공통평가기준(CC) 버전 3.0 분석

노병규* · 김영태** · 박두순*** · 김점구****

요 약

현재, ISO/IEC SC27 WG3에서는 공통평가기준 개발위원회(CCDB)를 주축으로 CC V3.0의 개정작업을 2008년까지 국제표준을 목표로 적극적으로 진행하고 있다. 따라서 CC V3.0의 변경내용을 분석하여 국가적 차원에서 CC V2.*에서 V3.0의 변화에 철저하게 대비할 필요가 있다. 이에 따라 본 논문에서는 현재 개정 중인 CC V3.0의 개선내용을 CC V3.0 개용내용 요약, 제1부-소개 및 일반모델 개정내용, 제2부-보안기능컴포넌트의 개정내용, 제3부-보안보증컴포넌트의 개정내용 등 크게 네 개의 영역으로 나누어 정밀분석하고 CC V3.0의 개선사항 및 변경내용에 대해 상세하게 설명한다.

Analysis on Common Criteria Improvements in Version 3.0

Byung-Gyu No* · Young-Tae Kim**
Doo-Soon Park*** · Jeom-Goo Kim****

ABSTRACT

Recently, ISO/IEC SC27 WG3 is actively working on the revision of CC V3.0 to be an international standard by 2008, principally supported by Common Criteria Development Board (CCDB). Hence, it is essential for Korea to review and analyze the changes in CC V3.0, so as to be completely prepared for any change to be occurred from CC V2.* to V3.0. Taking into account of CC V3.0 being revised currently, this paper gives a general overview of revision in CC V3.0 ; then, closely examines and explains the improvements and changes made by the revision in CC V3.0

Key words : CC V3.0, CC V2.3, CCDB, Security Target

* 한국정보보호진흥원
** 순천향대학교 공과대학
*** 정보기술공학부
**** 남서울대학교 컴퓨터학과

1. 서 론

현재, ISO/IEC SC27 WG3에서 공통평가기준(CC, Common Criteria) V3.0의 개정작업을 2008년까지 국제표준(IS : International Standard)을 목표로 한창 진행 중에 있다[1]. 이 개정 작업에는 미국, 캐나다, 영국, 독일, 프랑스, 네덜란드, 스페인, 일본, 호주/뉴질랜드 등 10개국이 참여하고 있다.

CC V3.0 개정은 평가대상(TOE, Target of Evaluation)의 보안요구사항을 표현하는 보안기능/보증컴포넌트를 구성하는 클래스와 패밀리간의 중복성 제거 및 재구성을 통해 평가활동의 중복을 줄임으로써 효율적인 평가를 지원하는데 그 목적이 있다. 부가적으로 CC에 반영되지 않은 총 126개의 해석 요구사항(RI : Request for Interpretation)을 평가자 활동의 작업단위(Work Units)에 반영하여 CC V2.* 자체의 문제점을 보완하였다. CC V3.0에 반영된 126개의 해석 요구사항은 ASE/APE 41개, ADV 26개, ALC/AGD 6개, AVA 7개, CC 제2부 36개로 분류된다.

향후, CC V3.0은 1999년 8월에 개정된 CC 2.1 이후로 가장 많은 내용이 변경될 전망이다. 2005년 4월 공개된 CC V3.0(초안)을 살펴보더라도, 전반적인 구성, 개념 및 용어, 보안기능/보증컴포넌트 등이 상당히 변경되었음을 짐작할 수 있다[2].

본 논문에서는 CC V2.*에서 V3.0으로 변경됨에 따라 CC V3.0의 변경사항에 대한 이해를 높이고 국가적인 차원에서 이에 적절히 대응하는데 도움을 제공하기 위해 CC V3.0의 개정내용을 상세하게 분석한다.

본 논문의 구성은 다음과 같다. 2장에서 전반적인 CC V3.0의 개정내용을 요약 설명한다. 3장에서 제1부-소개 및 일반모델, 4장에서 제2부-보안기능 컴포넌트, 5장에서 제3부 보안보증 컴포넌트의 변경사항을 분석한다. 6장에서는 결론에 대해 요약한다.

2. CC V3.0 개정내용 요약

CC V3.0의 개정사항을 다음과 같이 크게 네 가지로 요약할 수 있다.

- 개념 및 용어, 내용의 구체화, 명확화를 통한 CC의 이해도 향상
  모호한 개념 및 용어를 명확하게 다시 정의하고, CC에서 추상적으로 표현된 내용들을 보다 구체적이고 현실적으로 기술하여 CC의 전반적인 내용에 대한 이해도를 높인다.
- TOE 개발환경을 반영하여 정보보호제품 개발 시 TOE 취약성 사전 제거
  보안목적을 수립시, TOE 개발환경을 추가적으로 고려함으로써 개발환경으로부터 발생 가능한 위협을 사전에 분석하여 개발자 측면에서 TOE 구현의 정확성(Correctness)을 높이고, TOE 자체의 취약성을 줄인다.
- 보안행위 모델 개념을 적용하여 보안기능컴포넌트의 단순화
  보안기능요구사항을 효율적으로 표현하는데 '주체-연산-객체'의 보안행위 모델 개념을 모든 보안기능컴포넌트에 적용시켜 중복되거나 유사한 클래스/패밀리를 통합하여 효율적인 평가활동을 지원한다.
- 다양한 소프트웨어 공학기법을 적용하여 EAL5 이상의 평가/개발방법론 구체화
  실세계와 부적합한 '폭포수 모델(Waterfall model)' 대신, 구조적 설계(architectural design), 응집도(cohesion), 결합도(coupling) 등의 다양한 소프트웨어 공학기법을 적용하여 TOE를 안전하게 구현하고, TOE 보안기능의 복잡도를 줄이는 등 EAL5이상의 고등급 평가/개발방법론을 구현하기 위한 구체적인 방법을 제시한다.

CC에서 사용되는 모호한 용어의 예로, 목차인 '제2부-보안기능요구사항'을 들 수 있다. 제2부에

서는 보안기능요구사항을 표현하는 클래스, 패밀리의 집합으로 구성되어 있는데, 이는 보안기능컴포넌트로 정의되어 있지만 '보안기능요구사항'이 그대로 사용되고 있다. 따라서 제2부의 목차를 '제2부-보안기능컴포넌트'로 변경하였다. 이 외에 변경빈도가 가장 높은 용어인 'CC'는 'ISO/IEC 15408'로 변경되었다.

보안목적 수립시 TOE 개발환경의 반영 및 중복되거나 유사한 보안기능 및 보안보증 클래스/패밀리의 통합으로 인해 FDP(데이터 보호 및 프라이버시), FIA(식별, 인증 및 연결), FCO(통신), FAU(보안감사), FPT(TSF 보호) 등 보안기능컴포넌트와 APE/ASE(PP 평가/ST 평가), ADV(개발), ATE(시험), ALC(생명주기 지원), AGD(설명서), AVA(취약성 평가) 등 보안보증컴포넌트가 많이 변경되었다. CC V3.0은 CC 2.*에 비해 클래스/패밀리의 개수가 <표 1>과 같이 대폭 축소되었다.

〈표 1〉 CC V2.*과 CC V3.0의 클래스/패밀리 개수 비교

보안요구사항		V2.1	V2.2	V3.0
보안기능컴포넌트	클래스 개수	11	11	6
	패밀리 개수	66	67	45
보안보증컴포넌트	클래스 개수	10	10	6
	패밀리 개수	40	40	28

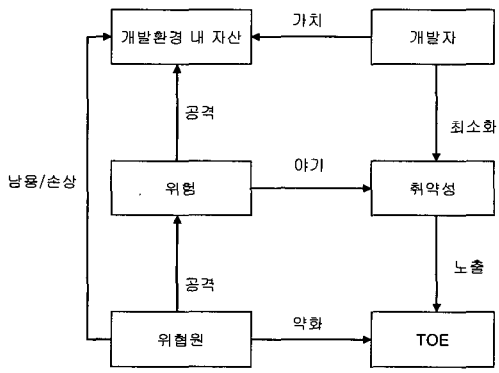
EAL5이상의 평가보증등급에서는 간단하고 안전한 TOE의 보안기능을 요구한다. 이를 위해 CC V3.0에서는 구조적 설계, 응집도, 결합도의 다양한 소프트웨어 공학 기법을 도입하였다. 구조적 설계는 초기화(initialization), 자체보호(self-protection) 및 비우회성(non-bypassability)을 분석하여 보안기능이 안전하게 구현되었는지를 분석한다. 응집도 및 결합도는 모듈 설계(modular design)의 모듈분해(module decomposition) 과정에서 소프트웨어 또는 모듈간의 연결 및 의존도를 판단하는데 사용되며, TOE 보안기능의 복잡도를 줄이는데 도움을 제공한다.

3. 제1부 소개 및 일반모델 개정내용

CC 제1부에서 주요 개정내용은 다음과 같다.

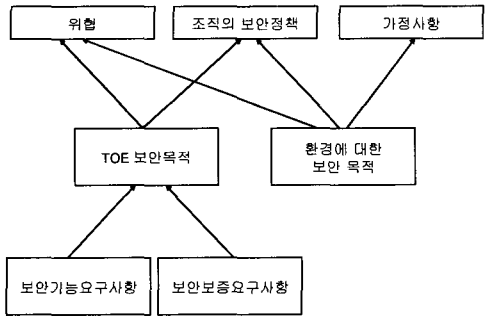
- 보안목적 수립을 위한 TOE 개발환경의 반영
- 보호프로파일/보안목표명세서 내용 변경
- EAL1에서 보호프로파일/보안목표명세서의 사용

보안목적을 수립할 때 TOE 개발환경의 반영한다는 것은 개발환경으로부터 발생되는 취약성을 사전에 제거하고, TOE의 정확한 구현을 통해 TOE의 안전·신뢰성을 충분히 보장함을 의미한다. (그림 1)은 CC V3.0에서 추가적으로 제시하고 있는 개발자 측면의 보안모델을 보여준다.

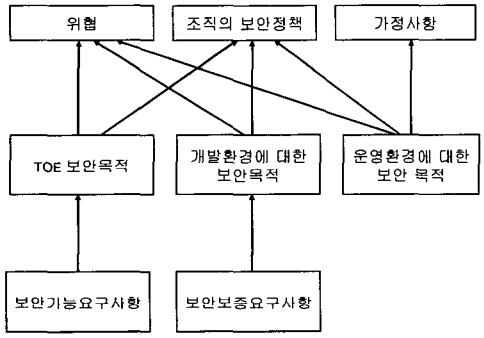


(그림 1) 개발자 개념 및 관계

(그림 2)와 (그림 3)은 개발환경에 대한 보안목적이 추가됨에 따라 보안요구사항인 보안기능요구사항과 보안보증요구사항을 도출하는 과정상의 차이점을 보여준다.



(그림 2) CC V2.*의 보안요구사항 관계



(그림 3) CC V3.0의 보안요구사항 관계

보호프로파일(PP, Protection Profile) 및 보안목표명세서(ST, Security Target) 내용에 대한 공통적인 변경사항은 다음과 같다. 첫째, TOE 설명로 통합되었다. 둘째, 이론적 근거(Rational)가 보안목적(Security objectives)과 보안요구사항(Security requirements)으로 통합되었다. 셋째, 적합성 수용(Conformance claims)이 추가되었다. 넷째, 보안목적(Security objectives)에 개발환경에 대한 보안목적(Security objectives for the development environment)이 추가되었다. 마지막으로, TOE 보안환경(TOE Security environment)이 보안문제 정의(Security problem definition)로 명칭이 변경되었다.

<표 2>, <표 3>, <표 4>, <표 5>는 CC V2.*과 V3.0에서 PP/ST 내용에 대한 변경사항을 전반적으로 보여준다.

〈표 2〉 CC V2.*의 PP 내용

PP 내용		패밀리 명
PP 소개	PP 식별	APE_INT
	PP 개요	
TOE 설명		APE_DES
TOE 보안환경	가정사항	APE_ENV
	위협	
	조직의 보안정책	
보안목적	TOE 보안목적	APE_OBJ
	환경에 대한 보안목적	
IT 보안 요구사항	TOE 보안기능요구사항	APE_REQ
	TOE 보증요구사항	
	IT 환경에 대한 보안요구사항	
보호프로파일 응용 시 주의사항		-
이론적 근거	보안목적의 이론적 근거	-
	보안요구사항의 이론적 근거	

〈표 3〉 CC V3.0의 PP 내용

PP 내용		패밀리 명
PP 소개	PP 참조	APE_INT
	TOE 개요	
적합성 수용	CC 적합성 수용	APE_CCL
	PP 수용	
	패키지 수용	
보안문제 정의	가정사항	APE_SPD
	조직의 보안정책	
	위협	
보안목적	TOE 보안목적	APE_OBJ
	개발환경에 대한 보안목적	
	운영환경에 대한 보안목적	
	보안목적의 이론적 근거	
확장컴포넌트 정의	확장 컴포넌트 정의	APE_ECD
보안 요구사항	TOE 보안기능요구사항	APE_REQ
	TOE 보증요구사항	
	보안요구사항의 이론적 근거	

〈표 4〉 CC V2.*의 ST 내용

ST 내용		패밀리 명
ST 소개	ST 식별	ASE_INT
	ST 개요	
TOE 설명		ASEDES
TOE 보안환경	가정사항	ASE_ENV
	위협	
	조직의 보안정책	
보안목적	TOE 보안목적	ASE_OBJ
	환경에 대한 보안목적	
IT 보안 요구사항	TOE 보안기능요구사항	ASE_REQ
	TOE 보증요구사항	
	IT 환경에 대한 보안요구사항	
TOE 요약명세	TOE 보안기능	ASE_TSS
	보증수단	
PP 수용	PP 참조	ASE_PPC
	PP 재정립	
	PP 추가사항	
이론적 근거	보안목적의 이론적 근거	-
	보안요구사항의 이론적 근거	

〈표 5〉 CC V3.0의 ST 내용

ST 내용		패밀리 명
ST 소개	ST 참조	ASE_INT
	TOE 참조	
	TOE 개요	
	TOE 설명	
적합성 수용	CC 적합성 수용	ASE_CCL
	PP 수용	
	패키지 수용	
보안문제 정의	가정사항	ASE_SPD
	조직의 보안정책	
	위협	
보안목적	TOE 보안목적	ASE_OBJ
	개발환경에 대한 보안목적	
	운영환경에 대한 보안목적	
	보안목적의 이론적 근거	
확장컴포넌트 정의	확장 컴포넌트 정의	ASE_ECD
보안 요구사항	TOE 보안기능요구사항	ASE_REQ
	TOE 보증요구사항	
	보안요구사항의 이론적 근거	
TOE 요약명세	TOE 요약명세	ASE_TSS

CC V3.0에서는 EAL1에서 낮은 보증이 가능한 PP/ST를 사용할 수 있다. EAL1에서 PP/ST가 사용될 경우, PP/ST 내용의 완전성(completeness)과 보안기능요구사항/보안보증요구사항의 의존성을 만족시킬 필요는 없다. 다시 말하면, PP/ST 내용을 모두 포함시켜 작성할 필요가 없다. 만일 낮은 보증 ST가 PP를 수용할 경우, 반드시 낮은 보증 PP를 수용해야 한다.

<표 6>과 <표 7>은 낮은 보증 PP/ST에 포함될 최소한의 PP/ST의 내용을 나타낸다.

〈표 6〉 EAL1의 PP내용

PP 내용		패밀리 명
PP 소개	PP 참조	APE_INT
	TOE 개요	
적합성 수용	CC 적합성 수용	APE_CCL
	보호프로파일 수용	
	패키지 수용	
확장컴포넌트 정의	확장 컴포넌트 정의	APE_ECD
보안목적	TOE 보안목적	APE_OBJ
	개발환경에 대한 보안목적	
	운영환경에 대한 보안목적	
	보안목적의 이론적 근거	
보안 요구사항	TOE 보안기능요구사항	APE_REQ
	TOE 보증요구사항	

〈표 7〉 EAL1의 ST 내용

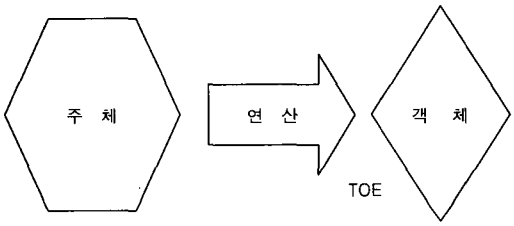
ST 내용		패밀리 명
보안목표명세서 소개	ST 참조	ASE_INT
	TOE 참조	
	TOE 개요	
	TOE 설명	
적합성 수용	CC 적합성 수용	ASE_CCL
	PP 수용	
	패키지 수용	
확장컴포넌트 정의	확장 컴포넌트 정의	ASE_ECD
보안목적	운영환경에 대한 보안목적	ASE_OBJ
보안 요구사항	TOE 보안기능요구사항	ASE_REQ
	TOE 보증요구사항	
TOE 요약명세	TOE 요약명세	ASE_TSS

4. 제2부 보안기능 컴포넌트 개정내용

CC 제2부에서 주요 개정내용은 다음과 같다.

- 개념적인 보안행위 모델 적용
- 보안기능 패밀리 구조 변경
- 보안기능 클래스 및 패밀리 변경

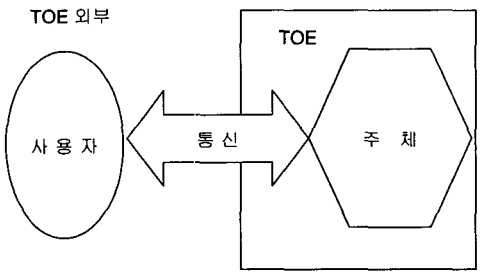
제2부의 모든 보안기능컴포넌트는 (그림 4)에서 정의된 '주체-연산-객체'의 개념적인 보안행위 모델을 사용한다.



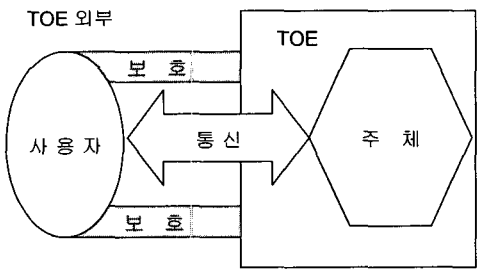
(그림 4) 보안행위 모델 개념

본래 CC V2.*에서는 세 개의 추상화된 모델을 사용한다. 첫째, 서로 다른 주체, 객체에 대한 구분 없이 TOE 전체에 대한 전역 속성을 설명하는 TSP(TOE 보안정책) 속성에 대한 모델로서 정보흐름, 프라이버시 등을 다룬다, 둘째, 서로 다른 주체, 객체간의 책임을 구분하는 TOE 자체의 보호를 위한 모델로서 접근통제, 보안관리 등을 다룬다. 마지막으로, 특정 구현을 설명하는 TSP 구현에 대한 모델로서 암호, 메커니즘, 알고리즘 등을 다룬다. 이와 같이, CC V2.*에서는 하나의 통일된 모델을 사용하지 않아 여러 개의 보안기능컴포넌트에 대해 독자의 이해가 매우 어려웠다. CC V3.0에서는 CC V2*에서 사용되는 세 개의 모델을 두 번째 모델('주체-연산-객체' 모델)로 통합하여 재구성하였다. 통합 및 재구성의 결과로써 보안기능컴포넌트의 클래스 및 패밀리 수가 각각 6개, 45개로 대폭 축소되었다.

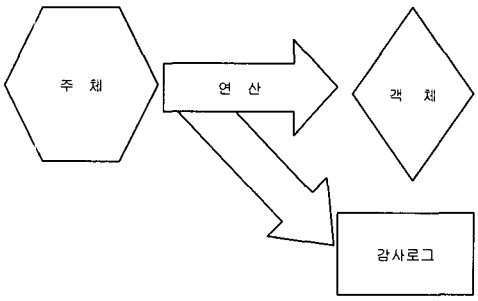
(그림 5), (그림 6), (그림 7), (그림 8)은 FDP(데이터 보호 및 프라이버시), FMI(기타) 클래스를 제외한, FIA(식별, 인증 및 연결), FCO(통신), FAU(감사), FPT(TSF 보호) 등 4개 클래스에 대한 개념적 구성을 보여준다. FDP는 위의 (그림 4)와 동일하며, TOE 내부 데이터 보호를 위한 보안행위를 다루며 기준과 보안속성을 정의한다. FIA는 사용자가 TOE 내의 주체와 어떻게 연결되어 있고, 주체에 대한 연결 결과가 무엇이며, 어떤 조건에서 연결이 해제되는 지를 정의한다. FCO는 사용자와 주체간의 안전한 통신을 제공하는 보안행위를 다룬다. FAU는 보안 사건의 기록 및 자동분석 등을 제공하는 보안행위를 다룬다. FPT는 고장, 물리적 공격, 자원고갈 등에 대한 TOE 자체의 보호를 위한 보안행위를 다룬다.



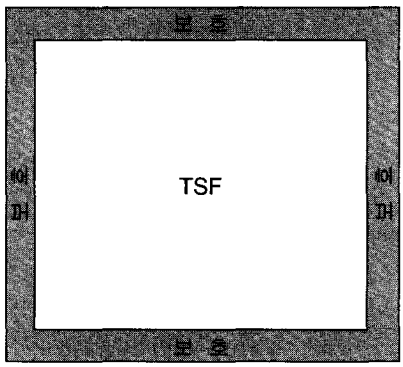
(그림 5) FIA(식별, 인증 및 연결)



(그림 6) FCO(통신)



(그림 7) FAU(감사)



(그림 8) FPS(TSF 보호)

(그림 5), (그림 6), (그림 7), (그림 8)은 FDP(데이터 보호 및 프라이버시), FMI(기타) 클래스를 제외한, FIA(식별, 인증 및 연결), FCO(통신), FAU(감사), FPT(TSF 보호) 등 4개 클래스에 대한 개념적 구성을 보여준다. FDP는 위의 (그림 4)와 동일하며, TOE 내부 데이터 보호를 위한 보안행위를 다루며 기준과 보안속성을 정의한다. FIA는 사용자가 TOE 내의 주체와 어떻게 연결되어 있고, 주체에 대한 연결 결과가 무엇이며, 어떤 조건에서 연결이 해제되는 지를 정의한다. FCO는 사용자와 주체간의 안전한 통신을 제공하는 보안행위를 다룬다. FAU는 보안 사건의 기록 및 자동분석 등을 제공하는 보안행위를 다룬다. FPT는 고장, 물리적 공격, 자원고갈 등에 대한 TOE 자체의 보호를 위한 보안행위를 다룬다.

<표 8>과 같이 보안기능의 패밀리 구조에서는 주체와 객체간의 연산이 필요한 경우 관련 연산(Associated operation)에 해당 연산을 기술하여 PP/ST 작성자가 쉽게 이를 사용할 수 있도록 하였다. 그리고 패밀리 구조에서 명칭이 일부 변경되었으며, 컴포넌트에서는 계층관계 바로 뒤에 종속관계를 위치시켰다.

〈표 8〉 CC V2.*과 V3.0의 패밀리 구조 비교

보안기능 패밀리 구조	
CC V2.*	CC V3.0
패밀리명	패밀리명
패밀리 개요	패밀리 설명
계층관계 및 설명	계층관계 및 설명
관리	관련 연산
감사	감사
컴포넌트	컴포넌트

<표 9>는 CC V3.0과 CC V2.*의 보안기능컴포넌트 변경내용을 종합적으로 보여준다. 'O'는 신규로 추가된 패밀리를 표시하며, 빈 칸은 CC V3.0과 CC V2.*의 변경사항이 거의 없다는 것을 의미한다. <표 9>를 자세히 살펴보면, CC V3.0에서는 TSP를 표현하는 패밀리를 전혀 찾아 볼 수 없다. 이것은 '주체-연산-객체' 모델이 적용된 일부 컴포넌트에서 TSP를 다루기 때문이다.

CC V2.*의 FDP(사용자 데이터 보호), FMT(보안관리), FPR(프라이버시)는 FDP(데이터 보호 및 프라이버시)에, FIA(식별 및 인증), FTA(TOE 접근)는 FIA(식별, 인증 및 연결)에 통합되었다. CC V2.*의 FDP_IFC(정보흐름통제 정책), FDP_IFF(정보흐름통제 기능) 등의 패밀리가 삭제되었다. CC V3.0에서 신규로 추가된 클래스는 FMI(기타)이며, 추가된 패밀리는 FIA_TBR(TSF 연결규칙), FIA_SUA(주체인증), FMI_RND(난수생성), FMI_CHO(선택) 등이 있다.

〈표 9〉 CC V3.0의 보안기능컴포넌트 변경내용 분석

CC V3.0 보안기능컴포넌트		CC V2.* 보안기능컴포넌트
클래스 명	패밀리 명	패밀리 명
FDP (데이터 보호 및 프라이버시)	FDP_ACC(접근통제)	FDP_ACC/ACF(접근통제 정책/기능)
	FDP_ROL(복구)	
	FDP_ISA(보안속성 초기화)	FMT_MSA.3(보안속성 관리)
	FDP_MSA(보안속성 관리)	FMT_MSA.1/2(보안속성 관리)
	FDP_OSD(객체/주체 소멸)	FMT_REV(폐기)
	FDP_UNL(연계불가성)	FPR_UNL(연계불가성)
	FDP_UNO(관찰불가성)	FPR_UNO(관찰불가성)
FIA (식별, 인증 및 연결)	FIA_URE(사용자 등록)	FIA_ATD(사용자 속성 정의)
	FIA_QAD(인증데이터 품질)	FIA_SOS(비밀정보의 검증 및 생성)
	FIA_UID(사용자 식별)	
	FIA_UAU(사용자 인증)	
	FIA_AFL(인증 실패)	
	FIA_TBR(TSF 연결규칙)	○
	FIA_USB(사용자-주체 연결)	
	FIA_SUA(주체 인증)	○
	FIA_TIN(TSF 정보)	FTA_TAB/TAH(TOE 접근경고/접근이력)
	FIA_LOB(연결 잠금)	FTA_SSL(세션잠금)
	FIA_TOB(연결 종료)	FTA_SSL(세션잠금)
FCO (통신)	FCO_ETC(TSF 통제 외부로 데이터 유출)	FDP_ETC(TSF 통제 외부로 데이터 유출)
	FCO_TED(유출 데이터의 번역)	FPT_TDC(TSF간 전송되는 TSF 데이터의 일관성)
	FCO_AED(유출 데이터의 가용성)	FPT_ITA(외부전송 TSF 데이터의 가용성)
	FCO_CED(유출 데이터의 비밀성)	FPT_ITC(외부전송 TSF 데이터의 비밀성)
	FCO_IED(유출 데이터의 무결성)	FPT_ITI(외부전송 TSF 데이터의 무결성)
	FCO_NRE(유출 데이터의 부인방지)	FCO_NRO(발신 부인방지)
	FCO_UNE(유출 데이터의 관찰불가성)	FTP_ITC/TRP(안전한 채널/경로)
	FCO_ITC(TSF 통제 외부로부터 데이터 유입)	FDP_ITC(TSF 통제 외부로부터 데이터 유입)
	FCO_TID(유입 데이터의 번역)	FPT_TDC(TSF간 전송되는 TSF 데이터의 일관성)
	FCO_CID(유입 데이터의 비밀성)	FDP_UTC(TSF간 전송되는 데이터 비밀성)
	FCO_IID(유입 데이터의 무결성)	FDP_UIT(TSF간 전송되는 데이터 무결성)
	FCO_NRI(유입 데이터의 부인방지)	FCO_NRR(수신 부인방지)
FAU (보안감사)	FAU_GEN(보안감사 데이터 생성)	
	FAU_SAA (보안감사 분석)	
	FAU_ARP(보안감사 자동생성)	
FPT (TSF 보호)	FPT_TOU(사용자 시험)	FPT_AMT(하부추상기계 시험)
	FPT_TST(TSF 자체 시험)	
	FPT_FLT(오류에 대한 내성)	FRU_FLT(오류에 대한 내성)
	FPT_FLS(안전한 상태유지)	
	FPT_RCV(안전한 복구)	
	FPT_PHP(TSF 물리적 보호)	
	FPT_PRI(자원사용 우선순위)	FRU_PRI(자원사용 우선순위)
	FPT_RSA(자원 할당)	FRU_RSA(자원 할당)
	FPT_RIP(잔여정보 보호)	FDP_RIP(잔여정보 보호)
FMI (기타)	FMI_RND(난수 생성)	○
	FMI_TIM(타임스탬프)	FPT_STM(타임스탬프)
	FMI_CHO(선택)	○

5. 제3부 보안 보증 컴포넌트 개정내용

CC 제3부에서 주요 개정내용은 다음과 같다.

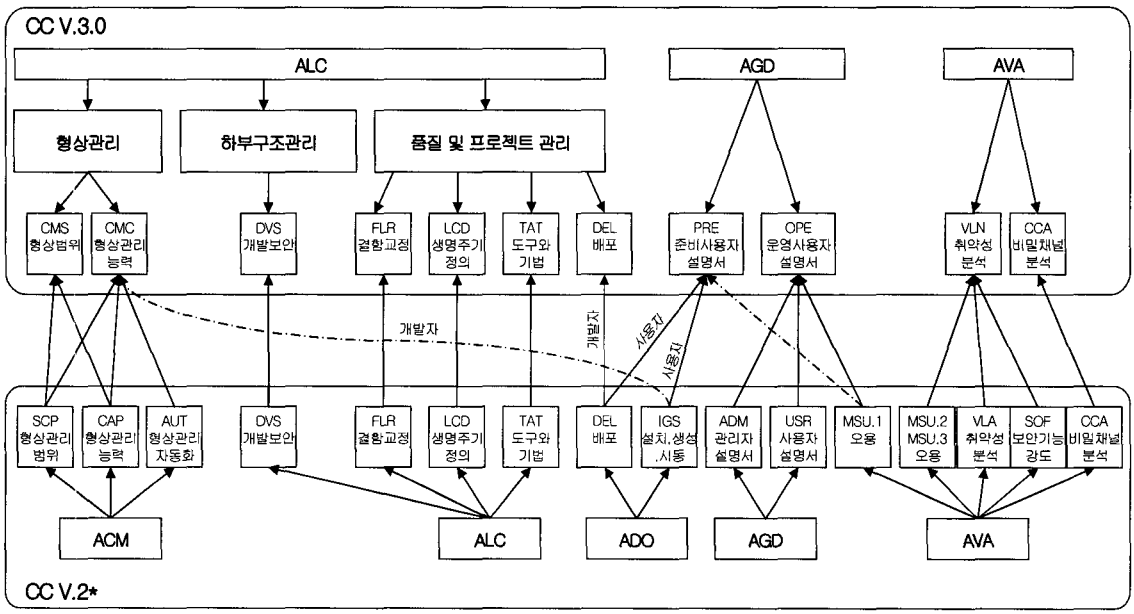
- 보안보증 클래스 및 패밀리 변경
- 평가보증등급(EAL1-7) 구성 변경

<표 10>은 CC V3.0과 CC V2.*의 보안보증컴포넌트 변경내용을 종합적으로 보여준다. 'O'는 신규로 추가된 패밀리를 표시하며, 빈 칸은 CC V3.0과 CC V2.*의 변경사항이 거의 없다는 것을 의미한다.

CC V2.*의 ADV에서 적용하는 폭포수 모델은 실세계에 적합하지 않아 CC V3.0에서 ATV_ARC (보안 아키텍처), ADV_TDS(TOE 설계), 등의 새로운 구조(architectural structure)를 채택하였다. CC V2.*의 ADV_HLD(기본설계)와 ADV(LLD)는 ADV_TDS에 통합되었다. EAL5 이상의 고등급 평가/개발방법론을 구체적으로 제시하기 위해 ADV INT(TOE 내부)을 확장시켰다. 특히, ADV_INT의 모듈설계에서는 높은 평가보증등급을 충족시키기 위해 TOE 기능의 복잡도를 줄이는 방안으로 소프트웨어 공학기법인 응집도, 결합도 개념을 도입하였다. ATE(시험)도 ADV가 내용이 변경됨에 따라 약간 변경되었다.

CC V2.*에서 사용되는 ACM/ALC/ADO/AGD/AVA는 사용자 사이트와 개발자의 사이트를 구분하여 (그림 9)와 같이 ALC/AGD/AVA로 재구성하였다.

<표 10>에서와 같이 현재 개발 중인 보증요구사항으로는 ADV 클래스의 ADV_CMP(복합 보증), ADV_PLT(플랫폼 보증)이 있다. ADV_CMP는 다른 TOE와 안전하게 결합될 수 있도록 TOE를 기술하기 위한 요구사항을 정의하고, 상위 TOE와 하위 TOE간의 의존성을 기술할 것을 요구한다. ADV_PLT는 TOE가 의존하는 상용 하드웨어 플랫폼을 지정하기 위한 요구사항을 정의하도록 권장한다.



(그림 9) CC V3.0의 ALC/AGD/AVA와 CC V2.*의 ACM/ALC/ADO/AGD/AVA의 비교

〈표 10〉 CC V3.0의 보안보증컴포넌트 변경내용 분석

CC V3.0 보안보증컴포넌트		CC V2.* 보안보증컴포넌트
클래스 명	패밀리 명	패밀리 명
ADV (개발)	ADV_ARC(구조적 설계)	○
	ADV_FSP(기능 명세)	
	ADV_IMP(구현 표현)	
	ADV_INT(TSF 내부)	
	ADV_SPM(보안정책 모델링)	
	ADV_TDS(TOE 설계)	ADV_HLD(기본설계) ADV_LLD(상세설계)
AGD (설명서)	AGO_OPE(운영 사용자설명서)	AGD_ADM(관리자 설명서) AGD_USR(사용자 설명서) AVA_MSU.1(오용)
	AGO_PRE(준비 사용자설명서)	ADO_DEL(배포) ADO_IGS(설치, 생성, 시동) AVA_MSU.1(오용)
ALC (생명주기 지원)	ALC_CMC(형상관리 능력)	ACM_SCP(형상관리 범위) ACM_CAP(형상관리 능력)
	ALC_CMS(형상 범위)	ACM_CAP(형상관리 능력) ACM_AUT(형상관리 자동화) ADO_IGS(설치, 생성, 시동)
	ALC_DEL(배포)	
	ALC_DVS(개발 보안)	
	ALC_FLR(결함 교정)	
	ALC_LCD(생명주기 정의)	
	ALC_TAT(도구와 기법)	
ASE (ST 평가)	ASE_CCL(적합성 수용)	ASE_PPC(PP 수용)
	ASE_ECD(확장 컴포넌트 정의)	ASE_REQ(보안요구사항)
	ASE_INT(ST 소개)	
	ASE_OBJ(보안목적)	
	ASE_REQ(보안요구사항)	
	ASE_SPD(보안문제정의)	ASE_ENV(보안환경)
	ASE_TSS(TOE 요약 명세)	
ATE (시험)	ATE_COV(범위)	
	ATE_DPT(상세수준)	
	ATE_FUN(기능시험)	
	ARE_IND(독립시험)	
AVA (취약성 평가)	AVA_CCA(비밀채널 분석)	
	AVA_VAN(취약성 분석)	AVA_SOF(TOE 보안기능 강도) AVA_VLA(취약성 분석) AVA_MSU.1/2(오용)

〈표 11〉 CC V2.*의 평가보증등급 요약

보증 클래스	보증 패밀리	평가보증등급에 따른 보증 컴포넌트						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
형상관리	ACM_AUT				**1**	1	2	2
	ACM_CAP	**1**	2	3	4	4	5	5
	ACM_SCP			**1**	2	3	3	3
배포 및 운영	ADO_DEL		**1**	1	2	2	2	3
	ADO_IGS	**1**	1	1	1	1	1	1
개발	ADV_FSP	**1**	1	1	**2**	**3**	3	4
	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
	ADV_SPM				**1**	**3**	3	3
	AGD_ADM	**1**	1	1	1	1	1	1
설명서	AGD_USR	**1**	1	1	1	1	1	1
	ALC_DVS			**1**	1	1	2	2
생명주기 지원	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
시험	ATE_COV		**1**	**2**	2	2	3	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
취약성 평가	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

〈표 12〉 CC V3.0의 평가보증등급 요약

보증 클래스	보증 패밀리	평가보증등급에 따른 보증 컴포넌트						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
개발	ADV_ARC		**1**	1	1	**2**	2	2
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**
	ADV_IMP				**1**	1	**2**	2
	ADV_INT					**2**	**3**	**4**
	ADV_SPM					**1**	1	1
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**
설명서	AGD_OPE	**1**	1	1	1	1	1	1
	AGD_PRE	**1**	1	1	1	1	1	1
생명주기 지원	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5
	ALC_DEL		**1**	1	1	1	1	1
	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	3
	ALC_TAT				**1**	**2**	**3**	3
보안목표 명세서 평가	ASE_CCL	**1**	1	1	1	1	1	1
	ASE_ECD	**1**	1	1	1	1	1	1
	ASE_INT	**1**	1	1	1	1	1	1
	ASE_OBJ	**1**	**2**	2	2	2	2	2
	ASE_REQ	**1**	**2**	2	2	2	2	2
	ASE_SPD		**1**	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
시험	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
취약성 평가	AVA_CCA					**1**	2	2
	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	**6**

CC V3.0에서는 ASE(보안목표명세서 평가)도 평가보증등급(EAL1-EAL7)을 결정하는 기준으로 이용되고 있다. CC V2.*의 ACM(형상관리)과 ADO(배포 및 운영)은 CC V3.0의 ALC(생명주기 지원)과 AGD(설명서)에 통합되었다. EAL1에서는 공용 도메인에 기반한 AVA_VAN(취약성 분석)이 추가로 요구된다.

<표 11>과 <표 12>에서는 CC V2.*과 CC V3.0의 평가보증등급 요약의 차이점을 보여 준다.

6. 결 론

본 논문에서는 CC V3.0의 개정내용을 상세하게 분석하였다. 분석내용을 요약하면 다음과 같다. 첫째, CC에서 사용되는 개념과 용어, 내용을 구체화하고 명확하게 표현하였다. 둘째, 보안목적 수립 시 개발자 보안환경을 추가시켜, 이를 통해 보안보증요구사항을 도출하도록 하였다. 셋째, CC V2.*의 보안기능컴포넌트에서 사용된 복수개의 모델을 '주체-연산-객체'의 보안행위 모델을 통합시켜 보안기능 컴포넌트를 단순화하였다. 마지막으로, 다양한 소프트웨어 공학기법 적용을 통해 EAL5 이상의 고등급 평가/개발방법론 구현을 구체화시켰다.

ISO CC 프로젝트는 2008년까지 국제표준을 목표로 CC V3.0 개정작업을 적극 추진 중에 있으며, 이와 동시에 CC가 근간이 되는 공통평가방법

론(18405), PP/ST 작성 가이드(15446), 암호모듈 보안요구사항(19790), 운영시스템 보안성 평가(19791)의 개정작업도 동시에 진행하고 있다.

향후, 국가적 차원에서 CC V2.*에서 V3.0의 변화에 신속하고 효율적으로 대처하기 위해서는 국제상호인정협정(CCRA)에 인증서 발행국으로 가능한 빨리 가입하여 CC V3.0의 개정작업에 적극적으로 참여하여야 할 것이다.

참 고 문 헌

[1] Haruki Tabuchi, "Business aspect of security evaluation and CCRA", 제10회 정보보호 심포지움, Jun 2005.

[2] Common Criteria Project/ISO, Common Criteria for Information Technology Security Evaluation Version 3 draft (ISO/IEC 15408), April 2005.

노 병 규

1988년 충남대학교 이과대학 전산학 학사
1995년 충남대학교 이과대학 전산학 석사
2006년 순천향대학교 공과대학 전산학 박사
1988년 한국전자통신연구원
1997년 한국정보보호진흥원 평가2팀장, 평가기준팀장, 기반보호기획팀장
2005년~현재 한국정보보호진흥원 보안성평가단 단장
관심분야 : 정보보호시스템 평가, 시스템·네트워크 정보보호

김 영 태

1997년 동국대학교 공과대학 전자계산학과 공학사
2001년 동국대학교 컴퓨터공학과 공학석사
1997년 한국상업은행 전산정보부 연구원
2001년~현재 한국정보보호진흥원 보안성평가센터 선임연구원
관심분야 : 홈네트워크 보안, 정보보증, 보안성평가

박 두 순

1988년 고려대학교 전산학전공 (이학박사)
1985년 순천향대학교 정보기술공학부 교수
2000년~현재 한국 멀티미디어학회 편집위원
2004년 미국 U. of Colorado 객원교수
2002년 순천향대학교 공과대학 학장
2000년 한국 멀티미디어학회 이사, 논문지 분과위원장
2001년 한국정보처리학회 편집위원
관심분야 : 병렬처리, 멀티미디어 컨텐츠, 데이터마이닝, 유비쿼터스 컴퓨팅, 컴퓨터 교육

김 점 구

광운대학교 전자계산학과 이학사
광운대학교 전자계산학과 이학석사
한남대학교 컴퓨터공학과 공학박사
(주) 제성프로젝트 연구원
(주) 시사컴퓨토피아 인터넷사업 본부장
현재 남서울대학교 컴퓨터학과 교수
관심분야 : 정보보호, 컴퓨터 네트워크, 무선통신