[정보보호] 국제표준화기구에서 “정보보호 거버넌스 프레임워크” 표준화 동시 시작

정보보호 거버넌스의 필요성

기업 정보보호의 효과적인 구현을 위해서는 최고경영층의 정보보호에 대한 전략과 통제체계를 규정하고 있는 거버넌스 체계(Governance Process)를 구축할 필요가 있다. 현재 정보보호관리체계(Information Security Management System: ISMS)는 주로 정보보호를 실행하는 측면에서 계획, 구현, 평가 등 정보보호 담당자 또는 정보보호 관리자가 참조할 수 있는 프로세스를 제시하고 있다. 그러나 ISMS를 적절히 지휘 및 통제할 수 있는 체계, 즉 정보보호 거버넌스가 존재하지 않는다면 비즈니스와 정보보호와의 연계성 부족, 중복 또는 과소 투자 등으로 인해 ISMS의 효과성, 효율성이 저해될 가능성이 높다.

정보보호 거버넌스는 정보보호의 영역을 전통적인 기술적, 관리적 이슈에서 보다 전략적 차원으로 확대시키고 있다. 전통적으로 비즈니스 정보에 영향을 미치는 위험은 주로 정보기술(IT) 기반구조 관점에서 다루어져 왔다. 바로 이러한 관점이 IT가 중요한 비즈니스 정보자산의 저장, 처리, 전송에 관해 중요한 역할을 수행하게 된 주요 이유가 되었다. 따라서 정보보호는 단순히 기술적인 이슈로만 인식되어 왔으며, 최고경영층과 이사진들의 주의를 끌지 못했다. 그러나 정보보호는 단순히 기술적 이슈가 아니라, 전략적 이슈이면서 심지어는 법적인 문제일 수가 있다. 중역진과 이사진들의 위험관리 노력, 보고체계, 책임을 강조하는 기업 거버넌스(corporate governance)의 일부로서 정보보호를 취급하여야 함을 강조하고 있다. 따라서 정보보호 거버넌스는 “이사회를 포함하는 중역진들이 정보보호에 대한 지시와 통제를 어떻게 수행해야 하는가에 대한 프로세스”라고 정의 내릴 수 있다.

정보보호가 단순한 기술적 이슈가 아니고 전략적이고 법규적 이슈라는 점은 정보보호의 접근방식의 새로운 차원을 요구하게 되었으며, 조직의 기업 거버넌스 프로그램에 통합시켜야 하는 필요성을 제기시켰다. 기업 경영의 투명성과 책임성을 강조하기 위해 최근 기업 거버넌스 구축이 활발해지고 있는 상황에서 정보기술 거버넌스에 대한 이슈와 더불어 정보보호 거버넌스 체계 구축이 실무에서 새롭게 논의되고 있는 실정이다. Corporate Governance Task Force (2004)에서는 “정보보호로 가는 길은 기업 거버넌스를 통해 간다.”라고 언급하였다. 이는 기업 거버넌스 프로그램에 포함시키기 위해서는 정보보호가 내부통제에 일부로서 포함시켜야 되며 전략적 측면에서의 방향 설정 등이 필요함을 강조하고 있다.

정보보호 거버넌스 국제표준화 동향

최근 기업 거버넌스의 중요성이 점차 대두되고, IT 거버넌스가 국제표준 ISO 38500 (Corporate Governance on ICT)으로 발표됨에 따라, 정보보호 거버넌스에 대한 위상을 놓고 여러 가지 논란이 일고 있다. 즉 SC7에서 작업한 ISO 38500에서는 정보보호를 IT 보안적 관정에서 접근하고 있으며, IT 거버넌스의 일부로서 자리매김하고 있다. 이에 반해 SC

27에서는 정보보호는 IT 보안이 다루지 않는 Non-IT 자산(종이 문서, 이미지 등)에 대한 보호까지 포함하고 있으므로 IT 거버넌스와 공통된 부분도 있으나 별도의 영역을 취급하고 있다. 따라서, 정보보호 거버넌스는 기업 거버넌스의 핵심적인 일부분으로서 IT 거버넌스와의 연계성은 인정하되 별도의 영역으로 간주되어야 한다는 것이 SC27에서의 공통된 견해이다.

정보보호 관리에 대한 국제표준화 활동의 주역인 ISO/IEC JTC1 SC27 WG1에서는 내부에서의 요구와 JTC1에서의 요구에 의해 정보보호 거버넌스 국제표준화 작업이 2008년 4월 회의부터 논의되기 시작하였다. 2008년 10월, 사이프러스에서 개최된 37차 회의에서 한국은 정보보호 거버넌스 프레임워크에 대해 기고문을 제출하였고 본 회의에서 약간의 수정을 거쳐 SC27의 공식의견으로 채택되었다. 기고문의 내용은 정보보호 거버넌스의 필요성과 개념을 언급하였으며, 기업과 IT 거버넌스와의 관계 및 ISMS와의 관계를 기술하였고, 정보보호 거버넌스의 프레임워크를 제시하였다. 프레임워크는 정보보호 거버넌스의 3가지 목표(Accountability, Business Alignment, Compliance)를 제시하였고, 이에 기반을 둔 10가지 원칙을 제시하였다. 또한 거버넌스를 구현하기 위한 프로세스와 주요 중점분야를 제시하였다.

이 회의에서 “정보보호 거버넌스 프레임워크(information security governance framework)”를 새로운 표준화 항목으로 상정하였고 편집인(editor)으로 한국의 중앙대 김정덕 교수와 캐나다의 Charles Provencher를 선정하였다. 회의 이후 2개월에 걸친 투표 결과, 새로운 프로젝트(NP: New Project)로 결정되었다.

한편 ITU-T에서는 2008년부터 한국의 건의로 “정보통신기업을 위한 정보보호 거버넌스”를 차기 회기년도(2009-2012) 신규 표준화 아이템으로서 논의하기 시작하였다. 2009년 2월 제네바 회의에서는 한국에서 제안한 기고문을 심층 검토하였고, ISO와의 공통 프로젝트(Joint Project) 진행 가능성에 대해 많은 논의가 있었다. 결론적으로 공통 프로젝트가 되기 위해서는 동일한 문서로서 제시되어야 하기 때문에 문서명을 “정보보호 거버넌스 프레임워크”로 수정하였고 내용도 일반적인 정보보호 거버넌스 이슈만을 포함시켰다. 수정 기고문과 함께 ISO에 공통 프로젝트로 수행하자는 내용의 협조문(Liaison Document)을 보냈다. 이 작업의 편집인(editor)도 한국의 중앙대 김정덕 교수가 담당하기로 하였기 때문에, 두 표준화 기구에서 공통프로젝트로 진행하는 것에 대해 큰 문제가 없을 것으로 예상된다. 정보보호 거버넌스 프레임워크 국제표준화 작업은 2011년 말을 목표로 진행할 계획이다.

김정덕 (중앙대학교 정보시스템학과 교수, jdkimsac@cau.ac.kr)