# 공통평가기준 기반의 보안성 평가를 위한 기존 보증방법론 조사 및 연구

이종숙* 이지은* 최병주*
이화여자대학교 컴퓨터학과*
{jslee01, jieun2, bjchoi}@ mm.ewha.ac.kr

# A Survey of the existing assurance methodology for Common Criteria based IT Security Evaluation

*Jongsook Lee** *Jieun Lee** *Byoungju Choi**
Dept. of Computer Science & Engineering, Ewha Womans University

## 요 약

기존에 수행되어 왔던 방법론들을 새롭게 바꾸는 것은 쉬운 일이 아니다. 기존의 보증방법론을 활용하여 CC기반의 정보보호시스템의 보안성 평가를 하는 것이 필요하다. 본 연구에서는 CC기반의 정보보호시스템의 보안성 평가를 위한 기존 보증 방법론의 접근 방안을 연구하기 위한 첫 단계로, 기존 보증 방법론을 조사 및 분석하여 활용하기에 적합한 방법론들의 목록을 도출한다. 본 연구에서 도출한 CC와 상호호환이 가능한 기존 보증 방법론을 이용하여 CC기반의 보안성 평가를 위한 기존 보증 방법론의 접근 방안의 연구는 평가를 효율적으로 수행할 수 있을 것이다.

## 1. 서론

1999년 ISO/IEC의 표준(ISO/IEC 15408)으로 보안성 평가 기준인 공통평가기준(Common Criteria,이하 CC라 칭한다)이 제정되었다. 최근 CC 기반의 평가·인증 결과에 대한 상호인정협정(Common Criteria Recognition Arrangement, CCRA)에 여러 나라들이 대거 가입함에 따라 CC의 영향력은 날로 커지고 있다. CC기반의 정보보호시스템의 보안성 평가는 기능이 제대로 구현이 되었는지에 대한 보증에 대한 평가이다.

기존에 수행되어 왔던 방법론들을 하루아침에 새롭게 바꾸는 것은 쉬운 일이 아니다. 기존의 보증방법론을 활용하여 CC기반의 정보보호시스템의 보안성 평가를 함으로써,이러한 문제점을 해결할 수 있다.

현존하는 정보기술 보안 평가절차를 개선하고, 보증성을 평가하는 더 좋은 메커니즘을 제공하기 위한 목적으로 AAWG (Alternative Assurance Working Group)이 결성되어, 수행된 결과를 토대로 하여 정보보호시스템 보증 프레임워크 파트에 의해서 "A framework for IT security assurance (ISO/IEC WD 15443)" 문서가 작성되어졌다. 그러나, 아직 Draft단계의 문서로 서술이 빠진 내용이 있는 등 불안전하며, 현존하는 보증 방법론들을 요약해놓은 문서에 지나지 않아 참고하기에는 무리가 있다.

본 연구에서는 CC기반의 정보보호시스템의 보안성 평가를 위한 기존 보증 방법론의 접근 방안을 연구하기 위한 첫 단계로, 기존 보증 방법론을 조사 및 분석하여 활용하기에 적합한 방법론들의 목록을 도출한다.

본 논문은 2장에서 공통평가기준에 대해, 3장에서는 보증방법론의 일반적인 소개에 대해 4장에서는 기존 보증 방법론의 분석 관점 및 결과를 5장에서는 결론 및 향후 연구 과제를 제시한다.

## 2. 공통평가기준

공통평가기준[1]은 독일, 미국, 영국, 캐나다, 프랑스 5개국이 다른 평가기준을 활용하는 국가에 판매하기 위해서는 그 국가가 사용하는 평가기준을 활용하여 재평가 받아야 한다는 문제점을 해결하기 위해 모든 정보보호시스템 유형을 포괄할 수 있는 보안 요구사항을 제시한 보안성 평가 기준으로 3개의 파트로 구성되어 있다. 첫 번째 파트에서는 제품/시스템의 보안 요구사항을 표현하기 위한 일반적인 모델에 대해, 두 번째 파트에서는 보안 기능 요구사항의 목록, 세 번째 파트에서는 보안 보증 요구사항의 목록을 <Class - Family - Component - Element>의 계층 구조로 제공하고 있다. 각 목록 중 Class의 목록은 다음 [표 1], [표 2]과 같다.

| Class | 이름 |
|---|---|
| FAU | Audit |
| FCO | Communication |
| FCS | Cryptographic Support |
| FDP | User Data Protection |
| FIA | Identification & Authentication |
| FMT | Security Management |
| FPR | Privacy |
| FPT | Protection of TOE Security Functions |
| FRU | Resource Utilization |

| | |
|---|---|
| FTA | TOE Access |
| FTP | Trusted Path / Channels |

[표 1] 보안 기능 요구사항 목록

| Class | 이름 |
|---|---|
| ACM | Configuration Management |
| ADO | Delivery & Operation |
| ADV | Development |
| AGD | Guidance Documents |
| ALC | Life Cycle Support |
| ATE | Tests |
| AVA | Vulnerability Assessment |
| APE | Protection Profile Evaluation |
| ASE | Security Target Evaluation |
| AMA | Maintenance of Assurance |

[표 2] 보안 보증 요구사항의 목록

CC기반의 정보보호시스템의 보안성 평가는 기능이 제대로 구현이 되었는지에 대한 보증에 대한 평가이며, CC는 EAL(Evaluation Assurance Level)이란 7단계의 평가 수준을 제시한다.

CC는 보호프로파일(Protection Profile) 혹은 보안목표명세서(Security Target)라는 별도의 산출물을 통해 개별 정보보호시스템의 평가에 적용된다.

또한 CC를 위한 평가 방법론에 대한 문서로 CEM (Common Evaluation Methodology)이 있다.

## 3. 보증 방법론

보증은 보안통제가 정확하게 운영되고 의도한 대로 시스템을 보호한다는 것에 대한 신뢰의 정도이다.[2] 일반적으로 보증은 평가를 통해 이루어지며, 평가의 대상에 따라 크게 산출물을 평가하는 방법, 산출물을 개발하거나 생산하기 위해 쓰이는 프로세스를 평가하는 방법, 사람이나 시설 등 환경을 평가하는 방법으로 나눌 수 있다. 현재 다양한 보증 방법론이 존재하며 [표 3]의 보증 방법론 들을 조사 및 분석하였다.

| 보증 평가 대상 | 보증 방법론 | |
|---|---|---|
| 산출물 | SCT | Strict Conformance Testing |
| | TTAP<br>TPEP<br>TCSEC | Trust Technology Assessment Program<br>Trusted Product Evaluation Program<br>Trusted Computer System Evaluation Criteria |
| | RAMP | Rating Maintenance Phase |
| | CC (ISO/IEC 15408) | Evaluation criteria for IT security |
| | ITSEC/ITSEM | Information Technology Security Evaluation Criteria and Methodology |
| | CTCPEC | Canadian Trusted Product Evaluation Criteria |
| | Penetration Testing | |
| | X/Open Branding | |
| | ISO/IEC 14598 | Software product evaluation |
| | IT Baseline Protection Manual | |
| 프로세스 | CMM | Capability Maturity Model® (for Software) |
| | SE-CMM ® | Systems Engineering Capability Maturity Model ® |
| | SA-CMM® | Software Acquisition Capability Maturity Model® |
| | CMMI | Capability Maturity Model ® Integration |
| | SSE-CMM | Systems Security Engineering Capability Maturity Model |
| | TSDM | Trusted Software Development Methodology |
| | TCMM | Trusted Capability Maturity Model |
| | ISO/IEC 13335 | Guidelines for the management of IT Security (GMITS) |
| | V-Model | |
| | ISO/IEC 17799 | Code of practice for information security management |
| | ISO/IEC 15504 | Software Process Assessment |
| | ISO/IEC 15288 | System Life Cycle Processes |
| | ISO/IEC 12207 | Software Life Cycle Processes |
| 환경 | ISO 9000 Series | Quality Management |
| | ISO/IEC 17025 | Accreditation Assurance |
| | ISO 13407 | Human Centered Design (HCD) |
| | CISSP | Certified Information Systems Security Professionals |

[표 3] 보증 방법론의 목록

## 4. 기존 보증 방법론의 분석 및 결과

### 4.1 분석 관점

각 보증 방법론마다 사용하는 용어나 접근 방법, 지향 방향 등이 다르므로, 다음의 특징을 중심으로 분석하였다.

(A) 적용 대상(모든 제품, 소프트웨어, ...)이 무엇인지?
(B) 평가의 목표가 무엇인지?
(C) 평가를 받기 위해 필요한 것은 무엇인지?
(D) 어떻게 평가가 수행되는지?
(E) 생명주기의 어느 단계를 고려하는지?
(개발, 통합, 배치, 작동)

주요 방법론의 특징은 [표 4], [표 5]의 내용과 같으며, [표 4]는 보증 평가 대상이 산출물인 보증 방법론의 특징이며, [표 5]는 보증 평가 대상이 프로세스인 보증 방법론의 특징이다. 보증 평가 대상이 환경인 경우에는 CC의 보증방법론과는 상이하므로 생략한다.

| | CC (ISO/IEC 15408) | TTAP / TPEP TCSEC | RAMP | ISO/IEC 14598 |
|---|---|---|---|---|
| (A) | 보안 제품 | 보안 제품 | 이미 평가된 보안 제품 | 모든 소프트웨어 |
| (B) | 기준 적합 검증 | 기준 적합 검증 | 수정된 제품의 재평가 | 품질 측정 및 평가 |
| (C) | 제품(산출물) | 제품(산출물) | 제품(산출물) | 제품(산출물) |
| (D) | 보증 증거물 분석 및 리뷰 | 보증 증거물 분석 및 리뷰 | 보증 증거물 분석 및 리뷰 | |
| (E) | 개발, 통합, 배치, 작동 | 개발, 통합 | 개발, 통합 | 개발 |
| | ITSEC/ITSEM | CTCPEC | Penetration Testing | |
| (A) | 보안 제품 | 보안 제품 | 보안 제품 | |
| (B) | 기준 적합 검증 | 기준 적합 검증 | 침투 가능성 평가 | |
| (C) | 제품(산출물) | 제품(산출물) | 제품(산출물) | |
| (D) | 보증 증거물 분석 및 리뷰 | 보증 증거물 분석 및 리뷰 | 침투 시행 | |
| (E) | 개발, 통합 | 개발, 통합 | 작동 | |

[표 4] 산출물 평가 보증 방법론의 특징

TCSEC, ITSEC, CTCPEC 등은 CC가 등장하기 이전에 각 나라별로 수행되었던 보안성 평가 기준들이다. CC의 EAL등급처럼 각 기준마다 평가수준을 나타내는 등급이 존재한다. 보안성 평가 기준들은 대부분 제품(산출물)을 대상으로 평가가 수행하였다는 것을 알 수 있다.

ISO/IEC 14598은 소프트웨어 제품의 품질을 측정하거나 평가하는 데 필요한 방법과 절차를 정의하고 있는 표준으로 평가 요구사항 도출, 평가명세서 작성, 평가계획 수립, 평가 수행 및 결과 도출 등의 단계를 제시한다.

| | CMM | SE-CMM ® | SA-CMM® | CMMI* |
|---|---|---|---|---|
| (A) | 모든 소프트웨어 | 시스템 | 모든 소프트웨어 | 모든 소프트웨어 |
| (B) | 성숙도 측정 및 향상 방향 제시 | 성숙도 측정 및 향상 방향 제시 | 성숙도 측정 및 향상 방향 제시 (획득) | 성숙도 측정 및 향상 방향 제시 (통합 관점) |
| (C) | 프로세스 존재 | 프로세스 존재 | 프로세스 존재 | 프로세스 존재 |
| (D) | 성숙도 측정 | 성숙도 측정 | 성숙도 측정 | 성숙도 측정 |
| (E) | 개발, 통합 | 개발, 통합 | 배치 | 개발, 통합, 배치, 작동 |
| | SSE-CMM* | TSDM | TCMM | ISO/IEC 13335 |
| (A) | 시스템 | 임무 치명적인 소프트웨어 | 시스템 | 보안 제품 |
| (B) | 성숙도 측정 및 향상 방향 제시 | 개발 방법론 | 성숙도 측정 및 향상 방향 제시 | 보안 관리 |
| (C) | 프로세스 존재 | · | 프로세스 존재 | 프로세스 존재 |
| (D) | 성숙도 측정 | 개발 방법론 제시 | · | · |
| (E) | 개발, 통합, 배치, 작동 | 개발, 통합 | 개발, 통합, 배치, 작동 | 통합, 배치, 작동 |
| | V-Model* | ISO/IEC 15504* | ISO/IEC 15288* | ISO/IEC 12207* |
| (A) | 모든 제품 | 모든 소프트웨어 | 시스템 | 모든 소프트웨어 |
| (B) | 적합한 생명주기 프로세스 제시 | 수행 능력 측정 및 개선 방향 제시 | 적합한 생명주기 프로세스 제시 | 적합한 생명주기 프로세스 제시 |
| (C) | · | 프로세스 존재 | · | · |
| (D) | 개발 프로세스 제시 | 수행 능력 측정 | 적합한 생명주기 프로세스 제시 | 적합한 생명주기 프로세스 제시 |
| (E) | 개발, 통합, 배치, 작동 | 개발, 통합, 배치, 작동 | 개발, 통합, 배치, 작동 | 개발, 통합, 배치, 작동 |

[표 5] 프로세스 평가 보증 방법론의 특징

프로세스 평가 보증 방법론들은 크게 CMM 계열과 ISO/IEC 15504와 같이 직접 프로세스를 평가하는 방법론과 직접 프로세스를 평가하지는 않지만 적절한 프로세스들의 집합을 제시하는 보증 방법론으로 나누어진다.

CMM은 자율적인 소프트웨어 개발 프로세스의 핵심 요소들을 기술하는 프레임워크이며 이를 기반으로 SE-CMM, SA-CMM, CMMI, SSE-CMM, TCMM 등이 개발되었다. CMM 계열은 주로 프로세스를 평가하여 조직의 개발 공정의 성숙도를 판단하거나 소프트웨어 개발 공정을 향상시키기 위해서 사용될 수 있다. ISO/IEC 15504는 소프트웨어의 프로세스에 대한 계획, 관리, 감시, 통제, 개선을 위한 능력심사와 프로세스 개선을 목적으로 한다.

V-Model, ISO/IEC 15288, ISO/IEC 12207, TSDM 등은 품질을 보장하기 위한 각종 프로세스의 집합들을 제시하여 효율적이고 실질적인 프로세스를 구축하도록 한다.

### 4.2 분석 결과

[표 3]의 내용과 같이 CC의 보증 방법론은 보안 제품을 대상으로 기준에 적합한지를 검증하기 위하여 주로 개발의 산출물을 평가하여 보증을 얻는 방법론이다. 산출물만을 평가하는 평가는 개발자가 보안 평가에 대비하기에도 어려우며, 평가 후 적합하지 않다는 결과가 나왔다고 하더라도 산출물의 요구사항만을 보고 개발을 수정·개선하기에도 어려움이 많다.

보증방법론을 확장 시키거나 개선시키는 노력의 일환으로 각 보증방법론의 대응(mapping)시키는 작업이 많이 수행되었다. TCMM은 TSDM의 개발원칙과 CMM의 핵심 공정 영역을 비교하여 유사한 것끼리 서로 대응시키고, CMM의 핵심 공정 영역과 대응되지 않는 TSDM의 개발원칙의 경우에는 새로운 핵심 공정 영역을 정의하여 개발되었다. 이와 유사하게 AAWG는 SSE-CMM, TCMM, ISO 9000, X/OPEN 과 CC의 보증 요구사항을 일대일 대응시키는 작업이 진행중이다. CC의 보증 요구사항을 기존 보증방법론과 서로 대응을 시켜보고 그 결과를 이용하여 CC의 보증방법론의 미비한 점을 보안할 수 있다.

여러 보증 방법론을 비교·분석한 결과 CC와 모든 항목이 일치하는 방법론은 없었다. 그러나 보증을 위해 고려하는 생명주기단계나 평가의 대상이 일치한다면, CC와의 상호호환이 가능하다고 여겨지며, 해당하는 보증방법론을 [표-4]와 [표-5]의 항목에 *으로 표시하였다.

## 5. 결론 및 향후 연구 과제

본 연구에서는 CC기반의 정보보호시스템의 보안성 평가를 위한 기존 보증 방법론의 접근 방안을 연구하기 위한 첫 단계로, 기존 보증 방법론을 조사 및 분석하여 활용하기에 적합한 방법론들의 목록을 도출하였다.

향후에는 도출한 보증방법론을 중심으로 내용을 체계적으로 분석하여, CC와 상호호환이 가능한 세부항목을 도출하여 CC기반의 보안성 평가를 위한 기존 보증 방법론의 접근 방안을 연구할 예정이다.

## 참고문헌


[1] ISO/IEC 15408 Information technology -Security techniques - Evaluation criteria for IT security

[2] "An Introduction to Computer Security: The NIST Handbook", NIST

[3] ISO/IEC 1st PDTR 15443 Information technology - Security techniques - A framework for IT security assurance

[4] Jeffrey R. Williams, David R. Wichers, " The Need for A Framework for Reasoning About Assurance"

[5] ISO/IEC 15288 CD2 Life Cycle Management - System Life Cycle Processes

[6] ISO/IEC 12207 Information technology - Software life cycle processes

[7] Common Methodology for Information Technology Security Evaluation

[8] ISO/IEC TR 15504 Software Process Assessment

[9] Trusted Computer System Evaluation Criteria (TCSEC), 1985, DOD 5200.28-STD

[10] Information Technology Security Evaluation Criteria (ITSEC, version 1.2)

[11] V-Model - Development Standard for IT Systems, VM 1997, IABG, Einsteinstraße 20, D-85521

[12] System Security Engineering Capability Maturity Model, Model Description (SSE-CMM Model), Version 1.1.

[14] System Security Engineering Capability Maturity Model, Appraisal Methodology (SSE-CMM Method), Version 1.1.