TTA표준 소개

국제 공통 평가기준(TTAE.CC-99.031, 032, 033)

조규민 · 한국정보보호진흥원 선임연구원

1. 표준 추진 배경

정보기술의 발달과 정보화의 확대로 인하여 정당한 사용자에 의한 정보의 공유에 대한 보장과 중요 자산으로서 정보보호가 중요한 문제가 되고 있다. 특히, 정당하지 않은 사용자로부터 정보를 보호하기 위해 정보보호 대책의 일환으로 정보보호시스템이 도입되어 운영되고 있다. 이러한 정보보호시스템은 다른 응용서비스 제품과 달리 사용자 신뢰를 획득하기 위하여 정보보호제품으로서의 보안기능에 대한 정확성(Correctness)과 효율성(Effectiveness) 검증을 통하여 제품의 신뢰성에 대한 보증이 요구된다.

선진 각국은 이러한 정보보호시스템의 보안성에 대한 신뢰성 확보를 위하여 국제 공통 평가기준을 개발하고 공정하고 객관적인 평가를 시행할 수 있는 평가체계를 구축하여 왔다. 특히 미국, 영국 등 선진국에서는 1980년대 초부터 국가기관에서 활용하는 정보시스템의 보안성을 평가하기 위하여 평가(Evaluation) · 인증(Certification)제도를 활용하여 왔다. 1990년대에 들어 국제적으로 신뢰 · 인정할 수 있는 평가기준의 개발이 요구되어 미국, 영국 등 6개국은 모든 정보시스템의 보안성 평가에 적용될 수 있는 평가기준의 개발을 추진하여 1998년 국제 공통 평가기준(Common Criteria) 버전2.0을 개발하였고, 1999년 6월 ISO/IEC에서 버전 2.1을 국제표준(ISO/IEC 15408)으로 제정하였다. 국제 공통 평가기준은 현재 대부분의 선진국에서 시행되고 있는 정보보호시스템 보안성 평가 · 인증제도에 적용되고 있으며, 이에 근거한 평가결과에 대한 상호인정협정(CCRA : Common Criteria Recognition Arrangement)에 미국, 영국, 프랑스, 독일, 캐나다, 호주, 뉴질랜드, 네덜란드, 이탈리아, 그리스, 핀란드, 노르웨이, 스페인, 이스라엘, 스웨덴, 오스트리아 등 16개국이 가입되어 있다.

국내에서는 1998년 침입차단시스템 평가기준과 평가 · 인증지침서를 근거로 보안성 평가를 시행하였고, 2000년 침입탐지시스템 평가기준을 고시하고, 정보보호시스템 평가 · 인증 지침을 개정하여 평가대상 제품을 확대하기 시작하였다. 또한, 향후 CCRA 가입 등을 고려하여 국제 공통 평가기준의 도입을 추진하여 CC 버전 2.1을 2001년 12월 국제 공통 평가기준(TTAE.CC-99.03)으로 제정하였고, 2002년 8월 한글화된 정보보호시스템 공통 평가기준(정보통신부 고시 제2002-40)을 국내 정보보호시스템 평가기준으로 고시하였다. 그리고 공통 평가기준의 평가를 시행할 수 있도록 평가 · 인증지침 개정안을 고시하여 향후 모든 제품에 대한 평가시행을 확대할 수 있는 제도의 근거를 마련하였다.

2. 국제 공통 평가기준의 국제표준화 과정

미국, 영국, 프랑스, 독일, 캐나다 그리고 네덜란드가 1993년에 국제 공통 평가기준 개발을 위하여 Common Criteria Project Sponsoring Organization을 구성하고, 각국 평가기준의 개념상 그리고 기술상의 차이점을 조화시켜 CC를 개발하게 되었고, 동시에 ISO/IEC JTC 1/SC 27/WG 3과 연계하여 1999년 9월 CC 버전 2.1(ISO/IEC 15408)을 완성하여 국제표준으로 제정하였다. 그리고 ISO/IEC 15408로 제정되는 과정에서 약간의 수정을 거치고 현재 CC version 2.1(2000. 1. 30 업데이트)에 이르렀다. 이와 같은 활동은 아래에 열거된 6개국의 7개 정부기관에 의해 만들어진 Common Criteria Project Sponsoring Organisation(CC 프로젝트 지원기구)에 의해 추진되어 왔다.

3. TTAE.CC-99.03 내용

가. 표준 개요

TTAE.CC-99.03은 3부로 구성되어 있다. 제1부에서는 정보보호시스템 평가기준에 대한 소개 및 일반 모델(Introduction and general model)을 제시하고 있으며, 제2부는 보안기능 요구사항(Security functional requirements), 제3부는 보증 요구사항(Security assurance requirements)을 기술하고 있다. 제2부의 부록에서는 보안기능 요구사항에 대한 부연설명을 기술하고 있다. TTAE.CC-99.03의 제2부와 제3부는 정보보호시스템이 제공해야 하는 보안기능 및 보증 요구사항을 기술하고 있으며, 개발자는 기술된 요구사항을 참조하여 정보보호시스템을 개발할 수 있다.

TTAE.CC-99.03에서 등급은 보증 요구사항만으로 구별되는데 EAL1 ~ EAL7의 7등급으로 구성되어 있다. 각각의 EAL(Evaluation Assurance Level)은 적절한 수준의 보증 요구사항을 묶어놓은 것으로 절

[표 1] 국제 공통 평가기준 개발참여 기관

지역	국가명	참여기관명
북미	미국	o National Security Agency(NSA) http://www.radium.ncsc.mil/tpep/ o National Institute of Standards & Technology(NIST) http://csrc.nist.gov/cc
	캐나다	o Communications Security Establishment(CSE) http://www.cse-cst.gc.ca/cse/english/cc.html
유럽	영국	o Communications and Electronics Security Group(CESG) http://www.cesg.gov.uk/cc.html
	프랑스	o Service Central de la Sécurité des Systémes d'Information(SCSSI)
	독일	o Bundesamt für Sicherheit in der Informationstechnik(BSI) http://www.bsi.bund.de
	네덜란드	o Netherlands National Communications Security Agency (NLNCSA) - http://www.tno.nl/instit/fel/refs/cc.html

대적인 등급체계를 의미하지는 않는다. 예를 들어, 한국에서 적용할 수 있는 KEAL(Korean EAL : 가칭) 등급을 새로 만들 수 있으며, 7개의 등급으로 구분하지 않을 수도 있다. 그러나, 평가결과를 일반적으로 인식하게 하고 세계적으로 통용될 수 있도록 하려면, 사실상 새로운 등급체계를 부여하기는 어렵다. 또한, CCRA와 같은 평가 · 인증결과에 대한 상호인정 협정에서도 EAL4 이하에 대해 적용하도록 규정하고 있으므로, 표준에서 제시된 등급체계가 일반적으로 사용되고 있다. 표준에서 제시된 등급체계의 다른 특징은 EAL3+ (EAL3 augmented라고 불림)와 같이 EAL3의 보증 요구사항에 필요한 보증 요구사항을 추가한 등급을 허용하고 있다는 것이다. 이러한 중간단계의 등급으로 평가된 제품이 많이 나타나고 있다.

TTAE.CC-99.03은 CC 평가기준을 활용한 평가체계를 1부에서 제시하고 있다. 평가체계는 평가기준과 기준에 의한 평가를 실제로 행하는 평가방법론(Evaluation Methodology) 및 평가스킴(Evaluation Scheme)에 의하여 이루어진다. 평가결과간의 호환성을 높이기 위하여 평가는 권위있는 평가스킴의 틀에 따라 평가된다. 평가스킴은 표준을 수립하고 평가의 질을 감시하며 평가시설과 평가자가 지켜야하는 규정을 관리한다. 평가결과의 상호인정을 위하여 위하여 서로 다른 평가기관의 규정 틀간의 일관성이 유지되어야 하며, 평가결과의 반복성, 객관성, 일관성을 유지하기 위하여 공통된 평가방법론을 따라야 한다. 또한 평가결과의 일관성을 높이기 위하여 최종 평가결과가 인증(Certification)과정에 제출되어 독립적인 정밀검사를 받은 후 인증되면 인증서가 발행되며 일반적으로 공개된다. 평가계획, 평가방법론 및 인증과정은 평가스킴을 수행하는 평가기관의 책임이긴 하지만 표준의 범위 내에 포함되지 않는다.

나. 보안기능 요구사항

TTAE.CC-99.03 제2부는 기준 개발자들이 고려

[표 2] 보안기능 요구사항 요약

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)	암호운용 및 키 관리
FDP	사용자 데이터 보호(User Data Protection)	사용자 데이터의 보호
FIA	식별 및 인증(Identification & Authentication)	사용자의 신원확인 및 인증
FMT	보안관리(Security Management)	TSF 데이터, 보안속성, 보안기능의 관리
FPR	프라이버시(Privacy)	허가되지 않은 사용자에 의한 개인의 신원 및 정보의 도용방지
FPT	TSF 보호(Protection of Trusted Security Functions)	TSF 데이터의 보호 및 관리
FRU	자원활용(Resource Utilization)	TOE의 가용자원 관리
FTA	TOE 접근(TOE Access)	TOE에 대한 사용자 세션의 보호
FTP	안전한 경로/채널(Trusted Path/Channel)	사용자와 TSF간 혹은 TSF간의 안전한 통신채널 확보

할 수 있는 모든 보안기능과 관련된 요구사항을 적절한 기준에 따라 분류하고, 표준의 형식에 맞추어 제시하고 있는 보안기능 요구사항의 백과사전이다. 표준의 보안기능 요구사항은 11개의 클래스(Class)로 구성되어 있다.

보안감사 클래스는 보안 관련 행동(즉, 보안정책에 의하여 통제되는 모든 행동)에 관련된 정보의 인식, 기록, 저장 및 분석을 포함한다. 감사기록 결과는 어떤 보안 관련 행동이 발생했으며, 누가 이에 대한 책임이 있는가를 결정할 때 이용할 수 있다. 통신 클래스에서는 데이터 교환에 참여하는 측의 신분보증에 구체적으로 관련된 2개의 패밀리를 제공한다. 이들 패밀리는 전송된 정보의 발신자(발신증명 : proof of origin)와 수신자(수신증명 : proof of receipt)의 신분보증에 관련되어 있다. 이 패밀리는 발신자가(originator) 메시지를 발신하였음을 부인할 수 없으며, 수신자(recipient)도 수신사실을 부인할 수 없음을 보장한다.

TOE 보안기능은 높은 수준의 여러가지 보안목적을 만족시키기 위하여 암호기능을 채택할 수 있다. 이들은 식별/인증, 부인방지, 안전한 경로, 안전한 채널 및 데이터 분리 등을 포함한다. 암호지원 클래스는 TOE가 암호기능을 구현할 경우 사용되며, 구현은 하드웨어, 펌웨어 및 소프트웨어로 이루어질 수 있다. 사용자 데이터 보호 클래스에서는 사용자 데이터의 보호와 관련된 TOE 보안기능 및 TOE 보안기능 정책을 위한 요구사항을 명시한다.

식별 및 인증 클래스의 패밀리에서는 요청된 사용자의 신분을 설정하고 증명하기 위한 기능요구 사항을 다룬다. 보안관리 클래스에서는 TSF의 관리내용을 다음과 같은 관점으로 나누어서 명시하고 있다. 속성(보안속성)관리, TSF 데이터 및 TSF 기능 관리측면에서 서로 다른 직무로 이들의 상호작용을 분리하여 서술하고 있다. 프라이버시 클래스에서는 프라이버시 요구사항을 포함한다. 이들 요구사항은 사용자에게 다른 사용자가 자신의 신분을 찾아내어 오용하지 못하도록 하는 것이다.

TSF 보호 클래스는 TSF를 제공하는 메커니즘의 무결성과 관리 및 TSF 데이터의 무결성에 관련된 기능 요구사항의 패밀리를 포함한다. 자원활용 클래스에서는 처리능력 및/또는 저장용량과 같은 요구된 자원의 가용성을 지원하는 3개의 패밀리를 제공한다. TOE 접근 클래스에서는 사용자 세션을 설정하기 위한 기능 요구사항을 서술한다. 안전한 경로/채널 클래스에서는 사용자들과 TSF간의 안전한 통신경로와 TSF와 다른 안전한 정보시스템간의 안전한 통신채널에 관한 요구사항을 정의한다.

다. 보증 요구사항

제3부 보증 요구사항은 보증을 측정하기 위한 척도를 정의하는 평가등급, 등급을 구성하는 각각의 보증 구성요소, 그리고 보호 프로파일과 보안목표 명세서 평가를 위한 기준을 포함한다. 보증 요구사항은 보증 컴포넌트, 보증 패밀리, 보증 클래스로 분류된다. 보증 요구사항을 요약하면 다음의 [표 3]과 같다.

형상관리는 TOE를 구현하는 과정에서 나타나는 기능 요구사항과 명세를 관리하는 방법 또는 수단을 말한다. 형상관리는 TOE 및 관련된 정보의 정교화 과정과 변경과정에서의 규율과 통제를 요구한다. 형상관리 시스템은 변경을 추적하는 수단을 제공하고 모든 변경이 인가되도록 보장함으로써 자신이 통제하는 TOE의 무결성을 보장한다. 배포 및 운영 클래스는 TOE의 정확한 배포, 설치, 생성, 그리고 시동에 대한 요구사항을 정의한다.

개발 클래스에는 기능 인터페이스에서 구현표현까

[표 3] 보증요구사항 요약

클래스명	클래스 제목	설명
ACM	형상관리(Configuration Management)	TOE의 무결성이 유지되고 있는지를 확인
ADO	배포 및 운영(Delivery and Operation)	TOE의 안전한 배포, 설치, 운영에 필요한 수단, 절차 및 표준을 확인
ADV	개발(Development)	TOE 개발과정의 일치성 및 완벽함을 확인
AGD	설명서(Guidance Documents)	TOE의 안전한 운영을 위한 지침서를 확인
ALC	생명주기 지원(Life Cycle Support)	TOE의 생명주기와 관련된 사항을 확인
ATE	시험(Tests)	TOE가 기술 요구사항을 만족하는지를 확인
AVA	취약성 평가(Vulnerability Assesment)	TOE의 개발과정 중에 발견되지 않은 취약성, 사용자에 의한 오용 등 잠재적인 취약성을 확인
APE	보호 프로파일 평가 (Protection Profile Evaluation)	PP가 완전하고 모순이 없으며, 기술적으로 충분함을 보임
ASE	보안목표 명세서 평가(Security Target Evaluation)	ST가 완전하고 모순이 없으며, 기술적으로 충분함을 보임
AMA	보증 유지(Maintenance of assurance)	TOE나 보안환경이 변화에도 ST를 지속적으로 만족시킴을 보임

지의 다양한 추상화 수준에서 TSF를 표현하기 위한 요구사항을 정의하는 4개의 패밀리가 있다. 또한 개발 클래스에는 다양한 TSF 표현(representation)간의 일치를 위한 요구사항 패밀리가 있다. 이것은 궁극적으로 가장 구체적인 TSF 표현으로부터 모든 중간 단계의 표현을 거쳐 보안목표 명세서에서 제공된 TOE의 요약명세까지 각각의 인접한 표현들이 서로 일치함을 보일 것을 요구한다. 또한 TOE 보안정책 모델에 대한 요구사항의 패밀리가 있으며 TOE 보안정책, TOE 보안정책 모델, 기능명세간의 일치성을 보이기 위한 요구사항의 패밀리가 있다. 마지막으로 TSF의 내부구조에 관한 요구사항을 가진 패밀리가 있다. 이것은 모듈화, 계층화, 복잡성의 최소화와 같은 측면을 다룬다.

설명서 클래스는 사용자와 관리자 설명서에 대한 요구사항을 제공한다. TOE의 안전한 관리와 사용을 위하여 TOE의 안전한 응용에 관련된 모든 측면이 서술되어야 한다. 생명주기 지원은 개발과 유지기간 동안 TOE의 정교화 과정에서 규율과 통제를 수립하는 측면이다. 보안을 분석하고 증거를 산출하는 작업이 개발과 유지 활동의 통합된 부분으로써 정규적인 기초 위에서 이루어진다면 TOE 보안 요구사항과 TOE 간의 일치성에 대한 신뢰가 더 커진다.

시험 클래스는 네 개의 패밀리를 포함한다 : 범위(coverage), 깊이(depth), 독립적인 시험(예 : 평가자가 수행하는 기능시험) 및 기능시험이다. 시험은 TOE가 보안기능 요구사항을 만족하는지를 입증한다. 시험은 TOE가 명시된 것 이상을 하지 않는다는 것은 입증할 수 없으나 최소한 보안기능 요구사항을 만족한다는 보증은 제공한다. 시험은 서브시스템과 모듈을 그 명세에 따라 시험하는 것처럼 TSF 내부구조에 직접적으로 수행할 수도 있다. 취약성 평가 클래스는 이용가능한 비밀 채널의 존재, TOE의 오용이나 부정확한 구성, 확률적이거나 조합적인 메커니즘이 파괴될

가능성, 그리고 악용가능한 취약성이 TOE 개발이나 운영중에 나타날 가능성을 다룬다.

보호 프로파일 평가의 목적은 보호 프로파일이 완전하고 일관성있고 기술적으로 건전하다는 것을 보이는 것이다. 평가된 보호 프로파일은 보안목표 명세서를 개발하기 위한 기초로 사용할 수 있다. 보안목표 명세서 평가의 목적은 보안목표 명세서가 완전하고 일관성있고 기술적으로 건전하여 상응하는 TOE 평가의 기초로 사용하기에 적절하다는 것을 보이는 것이다.

보증유지 클래스는 TOE가 국제 공통 평가기준에 따라 인증된 이후 적용될 요구사항을 제공한다. 이 요구사항은 TOE나 보안환경에 변경이 일어나더라도 TOE가 그 보안목표를 지속적으로 충족시킨다는 보증을 제공하는 것이 목적이다. 그런 변경은 새로운 위협이나 취약성의 발견, 사용자 요구사항의 변경, 그리고 인증된 TOE에서 발견된 결함의 교정을 포함한다.

인도, 한국, 중국 : 3G 이동통신의 일등공신

CDMA2000 및 UMTS 두 방식의 3G 무선 표준이 2005년 경에는 세계 이동통신의 75%를 점유하며 이 시장을 이끌어 갈 것이다. 올 해는 30%로 올랐다. 아태 지역의 텔레콤 사업자들은 3G 네트워크로의 세계적인 이전 추세을 염두에 두고 세계화에 앞장서고 있다. 지난 몇 달 간 아태지역을 중심으로 한 일련의 3G CDMA 기술의 승리는 이와같은 부상 세력의 전조이다. 또한 세계적인 주요 산업 리서치사들의 잇따른 보도는 3G 대역확산 방식(CDMA2000 1X, CDMA2000 1X EV, UMTS/Wideband CDMA 포함)이 무선 통신의 신규 가입자의 반 이상을 차지할 것임을 암시하고 있으며, 이 기술의 도입은 2007년까지 그 세를 이어갈 것으로 보인다. 이미 3G 대역확산 방식 개발의 주체 세력인 Lucent Technologies는 이런 추세를 등에 업고 아태 지역에서 지난 몇 개월 간 주요한 일련의 3G CDMA 방식을 공표하면서 큰 수익을 올리고 있다. Lucent는 최근 아태 지역의 주요 3 시장, 즉 중국, 한국, 인도의 유수 서비스 사업자와 손을 잡고 가입자 확보에 주력하고 있다. 이들 각 시장은 고급 무선 데이터 서비스의 빠른 발전을 경험한 바 있다. 세계에서 가장 빠른 이동통신 시장의 성장을 기록한 이 업계의 역군 China Unicom은 CDMA 무선접속 방식의 두 번째 단계인 CDMA1x 장비를 Lucent로부터 공급받고 있다. CDMA 1x의 성공적인 테스트와 시연을 거친 China Unicom은 10여 개 주에 고속 무선 데이터 서비스를 제공하며 중국을 이동통신 성장 제 1국으로 끌어 올렸다. 천만 가입자를 확보하고 있는 한국 무선 서비스 사업자 KTF는 2세대 네트워크 망에서 CDMA2000 1x로 향상시켰다. 이로써 초당 153kb 속도가 지원되는 고속 데이터 서비스가 가능하게 되었다. 인도의 주요한 서비스 사업자 Reliance Infocomm은 3G CDMA2000 1X가 지원되는 Lucent Flexent 기지를 이동통신 본부로 삼아 3G CDMA2000 기술을 인도 전역에 보급시켰다. 두 업체간의 5년 계약에는 기획 및 컨설팅 서비스, 설비 및 유지 보수의 지원은 물론 시설 일체가 포함된다. 인도 민영 유선 전화 사업자 Tata Teleservices 역시 국내 몇몇 주에 3G CDMA2000 고속 무선 네트워크를 구축하기 위해 Lucent의 Flexent 기지국과 이동통신 스위칭 센터를 배치하고 있다. 이로써 Tata Teleservices는 고속 데이터 서비스는 물론 양질의 음성 서비스를 제공하는 것이 가능해 질 것이다. 아태 지역 더 나아가 전 세계적으로 이동통신 사업자들이 3G 대역 확산 방식으로 전이하려는 주요 이유는 고속 데이터 전송이나 새로운 서비스 보급에 따른 잠재 매출의 막대함에 있다는 것이다.