

전문업체 선정 투명하고 공정해야

국가의 주요 정보통신 시설 보호 차원

과연 '정보보호전문업체'라는 명칭은 어느 업체에게 부여될 것인가? 드디어 전문업체 선정을 위한 실질적인 과정이 들어간다. 최근 정보통신부는 이러한 모든 절차를 끝내고 오는 9월 17일부터 22일까지 정보보호전문업체 신청을 접수받겠다고 발표했다. 2년여 동안 업계 및 전문가 공청회를 거쳐 결정된 이번 정보보호전문업체 선정 제도는 정보통신법 및 동법 시행규칙에 따라 주요정보통신기반시설에 대한 취약점 분석 및 보호대책수립 업무를 지원하는 정보보호컨설팅 분야의 전문능력과 안전·신뢰성이 있는 민간기업을 정보보호전문업체로 지정하는데 그 목적이 있다. 또한 정보보호전문업체 명칭은 업계 건의에 따라 영문으로는 컨설팅을 명시하는 Information Security Consulting Service Provider for Information Infrastructure로 명칭한다.

기본 방침은 지정기준을 사전에 공개하고 지정기준을 충족하는 모든 업체는 정보보호전문업체로 지정하는 절대평가 방식으로 추진한다. 다만, 지정기준을 모법의 취지와 국내 정보보호산업의 여건, 주요정보통신기반시설의 수 및 전문업체 자체의 보호대책 측면을 종합적으로 고려하여 합리적으로 설정한다는 것이다.

계량평가 비중 높여...투명성 고려

또한 비계량 요소를 최대한으로 줄이고 계량평가의 비중을 높임으로써 지정심사과정에서의 투명성과 객관성을 제고시키고, 지정신청업체의 자체 보호대책에 대한 현장실사를 강화하여 부적격업체의 진입을 사전에 차단할 방침이다. 지정심사와 관련된 일체의 정보는 비공개를 원칙으로 하되, 미지정된 업체의 요구가 있는 경우는 당해 미지정사유에 관한 정보를 개별적으로 통지하기로 했다.

관계법령으로는 정보통신기반보호법 제9조제3항에 의해 주요정보통신기반시설에 대한 취약점 분석·평가기관으로 한국정보보호진흥원, 정보공유·분석센터 등과 함께 정보보호전문업체를 규정하고 있으며, 제17조부터 제23조까지 1장 7개조를 할애하여 정보보호전문업체의 지정, 결격사유, 양도·합병, 지정

취소, 자료의 제출, 자료의 보존·폐기 등에 관한 사항을 규정하고 있다. 정보통신기반보호법 시행령 제18조 제3항에는 취약점 분석업무를 수탁 받은 기관은 이를 자기책임으로 직접 수행하도록 하게 명시하고 있다. 정보통신기반보호법 시행규칙은 상위법령의 위임에 따라 정보보호전문업체의 지정기준·절차·방법 등에 관한 사항과 제재처분의 기준 등을 정하고 있다.

정보보호전문업체의 지정심사에 관한 고시에서는 시행규칙의 위임을 받아 제출서류의 서식, 업무수행능력심사의 세부평가기준, 정보보호관리규정의 주요내용 등 정보보호전문업체의 지정심사에 필요한 세부사항을 규정하고 있다.

지정기준...15명, 20억 등

지정기준 및 절차로는 인력요건에 관해 고급인력 5인이상을 포함하여 기술인력 15인이상으로 명시되어 있다. 이는 컨설팅 프로젝트 4~5개를 동시에 수행할 수 있는 규모의 인력으로서 고급기술인력이란 과제책임자급(project manager)의 학력·자격·경력을 갖춘 기술인력을 말한다.

자본요건에 관해서는 납입자본금이 20억원 이상으로 정보보호전문업체는 주요정보통신기반시설에 대한 취약점분석정보라는 극히 민감한 정보를 취급하므로 입법취지에 따라 업체 자체의 안전·신뢰성이 확보되어야 하기 때문이다.

설비요건은 신원확인 및 출입통제설비, 업무수행 및 지원설비, 기록·자료의 안전관리설비를 갖추어야 하며, 능력요건으로 업무수행능력심사에서 정통부장관이 정하는 기준점수 이상을 취득해야 한다. 업무수행능력평가는 경험, 전문화, 신뢰도, 기술개발실적 분야의 계량평가항목 70점과 비계량평가항목인 기술심의위원회의 종합심사 30점으로 구성되어 있다.

정보보호요건으로는 업무수행구역 및 설비에 대한 보호대책, 인원에 대한 보호대책(교육훈련 및 인사관리)에 관한 사항을 포함한다. 문서 및 전산자료에 대한 보호대책 등을 갖추어야 한다. 전문업체 지정신청 공고는 시행규칙인 제4조에 의해 정보통신부장관은 정보통신기반보호법 제17조의 규정에 의하여 정보

보호전문업체를 지정할 필요가 있는 때에는 미리 신청접수기간과 신청요령 등을 정하여 20일 이상 관보에 공고해야 한다고 명시하고 있다. 공고의 내용은 접수처, 접수방법, 제출서류의 종류, 제출서류의 미반환, 속임수 기타 부정한 방법으로 지정을 받은 때의 제재 등의 신청서 유의사항이 공고된다.

공고의 시기 및 방법은 신청접수 개시일 20일 이전에 공고하여야 하므로 지난 8월 18일부터 28일 사이에 관보에 게재했다.

9월 17일부터 22일까지 접수

지정신청의 접수 기간은 오는 9월 17일부터 22일까지이며, 접수 방법은 정보통신부 정보보호산업과에 제출서류를 구비하여 인편으로 직접 접수해야 한다. 제출서류의 검토는 시행규칙 제5호각호의 규정에 따른 제출서류가 미비되거나 기재사항이 누락된 경우에는 일정한 기간을 정하여 이를 보완할 수 있게 한다.

서류 심사는 임원등이 법 제18조의 규정에 의한 결격사유에 해당하는지 여부를 '신원조회' 등을 통해 확인하고, 법 제17조 제2항의 규정에 따라 '법인격유무'를 확인하게 된다.

지정기준상의 인력·설비·자본요건 충족여부, 업무수행능력 심사 계량평가항목의 점수 및 정보보호관리규정의 적정여부를 제출서류를 통해 확인하고, 서류심사중 현장실사를 통하여 재확인이 필요한 사항이 발생하면 '실사필요사항'으로 정리하여 현장실사시 확인하게 된다. 고급기술인력의 자격확인, 컨설팅수행 실적의 사실확인 등 전문적인 의견이 필요한 경우에는 기술심의 위원회를 활용하며, 서류심사를 위한 조직으로는 정보보호산업과장을 반장으로 하는 5인내외의 지정심사반을 구성하게 된다.

현장 실사는 시행규칙 제7조제1항제5호 및 고시 별표3에 의거 정보보호관리규정의 적정성과 그 실효적 준수여부를 현장에서 확인한다. 실사 방법은 실사 착수전에 실사의 목적과 인적사항을 교부하고, 실사 과정에서 특이사항, 문제점 등이 발생하는 경우 '사실확인서'의 작성을 원칙으로 한다. 실사결과 처리로 현장실사반은 만장일치의 방법으로 실사의견을 적합, 부적합, 재실사로 정리하고 최종적으로 '부적합의견'이 제출된 경우에는 지정기준 미충족으로 탈락처리를 하게 된다.

현장실사를 위한 조직구성은 학계·연구기관·유관단체 전문가가 7~9인 내외로 구성되는 현장실사반에서 담당하게 된다.

학계·연구기관·유관단체 전문가로 구성

종합 심사는 기술책임자의 자질과 경험(5점), 정보보호대책(5

점), 정보보호컨설팅방법론(15점), 정보보호전문지식(5점)을 평가하게 되며, 심사 방법은 원칙적으로 지정신청업체의 프리젠테이션 후 질의응답을 진행하는 방식으로 심사한다. 이 때 발표자료의 구성, 제출시기, 발표자수, 발표방법, 종합심사일정 등에 관한 사항을 수록한 '종합심사준비요령'을 심사전에 미리 배포할 계획에 있다.

종합심사를 위한 조직 구성으로는 기술심의위원회 및 종합심사에 관한 사항은 지정신청업체의 수가 얼마인지에 따라 가변적 이므로 오는 9월중 별도의 계획을 수립·시행 할 계획이다.

심사결과와 검증은 서류심사, 현장심사, 종합심사를 모두 마치면 제출서류, 현장실사자료, 종합심사자료 등 지정심사와 관련된 일체의 자료를 재검토후 신청업체별로 편철하여 관리하며, 신원조사의 대상이 되는 지정예정업체를 확정한다.

지정서 교부는 신원조사결과 아무런 하자가 없는 경우에는 지정예정업체에 정보보호전문업체 지정서를 교부한다. 신원조사의 회보결과, 당해기술인력이 시행규칙 별표 1에서 정하는 기술인력으로 인정받지 못하는 경우에는 정보통신부장관이 정하는 일정기간동안 당해 인력과 동급의 기술인력을 추가 확보할 때까지 정보보호전문업체의 지정을 유보하게 된다.

다만, 이 경우에도 신뢰보호(信賴保護)의 원칙상 지정예정업체로의 지위에는 변동이 없는 것으로 한다.

미지정사유의 공개에 관해서는 지정심사와 관련된 정보는 법률에 다른 규정이 있지 않은 한 원칙적으로 비공개할 방침이나, 탈락업체의 요청이 있는 경우에는 당해 미지정사유에 관한 정보를 개별적으로 통지할 방침이다.

현재 정보보호전문업체를 준비하고 있는 대부분의 보안 컨설팅 업체는 기준안을 마련하기 위해 고심중에 있다. 몇몇 보안 컨설팅 업체의 사장에 의하면 "겉으로는 많은 기업들이 기준안을 통과할 것이라고 장담하지만, 실제로는 그러하지 못할 것"이라고 말하고 있다.

또 어느 한 업체의 사장은 "정확하게는 모르겠지만, 정보보호전문업체는 보안벤처업체에서 7~8개업체, 그리고 SI업체에서 2~3개, 국가기관에서 2~3개 정도로 총 12개 업체에서 15개업체 정도가 처음에 선정되지 않겠냐"고 예상하고 있다.

이젠 실질적인 정보보호전문업체를 선정하는 것만이 남은 것이다. 그러나 지금까지 해왔던 부분보다 가장 중요한 부분이 선정 과정일 것이다. 투명하고, 공익적인 차원에서 전문업체를 선정하여 국가의 주요 정보통신시설을 보호해야 할 것이다. ☞