Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.4, Aug. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.4.897

국내외 IT제품 도입제도 동향 분석 및 국내 제도 개선방안 도출

손 효 현,† 김 광 준, 이 만 희‡
한남대학교

Analysis of the Trends of Domestic/International IT Product Introduction Policy and Deduce Improvement Plan of Domestic Policy

Hyo-hyun Son,† Kwang-jun Kim, Man-hee Lee‡
Hannam University

요 약

정보통신기술이 발전함에 따라 정부의 행정전산화가 추진되었고, 이의 역기능으로 IT제품을 대상으로 한 사이버 공격이 전 세계적으로 확산되고 있다. 이에 따라 각국의 정부는 정보보호를 위하여 국가·공공기관의 IT제품 도입에 있어 보안성검증을 의무화하기 시작하였으며 도입 과정에서 요구되는 제도를 정립하였다. 본 연구는 현 국내 IT제품 도입제도를 분석하여 보완점을 파악한다. 또한 주요 선진국 미국, 영국, 일본, 캐나다, 호주 5개국의 IT제품 도입제도 동향을 분석하며, 최종적으로 국내 도입제도와의 비교 분석을 통하여 국내 도입제도의 개선방안을 제안한다.

ABSTRACT

As the Information and Communication Technology developed, the administration computerization of the government was promoted, and cyber attacks targeting IT products are spreading all over the world due to the reverse functions. Accordingly, governments in each country have begun to verify the security in the introduction of IT products by national and public institutions in order to protect information, and established the policy required in the introduction process. This research analyzes the introduction policy of domestic IT products to identify the supplement point. In addition, we analyze trends of introduction of IT products in the major developed countries such as USA, UK, Japan, Canada, and Australia. Finally, we propose the improvement method of domestic introduction policy through comparison analysis with domestic introduction policy.

Keywords: Introduction Policy, Security Conformance, Common Criteria, Cryptographic Module Validation Program, Common Criteria Recognition Arrangement

I. 서 론

정보통신기술의 발전과 IT 산업의 기하학적인 성장에 따라 전 세계적으로 국가의 행정업무가 전산화되는 정보화 사회가 형성되었다[1]. 그러나 정부의 행정전산화 추진과 맞물려 인터넷을 통한 기밀자료 유출, 해킹 등과 같은 사이버 공격이 전 세계적으로 확산되고 있다[2]. 그에 따라 국가 각 공공기관은 주도적으로 다양한 정보보호제품을 도입, 운영하여 정보를 보호하고 네트워크의 보안성을 제고하고 있다. 따라서 보안요구사항에 적합한 제품을 기관에 도입하기 위하여, 제품에 대한 공인된 안전성 평가 및 인증이 요구되고 있다.

Received(04. 22. 2019), Accepted(06. 09. 2019)
† 주저자, sonhyohyun.kr@gmail.com
‡ 교신저자, manheelee@hnu.kr(Corresponding author)

각국의 정부는 공통평가기준(CC, Common Criteria)을 통하여 기관에 도입하고자 하는 제품의 안전성을 평가하고, 각국의 환경에 맞는 평가 및 인증을 통해 국가·공공기관에서 사용할 IT제품의 신뢰성을 확보함으로써 국가의 정보보호 수준을 제고하고 있다. 따라서 발전하는 정보통신기술과 함께 그 제품을 평가·인증하는 제도 역시 지속적으로 미비한 부분을 파악하고 개선해야 할 방안을 도출할 필요성이 있다. 하지만 지난 10년간의 관련 연구를 파악한 결과 단순히 국내의 CC 평가·인증 제도에 대하여 소개하거나 CCRA(Common Criteria Recognition Arrangement) 발행국을 중심으로 평가·인증 체계를 분석한 연구, 그리고 암호 모듈 검증 제도에 대한 소개 및 CMVP 사용 국가와 제도 비교 수준의 연구에 그치고 있다[3,4,5,6,7,8]. 이에 따라 본 논문에서는 국내 및 주요 선진국들에서 시행하고 있는 CC 평가·인증 및 암호 모듈 검증 제도 등 정부 기관에 정보보호제품을 도입하기 위한 도입절차 및 제도에 대해 종합적으로 소개한 후 국가간 상호 비교 분석을 통하여 국내 도입제도의 개선방안을 도출한다.

본 논문은 다음과 같이 구성된다. 먼저 2장에서는 국내 IT제품 도입제도에 대해 소개하며, 3장에서는 국외 CCRA 발행국 중 주요 선진국을 중심으로 미국, 영국, 일본, 캐나다, 호주 총 5개 국가에 대한 IT제품 도입제도 및 동향을 기술한다. 4장에서는 앞서 소개한 국내외 도입제도를 상호 비교 분석하고, 마지막으로 5장에서는 국내 제도의 개선방안을 제안하며 결론을 맺는다.

II. 국내 IT제품 도입제도

정부는 공정하고 객관적인 평가 시스템을 통하여 정보보호제품의 보안성을 검증함으로써 안전성 있는 제품을 국가·공공기관에 도입 가능토록 요구한다. 한국은 국가정보화 기본법 및 전자정부법 등의 기준에 따라 정보보호 관련 제품 및 시스템을 검증하는 제도를 체계화하고 있다. 현재 국내 정보보호제품 도

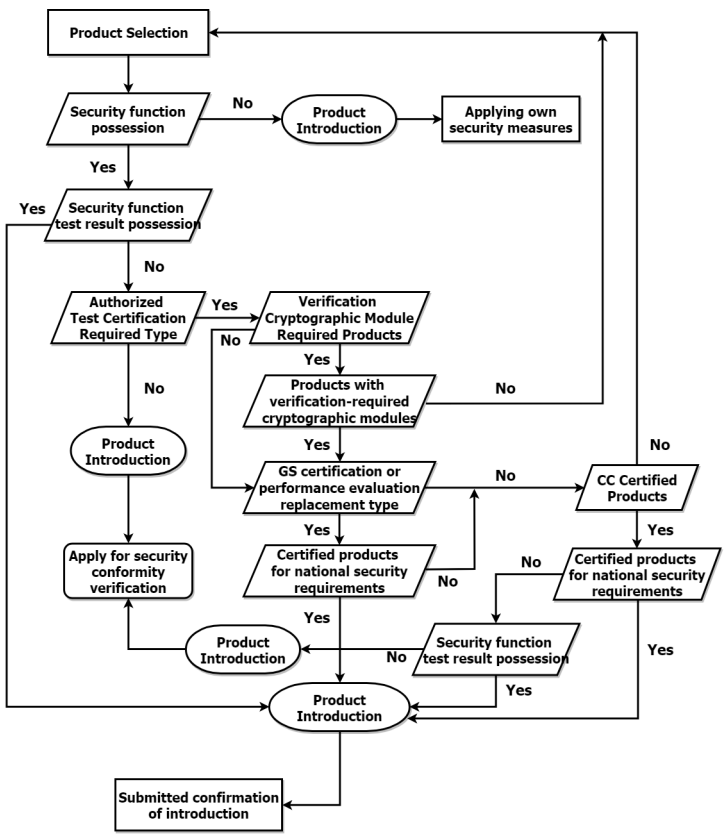


Fig. 1. Introduction Policy of Domestic

입제도는 정보보호제품 평가·인증제도(CC 평가·인증), 암호모듈 검증 제도, 보안적합성 검증 제도를 시행 중에 있다. 국내 도입제도에 대한 전체적인 절차는 Fig.1과 같다[9].

국내 제도의 경우 도입하려는 제품의 보안기능 보유 여부에 따라 구분된다. 보안기능을 포함하지 않을 경우, 기관은 제품을 도입한 후 자체보안대책을 적용하여 운용 가능하다. 그러나 보안기능을 보유할 경우 보안기능 시험결과서 보유 여부에 따라 구분된다.

먼저 해당 정보보호제품에 대한 보안기능 시험결과서를 발급받았다면 추가 검증 없이 제품 도입이 가능하다. 보안기능 시험결과서 발급제도는 국가용 및 네트워크 보안기능 요구사항에 따라 제품을 검증하며, 보안적합성 검증 제도의 일부이다. 또한, 본 제도는 국가정보원에서 주관하여 발급에 대한 정책업무를 진행하고 있으며, 보안적합성 검증기관으로 국가보안기술연구소에서 실무 업무를 담당한다[10]. 사전검증을 통한 보다 빠른 도입을 위해 2017년부터 운영하였으며, 시험결과서를 발급 받은 제품은 보안적합성 검증 생략이 가능하다. 그러나 시험결과서가 발급된 제품 목록에 대해서는 현재 공개하고 있지 않다.

또한, 정보보호제품이 보안기능은 보유하고 있으나 시험결과서를 보유하고 있지 않을 경우, 도입 인증 요건 필수 제품 유형에 해당하는지에 따라 구분한다. 이에 해당되지 않을 경우 보안적합성 검증 이전에 제품을 먼저 도입한 후 검증을 요청한다. 반대로 인증 필수 유형일 경우엔 다시 암호 모듈 필수 제품 여부를 판단하여 해당되는 검증 프로그램을 통하여 절차를 거친 후 국가용 보안요구사항 준용 인증 제품에 한하여 최종적으로 국가 공공기관에 제품 도입이 가능하다.

III. 국외 IT제품 도입제도

3.1 미국

미국은 NSA(National Security Agency)가 인정한 NSS(National Security System)를 미국 연방정부 및 연방기관, 국가 주요기반시설 운영기관에 도입하도록 의무화하고 있다. 이때 NSA는 CNSS(Committee on National Security Systems) 정책에 기반하여 NSS로 인정 가능한 IT제품을 정보 보증 및 정보 보증을 받은 COTS(Commercial-Off-The-Shelf)와

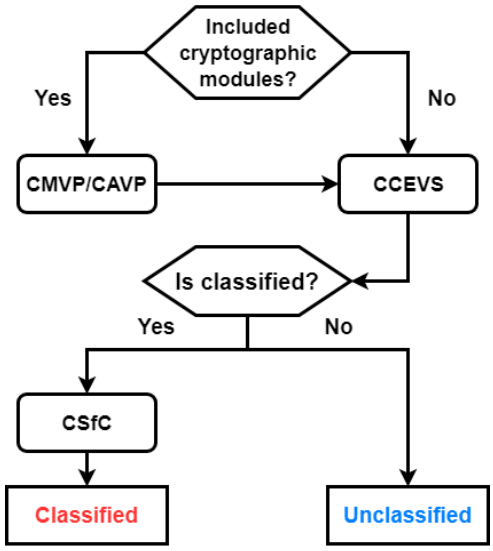


Fig. 2. Introduction Policy of USA

GOTS(Government-Off-The-Shelf)로 한정한다. 미국의 NSS 도입제도는 CMVP(Cryptographic Module Validation Program)와 CAVP(Cryptographic Algorithm Validation Program), CCEVS(Common Criteria Evaluation and Validation Scheme), CSfC(Commercial Solutions for Classified Program)가 있으며 전체적 절차는 Fig.2와 같다.

미국은 평가·인증에 앞서 IT제품의 암호 모듈 탑재 여부에 대하여 확인을 한다. 이때 암호 모듈을 탑재한 IT제품일 경우, CMVP 및 CAVP 검증을 받아야 한다. CMVP는 NIST(National Institute of Standards and Technology)에서 주관하며, 해당 기관에서 개발한 FIPS 140-2와 FIPS 140-3을 보안규격으로 적용하여 암호 모듈에 대한 암호학적 안전성을 검증하는 프로그램이다. 또한, 암호 모듈에 사용되는 암호 알고리즘은 CAVP를 통해 적합하지 않은 알고리즘 및 비승인 FIPS 알고리즘 사용 여부에 대하여 확인한다.

암호 모듈이 탑재되지 않은 IT제품 및 1차적으로 CMVP와 CAVP를 통해 인증된 IT제품은 CCEVS 평가·인증이 필요하다. CCEVS는 미국의 국내용 CC인증 스킴으로써 IT제품의 기밀성, 무결성 등 보안기능의 안전성 및 신뢰성을 검증하는 프로그램이다[11]. 주관기관은 NIAP(National Information

Assurance Partnership)로 CCEVS의 보안규격인 PP(Protection Profile)를 개발 및 승인하였으며, 인증기관은 PP를 기반으로 만든 CC를 활용하여 IT제품을 평가·인증한다.

평가·인증이 완료된 제품 중 기밀자료를 다루지 않을 경우 바로 NSS로 도입이 가능하다. 그러나 기밀자료를 다루는 IT제품은 NSA에서 주관하는 CSfC 프로그램의 보안성 검증을 받은 후 기관에 도입 및 운영해야 한다. CSfC 프로그램은 NSA 주체로 개발 및 승인된 CP(Capability Package)를 보안규격으로 사용하며, CP는 검증 대상 제품군의 환경설정 요구사항 및 추가 보안 요구사항을 명시한다. CSfC 프로그램을 통하여 검증 완료된 IT제품은 NSA와 개발업체가 합의각서(MOA)를 체결한 후 CSfC 구성 요소 목록에 등재 가능하다[12]. 이 목록은 공급업체가 정부에 IT제품을 제공하고자 할 때, 시스템 군별로 분류된 제품 중 적합한 기능을 가진 제품을 선택하여 도입 및 운용 가능토록 함에 목적을 가진다.

3.2 영국

영국 정부의 정보보증을 담당하는 주요 기관은 GCHQ(Government Communications Headquarters)이다. 해당 기관에서 파생된 NCSC(National Cyber Security Centre)는 2016년 영국의 정보보안기구인 CESG(Communication-Electronics Security Group)와 CERT-UK(Computer Emergency Response Team-United Kingdom) 등 영국 사이버보안 관련 기구를 통합하여 창설되었으며, 영국의 사이버 안보를 총괄한다. 영국은 정보시스템에 대한 보증 및 보안 위협에 대응하기 위하여 Cyber Security Consultancy, CPA(Commercial Product Assurance), CAPS(CESG Assisted Products Service) 제도를 운영하고 있다.

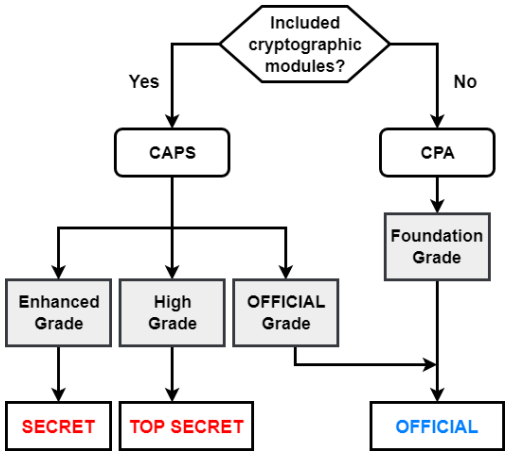


Fig. 3. Introduction Policy of United Kingdom

해당 제도를 통하여 인증된 제품은 Table.1과 같이 취급 정보에 따라 4가지 보안등급으로 분류된다. 보안등급에 따라 취급할 수 있는 보안 수준이 나뉘어 있으며, 각 등급과 수준의 내용은 Table.1과 같다[13]. 영국 제도에 따른 도입 절차는 Fig.3과 같다.

영국의 상용 제품 보증은 암호 모듈 여부에 따라 평가 제도가 구분된다. 암호 모듈을 포함하지 않은 제품의 경우 NCSC에서 주관하는 CPA 평가를 통하여 제품 평가·인증을 진행한다. 이때

Table 1. Security Level and Grade of United Kingdom

Levels of classification	Contents	Grade
OFFICIAL	Most of the information created or processed by the public sector	Foundation Grade, OFFICIAL Grade
SECRET	Very sensitive information that justifies strengthen protection measures to defend decisive and influential threats actors.	Enhanced Grade
TOP SECRET	Represents the most sensitive information in HMG(Her Majesty's Government), which requires the highest level of protection against the serious threats.	High Grade (TOP SECRET Grade)

SC(Security Characteristics)를 평가기준으로 하여 CPA Foundation Grade 평가 프로세스를 수행하며, 인증된 제품에 한하여 Foundation Grade의 보안 등급을 부여받을 수 있다. 해당 등급은 OFFICIAL 정보 취급만이 허용된다.

이에 반해 기밀자료를 취급하는 기관에서 암호 모듈이 포함된 상용 제품을 도입하고자 할 경우, CESG가 주관하는 CAPS의 승인이 필요하다. CAPS는 평가 대상 제품이 승인된 암호화 표준에 맞게 제작되었는지 평가하여, 사용기관에 대해 공식적으로 제품 사용을 허가한다. CESG는 CAPS 평가를 위해 평가 신청받은 제품에 대한 기밀정보를 요구하지만, 이에 대한 평가기준 및 상세한 자료는 외부에 공개하지 않는다. 평가 완료된 제품은 암호화 등급 및 범주에 따라 OFFICIAL Grade, Enhanced Grade, High Grade 3단계 중 하나의 보안등급을 부여받게 되며, 기밀자료 취급 기관은 Enhanced Grade 이상을 받은 제품만 도입 및 운용 가능하다.

3.3 일본

일본의 METI(Minister of Economy, Trade and Industry)는 정보보호 관련 업무를 수행하는 주요 기관으로 정보보호 정책 수립 업무를 담당한다. 일본 IT제품의 국가·공공기관 도입 제도 관련 업무는 METI의 산하기관인 IPA(Information Technology Promotion Agency)에서 운영한다[14]. 시행 중인 제도는 JISEC(Japan Information Technology Security Evaluation and Certification Scheme)와 JCMVP (Japan Cryptographic Module Validation Program)이며 절차는 Fig.4와 같다.

일본의 경우 미국과 동일하게 검증할 제품에 대하여 암호 모듈 여부를 판단한다. 이에 따라 암호 모듈이 존재할 경우 JCMVP를 통하여 암호화 모듈의 구현 및 기능을 검증하며, 이때 JCMVP 암호 모듈 보안 요구사항에 따라 평가를 진행한다. 인증된 제품에 한하여 암호화 알고리즘 확인서를 발급한다[15]. 또한, 암호 모듈 검증이 완료된 제품과 암호 모듈이 탑재되지 않은 제품 모두 JISEC 평가·인증을 받음으로써 IT제품 보안 기능의 적합성 및 신뢰성을 보장한다. JISEC는 IPA에서 주관하며, 일본 국가·공공기관에 IT제품 도입 시 정부의 보안요구사항을 충족하기 위해 CC를 기준으로 평가·인증을 진행한다[16]. 검증이 완료된 제품에 한하여 일본 정부기관에 도입 가능하다.

3.4 캐나다

정부 산하기구인 CSE(Communications Security Establishmnet)는 캐나다의 주요 보안 기관으로 외국의 정보를 수집하며, 컴퓨터 네트워크 및 캐나다의 주요 기밀정보를 보호하는 업무를 수행한다. CSE는 IT제품을 평가하고 정부의 정보보호를 위해 CMVP(Cryptographic Module Validation Program)와 CAVP(Cryptographic Algorithm Validation Program), CCCP(Canadian Common Criteria Program), COMSEC(Communications

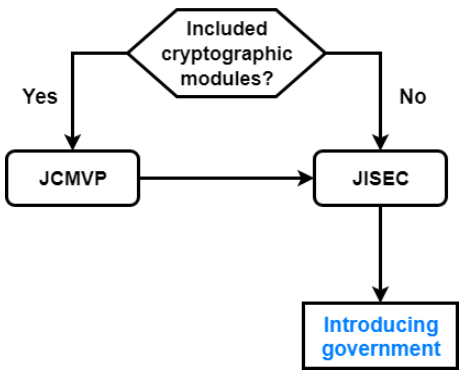


Fig. 4. Introduction Policy of Japan

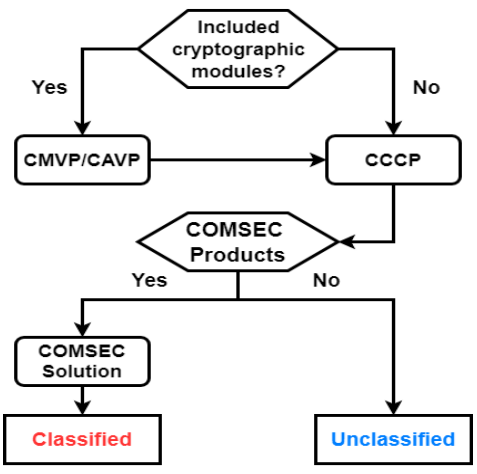


Fig. 5. Introduction Policy of Canada

Security) 제도를 운영하고 있으며, 절차는 Fig.5와 같다.

캐나다는 IT제품을 정부기관에 도입하기에 앞서 암호 모듈 탑재 여부에 따라 CMVP[17]와 CAVP[18]를 진행한다. 두 제도는 CSE와 미국 NIST가 공동 설립한 암호 검증 프로그램으로, 암호 모듈의 안전성을 평가·검증한다. 검증이 완료된 IT 제품 및 암호 모듈이 탑재되지 않은 IT제품 모두 CCCP의 평가·인증이 요구된다[19]. CSE는 CSE PP[20]를 기준으로 평가를 진행하며, CCRA에 속한 국가들 간의 CC 평가에 대하여 상호 인정한다[21]. 캐나다 국가·공공기관은 CC 평가·인증된 IT제품만이 도입 및 운용 가능하다.

마지막으로 기밀자료를 다루는 IT제품이 아닐 경우 바로 도입 가능하며, 반대로 기밀자료를 다루는 IT제품은 캐나다의 독립적 제도인 COMSEC에 따라 높은 보증 평가를 받은 후 정부기관에 도입 가능하다. CSE가 주관하는 COMSEC 제도는 COMSEC Products 목록을 통하여 IT제품의 선택 및 도입이 가능하며, 해당 목록에 등재된 IT제품은 COMSEC Solution을 거쳐 인증된 제품이다[22]. 하지만 해당 제도의 평가기준은 현재 외부에 공개되어 있지 않다.

3.5 호주

호주 주요 기관은 ASD(The Australian Signals Directorate)로 현대의 신호 정보 및 보안 기관에 요구되는 모든 업무 담당하며, 호주의 사이버 안보를 총괄한다. ASD는 호주 정부의 정보보호를 목적으로 ICT 제품 보안 평가를 위하여 ASD Cryptographic Evaluations, AISEP Evaluations and Certifications, High Assurance Evaluations 제도를 운영하며, 도입 제도의 절차는 Fig.6과 같다.

호주는 ICT 제품의 암호 모듈 사용 여부에 따라 구분하여 검증을 진행하며, 암호 모듈이 탑재된 ICT 제품은 암호의 취약점을 확인하고 검증하는 Cyptographic 제도를 수행한다. 본 제도는 ASD 주관으로 암호 기능이 포함된 ICT 보안 제품에 사용된 아키텍처 및 암호화 알고리즘의 정상 구현 여부를 검증함으로써 정부기관의 정보보호를 위한 안전성과 암호의 취약점을 확인할 수 있다. 호주는 암호 검증에 있어 Cryptographic 제도가 아닌 다른 국가

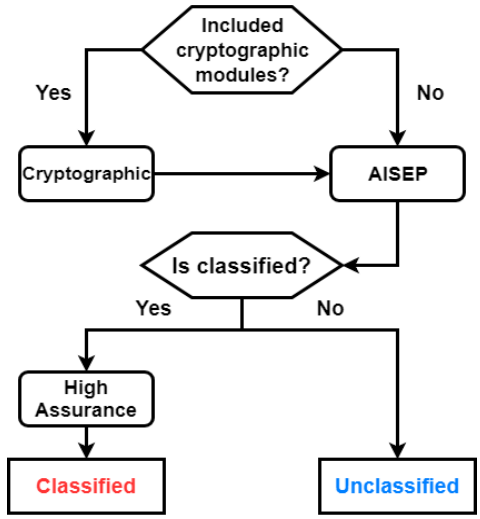


Fig. 6. Introduction Policy of Australia

의 암호화 평가를 인정하지 않으며 다른 암호화 평가 제도로 대체할 수 없다.

암호화 검증이 완료된 제품 및 암호 모듈을 사용하지 않은 ICT 제품 모두 AISEP 평가·인증 제도를 통하여 호주 정부의 보안요구사항을 충족시키는지 검증받아야 한다. 본 제도는 ICT 제품에 대한 보안 평가를 수행함으로써 시스템에 대한 안전성 및 신뢰성을 높인다. AISEP 평가·인증은 ASD가 인정한 PP 또는 CCRA가 인정한 PP를 평가기준으로 수행한다[21].

최종 단계로 ICT 제품의 기밀정보 취급 여부에 따라 높은 기밀정보를 보호하는 경우, ASD에서 주관하는 High Assurance Evaluations의 인증을 받아야 한다. 본 제도의 평가기준 및 방침은 ASD에서 결정하지만 그 기준에 대해선 외부에 공개하지 않는다. 그러나 ASD는 High Assurance Evaluations 평가 중이거나 평가 완료된 ICT 제품의 정보를 EPL(Evaluated Products List)에 공개하고 있다[23]. 이에 따라 호주 정부는 국가·공공기관에 기밀정보 취급 제품을 도입하고자 할 경우 EPL에 등재된 제품을 선택하여 운용하여야 한다[24].

IV. 국내외 도입제도 비교 분석

앞서 소개한 국외 도입제도를 분석하여 보았을 때, 공통적으로 진행되는 흐름은 다음과 같다. 먼저

도입하고자 하는 제품의 암호 모듈 사용 여부에 대하여 확인한다. 이에 따라 각국은 암호 모듈 검증 제도를 자체적으로 실시하여 1차적으로 암호화 구현 여부에 대한 유효성을 검증하고 보안성을 확인한다. 이후 인증된 IT제품 및 암호 모듈이 탑재 되지 않은 IT제품 모두에 대하여 2차적으로 평가·인증을 수행한다. 암호 모듈에 대한 검증이 완료된 제품일지라도 해당 IT제품이 각 국가 정부가 요구하는 보안요구사항의 충족 여부를 판단하고 평가한다. 마지막으로는 기밀정보 취급 여부에 따라 국가별 고유 제도를 통하여 최종 검증 및 국가·공공기관에 도입 운용을 가능하게 한다. 즉, 국외 도입제도의 공통적 특징은 IT제품을 도입하기 이전에 평가 및 검증을 진행하며 이를 통해 인증된 제품만 도입 가능하다는 것이다.

이에 반해, 국내의 보안적합성 검증은 우선 제품을 도입한 이후 검증 신청서 및 기술제안 요청서 등 제출물을 기반으로 검증을 신청한다. 보안적합성 검증이 종료된 후 운영 권고 사항을 신청기관에 전달하여 해당 사항의 실천을 권고하고 있다.

즉, 국내의 IT제품 도입제도는 제품 운영기관의 실천 여부에 따라 보안의 수준이 결정되므로 운영기관의 인식 및 전문성 부족으로 인한 보안 사고를 미연에 막기에 어려운 점이 있다. 따라서 국외의 IT도입 제도처럼 우리나라 또한 모든 정보보호제품에 대하여 보안적합성 검증 후 보안요구사항(국가용 PP)을 만족하지 못한 부분을 개선 또는 제거하여, 안전성이 검증된 제품에 한해 기관에 도입하도록 한다면 보다 높은 보안성을 제공할 수 있을 것으로 판단된다.

한편, 대부분의 국외제도들은 검증된 제품 목록을 인터넷에 공개하고 정부기관의 IT제품 선택 시 검증된 제품을 도입하게 함으로써 도입 및 운영의 편리성을 제공하고 있다. 우리나라에서도 보안기능 시험결과서 발급 현황을 공개하고 보안기능 시험결과서가 있는 제품을 도입하도록 제도를 수정한다면 보안 적합성 검증 기간을 크게 단축시키고 전체 절차가 매우 간소해질 것으로 사료된다.

따라서 본 연구에서 제안하고자 하는 국내 제도 개선 방향은 Fig.7과 같다. 국가·공공기관에 도입하고자 하는 정보보호제품에 암호 모듈이 포함되어 있을 경우, KCMVP를 통해 암호화 검증을 받는다. 검증을 받은 제품과 암호 모듈이 포함되지 않은 제품은 모두 정보보호제품 평가·인증을 받아야 하며, 이때 사용되는 기준은 국내용 CC를 기준으로 한다.

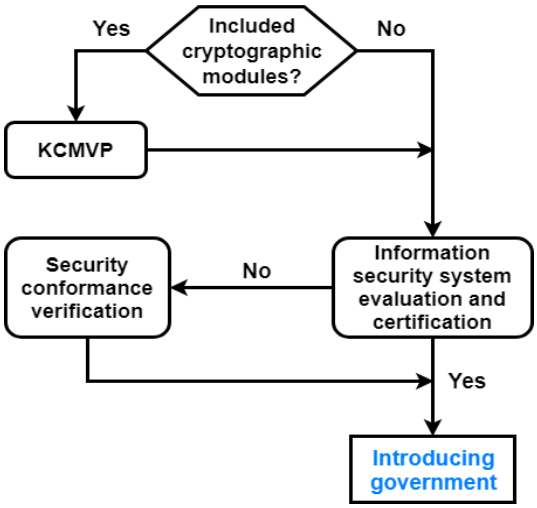


Fig. 7. Suggestion of Domestic Introduction Policy

국제용 CC는 국내용 보안요구사항을 만족하지 않을 수 있다. 이 경우 국내의 정부 및 공공기관에 도입하기 위해 국내용 CC를 통한 인증이 필요하다. 평가·인증을 모두 완료한 제품은 정부기관에 도입이 가능하지만, 정보보호제품 평가·인증을 받지 않은 제품은 보안적합성 검증을 실시 후 도입 및 운용 가능하다. 이때 시험결과서 발급 현황을 미리 공개하여 사전 검증된 제품을 선택하도록 유도하면 보다 빠른 검증이 이루어질 것으로 기대된다.

V. 결 론

전 세계적으로 발전하고 있는 정보통신기술과 함께 IT제품의 도입제도 역시 지속적인 개선을 통하여 각 국가의 환경에 맞추어 추가적인 제도 개발 및 문제점을 보완하고 있다. 본 논문은 한국과 주요 선진국 5개 국가 미국, 영국, 일본, 캐나다, 호주의 IT제품 도입제도의 동향을 파악하고, 운영 중인 보안성 검증 프로그램을 분석하여 국내외 도입제도의 전체적 흐름 및 특성에 대하여 비교하였다.

그 결과 해외의 도입제도 모두 IT제품을 도입하기 이전에 인증 제도를 수행함을 확인하였다. 현재 국내의 보안적합성 검증 제도의 경우 제품을 도입한 이후 보안적합성 검증을 신청하여 진행하고 있다. 이에 따라 검증 결과에 따른 운영 권고 사항을 신청 기관에 전달하더라도 강제할 방안이 마련되어 있지 않음을 확인할 수 있었다. 이로 인해 IT제품은 보안성이 취

약한 상태로 도입되어 운영될 가능성이 존재하며 이는 차후 보안사고로도 이어질 수 있다.

이를 보완하기 위해 본 연구에서는 해외 도입제도와 같이 제품을 도입하기 이전에 보안적합성 검증 제도를 신청하도록 변경하고, 또한 보안기능 시험결과서 제도 확대를 통해 사전에 인증을 획득한 제품 사용을 권장하는 것이 바람직한 것으로 판단된다. 이로써, 보다 빠르고 체계적으로 정보보호제품을 검증할 수 있을 것으로 예상되며, 최종적으로 국가·공공기관의 정보보안 수준이 크게 향상 가능할 것으로 기대된다.

향후 연구를 통하여 국외 CCRA 주요국을 중심으로 도입제도의 지속적인 동향 분석이 필요하며, 이를 통해 국내 제도의 간소화 및 체계적인 개선방안 확립이 요구된다. 또한, IT제품 도입과정에 있어 공급망 공격 사례가 증가하고 있음에 따라 공급 과정에서 발생 가능한 보안 사고를 예방하기 위한 제도의 필요성이 강조되고 있다. 이에 따라 정보보호제품 도입제도와 관련하여 공급망 위험 관리 체계에 대한 연구를 수행할 예정이다.

References

[1] National Archives of Korea, "Administration Computerization" http://www.archives.go.kr/next/search/listSubjectDescription.do?id=001951, Aug. 2019.

[2] KISA, "Cyber-threat intelligence network and '2017 seven Cyber attack forecast'", https://www.kisa.or.kr/jsp/common/downloadAction.jsp?bno=8&dno=1516&fseq=1, Dec. 2016.

[3] Nam-Kyun Baik, Min-Woo Son, Woong-Sang Kim, Ho-Jun Park and Jason Kim, "Analysis of security evaluation & certification scheme for CCRA CAP," Proceedings of Symposium of the Korean Institute of communications and Information Sciences, pp. 2009(06), pp. 1670-1673, Jun. 2009.

[4] Myeonggil Choi, Hacyun Na and Jaehun Jeong, "Analysis of international evaluation certification scheme," Korea Institute Of Information Security And Cryptology, 23(5), pp. 29-35, Oct. 2013.

[5] Nam-Kyun Baik, Minwoo Son and Jason Kim, "Foreign certificate issuing country CC-based information protection product evaluation trend," Korea Institute Of Information Security And Cryptology, 19(6), pp. 49-67, Dec. 2009.

[6] Lee Dae Seob and Hong Won Soon, "Status and future direction of domestic evaluation and certification policy," Korea Institute Of Information Security And Cryptology, 17(6), pp. 20-24, Dec. 2007.

[7] Choi, Myeong-Gil and Jeong, Jae-Hun, "A study on domestic and foreign policy trends of CMVP," Proceedings of Symposium of the Korean Academy Industrial Cooperation Society, pp. 471-474, May. 2010.

[8] Choi, Myeong-Gil and Jeong, Jae-Hun, "A study on the policy of cryptographic module verification program," Korea Academy Industrial Cooperation Society, 12(1), pp. 255-262, Jan. 2011.

[9] National Intelligence Service, "Security Conformance" https://www.nis.go.kr:4016/AF/1_7_2_1.do, Aug. 2019.

[10] National Intelligence Service, "Security function test result" https://www.nis.go.kr:4016/AF/1_7_2_3/view.do?seq=66&currentPage=1, Aug. 2019.

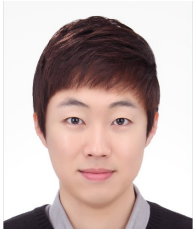
[11] National Information Assurance Partnership, "What is NIAP/CCEVS?" https://www.niap-ccevs.org/Ref/What_is_NIAP.CCEVS.cfm, Aug. 2019.

[12] Committee on National Security System, "CNSSP Policy No.11 - National Policy Governing the Acquisition of Information Assurance

(IA) and IA-Enabled Information Technology Products", Jun. 2013.
〔13〕 Government Security Classifications, "Government Security Classifications" https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf, May. 2018.
〔14〕 Information Technology Promotion Agency, https://www.ipa.go.jp/index-e.html, Aug. 2019.
〔15〕 Information Technology Promotion Agency, "Japan Cryptographic Module Validation Program" https://www.ipa.go.jp/security/english/jcmvp.html, Aug. 2019.
〔16〕 Information Technology Promotion Agency, "Japan Information Technology Security Evaluation and Certification Scheme" https://www.ipa.go.jp/security/jisec/jisec_e/index.html, Aug. 2019.
〔17〕 Canadian Centre for Cyber Security, "Cryptographic Module Validation Program" https://cyber.gc.ca/en/cryptographic-module-validation-program-cmvp, Aug. 2019.
〔18〕 EVALUATION OF CRYPTOGRAPHIC FUNCTIONALITY, https://cyber.gc.ca/sites/default/files/publications/instruction4-eng_0.pdf, Jul. 2016.
〔19〕 Canadian Centre for Cyber Security, "Canadian Common Criteria Program" https://cyber.gc.ca/en/common-criteria, Aug. 2019.
〔20〕 Canadian Centre for Cyber Security, "Protection Profiles" https://cyber.gc.ca/en/protection-profiles, Aug. 2019.
〔21〕 Australian Cyber Security Centre, "ARRANGEMENT on the Recognition of Common Criteria Certificates" https://acsc.gov.au/publications/aisep/ccra.pdf, Jul. 2014.
〔22〕 Canadian Centre for Cyber Security, "COMSEC" https://cyber.gc.ca/en/comsec, Aug. 2019.
〔23〕 Australian Cyber Security Centre, "Evaluated Products List" https://asd.gov.au/infosec/epl/, Aug. 2019.
〔24〕 Australian Cyber Security Centre, "Australian Government Information Security Manual" https://acsc.gov.au/publications/ism/Australian_Government_Information_Security_Manual.pdf, Feb. 2019.

〈저자소개〉

손 효 현 (Hyo-hyun Son) 학생회원
2019년 2월: 한남대학교 컴퓨터통신무인기술학과 학사
2018년 3월~현재: 한남대학교 컴퓨터공학과 학·석사연계과정
〈관심분야〉 정보보호, 정보보호정책, 소프트웨어 평가 및 검증, 보안적합성 검증



김 광 준 (Kwang-Jun Kim) 학생회원
2017년 2월: 한남대학교 컴퓨터공학과 학사
2019년 2월: 한남대학교 컴퓨터공학과 석사
2019년 3월~현재: 한남대학교 컴퓨터공학과 박사과정
〈관심분야〉 정보보호, 침입 탐지, 네트워크/시스템 보안

이 만 희 (Man-hee Lee) 종신회원
1995년 2월: 경북대학교 컴퓨터공학과 공학사
1997년 2월: 경북대학교 공학석사
2008년 8월: Texas A&M 대학교 컴퓨터공학과 공학박사
1997년~2003년: 한국과학기술정보연구원 연구원
2008년~2009년: Cisco Systems, San Jose
2010년~2012년: 국가보안기술연구소 선임연구원
2012년~현재: 한남대학교 부교수
〈관심분야〉 네트워크/시스템/스마트폰 보안, 고성능 시스템, 컴퓨터교육