국내외 암호모듈 검증 정책에 관한 연구

최명길*, 정재훈**,
*중앙대학교 사회과학대학
**중앙대학교 경영대학
**e-mail : selpine@naver.com

A Study of Domestic and Foreign Plicy for Cryptographic Module Verification

Myeong-Gil Choi*, Jae-Hun Jeong**
*College of Social Sciences, Chung-Ang University
**College of Business Adminstration, Chung-Ang University

요 약

정보화 사회에서 정보보호는 다소 불편하지만 정보를 이용하기 위하여 꼭 필요한 핵심기반 기술로 발전되어 왔다. 최근의 대부분의 IT 제품은 적어도 하나이상의 정보보호서비스를 제공하고 있으며, 정보보호서비스를 구현하기 위하여서 암호알고리즘 및 암호서비스가 구현되어야만 한다. 물론 컴퓨터 보안의 액세스 제어를 사용하는 안전한 운영체제 참조 모니터와 같이 정보의 주. 객체사이의 흐름을 관장하는 보호서비스는 별도로 하더라도, 시스템으로의 로그인만 하더라도 암호알고리즘의 사용은 피할 수 없는 필수적인 기능중의 하나이다. 따라서 암호서비스는 정보보호제품에 있어서 가장 중요하고 핵심적인 기본기능이 되었으며, 그 중요성을 감안하여 선진 제외국의 경우에는 국가에서 지정한 신뢰기관에서 알고리즘 구현에 대한 안전성 평가 및 암호 알고리즘을 사용한 암호모듈의 적합성 평가를 실시하고 있다.
본 논문은 정보보호 제품에 대한 안전성을 평가해 제품의 신뢰성을 높이고, 기술의 향상을 유도하는 국외의 정보보호 제품에 대한 평가 프로그램인 암호모듈 검증 정책을 연구한다. 또한 유사한 제도인 CC와의 비교를 통해 다가오는 국제 표준에 대비하여, 국내 정보보호 제품 보호와 기술보호를 위해 선진외국의 제도, 기술, 현황분석 및 국제 암호제도 공조체계 구축을 위한 기반을 제공코자 한다.

1. 서론

정보통신분야의 발전으로 인해 익명성의 사이버 사회가 도달하였고 해킹과 같은 역기능이 많이 발생함에 따라 정보보호를 위해 암호모듈에 대한 수요가 급증하고 있다. 하지만 국내에서는 암호모듈에 대한 평가 기준 정립이 미흡하여 수요자가 모듈 선택시 어려움이 있고, 모듈 및 제품 상호간의 운용 및 호환성 확보에 어려움이 있다.

여기서, 암호모듈은 보안서비스를 제공하기 위한 보안 프로토콜, 보안 매커니즘 및 암호 알고리즘이며 하드웨어, 소프트웨어 또는 펌웨어로 구현된다. 따라서, 정보시스템의 전체 보안성을 평가 및 보증하기 위해서는 시스템을 구성하고 있는 정보보호 제품 및 암호 모듈을 평가해야한다. 정보보호 제품의 '평가 및 인증'(evaluation & certification)은 국내·외적으로 국제공통기준인 CC(Common Criteria, ISO/IEC 15408)에 기반한 평가인증 체계를 통해 실시하며, 암호모듈의 '시험과 검증'(test & verification)은 CMVP(Cryptographic Module Verification Program)를 통해 실시한다. CMVP는 미국과 캐나다에서 운영 중인 암호검증체계이며 NIST FIPS 140-1(과거)과 NIST FIPS 140-2(현재) 기준과 이 기준으로부터 유도한 구체적인 시험기준인 DTR(derived test requirement)을 기반으로 하여 시험 및 검증한다.

FIPS 140-2는 사실상의 국제표준이며, 실제 암호모듈 검증을 위한 국제기준인 ISO/IEC 19790은 FIPS 140-2와 거의 동일하다. 또한, 아직 투표단계인 ISO/IEC 24759는 ISO/IEC 19790을 위한 시험기준인 DTR에 해당한다. 미국의 CMVP는 우리나라와 일본의 암호 모듈검증 체계의 모델이 되었으며, 향후, CCRA처럼 'CMVP 상호인정(CMVP RA) 제도'가 실시될 것으로 예상된다.

본 논문은 국내외의 암호 모듈 평가 프로그램에 대

하여 선진각국의 제도, 기술 동향을 분석하고, 특히 유사 제도인 CC와의 비교분석을 통해 향후 국내 정책과 방향을 정립하여 국내에서 진행 중인 KCMVP의 국제 표준화로의 체계 구축을 위한 환경과 기술 개발의 기반제공에 기여코자 한다.

2. CMVP와 CC와의 관계

CMVP는 정보시스템의 하위수준인 암호모듈을 시험 및 검증하기위한 것이고, CC는 상위수준인 정보보호제품이나 시스템을 평가 및 인증하기 위한 제도이지만, 둘 사이에는 공통점이 많다. [표 1]는 CC V.3.1과 CMVP(FIPS 140)간의 개념상의 대응을 표로 나타낸 것이다.

[표 1] CMVP와 CC간의 개념의 대응

CC V.3.1	CMVP(FIPS 140)
기능 클래스(10종) - 보안감사, 통신 암호지원, 사용자 데이터 보호, 식별 및 인증, 보안관리, 프라이버시, TSF 보호, 자원활용, TOE접근, 안전한 경로/채널	승인된 암호 알고리즘 - 승인된 보호함수, 난수발생기, 키설정 기법
보증 클래스(8종) - PP 평가, ST평가, 개발, 설명서, 생명주기지원, 시험, 취약성 평가, 합성	요구사항 영역(11종) - 암호모듈명세, 암호모듈 인터페이스, 역할- 인증 및 서비스, 소프트웨어/펌웨어 보안, 운영환경, 물리적 보안, 물리적 보안- 비침투공격, SSP 관리, 자가시험, 생명주기 보증, 기타공격에 대한 대응
보증 패밀리 - 보증 클래스당 1개 이상(예: '생명주기지원'클래스 내의 '형상관리능력' 패밀리)	부영역 - 영역당 1개 이상(예: '역할-인증 및 서비스'영역내의 '역할')
보증 컴포넌트 - 보증 패밀리당 1개 이상(예: ALC_CMC 패밀리내의 컴포넌트 ALC_CMC.1)	
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
증거요구사항 (content and presentation elements)	제출문서 (required vendor information)
평가자요구사항 (evaluator action elements)	시험절차(required test procedure)
평가자 공통요구사항 - 모든 보증 컴포넌트마다 공통이며 평가자는 제공된 정보가 모든 증거요구사항을 만족하는지 확인해야 함	시험자 공통 사항 - 제출문서를 검증하는 업무
보안목표명세서(ST)	암호모듈 보안정책
	- FIPS 140-1에서는 TOSEC으로 평가된 OS 권장 - FIPS 140-2이상에서는 CC로 평가된 OS 권장

CC와 CMVP 모두 평가대상물(제품 또는 암호모듈)의 보안기능과 보증수준을 별도의 차원으로 보고 있다. 예컨대, CC의 경우, 보안기능은 많지만 보증수준이 낮은(예: EAL1) 제품도 있고, 보안기능은 1가지이지만 보증수준이 높은(예: EAL7) 제품도 있다. 또한 CMVP의 경우 많은 수의 '승인된(approved)' 보안함수를 최저등급(1등급)으로 평가할 수도 있고(Open SSL처럼 대부분의 소프트웨어로 구현된 암호 라이브러리 해당), 한가지 암호 알고리즘(예: AES)만을 최고 보안등급(4등급)으로 검증할 수도 있다.

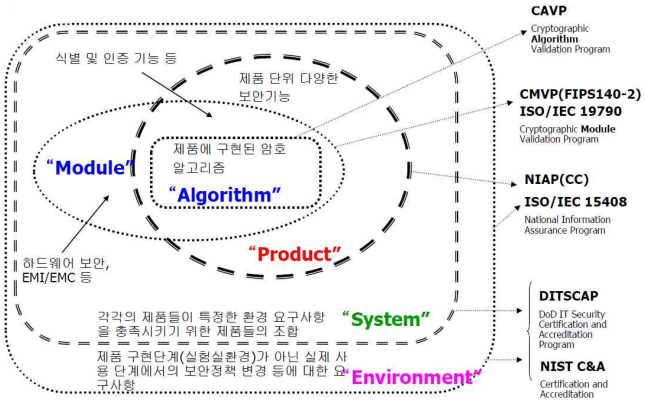
CMVP는 CC에 비해 계층성이 부족하다. 즉, CC의 요구사항은 클래스-패밀리-컴포넌트-엘리먼트로 계층구조화 되어있지만, CMVP에서는 영역과 부영역 및 시험항목(assertion)에 대응한다. CC의 보증 엘리먼트별 개발자 요구사항, 증거요구사항, 평가자 요구사항 및 평가자 공통요구사항은, CMVP에서 시험항목, 제출문서, 시험절차 및 시험자 공통사항에 각각 대응한다. 특히 CC에서 특정 제품에 대한 보안요구사항 명세서에 해당하는 '보안목표'는 CMVP에서는 '암호모듈 보안정책'에 해당한다.

3. 국내외의 암호모듈 검증 정책 연구

3.1. 미국

미국 NSA(National Security Agency)는 상용암호모듈 및 암호알고리즘 구현 적합성을 평가하고, 정부조달 기준으로 사용하기 위해 NIST와 캐나다 주정부의 CSE가 공동 개발한 CMVP를 활용한다. 그러나 CMVP를 통해 검증된 암호 모듈과 알고리즘은 비밀로 분류되지 않은 데이터 보호를 위해 국가기관에서 사용될 수는 있으나, 비밀로 분류된 데이터보호 및 국가보안시스템에서는 사용할 수 없다.

다음 [그림 1]는 미국의 각 평가체계의 범위를 나타낸 것이다.



[그림 1] 미국의 각 평가체계의 범위

3.2. 캐나다

캐나다 정부의 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 국가기관이 사용을 승인한다. 국가기관은 CMVP를 통해 검증된 제품에 탑재된 암호 모듈·알고리즘이나 CSE가 승인한 암호모듈 및 알고리즘을 사용해야 한다. IPPP(ITS Pre-qualification Product Program)를 통해서 정보조달을 위해서 암호제품에 등재된다.

3.3. 영국

영국의 정보보증업무를 총괄하는 CESG (Communication and Electronics Security Group)는 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.

3.4. 일본

일본 내각관방 산하 NISC(National Information Security Center)는 국가보안정책을 총괄하는 기구로 각급기관에 적용되는 표준 개발, 각급기관의 정보보호 대책 평가 및 안전한 보안환경 설계·구축 지원 서비스 등을 제공한다. 국가기관의 안전한 암호제품 도입 및 개발 지원은 2007년까지 IPA(Information Technology Promotion Agency)에서 운영하는 CRYPTREC(Cryptography Research and Evaluation Committees)을 통해 운영되었고, 2007년 4월부터 JCMVP가 그 역할을 대신한다.

JCMVP는 북미 CMVP와 동일한 암호모듈 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.

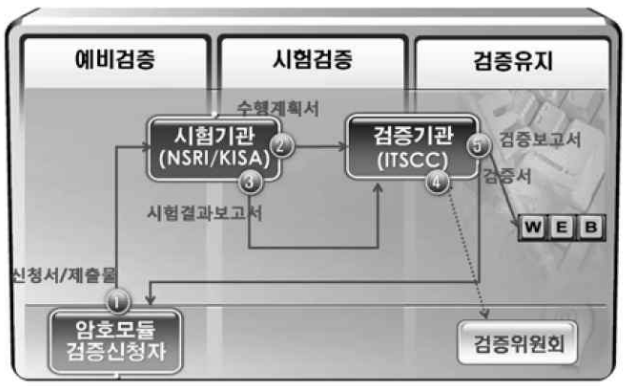
3.5. 우리나라

국가정보원은 정보화촉진기본법 및 전자정부법 등 관련 법규에 의거, 정보보호제품 평가·인증제도 운영 및 국가기관에 도입되는 상용 정보보호제품의 보안적합성 검증 서비스를 총괄한다.

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.

우리나라는 국제 협정에 가깝게 가기 위해 표준 암호화알고리즘(ARIA)을 최대한 국제 표준에 맞췄으며, 알고리즘 소스코드를 공개하기도 했다.

다음의 [그림 2]는 국내 상용 암호모듈 검증체계를 나타낸 것이다.



[그림 2] 국내 상용 암호모듈 검증체계

4. 암호모듈 검증정책의 향후 전망

CMVP 프로그램의 필요성은 2004년도 NIST 년차별 보고서에 의하면, 2004년 초기에 200개의 평가된 제품 중 약 48%의 모듈과 27%의 암호알고리즘이 평가 시험 중 교정되었으며, 이를 달리 해석해 보면, CMVP 시험이 없을 경우, 2005년도에 사용되는 정부기관의 암호서비스 중 50%가 불완전한 보안서비스를 제공하는 제품을 사용할 수도 있다는 결론에 도달된다.

[표 2] 연도별 CMVP 인증 현황

	2003년	2004년	2005년	2006년	2007년	2008년	2009년
CMVP 인증서	#283 ~ #372	#373 ~ #494	#495 ~ #613	#614 ~ #729	#730 ~ #884	#885 ~ #1079	#1080 ~ #1218

이러한 상황 속에서 현재, 각종 암호기술이 개발되어 이를 장착한 많은 제품들이 시장에 제공되고 있으나 모든 암호기술의 안전성이 평가/검증되고 있는 것은 아니다. 그 때문에 암호기술을 전자정부 등에서 이용하기 위해서는 암호기술을 객관적으로 평가하는 것이 무엇보다 중요하다.

2001년도부터 진행된 CMVP 제도는 2006년도 표준화의 평균 주기인 5년을 맞이하였고, 2006년도를 기준으로 국내에서도 KCMVP 가 본격적으로 추진되어 현재 3개의 평가인증제도가 시행되고 있다. 이제 다가오는 암호모듈 검증제도가 북미 및 일본 등 선진국에서 추진되어왔던 검증된 암호 알고리즘 및 암호 모듈을 분석하여 다가오는 세계 표준 검증제도에 대비하여 국내 기반기술 축적이 필요하다. 상기 CAVP 알고리즘 검증 및 CMVP 검증 암호모듈은 미국과 캐나다의 160개 업체가 1994년도부터 개발한 제품으로 이를 벤치마킹하여, 향후 전개되는 국제공조체계의 확립을 위하여 우선되어야 할 연구가 되겠다.

5. 결 론

본 논문에서는 현재 국내외에서 활발히 진행 중에 있는 암호 모듈 평가 프로그램을 분석하고, 유사 제도인 CC와의 비교 분석 및 암호모듈 검증정책의 향후 전망에 대해 연구하였다.

선진각국의 경우에 미국은 자국의 FIPS 표준을 ISO 표준화에 총력을 기울여 FIPS 140-2가 19170으로, DTR을 ISO 24759 로 국제표준화 시키고 있다. 캐나다의 경우에는 미국과 초창기부터 공동으로 CMVP를 진행하여 왔으며, 영국의 경우에는 CESG를 통하여 표준화에 동참하면서도 별도의 CAPS제도를 운영하고 있다. 일본은 미국의 CMVP를 JCMVP로 따라서 움직이며, 2개의 평가기관을 발빠르게 발족하여 표준화에 동참하고 있다.

이제 CMVP는 미국만의 것이 아니라, ISO 표준화로 책정되어 CC 평가와 함께 곧 세계적인 정보보호 제품 평가체계를 구축하게 되었다.

이를 위하여, 미국 및 일본 등의 경우와 같이 조달청 구매 물품 내에 암호모듈인증 제품이 현실적으로 사용될 수 있도록 정부 통합 조직을 구성, 운영되어야 할 것이며, 이를 뒷받침할 수법과 제도가 수립되어야 하며, 사용자, 개발자, 평가자에 대한 기준 및 기술 가이드라인이 정립되어야 한다.

참고문헌

[1] KISA, 공통평가기준 1부, 2부, 3부, 1999.8
[2] 한국 정보보호 진흥원, 암호제품 평가 체계 분석, 2002
[3] 박성근 외 5명, CMVP 테스트를 적용한 SEED 암호 알고리즘 모듈 구현, 2003.05
[4] NIST, Cryptographic Module Validation Program Conference, 2002.03
[5] NIST, Security Requirements for Cryptographic Modules(FIPS 140-2), 2001
[6] NIST, Security Requirements for Cryptographic Modules(FIPS 140-3 Revised DRAFT), 2009
[7] NIST, Cryptographic Module Validation Program(CMVP), http://csrc.nist.gov/cryptval
[8] 한국 정보보호 진흥원, http://www.kisa.or.kr
[9] Lee, Annabelle, Guideline for Implementing Cryptography in the Federal Government, Special Publication 800-21, Gaithersburg, MD, National Institute of Standards and Technology, November, 1999.
[10] 일본 JCMVP : http://www.ipa.go.jp/security/jcmvp
[11] 영국 CESG : http://www.cesg.gov.uk
[12] NIST, Data Encryption Standard(DES), FIPS 46-3, 1999
[13] NIST, DES Modes of Operation, FIPS 81, 1980
[14] NIST, Secure Hash Standard, FIPS 180-1, 1995
[15] NIST, MOVS, SP 800-17, 1998
[16] NIST, TMOVS, SP 800-20, 2000
[17] NIST, DSSVS User's Guide, 2001.01