情報保護學會論文誌
第13券 第4號, 2003. 8

PP 개발을 위한 보안정책 문장 생성방법

고 정 호*, 이 강 수**

A Security Policy Statements Generation Method for Development of Protection Profile

Jeong-Ho Ko*, Gang-Soo Lee**

요 약

보호프로파일(PP)은 특정제품군에 대한 공통 보안기능 및 보증 요구사항 명세서라 할 수 있다. 특히, PP내의 TOE (평가대상물) 보안환경 부분은 TOE의 물리적 환경, 보호해야할 자산 및 TOE의 용도를 분석하여 가정사항, 위협 및 보안정책을 기술해야한다. 본 연구에서는 PP내의 보안환경 부분 중 보안정책을 개발 또는 작성하는 방법을 제시한다. 정보보호부문에서의 보안정책에 대한 표준이나 지침을 조사 및 분석하여 보안정책 문서와 관련된 기반개념을 정리하고, 기존 PP들에서 실제 사용한 보안정책 문장, 미 국방부의 보안정책 문장, CC의 기능 및 보증요구사항 클래스를 조사 분석하였으며, 이를 토대로 하여 새로운 일반 보안정책 문장 목록과 이를 이용한 보안정책 문장 생성방법을 제시하였다.

ABSTRACT

The Protection Profile(PP) is a common security function and detailed statement of assurance requirements in a specific class of Information Technology security products such as firewall and smart card. The parts of TOE security environment in the PP have to be described about assumption, treat and security policy through analyzing purpose of TOE. In this paper, we present a new security policy derivation among TOE security environment parts in the PP. Our survey guides the organizational security policy statements in CC scheme through collected and analyzed hundred of real policy statements from certified and published real PPs and CC Toolbox/PKB that is included security policy statements for DoD. From the result of the survey, we present a new generic organizational policy statements list and propose a organizational security policy derivation method by using the list.

keyword : *Common Criteria, protection profile, security environment, threats statement*

Ⅰ. 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 선진각 국에서는 CC(common criteria)와 같은 평가 인증체계를 운영하고 있다.

CC체계에서는 정보보호제품(이를 평가대상물 또는 Target of Evaluation; TOE라 칭함)군별로 평가 및 인증된 PP(protection profile)를 사용하며 PP는 정보보

* 영진전문대학 컴퓨터정보기술계열(jhkont@yjc.ac.kr)
** 한남대학교 정보통신 · 멀티미디어공학부(gslee@eve.hannam.ac.kr)

호제품군의 공통 보안기능 및 보증 요구사항 명세서라 할 수 있다. 정보보호제품은 PP에 따라 개발 및 평가되며, PP의 개발은 CC체계 내에서 정보보호제품의 기능과 보증성에 관련되므로, 선진 각 국과 제품군별 협회에서는 PP의 개발을 활발히 진행하고 있다.

PP를 개발하기 위해서는 CC에서 표준화한 내용에 따라 세부사항을 개발해야한다. 특히, PP내의 보안환경 부분은 TOE의 환경에 관한 가정, 자산에 대한 위협, 조직의 보안정책 문장들로 구성되며, 본 연구는 이들 중 "조직의 보안정책 문장"을 작성하는 방법을 다룬다.

국내의 각 기관에서는 체계적인 보안정책이 수립되어 있지 못하며 활발한 연구도 이루어지고 있지는 못하다. 특히, 기존의 보안정책 문서들은 구조적인 측면에서 통일되어 있지 않으며 조직의 목적과 특성에 따라 작성되었으므로 보안정책을 새로 개발하거나 비교하기가 어렵다는 문제가 있다. 그러므로, 본 연구에서는 정보보호부문에서의 보안정책에 대한 표준이나 지침을 조사 및 분석하여 보안정책 문서와 관련된 사항을 정리한다. 또한, 기존 PP들에서 실제 사용한 보안정책 문장, 미 국방부의 보안정책 문장, CC의 보안기능 및 보증 요구사항 클래스를 조사 분석하여 새로운 "일반 보안정책 문장 목록"과 이를 이용한 보안정책 문장 생성방법을 제시한다.

제시한 방법은 분할정복 방법, 객체지향적 보안정책 문장 생성, CC기반의 보안정책 문장 분류 및 기존의 보안정책 문장의 통합 전략을 바탕으로 하고 있다.

본 논문의 2장에서는 보안정책에 관련된 기존의 연구결과를 보이며, 3장에서는 PP개발을 위한 기존 PP들과 PKB(CC Profiling Knowledge Base)내의 보안정책 문장에 대한 조사결과를 보인다. 4장과 5장에서는 보안정책관련 요구사항을 고려하여 PP를 위한 보안정책 문장의 생성방법을 "일반 보안정책문장 목록"과 함께 제시하고, 제시한 방법을 적용한 사례를 보인다. 끝으로, 6장에서는 제시한 방법의 특성을 분석하고 결론을 맺는다.

Ⅱ. 보안정책 문서

2.1 보안정책의 개요

2.1.1 보안정책의 정의

보안정책이란 "반드시 충족해야할 특정 요구사항 또는 규칙에 대한 윤곽을 명세한 문서"[1] 또는 "조직의 기술과 정보자산에 접근하는 사람들이 준수해야 하는 규칙에 대한 정형적 문장"[2]으로 정의한다. 또한, 정책은 컴퓨터보안 프로그램을 작성하고, 프로그램의 목적을 제시하며, 각자의 책임을 할당하는 등의 상급 관리자로부터의 지시라 할 수 있다.[3]

보안표준이란 "모든 사람에 의해 충족되어야할 모임(collection) 또는 시스템에 특화되거나 절차에 특화된 요구사항"[1] 또는 "기술, 파라미터 및 절차 등에 있어서 일원화된 사용방법이 조직에게 이익이 되는 경우 일관된 사용방법을 명시한 것"[2]이다.

보안지침(guideline)은 "최상의 실행을 위해 시스템에 특화되거나 절차에 특화된 제안(suggestions)의 모임"이다.[1] 지침은 반드시 충족되지 않아도 되지만 강력하게 권고하는 요구사항이다. 지침은 시스템을 보호하는데 있어서 사용자, 시스템 직원 및 제3자를 효율적으로 보조한다.

보안절차는 특정 보안과 관련된 작업을 수행하기 위한 것으로 더 상세하게 기술하며, 보안 정책, 표준, 지침을 잘 적용할 수 있도록 도와준다. 사용자, 시스템 운영자 및 운영자가 새로운 계정을 준비하고 적절한 권한을 할당하는 등의 특정 작업을 수행하는 사람들이 따라할 수 있는 자세한 내용을 말한다.[3]

2.1.2 보안정책의 목적과 참여자

보안정책의 목적은 사용자, 스텝 및 관리자에게 기술과 정보자산을 보호하기 위한 의무적인 요구사항을 알리는 것이며, 이들 요구사항을 충족시키는 메커니즘이 명세된다. 또한, 컴퓨터시스템과 네트워크의 획득, 구성 및 감사에 대해 정책을 준수하기 위한 베이스라인이 제공된다.[2]

2.1.3 보안정책의 분류와 내용

각 기관에서는 보안정책을 "정책의 운영 대상 수준"과 "정책의 특성"에 따라 [표 1]과 같이 분류하고 있다. 즉, ISO/IEC, NIST 및 ITSEM에서는 계층적(수직적)으로 보안정책을 분류하고 있으며 Boran에서는 기능(수평적)별로 분류하고 있다.

■ 계층적 분류(수직적)

ISO/IEC-13335에서는 조직(또는 기업, 기관)의 목표, 전략 및 정책을 다음과 같이 3가지 수준으로 분류하고 있다.[4]

- 기업 보안정책

〔표 1〕 보안정책의 수준별 분류

표준 / 관점	ISO-13335 [4]	NIST-핸드북 [3]	ITSEM [5]	Boran [6]
분류 관점	계층적 (수직적)	계층적 (수직적)	계층적 (수직적)	기능적 (수평적)
분류	기업보안정책	프로그램 정책	Level 1	정보 보안 정책
	기업 IT 보안정책(*)	개별 쟁점 정책	Level i	인사 보안 정책
	IT 시스템 보안정책	개별 시스템 정책	Level n	컴퓨터 & 네트웍 보안

(*) "싸이트 보안정책"이라 할 수 있음

- 기업 IT 보안정책
- IT 시스템 보안정책

한편, NIST 핸드북에서도 다음과 같이 3가지 수준으로 분류하고 있다.[3]

- 프로그램 정책
- 개별 쟁점 정책
- 개별 시스템 정책

■기능적 분류(수평적)

Boran은 조직의 보안정책을 계층적이 아닌 기능적으로 분류하고 있다.[6]

- 정보 보안정책
- 인사 보안정책
- 컴퓨터와 네트워크 보안정책

2.2 기업 IT 보안정책

ISO/IEC-13335에서 "기업 IT 보안정책"은 "싸이트 보안정책"이라고도 할 수 있으며 NIST 핸드북에서는 개별쟁점 정책에 대응된다.

2.2.1 ISO/IEC-13335

다음의 주제를 포함하고 있다.[4]

- 자산 소유자의 관점에서 본 비밀성, 무결성, 가용성, 프라이버시, 책임추적성, 신뢰성에 관한 IT 보안 요건
- 조직의 기반구조 및 책임 할당
- 시스템 개발, 조달과 보안의 통합
- 지침과 절차 및 정보분류 등급의 규정
- 위험관리 전략 및 비상 계획
- 인력 문제
- 인식, 훈련, 법과 규제의 준수
- 외주관리와 사고 처리

2.2.2 SEI/CMU

CMU대학 SEI의 싸이트 보안지침에는 싸이트 보안정책 내에 다음과 같은 사항을 포함할 것을 권고하고 있다.[2]

- IT 구입지침
- 프라이버시 정책
- 접근정책
- 책임성 정책
- 인증정책
- 가용성 문장
- 위반 보고정책
- 지원 정보
- IT 시스템과 네트워크 유지보수 정책

2.2.3 McMillan

McMillan은 싸이트 보안정책의 골격을 제시하고 있다.[7]

2.2.4 Robiette

Robiette는 다음과 같은 골격을 통해 보안정책을 작성할 것을 제시하고 있다.[8]

- 목적
- 범위
- 책임성
- 계약
- 제재 조치
- 추가정보

2.3 IT 시스템 보안정책

IT 시스템 보안정책은 조직내의 특정한 부서나 기능에 대한 보안정책이며 NIST 핸드북의 '개별시스템 정책'에 대응하고 Boran에서는 '컴퓨터 & 네트웍 보안정책'과 유사하다.

2.3.1 ISO-13335

ISO-13335에서는 다음과 같은 내용을 기준으로 하여 IT 시스템 보안을 결정할 것을 제시하고 있다.[4]

- 해당 IT 시스템 및 그 범위의 정의
- 시스템을 통해 달성하고자 하는 사업목표의 정의
- 잠재적인 사업상의 역충격
- IT 투자 수준
- IT 시스템 및 정보 취급에 대한 중대한 위협
- IT 시스템이 식별된 위협에 노출되는 결점을 비롯한 취약성
- 식별된 위험에 대응하기 위해 필요한 보안대책
- IT 보안 비용 즉, IT 자산보호 비용.
- 외주업체(컴퓨팅센터나 PC 지원센터)와의 관계 및 선정 원칙

2.3.2 SANS 보안정책 프로젝트

미국의 SANS(System Administration, Audit, Network Security) 연구소에서는 정보보안정책을 신속히 개발하고 구현할 수 있도록 25가지의 중요한 보안요구사항을 위한 보안정책 템플릿을 무료로 제공하고 있다[1]. 이들 보안정책 템플릿은 보안정책 전문가들과 실제 기관의 보안정책을 참고로 하여 작성한 것이다.

SANS의 보안정책 템플릿은 2~3쪽 분량이며 [그림 1]과 같은 목차로 구성된다.

보안정책 템플릿은 "<Company Name>"과 "InforSec"를 변수로 처리하므로, 템플릿을 가져다가 "<Company Name>"에 실제 조직명을 대입하고 "InforSec"에 보안책임 조직을 대입하면 된다. SANS에서 제공하는 조직내 중간수준의 보안정책 템플릿의 종류는 다음과 같다.[1]

수용가능한 암호화 정책, 수용가능한 사용정책, 아날로그/ISDN 라인 정책, 응용서비스 제공자(ASP) 정책, 획득 심사 정책, 감사 정책, 자동 Forwarded 이메일 정책, 데이터베이스 기밀 코딩 정책, 전화 접근 정책, DMZ 부서(Lab) 보안정책, 익스트라넷 정책, 정보 민감성 정책, 내부 부서(Lab) 보안정책, 인터넷 DMZ 장비정책, 부서(Lab) 안티바이러스 정책, 패스워드 보호 정책, 원격 접근정책, 위험평가 정책, 라우터 보안정책, 서버 보안정책, VPN 보안정책, 무선 통신정책, 제삼자 네트워크 접속 동의 정책

1.0 개요: 보안정책에 대한 개요가 기술되어 있다. 개요를 생략한 경우도 있다.
2.0 목적: 본 보안정책의 목적(purpose)이 기술되어있다.
3.0 범위: 조직 내에서 본 보안정책이 커버하는 범위(scope)가 기술되어있다.
4.0 정책: 통일된 절 이름이 없이 자유롭게 세부적인 보안정책들이 기술되어있다.
5.0 강화: 본 보안정책을 강화하기 위해 본 보안정책을 위반했을 때의 제재조치와 보안정책의 적용 대상업무 및 사람 등이 기술되어있다.
6.0 정의: 보안정책에서 사용한 용어에 대한 정의가 기술되어 있다.
7.0 수정이력: 본 보안정책의 개편에 관한 내용이 기술되어있다.

[그림 1] SANS의 보안정책의 골격

2.4 실제의 보안정책

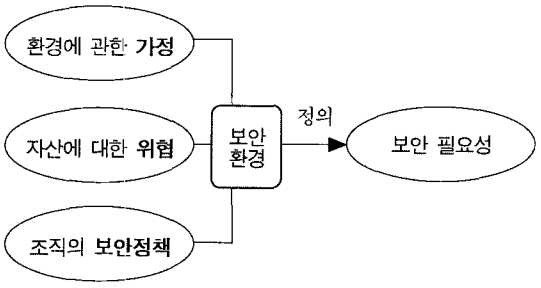
실제의 보안정책들은 조직마다 또는 조직내의 기능, 부서마다 존재하며 앞 절의 내용을 기반으로 하고 있다. 정부수준의 보안정책의 경우, 미국의 주요 보안정책은 "http://csrc.ncsl.nist.gov/secplcy/"에 게시되어 있으며 PKB에는 미 국방부의 보안정책이 수록되어 있다.[44] 캐나다의 경우에도 7종의 보안정책 및 지침이 "http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/siglist_e.html Security Policy"에 게시되어 있다.

기존의 보안정책 문서들은 골격 면에서 통일되어 있지 않고 조직의 목적과 특성에 따라 작성되어 있으므로, 보안정책을 새로 개발하거나 비교하기가 어렵다는 문제가 있다. 이를 해결하기 위해 보안정책문서의 골격과 내용상의 표준화작업이 요구된다. SANS의 보안정책 템플릿은 보안정책의 골격상의 표준화 작업의 시도라 할 수 있다. 참고문헌 [9~13]에는 세계 대학에서의 보안정책을 볼 수 있다.

Ⅲ. PP개발을 위한 기존의 보안정책 문장

3.1 관련 요구사항

PP는 정보보호제품(TOE)의 제품군별 공통 보안관련 요구사항 명세서라 할 수 있다. 특정한 TOE 제품군(예: 스마트카드)을 위한 PP를 개발하기 위해서는 [그림 2]와 같이 TOE의 보안 필요성을 도출하기 위해서 "보안환경" 부분을 작성해야한다. 보안환경 부분 내에서 다음과 같이 "조직의 보안정책" 문장을 작성해야한다.



[그림 2] PP의 개발시의 조직의 보안정책의 역할

- TOE가 정보보호 제품(즉, 솔루션)일 경우: TOE가 사용되거나 사용이 예상되는 조직(또는, 환경, 응용)에서 사용되고 있는 조직의 보안정책을 고려한다.
- TOE가 특정 조직의 정보보호시스템으로 사용중인 경우: 해당조직의 기존 보안정책을 통해 보안정책을 작성한다.

조직의 보안정책 작성과 관련하여 CC,[14] CEM [15] 및 PP/ST 작성가이드[16]에서는 다음과 같은 지침을

제시하고 있다. 이는 PP 개발시의 보안정책 문장의 요구사항에 해당한다.

- PP내의 보안정책 절에서는 TOE가 따라야하는 조직의 보안정책(규칙, 관습(practice) 또는 지침)을 기술해야 한다.
- TOE의 환경이 광범위할 경우, TOE 환경을 영역별로 구분하고 각 영역 별로 분리하여 보안정책을 설명한다.
- TOE내의 자산(asset)에 대한 기존의 위협 및 연관된 위협에 대하여 조직의 보안정책을 검토해야 한다.
- 보안의 필요성(need)을 간결하게 서술해야 한다.
- 다른 양식으로 서술한 조직의 보안정책을 포함할 수도 있다.
- TOE가 특정 조직 또는 조직의 유형에 의해 사용되도록 한 경우 또는 TOE가 위협 설명문에는 포함시킬 수 없는 규칙을 구현할 필요가 있을 때, 조직의 보안정책을 명세하는 것이 좋다. 다음은 그 예들이다:
  - 적용되어야 할 정보흐름 통제 규칙의 파악
  - 적용해야 할 접근통제 규칙의 파악
  - 보안감사에 따른 조직의 보안정책의 정의
  - 조직에 의해 강요된 솔루션기술(예: 특정한 승인된 암호알고리즘의 사용 또는 파악된 표준에의 준수)
- 패스워드 생성과 암호가 국가정부가 제정한 표준을 준수해야한다는 요구사항은 조직의 보안정책의 한 예이다.
- 조직의 보안정책은 위협을 다른 형태로 재기술할 뿐만 아니라, 보안필요성에 대처하기 위하여 제공된 보안목적을 정의할 때 다시 사용된다.

3.2 기존 PP에서의 보안정책 문장

〔표 2〕 본 연구에서 분석한 PP의 종류

제품군	종수	참고문헌
DB	1	[17]
네트워킹	7	[18-24]
OS	4	[25-28]
접근통제	8	[29-36]
침입탐지	3	[37-39]
스마트카드	1	[40]
우편물승인	1	[41]
생체인증	1	[42]

실제의 PP에서 보안정책 문장을 어떻게 작성하였는지 보기 위해 본 연구에서는 26종의 PP에서 사용된 보안정책 문장을 발최 및 분석하였다. [표 2]는 본 연구에서 조사한 PP의 정보를 보인다. PP들은 CC 홈페이지(http://www.commoncriteria.org)에서 조회할 수 있다.

3.3 CC-PKB에서의 보안정책 문장

NIST에서는 PP의 작성을 지원하는 도구로서 CC Toolbox[43]와 이를 위해 '미리 정의된' 위협, 공격, 보안목적, 가정 및 정책문장 데이터베이스인 CC Profiling Knowledge Base(PKB)를 개발 및 공개하고 있다.[44]

PP 개발자는 CC Toolbox를 이용하여 PKB내에 미리 정의된 문장들을 선택하여 PP를 쉽게 구성할 수 있도록 하고 있다. 보안정책은 조직마다 다르므로, PKB에서는 미 국방부의 보안정책을 제시하고 있다.

Ⅳ. 보안정책 제시방법

4.1 기존의 문제점과 해결 전략

4.1.1 기존의 보안정책의 문제점

2장에서 조사한 바에 따르면 국내의 각 기관에서는 체계적인 보안정책이 수립되어 있지 못하며 활발한 연구도 이루어지고 있지는 못하다. PP내의 보안정책 부분은 TOE 자체 또는 TOE의 응용환경(즉, 조직)의 보안정책에 의존해야하기 때문에, 보안정책 자체가 없거나 부실할 경우 PP를 위한 보안정책 부분을 작성하기는 매우 어렵다.

기존의 기관별 실제 보안정책들은 골격과 내용이 다양하므로 적어도 골격(목차수준)정도는 통일되어야 할 것이다. 보안정책 문서도 CC와 같은 수준으로 표준화하는 것이 필요하다. 다행히, SANS에서는 이러한 시도가 진행되고 있다.

정보보호 기능 및 보증성의 평가기준에서는 공통적으로 TOE자체 또는 TOE를 응용할 조직의 "보안정책"을 고려하고 있지만, 보안정책에 대한 세부내용은 제시하고 있지 않다. 또한, 보안평가기준 부문과 보안정책 부문에서는 서로 다른 접근방법을 취하고 있다.

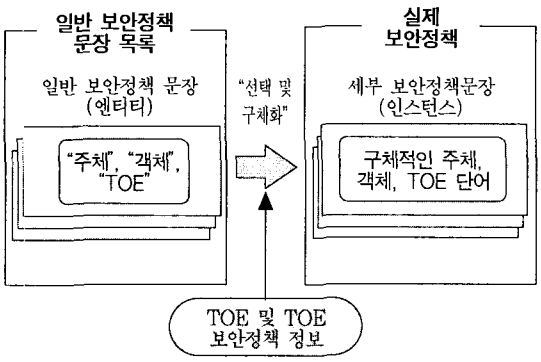
그리고, 기존 PP들을 조사한 결과 보안정책 문장들은 그 수준과 표현 방법이 일정하지 않으며 누락

된 문장들이 있다. 특히, 누락된 보안정책이 있는지 조차 파악하기도 어렵다. PKB에 있는 미 국방부의 보안정책 문장도 2개의 수준으로 계층화하고 있지만 보안정책 문장들이 주로 "보안기능 보호"와 "사용자 데이터 보호"에 편중되어 있다.

4.1.2 해결 전략

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

- 분할정복(divide and conquer)방법의 적용: 복잡하고 추상적인 보안정책을 클래스별로 나누어 클래스별로 보안정책 문장들을 생성해가고 이를 종합한다.
- 객체지향적(object-oriented) 보안정책 문장생성: 객체지향 개념을 사용해, 미리정의한 일반(generalization, generic) 보안정책 문장 목록 내의 일반 보안정책 문장을 선택하고 구체화하여 세부(specialization, instantiation) 보안정책문장을 도출한다. 예컨대, 일반 보안정책 문장 목록 내의 "P.Audit_Generation TOE내의 주체는 감사에 필요한 자료를 생성한다."는 세부 보안정책 문장인 "P.Audit_Generation 스마트카드의 감사자는 감사에 필요한 스마트카드 접근이력을 생성한다."로 구체화하여 사용할 수 있다.([그림 3] 참조)
- CC기반의 보안정책 문장 분류: TOE에 대한 PP 평가 뿐 아니라 TOE 자체의 평가시에도 일관성을 유지하기 위해 보안정책 문장을 CC의 기능 및 보증 요구사항의 클래스 스키마를 이용한다.
- 기존의 보안정책 문장을 통합



[그림 3] 객체지향적 보안정책 문장 생성방법

4.2 보안정책 문장의 작성 과정

앞 절에서 제시한 해결전략에 따라 다음 단계들을 통해 PP를 위한 조직의 보안정책을 작성한다.

[표 3]은 각 단계별 활동, 참조 및 입력물, 결과물 및 방법을 나타내며, 각 단계별 세부활동은 아래에서 설명한다. 그리고, 2단계에서 요구되는 미리 정의한 '일반 보안정책 문장 목록'은 부록에서 제시한다.

① 보안정책 파악 단계 : TOE의 관련자료 및 전문가로부터 TOE 및 사용환경에 대한 기존의 보안정책을 파악한다. 기존의 보안정책이 없다면, SANS에서 제공하는 TOE와 가장 유사한 보안정책 템플릿을 선택한다.

② 일반 보안정책 문장선택 단계 : '일반 보안정책 문장 목록'에서 [그림 4]의 클래스별로 일반 보안정책 문장을 선택한다.

③ 세부 보안정책 문장도출 단계 : 일반 보안정책 문장내의 일반용어(예: 객체, 주체, TOE 등)를 구체적인 용어(예: 관리자, 사용자, 인증자료, 응용자료, 스마트카드 등)로 대치하여 세부 보안정책 문장을 생성한다.

[표 3] 보안정책 문장의 작성과정

단계별 활동	참조 및 입력물	결과물	방법
1.보안정책 파악	TOE전문가, 보안정책문서	-	자문, 자료검토
2. 일반 보안정책 문장 선택	TOE전문가, 보안정책문서, '일반 보안 정책 문장 목록'	일반 보안 정책 문장	자문, 자료검토
3. 세부 보안정책 문장 도출	TOE전문가	세부 보안 정책 문장	자문
4. 세부 보안정책 문장 검토	PP의 보안가정 문장, 위협문장	실제 보안 정책	자료검토

1. 보안감사(Audit)
- ▸ 감사(Audit)
- ▸ 책임성(Accountability)
- ▸ 감시(Monitor)
- ▸ 발견(Detection)

2. 통신(Communication)
3. 암호(Cryptographic)
4. 접근통제(Access)
5. 식별 및 인증(I&A)
6. 보안관리(Management)
- ▸ 권한(Authority, privilege)
- ▸ 인가(Authorization)
- ▸ 마킹(Marking)
- ▸ 관리(Manage)
- ▸ 보안정책(Policy)
- ▸ 훈련(Train)

7. 보안기능보호(Function)
- ▸ 물리적 보호(Physical)
- ▸ 가용성(Avail)
- ▸ 무결성(Integrity)
- ▸ 기밀성(Sec)
- ▸ 복구(Recovery)

8. 경고/고지(Note)
9. 구성(Configuration)
10. 운영보호(Operation)
11. 지침(Guidance)
12. 생명주기(Lifecycle)
13. 취약성(Vulnerability)

[그림 4] 일반 보안정책 문장 목록의 스키마

〔표 4〕 보안정책 문장의 클래스별 분류의 대응성

CC보증 및 기능	본 결과	PKB(미 국방부)
보안감사(Audit) (대응, 자료생성, 분석, 검토, 사건선택, 사건저장)	**보안감사(Audit)** - 감사(Audit) - 책임성(Accountability) - 감시(Monitor) - 발견(Detection)	개인 책임성, 감사자료 생성, 보호된 감사자료 저장
통신(Comm) (부인봉쇄)	**통신(Communication)**	부인봉쇄 능력
암호(Crypto) (키관리, 연산)	**암호(Crypto)**	-
사용자데이터보호(접근통제) (UData, DataAccess) (AC정책, AC기능, 자료인증, 흐름정책, 통제외부로 유·출입, 내부전송, 잔여정보보호, 복귀, 저장자료 무결성, 사용자자료 비밀성/무결성 전송보호)	**접근통제(Access)**	인가된 사람이 보안자료를 변경, 자료내용 변경의 고지, 특권있는(privileged) 사용자 접근, 효과적인 저장 무결성의 보증, 전송된 사용자 자료의 암호화, 저장된 사용자 자료의 보호, 전송 사용자 자료의 보호, 접근제어(DAC)
식별 및 인증(I&A) (사용자속성 정의, 비밀정보 생성, 사용자-주체연결)	**식별 및 인증(I&A)**	사용자 식별 및 인증
보안관리(Mgmt) (기능관리, 속성관리, 자료관리, 폐지, 만료, 관리직무)	**보안관리(Mgmt)** - 권한(Authority, privilege) - 인가(Authorization) - 마킹(Marking) - 관리(Manage) - 보안정책(Policy) - 훈련(Train)	자료의 레이블링
프라이버시(Privacy) (익명, 가명, 링크불가, 관찰불가)	-	-
보안기능보호(Function) (추상기계시험, 고장안전, 유출 TSF데이터 가용성/비밀성/무결성, 내부 데이터 전송, 복구, 재시도, 참조중재, 영역분리, 상태동기, 타임, TSF간 자료일관성, 자체시험)	**보안기능보호(Function)** - 물리적 보호(Physical) - 가용성(Avail) - 무결성(Integ) - 기밀성(Sec) - 복구(Recovery)	문서화된 복구, 강력한 무결성 메커니즘, 운영적 무결성, 악의적 코드의 방지, 보안기능 무결성의 검증, 시스템 백업 절차, 최소한의 손실을 통한 복구(restoration), 효과적인 백업 복구(restoration), 보안기능 수정으로부터 보호, 신임된 시스템 복구, 물리적 탬퍼링 발견 및 고지
자원활용(Resource) (고장허용, 우선순위, 자원할당)	-	-
TOE접근(TOEAccess) (속성범위제한, 다중세션제한, 세션로킹, 접근경고, 접근이력, 세션이력)	**경고/고지(note)**	위협 및 취약성의 고지(notify), 시스템 접근 배너(banners), 사용자 스크린 로킹
안전 경로/채널(PathChannel)	-	-
형상관리(ConfMgmt) (자동화, 능력, 범위)	**구성(Config)**	운영적 형상관리의 구현
배포운영(Del&Oper) (배포, 설치 생성 운영)	**운영보호(Oper)**	예방적 유지보수
개발(Dev) (명세, 설계, 보안정책모델)	-	-
설명서(Guide) (관리자, 사용자)	**지침(Guidance)**	특권화된 사용자 문서, 일반 사용자 문서
생명주기(LifeCyc) (개발보안, 결함개선, 정의, 도구)	**생명주기(Lifecycle)**	생명주기 동안 보안
시험/취약성(Test&Vul) (범위,깊이,기능시험,독립시험,비밀채널,오용,기능강도,취약성분석)	**취약성(Vul)**	시스템 기능시험

④ 세부 보안정책 문장검토 단계 : PP의 개발 전 체기간동안 다음 활동을 반복 수행하여 잘 정의된 (well formed) 실제 보안정책 문장을 생성한다.

- 보안가정 문장과의 중복성을 파악함
- 가정문장과 중복되는 보안정책 문장은 가정 문장으로 처리함
- 정책 문장들간의 일관성을 체크하고 일관성을 유지함
- 문장을 정제하여 문장의 조리성을 제고함

〔표 5〕 일반 보안정책 문장의 일부

■ 보안감사(Audit)
▸ 감사(Audit)
P.Audit_Generation TOE내의 주체(특히, 감사자 및 감사기능)는 감사에 필요한 자료를 생성한다.
[적용사례] 감사자료 생성<DoD>
P.Audit_Analysis TOE내의 주체(특히, 감사자 및 감사기능)는 정기적 또는 필요시 감사자료를 분석하여 감사를 실시하고 감사결과에 따라 필요한 조치를 취한다.
[적용사례] 감사 데이터의 검토, 분석 및 적절한 행동<Net6>. 감사<SMC1>. 감사로그가 정기적으로 자주 검토되고 발견된 부정행위에 대해 적절한 행동 수행하도록 구현<AC5>
P.Audit_Admin TOE내의 주체(특히, TOE 관리자)의 행동에 대한 감사를 실시한다.
[적용사례] 관리자 데이터 감사<Net5>
P.Audit_Store TOE내의 객체(특히, 감사자료)는 안전한 장소에 저장한다.
[적용사례] 보호된 감사자료 저장<DoD>

4.3 일반 보안정책 문장 목록

'일반 보안정책 문장 목록'은 4.1절에서 제시한 해결전략에 기반하여 다음 과정을 통해 작성하였다.

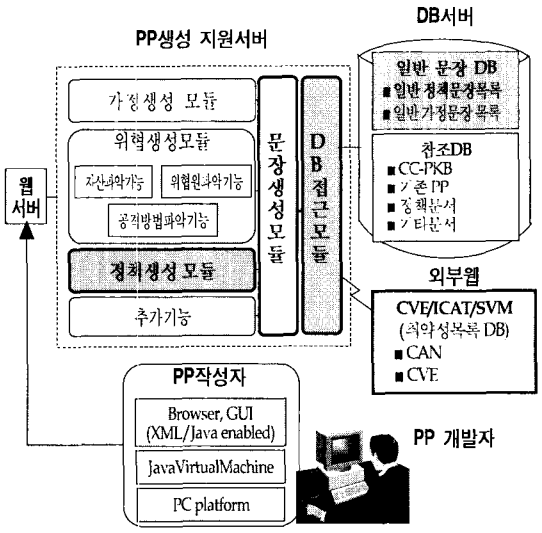
① 26종의 기존 PP와 PKB내의 미 국방부의 보안정책 문장을 분석하고 분류함
② CC의 보안기능 및 보증 클래스별로 재분류함([표 4]참조)
③ "주체", "객체", "TOE" 등과 같은 일반용어를 사용해 '일반 보안정책 문장'들을 작성함([표 5]참조)
④ 각 '일반 보안정책 문장별로' 대응되는 기존 PP와 PKB내의 미 국방부의 실제 보안정책 문장을 "[적용사례]"를 통해 보임(예: "감사자료 생성<DoD>"은 미 국방부의 보안정책 문장 중에 "감사자료 생성"이라는 문장이 있음을 나타내며, "< >" 내의 내용은 [표 2]에서 제시한 실제 PP의 식별자임)

4.4 지원도구의 구조

4.2절에서 제시한 보안정책 문장의 작성방법은 지원도구를 통해 부분적으로 자동화가 가능하다. 지원도구를 사용하는 경우의 각 단계별 시나리오는 다음과 같다.

① 보안정책 파악단계: 미리 구성해 놓은 "참조 DB"로부터 TOE 및 보안정책 자료를 검색하며 자문대상자(TOE 전문가)를 검색하고 자문일정을 조정한다. 전자우편을 통해 자문을 실시할 수도 있다.
② 일반 보안정책 문장선택 단계: 미리 구성해 놓은 "일반 보안정책 문장 목록"으로부터 보안정책 클래스별로 "일반 보안정책 문장"들을 GUI와 DB를 통해 선택한다.
③ 세부 보안정책 문장도출 단계: 문장 편집기를 통해 "일반 보안정책 문장"내의 일반용어(주체, 객체, TOE 등)를 구체적인 용어로 대체한다.
④ 세부 보안정책 문장검토 단계: 문서편집기의 단어 검색기능을 통해 문장 간의 중복성과 일관성을 체크하고 보안가정 문장들과의 중복성을 체크하여 중복된 문장은 보안가정 문장으로 간주한다.

이러한 시나리오에 근거하여 설계된 보안정책 문장 생성 지원도구의 구조는 [그림 5]와 같다. 그림에는 보안정책 뿐만 아니라 가정 및 위협문장 생성 기능도 포함된다.



〔그림 5〕 PP개발을 위한 보안정책 문장생성 지원도구의 구조

V. 조직의 보안정책 문장도출 사례

본 장에서는 제안한 방법을 적용하여 PP 작성시에 보안환경 부분에서 조직의 보안정책 부분을 도출한 예를 보이며, OS 제품군을 대상으로 작성한 내용을 아래에서 단계적으로 보인다.

[단계 1] 보안정책 파악

TOE의 관련자료 및 전문가로부터 TOE 및 사용환경에 대한 기존의 보안정책을 파악한다.

[단계 2] 일반 보안정책 문장 선택

'일반 보안정책 문장 목록'에서 다음의 클래스별로 일반 보안정책 문장을 선택한다.

P1. 보안감사	(○)
P2. 통신	(×)
P3. 암호	(○)
P4. 접근통제	(○)
P5. 식별 및 인증	(○)
P6. 보안관리	(○)
P7. 보안기능 보호	(○)
P8. 경고/고지	(∕)
P9. 구성	(○)
P10. 운영보호	(×)
P11. 지침	(×)
P12. 생명주기	(×)
P13. 취약성	(○)

[단계 3] 세부 보안정책 문장 도출

일반 보안정책 문장내의 일반용어(예: 객체, 주체, OS 등)를 구체적인 용어(예: 관리자, 사용자, 인증자료, 응용자료)로 대치하여 세부 보안정책 문장을 생성한다.

P1. 보안감사(Audit)

▸ 책임성(Accountability)

P1.1 Account_User TOE내의 주체(특히, 사용자)는 그 행동에 대해 책임을 진다.

▸ 감시(Monitor)

P1.2 Monitor_User TOE내의 주체(특히, 사용자)의 행동을 감시하고 적절한 조치를 취한다.

P3. 암호(Cryptographic)

P3.1 Crypto_Standard TOE에서 사용하는 암호 알고리즘 및 메커니즘은 **표준을 준수한다.

P4. 접근통제(Access)

P4.1 Access_Data TOE내의 인가된 주체만이 TOE 객체(특히, 보안관련 데이터)에 접근한다.

P5. 식별 및 인증(I&A)

P5.1 I&A_All TOE 및 TOE의 운영환경내의 모든 주체는 객체에 접근하기 전에 식별과 인증한다.

P6. 보안관리(Mgmt)

▸ 인가(Authorization)

P6.1 Authorization_Capability TOE의 보안관리자는 TOE의 주체에 대해 객체로 접근 및 활용할 수 있는 능력을 인가한다.

P6.2 Authorization_Use TOE의 주체는 그에게 인가된 능력 내에서만 객체에 접근 및 활용한다.

▸ 마킹(Marking)

P6.3 Marking_Level TOE내의 보안관련 객체에 대해 보안수준에 따라 ***수준의 등급을 부여한다.

P6.4 Marking_Output TOE의 보안관련 객체(특히 출력물)에 대해 보안수준에 따라 ***수준의 등급을 부여한다.

▸ 관리(Manage)

P6.5 Manage_Process TOE내의 보안관리자는 객체에 대해 보안관리를 실시한다.

P6.6 Manage_Persons TOE의 보안관리를 책임지는 보안관리자를 둔다.

P7. 보안기능보호(Function)

▸ 무결성(Integ)

P7.1 Integrity_System TOE의 객체(특히, 시스템)는 무결성이 유지되도록 보호한다.

▸ 복구(Recovery)

P7.2 Recovery_All TOE의 객체(특히, 시스템)는 고장 또는 보안기능 침해시 정상기능으로 정해진 시간과 피해정도 이내로 복구하는 절차와 기능을 갖는다.

P8. 경고/고지(note)

P8.1 Notify_Banner TOE의 주체(특히, 인간)가 객체에 접근하려할 때 가능한 위협과 위반시의 처벌내용을 알리는 경고문(배너)을 주체에게 표시한다.

P13. 취약성(Vul)

P13.1 Vulnerability_Test TOE의 취약성을 파악하기 위한 보안시험을 실시한다.
P13.2 Vulnerability_Search TOE의 알려진 취약성과 잠재적인 취약성을 조사 및 분석한다.

[단계 4] 세부 보안정책 문장 검토

PP의 개발 전체기간 동안 다음 활동을 반복 수행하여 잘 정의된 실제 보안정책 문장을 생성한다. 작성결과는 [표 6]과 같다.

- 보안가정 문장과의 중복성을 파악함
- 가정문장과 중복되는 보안정책 문장은 가정 문장으로 처리함
- 정책 문장들간의 일관성을 체크하고 일관성을 유지함
- 문장을 정제하여 문장의 조리성을 제고함

Ⅵ. 결 론

본 연구에서는 특히 CC 환경에서 TOE를 위한 PP 내에서 요구되는 보안정책에 관한 문장을 생성하는 방법을 제시하였다. 이와 유사한 연구는 NIST에서 PKB를 개발함으로서 시도되었지만 사용된 보안정책은 미 국방부의 보안정책을 그대로 인용한 수준이다.

PKB의 경우 "사용자 데이터 보호(접근통제)"와 "보안기능 보호" 클래스에 많은 세부 보안정책이 집중되어 있고 보안정책의 수준이 다양하다. 본 연구의 경우 접근통제 클래스에는 PKB와는 달리 세부 보안정책 문장이 적다. 이는 "접근통제"가 다른 클래스(예: 보안관리, TOE접근 등)와 중복된 개념이기 때문이다.

본 연구는 다음과 같은 장점을 갖는다.

① 복잡한 보안정책을 클래스별로 나누어 누락되거나 중복됨이 없이 보안정책 문장을 생성할 수 있다.
② "객체", "주체", "TOE" 등과 같은 일반적인 용어를 사용한 '일반 보안정책 문장 목록'을 제시하였고 PP 작성자는 이를 선택하여 구체적인 용어로 대치함으로써 쉽고 빠르게 실제의 보안 정책문장을 작성할 수 있다. 또한, 작성된 보안정책의 수준을 통일할 수 있다.
③ CC 환경하의 PP 개발 및 평가와 TOE 개발 및 평가시에 용어의 일관성이 제고된다.
④ 제시한 일반 보안정책 문장들을 기존의 PP들과 PKB 내의 보안정책 문장과 대응시킴으로서 이들과의 호환성을 높이고 있다.

[표 6] OS 제품군의 작성된 보안정책 예

P1.1 Account_User TOE내의 주체(특히, 사용자)는 그 행동에 대해 책임을 진다.
P1.2 Monitor_User TOE내의 주체(특히, 사용자)의 행동을 감시하고 적절한 조치를 취한다.
P3.1 Crypto_Standard TOE에서 사용하는 암호 알고리즘 및 메커니즘은 **표준을 준수한다.
P4.1 Access_Data TOE내의 인가된 주체만이 TOE객체(특히, 보안관련 데이터)에 접근한다.
P5.1 I&A_All TOE 및 TOE의 운영환경내의 모든 주체는 객체에 접근하기 전에 식별과 인증한다.
P6.1 Authorization_Capability TOE의 보안관리자는 TOE의 주체에 대해 객체로 접근 및 활용할 수 있는 능력을 인가한다.
P6.2 Authorization_Use TOE의 주체는 그에게 인가된 능력 내에서만 객체에 접근 및 활용한다.
P6.3 Marking_Level TOE내의 보안관련 객체에 대해 보안수준에 따라 ***수준의 등급을 부여한다.
P6.4 Marking_Output TOE의 보안관련 객체(특히, 출력물)에 대해 보안수준에 따라 ***수준의 등급을 부여한다.
P6.5 Manage_Process TOE내의 보안관리자는 객체에 대해 보안관리를 실시한다.
P6.6 Manage_Persons TOE의 보안관리를 책임지는 보안관리자를 둔다.
P7.1 Integrity_System TOE의 객체(특히, 시스템)는 무결성이 유지되도록 보호한다.
P7.2 Recovery_All TOE의 객체(특히, 시스템)는 고장 또는 보안기능 침해시 정상기능으로 정해진 시간과 피해정도 이내로 복구하는 절차와 기능을 갖는다.
P8.1 Notify_Banner TOE의 주체(특히, 인간)가 객체에 접근하려할 때 가능한 위험과 위반시의 처벌내용을 알리는 경고문(배너)을 주체에게 표시한다.
P13.1 Vulnerability_Test TOE의 취약성을 파악하기 위한 보안시험을 실시한다.
P13.2 Vulnerability_Search TOE의 알려진 취약성과 잠재적인 취약성을 조사 및 분석한다.

⑤ 제시한 방법을 지원할 수 있는 도구의 개발이 용이하다.

또한, 본 연구의 주요결과인 "보안정책 문장의 작성 과정"과 "일반 보안정책 문장 목록"은 가급적 많은 국제표준 및 지침(CC, CEM, PP/ST 작성가이드, ISO-13335), 평가와 인증된 문서(실제 PP 문서) 및 각종 보안정책관련 지침들에 근거하여 제시하므로 가급적 주관성을 배제하였다.

PP가 TOE의 보안 요구사항 문서라면, PP의 TOE 보안환경 부분은 PP자체의 보안 요구사항이다. 요구사항 공학(requirement engineering)기술이 연구되고 있지만, 요구사항을 도출하는 일과 이를 확인(validation)하는 일은 주로 인간의 능력에 의해 이루어지고 있다. 따라서, PP의 TOE 보안환경 부분은 자동적 또

는 정형적으로 생성될 수는 없으며 본 연구의 결과는 PP 개발자에게 지침을 제공할 뿐이다.

향후 연구과제로는 제시한 방법의 효과성을 검증하며, 활용을 통한 문제점을 발견하고 개선하는 것이다.

참 고 문 헌

[1] SANS, Security Policy Project, *http://www.sans.org/resources/policies/policies.htm.*

[2] B. Fraser(ed.), *Site Security Handbook*, SEI/CMU, September 1997, *http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2196.html.*

[3] NIST, "A Introduction to Computer Security : The NIST Handbook", pub 800-12, *http://www.nist.gov*, 1991.

[4] ISO/IEC TR 13335-1,2,3, IT 보안 개념 및 모델(1996), IT 보안 관리 및 계획(1997), IT 보안 관리 기법(1998).

[5] European Community, *Information Technology Security Evaluation Criteria(ITSEM)*, Ver. 1.0, 1993.

[6] Sean Boran, IT 보안 해설서, Boran Consulting(번역: 이혜연, 시만텍 코리아).

[7] R. Macmillan, Site Security Policy Development, *http://www.auscert.org.au/Information/Auscert_info/Papers/Site_Security_Policy_Development.txt*.

[8] Alan Robiette, Developing an Information Security Policy, *JISC Committee on Authentication and Security*, February 2001.

[9] Kingston University, Information Security Policy, December 1997, *http://www.kingston.ac.uk/info-security/policy.htm.*

[10] Lancaster University, Electronic Information Systems: Security Policy, *http://www.lancs.ac.uk/iss/rules/security.htm.*

[11] Oxford University, *University Rules for Computer Use.*

[12] Washington University in St. Louis, *Policies and Procedures Computer Use Policy, http://www.wustl.edu/policies/compolcy.html.*

[13] Policies and Procedures, Information Security Policy, *http://www.wustl.edu/policies/infosecurity.html.*

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

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

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

[17] Oracle, *DBMS Protection Profile.*

[18] NSA, *Traffic Filter Firewall Protection Profile For Medium Robustness Environments.*

[19] NSA, *Traffic Filter Firewall Protection Profile for Low Risk Environments.*

[20] NSA, *Application Level Firewall Protection Profile for Low Risk Environments.*

[21] BHTT, *Peer-to-Peer Wireless Local Area Network (WLAN) for Sensitive But Unclassified Environments.*

[22] NSA, *Protection Profile for Switches and Routers.*

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

[24] BHTT, *Infrastructure Wireless Local Area Network (WLAN).*

[25] NSA, *Labeled Security Protection Profile.*

[26] NSA, *Controlled Access Protection Profile.*

[27] NSA, *Protection Profile for Multilevel OS.*

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

[29] NSA, *Directory for DoD Class 4 PKI PP.*

[30] TCPA. *Trusted Platform Module(TPM) PP.*

[31] NSA, *Certificate Issuing and Management Components.*

[32] NIST, *Role-Based Access Control PP.*

[33] Authorizor, *Privilege Directed Content PP.*

[34] NSA. *Key Recovery for Third Party Requestors.*

[35] NSA. *Key Recovery for Agent Systems.*

[36] NSA. *Key Recovery for End Systems.*

[37] NIST, *Role-Based Access Control PP.*

[38] NSA, *Intrusion Detection System Analyzer -Draft 3.*

[39] NSA, *Intrusion Detection System Sensor.*

[40] SCSUG, *Smart Card Protection Profile.*

[41] Consignia, *Postage Meter Approval Protection Profile.*

[42] DoD Biometrics Management Office1. *U. S. Depar-*

tment of Defense Biometrics Office, Biometric System. Protection Profile For Medium Robustness Environments.

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

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

부 록. 일반 보안정책 문장 목록

■ 보안감사(Audit)

▸ 감사(Audit)

P.Audit_Generation TOE내의 주체(특히, 감사자 및 감사기능)는 감사에 필요한 자료를 생성한다.

[적용사례] 감사자료 생성<DoD>

P.Audit_Analysis TOE내의 주체(특히, 감사자 및 감사기능)는 정기적 또는 필요시 감사자료를 분석하여 감사를 실시하고 감사결과에 따라 필요한 조치를 취한다.

[적용사례] 감사 데이터의 검토, 분석 및 적절한 행동<Net6>. 감사<SMC1>. 감사로그가 정기적으로 자주 검토되고 발견된 부정행위에 대해 적절한 행동 수행하도록 구현<AC5>

P.Audit_Admin TOE내의 주체(특히, TOE 관리자)의 행동에 대한 감사를 실시한다.

[적용사례] 관리자 데이터 감사<Net5>

P.Audit_Store TOE내의 객체(특히, 감사자료)는 안전한 장소에 저장한다.

[적용사례] 보호된 감사자료 저장<DoD>

▸ 책임성(Accountability)

P.Account_User TOE내의 주체(특히, 사용자)는 그 행동에 대해 책임을 진다.

[적용사례] DB 사용자의 책임<DB1>. 시스템내의 사용자 행동에 대한 책임<OS1><OS2><OS3><OS4><POST1>. 인가된 사용자의 보안관련 행동 책임<Net4><Net5><Net6> <Net7>. TOE의 사용자 행동에 대한 책임<IDS1><IDS2> <IDS3>. 개인의 책임<AC1><AC2><AC7>. 개인 책임성<DoD>

P.Account_Step TOE내의 주체(특히, 관리자 또는 시스템)는 그 행동에 책임을 진다.

[적용사례] 인가된 시스템 또는 보안 관리자의 보안관련 행동 책임<Net4><Net5><Net6><Net7>

▸ 감시(Monitor)

P.Monitor_User TOE내의 주체(특히, 사용자)의 행동을 감시하고 적절한 조치를 취한다.

[적용사례] 사용자의 행동 감시<Net7>. 침입 결정을 위한 분석절차와 정보는 IDS 데이터와 적절한 대응에 적용<IDS1><IDS2>. 운영체제의 사용자 행동 검토 <OS3><OS4>

P.Monitor_Limit TOE내의 주체가 TOE에 접근을 시도할때 일정한 로그인 시도시간 또는 횟수를 설정하여 그 한계를 초과하는 경우 적절한 조치를 취한다.

[적용사례] 하나 이상의 요구 ID로 반복적인 검증을 시도하여 사칭자의 접근획득 방지<BIO1>

▸ 발견(Detection)

P.Detect_Event TOE내의 주체의 부적절하거나 특이한 행동과 관련된 사건을 발견하고 수집한다.

[적용사례] 부적절한 행동에 해당하는 사건 수집 <IDS1> <IDS3>

■ 통신(Communication)

P.Communication_Secure TOE내의 주체 사이에서의 안전한 통신을 보장한다.

[적용사례] TOE를 통한 통신은 인증된 사용자, 시스템 및 보안 관리자 사이에서 수행<Net6>. 믿을 수 있는 전송<Net5>. 안전한 통신<SMC1>. TCPA 보호된 저장소 이동과 비 이동<AC2>

P.Communication_Control TOE내의 객체(노드, 부품 등)간의 안전한 접속을 통제한다.

[적용사례] TSE와 외부 네트워크간의 모든 연결 통제 <Net6>. TCPA DIR 레지스터<AC2>. TCPA PCR 레지스터<AC2>

P.Communication_Repuation TOE내의 주체에 대해 데이터의 송수신에 대한 부인봉쇄 기능을 제공한다.

[적용사례] 부인봉쇄 능력<DoD>

■ 암호(Cryptographic)

P.Crypto_Standard TOE에서 사용하는 암호 알고리즘 및 메커니즘은 **표준을 준수한다.

[적용사례] 암호화 표준<SMC1>. 3-DES 암호화는 원격 관리기능 보호에 사용하며, 관련된 암호 모듈은 FIPS 140-1(level 1) 준수<Net1>. TOE에서 사용된 암호화 키관리, 키 운용 및 알고리즘은 기관의 표준을 따름 <POST1>. 암호화 및 암호모듈은 최소한 FIPS 140-1 (level 2) 준수<Net4><Net7>. 원격관리 보호를 위한 Triple DES(FIPS 46-3[3]) 사용 및 암호모듈은 FIPS 140-1(level 1) 준수<Net3>. 모든 암호연산에 FIPS 혹은

NITS를 따르는 암호기능 사용<AC3>. 시스템은 키관리 및 암호서비스를 위해 NIST FIPS를 따른 암호기법 사용<OS3><OS4>. 세션키 생성 및 전자서명에 X.509 인증서 클래스 3이나 4 사용<Net7><Net4>

P.Crypto_Key 암호키의 처리(생성, 전달, 사용, 폐기)와 관련된 **절차를 준수한다.

[적용사례] 사용자가 클라이언트 키의 교체 요구에 따른 관리자의 처리 절차 존재<AC5>. 관리자가 TOE에 의해 제어되지 않는 방법으로 사용자에게 클라이언트 키를 전송하여 키를 획득한 사용자가 옳은지 검증할 수 있는 절차 존재<AC5>

■ **접근통제(Access)**

P.Access_Data TOE내의 인가된 주체만이 TOE 객체(특히, 보안관련 데이터)에 접근한다.

[적용사례] 객체 접근<DB1>. 정보 접근제어<AC2>. TOE에 의한 모든 데이터는 인가된 목적에만 사용<IDS1> <IDS2><IDS3>. 시스템은 인가된 사용자가 요구하는 보호자원의 정보 접근 제한<OS1><OS2><OS3><OS4>. TOE의 데이터 공개 및 사용은 인가된 사용자에 따라 제한<Net6>. 클라이언트에 의해 손상된 정보는 사용자 공개를 위해 제한<AC5>. 클라이언트 사용자에게 공개할 정보는 일반화 및 일반공개에 적절한 자료에 제한<AC5>. 전송 사용자 자료의 보호<DoD>. 저장된 사용자 자료의 보호<DoD>. 전송된 사용자 자료의 암호화<DoD>. 효과적인 저장 무결성의 보증<DoD>. 자료내용 변경의 고지<DoD>. 특권있는(privileged) 사용자 접근<DoD>

P.Access_Role TOE내의 인가된 주체는 그에게 인가된 역할에 따라서 TOE 객체에 접근한다.

[적용사례] 역할로 접근 권한 결정<AC4>. 사용자 역할에 따른 데이터 접근<SMC1>. 사용자 역할에 따른 파일 구조<SMC1>. 임의 접근통제(DAC)<DoD>. 인가된 사람이 보안자료를 변경<DoD>.

P.Access_Policy TOE의 주체는 주체와 객체간의 접근통제 정책에 따라서 객체에 접근한다.

[적용사례] 우편 계량기의 서비스 접근 권한은 접근제어 정책에 의해 결정<POST1>. 접근제어 목록에 의한 정보접근 권한 결정<AC1>

P.Access_Node TOE내의 노드(특히 분산시스템의 노드)에 대한 접근을 통제한다.

[적용사례] 어떤 노드 접근을 정보보호를 위해 여과<Net5>

■ **식별 및 인증(I&A)**

P.I&A_All TOE 및 TOE의 운영환경내의 모든 주체는 객체에 접근하기 전에 식별과 인증한다.

[적용사례] TOE의 사용자는 TOE 접근시 식별 및 인증<Net7>. 제어된 자원 접근에 앞서 모든 사용자 식별 및 인증<OS3><OS4>. 사용자 식별 및 인증<DoD>. 증강된 사용자 식별 및 인증<DoD>

P.I&A_Identification TOE 및 TOE의 운영환경내의 모든 주체는 객체에 접근하기 전에 식별한다.

[적용사례] TOE 식별<SMC1>. TCPA 개체식별<AC2>

P.I&A_Authentication TOE 및 TOE의 운영환경내의 모든 주체는 객체에 접근하기 전에 주체가 객체를 일방향 인증 또는 주체와 객체간의 상호 인증한다.

[적용사례] 관리자 및 노드의 인증<Net5>

■ **보안관리(Mgmt)**

▸ **권한(Authority, privilege)**

P.Authority_Note TOE의 보안관리자는 TOE에 대한 위협과 TOE에 가해질 수 있는 모든 위협을 고할 수 있는 권한을 가진다.

[적용사례] 위협과 취약성의 고시<AC2>. 위협 및 취약성의 고지(notify) <DoD>.

P.Authority_Privilege TOE의 보안관리자는 TOE의 주체에 대해 객체로 접근할 수 있는 권한(특권)을 부여하고 이를 관리하는 권한을 갖는다.

[적용사례] 모든 사람에게 부여되는 권한과 그 권한의 범위를 레코드에 유지<AC5>. 권한을 가진 사용자 또는 서버관리자가 더 이상 요구하지 않으면 취소<AC5>

▸ **인가(Authorization)**

P.Authorization_Capability TOE의 보안관리자는 TOE의 주체에 대해 객체로 접근 및 활용할 수 있는 능력을 인가한다.

[적용사례] 시스템은 TSP를 따르는 각 사용자 능력의 범위를 제한<OS3><OS4>. 모든 COI 정보에 인가자는 특정한 COI 권한 수준에 맞는 특권 허가<Net6>. TOE 자원의 모든 인가자는 최소한의 민감한 특권수준 소유<Net6>. TCPA 권한<AC2>. 메시지 권한<AC2>. 시스템은 인가된 사용자에 의해 자원을 보호하기 위한 접근 제한<OS3>. 모든 사용자는 접근되는 데이터의 최대 보안성 및 무결성 수준을 식별하여 통과하는 수준을 가짐<OS3>

P.Authorization_Use TOE의 주체는 그에게 인가된 능력내에서만 객체에 접근 및 활용한다.

[적용사례] 정보는 인가된 목적으로만 사용<AC3>. TOE는 인가된 목적으로만 사용<Net4><Net6><Net7> 인가된 사용자들만 시스템에 접근 가능<OS1><OS2><OS3><OS4>

▸ 마킹(Marking)

P.Marking_Identification TOE내의 보안관련 객체에 대해 유일한 식별자를 부여한다.

[적용사례] 민감한 COI 정보는 물리적 또는 전자적인 표현에 관계없이 적절하게 식별<Net6>.

P.Marking_Level TOE내의 보안관련 객체에 대해 보안수준에 따라 ***수준의 등급을 부여한다.

[적용사례] 모든 자원은 포함된 데이터의 보안성 및 무결성 수준을 식별하도록 표시<OS3>. 정보의 표시<AC2>. 정보의 분류<OS1>. 모든 민감하지 않은 정보에 "Sensitive" 혹은 "COI" 표시<Net6>. 자료의 레이블링<DoD>

P.Marking_Output TOE의 보안관련 객체(특히 출력물)에 대해 보안수준에 따라 ***수준의 등급을 부여한다.

[적용사례] 출력문서의 모든 페이지 시작과 끝에 적절한 민감도 표시<OS3>

▸ 관리(Manage)

P.Manage_Process TOE내의 보안관리자는 객체에 대해 보안관리를 실시한다.

[적용사례] TOE는 운영되는 동안 실행되고 보존되는 보안기능처럼 관리 유지<AC7>. TOE는 운영되는 동안 실행되고 보존되는 보안기능처럼 관리유지<Net6>. 인가된 관리자는 IT 운영체제를 원격 관리<OS3><OS4>. 시스템 및 보안 관리자는 보호된 통신 채널을 통하여 TSE에서 장치를 원격 관리<Net6>. TCPA TPM과 개체 소유권<AC2>. TOE H/W, S/W 및 모든 다른 자원의 보안관련 문제 제어 관리<Net6>. 조직의 IT 시스템은 조직의 위험을 고려한 구현, 관리 및 운영<Net6>.

P.Manage_Persons TOE의 보안관리를 책임지는 보안관리자를 둔다.

[적용사례] TOE는 인가된 사용자만 관리<IDS1><IDS2><IDS3>. 인가된 관리자와 훈련된 유지보수자만 보안메커니즘 관리<Net6>. 인가된 관리자와 암호화 관리자는 역할을 따로 구분<OS3><OS4>. TOE 관리자들은 IT 환경의 보안성 유지를 보증할 책임<BIO1>. 각 서버 관리자의 권한은 그 관리자의 업무기능과 일관된 최소의 권한 부여<AC5>.

P.Manage_Procedure TOE의 보안관리를 위한 절차를 확립한다.

[적용사례] 정보관리를 위한 절차<Net5><Net6>

▸ 보안정책(Policy)

P.Policy_All TOE에대한 보안정책을 수립하고 이를 이행한다.

[적용사례] TOE 보안정책<AC2><AC6>. KRA는 KRA 정책 프레임워크에 의거하는 정책문서를 가져야하며, 이 정책에 따라 운영<AC7>. 키복구 정책의 명백한 정의 및 정책에 따른 TOE 구현<AC8>. TOE 구현 및 사용은 조직의 법률, 규칙 및 지침을 준수<Net4><Net6><Net7>

▸ 훈련(Train)

P.Training_All TOE의 인간 주체에 대해 보안관련 활동과 관련된 충분한 교육과 훈련을 실시한다.

[적용사례] 모든 사람들은 시스템 사용, 보안문제 및 취약성에 적절한 훈련이 필수<BIO1>. 모든 인가자의 책임 수준에 맞는 훈련<Net6>. TOE 모든 사용자 및 관리자는 TOE 운영에 앞서 TSF를 적절히 연습<AC7>

■ 보안기능보호(Function)

▸ 물리적 보호(Physical)

P.Physical_Control TOE의 객체(특히, 하드웨어)에 대해 물리적인 보호를 실시한다.

[적용사례] 물리적 보호<AC2>. 물리적 탬퍼링 발견 및 고지<DoD>

P.Physical_EMI TOE의 객체(특히 하드웨어)에 대해 물리적인 보호(특히, EMI)를 실시한다.

[적용사례] EMI 발행<AC2>

▸ 가용성(Avail)

P.Availability_All TOE의 객체는 인가된 객체의 요청에 대해 가용하도록 한다.

[적용사례] 정보의 가용성<AC2>. 통신망의 가용성<Net5> <Net6>

▸ 무결성(Integ)

P.Integrity_Contents TOE의 객체(특히, 데이터)는 무결성이 유지되도록 보호한다.

[적용사례] 내용 무결성<Net5><AC2>. TOE에 의한 데이터의 변경 보호<IDS1><IDS2><IDS3>. 악의적 코드의 방지<DoD>

P.Integrity_System TOE의 객체(특히, 시스템)는 무결성이 유지되도록 보호한다.

[적용사례] H/W, S/W 및 펌웨어의 무결성<Net5>. 시스템은 관리자의 도움으로 작동 상태 정기적 확인 및 감지된 오류 복구<OS3><OS4>. TOE 데이터와 기능 보

호<IDS1> <IDS2><IDS3>. TOE는 시스템 자원의 접근 제어 및 무결성 제공<AC7>. 정보를 낮은 권한 네트워크로 전송하기 위해 기밀성 및 무결성 보호 적용<Net6>. 강력한 무결성 메커니즘<DoD>. 운영적 무결성<DoD>. 보안기능 무결성의 검증<DoD>. 보안기능 수정으로부터 보호<DoD>.

▸ 기밀성(Sec)

P.Confidentiality_All TOE의 객체(특히, 시스템)는 기밀성이 유지되도록 보호한다.

[적용사례] 정보의 기밀성<Net5>

▸ 복구(Recovery)

P.Recovery_All TOE의 객체(특히, 시스템)은 고장 또는 보안기능 침해시 정상기능으로 정해진 시간과 피해정도 이내로 복구하는 절차와 기능을 갖는다.

[적용사례] TOE는 식별된 결점을 정정하는 절차 존재<AC6>. 원본 데이터를 포함하는 서버는 거의 즉시 복구 제공<AC1>. 통신망의 생존성 및 복구성<Net5>. 시스템 고장 후에 보호에 손상 없이 복구되는 안전한 절차 및/또는 메커니즘 제공<OS3><OS4>. 문서화된 복구<DoD>. 시스템 백업 절차, 최소한의 손실을 통한 복구(restoration)<DoD>. 효과적인 백업 복구(restoration)<DoD>. 신임된 시스템 복구<DoD>

■ 경고/고지(note)

P.Notify_Banner TOE의 주체(특이, 인간)가 객체에 접근하려할 때 가능한 위협과 위반시의 처벌내용을 알리는 경고문(배너)을 주체에게 표시한다.

[적용사례] 시스템은 사용자 제한, 정당한 일치 또는 사용자 시스템 접근 등의 초기 배너 표시<OS3><OS4>. 고장 경고<Net5>. 시스템 접근 배너(banners)<DoD>

P.Notify_Action TOE의 주체가 경고문의 내용을 위반했을 때 TOE는 이에 대한 적절한 행동을 취한다.

[적용사례] TOE에 의해 실시간 경고가 생성될 경우에는 관리자에 의해 신속하고 적절한 응답<AC5>. 사용자 스크린 로킹<DoD>

■ 구성(Config)

P.Configuration_All TOE는 설계된 대로 구성하고 형상을 관리한다.

[적용사례] 안전한 기본 설정<Net5>. TOE 서버설치 과정은 운영체제의 환경을 자동으로 검사하도록 수행<AC5>. 운영적 형상관리의 구현<DoD>

■ 운영보호(Operation)

P.Operation_Interoperability TOE는 분산적으로 운영시에 상호운용성을 갖도록 한다.

[적용사례] 상호운용성<Net5>

P.Operation_Update TOE의 운영관련 정보(또는 상태)를 최신의 것으로 갱신한다.

[적용사례] TOE 정보 갱신<Net5>

P.Operation_All TOE의 안전한 운영과 유지보수를 실행한다.

[적용사례] TOE는 통신 채널을 통한 공격의 부적절한 운영으로부터 방어<Net6>. 권한을 가진 클라이언트 사용자는 부재시 그의 기계를 안전한 상태로 유지<AC5>. 예방적 유지보수<DoD>

■ 지침(Guidance)

P.Guidance_All TOE는 TOE의 설치, 사용, 운영 등에 관한 지침을 문서로서 제공한다.

[적용사례] 설치 및 사용 안내서 제공<Net4><Net5><Net7><AC2>. 생체인증시스템 고장이나 비상시 포털 개방을 위한 매뉴얼 제공<BIO1>. 명세서 참조<AC2>. 특권화된 사용자 문서<DoD>. 일반 사용자 문서<DoD>

■ 생명주기(Lifecycle)

P.Lifecycle_All TOE의 개발 생명주기(분석, 설계, 구현, 시험, 운영 및 유지보수)전체동안 보안성을 유지한다.

[적용사례] 시스템 라이프사이클 단계들에 보안 통합<AC2>. 생명주기 동안 보안<DoD>

■ 취약성(Vul)

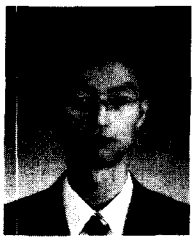
P.Vulnerability_Test TOE의 취약성을 파악하기 위한 보안시험을 실시한다.

[적용사례] 운영체제는 독립적인 취약성 분석의 부분으로 독립적인 시험<OS3><OS4>. 시스템 기능시험<DoD>

P.Vulnerability_Search TOE의 알려진 취약성과 잠재적인 취약성을 조사 및 분석한다.

[적용사례] 시스템의 명백한 취약성 분석<OS3><OS4>

〈著者紹介〉



고 정 호 (Jeong-Ho Ko) 정회원

1997년 : 한남대학교 전자계산공학과 공학사
1999년 : 한남대학교 컴퓨터공학과 공학석사
2002년 : 한남대학교 컴퓨터공학과 공학박사
2002년~현재 : 영진전문대학 컴퓨터정보기술계열 교수
<관심분야> 정보보호시스템, 소프트웨어공학, 객체지향 프로그래밍

이 강 수 (Gang-Soo Lee) 정회원

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