情報保護學會論文誌
第13券 第5號, 2003. 10

공통평가기준에 의한 보안정책모델 평가방법

김 상 호*, 임 춘 성**

An Evaluation Method for Security Policy Model Based on Common Criteria

Sang ho Kim*, Choon seong Leem**

요 약

보안정책모델은 평가대상제품(Target of Evaluation, TOE)의 보안정책을 비정형적, 준정형적, 또는 정형적 방법을 사용하여 구조적으로 표현하는 한 것이다. 보안정책모델은 보안기능요구사항과 기능명세간의 일관성 및 완전성을 제공함으로써 평가대상제품이 요구사항과 기능명세간 불명확성으로 인한 보안결점을 최소화할 수 있도록 보증성을 보장한다.[2][3] 이러한 이유로 ISO/IEC 15408(공통평가기준, CC) 등 IT 제품 및 시스템의 보안성 평가기준의 고등급 평가에서 보안정책모델을 요구하고 있다. 본 논문에서는 보안정책모델의 개념과 관련 연구 및 공통평가기준의 보안정책모델 보증요구사항을 분석하여 보안정책모델 평가방법을 제시한다.

ABSTRACT

Security Policy Model is a structured representation using informal, semiformal or formal method of security policy to be enforced by TOE. It provides TOE to get an assurance to mitigate security flaws resulted from inconsistency between security functional requirements and functional specifications. Therefore, Security Policy Model has been required under an high evaluation assurance level on an evaluation criteria such as ISO/IEC 15408(Common Criteria, CC). In this paper, we present an evaluation method for security policy model based on assurance requirements for security policy model in Common Criteria through an analysis of concepts, related researches and assurance requirements for security policy model.

keyword : *Security Policy Model, Common Criteria, Common Evaluation Methodology, Security Evaluation, Evaluation Method*

Ⅰ. 서 론

IT 기술의 진전으로 인한 디지털화로 정보시스템의 안전한 운영은 국가, 기업의 생존 및 성공의 중요한 전략적 요소로 인식되고 있다. 이와 함께 디지털 공간에서 신뢰할 수 있는 환경을 제공하기 위한 정보시스템의 보안성은 정보시스템 구축과 함께 병행하여야 하는 기반 요소로서 강조되고 있다.

이러한 정보시스템의 보안성은 정보시스템의 구축 단계에서부터 제공할 보안기능을 고려하여 설계하는 하여야 확보될 수 있다.[1] 일반적으로 설계하고자하는 시스템이 규모가 크고 복잡할 경우, 보안기능요구사항의 정확한 정의 및 정의한 보안기능의 정확한 명세 여부를 증명하는 것은 어려운 일이며, 정의 또는 명세 과정에서의 에러, 누락 또는 모호함 등으로 보안상의 문제를 야기하여 원하는 정보시스템의 보안기능 구현에 실패할 가능성이 있다.

보안정책모델은 평가대상제품(TOE, Target of Eva-

* 한국정보보호진흥원(shkim@kisa.or.kr)
** 연세대학교 컴퓨터산업공학과(leem@yonsei.ac.kr)

luation)의 보안정책을 구조적으로 표현하여 보안기능요구사항 및 기능명세를 정확하게 명세하고 해석할 수 있도록 하여 보안기능요구사항과 기능명세간 보안결점을 제거할 수 있도록 함으로 제품의 안전성을 보증할 수 있도록 한다.[4,5] 개발자는 보안정책모델을 활용하여 보안정책의 일관성을 점검할 수 있고, 보안기능요구사항과 기능명세간 모순점이 없도록 보증을 제공할 수 있으며, 평가자는 제시한 보안정책모델 평가를 통하여 보안정책과 보안기능요구사항 및 기능명세간의 일관성 및 완전성을 검증할 수 있다.

이러한 이유로 정보시스템의 보안성 평가기준인 미국의 TCSEC,[2] 유럽의 ITSEC,[3] 공통평가기준(Common Criteria, CC)[4,5]에서는 고등급의 보증요구사항에서 보안정책모델을 요구하고 있다. 또한, 국내의 정보통신망 침입차단시스템 및 침입탐지시스템 평가기준[6,7]에서도 K5등급 이상 보증요구사항에서 보안정책모델을 요구하고 있다.

기존의 보안정책모델에 대한 연구는 Bell-Lapadula Model, Biba 모델, Clark-Wilson 모델 등 접근통제 및 무결성 기능 중심의 보안모델[1,8,9]에 중점을 두어 진행되어왔다. 또한, 이러한 보안모델은 국방 등 주로 정보보호수준이 강화된 영역에의 적용에 초점을 두어 개발되어 기업 등 민간분야에 사용을 목적으로 하는 정보시스템에 이를 적용할 경우, 사용 또는 구현 환경에 따라 수정·보완하여 한다. 따라서 보안정책모델을 명세하는 일반화되고 구체적인 절차가 필요하며, 명세한 보안정책모델이 일관성 및 정확성을 검증을 위한 평가방법이 요구된다.

공통평가기준[4] 및 공통평가방법론(Common Criteria Evaluation Methodology, CEM)[11]은 보증요구사항 및 평가항목에서 보안정책모델에 대하여 명시하고 있으나, 개발자 및 평가자가 이를 적용하기 위한 절차 및 적용사례가 없어 어려움을 주고 있다. 또한, 보안정책모델에 대한 평가방법은 기존연구가 상대적으로 적고, 국내의 경우 보안정책모델을 적용한 제품 개발 및 평가사례가 전무한 실정이며 국외의 경우 이를 적용한 사례가 공개되지 않고 있다.

본 논문에서 개발자가 제품 개발 또는 평가 준비를 위하여 보안정책모델을 개발할 경우 활용할 수 있도록 공통평가기준에서 요구하는 보안정책모델 요구사항에 부합하는 일반화된 보안정책모델 절차를 Orange Book(NCSC-TG-010)[10] 등을 참조하여 제시하고, 평가자가 고등급의 제품 평가 시 활용할 수 있도록 공통평가방법론[11] 등을 참조하여 세부적인 보안모델정책 평가방법을 제안한다.

본 논문의 구성은 다음과 같다. 제 2장에서는 보안정책모델 관련 주요 용어와 개발과정에서 보안정책모델의 의미 등을 정리한다. 제 3장에서는 보안정책모델 관련 기존 연구 및 TCSEC, ITSEC, CC 등 평가기준 요구사항을 비교·분석한다. 제 4장에서는 공통평가기준을 기반으로 일반적으로 적용할 수 있는 보안모델 절차를 제시하고 공통평가방법론을 중심으로 보안정책모델 평가방법을 제안한다. 제 5장에서는 제안한 내용을 정리하고, 활용방안 및 향후 연구방향을 논한다.

II. 보안정책모델 개요

일반적으로 '모델'은 현실세계에서 발생하는 현상의 중요 사항을 단순화 또는 추상화하는 것으로 공학 분야에서는 복잡한 기능 또는 메커니즘을 명료하게 명세 또는 증명하고자 할 경우, 수학적 기법 등을 사용하여 표현하고 있다.[12] 그리고, '보안정책'은 조직의 중요한 정보를 관리, 보호, 분배하는 절차와 규칙, 법의 집합[4,13]이고, '보안정책모델'은 제품 또는 시스템에서 보안정책을 비정형적, 준정형적, 정형적인 방법으로 구조적으로 표현하는 것으로 정형적 보안정책모델의 예로 Bell-Lapadula Model 등이 있다.[14~16] 보안정책 및 보안정책모델은 다양하게 정의되고 있으나, 공통평가기준의 보증요구사항[4]에서는 보안정책(TSP, TOE Security policy)을 TOE를 통해 보호하고자하는 정보 또는 자산을 TOE 내에서 관리, 보호, 분배하는 규칙이 집합으로 정의하고 있으며, 보안정책모델(TOE Security Policy Model, TSPM)을 TOE에서 수행되는 보안정책을 구조적으로 표현한 것으로 정의하고 있다. TCSEC에서는 보안정책모델의 요구사항을 MAC(Mandatory Access Control), DAC(Discretionary Access Control) 등 접근통제정책을 중심으로 주체와 객체 및 이들간의 연산을 정의하여 정보상태 흐름의 통제를 수학적인 방법을 적용한 모델을 요구하고 있으나,[2,10] 공통평가기준에서는 그 범위를 접근통제 및 정보흐름 정책을 포함하여 무결성, 식별 및 인증 등으로 모델 가능한 정책으로 확장하여 평가보증등급에 따라 비정형, 준정형, 정형방법을 적용한 모델을 요구하고 있다.

이러한 보안정책모델은 보안기능요구사항으로 구체화되는 보안정책을 일관적이고 완전하게 비정형, 준정형, 또는 정형방법으로 명세하여 보안기능요구사

항이 정확하게 정의되어 구현되고 있음을 증명할 수 있어 보안기능요구사항과 기능명세 간 설계 단계에서 발생 가능한 오류를 최소화할 수 있도록 한다.[10,14,16] 즉, 기능명세와 보안정책과의 정확한 대응 관계를 증명함으로써 기능명세에서 보안기능을 일관적이고 완전하게 명세 하였음을 보증 받을 수 있다. 또한, 평가자는 보안정책모델 평가를 통하여 개발자가 보안기능요구사항 및 보안정책을 정확하게 이해하여 보안기능을 일관적이고 완전하게 구현하였는지 검증할 수 있다.[2,11]

2.1 주요 용어 정의

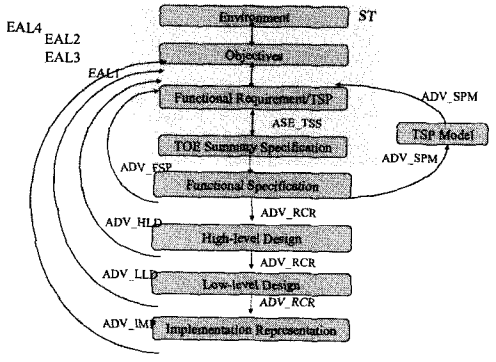
본 논문에서 사용되고 있는 용어를 공통평가기준 등[4,13,17]을 기초로 정리하면 아래와 같다.

- 평가대상제품(TOE, Target of Evaluation) : 평가의 대상인 IT 제품 또는 시스템으로 단일 또는 분산 구조의 제품 또는 특정목적과 운영환경을 가지는 시스템
- 보안목표명세서(ST, Security Target) : 식별된 TOE의 평가를 위한 근거로 사용되는 보안환경, 보안목적, 보안요구사항, TOE 요약명세로 구성된 문서
- TOE 보안기능(TSF: TOE Security Function) : TOE 보안정책에 기여하는 TOE의 모든 하드웨어, 소프트웨어, 펌웨어로 구성된 집합
- 기능명세(Functional Specification) : TSF의 외부 인터페이스와 보안기능 기본적인 동작을 서술
- 기본설계(High-level Design) : TSF를 주요 구성 단위(서브시스템)로 서술하고, 구성단위와 이들이 제공하는 기능 및 서브시스템간의 관계, 인터페이스를 서술
- 상세설계(Low-level Design) : 모듈과 모듈간 관계 및 종속성으로서 상세 수준의 설계를 서술
- 구현(Implementation) : 소스코드, 펌웨어, 하드웨어 설계도 등의 형태로 나타나며, 보안기능의 상세한 내부작업을 파악하게 함으로 분석을 지원
- 비정형 명세(Informal Specification) : 일반적인 자연어를 사용한 명세
- 준정형 명세(Semi-Formal Specification) : 제한된 그래픽한 표현 등 제약된 기호를 사용한 명세로서 자료흐름도, 상태전이도, 객체관계도, 자료구조도, 프로세스구조도 등을 이용한 명세
- 정형 명세(Formal Specification) : 수학적 개념에 기반한 형식적 표기법을 사용한 명세로서 [Z], [VDM], [GYPSY] 등을 이용한 명세

2.2 개발과정에서의 보안정책 모델

제품의 개발과정에서 보안정책모델은 보안기능 요구사항과 기능명세간 일관성과 완전성을 검증하는 역할을 하여 정의한 기능요구사항의 모호함 등에서 기인하는 보안기능의 구현상의 오류를 최소화하여 개발과정의 보증수준을 높이는데 기여한다.[10,16] 아래의 [그림 1]은 개발과정에서 보안정책모델을 위치를 도식화 한 것이다. 그림과 같이 보안정책모델은 위협, 가정사항, 조직의 보안정책 등 보안환경 및 보안목적으로부터 도출한 보안기능요구사항과 기능명세간에 일관성과 완전성을 제공하여 제품을 오류 없이 일관되게 기본설계, 상세설계, 구현으로 세분화 및 구체화되도록 한다. 공통평가기준에서 보안정책(TSP)은 일반적으로 보안기능요구사항 및 각 요구사항의 조합으로 표현하므로 특별하게 명시하지 않고 있다.

보안정책모델은 EAL4 이상의 보증요구사항에서 요구하고 있으며 평가보증등급에 따라 비정형, 준정형, 정형 방법을 사용하여 명세하도록 요구하고 있다.[4] 또한, 보안정책모델이 보안정책의 제약사항, 정보흐름 등을 제시하여 보안기능요구사항과 기능명세간의 일관성 검증 및 제품의 사용자, 개발자, 평가자에게 보안목적, 보안기능요구사항, 기능동작을 명확하게 하여 개발과정에서의 오류를 최소화하는 역할을 하므로 일정 수준 이상의 높은 보증 수준을 갖는 정보보호제품 개발을 위해서는 보안정책모델을 개발과정 초기부터 적용하여 개발하여야 한다.



〔그림 1〕 TOE개발과정에서의 보안정책모델

III. 관련 연구 및 평가기준 요구사항

본 장에서는 보안정책모델관련 연구를 고찰하여

기존 연구의 미비점을 알아본다. 또한 정보시스템 보안성 평가기준의 보안정책모델 요구사항을 비교·분석한다.

3.1 관련 연구

보안정책모델에 대한 기존 연구는 접근통제, 무결성 등 일부 보안기능의 보안정책을 정형방법을 사용하여 객체, 주체, 보안특성, 보안속성 등을 정의하고 정보상태흐름을 통제하는 BLP, Biba, Clark-Wilson 등 보안모델에 대한 연구가 대부분이다. 아래의 [표 1]은 주요 보안모델의 보안특성 및 특징을 비교·분석한 것이다.

제시한 보안모델은 일부 특정 보안정책 및 보안기능을 가지는 보안정책 모델에 한정하여 적용 가능하며, 국방분야 등 중요도가 높은 정보를 다루는 높은 수준의 보안을 요구하는 특수한 환경 등에 제한되어 적용되고 있다. 따라서 일반 환경에서는 적용시 많은 수정 및 보완이 필요하며, 특히 모델에서 포함하고 있지 않은 보안기능에 대한 정책 모델을 명세할 경우에는 적용하지 못하는 한계가 있다.

미국의 Orange Book(NCSC-TG-010)은 TCSEC의 요구사항을 기초로 보안정책모델 관련 요구사항 설명, 접근통제 정책에 대한 모델 방법을 중심으로 보안정책을 정형방법으로 명세 하는 방법을 설명하는 지침서이다.[10] 여기에서 주체, 객체, 연산자, 보안속성 등의

〔표 1〕 보안모델간 비교·분석

보안모델	통제 실체	보안특성	특 징	비고
BLP[15,16,18]	S: 주체의 집합 O: 객체의 집합 A: 접근모드의 집합 {실행, 읽기, 추가, 쓰기} L: 보안레벨의 집합	- simple security property (no read-up 보안정책 지원) - *-property(star property) (no write-down 보안정책 지원) - discretionary security property	- 보안레벨, 접근통제모델 기반 - 강제적, 임의적 접근통제 정책 지원 - 운영체제, DB의 일반적 보안모델로 활용가능	- 정보의 무결성 보호기능 미지원 - 접근통제 관리기능 미제공 - covert 채널 포함 - 매우 제한된 영역에 적용가능
Biba[18,19]	S: 주체의 집합 O: 객체의 집합 A: 접근모드의 집합 L: 보안레벨의 집합	- simple integrity property (no write-up 보안정책 지원) - integrity *-property (no read-down 보안정책 지원)	- 정보의 무결성 보호기능 지원모델 - 강제적, 임의적 접근통제 정책 지원 - 운영단계에서 무결성 레벨의 자동변경 기능	- 정보의 비밀성 보호기능 미지원 - 매우 제한된 영역에 적용가능
Clark-Wilson[18,20]	S: 주체의 집합 TP: 데이터 변환 절차들의 집합 CDI, UDI: 데이터 집합 IVP: 무결성 검증 절차	- well-formed transaction (WFT), separation of duty(SOD) 메커니즘을 기반으로 한 정보의 무결성 보호기능	- 정보의 무결성 보호 지원 - 5개의 인증 규칙과 4개의 실행 규칙 정의	- 상용환경의 보안 요구사항 반영 - 특정 보안모델의 지원보다는 보안정책 설계의 프레임워크로 활용
HRU[1,18]	S: 주체의 집합 O: 객체의 집합 R: 접근권한의 집합 M: 접근모델	- 주체, 객체의 생성, 삭제 등 보안관리기능 제공 - 객체, 주체, 접근행렬 조작을 위한 6개의 기본연산 정의	- 객체 소유자에 판단에 의해 접근권한 허가	- 복잡한 시스템의 보안모델로서 사용되는 경우 보안특성 유지 검증의 어려움
Lattice[1,21]	N: 객체의 집합 P: 프로세스의 집합 SC: 보안등급의 집합 ⊕: 보안등급 조합 연산자 →: 보안등급간 흐름관계	- <SC, →, ⊕>으로 구성된 보편적 유계격자 특성 - 유계격자 구조에서의 일방향 정보흐름 허용	- 정보에 대한 직접적인 접근통제보다는 정보의 비정상적인 흐름통제기능 제공 - 수학적인 격자구조 사용	
Chinese Wall[18]	C: 회사의 집합 O: 객체의 집합 S: 주체의 집합 y: 회사 자료집합 계산함수 x: 이해충돌 회사집합 계산 함수 L: 보안레이블 집합 (x(o),y(o))	- simple security property (객체에 대한 읽기접근 제한) - *-property (객체에 대한 쓰기권한 제한)	- 컨설팅 환경에서의 임무분리 특성 지원 - 객체에 대한 접근권한이 접근시점마다 재점검	- 간접적 경로를 통해 정보의 비정상적 흐름가능성 존재
역할기반 접근통제[27]	U: 사용자의 집합 R: 역할의 집합 P: 권한의 집합 UA: 사용자-역할 배정 PA: 역할-권한 배정 RH: 역할계층 C: 제약사항의 집합	- 관리역할에 배정된 보안관리자에 의해 UA, PA, RH, C 구성요소들의 형상변경 과정을 통하여 보안도메인의 보안정책 모델링	- 모델 자체를 기반으로 한 관리모델 제공 - 상용환경의 다양한 보안정책의 모델링 기능 제공(policy-neutral)	- 모델 구성요소의 설정이 임의적 특성을 가지고 있어, 정형적 검증 어려움 - 비교적 최근 제안된 보안모델로서 현재 관련연구가 진행중

구성요소와 운영체제, 네트워크 및 분산시스템, 데이터베이스 등 제품 특성별 적용 가능한 접근통제 및 무결성 정책에 대한 보안모델에 한정하여 명세방법을 수학적 논리에 바탕을 두어 보안정책을 정형화 언어로서 Ina Jo를 사용한 FDM(Formal Development Method) 및 Gypsy를 사용한 GVE(Gypsy Verification Environment) 등을 소개하여 설명하고 있어 일반환경에서 다양한 보안기능을 가지는 제품에 적용할 경우, 한계가 있다. 또한, Dennison의 보안정책모델링 방법[22]은 공통평가기준에 의한 보안정책 모델 방법을 단계적으로 제시하고 있으나 정형 명세 등에 대한 설명이 누락되어 있으며, 보안정책모델 평가에 대해서는 논하고 있지 않는 한계가 있다. 그리고 공통평가방법론은 보안정책모델 평가항목을 명시하여 평가방법을 서술하지 하고 있으나, 모델 범위 및 구체적인 평가방법이 명시되어 있지 않아 적용에 어려움이 있다. 국내의 경우에는 보안정책모델을 적용하여 개발 및 평가된 사례가 전무하며 관련연구도 다중등급 접근통제에 한하여 이루어지고 있는 실정이다. 따라서 보안기능을 가지는 정보시스템 제품 개발 및 평가에 실제로 적용 가능하도록 세부적으로 보안정책 모델을 명세하는 절차와 함께 보안모델정책을 평가하는 구체화된 방법에 대한 연구가 필요하다.

3.2 관련 평가기준 요구사항

보안정책모델은 앞서 언급한바와 같이 TCSEC, ITSEC, 공통평가기준(CC) 등 정보시스템 보안성 평가기준의 보증요구사항에서 요구하고 있으며, 요구사항을 분석·비교한 내용은 아래의 [표 2]와 같다.

표에서 보는바와 같이 보안정책모델은 고등급의 보증요구사항에서 요구하고 있으며, 공통평가기준은 ITSEC과 TCSEC의 내용을 포괄적으로 수용하고 있다.

즉, TCSEC은 접근통제기능(DAC, MAC 등)을 중심으로, ITSEC은 주요 기능에 대하여 보안정책모델을 요구하는 반면, 공통평가기준에서는 접근통제 및 정보흐름정책을 중심으로 모든 보안기능에 대하여 요구하고 있으며, 모델내의 내부적 일관·완전성의 근거제시 및 기능명세와의 일관성 및 완전성을 요구하고 있다.

Ⅳ. 보안정책 모델 절차 및 세부 평가방법

본 장에서는 공통평가기준의 보증요구사항[3]을 기초로 공통평가방법론(Common Criteria Evaluation Methodology, CEM),[11] Orange Book(NCSC-TG-010),[10] Dennison의 보안정책모델링 방법[22] 등을 참고하여 보안정책을 모델하는 절차를 제시하고 공통평가방법을 기반으로 보안정책모델의 세부 평가방법을 제안한다.

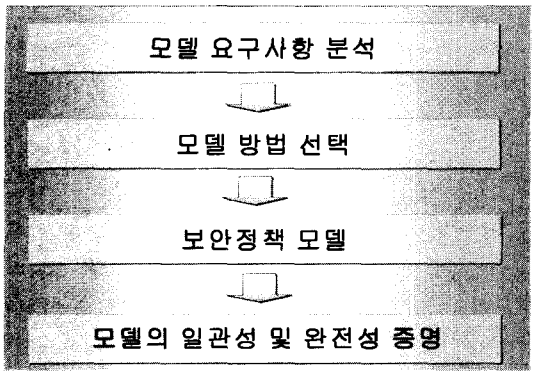
4.1. 보안정책 모델 절차

공통평가기준은 Waterfall approach, Rapid prototyping 등 특정 개발 방법론을 요구하지 않으므로 본 논문에서 제시하는 보안정책모델 절차는 특정 개발 방법론과 무관하다.

보안정책을 모델하는 첫 번째 단계는 보안목적, 보안기능요구사항 등 보안정책 모델을 위한관련 요

〔표 2〕 보안정책모델 관련 평가기준 비교·분석[2,3,5]

구분	TCSEC	ITSEC	CC
요구사항	• TCB(Trusted Computing Base)에 의해 지원된 보안정책의 비정형화 또는 정형화 모델은 정보시스템 생명주기 내에 유지되어야 하며, 공리(axiom)의 일관성이 보여져야 함	• TOE에 제공될 보안의 중요 원칙의 추상적 서술에 대한 정형적 보안정책 기반 모델 및 비정형적 해석 제공 • 정형적 모델은 ST에 명세한 모든 보안기능을 포함할 필요는 없음 • 보안정책과 모순되지 않음을 제공 • BLP, Clark-Wilson 등 보안 모델의 예 제시	• TSP 비정형화·준정형화·정형화 모델 제공 • 기능명세와 보안정책모델간 일치성 비정형화[EAL4]·준정형화·정형화[EAL5·6·7] 입증 • 접근통제 및 정보흐름정책을 포함한모델 가능한 보안정책의 규칙과 특성 서술 • 모델링 가능한 보안정책의 모든 정책이 일관성있고 완전함을 보이는 이론적 근거 제시 • 기능명세의 모든기능이 보안정책에 일관성있고 완전하게 포함하고 있는지 입증
평가등급	B1등급 이상	E4등급 이상	EAL4 등급이상



〔그림 2〕 보안모델 절차

구사항을 분석하는 것이다. 접근통제기능, 감사기록 기능, 무결성기능 등 보안기능 정의 및 구현에 필요한 정책을 분석한다. 이때 보안기능요구사항은 보안정책 모델 과정을 반복적으로 수행하면서 일관성 등을 고려하여 보완 가능하다. 두번째 단계는 평가보증등급(EAL4~EAL7)에 따라 비정형화, 준정형화 또는 정형화 등 명세방법을 선택하는 것이다.

준정형화 방법인 경우, 자료흐름도, 상태전이도 등을 사용하여 보안모델을 명세할 수 있으며, 정형방법의 경우, 기존의 보안모델 또는 정형언어를 사용한 모델을 적용할지 여부를 결정한다.

세 번째 단계는, 통제 개체(주체 및 객체), 보안특성, 연산자 등을 정의하여 보안정책(TSP)을 모델링한다. 준정형화, 정형화방법으로 명세한 경우에는 모델 명세에 참여하지 않은 개발자 또는 평가자의 이해를 돕기위하여 비정형적인 서술을 추가적으로 명세한다. 마지막으로 보안정책모델과 기능요구사항 또는 보안정책 및 기능명세서와 일관성과 완전성을 검증하고, 검증에 대한 이론적 근거를 서술한다. [그림 2]는 보안정책모델 절차를 도식화한 것이다.

4.1.1. 모델 요구사항 분석

모델 요구사항 분석 단계에서는 보안정책 모델에 필요한 평가대상제품의 보안기능요구사항과 보안정책, 조직의 보안정책 등 관련 사항을 작성 및 준비하여 보안정책모델에 요구되는 사항을 분석한다. 관련 문서로서 보안목표명세서의 보안환경, 보안목적, 기능요구사항, TOE 요약명세, 보안정책, 조직의 보안정책과 기능명세서가 있다. 보안환경 및 보안목적에서 도출된 보안기능요구사항은 보안감사(FAU), 통신(FCO), 암호지원(FCS), 사용자데이터보호(FDP), 식별 및 인증(FIA), 프라이버시(FPR), TSF 보호(FPT), 자원활용(FRU), TOE 접근(FTA), 안전한 경로/채널(FTP)로 분류하고 보안기능요구사항을 중심으로 조직의 보안정책을 고려하여 보안정책을 작성한다. 이때 보안정책은 보안기능별로 세분화하고 조직의 보안정책과 모순되지 않도록 한다. 하나의 보안정책은 두 개 이상의 보안기능으로도 구현가능하며, 보안기능요구사항을 만족하도록 명세한 TOE 요약명세 및 기능명세와 매핑하여 보안기능별 보안정책과 통제하고자하는 주체, 객체, 초기상태·안전한 상태 등 특성, 연산을 정의한다. 준정형, 정형방법을 적용할 경우, 보안기능요구사항 및 TOE 요약 명세를 고려하여 보안정책모델 가능한 보안정책을 중심으로 모델링 함을 원칙으로 한다. 또한, 기능명세에서는 보안정책 모델을 위해 보안기능 외부인터페이스와 명세한 기능동작을 분석한다.

4.1.2. 모델 방법 선택

보안정책모델은 보증평가등급에 따라 EAL4에서는 비정형방법, EAL5이상에서는 준정형, 정형 방법으로 명세하도록 요구하고 있다.[4] 비정형화 방법인 경우에는 자연어를 사용하여 간결하게 TOE 보안정책을 주체, 객체, 특성 등 통제 환경을 서술한다.

비정형적으로 명세할 경우에는 일반자연어를 사용하여 기존 보안모델 또는 개발 또는 평가대상 제품의 특성을 고려하여 주체, 객체 등을 정의하여 보안정책을 명세한다.

준정형 방법일 경우에는 그래픽한 표현 등 제약된 기호를 사용한 명세로서 자료흐름도, 상태전이도, 객체관계도, 자료구조도, 프로세스구조도, SDL 등을 사용하여 명세할 수 있다. 정형화방법으로 보안정책모델을 하고자하는 경우에는 모델 대상 기능에 따라 state transition, noninterference, information flow 등의 일반 모델을 사용하여 명세할 수 있다. 또한 Petri-net, communicating state machine, module logic 등 모델을 사용할 수 있다. 모델 선택 시에는 네트워크 제품 또는 분산구조의 제품 등 TOE 특성, 모델의 단순성, 모델하고자 하는 정책 적용의 적합성, 의도하는 수준의 정형화 정도 등을 고려하여 선택하며, 보안정책을 보안기능별로 세분화하고 통제 범위를 정하여 주체, 객체, 특성, 연산을 정한다. 즉, 보안정책모델은 보안기능별로 하부모델로 이루어 질 수 있으며, 하나의 모델이 둘 이상의 보안기능을 명세할 수 있다. 정형방법을 적용한 모델은 수학적 논리와 표기를 기초로 하는 정형화 언어인 Z,[25] VDM(vienna Development

Method),[26] Ina Jo 또는 Gypsy[11] 등을 사용하여 명세 및 검증할 수 있으며, 정형언어의 사용은 비정형적 언어를 사용한 명세에서 발생할 수 있는 모호성(ambiguity), 불완전성(incompleteness), 모순성(contradiction) 문제를 극복할 수 있으며, 기존 보안모델의 한계점 등을 극복하여 특성을 반영한 모델을 제시할 수 있다. 이러한 경우에는 정형언어에 대한 학습이 선행되어야 하며, 이를 해석하고 검증할 수 있는 방법도 고려하여야 한다.

4.1.3. 보안정책 모델

보안정책이 작성되고 모델 명세방법이 설정되면, 보안정책 모델을 수행한다. 일반적으로 보안정책모델은 통제 개체, 보안 특성, 연산 규칙으로 구성된다. 첫째, 통제개체 정의에서는 주체(능동적 개체), 객체(수동적 개체), 또는 개체 그룹, 개체의 속성 등 통제 범위 내의 모든 상태 변화 가능한 개체를 분류하여 정의한다. 둘째, 보안특성 정의에서는 보안특성 또는 속성을 공리로서 정의하며, 항상 전제조건으로서 가정되고 유지되도록 하며, 보안정책을 시행하는 방법, 요구되는 행위를 간결하게 표현한다. 보안특성의 예로서 BLP(Bell and La Padula) 모델의 Simple Security, *-Property, discretionary가 있다. 보안정책모델은 보안특성과 일관되게 명세하여 내부간 일관성을 유지하여야 한다. 셋째, 연산 규칙 정의에서는 주체와 객체간 상태전이함수 등에 관한 규칙을 정의한다. 주체와 객체간 읽기, 쓰기, 접근, 첨부 등의 연산을 보안특성을 고려하여 정의한다. 넷째, 연산규칙이 보안특성을 유지함을 각 상태전이함수 등이 보안특성을 만족함을 증명하고 초기상태가 안전함을 증명한다.

4.1.4. 모델의 일관성 및 완전성 검증

이 단계에서는 보안정책모델이 보안정책 및 정의한 보안기능요구사항과 일관된다는 근거를 명시하고 보안정책과 기능인터페이스를 고려한 기능명세와의 일관성 및 완전성을 각각 검증한다. 또한, 보안정책을 명세하여 모델한 범위와 부분을 명시한다. 비정형 방법으로 증명할 경우, 테이블 또는 적당한 표식을 사용하여 일치성을 서술할 수 있으며, 준정형 방법의 경우에는 세부 개체에 대하여 좀 더 완전하고 엄격하게 매핑하여 증명한다. 정형 방법인 경우에는 수학적인 개념을 적용하여 논리적으로 증명한다. 보안정책모델과 기능명세와의 일관성은 보안정책과 일관되고 완전하게 기능이 정확하게 모델 되었다는 것을 의미하여, 정의한 기능에 대한 설계 및 구현의 오류를 최소화하여 개발과정의 보증성을 확보할 수 있다. 설계하고자하는 제품의 평가보증등급에 따라 비정형적인 방법으로 보안정책모델을 명세하는 경우에는 위의 일부 절차가 생략 가능하며, 정형언어를 사용하여 명세하는 경우에는 언어 선택 및 언어 특성 등 추가적인 절차가 필요하다. 그리고 준정형적 또는 정형적 방법으로 모델한 경우에도 반드시 비정형적 방법을 사용하여 명세한 보안정책모델에 대한 설명을 추가하여야 한다.

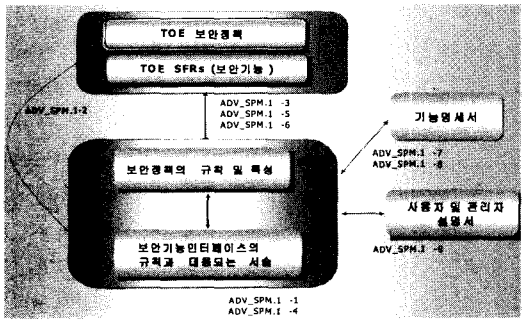
4.1.5. 제시한 보안모델 절차와 기존연구의 비교

본 논문에서는 공통평가기준에 의한 일반화되고 세부적인 단계별 보안정책 모델 절차를 이해하기 쉽도록 제시하여 BLP, NCSC-TG-010 등 비밀성, 무결성 등 일부 보안기능을 중심으로 정형적 방법을 일반환경에서 다양한 보안기능을 가지는 제품에 적용할 경우, 적용 범위 및 환경의 한계점을 해결하고 있다. 또한, Dennison의 보안정책모델링 방법[22]에서 논하고 있는 공통평가기준에 의한 모델 방법과 비교하여 기존 보안모델을 활용하는 방법, 정형명세 관련 사항 등과 관련된 누락 사항을 추가 및 보완하여 개발자가 모델 명세시 적용이 용이하도록 하고 있다. 고등급의 평가보증등급을 목표로 하는 제품 개발자는 본 논문에서 제시한 절차를 활용하여 공통평가기준에서 요구하는 보안정책모델을 명세할 수 있는 이점이 있다.

4.2. 보안정책모델 평가방법

보안정책모델 명세 후에는 이에 대한 일관성과 완전성 검증을 위하여 평가과정이 요구된다. 보안정책모델 평가관련 기존연구는 거의 없으며 다만, 공통평가방법론에서 공통평가기준의 요구사항을 기초로 평가자가 평가시 알아야 하는 주요 사항을 중심으로 제시하고 있으나, 구체적이지 않아 이를 평가에 직접적으로 활용하는데는 문제가 있다. 본 논문에서는 공통평가방법론의 평가항목[11,23,24]을 정리하고 추가적으로 보안정책모델의 단계적이고 세부적인 평가방법을 제안한다. 보안정책모델 평가의 목적은 모델이 보안정책의 규칙과 특성을 포함하여 명확하고 일관적으로 서술하고 있으며, 기능명세의 보안기능과 일관적이고 완전하게 서술하고 있는지 여부를 검증하는 것이다.

아래의 [그림 3]은 공통평가기준의 보안정책모델 평가항목을 평가를 위한 입력 요구문서와 연계하여



〔그림 3〕 평가항목과 요구문서의 연관 관계

공통평가방법론의 평가항목을 도식한 것이다. 그림에서와 같이 보안정책모델(SPM) 평가는 보안목표명세서(ST), 기능명세서, 보안정책모델(SPM), 사용자설명서, 관리자설명서가 필요하며 공통평가방법론의 세부평가항목과 입력 문서와의 관계는 [그림 3]과 같이 분류할 수 있다.

아래의 [표 3]은 공통평가방법론의 보안정책모델 평가항목을 요약하여 정리한 것이다. 서술한 평가항목에서 제시하는 내용([표 3]의 왼쪽 컬럼)만으로는 적용하는데 어려움이 있으므로 본 논문에서는 평가

〔표 3〕 공통평가방법론의 평가항목과 제안된 세부평가항목

평가항목	요 약	세부평가방법 제안
ADV_SPM.1-1	• 보안정책모델이 비정형 명세 여부 분석	• 보안정책모델이 **등급별로 비정형, 준정형, 정형 명세 여부 확인 후, 준정형, 정형 명세일 경우에도 비정형 서술이 있으며 내용이 명확한지** 평가
ADV_SPM.1-2	• ST에 명시한 보안정책이 보안정책모델에 포함되었는지 분석 - 보안기능요구사항에 FDP_ACC, FDP_IFC 여부 확인 - 준정형 또는 정형 모델이 불가능한 경우, 비정형 명세로 모델되어야함	• ST에 FDP_ACC, FDP_IFC가 있으며 모델되었는지 평가 - **접근통제, 정보흐름통제 기능이 ST에 포함되어 있으며, 주체 · 객체 · 연산자 · 보안속성 · 규칙을 세부적으로 명시하고 있는지 평가**
ADV_SPM.1-3	• ST의 보안기능요구사항에 의한 모든 보안정책이 되었는지 분석 - FIA, Reference mediation 등 FDP_ACC, FDP_IFC이외의 보안기능이 보안정책모델에 포함되어야 함 - 정형, 준정형 명세로 모델이 어려운 보안정책의 경우, 모든 보안정책을 비정형 명세로 모델하여야 함	• **FDP(데이터보호), FIA(식별 및 인증), FAU(감사기록) 기능 등이 있는지 점검하고 보안정책으로 서술된 모든 기능이 모델되었는지 평가** - **비정형방법으로 모델할 경우, 우 모든 보안정책이 모델되어야 하며, 정형적, 준정형적으로 모델이 어려운 보안정책의 경우에는 기능 및 보안정책 특성에 따라 예외로 할 수 있음** - 모델에 **주체 · 객체 · 연산자 · 보안속성 · 규칙을 세부적으로 명시**하고 있는지 평가
ADV_SPM.1-4	• 모델된 보안행위가 명확하게 구체화되고 있는지 보안정책모델의 특성과 규칙 분석 - TOE의 보안개념, 통제하는 개체의 보안속성, 보안속성을 변화시키는 TOE 행위 및 규칙 식별	• **TOE의 동작과 FDP, FIA, FAU, 기타보안기능 등 보안기능 특성에 따른 주체, 객체, 연산자, 규칙 등이 일관적이고 완전하게 정의되어 있는지 평가** - **임의적 접근통제의 경우(예)** ***객체 : 파일시스템, 프로세스, 메모리 등** ***주체 : 사용자를 대신한 프로세스, 관리자 등** ***객체 속성 : 소유자, 읽기/쓰기/실행,허용비트 등** ***주체속성 : UID, gid 등** ***규칙 : 주체와 객체간 보안속성변경을 위한 규칙(chmod, chown, chgrp 등)**
ADV_SPM.1-5	• ST의 보안정책에 서술된 정책과 모델된 행위가 일관되는지 모델의 이론적 근거 분석 - 보안정책모델에 서술된 특성과 규칙이 보안정책과 일관되는지 근거 검증	• ST의 보안요구사항과 보안정책모델간 상관관계를 분석하고 보안정책모델의 근거 점검 등을 통한 일관성 평가 - **모델된 특성, 보안속성 및 규칙이 일관**되는지 점검 - 보안정책모델의 근거에 보안정책의 의도하는 **규칙과 특성이 구체적으로 서술되었는지 검증**
ADV_SPM.1-6	• ST의 보안정책에 서술된 정책과 모델된 행위가 완전한지 모델의 이론적 근거 분석 - 보안정책에 서술된 특성과 규칙과 보안정책모델의 특성과 규칙간 상관 관계 분석	• ST의 보안요구사항과 보안정책모델간 상관관계를 분석하고 보안정책모델의 근거 점검 등을 통한 완전성 평가 - 모델된 모든 보안정책은 보안정책모델에 특성, 보안속성, 규칙을 포함하여 **누락없이 완전하게 명시**되어 있음을 검증
ADV_SPM.1-7	• 보안정책모델과 기능명세서와의 대응관계 등을 통하여 보안정책모델에 서술된 정책이 기능명세서에 모두 서술되어 있음을 분석 - 기능명세서를 점검하여 어떠한 기능과 보안정책모델과의 대응되어 있는지 분석	• 기능명세서에 명시한 기능 및 인터페이스를 고려하여 보안정책모델과의 대응관계를 분석하고 명세한 각 기능이 모델 되었음을 평가 - **식별 및 인증, 접근통제, 감사기록 생성, 보안기능 데이터 변경 기능 등을 중심으로 ST의 보안기능이 보안정책모델에 대응되는지 분석**
ADV_SPM.1-8	• 보안정책모델과 기능명세서의 서술 내용과의 일관성 분석 - 보안정책모델에 명시한 특성과 규칙이 기능명세서에 동일하게 적용되었음을 분석	• 보안정책모델에 **명시한 주체, 객체, 보안속성, 특성이 기능명세서에 서술한 기능동작 또는 기능인터페이스와의 일관성** 평가 - **기능명세서, 사용자 및 관리자설명서에 서술한 기능 동작과 보안정책모델간 차이점 및 모순점** 분석

항목을 보다 명확하고 구체적으로 제시하였으며, 단계별 평가방법을 제안하였다. [표 3]의 오른쪽 컬럼의 굵은 글씨는 본 논문에서 추가적으로 제안한 것이다.

본 논문에서는 보안정책모델 평가절차를 명세방법 평가, 보안정책모델의 완전성 평가, 보안정책모델의 일관성 평가, 기능명세와의 일관성 및 완전성 평가 단계로 다음과 같이 제안한다. []는 제안한 단계에 상응하는 공통평가방법론의 평가항목을 표시한 것이다.

4.2.1. 명세방법 평가[SPM1-1]

평가자는 개발자 또는 신청인이 제시한 보안정책모델을 검토하여 신청 보증등급을 기초하여 비정형[EAL4], 준정형·정형적[EAL5 이상] 여부를 확인하고, 준정형적 또는 정형적으로 모델된 경우, 비정형적으로 서술되어 있는지 평가한다. 준정형적 또는 정형적으로 명세된 경우에도 다른 개발자 및 평가자의 이해를 돕기 위하여 비정형적으로 명세하여야 하므로 이를 확인하여 평가한다.

4.2.2. 보안정책모델의 완전성 평가[SPM1-2~3]

보안목표명세서에 정의되어 보안정책으로 서술된 모든 보안기능이 보안정책 모델되었는지 확인하여 평가한다. 특히, FDP_ACC(접근통제 정책), FDP_IFC(정보흐름통제) 등 FDP(사용자데이터보호), FIA(식별 및 인증), FAU(감사기록) 기능 등을 중심으로 모델되어 있음을 확인한다. 또한, 비정형적으로 명세한 모델의 경우, 모든 보안기능이 포함되어야 하며, 준정형적 및 정형적으로 명세한 모델의 경우에는 분산구조와 불안전한 상태의 주체 및 개체를 가지는 제품일 경우 보안정책 특성 및 현재의 기술 수준을 고려하여 예외사항을 둘 수 있다. 예외 사항을 적용한 경우에는 근거를 제공하도록 하고 근거가 타당한지 확인한다. 그리고, 보안정책모델에 주체·객체·연산자·보안속성·규칙 등이 세부적으로 명시하고 있는지 평가한다.

4.2.3. 보안정책모델의 일관성 평가[SPM1-4~6]

보안목표명세서에 정의된 접근통제(FDP), 식별 및 인증(FIA), 보안감사(FAU) 등 보안기능이 평가대상제품의 동작과 기능의 특성에 따라 모델된 주체, 객체, 연산자, 규칙 등과 일관적인지 여부를 평가한다. 예로서, 임의적 접근 통제의 경우, 객체(파일시스템, 프로세스, 메모리 등), 주체(사용자를 대신한 프로세스, 관리자 등), 객체 속성(소유자, 읽기/쓰기/실행, 허용비트 등), 주체속성(UID, gid 등), 규칙(초기화를 위한 규칙, 주체와 객체간 보안속성변경을 위한 규칙, chmod, chown, chgrp 등)이 제품(TOE)의 동작과 기능의 특성과 일관적으로 모델되었는지 검증한다. 또한, 식별 및 인증의 경우, 사용자 생성/삭제/변경 규칙, 역할을 포함한 속성, 초기화 및 변경 규칙, 인증 규칙, 패스워드 시도 횟수 등 환경 옵션, 환경 설정 규칙 등을 고려하여 모델되었는지 검증한다. 그리고 감사기록생성 기능인 경우에는 감사대상사건, 감사생성 레코드 속성, 감사대상 환경 설정, 환경 설정 옵션, 감사데이터 접근 규칙 등이 적용되어 모델되었는지 검증한다. 준정형적 또는 정형적으로 명세한 모델의 경우, 각 방법을 사용한 모델과 비정형방적 서술이 구체적이며 정확한지 분석을 통하여 평가한다. 보안목표명세서의 보안요구사항과 보안정책모델간 상관관계를 제시하였는지 점검 및 분석하고 보안정책모델의 이론적 근거 점검 등을 통하여 모델된 모든 보안정책이 특성, 보안속성, 규칙을 포함하여 명시되어 있음을 검증한다.

4.2.4. 기능명세와의 일관성 및 완전성 평가[SPM1-7~8]

이 단계에서 평가자는 보안정책모델과 기능명세에서 서술한 보안기능 및 외부인터페이스와의 관계를 분석하고 식별 및 인증, 접근통제, 감사기록 생성, 보안기능 데이터 변경 기능 등을 중심으로 정의한 보안기능이 보안정책모델에 대응하여 모델되었음을 평가한다. 또한, 보안정책모델에 명시한 주체, 객체, 보안속성, 특성이 기능명세서에 서술한 기능동작 또는 외부인터페이스와의 일관성 여부를 평가한다. 기능명세의 기능동작은 사용자 및 관리자설명서에서 구체화되므로 기능명세서 뿐만아니라 사용자 및 관리자 설명서에 서술된 기능 동작과 보안정책모델간 차이점 및 모순점 여부를 분석 및 평가한다. 기능명세와 보안정책모델 간 일관성검증은 기능명세에서 정의한 보안기능이 보안목표명세서의 보안정책, 보안요구사항, TOE 요약명세를 일관적이고 완전하게 명세되었음을 의미하며, 정의하고 명세한 보안기능이 세부설계 과정을 통하여 정확하게 구현될 수 있음을 보증하는 것이다.

V. 결 론

정보시스템의 취약점 등을 이용한 공격으로 중요

정보의 유출, 전자상거래 중단 등 피해 사례가 빈번해 지고, 관련 위협이 증가함에 따라 정보보호제품의 수요가 증가하고 있으며, 이와 함께 제품의 보안성 평가에 대한 요구가 보편화되고 있다. 또한, 국가기반시설 등 정보시스템으로 중요정보를 처리하는 조직에서는 고 수준의 보안성을 갖는 정보보호제품의 요구가 증가할 것으로 예상되고 있다. 보안정책모델은 제품의 개발과정에서 보안기능요구사항과 기능명세간의 일관성과 완전성을 검증하는 역할을 하여, 요구사항 명세의 애매함 등에서 기인하는 보안기능의 구현상의 오류를 최소화하여 개발과정의 보증 수준을 높이고 요구사항에서 정의한 보안기능을 정확하게 구현할 수 있도록 한다. 따라서 공통평가기준의 고등급(EAL4 이상) 보증요구사항에서는 보안정책모델 명세를 요구하고 있다.

본 논문에서는 보안정책모델의 개요 및 관련연구 등을 분석하여 공통평가기준에 의한 보안정책모델 절차를 제시하여 평가방법을 제안하였다. 본 논문에서 제안한 보안정책모델 절차 및 평가방법은 공통평가기준 기반의 고등급(EAL4 이상)을 목표하는 제품 개발자 및 고등급(EAL4 이상) 제품 평가실무자에게 활용가능하다.

향후, 제안한 보안정책 모델절차 및 평가방법을 실제 제품에 적용한 사례 연구가 필요하다.

참 고 문 헌

[1] Silvana Castano et al., "*Database Security*", Addison-Wesly, 1994.

[2] National Computer Security Center, "*Department of Defense Trusted Computer System Evaluation Criteria*", DOD 5200.28-STD, December 1985.

[3] European Commission, "*Information Technology Security Evaluation Criteria V1.0*", June 1991.

[4] ISO/IEC15408, "*Common Criteria for Information Technology Evaluation Part3 : Security Assurance Requirements Version 2.1*", August 1999.

[5] ISO/IEC15408, "*Common Criteria for Information Technology Evaluation Part2 : Security Functional Requirements Version 2.1*", August 1999.

[6] 정보통신부, 정보통신망 침입탐지시스템평가기준, February 1998.

[7] 정보통신부, "정보통신망 침입탐지시스템평가기준", July 2000.

[8] Edward Amoroso, "*Fundamentals of Computer Security Technology*", Prentice-Hall, 1994.

[9] V. Portougal & Lech J. J anczewski, "Industrial information-weight security models", Information Management & Computer Security, 1998.

[10] National Computer Security Center, "*A Guide to Understanding Security Modeling in Trusted Systems*," NCSC-TG-010, October 1992.

[11] Common Criteria Editorial Board, "*Common Methodology for Information Technology Security Evaluation Version 1.0*, August 1999.

[12] Bernard P. Zeigler, "*Theory of Modeling and Simulation*", Wiley, New York, 1976.

[13] National Computer Security Center, *Glossary of Computer Security Terms*, NCSC-TG-004, October 1988.

[14] J. W. Freeman, R. B. Neely, *On Security Policy Modelling*, COMPASS'93, Jun, 1993.

[15] Bell D.E. and La Padular L.J., "*Secure Computer Systems: mathematical foundations*", Technical Report M74-244, Vol1-2, MITRE Corp. 1974.

[16] Bell D.E. and La Padular L.J., "*Secure Computer Systems: mathematical foundations*", MTR-2547, vol1-2, MITRE Corp. 1973.

[17] 정보통신부, "정보보호시스템 공통평가기준", August 2002.

[18] Edward Amoroso, "*Fundamentals of Computer Security Technology*", Prentice-Hall, 1994.

[19] Biba K.J., "*Integrity Considerations for Secure Computer Systems*", MTR-3153, MITRE Corp. 1977.

[20] D. D. Clark, D.R. Wilson, "*A Comparison of Commercial and Military Computer Security Policies*", IEEE Symp. on Security and Privacy, IEEE, New York, 1987.

[21] Ravi Sandhu, "Lattice-Based Access Control Models", *IEEE Computer*, November 1993.

[22] Mark W.L. Dennison, "*A Methodology for Security Policy Modeling*", ACITSS, 1997.

[23] Kris Rogers, "*Education Material for Evaluation of SPM*," CYGNACOM, March 2002.

[24] Louise Huang, "*Evaluation Procedure for ADV_SPM*", Mitretek, Norvember 2002.

[25] J. JACKY, "The way of Z Practical Programing with Formal Methods", Cambridge University

Press, 1997.

[26] C. B. Jhons, "Systematic Software Development using VDM", 2nd, Pretice Hall, 1990.

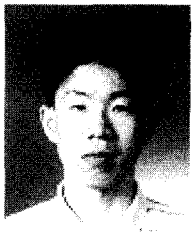
[27] Ravi S. Sandhu, Edward J. Coyne, "Role-Based Access Control Models", *IEEE Computer*, February 1996.

[28] European Commission, "*Information Technology Security Evaluation Methodology V1.0*", September 1993.

[29] Philip E. Fites, "Terry Fletcher, *Semi-Formal Firewall State Machine Model*", ACITSS, 1998.

[30] Anthony Boswell, "*Specification and Validation of a Security Policy Model*" IEEE TRANSACTION ON SOFTWARE ENGINEERING, Vol.21 No2, February 1995.

〈著者紹介〉



김 상 호 (Sang ho Kim) 정회원

1994년 : 명지대학교 전자공학과(공학사)
1997년 : 연세대학교 전자공학과 석사(공학석사)
2002년 : 연세대학교 컴퓨터산업공학과 박사과정수료
1994년~1996년 3월 : 한국생산기술연구원 연구원
1996년 7월~현재 : 한국정보보호진흥원 선임연구원
<관심분야> 정보보호제품 평가, 공통평가방법론, 프로세스 기반 보증성 평가

임 춘 성 (Choon seong Leem) 정회원

1985년 : 서울대학교 산업공학과(공학사)
1987년 : 서울대학교 산업공학과(공학석사)
1992년 : 미국 Univ. of California at Berkeley 산업공학과 박사
1993년~1995년 : 미국 Rutgers Univ. 산업공학과 조교수
1995년~현재 : 연세대학교 컴퓨터산업공학과 부교수
<관심분야> 정보보호제품 평가, 기업 정보화 수준 평가, 기업 정보보호 수준 평가