

보안 평가 기술: Common Criteria를 중심으로

Security Evaluation Technology: Focused on Common Criteria

최락만(R. M. choe) 소프트웨어공학연구실 책임연구원
송영기(Y. K. Song) 소프트웨어공학연구실 책임연구원
인소란(S. R. Ine) 소프트웨어공학연구실 책임연구원, 실장

정보제품에 대한 보안성 평가를 통해 정보보안 사고를 사전에 예방하기 위해 각 국에서는 독자적인 보안 평가기준을 만들어 시행하여 왔다. 이들 기준간에는 호환성이 없으며, 평가결과가 상호 인증되지 않기 때문에 평가의 중복성 문제를 유발하였다. 이러한 문제를 해결하기 위한 새로운 보안 평가기준으로 최근에 CC(Common Criteria)가 발표되었다. 본 고에서는 보안 평가기준의 중요성 인식제고와 이 분야의 국내 기술 발전계획을 수립하는 데 필요한 기초 자료를 제공하기 위해 우선 보안 평가기준의 발전과정을 전반적으로 살펴보고, 향후 국제 표준으로의 채택이 유력시 되어 주목을 받고 있는 CC가 무엇이며 어떤 특성을 갖는지 분석하였다. 또한 보안 평가기술의 향후 발전 전망과 이에 따른 우리의 바람직한 대응 방안을 제시하고자 한다.

I. 서론

최근들어 우리 사회의 각 분야에서 정보화가 추진됨으로써 국가 경쟁력 강화, 산업의 생산성 증대, 삶의 질 향상과 같은 정보사회가 가져다 주는 긍정적인 효과가 기대된다. 그러나, 정보통신의 대중화, 개방화, 광역화 추세에 따라 예전에는 그리 문제가 되지 않았던 정보의 누출, 변조, 오용과 같은 정보화 역기능 현상이 빈번하게 발생함으로써 정보보호 문제는 정보사회가 정착되기 위해서 선결되어야 할 주요 현안의 하나로 떠오르고 있다.

보안성 평가기술은 암호기술과 함께 정보보호를 위한 핵심기술의 하나이며, 세부기술로는 보안 평가기준과 보안 평가제도를 들 수 있다. 보안

평가기준은 정보제품이 예상되는 모든 보안 위협 요소들에 대해 어떻게 대응하고 있으며 보안성이 어느 정도 있는가를 평가할 수 있는 기준을 제공하여 준다. 보안 평가제도는 평가기준을 기반으로 실제 평가를 시행할 때, 누가 무엇을 가지고 어떤 절차로 평가하며, 그 결과는 어떻게 관리되어야 하는가 등에 관한 사항을 규정한다. 본 고에서는 두개의 구성요소중 평가기준을 중심으로 보안성 평가기술의 현황과 대책을 살펴보고자 한다.

보안 평가기준은 정보제품의 보안성 평가를 위한 기준을 제공할 뿐만 아니라, 제품 개발주기 전 단계에서 필요로 하는 객관적이고 체계적이며 미리 검증된 보안성 관련 기술자료를 제공하므로써 정보제품의 보안성 향상을 위한 수단으로 이용되

고 있으며, 보안성이 결여된 정보제품을 사용함으로써 발생할 수 있는 정보 보안사고의 사전 예방에 필수적인 기술의 하나로 인식되고 있다.

이에 따라 정보화를 적극적으로 추진하고 외국에서는 자국의 이익보호를 위해 국가별 기준을 경쟁적으로 발표하게 되었다. 현재 널리 알려진 평가기준으로는 TCSEC(Trusted Computer System Evaluation Criteria)[1], ITSEC(Information Technology Security Evaluation Criteria)[2], CTCPEC(Canadian Trusted Computer Product Evaluation Criteria)[3], FC(Federal Criteria)[4] 등이 있으며, 최근에는 세계 공통표준을 지향하고 있는 CC(Common Criteria)[5]가 발표되었다. 국내에서의 이러한 보안 평가기준에 대한 조사 분석은 어느 정도 있었으나[6, 7], 이들 중 CC는 국제 표준으로 채택이 유력시 되고 있으며, 향후 이 분야에 지대한 영향을 줄 것으로 예상되는데도, 국내에서는 아직도 CC가 무엇이며 어떤 의미를 갖는지에 대한 인식이 부족한 상황이다.

본 고에서는 보안 평가기준의 중요성 인식제고와 이 분야의 국내 기술 발전계획을 수립하는데 필요한 기초 자료를 제공하기 위해 제 II장에서는 보안평가 기준의 발전과정을 전반적으로 살펴보고, 제 III장에서는 CC의 기본 개념, 기능 및 보증 요구의 구성, 평가등급 및 특성 등을 조사·분석하였다. 제 IV장에서는 보안 평가기술의 향후 발전 전망과 이에 따른 우리의 바람직한 대응 방안을 제시하고자 한다.

II. 평가기준의 발전 과정

정보 선진국에서는 정보제품에 대한 효율적이

고 객관적인 보안성 평가를 위한 기준을 마련하고, 그것을 정보제품의 개발, 평가, 선정을 위한 수단으로 활용하고 있다. 이러한 목적으로 만들어진 최초의 평가기준으로는 1985년 미국 NCSC(National Computer Security Center)에 의해 만들어진 일명 오렌지북(Orange Book)이라 불리는 TCSEC가 있다. TCSEC에서는 정보제품의 보안성에 영향을 줄 수 있는 보안요구를 보안정책(security policy), 책임성(accountability), 신뢰성(assurance), 문서화(documentation)로 분류하여 기본 요구사항을 명시적으로 정의하고, 이들 기본 요구사항을 만족하는 수준에 따라 7단계 보안등급(A1, B1, B2, B3, C1, C2, D)을 규정한다. 1988년 3월에 발표된 미국방성 TCSEC 관련 지침에서는 비밀 또는 민감한 데이터를 처리하는 모든 컴퓨터는 최소한 1992년까지 C2 등급 이상을 충족시켜야 하며, 장기적으로는 2003년까지는 B3등급 이상을 충족할 것을 요구함에 따라 컴퓨터 공급자들은 TCSEC에 규정된 안전한 컴퓨터시스템 개발에 박차를 가하고 있다. TCSEC는 이후 모든 평가기준의 제정시 기본 자료로 활용됨으로써 각국의 평가기준에 많은 영향을 주고 있다. 그러나 TCSEC는 정보제품의 기본적인 보안 요소인 비밀성(confidentiality), 무결성(integrity), 가용성(availability) 중에서 주로 비밀성에 중점을 두고 있다. 따라서 비밀성을 우선으로 하는 군사 및 정보기관의 보안 기준으로 적용하기에는 문제가 없지만, 무결성과 가용성이 강조되는 금융 및 데이터 처리 분야에 적용하기에는 다소 취약한 면이 있다. 또한 TCSEC에서 상위 등급은 하위 등급의 모든 요구사항을 포함하면서 추가적인 요구사항이 부가되도록 규정하고 있다.

이와 같이 경직된 등급구조는 사용자의 특정 요구 사항을 융통성 있게 수용하기 어렵게 한다.

유럽 지역에서는 영국 CCSC(Commercial Computer Security Center)의 DTIEC(Green Book), 독일 GISA(German Information Security Agency)의 ZSIEC(Blue-White Book), 프랑스 SCSSI(Service Central de la Securite des Systems d'Information)의 Blue-White-Red Book 등과 같이 국가별로 독자적인 평가기준을 제정·운용하여 왔다. 그러나 영국, 독일, 프랑스, 네덜란드 등 유럽 4개국은 이 분야에서 주도권 확보와 기존 기준의 기술적인 제약 및 중복 평가 문제를 개선하기 위해 유럽 각국의 기준뿐 아니라, 미국의 TCSEC의 내용을 참조하여 새로운 유럽 공통 평가기준으로 ITSEC를 공동으로 마련하여 1991년에 발표하였다. ITSEC(버전 1.2)는 TCSEC에 상응하는 기밀성을 지원할 뿐 아니라 무결성 및 가용성에 관한 평가기준도 수용하고 있다. 한편 ITSEC는 획일적인 등급 구조를 갖는 TCSEC와는 달리 사용자의 필요에 따라 다양한 종류의 평가등급을 융통성 있게 정의하여 사용할 수 있도록 하였다. ITSEC는 보안 요구를 기능과 보증이라는 측면으로 명시적으로 분류하여 제시하고 있으며, 지역적인 제한은 있지만 국제표준을 지향하는 최초의 보안 평가기준이라는 점에서 평가받고 있다.

캐나다에서는 1991년 CSSC(Canadian System Security Centre)에 의해 자국의 평가기준으로 CTCPEC를 처음 발표하였으며, 1993년에는 버전3.0을 발표하였다. CTCPEC는 보안 요구를 기능과 보증 요구로 분류하고, 각각에 대해 등급을 규정하는 등 구조적인 측면에서 ITSEC와 유사하

나, 기능면에서 세부 분류 및 내용 등은 TCSEC와 비슷하다. CTCPEC에서는 기능요구를 유형별로 분류한 후, 각 유형에 대해 기본 보안서비스를 정의하고 있으며, 이들 각 기본서비스를 다시 요구 수준에 따라 최대 6단계의 등급을 정의하고 있다. CTCPEC는 상기 기본서비스 및 등급 이외도 기능프로파일(functional profile)이라는 보안 구조를 정의하여 사용하고 있다. 하나의 기능프로파일은 몇개의 서비스 등급이 모여져 구성되며, 이 프로파일 자체가 하나의 평가등급을 형성할 수 있도록 함으로써 사용자의 다양한 보안 요구를 융통성 있게 반영할 수 있도록 지원한다.

한편 TCSEC제정 이후 이것을 기반으로 정보제품을 평가해오던 미국에서는 NIST(National Institute of Standards and Technology)와 NSA(National Security Agency)가 캐나다 CSSC와의 협력으로 국방 분야뿐 아니라 민간분야 보안성 평가 요구를 수용할 수 있는 북미지역 공통 표준으로 FC를 1993년에 발표하였다. FC는 기존의 평가기준인 TCSEC, ITSEC, CTCPEC의 장점만을 취사·선택함으로써 기능과 구조적인 측면에서 보다 진보된 특성을 가지고 있다. 또한 FC는 보안성을 강조하는 군사분야뿐 아니라 기밀성과 가용성에 관한 민간분야의 보안요구를 수용하고 있다. FC는 보호프로파일(Protection Profile)이라는 보안 구조를 도입하여 보안요구를 보다 쉽게 정의할 수 있도록 지원하며, 보호프로파일의 확장 또는 재구성을 통해 기술의 발달과 경험들로부터 발생하는 변화를 쉽게 수용할 수 있도록 하였다.

이와 같이 나라 또는 지역별로 서로 다른 평가기준을 가짐에 따라 동일 제품에 대한 중복 평

<표 1> 보안 평가기준의 발전 과정

지역	국가명	보안 평가 기준		
북미	미국	TCSEC('85)		FC('93)
유럽	캐나다	CTCPEC('93)		
	영국	DTIEC('89)	ITSEC('91)	CC('96)
	독일	ZSIEC('89)		
	프랑스	Blue-White-Red Book		
	네덜란드			

가 문제가 발생하였다. 이를 해결하기 위한 방안으로 범 세계적인 보안 평가기준 표준화 작업이 ISO(International Standard Organization)와 같은 국제표준화기구에 의해 1990년경부터 진행되어 왔다[8]. 이러한 작업의 구체적인 결과의 하나로 북미 및 유럽국가들의 보안 관련 기관들이 모여 세계 공통기준을 지향하는 새로운 평가기준으로 CC 버전 1.0을 1996년 1월에 발표하였다.

이와 같이 TCSEC가 발표된 이래 약 10년 동안 보안 평가기준의 발전 과정을 종합적으로 살펴보면 <표 1>과 같다. 우선 지역이라는 관점에서 보면 국가별 표준에서, 지역별 표준을 거쳐, 세계 표준으로 발전해 가고 있다. 또한 평가기준의 특성 측면에서 보면 규격의 융통성을 부여하는 방향으로, 상업용 및 광범위한 산업 환경을 수용하는 방향으로, 또한 평가의 대상이 단위제품(component) 중심에서, 안전성이 입증된 단위제품들의 통합으로 구성되는 복합제품 및 시스템에 대한 평가 위주로 바뀌고 있다는 것을 알 수 있다.

III. Common Criteria

CC(Common Criteria)는 각 나라 및 지역별로 서로 다른 평가기준을 운용함으로써 발생하는 중

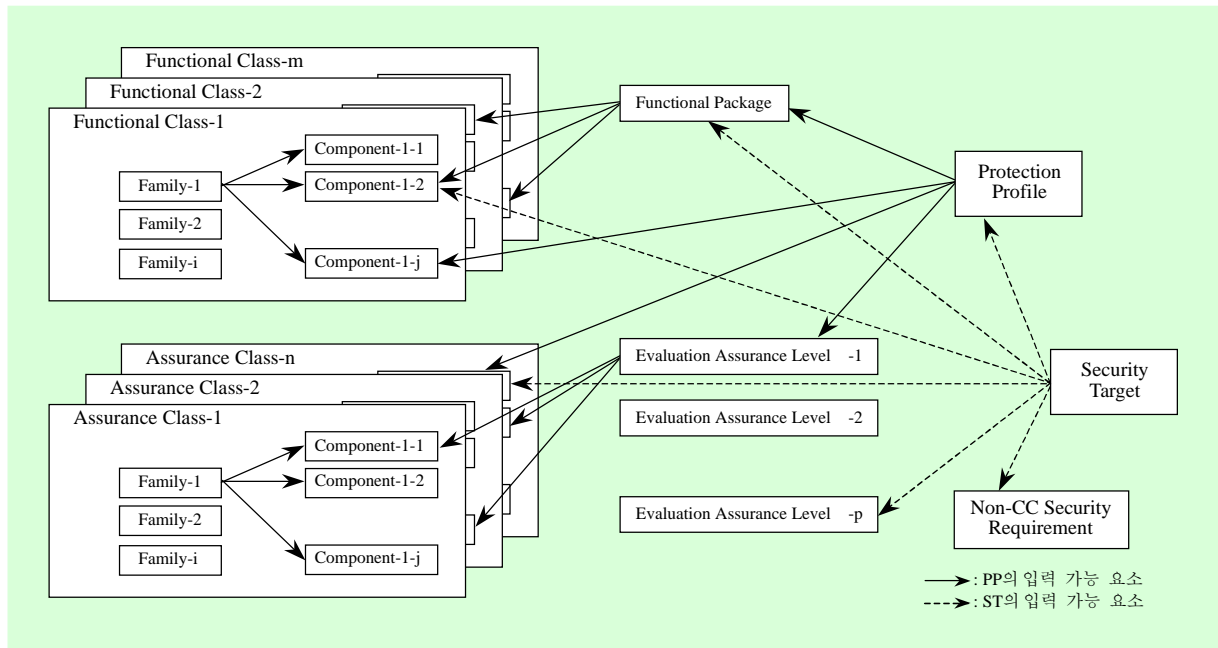
복평가 문제를 해소하고, 기술적으로 보다 진보된 범 세계 공통의 보안 평가기준을 지향하여 미국, 캐나다와 유럽 4개국의 공동작업에 의해 만들어졌다. CC의 기본개념, 구성 요소별 구조와 내용 및 특징은 아래와 같다.

1. CC의 기본 개념

CC는 6개의 문서로 아래와 같이 구성되어 있다.

- Part 1: 서론 및 일반 모델(Introduction and General Model)
- Part 2: 보안 기능 요구(Security Functional Requirements)
- Part 3: 보안 보증 요구(Security Assurance Requirements)
- Part 4: 미리 정의된 보호프로파일(Predefined Protection Profiles)
- Part 5: 보호프로파일 등록 절차(Protection Profile Registration Procedures)
- TR: 암호 평가 기준(안)(Evaluation Criteria for Cryptography(Draft))

CC에서는 보안 요구를 기능과 보증이라는 2개의 측면으로 나누어 정의한다. 각 기능 및 보증 요구는 사용자로 하여금 원하는 보안 요구사항을



(그림 1) CC 구성 개념도

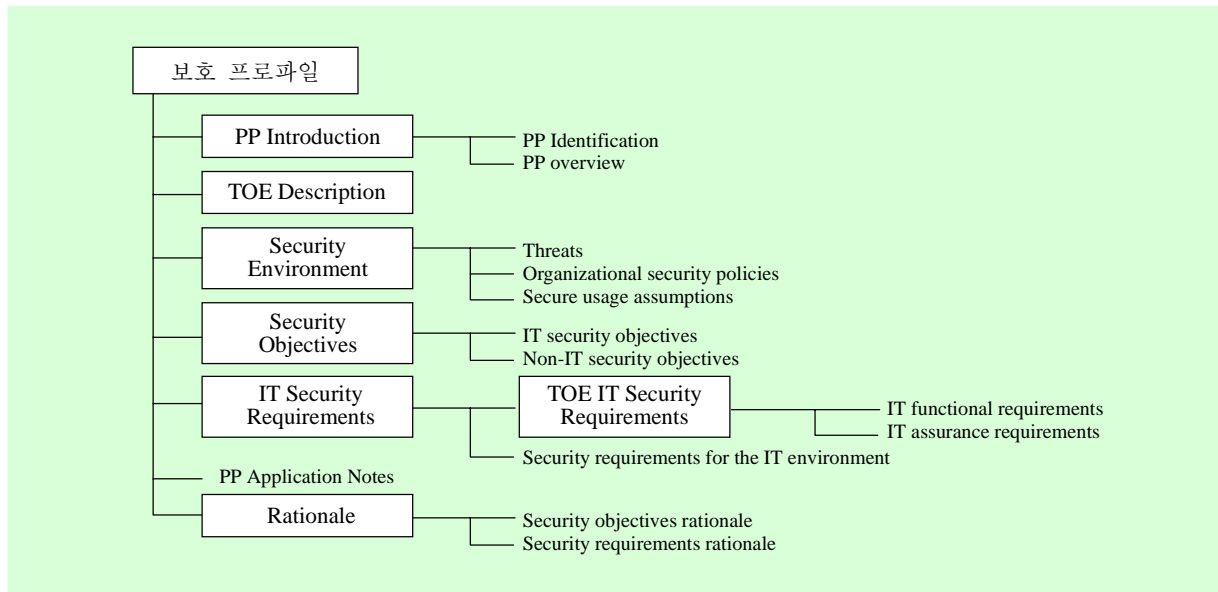
쉽게 활용할 수 있도록 class-family-component라는 형식의 계층적인 구조를 갖도록 정의되어 있다(그림 1). Component는 필요에 따라 하나 이상의 element를 가질 수 있으며, element는 보안 요구를 표현하는 최소 단위이다.

CC에서는 평가대상(target of evaluation: TOE)의 보안요구를 표현하는 수단으로 패키지(package), evaluation assurance level(EAL), 보호프로파일(protection profile: PP), 보안타겟(security target: ST) 등과 같은 보안구조들을 사용하고 있으며, 기본 개념은 아래와 같다.

- 패키지는 부분적인 보안목표를 만족시키기 위한 component들의 집합으로 구성된다. 패키지는 특정 보안목표에 효과적이며 유용한 요구사항의 모음으로 재사용이 가능하다. 하나의

패키지는 규모가 더 큰 패키지나 보호프로파일, 보안타겟을 구성하는데 이용될 수 있다.

- EAL은 보증요구에 관련된 component들의 집합으로 구성된 패키지의 일종이다. 각 EAL은 자체적으로 온전(complete)한 보증 component들의 집합이며, CC의 체계화된 보증 수준 즉, 보증 등급을 형성한다.
- 보호프로파일은 정보제품이 갖추어야 할 공통적인 보안 요구사항들을 모아 놓은 것으로, 새로 만들어진 보호프로파일은 기술적으로 안전(sound)하고, 완전(complete)하며, 실질적으로 보안 요구를 만족하는지가 검증되면 재사용이 가능하도록 보호프로파일 저장소(repository)에 등록/관리된다. 보호프로파일은 패키지, EAL, 기능 및 보증 요구 components 등의 집합으로 구성될 수 있으며, (그



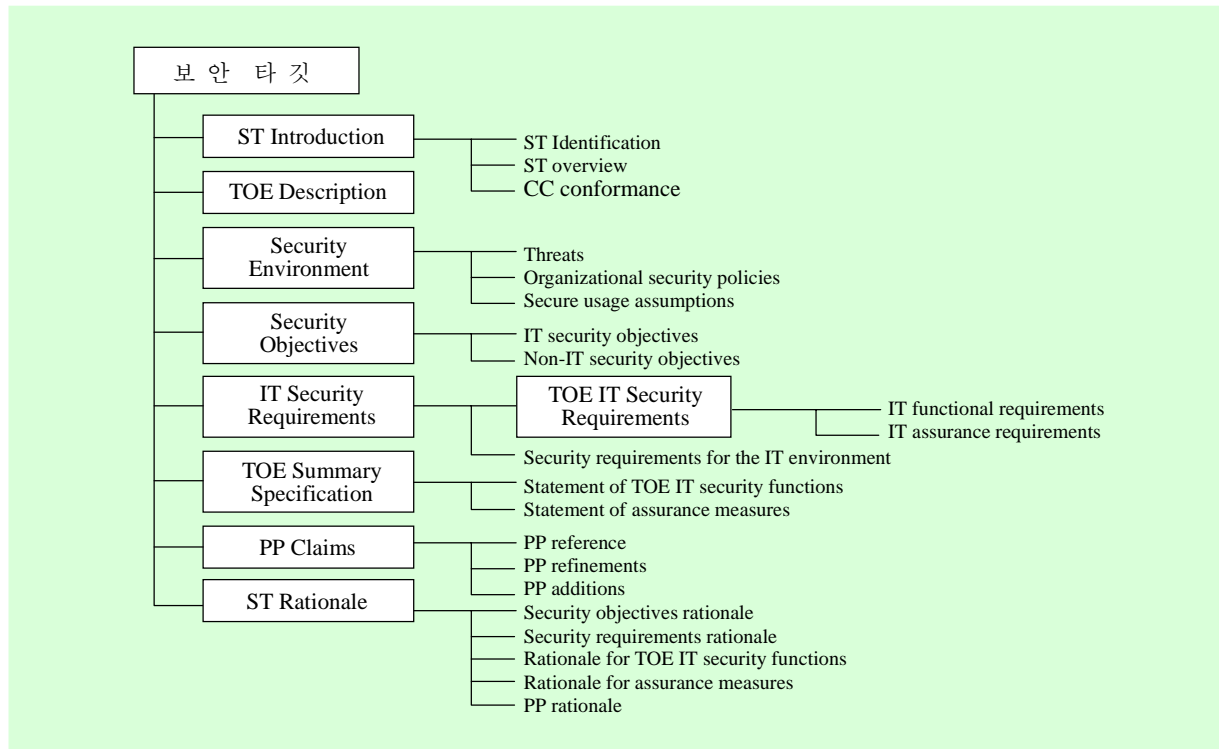
(그림 2) 보호 프로파일의 구조

림 2)와 같은 구조를 갖는다. 검증/등록된 보호프로파일은 보안타짓을 구성하는 입력 요소로 사용될 수 있다.

- 보안타짓은 TOE의 보안 요구사항을 표현하기 위해 정의된 최상위 수준의 보안구조이다. 보안타짓은 하위 구조인 보호프로파일, 기능 패키지, EAL, 기능 및 보증 components 등의 집합으로 구성할 수 있다. 보안타짓은 (그림 3)과 같이 보호프로파일과 유사한 요소들로 구성되어 있지만, 이외에도 TOE Summary Specification, PP Claims, ST Rationale 등을 갖는다. 보안타짓에는 필요에 따라서 CC에 정의되지 않은 보안 요구를 포함할 수도 있다.

CC에서는 TOE의 개발/평가/운용 프로세스를 중심으로, 각 프로세스의 입·출력 및 상호관계가 (그림 4)와 같은 보안평가 일반모델을 기반

으로 세부 보안 요구사항을 정의한다. CC에서의 평가에는 그 대상에 따라 3개의 유형(보호프로파일 평가, 보안타짓 평가, TOE평가)이 있다. 보호프로파일 평가에서는 보호프로파일이 TOE의 요구사항 기술에 적합한 것인지를 보호프로파일 평가기준을 이용하여 평가한다. 보안타짓 평가에서는 보안타짓이 보호프로파일의 요구사항을 적절하게 만족시키고 있으며, 보안타짓 자체가 TOE평가의 입력으로 유용하며 적합한지를 보안타짓 평가기준을 이용하여 평가한다. 위 2가지 유형에 대한 평가기준에 관한 세부 사항은 CC의 “Part 3: 보안 보증 요구”에 정의되어 있다. 이들 평가의 시행 결과는 성공 또는 실패 형식으로 나타난다. TOE평가는 TOE의 보안기능이 보안타짓에 기술된 기능요구를 만족시키는지, TOE의 보안목표를 달성하는 데 유효한지, 그리고 올바르게 구현되었는지 등을 평가하는 것이다. TOE평가 결과는



(그림 3) 보안타깃의 구조

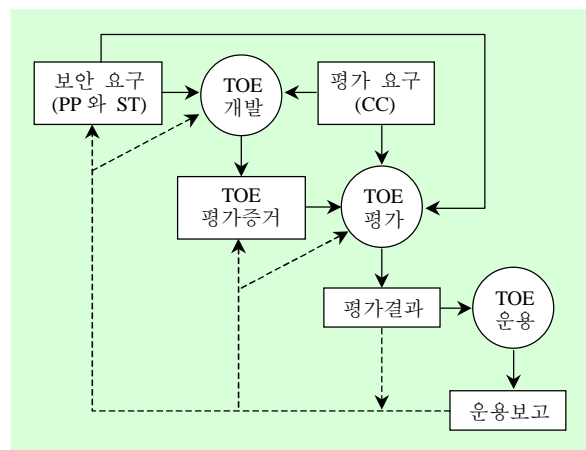
CC와의 적합성(conformation) 정도를 나타낸다.

2. 보안 기능 요구

CC 버전1.0의 Part 2에 정의된 보안 기능요구는 <표 2>에서 보는 바와 같이 9개의 class, 76개의 family, 184개의 component들로 구성되어 있다.

3. 보안 보증 요구

CC 버전1.0의 Part 3에 정의된 보증요구(Assurance Requirements)와 보호프로파일 및 보안타깃 평가기준에 대한 세부 사항이 정의되어 있다. 보증요구는 전체가 7개의 class, 25개의 family, 72개의 component들로 구성되며, PP 및 ST 평가



(그림 4) 보안 평가 일반 모델

기준은 2개의 class, 8개의 family, 8개의 component들로 구성된다(표 3).

〈표 2〉 기능요구의 종류

Class	Family 수	Component 수
식별·인증(Identification and authentication)	9	27
보안 감사(Security Audit)	12	35
사용자 데이터 보호 (User data protection)	15	46
TOE 접근(Access)	7	11
자원 이용 (Resource utilization)	3	8
안전 보안기능의 보호 (Protection of trusted security functions)	22	43
통신(Communication)	2	4
비밀성(Privacy)	4	8
안전한 경로/채널 (Trusted path/channels)	2	2

한편 CC에서는 보증요구를 기반으로 한 보증 등급으로 7개의 EAL(Functionally tested: EAL1, Structurally tested: EAL2, Methodically tested and checked: EAL3, Methodically designed, tested, and reviewed: EAL4, Semiformally designed and tested: EAL5, Semiformally verified design and tested: EAL6, Formally verified design and tested: EAL7)을 정의한다. CC에 정의된 7개의 EAL을 구성하는 보증요구 관련 class-family-component는 〈표 4〉와 같다.

4. CC의 특징

- CC에서는 보안요구를 기능과 보증으로 분류하고, 하나의 서비스를 여러 개의 수준으로 세분화하여 정의한 후 그것을 모아서 프로파일로 구성하는 방식 등은 CTCPEC와 유사하지만,

〈표 3〉 보증요구의 구성

구분	Class	Family 수	Component 수
보증 요구	구성관리 (Configuration management)	3	9
	개발(Development)	6	23
	안내문서 (Guidance documents)	2	2
	생명주기 지원 (Life cycle support)	4	12
	납품 및 운영 (Delivery and operation)	2	5
	시험(Tests)	4	11
	취약점 평가 (Vulnerability assessment)	4	10
PP/ ST 평가 기준	보호 프로파일 평가 (PP Evaluation)	3	3
	보안타깃평가 (ST Evaluation)	5	5

최상위의 프로파일 이전에 중간단계로 패키지라는 중간 구조를 도입함으로써 CTCPEC에 비해 보다 더 계층적인 구조를 가지며, 또한 보안요구를 보다 융통성 있게 구성할 수 있도록 한다.

- CC에 정의된 7개의 보증등급은 기존의 주요 평가기준에서 정의하고 있는 등급과 완전하게 일치하지는 않지만 대략적인 대응 관계는 〈표 5〉와 같다.
- CC를 기반으로 하여 평가를 실시할 때 평가 기준 적용의 일관성 유지와 평가결과가 상호 인증될 수 있도록 하기 위한 평가제도로써 CEM(Common Evaluation Methodology)이 수립중에 있다. CEM 추진 기본일정은 '97년까지 평가의 기본원칙과 일반모델, 보호프로파일과 EAL이외의 보증요구에 대한 평가 방

〈표 4〉 EAL 요약표

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT	-	-	-	1	1	2	2
	ACM_CAP	1	1	2	3	3	4	4
	ACM_SCP	-	-	1	2	3	3	3
Delivery and operation	ADO_DEL	-	-	-	-	-	-	-
	ADO_IGS	-	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	4	5	6
	ADV_HLD	-	1	2	2	3	4	5
	ADV_IMP	-	-	-	1	2	3	3
	ADV_INT	-	-	-	-	1	2	3
	ADV_LLD	-	-	-	1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	-
Life cycle support	ALC_DVS	-	-	1	1	1	2	2
	ALC_FLR	-	-	-	-	-	-	-
	ALC_LCD	-	-	-	1	2	2	3
	ALC_TAT	-	-	-	1	2	3	3
Tests	ATE_COV	-	1	2	2	2	3	3
	ATE_DPT	-	1	2	2	3	3	4
	ATE_FUN	-	1	1	1	1	1	1
	ATE_IND	1	1	2	2	2	2	3
Vulnerability assessment	AVA_CCA	-	-	-	-	1	2	2
	AVA_MSU	-	-	1	2	2	2	2
	AVA_SOF	-	1	1	1	1	1	1
	AVA_VLA	-	1	1	2	3	4	4

법 등을 완료하고, TOE 평가(EAL 1 - 7) 방법을 '98년까지 수립한 후, 최종 결과를 '99년 1/4분기에 발표할 예정으로 추진되고 있다.

- CC는 개발이 완료된 정보제품에 대한 보안성 평가뿐 아니라 제품의 설계, 구현, 시험 등 전

개발 단계에 이용이 가능한 보안성 평가 기준을 제공한다.

- CC의 개념구조는 ISO/IEC/JTC1 SC27/WG3에서 제시한 보안성 평가기준 일반모델을 기초로 하고 있어 향후 국제 표준으로의

채택에 큰 무리가 없을 것으로 예상된다.

(표 5) 주요 평가기준간 평가등급 대응 관계

TCSEC	ITSEC	CTCPEC	CC
-	-	T-7	-
A1	E6	T-6	EAL7
B3	E5	T-5	EAL6
B2	E4	T-4	EAL5
-	-	T-3	-
B1	E3	T-2	EAL4
C2	E2	T-1	EAL3
C1	E1	-	EAL2
-	-	-	EAL1
D	E0	T-0	-

IV. 향후 전망 및 대응 방안

정보 제품에 대한 보안 평가 수요는 그 동안 미국의 정부기관 특히 국방분야가 주류를 이루어 왔지만, 최근들어 정보화의 진전과 정보 보안에 대한 중요성 인식 확산으로 일반 부문에서의 수요 또한 급증하는 추세에 있다.

이에 따라 각국 또는 지역별로 독자적인 보안 평가기준과 제도를 마련하여 운용하고 있었다. 이와 같이 서로 다른 평가기준과 제도를 채택하게 되면 평가의 중복성 문제가 발생하게 된다. 즉, 이미 평가를 마친 제품을 다른 국가에서 사용할 경우 그 나라에서 요구하는 평가기준과 제도에 따라 재평가를 받아야 하는 상황이 벌어질 수 있다. 이러한 문제를 해결하기 위한 보안 평가기준의 국제 표준화 작업이 ISO 등에서 진행되고 있다. CC는 이러한 작업의 일환으로 국제 공통 평가기준을 지

향하여 탄생하게 되었다. CC는 '96년 1월에 발표된 버전1.0의 일부(Part 1~Part 4)가 ISO에 의해 표준안으로 채택됨에 따라 향후 보안 평가 분야에 서 중대한 영향을 미칠 것으로 예상된다.

몇년 전까지만 해도 국내 보안평가 분야의 연구는 일부 학계와 연구기관에 의한 CTSEC, IT-SEC와 같은 평가기준에 대한 조사·분석 활동이 고작이었다. 그러나 최근 들어 보안성 평가기술이 초고속정보통신기반구축과 같은 각종 정보화 사업의 원활한 추진을 위해 필히 확보해야 할 핵심 기술의 하나로 인식되고 있다. 이에 따라 정부에서는 정보보호시스템의 성능과 신뢰도에 관한 기준을 고시하고, 제조, 수입자 및 사용자에게 대하여 기준 준수를 권고하는 내용을 정보화촉진기본법에 명시하고, 정보보호 전문기관으로 한국정보보호센터를 설립하는 한편, 방화벽(firewall)과 같은 일부 정보제품에 대한 평가기준을 마련하는 등 보안성 평가에 대한 연구가 활성화 되고 있다. 그러나 아직까지 보안 평가기준의 국내 표준안이 마련되어 있지 않은 상태이며, 전반적으로 볼 때 국내 보안성 평가기술은 아직 초보 단계를 벗어나지 못하고 있는 실정이다.

최근과 같이 모든 분야에서 정보제품에 대한 보안성 검증요구가 확산되는 상황이 지속될 때, 2000년대 중반에는 국제기준에 의해 보안성이 검증되지 못한 정보제품은 생존할 수 없는 상황이 전개될 것이다. 이러한 여건에서 우리 스스로 보안성 평가능력을 확보하지 못하게 되면 국산 정보제품의 국제 경쟁력은 약화되고, 국가/사회/경제 및 개인의 이익에 민감한 사안인 정보보호 자체를 외국에 의존할 수 밖에 없게 된다. 이러한 상황에 효율적으로 대처하기 위해서는 우리의 기술

로, 우리의 정보제품에 대한 보안성을 자체적으로 평가할 수 있는 능력을 조기에 확보할 필요가 있다. 이 목표를 실현하기 위해서는 무엇보다도 우선 보안 중장기 발전계획이 마련되어야 한다. 현재와 같이 기술적으로 낙후된 상황에서 취할 수 있는 바람직한 실천 전략의 하나로는 궁극적으로 국내 보안성 평가기준으로 CC를 채택하고, CC가 세계 표준으로 채택되기 이전까지는 현재 이 분야에서 널리 이용되고 있는 TCSEC를 잠정 기준으로 삼아 조기에 부족한 기술을 확보하면서, CC가 세계 표준으로 채택되는 경우 곧 바로 지원할 수 있도록 CC를 기반으로 하는 평가시행 체계를 구축하여야 한다. 이와 더불어 이 분야에서 선진국과 경쟁하기 위해서는 평가 소요기간을 단축하고 평가결과와 객관성을 향상시킬 수 있도록 여러가지 보안성 평가 자동화용 도구들을 개발할 필요가 있다. 또한 전문가 그룹을 조직하여 국내 주요 현안 및 공통 관심사를 협의하고 공동 대책방안을 수립/실행할 수 있는 여건을 마련해줄 필요가 있다. 정책적인 측면에서는 보안 평가 분야를 국내 정보산업의 경쟁력 확보 및 정보화 촉진을 위한 전략 기술분야로 선정하여 육성하는 것이 바람직하다. 끝으로 이 분야의 국내 기술발전을 촉진시키기 위해서는 보안성 평가 관련 전문용어의 한글 표기방식의 통일안이 조기에 마련될 필요가 있다.

- [3] Canadian Trusted Computer Product Evaluation Criteria(CTCPEC), Version 3.0, Canadian System Security Centre, Communications Security Establishment, Government of Canada, Jan. 1993.
- [4] Federal Criteria for Information Technology Security (FC), Draft Version 1.0, jointly published by the NIST and NSA, US Government, Jan. 1993.
- [5] Common Criteria for Information Technology Security Evaluation, Version 1.0, Common Criteria Editorial Board, Jan. 1996.
- [6] 전산망 보안성 평가기준에 관한 연구, 한국전산원, 1993. 12.
- [7] 차성덕, “시스템 보안 평가기술” 제2회한국전산망보안기술워크숍 발표자료집, pp. 281~293, 1996. 5.
- [8] Evaluation Criteria for IT Security, Working Draft, ISO/IEC/JTC1 SC27/WG3, Jul. 1993.

참 고 문 헌

- [1] Trusted Computer System Evaluation Criteria(TCSEC), US DoD5200.28-STD, Dec. 1985.
- [2] Information Security Evaluation Criteria(ITSEC), Version 1.2, Office for Official publications of European Communities, Jun. 1991.