제 19 회 한국정보처리학회 춘계학술발표대회 논문집 제 10 권 제 1 호 (2003. 5)

# 적용을 위한 보증 방법론 연구

이지은*, 최병주*
*이화여자대학교 컴퓨터학과
e-mail : {jieun2,bjchoi}@ ewha.ac.kr

# A Study on the Assurance Methods for Application

Ji-Eun Lee*, Byoung-Ju Choi*
*Dept. of Computer Science & Engineering, Ewha Womans University

요 약

IT 시스템을 보증할 필요가 커지면서 이미 많은 보증 방법론이 제안된 바 있다. 이러한 여러 가지 보증 방법론들은 그 목적, 범위, 대상, 접근방법에서 모두 다르다. 따라서 상황에 맞도록 적합한 보증 방법론을 선택하여 적절한 방법으로 적용하기 위해서는 방법론들에 대한 분석이 선행될 필요가 있다. 이를 위하여 본 논문에서는 다양한 보증 방법론들을 분류하고 관련 보증 방법론들을 서로 비교 분석하였다.

## 1. 서론

정보화 시대로 접어들면서 IT 시스템에 대한 의존도가 높아지고 있다. 따라서 IT 제품, 시스템, 서비스 등의 품질을 보증할 필요가 있다. 이러한 필요에 의해 좋은 프로세스를 통하여 좋은 품질의 IT 시스템을 생산, 운영하고, 이를 평가하기 위한 많은 보증 방법론들이 제안되었다.

과거 제안된 여러 보증 방법론들은 그 목적과 범위, 대상 접근 방법 측면에서 서로 상이하다. 그러므로 조직의 프로세스를 개선하거나 생산된 시스템의 품질을 향상시키고자 하는 경우 각기 다른 특성을 가진 다양한 방법론 중 어떤 것을 선택하고 어떤 방법으로 받아들여야 효과적일 것인지에 관한 연구가 필요하다.

이를 위하여 본 논문에서는 먼저 다양한 보증 방법론들을 검토하고, 연구 결과에 따라 분류하여 서로 비교 분석하고자 한다.

본 논문은 2 장에서 관련 연구로써 ISO/IEC WD 15443[1]에 대해, 3 장에서는 다양한 보증 방법론의 분류에 대해 기술하고, 4 장에서는 서로 관련 있는 보증 방법론들의 비교 분석을, 5 장에서는 결론 및 향후 연구 과제를 제시한다.

## 2. 관련연구

기존의 정보기술 보안 평가절차를 개선하고, 더 좋은 보증성 평가 매커니즘을 제공하기 위해 AAWG(Alternative Assurance Working Group)이 결성되어 3 개의 Task 가 수행되고 있다. 그 중 Task3 의 결과가 ISO/IEC JTC 1/SC27/ WG3 에 기고 되었으며, 정보보호 시스템 보증 프레임워크 파트에 의해서 ISO/IEC WD 15443(A framework for IT security assurance)가 작성되었다.

ISO/IEC WD 15443 는 보증 요소(assurance element)와 보증 방법론들을 소개하고, 공통평가 기준(Common Criteria, ISO./IEC 15408)[2]의 평가 등급인 EAL 과의 호환을 위해 공통평가기준과 다른 방법론을 대응시키고 있다.

그러나 이 문서는 아직 Draft 버전으로 보증 방법론들의 목적과 간략한 개요를 소개하는데 그치고 있고, 분석과 자세한 사항은 그 구조만 잡혀있으며 내용이 완성되지 않아 실질적인 적용에 참조하기에는 부족함이 있다.

## 3. 보증 방법론 분류

본 연구에서 20 개의 보증 방법론의 평가 체계와 보증 매커니즘 등을 검토하였으며 연구 내용을 비교 분석하여 여러 기준으로 방법론들을 분류하였다.

[표 1] 보증 방법론 분류

| 분류 기준 | | 보증 방법론 |
|---|---|---|
| 접근방법 | 내용 | |

| | | |
|---|---|---|
| 프로세스 방법론 | 소프트웨어 개발 프로세스 | ISO/IEC 12207[3] |
| | 시스템 개발 프로세스 | ISO/IEC 15288[4], V-Model[5] |
| | 관리 프로세스 | ISO/IEC 13335[6], ISO/IEC 17799[7] |
| 평가 방법론 | 프로세스 평가 | CMM[8], SE-CMM[9], SA-CMM[10], SSE-CMM[11], TCMM[12], CMMI[13], SPICE(ISO/IEC15504)[14] |
| | IT 제품/ 시스템 평가 | ISO/IEC 9126[15], ISO/IEC 14598[16] |
| | 보안 제품/ 시스템 평가 | CC, CEM[17], ITSEC[18], ITSEM[19], TCSEC[20], CTCPEC[21] |

[표 1]과 같이 보증 방법론은 크게 프로세스 방법론과 평가 방법론으로 분류된다. 프로세스 방법론은 시스템의 개발 단계 및 활동, 산출물 등의 개발 공정을 위한 체계적인 절차를 제시한다. 이러한 프로세스 방법론은 [표 2]와 같이 어떤 프로세스에 중점을 두었느냐에 따라 다시 분류할 수 있다.

[표 2] 프로세스를 정의한 방법론

| 보증 방법론 | 프로세스 | 국가 |
|---|---|---|
| ISO/IEC 12207 | 소프트웨어 생명주기 프로세스 | 국제 |
| ISO/IEC 15288 | 시스템 생명주기 프로세스 | 국제 |
| ISO/IEC 13335 | 보안관리 프로세스 | 국제 |
| ISO/IEC 17799 | 보안 관리 프로세스 | 국제 |
| V-model | 시스템 개발 프로세스 | 독일 |

평가 방법론은 평가 절차 및 평가 산출물을 제시하며, 평가 대상이 프로세스인 경우와 제품 및 시스템인 경우로 다시 나뉜다. 평가 대상이 프로세스인 방법론은 좋은 프로세스를 통하여 개발된 제품의 품질은 우수할 것이라는 가정에 근거하며 [표 3]와 같이 세분할 수 있다.

[표 3] 프로세스 평가기준을 제시한 보증 방법론

| 보증 방법론 | 평가 대상 | 국가 |
|---|---|---|
| CMM | IT System | 미국 |
| CMMI | IT System | 미국 |
| SE-CMM | IT System | 미국 |
| SA-CMM | IT System | 미국 |
| SSE-CMM | Security System | 미국 |
| TCMM | Security System | 미국 |
| SPICE | IT System | 국제 |

분석한 방법론 가운데 특히 보안에 초점을 맞춘 보증 방법론을 [표 4]와 같이 분류하였다.

[표 4] 보안 중심의 보증 방법론

| 보증 방법론 | 접근방법 | 국가 |
|---|---|---|
| SSE-CMM | 평가 방법론 | 프로세스 평가기준 | 미국 |
| TCMM | | 프로세스 평가기준 | 미국 |
| CC; ISO/IEC 15408 | | 제품 보안 평가기준 | 국제 |
| ITSEC | | 제품/시스템 보안평가기준 | 유럽 |
| TCSEC | | 제품/시스템 보안평가기준 | 미국 |
| CTCPEC | | 제품/시스템 보안평가기준 | 캐나다 |
| ISO/IEC 13335 | 프로세스 방법론 | 보안관리 프로세스 | 국제 |
| ISO/IEC 17799 | | 보안관리 프로세스 | 국제 |

## 4. 관련 보증 방법론의 비교 연구

3 장에서의 분류한 결과를 토대로 서로 연관성이 있는 보증 방법론들을 비교 분석하였다.

### 4.1 CMM 계열의 프로세스 평가 방법론의 비교

미국의 SEI(Software Engineering Institute)는 프로세스의 성숙도 평가를 위하여 1991 년 CMM 을 개발한 이래 시스템 공학 SE-CMM, 소프트웨어 획득 SA-CMM, 보안 시스템 공학 SSE-CMM 및 TCMM 등 다양한 성격의 공학 프로세스 평가를 위한 CMM 모델들을 개발하였다. 또한, 다양한 CMM 모델들을 통합하여 CMMI 를 개발하였다.

□ 구조

CMM 계통의 프로세스 평가방법론은 [표 5]와 같이 프로세스 측정 대상인 프로세스 영역과 수행능력단계의 분리 여부에 따라 두 가지로 나뉠 수 있다.

먼저 성숙도 단계를 정의하고, 각 단계별로 수행해야 할 프로세스 영역을 정의함으로써 프로세스 영역과 수행능력단계를 함께 정의한 평가방법론이 있으며, CMM, SA-CMM, TCMM, Staged CMMI 가 이에 속한다.

프로세스 영역과 수행능력단계를 분리한 경우는 조직의 비즈니스 목적과 환경에 따라 평가대상이 되는 프로세스 영역을 자유롭게 선정할 수 있도록 하는 방법론으로,. 선정한 평가 대상 프로세스 영역에 대하여 수행능력단계를 유연성 있게 결정할 수 있다. SE-CMM, SSE-CMM, Continuous CMMI 가 이에 속한다.

[표 5] CMM 계열의 프로세스 평가 방법론

| 보증 방법론 | 구조 | 평가 방법 | |
|---|---|---|---|
| | | 측정 대상 | 등급 |
| CMM<br>SACMM<br>TCMM | - PA 별 Base Practices<br>- 능력 단계별 Generic Pratice | Process Area | Capability Level |
| Continuous CMMI | - PA 별 Specific Goal, Specific Practice<br>- 능력 단계별 Generic Practice | | |

| | | |
|---|---|---|
| SE-CMM | - 성숙도 단계별 Key PAs | Maturity Level |
| SSE-CMM | - PA 별 Goal, Key Practice | |
| Staged CMMI | - 성숙도 단계별 Key PAs<br>- PA 별 Specific Goal, Specific Practices, Generic Goal, Generic Pratice | |

□ 평가 등급

CMM 계열 방법론은 조직의 프로세스 수행능력의 정도를 평가할 수 있는 등급을 제시한다. 프로세스 영역과 수행능력단계를 분리한 방법론은 [표 6]과 같이 수행능력 단계(capability level)로, 단계별 프로세스 영역을 정의한 방법론은 [표 7]과 같이 성숙도 단계(maturity level)로 평가 등급을 나눈다.

[표 6] 수행능력 단계

| Capability Level | CMM | SA-CMM | Staged-CMMI |
|---|---|---|---|
| 5 | Optimizing | Optimizing | Optimizing |
| 4 | Managed | Quantitative | Quantitatively managed |
| 3 | Defined | Defined | Defined |
| 2 | Repeatable | Repeatable | Managed |
| 1 | Initial | Initial | Initial |

[표 7] 성숙도 단계

| Maturity Level | SE-CMM | SSE-CMM | Continuous-CMMI |
|---|---|---|---|
| 5 | Continuously Improving | Continuously Improving | Optimizing |
| 4 | Quantitatively Controlled | Quantitatively Controlled | Quantitatively managed |
| 3 | Well Defined | Well Defined | Defined |
| 2 | Planed & Tracked | Planed & Tracked | Managed |
| 1 | Performed | Performed informally | Performed |
| 0 | Not Performed | | Not Performed |

### 4.2 Continuous CMMI 와 SPICE 의 비교

CMMI 는 소프트웨어의 개발, 획득, 유지보수, 서비스 관리 능력을 측정하고 개선할 수 있도록 CMM 계열의 프로세스 평가 방법론을 통합한 모델이다. Staged 와 Continuous 두 가지 모델을 가지며, 조직의 상황에 맞는 모델을 적용하도록 권장하고 있다.

SPICE 는 소프트웨어 개발, 획득, 공급, 운영, 확장 등과 관련한 소프트웨어 프로세스를 심사하고 개선할 수 있는 프레임웍을 제시한다.

□ 구조

[표 8]과 같이 Continuous CMMI 와 SPICE 는 둘 다 프로세스 영역을 측정 대상으로 하여 프로세스별로 그 수행 능력을 평가하는 방법론이다.

SPICE 가 그룹(고객-공급자, 지원, 엔지니어링, 관리, 조직)별로 프로세스 영역을 제시하고 프로세스 수행 능력수준별로 요구되는 프로세스 속성을 정의하여 그 속성별로 제시한 관리 프랙티스 등을 달성한 정도에 따라 각 프로세스 능력수준의 등급을 측정하는 반면,.Continuous CMMI 는 그룹(프로젝트 관리, 지원, 엔지니어링, 프로세스 관리)별로 프로세스 영역을 제시하고 그 측정을 위해 프로세스 영역별 특수 목적과 특수 프랙티스, 일반 목적과 일반 프랙티스를 정의해 그 달성 여부로 프로세스 수행능력의 등급을 매긴다.

SPICE 는 프로세스 개선과 프로세스 능력 결정을 목적으로 프로세스 심사를 수행하기 위한 참조 모델과 심사 모델을 제시하고, 심사 수행을 위한 요구사항과 실제 심사를 수행하는 안내 지침, 프로세스 개선과 능력 결정을 위한 평가방법론의 사용 지침을 제시한다. 이와 달리 Continuous CMMI 는 평가 모델의 정의와 함께 그룹화된 프로세스 영역간의 상호작용 프레임웍과 모델의 테일러링 방안을 제시하고 각 프로세스 영역의 관련 목적과 프랙티스들을 SPICE 보다 상세하게 정의하고 있다. 또한 Continuous CMMI 는 'Appraisal Requirements for CMMI (ARC)'과 'Standard CMMI Assessment Method for Process Improvement (SCAMPI)' 라는 각각의 독립된 표준에서 CMMI 평가 요구사항, 프로세스 개선을 위한 심사 메소드, 심사원에 대한 가이드 등을 제시한다.

[표 8] Continuous CMMI 와 SPICE 의 구조 비교

| | Continuous CMMI | | SPICE | |
|---|---|---|---|---|
| 측정 대상 \ 단계 | Process Area | Capability Level | Process Area | Capability Level |
| 평가 모델 구성 | PA 별 Specific Goal, Specific Practice 단계별 Generic Goal, Generic Practice | | PA 별 목적과 Base Practice 단계별 프로세스 속성, Management Practice | |
| 내용 | - 평가모델과 프로세스 영역 제시<br>- 프로세스 영역간의 카테고리별 상호작용 프레임웍과 모델 테일러링 제시<br>- 평가 요구사항, 평가 지침 등은 독립된 표준에서 제시 | | - 심사모델과 프로세스 영역 제시<br>- 심사 수행 가이드 제시<br>- 심사원에 대한 지침과 SPICE 사용 가이드 제시 | |

□ 평가 등급

Continuous CMMI 와 SPICE 는 6 단계의 수행 능력 단계를 정의하며 각 단계의 이름은 차이가 있으나, 단계에서 요구하는 내용은 유사하다.

[표 9] Continuous CMMI 와 SPICE 의 단계 비교

| Capability Level | Continuous CMMI | SPICE |
|---|---|---|
| 5 | Optimizing | Optimizing process |
| 4 | Quantitatively managed | Predictable Process |
| 3 | Defined | Established Process |
| 2 | Managed | Managed Process |
| 1 | Performed | Performed Process |

| | | |
|---|---|---|
| 0 | Incomplete | Incomplete Process |

### 4.3 보안 제품 및 시스템 평가 방법론 비교

보안 제품 및 시스템을 평가하기 위해서는 ISO/IEC 9126 에 정의된 소프트웨어의 품질평가 특성들 가운데 특히 보안성(Security)에 중점을 두어 평가할 필요가 있다. 이러한 경우는 보안과 관련한 보안환경, 보안정책수립, 취약성분석, 위험분석 등 ISO/IEC 14598 의 평가기준에 비하여 추가적으로 고려해야 할 평가요소가 있기 때문에 개발 산출물 및 개발 후의 완제품을 대상으로 품질을 평가하는 것은 충분하지 않다.

여러 국가에서 보안 제품 및 시스템의 보안성 평가를 위한 표준이 개발되었으며 이를 기초로 하여 국제 표준화하기에 이르렀다. 유럽 표준인 ITSEC, 미국 표준인 TCSEC, 캐나다 표준인 CTCPEC, 국제 표준인 CC 가 이에 속한다.

□ 구조

보안 제품 및 시스템의 보안평가에는 보안 기능과 보안 보증의 두 관점이 중요하다. 보안 기능관점은 보안 제품 및 시스템이 가져야 할 보안기능에 중점을 두는 반면, 보안 보증관점에서는 보안기능이 개발과정을 통하여 제대로 개발되고 있는가에 중점이 둔다.

CC, ITSEC 은 보안 제품 및 시스템(일명 TOE)의 보안기능을 TOE 의 특성에 따라 개발 초기 단계에서 보안 기능 요구사항(ST)으로 명세하도록 하고, 보안 보증 등급 평가는 정의한 보안기능 요구사항이 잘 반영되어 TOE 가 개발되었는가에 따라 결정하도록 한다.

특히 CC 는 TOE 의 잘 개발된 보안 기능 요구 사항들을 PP 로 등록하도록 하여 유사 TOE 들의 보안기능 요구 사항들을 재정의하지 않고 등록된 PP 로부터 참고할 수 있도록 한다.

또 다른 기준과 달리 CTCPEC 는 각 기능 별로도 등급을 정의하여, 필요한 보안기능 및 기능의 등급을 선택해서 TOE 의 보안 기능 요구사항 명세서에 정의할 수 있도록 하였다.

□ 보증 등급

보안 제품 및 시스템에 대한 보증을 정량적인 평가 수치로 제공할 수 있도록 보안 보증 등급을 정의한다. 보증등급은 CC, ITSEC, CTCPEC 의 경우 보안 보증 기준에 따라 결정이 되며, TCSEC 은 보증기준과 함께 보안기능도 보증 등급 평가의 근거가 된다.

[표 10] 보안 평가 방법론의 단계 비교

| CC | ITSEC | CTCPEC | TCSEC |
|---|---|---|---|
| | | T0 | |
| EAL1 | E0 | T1 | D |
| EAL2 | E1 | T2 | C1 |
| EAL3 | E2 | T3 | C2 |
| EAL4 | E3 | T4 | B1 |
| EAL5 | E4 | T5 | B2 |
| EAL6 | E5 | T6 | B3 |
| EAL7 | E6 | T7 | A1 |
| | | (기능단계제외) | |

## 5. 결론 및 향후 과제

본 논문에서는 먼저 다양한 보증 방법론들의 평가체계, 보증 매커니즘 등을 검토하고 범위, 대상, 국가 등의 기준으로 분류하였다. 분류 결과, 평가 대상과 체계 면에서 유사하고 서로 연관성이 있는 방법론들은 여러 가지 측면에서 서로 비교 분석하고 각각의 특성을 도출하였다.

향후 보증 방법론들의 분류 체계와 분석 결과를 토대로 조직의 상황을 분류하고, 이에 적합하게 보증 방법론을 적용하는데 도움을 주는 사용자 가이드를 제시하고자 한다.

## 참고문헌


[1] ISO/IEC PDTR 15443 A framework for IT security assurance

[2] CC; ISO/IEC 15408 Information technology – Security technology – Evaluation criteria for IT security

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

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

[5] V-model: Development Standard for IT Systems of the Federal Republic of Germany

[6] ISO/IEC TR 13335 Guidelines for the management of IT Security

[7] BS 7799 Information Security Management

[8] CMM: Capability Maturity Model for Software

[9] SE-CMM: A Systems Engineering Capability Maturity Model

[10] SA-CMM: Software Acquisition Capability Maturity Model

[11] SSE-CMM System Security Engineering Capability Maturity Model

[12] TCMM Trusted CMM Release Summary

[13] CMMI: Capability Maturity Model Integration for System Engineering, Software Engineering, Integrated Product and Process Development, and Supplier Sourcing (CMMI-SE/SW/IPPD/SS, Version1.1)

[14] SPICE; ISO/IEC TR 15504 Software Process Assessment

[15] ISO/IEC 9126 Information Technology - Software Product Quality

[16] ISO/IEC 14598 Information Technology - Software Product Evaluation

[17] CEM: Common Methodology for Information Technology Security Evaluation

[18] ITSEC: Information Technology Security Evaluation Criteria

[19] ITSEM: Information Technology Security Evaluation Manual

[20] TCSEC: Trusted Computer System Evaluation Criteria

[21] CTCPEC: The Canadian Trusted Computer Product Evaluation Criteria