정 보 보 호 학 회 지
제 33 권 제4호, 2023. 8

보안 평가, 시험 및 규격에 대한 국제 표준화 동향: ISO/IEC 15408, 18045 개정 로드맵 중심으로

이 광 우*

요 약

사이버 보안 기술, 위협 및 대응책이 진화함에 따라 정보보호 관련 국제 표준도 지속적인 개정이 필요하다. 특히 ISO/IEC JTC 1/SC 27 (정보보안, 사이버보안 및 프라이버시)에서는 현재까지 233개 표준 출판이 완료되었으며, 65개 프로젝트가 활발하게 진행되고 있다. 본 논문에서는 ISO/IEC JTC 1/SC 27 산하 WG 3 작업반에서 진행되고 있는 보안평가, 시험 및 규격 표준 중에서 IT 보안 평가에 활용되고 있는 ISO/IEC 15408, ISO/IEC 18045을 중심으로 표준화 진행 현황과 향후 개정 추진 방향에 대해 살펴보고자 한다. 또한, 2023년 4월에 열린 ISO/IEC JTC 1/SC 27/WG 3 작업반 회의에서 논의된 주요 표준화 이슈와 대응 방안을 제시한다.

Ⅰ. 서 론

ISO/IEC JTC 1/SC 27은 정보보안, 사이버보안 및 프라이버시((Information security, cybersecurity and privacy)에 대한 국제 표준을 개발한다. SC 27 산하에는 총 5개의 작업반이 있는데, 보안 평가, 시험 및 규격 (Security Evaluation, Testing and Specification)에 대한 표준은 작업반 3 (WG 3, Working Group 3)에서 다루고 있다. 해당 작업반에서는 IT 보안 평가 기술과 암호모듈 시험기술을 중심으로 일반 시스템 보안 보증 및 프로세스, 특정 보안 평가 기술 분야의 다양한 표준을 개발하고 있다[1].

특히 ISO/IEC 15408:2022 시리즈 및 ISO/IEC 18045:2022는 공통평가기준(CC, Common Criteria for Information Technology Security Evaluation) 및 평가방법론(CEM, Common Methodology for Information Technology Security Evaluation)의 최신 ISO/IEC 국제 표준 버전으로 잘 알려져 있으며, 2022년 8월 ISO/IEC JTC 1/SC 27에서 출판된 이후, 2022년 11월에 CCRA 포털에 CC:2022, CEM:2022 (Release 1)으로 변환되어 출판된 바 있다.

개정 작업에 앞서 2016년부터 연구 회기 (Study Period)를 진행하였고, 2017년 4월에 에디터를 선정하여 본격적인 개정 작업이 진행되었는데, 2022년 출판까지 예상치 못한 많은 어려움이 있었다.

이에 2021년 4월 WG 3 작업반 회의에서는 향후 개정 작업을 진행하기에 앞서 보다 효율적이고, 효과적인 ISO/IEC 15408, ISO/IEC 18045 개정 및 유지관리 프로세스가 필요하다는데 합의하였고, PWI TR 7677 (Roadmap for the maintenance of ISO/IEC 15408 and ISO/IEC 18045) 프로젝트가 시작되었다.

본 논문에서는 ISO/IEC JTC 1/SC 27/WG 3 작업반에서 논의된 ISO/IEC 15408, ISO/IEC 18045 표준 개정 추진 방향을 소개하고, 2023년 4월 미국 레드몬드에서 진행된 ISO/IEC SC 27/WG 3 작업반 회의에서 진행되고 있는 표준화 활동 현황과 주요 이슈를 소개하고자 한다.

Ⅱ. ISO/IEC 15408 및 ISO/IEC 18045 개정 로드맵 프로젝트 추진 배경

공통평가기준 및 평가방법론은 IT 보안 평가 업무를 수행하는 평가기관, 인증 기간 및 관련 제품을 개발하는 업체에서 참고해야 하는 필수 표준으로 간주된다. 이 표준들은 전 세계적으로 다양한 제품과 맥락에서 활용되고 있다. 특히 ISO/IEC 27000 시리즈 표준과 함께 IT 보안과 관련된 다른 표준에서 다양한 방법으로 활용되고 있다. 이러한 표준은 위협, 기술,

* 에이치피프린팅코리아 (마스터, kwangwoo.lee@hp.com)

고려 대상 제품 범위, 활용 분야 등과 같이 끊임없이 변화하는 사이버 보안 환경에 대응해야 한다.

대표적으로 ISO/IEC 15408 및 ISO/IEC 18045는 생체인식 평가기준(ISO/IEC 19989) 또는 QKD 평가기준(ISO/IEC 23837) 등의 다른 응용 표준에 프레임워크를 제공하며, 평가자 및 시험자 역량 기준(ISO/IEC 19896) 등의 표준과도 관련되어 있다.

ISO/IEC 15408 및 ISO/IEC 18045 개정을 진행하는 과정에 있어 수많은 기고서 제출이 있었는데, 이는 해당 표준에 대한 지속적인 관심이 있음을 반증한다. 또한, 2017년부터 시작된 개정은 다양한 쟁점사항으로 인해 13명의 에디터가 선정되었음에도 불구하고 정해진 개정 기간 내에 모든 의견을 수렴하지는 못했다. 따라서, 2021년 4월에 열린 ISO/IEC JTC 1/SC 27/WG 3 작업반 회의에서는 전문가 토론이 진행되었고, 차기 개정은 보다 다음과 같이 체계적인 방법으로 접근이 필요하다는데 전문가들의 의견이 수렴되었다.

2.1. 단순화 (Simplication)

단순화는 표준의 이해도와 활용성을 향상시키는 것이다.

우선 ISO/IEC 15408 시리즈와 ISO/IEC 18045 표준은 문서의 반복적, 중복적 특성으로 인해 업데이트 시 일관성을 유지하기 어렵다는 문제가 있었다. 기존 표준은 체계적인 문서 생산 시스템이 아닌 워드프로세서를 편집 도구로 사용하다 보니 편집상의 오류 발생 확률이 높았다. 따라서, 문서 구조와 편집 방법에 대한 변화가 필요하다.

또한 표준의 가치를 줄이거나 본질에는 영향을 주지 않으면서 개념과 설명을 단순화하여 표준의 가독성과 사용성을 개선해야 한다.

2.2. 간소화 (Streamlining)

간소화는 원치 않는 부작용 없이 다양한 평가 접근 유형, 즉, 명세 기반 접근 방식 (Specification-based approach)와 공격 기반 접근 방식(Attach-based approach)에 모두 적용되고, 더 쉽게 적용할 수 있도록 문서를 간소화하는 것이다. 이번 개정 작업에서 반영된 변경사항은 기존에 존재하던 공격 기반 접근 방식에 명세 기반 접근 방식이 추가되었는데, 두 가지 서로 다른 유형이 혼재되어 개념을 혼란스럽게 할 수 있고, 사용을 어렵게 할 수 있다는 문제가 지적되었다.

2.3. 명료화 (Clarification)

지침, 설명 및 예제를 요구사항과 구분하여 명확하게 제시해야 한다.

또한 ISO 편집자의 조언에 따라 ISO/IEC 15408, 18045에 활용되는 개념 및 용어를 통일하는 작업을 수행하고 별도의 파트로 분리될 것이다. 이 부분에 대한 작업은 2019년에 일부 진행되었으나, 최종 출판 과정에서 예상치 못한 일정상의 이유로 모두 반영하지 못했다.

2.4. 지연된 항목 구현

초기 연구회기 및 개정 기간 동안에 제안된 일부 변경사항은 주어진 개정 기간 내에 구현하기가 어렵다고 판단되었었고, 차기 개정에서 반영하도록 연기한 바 있다. 따라서 차기 개정에서는 우선순위를 정해 표준화 작업을 진행할 필요가 있다.

2.5. 기타 표준과의 관련성

클라우드 서비스, 양자키분배, 패치 관리, 암호화 프로토콜 검증 등의 프로젝트와 같이 ISO/IEC 15408, 18045의 일부를 사용하거나 또는 사용을 제안하는 다른 SC 27 표준이 이미 존재한다. 따라서, 표준에 요구사항 또는 평가 활동을 추가하거나 보조 문서를 통해 다양한 필요에 따라 채택할 수 있는 방법을 고려해야 한다.

현재 출판된 ISO/IEC 15408:2022 시리즈 및 ISO/IEC 18045:2022는 향후에도 지속적으로 개정 및 유지 관리가 필요하지만, 주제의 특성상 해당 작업은 매우 복잡하며, 기존에 관행에 따라 ISO/IEC JTC 1/SC 27/WG 3에서 수행하였던 유지관리 접근방법으로는 분명 한계가 있다. 따라서, 해당 표준의 접근 방법에 대해서는 실 사용자 및 이해 관계자 간에 사전 협의가 필요하며, 상당 부분 변경되더라도 유연하게 대처할 수 있는 지원이 필요하다.

Ⅲ. 차기 개정 제안 항목[2]

ISO/IEC 15408:2022와 ISO/IEC 18045와 관련하여 현재까지 제안된 차기 변경사항에 대해 PWI TR 7677의 내용을 요약하여 살펴보도록 한다[2]. [표 1]은 유지관리를 위한 로드맵 프로젝트에 제시된 변경 제안사항을 유형별도 나누고, 영향받는 문서를 식별한 것이다.

〔표 1〕 로드맵에 제안된 ISO/IEC 15408/18045 변경사항

유형	변경 제안	영향받는 문서
Simplication (단순화)	변경 C	ISO/IEC 15408-3 ISO/IEC 15408-5 ISO/IEC 18045
	변경 E	ISO/IEC 18045 (Clauses 10-18)
	편집 도구	영향 없음
Streamlining (간소화)	변경 A	ISO/IEC 15408-3 (Clauses 10, 14) ISO/IEC 18045 (Clauses 13, 17)
Clarification (명료화)	변경 D	ISO/IEC 15408-1
기타 표준과의 관련성	변경 B	ISO/IEC 15408-1 ISO/IEC 15408-3 ISO/IEC 18045
	변경 F	추후 논의 예정

3.1. 변경 A: 공격 기반 평가 접근 방식에서 표준의 유용성 향상

변경 A는 AVA_VAN 컴포넌트에 정의된 대로 평가 대상의 취약성 분석을 기반으로 하는 공격 기반 평가 접근 방식에서 표준의 유용성을 개선하는 데 중점을 둔다. AVA 컴포넌트를 포함하는 평가 보증 패키지, 특히 AVA_VAN.3 이상은 선택한 공격 성공 가능성에 대한 제품의 견고성 평가에는 거의 영향을 미치지 않으면서도 ADV 및 ATE 요구사항을 통해 제품 증거의 정확성을 평가하기 위해 상당한 노력이 필요하다.

AVA_VAN에 적용되는 SAR 정의의 구조, AVA_VAN 패밀리의 광범위한 직•간접적 SAR 종속관계, 사전정의된 평가보증등급 (EAL, Evaluation Assurance Level)에서 AVA_VAN에 대한 종속관계의 의미와 역할, AVA, ATE의 평가보고서 (ETR, Evaluation Technical Report))에 대한 ISO/IEC 18045의 요구사항 불명확성 및 비효율성 등 여러 가지에 기인한다.

공격 기반 접근 방식에서 표준의 유용성과 관련된 또 다른 측면은 공격 성공 가능성 계산에 대한 것으로, 정보가 최신 상태이고 현재 모범 사례와 일치하는지 확인하기 위해 요소와 공격 성공 가능성 참조표를 정기적으로 검토해야 한다. 이 변경의 목표는 취약성 평가에 대한 모든 평가 활동을 의미 있게 만들고 최신 평가 방법론을 보장하기 위해 표준을 개선하는 것이다. 참고로 해당 부록 B.6.2.4는 기존 CCv3.1R5와 동일한 것으로 ISO/IEC 18045:2022 개정 과정 중에는 변경사항이 없었다.

이와 관련하여 예상되는 변경은 다음과 같다.

(1) AVA_VAN 종속관계, 즉 AGD, ADV, ATE 보증 컴포넌트의 종속관계 변경이 필요하다. 변경 목표는 취약성 분석에 대한 SAR의 관련성을 크게 개선하는 것이다.
(2) AVA_VAN의 종속관계 재정의. 변경 목표는 전반적인 효율성을 개선하고 다양한 보증 패키지의 정의를 용이하도록 하는 것이다. 특히 AVA_VAN.3, AVA_VAN.4 및 AVA_VAN.5에 대한 최소한의 종속관계 집합을 식별하는 것이다. 이는 ADV_IMP와 같은 일부 관련 보증 컴포넌트의 종속관계를 검토하고 수정하는 것을 포함한다.
(3) ISO/IEC 18045는 AVA 및 ATE에 대한 보고 요구사항 정의한다. 보고 요구사항으로 인증기관의 사전 승인에 따라 샘플링 기법을 도입하는 것을 검토한다.
(4) TOE 내성의 수준을 결정하기 위해 사용되는 공격성공 가능성 계산 인용표를 업데이트해야 한다.

3.2. 변경 B: 공격 기반 평가 접근 방식: 취약성 평가 강화

공격 기반 평가 접근 방식을 사용하는 AVA_VAN에 따른 취약성 평가는 현재 SFR에 의해 공식화되고 모델링되기 때문에 주로 TSF와 함께 TOE 범위에 초점을 맞추고 있다. 이는 평가 및 취약성 평가 시 제품

의 전체가 아닌 일부만이 고려될 수 있음을 의미한다. 또한, TOE의 생명주기모델, 보안문제정의, TOE의 PP/ST에 명시된 TOE 및 환경에 대한 보안목적, TOE의 보안 아키텍처 측면이 충분히 고려되지 않을 수 있다. 따라서 취약성 평가의 초점은 TOE의 보안 평가에서 모든 중요한 보안 측면을 식별하고 적절하게 고려할 수 있도록 보장한다는 관점에서 더 넓어져야 한다.

이 변경 제안은 취약성 평가에 체계적인 접근 방식을 도입하는 것이다. ADV_ARC에서 시작하여 최소한 ALC_LCD, ATE_DPT, ATE_IND 및 AVA_VAN을 포함하는 이 접근법은 TOE의 안전한 아키텍처, 즉 보안 설계를 장려하고 평가 중에 TOE의 전반적인 보안 및 견고성을 적절하고 철저하게 분석하는 것을 목표로 한다. 이 접근 방식은 취약성 평가가 SFR에만 국한되지 않고, 구현된 보안 서비스 및 메커니즘을 갖춘 TOE의 보안 설계를 비롯하여 생명주기모델, 보안문제정의, TOE 및 운영환경에 대한 보안목적도 고려하도록 보장해야 한다.

이 목표를 달성하기 위해 위협 모델링 개념을 포함하여 기존 ADV_ARC 패밀리를 보강할 계획이다. 이러한 ADV_ARC의 변경은 각각 취약성 평가 또는 AVA_VAN에서 위협 모델 개념을 사용하기 위한 전제 조건을 구축한다. 이 접근 방식에는 ADV_ARC 및 기타 관련 기존 패밀리(특히 ADV_IMP, ATE_DPT, ATE_IND, AVA_VAN)에 대해 새로운 D (개발자 요구사항), C (증거 요구사항) 및 E (평가자 요구사항) 엘리먼트를 추가하거나 조정하는 작업이 수반된다.

이 접근 방식을 통해 개발자는 TOE의 위협과 보안 서비스 및 대응책을 모델링하고 평가자가 의미있고 효율적인 방식으로 취약성 분석을 수행할 수 있도록 지원해야 한다. 개발자의 위협 모델링 및 완화 근거는 현재 ADV_ARC를 통해서만 암시적으로 제공되고 취약성 평가에는 없는 중요한 측면이다. 물론 이러한 분석은 평가자의 취약성 평가에 본질적으로 기여하게 된다. 따라서, 위협 모델링에 대한 일반적인 요구사항과 규칙이 명시되어야 한다. 단, 유연성을 위해 어떤 위협 모델이 각 TOE 또는 TOE 유형에 특별히 적합한지는 개방되어야 한다. 보안문제정의는 정형화된 문제 설명이 포함되지만, 위협 모델링은 TOE 설계가 완료되기 전에 보안에 대한 고려사항에 중점을 둔다.

이와 관련하여 예상되는 변경은 다음과 같다.

(1) ISO/IEC 18045의 기존 ADV_ARC 관련 작업 단위는 하나의 일반 작업 단위로 병합될 수 있으며, 기존의 주요 주제인 보안 초기화, 우회 불가능성, 도메인 분리 및 자체 보호는 보다 자세한 보안 아키텍처 측면에 대한 요청에 의해 강화될 수 있다.
(2) ADV_ARC를 간소화할 수 있으며 더 많은 TOE 도메인 유형별 보안 아키텍처 측면에 중점을 둘 수 있다. 이는 ISO/IEC 15408와 관련 없이 기존 보안 아키텍처 문서를 이미 보유하고 있는 개발자를 장려하고 지원할 수 있다. 즉, ALC 클래스 개정안에 보안 개발 프로세스 (SDL, Secure Development Life-cycle)를 고려할 수 있다.

3.3. 변경 C: 보증 패키지 정의

변경 C는 모든 표준 사용자가 보증 패키지를 쉽게 정의할 수 있도록 하기 위함이다. 보증 패키지의 정의를 용이하게 하면 표준의 확장성이 향상되고 다양한 요구사항과 평가 접근 방식에 대응할 수 있다. 이와 관련하여 예상되는 변경은 다음과 같다.

(1) 보증 컴포넌트에 적용되는 종속관계, 특히 AVA_VAN.3/4/5 및 ADV 클래스에 적용되는 종속관계의 개정 및 업데이트를 통해 패키지의 근거가 종속관계와 덜 연결될 수 있다.
(2) 일부 종속관계가 적절한 정당성을 가지고 제거된 패키지로 ISO/IEC 15408-5에 새로운 사전 정의된 보증 패키지를 정의한다.
(3) 특정 사용 환경에서 사전 정의된 패키지에서 일부 종속관계를 삭제하기 위해 SAR 수준에서 사전 정의된 이론적 근거를 추가한다.

3.4. 변경 D: ISO/IEC 15408-1 구조 조정 및 간소화

변경 D는 주로 비전문가 및 표준의 모든 세부사항이 필요하지 않은 사용자를 위해 표준의 접근성을 개선하기 목적으로 ISO/IEC 15408-1의 내용을 재구성하고 단순화하는 데 중점을 둔다.

현재 ISO/IEC 15408-1에는 정보의 손실 없이 제거

할 수 있는 중복된 부분이 있다. 이러한 반복을 제거하여 보다 간결한 문서를 만들 수 있으며, 문서의 접근성 및 가독성을 높일 수 있다. 특히 패키지, 보호프로파일, 보호프로파일 모듈, 보호프로파일 구성, 보안목표명세서 및 준수 유형과 같은 개념이 설명될 때 부록과 반복되고 있다.

3.5. 변경 E: ISO/IEC 18045의 구조 조정 및 간소화

변경 E는 주로 비전문가 및 표준의 모든 세부사항이 필요하지 않은 사용자를 위해 표준의 접근성을 개선하기 목적으로 ISO/IEC 18045의 내용을 재구성하고 단순화하는 데 중점을 둔다. ISO/IEC 18045의 작업 단위 표현을 단순화하고 반복되는 부분을 제거하여 보다 간결한 문서를 만들 수 있다.

현재 보증 패밀리의 하위 레벨에 적용되는 작업 단위는 동일한 보증 패밀리의 상위 레벨에 중복된다. 이에 따라 실제로 유용한 정보를 추가하지 않고도 문서를 탐색하고 작업하는 데 시간이 오래 걸린다. 보증 패밀리에 적용되는 모든 작업 단위를 한 번에 제시하고 각각에 고유한 참조를 부여하면 이러한 반복을 피할 수 있다. 이후에는 동일한 작업 단위를 다른 수준에서 참조할 수 있다. 각 레벨에 대해 적용 가능한 작업 단위는 보증 패밀리에 대해 제시된 작업 단위 집합의 하위 집합으로 표시될 수 있다.

ISO/IEC 18045 구조의 또 다른 특징은 동일한 보증 계열의 상위 수준에서 필수 입력으로 추가된 특정 증거는 하위 수준에서 공통으로 사용되는 작업 단위에서는 고려되지 않는다는 것이다. 예를 들어, ADV_FSP.5가 ADV_FSP.1-ADV_FSP.4와 공통으로 가지고 있는 작업 단위는 변경되지 않으며, 특히 필수 사항인 구현 표현에 맞게 조정되지 않는다. 작업 단위 수준에서 반복을 제거하면 문서의 길이를 상당히 줄일 수 있으므로 사용과 유지 관리가 모두 쉬워진다.

3.6. 변경사항 F: 클라우드 환경에서의 IT 제품

기존 독립된 네트워크 운영 환경에서 운용되던 제품 및 솔루션이 클라우드 환경으로 이동하고 있다. 하지만, 현재의 ISO/IEC 15408, 18045 및 CC 인증은 이러한 변화를 뒷받침 할 수 있는 체계가 잡혀 있지 않다. 따라서, 현행 CC 인증 체계 하에서는 클라우드 환경에서의 IT 제품 평가 및 보증이 거의 불가능하다. 이러한 요소를 해결하지 못한다면, 향후 많은 사례에서 CC는 더 이상 무의미해질 것이며, 고객은 추가적인 국가별/기관별 테스트를 진행해야 할 것이다.

시장이 이러한 클라우드 기반 솔루션으로 이동함에 따라 클라우드 시나리오에 대한 보안 보증을 제공하기 위해 ISO/IEC15408의 차기 개정은 이러한 조정을 고려해야 한다.

Ⅳ. 보안성 평가 관련 국제 표준화 동향

2023년 4월 미국 레드몬드에서 진행된 제79차 ISO/IEC JTC 1/SC 27/WG 3 국제표준화 작업반 회의에서 진행된 표준화 동향을 요약하면 다음과 같다.

4.1. ISO/IEC 15408:2022, ISO/IEC 18045:2022

CCDB는 연락 리포트를 통해 ISO/IEC 15408:2022 및 ISO/IEC 18045:2022의 Legal Notices에 명시되어 있는 2개 국가(미국, 스페인)의 기관명을 변경해 줄 것을 요청하였으며, 이를 반영하기로 하였다. 또한 WG 3 작업반은 ISO Committee Manager에게 ISO/IEC 15048 시리즈와 ISO/IEC 18045를 웹사이트를 통해 무료로 제공하도록 요청하였다.

ISO/IEC 15408-2 보안기능 요구사항, I5408-3 보증 요구사항, ISO/IEC 18045 작업 단위에 대하여 XML 버전 초안과 이에 상응하는 파일이 작성되었다. XML 버전 초안 작업 진행 과정 중에 표준에서 누락된 내용들이 확인되었으며, 이들은 PWI 19562 작업에 포함될 예정이다. XML 초안은 이번 회의의 결과로 회원국 및 관련 연락기관에 배포되었으며, 검토 의견을 받아 향후 배포될 XML 버전에 추가 수정 반영하기로 협의되었다.

CCUF와 한국은 PWI 19562 (Investigation of the feasibility and implementation of changes to ISO/IEC 15408 and ISO/IEC 18045) 프로젝트의 일환으로, CC:2022 2부 및 3부의 오류사항에 대해 기고문을 발표하였으며, 표준 개발 도구과 관련하여 asciidoc 파일 개발 현황을 보고하였다. 그 밖에 독일 BSI에서는 “변경 B: 공격 기반 평가 접근 방식: 취약성 평가 강화” 및 “변경 C: 보증 패키지 정의”에 대해 진행사항을 발표하였고, 프랑스 ANSSI는 “변경 A:

공격 기반 평가 접근 방식에서 표준의 유용성 향상”에 대해 발표하였다. 스페인에서는 XML을 활용한 표준 개발 방안과 향후 계획을 공유하였다. 영국 전문가는 “CC in the Cloud” 프로젝트 진행 현황에 대해 공유하였으며, 상세 내용에 대해서는 차기 회의에서 논의하기로 하였다. 마지막으로 미국 NIAP 전문가는 PWI 19562 프로젝트의 일환으로 공급망 보안인 SBOM (Software Bills of Material)의 필요성에 제안하였다.

4.2. ISO/IEC 19790 (암호모듈 보안 요구사항), ISO/IEC 24759 (암호모듈 시험 요구사항)

ISO/IEC 19790과 ISO/IEC 24759 CD1 단계 문서에 대해 각각 300개, 151개의 코멘트가 제출되었고, 이에 대해 다양한 주제별 토론이 진행되었다. 회의 결과, 해당 의견을 반영하여 DIS 추진이 승인되었다.

4.3. ISO/IEC 19896 (정보보안 시험자 및 평가자 적격성 요구사항)

개정 및 WD2 추진이 승인되었으며, 19896-1의 코에디터 최희봉 박사가 에디터로 변경 선임되었다.

4.4. ISO/IEC TS 20540 (암호모듈 현장 시험)

개정 및 WD1 추진이 승인되었으며, 에디터로 최희봉 박사, 코에디터로 윤승환 박사가 선임되었다.

Ⅴ. 결 론

본 논문에서는 ISO/IEC JTC 1/SC 27/WG 3 작업반에서 진행되고 있는 보안평가, 시험 및 규격 표준 중에서 IT 보안 평가에 활용되고 있는 ISO/IEC 15408, ISO/IEC 18045을 중심으로 표준화 진행 현황과 향후 개정 추진 방향에 대해 살펴보았다. 또한, 2023년 4월 미국 레드몬드에서 진행된 ISO/IEC JTC 1/SC 27/ WG 3 작업반 회의에서 논의된 보안 평가, 시험 및 규격 관련 주요 표준화 이슈에 대해 살펴보았다.

CCRA에서는 2022년 11월 CC:2022, CEM:2022의 발표[3]와 함께 이에 대한 전환 계획을 발표하였다. 이에 따라 국내 평가자, 개발자들도 변경된 표준을 파악하고 준비하기 위한 교육이 필요하며, 향후 개정 작업에서도 국제 표준화에 대한 에디터쉽을 확보할 수 있도록 지속적인 표준화 회의 참여와 기여가 필요하다. 본 논문이 CCRA의 전환 계획을 준비하고, 향후 국제표준화 개정 작업을 끌어나갈 전문가를 양성하는 시발점이 되었으면 한다.

참 고 문 헌

[1] 이광우, 이수연, 황현동, 성정호, 최희봉, “CC 평가 인증 기술 ISO/IEC 국제 표준화 동향”, *정보보호학회지* 31(4), pp. 45-53, August 2021

[2] ISO/IEC, PWI TR 7677 (4th WD), Roadmap for the maintenance of ISO/IEC 15408 and ISO/IEC 18045, October 2022

[3] CCRA Management Committee, Transition Policy to CC:2022 and CEM:2022, pp. 1-5, April 2023

〈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 : JTC 1/SC 27, SC 28 Liaison Officer
<관심분야> 보안공학, 시스템보안, 정보보호 평가·인증, 정보보호 표준화, 사무기기 표준화