情 報 保 護 學 會 誌
第 13 券 第 3 號, 2003. 6

전자정부와 프라이버시

이 경 호*, 김 소 정*, 임 종 인*

요 약

정보화가 성숙됨에 따라 정보보호의 중요성도 비례하여 커지고 있다. 지난 국민의 정부에서 시작된 전자정부사업은 우리나라의 앞선 정보인프라를 활용하기 위하여 야심차게 추진되었지만 과정의 비 조직성, 보안 특히 프라이버시 문제에 대한 몰이해로 인해 여러 가지 문제를 야기하고 있다. 본 논문에서는 전자정부사업 추진 시 반드시 고려해야 할 프라이버시 영향 평가(PIA) 문제를 소개하고자 한다.

Ⅰ. 서 론

전자정부사업은 지난 국민의 정부에서 국민에 대한 최고수준의 행정서비스를 제공하고, 기업 활동에 최적의 환경을 조성하며, 행정의 생산성·투명성·민주성을 극대화 하고자 하는 목표를 가지고 2000년 12월 김대중 대통령의 지시에 따라 2001년 2월에 전자정부 특별위원회를 출범시키고 11대 과제를 선정하여 2002년 11월 사업완료 보고를 마치고 2003 1월까지 마무리되었다[1].

이후 출범한 참여정부에서는 기 구축된 인프라를 활용한 행정혁신, 복지향상이라는 목표를 위해, 정부혁신위원회 내에 특위보다는 약화된 전자정부 전문위원회를 만들고 이를 계속 추진하고 있다.

전자정부 사업의 궁극적 모습은 국민이 안방이나 사무실에서 한번의 클릭으로 원하는 민원증명을 발급 받고, 기업창업신청을 가능하게 하는 혁명적인 민원행정서비스를 실현하는 것이다. 이와 동시에 서비스 실현 과정에서는 정부 내부의 대대적인 업무혁신도 병행된다. 불필요한 규제와 업무프로세스의 개혁 및 폐지, 문서감축과 표준화된 문서유통을 통한 부처간·기관간 정보공동이용, 단일창구 구축 등의 과정을 거치게 된다.

전자정부사업은 이제 막 첫걸음을 내딛기 시작했음에도 불구하고 전자정부사업이 갖는 사회·경제적 효과는 금전적인 가치로는 일일이 환산하기 어려울 만큼 큰 것으로 평가되고 있다. 특히 전자정부사업을 추진함으로써 우리나라의 행정은 효율성·투명성·민주성 등 다양한 측면에서 선진국가수준으로 향상되는 효과를 기대할 수 있다.

그러나 입법과정이 관계부처간의 충분한 협의를 통한 합의를 이끌어내지 못한 채 진행됨으로써 2002년 11월 open한 전자정부 site의 활용도는 초기의 기대와는 다르게 날이 갈수록 떨어지고 있다[2].

그 중에서도 전자정부 특별위원회가 의욕적으로 추진한 국가정보화 11대 과제 중 하나인 교육행정정보시스템(NEIS: National Education Information System)의 효용성과 안전성에 관해서는 각 이익단체는 물론 행정부, 심지어는 일선 학교의 정보화 담당 교사들마저 각기 다른 주장을 하고 있다. NEIS 대란으로 일컬어지는 작금의 사태는 그 동안 추진되어온 국가 정보화 사업에 내재된 문제점들을 전 국민들에게 노출시킨 계기가 되었다. 이것은 사업추진이 무엇보다 행정효율성과 국민편의에 치우쳐 국민의 기본 인권이나 정보보호문제라는 중요 이슈가 뒷전으로 밀려난 결과이다. 구미에서 국가정보화의 최우선순위를 프라이버시 보호를 비롯한 인권과 복지에 둔 것과는 상당히 대조적이다.

갈등의 본질은 프라이버시 중 개인정보(personal data)의 보호에 있다. 그러나 이익단체 및 정치권의 아전인수 식 해석과 전문적이지 못한 문제해결 접근은 갈등만을 증폭시킬 뿐 근본적 해결책 제시는

* 고려대학교 정보보호대학원, 정보보호기술연구센터

고사하고, 몇몇 집단의 세력다툼으로 변질되어가고 있다.

본 연구에서는 정부가 국가 정보화를 수행함에 있어서 최우선적으로 전제해야 할 프라이버시 보호에 대한 시스템 적인 틀인 PIA(Privacy Impact Assessmen 법론을 미국 연방정부 사례를 기반으로 검토 및 분석하여 내재된 철학과 논리가 기존의 접근방법과 어떤 차이가 있는지를 고찰한다.

이를 위하여 프라이버시의 대상인 개인정보에 대하여 정의하고 그 가치와 침해를 받았을 경우 발생하는 영향의 정도를 측정하여 프라이버시 보호 시스템의 최종적인 구성과 운영체계를 실증하고자 한다.

Ⅱ. 정보와 영향도

1. 정보의 정의

정보보호 관리에 대한 국제 표준인 ISO/IEC 17799 에서는 정보를 다음과 같이 정의한다.

Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected[3].

즉 정보를 가치를 가진 자산의 하나로서 분류하고 있다. 일반적으로 자산은 유형자산과 무형자산으로 분류할 수 있으며 유형자산은 빌딩, 토지와 같은 부동산과 설비와 같이 물리적인 형태를 가지고 존재하는 것을 말하며, 무형자산은 지적재산권, 영업권 등과 같이 행할 수 있는 권리의 형태로 존재한다.

기업에서는 이러한 자산을 평가하여 기업 가치를 측정하기 위하여 순자산 가치 측정 방법, 시장가치 측정방법, 이익가치 측정방법 등 다양한 방법으로 기업이 보유한 자산을 평가한다. 그러나 정보의 가치는 위에서 언급한 일반적인 기업의 자산가치 측정 방법으로 수용되지 않는다.

은행의 예를 들면, 은행이 보유한 빌딩의 자산은 재무제표 안의 자산 영역에 공시가 기준으로 평가되어 기술되나 은행 고객의 모든 금융정보가 들어 있는 고객원장 (Database)의 내용은 그 가치를 재무표 등 전통적인 기업가치 측정 틀 안에서 찾아 볼 수 없다.

그렇다면 프라이버시와 관련하여 개인정보를 보호한다는 것을 그 정보의 가치를 유지하고자 하는 것이라고 정의할 때 그 정보의 가치는 어떻게 측정될 수 있는가? 이러한 정보의 가치를 측정하기 위하여 다양한 접근이 이루어지고 있다. 그 정보가 손상되었을 경우 복구를 하기 위한 기회비용을 측정하는 방법, 그 정보를 둘러싼 환경을 복구하기 위한 대체비용을 측정하는 방법, 정보의 손상으로 인한 평판과 이미지 훼손을 브랜드 가치와 같은 형태로 측정하여 환산하는 방법 등이 연구되어 지고 있다.

그러나 본고에서는 정보가 가지는 고유의 특성, 즉, 기밀성, 무결성, 가용성이 결여되었을 경우 발생하는 영향도를 정보의 가치로 부여한다. 이 방법은 위에서 든 방법들이 가지는 측면들을 종합적으로 고려한 방법으로써 현재로써는 침해가 발생하였을 경우 그 손상 정도를 판단하는데 가장 적절한 기준이 될 수 있기 때문이다.

2. 정보의 특성

정보의 안전성을 보장한다는 것은 정보자산의 기밀성, 무결성, 가용성을 보장하는 것이다. 정보가 가지는 많은 특성 중에서 이들 3가지 특성은 정보의 가치를 측정하는데 유효한 기준점이 된다[4].

기밀성(Confidentiality)은 해당 정보를 볼 수 있록 허가받은 자만이 정보를 볼 수 있음을 보장하는 것이다. 무결성(Integrity)은 해당 정보가 원래 의한 정보와 틀림없을 것을 보장하는 것이다. 가용성(Availability)은 해당 정보를 원하는 시간에 항상 용할 수 있음을 보장하는 것이다.

프라이버시와 관련된 정보의 특성은 대부분 기밀성에 의존하고 있는 것으로 보여진다. 무결성은 정보의 변조와 왜곡이므로 프라이버시 측면보다는 오히려 사기와 같은 사이버 범죄 측면에서 접근하는 것이 바람직하다. 정보의 가용성은 사이버 테러로 인한 정보 서비스의 중단과 같은 경우를 의미하므로 본 논문에서는 기밀성을 중심으로 다루는 것이 합리적일 것이다.

다시 말하면, 프라이버시 측면에서 개인정보의 가치는 해당 정보의 기밀성의 보장에 있으며, 이러한 특성이 결여되거나 손상을 입었을 때 발생하는 영향 정도가 곧 가치가 된다고 정의 할 수 있다.

이와 같은 접근 방법은 이미 OECD 암호정책 가이드라인의 가장 중요한 원칙으로 제시된바 있다[5]. 기밀성이 보장되지 않아 개인정보 유출이 이루어지고 이로 인해 예상되는 피해와 그로 인한 영향이 개

인정보자산의 가치라고 볼 수 있는 것이다. 이제 기밀성 결여로 인한 정보의 영향도 측면을 다루어 보자.

3. 정보의 영향도

정보의 영향 중 기밀성의 결여로 인한 영향 측정을 언급하기 전에 영향 측정 시 전제되어야 할 사항은 다음과 같다.

첫째, 정보의 가치는 시간의 흐름에 따라 변화한다. 우리는 특종 보도라는 뉴스정보를 예를 들 수 있다. 특종보도는 보도 전 시점까지는 기밀성이 매우 높게 보장되어야 하나 보도 시점 이후에는 기밀성을 완전히 상실한다. 이와 같이 개개의 정보는 시간이 흐르고 활용도가 변화함에 따라 가치도 재평가되어야 한다는 전제가 성립한다.

둘째, 정보의 가치는 개개인마다 상이하다[6]. 자신에 관한 정보를 스스로 관리 통제할 수 있는 권리(Self-control on personal information)는 현대 프라이버시 개념의 적극적인 면을 잘 보여준다. 이러한 권리의 인정은 개개인의 정보는 각기 다르게 취급되어야 한다는 전제에서 그 다름을 판단하는 독점적인 기준을 개인에게 부여하는 것이다. 이는 다른 사람에 비하여 높게 가치를 매기는 사람이나 또는 낮게 책정하는 사람 모두를 보호한다. 이러한 전제는 어느 당사자에게도 손해가 되지 않는 선에서 타협이 이루어 질 것이라는 확신을 준다.

셋째, 개인정보의 프라이버시는 소유권이다. 이를 인정하면 정보를 획득하기 전에 협상을 요구하게 한다[7]. 정보를 가진 사람에게 정보에 대한 통제권과 권한이 있으므로 정보의 가치가 어느 정도 인지를 먼저 결정한 후 그 가치 정도에 따라 정보를 이전할 수 있다.

이러한 전제를 바탕으로 프라이버시 영향도를 평가 할 수 있다. 영향도는 시간의 흐름에 따라 변화하므로 주기적으로 이루어지거나, 프로젝트의 시작, 중간, 종료 시점 등 정해진 시간에 이루어 져야 한다.

또한 정보의 가치 평가의 주체마다 서로 상이한 가치를 부여하기 때문에 정보의 소유권(Ownership)을 진 사람에게 평가받아야 한다. 예를 들면 NEIS의 보건영역의 건강기록부 정보에 대한 가치는 오직 학생 당사자와 이를 대신하는 보호자만이 그 가치를 평가할 수 있다. 물론 각 사람에 따라 그 가치는 다르게 부여될 수 있다.

위 정보의 영향도를 건강기록부 정보가 볼 수 있는 권한을 가진 사람 외의 사람에게 노출되었을 때 발생하는 영향이 본인의 정상적인 삶의 영위에 치명적일 때(3), 상당히 큰 영향을 주지만 극복할 수 있을 때(2), 큰 영향이 없어 무시할 만 할 때(1) 등으로 구분하여 평가할 수 있다. 이러한 평가의 주체는 해당 정보의 소유권을 가진 사람에 의하여 이루어져야하며 적정한 절차를 통하여 위탁할 수 있다. 평가 방식과 평가 기준 또한 평가주체, 즉 정보 소유권을 가진 사람들의 협의를 통하여 조정될 수 있다. 이러한 평가는 주기적으로 이루어져서 적용 결과가 피드백 되어 오류가 수정되는 시스템으로 정착되어야 한다.

〔표 1〕 정보자산 영향평가표

평가항목	영향도			평가근거
	(1) 큰 영향이 없어 무시할 만 할 때	(2) 상당히 큰 영향을 주지만 극복할 수 있을때	(3) 정상적인 삶의 영위에 치명적일 때	
위의 정보자산이 외부에 유출 및 공개되었을 경우		V		정보 유출에 의한 프라이버시 문제로 부정적인 평판이 발생할 수 있거나 생활 영위에 치명적임

Ⅲ. 프라이버시 영향 평가

본 절에서는 앞 절에서 연구한 정보와 영향도 개념을 적용하여 프라이버시 영향평가(PIA: Privacy Impact Assessment) 방법론을 기술하고자 한다. PIA는 미국의 전자정부법(e-Government Act of 2002)에서도 IT 시스템 도입 시 반드시 고려해야 할 사항으로 명시할 만큼 그 중요성이 커지고 있으나 아직 그 방법론이 크게 발전되어 있지는 않다. 본 연구에서는 미국 연방정부 국세청(IRA)에서 실시한 PIA Best Practice를 바탕으로 프라이버시 영향평가의 방법론을 기술한다.

1. 프라이버시 영향평가란?

프라이버시 영향평가(PIA: Privacy Impact Assessment)란 정보시스템에서 프라이버시를 평가하는데 사용되는 프로세스를 말한다. PIA 프로세스는 시스템 소유자와 개발자가 개발의 초기 단계부터 프라이버시를 평가하도록 설계되어 있으며 다음과 같은 절차를 통하여 수행된다.

- 1단계 : 프라이버시 교육
- 2단계 : 프라이버시 이슈 및 데이터 수집
- 3단계 : 프라이버시 위험 식별 및 문제 해결
- 4단계 : 승인

PIA의 실시시기는 정보시스템 개발 초기 단계인 요구사항 분석 시부터 시스템 설계 등의 기획기간에 최초로 실시되며 시스템 개발주기(Life Cycle)의 전 과정에서 실시된다. 즉, 개발이 진행 중이거나 완료된 후 다시 한번 실시된다.

PIA의 수행주체는 시스템 소유자(Owner) 및 개발자(Developer)로서 시스템 소유자는 정보의 소유자와 일치한다. 또한 개발자는 해당 정보자산에 미치는 위협요소와 취약성의 발생가능성 및 정도를 평가한다.

PIA의 수행대상이 될 수 있는 시스템은 아래와 같다.

- 신규 정보시스템, 개발중인 시스템 또는 중대한 변경 중에 있는 시스템
- Legacy 시스템의 자동화 및 업그레이드로 인한 데이터 위험 발생 시 PIA 수행
- 현재 운영중인 시스템은 PIA 프로세스를 수행할 필요 없음. 그러나 시스템의 데이터 프라이버시가 우려된다면 PIA 프로세스 수행을 요구함.

2. Best Practice : 미 국세청 PIA[8]

美 국세청(IRS: Information Revenue Service)은 1862년 설립된 美 재무성 산하 세무 담당 기관이며 1995년, 美 국세청 산하 PA(The Office of the Privacy Advocate)에서 국세청 및 납세자 프라이버시 보호를 위하여 PIA 모델을 개발했다. 2000년, CIO Council은 국세청에서 개발한 PIA 모델을 프라이버시 보호와 관련하여 가장 훌륭한 Best Practice로 채택하여 범정부적 사용을 권고다. FBI는 이미 PIA 프로세스를 구축하였으며 기타 연방정부 기관, 교육기관 등도 국세청 PIA 모델을 확보 및 구축 中에 있다.

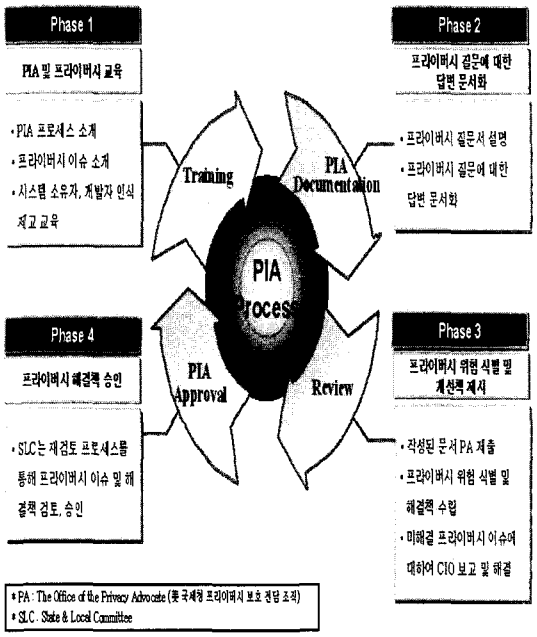
미 국세청의 PIA의 특징은 개인정보가 저장된 정보 시스템에 대한 프라이버시 평가에 적합하게 설계되었으며, 시스템 소유자와 개발자 및 운영자의 프라이버시 문제에 대한 인식 제고가 가능하였다는 점이다. 그리고 독립된 조직(PA)으로부터 프라이버시 평가를 실시하여 객관적인 평가가 가능하였고 PIA의 구현 및 이행 관점에서 간단(simple)하며, 간결(succinct)하고, 견고(robust)하다. 또한 프라이버시 이슈나 정보 시스템에 대한 비전문가들도 쉽게 이해하도록 작성되어 있으며 정보시스템의 전체적인 효율성을 저하시키지 않고, 각 기관 고유의 프라이버시 요구사항을 반영하여 적용이 가능한 형태이다.

세부적인 절차는 아래와 같다.

- Step 1 : PIA 교육 훈련 요청 및 수행
- Step 2 : 프라이버시 관련 질문에 대한 답변서 작성, PIA 관련문서화
- Step 3 : Step 2의 PIA 문서를 PA(Privacy Advocate)에 제출
- Step 4 : 프라이버시 위험 식별을 위한 PIA 문서 검토, 시스템 소유자 및 개발자로부터의 위험 원인 파악
- Step 5 : 시스템 소유자, 개발자 및 PA가 프라이버시 위험에 대한 해결책 및 개선책에 동의, 주요 이슈에 대한 해결책의 동의가 이루어지지 않을 경우 CIO에게 보고
- Step 6 : 시스템 소유자 및 개발자는 합의된 해결책을 설계 요구 사항에 포함시키고 식별된 위험을 해결한다.
- Step 7 : SLC에 참여하여 적법한 승인절차와 적절한 해결책에 대한 재검토

이러한 과정에서 도출된 주요 이슈는 5개 측면에서 언급되고 있다. 즉, 정보와 프라이버시 영향, 시스템 내의 데이터, 데이터에 대한 접근 이슈, 데이터 구성요소에 대한 이슈, 시스템 관리에 대한 통제와 유지보수에 대하여 아래와 같이 이슈를 제기 하고 있으며 이를 점검할 것을 가이드하고 있다.

- 정보와 프라이버시 영향 부문
  - 정보의 사용은 통제되어야 하며, 필요하고 적법한 목적으로만 사용되어야 함.



〔표 2〕 미 국세청 PIA 프로세스 구성도

- 개인들로부터 수집된 정보는 사용의 주된 목적이 개인들에게 통보되어야 함.
- 정보시스템에 저장되어 있는 개인정보는 정확하고, 적절하고, 최신의 상태로 유지되어야 함.

• 시스템 내의 데이터

국세청 시스템이 아닌 외부로부터의 수집된 정보의 경우 프라이버시 보호를 위해 다음의 특성이 증명되어야 함. 정보의 최신성, 완전성, 정확성

• 데이타에 대한 접근 이슈

시스템 상의 정보에 접근하는 사용자는 정의되고 문서화되어야 함.

- 개인 : 시스템 사용자, 관리자, 소유자, 개발자 등
- 타 시스템 : 국세청 시스템과 인터페이스 하거나, 데이터에 접근하는 프로그램 또는 프로젝트
- 다른 기관 : 국세청 시스템 데이터에 접근하는 국제, 연방, 주(지방) 기관 등

• 데이터 구성요소에 대한 이슈

시스템에 사용될 데이터의 요구사항 결정 및 설계時 다음의 프라이버시 속성 포함하도록 해야 함.

- 데이터는 시스템의 목적을 달성하는데 적절하고 필수적인 것이어야 함.
- 데이터는 완전하고, 정확하며 시기 적절해야함.

• 시스템 관리에 대한 통제, 유지보수 측면

- 시스템 자동화로 프로세스, 데이터, 통제의 통합이 발생할 경우, 적절한 수준의 관리 적 통제가 유지되는지 평가함.
- 데이터 보유 절차는 문서화되어야 함.
  - 법률에서 요구하는 절차를 준수하기 위한 검토를 요구함.
  - 정보를 보유하는 기간, 해당 보유기간 만료시 정보를 적절히 삭제하는 것을 보장하는 명확한 규정을 수립해야 함.
- 프라이버시 보호를 위하여 시스템의 모니터링 능력은 사전에 정의되어야 하며, 법적인 합리성을 가질 수 있도록 정의된 기준에 따라 최소한으로 제한되어야 함.

3. PIA 방법론

프라이버시 영향평가 방법론에 대해 ISO/IEC 17799에서 가이드 하는 정보자산에 대한 위험분석 방법론을 바탕으로 미 국세청 사례의 장점을 접목하여 개념과 논리를 고찰하고자 한다. 특히 정보자산 평가 기법은 정보자산 가치에 대한 BIA(Business Impact Assessment) 기법을 사용하여 정량화 하는 방법을 사용하였다. 개괄적인 절차는 아래와 같다.

- Step 1 : 정보자산의 가치측정
- Step 2 : 해당 정보의 위협요소 도출
- Step 3 : 대상 정보시스템 분석을 통한 취약성 도출
- Step 4 : 위험도 산출
- Step 5 : 보장수준 (Degree of Assurance) 평가

각 단계는 ISO/IEC 17799 에서 가이드 하는 위험분석 절차를 준수하지만 정보자산 가치 측정의 경우 평가기준과 항목을 사전에 명확히 하고 자산 소유자의 합의를 도출하는 것이 무엇보다도 중요하다. 각 단계 별 고려사항은 다음과 같다.

3.1. 정보자산의 가치측정

정보자산의 가치는 해당 정보의 기밀성이 결여되었을 경우 발생하는 Impact(영향도)로 정의한다. 즉 정보가 유출되어 접근권한이 없는 사람이 정보를 열람했을 경우 발생하는 영향의 잠재 정도이다. 이에 대한 평가는 해당 정보의 소유자만이 가능하며, 평가를 위하여 사전에 등급(Scale)과 각 등급의 판

단기준이 명시되어야 하며, 평가 결과는 유효성(Effectiveness)을 확보하기 위하여 현실과의 일치성을 검토하여야 한다.

3.2. 해당 정보의 위협요소 도출

대상 정보가 존재하는 물리적, 논리적 공간의 특성을 파악하고 출연할 수 있는 위협요소를 출연 빈도와 함께 DB화하여 각 정보자산과 맵핑시킨다. 위협요소는 이미 발생한 경우 히스토리 정보를 바탕으로 통계적 분석을 통하여 빈도를 측정하고 아직 발생하지 않은 위협은 기존 발생한 위협과 비교하여 빈도를 추정한다. 이러한 위협 DB는 사고 및 침해 발생 시 주기적으로 갱신하여 항상 현실과 부합하도록 유지한다.

3.3. 대상 정보시스템 분석을 통한 취약성 도출

대상 시스템의 취약성은 반드시 내재되어 있다. 취약성은 단순히 기술적인 요인에서부터 사회공학적인 요인에 이르기까지 다양하다. 특히 전자적 공간에서만 가질 수 있는 취약성은 정보 유통 및 이전 속도의 증가에 따른 위협과 관계가 있다. 실제로는 기술적 요인보다는 80% 이상이 접근권한의 불확실성, 권한관리자의 이해 부족, 오동작, 실수, 관리 절차의 미비, 규정, 절차 미 준수 등 사람에 의한 것이 대부분을 차지한다.

취약성은 위협요소와 연계되어 하나의 시나리오를 이룬다. 이러한 시나리오가 현실에서 발생 가능한 것인지를 검토한다.

3.4. 위험도 산출

정보의 영향도와 위협의 빈도, 취약성의 정도를 평가하여 위험도를 산출한다. 위험도는 위험이 높은 것부터 순서대로 나열되어 정리된다. 위험도가 가장 높은 것부터 각각 평가하여 조치를 취할 대상인지를 판단한다. 더 이상 조치를 취할 대상 위험이 아닌 감내할 만한 위험(Acceptable Risk)이라고 판단되면 그 정도를 DOA(Degree of Assurance)로 정의한다.

3.5 보장수준(Degree of Assurance)평가

보장 수준은 평가 때마다 환경 및 법적, 제도적 강제 수준에 따라 변화할 수 있다. 보장 수준을 합의하는 것은 자산의 소유자간에 합의가 도출되어야 한다.

4. PIA 수행의 의의

PIA는 활용하고자 하는 범위 내의 모든 정보에 대한 프라이버시와 관련된 주요 위협과 취약성을 나열하고 정량적으로 분석하며 이를 토대로 한 지표를 활용함에 따라 대상 영역의 모든 프라이버시 영향을 한번에 파악할 수 있다는 장점이 있다. 또한 이러한 절차를 시스템화하여 활용할 경우 정보의 각종 프로젝트 수행 시 필수 수행 항목으로 적용할 수 있다.

이를 확대하면 정부의 각 시스템 별 프라이버시 영향지수(Privacy Index) 체계를 수립하여 부 별, 조직별 정보 활용 평가 항목으로 활용 가능하다. 이러한 지표관리는 추이 분석을 통하여 프라이버시를 심각히 침해하는 정도, 즉 프라이버시 보장 수준(Degree of Assurance)을 넘어설 경우 사전 예보하는 등 다양한 용도로 사용될 수 있다.

Ⅳ. 결 론

1. 정보화와 데이터 분산

정보화가 이루어지면서 과거에는 무시되었던 새로운 위협이 사이버 공간에서는 매우 치명적인 형태로 나타나기도 한다. 과거의 학생생활기록부는 학부모가 학교에 가서 열람을 요청하면 볼 수 있는 정도로 해당정보의 유통 속도가 매우 낮고 변조나 악용의 소지도 낮았다. 하지만 이러한 정보가 DB화되어 하나의 서버에 통합될 경우 삶의 편의성과 업무의 효율성을 가져올 것으로 보였던 정보화가 정보를 사용하는 자에 의하여 의도했든지 의도하지 않았든지 차별화 된 서비스를 유발케 하여 평등을 저해하는 형태로 변화될 수 있다. 이는 자신도 모르는 동안에 마일리지 서비스나 CRM(Customer Relation Manage DB에 의하여 우리 현실에서 나타나고 있다.

이러한 우려 때문에 선진국에서는 개인정보가 수록된 DB의 중앙집권화는 민주주의 발전에 역행하는 제도이며, 데이터 분산화 (Fragmentation)를 시도하고 있다[9].

2. PIA의 시스템화

정부가 추진하는 전자정부는 시간적인 압박과 예산상의 제약, 그리고 부처간의 어려운 조정과정 등의 악조건 속에서도 많은 성과를 거두었다. 특히 프라이버시와 관련하여 개인정보의 등급화, 개인정보

파일 취급절차 요건강화, 행정자치부 주무 부서에 인력증원, 국무총리실 소속 개인정보심의위원회 운영의 활성화 등을 추진했고 장기적으로 독립행정기관으로서 프라이버시 보호 감독기구인 가칭 개인정보보호원의 설치를 권고했다.

하지만 현재 이런 권고가 체계적으로 진척되고 있지 않아 보이며, 현재 프라이버시 보호정책과 정부정책이 충돌할 때 이를 중재 및 조정할 기구가 존재하지 않는다. 하물며 국가 PIA와 같은 시스템은 머나먼 일로 보인다. 또한 NEIS의 경우 논쟁의 초점이 이익단체간의 힘 겨루기 양상으로 발전하여 논리적이며 냉정한 결론을 도출하기에는 이미 사건의 본질이 너무 변질되어 버렸다. 더 늦기 전에 프라이버시 중재를 위한 부처를 초월하는 대통령 직속의 중재 기구가 운영되어야 하며 이를 통한 프라이버시 영향평가 시스템이 즉시 가동되어야 한다.

즉, PIA는 정부의 정보화 사업의 시작과 끝에 항상 수행되어야 하는 필수적인 절차로서 정착되어야 한다.

3. 프라이버시는 21세기의 최고의 화두

21세기는 사이버 공간이라는 제 2의 삶의 터전을 인류에게 영위토록 하고 있다. 기존 현실에서의 틀은 새로운 사이버 공간에서의 현실에 부합하지 않을 가능성을 전제할 때, 기존 문화, 관습, 법, 구조들이 새로운 공간으로 이전되는 절차와 틀을 시스템화하여 준비하지 않는 다면 혼란은 계속될 수밖에 없다. 특히 프라이버시 문제는 침해의 정도가 크기 때문에 올 초 New York Times는 21세기 최대의 화두로 프라이버시 문제를 꼽은 바 있다.

참 고 문 헌

〔1〕 전자정부특별위원회, 전자정부백서, 17~19.

〔2〕 중앙일보, 2003. 5. 전자정부 시리즈.

〔3〕 ISO/IEC 2000, INTERNATIONAL STANDARD ISO/IEC 17799 Information technology Code of practice for information security management, viii.

〔4〕 ISO/IEC 2000, INTERNATIONAL STANDARD ISO/IEC 17799 Information technology Code of practice for information security management, viii.

〔5〕 OECD는 97년 8월에 암호정책의 배경과 쟁점에 관한 보고서를 발표하였고, 그 주요 8원칙은 암호의 신뢰, 암호의 선택, 암호 발전의 시장주도, 암호의 표준, 사생활 및 개인정보보호, 적법한 접근권 보장, 책임명시, 국제 협력 등이다. OECD Guidelines for Cryptography Policy, http://www.oecd.org 참고.

〔6〕 로렌스 레식 著, 김정오 역, 코드: *사이버 공간의 법이론*, 나남출판, 2002, p. 328.

〔7〕 supra note, p. 364.

〔8〕 FEDERAL CHIEF INFORMATION OFFICER'S COUNCIL, Best Practices : Privacy : IRS IT Privacy Impact Assessment Model, February 25, 2000, http://www.cio.gov.

〔9〕 영국의 경우, 2002년 4월에 발표한 "*Privacy and data-sharing: The way forward for public service*"를 통해 개인의 정보를 해당기관에서 특정의 목적으로만 사용할 수 있도록 유도하기 위해, 정보의 분산화를 잘 이행하는 부처에게 인센티브를 지급하는 등, 정보의 집적화와 프라이버시 침해 소지를 줄이기 위해 노력하고 있다.
UK Cabinet Office, "*Privacy and data-sharing: The way forward for public service*," A performance and innovation unit report, April 200.

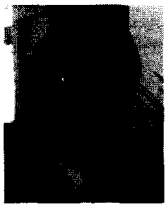
〈著 者 紹 介〉

이 경 호 (Kyoung-Ho Lee)

1989년 8월 : 서강대 수학과 졸업 (이학사)
1997년 8월 : 서강대 정보통신대학원 졸업 (전산학석사)
2003년~현재 : 고려대학교 정보보호대학원 정책박사과정 재학 중
1999~현재, 삼성, LG, SK, POSCO, 정부기관 등 정보보호 컨설팅 프로젝트 수행(PM)
2001 : 전자정부 특별위원회 內 프라이버시 및 보안 점검반
2002~현재 : 컨설팅하우스㈜ 대표이사
2003~현재 : 한국인정원(KAB) 인정심사, BS7799 자문 위원
관심분야 : 정보보호정책, 컨설팅.

김 소 정 (So-Jeong Kim)

1998년 8월 : 부산대학교 사학과 졸업(문학사)
2001년 2월 : 경희대학교 평화복지대학원 졸업(정치학 석사)
2001년 3월~2002년 9월 : 한국전파진흥협회 연구원
2002년~현재 : 고려대학교 정보보호대학원 정책박사과정 재학 중
관심분야 : 정보보호정책, e-privacy



임 종 인 (Jong-In Lim)
종신회원

1980년 2월 : 고려대학교 수학과 졸업(이학사)
1982년 2월 : 고려대학교 수학과 졸업(이학석사)
1986년 2월 : 고려대학교 수학과졸업(이학박사)
1986년 3월~현재 : 고려대학교 수학과 정교수, 고려대학교 정보보호대학원장, 고려대학교 정보보호기술연구센터장
관심분야 : 블록암호 및 스트림 암호 분석 및 설계, 암호 프로토콜, 공개키 암호 알고리즘 분석, 스테가노그래피, 컴퓨터 포렌식스 기술, 정보보호 정책