通信情報保護學會誌
第 10 券 第 3 號, 2000. 9

국내 정보보호시스템 평가·인증 제도 발전 방향 연구

이 완 석*, 이 경 구*

요 약

1995년 10월에 제정된 정보화촉진기본법과 동법 시행령에 의거 국내 평가·인증 제도가 구축되어 시행되어 왔다. 현재 한국정보보호센터에서는 1998년 2월 정보통신부에서 고시하였으며 2000년 2월에 개정한 정보통신망 침입차단시스템 평가기준과 2000년 7월에 고시된 침입탐지시스템 평가기준을 이용하여 두 개의 제품에 대한 평가를 실시하고 있으며 인증기관인 국가정보원에서 인증서를 발급하고 있다. 하지만 컴퓨터 및 통신 기술의 발달과 네트워크의 급속한 확산으로 인하여 다양한 정보보호제품이 개발되고 있으며 IT 제품 평가 관련 선진국들은 세계 여러 국가들에게 국제표준(ISO/IEC 15408)으로 재정된 국제공통평가기준에 기반을 둔 국제상호인정협정을 확산시키고 있다. 따라서 급변하는 IT 환경과 국제 상황을 고려하여 국내 평가·인증제도의 개선점들을 찾아본다.

Ⅰ. 서 론

정보보호시스템 평가의 선진국인 미국, 영국, 독일, 프랑스 및 캐나다 등은 1980년대부터 정보보호제품을 평가하기 위한 평가·인증 제도를 운영하여 왔으며 변화하는 사회와 국제환경에 적응하도록 평가·인증 제도를 수정하여 왔다. 초기에 이들의 국가들은 공공기관을 대상으로 평가·인증 제도를 운영하여 왔다. 하지만 해커, 크래커, 바이러스 등의 정보화 역기능들이 정보화사회에 위협으로 등장하면서 정보보호 마인드가 확산되었으며 이에 따른 민간분야에서의 정보보호 수요와 사용자들의 요구사항이 증가하였다. 따라서 이들의 국가들은 평가·인증 제도의 적용 범위를 민간분야에까지 확대하게 되었다.

또한 정보보호제품 시장이 민간분야에까지 확산되면서 개발된 정보보호제품을 해외로 수출하기에 이르렀으며 이들의 제품들은 자국의 평가·인증 제도에서 평가를 받아 인증서를 발급 받았다고 하여도 제품을 수입하는 국가들은 이를 인정하여 주질 않았다. 그리하여 미국을 비롯한 선진 5개국들은 평가인증서를 상호인정하는 협정을 구축할 것을 합의하였으며 협정의 기반이 되는 국제공통평가기준을 개발하기에 이르렀다. 5개국은 1998년 10월 국제공통평가기준과 국제공통평가방법론을 이용하여 제품을 평가하며 이에 따른 인증서를 상호인정하는 국제상호인정협정서에 서명하였다. 그후 1년뒤인 1999년 10월에는 호주와 뉴질랜드가 협정서에 서명함으로써 7개 국가가 국제상호인정협정에 가입하였다. 2000년 8월 현재 국제상호인정협정에 가입한 국가는 뉴질랜드, 독일, 미국, 영국, 프랑스, 캐나다 등 기존 맴버 7개국과 새로이 가입한 그리스, 네덜란드, 노르웨이, 스페인, 이탈리아, 핀란드 등 6개국을 포함하여 13개 국가에 이른다[1].

국제공통평가기준은 하나의 기준으로 다양한 정보보호제품을 평가할 수 있는 기준으로 1998년 버전 2.0이 개발되었으며 표준문서 양식에 맞게 수정되어 버전 2.1이 국제표준(ISO/IEC 15408)으로 제정되었다[2]. 정보보호제품 평가·인증 제도를 운영하고 있는 국가들은 현재 국제공통평가기준을 이용한 평가·인증 제도로 재정비하고 있는 상황이다.

국내에는 1995년 정보화 촉진 기본법이 제정되어 정보보호시스템 평가·인증 제도 구축의 기반을 구

* 한국정보보호센터 평가기준팀 (wsyi@kisa.or.kr, kglee@kisa.or.kr)

축하였다. 1998년 정보통신망 침입차단시스템 평가기준이 고시되어 실제적으로 국내 평가·인증 제도를 시행하게 되었다. 하지만 현재 국내 평가·인증 제도는 제품별 평가기준을 사용함으로 인하여 민간분야에서 요구하는 다양한 제품을 평가할 수 없어 융통성면에서 제약을 받고 있다. 따라서 다양한 제품을 평가할 수 있는 국제공통평가기준을 수용하고 국제상호인정협정에 가입할 수 있는 여건을 마련하기 위하여 국제 환경에 적합한 평가·인증 제도 구축이 필수라고 할 수 있다.

본 고의 제 2장에서는 국외 정보보호시스템 평가·인증 제도의 선진국인 미국, 영국, 독일 및 프랑스의 평가·인증 제도에 대해 알아보고 제 3장에서는 국내 평가·인증 제도의 변화와 현황에 대해 분석한다. 제 4장에서는 국내 평가·인증 제도의 개선점과 앞으로 나아가야 할 발전 방향에 대해 소개한다. 제 5장에서는 설명된 모든 내용을 요약 정리한다.

II. 국외 평가·인증 제도

1. 평가·인증 제도 소개

정보보호시스템 평가·인증 제도는 정보보호시스템 보안기능들에 대한 안전성을 공신력있는 제 3자로부터 입증받기 위한 것으로 인증기관, 인정기관, 평가기관, 평가기준, 평가방법론, 평가·인증 스킴 등 평가에 관련된 모든 제반 사항들을 의미한다.

정보보호시스템 평가·인증 제도의 선진국인 미국, 영국, 독일, 프랑스 및 캐나다 등에서는 10년에서 20여년의 평가 경험을 보유하고 있다. 이들은 크게 미국과 캐나다 그리고 유럽으로 구분할 수 있다.

국가들은 자국의 평가기준을 이용하여 정보보호제품을 평가하여 왔으나, 미국과 캐나다를 제외한 유럽 3개국의 경우, 1990년 초 유럽의 공통평가기준인 ITSEC(Information Technology Security Evaluation Criteria)을 개발하여 정보보호시스템을 평가하고 있다.

평가·인증 제도에는 평가기준, 평가·인증 스킴과 평가체계로 구성된다.

- 평가기준은 제품의 보안요구사항을 의미하며 보안기능 요구사항과 보증 요구사항으로 구성된다. 보안기능 요구사항은 정보보호제품 및 시스템이 특정 임무를 수행하는데 필요한 최소한의 보안기능을 의미하며 보증 요구사항은 보안기능 요구사항을 구현하기 위하여 작성된 문서들로서 보안기능의 신뢰성을 평가하는데 사용된다. 평가기준의 대표적인 예로는 미국의 TCSEC(Trusted Computer System Evaluation Criteria), TDI(Trusted DataBase Management System Interpretation of the TCSEC), TNI (Trusted Network Interpretation of the TCSEC), CSSI(Computer Security Subsystem Interpretation of the TCSEC)와 유럽의 ITSEC 그리고 캐나다의 CTCPEC (Canadian Trusted Computer Product Evaluation Criteria)이 있으며 국내에서는 1998년 2월에 고시되어 2000년 2월에 개정된 정보통신망 침입차단시스템 평가기준과 2000년 7월에 고시된 정보통신망 침입탐지시스템 평가기준이 있다[2].

- 평가·인증 스킴은 평가·인증 절차 및 관련 기관의 임무와 책임을 명시한 문서를 의미한다. 미국에는 TTAP(Trusted Technology Assessment Program)과 TPEP(Trusted Product Evaluation Program), CCEVS (Common Criteria Evaluation and Validation Scheme)가 있으며 유럽에는 ITSEM(Information Technology Security Evaluation Manual)이 있다. 한국에는 정보보호시스템 평가·인증 지침을 예로 들 수 있다[2].

- 평가체계는 정보보호제품을 평가하기 위한 관련 기관들을 의미한다. 평가체계에는 평가 결과를 최종 검증하여 인증서를 발급하는 인증기관, 정보보호제품을 평가하는 평가기관 및 평가기관의 자격을 심사하여 평가기관으로 선정하는 역할을 수행하는 인정기관 등이 있다.

다음은 정보보호제품 평가·인증 제도를 제일 먼저 시작한 미국과 유럽 국가들의 제도에 대해 알아

본다.

2. 미국의 평가·인증 제도

미국은 1952년 트루만 대통령의 지시에 의거 통신보안 프로그램을 실행하여 왔으며 1984년 대통령 지시(NSDD-145)에 의거 통신보안과 컴퓨터 보안에 대한 프로그램을 실행하였다. 이에 의하여 미국의 평가·인증 제도를 실행하여 왔다[3].

2.1 평가기준

미국은 선진 5개국들 중 정보보호시스템 평가에 있어서 가장 오래된 경험을 보유하고 있다. 미국은 1983년 오랜지 북이라 불리우는 TCSEC 초안을 개발하였으며 이는 1985년 미 국방성 표준(DoD STD 5200.28)으로 채택되었다. TCSEC은 국방기관 및 정부기관이 안전성 및 신뢰성이 입증된 운영체제를 도입할 수 있도록 운영체제를 6등급(C1, C2, B1, B2, B3, A1)으로 분류하였다. 미국 정부는 다양한 정보보호제품이 개발됨에 따라 1987년 네트워크 제품을 평가할 수 있는 TNI, 1991년 데이터베이스 시스템을 평가할 수 있는 TDI와 컴퓨터의 일부 부품을 평가할 수 있는 CSSI를 개발하였다. 그러나 제품별 평가기준을 사용하는데 한계를 느낀 미국은 다양한 정보보호제품을 평가할 수 있는 FC(Federal Criteria for Information Technology Security)를 개발하였으나 실제 제품 평가에는 사용하지 않았다. 대신 국제표준인 국제공통평가기준을 이용하여 정보보호제품을 평가하고 있다[3].

2.2 평가·인증 스킴

미국은 국방성을 중심으로 한 연방정부차원에서의 평가·인증 제도를 구축하였으며 이에 의한 평가·인증 스킴을 개발하였다. 초기의 평가·인증 스킴인 TPEP은 연방정부를 위한 것으로써 평가기준에 명시되어있지 않은 기술검토, 강력한 예비기술검토, 등급유지계획 및 문서화 등 평가절차를 규정하고 있다. TPEP에서는 제품을 평가하는데 있어서 개발자가 자체적으로 평가신청을 할 수 있는 것이 아니라 정부에서 특정 정보보호제품이 시장성이 있다고 판단되거나 정부기관에서 제품을 도입하기 이전 단계에 평가기관에 평가 의뢰함으로 인하여 평가 대상 제품이 선정되었다. 따라서 평가 대상 제품으로 선정되었다 하더라도 우선순위에 의해 오랜 기간을 대기해야 하는 문제점들이 있었다.

TPEP의 문제점을 해결하는 동시에 민간분야에서의 정보보호 마인드 확산 및 제품 수요의 증가로 인한 평가 수요 증가를 해결하기 위하여 TTAP을 개발하였다. TTAP에서는 C2 등급 이하의 정보보호제품을 민간평가기관에서 평가하는 것을 전제로 하였으나 그 등급을 상향조정하여 B1 등급까지 확대하였다. 평가기관은 TORA(TTAP Technical and Organizational Requirements for Accreditation)와 TC2PR(TTAP Evaluation Process for C2 Product)의 조건을 만족하는 민간평가기관을 지정하여 제품을 평가할 수 있도록 하였다[2].

최근 미국은 국제공통평가기준을 이용하기 위하여 평가·인증 제도를 재정비하면서 CCEVS(Common Criteria Evaluation & Validation Scheme)를 개발하고 있으며 스킴의 목록은 다음과 같다.

현재 파트 1과 2만이 완성되어 웹에 게재되어 있는 상태이며 그 외의 파트들은 개발되는 동시에 NIAP(National Information Assurance Partnership) 홈페이지에 게재될 예정이다[5].

표 2. 미국의 평가·인증 스킴 목록

Part #	제 목
1	NIAP Common Criteria Evaluation and Validation Security for IT Security Organization, Management and Concept of Operations
2	NIAP Common Criteria Evaluation and Validation Security for IT Security Validation Body Standard Operating Procedure
3	NIAP Common Criteria Evaluation and Validation Security for IT Security Technical Oversight and Validation Procedures
4	NIAP Common Criteria Evaluation and Validation Security for IT Security Guidance to Common Criteria Testing Laboratories
5	NIAP Common Criteria Evaluation and Validation Security for IT Security Guidance to Sponsors of IT Security Evaluations
6	NIAP Common Criteria Evaluation and Validation Security for IT Security Certificate Maintenance Program

2.3 평가체계

미국의 평가체계는 평가스킴에 따라 많은 변화가 있었다. 특히 미국은 국가기관용 제품을 평가하는 평가체계와 민간용 정보보호제품을 평가하는 체계로 이원화 되어있다[6].

표 3. 미국의 평가·인증 체계

	국가기관용	민수용	
	TPEP	TTAP	CCEVS
인증기관	NSA	TTAP (감독위원회)	NIAP
인정기관	none	TTAP (감독위원회)	NIAP
평가기관	NCSC	7개의 TEF	CCTL

※ NSA(National Security Agency)
※ NCSC(National Computer Security Center)
※ TTAP 감독위원회 : NSA와 NIST 직원으로 구성
※ NIST(National Institute of Standards and Technology)
※ TEF(Trusted Evaluation Facility)
※ NIAP : NSA와 NIST 직원으로 구성
※ CCTL(Common Criteria Testing Laboratory)

미국은 민수용 제품에 대한 평가를 위하여 7개의 평가기관을 지정하여 운영하고 있으며 이들의 목록은 다음과 같다[4].

표 4. 미국의 민간평가기관 목록

민간평가기관명
o Arca Systems Inc.
o Computer Sciences Corp.
o Cygnacom Solutions
o National Software Testing Laboratories
o Science Applications International Co.
o Booz, Allen, Hemilton
o CoAct Incorporated

3. 유럽의 평가·인증 제도

3.1 평가기준

미국에 이어 유럽의 영국, 독일, 프랑스에서도 정보보호제품에 대한 평가·인증 제도를 구축하여 실행하여 왔다. 초기에는 영국의 Green book, 프랑스의 Blue-White-Red Book, 독일의 Criteria for the Evaluation of Trustworthiness of Information Technology Systems 등 자국의 평가기준을 활용하여 정보보호제품을 평가하여 왔다. 국가들은 민간분야의 정보보호 중요성을 일찍이 파악하여 1980년대말 이미 민간평가기관을 설립하여 민간분야의 평가수요를 충족시켰다. 또한 각각의 국가에서 별도의 평가·인증 제도를 운영함에 있어 제품 수출시 중복 평가에 소요되는 시간, 비용 및 노력을 줄이기 위하여 단일의 평가기준을 개발하여 평가함으로써 상호 평가결과를 인정하기로 합의하였다. 따라서 이들은 ITSEC 버전 1.0을 1990년에 개발하여 정보보호제품을 평가하고 있다[6].

더불어 이들 3개 국가는 또한 국제공통평가기준 기반의 국제상호인정협정에 가입함으로 인하여 현재 ITSEC과 국제공통평가기준 두 개의 평가기준을 이용하여 정보보호제품을 평가하고 있으며 평가신청자가 두 개의 기준 중 하나를 선택하여 평가를 받도록 하고 있다.

3.2 평가·인증 스킴

유럽의 3개 국가는 ITSEM이라는 평가·인증 스킴을 개발하여 활용하고 있으며 미국의 스킴에 비해 매우 세부적으로 기술되어있다. 특히 암호알고리즘 평가방법 등 평가기준의 세부 분야에 대한 평가방법론을 기술하고 있으나 스킴 전체가 공개되어 있지는 않으며 그 일부분만이 공개되어 있다.

3.3 평가체계

유럽 3개국의 평가기준, 인증기관, 인정기관, 평가기관 등은 다음 표와 같다[6].

표 5. 영국, 독일 및 프랑스의 평가·인증 체계

		영국	독일	프랑스
인증기관		CESG	BSI	SCSSI
인정기관		UKAS	DAR	COFRAC
평가기관	국가기관	CESG	BSI	SCSSI
	민간기관	5개 기관	8개 기관	5개 기관

※ CESG(Communications-Electronics Security Group)
※ UKAS(United Kingdom Accrediation Service)
※ BSI(Bundesamt für Sicherheit in der Informationstechnik)
※ DAR(Deutscher AkkreditierungsRat)
※ SCSSI(Service Central de la Securite des Systemes d'Information)

영국, 독일, 프랑스 등의 민간평가기관 목록은 다음과 같다[6].

표 6. 영국, 독일, 프랑스의 민간평가기관 목록

국가명	민간평가기관명
영국	ㅇ Admiral Management Services Ltd. ㅇ EDS Ltd. ㅇ IBM Global Services ㅇ Logica UK Ltd. ㅇ Syntegra
독일	ㅇ IABG ㅇ CCI ㅇ debis Systemhaus Information Security Services GmbH ㅇ Tele-Consulting GmbH ㅇ TÜV Informationstechnik GmbH ㅇ TÜV Nord e.V. ㅇ Vossloh System-Technik GmbH ㅇ TÜV Product Service GmbH
프랑스	ㅇ CEA-LETI ㅇ AQL ㅇ SERMA Technologies ㅇ ALGORIEL Consulting ㅇ CEACI

※ IABG(Industrieanlagen-Betriebsgesellschaft mbH Abeteilumg ITE)
※ CCI(Competence Center Informatik GmbH Prufstelle IT-Sicherheit)
※ AQL(Alliance Qualite Logiciel)
※ CEACI(CNES-SOREP)

III. 국내 평가·인증 제도

1. 초기의 국내 정보보호제품 평가·인증 제도

국내에서는 1997년 2월 정보통신망 침입차단시스템 평가기준과 침입차단시스템 평가·인증 지침이 고시되면서 국내 평가·인증 제도가 시행되었다. 초기의 평가·인증 제도에서는 정보보호제품을 공공기관용과 민간용으로 분리하여 평가를 시행하는 이원화된 평가·인증 제도를 운영하였다. 민간용은 한국정보보호센터가 평가를 하여 평가필증이라는 것을 인증서 대신에 발급하였다. 하지만 공공기관용은 국정원과 한국정보보호센터가 동시에 평가를 시행하였으며, 평가가 성공적으로 종료되는 경우 인증기관인 국정원이 인증서를 발급하였다. 특히, 국정원에서 발급한 평가 인증서는 정보보호제품을 공공기관에 판매할 수 있는 허가증과 같은 역할을 하였다. 정보보호제품의 수요가 민간분야 보다는 공공분야가 더 크기 때문에 모든 평가신청 업체는 민간용이 아닌 공공기관용으로 평가를 신청하여 공공기관용으로는 5개의 제품이 평가인증서를 받았으나, 민간용으로 평가를 신청한 업체는 하나도 없었다.

이원화된 평가·인증 제도에서는 공공기관용으로 평가받은 제품은 민간용으로 판매할 수 없었으며 업체들이 민간용으로 평가를 신청하지 않는 관계로 민간분야에서는 평가받은 제품을 사용할 수 있는 기회가 주어지지 않았다. 또한 국정원과 한국정보보호센터가 동시에 제품을 평가하는 이유로 평가기간이 장기화될 수 밖에 없었다. 즉, 국정원에서 일정부분을 평가하고 이에 대한 보완요청서를 발급하면 센터는 업체가 보완요청해오는 부분을 다시 평가해야 하며 센터가 보완요청서를 발급하면 국정원에서 다시 보완된 부분을 평가해야 하는 어려움이 있었다. 다음은 국내 평가·인증 체계를 그림으로 나타낸 것이다.

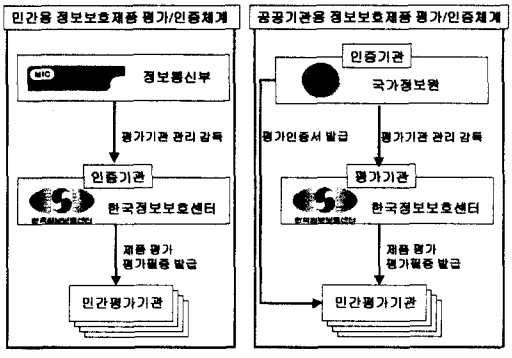

그림 1. 초기의 국내 정보보호시스템 평가·인증 체계

2. 개정된 국내 평가·인증 제도

위의 문제점들을 해결하기 위하여 국정원, 정통부 및 센터는 공공기관용과 민간용의 구분이 없는 평가·인증 제도를 구축하기 위하여 새로운 정보보호시스템 평가·인증 지침을 2000년 2월 17일 고시하였다. 새로운 평가·인증 제도에서는 한국정보보호센터가 평가기관의 역할을 수행하며 국정원이 인증기관의 역할을 수행하여 인증서를 발급한다. 특히, 공공기관용과 민간용의 구분이 없는 관계로 한번 평가를 받아 인증서를 발급받으면 민간분야와 공공분야에 모두 판매할 수 있게 된다. 따라서 국정원과 센터에서 수행되었던 중복 평가과정이 단일화되어 평가기간이 단축되는 효과가 있다.

또한 민간분야에서도 평가받은 제품을 구매하여 사용할 수 있으므로 제품의 보안성이 제 3자로부터 입증된 제품을 민간분야에서도 실제로 사용할 수 있게 됨으로써 국내 정보보호 수준을 한층 더 향상시킬 수 있는 계기를 마련하였다.

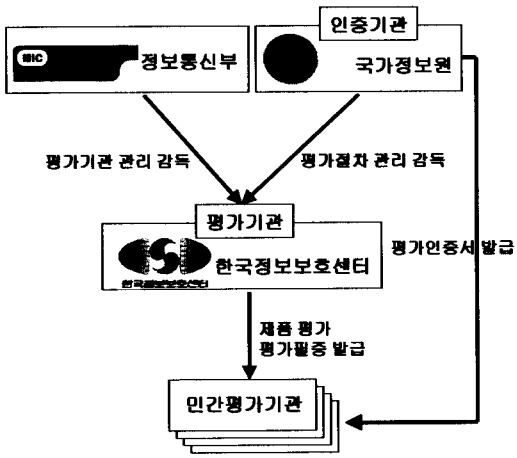

그림 2. 개정된 국내 정보보호시스템 평가·인증 체계

IV. 국내 평가·인증 제도의 개선 방향

1. 배 경

국내에서는 1998년 평가·인증 제도를 시행하여 왔으나 아직은 초보 단계라고 할 수 있다. 특히, 현재까지는 국내에 적합한 평가·인증 제도를 구축하는데 주력하였다고 볼 수 있다. 외국의 평가·인증 제도의 발전 과정을 보면 먼저 민간분야의 수요를 충족하기 위하여 민간평가기관을 설립하는 등의 노력을 하였으며 그 후 국제상호인정협정에 대비하여 평가·인증 스킴을 개발하는 등의 제도 개선을 위한 노력을 하였다.

국내에서도 정보보호산업의 수요가 2000년에 약 1400억원에 달하며 앞으로도 급속한 속도로 확장될 것으로 예측하고 있다. 따라서 업체들은 정보보호제품 평가에 많은 관심을 가지고 있으며 특히, 경쟁업체보다 빨리 평가를 받아야 시장확보에 유리한 위치를 선점할 수 있기 때문에 신속히 평가를 받기 위하여 노력하고 있다. 더불어 업체들은 더 이상 국내 시장에만 의존해서는 안되며 국외 시장을 확보하는 것이 앞으로 살아남을 수 있는 유일한 방법이라고 믿고 있다. 정부에서도 중국, 말레이시아, 이스라엘 등 외국 정부와 정보보호 분야의 협력을 위하여 많은 노력을 하고 있다. 따라서 국내에서 평가받은 정보보호제품의 인증서가 외국에서도 인정받기 위해서는 국제적으로 인정받은 국제상호인정협정에 가입할 수 있는 기반을 구축하는 것이 중요하다. 다음은 민간분야의 수요를 충족하며 국제상호인정협정에 가입하기 위하여 국내 정보보호 평가·인증 제도에서 개선되어야 할 점들을 소개한다.

2. 복수 평가기관 운영

외국의 평가·인증 제도 역시 공공기관을 위하여 제도가 구축되었다. 하지만 정보보호의 중요성과 마인드가 확산되고 민간분야에서의 수요가 급증함에 따라 민간평가기관들을 운영하게 되었다. 유럽의 국가들은 80년대 말부터 민간평가기관을 지정하여 정보보호제품들을 평가하기 시작하였다. 미국은 가장 오랜 기간 동안 평가·인증 제도를 운영하여 왔으나 최근에 TTAP을 발표하면서부터 민간분야에 대한 평가·인증 제도 운영을 위한 민간평가기관을 지정하여 운영하기 시작하였다. 현재 미국은 7개, 영국 5개, 독일 8개와 프랑스 5개의 민간평가기관을 지정하여 운영하고 있다.

국내에서도 정보보호제품 평가에 대한 업체의 관심도가 높아지며 평가의 필요성을 인지하여 평가를 신청하는 업체가 증가하고 있는 추세이다. 2년 동안의 침입차단시스템 평가를 거쳐 6개 제품이 인증서를 발급 받았으며 5개의 제품이 평가 대기 중이다. 현재 2개의 제품이 평가 신청을 위한 자문을 받고 있는 상태이다. 또한 정보통신망 침입탐지시스템 평가기준이 고시되면서 십여개의 업체들이 평가를 위한 평가자문을 신청한 상태이다. 더불어 새로운 평가기준들이 고시되어 평가 대상 제품의 수가 증가하게 되면 센터가 독립적으로 모든 제품을 평가하기에는 역부족이다. 따라서 복수의 평가기관의 운용이 불가피한 상황이다.

복수 평가기관이 운용될 경우, 한국정보보호센터와 민간평가기관과의 업무 분장이 필요하다. 한국정보보호센터는 공공기관의 수요에 따른 공공기관용 정보보호제품 평가, 평가기준 개발, 평가·인증 스킴 개발, 국제공통평가기준 수용 및 국제상호인정협정 대비 등을 주요 업무로 하며 새로이 지정된 민간평가기관은 정통부장관이 고시한 평가기준을 이용하

여 정보보호제품 평가를 그 임무로 한다.

3. 민간평가기관 인정 기준 및 인정기관 신설

정보보호제품 평가를 위하여 민간 평가기관을 지정하기 위해서는 민간평가기관이 공정하고 객관적으로 평가를 할 수 있는 능력을 보유하고 있는지를 심사하여야 한다. 외국의 경우, 민간 평가기관의 자격을 심사하여 평가기관으로 지정하는 임무를 수행하는 기관을 두고 있다. 미국의 경우 인증기관인 NIAP에서 평가기관을 지정하는 임무를 수행하고 있으며 영국은 UKAS(United Kingdom Accreditation Service), 프랑스는 COFRAC (Comite Francais d'Accreditation), 독일은 DAR (Deutscher AkkreditierungsRat) 등 별도의 기관을 지정하여 이러한 임무를 수행하고 있다[6].

이들의 인정기관들은 ISO의 표준으로 지정한 ISO Guide 25와 이를 기반으로 하는 평가기관 자격 요건을 정해두고 있다.

국내에서 민간평가기관을 평가·인증 제도에 포함하기 위해서는 평가기관을 심사할 수 있는 기준 및 평가기관의 자격 요건을 제시함은 물론 기관을 심사하여 평가기관으로 지정할 수 있는 인정기관을 두어야 한다.

4. 평가수수료 현실화

평가수수료는 정보화촉진기본법 시행령 제16조 3항에 의거 정보통신부 장관이 정한 수수료를 센터장에게 납부하도록 되어있다. 하지만 1998년 평가수수료를 책정할 당시에는 정보보호업체의 영세성을 감안하여 평가에 사용되는 장비의 감가상각비만을 고려하여 K4등급인 경우 218만원, K4E의 경우 221만원으로 책정하였다. 이는 정부에서 정보보호업체를 위한 순수 서비스 차원에서 책정된 것이라 할 수 있다. 외국의 경우에는 제품 평가에 필요한 인원 및 평가기간을 고려하여 수수료를 책정하고 있다. 영국에서 K4와 같은 수준의 등급으로 침입차단시스템을 평가받을 경우, 7개월의 기간과 약 1억3천만원의 평가수수료를 납부하여야 한다.

국제상호인정협정에 가입한 국가들 사이에서는 업체가 여러 평가기관의 수수료, 평가기간 및 얼마나 빨리 평가를 시작할 수 있는지를 고려하여 제품 평가를 위한 평가기관을 선정하며 타국의 평가기관이 업체에게 유리한 조건을 제시할 경우, 타국의 평가기관에서 평가를 받는 경우도 있다. 이는 국제상호인정협정에 가입한 어느 국가에서 평가를 받아 인증서를 발급받아도 인증서가 상호인정되기 때문이다.

국내의 경우, 1998년 이후로 정보보호산업체가 많은 발전을 거듭하여 왔으며 금년 매출 규모가 1400억원에 이르는 등 급성장하고 있다. 특히, 평가수수료가 저렴하며 평가 신청된 순서에 의해 제품을 평가한다는 제도적 취약점을 이용하여 제품 개발이 완료되지 않은 상태에서 평가를 신청하여 평가과정에서 제품을 수정 또는 개발하는 경향이 있다. 따라서 평가수수료 현실화는 필연적으로 이루어져야 한다. 또한 국내에 민간 평가기관이 지정되고 이들이 실제 정보보호제품을 평가할 수 있게 된다면 현재의 평가수수료만으로는 평가기관을 운영할 수 없는 상태이다. 따라서 외국과 같이 제품 평가에 투입되는 인원 및 기간을 고려한 수수료의 자율화가 도입되어야 한다.

5. 국제공통평가기준 수용

국내에서는 1998년에 고시되었으며 2000년 2월에 개정된 정보통신망 침입차단시스템 평가기준과 2000년 7월에 고시된 정보통신망 침입탐지시스템 평가기준을 이용하여 침입차단시스템과 침입탐지시스템을 평가하고 있다. 하지만 컴퓨터 및 통신 관련 기술의 발전으로 인하여 매우 다양한 정보보호제품이 개발되고 있으며 앞으로는 더욱 더 다양한 정보보호제품이 개발될 것으로 예측된다. 특히, 침입차단시스템 평가기준이 개발되고 고시될 당시만 하여도 정보보호제품이라고 하면 침입차단시스템이 가장 많이 거론되어 왔으나 현재 전자상거래를 비롯한 응용분야가 다양해지면서 CA 서버, 스마트카드, 침입탐지시스템, 사용자 인증 제품, VPN 등 많은 제품이 개발되어 판매되고 있는 상황이다.

미국의 경우, 한국과 같이 제품별 평가기준을 이용하여 평가·인증 제도를 운영하여 왔으나 제품이 다양해짐으로 인하여 모든 종류의 정보보호제품을 평가할 수 있는 평가기준 개발에 착수하여 FC (Federal Criteria)라는 기준을 개발하였으나 실제 제품 평가에는 사용하지 않았다. 유럽은 이미 ITSEC을 이용하여 다양한 제품을 평가할 수 있는 기준과 기반을 구축하였다. 최근에는 미국 및 유럽 국가들이 다양한 정보보호제품을 평가할 수 있는 단

일의 평가기준인 국제공통평가기준을 개발하여 활용하고 있다. 심지어는 국제상호인정협정에 가입하지 않은 국가들도 국제공통평가기준을 국가 표준으로 제정하여 정보보호제품 평가에 사용하고 있다.

현재까지 개발된 다양한 정보보호제품별로 평가기준들을 개발하기에는 인력이나 예산 면에서 볼 때 역부족이다.

더불어 앞으로 개발될 다양한 제품들을 고려하여 평가기준을 개발한다는 것은 더욱 더 어려운 일이다. 국제공통평가기준을 사용하는 것은 다양한 정보보호제품을 평가할 수 있는 단일 평가기준을 사용하게 되는 것이며 동시에 국제상호인정협정 가입에 대비하는 일석이조의 이익을 얻을 수 있게 된다.

6. 평가·인증 스킴 개발

평가·인증 스킴이란 평가신청자나 평가된 제품의 사용자에게 자국의 제도에 대한 신뢰도를 높이기 위하여 평가·인증 제도, 평가기준, 평가 방법론, 평가 관련 기관의 임무 등을 설명한 문서들을 의미한다. 이는 평가제도의 객관성 및 공정성을 타인에게 입증하기 위하여 사용된다.

스킴은 국제상호인정협정 가입신청 시 제출해야 하는 문서들 중 하나이다. 국제상호인정협정에 새로이 가입하기 위해서는 사전에 가입되어 있는 모든 국가들의 동의를 얻어야 한다. 이는 곧 가입되어 있는 모든 국가들로부터 신뢰를 받아야 한다는 것을 의미한다. 따라서 스킴은 단순히 제도를 설명하는 역할 뿐만 아니라 실제로 다른 사람들에게 평가·인증 제도에 대한 신뢰를 얻기 위하여 사용되는 가장 중요한 도구라고 할 수 있다.

V. 결 론

본 고에서는 미국을 비롯하여 영국, 프랑스, 독일 등 유럽 국가들의 평가·인증 스킴에 대해 알아보았으며 새로운 환경에 적응하기 위한 각 국가의 노력들을 살펴보았다.

한국은 이중화된 평가·인증 체계에서 단일화된 평가·인증 체계로 전환하였다. 하지만 다양화 되고 있는 정보보호제품을 평가하며 평가 수요를 충족하고 국제상호인정협정 가입할 수 있는 여건을 구축하기 위해서는 앞으로도 많은 노력을 하여야 한다.

특히 평가·인증 제도를 운영하고 있는 국가들의 know-how와 경험을 토대로 현실적이며 실용적인 평가·인증 제도를 구축하여야 한다.

이는 단순히 외국의 사례를 따라 제도를 구축하기보다는 이들의 경험을 바탕으로 국내 환경에 적합하면서도 국제화에 적합한 제도 구축이 중요하다.

급변하는 국내·외 환경에 적응하기 위해서는 복수의 평가기관 설립, 인정기관 지정, 평가기관 인정기준 개발, 평가수수료 현실화, 국제공통평가기준 수용 및 평가·인증 스킴 개발 등 앞으로 해결해 나가야 할 많은 과제들이 있다.

참 고 문 헌

[1] 이유신, "CCRA 최근동향 및 향후 전망", *한국정보보호센터*, 정보보호뉴스, 통권35호, 6-9, 2000. 8.

[2] 정보보호 평가기준 개발 최종보고서, 한국정보보호센터, 1999

[3] 정보보호시스템 평가체계, 한국정보보호센터, 1997

[4] http://www.radium.ncsc.mil/tpep/ttap/index.html

[5] http://niap.nist.gov/cc-scheme/

[6] 국내·외 정보보호시스템 평가 가이드, 한국정보보호센터, 1998

[7] 정보보호 평가기준 개발 제1차년도 연구개발 결과보고서, 한국정보보호센터, 1998

[8] 정보보호시스템 평가수수료 산정 방안연구, 한국정보보호센터, 1998

[9] 침입차단시스템 평가수수료 산정 방안연구, 한국정보보호센터, 1997

[10] http://www.radium.ncsc.mil/tpep/tpep.html

[11] http://www.itsec.gov.uk/

[12] http://niap.nist.gov/cc-scheme/iccc/

[13] 김석우, "국제공통평가기준(CC) 소개", 한국정보보호센터, 정보보호뉴스 통합권, p.180, 1999.

[14] 김학범, "미국의 국제공통평가기준(CC) 수용 현황", 한국정보보호센터, 정보보호뉴스 통합권, p.181-183, 1999.

[15] 이완석, "ISO/IEC JTC 1/SC 27/WG 3 표준화 현황 소개", 한국정보보호센터, 정보보호뉴스 통합권, p.184-185, 1999.

〈著者紹介〉

이 완 석(Wan S. Yi)
1991년 5월 : Va. Tech 전산과학과 졸업(이학사)
1994년 8월~1996년 7월 : 현대정보기술 CAD/CAM 사업부 사원
1998년 8월~현재 : 동국대학교 정보보호학과 석사과정
1996년 7월~현재 : 한국정보보호센터 선임연구원
〈관심분야〉 모빌코드 보안, 스마트카드 보안, 정보전, 네트워크 보안, PKI

이 경 구(Koung-goo Lee)
1975년~1982년 : 한양대학교 무시재료공학과 졸업(공학사)
1984년~1986년 5월 : University of central arkansas 전산학과 졸업(이학사)
1986년~1988년 5월 : University of arkansas 전산학과 졸업(이학석사)
1989년~1996년 5월 : Kent State University 전산학 졸업(이학박사)
1996년~현재 : 한국정보보호센터 평가기준팀 팀장
〈관심분야〉 정보보호, 시스템 성능분석, 네트워크 프로토콜