한편, 정부가 이와 같은 교육관련 개인정보를 수집하는 것이 인권침해라는 주장에 대하여 이와 비슷한 금융정보, 의료정보, 주민등록에 관한 정보 등은 국가에 의해 광범위하게 수집, 관리되고 있지만 인권침해라는 반발은 크지 않다. 따라서 문제는 정부에 의해 정보를 수집하는 것 자체가 문제가 아니라 사용자의 동의여부, 수집된 정보의 운영과 활용 등 관리적 차원에서 문제가 제기된다는 점을 인지해야 한다.

2) 강남구 CCTV 설치 사례

강남구는 각종 범죄 및 재난으로부터 시민의 생명과 재산을 보호하며 안전한 강남구를 만들기 위해 주택가 뒷골목 등에 방범용의 CCTV를 2002년 12월 논현동(CCTV 5개)에 설치를 시작으로 하여 강남구 전역에 230여 개를 설치하였다.강남구의 CCTV 설치는 개인의 인권침해의 문제에 대한 반대 의견이 있었지만, 다른 자치구나 지방정부에 비해 빈번히 발생하는 강남구의 강·절도 및 성범죄 등의 강력 범죄를 예방하고 적극 대처하기 위한 차원에서 사업이 추진하였다.

강남구의 CCTV 설치의 목표는 크게 두 가지로 나눌 수 있다. 먼저 각종 범죄로부터 시민의 보호. 타 자치구나 지방정부에 비해 소득수준과 생활수준이 높고 유동인구가 많아 각종 강력 범죄의 발생 빈도가 높다. '강남 떼강도'사건, 유괴사건, 성범죄가 타 지역에 비해 발생률이 높아 주민의 불안감이 높게 나타났다. 후미진 주택가나 인적이 드문 곳에서 발생하는 각종 범죄의 발생은 경찰력을 통한 방범활동 만으로 해결이 되지 못하고 있다. 이에 강남구는 경찰서와 협력하여 시민들의 설치 동의가 있는 지역을 대상으로 CCTV를 설치하여 범죄의 예방을 통해 시민들을 보호하고자 하였다.

둘째로, 자연재해와 테러, 화재 등과 같은 재해·재난의 예방·발생으로부터 시민의 생명과 재산의 보호이다. 자연재해뿐만 아니라 미국의 9·11테러나 대형화재는 많은 시민의 생명과 재산에 타격을 주고 있다. CCTV를 통해 이러한 재해·재난의 예방과 발생시 신속한 대처를 하여 피해를 최소화 하고자 하는 것이 CCTV 설치의 목표이다.

CCTV 확대 설치·운영 계획이 알려지자 각 언론에서 강남구의 방범용 CCTV에 대해 몰카 논란이 일어나면서, 찬·반 의견이 대립하였다. 찬·반의 의견 대립은 MBC 방송의 '100분 토론'의 주제가 되어 CCTV 설치·운영에 따른 시민의 보호와 인권침해에 대한 문제에 대한 논쟁이 있었다. 정보인권침해에 대한 비판이 많았지만 강남구와 각 언론사(연합뉴스, 한국일보, 한겨레 등)의 설문조사에서는 시민들이 CCTV 확대 설치·운영에 대해 찬성을 하였고, 서울시 경찰청의 치안 만족도 평가 결과에서 논현 1파출소가 최우수파출소로 선정되었고 전년도 동기간 대비 5대 범죄가 42.5% 감소한 것으로 나타나면서 CCTV 설치·운영에 대한 논란이 줄어들었다.

<표 2-11> 전년도 동기간 대비 5대 범죄 발생 비교

구분	계	살 인	강 도	강 간	절 도	폭 력
2002. 1~5(건)	40	-	6	1	29	4
2003. 1~5(%)	23	-	3	-	17	3
증 감(%)	-42.5	-	-50	-100	-47	25

반대여론이 줄어들고 범죄율 감소에 효과가 있다는 판단아래 2003년 7월 18일 뒷골목 CCTV 확대설치 계획방침을 추가경정예산에 반영했고, 7월 25일 주민공청회를 개최하여 설치에 대한 논란을 종식시키고 CCTV 설치·운영의 정당성을 높이려 했다. 또한 8월 11일 영국, 프랑스 등 CCTV를 설치 운영하고 있는 선진국의 사례견학을 하였고 8월 29일 '2003년 하반기 방범용 CCTV 설치(230대) 추진계획 방침'을 발표하였다.

강남구는 CCTV의 확대 설치·운영을 위해 10월 15일에 주민 준비위원회 구성[8], 16일 경찰청 소유 부지사용 승낙, 20일 주민 T/F팀 구성 및 전문설계업체 선정방법을 결정했다. 주민 T/F팀 구성은 준비위원(260명) 중 무작위 추첨으로 11명을 선정하였고 전문설계업체 선발방법 결정은 지명 경쟁 입찰방식으로 결정하였다. 2003년 12월 8일 강남구청과 강남경찰서는 CCTV 모니터를 분산 설치·운영보다는 한 곳에 종합상황실을 설치 통합운영으로 사건 발생 시 즉각 상황을 대처하고 인권 및 보안문제에 관리가용의 하다는데 의견을 같이하고 CCTV 관제센터 건립에 대해 협의하였다. 그 후 2004년 상반기까지 강남구는 범죄 취약지역에 320대의 CCTV를 설치할 계획이며, 관제시스템(종합상황실)을 통해 이를 운영·관리할 예정이다.

8) 주민 준비위원회의 구성은 각 동별 10명씩 학계 및 전문가, 주민 등 260명, 경찰자문위원 중 경찰서 추천 36명 등 총 296명으로 구성되었다.

<표 2-12> CCTV 설치 현황

동 명	설치수량	동 명	설치수량
신사동	17	도곡1동	10
논현1동	16	도곡2동	6
논현2동	17	대치1동	16
압구정1동	17	대치2동	7
압구정2동	16	대치3동	10
청담1동	16	대치4동	16
청담2동	16	역삼1동	33
삼성1동	17	역삼2동	16
삼성2동	16	개포4동	10

※ 논현1동, 역삼1동, 개포4동 등의 37개소는 현재 운영 중이고, 나머지는 설치 중

② 사업추진과정에서의 논란

강남구의 CCTV 설치·운영은 시민의 생명과 재산의 보호라는 긍정적 측면과 함께 개인의 정보인권침해라는 문제를 동시에 가지고 있다. 강남구의 CCTV 설치·운영 과정은 법·제도 미비, 설치·운영상의 문제에서 많은 논란의 여지를 가진다.

먼저 법·제도의 미비이다. 우리는 '공공기관의개인정보보호에관한법률'을 제외하고 개인정보보호에 관한 법적 토대를 가지고 있지 않고, 또한 개인정보보호를 담당하는 독립적인 감독기구 역시 없다. 이러한 법·제도적 기반에서 추진된 강남구의 CCTV는 아무런 법·제도적 뒷받침이 없어 논란의 여지를 제공한다. 지방정부 수준에서 마련할 수 있는 CCTV 설치·운영과 관련한 '조례'의 제정, '정보보호 가이드라인'은 만들어지지 않았다. 시민의 생명과 재산 보호라는 좋은 의도를 가지고 있다고 해도 개인의 정보인권이 침해될 수 있고 침해된 인권에 대한 법·제도적 보호가 불가능한 상태의 CCTV 설치·운영은 향후 문제발생의 잠재성을 갖고 있다. 강남구의 CCTV 프로젝트는 갈등의 주체가 행정조직과 시민단체, 언론 등으로 대별되면서 오히려 심각한 분쟁을 야기시키지 않았다. 다시 말하면 CCTV설치 지역의 직접적 이해당사자인 강남구민들이 논란의 과정에 적극적으로 개입하지 않았다는 것이다.

향후 CCTV 설치·운영이 순기능의 역할을 보다 잘 수행하기 위해서는 투명한 설치·운영 과정을 보여주어야 하고, 반대하는 개개인과 불특정 시민의 정보보호에 대한

정책적 배려가 되어야 한다. 어느 하나의 가치를 절대적으로 존중하기보다는 두 가지 가치 모두를 절충하여 범죄와 재난으로부터의 생명·재산 보호와 개인정보의 악용에 대한 보호가 함께 이루어져야 할 것이다. 절차적 정당성이 확보되지 않을 때는 언제나 문제가 발생할 잠재성을 앉고 있는 것이다.

3) 인터넷 실명제 사례

2003년 3월 정보통신부가 국내 인터넷 게시판에 실명제를 도입하겠다고 밝히면서 논란이 시작되었다. 실명제는 단순히 본인의 이름을 밝히고 글을 쓰는 제도가 아니라 개인정보 데이터베이스를 본인과 대조하여 신분이 확인된 사람만 글을 쓸 수 있게 하는 것이다. 정통부의 계획은 게시판이나 커뮤니티 운영자가 실명제 도입 여부를 결정하도록 하는 것이 아니라 일단 모든 정부기관 홈페이지에 의무적으로 실명제를 실시하고 향후 포털 사이트 등 민간에도 '여론수렴을 거쳐' 법제화하고 확대하겠다는 것이다. 즉, 건전한 국민정책 제안 및 의견 수렴 기능을 제고하기 위해 정부기관의 인터넷 게시판을 실명화 할 계획으로 공공기관 게시판 운용 가이드라인을 제정·보급하고, 관계부처와 협의를 거쳐 정부기관 인터넷 게시판 실명(확인)제를 실시할 계획이다.

또한 국회의 정치개혁특별위원회(이후 정개특위로 함)의 선거법 개정에서 논의 되었고 법안이 국회를 통과하면서 법적으로 추진이 되었다. 정개특위는 「공직선거및선거부정방지법」에 제82조 제6항을 신설하여 인터넷언론사 게시판·대화방의 실명확인 제도를 도입을 천명했다. 정보통신부는 실명제 게시판을 운용한 결과, 게시판 상에서의 명예훼손, 상업성 광고, 특정인에 의한 글 도배 등이 69%에서 2.1%로 대폭 감소되었고 게시판 이용자도 실명제 시행 전보다 30% 이상 증가하였다고 주장하면서 인터넷 실명제의 긍정적인 측면을 부각시키고자 하였다.

한편, 인터넷 실명제 실시와 관련하여 온라인 공간이 관련 논쟁으로 들끓었는데, 반대측의 주장은 첫째, 인터넷실명제가 실시되면 네트워크의 기술적 특성상 발신자와 수신자가 반드시 남기 때문에 네트워크에서 사람을 추적하고 정보를 수집하기가 용이해진다는 점, 둘째, 인터넷 실명제가 가능하려면 실명 데이터베이스가 하나 이상 구축되고 실명확인을 위한 상시적 대조시스템이 작동해야 하는데, 지금 구축된 그 어떠한 실

명 데이터베이스도 정보주체인 국민으로부터 실명확인용으로 이용하겠다고 동의를 받은 적이 없는 상태에서 사용되었기 때문에 개인의 자기정보통제권을 침해한다는 것이다.

이러한 논쟁은 현재에도 진행 중이다. 인터넷 게시판에서 프라이버시 침해가 우려되는 게시판의 경우 실명제를 도입해야 한다. 하지만 그 외의 게시판의 경우에는 익명성을 사용하여 표현의 자유를 보장하는 선택적 게시판 운영이 필요하다. 또한 학교교육과 전문기관의 정보화 교육을 통해 정보화 활용능력뿐만 아니라 인터넷 문화, 소양교육의 병행 실시해야 한다. 인터넷의 게시판에서의 프라이버시 보호의 필요성과 지나친 표현의 자유가 범죄행위라는 인식을 심어주는 지속적인 홍보가 필요하다.

제3장 서울시 전자정부의 개인정보 현황

1. 서울시 전자정부의 개인정보 유통관리 현황

서울시 전자정부에서의 개인정보 유통관리 현황은 자치구의 개인정보 실태조사를 통해 파악했다. 개인정보 유통관리현황을 ①개인정보보호 정책수립 및 지침준수, ②개인정보 파일의 수집 및 보관, ③개인정보 제공 및 열람·정정, ④개인정보 입출력자료, ⑤시스템 및 단말기 관리, ⑥시설보안, ⑦개인정보의 위탁처리 등의 부문으로 파악할 수 있으며, 본 연구에서는 4개 자치구(강남구, 강서구, 은평구, 중구)를 대상으로 개인저보 유통관리 현황을 파악하였다.

1) 개인정보보호 정책 수립 및 지침 준수여부

먼저 개인정보의 분실, 도난, 유출, 변조 또는 훼손 대책 등 개인정보의 보호·안전대책의 수립 여부, 개인정보보호에 관한 자체규정 및 지침의 제정·시행 여부, 개인정보보호 관련 업무담당자의 업무내용 및 의무의 숙지 등에 대한 기관자체의 개인정보보호계획의 수립 여부이다. 개인정보 유통의 핵심이 되는 부분으로서 각 자치구는 계획을 수립하여 시행 중이며, 강남구는 「강남구개인정보보호 방침」을 은평구는 「은평구개인정보보호규정」에 의거하여 계획을 수립하여 이에 따라 업무를 수행하고 있다.

더불어 개인정보보호 대상에 대한 인지와 규정된 안전대책에 따르고 있는 것으로 나타났다. 개인정보보호 정책의 수립과 지침의 준수 업무를 총괄하는 개인정보보호 책임관의 지정 및 적정여부에 대해 자치구는 지정을 하고 있었다. 강남구와 중구, 은평구는 전산정보과장, 강서구는 민원전산과장을 개인정보보호 책임관으로 지정하여 보다 전문적인 개인정보 유통 업무를 총괄하고 있다. 개인정보 화일의 보유현황·근거 및

보유목적, 열람 및 정정 청구 안내 등 웹사이트에서 유통되는 개인정보의 보호방침에 대한 규정은 모두 준수하고 있었으며, 개인정보 침해 신고처리대장의 비치 및 접수·처리결과와 관련된 장부를 비치하여 유통현황을 알 수 있게 하였다.

개인정보 유통에 관계하는 내부직원 및 산하기관, 산하투자기관 등에 대한 지도감독 및 교육실시가 함께 이루어져야 한다. 강남구, 강서구, 은평구는 개인정보보호에 관한 '행정자치부 지침'을 주요한 내용으로 한 교육을 실시하고 있었지만 중구의 경우 관련 교육을 실시하지 않았다. 교육주기를 보면 강서구가 년 1회 실시하고, 강남구와 은평구는 필요시에 교육을 하고 있다. 계획의 수립과 지침의 운영이 결국 사람에 의해 이루어지고 있고 개인정보 유통과 관련된 환경이 계속 변화고 있으므로 지속적인 교육이 필요하다.

2) 화일의 수집 및 보관

개인정보의 수집절차, 보유범위, 사용후 폐기, 백업자료의 관리, 개인정보의 열람에 해당되는 영역으로 관련 법령 또는 내부규정에 따라 적법하게 수집·보관이 이루어지고 있었다. 또한 4개 구청이 모두 개인정보의 보유범위, 수집된 개인정보의 이용목적 완료 후 폐기하고 있었다.

개인정보 백업자료의 관리는 은평구가 온라인과 오프라인으로 백업관리하고 있었고 강남구, 강서구, 중구는 온라인으로 관리하고 있다. 유통을 위해 수집·보관된 자료의 일반인 열람(개인정보화일대장)은 열람장소(민원 관련 부서)의 지정 및 고시를 통해 열람이 가능하였다.

3) 개인정보 제공 및 열람·정정

개인정보의 이용 및 타기관 제공의 적법성은 관련규정 검토 및 제공 항목·범위·절차 등을 고려하여 공공이용 근거에 따라 유통되고 있다. 다만 은평구의 경우 이에 대한 적법성 여부를 확인할 수 없었고, 강남구의 경우 개인정보를 서울시를 비롯한 관계기관에 유통하고 있다. 개인정보의 이용 및 타기관 제공과 관련된 개인정보의 경우 개인정보제공대장을 통한 기록, 유지관리를 하고 있다.

또한 열람장소 지정, 열람·정정과 관련해 미원봉사과(은평구), 민원전산실(강서구), 민원실(중구, 강남구)에 창구설치, 접수처리대장, 청구서를 비치하여 개인의 정보가 유통되는 과정을 한 눈에 볼 수 있게 하고 있었다. 이러한 처리정보에 대한 열람청구 및 결정 등의 절차는 규정에 의해 적법하게 이루어지고 있다.

4) 입출력자료

개인정보 유통과 관련해 이용목적이 완료된 개인정보의 입·출력자료에 대한 관리는 입·출력 자료의 폐기방법으로 은평구는 소각을 하고 있고, 강남구·강서구·중구는 파쇄 후 소각을 활용하고 있다. 입·출력관리대장의 기록과 관리실태는 양호한 것으로 조사되었고, 출력자료에 대한 출력일시·면수표시 및 출력장비의 고유번호 등의 자동기록이 이루어져 개인정보 유통 시 입·출력 관리가 잘 이루어지고 있음을 알 수 있었다. 하지만 입·출력 및 수정사항, 데이터 접근내역 등을 자동으로 기록하여 개인정보의 유통을 알 수 있는 로그 화일 생성은 강남구에서만 이루어지고 있었다.

5) 시스템 및 단말기 관리

개인정보 유통이 이루어지는 시스템의 운용을 담당하는 취급자가 지정되어 있었고 사용자는 ID 및 비밀번호를 사용하여 개인정보의 누출을 막고 있었다. 비밀번호의 변경은 은평구와 강남구는 담당자의 비밀번호를 주기적으로 하는데 비해, 강서구와 중구는 변경을 하지만 주기적이지 않고 필요시에 변경하고 있었다. 비밀번호 변경을 통한 개인정보의 누출방지 노력을 하고 비밀번호관리대장을 작성하여 임의적인 변경은 조사대상 자치구가 모두 막고 있었다. 시스템의 정보보호를 위한 기술적 장치로 통신보안장비와 방화벽 설치를 하고 있고 개인정보 화일의 명칭, 처리일시 및 사용자주체와 사용단말기가 컴퓨터에 자동으로 기록되는 시스템을 운용하고 있다.

6) 시설보안

개인정보 유통을 담당하는 전산실, 자료보관실은 보호구역(강남구는 통제구역으로 칭함)으로 설정하여 보안을 강화하고 있었고, 강남구와 중구의 경우 출입자 통제를 통

해 보호구역 내의 개인정보 유통을 관리하고 있었다.

7) 개인정보의 위탁처리

개인정보의 산하기관 또는 민간위탁은 아직 이루어지지 않고 있어 개인정보 유통을 위한 절차는 아직 없었다. 또한 개인정보 수탁자의 안전 확보는 은평구에서만 담당자 권한 하에서 이루어지고 있었고 나머지 자치구는 없었다.

이상의 내용을 요약적으로 보여주고 있는 것이 <표 3-2>이다.

<표 3-2 > 자치구 개인정보 유통관리 현황

분 야	점검 사항	조사결과			
		은평구	강서구	중구	강남구
개인정보보호 정책 수립 및 지침 준수여부	기관 자체의 개인정보보호계획의 수립여부	수립	수립	수립	수립
	개인정보보호 대상을 명확하게 인지여부: 온라인 및 오프라인 개인정보	인지	인지	인지	인지
	개인정보보호정책 적용기관 등 범위의 적절성: 소속기관 일괄적용 또는 소속기관 자체수립	적절	적절	적절	적절
	개인정보보호책임관 지정 여부	지정	지정	지정	지정
	개인정보 보호방침의 웹사이트 게재여부: 개인정보화일의 보유현황·근거 및 보유목적 등/ 열람 및 정정청구 안내 등	게재	게재	게재	게재
	개인정보침해신고처리대장의 비치 및 접수·처리결과 적정여부	적정	적정	적정	적정
	내부직원 및 산하기관, 산하투자기관 등에 대한 지도감독 및 교육실시 여부	실시	실시	-	실시
	개인정보 사무의 업무분장 및 위임전결규정, 자체감사규정의 개정·반영 여부	반영	반영	반영	반영
파일의 수집 및 보관	개인정보의 수집절차는 적법성 여부: 법령 또는 내부 규정 등	적법	적법	적법	적법
	개인정보의 보유범위는 적절성	적절	적절	적절	적절
	수집된 개인정보의 이용목적 완료 후 폐기	폐기	폐기	폐기	폐기
	백업자료의 관리	백업	백업	백업	백업
	일반인의 개인정보화일대장의 열람은 가능 여부	지정	지정	지정	지정
개인정보 제공 및 열람·청구	개인정보 이용 및 타기관 제공의 적법성 여부	-	적법	적법	적법
	공공이용의 근거 및 제공항목의 적정성	적정	적정	적정	적정
	개인정보제공대장의 기록 및 유지관리의 적정성	-	적정	적정	적정
	열람장소 지정 및 열람·정정 안내도 비치여부	비치	비치	비치	비치
	처리정보에 대한 열람청구·결정 등의 절차 타당성	타당	타당	타당	타당
입·출력 자료	개인정보 입·출력자료에 대한 관리대책" 폐기방법	소각	파쇄	파쇄	파쇄
	입출력관리대장의 기록·관리실태	적절	적절	적절	적절
	출력자료에 대한 출력일시·면수 표시 및 출력장비의 고유번호 등의 자동기록 여부	기록	기록	기록	기록
	입·출력 및 수정사항, 데이터 접근내역 등을 자동으로 기록하는 로그화일 생성여부	-	-	-	생성
시스템 및 단말기 관리	취급자가 지정 여부	지정	지정	지정	지정
	사용자 ID 및 비밀번호는 사용하고 있으며, 비밀번호는 주기적인 변경여부	주기적	필요시	필요시	주기적
	비밀번호관리대장의 작성 및 관리자는 적정성	적정	적정	적정	적정
	시스템의 정보보호를 위한 기술적 장치를 마련	마련	마련	마련	방화벽
	개인정보 화일의 명칭, 처리일시 및 사용자주체와 사용단말기가 컴퓨터에 자동으로 기록여부	자동 기록	자동 기록	자동 기록	자동 기록
시설보안	보호구역(통제구역)으로의 설정 여부	설정	설정	설정	설정
	보호구역 등 출입자에 대한 통제 여부	-	-	통제	통제
개인정보의 위탁처리	개인정보처리의 위탁시 제한이나 절차 이행	-	-	-	-
	개인정보 수탁자의 안전확보 대책	확보	-	-	-

2. 서울시 전자정부의 개인정보 유통축적 현황

1) 서울시 전자정부의 정보시스템에서 유통되는 개인정보 현황

■ 업무 아키텍처에서 보유하는 개인정보

서울시 전자정부의 업무 아키텍처는 생활정보, 행정정보, 산업정보, 도시기반정보로 구성되어있다 생활정보는 복지, 보건, 여성, 정보화로, 행정정보는 민원, 재산/세무, 신상정보로 구성되며, 산업정보는 고용/취업, 소비자보호, 도시기반정보는 교통, 주택, 지적정보로 분류가 가능하다. 이 분류에 따른 각 시스템에서의 개인정보 분류 예시가 <표 3-3>이다. 생활정보와 행정정보에 속하는 시스템이 다양하며 이들 시스템에서 산업정보나 도시기반정보에 비해 더 많은 개인정보를 취급하는 것을 볼 수 있다. 대부분의 정보시스템에 들어있는 개인정보의 유형은 이름, 주소, 전화번호, 연락처 등 속성에 관한 기본정보가 포함되어 있다.

그런데 생활정보의 보육정보센터, 보건위생관리시스템 등을 보면 활동정보와 민감성 정보들이 다수 포함되어 있는 것을 알 수 있는데, 병명, 치료현황, 직업, 신장, 체중 등이 그러한 것들이다. 사실 이러한 정보들은 개인정보 유형 중 민감한 정보에 해당하며 이들 정보는 개인의 사생활과 밀접한 관련이 있으므로 자체 데이터베이스의 관리는 물론, 정보에 대한 접근성에 대한 규정, 다른 기관으로 유통될 경우의 조건 등에 대한 세밀한 관리가 필요한 항목이라고 할 수 있다.

<표 3-3> 서울시 전자정부의 업무 아키텍처에 따른 개인정보 분류

분 류		관련시스템	예 시
생활정보	복지	보육정보센터	-보호자이름, 주소, 전화번호, 직업, 근무처 -보육아동 이름, 생년월일, 나이 등
	보건	보건위생관리 KT-EDI, 결핵정보감시	--이름, 주민번호, 주소, 전화번호, 보호자 및 친구 관계, 병명, 치료현황 등
	여성	늘푸른여성정보센터	-이름, 나이, 생년월일, 연락처, 보호자 이름 및 연락처, 상담내용 및 결과 등
	정보화	전자우편서비스 시민사이버정보화교육	-이름, 주민등록번호, 주소, 이메일주소, 학력, 나이, 직업 등
행정정보	민원	시군구행정정보시스템 민원처리온라인공개시스템	-이름, 주민등록번호, 주소, 학력, 나이, 생년월일, 신장, 체중, 전화번호, 사진, 지문, 가족관계, 결혼여부 등
	재산/세무	세무종합정보시스템 E-tax(지방세인터넷납부)	-이름, 주민등록번호, 주소, 학력, 나이, 과표, 세액, 수입, 임금 등
	신상	신원증명관리,	-이름, 주민등록번호, 주소, 학력, 나이, 죄명, 형량, 수형인 명부 등
산업정보	고용/취업	취업정보마당	-이름, 주민등록번호, 주소, 전화번호, 학력, 나이, 경력, 기능 및 자격 등
	소비자보호	소비자 종합정보	-이름, 주소, 전화번호, 나이, 구입 물품명, 상담내용 및 결과 등
도시기반정보	교통	자동차등록정보	-이름, 주민등록번호, 주소, 나이, 직업, 차량 제원, 차고지 등
		주정차위반과태료	-이름, 주민등록번호, 주소, 나이, 직업, 차량 제원, 위반사항, 벌점 등
	주택	건출물관리대장 부동산전산망,	-이름, 주민등록번호, 주소, 학력, 나이, 직업 등
		철거민세입자관리	-이름, 주민등록번호, 주소, 나이, 직업, 가족관계, 재산, 소득 등
	지적	지적관리시스템 제적부관리시스템	-소유자의 이름, 주민등록번호, 주소 -지번, 지목, 면적 등

■ 서울시 정보시스템에서 타 기관으로 유통되는 개인정보

서울시 전자정부에서 타기관으로 유통되는 개인정보는 자동차등록관리, 과세, 지방세 체납, 토지대장, 국토정보로 분류할 수 있다. 타기관으로의 제공은 「공공기관의개인정보보호에관한법률」 및 기타 개별법에 근거하여 통상적으로 다른 기관에 제공하는

개인정보 현황은 <표 3-4>와 같다.

개인정보의 피제공기관은 중앙부처(건교부, 감사원, 국세청 등)와 정부산하기관(국민건강보험공단, 대한적십자사 등), 서울시 본청(보건위생과) 및 산하기관(서울시정개발연구원), 서울시 자치구이다. 제공근거가 되는 법률은 「공공기관의개인정보보호에관한법률」, 「자동차관리법」, 「지적법」 등이 있고, 주요 제공항목은 성명, 주민번호, 주소의 일반정보와 과표, 세액, 압류·저당사항 등의 활동정보와 민감정보가 있다.

<표 3-4> 서울시 전자정부에서 타기관으로 유통되는 개인정보

분류	피제공 기관	제공근거	주요항목	제공주기
자동차등록 관리	감사원, 국세청, 경찰청	자동차관리법 제69조	소유자 인적사항 및 차량제원	수시
	서울자동차매매사업조합	자동차관리법 제69조	압류·저당사항	수시
과세	감사원, 시정개발연구원	공공기관의개인정보보호에관한법률 제10조	주민번호, 성명, 과표, 세액 등	수시
	국세청, 국민건강보험공단, 대한적십자사, 근로복지공단	공공기관의개인정보보호에관한법률 제10조	주민번호, 성명, 과표, 세액 등	년2회
	건교부	공공기관의개인정보보호에관한법률 제10조	주민번호, 성명, 과표, 세액 등	년1회
지방세 체납	전국은행연합회	공공기관의개인정보보호에관한법률 제10조	주민번호, 성명, 과표, 세액 등	년4회
토지대장	각 구청(지적과)	지적법제12조의3	전체항목	수시
국토정보	각 구청(주택과, 지적과, 지역경제과, 도시관리과, 인사행정과)		지번, 지목, 면적, 등록번호, 성명, 주소	수시
	서울특별시(보건위생과), 서울북부지방노동사무소관리과	지방세법시행령 제14조	지번, 지목, 면적, 등록번호, 성명, 주소	수시
	서울지방검찰청(남부·동부·서부) 집행과	형사소송법 제199조	지번, 지목, 면적, 등록번호, 성명, 주소	수시
	각 구청(민원봉사과, 민방위재난 관리과, 민원여권과, 구민봉사과)	병역법제80조	지번, 지목, 면적, 등록번호, 성명, 주소	수시
	각 세관 납세심사과	공공기관의개인정보보호에관한법률 제10조	지번, 지목, 면적, 등록번호, 성명, 주소	수시

2) 서울시 전자정부의 홈페이지에서 유통되는 개인정보 현황

■ 서울시 홈페이지 회원의 개인정보

서울시 전자정부는 웹사이트에 회원으로 가입 시에 기재하면서 분류가 시작된다. 개인정보를 필수정보와 선택정보로 나누어 작성하게 되어 있는데, 필수정보는 이름(한글 실명), 주민등록번호, 주소, 전화번호, E-mail address, 회원구분(개인, 외국인, 법인) 등이며, 선택정보는 생년월일, 결혼여부, 학력, 직업, 휴대전화번호, 닉네임을 기재하게 된다. 필수정보는 Weible의 개인정보 분류의 일반정보, 영국 정보위원회의 개인속성, 정부혁신지방부권위원회의 속성정보에 해당된다고 볼 수 있다. 한편, 선택정보는 그 외의 정보에 나누어 분포되어 있다. 서울시 전자정부 사이트는 회원의 민감성 정보나 고용, 금융, 신용 정보 등에 대한 정보는 보유하고 있지 않다

<표 3-5> 서울시 개인정보의 분류

분 류	예 시
필수정보	이름(한글 실명), 주민등록번호, 주소, 전화번호, E-mail address, 회원구분(개인, 외국인, 법인) 등
선택정보	생년월일, 결혼여부, 학력, 직업, 휴대전화번호, 닉네임, 메일링 서비스 및 메일서비스 이용여부 등

■ 서울시 전자정부 웹사이트의 개인정보 축적 현황

서울시 전자정부 웹사이트 이용자는 많이 증가했지만 아직은 오프라인에 비해 활성화되어 있지 못하다. 이는 시민들의 개인정보 축적에 있어 오프라인 정보에 비해 질적·양적인 면에서 서울시가 관리하고 있는 정보가 적다는 것을 의미한다. 즉 오프라인에서는 행정자치부의 지침에 의한 다양한 정보를 가지고 있지만 서울시 전자정부에서는 제한된 회원을 대상으로 한 정보만을 축적하고 있다.

물론 서울시의 통합 DB에 등록된 개인정보를 활용하고 있지만 그건 오프라인상의 정보를 일부 이용하는 것이라고 볼 수 있고 순수하게 전자정부를 통해 축적·관리되는 정보는 미미한 것이 현실이다. 서울시 전자정부는 웹사이트 통합회원과 E-mail Push 서비스 이용자의 가입시 정보를 통합DB에 수집·취급·활용하고 있다.

<표 3-6> 서울시 전자정부 통합회원 및 E-mail Push 서비스 이용자 현황

(단위: 명)

	통합회원	E-mail 서비스	탈퇴회원
이용자 수	59,020	17,182	1,215

한편, 서울시 전자정부의 개인정보 축적 관리에서 탈퇴한 회원의 개인정보를 관리하고 있어 문제소지가 있는 것으로 보인다. 서울시 전자정부 통합회원과 E-mail 회원이 탈퇴할 경우 개인의 정보는 가입 시 정보가 그대로 DB에 남아있다. 회원 가입·탈퇴 의사를 밝힌 회원(시민)에 대해 탈퇴 후에도 서울시가 개인정보 DB를 관리하고 있다는 것을 통보하지 않는다. 회원 탈퇴 시에는 가입자의 정보를 삭제해야 함에도 아직 이에 대한 체계적인 관리가 이뤄지지 않고 있다.

3. 서울시 전자정부의 개인정보보호 관련 법/조례

개인정보보호와 관련한 법은 중앙정부에서 만든 「공공기관의개인정보보호에관한법률」(이하에서는 개인정보보호법이라 함) 및 「공공기관의개인정보보호에관한법률시행령」이 있고, 서울시의 경우 「서울특별시정보화촉진조례」 및 「서울특별시정보화촉진조례규칙」, 「서울특별시인터넷시스템설치및운영에관한조례」가 있다.

서울시는 개인정보보호 및 정보보안을 포괄적으로 규정한 조례는 없고 각각의 조례에서 개인정보보호 및 정보보안에 대해 해당사항을 규정하고 있는 정도이다. 서울시 전자정부를 규정하는 조례의 부재는 서울시 전자정부의 개인정보보호 및 정보보안에 대한 서울시 전자정부 활성화를 저해하는 요인으로 나타나고 있다.

서울특별시정보화촉진조례와 규칙

■ 조례

서울시의 정보화에 대한 기본조례로서 제4조와 제20조에서 개인정보보호와 관련된 사항을 규정하고 있지만 다루고 있는 사항이 너무 포괄적이라 보다 실질적인 개인정보보호에 별다른 도움을 주지 못하고 있다.

조례를 살펴보면 먼저 제4조(기본계획)에서 ① 시장은 정보화촉진을 위하여 서울특별시정보화촉진기본계획(이하 "기본계획"이라 한다)을 수립하여야 한다, ② 기본계획은 정보화촉진기본법 제5조의 규정에 의한 국가정보화촉진기본계획을 고려하여 수립하되 다음 각호의 사항을 포함하여야 한다(6. 개인정보 보호에 관한 사항)라고 하였다.

둘째, 제20조(정보보호)에서 시장은 건전한 정보통신 질서의 확립과 정보의 안전한 유통을 위하여 정보보호에 필요한 다음 각호의 대책을 강구하여야 한다(1. 개인정보의 수집·처리·열람·정정시 보호 대책/2. 정보유출방지를 위한 보호대책/3. 정보윤리의식의 함양을 위한 홍보강화/4. 기타 정보보호를 위하여 필요하다고 인정하는 사항).

■ 규칙

「서울특별시정보화촉진조례」에 따른 규칙으로서 제6조와 제7조에서 정보보안에

관한 사항을 규정하고 있다.

먼저 제6조(정보보안)는 "주관부서장은 정보화관련 시설을 설치·운영하는 경우 서울특별시보안업무처리규칙 및 국가정보통신보안기본지침(국가안전기획부 훈령)의 범위내에서 정보화관련시설 및 정보 자료의 관리에 관한 지침을 수립 시행하여야 한다"(개정 2993.05.26)고 규정되어 있다.

다음으로 제7조(정보자료유출방지)에서는 "주관부서장은 정보통신망을 통해 주요 정보화자료를 송수신 할 경우에는 자료의 유출 방지대책을 강구하여야 한다"고 되어 있다.

서울특별시인터넷시스템설치및운영에관한조례

이 조례는 개인정보보호와 시스템 보안에 대해 제20조와 제21조에서 다루고 있다. 제20조 (개인정보보호)에서는 ① 시장은 인터넷시스템을 통해 개인정보가 타인에게 노출되지 않도록 하는 등 개인정보보호를 위하여 안전대책을 강구하여야 한다, ②시장은 인터넷 홈페이지 서비스 제공과 관련하여 취득한 개인정보를 본인의 승낙 없이 제3자에게 누설 또는 배포할 수 없으며 타용도로 사용할 수 없다. 다만 다음 각 호의 경우에는 예외로 한다(1. 관계 법령에 의하여 수사상 목적으로 관계기관으로부터 요구가 있는 경우/2. 통계작성, 학술연구 또는 시장조사를 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 가공하여 제공하는 경우/3. 기타 관계법령에서 정한 절차에 따라 요청한 경우), ③ 시장은 "개인정보보호방침"을 정하여 홈페이지에 게시하여야 한다, ④ 시장은 개인정보의 보호를 위하여 소속 공무원 중에서 "개인정보보호책임관"을 지정 운영하여야 한다, ⑤ 제1항 내지 제4항 규정의 시행에 필요한 사항은 규칙으로 정한다.

제21조 (시스템의 보안)에서는 ① 시장은 인터넷시스템의 보안을 위하여 안전대책을 강구해야 한다, ② 시장은 정보의 손상 및 파괴 등 사고에 대비하여 일정한 주기로 백업한 자료를 별도의 안전한 장소에 보관·관리하여야 하며 사고 발생시 신속한 복구가 가능하도록 조치하여야 한다, ③ 시스템의 보안에 관하여 기타 필요한 사항은 서울특별시보안업무처리규칙의 규정에 의한다.

4. 서울시민의 공무원의 개인정보보호 인식과 방안

1) 서울시민의 개인정보보호 인식

■ **조사 개요**

- 조사대상 : 서울시민 500명
- 조사방법 : 모바일 조사
- 표본추출방법 : 서울시 인구구성을 반영한 다단계 층화 할당 표집
- 표본오차 : 95% 신뢰수준에서 ±4.4%
- 조사일시 : 2004년 5월 25일

■ **조사 결과**

◦ **시민들은 주민등록번호를 신용카드번호보다 더 중요한 개인정보로 인식함**

서울시민들이 가장 중요하게 생각하는 개인정보는 '주민등록번호'와 '신용카드 번호'로 나타났다. 개인정보 중 가장 중요한 것과 그 다음으로 중요한 것 두 개를 고르게 한 결과(중복응답), 응답자의 45.6%는 주민등록번호가, 29.4%는 신용카드번호가 개인정보에서 중요하다고 생각하는 것으로 나타났다.

◦ **시민들이 생각하기에 공공적 목적으로 공개할 수 있는 개인정보로는 이름, 이메일 등을 들고 있음.**

서울시민 10명 중 4-5명(46%)는 공공적 목적으로 자신들의 이름을 공개할 수 있다고 생각하고 있으며, 21%는 이메일은 공공목적으로 공개가능하다고 생각하였다. 주민등록번호를 공공목적으로 공개가능하다고 생각하고 있는 시민은 9%에 지나지 않았으며, 다만, 50대 이상 연령층의 14%는 주민등록번호를 공공적 목적으로 공개가능하다고 생각하고 있는 것으로 나타나 다른 연령층에 비해 허용정도가 높게 나타났다.

◦ **시민 대다수는 개인정보 활용 실태에 대해 잘 모르고 있음**

서울시민에게 공공적으로 수집된 개인정보들이 어떻게 활용되고 있는지에 대해 알고 있는지 여부를 알아본 결과, 85.2%가 내용을 잘 모른다고 응답하여 전반적인 인지 정도가 낮게 나타났다.

◦ **시민들은 공공부문에서 개인정보 침해가 발생할 소지는 정보시스템의 보안의 허술 정보관리자들의 개인정보보호에 대한 낮은 인식, 법제도 체계 미비 순으로 높음**

서울시민의 44%는 정보시스템의 보안상의 문제 때문에 개인정보가 침해당할 우려가 있다고 생각하고 있으며, 31%는 개인정보 담당 공무원의 의식수준이 낮기 때문에 걱정스럽다는 의견을 보였으며, 응답자의 25%는 법제도적 체계의 미비가 문제라고 생각하고 있는 것으로 나타났다.

◦ **시민들은 민간부문과 공공부문에서의 개인정보보호 정도는 비슷한 수준으로 생각하고 있는 가운데, 40대 이상의 연령층에서 공공부문에서 더 잘한다는 비율이 20, 30대 연령층보다 높음.**

서울시민의 40%는 민간부문과 공공부문의 개인정보보호가 비슷한 수준이라고 생각하고 있으며, 26%는 민간부문이, 25%는 공공부문이 더 잘한다는 의견을 보였다.

◦ **시민 대다수는 향후 개인정보 누출 및 침해에 관한 법적 제도강화가 필요하다고 생각함.**

서울시민 10명 중 9명 이상(93%)이 향후 개인정보 누출 및 침해에 관한 법적 제제가 강화되어야 하는 것으로 생각하고 있는 것으로 나타났다.

◦ **현재 시점에서 개인정보가 침해당했을 경우 법적인 조치보다는 시민단체 등에 고발한다는 의견이 보다 많음.**

서울시민 10명 중 5-6명정도(56%)는 개인정보 노출로 인한 사생활 침해 사건이 발생할 경우 시민단체 등에 고발하겠다고 생각하고 있으며, 법적인 조치를 취하겠다는 비율은 39%로 나타났다.

2) 서울시 정보보호 담당자의 개인정보보호 인식과 방안

서울시 개인정보보호 담당 공무원을 대상으로 서울시 전자정부의 개인정보보호와 정보보안 정책, 정책의 저해요인, 개인정보 누출 및 침해시의 서울시의 문제해결 방안을, 자치구의 개인정보보호와 정보보안 항목으로 자치구의 개인정보보호 노력, 정보보안의 중점 사항 등에 대해 의견을 수집하였다(조사는 2004년 5월 17일에서 26일까지 수행되었다)

① 개인정보보호와 정보보안 정책에서 가장 우선되어야 할 정책

서울시의 자치구 업무담당자들은 서울시 전자정부의 개인정보보호와 정보보안 정책에서 가장 시급한 정책으로 '독립적인 개인정보보호 및 정보보안 기구의 설치/운영'으로 지적되었다(12개 구청에서 지적). 그 다음으로 '개인정보보호및정보보안관련조례 제정'(3명 응답), '개인정보보호 책임관 지정/운영의 활성화'(4명 응답), '최신의 정보보안 시스템 도입'(2명 응답)의 순이었다.

② 개인정보보호 및 정보보안 정책 저해요인

서울시 전자정부의 개인정보보호 및 정보보안 정책의 집행에 있어 저해요인으로 '전문인력 확보의 어려움'과 '담당자 및 정책결정자의 소극적인 자세'라고 16개의 담당자가 응답하였다. 업무담당자들이 개인정보보호와 정보보안에 대한 전문지식이 부족하여 업무수행에 있어 애로사항이 있음을 보여주며, 개인정보보호에 대한 정책결정자의 소극적인 자세로 개인정보보호 및 정보보안 정책의 집행이 신속·원활하지 못한 것으로 인식하고 있다. 반면에 '예산부족', '기술발전 속도에 뒤진 정보보안 시스템'은 큰 문제가 되지 않는다고 응답하였다.

③ 개인정보의 누출이나 침해 시 서울시의 문제해결 방안

서울시의 문제해결 방안으로 신속한 침해안내를 통보하고 사고에 따른 문제분석 및 예방방법 안내, 개인정보 침해대응센터를 통한 대응, 개인정보 해킹방지를 위한 개인정보의 암호화, 개인정보보호담당자에 대한 주기적인 교육실시, 개인정보침해 보상제도 운영, 정보시스템 구축시 개인정보의 오남용, 유출방지 프로그램을 설치 등을 해야

한다고 응답하였다.

④ 개인정보보호를 위한 노력

개인정보를 가장 많이 수집, 보관, 관리하는 자치구는 서울시의 개인정보보호 정책과 함께 자체의 정책을 함께 시행하고 있다. 자치구들이 가장 많이 활용하고 있는 것으로는 '개인정보보호 책임관 지정/운영'(20개 자치구 응답)이다. 대부분의 자치구가 개인정보보호 책임관을 지정/운영하고 있는데 이는 서울시의 지침에 의해 강제적으로 해야 하기 때문일 것이다. 다음으로 '최신의 시스템 체제의 구축'이라고 응답하였다. 이에 반해, '프라이버시영향 평가제도'와 '외부 위탁기업/단체 등의 선정요건 강화'를 시행하는 자치구는 없는 것으로 조사되었다.

⑤ 정보보안을 위해 중점을 두는 항목

자치구에서 정보보안을 위해 '업무상 중요한 사항에 관한 보안대책'에 가장 중점을 주는 항목으로, 다음으로 '패스워드/메일주소 등의 정보보안에 관한 기본항목'이라고 응답하였다. '정보보안의 담당부서 및 담당자의 명확화'도 상대적으로 높은 응답을 보였다. 하지만 '직원에 대한 보안교육 및 연수의 실시'와 '조직 내에서의 보안정보 공유'는 낮은 응답률을 보였다.

제4장 외국 전자정부의 개인정보보호 제도

1. 프라이버시영향 평가제도

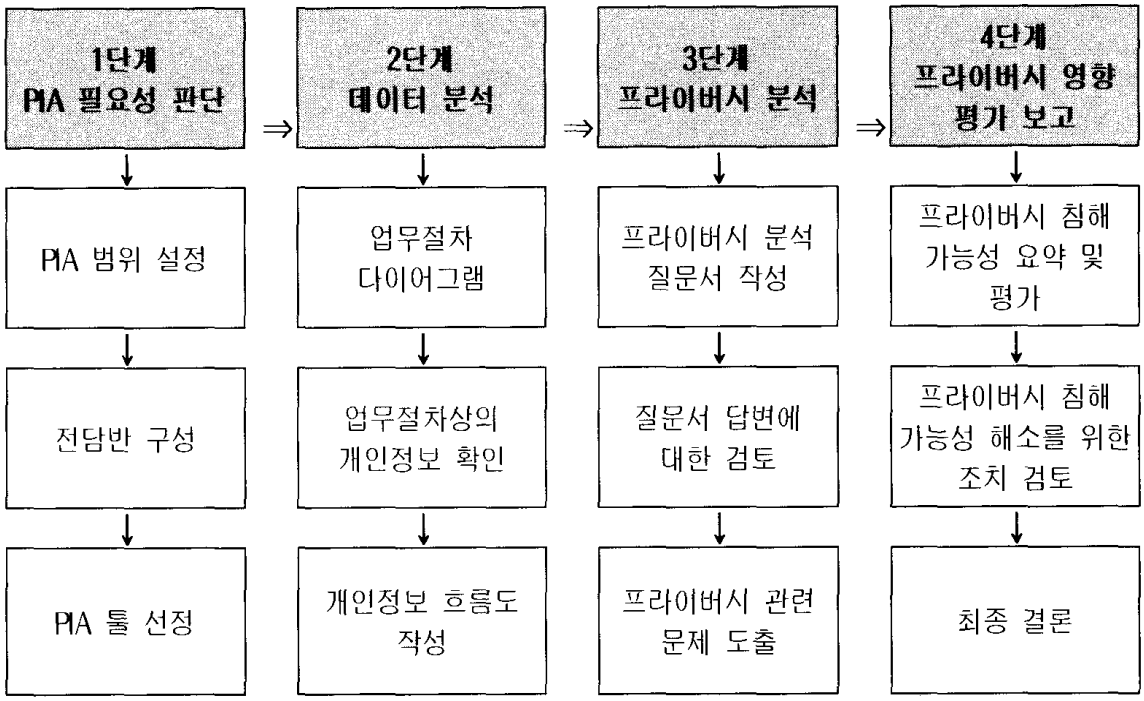
전자정부에서의 개인정보 및 프라이버시 보호를 위하여 전자정부 사업의 계획 단계에서부터 당해 사업이 '개인정보 및 프라이버시에 미치는 영향'을 검토하는 제도로 현재 캐나다와 미국에서 도입하고 있다. 캐나다의 경우 2002년 5월, '프라이버시 영향평가 정책'(Privacy Impact Assessment Policy)을 발표하고 동년 8월에는 이를 구체화한 '프라이버시 영향평가 지침'을 고시하였다. 이 지침은 캐나다 프라이버시법 제71조 제1항 제d호 및 재무관리법 제7조(재무부장관은 프라이버시법에 관한 지침을 시행할 수 있음에 근거한다. 적용범위는 모든 국각기관 및 공공기관에 적용한다.

이에 따라 각 기관은 대국민 프로그램 및 서비스를 개발 및 시행함에 있어 프라이버시 영향 평가를 의무적으로 실시하여야 한다. 대국민 프로그램 및 서비스가 프라이버시 관련 법률을 준수하고 있는지를 판단[9]하고, 관리책임자 또는 정책결정자로 하여금 프라이버시 침해 가능성을 해소하거나 경감할 수 있도록 지원한다. 또한 철저한 검증을 거쳐 각종 정책이나 프로그램, 시스템의 이용을 촉진할 수 있도록 지원한다.

캐나다 정부는 프라이버시 영향 평가 정책 및 지침을 발표 및 시행함으로써 정부의 프로그램이나 서비스의 구상에서부터 시행에 이르는 모든 단계에서 프라이버시 보호 문제가 적극 고려되도록 하고, - 프로그램 관리자 및 기타 관련자에 대하여 프라이버시 문제에 관한 책임을 명확히 하고, 프라이버시에 대한 이해를 바탕으로 철저한 검증을 거쳐 정책이나 시스템 등을 도입할 수 있도록 정책결정자에 대하여 필요한 정보를 제공한다. 사업추진 후에 프라이버시 문제를 이유로 사업을 중단하거나 변경하는 위험을 감소시키고, 정부기관이 이용하는 개인정보 관련 업무절차 및 흐름을 문서화하

9) 현재 캐나다는 개인정보 및 프라이버시 보호와 관련하여 공공부문은 프라이버시법(Privacy Act, 1983)이, 민간부문은 개인정보보호및전자문서법(Personal Information Protection and Electronic Documents Act 2001)이 일반적으로 규율하고 있음.

여 고객들과의 협의를 위한 기초 자료로 활용하고, 프라이버시위원회 및 일반 국민에 대하여 프라이버시 침해 가능성이 있는 신규 또는 변경된 프로그램 및 서비스 계획에 관한 정보를 제공함으로써 적극적인 프라이버시 보호에 관한 인식을 고취시켜야 한다. 캐나다의 프라이버시 영향평가제도의 흐름도는 <그림 4-1·>과 같다.



<그림 4-1> 캐나다 프라이버시 영향 평가 절차도

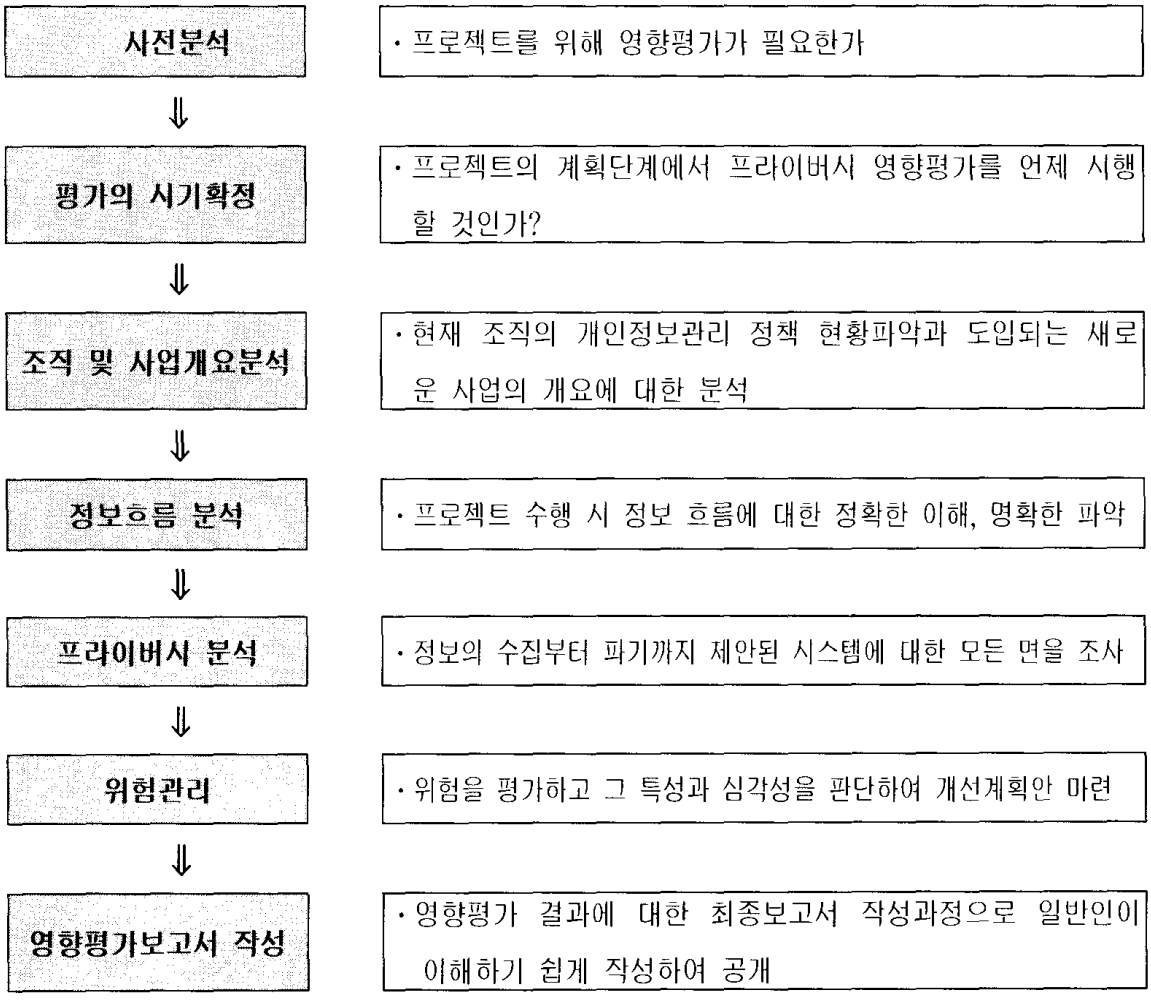
※ 주: 'PIA'는 Privacy Impact Assessment의 약어

미국은 2002년 「전자정부법」에서 국민 중심의 전자정부를 구현하는 과정에서 개인정보 및 프라이버시가 충분히 보호될 수 있도록 프라이버시 영향 평가를 실시할 것을 명문화하였다(제208조). 전자정부법상의 프라이버시 영향 평가는 각종 전자정부 사업을 추진함에 있어 당해 사업이 프라이버시에 미치는 영향을 사전에 조사함으로써 전자정부 사업에 따른 국가기관에 의한 프라이버시 침해를 최소화하는 데 그 의의가 있다.

프라이버시 영향 평가의 대상은 신원확인이 가능한 정보를 수집, 유지·관리 또는 유포하기 위하여 정보기술을 개발하거나 조달하는 경우, 정보기술을 이용하여 수집, 유지·관리 또는 유포될 정보를 새로이 수집하는 경우, 연방 정부기관, 그 대행기관 또는

직원을 제외한 10인 이상의 자에 대하여 신원확인에 관한 문제가 제기되거나 신원에 관한 보고의무가 부과되는 경우에 특정 개인에 대하여 물리적 또는 온라인 접속을 허용하는 신원확인이 가능한 여하한 정보 등을 새로이 수집하는 경우이다.

평가기관 및 절차는 프라이버시 영향 평가를 수행하는 기관은 프라이버시 영향 평가의 대상이 되는 전자정부 사업을 수행하는 당해 기관으로 하고 있다. 당해 기관장의 결정에 따라 '정보화책임관' 또는 그에 상당하는 공무원이 프라이버시 영향 평가하고 전자정부기금의 출연이 필요한 시스템의 경우, 당해 기관은 이에 대한 프라이버시 영향 평가서를 관리예산처장에게 제출하여야 한다.



<그림 4-2> 미국의 프라이버시 영향평가 제도의 절차

* 출처: 권선경, 2003. "국회 프라이버시 영향 평가 제도 시행 현황", KISA 국외동향보고서 참조

2. 개인정보보호지침

1) OECD의 개인정보보호 가이드라인

OECD는 프라이버시와 정보의 자유로운 유통이라는 기본적으로 경합되는 가치를 조화시킬 것을 목적으로 「프라이버시보호와 개인데이터의 국제유통에 관한 가이드라인(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)」를 채택하였다. OECD가 제시한 개인정보보호 8개 원칙은 <표 4-1>과 같다.

<표 4-1> 개인정보보호 8개 원칙

원 칙	정 의
수집제한의 원칙(Collection limitation principle)	개인정보는 적법하고 공정한 수단에 의해 수집되어야 하며 정보주체에게 알리거나 동의를 얻은 후 수집되어야 함
정보내용 정확성의 원칙 (Data quality principle)	개인정보는 그 이용목적에 부합하고 이용목적에 필요한 범위내에서 정확하고 완전하여 최신의 내용으로 유치되어야 함
목적명확화의 원칙 (Purpose specification principle)	개인정보 수집시 수집될 개인정보가 구체화되어야 하며 이를 이용할 경우에도 애초의 목적과 모순되거나 그 의도를 벗어나지 않아야 함
이용제한의 원칙 (Use limitation principle)	개인정보는 정보주체의 동의를 획득했거나 법률상 규정된 경우를 제외하고는 공개되거나 타인이 사용하거나 명확히 제시된 목적 이외의 용도로 쓰여서는 안됨
안전보호의 원칙 (Security safeguards principle)	개인정보의 분실, 불법적 접근, 파괴, 오용, 수정, 공개의 위험 등에 대비해 정보통제자는 합리적인 보안장치를 마련, 충분히 안정성을 확보해야 함
공개의 원칙 (Openness principle)	개인정보의 개발/운용 및 정책에 관해서는 공개해야 함. 개인정보의 존재, 성질 및 주요 이용 목적과 함께 정보관리자의 신원 및 주소를 쉽게 알 수 있도록 하는 방안이 강구되어야 함
개인참가의 원칙 (Individual participation principle)	정보주체인 개인은 자신과 관련된 정보를 정보관리자 혹은 그에 상응하는 기관이 갖고 있음을 확인해야 함. 또한 개인은 그 자신과 관련된 정보를 합리적인 기간 동안 과도하지 않은 비용으로 합당한 방법을 통해 쉽게 접근할 수 있는 형태로 유지하도록 정보관리자와 계속 연결되어 있어야 함. 개인은 상기의 요청에 대해 합당한 이유 없이 이의 시행을 거부당해서는 안되며, 필요한 업무가 끝난 후에는 자신과 관련된 정보의 삭제, 정정, 보완 청구권을 가짐
책임의 원칙 (Accountability principle)	개인정보 관리자는 상기 원칙들이 지켜질 수 있도록 필요한 제반 조치를 취해야 함

국가간 정보유통의 원칙은 각국의 실정에 맞는 정보처리, 유통과정 개발, 직접적인 수출이 아닌 단순 경유 시에도 내용이 침해되지 않게 해야 한다. 또한 본 가이드라인에서 정하는 수준의 개인정보보호체계를 갖추지 못하거나 재수출이 자국의 프라이버시 법률과 위배되지 않는 한, 제3국으로의 수출을 금지하지 말고 자유로이 정보가 국가간에 유통될 수 있도록 조장하며, 프라이버시 및 개인의 천부적 자유권을 보호하기 위한 명목으로 과도한 국내정책, 법안, 관행 등을 만들어 국가간 개인정보 유통에 지장을 초래하지 말 것을 강조한다.

정보집적의 장점은 서비스 제공 속도 증가, 사용자에게 이용 편의성 제공, 사용 환경이 간단하고 편리해짐, 자유로운 접속 보장이다. 정보주체의 프라이버시 보호는 실질적으로 수집되고 있는 정보의 양과 질은 오프라인상에서와 크게 다르지 않으나, 정보의 저장공간이 사이버상이라는 점 때문에 파생하는 문제이다. 안정성 보장을 위한 보호(security)의 문제, 이를 통한 정보통제자의 신뢰성(trust) 제고문제, security와 trust에 기반한 프라이버시 보호가 핵심이다.

정보의 집적을 통한 정보공유는 개인 및 사회에 엄청난 이익을 가져다 줄 수 있는 또 다른 가능성을 가진다. 또한 개인정보를 긍정적으로 유효 적절히 사용해 프라이버시가 제대로 보장되는 사회를 구성하기 위해, 공공부문에서 집적한 정보를 제대로 활용하고 있다는 신뢰를 주는 것이 무엇보다 중요하다. 프라이버시 보호자체가 이미 공공서비스인 것이다. 프라이버시 보호와 정보공유 간의 핵심 쟁점은 신뢰의 문제, 보유하고 있는 개인정보의 정확성과 신뢰도 향상, 안전한 방어책 마련, 개인정보 및 프라이버시 처리 방식의 현대화, 시민들에게 이익과 신뢰를 더하는 법제도적 틀 마련 등에 있다(UK Cabinet Office, 2002).

2) EU의 개인정보보호 지침

EU의 개인정보보호지침은 "any information relating to an identified or identifiable natural person"이다. 주요내용을 살펴보면, EU 내에서의 개인정보의 자유

로운 이전 보장, 기술적 보호 장치 강화, 정보주체에게 정보처리에 대한 통지 의무, 정보이전이 가능한 경우 규정, 온라인 네트워크상의 개인정보보호 외 정치, 경제, 행정 등 개인정보가 수집/처리되는 모든 영역을 규정, Adequate level of data protection(제3국으로의 수출금지근거), 지침 반영한 국내법 제정 촉구, 독립적인 감독기관 설치이다. 독립적인 감독기관의 개인정보에의 접근권, 수사권, 감독의무, 비디오 감시 등은 이 지침에 해당하지 않는다. EU의 규정은 <표 4-2>와 같이 나타낼 수 있다.

<표 4-2> EU의 개인정보보호지침

규 정	내 용
주요일반규정	제한적이고 합법적인 개인정보 수집목적, 이러한 목적에 부적합한 정보의 수집 및 처리 금지
	개인정보의 적절성, 관련성, 정확성 및 최신성 요구와 과장 및 필요이상의 내용 공개금지
	정보주체의 명백한 동의가 있는 경우와 개인정보 처리가 계약 또는 법률상의 의무에 포함되는 경우, 정보주체의 기본적인 자유와 권리가 정보수집자의 법적 이익보다 중요하지 않으며 개인 정보처리가 이러한 법적 이익의 추구에 필수적인 경우에 한하여 개인정보 처리 가능
개인정보 이전규정	제3국으로의 개인정보의 이전은 당해 제3국이 충분한 수준의 개인정보보호조치를 확보한 경우에 한하여야 함

지침의 내용은 협약 제5조와 제16조에서는 정보의 자동적 처리에 있어 ① 공정·합법한 획득, ② 구체적이고 정당한 목적을 위해서만 저장, ③ 저장목적과 해당 정보간에 적적할 관련성의 존재 및 ④ 개인정보가 올바르고 필요한 경우, 최신의 것이어야 하며 부정확하거나 불충분한 정보는 삭제·수정되어야 하고, ⑤ 정보는 저장목적을 위하여 필요한 시간만큼 보존되어야 한다. 또한 협약 제17조에서 인종, 정치적 견해, 종교적·철학적 신념이나 노동조합가입여부, 건강상태나 사생활정보와 같은 특별히 민감한 개인정보는 국내법이 적절한 보호를 제공하지 않는 한 자동적으로 처리될 수 없다고 규정하여 정보보호에 관한 광범위한 합의를 도출하고 있지만 개인정보보호원칙이 절대적이지는 않다(협약 제15조와 협약 제24조).

EU 프라이버시 보호지침의 목적은 사업목적으로 다른 기업에 판매하는 것처럼 기

업이 자신의 고객이 원하지 않는 방식으로 자신의 고객에 대한 정보를 사용하는 것을 금지하는 것으로, 유럽에서 영업하고 있는 모든 기업은 동등한 프라이버시보호를 보장하지 않는 모든 국가에 개인정보를 전송할 수 없는 것이다. EU 지침의 이행 현황은 <표 4-3>과 같다.

<표 4-3> 지침의 이행현황

회원국	입법 현황	차지조치
벨기에	-이행입법 의회 통과 -1999.2.3 관보 게재	
덴마크	-민간등록법(Civil Registration Act) 개정으로 부분이행 -입법안 L44제출 중	
독일	-아직 의회절차가 개시되지 않았음 -지방차원에서도 입법조치가 필요함	-정부 입법안을 준비중
스페인	-기존 'Ley Organica'의 개정안이 제출되어 의회 심의 중	-의회채택이 예상됨
프랑스	-의회절차 미개시	
그리스	-1997.4.10 이행입법 2472 채택	
이탈리아	-1996.12.31 법 675의 시행령 채택	
아일랜드	-1998.6 국무회의 정부안 상정	-의회제출
룩셈부르크	-정부안 작성 중	-의회제출
네덜란드	-1998.2.16 제2원에 법안제출	-의회(제1, 2원) 채택
오스트리아	-1999.3 입법안 의회제출	-의회 심의
포르투칼	-1998.10.26 법 67/98로 이행	
스웨덴	-1998.4.29 SFS 1998:204, 시행령 1998:1191로 이행	
핀란드	-1998.2.10 입법안 의회 채택	
영국	-1998 데이터보호법	-시행령 작성 중

3. 정보보호책임관제도

정보보안책임관은 미국 주(州)정부 또는 지방정부의 정보통신관련 정책과 함께 정보보안 관련한 업무를 책임지는 담당관으로서 대표적인 예로서 뉴욕주의 정보보호책임관을 들 수 있다. 뉴욕주는 미국에서 처음으로 정보보안책임관(ISO: Information Security Officer) 제도를 만들어 종합적인 정보보안정책을 수립한다. 뉴욕주 정보기술국(OFT)은 1997년 1월 "정보기술 정책지침 97-1"(Technology Policy 97-1)에서 정보보안의 중요성과 역할에 대해 언급하고 있다. 또한 1999년 2월 "정보기술 정책지침 99-2"(Technology Policy 99-2)에서 정보보안책임관의 기능, 역할, 교육, 자격 등을 구체적으로 규정하여 정보보안과 관련된 제도를 공식화하였다.

1999년 공식화된 ISO의 구체적 역할과 기능을 명시하였는데, ISO는 " 조직의 정보시스템을 구상, 설계, 개발, 운영, 유지, 폐기하는 전 과정엣 보안서비스를 제공하고 보안정책을 집행하여 규정에 의해 정해진 상위 관리자의 책임을 지는 사람'으로 정의를 내리고 있다. 또한 정부차원의 정보보안 정책을 체계화한 "New York State Standard and Procedure for Information Security"을 수립하였다. 이는 정보보안의 지침서로 정보보호 표준화와 절차에 대한 내용을 담고 있는 것으로 ISO의 포괄적인 관리적 요소를 구체적으로 다루고 있다.

이러한 뉴욕주의 시도는 이후 미국 내 다른 주정부들이 ISO를 임명하는 경우로 나아가고 있다(<표 4-4> 참조). 각 주정부의 정보보호책임관 제도는 주 특성상 약간 상이하게 운영되고 있는데, 유형별로 중앙집권적 유형, 분권적 유형, 세부분권적 유형 등으로 구분될 수 있다. 중앙집권적 유형이란 중앙에서 전체적인 정보보안 책임을 정보보호책임관이 지는 형태로 운영되는 것을 말하며, 분권적 유형이란 각 정보시스템에 대해 부처별로 정보보안을 책임지는 형태이며, 세부분권적 유형이란 분권적 유형보다 좀 더 하부 단위에서 정보시스템에 대한 보안을 책임지는 형태를 의미한다.

<표 4-4> 정보보호책임관 제도의 다양성

Organizational Structure 정보보호 조직특성		None (8)	Single Person (15)	Multiple (16)
	Centralized (14)		Illinois[3] North Dakota North Carolina[7] Rhode Island South Dakota Tennessee West Virginia Wyoming[9]	Alabama Michigan[4] Mississippi[5] Missouri[6] North Carolina[7] Pennsylvania Wisconsin[8] Wyoming[9]
	Decentralized (23)	Kansas Nebraska Puerto Rico South Carolina Vermont Washington	Arizona[1] Illinois[3] Iowa Maryland Montana New Jersy North Carolina[7]	Arizona[1] Idaho Kentucky (Louisiana) Michigan[4] Mississippi[5] Nevada New York North Carolina[7] Texas Utah Wisconsin[8]
	Decentralized & Locally Controlled (7)	Colorado Massachussetts	Illinois[3] Delaware[2] Maine Wyoming[9]	Delaware[2] Missouri[6] Wyoming[9]
		Primary Contact 정보보호책임자		

출처: www.nascio.org/publications/security.cfm (정익재, 2004에서 재인용)

이러한 경향은 미국 전자정부가 초기 단계에서는 전자정부 구축과 관련한 CIO의 역할을 강조하던 데에서 한발 더 나아가 고도화된 전자정부에서 개인정보보호를 포함한 정보보안의 중요성이 강조되면서 ISO의 역할이 중요해짐을 의미한다. 뉴욕주에서 최근 몇 년동안 매년 실시하고 있는 'New York State Cyber Security'는 이러한 변화의 경향을 잘 보여주고 있는데, 이 컨퍼런스는 정보보안국(Office of Cyber Security & Critical Infrastructure Coordination: 약칭 CSCIC)에서 주최하는 것이다.

정보보호책임관의 역할

뉴욕주의 모든 공공기관의 안전사고와 관련한 모든 활동의 중심에서 진행을 담당하며, 긴급대응팀(CIRT: Computer Incident Response Team)의 주요 구성원이 된다. 실제로 보안사고에 대응하는 절차를 집행하는 차원에서 정보보안관은 긴급대응팀을 소집하고 사고발생의 현장에서 사고대응 및 사후관리에 총괄적인 책임을 지고 문제를 해결한다. 조직 운영차원에서 사고가 발생했을 때 내부의 의사전달자(communicator) 기능을 담당할 뿐만 아니라 사고를 처리하는데 내부 조직간의 조정자(coordinator) 역할을 수행하여 조직간의 분절된 업무기능을 연계된다. 또한 외부기관과의 연계를 위한 통로 역할. 보안사고를 타기관에 알리거나 사고를 처리한 후, 결과를 상부기관에 보고하는 공식적인 대외창구 기능을 수행하게 된다. 따라서 정보보호책임관은 정보보안과 관련된 기술적 차원의 지원이나 자문 역할을 수행하는 정태적인 직책이나 특정 개인을 의미하는 것이 아니라 종합적인 위기관리체제(risk management system)로써 동태적인 제도이다.

정보보호책임관의 권한

정보보호책임관은 사고발생시 이를 책임지고 담당하는 공식적인 권한을 부여받았으며, 정보보안사고를 사전에 대비하는데 경찰과 같은 역할을 수행한다. 따라서 발생가능한 사고를 항상 염두에 두고 정보화 정책을 수립하는데 참여하기 때문에 정보보안관은 대체로 보수적인 행태를 보이며, 정보화를 전향적으로 추진하는 관리·행정 담당자들과 어느 정도의 의견대립이 상존하고 있다[10].

---

10) 정보보안관과 정보화를 추진하는 최고정보관리자(CIO) 및 행정관리자의 의견 및 태도 차이는 뉴욕주 정보기술국(New York State Office for Technology) 산하의 정보인프라(NYeNet) 구축팀의 일원인 Dave Strazzeri와 인터뷰에서 분명하게 나타나고 있다. 그는 정보보안관의 행동을 정보화정책을 추진하는데 "방해자" (breaker)라 표현할 정도로 시각차이를 보이고 있다. 이에 비해서 뉴욕주의 최고 정보보안관인 Laura Iwan은 자신의 보수적인 행동을 지극히 당연하다는 반응을 보이고 있다. "정보보안이 보장되지 않은 정보화정책이나 시스템 개발은 전혀 의미가 없다"는 입장을 강하게 표현했다. 동일한 맥락에서 뉴욕주 감사원(Office for State Comptroller)의 정보보안관인 Jim Brunt는 "우리의 역할은 경찰과 마찬가지다. 경찰은 시민들로부터 칭찬을 듣기보다는 항상 비난의 대상이다. 하지만 경찰은 사회의 안전을 위해서 반드시 존재해야 하듯이 정보보안관도 정보사회의 안전을 위해서 없어서

정보보호책임관 제도의 의의

이와 같은 정보보호책임관 제도가 갖는 의미는, 첫째, 위험관리시스템을 제도화했다는 데 있다. 이미 정보보호책임관 제도의 역할에서 밝힌 것처럼 개인정보남용 뿐 아니라 정보시스템에서의 문제가 발생했을 때는 의사전달자의 역할 뿐 아니라 내부 조정자의 역할을 수행할 수 있는 제도적 기제이다. 둘째, 정보보호책임관은 조직 내부의 경찰관의 역할로 정보시스템의 효율성론자들과 개인정보보호 조직 사이에서 견제와 균형의 역할을 수행할 수 있다. 마지막으로 이들은 안전에 관한 지식기반관리자로서의 역할을 수행하면서 다른 부서에 필요한 교육을 담당하는 역할을 할 수 있다.

는 안될 존재다"라고 본인의 역할을 강조하고 있다.

제5장 서울시 전자정부의 정보보호 추진전략

1. 서울시 전자정부 발전단계에 조응하는 개인정보보호의 기본방향

우리는 지금까지 서울시 전자정부의 개인정보보호와 관련하여 정보유통현황과 관리현황, 개인정보보호에 관한 시민들의 인식과 전자정부 조직구성원인 공무원들의 인식 조사 등을 통해 전자정부에서의 개인정보보호에 관한 인식과 문제의식이 전반적으로 낮은 단계이거나 출발 단계임을 알 수 있다. 한편, 서울시 전자정부의 발전단계는 도시정보화를 위한 기반시설이 확충된 이후 이의 활용성을 제고하기 위한 단계로 나아가고 있음을 알 수 있다. 이미 교통부문 등 일부에서는 모바일 전자행정 서비스를 도입하는 모바일 전자정부의 초기 형태를 현실화시키고 있는 가운데 유비쿼터스 정부로의 가능성에 대한 논의도 활발하게 나타나고 있다. 이처럼 전자정부 발전현황에 비해 정보보호 관련 현황은 낮은 단계인데 이 양자 사이의 간극을 좁혀지지 않는 한 전자정부의 발전에 걸림돌이 될 가능성이 많다. 유비쿼터스 전자정부의 핵심은 기술발전 뿐 아니라 이러한 기술을 현실화시키기 위해서는 정보보안과 정보보호의 문제가 동시에 고려되어야 한다는 의미이다.

최근 중앙정부의 개인정보보호 등 정보보안에 관한 논의들이 공통적으로 내리고 있는 결론은 보안관리의 미흡이라는 관리적 문제, 정보보호를 위한 통합기구의 부재 등이다. 관리문제의 경우 비전공 상위관리자의 보안의식의 부족이라던지 기관별 보호대책 및 대응체계의 미흡의 문제, 운영과 보안업무 겸임으로 인한 책임감의 결여 문제 등이 지적되고 있으며, 정보보호통합기구의 경우 개별 분산적 보안으로 인한 유기적 통합의 문제점이 드러나는데 정보통신망의 경우 영역구분이 무의미하다는 점을 고려한다면 이 문제도 해결되어야 할 것이라 지적한다(장태수, 2003)

이러한 맥락에서 서울시 전자정부에서의 개인정보보호의 기본 방향은 개인정보의 수집과 유통에 대한 허용여부를 결정하고, 행정서비스를 활성화하면서 동시에 시민들에 대한 신뢰를 제고하는 방향으로 나아가야 한다. 이러한 방향은 지금까지의 '정보의

차단 혹은 통제'라는 기존의 패러다임이 '정보의 공개 및 관리'라는 새로운 방향으로 바뀌어 나가는 것을 의미한다. 이 같은 방향으로의 전환을 위해서는 무엇보다도 전자정부에 대한 신뢰형성의 기제를 만들어야 한다. 시민들에게 정보보호 관리체계에 대한 인식을 확산시키고 홍보하여 사회적 합의에 도달하기위한 다양한 시도가 진행된다면 이러한 신뢰형성의 기제는 전자정부 내부에 뿌리내릴 수 있을 것이다.

2. 서울시 전자정부의 개인정보보호를 위한 추진전략

특히 개인정보보호의 문제와 전자정부의 행정서비스의 고도화는 밀접한 연관성이 있다. UN의 전자정부 고도화 단계에 따르면 상호작용이 일어나는 3단계를 거치면 실제 전자정부 내에서 거래가 이뤄지며, 이후 전체 과정이 이음새없이 유기적 결합을 통한 통합적 서비스가 달성된다. 이 과정에서 전자정부에 대한 시민들의 신뢰가 중요한 역할을 하는데, 이 때 개인정보보호에 관한 제도적 장치의 유무가 주요 바로미터라고 할 수 있다. 다시 말하면 전자정부에서의 전자적 거래가 이뤄지기 위해서는 시민들이 자신들의 정보가 보호될 수 있는 여러 가지 장치들에 대해 신뢰해야만 한다. 최근 민간부문에서 인터넷 뱅킹과 관련한 사고가 발생했을 때 시민들이 느끼는 불안감은 이용률의 하락으로 귀결된다.

공공부문의 경우 개인의 자발적 동의에 의해 수집된 개인정보와 행정운영의 필요성에 의해 획득된 개인정보 등이 혼재되어 있는 상황에서 신뢰의 기제가 없다면 행정업무 전체에 대한 불신으로 이어질 수 있다. 따라서 시민영역과의 신뢰기제를 구축하기 위한 전략을 구성하여야 한다. 추진전략은 앞서 논의한 개인정보보호의 기본방향을 구체화하기 위한 것이다.

정보보호조직의 역할 강화

미국 주정부의 정보보호책임관 제도를 비롯한 조직현황을 참고하여 서울시 전자정부에 조응하는 정보보호조직의 역할을 명확히 하고 권한을 강화할 필요가 있다. 서울시 전자정부의 경우, 정보통신담당관 산하 정보보호팀으로 2003년 새로운 조직편재에

등장하였다. 팀장과 5명의 팀원으로 구성되어 있는데, 정보보호팀이 태스크 포스(Task force)가 아닌 상근 조직으로의 위상을 갖고 있다는 것은 긍정적이 측면으로 파악된다. 정보보호팀의 역할은 이미 뉴욕주 정부 사례에서 살펴본 것처럼 앞으로 등장할 정보보안, 개인정보 오남용 등 정보화의 역기능을 최소화하기 위한 조정과 견제의 역할을 수행해야만 한다. 이를 위해서는 먼저 조직 내적으로 정보보호에 관한 인식제고를 위한 교육 프로그램 등이 실시되어야 한다. 또한 시민들을 대상으로 서울시 전자정부의 개인정보보호 기제에 대한 홍보와 더불어 다양한 정보를 공개하는 방향으로의 지속적 노력이 필요하다.

개인정보보호를 포함하여 차세대 정보보호 모델의 개발

앞으로의 정보보호는 변화하는 수요에 부합하는 정보보호요소를 반영하여 모델이 개발되어야 한다. 흔히 차세대 정보보호 모델은 사용자의 편의성이 증대된 통합보안기술로서의 easy security, 다양한 침해사고(사람에 의한 관리적 요소를 포함하는)에 대해 능동적으로 대응하는 보안기술로서의 active security, 신뢰가능한 보안서비스를 제공하는 상호연동성으로서의 secure networking 등으로 요약된다. 서울시 전자정부의 정보보호 추진전략은 이러한 차세대 정보보호 모델을 충분히 반영한 정보보호체계를 구축해야 한다.

개인정보보호에 관한 통합적 내용을 포괄하는 조례의 제정

현재의 분산적인 개인정보보호 관련 조례는 통합적으로 규정된 조례로 제정되어야 한다. 이 조례의 초안은 다음 절에서 제시하였다.

통합적 정보보호 감독기구에 대한 조직 구상

개인정보관련 처리규정의 세분화(매뉴얼화된 지침 필요)

현행법 상 개인정보보호관련 규정의 실효성 있는 준수를 위한 체크리스트 작성

3. 「서울특별시개인정보보호및정보보안에관한조례(안)」

「서울특별시전자정부개인정보보호및정보보안에관한조례」는 보다 나은 서울시 전자정부 행정서비스의 제공을 위해서 제정되어야 한다. 조례는 개인정보보호와 정보보안에 관해 폭넓게 다루어져야 한다. 조례는 총칙, 개인정보보호, 정보보안, 개인정보보호 감독기구, 개인정보 유통·관리로 나누어 구성하였다.

1) 총칙

「서울특별시전자정부개인정보보호및정보보안에관한조례」의 제정목적은 서울특별시 전자정부를 통하여 처리되는 개인정보의 보호를 위하여 그 수집·취급·활용에 관하여 필요한 사항을 정함으로써 행정서비스의 적정한 수행을 도모함과 아울러 서울시민의 권리와 이익을 보호함을 목적으로 한다.

이 조례에서 사용하는 용어는 「공공기관의개인정보보호에관한법률」에서 사용하고 있는 용어의 정의를 따르고, 이 법을 상위법으로 한다.

2) 개인정보보호 관련 일반 조항

먼저 개인정보 수집이다. 서울시 전자정부는 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니 된다. 다만, 정보의 주체의 동의가 있거나 다른 법률에 수집대상 개인정보가 명시되어 있는 경우에는 그러하지 아니하다.

둘째, 개인정보 화일의 보유범위이다. 서울시 전자정부는 업무를 수행하기 위하여 필요한 범위 안에서 개인정보 화일을 보유할 수 있다.

셋째, 개인정보의 이용과 제한이다. 보유기관의 장은 다른 상위 법률 및 조례에 의하여 보유기관의 내부에서 이용하거나 보유기관외의 자에게 제공하는 경우를 제외하고는 당해 개인정보 화일의 보유 목적외의 목적으로 처리정보를 이용하거나 다른 기관에 제공하여서는 아니 된다.

넷째, 개인정보보호지침이다. 서울시 전자정부는 개인정보보호에 관한 지침을 만들고 이를 서울시 전자정부에 게시하고 이를 이용하는 시민에게 공지하여야 한다.

다섯째, 개인정보보호 책임관제도의 지정·운영이다. 서울시 및 자치구는 개인정보보호 책임관의 지정·운영을 통해 개인정보의 수집·취급시에 이를 총괄하여야 한다.

여섯째, 개인정보 누출 및 침해시 대응방안이다. 서울시 전자정부는 개인정보의 누출 및 침해 방지를 위한 규정을 신설하고, 침해시에 법적·물질적·정신적인 보상과 담장자·책임자의 처벌조항을 만들어야 한다.

3) 정보보안 관련 조항

「서울특별시전자정부개인정보보호및정보보안에관한조례」는 「서울특별시정보화촉진조례규칙」 제6조와 「서울특별시인터넷시스템설치및운영에관한조례」 제21조의 규정을 토대로 하여야 한다.

첫째, 정보보안시스템 도입·구축과 운용에서의 법적인 미비이다. 서울시 전자정부는 정보보안시스템 구축 시 법적인 규정이 미비하여 신속한 도입·구축이 이루어지지 않았다. 시스템 의 도입과 구축을 위한 로드맵과 시스템 운용을 규정하는 조항이 들어가야 한다.

둘째, 정보보안 책임관의 지정·운영이다. 개인정보보호 책임관과 마찬가지로 정보보안시스템의 도입·구축·운용을 총괄하는 책임관을 지정이 필요하다.

4) 개인정보보호 감독기구

개인정보보호 법·조례의 제정도 중요하지만 시민의 개인정보를 효율적으로 보호하기 위해서는 공공기관이나 민간부문의 정보 수집, 취급, 활용을 감독·통제하는 기구의 설치 및 운영이 절대적으로 요구된다.

이러한 감독기구의 구성은 개인정보보호 관련 법률, 행정 전문가, 정보보안시스템 전문가 등으로 15인 정도로 구성하는게 바람직하다. 이 기구는 공공기관과 민간부문의 정보조사와 처리를 통제하는 것에 집중해야만 한다. 즉 감독기구는 개인의 정보보호를 우선적 목표로 하여 개인의 여러 권리들을 보장하고 강화하도록 노력해야만 한다.

또한 감독기구는 부당한 감시를 받고 있다고 느끼는 시민들의 권리보호를 위하여 노력하는 것 역시 중요한 기능에 속한다. 이를 넘어서서 감독기구는 다양한 방법을 통하여 공공기관의 정보처리과정에서 개인정보가 보호될 수 있도록 일반적이고 체계적인

감독과 대인제시의 역할을 수행해야 한다.

그리고 감독기구는 개인정보의 수집, 취급, 활용과 관계되는 중요사항에 대하여 매년 의회에 보고서를 제출하고 개인정보보호와 관련되는 사안에 대하여 언론매체 등을 통해 널리 알리고 시민에게 홍보해야 한다.

5) 개인정보 유통 및 관리 관련 조항

정보주체는 개인정보 화일대장에 기재된 범위안에서 서면으로 본인에 관한 처리정보의 열람을 보유기관의 장에게 청구할 수 있다. 보유괴간의 장은 앞의 규정에 의한 열람청구를 받은 때에는 청구인으로 하여금 당해 처리정보를 열람할 수 있도록 하여야 한다.

개인정보의 유통에 있어 해당기관은 「공공기관의개인정보보호에관한법률」의 규정외에 서울시에 국한된 문제에 대한 규정을 신설하여야 한다.

6) 조례의 구성

조례는 5개장 17개조로 구성되어 있다. 제1장 총칙은 제1조(목적), 제2조(용어의 정리)이다. 제2장은 제2장 개인정보보호, 제3조(개인정보의 범위), 제4조(개인정보의 수집), 제5조(개인정보의 취급), 제6조(개인정보의 활용), 제7조(개인정보보호의 지침), 제8조(개인정보 책임관 지정·운영), 제9조(개인정보 누출 및 침해시 대응방안)이다. 제3장 정보보안은 제10조(정보보안시스템 도입·구축), 제11조(정보보안시스템 운용), 제12조(정보보안 책임관 지정·운영)이다. 제4장 개인정보보호 감독기구은 제13조(설치 및 구성)과 제14조(기능)이다. 제5장은 개인정보 유통·관리로 제15조(개인정보의 열람·정정), 제16조(개인정보 유통 범위), 제17조(개인정보 유통 규칙)이다.

■ 참고문헌

1. 국내문헌

1) 단행본

고민정, 2003. **정보보호개론**, 서울: 세화출판.

메리 팻 맥카시 & 스튜어트 캠벨 저/ 앤드류 남 역, 2001. **정보 보안 혁명**, 물푸레.

숙명여자대학교, 2002. **정보시스템 보안을 위한 기반 및 응용 기술 연구**, 과학기술부.

이동영, 서광현, 정태명, 2002. **인터넷 정보 보호: 인터넷 정보 보호 알파에서 오메가까지**, 서울: 영진닷컴.

이민영 · 주지홍, 2003. "전자정부 시대의 개인정보보호: 법안분석 및 법제검토," **KISDI 이슈 리포트**, 과천: 정보통신정책연구원.

조완수, 2003. **정보시스템 보안**, 서울: 홍릉과학출판사.

전자정부특별위원회, 2003. **전자정부백서**, 서울: 전자정부특별위원회.

정철현, 2003. **PKI: 전자서명과 인증제도**, 서울: 다산출판사.

Matthew Strebe 저/김동우 역, 2003. **개인정보보호와 해킹 방어를 위해 해야할 것과 하지 말아야 할 것**, 서울: 크라운 출판사

조화순, 2003,「공공부문의 개인정보보호 : 현황과 개선방안」, **정보화정책 이슈**, 한국전산원

한국정보보호진흥원, 2002. **정보보호시스템 평가 · 인증 가이드**, 서울: 한국정보보호진흥원.

한국정보보호진흥원, 2003. 제8회 정보보호심포지엄 발표논문집, 한국정보보호진흥원.

행정자치부, 2003. 공공기관의 개인정보보호제도 이해와 해설, 서울: 행정자치부.

황주성 · 최선희, 2003. "전자정부 사업과 개인정보보호 이슈," **KISDI 이슈 리포트**, 과천: 정보통신정책연구원.

2) 논문

김대호 · 오일석, 2003. "미국 전자정부 정보보안 법제 동향," **정보보호학회지**, 제13권 제3호.

김진영, 2002. **정보보호수준 평가 방법론 개발에 관한 연구**, 연세대학교 석사논문.

김철, 2003. "개인정보 보호와 정부의 역할: 통합 프라이버시보호위원회의 필요성", **행정학회 동계학술대회 발표 논문집**.

김현수 · 박춘식, 2003. "일본 개인정보보호법제 정비동향에 관한 고찰", **정보보호학회지**, 제13권 제5호.

신종철, 2001. **프라이버시 보호를 위한 규제에 대한 연구**, 성균관대학교 행정대학원

이종성, 2001. **인터넷 출현과 개인정보보호를 위한 법률적 고찰**, 연세대 정보대학원

장태우, 1998. **정보시스템 구축시 정보보호를 위한 보안체계**, 연세대 산업대학원

조인희, 2002. **정보사회의 프라이버시 침해: 중 · 고등학교 학생의 인식조사를 중심으로**, 아주대 교육대학원 논문.

2. 외국문헌

Acisp 2003 & Seberry, Jennifer (Edt)., 2003. *Information Security and Privacy*, New York: Springer-Verlag New York Inc.

Amitai Etzioni., *The limits of privacy*, New York : Basic Books.

Bennett, C. J., 1995. "Privacy protection on the information highway", *Policy Options*,6(8), pp. 43-45.

Bert-Jaap Koops, Anton Vedder., 2002. "Privacy in Criminal Investigations: A Survey: Criminal investigation and privacy: Opinions of citizens", *Computer Law & Security Report*, Volume 18, Issue 5, October, pp. 322-326.

_____, 2003. "The Shifting "Balance' Between Criminal Investigation and Privacy: A case study of communications interception law in the Netherlands", *Information, Communication & Society*, Volume 6, Number 3/September, pp. 380-403.

Cady, Glee Harrah & McGregor, Pat., 2001. *Protect Your Digital Privacy-Survival Skills for the Information Age*, Macmillan Computer Pub.

Charles D. Raab, David Mason., 2003. "Privacy, Surveillance, Trust and Regulation

The interception of communication: two studies", *Information, Communication & Society*, Volume 6, Number 3/September, pp. 377-379.

_____, 2003. "Privacy, Surveillance, Trust and Regulation Identifying people: siometric discourse identifying people: biometric discourse", *Information, Communication & Society*, Volume 6, Number 1/March. pp. 83-84.

Charlie Kaufman. & Radia Perlman & Mike Speciner., 2002. *Network security : private communication in a public world*, Prentice Hall PTR.

Chesbro, Michael., 2002. *The Privacy Handbook- Proven Countermeasures for Combating Threats to Privacy, Security, and Personal Freedom*, Paladygm Press.

Colin J. Bennett, Charles D. Raab., 1997. "The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response", *The Information Society*, Volume 13, Number 3/September 1, pp. 245-264.

Connolly, Kevin., 2003. *Law of Internet Security and Privacy*, Aspen.

David Lyon., 2002. "Everyday Surveillance: Personal data and social classifications", *Information, Communication & Society*, Volume 5, Number 2/April 01, pp. 242-257.

Davis, J. C., 2000. "Protecting privacy in the cyber era", *Technology and Society Magazine*, Volume: 19, Issue: 2, pp. 10-22.

Diffie, Whitfield & Eva Landau, Susan, 2002. *Privacy on the Line : The Politics of Wiretappiing and Encryption*, MIT Press.

Dingledine, R. & Dingledine, Roger., 2003. *Privacy Enhancing Technologies*, New York: Springer-Verlag New York Inc

Erbschloe, Michael & Vacca, John., 2001. *Net Privacy*, McGraw-Hill.

Fischer-Hubner, Simone., 2001. *It-Security and Privacy*, Springer Verlag.

Frackman, Andrew & Ray, Claudia. & Martin, Rebecca C., 2002. *Internet and Online Privacy- A Legal and Business Guide*, Independent Pub Group.

Garfinkel, Simson., 2002. *Web Security, Privacy and Commerce*, O'Reilly.

Ghosh,Anup K., 2001. *Security & Privacy for E-Business*, Wiley.

Gralla, Preston., 2002. *The Complete Idiot's Guide to Internet Privacy and Security*,

Alpha Books.

Gritzalis, Dimitris., 2003. *Security and Privacy in the Age of Uncertainty*, Kluwer.

Gutwirth, Serge & Casert, Raf (Trn)., 2002. *Privacy and the Information Age*, Rowman & Littlefield.

Haggerty, K. and Ericson, R. V., 2000. "The surveillance assemblage", *British journal of Sociology*, 51(4): 605-22.

Hunter, Richard S., 2002. *World Without Secrets Business, Crime and Privacy in the Age of Ubiquitous Computing*, Wiley.

IEEE Symposium on Security and Privacy (Cor), 2002. *Proceedings 2002 IEEE Symposium on Security and Privacy*, IEEE.

Imparato, Nicholas (Edt), 2003. *Public Policy and the Internet : Privacy, Taxes, and Contract*, Hoover Inst.

Jemmimgs, Charles & Fena, Lori., 2000. *Protecting Your Privacy and Security in the Age*, Free.

John Woulds., 1997. "Information privacy and security: A regulator's priorities", *Information Security Technical Report*, Volume 2, Issue 1, p. 7.

Klosek, Jacqueline., 2000. *Data Privacy in the Information Age*, Greenwood Pub Group.

L. Jean Camp., 1999. "Web Security and Privacy: An American Perspective", *The Information Society*, Volume 15, Number 4/November 1, pp. 249-256.

Lynn Batten, Jennifer Seberry, eds., 2002. *Information security and privacy : 7th Australasian Conference, ACISP 2002*, Springer.

Lyon, David (Edt) & Zureik, Elia (Edt)., 1996. *Computers, Surveillance, and Privacy* Minnesota: Univ of Minnesota Press.

Marcella, Albert J., 2003. *Privacy Handbook*, Wiley.

Merkow, Mark S. 2002. *E- Privacy Imperative*, Amacom.

Mizell, Louis R., 1998. *Invasion of Privacy*, Berkley Pub Group.

Neill, Elizabeth., 2001. *Rites of Privacy and the Privacy Trade*, McGill Queens Univ Press.

Nigel Hickson. (1997). "Security evaluation and certification: The future of a national scheme", *Information Security Technical Report*, Volume 2, Issue 1, p. 6.

OECD, 1994. *Privacy and Data Protection- Issues and Challenges*, Bernan Assoc.

OECD., 2003. *Privacy Online OECD Policy and Practical Guidance*, Bernan Assoc.

Othmar Kyas., 1997. *Internet security : risk analysis, strategies and firewalls*, International Thompson Computer Press.

Pfaffenberger, B., 1999. *Protect Your Privacy on the Internet*, Wiley.

Priscilla M. Regan., 2002. "Privacy as a Common Good in the Digital World", *Information, Communication & Society*, Volume 5, Number 3/September 01, pp. 382-405.

Raab, C. D., Bennett, C. J., 1994. "Protecting privacy across borders: European policies and prospects", *Public Administration*, 73, pp. 95-112.

Raul, Alan Charles., 2001. *Privacy and the Digital State- Balancing Public Information and Personal Privacy*, Kluwer Academic Pub.

Rilly, Thomas & Gillis, Robert P., 1996. *Privacy in the Information Age*, Government Technology.

Sander, Tomas (Edt)., 2002. *Security and Privacy in Digital Rights Management*, Springer Verlag.

Sandra C. Henderson, Charles A. Snyder., 1999. "Personal information privacy: implications for MIS managers", *Information & Management*, Volume 36, Issue 4, October, pp. 213-220.

Santiago, J. K. & Love, Patricia (Edt)., 1999. *Internet Privacy Protection Guide- A Navigational Aid*, Boggy Cove Pub.

Schneier, Bruce (Edt) & Banisar., 1997. *Electronic Privacy Source book*, Wiley.

Schreck, Jorg., 2003. *Security and Privacy in User Modeling*, Kluwer.

Sheizaf Rafaeli., 1996. "Who Owns Information? From Privacy to Public Access", *The Information Society*, Volume 12, Number 2/June 1, pp. 207-208.

Solove, Daniel J. & Rotenberg, Marc., 2003. *Information Privacy Law*, Aspen.

Sykes, Charles., 1999. *End of Privacy*, St. Martin's.

Tony Fitzpatrick., 2002. "Critical Theory, Information Society and Surveillance Technologies", *Information, Communication & Society*, Vol.5, No.r 3/September 01 pp. 357-378.

Turkington, Richard C. & Allen, Anita L., 2002. *Privacy Law*, West.

Whitaker, Reg & Whitaker, Reginald., 1999. *The End of Privacy- How Total Surveillance Is Becoming a Reality*, W W Norton & Co Inc.

3. 웹사이트

http://www.kisa.or.kr(한국정보보호진흥원)

http://www.kado.or.kr(한국정보문화진흥원)

http://www.kisdi.re.kr(정보통신연구진흥원)

http://www.nca.or.kr(한국전산원)

http://www.mogaha.go.kr(행정자치부)

http://www.mic.go.kr(정보통신부)

http://www.innovation.go.kr(정부혁신지방분권위원회)