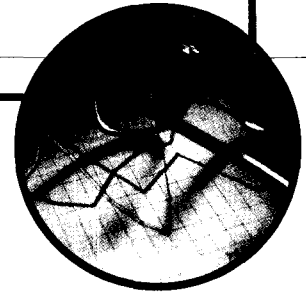


정보보호전문업체 지정에 즈음하여

About the Designation of Privacy and Information Protection Firm



글 / 申 勳

(Shin, Hoon)

정보관리기술사, (주)금호엔지니어링 대표이사,
분회 이사, 정보처리부문회장.

E-mail: hshin@kumhoeng.co.kr

2001년 7월을 기하여 정보통신기반보호법이 발효되고 통신, 전력, 상수도, 공항, 철도, 정부주요 시설, 제1금융권 등 국가 주요 정보통신 기반시설에 대해서 정보보호 감리가 의무화된다. 미국의 경우도 유럽의 강화된 정보보호지침에 대응하기 위해 2003년 발효 예정인 세이프하버법에 대응하기 위한 각 기관, 단체, 기업들의 노력이 가시화되고 있다. 전세계의 정보보호 관련법이 각 자 국가의 이익을 중심으로 제정 중인 시점에서 기술 분야의 전문가들이 좀 더 국가의 이익과 공공의 안녕에 부응하는 대응책을 마련하여 국익에 도움이 되는 방향으로 법, 제도가 운용될 수 있도록 관련법을 숙지해야 할 때이다. 그리고 전체 기술사들이 한마음으로 정치, 경제, 학술 등 각자 맡은 분야에서 분발할 것을 촉구한다.

1. 제도배경

- 정보통신기반보호법의 7월 1일 발효에 따라 지정되는 국가주요정보통신기반시설의 정보 보호 업무를 전문능력과 신뢰성을 갖춘 민간 업체에 위탁, 대행할 수 있도록 하는 제도.

As of July 1, 2001, the Law of Information & Telecommunication Protection has been compulsory to audit protection status on national information and Telecommunications infra facilities such as communication, electricity, waterworks, airport, railway, primary facilities of government and the first financial circles. In U.S. institutions, organizations and corporations in each field are trying to prepare for Safe Harbor agreed on Internet privacy regulation between U.S. and Europe to be effective in 2003. The Safe Harbor was motivated by strict European standard. Other countries make privacy and information protection law according to their own interest. Therefore Korean technical experts have to develop the law responding to national interest and public welfare. Besides scientific field, experts in the field of politic, economy and academy also have to work hard to develop the law.

- 정보통신기반보호법이란?

- 해킹 등의 전자적 침해행위로부터 국가기반 시설을 보호하기 위하여 우선적으로
- 공공시설물(통신, 전력, 상수도, 공항, 철도 등), 정부중앙부처, 제1금융권 등의 국가기반 시설을 선정하고,
- 종합적 정보보호대책을 의무적으로 시행하도록 강제함과 동시에 정보보호센터 및 민간 정보보호전문업체로 하여금 최소 연간 1회 이상의 취약점 분석 및 평가, 컨설팅 업무를 수행케 함.

- 즉, 정보보호전문업체로 지정 받은 업체만이 국가기반시설을 대상으로 정보보호 분야의 취약점 분석, 평가 등의 컨설팅업무를 수행할 수 있게 됨.

2. 경 과

- 2000년 12월부터 정보통신부 정보보호산업과 주관으로 주요보안업체로 구성된 업체연구반을 운영하여 왔으며, 2001년 4월 4일 최종 공청회를 거쳐 시행세부안이 확정됨.
- 전문업체 선정을 위한 향후 시행일정은
 - '01년 7월 : 정보통신기반보호법 발효
 - '01년 9월 : 전문업체 지정신청 접수 및 실사 실시
 - '01년 11월 : 전문업체 지정완료
- 지정을 위한 기본방침으로서는
 - 지정요건으로서 자본, 시설, 인력 등의 **일반요건**과 업무수행능력, 컨설팅방법론, 과거실적 등의 **능력요건**으로 구분
 - 지정절차로서 사전서류심사, 현장실사, 기술위원회심사의 단계를 거치고, 기술위원회에서 컨설팅 방법론, 기술책임자 능력 등을 비계량평가
 - 기술위원회는 관계기관, 학계 등에서 70~100명의 전문가 인력 Pool을 구성토록 하나 KISIA 회원사 임직원은 대상에서 제외됨.

3. 산업계에 미치는 영향

- 정보보호는 이제 정보시대의 필수 인프라로 자리잡고 있으며 공공의 안녕에 지대한 영향을 미치게 되므로 그 중요성에 있어서 기술사를 비롯한 공인 전문가의 적극적인 참여가 절실함.
- 컨설팅 사업부문
 - 현재 발표된 국가기반시설 지정범위(공공, 정부중앙부처, 금융, 에너지, 통신)에 따라 국가

기반시설로 지정될 대상은 대략 150~ 200개소가 될 것으로 보임.

- 전체 지정 시설의 40%를 KISA, ETRI에서 담당하더라도 **100여 개의 시설은 민간 전문업체가 담당하게 될 것으로 예상.**
- 현재 소형컨설팅업체의 여건을 고려할 때, 지정이 가능한 업체는 최대 15개 미만일 것으로 예상되고, 각 업체의 업무능력으로는 연간 5, 6개 이상의 컨설팅 수행은 어려울 것으로 판단.
- 공공/금융 SI사업부문
 - 최근 금융 IT심사에서도 보안부문이 크게 대두되고 있고, 특히 공공부문에서는 보안전문 인력의 시스템개발 참여를 요구하고 있음. 시스템 보안컨설팅과 개발이 협력하여 프로젝트를 수주하는 형태가 예상됨.

구분	관련정책	정보보호정책
국제상공회의소	ICC모델	- 정보주체나 감독기관이 정보침해문제에 대해 정보수출입업자에게 배상을 요구할 수 있는 권리부여(사전인증서)
OECD	소비자보호 가이드라인	- 수집제한의원칙, 정보내용정확성(&목적성)의원칙, 정보수집목적명확화의원칙, 이용제한의원칙, 안전성확보의원칙, 공개의원칙, 개인참가의원칙, 책임의원칙
유럽연합	정보보호지침	- 원칙과기본규칙, 기술적조적조치, 독립감독기구, 3국으로의 정보전송, 적절한 보호수준과 원칙(합목적성 등)
미국	세이프하버원칙	- 고지선택, 제3자제공, 안전성, 무결성, 접근, 법집행, (자율규제, 유럽정보보호원칙에 동참한 신고제외무화)
일본	정보보호 가이드라인	- 정보관리체계, 교육 및 연수, 정보보호감사, 상담창구공개, 보호안전조치, 정보유통안전체계

- 국제거래시 개인정보 보호 규제 심화 예상
 - 인터넷을 이용한 국제거래를 추진하기 위해서는 해당국의 정보보호 관련 규제 및 국제적인 보안표준에 대한 사전지식이 필요하며 특히 금번에 시행되는 정보보호관련 각종 지침을

기 획 특 집

준수하는 것이 사업수행의 필수요건으로 자리 잡게 될 것으로 적극적인 대응이 필요.
 미국의 경우도 2003년 시행 예정인 개인정보 보호법의 발효를 앞두고 금융산업을 필두로 보안솔루션 도입에 적극적으로 대응하고 있음.

4. 전문업체 지정기준(案) ('01년 6월 현재)

4.1. 전문업체 지정 절차

1. 지정신청 접수 및 제출서류의 보완
2. 서류심사 (계량평가)
 - ① 경험 ② 전문화정도
 - ③ 신뢰도 ④ 기술개발실적
 - ⑤ 기타항목 심사
3. 현장실사
 - 서류심사 항목의 실제 이행, 준비여부 점검
4. 기술심의위원회 종합심사 (비계량 평가, 60점 이하 과락)
 - 기술책임자 자질/경험, 정보보호컨설팅 방법론, 전문지식 평가, 프레젠테이션
5. 심사결과에의 검증/확정과 신원조사

4.2. 일반요건

기준항목	기준치	상세내역	비고
납입자본금	20억 이상	-	- 영세업체 배제
기술인력	10인 이상	- 학사학위이상 소지자 - 기사 자격 소지자 - 최근 3년, 2건 이상 보안 컨설팅 경력자	- 정규직원 한정 - 해당 기술인력은 별도 신원관리
고급기술인력	5인 이상	- 박사학위, 기술사, CISA, CISSP + 경력2년 이상 - 석사학위, 경력5년 이상 - 학사학위, 경력6년 이상 - 최근 3년간 1억 이상, 2건 이상의 PJT PM	- 해당 컨설팅수행 인력은 별도의 사업부로 관리

기준항목	기준치	상세내역	비고
업무수행공간	7인 이상 격리공간	- 시설 및 장비요건을 만족하는 별도 구역	-
시설및장비	출입통제 업무지원 안전설비	- 신원확인 및 출입통제 - NW장비, 취약점분석도구 - 문서세단기, 문서보관함	- 보안관계센터
정보보호관리 규정	조직관리 업무관리 교육관리 기록관리 보안감사 협력업체	- 보안조직 및 역할 - 보안업무 관리 - 채용, 전보, 퇴직자 관리 - 비밀 서약서 - 문서 및 자료의 반출입, 폐기 및 기타 절차	-

4.3. 업무수행능력 평가(100점) 및 현장실사

평가항목	상 세 내 역	비 고
1. 경험 (30)	- 최근 3년간 정보보호컨설팅 수행실적 (25) - 최근 3년간 계약금 1억원 이상의 정보보호컨설팅 수행실적 (5)	- 견수, 금액 - 견수
2. 전문화정도 (20)	- 고급기술인력의 수 (8) - 고급기술인력의 평균재직기간 (5) - 기술인력중 특수경력자의 수 (5) - 정보보호분야 정부과제수행실적(2)	
3. 신뢰도 (15)	- 부채비율, 자기자본이익률 (9) - 추천서의 수 (3) - 상훈실적 (3)	
4. 기술개발실적 (5)	- 정보보호분야 특허보유, 소프트웨어 등록실적 (5)	
5. 기술심의위 위원회 종합 심사(30)	- 기술책임자의 자질과 경험 (3) - 정보보호컨설팅 방법론 (15) - 분야별 정보보호 전문지식 (12)	- 우수미양 가로 평가
6. 기타 (가점)	- 벤처기업육성에관한특별조치법에 근거 벤처기업으로 확인을 받은 기업 (가점) - 최근 3년간 관례법령에 따라 정당업자로 지정되어 입찰참가 제한을 받은 개월수(감점)	

(원고 접수일 2001년 7월 10일)