情報保護學會論文誌
第15卷 第4號, 2005. 8

# 반자동화 평가워크플로우 관리 시스템 설계 및 구현*

강 연 희,†‡ 김 정 대, 이 강 수
한남대학교

# Design and Implementation of the Semi-automated Evaluation Workflow Management System(Sa-EWMS)*

Yeon-hee Kang,†‡ Jung-dae Kim, Gang-soo Lee
Hannam University

## 요 약

정보화 역기능을 해결하기 위한 정보보호의 중요성이 높아짐에 따라 정보보호제품 및 시스템의 평가인증 수요가 증가하고 있으며 비용-효과적인 평가관리가 필요하다. 따라서, 본 논문은 평가자가 정보보호시스템에 대한 평가를 수행할 때 일련의 절차에 따라 평가업무를 수행 및 관리할 수 있는 CC(Common Criteria :공통평가기준)기반의 반자동화 평가워크플로우 관리 시스템(Sa-EWMS : Semi-automated Evaluation Workflow Management System)을 제시하였다. 본 시스템은 종래 수동적인 평가업무로 인한 시간과 노력의 소비 문제점을 해결하고 효율적인 평가수행을 위한 것으로, 각 엔진별 업무에 대한 워크플로우 프로세스를 추적하고 수행을 조정하는 역할을 하며 평가수요 및 시장창출에 대응하는 민간평가기관에서 유용하게 이용할 수 있을 것이다.

## ABSTRACT

An evaluation demand and a market growth regarding evaluation and certification are increasing because the importance of Information Security is gradually rising to solve the information disfunction. Therefore, it is necessary the cost-effect evaluation management of the Information Security System(ISS). In this paper, we propose the Semi-automated Evaluation Workflow Management System(Sa-EWMS) based on the Common Criteria(CC) which performs and manages evaluation work through the procedure when evaluator evaluates the Information Security System(ISS). The Sa-EWMS is solving a problem of consumption of time and effort and performing efficient evaluation, it is playing a significant role that traces workflow process of each work of the Engines and controls performance. It will be able to use useful the private evaluation enterprise which confront in an evaluation demand and a market growth.

**Keywords** : *Common Criteria, Evaluation, Evaluation Workflow management, Workflow System*

## Ⅰ. 서 론

정보화 역기능을 해결하기 위해서는 안전성과 신뢰성이 검증된 정보보호시스템을 사용하여 정보보호 수준을 향상시킬 수 있는 정보보호시스템 평가·인증의 필요성에 대한 관심이 고조되고 있다. 그러나 서로 다른 평가기준을 적용하여 정보보호시스템을 평가함으로써 이중의 비용소모와 시간소모의 문제점이 발생하게 되었다. 이를 해결하기 위하여 평가결과의 상호인증 추진과, 현존하는 평가기준을 조화하기 위

접수일 : 2005년 2월 15일 ; 채택일 : 2005년 6월 17일
* 본 연구는 산업자원부 지역협력연구사업(과제번호: R12-2003-004-01001-0) 지원으로 수행하였음.
† 주저자, ‡ 교신저자, dusi82@se.hannam.ac.kr

한 노력의 결과로 CC Version 2.1 (ISO/IEC 15408)을 1999년 6월에 국제표준으로 발표했으며 우리나라에서는 정보통신부에서 정보보호시스템 공통평가기준으로 고시하고 있다.[1] 현재 CC는 적절하고 비용 효과적인 평가를 수행할 수 있는 골격을 제시하고 있으며 유럽과 호주/뉴질랜드만이 ITSEC과 CC를 병행하여 평가에 사용하고 미국, 캐나다 등은 CC만을 사용하고 있다. 또한, CC를 기반으로 하는 평가기술 및 방법론을 확보하여 평가업무를 수행하며 평가수요 증가, 평가시장 창출 등을 목적으로 국가별로 민간평가기관을 지정하여 운영하고 있다. 그러나, 우리나라는 아직 평가기술 미비 및 민간평가기관 부재 등 평가수요 대응에 부족하지만 2004년에 CC 상호인정협정(CCRA)에 가입을 신청하였고 이미 KISA와 국가정보원에서는 CC를 이용한 평가 및 인증이 이루어지고 있으며 향후 평가수요에 맞는 민간평가기관이 지정 및 운영될 것이다.

그러므로 평가기술을 개발하고 평가기관에서 손쉽게 활용가능한 도구의 개발이 요구되고 있다. 본 논문에서는 현재 발표된 CC 및 워크플로우를 기반으로 국내의 민간기관에서 일련의 절차에 따라 평가업무를 효율적으로 수행 및 관리할 수 있는 CC기반 Sa-EWMS(반자동화 평가워크플로우 관리 시스템, Semi-automated Evaluation Workflow Management System)을 설계 및 구현하였으며 본 시스템은 CMVP나 CC와 같은 평가기준의 평가업무 프로그램을 분석 및 적용 가능하다. 본 논문의 2장에서는 CC 및 CMVP, 워크플로우의 개념에 대해서 조사(연구)하였으며, 3장에서는 Sa-EWMS에 대한 구조 설계 및 구현결과를 보였고 마지막으로 4장에서 위의 사항들에 대한 평가 및 결론을 맺는다.

## II. 관련 연구

### 2.1 공통평가기준

CC(Common Criteria)는 미국의 TCSEC, 유럽의 ITSEC, 캐나다의 CTCPEC기준을 통합한 표준으로써 평가기준의 상호인증을 위한 골격 제시를 위해 개발되었으며, 정보보호시스템을 위한 평가기준의 국제표준일 뿐 아니라 우리나라의 정보통신부 표준이다.[2,3] CC는 모든 정보보호시스템에서 필요로 하는 보안기능요구사항의 전체집합을 클래스-패밀리-컴포넌트를 통해 계층적으로 분류하고 있다. 또한, 보증요구사항(컴포넌트)에 대해서 EAL1~EAL7과 같이 7단계의 보증수준별로 정의하고 있으며 상위의 보증수준은 하위의 보안수준보다 완전하고, 엄격하며 정형적이므로 보증수준간에는 완전성, 엄격성 및 정형성 관계를 갖는다.[1,2,4] 정보보호시스템(TOE: Target of Evaluation, 평가대상물)의 제품유형에 따라 보안기능요구사항의 일부를 선택하고 보안수준 중 하나를 택하여 보호프로파일(PP: protection profile)또는 보안목표명세서(ST: security target)를 구성한다.

### 2.2 암호모듈 평가체계

CMVP(Cryptographic Module Validation Program)는 1995년 7월 미국의 NIST와 캐나다 CSE가 공동으로 개발하였으며 FIPS 140-2 (Security Requirements for Cryptographic Modules)를 준수하는 암호모듈 검증 프로그램으로 FIPS 140-2에 따라 암호알고리즘, 해싱알고리즘, 인증알고리즘, 서명알고리즘, 키 관리를 포함한 암호모듈을 시험한다.[5] 암호모듈의 보안등급은 LEVEL1~LEVEL4로 구분되며 Level이 높을수록 보안수준이 높다. LEVEL1~LEVEL 4는 CC의 EAL1~EAL4와 대응되며 CMVP는 4가지 보안등급에 따라 11가지 영역에 대한 보안요구사항이 존재한다. 또한, 응용시스템 및 정보보호제품의 보안모듈의 평가는 CC 및 CC 인증가이드에서 명세하며 보안암호모듈 및 DES와 같은 알고리즘은 FIPS PUB 140-1과 FIPS PUB 46-3에서 명세한다.

### 2.3 워크플로우 시스템의 정의

워크플로우는 'Work+Flow'의 구성으로 '일이 흐른다'는 것을 의미하며 WfMC(Workflow Management Coalition) 에서는 워크플로우를 "일련의 절차에 따라 한 참여자에서 다른 참여자로 문서와 정보 혹은 업무가 전달되는 비즈니스 프로세스의 전부 또는 부분적인 자동화"로 정의하였다.[6] 또한, 그림 1과 같이 사전에 정의된 일정한 업무절차 규칙(Process logic)에 따라 다른 사용자(Human Resources)에게 전달되는 문서, 정보 및 태스크(Information resources)의 흐름을 자동화하는 시스템을 말한다.[7,8] 워크플로우 관리 시스템은 하나 또는 그 이상의 워크플로우 엔진을 실행하는 소

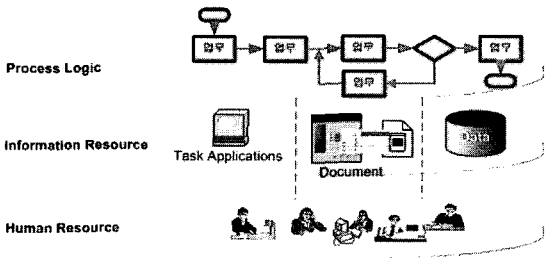


그림 1. 워크플로우 시스템의 정의

프트웨어를 이용하여 워크플로우의 수행을 정의, 생성, 관리하는 시스템이다.

## Ⅲ. Sa-EWMS 구조 설계 및 구현

### 3.1 Sa-EWMS 구조 및 워크플로우 수행 단계

프로세스를 수행할 때 사람의 개입 없이는 수행 불가능한 '인간기반 비즈니스프로세스'와 시스템이 자동적으로 수행하는 'rule기반 자동프로세스'가 존재하며 이를 통합한 것을 "반자동화 평가워크플로우 관리 시스템(Sa-EWMS)"라 정의한다. 그림 2는 Sa-EWMS의 워크플로우 수행 단계를 나타내며 기준별, 등급별 변경 가능한 평가업무 프로그램의 하위 워크플로우와 실질적인 평가관리를 수행하는 상위 워크플로우로 구분된다. 상위 워크플로우는 규칙에 따라 다음과 같이 각 단계별로 업무가 수행된다.

- 1단계 : 평가프로젝트 생성
- 2단계 : 평가제출물 관리
- 3단계 : 평가 스케줄링
- 4단계 : 평가업무 할당 및 조회
- 5단계 : 평가업무 수행 및 보고서 발행
- 6단계 : 결제/승인 및 보고서 발행

1,2단계는 정의단계(build time)에 해당하며 평가워크플로우 관리 시스템에서 평가업무를 수행 가능한 상태로 설정한다. 3단계는 프로세스 인스턴스화 및 제어상태로서 프로젝트내의 평가수행에 관한 활동을 스케줄링하며 자원(예 : 제출물, 평가기준, 평가자 등)을 할당한다. 5,6단계는 수행단계(run time)로서 특정프로세스에 대한 활동을 수행하며 간트차트 등을 통한 평가프로젝트를 모니터링한다. 3~6단계는 실질적인 평가업무 수행을 나타내며 "평가워크플로우 엔진(EWE : Evaluation Workflow Engine)"에서 관리한다. 또한, 3단계에서는 하위 워크플로우를 적용하여 평가 스케줄링을 작성하게 된다. 하위 워크플로우를 평가기준별, 등급별로 다르게 작성될 수 있으며 상위 워크플로우와 하위 워크플로우는 독립적이다. 본 논문에서는 상위 워크플로의 기반이 되는 하위 워크플로우에 대해서 설명한 후 상위 워크플로우의 상세사항을 설명하도록 한다.

### 3.2 하위 워크플로우

평가에 필요한 평가의 흐름을 정의해주는 프로그램을 "평가업무 프로그램(EAP : Evaluation Activity Program)"이라 하며 EAP는 평가기준에 따라 다르게 구성된다. 본 논문에서는 CC를 기반으로 제시된 평가업무에 대한 분석, 즉 "EAP(평가업무 프로그램)" 사례를 도출하였다.

#### 3.2.1 CC기반 평가업무 프로그램 사례

EAP는 CC에서의 보증요구사항 등급에 따라 다르게 구성된다. 그러나, 보증요구사항 등급별 컴포넌트 자체만으로는 불충분하여 다른 컴포넌트에 의존해야만 하는 경우가 발생하며 이를 "종속성(dependency)"이라 한다. 평가프로젝트에서 보증클래

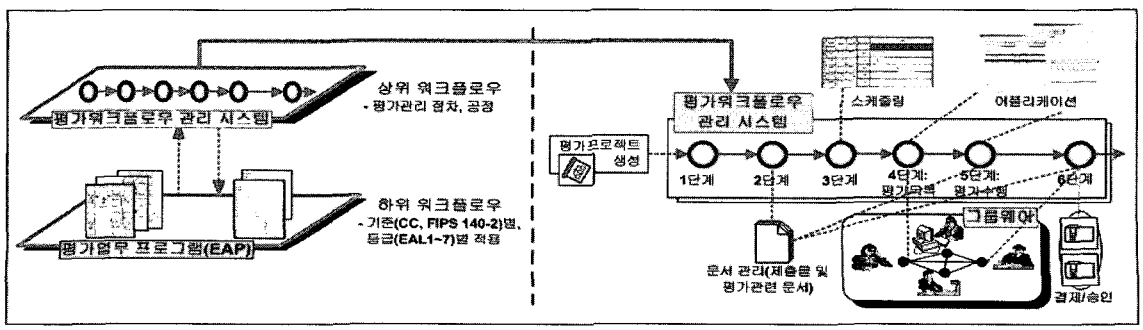


그림 2. Sa-EWMS의 워크플로우 수행 단계

**[EAP 생성 알고리즘]**

```
S# = 1;      // STG number
Temp = Original;
// Temp는 임시 저장소(i.e., EAL1에 정의된 종속성
   관계 목록).
For each component COM in Temp that don't
    have 'in-going' dependency relation,
  do
    Draw the COM as an AN on STGp of EAP;
    // AN은 "활동 노드"
    Delete COM's "out-going" dependent
    relations from Temp;
  end-do
repeat
  for each component COM in Temp that don't
      have 'in-going' dependent relation,
   do
     Draw the COM as an AN in STGQ of EAP;
     Delete the COM's "out-going" depen-
     dent relations from Temp;
     Draw arcs from AN in STGp to AN in
     STGQ by using Original;
   end-do
P = Q; S# = S# + 1;
until (there is no more relation in
      Original.)
if(A has an ARC to B) and (B has an ARC
  to C) and (A has an ARC to C),
  then delete ARC that is from A to C.
// A, B, C는 EAP의 AN임. 만일 EAP에 '이행관계'가
존재하면, 간소화하기 위해 삭제함.
```

스, 컴포넌트, 평가자행동과 개발자행동과 내용 & 증거의 표현이 각각 활동, 부활동, 행동과 업무단위에 대응함을 상기하여야 한다.[12]

종속관계 목록은 종속관계에 있는 보증 컴포넌트들의 최소집합을 나타내며 이는 비반사적, 비대칭적인 특징을 가진 "부분종속성"에 속한다. "부분종속성"은 단순하고 편리하지만 각 컴포넌트간 독립성을 무시하고 범위 유지가 어려우므로 평가프로젝트를 수행하기 위해서는 이해적이며 반사적인 "전체종속성"을 따라야 한다. 따라서, 컴포넌트들간의 부분종속관계를 전체종속관계로 변환하기 위해 "EAP 생성 알고리즘"을 적용할 수 있다.[10]

또한, 평가프로젝트의 문맥에서 평가부활동의 선행관계로서 보증컴포넌트의 의존관계에 주의하여야 하며 EAL1~EAL7의 보증컴포넌트 사이의 관계를 표현한 "템플리트(예 : EAP1~EAP7)"를 따라야 한다. "템플리트"는 TOE와 평가환경에 독립적이며 CC에서 유도되었다. "템플리트"는 다음과 같다.

$$EAP = (AN, ARC, STG)$$

- ***AN***은 "활동노드"의 집합이다. AN은 컴포넌트명, 제출물명, 자원(예 : 평가기간, 비용, 개발자, 평가도구)과 같은 세 가지 애트리뷰트를 포함하며 평가활동과 보증컴포넌트 평가시 필요한 제출물 및 평가기간, 비용 등을 할당하여 표현한다. EAP 템플리트에서는 할당에 관한 사항은 표현하지 않는다. 특히, 할당 애트리뷰트는 평가프로젝트 관리의 목적으로 사용된다.
- ***ARC***는 다른 "stage"에서 AN과 AN사이의 "아크(arcs)"이다. ARC는 두 개의 AN사이의 절차 관계를 표현하며 AN은 프로젝트 관리면에서 "stage"상에서 독립적으로 수행될 수 있다.
- ***STG***는 "stage"의 집합이며 $stage_1$에서 마지막 stage까지의 패스는 AN의 전체종속성을 표현한 것이다.
- ***EAP***는 "EAP 생성 알고리즘"을 의미하며 템플리트는 그림 3과 같이 활동네트워크 또는 간트챠트로 표현될 수 있다.

### 3.2.2 CC기반 평가업무 프로세스 정의

CC기반 평가업무는 평가업무 프로그램에 적용된 "EAP 생성 알고리즘"을 이용하여 그림 4의 Work-

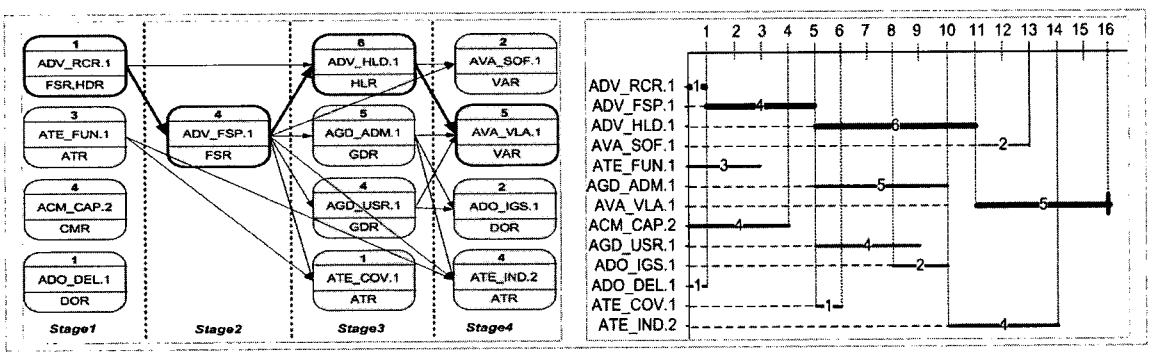


그림 3. EAP 2의 활동 네트워크 및 간트챠트(예)

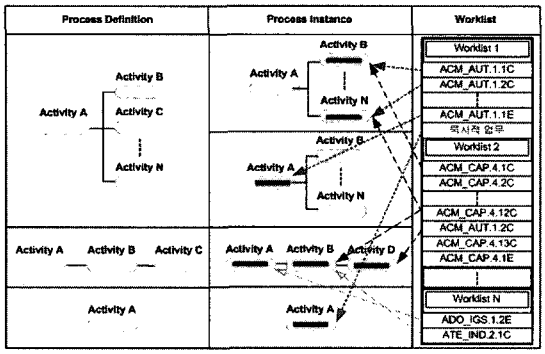


그림 4. EAL4 평가업무(Worklist)와 객체(정의)간의 관계

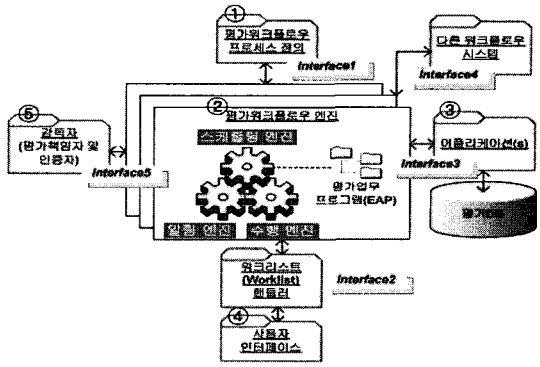


그림 5. Sa-EWMS의 오브젝트 모델

list와 같이 순서화할 수 있다. 다음은 평가업무 프로세스에 관한 용어를 정의한 것이며, 그림 4는 CC 기반 EAL4등급 평가업무(Worklist)와 객체간의 관계를 나타낸다.

- ***Process Definition*** : 프로세스에 관련된 사람, 자원, 정보들의 구체화된 표현으로 워크플로우 시스템에서 실행 가능한 형태이다.
- ***Process Instance*** : 워크플로우 시스템에서 실제 처리를 위해 생성된 프로세스이다.
- ***Work item*** : 워크플로우 참여자(평가자)의 관점에서 실제 처리되어질 활동 인스턴스(평가업무)이다.
- ***Worklist*** : 워크플로우 참여자(평가자)에게 주어진 Work item(예:ACM_AUT.1.1C 등)의 평가업무목록. CC에서는 평가자 행동을 말하며 개개의 Worklist는 EAP의 "활동노드(AN)"와 같다.

### 3.3 상위 워크플로우

평가시 다수의 "인원"과 다종 및 다수의 "평가도구"에 다수의 "제출물"이 적시 적소에 공급되어야 하며, 이들 간의 조정(coordination)과 스케줄링이 중요하다. 본 절에서는 EAP를 적용하여 실질적인 평가관리와 평가업무를 수행하는 상위 워크플로우 즉, 평가워크플로우 관리 시스템을 설계하였으며 그림 5에서 제시한 오브젝트 모델의 각 구성요소에 관하여 정의하도록 한다.

#### 3.3.1 평가워크플로우 프로세스 정의 - ①

(1) 평가워크플로우 엔진의 프로세스 정의

상용제품마다 노드명세 및 프로세스 정의가 다르지만 큰 골격은 WfMC의 노드명세 및 프로세스 제어구조를 기반으로 정의하였으며 본 평가워크플로우 엔진에서도 표 1에서와 같이 프로세스 노드 및 제어구조를 정의하였다. Sa-EWMS의 프로세스 노드는 업무노드(Manual Activity, Automated Activity), 라우팅노드(Conditional, OR/AND(Join/Split)), 시작 및 완료노드(Start, Abort, End), 기타(워크플로우 엔진 : Workflow Engine)으로 분류될 수 있다. Sa-EWMS 워크플로우 엔진의 구조는 워크플로우 엔진 상호연동 시나리오(연결프로세스, 서브프로세스, 병렬 동기화)의 규칙을 따른다.[7]

표 1. Sa-EWMS 평가워크플로우 엔진 프로세스 노드 및 제어구조 정의

| Notification | Name | description |
|---|---|---|
| | Start | 워크플로우의 시작을 나타낸다. |
| | Abort | 워크플로우의 중지 및 종료를 나타낸다. |
| | End | 워크플로우의 종료를 나타낸다. |
| | Manual Activity | 워크플로우의 업무 노드로써 일을 수행하며 사람의 개입 없이 처리될 수 없는 노드이다. |
| | Automated Activity | 워크플로우 시스템이 자동적으로 처리할 수 있는 노드이다. |
| | Conditional | '참' 또는 프로세스 제어구조의 'XOR'에 해당한다. |
| | OR/AND | 'OR-Join/ADN-Join'또는'OR-Split /AND-Split'을 나타낸다. |
| | e-mail | e-mail 수신 및 발신을 나타낸다. |
| | Workflow Engine | '워크플로우 엔진'을 나타낸다. |

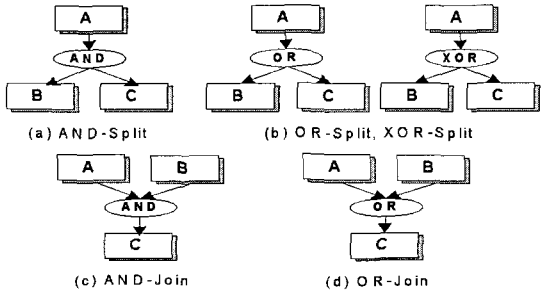


그림 6. 프로세스 제어구조 그래픽 표현

(2) 프로세스 제어 구조[9]

- AND-Split : 워크플로우 내에서 단일스레드가 병렬적으로 실행되는 복수활동을 허용하며 적어도 2개의 선으로 나뉘는 포인트이다. 워크플로우 시스템 내에서 AND-Split에 만들어지는 모든 스레드는 보통 AND-Join포인트에서 생성되며 다른 AND-Join포인트에서 발생할 수 있는 스레드의 부분집합에서 발생한다. 또한 잠재적으로 다른 AND-Split 포인트에서 생성된 입력쓰레드를 포함한다.
- OR-Split : 워크플로우 내에서 단일스레드가 복수의 대안 워크플로우가 존재할 때 분기에 대한 결정을 하는 포인트이다. WfMC는 유일한 하나의 경로를 구별하지 않으며 경로는 여러 개가 될 수 있다. XOR-Split은 구별에 대한 모호함을 피하기 위한 포인트로써, 유일한 경로에서 나눠진다.
- AND-Join : 워크플로우 내에서 적어도 2개의 병렬활동이 단일스레드로 집중되는 포인트이다. 다음 활동에서 모든 스레드 트랜지션이 완료될 때까지 병렬활동이 수행되며 이 경우가 아니면 양쪽 병렬스레드가 "도착(reach)"한다는 가정을 내재하고 있다.
- OR-Join : 워크플로우 내에서 적어도 2개의 대안활동 워크플로우 가지가 워크플로우 내의 다음 단계, 즉 단일공통활동으로 재병합되는 포인트이다. 이는 병렬 활동이나 동시성을 요구하지 않는다. 만일 병행실행이 join포인트에서 일어난다면 OR-Join이 어떻게 행동해야 하는가는 명확하지 않다.

### 3.3.2 평가워크플로우 엔진(EWE) - ②

본 절에서는 Sa-EWMS를 구축하기 위해서 분석된 EAP를 이용하여 실제 "평가워크플로우 엔진"에 적용하였다. 한편, CMVP에 대한 평가업무 프로그램을 도출하여 본 "평가워크플로우 엔진"에 적용가능하며 본 논문에서는 CC를 중점으로 도출된 결과를 보인다. "평가워크플로우 엔진"이란 평가업무에 대한 워크플로우 프로세스를 추적하고 각 워크플로우 단계의 수행을 조정하며 클라이언트 즉, 사용자와 워크플로우 절차를 주고받는 본 시스템에서 가장 중요한 역할을 수행한다.

#### 3.3.2.1 스케줄링 엔진 시나리오

스케줄링 엔진에서는 병렬 동기화, 즉 2개의 독립된 워크플로우 시스템에 있는 프로세스 실행 시점 중 일부가 동기화된다. 스케줄링 엔진은 평가프로젝트를 수행하기 위해 목표 평가보증등급에 따른 EAP를 이용하여 해당업무의 실행순서를 판별 및 자동 스케줄링하며 부가적인 작업일 및 자원 할당 역할을 한다. 그림 7은 Sa-EWMS의 "스케줄링 엔진" 시나리오를 나타내며, 제시된 바와 같이 스케줄링 엔진은 활동이 시작되면 동시에 두 가지 업무노드로 나누어진다. 업무 중 하나는 날짜를 비교하여 스케줄을 **A:실시간으로 검사**하며 알림 엔진을 호출하여 해당 참여자에게 업무공지를 해준다. 다른 업무는, **B:평가프로젝트 정보**를 **호출**하여 해당 평가프로젝트에 대한 **C:스케줄이 입력**되었는지를 확인 및 검사한다. 스케줄이 입력되지 않았을 때 **D:권한 검사**를 통하여 평가책임자가 아니면 수행 흐름을 중지시킨다. 반면, 평가책임자의 권한이 확인되면 **E:"EAP"**를 **구동**시키며, 해당 프로젝트의 "EAP"에서 자동적으로 구성된 **F:단위업무의 스케줄을 출력**한다. 이후 작업은 평가책임자에 의해 선택적으로 행해지는 활동노드로 구성되며, 평가책임자는 **G:출력된 단위업무 스케줄 GUI**에서 **H:자원(평가자, 평가도구, 평가제출물 등)을 할당** 및 **I:평가시간을 조정**한다. 자원할당과 평가시간 조정은 하나만 이루어져야 하는 활동이 아닌 두 가지 모두 이루어져야 하는 활동이므로 워크플로우 내에서 단일 스레드가 병렬적으로 실행되는 복수의 활동을 허용하는 선으로 나누어진다. 자원을 할당할 때 자원에 대한 정보는 스케줄링 엔진을 통해 자동적으로 검색 가능하며 "자원을 더 할당할 것인가?"의 조건문을 통하여 자원할당 업무를 수행할 수 있도록 2개의 대안활동 워크플로우 가지가 워크플로우 내의 다음단계, 즉 단일 공통 활동으로 재병합된다. 자원할당과 평가시간 조정이 모두 완료되면 이 2개의 활동이 단일

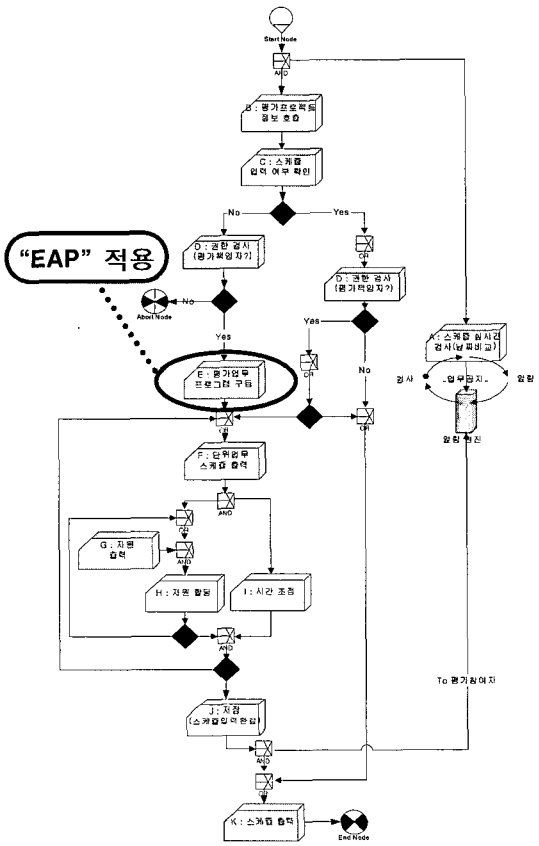


그림 7. Sa-EWMS 스케줄링 엔진 시나리오

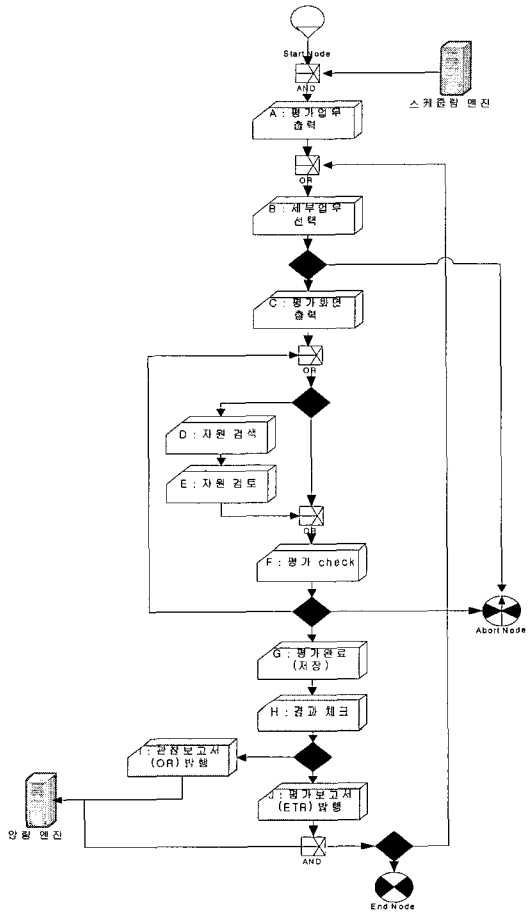


그림 8. Sa-EWMS 평가수행 엔진 시나리오

스레드로 집중되며 조정한 스케줄링에 대한 저장여부를 선택한다. 여기에서, **J:스케줄링한 내용을 저장**하면 스케줄 입력이 완료되며, **K:저장된 스케줄을 화면에 출력**하고, 스케줄된 내용에 대해 알림 엔진을 호출하여 업무공지를 하는 병렬적인 활동을 수행한다. 반면, 스케줄링한 내용을 저장하지 않고 새로운 내용으로 대체하고자 한다면 "EAP"를 통하여 단위업무 스케줄을 출력하는 단일 공통 활동으로 재병합된다.

### 3.3.2.2 수행 엔진 시나리오

수행 엔진은 나머지 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 8은 "평가수행 엔진" 시나리오를 나타내며 참여자(평가자, 평가책임자, 감독자)의 역할에 따라 각각의 업무를 흐름에 맞추어 수행할 수 있도록 제어하는 역할을 한다.

할당된 평가프로젝트에 대한 평가업무에 대해 호출할 때, 스케줄링 엔진을 통하여 기작성된 스케줄링에 대한 활동을 집중시켜, **A:평가업무 활동을 화면에 출력**한다. 다음으로 평가책임자 또는 에이전트가 **B:세부 업무를 선택**하면 **C:평가 화면이 화면에 출력**되며 평가자가 세부업무를 수행할 때 자원이 필요하다면 **D:자원 검색** 및 **E:검토**를 통하여 **F:평가업무를 수행**한다. 평가자는 수행한 **G:평가업무를 저장**하며 저장된 평가업무에 대해서 평가수행 엔진은 **H:결과를 체크**한다. 평가결과가 "유보" 또는 "실패"가 나왔을 경우 평가수행 엔진은 **I:"관찰보고서(OR : Observation Report)"를 발행**하며, 평가결과가 "통과"가 나왔을 경우에는 **J:"평가기술 보고서(ETR : Evaluation Technology Report)"를 발행**한다. 상기와 같은 두 가지 경우, 평가수행 엔진은 알림 엔진에 진행 중인 프로세스를

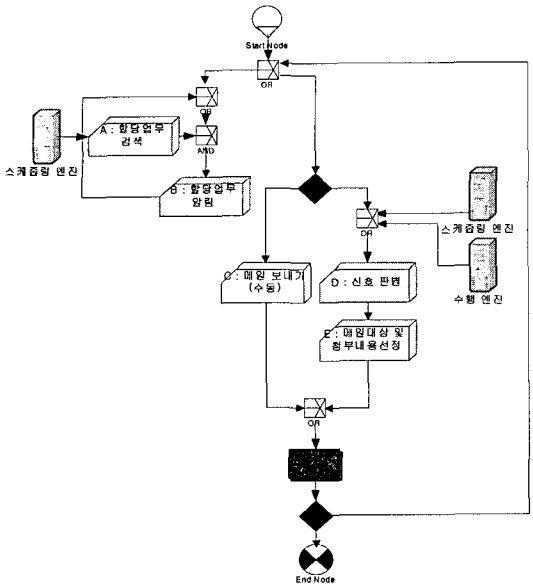


그림 9. Sa-EWMS 알림 엔진 시나리오

넘겨주어 활동을 수행한다. 평가결과를 체크하여 OR과 ETR을 발행할지를 결정할 때, CC기반 정보보호시스템 평가는 배타적구조를 가지며 평가단위 계층구조에도 배타적인 평가구조가 적용된다. 따라서, 평가주기에 따른 범위를 정의하고 배타적 평가구조에 따라 작성된 "평결 알고리즘"을 평가수행 엔진에 적용할 수 있다.

#### 3.3.2.3 알림 엔진 시나리오

알림 엔진은 "서브프로세스(특정 워크플로우 시스템의 프로세스가 다른 워크플로우 시스템 프로세스의 일부분으로 수행되는 경우)"로서, 스케줄링 엔진과 평가수행 엔진에서 발생하는 알림업무를 프로세스의 일부분으로 수행하는 역할을 한다. 그림 9는 "알림 엔진" 시나리오를 나타내며 반복적인 활동을 한다. 또한, 자동적인 부분과 수동적인 부분의 대안 워크플로우가 존재하며 활동이 분기된다. 알림 업무는 업무 공지를 위해 스케줄링 엔진을 통한 **A:할당업무를 검색**하여 자동적으로 업무를 알리는 경우와 이러한 활동들을 반복적으로 수행하면서 발생하는 경우 모두 **B:할당업무 알림**이라는 단일 활동으로 집중된다. 할당업무 알림 활동은 단일 공통 활동으로 재병합되어 상기와 같은 활동을 스케줄링 엔진의 일부분으로서 반복적으로 수행한다. 한편, 알림 엔진은 평가관리 도구를 사용하는 사용자가 **C:수동적으로 메일을 보내는 활동**과 다른 워크플로우 엔진으로부터 입력된 신호에 의해 활동을 하는 부분으로 분류된다. 스케줄링 엔진과 평가수행 엔진에서 입력된 신호, 예를 들어 평가수행 엔진에서 "관찰 보고서(OR)"를 발행한다는 신호가 입력된다면 공통 활동으로 병합되어, 알림 엔진은 **D:신호를 판별**한 후, 신호에 따른 **E:메일 대상 및 첨부 내용을 자동적으로 선정**해준다. 이러한 수동적인 메일작성과 자동적인 메일작성 부분이 이메일(e-mail) 발신 활동을 수행한다. 알림 엔진은 프로세스를 종료하지 않는 한 반복적으로 계속 병합되어 수행된다.

#### 3.3.2.4 평가워크플로우 엔진에 적용된 알고리즘

(1) 평결 알고리즘

CC기반 정보보호시스템 평가는 배타적인 구조를 가지며 평가 단위 계층구조에도 배타적인 평가구조가 적용된다. 따라서, 평가주기에 따른 범위를 정의하고 배타적인 평가구조에 따라 작성된 평결 알고리즘을 평가수행 엔진에 적용하였다.

(2) 평가스케줄링 알고리즘

평가업무 스케줄링 시, "EAP 템플리트"를 이용하여 등급별 평가업무 $E_w$ (n개의 단위업무로 이루어져 있음)를 얻게 되며 각 단위업무 i에는 ($S_i$, $E_i$)가 지정된다($S_i$ : 시작시간, $E_i$ : 마감시간). 다음과 같은 평가스케줄링 알고리즘은 최소의 평가자가 중복되지 않은 평가업무를 수행할 수 있도록 단위업무를 할당하기 위해 욕심쟁이 알고리즘 방법을 응용하여 적용하였다.

#### 3.3.2.5 효과 및 발전방향

정보보호시스템의 CC기반 평가워크플로우 엔진으로서의 역할 이외에도 다른 종류의 평가워크플로우 엔진으로 활용할 수 있으며, 더 나아가 워크플로우 엔진에 대한 모델링을 페트리 넷이나 UML의 활동도로 명세화할 수 있다. 즉, 사용자 혹은 클라이언트가 어떤 일을 해야 할지 직접 찾지 않고 사용자가 처리해야 할 작업들을 시스템이 제시해주며, 각 참여자가 후속 처리 담당인원이 누구인지 알 필요 없이 자신이 수행할 일만 처리하면 되므로 필요한 시간 내에 오류 없이 처리되는 워크플로우 프로세스를 기대할 수 있다. 또한, 업무의 중복을 미연에 검토하여 방지할 수 있으며, 프로세스를 반복적으로 모니터링해 나감으로써 투명한 관리 및 비용절감의 효과를 볼 수 있다.

**[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 in-
         conclusive)
       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 관찰보
  고서(OR)
  else if sub-activity ="pass", ⑤ write 평가
  기술보고서(ETR)
    If any work unit = "inconclusive",
    evaluation result= "inconclusive"
```

**[평가스케줄링 알고리즘]**

```
Algorithm EvaScheduling()
/* 평가업무프로그램(EWP)의 등급별 평가업무 Ew를 입력

int AllocateWork(Ew, n) // 욕심쟁이 알고리즘
/* 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 평가자 Evaper
 에 할당 }
 else {
 NewEvaper = NewEvaper + 1;
 NewEvaper = Ewi ; //단위업무 i를 NewEvaper에
 할당 }
 } returen NewEvaper; }
```

### 3.3.3 외부 어플리케이션 및 인터페이스 - ③,④

#### 3.3.3.1 외부 어플리케이션

Sa-EWMS의 외부 어플리케이션은 워크플로우 엔진으로부터 데이터를 받아 업무수행을 하고 결과를 반환하는 역할을 하며 정보보호시스템에 대한 정형화 검증도구, 형상관리도구 등의 평가도구가 존재한다.

#### 3.3.3.2 인터페이스

그림 10은 개발자 Client와 평가자 Client, 평가웹서버 및 평가 DB의 관계를 보이며 개발자 Client와 평가자 Client의 인터페이스를 나타낸다. 개발자 입장에서는 평가받고자 하는 목표등급에 맞추어 제출물을 손쉽게 작성하며, 평가 웹서버에 제출하게 된다. 평가자 입장에서는 제출물을 확인하고

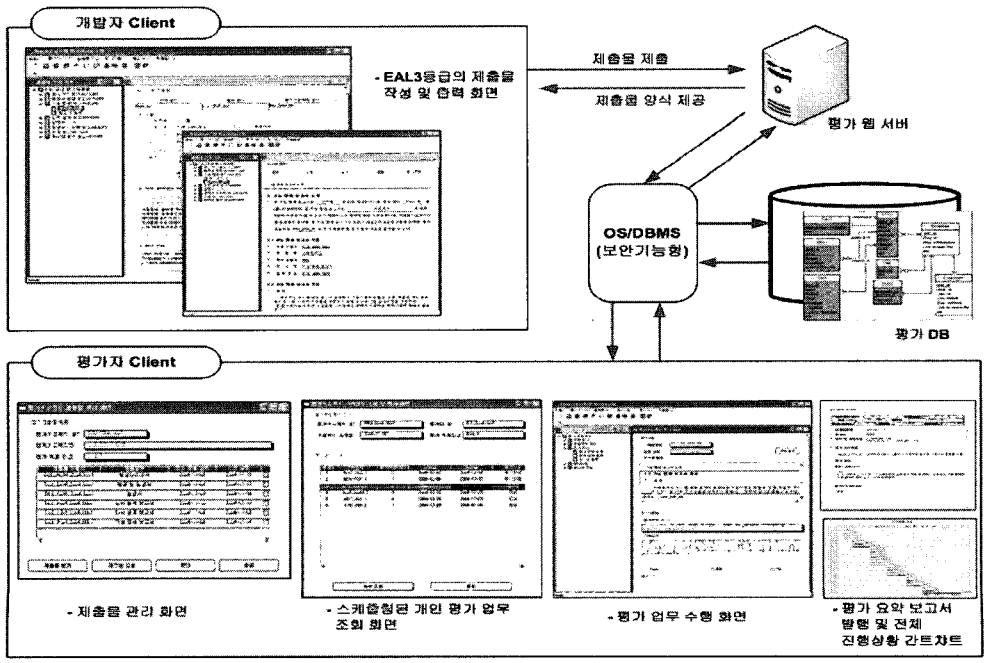


그림 10. Sa-EWMS 평가 사례 인터페이스

평가 기준에 따라 평가 업무 수행 및 모니터링을 할 수 있으며 최종적으로 보고서를 발행한다. 이러한 인터페이스에는 트리구조 및 버튼 등의 워크리스트 핸들러가 존재한다. 정보보호시스템의 시험/평가는 대외비 자료라 할 수 있으므로 평가자 이외에는 기밀로 처리해야 한다. 따라서, 평가관리시스템 자체에도 보안기능이 요구되며, Sa_EWMS는 웹기반 및 인트라넷기반(클라이언트-서버)으로서 보안기능이 강화된 OS, DBMS, 웹서버를 이용한다. 또한, 각 서브시스템간에는 인증, 기밀, 무결성, 부인봉쇄 등의 보안서비스를 제공한다.

### 3.3.4 감독자(Supervisor) - ⑤

본 시스템에서 평가에 관한 모든 사항을 관리하는 감독자 및 인증자는 평가자 중의 한명으로 평가책임자가 된다. Sa-EWMS에서는 역할기반 접근통제

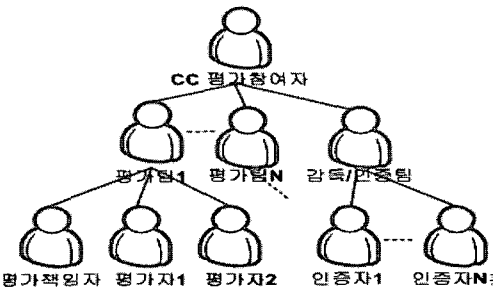


그림 11. CC 평가참여자 구성도

(권한검사)를 사용하여 평가책임자에게 권한을 부여하고 평가프로젝트 생성 및 제출물 관리, 평가 스케줄링, 평가 모니터링을 할 수 있다. 또한, 일부 평가결과에 대한 감독/인증의 업무를 수행하는 제한적인 인증자가 존재한다. 그림 11은 Sa-EWMS의 CC 평가참여자 구성도를 나타낸다.

표 2. CC기반 평가 관련 지원 시스템 비교[13,14]

| | 범위 | 특이사항 |
|---|---|---|
| AGTER v1.0<br>(평가결과 자동생성도구) | - CC기반 | - 평가결과 (보고서:OR,EWP,ETR)에 중점을 둠<br>- KISA에서 참여 |
| 기타<br>(자동화된 CC평가프로세스) | - CC기반 | - 연구 및 개발중 (공개안함.)<br>- CCTL에서 참여<br>- CC 평가 프로세스를 자동화하는데 중점을 둠 |
| 제시한 시스템<br>(Sa-EWMS) | - CC기반(향후 FIPS140-2로 확장 가능-EAP이용) | - 평가 준비 및 수행, 결과 모두를 관리하는데 중점을 둠. |

표 3. 프로젝트 관리면에서의 시스템 비교[15,16]

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

O : 기능 존재 △ : 기능의 일부 존재 × : 기능 부재

## Ⅳ. 평가 및 향후 연구과제

본 논문에서는 평가수요 증가에 따른 기존의 정보보호시스템에 대한 평가기술 부족과 수동적인 평가업무 등의 문제점을 해결하기 위해 반자동화 평가워크플로우 관리 시스템(Sa-EWMS)을 제시하였다. 이와 유사한 시스템으로서 표 2, 3에 각각 CC기반 평가 관련 지원 시스템에 대한 비교와 프로젝트 관리 면에서 MS Project(Microsoft), Project Kick-Start(Experience In Software), ProChain Project Management (ProChain Solutions) 등을 비교하여 제시하였다. MS Project 등은 단순히 스케줄링을 통해 워크리스트를 만들고 업무관리를 할 수 있지만 절차적 자동화를 지원하는 워크플로우에는 한계가 있다. 평가워크플로우 관리 시스템은 다양한 단계에 걸쳐 있는 평가자 혹은 평가도구, 평가관련 문서 등을 적절하게 배치 혹은 관리함으로써, 비즈니스 프로세스의 절차적 자동화를 지원하고, 이로 인한 업무능력 향상과 비용효과적인 결과를 도출할 수 있는 이점이 있으며 이중의 워크플로우를 설정하여 서로 독립적으로 수행되도록 설계하였다. 이러한 워크플로우의 도입의 효과로 Sa-EWMS를 사용하는 사용자의 만족도가 향상되며 평가업무 수행 및 개선시에 수반되는 변화의 비용감소를 기대할 수 있다. Sa-EWMS는 향후 평가를 수행하는 평가기관에서 평가수요에 대응하여 평가업무를 효율적으로 수행 및 관리할 수 있으며 정보보호시스템의 평가/인증에 대한 최적의 보안성을 높이고 CC 이외의 CMVP와 같은 다른 평가기준 및 평가체계 업무를 적용시켜 시장성을 높일 수 있을 것이다.

향후 연구과제로는 자체 정보 및 시스템에 대한 보안성을 높여야 하며, 적은 인원이 동시에 여러 개의 평가 프로젝트에 참여할 수 있는 동시평가관리 기능을 고려하여야 할 것이다. 또한, 다른 평가 기준에 대한 EAP를 개발하여 본 시스템에 적용할 수 있도록 연구 및 개발 중이다.

## 참 고 문 헌


[1] 한국정보보호진흥원, "정보보호시스템 평가·인증 가이드", www.kisa.or.kr, pp.52-68, 2002. 12.

[2] European Community,□*Information Technology Security Evaluation Criteria (ITSEM)*, Ver.1.0, http://www. cesg.gov.uk /assurance/iacs/itsec/index.htm, 1993.

[3] DoD, *Department of Defense Trusted Computer System Evaluation Criteria (TCSEC)*, US DoD 5200.28-STD, Dec. 1985.

[4] CC, *Common Criteria for Information Technology Security Evaluation(CC)*, CCIMB-2004-01-003, Version 2.2 : ISO/IEC 15408, Jan. 2004.

[5] 이상진, Cryptographic Module Validation Program(CMVP) and Common Criteria(CC), KR-Net발표자료, http:// www.krnet.or.kr/technical_sum.php, 2003.

[6] Workflow Management Coalition, Interface 1 - Process Definition Interchange V1.1, WfMC Specification, WfMC-TC-1016-P, 1999.

[7] Cichocki. A., Helal A. and Woelk D., *Workflow and Process Automation Concepts and Technology*, Kluwer Academic Publishers, 1998.

[8] Gustavo Alonso et al., *Web Services : Concepts, Architectures and Applications*, Springer-Verlag Berlin Heidelberg, pp.82-90, 2004.

[9] Workflow Management Coalition, Interface 4 - Interoperability Abstract Specification, WfMC- TC-1003, 1995.

[10] Workflow management Coalition, *Terminology & Glossary*. Document Number WFMC-TC-1011, Document Status-Issue 3.0, Feb. 1999.

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

[12] 한국정보보호진흥원, "공통평가기준 기반 평가기간 산정 방안 및 평가수수료 정책 연구", *한국정보보호진흥원*, 수탁기관 : 한남대학교, 2003. 11.

[13] Hwa-Jong Shin, "Development and Utilization of Automatic Generation Tool for Evaluation Report", 5th ICCC: KISA, Sep. 2004.

[14] Ruben Prieto-Diaz, "Automating the Common Criteria Evaluation Process", *CISC*, http://www.jmu.edu/cisc/research/prietodiaz2.html
[15] Jeff Crow, "Project Management Tips", http://www.projectkickstart.com
[16] Robert C. Newbold, "Introduction to Critical Chain Project Management", ProChain Solutions, Inc. http://www.prochain.com/articles/Critical-Chain-Article.asp. 2002.

## 〈著者紹介〉

**강 연 희 (Kang Yeon Hee)** 정회원
2003년: 한남대학교 컴퓨터멀티미디어공학과 졸업(학사)
2003년~현재: 한남대학교 컴퓨터공학과 석사 과정
〈관심분야〉 소프트웨어공학, 정보보호시스템 평가, 보안공학, 프로젝트 관리, 시스템 모델링

**김 정 대 (Kim Jung Dae)** 정회원
2003년: 한남대학교 컴퓨터공학과 졸업(학사)
2004년~현재: 한남대학교 컴퓨터공학과 석사과정
〈관심분야〉 소프트웨어 품질 평가 및 보증, 소프트웨어 표준화, 보안공학

**이 강 수 (Lee Gang Soo)** 종신회원
1981년: 홍익대학교 전자계산학과 학사
1983년: 서울대학교 대학원 전산학과 석사
1989년: 서울대학교 대학원 전산학과 박사
1985년~1987년: 국립한밭대학교 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