

정보보호시스템 평가 및 인증기관의 도입 및 법적 과제

張 校 湜

(建國大學校 法科大學 助敎授)

< 目 次 >

I. 서론	IV. 인정기관의 도입 필요성 및 법제도의 개선방안
II. 인정기관에 대한 입법례	1. 인정기관의 도입 필요성
1. CCRA의 요구사항	2. 인정기관의 도입방안
2. 외국의 입법례	3. 인정기관 도입방안에 대한 검토
III. 평가기관의 도입필요성 및 법제도의 개선방안	V. 결론
1. 평가기관에 관한 현행법률의 검토	參考文獻
2. 개선방안에 대한 검토	SUMMARY

I. 서론

인터넷을 중심으로 한 정보통신기술의 발전은 우리의 일상생활에 많은 편리함을 주고 있으나, 그에 따른 부작용도 만만치 않게 등장하고 있다. 특히 해킹 등 정보침해행위는 커다란 사회 문제로 등장하고 있으며, 각 국은 이를 막기 위해 정보보호시스템의 개발을 위한 노력을 경주하고 있는 상황이다.

미국을 비롯한 유럽의 국가들은 오래 전부터 나름대로 기준을 정하여 효과적인 정보보호시스템의 구축을 위한 평가 및 인증제도를 마련하고 있다. 뿐만 아니라 이들 국가들은 공통된 평가 기준을 통해 평가·인증된 제품에 대해 각국이 상호승인하기 위한 협약인 CCRA(Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security)를 체결하고 있다. 동 협약은 참가국이 갖고 있는 평가·인증제도에 의해 인증된 IT제품에 대해서는 다른 참가국 스스로에 의해 평가·인증된 것과 동등하게 취급하는데 동의하는 것이다. 따라서 동 협약에 가입한 국가는 자국에서 생산한 IT제품에 대해 공통평가기준에 기초

하여 평가·인증하였다면 수출상대국의 제도에 의해 재평가·인증 받지 않아도 됨에 따라 평가비용의 절약 및 평가기간의 소요에 따른 기회상실을 방지할 수 있는 등 많은 이점을 가질 수 있게 되었다.

이미 IT기술의 수준 및 사용량이 세계적인 수준에 이르고 있는 우리나라의 경우도 효과적인 정보보호시스템의 구축이 절실히 요구되고 있으며, 이를 위한 법제도적인 정비가 요구되고 있는 상황이며, 또한 우리나라의 IT제품이 국제경쟁력을 갖기 위해서는 CCRA에 가입도 절실히 필요한 시기이다.

CCRA에 가입하기 위해서는 CCRA에서 요구하고 있는 평가기준·방법 및 평가기관, 인증기관, 인정기관 등 참여기관의 조직 및 운용에 관한 기준을 철저히 준수하여야 한다. 이미 CCRA에 가입한 국가들은 나름대로 차이점은 있으나 이러한 CCRA 기준에 부합하는 조직체계를 갖추기 위한 법제도적인 기반을 갖추고 있다.

따라서 우리나라의 경우도 효과적인 정보보호시스템에 대한 평가·인증제도를 갖추고 CCRA에 가입하기 위해서는 CCRA에서 요구하는 평가·인증 제도 및 조직체계를 갖추어야 하며, 이를 위해서는 후발주자의 장점을 최대한 살려 CCRA 가입국들의 제도와 조직에 관한 법체제에 대한 분석을 통해 가장 효과적이고 우리의 현실에 부합하는 제도 및 조직체계를 찾는 작업이 선행되어야 할 것으로 생각된다.

이를 위해서는 평가 및 인증제도와 관련된 인증기관, 평가기관 및 인정기관에 대한 법적정비가 이루어져야 할 것이나 본 논문에서는 세계적인 추세인 민간평가기관의 도입과 관련한 인정기관의 도입 필요성 및 법제도의 정비방안을 중심으로 살펴보고자 한다.

II. 인정기관에 대한 입법례

1. CCRA의 요구사항

1) 평가기준인 CC의 성립

정보보호(security) 평가·인증제도는 미국 및 유럽에서 주로 군 및 정부조달 물품의 평가를 위한 제도로서 시작되었다. 각 국은 나름의 평가기준을 마련하여 군 및 정부에서 사용할 컴퓨터 관련제품의 security를 확보하고자 하였던 것이다.

미국은 1983년에 국방성산하의 NSA(National Security Agency)내의 NCSC(National Computer Security Center)가 군용물품의 조달을 위한 컴퓨터 부품 평가기준으로서 1983년에 TCSEC(Trusted Computer System Evaluation Criteria)을 작성하였다. 또한 1991년에는 영국,

독일, 프랑스 및 네덜란드가 공동으로 통일 평가기준인 ITSEC(Information Technology Security Evaluation Criteria)을 작성하였다.¹⁾

그후 미국을 중심으로 TCSEC와 ITSEC을 통합한 새로운 평가기준의 마련을 위한 노력이 시작되었으며, 1993년 미국, 영국 등 6개국 7개 조직²⁾의 대표자들의 합의로 새로운 통일기준으로서 CC(Common Criteria)를 마련하기 위한 소위 CC프로젝트가 시작되었다. CC프로젝트에 의해 마련된 새로운 평가기준인 CC는 1999년 6월에 국제규격(ISO/IEC 15408)으로 승인되었으며, 오늘날 통상 CC로 통칭되는 평가기준은 구체적으로 ISO/IEC 15408을 의미하고 있다.

2) CCRA의 성립

CC프로젝트의 중요한 목표중 하나는 공통된 평가기준인 CC에 의해 평가·인증된 제품에 대해 각국이 상호승인하는 것을 가능하게 하는 것이었다. 이러한 목적으로 위해 형성된 협약이 바로 CCRA(Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security)이다. 동 협약은 참가국이 갖고 있는 평가·인증제도에 의해 인증된 IT제품에 대해서는 다른 참가국 스스로에 의해 평가·인증된 것과 동등하게 취급하는데 동의하는 것이다. 따라서 동 협약에 가입한 국가는 자국에서 생산한 IT제품에 대해 CC에 기초하여 평가·인증하였다면 수출상대국의 체도에 의해 재평가·인증 받지 않아도 됨에 따라 평가비용의 절약 및 평가기간의 소요에 따른 기회상실을 방지할 수 있는 등 많은 이점을 가질 수 있게 되었다.

3) CCRA의 참가요건

이처럼 동 협약에 참가한 국가간의 평가·인증에 대해 상호승인이 계속적으로 가능하도록 하기 위해서 동 협약에 참가하기 위한 요건을 엄격하게 정하고 있다.

동 협약에 참가하고자 하는 국가는 ① 평가기준이 공통평가기준인 CC, 즉 ISO/IEC 15408을 기초로 할 것 ②평가방법이 공통평가방법인 CEM(Common Methodology for Information Technology Security Evaluation)을 사용할 것 ③평가기관의 조직, 운용 및 평가활동에 대한 요구사항인 ISO/IEC 17025를 준수할 것 ④인증기관의 조직, 운용 및 인증활동에 대한 요구사항인 ISO/IEC Guide 65를 준수할 것 ⑤CC인증서 및 인증보고서가 CCRA에서 정한 목적을 달성하고 있을 것 등을 요구하고 있다.

아울러 평가기관과 관련하여 평가기관의 설립은 법률에 의하거나 인정기관의 인정절차를 통

1) NIAP, Historical Perspective(Mar. 2003) <<http://www.niap.nist.gov/cc-scheme/historical-perspective.html>> .

2) 참가단체는 미국의 NSA와 NIST, 캐나다의 CSE, 영국의 CESG, 독일의 BSI, 프랑스의 DCSSI, 네덜란드의 NLNCSA이다.

해 설립할 것을 정하고 있다. 따라서 법률에 의해 설립되는 국가 평가기관이 아닌 민간평가기관의 경우에는 반드시 인정기관에 의해 인정을 얻어야 한다.

2. 외국의 입법례

CCRA 가입국인 미국, 영국, 일본³⁾의 경우에는 최근 민간평가기관을 적극적으로 활용하고 있으며, 이를 위해 인정기관에 관한 법제도를 정비하고 있다. 이하에서는 각국의 법제에 대해서 구체적으로 살펴보기로 한다.

1) 미국

Computer Security Act on 1987'은 NSA 및 NIST에게 컴퓨터시스템의 정보보호에 대한 가이드라인을 정하고 실행할 것을 정하고 있다. 이에 근거하여 NSA는 주로 군수품 등 정부조달 물품에 대해 정보보호시스템에 대해 평가하는 임무를 수행하여 왔으며, 국가 표준체계의 확립을 목적으로 하는 NIST는 주로 민수품에 대한 평가를 실행하여 왔다.

그 후 미국정부는 두 기관의 축적된 기술을 이용하여 보안성 높은 제품의 사용을 보장하고, 아울러 이러한 과정에서 정보통신기술에 있어서 정부부문과 민간부문의 긴밀한 협조를 도모하기 위한 노력의 일환으로 NIAP를 설립하게 된다.⁴⁾

NIAP은 평가 및 인증에 대한 새로운 스킴으로서 CCEVS를 제정하였으며, 동 스킴은 평가기준으로서 기존의 TCSEC가 아닌 CC를 채택하고 있다. CCEVS는 NIAP에 의해 운영되는 평가 및 인증제도에 대한 기본 지침으로서 인증기관, 평가기관 및 인정기관의 설립과 그 역할 및 책임 등에 대해서는 'Scheme Publication #1'에서 규정하고 있다.⁵⁾ 동 제도는 NIAP의 내부규정에 의해 규율되고 있으며, 민간 평가기관의 육성을 위한 노력의 연장선상에서 이루어진 것이다.

NIAP의 내부규정들은 CC 및 CEM에 근거한 민간기관의 평가와, 이에 대한 NIAP 산하의 인증기관(Validation body)의 인증을 중심내용으로 하고 있다. 아울러 평가기관은 인정기관인 NVLAP(NIST's Voluntary Laboratory Accreditation Program)에 의해 인정을 받고 인증기관의 승인을 얻어야 한다. 이렇게 승인을 얻은 평가기관을 CCTL(Common Criteria Testing Laboratory)라 한다.

인정기관은 평가기관이 CCEVS에서 요구하는 조건에 부합하는 조직 및 운영을 행하는지에

3) 일본의 경우에는 CCRA 가입을 위한 법제도의 정비를 통한 준비기간을 거쳐 2003년에 CCRA에 가입하였다.

4) 이에 대한 설명은 NIAP 홈페이지(<http://www.nist.gov>)참조.

5) CCEVS에 대한 NIAP의 문서는 총 6가지가 있는데, 그 중 조직 및 운영의 기본원칙에 대한 규정은 'NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Scheme Publication #1 Organization, Management, and Concept of Operations(이하 'Scheme Publication #1으로 인용함)'에서 상세히 규정하고 있다. 이하에서는 동 문서의 내용을 바탕으로 각 기관에 대해 살펴보기로 한다.

대해 조사·인정하는 프로그램을 의미한다. 인정기관은 ISO/IEC 17025 및 Guide 58의 규정에 따라 조직되어야 하며, 아울러 인정프로그램의 경우에는 ISO/IEC Guide 25의 규정에 따라 운영되어야 한다.

인정기관은 평가기관에 대해서 상술한 NIST Handbook 150 및 NIST Handbook 150-20를 기준으로 평가를 행하며, 필요한 경우 평가기관의 평가수행 능력을 직접 테스트하여 평가수행 능력을 평가할 수 있다.

평가기관이 NVLAP에 의해 평가기관으로서 인정을 얻고자 하는 경우에는 반드시 그 범위를 특정하여 신청하여야 하며, 이 경우 NVLAP은 당해 범위에 대해 심사를 하고 그 범위에 한해서 인정을 할 수 있다.

따라서 이미 승인을 얻은 평가기관이라 할지라도 그 범위를 달리하여 신청하는 경우에는 NVLAP은 신청 분야에 대해서 심사를 행하고 이에 대한 인정여부를 결정하여야 한다.

2) 영국

영국의 평가 및 인증제도는 1991년 통산성(the Department of Trade and Industry)과 CESG(Communication-Electronics Security Group)의 공동노력으로 형성되었다. 평가 및 인증 제도는 CESG에 소속된 인증기관(The UK IT Security, Evaluation and Certification Body)이 운영하도록 되어 있으며, 인증기관의 운영은 통산성과 CESG가 공동으로 운영하고 있다.

이에 따라 인증기관은 평가 및 인증제도에 대한 기본지침을 제정하고 있다. 동 지침의 명칭은 'UK Scheme Publication No.1 Description of the Scheme(이하 인증 및 평가지침)'으로 인증기관과 평가기관 및 인정기관에 대한 상세한 내용을 정하고 있다.

또한 인정기관의 경우는 통산성과 양해각서를 체결하여 인정기관으로서 인정받고 있는데, 동 문서에는 정부의 지원 및 감독과 인정기관의 역할과 의무에 대해서 정하고 있다. 인증기관은 비영리민간조직으로서 통산성과의 양해각서를 통해 영국유일의 인증에 관한 국가기관으로서 인정되고 있다. 통산성은 인정기관에 대해 적절한 지원을 강구해야 하며, 적절한 조직을 갖추도록 하여야 한다. 인정기관의 운영예산은 수수료 수입에 의해 자체적으로 해결하여야 하나, 인정기관이 정보정책에 따라 새로운 서비스를 행하고 이를 통해 수입이 보장되지 않는 경우에는 적절하게 예산지원을 하는 것이 가능하다.

인정기관의 활동에는 정부대표가 참여할 수 있으며, 정부는 인정에 관한 정부정책의 변화에 대해서 인정기관에 통보하여야 한다. 또한 인정기관은 인정업무와 관련하여 통산성 및 다른 정부부처에 합리적으로 조력해야 할 의무도 있으며, 정책과 관련한 문제가 있는 경우 해당 자문위

6) 정식명칭은 'Memorandum of Understanding Between the Secretary of State for Trade Industry and the United Kingdom Accreditation Service' 이다.

원회에 정부의 참여를 요구할 수 있다.

아울러 인정기관은 영국의 인정시스템의 우수성을 국제적으로 알리는데 최선의 노력을 해야 하며, 영국의 시스템이 국제기준에 적합하게 개선될 수 있도록 노력해야 한다. 또한 인정업무를 수행함에 있어 영국의 단일 인정기관으로서 투명하고 공명정대하게 업무를 수행해 하며 합리적인 기준과 원칙을 가지고 제도를 운영해야 한다.

3) 일본

일본의 평가 및 인증제도의 주체는 NITE이다. NITE는 '獨立行政法人通則法'에 의해 설립된 독립행정법인으로서 그 업무 및 역할에 대해서는 '獨立行政法人製品評價技術基盤機構法(이하 NITE법)'에서 정하고 있다. NITE법은 인증 및 평가업무를 NITE의 업무범위로 규정하고 있으며, 그 구체적인 내용에 대해서는 NITE 자체적으로 정하도록 위임하고 있다. 이에 따라 NITE는 인증 및 평가제도의 기본 지침에 해당하는 'IT시큐리티 평가 및 인증제도'⁷⁾를 통해 동 제도에 대해 규율하고 있다.⁸⁾

동 지침은 인증기관의 설립 및 운영과 그 책임에 대해서 정하고 있으며, 평가기관에 대한 내용의 설립 등에 대한 구체적인 내용을 정하고 있다. 또한 인정기관에 대해서는 별도로 정하고 있으며, 그 내용은 동 지침의 참고자료에서 정하고 있다.

인정기관으로부터의 인정을 희망하는 평가기관이 인정을 받기 위해 필요한 절차, 인정심사의 요건, 인정 받은 후에 인정을 유지하기 위하여 필요한 절차 및 의무 등에 대한 내용 등의 인정프로그램에 대한 내용은 NITE에 의해 구체적인 내용을 정하도록 하고 있는데,⁹⁾ 인정기관은 인정프로그램을 운용하여 평가기관에 대한 심사와 인정을 행하는 역할을 담당하게 된다.

인정기관은 평가기관이 동 제도에서 정하고 있는 기준에 부합하는지를 심사하고 인정하는 역할을 하고 있으며, 인정된 평가기관에 대해서 감시, 재조사 및 재인정과 취소를 행하는 역할을 담당하고 있다.

또한 인정기관은 인정프로그램에 의해 평가기관을 인정함에 있어서 평가기관이 보유하는 자원, 조직, 기술적 능력 및 설비 등을 기준으로 평가할 수 있는 정보보호시스템의 등급(EAL)을 특정해야 한다.¹⁰⁾

7) 동 지침의 정식명칭은 'ITセキュリティ評價及び認證制度'이다(이하 NITE, 評價 및 認證制度로 인용).

8) 일본의 정보보호시스템 평가 및 인증제도에 관한 상세한 내용은, 장교식, "일본의 정보보호시스템의 평가 및 인증제도에 관한 고찰", 『토지공법연구』, 제18집(2003. 6), 193면 이하 참조.

9) NITE, 評價 및 認證制度, 44頁.

10) NITE, 評價 및 認證制度, 44頁.

Ⅲ. 평가기관의 도입필요성 및 법제도의 개선방안

1. 평가기관에 관한 현행법률의 검토

정보화촉진기본법 시행령은 정보보호시스템의 제조업자나 수입업자가 당해 제품이 정보통신부장관이 정하는 기준에 적합한지의 여부를 평가받기 원하는 경우 정보통신부장관이 한국정보보진진흥원으로 하여금 당해 정보보호시스템의 조사 또는 시험·평가를 행할 수 있도록 규정하고 있다.

동 조항은 한국정보보호진흥원이 평가기관으로서 역할을 할 수 있는 근거조항이 되고 있으며, 한국정보보진진흥원 외의 기관이 평가기관으로서 역할을 하는 것에 대해서 금지하고 있지 않다. 따라서 정보통신부장관이 원하는 경우 현행법 하에서도 별도의 평가기관을 지정하는 것이 가능하다고 생각된다.

그러나, 평가기관의 경우 그 평가능력에 대한 검증이 이루어져야 하며, 특히 CCRA의 요구사항은 평가기관이 법률에 의해 설립되지 않는 경우에는 반드시 인정기관의 인정절차를 거치도록 하고 있다. 이는 객관적이고 정확한 평가가 담보되지 않은 상태에서의 인증은 아무런 의미가 없기 때문이다. 이러한 점을 고려할 때, 평가기관에 대한 검증절차가 전혀 마련되지 않은 상태에서 한국정보보호진흥원외의 기관이 평가기관으로 역할을 하는 것은 사실상 불가능하다고 생각된다.

2. 개선방안에 대한 검토

상술한 바와 같이 현행법상 한국정보보호진흥원만이 평가기관으로 역할하는 것이 가능하다고 보여지며, 정보통신부의 '정보보호시스템 평가·인증지침'에서도 한국정보보호진흥원을 평가기관으로 명시적으로 규정하고 있다.

그러나 상술한 바와 같이 외국의 경우에는 복수의 평가기관들이 운영되고 있으며, 특히 민간 평가기관을 적극적으로 활용하고 있는 추세이다. 이는 정보보호시스템의 평가 및 인증제도가 새로운 방향으로 전개되고 있다는 점을 보여주고 있는 예이며, 우리의 제도도 이러한 추세에 따라 변화가 요구되고 있다.

따라서 향후 평가수요의 증대 및 평가기관의 국제경쟁력강화를 위해서는 복수의 평가기관을 도입할 필요성이 있으며, 그 구체적인 방안으로 생각해 볼 수 있는 것이 민간평가기관의 설립을 허용하는 것이다.

1) 복수평가기관의 도입

점차 국경의 개념이 희미해지고 있는 경제사회에서 국제경쟁력의 강화는 생존을 위한 당면과제라고 할 수 있다. 이는 평가기관의 경우도 예외가 아니며, 특히 CCRA의 성립을 통해 공통의 평가기준 및 평가방법이 사용됨에 따라 전세계 평가기관간의 경쟁이 치열해 질 것으로 예상된다. 이러한 상황에서 우리 평가기관도 국제경쟁력을 강화가 요구되고 있으며 복수평가기관의 도입은 이러한 의미에서도 그 필요성이 크다고 생각된다.

복수평가기관의 도입은 (i)향후 평가수요 증가에 대비하고 (ii)평가기관간의 경쟁을 통한 기술력 및 서비스의 제고 및 이를 통해 (iii)평가기관의 국제경쟁력 강화와 (iv)평가수요의 개발이라는 측면에서 그 필요성이 있다고 생각된다. 또한 정보통신기술의 발전에 따라 단일 평가기관이 모든 정보보호시스템에 대한 평가를 전문적으로 행하기 어려운 상황에서 (v)평가분야의 분담을 통한 효율적인 평가를 도모할 수 있다는 측면에서도 의미를 가지고 있다고 생각된다.

복수평가기관을 도입하는 방안은 크게 두가지의 경우를 생각해 볼 수 있다. 첫 번째로 복수의 공공평가기관을 설립하는 방안과 두 번째로 민간평가기관의 설립을 허용하는 방안이다. 그러나 대부분의 국가가 민간평가기관의 설립을 허용하고 있는 상황에서, 공공평가기관이 시장원리에 따라 생존을 위해 적극적인 마케팅과 기술개발을 행하는 외국의 민간평가기관에 대해서 경쟁력을 가질 수 있을지가 의문이다. 따라서 보다 바람직한 방법은 민간평가기관의 설립을 허용하고 이를 적극 활용할 수 있는 제도적 장치를 마련하는 것이라고 생각된다.

2) 민간평가기관의 설립 허용

일본을 비롯한 대부분의 국가에서는 민간기관을 평가기관으로 활용하기 위한 노력을 경주하고 있다. 이에 따라 일본의 경우도 정보보호시스템의 평가 및 인증제도에 관한 모든 권한과 책임을 인증기관에 부여하고 있으며 평가기관에 대한 효율적인 감독체계를 갖추고자 노력하고 있다. 즉, 평가기관이 효율적인 평가를 행할 수 있는 제도적 장치를 마련하고, 대신에 어떠한 민간기관이라도 평가기관으로서 요건을 갖춘다면 동 제도의 평가기관이 될 수 있도록 하고 있는 것이다.

이러한 민간평가기관의 활용은 평가의 효율성 확보라는 측면에서 중요한 의미를 가지고 있다. 정부기관이 평가기관으로서 역할을 하는 경우 정확하고 공정한 평가가 담보될 수 있다는 점에서 긍정적인 측면이 있으나, 평가에 따른 비용을 국가가 부담해야 한다는 측면 및 민간의 발전된 정보통신기술을 활용하는데 어려움이 있다는 측면에서 문제가 있기 때문이다.

물론 현재 국내의 평가수요를 고려할 때 복수의 평가기관을 인정할 필요가 있는가에 대해서는 의문이 있다. 그러나 민간평가기관을 도입하자는 것은 복수의 평가기관을 도입하는 것이 아니라, 한국정보보호진흥원만이 평가기관으로서 역할을 할 수 있도록 하고 있는 현행법령을 개정하여 민간 평가기관의 설립이 가능하도록 하자는 것이다.

민간평가기관은 기본적으로 시장원리에 따라 움직이는 기업 및 연구소 등이 될 것이고, 동 기업 등은 수익이 없는 사업에 참여하지는 않을 것이다. 따라서 현실점에서 설립이 허용된다고 하여도 실제로 설립되는 민간 평가기관이 존재하지 않을 수도 있다. 그러나 중요한 것은 국외의 많은 평가기관들이 나름대로 기술을 개발하고 평가수요를 개발하고 있는 상황에서 우리의 경우 평가기관 설립자체를 제한한다면 향후 평가수요가 증가한다고 하여도 해외 평가기관에 대항하여 경쟁력을 갖는 것은 기대하기 어려울 것이다.

따라서 법령의 정비를 통해 민간평가기관이 설립될 수 있도록 허용하는 것이 필요하며, 평가수요의 개발 및 외국 평가기관과의 경쟁의 문제는 시장원리에 맡기는 것이 타당할 것이다.

IV. 인정기관의 도입 필요성 및 법제도의 개선방안

1. 인정기관의 도입 필요성

(1) 인정기관의 개념¹¹⁾

인정기관이란 평가기관이 적절하게 평가를 행할 능력을 가지고 있는지를 심사·인정하는 기관을 의미한다. 즉, 평가기관이 자국의 평가·인증제도의 기준에서 요구하는 사항을 만족시키는 조직을 가지고 운영되는지를 확인하는 것을 말한다.

대부분의 CCRA가입국 및 일본 등의 경우 CCRA 요구사항에 맞추어 자국의 평가·인증제도를 운용하고 있으므로, 인정기관에 요구되는 사항도 CCRA에서 요구사항과 동일하다고 할 수 있다.¹²⁾ 이러한 의미에서 보았을 때 우리나라의 인정기관의 경우도 궁극적으로 CCRA 요구사항에 맞는 형태로 구성되고 운영되어야 할 것이다. 따라서 인정기관의 경우 'ISO/IEC Guide 58(교정 및 시험을 위한 시험소 인정기관의 운영 및 승인에 관한 일반요구사항)'의 요구사항에 만족할 수 있는 조직을 갖추고 운영되어야 할 것이다. 또한 인정은 대상 평가기관이 'ISO/IEC 17025(시험소 및 교정기관의 능력에 관한 일반요구사항)'에 규정된 요구사항을 만족시키는 조직을 가지고 운영되는지를 확인하는 방법에 의해 이루어질 것이다.

(2) 인정기관의 도입필요성

11) 우리나라의 경우 인정기관을 도입하고 있지 않음에 따라 인정기관에 대한 명확한 개념정의가 이루어지고 있지는 않다.

따라서 이하에서는 제도적으로 인정기관을 도입하고 있는 일본의 개념을 중심으로 논의하고자 한다.

12) 일본의 경우 본문에서 설명하는 ISO/IEC Guide 58을 자국어로 번역한 JIS Z 9358 및 ISO/IEC 17025를 자국어로 번역한 JIS Q 17025를 기준으로 하고 있다.

우리법은 현재 평가기관으로서 한국정보보호진흥원만을 인정하고 있으나, 평가수요 등과 관련하여 민간평가기관의 도입 필요성이 제기되고 있다. 현재 대부분의 국가들이 민간평가기관을 허용할 뿐만 아니라 적극적으로 활용하고자 하는 추세에 비추어 보았을 때, 향후 민간평가기관의 도입이 불가피한 것으로 보여진다.

평가기관에 관해서 CCRA 요구사항은 (i)법에 의해 설립되거나, (ii) 인정기관으로부터 자격요건을 갖추어 인정받고 인증기관으로부터 평가역량에 대해 승인 받을 것을 규정하고 있다. (i)의 경우는 공공평가기관을 의미하는 것으로 우리나라의 정보보호진흥원이 이에 해당하며 (ii)의 경우는 민간평가기관을 의미하는 것이다.

법률에 근거하여 설립되지 않은 민간평가기관의 경우는 CCRA의 요구사항을 충족하고 있는지의 여부에 대해 별도의 심사절차를 요구하고 있으며, 이를 담당하는 기관이 바로 인증기관이다. 따라서 민간평가기관을 도입하기 위한 전제조건으로 인정기관의 설치가 요구되어 진다.

상술한 바와 같이 우리나라의 경우에도 민간평가기관의 설립을 허용할 필요성이 존재한다. 민간평가기관의 설립을 허용하기 위해서는 전제가 되어야 하는 것이 민간평가기관의 평가역량 및 조직이 공정하고 정확한 평가를 수행할 수 있는가에 대한 검증이 요구되며, 이는 향후 CCRA가입을 위해서도 필수적인 사항이다. 따라서 민간평가기관 설립허용을 염두했을 때 인정기관의 도입할 필요성이 존재한다.

2. 인정기관의 도입방안

(1) 인정기관 도입의 기본방향

외국의 경험에 비추어 볼 때, 인정기관을 도입하는 방안은 (a)기존 정부기관의 활용, (b)새로운 정부기관의 구성 및 (c)민간기관과의 제휴의 방법을 생각해 볼 수 있다. 이 중 (b)의 경우에는 인정업무의 규모에 비추어 볼 때 별도의 정부기관을 구성한다는 것은 현실성이 없다고 보여진다. 아울러 (c)의 경우는 인정업무를 담당하는 민간기관의 독립성과 공정성을 담보하고 CCRA의 요구사항에 만족하도록 운영하기 위해서는 이에 대한 별도의 감독기구가 필요하므로, 이종의 노력이 요구된다는 점에서 바람직하지 않다고 생각된다.

결국 가장 바람직한 방법은 기존의 정부기관을 활용하여 인정업무를 담당하게 하는 것이라 생각되며, 그 구체적인 대상으로 생각해 볼 수 있는 것은 국가표준과 관련한 인정기관인 기술표준원과 정보보호시스템의 인증업무의 정책기관인 정보통신부이다. 이하에서는 각각의 경우를 구분하여 인정기관으로서의 역할가능성에 대해서 살펴보겠다.

(2) 기술표준원에 대한 검토

(가) 기술표준원의 성립 및 역할

국가표준기본법은 적합성평가체제¹³⁾의 인정 및 인증사업을 추진하고 표준의 제정 및 적합성 평가절차를 국제가이드 및 규격과 일치시키기 위한 노력을 할 것을 정하고 있으며(21조 1항), 필요한 경우 관련행정기관의 장은 시험·검사기관 공인제도의 확립을 위한 인정기구와 운영기관의 지정, 인정기준 및 절차 등을 마련할 수 있으며, 기술표준원을 인정기구로 지정할 수 있도록 하고 있다(23조 2항, 동법 시행령 제16조 1항 및 2항).

동 법률에 근거하여 산업자원부장관은 '국제공인시험기관및검사기관인정제도운영요령(이하 운영요령이라 한다)'을 제정하여 인정제도에 대한 세부사항을 정하고 있으며, 인정기구로서 기술표준원 내에 '한국교정시험기관인정기구(Korea Laboratory Accreditation Scheme: KOLAS)'을 둘 것을 정하고 있다(운영요령 제3조 1항).

운영요령은 인정기구에 대해서 법 및 국제표준관련기구에서 정한 국제기준에 의거 교정기관, 시험기관 및 검사기관을 평가하여 공인하는 기구라고 정의하고 있다(운영요령 제2조 1호). 다시 말해서 KOLAS가 인정할 수 있는 기구는 교정 및 시험·검사기관으로 한정되며, 인정기구의 품질시스템 구축 및 운영, 인정업무와 관련된 정책수립 및 시행과 공인기관¹⁴⁾의 인정 또는 취소 및 사후관리와 처분 등에 대한 업무를 수행한다.¹⁵⁾ 또한 동 기구는 'ISO/IEC Guide 58(교정 및 시험을 위한 시험소 인정기구의 운영 및 승인에 관한 일반요구사항)'¹⁶⁾과 국제시험소인정기구(ILAC)에서 정한 지침문서와 기타 국제기구에서 정한 기준에 따라 운영된다(운영기준 제5조 1항).

(나) KOLAS에 인정업무 부여 가능성에 대한 검토

상술한 바와 같이 KOLAS는 이미 교정기관 등의 인정기구로서 역할을 하고 있으며, 따라서 정보보호시스템의 평가기관에 대한 인정기관으로 활용하는 방안을 생각해 볼 수 있다. 그러나 현행 제도 하에서 KOLAS가 정보보호시스템의 평가기관에 대한 인정업무를 행하는 것은 가능하지 않다고 생각된다. 현행법 하에서 KOLAS가 인정할 수 있는 기관은 교정 및 시험·검사기관으로 정해져 있기 때문이다.

13) 적합성평가라 함은 제품, 서비스, 공정, 시스템, 기관의 표준, 제품규격, 기술규정 등에서 규정된 요건에 적합한지의 여부를 평가하는 것을 말한다(국가표준법 제3조 20호).

14) 공인기관이라 함은 한국교정시험기관인정기구(KOLAS)로부터 인정을 획득한 교정기관, 시험기관, 검사기관을 말한다(운영요령 제2조 2호).

15) 인정기구는 그 외에도 ①공인기관 인정업무와 관련된 위원회 구성 및 운영에 관한 사항 ②공인기관 인정업무와 관련된 기준의 제정 또는 개정에 관한 사항 ③숙련도시험 운영에 관한 사항 ④숙련도시험운영기관 및 교육기관의 지정 및 관리에 관한 사항 ⑤공인기관 인정업무와 관련된 표준화에 관한 사항 ⑥상호인정 등 국제협력에 관한 사항 ⑦기타 공인기관 인정업무 수행에 필요한 사항 등을 담당한다(운영요령 제4조 참조).

16) 이는 CCRA의 요구사항과 동일한 기준이다.

동 규정에서의 교정기관이란 특정조건 하에서 측정기기, 표준물질, 물적척도 또는 측정시스템 등에 의하여 결정된 값을 표준에 의하여 결정된 값 사이의 관계로 확정하는 일련의 작업을 행하는 기관을 의미한다(국가표준기본법 제3조 17호).¹⁷⁾ 또한 시험기관 및 검사기관의 경우에는 인정받을 수 있는 분야를 운영요령에서 정하고 있다.¹⁸⁾ 인정의 대상이 되는 시험분야는 역학시험, 화학시험, 전기시험, 열 및 온도측정, 비파괴시험, 음향 및 진동시험, 광학 및 광도측정, 의학시험, 생물학적 시험, 패스너, 화학제품의 공정관행시험 등이다(운영요령 제14조 1항 및 별표1). 아울러 검사기관의 인정분야는 관련 개별 법에서 규정한 검사분야 및 기타 인정기구의 장이 필요하다고 인정한 분야로 정하고 있다(운영요령 제14조 1항).

따라서 정보보호시스템의 평가 및 인증제도 하에서 정보보호시스템 및 보호프로파일에 대한 평가를 실시하는 평가기관에 대한 인정업무는 KOLAS의 업무범위에 포함되지 않고 있으며, KOLAS가 동 업무를 담당하기 위해서는 법령 및 운영요령의 개정이 이루어져야 할 것이다.

상술한 바와 같이 CCRA의 요구조건은 평가기관에 대해서 인정기관으로부터 자격요건을 갖추어 인정받고 인증기관으로부터 평가역량에 대해 승인 받을 것을 규정하고 있다. 따라서 KOLAS가 인정기관으로서 역할을 하는 경우에는 당해 인정에 대해서 승인을 할 수 있는 인증기관이 필요하므로 인증기관 및 그 승인절차에 대한 법규정의 마련이 필요하다.

또한, 법령 및 운영요령의 개정을 통해 평가기관에 대한 인정업무를 KOLAS의 업무범위에 포함시킨다고 하여도, 실질적으로 동 업무를 수행하기 위해서는 별도의 조직과 인력을 갖추어야 할 것이다. 현재 KOLAS의 경우 정보보호시스템에 대한 전문인력을 갖추고 있지 못하고 있기 때문이다.¹⁹⁾

(3) 정보통신부에 대한 검토

(가) 정보통신부의 역할

현행 정보보호시스템의 평가 및 인증제도는 정보통신부가 그 주체로서 동 제도관련 정책을

17) 교정기관 측정기의 정밀·정확도를 지속적으로 유지시키기 위하여 정밀정확도가 더 높은 표준기와 주기적으로 교정을 실시하여 국가측정표준과의 소급성을 유지시킴으로써, 측정기의 계속 사용, 마모, 내용연수 경과 및 사용환경 변화 등으로 발생할 수 있는 측정오차를 함시 허용 공차 이내로 유지시키는 것을 말한다. 이 제도의 궁극적인 목적은 제조공정에서 제품의 균질성과 성능을 보장하고, 시험·연구기관에서 산출하는 측정결과와 대의 신뢰도를 확보하는데 있다.

18) 시험이란 특정한 제품, 공정 또는 서비스를 대상으로 하나 또는 그 이상의 특성을 규정된 절차에 따라 측정하는 기술적인 작업을 의미하며, 검사란 제품설계, 제품, 서비스, 공정 또는 시설에 대하여 특정요건에 대한 적합성 판정을 말하며 검사에는 경험, 전문적 판단에 연계된 육안검사가 포함된다. 이에 대한 내용은 KOLAS 홈페이지 참조.

19) 운영요령 제35조 및 [별표3]에서는 시험요원 및 검사요원의 자격기준에 대해서 정하고 있는데, 동 기준에서 정하고 있는 해당분야는 역학시험, 전기시험, 열 및 온도측정, 비파괴시험, 음향 및 진동시험, 광학 및 광도측정, 패스너와 화학시험, 의학시험, 생물학적 시험, 화학제품의 GLP시험으로 정하고 있다. 즉, 정보보호시스템은 해당분야에 포함되지 않고 있다.

수립하고 운영하도록 되어 있으며(정보화촉진기본법 제15조), 한국정보보호진흥원을 평가기관으로 둘 수 있도록 하고 있다(동법 시행령 제16조). 이에 근거하여 정보통신부는 '정보보호시스템 평가·인증 지침(이하 '평가·인증지침'이라 한다)'을 제정하고 있으며, 동 지침에서는 인증기관은 국가정보원, 평가기관은 한국정보보호진흥원으로 정하고 있다. 인정기관에 대해서는 아무런 정함이 없는데, 이는 단일 공공평가기관을 정하고 있음에 따라 별도 인정기관을 둘 필요성이 없었기 때문으로 보여진다.

(나) 평가·인증지침에 의한 인정기관 도입 방안에 대한 검토

외국의 경우 인정기관은 정보보호시스템의 평가 및 인증제도의 하나의 축으로서 중요한 역할을 하고 있으며, 인증기관 및 평가기관과 유기적 연관성을 가지고 운영되고 있다. 따라서 우리나라의 경우도 향후 인정기관을 도입하는 경우 인증·평가기관과의 유기적 관계를 고려하여 기존의 '평가·인증지침'에서 인정기관을 규정하는 방안을 생각해 볼 수 있다.

이를 위해서는 먼저 법령의 개정을 통해 인정기관의 설립근거를 마련하는 것이 필요하다. 인정기관의 설립의 전제는 민간평가기관의 도입이며, 이를 위해서는 현행 정보화촉진기본법 시행령 제16조를 개정하여 한국정보보호진흥원 외에 민간평가기관을 설치할 수 있는 근거를 마련해야 하며, 이 경우 민간평가기관에 대한 인정을 행하는 인정기관의 설립에 대해서도 근거규정을 마련하는 것이 필요하다.

법령에서 인정기관의 도입에 대한 근거규정을 마련한 경우, 그 구체적인 내용, 즉 인정업무의 담당기관, 인정기관의 요건, 인정절차 등에 대해서는 '평가·인증 지침'에서 정하는 것이 타당할 것이다. 인정제도도 정보보호시스템의 평가 및 인증제도에 포함되는 부문이기 때문이다. 아울러 인정기관의 평가기관에 대한 인정의 승인은 동 지침 상의 인증기관이 담당하게 한다면 동 제도가 보다 효율적으로 운용될 수 있을 것으로 생각된다.

3. 인정기관 도입방안에 대한 검토

살펴본 바와 같이 인정기관을 도입방안은 KOLAS가 인정업무를 담당하는 방안과 정보통신부가 동 업무를 담당하는 방안이 있으며, 어느 방안을 택하더라도 법령의 개정이 요구된다. 결국 현행법 하에서는 어느 누구도 인정업무를 담당하지 못하므로, 향후 인정기관 도입에 있어 중요하게 고려해야 할 점은 보다 효과적인 방향으로 법령의 개정이 이루어져야 한다는 것이다.

먼저 살펴본 KOLAS의 경우 이미 인정업무를 행하고 있다는 점에서 장점을 가지고 있다고 할 수 있다. 그러나 KOLAS가 담당하는 국가표준에 관한 사항과 정보보호시스템에 대한 사항은 그 차원을 달리한다는 점에서 문제가 있다. 살펴본 바와 같이 KOLAS의 근거법인 국가표준

기본법은 국가표준제도의 확립을 위한 기본적인 사항을 규정하고 있으며(제1조), 과학기술을 기반으로 한 국가표준²⁰⁾을 준용하여야 하는 경제사회 활동의 모든 영역에 대해서 적용되는 법이다(제2조). 이에 비해 정보보호시스템의 평가 및 인증제도의 근거법인 정보화촉진기본법은 정보화를 촉진하고 정보통신산업의 기반을 조성하기 위한 것이며(제1조), 이를 위한 정보보호시스템의 구축을 위해 마련된 법이다.

다시 말해서 정보보호시스템의 평가 및 인증제도는 궁극적으로 정보보호, 즉 정보의 수집·가공·저장·검색·송신·수신 중에 정보의 훼손·변조·유출 등을 방지하기 위한 관리적·기술적 수단을 강구하기 위한 제도이며(정보화촉진기본법 제2조 4호), 국가표준의 확립을 위한 KOLAS와는 그 존립근거를 달리하고 있다고 할 수 있다.

국가표준기본법 및 시행령 등에서 시험기관과 검사기관을 두고 있음에도 불구하고, 유사한 업무를 행하는 정보보호시스템에 대한 평가기관에 대해서는 별도로 정보화촉진기본법 시행령에서 한국정보보호진흥원을 두고 있는 것도 이러한 맥락에서 이해하는 것이 타당할 것이다. 결국 법령개정 및 조직과 전문인력의 확충이라는 부담을 감수하면서까지 KOLAS로 하여금 인정 업무를 담당케 해야 할 이유는 없을 것이다.²¹⁾

정보보호시스템의 평가 및 인증제도가 보다 효율적으로 이루어지기 위해서는 동 제도의 중심축인 인증기관, 평가기관 및 인정기관이 상호보완을 이루는 체계를 갖추어야 하며, CCRA 가입이라는 당면과제를 고려할 때 그 필요성은 더욱 커진다. 따라서 평가 및 인증제도의 정책주체인 정보통신부가 '평가·인증 지침'을 통하여 인증기관, 평가기관 및 인정기관을 정하고 통일적으로 관리할 수 있는 시스템을 갖추는 것이 바람직할 것이며 입법취지에도 부합할 것으로 생각된다.

V. 결 론

정보통신기술의 이용은 이미 일상생활의 중요한 일부분이 되었으며, 이에 따라 정보보호의 필요성은 국가기관뿐만 아니라 민간에서도 중요한 의미를 갖게 되었다. 정부기관뿐만 아니라 민간기업 및 개인에게 있어서도 해킹 등의 정보침해사고에 따른 문제점 및 재산상의 피해도 이미 상당정도에 이르고 있는 상황이다.

20) 국가표준이라 함은 국가사회의 모든 분야에서 정확성, 합리성 및 국제성 제고를 위하여 국가에서 통일적으로 준용하는 과학적·기술적 공공기준으로서 측정표준, 참조표준, 성분표준 등 국가표준기본법에서 정하고 있는 모든 표준을 말한다(국가표준기본법 제3조 1호).

21) 물론 현실적으로 정보통신부가 직접 인정기관으로서 역할을 하지 않고 타 기관에 대해 업무를 위임하는 경우, 수입기관이 KOLAS가 될 수 있을 것이다. 그러나 이 경우에도 인정업무에 관한 주체는 정보통신부가 된다는 점에서, 본문에서 서술한 경우와 같이 KOLAS가 독립적인 인정기관으로서 역할을 하는 경우와는 구별될 것이다.

이러한 상황에서 정보보호시스템의 평가 및 인증제도는 정보통신시스템의 수요자에게 보안성 높은 제품을 공급한다는 점에서 중요한 의미를 가지고 있으며, 아울러 공급자의 경우 제품의 경쟁력을 강화시킬 수 있는 수단이 된다는 점에서 중요한 의미를 가지고 있다. 소위 정보통신기술의 선진국들이 CCRA의 설립 등을 통해 공통된 평가기준 및 평가방법을 갖추고 상호인증을 위한 노력을 경주하는 이유도 이러한 의미에서 생각해 볼 수 있다.

인터넷 등 정보통신기술의 사용이 이미 세계적인 수준에 이르고 있는 우리나라의 경우도 정보보호시스템의 중요성은 날로 증가하고 있다. 우리나라의 경우도 나름의 평가 및 인증제도를 구축하고 있으며, 현실적인 기능의 측면에서 큰 문제는 없는 것으로 보이나 최근의 변화의 추세를 반영하지 못하고 국가조달물품에 대한 평가 및 인증을 위한 제도가 그대로 유지되고 있는 것으로 보여진다. 그 가장 큰 이유는 평가 및 인증제도를 담당하고 있는 각 기관들에 대한 법적 근거가 불명확하며, 이에 따라 정부기관의 필요성에 의해 동 제도가 이용되고 있기 때문이라고 보여진다.

이에 비해 외국의 경우는 평가 및 인증제도가 통일적으로 정비되고 있으며, 이에 대한 법적근거를 명확히 갖추어 운영되고 있다. 상술한 영국과 미국의 경우는 법령에서 평가 및 인증제도의 주체를 정하고 동 주체가 평가 및 인증제도의 구체적 내용을 마련하여 시행하도록 하고 있다. 또한 우리나라와 법체계가 유사한 독일이나 일본의 경우는 평가 및 인증제도의 주체인 인증기관에 관한 근거법령을 마련하거나 기존의 기관의 업무로서 인증업무를 부여하고 있다. 또한 인증기관으로 하여금 평가 및 인증제도에 대한 구체적인 내용을 정하여 시행하도록 하고 있다.

이에 비해 우리나라의 경우는 현행법상 평가 및 인증제도의 운영주체 및 인증기관에 대한 명확한 근거규정이 마련되지 않고 단지 정보통신부의 지침에 의해 양 기관을 정하고 있는 상황이다.

이는 국민의 권리와 의무에 영향을 미칠 수 있는 기관의 설립을 법률에 의하지 않는다는 점에서도 문제가 있으며, 기관간의 역할에 대한 구분이 불분명해짐에 따라 평가 및 인증제도의 실효성을 확보하는데도 어려움이 있을 것으로 생각된다. 아울러 향후 CCRA에의 가입을 전제로 생각해 볼 때도 CCRA의 요구조건에 따라 평가 및 인증제도에 대한 통일적인 정비가 요구된다.

CCRA에의 가입은 우리 정보보호제품의 질적향상을 통해 날로 국제화되고 있는 경제상황 하에서 국제경쟁력을 강화한다는 측면에서 중요한 의미를 갖게된다. 그러나 이는 곧 평가 및 인증제도 자체의 국제적인 경쟁의 시작을 의미하는 것이며, 따라서 국내의 평가 및 인증제도, 다시 말해서 인증기관, 평가기관 등이 세계의 다른 기관과 경쟁력을 갖도록 하기위한 제도적 정비가 필요하다고 생각된다.

이러한 법제도의 첫 번째 단계로서 이루어져야 할 것이 바로 민간평가기관의 설립허용 및 이를 위한 인정기관의 도입 등에 대해서도 적극적인 검토가 필요하다고 생각된다. 다만, 구체적인 방안은 국내의 평가수요, 인증된 제품의 수요와 평가 및 인증의 기술적 수준과 제품을 생산하는

기업 및 수요자의 이해관계 등이 고려되어야 할 것이며, 이를 위해서는 향후 보다 구체적이고 현실적인 연구가 지속적으로 이루어질 필요가 있다고 생각된다.

《參考文獻》

- 장교식, "일본의 정보보호시스템의 평가 및 인증제도에 관한 고찰", 「토지공법연구」 제18집 (2003. 6).
- AKAS, About UKAS(Mar. 2003)
<http://www.ukas.com/new_docs/about.htm>
- BSI, Bundessmt für Sicherheit in der Informationstechnik(2001).
- CESG, Common Criteria Certification in the UK(Aug. 1999)
- NVLAP, National Voluntray Laboratory Accreditation Program(Nov. 2003)
<<http://www.niap.nist.gov/cc-scheme/nvlap.html>>
- NIAP, CCEVS Validation Body(Nov. 2003)
<<http://www.niap.nist.gov/cc-scheme/Validation-body.html>>
- NIAP, Historical Perspective(Mar. 2003)
<<http://www.niap.nist.gov/cc-scheme/historical-perspective.html>>
- NIAP, Common Criteria Evaluation and Validation Scheme for Information Technology Security - Organization, Management and Concept of Operations -, Scheme Publication #1 Version 2.0(May 1999).
- UKITSEC, Security Evalution for It Products(Mar. 1996)
- UKITSEC, UK Scheme Publication No.1 Description of the Scheme(July 2002).
- 情報處理振興事業協會, "情報技術セキュリティ評價のためのコモンクライテリア" (1999. 8).
- 情報處理振興事業協會, "1st ICCC 出張報告書"
<http://www.ipa.go.jp/security/ccj/report/h12/iccc2000/iccc2000_2.htm>
- 獨立行政法人 製品評價技術基盤機構, "ITセキュリティ認證申請者・登録者に對する要求事項" (2002.4)
<<http://www.nite.go.jp/asse/its/pdf/itaplreq.pdf>>
- 獨立行政法人 製品評價技術基盤機構, "ITセキュリティ認證申請等の手引き" (2002. 4)
<<http://www.nite.go.jp/asse/its/pdf/itaplgd.pdf>>
- 獨立行政法人 製品評價技術基盤機構, "ITセキュリティターゲットの確認申請者・登録者に對する要求事項" (2002. 4) <<http://www.nite.go.jp/asse/its/pdf/staplreq.pdf>>
- 獨立行政法人 製品評價技術基盤機構, "ITセキュリティターゲットのターゲット評價, 確認申請等の手引き" (2002. 4) <<http://www.nite.go.jp/asse/its/pdf/staplgd.pdf>>
- 獨立行政法人 製品評價技術基盤機構, "ITセキュリティ評價機關承認に對する要求事項" (2002. 4)
<<http://www.nite.go.jp/asse/its/pdf/efapvreq.pdf>>

SUMMARY

A Study on Legal Aspect of the Certification body and the Accreditation body for the Information Technology Security

Jang, Kyo-Sik

(A Assistant Professor, Department of Law, College of Law, Konkuk University)

Although the level of Information Technology(IT) and usage has already followed the advanced country's level, it still requires that the legislative system should be re-organized. An effective IT Security System (ITSS) also needs to be established. With this motivation as a foundation, this study will analyze the member of CCRA's Evaluation Facility, Certification Body, and Accreditation Body's laws and regulations related to establishment, administration, and scope of business. In addition, the strength and weakness of each nation's legislative system will be explored. In conjunction with that, this study will be investigated problems of certification system and evaluation of ITSS. It also will be demonstrated that policy implications for solving the problem. Finally, the effectiveness of ITSS and the required items for joining CCRA will be considered throughout this study.

The span of this study is important nations among the member of CCRA included U.S.A, Germany, England and Japan. The reason for choosing these countries is that U.S.A, Germany, England had been established their evaluation and certification scheme, and advanced legislative systems. In other words, we can learn their know-how and techniques throughout their systems. Especially, Japan recently is trying to re-organize their legislative system for joining CCRA like our country. Many researches related to this issue also have been done. For these reasons, this study includes U.S.A, Germany, England, and Japan. It, however, should be mentioned that this study focuses on analysis of laws related to evaluation, certification, and organizations rather than detailed guideline and technical parts. Therefore, detailed guideline and technical parts of evaluation and certification have been excluded from this study.