[정보보안] CC의 국제 표준 개정 시작, 2020년 발행 예정

1. 개요

공통평가기준(CC, Common Criteria)의 국제표준은 ISO/IEC15408, ISO/IEC18045로 CC인증에 관련된 업무를 수행하는 사람들에게는 바이블이나 다름없다. 국제표준 개정을 위해 1년 넘게 연구기간(SP, Study Period)을 거치고, 문서 작업을 위해 지난 4월 뉴질랜드 해밀턴 회의에서 한국, 미국, 영국, 독일, 프랑스, 폴란드 6개국에 11명의 에디터를 선정하였다. 11월 베를린 회의에서 중국과 남아프리카공화국의 전문가가 에디터로 추가 선정되어, 총 13명의 에디터가 ISO/IEC15408, ISO/IEC18045, ISO/IEC22216의 개정 작업을 진행한다. 한국은 총 3명이 에디터로 참여하고 있다.

평가기준 ISO/IEC15408은 Part1~5까지 5개 파트로 재구성되고, 평가방법론 ISO/IEC18045는 ISO/IEC15408의 변경 사항을 포함하여 개정한다. 변환 가이드인 ISO/IEC22216은 구 버전에서 신규 버전으로 변경된 사항을 설명하고, 사용자들의 개정된 버전에 대한 이해를 돕는다. CC 관련된 7건의 국제표준과 변경 사항은 <표 1>과 같다.

<표 1> CC 관련 7건의 국제표준과 변경 사항

ISO/IEC	타이틀	진행 정도	변경 사항	에디터
15408-1	Evaluation criteria for IT security -- Part 1: Introduction and general model	개정	IT보안 평가를 위한 소개 및 일반 사항 검토, 용어 재정의	Fiona Pattinson (미국) Guillaume Tétu (프랑스) Elzbieta Andrukiewicz (폴란드)
15408-2	Evaluation criteria for IT security -- Part 2: Security functional components	개정	기존 보안 기능 요구사항 검토, 신규 추가 검토	Fiona Pattinson(미국) Nicholas Muthambi(남아공) Shi Hongsong (중국)
15408-3	Evaluation criteria for IT security -- Part 3: Security assurance components	개정	보증 활동 요구사항 검토, 신규 보증 사항 추가	Christian Noetzel (독일) Soohyeun Lee (한국)
15408-4	Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities	신규	PP와 ST, SD등을 활용한 평가방법과 보증 활동의 프레임	Dietmar Bremser (독일) Helmut Kurth (미국) Tony Boswell (영국)
15408-5	Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements	신규	평가 보증레벨, 합성평가	Fiona Pattinson(미국) Heebong Choi (한국)

18045	Methodology for IT security evaluation	개정	ISO/IEC15408에서 변경된 사항 반영한 평가방법론	David Martin (영국) Kwangwoo Lee (한국)
22216	Introductory guidance on Evaluation for IT security	신규	구 버전에서 신규 버전으로 전환 가이던스	Guillaume Tétu(프랑스) Fiona Pattinson(미국)

2. 모듈라이제이션, 정확한 준수, 패치관리, 퍼징 시험

ISO/IEC15408의 1차 WD문서에는 지난 4월 CCRA에서 발표한 CC V3.1r5가 반영되었고, 5월에 발표한 정확한 준수(Exact Conformance)사항이 반영된 상태였다.

- **Part1**은 PP와 ST의 모듈라이제이션, 정확한 준수에 관련된 사항이 포함되고, 용어에 대해 전반적인 검토가 이뤄졌다.
- **Part2**는 cPP에 적용된 보안기능 요구사항들이 포함되었다. 하지만, 특정 기술 분야에 적용되는 보안기능 요구사항들은 제거하는 것으로 하였다.
- **Part3**은 모듈라이제이션과 정확한 준수, TOE의 재구성에 대한 보증요구사항들이 논의되었다. 또한 퍼징테스트의 추가와 패치관리에 대한 요구사항은 가장 논의가 많이 된 이슈들로 패치관리는 SP에서 연구하기로 하고, 퍼징테스트는 다음 회의에서 더 논의하기로 하였다. 생명주기지원(ALC)에 대한 보증은 ISO/IEC27001과 같이 다른 표준에서 보증하고 있는 사례을 조사하여 제품 개발 환경에서의 보안성을 보증할 수 있을 것인지 SP를 하기로 하였다.
- **Part4**는 CEM에서 정의된 평가활동에 대해 신규 활동이 필요한 경우 작업단위(work unit)를 어떻게 도출하여 평가 할 것인지에 대한 방향성으로 문서 목적을 명확하게 하였다.
- **Part5**는 PP의 평가관련 패키지들에 대한 내용을 Part3과 Part5로 위치를 조정하고 비기능 패키지에 대한 사항은 Part5에 남기는 것으로 하였다.

ISO/IEC18045는 Part3과 Part4의 내용이 어느 정도 정리되는 시점에 업데이트를 하고, **ISO/IEC22216**은 다른 파트 문서들의 변경을 지속 모니터링하여 작업을 계속하기로 하였다.

3. 맺음말

IT기술의 변화는 평가기준도 계속 진화 할 것을 요구하고 있다. 이번 회의에서는 IT제품을 개발하고 있는 조직의 개발활동과 패치관리를 커버할 수 있는 평가방법에 대한 연구, 타 표준의 보안과 관련된 보증활동 사례 조사에 대한 연구가 제안되었다. 또한, 지난 2년간 진행해 오던 암호모듈의 시험자와 CC인증 평가자의 자격 요구사항에 대한 표준이 FDIS와 DIS로 진행되며, 추가로 평가기관의 자격 요구사항에 대한 연구가 제안되었다. 평가기관들은 이미 ISO/IEC17025를 통해 시험기관 능력을 인정받지만, CC인증에서 특화된 사항들을 포함할 것으로 전망된다.

IT보안성 평가에 관한 국제표준 전문가들은 지금 어느 때보다 조심스럽게 기술 변화를 실감하며, 더 나은 변화를 향해 움직이고 있다. 13명의 에디터들은 2020년 발행을 목표로 2018년도 4월 중국 우한에서 열릴 회의 준비를 시작하고 있다.

이수현 (㈜윈스 보안인증팀장, leeshn@wins21.co.kr)

[주요용어풀이]

CCRA: Common Criteria Recognition Arrangement

PP: Protection Profile

ST: Security Target

cPP: Collaborative Protection Profile

TOE: Target of Evaluation

CEM: Common Methodology for Information Technology Security Evaluation