[정보보안] CC의 국제표준 개정을 위한 긴 여정이 시작되다.

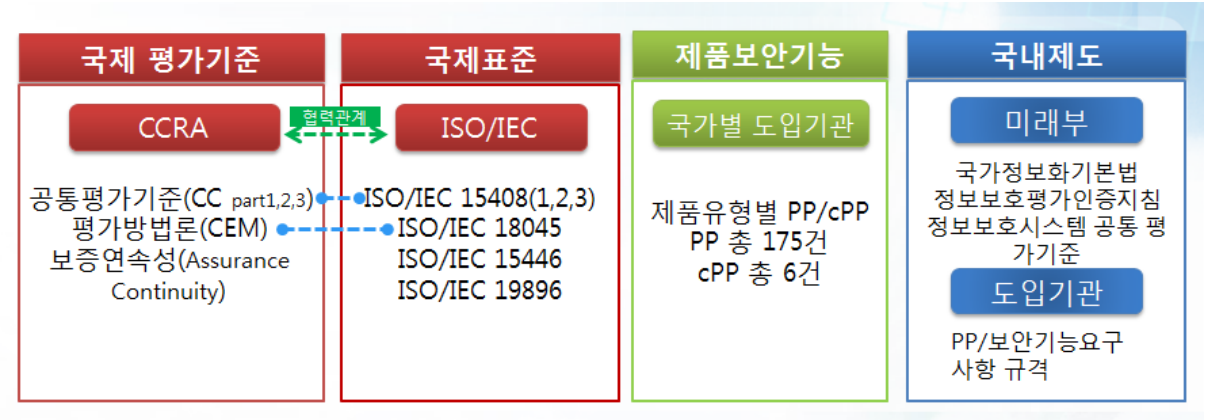
개요

IT제품의 보안성 평가 기준을 다루고 있는 공통평가기준(CC : common Criteria)은 국내에서 'CC인증'으로 많이 알려져 있다. CC는 공통평가상호인정협정(CCRA)에 의해 25개국에 통용되고 있으며 2005년에 ISO/IEC 15408과 ISO/IEC 18045로 등록된 후 3차례 개정되었다.

CCRA에 가입하지 않은 중국과 러시아는 ISO/IEC 15408과 ISO/IEC 18045를 활용하여 자국의 IT제품들에 대한 보안성을 검증하는 제도에 활용하고 있다.

공통평가기준 관련 표준들의 개발

IT제품의 보안성 평가를 위한 관련 국제 표준은 아래 그림과 같이 CCRA와 ISO/IEC에서 주로 만들어 지고 있다.



[그림1] 보안성 평가 관련 표준 및 기준 문서들의 개발

CC는 공통평가기준 상호인정협정(CCRA)에서 만들어 지고, ISO/IEC에서 국제표준으로 작업된다. CCRA의 CC는 Part1 일반 개요, part2 보안기능 요구사항, part3 보안보증 요구사항로 구성되고 각 part가 ISO/IEC 15408과 매핑된다. CCRA의 평가방법론인 CEM은 ISO/IEC 18045와 매핑된다. 각 제품별 보안성 기능에 대한 기준을 포함하는 보호프로파일(PP)는 각 나라마다 제품의 특성을 반영하여 만들어져 CCRA 포탈 사이트에 총 175건이 등재되어 있다. 국내의 경우에는 해외 평가

방법론을 수용하며 국내 환경에 적합하도록 다양한 보안 규격들이 추가적으로 개발되어 있다. 이러한 각국의 노력은 IT제품의 보안성을 검증하는 방법론이 정착하는데 도움이 되었으나, 새로운 기술의 변화에 신속하게 대응하지 못하는 부분과 제품별 보안 기능의 규격을 각각 개발하여 적용하는 것에 대한 이슈을 갖게 되었다.

CCRA의 CC개발위원회 (CCDB)는 연구 분야별 기술그룹(iTC)을 구성하고, 각 국의 전문가 참여를 통해 공동 보호프로파일(cPP : collaboration PP)과 cPP 평가를 지원하는 문서(SD :supporting document)를 개발하고 평가에서 적용을 추진하고 있다.

ISO의 각 국 전문가들은 cPP가 보호프로파일의 확장된 형태로 인지하고 SD와 함께 평가의 실무영역을 지원하는 매우 실질적인 기준으로 보고 있다. 그리고 IOT, Cloud, 프라이버시, 바이오 영역 등 다양한 산업 분야에서 개발된 IT 제품에 대한 보증 요구에 대한 지원, 문서 중심의 보증 작업과 취약성에 대한 보증 이슈, 여러 표준 또는 실무 기준서들의 일관성 저하 등의 이슈 사항들을 국제표준의 개정방향으로 검토해왔다. 이에 ISO/IEC JTC1 SC27의 WG3에서는 ISO/IEC 15408과 18045의 개정을 위한 준비로 1년 동안의 연구기간(SP: Study period)를 갖고 지난 10월의 아부다비 회의에서 개정 중점 사항을 정리하여 ISO/IEC 15408과 ISO/IEC 18045의 개정 및 신규 표준을 제안하였다.

개정 방향

국제 표준의 개정은 과거의 개정과 다르게 좀 더 큰 폭의 개정이 이뤄질 예정이다. ISO/IEC 15048에는 Part4(평가 방법과 활동의 명세를 위한 프레임워크)와 와 Part5(이미 정의된 보안요구사항 패키지)를 추가하고, 신규 프로젝트로 ISO/IEC 15408과 ISO/IEC18045 리비전에 대한 추적성과 변경 사항의 매핑, 연구기간(SP)중에 제시되었던 사항들의 반영 여부들이 포함될 예정이다. 평가자들이 평가시 활용하게 되는 ISO/IEC 18045는 ISO/IEC 15408의 변경된 사항을 포함하여 개정 작업이 이뤄진다.

CC와 CEM의 개정 작업은 긴 여정이 될 것이다. 약 2년 간의 WD(Working Draft)과정 이후 다시 약 2년 간의 국제 표준문서가 만들어지는 단계인 CD-DIS-FDIS의 과정을 거쳐 최종 국제 표준으로 나오게 될 것이다. 물론 각 단계마다 ISO/IEC와 CCRA의 CCDB간 긴밀한 상호 연락을

통해 세부 사항이 지속적으로 토의될 예정이다. CCRA는 국제적인 상호 인정 협정으로 주로 각 국의 정부 기관 전문가 참여로 이뤄지며 민간 전문가 참여가 제한적인 것에 반에 ISO/IEC는 해당 분야의 모든 전문가 참여가 가능하다. CC 개정의 긴 여정은 폭 넓은 각 국 전문가들의 참여로 인해 더욱 가치있는 작업이 되고, 현재의 기술 트랜드를 반영하는 합리적인 보안성 검증 기준이 되길 기대해 본다.

이수현 (㈜윈스 보안인증팀장, leeshn@wins21.co.kr)