CC 개념을 이용한 공통 보안요구사항명세서 개발방법론

장세진*, 최상수*, 이강수*, 채수영**, 김춘수**
*한남대학교 컴퓨터공학과
**국가보안기술연구소
{dar, gcss09}@se.hannam.ac.kr*, gslee@mail.hannam.ac.kr*, {sychae, jbr}@etri.re.kr**

A Common Security Requirement Specification by Using CC Paradigm

Se-Jin Jang*, Sang-Soo Choi*, Gang-Soo Lee*, Soo-Young Chae**, Choon-Soo Kim**
*Dept of Computer Engineering, Han-Nam University
**National Security Research Institute

요 약

조직의 정보를 안전하게 관리하기 위해서는 보안정책이 마련되어야 하며, 이에 따라 보안시스템을 개발하고 보안정책에 따라 보안관리가 이루어져야 한다. 이를 위해 조직의 정보시스템에 대한 위협 및 취약성을 파악하고 그에 따른 조직의 보안환경을 분석하여 보안시스템의 정확성(Correctness)과 효율성(Effectiveness)을 증대 시켜야 한다. 본 논문에서는 CC의 개념을 이용하여 조직을 대상으로 한 공통 보안요구사항 명세서 개발방법론을 제시한다.

1. 서론

정보기술의 발달과 정보화가 확대됨에 따라 정보시스템에 대한 중요도가 커져가고, 조직내의 자원과 정보시스템을 보호하는 조직의 보안시스템의 중요성 또한 커져가고 있다. 조직에서는 다양한 정보시스템을 운영하고 있으며 이러한 정보시스템은 조직에 관련된 민감한 정보를 소유하고있다. 따라서, 정보시스템을 안전하게 관리, 유지하기 위하여 조직의 정보시스템에 대한 보안환경 분석 및 보안정책에 따른 보안시스템 개발과 보안관리가 이루어져야 한다. 이를 위하여 조직의 정보시스템에 대한 위협 및 취약성 파악 등의 보안환경 분석을 통하여 조직의 정보보호 시스템의 신뢰성을 증대 시켜야 한다.

이러한 배경에서, 본 논문에서는 CC의 개념을 이용하여 조직의 주요업무, 주요자료, 주요 정보시스템 등에 따른 "공통 보안요구사항명세서" 개발 모델을 제시한다.

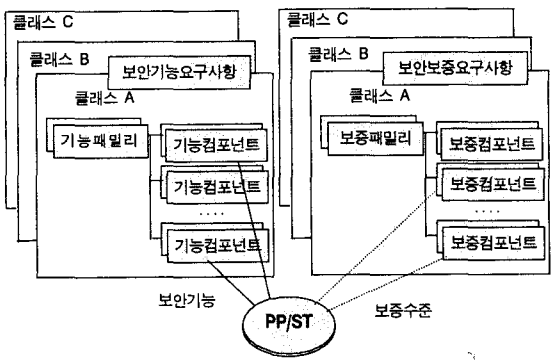
본 논문의 2장에서는 관련연구로써 CC[1~4]의 개념 및 평가·인증 절차와 CCToolBox/PKB[5,6]를 소개하고, 3장에서는 보안요구사항명세서 개발 모델을 제시한다. 4장에서는 제시한 개발 모델을 이용하여 실제 특정 조직에 대한 보안요구사항명세서 개발 시나리오를 제시하고, 끝으로 5장에서 결론을 맺는다.

2. 관련연구

2.1 CC의 개념

CC는 모든 정보보호시스템에서 필요로 하는 보안기능요구사항의 전체집합을 계층적으로 분류하고 있으며, 보안기능에 대한 구현의 정확성에 대한 보증요구사항의 전체집합을 계층적으로 분류하고 있다. 특히, CC에서 제시된 전체 보안기능 및 보증요구사항으로부터 제품군별 공통보안요구사항인 보호프로파일(PP: Protection Profile)과 특정 보안제품별 보안요구사항인 보안목표명세서(ST: Security Target)를 이용하여 개발 및 평가를 수행하고 있다.

즉, 공통평가기준은 IT 제품 및 시스템의 보안성을 평가하기

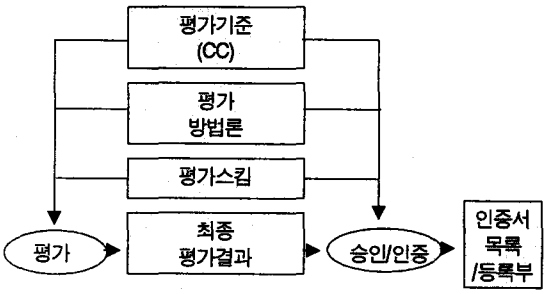


<그림 1> CC의 구성과 사용의 개념

위한 기초가 되는 기준을 정의하며 <그림 1>에서처럼 특정의 보안요구사항을 설정하기 위하여 클래스-패밀리-컴포넌트로 구성된 공통의 보안기능요구사항 및 보안보증요구사항이 제공된다. 그리고, 보안기능과 보안기능의 평가과정에 적용되는 보증수단에 대한 공통의 요구사항을 제시함으로써, 독립적으로 수행한 보안성 평가 결과들간에 상호비교를 가능하게 한다. 이를 통해 일관성 있는 평가 수행으로 IT 제품 및 시스템의 보안성 및 신뢰성을 향상시킬 수 있고 이러한 단일의 기준을 준수함으로써 평가의 불필요한 중복을 방지하고 공정하고 재사용성을 높일 수 있는 기반을 마련하게 된다.

2.2 CC에서의 평가 · 인증 절차

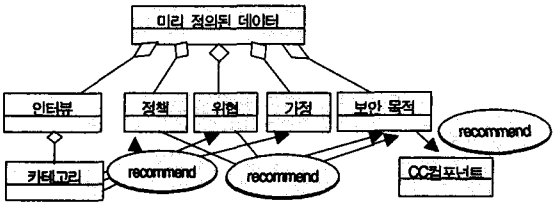
평가결과간의 비교가능성을 높이기 위하여 평가는 평가스킴의 틀에 따라 수행되어야 한다. 평가스킴은 규범을 수립하고 평가의 신뢰도를 검증하며, 평가기관과 평가자가 지켜야 하는 규정을 감독한다. <그림 2>는 CC에서의 평가 · 인증절차 구성요소를 보여준다[1,2]. 이러한 인증절차에 따른 공통평가기준은 평가결과의 반복성과 객관성을 높여준다.



<그림 2> CC에서의 평가인증절차

2.3 CCToolBox/PKB의 구조

NIST에서는 보호프로파일과 보안목표명세서의 개발을 지원하기 위하여 공통평가기준을 기반으로 한 CCToolbox라는 도구를 개발하였다. 또한 이 도구에서 사용되는 미리 정의된 위협, 공격, 보안목적, 가정사항, 정책문장인 Profiling Knowledge Base(PKB)라는 데이터베이스를 개발하여 공개하고 있다. CCToolBox/PKB는 <그림3>와 같은 구조를 갖고 있다. 인터뷰를 이용하여 PKB에서 미리 정의된 정책, 위협, 가정의 보안환경을 검색하여 보안목적을 도출한다. 그리고 보안목적을 구현하기 위하여 각 보안목적에 해당하는 CC의 보안요구사항 컴포넌트를 제시하여 준다. CCToolBox는 미리 정의된 데이터를 이용하여 PP/ST를 편리하고 빠르게 작성할 수 있도록 지원해준다[5,6].



<그림 3> CCToolBox/PKB의 구조

3. 보안요구사항명세서 개발 모델

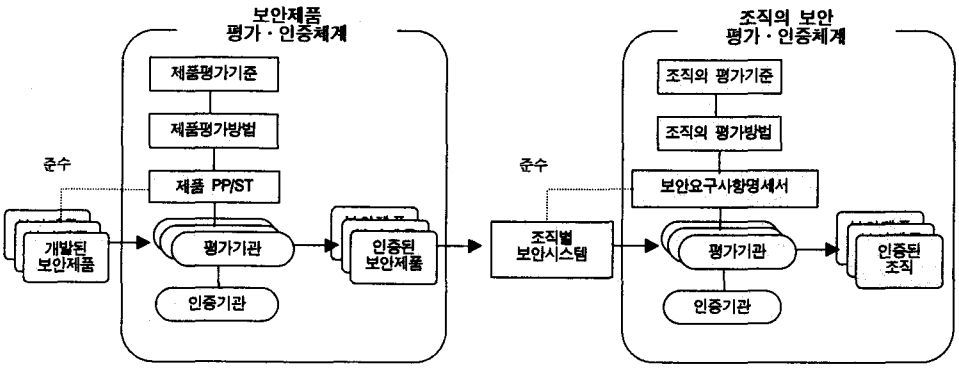
3.1 조직의 보안평가 · 인증체계

<그림 4>에서의 왼쪽의 "보안제품 평가 · 인증체계"는 <그림 2>의 현행체제(CC에서의 평가인증절차)를 확장한 것이며, 오른쪽의 "조직의 보안 평가 · 인증체계"는 조직의 공통 보안요구사항 명세서가 개발되어질 가상의 평가 · 인증체계를 나타낸다. 본 논문에서는 "조직의 보안평가 · 인증체계"에서 필요로 하는 "공통 보안요구사항명세서"를 개발하는 것이다.

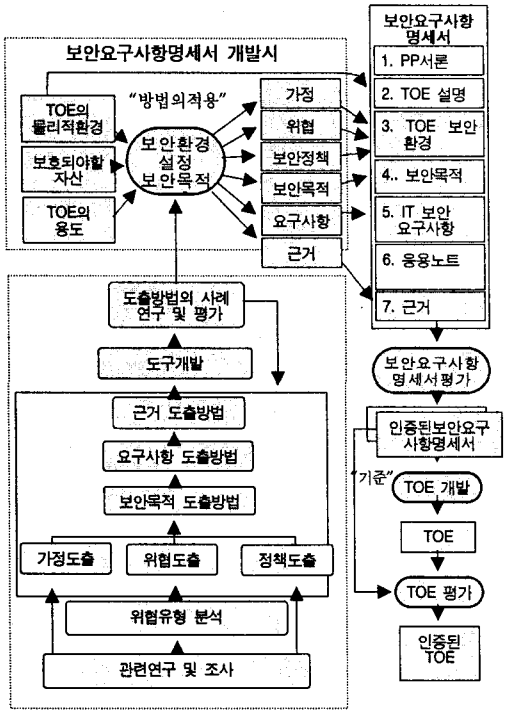
3.2 제안 모델

본 논문에서 제시하는 공통 보안요구사항명세서 개발 모델은 <그림 5>와 같다.

(1) 위협유형의 분석



<그림 4> 보안제품과 조직의 보안평가 · 인증체계의 구성



<그림 5> 조직의 보안요구사항명세서 도출 과정

조직의 자산을 일정한 수준으로 체계화시키기 위하여 PP/ST 작성가이드, CC, OCTAVE[7], CSE[8], BS7799[9], PRAM[10]등에서의 자산분류체계를 분석한다. 결과를 바탕으로, 조직의 자산분류 체계를 정의하여 보안요구사항명세서 작성도구의 자산 DB 스키마로 사용한다.

(2) 보안환경(가정, 위협, 정책)도출

① CC 및 PP/ST 작성가이드[11]의 가정사항문장과 기존 PP[12,13]의 가정사항문장, 그리고 CCToolBox/PKB에서의 가정사항문장을 조사하고 분류하여 "공통가정사항문장"을 도출하고 보안요구사항 명세서 작성 도구에서 가정사항문장 DB로 사용한다. ② 기존의 PP, CVE 및 CC ToolBox/PKB에서의 취약성 및 위협을 조사하여 "공통위협사항문장"을 도출하고 도구에서 위협사항문장 DB로 사용한다. ③ SANS[14]와 BS7799등의 보안관련 문서에서 보안정책에 관한 일반사항을 조사하고 실제로 사용중인 DoD, 국가기관, 민간기관등의 조직에서의 보안정책을 조사·분석하여 "공통보안정책목록"을 도출하고 이를 도구에서 보안정책문장 DB로 사용한다.

(3) 보안목적도출

기존의 PP 및 CC ToolBox/PKB로부터 보안목적을 조사하고 보안환경(가정, 위협, 정책)과 보안목적과의 대응관계를 파악하여 보안환경에 대한 "공통보안목적"을 도출하고 도구에서 보안목적 문장 DB로 사용한다.

(4) 보안요구사항 도출

기존 PP 및 CC ToolBox/PKB로부터 보안목적에 해당하는 보안요구사항을 파악하고 보안환경과의 대응관계를 분석하여 보안목적에 대한 "공통의 보안요구사항"을 도출하고 도구에서 보안요구사항문장 DB로 사용한다.

(5) 근거 도출 방법

기존 PP 및 CC ToolBox/PKB에서의 보안환경, 보안목적, 보안요구사항간의 대응관계를 분석하여 대응관계의 타당성을 파악한다.

(6) 조직의 보안요구사항명세서 개발도구

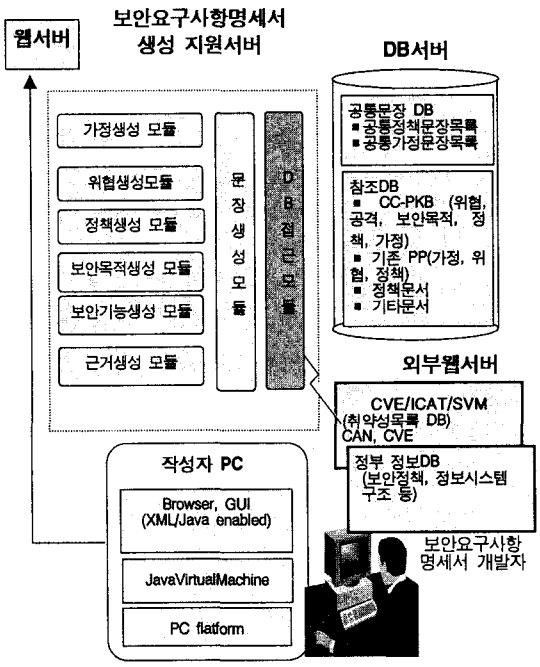
CC ToolBox의 분석을 통하여 문제점을 파악한다. (1)~(5)의 결과를 바탕으로 도구에서 사용될 수 있도록 데이터베이스를 설계한다. CC ToolBox의 문제점을 극복할 수 있는 방안을 제시하고 DB설계를 토대로 <그림 6>과 같은 구조를 갖는 시제품을 개발한다. <그림 7>은 보안요구사항명세서 개발도구의 사용자 인터페이스를 보인다.

(7) 도출방법의 사례 연구 및 평가

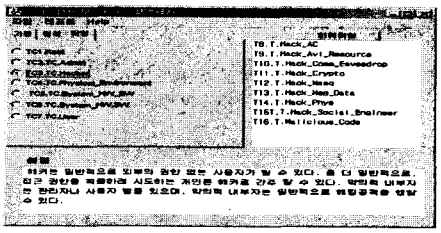
개발된 도구를 이용하여 모의 테스트 등의 자체 검증을 통하여 도구의 실효성을 시험해 본다. 시험의 결과가 미흡할 경우에는 하위 작업을 반복하여 도구의 효율성을 높인다.

(8) 보안요구사항명세서 개발

특정 조직을 선정하여 자산, 보안정책, 위협, 가정사항을 파악하고 도구를 활용하여 보안환경을 분석한다. 보안환경 분석을



<그림 6> 보안요구사항명세서 개발도구의 구조



<그림 7> 보안요구사항명세서 개발도구 사용자 인터페이스

통하여 조직의 보안목적과 이를 구현할 수 있는 보안요구사항들을 도출한다. 그리고 이러한 요구사항도출의 타당성을 입증할 수 있는 근거를 작성한다.

4. 조직의 보안요구사항명세서 개발 시나리오

본 논문에서는 조직의 보안요구사항명세서 개발 시나리오를 수행하기 위하여 다음과 같은 가정을 세웠다.

- 조직에 대한 보안평가/인증체계가 구성되어 있다.
- 보안요구사항명세서 개발도구가 개발되어 있다.

① 조직의 업무별 보안환경(자산, 가정, 위협, 정책)을 파악하여 관련자로부터 검토를 받는다. <표 1>은 보안환경 기술양식의 예를 보여준다.

<표 1> 조직별 보안환경 분석결과 기술 양식

조직	업무	보안정책	위협	가정	확인
조직1	업무1	P.Notify,..	T.Modify,..	A.Admin,..	
	업무2				
조직2					
조직n					

② 보안요구사항명세서 개발도구를 활용하여 보안목적문장들을 자동생성하고 조직의 관련자로부터 검토를 받는다.

③ 보안환경과 보안목적을 바탕으로 보안요구사항을 도출한다. 보안보증수준 및 보안강도를 선택한다. <표 2>는 업무별 보증수준, 보안강도, 보안기능을 기술하는 양식의 예를 보여 준다.

<표 2> 업무별 보증수준의 도출의 예

조직/업무	보안보증수준 요구사항	보안강도 요구사항	필요보안기능
회계자료처리	EAL 4	중(Medium)	F1, F3, F6....
인사자료처리	EAL 2	하(High)	F5, F7, F9...
..	..	..	..

④ 보안환경, 보안목적, 보안요구사항과의 대응관계를 바탕으로 근거를 작성한다. <표 3>은 조직의 근거 작성의 기술양식의 예를 보여준다.

5. 결론

<표 3> 보안목적, 보안요구사항 및 근거의 작성표

조직	업무	보안목적	보안요구사항	근거
조직1	업무1	O.AUDIT,...	FIA_UID, ...	
	업무2			
조직2				
조직n				

본 논문에서는 조직의 보안환경 분석을 기반으로 조직의 정보시스템의 신뢰성과 안정성을 보장하기 위하여, CC의 개념 즉, 전체 보안기능 및 보증 요구사항 집합으로부터 제품군별 또는, 특정 제품별 보안기능 및 보증 요구사항인 PP/ST를 작성하는 클래스와 인스턴스의 객체지향적 개념을 응용하여 조직에 대한 공통 보안요구사항명세서 개발방법을 제시하였다. 또한, CCToolBox를 보완한 조직의 공통 보안요구사항 명세서 개발도구를 제시하였다. 조직에 대한 공통 보안요구사항 명세서 개발은 기존에 시행된 적이 없으므로 본 개발방법에 대한 실용성과 효과성에 대해 검증할 방법이 마련되어 있지 않다. 향후 이와 같은 문제점은 보안요구사항 명세서 개발자들이 본 방법론을 검증하고 문제점을 발견하고 개선함으로서 다소 극복되어질 수 있을 것이다.

6. 참고문헌

[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] NIAP, CC Toolbox Reference Manual, Version 6.0f.

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

[7] OCTAVE, "OCTAVE Criteria, Version 2.0", Carnegie Mellon Software Engineeirng Institute(2001.12), OCTAVE Method Implementation Guide Version 2.0, 2001. 6.

[8] CSE, "A Guide to Security Risk Manaement for IT Systems", Government of Canada, Communications Security Establishment, 1996.

[9] ISO/IEC, Internation Standard ISO/IEC 17799:2000 - Code of Practice for Information Security Management, ISO17799/BS7799, 2000. 12.

[10] 김정덕(외), "위험분석도구 기초기술 개발에 관한 연구", ETRI 연구보고서, 2001.

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

[12] Protection Profiles http://www.commoncriteria.org/protection_profiles/index.html.

[13] 정보보호시스템 보호프로파일, 국가정보원, 2003. http://www.nis.go.kr.

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