情 報 保 護 學 會 誌
第18卷 第6號, 2008. 12

개인정보보호를 위한 관리체계와 거버넌스

김 정 덕*

요 약

개인정보보호가 단순히 개인의 권익에 관한 문제로 국한되지 않고, 기업의 사활을 좌우하는 이슈로 대두되고 있다. 또한 개인정보의 활용과 보호라는 두 가지 상충되는 기업 내 목표와 관련 개인정보보호법이나 규정 준수 등 대내외 요구사항을 만족시켜야 한다. 기업 내 개인정보보호활동의 효과성을 높이기 위해서는 현재 산발적으로 진행되는 개인정보 영향평가 등 단순 기법이나 정보유출방지 솔루션 도입 등의 접근방법으로는 한계가 있으며 새로운 접근방법이 필요하다. 본 고에서는 일상적 관리활동의 하나로서 개인정보보호를 위한 관리체계의 필요성과 관리과정을 소개하며 이를 평가, 지시 및 모니터링할 수 있는 거버넌스의 목표와 중요성에 대해 기술한다.

1. 서 론

기업의 활동이 IT를 통해 수행됨에 따라 전통적으로 기업이 관리해 오던 고객 정보가 디지털화 되어 정보시스템에 입력, 처리, 저장, 전송되고 있으며 이러한 정보의 축적 및 연계 활용은 더욱 가속화되고 있다. 이러한 대량의 개인정보의 집중화 관리체계와 이를 다루는 서비스 인력의 증가로 인해 개인정보의 오남용 위험 역시 급속도로 증가하고 있다.

그러나 우리 나라는 개인정보보호에 관한 한 아직 후진국 수준에 머물고 있다. 한국은 인터넷 강국이며 2007년 UN 보고서에 의하면 세계 5위의 전자정부, 국가정보화지수 3위 임에도 불구하고 정보보호, 또는 개인정보보호 수준은 20위권 밖에 머물고 있다고 판단된다. 그동안 정부를 위시하여 정보보호 수준제고를 위해 많은 노력을 하였지만, 여전히 네트워크나 서버에서의 기술적 측면에서의 정보보호에 치중하였고 업무 차원에서의 정보보호 노력은 상대적으로 매우 미흡하였다고 할 수 있다. 개인정보보호를 위해서는 특히 업무 차원에서의 개인정보흐름과 유출 가능성 분석을 통한 대책 수립이 매우 중요하기 때문에 실질적인 개인정보보호 노력은 매우 미흡하다고 볼 수 있다[1].

더우기 인터넷으로 인해 정보공유의 위력은 인지하고 있으나, 그 정보의 가치는 "공짜로 얻을 수 있다"라는 생각이 강한 디지털 세상에서 개인정보보호는 매우 어려운 과제이다. 특히 학연, 혈연, 지연 등 다양한 그룹에서 각 개인을 중심으로 형성되는 네트워크 안에서의 한국인의 정보공유 행위는 매우 강하다. 마치 공공재와 같이 생각하여, 개인정보를 제공, 이용, 취급하는 일반인이나 기업인 모두 거리낌 없이 개인정보를 주고 받으며 심지어 경제적 목적으로 매매하는 행태를 보여주고 있다.

아직도 강하게 남아있는 공동체 문화와 "우리가 남이가"라는 생각이 지배적인 한, 개인정보보호나 정보보호는 여전히 "자신의 일"이 아닌 "남의 일"인 것이다. 최근 뉴스에서 빈번하게 나오듯이 정부, 지자체, 민간기업, 병원 등 대부분의 개인정보 보유 조직에서의 "개인정보유출 불감증"이 만연한 현실을 고려할 때, 개인정보 제공자인 개인보다는 개인정보를 수집, 이용, 관리하는 조직에서의 개인정보보호 노력이 우선되어야 할 것은 당연하다 하겠다.

조직에서의 개인정보보호활동의 효과성을 높이기 위해서는 현재 산발적으로 진행되는 개인정보 영향평가 등의 단순 기법이나 정보유출방지 솔루션 도입 등의 접근방법으로는 한계가 있음을 많은 전문가들이 지적하고 있다. 즉 일회성 프로젝트 성격의 개인정보 영향평가 또는 기술적 솔루션 도입과 같은 방식으로는 상존하는 개인정보유출 위험을 효과적으로 관리하기 어렵다. 고객의 개인정보를 보호하기 위한 지속적, 순환적 프로세스를 포함하는 관리체계를 수립, 운영, 개선하는 노력이

* 중앙대학교 정보시스템학과 교수(jdkimsac@cau.ac.kr)

필요하다.

본 논문에서는 일상적 관리활동의 하나로서 개인정보보호를 위한 관리체계의 필요성과 관리과정을 소개하며 이를 평가, 지시 및 모니터링할 수 있는 거버넌스의 목표와 중요성에 대해 기술한다.

Ⅱ. 개인정보보호 관리체계 필요성과 과정

2.1 개인정보보호와 정보보호와의 관계

정보보호와 개인정보보호와의 관계에 대해 많은 논의가 있다. 혹자는 개인정보는 '민감 정보'로서 정보보호의 기밀성(confidentiality) 측면에서 다루고 있는 분야로서 개인정보보호는 정보보호의 일부분이라는 견해가 있다. 한편, 개인정보의 특성 상, 수집, 배포, 활용 등 면에서 개인으로부터 통지 및 동의를 얻어야 하는 특수한 상황이 있기 때문에 별도의 영역으로 접근해야 한다는 의견도 있다.

개인정보는 전통적으로 정보보호의 대상이 된 온라인 상의 처리, 저장 과정 뿐만 아니라 수집, 제공, 화면 및 문서출력, 폐기 등의 오프라인 과정 및 외주, 계약직 등을 통한 유출 가능성을 고려해야 하기 때문에 기존의 정보보호관리체계의 범위를 개인정보의 전체 생명주기를 포함하도록 확장하여 적용할 필요가 있다는 주장도 있다.

일반적으로 정보보호가 관리 및 책임 주체가 내부 구성원인 반면, 개인정보보호는 조직 외부의 고객이라는 또 다른 권리 주체를 상대로 해야 하기 때문에 개인정보보호는 전통적인 정보보호의 범위를 포함하고 있으며, 보다 폭넓은 영역을 다루어야 할 필요가 있다.

2.2 체계적 개인정보보호 관리의 필요성

정보보호관리체계가 기타 정보보호를 위한 여러 제도나 활동과의 근본적인 차이점은 바로 조직의 목표와 연계된 정보보호 목표를 달성하기 위한 제반 정보보호 활동을 중시한다는 점이다. 즉, PDCA (Plan, Do, Check, Act) 사이클로 대변되는 정보보호 활동이 정보보호관리체계의 요체라고 할 수 있다. 방화벽, 안티바이러스 등 보안기술 솔루션이나 정책서, 지침 등 문서의 존재 및 작동 유무를 확인하는 정보보호 통제 중심의 접근방법이기 보다는 정보보호가 지속적인 경영활동의 하나로서, 정보보호 프로세스 중심의 접근방법이라는 점이다. 다시 말해, 비즈니스와의 연계를 고려한 정보보호 목표 설정, 계획 수립, 위험분석을 통한 통제의 선택과 구현, 관리체계 운영에서 나타나는 제반 이슈들에 대한 검토와 개선 등으로 구성되는 일련의 활동 (프로세스)으로 본다는 점이 특징이다. 여기에서 통제는 특정 시점에서의 하나의 인스턴스이며 이는 조직마다 달라야 하고, 또한 환경변화에 따라 역시 변화되어야 한다.

한 예로 위험분석 없이 솔루션 중심의 통제 선택 및 구현은 대부분 예산 낭비와 비효과적인 정보보호 수준을 초래한다는 점은 많은 사례를 통해 입증되었고 대부분의 전문가들이 공감하는 바이다.

마찬가지로, 개인정보보호도 특정 통제의 구현과 운영으로 접근하기 보다는, 효과적인 개인정보보호를 위한 제반 활동과 이를 수행하기 위한 필요 조직 구성과 적절한 역할/책임이 규명된 하에서의 필요 통제가 구현 및 운영되어야 하는 시스템적인 접근방법이 필요하다.

Ⅲ. 개인정보보호관리과정과 고려사항

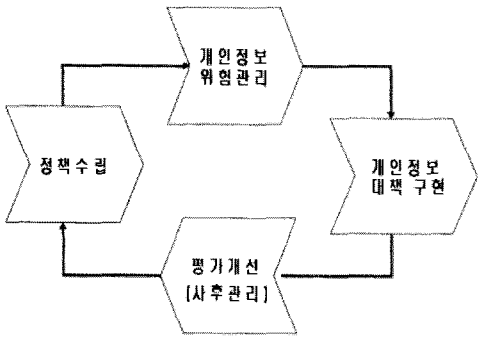
3.1 개인정보보호 관리과정

개인정보보호 관리과정은 [그림 1]과 같이 크게 4가지 단계로 구성할 수 있다, 첫째, 개인정보보호의 목표와 기본적으로 수행해야 할 사항들을 포함하는 개인정보보호 정책을 수립하는 것이다. 여기서는 정보의 활용을 극대화하면서 생성과 소멸을 책임질 수 있는 오너쉽(ownership)과 관리 책임(custodianship)을 구분하여 역할과 책임을 분명히 정의해야 한다.

둘째, 보호해야 할 개인정보와 관련된 업무와 자산을 식별하고 개인정보영향평가/위험분석을 통하여 개인정보의 수집, 이용, 보관, 파기 등의 개인정보보호름 전 과정에 대한 유출 위험성을 파악하고, 위험을 감소시킬 수 있는 대책들을 선택하는 개인정보 위험관리 활동이 수행되어야 한다. 특히 개인정보 흐름도 분석은 잠재적 위험을 식별하는데 매우 유용한 과정으로서 현업에서의 참가와 협조가 절대적으로 필요하다.

셋째, 선택된 개인정보대책을 구현하며 동시에, 개인정보관련 교육/훈련을 통해 인식변화와 문제해결 능력을 제고해야 한다.

넷째, 보호과정에서의 성과를 측정해서 문제점을 해결하고 향후 개선점을 파악하며 수정 보완하는 노력이 있어야 한다. 또한 개인정보보호 사고 발생시 신속하고 효과적으로 처리할 수 있는 법적, 기술적 사고대응체계도 구축해야 한다[2].



〔그림 1〕 개인정보보호 관리과정

3.2 개인정보보호관리체계 수립시 고려사항

이러한 관리과정을 중심으로 관리체계를 수립하고 운영하기 위해 아래와 같은 사항을 고려할 필요가 있다.

첫째, 개인정보를 활용하는 부서(예: 고객지원부서)와 개인정보보호를 담당하는 부서, 그리고 정보보호를 담당하는 부서간의 긴밀한 협조와 연계가 필요하다. 마이크로소프트 사가 2007년도에 조사한 서베이에 의하면 세 부서간의 협력의 중요성을 피력하고 있으며 실제로 개인정보유출 사건도 적은 것으로 나타났다.

따라서 실무위원회의 정기적 개최 등 관련 부서간의 의사소통체계를 구축하고 실질적인 협력이 이루어질 수 있도록 거버넌스 체계가 구축될 필요가 있다.

둘째, 관리 과정 중에서도 제일 중요한 개인정보 위험관리가 반드시 수행되도록 어느 정도의 강제적 조치가 필요할 수도 있다. 개인정보 위험관리는 중요한 만큼 수행하기 어려운 점도 많은 과정이다. 따라서 이 과정을 누락하고 단순히 시장에 유통되고 있는 유출방지솔루션에 대한 정보에 의지하여 선택, 구현하는 것이 대부분의 실태이다. 이 방법은 사후적인 접근방법이며 해당 응용시스템이나 서비스에 적합하지 않은 경우가 많아 효과성이 떨어지는 가능성이 높다. 신 정보서비스를 개시하거나 할 경우에는 반드시 개인정보 위험관리를 수행하도록 강제화하고 이의 결과를 토대로 신 서비스 사업 승인을 하도록 하는 대내외적인 강제조치도 필요하다.

셋째, 개인정보보호 기능을 가능하면 정보시스템부서에 위치시키는 것 보다는 별도의 전담조직을 구성하거나 위험관리조직에 위치시키는 것이 바람직할 것이다. 현재 정보보호 업무가 대부분 전산조직에 위치함에 따라 적절한 감시 및 통제 기능이 수행되지 못하는 것처럼 업무와 더 밀접한 관계를 가지고 있는 개인정보보호 업무를 전산조직에게 맡기는 행위는 피해야 할 것이다. 선진 조직에서는 점차 정보보호의 업무를 비즈니스 보안 또는 기업보안 차원에서 통합관리하려는 동향이 있다. 우리 나라도 이러한 추세로 가야 하며, 기업보안 차원에서 개인정보보호, 일반 정보보호, 물리적 보안 등을 통합해서 관리하는 체제로 진화해야 할 것이다.

이와 같은 세 가지 고려사항은 모두 경영층의 지시/지휘와 통제 행위를 규명하는 거버넌스 이슈로 해석할 수 있다. 따라서 개인정보보호 활동의 효과성을 위해서는 거버넌스 체계 구축이 필요하다.

Ⅳ. 개인정보보호 거버넌스

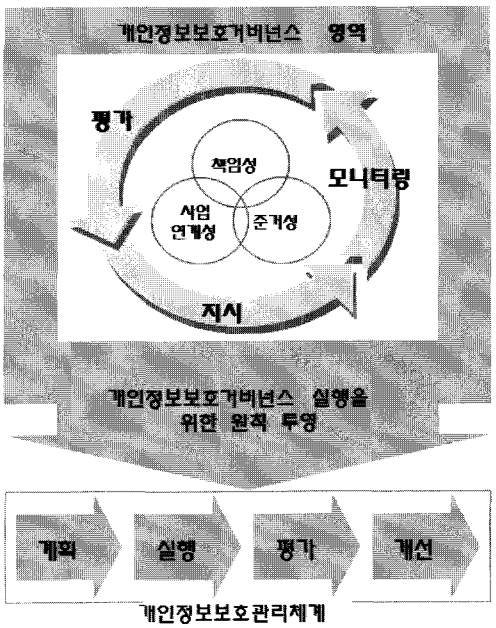
보다 효과적인 개인정보보호 활동을 위해서는 개인정보보호와 상당히 중복 관계가 있는 정보보호 활동의 발전과정을 살펴보면 많은 시사점을 얻을 수 있을 것이다.

컴퓨터가 상용화되기 시작한 1950년대 이후, 많은 기술적, 관리적 정보보호 대책 구현 노력이 있었지만, 2000년대에 진입하면서 인식하기 시작한 중요한 변화는 이사회나 상위 경영층의 정보보호에 대한 지원과 참여가 없으면 성공할 수 없다는 점이다. 즉, 정보보호의 새로운 패러다임으로서 상위 경영층의 역할과 책임을 중요시 하는 "정보보호 거버넌스" 체계 구축이 바로 그것이다. 따라서 우리가 배울 수 있는 교훈은 최근 국내에서도 많은 관심을 표하고 있는 개인정보보호를 위한 기술적, 관리적 노력에 추가하여 "개인정보보호를 위한 거버넌스" 체계를 동시에 구축해야 한다는 점이다.

개인정보보호를 위한 거버넌스란 무엇인가? 이는 "비즈니스에 존재하는 개인정보에 관한 위험관리를 통해, 기업내 개인정보보호 문화 형성을 도모하고, 이를 위해 기업의 모든 이해관계자를 고려하여 이사회와 최고 경영층의 개인정보보호 프로그램에 대한 지시 및 통제 활동과 이를 위한 조직, 역할과 책임, 절차를 포함" 하는 것이다. 개인정보보호를 위해서는 개인정보를 취

급 관리하는 여러 일선 부서의 노력과 협력도 중요하지만, 무엇보다도 CEO, CFO, CPO, CSO 등 최고 경영자를 위시한 임원급의 적극적인 역할과 책임을 강조하는 것이다.

이러한 개인정보보호 거버넌스는 [그림 2]와 같이 세 가지 목표(ABC)로 요약할 수 있다. 즉 책임성(Accountability), 비즈니스 연계성(Business alignment), 준거성(Compliance)이 그것이다. 책임성이라 함은 최고 경영층을 위시한 모든 조직 구성원의 개인정보보호에 대한 역할과 책임이 명확히 규명되고, 경영층의 지시 및 통제를 수행하기 위한 적정 자원 할당이 이루어져야 함을 의미한다. 비즈니스 연계성은 개인정보보호가 조직의 사활을 결정짓는 전략적 이슈로서 간주되어야 하며, 따라서 전사적 위험관리 차원에서 업무활동에 기반을 둔 개인정보보호 체계가 구축되도록 해야 한다. 단순한 네트워크나 서버 수준에서의 개인정보보호 조치로는 한계가 있으며 "개인정보의 활용과 보호"라는 양날의 칼을 염두에 둔 균형있는 보호 조치가 실행되도록 해야 한다는 점이다. 준거성은 조직이 준수해야 할 관련 법과 규제는 물론이고 조직 내부의 개인정보보호 관련 정책/내규와 내부감사 활동 결과에 대한 준거 여부를 상시 모니터링하고 실행, 개선할 수 있는 체계를 구축해야 한다[3].



〔그림 2〕 개인정보보호거버넌스와 관리체계

V. 결 론

최근 발생한 개인정보유출 사건과 이에 대한 정부 및 법원, 그리고 미디어로부터의 반응을 볼때, 개인정보보호는 개인의 정신적, 경제적 문제가 아닌 기업의 사활을 좌우할 수 있는 중요한 문제로 대두되고 있음을 경영자는 인식해야 한다.

효과적인 개인정보보호가 되기 위해서는 정보유출 솔루션 도입 및 구축으로 만족해서는 안되며 지속적인 관리활동으로서 개인정보보호관리체계를 구축해야 하며 이를 지시, 통제할 수 있는 거버넌스 체계가 작동되어야 한다. 조직 내 개인정보보호 활동을 지휘, 통제, 평가할 수 있도록 최고경영층의 역할과 책임이 규명되고 이를 수행하기 위한 일련이 메커니즘이 지원되지 않는 한, 실무부처에서의 노력만으로는 실효를 거두기 어렵다는 점이다. 개인정보보호에 대한 낮은 인식수준을 제고시키고 새로운 문화로 정착시키기 위해서는 최고 경영층이 직접 챙기고 지시하며 책임지는 활동이 전제되어야 할 것이다. 마지막으로 한가지 덧붙이고 싶은 것은 개인정보보호 거버넌스의 실행 주체로서 역량을 갖춘 CPO들이 더 많이 임명되어 활동해야 할 것이며, 조직 내에서 확실한 위상을 차지해야 할 것이다

참고문헌

[1] 이강신, 국내 개인정보보호 법규 현황 및 방향, 한국정보보호진흥원, 2008

[2] 한국정보보호진흥원, "개인정보보호 등을 위한 ISMS 모델 및 보호대책 개발," 2007. 1

[3] 김정덕, "Business Security Governance Framework," Joint Workshop on Information Security, 2008.7.

〈著者紹介〉

김 정 덕 (Kim, Jungduk)
종신회원
1979년 연세대학교 정치외교학과, 학사
1981년 연세대학교 경제학과 대학원, 석사
1986년 University of S. Carolina, MBA
1990년 Texas A&M University, Ph.D. in MIS
1991년 - 1993년 한국전산원, 선임연구원
1993년 - 1995년 원광대학교, 조교수
1995년 - 현재 중앙대학교, 교수
관심분야 : 정보보호 거버넌스, 정보보호 관리, IT 감사, 정보시스템의 전략적 응용 등