정보보호시스템 평가관리시스템 설계

강 연 희*, 방 영 환*, 이 강 수**
(*) 한남대학교 컴퓨터공학과 ({ dusi82, bangyh}@se.hannam.ac.kr)
(**) 한남대학교 정보통신멀티미디어공학부 교수(gslee@eve.hannam.ac.kr)

A Design of Evaluation Management System for Information Security System

Kang Yeon hee*, Bang Young hwan*, Lee Gang Soo**
(*)Dept. of Computer Engineering. Han Nam University
(**)Dept. of Computer Science, Han Nam University

요 약

정보화 역기능으로부터 주요 데이터를 보호하기 위해서는 안전성과 신뢰성이 검증된 정보보호시스템을 사용하여 정보보호 수준을 향상시킬 수 있도록 정보보호시스템 평가·인증제도에 대한 필요성이 더욱 높아지고 있다. 또한, 정보보호시스템의 수가 많아지고 다양화됨에 따라, 시험/평가업무량도 증대 될 것이며 국내 평가관리의 중요성이 점차 증가하고 있다. 따라서 본 논문에서는 각종 평가기관에서 평가의 효율성(최소의 비용으로 최대의 평가업무를 수행)을 기하기 위해, 세부평가기술의 통합하고 평가결과 관리를 위한 그룹웨어인 정보보호시스템 평가관리시스템(EMS)을 제시한다.

1. 서론

최근 평가·인증의 인식이 확산되면서 정보보호시스템의 경우에도 공정한 평가 및 인증이 필수가 되며 다른 응용서비스 제품과 달리 정보보호시스템은 사용자의 신뢰를 획득하기 위해 보안기능에 대한 정확성과 효율성 검증을 통하여 제품의 신뢰성에 대한 보증이 요구된다. 평가 및 인증의 결과는 마케팅 전략으로 활용되며 좋은 평가는 정보보호시스템 제품의 신뢰도를 높여 생존률을 높여준다.

1990년대 이후로 정보보호시스템의 수와 평가와 인증에 대한 수요가 폭발함에 따라 평가업무 또한 증대되고 있으며 선진 각국에서는 정보보호시스템의 보안성에 대한 신뢰성 확보를 위하여 평가와 인증을 위한 기준(예:TCSEC, ITSEC 등)들을 개발하고, 공정하고 객관적인 평가를 시행할 수 있는 평가체계를 구축하여 왔다. 90년대 후반부터는 국제 표준 평가기준이라 할 수 있는 노력의 산출물로서 국제공통평가기준(CC : Common Criteria)[1]을 개발하기 시작하여 ISO/IEC에서 그 최종 기준을 CC Version 2.1(ISO/IEC 15408)을 1999년 8월에 발표했으며 국제 공통 평가기준은 현재 대부분의 선진국에서 평가·인증제도에 적용되고 있다.[2]

선진국에서는 정보보호시스템의 평가방법론 등 평가기술을 확보하고 있고 국내에는 한국정보보호진흥원에서 시험/평가 업무를 수행하고 있다. 그러나 실제평가를 위해서는 평가자들의 세부평가기술(예: 시험기술, 도구기술 등)이 필요하며 국내에는 시험 도구 및 시험방법론의 부재 등 세부평가기술이 부족한 실정이다. 국내 시험기술력 향상 및 보급을 통한 국가 경쟁력 향상과 효율적인 평가(최소비용 최대효과)를 이루기 위한 국내 시험평가 기반마련이 필요하다.[3]

본 논문에서는 CC를 기반으로 평가기관에서 효과적으로 각종 세부평가기술을 통합하고 평가결과를 관리 할 수 있는 그룹웨어인 정보보호시스템 평가관리시스템(EMS : Evaluation Management System)을 설계하였다. 본 논문의 2장에서는 평가관리시스템 설계를 위해 정보보호시스템 평가 및 절차에 대해서 조사(연구)하였으며 3장에서는 평가관리를 정의하고 평가관리시스템의 요구사항을 보였다. 4장에서는 평가관리의 기반이 되는 일반평가모델과 평가 데이터베이스 스키마 및 평가 워크플로우 모델을 정의하였으며 5장에서는 본 연구에서 설계한 정보보호시스템 평가관리시스템 개발 환경 및 구조 등의 설계사항에 대하여 제시하였다. 마지막으로 6장에서 결론을 맺는다.

2. 정보보호시스템의 평가절차

2.1 정보보호시스템의 평가체계

정보보호시스템의 공정하고 객관적인 평가는 필수적이며 그 결과는 제삼자에 의해 평가되고 인증된다. 인증체계를 구성하는 주체들은 평가기준에 따라 평가를 실시할 때 적절성, 공정성, 완전성, 객관성, 반복 및 재생성 등의 평가원칙을 지켜야 하며 그림 1은 정보보호시스템의 시험/평가시 주체들간의 관계를 보인다. 다음은 평가에 관련된 구성요소들이다.

1) 평가대상물(정보보호시스템) : 침입차단시스템(firewall), 침입탐지시스템(IDS), 바이러스백신, 스마트카드, 보안 운영체제 등이 평가대상물이 될 수 있으며 평가대상물의 실체를 그대로 반영한 모든문서((예 : 설계명세서, 분석명세서, 소스코드, 시험결과서, 운영문서, 개발환경문서 등의 전달물)를 이용한다.
2) 평가기준 : 일반적인 정보보호시스템에 적용할 수 있는 기준들로서 현재 ISO/IEC 15408(국제표준이며 CC라함[1]), ITSEC(유럽연합표준), TCSEC(미국표준), CTCPEC(카나다표준), 「침입차단시스템평가기준」(한국) , 「침입탐지시스템평가기준」(한국), 「공통평가기준」(한국) 등이 나와 있다.
3) 평가지침 : 평가기준을 각 국가의 법률 및 보안정책에 따라 수정하여 운영하는 것을 말하며 CEM(CC 평가지침[4]), ITSEM(ITSEC 평가지침[5]), 침입차단/침입탐지시스템 평가지침(한국), 공통평가지침(한국) 등이 있다.
4) 평가방법론 : 평가원칙 준수를 위해 평가기준들에 대한 평가방법론(How)이 필요하며 평가방법론은 추상적인 개념으로서 평가기관의 평가기술(노하우)이다.
5) 국가스키마 : 한국 정보보호시스템 평가 및 인증체계(국가정보원, 한국정보보호센터), 영국 UK-ITSEC Scheme, 미국 CCEVS, 카나다 CCBCCS, 프랑스 FECS, 독일 GBCS, 호주 AISEP 등이 존재한다.

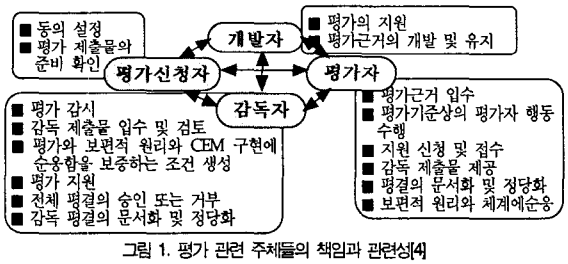


그림 1. 평가 관련 주체들의 책임과 관련성[4]

2.2 평가 절차

평가는 수개월에서 2년 이상이 걸리며 수 천만원에서 수 억원의 비용이 소요되는 업무로서 일반적으로 다음과 같은 단계를 거쳐 평가가 행해진다.

① 준비 단계 : 평가의 계약, 예비 평가, 제출물에 관한 합의가 이루어지며 미국 TPEP의 경우 7~10일에 5명의 평가자가 참여한다.
② 평가 단계 : 정식평가가 이루어진다. 평가보고서(ETR)와 관찰보고서(OR)를 작성하며 평가신청인과 긴밀히 접촉해야한다. 보증수준 및 제품 유형에 따라 수 개월부터 수 년이 소요된다.
③ 인증 단계 : 인증기관은 평가자가 제출한 평가보고서를 검토하고 평가요약보고서(ESR)와 인증보고서(CR)를 작성하여 공표하며 수 개월정도 소요된다.
④ 인증유지 또는 재평가단계 : 평가되어 사용중인 제품의 버전을 확장하거나 플랫폼이 바뀐 경우 이전의 보증수준을 유지하는 과정이다. 이전의 평가결과와 제출물을 사용하므로 최초의 평가비용보다는 적게 소요된다.[3,6]

3. 평가관리의 정의 및 평가관리시스템의 요구사항

3.1 평가관리의 정의

평가대상에 따라 평가구조를 결정한 후 평가구조에 의거하여 평가환경을 조성하는 것을 "평가관리"라 하며 평가관리는 프로젝트 및 프로세스 관리의 개념으로부터 발전한 개념이다. 관리자는 평가신청자에 의해 제출된 평가대상물(정보보호시스템) 및 평가자들간의 업무 및 자원할당(예 : 평가도구, 제출물(문서, 소스코드), 평가기준, 평가지침 등)을 하고 평가자들에 의해 도출된 평가결과의 흐름을 관리하며 평가관리의 흐름은 평가 원칙과 절차를 따른다.

* 본 논문은 한국과학재단 RRC(과제번호 : R12-2003-004-01001-0) 연구비지원에 의하여 수행되었음.

3.2 평가관리 시스템의 요구사항

평가의 공정성과 평가제도의 합리성에 대한 소비자와 개발자의 요구가 증대되었으며 객관성이 보장되도록 평가업무를 원활하게 처리하기 위하여 평가관리의 필요성이 대두되었다. 평가관리시스템(EMS)에서 요구되는 사항은 다음과 같다.

- "평가 흐름 관리"기능 : "정보통신" 및 "분산" 컴퓨터 환경에서 평가신청자(개발자)의 평가제출물 및 평가자의 업무분담과 자원(평가도구, 평가기준 등)할당 등의 평가의 흐름을 관리할 수 있어야 함.
- "현황" 파악 기능 : 평가제출물과 자원에 대한 현황 파악과 모든 관련된 평가 업무들의 파악 가능해야함.
- 평가에 대한 정보공유 및 관리 : 중앙형 평가 DB를 사용하여 제출물, 평가도구, 평가자활동, 평가기준, 평가결과 등을 평가서버에 설치.
- "평가자의 업무분할 구조"기능 : 평가신청자가 제출한 제출물의 특성과 평가방법, 평가도구 등에 따라 평가업무를 분할하는 것이 가능할 것.
- "비용 관리"기능 : 평가에 관한 예산과 실제 비용 추적이 가능해야 함.
- "문서일관성 분석"기능 : 평가기준에 따라 제출물의 문서내용이 일치함을 분석 가능할 것.

4. 정보보호시스템 평가모델

4.1 일반 평가모델

일반적으로 정보보호시스템의 평가모델이란 국내외의 평가기준 및 절차들을 추상화한 것으로서, 정보보호시스템의 평가체계를 이해하는데 활용할 수 있다. 평가모델은 CC와 ITSEC에 기반을 두고 있으며 그림 3은 본 연구에서 사용할 정보보호시스템의 개발 및 시험/평가 시스템의 모델이다. 개발활동에서는 개발자가 요구사항 명세서, 평가기준 및 개발도구를 이용하여 XML기반 DTD문서 스키마를 사용한 개발 결과(제출물)[7]를 생성하고 "평가활동"에서는 평가자가 평가기준과 개발결과를 이용하여 평가도구를 활용하여 평가결과(평가보고서)를 생성한다. 특히, 평가기준은 개발활동과 평가활동에서 동시에 사용된다.

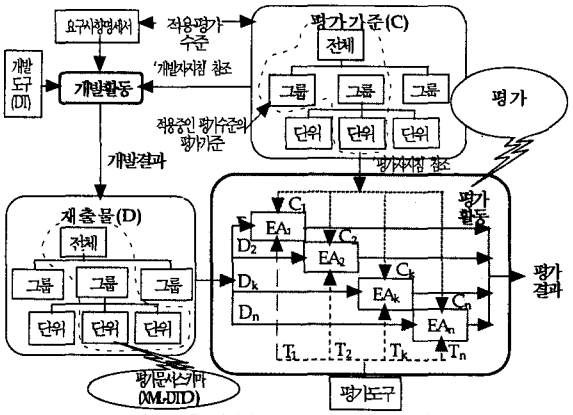


그림 3. XML 기반의 정보보호시스템 시험/평가의 모델

4.2 평가 데이터베이스 스키마

평가 전체를 관리하고자 할 때 평가대상물 즉, 제출물에 평가자 및 평가도구를 할당하고 이를 조정, 관리, 실행하는 시스템을 "평가 워크플로우 관리시스템(EWFMS)"이라 하며 EWFMS내부에는 평가 데이터베이스와 그룹웨어(CSCW)를 포함하고 있다. 다음은 EWFMS를 구축할 때 필요한 "평가 데이터베이스(EDB)스키마"를 정의한다.[8,9]

CC기반 정보보호시스템의 평가환경을 구축하기 위해서는 CC 평가를 위한 entity와 그들과의 관계(즉, Entity-Relationship)를 모델링할 필요가 있다. 본 결과는 평가기관내의 평가관리 데이터베이스 또는 EWFMS의 개발을 위한 설계명세로써 직접 활용될 수 있다. 그림 4는 정보보호시스템의 평가모델로부터 도출한 ER 다이어그램을 보인다(각 엔티티의 속성들은 생략함) .

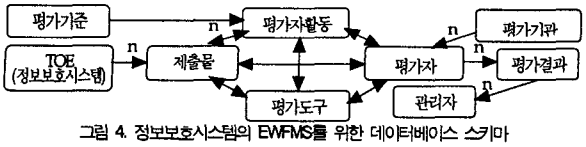


그림 4. 정보보호시스템의 EWFMS를 위한 데이터베이스 스키마

① 엔티티 정의(엔티티 테이블)

- 평가대상물 = **<평가대상물_id**, 개발자_id, 평가신청자_id, 기타>
- 제출물 = **<제출물_id**, 경로, 소속평가대상물_id, 제출물내용, 전달일, 기타>
- 평가기준 = **<기준_id**, 경로, 등급, 기타>
- 평가자활동 = **<평가자활동_id**, 경로, 소속기준, 종속활동_id, 기타>
- 평가기관 = **<평가기관_id**, 경로, 평가기관주소, 지정만료일, 최고평가수준, 기타>
- 평가자 = **<평가자_id**,경로, 평가자명, 소속, 직무, 비밀취급등급, 주소, 기타>
- 평가도구 = **<평가도구_id**, 경로, 도구기능, 기타>
- 평가결과 = **<평가결과_id**, 경로, 평가등급, 기타>
- 관리자 = **<관리자_id**, 경로, 관리자명, 직무, 비밀취급등급, 기타>

② 속성 정의(속성 테이블)

- 평가대상물-제출물 = **<평가대상물_id, 제출물_id**, 제출일, 기타>
- 제출물-평가자활동 = **<제출물_id, 평가자활동_id**, 기타>
- 제출물-평가도구 = **<제출물_id, 평가도구_id**, 기타>
- 제출물-평가자 = **<제출물_id, 평가자_id**, 할당일, 기타>
- 평가기준-평가자활동 = **<평가기준_id, 평가자활동_id**, 기타>
- 평가자활동-평가도구 = **<평가자활동_id, 평가도구_id**, 기타>
- 평가자활동-평가자 = **<평가자활동_id, 평가자_id**, 시작일, 종료일, 기타>
- 평가기관-평가자 = **<평가기관_id, 평가자_id**, 발령일, 기타>
- 평가자-평가도구 = **<평가자_id, 평가도구_id**, 할당일, 종료일, 기타>
- 평가자활동-평가결과 = **<평가자활동_id, 평가결과_id**, 평가결과, 평가일, 기타>
- 평가결과-관리자 = **<평가결과_id, 관리자_id**, 평가결과, 할당일 종료일 기타>

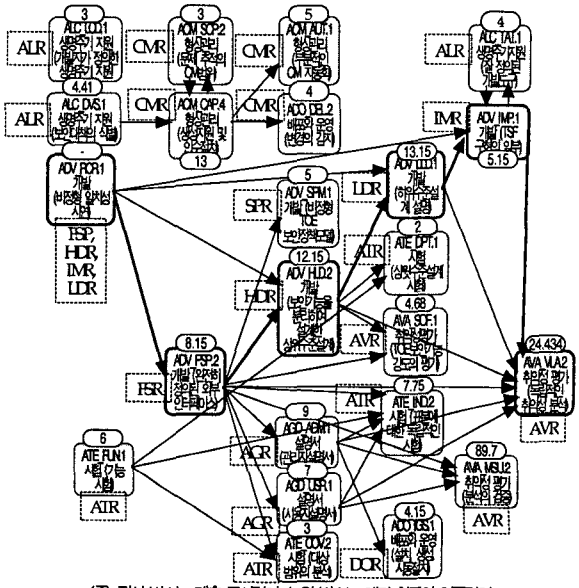
③ 질의의 예

각 테이블로부터 다음과 같은 사항들을 검색할 수 있다.

- 평가자 목록을 검색하라 : '평가자' 테이블 전체 출력
- 평가자가 평가한 평가결과를 검색하라
- 제출물의 제출현황과 침투시험도구를 사용해야할 시간과 평가자를 검색하라.
- 상세설계 보고서의 평가시에 필요한 평가도구를 검색하라
- 오는 2003년 12월에 인가가 만료되는 평가기관명을 검색하라 : '평가기관' 테이블 중 selection

4.3 평가 워크플로우 모델

"평가 워크플로우 모델"이란 평가에 관련된 일련의 단위업무들로 구성되는 워크플로우를 정의 및 분석하는 것이며 평가환경과 평가업무 프로세스를 적절히 표현한 것이다. CC의 평가등급은 EAL1~EAL7등급까지이며 TCSEC과는 달리 보안기능에 대한 등급은 없다. 그림 5는 CC/EAL4를 위한 워크플로우 예(평가실시 활동 부분)이며, 평가에 필요한 제출문서와 해당활동의 평가 업무량을 함께 기록하였다. EAL4는 일반적으로 평가를 염두에 두고 개발되지 않은 제품과 시스템에 적용 가능하며 본 연구의 평가실시에 사용될 수 있다.



(주) 점선 박스는 제출 문서명이며, 원 박스는 해당 활동의 업무량임
그림 5. CC/EAL4를 위한 워크플로우의 예(평가실시 활동 부분)

5. 정보보호시스템 평가관리시스템 설계

5.1 평가 기반기술

평가관리시스템(EMS)에서는 평가기준의 통합관리 및 시험/평가관리와 평가도구기술, 문서일관성 분석기술, 침투시험기술이 기반이 되어야 한다. 이러한 기술들을 개발하기 위해 SW시험기술, 컴포넌트기반 SW공학, 그룹웨어, 워크플로우, 프로세스관리, 문서공학, 데이터베이스 등의 기술을 활용한다.

1) 평가기준 통합관리 기술 : CC를 기반으로 ITSEC, TCSEC 등의 다양한 평가기준들을 분석 및 식별한 평가기준의 스키마를 평가 DB에 활용한다.
2) 평가도구기술 : 오류발견과 분석기술 등의 평가기술을 적용한 평가도구를 사용하여 정보보호시스템의 성능시험에 활용하며 평가도구는 자원으로서 평가 DB에 저장된다.
3) 침투시험기술 : "정보보호시스템 평가의 최후의 수단"이며 효과성 평가에 가장 적절한 방법이다. 침투자가 시스템의 보안수단(메커니즘, 기능 등)을 우회할 수 있는지 시험하며 가장 중요한 평가도구기술이 된다. 침투시나리오의 명세언어는 추상적이며 이 분야는 향후 연구 과제로 미룬다.
4) 문서일관성 분석기술 : 정보보호시스템의 개발시 요구되는 보안 기능들의 완전하고, 정확한 표현과 내부적인 일관성의 충족, 그리고 상위 단계의 내용을 제대로 따른다는 합리적인 증명을 위해서는 문서의 일관성은 필수적이다. 문서일관성 분석도구로는 SODOS 등이 존재한다.[3]
5) 시험/평가관리기술 : 정확성과 효율성을 시험 및 평가하기 위해 평가신청자(개발자)의 평가제출물 및 평가자의 업무분담과 자원(평가제출물, 평가도구, 평가기준, 시험 기술(DB) 등)할당 등의 평가 흐름관리 기술로서 본 논문에서 평가관리시스템(EMS)의 기반 기술이 된다.

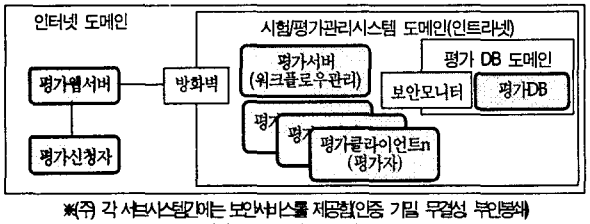
5.2 개발환경

해당 시스템 구조는 웹기반 및 인트라넷 기반(클라이언트-서버)으로서 보안기능이 강화된 Windows 계열(98/2000/NT)과 MySql ODBC Driver, JDBC Driver를 사용한다. 개발 언어는 Java(Swing API), 파워스크립트를 사용하며 유지보수 환경은 별다른 환경을 필요로 하지 않는 방향으로 개발될 것이나, 실제 정보보호시스템 평가관리를 수행 시 발생할 수 있는 특수한 상황으로 인한 필요 기능이 있을 때 추가할 수 있도록 한다.

5.3 구조 설계

1) 도메인구조

정보보호시스템의 시험/평가는 대외비 자료라 할 수 있으므로 평가자 이외에는 기밀로 처리해야 한다. 따라서, 평가관리시스템 자체에도 보안기능이 요구된다. 평가관리시스템구조는 웹기반 및 인트라넷기반(클라이언트-서버)이며 보안기능이 강화된 OS, DBMS, 웹서버, 암호라이브러리(공개된 Java암호라이브러리(예:DSTC의 JCSI)를 이용한다. 평가관리시스템의 구조는 그림 6과 같다.



※(주) 각 서브시스템간에는 보안서비스를 제공함(인증, 기밀, 무결성, 부인봉쇄)

그림 6. 평가관리시스템(EMS)의 도메인 구조

2) 물리적 구조

그림 7은 본 논문에서 제안하는 정보보호시스템 EMS의 물리적 구조이다. 평가 신청인에 의해서 평가 신청이 접수되면(WEB), 평가 프로젝트가 시작되고, 정보보호시스템(TOE)에 대한 평가가 이루어진다. 평가결과 및 평가기준은 평가서버에서 모든 처리가 이루어지며, 정량적인 평가결과를 제공한다.

3) 서버 · 클라이언트 구조

평가시스템의 서버 · 클라이언트 또한 암호라이브러리(공개된 Java암호라이브러리)를 이용하였다. 평가 서버 구조는 크게 워크플로우 관리시스템과 데이터베이스로 나누며 구조는 그림 8과 같다. 데이터베이스는 평가워크플로우의 내용과 평가프로세스의 상태를 포함하는 "워크플로우 DB"와 평가환경에 관한 데이터를 포함한다. 평가 클라이언트 구조는 평가/승인자 인터페이스(평가대상물 및 평가환경)와 워크플로우 클라이언트, 파일시스템, 서버와의 통신을 위한 플랫폼으로 구성되어 있으며 평가시와 승인시에 사용된다.

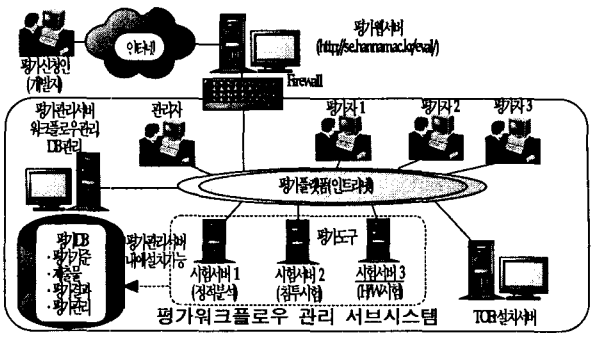


그림 7. 평가관리시스템(EMS)의 물리적구조

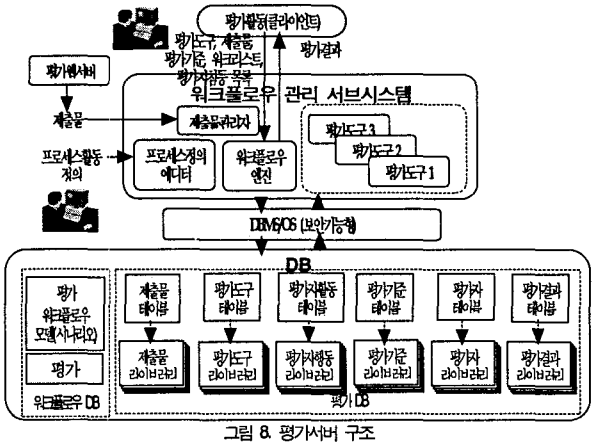


그림 8. 평가서버 구조

6. 결론

본 논문에서는 먼저, 평가 및 인증의 중요성과 정보보호시스템의 신뢰성 확보의 필요성을 문제제기하였으며 평가관리시스템을 위한 평가체계 및 절차에 대해 간략하게 보였다. 그리고 평가를 위한 평가환경의 구축, 즉 평가관리시스템(EMS)의 요구사항에 대하여 알아본 후 CC를 기반으로 본 시스템에서 활용될 평가모델과 평가 워크플로우 모델에 대해서 정의하였다. 마지막으로, 정보보호시스템 EMS에 대한 평가기반 기술과 개발환경 및 구조 등의 설계사항에 대하여 제시하였다. 본 논문에서 제안하는 EMS는 평가기술을 확보하여 외국에만 의존해야 하는 평가업무의 시간과 비용을 줄일 수 있으며 정보시스템의 평가 및 인증을 통하여 최적의 보안성과 시장성을 높일 수 있다. 또한 CC의 도입은 거를 수 없는 대세로 자리잡고 있으며 국내에서도 CC도입을 위해 인증기관, 평가기관 차원 뿐만 아니라 개발자 입장에서도 만반의 준비를 하고 있다. 그러므로 본 시스템은 CC기반의 정보보호시스템 평가기관에서의 평가관리시스템으로 활용할 수 있으며 향후과제로는 제안된 구조를 바탕으로 보다 효율적이고 보안 강화된 평가관리시스템의 개발 및 구현이다.

참고 문헌

[1] CCEB, "Common Criteria for Information Technology Security Evaluation(CC)," Version 2.1, CCIMB-99-033, http://csrc.ncsl.gov, August 1999. (정보보호시스템 공통평가기준, 정보통신부, 2002.8과 내용 동일)
[2] 김광식, 남택용, 정보보호시스템 공통평가기준 기술동향 http://kidbs.itfind.or.kr, 2002.10
[3] 한국정보보호진흥원, "정보보호 시스템 평가방법론," 수탁기관: 한남대학교, 1996.12
[4] CCEB, "Common Evaluation Methodology for Information Technology Security". Part 1(CEM-97/07), Part2(Version 1.0, CEM-99/045), http://csrc.ncsl.gov.
[5] Information Technology Security Evaluation Manual (ITSEM), Commission of European Communities, http://www.cesg.uk, 1998.
[6] 한국정보보호진흥원, "정보보호시스템 평가·인증 가이드, 한국정보보호진흥원, 2002.12.
[7] 한국정보보호진흥원, "국제공통평가기준 기반의 평가제출물 작성법 연구", 수탁기관: 한남대학교, 2001.10.
[8] S. Shrivastava and S.Wheater (ed.), "Special Issue of Workflow Management Systems," *IEEE Concurrency*, July-Sep. 1999.
[9] P.Lawrence(ed.), *Work flow Handbook*, Wiley & Sons, 1997.