공통평가기준을 기반으로 한 보안평가관리 시스템의 개발

Development of Security Evaluation Management System Based on Common Criteria

강연희(Yeon-Hee Kang)*, 방영환(Young-Hwan Bang)*, 이강수(Gang-Soo Lee)**

초 록

CC(공통평가기준 : Common Criteria, ISO/IEC 15408)는 국가간에 서로 다른 평가기준을 적용하여 평가함으로써 발생되는 문제점을 해결하기 위해 1999년 6월에 발표되었으며, 현재 공식버전은 v2.2이며 드래프트 버전으로 v3.0이 나와 있다. 국내외적으로 CC기반의 평가 수요가 증가되고 있으며 이에 따라 평가시장 창출이 예상되고 실제 평가지침 및 평가활동의 자동화, 평가프로젝트의 관리가 필요하다. 본 논문에서는 평가자원(예: 제출물, 평가기준, 평가자 등)을 관리하고 평가환경에서 효율적으로 이용 가능한 CC 기반 보안평가관리시스템(CC-SEMS : CC based Security Evaluation Management System)을 제시하였다. CC-SEMS는 프로젝트관리, 워크플로우관리, 프로세스관리의 어플리케이션을 통합한 것이며 제출물, 평가업무 프로그램, 관리 객체, 평가워크플로우 엔진으로 구성되어 있다.

ABSTRACT

Common Criteria(CC) was announced in June, 1999 in order to solve a problem which be happened by applying a different evaluation criteria among nations. Currently, a official version is v2.2 and v3.0 is a draft version. Because an evaluation demand is increased in the inside and outside of the country, an evaluation market growth is expected. Also, It needs methodology and work automation and project management for evaluation. In this paper, we propose A CC based Security Evaluation Management System(CC-SEMS) that is managing evaluation resources(deliverables, evaluation criteria, evaluators) and is useful in evaluation environment efficiently. CC-SEMS is to have integrated project management, workflow management, process management and is composed of deliverables, Evaluation Activity Program(EAP), Management Object(MO), Evaluation Database(EDB), Evaluation Workflow Engine(EWE).

키워드 : 공통평가기준, 공통평가방법론, 평가, 평가 관리

Common Criteria, Common Evaluation Methodology, Evaluation, Evaluation Management

---

본 연구는 산업자원부 지역협력연구사업(과제번호: R12-2003-004-01001-0) 지원으로 수행되었음.

* 한남대학교 대학원 컴퓨터공학과

** 한남대학교 정보통신·멀티미디어공학부 교수

1. 서 론

1980년대 중반 이후로 다양한 유형의 정보보호 제품 및 시스템이 다양한 평가 기준(예를 들면, TCSEC, ITSEC/ITSEM, CTCPEC, CC/ CEM)하에 개발 및 평가, 보증되어 왔으며, CC(공통평가기준 : Common Criteria)는 서로 다른 평가기준을 적용하여 평가함으로써 발생되는 이중의 비용소모와 시간소모의 문제점을 해결하기 위해 1999년 6월에 ISO/IEC 15408로 발표되었다[1]. 현재 CC의 평가 공식 버전은 v2.2이며 드래프트 버전으로 v3.0이 발표되었으며 향후 공식버전이 될 수 있다. ITSEM과 CEM은 평가에 관한 총체적인 지침서로서, 평가기관에서는 이를 참조해야 한다. ITSEM은 ITSEC에 대한 높은 수준의 평가지침서이며, CEM은 CC에 대한 평가지침서이다. 그러나 ITSEM은 오직 한 개의 "평가업무 프로그램(EAP)"만을 보유하고 있으며, 본 논문에서 제시하는 CC-SEMS에서는 CC의 보증요구사항(컴포넌트)에서 7단계로 정의한 평가보증등급(EAL)에 대한 7개의 EAP를 필요로 한다[2,3]. 현재 CC는 CEM과 더불어 적절하고 비용 효과적인 평가를 수행할 수 있는 골격을 제시하고 있으며 유럽과 호주/뉴질랜드만이 ITSEC와 CC를 병행하여 평가에 사용하고 미국, 캐나다 등은 CC만을 사용하고 있다. CC를 기반으로 CEM은 평가자행동에 대한 상세한 지침서로서 v2.2까지는 EAL1에서 EAL4등급까지에 대한 지침만 존재하며 v3.0(드래프트 버전)은 이를 보완하여 EAL1에서 EAL7등급까지 정의하였다. 우리나라는 2004년에 CC 상호인정협정(CCRA)에 가입을 신청하였고 이미 KISA와 국가정보원에서는 CC를 이용한 평가 및 인증이 이루어지고 있다. 이러한 CC와 CEM을 기준으로 계속적인 평가 수요 증가되고 있으며 평가시장 창출이 예상되고 있다. 또한, 평가프로젝트에 대한 실제 평가지침 및 평가활동의 자동화, 평가프로젝트의 관리가 필요하다.

평가기관은 평가자원(예: 제출물, 평가기준, 평가자, 평가도구 등)을 동시에 관리하는 목적으로 그들의 평가 환경에서 효과적인 CC기반 보안 평가 관리 시스템(CC-SEMS : CC based Security Evaluation Management System)을 운용할 수 있다. CC-SEMS는 프로젝트 관리, 워크플로우 관리, 프로세스 관리의 어플리케이션을 통합한 것이며 본 논문에서는 UML을 이용하여 모델링하였다[4~6]. 본 논문의 2장에서는 CC기반 UML 모델링을 위한 관련 사항을 조사(연구)하였으며, 3장에서는 CC-SEMS의 전체 구조를 바탕으로 각각의 구성요소에 대하여 정의하였다. 또한, 4장에서는 CC-SEMS에 대한 UML 모델링 설계 및 구현 결과를 보였으며 마지막으로 5장에서 평가 및 결론을 맺는다.

2. 관련연구

2.1 기존 프로젝트 관리

본 논문에서 제시하고 하는 도구는 크게 프로젝트 관리와 유사하며 이와 유사한 시스템으로는 MS-Project(Microsoft Office Project)

및 KickStart, ProChain이 존재한다[7~9].

- MS-Project : Microsoft 핵심 프로젝트 관리 프로그램으로서 현재 2003이 개발되어 있다. MS-Project 2003은 유동적이므로 프로젝트를 개별적으로 관리하든 팀, 부서 또는 조직 전체의 포트폴리오로 관리하든 관계없이 작업 및 작업자 관리 요구 사항을 충족한다. 또한, MS-Project는 가시적인 프로젝트 관리에 중점을 두었으며, 프로젝트 계획, 자원 할당, 보고서 작성 등의 기능을 보유한다. 스케줄링 충돌을 예상 가능하며, 적당한 자원의 사용, 프로젝트의 선행 및 의존관계 보증, 제출 날짜 결정, 임계 경로 및 병목 현상 확인, 팀 멤버간의 커뮤니케이션이 가능하다는 장점이 존재하며, 자원 및 작업을 수동적으로 생성함으로써 여러 유형의 프로젝트 관리에 적용가능하다. 그러나 프로젝트의 업무 확인, 업무 의존성의 확립, 수행자의 기술 평가, 업무 시간의 배제 및 제거 등이 결여된 단점이 있다.

  프로젝트는 매우 상세한 업무를 수반하며, 수행자의 프로젝트 수행 기간 및 자원의 재할당 등에 대한 수정은 빈번히 일어나므로 MS-Project에서는 특정 프로젝트의 계획면에서는 간트차트 및 보고서 등의 출력물에 의해 뛰어난 프로젝트 관리 특징을 가지지만 이외의 프로젝트 수행 및 제어 등에 대한 프로세스에는 적합하지 못하다.
- Project KickStart : 어떤 크기의 프로젝트의 관리에도 가능하며, 드래그&드롭 기능 및 간트차트, Microsoft 도구와의 연결, 초보자의 사용에 유리한 특징을 가지고 있다. 또한, 샘플 프로젝트를 제공하여 프로젝트를 계획하는데 좀 더 용이하게 한다. KickStart의 8 단계 계획 아이콘은 프로젝트 성공을 위한 목표, 자원, 장해물과 임계 경로상의 다른 전략적 이슈 등의 프로젝트 구조이며, 부분적으로 잊을 수 있는 사항에 대해 계획할 수 있도록 보증한다.
- ProChain Project Management : 프로젝트 관리 기법 중 CCPM의 기능을 이용하여 개발한 도구이며, 개인 프로젝트의 critical chain 스케줄링을 지원하는 ProChain Project Scheduling과 다중 프로젝트를 제공하는 ProChain Pipeline, 조직에 대한 어플리케이션을 문서화 하고 수정하는 기능을 가진 ProChain Enterprise 등 세 가지가 존재한다.

  KickStart와 ProChain등은 모두 MS-Project에 기반을 두어 생성되었으며 MS-Project와 통합 가능하고 이외에도 Interneer, AceProject 등과 같은 많은 상용 제품들이 존재한다.

본 논문의 CC-SEMS는 평가 워크플로우 엔진을 이용하여 CC기반의 평가프로젝트를 수행하는데 평가노력을 절감할 수 있도록 설계 및 개발하였으며 MS-Project, KicjStart 및 ProChain 등과 같은 프로젝트 관리 도구보다 좀더 자동화되어 업무를 수행한다.

2.2 워크플로우 모델링 언어 비교

〈표 1〉은 워크플로우 모델링 언어에 대한 평가의 요약을 나타내며, "+" 표시는 표준으로서 충족되고, "-" 표시는 그렇지 않음을 의미한다. "?" 표시는 공식적인지와 표준이 아닌지를 구별하기 불가능함을 의미한다. 표에서 보듯이 WfMC와 EPC 공식성은 대부분의 기준에서 미달됨을 볼 수 있으며 ANSI는 부분적인 호출 어플리케이션에서 표현되지 않을 뿐만 아니라 제한적이다. 페트리 넷과 UML은 비즈니스 프로세스 모델링에서 정형성과 효과적인 도해(그림) 사이의 전형적인 언어로서 남아 있으며 계속적인 논쟁으로 부각되어 오고 있다[10]. 비록 UML 프로세스가 페트리 넷보다 기초에서 덜 정형화되었을지라도, UML은 효율적인 모델의 본질인 워크플로우 범위를 표현한다. 페트리 넷은 기본적으로 활동을 자동화여 사용하는 IT 자원의 표현을 허락하지 않으므로 너무 제한적이다.

2.3 페트리 넷과 활동 다이어그램 변화 비교

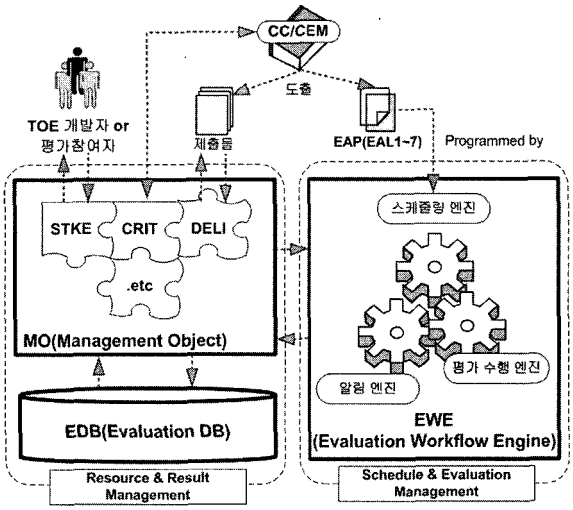
페트리 넷은 워크플로우 모델링 기술로서 광범위하게 사용되어져 왔으며, 최근에는 아직까지 구문과 의미가 충분히 사용되지는 않지만 같은 목적으로 사용되고 있는 UML 활동 다이어그램이 있다. 페트리 넷은 비반동적이며 폐쇄적인 활동시스템의 자원 사용을 모델화하는데 반하여 UML 활동 다이어그램은 반동적이며 개방적인 시스템을 모델화한다. 그러나 페트리 넷은 구문과 의미를 확장하지 않는 한 반응성에 대한 일의흐름을 정확히 모델화하기 어렵다[11].

2.3 활동 다이어그램의 진화

UML1.x도 활동 다이어그램을 가지고 있지만, UML 2.0은 활동 다이어그램을 새로운 수준으로 끌어올렸다. 이전의 활동 다이어그램은 특별한 종류의 상태 다이어그램이었다. 활동 다이어그램은 하나의 오퍼레이션에서 다

〈표 1〉 워크플로우 모델링 언어 비교

	Formal Basis	Executability	Visulization	Distinct Organizations	Document Exchange	W3
Petri Nets	+	+	+	+	+	-
WfMC	-	-	+	-	-	+
UML	?	+	+	+	+	+
ANSI	-	+	+	+	+	-
EPC	-	-	+	-	-	-



〈그림 1〉 CC-SEMS의 전체 구조

른 하나로의 control across classes의 흐름을 보여줄 수 있었으나 보여줄 수 있는 흐름의 종류가 제한되었다. UML 2.0은 페트리 넷과 같은 활동을 하는 활동 다이어그램을 제공한다. "토큰"으로 알려진 객체들은 노드에서 노드로 움직일 수 있으며 활동(activities)과 행동(actions)은 "토큰"을 소비 및 생산한다. 그러므로 "토큰"을 차례로 돌리는 순수한 흐름 다이어그램을 만들 수 있으며 "워크플로우 활동 다이어그램"을 작성할 수 있다[12].

3. CC-SEMS 구성 요소

〈그림 1〉은 본 논문에서 최종적으로 개발하고자 하는CC-SEMS의 전체 구조를 나타내며 자원 및 결과 관리 부분과 스케줄 및 평가 관리 부분으로 나뉜다. 본 장에서는 평가 플랫폼에 적용되는 요구사항에 대하여 제시하도록 한다. 또한, "평가업무 프로그램"과 "평가워크플로우 엔진"을 정의하도록 한다. 본 절의 내용은 민간평가기관에서 평가수행을 위한 시스템을 구축할 때 분석 및 설계자료로 직접 활용 할 수 있다.

3.1 제출물(Deliverables)

평가에 필요한 제출물은 "제출물 생성 알고리즘"을 사용하여 평가보증등급(EAL)별 제출물의 목록과 내용을 유도하였다. 알고리즘은 두 가지 단계로 구성된다[16].

[단계 1] 최소한의 내용 도출: CC 보증요구사항의 각 컴포넌트에 정의된 "평가자행동" 및 "근거요구사항"(즉, 개발자의 자체평가 업무 및 평가자에게 제출해야할 전달물 내용과 수준을 명시한 문장)을 고려하여 제출물의 구조와 내용으로 유도한다. CC 보증 요

구사항내의 각 클래스, 패밀리 및 컴포넌트는 각각 제출물의 제목, 장 그리고 제출물의 절로 매핑된다.

[단계 2] 최소한의 내용 정교화: 만일 1개의 보증 클래스당 1개의 문서가 유도된다면, 13개의 문서가 필요하며 최대 91(13×7) 유형의 문서가 필요하다. 이는 중복되며 너무 짧거나 긴 문서들이므로 제출물의 양을 최소화할 뿐만 아니라 문서 사이의 일치성을 보증해야 한다. 많은 중복된 문서와 문서 사이에 일치성이 적은 문서가 존재할 수 있다. 그러므로 다음과 같은 규칙을 사용하여 중복성을 제거할 수 있다.

- CC 기반 적합성 규칙(CC conformance rule): 명시된 문서는 CC에 명시된 보증 엘리먼트의 최소 내용과 표현을 포함한다.
- 부분집합 규칙(Subset rule): 상위 EAL 문서는 하위 EAL의 내용을 포함한다.
- 병합 규칙(Merge Rule): 너무 적거나 중복되는 보증 클래스에 대한 두 개 또는 더 많은 문서를 하나의 문서로 병합해야 한다.
- 최소화 규칙(Minimal Rule): 내용이 같은 보증 클래스에 대한 두 개 또는 더 많은 문서를 하나의 문서로 병합해야 한다.

위와 같은 규칙을 사용함으로써, 51개의 문서로 줄일 수 있으며 〈표 2〉에서 그 결과를 보인다. 이러한 접근은 FAA의 자료 항목 설명(Data Item Description)보다 유용하며 실용적이다[13].

3.2 평가업무 프로그램(EAP)

평가에 필요한 평가의 흐름을 정의해 주는 프로그램을 "평가업무 프로그램(EAP :

〈표 2〉 제출물 목록

Deliverables(documents)	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7	Corresponding assurance class-family
Security target report (STR)	STR.1							ASE
Configuration management Report (CMR)	CMR.1	CMR.2	CMR.3	CMR.4	CMR.5	CMR.6		ACM
Delivery and operation report (DOR)	DOR.1	DOR.2		DOR.3			DOR.4	ADO
Functional Specification (FSR)	FSR.1			FSR.2	FSR.3		FSR.4	ADV_FSP, ADV_RCR
High-level design specification (HDR)		HDR.1	HDR.2		HDR.3	HDR.4	HDR.5	ADV_HLD, ADV_RCR
Implementation report (IMR)				IMR.1	IMR.2	IMR.3	IMR.4	ADV_IMP, ADV_RCR
Structural specification (INR)					INR.1	INR.2	INR.3	ADV_INT, ADV_RCR
Low-level design specification (LDR)				LDR.1	LDR.2	LDR.3	LDR.4	ADV_LLD, ADV_RCR
Security policy sped (SPR)				SPR.1	SPR.2		SPR.3	ADV_SPM
Guidance document (GDR)	GDR.1							AGD
Lifecycle support report (ALR)			ALR.1	ALR.2	ALR.3	ALR.4	ALR.5	ALC
Test report (TSR)	TSR.1	TSR.2	TSR.3		TSR.4	TSR.5	TSR.6	ATE
Vulnerability analysis report (VAR)		VAR.1	VAR.2	VAR.3	VAR.4	VAR.5		AVA

Evaluation Activity Program)"이라 하며, 이는 CC에서의 보증요구사항 등급에 따라 다르게 구성된다. 그러나, 보증요구사항 등급별 컴포넌트 자체만으로는 불충분하여 다른 컴포넌트에 의존해야만 하는 경우가 발생하며 이를 "종속성(dependency)"이라 한다. 평가프로젝트에서 보증 클래스, 컴포넌트, 평가자 행동과 개발자 행동과 내용 & 증거의 표현이 각각 활동, 부활동, 행동과 업무 단위에 대응하며 위와 같은 규칙을 따른다[5].

컴포넌트들간의 전체관계는 스테이지별로 출력되며 선행순서를 갖지만 각각의 컴포넌트들은 독립성을 유지한다. 따라서, 각각의 스테이지 내의 컴포넌트들은 동시에 평가할 수 있는 이점을 가지며 스테이지 개념은 대학교에서의 커리큘럼 상의 학기 개념과 같다. 출력된 전체관계는 UML의 활동도 형태가 되며 평가기간을 단축하기 위한 임계경로(critical path)를 식별하여 경로내에 평가인원과 도구를 집중함으로써, 평가 완료시간을 단축할 수 있다[14].

- **환원** : 만약 한 컴포넌트(즉, 요구사항) C_i가 그 목적을 만족하는지의 여부가 다른 컴포넌트(즉, 요구사항) C_j가 정상적으로 만족되는지에 의존(종속)되는 컴포넌트들 간의 관계로 정의하며 다음과 같이 기호화한다.
  $C_i \rightarrow C_j$(여기서,$C_i C_j \in ENT, \rightarrow$:dependency)
- **확장**
  - 패밀리간 종속성 : 한 패밀리 Fi내의 모든 컴포넌트 C_k가 다른 패밀리 F_j내의 컴포넌트 C_m과 종속적이면, 두 패밀리 F_i 및 F_j는 종속적이다.
    For $\forall F_k \in C_i$ and $\exists F_m \in C_j$, if$(C_i \rightarrow C_j)$then$(F_i \rightarrow F_m)$
  - 클래스간 종속성 : 한 클래스 CLi내의 모든 패밀리 F_k가 다른 클래스 CL_j내의 패밀리 F_m과 종속적이면, 두 클래스 CL_i 및 CL_j는 종속적이다.
    For $\forall F_k \in CL_i$ and $\exists F_m \in CL_j$, if$(F_i \rightarrow F_m)$ then $(CL_i \rightarrow CL_j)$
- **추이성(이행적)** : 한 컴포넌트 Ci가 다른 컴포넌트 C_j와 종속적이고 C_j가 또 다른 컴포넌트 C_k와 종속적이면 C_i는 C_k와 종속관계로 정의될 수 있다.
  if$(C_i \rightarrow C_j) \wedge (C_j \rightarrow C_k)$then$(C_i \rightarrow C_k)$

3.3 관리 객체 (MO : Management Object)

관리 객체는 관리의 자원 또는 대상이며 다음과 같이 정의할 수 있다.

MO = (STKE, DELI, CRIT, ETC)

- **STKE** (stakeholder) : TOE, 평가 참여자와 평가 사용자 등을 말하며 STKE의 서브 타입으로서 "TOE Producer"는 신청자, 개발자이며 "컨설턴트 평가참여자"는 평가책임자, 평가자, 감독자이다. 주의할 점은 감독자는 인증/감독보고서를 발행해야 하며 CC 평가자는 평가기관의 평가자로서 평가 및 승인 업무를 수행하여야 한다.
- **DELI** (Deliverables) : DELI의 서브타입은 입력물(예:TOE 관련문서), 평가 관련된 모든문서, 출력물(예:결과문서) 등을 말한다.
- **CRIT** (criteria) : 평가기준(예:CC 또는 PP, ST)을 말한다. PP와 ST, 또는 다른 CMVP와 같은 다른 평가기준이 될

수 있다.

- **ETC** (etc) : 평가도구 및 평가기간 (예:10개월), 평가비용 등이 있다.

3.4 평가 워크플로우 엔진

분석된 "MO(관리 객체)"와 "EAP(평가업무 프로그램)"을 이용하여 실제 평가관리 도구를 구축하기 위해서는 "평가워크플로우 엔진(EWE : Evaluation Workflow Engine)"이 요구된다. "평가 워크플로우 엔진"이란 평가업무에 대한 워크플로우 프로세스를 추적하고 각 워크플로우 단계의 수행을 조정하며 클라이언트 즉, 사용자와 워크플로우 절차를 주고받는 평가관리시스템에서 가장 중요한 역할을 수행한다. 또한, MO는 평가워크플로우 엔진 또는 관리자에 의한 프로젝트 계획에 따라 제어된다. 제어란 비용, 개발자, 평가 도구와 같은 MO의 할당, 처리 및 승인 등을 의미한다. 평가워크플로우 엔진은 스케줄링 엔진, 평가 수행 엔진, 알림 엔진의 서브 워크플로우 엔진을 포함하며 CC의 평가보증등급(EAL)에 따라 평가업무에 대한 워크플로우 프로세스를 추적하고 각 워크플로우 단계의 수행을 조정하며 클라이언트 즉, 사용자와 워크플로우 절차를 상호작용하는 것을 특징으로 한다. CC-SEMS 워크플로우 엔진의 구조는 워크플로우 엔진 상호 연동 시나리오 (연결 프로세스, 서브 프로세스, 병렬 동기화)의 규칙을 따르며 자세한 사항은 다음 장에서 상세하게 다룬다.

4. CC-SEMS의 UML 모델링

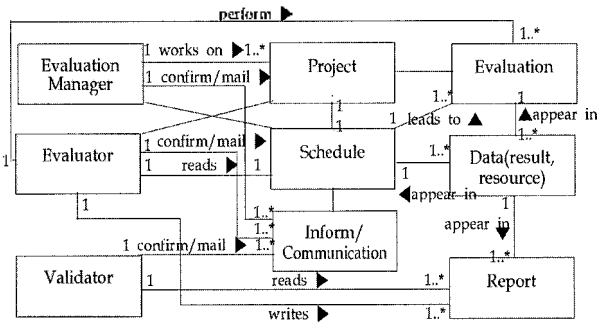
객체지향적 분석·설계 방법을 채택하여, 시나리오를 토대로 워크플로우를 설정하고 분석한 후, 이를 지원하는 CC-SEMS를 추가적으로 분석·설계하였다. 분석 및 설계 단계에서 나온 UML은 준정형 모델링기술로서, 클래스 다이어그램(class diagram), 유스케이스 다이어그램(use-case diagram), 활동 다이어그램(activity diagram), 상태 다이어그램(statechart diagram) 등을 기초로 프로토타입을 구현하였다.

4.1 CC-SEMS의 도메인 모델

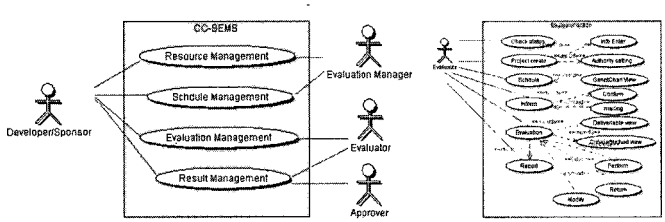
<그림 2>는 CC-SEMS의 도메인에서 개념적 클래스와 실세계 객체들을 가시적으로 표현한 도메인 모델이며, 각각의 관계를 표현하였다. 예를 들어, 평가책임자는 스케줄링을 작성하며 이를 해당 평가 참여자에게 알리고 해당 참여자(평가자)는 평가수행 및 보고서를 작성한다.

4.2 전체 관리 및 평가 수행 관계

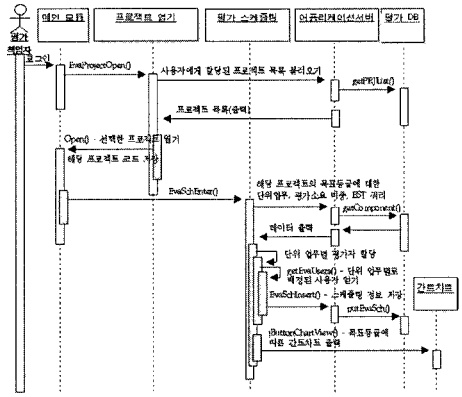
<그림 3>은 CC-SEMS의 전체적인 관리 및 평가자와 평가 수행 관계를 유스케이스 다이어그램을 이용하여 모델링한 것이며 이를 통하여 관리자 및 평가자와 개발자의 상호 의사소통을 원활하게 하고 개발업무를 쉽게 파악할 수 있도록 한다. CC-SEMS는 자원관리(평가참여자, 평가도구, 제출물 등), 스케줄 관리, 평가 관리(평가수행 및 인증), 결과 관리(OR



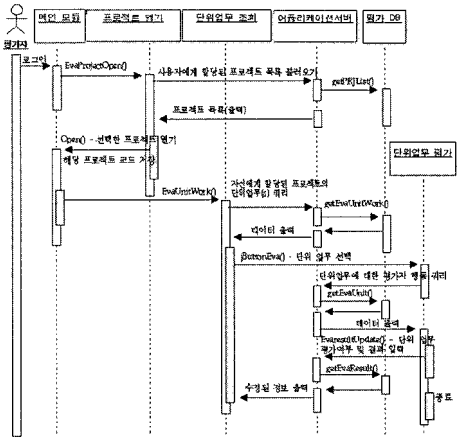
〈그림 2〉 CC-SEMS의 도메인 모델



〈그림 3〉 CC-SEMS의 관리 및 평가 수행 관계 모델링



〈그림 4〉 스케줄링 시퀀스 다이어그램

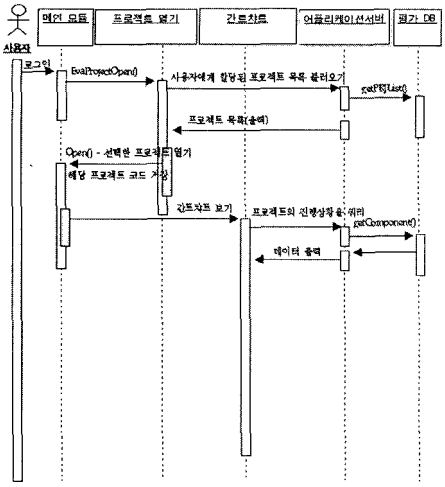


〈그림 5〉 단위업무 조회 및 평가 시퀀스 다이어그램

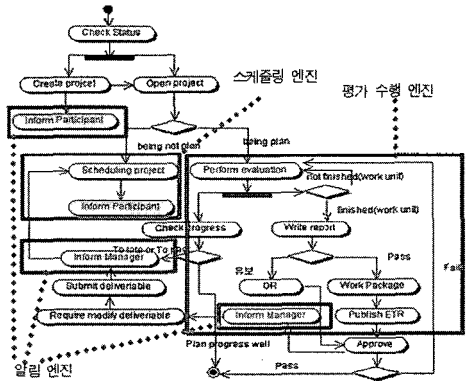
및 ETR)의 4부분으로 나뉠 수 있다.

4.3 시퀀스 다이어그램 모델링

〈그림 4〉~〈그림 6〉은 각각 스케줄링, 단위 업무 조회 및 평가, 간트차트 보기의 시퀀스



〈그림 6〉 간트챠트 보기 시퀀스 다이어그램



〈그림 7〉 CC-SEMS 평가 프로세스 워크플로우 모델링

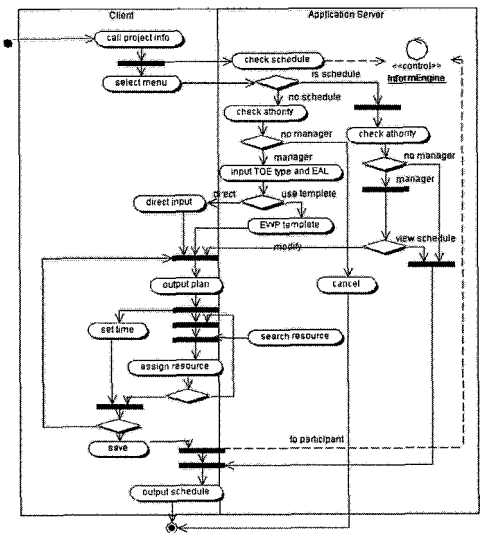
도 모델링을 나타내며 이외의 것은 본 논문에서는 생략한다.

4.4 평가 프로세스 및 워크플로우 엔진

〈그림 7〉은 CC-SEMS 평가 프로세스를 워크플로우로 모델링한 것이며 평가워크플로우 엔진은 스케줄링, 알림, 평가수행 엔진으로 구분된다.

스케 줄링 엔진에서는 병렬 동기화, 즉 동시에 특정 액티바티가 시작되는 경우로서 2개의 독립된 워크플로우 시스템에 있는 프로세스 실행시점 중 일부가 동기화 된다. 스케줄링 엔진은 평가프로젝트를 수행하기 위해 목표 평가보증등급에 따른 "EAP"를 이용하여 해당업무의 실행순서를 판별하여 자동적으로 스케줄링하며 부가적인 작업일 및 자원할당 등의 역할을 한다. 〈그림 8〉은 CC-SEMS의 스케줄링 엔진을 활동 다이어그램으로 모델링한 것이다.

스케줄링시 평가프로젝트 수요 증가 및 평가자 부족의 문제점이 발생하며 짧은 시간 내

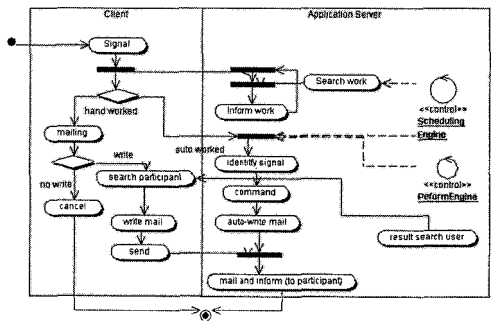


〈그림 8〉 CC-SEMS 스케줄링 수행 엔진 활동 다이어그램

```
[평가스케줄링 알고리즘]
Algorithm EvaScheduling()
/* 평가업무프로그램(EWP)의 등급별 평가
업무 Ew를 입력

int AllocateWork(Ew, n) // 욕심쟁이 알고리
즘
/* 입력된 Ew[0..n-1][0..1], 여기에서
Ew[i][0], Ew[i][1]은 각각 단위업무 i의
시작시간, 마감시간임.
    출력 : 평가업무 스케줄링 결과
    Ew를 시작시간 순서로 정렬 */
int i, j, Evaper, NewEvaper = 0;
for (i=0; i<n; i++) {
    j = i + 1;
  if (Ewu[i][1] ≤ Ew[j][0] || Ew[j][1] ≤
Ew[i][0] ) {
//단위업무 i와 일정이 겹치지 않는 평가자
Evaper가 존재한다.
     Evaper = Ewi ; // 단위업무 i를 평
가자 Evaper에 할당 }
  else {
   NewEvaper = NewEvaper + 1;
    NewEvaper = Ewi ; //단위업무 i를
NewEvaper에 할당 }
  } returen NewEvaper; }
```

에 적은 인력으로 많은 평가프로젝트를 수행하는 등 효율적인 면을 고려하여야 한다. 효율성을 높이기 위한 방법에는 두 가지 측면으로 고려할 수 있다.



〈그림 9〉 CC-SEMS 알림 엔진 활동 다이어그램

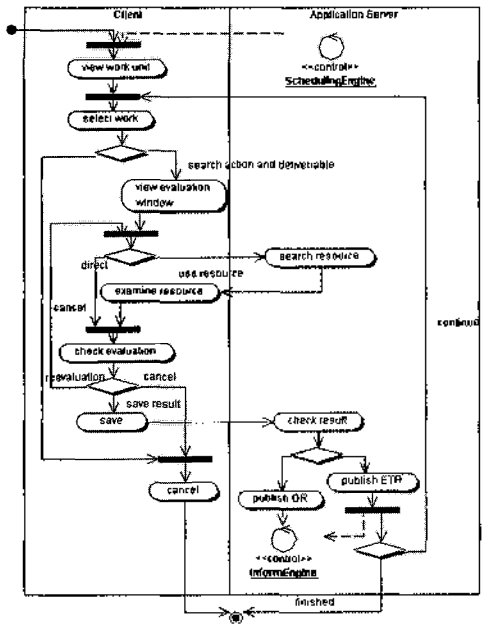
- **Time 중점** : 적은 평가인력을 이용하여 최대한 각각의 평가프로젝트의 배정. 빠른 시간 안에 평가프로젝트를 수행할 수 있음.
- **Project 중점** : 적정 평가업무만을 할당. 보안성을 높이고 평가인력의 배정에 쉬운 방법.

이 두 가지 측면은 서로 반비례하며 모두 충족시키기 어려우며 최대한 고려하여 스케줄링을 해야 한다. 그러므로 스케줄링 엔진에서는 "평가스케줄링 알고리즘"을 최소의 평가자가 중복되지 않은 평가업무를 수행할 수 있도록 단위업무를 할당하기 위해 욕심쟁이 알고리즘 방법을 응용하여 적용하였다. 적용하였으며 알고리즘은 다음과 같은 순서를 따른다.

[단계 1] "EAP" 적용 : 등급별 평가업무 Ew(n개의 단위업무로 이루어져 있음)를 얻음.

[단계 2] 자원 할당 : 각 단위업무 i에는 (Si, Ei)가 지정됨 (Si : 시작시간, Ei : 마감시간).

알림 엔진은 "서브 프로세스(특정 워크플로우 시스템의 프로세스가 다른 워크플로우 시스템 프로세스의 일부분으로 수행되는 경우)"로서, 스케줄링 엔진과 평가 수행 엔진에서 발생하는 알림업무를 프로세스의 일부분으로 수행하는 역할을 한다. 〈그림 9〉는 알림 엔진을 활동 다이어그램으로 모델링한 것이며 반복적인 활동을 한다. 알림 엔진이 시작되면 자동적인 부분과 수동적인 부분의 대안



〈그림 10〉 CC-SEMS 수행 엔진 활동 다이어그램

[평결(Verdict) 알고리즘]

Algorithm Verdict()
For 주어진 평가 유형내의 모든 activity :
For 주어진 activity내의 sub-activity :
For 주어진 sub-activity내의 모든 action :
① 정의되어 있다면, 내용 및 표현 증거를 식별
For 주어진 평가 행동내의 모든 work unit :
② 수행지시에 따라 요구사항을 평가
Emit verdict (pass, fail, or inconclusive)
If any work unit = "fail", action = "fail"
If any action = "fail", sub-activity = "fail"
③ write 관찰보고서(Observation Report)
else if action = "pass",
④ write 평가기술보고서(Evaluation Technical Report)
If any sub-activity = "fail", write 관찰보고서(OR)
else if sub-activity = "pass", ⑤ write 평가기술보고서(ETR)
If any work unit = "inconclusive", evaluation result = "inconclusive"

워크플로우가 존재하므로 활동이 분기된다.

수행 엔진은 나머지 두 개의 엔진과 연결되며 연결 프로세스의 시나리오를 따른다. 수행 엔진은 스케줄링 엔진에서 설계된 "EAP"에 의해 평가자에게 할당된 업무를 수행하는 역할을 하며 평가업무가 완료된 후에는 알림 엔진에 진행 중인 프로세스를 넘겨준다. 〈그림 10〉은 평가 수행 엔진을 활동 다이어그램으로 모델링한 것이며 참여자(평가자, 감독자)의 역할에 따라 각각의 업무를 흐름에 맞추어 수행할 수 있도록 제어하는 역할을 한다. 또한, CC기반 평가는 배타적인 구조를 가지며 평가 단위 계층구조에도 배타적인 평가구조가 적용된다. 따라서, 평가주기에 따른 범위를 정의하고 배타적인 평가구조에 따라 작성된 "평결 알고리즘"을 평가 수행 엔진에 적용하였다[15].

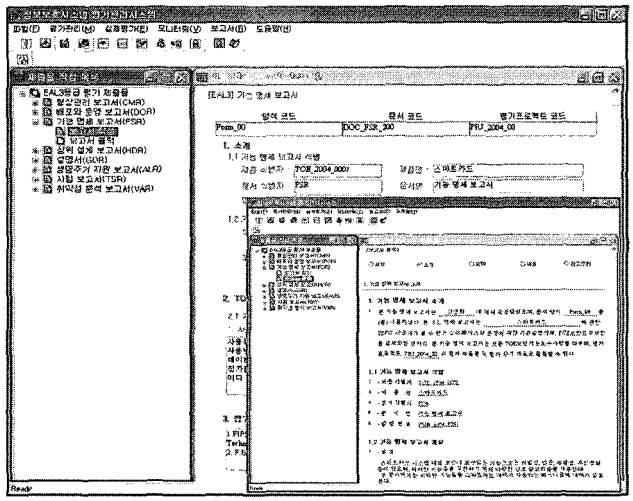
4.5 CC-SEMS 인터페이스

〈그림 11〉, 〈그림 12〉는 CC-SEMS의 개발자 제출물 작성 및 출력, 평가 화면 등의 인터페이스를 나타낸다.

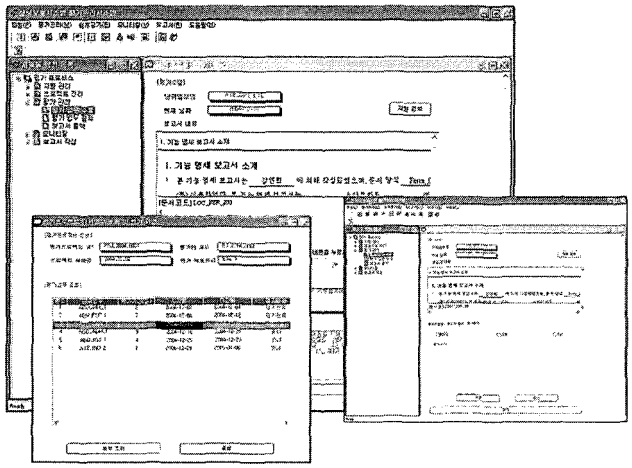
5. 평가 및 결론

5.1 기존 연구와의 비교

선진국에서는 자동화된 평가관리를 수행하는지 공개하지 않으며 우리나라는 아직 수동화된 업무에 의존하고 있다. CC-SEMS는 평



〈그림 11〉 개발자 제출물 작성 및 출력화면



〈그림 12〉 개발자 제출물 작성 및 출력화면

가제출물 관리 및 평가, 자원 관리를 수행하며 일의흐름에 맞추어 업무를 수행할 수 있도록 관리하는 워크플로우 엔진이 존재한다. 또한, 이러한 자동적인 워크플로우를 이용하여 개발자는 평가 제출물을 손쉽게 작성할 수 있으며 평가자는 일관된 문서를 이용하여 평가를 수행하며 평가 보고서 또한 자동적으로 생성할 수 있으므로 평가노력을 절감할 수 있다. 〈표 2〉와 〈표 3〉은 각각 본 시스템과 CC 기반 평가 관련 시스템, MS-Project 및 기타

〈표 2〉 CC기반 평가 관련 지원 시스템 비교[34, 35]

	범 위	특이사항
AGTER v1.0 (평가결과 자동생성도구)	- CC기반	- 평가결과 (보고서 :OR,EWP,ETR)에 중점을 둠 - KISA에서 참여
기타 (자동화된 CC평가프로세스)	- CC기반	- 연구 및 개발 중 (공개안함.) - CCTL에서 참여 - CC 평가프로세스를 자동화하는데 중점을 둠
제시한 시스템	- CC기반(향후 FIPS140-2로 확장 가능- EAP이용)	- 평가 준비 및 수행, 결과 모두를 관리하는데 중점을 둠.

〈표 3〉 프로젝트 관리면에서 시스템 비교[19, 37]

	스케줄 중복 구별	자원 할당	업무 종속성 구별	커뮤니케이션	deadline 설정	프로젝트 업무 수행 확인	특이사항
MSProject	O	O	△(선행 작업 및 종속성 보증, but 업무 종속성 확립 부족)	O	O	×	-여러 유형의 프로젝트 스케줄링 적용 가능 -자원 및 작업을 수동 생성
Project KickStart	×(수동)	O	×	×	O	×	-MSProject와 유사 -목표설정에 따른 샘플 프로젝트 제공
ProChain Project Management	×(수동)	O	△(임계사슬(critical chain)에 의한 시간 설정)	△(커뮤니케이션 없는 프로젝트 수행이 목적)	O	×	-MSProject와 유사하며 통합가능 -프로젝트의 규모에 따라 다른 소프트웨어 적용
제시한 시스템	O	O	O (종속성 관계 구별, EAP 생성)	O	O	O (간트차트 및 결제라인, 평가보고서)	-목표평가등급에 따른 EAP(평가업무프로그램)을 통한 평가업무 자동생성 -평가의 절차에 따른 워크플로우를 따름.

O : 기능 존재 △ : 기능의 일부 존재 ×: 기능 부재

시스템과의 비교사항을 나타낸다.

5.2 결론

정보보호시스템의 사용도는 증가하고 있으며 이러한 정보보호시스템의 신뢰성 확보와 상호인증을 위해 CC는 필요 불가결한 존재가 되고 있다. CC기반 평가는 국제적으로 정보보호제품 및 시스템의 평가에 관한 일원화, 효율성, 그리고 관리의 표준화를 위한 방향제시를 하고 있다. 또한, 미국과 캐나다 등 국외적으로 평가수요의 증가로 인한 민간평가기관 설립 등 평가시장을 활성화하고 있는 추세이며 우리나라도 이러한 흐름에 동참하려 노력중이다. 그러나, 우리나라는 아직 민간평가기관이 존재하지 않으며 평가기술 또한 부족하므로 이러한 흐름에 맞추어 가기 위해서는 평가기술 확보가 중요시되고 있다.

그러므로 본 논문에서는 국제공통평가기준인 CC를 기반으로 평가기관에서 활용할 수 있는 CC-SEMS를 제시하였으며 UML을 이용하여 체계적이며 개방적으로 모델링하였다. 또한, 사용자의 만족도를 향상시키며 평가업무 수행 및 개선시에 수반되는 변화의 비용 또한 감소되는 이점을 기대할 수 있다. 이러한 CC-SEMS는 향후 평가를 수행하는 평가기관에서 평가수요에 대응하여 평가업무를 효율적으로 수행 및 관리할 수 있으며 정보보호시스템의 평가 및 인증을 통하여 최적의 보안성과 시장성을 높일 수 있다.

참 고 문 헌

[1] 한국정보보호진흥원, "정보보호시스템 평가 · 인증 가이드", KISA, 2002.12.

[2] CC, Common Criteria for Information Technology Security Evaluation, Version 2.2, Jan. 2004.

[3] Common Methodology for Information Technology Security Evaluation (CEM), CCIMB-2004-01-04, Version 2.2, Jan. 2004.

[4] W. Royce, Software project management - A Unified Framework, AW, 1998.

[5] P.Lawrence (ed.), Workflow handbook - 2000, John Wiley & Sons, 2000.

[6] A.Fuggetta and A.Wolf (ed.), Software Process, John Wiley & Sons, 1996.

[7] PMI, "A Guide to the Project Management Body of Knowledge(PMBOK Guide)," 2000.

[8] Jeff Crow, "Project Management Tips," http://www.projectkickstart.com/html/tips2.htm.

[9] Robert C. Newbold, "Introduction to Critical Chain Project Management," ProChain Solutions, Inc. http://www.prochain.com/articles/CriticalChainArticle.asp, 2002.

[10] Aymeric Dussart, Benoit A.Aubert and Michel Patry,, "An Evaluation of Inter-Organizational Workflow Modeling Formaliams," CIRANO, June, 2002.

[11] H.Ehrig et al., Petri Net Technology for

Communication-Based Systems, LNCS2472, Springer, pp.321-351, 2003.

[12] Marlon Dumas and Arthur H.M.ter Hofstede,. "UML Activity Diagrams as a Workflow Specification Language," In Proc. of the UML'2001 Comference. 2001.

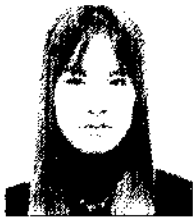
[13] Data Item Description, Federal Aviation Administration, www.faa.gov/aio/cuiefsci/PP- library/index.htm.

[14] 한국정보보호진흥원, "공통평가기준 기반 평가기간 산정 방안 및 평가수수료 정책 연구," 수탁기관 : 한남대학교, Nov. 2003.

[15] Ruben Prieto-Diaz. "The Common Criteria Evaluation Process," CISC, pp.24-33, Dec. 2002.

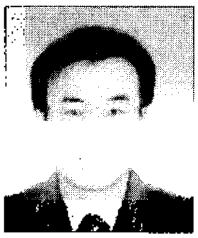
[16] Young-hwan Bang, Yeon-hee Kang, Gang-soo Lee, "CC-SEMS : A CC based Information System Evaluation Management System." PARA'04 WORKSHOP, Vol.2, pp 91~96, June 20-23, 2004.

저 자 소 개



강연희 (E-mail : dusi82@se.hannam.ac.kr)
2003. 한남대학교 컴퓨터멀티미디어공학과 졸업(학사)
2005 ~ 현재 한남대학교 컴퓨터공학과 석사 과정
관심 분야 소프트웨어공학, 정보보호시스템 평가, 보안공학, 프로젝트 관리, 시스템 모델링

방영환 (E-mail: bangyh@se.hannam.ac.kr)
1997. 한남대학교 컴퓨터공학과 졸업(학사)
2002. 대전대학교 대학원 컴퓨터공학과 졸업(석사)
2002 ~ 현재 대전보건대학 컴퓨터정보처리과 프로그래밍 전문강사
한남대학교 대학원 컴퓨터공학과 박사과정
관심 분야 소프트웨어 품질 평가 및 보증, 소프트웨어 표준화, 보안공학



이강수 (E-mail: gslee@mail.hannam.ac.kr)
1981. 홍익대학교 전자계산학과(학사)
1983. 서울대학교 대학원 전산학과(석사)
1989. 서울대학교 대학원 전산학과 박사
1985 ~ 1987. 국립한밭대학교 전자계산학과 전임강사
1992 ~ 1993. 미국일리노이대학교 객원교수
1995. 한국전자통신연구원 초빙연구원
1998 ~ 1999. 한남대학교 멀티미디어학부장
1987 ~ 현재 한남대학교 컴퓨터공학과 정교수
관심 분야 소프트웨어공학, 병행시스템 모델링 및 분석, 보안공학, 정보보호시스템 평가, 멀티미디어교육 커리큘럼