‘ISMS 인증 의무대상 교육기관 확대’에 대한 우리의 입장

지난해 12월 1일 ‘정보통신망 이용촉진 및 정보보호 등에 관한 법률’의 개정과 후속조치로 올 6월 2일 시행된 동법 시행령에 따라 정보보호 관리체계(ISMS) 인증제도의 인증 신규 의무대상을 대학으로 확대한 것과 관련하여 아래의 이유들로 원점에서 재고하기를 간곡히 요청한다.

첫째, ISMS 인증을 획득하고 유지와 갱신을 위해선 많은 비용이 소요된다. 또한 의무대상기관이 인증을 받지 않을 경우 매년 과태료가 부과되는데 교육기관에 이러한 규제가 과연 온당한 것인지 묻지 않을 수 없다. 규모에 따라 차이가 있지만, 인증획득까지 종합대학의 경우 약 1~2억의 비용 소요, 매년 사후심사, 인증 3년차마다 갱신 심사를 받아야 하는 등 인증을 획득하고 유지하는데 큰 비용이 지불된다. 과태료는 기존 1000만원에서 3000만원으로 상향 조정되어 인증 미 획득에 따른 부담이 더 커진 상황이다. 대학의 열악한 재정상황에 이러한 비용 부담이 옳은 것인가? 대학에 ISMS 인증이 꼭 필요하다면 인증획득 및 유지에 필요한 모든 제반 비용을 100% 국가에서 부담하기 바란다. 그렇지 않다면 금번 법 개정은 반드시 원점에서 재고되어야만 할 것이다.

둘째, ISMS인증대상범위를 기존 영리목적의 정보통신서비스 제공자에서 비영리기관인 고등교육기관으로 확대시킨 것에 우려를 표명한다. 특히, 금번 법 개정에서는 (1) 2014년말부터 ISMS 인증 의무대상이었던 금융권을 ISMS 인증 의무 대상에서 제외하고 자율규제로 전환시켰으며 (2) 국가/사회적으로 아주 민감한 개인정보를 가장 많이 취급하는 국민건강보험공단, 국세청, 출입국사무국

등의 정부기관과 지자체 등의 공공기관은 ISMS인증 의무대상에 포함시키지 않았다. 개인정보가 대학에 더 많은가? 공공기관/금융기관에 더 많은가, 또한 개인정보 유출, 해킹사고 및 오남용 등의 사고가 대부분 어디에서 발생했었던가? 지난 2014년 1월 1억 400만 건의 카드사 개인정보 유출사고는 잊었단 말인가? 국민의 삶과 직결된 중요 개인정보를 가장 많이 취급하는 공공기관은 포함되지 않았고, 온갖 사고의 온상이 되어 온 금융권은 인증대상에서 제외시키면서, 굳이 대학을 시행령에 명시적으로 적시하면서까지 포함시킨 실질적인 이유는 무엇인가? 혹시라도 금융기관을 인증대상에서 제외시킴으로써 생긴 인증대상기관의 규모축소를 대학기관으로 충당하려는 의도는 없었는지 묻고 싶다.

대학의 ISMS인증 획득의 궁극적인 목적이 무엇인가? 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하도록 하기 위한 것이 이 인증의 목적이다. 대학은 이미 개인정보보호, 정보보안 관리체계 및 침해예방 활동 등을 진단하고 평가하는 '정보보호 수준진단'을 실시해 오고 있다. 또한 그 결과를 대학 알리미에 '정보공시'하고 대학평가에 반영하면서 정보보안에 최선을 다할 수밖에 없는 상황이다. 더욱이 대학이 포함된 공공기관에만 의무를 부과한 '개인정보 영향평가'도 충실히 이행하고 있지 않은가? 대학은 영리기관도 아니고, 빈번한 개인정보 유출 및 오남용 사고가 발생하는 기관이 아님에도 ISMS 인증의무대상에 포함시켜 막대한 재정적 부담을 갖게 한 것은 필요 이상의 규제를 적용한 것이다. 조속한 시일 내에 법의 재개정을 촉구하는 바이다.

2016. 6. 16.

(사단법인) 한국대학정보화협의회, 전국대학 IT 관리자협의회