보 안 공 학 연 구 논 문 지
제 2 권, 제 3 호, 2005 년 11 월

# 정보보호시스템 적절성 평가 방법론

최 상 수[1], 김 소 연[2], 이 강 수[1]
[1] 한남대학교 컴퓨터공학과
e-mail : gcss09@se.hannam.ac.kr, gslee@mail.hannam.ac.kr
[2] 충주대학교 BK21 사업단
e-mail : sykim-513@hanmail.net

# Suitability evaluation methodology for information security system

Sang-soo Choi[1], So-yeon Kim[2], Gang-soo Lee[1]
[1]Department of Computer Engineering, Hannam University
[2]Department of Computer Engineering, Chungju National University

요 약

We can regard an application information system as an IT security system. Most application information system is constructed by integrating a set of IT security products with out the suitability analysis. In this paper, we research and develop the suitability analysis methodology by applying Mis-usecase model. Our results are to be used for the purposed of the certification and accreditation of IT security product or information system in a organization.

## 1. 서론

정보통신 인프라의 발달과 더불어 정보보호에 대한 인식 또한 급속히 증가하고 있다. 따라서, 각급 조직에서 운영하고 있는 정보시스템은 각종 정보보호제품들을 도입 (또는 엔지니어링)하여 정보보호시스템을 구축 및 운영하고 있다.
그러나, 기존의 각급 조직들은 정보보호시스템을 구축하기 위하여 네트워크 보안의 강화를 목적으로 유명한 보안제품 회사의 네트워크 보안장비 (예컨대, 침입탐지시스템 또는 침입차단시스템)를 도입하여 주먹구구식으로 구축하고 있다. 즉, 체계적으로 해당 조직에서 필요로 하는 보안요구사항이 무엇인지, 그리고 도입하려는 정보보호제품이 해당 보안요구사항을 충족시킬 수 있는지 여부를 평가하지 않고 있다. 이는 과도한 정보보호제품의 도입으로 인한 보안기능의 중복, 불필요한 예산의 낭비뿐만 아니라 조직의 정보보호시스템 전체의 보안성을 저하시키는 요인이 되고 있다.

이러한 문제를 인식한 선진 각국에서는 정보보호시스템을 위한 평가 및 인가 기준들을 제정하고 시행하고 있으며, 국내의 경우 2004 년부터 "보안성 검토제도"를 제정하고 이에 대한 활발한 연구를 진행중에 있다.

따라서, 본 논문에서는 도입하고자 하는 정보보호제품이 해당 조직의 정보보호시스템 환경에 적합한지 여부를 "적절성(suitability)"이라 정의하며, 이를 평가하기 위한 "적절성 평가 방법론"을 제시한다. 특히, 특히, 각급 조직에서 도입하고자 하는 정보보호제품들은 이미 활발하게 수행중인 국제공통평가기준 (CC: Common Criteria) [1-3]으로 평가 받은 제품들이다. 따라서, 제시한 방법론에서는 CC 평가체계와의 호환성을 고려하여 중복성 문제를 고려하였으며, 선진 각국에서 운영중인 유사 제도를 참고하였다. 제시된 방법론을 통하여 정보보호제품을 도입 및 정보보호시스템을 구축하면, 보안공학적으로 (즉, 비용효과적) 조직의 보안수준을 제고할 수 있을 것으로 기대된다.

본 논문의 2 장에서는 정보보호시스템을 평가하고 인가하기 위한 기준 및 체계들을 소개한다. 3 장에서는 적절성 평가 방법론의 요구사항 분석 및 설계 결과와 이를 구현한 모델을 보이며, 끝으로 4 장에서 결론을 맺는다.

* 본 논문은 산업자원부 지역협력연구사업 (R12-2003-004-01001-0) 지원으로 수행되었음.

## 2. 관련연구

### 2.1 정보보호시스템 평가 방법

정보보호시스템을 평가 및 인가하기 위하여 선진 각국에서는 다양한 제도와 기준들을 수립하여 시행하고 있다. 특히, 시스템 측면에서의 평가 및 인가 방법들을 정리하면 다음과 같다.

(1) 운영시스템 평가[4, 5]

평가대상물 (TOE)은 제품과 시스템으로 구분하며, 시스템은 "운영" 시스템을 의미한다. 즉, 운영시스템은 "설치"된 특정 제품이라 할 수 있다. 따라서, 운영시스템은 "동적"이며, 설치 및 운영환경을 모두 포함한다.

따라서, IT 적 보안기능(또는 통제, 대책) 뿐 아니라, 절차적, 관리적, 인사적, 비 IT 적 통제를 포함하며, 제품 평가보다 어렵다(환경을 고려하여야 함). 특히, 위험분석/평가/관리 및 보안관리 부분도 평가하도록 명시하고 있다.

운영시스템 평가를 위한 기준은 2004 년 12 월 현재 ISO/IEC TR 19791-2(2004.12)를 따른다. 그러나, 구체적인 평가방법에 대한 설명이 부족하며 보증별 평가방법이 존재하지 않는다.

(2) 정보시스템 인증 및 인가(C&A) 제도[6-9]

선진 각국에서는 기관의 정보시스템을 일정수준 이상의 보안성을 가지도록 입법화하고 있다 (예컨대, 미국의 FISMA : Federal Information Security Management Act, = Title III of the E-Government Act, Public Law 107-347). 특히, 이 제도는 각 기관의 응용정보시스템에 대한 평가 및 인가를 위한 제도로써, 보안관리 수준의 평가 및 위험분석/관리도 포함하고 있다. 따라서, 평가경험이 있는 3 명이 6 개월 정도 소요된다고 알려져 있다.

정보시스템 인증 및 인가 제도를 위한 평가기준으로는 ISO/IEC 13335, NIST SP 800-37, NIST SP 800-53 등이 있다. 특히, 평가체계는 민간용과 국가기관용을 구분하여 시행하고 있다(국방부 - DITSCAP : Defense Information Technology Systems Certification and Accreditation Process, DoDI 5200.40 (향후 DIACAP 으로 변경 예정), 국방부를 제외한 미연방기관 - NIACAP : National Information Assurance Certification and Accreditation Process, OMB Circular A-130).

### 2.2 보안요구사항 분석 및 명세 모델

소프트웨어공학 분야에서는 소프트웨어 시스템에 대한 분석 및 명세를 위한 다양한 연구가 진행되어 왔으며, 대표적으로 UML 과 같은 모델 기반의 요구분석 공학 이론들이 체계적으로 수행되어 왔다. 특히, UML 의 UC(Use Case)는 대표적인 요구사항 분석 모델로써 개발자 및 분석자들 사이에 널리 사용되고 있다. 그러나, UC 는 기능요구사항을 반영하기에는 매우 우수하지만, 비기능요구사항이라 할 수 있는 보안요구사항의 분석 및 명세에는 매우 취약하며, 이를 해결하기 위하여 기존의 UC 를 확장한 MUC 모델이 제시되었으며, 이에 대한 활발한 연구들이 진행중이다[10].

(1) Sindre&Opdahl 의 MUC 모델[11]

Sindre&Opdahl 은 시스템이 허용해서는 안되는 기능이라 하더라도 여전히 기능에 해당하며 이것은 잠재적으로 UC 에 의하여 다루어질 수 있다고 분석하였으며, 비기능 요구사항 중에서 보안요구사항에 초점을 맞추어 UC 를 확장한 MUC 모델을 제안하였다. 제안된 MUC 모델은 UC, MUC 와 Actor, Mis-Actor 로 구성되며, 이들 사이에는 prevents 및 detects 의 두 가지 관계를 추가 제시하였다. 특히, MUC 와 전통적인 UC 를 표현하기 위해서는 UC 와 MUC 를 동시에 표현하는 방법을 제시하였으며, 전통적인 UC 에 대한 템플릿을 확장하여 명백하고 단순한 경로를 작성하는데 도움을 주기 위하여 MUC 를 위한 템플릿 아이템 (name, summary 등 19 항목)과 템플릿을 제시하였다.

(2) Alexander 의 MUC 모델[12]

Alexander 는 그의 연구에서 사람 또는 조직이 추구하는 목표를 달성하기 위한 행위들의 순서에 해당하는 시나리오 개념을 확장하여 조직에 있어서 발생하지 않기를 원하는 목표의 시나리오 또는 악의자가 원하는 목표의 시나리오라 할 수 있는 부정적인 시나리오를 도출하기 위하여 MUC 를 제안하였다. 특히, 위협 및 대응책이 플레이 및 대응플레이의 균형화된 지그재그 패턴을 띈다는 게임이론의 MiniMax 이론을 적용하여 MUC 를 통해 UC (즉, 시스템 기능)의 Best Move (서브시스템 기능 즉, 보안요구사항의 도출)는 분석된 MUC 에 대응하는 것으로써 보안요구사항을 도출하는 방법을 보였다. 이러한 MUC 모델을 표현하기 위하여 threatens 과 mitigates 관계를 추가 제시하였으며, 자동화 도구인 시나리오 플러스 (Scenario Plus)를 제시하였다.

(3) McDermott 의 AUC 모델[13]

McDermott 는 그의 연구에서 기존의 수학적 보안모델의 문제점을 인식하고 보안에 대한 전문지식 없이도 간단하게 보안요구사항을 분석할 수 있도록 UC 모델을 확장한 AUC (abuse case) 모델을 제시하였다. AUC 란 시스템과 하나 또는 그 이상의 행위자들 사이에서 시스템 혹은 Actor 에게 해로운 결과를 초래하는 상호작용의 유형에 대한 명세라 정의된다. AUC 모델을 표현하기 위하여 Actor 에 3 가지 속성 (자원, 기술, 목표)을 부여하였으며, 6 단계 (사전 모델링, 행위자 식별, AUC 파악, AUC 정의, granularity 검사, 완전성 및 최소성 검사)의 모델링 프로세스를 제시하였다. 또한, SFTA (soft-ware fault tree analysis) 및 SFA (survivable network analysis), 침투시험 기법들을 응용하고 AUC 모델을 확장하여 보증 프로세스를 제시하였다.

(4) Firesmith 의 SUC 모델[14]

Firesmith 는 그의 연구에서 기존의 연구들의 문제점 즉, MUC 모델 및 AUC 모델은 UC 를 이용하여 실제 보안요구사항 대신에 불필요한 보안 메커니즘에 대하여 명세하고 있다는 문제점을 해결하기 위하여 SUC (security use case) 모델을 제시하였다. 즉, 보안요구사항이란 보호되어야 할 자산(또는 서비스)과 이러한 자산이 보호해야 하는 보안 위협에 대한 분석을 기초로 하여 도출되어야 한다. 따라서, 기존의 연구들은 보안 메커니즘에 초점을 두고 있으나 상대적으로 보안위협 및 보안요구사항에 대해서는 분석 및 명세 방법이 미비하다고 지적하였다. 특히, MUC 는 보안 위협 분석 및 명세를 위한 모델이라 할 수 있으며, 이러한 MUC 모델을 다시 확장하여 분석된 보안위협을 막기 위한 보안요구사항을 분석하기 위하여 접근통제, 무결성 및 프라이버시 등의 UC 를 사례로 하여 분석용 템플리트와 분석 가이드라인을 제시하였다.

그러나, Firesmith 가 그의 논문에서 지적한 것과 같이 기존의 MUC 기반의 보안요구사항 분석 및 명세 모델은 실제적인 보안요구사항 보다는 보안위협이나 보안 메커니즘에 대한 분석을 위한 방법이라 할 수 있으며, 구체적으로 보안위협 또는 보안위협에 대응하기 위한 보안요구사항, 그리고, 보안요구사항을 구현하기 위한 보안기능요구사항(보안메커니즘)의 분석 및 명세 방법에 대해서는 언급하지 않고 있다.

## 3. 적절성 평가 방법론

본 논문에서는 특정 조직의 정보보호시스템을 구축하기 위하여 도입하려는 정보보호제품이 해당 조직의 보안환경에 적합한 것인지를 평가하는 것을 "적절성 평가"로 정의한다. 즉, 이것은 기존의 정보보호 평가 체계에서 일반적으로 사용되던 표준 적합성 (conformance) 평가 (또는, 시험)와는 차이가 있다.

즉, 본 논문에서는 적절성 여부를 평가하기 위하여 해당 조직의 보안환경을 분석 및 명세한 보안요구사항명세서를 작성하고 이를 기준으로 CC 평가된 정보보호제품 (예컨대, EAL3+로 평가된 침입차단시스템) 도입시 정보보호제품의 보안요구사항 명세서라 할 수 있는 보안목표명세서를 크로스 체킹하여 적절성 여부를 평가한다. 특히, 이러한 작업을 도식화하여 분석 및 명세가 용이하도록 기존의 MUC 모델을 적용하였다.

### 3.1 방법론의 요구사항 분석

(1) 문제 정의

적절성 평가 문제는 다음과 같이 정의할 수 있다. 즉, CC 로 평가된 정보보호제품을 특정 조직에서 도입하고자 할 경우, 해당 조직에 "적합"한지 여부의 평가가 필요하다. 따라서, 최소의 비용, 기간 및 인원을 투입하여 정확한 평가결과를 도출할 수 있는 "적절성 평가 방법론"이 요구된다. 특히, 기존의 CC 기반 정보보호제품 평가 업무와의 중복성을 없애야 한다.

또한, CC 평가제도를 준수하여 용어 및 평가기준과 모순이 없어야 하며, CC 기반의 운영시스템 평가기준(ISO/IEC TR 19791) 및 기타 관련 제도(ISMS 및 C&A 등)와도 연동이 가능하여야 한다.

(2) 기능요구사항

적절성 평가 방법론이 제공하여야 하는 기능은 다음과 같다.

- 조직의 보안요구사항 분석 및 명세 기능 : 특정 조직의 실제 보안환경을 분석하여 CC 기반의 용어 및 컨텐츠를 사용하는 정보보호시스템을 위한 보안요구사항을 분석 및 명세할 수 있어야 한다.
- 보안환경 검토 기능 : 분석 및 명세된 조직의 정보보호시스템을 위한 보안요구사항명세서와 CC 평가된 특정 정보보호제품의 보안요구사항명세서라 할 수 있는 보안목표명세서 사이의 보안환경을 검토할 수 있는 기능을 제공하여야 한다.
- 기능/보증 검토 기능 : 조직의 보안요구사항명세서와 정보보호제품의 보안목표명세서 사이의 보안기능 및 보안보증을 검토할 수 있는 기능을 제공하여야 한다.
- 세부 단위시험 기능 : 보안환경 및 기능/보증 검토 이외에 보다 정교한 시험이 요구될 경우 이를 지원하기 위한 세부 단위시험 기능을 제공하여야 한다.

(3) 성능요구사항

적절성 평가 방법론이 제공하여야 하는 성능은 다음과 같다.

- 최소의 비용, 시간 및 인력으로 평가 실시
- 평가 방법론을 지원하기 위한 도구 제공
- 기타 방법론에서 필요한 성능을 제공

### 3.2 방법론의 설계

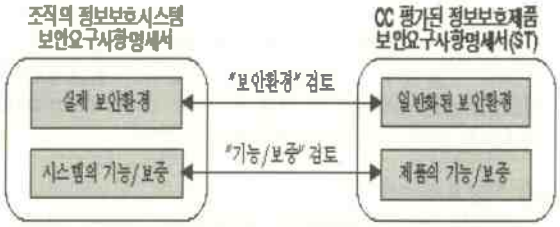
(1) 방법론의 개념설계

3.1 절에서 분석된 적절성 평가 방법론을 위한 요구사항들을 토대로 하여 방법론의 전체 개념을 도식화하면 (그림 1)과 같다. 즉, 적절성 평가를 위하여 "보안환경 검토"와 "기능/보증 검토"의 개념을 이용할 수 있다.

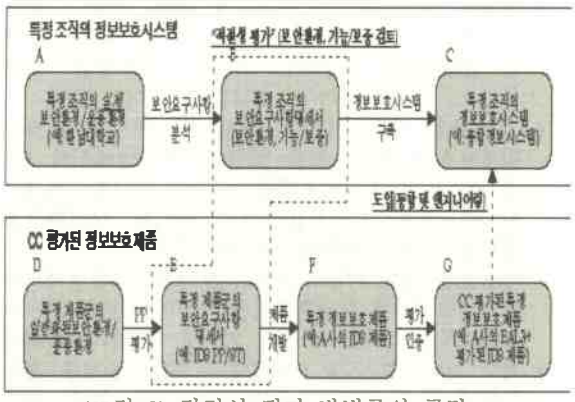
(2) 방법론의 개념 및 정의

(그림 1)의 개념 설계 결과를 확장한 적절성 평가 방법론의 골격은 (그림 2)와 같으며, 제시한 적절성 평가 방법론에 대한 정의는 다음과 같다.

- 정보보호시스템 확인 (validation) : A=B=C 인가?
- 정보보호시스템 검증 (verification) : B=C 인가?
- 정보보호제품 PP 평가 : D=E 인가?
- 정보보호제품 평가 (검증) : E=F 인가?
- 적절성 평가 : (b⊆e) 인가? (이미 E=F, b∈B, e∈E 이다)
- 개발물 측면: C ⊆ (g1∪g2∪gn) (제품은 모든 요구사항을 수용(커버)해야 함)




(그림 1) 적절성 평가 방법론의 개념 설계




(그림 2) 적절성 평가 방법론의 골격

- 요구사항 측면: B⊆(e1∪e2∪en) (제품은 모든 요구사항을 수용해야 함)
- (g1∩g2∩gn)≠ pi (제품의 보안기능간 중복허용)

따라서 적절성 평가는 다음과 같이 정의할 수 있다.

**For all b∈B, determine whether (b ⊆ e ) or not, where e is a product.**

즉, 특정 정보보호시스템의 실제 보안요구사항 명세서상의 '일부분'이 인증된 정보보호제품의 보안요구사항명세서와 같은지를 결정한다. 다시 말하면, 정보보호제품의 개발시 일반화된(가정된) 보안환경이 실제의 보안환경을 포함하는지를 파악하는 것이다. 위의 정의에서 (b⊆e)의 의미는 다음과 같다.

- e 의 보안기능은 b 의 보안기능을 포함
- b 의 보증수준보다는 e 의 보증수준이 높음
- e 의 보안환경은 b 의 보안환경을 포함

만일 (b⊆e)라면, e 라는 인증된 정보보호제품(예: A 사의 IDS 제품)는 특정 정보보호시스템(예: 한남대학교 종합정보시스템)내의 일부분(예: IDS 보안기능그룹)인 b 에 적합하다. 즉, 종합정보시스템을 구축할 때, IDS 솔루션을 위해 A 사의 IDS 제품을 사용해도 된다.

(3) 적절성 평가를 위한 업무

본 논문에서 제시한 적절성 평가 방법론을 위한 업무 목록은 다음과 같다.

- e 의 보안기능은 b 의 보안기능을 포함하는지 "체크" 또는 "기능시험" : 정보보호제품의 ST (즉, e) 및 평가보고서와 정보보호시스템의 ST (즉, b)를 크로스 체크한다. 필요시 기능이 달성되는지에 대하여 단위 기능시험을 수행할 수 있다.
- b 의 보증수준보다는 e 의 보증수준이 높은지 "체크" : 정보보호제품의 ST (즉, e)와 정보보호시스템의 ST(즉, b)를 크로스 체크한다.
- e 의 보안환경은 b 의 보안환경을 포함 : 정보보호제품의 ST (즉, e)와 정보보호시스템의 ST (즉, b)의 보안환경 부분을 크로스 체크한다.

(4) 적절성 평가를 위한 가정사항

본 논문에서 제시한 적절성 평가 방법론을 적용하기 위한 가정사항은 다음과 같다.

- 정보보호제품을 도입하여 활용하고자 하는 특정 조직은 자신의 보안요구사항을 분석하고 명세한 "보안요구사항명세서"를 개발하여 보유하고 있다.
- 특히, 보안요구사항명세서는 해당 조직의 실제 환경과 보안요구사항을 올바르게 기술하고 있다.

### 3.3 방법론의 구현 모델

본 논문에서 제시한 적절성 평가 방법론을 이용하여 준정형적으로 분석 및 명세, 평가할 수 있는 구현 모델로써 MUC 모델을 적용하였다.

특히, 본 연구팀은 조직의 보안요구사항을 준정형적으로 분석 및 명세하기 위하여 UC 모델을 확장한 MUC 모델과 개발 지원도구를 제시한 바 있다[15,16]. 따라서, 본 논문에서는 기존의 연구결과를 적절성 평가를 지원할 수 있도록 보완 및 확장하였다.

(1) MUC 모델의 정의

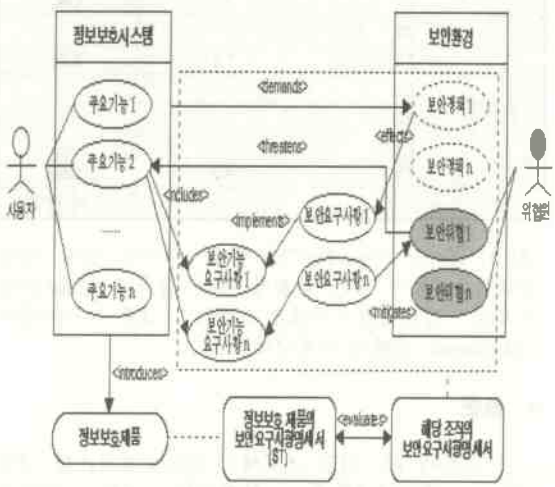
특정 조직의 보안요구사항을 분석 및 명세하고, 이를 토대로 적절성 평가를 수행하기 위하여 기존의 UC 와 MUC 모델의 정의를 확장하여 (그림 3)과 같이 확장된 MUC 모델을 정의한다.

- Actor : 특정 조직의 정보보호시스템 사용자들이 해당 시스템 자산과 상호작용시 수행할 수 있는 사용자들의 역할의 집합 (즉, 시스템 사용자)이다.
- Mis-Actor : 특수한 형태의 Actor 로써 MUC 를 발생시키는 행위자 (즉, 위협원)로써, Actor 의 반전된(음영처리) 형태로 표시한다.
- UC (use case) : 정보보호시스템 자산의 소유자가 제공하기를 원하는 행위에 대한 설명 (즉, 기능요구사항) 또는, 분석된 보안위협을 완화시키기 위한 보안요구사항을 구현하는데 필요한 행위에 대한 설명(즉, 보안기능요구사항)이다.
- MUC (misuse case) : 정보보호시스템 자산의 소유자가 발생하기를 원하지 않는 행위에 대한 설명 (즉, 보안위협)으로써, UC 의 반전된 (음영처리) 형태로 표시한다.
- PUC (security-policy use case) : 특정 조직에서 운영중인 보안관련 정책에 대한 설명 (즉, 보안정책)으로써, UC 의 테두리를 점선으로 표시한다.

- SUC (security use case) : 정보보호시스템 자산의 소유자가 분석된 보안위협을 완화시키기 위하여 필요로 하는 행위에 대한 설명(즉, 보안요구사항/보안목적)으로써, UC 의 테두리를 진한 선으로 처리하여 표시한다.
- SPC (security product case) : 정보보호시스템 자산에 대하여 분석된 보안위협을 완화시키기 위하여 필요한 보안기능 요구사항들을 제품화 (즉, 해당 조직에서 정보보호시스템 구축을 위하여 도입하고자 하는 정보보호제품) 한 것으로써, 끝이 둥근 반원형 사각형으로 표시한다.

또한, 제시한 확장된 MUC 모델의 7 가지 구성요소 사이에 발생할 수 있는 관계는 다음과 같다.

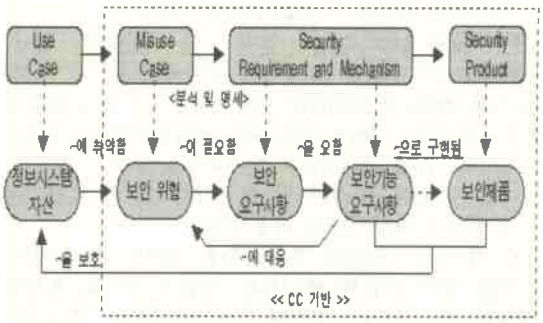
- threatens : 해당 UC(특히, 기능요구사항)는 해당 MUC 로부터 위협을 받음을 의미한다.
- demands : 해당 PUC 는 조직의 정보보호시스템 자산을 구축 및 운영하기 위한 보안관련 정책들에 의하여 요구되어짐을 의미한다.
- mitigates : 해당 SUC 는 해당 MUC 를 완화시킴을 의미한다.
- effects : 해당 SUC 는 조직의 보안정책에 영향을 받았음을 의미한다.
- implements : 해당 SUC 는 해당 UC (특히, 보안기능요구사항) 로 구현될 수 있음을 의미한다.
- includes : 해당 UC(특히, 기능요구사항) 또는 시스템 자산은 해당 UC(특히, 보안기능요구사항)를 포함할 수 있음을 의미한다.
- introduces : 해당 정보보호시스템은 해당 SPC 를 도입 및 통합 (또는, 엔지니어링)함으로써 보안요구사항을 충족시킬 수 있음을 의미한다.
- evaluates : 해당 SPC 를 도입할 것인지 여부를 평가 (즉, 적절성 평가) 하기 위하여 조직의 보안요구사항 명세서와 SPC 의 ST 를 기준으로 적절성 평가를 수행함을 의미한다.




(그림 3) MUC 기반의 적절성 평가 모델

(2) MUC 기반의 적절성 평가 프로세스

본 절에서는 제시한 적절성 평가 방법론과 이의 구현모델인 MUC 모델을 적용한 적절성 평가 프로세스를 제시한다. 특히, 본 논문에서는 도입하고자 하는 정보보호제품을 CC 평가된 제품이라 가정하며, 따라서 전체 프로세스 동안에 사용되는 용어 등을 모두 CC 기반으로 표준화하여 사용하였다. 이를 위하여, (그림 4)와 같이 CC 의 보안요구사항 분석 개념을 MUC 에 적용하였다.




(그림 4) MUC 모델에 적용한 CC 의 보안요구사항 분석 개념

다음은 특정 조직에서 보안요구사항명세서를 작성하고 이를 토대로 특정 정보보호제품을 도입하고자 할 경우, 이에 대한 적절성 평가를 수행하는 프로세스를 보인다. 그러나, 기본적인 보안요구사항 도출 과정은 본 연구팀의 기존 연구논문에서 상세히 설명한 관계로 간략한 설명만을 제시한다.

가. 단계 1 : UC 모델링

첫 번째 단계에서는, 정보보호시스템 자산에 대하여 전통적인 방법으로 UC 모델링을 수행한다.

나. 단계 2 : MUC/PUC 모델링

두 번째 단계에서는, 분석된 정보보호시스템 자산 및 주요기능에 대하여 MUC 모델링을 수행한다. 이때, Mis-Actor 는 해당 정보보호시스템 자산 자체 및 주요 기능에 대한 위협원 (threat agent)에 해당하며, MUC 는 위협원에 의해 발생 가능한 위협이 된다. 분석된 보안위협과 정보보호시스템 자산 또는 주요 기능 사이에는 <threatens> 관계가 적용된다.

또한, 해당 조직에서 운영중인 보안관련 정책들이 요구하는 PUC 모델링을 수행한다. 분석된 보안정책과 정보보호시스템 자산 사이에는 <demands> 관계가 적용된다.

다. 단계 3 : SUC 모델링

세 번째 단계에서는, 두 번째 단계의 MUC 모델링을 통해 분석된 각각의 보안위협을 완화시키기 위한 SUC 모델링을 수행한다. SUC 는 기능요구사항이 아닌

순수한 보안요구사항이라 할 수 있으며, CC 에서의 보안목적에 대응된다. 분석된 SUC 와 MUC 사이에는 <mitigates> 관계가 적용된다.

또한, 이전 단계의 PUC 모델링을 통해 분석된 각각의 보안정책에 따라 이를 지원하기 위한 SUC 모델링을 수행한다. 분석된 SUC 와 PUC 사이에는 <effects> 관계가 적용된다.

라. 단계 4 : UC 모델링

네 번째 단계에서는, 세 번째 단계에서의 SUC 모델링을 통해 분석된 각각의 보안요구사항 (즉, 보안목적)을 구현하기 위한 UC (즉, 보안기능요구사항 또는 보안메커니즘)을 분석 및 모델링 한다. 보안기능요구사항도 단순히 보안메커니즘을 기술 (예컨대, RSA 암호화)하면 개발자 및 분석자들 사이에 혼동 (분석자는 RSA 암호화를 제시하였다 하더라도, 구현상에 DES 암호화가 더 비용효과적일 경우)을 야기할 수 있다. 따라서, 본 연구팀은 CC 의 보안기능 및 보안보증 요구사항을 이용하였다.

CC 의 보안기능/보증 요구사항을 제시함으로써 얻는 이점은 앞서 언급한 분석자와 개발자 사이의 혼동을 제거할 수 있다는 점이다. 즉, 분석자는 추상적인 보안기능요구사항을 제시하고 개발자는 개발환경에 적합한 구체적인 구현 알고리즘을 채택하여 해당 보안기능요구사항을 충족시킬 수 있기 때문이다.

분석된 보안기능요구사항과 보안요구사항 (즉, 보안목적) 사이에는 <implements> 관계가 적용되며, 정보보호시스템 개발 단계라면 시스템의 기능요구사항과 보안기능요구사항 사이에는 <includes> 관계가 적용된다.

마. 단계 5 : 적절성 평가

다섯 번째 단계에서는, 정보보호시스템 개발 단계가 아닌 특정 정보보호제품의 도입시에 조직의 보안요구사항명세서와 도입하고자 하는 제품의 보안요구사항명세서 사이의 <evaluates> 관계를 분석하는 단계이다.

특히, 조직의 보안요구사항명세서는 첫 번째 단계에서 네 번째 단계를 거쳐 분석 및 명세된 내용들을 토대로 CC 평가환경에서의 PP/ST 의 목차를 준수하여 작성하게 된다. 또한, 도입하고자 하는 정보보호제품의 보안요구사항명세서는 CC 평가시에 TOE 와 함께 평가된 ST 라 할 수 있다. 따라서, 3.2 절의 (3)에서 제시한 것과 같이 보안기능/보증수준/보안환경 검토를 수행한다.

- 기능 검토 : [표 1]과 같이 정보보호시스템의 보안요구사항명세서와 도입하고자 하는 정보보호제품의 보안요구사항명세서 (ST)에 각각 명세된 보안기능요구사항들을 크로스 체킹한다. 예컨대, 정보보호제품 A 의 제공 기능들이 일정수준 (예컨대, 80%) 시스템의 필요 기능들과 부합된다면 "Pass" 판정을 내릴 수 있다.

[표 1] 기능 적절성 평가 사례

| 한남대학교 종합정보시스템의 보안기능요구사항 | X 사의 정보보호제품 A 의 보안기능요구사항 | 기능 적절성 평가 결과 |
|---|---|---|
| FAU_GEN.2 | FAU_GEN.2 | OK |
| FAU_SAA.1 | | |
| FCS_CKM.2 | FCS_CKM.1 | OK |
| FDP_ACC.1 | | |
| FDP_ACF.1 | FDP_ACF.1 | OK |
| FDP_SDI.1 | | |
| FDP_ETC.2 | | |
| FDP_IFC.1 | FDP_IFC.1 | OK |
| FDP_IFF.1 | | |
| FPT_TDC.1 | FPT_TDC.1 | OK |
| FPT_TST.1 | | |
| FTA_MCS.2 | | |
| FTA_TSE.1 | FTA_TSE.1 | OK |
| FTP_TRP.1 | FTP_TRP.1 | OK |
| | | 전체: OK |

- 보증 검토 : 보증수준 적절성 검토는 정보보호시스템 보안요구사항명세서 내에 정의된 보증수준과 도입하고자 하는 정보보호제품의 CC 평가된 보증수준을 비교한다. 특히, 시스템의 보증수준보다 제품의 보증수준이 크거나 같아야 한다.
- 보안환경 검토 : 보안환경 적절성 검토도 기능 검토와 유사한 방법으로 수행한다. 보안환경 적절성 검토 사례는 [표 2]에서 보인다.

[표 2] 보안환경 적절성 평가 사례

| | 한남대학교 종합정보시스템의 보안환경 | X 사의 정보보호제품 A 의 보안환경 | 보안환경 적절성 평가 결과 |
|---|---|---|---|
| 정책 | P1 | P1 | OK |
| | P2 | | |
| | P3 | P2 | OK |
| | P4 | | |
| 위협 | T1 | T1 | OK |
| | T2 | | |
| | T3 | | |
| | T4 | | |
| | T5 | T2 | OK |
| | | | 전체 : OK |

평가 결과는 "Pass/Fail"의 형태가 되며, 만약 해당 정보보호제품에 대한 적절성 평가 결과가 "Pass"라면 조직의 정보보호시스템과 해당 제품 사이에는 <introduces> 관계가 적용된다.

## 4. 결론

본 논문에서는 각급 조직에서 정보보호시스템 구축 (또는, 엔지니어링)을 목적으로 CC 평가된 정보보호제품을 도입하고자 할 때, 적절성 평가를

수행하기 위한 방법론과 구현모델을 제시하였다. 특히, 해당 정보보호제품이 특정 조직의 정보보호시스템에 적합한지 여부를 평가하기 위하여 조직의 보안요구사항명세서와 정보보호제품의 보안요구사항 명세서 (ST)의 일치 여부를 확인함으로써 달성할 수 있다. 이를 위해서는 조직의 보안요구사항을 CC 체계상의 용어나 구조로 작성하여야 한다. 따라서, 본 논문에서는 조직의 보안요구사항을 CC 체계와 호환되도록 분석 및 명세할 수 있는 MUC 모델을 제시하였으며, 이를 토대로 적절성 평가 (특히, 기능/보증/환경 검토를 수행)를 수행하는 프로세스를 제시하였다.

본 논문에서 제시한 방법론과 구현모델은 각급 조직의 정보보호시스템 구축 및 정보보호제품 도입시에 활용할 수 있다. 이를 토대로 보다 체계적이고 보안공학적으로 해당 정보보호제품의 도입 여부를 결정할 수 있으며, 따라서 각급 조직의 정보보호수준도 제고될 수 있을 것으로 기대된다.

그러나, 적절성 평가는 다수의 인력과 시간 및 비용을 소요하기 때문에 이를 지원하기 위한 자동화 도구가 요구된다. 또한, 적절성 평가를 위한 세부적인 단위 기능시험이 요구될 수 있으며 이를 위해서는 CC 의 보증패키지와 유사한 형태의 시험 패키지가 요구된다. 따라서, 이에 대한 연구를 향후 연구과제로 남긴다.

## 참고문헌

[1] CC, Common Criteria for Information Technology Security Evaluation, Version 2.1, CCIMB-99-031, August 1999, http://www.commoncriteria.org/ site_index.html.

[2] CC, Common Evaluation Methodology, Version 1.0, CEM-99/045, August 1999, http://www.commoncriteria.org/site_index.html.

[3] CCRA(Arrangement on the Recognition of Common Criteria Certificates) http://www.commoncriteria.org.

[4] ISO/IEC 19791, "Information technology - Security techniques - Security assessment of operational systems," 2004. 12.

[5] 일본전자정보기술협회, "An Enhanced ISO/IEC 15408 Standard for System Security Specification and Evaluation," v1.1, 2004. 12.

[6] DITSCAP : DoD 5200.40, "Defense Information Systems Certification and Accreditation regulation," 1997.

[7] NIACAP, "National Security Telecommunications and Information System Security Instruction," 2000.

[8] DIACAP, "The Defense Information Assurance Certification and Accreditation Process," 2002.

[9] NIST SP 800-37, "Risk Management & Certification and Accreditation Tasks," 2004.

[10] S. Lilly, "Use Case Pitfalls : Top 10 Problems from Real Projects Using Use Cases," Proc. TOOLS-USA'99, pp.174-183, 1-5, Aug 1999.

[11] G. Sindre, A. L. Opdahl, "Capturing Security Requirements through Misuse Cases," Proc. 14th Norwegian Infor-matics Conference(NIK'2001), Tromsø, Norway, pp.26-28, Nov, 2001.

[12] I. Alexander, "Misuse Cases - Use Cases with Hostile Intent," IEEE Software, 20, 1 (January-February 2003), pp.58-66.

[13] J. McDermott, "Eliciting Security Requirements by Misuse Cases," Proc. 37th Technology of Object-Oriented Languages and Systems(TOOLS-37 Pacific 2000), Sydney, Australia, pp.120-131, 20-23, Nov 2000.

[14] Donald G. Firesmith, Security Use Cases, Journal of Object Technology (JOT), 2(3), Swiss Federal Institute of Technology (ETH), Zurich, Switzer-land, pp.53-64, May/June 2003.

[15] 최상수, 이강수 외 2 인, "Misuse Case 모델을 이용한 CC 기반의 보안요구사항 분석 및 명세 방법론," 한국정보보호학회 논문지, 14 권 3 호, pp.85-100, 2004 년 6 월.

[16] Sang-soo Choi, Soo-young Chae, and Gang-soo Lee, "SRS-Tool: A Security Functional Requirement Specification Development Tool for Application Information System of Organization," Lecture Notes in Computer Science(LNCS), Vol. 3081, Part2, pp.458-467, May. 2005.

## 저자소개

최 상 수 (Sang-Soo Choi)
2001 년 : 한남대학교 컴퓨터공학과 학사
2003 년 : 한남대학교 대학원 컴퓨터공학과 석사
2003 년 ~ 현재 : 한남대학교 대학원 컴퓨터공학과 박사과정
<관심분야> 소프트웨어공학, 웹공학, 보안공학, 정보보호 컨설팅 및 위험분석

김 소 연 (So-Yeon Kim)
1989 년 : 한남대학교 컴퓨터공학과 학사
1991 년 : 한남대학교 대학원 컴퓨터공학과 석사
2000 년 : 한남대학교 대학원 컴퓨터공학과 박사
2000 년~현재 : 충주대학교 BK21 사업 교수
<관심분야> 소프트웨어 모델링, 병행시스템 모델링, 정보보호 시스템 모델링

이 강 수 (Gang-Soo Lee)
1981 년 : 홍익대학교 전자계산학과 학사
1983 년 : 서울대학교 대학원 전산학과 석사
1989 년 : 서울대학교 대학원 전산학과 박사
1985 년 ~ 1987 년 : 국립한밭대학교 전자계산학과 전임강사
1992 년 ~ 1993 년 : 미국일리노이대학교 객원교수
1995 년 : 한국전자통신연구원 초빙연구원
1998 년 ~ 1999 년 : 한남대학교 멀티미디어학부장
1987 년 ~ 현재 : 한남대학교 컴퓨터공학과 정교수
<관심분야> 소프트웨어공학, 병행시스템 모델링 및 분석, 보안공학, 정보보호시스템 평가, 멀티미디어교육 커리큘럼