양질의 평가서비스 제고를 위한 CCRA 요구사항 수준의 평가기관 요구사항 분석

이유리[1], 박동규[1], 김상호[2], 김재성[2]

순천향 대학교 정보기술 공학부[1], 한국정보보호진흥원[2]

The analysis of requirements for evaluation facilities to meet requirements of CCRA in order to support qualities for evaluation service

You-Ri Lee, Dong-Gu Park, Sang-Ho Kim, Jae-Sung Kim

Department of Information and Technology Engineering, College of Engineering

SoonChunHyang University[1],

Korea Information Security Agency[2]

요약

본 논문에서는 정보보호제품의 평가 수요 증가에 적극적으로 대처하고, 양질의 평가서비스 제고를 위한 CCRA 요구사항 수준의 평가기관 요구사항을 분석 및 도출한다. 이를 위하여 CCRA의 평가기관 요구사항 및 ISO/IEC17025의 요구사항을 분석하였으며, NIST Handbook 150, NIST Handbook150-20 등 CAP 국가들의 평가기관 인정과 관련된 표준문서들을 연구하여 각 CAP 국가들의 평가기관 요구사항들을 분석하고 평가기관의 평가자 양성을 위한 교육 및 자격 부여 프로그램들을 비교 분석하였다.

I. 서 론

정보통신기술의 발달로 전자적으로 처리되는 정보량이 증가함에 따라 사회 각 분야에서 구축·운영되는 공공 및 민간분야 정보통신시스템의 안전성 확보의 필요성이 증대하고 있다.

최근에 발생한 유명사이트들의 해킹사건을 통하여 안전성이 입증되지 않은 취약한 정보보호시스템을 사용한 정보시스템 구축은 오히려 그 취약성을 증가시키는 위험성을 내포하고 있음을 알 수 있으며, 따라서 정보 보호 시스템의 안전성 및 신뢰성 검증이 새삼 중요해 지고 있다.

국내외에서도 정보 보호 시스템의 안전성 및 신뢰성 검증을 위한 여러 가지 기준을 마련하고, 다양한 노력을 기울이고 있다.

정보보호제품을 상호인정하자는 논의는 미국, 영국, 독일, 프랑스, 캐나다 등 선진 5개국을 중심으로 시작되었으며, 그 결과로 1998년 10월 공통평가기준(CC) 기반의 상호인정협정(CCMRA)을 체결하여, 협정가입국가에서 평가받은 제품에 대해서는 재평가를 실시하지 않고 자국내 사용을 허가 또는 권고하게 하였다. 이후 2000년 5월 미국 볼티모어에서 개최된 제1회 ICCC(International Common Criteria Conference)에서 CCMRA 체제가 CCRA(Common Criteria Recognition Arrangement) 체제로 13개국이 참여하는 협정으로 확대 개편되었으며, 2000년 이후 현재 18개국으로 늘어나게 되었다.

국내에서도 정보화촉진기본법과 동법 시행령에 근거한 제품별 평가기준에 근거하여 침입차단시스템 및 침입탐지시스템 등 정보보호제품에 대한 평가를 1998년부터 시행하고 있으며, 2002년 8월 현

재 침입차단시스템 23개, 침입탐지시스템 11개에 대하여 평가를 완료한 상황이다. 또한, 2002년 8월부터는 공통평가기준(CC)을 국내평가기준으로 고시하여 공통평가기준기반의 평가를 시행 중에 있다.[3][4] 그러나 공통평가기준을 국내평가기준으로 수용하였지만 CCRA에 가입하지 않는다면, 업체들이 제품을 해외에 수출하기 위해 동일한 제품에 대해 두 번의 평가를 받아야 함으로써 시간과 비용의 낭비를 초래할 수 있으며, 대부분의 IT선진국이 가입한 CCRA 협정이 향후 정보보호제품의 국제거래에 있어서 사실상의 보이지 않는 교역장벽으로 작용하게 되는 문제도 초래하게 된다. 따라서 정보보호강국으로 발돋움하기 위해서는 CCRA가입이 필수적이라고 할 수 있다.

따라서 본 논문에서는 정보보호제품의 평가 수요 증가에 적극적으로 대처하고, 양질의 평가 서비스 제고를 위한 CCRA 요구사항 수준의 평가기관 요구사항을 분석하기위해 다음과 같이 논문을 구성한다. Ⅱ장에서는 CAP국가의 평가기관 요구사항을 분석하며 Ⅲ장에서는 CAP국가의 평가자 양성을 위한 교육 및 자격부여 프로그램을 분석한다. 또한 Ⅳ장에서 CCRA 가입을 위한 평가기관 요구사항을 분석하고 Ⅴ장에서 본 논문의 결론을 맺고자 한다.

II. CAP국가의 평가기관 요구사항

1. ISO/IEC17025의 요구사항 분석

ISO/IEC17025 국제규격은 샘플링을 포함하여 시험 및 교정을 실시할 자격에 대한 요구사항을 규정한 것으로 표준방법, 표준방법에 없는 방법과 시험 및 교정 기관에서 개발한 방법 등을 사용하여 실시한 시험 및 교정을 대상으로 한다. 이 국제규격은 시험 및 교정을 실시하는 모든 기관에 적용 가능하며 직원의 숫자, 시험 및 교정 활동의 범위 정도에 관계없이 모든 해당기관에 적용 가능하다. 이 국제규격은 해당기관이 조직의 운영을 관리하는 품질, 행정 및 기술 시스템 개발 시 활용하는 문서로서 경영 요구사항과 기술 요구사항으로 나누어져 있으며, 시험소 고객, 규제기관 및 인정기구에서 해당기관의 자격을 확인 또는 인정하는데 이용할 수 있다. 이 규격은 해당기관의 운영상의 규제 및 안전 요구사항에 대한 부합은 포함하고 있지 않으며, 해당기관이 이 국제규격의 요구사항에 부합하면, 이들의 시험 및 교정활동에 대한 품질시스템은 표준화된 것과 표준화되지 않은 시험/교정 방법을 결합하여 신규 방법의 설계/개발에 참여할 경우 및/또는 시험 프로그램을 개발할 경우에는 ISO 9001의 요구사항을, 이들이 단지 표준화된 방법을 사용할 경우에는 ISO 9002의 요구사항을 충족하고 있는 것으로 간주한다. ISO/IEC 17025는 ISO 9001 및 ISO 9002에 포함하지 않는 몇 가지 기술적 자격요구사항을 포함하고 있다. 이 규격은 경영 요구사항과 기술요구사항으로 나누어져 있다. 경영요구사항은 조직, 품질시스템, 문서 관리, 의뢰, 입찰 및 계약의 검토, 시험 및/또는 교정의 위탁서비스 및 물품 구매, 고객에 대한 서비스, 불만사항, 부적합 시험 및/또는 교정 작업의 관리, 시정 조치, 예방 조치, 기록의 관리, 내부 감사, 경영 검토 등의 내용을 다루고 있으며, 기술요구사항은 일반사항, 직원, 시설 및 환경 조건, 시험 및/또는 교정 방법과 방법의 유효성 확인, 장비, 측정 소급성, 샘플링, 시험 및/또는 교정 품목의 취급, 시험 및/또는 교정 결과의 품질보증, 결과보고 등의 내용을 다룬다.[1][2]

2. CAP 국가의 평가기관 요구 사항 분석

1) 미국의 평가기관 요구사항 분석

NIST 핸드북 150은 NVLAP이 시험과 교정기관을 인정하기 위한 중립적인 제3의 기관으로 동작하기 위한 절차와 일반적인 요구사항을 설명한다. 보완적인 기술 요구사항과 관리 요구사항은 지원 핸드북(NIST 핸드북 150시리즈)과 관련된 문서들에서 제공된다.

NIST 핸드북 150-20은 CC 스킴 하에서 정보기술 보안 평가를 실행하기 위하여, 인증을 할 수 있는 시험소를 위한 NVLAP의 절차와 기술적인 요구사항을 나타낸다.[5][6]

미국의 평가기관 요구사항을 분석해 보면 평가인정 절차는 인정신청과 인정심사, 인정 결정이 되는 1단계 방식이며, 평가기관 운영에 대한 항목으로 인정범위 변경, 인정 종결, 인정 재 갱신, 인정 중지 및 취소, 분쟁 처리에 대한 문제를 설명하고 있다. 그리고 평가자들의 요구사항은 평가자들이 훈련받아야하는 분야에 대한 설명으로 정리하고 있으며, 평가기관 인정조건으로 ISO/IEC 17025를 채택하고 있다. 그리고 이것에 부가적으로, CCT에 적용될 수 있도록 하는 부가적인 요구사항을 설명하고 있다.

2) 캐나다의 평가기관 요구사항 분석

캐나다의 평가기관 요구사항 표준문서는 CAN-P-1591으로 ITS 평가와 시험을 수행할 수 있는 시설의 SCC 인가를 위하여 기술적이고 조직적인 문제에서 ISO/IEC Guide 25 (CAN-P-4)에

서 주어진 요구사항에 부가적인 요구사항을 확립하는 것으로 CAN-P4C(교정과 시험 시험소의 인가를 위한 일반 요구사항)를 확대한 자세한 지침 문서이다. 여기에서 CAN-P4C는 ISO/IEC Guide25(교정과 시험 시험소 운영과 인가를 위한 일반 요구사항)의 캐나다 채택문서이다.[7][8]

캐나다의 평가기관 요구사항을 분석해 보면 평가 인정 절차는 인정신청과 인정심사, 인정 결정이 되는 1단계 방식이며, 평가기관 운영에 대한 항목으로 인정 중지 및 취소에 대한 문제를 설명하고 있다. 그리고 평가기관 인정조건으로 ISO/IEC 17025를 채택하고 있으며, 이것에 부가적으로 기술적이고 조직적인 문제에서 부가적인 요구사항을 설명하고 있다는 것이 특징이라고 할 수 있다. 평가자들의 요구사항은 평가자들이 훈련 받아야하는 분야에 대한 설명으로 정리하고 있다.

3) 영국의 평가기관 요구사항 분석

영국의 평가기관 요구사항 표준문서 UKSP02는 평가기관 CLEF로 선정되기를 원하는 업체를 위해 평가기준과 증거 요구사항에 관한 것을 제시하며, CLEF는 이 문서에서 상세히 열거한 기본적인 요구사항들과 수행규칙들을 준수해야 한다. UKSP02는 ITSEC에 대한 평가를 위해 UKAS 인가를 허락하기 위한 CLEF선정의 근거로 사용된다. [9][10]

영국의 평가기관 요구사항을 분석해 보면 평가 인정 절차는 임시선정 이후에 완전선정이 되는 2단계 방식이며, 평가기관 운영에 대한 항목으로 인정범위 변경, 인정 종결, 인정 재 갱신, 인정 중지 및 취소, 분쟁 처리 등을 설명하고 있다. 그리고 평가기관 인정조건으로 ISO/IEC 17025를 채택하고 있으며, 평가자들을 3개의 등급으로 구분하여 등급별 자격과 등급별 평가원이 되기 위한 훈련 프로그램을 모듈별로 자세하게 정리하고 있는 것이 특징이라고 할 수 있다.

4) 호주의 평가기관 요구사항 분석

호주의 평가기관 요구사항 표준 문서 AISEP02는 AISEF의 제정과 운영을 위한 기본적인 요구사항과 규칙을 지정하며, 선정과 승인, 관리, 품질, 보안과 기밀성, 직원 권한 부여와 같은 문제들을 설명한다. AISEF의 선정과 승인에서는 AISEF의 선정, AISEF의 운영관리체계, 품질 및 기밀성, 보안, 평가자들을 위한 요구사항, 시험평가, 정식 승인 등을 설명하며, 관리에서는 관리체계 등을 설명한다.[13][14]

호주의 평가기관 요구사항을 분석해 보면 평가 인정 절차는 임시선정 이후에 완전선정이 되는 2단계 방식이며, 평가기관 운영에 대한 항목으로 인정 종결, 인정 재 갱신, 인정 중지 및 취소, 분쟁 처리 등을 설명하고 있다. 그리고 평가기관 인정조건으로 ISO/IEC 17025를 채택하고 있으며, 평가자들을 3개의 등급으로 구분하여 등급별 자격과 등급별 평가원이 되기 위한 훈련 프로그램을 자세하게 정리하고 있는 것이 특징이라고 할 수 있다.

5) 프랑스의 평가기관 요구사항 분석

프랑스의 평가기관요구사항 표준문서 ECF02는 인정절차, 승인절차, CESTI 승인기준 등을 설명하고 있다.[11][12]

프랑스의 평가기관 요구사항을 분석해 보면 평가 인정 절차는 임시선정 이후에 완전선정이 되는 2단계 방식이며, 평가기관 운영에 대한 항목으로 인정 종결, 인정 재 갱신, 인정 중지 및 취소, 분쟁 처리 등을 설명하고 있다. 그리고 평가자의 훈련 프로그램에 대한 자세한 설명보다는 평가자들이 훈련받아야하는 분야에 대한 설명으로 평가자들의 요구사항을 정리하고 있으며, 다른 나라들과는 달리 평가기관 인정조건으로 EN45001을 채택하고 있는 것이 특징이라고 할 수 있다.

6) 일본의 평가기관 요구사항 분석

일본의 평가기관 요구사항 표준 문서는, 독립행정법인 제품 평가 기술 기반 기구가 경제 산업성으로부터의 위탁을 받아 실시하는 IT보안 평가・인증 프로그램 하에서 IT제품 및 시스템의 보안이 국제 규격에 적합한지를 판단하기 위하여, 적합성을 평가하는 IT보안 평가 기관이, 인증 프로그램에 의해 승인을 얻기 위한 요구 사항에 대해서 설명하고 있다.

일본의 평가기관 요구사항을 분석해 보면 평가 인정 절차는 인정신청, 인정심사, 인정 결정이 되는 1단계 방식이며, 평가기관 운영에 대한 항목으로 인정범위 변경, 인정 종결, 인정 재 갱신, 인정 중지 및 취소, 분쟁 처리 등을 설명하고 있다. 그리고 평가기관 인정조건으로 ISO/IEC 17025를 채택하고 있으며, 평가자들이 훈련 받아야하는 분야에 대한 설명으로 평가자들의 요구사항을 정리하고 있다. 일본에서는 평가자들이 평가할 수 있는 영역들을 인정받고, 평가기관의 역량은 평가기관에 소속하고 있는 평가자들의 평가 역량에 의해서 결정되는 것이 특징이라고 할 수 있다.

III. CAP국가의 평가자 양성을 위한 교육 및 자격부여 프로그램

1. 미국의 평가자 양성 교육 프로그램

미국에서 IT 보안 평가 활동을 수행하는 시험소 직원은 컴퓨터 과학 또는 컴퓨터 공학 또는 관련된 기술 적인 분야의 석사학위 또는 동등한 경험을 가지고 있어야 하며, 시험소 직원은 운영체제, 자료구조, 알고리즘의 설계와 분석, 데이터베이스, 프로그래밍 언어, 컴퓨터 시스템 구조와 통신과 같은 분야에 지식과 경험이 있어야 한다. 그리고 시험소 직원에 대한 훈련은 평가 보고서의 생성을 포함한 시험 방법들에 대한 일반적인 요구사항, 컴퓨터과학 개념, 컴퓨터 보안 개념, 국제공통평가기준에 대한 작업 지식, 국제공통평가방법론에 대한 작업 지식과 같은 분야에 대하여 집중적으로 수행된다.

2. 캐나다의 평가자 양성 교육 프로그램

캐나다의 평가기관은 적어도 세 사람의 기술직원들이 있어야 한다. 이 기술직원들은 적당한 교육지식(컴퓨터 학, 공학, 또는 관련 학과에 대한 대학 정도 또는 단과대학정도의 졸업증 또는 전문가 증명서)을 가지고 적어도 2년은 보안 제품 개발, 시험, 또는 평가 경험이 있어야 한다. 평가기관 직원은 표준문서에서 지정한 다양한 영역에서의 지식과 경험을 선택적으로 가지고 있어야 하며, 영역들과 관련된 학식이나 경험뿐만 아니라, 이 지식영역과 관련된 장비를 적절하게 사용해야 한다. 시험소의 직원은 부여받은 의무에 대하여 훈련을 받아야 하며, 훈련은 새로운 시험 방법 적용, 구현 지침 검토와 시험 수행을 포함한다. 각 직원 멤버는 작업 훈련 또는 형식적 교실 연구 혹은 다른 적합한 절차를 통하여 부여받은 의무에 대한 훈련을 받을 수 있다.

3. 영국의 평가자 양성 교육 프로그램

영국의 평가자 훈련은 컴퓨터 보안의 개념과 원리를 이해하고, ITSEC에 기초를 둔 원리를 완전히 이해하며, 모든 기준을 선정 조건에서 지정된 임의의 평가 레벨에 적용할 수 있도록 양성한다.

영국의 스킴은 평가자에 대하여 훈련받는 평가자, 자격이 있는 평가자, 그리고 상급 평가자 3단계의 자격을 인정하며, 평가자 직원 훈련프로그램으로 M1 -기본 보안 컨셉, M2 -평가 기술 접근, M3 -계획과 업무, M4 -외부의 기관 등 4개 모듈을 설명하고 있다.

평가 후보자가 모듈 M1과 M2를 만족하게 완성하면, 그들은 훈련받은 평가원으로 간주되며, 자격을 갖춘 평가자가 되기 위해서는 관련 OJT 경험과 함께 모든 4개 모듈의 만족스러운 완료가 필요하다. 자격을 갖춘 평가자는 그들의 평가업무를 통하여 경험을 계속적으로 얻게 될 것이고, 그런 경험의 축적으로 상급 평가자로서의 승인을 얻게 된다.

4. 호주의 평가자 양성 교육 프로그램

호주의 평가자들은 훈련받은 평가자, 자격이 있는 평가자, 상급 평가자등 3개의 등급이 있으며, 평가자의 훈련 과정은 평가자의 활동에 대한 모든 측면을 포함하며 기본적인 평가의 연습과 평가관리 2파트로 이루어지고 있다. 호주의 표준문서에서는 각 등급의 평가자가 되기 위한 자격과 권한을 상세하게 설명하고 있다.

5. 프랑스의 평가자 양성 교육 프로그램

프랑스 평가 기관인 CESTI 평가자는 기술정보에 정통해야 하며 보안검증에 경험과 능력을 갖춰야 한다. 경험에 대한 평가는 인증기관이 관리하며, 특히, CESTI 평가자의 능력은 승인서로 인정되어야 한다. 또한 ITSEC 기준, ITSEM 설명서에 나타난 평가방법론과 평가 활동에 쓰이는 방식에 대한 훈련을 받아야 하며, 이후에는 인증기관에서 제시하는 승인서를 만족하는 이론과 실습을 받아야 한다.

6. 일본의 평가자 양성 교육 프로그램

일본의 인증기관은 평가기관에 대하여 평가자의 자격을 부여하기 위한 요구 사항을 규정하고 있으며, 인증기관은 요구 사항에 적합한 평가자 후보를 신청과 관련되는 보증 요소의 평가자로서 자격을 부여해서 등록하며, 평가 업무의 감독에 있어 요구 사항에 적합하지 않다고 판단할 경우에는 평가자로서의 등록을 말소할 수 있다.

IV. CCRA 가입을 위한 평가기관 요구사항 분석

1. CCRA내의 평가기관 인정조건

CCRA내의 평가기관과 관련된 인정조건은 5조

에 정리되어 있으며, CCRA 내의 5조 인정조건에서 정리하고 있는 최소 평가기관 인정조건은 CCRA 부록 B.3에 정리되어 있다. 이를 분석해 보면 CCRA에서 요구하고 있는 평가기관으로 인정받기 위해서는 평가기관은 다음 조건중의 하나를 충족시켜야 한다.

· EN 45001 이나 ISO Guide 25, 혹은 이들에 대하여 모든 참가체들에 의해 공인된 해석에 의거하여 인정된 인정수여기관(Accreditation Body : AB)에 의해 각 국에서 공인되고, 그리고 부록 B.3에 의해 공인받거나,

· 각국의 법, 법적 수단, 혹은 행정절차에 의해 설립되고, 부록 B.3의 모든 요구조건을 충족한다.

2. CAP 국가의 인정절차 비교 분석

CAP 국가들의 평가기관 인정절차를 비교하면 다음 표1과 같다.

표 1: CAP 국가들의 인정절차 비교

		미국	캐나다	일본	영국	호주	프랑스
1단계	인정신청	○	○	○			
	인정심사	○	○	○			
	인정결정	○	○	○			
2단계	인정신청				○	○	○
	인정심사				○	○	○
	인정결정				○	○	○

표1에서 나타난 바와 같이 인정 절차는 크게 1단계로 인정이 되는 방식과 임시선정 그 이후에 완전선정이 되는 2단계 방식으로 나누어진다. 1단계로 인정되는 방식은 미국, 캐나다, 일본 등이며, 2단계로 인정되는 방식은 영국, 호주, 프랑스에서 채택하고 있다.

3. CAP 국가의 평가기관 운영 비교 분석

CAP 국가들의 평가기관 운영을 비교하면 다음 표 2와 같다.

표 2: CAP 국가들의 평가기관 운영 비교

	미국	일본	캐나다	영국	호주	프랑스
인정범위변경	○	○		○		
인정종결	○	○		○	○	○
인정재평가	○	○		○	○	○
인정중지, 취소	○	○	○	○	○	○
분쟁처리	○	○		○	○	○

각 나라들의 평가기관 운영 요구사항을 분석해 보면 평가기관 운영에 대한 항목으로 인정범위 변경, 인정 종결, 인정 재 갱신, 인정 중지 및 취소, 분쟁 처리 등을 들 수 있으며, 이중에서 인정의 종결은 평가기관 스스로 인정의 자발적인 종료와 인정(인증)기관에 의한 종료로 나눌 수 있다.

4. CAP 국가의 평가기관 인정조건 비교 분석

CCRA의 평가기관 인정을 위한 조건에서는 평가기관의 인정조건으로 EN 45001 이나 ISO Guide 25을 만족해야 한다는 내용이 있다. 따라서 평가기관으로 인정을 받기 위해서는 기본적으로 EN 45001 이나 ISO Guide 25을 만족해야 한다. CAP 국가들의 평가기관 요구사항들을 비교 분석해 보면 모든 국가에서 이 조건을 만족하고 있음을 알 수 있다.

CAP 국가 평가기관의 인정조건을 비교하면 다음 표3과 같다.

각 나라들의 평가기관 인정조건 요구사항을 분석해 보면 CCRA 평가기관 인정조건 요구사항을 만족하기 위하여 미국, 캐나다, 영국, 호주, 일본등은 평가기관 인정조건으로 ISO/IEC 17025를 채택하고 있으며, 프랑스는 EN45001을 채택하고 있다. 그중에서도 미국과 캐나다는 ISO/IEC 17025를 기본조건으로 하고 평가기관이 국제공통평가기준과 국제공통평가방법론을 사용하여 IT 보안 평가를 수행하는데 대한 경쟁력이 있는지를 증명하기 위한 특별한 요구사항으로 부가적인 조건을 채택하고 있다.

표 3: CAP 국가들의 평가기관 인정조건 비교

	미국	캐나다	일본	영국	호주	프랑스
기본조건	ISO/IEC 17025	ISO/IEC 17025	ISO/IEC 17025	ISO/IEC 17025	ISO/IEC 17025	EN45001
기본조건 포함문서	NIST Handbook 150	CAN-P-4D	JIS Q 17025	UKSP 01 18조 명시	AISEP Publication No1. 명시	ECF02
부가조건 포함문서	NIST Handbook 150-20	CAN-P-1591				

5. CAP 국가의 평가기관 평가자 비교 분석

CCRA의 평가기관 인정을 위한 조건에서는 평가자에 대한 요구사항으로"각각의 스킴의 공인 정책에는 보안 요건과 훈련 요건의 세부항목이 포함되어 있다"라는 내용이 정리되어 있다. 그러므로 평가기관으로 인정을 받기 위해서는 각 스킴의 정책 내에 평가자의 훈련요건에 대한 내용이 정리되어 있어야 한다. CAP 국가들의 평가기관 평가자를 비교하면 다음 표4와 같다.

표 4: CAP 국가들의 평가기관 평가자 비교

	미국	캐나다	일본	영국	호주	프랑스
자격	O	O	O	O	O	O
훈련 프로그램	O	O	O	O	O	O
등급 구분				O	O	
등급별 자격				O	O	

각 나라들의 평가기관 인정조건 요구사항을 분석해 보면 CCRA 평가기관 평가자 요구사항을 만족하기 위하여 모든 나라들이 평가지의 자격과 훈련 요건에 대한 항목을 채택하고 있으며, 그 중에서도 영국과 호주 등은 평가자들을 3개의 등급으로 구분하여 등급별 자격과 등급별 평가원이 되기 위한 훈련 프로그램을 자세하게 정리하고 있다.

6. 평가기관 요구사항 비교 분석

앞 절의 CAP국가의 평가기관 요구사항 항목별 비교 분석한 결과를 CCRA요구사항과 CCRA가입을 위해 필요한 평가기관 요구사항과 같이 요약 정리하면 다음 표 5, 표 6과 같다.

표 5: 평가기관 요구사항 비교(1)

항목	CCRA	미국	캐나다	일본
인가	CB에 의한 인가가 필요함	1단계 인증절차	1단계 인증절차	1단계 인증절차
인정절차	공인신청 절차의 세부항목	인정신청	인정신청	인정신청
		인정심사	인정심사	인정심사
		인정결정	인정결정	인정결정
운영	공인신청 처리의 세부항목	범위변경		범위변경
		인정종결		인정종결
		재평가		재평가
		중지,취소	중지,취소	중지,취소
		분쟁처리		분쟁처리
인정조건	ISO/IEC 17025 EN45001	ISO/IEC 17025	ISO/IEC 17025	ISO/IEC 17025
부가조건		NIST Handbook 150-20	CAN-P-1591	
평가자	훈련 요건의 세부항목	자격	자격	자격
		훈련 프로그램	훈련 프로그램	훈련 프로그램

표 6: 평가기관 요구사항 비교(2)

항목	영국	호주	프랑스	필요한 평가기관 요구사항 항목
인가	2단계 인증절차	2단계 인증절차	2단계 인증절차	1단계 인증절차
인정 절차	인정신청	인정신청	인정신청	인정신청
	인정심사	인정심사	인정심사	인정심사
	인정결정	인정결정	인정결정	인정결정
운영	범위변경			범위변경
	인정종결	인정종결	인정종결	인정종결
	재평가	재평가	재평가	재평가
	중지,취소	중지,취소	중지,취소	중지,취소
	분쟁처리	분쟁처리	분쟁처리	분쟁처리
인정 조건	ISO/IEC 17025	ISO/IEC 17025	EN45001	ISO/IEC 17025
부가 조건				평가기관요구사항
평가자	자격	자격	자격	자격
	훈련 프로그램	훈련 프로그램	훈련 프로그램	훈련 프로그램
	등급구분	등급구분		등급구분
	등급자격	등급자격		등급자격

V. 결 론

본 논문에서는 정보보호제품의 평가 수요 증가에 적극적으로 대처하고, 양질의 평가 서비스 제고를 위한 CCRA 요구사항 수준의 평가기관 요구사항을 도출하기 위하여, CCRA 평가기관 요구사항을 분석하고, CCRA 평가기관 인정조건인 ISO/IEC17025의 요구사항을 분석하였다. 그리고 NIST Handbook 150, NIST Handbook150-20 등 CAP국가들의 평가기관 인정과 관련된 표준문서들을 연구하여, 각 CAP국가들의 평가기관 요구사항들을 분석하였으며, 평가기관의 평가자 양성을 위한 교육 및 자격부여 프로그램들을 비교 분석하였다. 앞의 분석한 결과를 바탕으로 평가기관 요구사항으로 평가기관 인정절차, 평가기관 운영, 평가기관 인정조건 및 부가조건 그리고 평가자와 관련된 항목들을 도출하였다. 본 논문의 연구 결과를 통하여 새로운 평가기관의 선정을 위한 기초 자료로 활용이 가능하며, 평가기관의 인력 양성을 위한 프로그램 개발에 대한 기초 자료로도 사용이 가능하리라 생각된다.

참고문헌

[1] ISO/IEC 17025 - General requirements for the compentence of testing and calibration laboratories

[2] KOLAS SG-1 시험 및 교정기관 자격에 대한 일반 요구사항 및 해설

[3] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Part 2: Security functional requirements, Part 3: Security assurance requirements, Common Criteria Interpretations Management Board.

[4] Common Methodology for Information Technology Security Evaluation, Part I: Introduction and General Model, Part II: Evaluation Methodology, Common Evaluation Methodology Editorial Board.

[5] NIST Handbook 150, Procedures and General Requirements

[6] NIST Handbook 150-20, Information Technology Security Testing Common Criteria

[7] Guidelines for the Accreditation of Information Technology Security Evaluation and Testing Facilities(CAN-P-1 591)

[8] Candian Common Criteria Evaluation and Certificate Scheme sponsored by Communications Security Establishment, from Canada

[9] UK Scheme Publication No 1 Description of the Scheme

[10] UK Scheme Publication No 2 - The Appointment of Commercial Evaluation Facilities

[11] ECF 02 - Licensing of the IT security evaluation facilities

[12] Scheme d'Evaluation et Certification Francais sponsored by Service Central do la Sécurité des Systémes d'Information, from France

[13] AISEP Publication No 1 Australasian Information Security Evaluation Program

[14] AISEP Publication No 2 -Framework for the Selection and Licensing of Australasian Information Security Evaluation Facilities