

12. CMVP

먼저, CMVP는 Cryptographic Module Validation Program 약어이다.

1. CMVP 개요

- CMVP는 암호모듈의 안전성을 검증하기 위한 프로그램이다.
- CMVP는 미국의 NIST와 캐나다 주정부의 CSE가 공동으로 개발하였다.
- CSE는 Communications Security Establishment의 약어이다.
- CMVP는 암호모듈 시험평가 후 Level 1~4를 부여하고,
- 평가 결과를 List of Validated FIPS 140-1(FIPS 140-2) modules'에 등재하여 평가제품으로서 효력을 발휘할 수 있도록 한다.
- 현재, 많은 암호모듈이 검증을 받고 있다.

2. CMVP의 암호모듈에 대한 안전성 요구사항

① 구현 적합성 평가

- 구현된 암호기술이 표준에 따라 제대로 구현되었는지를 평가한다.
- 각 표준에 따라 평가하는 방법이 다르다.

② 암호키 운용 및 관리 평가

- 암호기술의 안전성에 직접 영향을 미치는 암호키의 생성, 확립, 분배, 입출력, 저장, 파괴 등에 대한 방법 및 과정을 평가한다.
- 즉, 잘못된 암호키 운용 및 관리에 따른 암호키의 유출 가능성을 평가하는 것이다.
- 암호모듈의 안전성 평가 중 가장 중요한 부분이라 할 수 있다.

③ 물리적 보안 평가

- 물리적 보안 평가는 암호모듈의 사용 환경에 대한 평가이다.
- 물리적 보안 평가는 암호모듈의 운영환경, EMI/EMC, 자기테스트 등에 대한 평가이다.
- EMI/EMC(ElectroMagnetic Interference/ ElectroMagnetic Compatibility)
- EMI/EMC는 전자파장애이다. 기술 발전으로 전자파장애 기준이 강화되고 있다.
- 암호모듈의 운용환경에 따라 암호모듈에 대해 직간접적인 물리적 공격을 할 수 있다.
- 해서, 암호모듈에 대해 물리적인 보안 평가를 실시한다.

기출문제 분석

1. 미국의 NIST와 캐나다의 CSE가 공동으로 개발한 평가체계로 암호모듈의 안전성을 검증하는 것은? [2014년 지방 9급]

- ① CMVP ② COBIT ③ CMM ④ ITIL

☞ CMVP(Cryptographic Module Validation Program)

• CMVP는 암호모듈의 안전성 검증 프로그램(미국의 NIST와 캐나다 CSE가 공동 개발

정답 : ①

2. 암호모듈을 KS X ISO/IEC 19790에 따라 검증하고 암호모듈의 안전성을 보증하는 국내 제도는? [2017년 국가 7급]

- ① KCMVP ② TCSEC ③ ITSEC ④ METI

☞ 한국암호모듈검증제도 - KCMVP

• KCMVP는 한국에서 시행되는 암호모듈의 안전성과 구현 적합성을 검증하는 제도이다.

정답 : ①

3. KCMVP에 대한 설명으로 옳은 것은? [2019년 지방 9급]

- ① 보안 기능을 만족하는 신뢰도 인증 기준으로 EAL1부터 EAL7까지의 등급이 있다.
② 암호 알고리즘이 구현된 프로그램 모듈의 안전성과 구현 적합성을 검증하는 제도이다.
③ 개인정보 보호활동을 체계적·지속적으로 수행하기 위한 관리체계의 구축과 이행 여부를 평가한다.
④ 조직의 정보자산을 효과적으로 보호하고 있는지 평가하여 일정 수준 이상의 기업에 인증을 부여한다.

☞ 한국암호모듈검증제도 - KCMVP

• KCMVP는 한국에서 시행되는 암호모듈의 안전성과 구현 적합성을 검증하는 제도이다.
• 검증대상 암호모듈은 소프트웨어, 하드웨어, 펌웨어를 개별 또는 조합으로 구현될 수 있다.
• 보안제품에는 암호모듈검증제도를 통해 검증 받은 암호모듈이 탑재되어야 한다.
• 보안제품 : 매일 암호화 모듈, PKI 제품, SSO 제품, 키보드 암호화 모듈 등

정답 : ②