情 報 保 護 學 會 誌
第21卷 第5號, 2011. 8

개인정보보호관리체계 인증제도 구축 사례 연구

박 은 엽*, 최 진 원**, 조 태 희***

요 약

국내 주요기업(83개)의 개인정보보호책임자를 대상으로 조사한 결과 1백만명 이상의 개인정보를 수집하고 있는 기업이 61.4%(08년 기준)나 되고 국내 개인정보 침해건수는 2005년 18,000여건이던 건수가 급격하게 증가하여 2008년에는 39,000여건에 이르고 있다. 국민들이 개인정보를 안전하게 관리하는 기업을 손쉽게 식별할 수 있는 기준이나 정보가 미흡한 실정이며, 기업 스스로가 개인정보 침해사고를 사전에 방지하고 개인정보를 안전하게 관리할 수 있는 개인정보보호 체계의 필요성이 절실한 시기이다.

이에 본고에서는 국내·외 (개인)정보보호관리체계 동향을 비교·분석하고 국내 환경에 적합하도록 개인정보보호에 특화된 개인정보보호관리체계 인증제도를 소개하고 구축에 필요한 방법을 선구축한 기업의 입장에서 살펴보고자 한다.

Ⅰ. 서 론

인류의 삶은 정보통신의 발달 및 인터넷 문화의 급속한 변화로 인하여 일상의 생활방식뿐만 아니라 기업의 문화까지 변화되고 있다. 그러나 이러한 긍정적인 발전과 더불어, DDoS 등의 해킹, 악성코드 유포, 개인정보 유출 등의 역기능과 순기능이 공존하는 시대에 살고 있다.

특히, 최근에 거의 매일같이 발생되고 있는 개인정보 유출사고는 기존의 해킹, 바이러스 사고에 비해서 사회, 문화, 경제적 피해가 급격히 증가되고 있어 국민들뿐만 아니라, 관련 정부부처와 개인정보를 취급하는 기업들의 초유의 관심사로 급부상하고 있다.

최근 쇼핑몰, 유통업체 등의 개인정보 유출사고가 발생되면서 그 동안 소홀히 여겨왔던 개인정보가 핫이슈가 되고 있으며, 정부를 비롯한 업체 스스로 개인정보보호 체계 수립을 위한 많은 노력을 기울이고 있다. 고객 맞춤형 서비스에 대한 요구 증가로 기업은 물론 공공기관에서 취급하는 개인정보가 다양해지고 활용 범위도 복합, 융합되는 등 범위가 증가되고 있는 추세이다.

통계 자료에 따르면 주요 기업(83개)의 개인정보보호 책임자 대상 설문조사를 한 결과 1천만명 이상의 개인정보를 수집하는 기업이 16.9%이며, 주민등록번호 등 평균 9.8개 항목의 개인정보를 수집하고 있는 것으로 밝혀졌다.

대량 개인정보 침해사고는 법률소송, 배상 등을 연계되어 기업의 생존에 영향을 미치는 중요한 위험요소로 등장하였고 기존의 기밀정보 보호중심의 보호체계로는 전사적 차원으로 활용되고 있는 개인정보를 보호하는데 어려움이 발생되고 있다.

정보보호에 대한 각종 기술적, 관리적, 물리적 보호대책을 종합적이고 체계적으로 운영·관리하기 위해서 많은 기업들이 많은 예산 등을 투입하여 외부 정보보호 전문업체의 정보보호 컨설팅뿐만 아니라, 정보보호관리체계를 수립·운영하기 위하여 한국인터넷진흥원에서 수행하고 있는 정보보호관리체계인증을 취득하고 있으며, 국제표준인 ISO27001 인증도 같이 추진하여 외부의 공신력이 있는 인증기관으로부터 기업의 정보보호의 수준을 측정하고 지속적으로 관리체계를 유지·관리할 수 있도록 많은 노력을 하고 있다.

개인정보보호는 기존의 정보보호의 영역에 대부분이 포함되고 있으며, 기존 정보보호와 달리 법적 의무사항이 상당히 많이 존재하고 있으며, 위반시 기업 매출액의 1%, 최대 5천만원의 과태료뿐만 아니라 최대 5년간의 형사처벌 까지의 따르고 있어, 기업에 많은 부담감을 주고 있다.

* 고려대학교 정보보호 대학원 석사과정(aneus@nhn.com)
** 고려대학교 정보보호 대학원 박사과정(pepsicola@nhn.com)
*** NHN(주) 정보보안팀(thcho@nhn.com)

기업 입장에서는 개인정보보호관리체계 구축을 위해서 전사차원의 다양한 보호조치 구현이 요구됨으로 합리적 구축과 투자를 결정하기 위한 최소한의 기준 필요하고 침해사고로 인한 법률 분쟁 시 집단손해배상 등의 위험을 완화하기 위해서, 신뢰할 수 있는 기관으로부터 해당 기준의 부합성을 검증받으려는 기업의 요구 증가되고 있다.

자체적으로 개인정보보호관리체계를 수립하여 운영하고 있더라도 조직 전반적인 차원에서 그 신뢰성과 효과에 대한 확신을 갖기는 어렵다. 자체 검토는 평가의 신뢰성을 손상시킬 수 있다. 따라서 내부적인 평가만으로 대외 신뢰도를 제고하기는 힘들다.

대외적인 측면에서 개인정보보호 관리 능력에 대한 검증은 특히 아웃소싱 등 긴밀한 관계를 맺고 있는 사업 파트너의 경우 상대 조직의 개인정보 관리수준을 확인하기를 원할 수 있지만 그런 요구를 만족시켜주기 위해 내부의 감사나 세부사항을 공개하기는 어렵다. 따라서 이러한 의문을 해소하고 조직의 개인정보보호 수준에 대한 대내외적 신뢰도를 높이기 위해서 전문적이고 객관적이고 공신력이 있는 제3자에 의한 평가가 필요하다.

본 논문에서는 국내·외 (개인)정보보호관리체계에 대한 비교·분석하고 방송통신위원회와 한국인터넷진흥원이 추진하고 있는 개인정보보호관리체계 인증제도에 대한 개요, 절차, 현황 등을 살펴보고, 개인정보보호관리체계를 수립하는 과정에서의 고려사항과 운영상의 문제점을 분석하여 개인정보보호관리체계 수립시 중점적으로 고려해야할 요구사항 관점에서의 구축 사례에 대해서 논하려고 한다.

Ⅱ. 국내·외 (개인)정보보호관리체계 동향

2.1 유사 (개인)정보보호관리체계 인증제도

2.1.1 개인정보보호관리체계 인증

개인정보보호에 관련하여 인증제도를 제일 우선적으로 적용·구축한 것이 일본의 프라이버시마크 제도이다. 기업에서 구축·운영하는 개인정보보호체계를 평가하여 기업에 인증을 부여하는 제도로 일본정보처리개발협회(JIPDEC)가 인정 및 인증기관의 역할을 병행하며, JIPDEC에서 지정한 다수의 인증기관이 활동 중이다. 서류심사 중심으로 현장심사는 최소화 운영, 유효기간은 2년으로 사후관리 심사는 없다.

국내에도 이와 유사한 개인정보보호마크제도(e-Privacy)가 있다. 기업에서 운영하는 웹사이트의 개인정보보호 정책 및 관리수준을 종합적으로 평가하여 일정기준을 충족하는 경우 웹사이트에 인증 마크 부여하는 것으로 한국정보통신산업협회(KAIT)가 인증기관으로 심사 수행 및 인증위원회를 함께 운영하고 있다. 웹사이트 점검 및 서류, 현장심사를 수행하며, 마크 유효기간은 1년으로 사후관리 심사 대신 사후관리 모니터링을 실시(반기별)하고 있다.

일본의 프라이버시마크제도와 한국의 개인정보보호마크제도는 관리체계의 관점이라는 보다는 관리체계의 보호대책을 체크리스트화하여 기업 자체적으로 이행 여부를 확인하는 방식으로 운영한다고 볼 수 있다.

반면, 2009년 영국에서 BSI가 BS10012 : "데이터보호-개인정보경영정보 시스템에 대한 표준을 제정했다. BS10012는 개인정보의 효과적 관리를 위한 체계에 관한 표준으로써, 개인정보관리를 위한 기본체계 및 신뢰를 제공하고 컴플라이언스에 대한 평가를 위해 내부 및 외부 평가가 효과적으로 이루어 질 수 있도록 하며, 조직 내 개인정보보호관리체계에 대한 수립, 책임, 구현 및 유지를 위함이다. 또한 공공 및 민간 부문 등 조직 규모에 제한 없이 모든 조직에 적용 가능한 국제규격이다.

하지만 규격이 DPA(Data Protection Act 1998:영국의 개인정보보호법)을 기반으로 하고 있는 관계로 국내 관련 법률를 일부 충족하기 어려운 부문이 있으나, 개인정보 보호를 위한 프레임워크 및 요구사항이 국내에서 적용이 가능하며, 실제 2010년도에 세계 최초로 국내 게임업체에서 적용하여 인증을 획득한 사례가 있다.

2.1.2 정보보호관리체계 인증

정보보호와 관련된 인증제도는 ISO 27001 (정보보안경영시스템 인증)이 있다. 조직의 경영시스템 중 정보보호관리체계 시스템을 심사하고 인증하는 제도로 ISO와 IEC가 2005년에 제정한 국제표준이다. 각 나라별로 인정기관 및 인증기관을 지정하여 운영하고 있으며, 인증기관 내 인증위원회에서 인증결과를 심의하고 의결하고 있다.

인증심사는 문서심사와 현장심사로 이루어지며, 인증 유효기관은 3년으로 인증취득 후 연 1회 이상 사후관리를 받아야 한다.

국내에는 정보보호관리체계 인증(ISMS, Information Security Management System)이 있다. 기업이 정보자산의 비밀성, 무결성, 가용성 보장을 위해 구축 운영 중인 정보보호관리체계에 대해 제3자 인증기관(한국인터넷진흥원, KISA)이 적합성을 평가하여 인증을 부여하는 제도로 정보통신망 이용촉진 및 정보보호 등에 관한 법률에 따라 인정기관은 방송통신위원회가, 인증기관은 한국인터넷진흥원 및 방송통신위원회가 지정하는 기관으로 하고 있으며, 인증기관(KISA)에서 인증위원회를 구성하여 인증심사 결과의 적절성을 검토하고 있다. 문서심사와 현장심사로 이루어지며, 인증 유효기간은 3년으로 인증 취득 후 연 1회 이상 사후 관리 심사를 받아야 한다.

행정안전부에서 정부부처 및 공공기관을 대상으로 정보보호관리체계 수립 운영에 대한 필요성을 인식하고 KISA ISMS와 ISO27001 기반의 정부용 정보보호관리체계 인증제도인 G-ISMS를 제정하여 시범인증을 결쳐, 2010년 하반기부터 본격적인 인증심사 업무를 수행하고 있다. G-ISMS의 인증체계는 대부분을 ISMS를 준용하고 있으며, 인증심사원도 ISMS 인증심사원을 G-ISMS 인증심사 전환교육을 통해서 확보하여 운영하고 있는 상황이다.

Ⅲ. 개인정보보호관리체계 인증제도

3.1 개요

기업의 개인정보 이용 확산에 따라서 대량 개인정보 유출 사고가 지속적으로 증가되고 있는 문제점을 해결하고자, 방송통신위원회와 한국인터넷진흥원은 기업이 체계적이고 지속적인 개인정보 보호활동을 위한 관리체계를 제공하여 개인정보 침해 가능성 최소화하고 기업의 자율적인 개인정보 보호 활동을 유도하고 국민들이 개인정보를 안전하게 관리하는 기업을 식별할 수 있는 기준을 제공하여 기업 스스로 개인정보 침해사고에 대한 사전적 예방을 유도하고 정보 주체인 국민들에게 구체적이고 믿을 수 있는 판단의 근거를 제공하기 위하여 개인정보보호관리체계(PIMS, Personal Information Security Management System) 인증제도를 제정하였다.

3.2 개인정보보호관리체계 구축의 필요성

기업이 전사차원에서 개인정보보호 활동을 체계적·지속적으로 수행하기 위해 필요한 일련의 관리체계 구축의 필요성을 알아보면 다음과 같다.

첫째, 개인정보보호관리체계의 지속적인 운영 및 유지를 통해 개인정보보호 관련 기술 및 노하우를 조직 내부에서 시행착오를 통해 그 경험을 축적하여 개인정보 침해사고에 즉각 대응할 수 있는 능력을 갖추게 하여 사고발생 피해를 감소시킬 수 있다.

둘째, 정보통신서비스제공자는 관련 법률에서 개인정보의 수집, 이용 및 제공, 저장 및 관리, 파기에 이르는 생명주기를 관리하여 운영해야 한다. 개인정보보호관리체계를 수립하게 되면 일회적인 관리가 아닌 개인정보와 관련된 법률요구사항을 지속적으로 관리함으로써 법적 의무사항에 대해서 적절한 대응이 이루어질 수 있다.

셋째, 개인정보보호관리체계를 수립하면 조직의 인식제고를 보다 효율적으로 수행할 수 있다. 기존의 정보보호와는 달리 개인정보보호는 개인정보취급자의 역할이 상당히 중요하다. 이러한 개인정보취급자는 기획, 개발, 영업, 고객센터 등의 조직의 다양한 직무에 분포되어 있다. 이러한 개인정보취급자는 관련 개인정보보호 법률요구사항과 보호대책 수립을 이해하고 실천함으로써 조직에 보안성 향상을 위한 인식제고에 영향을 미친다.

3.3 인증체계 구성 및 운영

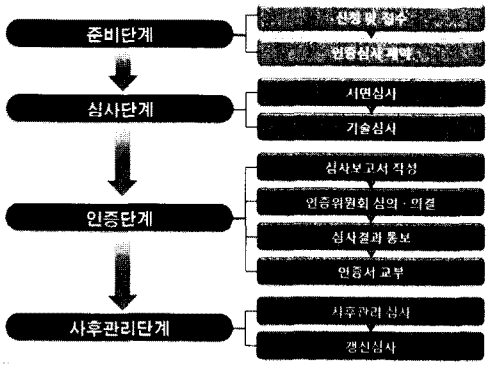
개인정보보호관리체계 인증은 정보보호관리체계 인증제도를 모태로 하여 개인정보보호에 특화하여 신설된 인증제도이기 때문에 인증체계 구성 및 운영방식이 거의 동일하다. 개인정보보호관리체계 인증제도는 객관성 및 신뢰성 확보를 위해 인정기관, 인증위원회, 인증기관을 분리하여 운영하는 체계로 구성되어 있다.

- 인정기관 : 인증제도를 관리·감독하는 인정기관을 방송통신위원회가 직접 수행
- 인증위원회 : 산업계, 학계, 정부의 전문가로 인증위원회를 구성하여 인증결과를 심의
- 인증기관 : 한국인터넷진흥원을 인증기관으로 지정하여 심사의 객관성 확보

3.3.1 인증 절차

개인정보보호관리체계 인증은 크게 4단계로 진행된다. 첫째, 인증신청 및 계약을 준비하는 준비단계, 심사

팀이 문서심사 및 기술심사를 한 후 그 결과 발견된 결함사항을 신청기관(기업)이 보완조치(1개월)하는 심사단계, 인증위원회가 인증심사결과를 심의하여 인증서를 교부하는 인증단계, 인증취득 심사하는 사후관리단계로 구분된다. 이러한 절차를 기본적인 흐름으로 도식화하면 [그림 1]과 같다.



〔그림 1〕 개인정보보호관리체계 인증 절차도

3.3.2 인증심사의 종류

인증심사에는 최초인증심사, 사후관리심사, 갱신심사, 재심사 4가지로 분류된다.

• 최초인증심사

기업이 수립하여 운영하는 개인정보보호관리체계가 방송통신위원회에서 의결된 개인정보보호관리체계 인증심사 기준에 적합한지에 대하여 최초로 확인하는 심사를 말한다.

• 사후관리심사

인증을 취득한 기업이 인증심사기준에 적합하게 개인정보보호관리체계를 운영 및 유지하고 있는 지 1년에 1회 이상 점검하는 심사를 말한다.

• 갱신심사

인증을 취득한 기업이 3년의 인증 유효기간 만료일 이전에 인증 유효기간을 연장하기 위한 심사를 말한다.

• 재심사

인증을 취득한 기업이 인증의 유효기간 내에 인증 받은 개인정보보호관리체계 범위 내에서 중대한 변화가 발생하였을 경우, 신청기업의 신청에 의해 인증기관이 다시 심사하는 것을 말한다.

3.4 개인정보보호관리체계 인증 요구사항

개인정보보호관리체계 인증심사 기준은 KISA ISMS, ISO/IEC 27001, BS10012 등 국내·외의 표준과 정보통신망 이용촉진 및 정보보호 등에 관한 법률에 명시된 개인정보보호조치를 고려하여 국내 환경에 적합하도록 보완하여 개발한 것으로, 타 기준에 비해 개인정보 유관 컴플라이언스를 대응하기 위한 최소한의 구현사항과 법적 준거성 측면, 그리고 체계운영 측면이라는 부분을 보강하였다. 또한, 현업에 있는 사업부서 담당자나 개인정보보호 조직담당자가 할 수 있는 부분을 명확히 구분하여 실제 활용 측면을 강조하였다.

3.4.1 개인정보보호관리체계 인증 기준

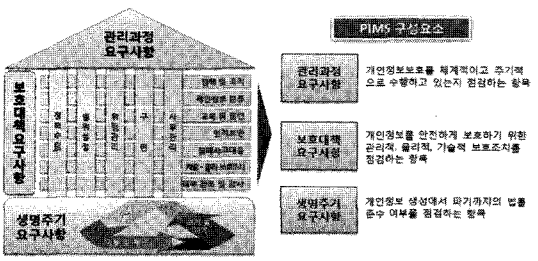
개인정보보호관리체계 인증심사 기준은 개인정보관리과정(5단계, 11개 통제사항), 개인정보보호대책(5단계 79개 통제사항) 및 개인정보생명주기(3단계, 29개 통제사항)으로 구성되었고 총 3개 분야의 119개 통제항목, 325개의 세부점검 사항으로 구성된다.

• 개인정보 관리과정

개인정보의 지속적이고 체계적인 보호를 위해 필요한 구성요소들로 ①정책수립, ②범위설정, ③위험관리, ④구현, ⑤사후 관리로 구성된다.

• 개인정보 보호대책

개인정보보호를 위한 관리적·물리적·기술적 요구사항들로 ①개인정보보호 정책, ②개인정보보호 조직, ③개인정보 분류, ④교육 및 훈련, ⑤인적 보안, ⑥침해사고 처리 및 대응절차, ⑦기술적 보호조치 ⑧물리적



〔그림 2〕 개인정보보호관리체계 인증 기준 구성도

보호조치 ⑨내부 검토 및 이행점검으로 구성된다.

• 개인정보 생명주기

개인정보 생명주기에 따른 법규 준수와 관련한 요구사항들로 ①수집에 따른 조치, ②이용 및 제공에 따른 조치, ③관리 및 파기에 따른 조치 사항으로 구성된다.

3.4.2 개인정보보호관리체계 인증 기준 항목

개인정보 관리과정, 개인정보 보호대책, 개인정보 생명주기는 크게 통제사항과 세부적인 점검항목으로 구성되어 있다. 점검항목은 해당 점검 시에 필수적으로 점검해야 되는 사항과 선택적으로 해당 기업에 맞게 선택할 수 있도록 구성되어 있다. 기존 유사 인증제도와 달리 PIMS는 개인정보보호에 대한 법률적 요구사항을 반영하고 있어서 법률근거가 포함된 점검항목수가 111개나 되며, 이러한 점검항목은 반드시 수행되어야 하는 사항이다.

〔표 1〕 개인정보보호관리체계 인증심사 기준

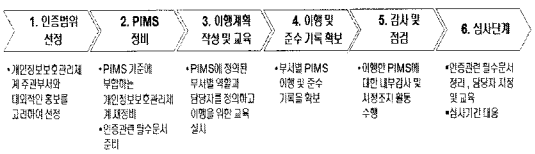
분야	세부분야	통제 사항수	점검 항목수	법률 근거
관리 과정	1. 정책수립	3	5	1
	2. 범위설정	2	5	0
	3. 위험관리	3	7	0
	4. 구현	1	2	0
	5. 사후관리	2	4	0
소계		11	23	1
보호 대책	1. 개인정보보호정책	6	11	0
	2. 개인정보보호조직	5	9	4
	3. 개인정보 분류	4	7	0
	4. 교육 및 훈련	4	7	5
	5. 인적 보안	3	9	5
	6. 침해사고처리및대응절차	7	20	2
	7. 6기술적 보호조치	36	125	33
	8. 물리적 보호조치	5	12	2
	9. 내부검토 및 감사	9	24	6
소계		79	224	57
생명 주기	1. 수집	8	17	13
	2. 이용 및 제공	16	49	34
	3. 관리 및 파기	5	12	6
소계		29	78	53
합계		119	325	111

Ⅳ. 개인정보보호관리체계 구축 절차

4.1 인증기관 관점에서의 인증 준비를 위한 절차

개인정보보호관리체계 구축이 단지 인증서 취득을 목적으로 준비하는 것보다는 기업이 개인정보보호에 대해 종합적이고 체계적으로 준비하여 개인정보 침해사고를 사전에 예방하려는 목적으로 구축을 한다. 기업이 스스로 개인정보보호관리체계를 수립한 결과에 대한 검증을 받기 위해서는 공신력과 신뢰성이 있는 제3의 기관으로부터 점검받는 것이 반드시 필요하며, 이를 인증이라는 수단을 통해서 확인할 수 있다.

인증기관 입장에서의 기업이 개인정보보호관리체계를 수립하고 인증을 받기 위해서 인증을 취득하기 위해서 고려해야 될 사항을 아래의 그림과 같은 절차로 준비를 해야 한다.



〔그림 3〕 개인정보보호관리체계 인증 준비 절차도

4.1.1 개인정보보호관리체계 구축 범위 설정

개인정보보호관리체계 인증준비를 하기 위해서 우선적으로 고려해야 되는 것은 인증범위의 선정이다. 인증범위의 선정에 따라 인증을 취득하기 위해 필요한 기간, 참여 인원 등이 참여 리소스뿐만 아니라 개인정보 관리체계의 구축하려는 해당 기업의 개인정보 파악과 사업모델 분석이 필요하기 때문이다.

기업의 개인정보 이용 현황 분석을 위해 전사적으로 개인정보 취급과 관련된 부서, 인력 및 취급시스템 등이 도출되면 모두 인증범위에 해당된다.

4.1.2 개인정보보호관리체계 정비

기업에서 서비스를 제공하기 위해서 내부적으로 운영하고 있는 개인정보보호 정책, 지침, 가이드, 매뉴얼 등을 개인정보보호관리체계 인증심사 기준과 매핑하여 개인정보보호 대책명세서를 작성하여 개인정보보호관

리체계를 수립, 구현 및 유지하기 위하여 필요한 문서들을 적절하게 준비하고, 그 문서들이 실질적으로 적용될 수 있는가를 검토 및 평가하는 것이 필요하다.

이를 통해서 인증을 준비하고 있는 기업에서 운영 중인 정책, 지침 등이 인증심사기준에 어느 정도 부합되는가를 확인할 수 있다.

4.1.3 이행 계획 작성 및 교육

인증심사기준에 맞게 수정 · 보완된 정책, 지침 및 서비스 운영기준을 정리하여 개인정보보호관리체계에 필요한 계획을 수립하여 관련 담당자들에게 인증에서 요구하는 기준에 대해서 교육을 통해서 숙지시키고 관련된 활동 등을 수행하면서 인증 준비를 이행해야 한다.

4.1.4 이행 및 준수 기록 확보

인증준비에 필요한 수립된 계획을 일정에 맞게 기간을 설정하고 인증 준비에 차질이 없도록 조치를 한다. 인증준비를 총괄하는 담당자는 이행 과제 진도를 점검하고 수행 여부를 감독하면서 인증 전반에 관련된 사항을 총괄 감독한다.

개인정보보호관리체계 활동 및 업무 수행 중에 발생되는 관련 문서들과 기록 등을 정리하여 유지 관리하여야 하며, 정책, 지침에 기록된 모든 사항들에 대해서 잘 이행되는지를 정기적으로 검토해야 한다.

4.1.5 감사 및 점검

이행 및 준수 기록 확보 단계에서 언급했던 정책, 지침, 인증심사기준에서 요구하고 있는 운영, 관리활동 및 기록에 대해 개인정보보호 감사 및 점검을 정기적으로 수행해야 한다.

자체 감사 및 점검을 통해서 문제점이 발견하고 개선하기 위한 필수적인 단계이므로 지속적으로 개인정보보호관리체계를 운영하기 위해서 필요한 과정이므로 매년 감사 및 점검 계획을 수립하고 운영해야 한다.

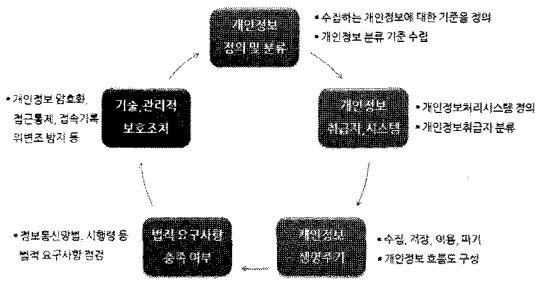
4.1.6 심사단계

인증심사 준비가 완료되면 심사단계에서는 개인정보보호관리체계에서 수립된 문서의 적정성 및 실질적인 적용 여부를 중점적으로 심사한다. 심사는 정책, 지침 등에 관련된 문서화된 형태의 적절성 심사와 보호대책과 생명주기에 필요한 기술적, 관리적 보호대책이 적절하게 선택되고 운영되는지를 심사하게 된다.

심사절차에는 사전심사, 문서심사, 현장심사로 구분되며 이를 통해서 운영되는 사항들이 문제가 발생될 경우 결함사항으로 지적하고 이를 30일 이내에 보완조치를 한 이후에 인증기관에 통보하면 보완조치의 적절성을 검토하고 인증서를 부여하도록 되어 있다.

4.2 기업 관점에서의 관리체계 구축을 위한 절차

인증기관에서 보는 개인정보보호관리체계 구축을 위한 절차와 기업 관점에서의 관리체계 구축을 위한 절차의 차이점은 인증심사 수행하거나 받는 입장에서의 관점의 차이만 있을 뿐이지, 개인정보보호관리체계를 수립 · 운영 · 유지하는 관점은 동일하다. 관리체계를 구축하려는 기업은 실무적이고 효율적으로 관리체계를 수립하기 위한 다양한 방법을 모색할 수 있을 것이다. 그림에 있는 절차는 개인정보보호관리체계 인증제도화가 되기 전에 고려하여 수립하여 운영했던 절차와 방법이므로 이를 활용하여 각 기업의 특성에 맞게 재구성하는 것이 바람직할 것이다.



〔그림 4〕 개인정보보호관리체계 구축 절차도

4.2.1 개인정보 정의 및 분류

기업들이 서비스를 제공하기 위하여 고객의 개인정보를 수집하고 이를 이용하고 필요한 경우, 위탁이나 제3자 제공 등의 다양한 형태로 개인정보를 활용하고 있다. 기업이 수집한 고객의 개인정보에 대한 정확한 사용과 통제를 위해서는 고객의 개인정보에 대한 법률적 정의를 명확하게 하고 기업의 각 특성에 맞게 개인정보를

단독 개인정보나 개인정보의 조합 등으로 개인을 식별할 수 있는지 여부를 판단하고 이를 중요도에 따라 분류하여 이에 적합한 보호대책을 마련해야 한다.

우선 개인정보를 분류하는 방법을 예를 들면, 개인정보의 중요도에 따라 등급으로 분류하기 위해 법률에서 단독정보로서 암호화를 반드시 해야 되는 개인정보를 최상의 1등급으로 분류하고 다른 개인정보와 조합되어 본인을 식별할 수 있는 경우를 2등급으로 분류하고 단독정보로서 중요하지는 않지만, 1, 2등급의 개인정보와 결합이 되어 더 민감한 개인정보가 되는 경우는 3등급으로 분류하여 등급별 관리 기준과 기업의 서비스 특성에 맞게 분류하여 운영할 수 있다.

4.2.2 개인정보취급자 및 개인정보처리시스템 지정

일반적으로 개인정보를 중요 등급에 따라 개인정보를 취급하는 자를 개인정보취급자로 정의하고 개인정보를 보유하거나 이를 통해서 전산적 처리를 하는 데이터베이스시스템을 개인정보처리시스템으로 정의한다. 여기서 고려해야 되는 것은 취급자와 처리시스템을 정의된 기준을 충족하는 모든 기업 임직원과 시스템을 모두 지정하는 것이 아니라, 개인정보를 취급하는 임직원을 최소한으로 하고 개인정보처리시스템도 꼭 필요한 시스템에서만 개인정보를 저장, 사용할 수 있도록 조치를 취하는 것이 제일 중요하다. 또한, 정기적으로 개인정보취급자에 대한 모니터링도 주기적으로 시행하여야 한다.

기업마다 취급자와 처리시스템의 관계를 정확하게 하지 않을 경우에는 기준이 애매하여 관리체계 수립에 어려움이 있을 수 있으므로 기준을 명확하게 정의해야 한다. 일반적으로 개인정보취급자는 개인정보처리시스템에 접근권한을 보유한 사용자 중 개인정보 관련 내용을 조회할 수 있는 권한을 보유한 자를 의미하고 개인정보처리시스템은 고객 정보를 저장하거나 고객 DB와 연동되어 고객 정보를 보유, 열람할 수 있는 시스템으로 정의할 수 있다.

4.2.3 개인정보 생명주기

개인정보 생명주기는 고객의 개인정보를 수집, 저장, 이용, 파기까지의 개인정보의 흐름을 파악하는 것으로 기업이 수집한 개인정보가 어떤 곳에서 어떻게 사용하는지를 파악하여 관리해야 한다. 서비스 별 개인정보 유통경로를 수집부터 파기까지 흐름을 파악하고 정리하고 개인정보를 체계적으로 관리하기 위해서 우선적으로는 온·오프라인 상에서 개인정보가 수집되는 경로를 찾고 어떤 개인정보를 수집하고 어떤 용도로 사용하는 지를 파악하여 항상 최신성을 유지하고 불필요한 개인정보 수집을 지양하고 최소한으로 하는 것이 바람직하다.

그리고 수집된 개인정보를 저장하는 시스템에 대한 현황을 조사하고 데이터베이스 시스템에 중앙관리를 할지 분산관리를 할지는 해당 기업의 특성에 맞게 고려하여 최소한의 시스템에서만 저장하거나 열람할 수 있는 제도적 장치가 필요하다. 이를 개인정보처리시스템으로 지정하고 법률에서 요구하는 기술적, 관리적 보호조치를 취하여야 한다.

개인정보처리시스템에 개인정보에 접근할 수 있는 권한을 가지고 있는 임직원을 개인정보취급자로 지정을 해야 하며, 처리시스템을 통해서 추출된 개인정보를 개인정보취급자로부터 제공받는 경우 등을 포함해서 개인정보를 열람할 수 있는 모든 임직원을 개인정보취급자로 추가 지정해야 한다.

기업이 업무 목적상 개인정보를 수집하고 저장하고 이용하는 행위가 그 목적을 모두 달성하거나 고객이 탈퇴 혹은 개인정보 삭제 요청을 할 경우에는 즉시 해당 개인정보를 삭제해야 하고 제대로 삭제되는지를 검토하는 관리적, 기술적 프로세스를 수립하여 운영해야 한다.

이러한 생명주기를 지속적이고 효율적으로 관리하기 위해서는 서비스 특성에 따라 다를 수 있는데 생명주기가 복잡하지 않고 변동이 많지 않은 경우에는 간단한 개인정보 흐름도를 작성하여 관리할 수 있지만, 서비스의 변화 및 연계된 시스템 및 서비스가 복잡한 경우에는 개인정보영향평가 등의 알려진 프로세스를 시스템화하여 운영하는 것이 편리할 수 있다.

4.2.4 법적 요구사항 충족 여부 검토

기업이 개인정보에 관련된 법적 요구사항을 충족하는지 여부에 대해서 서비스가 기획, 개발, 운영하는 전 단계에서 법률적 검토를 반드시 수행해야 한다. 예를 들면, 개인정보취급방침에 법률에서 요구하는 사항을 명시하도록 되어 있으나, 최신성을 유지 못하고 법률 위반 사항이 발생되는 가장 큰 원인은 서비스에 대한 이해도 부족과 주기적, 정기적 검토가 적절하지 못해서 발생되는 경우가 많다.

개인정보보호관리체계를 수립에서 있어서 제일 중요한 부분이 법적 준거성 확보임을 고려하여 고객의 개인정보를 수집에서 파기까지의 단계에서 발생 가능한 문제점을 모두 분석하고 적절한 보호대책을 수립하기 위한 법적 요구사항 충족 여부를 정기적으로 검토해야 한다.

4.2.5 개인정보의 기술적, 관리적 보호조치

앞에서 언급된 절차에 대한 구체적이고 실무적인 단계가 개인정보의 기술적, 관리적 보호조치를 취하는 것이다. 개인정보처리시스템에 접근하는 개인정보취급자 접근통제규칙 상세화, 침해대응을 위해 개인정보취급자 접속기록의 관리·감독의 강화, 민감한 개인정보의 불법사용을 방지하기 위한 개인정보의 암호화 강화 등이 포함되어 있다.

개인정보의 기술적, 관리적 보호조치는 매년 계획을 수립하고 계획에 맞게 정기적으로 이행 여부를 확인하거나 문제점이 도출되었을 때의 보호대책을 마련하는 등의 일련의 과정을 정규화하여 실시하고 이행 점검 결과를 경영진 혹은 개인정보관리책임자에게 보고할 수 있는 체계로 운영하는 것이 필요하다.

4.3 유사 인증제도의 중복성에 대한 기업의 고민

4.3.1 ISMS vs PIMS 인증제도의 문제

방송통신위원회와 한국인터넷진흥원이 운영하고 있는 정보보호관리체계(ISMS) 인증제도와 개인정보보호관리체계(PIMS) 인증제도의 유사성에 논란이 제도 도입 시기부터 논의되었다. PIMS와 ISMS간의 인증 대상 기업의 중복, 인증 기준 및 인증 체계의 유사성에 대한 논란과 인증제도 운영 측면에서 인증절차 수립, 인증위원회 구성·운영, 인증 심사원 양성 등 중복 투자가 발생될 우려가 있었다.

인증 대상기업은 중복될 수 있으나 인증 범위와 보호대상이 상이하므로 인증 목적에 따른 기업의 선택권이 확대된다고 할 수 있겠지만, 최근의 정보보호와 개인정보보호는 별도로 구분되는 것이 아니라 컨버전스 개념으로 모두를 포괄하고 있는 상황이어서 인증을 준비하는 기업으로서는 부담이 되는 것이 사실이다.

두 제도를 비교하면, PIMS는 개인정보를 취급하는 전체 조직 및 서비스를 인증 범위로 하는데 반해 ISMS는 특정 조직의 일부 서비스로 한정하여 인증 범위를 정할 수 있는 부분이 다소 차이가 있으며, PIMS는 개인정보를 기업의 자산으로 파악하여 수집에서 파기까지의 보호 활동을 인증하는 반면 ISMS는 개인정보를 포함한 기업의 모든 자산을 대상으로 하는 것이 차이가 난다.

ISMS와 PIMS를 모두를 고려하여 관리체계를 수립하고 인증을 받는 경우는 정보보호나 개인정보보호에 국한하지 않고 모두를 고려하고 개인정보보호와 정보보호가 유기적으로 관리할 수 있게 되어 기업의 입장에서는 체계적으로 관리할 수 있는 이점이 있다. 하지만, 인증심사를 받는 경우에는 동시에 인증심사를 진행하거나 중복항목에 대한 간편화를 하거나 행정절차의 간소화 등은 해결해야 될 문제이다.

4.3.2 ISMS vs PIMS 인증 기준의 중복성

두 인증제도의 인증기준을 비교·분석하면, 정보보호 정책, 인적 보안 등 관리적 보호조치는 공통적 심사항목으로서 정보보호 또는 개인정보보호 관점으로 표현한 것 뿐이지 관련 내용을 동일하다고 볼 수 있다. 공통 심사항목은 전체에서 41개 항목이 공통적으로 동일하고 55개 항목이 유사한 형태이다.

반면, ISMS 고유 심사 항목은 보안사고 관리, 시스템 개발 보안, 전자거래 보안 등 정보보호 중심의 보호대책이 41개이며, PIMS 고유 심사 항목인 개인정보 수집, 이용·제공, 관리, 파기 등 개인정보보호 관련 보호조치는 법률 중심으로 29개가 PIMS 고유 인증심사 항목으로 분류할 수 있다.

두 인증 기준에 따른 보호대책을 나눠서 별도로 관리하는 것보다는 통합하여 관리하는 것이 관리체계를 거시적인 관점에서 볼 수 있어서 더 좋을 것이다. 유사하거나 중복되는 심사항목의 보호대책을 동일하게 관리하고 고유한 두 인증심사 기준도 전체 보호대책에 포함하여 정보보호 체계 안에서 개인정보보호에 대책이 융화할 수 있도록 관리한다면, 중복 등의 문제보다는 통합적으로 관리할 수 있다는 장점이 있다.

4.3.3 기업 관점에서의 인증제도 간의 상생 방안

앞서 언급된 것과 같이 두 인증제도가 유사한 성격을 지니고 있고 중복성에 대한 논란으로 인해 인증 도입을 준비하는 기업들에게는 부담이 될 수 있으므로 다음의

사항을 고려하여 개선한다면, 일부 문제를 해결할 수 있지 않을까 판단된다.

우선 두 인증제도가 상호 인정하여 심사범위가 동일할 경우 공통되는 심사항목에 대하여 심사결과를 상호 인정하여 중복심사로 인한 기업의 부담을 최소화할 수 있다.

둘째, 인증심사의 증적자료를 활용하여 유사항목에 대해서는 기존 심사 증적을 최대한 활용하여 개인정보 측면 고려사항이 반영되었는지 점검하는 방법도 부담을 완화하는 방법이다.

셋째, 두 인증제도의 인증체계 구성 및 운영절차 등을 동일하게 마련하면 인증 신청 기업의 혼란을 최소화시킬 수 있고 인증 심사원 공동 활용, 심사 신청 및 처리절차 등을 같은 방식으로 운영을 하면 인증 신청 기업들의 혼란을 최소할 수 있다. 향후 두 관리체계를 동시에 수립하려는 기업을 위한 통합 관리체계 방법론을 제시하고 궁극적으로 두 제도를 통합한다면, 정보보호와 개인정보보호의 두 마리를 토끼를 모두 잡을 수 있을 것이다.

V. 결 론

기업이 고객정보를 수집하고 이용하는 과정에서 대량의 개인정보 유출사고가 지속적으로 발생되고 있으며, 대량의 개인정보 침해사고는 법률적 집단 소송, 배상 등의 기업의 책임과 의무가 증가되고 있어 개인정보 침해사고로 인해 집단 소송 등을 통해 배상요청이 보편화되는 추세이어서 기업의 생존에 영향을 미칠 수 있는 중요한 위험 요인이 되고 있다.

또한, 개인정보 유·노출 등으로 인한 민원이 급증되고 있는 상황을 고려해 볼 때, 기업이 자율적으로 개인정보 침해사고에 대한 사전적 예방과 고객의 개인정보를 안전하게 관리할 수 있는 새로운 보호체계의 필요성이 강조되고 있는 추세이다.

이러한 개인정보 침해사고를 예방하고 법률 분쟁시 개인정보보호에 대한 객관적으로 증빙할 기준과 방법을 공신력 있는 기관으로부터 적합성 인증을 증빙할 수 있도록 개인정보보호관리체계 인증제도가 탄생되었고 이를 통해서 기업이 스스로 개인정보보호관리체계를 수립하는데 많은 기여를 할 수 있을 것이라고 생각한다.

비록 유사제도와의 중복성 문제로 인하여 운영체계와 인증심사 기준 등에 대한 정부차원에서의 조율이 필요하지만, 기업 특성에 맞게 잘 운영을 한다면, 중복성 등의 문제보다는 기업이 개인정보보호에 대한 종합적이고 체계적으로 수립하는데 많은 도움을 줄 것이라고 기대가 된다.

아직 개인정보보호관리체계 인증제도가 정착되지 않은 시점이지만, 여러 시행착오를 통하여 국내 개인정보보호체계 강화에 큰 기여를 하는 인증제도가 될 것이라고 생각하며, 향후 각 기업의 특성에 맞는 개인정보보호관리체계 구축 방법론과 통합 구축 방법론 등이 다양하게 개발되어 적용한다면, 모든 기업이 고객의 개인정보보호를 위한 노력이 향상될 수 있다고 기대한다.

참고문헌

[1] 방송통신위원회, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 시행령, 시행규칙, 2011.

[2] 방송통신위원회, "정보보호관리체계 인증심사 기준," 방송통신위원회 고시 제2002-22호, 2002

[3] 방송통신위원회, "개인정보보호 관리체계 인증제 도입에 관한 건," 방송통신위원회 66차 회의 (2010-66-273호), 2010

[4] 한국인터넷진흥원, "정보보호관리체계 인증업무지침," 2003

[5] 한국인터넷진흥원, "개인정보보호관리체계 인증업무지침," 2011

[6] 한국인터넷진흥원, "개인정보보호관리체계 인증 준비 안내서", 2011

[7] 심미나, "효율적인 개인정보보호관리체계(PIMS) 인증제도 도입방안 연구," 박사학위논문, 고려대학교, 2009년 12월

[8] 장상수, 이호섭, "정보보호관리체계(ISMS) 인증심사 결함사항 분석에 관한 연구," 정보보호학회지, 20(1), pp. 31-38, 2010년 2월.

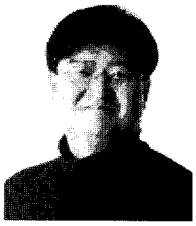
[9] 김정덕, "개인정보보호를 위한 관리체계와 거버넌스," 정보보호학회지, 18(6), pp. 1-5, 2008년 12월.

[10] 장상수, 김학범, 이홍섭, "정보보호관리체계 인증제도 소개 및 추진 방향," 정보보호학회지, 11(3), pp. 1-15, 2001년 6월.

〈著者紹介〉

박 은 엽 (Park EunYeop)
정회원
2001년 2월 : 서울여자대학교 컴퓨터학부 졸업
2005년 3월 : 고려대학교 정보보호대학원 석사과정
2007년~현재 : NHN(주), 정보보안팀
<관심분야> 정보보호, 개인정보보호, 정보보호 교육

최 진 원 (Jinwon Choi)
종신회원
2005년 8월 : 동국대학교 정보보호학과 석사
2007년 3월~현재 : 고려대학교 정보보호학과 박사과정
2006년 3월~현재 : NHN(주), 정보보안팀
<관심분야> 보안경제학, 정보보호 성과측정, 내부통제



조 태 희 (Taehee Cho)
정회원
1998년 11월 : RoyalHolloway, University of London 정보보호학과 석사 졸업
1999년 7월 : LG전자
2001년 4월 : 한국정보보호진흥원, ISMS 선임심사원
2008년 1월~현재 : NHN(주), 정보보안팀
<관심분야> 정보보호관리체계 인증, 위험관리, 정보보호정책