「정보보호시스템 평가·인증 지침」(고시) 일부개정

1. 개정이유

○ 인증기관 변경으로 인한 소관 기관 명칭 변경

2. 주요내용

○ 인증기관 변경으로 인한 소관 기관 명칭 변경

- 국가정보원 → 한국전자통신연구원 부설 국가보안기술연구소

3. 참고사항

가. 관련법령 : 생략

나. 예산조치 : 별도조치 필요 없음

다. 합의 : 해당사항 없음

라. 기타 조치사항 : 해당사항 없음

미래창조과학부고시 제2016-73호

「국가정보화기본법」 제38조 및 동법 시행령 제35조 규정에 따른 「정보보호시스템 평가·인증 지침(미래창조과학부고시 제2013-52호)」 일부를 개정하고, 다음과 같이 고시합니다.

2016년 6월 27일

미래창조과학부장관

정보보호시스템 평가·인증 지침

제1장 총 칙

1.1 목적

1이 지침은 「국가정보화기본법」 제38조 및 동법 시행령 제35조 규정에 의하여 미래창조과학부장관이 고시하는 「정보보호시스템 공통평가기준」에 따라 정보보호시스템 또는 보호프로파일의 평가 및 인증업무를 수행하는데 필요한 사항을 규정한다.

1.2 평가인증 원칙

2평가기관 및 인증기관은 평가의 신뢰성을 보장하기 위하여 평가
인증 수행과정에서 다음 각 호의 사항을 준수하여야 한다.

1. 평가대상 정보보호시스템, 보호프로파일, 그리고 평가신청인(이하 “신청인”이라 한다)에 대한 편견과 선입관을 배제하고 공정한 평가인증 수행
2. 주관적인 견해를 배제하여 객관적인 평가인증 수행

1.3 용어 정의

3“공통평가기준”이라 함은 미래창조과학부장관이 고시한 「정보보호시스템 공통평가기준」을 말한다.

4“평가대상”이라 함은 “정보보호시스템”과 “보호프로파일”을 말한다.

5“정보보호시스템”이라 함은 정보의 수집저장검색송신수신 중에 정보의 훼손 변조유출 등을 방지하기 위한 기술적 수단을 총칭한다.

6“보호프로파일”이라 함은 정보보호시스템이 사용될 환경에서 필요한 보안기능 및 보증 요구사항을 공통평가기준에 근거하여 서술한 문서를 말한다.

7“신청인”이라 함은 평가제출물(이하 “제출물”이라 한다)을 평가기관에 평가 신청한 자를 말한다.

8“평가기관”이라 함은 평가업무를 담당하는 기관을 말한다.

9“평가”라 함은 신청인이 제출한 정보보호시스템 또는 보호프로파일이 공통평가기준에 부합하는지 여부를 평가기관이 확인하는 것을 말한다.

10“재평가”라 함은 인증서를 교부받은 인증제품이 보안기능의 향상, 추가 등으로 버전이 변경된 경우에 신청인이 의뢰하는 평가를 말한다.

11“국가기반전략사업”이라 함은 전자여권전자주민증, 전자정부 전략사업 등 IT기반 구축 및 서비스 제고를 위하여 국가가 전략적으로 추진하는 사업을 말한다.

12“인증기관”이라 함은 인증업무를 담당하는 기관을 말한다.

13“인증”이라 함은 평가기관이 수행한 정보보호시스템 또는 보호프로파일의 평가결과를 인증기관이 승인하는 것을 말한다.

14“제출물”이라 함은 신청인이 정보보호시스템을 평가받기 위하여 평가기관에 제출하는 제품 및 모든 문서를 말한다.

15“평가제품”이라 함은 신청인이 평가신청한 후 인증서를 교부받기 전까지의 제품을 말한다.

16“인증제품”이라 함은 인증서를 교부받은 제품을 말한다.

17“평가보고서”라 함은 평가기관의 장이 정보보호시스템 또는 보호프로파일의 평가결과에 관하여 인증기관의 장에게 제출하는 문서를 말한다.

18“인증보고서”라 함은 인증기관이 인증결과를 요약한 문서를 말한다.

1.4 적용 범위

19이 지침은 신청인이 의뢰한 정보보호시스템 또는 보호프로파일을 평가 및 인증하는데 필요한 다음의 업무에 적용된다.

1. 평가인증업무 수행
2. 평가인증 관련 기관간의 역할 및 책임
3. 인증제품의 사후관리

제 2 장 평가인증체계

2.1 개요

20이 장에서는 정보보호시스템 또는 보호프로파일의 평가인증과 관련된 기관의 역할과 상호 관계를 명시한다.

2.2 관련 기관

21관련 기관은 역할과 책임에 따라 인증기관, 평가기관, 신청인으로 구분한다.

2.2.1 인증기관

22인증기관은 **한국전자통신연구원 부설 국가보안기술연구소**로 하며, 다음 각 호의 업무를 수행한다.

1. 평가기관의 평가업무 감독
2. 인증보고서 작성 및 인증서 발급
3. 신청인과 평가기관간의 분쟁조정
4. 인증제품 소개책자 발간
5. 국제상호인정협정 관련 정책결정
6. 인증제품에 대한 사후관리
7. 인증업무 수행에 관한 규정수립 및 시행
8. 인증받은 보호프로파일 등록 및 관리
9. 관계 국제협약에서 정한 기준에 맞는 기관을 평가기관으로 승인하는 업무

23인증기관의 책임은 다음 각 호와 같다.

1. 인증 원칙 및 절차 준수
2. 인증업무 수행규정 준수

2.2.2 평가기관

24평가기관은 한국인터넷진흥원과 인증기관으로부터 승인받은 기관으로 한다.

1. 삭제
2. 삭제
3. 삭제
4. 삭제
5. 삭제

24의2 한국인터넷진흥원은 다음 각 호의 업무를 수행한다.

1. 정보보호시스템의 평가시행
2. 공통평가기준, 평가지침서, 공통평가기준해설서 개발 및 발간
3. 미래창조과학부장관으로부터 위임받은 평가관련 기술개발방법론 및 간행물 발간
4. 국제상호인정협정 관련 연구 및 활동
5. 평가업무 수행에 관한 자체 규정수립 및 시행
6. 정보보호시스템 공통평가기준 제5조제1항에 따른 EAL1 내지 EAL7의 7개 등급의 평가
7. 국가기반전략사업의 정보보호시스템 평가

24의3 인증기관으로부터 승인받은 평가기관은 다음 각 호의 업무를 수행한다.

1. 정보보호시스템의 평가시행
2. 평가업무 수행에 관한 자체 규정수립 및 시행
3. 국제상호인정협정에 따라 인증기관이 부여한 등급의 평가

25평가기관의 책임은 다음 각 호와 같다.

1. 평가 원칙 및 절차 준수
2. 평가업무 수행규정 준수

2.2.3 신청인

26신청인의 의무는 다음 각 호와 같다.

1. 평가인증에 필요한 제출물 작성 및 제출
2. 정보보호시스템 평가수수료 납부
3. 삭제
4. 평가인증에 필요한 평가환경 제공 및 추가자료 제출
5. 평가제출물에 대한 법적 권리확보 및 평가기관과 인증기관의 사용 보장
6. 평가인증 결과에 대한 허위사실 관련 유포 및 홍보행위 등의 금지
7. 인증서를 교부받은 신청인은 인증제품의 평가등급 유지

제 3 장 평가 절차

3.1 개요

27이 장에서는 (그림 1)의 절차도에서 평가신청을 위한 준비단계부터 평가보고서 작성까지의 평가수행 과정의 주요절차를 명시한다. 또한 평가기관이 정보보호시스템의 평가를 수행하는데 필요한 세부 활동 사항을 명시한다.

3.2 평가신청 준비

28평가기관의 장은 신청인의 요청이 있는 경우 평가등급에 영향을 미치지 않는 범위 내에서 평가신청 준비에 필요한 도움을 줄 수 있다.

3.3 평가신청 및 평가계약 체결

29정보보호시스템을 평가받고자 하는 신청인은 별지 제1호 또는 제1-1호서

식의 평가신청서와 제출물을 구비하여 평가기관의 장에게 평가신청을 하여야 한다.

30동일한 정보보호시스템을 2인 이상의 신청인이 평가를 받고자하는 경우에는 그중 1인을 대표신청인으로 선정하고, 다른 신청인은 별지 제2호서식의 공동신청인명부에 연서하여 공동으로 평가를 신청할 수 있다.

31신청인이 평가제품과 함께 제출하여야 하는 문서는 한글 또는 영어로 작성되어야 한다.

32삭제

33평가기관은 신청인으로부터 평가신청을 접수한 경우에는 평가신청접수증을 발급하여야 한다.
33의2평가기관의 장은 제출물의 내용에 미비점이 발견될 경우에는 신청인에게 보완을 요청할 수 있으며, 신청인이 이를 이행하지 않을 경우에는 인증기관과 협의를 거쳐 평가신청접수증을 발급하지 아니할 수 있다.

34평가기관의 장은 평가신청접수증 발급 후 상호 협의하여 신청인과 평가계약을 체결한다.

35평가기관 및 인증기관의 장은 제출물을 평가인증업무 이외의 목적으로 외부에 유출하거나 공개하여서는 안되며, 평가인증 수행규정에 따라 관리하여야 한다.

36평가기관의 장은 평가계약이 체결된 후 평가계약내용 및 제출물 1부를 인증기관의 장에게 제출한다.

3.4 평가

3.4.1 평가반 구성

37평가기관의 장은 평가계약에 따라 평가를 실시한다. 다만, 시급을 요하는 국가기반전략사업인 경우에는 우선평가를 실시할 수 있다.

38평가기관의 장은 평가수행을 위한 평가반을 구성한 후 평가수행계획서를 인증기관의 장에게 제출한다.

3.4.2 제출물 설명회

39평가기관의 장은 제출물에 대한 평가반의 이해를 도모하기 위하여 신청인에게 제출물에 대한 설명을 요청할 수 있다

3.4.3 개발환경 보안점검

40평가기관의 장은 평가제품 개발환경의 보안점검을 위해 필요할 경우 개발업체를 방문하여 실사를 수행할 수 있으며, 이 때 발생되는 제반 비용은 신청인이 부담한다.

41신청인은 제40항의 개발환경 보안점검 결과에서 지적된 미비점을 보완하여야 한다.

3.4.4 평가수행

42평가기관의 장은 평가제품이 공통평가기준에 명시된 요구수준을 만족하는지 여부를 평가한다.

43평가기관의 장은 평가과정에서 제출물이 미비하여 평가수행이 불가능한 경

우에는 일정 기한을 정하여 신청인에게 제출물 보완을 요청할 수 있다.

44평가기관의 장은 원활한 평가진행을 위하여 신청인에게 평가환경의 지원을 요청할 수 있다.

45평가기관의 장은 평가를 원활히 수행하기 위해 필요할 경우 외부 전문가를 활용할 수 있다.

3.4.5 평가 중단

46평가기관의 장은 신청인과 체결한 평가계약서에 명시된 평가중단 사유가 발생하는 경우 평가기관 내부 규정에 따라 평가를 중단할 수 있다.

1. 삭제
2. 삭제

47평가기관의 장은 평가를 중단하고자 하는 경우 그 사유를 신청인과 인증기관의 장에게 문서로 통보하고 일정 기한을 정하여 평가를 계속 진행시키기 위한 조치를 요청할 수 있다.

48평가기관의 장은 신청인이 제47항에 의한 조치를 취하지 아니하는 경우 평가를 중단하고 평가계약을 해지한다.

3.4.6 평가종료 및 평가보고서 작성

49평가기관의 장은 평가가 종료된 경우 평가보고서 및 최종제출물을 인증기관의 장에게 제출한다.

49의2평가기관의 장은 신청인이 평가보고서의 열람 및 제공을 요구할 경우

이를 허용하여야 한다.

50평가보고서에 포함되어야 하는 내용은 다음과 같다.

1. 평가보고서 개요
2. 평가제품의 기본 구조 및 운영환경
3. 평가제품의 평가내용 및 결과
4. 결론 및 권고사항

제 4 장 인증절차

4.1 개요

51이 장에서는 (그림 1)의 절차도에서 평가단계부터 인증서 교부까지의 인증 수행 과정의 주요절차를 명시한다.

4.2 인증

52인증기관의 장은 제49항에 의하여 평가기관의 장이 제출한 최종제출물 및 평가보고서를 검토하여 보완사항이 있을 경우 평가기관의 장에게 보완을 요청하고 평가기관의 장은 이에 대한 적절한 조치를 취하여야 한다.

53인증기관의 장은 평가기관의 장이 수행한 평가과정이 공정하고 객관적인지 여부를 확인한다.

54인증기관의 장은 평가내용의 적절성과 평가결과가 평가등급의 요구사항에 적합한지 여부를 확인한다. 다만, 평가내용 및 과정이 부적합하다고 판단되는 경우에는 평가기관의 장에게 보완을 요청할 수 있다.

55인증기관의 장은 필요시 평가기관의 장에게 평가내용 및 평가결과에 대하

여 구체적인 설명을 요청할 수 있다.

4.3 인증위원회

56인증기관의 장은 평가결과의 타당성공정성에 대한 심의의결 및 신청인과 평가기관간의 분쟁 조정 등을 위하여 인증위원회(이하 “위원회” 라 한다)를 구성운영할 수 있다.

57위원회는 인증기관, 평가기관, 관계기관, 학계 및 연구기관 등의 전문가 12인 이내로 구성하며, 위원 및 위원장은 인증기관의 장이 위촉한다.

58위원회는 재적위원 과반수 출석으로 개최하고 출석위원 전원의 찬성으로 의결한다.

59삭제

60긴급한 사유 등으로 인해 위원회를 개최할 수 없거나 의결안건이 경미하다고 위원장이 판단할 경우 서면으로 심의의결할 수 있다.

61위원회는 평가결과가 부적합하다고 심의한 경우에는 부적합 판정을 내릴 수 있다.

62위원은 위원회 활동 과정에서 알게 된 사항을 외부에 유출하거나 공개하지 못한다.

63이 지침에서 정한 것 이외에 위원회의 구성 및 운영 등에 관하여 필요한 사항은 인증기관의 장이 별도로 정하여 운영한다.

4.4 인증종료

64인증보고서에 포함되어야 하는 내용은 다음과 같다.

1. 인증보고서 개요
2. 공통평가기준에 의한 주요 평가 내용
3. 인증결과

65인증기관의 장은 인증보고서를 홈페이지 등에 공개하여야 한다.

66인증기관의 장은 위원회의 심의 결과에 따라 부적합 등급을 부여하거나 해당 공통평가기준에 따른 평가등급을 부여할 수 있다.

67인증기관의 장은 위원회가 심의한 결과를 평가기관의 장 및 신청인에게 통보한다.

4.5 인증제품 소개책자

68인증기관의 장은 정보보호시스템 인증제품 소개책자에 다음 사항을 등재하여 관리한다.

1. 인증제품에 대한 설명, 제품명, 제품분류
2. 인증서 인증번호, 발급번호, 발급일
3. 평가등급
4. 제조자, 원산지, 신청인 연락처
5. 공통평가기준 및 버전번호
6. 보호프로파일을 준수한 경우 해당 보호프로파일명

69인증기관의 장은 정기적으로 인증제품 소개책자를 발간하여 배포할 수 있다.

4.6 인증서

70인증기관의 장은 위원회의 심의결과에 따라 별지 제3호 또는 제3-1호서식의 인증서를 발급한다.

71인증서를 교부받은 신청인은 별표 2의 정보보호시스템 인증마크를 사용하고자 할 경우 별지 제4호서식의 인증마크 사용신청서를 인증기관의 장에게 제출하여야 한다.

72삭제

제 5 장 평가인증 사후관리

5.1 제출물 처리

73평가기관의 장은 평가계약 해지 및 인증이 완료된 경우에는 제출물을 신청인에게 반환하여야 하며, 반환이 불가능한 경우에는 폐기하여야 한다.

73의2인증기관의 장은 평가과정에서 평가계약이 해지되거나, 인증을 완료한 경우 제출물을 신청인에게 반환하고, 반환이 불가능한 경우 이를 폐기하여야 한다.

7473의2 규정에도 불구하고 업무상 계속 제출물(원시프로그램 및 하드웨어 설계서는 제외)을 보관할 필요가 있을 경우에는 신청인과 협의하여 5년간 보관할 수 있다.

5.2 인증효력 유지

75인증기관의 장은 인증제품을 표본 추출하여 인증제품 소개책자에 등재된 내용과 동일한지 여부를 확인할 수 있다.

76인증기관의 장은 인증제품에 새로운 취약점이 발견되는 등 평가등급을 유지할 수 없는 경우 인증서를 교부받은 신청인에게 필요한 조치를 요청할 수 있다.

77인증기관의 장은 다음의 경우에 대하여 인증제품의 인증을 취소하고 그 사유를 해당 신청인에게 통보한다.

1. 사위(詐僞) 또는 기타 부정한 방법으로 평가인증을 받은 경우
2. 제71항에 의하지 않고 인증마크를 사용하는 경우
3. 제75항의 결과가 인증제품 소개책자의 내용과 동일하지 않을 경우
4. 신청인이 정당한 사유 없이 제76항의 규정에 의하여 요청받은 조치를 이행하지 않는 경우
5. 삭제

78인증기관의 장은 인증제품의 인증이 취소된 경우에는 해당 인증제품을 인증제품 소개책자에서 삭제하고 이를 공고한다.

79신청인은 인증이 취소되는 경우 지체 없이 인증서를 인증기관의 장에게 반납하여야 한다.

80삭제

81신청인은 다음 각 호의 경우 별지 제5호서식의 인증효력유지 신청서를 작성하여 인증기관의 장에게 제출할 수 있다.

1. 인증제품의 보안기능 및 운영환경의 변경이 필요한 경우
2. 인증제품에 새로운 취약점이 발견되어 수정보완해야 되는 경우
3. 인증제품이 다른 계열의 운영체제에 적용될 경우
4. 삭제
5. 기타 인증제품의 형상변경이 필요한 경우

82인증기관의 장은 제81항의 변경 내용을 검토하여 변경승인, 재평가를 결정하여 그 결과를 신청인에게 통보한다.

83제82항에서 변경승인된 경우에는 인증의 효력이 그대로 유지된다.

84신청인은 인증기관의 장의 결정에 따라 재평가를 평가기관의 장에게 신청할 수 있다.

85평가기관의 장은 재평가시 이전에 제출한 대체 가능한 제출물에 대해서는 그 일부를 면제할 수 있다.

86삭제

87삭제

88삭제

제 6 장 보호프로파일 평가인증절차

6.1 보호프로파일 평가

89보호프로파일의 평가를 받고자 하는 신청인은 별지 제1호서식의 평가신청서와 보호프로파일을 구비하여 평가기관의 장에게 평가신청을 하여야 한다.

90보호프로파일의 평가는 정보보호시스템의 평가절차를 준용한다. 다만, 보호프로파일의 경우에는 개발환경 보안점검을 시행하지 않는다.

6.2 보호프로파일 평가보고서 작성

91평가기관의 장은 평가가 종료된 경우 보호프로파일 평가보고서를 작성하여

인증기관의 장에게 제출한다.

92보호프로파일의 평가결과에 대한 평가보고서에 포함되어야 하는 내용은 다음과 같다.

1. 평가보고서 개요
2. 공통평가기준의 평가항목별 평가내용 및 결과
3. 평가기관 권고사항

6.3 보호프로파일 인증

93인증기관의 장은 평가기관의 장이 수행한 보호프로파일의 평가 과정이 객관적이며, 공통평가기준에 적합하게 수행되었음을 인증하는 경우 다음 사항을 정보보호시스템 인증제품 소개책자에 등재하여 관리한다.

1. 보호프로파일에 대한 설명, 보호프로파일명
2. 인증번호, 인증일
3. 개발자 또는 작성자
4. 공통평가기준 버전

94인증기관의 장은 위원회의 심의결과에 따라 별지 제3-2호서식의 보호프로파일 인증서를 발급한다.

제 7 장 평가수수료

7.1 평가수수료 산정

95평가기관이 국가정보화기본법 시행령 제35조제3항에 따라 수수료를 산정할 때에는 직접인건비, 직접경비, 제경비 및 기술료로 구분하여야 하며 직접경비, 제경비, 기술료는 엔지니어링기술진흥법 제10조의 「엔지니어링 사업대가의 기준」을 적용하여야 한다. 다만, 직접인건비는 소프트웨어산업진흥법 시

행령 제16조에 의한 「소프트웨어기술자 등급별 노임단가」를 준용 할 수 있다.

96평가기관은 「중소기업기본법」 제2조에 따른 중소기업이 평가를 신청하는 경우에 예산의 범위 안에서 수수료 감면 등 필요한 지원을 할 수 있다.

7.2 평가수수료 공지

97평가기관은 7.1에 따라 산정된 수수료를 공지하여야 한다.

부칙 <제2009-51호, 2009.9.1>

제1조(시행일) 이 지침은 고시한 날부터 시행한다.

제2조(경과조치) ①이 지침의 시행 전에 평가계약이 체결된 평가제품은 평가신청서에 명시된 평가기준을 적용한다.

②이 지침 시행 전의 인증제품에 대해서는 다음 각 호를 적용한다.

1. 신청인은 기존 인증서의 유효기간이 만료된 경우, 이를 연장하기 위해서는 재평가를 신청해야 한다.
2. 「정보통신망 침입차단시스템 평가기준」 또는 「정보통신망 침입탐지시스템 평가기준」(이하 “K기준”이라 한다)에 따른 인증제품의 경우, 신청인은 재평가에 한해 적용할 평가기준을 공통평가기준 또는 K기준 중에서 선택할 수 있다.
3. K기준이 적용된 재평가를 통해 발급된 인증서의 유효기간은 3년으로 한다. 이 경우 최장 2008년 12월 31일을 초과하지 못한다.

제3조(재검토기한) 「훈령·예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제248호)에 따라 이 고시 발령 후의 법령이나 현실여건의 변화 등을 검토하여 이 고시의 폐지, 개정 등의 조치를 하여야 하는 기한은 2012년 8월 31일까지로 한다.

부칙 <제2013-52호, 2013.8.8>

제1조(시행일) 이 지침은 고시한 날부터 시행한다.

제2조(재검토기한) 「훈령·예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제248호)에 따라 이 고시 발령 후의 법령이나 현실여건의 변화 등을 검토하여 이 고시의 폐지, 개정 등의 조치를 하여야 하는 기한은 2016년 3월 23일까지로 한다.

부칙 <제2016-73호, 2016.6.27>

제1조(시행일) 이 지침은 고시한 날부터 시행한다.

제2조(재검토기한) 「훈령·예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제334호)에 따라 이 고시 발령 후의 법령이나 현실여건의 변화 등을 검토하여 이 고시의 폐지, 개정 등의 조치를 하여야 하는 기한은 2019년 6월 26일까지로 한다.