시정연 2004-R-41

서울시정개발연구원 2004

서울시 전자정부의 개인정보보호에 관한 연구

변 미 리

서울시정개발연구원

시정연 2004-R-41

서울시 전자정부의 개인정보보호에 관한 연구

변 미 리

SDI 로고
서 울 시 정 개 발 연 구 원
Seoul Development Institute

연 구 진

연구책임 변 미 리 도시정보연구센타 부연구위원
연구참여 김 종 업 도시정보연구센타 연구원

시정연 2004-R-41

서울시 전자정부의 개인정보보호에 관한 연구

발 행 인 백 용 호
발 행 일 2004년 7월 31일
발 행 처 서울시정개발연구원
137-071 서울시 서초구 서초동 391
전화: (02)2149-1290 팩스: (02)2149-1319

ISBN 89-8052-373-4-93350

목 차

표 목 차

그림 차례

제1장 연구 개요

제1절 연구 배경 및 목적

제2절 연구 내용 및 방법

제1장 연구개요

제1절. 연구배경 및 연구목적

1. 연구배경

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

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.

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

---

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.

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. 연구목적

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.

제2절. 연구내용 및 연구방법

1. 연구내용

- 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 개인정보보호 법과 제도
  - 서울시 전자정부의 정보보안 현황
  - 서울시 전자정부의 개인정보 현황 분석
- 서울시 전자정부의 개인정보보호 관련 인식(시민인식과 공무원 인식 조사)
- 외국 전자정부의 개인정보보호를 위한 제도적 기제 분석
- 서울시 전자정부의 개인정보보호 정책방향과 추진전략

2. 연구방법

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.

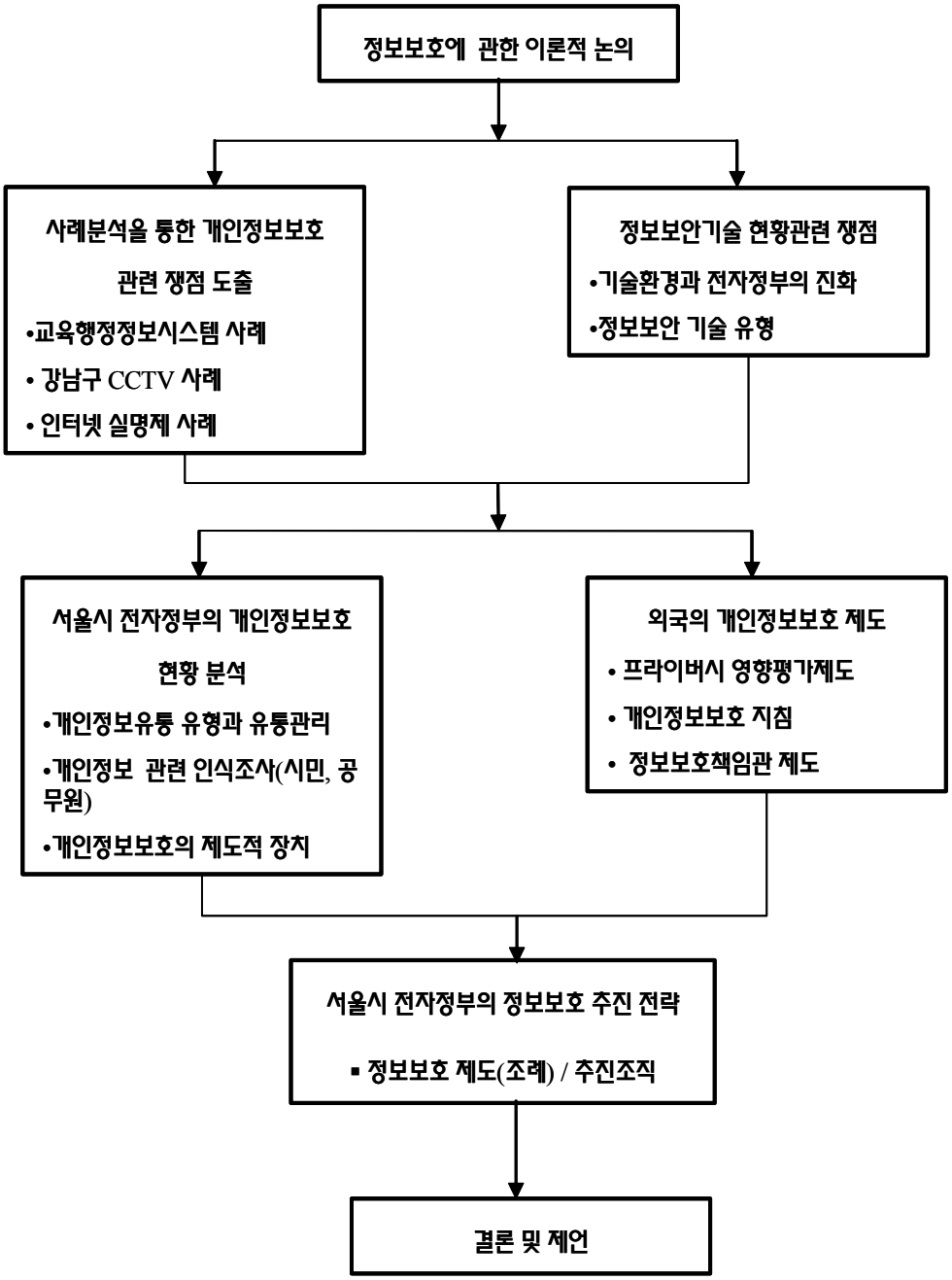
(2) 인터뷰(depth-interview) : 서울시 · 기초 자치단체 정보보호 담당자 대상

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.

3. 연구체계



<그림 1-1> 연구체계도

제2장 전자정부와 정보보호

제1절 전자정부와 개인정보보호

제2절 전자정부와 개인정보보호 쟁점사례

제2장 전자정부와 정보보호

제1절 전자정부와 개인정보 보호

1. 정보사회와 개인정보: 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(physical capital)이 정보사회에서는 지식자본(knowledge capital)으로 전화되는 정보적 생산양식으로의 변환(transformation)에 대한 논의로 이어지고 있다.

정보사회로의 이러한 변화는 일상생활을 전면적으로 바꾸고 있는데 인터넷으로 대별되는 일상생활의 혁명은 우리에게 유토피아적 이상사회를 꿈꾸게 한다. 최근 5년 사이에 일어난 변화를 그려보자. 인터넷으로 대표되는 사회구조와 조직, 커뮤니케이션 방식의 변화, 수없는 새로운 기업이 창출과 엄청난 부의 증대 등은 정보사회의 유토피아적 담론이 얼마나 매혹적일 수 있는가를 증명하는 듯하다. 이러한 변화는 공공영역에서도 지속적으로 나타나고 있는바, 전자정부의 구현은 시민들의 일상생활의 편리성을 증대시키고 정부조직의 투명성을 제고하며 조직생산성을 증대라는 긍정적 변화로 나아가고 있다. 몇날 며칠이 걸리던 행정서류의 발급(불과 몇 년 전 만 해도 호적등본은 본적지에서만 발급했던 것을 기억해 보자!)은 온라인 전자정부 사이트에서 발급되어 사용자의 프린트로 인쇄할 수 있으며, 행정서비스에 대해 의문사항이 있으면 인터넷 사이트에서 전자메일로 담당자에게 즉각적으로 질문할 수 있을 만큼 모든 것이 편리해졌다. 정보사회에서 누릴 수 있는 이러한 편이성은 우리의 상상을 훨씬 넘어서고 있다.

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 네트워크화 된 세상은 우리가 상상

하지 못할 정도의 위험이 도처에 파급시키고 있다. 네트워크의 마비로 인터넷이 불과 몇 시간만 단절되어도 사람들은 불안감과 초초를 느끼며 심리적 공황상태를 경험한다는 것이 바로 얼마 전 우리 앞에 일어난 일이다. 내가 아닌 또 다른 내가 네트워크에서 나를 행사하며 돌아다니고 있으며, 나이 통장에서 나도 모르는 사이에 돈이 빠져나간다. 나에 관한 모든 정보를 누군가가 모니터링 하는 순간 이미 나는 나의 정보에 대한 통제권을 상실하게 된 것이 아닐까?

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 사실이다. 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. (긍정적 관점과 부정적 관점에 대한 논의는 동전의 양면과 같아서 논쟁 자체는 이데올로기적 성격이 짙기 때문이다.) 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 정보사회 위험론 일반에 대한 논의는 공공조직의 정보화로서의 전자정부에도 동일하게 적용될 수 있다. 이미 언급한 것처럼 전자정부는 개인에 대한 행정서비스를 최적화하기 위한 지속적인 시도를 하고 있는데, 초기 단계의 전자정부의 오프라인 행정서비스의 온라인화를 목표로 정보시스템의 구축, 온라인 행정업무의 비율 증대 등을 실현하기 위해 노력했다. 물론 현재 단계도 이 과정이 진행 중이긴 하지만 일단 정보시스템의 확장 등 전자정부 인프라 확충에 중점을 두었다면 전자정부 발전단계를 보다 고도화시키기 위해 이제 구축된 전자정부의 활용성을 제고하기 위한 시민중심의 전자정부 서비스에 대한 논의가 활발해지고 있다. 이 과정은 정보접근성의 확장과 정보활용성의 증대로 요약할 수 있으며, 이러한 편익의 증대는 개인의 정보침해와 노출, 통제되지 않은 데이터베이스의 유통 등 정보보호와 관련된 광범위한 문제를 야기

시킨다.

기존 연구에 의하면 미국 연방정부와 주정부의 CIO를 대상으로 한 조사에 따르면, 전자정부의 진행과 함께 중요하게 대두할 정책분야로 전자상거래, 인터넷과 공공정보 접근성, 정보시스템 보안 등이 지적되었다(한국정보보호센터, 2000). 전자정부의 정보서비스의 심화는 효율성의 증대임과 동시에 개인의 정보침해에 대한 위협요인이 될 수 있는 가능성을 확장시킨다. 문제는 이러한 현상은 전자정부 발전단계에 따라 필연적으로 나타날 수밖에 없다.

전자정부 발전과정에서 행정서비스를 최대화하기 위한 최적의 상태는 공공부문이 개인에 관한 가능한 많은 정보를 집적하는 것이다. 그리고 이를 통합적으로 관리한다면 서비스를 받는 개인은 행정서비스가 필요할 때마다 정보를 제공하지 않아도 되는 편리함을 누릴 수 있다. 문제는 이 과정은 필연적으로 개인의 정보인권에 대한 침해라는 문제를 야기할 수 있다는 점이다. 민간부문의 경우 개인의 정보 제공에 대한 동의에 기반해 다양한 정보집적이 이뤄지고, 이는 고객관계관리(CRM)라는 데이터마이닝을 통해 최대한의 서비스를 제공하는데 심각한 문제를 발생시키지 않는다. 개인의 동의절차를 거쳤기 때문이다.

그런데 전자정부에서는 이러한 개인의 정보제공에 대한 동의여부가 세분화되어 있지 않는 상태이며, 공공부문이 개인에게 정부의 권리로서 강제할 수 있는 부분이 존재한다는 것이다. 국세청의 정보는 개인의 동의여부와 상관없이 국가의 정보데이터베이스에 축적되어 있다. 이러한 현황은 개인정보에 대한 위험이나 관리의 불확실성으로 파악할 수 있으며, 이는 경제학적 관점에서의 거래비용(transaction cost)의 증대를 의미한다. 전자정부의 편익을 누리기 위해 지불되어야 하는 비용으로서의 거래비용의 관점에서 접근한다면 개인정보보호나 정보보안의 문제는 기술적 관점에서의 사건이나 사고라기보다는 위험관리적 차원의 정책적 관점이 선행되어야 할 것이다. 이는 정보사회에서 필연적으로 지불해야 할 사회적 비용으로 이해하는 것이다. 더욱이 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 더

욱 강조된다고 하겠다. 따라서 전자정부의 개인정보보호를 포함한 정보보안의 문제는 하드웨어, 소프트웨어, 오르가웨어(orgaware)[3] 등의 세 차원을 동시에 고려하는 통합적 관점에서의 접근이 필요하다.

2. 정보보호의 다차원성과 개인정보 분류

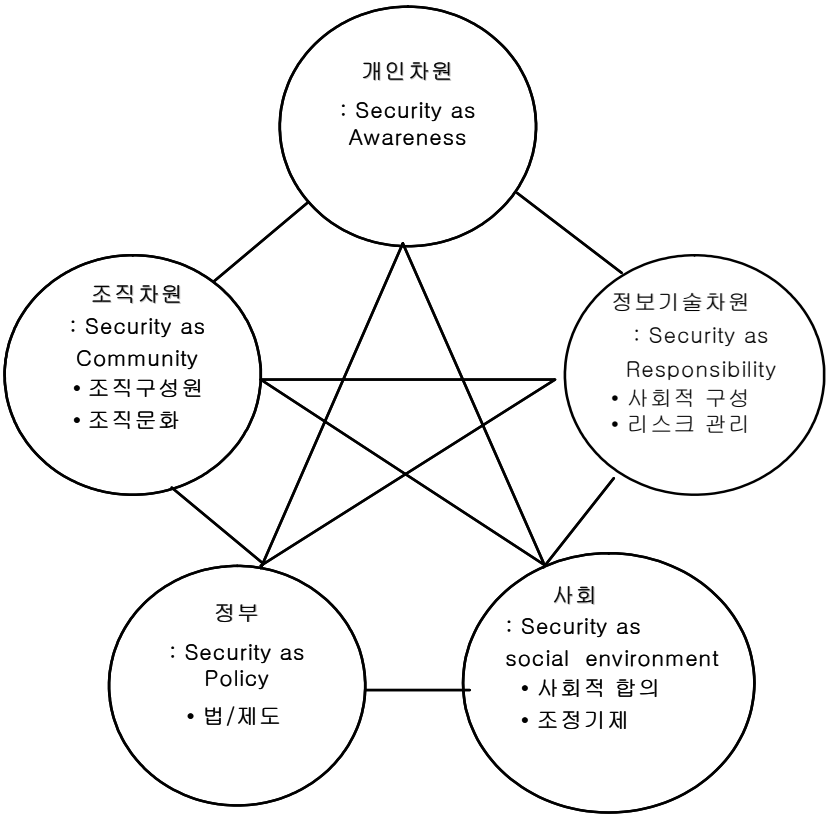
1) 정보보호의 다차원성

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). 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.

---

3) 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

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.

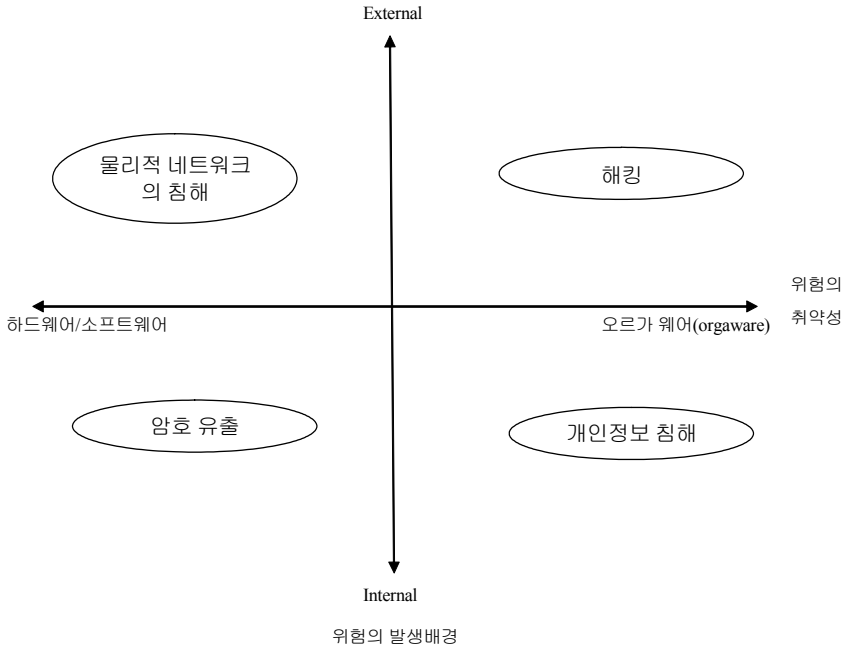
정부영역의 정보보안 접근은 주로 법제도 부문에서 나타날 수 있다. OECD(2003)가 전자정부의 장애요인으로 들고 있는 첫 번째 항목이 법·제도적 요인임을 고려한다면 특히 전자정부의 동태성을 고려한 법·제도적 측면의 정보보호에 대한 접근은 중요요소이다. 우리가 이후 논의할 것이지만 서울시 전자정부 역시 전자정부 발전단계에 조응하는 정보보호를 위한 법·제도적 대안의 제시 역시 이 측면을 고려한 것이다. 마지

막으로 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 일면적으로 이해되어서는 안되며 각 행위주체들의 관점을 포괄하는 전체적 관점을 견지할 때 바람직한 정책방향이 도출될 것이다.

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



<그림 2-2> 정보보안에서의 개인정보보호의 위상

of Threat)이라는 한축과 위험의 취약점(Focus of Vulnerability)이라는 또 다른 축을 기준으로 정보보안 유형을 구분한 것이다. 가로축은 위험의 취약점이 하드웨어 혹은 소프트웨어에서 있는 것인지, 아니면 오르가웨어(각주 3 참조) 쪽에서 발생하는지를 기준으로 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.

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 조직원의 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 보편

화된 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).

(1) 관리주체별 분류

관리주체별 분류에서는 개인정보는 크게 공공개인정보와 민간개인정보로 나뉜다. 공공개인정보를 공공기록, 정보주체로부터 직접 수집한 기록과 정보주체 이외의 자로부터 수집한 기록 등으로 구분하기도 한다(황인호, 2001). 그러나 공공부문과 민간부문으로 구분하는 것 이외에는 의미가 적다고 볼 수 있다. 공공기록이라는 것은 결국 개인정보보다 더 큰 범주에 속하며 직접 또는 간접 수집은 수집경로에 다른 분류일 뿐 모두 공공기록의 범주 내에 있는 것이기 때문이다.

공공개인정보는 수집단계에서부터 각종 법적 근거에 의하여야 하는 정보인데 비해 민간개인정보는 원칙적으로 당사간의 계약에 의하여 수집, 취급, 활용되는 정보이다. 개인정보보호에 있어서도 공공부문은 국가권력으로부터 개인 사생활의 안저한 보호가 주요 목적이 되며 정보사회에서 중요한 개인정보에 대한 국가의 부당한 침해를 방지하는데 그 목적이 있다고 할 수 있고, 반면에 민간부문에서는 개인정보에 재산적 가치를 인정하여 이를 처분할 수 있도록 하는 것이다.

공공부문의 관리주체별 분류체계는 논리적으로 개별 행정주체별 체계에 연동될 수밖에 없다. 부문별 행정기관이 모두 개인정보를 취급하는 주체이기 때문이다. 따라서 엄격히 분류하자면 행정분야로서 행정자치부의 소관업무[4]에 해당하는 일반적 공공개인정보 이외의 분야별 개인정보는 모두 그 주체별 개인정보로 분류될 수 있을 것이다.

민간부문의 개인정보는 거래관계에 따라 다양하게 나타나지만 대개 개인정보를 제공하고 반대급부를 받는 정보주체에 대한 보호차원에서 규제가 이루어진다. 따라서 이에 대한 분류에서도 규제가 필요한 위험영역을 어떻게 설정하느냐의 문제로 되고 그 기준은 관리주체의 사업영역으로 한다. 대표적으로 신용정보, 의료정보, 통신정보, 인터넷거래정보, 고용 및 근로정보 등을 예로 들 수 있다.

이러한 분류체계와 위험도가 사회적으로 부각되는 시점에 따라서 관련 개인정보입

4) 이는 개별부처의 업무가 아닌 분야로서의 일반행정분야가 될 것이다.

법이 이루어져 왔다. 그러나 아직도 공공부문의 경우 교육・국방・보건복지・국세・사법행정 등 고위험군의 개인정보처리에 대한 구체적 규정사항은 상세 절차까지 명확하게 정리하지 못하고 있고 의료정보나 고용 및 근로정보 등에서 대해서는 관련 입법이 미비한 상황이다(김일환, 2004).

(2) 성격별 분류

개인정보를 민감도에 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. 대체로 개인 신분이나 가족에 관한 기본적인 인적 사항을 제외하고 나면 개인정보는 인격적 특성과 재산적 특성을 동시에 가지고 있는 경우가 대부분이라서 이러한 개념적 구분에 따라 모든 개인정보가 명확히 분류되는 것은 아니라고 본다(황인호, 2001).

(3) 내용별 분류

개인정보를 그 내용에 따라 분류하면서 구체화시킨 연구는 비교적 근간에 이루어진 일이다. Weible(1993)는 개인종보를 비교적 상세히 구분했는데, 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
습관/취미 정보	흡연량, 음주량, 취미의 종류, 여가활동, 도박성향, 비디오 대여기록 등

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

<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

5) 행정자치부로 통합되기 전의 총무처에서 분류함.

한편 2002년 영국의 정보위원회 사무국[6]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, 사회환경	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 시도한바 있다. 이 위원회에서는 영국 정보위원회의 분류체계를 대체로 따르고 있으면서 한국의 실정에 맞게 분류체계를 보다 광역화하고 하였다(정부혁신지방분권위원회, 2004).

6) Information Commissioner's Office.

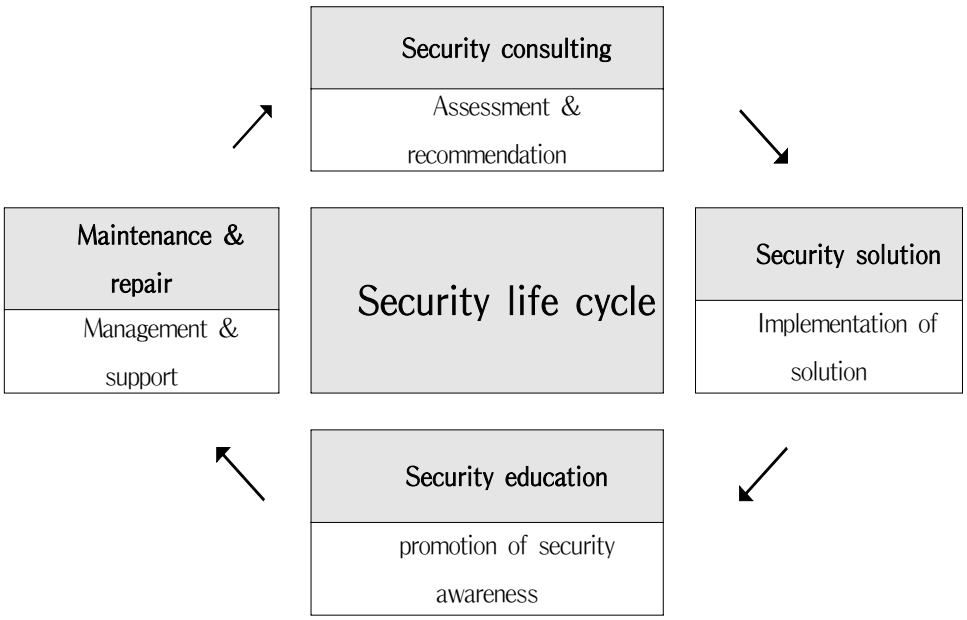
<표 2-4> 정부혁신지방분권위원회의 개인정보 분류표

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. 정보보안기술의 유형과 발전

1) 정보보안기술의 생애주기(life cycle)

정보기술의 발전과정을 살펴보면 정보보안기술의 실행(implementation)은 일회적으로 완성, 소멸되는 것이 아닌 일련의 과정으로 파악된다. 다시 말하면 정보보안기술의 실행은 한번의 임무가 아니라 지속적인 과정으로 볼 수 있으며 이는 정보기술을 생애주기 측면에서 이해해야 함을 뜻한다. 이러한 접근에서 파악된 효과적인 정보보안시스템은 <그림 2-3>과 같다.



<그림 2-3> 효과적인 정보보안시스템 생애주기

정보보안시스템의 생애주기는 보안컨설팅→보안솔루션→보안교육→시스템 유지·보수라는 일련의 순환과정을 거친다. 보안컨설팅 단계에서는 정보시스템에 대한 객관적 평가를 통해 적절한 보안시스템을 선정하며, 이렇게 선정된 보안시스템이 실제 이행되는 단계가 보안 솔류션 단계이다. 이 단계에서는 실제 보안시스템이 적용되는 과정이다. 선정된 보안시스템은 보안교육 단계를 거치면서 보안에 대한 인식이 진전되면서 정보보안시스템에 대한 이해가 제고된다. 이후 유지·보수단계에서는 시스템에 대

한 관리가 이뤄지며 이러한 유지관리 과정을 통해 정보보안시스템에 대한 신뢰가 구축될 수 있다. 어떠한 정보시스템의 보안시스템은 이러한 과정을 반복하면서 새로운 정보기술환경 변화에 대응력을 키우게 된다.

보안 제품들을 선택하고 실행 동안에 대부분의 보안 제품 공급자(vendor)들은 정보보안 생애주기의 실행 측면에 초점을 맞추는 경향이 있고, 많은 투자를 하고 눈에 띄는 변화를 나타내는 곳에 제품 실행 전략이 있어야 한다. 이를 위해서는 먼저 기술적인 면을 고려할 필요가 있다. 적인 면이다. 방화벽이나 백신 소프트웨어 같은 기본적인 보안 제품들의 설치(deployment)는 정보보안 시스템 이해의 체제에서 중요한 출발점이다. 둘째, 관리자의 역할이다. 기본 보안 제품들의 효과와 성과는 네트워크 관리자에게 적절한 유지와 관리를 의존하게 하고, 뿐만 아니라 조직의 모든 수준에서 정보보안의 중요성에 대한 인식을 가지게 해야 한다. 셋째, 일반적인 정보보안에 대한 인식이다. 네트워크 환경의 지속적인 변화와 복잡하고 불가능하며 예측이 어려운 보안 위험요소들의 증가에 따라, 주기의 각각 단계에서 적절한 제품을 사용하는 것이 필수적이다.

2) 정보보안기술의 유형

정보보안은 네트워크 환경 내에서 비즈니스 정보와 서비스의 전달이 허용되는 안전한 솔루션들의 기본적인 서비스에 의존하고 있다. 주요 정보보안 기술을 살펴보면 <표 2-5>와 같다.

<표 2-5> 정보보안기술의 유형

종류	기술의 정의
사용자 인증	- 사용자의 신원을 증명하는 것으로 정보시스템에서 정보의 생성, 전송, 처리 등의 행위에 관여한 사용자를 보증하는 것
Access control	- 적합한 인증과 접근 권한을 함께 가진 개인에게만 접근을 허락하는 것
기밀성 (Confidentiality)	- 데이터가 인증되지 않은 부분을 드러내지 않는 것과 encryption(부호매김)/decryption 기술들은 정보를 약속한 수신자만이 단지 이해할 수 있게 하는 방법
무결성(Integrity)	- 인정받지 않는 데이터의 modification과 alteration에 대비하여 보호하는 것
부인방지 (Non-repudiation)	- 메시지의 송신자나 수신자가 메시지를 송신한 사실이나 수신한 사실을 부인하지 못하도록 막는 것
가용성(Availability)	- 정보와 데이터를 인정받은 사용자가 이용할 수 있게 보증하는 것
암호(Cryptography)	- 텍스트와 숫자뿐만 아니라 음성・이미지・동화상 등 모든 전자적 형태의 문서를 숨기는 기술로서 가장 보편적인 보안기술
데이터 마이닝 (Data Mining)	- 대량의 데이터 사이에 묻혀 있는 패턴을 발견하고 규칙을 추론함으로써, 의사결정을 지원하고 그 효과를 예측하기 위한 기법
사회관계망 분석	- 지식 관리 향상, 컴퓨터 바이러스 확산에 대비한 보안 구축, 시장 분할 및 침입자 식별하는 방법
생체인식	- 개인의 생리학적 혹은 행동학적 특성을 측정하고 분석하여 이에 따라 확인・식별하는 자동화된 방법

첫째, 사용자 인증(Authentication)이다. 사용자 인증은 사용자의 신원을 증명하는 것으로 정보시스템에서 정보의 생성, 전송, 처리 등의 행위에 관여한 사용자를 보증한다. 사용자 인증은 사용자만이 가지고 있는 것(예를 들면, 토큰, 스카트 카드 등), 사용자만이 알고 있는 것(패스워드, PIN), 사용자만이 유일하게 지닌 것(지문, 홍채 등의 생체인식) 등이 있다.

둘째, Access control이다. 적합한 인증과 접근 권한을 함께 가진 개인에게만 접근을 허락하는 것, 패킷(한 번에 전송하는 정보 조작 단위) 필터링 또는 인증 체계들은 일반적으로 시스템과 데이터에의 접근 제어에 사용되고, 접근 제어 정책들은 조직의 정보보안 정책에서 규정된다.

셋째, 기밀성(Confidentiality)이다. 기밀성은 데이터가 인증되지 않은 부분을 드러내지 않는 것과 encryption(부호 매김)/decryption 기술들은 정보를 약속한 수신자만이 단지 이해할 수 있는데 이용되고 있다.

넷째, 무결성(Integrity)이다. 무결성은 인정받지 않는 데이터의 modification과 alteration에 대비하여 보호하는 것과 문서를 작성한 사람 이외의 어떤 사람도 그 문서를 변조하거나 위조할 수 없고, 암호화되어 수신자에게 보내지므로 송신된 전자문서와 비교되기 때문에 두 문서가 동일하지 않다면 송수신 과정에서 위·변조되었음을 알 수 있다. 즉 생성키를 소유한 사람이 아닌 어느 누구에 의해서도 문서가 변경되거나 위조될 수 없다는 것을 의미한다.

다섯째, 부인방지(Non-repudiation)이다. 부인방지는 메시지의 송신자나 수신자가 메시지를 송신한 사실이나 수신한 사실을 부인하지 못하도록 막는 것과 발신부인방지(Non-repudiation of Origin)과 수신부인방지(Non-repudiation of Receipt)가 사용되고 있다.

여섯째, 가용성(Availability)이다. 가용성은 정보와 데이터를 인정받은 사용자가 이용할 수 있게 보증하는 것으로서 공격자가 서버에 과부하를 주기 위해 공격하고, 이로 인해 shut down 되는 원인이 되고, 서버를 이용하지 못하게 하는 것이다. 예로서 정보위협이 있다.

일곱째, 암호(Cryptography)이다. 암호는 텍스트와 숫자뿐만 아니라 음성·이미지·동화상 등 모든 전자적 형태의 문서를 숨기는 기술로서 가장 보편적인 보안기술로서 폭넓게 이용되고 있다.

여덟째, 데이터 마이닝(Data Mining)이다. 데이터 마이닝은 대량의 데이터 사이에 묻혀 있는 패턴을 발견하고 규칙을 추론함으로써, 의사결정을 지원하고 그 효과를 예측하기 위한 기법이다. 예를 들면, 마이닝의 결과로 어떤 고객은 다른 고객에 비해 특정 상품을 더 잘 구매하는 경향이 있다는 사실을 알아낼 수 있다. 기업은 이 두 유형의 고객에 대한 차이를 알게 됨으로써 불특정 대중이 아닌 목표 고객에 집중된 마케팅을 수행할 수 있을 것이다.

아홉째, 사회관계망 분석이다. 이것은 분석 도구, 시각화(visualization), 보완 기술 및 데이터 가용성 덕분에 사용이 보편화되고 있다. SNA는 지식 관리 향상, 컴퓨터 바이러스 확산에 대비한 보안 구축, 시장 분할 및 침입자 식별 등에 사용된다. 사법 당

국, 공중 보건 분야에서 활용되고 있다.

열번째, 생체인식이다. 생체인식은 개인의 생리학적 혹은 행동학적 특성을 측정하고 분석하여 이에 따라 확인·식별하는 자동화된 방법이다. 이것은 얼굴인식, 지문, 음성, 홍채, 망막, 손금, 서명, 정책, 키스트록(Key stroke), 걸음걸이, DNA 등 인간의 생리적 혹은 행동학적 특성을 모두 포괄한다.

그밖에 다른 보안 제품들은 보안 메커니즘들의 결합을 통하여 다양한 보안 위험들의 운용을 할 수 있어야 한다. 예를 들어, 방화벽은 인증과 허가뿐만 아니라 데이터의 기밀성과 무결성이 허락되며, 전자서명(Digital signature)은 무결성과 부인방지를 보증하고, 전자인증(Digital certificate)과 ID/패스워드는 인증에서 이용된다. 보다 확실한 정보보안 시스템을 구축하기 위해서는 조직의 활동과 정보보안 요구에 따라, 여러 가지 보안제품들의 적절한 조합을 통해 보안시스템을 실행해야 그 효과가 클 것이다.

3) 정보보안기술의 발전방향

인터넷이 빠르게 발전하면서 정보보안 산업은 새롭고 성장 가능한 산업분야로 등장하고 있다. 가트너 그룹(Gatner Group)에 따르면, 2001년에 세계적으로 IT 소비는 하드웨어와 소프트웨어에서 각각 13%와 1%롤 감소하였다. 하지만 재정분석가들은 2001년부터 2006년까지 정보보안 부문에서의 소비가 매년 19%의 성장률로 증가할 것으로 예상한다. 정보산업의 규모가 커지고 사용환경의 변화에 발맞추어 정보보호 기술은 본래의 기능에 충실하면서 설치, 관리의 편의성, 확장성을 도모하는 방향으로 발전하고 있다. 이러한 방향은 기능의 확장, 표준화, 통합화 등의 방향으로 정보보안기술이 발전하고 있음을 의미한다.

많은 보안 기술들이 상용화되었고, 보안 제품들은 현재 높은 성과가 있으며 다양한 보안 요소들을 통합한 다기능 제품들이 있는데 PKI 사용자는 EAM를 포함하여 적용 서비스의 범위를 넓히고 있다. PKI(공개키 기반구조)는 전자서명을 사용하기 위한 기술적·운영적 토대를 제공해 주는 핵심 보안기능이다. 사이버상의 전자적 거래에서 일반적으로 사용되는 패스워드보다 더욱 안전한 보안 기술을 제공해 준다. 또한 다양한 보안체계를 통합 관리하는 통합인증관리(EAM) 기술을 통해 기존에 비해 강화된 응용 프로그램 보안수준을 갖추게 하는 시스템으로 여러 개의 ID를 갖고 있는데 따르는 비

밀번호 유출 위험도 줄여준다. 즉, 기능의 확장 측면에서 보면 단순한 사용자 인증으로 사용되던 공개키 기반에서 권한관리까지 가능한 PMI로 발전하고 있다. 표준화 영역의 경우 IDS의 경우 특정 시스템뿐 아니라 일반 시스템에서도 보안사항을 확인할 수 있도록 하는 표준화방안으로 나아가고 있다. 통합화 경향은 비단 정보보호기술의 발전방향에만 국한되는 것은 아니며 IT기술 자체가 개별시스템에서 통합관리 시스템으로 나아가는 방향과 궤를 같이하고 있는 것으로 판단된다.

제2절. 전자정부와 개인정보보호 쟁점 사례

1. 교육행정정보시스템(NEIS) 사례

1) 개요

(1) NEIS의 추진배경과 사업목표

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 시스템을 말한다.(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.

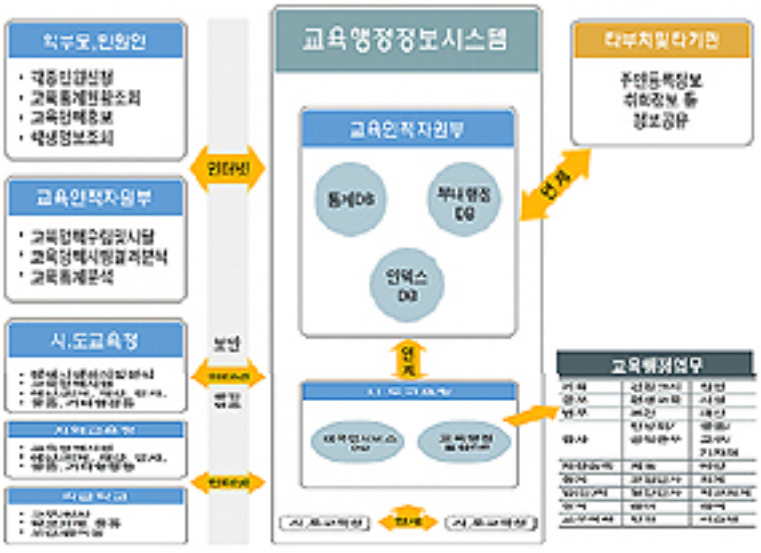
NEIS가 구현하고자 한 사업목표는 먼저, 교원의 업무경감 및 교육활동 전념을 통한 교육의 질 향상이다. 교원의 통계작성 등 단순 반복적인 행정업무를 전산처리하고, 복잡 다양한 업무를 표준화하여 일상적인 잡무를 줄이는 것이다. 둘째, 인터넷을 통한 학부모와의 정보공유로 가정과 학교의 만남의 활성화이다. 인증보안이 적용된 인터넷을 이용하여 자녀의 성장 관련 자료를 안방에서 온라인으로 열람할 수 있어, 자녀의 학교생활 문제점을 조기 발견, 상담을 통해 문제를 해결하는 것이다. 셋째, 서비스의 획기적 개선을 통한 대국민 만족도 제고이다. 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.

(2) NEIS의 구성과 내용

NEIS는 시·도교육청 및 교육인적자원부에 시스템을 구축하고 모든 교육행정기관 및 초·중등학교를 인터넷으로 연결하여 단위학교 내 행정처리는 물론 교육행정기관에서 처리해야 할 학사, 인사, 회계 등 교육행정 전반업무를 전자적으로 연계하는 시스템이다.

NEIS의 27개 영역 중 교무/학사 영역 중 학적, 성적, 학생생활기록부, 학생생활업무와 보건 영역 중 건강기록부 및 보건통계업무, 그리고 물품, 예산, 회계업무 등을 제외하면 NEIS로 개발되면서 새롭게 포함된 내용이라 할 수 있음다. 학교종합행정정보관리시스템(CS)는 교원용 PC와 Server를 교내 전산망으로 연결하여 자료를 종합하는 방식으로 학교생활기록부를 비롯한 일선학교의 교무업무 전체를 종합적으로 전산처리하는 시스템으로서 1998~2001년까지 보급이 완료되었다



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

<그림 2-4> NEIS 관리체제

하지만 두 가지 문제점이 대두되었다. 첫째, 정보의 과다집중이다. 기존의 CS에서 집적되었던 학적관리, 학생생활기록부 등의 내용이 NEIS로 옮겨짐에 따라 교무수첩, 학생면담, 건강기록 등 행정에 불필요한 개인신상관련 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.

(3) 개인정보보호와 관련한 대립과정

NEIS는 2002년 10월 개발을 완료하고 2003년 3월 전면시행을 앞두고 인권침해 등의 이유로 교육인적자원부, 전국교직원노동조합(이하 전교조로 함), 시도/지방교육청, 학부모, 일선 정보담당교사들간에 갈등이 고조되었다. 2002년 10월 조기개통을 앞두고, 2002년 8월 27일 전교조에서 전언론기관에 NEIS사업에 대한 보도자료를 배포하고, 교무/학사 영역 시행에 대해 교원단체들이 시범기간 연장 및 시스템 개선을 건의했다. 교육부는 전자정부 특위 사업의 추진 일정상 시범기간 연장이 불가능한 입장이었으나, 2002년 9월 교원단체와의 협의결과 본격서비스를 2002년 10월에서 2003년 3월로 연장하고 2003년 2월까지 시범운영기간을 갖기로 하였다. 시범기간 중 교육미비에 대한 대책으로 교무/학사부문에 대한 비디오 및 CD(120분 분량) 제작, 일선학교 배포, 온라인 교육강화, 학교 자체교육 내실화, 자문교사단(200명) 활성화 등을 수행하며, 교육전문지와 기타언론기관을 통해서 홍보도 실시했다. 2003년 3월 서비스 재개통을 앞두고 2월 19일 전교조 등 교육·시민단체가 국가인권위에 NEIS 관련 진정서를 제출하였으며, 교육부는 3월 학생정보를 15개에서 5개로 줄이고, 학부모를 15개에서 3개로 입력항목을 줄이면서 교무/학사 등 3개 영역을 개통하였다.

전교조와 교육부가 NEIS의 강행문제를 놓고 대립하는 중에 국가인권위가 개입하고, 교육부총리는 2003년 5월 12일 국가인권위원회의 권고사항[7]을 수용함으로써 NEIS에 대한 재검토 결정을 내렸다. 하지만 교육부 내부직원, 전국교장단, 각 학교 정보담당교사, 학부모, 정치권 등으로부터 CS 이전체제로의 복귀에 대하여 강력한 반대에 직면, 큰 혼란이 거듭되었다. 이에 6월 1일 다시 일선학교 차원에서 자율적으로 결정하라는 새 지침을 발표하였지만 전교조, 교총 모두가 반발하였다. 전교조는 6월 21일 NEIS 반대를 위한 연가투쟁을 통해 교육부의 NEIS 시행에 반대하였고 전교조 간부가 구속되면서 사태는 더욱 악화되었다. 이로 인해 실마리를 찾지 못하던 NEIS 문제는 8월11일 국무총리 산하 교육정보화위원회의 이세중 위원장은 “중립적 입장에서 교육행정정보시스템(NEIS) 문제를 원점에서 재검토하겠다”고 발표했다.

이렇게 끝이 없어 보이던 논쟁은 NEIS의 재검토를 위해 설치된 교육정보화위원회

7) 인권위 결정은 NEIS 중 교무/학사, 보건, 입(진)학 영역 제외하고, 제외영역은 CS를 보완하여 적용하라는 것임.

<표 2-7> NEIS 구축과정에서의 대립

단 계	시 기		내 용
시스템 구축	2002년	8월 27일	-전교조 보도자료 배포 -교원단체: 교무/학사 영역 시행에 대해 시범기간 연장 및 시스템 개선 건의
		9월	-교육부와 교원단체의 협의: 시범운영기간 연장
↓			
시스템 1차 개통	2002년	10월 - 2003년 2월	-시범기간 중 교육미비에 대한 대비책 마련
↓			
대립 시작	2003년	2월 19일	-전교조 등 교육·시민단체: 국가인권위에 진정서 제출
↓			
시스템 2차 개통	2003년	3월	-교육부: 학생정보를 교무/학사 등 3개 영역 대상으로 NEIS를 개통
↓			
대립 고조	2003년	5월 12일	-교육부총리: 국가인권위의 권고사항을 수용하면서 NEIS에 재검토 결정 -교육부 공무원, 전국교장단, 각학교 정보담당교사의 반발
		6월 1일	-NEIS로의 전환을 일선학교의 자율에 맡긴다는 지침 발표. 교원단체 반발
		6월 21일	-전교조의 연가투쟁과 전교조 간부구속. 사태악화
↓			
대립 수습	2003년	8월 11일	-교육정보화위원회의 NEIS 재검토 발표
		9월 8일	-교육정보화위원회에서 정상화에 합의
↓			
2차 대립	2003년	9월 17일	-NEIS에 관한 찬·반 토론개최: 서로의 입장차이로 원점으로 돌아감
↓			
수습 및 재개통	2003년	12월 15일	-국무총리실 정보화위원회: 교무/학사, 보건, 진/진학 3개 영역을 제외하고 NEIS 운영하기로 함, 별도의 독립기구 설치에 합의 -전교조의 정부방치 수용으로 문제해결

전체회의가 9월8일에 정부 종합청사 대회의실에서 이세중위원장 주재로 열렸고, 이를 통해 전교조, 참교육학부모회, 참여연대, 민변의 위원 추천 거부로 파행 운영돼오다 2개월만에 정상화되면서 해결의 실마리를 보이게 되었다. 하지만 9월17일의 NEIS와 관

련한 찬·반 토론회에서는 'NEIS의 효율성과 CS보다 높은 보안성을 이유로 당연히 시행해야 한다'는 찬성론자와 '자기정보에 대한 인권문제를 원칙'을 내세운 반대론자의 대립으로 원점으로 돌아갔다. 해결이 불가능해 보이던 NEIS 문제는 12월 15일 국무총리실 정보화위원회 회의에서 교무/학사, 보건, 진/입학 등 3개 영역을 제외하고 NEIS를 운영하기로 함. 별도의 독립적 감독기구의 설치, 보안성을 높이기 위한 자료의 암호화 등을 결정하였고, 이를 전교조가 정부의 최종방침을 수용하면서 문제는 해결되었다.

2) 쟁점과 갈등관련[8] 행위주체

(1) NEIS와 관련된 쟁점사항

NEIS와 관련해 논쟁을 불러일으킨 주요 내용은, 개인정보침해, 일방적인 추진과정, 행정효율성 우선의 추진, 법적 근거 미비, 교원통제 문제, 교원잡무증가 등의 많은 쟁점이 있었다. 여기에서는 일방적인 사업추진, 미약한 개인정보보호, 기술우선·행정효율성 우선의 추진을 중심으로 살펴보겠다.

① 전자정부 출범에 맞추기 위한 무리한 사업추진

교육부는 2002년 11월 전자정부의 출범에 따른 NEIS를 통한 서비스를 함께 하려는 무리한 일정에 맞추기 위해 관련주체 및 대국민 설득 작업과 이해를 구하는 노력이 없었다. 먼저 NEIS의 목표 중 교원의 행정업무를 경감하고 학부모에게 다양한 정보를 제공한다는 취지가 있었으나, 교육관련 다양한 계층에 대한 홍보가 부족하였다. 또한 정보수집의 대상인 학생, 학부모, 일선교사들로부터의 의견청취노력이 부재하였고, 주로 정보담당교사들을 중심으로 의견수렴이 진행되었다.

NEIS 반대의견에 대한 검토 미비. 전교조 등이 제기한 시범기간을 좀더 연장 실시하거나 전면개통을 연기하는 방안이 적극 검토되지 못하였다. 문제의 조기발견 및 보완 운영을 위해서라도 전국 확산 전 시범운영을 보다 연장·운영했어야 하고, 우선 시범학교를 중심으로 하드웨어가 보급되었어야 하며, 시스템 구축과 운영이 안정화된 이후에 CS에서 NEIS로 업무를 전환하는 등 전자정부 백서에 나온 원래의 시범운영기간

8) 황주성·최선희(2003), "전자정부 사업과 개인정보보호 이슈"를 중심으로 재구성.

(2004년 2월까지)을 철저히 지켰어야 했으나 전자정부 서비스에 맞추기 위한 일정을 내세워 이를 무시하고 무리하게 사업을 추진하였다.

② 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 검토하였다.

인권위는 사생활의 비밀과 자유 침해 여부에 대해 헌법 제10조, 제17조, 제37조제2항의 근거에 따라 개인정보의 수집은 적법한 권한이 있는 기관에서 하되 침해우려가 있는 경우 수집하여서는 안됨을 제시했다. NEIS 정보집적의 법적근거 여부는 초·중등교육법 제25조, 교육기본법 제23조제2항에 근거하여 학교에서 수집한 학생관련 개인정보를 16개 시도교육청 서버에 집적 관리하는 NEIS 법적근거를 불분명하다고 밝혔다. 이는 민원사무처리에관한법률 제5조제1항, 법시행령 제11조제2항에 근거하여 학교에서 수집 작성된 개인정보를 NEIS에 집적하는 법적 근거의 모호성의 제시되었다.

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 권고함. 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	×

③ 행정효율성 우선의 사업추진

NEIS에 대한 BPR 결과 검토 당시 교사, 학부모 등 관련 당사자의 참여가 있었다면 논란은 정책결정 되는 단계에서 상당부분 예방되었을 것이다. 하지만 사업추진의 효율성 측면에서 시급한 사업추진이 논의되면서 이러한 절차를 무시하고 행정의 효율성에 우선하여 사업이 추진되었다. 초기에 교육행정정보화 사업추진단은 BPR 결과에 의해 16개 시도교육청 중심으로 서버를 운영하는 통합안과 연계안을 모두 검토하였다.

당시 통합안에 대해 시도교육청과 각 학교는 대체로 찬성하고 있으나, 교육부 담당부서(정보화지원담당관실)는 반대하였다. 법/제도도 함께 변경해야 하는 어려움과 학교의 정보에 대한 보유·유지·관리의 책임은 1차적으로 교장에게 있으므로 통합안으로 결정될 경우 책임소재가 불분명하다는 점 때문이었다. 이에 따라 교육부는 BPR 결과 보고서 내용을 수정 요구하며, 계획서 상 통합시스템 구축을 분산구축으로 수정하고, 기존 보급된 시스템의 연계방안을 요구하였다.

<표 2-10> 통합안과 연계안의 비교

구분	NEIS로 통합안	CS와 NEIS의 연계안
업무처리방식	· 통합시스템 1개로 각급기관 사용 애플리케이션만 사용 · 처리	· 업무에 따라 학교정보시스템과 교육행정시스템 이원화
시스템 구조	· Web기반 시스템으로 서버 및 데이터는 시도교육청에 존재 · 데이터의 온라인 확인가능	· Web 방식과 CS 방식의 혼재 · 서버 및 데이터의 물리적 위치 이원화 · DB간 정기적인 데이터 일원화 작업 발생
구축방식	· 기존 학교정보시스템 데이터 변환 · 학교정보시스템 업무처리로직 재개발	· 교육행정정보시스템 개발 및 기존 학교정보시스템 기능보완 필요(개발주체가 이원화될 가능성 상존)
시스템운영	· 시도교육청별 소수 유지보수팀 운영(학교단위 관리자 불필요)	· 시도교육청별 유지보수팀 및 학교단위 유지보수자 필요
데이터 및 시스템 보안	· 장애 및 보안관련 사고시 파급영향이 심각(시도단위 장애 발생가능)	· 해킹의 가능성 많음
사용자 환경	· 1개 시스템 사용법 습득 · 개인 PC디스크 자원 활용	· 2개 시스템 사용법 습득 · 개인 PC디스크 자원 점유
프로그램 유지보수	· 시도교육청 단위의 유지보수 · 프로그램 배포 불필요	· 유지보수 · 프로그램 변경시 학교단위 배포 어려움

그러나 NEIS 구축 사업이 전자정부 11대 사업으로 선정되면서 행정효율성 측면에서 전자정부의 비전 · 추진원칙에 따라 통합안을 수용하게 되어다. 연계안대로 각 학교에 서버를 두는 경우 법, 제도, 절차 등의 변경사항이 발생할 경우, 전국 1만여 개의 각 학교에 변경요청을 해야 하는 비효율을 초래했다. 학교별로 각각 서버를 구축한 경우 정보의 안전한 유지 · 관리를 위한 백업시스템 구축에 기술적으로 한계가 많고, 보안시스템 설치에 많은 노력과 비용이 소요된다는 지적이 있었다.

BPR 결과에 따라 통합안과 연계안을 비교할 때, 교육주체와 대국민의 의견수렴 과정을 거쳤다면 개인정보보호 문제에 대한 논란을 예방할 수 있었지만 그러한 노력이 이루어지지 않았다. 또한 NEIS로의 결정 이후에도 충분한 시간적 여유를 가지고 사업추진을 했어야 하나, 전자정부 사업추진 일정상 2002년 10월까지 11대중점사업의 완료화를 계획함에 따라 충분히 의견 수렴할 시간적 여유가 없었다.

(2) 갈등관련 행위주체

NEIS 도입문제와 관련한 갈등의 주체는 교육인적자원부, 국가인권위원회, 전교조, 시민단체(참교육학부모회 등), 전국교장단, 학부모 등이 있다.

① 교육인적자원부(시도교육청 포함)

NEIS 구축의 주무부처로서 시스템 도입·구축과 관련한 갈등 원인의 제공자이다. 학교종합정보관리시스템(CS)로 업무를 처리하던 것을 전국적인 네트워크인 NEIS 체제로 바꾸기 위해 교육관련 주체들과의 합의 없이 일방적인 사업을 추진했으며, 전자정부 서비스의 일정에 맞추기 위해 충분한 시범운영을 통한 문제해결을 하지 못하였다.

NEIS 구축 후 시범운영, 전면시행 과정에서 일관성 없는 정책의 추진하여 갈등을 증폭시켰다. 교육주체들의 찬성과 반대에 대해 정책 혼선을 빚었다. 또한 논란에 대한 해결 의지의 부족인데 NEIS 전면 시행에 대한 찬·반에 대해 문제해결을 위한 책임 있는 자세가 부족했다.

② 국가인원위원회

NEIS가 가지고 있는 개인정보침해에 시정을 권고하는 등 적극적 중재자 역할을 하였다. 전교조와 시민단체 등의 개인정보침해와 관련한 진정서를 바탕으로 문제점을 지적하였다. 하지만 NEIS와 CS의 병행을 권고하는 등 때늦은 논란을 야기 시켰고, 정보인권의 측면에서의 문제제기를 통해 NEIS에 근원적인 의문을 가지게 하였다.

③ 전교조

NEIS의 도입·구축에 가장 적극적으로 반대하였다. 개인정보침해에 대한 문제를 제기하였고, BPR, 시범운영기간 등에 대한 교육인적자원부의 일방적인 결정에 이의를 제기하면서 쟁점화 시켰다.

제 교육주체들의 참여를 통한 해결을 요구했는데, NEIS 입력대상, 정보침해에 대한 보호조치, 독립적인 감독기구 구성 등에 참여를 요청하고 교육인적자원부와 직접적인 대화를 통한 논란의 종식을 원하였다. 또한 요구사항의 관철을 위해 연가투쟁, 대 국민 홍보 등의 방법을 통해 문제해결 의지를 보였다.

하지만 지나친 반대로 학사일정에 차질을 주어 대학입학전형을 위한 성적처리를 어렵게 하였다.

④ 교총/전국교장단/일선학교 정보담당교사

대체로 NEIS의 도입·운영에 찬성하는 입장을 취하였다. 대립하는 교원단체인 전교조의 영향력을 줄이기 위해 정부정책에 지지를 보냈지만(교총/전국교장단), NEIS 문제에 대해 적극적인 해결의 의사표시는 없었다(일선학교 정보담당교사).

⑤ 학부모

찬성과 반대로 나누어졌다. 하지만 찬성측 보다는 반대측 학부모(예, 참교육학부모회의)의 활동이 두드러졌는데 NEIS에 대한 논란으로 학생들의 피해에 대해 우려를 표시했으나 적극적인 문제해결 의지는 부족하였다.

3) NEIS 쟁점의 처리방식과 함의

(1) NEIS 문제의 처리방안

NEIS의 검토를 위해서는 전자정부 추진방식과 개인정보보호 차원에서 문제제기를 하여야 하였다. 또한 NEIS에 관련된 문제는 상당부분 '국민의 정부'가 추진해 온 전자정부 사업 전반이 갖고 있는 한계에 기인하며 이미 예견된 것이었다. 하향식(top-down), 공급·기술중심(supply-driven)의 전자정부 추진방식이 아닌 상향적, 수요자 중심으로의 전환이 필요하다.

각 부처의 의견을 취합하는 절차를 거쳐 사업들을 선정하였으나, 시간적인 제약 때문에 국민의 요구에 대한 조사나 심도 있는 검토 없이 진행되었고, 추진과정에서도 중요한 의사결정을 과정에 이해당사자, 전문가, 시민단체, 업계의 의견이 광범위하게 반영되어야 한다. 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 기본인권

을 침해한다는 것이 문제이다. 강화된 보안체계하에 학생정보가 수집된다고 하더라도 정부업무의 효율성을 위해서 개인정보가 정보주체의 동의 없이 수집·집적될 수 있느냐 하는 점에서 정보인권 문제로까지 확대되었다(김보경, 2003).

(2) NEIS 논쟁이 주는 함의

① 개인정보보호과 행정작용간의 갈등

정보화가 촉진되고 전자정부 서비스가 또 다른 행정작용으로 대두되면서 개인정보보호 침해사례가 증가하고 그 문제의 심각성이 대두되었다. 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.

최근에 '자기정보통제권'은 기존의 '사생활을 침해받지 않을 권리'라는 소극적 의미인 프라이버시권이 개인정보의 수집과 이용, 보관에 대해 정보주체가 스스로 결정할 수 있어야 한다는 개념으로 발전하였다. 그리하여 정보화 시대의 개인정보보호권은 정보화 시대에도 개인의 자유와 평등을 보장받기 위한 최소한의 권리이면서 동시에 정보화하고 있는 사회의 민주화를 위한 중요 이념이라고 볼 수 있다.

그러나 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 요구된다.

② 정보화와 전자정부에 대한 근본적인 불신

전자감시사회에 대한 불안감이 증대함. 선진 각국의 사회보장번호제도는 상업기관

들이 개인정보를 추적하는 자료로 활용될 수 있지만 동시에 실업자에 대한 실업수당을 지급하는 자료로도 활용되는 이점이 있기 때문에 개인식별번호를 부정적으로 볼 수 없다.

기술의 발달로 많은 사람들이 혜택을 입는 반면, 데이터베이스화된 정보가 자신의 의도와는 관계없이 널리 유통되고 있으며 특정목적의 감시와 통제의 수단으로 사용되는 경우에 대한 우려가 있다. 새로운 기술이 도입될수록, 최신 정보시스템이 구축될수록 정보집적에 따른 개인정보의 유출에 따른 사생활 침해와 국가권력에 의한 감시에 대해 민감해질 것이다.

하드웨어적인 것이 아니라 인적 유출, 해킹 등의 위험성이 문제이다. 민간 웹사이트에서 회원탈퇴를 하여도 여전히 DB에는 개인정보가 남아있어 이러한 개인정보 목록들이 거래되고 있으며, 주로 인적 유출에 의한 개인정보보법 위반사례가 증가하고, 해킹사고도 빈번하게 일어난다.

③ NEIS 논쟁을 통한 개인정보보호에 대한 교훈

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. 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. 또한 그렇게 보면 정부에 의해 정보를 수집하는 것이 인권침해에 해당하는 게 아니라 그 정보의 열람에 달려 있는 것으로 보아야 한다는 반론이 제기되기도 한다.

물론 개인정보의 제공이나 처리・가공・이용, 제3자에 대한 공개나 일반 공개 여부에 대한 개인의 처분권, 즉 동의권을 인정하지 않을 도리는 없다. 또한 국가나 공공기관에게 제공될 수 있는 개인정보의 범위나 그 이용 상의 한계, 정보처리의 조건・제한 등에 관한 한, 국가나 사회, 시대, 환경 등에 따라 상이한 합의가 성립될 수 있는 여지가 있는 것도 사실이다. 그러나 행정기관이 대다수의 구성원들이 합의를 하거나 다수결 등 민주적 의사결정방법을 통해 개인정보를 수집・접근하는데 합의를 한다고 해도

함부로 접근하거나 침해할 수 없는 최소한의 개인정보보호가 되어야 한다. NEIS 논쟁을 통해 우리는 정책결정자와 정보기술자의 개인정보보호에 대한 인식의 제고 없이는 신뢰받고 효율적인 전자정부 서비스가 불가능함을 알 수 있다.

2 강남구 CCTV 설치 사례

1) 개요

(1) 추진배경

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.

(2) 사업목표

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.

2) 쟁점과 갈등관련 행위주체

(1) CCTV 설치와 관련한 쟁점사항

① CCTV 설치과정

강남구의 CCTV 설치는 2002년 9월 30일 논현1파출소 관내의 5개소에 대한 CCTV 설치 협조 요청을 시작으로 추진되기 시작하였다. 동년 10월 18일 방범취약지역 CCTV 설치 계획을 수립하였고, 21일 정책회의에서 무단쓰레기투기감시용 CCTV와 병행하여 운영하기로 결정하였고, 23일 뒷골목 CCTV 시범 설치계획을 수립하였다.

11월 11일 '뒷골목 CCTV 설치를 위한 주민 설명회'의 개최, 11월에 '뒷골목 CCTV 시범 설치를 위한 주민설문(인터넷)'을 통해 주민의 의견을 하고 12월 27일 뒷골목 CCTV 시범 설치·운영을 시작하였다.

2003년 3월 31일 뒷골목 CCTV 설치 계획 수립을 통해 3개동 37개소[9]의 설치를 결정했다. 또한 6월 18일 강남 '납치 떼강도' 사건이 발생하면서 CCTV 확대 설치는 탄력을 받게 되었다. 이에 강남구는 뒷골목 CCTV 확대 설치를 위한 주민여론조사[10]를 실시했고, 6월 23일에는 강남경찰서장이 강남구청을 방문하여 각종 강력범죄 발생에 따른 강남구 전지역에 CCTV의 확대 설치·운영에 대해 협의를 하였다. 협의 후 6월 26일 뒷골목 CCTV 확대 설치 계획이 수립되었는데 이 계획에서는 20개동에 320대의 설치 계획이 수립되었다(아파트 밀집 동은 제외).

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

9) 논현 1동 1개소, 역삼 1동 16개소, 개포 4동 10개소에 설치.

10) 주민여론조사는 2003년 6월 18일~20일(3일간)에 실시되었고, 조사 대상은 강남구 홈페이지의 이메일리스트에 등재된 45,000명을 대상으로 하였다. 총 237명이 조사에 응하였고 찬성 211, 반대 19, 기타 7로 찬성이 많은 것으로 나타났다.

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[11], 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 관리가 용의 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.

11) 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'을 만들지 않은 체 행정편의적·기술 우선적인 사업 추진이 이루어졌다. 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 명백한 위법이다. CCTV를 설치·운영 중이고 추가 설치를 계획하고 있으면서도 CCTV로 인해 침해될 여지가 있는 정보인권 침해에 대한 조례나 정보보호를 위한 가이드라인이 없음. 또한 CCTV 설치·운영과 관련해 이를 통제할 독립적인 감독기구의 설치도 이루어지지 않고 있다.

둘째, 일방적인 설치·운영과 의견수렴 절차의 문제이다. 강남구가 2002년 12월 논현동에 5대의 CCTV를 설치와 2003년에 230대 추가설치·운영을 하면서 설치·운영

과정에서의 시민의 참여와 의견수렴 절차를 거치지 않았다. 강남구청과 강남경찰서에 의한 시범 설치 후에 추가설치를 위한 예산과 계획이 이미 완료된 후에 시민의 의견을 청취하는 방법을 택하였다.

강남구는 시민설문조사를 통해 시민의 의견을 충분히 수렴했고 시민들이 찬성정도가 높아 절차상의 문제가 없다는 입장을 견지하다가 방송매체를 통해 시민단체에서 정보인권침해에 대한 논란이 불거지면서 구민 공청회를 통해 의견을 수렴하는 과정을 거쳤다. 사실 개인정보보호는 시민의 주도적 참여가 다른 어떤 정책보다 필요한 경우라고 할 수 있느데, 강남구 CCTV의 설치와 운영과정을 보면 행정적 편의에 의해 일단 설치 한 다음 이후 주민들의 동의를 얻는 사후적인 절차를 통한 해결을 모색하는 한계를 보였다.

(2) 갈등관련 행위주체

강남구의 CCTV 설치와 관련한 갈등은 NEIS 문제에서와는 달리 주체가 CCTV 설치에 직접적인 영향 받는 시민들보다는 시민단체(함께하는 시민행동, 참여연대 등)가 적극적인 반대를 보였다.

① 강남구

시민의 생명과 재산보호라는 명분으로 CCTV 설치에 찬성하였따. CCTV 설치를 위한 예산의 지원하였다.

법적·제도적으로 뒷받침 없이 형식적인 주민공청회를 통한 일방적 의사결정과 개인정보침해에 대한 고려 없이 사업추진 했고, 법·제도적 미비점에 대한 해결의지를 보이지 않았다.

② 강남경찰서

강남구청과 함께 CCTV 설치를 주도하였다. CCTV 설치가 범죄 억제에 큰 도움이 되고 부족한 경찰력을 대신할 수 있다고 믿었고, CCTV 설치 외의 방법에 의한 방범에는 소극적인 태도를 보였다.

③ 시민단체

CCTV 설치와 관련해 개인정보 침해와 강남구의 일방적 사업추진에 대해 반대를 하였다. 법·제도적 뒷받침이 없는 CCTV 설치는 분명한 위법이라는 것을 강조했고, 설치에 따른 주민설문조사, 공청회 등의 의견수렴 과정이 설치를 위한 형식적인 절차라고 주장(개인정보침해 등에 대한 설치 후의 문제에 대한 주민인지를 충분히 시키지 않았다고 봄)하였다. 강남구가 1차적으로 설치한 CCTV에 대한 관리·감독의 문제 제기하면서, 개인정보침해 시 이를 해결할 독립적인 관리·감독기구의 부재에 대한 해결방안을 요구하였다.

④ 시민

적극적인 찬성·반대의 입장을 뚜렷이 보이지 않았으며 실제적으로 설치와 관련한 문제의식이 없다.

⑤ 언론

'몰카' 논쟁을 유발하였는데 방송과 신문에서 1차적으로 논현동에 설치된 5대의 CCTV에 대한 보도를 했다. 하지만 문제해결에 대한 적극적인 의지를 보이지는 않았다.

3) 쟁점의 처리방식과 함의

(1) CCTV 문제의 처리방안

강남구의 CCTV 설치·운영과 관련한 논쟁은 지방정부의 개인정보보호에 대한 이해와 현실을 파악하는데 좋은 본보기가 된다고 볼 수 있다. 앞서 말했듯이 강남구의 행정편의적 의사결정과 기술우선적 정책결정, 법·제도의 미비는 개인정보보호에 대한 지방정부의 인식을 보여준 단적인 예가 된다.

기존에 설치된 CCTV(37개소)에 대한 관리·감독의 강화를 위한 독립적인 기구의 설치가 우선되어야 한다. 운영·관리를 하는 관제실(종합상황실)이 아닌 개인의 정보보호를 최우선으로 하는 CCTV 관리·감독 기구가 필요하다. 추가 설치(320개소)시 개인정보 침해에 대한 조사와 시민의 의견수렴이 필요하며, 방범체계의 개선을 통해 설치

를 최소화하고, 설치가 필요한 경우 개인정보 침해에 대한 '개인정보침해 영향평가조사' 실시를 통한 설치, 설치장소 거주 주민뿐만 아니라 유동인구에 대한 고려를 통한 의견수렴과 설치 장소 협의 과정 요구가 있어야 한다.

(2) CCTV 논쟁이 주는 시사점

① 상반된 가치의 절충

CCTV 설치·운영은 시민의 생명·재산 보호와 정보인권침해라는 두 가지 상반된 가치를 함께 고려해야 한다. 강력 범죄와 재난으로부터 한 사람의 생명을 구하는 것 이상으로 불특정 다수의 개인정보에 대한 보호가 필요하다.

강남구 전역에 설치된 CCTV가 순기능인 시민의 생명과 재산 보호에 사용된다면 순기능적인 가치가 실현이 되는 것이다. 하지만 강남구가 설치·운영의 정당성 확보를 위한 기준으로 제시한 2/3의 시민 찬성만 되면 문제가 없는, 나머지 시민에 대한 고려가 없는 것은 두 가지 가치를 모두 고려한 것이 아니라고 볼 수 있다. 이러한 사항을 고려하여 의회에서 '조례'나 '정보보호가이드라인'의 제정을 통해 제도적 뒷받침을 해야 한다.

다시 말하면 CCTV 설치·운영이 순기능을 발휘할 수 있게 보다 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.

② 절차적 정당성의 확보와 제도적 구비

CCTV 설치·운영에 대한 법·조례와 정보보호 가이드라인의 부재, 독립적인 감독기구 없이 설치·운영되고 있어 우선적으로 정당성의 확보가 중요하다.

CCTV가 개인정보보호(또는 정보인권 침해)를 위한 상위법이 없이 설치·운영되고 있어 위법의 논란과 정당성 확보에 문제가 되고 있다. 상위법의 제정은 강남구의 권한을 넘어서는 것이므로 국회에 지속적으로 건의를 하여 법제정이 이루어지도록 하여야 한다. 또한 강남구 의회와 협의하여 CCTV 설치·운영·관리에 관한 조례의 제정과

정보보호 가이드라인을 만들어야 할 것이다. 조례와 정보보호 가이드라인 제정을 통해 CCTV 설치·운영을 전담하는 독립적인 감독기구를 만들어 시민의 생명과 재산 보호, 정보인권 보호라는 두 가지 가치가 모두 달성될 수 있는 제도적인 장치를 마련하여야 한다.

③ 기술우선적 정책에 대한 반성

CCTV의 설치를 통한 생명과 재산 보호는 지나친 기술신봉적인 정책이라고 볼 수 있다. 물론 경찰력과 예산에 한계가 있어 방범활동이 제한을 받고 있는 것은 현실을 부정하는 것은 아니다. 하지만 CCTV의 설치·운영만이 시민의 생명과 재산을 보호해 주는 아니라는 것을 알아야 한다. CCTV의 설치·운영은 경찰력의 보조수단으로서 부득이한 경우 활용하여야 할 정책이라고 할 수 있다. 시민의 사생활 침해라는 부작용이 상존하는 정책을 아무런 반성 없이 집행하는 것은 피해야 한다.

3. 인터넷 실명제 사례

1) 개요

(1) 추진배경

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 되

었고 법안이 국회를 통과하면서 법적으로 추진이 되었다. 정개특위는 「공직선거및선거부정방지법」에 제82조 제6항을 신설하여 인터넷언론사 게시판·대화방의 실명확인 제도를 도입을 천명했다.

(2) 도입목표

① 정보통신부

정부는 인터넷 게시판이 우리나라만이 가진 독특하고 선진적인 인터넷 문화라고 생각하는바, 이러한 게시판 본래의 기능을 회복하여 국민과 정부간 의사소통을 보다 활성화하기 위해서는 현재 문제가 되고 있는 익명성으로 인한 부작용을 적절히 관리하기 위해 도입하였다.

정통부가 실명제 게시판을 운용한 결과, 게시판 상에서의 명예훼손, 상업성 광고, 특정인에 의한 글 도배 등이 69%에서 2.1%로 대폭 감소되었고 게시판 이용자도 실명제 시행전보다 30% 이상 증가하여 정보통신 정책관련 토론과 정보교환의 장으로서의 본연의 기능 회복을 목표로 하였다.

② 정책특위

정개특위는 인터넷을 통한 선거운동과 정책홍보, 유권자의 선거에 대한 자유로운 의견표시를 활성화하되, 이 게시판을 통하여 허위정보나 근거 없는 비방의 게시와 유통이라는 부작용이 발생하는 것을 예방하기 위한 것이라고 도입의 목표를 밝혔다.

2) 쟁점과 갈등관련 행위주체

(1) 인터넷 실명제와 관련한 쟁점사항

① 프라이버시권 침해

개인정보 유출사고가 증가하면서 프라이버시권이 중요하게 부각되고 있음. 네트워크의 기술적 특성상 발신자와 수신자가 반드시 남기 때문에 네트워크에서 사람을 추적하고 정보를 수집하기가 용이해지고 있은 것이다. 검사를 비판한 네티즌도 쉽게 추적되고 구속되었다

국가권력에 의한 전자감시사회가 가능하기 때문에 최근 국제사회는 오히려 국민의 익명권을 보장하기 위해 노력하고 있다. 벨기에, 프랑스, 독일, 영국에서 법률적으로 익명이나 가명의 사용을 권장하고 있으며, 미국의 경우 역시 온라인 익명으로 인한 소송이 잇따르고 있는데 법원에서는 익명권을 인정하고 있다. 한국의 경우 「통신비밀보호법」에서 통신의 비밀을 보장하고 있다.

② 자기정보통제권 침해와 민주주의 원칙의 위협

인터넷 실명제가 가능하려면 실명 데이터베이스가 하나 이상 구축되고 실명확인을 위해 상시적으로 대조되어야 한다. 하지만 지금 구축된 어떠한 실명 데이터베이스도 정보주체인 국민으로부터 실명확인용으로 이용하겠다고 동의를 받은 적인 없이 사용되어 자기정보통제권을 침해하고 있다. 이는 '개인정보의 목적 이외 전용'에 해당하는 것으로서 프라이버시 보호 원칙에서 금지하고 있는 행위이다.

정부기관 홈페이지는 공공장소로서 오히려 익명의 고발을 철저하게 보장해야 하고 로그기록이나 개인정보를 오히려 특별하게 보호해야 한다. 공공게시판에 실명제를 도입하는 것은 오프라인에서 고발함을 만들어 놓고 고발쪽지의 지문을 추적하는 것과 마찬가지로 민주주의 원칙을 위협하고 있다.

③ 표현의 자유 침해

표현의 자유는 아무 말이나 행동을 하겠다는 뜻으로 오인되는 경우가 많은데, 표현의 자유는 자신의 표현행위에 대해 문제가 발생하면 법적 책임을 진다는 것을 내포하고 있다.

가장 논란이 되는 것은 글 쓰는 사람의 심리를 사전에 정부가 위축시키려는 한다는 것이다. 이는 헌법에서 금지하고 있는 표현의 자유에 대한 검열이라 볼 수 있다. 특히 실명을 드러내기 어려운 사회적 소수자와 내부 고발자에게 무조건 실명을 쓰라고 정책적으로 강요하는 것은 표현의 자유를 침해하는 행위이자 사회적 약자에 대한 국가의 폭력일 수 있다.

(2) 갈등행위의 주체

인터넷 실명제 도입과 관련한 논쟁은 찬성과 반대가 분명하게 드러남. 정부와 정치권은 찬성하는 반면에 시민단체, 네티즌, 포털사이트 및 인터넷 신문사 등은 반대의 입장을 보였다.

① 정개특위

선거에 직접적인 영향을 받을 것으로 보고 선거운동과 관련해 익명으로 운영되는 게시판을 실명제로 전환하는 「공직선거및선거부정방지법」의 통과를 주도했다. 프라이버시 침해, 사이버 범죄 등의 문제보다는 인터넷 게시판의 익명성으로 인해 발생할지 모르는 선거에서의 불이익에 초점을 두고 법을 개정하였다.

2004년 2월 법안 통과를 주도함으로써 인터넷 실명제에 대한 논쟁을 재점화 시켜다.

② 정보통신부

2003년 3월 전자정부의 구현을 통해 건전한 여론형성의 도구로서의 인터넷 게시판의 기능을 합법화하기 위해 인터넷 실명제 도입을 처음을 제기했고, 실명제 도입을 적극 추진하다가 반대여론에 굴복하여 추진을 유보했다.

③ 행정자치부

정통부가 인터넷 실명제 도입을 추진하려다 실패하자 정부부처의 인터넷 게시판에 실명제를 실시할 계획이 없다고 밝혔다. 실명제는 각 행정기관이 자율적으로 판단할 문제라고 함. 주도적 역할을 하지 않았다.

④ 시민단체

프라이버시와 표현의 자유 침해를 야기할 수 있으므로 인터넷 실명제보다는 익명성으로 하는 것이 바람직하다는 입장을 견지하면서 반대를 하여다. 정통부의 추진 계획을 좌절시켰다.

정개특위가 선거를 빌미로 인터넷 실명제를 도입하는 법안을 통과시키자 적극적인

반대운동을 주도했는데, 반대성명 발표, 인터넷 실명제 불복종 선언 등을 하였다.

⑤ 네티즌

인터넷 실명제와 관련해 직접적인 당사자 중의 하나로 사이버 시위를 통해 반대운동에 동참했다. 포털사이트에 찬·반 사이버 투표 등을 통해 반대입장을 취하였다.

3) 쟁점의 처리방식과 함의

(1) 인터넷 실명제 논란의 해결방안

선거에 따른 정치권의 이해관계에 의해 충분한 논의를 거치지 않고 '인터넷 실명제' 관련 법안의 개정이 이루어졌다. 익명성이 보장된 인터넷 게시판에서 상호비방과 사이버 선거홍보에서의 불리함, 낙선·당선 운동에 대한 두려움으로 졸속 통과된 법안을 개정해야 한다. 즉, 인터넷 실명제는 행정기관에 의한 사이버 여론 통제가 아니라 건전한 사이버 여론 형성의 장으로 유도해야 한다. 행정자치부가 밝혔듯이 선택적 실명제 도입을 통해 프라이버시 침해가 심한 경우와 악의적인 스팸성 글을 삭제하는 방법을 통해 건전한 여론형성이 가능하도록 해야 한다.

또한 시민단체와 네티즌의 건전한 사이버 여론형성을 위한 홍보와 교육, 익명성을 이용한 프라이버시 침해와 표현의 자유를 악용한 스팸성 글에 대한 자정(自靜) 운동이 함께 되어야 한다.

(2) 인터넷 실명제 논란이 주는 함의

① 실명제와 익명성의 상호 절충

인터넷 게시판에서 프라이버시 침해가 우려되는 게시판[12]의 경우 실명제를 도입해야 한다. 하지만 그 외의 게시판의 경우에는 익명성을 사용하여 표현의 자유를 보장하는 선택적 게시판 운영이 필요하다.

12) 정부기관, 교육관계, 언론사 게시판 등.

② 정보화 교육과 홍보의 강화

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 보호 현황

제1절 서울시 전자정부와 개인정보

제2절 서울시 전자정부의 개인정보 현황

제3절 서울시 개인정보보호 관련 인식 조사

제3장 서울시 전자정부의 개인정보보호 현황

제1절 서울시 전자정부와 개인정보

1. 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.

1) 공공기관의개인정보보호에관한법률(개인정보보호법)

개인정보보호법은 공공기관의 공공업무의 적정한 수행과 국민의 권리와 이익을 보호하기 위한 개인정보보호의 기본법적 의미를 가진다. 개인정보보호법은 중앙정부와 지방정부를 포함한 모든 공공기관의 개인정보보호에 영향력을 미친다.

2003년 8월 입법예고된 '공공기관의개인정보보호에관한법률'은 개인정보보호원칙을 구체적으로 명시하고, 공공기관의 장은 법률의 규정에 의하거나 정부주체의 동의 등을 얻은 경우에 한해서만 개인정보를 수집하도록 하고, 개인정보를 수집하면서 개인정보 수집의 법적근거, 목적 및 이용범위, 정보주체의 권리 등에 관하여 서면 또는 인터넷 홈페이지 등을 통하여 정보주체가 그 내용을 쉽게 확인할 수 있도록 안내하여 하며, 공공기관의 장이 개인정보를 통합·유지 및 관리하거나, 별도의 개인정보데이터베이스를 구축하여 집적·운용하고자 하는 경우, 소관법령중 개인정보 관련 법령 제·개정의 경우에는 행정자치부장관과 사전 협의하여야 하고, 공공기관의 장이 개인정보를 통합

관리 또는 별도의 개인정보데이터베이스를 구축 운영하거나 중앙행정기관의 장이 개인정보 관련 법령을 제·개정하고자 하는 경우에는 개인정보보호심의위원회에서 사전심의를 하는 등 개인정보보호심의위원회의 기능을 강화하였다(김일환, 2004).

「공공기관의개인정보보호에관한법률」은 행정자치부를 통해 서울시에 개인정보보호에 관한 지침을 내리는 근거가 된다. 서울시 전자정부에서의 개인정보보호에 관해 포괄적인 내용을 담고 있으며, 서울시의 개인정보보호 관련 조례의 모법(母法)이 된다고 볼 수 있다.

2) 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.

3) 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.

2. 서울시 전자정부의 정보보안 현황

인터넷 이용자 수가 증가하고 있고, 서울시 전자정부 홈페이지 방문을 통한 온라인 행정서비스의 이용이 확산되고 있다. 서울시에서도 개인정보의 유출, 스팸메일, ID도용, 인터넷 사기 등과 같은 다양한 차원의 정보보안 문제가 발생하고 있다.

이 중에서도 컴퓨터·통신기술의 발전으로 정보의 복제·탈취 및 변조가 가능해짐에 따라 개인정보 유출에 대한 우려가 커지고 있다. 서울시에서는 e-Seoul Net의 초고속, 광대역 통신만의 정보 유통량에 대응하는 정보보안체계를 구축함으로써 보안사고를 예방과 신속한 대응을 위해 통합 보안관제의 필요성을 느끼고 있다.

서울시의 정보보안 적용대상은 먼저 물리적 시설로 e-SNOC, SIDC, LAN실, 시스템실, 데이터센터가 있고, 네트워크는 Seoul Net(서울시초고속정보통신망: 1식), LAN 장비(본청 177, 전산소 97대)가 있다. 또한 서버시스템(81종), PC(본청 3,190, 본부 및 사업소 등 1,430), 컨텐츠(서울시 행정정보업무 192종, 시민·직원 개인정보)가 있다.

서울시의 정보시스템은 H/W 수치적으로 방대한 양을 보유하고 있으며, 이에 따른 각 시스템별로 유통되는 정보의 양 또한 엄청나다고 할 수 있다. 특히 정부기관 특성상 정보보안에 대한 중요성이 주요 고려 대상이 된다.

하지만 정보보안에서 보안을 통제·관리하는 핵심시스템이라고 할 수 있는 보안관제시스템을 보유하고 있지 않다. 보안관제시스템의 미비는 통합정보보안시스템 체제로의 전환이 불가능하다. 이로 인해 각 기관은 보안시스템으로 보안방화벽, 침입탐지시스템 등을 설치·운영하고 있다. 부서별 보안시스템 개별도입, 운영으로 통합 보안정책 적용이 미흡하고 보안관제 시스템 부재는 해킹에 대한 대비가 전혀 없어 해킹피해 파악 및 능동적 대처가 이루어지지 않고 있다. 또한 정보이용 증가에 따른 인터넷 접속점 방화벽 성능에 한계가 있어 속도가 저하되고 있다. 전산소 서버팜 내 방화벽 및 IDS의 통합 보안관리가 어려운 상황이다. 그리고 자치구의 가상사설망(VPN)을 본청 수준으로 향상시켜 보다 완벽한 정보보안시스템으로의 구축이 이루어져야 한다.

<표 3-1> 정보보안 시스템 운영현황

장비명	시본청	전산소	구청
보안관제시스템	-	-	-
보안방화벽	2	10	25
침입탐지시스템	7	6	18
가상사설망(VPN)	16유저	23유저	8유저
인증등록서버	1식	-	-

이와 함께 정보보호 책임관의 지정이 형식적이고 전문인력이 부족하고, 정보보호담당 부서별로 관련예산의 분산편성과 개별사업 시행으로 인해 종합적인 정보보안 시스템의 구축과 운영이 원천적으로 이루어질 수 없게 되어 있다.

3. 서울시 전자정부의 개인정보보호 관련 제도적 쟁점

1) 개인정보보호조례 제정의 필요성

중앙정부의 경우 미비한 점이 있지만 개인정보보호를 위한 기본법으로서 「공공기관의개인정보보호에관한법률」이 존재한다. 중앙정부는 이 법률에 근거하여 개인정보보호에 관해 중앙부처와 자치단체에 지침을 전달한다.

현재 서울시는 행정자치부에서 내려오는 지침에 따라 개인정보보호에 관한 업무를 하고 있다. 자치단체라 독자적인 법률을 가질 수는 없지만 서울시 전자정부에서의 개인정보보호를 총괄하는 조례가 필요하다. 「서울특별시정보화촉진조례」와 동조례의 규칙, 「서울특별시인터넷시스템설치및운영에관한조례」로 나누어져 있고 명확한 개인정보보호 내용을 담고 있지 않아 개인정보보호와 정보보안에 관한 법적인 근거가 약하다. 이는 개인정보의 누출 및 침해, 정보보안 위험 상황이 발생했을 때 대응할 방안이 없다. 또한 개인정보보호와 정보보안을 다루는 조례가 없으므로 인해 담당업무에 대한 서울시와 자치구의 역할이 분명하지 않아 문제 발생시에 책임공방이 일어날 수 있다.

「공공기관의개인정보보호에관한법률'」 모법으로 한 조례의 제정은 개인정보보호

및 정보보안에 대한 서울시와 자치구의 역할 규정, 명확한 업무분담, 서울시 전자정부 이용의 활성화를 위해서도 필요하다.

2) 개인정보보호 권리구제시스템의 미비

(1) 개인정보보호 영향평가제도

공공기관의 행정작용으로 인한 시민의 권리침해가 발생하기 이전에 처음부터 부당한 행정작용이 이루어지지 않도록 예방하는 사전적·절차적 제도를 통한 권리보호가 더 중요하게 부각되고 있다.

개인정보 관련 정보시스템의 도입이 증가하여 개인정보 누출의 위험도 증가하고 있지만, 새로운 정보시스템 도입이나 변경시 개인의 프라이버시에 미칠 영향을 사전에 조사하여 예측·검토하여 개인정보 침해를 사전에 방지하는 제도는 중앙정부나 서울시에 도입하고 있지 않다. 이에 반해 미국과 캐나다의 경우 공공부문에서 프라이버시영향평가를 의무적으로 시행하고 있고, 뉴질랜드·홍콩, 호주 등에서는 공공·민간 부문 모두에 대하여 시행을 권고하고 있다(김일환, 2004).

따라서 공공부문에서 불필요한 개인정보의 수집을 막고 정보시스템 구축시 사전평가과정과 후속조치를 통해 지속적인 정보시스템의 보완을 가능하게 함으로써 개인정보 침해를 최소화하기 위하여 개인정보보호 사전영향평가제도를 도입하고 이에 과한 통제를 개인정보보호기구가 맡는 법·제도적 뒷받침이 있어야 한다.

(2) 불충분한 사후구제 법·제도

「공공기관의개인정보보호에관한법률」를 바탕으로 한 행정자치부의 규정만으로는 누출 및 침해당한 개인정보에 대해 구제할 수 없고, 특히 서울시의 조례의 경우 사후의 구제에 관한 규정이 전무한 실정이다.

개인의 권리보호에 관한 규정의 미비는 개인의 동의를 무의미하게 만들거나 개인을 충분히 보호하지 못하도록 만들 수 있다. 따라서 우선 열람권만이 아니라 자신에 관한 정보의 수집, 취급, 활용, 타기관으로의 유통에 관한 설명을 들을 권리가 개인에게 인정되어야 하고 잘못된 정보에 관하여 정정할 권리뿐만 아니라 이러한 정보에 대

한 삭제권과 보충권이 인정되어야 한다. 또한 정보에 대한 공공기관과 개인간의 의견 차이에 있는 경우에 해당 개인의 의견이 기록에 첨부될 수 있어야 한다. 그리고 개인정보를 처리하는 기관은 관련자를 위해서뿐만 아니라 개인정보보호 감독기관을 위해서도 어떠한 방법으로든 이를 기록해야 한다(김일환, 2004). 또한 보유기관의 장에게만 인정되고 있는 잘못된 개인정보에 대한 정정·삭제 청구권의 부여를 법·제도적으로 보장해야 한다.

3) 전문적이고 독립된 감독기구의 설립·운영

전자정부의 이용이 확대되고 정보보안 시스템에 대한 해킹 등 개인정보의 누출 및 침해의 위험성이 높아지고 있다. 개인정보보호는 법이나 조례의 제정, 제도적 장치만으로 해결할 수 없다.

따라서 개인정보보호 법·조례의 제정도 중요하지만 시민의 개인정보를 효율적으로 보호하기 위해서는 공공기관이나 민간부문의 정보 수집, 취급, 활용을 감독·통제하는 기구의 설치 및 운영이 절대적으로 요구된다. 공공부문에서 이러한 감독기구를 설치하는 근본적인 이유는 공공기관의 지나친 정보조사와 처리로부터 시민들을 보호하는 데에 있다. 이러한 감독기구가 없다면 공공기관의 무제한적인 개인정보의 수집, 취급, 활용, 타기관으로의 유통으로 인한 개인사생활의 지나친 감시를 방지한다는 것은 불가능할 것이다(김일환, 2004).

이러한 감독기구는 그들의 활동과 정책을 공공기관과 민간부문의 정보조사와 처리를 통제하는 것에 집중해야만 하는데, 즉 개인의 정보보호를 우선적 목표로 하여 개인의 여러 권리들을 보장하고 강화하는 역할을 수행해야 한다. 또한 이 기구는 부당한 감시를 받고 있다고 느끼는 시민들의 권리를 보호해야 하며, 더 나아가 다양한 방법을 통하여 공공기관의 정보처리과정에서 개인정보가 보호될 수 있도록 일반적이고 체계적인 감독과 대인제시의 역할을 수행해야 한다. 동시에 개인정보의 수집, 취급, 활용과 관계되는 중요사항에 대하여 매년 의회에 보고서를 제출하고 개인정보보호와 관련되는 사안에 대하여 언론매체 등을 통해 널리 알리고 시민에게 홍보하는 역할도 수행할 필요가 있다.

제2절 서울시 전자정부의 개인정보 현황

1. 서울시 전자정부의 개인정보 유통관리 현황

서울시 전자정부에서의 개인정보 유통관리 현황은 자치구의 개인정보 실태조사를 통해 알 수가 있다. 서울시는 지침을 통해 자치구에 개인정보 유통과 관련한 조사를 의뢰하고 자치구는 서울시의 지침에 따라 개인정보 유통관리현황을 조사한다.

서울시가 자치구에 내려 보내는 지침을 통한 조사는 ①개인정보보호 정책수립 및 지침준수, ②개인정보 파일의 수집 및 보관, ③개인정보 제공 및 열람·정정, ④개인정보 입출력자료, ⑤시스템 및 단말기 관리, ⑥시설보안, ⑦개인정보의 위탁처리 등의 분야이다.

본 연구에서는 4개 자치구(강남구, 강서구, 은평구, 중구)의 개인정보보호 관련 업무담당자와의 면접조사를 통해 서울시 전자정부의 개인정보 유통관련 관리 현황에 대한 조사를 수행하였다.

1) 개인정보보호 정책 수립 및 지침 준수여부

먼저 개인정보의 분실, 도난, 유출, 변조 또는 훼손 대책 등 개인정보의 보호·안전대책을 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.

전자정부의 출범으로 오프라인 보다 온라인을 통한 개인정보의 유통이 더 많아지면서 그만큼 개인정보보호의 중요성이 높아졌다. 그래서 개인정보보호 대상을 명확하게 인지하고 있는지가 중요하다. 조사대상인 4개 자치구가 모두 인지하고 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.

전자정부를 통한 행정서비스의 제공으로 서울시 전자정부 웹사이트를 이용하는 빈도가 높아졌다. 개인정보 화일의 보유현황·근거 및 보유목적, 열람 및 정정 청구 안내 등 웹사이트에서 유통되는 개인정보의 보호방침의 웹사이트 게재는 의무사항이다. 서울시를 비롯한 조사대상 자치구가 게재를 하고 있다. 또한 개인정보 침해 신고처리대장의 비치 및 접수·처리결과와 관련된 장부를 비치하여 유통현황을 알 수 있게 하였다.

더불어 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 교육을 실시하지 않는 것으로 조사되었다. 교육은 강서구가 년 1회 실시하고 있으며, 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.

또한 개인정보 사무의 업무분장 및 위임전결 규정, 자체감사규정의 개정·반영은 업무분장을 통해 이루어지고 있었다.

2) 화일의 수집 및 보관

개인정보의 유통에 있어 개인정보 파일의 수집과 보관은 필수적이다. 여기에는 수집절차, 보유범위, 사용후 폐기, 백업자료의 관리, 개인정보의 열람이 해당된다.

개인정보의 수집절차는 유통의 기본적인 요소이다. 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 유통시 입·출력 관리가 잘 이루어지고 있음을 알 수 있었다. 하지만 입·출력 및 수정사항, 데이터 접근내역 등을 자동으로 기록하여 개인정보의 유통을 알 수 있는 로그화일 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 통해 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

(1) 서울시 전자정부 업무 아키텍처의 개인정보 내용

서울시 전자정부의 업무 아키텍처는 오프라인 정보와 다르게 분류해야 한다. 서울시 전자정부의 업무 아키텍처에 따른 정보 분류는 오프라인에서의 개인정보 분류방식인 속성정보, 활동정보, 민감정보를 동일하게 적용하기에는 한계가 있다. 왜냐하면 서울시 전자정부 아키텍처는 『서울시 정보화 기본계획』을 바탕으로 구성되어 있으며, 이 때 업무 아키텍처에서는 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- >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	--이름, 주민번호, 주소, 전화번호, 보호자 및 친구 관계, 병명, 치료현황 등
		KT-EDI, 결핵정보감시	
	여성	늘푸른여성정보센터	-이름, 나이, 생년월일, 연락처, 보호자 이름 및 연락처, 상담내용 및 결과 등
	정보화	전자우편서비스	-이름, 주민등록번호, 주소, 이메일주소, 학력, 나이, 직업 등
		시민사이버정보화교육	
행정정보	민원	시군구행정정보시스템	-이름, 주민등록번호, 주소, 학력, 나이, 생년월일, 신장, 체중, 전화번호, 사진, 지문, 가족관계, 결혼여부 등
		민원처리온라인공개시스템	
	재산/세무	세무종합정보시스템	-이름, 주민등록번호, 주소, 학력, 나이, 과표, 세액, 수입, 임금 등
		E-tax(지방세인터넷납부)	
	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	-이름, 주민등록번호, 주소, 학력, 나이, 직업 등
		부동산전산망,	
		철거민세입자관리	-이름, 주민등록번호, 주소, 나이, 직업, 가족관계, 재산, 소득 등
	지적	지적관리시스템	-소유자의 이름, 주민등록번호, 주소 -지번, 지목, 면적 등
		제적부관리시스템	

(2) 서울시 전자정부 정보시스템에서 타 기관으로 유통되는 개인정보의 분류

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- >과 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

(1) 서울시 홈페이지 회원의 개인정보 분류

서울시의 오프라인의 개인정보 분류는 행정자치부 분류의 지침을 따르고 있다. 여기에서는 서울시 전자정부의 개인정보 분류를 필수정보와 선택정보로 나누었다(<표 3-5> 참조).

<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 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 있음을 앞에서 정리한 표를 보면 알 수 있다.

서울시 전자정부의 개인정보 분류는 민감성 정보나 고용, 금융, 신용 정보 등에 대한 정보는 거의 가지고 있지 못한 것으로 보인다.

(2) 서울시 전자정부 홈페이지의 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 전자정부에

서는 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 가입시의 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

하지만 서울시 전자정부의 개인정보 축적 관리에서 탈퇴한 회원의 개인정보를 관리하므로 인해 문제가 되고 있다. 서울시 전자정부 통합회원과 E-mail 회원이 탈퇴할 경우 개인의 정보는 가입 시 정보가 그대로 축적되어 그 정보를 관리하고 있다. 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 규정을 어기면서 그 개인정보를 가지는 것은 개인정보보호에 있어 누출·침해라고 볼 수 있다.

제3절 서울시 개인정보 보호관련 인식조사

1. 서울시민의 개인정보보호 인식

1) 조사개요

(1) 조사대상과 조사방법

이 조사는 서울시민을 대상으로 모바일을 통한 전화 조사를 실시하였다. 조사의 객관성을 확보하기 위해 서울시 인구구성을 반영한 표본을 구성하였는데, 이 과정에서 권역별 할당표본을 실시한 다음 권역별 인구규모를 반영한 가중치를 부여한 다음 분석을 실시하였다.

(2) 조사내용 및 조사기간

설문지는 개인정보의 종류, 공공부문에서의 개인정보 관리, 개인정보 공개 범위, 개인정보의 취급에 대한 공개, 공공부문과 민간부문의 개인정보보호 차이, 반드시 보호되어야 할 개인정보, 서울시 전자정부 사이트 방문경험, 개인정보 누출 및 침해에 대한 형·사법 제도 강화, 개인정보 누출로 인한 침해시의 대응 등에 대해 응답자의 판단을 묻기로 하였다. 조사는 2004년 5월 24-25일에 실시되었다.

(3) 응답자의 특성

설문 응답자는 총 513명이었으며 이들을 성별, 연령대, 직업, 거주 권역, 교육수준 분포는 <표 3-7>과 같다.

<표 3-7> 시민조사 응답자의 특성

		사 례 수	빈도(%)
전 체		513	100.0
성 별	남자	252	49.1
	여자	261	50.9
연 령 대	10대	49	9.6
	20대	127	24.8
	30대	116	22.6
	40대	100	19.5
	50대이상	121	23.6
직 업	자영업	54	10.5
	블루칼라	61	11.9
	화이트칼라	153	29.8
	학생	97	18.9
	가정주부	86	16.8
	무직/기타	63	12.3
권 역	도심	29	5.7
	동북	167	32.6
	서북	63	12.3
	서남	150	29.2
	동남	104	20.3
교육수준	중졸이하	24	4.7
	고졸	235	45.8
	대졸	221	43.1
	대학원졸이상	34	6.6

※ 권역의 구분은 도심(중구, 종로구, 용산구), 동북(성동, 광진, 동대문, 중랑, 성북, 강북, 도봉, 노원), 서북(은평, 서대문, 마포구), 서남(양천, 강서, 구로, 금천, 영등포, 동작, 관악), 동남(서초, 강남, 송파, 강동) 이다.

2) 조사결과 분석

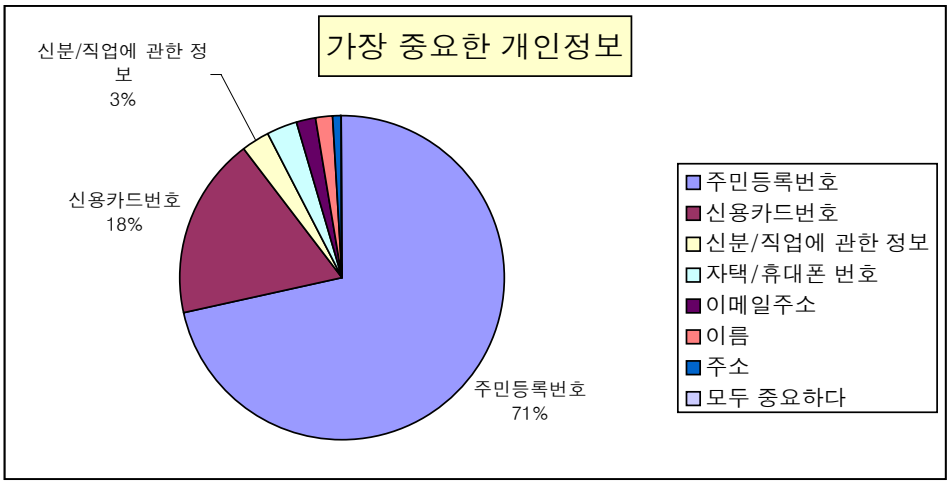
(1) 개인정보 일반

① 중요한 개인정보의 순위

개인정보보호와 관련한 조사에서 시민들이 가장 중요하게 여기는 개인정보는 주민등록번호(71.3%)로 나타났다. 신용카드번호(18.3%)로 그 다음이지만 그 차이가 많았다. 개인정보 중에서 주민등록번호가 높다는 것은 성별, 연령, 교육수준 등과 상관없이 높게 나타났다. 즉 주민등록번호가 개인정보 중 가장 중요하게 여기는 개인정보로 보호가 가장 필요하다고 할 수 있다.

<표 3-8> 가장 중요한 개인정보의 종류

	사례 수	주민등록번호	신용카드번호	신분 직업에 관한 정보	자택 휴대폰 전화번호	이메일 주소	이름	주소	모두 중요하다	무응답	합계
합계	513	71.3	18.3	3.0	2.9	2.0	1.6	0.8	0.1	0.0	100.0

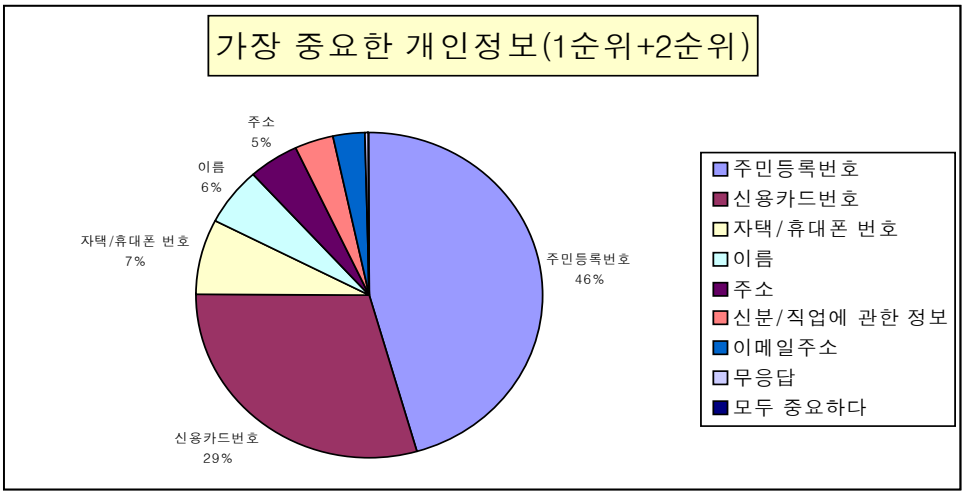


<그림 3-1> 가장 중요한 개인정보

가장 중요한 개인정보를 1순위/2순위로 응답해 달라는 질문 역시 가장 중요한 개인정보는 주민등록번호와 신용카드번호라고 응답하는 것을 <표 3- >에서 볼 수 있다.

<표 3-9> 가장 중요한 개인정보(1순위+2순위)

		사례 수	이름	주소	주민등록번호	이메일 주소	자택 휴대폰 전화번호	신용카드 번호	신분 직업에 관한 정보	모두 중요하다	무응답
합계		513	11.5	9.6	91.4	6.0	15.0	58.9	7.2	0.2	0.6
성별	남자	252	9.1	11.5	87.7	7.5	17.9	56.3	9.9	0.4	0.0
	여자	261	13.8	7.7	94.6	4.6	12.6	61.3	4.6	0.0	1.1
연령대	10대	49	12.2	14.3	98.0	0.0	12.2	55.1	10.2	0.0	0.0
	20대	127	11.8	5.5	90.6	6.3	20.5	57.5	8.7	0.0	0.0
	30대	116	5.2	12.9	92.2	3.4	16.4	62.1	6.0	0.9	0.0
	40대	100	9.0	11.0	86.0	11.0	19.0	56.0	9.0	0.0	0.0
	50대이상	121	19.0	7.4	93.4	6.6	5.8	60.3	4.1	0.0	2.5
직업	자영업	54	24.1	14.8	90.7	5.6	16.7	40.7	5.6	0.0	0.0
	블루칼라	61	8.2	11.5	91.8	6.6	14.8	57.4	8.2	1.6	0.0
	화이트칼라	153	8.5	5.2	89.5	7.8	19.6	57.5	11.8	0.0	0.0
	학생	97	14.4	13.4	91.8	1.0	13.4	56.7	9.3	0.0	0.0
	가정주부	86	8.1	9.3	95.3	3.5	5.8	74.4	1.2	0.0	3.5
	무직/기타	63	9.5	7.9	92.1	11.1	19.0	57.1	1.6	0.0	0.0



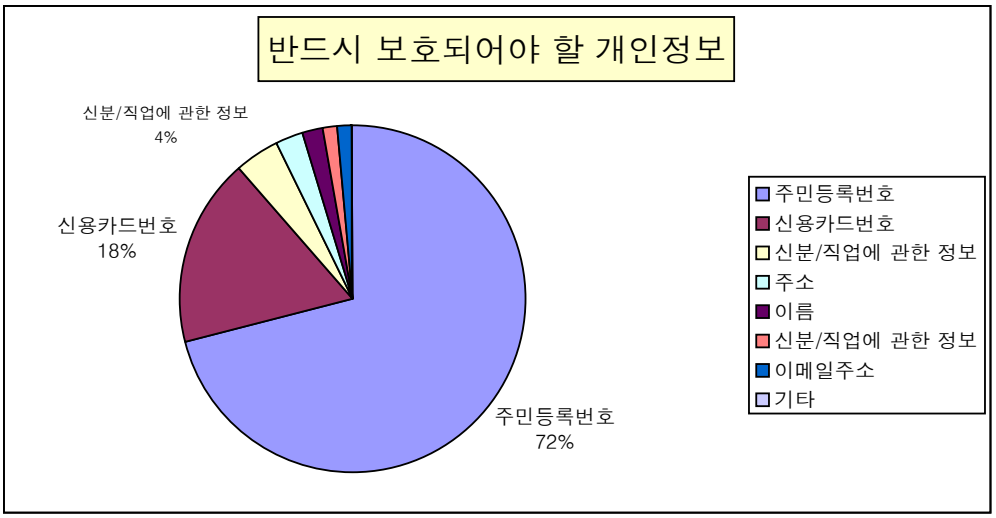
<그림 3-2> 가장 중요한 개인정보(1순위+2순위)

② 사생활보호를 위해 반드시 보호되어야 할 개인정보

서울시민들은 사생활 보호를 위해 반드시 보호되어야 할 개인정보 역시 주민등록번호라고 응답하였고, 다음으로 신용카드번호를 꼽았다. 이에 비해 이름, 주소, 이메일 주소, 신분/직업에 관한 정보는 응답이 미미하였다. 정보보호에서 가장 중요한 개인정보와 사생활보호를 위해 보호되어야 할 개인정보가 일치함을 알 수 있다.

<표 3-10> 반드시 보호되어야 할 개인정보

	사례 수	주민등록번호	신용카드번호	자택/휴대폰 전화번호	주소	이름	이메일 주소	신분/직업에 관한 정보	기타	합계
합계	513	70.9	17.8	4.3	2.4	1.8	1.4	1.4	0.0	100.0



<그림 3-3> 반드시 보호되어야 할 개인정보

(2) 서울시의 개인정보 관리

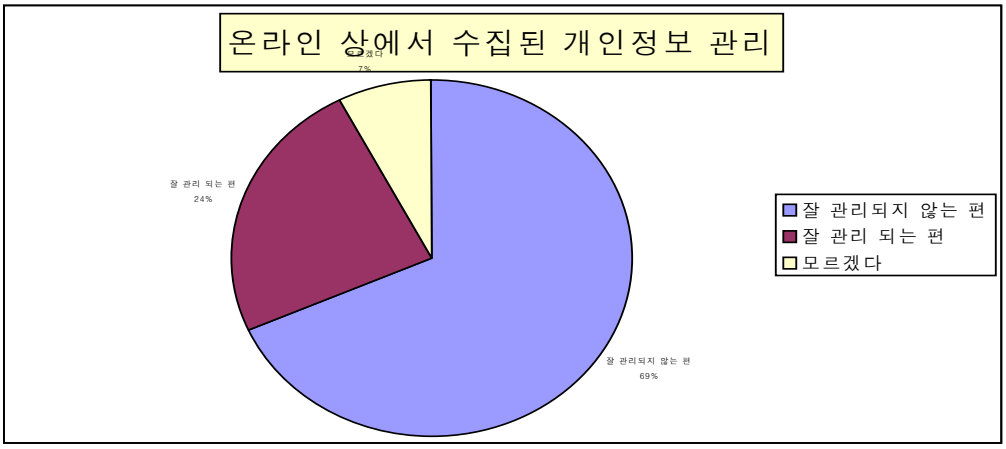
서울시에서 홈페이지를 통해 축적한 개인정보에 대해 시민들은 서울시가 어떻게 관리, 활용, 취급하고 있는가에 대한 인식을 물었다.

① 서울시 홈페이지의 개인정보 관리

서울시 홈페이지를 통해 온라인 상에서 수집된 개인정보의 관리에 대해 68.3%의 시민들이 관리가 '잘 되지 않고 있다'고 인식하고 있다. 서울시가 개인정보의 수집 후 사후관리가 잘 안 된다고 보고 있다. 반면 잘되고 있다고 응답한 응답자는 30%에 미치지 못함을 알 수 있는데 서울시의 개인정보 관리에 있어 변화가 있어야 함을 알 수 있다.

<표 3-11> 온라인 상에서 수집된 개인정보 관리

		사례 수	아주 잘 관리한다	어느 정도 잘 관리하는 편이다	별로 잘 관리하지 않는 편이다	거의 잘 관리하지 않는다	잘 모르겠다	합계
합계		513	3.0	21.3	55.4	12.9	7.4	100.0
성별	남자	252	3.3	24.0	48.4	16.9	7.4	100.0
	여자	261	2.6	18.8	62.2	9.0	7.4	100.0
연령대	10대	49	7.7	13.8	54.4	19.0	5.1	100.0
	20대	127	5.3	19.1	47.5	19.8	8.3	100.0
	30대	116	0.3	24.2	51.1	16.3	8.1	100.0
	40대	100	2.8	28.3	53.8	5.1	9.9	100.0
	50대이상	121	1.3	18.3	69.6	6.2	4.6	100.0



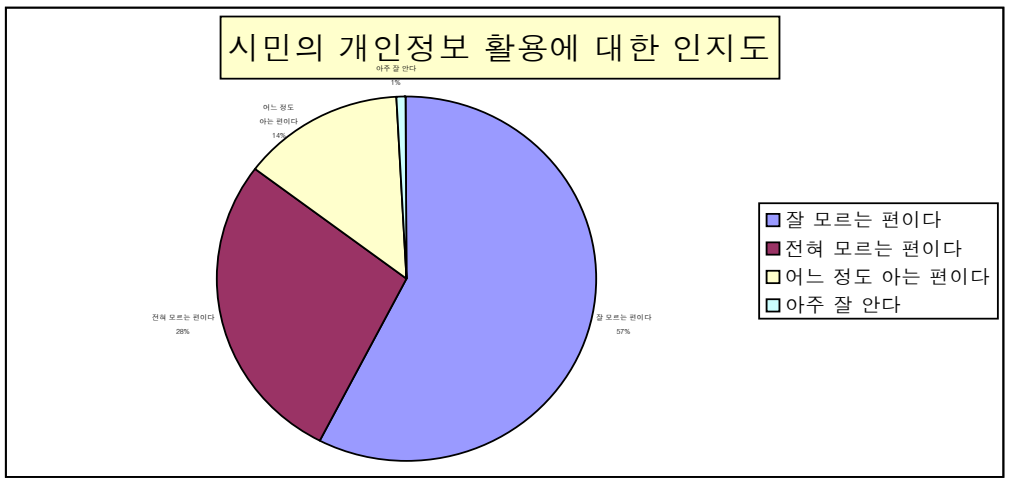
<그림 3-4> 온라인 상에서 수집된 개인정보 관리

② 수집된 개인정보의 활용에 대한 인지도

서울시 전자정부 웹사이트에서 수집된 시민의 개인정보 활용에 있어 서울시가 어떻게 활용하고 있는지에 대해 80% 이상의 시민들이 인지하고 못하고 있다. 자신의 개인정보가 어떻게 활용되고 있는지에 대해 알아야 하지만 서울시의 개인정보 활용에 대한 정보제공은 거의 없다고 보여진다.

<표 3-12> 웹사이트에서 수집된 시민의 개인정보 활용에 대한 인지도

		사례 수	아주 잘 안다	어느 정도 아는 편이다	별로 모르는 편이다	전혀 모른다	합계
합계		513	0.9	13.9	57.5	27.7	100.0
성별	남자	252	1.2	10.1	57.2	31.5	100.0
	여자	261	0.6	17.6	57.8	24.0	100.0
연령대	10대	49	0.0	8.2	59.7	32.1	100.0
	20대	127	0.0	14.4	53.7	31.9	100.0
	30대	116	0.6	8.1	52.1	39.2	100.0
	40대	100	2.8	11.4	57.5	28.3	100.0
	50대이상	121	0.8	23.5	65.9	9.7	100.0



<그림 3-5> 시민의 개인정보 활용에 대한 인지도

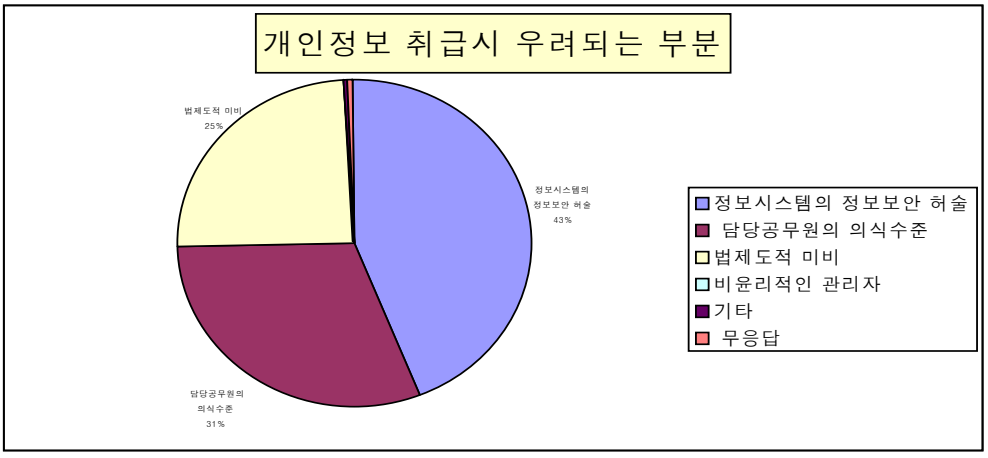
③ 개인정보의 취급

전자정부 서비스의 제공 이후 온라인 웹사이트를 통해 개인정보의 수집, 보유, 활용하는 빈도가 높아지고 있다. 개인정보의 수집, 보유, 활용이 늘어나면서 개인정보의 취급시에 위험이 상존하고 있다. 시민들은 개인정보의 취급시에 가장 우려하는 부분으로 기술적인 요인의 '정보시스템의 정보보안 허술'을 가장 높게 꼽았다. 인적 요인의 '담당공무원의 의식수준'을, 제도적 요인의 '법/제도적 체계의 미비'이라고 각각 응답하였다. '정보시스템의 정보보안 허술', '담당공무원의 의식수준', '법/제도적 체계의 미비'가 높

게 나타난 것은 개인정보의 수집, 보유, 활용 등의 취급에 대해 우려되는 부분이 많다고 느끼고 있음을 보여준다.

<표 3-13> 개인정보 수집/보유/활용 등의 취급시에 우려되는 부분

		사례 수	법/제도적 체계의 미비	담당공무원의 의식수준	정보시스템의 정보보안 허술	비윤리적인 관리자	기타	잘모름/ 무응답	합계
합계		513	24.6	30.7	43.8	0.2	0.1	0.6	100.0
성별	남자	252	24.5	36.7	37.6	0.0	0.1	1.1	100.0
	여자	261	24.7	24.9	49.8	0.4	0.0	0.2	100.0
연령대	10대	49	30.1	9.2	60.7	0.0	0.0	0.0	100.0
	20대	127	28.0	31.0	39.8	0.8	0.0	0.3	100.0
	30대	116	22.8	31.9	44.6	0.0	0.0	0.6	100.0
	40대	100	22.1	38.2	39.4	0.0	0.3	0.0	100.0
	50대이상	121	22.6	31.6	44.0	0.0	0.0	1.8	100.0



<그림 3-6> 개인정보 취급시에 우려되는 부분

(3) 개인정보의 공개

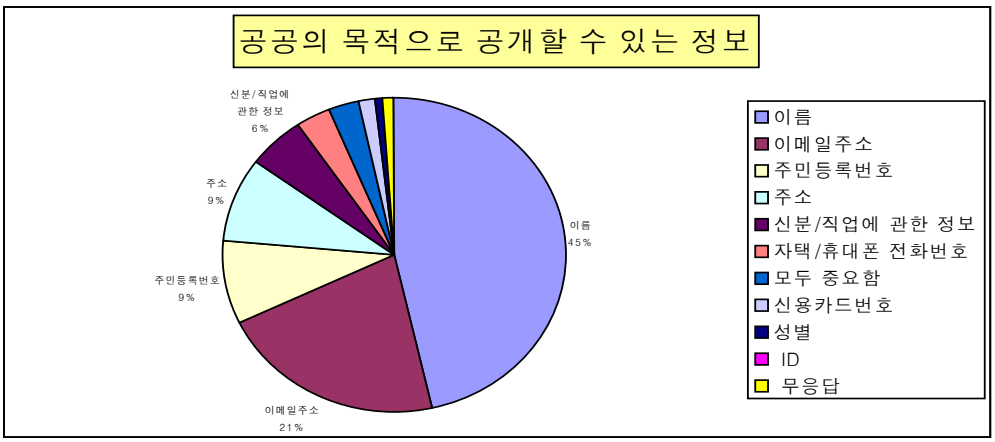
① 개인정보 중 공공적 목적으로 공개할 수 있는 정보

서울시에서 공공의 목적에 활용할 경우 시민들은 웹사이트를 통해 공개할 수 있는 개인정보로 이름(46.3%)을 가장 많이 꼽았고 다음으로 이메일주소(21.4%)라고 응답하였다. 공공의 목적에 활용에 경우에 한해 주민등록번호를 공개할 수 있다는 응답자가

‘신분/직업에 관한 정보’, ‘신용카드번호’ 응답자에 비해 높다. 이는 공공의 목적에 활용된다고 해도 ‘신분/직업에 관한 정보’, ‘신용카드번호’의 경우 공개로 인한 위험이 더 크다고 인식하고 있는 것으로 보인다.

<표 3-14> 개인정보 중 서울시에서 공공적 목적으로 공개할 수 있는 정보

		사례수	이름	주소	주민등록번호	이메일주소	자택 휴대폰 전화번호	신용카드번호	신분/직업에 관한 정보	모두 중요함	성별	ID	무응답	합계
합계		513	46.3	8.5	8.7	21.4	3.3	1.7	5.7	2.6	0.6	0.1	1.0	100.0
성별	남자	252	44.4	10.9	8.9	20.6	3.2	1.0	7.1	2.3	0.0	0.3	1.3	100.0
	여자	261	48.1	6.2	8.5	22.3	3.3	2.4	4.4	2.9	1.1	0.0	0.8	100.0
연령대	10대	49	63.8	6.8	6.1	17.2	4.1	0.0	2.0	0.0	0.0	0.0	0.0	100.0
	20대	127	48.1	10.0	5.4	20.9	5.0	1.4	6.5	1.8	0.0	0.0	0.9	100.0
	30대	116	41.1	11.0	9.7	19.6	2.1	1.0	4.6	5.6	2.5	0.6	2.1	100.0
	40대	100	47.6	7.6	6.2	20.4	1.3	4.3	10.3	1.6	0.0	0.0	0.8	100.0
	50대 이상	121	41.1	5.9	14.3	26.3	3.8	1.4	3.8	2.5	0.0	0.0	0.8	100.0



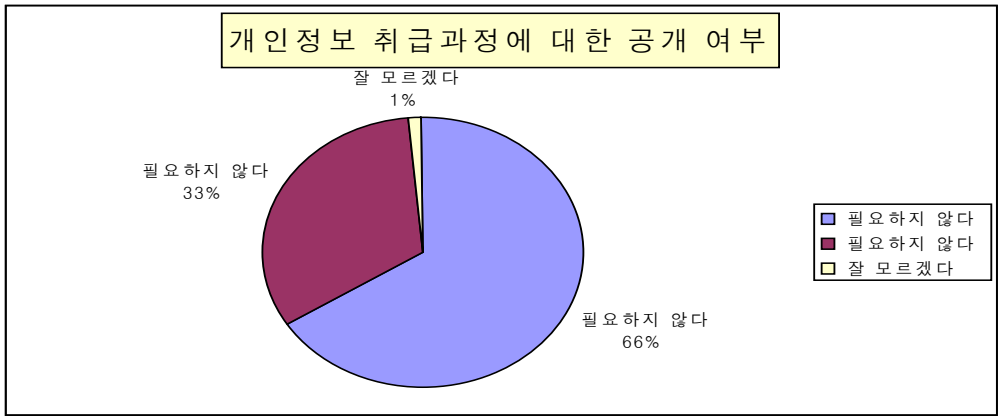
<그림 3-7> 공공의 목적으로 공개할 수 있는 정보

② 개인정보 취급과정에 대한 정보의 공개 여부

서울시에 축적된 개인정보의 취급과정에 대한 정보의 공개 여부에 대해 시민들은 공개해야 한다는 의견이 많았다. 특히 10대의 경우 80%가 넘는 응답자가 필요하다라고 응답하였고, 20대는 ‘필요하지 않다’ 라는 응답(39.6%)이 타 연령대에 비해 높았다.

<표 3-15 > 개인정보 취급과정에 대한 정보의 공개 여부

		사례 수	전혀 필요하지 않다	별로 필요하지 않다	어느정도 필요하다	매우 필요하다	잘 모르겠다	합계
합계		513	16.4	16.5	38.1	27.6	1.4	100.0
연령대	10대	49	13.8	4.8	40.3	41.2	0.0	100.0
	20대	127	17.8	21.8	31.4	26.5	2.4	100.0
	30대	116	16.0	18.9	34.3	30.3	0.5	100.0
	40대	100	18.3	17.0	31.2	30.5	3.0	100.0
	50대이상	121	14.9	13.2	53.5	18.1	0.5	100.0



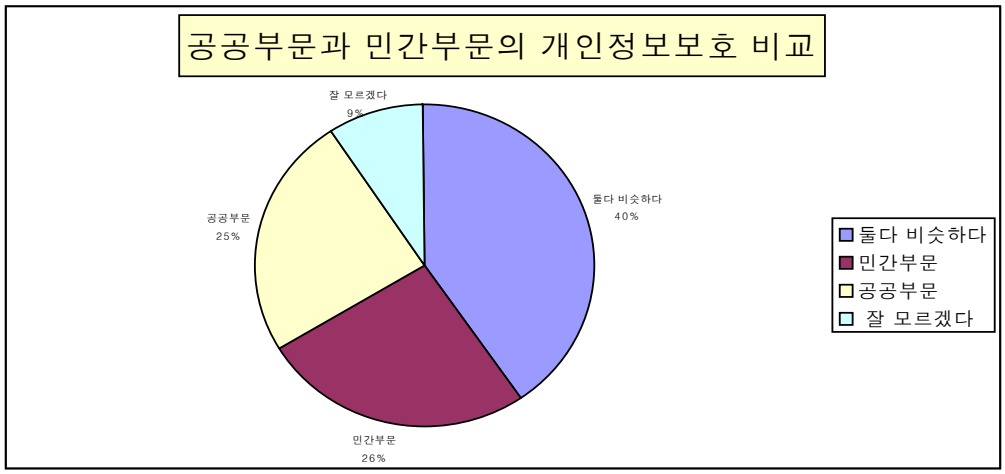
<그림 3-8> 개인정보 취급과정에 대한 정보의 공개 여부

(3) 공공부문과 민간부분의 개인정보보호 비교

웹사이트에서의 개인정보보호와 관련해 공공부문과 민간부문 중 어느 부문이 더 잘 보호하고 있는가에 대해 시민들은 차이가 별로 없다고 응답하였다. 하지만 연령대와 직업에 따라서는 조금 차이가 있다. 먼저 연령대를 비교해 보면 10대, 20대, 30대는 민간부문이 더 개인정보보호를 잘 하고 있다고 인식하는데 비해 40대, 50대 이상의 연령대에서는 공공부문이 더 잘 하고 있다고 응답하였다. 또한 직업에 따라 블루칼라, 화이트칼라, 학생은 민간부문이, 자영업, 가정주부, 무직/기타는 공공부문이 높다고 응답하였다.

<표 3-16> 공공부문과 민간부분의 개인정보보호 비교

		사례 수	민간부문	공공부문	둘 다 비슷하다	잘 모르겠다	합계
합계		513	25.9	24.6	40.3	9.2	100.0
연령대	10대	49	24.5	17.3	47.3	10.9	100.0
	20대	127	29.6	18.3	43.1	9.1	100.0
	30대	116	28.7	26.0	35.8	9.5	100.0
	40대	100	25.0	27.1	34.2	13.7	100.0
	50대이상	121	20.7	30.6	43.9	4.8	100.0
직업	자영업	54	23.9	27.3	37.9	10.9	100.0
	블루칼라	61	34.2	26.4	30.9	8.5	100.0
	화이트칼라	153	28.8	22.4	39.8	9.1	100.0
	학생	97	29.7	18.0	41.0	11.3	100.0
	가정주부	86	16.2	36.2	39.2	8.4	100.0
	무직/기타	63	19.8	20.1	53.0	7.1	100.0



<그림 3-9> 공공부문과 민간부분의 개인정보보호 비교

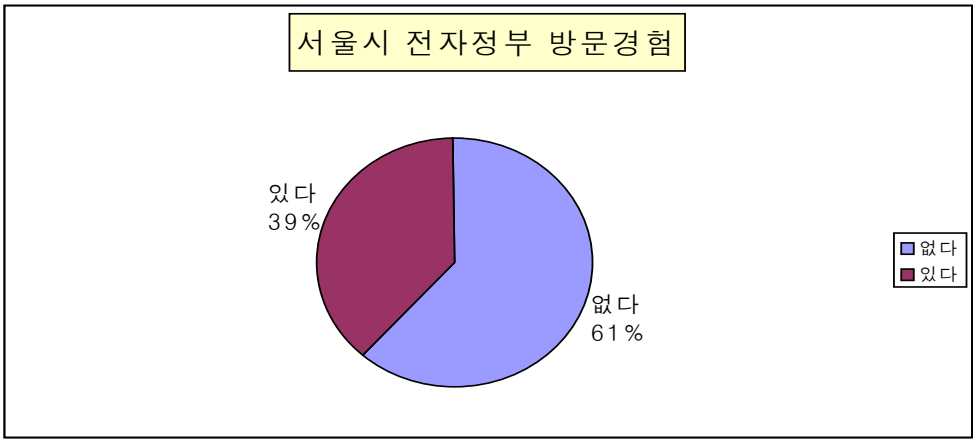
(4) 서울시 전자정부 방문 경험 여부

서울시는 전자정부를 통해 행정서비스를 제공하고 있다. 오프라인 위주의 행정서비스에서 온라인 행정서비스의 비중이 높아지고 있지만 서울시 홈페이지를 방문한 경험은 아직 적음을 알 수 있다. 여자보다는 남자가, 30대와 40대가, 블루칼라와 화이트칼라가 상대적으로 방문경험이 높음을 알 수 있다. 보편적인 행정서비스로 자리 잡기 위

해서는 성별, 연령대, 직업에 관계없이 방문경험이 방문하지 않은 응답자 보다 높을 때 전자정부의 활성화가 이루어질 수 있을 것이다.

<표 3-17> 서울시 전자정부 홈페이지 방문경험

		사례 수	있다	없다	합계
합계		513	38.5	61.5	100.0
성별	남자	252	47.7	52.3	100.0
	여자	261	29.6	70.4	100.0
연령대	10대	49	22.8	77.2	100.0
	20대	127	31.2	68.8	100.0
	30대	116	49.3	50.7	100.0
	40대	100	49.8	50.2	100.0
	50대이상	121	32.8	67.2	100.0
직업	자영업	54	35.2	64.8	100.0
	블루칼라	61	40.9	59.1	100.0
	화이트칼라	153	51.3	48.7	100.0
	학생	97	30.4	69.6	100.0
	가정주부	86	26.8	73.2	100.0
	무직/기타	63	36.4	63.6	100.0



<그림 3-10> 서울시 전자정부 홈페이지 방문경험

(5) 개인정보 누출 및 침해

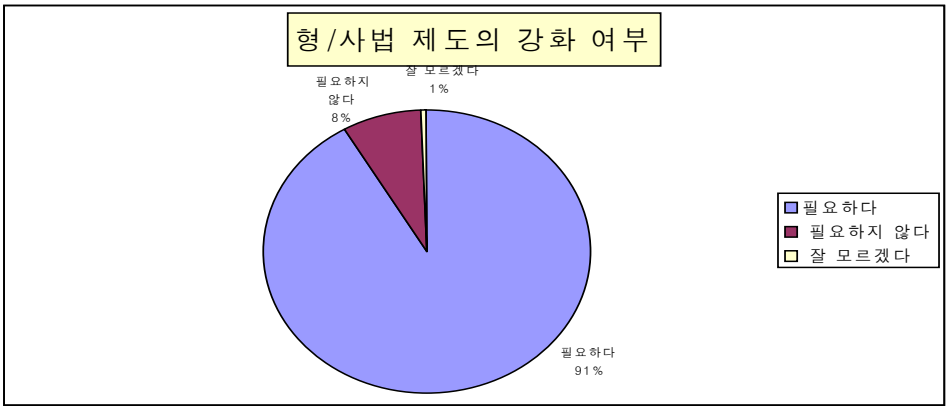
① 개인정보 누출 및 침해에 대한 형·사법 제도의 강화

서울시 전자정부 DB에 축적된 개인정보는 여러 가지 이유로 누출 및 침해될 수 있

다. 개인정보의 누출 및 침해를 막기 위한 한 수단으로 형·사법 제도의 강화에 대해 대다수의 시민들은 '매우 필요하다'는 응답을 하였다.

<표 3-18> 개인정보 누출 및 침해에 대한 형·사법 제도의 강화 여부

		사례 수	전혀 필요하지 않다	별로 필요하지 않다	어느 정도 필요하다	매우 필요하다	잘 모르겠다	합계
합계		513	3.8	3.9	26.6	65.2	0.5	100.0
연령대	10대	49	9.9	0.0	19.6	68.5	2.0	100.0
	20대	127	5.2	4.0	19.4	71.4	0.0	100.0
	30대	116	4.3	5.2	21.7	68.8	0.0	100.0
	40대	100	1.8	2.5	19.6	74.7	1.5	100.0
	50대이상	121	1.1	5.4	47.5	46.0	0.0	100.0



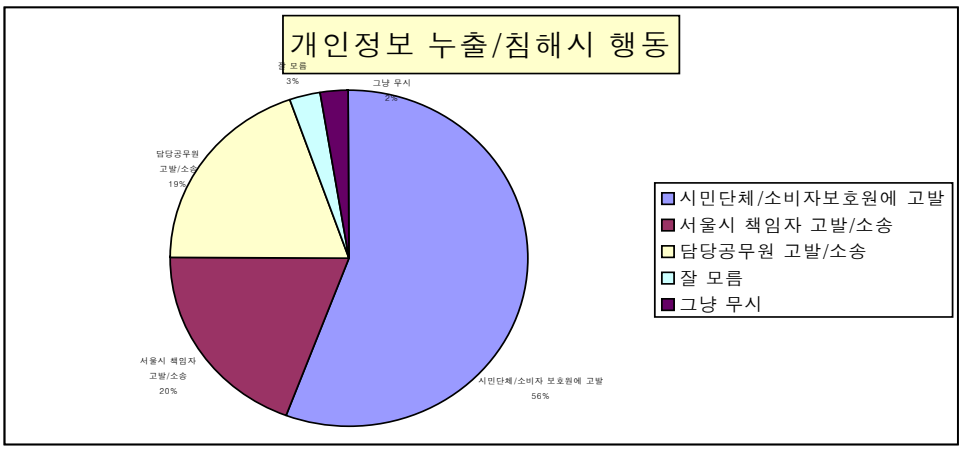
<그림 3-11> 개인정보 누출 및 침해에 대한 형·사법 제도의 강화 여부

② 개인정보 누출 및 침해시 대응 방안

서울시 전자정부에 축적된 개인정보가 누출 및 침해시에 어떠한 대응을 하겠는가라는 질문에 '시민단체 소비자보호원에 고발한다'라는 응답이 가장 높았다. '담당공무원의 고발/소송', '서울시 책임자 고발/소송' 보다 훨씬 높음을 볼 수 있는데, 고발/소송보다는 시민단체나 소비자보호원에 고발 하는게 문제 해결에 더 도움이 된다고 보고 있는 것은 법적인 대응에 대한 믿음이 부족하다고 인식하고 있다고 보여진다.

<표 3-19> 개인정보 누출 및 침해시 행동

		사례 수	담당공무원 고발/소송	서울시 책임자 고발/소송	시민단체 소비자보호원에 고발한다	그냥 무시하겠다	잘 모르겠다	합계
합계		513	19.5	19.7	55.5	2.5	2.9	100.0
연령대	10대	49	23.6	35.4	37.9	3.1	0.0	100.0
	20대	127	24.1	20.8	51.8	0.0	3.3	100.0
	30대	116	24.0	18.0	55.4	2.2	0.3	100.0
	40대	100	15.5	13.2	58.7	7.0	5.5	100.0
	50대이상	121	11.9	19.0	63.8	1.3	4.0	100.0



<그림 3-12> 개인정보 누출 및 침해시 행동

3) 조사결과의 요약 및 함의

서울시 전자정부의 개인정보보호에 대한 조사 내용으로는 개인정보의 종류와 중요도 순위, 공공부문에서의 개인정보 관리, 개인정보 공개 범위, 개인정보의 취급에 대한 공개, 공공부문과 민간부문의 개인정보보호 차이, 반드시 보호되어야 할 개인정보, 서울시 전자정부 사이트 방문경험, 개인정보 누출 및 침해에 대한 형·사법 제도 강화, 개인정보 누출로 인한 침해시의 대응 등이다. 조사결과를 통해 우리는 개인정보보호의 정책방향 설정이 필요한 기초 자료를 확보하였으며, 시민들의 개인정보보호에 대한 인식 정도를 파악할 수 있었다.

(1) 개인정보의 종류와 중요도

개인정보보호와 관련한 조사에서 시민들이 가장 중요하게 여기는 개인정보는 주민등록번호, 신용카드번호였다. 시민 개개인의 주민등록번호와 신용카드번호 보호에 중점을 두고 개인정보보호 방안을 찾으면 개인정보보호와 관련해 발생하는 문제의 상당부분을 사전에 방지할 수 있을 것이다. 또한 사생활보호를 위해 반드시 보호되어야 할 개인정보로 인식하는 정보도 주님등록번호와 신용카드번호를 꼽았는데 중요도 높은 개인정보와 일치하였다. 시민들은 개인정보보호에 있어 주민등록번호와 신용카드번호는 반드시 보호되어야 한다는 인식을 나타냈다.

(2) 서울시의 개인정보 관리

서울시에서 홈페이지를 통해 축적한 개인정보의 관리에 대해 시민들은 '잘 되지 않고 있다'고 인식하고 이에 대한 대응방안이 필요한 것으로 생각하고 있었다. 또한 행정적인 필요성에 의해 수집된 개인정보의 활용에 있어 서울시가 어떻게 하고 있는지에 대한 인지도가 낮았다. 이러한 결과는 서울시가 시민들의 개인정보 활용현황에 대해 좀 더 충분하게 공지할 필요가 있음을 말하는 것이다.

개인정보의 취급에 있어서 '정보시스템의 정보보안 허술', '담당공무원의 의식수준', '법/제도적 체계의 미비' 등의 항목이 높게 나타난 것은 개인정보의 수집, 보유, 활용 등의 취급에 대해 우려되는 부분이 많다고 느끼고 있음을 보여준다.

(3) 개인정보의 공개

개인정보 중 공공적 목적으로 활용할 때 공개할 수 있는 정보로 이름, 이메일주소를 높게 꼽았고 반면에 개인정보보호가 필요한 중요정보라고 인식하였던 '신용카드번호'는 공개를 할 수 없다는 입장을 취하였다. 서울시에 축적된 개인정보의 취급과정에 대한 정보의 공개 여부에 대해 시민들은 공개해야 한다는 의견이 많았다.

(4) 공공부문과 민간부분의 개인정보보호 비교

웹사이트에서의 개인정보보호와 관련해 공공부문과 민간부문 중 어느 부문이 더

잘 보호하고 있는가에 대해 시민들은 차이가 별로 없다고 응답하였다. 이는 광범위한 개인정보를 수집, 활용하고 있는 공공부문의 개인정보보호에 있어 보다 강화할 필요가 있다고 생각하는 것으로 보여진다.

(5) 서울시 전자정부의 방문 경험 여부

서울시는 전자정부를 통해 행정서비스를 제공하고 있다. 오프라인 위주의 행정서비스에서 온라인 행정서비스의 비중이 높아지고 있지만 서울시 홈페이지를 방문한 경험은 아직 적음을 알 수 있다. 전자정부의 이용율을 높이기 위한 방안이 개인정보보호 방안과 함께 이루어져야 할 것이다.

(6) 개인정보 누출 및 침해

개인정보의 누출 및 침해를 막기 위한 한 수단으로 형·사법 제도의 강화에 대해 대다수의 시민들은 '매우 필요하다'는 응답을 하였고, 개인정보의 누출·침해에 대해 '시민단체 소비자보호원에 고발한다'하는 것이 누출 및 침해를 행한 담당자나 기관을 고발/소송하는 것보다 시민단체나 소비자보호원에 고발하는 것이 문제 해결에 더 도움이 될 것으로 생각하고 있었다.

2. 서울시 공무원 정보보호 인식

1) 조사개요

(1) 조사대상과 조사방법

이 조사는 서울시 25개 자치구의 개인정보 및 정보보안 업무를 담당하는 공무원을 대상으로 하여 면접조사와 전화조사, E-mail조사를 병행해서 실시하였다.

(2) 조사내용 및 조사기간

설문지는 공통항목으로 개인정보의 종류, 개인정보 공개범위, 가장 중요한 개인정보로, 서울시 개인정보보호와 정보보안 항목으로 서울시 전자정부의 개인정보보호와 정

보보안 정책, 정책의 저해요인, 개인정보 누출 및 침해시의 서울시의 문제해결 방안을, 자치구의 개인정보보호와 정보보안 항목으로 자치구의 개인정보보호 노력, 정보보안의 중점 사항 등에 대해 응답자의 판단을 묻기로 하였다. 조사는 2004년 5월 17-26일에 실시되었다.

2) 조사결과 분석

(1) 공통항목: 개인정보 종류, 공개범위, 중요한 개인정보

① 보호가 필요가 개인정보의 종류

개인정보보호 및 정보보안 업무를 담당하는 자치구의 공무원들은 보호가 필요한 개인정보로 주민등록번호와 신용카드라고 응답하였다. 이는 시민조사에서의 결과와 비교해 보면 담당공무원과 시민의 인식이 일치함을 알 수 있다.

② 개인정보의 공개 범위

행정서비스 제공 시에 공개할 수 있는 개인정보의 범위에 대해 이름과 E-mail address라고 응답했는데 이것 역시 시민조사와 큰 차이가 없음을 알 수 있다.

③ 가장 중요한 개인정보의 우선순위

개인정보 중에서 보호되어야 할 가장 중요한 개인정보의 순위에 대해 1순위 개인정보로 '주민등록번호'가 가장 많았고 다음으로 '신용카드번호'였다. 2순위는 '신용카드번호'라고 가장 많은 응답을 하였고 다음으로 '주민등록번호'를 꼽았다. 3순위는 '주소'와 '이메일 주소'를 응답하였다. '신분/직업에 대한 정보'나 '자택/휴대폰 전화번호'는 응답이 적었다.

(2) 서울시 자치구 공무원의 개인정보보호와 정보보안 항목

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'

이라고 12개 구청의 담당자가 응답하였다. ‘개인정보보호및정보보안관련조례 제정’(3명 응답), ‘개인정보보호 책임관 지정/운영의 활성화’(4명 응답), ‘최신의 정보보안 시스템 도입’(2명 응답)에 대해서는 응답률이 낮았다. 자치구의 업무담당자들은 서울시 전자정부의 개인정보보호 및 정보보안을 담당하는 독립기구의 설치/운영을 통해, 통합된 개인정보보호 및 정보보안 정책이 이루어져야 한다는 생각을 가진 것으로 보인다.

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’(2명 응답), ‘기술발전 속도에 뒤진 정보보안 시스템’(4명 응답)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.

(3) 자치구의 개인정보보호와 정보보안 항목

① 소속기관의 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 자치구가 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.

② 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 응답률이 낮거나 응답이 없었다.

3) 조사결과 요약 및 함의

(1) 공통항목

개인정보보호 및 정보보안 업무를 담당하는 공무원들은 보호가 필요한 개인정보로 주민등록번호와 신용카드라고 응답하였고, 개인정보 공개 범위에 대한 질문에 공개가 가능한 개인정보로 이름과 E-mail address라고 응답했다. 또한 보호되어야 할 가장 중요한 개인정보의 우선순위에서 1순위에는 주민등록번호, 2순위에는 신용카드번호, 3순위에는 주소와 이메일 주소라고 인식하고 있다.

(2) 서울시 개인정보보호와 정보보안 항목

업무담당자들은 서울시 전자정부의 개인정보보호와 정보보안 정책에서 가장 시급한 정책으로 '독립적인 개인정보보호 및 정보보안 기구의 설치/운영'을, 저해요인으로 '전문인력 확보의 어려움'과 '담당자 및 정책결정자의 소극적인 자세'라고 응답하였다.

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

하였다.

(3) 자치구의 개인정보보호와 정보보안 항목

개인정보를 가장 많이 수집, 보관, 관리하는 자치구는 서울시의 개인정보보호 정책과 함께 자체의 정책을 함께 시행하고 있고, 정보보안을 위해 '업무상 중요한 사항에 관한 보안대책'에 가장 중점을 주는 항목으로, 다음으로 '패스워드/메일주소 등의 정보보안에 관한 기본항목'이라고 인식하고 있다.

3. 공통점과 차이점

1) 공통점

공공부문과 시민영역의 조사에서 일치하는 항목은 가장 중요한 개인정보와 공개 가능한 개인정보의 종류이다.

(1) 가장 중요한 개인정보의 종류

공공부문과 시민영역을 대상으로 공통으로 조사를 한 가장 중요한 개인정보라고 응답한 것은 '주민등록번호'였고 그 다음으로 '신용카드번호'였다. 이는 공공부문과 시민영역에서의 인식이 일치함을 볼 수 있고 개인정보보호에 있어 가장 우선되어야 할 것으로 두 가지가 고려되어야 함을 보여준다.

(2) 공개 가능한 개인정보

공공부문과 시민영역의 응답자들은 가장 중요한 개인정보보호 항목과 마찬가지로 이름과 E-mail address를 꼽았다. 서로 다른 부문의 응답자들이 같은 항목을 응답한 것은 이름과 E-mail address가 다른 개인정보에 비해 누출시 피해가 적기 때문인 것으로 보인다.

2) 차이점

개인정보의 누출 및 침해의 예방과 침해시의 대응방안에 있어 공공부문은 신속한 침해안내를 통보하고 사고에 따른 문제분석 및 예방방법 안내, 개인정보 침해대응센타를 통한 대응, 개인정보 해킹방지를 위한 개인정보의 암호화, 개인정보보호담당자에 대한 주기적인 교육실시, 개인정보침해 보상제도 운영, 정보시스템 구축 시 개인정보의 오남용, 유출방지 프로그램을 설치 등을 제시하였다. 반면에 시민영역은 ' 시민단체 소비자보호원에 고발한다'라는 응답이 많았다. 이는 공공부문은 사전 예방적 문제해결에 중점을 두는 반면에 시민영역은 공공부문의 사전예방 방안을 신뢰하기보다는 사후문제 해결 방법에 더 중점을 두는 것으로 보여 진다.

제4장 외국 전자정부의 개인정보보호 제도

제1절 프라이버시 영향 평가제도

제2절 개인정보보호 지침

제3절 뉴욕주의 정보보호 정책

제4장 외국 전자정부의 개인정보보호 제도

제1절 프라이버시 영향 평가제도

1. 프라이버시영향 평가제도

1) 개념

전자정부에서의 개인정보 및 프라이버시 보호를 위하여 전자정부 사업의 계획 단계에서부터 당해 사업이 '개인정보 및 프라이버시에 미치는 영향'을 검토하는 것을 말한다.

2) 필요성

전자정부 사업의 계획 단계에서부터 프라이버시 영향 평가를 실시함으로써 정부기관에 의한 프라이버시 침해 가능성을 최소화하고 국민의 전자정부 사업에 대한 불신감을 해소하였다.

프라이버시 영향 평가의 성공적인 수행을 통해 전자정부 사업추진 후에 개인정보 및 프라이버시 보호 문제를 이유로 당해 사업을 중단하거나 변경하게 되는 위험성을 제거함으로써 예산의 낭비를 미연에 방지한다.

2. 캐나다의 프라이버시 영향 평가제도

1) 도입과정 및 배경

(1) 도입과정

캐나다는 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(재무

부장관은 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[13]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.

동 정책 및 지침은 캐나다 국민에 대해 프라이버시 영향 평가 방법의 개발 및 유지에 관한 사항을 고지하고 프라이버시 영향 평가 결과를 정기적으로 공개함으로써 캐나다 정부가 프라이버시 침해 가능성이 있는 프로그램 및 서비스를 추진함에 있어 프라이버시 보호 원칙을 적극 반영하고 있음을 주지시키는 것을 목적으로 하고 있다.

(2) 도입배경

정부기관은 당해 기관이 제공하는 프로그램 및 서비스의 구상, 분석, 고안, 개발, 시행 및 사후 검토에 이르기까지 전 과정에 걸쳐 개인정보의 수집, 이용 및 공개 등과 관련하여 프라이버시법 및 프라이버시 보호 원칙을 준수하고 있음을 명백히 밝힐 책임이 있다.

또한, 정부기관은 개인정보의 수집이유, 개인정보의 이용 및 공개방법 등에 관하여 일반 국민과 지속적으로 의견을 교환해야 하며, 신규 프로그램 및 서비스를 제공하는 경우에는 동 프로그램 및 서비스가 프라이버시에 미치는 영향 및 그 해결방안에 대해 설명할 책임이 있다.

따라서, 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 필요

13) 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.

한 정보를 제공한다. 사업추진 후에 프라이버시 문제를 이유로 사업을 중단하거나 변경하는 위험을 감소시키고, 정부기관이 이용하는 개인정보 관련 업무절차 및 흐름을 문서화하여 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.

2) 프라이버시 영향 평가의 내용 및 절차

(1) 1단계: 프라이버시 영향 평가 필요성 판단(Project Initiation)

프라이버시 침해 가능성이 있는 신규 프로그램 및 서비스에 대하여 사전에 프라이버시 영향 평가의 필요성을 판단하고 평가 범위를 확정하는 단계이다.

프라이버시 영향 평가를 실시할 필요가 있는 경우이다. 개인의 동의여부를 불문하고 개인정보를 신규로 수집, 이용, 공개하거나 기존의 개인정보 수집, 이용, 공개 범위 확대한다. 개인정보의 수집대상 확대, 개인정보의 수집방법을 직접적인 방법에서 간접적인 방법으로 변경, 프로그램의 통합, 관리 등을 목적으로 한 개인정보의 수집 확대, 프로그램간, 기관간, 공공·민간부문간 개인정보의 일치 및 공유, 공통된 개인 식별자의 신규 개발 또는 사용 확대, 개인정보의 물리적 또는 논리적 분리와 관계 있는 업무절차나 업무시스템, 또는 개인정보에 대한 접근을 관리 및 통제하기 위하여 사용되는 보안체계의 중대한 변화, 계약 등을 통한 프로그램이나 서비스의 정부기관 또는 민간부문 이전[14]이다.

한편, 프로그램이나 서비스에 대한 구체적 사업계획이 수립되기 전 초기 단계에서는 예비적 프라이버시 영향 평가(Preliminary PIA)를 실시할 수 있으며 이후 필요에 따라 전면적인 프라이버시 영향 평가 실시이다. 예비적 프라이버시 영향 평가의 필요성에 대해서는 각 기관의 담당자가 판단하고 프라이버시 영향 평가의 필요성이 명백히 드러나지 않는 경우에도 예비적 프라이버시 영향 평가는 실시 가능하다.

---

14) 본 정책 시행 전에 추진된 프로그램이나 서비스의 경우에는 전자정부의 특성상 개인정보의 수집, 이용 또는 공개되는 형태 등에 있어 본질적인 부분에 대한 변경이 있는 경우에만 프라이버시 영향 평가의 필요성 인정

예비적 프라이버시 영향 평가의 주요 내용을 보면 수집, 이용, 공개되는 개인정보의 양 및 유형 확인, 당해 프로그램 또는 서비스에 관한 법률 및 정책상의 권한 확인 , 주요 관계자의 역할, 책임 및 법적 지위 확인, 프로그램 또는 서비스에서 프라이버시 침해 가능성이 있는 부분 확인, 프라이버시위원회와의 협의 절차 구상, 최종 평가 범위 및 일정 확정이다.

공동관리책임에 의한 프라이버시 영향 평가이다. 프로그램이나 서비스 사업계획의 범위 및 복잡성 등에 따라 프라이버시 영향 평가에 요구되는 전문적 기술이 다양하다. 따라서, 프로그램 및 프로젝트 매니저, 프라이버시 정책 및 법률 전문가, 기능별 또는 기술 전문가 등 관련자에 대해 공동관리책임 부여한다. 다만, 프라이버시 영향 평가의 필요성 여부를 판단할 수 있는 권한은 정부기관의 부기관장에게 있다.

(2) 2단계: 데이터 흐름 분석(Data Flow Analysis)

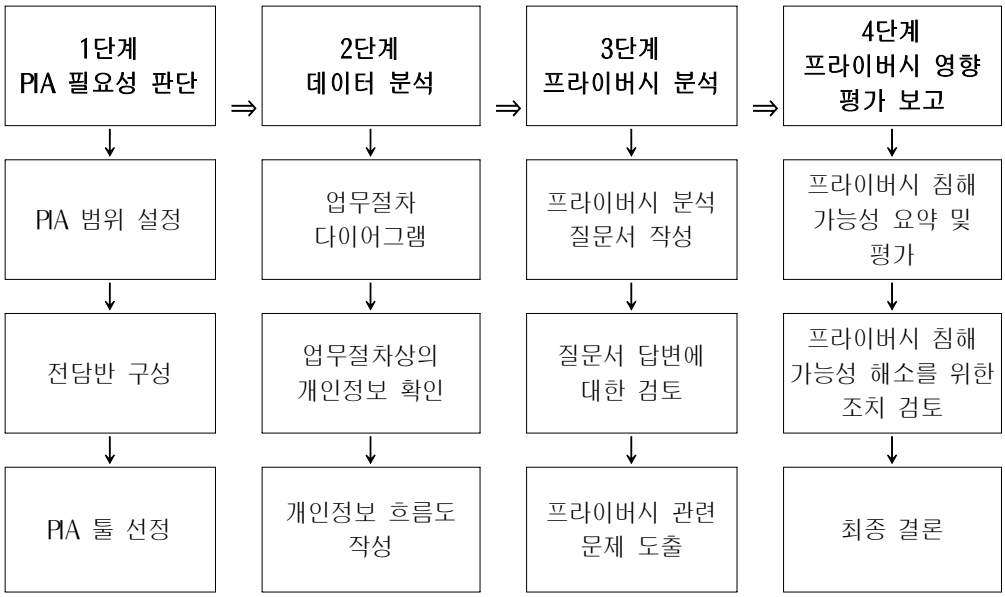
분석하는 단계로서 개인정보의 흐름을 파악하는 것이 목적이다. 데이터 흐름 분석의 3대 구성요소는 첫째, 업무절차 다이어그램으로서 특정 활동 관련 정보흐름에 대한 일반적 기술이다. 둘째, 데이터 흐름도인데 누구의 개인정보가 누구에 의하여 어떠한 방식으로 수집, 이용, 공개 및 보존되는가? 셋째, 시스템 및 인프라 아키텍처 : 개인정보의 물리적 또는 논리적 구분, 개인정보에 대한 부당한 접근을 방지하기 위한 보안체계 등을 문서화이다.

(3) 3단계: 프라이버시 분석(Privacy Analysis)

프라이버시 관련 법률 및 정책 하에서 데이터 흐름을 검토하는 단계이다. 당해 사업계획과 관련된 주요 프라이버시 침해 가능성이나 취약점을 용이하게 확인하기 위하여 질문서 활용한다. 정부기관은 프로그램 및 서비스를 제공하는 과정에서 프라이버시 원칙, 정책 및 법률을 준수하고, 관련 프라이버시 영향 및 침해 가능성이 해소되거나 경감되도록 할 의무가 있다.

(4) 프라이버시 영향 분석 보고(Privacy Impact Analysis Report)

프라이버시 침해 가능성 평가, 프라이버시 침해 가능성 및 관련 문제 해소 또는 경감을 위한 방안 등을 포함하여 이전 단계에서 나온 산출물을 문서화하는 단계이다.



<그림 4-1> 캐나다 프라이버시 영향 평가 절차도

※ 주: 'PIA'는 Privacy Impact Assessment의 약어

3. 미국의 프라이버시 영향 평가제도

1) 프라이버시 영향 평가 제도의 법제화 및 도입배경

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.

2) 프라이버시 영향 평가의 내용

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.

사전분석	· 프로젝트를 위해 영향평가가 필요한가
⇓	
평가의 시기확정	· 프로젝트의 계획단계에서 프라이버시 영향평가를 언제 시행할 것인가?
⇓	
조직 및 사업개요분석	· 현재 조직의 개인정보관리 정책 현황파악과 도입되는 새로운 사업의 개요에 대한 분석
⇓	
정보흐름 분석	· 프로젝트 수행 시 정보 흐름에 대한 정확한 이해, 명확한 파악
⇓	
프라이버시 분석	· 정보의 수집부터 파기까지 제안된 시스템에 대한 모든 면을 조사
⇓	
위험관리	· 위험을 평가하고 그 특성과 심각성을 판단하여 개선계획안 마련
⇓	
영향평가보고서 작성	· 영향평가 결과에 대한 최종보고서 작성과정으로 일반인이 이해하기 쉽게 작성하여 공개

<그림 4-2> 미국의 프라이버시 영향평가 제도의 절차

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

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.

평가결과의 공개는 프라이버시 영향 평가 후 가능한 범위 내에서 기관 웹사이트, 연방관보 또는 기타 수단을 통해 프라이버시 영향 평가의 결과 공개한다. 다만, 보안상의 이유로 또는 프라이버시 영향 평가에 포함되어 있는 민감한 정보나 개인정보를 보호하기 위하여 공개에 관한 사항을 변경하거나 공개 자체를 배제할 수 있다. 평가의 정도 및 내용을 살펴보면 평가되는 정보체계의 규모, 당해 체계에서 신원확인을 가능하게 하는 정보의 민감성, 당해 정보의 무단 공개로 초래되는 위험에 비례하여 프라이버시 영향 평가 수행, 수집할 정보, 당해 정보를 수집하는 이유, 당해 정보의 용도, 정보 공유의 기관, 수집되는 정보 내용과 이를 공유하는 방식과 관련하여 개인의 동의를 얻기 위한 고지 등의 절차, 정보보호 방안, 프라이버시보호법에 따른 기록체계의 생성 여부 등 평가이다.

한편 관리예산처장의 책임으로는 기관의 프라이버시 영향 평가 수행을 위한 정책 및 지침 개발, 범정부적으로 프라이버시 영향 평가의 시행을 감독, 적절하다고 판단하는 범위 내에서 각 기관에 대해 기존 정보 체계나 신원확인이 가능한 정보의 계속적 수집에 관한 프라이버시 영향 평가수행이 가능하다.

4. 함의

1) 도입 및 법제화의 필요성

개인정보 및 프라이버시 침해 가능성이 있는 전자정부 사업을 추진하는 경우, 사업계획 단계에서부터 프라이버시 영향 평가를 실시함으로써 정부기관에 의한 프라이버시 침해 가능성을 최소화하고 일반 국민의 전자정부 사업에 대한 불신감 해소할 수 있다.

프라이버시 영향 평가의 성공적인 수행을 통해 전자정부 사업추진 후에 개인정보 및 프라이버시 보호 문제를 이유로 당해 사업을 중단하거나 변경하게 되는 위험성을

제거함으로써 국가 예산의 낭비를 미연에 방지할 수 있다. 현행 관련 법률은 개인정보의 수집, 관리, 이용 등 개인정보의 취급전반에 관해서는 명문 규정을 두고 있으나, 그 이전 단계인 개인정보와 밀접한 관련이 있는 정보기술을 도입하거나 전자정부 사업을 계획하는 과정에 대해서는 프라이버시 보호 장치가 마련되어 있지 않다.

2) 도입 방향

프라이버시 영향 평가 제도의 국내법적 도입 문제는 기본적으로 '정보화 사업'을 추진하는 과정에서 당해 정보화사업이 개인정보 및 프라이버시에 미치는 영향을 평가하여 그 해결방안을 강구한다는 차원에서 접근하여야 한다. 따라서 프라이버시 영향 평가 제도의 입법 방법으로는 '정보화촉진기본법' 등 정보화 사업 관련 법률에서 제도 도입을 명문화하고 구체적인 내용에 대해서는 지침 등으로 고시하는 것이 바람직하다. 효과적이고 효율적인 프라이버시 영향 평가를 위해서는 프라이버시 영향 평가를 위한 공통 Framework을 개발하여 적용하는 것이 필요하며, 통일된 기준의 활용으로 프라이버시 영향 평가에 따른 각 정부기관의 부담도 줄일 수 있다.

프라이버시 영향 평가는 당해 사업을 추진하는 기관에서 자체적으로 실시하도록 하되, 프라이버시 영향 평가의 객관성을 담보하고 영향 평가를 위한 전문적 기술을 보다 용이하게 확보하기 위해서는 관련 지식이나 경험이 풍부한 전문기관으로부터 지원을 받고, 프라이버시 영향 평가 과정에 민간이 참여하는 방안을 강구할 필요가 있다. 프라이버시 영향 평가에 따른 결과는 반드시 관보, 기관 홈페이지 등에 공개함으로써 일반 국민의 국가기관에 의한 개인정보 및 프라이버시 침해 가능성에 대한 염려를 제거할 필요가 있다. 프라이버시 영향 평가의 법제화에 포함되어야 할 주요내용을 보면, 프라이버시 영향 평가가 필요한 경우, 구체적인 프라이버시 영향 평가의 내용, 프라이버시 영향 평가 기관 및 절차, 프라이버시 영향 평가 결과의 대국민 공개에 관한 사항 등이다.

제2절 개인정보보호 지침

1. OECD의 개인정보보호 정책

1) OECD의 프라이버시 개념과 개인정보

개인의 사생활보호로서의 프라이버시에 대해 OECD는 소극적 의미와 적극적 의미로 구분하여 접근하고 있다. 소극적 의미의 프라이버시는 혼자 있을 권리, 인간의 존엄과 관련된 기본적 인권이나 초상권의 문제등과 관련이 있다(Samuel Warren & Louise Brandels, 1990). 이에 비해 적극적 의미의 프라이버시는 자신에 관한 정보를 스스로 관리하고 통제할 수 있는 권한(Self control on Personal Information)까지를 포함하고 있다. 이러한 프라이버시 개념의 핵심에는 개인정보의 문제가 자리잡고 있다.

개인정보가 사생활보호 측면에서 기본적으로 다뤄져야 하는 것은 개인정보는 수집되고 집적되었을 때 확장적이고 부가가치적 특성을 나타낼 수 있기 때문이다. 예를 들어 기업이 고객의 정보를 집적한다는 것은 단순히 개별적 정보만을 수집한다는 의미뿐 아니라 개인의 사회경제적 지위와 개인의 기호, 선호하는 구매형태 등 개인의 라이프스타일과 관련된 일련의 정보흐름을 파악할 수 있다는 것으로 이는 정보를 제공하는 개인이 깊이 생각하지 못한 측면까지가 드러날 수 있다는 의미이다. 또한 정부조직이 개인의 사회복지 관련 정보를 축적하고 의료정보의 데이터베이스화를 구축한다는 것은 개인정보에 대한 접근이 다양해지면서 정보관리 주체가 보편화되거나 개별화될 가능성이 높아진다는 것이며, 이는 개인에 대한 모니터링이 언제 어디서나 가능하다는 의미이다.

이런 맥락에서 본다면 프라이버시보호를 위한 개인정보는 개인에 관한 비밀에 관한 사항은 아닐지라도 일정한 통제 하에서 정보주체의 자기결정권 활용 대상이 되는 정보(장영민, 1996)로 정의되는 것이 Any Information relating to an Identified or Identifiable natural person(EU 개인정보보호지침)이다.

2) 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>와 같이 정리될 수 있다.

<표 4-1> 개인정보보호8개 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 범위 내에서 정확하고 완전하여 최신의 내용으로 유지되어야 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 경유시에도 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.

3) 정보집적과 개인정보보호

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 공공서비스이다(the protection of privacy is in itself a public service). Privacy and data-sharing는 The way forward for public services(UK Cabinet Office, 2002)는 프라이버시 보호 vs. 정보공유(신뢰회복, 보유하고 있는 개인정보의 정확성과 신뢰도 향상, 안전한 방어책 마련, 개인정보 및 프라이버시 처리 방식의 현대화, 시민들에게 이익/신뢰를 더하는 법제도적 틀 마련)이다.

2. EU의 개인정보보호 지침

EU의 개인정보보호지침은 “any information relating to an identified or

identifiable natural person"이다. 주요내용을 살펴보면, EU 내에서의 개인정보의 자유로운 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

1) 자동처리되는 개인정보 보호를 위한 협약(Council of Europe Convention for the Protection of Individuals with regrad to Automatic Processing of Personal Data)

EU는 자유로운 정보교환의 부당한 제한을 제거하기 위해 1981년 2월 28일 서명하고 1993년에 개정했다. 그 적용대상을 보면 개인의 자유와 권리, 특히 자연인의 사적영역을 그 보호대상으로 하며, 공적영역을 위한 특별규정이 없는한 공적영역과 사적영역에 동일한 규정이 원칙적으로 적용한다. 주요기능으로는 국경 없는 정보의 흐름에 관한 특별규정의 제정과 제반조치의 이행에 관한 협의장치 확립과 개개서명국가들에 의하여 국내적으로 채택될 수 있는 개인정보보호에 관한 기본원칙 확정이다.

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).

2) 개인정보의 유통과정에서의 개인정보보호 방향(Directive on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of Such Data)

유럽연합에 의해 1995년 10월 28일 발효된 내용이다. 개인정보의 처리와 원활한 이동을 보장하기 위해 프라이버시가 존중되어야 함을 강조하고, 프라이버시보호가 미흡한 국가로의 개인데이터 이전을 금지함으로써 개인정보보호논의를 국제사회에서 중요한 문제로 부각시켰다. 또한 EU회원국과 교역하는 다른 국가들에 중요한 의미를 지니며, 민간부문의 정보보호에 있어 자율규제를 취하고 있는 미국 정보산업계의 반발을 불러일으켰다. 프라이버시 보호지침의 의무사항으로는 1998년 10월까지 자국의 「프라이버시법」을 제·개정 할 것, 개인정보의 수집·관리·이용활동 등을 조사·감독할 수 있는 독립적인 감독기구 설치, EU 수준의 개인정보보호 수준을 갖추지 않는 국가로는 개인자료의 이전금지이다.

EU 프라이버시 보호지침의 목적은 사업목적으로 다른 기업에 판매하는 것처럼 기업이 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

제3절 뉴욕주의 정보보호정책

1. 개요

정보보안책임관은 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	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]
		None (8)	Single Person (15)	Multiple (16)
		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.

2. 정보보호책임관(ISO)의 역할과 권한

1) 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.

2) 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[15].

---

15) 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 감사

3. 정보보호책임관 제도의 활용방안

정보보호책임관 제도를 공식화, 상시화 함으로써 정보보안 문제가 발생하였을 때 실질적인 긴급대응을 가능케할 수 있다. 정보보안 문제는 그 성격 상 즉각적인 대응조치가 필요한데 긴급대응조직을 편성되어 있었을지라도 이를 주도적으로 이끌어갈 수 있는 책임자가 없다면 대응활동의 효과성이 반감될 수 있다. 전통적인 조직이론에 따르면 이와 같은 긴급 대응팀은 상시조직이 아니라 임시조직, 즉 taskforce team의 성격을 갖고 만들이지는 경우가 많다. 그만큼 위험이나 보안문제를 부수적인 업무로 간주하고 있다는 의미이다. 한편, 상시적인 조직으로서의 정보보호책임관제도와 이에 따른 긴급 대응팀의 조직논리는 임시조직이 갖는 한계성(업무권한의 한계, 작동시간의 지연, 업무의 비연속성)을 극복하고자하는 제도라고 볼 수 있다.

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.

원(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 없어서는 안될 존재다”라고 본인의 역할을 강조하고 있다.

제5장 서울시 전자정부의 정보보호 추진 방안

제1절 서울시 전자정부의 개인정보보호 정책의 방향

제2절 서울시 전자정부의 개인정보보호의 제도적 체계

제5장 서울시 전자정부의 정보보호 추진방안

제1절 서울시 전자정부의 개인정보보호 정책의 방향

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 추진 체계

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 이음새 없이(seamless) 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.

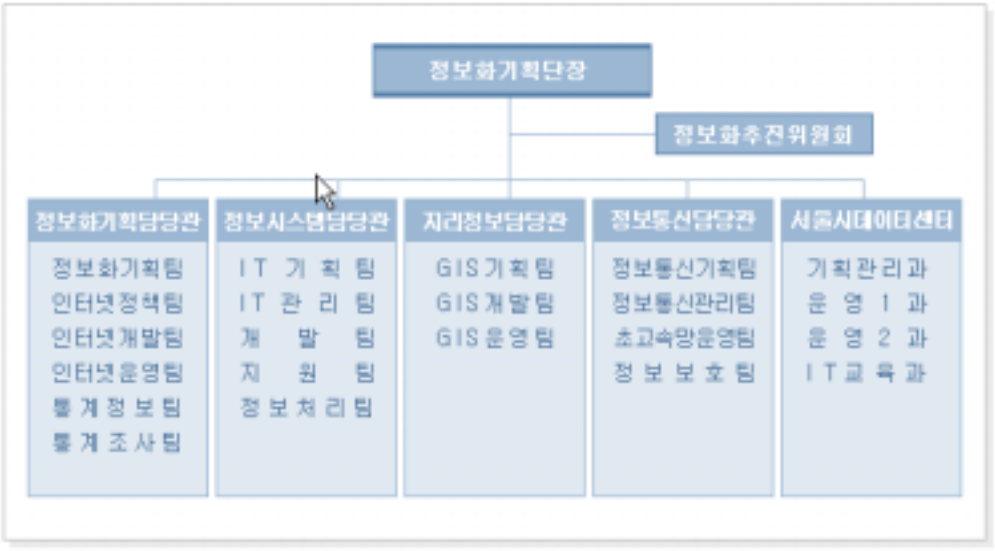
공공부문의 경우 개인의 자발적 동의에 의해 수집된 개인정보와 행정운영의 필요성에 의해 획득된 개인정보 등이 혼재되어 있는 상황에서 신뢰의 기제가 없다면 행정업무 전체에 대한 불신으로 이어질 수 있다. 따라서 시민영역과의 신뢰기제를 구축하기 위한 전략을 구성하여야 한다. 추진전략은 앞서 논의한 개인정보보호의 기본방향을 구체화하기 위한 것이다.

▪ 정보보호조직의 역할 강화에 따른 조직체계

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(<그림 5-1> 참조). 팀장과 5-7여명의 팀원으로 구성되어 있는데,

정보보호팀이 태스크 포스(Task force)가 아닌 상근 조직으로의 위상을 갖고 있다는 것은 긍정적이 측면으로 파악된다.



<그림 5-1> 서울시 정보화기획단 조직도

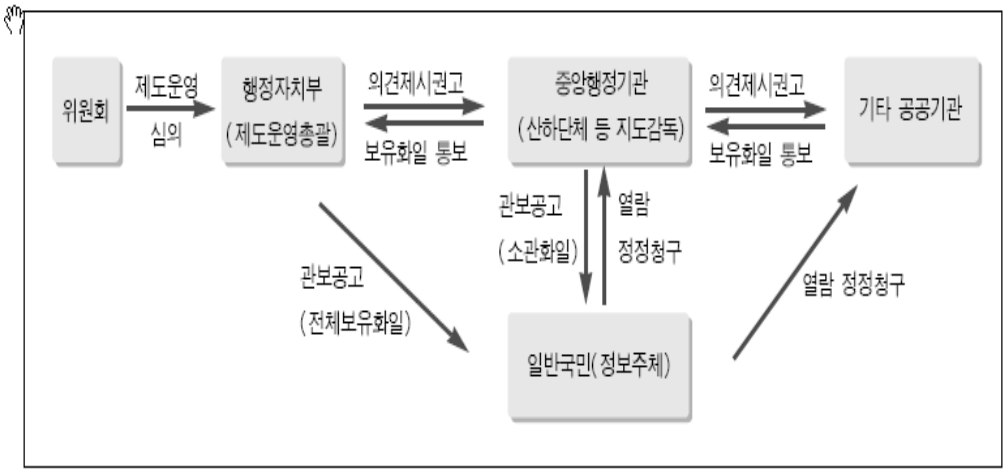
정보보호팀이 조직업무로 규정하고 있는 사항은 다음 <표 5-1>에 항목별로 제시되어 있다. 업무분장별로 살펴보면 개인정보보호에 관한 기본 계획의 수립부터, 기술적인 정보보안시스템, 전자서명에 따른 암호화 업무 등 기술적인 보안 영역, 정보보호시스템 운영 매뉴얼 작성 등 영역별로 세세한 업무들을 제시하고 있다. 그런데 전체적으로 보면 정보보안에 관한 업무에 비해 개인정보보호에 관한 업무관련 사항은 상대적으로 포괄적인 방안만 제시되어 있는 것을 알 수 있다. 더욱이 이러한 방향에 따라 실제 어떤 업무성과들이 아직은 나오지 않은 상태이다.

<표 5-1> 정보보호팀 업무분장

○ 개인정보보호 계획 수립 및 조회
○ 개인정보 실태조사 및 현황관리
○ 정보보호 의식 확산(교육 등) 및 피해예방
○ 정보보호 관리체계 인식 확산 및 홍보
○ 정보보호 추진계획, 중장기 계획 수립 및 조회
○ 정보통신 보안감사, 지도 감독 및 심사평가
○ 정보보호 법, 제도 제정 및 정비
○ DMC 정보도시 조성 지원 업무
○ 정보통신보안성 검토
○ 정보보호 시스템(네트워크 기반) 도입
○ Cert-Seoul 체계 구성, 운영
○ 통합정보보호시스템 기능 향상
○ 전자서명 암호화 업무
○ 정보보호 시스템(서버기반)도입
○ 정보자료 보호대책 수립,모의해킹,취약점점검
○ 정보보호 관리체계 구축, 운영
○ TSM 운영 및 기능 향상
○ 정보보호시스템(방화벽,침입차단시스템)운영
○ 컴퓨터바이러스, 해킹 대응 및 기술자원
○ 정보보호시스템 운영 메뉴얼 작성
○ 정보보호시스템(방화벽,침입차단시스템)운영
○ 컴퓨터바이러스, 해킹 대응 및 기술자원
○ 정보보호시스템 운영 메뉴얼 작성
○ 정보보호시스템(방화벽,침입차단시스템)운영
○ 컴퓨터바이러스, 해킹 대응 및 기술자원
○ 정보보호시스템 운영 메뉴얼 작성

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.

그렇다면 이러한 부분을 반영하여 서울시 개인정보보호 추진조직도를 구상해보자. 이를 위해 중앙정부의 개인정보보호 운영조직을 살펴볼 필요가 있다. <그림 5-2>에 따르면 중앙정부에서는 위원회에서 제도운영을 하고 있으며, 실제 행정자치부에서 개인정보보호와 관련된 의견을 제시하고, 각 행정기관이 보유하고 있는 파일을 확인하여 행정정보의 열람과 정정에 대한 절차를 수행하고 있다.



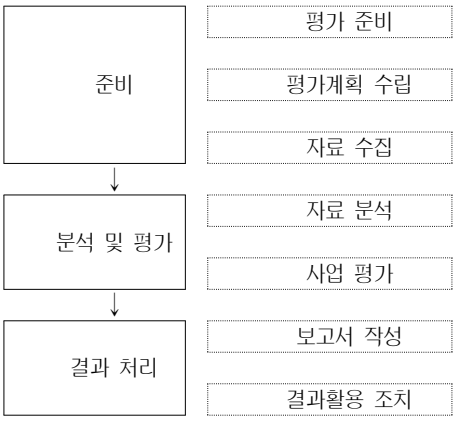
자료: 행정자치부(2000: 1)

<그림 5-2> 중앙정부의 개인정보보호 조직과 절차

그런데 지금까지 우리가 논의한 것처럼 개인정보보호의 문제는 기술적인 보안을 간으로 하되, 조직이나 제도의 운영과 절차, 관리의 문제 등이 주요한 역할을 하고 있다는 것을 확인하였다. 따라서 서울시 정보화기획단 산하에 정보보호와 관련된 조직체계를 제도, 정책부문과 기술부문으로 나눠 각각 담당팀을 구성할 필요가 있다. 즉, 정보화기획담당관 산하 정보화기획팀이 정보보호정책이나 제도에 관한 업무를 관장해야 하며, 정보통신담당관 산하에서는 정보보안기술과 관련한 업무를 담당하는 방식으로 구분되어야 한다. 왜냐하면 개인정보보호에 관한 제도적인 문제는 인터넷정책 등과도 긴밀하게 연관되어 있으며, 이는 기획담당관 산하에서 관장해야 할 필요가 있기 때문이다. 중앙부처인 정보통신부의 경우도 개인정보보호기능을 강화하기 위해 정보화기획실에 과장급을 팀장으로 하는 '개인정보보호전담팀'을 구성한 것을 보면 서울시 역시 개인정보보호전담팀을 기획담당관 산하에 설치해야 한다.

또한 현재 정보화추진위원회 산하에 개인정보보호위원회라는 하부 위원회를 구성하여 개인정보보호에 관한 심의 역할을 담당하게 해야 한다.

이러한 추진체계가 원활하게 운영되기 위해서는 개인정보보호 현황과 침해정도를 파악할 수 있는 개인정보보호 평가체계 구축 역시 추진할 필요가 있다. 이 과정의 절차는 다음과 같이 진행될 수 있다.



<그림 5-3> 개인정보보호 평가체계의 절차

또한 법적인 측면에서는 개인정보보호에 관한 통합적 내용을 포괄하는 조례의 제정이 필요하다. 현재의 분산적인 개인정보보호 관련 조례는 통합적으로 규정된 조례로 제정되어야 한다. 이 조례의 초안은 다음 절에서 제시하였다.

마지막으로 정보기술적 요소의 강화 측면으로 개인정보보호를 포함하여 차세대 정보보호 모델의 개발할 필요가 있다. 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.

제2절 서울시 전자정부의 개인정보보호의 제도적 체계 : 통합 개인정보보호 조례(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.

아르민 퐁스 엮음, 윤도형 옮김, 『당신은 어떤 세계에 살고 있는가? 2』, 한울

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

이민영・주지홍, 2003. "전자정부 시대의 개인정보보호: 법안분석 및 법제검토," 한국정보정책연구원 이슈 리포트, 과천: 정보통신정책연구원.

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・인증가이드, 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

2) 논문

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

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

김현수・박춘식, 2003. “일본 개인정보보호법제 정비동향에 관한 고찰”, 정보보호학회지, 13권 5호.

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

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)

부 록

1. 서울시 개인정보보호 인식조사 질문지
2. 서울시 개인정보처리 실태조사표

▪ 부록 1 : **질문지**

서울시민의 개인정보보호와 정보보안 의식조사

1. 귀하가 개인에 관한 정보라고 생각하는 것은 어떤 것들입니까? 다음의 보기 중 가장 중요하다고 생각하는 정보는 무엇입니까?

   ① 이름
   ② 주소
   ③ 주민등록번호
   ④ 메일 Address
   ⑤ 전화번호(자택/휴대폰)
   ⑥ 신용카드번호
   ⑦ 신분/직업에 관한 정보
   ⑧ 기타(　　)

2. 그럼 그 다음으로 중요하다고 생각하는 개인정보는 무엇입니까? 앞의 문항에서 선택하신 내용을 제외한 보기를 선택해 주세요.

   ① 이름
   ② 주소
   ③ 주민등록번호
   ④ 메일 Address
   ⑤ 전화번호(자택/휴대폰)
   ⑥ 신용카드번호
   ⑦ 신분/직업에 관한 정보
   ⑧ 기타(　　)

3. 귀하가 보시기에 서울시에서 웹사이트 등 온라인 상에서 수집된 개인정보를 잘 관리하고 있다고 생각하십니까? 아니면 별로 그렇지 않다고 생각하십니까?

① 아주 잘 관리한다
② 어느 정도 잘 관리하는 편이다
③ 별로 잘 관리하지 않는 편이다
④ 거의 잘 관리하지 않는다
⑤ 잘 모르겠다

4. 귀하는 서울시에서 웹사이트 등에서 수집된 시민의 개인정보를 어떻게 활용하는지 알고 계십니까?
① 아주 잘 안다
② 어느 정도 아는 편이다
③ 별로 모르는 편이다
④ 전혀 모른다

5. 중앙정부나 서울시에서는 시민의 동의를 얻어 온라인 상에서 많은 개인정보를 수집, 보유하며 활용하고 있습니다. 이러한 공공부문에서 개인정보를 취급하는데서 귀하가 가장 걱정스럽게 생각하는 부분은 무엇입니까?
① 개인정보보호 체계의 미비(법/제도)
② 담당공무원의 개인정보보호에 대한 의식수준
③ 웹사이트 정보시스템의 정보보안체계의 허술함
④ 기타( )

6. 귀하의 개인정보 중 서울시에서 공공적 목적으로 공개할 수 있는 개인정보는 무엇이라고 생각하십니까?
① 이름
② 주소
③ 주민등록번호
④ 메일 Address
⑤ 전화번호(자택/휴대폰)
⑥ 신용카드번호

⑦ 신분/직업에 관한 정보
⑧ 기타(　　)

7. 서울시가 시민의 개인정보를 어떻게 관리하는지 등 개인정보 취급에 관한 정보를 공개할 필요가 있다고 생각하십니까?
① 전혀 필요하지 않다
② 별로 필요하지 않다
③ 어느정도 필요하다
④ 매우 필요하다
⑤ 잘 모르겠다

8. 귀하가 보시기에 온라인 상에서 민간부문과 공공부문 중 어디가 더 개인정보를 잘 보호하고 있다고 생각하십니까?
① 민간부문
② 공공부문
③ 둘 다 비슷하다
④ 잘 모르겠다

9. 그렇다면 개인의 사생활보호를 위해 반드시 보호되어야 할 개인정보는 무엇입니까? 가장 중요하다고 생각되는 개인정보를 선택해 주세요.
① 이름
② 주소
③ 주민등록번호
④ 메일 Address
⑤ 전화번호(자택/휴대폰)
⑥ 신용카드번호
⑦ 신분/직업에 관한 정보
⑧ 기타(　　)

10. 귀하는 서울시 전자정부 홈페이지에 들어가본 경험이 있으십니까?

① 있다 ② 없다

11. 귀하는 앞으로 개인정보 누출 및 침해에 관한 형·사법 제도의 강화가 필요하다고 생각하십니까? 아니면 별로 그렇지 않다고 생각하십니까?

① 전혀 필요하지 않다
② 별로 필요하지 않다
③ 어느정도 필요하다
④ 매우 필요하다
⑤ 잘 모르겠다

12. 만일 귀하의 개인정보가 누출되어 귀하의 사생활이 침해받았다면 귀하는 어떤 행동을 하시겠습니까?

① 담당공무원 고발/소송
② 서울시 책임자 고발/소송
③ 시민단체나 소비자 보호원에 고발한다
④ 그냥 무시하겠다
⑤ 잘 모르겠다

※ 개인신상에 관한 질문입니다.

13. 귀하의 연령대는?

① 10대 이하 ② 20대 ③ 30대 ④ 40대 ⑤ 50대 이상

14. 귀하의 학력은?

① 중졸이하 ② 고졸 ③ 대졸 ④ 대학원졸 이상 ⑤ 기타( )

15. 귀하의 직업은?

① 교수·연구직 ② 관리사무직 ③ 영업판매직 ④ 자영업
⑤ 학생 ⑥ 무직 ⑦ 기타( )

16. 귀하가 거주하는 지역은? (　　구)

권역

도심 : 중구, 종로구, 용산구

동북 : 성동, 광진,동대문, 중랑, 성북, 강북, 도봉, 노원

서북 : 은평, 서대문, 마포구

서남 : 양천, 강서, 구로, 금천, 영등포, 동작, 관악

동남 : 서초, 강남, 송파, 강동

※ 응답해 주셔서 감사합니다.

▪ 부록 2 : **개인정보처리 실태조사표**

(기관명 :)

1 개인정보 보유현황

(2003. 11월 현재)

보유부서	보유화일명①	보유근거②	비 고 (주관부처③)

① 화일명 : 기존 화일은 목록집의 화일명과 일치, 신규화일은 특성을 알기 쉽게 명명(이하 같음)
② 보유근거가 되는 법률, 대통령령, 부령의 명칭을 기재
③ 주관부처 : 화일보유 근거가 되는 법령의 소관 중앙부처명

2 개인정보화일내역 관보공고 실적

(2002. 1~현재)

공고 기관①	화 일 명	공고일자	미공고사유	공고계획②

① 단위기관별로 보유중인 개인정보화일에 대해 소관 중앙행정기관에 요청한 실적
② 금년말까지 공고계획인 개인정보화일

3 개인정보화일의 보관

(2002. 1~현재)

보관장소① (관리부서)	보관형태②	보관화일	보안·방범 등 조치사항

① 전산실, 자료보관실 또는 일반사무실

② 개별 보관 또는 집중보관 여부(보관장소의 보안상태를 명확히 알 수 있도록 기재)

4 개인정보화일 제공 실적

(건수, 2002. 1~현재)

보유부서	화일명	제공 대상 기관①	제공 근거	제공내용 ②	용 도③	제 공 형태 ④	제 공 주 기	

① 제공대상기관은 기관의 정식명칭 기재

② 제공내용은 제공항목을 열거하거나 내용을 자세히 기재

③ 용도는 요청기관의 공문상 기재된 내용을 구체적으로 적시

④ 디스켓, 온라인, 자기 테이프 등

5 개인정보화일 제공거부 사례

(건수, 2002. 1~현재)

화일명	요청기관	요청내용	용도(근거)	거부사유

6 유출사고 등 법 위반사례 발생여부 및 조치결과 (법 제23조)

(건수, 2002. 1~현재)

사 건 적발일자①	사건내용	관 련 자			
		소속	직급	성명②	처벌내용

① 형사처리 및 자체 징계사례 기재

② 성명은 김 ○○로 비실명 기재

7 개인정보의 위탁처리 내역

(건수, 2002. 1~현재)

위탁기관명	위탁일자	화일명	수탁기관	위탁처리내용	안전조치내용

8 개인정보의 열람·정정 청구현황 및 처리실적

(2002. 1~현재)

보유부서	화일명	열람청구①		정정청구②	
		청구건수	처리건수	청구건수	처리건수

①, ② 개인정보보호법령에 따라 처리한 현황을 기재

9 관련 산하단체에 대한 지도·점검 실적

(2002. 1~현재)

산하단체명 ①	점검일자	지도·점검 내용	비 고

① 개인정보보호법 적용대상기관인 정부투자기관 및 재투자기관 등 (공무원연금법시행령 참조)

10 개인정보의 유출신고 접수사례 및 처리결과

(2002. 1~현재)

접수 부서	접수 일자	접수내용①	조치사항	비 고

① 기관별로 신고받아 자체적으로 접수·처리한 유출사건 기재

11 입·출력자료의 관리

(2002. 1~현재)

단계 / 부서	입력ID 및 비밀번호 부여①				출력색인 표시화일수	방화벽 설치	비 고
	1회	2회	3회	4회이상			

① 부팅시 암호, 로그온 암호, 파일접근·수정시 비밀번호 등 입력 및 출력을 위해 필요한 횟수

12 단말기의 설치·관리

(2002. 1~현재)

설치부서 (관리부서)	화일수	단말기수	비 고
계			

13 기타 건의사항

작성자 직위(급) : 성명 : 서명

※ 작성 양식 화일은 행정자치부 홈페이지(mogaha.go.kr) 전자정부 구현 -행정정보화 게시목록에서 다운받아 작성할 것

개인정보처리 실태조사 점검사항

조사 기관명 :

분 야	점검 사항	조사 결과
1. 개인정보 보호 정책 수립 및 지침 준수여부	○ 기관 자체의 개인정보보호계획의 수립여부? - 개인정보에 대한 보호·안전대책을 수립하고 있는가? (분실·도난·유출·변조 또는 훼손 대책 등) - 개인정보보호에 관한 자체규정 및 지침을 제정·시행하고 있는가? - 개인정보보호 업무담당자는 업무의 내용 및 의무를 숙지하고 있는가?	
	○ 개인정보보호 대상을 명확하게 인지하고 있는가? - 온라인 및 오프라인 개인정보	
	○ 개인정보보호정책 적용기관 등 범위는 적절한가? - 소속기관 일괄적용 또는 소속기관 자체수립	
	○ 개인정보보호책임관 지정 및 적정여부?	
	○ 개인정보 보호방침의 웹사이트 게재여부? - 개인정보화일의 보유현황·근거 및 보유목적 등 - 열람 및 정정 청구 안내 등	
	○ 개인정보침해신고처리대장의 비치 및 접수·처리결과 적정여부	
	○ 내부직원 및 산하기관, 산하투자기관 등에 대한 지도감독 및 교육실시 여부	
	○ 개인정보 사무의 업무분장 및 위임전결규정, 자체감사규정의 개정·반영 여부	

분 야	점검 사항	조사 결과
2. 화일의 수집 및 보관	○ 개인정보의 수집절차는 적법한가? - 관련 법령 또는 내부 규정 등	
	○ 개인정보의 보유범위는 적절한가?	
	○ 수집된 개인정보의 이용목적 완료 후 적절하게 폐기하고 있는가?	
	○ 백업자료의 관리는 적정한가?	
	○ 일반인의 개인정보화일대장의 열람은 가능한가? - 열람장소의 지정 및 고시	
3. 개인정보 제공 및 열람·정정	○ 개인정보 이용 및 타기관 제공의 적법성 여부? - 관련규정 검토 및 제공항목·범위·절차 등에 조치 여부	
	○ 공공이용의 근거 및 제공항목의 적정여부?	
	○ 개인정보제공대장의 기록 및 유지관리의 적정성?	
	○ 열람장소 지정 및 열람·정정안내도 비치여부? - 민원실 창구설치, 접수처리대장, 청구서 비치 등	
	○ 처리정보에 대한 열람청구 및 결정 등의 절차는 타당한가?	
4. 입출력자료	○ 개인정보 입·출력자료에 대한 관리대책은? - 입·출력자료에 대한 폐기방법	
	○ 입출력관리대장의 기록·관리실태는?	
	○ 출력자료에 대한 출력일시·면수표시 및 출력장비의 고유번호 등의 자동기록 여부?	
	○ 입·출력 및 수정사항, 데이타 접근내역 등을 자동으로 기록하는 로그화일 생성여부?	

분 야	점검 사항	조사결과
5. 시스템 및 단말기 관리	○ 취급자가 지정되어 있는가?	
	○ 사용자 ID 및 비밀번호는 사용하고 있으며, 비밀번호는 주기적으로 변경하는가?	
	○ 비밀번호관리대장의 작성 및 관리자는 적정한가?	
	○ 시스템의 정보보호를 위한 기술적 장치를 마련하고 있는가?	
	○ 개인정보화일의 명칭, 처리일시 및 사용자주체와 사용단말기가 컴퓨터에 자동으로 기록되고 있는가?	
6. 시설보안	○ 전산실, 자료보관실은 보호구역(통제구역)으로 적절하게 설정되었는가?	
	○ 보호구역 등 출입자에 대한 통제는 적절하게 이루어지고 있는가?	
7. 개인정보의 위탁처리	○ 개인정보처리를 위탁하고 있는가? - 필요한 제한이나 절차는 이행하고 있는가?	
	○ 개인정보 수탁자의 안전확보 대책은 ?	
8. 기타사항	○ 개인정보 DB를 이용한 업무처리시 문제점은 없는가?	

확인자 : 부서명 직위(급)
성명 서명

The Study on the Personal Information Protection of Seoul e-Government

Project Number	SDI 04-R-41
Research Staff	Mi-Ree Byun (in Charge)
	Jong-Yeop Kim

The Seoul e-Government is trying to reform the structure of administrative organization continuously. This efforts focus on the organizational restructuring and reengineering to promote the public service. As a result, Seoul e-government has performed the projects, such as the Integration of Information System, ITA(Information Technology Architecture), Single Interface of Portal Internet Sites, etc.

These Seoul Metropolitan e-Government performances are the realization of the vision of the 'citizen-centric information city of world standing, e-Seoul'.

Despite these efforts to create the citizen-centric e-Seoul, there are certain critical points, such as the debates between the development of the user-friendly administrative services and the personal information protection. The positive aspects of the e-Government are the efficiencies and conveniences for citizens. But in the shadow of information Society, there are negative scenes. In other words, monitoring and controling the person are inevitable. The user-friendly and convenient database is not only the condition for the good administrative services, but also the necessary situation for the control and violate the person's privacy.

The network's efficiency and panopticon are the two contradictory features of the information society. Recently many researchers focus on the agenda for the

personal information protection in the discussing of the ubiquitous government. In the era of embedded-network, that is to say the ubiquitous network, personal information protection will be the top issue.

Therefore, to prepare the proper trajectory of e-Government, we should study the personal information protection theoretically and empirically.

This research includes four parts as follows. First, we review the theoretical approach of personal information protection. As we said, information society and privacy have the contradictory aspects. We deal the multi-dimension of the personal information protection and analyse the several social issues concerning the privacy, such as NEIS(Nation Education Information System), Gangnam-Gu CCTV and the Internet Real Name.

Secondly, we research the present state of personal information protection of Seoul e-government. In this part, we research the management situation of the database flows and storage. And we survey the citizen and the public servants concerning the attitude of personal information protection.

Thirdly, we review the policy of personal information protection of foreign e-government, such as the privacy impact assessment and guidelines.

Finally, we summarize our study and recommend the policy and the institutional system for the personal information protection of Seoul e-government.

Table of Contents