제품, 프로세스, 통제 관점의 통합된 보안평가 모델

(A Security Evaluation Model in Aspects of Product, Process and Control)

이 지 은 † 최 병 주 ††
(Jieun Lee) (Byoungju Choi)

요 약 정보 보호에 대한 평가가 중요시 되고 있으며 보안 평가 방법론이 제안되었다. 이러한 보안 평가 방법론들은 크게 제품, 프로세스, 통제 중심의 세 가지 관점으로 분류될 수 있다.

본 논문에서는 제품, 프로세스, 통제 각기 하나의 관점에서 보안 평가할 때에 발생하는 문제점과 위협의 실례를 파악한다. 이 문제점을 해결하기 위하여 제품, 프로세스, 통제의 세 가지 관점을 통합한 보안평가 모델을 제안한다.

키워드 : 평가 방법론, 보안 제품 평가, 보안평가 모델

Abstract As the evaluation for the information security has been an important issue, numerous security evaluation methods have been proposed. Those security evaluation methods can be categorized into three different aspects in large including product, process and control.

In this paper we identify the possible problems that may occur when one-sided security evaluation is conducted that is on the aspect of product, process or control alone, present with the actual example of threat, and propose an approach to resolve each problem. Based on these approaches, we propose the security evaluation model, which incorporates these three aspects of product, process and control.

Key words : Evaluation Methodology, Security Product Evalution, Security Evaluation Model

1. 서 론

대부분의 정보 시스템이 네트워크를 기반으로 운영되면서 정보 유출 및 침해 등의 위협이 증가하고 있다. 정보 보호 시스템의 보안에 관한 신뢰성을 보증하기 위하여 보안 평가 방법론이 필요하게 되었다.

보안 평가 방법론들은 다음과 같이 제품, 통제, 프로세스의 세 가지 관점으로 분류할 수 있다. 정보 보호 초기에는 제품 단위로 보안 기능에 대한 기술적 평가를 수행하고자 하였다. 이러한 제품 관점의 보안 평가 방법론으로는 정보 보호 제품의 보안 기능성과 보증성 평가를 다룬 TCSEC (Trusted Computer System Evaluation Criteria)[1], ITSEC (Information Technology Security Evaluation Criteria)[2], CC (Common Criteria)[3] 등이 있었다. 그러나 제품 관점의 보안 평가 방법론은 조직 전체에 걸쳐 효과적인 정보 보호의 수준을 달성하기 어렵다는 단점이 있다.

80년대 중반 이후 관리적 관점의 정보 보호의 중요성이 대두되면서 정보 시스템의 기술적 환경 변화에 따른 조직내 보안 통제의 구현 여부에 초점을 둔 통제 관점의 보안 평가 방법론인 BS7799 (ISO/IEC 17799)[5], NIST(National Institute of Standards and Technology)의 시스템 정보 보호 자가 평가 지침(Security Self Assessment Guide for Information Technology System, NIST Special publication 800-26) 등이 제안되었다. 그러나 이러한 방법론은 지속적인 정보 보호의 개선에 대한 평가가 부족하였다.

최근에는 정보 보호에 대한 지속적 개선을 수행할 수 있도록 조직의 정보 보호 체계 수립 및 운영 프로세스에 초점을 둔 프로세스 측면의 보안 평가 방법론인 ISO/IEC 13335 GMITS (Guidelines for the Management of IT Security), SSE-CMM (System Security

· 본 연구는 한국과학재단 목적기초연구(과제번호:2003-000-10139-0)의 부분지원 및 대학 IT 연구센터 육성 지원사업의 부분지원으로 수행되었음
† 비 회 원 : LG전자 홈넷사업팀 연구원
kinye@paran.com
†† 종신회원 : 이화여자대학교 컴퓨터학과 교수
bjchoi@ewha.ac.kr
논문접수 : 2004년 3월 30일
심사완료 : 2005년 1월 12일

Engineering Capability Maturity Model) [4], ISACA (Information Systems Audit and Control Association)의 ISG (Information Security Covernance) 등이 등장하여 보안 평가 지침으로 사용되고 있다.

보안 평가를 체계적으로 수행하기 위해 TCSEC (Trusted Computer System Evaluation Criteria)[1], ITSEC (Information Technology Security Evaluation Criteria)[2], CC (Common Criteria)[3], SSE-CMM (System Security Engineering Capability Maturity Model)[4], BS7799 (ISO/IEC 17799)[5]등이 제안되었다. 이들 보안 평가 방법론들은 제품, 프로세스, 통제의 세 가지 관점으로 분류할 수 있다. 제품 관점의 정보 보호 방법론으로 TCSEC, ITSEC, CC 등이 있으며, 이들은 정보 보호 제품의 보안 기능성과 보증성 평가를 위한 표준을 제시한다. 프로세스 관점의 정보 보호 방법론으로 SSE-CMM이 있으며, 조직의 정보 보호 프로세스 수준을 평가한다. 통제 관점의 정보 보호 방법론에는 BS7799 등이 포함되며 조직에서 수행되는 통제를 통한 정보 보호의 구현을 평가한다.

세 가지 관점의 보안 평가 방법론은 적용 방법, 평가 대상, 평가 단계가 상이하므로 그 가운데 어느 하나만으로는 보안 보증의 허점이 존재할 수 있다. 따라서 본 논문에서는 이러한 보안 평가의 허점을 파악한다. 이를 개선하기 위하여는 세 가지 관점의 평가 방법론이 모두 고려할 필요가 있다.

본 논문에서는 제품, 프로세스, 통제 관점인 CC, SSE-CMM, BS7799의 상호 호환성의 분석을 토대로 효율적인 통합 평가를 수행할 수 있도록 하는 구체적이고도 실행 가능한 통합 보안 보증 모델을 제안한다. 또한 제안한 모델로 파악한 보안 허점을 개선할 수 있음을 보이고 효율적인 평가를 수행하는 지침을 제시한다.

본 논문의 구성은 다음과 같다. 2절에서 보안 평가 방법론과 관련된 연구를 기술하고, 3절에서 보안 평가에서의 세가지 관점을 함께 고려하지 않은 경우의 문제점과 그 사례를 제시한다. 그리고 4절에서 세가지 관점을 함께 고려하는 평가 방안을 제안하여 제안된 모델의 장점을 제시한다. 5절에서는 결론 및 향후 연구에 대하여 기술한다.

2. 관련 연구

CC의 제품 평가와 프로세스 평가를 통합하여 보안 보증의 효율성을 향상시키기 위한 기존 연구로써 AAWG(Alternative Assurances Working Group)의 보증 방법론 대응 보고서와 CC기반의 보안 평가 개선 방안에 대하여 기술한다.

2.1 AAWG의 보증 방법론 대응 보고서

AAWG는 보안 보증의 효율성을 향상시키기 위하여 다양한 보증 방법론들을 개발 프로세스 보증 방법론, X/Open Branding 보증 방법론, 평가 보증 방법론의 세 가지로 나누고, 평가 보증 방법론 중 하나인 CC를 개발 프로세스 보증 방법론과X/Open Branding 보증 방법론과의 대응 작업을 진행하였다[6,7]. 공개된 연구 결과 문서로써 CC EAL3 보증 요구사항에 SSE-CMM을 대응시킨 AAP3/SSE-CMM[6]이 있다.

AAP3/SSE-CMM은 CC EAL3의 각 보증 컴포넌트의 엘리먼트에 대하여 일치되는 SSE-CMM 프로세스 영역의 기본 프랙티스와 수행 능력단계 2의 일반 프랙티스를 대응시키고 있다. 대응 정도가 FULL, PARTIAL인 CC EAL3 보증 요구사항으로 구성된 DAL (Development Assurance Level)과 대응 정도가 NONE인 CC EAL3 보증 요구사항으로 구성된 SEAL (Subset Evaluation Assurance Level)을 구별하여 두 보증 방법론 평가를 상호 호환할 수 있게 한다.

그러나 AAWG는 보증 방법론 대응 결과를 완전히 공개하지 않았다. AAP3/SSE-CMM은 보증 방법론과 CC 평가의 상호 호환에만 초점을 맞추고 있는 반면 보안 평가 프로세스 정립 혹은 개선을 직접 반영하고 있지 않다.

2.2 CC 기반 보안 평가의 개선방안

CC 기반의 TOE(Target of Evaluation) 보증 평가를 수행할 때 SSE-CMM, BS7799, IT Baseline Protection Manual 등의 다른 관점의 평가 방법론을 함께 고려한다면 보안 평가를 개선할 수 있을 것이다[8-10].

조직의 정보 보안 상태(information security status)를 개선하기 위해 평가된 제품을 사용하는데 초점을 맞출 것인가, 좋은 보안 공학 프로세스를 따르는데 초점을 맞출 것인가에 대한 연구가 진행되었다[8]. 이 연구에서는 먼저 보안 보증 방법론을 제품/시스템 평가 기준과 프로세스 인증 기준으로 분류하여 그 특성을 살펴본 후, 제품이 사용될 IT 환경은 모두 유일(unique)하므로 평가된 제품이 전체 정보 보안에 끼치는 영향을 측정하기 위해서는 제품 자체 뿐만 아니라 제품이 사용될 조직의 프로세스까지 고려해야 한다고 보았다. 따라서 보안평가는 전체 시스템에서 CC기반으로 평가된 제품이 차지하는 비율과 조직 프로세스의 BS7799 일치 정도(compliance rate)를 함께 고려해야 한다는 결론을 내리고 있다. 이 연구는 CC와 BS7799 평가를 함께 고려해야 함을 보였으나 두 가지 평가를 함께 수행하기 위한 효율적인 방안을 제시하지는 못했다.

보안을 위한 요구사항을 IT 요구사항(IT-Requirements)과 IT 요구사항이 아닌 경우로 나누고, IT 요구사항의 평가는 CC를 기준으로, non-IT 요구사항의 평

가는 IT Baseline Protection Manual 등의 기준으로 평가하는 방안이 제시되었다[9]. 이 연구에서는 CC와 IT Baseline Protection Manual을 함께 고려하여 모든 보안 필요(Needs)를 만족시키는 사용자 친화적인 체크리스트(User-Friendly Check List)를 작성하고자 한다. 이 연구 또한 보안을 위하여 두 가지 기준을 모두 고려해야 할 필요를 제시하였으나 효율적으로 통합하는 방안을 제시하지는 못하였다.

CC 평가를 위한 일종의 요구 명세 문서인 보호프로파일(Protection Profile)의 효율적인 작성을 위해 SSE-CMM의 PA(Process Area)를 적용하는 P3I 연구가 제안되었다[10]. 보호프로파일의 생성에 필요한 활동과 대응되는 SSE-CMM의 프로세스 영역을 다음과 같이 제시한다.

- Understanding the Risk: PA02, PA03, PA04, PA05
- Understanding Policy, Assumptions, and Objectives: PA07, PA08, PA10
- Identifying Requirements: PA01, PA07, PA09, PA10
- Understanding Assurance: PA06, PA07, PA09, PA10
- Checking for Consistency and Completeness: PA11, PA06

이 연구는 보호프로파일 개발 프로세스에 해당하는 SSE-CMM의 공정영역을 나열하는 정도에 그칠 뿐 프로세스 성숙도의 지표가 되는 SSE-CMM의 기본 프랙티스에 대해서는 언급하고 있지 않으므로 어떻게 보호프로파일 개발 프로세스가 개선이 될 수있는지를 알기 어렵다.

기존의 연구들은 CC 기반의 보안 평가를 개선하기 위해 다른 관점의 방법론을 함께 고려하는 방안을 찾았으나 함께 고려해야 하는 실질적인 이유를 제시하지 못하였고, 실제로 보안 평가에서 사용할 수 있는 구체적이고 효율적인 평가 모델을 제시하지 못하였다. 따라서 본 논문에서는 더 나은 보안 보증을 위해서 다른 관점의 보안 보증 방법론들을 함께 고려해야 할 필요성을 확인하고 구체적인 문제점의 사례를 든다. 그리고 효율적으로 평가를 수행하기 위한 방안으로써 통합 보안 보증 방법론을 제안한다.

3. 단독 평가의 문제점과 그 사례

제품, 프로세스, 통제 가운데 한 가지 관점만으로 보안 평가를 수행할 경우 어떠한 문제점이 발생할 수 있는지를 파악한다. 이를 위해 제품, 프로세스, 통제 관점의 보안 평가 방법론 가운데 국제적으로 통용되는 기준인 CC, SSE-CMM, BS7799를 각각 선택하여 평가 요구사항을 항목별로 대응한다. 대응 결과로부터 중복되지 않는 평가 요구사항을 추출하여 단독 평가에서는 평가되지 않는 부분을 파악한다. 파악한 각 부분에 대하여 보안 평가에서 고려하지 않음으로 인하여 발생할 수 있는 문제점을 기술하고 사례를 제시한다.

3.1 제품 단독 보안 평가의 문제점 및 사례

제품 평가만으로 보안 평가를 수행한 경우의 문제점을 파악하기 위해 제품평가에서는 수행하지 않는 프로세스 평가와 통제 평가의 요구사항을 분석하고 이를 통해 발생 가능한 문제점을 찾는다.

3.1.1 제품 평가에서 수행하지 않는 프로세스 평가 요구사항

제품 평가에서는 평가하지 않고, 프로세스 평가에서 평가 대상으로 보는 평가요구사항을 도출한다. 이 결과 CC의 보증 컴포넌트와 대응되지 않는 SSE-CMM의 기본 프랙티스는 표 1과 같다.

표 1 CC의 보증 컴포넌트와 대응되지 않는 SSE-CMM의 PAs

PA no.	PA
PA12	Ensure quality
PA14	Manage project risk
PA15	Monitor and control technical effort
PA17	Define organizational systems engineering process
PA18	Improve Organization's Security Engineering Process
PA19	Manage product line evolution
PA20	Manage Systems Engineering Support Environment
PA21	Provide Ongoing Skills and Knowledge
PA22	Coordinate with suppliers

SSE-CMM의 PA들 가운데 CC가 평가하지 않는 부분은 주로 Project and Organizational Process Areas에 속하는 PA들이다. 이러한 PA들은 프로젝트와 조직의 능력을 평가하고 개선하기 위한 기준이므로 제품 평가에서 이러한 부분은 평가 기준이 될 수 없다. SSE-CMM과 CC의 대응 결과에서 제품 평가와의 차별성을 잘 보여주는 프로세스 평가 요구 사항들은 조직의 프로젝트와 프로세스 관리, 환경 관리, 조직원의 훈련 부분이다.

3.1.2 제품평가에서는 수행하지않는 통제 관점의 평가 요구사항

제품 평가에서는 평가하지 않고, 통제 관점 기준에서만 평가 대상으로 보는 평가 요구사항은 표 2와 같다.

BS7799-1의 보안 프랙티스과 CC의 보증 컴포넌트를 대응시키면 주로 명세 관련 부분과 테스팅 관련 부분들과 대응되며, 이러한 부분을 제외한 보안 조직과 인적

표 2 CC와 대응되지 않는 BS7799의 프랙티스

Security Practice category	Security Practice
Security Organization	Security of third party access
	Outsourcing
Personnel security	User training
Physical and environmental security	Secure areas
	Equipments security
	General controls
Communications and operations management	System planning and acceptance
	Protection against malicious software
	Housekeeping
	Network management
	Media handling and security
Access control	Mobile computing and teleworking
System development and maintenance	Security in application systems
	Security of system files
Business continuity management	Aspects of business continuity management
Compliance	System audit considerations

자원, 물리적인 보안 환경과 보안 기술에 관련된 프랙티스와는 대응되지 않는다.

3.1.3 제품 평가의 문제점과 사례

제품 평가에서는 수행하지 않는 프로세스 평가 요구사항과 통제 평가 요구사항으로부터 파악한 제품 평가만으로 이루어지는 보안 보증시의 문제점과 사례를 다음과 같이 제시하고, 제시한 문제점에 대한 근거로써 표 1, 2의 대응되지 않은 관련 평가 요구사항을 제시한다.

Pd 1 보안 시스템 운영시의 보안 관리, 통제를 고려하지 못한다.

(문제점의 근거: SSE-CMM PA 14, 15. BS7799 Physical and environmental security, Communications and operations management)

Ex1_1 높은 보안성 레벨을 받은 방화벽 제품을 사용해도 네트워 관리자가 설정을 잘못하면 방화벽의 기능을 충분히 활용하지 못하여 시스템에 대한 침입을 제대로 막아낼 수 없다.

Ex1_2 새로운 보안 소프트웨어를 서버에 설치했음을 모르는 조직원이 시스템의 보안 소프트웨어의 데몬을 죽인다거나 설정에 손상을 가할 수 있다.

Pd 2 IT 환경의 중요성을 간과한다. 즉 조직과 조직 구성원, 환경적 특성에 대해 평가하지 않는다는 문제점이 있다.

Pd 2.1 구체적인 기술적 운영 환경을 고려해야 알 수 있는 위협의 발생 가능성에 대한 평가가 어렵다.

(문제점의 근거: SSE-CMM PA 14, 15. PA20. BS7799 Physical and environmental security, Communications and operations)

Ex2.1_1 서버에 높은 보안성 레벨을 소프트웨어 제품을 설치해도 해당 서버에 설치된 다른 소프트웨어와의 연관성, 서버의 하드웨어적 구성 등을 고려하지 못하면 충돌이 발생하여 보안성을 제대로 발휘하지 못할 수 있다.

Ex2.1_2 시스템이 연결된 백본 망이 정책에 따라 DOS 공격에 취약하여 이에 따른 위협의 발생 가능성이 높음을 미리 평가할 수없다.

Pd 2.2 보안에서 조직적 측면을 고려하지 못한다. 즉, 제품을 사용할 조직의 특성, 보안 정책 등을 고려하지 못한다.

(문제점의 근거: SSE-CMM PA17, BS7799 Security Organization)

Ex2.2_1 네트워의 전체 구성도와 보안 정책을 충분히 고려하지 않은 서버 추가, 혹은 변경은 시스템 전체의 보안성을 깨뜨리는 결과를 가져올 수 있다.

Pd 2.3 조직 구성원 측면을 고려하지 못한다. 보안 구축 및 유지를 위해서는 조직 구성원, 특히 고위직의 보안 의지가 중요하며, 조직원 전체에 대한 보안훈련이 요구된다.

(문제점의 근거: SSE-CMM PA 21, BS7799 Personnel Security)

Ex2.3_1 보안에 대한 교육을 받지 못한 한 조직원이 조직 내 개인적인 PC의 보안을제대로 설정하지 않음으로써 조직의 전체 시스템을 외부 공격 위험에 빠뜨릴 수있다.

Ex2.3_2 관리 소홀로 보안 패치를 하지 않은 데이타

베이스 서버의 보안 허점을 이용한 웜바이러스로 인하여 네트웍에 대량의 트래픽이 유발되어 2003년 1월 25일 전국적인 인터넷의 마비 사태를 빚은 바 있다.

Pd 2.4 보안에서 건물 시설(building infrastructure) 측면을 고려하지 못 한다.

(문제점의 근거: BS7799 Physical and environmental security)

Ex2.4_1 정전, 낙뢰, 침수 등의 물리적인 재해로 인하여 제품이 손상을 입어 제대로 작동하지 않음으로써 정보 유출과 비정상적인 작동을 야기할 수있다.

Pd 2.5 보안 시스템에 영향을 끼치는 제품 외부의 기술적 측면을 고려하지 못 한다.

Ex2.5_1 시스템에 설치될 소프트웨어 제품 자체의 기술적 측면뿐 아니라 제품과 함께 사용되는 이 메일 클라이언트나 오피스 프로그램의 보안 측면을 고려할 필요가 있다.

Pd 3 시스템 내의 한 부분으로서의 제품을 평가하는 개념이 부족하다. 시스템은 일반적으로 여러 가지 상이한 제품들의 조합으로 이루어진다. 단일 제품 평가로 그 제품이 시스템 전체의 보안에 끼치는 영향을 평가할 수 없으며, 각각의 제품에 대한 평가로는 전체 시스템의 보안을 평가했다고 볼 수 없다.

(문제점의 근거: SSE-CMM PA 20, BS7799 System development and maintenance)

Ex3_1 제품 A가 제품 B, C, D 등과 함께 시스템 X를 이룰 때 제품 A와 제품 B간에 충돌이 발생하여 비록 각각의 제품은 높은 보안성 레벨을 받았음에도 불구하고 그 보안 기능을 제대로 발휘하지 못할 수 있다.

3.2 프로세스 단독 보안 평가의 문제점 및 사례

3.1절과 동일한 방법으로 프로세스 평가만으로 보안 평가를 수행한 경우의 문제점을 파악하기 위해, 프로세스 평가에서는 수행하지 않는 제품 평가와 통제 평가의 요구사항을 분석하고 이를 통해 발생 가능한 문제점을 찾는다.

3.2.1 프로세스 평가에서 수행하지 않는 제품 평가 요구사항

프로세스평가에서는 평가하지 않고 제품 평가에서만 평가 대상으로 보는 평가요구사항을 도출한다. 그 결과, SSE-CMM의 기본 프랙티스와 대응되지 않는 CC의 보증 컴포넌트는 표 3과 같다.

프로세스 평가 기준은 조직의 프로세스를 평가대상으로 하므로 제품의 최종 산출물, 외부 품질에 해당되는 부분의 평가가 부족하다. 대응 결과에서 프로세스 평가와의 차별성을 잘 보여주는 보증 컴포넌트들은 실질적인 구현과 개발 도구, 기법에 관련된 부분이다.

3.2.2 프로세스 평가에서 수행하지 않는 통제 관점 평가 요구사항

프로세스 평가에서는 평가하지 않고 통제 관점 기준에서만 평가 대상으로 보는 평가 요구사항을 도출한다. BS7799-1의 보안 프랙티스와 SSE-CMM의 프랙티스를 대응시킨 결과 보안조직의 정책, 책임, 조직원의 훈련과 같은 요구 사항들은 완전히 혹은 부분적으로 대응되나, 구체적인 기술적, 물리적 요구 사항들은 대응되지 않는다. 대응되지 않은 BS7799-1의 보안 프랙티스 영역은 표 4와 같다.

3.2.3 문제점과 사례

프로세스 평가에서는 수행하지 않는 제품 평가 요구사항과 통제 평가 요구사항으로부터 파악한 프로세스 평가만으로 이루어지는 보안 보증시의 문제점과 사례를 다음과 같이 제시하고, 제시한 문제점에 대한 근거로써 표 3, 4의 대응되지 않은 관련 평가 요구사항을 제시한다.

표 3 SSE-CMM과 대응되지 않는 CC의 보증 컴포넌트

Families	Components
ACM_CAP	Version numbers (ACM_CAP1)
ADO_DEL	Delivery procedures (ADO_DEL1) Detection of modification (ADO_DEL2) Prevention of modification (ADO_DEL3)
ADV_IMP	Subset of the implementation of the TSF (ADV_IMP1) Implementation of the TSF (ADV_IMP2) Structured implementation of the TSF (ADV_IMP3)
ALC_LCD	Developer defined life-cycle model (ALC_LCD1) Standardised life-cycle model (ALC_LCD2) Measurable life-cycle model (ALC_LCD3)
ALC_TAT	Well-defined development tools (ALC_TAT1) Compliance with implementation standards (ALC_TAT2) Compliance with implementation standards all parts (ALC_TAT3)

표 4 SSE-CMM과 대응되지 않는 BS7799의 프랙티스

Security Practice Category	Security Practice
Physical and environmental security	Secure areas
	Equipments security
	General controls
Communications and operations management	Protection against malicious software
	Network management
	Media handling and security
	Exchanges of information and software
Access control	Operation system access control
	Mobile computing and teleworking
Systems development and maintenance	Security in application systems
	Cryptographic controls
	Security of system files
Business Continuity management	Aspects of business continuity management

Pc 1 프로세스 평가는 제품 평가를 대체할 수 없다. SSE-CMM에서도 명백히 언급하고 있는 것과 같이 SSE-CMM 프로세스 평가는 제품 평가를 대체할 수 없다. 좋은 프로세스가 제품의 결함 없음을 의미하지는 않으며, 다만 결함을 어느 정도까지 더 예측 가능하게 한다.

(문제점의 근거: SSE-CMM "The SSE-CMM is a replacement for product evaluation")

Ex1_1 프로세스 평가에서 높은 레벨을 받은 조직이 생산한 제품이 반드시 높은 보안레벨을 보장할 수 있는 것은 아니다.

Pc 2 프로세스 평가 기준은 조직의 프로세스를 평가 대상으로 하므로 TOE의 최종산출물과 외부 품질, 특히 보안에 해당되는 부분의 평가가 부족하다.

Pc 2.1 제품의 보안 기능 요구사항이 제대로 구현되었는가에 대한 평가가 부족하다. 즉, 소스 코드나 펌웨어, 하드웨어 설계도 등 구체적으로 TOE 제품의 구현을 나타내는 부분을 평가하지 않으며, TOE를 개발하는데 사용된 프로그래밍 언어, 구현기술, 라이브러리와 같이 직접적으로 TOE의 특성과 관련될 수있는 부분에 대한 평가가 부족하다. 또한, TOE의 보안기능 요구사항과 구현의 표현간에 일치성을 평가할 필요가 있다.

(문제점의 근거: CC ADV_IMP, ALC_TAT)

Ex2.1_1 개발에 사용되는 데이타 베이스 시스템이 TOE의 보안기능 요구사항을 충분히 구현할 수 있는지, 성능과 표현력, 안정성을 고려할 필요가 있다. 시스템에 MySQL이 사용된 경우, MySQL은 transaction과 trigger 기능을 지원하지 않음을 미리 고려하고 TOE의 구현에 이러한 기능이 필요하다면 다른 방법으로 대체할 가능성과 대체 코드의 보안성을 평가에서 고려할 필요가 있다.

Ex2.1_2 TOE를 개발하는데 사용된 언어에서 제공하는 라이브러리가 TOE의 특성에 맞고, 충분한 신뢰성을 발휘하는지 평가할 필요가 있다.

Pc 2.2 프로세스 평가는 제품에 대한 평가가 아니므로 TOE 제품의 결함에 대한 평가는 부족하다.

(문제점의 근거: CC ALC_TAT)

Ex2.2_1 높은 프로세스 평가 등급을 받은 조직이 생산한 보안 제품도 운영 시 결함이발생할 수 있다.

Pc 2.3 구체적인 기술적, 물리적 보안 사항들에 대한 평가가 부족하다

(문제점의 근거: CC ADV_IMP, BS7799 Physical and environmental security)

Ex2.3_1 프로세스 평가에서 보안 환경에 대한 평가는 구체적으로 전원공급, 케이블 보안, 집기의 보안, 사용자 출입 제한 등의 구체적인 보안 항목에 대한 평가를 제시하지는 않는다.

Pc 3 작은 조직은 평가를 받을 만한 체계적인 프로세스가 잡혀있지 않을 수 있다.

(문제점의 근거: CC ADV, ALC, ATE)

Ex3_1 보안 소프트웨어 개발업체가 아니라 일반 소프트웨어 업체이거나, 소규모 업체의 경우는 개발된 제품은 있으나, 체계적인 프로세스가 정립되지 않아 프로세스 평가를 수행할 만한 기반이 미흡할 수 있다.

3.3 통제 단독 보안 평가의 문제점 및 사례

통제 평가만으로 보안 평가를 수행한 경우의 문제점을 파악하기 위해, 통제 평가에서는 수행하지 않는 제품 평가와 프로세스 평가의 요구사항을 분석하고 이를 통해 발생 가능한 문제점을 찾는다.

3.3.1 통제 관점 평가에서 수행하지 않는 제품 평가 요구사항

통제 기준 평가에서는 평가하지 않고, 제품 평가 기준에서만 평가 대상으로 보는 평가요구사항을 도출한다. 제품의 보안 평가 기준은 산출물을 근거로 제품에 대한 보안 보증을 수행하는 것이므로 시스템 운영 상의 통제와 관리에 중점을 두는 통제 관점 보안 요구사항과는 평가 대상에 차이가 있다. 따라서 본 연구에서는 CC의 TOE를 BS7799에서의 정보보안 관리시스템으로 보고 대응시켰으며 대응되지 않는 CC의 보증 컴포넌트는 표 5와 같다.

표 5 BS7799의 프랙티스와 대응되지 않는 CC의 보증 컴포넌트

Class	Families
ACM	Configuration automation (ACM_AUT) Configuration scope (ACM_SCP)
ADO	Delivery (ADO_DEL) Installation, generation and start-up(ADO_IGS)
ADV	Functional specification (ADV_FSP) High-level design (ADV_HLD) Implementation representation (ADV_IMP) TSF internals (ADV_INT) Low-level design (ADV_LLD) Representation correspondence (ADV_RCR)
AGD	Administrator guidance (AGD_ADM)
ALC	Development security (ALC_DVS) Life cycle definition (ALC_LCD) Tools and techniques (ALC_TAT)
ATE	Coverage (ATE_COV) Depth (ATE_DPT) Independent testing(ATE_IND)
AVA	Misuse (AVA_MSU) Strength of TOE security functions (AVA_SOF)

보안 통제관점의 평가는 운영과정의 보안 관리를 중점적으로 평가하므로 제품의 전체 생명주기에 대한 개념과 생명주기 중 운영을 제외한 설계, 개발 등에 대한 평가가 부족하다.

3.3.2 통제 관점 평가에서 수행하지 않는 프로세스 평가 요구사항

통제 기준 평가에서는 평가하지 않고, 프로세스 평가 기준에서만 평가 대상으로 보는 평가 요구사항을 표 6과 같이 도출한다. 프로세스의 보안 평가 기준은 조직의 보안 프로세스에 대한 평가하고 보증하는 것으로 시스템 운영상의 통제와 관리에 중점을 두는 통제 관점 평가 요구사항이 더 구체적이고 보안 관리프로세스에 한정되어 그 범위가 좁다. 즉, 조직의 전체 보안 공학 프로세스를 정의하고 이를 개선해나가는 부분에 대한 평가가 부족하다.

3.3.3 문제점과 사례

통제 관점의 평가에서 수행하지 않는 제품 평가 요구사항과 프로세스 평가 요구사항으로부터 파악한 통제 평가만으로 이루어지는 보안 보증시의 문제점과 사례를 다음과 같이 제시하고, 제시한 문제점에 대한 근거로써 표 5, 6의 대응되지 않은 관련 평가 요구사항을 제시한다.

Ct 1 제품의 전체 생명주기에 대한 개념과 생명주기 중 운영을 제외한 설계, 개발 등에 대한평가가 부족하다.

(문제점의 근거: CC ALC_DVS, ALC_LCD. SSE-CMM PA 17)

Ex1_1 운영 시에 아무리 보안 관리와 통제를 고려하더라도 시스템의 보안 취약점으로 인해 보안에 결함이 존재할 수 있다.

Ct 2 조직의전체 보안 공학 프로세스에 대한 평가가 부족하다. 프로세스 개선에 대한 개념이 없다.

(문제점의 근거: SSE-CMM PA 17, 18, 19)

Ex2_1 각각의 보안 항목이 분리되어 있어 전체 프로세스를 개선하여 조직의 능력이 향상되는 개념이 아니므로, 평가만을 위해 표준에서 언급한 특정 항목에 대한 평가에 대비하여 실제 조직의 능력보다 더 높은 통제 평가 등급을 받을 수 있다.

Ct 3 시스템을 평가를 받은 제품으로 구축하는가에 대한 평가가 없다.

(문제점의 근거: CC ALC, ATE)

Ex3_1 보안 평가를 받지 않은제품으로 보안 시스템을 구축한 조직이 높은 보안 통제 평가를 받을 수 있다. 이런 경우 조직이 높은 보안 통제 평가 레벨을 받았음에도 불구하고 시스템 운영 중에 제품의 취약점을 악용한 보안 사고가 발생할 수 있다.

4. 통합 보안평가 모델

표 6 BS7799의 프랙티스와 대응되지 않는 SSE-CMM의 기본 프랙티스

PA 분류	PA
Security Engineering Process Areas	PA04-Assess Threat PA09-Provide Security Input
Project and Organizational Process Areas	PA12-Ensure quality PA17-Define organizational systems engineering process PA19-Manage product line evolution

각각 제품, 프로세스, 통제 세 가지 관점 보안 평가 방법론은 적용방법, 평가 대상, 평가 단계 등의 면에서 서로 상이하므로, 하나의 관점에서만 보안을 보증한 경우 다른 관점을 고려하지 못하여 3장에서 제시한 것과 같은 보안 결함이 발생할 수 있다. 이러한 문제점은 제품 단독 평가의 경우 대부분 프로세스 평가를 고려하지 않은 결과이고, 프로세스 단독 평가의 경우 제품 평가를 고려하지 않은 결과이다. 또한 통제 기준의 평가는 보안 시스템 관리에 초점을 두어 전체를 고려하지 못한 결과이다. 따라서 이 장에서는 문제점을 해결하기 위해 제품, 프로세스, 통제 관점의 평가 기준을 통합한 보안평가 모델을 제안한다.

4.1 보안평가 모델 개발 방안

여러 관점을 두루 고려한 방법론을 제안하기 위해 다양한 보안 보증 방법론을 분석한 후 그 가운데 통합 방법론의 기반이 될 평가 기준을 선정한다. 먼저 제품 보안 평가 기준 가운데 국제 표준인 CC를 기반으로 하여 CC와 호환성이 높은 SSE-CMM을 선택하였다. CC의 보증 요구 사항인 형상 관리(Configuration management), 배포 및 운영(Delivery and operation), 개발(Development), 설명서(Guidance documents), 생명주기지원(Life cycle support), 시험(Tests), 취약성 평가(Vulnerability assessment) 클래스를 중심으로 관련 보증 방법론을 비교 분석한 결과는 표 7과 같다. CC의 보증 요구사항 클래스의 내용이 이들 보증 방법론에 관련항목이 언급되어 있는 정도를 비교하여, 거의 일치되는 항목이 있는 경우는 O, 어느 정도 있는 경우는 △, 없는 경우는 X로 표기하였다.

표 7에서 보면 CC 보증 요구사항에 관련된 내용이 관련 보증 방법론 중 SSE-CMM에 충실히 언급되어 있음을 알 수 있다. 따라서 CC 보증 요구사항 중에서 대부분의 관련 보증 방법론에 언급되어 있는 형상관리, 배포 및 운영, 개발, 설명서, 생명주기지원, 시험의 6개의 클래스를 대상으로 CC 보증 요구사항에 관련된 내용을 가장 많이 언급하고 있는 SSE-CMM 보안 프로세스를 중심으로 CC 기반 보안 프로세스 평가 모델을 개발하는 것이 적합하다.

또한 여기에 통제 관점의 평가 방법론을 통합함으로써 CC와 SSE-CMM으로는 평가가 미흡한 보안 관리에 대한 보증을 수행할 수 있다. 그러나 통제 관점의 평가 방법론 가운데 NIST 800-26은 미 정부 산하 기관에서 주로 사용되는 것으로 일반 기업에서 수용하기에는 어려움이 있다. 따라서 최근 ISO 표준으로 채택되었으며 국내외 대다수의 조직에서 적용하고 있는 BS7799와의 호환을 통해 제안하는 평가 모델의 도입이 더 용이하게 이루어 질 수 있도록 한다.

또한 여기에 BS7799을 통합함으로써 CC와 SSE-CMM으로는 평가가 미흡한 보안 관리에 대한 보증을 수행할 수 있으며, 일반적인 기업과 보안 조직이 더 쉽게 통합 평가모델을 받아들일 수 있도록 한다.

선정한 CC, SSE-CMM, BS7799로 통합 보안평가 방법론을 개발하기 위하여 다음과 같은 개발 방안을 제안한다.

- SSE-CMM과 CC, BS7799의 대응
- CC 컴포넌트와 BS7799 프랙티스 별로 SSE-CMM 수정

4.1.1 SSE-CMM와 CC, BS7799의 대응

통합 보안평가 모델을 제안하기 위해 먼저 SSE-CMM의 22개 프로세스 영역에 대한 기본 프랙티스 및 수행 능력 단계별 일반 프랙티스를 CC의 보증 컴포넌트의 각 엘리먼트와 비교한다. 비교 결과 SSE-CMM의 평가 요구사항으로 해당 CC의 평가 요구사항을 만족시키는 정도를 FULL, PARTIAL, NONE으로 구분하여 나타내었으며, 그 결과는 표 8과 같다.

- FULL: 완전히 대응되는 SSE-CMM BP(Base Practice) 혹은 GP(Generic Practice)가 있다.
- PARTIAL: 일부 대응되는 SSE-CMM BP 혹은 GP가 있다.
- NONE: 대응되는 SSE-CMM BP 혹은 GP가 없다.

BS7799의 경우는 보안 보증에 해당되는 프랙티스와 시스템의 기능에 해당하는 프랙티스, 시스템의 운영 환경의 보안에 대한 프랙티스들이 섞여 있다. 이 프랙티스들을 종류에 따라 분류하고 BS7799 프랙티스 가운데 보안 보증에 해당되는 프랙티스들은 CC와 SSE-CMM

표 7 CC와 관련 방법론의 상호호환성 분석

	CMMI	SSE-CMM	SPICE	ISO/IEC 15288	ISO/IEC 12207
형상관리	O	O	O	O	O
배포 및 운영	X	△	O	O	O
개발	O	O	O	O	O
설명서	O	O	O	X	X
생명주기지원	△	O	X	△	X
시험	O	O	O	O	O
취약성 평가	X	O	X	X	X

표 8 SSE-CMM와의 대응 정도에 따른 CC 보증 컴포넌트

CC 보증 패밀리	SSE-CMM과의 대응 CC 보증 컴포넌트		
	FULL	PARTIAL	NONE
APE_DES	1.1D, 1.1C, 1.1E		1.2E,1.3E
APE_ENV	1.1D	1.1C, 1.2C, 1.3C, 1.1E	1.2E
APE_INT			1.1D, 1.1C, 1.2C, 1.1E, 1.2E, 1.3E
APE_OBJ	1.1D, 1.2D, 1.1C	1.2C, 1.3C, 1.4C, 1.5C, 1.1E	1.2E
APE_REQ	1.1D, 1.2D, 1.4C, 1.5C	1.13C, 1.14C, 1.1E	1.1C, 1.2C, 1.3C, 1.6C, 1.7C, 1.8C, 1.9C, 1.10C, 1.11C, 1.12C, 1.2E
APE_SRE	1.1D, 1.2D, 1.1C, 1.2C, 1.6C	1.7C, 1.1E	1.3C, 1.4C, 1.5C, 1.2E
ASE_DES	1.1D, 1.1C, 1.1E		1.2E, 1.3E
ASE_ENV	1.1D	1.1C, 1.C, 1.3C,1.1E	1.2E
ASE_INT			1.1D, 1.1C, 1.2C, 1.3C, 1.1E, 1.2E, 1.3E
ASE_OBJ	1.1D, 1.2D, 1.1C	1.2C, 1.3C, 1.4C, 1.5C, 1.1E	1.2E
ASE_PPC			1.1D, 1.2D, 1.1C, 1.2C, 1.3C, 1.1E, 1.2E
APE_REQ	1.1D, 1.2D, 1.4C, 1.5C	1.13C, 1.1E	1.1C, 1.2C, 1.3C, 1.6C, 1.7C, 1.8C, 1.9C, 1.10C, 1.11C, 1.12C, 1.2E
APE_SRE	1.1D, 1.2D, 1.1C, 1.2C, 1.6C	1.7C, 1.1E	1.3C, 1.4C, 1.5C, 1.2E
ASE_TSS			1.1D, 1.2D, 1.1C, 1.2C, 1.3C, 1.4C, 1.5C, 1.6C, 1.7C, 1.8C, 1.9C, 1.10C, 1.1E, 1.2E
ACM_CAP			1.1D, 1.1C, 1.2C, 1.1E
	2.2D, 2.3D, 2.3C, 2.4C	2.5C, 2.6C, 2.1E	2.1D. 2.1C, 2.2C
	3.2D, 3.3D, 3.3C, 3.4C, 3.7C, 3.8C, 3.9C, 3.10C	3.5C, 3.6C, 3.1E	3.1D, 3.1C, 3.2C
	4.2D, 4.3D, 4.3C, 4.4C, 4.7C, 4.8C, 4.9C, 4.10C, 4.12C	4.5C, 4.6C, 4.1E	4.1D, 4.1C, 4.2C, 4.11C
	5.2D, 5.3D, 5.3C, 5.4C, 5.7C, 5.8C, 5.9C, 5.10C, 5.12C, 5.16C	5.5C, 5.6C, 5.15C, 5.18C, 5.1E	5.1D, 5.1C, 5.2C, 5.11C, 5.13C, 5.14C, 5.17C, 5.19C, 5.20C, 5.21C
ACM_AUT	1.1D, 1.2D, 1.1C, 1.3C	1.4C, 1.1E	1.2C
	2.1D, 2.2D, 2.1C, 2.3C, 2.6C	2.4C, 2,1E	2.2C, 2.5C
ACM_SCP	1.1D, 1.1C	1.1C, 1,1E	
	2.1D, 2.1C	2.1C, 2.1E	
	3.1D, 3.1C	3.1C, 3.1E	
ADO_DEL			1.1D, 1.2D, 1.1C, 1.1E
			2.1D, 2.2D, 2.1C, 2.2C, 2.3C, 2.1E
			3.1D, 3.2D, 3.1C, 3.2C, 3.3C, 3.1E
ADO_IGS	1.1D, 1.1C, 1.2C, 1.4C	1.1E	1.3C, 1.2E
ADV_FSP	1.1D, 1.1C, 1.2C, 1.4C	1.1E	1.3C, 1.2E
	2.1D, 2.1C, 2.2C, 2.4C	2.1E	2.3C, 2.5C, 2.2E
	3.1D, 3.2C, 3.4C	3.1C, 3.1E	3.3C, 3.5C, 3.2E
	4.1D, 4.2C, 4.4C	4.1C, 4.3C, 4.1E	4.5C, 4.2E
ADV_HLD	1.1D, 1.1C, 1.2C, 1.3C, 1.4C, 1.5C, 1.6C, 1.7C	1.1E	1.2E
	2.1D, 2.1C, 2.2C, 2.3C, 2.4C, 2.5C, 2.6C, 2.7C	2.8C, 2.1E	2.9C, 2.2E
	3.1D, 3.2C, 3.3C, 3.4C, 3.5C, 3.6C, 3.7C	3.1C, 3.8C, 3.1E	3.9C, 3.2E
	4.1D, 4.2C, 4.3C, 4.4C, 4.5C, 4.6C, 4.7C, 4.8C	4.1C, 4.1E	4.9C, 4.10C, 4.11C, 4.2E
	5.1D, 5.2C, 5.3C, 5.4C, 5.5C, 5.6C, 5.7C, 5.8C	5.1C, 5.1E	5.9C, 5.10C, 5.11C, 5.2E
ADV_IMP			1.1D, 1.1C, 1.2C, 1.1E, 1.2E
			2.1D, 2.1C, 2.2C, 2.3C, 2.1E, 2.2E
			3.1D, 3.1C, 3.2C, 3.3C, 3.1E, 3.2E
ADV_INT	1.1C	1.1E	1.1D, 1.2D, 1.2C, 1.3C, 1.2E
		2.1C, 2.1E	2.1D, 2.2D, 2.3D, 2.4D, 2.1C, 2.2C, 2.3C, 2.4C, 2.5C, 2.6C, 2.2E
ADV_LLD	1.1D, 1.1C, 1.2C, 1.3C1.7C, 1.8C	1.9C, 1.1E	1.4C, 1.5C, 1.6C, 1.10C, 1.2E
	2.1D, 2.2C, 2.3C, 2.7C, 2.8C	2.1C, 2.9C, 2.1E	2.4C, 2.5C, 2.6C, 2.10C, 2.2E

ADV_RCR	1.1D, 1.1C, 1.1E		
	2.1D, 2.1C, 2.1E		
	3.1D, 3.1C, 3.2C, 3.3C, 3.1E		
ADV_SPM	1.2D	1.1D, 1.1C, 1.1E	1.2C, 1.3C, 1.4C
	3.2D	3.1D, 3.1C, 3.1E	3.2C, 3.3C, 3.5C, 3.6C
AGD_ADM	1.1D, 1.1C, 1.2C, 1.4C, 1.5C, 1.7C, 1.8C	1.3C, 1.1E	1.6C
AGD_USR	1.1D, 1.1C, 1.2C, 1.4C, 1.5C, 1.6C	1.3C, 1.1E	
ALC_DVS	1.1D, 1.1C, 1.2C, 1.1E	1.2E	
	2.1D, 2.1C, 2.2C, 2.1E	2.2E	
ALC_LCD			1.1D, 1.2D, 1.1C, 1.2C, 1.1E
			2.1D, 2.2D, 2.3D, 2.1C, 2.2C, 2.3C, 2.4C, 2.5C, 2.2E
			3.1D, 3.2D, 3.3D, 3.4D, 3.1C, 3.2C, 3.3C, 3.4C, 3.5C, 3.6C, 3.1E
ALC_TAT			1.1D, 1.2D, 1.1C, 1.2C, 1.3C, 1.1E
			2.1D, 2.2D, 2.3D, 2.1C, 2.2C, 2.3C, 2.1E, 2.2E
			3.2D, 3.3D, 3.1C, 3.2C, 3.3C, 3.4C, 3.1E, 3.2E
ATE_COV	1.1D, 1.1C, 1.1E		
	2.1D, 2.1C, 2.2C, 2.1E		
	3.1D, 3.1C, 3.2C, 3.1E		
ATE_DPT	1.1D, 1.1C, 1.1E		
	2.1D, 2.1C, 2.1E		
	3.1D, 3.1C, 3.1E		
ATE_FUN	1.1D, 1.2D, 1.1C, 1.2C, 1.3C, 1.4C, 1.5C, 1.1E		
	2.1D, 2.2D, 2.1C, 2.2C, 2.3C, 2.4C, 2.5C, 2.1E		
ATE_IND		1.1C, 1.1E	1.1D, 1.2E
		2.1C, 2.1E	2.1D, 2.2E, 2.3E
		3.1C, 3.1E	3.1D, 3.2E, 3.3E
AVA_CCA	1.1D, 1.2D. 1.1C, 1.1E	1.2C, 1.3C, 1.4C, 1.5C, 1.2E, 1.3E	
	2.1D, 2.2D, 2.1C, 1.6C, .2.1E	2.2C, 2.3C, 2.4C, 2.5C, 2.2E, 2.3E	
	3.1D, 3.2D, 3.1C, 3.6C, 3.1E	3.2C, 3.3C, 3.4C, 3.5C, 3.2E, 3.3E	
AVA_MSU	1.1D, 1.2D, 1.1C, 1.2C, 1.3C, 1.4C, 1.1E		1.2E, 1.3E
	2.1D, 2.2D, 2.1C, 2.2C, 2.3C, 2.4C, 2.1E		2.2E, 2.3E, 2.4E
	3.1D, 3.2D, 3.1C, 3.2C, 3.3C, 3.4C, 3.1E		3.2E, 3.3E, 3.4E, 3.5E
AVA_SOF		1.1D, 1.1C, 1.2C, 1.1E, 1.2E	
AVA_VLA	1.1D, 1.2D, 1.1C, 1.1E, 1.2E		
	2.1D, 2.2D, 2.1C, 2.2C, 2.1E, 2.2E, 2.3E, 2.4E, 2.5E		
	3.1D, 3.2D, 3.1C, 3.2C, 3.3C, 3.1E, 3.2E, 3.3E, 3.4E, 3.5E		
	4.1D, 4.2D, 4.1C, 4.2C, 4.3C, 4.4C, 4.1E, 4.2E, 4.3E, 4.4E, 4.5E		
AMA_AMP	1.1D	1.1C, 1.2C, 1.4C, 1.7C, 1.11C, 1.1E	1.3C, 1.5C, 1.6C, 1.8C, .1.9C, 1.10C, 1.2E
AMA_CAP			1.1D, 1.1C, 1.2C, 1.3C, 1.1E, 1.2E
AMA_EVD	1.1D,	1.1C, 1.2C, 1.3C, 1.4C, 1.1E, 1,2E, 1.4E	1.3E, 1.5E
AMA_SIA		1.1D, 1.1C, 1.3C, 1.7C, 1.1E,	1.2C, 1.4C, 1.5C, 1.6C, 1.2E
		2.1D, 2.1C, 2.3C, 2.7C, 2.1E	2.2C, 2.4C, 2.5C, 2.6C, 2.2E

을 비교한 것과 동일한 방법으로 각 프랙티스별로 SSE-CMM의 BP 및 GP와 비교하여 비교 결과를 FULL, PARTIAL, NONE으로 구분한다. 그 결과는 표 9와 같다.

BS7799의 시스템 보안 기능과 관련된 프랙티스들은 CC의 보안 기능 요구사항의 각 엘리먼트들과 비교한다. 그리고 운영 환경과 관련된 프랙티스는 SSE-CMM의 보안 환경을 관리하는 프랙티스에서 참조하여 사용할 수 있도록 한다.

4.1.2 CC 컴포넌트와 BS7799 프랙티스 별로 SSE-CMM 수정

비교 결과에 의하여 대응 정도가 PARTIAL이나

표 9 SSE-CMM과의 대응 정도에 따른 BS7799 보안 프랙티스

	구분	대응 정도	프랙티스 번호
BS 7799 보안 프랙티스	보증	FULL	3.1.1, 3.1.2, 4.1.1, 4.1.2, 4.1.3, 4.1.6, 5.1.1, 5.2.1, 5.2.2, 6.1.1, 6.2.1, 6.3.1, 6.3.2, 6.3.3, 6.3.5, 8.1.1, 8.1.2, 8.1.3, 8.2.1, 8.2.2, 8.6.1, 8.6.2, 8.6.3, 8.6.4, 10.1.1, 10.5.1, 10.5.2, 10.5.3, 10.5.4
		PARTIAL	4.1.4, 4.1.5, 4.1.7, 4.2.1, 4.2.2, 4.3.1, 6.1.2, 6.1.3, 6.1.4, 6.3.4, 8.1.6, 9.3.2, 10.2.1, 12.1.1, 12.1.2, 12.1.3, 12.1.4, 12.1.5, 12.1.6, 12.1.7, 12.2.1, 12.2.2, 12.3.1, 12.3.2
		NONE	8.1.4, 8.1.5, 10.2.2, 10.2.3, 10.4.1, 10.4.2, 10.4.3, 10.5.5, 11.1.1, 11.1.2, 11.1.3, 11.1.4, 11.1.5
	기능	N/A	8.3.1, 8.4.1, 8.4.2, 8.4.3, 8.7.1, 8.7.2, 8.7.3, 8.7.4, 8.7.5, 8.7.6, 8.7.7, 9.1.1, 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.3.1, 9.4.1, 9.4.2, 9.4.3, 9.4.4, 9.4.5, 9.4.6, 9.4.7, 9.4.8, 9.4.9, 9.5.1, 9.5.2, 9.5.3, 9.5.4, 9.5.5, 9.5.6, 9.5.7, 9.5.8, 9.6.1, 9.6.2, 9.7.1, 9.7.2, 9.7.3, 9.8.1, 9.8.2, 10.2.1, 10.2.4, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5
	운영	N/A	7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.1.5, 7.2.1, 7.2.2, 7.2.3, 7.2.4, 7.2.5, 7.2.6, 7.3.1, 7.3.2, 8.5.1

NONE인 CC 컴포넌트와 BS7799 프랙티스의 경우, 관련 SSE-CMM 프랙티스를 대응 정도가 FULL이 될 수 있도록 수정한다.

- 대응 결과가 PARTIAL인 경우: 일부 대응되는 프랙티스를 FULL이 될 수 있도록 수정한다.
- 대응 결과가 NONE인 경우: 관련 있는 프랙티스를 FULL이 될 수 있도록 수정하거나, 관련 있는 프랙티스를 새로이 추가한다.

예를 들어, 대응 결과가 PARTAIL인 경우와 NONE인 경우 SSE-CMM의 해당 프랙티스를 각각 그림 1, 2와 같이 FULL이 되도록 수정하였다. 수정, 추가된 부분은 밑줄로 표시하였고, 나머지 부분은 SSE-CMM의 프

BP.13.02-Identify Configuration Units Uniquely
Identify configuration units that constitute identified baselines uniquely.

Description
A configuration unit is one or more work products that are baselined together... (abbreviated)
It should provide a reference to TOE by label, TOE is only referenced without vagueness.

Example Work Products
- baselined work product configuration
- identified configuration units

Notes
Configuration units in the area of requirements management could vary from individual requirements... (abbreviated)

그림 1 대응 결과가 PARTIAL인 경우 수정된 BP 예

BP.09.03 - Identify Security Alternative
Identify solutions to security related engineering problems.

Description
The purpose of this base practice is to identify alternative solutions to security... (abbreviated)

Example Work Products
security views of system architecture - describe at an abstract level relationships...(abbreviated) using semiformal or formal style depending on requirements.
... (abbreviated)

Notes
The solution alternatives include architecture, design, and implementation solutions... (abbreviated)

그림 2 대응결과가 NONE인 경우 수정된 BP의 예

BP.20.02 Determine Support Requirements

Determine requirements for the organization's systems engineering support environment based on organizational needs.

Description

An organization's needs are primarily determined by assessing competitiveness issues. For example, does the organization's support environment hinder the organization's competitive position? Does each major element of the organization's support environment allow systems engineering to operate with sufficient speed and accuracy?

Example Work Products

• requirements for systems engineering support environment BS7799의 Physical and environmental security, network management 항목을 참조하여 요구사항을 정의한다.

Notes

Determine the organization's needs for computer network performance, improved analysis methods, computer software, and process restructuring.

그림 3 BS7799와의 대응 결과에 따라 수정된 GP 예

랙티스와 동일하다.

BS7799에서 시스템의 운영환경 보안에 해당되는 것으로 분류된 프랙티스들을 보안 환경을 관리하는 SSE-CMM의BP.20.02 - Determine Support Requirements, BP.20.03 - Obtain Systems Engineering Support Environment 프랙티스에서 그림 4와 같이 참조할 수 있도록 한다.

4.2 통합 보안평가 모델, CC_BS7799_SSE-CMM

대응 및 수정 결과로부터 제품, 프로세스, 통제 관점을 통합한 보안평가 모델을 다음과 같이 제안한다. 통합된 보안평가 모델은 앞에 기술하였듯이 SSE-CMM을 CC와 BS7799에 적합하도록 테일러링한 것으로 "CC_BS7799_SSE-CMM"이라고 한다. CC_BS7799_SSE-CMM는 23개 프로세스 영역의 기본 프랙티스와 일반 프랙티스로써 다음과 같이 구성한다.

- Part 1: CC_BS7799_SSE-CMM
  - (1-1) 기본 프랙티스 BP와 일반 프랙티스 GP
  - (1-2) CC 기능 컴포넌트와 BS7799 보안 기능 관련 프랙티스
- Part 2: CC, BS7799와 : CC_BS7799_SSE-CMM의 대응 결과
  - (2-1) CC 보증 컴포넌트 별로 대응되는 CC_BS7799_SSE-CMM의 BP와 GP
  - (2-2) BS7799 보안 프랙티스 별로 대응되는 CC_BS7799_SSE-CMM의 BP와 GP

Part 1의 통합 보안평가 방법론은 4.1.1절의 제품, 프로세스, 통제 요구사항의 상호 비교를 통하여 제품, 통제 요구사항의 대응되지 않는 부분에 따라 프로세스 요구사항의 내용을 4.1.2절과 같이 수정하거나 추가한 형태이다. 따라서 프로세스 평가 기준인 SSE-CMM의 프랙티스의 내용을 대응 정도에 따라 수정하거나 추가한다. 통합 보증 방법론은 수정된 23개의 PA별 기본 프랙티스와 프로세스수행 능력 단계 별 일반 프랙티스로 구성한다.

CC_BS7799_SSE-CMM과 SSE-CMM의 프랙티스와의 관계를 동일, 수정, 추가로 구분한 내용은 표 10, 11과 같다. 관계가 수정과 추가인 경우 그 근거가 되는 기준의 평가 요구사항을 적용하여 기존 SSE-CMM의 프랙티스를 수정하거나 새로운 프랙티스를 추가함을 나타내고, 동일인 경우는 SSE-CMM의 프랙티스와 동일함을 나타낸다.

Part 2는 CC 보증 컴포넌트, BS7799의 보안 프랙티스별로 대응되는 CC_BS7799_SSE-CMM의 기본 프랙티스와 일반 프랙티스를 표 12와 같이 기술한다.

4.3 분석

본 논문에서 제안한 보안보증 모델 CC_BS7799_SSE-CMM은 보안 제품과 조직의 보안 프로세스, 보안 통제 활동을 동시에 평가할 수 있게 하는 평가 모델로써, 보안 평가에서 세 가지 관점을 모두 고려하여야 높은 보안성을 보증할 수 있다는 필요성에 의하여 개발하였다. CC와 SSE-CMM, BS7799의 상호호환성을 토대로 실행 가능한 보안평가 모델을 제안하였다.

보안 보증에 제안한 방법론을 적용하여 세 가지 관점을 함께 평가한다면 3장에서 제시한 단독 평가의 문제

표 10 CC_BS7799_SSE-CMM의 프로세스 영역과 기본 프랙티스

PA	BP	비고(수정 근거)
PA01	BP.01.03, BP.01.04	동일
	BP.01.01, BP.01.02	수정(BS7799)
PA02	BP.02.01, BP.02.02, BP.02.03, BP.02.04, BP.02.05, BP.02.06	동일
PA03	BP.03.01, BP.03.03, BP.03.04, BP.03.05, BP.03.06	동일
	BP.03.02	수정(BS7799)
PA04	BP.04.01, BP.04.02, BP.04.03, BP.04.04, BP.04.05, BP.04.06	동일
PA05	BP.05.01, BP.05.02, BP.05.03, BP.05.04, BP.05.05	동일
PA06	BP.06.01, BP.06.02, BP.06.03, BP.06.04, BP.06.05	동일
PA07	BP.07.01, BP.07.02, BP.07.03, BP.07.04	동일
PA08	BP.08.01, BP.08.02, BP.08.03, BP.08.04, BP.08.05, BP.08.06, BP.08.07	동일
PA09	BP.09.01, BP.09.02, BP.09.04	동일
	BP.09.03, BP.09.05, BP.09.06	수정(CC)
	BP.09.07	추가 (CC)
PA10	BP.10.01, BP.10.04, BP.10.06, BP.10.07	동일
	BP.10.02, BP.10.03	수정(BS7799)
	BP.10.05	수정(CC)
PA11	BP.11.02, BP.11.03, BP.11.05	동일
	BP.11.01, BP.11.04	수정(BS7799
PA12	BP.12.01, BP.12.02. BP.12.03, BP.12.04, BP.12.05, BP.12.06, BP.12.07	동일
PA13	BP.13.01. BP.13.05	동일
	BP.13.02, BP.13.03, BP.13.04	수정(CC)
PA14	BP.14.01, BP.14.02, BP.14.03, BP.14.04, BP.14.05, BP.14.06	동일
PA15	BP.15.01, BP.15.02, BP.15.03, BP.15.04, BP.15.05, BP.15.06	동일
PA16	BP.16.01, BP.16.02, BP.16.03, BP.16.04, BP.16.05, BP.16.06, BP.16.07, BP.16.08, BP.16.09, BP.16.10	동일
PA17	BP.17.01, BP.17.02, BP.17.04	동일
	BP.17.03	수정(BS7799)
PA18	BP.18.03, BP.18.04	동일
	BP.18.01, BP.18.02	수정(BS7799)
PA19	BP.19.01, BP.19.02, BP.19.03, BP.19.04, BP.19.05	동일
PA20	BP.20.01, BP.20.02, BP.20.03, BP.20.04, BP.20.05, BP.20.06, BP.20.07	동일
PA21	BP.21.01, BP.21.03, BP.21.05, BP.21.06, BP.21.07	동일
	BP.21.02, BP.21.04	수정(BS7799)
PA22	BP.22.01, BP.22.02, BP.22.03, BP.22.04, BP.22.05	동일
PA23	BP.23.01	추가(CC)

표 11 CC_BS7799_SSE-CMM의 수행능력 단계와 일반 프랙티스

Capability Level	GP	비고(수정 근거)
1	GP1.1.1	동일
2	GP2.1.1, GP2.1.2, GP2.1.3, GP2.1.4, GP2.1.5, GP2.1.6, GP2.2.1, GP2.2.2, GP2.3.1, GP2.3.2, 2.4.1, GP2.4.2	동일
3	GP3.1.1, GP3.1.2, GP3.2.1, GP3.2.3, GP3.3.1, GP3.3.2, GP3.3.3	동일
	GP3.2.2	수정(BS7799)
4	GP4.1.1, GP4.2.1, GP4.2.2	동일
5	GP5.1.1, GP5.1.2, GP5.2.1, GP5.2.2, GP5.2.3	동일

점을 해결할 수 있다. 이는 그림 4와 같이 3장에서 제시한 문제점 및 사례가 발생 가능했던 이유가 제품 평가만으로는 조직 프로세스의 보안성을 보증하기 어렵고, 프로세스 평가만으로는 생산한 제품 보안성을 보증할 수 없으며, 통제 평가는 운영 관리 과정에 초점을 두어 프로세스와 제품의 보안성을 보증할 수 없다는 점에서 기인했기 때문이다. 3장에서 제시한 문제점 별로 그 부분을 보완할 수 있는 CC_BS7799_SSE-CMM의 평가 요소를 표 13과 같이 나타내었다. 각 문제점이 CC_BS7799_SSE-CMM의 어떤 요구사항으로 해결 될 수

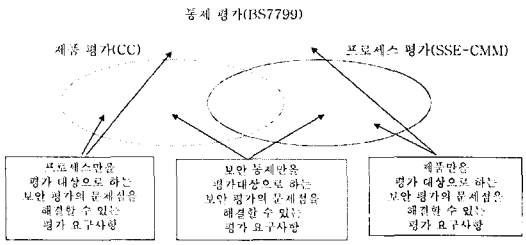

그림 4 CC_BS7799_SSE-CMM의 보안 문제점 해결

표 12 CC 보증 엘리먼트별로 관련된 CC_BS7799_SSE-CMM의 일부

CC 보증 엘리먼트	일치정도	관련 통합 보안 평가 방법론
ACM_AUT.1.1D	FULL	PA13, GP 2.2.2
ACM_AUT.1.2D	FULL	GP 2.1.3 applied to PA13
ACM_AUT.1.1C	FULL	GP 2.1.4 applied to BP.13.04
ACM_AUT.1.2C	FULL	BP.23.01
ACM_AUT.1.3C	FULL	GP 2.2.1 applied to PA13
ACM_AUT.1.4C	FULL	GP 2.2.1 applied to PA13

있는지 확인할 수 있다.

본 논문에서 제안한 CC_BS7799_SSE-CMM은 제품 평가, 프로세스 평가, 통제 평가를 모두 고려해야 한다는 필요성에 의하여CC, SSE-CMM, BS7799의 보안 요구사항을 대응시키고 세 가지 관점의 평가를 동시에 수행할 수 있는 하나의 통합 평가 모델이다.

기존의 비슷한 연구로 AAWG의 연구는 다양한 보증 방법론과 CC를 대응시키고 그 결과를 토대로 보증 방법론과 CC 평가의 상호호환성을 제시하고자 하였다. 그러나 보증 방법론 대응 결과가 완전히 공개되지 않았고, AAP3/SSE-CMM은 보증 방법론과 CC 평가의 상호 호환에만 초점을 맞추고 있는 반면 보안 평가 프로세스 정립 혹은 개선을 직접 반영하고 있지 않다.

조직의 정보 보안 상태를 평가하기 위해서는 시스템을 구성하는 제품뿐만 아니라 조직의 프로세스까지 고려할 필요가 있으므로 CC와 BS7799 평가 결과를 모두 참고하여야 한다는 "An Approach to Combine Process Certification And Product Evaluation" 연구는 제품이 사용될 IT 환경이 유일하다는 이외에 제품과 프로세스를 모두 고려할 필요성을 명확하게 검증하지 못했다. 또한 CC와 BS7799 평가를 효율적으로 수행하기 위한 방안에 대한 연구가 부족하다.

사용자의 필요를 모두 만족시키기 위해 IT 요구사항은 CC를 기준으로 평가하고, non-IT 요구사항은 IT Baseline Protection Manual로 평가하는 연구인 "Meeting User Needs by a Combination of Common Criteria and IT-Baseline Protection"은 보안을 위하여 두 가지 기준을 모두 고려해야 할 필요를 제시하였으나 효율적으로 평가를 수행하는 방안을 제시하지는 못하였다.

보호프로파일의 개발 프로세스에 SSE-CMM의 PA를 대응시킨 P3I 연구는 보호프로파일 개발 프로세스에 해당하는 SSE-CMM의 공정영역을 나열하는 정도에 그칠 뿐 프로세스 성숙도의 지표가 되는 SSE-CMM의 기본 프랙티스에 대해서는 언급하고 있지 않으므로 어떻게 보호프로파일 개발 프로세스가 개선이 될 수 있는지를 알기 어렵다. 또한 보호프로파일의 개발 프로세스에 SSE-CMM의 PA를 적용하여 전체 보안 평가의 개선에 기여하지는 못한다는 단점이 있다.

즉, 기존의 연구들은 CC 기반의 보안 평가를 개선하

표 13 단독 평가 문제점과 CC_BS7799_SSE-CMM의 해결 근거

문제점	문제점을 보완하는 CC_BS7799_SSE CMM의 평가 요구사항
Pd 1	CC_BS7799_SSE-CMM PA 14, 15, 17, 18
Pd 2.1	CC_BS7799_SSE-CMM PA20
Pd 2.2	CC_BS7799_SSE-CMM PA17, 20.21
Pd 2.3	CC_BS7799_SSE-CMM PA21
Pd 2.4	CC_BS7799_SSE-CMM PA20
Pd 2.5	CC_BS7799_SSE-CMM BP.01.01, BP.10.03, PA20
Pd 3	CC_BS7799_SSE-CMM PA20
Pc 1	CC_BS7799_SSE-CMM BP.09.03, BP.09.05, BP.09.06, BP.10.05, BP.13.02, BP.13.03, BP.13.14, BP.17.03
Pc 2.1	CC_BS7799_SSE-CMM BP.09.03, BP09.05
Pc 2.2	CC_BS7799_SSE-CMM BP.09.03, BP.09.05, BP.09.06, BP.10.05, BP.13.02, BP.13.03, BP.13.14, BP.17.03
Pc 2.3	CC_BS7799_SSE-CMM PA 15, PA20
Pc 3	CC_BS7799_SSE CMM BP.09.03, BP.09.05, BP.09.06, BP.10.05, BP.13.02, BP.13.03, BP.13.14, BP.17.03
Ct 1	CC_BS7799_SSE-CMM PA17
Ct 2	CC_BS7799_SSE-CMM PA17
Ct 3	CC_BS7799_SSE CMM BP.09.03, BP.09.05, BP.09.06, BP.10.05, BP.13.02, BP.13.03, BP.13.14, BP.17.03

기 위해 다른 관점의 방법론을 함께 고려하는 방안을 찾았으나 함께 고려해야 하는 실질적인 이유를 제시하지 못하였고, 실제로 보안 평가에서 사용할 수 있는 구체적이고 효율적인 통합된 보안 평가 모델을 제시하지 못하였다. 따라서 본 논문에서는 새로운 평가 모델을 제안하는데 앞서 더 나은 보안 보증을 위해서 다른 관점의 보안 보증 방법론들을 함께 고려해야 할 필요성을 확인하고 구체적인 문제점의 사례를 들었다. 그리고 이러한 필요성에 따라 CC와 SSE-CMM, BS7799의 상호 호환성을 토대로 효율적으로 평가를 수행하기 위한 방안을 개발하고자 하였으며, 그 결과로써 구체적이고 실행 가능한 CC_BS7799_SSE-CMM을 제안하였다.

통합 보안평가 방법론은 다음과 같은 측면에서 활용할 수 있다. CC 기반의 평가를 받았던 조직이 통합 보안 보증을 수행하고자 한다면 CC의 보증 컴포넌트와 대응되는 CC_BS7799_SSE-CMM의 BP와 GP를 참고하여 CC의 EAL에 해당하는 프로세스 영역을 선정할 수 있다. 평가자는 선정한 프로세스 영역을 기반으로 SSE-CMM의 수행능력 단계와 만족시키는 BS7799의 통제 프랙티스를 판단할 수 있다. 이를 통해 더 높은 SSE-CMM 수행능력 단계로 발전하기 위한 경로를 추출할 수 있으며, 인증 받을 BS7799의 통제 영역에서 추가로 수행해야 하는 프랙티스를 확인할 수 있다. 예를 들어 CC EAL3으로 평가를 받았다면, CC EAL3에 해당하는 프로세스 영역으로써 PA01, PA04, PA05, PA08, PA09, PA10, PA11, PA13을 선정할 수 있다. 선정한 프로세스 영역의 평가 결과가 다음 그림 5와 같다면 평가 결과 성숙도 단계가 1로 나온 PA05, PA11 경우 성숙도 단계를 구성하는 일반 프랙티스를 참고하여 성숙도 단계가 2가 되도록 프로세스 개선 계획을 세울 수 있다.

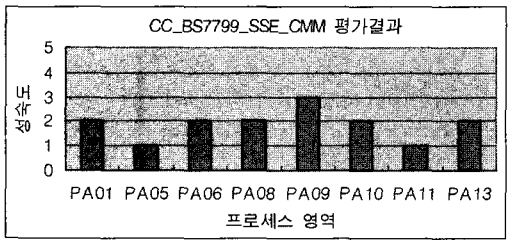

그림 5 CC_BS7799_SSE-CMM 평가 결과의 예

또한 SSE-CMM 기반의 평가를 받았던 조직이 통합 보안평가 방법론을 받아들이고자 하는 경우 CC와 BS7799에 따라 수정, 추가된 CC_BS7799_SSE-CMM의 프랙티스 내용을 참고하여 부족한 영역을 확인하고 CC 평가 혹은 BS7799 인증에 대비할 수 있다.

5. 결 론

정보 보호의 필요성이 커지면서 많은 정보 보호 기준이 제안되어 산업계에 적용되고 있다. 이러한 기존의 방법론들은 크게 프로세스, 제품, 통제 관점으로 분류할 수 있다. 그러나 세 가지 관점의 보안 평가 방법론은 적용 방법, 평가 대상, 단계 등이 상이하므로 그 가운데 어느 하나만을 고려하여서는 정보 보호에 결함이 존재할 수 있으므로 더 나은 보안 보증을 위해 방법론의 통합이 필요하다.

본 논문에서는 한 가지 관점의 방법론만을 고려하여 보안을 평가할 때 발생할 수 있는 문제점과 그 사례를 구체적으로 제시하였다. 이러한 문제점은 제품 단독 평가의 경우 대부분 프로세스 평가를 고려하지 않은 결과이고, 프로세스 단독 평가의 경우 제품 평가를 고려하지 않은 결과이다. 또한 통제 기준의 평가는 보안 시스템 관리에 초점을 두어 전체를 고려하지 못한 결과이다. 따라서 이러한 문제점의 해결방안으로써, CC, SSE-CMM, BS7799의 상호 호환성의 분석을 토대로 효율적인 통합 평가를 수행할 수 있도록 하는 새로운 통합 보안보증 모델인 CC_BS7799_SSE-CMM을 제안하였다. 제안한 모델은 구체적이고도 실행 가능한 프랙티스 들로 구성된다.

또한 제안된 CC_BS7799_SSE-CMM 모델이 앞서 제시한 보안 문제점을 개선할 수 있음을 확인하였다. 그리고 CC 기반의 보안 평가를 받았던 조직이 통합 보안 보증을 수행하고자 하는 경우와 SSE-CMM 기반의 프로세스 평가를 받았던 조직이 통합 보안 보증 방법론을 받아들이고자 하는 경우를 가정하여 제안된 모델의 활용방안을 모색하였다.

본 연구진은 통합방법론의 기본 아이디어 만을 발표[11]하여 인정 받은 바 있다. 이에 더 나아가 본 논문에서의 주요 기여내용은 통합의 필요성을 통합하지 않았을 때의 단독 평가의 문제점을 구체적으로 파악하고, 본 논문에서 제안한 통합 보안보증 모델이 파악한 문제점을 해소할 수 있음을 구체적으로 분석한 데 있다. 향후 통합 보안평가 모델을 실제 보안평가에의 적용연구가 필요하다. 이를 위하여 통합 평가를 수행하고자 하는 개발자 및 관리자, 평가자를 위한 지침을 개발할 예정이다.

참 고 문 헌

[1] TCSEC: Trusted Computer Evaluation Criteria, DOD5200.28STD, 1985.
[2] ITSEC: Information Technology Security Evaluation Criteria, V1.2, 1991.
[3] CC; ISO/IEC 15408 Information Technology -

Security Technology - Evaluation Criteria for IT security V2.1, 1999.
[4] SSE-CMM: System Security Engineering Capability Maturity Model, 1999.
[5] BS7799 - Code of Practice for Information Security Management, British Standards Institute, 1999.
[6] AAWG Task 1 Report - An Alternative Assurance Package to the CC's EAL3 assurance level, draft v0.9, 1997.
[7] ISO/IEC 15443 Information technology - Security techniques - A framework for IT security assurance, 2001.
[8] M.M. Eloff and S.H. von Solms, "Information Security Management: An Approach to Combine Process Certification And Product Evaluation," Computer and Security Journal volume 19, Issue 8, Pages 698-709, 2000.
[9] Markus Mackenbrock, "Meeting User Needs by a Combination of Common Criteria and IT-Baseline Protection," 3rd International Common Criteria Conference, 2002.
[10] Jeffrey R. Williams, Karan M. Ferraiolo, "P3I Protection Profile Process Improvement," 22nd National information System Security Conference, 1999.
[11] Jieun Lee, SungHee Lee, Byoungju Choi, "A CC-based Security Engineering Process Evaluation Model," 27th International Computer Software and Applications Conference (COMPSAC'2003), pp130-135, Dallas USA, 2003.

이 지 은

1997년~2001년 이화여대 수학과 이학사 컴퓨터학과 공학사. 2002년~2004년 이화여대 컴퓨터학과 공학석사. 2003년~현재 LG전자 홈넷사업팀 연구원. 관심분야는 Software Engineering, Testing, Product-line Engineering. Software Quality Assurance, Embedded Software

최 병 주

1979년~1983년 이화여대 수학과 학사 1984년~1985년 Purdue Univ. Computer Science 학사수료. 1986년~1987년 Purdue Univ. Computer Science 석사 1987년~1990년 Purdue Univ. Computer Science 박사. 1991년~1992년 삼성종합기술원. 1992년~1995년 용인대 전산통계학과 조교수 1995년~현재 이화여대 컴퓨터학과 교수. 관심분야는 소프트웨어공학, 소프트웨어 테스트, 소프트웨어 및 데이타 품질 측정