情 報 保 護 學 會 誌
第23卷 第5號, 2013. 10

개정 고시에 따른 개인정보보호 관리체계(PIMS)인증의 주요변화

전 진 환*, 조 강 래**

요 약

방송통신위원회는 2011년부터 개인정보보호 관리체계(PIMS)를 시행하고, 심사를 통해 신청기업이 개인정보보호를 위해 일정수준 이상의 관리적·기술적·물리적 대책을 수립 및 운영하고 있을 경우 인증을 부여하고 있다. 이에 따라 이용자 및 정보주체는 해당 기관의 인증취득 여부를 통해 개인정보의 누출가능성을 최소화하고 효과적으로 보호하고 있음을 갈음하는 수단이 되고 있다.

본고에서는 개정 정보통신망법에 따라 지난 9월11일 방통위 의결을 통과한 개정 PIMS 고시에서의 주요하게 변화된 내용 중 민간인증기관 지정, 인증심사 항목의 개선에 대해 살펴보고, PIMS 인증을 준비 중인 기업의 이해를 돕고자 한다.

Ⅰ. 서 론

국내 사업자, 공공기관, 협·단체가 정보주체로부터 수집한 개인정보를 업무에 이용 및 제공하기 위해서는 개정 정보통신망법이나 개인정보보호법 등 엄격한 법률의 적용을 받을 수밖에 없기 때문에 활용에 있어 많은 제약이 따른다. 물론, 이러한 법적 제재가 개인정보 누출 등의 관련 보안사고를 예방하기 위한 필수조건임에는 분명하지만, 법규제의 이행만으로 개인정보 침해사고 대응에 효과적인 예방책이라 보기에는 어렵다.

더욱이 대부분의 기업들이 개인정보를 안전하게 관리하고 있는지에 대한 현황은 현실적으로 파악이 불가능하고, 기업이 자율적으로 개인정보 침해사고를 예방 및 관리할 수 있도록 적정 방법론을 제시하는 것 역시 개별 기업들의 특수성으로 인해 어려운 것이 사실이다.

이에 개인정보보호 관리체계(PIMS ; Personal Information Management System) 인증은 2011년부터 시행되어 개인정보보호를 잘 관리하는 기업들을 식별하는 수단으로 활용되어 왔으며, 시행 이후 2011년에 10건, 2012년에 10건, 2013년 10월 현재 10건의 취득함으로서 총 30개의 기업을 대상으로 인증을 부여[1]하였다.

또한, 2013년 9월, 방송통신위원회는 의결을 통해 개정「개인정보보호 관리체계 인증 등에 관한 고시」[2]를 통과시키고, 개정 정보통신망법에 따라 개인정보보호 관리체계(PIMS) 인증을 기존 방통위 의결사항에서 법적 권고사항으로 변경하였으며, 민간인증기관 지정과 인증심사 기준변경 등에 관한 내용을 주요골자로 하고 있다.

이에 따라 본고에서는 개정된 PIMS 인증고시의 두 가지 주요 내용을 살펴보고, 향후 인증기관 지정 및 인증취득을 준비하는 기업의 이해를 돕고자 한다.

Ⅱ. 본 론

개정 고시(방통위 고시 제2013-17호)에 따른 개인정보보호 관리체계(PIMS) 인증의 두 가지 주요 변경내역은 다음과 같다.

2.1 민간인증기관의 지정

개정된 고시에서 가장 큰 변화는 기존 PIMS인증 및

* 개인정보보호협회, PIMS인증팀 (jhjeon@opa.or.kr)
** 중앙대학교 일반대학원 경영학과 MIS전공 석사과정 (netheus@hanmail.net)

인증관련 업무를 수행해오던 한국인터넷진흥원(KISA) 이외에 민간인증기관을 추가로 지정할 수 있다는데 있다.

방송통신위원회는 정보통신망법 제47조제5항 및 영 제53조의2에 따라 인증기관을 지정할 필요가 있는 때 지정대상 기관의 수, 업무의 범위 및 신청방법 등을 정하여 관보 및 인터넷 홈페이지에 20일 이상 공고하여 인증기관을 지정하도록 하였다.

민간인증기관의 추가지정은 한국인터넷진흥원과 동등한 지위에서 PIMS 인증심사를 수행하고, 인증위원회 운영, 인증부여 등 관련 업무를 독립적으로 수행할 수 있다는 점에서 향후 인증활성화를 위해 고무적인 변화라 할 수 있다.

민간인증기관 지정을 원하는 신청기관은 업무수행요건 및 능력심사를 통해 방통위가 공고한 지정대상 기관의 수만큼 점수의 합이 높은 순으로 선별하게 된다.

인증기관 지정을 위한 신청기관 심사기준은 다음과 같이 업무수행요건과 수행능력을 평가하는 총 7개의 항목으로 구성되어 있다.

먼저, 업무수행요건은 세부기준은 [표1]과 같이 2개 항목으로 구성되어 있다.

〔표 1〕 업무수행 요건 심사 세부기준

평가항목	세부 평가 기준
인증심사원 5명 이상 상시 고용	인증심사원 5명 이상을 상시 고용하고 있어야 함
인증기관 공정성 확보	PIMS 구축과 관련된 컨설팅 업무를 수행하지 않아야 함

첫 번째는 신청기관이 PIMS 인증 업무를 원활히 수행하기 위해 상시 고용하고 있어야 할 최소한의 인증심사원의 수는 5명이다. 인증기관의 인증심사(서면심사 및 기술심사) 전문성과 신뢰성을 확보하기 위해 신청기관은 인증심사원(보) 이상의 심사원 5명을 반드시 상근으로 고용하고 있어야 한다. 또한, 자체 심사팀을 구성할 수 있도록 인증심사원 중 1명 이상은 반드시 선임심사원 자격을 가지고 있어야 한다.

그리고 인증기관의 독립성과 객관성을 확보하고, 공정한 인증심사의 기능을 적절히 수행할 수 있도록 컨설팅 관련 업무 수행은 제한하도록 하고 있다.

다음으로 업무수행 능력 심사 세부 기준은 5개 항목으로 [표2]와 같다.

〔표 2〕 업무수행 능력 심사 세부기준

평가항목	평가요소
조직 내 직원들의 개인정보보호 전문성	개인정보보호 업무 전문성
	개인정보보호 관리체계 인증심사 참여 실적
시설	사무공간·인증심사 서류 보관 장소 및 보안설비, 시설 확보
신뢰도/재정상태/건실도	부채비율 및 자기자본 이익률
인증업무 운영체계	인증기관의 운영체계 및 인증 품질 관리 인증업무를 수행하는 직원에 대한 운영·관리 등의 내부 규정 인증업무 수행 방법 및 절차 인증업무 지원체계
가점 및 감점	인증심사업무를 전담하는 인증심사원 보유수
	개인정보보호 관리체계 인증의 취득 및 유지
	자격취소 사실

먼저, 신청기관 임직원의 개인정보보호 업무의 전문성을 확인할 수 있는 최소한의 자격기준을 구비해야 하며, 인증심사 경력, 박사학위 및 기술사 자격, 기타 자격증 등을 통해 (개인)정보보호 분야의 자격을 유효하게 보유하고 있는 소지자를 1명 이상을 확보하고 있어야 한다.

두 번째, 신청기관은 원활한 인증심사의 상담, 인증심사, 인증 관련 업무를 원활히 수행할 수 있도록 최소한의 물리적 사무공간, 보안설비, 시설을 갖추고 있어야 하고, 각종 장비 및 인증관련 서류의 물리적 보호대책을 제공하기 위한 요건을 마련해야 한다.

세 번째, 신청기관은 안정적인 재정 상태를 확보하고 있어야 하며, 추후 인증기관으로 운영 중 재정적 미비로 인해 인증심사를 수행하는데 있어 부담으로 작용하지 않아야 한다. 따라서 직전년도 부채비율이 50% 미만이며, 자기자본이익률이 20% 이상이어야 하나 비영리 법인 또는 비영리 민간단체는 평가기준에서 제외한다.

네 번째, 신청기관은 엄격한 인증심사 업무규정을 수립하여 인증기관의 공정성, 객관성, 신뢰성, 독립성을 보장하고, 인증심사 결과에 대한 신뢰성과 정확성, 품질을 보장할 수 있어야 한다.

다섯 번째는 가점과 감점으로 상기 4개 항목에 대한

평가 이후 신청기관의 현황에 따라 추가적인 점수를 가감하게 된다. 신청기관이 인증심사 업무를 위해 전담조직을 구성하고 인증심사원 10명을 상시 고용하고 있거나 PIMS 인증을 취득한 경우 을 경우 추가배점하고, 인증이 취소된 경우 감점하게 된다.

민간인증기관으로 지정된 기관은 매년 인증심사 실적을 방통위에 보고해야 하고, 인증기관 재지정은 유효기간이 끝나기 6개월 전 재지정 신청과정을 통해 인증기관의 지위를 계속 유지할 수 있도록 하고 있다.

2.2 인증심사 기준 변경

2012년 8월, 개정 정보통신망법의 시행되면서 기업들이 습관적으로 수집해오던 인터넷에서 주민등록번호 수집 및 이용금지, 개인정보 누출 시 통지 및 신고, 장기간 미사용자에 대한 개인정보 파기, 개인정보 이용내역 통지 등 신규 내용이 추가하여 강화하였다.

개정 PIMS 고시 역시 변경된 내용을 포함하여 개정되었으며 기존 118개 통제항목에서 신규항목을 추가하거나 유사한 인증기준을 통폐합하여 124개로 심사항목을 변경하였다. 이렇게 변경된 심사항목의 변경은 다음의 [표3]과 같다.

〔표 3〕 PIMS 인증심사 기준 변경

통제영역	변경 전	변경 후	비고
관리과정	11	13	2(+)
보호대책	79	79	0
생명주기	28	32	4(+)
합 계	118	124	6(+)

먼저, 특히 개정 정보통신망법, 개인정보보호법에서 인증심사 시 반영이 필요한 부분을 도출하여 통제항목으로 추가함으로써 법률 변경 등에 따른 최신화한 것이 특징이다. 예를 들어, 개인정보 수집에 따른 조치에서 주민등록 수집 이용제한, 주민등록대체수단 제공 등은 정보통신망법을 반영한 것이고, 영상정보처리기기에 대한 심사기준 반영은 개인정보보호법을 근간으로 하고 있다.

두 번째, 기존 통제항목에 대한 현실성, 중복성, 불명확성을 재검토함으로써 인증심사에 발생할 수 있는 혼란을 최소화 하고자 하였다. 출력, 복사통제, 외부위탁 및 제3자 제공시 개인정보 영역을 중심으로 중복 또는 유사항목은 개인정보 출력용도의 특정 및 보호대책에 통합한 것이 일례라 할 수 있다.

세 번째, 최신기술에 대한 인증심사 기준을 추가되었다. 모바일 기기 접근(모바일 기기의 네트워크 연결), 인터넷 접속 통제(인터넷망과 업무망 분리), 스마트워크 보안, 무선 네트워크 보안(인증, 암호화), 패치관리, 휴대용 저장매체 관리(절차마련), 외주개발 보안, 모바일 기기 반출입(통제 절차) 등 최근 이슈가 되고 있는 기술에 대해 많은 부분 인증심사기준에서 고려 대상이 되었다.

네 번째, 법적 준거성에 대해 더욱 엄격해졌다. 관리과정에서 개인정보 흐름파악 항목을 추가하였고, 생명주기 심사기준에서 주민등록번호 수집 이용제한, 주민등록대체 수단 적용, 고유식별번호 별도 동의 여부, 휴면 이용자의 개인정보 파기 등이 추가되어 법률을 현행화여 반영함과 동시에 상당부분 엄격해졌다.

다섯 번째, 케이블 보호, 장비의 안전한 폐기 및 재사용 등 중요도가 낮았던 기존 심사 항목들은 삭제되었다.

Ⅲ. 결 론

지금까지 개정 PIMS 인증고시의 두 가지 주요변경 내용에 대해 살펴보고, 기업체, 공공기관, 협·단체가 PIMS 인증을 이해하고, 인증기관 지정 및 PIMS 인증을 취득하기 원하는 기업의 이해를 돕고자 하였다.

먼저, 민간인증기관의 추가지정은 언급한 바와 같이 PIMS 인증의 활성화를 꾀하는 주요 수단이 될 수 있다. 하지만, 민간인증기관의 수익보전을 위한 부적격한 인증서의 남발이나 부실한 인증심사 오남용을 막기 위해 방통위나 제3자의 기관에서 철저한 관리감독이 필요할 것이다. 또한, 민간인증기관은 인증심사와 인증관련 업무에 있어 기존의 한국인터넷진흥원이 보유한 전문성과 인증심사의 품질 확보 및 유지가 반드시 선행되어야 할 것이다.

인증심사 기준의 변경과 관련하여 국내 개인정보보호와 관련된 포괄적인 인증으로서 자리매김하기 위해 통제항목의 현실화에 많은 노력이 있었음을 확인할 수 있었다. 하지만, 아직 실무에서는 변경된 기준을 적용하지 않고, 기존 인증기준으로 컨설팅하거나 인증준비를 마친 상태이므로 가급적 인증기준의 적용에 혼란을 축소할 수 있어야 할 것이다.

마지막으로 기업들이 PIMS 인증취득에 많은 시간과

노력을 투자하고, 취득이 어려운 인증으로 인지하는 만큼 인증취득을 통해 이용자의 개인정보의 보호수준을 질적으로 향상시키고, 인증취득 기업에 특화되고 차별화된 혜택이 현재보다 더 지원될 수 있다면 인증 활성화에 추가적인 기여가 발생할 것으로 예상한다.

참고문헌

[1] 한국인터넷진흥원, http://isms.kisa.or.kr/
[2] 방송통신위원회, 개인정보보호 관리체계 인증 등에 관한 고시 제정(고시 제2013-13호), 2013.

〈著者紹介〉

전 진 환(Jeon, Jin-Hwan)
정회원

2006년 2월: 부산대학교 일반대학원 경영학과 박사
2010년 2월: 부산대학교 경영경제연구소 박사후 연구원
2012년 2월: 한국인터넷진흥원 보안관리팀 책임연구원
2012년 3월~현재: 개인정보보호협회 PIMS인증팀 과장
<관심분야> 개인정보보호 관련 인증 표준화, PIMS 인증

조 강 래 (Cho Kangrae)
비회원

2012년 8월: 중앙대학교 경영과 졸업
2012 9월~현재: 중앙대학교 경영학과 석사과정
<관심분야> 경영정보시스템, 정보보안