7

CCRA 동향 및 CC 버전 3 소개

한국정보보호진흥원 ▌이 완 석

1. 서 론

미국, 영국, 독일, 프랑스 등 IT 보안 분야의 선진국들은 80년대부터 국가/공공기관의 정보보호 수준 제고를 목적으로 정보보호시스템 평가·인증 제도를 운영하여 왔다. 하지만, 인터넷의 확산에 따른 정보보호 제품 시장이 글로벌화 됨에 따라 자국의 제품을 수출하기 위해 수출대상 국가에서 또 다른 평가를 받아야 했으므로 이에 소요되는 시간, 인력, 비용을 절약하기 위한 대책 마련 필요성이 제기되었다. 이에, 이들 국가를 중심으로 평가받은 제품을 국가간 상호인정하기 위해 국제 공통평가기준 상호인정협정(CCRA : Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security)을 체결하고, '96년 공통평가기준(CC : Common Criteria for Information Technology Evaluation) 및 '99년 방법론(CEM : Common Methodology for Information Technology Evaluation) 버전 1.0을 개발하였다. 현재, CCRA는 24개 국가로 회원국이 증가되었으며, 신규 평가기준 및 방법론 개발 등 새로운 정책 발표 및 신규 회원국 확보를 위한 홍보활동을 적극 전개하고 있다.

우리나라도 이러한 국제적 흐름에 동참하기 위해 '06년 5월 CCRA에 가입하였으며, 이를 통해 국산 제품의 국제 경쟁력을 제고하고 사용자 측면에서는 안전성이 검증된 다양한 제품을 선택 사용할 수 있도록 하였다. 향후, CCRA 정책이 우리나라 정보보호 시장 및 업체에 미치는 영향이 크므로 우리나라에 유리하게 CCRA 정책이 수립될 수 있도록 정책 변화에 많은 관심을 가지고 지속적으로 의견을 제시하여야 한다.

본 고의 제2장에서는 우리나라의 평가·인증 제도를 소개하고, 제3장에서는 CCRA의 체계 및 역할을 살펴보며, 제4장에서는 CC 및 CEM 버전 3의 변경사항에 대해 분석해 보며, 마지막으로 제 5장에서는 결론으로 본 고를 마무리 한다.

2. 정보보호시스템 평가·인증 제도 소개

2.1 평가인증 체계 및 연혁

정보보호시스템 평가·인증 제도는 정보보호제품의 안전·신뢰성을 검증하고 검증된 제품의 사용을 권고

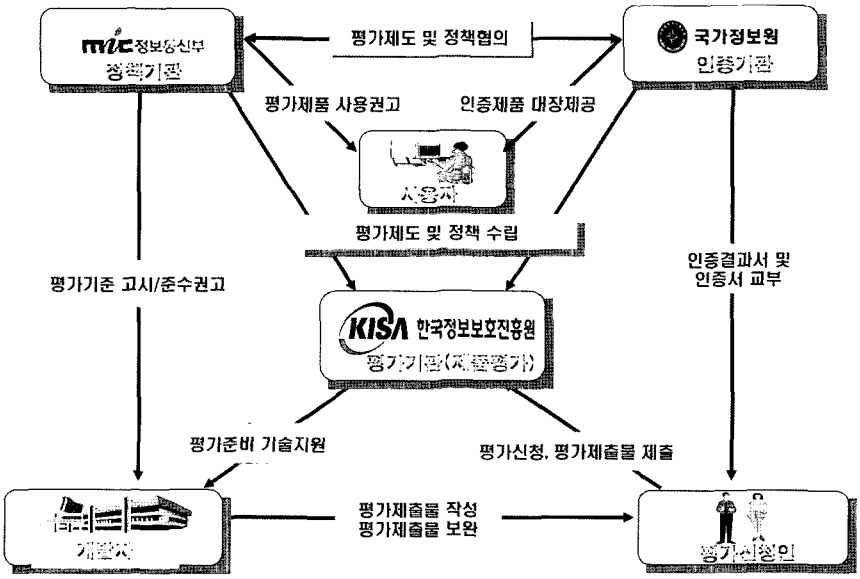

그림 1 정보보호시스템 평가·인증 체계도

함으로써 국가 정보보호 수준과 국산 정보보호제품의 국제 경쟁력을 제고하기 위한 목적으로 '98년부터 운영되었다.

정보보호시스템 평가·인증 제도의 정책기관인 정보통신부는 평가제도의 근거인 정보화촉진기본법 제·개정, 정보보호시스템 평가·인증 지침 및 평가기준 고시 업무를 담당하며 인증기관인 국가정보원은 평가기관의 평가업무 관리·감독, 평가결과 승인 및 인증서 발급, 인증제품에 대한 사후관리 및 인증정책을 결정한다. 평가기관인 한국정보보호진흥원은 정보보호제품 평가, 평가기술 및 방법론 개발, 평가기준 및 평가 지침 개발 등의 업무를 수행한다.

초기의 정보보호시스템 평가기준은 자체 개발한 국내 평가기준인 K기준을 사용하였으며 '98년에는 침입차단시스템을 '00년에는 침입탐지시스템을 대상으로 평가를 시행하였다. '02년에는 CCRA 체계를 구축하기 위하여 CC를 국내 수용하였으며 '02년 가상사설망, '03년 운영체제보안시스템, 지문인식시스템, 스마트카드, '04년 침입방지시스템, 그리고 '05년에는 보안기능이 구현된 모든 정보보호제품으로 평가대상을 확대하였다. 그 결과 '07년 3월 현재 130여개의 제품과 보호프로파일(PP : Protection Profile)을 평가 완료하였다.

2.2 CCRA 소개 및 우리나라의 가입 노력

CCRA 가입은 우리나라 정보보호제품의 품질과 평가제도를 선진국 수준으로 끌어올리기 위한 노력의 일환으로써 가입의 필요성은 평가제도 구축 초기부터 제기되어 왔다. CCRA는 현재 북미, 서유럽 등 정보보호 선진국뿐만 아니라 아시아, 동유럽 국가인 인도, 싱가포르, 체코, 헝가리 등 총 24개 국가가 회원으로 가입되어 있다.

우리나라는 '04년 CCRA 가입 준비를 위한 TFT를 구성하여 ISO Guide 65에 기반한 인증기관 운영매뉴얼을 개발하였으며, ISO/IEC 17025에 기반한 평가기관 품질매뉴얼을 개발하였다. '04. 9월 우리나라는 CCRA 의장국인 호주를 방문하여 CCRA 가입 신청서를 제출하였으며 '05. 8월부터 3개월간 제도 및 기술심사를 받았으며 동년 11월 21일부터 29일까지 호주, 일본, 네덜란드로 구성된 심사팀으로부터 현장심사를 받았다.

그 결과 '06. 5월 CCRA 가입 승인 통보를 받았으며 5월 9일 국가정보원장의 서명을 받아 공식적으로 CCRA 회원국이 되었다. 회원 가입의 마지막 공식적인 자리인 '06. 9월 스페인 란자로떼에서 개최된 국제 공통평가기준 컨퍼런스에서 CCRA 인증서발행국 자격증을 수여 받음으로써 정보보호제품 평가·인증 선진국으로 인정받았으며 무한 경쟁시대에 첫 발을 디디게 되었다.

표 1 평가기준 및 평가대상 제품군 확대 연혁

평가기준	연도	평가대상 제품군 확대
K-기준	1998. 2	침입차단시스템
	2000. 7	침입탐지시스템
CC	2002. 8	가상사설망
	2003. 11	운영체제보안시스템, 지문인식시스템, 스마트카드
	2004. 10	침입방지시스템
	2005. 5	모든 정보보호제품군으로 확대

3. CCRA 구성 및 역할

'07. 3월 현재 CCRA에는 총 24개 국가가 회원국으로 활동하고 있으며 회원국가는 다시 인증서발행국(CAP : Certificate Authorizing Participant)과 인증서수용국(CCP : Certificate Consuming Participant)으로 구분된다. CAP 국가는 자국에 평가·인증 제도를 구축하여 운영하고 있으며 CCRA에서 인정되는 인증서를 발급하는 국가이다. CCP 국가는 CAP 국가에서 발행한 인증서를 수용하는 국가를 의미한다.

CCRA는 CCRA 관리위원회(MC : Management Committee), CCRA 집행위원회(ES : Executive Sub-Committee), CC 개발위원회(DB : Development Board), CC 개발실무위원회(MB : Management Board)로 구성된다.

① CCRA MC : 모든 회원국에서 2명이 참여할 수 있으며 년 1회 회의를 개최한다. 이들은 신규 회원국 가입, CCRA의 사업계획, 새로운 버전의 평가기준 및 평가방법론, CCRA 인정범위 등 모든 업무에 대해 최종 결정권을 행사한다.

② CCRA ES : CAP 국가 또는 MC의 승인을 득한 CCP 국가에서 2명이 참여할 수 있으며 년 2회 회의를 개최한다. 이들은 CCRA 사업계획 및 절차 수립, 신규 회원국의 평가·인증 능력 심사, 회원국 정기심사, 기술적 이견을 해소하며 보안성 평가 홍보를 담당한다.

③ CC DB : CAP 국가에서 2명과 MC의 승인을 득한 전문가가 위원 자격으로 CCP 국가에서는 2명까지

표 2 CCRA 회원국명 및 구분

구분	설명	가입국명
인증서 발행국 (12개국)	자국의 인증서가 회원국으로부터 인정받는 국가	미국, 캐나다, 영국, 프랑스, 독일, 호주, 뉴질랜드, 일본, 네덜란드, 노르웨이, 대한민국, 스페인
인증서 수용국 (12개국)	인증서발행국의 인증서를 인정하는 국가	이탈리아, 그리스, 핀란드, 이스라엘, 스웨덴, 오스트리아, 터키, 헝가리, 체코슬로바키아, 싱가폴, 인도, 덴마크

관찰자 자격으로 참여할 수 있으며 년 2회 회의를 개최한다. 이들은 CC와 CEM 개발을 관리하고 모든 회원국이 동일하게 이를 적용할 수 있도록 지원하며 ISO 표준화를 위한 연락관 역할을 수행한다.

표 3 CCRA 세부 위원회 및 업무구분

위원회 명	업무
CCRA 관리위원회(CCRA Management Committee)	CCRA 모든 업무에 대한 최종 결정
CCRA 집행위원회(CCRA Executive Subcommittee)	CCRA 사업계획 수립 CAP 회원국 정기 심사 및 신규 회원국가 심사 기술적이견 해소, 평가 홍보
CC 개발위원회 (CC Development Board)	인증제품 사후관리, 개발환경 평가기준/방법론 적용, ISO 표준화
CC 개발실무위원회 (CC Management Board)	평가기준 및 방법론 개발 실무

④ CC MB : 관심을 가지고 있는 모든 회원 국가에서 참여할 수 있으며 CC 및 CEM을 실제 개발하고 각 국가에서 제기한 의문사항에 대한 해설서를 작성한다.

4. CC 버전 3.1 소개

4.1 CC 버전 3.1 개발 배경

CC 버전 3.1은 CC 버전 2.3의 후속 버전으로써, 지난 '06. 9 CCRA에서 공식버전으로 채택되었다.

CC 버전 3.1은 불필요하거나 효과가 낮은 평가 업무 배제, 명확한 용어 정의, 평가 업무 재구성·재조명, 새로운 요구사항 추가를 용의하게 함을 목적으로 한다. 기존의 CC 버전 2.x가 가지고 있는 문제점을 해결하기 위해 CC 버전 3.1이 제시한 목표는 다음과 같다.

① 단순·명료함, 일관성 : CC 버전 3.1은 기존의 CC

표 4 CC버전 2.3과 3.1의 PP/ST 구조 비교표

CC 2.3	CC 3.1	
PP/ST 구조	EAL1 PP/ST 구조	EAL2 이상 PP/ST 구조
1. PP/ST 소개 - PP/ST 식별 - TOE 개요 - 공통평가기준 적합성	1. PP/ST 소개 - PP/ST 참조, TOE 참조 - TOE 개요 - TOE 설명(ST)	1. PP/ST 소개 - PP/ST 참조, TOE 참조 - TOE 개요 - TOE 설명(ST)
2. TOE 설명		
-	2. 준수 선언 - 공통평가기준 준수 선언 - 보호프로파일, 패키지 준수 선언 - 준수 선언의 이론적근거 - PP 준수방법 서술(PP)	2. 준수 선언 - 공통평가기준 준수 선언 - 보호프로파일, 패키지 준수 선언 - 준수 선언의 이론적근거 - PP 준수방법 서술(PP)
3. TOE 보안환경 - 가정사항 - 위협 - 조직의 보안정책	-	3. 보안문제 정의 - 위협 - 조직의 보안정책 - 가정사항
4. 보안목적 - TOE 보안목적 - 환경에 대한 보안목적	3. 보안목적 - 운영환경에 대한 보안목적	4. 보안목적 - TOE 보안목적 - 운영환경에 대한 보안목적 - 보안목적의 이론적근거
-	4. 확장 컴포넌트 정의	5. 확장 컴포넌트 정의
5. 보안요구사항 - 보안기능요구사항(SOF 선언 포함) - 보증요구사항 - IT 환경에 대한 보안요구사항	5. 보안요구사항 - 보안기능요구사항(SOF 선언 없음) - 보증요구사항 - 보안요구사항의 이론적 근거	6. 보안요구사항 - 보안기능요구사항(SOF 선언 없음) - 보증요구사항 - 보안요구사항의 이론적 근거
6. TOE 요약명세(ST)	6. TOE 요약명세(ST)	7. TOE 요약명세(ST)
7. 보호프로파일 수용(ST) - 참조, 재정립, 추가사항	-	-
8. 이론적 근거 - 보안목적의 이론적근거 - 보안요구사항의 이론적근거 - TOE 요약명세의 이론적근거(ST) - 보호프로파일 수용의 이론적근거(ST)	-	-

버전 2.x에 비해 보다 단순하고 명료해졌다. 장황하고 불필요한 부분은 축소 기술하였으며, 부정확하거나 추가 설명이 필요한 부분은 확대 기술하였다. 또한 용어를 일관성 있고 명확하게 정의하였다.

② 합리성 및 중복성 제거 : CC 3부 보증요구사항을 재작성 및 재구성하였다. 전체적으로 유사한 평가업무를 제거하였고 보증에 필요한 부분을 강조하였다.

③ 개발자의 사용 편이성 향상 : ADV 클래스를 간소화하는 등 개발자가 쉽게 읽을 수 있도록 CC와 CEM의 구성을 재편집하였다.

④ 합성제품의 평가를 위한 요구사항 추가 : CC V3.1은 호환되는 인증제품들 간의 합성형 제품에 대한 평가를 지원한다.

4.2 주요 변경 내역

4.2.1 PP & ST의 변경 내역

그림에서 보는 바와 같이 TOE 설명(TOE Description)은 PP 및 ST 소개(PP/ST Introduction)로 통합되었고, 이론적 근거(Rational)는 보안목적(Security Objectives)과 보안요구사항(Security Requirements)으로 통합되었으며, 준수 선언(Conformance Claims)절이 새롭게 추가되었다. 또한, TOE 보안환경(TOE Security Environment)은 보안문제 정의(Security Problem Definition)로 명칭이 변경되었고, IT 환경에 대한 보안요구사항이 삭제되었다.

4.2.2 EAL1 등급의 PP & ST 변경 내역

PP/ST 작성 시 EAL1 등급은 그 상위 등급(EAL2 이상)에서 요구하는 수준으로 문서를 작성할 필요가 없음을 인지하고 작성 양식을 간소화하였다. 즉, CC 버전 3.1에서는 EAL1과 EAL2 이상에서의 PP/ST 구조를 구분한다.

EAL1 등급의 PP 및 ST에서는 위협, 조직의 보안정책, 가정사항 등 보안문제 정의 부분, TOE에 대한 보안목적 및 보안목적에 대한 이론적 근거를 삭제함으로써 저등급 PP 및 ST에 대한 요구사항을 최소화하였다.

4.2.3 PP 준수 선언 방법 변경 내역

CC 버전 3.1에서는 기존의 PP 준수 선언의 방법을 엄격한 준수(Strict)와 입증가능한 준수(Demonstrable)로 구분하였다.

엄격한 준수에서는 PP와 ST 간에 부분-포함의 엄격한 관계가 존재한다. 이 관계는 "ST는 PP 내에 있는 모든 서술문을 포함해야 하며, 별도의 서술을 포함할 수도 있다."와 같이 정의될 수 있다. 엄격한 준수는 정해진 한 가지 방법으로 준수되어야 하는 요구사항에 적용될 것이다.

입증가능한 준수에서는 해결책을 명세하는데 한 가지 이상의 방법이 있다는 전제 하에 PP 작성자가 해결되어야 할 일반적인 보안 문제를 서술하고 그 해결에 필요한 요구사항의 포괄적인 지침을 제공할 수 있게 한다. 입증 가능한 준수는 몇몇의 비슷한 PP가 존재하는 (또는 존재할 가능성이 있는) TOE에 적합하기 때문에, ST 작성자는 그 PP 모두를 동시에 준수해서 수고를 덜 수 있다.

4.2.4 종속관계

종속관계는 보안기능 요구사항과 보증 요구사항간의 종속관계가 제외 되었으며 보안기능은 보안기능간의 종속관계와 보증 요구사항은 보증 요구사항간의 종속관계만이 존재한다.

4.3.5 보안기능 요구사항 변경 내역

CC 버전 3.1의 보안기능 요구사항은 CC 버전 2.3과 거의 동일하다. 변경사항으로 우회불가성(FPT_RVM)과 영역분리(FPT_SEP)가 실제 제품의 보안기능으로 구현하기 어려운 점이 있어 보증 요구사항으로 이동하였다.

4.3.6 보증 요구사항 변경 내역

① ACO 클래스의 추가

CC 3.1에서 새롭게 추가된 클래스로, 합성평가는 한 개 이상의 인증제품을 포함한 통합 제품 평가를 위한 요구사항이다. 합성 TOE는 기본 컴포넌트와 종속 컴포넌트로 구성되며 서비스를 제공하는 TOE는 기본 컴포넌트이고 서비스를 받는 TOE는 종속 컴포넌트이다. 합성평가는 각 컴포넌트의 평가결과를 기초 자료로 활용하며 최소한 기본 컴포넌트는 인증제품이어야 하고 종속 컴포넌트는 인증제품 또는 평가가 진행중인 TOE일 수도 있으나 합성평가가 끝나기 전까지는 종속 컴포넌트 평가가 완료되어야 한다.

표 5 ACO 클래스의 등급 비교표

CAP 등급	주요내용	기본 컴포넌트 최소 등급
CAP-A	ST, 설명서, 기능명세 평가결과 활용 합성 TOE의 평가자 독립 시험	EAL1
CAP-B	ST, 설명서, 기능명세, TOE 설계문서(TDS.1 수준 이상) 평가결과 활용 합성 TOE의 평가자 독립 시험 취약성 분석 : 기본 공격 성공 가능성	EAL2
CAP-C	ST, 설명서, 기능명세, TOE 설계문서(TDS.3 수준 이상) 평가결과 활용 합성 TOE의 평가자 독립 시험 취약성 분석 : 강화된-기본 공격 성공 가능성	EAL4

합성평가는 기존의 평가등급(EAL)과는 별도의 등급을 가지고 있으며 3개로 정의(CAP-A, CAP-B, CAP-C)한다. 합성평가의 등급은 기본 컴포넌트의 평가등급과 연관이 있으며 CAP-A 등급의 경우, 기본 컴포넌트의 등급이 EAL1 이상이여야 하며, CAP-B는 EAL2 이상, CAP-C는 EAL4 등급 이상이어야 한다.

② ADV 클래스 변경내역

CC 버전 2.3에서는 기능명세서(FSP), 기본설계서(HLD), 상세설계서(LLD), 구현표현(IMP), 표현의 일치성(RCR), TST 내부(INT), 보안정책모델(SPM)으로 구분되었으나 기본설계와 상세설계는 TOE 설계(TDS)로 통합되었으며 표현의 일치성(RCR)의 경우 각 패밀리 요구사항으로 통합되었다. 특히 큰 변화는 TOE 보안 구조(ARC)가 추가된 점이다.

TOE 보안 구조에서는 자체보호, 우회불가성, 영역분리, TSF 초기화의 안전성에 대해 서술하며, 이는 SFR-수행 설명과 동일한 상세수준으로 제공되어야 한다. 자체보호와 우회불가성의 경우, 보안기능이 제대로 구현되었는가를 검증하는 것이 어려우며 오히려 보안기능 측면보다는 TOE 설계의 정확한 구현을 통해 수행되는 TSF 특성이 있으므로, 보안기능 요구사항에서 보증 요구사항으로 이동되었다.

그 외의 변경사항은 다음과 같다.

- TSFI는 SFR 관련성에 따라 SFR-수행, SFR-지원, SFR-비-간섭으로 구분하여 서술할 것을 요구한다.
- CC 버전 2.3에서는 EAL5부터 전체 소스코드를 요구하였으나, CC 버전 3.1에는 EAL6부터 전체 소스코드를 요구한다.

③ 형상관리, 생명주기 지원, 배포 및 운영, 설명서 클래스 변경 내역

이들 4개 클래스는 개발자 측면과 사용자 측면을 고려하여 생명주기 지원과 설명서 등 2개의 클래스로 재구성되었다. 형상관리 및 생명주기 지원은 생명주기 지원 클래스로, 설명서는 설명서 클래스로 구분되었으며, 배포 및 운영 클래스에서 배포는 생명주기 지원 클래스로 운영은 설명서 클래스로 분리되었다.

④ 시험 클래스 변경 내역

시험 클래스는 버전 2.3의 내용과 거의 동일하다. 단, 3.1에서는 EAL4부터 SFR-수행 모듈에 대한 시험을 추가 요구하였다.

⑤ 취약성 평가 클래스 변경 내역

CC 버전 3.1에서는 개발자의 취약성 분석이 없어지고 EAL1부터 평가자의 취약성 분석을 요구함으로써 개발자의 업무량을 줄이고 평가자의 업무량을 증가시켰다.

4.3 적용 시점

CCRA는 '06. 9월 CC 버전 3.1을 공식 발표하였으며 '08. 4월까지는 현 CC 버전 2.3과 3.1을 정보보호제품 평가에 선택 적용하여 평가하되 그 이후부터는 CC 버전 3.1만을 사용하도록 의무화하였다.

우리나라의 경우, 평가 중이거나 대기 중인 제품

표 6 CC버전 2.3과 3.1의 보증요구사항 비교표

<table>
<tr><th colspan="2">CC v2.3</th><th colspan="2">CC v3.1</th></tr>
<tr><td colspan="2">7개 클래스</td><td colspan="2">6개 클래스</td></tr>
<tr><td>TOE의 무결성이 유지됨을 보장</td><td>ACM
(형상관리)</td><td rowspan="2">ALC
(생명주기 지원)</td><td rowspan="2">개발자 측면 요구사항</td></tr>
<tr><td>TOE의 생명주기와 관련된 요구사항</td><td>ALC
(생명주기 지원)</td></tr>
<tr><td>TOE의 안전한 배포,
설치 등에 필요한 요구사항</td><td>ADO
(배포 및 운영)</td><td rowspan="2">AGD
(설명서)</td><td rowspan="2">사용자 측면 요구사항</td></tr>
<tr><td>TOE의 안전한 운영을 위한 지침</td><td>AGD
(설명서)</td></tr>
<tr><td>TOE의 개발과정 세분화
(요약명세, 설계, 구현단계)</td><td>ADV
(개발)</td><td>ADV
(개발)</td><td>ARC 패밀리 추가, CC 2.3의
HLD/LLD가 TDS 패밀리로 통합</td></tr>
<tr><td>TOE가 보안기능요구사항을 만족함을
입증</td><td>ATE
(시험)</td><td>ATE
(시험)</td><td>변경된 개발요구사항 반영</td></tr>
<tr><td>악용가능한 취약성 식별, 침투시험</td><td>AVA
(취약성 평가)</td><td>AVA
(취약성 평가)</td><td>평가자 취약성 분석만 요구</td></tr>
<tr><td></td><td>-</td><td>ACO
(합성)</td><td>클래스 추가</td></tr>
</table>

수를 고려하면 '07. 4월부터 계약되는 제품은 '08. 4월 이후에 평가착수될 가능성이 높다. 따라서 이들 제품은 CC 버전 3.1에 의해 평가제출물을 준비해야만 '08. 4월 이후 평가착수되는 경우에 대비할 수 있다.

5. 결 론

우리나라는 국가 정보보호 수준 및 국산 정보보호 제품의 국제 경쟁력을 제고하기 위하여 정보보호시스템 평가·인증제도를 '98년부터 운영하여 왔다. '07. 3월 현재 130여개의 정보보호제품이 평가를 받았으며, 매년 25개 이상의 제품이 평가를 받고 있다.

국제적으로는 정보보호를 주도하는 국가들이 CCRA를 체결하여 평가한 결과를 국가간 상호인정하고 있으며 협정에 가입한 국가가 '07. 3월 현재 24개 국가에서 점차 증가하고 있으며 대만, 말레이시아가 최근 협정에 가입하고자 노력하고 있다. 더욱이 이들 국가들은 국가/정부에서는 평가받은 제품을 사용할 것을 권고 또는 강제하고 있다. 특히, 우리나라는 미국(24%), 일본(28%), 유럽(19%) 등에 정보보호제품의 수출이 전체 수출의 71%에 해당하여 큰 영향을 미칠 수 있다[4].

따라서 우리나라 제품이 해외에 원활히 수출되기 위해서는 CCRA의 정책 변화에 빠르게 대응하여야 하며 정책이 우리나라에게 유리한 방향으로 변경될 수 있도록 CCRA에 적극 참여하여야 한다.

참고문헌

[1] "Common Criteria for Information Technology Security Evaluation" CCRA, V3.1, 2006.

[2] "Common Methodology for Information Technology Security Evaluation" CCRA, V3.1, 2006.

[3] "공통평가기준 3.0 분석", 성균관대학교, 2006.

[4] "국내 정보보호시장에 미치는 영향을 고려한 CCRA 가입 정책 연구", 한국정보보호학회, 2003.

이 완 석

1986. 9~1991. 5 미국 버지니아공대 전산과학 전공
1998. 9~2001. 2 동국대학교 정보보호학과 석사
2004. 9~현재 성균관대학교 컴퓨터공학 박사과정
1994. 8~1996. 7 현대정보기술 CAD/CAM 사업부 사원
1996. 7~현재 한국정보보호진흥원 보안성평가단 평가기획팀장

관심분야 : 보안성 평가, 정보보증, 시스템 인증
E-mail : wsyi@kisa.or.kr