

정보보호시스템

# 공통평가기준

2009. 9.

행 정 안 전 부

● 행정안전부고시 제2009-52호

국가정보화 기본법 제38조 제1항의 규정에 의하여 정보보호시스템 공통평가기준(행정안전부고시 제2008-26호, 2008. 7. 16)을 다음과 같이 개정·고시합니다.

2009년 9월 1일

행정안전부장관

## 정보보호시스템 공통평가기준

**제1조(목적)** 이 기준은 「국가정보화 기본법」 제38조제1항 및 동법 시행령 제35조의 규정에 의하여 정보보호시스템을 평가하기 위한 요구 사항을 정함을 목적으로 한다.

**제2조(적용 범위)** 이 기준은 「국가정보화 기본법」 제38조제1항 및 동법 시행령 제35조에서 규정한 정보보호시스템을 평가하는 데 적용한다.

**제3조(용어 정의)** 이 기준에서 사용하는 용어의 정의는 다음과 같다.

1. 삭제
2. 삭제
3. 삭제
4. 삭제
5. 삭제
6. 삭제

7. “엘리먼트”라 함은 컴포넌트를 구성하는 분할할 수 없는 보안요구 사항의 최소 단위를 말한다.

8. “컴포넌트”라 함은 보호프로파일, 보안목표명세서에 포함될 수 있는 보안요구사항의 가장 작은 선택 단위로서 엘리먼트의 모음을 말한다.
9. “패밀리”라 함은 같은 보안목적은 가지지만 강조점이나 엄격함이 서로 다른 컴포넌트의 모음을 말한다.
10. “클래스”라 함은 같은 보안목적은 가지는 패밀리의 모음을 말한다.
11. “보호프로파일”이라 함은 평가대상 범주를 위한 특정 소비자의 요구에 부합하는 구현에 독립적인 보안요구사항의 집합을 말한다.
12. “보안목표명세서”라 함은 식별된 평가대상의 평가를 위한 근거로 사용되는 보안요구사항과 구현 명세의 집합을 말한다.
13. “평가보증등급”이라 함은 공통평가기준에서 미리 정의된 보증수준을 가지는 보증 컴포넌트로 이루어진 패키지를 말한다.

**제4조(평가기준 구조)** 공통평가기준은 별첨과 같이 총 3부로 구성된다.

1. 1부는 정보보호시스템 보안성 평가의 원칙과 일반개념을 정의하고 평가의 일반적인 모델을 설명하는 소개부분으로, IT 보안목적을 표현하고 IT 보안요구사항을 선택·정의하며, 제품 및 시스템의 상위수준 명세를 작성하기 위한 구조를 소개한다.
2. 2부는 보안기능요구사항을 표준화된 방법으로 표현한 것으로 기능 컴포넌트들의 집합으로 구성되며, 기능 클래스, 기능 패밀리, 기능 컴포넌트로 분류된다.
3. 3부는 보증요구사항을 표준화된 방법으로 표현한 것으로 보증 컴포넌트들의 집합으로 구성되고, 보증 클래스, 보증 패밀리, 보증 컴포넌트로 분류되며, 보호프로파일 및 보안목표명세서에 대한 평가 기준을 정의한다.

**제5조(평가보증등급)** ① 정보보호제품의 보증수준을 정하기 위한 공통평가기준에서 미리 정의된 보증등급으로, EAL1, EAL2, EAL3, EAL4, EAL5, EAL6, EAL7의 7개의 등급으로 구분된다. EAL1은 최저의 평가보증등급이고, EAL7은 최고의 평가보증등급이다.

②기존의 평가보증등급에 포함되지 않은 보증 컴포넌트나 계층적으로 더 높은 다른 보증 컴포넌트를 포함하여 제1항에 명시된 평가보증 등급 외의 등급을 생성할 수 있다.

## 부 칙

이 기준은 고시한 날부터 시행한다.

**[별 첨]**

1. 정보보호시스템 공통평가기준 제1부, 제2부, 제3부(한글판)
2. 정보보호시스템 공통평가기준 제1부, 제2부, 제3부(영문판)