제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

공공부문을 위한 프라이버시 영향평가 모델 개발

송 세 현* 유승재** 김귀남*
* 경기대학교 정보보호기술공학과
** 중부대학교 정보보호학과

요 약

전자정부가 출범하면서 국민의 편익과 업무의 효율을 가져오는 혁신적인 계기가 되었다. 그러나 전자정부 서비스 실현을 위한 11개의 국책사업 중 교육행정정보시스템(NEIS)의 문제로 인해 개인정보보호에 대해 사회적인 관심을 가지게 되었다. 이에 대한 해결방안으로 미국과 캐나다에서 실시하는 프라이버시 영향 평가(Privacy Impact Assessment)를 도입하여 위험분석 방법과 통합한 새로운 PIA모델을 제시한다. 또한 외국의 PIA 적용사례(Canada PIA report)를 통해 PIA를 실시해야 하는 이유에 대해 기술하고자 한다.

1. 서 론

우리 정부는 2002년 4월 전자정부(www.egov.go.kr) 서비스를 시작하였다. 전자정부 서비스는 민원 행정을 안방에서 클릭 한번으로 민원 서비스를 받을 수 있는 민원행정 서비스를 실현하는 것이 궁극적이 목표라고 할 수 있다. 또한 이런 민원행정뿐만이 아니라 전자거래 등 다양한 서비스를 온라인화하여 국민들의 편의도모와 행정업무의 효율성을 높이는데 그 목적이 있다. 이처럼 전자정부의 본격적인 구현으로 국가기관이나 기업체에서도 개인정보의 수집과 활용이 크게 늘어나게 되었다. 개인의 이름이나 전화번호에서부터 정치적인 성향이나 취미활동 같은 다양한 개인정보를 수집 및 이용을 하고 있는 것이다. 개인정보는 단순히 정보(information)를 수집하는 것이 문제라는 것보다 정보가 오용이나 노출이 되었을 경우 개인에게 발생할 수 있는 문제점을 고려해 보아야 한다. 특히 전자정부의 실현을 위해 국민들의 정보를 정보시스템에 집적화한다는 것은 대단히 위험하고 신중히 진행해야할 부분인 것이다. 따라서 개인정보의 수집 및 관리 등에서 오는 피해에 대해 개인의 정보 및 프라이버시 보호를 위한 법제와 프로세스가 필요하게 되었다. 특히, 전자정부가 추진하는 11대 국책사업의 하나인 교육행정정보시스템(NEIS)-개별적인 업무시스템인 CS시스템을 대체하여 시도교육청에 통합시스템을 구축하려는 시스템-의 시행으로 정부기관에 의한 개인정보 및 프라이버시침해 문제가 사회적인 이슈화가 되었다. 정보시스템을 구축하면서 정보의 집적화로 인한 개인들의 정보수집과 노출의 위험성이 프라이버시에 문제가 될 수 있는 소지가 있기 때문이다. 이런 문제로 인한 교총과 전교조간 대립을 통해 여러 가지 갈등사항으로 커다란 진통을 겪었고, 현재도 계속적으로 문제점에 대한 논의가 진행중이다. 교육행정정보시스템(NEIS)[1]의 예로 전자정부를 시행하면서 개인정보보호 문제가 다른 국책사업 추진에 대해서도 많은 어려움을 동반하게 될 것을 예견하였다. 따라서 정부의 국책사업을 추진함에 있어 국민들의 신뢰감을 높이고, 프라이버시에 대한 논란으로 인한 국책사업의 지장을 초래하거나 예산의 낭비를 줄이기 위한 방안을 필요로 하게되었다. 시민 단체들은 정부가 사업을 수행함에 있어 개인정보침해에 대한 위험성을 인지하고 이런 위험성의 여부를 사전에 미리 평가를 하자는 의견-법제의 개편이나 보호정책에 대한 방안-을 제시하고 있다. 외국에서는 이미 오래전부터 개인정보에 대한 위험성을 인지하여 공공부문과 민간부문에서 정보시스템사업 구축이나 시스템 변경 등을 할 경우 프라이버시 영향평가(Privacy Impact Assessment : PIA)를 실시[2]하도록 하고 있다. OECD[3][4][5][6]나 EU[7]에서도 개인정보보호 지침을 제시한 바 있고 각국에서도 이런 지침을 근간[8]으로 자국의 법제와 환경에 맞게 PIA를 실시하고 있다. PIA는 개인정보보호를 위한 시스템적인 틀을 의미한다. 이 연구에서는 PIA를 통해 정부의 국가 정보화를 수행함에 있어서 최우선적으로 고려해야 할 사항인 개인정보보호에 대한 국민들의 신뢰성 향상을 위해 방법론을 캐나다 연방정부 사례기반[9][10]으로 검토 및 분석하여 PIA (Privacy Impact Assessment) 모델을 제시하고자 한다.

2. 프라이버시 영향평가(Privacy Impact Assessment)

2.1 프라이버시란 무엇인가?

프라이버시란 무엇인가?[11] 1890년 Samuel Warren과 Louise Brandeis가 "Right to be let alone"이라고 정의를 내린 이래로 인간의 존엄

성과 관련된 천부적 인권이라는 소극적인 개념에서 "Self control on Personal Information"이라는 적극적인 개념으로 진화되었다. 그만큼 정보의 중요성이 커진다는 의미이기도 하고 특히나 개인정보의 대한 관심도가 커졌다는 의미이기도 하다. 정부나 기업에서 개인의 정보를 획득하는 것은 단순한 정보획득 이상의 가치를 지니게 된다. 개인의 사회적, 경제적 지위와 기호, 선호하는 구매형태 등 노출되기를 의도하지 않았던 모든 정보를 알 수 있게 된다는 것에 그 의의가 있다. 예를 들어 NEIS의 문제처럼 학생들의 아주 민감한 식별정보(이름, 주민등록번호 등)에서부터 의료나 보건 같은 개인정보들을 정보시스템에 집적화하고 이용을 했을 때 개인 정보의 유출이나 오용의 문제를 간과할 수 없게 되는 것이다.

개인정보도 하나의 정보자산으로 인식할 수 있으므로 정보의 특성, 즉 기밀성(Confidentiality), 가용성(Availability), 무결성(Integrity)으로 가치를 측정할 수 있다. 프라이버시와 관련된 정보의 특성은 대부분 기밀성에 의존하는 것으로 여겨진다. 기밀성은 개인정보가 소유자 외에 다른 사용자에게 노출된다면 개인에게 심각하게 피해를 초래할 수 있기 때문이다. 프라이버시 측면으로 봤을 때 다른 정보자산들(하드웨어, 소프트웨어, 브랜드 이미지 등)에 비해 개인정보는 기밀성 보장에 그 의의를 들 수 있으며, 이런 특성을 중심으로 프라이버시 영향평가를 실시해야 할 것이다.

2.2 프라이버시 영향평가 개요

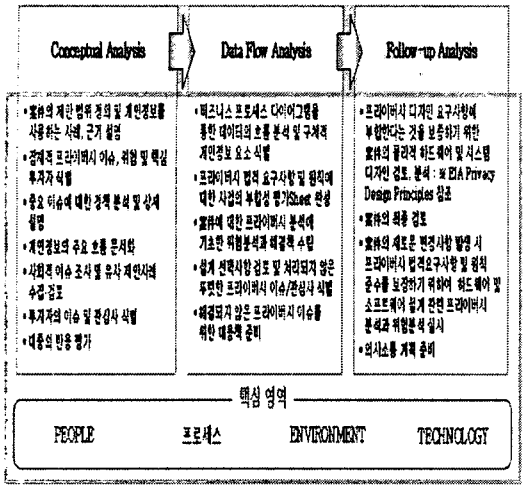
프라이버시 영향평가 즉 PIA는 미국의 전자정부법(e-Government Act of 2002)에서도 IT 시스템 도입 시 반드시 고려해야 할 사항으로 명시할 만큼 그 중요성이 커지고 있으나 아직 그 방법론이 크게 발전되어 있지는 않다. 캐나다 역시 공공부문과 민간부문으로 구분되어 PIA를 실시할 것을 법제화하고 있다. 미국이나 캐나다에서 이처럼 정보시스템 도입시 PIA를 실시하도록 하는 것은 프라이버시의 문제를 중요하게 인식하고 있기 때문이다. 이들 국가 외에 여러 국가들에서도 감독관을 배치하여 개인정보를 관리한다던지 영향평가 전담기구를 두어 PIA를 실시와 관리를 하도록 하는 등 자국의 환경에 맞게 개인정보를 보호하고 있다. 이들 국가 중 캐나다의 PIA모델[12]을 근간으로 위험분석 부분을 도출하여 하나의 프로세스 모델을 개발하고자 한다.

2.3 프라이버시 영향평가 필요성

프라이버시 영향평가(PIA: Privacy Impact Assessment)란 새로운 정보시스템 도입이나 개인정보 수집에 앞서 시스템의 구축·운영이 고객 및 국민의 프라이버시에 미치는 영향을 평가하는 체계적인 절차를 의미한다. 앞절에서도 언급했듯이 NEIS의 문제로 국내에서도 프라이버시 침해에 대한 논쟁이 있었다. 가장 큰 문제가 바로 개인들의 민감한 정보가 정보시스템 안에 정보의 집적화와 노출의 위험성 때문이 아닐까 한다. 전자정부가 출범하면서 정부기관에서 국민들의 개인정보를 수집 및 이용하는데 시스템을 이용하여 업무효율을 기대하였으나, 시스템 취약성 및 물리적 관리허술로 인해 정보가 유출이 된다면 개인들에게 가는 피해는 엄청날 것이다. 이를 방지하기 위해 시스템 도입시 PIA를 실시하여 정보자산 중 개인정보의 범위를 알아내고 정보의 흐름을 분석하여 적절한 해결방안을 제시하는 것이다.

3. 프라이버시 영향평가 모델

PIA 프로세스는 시스템 소유자와 개발자가 개발의 초기 단계부터 프라이버시를 평가하도록 설계되어 있으며(그림 1)과 같은 절차를 통하여



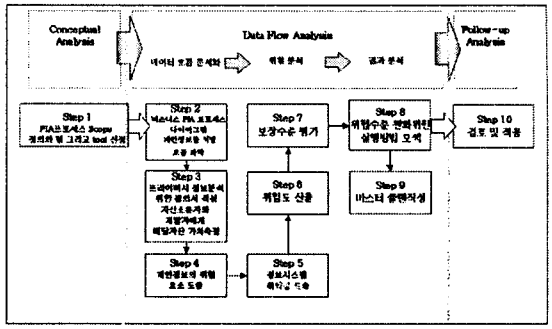
(그림 1) 캐나다 PIA process

수행된다. 크게 3영역으로 나눌 수 있고 각 단계별로 수행하는 업무가 나타나있다.

특히, 4가지 핵심영역 사람(people), 프로세스(process), 환경(environment), 기술(technology)을 3단계의 개념적인 분석(conceptual analysis), 데이터 흐름 분석(data flow analysis) 그리고 검토 및 적용단계(follow-up analysis)로 프라이버시의 위험도를 분석 및 적용한다. 이 중 데이터 흐름 분석단계에서 위험분석을 실시하여 자산에 대한 위험성을 개선한다. 이는 캐나다의 PIA모델에서 ISO/IEC 17799에서 가이드[13]하는 정보자산에 대한 위험분석 방법론[14]을 적용하여 PIA 모델(그림 2)과 (그림 3)에서 실제 적용시 적용할 수 있는 세부 프로세스를 개발하였다.

PIA 프로젝트 진행방안에 대한 각 단계별로 살펴보면 다음과 같다. 이 프로세스는 사전에 프라이버시 침해가능성이 있는 정보인지 판단을 하고 프라이버시 영향도가 있는 경우에 실시하는 것을 전제로 한다.

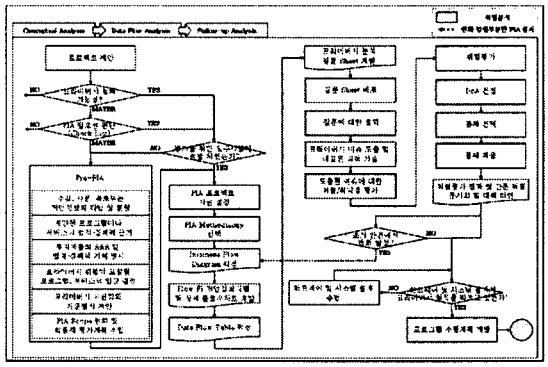
- Step 1 : PIA 프로세스 scope 정의와 팀 그리고 tool 선정
- Step 2: 비즈니스 PIA 프로세스 다이어그램



(그림 2) PIA 모델

을 그리고 개인정보를 식별하고 흐름을 파악

- Step 3: 프라이버시 정보를 분석하기 위해 질의서를 생성. 자산 소유자와 개발자에게 해당 자산의 가치 측정
- Step 4 : 개인정보의 위험요소 도출
- Step 5 : 정보시스템의 취약성 도출
- Step 6 : 위험도 산출
- Step 7 : 보장수준(Degree of Assurance) 평가
- Step 8 : 위험수준을 완화하기 위한 실행방법 모색
- Step 9 : 마스터 플랜 작성
- Step 10 : 실제 적용 후 검토



(그림 3) PIA 세부 process

PIA는 일련의 개인정보보호를 위한 정책절차라고 볼 수 있으며 실질적인 해결방안을 제시하

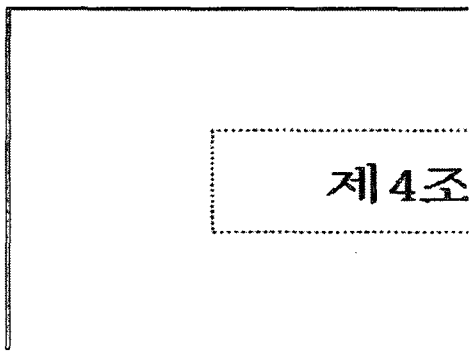
는 것이 아니라 방안을 모색하기 위해 사전적으로 문제를 고려하는 예방차원이라고 얘기할 수 있다. 따라서 이를 실질적으로 활용범위를 넓히고 시스템 도입 부분부터 위험분석 방법론을 같이 활용할 경우 시스템적으로 신뢰성을 높일수 있는 효과를 가져온다. 위험분석은 정보시스템과 물리적인 자산 등을 포함한 정보자산에 대한 위험도를 산출하여 정보시스템 취약성 분석과 위험도에 대한 보장 수준을 평가한다. 이런 통합방법으로 시스템 취약성을 해소하고 개인정보 자산에 대해 위험도를 낮춰주는 실질적인 방안이라 여겨진다. 따라서 권고사항으로서의 위험분석이 아닌 필수요건사항으로 정형화하여 모델을 구체화한 것이다.

4. 프라이버시 영향평가의 실시이유

프라이버시 영향평가는 왜 실시해야 하는가? 캐나다나 미국 등의 여러 국가들은 개인정보보호에 대해 OECD나 EU의 개인정보보호 지침을 근간으로 자국의 법제와 환경에 맞게 PIA프로세스를 진행한다. 정보화 사회로 세계가 발전하면서 정보 집적화로 인한 개인정보 수집 및 이용 등에 대한 프라이버시 침해문제를 사전적으로 고려하여 국민의 정보를 보호하기 위해 PIA를 실시하고 있다. 이를 위해 자국의 개인정보보호에 대한 법률제정을 강화하고 PIA실시 또한 의무화 하고 있다.

4.1 프라이버시 보호 법제

현재 국내에서도 개인정보보호에 대한 관심이 높아지면서 개인정보보호 법제강화와 개정을 하고 있고, 시민단체에서도 PIA실시 의견을 제시하고 있다. 국내법[16]에서는 크게 공공기관을 위한 개인정보보호 관련 법률과 정보통신망 이용촉진 및 개인정보보호 등에 관한 법률 외에 개별법에서 개인정보보호에 대한 법항이 있지만 구체화되고 범용적인 보호법에 대한 법률제정은 미비하다. 그러나 공공기관을 위한 개인정보보호 관련 법률은 OECD 개인정보보호 8원칙에 근간하여 제정하여 PIA 프로세스 진행시 이를 기준으로 각 시스템에 맞게 진행할 수 있을 것이다. 법에 대해 우리가 고려해야 하는 이유는 법제화 되었을 때 공공부문이나 민간부문 모두가 정책적으로 사용하도록 하기 위함이다(그림 4).



(그림 4) 공공기관을 위한 개인정보보호 관련 법률과 OECD 개인정보보호 8원칙

4.2 PIA 실시이유

PIA는 단순한 시스템 평가차원을 넘어 불필요한 개인정보의 수집을 막고 더 이상 필요치 않는 개인정보는 삭제함으로써 수집 및 관리하는 개인정보의 양을 감소시킨다. 또한, 프라이버시에 관해 NEIS 문제처럼 국민의 불만 등 외부개입이전에 내부적으로 문제를 해소함으로써 기관의 신뢰를 향상시키기 위함이다.

4.3 PIA 사례분석

캐나다의 SASKATCHEWAN 주정부의 17개 분야에 대해 프라이버시 영향평가를 실시한 report이다[16]. 17개의 분야중 Finance분야와 Information Service Corporation 2가지 분야에 대해 프라이버시 평가를 실시한 report 자료를

추출하여 예시로 제시하였다. 이 사례는 PIA 3단계 중에서 Data Flow Analysis을 통해 10가지 요소(그림 5)에 대한 프라이버시 영향평가를 실시한 사례이다[10].

1	Accountability	• 개인정보에 대한 통제 및 관리 책임자(Project Privacy Manager)를 지정한다. - PIA에 대한 책임이 프로젝트 Privacy 매니저에게 있는가? - Privacy에 대한 일련의 신뢰성이 문서화되어 있는가?
2	Identifying Purposes	• 회사는 개인정보가 수집되기 전에 수집할 개인정보의 목적을 식별해야 한다. - 수집된 개인정보와 프로그램의 기능적인 요구사항이 명확한 관계를 갖고 있는가? - 개인정보의 식속적인 수집을 최소화하기 위한 방법이 고려되고 있는가?
3	Consent	• 개인정보의 수집, 사용 및 공개를 위해서는 이에 대한 각 개인의 인지 및 동의가 있어야 한다. - 개인정보 사용에 대한 동의가 고객으로부터 공정적 답변을 받아야 하는가? - 개인정보 사용에 대한 동의가 간접적인 수집 및 사용을 허락하는가?
4	Limiting Collection	• 개인정보의 수집은 회사에 의해 승인된 목적에 필요한 경우로만 제한해야 한다. 또한 개인정보은 정당하고 법률적인 문제가 없는 범위에서 수집되어야 한다. - 개인정보의 수집이 규정에 의해 명시되어 있는가? - 개인정보가 각 개인으로부터 적절 수집되고 있는가?
5	Limiting Use, Disclosure, and Retention	• 개인정보는 각 개인의 동의 또는 법률에 의한 요구 동의 경우를 제외하고는 다른 목적으로 사용되어서는 안된다. - 개인정보가 명시된 목적을 위해서만 사용되고 있는가? - 주민번호 등과 같은 개인 식별 수단이 타당한 데이터베이스의 링크 목적으로 사용되는가?
6	Accuracy	• 개인정보는 정확성, 완전성 및 추가적인 업데이트가 이루어져야 한다. - 개인정보의 기록이 최근 정보를 유지하고 있는가? - 변경관리에 사용되는 개인정보의 기록이 유지되고 보관되는가?
7	Safeguards	• 개인정보는 정보의 민감성을 고려하여 적절한 보안 대응책에 의해 보호되어야 한다. - 개인정보에 대한 비인가된 접근, 수집 및 사용 등에 대한 대응책이 수행한단한단한단한단한단한단한단 한단한단계획이 수립, 검증, 저장 및 처리에 대한 보안 절차가 수립되어 있는가? - 개인정보에 대한 접근 및 변경을 위한 시스템이 구성되어 있으며 주기적인 감사를 실시하고 있는가?
8	Openness	• 회사는 개인정보 관리와 관련된 정책이나 조치 등에 대하여 각 개인이 쉽게 활용할 수 있도록 해야 한다.
9	Individual Access	• 각 개인의 요청에 의하여 개인정보에 대한 사용 및 공개는 유지되어야 한다. 또한, 개인정보의 정확성과 완전성에 오류할 수 있고 적절한 수정을 가할 수 있다. - 해당 업무에 사용되는 개인정보 데이터가 안정하게 저장될 수 있도록 시스템이 디자인 되어 있는가?
10	Challenging Compliance	• 개인정보 사용의 법률 및 규정에 관리하여 사용되어야 한다. - 개인정보 등에 대한 법률적인 문제 절차가 수립되어 있는가?

(그림 5) Privacy Analysis Principle

Accountability	Yes	No
PPM이나 다른 개인이 PIA에 대한 책임을 지고 있는가?		
어느 부문에서 개인정보에 대한 관리나 통계가 프로젝트의 일환으로 다른 대중이나 사적인 파트너에게 이전되는가?		
Privacy에 대한 책임이 문서화 되어 있는가?		
담당 부서의 수행 요구사항이 측정할 수 있는 방법으로 충분히 명시되었으며, 특정 수행이나 책임성 검토를 필요로 하는가?		
법적인 검토가 이루어 지는가?		
공적이 개인정보를 수집하고 어떤 목적으로든 제3자에게 공개하는 메커니즘을 계획하기 위한 법적, 계약적 권리를 유지하는가?		
조직은 공공기관이나 사적 기타 기관이 개인정보의 수집과 사용, 공개를 조사하는 특별 감사 및 검토실행 메커니즘을 가지고 있는가?		
• 대중의 기대 예측을 위한 질문 - 조직은 실제로 혹은 이해할만한 대중의 책임 감소를 수반하는가? - 대중에게 적절한 책임성을 보장하는 방법에 대하여 의사소통 할 전략이 개발되었는가?		

(그림 6) 프라이버시 분석시트(10개의 영역 중 제1영역)

각 영역별로 해당 분야의 책임자나 관리자 등 개인정보의 수집과 활용 및 폐기를 관리하는 사람에게 질의문(그림 6)을 보내 프라이버시 분석을 한다. 프라이버시 평가분석을 실시한 후 취약한 부분이나 개선해야 할 사항 등에 관한 권고사항을 명시한다<표 1>.

Department	Recommendations
• Finance • Information Services Corporation	• The FOI Act 와 프라이버시 핵심요소의 재시행과 의무적으로 교육을 해야하고 진행사항을 제공해야 한다. • Saskatchewan 주정부의 프라이버시 framework의 전반적인 정책과 절차를 세워야 한다. • 기관에서 프라이버시를 위해 형식상의 책임을 명시하여야 한다. • 외부기관과의 업무연계시 개인정보의 보호를 보증해야 하고 프라이버시 조항은 약정에 의해 만든다.

<표 1> PIA적용 후 권고사항(일부 발췌)

5. 결 론

5.1 법제화를 통한 PIA의 의무시행

정보화가 이루어지면서 많은 데이터가 정보시스템 속에 집적화되었다. 정보는 어떤 의미를 가질 때 진정한 가치를 가질 수 있는 개체이다. 개인정보의 매매나 오용으로 인해 프라이버시 침해문제는 나날이 두드러지게 나타났다. 이런 피해를 최소한 하기 위해서는 시스템의 도입시 이런 문제를 해소하고 법제도를 재정비하여 PIA 시행시 법의 보호를 받을 수 있도록 해야 한다. 개인정보보호에 관련한 법을 근거로 정보자산의 위험분석을 겸한 PIA를 실시함으로써 신뢰성있는 시스템을 구축하고 관리자들의 정보관리 책임을 부여해야 한다. 이런 시행과정이 없다면 전자정부 사업의 추진시 국민의 신뢰와 지지를 얻을 수 없고, 프라이버시 문제로 사업의 시행자체에 제제를 받게 된다면 비용적인 면에서도 많은 손실을 예상할 수 있다. 또한 시민단체나 여론에서도 프라이버시를 이슈화하여 다

각도로 연구하고 개인정보보호지침을 발간할 정도로 많은 관심을 가지고 있다.

5.2 정보의 분산화

정보를 집적화하여 관리하는 것은 사이버 공간에서는 매우 치명적인 형태로 나타날 수 있다. NEIS의 문제에서도 보듯 정보의 집적화로 인한 정보유출의 위험성을 배제할 수 없기 때문이다. 이를 해소하기 위해서는 정보의 기밀성의 관점에서 정보의 유출시 그 위험성을 최소화하는 방안을 모색해야 한다. 개인의 식별이 가능한 정보에 대해서 즉 민감성이 높은 정보는 시스템안에서 분산화시켜야 한다. 유출이 되어도 식별자체를 방지하기 위함이다.

현대는 모든 정보의 흐름이 오프라인에서 점차적으로 온라인상으로 유통이 되고 있다. 공공기관에서나 영리를 목적하는 기업에서도 정보의 수집과 이용은 필수요소라고 할 수 있다. 이런 정보의 집적이 사이버상에서 유출과 오용 등 여러 가지 위험 요소에 노출되어 있는지는 우리 모두가 인지하고 있는 사실이다. 그러나 정보시스템에서 정보의 집적은 시대에 도태되지 않고 효율적인 업무향상 그리고 국민의 편익을 위해서는 꼭 수행되어져야 할 일 중 하나일 것이다. 이를 위한 보안정책이나 기술들로 정보시스템 보안을 철저히 하고 있음에도 불구하고 정보의 노출 및 오용은 계속적으로 나타나고 있다. 특히 프라이버시는 그 중에서도 침해의 정도가 크기 때문에 이를 위한 적절한 방안이 필요한 때이다. 이를 위해 현재 개정안이 추진 중인 개인정보보호기본법을 근간으로 의무적인 프라이버시 영향평가를 실시해야 한다. 향후 더 발전적인 PIA Architecture와 Methodology를 개발하고, 또한 법적으로나 기술적으로도 개인정보구제 방안을 강화해야 할 것이다.

참고문헌

[1] 조화순, 거버넌스 관점에서 본 NEIS의 문제점, 정보화정책 제11권 제1호 pp.35~50, 2004

[2] 권선경, 국외프라이버시 영향 평가제도 시행현황,2003.08

[3] OECD Guidelines on the Protection of Privacy and Transboader Flows of Personnal Data.

[4] OECD 프라이버시 보호와 개인정보의 국제적 유통에 관한 가이드, 1980

[5] IMPLEMENTING THE OECD "PRIVACY GUIDELINES" IN THE ELECTRONIC ENVIRONMENT: FOCUS ON THE INTERNET, May-1998.

[6] 신종철, 프라이버시 보호를 위한 규제에 대한 연구, 성균관대 행정대학원,2002

[7] 이종호, 개인정보 침해사례분석과 방안에 관한 연구, 동국대 국제정보대학원, 2001

[8] 박춘식, OECD 프라이버시 그리고 시큐리티, 통신정보학회 제6권 제3호, 1996

[9] Privacy Impact Assessment, "A user's Guide", Ontario, June, 2001

[10] Goverment of Saskatchewan Privacy Assessment, Deloitte & Touche, 2003

[11] 김소정, OECD 정보보호가이드라인과 NEIS, 정보보호진흥원, 제8회 정보보호심포지움 2003

[12] Privacy Impact Assessment Guidelines, June 2001(http://www.gov.on.ca/)

[13] ISO/IEC 2000, INTERNATIONAL STANDARD ISO/IEC 17799
Information technology Code of practice for information security management, viii.

[14] 김강 외 2명, 정보시스템보안을 위한 위험분석모델, 한국 OA학회, 제7권 제3호, 2002.9

[15] 구병문, "캐나다 및 미국의 프라이버시 영향 평가 제도 분석과 국내 전자정부 법제로의 도입방향 검토", 정보화 정책 제10권 제3호 PP208-126 , 2003년
[16] 공공기관의 한 개인정보보호에 관한 법률/ 정보통신망 이용촉진 및 정보보호 등에 관한 법률(법제처 : http://www.moleg.go.kr/)
[17] 이경호 외 2인, 전자정부와 정보보호: 전자정부와 프라이버시, 한국정보보호학회지 제13권 제3호, 2003

송 세 현

2000년 전남대학교 응용식물학과(농학사)
2003년 3월~2003년 12월 (주)KTHsolutions
2004년 3월~현재 (주)컨설팅하우스 재직 중