情 報 保 護 學 會 誌
第 14 券 第 4 號, 2004. 8

공통평가기준(CC)과 공통평가방법론(CEM)의 변경내용 분석*

강 연 희**, 김 정 대**, 방 영 환**, 최 성 자**, 이 강 수**

요 약

국가 사회 각 분야(정부, 공공기관 및 민간기관)의 정보보호시스템에 의한 정보처리 의존도가 증가하고 있으며 정보보호 수준강화를 위한 평가업무의 수요 또한 늘어가고 있다. 이에 발맞추어 현재 정보보호시스템 평가에 대한 상호인증을 위해 공통평가기준(CC : Common Criteria)과 공통평가방법론(CEM : Common Evaluation Methodology)을 사용하고 있다. 본 논문에서는 정보보호시스템의 신뢰성의 확보와 상호인증을 위한 지침으로써 CC와 CEM에 대한 변화과정 및 특징을 분석하였으며 앞으로 이를 반영한 국제동향에 능동적인 대처와 효율적인 평가에 기여할 것으로 기대된다. 또한, 평가참여자(평가신청자, 개발자, 평가자, 감독자 등)의 역할도 변화의 흐름에 유연하게 대응해야 하며 이러한 지식을 토대로 객관적이며 체계적인 평가계획을 수립하는데 이용할 수 있을 것이다.

Ⅰ. 서 론

정보화 역기능을 해결하기 위해서는 안전성과 신뢰성이 검증된 정보보호시스템을 사용하여 정보보호 수준을 향상시킬 수 있는 정보보호시스템 평가·인증에 대한 필요성이 높아지고 있다. 그러나 정보보호시스템을 서로 다른 평가기준을 적용하여 평가를 함으로써 발생되는 이중의 비용소모와 시간소모의 문제점이 발생하게 되었다. 이를 해결하기 위하여 평가결과의 상호인증 추진을 목적으로 현존하는 평가기준을 조화하기 위한 노력의 결과로 ISO/IEC에서 CC Version 2.1 (ISO/IEC 15408)을 1999년 6월에 국제표준으로 발표했으며 우리나라에서는 정보통신부에서 정보보호시스템 공통평가기준으로 고시하고 있다[1]. 현재 CC는 CC version 2.2를 2004년 1월 공식적으로 발표했으며 비공식 문서인 CC version 2.4를 개발중에 있다. 또한 CC를 기반으로 적절하고 비용 효과적인 평가를 수행할 수 있는 골격을 제시하며 효율적인 평가도출을 위해 평가받은 제품의 등급유지 및 평가결과의 상호인정을 목적으로 하는 CEM 역시 CC와 함께 개정 작업이 계속되고 있다. 이러한 CC와 CEM의 현재 동향을 분석함으로써 실제 평가에 적용하기 위한 방향을 살펴보고 변화 특징에 대해서 정확히 파악하고 대처할 필요성이 존재한다.

본 논문에서는 현재 발표된 CC와 CEM에 대한 변화과정에 대해서 파악한 후 효율적인 평가를 할 수 있도록 방향을 제시한다. 본 논문의 2장에서는 CC와 CEM의 간략한 개념소개와 공식 문서의 개발 및 변화 과정에 대해서 조사(연구)하였으며 CC와 CEM의 총체적 변화 흐름을 제시하도록 한다. 3장에서는 향후 CC와 CEM의 동향에 대해 분석 및 제시하며 변화에 대한 특징과 평가 적용 방안에 대해 살펴보도록 한다. 마지막으로 4장에서 위의 사항들에 대한 평가 및 결론을 맺는다.

Ⅱ. CC와 CEM의 배경

1. 공통평가기준(CC)

CC는 미국의 TCSEC, 유럽의 ITSEC, 카나다의

* 본 논문은 과학기술부 지역협력연구사업(R12-2003-004-01001-0) 지원으로 수행되었음.
** 한남대학교 컴퓨터공학과 {dusi82, bangyh, jdcom}@se.hannam.ac.kr, irecomm@dreamwiz.com, lee@eve.hannam.ac.kr

CTCPEC기준을 통합한 표준으로써 평가기준의 상호 인증을 위한 골격 제시를 위해 개발되었으며, 정보보호시스템을 위한 평가기준의 국제표준일 뿐 아니라 우리나라의 정보통신부 표준이다[2,3]. CC는 모든 정보보호제품 및 시스템에서 필요로 하는 보안기능요구사항의 전체집합을 클래스-패밀리-컴포넌트를 통해 계층적으로 분류하고 있다. 보증요구사항(컴포넌트)에 대해서 EAL1~EAL7과 같이 7단계의 보증수준별로 정의하고 있으며 상위의 보증수준은 하위의 보안수준보다 완전하고, 엄격하며 정형적이므로 보증수준간에는 완전성, 엄격성 및 정형성 관계를 갖는다[1,6,7].

정보보호시스템(TOE : Target of Evaluation, 평가대상물)의 제품유형에 따라 보안기능요구사항의 일부를 선택하고 7단계의 보안수준 중 하나를 택하여 보호프로파일(PP : protection profile) 또는 보안목표명세서(ST : security target)를 구성한다. PP는 정보보호제품의 유형(방화벽, 스마트카드, 운영체제 등)의 특성에 따라 CC의 보안기능요구사항과 보증요구 사항으로부터 선택한 제품 유형별 공통 보안요구사항명세서에 해당하며 ST는 특정 제품(예 : Oracle 9i)의 보안요구사항명세서에 해당한다[8].

2. 공통평가방법론(CEM)

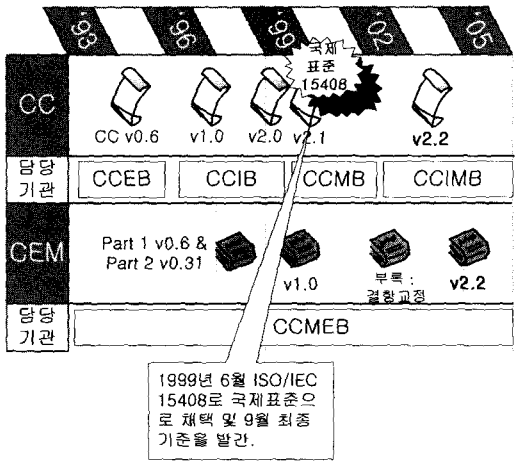
CEM은 IT 보안평가를 위한 공통평가기준(CC)을 위한 지침 문서로써 적절하고 비용 효과적인 평가를 수행할 수 있는 골격을 제시하여 효율적인 평가결과를 도출할 수 있도록 하며 평가받은 제품의 등급유지 및 평가결과의 상호인정을 목적으로 한다. CEM은 CC에 정의된 기준과 평가증거를 사용하여, CC 평가 지침에 따른 평가자가 수행해야하는 최소한의 행동을기술하고 있다. CC 구조(즉, 클래스, 패밀리, 컴포넌트, 요소)와 CEM의 구조사이에는 직접적인 관계가 있으며 CC의 클래스-컴포넌트-평가자요구사항이 각각 CEM의 활동-하부활동-행동과 매핑된다[1,12]. 그러나, 몇몇 CEM 업무단위는 CC 개발자 행동, 내용과 표현 요소의 주된 요구사항으로부터 생성될 수 있다. CEM은 1997년도 CEM Part 1 Version 0.6 발표를 시작으로 반복된 개정을 통하여 현재 EAL1~4까지의 정보보호제품 평가에 활용하고 있으며 비공식 문서로 Version 2.4가 개발 중에 있다.

3. CC와 CEM의 개발 배경 및 연혁

CC와 CEM은 정보보호제품의 평가에 관한 지침으로써 국제적으로 단일화하려는 노력의 산물이다. 정보보호 기술의 시장성 확보와 기술개발의 방향성을 제공하며 수요자 측면에서는 제품에 대한 불확실성을 감소시키는 효과를 가져온다. 근본적으로 각 국의 상이한 평가기준을 단일화하고자 하는 요인은 정보의 국제화에 기인한다고 할 수 있으며 국제적 정보화를 촉진시키기 위해서 평가기준 및 방법론의 단일화에 관심이 고조된 결과이다.

3.1 CC와 CEM의 개발 연혁

TCSEC, ITSEC, CTCPEC 등 기존의 서로 다른 평가기준의 시행은 비용과 시간 소모 등의 문제점을 야기했으며 이를 극복하기 위해서 1994년 6월 CC 개발을 시작으로 현재 CC v2.2를 2003년 12월에 제정하였다. CEM은 범위를 확정하는 1단계, CC를 분석하는 2단계, CEM 모델의 드래프트를 작성하는 3단계, PP와 TOE를 위한 평가방법론을 제시하는 4단계, 향후 평가방법론을 개발하는 5단계를 거쳐 CEM을 시험적으로 적용시키는 총 6단계로 나누어 개발을 시작하였다. [그림 1]은 공식적으로 발표된 CC와 CEM의 개발 연혁을 그림으로 나타낸 것이며 개정 작업이 계속되어 오면서 담당기관의 변화도 볼 수 있다.

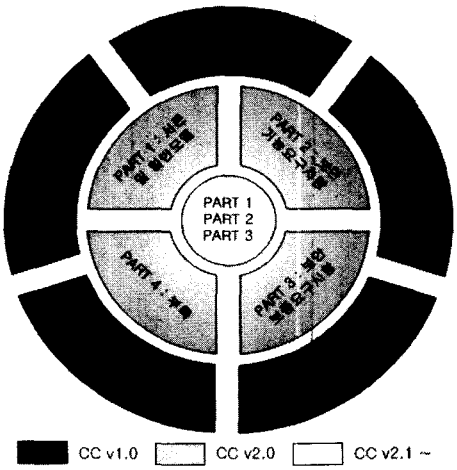


[그림 1] CC와 CEM의 개발 연혁

3.2 공식적인 CC와 CEM의 변경 내용

(1) CC의 변화

CC는 국제표준 15408로 채택되기 이전 CC v1.0



〔그림 2〕 CC 구성 변화

에서 CC v2.0, CC v2.1로의 개정 문서에 괄목할 만한 변경사항이 존재한다. 〔그림 2〕는 CC 구성 변화를 나타내며 CC v1.0은 서론 및 일반모델, 보안기능요구사항, 보안보증요구사항, 미리 정의된 보호프로파일, 등록 절차의 5개 파트로 구성되며 CC v2.0은 소개 및 일반모델, 보안기능요구사항, 보안보증요구사항, 부록의 4개 파트로 구성된다. CC v2.1 이후부터는 소개 및 일반모델, 보안기능요구사항, 보안보증요구사항의 3개 파트로 구성되며 CC가 개정됨에 따라 불필요하게 나뉘어져 있던 파트들을 연관된 파트에 통합시키거나 제외시켰다. 또한 Part 2와 Part 3의 클래스가 추가되었으며 패밀리의 평가보증등급별로의 분류사항 개정, PP 및 ST에 패밀리가 추가되었다 [13,14,15]

〔표 1〕과 〔표 2〕는 보안기능요구사항과 보증요구사항에 대한 추가된 클래스 변화를 나타내며 〔그림 3〕과 〔그림 4〕는 각각 PP와 ST의 패밀리 변화를 보여준다. 문서가 개정되면서 PP와 ST에 추가된 패밀리가 존재하지만 문서에 포함될 구성요소, 즉 목록은 변화하지 않으며 CC v2.0부터 구성요소와 패밀리의 1대 1 대응을 이루도록 구성되었다. 마지막으로 CC v2.0부터 개발(ADV) 클래스의 보안정책모델(ADV_SPM) 패밀리가 추가되었다.

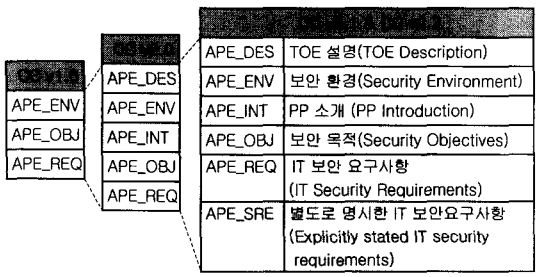
내용상 CC v2.0과 CC v2.1과의 차이점은 거의 없으나, CC v2.1은 ISO/IEC 15408 획득 과정에서 표준문서로의 수정되어 국제표준으로 채택되었다. 최근 CC v2.1과 CC v2.2로의 변화 또한 "최소한"이라는 용어 삭제 이외 차이점은 거의 존재하지 않으며 CC v2.1과 CC v2.2는 현재 평가에 적용 가능하다.

〔표 1〕 CC v2.0에 추가된 보안기능요구사항 클래스

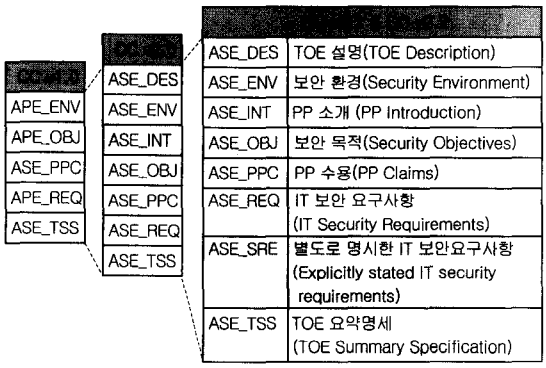
FAU	보안감사 (Security Audit)	보안활동과 관련된 정보를 인식, 기록, 저장 및 분석
FCO	통신(Communication)	데이터 교환시 송수신자의 신원 보증 및 확인
FCS	암호지원 (Cryptographic Support)	암호 운용 및 키관리
FDP	사용자 데이터 보호 (User Data Protection)	사용자 데이터 보호
FIA	식별 및 인증 (Identification & Authentication)	사용자의 신원확인 및 검증
FMT	보안관리 (Security Management)	TSF 데이터, 보안속성, 보안기능의 관리
FPR	프라이버시(Pricvacy)	인가되지 않은 사용자의 ID 및 정보 도용 방지
FPT	TSF 보호 (Protection of Trusted Security Functions)	보안기능 관련 데이터 보호 및 관리
FRU	자원활용 (Resource Utilization)	TOE 자원의 가용성 지원
FTA	TOE 접근(TOE Access)	TOE에 대한 세션 설정 및 보호
FTP	안전한 경로/채널 (Trusted Path/Channel)	사용자-TSF, TSF-TSF간의 안전한 통신채널 확보

〔표 2〕 CC v2.0에 추가된 보안보증요구사항 클래스

APE	보호프로파일 평가 (Protection Profile Evaluation)	PP 구성의 완전성과 일치성 확인 및 검토
ASE	보안목표명세서 평가 (SEcurity Target Evaluation)	ST 구성의 완전성과 일치성 확인 및 검토
ACM	형상관리 (Configuration Management)	TOE의 무결성이 유지되고 있는지 확인
ADO	배포 및 운영 (Delivery and Operation)	TOE의 배포, 생성, 설치, 시동에 필요한 수단, 절차 및 표준을 확인
ADV	개발 (Development)	TOE의 개발 과정의 완전성 및 일치성 확인 및 검토
AGD	설명서 (Guidance Documents)	TOE를 안전하게 운영하기 위한 지침서 확인
ALC	생명주기 지원 (Life Cycle Support)	TOE의 생명주기와 관련된 사항 확인
ATE	시험(Test)	TOE가 기능요구사항을 충족시키는지 확인
AVA	취약성 분석 (Vulnerability Analysis)	TOE 개발 및 운영 중에 나타나거나 잠재적인 취약성 확인
AMA	보증의 유지 (Maintenance of Assurance)	TOE나 환경에 변경에도 보안목표를 만족시킴을 보임 (보증)



〔그림 3〕 PP 패밀리 변화



〔그림 4〕 ST 패밀리 변화

(2) CEM의 변화

CEM Part 1 v0.6은 드래프트 문서로써 CEM v2.2까지 변화가 없으며 CEM Part 2는 v0.31이 발표된 이후 CEM v1.0을 제정하였고 2002년 1월 Part 2의 부록으로 "결함교정" 문서가 발간되었다. 이후 CEM은 CC v2.2의 변경사항을 반영하여 CEM v2.2로 개정되었다. CEM의 주목할 만한 변화는 CC v2.2에서 CC의 증거요구사항과 평가자요구사항에 대한 문장 표시 이외에 CC의 개정에 따른 변화를 들 수 있다.

Ⅲ. CC와 CEM의 동향

CC v2.4는 비공식 문서로써 현재 개발 중에 있으며 본 장에서는 CC v2.2와 CC v2.4를 비교 분석함으로써 평가의 향후 발전 방향에 능동적으로 대처할 수 있다.

1. CC v2.2와 CC v2.4의 비교 및 분석

CC v2.4는 CC v.2.2와 같이 Part 1, 2, 3의 총 3부로 구성되어 있으며 Part 2는 CC v2.4에서 그대로 사용한다.

1.1 Part 1 : 소개 및 일반모델의 변경 사항[4,9]

(1) 용어 추가

- OSP (Organizational Security Policy) : 조직의 보안 정책
- SAR (Security Assurance Requirement) : 보안 보증 요구사항
- SFR (Security Functional Requirement) : 보안 기능 요구사항

(2) 자산(assets) 의미 변경

CC v2.4에서는 자산의 의미가 개발 환경과 운용 환경으로 분류되며 의미의 분류로 인해 개발 환경상의 보안의 개념 및 관계가 확장되었다. 또한 운용 환경상의 보안, 즉 평가 개념과 관계에서 환경상의 자산에 대한 보안대책의 충족여부(취약성존재여부 : sufficient 또는 vulnerabilities)를 파악하여 취약성을 최소화한다. 변경된 사항은 〔표 3〕과 같다[6,7].

〔표 3〕 CC v2.2와 CC v2.4의 자산 의미 변경

	version 2.2	version 2.4
assets (자산)	- TOE의 보안대책으로 보호되는 정보 또는 자원	- 개발 환경상 : TOE 개발자가 가치를 두는 주체 - 운용 환경상 : TOE의 소유자가 가치를 두는 주체

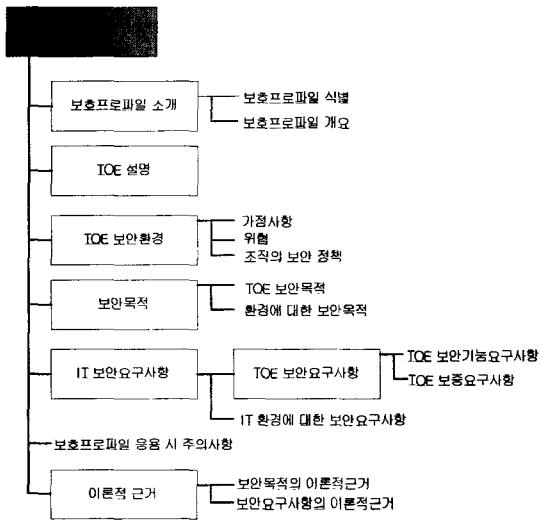
(3) 간소화 및 구체적 예시

CC v2.2에서 "보안기능이나 보증수단에 의해 식별된 요구사항"을 CC v2.4에서는 단순히 "요구사항" 이라 표현하는 등 군더더기 말들을 간소화시켰으며 실제 평가를 수행한 실례를 제시함으로써 평가 전반에 걸쳐 개발자 및 평가자의 이해력을 높일 수 있게 하였다.

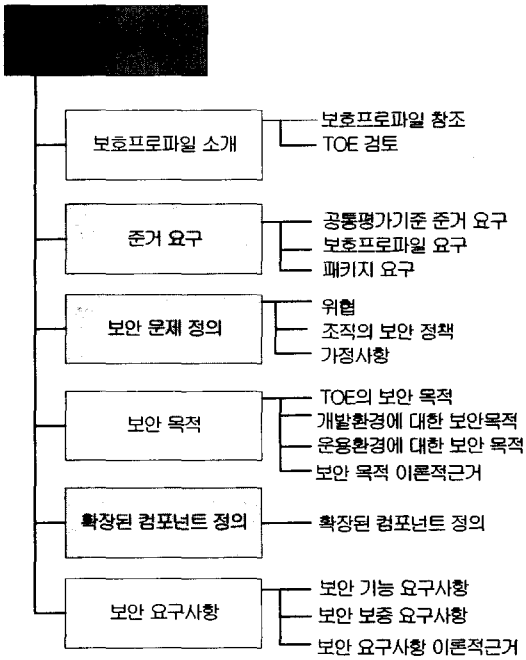
(4) 보호프로파일(PP) 평가 구성요소 변경

APE_DES(TOE설명), APE_ENV(TOE 보안환경), APE_INT(보호프로파일 소개), APE_OBJ(보안 목적), APE_REQ(IT보안요구사항), APE_SRE(별도로 명시한 IT보안요구사항)의 총 6개의 패밀리와 이론적 근거로 조합된 구성요소들이 CC v2.4에서 APE_INT(보호프로파일 소개), APE_CCL(준거 요구), ASE_SPD(보안 문제 정의), ASE_OBJ(보안 목표), ASE_ECD(확장된 컴포넌트 정의), ASE_

REQ(보안요구사항)로 변경되며 패밀리에 속한 컴포넌트 또한 변경된다. [그림 5]와 [그림 6]은 CC v2.2의 PP 평가 구성요소와 CC v2.4의 PP 평가 구성요소를 나타내며 TOE설명은 보호프로파일 소개 부분에 통합되었으며 APE_CCL(준거 요구), ASE_ECD(확장된 컴포넌트 체정의) 패밀리가 추가된 것을 볼 수 있다. 또한 TOE 보안 환경은 ASE_SPD(보안 문제 정의) 패밀리로 대되었으며 보안 목적에서는 환경에 대한 보안 목적을 좀더 세분화하였다. PP 평가 시에는 ST와 TOE 평가와 달리 평가 요약 보고서(ESR)를 작성하지 않으며 낮은 보증 보호프로파일(PP)에 대해서 보호프로파일 소개, 준거 요구, 확장된 컴포넌트 정의, 보안 요구사항으로 구성되며 보안 문제 정의와 보안 목적은 생략한다.



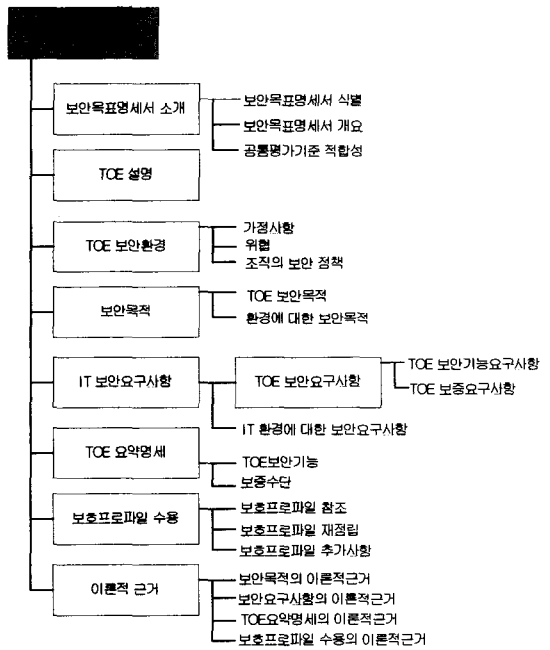
[그림 5] CC v2.2의 보호프로파일(PP) 구성요소



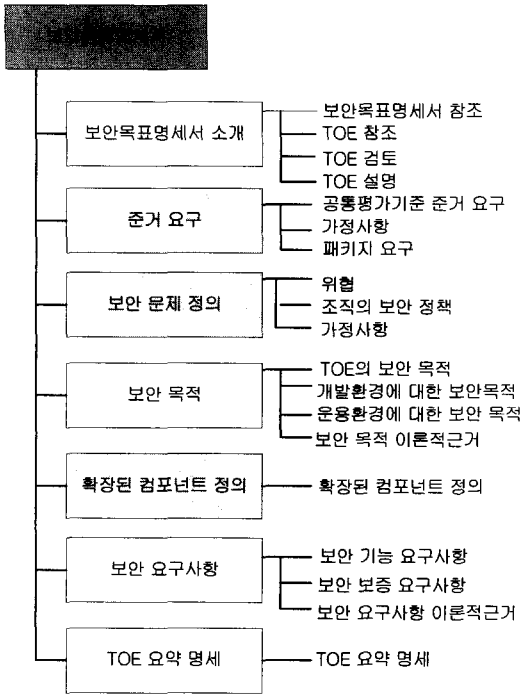
[그림 6] CC v2.4의 보호프로파일(PP) 구성요소

(5) 보안목표명세서(ST) 평가 구성요소 변경

보안목표명세서(ST)의 구성요소 변경은 보호프로파일(PP)의 구성요소 변경과 유사하다. ASE_DES(TOE설명), ASE_ENV(TOE보안환경), ASE_INT(보안목표명세서 소개), ASE_OBJ(보안 목적), ASE_PPC(보호프로파일 수용), ASE_REQ(IT보안요구사항), ASE_SRE(별도로 명시한 IT보안요구사항), ASE_TSS(TOE 요약명세)의 총 8개의 패밀리와 이론적 근거로 조합된 구성요소들이 CC v2.4에서 ASE_CCL(준거 요구), ASE_ECD(확장된 컴포넌트 정의), ASE_INT(보안목표명세서 소개), ASE_OBJ(보안 목표), ASE_REQ(보안요구사항), ASE_SPD(보안 문제 정의), ASE_TSS(TOE 요약명세)로 변경되며 구성요소 또한 변경되며 패밀리에 속한 컴포넌트 또한 변경된다. ST는 PP에서 파생적으로 생성된 것이므로 PP의 클래스 및 컴포넌트가 변화함에 따라 유사하게 변화하며 CC



[그림 7] CC v2.2의 보안목표명세서(ST) 구성요소



〔그림 8〕 CC v2.4의 보안목표명세서(ST) 구성요소

v2.4는 CC v2.2에 비하여 통합 및 간소화된 특징을 가진다. 예를 들어 CC v2.2에서 부가적으로 포함시켰던 "이론적 근거" 구성요소를 다른 패밀리와 통합시켰으며 ASE_CCL(준거 요구) 패밀리가 추가됨에 따라 CC v2.2에서의 ASE_PPC(보호프로파일 수용) 패밀리가 준거 요구사항으로 간소화되었다. 〔그림 7〕과 〔그림 8〕은 CC v2.2의 ST 평가 구성요소와 CC v2.4의 ST 평가 구성요소를 나타낸다. 낮은 보증 보안목표명세서(ST)에 대해서는 보안목표명세서 소개, 준거 요구, 확장된 컴포넌트 정의, 보안요구사항, TOE 요약 명세로 구성되며 보안 문제 정의와 보안 목적은 생략한다.

1.2 Part 2 : 보안기능요구사항의 변경 사항〔5〕

CC v2.2와 CC v2.4로 변경 시 Part 2는 변경되지 않는다. CC v2.4에서의 Part 2는 CC v2.2를 그대로 사용한다.

1.3 Part 3 : 보증요구사항의 변경 사항〔6,10〕

(1) 보증클래스 변경

현재 CC v2.2에서는 형상관리(ACM), 배포 및 운영(ADO), 개발(ADV), 설명서(AGD), 시험(ATE), 취약성평가(AVA)의 총 6개의 보증 클래스로 구성되어 있으나 CC v2.4에서는 독립적인 클래스로 구성되어 있던 보안목표평가(ASE) 보증클래스가 평가보증등급과의 상관관계에 추가된다. 〔그림 9〕와 〔그림 10〕은 CC v2.2와 CC v2.4의 보증클래스 변경사항과 보안목표평가(ASE) 클래스의 평가보증등급과의 관계를 나타낸다. 보안목표평가(ASE) 클래스가 포함되면서 TOE보안기능강도(AVA_SOF) 패밀리가 삭제되었으며 취약성분석(AVA_VLA) 패밀리의 종속성이 삭제된다.

Version v2.2			Version v2.4		
보증클래스	보증패밀리	약칭	클래스	보증패밀리	약칭
형상관리 (ACM)	형상관리자동화	ACM_AUT			
	형상관리능력	ACM_CAP			
	형상관리범위	ACM_SCP			
배포및운영 (ADO)	배포	ADO_DEL			
	설치,생성,시동	ADO_IGS			
개발 (ADV)	기능명세	ADV_FSP			
	상위설계	ADV_HLD			
	구현의표현	ADV_IMP			
	TSF내부	ADV_INT			
	하위설계	ADV_LLD			
	표현의 일치성	ADV_RCR			
	보안모델정책	ADV_SPM			
설명서 (AGD)	관리자설명서	AGD_ADM			
	사용자설명서	AGD_USR			
생명주기 지원 (ALC)	개발보안	ALC_DVS			
	결함교정	ALC_FLR			
	생명주기정의	ALC_LCL			
	도구와 기법	ALC_TAT			
시험 (ATE)	범위	ATE_COV			
	상세수준	ATE_DPT			
	기능시험	ATE_FUN			
	독립적인시험	ATE_IND			
취약성평가 (AVA)	비밀채널분석	AVA_CCA			
	오용	AVA_MSU			
	TOE보안기능강도	AVA_SOF			
	취약성 분석	AVA_VLA			
			보안목표평가 (ASE)	준거요구	ASE_CCL
				확장컴포넌트정의	ASE_ECD
				ST소개	ASE_INT
				보안목적	ASE_OBJ
				보안요구사항	ASE_REQ
				보안문제정의	ASE_SPD
				TOE요약명세	ASE_TSS
			TOE보안기능강도(AVA_SOF)삭제		
			취약성분석(AVA_VLA) 종속성 삭제		

〔그림 9〕 CC v2.2와 CC v2.4 보증클래스 변경사항

클래스	보증패밀리	약칭	평가보증등급과의관계						
			1	2	3	4	5	6	7
보안목표평가 (ASE)	준거요구	ASE_CCL	1	1	1	1	1	1	1
	확장컴포넌트정의	ASE_ECD	1	1	1	1	1	1	1
	ST소개	ASE_INT	1	1	1	1	1	1	1
	보안목적	ASE_OBJ		1	1	1	1	1	1
	보안요구사항	ASE_REQ	1	2	2	2	2	2	2
	보안문제정의	ASE_SPD		1	1	1	1	1	1
	TOE요약명세	ASE_TSS	1	1	1	1	1	1	1

〔그림 10〕 보안목표평가(ASE) 클래스 평가보증등급과의 관계

〔표 4〕 일관성 관련 변경 예 (ATE DPT.1.1C)

변경전	ATE_DPT.1.1C	시험의 상세수준 분석은 시험 문서에 식별된 시험항목이 기본설계에 따라 TSF가 동작함을 입증하기에 충분하다는 것을 입증해야 한다.
변경후	ATE_DPT.1.1C	시험의 상세수준 분석은 시험 문서내의 시험과 기본설계내의 인터페이스 사이의 일관성을 입증해야 한다.

(2) "일관성" 관련 변경

추상적인 "일관성" 요구사항을 삭제 및 축소하였다. "일관성" 요구사항 추가 및 변경에 대한 사항은 다음과 같으며 〔표 4〕는 일관성 관련 변경 예를 나타낸다.

① 삭제

- ADV_FSP(기능명세) : ADV_FSP.1.2C, ADV_FSP.2.2C, ADV_FSP.3.2C, ADV_FSP.4.2C ("기능명세는 내부적으로 일관성이 있어야 한다.")
- ADV_HLD(상위설계) : ADV_HLD.1.2C, ADV_HLD.2.2C, ADV_HLD.3.2C, ADV_HLD.4.2C, ADV_HLD.5.2C("기본설계는 내부적으로 일관성이 있어야 한다.")
- ADV_IMP(구현의 표현) : ADV_IMP.1.2C, ADV_IMP.2.2C, ADV_IMP.3.2C ("구현의 표현은 내부적으로 일관성이 있어야 한다.")
- ADV_LLD(하위설계) : ADV_LLD.1.2C, ADV_LLD.2.2C, ADV_LLD.3.2C("상세설계는 내부적으로 일관성이 있어야 한다.")
- AGD_ADM(관리자설명서) : AGD_ADM.1.7C
- AGD_USR(사용자설명서) : AGD_USR.1.5C
- AVA_MSU(오용) : AVA_MSU.1.2C ("설명서는 완전하고, 명확하고, 타당해야 한다.")

② 추가 및 변경

- ADV_FSP(기능명세) : ADV_FSP.1.3E, ADV_FSP.2.3E, ADV_FSP.3.3E, ADV_FSP.4.3E 추가 ("평가자는 기능명세가 TOE 요약 명세와 일관성이 있는지 결정해야 한다.")
- ATE_DPT(상세수준 시험) : ATE_DPT.1.1C (ATE_DPT.2.1C, ATE_DPT.3.1C도 변경 및 추가), ATE_DPT.1.2C ("시험의 상세수준 분석은 상세설계내의 인터페이스와 시험 문서의 시험이 완전하게 일관성이 있는지를 입증해야 한다."), ATE_DPT.2.2C, ATE_DPT.2.3C, ATE_DPT.3.2C, ATE_DPT.3.3C, ATE_DPT.3.4C 추가
- ATE_FUN(기능시험) : ATE_FUN.1.5C, ATE_FUN.2.5C 변경

(3) "보안기능" 관련 변경

"보안기능(security functions)"이란 용어가 "TSF에 대한 외부 인터페이스(external interfaces to the TSF)"로 변경되었다. 이는 PP 및 ST의 변경으로 인해 "보안기능"이란 용어 및 평가 관련 지침이 변경되는 결과를 낳았으며 〔표 5〕는 보안기능 관련 변경 예를 보인다.

〔표 5〕 보안기능 관련 변경 예 (ADV SPM.1.4C)

변경전	ADV_SPM.1.4C	TSP 모델과 기능명세간의 일치성을 보일 경우에는 기능명세에 명시된 모든 보안기능이 TSP 모델에 대하여 일관성 있고 완전한지 입증해야 한다.
변경후	ADV_SPM.1.4C	TSP 모델과 기능명세간의 일치성을 보일 경우에는 기능명세에 명시된 모든 TSF에 대한 외부 인터페이스가 TSP 모델에 대하여 일관성 있고 완전한지 입증해야 한다.

- ADV_SPM(보안모델정책) : ADV_SPM.1.4C 변경 (ADV_SPM.2.4C, ADV_SPM.3.4C도 동일)

이외에도 보안기능과 관련하여 AGD_ADM.1.5C, AGD_USR.1.1C, AGD_USR.1.2C, AGD_USR.1.3C는 삭제되었으며 변경된 사항은 AGD_USR.1.6C, ATE_FUN.1.2C와 ATE_FUN.1.3C가 존재한다.

(4) "확률 또는 순열 메커니즘이 파괴될 가능성" 문맥 삭제

- AVA_SOF(TOE 보안기능강도) 패밀리 삭제
- AVA_MSU(오용) : AVA_MSU.1.3C 변경, AVA_MSU.1.4C 삭제 ("설명서는 (외부의 절차적, 물리적, 인적 통제를 포함한) 외부 보안대책에 관한 모든 요구사항을 나열해야 한다. ")

(5) "잠재적"이란 용어 추가(침투 공격 추가)

AVA_VLA(취약성) 패밀리의 종속관계가 모두 삭제되었으며 다음은 AVA_VLA(취약성) 패밀리의 변경사항을 보이며 〔표 6〕은 "잠재적(potential)" 용어 추가 관련 변경 예를 나타낸다.

① 삭제

- AVA_VLA(취약성) : AVA_VLA.3.4C, AVA_

〔표 6〕 "잠재적(potential)" 용어 추가 관련 변경 예 (AVA VLA.1.2E)

변경전	AVA_VLA.1.2E	평가자는 명백한 취약성이 다루어졌음을 보장하기 위하여 개발자의 취약성 분석에 근거한 침투시험을 수행해야 한다.
변경후	AVA_VLA.1.2E	평가자는 운용 환경상의 TOE가 공격자에 의한 기본적인 잠재적 공격인 침투 공격에 저항함을 결정하기 위해, 개발자 취약성 분석을 검사하고, 직면한 잠재적 취약성을 고려하여 침투시험을 수행해야 한다.

VLA.3.5C, AVA_VLA.2.2E (AVA_VLA.3.2E, AVA_VLA.4.2E도 동일), AVA_VLA.2.3E~AVA_ VLA.2.5E (AVA_VLA.3.3E~AVA_VLA.3.5E, AVA_VLA.4.3E~AVA_VLA.4.5E)

② 변경 및 추가

- AVA_VLA(취약성) : AVA_VLA.1.1C, AVA_VLA. 1.2C, AVA_VLA1.3C, AVA_VLA.2.2C (AVA_ VLA.3.2C, AVA_VLA.4.2C도 동일), AVA_VLA .2.3C (AVA_VLA.3.3C, AVA_VLA.4.3C도 동일), AVA_ VLA1.1E 변경

(6) 기타

- "보증 컴포넌트(Assurance components)"가 "보안 보증 요구사항(SARs)"로, "TOE 보안정책(TSP)"이 "TOE 보안 기능 요구사항(SFRs)"로 변경되었다.
  ※ SARs(Security Assurance Requirement)
  ※ SFRs(TOE security functional requirements)
- ATE_COV(시험범위) : "식별된(identified)"이란 용어 삭제, "기술된 TOE 보안기능(TSF as described)"이 "인터페이스(interfaces)"로 변경되었으며 "~의 부분집합(a subset of the)", "적당한(as appropriate)"과 같은 추상적이며 주관적인 용어는 삭제하고 명확하면서도 간략한 언어로 용어로 통일화한 특징을 보여준다.
- AGD_ADM.1.4C 삭제
- ATE_DPT(상세수준 시험) : ALC_FLR(결함 교정) 패밀리가 독립적으로 존재하므로 목적에서 "결함이 존재하는지 입증하기 위하여"란 문맥을 삭제하였다.
- ATE_FUN.1.1C에서 "시험 절차 설명"을 삭제하였다.
- 순서 변경 : ATE_IND.2.2E와 ATE_IND. 2.3E, ATE_IND.3.2E와 ATE_IND.3.3E의 순서가 변경되었다.

2. CEM v2.2와 CEM v2.4의 비교 및 분석

CEM v2.4는 CEM v2.2까지 Part 1과 Part 2, 독립적인 "결함 교정" 부록으로 분류되어 있는 문서를 하나로 통합하여 작성되었다. CC가 v2.4로 변경되면서 ST 평가 패밀리가 평가보증등급에 관여함에 따라 CEM에서도 역시 ST 평가의 부활동이 평가보증등급에 관계하여 포함된다. 또한, CEM v2.2에서는 PP와 ST, EAL1~4의 부활동이 명시되어 있으나 CEM v2.4에서는 PP와 EAL1, EAL4 부분의 부활동만이 존재하며 EAL2와 EAL3등급에 관한 사항은 특별한 평가활동으로 분류해놓고 있다[12,16].

CEM v2.4에 추가된 사항은 다음과 같으며 현재 평가에 적용 시 참고 가능한 요구사항이 된다. CEM v2.4에서 "평가프로젝트 생성 시 평가자(평가책임자 포함)를 3명으로 구성한다."라고 직접적으로 제시하므로 평가를 할 때 가장 적정 평가인원으로 3명으로 구성할 수 있다. 또한 평가기술보고서(ETR)과 관련하여 평가기술보고서에는 입력작업과 출력작업에 관련된 식별자 및 관련된 사항을 보고서 자체나 평가프로젝트 정보에 포함하도록 명시하고 있다. 그리고 평가참여자의 역할 중 "감독자(Overseer)"가 "평가 권위자(evaluation authority)"로 명칭이 바뀌며 증명/검증보고서를 발행하는 업무가 부가된다.

3. 변화의 특징

현재 평가는 해석된 CC v2.1과 v2.2(2003년 12월 31일)를 적용할 수 있으며 CC v2.4와 CEM v2.4는 아직 드래프트 문서이므로 개발 중에 있으며 비공식적이다. CC v2.2에서 CC v2.4로의 변화는 이전의 변화보다 괄목할 만한 변화를 보인다. 특징으로는 ST가 평가보증등급(EAL)과 관계되었으며 PP 및 ST의 보증패밀리 목록이 변경되었다. 또한 ST가 평가보증등급(EAL)에 관계되면서 AVA_SOF(보안기능강도)가 삭제되는 등 큰 변화를 보이고 있다. 이렇듯 보안기능에 중점을 둔 CC v2.2에 비해 CC v2.4는 TOE의 요구사항에 관련한 기능에 초점을 맞추고 있다.

CEM의 경우 Part 1과 Part 2가 통합되는 특징

을 보였으며 추상적이고 주관적인 내용의 간소화 및 명확화, 그리고 실례를 적용한 평가방법을 제시함으로써 개발자 및 평가자가 평가에 대해 좀더 쉽게 이해할 수 있도록 상세화된 특징을 보인다.

4. 평가 적용방안

본 논문에서 제시한 변경 내용을 파악하여 이를 기반으로 향후 평가를 자동화할 수 있는 평가수행 및 관리 시스템에 반영할 수 있다. 아직까지는 CC v2.4와 CEM v2.4는 비공식 버전이지만 그 변경 내용을 살펴봄으로써 실제 평가를 적용하는데 있어 향후 평가방법에 대한 변화에 빠르게 대처하여 좀더 손쉽고 정확한 평가를 수행할 수 있는 이점이 존재한다. 현재 평가를 하기 위해 자동화된 평가관리도구를 개발할 때 평가 적용기준인 CC v2.2와 연계하여 CC v2.4의 요구사항을 최소한 반영하여 변화에 대응하여야 하며 실제적으로 완전히 삭제된 AVA_SOF 패밀리나 ST의 평가보증등급 내의 포함, AVA_VLA의 종속성 삭제 등 v2.4는 많은 부분은 변화했으므로 그 변화에 유연하게 대처해야 할 것이다. AVA_VLA의 경우 종속성 자체가 사라졌으므로 독립적으로 수행해도 되며 이는 평가를 스케줄링 할 때 큰 변수로 작용된다.

Ⅳ. 결 론

본 논문은 국제공통평가기준인 CC에 대한 간략한 개념소개와 공통평가기준(CC)과 공통평가방법론(CEM)에 명시된 평가 요구사항에 관하여 논하였으며 현재 평가에 직접 적용하는 버전과 향후 변경될 버전에 대하여 비교함으로써 변경 내용을 살펴보았다. CC기반 평가는 국제적으로 정보보호제품 및 시스템의 평가에 관한 일원화, 효율성, 그리고 관리의 표준화를 위한 방향 제시를 하고 있다. 국내뿐만 아니라 국제적으로 정보보호시스템의 사용도는 증가하고 있으며 이러한 정보보호시스템의 신뢰성 확보와 상호인증을 위해 CC는 필요 불가결한 존재가 되고 있다.

CC 변경 내용에 대처하기 위해 평가를 순차적이고 정확하게 진행할 수 있도록 버전의 변화에 대한 체계적인 분석 및 적용이 필요하다. 현재 CC v2.4와 CEM v2.4는 비공식 문서이므로 앞으로도 CC와 CEM은 국제동향에 맞추어 계속된 변화가 예상되며 이에 따른 평가참여자(평가신청자, 개발자, 평가자, 감독자 등)의 역할도 변화의 흐름에 대응해야 할 필요가 존재한다.

참 고 문 헌

[1] 한국정보보호진흥원, "정보보호시스템 평가·인증 가이드," KISA, pp.52-68, 2002. 12.

[2] European Community, "Information Technology Security Evaluation Criteria (ITSEM)," Ver.1.0, http://www.cesg.gov.uk/assurance/ iacs/itsec/index.htm 1993.

[3] DoD, "Department of Defense Trusted Computer System Evaluation Criteria (TCSEC)," Dec. 1985.

[4] Part 1 : Introduction and General Model, Common Criteria for Information Technology Security Evaluation(CC), CCIMB-2004-01-001, Version 2.2 : ISO/IEC 15408, Jan. 2004.

[5] Part 2 : Security Function Requirements, Common Criteria for Information Technology Security Evaluation(CC), CCIMB-2004-01-002, Version 2.2 : ISO/IEC 15408, Jan. 2004.

[6] Part 3 : Security Assurance Requirements, Common Criteria for Information Technology Security Evaluation(CC), CCIMB-2004-01-003, Version 2.2 : ISO/IEC 15408, Jan. 2004.

[7] Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), US Dod 5200.28-STD, Dec. 1985.

[8] 김광식, 남택용., "정보보호시스템 공통평가기준 기술동향," http://kidbs.itfind.or.kr, pp.2-15, Oct. 2002.

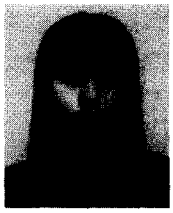
[9] Part 1 : Introduction and General Model, Common Criteria for Information Technology Security Evaluation(CC), CCIMB-2004-03-001, Version 2.4 : ASE/APE Trial Use version, Mar. 2004.

[10] Part 3 : Security Assurance Requirements, Common Criteria for Information Technology Security Evaluation(CC), CCIMB-2004-03-003, Version 2.4 : ASE/APE Trial Use version, Mar. 2004.

[11] Part 1 : Introduction and general model,

Common Evaluation Methodology for Information Technology Security(CEM), CEM-97/017, Version 0.6, Jan. 1997.
[12] Part 2 : Evaluation Methodology, Common Evaluation Methodology for Information Technology Security(CEM), CCIMB-2004-01-04, Version 2.2, Jan. 2004.
[13] 이유신, 이경구., "국제공통평가기준(CC)기반의 상호인정협정(MRA) 동향 분석," 통신정보보호학회지, 제 10권 3호, pp.49-61, 2000. 9.
[14] Part 1, 2, 3, 4 : Common Criteria for Information Technology Security Evaluation(CC), CCEB-96/011~014, Version 1.0, Jan. 1996.
[15] Part 1, 2, 3, 4 : Common Criteria for Information Technology Security Evaluation(CC), CCEB-98, Version 2.0, May. 1998.
[16] Evaluation Methodology, Common Evaluation Methodology for Information Technology Security(CEM), CCIMB-2004-03-04, Version 2.4 : ASE/APE Trial Use version, Mar. 2004.
[17] Reuse of Evaluation Results and Evidence, 2002-08-009-002, CCRA, Version 1 Final, pp.1-2, Oct. 2002.
[18] Ruben Prieto-Diaz, "The Common Criteria Evaluation Process," CISC, pp.24-33, Dec. 2002.

〈著 者 紹 介〉



강 연 희 (YeonHee Kang)
학생회원

2003년 : 한남대학교 컴퓨터멀티미디어공학과 졸업(학사)
2003년~현재 : 한남대학교 컴퓨터공학과 석사 과정
〈관심분야〉 소프트웨어공학, 정보보호시스템 평가, 보안공학

김 정 대 (JungDae Kim)
학생회원

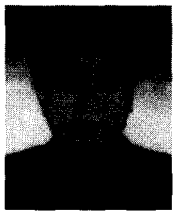
2003년 : 한남대학교 컴퓨터공학과 졸업(학사)
2004년~현재 : 한남대학교 컴퓨터공학과 석사과정
〈관심분야〉 소프트웨어 품질 평가 및 보증, 소프트웨어 표준화, 보안공학

방 영 환 (YoungWhan Bang)
학생회원

1997년 : 한남대학교 컴퓨터공학과 졸업(학사)
2002년 : 대전대학교 대학원 컴퓨터공학과 졸업(석사)
2002년~현재 : 대전보건대학 컴퓨터정보처리과 프로그래밍 전문강사
2002년~현재 : 한남대학교 대학원 컴퓨터공학과 박사과정
〈관심분야〉 소프트웨어 품질 평가 및 보증, 소프트웨어 표준화, 보안공학

최 성 자 (SungJa Choi)
학생회원

1991년 : 한남대학교 컴퓨터공학과 졸업(학사)
1997년 : 한남대학교 컴퓨터공학과 졸업(석사)
2002년~현재 : 한남대학교 컴퓨터공학과 박사과정
〈관심분야〉 소프트웨어공학, 자바, 워크플로우 모델링, 보안평가 EDI 보안, 패트리넷 등



이 강 수 (GangSoo Lee)
종신회원

1981년 : 홍익대학교 전자계산학과 학사
1983년 : 서울대학교 대학원 전산학과 석사
1989년 : 서울대학교 대학원 전산학과 박사
1985년~1987년 : 국립한밭대학교 전자계산학과 전임강사
1992년~1993년 : 미국일리노이대학교 객원교수
1995년 : 한국전자통신연구원 초빙연구원
1998년~1999년 : 한남대학교 멀티미디어학부장
1987년~현재 : 한남대학교 컴퓨터공학과 정교수
〈관심분야〉 소프트웨어공학, 병행시스템 모델링 및 분석, 보안공학, 정보보호시스템 평가, 멀티미디어교육 커리큘럼