情 報 保 護 學 會 誌
第19卷 第2號, 2009. 4

캐나다 정보기술보안 제품 사전 검증 제도에 관한 분석

김 준 섭*, 손 경 호**, 이 완 석**, 곽 진***

요 약

국내·외 IT 제품은 그 제품이 가지고 있는 안전성 및 신뢰성에 대한 검증을 통해 국가 및 공공기관에 제품 공급 및 이용 촉진을 도모하고 있다. 또한 각 국가마다 보안제품 특징과 성격에 맞는 평가와 인증을 수행하기 위한 보안성 평가 서비스를 제공하고 있으며, 시스템 평가 기준과 방법론이 개발 및 운영되고 이에 따라 캐나다에서는 정보기술보안 제품의 안전성을 사전에 검증하기 위한 제도를 시행하고 있다. 본 고에서는 캐나다의 정보기술보안 제품 사전 검증 제도에 대한 분석을 통해 국내 적용가능성에 대하여 분석한다.

Ⅰ. 서 론

공공기관 및 국가기관으로부터 정보보호 시스템을 구축하려는 움직임이 활발해 지면서 보안성이 평가되고, 인증된 제품을 선호하게 되었다. 이로 인해 제품에 대한 보안성 인증 문제가 대두되기 시작하면서 국내·외에서 다양한 평가 서비스의 필요성이 증가하였다. 국내에서도 이러한 필요성의 증가로 암호 기능의 보증을 위한 '암호검증제도', 국제공통평가기준(CC)을 통한 '정보보호제품 평가·인증제도', 국가 및 공공기관에 신뢰된 IT 제품을 도입하기 위한 '보안적합성 검증제도', 운영 수준의 보증을 위한 '정보보호관리체계(ISMS) 제도' 등 다양한 보안성 평가 서비스를 제공함으로써 IT 제품의 보안기능을 검증하여 국가 정보보호 수준을 향상시키고 있다, 또한, 정보화 역기능으로부터 주요 자산을 보호할 수 있도록 국가 및 공공기관 사용자에게 신뢰할 수 있는 정보보호 제품을 선택하는 방안을 마련하고 있다.

그러나 대부분의 제도는 제품 수준의 보증제도이거나 이미 운영되는 정보시스템에 대한 보안 관리 수준이며, 운용 시스템 또는 응용 시스템에 대한 보증제도는 정착되고 있지 못하고 있다.

이러한 문제를 해결하기 위하여 미국의 연방정보보안관리법(FISMA), 영국의 정보보증 및 컨설턴트 서비스(IACS), 일본 ST 확인 제도 등 각 나라마다 보안제품 특징과 성격에 맞는 평가와 인증을 수행하기 위한 보안성 평가 서비스를 제공하며, 시스템 평가 기준과 방법론이 개발 및 운영되고 있다[1][2][3]. 캐나다의 경우는 정보기술보안 제품 사전 검증 제도를 시행하고 있다. 본 고에서는 캐나다 정보기술보안 제품 사전 검증 제도에 대해서 분석하고자 한다.

Ⅱ. 정보기술보안 제품 사전 검증 제도

2.1 개요

캐나다의 정보기술보안 제품 사전 검증 제도(IPPP : ITS Product Pre-qualification Program)는 캐나다 정부 내에서 정보기술보안 제품들을 사용하기 위한 자격을 부여하기 위해서 캐나다 통신보안국, 공공사업서비스처에서 공동으로 개발하였다. 이 제도의 목적은 캐나다 정부 내에서 통신보안국의 사전 자격 기준에 알맞게 정보기술보안 제품의 구매를 용이하게 하기 위한 목적을 가지고 있다[4].

* 순천향대학교 정보보호학과 (jskim0911@sch.ac.kr)
** 성균관대학교 정보보호그룹 (khson@security.re.kr, wsyi@kisa.or.kr)
*** (교신저자) 순천향대학교 정보보호학과 교수 (jkwak@sch.ac.kr)

2.2 요구사항

정보기술보안 제품 사전 검증 제도는 캐나다 통신보안국에 의해 자격을 부여받은 정보기술보안 제품에 대하여 정보기술보안 사전 자격 제품 목록(IPPL: ITS Pre-qualification Product List)에 제공한다.

정보기술보안 제품이 정보기술보안 사전 검증 제품 목록에 포함되기 위해서는 캐나다 통신보안국에서 규정한 다음의 요구사항 중 하나 이상을 만족해야 한다.

- FIPS 140-1 또는 FIPS 140-2로 검증하거나, 암호모듈검증제도에서 FIPS 140-1 또는 FIPS 140-2로 검증된 통합 암호모듈
- 캐나다 통신보안국의 암호보증제도로 보증된 제품
- 캐나다 공통평가기준으로 인증된 제품

정보기술보안 제품이 하나 이상의 요구사항을 만족하더라도 IT 제품에 대한 성공적인 사전 심사를 하기 위해서는 캐나다 통신보안국에 의해 수행된 시험 과정을 요구한다.

캐나다 통신보안국은 다음의 사항에 대하여 검증을 수행한다.

- 캐나다 통신보안국이 인가한 암호 알고리즘과 FIPS 140-1 또는 FIPS 140-2로 검증된 암호모듈을 사용한 제품
- CMVP, 암호보증제도, 캐나다 공통평가기준에서 검증된 제품
- 취약성이 존재하지 않는 제품

위의 조건을 만족할 경우, 캐나다 인증기관의 웹사이트에서 정보기술보안 사전 검증 제품 목록표로 유지 및 관리된다.

정부 기관에서는 정보기술보안 제품의 선택을 위해 제품 목록을 참고하고, 해당 제품의 구성과 사용에 관하여 캐나다 통신보안국에서는 지침을 제공한다.

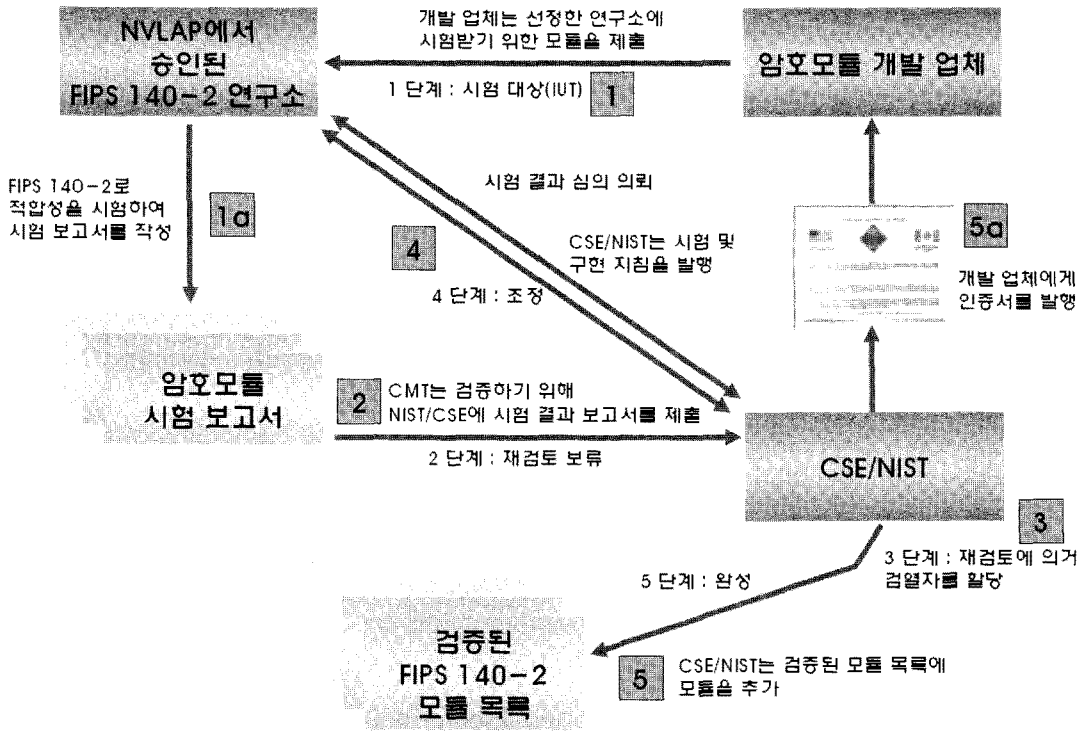
2.3 정보기술보안 제품 사전 검증 제도 구성 프로그램

2.3.1 암호모듈검증제도

캐나다 통신보안국과 미국표준기술연구소(NIST: National Institute of Standards and Technology)는 1995년 7월 17일에 CMVP 제도를 공동으로 발표했다[5]. 암호모듈검증제도(CMVP : Cryptographic Module Validation Program)는 FIPS 140-2 및 기타 암호 알고리즘을 근거하는 표준과 상용 암호모듈의 검증을 실시한다. CMVP는 미국표준기술 연구소와 캐나다 통신보안국에 의해 공동으로 관리되고 있으며, FIPS 140-1 또는 FIPS 140-2에 의해 검증된 제품은 양국의 연방 정부 기관에 의해 인정받는다. CMVP의 목표는 검증된 암호모듈의 사용을 장려하고, 검증된 암호모듈을 포함하고 있는 조달 장비를 사용하는 것에 대한 보안 측정 기준을 연방 정부 기관에 제공한다. CMVP에 있어서 상용 암호모듈의 개발 업체는 개발한 모듈을 시험받기 위해서 인가된 암호모듈시험(CMT : Cryptographic Module Testing) 연구소를 독립적으로 이용한다. 국립자율시험기관인증프로그램(NVLAP : National Voluntary Laboratory Accreditation Program) 또는 캐나다 표준위원회(SCC: Standards Council of Canada)에 의해 인가된 연구소는 암호모듈의 준수 및 적합성 시험을 수행한다.

2002년 5월 25일 이전의 상용 암호모듈은 FIPS 140-1을 적용하여 암호모듈에 대한 보안 요구사항을 검증받고 있으며, 2002년 5월 26일 이후는 FIPS 140-2를 적용하여 암호모듈에 대한 보안 요구사항을 검증하다. FIPS 140-2는 정보를 보호하고 있는 보안 시스템 내에서 활용되는 암호모듈을 만족시키는 보안 요구사항을 지정한다. 이 표준은 4개의 보안 등급을 제공한다(level 1, level 2, level 3, level 4). 제시된 등급은 암호모듈을 사용하는 잠재적 애플리케이션의 넓은 범위와 환경을 포함하고 있다. 보안 요구사항은 암호모듈의 안전한 설계 및 구현과 관련된 11개의 영역을 포함한다. 이러한 영역은 암호모듈 명세, 암호모듈 포트와 인터페이스, 역할·서비스·인증, 유한 상태 모델, 물리적 보안, 운영환경, 암호 키 관리, 전자파 장해/전자파 적합성, 자가 시험, 설계 보증, 기타 공격들에 대한 완화를 포함한다. FIPS 140-2로 검증한 인증서는 각각의 검증된 모듈을 위해 발급된다.

개발 업체와 사용자를 위한 암호모듈이 FIPS 140-2에 정해진 보안 요구사항들에 적합하다고 해도 반드시 그 모듈이 안전하다고 볼 수 없다. 개별 영역의 등급은 암호모듈이 구현되는 환경에 의존하므로 보안 등급보다 중요하다.



〔그림 1〕 FIPS 140-2 시험 및 검증의 일반적인 흐름도

조직에서는 암호모듈을 사용하기 전에 FIPS 140-1 또는 FIPS 140-2로 검증한 인증서의 사본을 제공하기 위해 CMVP로 검증하거나 검증 인증서 번호를 개발 업체에 요청해야 한다. 배포된 암호모듈의 버전 번호는 요구된 인증서에 대해 나열된 번호와 동일해야 하며, 검증된 암호모듈에 대한 버전 번호는 FIPS 140-1 및 FIPS 140-2로 검증된 암호모듈의 온라인 목록에서 검증한다.

미국표준기술연구소/캐나다 통신보안국의 CMVP에 대한 주요 내용을 포함한 웹사이트는 미국표준기술 연구소에 의해 관리되며, FIPS 140-1 및 FIPS 140-2로 검증된 암호모듈의 기관 목록뿐만 아니라 관련된 표준과 문서는 프로그램에 대한 세부 내용을 포함하고 있다. 또한 FIPS 140-1 및 FIPS 140-2로 검증된 암호모듈의 목록을 위해 수정된 캐나다 버전을 유지한다.

2.3.1.1 시험 요구사항

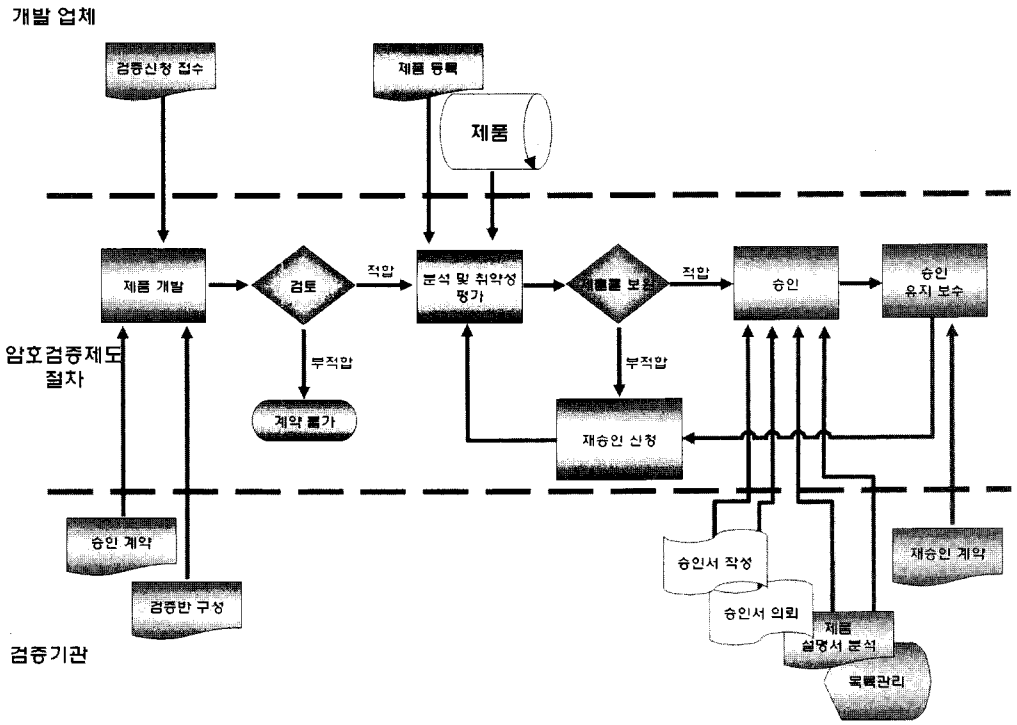
국립자율시험기관인증프로그램에서 승인된 암호모듈 시험 연구소는 암호모듈의 검증 시험을 수행한다. 암호모듈은 FIPS 140-2의 암호모듈에 대한 보안 요구사항에 근거하여 시험을 실시한다. 암호모듈 검증 시험은 FIPS 140-2 DTR(Derived Test Requirement) 문서를 분석하며, 암호모듈을 검증하기 위해 개발 업체와 평가자 요구사항의 모든 문서 목록은 암호모듈시험에서 인정된 연구소에 의해 수행된 시험을 기반으로 제공한다.

[그림 1]은 FIPS 140-2에 대한 시험 과정의 일반적인 흐름을 정리한 것이다.

2.3.1.2 FIPS 140-3

캐나다 통신보안국과 미국표준기술연구소는 표준의 주요 영역이 현재 기술과 일치하도록 유지하고, 개발 업체뿐만 아니라 연방 기관들의 제안사항을 포함한다. 또한 요구사항을 강화하기 위해 FIPS 140-2의 재검토 및 갱신을 수행한다. FIPS 140-3은 새로운 보안 등급을 추가하고, 향상된 최근 기술을 반영하기 위해 광범위하고 새로운 보안 특징을 통합한다[6]. FIPS 140-3에서는 11개의 요구사항 영역을 각각 정의하고 있으며, 5개의 보안 등급을 제공한다.

이 표준에 지정된 보안 요구사항은 암호모듈에 의해 제공된 보안이 유지되더라도 표준에 대한 적합성은 특정한 모듈이 안전하다는 것을 보증하지 못한다. 암호 모



〔그림 2〕 암호보증제도 과정

듈의 운영자는 모듈이 제공하는 보안이 정보의 소유자에게 용인할 수 있는 것을 보증하기 위한 책임이 있으며, 잔여 위험을 수용하고 받아들인다. 마찬가지로 컴퓨터 또는 통신 시스템에 검증된 암호 모듈의 사용은 전반적인 시스템의 보안을 보증하지 못한다. 암호 모듈의 전반적인 보안 등급은 애플리케이션의 보안 요구사항과 모듈을 제공하기 위한 보안 서비스뿐만 아니라 활용될 수 있는 환경에 대한 보안 등급을 제공하기 위하여 선택되어야 한다. 또한 FIPS 140-3은 물리적인 영역, 소프트웨어 보안, 모듈 보증에 대한 변화를 포함하고 있다.

2.3.2 암호보증제도

암호보증제도(CEP : Cryptographic Endorsement Program)는 캐나다 통신보안국과 개발 업체가 함께 정보기술보안 제품의 암호 기능을 평가하기 위해 캐나다 정부에서 제품의 사용을 승인하는 프로그램이다. 캐나다 통신보안국은 웹사이트를 통하여 승인한 제품의 목록을 유지·관리한다.

캐나다 통신보안국은 암호보증제도를 활용하여 FIPS 140-1 및 FIPS 140-2로 검증된 암호모듈을 포함하고 있는 제품의 암호운영을 평가하며, 제품의 취약성 분석을 수행한다. 이러한 과정은 연방 정부에서 FIPS 140-1 또는 FIPS 140-2로 검증된 암호모듈을 포함하고 있는 제품에 대한 추가적인 보증을 제공하며, 개발 업체에게 제품의 독립적인 평가 승인을 성공적으로 수행하기 위한 신뢰성을 제공한다. [그림 2]는 암호보증제도의 과정을 도식화한 것이다.

2.3.3 캐나다 공통평가기준

캐나다 공통평가기준(CCS : Canadian Common Criteria Scheme)은 IT 보안 제품과 시스템의 신뢰성을 평가하기 위한 캐나다의 독립적인 평가 및 인증 서비스이다[7]. 캐나다 공통평가기준에서는 간소화된 공통평가기준의 평가서비스를 포함하며, 인증기관의 운영을 위한 다양한 세부 지침을 제공하여 효과적인 IT 보안 평가 능력을 제공한다.

캐나다 공통평가기준은 연방 정부와 산업체 사이의 협력적 관계로 승인된 민간 부문의 평가 연구소에서 공통평가기준 평가가 수행된다. 평가 기술 심의와 결과에 대한 인증은 캐나다 정부 내의 인증기관 및 통신보안국에 의해 운영된다. 캐나다는 공통평가기준을 위한 1개

의 인증기관, 인정기관과 3개의 평가 기관을 운영하고 있다. [표 1]은 캐나다 공통평가기준을 수행하는 관련 기관을 정리한 것이다.

〔표 1〕 캐나다 공통평가기준의 관련기관

기 관	명칭 및 웹사이트
인증기관	CSEC (http://www.cse-cst.gc.ca)
인정기관	Standard Council of Canada (http://www.scc.ca)
평가기관	CGI Information Systems and Management Consultants Inc (http://www.cgi.com)
	DOMUS IT Security Laboratory (http://www.domusitsl.com)
	EWA Delivering the Right Assurance (http://www.ewa-canada.com)

Ⅲ. 정보기술보안 사전 자격 제품 목록

3.1 개요

정보기술보안 사전 자격 제품 목록은 정보기술보안 제품 사전 검증 제도에서 캐나다 통신보안국에 의해 자격을 부여받은 제품의 목록을 나타내며, 캐나다 정부의 조달 목적으로만 사용된다. 제품의 사전 자격은 캐나다 통신보안국에 의한 보증을 의미하지는 않으며, 제품의 운영 환경에서 요구되는 보증 등급을 평가하기 위한 전제 조건이다.

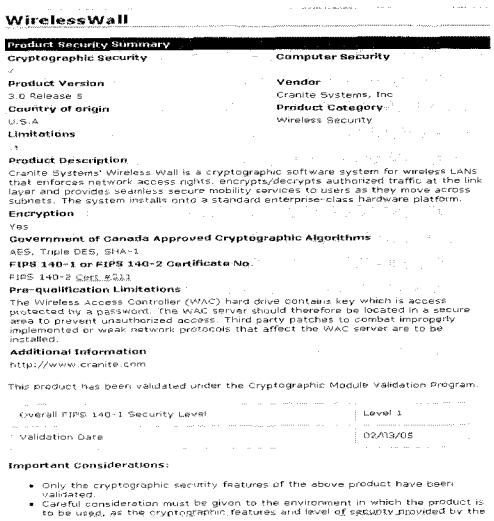
3.2 정보기술보안 사전 자격 제품 목록 분류

[표 2]는 정보기술 보안 사전 자격 제품 목록에 대한 분류를 나타낸다.

〔표 2〕 정보기술보안 사전 자격 제품 목록 분류표

정보기술보안 사전 자격 제품 목록 분류	
암호화 가속기	디스크 암호화
전자상거래 응용프로그램	팩스밀리 암호화
방화벽	침입 탐지 및 방지 시스템
다기능 인쇄 및 복사	네트워크 암호화
네트워크 관리	보안 원격 접근 암호화
통신 방화벽	토큰 응용프로그램
토큰	가상 사설망
음성 암호화	무선 보안

3.3 제품 목록 설명



WirelessWall

Product Security Summary

Cryptographic Security — **Computer Security**

Product Version: 3.0 Release 5 — **Vendor**: Cranite Systems, Inc

Country of origin: U.S.A — **Product Category**: Wireless Security

Limitations: -

Product Description: Cranite Systems' Wireless Wall is a cryptographic software system for wireless LANs that enforces network access rights, encrypts/decrypts authorized traffic at the link layer and provides seamless secure mobility services to users as they move across subnets. The system installs onto a standard enterprise-class hardware platform.

Encryption: Yes

Government of Canada Approved Cryptographic Algorithms: AES, Triple DES, SHA-1

FIPS 140-1 or FIPS 140-2 Certificate No.: FIPS 140-2 Certs. #211

Pre-qualification Limitations: The Wireless Access Controller (WAC) hard drive contains key which is access protected by a password. The WAC server should therefore be located in a secure area to prevent unauthorized access. Third party patches to combat improperly implemented or weak network protocols that affect the WAC server are to be installed.

Additional Information: http://www.cranite.com

This product has been validated under the Cryptographic Module Validation Program.

Overall FIPS 140-1 Security Level	Level 1
Validation Date	02/13/05

Important Considerations:

- Only the cryptographic security features of the above product have been validated.
- Careful consideration must be given to the environment in which the product is to be used, as the cryptographic features and level of security provided by the

〔그림 3〕 웹사이트에 기재되어 있는 제품 예시

[그림 3]은 정보기술보안 사전 자격 제품 목록의 웹사이트에 기재되어 있는 제품에 대한 예시를 나타낸다. 정보기술보안 제품 사전 검증 제도로 검증된 해당 IT 제품의 목록에는 [그림 3]과 같이 암호화 보안, 제품에 대한 사전 자격 표시, 제품 버전, 개발 업체, 제품 분류, 제품 설명, 암호화 여부, 암호 알고리즘, 사전 자격 표시 여부에 따른 사전 자격 제한 내용 등을 기록하여 유지·관리한다.

다음은 정보기술보안 사전 자격 제품 목록에 대한 세부 사항을 분석하고, [표 4]에서 정리하였다. 또한 [표 5]~[표 20]은 캐나다의 정보기술보안 사전 자격 제품 목록의 사양을 정리한 것이다.

- ○ 제품 명칭 : 해당 IT 제품에 대한 명칭을 나타낸다.
- ○ 암호화 보안 : 암호화 보안 부분에 ✓(붉은색) 표시가 있으면 CMVP에서 암호모듈을 인가하거나 암호보증제도에서 승인된 사전 자격이 있는 IT 제품을 나타낸다.
- ○ 컴퓨터 보안 : 컴퓨터 보안 부분에 ✓(파란색) 표시가 있으면 캐나다 공통평가기준에서 보증하거나 승인된 사전 자격이 있는 IT 제품을 나타낸다.
- ○ 제품 버전 : 해당 IT 제품에 대한 특정 소프트웨어나 펌웨어의 버전 번호 및 배포 번호를 나타낸다. 필요에 따라 패치 등급을 포함한다.

  - Version 3.0 Release 5(예시)

○ 개발 업체 : 해당 IT 제품을 개발한 업체를 나타낸다.
○ 개발 국가 : 해당 IT 제품을 개발한 국가를 나타낸다.
○ 제품 분류 : 정보기술보안 사전 자격 제품 목록 분류에 나타낸 것과 같이 제품 분류에 대한 정보를 나타낸다.
- [표 2] 참조
○ 제한 : 제한 부분에 있는 ! 기호는 사전 자격이 있는 IT 제품을 사용해야 하는 방법에 대한 제품 보안 요약의 중요한 지침을 나타낸다.
○ 제품 설명 : 해당 IT 제품에 대한 소개와 보안 구성 및 기술적 세부 사항에 대한 설명을 나타낸다.
○ 캐나다 공통평가기준 인증 정보 : 캐나다 공통평가기준으로 평가된 인증 정보 및 평가 내용에 대한 간략한 설명을 나타낸다.
○ 암호화 여부 : 해당 IT 제품에 대한 암호화 여부를 표시한다.
- 암호화 기능(유, 무)
○ 암호 알고리즘 : [표 3]은 해당 IT 제품의 암호화 알고리즘 사양을 나타낸다.

〔표 3〕 암호화 알고리즘 사양

구 분	알고리즘
암호화	Triple DES, AES, RSA, CAST, CAST-128, Skipjack 등
디지털 서명	RSA, DSA 등
키 교환	Diffie-Hellman, RSA 등
해쉬	SHA-1, SHA-256, SHA-384, SHE-512 등

○ FIPS 140-1/140-2 인증서 번호 : 해당 IT 제품의 FIPS 140-2 또는 140-2 인증서 번호를 나타낸다.
- FIPS 140-2 Cert #311(예시)
○ 사전 자격 제한 : 해당 IT 제품에 대한 사전 가격이 있는 제품 보안의 요약에 대한 중요한 지침을 나타낸다.
- 무선 접근 컨트롤러(WAC) 하드 드라이브는 패스워드로 보호된 키를 포함한다(예시).
○ 추가 정보 : 필요에 따라 해당 IT 제품의 추가적인 정보를 제공한다.
- 공통평가기준 평가 등급
- CMVP 보안 등급
- 개발 업체 웹사이트, 인증 날짜
- 인증서, 인증 국가
- 제품 ST 문서
○ 중요 고려사항 : 해당 IT 제품을 도입하거나 사용하는 것에 대한 중요 고려사항을 나타낸다.

〔표 4〕 정보기술보안 사전 자격 제품 목록

구 분	분 류
제품 명칭	IT 제품에 대한 명칭 표시
암호화 보안	CMVP로 인가 및 암호보증제도로 승인된 사전 자격이 있는 IT 제품 표시
컴퓨터 보안	캐나다 공통평가기준으로 인증 및 승인된 사전 자격이 있는 IT 제품 표시
제품 버전	IT 제품의 버전, 배포 번호 표시
개발 업체	IT 제품의 개발 업체를 표시
개발 국가	IT 제품을 개발한 국가를 표시
제품 분류	IT 제품의 주요 제품 분류
제한	사전 자격이 있는 IT 제품에 대한 표시
제품 설명	IT 제품 설명 및 구성에 대한 요약
캐나다 공통평가기준 인증 정보	캐나다 공통평가기준으로 인증된 인증 정보 표시
암호화 여부	IT 제품의 암호화 여부 표시
암호 알고리즘	IT 제품의 암호화 알고리즘 표시
FIPS 140-1/140-2 인증서 번호	FIPS 140-1/140-2 인증서 번호 표시
사전 자격 제한	IT 제품의 사전 자격 제한에 대한 설명 요약
추가 정보	IT 제품의 공통평가기준/CMVP로 검증된 검증 등급, 인증 날짜, 인증 국가 등 표시
중요 고려사항	IT 제품에 대한 중요 고려사항 설명 요약

〔표 5〕 토큰 응용프로그램의 제품 목록 사양

제품 분류	제품명	개발 업체	평가 등급	보증 등급	검증 일자
토큰 응용 프로그램	Portico Version 1.1	Spyrus, Inc.	-	FIPS 140-1 Level 2	2000. 10
	iKey 2032 FIPS tokens	SafeNet Inc.	-	FIPS 140-1 Level 2	2001. 08

〔표 6〕 디스크 암호화의 제품 목록 사양

제품 분류	제품명	개발 업체	평가 등급	보증 등급	검증 일자
디스크 암호화	Endpoint Full Disk Encryption	Check Point Software Technologies Inc.	-	FIPS 140-1 Level 1	2002. 03
	RASP Secure Media	Kasten Chase Applied Research	-	FIPS 140-1 Level 2	2000. 09
	SecureDoc Disk Encryption Version 4.3	WinMagic Inc.	-	FIPS 140-2 Level 2	2007. 07
	MXI Stealth MXP and Stealth Passport v3.3.3	Memory Experts International	-	FIPS 140-2 Level 2	2007. 08
	McAfee Endpoint Encryption for Devices	McAfee Inc.	-	FIPS 140-2 Level 1	2007. 04
	SafeGuard Enterprise 5.2	Utimaco	-	FIPS 140-2 Level 1	2007. 10

〔표 7〕 암호화 가속기의 제품 목록 사양

제품 분류	제품명	개발 업체	평가 등급	보증 등급	검증 일자
암호화 가속기	CSA 8000 AKA protectserver orange	Eracom Technologies Group, Eracom Technologies Australia, Pty. Ltd.	-	FIPS 140-1 Level 3	2007. 07
	CryptoSwift HSM-150	SafeNet Inc.	-	FIPS 140-1 Level 3	2001. 08
	Luna® XPplus	SafeNet Inc.	-	FIPS 140-1 Level 3	2001. 10
	nCipher DSE200 Document Sealing Engine	nCipher Inc.	-	FIPS 140-1 Level 3	2005. 05
	nForce 150 SCSI and nForce 400 SCSI	nCipher Inc.	-	FIPS 140-2 Level 2	2005. 05
	nForce 800 PCI, nForce 1600 PCI	nCipher Inc.	-	FIPS 140-2 Level 2, 3	2005. 05
	nShield F2 SCSI and nShield F2 Ultrasign SCSI	nCipher Inc.	-	FIPS 140-2 Level 2	2005. 05
	nShield F2 PCI and nShield F2 Ultrasign PCI	nCipher Inc.	-	FIPS 140-2 Level 2	2005. 05
	nShield F3 PCI, nShield F3 Ultrasign PCI, nShield Lite	nCipher Inc.	-	FIPS 140-2 Level 3	2005. 05
	nShield F3 SCSI and nShield F3 Ultrasign SCSI	nCipher Inc.	-	FIPS 140-2 Level 3	2005. 05
	nShield F3 800 PCI and nShield F3 4K PCI	nCipher Inc.	-	FIPS 140-2 Level 2, 3	2005. 05
	net HSM	nCipher Inc.	-	FIPS 140-2 Level 2, 3	2005. 05

〔표 8〕 음성 암호화의 제품 목록 사양

제품 분류	제품명	개발 업체	평가 등급	보증 등급	검증 일자
음성 암호화	Privatel Model 960v	L-3 Communication Systems East	-	FIPS 140-1 Level 1	2000. 09

〔표 9〕 네트워크 관리의 제품 목록 사양

제품 분류	제품명	개발 업체	평가 등급	보증 등급	검증 일자
네트워크 관리	Citrix MetaFrame™ XP Presentation Server for Windows® with Feature Release 3	Citrix Systems, Inc.	EAL 2+	-	2004. 04
	Intellitactics™ Incorporated Network Security Manager™ (NSMTM) v4.1	Intellitactics™ Incorporated	EAL 2	-	2004. 12
	STAT Guardian Vulnerability Management Suite	Harris Corporation	EAL 2+	-	2006. 05
	STAT® Scanner Professional Edition	Harris Corporation	EAL 2+	-	2003. 04
	nCircle™ Vulnerability Management System	nCircle™ Inc	EAL 3	-	2005. 05

〔표 10〕 전자상거래 응용프로그램의 제품 목록 사양

제품 분류	제품명	개발 업체	평가 등급	보증 등급	검증 일자
전자상거래 응용프로그램	CipherShare™	Kasten Chase Applied Research	-	FIPS 140-2 Level 1	2004. 12
	Cisco Intrusion Detection System Module	Cisco	EAL 2	-	2004. 05
	Cisco Intrusion Detection System Sensor Appliance IDS-4200 Series v4.1	Cisco	EAL 2	-	2004. 05
	Cisco VoIP Telephony System	Cisco	EAL 1	-	2005. 05
	CoreStreet Real Time Credential Validation Authority	CoreStreet, Ltd	EAL 3	-	2004. 09
	Customs Internet Gateway Exchange	Logistics Software Corp.	-	FIPS 140-1 Level 1	2004. 05
	Focal Point Version 2.3.2	Okiok Ltd.	-	FIPS 140-1 Level 1	2004. 01
	Image Overwrite Security for Xerox® WorkCentre® M35™/M45™/M55™ and WorkCentre® Pro 35/45/55 Advanced Multifunction System	Xerox Corporation	EAL 2	-	2004. 05
	MetaFrame Password Manager	Citrix Systems, Inc.	-	FIPS 140-1 Level 1	2004. 06
	Sun Java™ System Identity Manager	Sun	EAL 2	-	2005. 08
	ViaSafe® Agent Version 2.0	ViaSafe Inc	-	FIPS 140-1 Level 1	1999. 05
	e-witness Fortrus™	E-witness Internet Security Inc.	-	FIPS 140-1 Level 2	2001. 09

〔표 11〕 팩스밀리 암호화의 제품 목록 사양

제품 분류	제품명	개발 업체	평가 등급	보증 등급	검증 일자
팩스밀리 암호화	CF3102 Facsimile Encryptor	Certifax (AOS Inc.)	-	FIPS 140-1 Level 3	1999. 09

〔표 12〕 네트워크 암호화의 제품 목록 사양

제품 분류	제품명	개발 업체	평가 등급	보증 등급	검증 일자
네트워크 암호화	Contivity Extranet Switch Model 4500	Nortel Networks	-	FIPS 140-1 Level 2	2000. 05
	Datacryptor 2000 Release 3.1	Thales-eSecurity Limited	-	FIPS 140-1 Level 3	1999. 09
	Tenix Interactive Link V5.1	Tenix Datagate Inc	EAL 5+	-	2005. 08
	Tenix Interactive Link Data Diode Device, Gigabit Variant, V3.0	Tenix Datagate Inc	EAL 7	-	2006. 11
	Tenix Interactive Link Data Diode Device V2.1	Tenix Datagate Inc	EAL 7	-	2005. 08

〔표 13〕 방화벽의 제품 목록 사양

제품 분류	제품명	개발 업체	평가 등급	보증 등급	검증 일자
방화벽	BorderWare Firewall	BorderWare Technologies Inc.	EAL 4	-	2002. 01
	BorderWare MXtreme Mail Firewall	BorderWare Technologies Inc.	EAL 4+	-	2004. 07
	Cisco Secure PIX Firewall	Cisco	EAL 4	-	2002. 12
	ConSeal Private Desktop Version 1.4	Signal9 Solutions	EAL 1	-	1999. 05
	CyberGuard Firewall for UnixWare/ Premium Appliance Firewall Version 5.1	CyberGuard Corporation	EAL 4+	-	2000. 12 2003. 02
	CyberGuard Firewall for UnixWare/ Premium ver 5.2	Secure Technologies International Inc.	EAL 2, 4	-	2005. 02
	CyberGuard Firewall/VPN v6.2.1	Secure Technologies International Inc.	EAL 4+	-	2005. 12
	FortiGate™ Family of Antivirus Firewalls	Fortinet	EAL 4+	-	2005. 02
	Gauntlet Firewall for Solaris 8	Secure Computing Corporation	EAL 4	-	2002. 04
	Sidewinder Firewall Version 5.2.1	Secure Computing Corporation	EAL 2	-	2002. 09
	Sidewinder G2 Firewall	Secure Computing Corporation	EAL 4+	-	2003. 05
	Sidewinder G2™ Security Appliance Models 210, 310, 315, 410, 415, 510, 515, 1100, 1150, 2150, 4150 and Sidewinder G2™ Software v6.1	Secure Computing Corporation	EAL 4+	-	2004. 07
	Symantec Enterprise Firewall Version 7.0	Symantec Corporation	EAL 2, 4	-	2002. 06
	Symantec Gateway Security Version 2.0 5400 Series	Symantec Corporation	EAL 4+	-	2004. 04

〔표 14〕 보안 원격 접근 암호화의 제품 목록 사양

제품 분류	제품명	개발 업체	평가 등급	보증 등급	검증 일자
보안 원격 접근 암호화	Optiva Secure Plus Access Server Version 4.3.02	Kasten Chase Applied Research	-	FIPS 140-1 Level 1	2000. 09
	MobiKey v1.2 and v1.3	Route 1	-	FIPS 140-1 Level 2	2001. 08

〔표 15〕 무선 보안의 제품 목록 사양

제품 분류	제품명	개발 업체	평가 등급	보증 등급	검증 일자
무선 보안	SpectraGuard Enterprise v5.0 & SpectraGuard SAFE v2.0	AirTight Networks, Inc	EAL 2	-	2005. 08
	WirelessWall	Cranite Systems, Inc	-	FIPS 140-1 Level 1	2002. 03 2005. 03

〔표 16〕 토큰의 제품 목록 사양

제품 분류	제품명	개발 업체	평가 등급	보증 등급	검증 일자
토큰	Luna® CA3	SafeNet Inc.	EAL 4+	-	2002. 11
	Luna® PCI	SafeNet Inc.	-	FIPS 140-2 Level 2, 3	2005. 12
	Luna® SA	SafeNet Inc.	-	FIPS 140-2 Level 2, 3	2005. 12
	Luna® SP	SafeNet Inc.	-	FIPS 140-2 Level 3	2005. 12
	Rosetta SmartCard Version 2.01	Spyrus, Inc.	-	FIPS 140-1 Level 2	2000. 05

〔표 17〕 가상 사설망의 제품 목록 사양

제품 분류	제품명	개발 업체	평가 등급	보증 등급	검증 일자
가상 사설망	2621 and 2651 Modular Access Routers	Cisco Systems, Inc.	-	FIPS 140-1 Level 2	2001. 12
	2621 and 2651 Modular Access Routers with Crypto Accelerator Card	Cisco Systems, Inc.	-	FIPS 140-1 Level 2	2001. 12
	3640 and 3660 Modular Access Routers	Cisco Systems, Inc.	-	FIPS 140-1 Level 2	2001. 12
	3640 and 3660 VPN Routers with Crypto Accelerator Card	Cisco Systems, Inc.	-	FIPS 140-1 Level 2	2001. 12
	7140 VPN Router	Cisco Systems, Inc.	-	FIPS 140-1 Level 2	2001. 12
	7140 VPN Router with ISM Accelerator Card and 7140 VPN Router with Dual Accelerator Cards	Cisco Systems, Inc.	-	FIPS 140-1 Level 2	2001. 12
	7206 VXR Router	Cisco Systems, Inc.	-	FIPS 140-1 Level 2	2001. 12
	7206 VXR Routerwith ISA Accelerator Card	Cisco Systems, Inc.	-	FIPS 140-1 Level 2	2001. 12
	DiamondLink™	Cryptek Inc.	-	FIPS 140-1 Level 2	2002. 10
	DiamondPak™	Cryptek Inc.	-	FIPS 140-1 Level 2	2002. 10
	DiamondVPN™	Cryptek Inc.	-	FIPS 140-1 Level 2	2002. 10
	VPN 3000 Concentrators	Cisco Systems, Inc.	-	FIPS 140-1 Level 2	2002. 03
	VPN 3002 Hardware Client	Cisco Systems, Inc.	-	FIPS 140-1 Level 2	2002. 03

〔표 18〕 통신 방화벽의 제품 목록 사양

제품 분류	제품명	개발 업체	평가 등급	보증 등급	검증 일자
통신 방화벽	SecureLogix Corporation® Enterprise Telephony Management System 4.0.1	SecureLogix Corporation	EAL 2+	-	2003. 04
	SecureLogix Corporation® Enterprise Telephony Management System 4.1	SecureLogix Corporation	EAL 2+	-	2004. 03
	SecureLogix Corporation® TeleWall® system	SecureLogix Corporation	EAL 2+	-	2000. 10

〔표 19〕 침입 탐지 및 방지 시스템의 제품 목록 사양

제품 분류	제품명	개발 업체	평가 등급	보증 등급	검증 일자
침입 탐지 및 방지 시스템	SpectraGuard Enterprise v5.0 & SpectraGuard SAFE v2.0	AirTight Networks, Inc	EAL 2	-	2005. 08
	Symantec™ Critical System Protection v5.0.5	Symantec Corporation	EAL 2+	-	2006. 11
	Third Brigade Deep Security 5.0	Third Brigade Inc.	EAL 3+	-	2008. 04

〔표 20〕 다기능 인쇄 및 복사의 제품 목록 사양

제품 분류	제품명	개발 업체	평가 등급	보증 등급	검증 일자
다기능 인쇄 및 복사	HP LaserJet M4345 MFP,HP LaserJet M3027 MFP, HP LaserJet M3035, HP LaserJet M5025 MFP, HP LaserJet M5035 MFP, HP Color LaserJet	Hewlett-Packard Development Company, L.P	EAL 3	-	2007. 07

Ⅳ. 결 론

본 고에서 분석한 바와 같이, 캐나다 정보기술보안 제품 사전 검증 제도는 보안제품 특징과 성격에 부합하는 평가와 인증을 수행하기 위한 보안성 평가 서비스이다. 또한, 신뢰할 수 있는 IT 제품을 선택하기 위하여 정보기술보안 사전 자격 제품 목록을 제공함으로써 국가 및 공공기관 사용자에게 신뢰할 수 있는 정보보호제품을 선택하는 방안을 마련하고 있다.

본 고에서 분석한 캐나다 정보기술보안 제품 사전 검증 제도 및 제품 목록을 바탕으로 국외 보안성 평가 서비스 연구에 대한 사전자료 및 참고자료로 활용이 용이할 것으로 예상된다.

참고문헌

[1] http://csrc.nist.gov/groups/SMA/fisma/(FISMA 홈페이지).

[2] http://www.cesg.gov.uk(CESG 홈페이지).

[3] http://www.ipa.go.jp(IPA 홈페이지).

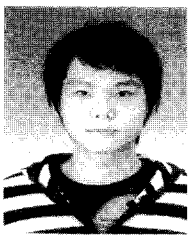
[4] http://www.cse-cst.gc.ca/index-eng.html (CSEC 홈페이지).

[5] http://csrc.nist.gov/groups/STM/cmvp/index.html (CMVP 홈페이지).

[6] NIST, FIPS Publication 140-3(Draft), Security Requirements for Cryptographic Modules, July 2007.

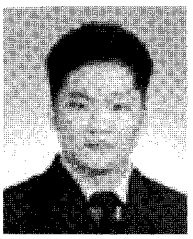
[7] CSEC, CCS-Guide-001 Version 0.96, Canadian Common Criteria Evaluation and Certification Scheme(CCS), Scheme Description, May 2000.

〈著者紹介〉



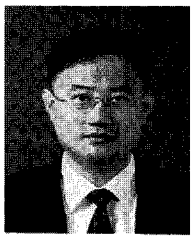
김 준 섭 (JunSub Kim)
학생회원

2003년 3월~현재: 순천향대학교 정보보호학과 재학
<관심분야> 정보보호, 정보보호제품 평가



손 경 호 (Kyungho Son)
특별회원

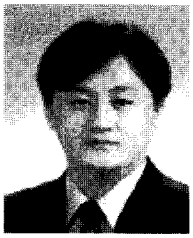
2001년 2월: 성균관대학교 전기전자컴퓨터공학과 학사
2004년~현재: 성균관대학교 컴퓨터공학과 석·박사과정 재학중
2001년 1월~현재: 한국정보보호진흥원(KISA) 선임연구원
<관심분야> 정보보호, 정보보호제품 및 시스템 보안성평가, 스마트카드 취약성



이 완 석 (Wan S. Yi)

정회원

1991년 5월: Va. Tech. 전산과학과 학사
2001년 2월: 동국대학교 정보보호학과 석사
2004년~현재: 성균관대학교 전자공학과 박사과정
1994년~1996년: 현대정보기술 CAD/CAM사업부 사원
1996년~현재: 한국정보보호진흥원 IT기반보호단 u-IT서비스 보호팀 팀장
<관심분야> 정보보증, 정보보호 제품 평가, 정보통신기반보호, 신규 IT서비스 보호



곽 진 (Jin Kwak)

종신회원

성균관대학교 학사, 석사, 박사
2006년 4월~2006년 11월: 일본 큐슈대학교 시스템정보공학부 방문연구원
2006년 8월~2006년 11월: 일본 큐슈시스템정보기술연구소 특별연구원
2006년~2007년 2월: 정보통신부 정보보호기획단 개인정보보호팀 통신사무관
2007년 2월~현재: 순천향대학교 정보보호학과 교수
<관심분야> 암호프로토콜, RFID 시스템 응용 보안, 개인정보보호, 정보보호제품 평가, u-City 정보보호 기술 등