5

# 국내 · 외 商用 암호모듈 검증정책

IT 보안인증사무국
http://www.kecs.go.kr

## 1. 배 경

초기 암호기술은 군사목적이나 외교통신 등 주로 국가안보와 연계된 분야에서 은밀히 사용되어져왔다. 그 후 1970년대 후반 공개키 암호알고리즘으로 대표되는 현대 암호기술이 개발되면서 암호기술은 개방된 네트워크 환경에서의 통신이나 이를 이용한 전자상거래 등 민간 분야에서의 안전 · 신뢰성을 확보하는데 있어서 꼭 필요한 기술이 되었다. 이는 주로 비밀유지를 목적으로 하던 정부주도의 암호기술 개발체계가 사회 · 경제적 가치 보호를 위한 민간주도 암호기술 개발체계로 확장되었음을 의미한다.

세계 암호기술을 선도하는 미국의 경우 정부주도로 개발한 블록 암호알고리즘 표준인 DES(Data Encryption Standard)를 대체하여 민간주도로 개발한 AES (Advanced Encryption Standard)를 국가표준으로 채택하였으며, 지난 1월 기존의 해쉬함수 표준인 SHS(Secure Hash Standard)를 대체할 새로운 해쉬함수 표준을 공모사업을 통해 선정하기로 발표하였다. 향후 암호기술의 급속한 발전 속도를 감안할 때, 이러한 민간주도 암호기술의 개발 및 표준화 활동은 더욱 강화될 것으로 전망된다[6].

또한 북미를 비롯한 세계 각국은 국가기관에서 소통되는 중요자료(비밀자료 제외)의 위 · 변조, 훼손, 유출 등을 방지하기 위해 안전성이 검증된 암호모듈의 사용을 의무화하고 있다. 이러한 추세에 따라 각국 정부는 민간에서 개발한 암호모듈이 갖추어야 할 최소 요구사항과 이를 시험하기 위한 평가기준을 개발하여 암호모듈의 객관 · 신뢰성 확보를 위한 암호모듈 검증제도를 구축 · 운영하고 있다[2-4][8-9].

따라서 본 논문에서는 국가기관에서 사용되는 암호기술의 안전성을 검증하기 위해 북미를 중심으로 시작되어 현재 국제표준으로 인식되고 있는 CMVP(Cryptographic Module Validation Program)[8]에 대해 알아보고, 미국, 영국, 일본 등 세계 각국 국가기관에서 암호기술을 사용하기 위해 운영 중인 정책에 대해 소개한다[12-16].

## 2. CMVP (Cryptographic Module Validation Program)

CMVP는 1995년 미국 NIST(National Institute of Standards and Technology)와 캐나다 주정부의 CSE(Communications Security Establishment)가 공동으로 개발한 암호모듈 검증제도로, 표준에 따라 구현된 암호 모듈 · 알고리즘의 보안적합성을 평가한다.

이를 위해 CMVP는 1994년 미국의 NIST가 제정한 FIPS 140-1(Security Requirement for Cryptographic Modules)과 2001년 개정된 FIPS 140-2 표준문서를 통해 암호모듈이 갖추어야 할 보안 요구사항을 11개 영역으로 구분하여 정의하고 있으며, DTR(Derived Test Requirements) 표준문서를 통해 암호모듈 시험 요구사항을 정의하고 있다[9]. 현재 FIPS 140-2는 국제 표준화기구(ISO/IEC) JTC1/SC27 분과에서 국가별 요구사항이 상이한 부분(EMI/EMC 등)을 배제하고 ISO 19790 국제표준으로 채택되었으며, DTR은 Project 24759로 국제표준화가 진행 중이다[5].

CMVP에 따른 모든 시험은 NVLAP(National Voluntary Laboratory Accreditation Program) 또는 SCC(Standards Council of Canada)에 의해 CMTL(Cryptographic Module Testing Laboratory)로 인정된 제3자 시험기관에서 수행되며, 검증신청자는 인정된 시험기관 중 하나에 시험을 의뢰할 수 있다. 아래 그림은 NIST/CSE를 검증기관, CMTL이 시험기관 역할을 수행하는 암호모듈 검증절차를 설명한다.

### 2.1 암호모듈 보안 요구사항

ISO 19790은 S/W, H/W, F/W 등의 형태로 구현된 암호모듈이 갖추어야 할 최소 요구사항을 4단계의 보안등급 및 10개의 보안 요구사항 영역으로 명시하고 있다. 높은 수준의 보안등급은 낮은 수준의 보안등급이 요구하는 보안 요구사항을 모두 만족하며, 보안등급에 따른 각 영역별 보안 요구사항은 아래 내용을 포함한다[2,7,9].

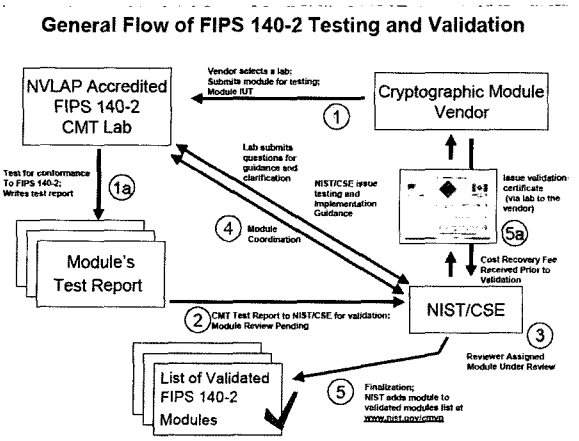


그림 1 CMVP 수행체계 및 검증절차

### 2.2 CMTL(Cryptographic Module Testing Laboratory)

미국 NIST NVLAP 또는 캐나다 SCC에 의해 인정되는 CMTL은 'NIST Handbook 150-XX' 표준문서에 명시된 모든 요구사항을 충족해야 한다. NIST Handbook 150(NVLAP Procedures and General Requirements)은 시험기관이 갖추어야 할 기본적인 기술·관리적 요구사항[10]을 명시하고 있으며, NIST Handbook 150-17 (IT Security Testing- Cryptographic Module Testing)은 암호모듈 시험을 위한 보다 세부적인 요구사항[11]을 정의하고 있다.

현재 전 세계적으로 13개 CMTL이 운영되고 있으며, FIPS 140-1(2)에 따라 안전성이 검증된 암호모듈은 742개에 달하고 있다(오스트레일리아, 브라질, 캐나다, 핀란드, 프랑스, 독일, 이스라엘, 일본, 노르웨이, 중국, 싱가포르, 남아메리카공화국, 스페인, 스위스, 미국, 영국 등 16개국 참여).

## 3. 국내·외 상용 암호모듈 검증정책 동향

### 3.1 미국의 상용 암호모듈 검증정책[12]

미국 NSA(National Security Agency)는 상용 암호모듈 및 암호알고리즘 구현의 보안적합성을 평가하고 이를 정부조달을 위한 기준으로 사용하기 위해 NIST와 캐나다 주정부의 CSE가 공동 개발한 CMVP를 활용한다. 그러나 CMVP를 통해 검증된 암호 모듈·알고리즘은 비밀로 분류되지 않은 데이터보호를 위해 국가기관에서 사용될 수는 있으나, 비밀로 분류된 데이터보호 및 국가보안시스템에서는 사용할 수 없는 제한을 가진다.


그림 2 암호모듈 시험기관 현황

표 1 10개 영역별 보안 요구사항 요약

| | 보안등급 1 | 보안등급 2 | 보안등급 3 | 보안등급 4 |
|---|---|---|---|---|
| 암호모듈 명세 | 암호모듈 경계, 검증대상 보호함수 및 검증대상 동작모드 명세, H/W 및 S/W 등 구성요소를 포함한 암호모듈에 대한 서술, 암호모듈 보안정책 | | | |
| 포트/인터페이스 | 필수/선택적 인터페이스, 모든 인터페이스 및 입/출력 데이터 경로 명세 | | 다른 데이터 포트와 논리적/물리적으로 분리된 핵심 보안변수 데이터 포트 | |
| 역할/서비스 인증 | 필수/선택적 역할과 서비스의 논리적분리 | 역할기반/신원기반 운영자 인증 | 신원기반 운영자 인증 | |
| 유한상태모델 | 유한상태모델 명세, 상태천이 다이어그램, 상태천이 명세 | | | |
| 물리적보안 | 상용 품질수준 장비 | 잠금장치/불법조작 증거 | 덮개/문에 대한 불법조작 탐지/대응 | 모든 불법조작 탐지/대응 |
| 운영환경 | 단일 운영자, 실행 가능한 코드, 검증대상 무결성 | EAL2 수준의 운영체제 | EAL3 수준의 운영체제 | EAL4 수준의 운영체제 |
| 암호키관리 | 난수 발생 및 키 생성, 키 설정, 키 분배, 키 주입/출력, 키 저장 및 제로화 관리 | | | |
| | 개인/비밀키 수동 설정시, 평문형태로 암호모듈 주입/출력 가능 | | 개인/비밀키 수동 설정시, 암호화된 형태로 암호모듈에 주입/출력 | |
| 자가시험 | 전원인가 시험, 암호알고리즘 시험, 무결성 시험, 조건부 시험 | | | |
| 설계보증 | 형상관리, 안전한 설치, 설계/정책의 일치성 설명 | 형상관리시스템, 안전한 배포, 기능명세 | 고급언어를 사용한 구현 | 정형모델, 비정형적 증명을 포함한 설명 |
| 기타공격 대응 | 차분전력분석, TEMPEST 등 해당공격을 완화하기 위한 보안정책과 메커니즘 명세 | | | |

이와 함께, NSA는 국가기관에서 비밀로 분류된 데이터보호 및 국가보안시스템에서의 상용 암호 모듈·알고리즘의 사용을 통제하기 위하여 'Suite B·A'로 알려진 암호정책을 운용한다. 'Suite B' 정책은 특정 암호알고리즘의 사용(AES 등), 암호키 길이의 통제(해쉬 256비트 등), 특정 암호키 분배·관리 메커니즘의 사용(Elliptic Curve Diffie-Hellman 등) 등 필수 요구사항을 정의하고 있으며, 'Suite A' 정책은 'TOP SECRET' 수준의 비밀자료 보호를 위해 비공개 암호알고리즘의 사용 등을 명시하고 있다.

또한, NSA는 'Suite B·A' 정책을 준수하는 암호모듈을 탑재한 암호제품의 국가기관 조달을 지원하기 위해 CCEP(Commercial COMSEC Evaluation Program) 및 UPA(User Partnership Agreements)를 운영한다.

CCEP는 상용 통신보안제품 보증을 위한 평가제도로, NSA는 CCEP 평가를 신청한 업체의 제품이 DoD(Department of Defense)에서 요구하는 보증등급을 획득할 수 있도록 지원한다. 이 때 NSA는 이러한 제품이 품질, 가격, 안전성 측면에서 국가기관에서 사용가능한지의 여부를 평가하기 위해 비공개 기준을 적용한다.

UPA는 각급 국가기관의 특정 요구사항을 만족하는 제품을 효율적으로 개발하도록 지원하는 제도로, NSA는 해당 요구사항을 제기한 각급 국가기관의 프로그램관리자와 협력하여 보안요구사항 및 규격을 도출하고, 개발이 완료된 제품이 해당 요구사항을 만족하는지를 평가한다.

### 3.2 캐나다의 상용 암호모듈 검증정책[13]

캐나다 주정부의 CSE(Communications Security Establishment)는 TB(Treasury Board)의 GSP(Government Security Policy)에 따라 모든 IT 제품·시스템의 정보보증서비스 업무를 총괄한다.

그 중에서 CEP(Cryptographic Endorsement Program)는 암호모듈 및 암호알고리즘을 탑재한 암호제품이 GSP에 적합한지를 평가하여 국가기관에서의 사용을 승인한다. 이 때 제품에 탑재된 암호 모듈·알고리즘은 CMVP를 통해 검증된 것이거나 또는 CSE에서 승인된 것을 사용해야 한다. 승인된 암호제품은 정부조달을 지원하기 위해 IPPP(ITS Pre-qualification Product Program)를 통해 등재한다.

### 3.3 영국의 상용 암호모듈 검증정책[14]

영국의 GCHQ(Government Communications Headquarters) 산하에서 정보보증업무를 총괄하는 CESG(Communication and Electronics Security Group)는 다원화된 정보보증서비스를 IACS(Information Assurance and Consultancy Services)로 일원화하여 운영하고 있으며, 이 중에서 상용 암호모듈을 탑재한 암호제품의 정부 조달을 지원하기 위해 CAPS(Cryptographic Assisted Products Scheme)를 시행하고 있다.

CAPS는 국가기관에서 사용되는 암호제품을 3단계의 보안등급(Baseline, Enhanced, High)으로 구분하고 있으며, 비밀로 분류되지 않은 데이터보호를 목적으로 암호제품에 탑재된 암호모듈 및 암호알고리즘의 경우 CMVP를 통해 검증된 것의 사용을 권고한다. 현재 영국에는 2개의 CMTL이 존재하며, 10개의 검증완료 암호모듈이 존재한다.

한편, CESG는 검증이 완료된 제품이 각급기관의 운영환경에서 발생할 수 있는 위협 및 취약점에 대해 적절한 대응책을 가지고 있음을 재평가하고, 국가정책(Infosec Standard No.1) 부합 여부를 검증하기 위해 TAS(Tailored Assurance Service)를 추가로 시행한다.

### 3.4 일본의 상용 암호모듈 검증정책[15]

일본 내각관방 산하 NISC(National Information Security Center)는 국가보안 정책을 총괄하는 기구로 각급기관에 적용할 수 있는 표준 개발, 각급기관의 정보보호 대책 평가 및 안전한 보안환경 설계·구축 지원 서비스를 제공한다. 그 중에서 국가기관의 안전한 암호제품 도입 및 개발 지원은 METI(Ministry of Economy, Trade and Industry) 산하 IPA(Information Technology Promotion Agency)에서 운영하는 CRYPTREC(Cryptography Research and Evaluation Committees)을 통해 운영된다.

CRYPTREC은 2000년 일본의 통상성에 의해 전자정부의 안전성을 보증하는 암호기술을 평가하기 위해 만들어졌으며, 현재는 일본 전자정부에 사용가능한 암호기술의 평가기준 및 시험방법론 등 암호기술의 모든 것을 책임지고 있다. 즉, 암호기술 및 상용 암호제품을 대상으로 보안적합성 및 보안강도를 평가하여 안전한 전자정부 구현을 위한 국가기관에서의 암호기술 사용 지침으로 사용되고 있다.

최근에는 비밀로 분류되지 않은 데이터보호 목적으로 사용되는 암호모듈 및 암호알고리즘의 국가기관에서의 사용을 허용하기 위해 JCMVP(Japan CMVP)를 운영하고 있다. JCMVP는 북미 CMVP와 동일한 암호모듈 보안요구사항 및 시험기준을 채택하고 있으며, 2006년 6월 시험운용을 통해 올해 4월부터 정식 시행되고 있다.

### 3.5 우리나라의 상용 암호모듈 검증정책[16]

국가정보원은 정보화촉진기본법 및 전자정부법 등 관련 법규에 의거, 정보보호제품 평가·인증제도 운영

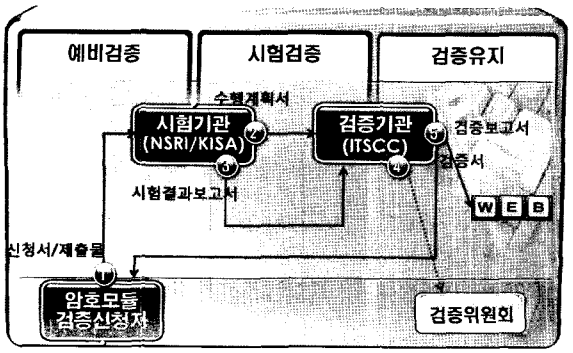


그림 3 국내 상용 암호모듈 검증체계

및 국가기관에 도입되는 상용 정보보호제품의 보안적합성 검증 서비스를 총괄한다. 이중에서 국가기관에서 사용하는 상용 암호모듈의 시험 및 검증 등에 필요한 사항은 "암호모듈 시험 및 검증지침"(행자부고시, 제2004-45호)[1]에 규정하고 있다. 물론, 이러한 제도는 비밀로 분류된 중요자료 및 국가용 보안시스템 보호를 목적으로 사용할 수 없다.

이를 위해 국가정보원은 아래 그림과 같은 수행 체계를 운영하고 있다. 현재 국가보안기술연구소와 한국정보보호진흥원이 시험기관의 역할을 수행하고 있으며, 국가정보원이 검증기관의 역할을 수행한다. 이와 함께, 시험·검증결과의 타당·공정성에 대한 심의를 위해 검증위원회를 독립적으로 구성·운영한다.

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

## 5. 결 론

현대 사회는 네트워크를 통해 디지털화된 정보가 공유되는 유비쿼터스 시대로 표현된다. 이에 따라 암호기술은 유통되는 정보에 신뢰성을 부여하여 사이버세상을 현실 세계와 유기적으로 연결하는 사회 인프라로써의 역할을 수행하게 될 것이다.

이러한 사회 인프라로써의 암호기술의 사용은 세계 각국의 전자정부 구현을 위한 보안대책으로까지 그 중요성이 증가하고 있으며, 신뢰성이 검증된 민간 개발 암호제품의 국가기관 도입을 위한 다양한 제도를 강화하기 시작하였다.

따라서 미국을 비롯한 세계 각국은 상용 암호모듈 및 암호제품에 대한 객관성과 신뢰성을 확보하기 위해 CMVP와 같은 검증제도를 강화하고 있으며, ISO 19790과 같은 국제 표준화를 통해 활성화 방안을 모색하고 있다. 우리나라의 경우도 2005년 1월부터 시행하고 있는 암호검증제도를 활성화하고 안전성이 검증된 상용 암호모듈 및 암호제품의 국가기관 도입을 지원하기 위해 검증제도 강화, 암호키관리 가이드라인 개발 등 다양한 정책을 마련하고 있다.

향후 암호기술의 급속한 발전은 이에 대한 검증 수단의 발전을 동반하게 될 것이다. 이러한 검증 수단은 국가의 입장에서는 안보를 위한 중요 요소로 작용되고 있으며, 경제적 측면에서도 막대한 자산의 손실을 유발할 수 있다는 점에서 사회 구성원 모두가 관심있게 만들어 나가야 될 것이다.

## 참고문헌

[1] IT보안인증사무국, 암호모듈 시험 및 검증지침, 행자부 고시 제2004-45호, 2004.12.
[2] IT보안인증사무국, 암호검증기준 V1.2, 2006.12.
[3] IT보안인증사무국, 암호시험기준 V1.0, 2006.12.
[4] IT보안인증사무국, 암호알고리즘 검증기준, 2005.9.
[5] 국가보안기술연구소, CRYPTOPIA, 제9권, 제1호, 2005.
[6] NIST, "Announcing the development of new hash algorithm(s) for the revision of federal information processing standard(FIPS) 180-2, Secure Hash Standard," Federal Register, Vol. 72, No. 14, January, 2007.
[7] International Organization for Standardization, http://www.iso.org
[8] Cryptographic Module Validation Program, http://csrc.nist.gov/cmvp
[9] National Institute of Standards and Technology, FIPS 140-2 : Security Requirements for Cryptographic Modules, 2001.5.
[10] National Institute of Standards and Technology NIST Handbook 150 : NVLAP Procedures and General Requirements, 2006.2.
[11] National Institute of Standards and Technology, NIST Handbook 150-17 : IT Security Testing-Cryptographic Module Testing, 2000.6.
[12] National Security Agency, http://www.nsa.gov
[13] Communications Security Establishment, http://www.cse-cst.gc.ca
[14] Communications and Electronics Security Group, http://www.cesg.gov.uk
[15] Information Technology Promotion Agency, http://www.ipa.go.jp
[16] Information Technology Security Certification Center, http://www.kecs.go.kr