情 報 保 護 學 會 誌
第 13 券 第 5 號, 2003. 10

국제 공통평가기준(CC)의 교육 동향 및 평가된 정보보호 제품 분석

오 흥 룡*, 염 흥 열*

요 약

IT(Information Technology) 제품의 보안 기능을 평가하기 위한 서로 다른 체계를 이용함으로써 평가를 위한 이중의 비용 소요와 추가의 시간 소모 등의 문제점을 해결하기 위하여, 미국, 영국 등의 선진국들은 국제간에 상호 인정이 가능한 공통평가기준(CC : Common Criteria)에 대한 연구를 활발히 수행하고 있고, CCRA(Common Criteria Recognition Agreement)에 가입한 나라에서 평가된 제품은 다른 나라에서 재평가 과정을 거치지 않고 상호 인정하는 CCRA 라는 평가를 위한 국제 조약을 체결하여 시행 중에 있다. 그러나 CC는 다양한 보안 제품에 대하여 시행되고 있고, 표준안의 분량이 매우 많을 뿐만 아니라 복잡하며, 개발자와 평가자, 그리고 이용자 모두가 평가를 위한 기술적, 관리적, 절차적 과정의 이해가 무엇보다도 중요하다. 따라서 CC 주요 주체에 대한 평가 교육의 필요성이 매우 중요하게 대두되고 있다. 또한 우리 나라도 국제공통평가기준 인정 협정인 CCRA로의 가입을 준비중에 있고, 다양한 제품으로 평가 제도의 확대를 준비하고 있다. 본 논문에서는 각 나라의 CC 교육 과정을 분석하고, 현재 CC 체제하에서 평가된 정보보호 제품들의 특성을 분석하며, 이를 바탕으로 우리의 평가 교육 현실을 살펴본 후, 국내 CC 교육 프레임워크와 실천 방안을 제시한다.

Ⅰ. 서 론

CC는 IT 제품에서 보안성을 평가를 위해 평가기준을 발전시킨 노력의 결과로써 기술 선진국 각국에 널리 사용되고 있다. CC는 유럽, 미국, 캐나다 등의 평가기준을 정리하고 발전시킨 것이기도 하고, 또한 다양한 평가기준의 개념적 차이와 기술적 차이를 해결한 것이며, 평가결과를 해당 상호국가간에 인정해주는 방식이기도 하다. CC 버전 2.1은 1999년 국제 표준화 기구(International Organization for Standardization/International Electrotechnical Commission) 15408: "Evaluation criteria for information technology security"에 채택되어 있다. CC의 주요 내용으로 Part1은 일반적인 모델의 보안 설명서 및 평가 그리고 기본적인 개념 소개를 다루고 있다.

이들의 개념은 보호프로파일(PP : Protection Profile)과 보안목표명세서(ST : Security Target)를 기본적으로 포함한다. CC는 제품과 시스템의 IT 보안을 위해 요구되는 등급을 다루는 분야이고, CC Part2는 기본적으로 요구되는 보안기능을 CC Part3은 보안보증 요구를 다루고 있다[10].

CC는 IT 제품과 시스템의 보안 적합성에 대한 발전과 유효성을 관리하는 보안 명세의 개발을 위해 요구되는 명세 구조이다. CC는 원칙적으로 IT 보안 실행의 정확함을 검증하기 위한 도구로써 정형화된 평가에 초점을 맞추고 있지만 요즘은 일반화된 시스템 보안 기술과 검증 과정을 제공하기 위해 광범위하고 다양한 응용 상황에도 사용되고 있다.

현재에서는 IT 소비자, 개발자, 평가자, 그리고 국가 해당기관들은 제품이나 시스템 보안에 대한 신뢰가 적절한 것인지를 판단할 수 있는 지식, 전문성, 자원 등이 상당히 부족한 상태이다. 따라서 CC 교육과정을 통해 소비자들은 IT 제품이나 시스템의 보안수단에

* 순천향대학교 정보보호학과(master@elec.sch.ac.kr, hyyoum@sch.ac.kr)

대한 평가신뢰를 높이고 개발자들은 IT 제품과 시스템 개발 시에 공통평가기준에 맞추어서 개발하는데 도움이 될 수 있고, 평가자들은 IT 제품의 유효성을 평가하기 전에 부족한 부분의 CC 지식을 교육받음으로 좀 더 능숙해 질 것이고, 기업 관계자들도 스스로 자기 제품에 대한 평가를 할 수 있을 것이다.

본 논문에서는 이와 같은 CC 교육과정에 대한 각국의 동향과 평가된 정보보호 제품들의 실태를 파악하고 국내의 CC 교육과정에 대하여 간략히 논하고 이를 근거로 새로운 평가 교육환경을 예측하며, 이에 대비한 평가 교육체계를 마련하고 구체적인 운영방안을 제안한다. 주요 내용으로 본론의 II장에서는 대표적인 기술 선진국의 몇몇 교육기관에 진행하고 있는 교육과정을 소개하고 각 교육 내용의 특징들을 분석할 것이며, III장에서 결론을 맺는다.

II. 본 론

CC는 보안시스템 유형이 전반적으로 전제된 보안평가기준을 제시하고 있다. 2000년 5월에 미국(NIST/NSA, National Institute of Standards and Technology/National Security Agency), 독일(BSI, Bundesant fur Sicherheit in der Informationstechnik), 호주(AISEP, Australasion Information Security Evaluation Programme), 캐나다(CSE, Communications Security Establishment), 영국(CESG, Communication Electronics Security Group), 프랑스(SCSSI, Direction Centrale de la Securite des Systemes d 'Information) 등 IT 선진 15개국 정부의 정보보안기관이 CC EAL(Evaluation Assurance Level) 4 등급까지 평가결과를 국가간 공통평가기준 상호인정협정(CCRA : Common Criteria Recognition Arrangement)에 서명함으로써 시큐리티 라운드(security round)로 연결될 가능성이 점점 커지고 있다는 우려가 제기되고 있다. 현재(2003년 6월) 이 CCRA에 서명한 파트너 국가는 16개국(호주와 뉴질랜드, 오스트리아, 캐나다, 핀란드, 프랑스, 독일, 그리스, 이스라엘, 이태리, 네덜란드, 노르웨이, 스페인, 스웨덴, 영국, 미국)으로서 관련 기관 그리고 기관의 홈페이지는 공통평가기준 홈페이지 "http://www.commoncriteria.org/"에 자세히 설명되어 있다.

CC는 관련 내용에 따라 크게 3부분으로 나누어 볼 수 있다. 첫 번째 CC Part1에서는 CC의 소개 및 일반적인 개요사항을 다루고 있고 Part2에는 기본적으로 요구되는 보안 기능사항을 CC Part3은 보안 보증 요구사항을 다루고 있다. 분야별로 이용자, 평가자 그룹간의 적용 내용이 다르며 사용자, 개발자의 기술적 원리와 가이드 자료 역시 목적에 따라 차이가 존재한다. 다음 내용은 CC Part와 이용자 그룹과의 관계를 보여 준다[1].

- CC Part1 : CC의 일반적 개념 및 원칙에 대한 소개 부분
  - 사용자 : 기본 정보와 참고 목적을 위한 사용 및 PP를 위한 가이드 구조
  - 개발자 : 요구사항 개발과 TOE(Target of Evaluation)을 위한 보안규격을 표준화하기 위한 기본 정보 및 참고를 위한 사용
  - 평가자 : 배경 정보와 참고 목적을 위한 사용 및 PP와 ST를 위한 가이드 구조

- CC Part2 : 보안기능 요구 사항을 표현하는 표준 방법 설명
  - 사용자 : 보안기능의 요구사항 진술을 공식화 할 때 가이드와 참고를 위한 사용
  - 개발자 : 기능요구사항의 진술을 해석하고 TOE를 위한 기능 규격을 공식화할 때 참고를 위한 사용
  - 평가자 : TOE가 주장하는 기능이 있는지 여부를 결정할 때 평가기준의 필수 진술로서 사용

- CC Part3 : 보안보증 요구 사항을 표현하는 표준 방법 설명
  - 사용자 : 보증의 요구레벨을 결정할 때 가이드를 위한 사용
  - 개발자 : 보증요구사항의 진술 해석과 TOE를 위한 보증 접근법을 결정할 때 참고를 위한 사용
  - 평가자 : TOE의 보증을 결정할 때와 PP와 ST를 평가할 때 평가기준의 필수 진술로서 사용

이와 같이 CC는 3가지 파트로 분류되고 분야별 이용자 그룹 역시 3가지 부분으로 나누어지기 때문에 CC의 분야별 기술적 원리 자료 및 가이드 문서가 다른 만큼 CC 이용자 그룹들에게도 서로 다른 흥미로 제공되게 된다.

현재 개발자들과 평가자들의 역동적인 활동으로 인해 가장 단순한 제품과 다른 어떠한 제품들의 공식적인 분석을 위한 최신 기술을 제시하는 것은 상당히 어려워지고 있다. 이에 따라 사용자 및 기타

개발자 및 평가자들의 대한 교육 활동 역시 상세하고 분야별로 특수화된 접근을 하지 못한다면 CC에 대한 이해가 난해해질 수밖에 없다. 국제간 대표적 교육 활동 중 캐나다는 위 사항에 적합하도록 청취 대상을 세분화하여 CC 교육에 참여하고 있는 반면 미국, 독일, 그리고 영국 같은 경우에는 피교육자 대상을 구분하지 않고 있는 추세이다. 앞으로 이와 같은 교육에 대한 세부 사항을 대표적인 국가 캐나다, 미국, 네덜란드, 독일, 그리고 영국별로 나누어 검토해 보고 CCRA의 기준에 준수하여 평가되고 검증된 미국연방정부의 정보보호 제품들을 살펴보기로 한다.

1. 캐나다

캐나다의 대표적인 CC 교육기관은 CSE(Communication Security Establishment)의 한 부서인 ITS(Information Technology Security) 교육센터이다. ITS 교육센터의 교육 목표는 캐나다의 정보 시스템 보안을 향상시키고, 전문가와 프로그램 관리자, 각 기관의 공무원들의 질적 향상을 통해 캐나다의 IT 분야 발전을 도모하는데 있다. 교육 과정은 정해진 과정과 직접 선택 할 수 있는 과정으로 이루어져 있으며 각 교육과정의 필요한 준비사항이 설명되어 있다. CSE ITS 교육센터의 다양한 교육 분야는 일반적인 IT 보안, 네트워크 리스크 관리, 암호학, 공개키 기반구조, 캐나다의 공통평가기준 기술 분야이고, 이 다섯 분야를 중심으로 [표 1]과 같이 좀더 세부적인 교육과정으로 나누어져 있다[4].

1.1 '암호키의 개념과 절차' 과정

이 과정의 목표는 CSE에서 CCF(Canadian Central Facility)에 의해 제공되는 다양한 키타입, 키 요구 절차와 다른 서비스들의 개념을 배우고 발견하는데 목표를 두고 있다. 교육 과정의 개요로는 GoC (Government of Canada) 전자 키관리 시스템의 개요, 키의 개념과 키의 형태들, 정부의 안정한 네트워크 키관리 시스템(Government Secure Telephone Network Key Management System)에서 나온 보고서, 규칙과 책임의 내용을 다루고 있다. 교육 대상으로는 COMSEC(Communication Security)의 관리자들과 키관리를 수행하는 정부 기관의 대표자들로 하고 있다. 또한, 공무원에 한해서 교육을 받을 수 있는 제한이 따르고 있다.

[표 1] ITS 교육센터의 교육소개

과정 넘버	교육 과정 이름	선행조건	등급	기간	비용	
					공무원	비공무원
1	암호키의 개념과 절차	COMSEC계정필요	중급	1일	$180	N/A
2	Motorola의 STU-III 사용법	없음	중급	1일	$180	N/A
3	AT&T의 STU-III 사용법	없음	중급	1일	$180	N/A
4	COMSEC 관리자 교육	1과정 이수와 COMSEC계정필요	중급	2일	$290	N/A
5	데이터 전송 장비 사용법	없음	중급	2일	$290	N/A
6	ITS의 소개	없음	초급	2일	$530	$660
7	네트워크 리스크 관리	5과정이나 이에 대등한 조건	중급	3일	$660	$790
8	암호학의 소개와 응용	5과정이나 이에 대등한 조건	초급 중급	1일	$370	$470
9	안전한 전자상거래 정부: 구조	5,6,7과정이나 이에 대등한 조건	중급 고급	2일	$530	$660
10	안전한 전자상거래 정부:실용적인 관점	없음	초급 중급	1/2일	$250	$320
11	전자상거래 정부에서 상호인증 이론과 방법	5,6,7,8과정이나 이에 대등한 조건	고급	3일	$660	$790
12	평가인증등급 - 1	보증된 IT 보안 전문가	고급	2일	N/A	$150
13	평가인증등급 - 4	EAL-1시험을 통과하고, 평가 경험이 증명되어야 함	고급	5일	N/A	$275
14	보호프로파일과 보안목표명세서	6,7,8과정이나 이에 대등한 조건	중급	2일반	$660	$790
15	보증인/개발자를 위한 CC	6,7,8과정이나 이에 대등한 조건	중급	1일	$370	$470

1.2 'Motorola, AT&T의 STU-Ⅲ 사용법' 과정

이 과정의 목표는 Motorola, AT&T의 STU-Ⅲ 사용법을 배우고, 각 기관에서 STU-Ⅲ을 다른 사용자들에게 가르치기 위한 충분한 지식을 배우는데 있다. 교육 과정의 개요로는 Motorola STU-Ⅲ Sectel 1500 또는 AT&T STU-Ⅲ 1100의 설치 방법, Motorola나 AT&T STU-Ⅲ의 프로그램 사용법, Motorola나 AT&T STU-Ⅲ의 작동법, 안전한 접근제어시스템(Secure Access Control System) 사용하는 방법과 구성방법의 내용을 다루고 있다. 교육 대상으로는 GoC 부서들과 기관의 대표자들로 하고 있다. 또한, 공무원에 한해서 교육을 받을 수 있는 제한이 따르고 있다.

1.3 COMSEC 관리자 교육

이 과정의 목표는 COMSEC 관리자의 의무를 수행하기 위해서 필요한 기술과 지식을 개발하고 발전하는데 있다. 교육 과정의 개요로는 COMSEC 환경의 인식, COMSEC 용어, 지침 그리고 진행과정, 개인적 관리의 의무와 책임, COMSEC 구체적인 회계와 통제과정을 다루고 있다. 교육 대상으로는 COMSEC 기관에 임명되거나 COMSEC 관리자들이나 차후에 관리자가 될 GoC 부서나 각 기관의 대표자들, 흥미를 가지고 있는 대표자들로 하고 있다. 또한 공무원에 한해서 교육을 받을 수 있는 제한이 따르고 있다.

1.4 데이터 전송 장비(DTD)의 사용법

GoC EKMS(GoC Electronic Key Management System)의 대부분으로, DTD(Data Transfer Device)는 시스템의 독특한 저장/로딩 장비와 하드복사 시 키요청과 연관된 공통 장비들을 제거하기 위하여 설계되어졌다. 이 과정에서는 DTD의 개념을 배우고 개발하는데 있다. 교육 과정의 개요로는 GoC EKMS의 개요, DTD의 기능, DTD의 응용을 다루고 있다. 교육 대상으로는 GoC 부서들과 기관들의 대표자로 하고 있으며, 공무원에 한해서 교육을 받을 수 있는 제한이 따르고 있다.

1.5 ITS의 소개

이 과정에서는 ITS의 원칙과 기본적인 개념을 응용하고 이해하려는 관련자들에게 도움을 주고, 캐나다 정부의 현재와 미래의 ITS 독창성을 고수하는데 목적이 있다. 교육 과정의 개요로는 ITS의 기본 개념, 캐나다 정부의 보안정책의 범위와 목적, 평가와 관리의 취약성 소개, 취약점에 대한 증거, ITS 원리와 원칙(암호학 개요와 키관리, 안전한 통신프로토콜, 무선네트워크 보안, 방화벽 응용, 침입탐지시스템의 전반적인 개요), 평가되고 유용한 IT 제품들 소개, PKI와 같은 현재와 미래의 ITS 독창성을 다루고 있다. 교육 대상으로는 사용자에게 제품에 대한 설명자나 IT 시스템 관리자, ITS 교육에 관심이 있는 개인을 대상으로 하고 있다. 공무원과 비공무원 모두 교육을 받을 수 있다.

1.6 네트워크 리스크 관리

이 과정의 목표는 표준 네트워크 컴포넌트의 많은 연구와 문제되는 환경과 관리방법을 실제적인 연습을 통하여서 체계적으로 보강하는데 목표를 두고 있다. 교육 과정의 개요로는 문제되는 평가(이론과 실습), IT 네트워크의 본질(OSI 모델, 프로토콜과 IPv4/IPv6의 차이), 취약한 에이전트(설명서, 데모와 탐지), 보호물(설명서, 취약점에 대한 통계, IDS 데모), 세밀한 방어(설치된 보안구조), 무선네트워크 보안, 차후 연구를 다루고 있다. 교육 대상으로는 네트워크의 기본을 배우려는 네트워크 설계자, 구현자, 관리자나 보수자를 대상으로 하고 있다. 공무원과 비공무원 모두 교육을 받을 수 있다.

1.7 암호학의 소개와 응용

이 과정의 목표는 암호학의 기본 개념과 키관리 시스템, 암호학이 정보보호에 사용되는 방법에 대한 증명을 교육하는데 목표를 두고 있다. 교육 과정의 개요로는 암호학의 역사, 왜 암호학이 필요한가?, 개인키와 공개키를 포함한 암호학의 기본적인 개념, 공통 알고리듬의 연구, 키관리 시스템의 현재와 미래, 암호학의 응용(이메일, 전화, 전자서명), 이용 가능한 시스템과 사용법, PKI의 개요를 다루고 있다. 교육 대상으로는 ITS의 기본지식을 가지고 있는 IT분야 종사자를 대상으로 하고 있으며, 공무원과 비공무원 모두 교육 받을 수 있다.

1.8 안전한 전자상거래 정부 - 구조

이 과정의 목표는 GoC PKI의 원리와 개념을 이해하려는 관련자들을 위한 과정으로 다양한 보안서비스와 구조 그리고 GoC PKI의 장점을 증명하는데 목표를 두고 있다. 교육 과정의 개요로는 기반구조(정책관리기관, 캐나다 연방기관 등), GoC PKI의 세부적인

구조, 위탁 시 수반되는 부속물(VPN, 인증서비스, 권한관리기반구조 제품), PKI의 네트워크구조(방화벽 역할/군사지역(DMZ)/디렉토리), X.500, 상호인증, 체인/숨긴 디렉토리, 계층형 디렉토리 정보(DIT)/스키마, PMI(Privilege Management Infrastructure), 위탁 컨포넌트의 세부사항(접근시도(Get Access), 타임서버, 로밍서버), GOL 안전한 채널 PKI (등록과 enrolment, MBUN, RAP 등), 바른 패스워드, 공증서버, 부인방지, 사용자 처리사항/등록/교육(암호화와 전자서명을 사용하기 위해 수신자로부터 수신되어진 인증서의 위탁제품 설명), 유지를 위한 요구사항과 문서, 공통문제와 결점, 높은 가용성과 복원 계획들을 다루고 있다. 교육 대상으로는 시스템 보수나 관리자, 보안 업체로 하고 있으며, 공무원과 비공무원 모두 교육 받을 수 있다.

1.9 안전한 전자상거래 정부 - 실용적인 관점

이 과정의 목표는 GoC PKI의 실행 전망을 공개적인 토론 과정으로 다음의 질문과 답변을 통해 프로그램 관리자와 실행관리자의 능력을 향상시키는데 목적을 두고 있다. 질문으로는 PKI는 무엇인가?, PKI를 누가 사용하는가?, GoC는 PKI를 어떻게 구현하기 시작하였는가?, 이것을 어떻게 사용하여야 서비스전송에 유용한가? 등이다. 교육 과정의 개요로는 PKI의 역사, PKI 프로그램, 인증서 정책 문서와 인증업무준칙(CPS : Certification Practice Statement), 정책관리기관(PMA : Policy Management Authority) 기반구조, 관리 에이전트(MA : Management Agency), CCF(Canadian Central Facility), PKI의 선택 방법, 권한관리기반구조(PMI : Privilege Management Infrastructure), PKI 등록과 전자서비스 전달 프로그램 등록 제어와 프라이버시 이슈, 정부의 현재 사용현황, GoC PKI 구조의 문서들을 다루고 있다. 교육 대상으로는 전자서비스 전달 프로그램 관리자, 공개 섹터서비스 전달에 요구되는 실행관리자이고 공무원과 비공무원 모두 가능하다.

1.10 전자상거래 정부 - 상호인증 원리와 방법

이 과정의 목표는 다중 PKI 영역사이에서 상호운영성(Interoperability)을 유지하고 성취하는 방법을 세부적으로 이해시키고, GoC PKI와 상호인증을 통해 발전된 방법과 산업제어를 세부적인 예로 이해시키고, 다른 PKI 상호운영성 기술에 응용하는데 목적을 두고 있다. 교육 과정의 내용으로는 PKI 컴포넌트 (PKI 개요, X.509 공개키 인증서, 인증성 복구옵션, 상호운영성 관련, 신뢰된 모델), 저장 개요(프로토콜, 기술, 정보공유옵션), 상호인증과 상호인정을 포함한 영역사이에서 신뢰된 관계를 설립하기 위한 다양한 옵션, 규칙과 목적(인증업무준칙, PKI 공개준칙, 인증서 정책), GoC PKI 상호인증 방법과 기준, 위탁제품 스팩(배포판 5.0, 5.1과 6.0), 표준화와 상호운영성의 독창성, 확장되는 신뢰(GoC PKI), 상호인증의 사실적인 증명과 산업통제집행들을 다루고 있다. 교육 대상으로는 IT분야 관련자들과 이들을 상호운영 할 수 있는 PKI 기술을 검증하고 승인하는 사람들을 대상으로 하고 있다. 공무원과 비공무원 모두 교육 가능하다.

1.11 평가인증등급 - 1

이 교육 과정의 목표는 캐나다 공통평가기준과 인증 체계, ISO 15408 CC에 대하여 교육하는 데 있고, 3시간의 필기시험을 통하여서 관련자들을 EAL-1 (Evaluation Assurance Level-1) 등급의 평가자로 완벽히 만드는데 있다. 교육 대상으로는 EAL-1 평가를 실행하기 위해 인가된 평가 기관에 의하여 보증된 IT 전문가들로 공무원은 교육 대상자가 아니다.

1.12 평가인증등급 - 4

이 교육 과정은 전 과정 보다 평가자들의 평가레벨을 더 높이기 위한 과정으로, 현재 CC 평가 이슈를 포함한 전반적인 주제, 캐나다 CC의 평가 체계, 국제적인 발전을 목표로 하고 있다. 또한, 3시간의 필기시험을 통하여서 관련자들을 EAL-2에서 EAL-4 등급까지의 평가자로 완벽히 만드는데 있다. 교육 대상으로는 EAL-2에서 EAL-4 등급까지 평가를 실행하기 위해 인가된 평가기관에서 보증되고 경험이 있는 IT 전문가들로 공무원은 교육 대상자가 아니다.

1.13 보호프로파일과 보안목표명세서

이 교육 과정의 목표는 제품개발자들이 소비자들의 요구에 응답 할 수 있게 CC 포맷에 기술되어 있는 보호프로파일과, 개발자들이 제품의 보안 기능성을 표현하기 위한 보안목표명세서을 효과적으로 작성 할 수 있게 교육하는데 있다. 교육 과정의 개요로는 공통평가기준의 개요, 보호프로파일과 보안목표명세서의 내용과 목적, 효율적인 보호프로파일 작성법, 일반적인 보안목표명세서 작성법, 보호프로파일의 각각의 개념

을 돕기 위한 예와 보안목표명세서에 쓰이는 과정을 다루고 있다. 교육 대상으로는 IT 보안 제품의 개발자와 소비자들이고, 공무원과 비공무원 모두 교육 가능하다.

1.14 보증인/개발자를 위한 CC

이 교육 과정의 목표는 CC 개요 관련사항과 평가과정을 자세히 교육하고, 캐나다의 CC 평가와 인증서 작성을 통하여 보증인과 개발자의 가이드라인을 교육하고, 이런 원리들이 세계의 다른 CC 평가 기술에 이용되는 과정을 교육하는데 목적이 있다. 교육 과정의 내용으로는 공통평가기준의 개요, 평가과정에서의 역할과 책임의 정의, 개발자가 준비해야 할 다양한 문서에 대한 설명, 평가과정의 설명을 다루고 있다. 교육 대상으로는 IT 보안 제품의 보증인, 제조업자, 개발자들이고, 공무원과 비공무원 모두 교육 가능하다.

2. 미국

미국의 대표적인 CC 교육기관은 COACT사와 Decisive Analytics사가 교육 프로그램을 운영하고 있다. 대부분의 교육과정이 공통평가기준과 IT 습득정책의 중요성에 대해서 소수의 IT 전문가들만을 대상으로 교육했는데, COACT사는 일련의 교육 과정을 통해서 IT 분야의 노련한 전문가뿐만 아니라 미숙한 사람들에게도 교육 과정을 통해서 공통평가기준에 대한 소개와 개요, 용어를 간파하고 맡은 분야의 업무를 수월하게 도와주도록 운영하고 있다. Decisive Analytics사는 공통평가기준 개념과 실제적인 응용을 통해서 IT 제품과 시스템의 보안 적합성을 판단 할 수 있도록 도와주고, 요즘 일반화된 시스템 보안 기술과 검증 과정을 광범위하고 다양한 응용 상황을 통해 교육함으로 개인적으로 충분한 관리와 기술적인 역할을 할 수 있는 것을 교육의 목표로 하고 있다[5,6].

2.1 COACT의 교육 과정

COACT의 교육 과정은 다음과 같이 CC의 역사, CC의 주요사항 설명, 보호프로파일, 보안목표명세서, CC 평가 체계의 개요, 역할과 책임, IT 보안 평가, 공통평가기준 인증서, 인증서 관리 프로그램(Certificate of Maintenance Program)으로 이루어졌다[5].

2.1.1 CC의 역사

- 유럽인의 업적, IT 보안 역사, 후원 기관

2.1.2 CC의 주요사항 설명

- 평가대상
- 보안 요구사항과 보증 요구사항
- 기능적 요구사항 - 클래스
- 보증 요구사항 - 클래스
- 보안 기능사항 - 패밀리
- 보안 기능, 컴포넌트
- 컴포넌트 신원증명, 정의

2.1.3 보호프로파일

- 보호프로파일 요구사항
- 신원증명, 개요, 평가대상 체계, 평가대상 보안 환경
- 보안 목적, 평가대상 보안 요구
- IT 환경과 Non-IT환경을 위한 보안 요구사항, 공통 상황
- 응용의 중요성, 이론적 해석

2.1.4 보안목표명세서

- 보안 목표 명세서 요구사항
- 신원증명, 개요, 평가대상 체계, 평가대상 보안 환경
- 보안목표명세서 규격
- 평가대상 요약 명세
- 보호프로파일 요구 진술
- 평가대상 요약 명세서의 이론적 해석
- 보호프로파일 요구의 이론적 해석

2.1.5 CC 평가 체계의 개요

- 참여자, 인증기관, 평가기관

2.1.6 역할과 책임

- 평가기관을 위한 가이드라인
- 검증기관을 위한 가이드라인
- 고객을 위한 가이드라인

2.1.7 IT 보안 평가

- IT 보안 평가를 위한 준비
- 사전 활동
- 자문 활동
- 보안 목표 명세서
- 실행 가능성
- 평가를 위한 준비사항
- 평가 돌입
- IT 보안 평가의 수행
- 평가의 수행과 결론

2.1.8 인증서 관리 프로그램

- 개요
- 보증 관리 패러다임
- CMP 적용
- 평가대상 승인
- 평가대상 모니터링
- 평가대상 재평가
- 보증 활동을 위한 CCTL(Common Criteria Testing Laboratory) 선택

2.2 Decisive Analytics의 교육 과정

Decisive Analytics의 교육 과정은 시스템 생명주기 활동을 지원하는 데 있어서 CC의 적용을 이해하기 위한 기본으로써 CC의 개념을 이해하는 것에 초점을 맞추고 있다. 이 교육 과정은 3일 이상의 기간 동안 진행되고 발표, 연습과 열린 토론을 통해 질문과 답변의 상호-교환적인 토론으로 진행되며, 시스템 보안에 대한 개인적으로 충분한 관리와 기술적인 역할을 할 수 있도록 도와 줄 것이다. 교육 내용은 다음과 같다[6].

- 시스템/보안 기술과 시스템 개발
- 시스템/제품 파악
- 시스템/제품 통합과 유효성(정형화된 평가, 검증& 용인, 승인 평가)

2.3 NSA의 우수 교육센터

NSA(National Security Agency)에서는 다양한 학문 분야에서 정보 보증 전문가의 수요에 대처하기 위하여 '정보보증 분야의 우수 교육센터' 지원 프로그램을 마련하고, 이를 기초로 1999년 5월부터 시작하여 2002년 8월까지 미국 36개 대학을 정보 보증과 관련된 우수 교육센터로 지정하였다. NSA는 각 대학으로부터 신청을 받아서 NSTISSC(National Security Telecommunications and Information Systems Security Committee)에 의해 마련된 교육 표준에 기초한 공개 기준을 만족하는지에 대한 엄격한 심사를 수행하고, 36개 대학을 교육센터로 지정하였다. 우수 교육센터는 보안 전문가를 채용하기 위한 구심점이 될 것이며, 정보 보증 분야의 연구를 촉진시키는 환경을 마련할 것으로 기대하고 있다. 매년 새로 지정되는 교육센터가 매년 열리는 정보 시스템 및 보안 교육 전문가 회의의 수여식을 통하여 승인될 것이다. 이 전문가 회의에서는 정보보증 교육에 대한 현재와 미래의 요구사항이 무엇인지를 집중적으로 파악하고 대학과 대학원에 관련 교과과정의 개발과 확장을 격려하기 위하여 정부, 산업체, 대학의 주요 공무원을 위한 토론장을 제공한다. NSA에서는 학생들을 위한 장학제도를 마련하고 있어 미국 시민이고 나이가 18세 이상이며 학교에서 추천을 받은 대학 3,4학년과 대학원 석·박사 학생들에게 장학금을 지급하고 있다. 36개의 정보보증 분야의 우수 교육센터는 [표 2]와 같다[7].

3. 네덜란드

네덜란드의 대표적인 교육 센터로는 TNO-ITSEF (Information Technology Security Evaluation Facility)이다. TNO-ITSEF의 CC 교육과정은 다음과 같은 3가지의 주된 과정을 통해서 교육을 하고 있으며, 특별한 개발자들을 대상으로 보다 전문화된 평가 교육을 실시하고 있다. 평가의 세부적인 개요에서 특별한 평가보증등급을 사용하기 위함과 공통평가기준을 어떻게 적합한지 보고, 어떻게 개발과정에 사용할 수 있는지를 교육하고 있다[8].

- 소개 과정 : 이 과정은 공통평가기준의 기본적인 개요와 개념을 소개하고, 보안 지식은 있지만 공통평가기준의 경험이 없는 사람들을 대상으로 1/2~1일 과정이다.
- 개발 과정 : 이 과정은 개발자들로부터 공통평가기준에 요구사항을 교육하고, 보호의 지식은 있지만 공통평가기준의 경험이 없는 개발자들을 대상으로 1~2일 과정이다.
- 전문가 과정 : 이 과정은 공통평가기준의 한 영역 또는 그 이상의 영역 지식 레벨을 교육받은 자로써 교육자들의 기본적인 높은 레벨에 맞추어서 2일이나 그 이상의 과정으로 교육하고 있다.

3.1 소개 과정

- 일반적인 컴퓨터 보안과 공통평가기준의 역할

이 과정은 다음과 같은 질문으로 이루어져 있다. 불안전한 컴퓨터 제품은 무엇인가?, 왜 컴퓨터 제품이 불안전한가?, 공통평가기준은 이것에 적합한가? 그리고 평가된 제품의 가치는 무엇인가?

- 보안 대상과 보호프로파일

이 과정은 다음과 같은 질문으로 이루어져 있다. 이것들은 무엇인가?, 왜 중요한가? 그리고 이것을 한번

〔표 2〕 미국 NSA의 정보보증 분야의 우수 교육센터

	교육센터	URL
1	Air Force Institute of Technology	http://www.afit.edu/
2	Carnegie Mellon University	http://www.heinz.cmu.edu/infosecurity/
3	Drexel University	http://www.ece.drexel.edu/
4	Florida State University	http://www.cs.fsu.edu/infosec/
5	George Mason University	http://www.isse.gmu.edu/~csis/index.html
6	George Washington University	http://www.seas.gwu.edu/%7Einfosec/
7	Georgia Institute of Technology	http://www.cc.gatech.edu/
8	Idaho State University	http://security.isu.edu/
9	Indiana University of Pennsylvania	http://www.iup.edu/
10	Information Resources Management College of the National Defense University	http://www.ndu.edu/irmc/
11	Iowa State University	http://www.issl.org/
12	James Madison University	http://www.infosec.jmu.edu/
13	Mississippi State University	http://www.cs.msstate.edu/~security/
14	Naval Postgraduate School	http://cisr.nps.navy.mil/
15	New Mexico Tech	http://www.cs.nmt.edu/page_home.html
16	North Carolina State University	http://ecommerce.ncsu.edu/infosec/
17	Northeastern University	http://www.northeastern.edu/
18	Norwich University	http://www.norwich.edu/biz/cs/
19	Polytechnic	http://www.poly.edu/
20	Purdue University	http://www.cerias.purdue.edu/
21	Stanford University	http://crypto.stanford.edu/seclab/
22	State University of New York, Buffalo	http://www.cse.buffalo.edu/caeiae/
23	State University of New York, Stony Brook	http://www.sunysb.edu/
24	Syracuse University	http://www.csa.syr.edu/
25	Towson University	http://www.towson.edu/CAIT/HomePage/Welcome.html
26	University of California at Davis	http://seclab.cs.ucdavis.edu/
27	University of Idaho	http://www.csds.uidaho.edu/
28	University of Illinois at Urbana-Champaign	http://ciae.cs.uiuc.edu/
29	University of Maryland, Baltimore County	http://www.cisa.umbc.edu/
30	University of Maryland, University College	http://www.umuc.edu/
31	University of Nebraska at Omaha	http://nucia.ist.unomaha.edu/
32	University of North Carolina, Charlotte	http://www.sis.uncc.edu/LIISP/
33	University of Texas, San Antonio	http://www.utsa.edu/
34	University of Tulsa	http://www.cis.utulsa.edu/
35	U.S. Military Academy, West Point	http://www.itoc.usma.edu/
36	West Virginia University	http://www.lcsee.cemr.wvu.edu/

읽었을 때 무엇을 중요하게 기억해야하는가?

- 평가의 일반적인 개요

이 과정은 평가하는 동안에 실제적으로 무엇이 발생하는 지에 대한 개요를 제공한다. 일반적인 양상(설명되는 부분)뿐만 아니라 특별한 양상(평가되는 과정)도 다루고 있다.

3.2 개발자 과정

· 공통평가기준에서의 개발자의 역할

이 과정은 공통평가기준 평가를 받을 때 개발자로부터 요구되어지는 사항을 다룬다. 그들이 무엇을 기대할 수 있는가?, 무엇을 가져야만 하는가?

· 보안 목표 명세서와 보호프로파일

이 과정은 다음의 기본적인 질문을 다룬다. 이것들은 무엇인가? 그리고 우리에게 무엇이 중요한가? 이것을 어떻게 쓰는가? 그리고 이들을 사용하여 평가하는 동안 접하게 되는 어려움은 무엇인가?

· 평가의 세부적인 개요

이 과정은 실행 가능성과 관계된 세부적인 평가를 다루고 이들의 가능성에 요구되는 항목들과 어떻게 평가되는지 교육하고 있다.

· 평가와 개발과정

공통평가기준의 대한 개발 과정에서 공통평가기준에 요구되는 통합 과정으로 어떻게 개발 과정에서 최소의 시간과 최소의 노력으로 생산할 수 있는가?

3.3 전문가 과정

· 보안 목표명세서와 보호프로파일의 활용

이 과정에서는 보안문제를 확실히 해결하고 평가기준에 맞게 보호프로파일/보안 목표명세서를 올바르게 사용 할 수 있는 방법과 보호프로파일이나 보안 목표명세서의 예를 통해 교육한다. 또한, 요구 사항이 다른 그룹을 위해 보호프로파일은 어떻게 쓸 것이며, 보호프로파일/보안 목표명세서는 제품 개발과정에 어떻게 사용되는가? 를 다룬다.

· 보안 대상과 보호프로파일의 평가

이 과정에서는 공통평가기준에 의해 요구되는 모든 사항을 교육하고 보안 대상이나 보호프로파일은 무엇을 보고 어떻게 평가되며 제품 개발자와 제품 구매자를 위한 평가자의 역할을 교육하고 있다.

· 평가 제품들

이 과정에서는 공통평가기준에 의해 평가되는 제품들은 무엇을 보고 어떻게 평가되고 제품과 평가대상의 다른 점은 무엇인지를 교육하고 있다. 또한, 제품 개발자의 역할을 자세히 교육하고 있다.

4. 독일

독일의 대표적인 교육 센터로는 @SEC Information Security GmbH이다. @SEC은 기업과 기관을 위한 IT 보안의 특별하고 독자적인 매각 회사이다. 질 높은 상담 서비스와 무결성을 통해 고객과의 신뢰된 관계를 유지하며 고객의 최고 이익을 위해 일하고 있다. @SEC 컨설턴트는 국제적인 컨퍼런스와 워크샵을 통해 발표 훈련을 가지며, 고객들은 상담 서비스와 연결하여 교육 받는다. 이 곳의 교육과정과 연습과정은 온라인으로도 제공하고 있으며, 시스템, 응용, 기관에서 보안 기능을 병행해서 이용할 수 있는 실제적인 예로 교육하고 있다. 교육 과정은 다음과 같다[9].

· 운영체제 보안

Window NT, Linux and Unix 등 특별한 운영체제 보안 기능과 특징, 안전 시스템 구성, 추가적인 보안 제품들, 보안 기능의 관리, 함정과 취약점들.

· 방화벽

인터넷을 통한 보안 위험, 인터넷을 통한 시스템 침입방법, 방화벽의 성능, 방화벽 구조의 장단점, 방화벽 시스템의 구성, 방화벽 시스템의 관리, 추가적인 보안 수단, 가상사설망, 방화벽을 사용한 안전한 인증.

· PKI와 안전한 전자상거래

PKI의 정의, PKI 시스템의 구조, 증명서 프로파일, 인증서 관리(복호 방법), 디렉토리 서비스, PKI 제품의 예와 그것들의 특징, 공개키의 암호화를 기반으로 하는 암호화 프로토콜, 회사 안에서 PKI의 사용, 전자상거래 응용 안에서 PKI의 사용.

· ISO/IEC 17799 - 정보보안관리

정보보안관리의 정의, 방법기술의 위험, ISO17799, 정식으로 알려진 BS7799, 그리고 관련된 표준, 기관으로써 정보보안관리의 설립, ISO117799 과정과 인증.

· 암호 응용

암호의 기초, 실무 처리에서 암호의 사용, 암호의 표준과 프로토콜, 암호 사용의 취약점들, 암호 라이브러리들, CDSA, 그리고 Microsoft CryptoAPI.

· 인터넷과 웹 보안

보안 연결의 설정, 여러분의 통신파트너의 인증과정,

Java 보안, JavaScript, ActiveX, CGI-Scripts, ASP, 새로운 인터넷 프로토콜과 구조(IPv6, SSL, S/MIME, PKIX)

5. 영국

공통평가기준은 보안제품과 시스템, 서비스의 평가와 설명서를 다룬 새로운 국제표준(ISO 15408:1999)이다. CC의 사용에 있어 장점을 이해하고 CC의 접근과 개념을 충분히 이해하는 것은 기본적인 것이다. 영국의 대표적인 교육 센터인 Syntegra는 세계에서 CC교육의 가장 많은 경험을 가지고 있고, CLEF (Common Criteria Testing Laboratory)는 상용 보안평가 설비를 갖추어진 가장 오래된 곳 중에 하나이다.

CC는 많은 분량과 복잡한 표준이며 효과적으로 사용하기 위해서는 많은 경험과 이해가 요구된다. CC교육에 대한 투자 없이 CC의 개념을 올바르게 응용하기는 힘들고, 일을 처리한 후에 수정하기에는 더 많은 대가가 초래된다. Syntegra의 교육과정은 다음과 같다[10].

- CC의 개요와 기본적인 개념 및 기본적인 요구사항
- 보증요구사항
- 보호프로파일과 보안목표명세서
- 평가대상 개발
- 지침서의 안내
- 개발 환경(관리구조, 전송과 운영, 생명주기)
- 기본적인 테스트 및 보증의 취약점
- 인증서의 유지
- 운영되는 평가기술 및 적합한 시스템

이 교육 과정은 예증, 그룹과 개인적인 연습, 그리고 테스트를 통해 진행되며 실무적인 업무를 중심으로 이루어지고 있다.

6. 평가된 정보보호 제품분석

다음 제품들은 NIAP(National Information Assurance Partnership) 공통기준평가 및 검증 기법과 CCRA의 기준에 준수하여 평가되고 검증된 제품들이다. 목록상의 제품들은 미국 또는 IT 보안 평가를 위한 공통 기준에 순응하기 위하여 CCRA에 참여한 국가중에 한 나라에 존재하는 인가/허가된 시설에서 평가되고 인가되었다.

IT 제품들을 위하여 발행된 공통 기준 인증서는 이 제품의 정해진 버전과 제품명(release)에 대해서만 적용된다. 인증서를 승인하고 효력을 주는 NIST, NSA, 또는 다른 조직들에 의해 주어지는 인증서는 IT 제품의 우수함을 보증하지는 않는다. 인증서는 그 제품이 CC 요구사항을 만족하는 검증을 성공적으로 완료했음을 의미한다[3].

6.1 정보보호 제품군 및 제품 유형

검증된 제품들의 목록은 NIAP-CCEVS(Common Criteria Evaluation and Validation Scheme)로 평가된 제품들과 요구되는 평가 자료(ST와 최종 평가 보고서)를 제공했던 다른 나라의 기법에서 평가된 제품들로 구성된다. CCRA에 의한 이 중요한 요약 문서는 평가 팀에 의하여 이루어진 판정이 완전한 것이고 일관된 것이라는 것을 확신하기 위한 정보와 수행된 검증 활동들, 그리고 평가의 결과를 보여주도록 설계되었다.

검증된 제품들의 확장된 목록은 http://www.commoncriteria.org 웹 사이트에 가면 구할 수 있을 것이다. 이 웹사이트는 CC의 국제적인 사용자를 위한 정보 역할을 한다. 다음 〔표 3〕의 정보보호 제품군 구분은 미국 연방 정부가 마련한 PP의 존재에 따라서 구분한 것이다.

〔표 3〕 미국연방정부의 정보보호 제품군

네트워크 인프라 정보보호 제품군	• 스위치/라우터 • 라우터 • 무선 LAN
네트워크간 정보보호 제품군	• 방화벽 • 가상사설망 • 원격 접근 • 이동 코드 • 다중 영역 솔루션 • 가드(guard)
컴퓨터 환경 정보보호 제품군	• 운영체제 • 바이오메트릭 • 보안 메신저 • 토큰 • 단일-레벨 서버 • 민감한 데이터 보호 • 신뢰된 데이터베이스 관리 시스템 • PC 접근 제어 • 주변장치 공유 스위치 • 기타
인프라 지원 정보보호 제품군	• 망관리 • 키복구 • 스마트 카드 • PKI/PMI • 침입탐지시스템 • 기타

〔표 3〕에서 제품 유형의 기술 범주를 위한 검증된 미국 정부 드래프트 PP가 이용 가능하지만 이 기술 범주 내에 존재하는 모든 개개의 제품들이 반드시 PP를 만족한다고 추론할 수는 없다. 드래프트 PP들은 여러 개발 단계에 존재하고 쓰여지고 있거나, 검토되거나, NIAP CCEVS CCTL(Common Criteria Testing Laboratory)에서 평가중에 있다.

6.1.1 네트워크 인프라 정보보호 제품군

네트워크 인프라 정보보호 제품군의 제품 설명은 〔표 4〕와 같다.

〔표 4〕 네트워크 인프라 정보보호 제품군

제품 유형	설 명	비 고
스위치/라우터	근거리통신망 구축시 단말기의 집선 장치로 이용되는 스위칭 기능을 가진 통신장비. 스위치와 라우터 기능을 동시에 수행하는 장치	
라우터	통신망 간을 연결해주는 장치로서, 한 통신망에서 오는 패킷을 수신하고, 패킷에 발신지 주소를 읽고 경로배정 테이블을 참고로 가장 적절한 통신로를 이용하여 다른 통신망으로 전송하는 장치	
무선 LAN	전파나 적외선 전송방식을 이용하는 근거리통신망(LAN)	

6.1.2 네트워크간 정보보호 제품군

네트워크간 정보보호 제품군의 제품 설명은 〔표 5〕와 같다.

6.1.3 컴퓨터 환경 정보보호 제품군

컴퓨터 환경 정보보호 제품군의 제품 설명은 〔표 6〕과 같다.

6.1.4 인프라 지원 정보보호 제품군

인프라 지원 정보보호 제품군의 제품 설명은 〔표 7〕과 같다.

7. 국내 교육 동향 및 평가 교육 체계 제안

7.1 우리 나라의 평가 교육 체계 및 운영

CC에 대한 국내의 대표적인 교육 기관은 한국정보보호진흥원(KISA: Korea Information Security Agency)이다. 국내에서는 정보화촉진기본법과 동법 시행령에 근거한 제품별 평가기준에 근거하여 침입차단시스템 및 침입탐지시스템 등 정보보호제품에 대한 평가를 1998년부터 시행하고 있으며, 2003년 6월 현재 기준 K4 체계 하에서 침입차단시스템 27개, 침입탐지시스템 17개에 대한 평가가 완료되었고, 침입차단시스템 5개, 침입탐지시스템 5개가 평가가 진행 중에 있다. 또한 새로운 CC 체계 하에서 3개 제품에 대한 평가를 진행 중에 있다. 이에 대한 자세한 사항은 KISA Homepage, http://www.kisa.or.kr를 참조하기 바람.

KISA 교육 과정의 목표는 "정보보호시스템 공통평가기준"(정통부 고시 2002-40호, 2002.8.5)을 적용한 보안성 평가를 위하여 기본적인 개념의 이해와 공통평가기준 기반 평가의 기본이 되는 보호프로파일 및 보안목표명세서에 대한 개념과 작성방법 등 실습을 통한 교육에 있다. 교육 대상으로는 IT 업체의 개발자와 각 기관의 보안담당자를 대상으로 교육하며, 2002년의 경우 년 5회에 걸쳐 최대 40명, 최소 10여명의 인원에 대하여 수행하고 있다. 교육과정은 다음과 같다[11][12].

- 국내/외 평가제도, CC 개념 및 도입 배경, CC Part1 소개

〔표 5〕 네트워크간 정보보호 제품군

제품 유형	설 명	비 고
방화벽	조직의 보안 정책을 지원하기 위하여 취약성 있는 서비스를 제한하고 특정 서비스로의 접근을 제어하기 위하여 네트워크 경계나 자국 호스트/서버 상에 배치됨	
가상사설망	공공 네트워크 상에 암호화된 터널을 생성함으로써, 이해 당사자간에 통신을 보호하거나 분리하는데 사용되는 기술	
원격 접근	원격 접근을 위한 기술	
이동코드	이동 코드상에 보안 정책 제한을 집행하는 기술. 이 제한은 경계가 있는 보안 솔루션 내에서 실현되거나 사용자 호스트 또는 서버 상에서 집행됨	
다중 영역 솔루션	다중의 보안 영역간의 안전한 데이터의 전송을 위한 기술	
가드	등급화된 네트워크에서 비등급화된 네트워크로 연결을 보호하기 위하여 사용됨. 고보증 방화벽과 유사하나, 높은 등급 데이터의 누설을 보호하기 위한 추가적인 기능을 가짐	

〔표 6〕 컴퓨터 환경 정보보호 제품군

제품 유형	설 명	비 고
운영체제	시스템 관리자나 사용자에 의하여 설정된 보안 정책을 실행하기 위하여 인증, 접근 제어, 데이터 구분, 감사 등의 보안 메카니즘을 제공하는 운영체제	
바이오메트릭	당신이 알고 있는 것에 당신이 가지고 있는 것을 부가하여 구현한 설비나 워크스테이션에게 강한 인증을 제공하는 기술. 바이오메트릭 능력은 지문, 장문, 얼굴 인식, 또는 망막 스캔 장치와 연관됨	
보안메신저	사용자 데이터를 위한 비밀성과 무결성 서비스를 제공하기 위한 인증, 서명, 암호 메카니즘을 제공하는 메신저 응용. 이 서비스는 공개된 키인증 기법을 사용하여 제공됨	
토큰	스마트카드를 포함하는 넓은 의미의 토큰으로 주로 크리덴셜 정보를 저장하는 수단을 제공함	
단일-레벨 서버	고수준의 네트워크를 사용하기 위하여 접근 제어, 감시 그리고 인증 및 데이터 암호 서비스를 제공하는 웹서버	
민감한 데이터 보호	데이터로의 비인가된 접근을 보호하기 위한 관리적, 기술적, 또는 물리적 조치들의 실현	
신뢰된 데이터베이스 관리 시스템	데이터베이스를 생성하고 유지하는 것과 데이터베이스를 사용하는 컴퓨터 프로그램의 수행을 지원하는 신뢰된 소프트웨어 시스템. 데이터베이스는 특정 목적을 위하여 요구되는 데이터의 집합이거나 시스템이나 프로젝트, 또는 기업에 기본이 되는 데이터의 집합	
PC 접근 제어	저장 장치로 데이터를 두거나 저장 장치로 데이터를 가져오기 위한 개별 또는 응용 프로그램의 권한을 정의하거나 제한하기 위하여 사용되는 기술. 정보 시스템의 자원으로의 접근을 인가된 사용자, 프로그램, 프로세스, 또는 다른 시스템으로만 제한하는 기술	
주변장치 공유 스위치	서로 다른 고수준의 네트워크 상에서 동작하는 두 개의 워크스테이션을 통한 통신을 위하여 사용자에게 하나의 주변장치를 사용 가능케 하는 신뢰된 전자 또는 물리 장치. 스위치는 두 개의 네트워크를 통하여 전달되는 데이터의 누설을 예방해야 함	

〔표 7〕 인프라 지원 정보보호 제품군

제품 유형	설 명	비 고
네트워크 관리	네트워크 사용 또는 접근을 거부하는 악의적인 공격으로부터 네트워크를 보호하기 위한 기술. 예를 들어, 네트워크 관리 센터로의 접근을 제어하기 위하거나 여러 종류의 공격으로부터 네트워크 관리 트랜잭션을 보호하기 위하여 사용되는 기술	
인증서 관리	암호학적 시스템의 사용자를 위한 공개키 인증서의 생성, 분배, 그리고 훼손 복구를 관리하기 위하여 사용되는 기술	
키복구	사용자의 개인키를 제삼의 위탁기관에 맡기고, 필요시 복구하는 기술	
스마트카드	사용자의 인증 크리덴셜을 안전하게 저장하고 이 크리덴셜(예를 들어, 공개키 재료의 비밀키 부분)의 사용과 접근을 제어하기 위하여 사용되는 작은 사용자 토큰	
공개키 기반구조	암호학적 제품 사용자에게 공개키와 키관리 서비스 설비를 관리하기 위하여 사용되는 기술, 설비, 사람, 그리고 절차의 집합을 나타냄	
침입탐지 시스템	비인가된 네트워크 침입이나 네트워크를 찾기 위하고 네트워크의 트래픽을 감시하기 위하여 네트워크 또는 사용자 호스트 상에 배치되는 장치	

- 용어 소개, 보호프로파일 및 보안목표명세서 개념 및 구성
- CC Part2, CC Part3 구성 설명, 국외 CC 평가 및 인증 예시
- 실습 : 보호프로파일 작성하기(보호프로파일 소개, TOE 설명, 응용 시 주의사항)
- CC ToolBox 소개, 보호프로파일 및 보안목표명세서 평가 클래스
- 실습 : 보안목표명세서 작성, 형상관리, 배포 및 운영, 생명주기지원
  - ACM_CAP.3, ACM_SCP.1 설명
  - ADO_DEL.1, ADO_IGS.1 설명
  - ALC_DVS.1 설명
- 실습 : 기능명세, 기본설계, 설명서, 시험서, 취약성분석

7.2 우리 나라의 평가 교육 현황, 문제점, 미래 환경, 대안 제안

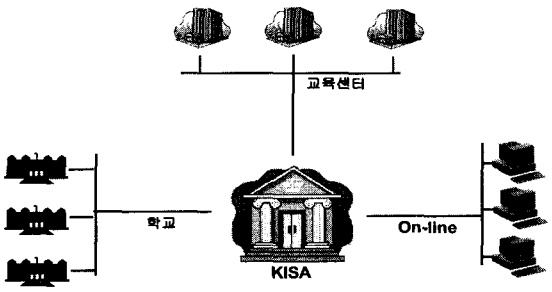
우리 나라는 현재 방화벽, VPN, 그리고 IDS 등과 같은 제품에 대한 평가를 시행하고 있고, 차후에 PKI 제품, 서버보안, 생체인식, 스마트카드 등과 같은 다양한 제품으로 평가를 확대할 예정이다. 현재 평가를 위한 교육은 KISA을 중심으로 개발자, 관리자, 그리고 평가자 위주로 시행중에 있다. 또한 우리 나라는 우리 개발업체의 능력, 평가기관의 능력, 평가 제품의 시장규모, 사용자의 요구사항을 고려하여 CCRA 가입 시기를 조절해야 할 필요성이 있다. CCRA 가입 시기는 국내외 산업 규모, 산업체에 대한 파급효과 등을 고려하여 결정되어야 하나, 무엇보다도 우리 개발자 및 평가자, 그리고 사용자에 대한 평가 체계의 이해와 평가 기술의 확보, 평가 방법의 개발, 그리고 평가 교육 개발이 선행되어야 함은 두말할 나위가 없다. 현재의 평가를 위한 교육 과정은 평가를 위한 일반적인 사항을 중심으로 마련되어 있다. 현재의 교육 대상자도 주로 개발자와 조직의 관리자를 중심으로 수행되고 있으며, 평가자에 대한 교육은 캐나다, 호주 등의 외국의 평가기관의 교육과정을 활용하고 있다.

그러나 우리는 앞으로 다가올 다양한 평가 환경을 고려하여 국내 정보보호 주요 주체간의 역할의 할당과 협력을 강화하고, 다양한 평가 기술의 개발과 이를 지원할 수 있는 교육체계의 마련이 요구되고 있는 시점이다. 또한 교육대상자도 사용자, 평가자, 그리고 개발자로 확대가 요구되며, 또한 앞으로 다양한 평가 제품을 고려한 전문화되고 세분화된 평가 교육 체계의 마련이 요구되고 있다. 또한 평가 교육은 다양한 분야에 대한 교육 필요성 대두, 평가 교육의 필요성 확대, 평가자에 대한 교육기회의 제공 등을 고려하여 KISA를 중심으로 한 체계를 상호 보완하여 대학의 인력 지원을 받는 새로운 평가 교육 체계의 구축이 요구되고 있다.

평가 교육은 기존의 방법대로 KISA를 중심으로 한 방법(방안 1)과 대학에 교육센터를 신설하여 KISA와 상호 보완적인 관계를 유도하는 체계(방안 2)로 대별될 수 있다.

첫 번째 방안의 장점은 평가 체계를 일원화할 수 있고, 평가와 교육을 상호 연동시킬 수 있으며, 평가기관으로써의 신뢰성 부여 가능, 전문성을 살린 교육 가능, 그리고 평가 사업의 일원화가 가능 하는 등의 장점이 있다. 이 방안의 단점은 평가자에 대한 교육 필요성, 대상 제품의 다양화와 세분화로 인한 교육 전담 인원의 추가 확보, 개발자의 평가 교육시의 활용이 불가능, 교육과 평가가 연계되어 평가의 공정성 확보의 문제점이 대두될 수 있는 등의 문제점을 해결해야 한다. 두 번째 방안의 장점은 대학 인력의 확보, 미래의 민간평가기관을 위한 토대 마련, 다양한 평가 제품을 고려한 특성화된 교육 가능, 개발자의 평가 교육으로의 활용, 그리고 대학의 평가 기술 개발의 자극 등의 다양한 이점이 있다. 두 번째 방안의 단점은 대학 인력의 평가에 대한 이해 부족, 평가 경험의 미흡, 평가를 위한 교육 인력의 미흡, 대학의 평가 교육 공간 마련과 시설의 미흡, 평가자 및 개발자의 대학에 대한 신뢰 부족, 대학 교수의 평가 교육에 대한 자발적 참여 부족 등 다양한 문제점을 해결해야 한다.

본 논문에서는 두 번째 방안의 단점을 고려했음에도 불구하고 앞으로의 다양한 평가 제품의 교육 필요성 확보, 대학 정보보호 인력의 활용, 그리고 민간 평가기관의 토대마련, 개발자의 활용, 그리고 평가 교육의 다양화와 전문화 등을 고려하여 국내 평가 교육을 위하여 두 번째 방안의 채택을 제안하며, 이를 위한 평가 교육 체계와 교과과정을 중심으로 제시한다. 이 방안은 앞으로 다가올 다양한 제품 평가 요구, 세분화되고 전문화된 평가 교육의 확보 등의 교육 평가 수요에 능동적으로 대처할 수 있는 장점이 있다. 이를 위하여 구체적으로 주요 거점 대학에 특성화된 평가를 위한 교육센터의 신설 지정하고, KISA와 상호 보완적인 평가 교육체계를 구축하는 방안이다. 이 교육센터는 연구 기능과 평가 기술과의 상이, 대학 인력의 활용 기회 확대, 지방화 시대에 대비한 정보보호 거점 대학의 다양화 등을 고려하여 기존의 ITRC 센터와 독립적으로 운영하는 것이 요구된다. 여기서 ITRC에 이 교육 기능의 부여도 고려될 수 있으나, 추가의 재원 마련, 연구 기능과 평가 교육 기능과의 상이성, ITRC 참여자의 평가 기술의 이해 부족 및 의욕 부족 등의 문제점을 해결해야 한다. 따라서 이를 위해서는 4개의 거점 대학을 중심으로 평가 교육센터를 신설하고 육성하며, 각 대학별로 특성화된 평가 교육센터의 운영을 유도한다. 4가지 분야는 네트워크 보안 제품, 컴퓨터 정보보호 제품, 인프라 지원 제품, 그리고 응용 제품 등이다. 이를 위하여 한국정보보호진흥원을 중심으로 평가를 위한 교육 센터와 협력하는 [그림 1]과 같은 체계로의 평가 교육 체계의 확장이 요구된다. KISA는 개발자와 사용자(공무원 포함)를 대상으로 한 일반적인 평가 교육을 시행하고, 각 대학의 교육센터는 개발자, 사용자(공공영역 IT 관리자 포함), 특히



〔그림 1〕 평가 교육 체계로 확장

평가자를 대상으로 한 특성화되고 전문화된 전문 평가 분야의 교육을 시행한다. 또한 대학의 평가 교육은 전문화된 개발자를 교육에 활용이 가능하여 평가 교육의 향상할 수 있을 뿐만 아니라, 평가 교육의 질을 향상할 수 있는 장점이 있다.

시간과 공간의 제약을 방지하기 위하여 인터넷을 이용한 온라인 강의의 활성화가 요구된다. 이는 한국정보보호진흥원에 정보보호를 위한 사이버 교육센터를 신설하고, 이를 중심으로 각 대학의 교육센터와 협력하여 시행하는 것도 가능하다.

또한, 평가를 위한 전반적인 내용만을 운영하는 것을 지양하고, 교과과정을 특성화하여서 암호 지원 모듈, 하바이러스, 암호 소프트웨어, 생체인식, 스마트카드, PKI 인증 솔루션, 네트워크간 구성요소, 네트워크 기반 구성요소 등과 같은 다양한 제품에 적합한 평가 교육 과정의 개발도 요구된다. 도출 가능한 교육과정은 〔표 8〕과 같다.

또한 선진 평가기술 및 교육 내용을 조기에 습득하기 위하여 선진외국의 평가 교육기관과의 국제 협력 강화도 요구된다.

두 번째 방안을 시행하기 위하여 요구되는 사항은 다음과 같다. 초기에 한시적으로 교육센터 설비 투자를 지원한다. 지속적으로 교육 내용 개발과 사이버 강의 개발을 지원한다. 대학의 전문 인력과 KISA와의 협조 체계를 구축하기 위한 창구를 마련한다. 외국의 평가 기관간의 공동 운영의 경우와 다양한 대학이 연합하여 구성하는 경우 교육센터 선정시 우선한다.

Ⅲ. 결 론

본 논문에서는 각국에서 시행하고 있는 평가 교육 내용과 평가된 정보보호 제품들에 대해 분석하였다. CC는 많은 분량과 복잡한 표준으로 되어 있어 효과적으로 사용하기 위해서는 많은 경험과 교육이 요구되며, CC교육에 대한 투자 없이 CC의 개념을 올바르게 응용하기란 힘들고 일을 처리한 후에 수정하기에는 더 많은 대가가 초래한다. 따라서 본 논문에서는 캐나다의 CSE ITS, 미국의 COACT와 Decisive Analytics, 네덜란드의 TNO-ITSEF, 독일의 @SEC Information Security GmbH, 영국 Syntegra 교육 센터의 교육 동향을 살펴보았다. 캐나다의 교육 과정이 우리에게 많은 시사점을 제시하고 있다.

〔표 8〕 평가를 위한 국내 교육과정 제안

대분류	과목명	내 용	대 상자	등 급
인프라지원	암호이론, 암호모듈평가, 암호소프트웨어	암호 API, 모듈, 불건전정보차단도구, 통합보안솔루션	IT 개발자, 평가자, 공무원 등 사용자	중급 이상
	생체인식	지문, 얼굴, 홍채, 정맥, 서명, 화자인식	IT 개발자, 평가자, 공무원 등 사용자	중급 이상
	스마트카드, USB 토큰, PCMCIA	칩, COS(Chip Operating System), 카드판독기, 응용제품	IT 개발자, 공무원 등 사용자	중급 이상
	PKI 인증 솔루션	CA, RA, EAM, OCSP, SCVP, TSA, DVCS, KMI, DPD/DPV	IT 관리자, 평가자	중급 이상
네트워크 정보보호제품	네트워크 구성요소	Firewall, VPN, IDS, IPS	네트워크 설계자, 구현자, 관리자	모두
	네트워크기반	라우터, 스위치, 망관리 장치	IT 개발자, 관리자	중급 이상
컴퓨터 환경 정보보호 제품	신뢰된 운영체제	리눅스, 유닉스, 윈도우즈 기반	IT 관리자, 기관의 대표자, 개인	모두
	데이터베이스	관계형 데이터베이스	IT 관리자, 기관의 대표자	모두
	메일보안	SMIME, PGP 메일보안 제품	IT, 관리자, 기관의 대표자, 개인	모두

국내 평가 분야 교육은 KISA 중심으로 각 대학에서 특성화된 평가를 위한 교육 센터와 함께 수행하는 것이 바람직하며, 인터넷을 통한 사이버 교육으로 좀 더 확대해야 하고 현재 시행하고 있는 공통평가기준 기반의 교육에서 탈피하여 암호소프트웨어, 생체인식, 스마트카드, PKI 인증솔루션, 네트워크 구성요소 등과 같이 좀더 다양하고 세분화된 교육 과정의 개발이 요구된다. 더 나아가 우리 나라의 CC 교육 과정의 선진화하여 CCRA 가입에 대비해야 할 시점이라고 생각한다.

참 고 문 헌

[1] 김광식, 남택용, "정보보호시스템 공통평가기준 기술동향," 전자통신동향분석, 제17권, 제5호, 2002. 10, pp.89~101.

[2] 김광식, 남택용, 손승원, 박치항, "국제공동평가기준의 평가를 받기 위한 개발자 고려사항 분석," 제18권, 제1호, 2003. 2, pp.17~24.

[3] Common Criteria Homepage, http://www.com-moncriteria.org/

[4] CSE Information Technology Security (ITS) Learning Centre Homepage, http://www.cse.-dnd.ca/en/education/education.html

[5] COACT Homepage, http://www.coact.com-/training/training.html

[6] Decisive Analytics Homepage, http://www.-commoncriteria.com/training.html

[7] NSA Homepage, http://www.nsa.gov/isso/- programs/nietp/newspg1.htm

[8] TNO-Information Technology Security Evaluation Facility Homepage, http://www.- commoncriteria.nl/

[9] @SEC Information Security GmbH Home page, http://www.atsec.com/

[10] Syntegra Homepage, http://www.syntegra.-com/enterprisesecurity/security_evaluations/training.htm

[11] 원현심, "CCRA 가입 추진 전략 및 현황" 2002. 9. pp.13~15, KISA 정보보호뉴스.

[12] KISA Homepage 정보보호평가 평가인증제품 현황. 2003. 6, http://www.kisa.or.kr

〈著 者 紹 介〉

오 흥 룡 (Heung-Ryong Oh)
학생회원

2002년 2월 : 순천향대학교 전자공학과 졸업
2002년 3월~현재 : 순천향대학교 일반대학원 정보보호학과 석사과정
〈관심분야〉 공개키 기반구조, 보안 프로토콜

염 흥 열 (Heung-Youl Youm)
정회원

1981년 2월 : 한양대학교 전자공학과 졸업
1983년 2월 : 한양대학교 전자통신공학과 석사
1990년 2월 : 한양대학교 전자통신공과 박사
1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보기술공학부 교수
1997년 3월~2000년 3월 : 순천향대학교 산업기술연구소 소장
2000년 4월~현재 : 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재 : 한국통신정보보호학회 총무이사, 학술이사, 교육이사
관심분야 : 네트워크 보안, 전자상거래 보안, 공개키 기반 구조, 부호이론, 이동통신보안