정보보호관리 표준화 및 인증제도 연구

정현준(대전대학교 산업정보대학원 석사과정)*
강기찬(대전대학교 창업보육센터 전문매니저)**
이 형(대전대학교 컴퓨터정보통신공학부 교수)***
hjjeong@dju.ac.kr* kckang@dju.ac.kr** hlee@dju.ac.kr***

키워드 : 정보보호관리, 인증

요 약

정보보호관리(Information Security Management)는 정보보호의 분류 방식 중 하나인 관리적, 기술적, 물리적 대책 분류에서의 관리적 대책만을 다루는 것이 아니라 보안정책의 수립, 위험 분석, 보안 대책의 선택 및 구현, 정보보호 시스템 구축, 보안대책 평가 등을 하나의 과정(Process)으로 인식하여 체계적이고 종합적으로 관리하는 활동을 총칭한다. 최근 전세계적으로 해킹과 바이러스 등의 침해사고가 빈발하고 인터넷을 활용한 서비스 제공이 본격화되면서 정보보호라는 것이 기술적인 이슈가 아닌 관리상의 문제라는 인식이 빠르게 확산되고 있으며, 정보보호를 조직의 전체적인 차원에서 체계적으로 관리하는 정보보호관리(Information Security Management)에 대한 국제적인 관심이 고조되고 있다. 또한 정보자산 등에 대해서 정보보호 관리체계 인증제도를 적용하여 안전한 전자상거래의 활성화를 도모하고 정보통신 환경의 안전과 신뢰성을 확보할 필요성을 인식하고 있다. 아울러 국가 주요 정보통신 시설에 대한 보호대책 및 안정적 운영의 확보 방안이 절실히 요구되고 있다.

현재 정보보호를 위한 방화벽, 하드웨어, 소프트웨어 등 각종 보안장치가 가동 중에 있지만, 많은 정보시스템은 안전하게 설계되어 있지 않다. 기술적인 수단에 의해 달성되는 보호는 제한적이며, 적절한 관리와 절차에 의해 지원되어야만 한다. 정보보안에 대한 인증이 필요한 조직들의 요청에 의해 지난 1998년 2월 15일 제정된 정보보호 경영시스템 인증규격인 BS7799는 정보보호를 위한 유일한 국가표준으로 최상의 실행을 위한 포괄적인 일련의 관리 방법에 대해 요건별로 해석해 놓은 규격이다. 향후 ISO 17799로 발전하여, ISO/IEC JTC1/SC27에 Working Group이 구성되어 활동하고 있다.

국내의 정보보호관리 관련 표준화 활동은 1992년 SC27의 국내위원회가 기술표준원 산하에 구성되면서 시작되었으며, 현재에는 정보통신부장관이 인증하는 정보보호 경영시스템 인증제도를 도입하고자 BS7799를 기반으로 연구하고 있다. 이에 따라 지난 5월 1일부터는 "정보보호관리체계 인증제도"가 시행되었고 금융권과 증권, 보험사 등을 중심으로 정보보호 인증제도에 대한 관심이 높아가고 있다.

정보보호관리체계 인증제도는 정보통신 서비스 제공 업체와 이들에게 물리적 시설을 제공하는 업체들의 내부 정보보호관리체계 수준을 평가하고 인증해 주는 것이다. 이러한 인증을 받는다는 것은 정보보호관리를 제대로 하고 있다는 것을 국제적인 기관으로부터 인증받게 되는 것이므로 대외적인 신뢰도와 경쟁력을 제고할 수 있다.

본 논문에서는 정보보호관리체계의 표준화에 대한 국내외의 동향을 알아보고, 정보보호관리체계를 수립하고 인증받기 위한 과정을 전개함으로써 통신사업자를 비롯해서 인터넷 서비스 제공업체, 인터넷 데이터센터, 온라인 소프트웨어 임대업체, 정보통신 관련 서비스를 제공중인 금융권 등에 인증제도의 일반적인 적용을 유도하고 정보화의 역기능을 축소시키고자 한다.