PP의 보안환경을 위한 가정문장 생성방법

A Assumptions Statement Generation Method for Security Environment of Protection Profile

고 정 호* 이 강 수**
Jeong-Ho Ko Gang-Soo Lee

요 약

본 논문에서는 PP내의 보안환경 부분 중 환경에 대한 가정문장을 작성하는 방법을 제시한다. CC에서 가정에 관련된 요구사항을 살피고, 기존 PP들에서 실제 사용한 가정문장과 NIST의 PKB내의 가정문장을 토대로 하여 새로운 "일반 가정문장 목록"과 이를 이용한 가정문장 생성 방법을 제시하였다.

Abstract

This paper presents a new assumptions statement generation method for developing TOE security environment section of PP. We surveyed on guides on the assumption statement in CC scheme, and collected and analyzed hundred of assumption statements which are in 26 certified and published real PPs and CC Toolbox/PKB. The CC Toolbox/PKB is included a class of pre-defined assumption statements. From the result of the survey, we developed a new generic assumption statement list, and proposed a assumption derivation method by using the list.

Keyword : Information security system evaluation, CC, Protection profile, Security environment, Assumptions statement

1. 서 론

조직이나 개인의 모든 업무에서 정보시스템에 대한 의존도가 커질수록, 조직내의 자원과 정보시스템을 보호하는 정보보호시스템이나 정보보호제품의 보안성이 중요해진다. 따라서, 정보보호시스템이나 제품의 보안성에 대한 평가와 인증이 필요하므로, 국내에서는 침입차단 및 침입탐지시스템 평가기준을 운영하고 있다. 또한, 각 선진국에서는 CC(common criteria)를 이용하여 다양한 시스템과 제품을 평가하고 있으며, 다양한 PP(protection profile)가 개발되어 제품 구현 전 개발단계와 평가에 활용하고 있다.

PP를 개발하기 위해서는 CC에서 표준화한 내용에 따라 세부사항을 개발해야한다. 특히, PP 내의 보안환경 부분은 TOE의 환경에 관한 가정, 자산에 대한 위협, 조직의 보안정책 문장들로 구성되며, 본 논문에서는 이들 중 "환경에 대한 가정문장"을 작성하는 방법을 제시한다.

"환경에 대한 가정문장"을 작성하는 방법에 대한 기존의 연구는 매우 부족하다. 다만 CC, CEM 및 PP/ST 작성지침에 가정문장의 평가기준과 생성지침이 수록되어있고, 기존의 PP들에서는 가정문장들을 실제로 사용하고 있다[1,2,3]. 또한, NIST에서 PP의 개발을 지원하는 도구로 개발한 CC ToolBox에서 사용하는 PKB(Profiling Knowledge Base)에는 실제로 사용할 수 있는 표준 가정문장 목록이 있을 뿐이다[4,5].

이들 자료는 PP개발시의 가정문장 작성 지침정도이며 어떻게 가정을 세워야하는지에 대한 상세한 방법이 제시되어있지는 않다. PP개발시의 가정문장을 작성하는 방법을 제시하기 위해, 본 논

* 정 회 원 : 영진전문대학 컴퓨터정보기술계열 교수
jhkont@yjc.ac.kr(제 1 저자)
** 정 회 원 : 한남대학교 컴퓨터공학과 정교수
gslee@eve.hannam.ac.kr(공동저자)

문에서는 기존 PP들에서 실제 사용한 가정문장과 PKB내의 가정문장을 조사 및 분석하고, CC에서 추천하고 있는 가정문장의 생성에 대한 요구사항을 분석하였고, 이를 토대로 "일반 가정문장 목록"과 이를 이용한 가정문장 생성 방법을 제시한다. 제시한 방법은 객체지향적이며 기존의 가정문장을 통합하는 전략을 바탕으로 하고 있다.

본 논문의 2장에서는 가정문장에 관련된 요구사항들과 조사하고 PP개발을 위한 기존의 가정문장들을 조사 및 분석하였고, 3장에서는 가정문장에 관한 요구사항을 고려하여 PP를 위한 가정문장의 생성방법을 "일반 가정문장 목록"과 함께 제시한다. 끝으로, 4장에서는 제시한 방법의 특성을 분석하고 결론을 맺는다.

2. 기존의 가정문장

2.1 가정문장에 대한 CC의 요구사항

PP는 정보보호제품(TOE)의 제품군별 공통 보안관련 요구사항 명세서라 할 수 있다. 특정한 TOE 제품군(예: 스마트카드)을 위한 PP를 개발하기 위해서는 먼저, TOE의 보안필요성을 도출하기 위해서 "보안환경" 부분을 작성해야한다. 특히, 환경에 관한 가정은 PP 및 TOE 평가시의 공리(axiom)의 역할을 한다. 보안환경 부분 내에서 다음과 같이 "환경에 관한 가정"문장을 작성해야 한다.

- TOE가 정보보호 제품(즉, 솔루션)일 경우 : TOE가 사용되거나 사용이 예상되는 조직(또는, 환경, 응용)의 환경에 관련된 가정을 고려한다. 예를 들어, 스마트카드의 경우 금융관련 조직의 가정을 고려할 수 있다.
- TOE가 특정 조직의 정보보호시스템으로 사용중인 경우 : 해당 조직의 환경에 대한 가정을 고려한다.

환경에 관한 가정문장의 작성과 관련하여 CC, CEM 및 PP/ST 작성가이드에서는 다음과 같은 지침을 제시하고 있다[1,2,3]. 이는 PP 개발시의 환경에 관한 가정문장의 요구사항에 해당한다.

(1) TOE의 의도된 사용에 대한 가정

TOE의 응용에 대한 가정, TOE가 보호해야할 자산의 가치 및 TOE의 한계(제약조건)에 대한 가정을 기술해야 한다.

(2) TOE의 사용환경에 대한 가정

환경에 대한 가정을 다음과 같이 물리적, 인적 및 접속적 측면으로 각각 분리하여 작성한다.

- 물리적 측면 : TOE 또는 부속 주변장치의 물리적 위치에 관한 가정이다. 예를 들어, "관리자 콘솔은 오직 관리원만으로 제한된 영역 내에 있다고 가정한다"와 "TOE의 파일저장소는 TOE가 실행되는 워크스테이션 상에 있다고 가정한다"는 물리적 측면의 가정문장이다.
- 인적 측면 : 사용자와 관리자 또는 TOE의 환경 내의 기타 개인(잠재적 위협원 포함)에 관한 가정이다. 예상되는 사용자 직무의 유형, 사용자의 일반적인 책임 및 이들 사용자들이 갖는 신뢰도 등에 관한 가정이 포함된다. 예를 들어, "사용자는 특정한 기술과 전문성을 갖는다고 가정한다", "사용자는 최소한의 허가(clearance)를 갖는다고 가정한다" 및 "관리자는 바이러스 퇴치 DB를 주기적으로 갱신한다고 가정한다"는 인적 측면의 가정이다.
- 접속적 측면 : TOE와 TOE 외부의 정보기술 시스템/제품(하드웨어, 소프트웨어, 펌웨어 또는 이들의 결합)간의 접속에 관한 가정이다. 예를 들어, "TOE가 생성한 로그파일을 저장하기 위해 최소한 100MB의 외부 디스크 공간이 가용하다고 가정한다", "TOE는 오직 특정 워크스테이션에서 실행되는 OS가 아닌 응용일 뿐임을 가정한다", "TOE의 플로피 디스크 드라이버는 비활성화(disable)되어 있다고 가정한다", "TOE는 신임되지 않은 네트워크에 접속하지 않는다

고 가정한다" 및 "침입차단시스템을 통해서만 사설망과 위해가능한(hostile) 외부망이 접속되도록 구성해야한다"는 접속적 측면의 가정이다.

(3) 가정에 대한 주요지침

가정에 관련된 주요 지침은 다음과 같다.

- 가정들은 TOE의 소비자가 그들의 의도된 사용(환경)과 가정이 일치하는지 결정할 수 있도록 충분하고 상세히 설명해야한다.
- 정형적으로 파악된 가정은 보안목적에 의해 확인(uphold) 될 수 있어야한다.
- 해당 보안목적을 추적할 수 없는 일반적인 가정은 PP내에서 설명문으로 처리한다.
- PP 개발과정 전체동안 가정을 추가 또는 삭제한다.
- 보안정책 문장과 중복되는 가정은 가정문장으로 처리한다.
- 특정한 TOE의 보안기능의 효과적인 사용에 관련되고, 근거의 작성과정에서 파악한 가정은 비정보기술 환경에 대한 보안요구사항으로 처리한다.

2.2 기존 PP에서의 가정문장

실제의 PP에서는 가정문장을 어떻게 작성하였는지를 보기 위해 본 연구에서는 26종의 PP에서 사용된 가정문장을 발췌 및 분석하였다. 표 1은 본 연구에서 조사한 PP의 정보를 보이며 각 PP의 가정문장을 분석하였다[6~31]. PP들은 CC 홈페이지(*http://www.commoncriteria.org/site_index.html*)에서 입수할 수 있다.

〈표 1〉 본 연구에서 분석한 PP의 종류

제품군	종수	참고문헌
DB	1	[6]
네트워킹	7	[7-13]
OS	4	[14-17]
접근통제	8	[18-25]
침입탐지	3	[26-28]
스마트카드	1	[29]
우편물승인	1	[30]
생체인증	1	[31]

2.3 PKB에서의 가정문장

NIST에서는 PP의 작성을 지원하는 도구로서 CC ToolBox와 이를 위해 '미리 정의된' 위협, 공격, 보안, 목적, 가정 및 정책문장 데이터베이스인 PKB를 개발 및 공개하고 있다[4,5]. PP의 개발자는 CC ToolBox를 이용하여 PKB내에 미리 정의된 문장들 선택하여 PP를 쉽게 구성할 수 있게 하고있다.

3. 가정문장 생성방법

3.1 기존의 문제점과 해결 전략

(1) 기존의 문제점

기존 PP들의 가정문장을 보면 그 수준이 다양하며(예: 네트워크 제품에서 "A.ADMIN 사이트는 상주 시스템과 보안 관리자가 존재하며, 조직의 중대한 역할과 많은 의무가 주어짐"과 "A.INFO_SECURITY_OFFICER 정보 보안담당자는 사이트 보안정책 및 과정의 일관된 구현을 생성, 유지, 해석 및 감독할 책임"의 상위수준의 가정이라 할 수 있다.), 가정간에 중복된 내용(예: 데이터베이스 제품에서 "A.TOE.CONFIG TOE는 평가된 설정에 따라 설치, 형성 및 관리"와 "A.SYS.CONFIG 안전한 환경에서 설치 및 관리"는 중복되어 있다)이 존재한다.

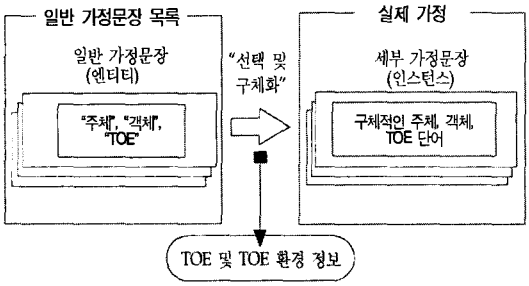
PKB내의 가정들의 경우, CC에서 권고하고 있는 3가지 가정의 분류(즉, 물리적 가정, 인적가정, 접속적가정)와 일치하지 않으며(예: "Procedures(절차적 보안) TOE의 적절한 관리를 보장하기 위한 절차"내의 세부가정들은 물리적, 인적 또는 접속

적 가정 중 어느 곳에 포함해야 할지의 문제가 발생함), 하나의 세부가정이 다수의 가정 클래스에 포함되므로 중복이 있다(예: Admin(관리자 가정) 내의 Admin_Motive(시스템 관리자의 동기)내의 "Admin_Cor_Usr_Data(통과중인 자료의 변조) 시스템 관리자는 시스템으로부터(으로) 통과중인 자료를 변조할 수 있는 능력을 갖는다"는 Data(가정된 보호)내에도 존재한다).

(2) 해결 전략

본 논문에서는 위와 같은 문제점들을 해결하기 위해 다음과 같은 접근방법을 이용할 것이다.

- 객체지향적(object-oriented) 가정문장 생성 : 객체지향 개념을 사용해, 그림 1처럼 미리정의한 '일반(generalization, generic) 가정문장 목록'내의 '일반 가정문장'을 선택하고 구체화하여 '세부(specialization, instantiation) 가정문장'을 도출한다. 예컨대, "A.Locate_Physical TOE의 객체는 물리적으로 안전한 장소에 위치한다고 가정한다"는 "A.Locate_Physical TOE의 서버는 물리적으로 안전한 장소에 위치한다고 가정한다"로 구체화 할 수 있고, "A.Function_Certification TOE에는 TOE 주체에 대한 인증기능을 제공한다고 가정한다"는 "A.Function_Certification TOE에는 TOE 사용자에 대한 인증기능을 제공한다고 가정한다"로 구체화 할 수 있다.
- 기존의 가정문장을 통합: 기존 PP의 가정문장과 PKB의 가정문장을 통합함으로서 가정문장이 기존의 PP나 PKB와 "호환성"이 유지될 수 있으며, 기존의 가정문장들을 "일반화"할 수 있다.



〈그림 1〉 객체지향적 가정문장 생성 방법

3.2 가정문장의 작성 과정

가정문장은 PP 및 TOE의 공리에 해당하며 위협문장의 수를 결정짓는다. 즉, 가정이 없다면 위협문장의 수는 무한대가 되며, 모든 위협이 없다고 가정하면 위협문장은 존재하지 않는다. 따라서, 적절한 가정을 통해 위협문장의 수를 조정하는 것이 필요하다.

적절한 가정을 도출하기 위해 앞 절에서 제시한 해결전략에 따라서 PP를 위한 실제의 가정을 작성한다. 표 2는 각 단계의 세부활동, 참조 및 입력물, 결과물 및 방법을 나타낸다. 미리정의한 '일반 가정문장 목록'은 부록에서 제시한다.

먼저, 단계 1에서는 보안환경을 파악하는 단계로 TOE관련자료와 전문가로부터 TOE와 TOE 응용에 대한 환경에 대한 정보를 파악한다. 단계 2는 일반 가정문장을 선택하는 단계로 TOE전문가의 자문을 통해 '일반 가정문장 목록'에서 각 클래스별(인적가정, 물리적/기능적 가정, 접속적/통신적 가정)로 일반 가정문장을 선택한다. 단계 3은 세부 가정문장을 도출하는 단계로 일반 가정문장내의 일반용어(예: 객체, 주체, TOE 등)를 구체적인 용어(예: 관리자, 사용자, 인증자료, 응용자료, 스마트카드 등)로 대치하여 TOE에 특화된 세부 가정문장을 작성한다. 끝으로 단계 4에서는 세부 가정문장을 검토하는 단계로 다음 과정을 PP의 전체 개발기간동안 반복적으로 실시하여 잘 정의된(well formed) 실제가정문장을 생성한다.

- 세부가정문장과 정책가정 문장과의 중복성을 파악한다.
- 세부가정문장과 중복되는 정책문장은 가정문장으로 처리한다.
- 문장간의 일관성을 체크하고 일관성을 갖도록 한다.
- 가정문장을 다듬어 문장의 조리성을 제고한다.

〈표 2〉 가정문장의 작성과정

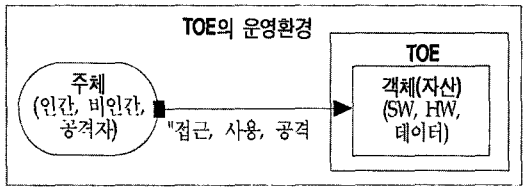
단 계	활 동	참조 및 입력물	결 과 물	방 법
1. 보안 환경 파악	TOE 및 TOE 응용에 대한 환경을 파악함	TOE 전문가, TOE 자료	-	자문, 자료 검토
2. 일반 가정문장 선택	'일반 가정문장 목록'에서 다음의 클래스별로 일반 가정문장을 선택함 - 인적가정: 관리자(감사자)의무, 관리자 태도, 사용자, 공격자를 파악함 ("주체"에 해당함) - 물리적 및 기능적 가정 파악 - 접속적 및 통신적 가정 파악	TOE 전문가, '일반 가정문장 목록'	일반 가정 문장	자문, 자료 검토
3. 세부 가정문장 도출	일반 가정문장내의 일반용어(예: 객체, 주체, TOE 등)를 구체적인 용어(예: 관리자, 사용자, 인증자료, 응용자료, 스마트카드 등)로 대치함	TOE 전문가	세부 가정 문장	자문
4. 세부 가정문장 검토	- 정책가정 문장과의 중복성을 제거함 - 가정과 중복되는 것을 가정으로 처리함 - 문장간 일관성 유지 - 문장의 조리성 제고 - PP개발 전체기간 동안 실시	PP의 보안정책 문장, 위협문장	실제 가정 문장	자료 검토

3.3 일반 가정문장 목록

(1) 용어 정의

- 주체(subject) : TOE와 TOE의 운영환경에 관련된 인간 또는 프로그램, 시스템(예: TOE의 사용자, TOE의 관리자(스텝), TOE 운영환경의 사용자, TOE 운영환경의 관리자(스텝), 감사자, 개발자, 평가자 등)
- 객체(object) : 주체와 직접 또는 간접적으로 연관된 자산(예 : 인증데이터, 사용자데이터, 보안장비, 하드웨어, 통신망 등)
- TOE : PP의 작성대상 정보보호 제품 또는 시스템(예: OS, DB, 네트워킹, 접근통제, 침입차단시스템, 침입탐지시스템, 바이러스 방지, 스마트카드, 생체인증 등)
- TOE의 운영환경: TOE를 적용하여 운영하는 정보시스템(예 : 인사관리시스템, 환자관리시스템, 재무관리시스템, 전자상거래시스템, 정보제공시스템 등). TOE로 통칭함.

(그림 2)는 용어들간의 관계를 보인다.



〈그림 2〉 용어간의 관계

(2) 일반 가정문장 목록

부록에서 기술한 '일반 가정문장 목록'은 3.1절에서 제시한 해결전략에 기반하여 다음 과정을 통해 작성하였다.

① 26종의 기존 PP와 PKB 내의 가정문장을 분석하고 분류함

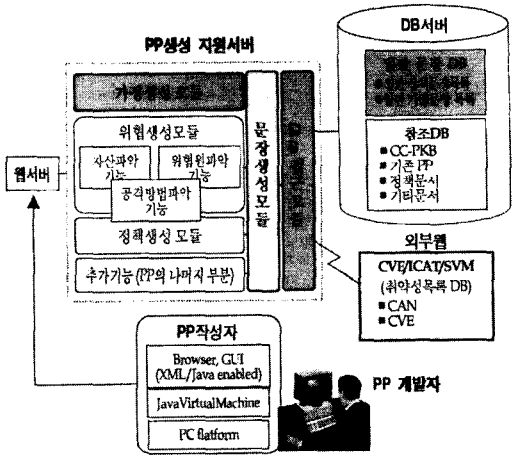
② 가정문장을 재분류함 (그림 3 참조)

③ "주체", "객체", "TOE" 등과 같은 일반용어를 사용해 '일반 가정문장'들을 작성함

④ 각 '일반 가정문장별로' 대응되는 기존 PP와 PKB내의 가정문장을 "[적용사례]"를 통해 보임(예 : "적절한 관리자(운영자, 감사원포함)배정<AC3>"은 "적절한 관리자(운영자, 감사원포

- 인적 가정(TOE 내의 주체)
  - 관리 및 감사자
    - 관리자 의무(Duty)
    - 관리자 태도
  - 사용자(User)
  - 공격자(Attacker)
- 물리적 및 기능상의 가정
  - 물리적 위치(Location)
  - 기능(Function)
- 접속 및 통신적 가정
  - 접속(Connection)
  - 통신(Communication)

〈그림 3〉 일반 가정문장 목록의 스키마



〈그림 4〉 PP개발 지원도구의 구조

함) 배정"이라는 가정문장이 PP번호 <AC3>에 있음을 나타내며, 여기서, "< >"내의 내용은 표 1의 실제 PP의 식별자임)

⑤ 일반가정문장 모두를 선택한다면, TOE에는 보안문제가 전혀 발생하지 않으며, 가정을 하지 않는다면 수많은 보안문제가 발생한다.

⑥ 어떤 가정클래스의 모든 세부가정을 선택할 때는 "대표가정"(부록의 일반가정목록내의 박스내의 가정문장)만을 사용한다.

3.4 지원도구의 구조

3.2절에서 제시한 가정 문장의 작성방법은 지원도구를 통해 부분적으로 자동화가 가능하다. 지원도구를 사용하는 경우의 각 단계별 시나리오는 다음과 같다.

① 보안환경 파악단계: 미리 구성해 놓은 "참조DB"로부터 TOE 및 환경자료를 검색하며 자문대상자(TOE 전문가)를 검색하고 자문일정을 조정한다. 이메일을 통해 자문을 실시할 수 있다.

② 일반 환경문장 선택단계: 미리 구성해 놓은 "일반 가정문장 목록"으로부터 가정문장 클래스별로 "일반 가정문장"들을 GUI와 DB를 통해 선택한다.

③ 세부 가정문장 도출단계: 문장 편집기를 통해 "일반 가정문장"내의 일반용어(주체, 객체, TOE 등)를 구체적인 용어로 대체한다.

④ 세부 가정문장 검토단계: 문서편집기의 단어 검색 기능을 통해 문장 간의 중복성과 일관성을 체크하고 보안정책문장들과의 중복성을 체크하여 중복된 문장은 가정문장으로 간주한다.

이러한 시나리오에 근거하여 설계된 가정문장 생성 지원도구의 구조는 그림 4와 같다. 그림에는 가정문장 뿐 아니라 보안정책 및 위협문장 생성 기능도 포함된다.

4. 분석 및 결론

PP작성시의 환경에 관한 가정을 기술하는 방법은 구체적으로 알려져 있지 않으며 주로 경험에 의존하고 있는 실정이다. 이에 따라, 가정들의 수준이 일정하지 않고 가정들간의 중복성 및 일관성이 결여될 수 있다.

가정문장은 PP 및 TOE의 공리에 해당하며 위협문장의 수를 결정짓는다. 즉, 가정이 없다면 위협문장의 수는 무한대가 되며, 모든 위협이 없다고 가정하면 위협문장은 존재하지 않는다. 따라서, 적절한 가정을 통해 위협문장의 수를 조정하는 것이 필요하다.

본 논문에서 제시한 "가정문장의 작성 과정"은 CC ToolBox와 PKB를 보완한 것이며, "일반 가정문장 목록"은 CC에서의 가정에 관련된 요구사항을 준수하여 PKB와 기존의 PP에서 사용된 가정을 보완한 것이다[1~31]. 표 3에서는 본 논문에서 제시한 "일반 가정문장 목록"과 PKB의 가정문장 목록을 비교하고 있다.

본 논문은 다음과 같은 독자적인 접근방법을 이용하고 있다.

- 객체지향적(object-oriented) 가정문장 생성 및 대표가정의 개념
- 기존의 가정문장을 통합

이와 같은 접근방법은 다음과 같은 장점을 갖는다.

① PKB와는 달리 "객체", "주체", "TOE" 등과 같은 일반적인 용어를 사용한 '일반 가정문장 목록'을 제시하였고 PP 작성자는 이를 선택하여 구체적인 용어로 대치함으로써 쉽고 빠르게 실제의 가정문장을 작성할 수 있다. 또한, 작성된 가정문장의 수준을 통일할 수 있다.

② CC와 PP/ST작성 가이드에 있는 가정문장에 대한 요구사항에서는 가정을 인적, 물리적 및 접속적으로 크게 분류할 것을 권고하였으므로 본 연구에서도 이를 수용하고 있다. PKB의 경우는 분류방법이 다르다.

③ 본 연구에서는 PKB보다 2배에 가까운 71가지의 세부 가정문장을 제시하고 있으므로 선택의 폭이 넓어진다. 또한, 대표가정의 개념을 사용한다.

④ PKB의 경우 하나의 세부가정문장은 2개 이상의 가정 클래스(중간 분류)에 속하므로 혼동이 발생할 수 있지만 본 연구의 경우는 중복되어 있지 않다.

⑤ PKB와는 달리 본 연구는 26개의 실제 PP에서 사용된 가정과 PKB의 가정을 고려하여 가정문장을 구성하였으며 각 가정문장마다 기존의 가정문장을 대응시킴으로서 가정문장들은 호환성이 제고된다.

⑥ 제시한 방법을 지원할 수 있는 도구의 개발이 용이하다.

그러나, 본 연구의 주요결과인 "가정문장의 작성 과정"과 "일반 가정문장 목록"은 가급적 많은 국제표준 및 지침(CC, CEM, PP/ST작성가이드), 평가와 인증된 문서(실제 PP문서)에 근거하여 제

〈표 3〉 가정문장 스키마의 비교

스키마 / 비교기준	일반 가정문장 목록(본 논문)	PKB
스키마 구조	■인적 가정(TOE 내의 주체) ▸관리 및 감사자 - 관리자 의무 - 관리자 태도 ▸사용자 ▸공격자 ■물리적 및 기능상의 가정 ▸물리적 위치 ▸기능 ■접속 및 통신적 가정 ▸접속 ▸통신	■관리자 가정 ▸시스템 관리자의 태도 ▸시스템 관리자의 동기 ■사용자 가정 ▸사용자 동기 ■물리적 보안 가정 ■가정된 보호 ■절차적 보안 ■통신 가정
가정 클래스 수	상위 3, 중위 7, 하위 2	상위 6개, 중위 3
세부 가정문장 수	71	38
세부가정의 중복성	없음	있음

시한 것이긴 하지만, 다소 주관성이 포함되어 있을 수 있다. 또한, 아직 실제의 PP 작성시에 활용한 실적이 없으므로, 제시한 방법의 효과성이 검증되어 있지 않다. 이러한 문제점은 향후에 PP 개발자들이 본 연구결과의 활용을 통해 문제점을 발견하고 개선함으로서 다소 극복될 수 있을 것이다.

참 고 문 헌

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

[4] NIAP, *CC Toolbox Reference Manual*, Version 6.0f. http://niap.nist.gov/tools/cctool.html, 2000,

[5] NIAP, *List of Threat, Attack, Policy, Assumption, and Environment Statement Attribute*, CC Profiling Knowledge base Report, 2002. http://niap.nist.gov/tools/CCTB60f-Documentation/CC_PKB/Reports/Index.htm.

[6] Oracle, *DBMS Protection Profile*, EAL3, Issue 2.1, May 2000.

[7] NSA, *Traffic Filter Firewall Protection Profile For Medium Robustness Environments*, EAL2+, 2000.

[8] NSA, *Traffic Filter Firewall Protection Profile for Low Risk Environments (Version1.1)*, EAL2, 1999.

[9] NSA, Application *Level Firewall Protection Profile for Low Risk Environments (Version1.d)*, EAL2, 1999.

[10] BHTT, *Peer-to-Peer Wireless Local Area Network(WLAN) for Sensitive But Unclassified Environments -V0.6*, EAL3, Boozollen & Hamilton Tresys Technology, 2001.

[11] NSA, *Protection Profile for Switches and Routers*, EAL3, 2001.

[12] NSA, *A Goal VPN Protection Profile For Protecting Sensitive Information - V2.0*, EAL3, 2000.

[13] BHTT, *Infrastructure Wireless Local Area Network (WLAN) For Sensitive But Unclassified Environments*, EAL3, Boozollen & Hamilton and Tresys Technology, 2001.

[14] NSA, *Labeled Security Protection Profile Version 1.b*, EAL3, 1999.

[15] NSA, *Controlled Access Protection Profile*, EAL3, 1999.

[16] NSA, *Protection Profile for Multilevel OS - Requiring Medium Robustness*, EAL4+, 2001.

[17] NSA, *Protection Profile for Single-level OS's in Environments Requiring Medium PP*, EAL4+, 2001.

[18] NSA, *Directory for US Department of Defense Class 4 PKI PP*, EAL3. 2000.

[19] TCPA. *Trusted Platform Module (TPM) Protection Profile*, EAL2, Trusted Computing Platform Alliance, 2001.

[20] NSA, *Certificate Issuing and Management Components*, EAL4, 2001.

[21] NIST, *Role-Based Access Control Protection Profile Version 1.0*, EAL2, 1998.

[22] Authorizor Ltd, *Privilege Directed Content Protection Profile*, EAL2, Authorizor Ltd, 2001.

[23] NSA. Key Recovery for Third Party Requestors Ver. 1.0, EAL3, NSA, 2000.

[24] NSA. *Key Recovery for Agent Systems Ver. 1.1*, EAL3, 2000.

[25] NSA. *Key Recovery for End Systems Ver. 2*, EAL1, NSA, 2000.
[26] NIST, Role-Based Access Control Protection Profile Version 1.0, EAL2, 1999.
[27] NSA. *Intrusion Detection System Analyzer -Draft 3*, EAL2, NSA, 2000.
[28] NSA. *Intrusion Detection System Sensor - Draft 3*, EAL2, NSA, 2000.
[29] SCSUG, *Smart Card Protection Profile*, EAL4+, 2001.
[30] Consignia, *Postage Meter Approval Protection Profile*, EAL2+, 2001.
[31] DoD Biometrics Management Office1. *U. S. Department of Defense Biometrics Office, Biometric System. Protection Profile For Medium Robustness Environments, v0.01*, EAL4, 2001.

〈부록〉 일반 가정문장 목록

(주) 박스내의 가정문장은 해당 가정클래스의 대표 가정임

1. 인적 가정(TOE 내의 주체)

■ 관리 및 감사자

A.Admin TOE의 관리자(운영자, 감사자 포함)는 그 의무를 올바르게 수행한다고 가정한다.

▶ 관리자 의무(Duty)

A.Admin_Duty_Assign TOE에는 적절한 관리자(운영자, 감사자 포함)가 배정되었다고 가정한다.

[적용사례] 적절한 관리자(운영자, 감사원포함) 배정<AC3>. TOE, 기존 시스템 및 정보보안 관리<DB1>. 정보보안 관리를 위해 개인 존재<OS1> <OS2><AC4> <IDS1><IDS2><IDS3>

A.Admin_Duty_Audit TOE의 관리자(감사사 포함)는 감사로그를 검토하는 등의 감사업무를 안전하고 올바르게 수행한다고 가정한다.

[적용사례] 관리자(감사자)는 감사로그를 검토<AC3><Net5>, 관리자가 감사로그를 검토<PKB>

A.Admin_Duty_Auth TOE의 관리자는 사용자 인증데이터를 안전하고 올바르게 관리한다고 가정한다.

[적용사례] 관리자는 인증데이터를 관리함<AC3>, 사용자 순응(compliance)을 촉진(promoting) 하는 패스워드 관리 <PKB>

A.Admin_Duty_Comm TOE의 관리자는 TOE의 통신을 안전하고 올바르게 관리한다고 가정한다.

[적용사례] 관리자는 TOE 통신을 보안정책 제약 하에 가동<AC1>

A.Admin_Duty_Config TOE의 관리자는 TOE의 설치, 운영 및 형상을 안전하고 올바르게 관리한다고 가정한다.

[적용사례] 관리자는 TOE를 평가된 설정에 따라 설치, 형성 및 관리<DB1>, 바이러스 체크 절차<PKB>, 사용자 자료의 폐기 (정책으로)<PKB>

A.Admin_Duty_Conform TOE의 관리자는 TOE가 따라야하는 기준, 법규 및 표준에 TOE가 안전하고 올바르게 준수하도록 관리한다고 가정한다.

[적용사례] 관리자는 일치성 보증함.(Conformance guarantee)<AC2>. 관리자는 계량기내 EMI/ EMC 관련 설계는 국가의 법률 준수<POST1>

A.Admin_Duty_Env TOE의 관리자는 TOE를 안전한 환경하에서 설치 및 운영한다고 가정한다.
[적용사례] 관리자는TOE를 안전한 환경에서 설치 및 관리<DB1>. 관리자는 IT 컴포넌트를 같은 관리제어 및 보안정책 하에서 운영<DB1>
A.Admin_Duty_Policy TOE의 관리자는 TOE의 보안정책을 준수하여 TOE를 안전하고 올바르게 관리한다고 가정한다.
[적용사례] 관리자는 사이트 보안정책 및 과정의 일관된 구현을 생성, 유지, 해석 및 감독함<Net6>
A.Admin_Duty_Reaction TOE의 관리자는 보안관련 사건이 발생하면 신속 및 안전하고 정확하게 이에 이를 처리한다고 가정한다.
[적용사례] 관리자는 TOE가 실시간으로 경고를 생성하면 신속하고 적절한 행동을 수행<AC5>
A.Admin_Duty_Report TOE의 관리자는 보안관련 사건이 발생하면 신속 및 안전하고 정확하게 해당 객체의 소유자에게 보고한다고 가정한다.
[적용사례] 도난을 감지하자마자 합법적인 소유자에게 보고<AC5>
A.Admin_Duty_Role TOE의 관리자에게 보안관리에 관련된 의무와 책임이 주어진다고 가정한다.
[적용사례] 관리자는 조직의 중대한 역할과 많은 의무가 주어짐<Net6><AC1> <AC2>
A.Admin_Duty_User TOE의 관리자는 TOE의 주체(특히, 사용자)에 대해 그 역할에 따라 직무, 책임, 제한 및 자격을 부여하고 이를 안전하고 정확하게 관리한다고 가정한다.
[적용사례] 관리자는 사용자에게 역할에 따른 직무, 책임, 제한 및 자격을 부여하고 관리함<AC4> <DB1><BIO1> <OS1><SMC1>.

▶ 관리자 태도
A.Admin_Attitude_Access TOE의 관리자는 원격적으로 TOE를 관리할 수 있다고 가정한다.
[적용사례] 관리자는 원격 접근이 가능함<Net1><Net2><Net3>, 원격 관리(adminstration)<PKB>
A.Admin_ Attitude_Accident TOE의 관리자는 직무수행에 악의가 없으며 실수를 할때도 있다고 가정한다.
[적용사례] 관리자(사용자 포함)는 악의가 없고 실수가 가능함<Net1> <Net2><Net3><AC6><AC7><AC8>, 관리자 오류에 대한 잠재성(potential)<PKB>, 악의적 시스템 관리자<PKB>
A.Admin_Attitude_Audit TOE의 관리자(감사자 포함)는 감사를 위해 감사로그를 안전하고 정확하게 관리한다고 가정한다.
[적용사례] 관리자는 서버 감사로그를 자주 검사함<AC5>
A.Admin_Attitude_Backup TOE의 관리자는 안전한 장치에 TOE의 객체(특히, 데이터와 프로그램)를 백업을 실시한다고 가정한다.
[적용사례] 관리자는 백업을 위해 다른 장치를 사용함<AC5><Net6>
A.Admin_Attitude_Document TOE의 관리자는 관리자용 문서의 내용을 준수한다고 가정한다.
[적용사례] 관리자는 관리자 TOE 문서를 준수함 <IDS1><IDS2> <IDS3> <OS1><OS2>, 잘 행동하는 시스템 관리자(관리자를 위한 문서화, 유능한 시스템 관리자, 남용하지 않는 시스템 관리자와 통합)<PKB>, 관리자를 위한 문서화 <PKB>
A.Admin_Attitude_Policy TOE의 관리자는 TOE 또는 TOE의 운영환경내의 보안정책을 준수한다고 가정한다.
[적용사례] 관리자(사용자포함)는 보안정책을 준수함<Net6>, 유능한 시스템 관리자<PKB>
A.Admin_Attitude_Reliable TOE의 주체(특히, 인간)는 부여된 권한을 남용하지 않고 신뢰된다고 가정한다.
[적용사례] 관리자(모든 인가자포함)는 권한을 남용하지 않고 신뢰할만함<AC6><AC8><AC3><BIO1> <POST1><AC5>, 인증된 관리자<PKB>, 남용하지 않는 시스템 관리자<PKB>, 통과중인 자료의 변조<PKB>
A.Admin_Attitude_Secure TOE의 관리자는 물리적으로 안전한 장소에서 TOE를 관리한다고 가정한다.

[적용사례] 관리자는 물리적으로 안전한 장소에서 관리함<AC5>

A.Admin_Attitude_Trained1 TOE의 주체(특히 인간)는 그 역할을 안전하고 올바르게 수행 할 수 있도록 교육 및 훈련되어 있다고 가정한다.

[적용사례] 관리자(모든 인가자 포함)는 훈련되어 있음<Net4><Ne5> <Net6><Net7>, 훈련 안된 시스템 관리자<PKB>, 태만한 시스템 관리자(<PKB>. 관리자(운영자, 감사원포함)는 사회공학적 공격의 방어기술에 훈련되어있음<AC3>

■ 사용자(User)

A.User TOE의 사용자는 그 직무를 안전하고 올바르게 수행한다고 가정한다.

A.User_Access TOE의 사용자는 접근이 인가된 객체에 대해서만 접근을 한다고 가정한다.

[적용사례] 사용자는 인가되었을 때만 원격 접근함<Net1><Net2> <Net3> <IDS1><IDS2><IDS3>. 사용자 접근 <PKB>

A.User_AccessDirect TOE의 사용자는 간접적이 아니라 직접적으로 TOE 객체에 접근한다고 가정한다.

[적용사례] 사용자는 직접 TOE에 접근함<Net1><Net2><Net3>

A.User_Application TOE의 사용자는 TOE내의 객체(특히 응용프로그램)를 사용한다고 가정한다.

[적용사례] 사용자는 TOE 애플리케이션을 사용함<AC2>. TOE-환경 분리 <PKB>

A.User_Auth TOE의 사용자는 TOE의 인증정책에 익숙하고 이를 준수한다고 가정한다.

[적용사례] 사용자는 TOE가 운영하는 인증서 정책 및 인증실무 준칙에 정통<AC3>

A.User_Coop TOE의 사용자는 TOE의 보안정책을 협력적으로 준수한다고 가정한다.

[적용사례] 사용자는 보안정책에 협력적(준수)임<OS1><OS2><AC3> <AC1>, 협력적 사용자<PKB>

A.User_Notify TOE의 사용자는 TOE 사용중 보안문제가 발생했을 때 이 사실을 즉시 담당 주체(특히, 보안관리자)에게 보고한다고 가정한다.

[적용사례] 사용자는 보안문제 발생시 적절한 기관에 통보함<AC3>

A.User_Owner TOE의 사용자는 인증데이터와 같은 데이터의 소유자라 가정한다.

[적용사례] 사용자(사용자 집합)는 데이터 객체의 소유자임<AC4>, 사용자가 패스워드에 접근<PKB>

A.User_Reliable TOE의 사용자는 신뢰할만하며 협력적이라 가정한다.

[적용사례] 사용자는 신뢰할만함<Net6><Net7>, 신임된 사용자<PKB>

■ 공격자(Attacker)

A.Attacker TOE의 공격자는 충분한 공격동기, 공격도구를 가지며 객체에 공격을 효과적으로 실시한다고 가정한다 .

A.Attacker_Asset TOE의 공격자는 가치있는 TOE의 객체(자산)에 대해 공격을 실시한다고 가정한다.

[적용사례] 공격자는 자산에 대해 침투 및 공격을 함<AC4>, 시스템 자료의 변조(corruption) <PKB>

A.Attacker_Insident TOE의 공격자는 악의를 가진 TOE의 주체(특히, 사용자)라 가정한다.

[적용사례] 공격자는 악의를 가지는 사용자임<AC2>, 악의적 사용자 <PKB>. 악의 있는 공격 위협을 고려함 <Net1><Net3>

A.Attacker_Accident TOE의 공격자는 악의가 없으며 실수를 할 수 있는 TOE의 주체(특히, 사용자)라 가정한다.

[적용사례] 사용자의 실수<PKB>

A.Attacker_Bypass TOE의 공격자는 TOE를 우회하여 공격한다고 가정한다.

[적용사례] 공격자는 TOE의 외부로부터 우회 공격함<Net6>, 원격 사용자<PKB>

A.Attacker_MalCode TOE의 공격자는 바이러스와 같은 악의적 코드를 제작 및 배포한다고 가정한다.
[적용사례] 공격자는 악의적 코드를 제작 및 배포함<AC3>, SW 바이러스 스캐닝<PKB>
A.Attacker_Motive TOE의 공격자는 [상, 중, 하]수준의 공격 동기를 갖는다고 가정한다.
[적용사례] 공격자는 **수준의 공격동기를 가짐<AC1>
A.Attacker_Resource TOE의 공격자는 [상, 중, 하]수준의 자원(계산능력, 메모리, 시간)을 갖는다고 가정한다.
[적용사례] 공격자는 ** 수준의 가용자원(계산능력, 메모리, 시간)을 가짐<AC1><Net1><Net2><Net3><Net4><Net5><Net6><Net7>
A.Attacker_Technique TOE의 공격자는 [상, 중, 하]수준의 공격기술을 갖는다고 가정한다.
[적용사례] 공격자는 **수준의 전문기술을 가짐<AC1><AC2><Net5>, 전문가 위협원 (위협으로)<PKB>, 일반인(laymen) 위협원 (위협으로) <PKB>, 능숙한(proficient) 위협원<PKB>
A.Attacker_Vul TOE의 공격자가 TOE의 취약성을 탐지만하려 할 때는 이를 위협으로 간주하지 않는다.
[적용사례] 취약성 탐지만을 목적으로 하는 공격 위협은 고려하지 않음<Net2>

2. 물리적 및 기능상의 가정

■ 물리적 위치(Location)

A.Locate TOE는 올바르고 안전한 위치에 존재한다고 가정한다.

A.Locate_Client TOE는 그 클라이언트의 위치가 결정되어있다고 가정한다.
[적용사례] TOE 클라이언트의 공동위치 결정<Net4><Net7>
A.Locate_Address TOE는 IT시스템의 주소(IP 주소)를 변경할 수 있다고 가정한다.
[적용사례] TOE가 IT 시스템 주소를 변경<IDS1>
A.Locate_Detection TOE의 오용탐지 매커니즘은 TOE외부에 위치한다고 가정한다.
[적용사례] 오용탐지(MD) 매커니즘은 TOE의 외부에 위치함<Net6>. 통신 보호 <PKB>
A.Locate_Environ TOE의 환경은 보안공격에 취약하다고 가정한다.
[적용사례] 환경은 취약성의 탐지를 위한 공격위협에 취약함<Net4><Net7>. 환경의 보호<Net5>
A.Locate_Physical TOE의 객체는 물리적으로 안전한 장소에 위치한다고 가정한다.
[적용사례] TOE는 물리적 접근을 방지하기 위해 제어된 접근장치 내에 위치<OS1><OS2><IAC4> <IDS1><IDS2> <IDS3>. TOE는 물리적으로 안전 <Net1><Net2><Net3>. 보안정책 시행에 중요한 TOE H/W, S/W 및 펌웨어는 무인가적인 물리적 변경으로부터 보호 <AC1><Ac2><AC3> <AC8>. TOE 접근점 구성은 무인가적인 물리적 접근으로부터 물리적 보호 <Net4><Net5> <Net7>. 무인가 물리적 접근 방지<DB1>. 적절한 물리적 보안 제공 <OS3> <OS4>. 기관사용자 사이트에서 TSE의 물리적 보안은 기밀 취급받지 않는 민감한 정보 보호에 충분 <Net6>. H/W와 S/W의 무인가적인 물리적 수정으로부터 보호<IDS1><IDS2> <IDS3> <AC4> <OS1><OS2>. 물리적 접근)<PKB>. 자연재해로부터의 보호<PKB>. 외부자로 부터의 TOE 보호<PKB>
A.Locate_Scope TOE는 정보시스템과 [같은, 다른] 범위(영역)에 위치한다고 가정한다.
[적용사례] IT 시스템에서의 TOE의 범위<IDS1>

■ 기능(Function)

A.Function TOE는 보안관련기능을 올바르게 제공한다고 가정한다.

A.Function_Access TOE에는 TOE 내의 객체로의 접근기능을 제공한다고 가정한다.
[적용사례] TOE는 IT 시스템 데이터에 접근<IDS1><IDS2><IDS3>. 시스템 기술<AC2>
A.Function_Certification TOE에는 TOE 주체에 대한 인증기능을 제공한다고 가정한다.
[적용사례] 개체 인증<AC2>
A.Function_Crypto_Support TOE는 암호 지원기능을 갖는다고 가정한다.
[적용사례] 암호의 기반구조는 TOE의 처리와 외부 메커니즘 제공<Net6>
A.Function_Crypto_Conform TOE는 따라야할 암호표준을 준수한다고 가정한다.
[적용사례] 암호화 연산은 FIPS 140-1 Level 3 준수 암호모듈 사용<AC1> <AC7>. 암호화 연산에 사용되는 암호모듈은 FIPS 140-1 level 1 준수<AC8>
A.Function_Crypto_KeyIssue TOE는 사용자에 대해 암호키 발급기능을 갖는다고 가정한다.
[적용사례] 클라이언트 활성화 키 발행시 사용자 키의 수신에 대한 응답<AC5>
A.Function_Crypto_KeyReport TOE는 사용자에 대해 암호키 보고기능을 갖는다고 가정한다.
[적용사례] 권한부여에 실패시 클라이언트 활성화 키를 사용자에게 보고<AC5>
A.Function_Crypto_KeySuport TOE는 사용자에 대해 암호키 지원기능을 갖는다고 가정한다.
[적용사례] 암호화키의 안전한 지원<SMC1>
A.Function_Crypto_Streng TOE는 충분한 강도의 암호기능을 갖는다고 가정한다.
[적용사례] TOE에 사용된 암호화 기법은 암호분석 공격을 방지하며, 민감한 데이터 보호에 적절한 강도<Net6>. 견고한 암호화<Net5>
A.Function_OS TOE는 안전한 운영체제상에서 실행된다고 가정한다.
[적용사례] 운영체제는 적절한 보안수준의 감지된 위협에 대응하는 기능을 제공하도록 선택<AC3>. OS 운영체제는 보안서비스를 수행하는 TOE에 의존<AC6><AC7><AC8>
A.Function_Output TOE는 모든 출력물에 대해 보안수준을 표시한다고 가정한다.
[적용사례] 모든 출력의 민감도 수준 표시<OS1>
A.Function_PKI TOE는 PKI관련 기능을 제공한다고 가정한다.
[적용사례] PKI는 X.509 인증서의 클래스 3 또는 4를 제공<Net4><Net7>
A.Function_Platform TOE는 안전한 하부구조상에서 실행된다고 가정한다.
[적용사례] 운영체제, 하드웨어 및 부가된 통신망은 적절하게 설치, 구성 및 운영되고 요구되는 용량을 만족<AC1>. TOE의 기존 정보기술 환경은 TOE의 안전한 운영을 손상시키는 취약성을 포함하지 않음<Net4> <Net7>. TOE는 믿을 수 있는 접근 설비 내에서 작동<AC6><AC7>
A.Function_Power TOE는 전력 및 클럭 중단에 대한 복구기능을 갖는다고 가정한다.
[적용사례] CAD의 전원 및 클록 사용<SMC1>. 전력 중단으로부터의 보호<PKB>
A.Function_Recovery TOE는 고장발생에 대한 복구기능을 갖는다고 가정한다.
[적용사례] 고장이 발생시 TSE에 서비스를 빨리 복구 가능하도록 구현<Net6>
A.Function_Root TOE는 시스템의 루트에 대한 보호기능을 갖는다고 가정한다.
[적용사례] 루트에 대한 대책<AC2>
A.Function_Store TOE는 안전하게 데이터를 저장하는 기능을 갖는다고 가정한다.
[적용사례] TOE 외부에 데이터를 저장<SMC1>. 사용자의 생체인증 템플릿은 카드에 전송 및 저장시 적절한 보안 대책<BIO1>
A.Function_Tempest TOE는 하드웨어공격을 대처할 수 있도록 설계되었다고 가정한다.
[적용사례] TOE 데이터의 위험이 최소가 되도록 TOE 설계<Net6>

3. 접속 및 통신적 가정

■ 접속(Connection)

A.Connect TOE는 다른 시스템과 안전하게 접속 및 상호 운용된다고 가정한다.

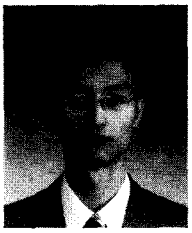
A.Connect_Potal TOE내의 하나의 보안장벽을 통과한다면 TOE 객체는 보호되지 않는다고 가정한다.
[적용사례] 하나의 포털을 통과한다면 자산은 보호되지 않음<BIO1>
A.Connect_Availability TOE는 인터넷, PSTN등 통신인프라를 언제든지 사용할 수 있다고 가정한다.
[적용사례] 인터넷, PSTN 또는 다른 공중 네트워크 연결은 필요할 때 이를 사용가능<Net6>
A.Connect_Conf TOE는 사전에 설정된 통신망구조를 갖는다고 가정한다.
[적용사례] TOE는 유선 네트워크와 연결안됨<Net4><Net7>. TPM 설정<AC2>. 다른 시스템으로 접속(정책으로) <PKB>
A.Connect_Device TOE는 접근장치를 통해서 주변장치에 접속되어 있다고 가정한다.
[적용사례] 주변장치로의 모든 연결은 접근장치로 제어<AC4><OS1> <OS2>
A.Connect_Public TOE는 호스트관련 데이터를 공개하지 않는다고 가정한다.
[적용사례] 호스트 데이터를 공개하지 않음<Net1><Net2><Net3>
A.Connect_Remote TOE는 보다 낮은 보안수준으로부터의 접근을 제한한다고 가정한다.
[적용사례] 위협수준이 높은 원격 사용자로부터의 접속을 제한함<Net6>
A.Connect_TOE 정보시스템상의 모든 정보는 반드시 TOE를 통과한다고 가정한다.
[적용사례] 정보는 반드시 TOE를 통과함<Net1><Net2><Net3>

■ 통신(Communication)

A.Comm TOE내부 및 TOE외부와 통신은 안전하다고 가정한다.

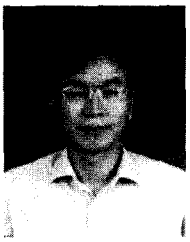
A.Comm_Protect TOE내부 및 TOE외부와 통신은 물리적으로 보호되어있다고 가정된다.
[적용사례] 통신 실패에 대하여 시스템은 물리적으로 보호<AC3>. 통신의 물리적 보호<PKB>
A.Comm_Protocol TOE내부 및 TOE외부와 통신은 안전한 프로토콜을 통해 실행된다고 가정한다.
[적용사례] 통신망 서비스는 안전한 프로토콜 기반<DB>
A.Comm_Secure TOE내부 및 TOE외부와 통신은 안전하게 이루어진다고 가정한다.
[적용사례] CAD(Card Acceptor Device)의 안전한 통신<SMC1>. 외부인이 엿듣기(eavesdrop)<PKB>

◐ 저 자 소 개 ◑



고 정 호

1997년 한남대학교 전자계산공학과 졸업(학사)
1999년 한남대학교 대학원 컴퓨터공학과 졸업(석사)
2002년 한남대학교 대학원 컴퓨터공학과 졸업(박사)
2002년~현재 : 영진전문대학 컴퓨터정보기술계열 교수
관심분야 : 정보보호시스템, 네트워크보안, 소프트웨어공학
E-mail : jhkont@yjc.ac.kr



이 강 수

1981년 홍익대학교 전자계산학과 졸업(학사)
1983년 서울대학교 대학원 전산학과 졸업(석사)
1989년 서울대학교 대학원 전산학과 졸업(박사)
1987년~현재 : 한남대학교 컴퓨터공학과 정교수
관심분야 : 소프트웨어공학, 병행시스템 모델링 및 분석, 보안공학, 정보보호시스템 평가, 멀티미디어교육 커리큘럼
E-mail : gslee@eve.hannam.ac.kr