情報保護學會論文誌
第14券 第3號, 2004. 6

Misuse Case 모델을 이용한 CC기반의 보안요구사항 분석 및 명세 방법론

최 상 수,[a)†] 장 세 진,[a)‡] 최 명 길,[b)] 이 강 수[a)]
한남대학교,[a)] 국가보안기술연구소[b)]

A Methodology for CC-based Security Requirements Analysis and Specification by using Misuse Case Model

Sang-Soo Choi,[a)†] Se-Jin Jang,[a)‡] Myung-Gil Choi,[b)] Gang-Soo Lee[a)]
Hannam University,[a)] National Security Research Institute[b)]

요 약

모든 정보시스템은 보안기능이 강화된 정보보호시스템이라 할 수 있으며, 정보보호시스템의 품질을 높이기 위해서는 초기 요구사항 분석 단계에서 보안요구사항을 정형적이며 일관적으로 분석 및 명세하여야 한다. 본 논문에서는 UML의 Use Case 모델을 확장한 Misuse Case 모델을 이용하여 보안요구사항을 분석 및 명세하는 모델과 프로세스를 제시하였으며, 도출된 보안기능요구사항들을 제품화한 비용효과적인 보안제품 선정 알고리즘을 제시하였다. 제시한 모델 및 프로세스를 통해 개발된 정보보호시스템의 품질을 제고할 수 있을 것이다.

ABSTRACT

All information system is information security system that enforced security function. To improve quality of information security system, security requirement analysis and specification must be performed by consistently and typically at early requirement analysis step. In this paper, we propose a security requirements analysis and specification model and process by using Misuse Case Model that extends UML's Use Case Model. And, we propose a cost-effective security product selection algorithm that security product is sufficient of all constructed security functional requirements. It may raise quality of information security system that developed through proposed model and process.

Keywords : *Security Requirement, Misuse Case Model, Common Criteria*

Ⅰ. 서 론

정보화사회에서 보안 및 프라이버시 문제와 같은 정보화의 역기능 문제는 필연적이며, 정보보호기술은 정보화의 역기능을 예방, 방지, 발견 및 복구하기 위한 종합기술이다. 특히, 모든 정보시스템은 보안기능이 강화된 정보보호시스템이라 할 수 있으며, 종합적인 정보보호기술들을 포함하여 개발되고 있다. 또한, 정보보호시스템 평가를 위하여 국가마다 서로 상이한 평가기준들을 연동시키고 평가결과를 상호인증하기 위해 사실상의 표준이라 할 수 있는 CC(Common Criteria, ISO/IEC 15408)가 제정되어 운영되고 있으며, 이를 통해 정보보호시스템의 품질을 평가 및

접수일 : 2004년 3월 3일 ; 채택일 : 2004년 6월 2일
* 본 연구는 2004년도 국가보안기술연구소의 연구비지원으로 수행된 결과의 일부임.
† 주저자, gcss09@se.hannam.ac.kr
‡ 교신저자, sjjang@se.hannam.ac.kr

공인하고 있다[1~5]. 그러나, 정보보호시스템의 분석 및 구현을 위한 연구들은 매우 미비한 실정이다.

보안요구사항(security requirements)이란 비기능요구사항(non-functional requirements)으로써 보호되어야 할 자산 및 서비스와, 이러한 자산 및 서비스가 보호해야 하는 보안 위협에 대한 분석을 기초로 하여 분석된 보안 위협을 완화시키기 위한 보안관련 요구사항들을 말한다. 전통적인 정보시스템 개발자들은 보안요구사항을 분석하기 위하여 보안관련 전문지식이 요구되기 때문에, 실제 정보보호시스템 개발시 설계 및 구현 단계에서만 보안관련 요구사항들을 반영하고 있는 실정이다. 따라서, 높은 품질의 정보보호시스템을 개발하기 위해서는 개발 초기의 요구사항 분석 단계에서 보안요구사항을 정형적이며 일관적으로 분석 및 명세하여야 한다.

또한, 전통적인 요구사항 분석 모델인 UML (unified modeling language)의 UC(use case) 모델은 기능요구사항의 분석 및 명세에는 매우 강력하지만 보안요구사항과 같은 비기능요구사항의 분석 및 명세에는 적합하지 않다[6~8]. 따라서, 전통적인 요구사항 분석 및 명세를 위한 UC 모델을 확장하여 보안요구사항을 분석 및 명세하기 위한 모델에 대한 연구가 활발하게 진행되고 있다[9~17]. 그러나, 기존의 MUC(misuse case) 모델로 대표되는 보안요구사항 분석 및 명세 모델들은 보안위협의 분석 및 명세에 초점을 맞추고 있으며, 보안위협과 보안요구사항, 보안기능요구사항(보안메커니즘)에 대한 명확한 근거를 제시하지 못하고 있다. 또한, 각각의 컨텐츠에 대한 정형적이며 일관적인 명세 방법에 대한 연구도 미흡한 실정이다.

이러한 배경에서, 본 논문에서는 전통적인 요구사항 분석 및 명세 모델인 UML의 UC 모델을 확장하여 보안요구사항을 분석 및 명세하는 모델과 프로세스를 제시하며, 컨텐츠의 정형성 및 일관성을 제시하고 이들간의 관계에 대한 명확한 근거를 제시하기 위하여 정보보호시스템 평가·인증을 위한 국제표준인 CC를 분석하여 보안위협, 보안요구사항, 보안기능요구사항의 명세방법을 제시한다. 또한, 정보보호시스템 재구성(유지보수) 단계에서 분석 및 명세된 보안기능요구사항을 제품화한 보안제품군을 비용효과적으로 선정할 수 있는 알고리즘을 제시한다. 본 논문에서 제시한 모델 및 프로세스와 컨텐츠를 이용함으로써, 초기 개발단계 및 재구성 단계에서 정보보호시스템의 보안성을 제고할 수 있을 것이다.

본 논문의 2장에서는 CC기반의 정보보호시스템의 기본개념과 기존의 UC를 확장한 보안요구사항 분석 및 명세 모델들을 소개하고, 3장에서는 UC 모델을 확장한 MUC 기반의 보안요구사항 분석 및 명세 모델과 프로세스를 제시한다. 4장에서는 기존의 연구결과와의 차이를 제시하며 5장에서 결론을 맺는다.

Ⅱ. 관련연구

2.1 CC의 기본 개념 및 요구사항 분석과정

CC는 그림 1과 같이 모든 정보보호시스템에서 필요로 하는 보안기능요구사항의 전체집합을 클래스-패밀리-컴포넌트-엘리먼트를 통해 계층적으로 분류되어 있다. 또한, 보안기능에 대하여 구현의 정확성에 대한 보증요구사항의 전체집합을 계층적으로 분류하였고 7단계의 보증수준별로 요구하는 보증요구사항(컴포넌트)을 정의하고 있다. 상위의 보증수준은 하위의 보증수준보다 완전하고, 엄격하며 정형적이므로, 보증수준간에는 완전성, 엄격성 및 정형성관계를 갖는다[2,3].

정보보호시스템(TOE : target of evaluation, 평가대상물)의 제품유형에 따라 CC 보안기능요구사항의 일부를 선택하고 7수준의 보안수준 중 하나를 택하여 PP(protection profile) 또는 ST(security target)를 구성한다.

PP는 제품유형별 공통보안요구사항명세서이며 특정한 제품유형의 운영에 대한 보안환경(가정사항, 보안위협, 보안정책), 보안목적, 보안요구사항(보안기능요구사항 및 보안보증요구사항)으로 구성된다. 보안요구사항에서의 보안기능은 CC의 보안기능요구사항집합의 부분집합이며, 보안보증은 보안보증요구사항집합의 부분집합이다. 일반적으로 PP는 사용자(PP 개발자)가 원하는 요구사항을 포함하여 개발하며 별도의 PP평가와 인증이 요구된다.

ST는 특정한 정보보호제품(즉, 평가대상물, TOE)의 보안요구사항명세서이다. 해당 제품유형의 PP가 존재할 경우, 기존의 PP에 개발환경을 부가하여 사용할 수 있으며 이 경우 "PP 준수선언"이 필요하다. ST는 TOE의 보안요구사항명세서에 해당하므로, ST도 TOE와 함께 평가 및 인증한다.

또한, CC에서는 요구사항의 분석과정을 그림 2와 같이 제시하고 있다. 즉, 보호되어야 할 자산에 대하여 보안환경을 분석하고 이를 통해 보안목적(즉, 보

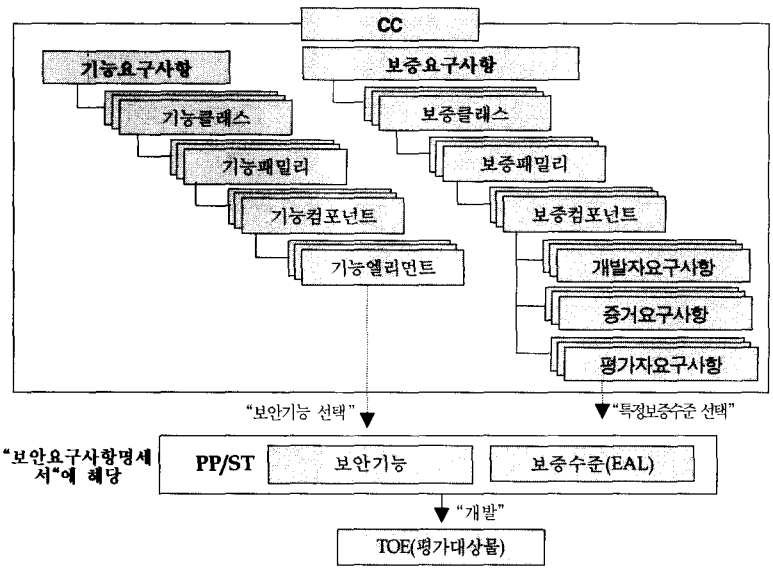

그림 1. CC의 구성과 사용의 개념

안요구사항)을 분석하며, 해당 보안목적을 실현하기 위한 보안기능요구사항 및 보안보증요구사항들을 분석하게 된다[2,3].

2.2 Misuse Case 모델

소프트웨어공학 분야에서는 소프트웨어 시스템에 대한 분석 및 명세를 위한 다양한 연구가 진행되어 왔으며, 대표적으로 UML과 같은 모델 기반의 요구분석 공학 이론들이 체계적으로 수행되어 왔다. 특히, UML의 UC는 대표적인 요구사항 분석 모델로써 개발자 및 분석자들 사이에 널리 사용되고 있다. 그러나, UC는 기능요구사항을 반영하기에는 매우 우수하지만, 비기능요구사항이라 할 수 있는 보안요구사항의 분석 및 명세에는 매우 취약하며[8], 이를 해결하기 위하여 기존의 UC를 확장한 MUC 모델이 제시되었으며, 이에 대한 활발한 연구들이 진행중이다[9~17].

(1) Sindre&Opdahl의 MUC 모델

Sindre&Opdahl[9~10]은 시스템이 허용해서는 안되는 기능이라 하더라도 여전히 기능에 해당하며 이것은 잠재적으로 UC에 의하여 다루어질 수 있다고 분석하였으며, 비기능 요구사항 중에서 보안요구사항에 초점을 맞추어 UC를 확장한 MUC 모델을 제안하였다. UC를 확장한 MUC의 기본 개념은 다

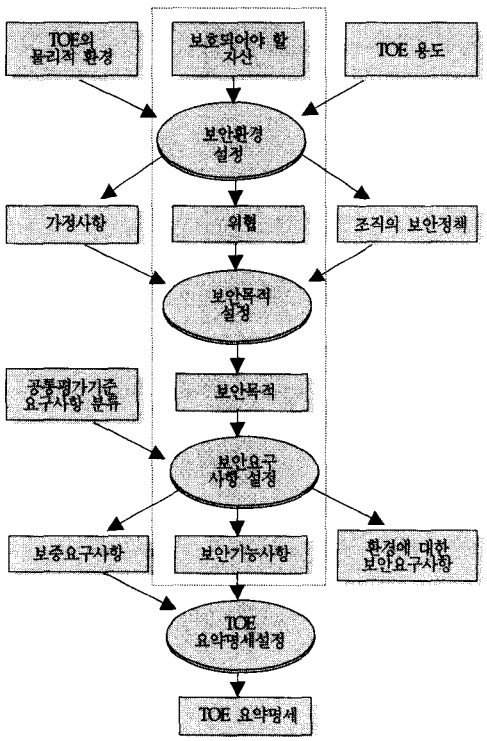

그림 2. CC의 요구사항 분석과정

음과 같다.

- UC : UC는 시스템/엔티티 소유자가 제공하기를 원하는 행위에 대하여 설명

- MUC(UC 확장) : 특수한 형태의 UC로써, 시스템/엔티티 소유자가 발생하길 원하지 않는 행위에 대하여 설명
- Actor : 엔티티의 사용자들이 해당 엔티티와 상호작용시 수행할 수 있는 사용자들의 역할 집합
- Mis-Actor : 특수한 형태의 행위자로써, MUC를 발생시키는 행위자

여기서, MUC와 Mis-Actor는 반전된 형태로 표현하며, MUC 모델 표현을 위해 다음과 같은 두 가지 관계(relation)를 추가 제시하였다.

- prevents : 해당 기능이 MUC 활성화를 방지함
- detects : 해당 기능이 MUC 활성화를 탐지함

또한, MUC와 전통적인 UC를 표현하기 위해서는 ① 표준 다이어그램을 그대로 이용하거나, ② UC와 MUC를 분리하여 표현, 또는 ③ UC와 MUC를 동시에 표현하는 세 가지 방법이 존재하며, Sindre& Opdahl은 ③번째 표현방법을 제시하였으며, 전통적인 UC에 대한 템플릿을 확장하여 명백하고 단순한 경로를 작성하는데 도움을 주기 위하여 MUC를 위한 템플릿 아이템(name, summary 등 19항목)과 템플릿을 제시하였다.

(2) Alexander의 MUC 모델

Alexander[11~13]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 시나리오(negative scenario)를 도출하기 위하여 MUC를 제안하였다. 특히, 위협 및 대응책이 플레이 및 대응플레이의 균형화된 지그재그(balanced zigzag) 패턴을 띈다는 게임이론의 MiniMax 이론을 적용하여 MUC를 통해 UC(즉, 시스템 기능)의 Best Move(서브시스템 기능 즉, 보안요구사항의 도출)는 분석된 MUC에 대응하는 것으로써 보안요구사항을 도출하는 방법을 보였다. 이러한 MUC 모델을 표현하기 위하여 다음과 같은 두 가지 관계를 추가 제시하였다.

- threatens : 해당 기능이 MUC로부터 위협을 받음
- mitigates : 해당 보안기능이 MUC를 완화시킴

또한, 세 가지 관점 즉, 직접적인 충돌(direct conflict), 위협/완화 사이클, 완화/악화를 통한 간접적인 충돌(indirect conflict)에 대하여 분석을 수행하였으며, 자동화된 도구인 Scenario Plus를 제시하였다.

(3) McDermott의 AUC 모델

McDermott[14~16]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. AUC란 시스템과 하나 또는 그 이상의 행위자들 사이에서 시스템 혹은 Actor에게 해로운 결과를 초래하는 상호작용의 유형에 대한 명세라 정의된다. AUC 모델을 표현하기 위하여 Actor에 3가지 속성(자원, 기술, 목표)을 부여하였으며, 6단계(사전 모델링, 행위자 식별, AUC 파악, AUC 정의, granularity 검사, 완전성 및 최소성 검사)의 모델링 프로세스를 제시하였다. 또한, SFTA(software fault tree analysis) 및 SFA(survivable network analysis), 침투시험 기법들을 응용하고 AUC 모델을 확장하여 보증 프로세스를 제시하였다.

(4) Firesmith의 SUC 모델

Firesmith[17]는 그의 연구에서 기존의 연구들의 문제점 즉, MUC 모델 및 AUC 모델은 UC를 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, MUC는 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 UC를 사례로 하여 분석용 템플리트와 분석 가이드라인을 제시하였다.

그러나, Firesmith가 그의 논문에서 지적한 것

과 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.

따라서, 본 논문에서는 MUC 모델과 SUC 모델을 확장하여 실제적인 보안요구사항과 이를 구현할 수 있는 보안기능요구사항을 도출할 수 있는 모델 및 프로세스를 제시한다.

Ⅲ. 보안요구사항 분석 및 명세 모델

본 장에서는 정보시스템에 대한 보안 위협을 분석하고 해당 위협에 대응하기 위한 보안요구사항 그리고, 보안요구사항을 구현하기 위한 보안기능요구사항을 분석 및 명세 방법을 제시하기 위하여 기발표된 MUC 모델을 확장한 모델을 제시한다.

3.1 MUC 모델의 정의

본 논문에서는 보안요구사항의 분석 및 명세를 위하여 기존의 UC와 MUC 모델의 정의를 확장하여 다음과 같이 확장된 MUC 모델을 정의한다.

- Actor : 정보시스템 자산의 사용자들이 해당 정보시스템 자산과 상호작용시 수행할 수 있는 사용자들의 역할의 집합(즉, 정보시스템 사용자)이다.
- Mis-Actor : 특수한 형태의 Actor로써 MUC를 발생시키는 행위자(즉, 위협원)로써, Actor의 반전된(음영처리) 형태로 표시한다.
- UC(use case) : 정보시스템 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) : 정보시스템 자산의 소유자가 발생하기를 원하지 않는 행위에 대한 설명(즉, 보안위협)으로써, UC의 반전된(음영처리) 형태로 표시한다.
- SUC(security use case) : 정보시스템 자산의 소유자가 분석된 보안위협을 완화시키기 위하여 필요로 하는 행위에 대한 설명(즉, 보안요구사항)으로써, UC의 테두리를 진한 선으로 처리하여 표시한다.
- SPC(security product case) : 정보시스템 자산에 대하여 분석된 보안위협을 완화시키기 위하여 필요한 보안기능 요구사항들을 제품화(즉, 보안제품 또는 정보보호제품)한 것으로써, 끝이 둥근 사각형으로 표시한다.

또한, 제시한 확장된 MUC 모델의 6가지 구성요소 사이에 발생할 수 있는 관계는 다음과 같다.

- threatens : 해당 UC(특히, 기능요구사항)는 해당 MUC로부터 위협을 받음을 의미한다.

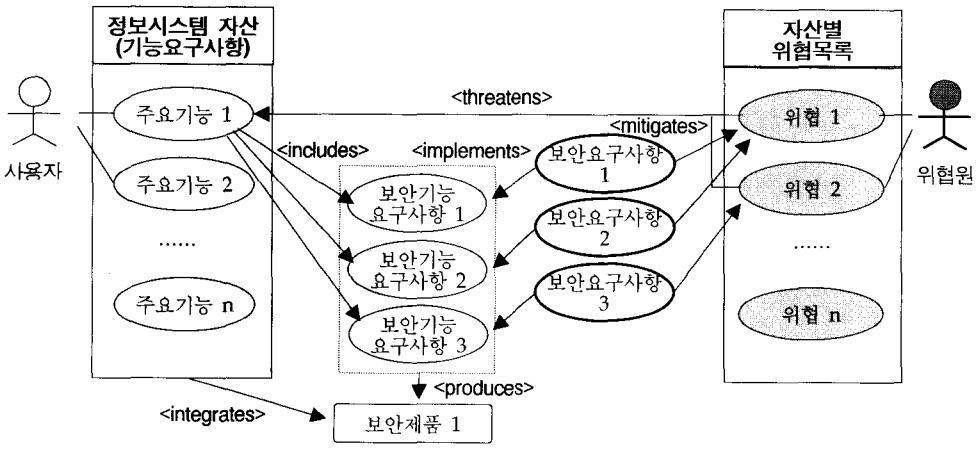

그림 3. MUC 기반의 보안요구사항 분석 및 명세 모델

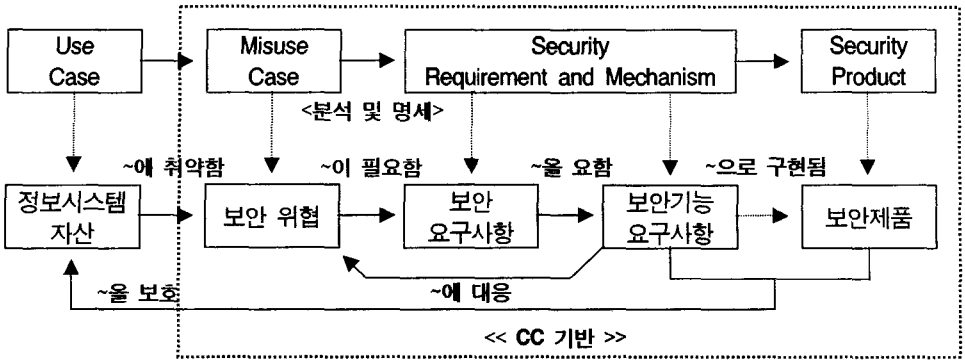

그림 4. CC의 개념을 MUC 모델에 적용한 보안요구사항 분석 및 명세 프로세스

- mitigates : 해당 SUC는 해당 MUC를 완화시킴을 의미한다.
- implements : 해당 SUC는 해당 UC(특히, 보안기능요구사항)로 구현될 수 있음을 의미한다.
- includes : 해당 UC(특히, 기능요구사항) 또는 정보시스템 자산은 해당 UC(특히, 보안기능요구사항)를 포함할 수 있음을 의미한다. 이 경우는, 정보시스템 개발 단계에서 적용할 수 있는 방법이다.
- produces : 해당 UC(특히, 보안기능요구사항)의 집합은 해당 SPC로 제품화 될 수 있음을 의미한다. 즉, 해당 보안기능요구사항들이 포함된 보안제품을 제시하는 방법이다.
- integrates : 해당 정보시스템은 해당 SPC를 통합함으로써 보안요구사항을 충족시킬 수 있음을 의미한다. 이 경우는, 정보시스템 재구성 단계에서 적용할 수 있는 방법이다.

본 논문에서 제시하는 MUC 기반의 보안요구사항 분석 및 명세 모델을 도식화하면 다음 그림 3과 같다.

3.2 CC 기반의 보안요구사항 분석 및 명세 프로세스

본 절에서는 3.1절에서 제시한 MUC 모델과 2.1절에서 설명한 CC의 요구사항 분석과정을 적용하여 MUC 모델을 이용한 CC기반의 보안요구사항 분석 및 명세 프로세스를 제시한다.

CC의 요구사항 및 명세 유도과정을 MUC에 적용한 결과를 도식화하면 그림 4와 같다.

그림 4의 프로세스를 기준으로 보안요구사항을 분석 및 명세하는 단계는 다음과 같다.

(1) 1단계 : UC 모델링

첫 번째 단계에서는, 정보시스템 자산에 대하여

표 1. 종합정보시스템에 대한 Use Case 시나리오 분석 예

정보시스템 자산			자산의 주요기능	주 사용자
주요자산명	자산구분	세부정보		
종합정보시스템	하드웨어	Solaris Server	시스템 로그인	학생, 교수
			금학기 성적조회	학생
			전체학기 성적조회	학생
	소프트웨어	Solaris OS Oracle DB	학사일정 조회	학생
			학점포기 신청	학생
			학점포기 과목조회	학생
	데이터	사용자 정보 과목 데이터 성적 데이터	성적 입력	교수
			성적 정정	교수
			성적표 출력	교수
	...	...	...	...

전통적인 방법으로 UC 모델링을 수행한다. 이때, 정보시스템 개발 단계일수도 있으며, 또는 재구성 단계일 수도 있다. 대학교의 종합정보시스템을 예로 하여 1단계 모델링을 수행한 예는 표 1 및 그림 5와 같다.

(2) 2단계 : MUC 모델링

두 번째 단계에서는, 분석된 정보시스템 자산 및 정보시스템의 주요기능에 대하여 MUC 모델링을 수행한다. 이때, Mis-Actor는 해당 정보시스템 자산 자체 및 정보시스템의 주요 기능에 대한 위협원(threat agent)에 해당하며, MUC는 위협원에 의해 발생 가능한 위협이 된다. 그러나, 위협원과 위협은 체계적인 분류에 대한 연구가 매우 미흡하여 분석 및 명세시에 개발자 및 분석자들 사이에 혼동을 야기할 수 있다.

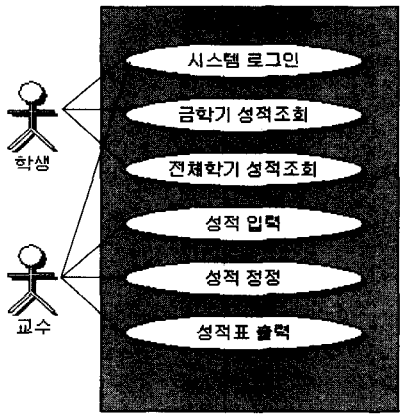

그림 5. 1단계 UC 모델링 예

따라서, 본 연구팀의 이전 연구결과인 정보보호제품 평가·인증 체계의 국제표준이라 할 수 있는 CC를 기반으로 하는 위협문장 생성모델을 적용한다[18]. 즉, 본 연구팀이 제시한 위협문장 생성모델은 CC와 PP/ST 작성가이드[19], CCToolBox/PKB[20], 2003년 6월 기준으로 CC 홈페이지를 통해 공개된 33종의 PP[21]와 67종의 ST[22]들을 분석하여 체계적이며 정형적으로 개발된 모델이며, 그림 6과 같다.

따라서, 그림 6의 위협문장 생성모델에 따라 MUC 모델링 단계에서는 7가지 Mis-Actor와 해당되는 목적 및 동기, 공격방법과 영향을 분석하여 MUC(즉, 위협문장)를 생성한다. 본 위협문장 생성모델을 이용하면 7×4×4×5×4=2240개의 위협문장을 생성할 수 있으며, 분석된 위협문장과 정보시스템 자산 또는 기능요구사항 사이에는 〈threatens〉 관계가 적용된다.

그림 5의 1단계 모델링 결과를 이용하여 2단계 모델링을 수행한 예는 그림 7과 같다.

(3) 3단계 : SUC 모델링

세 번째 단계에서는, 두 번째 단계의 MUC 모델링을 통해 분석된 각각의 위협을 완화시키기 위한 SUC 모델링을 수행한다. SUC는 기능요구사항이 아닌 순수한 보안요구사항이라 할 수 있다. 그러나, MUC와 마찬가지로 보안요구사항에 대한 체계적인 분류 및 명세방법에 대한 연구가 매우 미흡하며, 분석 및 명세시에 개발자 및 분석자들 사이에 혼동을 야기할 수 있다.

따라서, 본 연구팀은 CC의 보안목적 개념을 보안요구사항으로 채택하였다. CC에서는 보안목적을 다음과 같이 정의하고 있다.

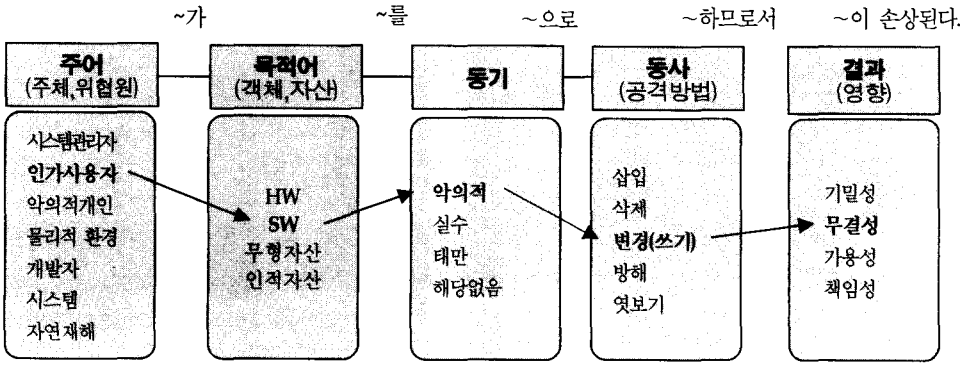

그림 6. CC 기반의 위협문장 생성모델

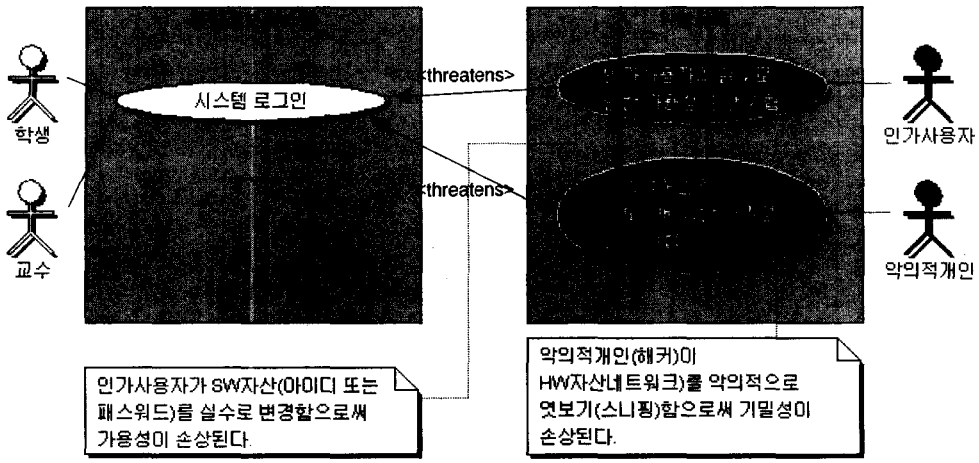

그림 7. 2단계 MUC 모델링 예

보안목적(security objective) : 식별된 위협에 대응하거나 식별된 조직의 보안정책과 가정을 만족시키기 위한 의도를 서술하는 것

즉, 보안목적이란 분석된 위협에 대응하기 위한 보안요구사항이라 할 수 있다. 따라서, 본 논문에서는 PP 및 ST 작성을 지원하기 위하여 개발된 CCToolBox/PKB에서 제공하는 미리 정의된 보안목적 문장들을 확장하여 보안요구사항으로 제안한다. CCToolBox/PKB의 미리 정의된 보안목적 문장들을 보안요구사항으로 사용하면 보안기능요구사항을 CC의 보안기능요구사항으로의 도출이 용이하며, 위협으로부터 보안목적 도출을 위하여 CCToolBox/PKB의 보안목적 분석방법을 적용할 수 있다는 장점을 갖는다. 즉, 본 연구팀이 제시한 위협문장의 위협원과 공격방법 및 영향을 CCToolBox/PKB의 미리 정의된 공격문장과 매핑하면 그림 8과 같이 간단하게 보안목적을 도출할 수 있다.

또한, 분석된 위협문장과 보안요구사항 사이에는 〈mitigates〉 관계가 적용되며, 그림 7의 2단계 모델링 결과를 이용하여 3단계 모델링을 수행한 예는 그림 9와 같다.

(4) 4단계 : UC 모델링

네 번째 단계에서는, 세 번째 단계에서의 SUC 모델링을 통해 분석된 각각의 보안목적을 구현하기 위한 UC 즉, 보안기능요구사항 또는 보안메커니즘을 분석 및 모델링한다. 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 CC를 기준으로 하여, 세 번째 단계에서 분석된 PKB 보안목적을 구현하기 위한 CC의 보안기능요구사항을 제시한다. CCToolBox/PKB의 미리 정의된 보안목적 목록은 CC의 보안기능요구사항과의 관계를 제시하고 있으며, 이를 통하여 국제표준에 해당하는 보안기능요구사항을 그림 10과 같이 간단하게 도출할 수 있다.

CC의 보안기능요구사항을 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, 정보시스템 개발 단계라면 정보시스템의 기능요구사항과 보안기능요구사항 사이에는 〈includes〉 관계가 적용된다.

그림 9의 3단계 모델링 결과를 이용하여 4단계 모델링을 수행한 예는 그림 11과 같다.

(5) 5단계 : SPC 모델링

다섯 번째 단계에서는, 정보시스템 개발 단계가

Misuse Case (위협문장)	악의적개인(해커)이 HW자산(네트워크)을 악의적으로 엿보기(스니핑)함으로써 기밀성이 손상된다.	
위협관련 PKB 공격문장	A36. Hack_CommEaves_Eman : 통신 메커니즘이 자료를 방사 ※ 선택여부 : ×	
	설명	외부인이 통신선로로부터의 방사를 캡쳐링하기 위해 특수장비를 사용
	선택지침	본 공격에 관련된 것은 통신매체에 의한 방사의 정보에 직접 비례한다. 본 공격은 의도적인 방사가 있는 방송통신 기술에 대해 고유한 것이다. 외부인이 특수장비를 이용해 마이크로웨이브 전송을 가로채거나 무선 전송을 방송할 때가 본 공격의 예이다.
	보안목적 (대응책)	O38. 자료교환 기밀성의 강화
	A37. Hack_CommEaves_Intrc : 외부인이 사용자 통신을 가로챔 ※ 선택여부 : ○	
	설명	수신자가 아닌 외부인이 사용자 자료 통신을 가로챔
	선택지침	예컨대, 외부인은 원격시스템에 스니핑 장치를 설치할 수 있음. 외부인은 본 공격을 위해 원격시스템에 대한 특권이 필요할 수 있음. 그러나, 원격시스템 내의 통제를 완화하는 것은 이 제한을 우회할 수 있게함.
	보안목적 (대응책)	O38. 자료교환 기밀성의 강화
	A38. Hack_CommEaves_Tap : 외부인이 통신 선로를 태핑 ※ 선택여부 : ○	
	설명	외부인이 통신 선로를 물리적으로 태핑하기 위한 장비를 사용
	선택지침	본 공격에 관련된 것은 통신선로가 제한을 안한 위협원에 노출되어 있을때임. 외부인은 상대적으로 능숙하고 본 공격을 위한 본질적인 자원을 가져야함. 어떤 통신 선로는 본 공격에 대해 상대적으로 영향을 받지 않음. 통신선로에 응용시, 이들 목적의 효과성은 공격의 능숙성과 이들 공격의 발견 또는 저항능력의 함수로써, 통신선로의 물리적 특성에 종속됨. 통신수신자가 원격사이트일 경우 외부 통신선로의 물리적 보호를 제공하는 것은 거의 불가능함. 통신선로의 소유자가 제공하는 부가적인 보호가 필요함. 외부인이 시스템 영역내의 보호되지 않은 통신선로 또는 보호될 수 없는 광범위한 노출영역 내의 통신선로의 태핑이 본 공격의 예임
	보안목적 (대응책)	O23. 통신선로의 물리적 보호 O128. 탬퍼링의 발견 (공격을 발견하고자 할 경우 선택) O129. 탬퍼링에 대한 저항 (공격을 방지하고자 할 경우 선택)
Security Use Case (PKB 보안목적)	※ 보안요구사항 분석자가 위협관련 PKB 공격 선택에 따라 해당 보안목적 목록이 선택됨 O23. 통신선로의 물리적 보호 O38. 자료교환 기밀성의 강화 O128. 탬퍼링의 발견 O129. 탬퍼링에 대한 저항	

그림 8. 위협문장으로부터 PKB 보안목적문장 도출 예

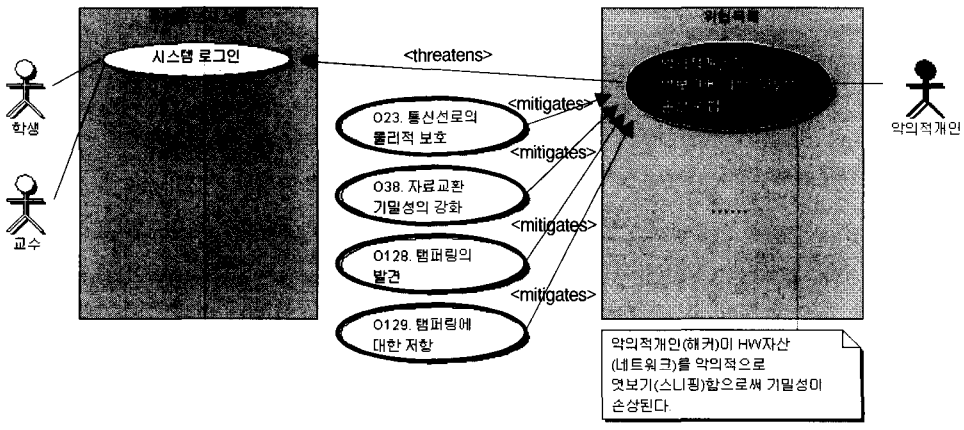

그림 9. 3단계 SUC 모델링 예

Security Use Case (PKB 보안목적)	O23. Comm_Line_Protection : 통신선로의 물리적 보호	
	설명	물리적인 탬퍼링으로부터 통신선로를 보호한다.
	선택지침	없음
	[주]	특정목적, 일반응용
	구현을 위한 CC 컴포넌트	FPT_PHP.1 : 물리적 공격의 수동 탐지 ※ 선택여부 : O
	O38. Data_Exchange_Conf : 자료교환 기밀성의 강화	
	설명	원격시스템과의 자료교환시, 전송자 자료 기밀성을 보호한다.
	선택지침	본 목적은 오직 허가된 통신을 금지하고, 통신선로상으로 송신될 수 있는 정보의 유형을 제한함으로써, 여타 자료 교환정책 유형을 지원할 수 있다.
	[주]	특정목적, 일반응용
	구현을 위한 CC 컴포넌트	FCS_COP.1 : 암호연산 ※ 선택여부 : O
	O128. Tamper_ID : 탬퍼링의 발견	
	설명	시스템 컴포넌트의 물리적 탬퍼링을 발견하고 이 특질을 보안위반을 제한하는데 사용하는 시스템 특질을 제공한다.
	선택지침	O128은 TOE(정보시스템)의 정제된 부분에 대한 물리적 공격을 발견하는 능력을 제공한다.
	[주]	일반목적
	구현을 위한 CC 컴포넌트	FPT_PHP.1 : 물리적 공격의 수동 탐지 ※ 선택여부 : O FPT_PHP.2 : 물리적 공격의 탐지 및 통보 ※ 선택여부 : O
	O129. Tamper_Resistance : 탬퍼링에 대한 저항	
	설명	정제된 시스템 장치의 컴포넌트를 이용해 물리적 탬퍼링의 방지 또는 저항
	선택지침	O129는 TOE(정보시스템)의 정제된 부분에 대한 물리적 공격에 자동대응하는 능력을 제공한다. 여러유형의 자동 대응이 있으나 일반적으로 '통지' 보다는 적극적인 '행동'을 수행한다.
	[주]	일반목적
	구현을 위한 CC 컴포넌트	FPT_PHP.3 : 물리적 공격에 대한 저항 ※ 선택여부 : O
Use Case (보안기능요구사항)	※ 보안요구사항 분석자가 분석한 CC 보안기능 컴포넌트등 선택한 보안기능요구사항이 제택됨 FCS_COP.1 : 암호연산 FPT_PHP.1 : 물리적 공격의 수동 탐지 FPT_PHP.2 : 물리적 공격의 탐지 및 통보 FPT_PHP.3 : 물리적 공격에 대한 저항	

그림 10. 보안목적으로부터 CC 보안기능요구사항 도출 예

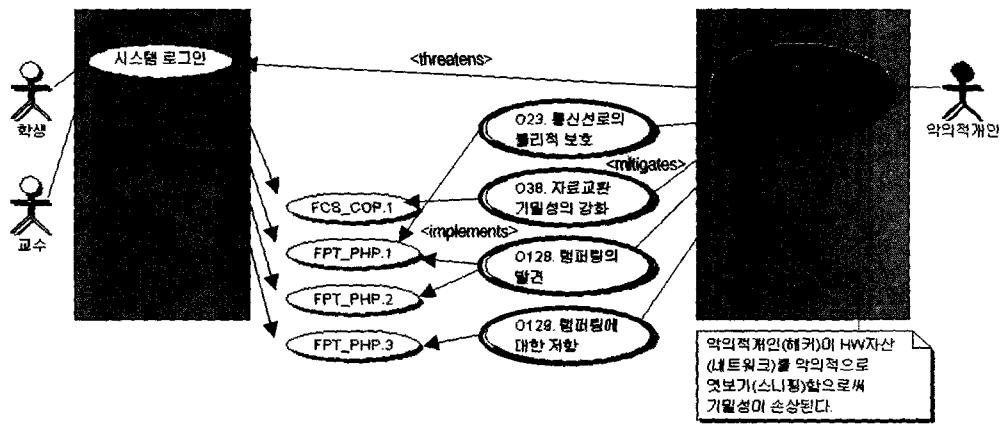

그림 11. 4단계 UC 모델링 예

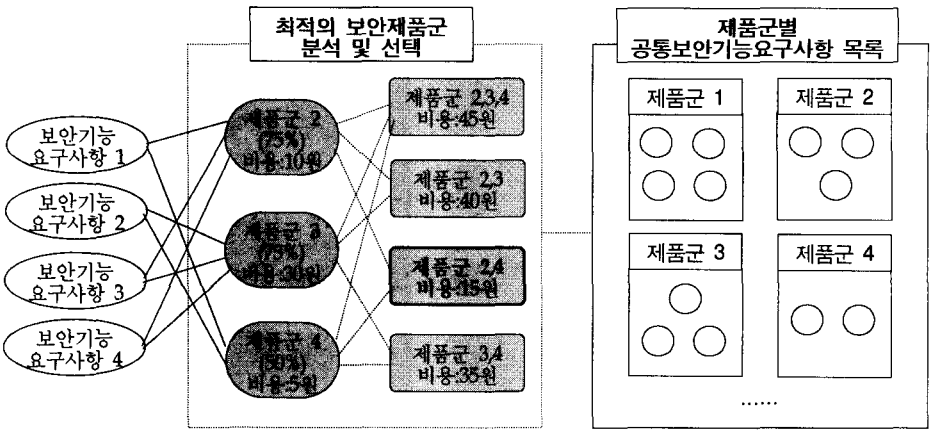

그림 12. 최적의 보안제품군 제시 모델

아닌 재구성(또는, 유지보수) 단계일 경우 첫 번째에서 네 번째 단계를 거쳐 분석된 보안기능요구사항들을 제품으로 구현한 보안제품군을 선택하여 기존의 정보시스템 자산에 통합하기 위하여 최적의 보안제품군(솔루션)을 분석하는 단계이다. 본 단계에서 사용되는 최적의 보안제품군 제시를 위한 모델은 그림 12와 같다.

본 연구팀은 인터넷을 통해 기발표된 33종의 PP를 분석하여 제품군별 공통보안기능요구사항 목록을 도출하였으며, 이를 DB로 구축하였다. 따라서, 구축된 DB를 이용하여 본 논문에서 제시한 보안요구사항 분석 및 명세 프로세스를 통해 분석 및 명세된 보안기능요구사항과 비교하여 해당 보안기능요구사항이 구현된 보안제품군을 분석한다. 이때, 그림 12와 같이 일치여부를 백분율로 표시(예컨대, 방화벽 제품군이 분석된 10개의 보안기능요구사항 중에서 8개를 포함한다면 80%로 표시)할 수 있으며, 필요하다면 해당 보안제품군의 평균적인 구매비용을 분석하여 표

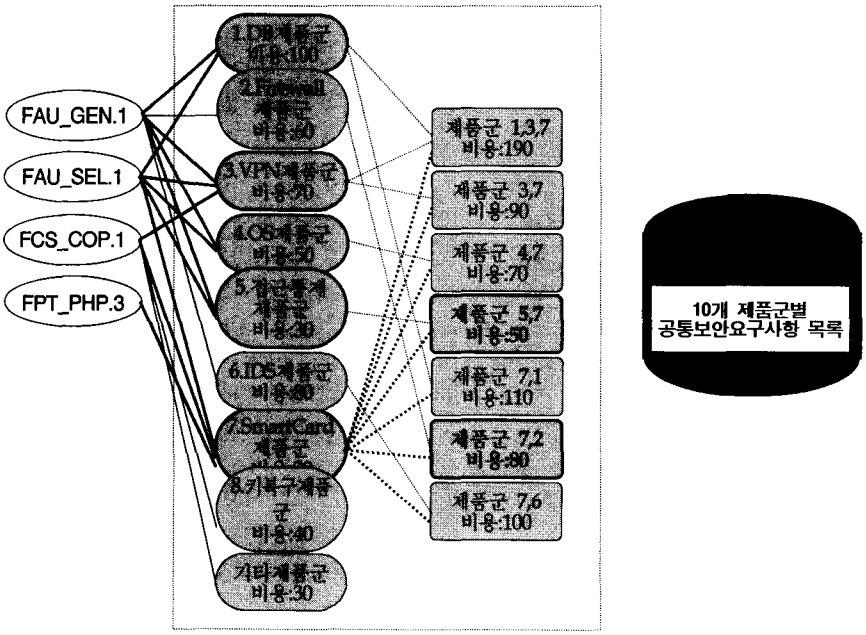

그림 13. 4단계에서 분석된 보안기능요구사항을 만족하는 최적의 보안제품군 분석 예
(비용은 임의의 값을 적용함)

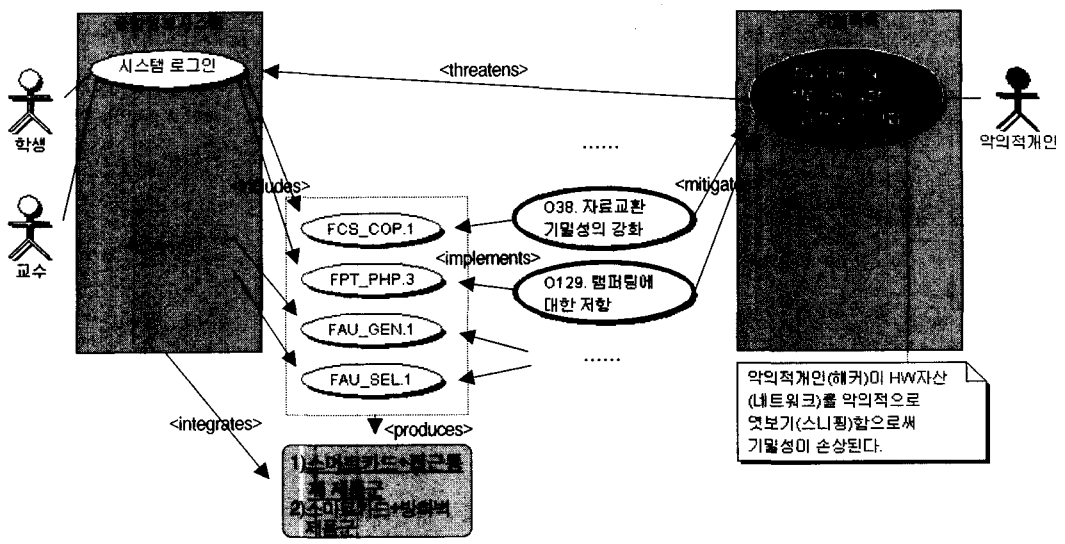

그림 14. 5단계 SPC 모델링 예
(최소비용 최대효과를 위하여 접근통제+스마트카드 제품군을 선택한 경우)

시할 수 있다. 이것은 최적의 보안제품군 선택을 위한 가이드라인으로 사용될 수 있다. 이와 같은 방법으로 가능한 모든 조합을 분석한 후, 분석된 전체 보안기능요구사항을 수용할 수 있는 보안제품군 또는 보안제품군 집합을 선택하면 된다. 이때, 집행가능예산 등을 고려하여 개발 및 재구성 환경에 적합한 최적의 보안제품군을 선택한다.

그림 11의 4단계 모델링 결과(분석과정을 간단하게 보이기 위하여 보안기능요구사항은 FAU_ GEN.1, FAU_SEL.1, FCS_COP.1, FPT_PHP.3의 네 가지로 가정함)를 이용하여 최적의 보안제품군을 분석하는 예는 그림 13과 같다.

그림 13의 예에서, FPT_PHP.3의 보안기능요구사항을 충족시키기 위해서는 스마트카드 제품군이 꼭 필요하다는 것을 알 수 있으며, 따라서 스마트카드+접근통제 제품군 또는 스마트카드+방화벽 제품군의 두 가지 보안제품 솔루션을 적용할 수 있다. 이때, 분석자 및 개발자가 비용만을 고려할 경우 스마트카드+접근통제(비용 : 50, 중복율 : 25%) 솔루션을 채택할 수 있다. 그러나, 보안기능요구사항의 중복을 최소화하면서 비용을 함께 고려할 경우 스마트카드+방화벽(비용 : 80, 중복율 : 0%) 솔루션을 채택할 수도 있다.

분석된 보안기능요구사항들의 집합과 보안제품 솔루션 사이에는 〈produces〉 관계연산이 적용되며, 정보시스템 재구성 단계라면 정보시스템 자산과 보안제품 솔루션 사이에는 〈integrates〉 관계연산이 적용된다. 5단계 모델링까지 수행한 최종 결과는 그림 14와 같다.

Ⅳ. 방법의 분석 및 비교

본 논문에서는 UML의 UC 모델을 확장한 MUC 모델을 이용하여 CC 기반의 보안요구사항 분석 및 명세 모델 및 프로세스를 제시하였다. 본 논문에서 제시한 보안요구사항 분석 및 명세 방법론의 특징은 다음과 같다.

- **MUC 모델 기반의 명세 및 분석 방법론** : 본 모델 및 프로세스는 UML의 UC 모델을 보안요구사항 분석에 적합하도록 확장한 MUC 모델을 기반으로 하고 있다. 특히, Sindre& Opdahl의 MUC 모델과 Firesmith의 SUC 모델을 기반으로 하여 보안위협과 보안위협을 완화하기 위한 보안요구사항, 그리고 보안요구사항을 구현하기 위한 보안기능요구사항을 모두 분석할 수 있다. 이것은, 기존의 UC 기반의 분석 모델들이 가지고 있었던 보안요구사항과 보안기능요구사항(메커니즘)의 구분 문제를 확실하게 해결할 수 있는 방법이다.
- **CC 기반의 보안요구사항 분석 방법론** : 본 모델 및 프로세스는 CC를 기반으로 하고 있다.

특히, 분석 및 명세 단계에서 개발자 및 분석자들 사이에 혼란을 초래할 수 있는 컨텐츠들을 순수 CC를 기반으로 하여 도출하였기 때문에 정형성 및 일관성 문제를 해결하였다. 이를 통해, 분석 및 명세된 보안요구사항과 보안기능요구사항들을 구현함으로써 해당 정보시스템은 정보보호시스템이 될 수 있으며 이를 CC를 통해 다시 평가·인증받을 수 있다는 장점을 갖는다.

- **시스템 개발자 및 CC 전문가 모두 이용 가능한 방법론** : 본 모델 및 프로세스는 UML의 UC 모델을 기반으로 하고 있기 때문에, CC에 대한 전문지식이 없는 시스템 개발자들도 쉽게 보안요구사항을 분석 및 명세할 수 있다. 또한, CC의 컨텐츠와 프로세스(보안위협, 보안목적, 보안기능요구사항)를 기반으로 하고 있기 때문에, CC 전문가(또는, PP/ST 개발자)들도 쉽게 보안요구사항을 분석 및 명세할 수 있다는 장점을 갖는다.
- **보안요구사항 및 보안기능요구사항을 모두 분석 가능한 방법론** : 본 모델 및 프로세스는 보안요구사항 분석 및 명세를 3단계 즉, 보안위협 분석 및 명세, 보안요구사항 분석 및 명세, 그리고 보안기능요구사항 분석 및 명세로 구분함으로써, 기존의 MUC 모델을 이용한 보안요구사항 분석 및 명세 방법론들의 보안요구사항(비기능요구사항)과 보안기능요구사항(기능요구사항)간의 혼동 문제를 해결하였다. 따라서, 비기능요구사항인 보안요구사항과 기능요구사항인 보안기능요구사항을 모두 분석할 수 있다는 장점을 갖는다.
- **정보시스템 개발 및 재구성시에도 이용 가능한 방법론** : 본 모델 및 프로세스는 시스템 개발 단계에서 이용 가능하다. 즉, 시스템 개발 단계에서 분석된 기능요구사항들을 이용하여 관련위협 및 보안요구사항, 보안기능요구사항을 분석하고 분석된 보안기능요구사항들을 포함시킬 수 있다. 또한, 시스템 재구성 단계에서는 기존의 정보시스템의 기능요구사항들을 분석하여 관련 위협 및 보안요구사항, 보안기능 요구사항을 분석하고 분석된 보안기능요구사항들을 구현한 보

표 2. 기존 연구들과 본 연구의 비교·분석결과

	UC 모델	MUC 모델[9,10] (Sindre&Opdahl)	MUC 모델[11~13] (Alexander)	AC 모델[14~16] (McDermott)	SUC 모델[17] (Firesmith)	본 모델
목표	기능요구사항의 분석 및 명세	보안위협의 분석 및 명세	보안위협의 분석 및 명세	보안위협시나리오의 분석 및 명세	보안요구사항의 분석 및 명세	보안위협, 보안요구사항 및 보안기능요구사항의 분석 및 명세
이용자	개발자/분석자	개발자/분석자	개발자/분석자	개발자/분석자	개발자/분석자	개발자/분석자
이용단계	시스템 개발	시스템 개발	시스템 개발	시스템 개발	시스템 개발	시스템 개발/유지보수(재구성)
모델링	UML 기반의 UC 다이어그램	UML 기반의 UC 다이어그램	UML 기반의 UC 다이어그램	UML 기반의 UC 다이어그램, 트리모델	UML 기반의 UC 다이어그램	UML 기반의 UC 다이어그램
관계 연산	includes, extends	includes, extends, prevents, detects	includes, threatens, mitigates	-	-	threatens, mitigates, implements, includes, products, integrates
분석 프로세스	행위자 기능요구사항	기능요구사항 위협원/위협 보안메커니즘	기능요구사항 위협원/위협 대응책(보안메커니즘) 2번째부터 반복(게임이론)	시나리오 위협원/위협시나리오식별 위협시나리오정의 Granularity 검사 Completeness/Minimality 검사	자산및서비스 위협원/위협 보안요구사항 보안메커니즘	기능요구사항 위협원/위협 보안요구사항 보안기능요구사항 보안제품
결과	기능요구사항	보안위협, 보안메커니즘	보안위협, 대응책	위협시나리오	보안요구사항, 보안메커니즘	보안기능요구사항/보안제품
모델의 유도	-	UC	UC, 게임이론	UC, 침투시험 및 소프트웨어결함트리분석, 침투시험	MUC	MUC, SUC, CC
모델의 컨텐츠	-	언급없음	언급없음	언급없음	언급없음	CC, PP, CCToolbox/PKB
기타	-	UC에 대한 설명을 위하여 템플릿 제시	위협 및 대응책 사이의 관계를 게임이론과 연관시킴	Actor에 속성(자원, 기술, 목표) 부여, 보증문제에 적용함	보안요구사항을 3가지로 구분하고 템플릿 제시	비용효과적 보안제품 선정 알고리즘 제시

안제품(정보보호제품)을 비용효과적으로 선정함으로써 기존의 정보시스템과 통합할 수도 있다.

본 논문에서 제시한 모델 및 프로세스를 기존의 MUC 기반의 보안요구사항 분석 및 명세방법들과 비교 분석한 결과는 표 2와 같다.

V. 결 론

본 논문에서는 MUC 모델을 확장하고 CC의 보안요구사항 분석 및 명세 프로세스를 응용하여 보안요구사항을 분석 및 명세하기 위한 모델과 프로세스를 제시하였다. 또한, 보안위협과 보안요구사항, 보안기능요구사항의 일관성 및 정형성을 제공하기 위하여 CC와 CCToolBox/PKB, 기발표된 PP들을 조사 분석하여 순수 CC 기반의 컨텐츠들을 도출하였으며, 유지보수 단계에서 분석 및 명세된 보안기능요구사항들을 통합하기 위한 비용효과적인 보안제품 선정 알고리즘을 제시하였다.

본 논문에서 제시한 보안요구사항 분석 및 명세 모델과 프로세스를 통하여 UC를 기반으로 하여 보안요구사항의 분석 및 명세를 단순화할 수 있으며, 이를 통하여 개발된 정보보호시스템의 품질을 제고할 수 있을 것이다.

그러나, 보안위협 이외에도 정보시스템을 운영하는 조직의 보안정책에 대한 분석을 통하여 보안요구사항 도출이 가능하며 이를 위한 분석 및 명세 방법에 대한 연구를 향후 연구과제로 남긴다.

참 고 문 헌

[1] "정보보호시스템 평가/인증 가이드", 한국정보보호진흥원, 2002.12.

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

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

[4] Final Interpretations, http://www.commoncriteria.org/docs/PDF/CCPART1V21.PDF.

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

[6] S. Alhir, *UML in a Nutshell*, O'Reilly, 1998.

[7] I. Jacobson, et al. Object-Oriented Software Engineering : A Use Case Driven Approach, Addison-Wesley, 1992.

[8] 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.

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

[10] G. Sindre, A. L. Opdahl, "Templates for Misuse Case Description," Proc. 7th International Workshop on Requirements Engineering : Foundation of Software Quality(REFSQ'2001), Interlaken, Switzerland, pp.4-5, June 2001.

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

[12] I. Alexander, "Misuse Cases Help to Elicit Non-Functional Requirements," Computing and Control Engineering, 14, 1 (February 2003), pp.40-45.

[13] I. Alexander, "Modeling the Interplay of Conflicting Goals with Use and Misuse Cases," Proc. 8th International Workshop on Requirements Engineering : Foundation for Software Quality(REFSQ'02), (September 2002), pp.145-152.

[14] 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.

[15] J. McDermott, C. Fox, "Using Abuse Case Models for Security Requirements Analysis," Proc. Annual Computer Security Applications Conference (ACSAC'99), Dec 1999.

[16] J. McDermott, "Abuse Case Based Assurance Arguments," Proc. 17th Annual Computer Security Applications Conference(ACSAC'01), 2001.

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

[18] 고정호, 이강수, "PP의 보안환경을 위한 위협문장 생성방법," 한국전자거래학회지, 8권 3호, pp.69-86, 2003년 8월.

[19] ISO/IEC PDTR 15446, "Information technology-Security techniques-Guide for the production of protection profiles and security targets," Draft, Apr 3, 2000.

[20] NIAP, List of Threat, Attack, Policy, Assumption, and Environment Statement Attribute, CC Profiling Knowledge base Report, 2002.

[21] Oracle, PP-008, DBMS Protection Profile, EAL3, Issue 2.1, May 2000 외 32종(기재생략).

[22] Oracle 8, Security Target, Release 8.0.5, April 2000외 66종(기재생략).

〈著者紹介〉

최 상 수 (Sang-Soo Choi) 학생회원
2001년 2월 : 한남대학교 컴퓨터공학과 졸업 (학사)
2003년 2월 : 한남대학교 대학원 컴퓨터공학과 졸업 (석사)
2003년 3월~현재 : 한남대학교 대학원 컴퓨터공학과 박사과정
〈관심분야〉 소프트웨어공학, 웹공학, 보안공학, 정보보호 컨설팅 및 위험분석

장 세 진 (Se-Jin Jang) 학생회원
2003년 2월 : 한남대학교 컴퓨터공학과 졸업 (학사)
2003년 3월~현재 : 한남대학교 대학원 컴퓨터공학과 석사과정
〈관심분야〉 소프트웨어공학, 보안공학, 정보보호시스템 평가 및 보안컨설팅

최 명 길 (Myung-Gil Choi) 정회원
1993년 2월 : 부산대학교 경영학과 졸업 (학사)
1995년 2월 : 부산대학교 경영정보전공 (석사)
2004년 2월 : 한국과학기술원(KAIST) 정보보호전공 박사과정 수료
1995년~2000년 : 국방과학연구소 연구원
2000년~현재 : 국가보안기술연구소 선임연구원
〈관심분야〉 인터넷 보안, 정보보호시스템 평가, 취약성 예측 모형, 정보보호경영

이 강 수 (Gang-Soo Lee) 종신회원
1981년 : 홍익대학교 컴퓨터공학과 졸업 (학사)
1983년 : 서울대학교 대학원 전산학과 졸업 (이학석사)
1989년 : 서울대학교 대학원 전산학과 졸업 (이학박사)
1985년~1987년 : 국립대전산업대학교 전자계산학과 전임강사
1992년~1993년 : 미국일리노이대학교 객원교수
1995년 : 한국전자통신연구원 초빙연구원
1998년~1999년 : 한남대학교 멀티미디어학부장
1987년~현재 : 한남대학교 컴퓨터공학과 정교수
〈관심분야〉 소프트웨어공학, 병행시스템 모형화 및 분석, 보안공학, 정보보호시스템 평가, 멀티미디어교육 커리큘럼