한국산학기술학회논문지
Vol. 12, No. 1 pp. 255-262, 2011

암호모듈 검증 정책에 관한 연구[1]

최명길[2*], 정재훈[3]
[2]중앙대학교 사회과학대학 상경학부
[3]중앙대학교 일반대학원 경영학과

A Study on the Policy of Cryptographic Module Verification Program[1]

Myeonggil Choi[2*] and Jaehun Jeong[3]
[2]College of Social Sciences, Chung-Ang University
[3]College of Business Adminstration, Chung-Ang University

요 약 정보통신분야의 발전은 해킹 등의 역기능을 발생에 따라 정보보호를 위한 암호모듈의 한 수요가 급증한다. 국내 암호모듈 평가 기준의 불명확성과 모듈 선정의 어려움은 모듈 및 제품 상호간의 운용 및 호환성 확보를 어렵게 한다. 본 연구는 국외 암호모듈 평가 프로그램인 CMVP(Cryptographic Module Verification Program)를 분석하여 국내 암호모듈 암호 모듈 검증 기준 및 평가 절차, 검증 정책 발전 방향을 제안한다. 본 연구는 국내 암호모듈 발전정책을 제안하여 암호모듈 국제 표준화, 국제 암호모듈 제도에 대한 공조를 기반을 제공한다.

Abstract The advancement of information and communication technology has caused a few dysfunction such as hacking. To keep an organization from a harmful hacking, demands for cryptographic modules have been increased. However, the evaluation criteria of cryptographic modules in Korea have been less firmly established. It is difficult for the consumers of cryptographic module to choose an appropriate cryptographic module, and to establish interoperability between applications and cryptographic modules. This study analyzes evaluation criteria, evaluation processes and evaluation policy of CMVP(Cryptographic Module Verification Program) in the advanced countries. The paper suggests a policy for Korea CMVP, in resulting a provision of foundations for international standard and cooperations for international cryptographic policies and systems.

Key Words : CMVP, Cryptography Module, Cryptographic Module Verification Program

1. 서론

암호 기술의 표준화로 인하여 정보 보호 업체들은 표준화된 암호 기술을 채택하여 안전하고 신뢰성 있는 제품을 생산할 수 있게 되었다. 그러나 이러한 암호 기술의 이해 부족 및 실제 구현상의 미스 등으로 인해 실제 제품에 탑재하는데 완전성을 보장하는데 불충분하는 경우가 발생하기도 한다.

특히 국내 암호모듈 검증 수준은 미국, 캐나다 등 암호모듈검증을 조기에 도입한 선진국과 비교하면 검증 기준 및 제도가 성숙하지 않다. 선진국 수준의 암호모듈 검증 정책 및 제도의 수립 및 정착이 시급하다.

정보보호 기능은 모든 유형의 '정보시스템'의 기본 기능이다. 정보시스템이 정보보호 기능 중 기밀성, 무결성 등의 보안 서비스를 제공하기 위해 '암호모듈'을 상요한다.

최근의 이러한 암호기술의 안전성 평가는 가장 기본이 되는 안전성 요구이므로 국내외적으로 암호알고리즘의 안전성 분석 및 암호모듈의 안전성 평가에 대해 많은 관심을 보이고 있으며, 미국은 총 16개의 시험기관, 일본은

이 논문은 2009년도 중앙대학교 연구장학기금 지원에 의한 것임
*교신저자 : 최명길(mgchoi@cau.ac.kr)
접수일 10년 10월 28일 수정일 11년 01월 12일 게재확정일 11년 01월 13일

3개의 시험 기관을 운영하고 있다. 미국은 NIST가 암호 모듈 검증기준을 제정하고 있다. NIST는 2007년 7월에 FIPS 140-3을 발표하였고, 미국은 향후 FIPS 140-3을 국제표준으로 재정할 것으로 예측된다[6].

향후 CMVP와 관련된 국제적인 변화 동향을 살펴보면 다음과 같다. 미국 및 캐나다는 일찍이 FIPS 표준을 기반으로 CMVP를 정착시켰다. 우리나라를 비롯한 유럽 및 호주 등은 암호모듈 검증정책이 정착시키고 있는 중이다. 향후 후발 암호모듈 검증국가와 선진 암호모듈 검증의 호환성을 위해서 국제상호인증제도(CCRA)와 유사한 'CMVP 상호인정(CMVP RA) 제도'가 실시가 예상된다.

본 연구는 국외 암호모듈 정책 및 제도의 동향을 분석한다. 분석대상 국가는 미국, 캐나다, 영국, 독일, 프랑스, 이탈리아 등의 유럽, 일본, 호주 등의 정보보호선진국이다. 본 연구는 정보보호 선진국의 암호모듈 동향 분석을 바탕으로 우리나라에 적용할 수 있는 암호모듈 정책 및 제도 추진 방향을 제시한다. 본 연구가 제안하는 암호모듈 정책 방향은 국내 암호모듈 검증제도가 선진국 수준으로 발전하는 토대 마련에 기여할 수 있다.

2. 암호모듈 검증 프로그램

2.1 CMVP(Cryptographic Module Verification Program)

암호모듈 검증 프로그램은 미국 및 캐나다가 가장 먼저 시작하였다. CMVP는 1995년 미국 NIST와 캐나다 주정부의 CSE(Communications Security Establishment)가 공동으로 개발한 암호모듈 검증제도로, 표준에 따라 구현된 암호모듈/알고리즘의 보안 적합성을 검증한다[8,9].

CMVP는 1994년 미국의 NIST가 제정한 FIPS 140-1(Security Requirement for Cryptographic Modules)과 2001년 개정된 FIPS 140-2 표준문서에 정의된 암호모듈이 구비해야 할 보안요구사항을 11개 영역으로 정의하며, DTR(Derived Test Requirements) 표준문서에 정의된 암호모듈 시험요구사항을 정의한다.

FIPS 140 시리즈는 사실상 국제표준이며, 암호모듈검증 국제기준인 ISO/IEC 19790은 FIPS 140-2와 거의 동일하다. ISO/IEC 24759는 ISO/IEC 19790을 위한 시험기준인 DTR에 해당한다.

DTR은 FIPS 140-2를 기준으로 시험 및 검증시 각 보안요구사항 영역(area)별로 '시험항목'(개발자가 제출해야 할 문서이며 개발자의 행동을 정의하고, 시험 항목을 위해 '제출문서'에 명세한 것) 및 '(시험자가 행할) 시험절차'를 명세한 문서이다. NIST의 CMVP 체계에서는 DTR에 따른 시험 지침을 별도의 '구현지침'으로 발표하고 있다[13,15].

CMVP의 시행 주체는 다음과 같다. CMVP에 따른 모든 시험은 NVLAP(National Voluntary Laboratory Accreditation Program) 또는 SCC(Standards Council of Canada)에 의해서 CMTL(Cryptographic Module Testing Laboratory)로 인정된 제3자 시험 기관이 수행하며, 검증 신청자는 인정된 시험 기관에 시험을 의뢰할 수 있다.

2.2 암호 모듈 정책 연구의 필요성

기존의 정보보호제품의 보안성 및 안전성을 강화하기 위해서 정보보호제품에 대한 다양한 평가제도 및 평가기술이 존재하고 있지만 상대적으로 암호 모듈에 대한 평가는 국내 정립이 미흡하다.

암호 모듈의 안정성 평가는 암호 모듈을 기반으로 한 정보보호제품 평가에 있어서 가장 기본이 되는 평가이며, 검증된 암호 모듈을 사용한 제품에 대해 신뢰성을 보장해준다. 우리나라는 CMVP를 기반으로 하여 암호 모듈 검증절차를 마련했음에도 불구하고 일본과 달리 미국과 상호협력체계를 구축하지 않아 국내 업체가 암호 모듈을 이중으로 평가 받아야 하는 어려움이 있다[3].

NIST는 2007년 7월에 FIPS 140-3을 발표하였고, 2009년 11월에 FIPS 140-3 개정초안을 발표하였다. 이후 공람한 후에는 FIPS 140-2를 대체할 것으로 예상된다. 현재 우리나라의 암호 모듈 검증절차는 FIPS 140-2를 참조하였으므로, 미국 내에서 FIPS 140-3이 표준화 될 경우, 절차를 정립할 필요성이 보인다. 특히 FIPS 140-3은 기존 140-1, 2와 달리 최신의 암호 모듈 검증 동향을 반영하여 상당히 많은 부분이 교체되고 있으므로, 우리는 국내 암호 모듈 검증절차의 확립을 위해 국외 암호 모듈 정책, 제도, 법 등의 연구 동향과 흐름을 예의주시할 필요가 있다[3].

미국은 FIPS 140-3을 위한 DTR을 개발할 것이고, 현존하는 암호제품에 대한 평가 방식은 이러한 추세를 반영하기 위해서 변경되어야 한다. 즉 CMVP의 신 기준인 FIPS 140-3에 나타난 기준에 대한 비용효과적인 시험 및 검증 방법을 개발해야 한다.

2.3 국내외 암호 모듈 검증 제도

2.3.1 미국, 캐나다 암호모듈 검증 제도

1995년 7월 미국의 NIST와 캐나다의 CSE는 공동으로 암호 모듈을 검증하기 위하여 CMVP 제도를 개발하였다.

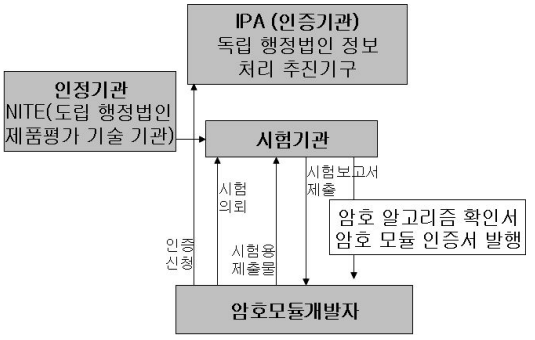
본 제도는 국제 표준인 ISO/IEC 19790의 원형이 되는

FIPS 140-2를 통하여 검증을 수행하며 암호 알고리즘, 해싱알고리즘, 인증알고리즘, 서명 알고리즘, 키관리를 포함한 암호모듈을 시험한다.

2.3.2 일본 암호모듈 검증 제도

일본 정부는 비밀로 분류되지 않은 데이터 보호를 위해서 사용되는 암호 모듈 및 암호알고리즘을 국가기관의 사용을 위해서 JCMVP(Japan CMVP)를 운영한다. JCMVP는 북미 CMVP와 동일한 암호 모듈 보안요구사항 및 시험기준을 채택하고 있다. 2006년 6월 시험운용을 통해 2007년 4월부터 정식 시행 중이다. 최근 미국과 상호협력체계를 구축하여 각 지역의 시험기관에서 시험한 제품에 대해 미국과 일본 기관은 상호 인증하고 있다[11].

다음 그림 1는 JCMVP 제도의 구조를 나타낸 것이다.



[그림 1] JCMVP제도의 구조

2.3.3 국내의 암호모듈 검증제도 분석

국가정보원은 정보화촉진기본법 및 전자정부법 등 관련 법규에 의거, 정보보호제품 평가·인증제도 운영 및 국가기관에 도입되는 상용 정보보호제품의 보안적합성 검증 서비스를 총괄한다. 이중에서 국가기관이 사용하는 상용 암호모듈의 시험 및 검증 등에 필요한 사항은 “암호모듈 시험 및 검증지침”(행자부고시, 제2004-45호)에 규정하고 있다.

국가정보원은 검증된 암호모듈을 탑재한 정보보호제품의 국가기관 도입을 지원하기 위해 보안적합성 검증제도를 시행하고 있고, 이러한 제품이 암호논리의 안전성, 구현 적합성, 공격에 대한 내구성 측면에서 국가기관에서 사용이 가능한지의 여부를 결정하기 위해 비공개 기준을 적용한다.

3. 암호모듈 검증 기준

3.1 암호모듈 검증 기준

미국 CMVP 기준의 모체는 Federal Standard 1027이며, 동 기준은 DES 암호 알고리즘을 사용하는 정보보호 시스템의 일반 보안요구사항으로 하드웨어 중심적이며, 암호모듈 검증절차를 제한적으로 적용하고 있다. 따라서 Federal Standard 1027을 대체하기 위해 NIST는 FIPS 140 기준을 제정하였다[4].

현재 FIPS 140 시리즈는 3번째 버전이 발표되었고, NIST는 2009년 11월에 개정된 FIPS 140-3이 발표하였다. FIPS 140 시리즈의 내용은 다음과 같다[4].

- FIPS 140-1(1994년)은 암호모듈 검증정책 및 검증절차를 4개의 보안등급과 10개의 요구사항 영역으로 구분한 최초의 기준이다. FIPS 140-1은 하드웨어 중심으로 소프트웨어로 구현된 암호모듈도 암호모듈로 간주한다[12].
- NIST는 FIPS 140-1을 재구성하여 요구사항을 명확히 정의한 FIPS 140-2를 발표하였다. FIPS 140-2는 요구사항을 11개 영역으로 증가시킨다. NIST는 FIPS140-2에서 개발자가 검증자를 위해서 DTR을 개발할 것을 요구하고 있으며, 설계보증개념을 추가하였다. ISO/IEC 는 FIPS 140-2를 기반으로 국제표준인 ISO/IEC 19790(2006년)은 제정하였다[15].
- NIST는 2007년 7월에 FIPS 140-3의 초안을 발표하였고, 2009년 11월에 개정 초안을 발표하였다. NIST는 FIPS 140-3에 최신의 고급 보안 기술 및 방법을 반영하기 위해 기존의 문서에 새로운 보안 기능을 추가하였다. 새로운 소프트웨어 및 펌웨어 보안 영역과 보호되지 않는 요구사항을 포함한 비침투공격을 고려하여 소프트웨어 및 펌웨어 요구 사항을 지정하였다[16,17].

현재 대부분의 국가가 암호모듈 검증절차로 CMVP를 사용하고 있다. 가장 활성화된 암호모듈 검증절차가 미국 및 캐나다의 CMVP이고, 실제 암호 모듈 검증을 위한 국제기준인 ISO/IEC 19790은 FIPS 140-2와 거의 동일하다[10].

국내외 암호모듈 정책의 현황 분석을 위해서는 국내외 암호모듈 정책의 모태가 되고 있는 CMVP 분석이 필수적이다. 표 1은 각 국가가 사용하고 있는 CMVP 버전을 보여주고 있다.

[표 1] 각국의 CMVP 기준의 분류

기준별 / 국가별	암호모듈 검증기준 (CMVP)			암호모듈 시험기준 (DTR)		
	기준년	발행년도	상태	기준년	발행년도	상태
미국 및 캐나다 (CMVP)	NIST FIPS 140-1	1994.1	폐지	DTR for FIPS 140-1	1995.3	폐지
	NIST FIPS 140-2	2001.5	현재 표준	DTR for FIPS 140-2	2004.3	현재 표준
	NIST FIPS 140-3	2007.7	초안 (2009.11 개정초안)	DTR for FIPS 140-3	N/A	N/A
국제	ISO/IEC 19790	2006.3	현재 표준	ISO/IEC 24759	2007.5	현재 표준
한국 (KCMVP)	암호검증기준 (FIPS 140-2 참조)	2006.11	현재 표준	암호시험기준 (DTR 참조)	2007.3	현재 표준
	KS X ISO/IEC 19790	2007.12	현재 표준	KS X ISO/IEC 24759	2007.12	현재 표준
일본 (JCMVP)	JIS X 19790 (FIPS 140-2 참조)	2007.3	현재 표준	JIS X 5091 (DTR 참조)	2007.3	현재 표준

3.2 암호 모듈 검증기준과 국제공통평가기준 (CC)와의 관계

CMVP는 정보시스템의 컴포넌트인 암호모듈을 시험 및 검증하는 기준 및 절차이고, 국제공통평가기준(CC)은 정보보호제품 및 정보시스템을 평가 및 인증하는 기준이다. 표 2는 CC V.3.1과 CMVP(FIPS 140)간의 개념을 비교한다[5].

[표 2] CMVP와 CC간의 개념의 대응

CC V.3.1	CMVP(FIPS 140)
기능 클래스(10종)	승인된 암호 알고리즘
보증 클래스(8종)	요구사항 영역(11종)
보증 엘리먼트 - 보증 컴포넌트당 1개 이상	시험항목 (Assertions) - 부 영역당 1개 이상
평가수준 - Evaluation Assurance Level 1~7)	평가수준 - Security Level 1~4
종속관계 있음	종속관계 없음
개발자 요구사항	시험항목
평가자요구사항 (evaluator action elements)	시험절차(required test procedure)
보안목표명세서(ST)	암호 모듈 보안정책

CC와 암호모듈 검증기준은 모두 평가대상물(제품 또는 암호 모듈)의 보안기능과 보증수준을 별도로 정의한다. CC는 보안 기능을 대상으로 평가를 하고, 보증 수준에 따라 보안 등급을 평가한다. 암호모듈 검증기준은 '승인된(approved)' 보안함수를 최저등급(1등급)에서 최고 보안등급(4등급)으로 검증할 수 있다.

3.3 암호모듈 검증 기준 분석

2009년 개정된 FIPS 140-3은 보안등급을 4단계로 나누고 있다. FIPS 140-3 초안에는 보안등급을 5단계로 나누고 있으나, 개정된 FIPS 140-3은 5단계의 보안등급을 FIPS 140-1, 2와 동일하게 4단계로 구분한다[17].

개정된 FIPS 140-3의 4단계 보안등급은 다음과 같다.

보안등급 1 : 보안등급 1은 가장 기본 등급의 안전성을 보장한다. 보안등급 1에 해당하는 암호모듈은 적어도 하나 이상의 승인된(표준) 알고리즘 혹은 승인된 안전한 함수를 사용해야 한다. 보안등급 1은 높은 수준의 CPS가 필요하지 않은 암호 모듈을 사용하는 환경에서 비용 효과적으로 적용된다.

보안등급 2 : 보안등급 2는 보안등급 1에 물리적 보안 메커니즘 부분을 보완시킨 등급이다. 물리적 보안 메커니즘은 tamper-evidence에 대한 안전성 요구사항을 포함한다. tamper-evident coating과 봉인은 암호모듈 내에서 CPS에 속하며, 침입자의 물리적 접근을 차단한다. 보안등급 2는 역할 기반의 암호모듈을 통해 관리자 인증 및 인가를 수행할 것을 요구한다. 보안등급 2는 소프트웨어 암호 모듈에 대한 최대 안전 수준이다.

보안등급 3 : 보안등급 3은 보안등급 2의 물리적 보안 요구사항에 암호모듈 내의 CPS에 대한 허가되지 않은 접근을 차단하는 것을 추가한다. 보안등급 3에서 요구되는 물리적 보안 장치에는 구멍 또는 틈새를 통하여 암호 모듈로 침입하려는 시도를 검출하는 기능이 요구된다. 보안등급 3은 보안등급 2에서 요구된 역할 기반의 인증 메커니즘을 강화하여 신원 기반의 인증 메커니즘을 요구한다. 보안등급 3은 소프트웨어 암호 모듈을 위한 기준을 제안하지 않는다.

보안등급 4 : 보안등급 4는 FIPS 140-3에서 제정한 가장 높은 안전성을 제공하는 등급이다. 보안등급 4는 물리적 보안 메커니즘이 해당 암호모듈의 인가되지 않은 모든 물리적 접근을 완벽하게 방어, 봉쇄해야 한다. 보안등급 4의 물리적 보안 메커니즘은 암호모듈의 내부에 침입이 있을 경우에는 탐지가 가능해야 하며, 모든 CSP와 하드웨어 자체에 대한 보안이 수행되어야 한다. 보안 등급 4의 암호모듈은 물리적으로 위험한 보안 환경에서 효과적이다. 보안 등급 4에서는 관리자에 대해 적어도 암호, 물리적 인증도구, 생체인식 등의 세 가지 방법 이상으로 인증할 것을 권장하고 있다.

4. 암호모듈 보안 요구사항 연구

4.1 암호모듈 명세

4.1.1 보안요구사항 명세

FIPS 140-3의 보안 요구사항 명세는 암호 모듈의 보안 설계와 배치에 관련되어 있다. 다음의 요구사항은 보안 암호모듈의 보안 목적을 나타낸 것이다[17].

- 민감한 정보의 보호를 위해 입증되거나 허락되어진 보안 기능이 바르게 사용되고 배치되게 유지함.
- 암호 모듈의 내용이 노출이 되지 않게 방지함.
- 암호 모듈과 암호알고리즘이 SSP의 인증되지 않은 변경, 교체, 삽입, 삭제가 되지 않도록 함.
- 암호 모듈의 운영상의 오류를 찾고 민감한 데이터와 SSP의 오류로 인한 손상이나 변경을 방지함.
- 암호 모듈의 적절한 설계, 배포 및 구현을 보증함.

4.1.2 암호 모듈의 유형

암호모듈은 하드웨어, 소프트웨어, 펌웨어 등의 유형으로 나누어지고, 승인된 암호알고리즘, 기능, 프로세스 등으로 구성된다. 암호 모듈의 유형은 다음과 같다[17].

- 하드웨어 모듈은 암호모듈이 하드웨어 형태로 존재한다. 운영 시스템을 포함하는 펌웨어도 하드웨어 암호모듈에 포함되어야 한다.
- 소프트웨어 모듈은 수정 가능하고 한계적인 운영 환경에서 사용되는 소프트웨어 컴포넌트이다. (하나 또는 다중 소프트웨어 컴포넌트)
- 펌웨어 모듈은 수정 불가능하고, 제한된 운영 환경에서 사용되는 펌웨어 컴포넌트이다.
- 하이브리드 모듈은 소프트웨어와 펌웨어 컴포넌트가 합성된 모듈이거나, 하드웨어 컴포넌트가 분해된 형태이다. (소프트웨어와 펌웨어 컴포넌트의 합성으로 이루어진 하이브리드 모듈은 물리적 암호 하드웨어에 포함되지 않는다.)

4.2 암호 모듈 인터페이스

4.2.1 암호 모듈 인터페이스의 종류

암호 모듈은 모듈의 암호 범위에서 입구와 출구로 물리적인 접근 지점과 논리적인 인터페이스에 있는 모든 논리적인 정보 흐름을 제한한다. 암호 모듈 인터페이스는 1개의 물리적인 포트를 공유하더라도 서로에게 논리적으로 별개로 존재할 수 있고, 또는 1개 이상의 물리적인 포트에 분배될 수 있다.

4.2.2 인터페이스상의 신뢰 채널

암호 모듈은 전용 인터페이스나 포트에 신뢰성 있는 채널을 제공하고, 이 채널을 통해 SSP, 서비스 요구 및 서비스를 안전하게 제공해야 한다. 신뢰성 있는 채널은 다음과 같은 요구조건이 필요하다[17].

- 모듈 문서는 신뢰성 있는 채널을 지원하기 위하여 프로토콜과 승인된 보안 기능을 명세해야 한다.
- 승인된 암호 보안 기능은 신뢰성 있는 채널을 지원하기 위해 모듈을 사용해야 한다.
- 모듈은 모듈 운영자에게 신뢰된 채널의 사용 여부를 표시해야 한다.

4.3 역할, 인증 및 서비스

4.3.1 역할

암호 모듈은 운영자를 위해 운영자를 인증 지원해야 하고, 역할에 따른 서비스를 지원해야 한다. 암호 모듈은 최소한 암호 관리자 권한을 지원해야 한다. 암호관리자는 암호 초기화 설정, 관리적 기능, 일반적인 보안 서비스 등을 실행할 수 있어야 한다[17].

암호 모듈은 신뢰할 수 있는 권한을 지원해야 한다. 신뢰할 수 있는 권한은 모듈이 암호 환경에서의 실행과 기타 승인된 보안 기능을 수행할 수 있도록 한다. 암호 운영자가 신뢰할 수 있는 권한을 구성한다.

4.3.2 인증

인증 메커니즘은 암호 모듈에 접근하는 운영자를 인증하고, 운영자의 권한을 수행하게 하고, 권한에 필요한 서비스 수행을 검증해야 한다[17].

인증 메커니즘에서 사용되는 인증 유형은 역할 기반 인증과 신원 기반 인증 등이 있다.

운영자가 성공적으로 인증이 되기 전까지, 운영자에게 권한 및 신뢰된 채널 설치를 제외하고, 승인된 서비스나 보안기능이 제공되지 않는다.

5. 보안 요구사항 영역별 변화 연구

5.1 목차 비교

표 3은 CMVP의 각 기준, FIPS 시리즈의 목차 차이를 나타낸다.FIPS 140-1과 2는 큰 변화가 없고, 특히 FIPS 140-2는 ISO/IEC 19790과 매우 흡사하다. 반면에 FIPS 140-3 초기버전은 기존의 문서에 비해 많은 변화가 있었다. 따라서 기존 CMVP 기준의 척도였던 FIPS 140-2에 맞춘 국내 기준의 변화가 예상된다.

5.2 관련법의 변화

FIPS 140-2는 “Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106”에 근거를 두고 있지만, FIPS 140-3은 이것과 FISMA로 알려진 “Federal Security Management Act of 2002(Public Law 107-347)”에 근거를 두고 있다.

5.3 보안 등급의 변화

2009년 11월에 발표된 FIPS 140-3 개정안은 기존과 같이 다시 4개 등급으로 조정되었다. 기존의 FIPS 140-3에서 추가되었던 5등급은 4개 등급으로 조정되면서 4등급으로 흡수되었으며, 일부 최신의 동향에 맞지 않는 문항은 삭제되었다[17].

- 1등급 : 기존과 동일
- 2등급 : 접근제어목록(access control lists, ACL)을 통해 변경 가능한 환경에서의 운영자 역할 인증 절차 수립
- 3등급 : 비침투성 공격 차단 추가
- 4등급 : 운영자에 대해 암호, 물리적 인증도구, 생체인식의 세 가지 방법으로 인증할 것을 권장

6. 국내 암호모듈 검증제도 발전 방향

6.1 국내 암호 모듈 검증 제도 연구

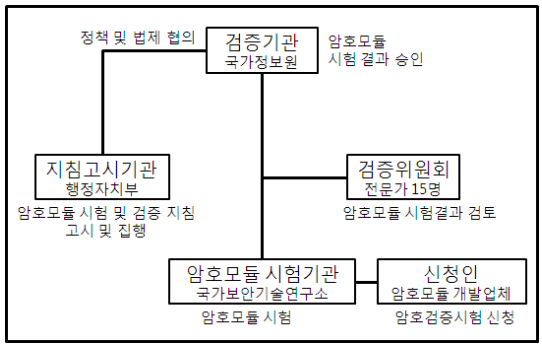
6.1.1 암호검증제도

암호검증제도는 암호구현 오류 발생 및 무분별한 공개 프로그램 사용, 암호제품 상호 호환성 확보 곤란, 안전한 제품의 개발을 위한 가이드라인의 부재 등의 필요성을 인식하고, 암호 모듈 시험 및 검증지침에 따라 2008년 말부터 국가정보원에서 수립한 제도이다[1,2].

암호검증제도의 목적은 국가 암호정책을 바탕으로 국가용 암호알고리즘을 선정하고, 암호 알고리즘을 바탕으로 구현된 상용 암호 모듈의 정확성 및 안전성에 대한 독자적인 시험평가체계 구축을 통해 국가기관의 암호 사용의 안전성을 확보한다.

암호검증제도의 적용대상은 행정 기관용 및 대국민 행정업무용 암호 모듈이다[1,2].

그림 2는 암호 모듈 시험 및 검증 수행체계를 나타낸다. 그림 2과 같은 수행체계를 통해 국내 암호검증제도를 수행한다.



[그림 2] 암호 모듈 시험 및 검증 수행체계

6.2 국외 CMVP와의 비교 연구

미국, 유럽 및 일본은 각자 암호모듈 검증 제도를 도입했고, 특히 미국 CMVP 제도는 검증을 받은 모듈이 1,000개를 넘어설 정도로 활성 되어 있다. 일본은 JCMVP제도를 도입하였다. 미국과 일본은 상호협력체계를 구축하여 지역의 시험기관이 시험한 제품에 대해 상호 검증필을 부여하고 있다. 미국은 총 16개의 시험기관, 일본은 3개의 시험 기관을 운영하고 있어 수요자가 편리하게 암호모듈 시험을 받을 수 있다[11].

향후 우리 암호모듈 검증제도의 발전 방안을 살펴보면 다음과 같다.

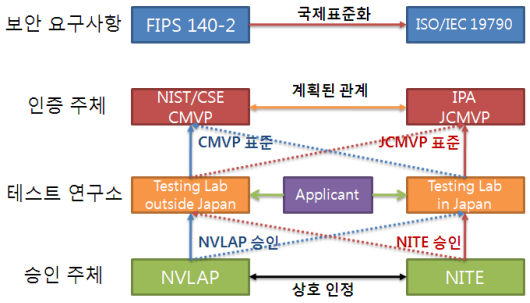
첫째, 우리나라는 암호검증기준을 FIPS 140-3의 개정된 기준을 반영해야 한다. 국외의 암호모듈 검증 정책과 우리나라의 암호검증제도는 시발점이 같으나 독자적으로 발전함에 따라 현재는 다른 모습을 보이고 있다. 새롭게 개발된 FIPS 140-3의 바뀐 규정을 현재 우리나라의 암호검증제도는 반영하지 못하고 있다. 표 4는 한국, 미국, 일본의 암호검증 체계를 비교 분석한다.

[표 4] 각국의 암호검증체계 비교

	암호검증제도(한국)	CMVP (미국/캐나다)	JCMVP(일본)
시작년도	2005년 1월	1995년 7월	2006년 6월
검증기관	인증사무국	NIST/CSE	IPA
시험기관	국가보안기술연구소	16개 시험소 운영 미국(9), 캐나다(2), 영국(1), 독일(1), 스페인(1), 일본(1), 대만(1)	- IT Security Center, IPA - ECSEC lab - Kanasai Testing Center, JQA
검증기준	KS X ISO/IEC 19790	FIPS 140-2	JIS X 19790
시험기준	KS X ISO/IEC 24759	FIPS 140-2 DTR	JIS X 5091
알고리즘 검증기준	암호알고리즘 검증기준	각 알고리즘 별로 FIPS SP(Special Publication) 문서에 명시되어 있음	JCMVP Cryptographic Algorithm Implementation Testing Requirements (ATR-01)
상호협력	상호협력 없음	일본 JCMVP와 상호협력	미국 CMVP와 상호협력

둘째, 해외 국가와의 상호협력 체계의 구축을 위한 정책 및 제도의 보완이 필요하다. 현존 암호모듈 검증체계는 국내 암호모듈만을 대상으로 검증을 실시하고 있고, 국내에서 검증된 암호모듈 검증이 국외에서 사용되는 경우 추가적인 검증이 필요하다. 외국과의 부분적인 상호인증체계의 구축을 통해서 국내 암호모듈의 국제인증이 필요하다.

그림 3은 미국과 일본의 암호검증 상호협력 체계를 나타낸다[11].



[그림 3] 미국, 일본의 암호검증 상호협력 체계

암호모듈 검증 체계는 CCRA처럼 국제적인 상호협력 인증 체계가 구축되지 않았지만, 암호검증 체계의 선진국이라 할 수 있는 미국과 일본을 필두로 하여 CMVP RA가 구축될 것으로 예상된다. 우리나라는 자국의 암호검증 체계를 최대한 표준화 동향에 맞추어 향후 예상되는 협력 체계에 참여해야 할 것이다.

셋째, 암호모듈 시험기관의 시험 능력 확충이 필요하다. 향후 암호모듈 시험 수요가 기하급수적인 증가가 예상된다. 따라서 현재 2곳의 암호모듈 시험기관 시험 능력 확충이 필수적이다. 암호모듈 시험기관의 추가 지정 등은 대안이 될 수 있지만, 현재 국내 암호모듈 시험 기술이 높지 않은 상황에서 암호모듈의 추가적인 지정은 시험기술 발전에 도움이 되지 않는다. 현재 암호모듈 시험기관의 시험 능력 확충 및 발전에 필요한 투자를 통해서 우리나라 암호모듈 시험 기관의 수준을 향상시키는 전략이 필요하다.

6. 결론

국외 선진국은 암호모듈의 안정성을 활발히 검증하고 있어 정보보호제품에 대한 신뢰성을 증가시키고 있고, 개발자에게 제품 개발에 대한 가이드라인을 제공하고 있다. 그러나 국외 선진국은 암호모듈 검증기술을 공개에 소극적임으로 우리나라는 최신 암호모듈 검증 기술을 반영하여 새로운 암호모듈 검증 절차를 개발할 필요가 있다. 특히 우리나라는 최신 암호 모듈기술을 발전시키고 있는 추세이며, 선진국과 기술적인 차이가 좁혀지고 있는 상황이다. 암호모듈에 대한 안정성 평가 체계 확립은 국외 선진국과의 정보보호 분야에서 경쟁 우위를 확보할 수 있는 수단이다.

본 연구는 다음과 같이 활용할 수 있다. 국외의 활성화된 암호 모듈 검증절차를 분석을 통해 국내 암호모듈 검증절차 발전에 기여할 수 있다.

본 연구는 최근 변경된 FIPS 140-3을 중심으로 FIPS 140-1, FIPS 140-2 등을 비교하여 국내 연구기관이 미국 및 캐나다의 CMVP 정책 및 제도를 활용할 수는 시사점을 제공한다.

본 연구는 미국 및 캐나다 이외에도 일본의 암호모듈 검증 제도의 현황 및 발전 추세를 분석하고 있다. 동 국가는 암호모듈 검증에 있어서 북미국가에 비하여 후발국이다. 향후 우리나라와 암호모듈 검증 제도 발전에 있어서 상호 이익을 공유할 가능성이 매우 높은 국가이다. 동 국가의 암호모듈 검증제도의 발전 현황, 추세 및 전망은 우리나라의 암호모듈 발전에 시사점이 될 수 있다.

본 연구는 국외 암호모듈 검증 정책 및 제도의 발전 현황 및 전망을 토대로 우리나라의 암호모듈 검증제도의 발전 방향 및 정책 수립과 관련된 정책을 제언하고 있다. 본 연구가 제언하고 있는 정책 방향은 향후 우리나라의 암호모듈 검증제도 발전에 있어서 시사점이 될 것으로 판단된다.

참고문헌

[1] 기술표준원, "암호검증기준", KS X ISO/IEC 19790, December 2006.

[2] 기술표준원, "암호시험기준", KS X ISO/IEC 24759, December 2007.

[3] IT보안인증사무국, "국내외 상용 암호 모듈 검증정책", 정보과학회지 제25권 제5호, May 2007.

[4] 고갑승, 배익환, 최성자, 이강수, "신 암호 모듈 검증 기준 FIPS PUB 140-3의 변경내용 분석", 정보보호학회지 제17권 제6호, December 2007.

[5] CC, “Common Criteria for Information Technology Security Evaluation”, Part1~Part3, Version 2.1, CCIMB-99-031, August 1999.

[6] Christopher King. “Extranet Access Control Issues,” in Harold F. Tipton and Micki Krause, ed., Information Security Management Handbook. Vol. 2,

New York: Auerbach, 2000
[7] CMVP, http://csrc.nist.gov/groups/STM/cmvp/index.html
[8] CSE, Guide to Certification and Accreditation of Information Technology Systems, Government of Canada, Communications Security Establishment, 1996.
[9] CSE, Guide to Security Risk Management for IT Systems, Government of Canada, Communications Security Establishment, 1996.
[10] ISO/IEC, "Information technology- Security techniques -Security requirements for cryptographic modules", ISO/IEC 19790, March 2006.
[11] JCMVP, http://www.ipa.go.jp/security/english/jcmvp.html
[12] NIST, "Security Requirements for Cryptographic Modules", NIST FIPS 140-1, January 1994.
[13] NIST, "Security Requirements for Cryptographic Modules", NIST Derived Test Requirements for FIPS 140-1, March 1995.
[14] NIST, "Security Requirements for Cryptographic Modules", NIST FIPS 140-2, May 2001.
[15] NIST, "Security Requirements for Cryptographic Modules", NIST Derived Test Requirements for FIPS 140-2, March 2004.
[16] NIST, "Security Requirements for Cryptographic Modules", NIST FIPS 140-3(Draft), July 2007.
[17] NIST, "Security Requirements for Cryptographic Modules", NIST FIPS 140-3(Revised DRAFT), November 2009.

최 명 길(Myeonggil Choi) **[정회원]**

- 2004년 9월 : 한국과학기술원 박사
- 1995년 9월 ~ 2000년 1월 : 국방 과학연구소 연구원
- 2000년 2월 ~ 2005년 8월 : 한국 전자통신연구원 선임연구원
- 2005년 9월 ~ 2008년 2월 : 인제 대학교 조교수
- 2008년 3월 ~ 현재 : 중앙대학교 조교수

<관심분야>
창업정책, 기술창업, 보안성평가, 정보보호정책 및 관리

정 재 훈(Jaehun Jeong) **[준회원]**

- 2003년 3월 ~ 2009년 2월 : 인제 대학교 시스템경영공학과 학사 졸업
- 2009년 3월 ~ 현재 : 중앙대학교 일반대학원 경영학과 석사 재학

<관심분야>
기술창업, 암호모듈 및 알고리즘, 시스템 보안