서울시 전자정부의 개인정보 관리실태와 강화방안

■ 전자정부에서의 개인정보보호의 필요성
■ 전자정부에 대한 서울시민의 개인정보보호 관련 인식
■ 서울시 전자정부의 개인정보보유 및 관리 현황
■ 전자정부에서의 개인정보보호 위상과 다차원성
■ 외국 전자정부의 개인정보보호 제도
■ 서울시 전자정부의 개인정보보호 강화방안

전자정부에서의 개인정보보호의 필요성

○ 네트워크의 효율성과 판옵티콘(panopticon)의 경계에 선 전자정부

- 정보기술의 확산과 시스템 통합에 따른 정보의 집적과 접근허용성의 증대는 프라이버시 침해의 가능성을 높이며, 따라서 정보보안과 개인정보보호 문제가 전자정부 추진에서의 주요 쟁점으로 등장함.
- '나는 언제, 어디서든 관찰되고 있다'. 나에 관한 모든 정보는 정부의 데이터베이스에 축적되어 있으며, 정부에서는 원한다면 언제든지 나에 관해 시시콜콜한 정보, 개인의 사생활에 관한 정보 등을 열람할 수 있음. 더욱이 정보보안의 허점으로 정부 데이터베이스에 해커가 침입하여 나에 관한 정보를 빼내간다면 어떻게 될 것인가? 위험은 전자정부가 발전할수록 새로운 가능성으로 노출됨.
- 개인정보보호와 정보보안의 문제는 전자정부 추진과정에서 나타날 수 있는 제도적(법·제도), 인식적(사회적 인식·윤리·문화), 기술적 문제의 복합체임.

○ 전자정부 진화에 따른 위험요소 관리 차원의 정책적 가이드라인 필요성 대두

- 최근 교육행정정보시스템 구축과 관련한 일련의 논쟁은 정보시스템의 효율성 측면과 개인정보보호와 정보보안에 관한 사회제도적 합의절차의 부재로 인한 대립된 의견의 충돌임.
- 전자정부는 정체된 개념이 아닌 지속적으로 변화 발전하는 동태적 개념으로, 이를 고려하여 불확실성을 제거하고 신뢰형성 구조로서 개인정보보호와 정보보안에 관한 정책방향이 수립되어야 함.

전자정부에 대한 서울시민의 개인정보보호 관련 인식

○ 서울시 전자정부 발전단계에 비해 전반적으로 낮은 시민 인식

- 서울시민에게 공공적으로 수집된 개인정보들이 어떻게 활용되고 있는지에 대해 알고 있는지 여부를 알아본 결과, 85.2%가 내용을 잘 모른다고 응답하여 전반적인 인지정도가 낮음.

○ 한국적 특수성 - 신용카드번호보다 주민등록번호가 더 중요함.

- 서울시민들이 가장 중요하게 생각하는 개인정보는 '주민등록번호'와 '신용카드번호'로 나타남. 개인정보 중 가장 중요한 것과 그 다음으로 중요한 것 두 개를 고르게 한 결과(중복응답), 응답자의 45.6%는 주민등록번호가, 29.4%는 신용카드번호가 개인정보에서 중요하다고 생각함.
- 서울시민 10명 중 4-5명(46%)은 공공적 목적으로 자신들의 이름을 공개할 수 있다고 생각하고 있으며, 21%는 이메일주소는 공공목적으로 공개가능하다고 함. 주민등록번호를 공공목적으로 공개가능하다는 시민은 9%에 지나지 않았으며, 다만, 50대 이상 연령층의 14%는 주민등록번호를 공공적 목적으로 공개가능하다고 생각하고 있는 것으로 나타나 다른 연령층에 비해 허용정도가 높음.

○ 공공부문에 대한 신뢰정보는 민간부문과 비슷함.

- 시민들은 민간부문과 공공부문에서의 개인정보보호 정도를 비슷한 수준으로 생각하는 가운데, 40대 이상의 연령층에서 공공부문에서 더 잘한다는 비율이 20, 30대 연령층보다 높음.

○ 개인정보침해는 기술적인 문제이면서 동시에 운영관리상의 문제임을 인식함.

- 서울시민의 44%는 정보시스템의 보안상의 문제 때문에 개인정보가 침해당할 우려가 있다고 생각하고 있으며, 31%는 개인정보 담당공무원의 의식수준이 낮기 때문이라고 생각함. 25%의 시민은 법제도적 체계의 미비로 개인정보침해 가능성이 높다고 생각함.

서울시 전자정부의 개인정보보유 및 관리 현황

○ 서울시 전자정부 업무 아키텍처에 따른 개인정보보유 현황

- 정보시스템 특성에 따라 민감성 정보가 다수 포함되어 있음(생활정보 관련 시스템, 행정정보 관련 시스템 등).
- 민감성 정보에 관한 관리체계가 구체화되어야 함.

<표 1> 서울시 전자정부의 업무 아키텍처에 따른 개인정보 보유 현황

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

○ 서울시 자치구의 개인정보보호 관리 현황

- 서울시 4개 자치구 개인정보보호 관리 현황 조사를 통해서 볼 때, 개인정보보호 관리의 절차 및 점검사항에 관한 일반적인 관리는 이뤄지고 있음. 향후 보다 강화된 체계적이고 구체적인 관리원칙의 수립이 보완·시행되어야 할 것임.

분 야	점검 사항	조 사 결 과			
		은평구	강서구	중구	강남구
개인정보 보호 정책 수립 및 지침 준수여부	기관 자체의 개인정보보호계획의 수립 여부	수립	수립	수립	수립
	개인정보보호 대상에 대한 명확한 인지 여부: 온라인 및 오프라인 개인정보	인지	인지	인지	인지
	개인정보보호정책 적용기관 등 범위의 적절성: 소속기관 일괄 적용 또는 소속기관 자체 수립	적절	적절	적절	적절
	개인정보보호책임관 지정 여부	지정	지정	지정	지정
	개인정보 보호방침의 웹사이트 게재 여부: 개인정보 파일의 보유현황·근거 및 보유목적, 열람 및 정정 청구 안내 등	게재	게재	게재	게재
	개인정보침해신고처리대장의 비치 및 접수·처리결과 적정 여부	적정	적정	적정	적정
	내부직원 및 산하기관, 산하투자기관 등에 대한 지도·감독 및 교육실시 여부	실시	실시	-	실시
	개인정보 사무의 업무분장 및 위임전결규정, 자체감사규정의 개정·반영 여부	반영	반영	반영	반영
파일의 수집 및 보관	개인정보 수집절차의 적법성 여부: 법령 또는 내부 규정 등	적법	적법	적법	적법
	개인정보 보유범위의 적절성	적절	적절	적절	적절
	수집된 개인정보의 이용목적 완료 후 폐기 여부	폐기	폐기	폐기	폐기
	백업자료의 관리	백업	백업	백업	백업
	일반인의 개인정보파일대장 열람 가능 여부	지정	지정	지정	지정
개인정보 제공 및 열람·청구	개인정보 이용 및 타 기관 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 비치 여부	비치	비치	비치	비치
	처리정보에 대한 열람청구·결정 등의 절차 타당성	타당	타당	타당	타당
입·출력 자료	개인정보 입·출력 자료에 대한 관리대책 폐기방법	소각	파쇄	파쇄	파쇄
	입출력관리대장의 기록·관리 실태	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 로그파일 생성 여부	-	-	-	생성
시스템 및 단말기 관리	취급자 지정 여부	지정	지정	지정	지정
	사용자 ID 및 비밀번호는 사용하고 있으며, 비밀번호는 주기적으로 변경하는지 여부	주기적	필요시	필요시	주기적
	비밀번호관리대장의 작성 및 관리자의 적정성	적정	적정	적정	적정
	시스템의 정보보호를 위한 기술적 장치를 마련	마련	마련	마련	방화벽
	개인정보파일의 명칭, 처리일시 및 사용자주체와 사용단말기가 컴퓨터에 자동으로 기록하는지 여부	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	-	-	-

○ 서울시 자치구 정보보호담당자들이 인식하는 개인정보보호 방안

- 개인정보보호를 위해서는 독립적인 개인정보보호 기구가 설치 운영되어야 함. 현재 전문 인력을 확보하기가 어려움.
- 관련 조례 제정, 정보보호책임관 지정, 운영의 독립성과 활성화가 필요함.
- 개인정보보호를 위해서는 패스워드, 이메일 등 기본항목에 대한 철저한 관리원칙을 수립해야 하며, 정보보호 담당부서와 담당자의 권한을 명확하게 규정해야 함. 더불어 관련 업무의 원활한 수행을 위해 담당자의 주기적 교육이 필요함.

전자정부에서의 개인정보보호 위상과 다차원성

○ 전자정부에서의 개인정보보호의 문제는 전자정부의 편익을 위해 지불되어야 하는 일종의 거래비용(transaction cost)으로 인식해야 함. 즉, 개인에 관한 정보노출에 따른 위험을 관리하는 비용임.

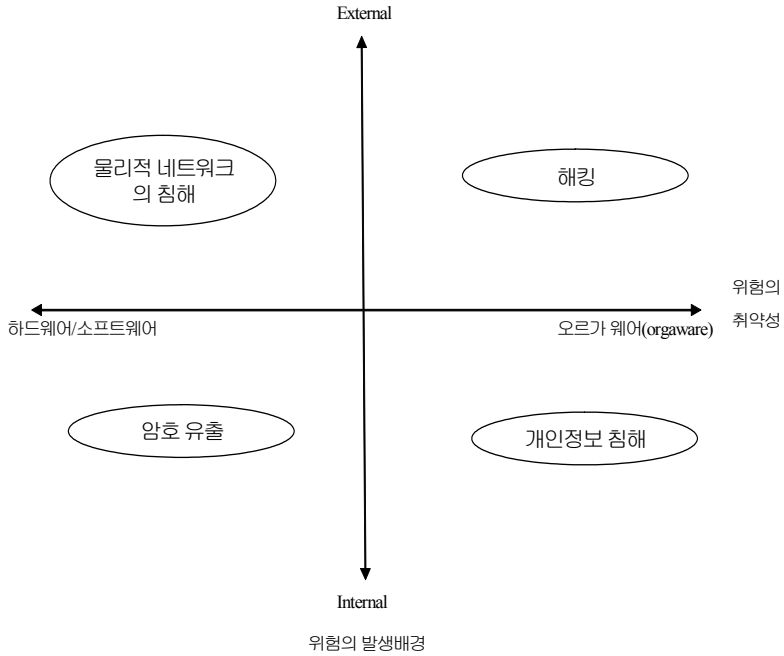
- 전자정부의 공공적 특성은 개인에게 정부의 권리로서 강제할 수 있는 부분이 존재함[1]. 이러한 조건으로 인해 개인정보 노출에 대한 위험이 상시적으로 있을 수밖에 없으며, 이러한 위험을 관리하기 위한 비용은 필수적으로 지불되어야 함.
- 따라서 전자정부 진화에 따른 개인정보보호 문제는 일시적으로 일어나는 사건이나 사고(accident)라기보다는 언제나 존재하는 위험관리를 위한 비용이라는 관점이 중요함. 이는 정보사회에서 필연적으로 지불해야 할 사회적 비용임.

○ 개인정보의 침해는 조직관리차원의 내부에서 일어날 가능성이 높음.

- 정보보호 관련 항목을 '위험의 발생배경'과 '위험의 취약성'이라는 두 차원에서 파악하면, 개인정보의 침해는 오르가웨어* 차원의 조직 내부에서 발생할 가능성이 상대적으로 높아 관리의 어려움이 예상됨.

  (*오르가웨어 orgaware 란 하드웨어와 소프트웨어의 상대적인 의미로 사용되는 개념으로 인간, 제도, 의사결정과정, 교육 등 조직의 정보시스템을 운영하고 관리하는 데 필요한 인적·조직적 요소를 지칭하는 의미로 사용됨(Andersen, 1991).)

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

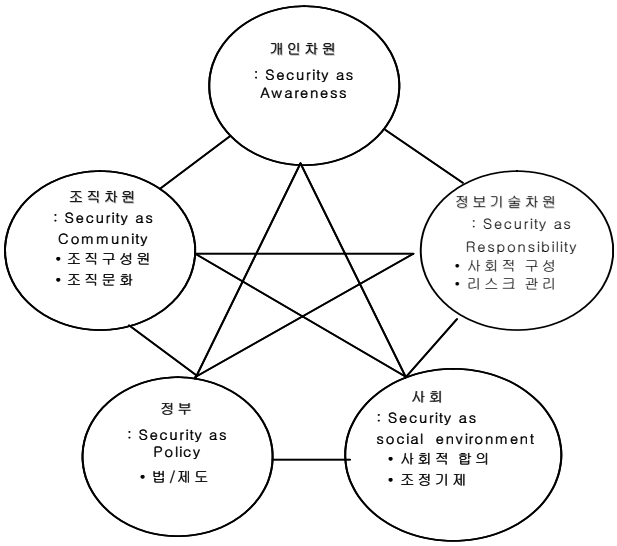


<그림 1> 정보보호 관련 항목별 위상

- 따라서 개인정보침해를 방지하기 위한 방안은 기술적인 측면을 포함하기는 하지만 전자정부의 운영과 관련한 제도적, 정책적 차원의 고려가 중요함.

○ 개인정보보호는 개인, 조직, 정보기술, 정부, 사회적 관점의 다차원적 접근이 필요함.

- 개인정보보호는 개인차원에서는 인식의 문제로, 조직차원에서는 조직구성원의 인식과 조직문화 형성이 중요함.
- 정보기술차원에서는 정보침해에 대한 리스크 관리로서 기술의 사회적 구성이 중요한 역할을 하며, 정부차원에서는 법·제도 등 정책적 문제 형성이, 사회적 차원에서는 공공부문에서의 개인정보보호에 대한 사회적 합의와 문제 발생 시 이를 해소하기 위한 조정 기제 형성이 중요한 역할을 함.

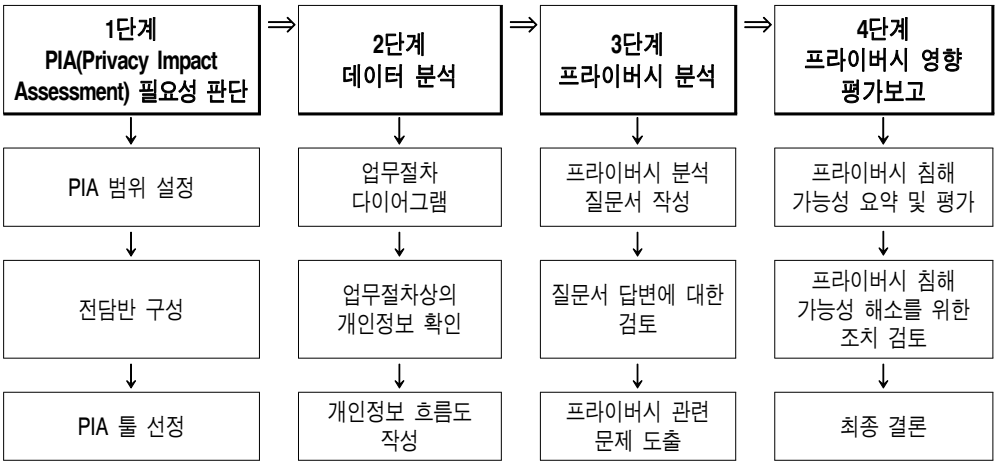


<그림 1> 개인정보보호를 위한 영역의 다차원성

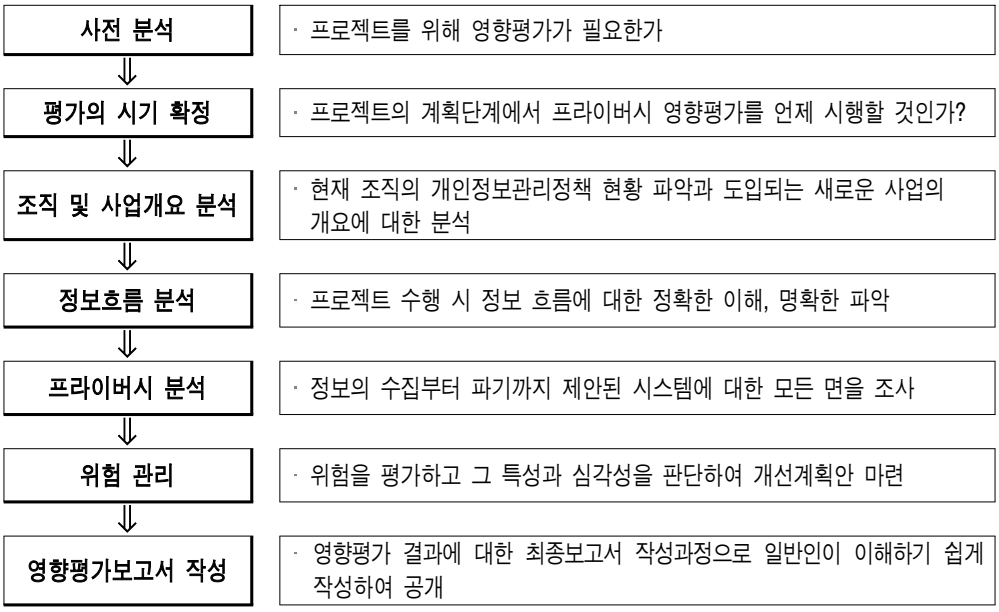
외국 전자정부의 개인정보보호 제도

○ 프라이버시 영향평가제도

- 프라이버시 영향평가제도란 전자정부 사업계획 시점부터 당해 사업이 개인정보 및 프라이버시에 미치는 영향을 검토하는 제도
- 미국 전자정부와 캐나다 전자정부에서 2002년부터 시행하고 있음.



<그림 2> 캐나다 전자정부의 프라이버시 영향평가 절차도



<그림 3> 미국 전자정부의 프라이버시 영향평가제도의 절차

○ 정보보호책임관 제도

- 정보보호책임관은 미국 주(州)정부 또는 지방정부의 정보통신 관련 정책과 정보보안 관련 업무를 책임지는 담당관임.
- 뉴욕주는 미국에서 처음으로 정보보안책임관(ISO: Information Security Officer) 제도를 만들어 종합적인 정보보안정책을 수립했음. 뉴욕주 정보기술국(OFT)은 1997년 1월 "정보기술 정책지침 97-1"(Technology Policy 97-1)에서 정보보안의 중요성과 역할에 대해 언급하며, 1999년 2월 "정보기술 정책지침 99-2"(Technology Policy 99-2)에서 정보보안책임관의 기능, 역할, 교육, 자격 등을 구체적으로 규정하여 정보보안과 관련된 제도를 공식화하였음.
- 뉴욕주의 시도 이후 미국 내 다른 주정부들이 전자정부 운영에서 ISO를 임명하고 있음. 각 주정부의 정보보호책임관 제도는 주 특성에 따라 상이하게 운영됨. 정보보호책임관의 권한 집중과 관련하여 중앙집권적 유형, 분권적 유형, 세부분권적 유형 등으로 구분됨.
- 중앙집권적 유형이란 중앙에서 전체적인 정보보안 책임을 정보보호책임관이 지는 형태로 운영되며, 분권적 유형은 각 정보시스템에 대해 부처별로 정보보안을 책임지는 형태이며, 세부분권적 유형이란 분권적 유형보다 좀더 하부 단위에서 정보시스템에 대한 보안을 책임지는 형태임.
- 정보보호책임관 제도의 의의는 위험관리시스템의 제도화, 조직 내외부의 조정자 역할의 제도적 기제, 전자정부의 효율성과 개인정보보호 사이의 견제와 균형의 기제 확립을 의미함.

서울시 전자정부의 개인정보보호 강화방안

○ '정보차단 혹은 통제'의 패러다임에서 '정보공개 및 관리'의 방향으로

- 서울시 전자정부에서의 개인정보보호의 기본 방향은 개인정보의 수집과 유통에 대한 허용 범주 여부를 결정하고, 행정서비스를 활성화하면서 동시에 시민들에 대한 신뢰기제를 정착시켜야 하는 것으로 가야 함.
- 이 과정에서 정보보호의 핵심은 기술뿐 아니라 사람에 의한 관리의 문제가 중요하다는 점을 공유해야 함.

○ 정보보호조직의 역할 강화

- 서울시는 정보통신담당관 산하 정보보호팀이 2003년 조직편제에 등장함. 팀장과 5명의 팀원으로 구성되어 있음. 이는 정보보호팀이 임시조직이 아닌 상근조직의 위상을 가졌다는 긍정적 측면을 갖고 있음.
- 이러한 상근조직으로서의 서울시 정보보호팀은 뉴욕주 정보보호관제도가 시사하는 바처럼 전자정부의 효율성을 보장하면서도 동시에 정보보안, 개인정보 오남용 등 정보화의 역기능을 최소화하기 위한 조정과 견제의 역할을 수행해야만 함.

○ 정보보호를 위한 통합적이고 포괄적 조례의 제정 필요

- 「서울특별시개인정보보호및정보보안에관한조례(안)」(가칭) 제정이 필요함.

○ 시민의 개인정보보호 인식제고를 위한 교육홍보활동 강화

- 대(對)시민 개인정보인식 확산을 위한 웹사이트 배너 마련
- 개인정보침해 자가진단 도구(tool) 제공
- 서울시 전자정부의 개인정보보호 활동관련 정보 제공

(예: "시민의 정보, 이렇게 이용됩니다", "교통시민카드, 시민정보 보호의 시작과 끝")

변미리 | 서울시정개발연구원 부연구위원
02-2149-1303
miree21@sdi.re.kr