[CC인증 국제 동향] CC인증의 개선 방향은?

공통평가기준(CC: Common Criteria for Information Technology Security Evaluation, 이하 CC)은 IT제품의 보안성 평가에 사용되는 기준으로 한국을 비롯하여 세계 25개국에서 사용하고 있는 표준이다. CC는 공통평가상호인정협정(CCRA)에서 개발되어 1999년 ISO/IEC 15408로 국제 표준으로 등록되었다. ISO/IEC 15408은 part1 일반사항, part2 보안기능요구사항, part3 보증요구사항으로 구성되어 있다. 평가방법론(CEM: Common Methodology for Information Technology Security Evaluation)은 ISO/IEC 18045로 등록되었다. 2005년, 2008년 2차례 개정되었으며, 2015년 CCDB에서 CC와 CEM의 개정을 결정하여 ISO/IEC JTC1 SC27의 WG3와 연구프로젝트(SP:study pierod)를 시작하였다.

ICT기술이 발전하며 CC는 취약점 보증, 효율성과 효과성 등 여러 가지 문제점을 갖게 되었으며, CCRA의 CCDB는 CC사용자포럼(CCUF: Common Criteria Users Form)와 협력관계를 통해 해결을 위한 노력을 하고 있다. CCUF는 2014년 5월에 만들어진 커뮤니티로 미국의 시스코, 오라클, 마이크로소프트와 같은 글로벌 벤더가 리드하고 있으며, 전세계 회원수는 532명으로 학교, 컨설턴트, 시험 평가기관, 사용자, 정책기관, 표준화기관, 벤더 등이 참여하고 있다.

CC 무엇이 문제인가?

CC는 IT제품의 보안성을 보증하는 하나의 방법으로 보안에 대한 위협과 조직의 보안정책을 명확하게 표현하고, 제안된 보안 수단이 본래 의도된 목적을 만족시키는데 충분함을 입증하는 철학을 갖는다. 따라서 CC인증을 받고자 하는 개발자는 개발된 IT제품에 대해 보안문제에 대한 정의와 보안목적, 보안요구사항을 식별하고 보증요구사항을 만족하여 평가를 신청한다. 평가자는 개발자가 제공하는 증적을 평가하여 기준에 부합하는지 확인하고 최종 IT제품을 보증하게 된다.

CC가 국제 표준으로 등록되고 16년 동안 여러 나라에서 CC평가제도가 운영되며 여러 문제점들이 발생되었다. CC 평가에서 활용되는 증적은 주로 문서 위주로, 개발자는 개발에서 산출된 결과물의 형태와 다르게 CC인증을 받기위해 많은 양의 문서를 작성해야 했다. 또한 기술의 변화에 따라 IOT 또는 Cloud 환경에서 사용되는 다양한 제품들이 개발되며 CC평가가

제품의 다양한 특성을 포함할 수 있는 유연성을 갖고 있는지 고민하게 되었다. 그리고 개발자들은 CC평가에 소요되는 비용과 기간 그리고 평가가 개발자가 기대하는 목적을 만족하는지 효율성과 효과성에 대해 연구하고, 개발자들이 사용하는 다양한 개발 방법론과, 자동화 도구를 CC평가에서 활용하여 인력투입과 비용을 줄이고자 하는 CC의 변화를 요구하게 되었다. CCRA는 개발자, 평가자, 고객의 이해관계자 간의 상충되는 이해관계를 조정하며 CC와 CEM의 개정을 추진하게 되었다.

올해 4월 한국와 미국에서 두 건의 회의가 개최되었다. 4월초 한국에서 있었던 회의는 CCRA의 CCDB와 CCUF의 공동 회의로, 한국의 CC사용자 포럼(KCCUF)가 회의에 참여하였다. 4월 중순 미국 탬파에서 열린 ISO/IEC JT1 SC27 회의에서는 ISO/IEC 15408과 ISO/IEC18045의 개정에 따른 토의가 진행되었다. 어떠한 방향으로 개정을 진행할 것이지 각 국의 전문가들에 의해 9개의 주요토픽이 선정되었다.

선정된 핫토픽

1. 표준의 일관성

표준의 일관성은 CC와 CEM의 전반적인 부분에서 대해 검토하는 것으로, CC가 보안성을 보증하는 일반적인 모델이고, IT제품에 대한 보안요구사항으로 작성되는 보호프로파일(PP: Protection Profile)이 현재 상태로 충분하며 더 개선할 사항은 없는지, 개발자가 작성하게 되는 IT제품의 보안요구사항과 보증 요구사항은 현재 상태로 충분하며 개선사항이 없는지 점검한다. 보안요구사항을 설명하는 구조의 컴포넌트와 클래스, 패밀리에 대한 개념이 적절한지 일관성 관점에서 재점검한다.

2. 증거 요구사항의 명확성과 간소화

증거 요구사항의 명확성과 간소화는 보안성 보증을 위해 평가시 개발자에게 요구할 증적과 증적이 타당한지, 제공된 증적이 명확한지, 개발자 부담을 줄이기 위해 할 수 있는 방안은 없는지 검토한다.

3. CEM의 재조정

CEM의 재조정(reposition)은 평가방법론에 대한 검토이다. CEM은 평가과정과 평가 업무에 관련된 사항, PP와 ST의 평가, 개발, 설명서, 생명주기, 시험, 취약성 등의 평가활동을 규정하고 있다. 이러한 평가활동 중에 중복된 평가활동은 제거하거나 줄이고, 취약성 평가 활동중 제품의 잠재적인 공격에 대한 계산 방법과 계산 결과가 의미 있는지 점검하고, 추가적으로 필요한 사항과 개선할 사항에 대해 검토한다.

4. 모듈화

모듈화는 이미 2014년도에 CCDB에서 승인한 모듈러 PP(Modular PP)를 ISO/IEC 15408에 반영하여 개정하는 것이다. 모듈러 PP는 기존에 개발된 여러 PP를 기반으로 새로운 PP를 만들어 사용하는 것이다. 이러한 모듈러 PP의 사용은 새로운 유형 제품의 PP개발에 유연하게 적용될 수 있다.

5. 취약성 보증 검토

취약성 보증 검토는 용어 정의, 제품의 생명주기, 고객의 가치, 책임성의 4가지 세부 토픽으로 검토되고 있다. 취약점 검토는 제품이 개발되는 과정 즉, 개발 모델과 프로세스, 또한 제품의 설계, 구현, 시험 등 각 내부 절차와 고객에게 제품이 전달되는 배포과정에서도 이뤄진다. 이렇게 개발 과정에서부터 배포과정에 이르는 전반적인 절차에서의 취약점 보증과 공격자의 공격 경로, 침입 위치 등이 모두 가정사항으로 고려되어 보증되고 있는지 검토한다. 또한 식별된 취약점에 대한 처리 방법으로 어떠한 방법론을 보유하는지 ISO/IEC 15408에서 이러한 사항들을 포함하고 있는지 관점에서 검토한다. 그리고 고객의 위험관리를 지원할 수 있도록 더 많은 가이드를 필요로 하는지와 취약점 보증을 통해 안전한 상태를 유지하기 위한 최선의 방법을 제안할 수 있을 것인지 검토한다. 책임성은 취약점 목록을 업데이트할 주체와 인증된 제품에 잔류 취약점이 없다고 보증할 수 있을 것인가에 대한 검토이다.

6. 일관성 있는 표준 매트릭스

CC에서 많은 보증 및 평가 활동들이 매트릭스 없이 수행되고 있는데, 활동의 효과성을 보장하기 위해 일관성 있는 표준 매트릭스가 필요하다는 것이다. 이번 CC와 CEM의 개정 연구 프로젝트에서 전문가들의 의견을 받아 매트릭에 대한 제공과 방법을 찾아 표준 개정에 반영하는 것이다.

7. CC의 차이

CC의 차이에 대한 검토는 CCRA 내부와 외부 이해 관계자들의 CC 사용에 대한 생각을 이끌어 내는 것이다. CC 및 CEM 사용자는 IT제품을 개발하여 평가를 받고자 하는 개발자와 기준에 따라 평가를 수행하는 평가기관, 그리고 평가된 제품을 사용하는 고객으로 그들 간의 이해 관계는 상당히 복잡하다. 따라서 ISO/IEC 15408에 대한 유효성을 다시 검토하여 IT제품에 대해 보안성 보증이 필요한 곳이라면 본 표준을 사용할 수 있도록 유연하게 대응 가능한지 검토한다.

8. 개발 프로세스와 더 나은 활용

개발 모델과 프로세스 활용은 평가시 벤더가 사용하고 있는 개발 모델과 절차를 CC평가에 증적 자료로 사용할 수 있을 것인가에 대한 검토이다. 개발자들은 제품 개발을 위해 조직내 정의된 개발 방법론을 적용하여 제품을 개발하고, 제품에 대한 전반적인 생명주기를 관리하게 된다. CC part3에 평가제품의 보증에 대한 요구사항으로 생명주기지원(life-cycle support)를 요구하고 있다. ALC는 형상 관리(ALC_CMC)와 형상의 범위(ALC_CMS), 배포(ACL_DVS), 개발 보안(ALC_DVS), 취약점 조치(ALC_FLR), 생명주기의 정의(ALC_LCD). 도구 및 기술(ALC_TAT)로 구성된다. CEM은 평가 방법론으로 ALC에 따른 평가 방법을 기술하고 있다. 그 동안 CC 평가를 받는 개발자들은 CC에서 정해진 요구사항에 따라 절차와 문서를 만들고 필요시 시스템을 구축하기도 했다. 하지만 이러한 증적을 개발자가 자체적으로 구축하고 있는 개발 방법론과 절차에서 산출된 결과물을 CC인증의 평가 증적으로 사용할 수 있는가에 대한 재검토를 한다.

9. 도구와 기술 검토

도구와 기술에 대한 검토는 CC part3 생명주기 지원의 개발에 사용되는 도구와 개발자가 구현에

사용하는 도구에 대한 보증을 포함한다. 도구 및 기술(ALC_TAT)은 ALC_TAT.1 잘 정의된 개발 도구(Well-defined development tools), ALC_TAT.2 구현 표준 준수(Compliance with implementation standards), ALC_TAT.3 모든 부분에서 구현 표준 준수(Compliance with implementation standards - all parts)로 구성된다. 본 토픽은 개발자와 평가자 관점에서 도구와 기술의 적절성을 검토하는 것이다. 또한 개발자는 자동화된 형상도구를 사용하고 있으므로 증적자료로 문서화 요구를 재검토 한다.

추후 방향

ISO 전문가들에 의해 선정된 9개 토픽은 그 동안 개발자와 평가자들이 평가 중에 겪는 현실적인 차이를 정리한 것이다. 선정된 9개 주제는 올해 9월 터키에서 열리는 CCDB와 CCUF의 회의에서 다시 토의될 예정이다. 개정안이 국제표준으로 승인되기 까지는 약 3년 정도 소요될 것으로 보인다. ISO 국제 전문가들과 CCDB, CCUF 관계자들은 활발한 교류를 통해 IT제품의 보안성을 보증하기 위해 더 실질적인 방향으로 CC를 바꿔 나갈 것이다.

이수현 (윈스 팀장, leeshn@wins21.co.kr)