정 보 보 호 학 회 지
제 31 권 제4호, 2021. 8

CC 평가인증 기술 ISO/IEC 국제 표준화 동향

이 광 우*, 이 수 연**, 황 현 동***, 성 정 호****, 최 희 봉*****

요 약

공통평가기준(CC, Common Criteria)의 국제 표준인 ISO/IEC 15408, ISO/IEC 18045는 정보보호제품에 구현되어 있는 보안 기능의 보증과 안전성을 시험하기 위한 평가 기준을 제시하는 국제 표준으로 정보보호제품에 대한 국제적인 신뢰성을 보장할 수 있도록 기준을 제시하고 있다. 특히 ISO/IEC 15408, ISO/IEC 18045는 ISO/IEC 27000, ISO/IEC 19790과 함께 ISO/IEC JTC 1/SC 27을 대표하는 국제 표준이다. 본 논문에서는 ISO/IEC JTC 1/SC 27/WG 3 작업반에서 개정을 진행하고 올해 말에 출판 예정인 ISO/IEC 15408 및 ISO/IEC 18405의 주요 변경 내용 및 신규 개념에 대해 설명하고, 최근 WG 3 작업반에서 추진하고 있는 국제 표준화 활동 현황 및 주요 현황을 소개하고자 한다.

Ⅰ. 서 론

ISO/IEC JTC 1/SC 27 (Information security, cybersecurity and privacy)은 정보보안 기술에 대한 국제 표준 개발을 진행하고 있다. 산하 WG 3 작업반(Working Group)에서는 보안 평가, 시험 및 규격(Security evaluation, testing and specification)을 다루고 있으며, IT보안성 보증 및 평가와 관련된 국제 표준을 개발하고 있다. 특히 공통평가기준(CC, Common Criteria)의 국제 표준인 ISO/IEC 15408 및 ISO/IEC 18045는 정보보호제품에 구현된 보안기능의 보증과 안전성을 평가하기 위한 기준을 제시하는 표준으로써, 정보보안관리시스템 (ISMS)로 알려진 ISO/IEC 27000 시리즈 및 암호모듈 시험 기술 국제 표준인 ISO/IEC 19790과 함께 ISO/IEC JTC 1/SC 27을 대표하는 국제 표준이다.

본 논문에서는 ISO./IEC JTC 1/SC 27/WG 3 작업반에서 지난 5년 간의 개정 작업을 거쳐 올해 말에 출판 예정인 ISO/IEC 15408 및 ISO/IEC 18405의 주요 변경 내용 및 신규 개념에 대해 설명하고, 최근 WG 3 작업반에서 추진하고 있는 국제 표준화 활동 현황 및 주요 이슈를 소개하고자 한다. 본 논문에서 소개하고 있는 보안 평가, 시험 및 규격은 향후 정보보호제품의 개발, 평가, 인증 및 도입에 활용될 수 있으므로, 개발업체를 비롯하여 평가기관, 인증기관, 사용자에게 유용한 정보를 제공하고, 향후 정책기관이 평가·인증 정책을 수립하는데 활용될 수 있기를 바란다.

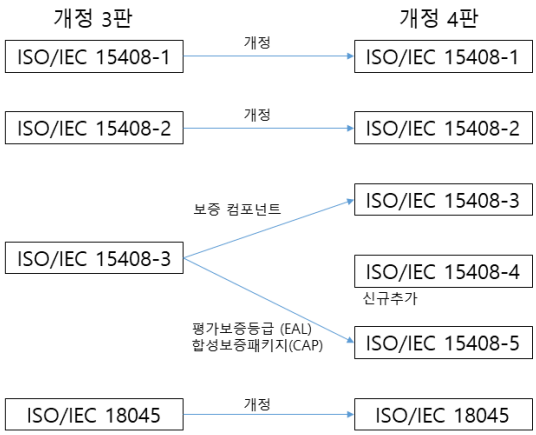
Ⅱ. ISO/IEC 15408 및 ISO/IEC 18045 개정 추진 동향 및 주요 변경사항

2.1. 개정 추진 동향

ISO/IEC 15408 및 ISO/IEC 18045는 정보보호제품 평가·인증 및 관련 정보보호제품을 개발하고 있는 업체에서 참고해야 하는 공통평가기준의 국제 표준 문서이다. WG 3 작업반에서는 2016년부터 ISO/IEC 15408 및 ISO/IEC 18045에 대한 개정 작업을 위해 연구회기(Study Period)를 진행하였고, 2017년 4월에 열린 뉴질랜드 해밀턴 회의에서 한국을 포함한 미국, 영국, 독일, 프랑스, 폴란드의 11명 전문가를 에디터(Editor)로 선정하였다. 그리고 2017년 11월 독일 베를린 회의에서 중국, 남아프리카공화국 전문가를 추가로 선정하여 13명의 에디터가 ISO/IEC 15408, ISO/IEC 18045, TR 22216의 개정 작업에 착수하였다.

* 에이치피프린팅코리아 유한회사 (마스터, kwangwoo.lee@hp.com)
** ㈜윈스 (수석연구원, ockdol@wins21.co.kr)
*** 한국정보보안기술원 KOIST (주임연구원, hdhwang@koist.kr)
**** ㈜아이큐패드 (이사, jungho.sung@iqpad.com)
***** ETRI부설 국가보안기술연구소 (책임연구원, gold@nsr.re.kr)

이번 표준 개정 작업에 있어 가장 중요한 목표는 2008년 ~ 2009년에 출판된 개정 3판 (3rd Edition)인 ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008, ISO/IEC 15408-3:2008와 ISO/IEC 18045:2008에 대하여 4차 산업 보안기술에 적용 가능한 보안 평가 접근 방법 및 최신 요구사항 (신규 보안기능 요구사항, 신규 보증요구사항)을 반영하는 것이었다. 국내에서는 정보보호제품의 보안성을 평가하는 기준으로 공통평가기준 (CC, Common Criteria)과 공통평가기준방법론 (CEM, Common Methodology for Information Technology Security Evaluation)이 잘 알려져 있으나, 이 기준은 국제상호인정협정(CCRA) 회원국이 평가결과를 상호인정하기 위해 평가·인증 업무에 적용하는 단일 평가 기준 및 평가 방법론이며, CCRA 회원국이 아닌 일부 국가에서는 ISO/IEC 15408 및 ISO/IEC 18045를 평가 기준으로 활용하고 있다[1]. 따라서, WG 3 작업반에서는 CCRA 회원국이 현재 사용하고 있는 최신 버전인 CC v3.1 R5 및 CEM v3.1 R5[2][3][4][5]를 기반으로 일부 국가에서 각기 다른 방식으로 활용하고 있는 다양한 평가·인증 방법론을 반영하고, 이에 따라 추가되는 신규 개념인 완전한 준수(Exact Conformance), 모듈화(Modularity) 등을 제시하였다. 이를 효과적으로 제시하기 위해 기존 개정 3판 (ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3)을 ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3, ISO/IEC 15408-4, ISO/IEC 15408-5로 재구성하였으며, [그림 1]과 같이 관련 내용을 신규 추가, 삭제, 변경하였다.



〔그림 1〕 ISO/IEC 15408, 18045 개정 3판 및 개정 4판의 관계

현재 ISO/IEC 15408 및 ISO/IEC 18045에 대한 개정 작업을 마무리하고 출판을 준비하는 단계에 있으며, 해당 표준에 대한 사용자들이 기존 공통평가기준/공통평가기준방법론과 동일한 방식으로 표준을 인용하여 활용할 수 있도록 하기 위한 저작권에 대한 논의가 남아 있다. 지난 2021년 4월 ISO/IEC JTC 1/SC 27/WG 3 작업반 회의에서는 2021년 말까지 출판하는 것을 재확인한 상태이다.

2.2. ISO/IEC 15408 및 ISO/IEC 18045 주요 변경사항

2.2.1. 보안평가에 대한 접근 방법

이번 개정 4판 (Forth Edition)에는 보안 평가에 대한 접근방법으로 “공격 기반 접근 방법(Attack-based approach)”과 “명세 기반 접근 방법 (Specification-base approach)”을 소개한다. 기존 개정판에도 존재하는 전통적인 방식을 공격 기반 접근 방법이라고 하며, 기존 개정판에는 없었지만, 이번 개정판에서 소개하는 방식을 명세 기반 접근 방법이라고 부른다.

공격 기반 접근방법은 조사 활동에 기반을 둔 방식으로 여전히 입증 가능한 준수 또는 엄격한 준수를 사용하며, 평가보증등급과 AVA_VAN(취약성 평가) 컴포넌트, TOE에 특화된 평가 방법론을 정의하기 위한 확장 컴포넌트 및 정교화를 사용한다. 이 방식은 새로운 공격 기법을 반영하여 평가가 이루어지므로 개발자는 평가자가 어떤 테스트를 고려하고 수행할지 완전하게 예측할 수 없다. 이 방법에서는 AVA_VAN 컴포넌트를 사용하므로 침투시험을 수행하게 된다. 즉, 평가자는 잠재적인 취약점이 존재하는지 확인하기 위해 시험 계획을 정의해야 한다. 반면에 새로운 접근 방법인 명세 기반 접근 방법은 보호프로파일 수준, 요구사항, 그리고 평가 활동의 정의를 포함한다. 이 접근방법에서는 보호프로파일에 대한 완전한 준수를 사용하며, 대부분 평가보증등급을 사용하지 않는다. 그리고 간소화된 이론적 근거 보호프로파일 및 보안목표명세서를 사용할 수 있다. 이 방법은 비록 사전에 고려하지 못한 새로운 공격 시나리오에 대해서는 새롭게 고안하여 시험을 수행되지 않지만, 평가대상이 사전에 알려져 있는 시험 집합을 만족함을 확인하는 방식이다. 따라서, 평가자는 사전에 알려져 있는 시험 계획에 따라 화이트

리스트 방식으로 시험을 진행하므로 평가기간을 단축할 수 있고, 평가 결과가 평가자의 수준에 따라 달라지는 부분을 최소화할 수 있다.

다음 [표 1]은 명세 기반 접근방법과 공격 기반 접근방법을 비교한 것이다.

〔표 1〕 보안 평가에 대한 접근 방법 비교

구분	명세 기반 접근방법 (Specification-based approach)	공격 기반 접근방법 (Attack-based approach)
평가 목표	주어진 요구사항을 기준으로 TOE가 평가되어야 함.	위협을 기준으로 TOE가 평가되어야 함.
준수 선언	완전한 준수	엄격한 준수 입증가능한 준수
보증패키지	“간소화된 이론적 근거 보호프로파일 (Direct rationale Protection Profile)” 기반 평가	평가보증등급
시험 방법	사전에 정의된 시험에 대해서는 진행함	최신 공격 기법을 고려하여 AVA_VAN을 수행함

2.2.2. 완전한 준수 (Exact Conformance)

완전한 준수는 보호프로파일/보호프로파일 합성(PP Configuration) 과 보안목표명세서 간의 계층적 관계를 정의하는 새로운 개념으로, 기존에 있던 엄격한 준수, 입증 가능한 준수에 비해 보다 완전하게 일치하는 준수를 요구하고 있다. 즉, 보안목표명세서의 모든 요구사항은 보호프로파일 또는 보호프로파일 합성으로부터 가져와야 하며, 새롭게 추가하거나 삭제할 수 없다. 보안목표명세서는 정확히 하나의 PP-Configuration에 대해서만 완전한 준수가 허용되며, 보호프로파일에 대해서는 하나 또는 그 이상의 완전한 준수가 허용된다. 만약, 보호프로파일이 완전한 준수를 기술하고 있다면 보안목표명세서는 보호프로파일을 그대로 완전하게 준수해야 한다. 예를 들어 보안목표명세서의 보안문제정의, 보안목적은 보호프로파일과 동일해야 하며, 보안기능요구사항의 보안기능요구사항은 보호프로파일의 보안기능요구사항과 동일해야 하며, 여기에 할당/선택 오퍼레이션이 수행되어야 한다.

2.2.3. 간소화된 이론적 근거 보호프로파일

전통적인 공격기반 접근방법에서는 보안문제정의(Security problem definition)에 대응하는 보안목적에서 보안기능요구사항을 도출하였다. 반면에 새롭게 도입된 명세기반 접근방법은 더 이상 보안목적을 통해 보안기능요구사항을 도출할 필요가 없어졌다. 이로 인해 보안목적 없이 위협과 보안기능요구사항을 바로 연결하는 “간소화된 이론적 근거 보호프로파일” 개념이 도입되었다.

기존 낮은 보증수준의 보호프로파일(Low assurance PP)은 간소화된 이론적 근거 보호프로파일과 일부 개념이 중복되어 삭제되었다.

2.2.4. 합성 TOE (Composed TOE)와 혼합 TOE (Composite TOE)

재사용성을 높이기 위한 모듈화 개념의 하나로 평가 프로세스의 모듈화를 제공한다. 서로 다른 TOE간에 제품을 분할하여 여러 보안목표명세서를 생성하고 구성 메커니즘을 통해 완전한 제품을 평가한다. 두 개 이상의 평가된 제품을 합성하여 TOE (Composed TOE)를 구성한 후 평가하는 방법과 기본 구성요소에 종속된 구성요소를 추가하여 혼합 TOE (Composite TOE)를 구성한 후 평가하는 방법이다.

예를 들면, 각기 다른 공급업체가 소프트웨어 및 하드웨어 계층을 각각 개발하여 하나의 제품으로 제공하는 경우, 합성 평가를 이용해 하나의 제품으로 평가할 수 있다.

2.2.5. 보호프로파일 모듈(PP-Module), 보호프로파일 합성(PP-Configuration)

재사용성을 높이기 위한 모듈화 개념의 하나로 다양한 보호프로파일의 조합이 가능하도록 보호프로파일 모듈과 베이스 보호프로파일(Base PP) 개념을 도입하고 이를 보호프로파일 합성으로 사용하는 모듈화 보호프로파일(Modular PP) 개념이 도입되었다.

새로운 제품군에 대해서는 보호프로파일을 신규 개발하지 않고 기존 보호프로파일을 재사용하는 보호프로파일 모듈을 활용할 수 있다. 스마트카드 및 모바일 장치와 같은 다양한 생태계에서 발견되는 응용 프로그

램에 대한 보호프로파일을 정의하고자 할 때, 모듈화 보호프로파일 개념을 사용하면 각 기본 플랫폼의 특정 위협을 해결할 수 있게 된다.

2.2.6. 다중보증평가 (Multi-assurance evaluation)

이전 버전의 표준에서는 전체적으로 동일한 수준의 보증 요구사항이 강제되어 각 기능에 적합한 보증 요구사항을 적용하여 평가하는데 어려움이 있었다. 이를 해결하기 위해 이기종 제품 또는 시스템을 다룰 수 있는 다중보증평가 패러다임이 생성되었다. 다양한 기능으로 이루어진 제품에서 특정 기능만 높은 보안성이 필요한 경우, 다중보증평가 패러다임을 이용해 하나의 제품 안에서 각 기능별로 각기 다른 수준의 보증 요구사항을 적용할 수 있다.

2.3. ISO/IEC 15408 및 ISO/IEC 18045 세부 변경사항

2.3.1. ISO/IEC 15408-1 변경사항 [7]

용어 정의가 검토되어 개정되었으며, ISO/IEC 15408-1에 기술된 용어만 용어 정의에 포함하도록 문서 구조가 변경되었다.

완전한 준수 개념이 도입되었다. 낮은 보증등급 보호프로파일이 삭제되었으며, 간소화된 이론적 근거 보호프로파일 개념이 도입되었다. 모듈 평가를 위한 보호프로파일 모듈 및 보호프로파일 합성 개념이 도입되었다. 그리고 다중보증평가 개념이 도입되었다.

2.3.2. ISO/IEC 15408-2 변경사항 [8]

ISO/IEC 15408-2: Security functional components는 기존 CC v3.1 R5 2부 대비 동일한 목차 구조와 유사한 내용으로 개정이 진행되었다.

다만, SFR(Security Functional Requirement)이라는 보안기능 요구사항이 변경되었다. 기존에 존재하였던 클래스 11개는 개정 중인 표준에 동일하게 존재하나, 기존의 패밀리 65개는 9개가 추가되어 74개로 패밀리 개수가 증가되었다. 기존의 컴포넌트 134개는 22개가 추가되어 156개로 컴포넌트 개수가 증가되었다. 보안기능 요구사항 변경에 대한 요약은 다음 [표 2]와 같다.

〔표 2〕 보안기능 요구사항 컴포넌트 비교

분류	CC v3.1 R5 2부	ISO/IEC 15408-2
클래스	11개 FAU, FCO, FCS, FDP, FIA, FMT, FPR, FPT, FRU, FTA, FTP	11개(동일) FAU, FCO, FCS, FDP, FIA, FMT, FPR, FPT, FRU, FTA, FTP
패밀리	65개 FAU(6), FCO(2), FCS(2), FDP(13), FIA(6), FMT(7), FPR(4), FPT(14), FRU(3), FTA(6), FTP(2)	74개(9개 추가) FAU(6), FCO(2), FCS(4), FDP(15), FIA(7), FMT(8), FPR(4), FPT(16), FRU(3), FTA(6), FTP(3)
컴포넌트	134개 FAU(15), FCO(4), FCS(5), FDP(31), FIA(14), FMT(14), FPR(10), FPT(23), FRU(6), FTA(10), FTP(2)	156개(22개 추가) FAU(16), FCO(4), FCS(14), FDP(34), FIA(15), FMT(16), FPR(10), FPT(26), FRU(6), FTA(10), FTP(5)

추가된 보안기능 요구사항 패밀리를 살펴보면 암호지원 클래스에서 FCS_RBG(Random bit generation), FCS_RNG(Generation of random numbers) 2개가 추가되었으며, 사용자 데이터 보호 클래스에서는 FDP_IRC(Information Retention Control), FDP_SDC(Stored data Confidentiality) 2개가 추가되었다. 식별 및 인증 클래스에서는 FIA_API (Authentication proof of identity) 1개가 추가되었으며, 보안관리 클래스에서는 FMT_LIM(Limited capabilities and availability) 1개가 추가되었다. TSF 보호 클래스에서는 FPT_EMS(TOE emanation), FPT_INI (TSF initialization) 2개가 추가되었고, 신뢰된 경로/채널 클래스에서는 FTP_PRO(Trusted channel protocol) 1개가 추가되었다.

주목할 사항으로 기존 대비 추가된 보안기능 컴포넌트 22개 중에 40%에 해당하는 9개의 보안기능 컴포넌트가 암호지원 클래스에서 추가되어 암호와 관련된 컴포넌트가 높은 비중을 차지하였다. FCS_RBG 패밀리에서만 6개의 컴포넌트가 추가되었으며, FCS_RNG 패밀리에서 1개의 컴포넌트가 추가되어 난수 발생 기능을 위한 보안기능 컴포넌트가 총 7개 추가되었다. 또한, 기존의 암호지원 클래스에서 존재하지 않았던 FCS_CKM.5(Cryptographic key derivation) 및

FCS_CKM.6(Timing and event of cryptographic key destruction) 암호키 관련 보안기능 컴포넌트가 2개 추가되었다.

2.3.3. ISO/IEC 15408-3 변경사항 [9]

ISO/IEC 15408가 재구성되면서 보증 패키지에 해당하는 평가보증등급(EAL), 합성보증패키지(CAP)와 관련된 내용은 ISO/IEC 15408-3에서 15408-5로 분리되었다. ISO/IEC 15408-3에는 보증요구사항(SAR, Security Assurance Requirement)에 대한 내용이 서술되어 있으며, 새로운 접근방법과 모듈화 개념 강화로 인해 엘리먼트(elements) 수준의 세부 내용이 변경된 보증요구사항(SAR)이 다수 존재한다.

기존에 존재하였던 클래스 9개는 개정 중인 표준에 동일하게 존재하나, 기존의 패밀리 46개는 6개가 추가되어 52개로 패밀리 개수가 증가되었다. 기존의 컴포넌트 96개는 10개가 추가되어 106개로 컴포넌트 개수가 증가되었다. 보증 요구사항 변경에 대한 요약은 다음 [표 3]과 같다.

추가된 보안보증 요구사항 패밀리를 살펴보면 ASE (보안목표명세서), ADV(개발), ALC(생명주기지원), ATE(시험), AVA(취약점) 클래스 각각에 혼합평가 (composite evaluation)와 관련된 _COMP 패밀리가 추가되었으며, 생명주기지원 클래스에서는 개발 프로세스의 신뢰성 평가를 위한 산출물 생성과 관련된 ALC_TDA(TOE development artefact) 패밀리가 추가되었다.

〔표 3〕 보증 컴포넌트 비교

분류	CC v3.1 R5 3부	ISO/IEC 15408-3
클래스	9개 APE, ACE, ASE, ADV, AGD, ALC, ATE, AVA, ACO	9개 (동일) APE, ACE, ASE, ADV, AGD, ALC, ATE, AVA, ACO
패밀리	46개 APE(6), ACE(8), ASE(7), ADV(6), AGD(2), ALC(7), ATE(4), AVA(1), ACO(5)	52개 (6개 추가) APE(6), ACE(8), ASE(8), ADV(7), AGD(2), ALC(9), ATE(5), AVA(2), ACO(5)
컴포넌트	96개 APE(8), ACE(8), ASE(10), ADV(19), AGD(2), ALC(21), ATE(12), AVA(5), ACO(11)	106개 (10개 추가) APE(8), ACE(10), ASE(11), ADV(20), AGD(2), ALC(25), ATE(13), AVA(6), ACO(11)

변경된 보증 요구사항 패밀리를 살펴보면 ACE(보호프로파일합성평가) 클래스가 완전한 준수, 다중보증평가, 모듈러 PP 개념을 반영하여 변경되었으며, APE (보호프로파일평가)와 ASE(보안목표명세서평가) 클래스에는 완전한 준수, 간소화된 이론적 근거 보호프로파일 및 ISO/IEC 15408-4를 사용한 평가 방법/활동의 명세가 포함되었다. 개발 클래스에서 ADV_SPM (Security policy modelling) 패밀리는 TSF의 정형화된 모델에 초점을 맞춰 재정의 되었다.

2.3.4. ISO/IEC 15408-4 변경사항 [10]

ISO/IEC 15408-4는 평가 방법 및 평가 활동의 명세에 대한 프레임워크 (Framework for the specification of evaluation methods and activities)를 제시하고 있다. 기존에 존재하지 않았던 표준으로 새롭게 추가되어 개정을 진행하고 있다.

해당 표준에서는 특정 TOE 유형이나 특정 기술 유형의 평가 상황에서 ISO/IEC 18045의 일반적인 작업 단위로부터 새로운 평가 활동을 도출하여 평가 방법으로 결합하는 방법을 명세하고 있다.

평가 방법 및 평가 활동을 도출하기 위한 절차로 2가지 방법을 가이드라인으로 제시하고 있는데 첫 번째 방법으로 보증요구사항으로부터 평가 방법 및 평가 활동을 정의하는 방법을 제시하고 있으며, 두 번째 방법으로는 보안기능요구사항으로부터 평가 방법 및 평가 활동을 정의하는 방법을 제시하고 있다.

보증요구사항 또는 보안기능요구사항으로부터 평가 방법 및 평가 활동을 정의하는 세부적인 절차는 다음 [표 4]와 같다.

해당 표준에서 평가 방법에 대해 명세하는 목적은 평가에 사용된 보증 기술이 명확하게 식별될 수 있도록 하는 것과 평가 방법이 일관성 있는 평가 결과를 뒷받침하도록 적절히 사용됨을 보장하는 것이다.

새롭게 정의할 수 있는 평가 방법 및 평가 활동에 대해 보다 구체적으로 참고할 수 있도록 다음의 세부

〔표 4〕 평가 방법 및 평가 활동 정의에 대한 가이드라인

보증요구사항	보안기능요구사항
1) 적어도 하나의 개별 평가 활동 또는 평가 활동 그룹을 도출할 수 있는 관련 ISO/IEC 18045 작업 단위 식별 2) 평가 활동이 도출되는 각 작업단위: 2-1) 수행할 특정 작업 및 평가 기준의 관점에서 새로운 평가 활동 정의 2-2) 필요한 경우 평가 활동을 평가 방법으로 그룹화 2-3) 새로운 평가 활동에 대한 근거와 이러한 평가 활동이 그룹화된 평가 방법 기술	1) 관련 SFR 식별 2) 특정 SFR에 대응할 SAR 및 해당 ISO/IEC 18045 작업 단위 식별 3) 수행할 특정 작업 및 평가 기준의 관점에서 새로운 평가 활동 정의 4) SAR의 영향을 받는 작업 단위를 새로운 평가 활동에 매핑 5) 새로운 평가 활동에 대한 근거와 이러한 평가 활동이 그룹화된 평가 방법 기술

적인 항목으로 구분하여 추가 설명을 포함하였다.

1) 평가 방법의 정의 및 유지에 책임이 있는 실체의 식별
2) 평가 방법의 의도된 범위
3) 평가 방법에 포함된 평가 활동 수행에 필요한 도구 유형 및 평가자 역량
4) 평가 방법을 적용한 결과 보고에 대한 요구사항
5) ISO/IEC 18045 각 작업 단위 식별
6) 평가 방법이 도출된 확장 보증요구사항의 식별
7) ISO/IEC 15408-1에 정의된 동사 대신 평가 활동 설명에 사용된 추가 동사

2.3.5. ISO/IEC 15408-5 변경사항 [11]

ISO/IEC 15408가 재구성되면서 보증 패키지에 해당하는 평가보증등급(EAL), 합성보증패키지(CAP)와 관련된 내용은 ISO/IEC 15408-3에서 15408-5로 분리되었다.

합성 평가와 간소화된 이론적 근거 보호프로파일과 보안목표명세서(Direct Rationale PPs 및 STs) 평가를 용이하게 하기 위한 새로운 보증 패키지가 다음과 같이 제안되었다.

- COMP (Composite Product)
- PPA (Protection Profile Assurance)
- STA (Security Target Assurance)

2.3.6. ISO/IEC 18045 변경사항 [12]

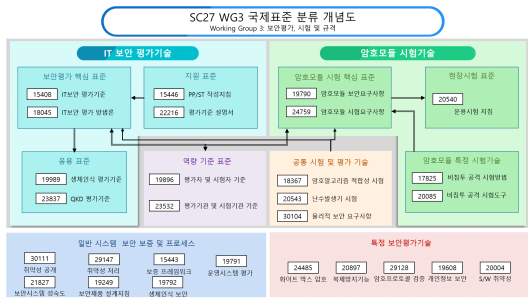
ISO/IEC 18045는 ISO/IEC 15408-3와 ISO/IEC 15408-4의 변경 사항을 반영하여 공격 기반 접근방법과 명세 기반 접근방법을 지원하는 평가 방법론이 추가되었다. 특히 “JIL Composite product evaluation for Smart Cards and similar devices”[6]의 Appendix 1.1에 정의되어 있는 ASE_COMP, ALC_COMP, ADV_COMP, ATE_COMP, AVA_COMP 등의 작업 단위가 추가되었으며, 평가 방법 및 평가 활동을 기술하고 있는 APE, ACE, ASE를 위한 새로운 작업 단위가 정의되었다. 또한 완전한 준수, 다중보증평가의 개념이 추가됨에 따라 APE, ACE, ASE에 대한 작업 단위가 정의되었고, TSF의 정형화된 모델에 대한 ADV_SPM에 대한 작업 단위가 정의되었다.

Ⅲ. 보안성 평가 관련 국제 표준화 동향

3.1. ISO/IEC JTC1 SC 27 WG 3 표준화 추진 현황

ISO/IEC JTC 1/SC 27/WG 3 표준화 현황은 [그림 2]과 같다. WG 3에 추진되고 있는 표준들은 크게 두 부류로 나눌 수 있는데, ISO/IEC 15408 IT 보안평가 기준을 핵심으로 하는 IT보안 평가기술 패밀리 국제 표준과 ISO/IEC 19790 암호모듈 보안요구사항을 핵심으로 하는 암호모듈 시험기술 패밀리 국제 표준이 있다.

SC 27 WG 3에서 진행하는 ISO/IEC 15408과 관련된 표준화 동향을 요약하면 다음과 같다.



〔그림 2〕 SC27 WG 3 국제 표준 분류 개념도

3.1.1. ISO/IEC 18367

“암호 알고리즘과 보안 메커니즘의 적합성 시험”은 암호 알고리즘과 보안 메커니즘을 기능별로 분류하고 적합성 시험에 필요한 방법론과 가이드라인을 제시하고 있다.

3.1.2. ISO/IEC 20543

“ISO/IEC 19790 및 ISO/IEC 15408에서의 난수 발생기 평가 분석 방법”은 암호모듈 및 보안시스템에 사용되는 난수발생기의 표준 모델과 함께 안전성 평가를 위한 적합성 평가 및 통계적 평가의 방법론을 제시하고 있다.

3.1.3. ISO/IEC TS 23532-1

“IT 보안 시험기관 및 평가기관 역량 요구사항”은 일반 시험기관 요구사항(ISO/IEC 17025)을 보충한 문서로써 IT보안 평가기준(ISO/IEC 15408/18045) 및 암호모듈 시험기준(ISO/IEC 19790/24759)에 특정한 요구사항을 추가로 제공하고 있다.

3.1.4. ISO/IEC 23837-1,2

“양자 키 분배 시스템의 보안 요구사항과 시험평가 방법”은 IT보안평가기준(ISO/IEC 15408)에 기반을 둔 양자 키 분배 시스템의 광학적, 비광학적 구성요소에 대한 보안 요구사항과 시험평가 방법을 명세하고 있다.

3.1.5. ISO/IEC 15408 관련 예비 작업 과제(PWI)

“ISO/IEC 15408 및 18045 유지 로드맵”은 향후 ISO/IEC 15408 및 18045 개정을 대비하기 위한 사전 연구 과제이다.

“IT 보안 평가 및 시험을 위한 인증자 역량 요구사항”은 CC 인증기관 및 암호모듈 검증기관에 근무하고 있는 인증자 역량 기준을 제시하고 있다.

“클라우드에서의 ISO/IEC 15408”은 클라우드 환경의 IT 제품에 대한 보안성 평가 방법에 관한 과제로 지속적으로 변경되는 클라우드 환경 제품의 특성을 고려한 보안성 평가 방법 제시에 목적이 있다.

“ISO/IEC 15408에 기반한 복잡한 시스템의 사이버 보안 보증”은 다양하고 복잡한 시스템에 대한 보안성 평가 방법을 제시하고 있다.

“패치 관리를 위한 ISO/IEC 15408 및 18045 확장 요구사항 생성”은 인증된 TOE 형상변경 시 이를 보증하기 위한 효율적인 방법을 제시하기 위한 과제로 예비 작업 과제에서 기술 보고서(Technical Report) 작성 단계로 진입하였다.

“ISO/IEC 15408 기반 커넥티드 카 정보보안 평가 기준”은 ISO/IEC 15408 기반 커넥티드 카 디바이스의 보안요구사항 및 평가 활동 제공에 목적이 있으며 국제 표준 문서로 작업 예정이다.

Ⅳ. 한국 WG 3 표준화 참여 동향

한국 WG 3 전문가 그룹은 ISO/IEC JTC1/SC 27/WG 3에서 수행되고 있는 CC 평가·인증기술 국제 표준화 과제들에 대해 검토하고 토의해 한국 측 기고문을 작성하는 등 한국을 대표하는 표준화 활동을 수행하고 있다. 한국 WG 3 전문가 그룹은 국가보안기술연구소 최희봉 박사, 한상윤 선연, 국민대 염용진 교수, 김예원 연, ETRI 강유성 실장, 윈스 이수현 실장, 이수연 팀장, 시큐아이 김은아 박사, 에이치피프린팅코리아 이광우 박사, 아이큐패드 성정호 이사, 시큐브 김지원 선연, KOIST 황현동 주임, KT 윤춘석 주임, 안랩 김응수 수석 등으로 구성되어 있다.

ISO/IEC JTC 1/SC 27/WG 3에서 수행되고 있는 15408-3에 코에디터 이수현, 15408-5에 코에디터 최희봉, 18045에 코에디터 이광우, 23532-1에 에디터 최희봉, 예비 작업 과제(PWI) ISO/IEC 15408 및 18045 유지 로드맵에 코에디터 최희봉 및 이광우, 예비 작업 과제(PWI) 인증자 역량기준에 코에디터 최희봉 등의 전문가가 참여해 CCRA에 가입된 전 세계 인증기관/평가기관 전문가 및 개발업체 전문가들의 의견을 검토 및 반영하는 표준화 작업을 진행하고 있다. 또한 한국 WG3 전문가 그룹은 표준 컨퍼런스 개최 및 한국 CC 사용자 포럼(Korea Common Criteria Users Forum, 이하 KCCUF) 등을 통해 선진 국제 표준 CC 평가·인증기술들을 국내 산·학·연에 전파하기 위해 노력하고 있다.

V. 결 론

본 논문에서는 ISO/IEC 15408-1,2,3,4,5 및 ISO/IEC 18405의 주요 변경 내용 및 신규 개념에 대해 설명하고, WG 3 작업반에서 추진하고 있는 국제 표준화 활동 현황 및 주요 현황을 소개하였다. 기존 CCv3.1 R5를 기반으로 개정되었기 때문에 공격 기반 접근방법으로 ISO/IEC 15408, ISO/IEC 18045를 참조하는 경우에는 기존과 크게 다르지 않다고 판단할 수 있다. 하지만, 최근 국제기술커뮤니티(iTC, international Technical Community)에서 개발하고 있는 명세 기반 접근방법을 포함하고 있고, 복잡도가 높은 고등급 평가와 모듈화 평가, 혼합 평가 등을 포함하고 있으므로 이러한 평가 방법 및 평가 활동에 익숙하지 않은 CC 평가·인증 이해당사자는 새로운 평가 방법이나 평가 활동이 다소 상이하여 개정된 국제 표준을 이해하는데 어려움이 있을 수 있다. 이러한 상황을 고려하여 ISO/IEC JTC 1/SC 27/WG 3에서는 개정된 국제 표준에 대한 변경사항을 요약 정리한 ISO/IEC TR 22216 [13]을 출판할 예정이며, 이를 통해 해당 표준 사용자들의 보다 변경된 사항을 쉽게 파악할 수 있도록 하였다.

참 고 문 헌

[1] 2019 정보보호제품 평가·인증 안내서, IT보안인증사무국, 2020

[2] Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 5, April 2017. Part 1: Introduction and general model.

[3] Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 5, April 2017. Part 2: Functional security components.

[4] Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 5, April 2017. Part 3: Assurance security components.

[5] Common Methodology for Information Technology Security Evaluation, Version 3.1, revision 5, April 2017.

[6] Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018.

[7] ISO/IEC 15408-1:20XX, Information technology - IT Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general requirements, FDIS text, 2021

[8] ISO/IEC 15408-2:20XX, Information technology - IT Security techniques - Evaluation criteria for IT security - Part 2: Security functional components, FDIS text, 2021

[9] ISO/IEC 15408-3:20XX, Information technology - IT Security techniques - Evaluation criteria for IT security - Part 3: Security assurance cmponents, FDIS text, 2021

[10] ISO/IEC 15408-4:20XX, Information technology - IT Security techniques - Evaluation criteria for IT security - Part 4: Framework for the specification of evaluation methods nd activities, FDIS text, 2021

[11] ISO/IEC 15408-5:20XX, Information technology - IT Security techniques - Evaluation criteria for IT security - Part 5: Pre-defined packagesof securit requirements, FDIS text, 2021

[12] ISO/IEC 18045:20XX, Information technology - IT Security techniques - Evaluation criteria for IT security - Methodology for IT security evaluation, FDIS text, 2021

[13] ISO/IEC JTC 1/SC 27 N21524, Text for DTR 22216, 2021

〈저 자 소 개〉

이 광 우 (Kwangwoo Lee)

종신회원

2005년 2월 : 성균관대학교 정보통신공학부 졸업
2007 2월 : 성균관대학교 일반대학원 컴퓨터공학과 공학석사
2011년 8월 : 성균관대학교 일반대학원 컴퓨터공학과 공학박사
2011년 8월~2012년 2월 : 성균관대학교 정보통신기술연구소 연구원
2012년 3월~2016년 10월 : 삼성전자주식회사 책임연구원
2016년 11월~현재 : 에이치피프린팅코리아 마스터
2016년~현재 : SC27 한국 WG3 전문가 활동
2017년~현재 : ISO/IEC 18045 Co-Editor
2018년~현재 : ISO/IEC JTC 1/SC 27/WG 3 & CCUF Liaison Officer, CCUF 관리그룹, SC27 한국 WG3 전문위원
2019년~현재 : HCD iTC 의장, CCUF 부의장
2020년~현재 : ICT 국제표준화 전문가
2021년~현재 : ISO/IEC JTC 1/S 28 Liaison Officer
<관심분야> 보안공학, 시스템보안, 정보보호 평가·인증, 정보보호 표준화

이 수 연 (Lee Su Yeon)

2012년 2월 : 성균관대학교 정보보호학 석사
2011년 7월~현재 : ISO/IEC SC27 WG3 한국 전문가 위원
2013년 6월~현재 : ㈜윈스
<관심분야> CC평가·인증 기술 표준화, 정보보호

황 현 동 (Hyundong Hwang)

정회원

2014년 2월 : 성균관대학교 시스템경영공학/통계학 졸업
2017년 2월 : 중앙대학교 융합보안학 석사
2017년 3월~현재 : ㈜한국정보보안기술원
2019년~현재 : SC27 WG3 전문가 활동
<관심분야> 정보보호 표준화, 정보보호 평가·인증, 정보시스템 감리·감사

성 정 호 (Jungho Sung)

1997년 8월 : 계명대학교 전자계산학과 졸업
2002년 3월~현재 : ㈜아이큐패드
2016년~현재 : SC27 WG3 전문가 활동
<관심분야> 문서 암호화(DRM), PC 권한조정, CC 평가·인증 기술 표준화

최 희 봉 (Heebong Choi)

종신회원

1984년 2월 : 부산대학교 전기공학과 졸업
1987년 2월 : 부산대학교 전기공학과 석사
2002년 2월 : 성균관대학교 전전컴공학부 박사
1987년 3월~2000년 1월 : 국방과학연구소 선임연구원
2014년 8월~2015년 7월 : 미국 NIST 객원 연구원
2000년 2월~현재 : 국가보안기술연구소 책임연구원
2008년~현재 : SC27 한국 WG3 전문가 활동
2021년~현재 : SC27 한국 HoD
<관심분야> 정보보호 평가/인증, 정보보호 표준화