정 보 보 호 학 회 지
제 30 권 제3호, 2020. 6

암호모듈 검증제도 체계 개선방안 연구

장 찬 국*, 이 재 훈**, 윤 승 환**, 이 옥 연*

요 약

사물인터넷 시장의 엄청난 확대와 기술의 발전 및 융합에 따라 기존 ICT 환경은 급속도로 발전하여 새롭게 신 ICT 환경이 형성되고 있다. 하지만, 신 ICT 환경은 다양한 기술과 통신 환경 및 수많은 기기로 구성되어 공격자들의 공격 방법 및 공격 경로가 다양화 되고 있는 추세이며, 특히, 기존 ICT 환경에서 사용하던 암호 알고리즘을 그대로 차용하고 기존의 프로토콜 또한 그대로 사용하고 있다.

이에 정보보안제품의 무분별한 도입을 방지하고 국가 및 공공기관의 안전성을 확보하기 위하여, 유·무선 인터넷 환경에 적용 가능한 암호모듈을 검증 시험함으로써 정보보안 산업의 활성화에 기여하고 있다. 본 논문에서는 국내 암호 산업의 활성화를 위해 관련 암호 정책을 이끌어 나가는 암호모듈 검증제도의 발전을 위해 국내·외 암호모듈 검증제도의 비교 내용을 소개한다.

Ⅰ. 서 론

글로벌 각국은 다양한 국가기관을 위한 제도를 통해 각국의 암호 정책을 수립함으로써, 자국 암호 산업의 발전을 모색하고 있다. 각국은 다양한 암호 정책 중에서도 암호모듈 및 정보보안 제품의 무분별한 도입을 방지하고 국가 및 공공기관의 안전성을 확보하여, 유·무선 인터넷 환경에 적용이 가능하도록 암호모듈을 시험하는 제도인 암호모듈 검증제도를 운영하여 정보보안 산업의 활성화에 기여하고 있다. 이러한 암호모듈 검증제도는 한국, 미국, 캐나다, 일본 등 세계 각국에서 운영하는 제도이다.

본 논문에서는 국내 암호모듈 검증체계 개선 방안을 마련하기 위해 각국의 암호모듈 검증제도를 조사하고, 검증 제도의 기준 및 절차 분석을 통해 국내 암호모듈 검증제도의 발전방안을 마련하고자 한다. 2장에서는 국내·외 암호모듈 검증제도의 체계, 역할, 대상, 기준등을 분석하고. 이를 바탕으로 3장에서는 국내 암호모듈 검증제도의 효율화 방안을 제시하고 4장에서 결론으로 마무리한다.

Ⅱ. 국내·외 암호모듈 검증제도

본 장에서는 대한민국과 미국/캐나다, 일본의 암호모듈 검증제도를 각각 설명하며 검증제도별 요구사항을 비교하고자 한다.

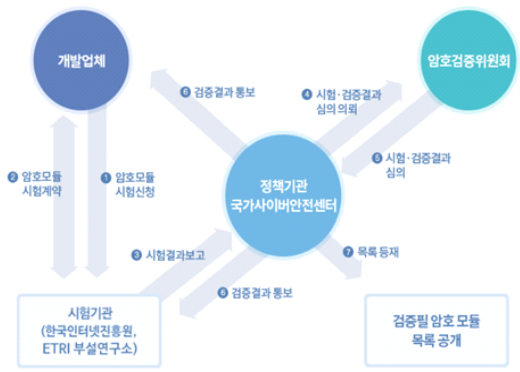
2.1. 암호모듈 검증제도별 체계 및 절차

2.1.1. 대한민국

대한민국의 암호모듈 검증제도(KCMVP, Korea Cryptographic Module Validation Program) 제도는 국가사이버안전센터에서 2005년부터 시행하고 있는 제도로써, 행정기관 등 국가 및 공공기관 정보통신망에서 소통되는 자료 중 중요정보의 보호를 위해 사용되는 암호모듈의 안전성과 구현 적합성을 검증하는 제도이다[1]. KCMVP 검증제도 체계는 개발업체(Vendor)가 검증신청서 및 제출물을 작성하여 시험기관인 한국인터넷진흥원과 국가보안기술연구소에 시험신청을 하게 된다.

시험기관은 제출물에 대한 사전검토를 수행하며, 제출물의 완성도가 미비할 경우, 개발업체에게 제출물 보완을 요청할 수 있다. 사전 검토 결과 제출물이 암호모

본 연구는 2019년 과학기술정보통신부의 재원으로 한국인터넷진흥원의 지원을 받아 수행되었습니다.
* 국민대학교 일반대학원 금융정보보안학과 (대학원생, jangchankuk@kookmin.ac.kr / 교수, oyyi@kookmin.ac.kr)
** 국민대학교 산학협력단 (연구교수, guderian88@kookmin.ac.kr / 연구교수, schneeleopard@kookmin.ac.kr)



〔그림 1〕 암호모듈 검증제도 검증절차

듈 시험 수행이 가능한 경우, 시험기관과 개발업체는 시험기관과의 계약을 진행하게 된다. 시험기관은 계약 후 시험반을 구성하여 관련 기준에 따라 시험을 수행하며, 시험기관은 제출물 또는 암호모듈의 취약성 등 보완사항 발견 시 개발업체에게 보완을 요청할 수 있다.

시험 완료 후 시험기관은 결과보고서를 작성하여 검증기관인 국가사이버안전센터에 제출하며 검증기관은 시험결과보고서를 검토하여 암호검증위원회에 시험결과에 대한 심의를 요청하고 심의결과에 따라 검증여부를 판정하게 된다.

검증이 완료된 암호모듈의 형상이 변경 될 경우, 개발업체는 시험기관에 재검증을 신청할 수 있다. 시험기관은 암호모듈의 변경 및 개선사항에 대한 타당성과 적절성을 검토하여 재검증 수행여부를 결정한다.

형상변경의 범위가 넓어 재검증 대상에 해당되는 경우, 재검증계약을 체결하여 진행하게 된다. 형상변경에 의한 검증 유지 또는 사후관리는 검증필암호모듈이 타사의 정보보호제품에 탑재되는 경우에 빈번하게 발생하게 되며 이 경우, 개발업체는 시험기관에 사후관리 절차를 문의할 수 있다. KCMVP 제도에서 인정하는 검증대상 암호 알고리즘은 안전성, 신뢰성, 상호운용성 등이 적합한 국산 암호 알고리즘과, 국내·외 표준 암호 알고리즘으로 선정하며, 암호모듈에 탑재된 암호 알고리즘은 2020년부터 '암호알고리즘검증기준 V3.0'에 따라 진행되고 있다.

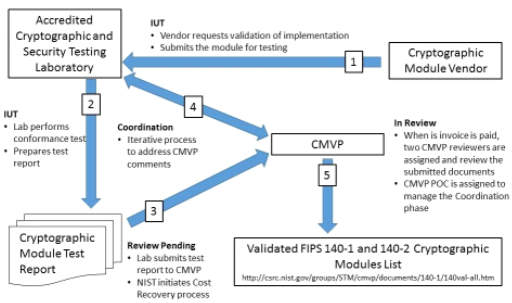
'암호알고리즘검증기준 V3.0'에서는 해시함수에 LSH와 SHA-3 알고리즘이 추가되고 해당 알고리즘을 사용하는 해시함수 기반 메시지인증코드와 해시함수 기반 난수발생기, 키유도함수가 추가되었다.[1]

2.1.2. 미국/캐나다

미국과 캐나다의 암호모듈 검증제도(Cryptographic Module Validation Program, CMVP) 제도는 미국의 NIST(National Institute of Standards and Technology)와 캐나다의 CCCS(Canadian Centre for Cyber Security)가 공동으로 주관하는 제도이다[2]. 대한민국의 KCMVP와 마찬가지로, 개발업체(Cryptographic Module Vendor)가 검증신청서 및 제출물(Implementation Under Test, IUT)을 구현 및 작성하여 시험기관(Accredited CST Lab)에 시험신청을 하게 된다.

시험기관은 계약 후 암호모듈 검증 기준인 FIPS 140-2에 따라 시험을 수행하며, 시험기관은 제출물 또는 암호모듈의 취약성 등 보완사항 발견 시 개발업체에게 보완을 요청할 수 있다. 시험 완료 후 시험기관은 결과보고서를 작성하여 NIST에게 제출하게 된다. NIST에서는 결과보고서를 바탕으로 부족한 점을 다시 시험기관에 요구할 수 있고, 인증이 잘 수행된 경우 인증서를 개발업체에게 발급하고 FIPS 140-2 모듈 목록에 올리게 된다. 이러한 FIPS 140-2는 2026년 까지 검증이 계속되지만, 2019년 미 상무부는 FIPS 140-2를 대체할 FIPS 140-3을 승인하였고, 2019년 5월 발효되었다. FIPS 140-3은 FIPS 140-2와 달리 모듈의 요구사항을 직접 포함하지 않고, ISO/IEC 19790:2012와 ISO/IEC 24759:2017을 따르게 된다. 주요 기술적 요구사항의 변경은 거의 없지만 ISO 국제 표준을 따르게 되면서 절차적 변경만이 진행되었다. 또한, FIPS 140-3의 내용을 NIST SP 800-140x 시리즈로 식별하였다. NIST SP 800-140x 시리즈는 ISO 표준의 부록 요구사항을 담은 내용으로 2020년 3월 Final 버전이 등재되었다.

또한, 미국, 캐나다의 CMVP는 국내 KCMVP 제도



〔그림 2〕 CMVP 암호모듈 검증제도 검증절차

와는 달리 CAVP(Cryptographic Algorithm Validation Program)이 따로 분리되어 존재한다. CAVP는 1995년 7월 미국의 NIST와 캐나다의 CSE에 의해 진행되었다. CAVP 기준은 FIPS 140-1에서부터 시작하여 2001년 5월부터 FIPS 140-2를 기준으로 진행되고 있다. CAVP 시험은 FIPS 승인 및 NIST 권장 알고리즘을 시험하며, 모든 CMVP 검증의 전제조건으로 CST Lab을 통해 시험받을 수 있다. 검증 후에는 CMVP 검증 목록과는 별개로 CAVP 검증 목록에 등재된다. NIST는 CAVP와 동시에 자동 암호 알고리즘 검증(ACVP, Automated Cryptographic Validation Testing)을 지원하기 위해 프로젝트를 진행하고 있으며, 현재 Phase 3, 4가 동시에 진행 중이다.

2.1.3. 일본

일본의 암호모듈 검증제도인 JCMVP는 비밀로 분류되지 않은 데이터 보호를 위해 사용되는 암호모듈 및 암호 알고리즘의 국가기관 사용을 위해 운영된다. 일본의 IT 국가 전략 정보처리추진기구인 IPA (Information-technology Promotion Agency)에서 2006년 6월 시험 운용한 뒤 2007년 4월부터 정식 시행한 제도로써, 국제 표준 암호모듈 보안 요구사항인 ISO/IEC 19790:2012을 만족하여야 하고, ISO/IEC 24759:2017를 따라 검증을 수행한다. 2020년 6월까지는 이전 버전인 ISO/IEC 19790:2006과 ISO/IEC 24759:2008을 기반으로 한 검증 또한 승인된다.

JCMVP는 크게 신청자, 시험기관, 검증기관으로 나뉜다. 신청자의 경우, 암호모듈의 공급 및 개발업체(Vendor)이며 ‘Rules for the Application Procedures for Cryptographic Module Validation(CBM-02)’를 따라야 한다. JCMVP 시험기관은 JCMVP 검증 기준에 따라 암호 모듈을 시험하는 기관으로, 2019년 현재 3개가 운영 중이다.

이 3개의 시험기관은 미국 CMVP CST Lab으로도 운영 중이며, ‘Mizuho Information and Research Institute, Inc.’ 시험기관은 2019년 10월 31일 부로 시험기관 승인이 종료되었다. JCMVP 시험기관이 되기 위해서는 미국의 NVLAP 프로그램과 마찬가지로, 일본의 NITE에서 진행하는 ASNITE-IT 프로그램에 따라 인증을 받아야 하며 JCMVP 인증기관인 IPA로부터 ‘Rules for the Application Procedures for Recognition as Cryptographic Module Testing Laboratories (CBM-03)’의 절차를 통해 인증되어야 한다. 인증기관은 IPA로, 시험기관에서 수행한 검증 결과를 기반으로 인증을 수행한다. 검증기관은 검증 절차를 수행할 때 JIS Q 0065에 규정된 요구사항을 만족시켜야 한다[3]. 특히, JCMVP는 미국/캐나다의 CMVP와 상호협력체계를 구축하여 각 지역의 시험기관에서 시험한 제품에 대해 각 국가기관은 상호 인증하고 있다.

JCMVP 검증 절차는 다음과 같다. 암호모듈 검증 신청자(Vendor)는 CBM-02에 명시된 절차에 따라 검증기관에 암호모듈 검증 또는 암호 알고리즘 검증을 위한 신청서를 제출하고 검증기관은 CBM-02에 따라 신청서를 받는다. 시험기관은 신청자가 지정한 보안요구사항에 따라 암호 알고리즘 검증 시험과 암호 모듈 검증 테스트를 수행하여야 하고 시험 결과에 근거하여 보고서를 작성하고 신청자가 제출한 보안 정책 문서와 함께 검증기관에 제출한다. 보고서를 받은 검증기관은 보고서와 보안 정책 문서를 확인한 후 신청자에게 인증서를 제공한다.

재검증 절차는 변경 사항의 정도에 따라 나뉘게 된다. 먼저 변경사항이 보안에 영향을 미치지 않는 경우 신청자는 ‘암호모듈 영향분석 보고서’를 작성하여 검증기관에 제출한다. 검증기관은 해당 보고서를 분석하여 유효하다고 판단되면 보증 연속성 절차를 통해 검증을 승인한다. 하지만 변경사항이 보안에 영향을 미치는 경우 신청자는 변경사항을 시험할 수 있도록 변경 범위를 설명하는 보고서를 시험기관에 제출하고, 시험기관은 재확인 절차에 따라 암호모듈 시험을 수행한다.

JCMVP에서 인정하는 암호 알고리즘은 CMVP 검증 대상 알고리즘을 모두 포함하고, 몇가지의 일본 자국 암호 알고리즘을 포함한다. 해당 내용은 ‘The specification about the approved security functions(ASF-01)[4]’에 명시되어 있다. 이 중에서, 블록암호 3TDES와 3TDES를 이용하는 CMAC, CTR_DRBG의 경우 2019년 12월까지만 유효하고, 2020년 이후부터는 제외된다.

2.2. 검증제도별 보안 및 시험 요구사항 비교

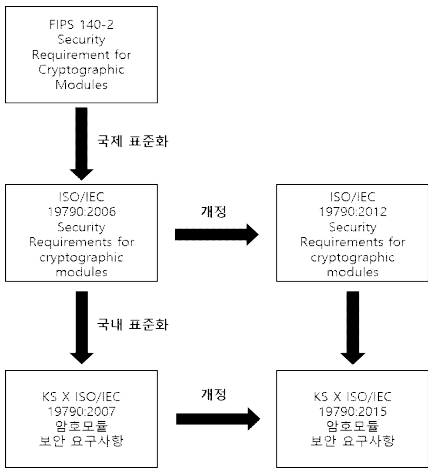
2.2.1. 보안 요구사항

CMVP는 ‘FIPS 140-2, Security Requirement for Cryptographic Modules’[5]를 참조하고 있고, KCMVP는 ‘KS X ISO/IEC 19790:2015, 정보기술 - 보안기술 - 암호모듈 보안 요구사항’[6], JCMVP는 ‘ISO/IEC 19790:2012, Information technology – Security techniques – Security requirements for cryptographic modules’[7]를 보안 요구사항으로 참조하고 있다.

각각의 표준문서는 부속서의 검증대상 암호알고리즘, 검증대상 중요 보안매개변수 생성 및 설정 방법 등의 일부 내용을 제외하고 동일하다. 검증대상 암호알고리즘의 경우 위 3장 1절에서 설명하였고, 검증대상 중요 보안매개변수 생성 및 설정 방법은 [6]에만 존재한다. 해당 표준들의 관계도는 그림 3과 같다.

KS X ISO/IEC 19790:2007[8]에서 KS X ISO/IEC 19790:2015[6]로 개정되면서 8개가 변화하였다, 첫 번째로는 ‘영역별 보안요구사항의 변화’이다. KS X ISO/IEC 19790: 2007과 2015의 영역별 보안 요구사항의 변화를 요약하면 표 1과 같다.

KS X ISO/IEC 19790:2007[8]에서는 총 11개의 영역별 보안 요구사항으로 나누고, 보안등급 1부터 4까지 구분하였지만, KS X ISO/IEC 19790:2015[6]에서는 총 11개의 영역별 보안 요구사항으로 나누고, 보안수준 1부터 4까지 구분하였다. 특히 기능적 보안 목적에서



〔그림 3〕 검증제도별 보안 요구사항 표준 관계

〔표 1〕 KS X ISO/IEC 19790: 2007[8]과 KS X ISO/IEC 19790: 2015 〔6〕의 영역별 시험 요구사항 변화

KS X ISO/IEC 19790: 2007〔8〕 (ISO/IEC 19790: 2006)	KS X ISO/IEC 19790: 2015 〔6〕 (ISO/IEC 19790: 2012)
암호모듈 명세	암호모듈 명세
암호모듈 포트와 인터페이스	암호모듈 인터페이스
역할, 서비스 및 인증	역할, 서비스 및 인증
유한상태모델	소프트웨어/펌웨어 보안
물리적 보안	운영환경
운영환경	물리적 보안
암호 키 관리	비침투 보안
자가시험	SSP 관리
설계보증	자가시험
기타 공격에 대한 대응	생명주기 보증
전자파 장애 및 전자파 적합성	기타 공격에 대한 대응

‘보안등급’을 ‘보안수준’으로 명칭을 변경하고, 보안수준 4가 가장 높은 보안 목적을 가짐을 명확히 하였다.

두 번째로는 ‘암호모듈 유형에 대한 정의 추가’이다. KS X ISO/IEC 19790:2015[6]로 개정되면서 암호모듈 명세 중 암호모듈 유형에 대한 정의가 표 2와 같이 추가되었다. 특히 하이브리드 소프트웨어 모듈과 하이브리드 펌웨어 모듈의 경계가 명확해졌다.

세 번째로는 ‘암호모듈 인터페이스 유형 및 정의 추가’이다. KS X ISO/IEC 19790: 2007[8]의 암호모듈 포트와 인터페이스 영역이 KS X ISO/IEC 19790:2015[6]의 암호모듈 인터페이스로 변경되었다. KS X ISO/IEC 19790: 2007[8]에서는 4개의 논리적 인터페이스가 정의되어 있었지만, KS X ISO/IEC 19790:2015[6]에서 제어 입력 인터페이스와 전원 인터페이스의 정의를 추가하여 총 6개의 인터페이스 정의를 명시하였다.

네 번째로는 ‘신뢰 채널 추가’이다. KS X ISO/IEC 19790: 2007[8]에서의 보안등급 3과 4에서 신뢰된 경로에 대한 내용에 대하여 KS X ISO/IEC 19790:2015[6]에서 보안수준 3과 4는 보호되지 않은 평문 CSP, 키 구성 요소, 인증 데이터의 전송을 위하여 암호모듈은 신뢰 채널을 구현하고, 특히 보안수준 4는 다중체계 신원 기반 인증을 적용하게끔 변경되었다.

다섯 번째로는 ‘펌웨어/소프트웨어 무결성 검증 방법 정의 추가’ 이다. KS X ISO/IEC 19790 :2015[6]에서

〔표 2〕 암호모듈의 유형 및 주요 특징

구분	주요 특징
하드웨어 모듈	- 하드웨어 경계를 이용하여 암호경계를 구분함 - 펌웨어 또는 소프트웨어를 포함할 수 있음
소프트웨어 모듈	- 소프트웨어 경계로 암호경계를 구분함 - 변경 가능한 운영환경에서 실행하는 소프트웨어 구성 요소임 - 연산 플랫폼와 운영체제는 경계 외부에 있음
펌웨어 모듈	- 펌웨어 경계를 이용하여 암호 경계를 구분함 - 제한되거나 변경이 불가능한 운영환경에서 실행하는 펌웨어 구성 요소임 - 연산 플랫폼이나 운영체제는 경계 외부에 있으나 펌웨어 모듈과 항상 결합된 형태임.
하이브리드 소프트웨어 모듈	- 소프트웨어 및 하드웨어 구성 요소를 조합함 - 소프트웨어 구성 요소와 하드웨어 모듈 경계는 분리됨 - 연산 플랫폼 및 운영체제는 경계 외부에 있음
하이브리드 펌웨어 모듈	- 펌웨어 구성 요소 및 하드웨어 구성 요소를 조합한 유형임 - 펌웨어 구성 요소와 하드웨어 모듈 경계는 분리됨 - 연산 플랫폼 또는 운영체제는 경계 외부에 있으나 항상 결합된 형태임

보안수준에 따라 무결성 검증 방법을 정의하고 [AS05.01]부터 [AS05.21]까지 시험 요구사항을 제시하였다.

여섯 번째로는 '운영환경에서 CC 인증요구사항 삭제 및 최대 보안수준 4에서 2로 조정'이다. [9]에서 운영환경 영역은 보안수준 2, 3, 4에서 각각 CC 인증 요구사항인 EAL 2, 3, 4 수준을 요구하지만, [6], [10], [11]에서는 EAL 등급을 명시하지 않는다.

일곱 번째는 '암호알고리즘 동작 전 자가시험을 조건부 자가시험'으로의 변경이다. KS X ISO/IEC 19790: 2007[8]에서 암호모듈의 전원 인가 시 자동 천이하는 전원인가 자가시험 영역이 KS X ISO/IEC 19790:2015[6]에서 동작 전 소프트웨어/펌웨어 무결성 시험, 동작전 우회 기능시험, 동작 전 핵심 기능시험으로 변경되었고, 암호알고리즘 자가시험, 암호키 쌍 일치 시험, 소프트웨어/펌웨어 로드 시험, 수동 주입 시험, 조건부 우회 기능 시험 및 조건부 핵심 기능시험 등이 조건부 자가시험 영역으로 포함되었다. 특히, KS X ISO/IEC 19790: 2007[8]에서의 전원인가 시험 시 암호알고리즘 자가시험을 [6]의 조건부 암호알고리즘 시험 영역으로 이동하였다.

마지막 여덟 번째는 '주기적 자가시험 추가'이다. KS X ISO/IEC 19790: 2007[8]에서 운영자의 요구 시 자가시험을 수행할 수도 있었던 기능이 KS X ISO/IEC 19790:2015[6]에서는 주기적인 자가시험 영역으로 추가되었다.

2.2.2. 시험 요구사항 비교

현재 CMVP는 FIPS 140-2의 시험 요구사항으로 'Derived Test Requirement for FIPS PUB 140-2, Security Requirements for Cryptographic'[9]을 사용하며 이는 KS X ISO/IEC 19790:2007의 시험 요구사항과 거의 일치한다. KCMVP는 KS X ISO/IEC 19790:2015의 시험 요구사항으로 'KS X ISO/IEC 24759: 2015, 정보기술 - 보안기술 - 암호모듈 시험 요구사항'[10]을 사용하며, JCMVP는 'ISO/IEC

〔표 3〕 검증 제도별 시험 요구사항

시험 요구사항	FIPS 140-2 DTR, 2011	KS X ISO/IEC 24759: 2015
일반사항	-	4(-)
암호모듈 명세	16(31)	32(53)
암호모듈 인터페이스	18(38)	22(49)
역할, 서비스 및 인증	32(46)	59(69)
소프트웨어/펌웨어 보안	-	21(15)
운영환경	27(36)	29(51)
물리적 보안	69(71)	86(81)
비침투 보안	5(-)	7(5)
중요 보안매개변수 관리	-	37(59)
자가시험	48(61)	55(79)
생명주기 보증	-	39(46)
기타 공격에 대한 대응	1(2)	4(5)
암호 키 관리	42(59)	-
유한상태모델	5(12)	-
설계보증	25(22)	-
EMI/EMC	5(6)	-
총 18 항목	293항목 (384항목)	395항목 (512항목)

24759:2017, Information technology − Security techniques −Test requirements for cryptographic modules'[11]에 기초하고 있다.

본 소소단원에서는 보안 요구사항의 개정에 따라 [10]에서 다양한 영역에서 변화가 있었으며, [9]과 [10]를 크게 다섯가지에 대해 비교하고자 한다.

각각의 검증제도별 시험 요구사항은 다음 표3과 같다. 표 내의 항목은 시험 항목이며 괄호 안은 시험 절차에 대한 요구사항 항목이다.

첫 번째로는 '암호모듈 유형 영역에 관련된 시험 요구사항'의 변화이다. [6]에서 '암호모듈 유형에 대한 정의 추가'가 추가됨에 따라, [10]에서 추가된 하이브리드 모듈 영역에 관련된 시험 요구사항은 다음 표와 같다.

〔표 4〕〔10〕의 하이브리드 모듈 영역에 관련된 시험 요구사항

구분	관련 시험 요구사항
암호모듈 유형	AS02.06
물리적 보안	AS07.01 ~ AS07.86
비침투 보안	AS08.01 ~ AS08.07

두 번째로는 '인터페이스 유형 영역에 관련된 시험 요구사항'이다. [6]에서 제어 입력 인터페이스와 전원 인터페이스의 정의를 추가하여 총 6개의 인터페이스 정의됨에 따라, [10]에서 추가된 인터페이스 영역에 관련된 시험 요구사항은 다음과 같다.

〔표 5〕〔10〕에서 인터페이스 영역에 관련된 시험 요구사항

구분	관련 시험 요구사항
인터페이스 정의	AS03.04
데이터 입력 인터페이스	AS03.05
데이터 출력 인터페이스	AS03.06 ~ AS03.07
제어 입력 인터페이스	AS03.08
제어 출력 인터페이스	AS03.09 ~ AS03.10
상태 출력 인터페이스	AS03.11
전원 인터페이스	AS03.12 ~ AS03.13

세 번째로는 '신뢰 채널 영역에 관련된 시험 요구사항'이다. [6]에서 보안수준 3과 4는 보호되지 않은 평문 CSP, 키 구성 요소, 인증 데이터의 전송을 위하여 암호모듈은 신뢰 채널을 구현하고, 특히 보안수준 4는 다중체계 신원 기반 인증을 적용하게끔 변경됨에 따라 [10]에서 추가된 신뢰 채널 영역에 관련된 시험 요구사항은 다음과 같다.

〔표 6〕〔10〕에서 신뢰 채널 영역에 관련된 시험 요구사항

구분	관련 시험 요구사항
신뢰 채널	AS03.16 ~ AS03.21
다중체계 신원 기반 인증	AS03.22

네 번째로는 '펌웨어/소프트웨어 무결성 검증 방법 영역에 관련된 시험 요구사항'이다. [6]에서 보안수준에 따라 펌웨어/소프트웨어 무결성 검증방법이 추가됨에 따라, 관련된 시험 요구사항 또한 추가되었다.

〔표 7〕〔10〕에서 펌웨어/소프트웨어 무결성 검증 방법 영역에 관련된 시험 요구사항

구분	관련 시험 요구사항
소프트웨어/펌웨어 보안	AS05.01 ~ AS05.21
배포 및 운영	AS11.32 ~ AS11.35

마지막 다섯 번째로는 '조건부 암호알고리즘 시험 영역에 관련된 시험 요구사항'이다. 기존 전원인가 자가시험에 포함되었던 암호알고리즘 시험은 [10]에서 조건부 시험 알고리즘 시험 영역으로 변경되었다.

2.3. 검증제도별 암호 알고리즘 구현 적합성 시험 비교

본 절에서는 대한민국과 미국/캐나다에서 시험하고 있는 암호 알고리즘 구현 적합성 시험(CAVP, Cryptography Algorithm Validation Program)에 대해 비교 분석한다. KCMVP에서의 CAVP는 2020년부터 '암호알고리즘검증기준 V3.0'에 따라 진행되고 있다. '암호알고리즘검증기준 V3.0'에서는 기존 '암호알고리즘검증기준 V2.0'과 비교하여 해시함수에 LSH와 SHA-3 알고리즘이 추가되고 해당 알고리즘을 사용하는 해시함수 기반 메시지인증코드와 해시함수 기반 난수발생기, 키유도함수가 추가되었다.

대한민국의 CAVP는 KCMVP 검증 내에 포함되어 있으며, 모든 모듈이 수행하여야 하는 시험이며, 모듈 내 포함된 암호알고리즘의 종류에 따라 시험을 수행한다. 반면 CMVP에서의 CAVP는 1995년 7월 미국의 NIST와 캐나다의 CSE에 의해 진행되었다.

CAVP 기준은 FIPS 140-1에서부터 시작하여 2001년 5월 FIPS 140-2를 기준으로 진행된다. CAVP 시험은 FIPS 승인 및 NIST 권장 알고리즘을 시험하며, 대한민국의 KCMVP와는 달리 '구성요소 시험(Component Test)'가 존재한다. 구성 요소 시험(Component Test)란 개별 알고리즘 구성요소의 유효성 시험으로 다양한 응용 프로그램에서 사용되는 암호 알고리즘 중 전체 암호 알고리즘이 사용되는 경우가 아니라 일부분만 사용되는 암호 알고리즘에 대한 시험이다.

이러한 경우 전체 알고리즘에 대한 유효성 검사를 진행하는 것이 아니라 구성 요소만 시험을 하는 것 이다. 구성 요소 시험이 가능한 알고리즘 종류는 총 5개로 'ECCCDH(Elliptic Curve Cryptography Cofactor Diffie-Hellman) Primitives', 'ECDSA Signature Generation Primitive', 'KDF', 'RSADP Decryption Primitive', 'RSA PKCS 1.5 and PSS Signature Generation Primitive' 이다.

미국의 CAVP는 모든 CMVP 검증의 전제조건으로 CST Lab을 통해 시험받을 수 있다. 즉, 미국과 캐나다에서는 CMVP와 CAVP를 분리하여 운영하고 있다. 검증 후에는 CMVP 검증 목록과는 별개로 CAVP 검증 목록에 등재된다. NIST는 CAVP와 동시에 자동 암호 알고리즘 검증 시스템(ACVP, Automated Cryptographic Validation Testing) 또한 지원하기 위해 프로젝트를 진행하고 있으며, 현재 Phase 3, 4가 동시에 진행 중이다.

Ⅲ. 암호모듈 검증제도의 제도적 차이점

3.1. 암호 시스템 정합성 시험

국내 KCMVP 제도와 미국 CMVP 제도의 첫 번째 차이점은 KCMVP 제도에선 암호 시스템 정합성 시험 체계가 없다는 것이다. 국가 및 공공기관에 도입되는 정보보호시스템 제품에 대한 안전성 검증제도는 '보안적합성 시험'또는 '보안기능 시험결과서 발급제도'로 존재한다. 이 시험들은 네트워크 장비와 CC 인증 필수 제품 유형 24종에 대한 평가이다.

하지만, 다양한 공공시장에서 요구되는 검증필암호모듈을 탑재한 제품들에 대한 시스템 정합성 시험과 정합성 시험에 대한 인증체계가 현재 국내에는 존재하지 않는다. 국제 표준인 ISO/IEC 20540:2018, Information technology − Security techniques − Testing cryptographic modules in their operational environment'에서는 보안 시스템 내에서 암호모듈의 운영에 대한 시험을 정의하고 있다. 국내에서는 [7]과 [11]을 국내 표준에 반영하여 암호모듈 검증 제도를 운영하고 있지만, ISO/IEC 20540과 같은 표준은 아직 반영되어 있지 못한 실정이다.

암호 시스템 정합성 시험이 필요한 이유는 실제 검증필암호모듈의 오용이 가능하기 때문이다. 다양한 공공시장에서 요구되는 검증필암호모듈을 탑재한 제품들은 CC 인증이나, 보안 적합성 검증을 통해 공공시장에 납품된다. 하지만, 해당 장비들이 실제 운용될 때 Vendor의 실수나 고의적으로 검증필암호모듈의 미사용하거나 검증보고서에 명시된 정당한 운영환경이 아닌 곳에서 오용되는 경우도 있다.

따라서, 검증필암호모듈의 오용을 방지하기 위한 암호시스템 정합성 시험 체계 마련은 KCMVP 제도의 결과물인 검증필암호모듈의 정확한 사용을 통해 KCMVP 제도의 신뢰성을 높여줄 뿐 아니라, 국가 및 공공기관의 주요 정보에 대한 보호에 이바지할 것이라 생각된다.

따라서 국제 표준인 ISO/IEC 20540:2018, Information technology − Security techniques − Testing cryptographic modules in their operational environment'의 국내 표준화와, 해당 표준화를 통해 검증필암호모듈이 사용되는 시스템 정합성 시험에 대한 인증체계 마련이 필요하다.

3.2. 알고리즘 적합성 시험과 자동화 도구

국내 KCMVP제도와 미국 CMVP 제도의 두 번째 차이점은 암호 알고리즘 적합성 시험 체계(CAVP)가 KCMVP 제도와 분리되어 있지 않다는 것이다. 현재 CMVP 제도에서는 CAVP와 CMVP가 나뉘어 있으며 CAVP 시험을 CMVP 검증의 전제 조건으로 하며, 지정된 시험기관을 통해 별도의 시험으로 진행하여 개발업체의 CMVP 검증에 용이하도록 한다.

또한, CMVP 제도에서는 온라인으로 CAVP 제도를 Vendor에게 제공하는 ACVP 프로젝트를 진행한다. 자동화 도구는 시험기관의 CAVP 효율성을 높일 수 있는 제도로 시험기관의 부담을 줄일 수 있고, Vendor 또한

비용 감소로 이루어 질 수 있다.

3.3. 시험 상태 공개 제도 및 검증서 교부 제도

국내 KCMVP 제도와 미국 CMVP 제도의 세 번째 차이점은 시험 상태 공개 제도의 유무이다. CMVP 제도의 경우 CMVP 검증을 신청한 Vendor나 CMVP 모듈을 사용하고자 하는 사용자가 'Module In Process'라는 웹 페이지를 통해 현재 검증되고 있는 CMVP 모듈에 대한 상태를 검색할 수 있다. 하지만, 현 KCMVP 검증제도에서 Vendor는 검증과정을 확인할 수 있는 방법은 실제 계약 후 피드백 과정에서만 가능하다.

시험 상태 공개 제도의 장점은 Vendor와 암호모듈 구매자에게 현 시험 상태를 제공한다는 점이다. 암호모듈의 개발 및 시험 완료는 해당 모듈의 Vendor와 구매자에게 정보보안 제품의 개발 및 납품, 사업화를 계획할 단계에서부터 큰 영향을 줄 수 있는 요인이며 이는 암호 산업의 계획적 발전 입장에서 큰 장점이다.

또한, 검증서 교부는 CMVP, JCMVP 제도에서 진행하는 제도로, 발급된 검증서를 통해 Vendor의 제품 판매를 용이하게 하며 다른 제품과의 차별성을 줄 수 있는 제도이다. 암호 시장에서 KCMVP 검증필암호모듈이 탑재된 제품을 공공시장에 납품할 경우 담당자가 해당 제품이 실제 검증필암호모듈인지, 검증필암호모듈을 탑재한 제품인지를 확인할 수 있는 방법이 어려운 상황이다.

따라서, 검증서 교부 제도는 발급된 암호모듈 검증서를 통해 국가 및 공공기관에 납품할 제품에 검증필암호모듈이 포함되어 있다는 일차적 검증이 될 수 있다. 암호 시스템 적합성 시험 제도 이전에 수요기관에서 일차적으로 해당 제품 또는 판매자에 대한 검증이 진행될 수 있고, 암호모듈 판매 사업이라는 측면에서도 구매자가 구매할 검증필암호모듈에 대한 근거 서류가 되며 암호모듈에 대한 신뢰성 또한 높아질 수 있다.

Ⅳ. 결 론

본 논문에서는 국내외의 암호모듈 검증제도와 검증체계별 차이점의 비교에 대해 소개하였다. 각국의 암호모듈 검증제도는 다양한 암호 정책 중에서도 외산 암호모듈 및 정보보안제품의 무분별한 도입을 방지하고 국가 및 공공기관의 안전성을 확보하여 유·무선 인터넷 환경에 적용 가능한 검증된 암호모듈을 시험하는 제도이며, 각국의 암호 시장 및 암호 정책에 가장 중요한 역할을 하는 제도이다. 국외 제도와의 비교 분석을 통해 향후 KCMVP 제도의 발전과 검증필암호모듈의 올바르고 안전한 사용, 국내 암호산업의 발전을 도울 역할을 수행할 수 있을 것이라 기대된다.

참 고 문 헌

[1] https://www.nis.go.kr:4016/AF/1_7_3_1.do

[2] https://csrc.nist.gov/Projects/cryptographic-module-validation-program

[3] Basic Rules for the Japan Cryptographic Module Validation Program(JCM-01), Information Technology Promotion Agency, Japan, 2014.05.

[4] The specifications about the approved security functions (ASF-01), Information Technology Promotion Agency, Japan, 2019.07.

[5] FIPS 140-2, Security Requirement for Cryptographic Modules, NIST, 2002.12

[6] KS X ISO/IEC 19790:2015, 산업통상자원부 국가기술표준원, 2015.08.

[7] ISO/IEC 19790:2012, ISO, 2012.08

[8] KS X ISO/IEC 19790:2007, 산업통상자원부 국가기술표준원, 2007

[9] Derived Test Requirement for FIPS PUB 140-2, Security Requirements for Cryptographic, NIST, 2011.01.

[10] KS X ISO/IEC 24759:2015, 산업통상자원부 국가기술표준원, 2015.08

[11] ISO/IEC 24759:2017(E), Information technology — Security techniques — Test requirements for cryptographic modules

〈저 자 소 개〉

장 찬 국 (Chan-Guk Jang)

학생회원

2016년 2월 : 국민대학교 수학과 졸업

2018년 2월 : 국민대학교 금융정보보안학과 석사

2018년 3월 ~ 현재 : 국민대학교 금융정보보안학과 박사과정

<관심분야> 네트워크보안, 이동통신보안, 암호모듈 검증제도

이 재 훈 (Jaehoon Lee)

정회원

2013년 2월 : 국민대학교 수학과 졸업

2019년 2월 : 국민대학교 금융정보보안학과 박사

2019년 2월 : 국민대학교 금융정보보안학과 박사

2019년 3월~현재 : 국민대학교 BK 계약교수

<관심분야> 네트워크보안, 이동통신보안, 암호모듈 검증제도

윤 승 환 (Seunghwan Yun)

정회원

2005년 2월 : 국민대학교 수학과 졸업

2007년 2월 : 국민대학교 수학과 석사

2019년 2월 : 국민대학교 금융정보보안학과 박사

2019년 3월~현재 : 국민대학교 BK 계약교수

<관심분야> 보안칩, 이동통신보안, 암호모듈검증제도

이 옥 연 (Okyeon Yi)

정회원

1988년 2월 : 고려대학교 수학과 학사

1990년 2월 : 고려대학교 일반대학원 수학과 석사

1996년 8월 : University of Kentucky 대수학 박사

1999년~2001년 : ETRI 선임연구원/팀장

2001년 9월~현재 : 국민대학교 정보보안암호수학과, 금융정보보안학과 교수

<관심분야> 5G/6G 보안, 위성통신 보안, 양자난수 기술, 암호기술