□특집□

정보보호시스템 평가기준 및 제도

김 영 문†

◈ 목 차 ◈

1. 서 론

새천년은 지식과 정보가 국가경쟁력의 원천이 되는 지식혁명의 시대로, 지식·정보화가 국가경제와 사회발전을 결정하는 핵심 패러다임이 되고 있다.

하지만 이러한 지식·정보화가 진전될수록 해킹, 바이러스 유포 등 정보화역기능도 급격히 증가하고 있어, 정부에서는 관련 법과 제도를 정비하고 조직을 보강하는 등 정보화에 따른 역기능을 방지하기 위한 종합적인 대책을 마련하여 추진하고 있다.

이중에서 특히 현재 사회문제로 크게 대두되고 있는 정보시스템에 대한 해킹에 효과적으로 대비할 수 있도록 안전·신뢰성이 검증된 정보보호시스템을 국내 시장에 보급하고자 '98년 2월부터 평가제도를 운영하고 있다.(정보화촉진기본법 제15조 및 동법시행령 제16조에 따라 정보보호시스템의 성능과 신뢰도에 관한 기준을 고시하여 해당제품을 제조 및 수입하고자 하는 자에게 동 기준의 준수를 권고)

현재 정보보호시스템중 가장 많이 사용되고 있는 침입차단시스템에 대한 평가를 수행하여 현재까지 4개제품을 평가하여 공공기관에 보급하고 있다.

2. 국내 평가제도 운영현황 및 주요개정 사항

그동안 정통부에서는 정보보호시스템의 성능과 신뢰도에 관한 평가기준을 정하여 정보보호업체에서 개발한 침입차단시스템의 보안성 평가를 실시하여 왔으며, 2000. 2월 현재 시큐어소프트(주)의 SecureShield, 어울림기술(주)의 SecureWorks, 한국정보공학(주)의 InterGuard, 퀵신시스템(주)의 화랑, 시큐어소프트(주)의 수호신 등 5개의 제품이 K4등급을 획득한 바 있다.

정보보호시스템에 대한 평가기준이 강화되고 평가대상이 확대됨에 따라, 앞으로 해당 업체들의 기술력을 향상시켜 정보보호시스템의 품질향상을 촉진하고, 정보보호시스템의 이용자는 보다 안정성이 향상된 정보보호시스템을 구입하여 사용할 수 있게 되었다.

국가로부터 보안성을 인정받은 정보보호 제품은 이용자들의 신뢰도가 높기 때문에 국내시장은 물론 해외시장에 진출하는 데 상대적으로 유리할 것으로 전망된다. 또한, 정보보호시스템에 대한 평가지침 및 기준이 새롭게 개정됨에 따라, 앞으로 보다 더 신뢰할 수 있는 정보보호시스템의 개발·이용을 촉진시킬 것으로 보인다.

† 정회원 : 정보통신부 정보보호산업과 사무관

(침입차단시스템 평가현황)

제품명	개발 업체명	신청 등급	평가 현황
SecureShield-Firewall V1.0	시큐어소프트	K4	'98.11. 평가 완료
SecureWorks V1.0	어울림정보기술	K4	'99. 1. 평가 완료
인터가드 V1.5	한국정보공학	K4	'99. 6. 평가 완료
화랑 V2.0 (공공기관용)	퀀신시스템	K4	'99. 12. 평가 완료
수호신 V2.0 for Solaris 2.5.1(공공기관용)	시큐어소프트	K4E	'99. 12. 평가 완료
매직캐슬 V1.0 (공공기관용)	매직캐슬	K4	평가 중
SecureWorksV2.0 for Solaris 2.7(공공기관용)	어울림정보기술	K4	평가 중
수호신 V3.0 for AIX4.3(공공기관용)	시큐어소프트	K4E	평가 중
SecureWorksV2.0 for Solaris 2.7 on sparcs	어울림정보기술	K4	평가 중
수호신 V3.0 for Solaris 2.7 on .X86	시큐어소프트	K4E	평가 중
수호신 V3.0 for Solaris 2.7 on sparcs	시큐어소프트	K4E	평가 중

즉, 해당제품의 개발자에게는 정보보호시스템의 품질향상을 촉진하여 간접적으로 개발업체들의 기술력 향상을 유도하고 제품의 안전·신뢰성을 높여 국내 정보보호산업을 활성화하고 국제 경쟁력 확보에 큰 기여를 하고 있으며, 실제로 정보보호시스템 사용자에게는 적정한 정보보호시스템 구매지침을 제공하게 되는 등, 전체적으로 동 제도를 통해 우리는 정보보호시스템 보안기능의 향상을 유도하고 해킹 등에 대비한 국가 및 민간의 보안유지비용의 상당한 절감효과가 기대할 수 있겠다.

사실 외국제품이 대다수를 차지하고 있던 국내 정보보호시장에서, 아직 영세한 국내 정보보호산업이, 동 평가제도를 통하여 평가기관의 전문적인 기술검증을 받음으로써 업체들의 개발기술력의 향상되고 제품의 완성도를 높여 최종적으로 제품의 시장점유율을 크게 높였다고 할 수 있다.

2.1 침입차단(방화벽)시스템 평가기준 개정 주요내용

침입차단시스템은 현재 대두되고 있는 인터넷상의 해킹을 원천 차단하기 위해 외부에서 내부망에 무단접속하려고 하는 사용자의 신분을 확인하여 불법침입을 차단하고, 전송하는 데이터의 무결성, 기밀성 등을 제공해주는 필수적인 정보보호시스템이라고 할 수 있다.

이러한 중요한 정보보호시스템의 안전·신뢰성을 확보하고 해당 시스템을 도입하고자 하는 기관에 적정수준의 구매지침을 주고자, 정보보호전문기관인 한국정보보호센터에서 평가신청한 제품에 대해 성능과 신뢰도에 따라 해당 평가등급(7등급(K1~K7))을 부여하고 있었는데, 개정된 기준에서는 침입차단시스템 평가기준의 보안기능(신분확인, 접근통제, 무결성, 비밀성, 감사기록 및 추적, 보안관리 기능등), 보증요구사항(보안기능이 정상적으로 동작하는지 확인하는데 필요한 요구사항) 일부기능의 개선이 포함되었다.

즉, 암호키 관리 및 안정성이 검증된 알고리즘 사용 권고 및 시스템의 신뢰성을 높이기 위한 수단 등 전반적으로 보안성 평가기준을 강화하여 정보보호기술의 발전속도를 반영하고 평가제도의 신뢰도를 높이고 관련업체의 평가작업의 편의를 최대한 반영하고자 하는 것이 주요 골자라 할 수 있다.

2.2 정보보호시스템 평가·인증지침 개정 주요내용

또한, 정보보호시스템에 대한 평가원칙 및 절차를 규정하는 정보보호시스템 평가·인증지침을 개정하여 공공기관용 및 민수용평가의 구분을 없애 평가기관를 한국정보보호센터로 단일화하고 평가지침을 침입차단시스템에서 전체 정보보호시스템으로 확대하였다.

이러한 평가대상확대, 평가업무 일원화와 더불어 특히, 그동안 비공개적으로 수행하던 암호관련 업무를 동지침에서 규정함으로써 향후에는 국가정보원의 암호논리 및 민간업체의 암호제품을 평가하도록 하여 사실상 민간 암호이용기술이 발전을 촉진할 수 있는 역할을 하리라 기대된다.

새 지침에 따라, 침입차단/탐지시스템, 스마트카드 등의 보안성 평가를 원하는 업체는 한국정보보호센터에 평가신청서와 관련서류를 제출하면 새로 개정된 지침 및 기준에 따라 평가서비스를 받게 되며, 평가제도 개정이전에 진행중인 신청제품에 대해서도 본 규정이 소급적용된다.

새로 개정된 평가제도에서는 침입차단시스템(방화벽:firewall) 한 제품에 머물러 있는 평가대상을 침입탐지시스템, 스마트카드, 전자상거래 인증서버 등 모든 정보보호시스템으로 대폭 확대하고, 공공기관용은 국가정보원이, 민수용은 한국정보보호센터로 이원화되어 있던 평가기관을 한국정보보호센터로 일원화된다. 또한 평가결과에 대해서는 국가정보원이 최종적으로 인증을 하도록 하였다.

(주요 개정내용)

구 분	개 정 전	개 정 후
평가정책 수립기관	○정보통신부	○정보통신부
평가대상	○침입차단시스템	○모든 정보보호시스템
평가기관	○민간용: 한국정보보호센터 ○공공기관용: 국가정보원	○한국정보보호센터
인증기관	○민간용: 평가위원회 ○공공기관용: 국가정보원	○국가정보원 (인증위원회)

3. 외국 동향

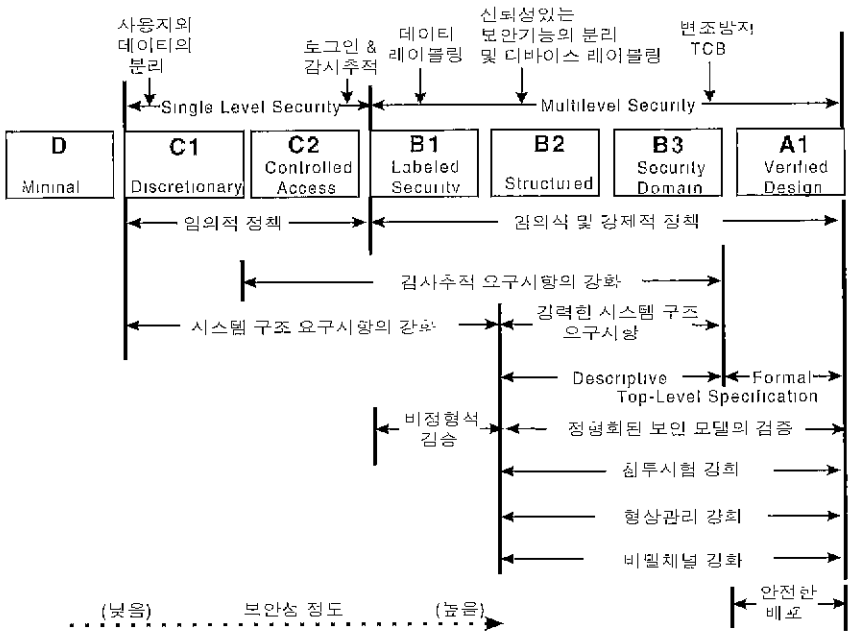
주요 선진국들은 80년대 초반부터 정보보호시스템 평가제도를 실시하고 있으며 최근 민간평가기관을 지정하여 증가하는 평가수요에 대처하고 있으며 상대국 평가제품을 인정하여주는 국제상호인정협정을 체결함

미 국

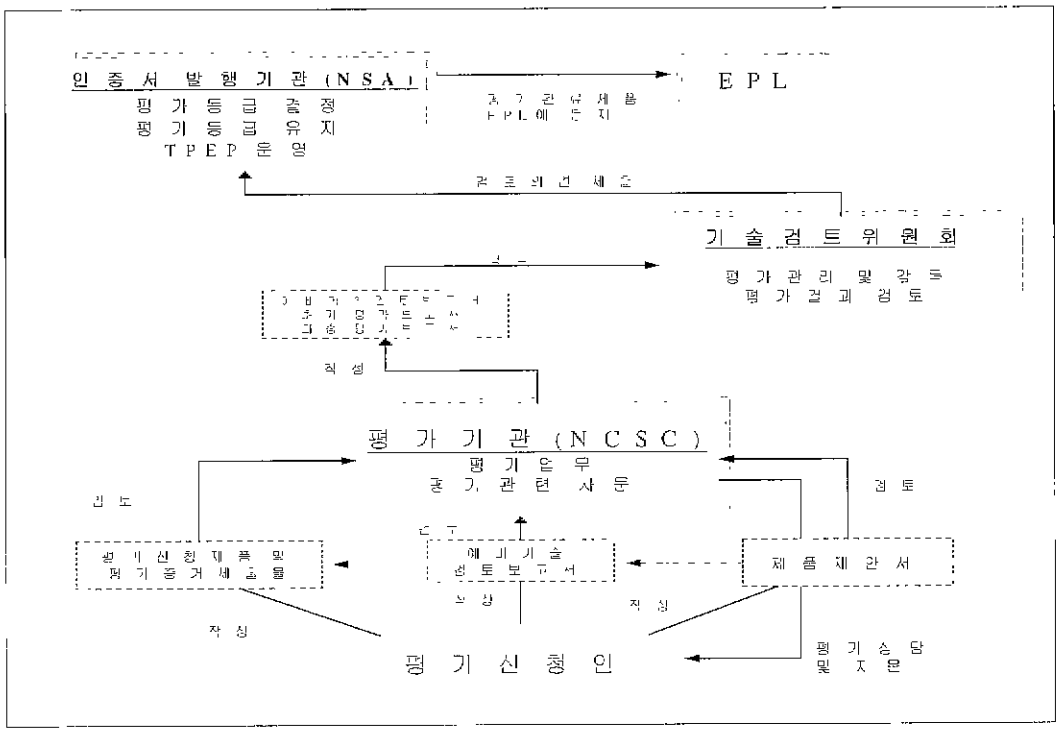
'83년부터 컴퓨터시스템부터 평가하기 시작하여 네트워크, 데이터베이스, 침입차단시스템, 사용자인증시스템 등으로 평가품목을 확대하고 있으며, 평가기관은 국가용을 평가하는 NCSC(국가전산보안센터)와 민수용을 평가하는 민간평가기관(7개)으로 구분되어 있으며, 평가결과의 적합여부를 판단하는 인증기관은 국가용을 인증하는 NSA와 민수용을 인증하는 평가감독위원회(NSA와 NIST가 공동구성)으로 구분되어 있다.

실제 평가작업을 위해 1985년 국방부 표준으로 TCSEC을 개발하였으며, 1987년에는 이를 네트워크 제품에 적용하기 위한 TNI가 만들어졌고, 1991년에는 데이터베이스에 적용하고자 TDI가 개발되어 이에 따른 평가가 이루어지고 있으며, 이들 기준에 의거한 평가를 수행하기 위하여 TPEP (Trusted Product Evaluation Program)을 개발하여 이에서 규정한 절차와 방법에 따라 평가를 수행하고 있다.

TPEP에는 기술검토, 강력한 예비기술검토, 등급유지계획 및 문서화 등 평가절차를 규정하고 있으며 이 절차에 따라 1983년부터 NSA가 주축이 되어 평가를 시행하고 있다으며, 1997년부터는 C2급 이하의 평가등급을 갖는 정보보호시스템의 평가는 민간기관에서 수행할 수 있도록 하는 TTAP (The Trust Technology Assessment Program)을 시범적으로 시행하고 있다.



(TCSEC의 등급별 특성)



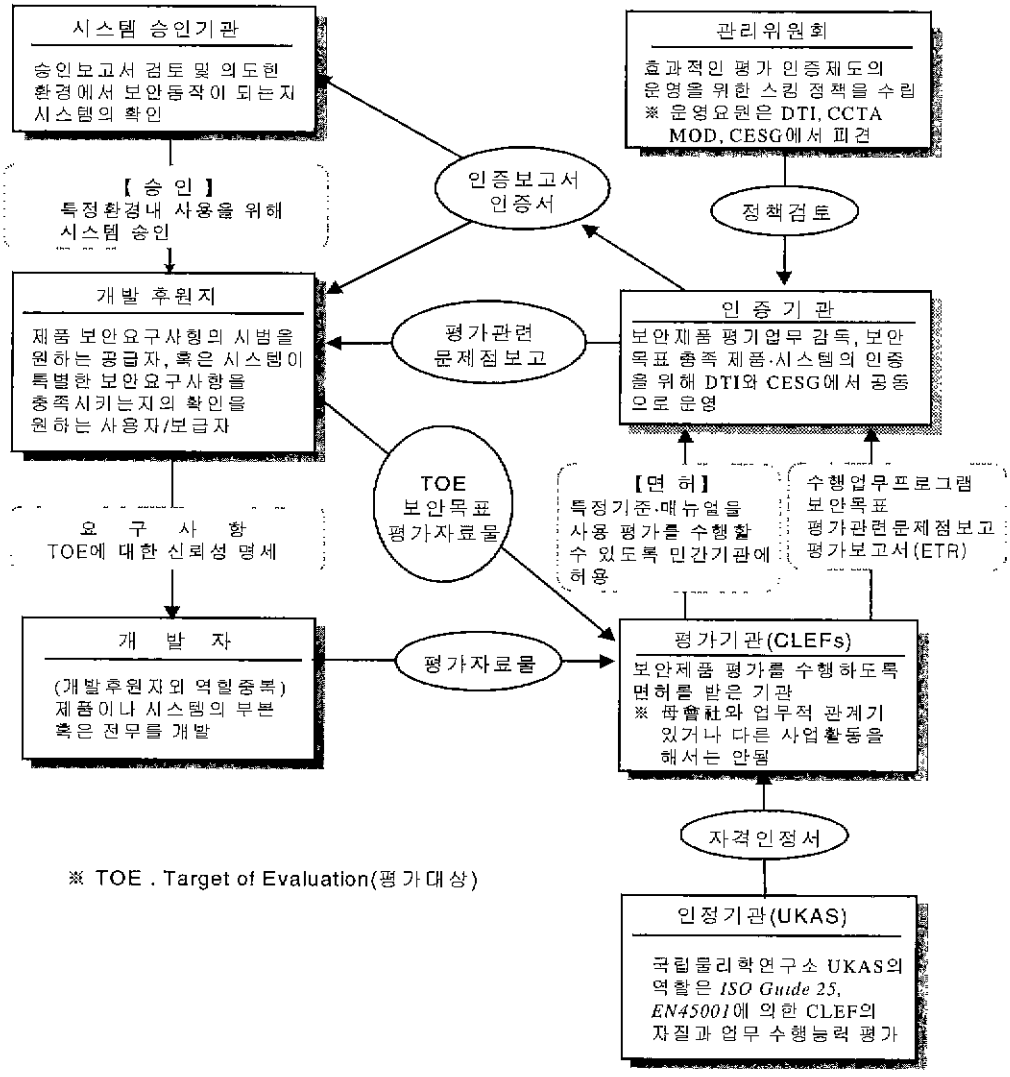
(TPEP에서의 평가·인증체계도)

유 럽

'80년대 중반부터 영국, 독일, 프랑스 등 유럽 국가들은 유럽공통의 평가기준(ITSEC)에 의하여 평가를 실시하여 유럽내에서 평가된 제품을 상호 인정하기 위하여 민간평가기관을 지정(영국 5개, 독일 7개)하여 평가하고 있다.

ITSEC은 TCSEC과는 달리 단일 기준으로 모든 정보보호 제품을 평가한다. 따라서 보안기능은 개발자가 제품이 사용될 환경을 고려하여 보안 기능을 설정하거나 TCSEC 혹은 독일의 ZSIEC(Criteria for the Evaluation of Trustworthiness of Information Technology Systems)에서 미리 정의한 보안기능을 사용토록 하였으며, 제품에 대한 평가는 보증부분만 가지고 수행이 된다

ITSEM은 ITSEC을 운영하는 유럽의 4개국이 ITSEC 기준 및 평가 철학을 통일함으로써 국가간 평가업무와 평가결과에 대한 상호 교류 및 인정을 위해 개발되었는 데, 여기에는 평가자의 편



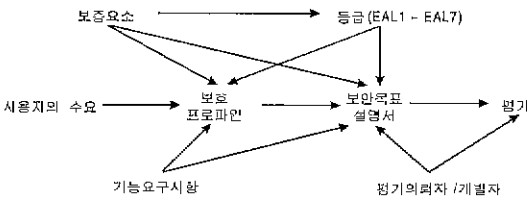
※ TOE . Target of Evaluation(평가대상)

(영국의 평가·인증 체계도)

견을 배제하는 공정성(Impartiality), 평가자의 주관적 요소 및 사견을 최소화하는 객관성(Objectivity), 동일한 평가기관에서 같은 평가대상물을 반복하여 평가해도 똑같은 평가결과가 나와야 한다는 반복성(Repeatability), 여러 개의 평가기관에서 하나의 평가대상물을 반복하여 평가해도 똑같은 평가결과가 나와야 한다는 재생성(Reproducibility)을 평가원칙으로 강조하고 있다.

국제공통평가기준(CC)

CC의 개발목적은 현존하는 다양한 평가기준의 조화(Harmonization)를 통하여 평가결과의 상호인정(Mutual Recognition)을 추진하기 위한 것이다. 즉, CC는 정보보호시스템의 보안기능 요구사항과 이를 평가하는 동안 적용하는 보증요구사항에 대한 공통의 집합을 정하여 서로 독립적으로 수행한 평가결과들을 호환할 수 있도록 하기 위한 것이다.



(CC 평가체계)

사용자는 평가결과를 통하여 해당 정보보호시스템이 자신의 응용에 적절한 보안기능 요구사항과 보증요구사항을 갖추고 있는지를 결정할 수 있다. 또한 사용중에 내재하는 보안위협에 대하여 그 정보보호시스템이 어느 정도의 내구성을 가지고 있는지 결정할 수 있다.

CC는 크게 5가지 부분으로 구성되어 있는데 Part 1에서는 소개 및 일반모델을 제시하고 있으며 Part 2는 보안기능 요구사항, Part 3은 보증 요구사항, Part 4는 이미 정의된 보호 프로파일을 기술하고 있으며 Part 5에서 보호 프로파일을 등록하는 절차를 포함하고 있으며, ISO/IEC JTC 1/SC27/WG3에서 '99.6월에 CC를 국제표준으로 채택되었다.

4. 평가제도 발전방안

정보보호시장의 성장추세에 따라 정보보호업체들의 보호제품평가수요가 급증하고 있으나, 현재의 관련 평가인력의 부족으로 정보보호산업육성에 지장을 초래하여 평가인력확대가 시급하다. 특히 현재는 침입차단시스템 한 제품을 평가하고 있으나, 앞으로 침입탐지시스템, 스마트카드 등 평가신청이 폭주할 것으로 예상된다.

(CC의 보안기능 요구사항)

클래스명	클래스 제목	설명
FAU	보안감사(Security Audit)	보안활동과 관련된 정보를 감지, 기록, 저장, 분리
FCO	통신(Communication)	데이터를 교환하는 주체의 신원을 감지
FCS	암호지원(Cryptographic Support)	암호 운용 및 키관리
FDP	사용자 데이터 보호	사용자 데이터의 보호
FIA	식별 및 인증	사용자의 신원확인 및 인증
FMT	보안관리(Security Management)	TSF 데이터, 보안속성, 보안기능의 관리
FPR	프라이버시(Privacy)	허가되지 않은 사용자에 의한 개인정보의 도용방지
FPT	TOE 보안기능의 보호	TSF 데이터의 보호 및 관리
FRU	자원활용(Resource Utilization)	TOE의 가용자원을 확보
FTA	TOE 접근(TOE Access)	TOE에 대한 사용자 세션의 보호
FTP	안전한 경로/채널	사용자와 TSF간 혹은 TSF 간의 안전한 통신채널확보

(CC의 보증요구사항)

클래스명	영문 설명	설명
ACM	형상관리	TOE의 무결성이 유지되고 있는지를 확인
ADO	배포와 운영	TOE의 안전한 배포, 설치, 운영에 필요한 수단, 절차 및 표준을 확인
ADV	개발(Development)	TOE 개발 과정의 일치성 및 완벽함을 확인
AGD	설명서(Guidance Documents)	TOE의 안전한 운영을 위한 지침서를 확인
ALC	생명주기 지원	TOE의 생명주기와 관련된 사항을 확인
ATE	시험(Tests)	TOE가 기술요구사항을 만족하는 지를 확인
AVA	취약성 분석 (Vulnerability Analysis)	TOE의 개발과정 중에 발견되지 않은 취약성, 사용자에 의한 오용 등 잠재적인 취약성을 확인
APE	보호프로파일 평가	PP가 완전하고 모순이 없으며, 기술적으로 충분함을 보임
ASE	보안목표명세서 평가 (Security Target Evaluation)	ST가 완전하고 모순이 없으며, 기술적으로 충분함을 보임
AMA	보증의 유지 (Maintenance of assurance)	TOE나 보안환경이 변화에도 ST를 지속적으로 만족시킴을 보임

'99년의 경우 1개제품당 3명의 전문인력이 평균 7~8개월이 소요되었으며, 장기간의 평가소요기간이 업체들에 부담으로 작용하였다. 참고로 미국(NCSC)은 100여명, 영국(Logica)은 200여명의 평가인력(추정)을 확보하고 있는 데, 국내의 경우는 고작 14명에 불과하여 향후 민간평가기관 도입 검토 등과 더불어 한국정보보호센터의 평가관련 조직의 대폭적인 확대가 필수적이다.

또한 정보보호시스템의 평가품목을 지속적으로 확대하여 당장 2000년도내에 스마트카드, 침입탐지시스템, 전자상거래 인증서버 등의 평가대상 품목에 대하여 평가기준을 마련하여 평가를 실시할 예정이며, 앞서 언급한 국제공통평가기준의 타당성 분석을 위해 정통부, 국가정보원, 정보보호센

(주요 국가의 정보보호시스템 평가·인증체계)

	미 국	캐나다	영 국	독 일	한 국
인정기관	NSA, NIAP	Standard Council of CANADA	UKAS	COFRAC	-
인증기관	NSA, NIAP	CSE	CESG, DTI	BSI	국정원
평가기관	국가용 : NCSC 민간 :7개의 TEF	CCEF	국가용 . CESG 민간 5개의 CLEF	국가용 : BSI 민간 : 7개의 ITSEF	한국정보보호센터
평가제도 시행년도	'83	'90	국가용 : '85 상 용 : '89	국가용 : '89 상 용 '93	'98
강제성	권 고	권 고	권 고	권 고	권 고
평가기준 (등급)	TCSEC (D, C1, C2, B1, B2, B3, A1)	CTCPEC (T0 ~ T7)	ITSEC (E0 ~ E6)	ITSEC (E0 ~ E6)	침입차단 시스템 평가기준 (K1 ~ K7)
	CC (EAL1~EAL4)	CC (EAL1~EAL4)	CC (EAL1~EAL4)	CC (EAL1~EAL4)	
평가지침서	TPEP, TTAP, CCEVS(작업중)	TPEP	ITSEM	ITSEM	정보보호시스템 평가지침

터, 외부전문가 등으로 평가제도 발전방안 연구반을 구성하여 정보보호제품의 국제경쟁력 제고를 위한 국제공통평가기준('99.6, ISO표준) 수용 등 평가제도 발전방안을 지속적으로 연구해 나가고, 중장기적으로는 국내에서도 외국의 경우처럼 민간평가기관 도입을 추진할 수 있도록 기초 환경분석 작업연구가 선행되어야 하겠다.

참고문헌

'98~'99년 한국정보보호센터, 정통부 발간 정보보호보호시스템 평가기준, 체계, 방법론 등의 보고서 참조.

김 영 문

1997년 숭실대학교 전자계산학과 학사
1998년-현재 정보통신부 근무 (기술고시32회)
정보화기획실 정보보호산업과 사무관

담당업무 : 정보보호기술개발 및 정보보호시스템 평가제도