KOLAS-SR-010 : 2020

정보보호시스템 시험기관 인정을 위한 추가기술요건

한국인정기구

Korea Laboratory Accreditation Scheme

Korean Agency for Technology and Standards, MOTIE, Korea

1. 서론

1.1 이 문서는 정보보호시스템 평가를 수행하는 시험기관을 인정하기 위하여 준수되어야 할 특별 요건을 기술한 것이다.

1.2 정보보호시스템 KOLAS 공인시험기관(이하 “공인시험기관”이라 칭한다.) 인정은 정보기술(Information Technology : IT) 제품 및 시스템 보안성 평가에 대한 국제규격적합성에 반드시 부합되어야 한다는 점에서 출발하였으며, 정보보호시스템에 대한 적합성을 평가하는 공인시험기관을 인정하기 위하여 본 추가기술 요건을 개발하였다.

1.3 이 문서는 KS Q ISO/IEC 17025:2017 및 KOLAS가 발행한 기술문서 시리즈와 함께 검토되어야 한다.

2. 적용범위

2.1 이 문서는 정보보호시스템 보안성 평가를 위한 공인시험기관 인정을 희망하는 사업자 (이하"신청사업자"라 칭한다.) 및 정보보호시스템 보안성 평가의 공인시험기관 인정을 받은 사업자에 적용한다.

3. 인용규격

3.1 이 문서는 다음에 열거하는 규격을 인용하며 개정 내용을 포함하는 최신 버전이 적용된다.

(1) KS Q ISO/IEC 17025:2017 시험 및 교정기관의 적격성에 대한 일반요구사항
(2) ISO/IEC 15408 IT 보안성 평가기준
(3) ISO/IEC 18045 IT 보안성 평가방법론
(4) 정보보호시스템 평가・인증지침 (행정안전부 고시)
(5) 정보보호제품 평가인증 수행규정 (국가정보원 고시)

4. 정의

4.1 IT 보안성 평가기준 : 이 문서에 있어 “IT 보안성 평가기준”이라 함은, IT 제품 및 시스템, 보호프로파일 등의 보안성 평가에 이용되는 평가기준으로서 다음에 열거하는 것을 말한다.(이하 “평가기준” 또는 “CC”라 칭한다.)

(1) [ISO/IEC 15408] Information technology - Security techniques - Evaluation criteria for IT security
(2) Common Criteria for Information Technology Security Evaluation

4.2 IT 보안성 평가방법론 : 이 문서에 있어 “IT 보안성 평가방법”이라 함은, IT 제품 및 시스템, 보호프로파일 등의 보안성 평가에 사용되는 평가방법으로서 다음에 열거하는 것을 말한다.(이하 “평가방법론” 또는 “CEM(Common Evaluation Methodology)"이라 칭한다.)

(1) ISO/IEC 18045 Information technology - Security techniques - Methodology for IT Security Evaluation
(2) Common Methodology for Information Technology Security Evaluation

4.3 보증등급패키지 : 평가기준에서 미리 정의된 보증수준(Evaluation Assurance Level, EAL)을 나타내는 보증 요구사항들의 집합

4.4 합성보증패키지 : 평가기준에 따라 성공적으로 평가된 두 개 이상의 IT 실체를 더 이상의 개발과정 없이 결합시킨 제품에 대한 보증수준(Composed Assurance Package, CAP)을 나타내는 보증 요구사항들의 집합

4.5 품질매뉴얼 : KS Q ISO/IEC 17025:2017, 기타 내부 규정을 준수하여 공인시험기관의 경영 요구사항과 기술 요구사항을 기술한 운영문서

4.6 선임평가자 : 국가정보원 IT보안인증사무국이 제정한 「정보보호제품 평가인증 수행규정」의 평가자 자격부여 요건을 충족시키는 자

4.7 주임평가자 : 국가정보원 IT보안인증사무국이 제정한 「정보보호제품 평가인증 수행규정」의 평가자 자격부여 요건을 충족시키는 자

4.8 수습평가자 : 국가정보원 IT보안인증사무국이 제정한 「정보보호제품 평가인증 수행규정」의 평가자 자격부여 요건을 충족시키는 자

4.9 인증기관 : 정보보호시스템 공인시험기관이 수행한 평가 결과를 바탕으로 적정성 및 공정성 여부 등을 확인한 후 인증서를 발급하는 기관

4.10 앞에 열거한 것을 제외한 용어의 정의는 3.1 인용규격 문서에 해당되는 정의를 적용한다.

5. KS Q ISO/IEC 17025:2017에 근거한 일반요구사항

5.1 신청사업자 및 공인시험기관에 대하여 KS Q ISO/IEC 17025:2017의 해당되는 항목에 대하여 IT 보안성 평가의 인정을 취득하기 위한 일반요구사항으로서 적용한다.

5.2 이 문서의 6부터 22까지 열거한 규정을 5.1의 규정에 근거한 일반요구사항의 적용방침으로서 적용한다.

6. 인정범위

6.1 신청사업자 및 공인시험기관 평가역량의 기본적인 인정범위는 다음과 같다.

(1) 보호프로파일 평가(APE 클래스)
(2) EAL4 이하 보증등급패키지
(3) 결함 교정(ALC_FLR 패밀리)
(4) CAP-C 이하 합성보증패키지

6.2 신청사업자 및 공인시험기관은 6.1항 평가역량의 인정범위에 EAL5 보증등급패키지를 추가할 수 있다.

6.3 신청사업자 및 공인시험기관은 6.1의 인정범위에 관하여 KS Q ISO/IEC 17025:2017에 따라 수립한 문서(품질매뉴얼 등)로 평가업무를 명확히 정의하여야 하고, 해당 품질경영시스템은 공인시험기관으로 인정받고자 하는 평가수행범위를 충족하는 정보보호시스템에 적용한 이행 실적을 갖추고 적용결과는 내부심사와 경영검토를 통해 적절함을 입증할 수 있어야 한다.

6.4 공인시험기관은 인정범위에 포함되는 평가가능 보증컴포넌트(별표 참조) 외 정형기법이나 고도의 취약성 분석 등 추가적인 보증컴포넌트에 대해 평가를 수행하고자 할 경우, 해당 컴포넌트에 대해 별도 인정을 득하여야 한다.

7. 직원의 자격

7.1 신청사업자 및 공인시험기관 기술책임자의 적격성

(1) 기술책임자는 평가업무의 기술적 사항에 있어 모든 책임을 진다.
(2) 기술책임자는 평가업무에 관련하여 충분한 기술적 지식을 보유하며 정확한 평가결과를 도출할 수 있는 능력을 보유하여야 한다.
(3) 기술책임자는 아래에 열거한 지식, 시험요원(평가자)의 교육·훈련 및 적절한 감독·지시를 수행할 수 있는 능력을 보유하여야 한다.
  ① 평가보고서 등의 작성을 포함한 평가업무
  ② CC에 관련된 지식
  ③ CEM에 관련된 지식
(4) 기술책임자는 선임평가자 자격을 가진 자로서 정보통신분야 공인시험기관이나 정보보호 관련 업체에서 평가 또는 개발 유관업무에 4년 이상의 경험을 가진 자여야 한다.

7.2 신청사업자 및 공인시험기관의 시험요원(평가자)의 적격성 및 자격

(1) 시험요원(평가자)은 평가업무에 관련된 내부자격을 보유하고 있어야 한다.
(2) 시험요원(평가자)은 7.1의 (3)에 규정된 지식을 보유하고 있으며, 내부자격기준은 적절함을 요한다.

7.3 신청사업자 및 공인시험기관의 인력 보유요건

(1) 신청사업자 및 공인시험기관은 기술책임자 1인을 포함한 선임평가자 3인 이상, 주임평가자 2인 이상의 시험요원(평가자)을 확보하여야 한다.

8. 교육 훈련

8.1 신청사업자 및 공인시험기관의 경영자는 기술책임자 및 시험요원(평가자)을 포함한 요원에 대한 교육·훈련을 제공하기 위한 방침 및 절차를 준비하여야 한다. 해당 교육·훈련프로그램은 신청사업자 및 공인시험기관의 업무에 대하여 적합성을 보장하여야 한다.

8.2 8.1의 교육·훈련프로그램은 7.1의 (3)에 집중하여 이루어져야 한다. 또한, 평가업무에 필요한 경우에는 전산분야 전문지식 등 업무와 관련된 교육·훈련프로그램을 수행하여야 한다. 교육·훈련은 적합한 평가를 계속하여 수행하고 최신기술에 대응할 수 있도록 기술책임자 및 시험요원(평가자)에 대하여 정기적이고 계획적으로 이루어져야한다.

9. 시설 및 환경조건

9.1 시설의 기밀보호 및 소유권보호

(1) 신청사업자 및 공인시험기관은 시설에 대하여 정보보호제품 등의 평가를 의뢰한 기관, 업체 또는 개인(이하 “신청기관”이라 칭한다.)의 기밀보호 및 소유권보호를 확실히 담보하기 위한 방침 및 절차를 보유하여야

한다. 특히 평가가 이루어지는 시설(이하 “평가시험실”이라 칭한다.), 평가 중 습득한 기밀정보를 보관하는 시설, 해당정보를 전송하는 도구(FAX, 이메일 등)의 기밀보호 및 소유권보호를 확실히 보장하기 위한 방침 및 절차를 보유하여야 한다.

(2) 신청사업자 및 공인시험기관은 평가시험실에 대한 접근을 기밀보호 및 소유권보호의 관점에서 평가작업에 필요한 최소한의 권한으로 제한하여야 한다.

(3) 평가에 관계된 기밀정보를 보관하는 시설에 관련된 방침 및 절차에는 아래의 항목을 포함하는 것이 바람직하나, 이를 강제하지는 않는다.

① 평가에 관련된 기밀정보는 신청기관에서 시험하는 경우, 인증기관과의 연락사항 등 업무에 요구되는 경우를 제외하고는 외부로 가지고 나올 수 없다.

② 평가에 관련된 기밀정보 중 불필요해진 정보는 신청기관에게 확실히 반납하거나 복원불가능한 상태로 폐기・소거하여야 한다.

예) 복원불가능한 상태로 폐기・소거의 예로써 종이류의 경우 절단기, 용해처리기를 통한 용해, 전자기기의 경우 해당기기의 초기화, 물리적 파괴 등이 있다.

(4) 신청사업자 및 공인시험기관은 평가에 관련된 기밀정보를 전송하는 도구가 속해 있는 시설에서 송수신을 할 경우 송신측, 수신측을 포함한 해당 도구의 전송경로의 기밀보호를 확실히 하여야 한다.

예1) 평가에 관련된 기밀정보를 이메일로 송수신하는 경우, 기밀정보는 해당메일의 본문에는 포함시키지 않고, 첨부파일에 첨부하여 비밀번호를 설정하는 방법이 있다. 또한, 전송경로에서 기밀정보의 보호가 확실하다고 판단되지 않을 때에는 기밀정보의 보호를 위한 수단을 강구하여야 한다.

예2) 부득이하게 팩스를 이용하여 기밀정보를 전송하는 경우 기밀보호의 수단으로써 송신 전에 미리 수신자에게 연락하여 팩스기기 앞에 대기하도록 하는 등의 방법이 있다.

(5) 신청사업자 및 공인시험기관은 신청기관의 기밀정보 및 소유권보호에 관련된 윤리규정을 정비하여야 한다.

(6) 신청사업자 및 공인시험기관은 소유권보호 시스템을 보유하고 있어야

한다. 이 시스템은 신청기관 등이 소유권을 가지고 있는 하드웨어, 소프트웨어, 평가 관련 데이터, 문서 기록 및 기타의 자료를 보호하기에 충분한 기능을 가져야 한다.

(7) (6)의 소유권보호 시스템은 신청사업자 및 공인시험기관의 외부직원, 방문자, 평가 정보를 접할 필요가 없는 관계 직원 및 권한이 없는 자로부터 소유권이 있는 자료 및 정보를 보호할 수 있어야 한다. IT 보안성 평가를 위하여 사용되는 신청사업자 및 공인시험기관의 네트워크는 외부 네트워크와 분리하거나 이와 동등한 수준으로 운영하여야 한다.

(8) 신청사업자 및 공인시험기관은 평가 대상 제품의 전부 또는 일부가 소프트웨어로 구성되어 있는 경우에는 평가 중 소프트웨어 부분이 부주의로 인하여 변경되지 않도록 적절한 형상관리를 하여야 한다.

9.2 평가를 행하는 시설 및 환경의 조건

(1) 신청사업자 및 공인시험기관은 외부에서 평가를 행하는 경우, 그에 따른 환경을 공인시험기관 요구사항과 동등하도록 KS Q ISO/IEC 17025:2017 6.3항의 요구사항을 만족시켜야만 한다.

(2) 신청사업자 및 공인시험기관은 평가 중에 권한이 없는 자로부터 접근할 수 있는 환경에서 평가하는 경우, 접근을 차단할 수 있는 방법으로 평가환경을 통제하여야 한다.

(3) 신청사업자 및 공인시험기관은 복수의 평가대상을 동시에 평가하는 경우, 평가중의 제품, 평가 플랫폼 및 주변시설, 증거서류가 섞이는 것을 방지하기 위하여 서로 다른 신청기관의 제품과 평가를 구별해 주는 시스템을 유지하여야 한다. 단, 제품의 운영환경(운영체제, 하드웨어 사양 등)은 다르나 보안기능이 동일한 정보보호시스템을 각각의 운영환경에서 동시에 평가하는 경우는 예외로 한다.

10. 시험방법

10.1 신청사업자 및 공인시험기관은 시험방법으로 "CC" 및 "CEM"을

이용하여야 한다.

10.2 신청사업자 및 공인시험기관은 "CC" 및 "CEM"에 규정된 평가기준, 평가방법을 보조하기 위하여 인증기관이 기술지침과 기술해석을 발행하는 경우, 해당지침과 해석을 참조하여야 한다. "CC" 및 "CEM"이 원래의 상태로 특정의 IT제품이나 시스템 평가에 사용할 수 없는 경우, 필요에 따라서 "CC" 및 "CEM" 규정과 모순되지 않는 내용으로 문서화된 매뉴얼을 보유하여야 한다.

11. 방법의 선정

11.1 신청사업자 및 공인시험기관은 기술적 이유로 인하여 예외적인 평가방법이 필요하다고 판단되는 경우, 반드시 신청기관에게 통지하고 평가보고서에 상세한 사항을 기술하여야한다. 예외적인 평가방법에는 CC에 규정된 평가항목이외의 평가항목을 추가하여 보안성 평가를 행하는 경우가 있으나 이를 강제하지는 않는다.

11.2 보안성 평가에 적용하기 위하여 인정기관이 발행한 가이드문서, 인증기관이 발행한 가이드문서를 "합의규격"으로 간주한다.

12. 방법의 유효성 확인

12.1 KS Q ISO/IEC 17025:2017 7.2.2.1항 “비고 2”의 각 방법 중 몇 개의 항목은 IT 보안성 평가에 있어 적용하지 않는다.

13. 측정 불확도 추정

13.1 KS Q ISO/IEC 17025:2017 7.6항은 IT 보안성 평가에 있어 적용하지 않는다.

14. 설비의 보유

14.1 신청사업자 및 공인시험기관은 조직이 관리하는 모든 설비에 관련된 기록을 관리·유지하여야 한다. 이 설비에는 신청기관이 준비한 평가에 이용하는 설비를 포함한다.

14.2 신청사업자 및 공인시험기관은 조직이 관리하는 모든 설비의 조작 방법 매뉴얼을 보유하고 있어야 한다.

14.3 앞의 2항에 있어서의 "설비"에는 IT 보안성 평가를 행하기 위한 신청사업자 및 공인시험기관이 사용하는 소프트웨어 평가 도구와 기타 평가용 기계장치가 포함된다. 다만, 시험요원(평가자)이 독자적인 판단을 위해 사용할 뿐 그 결과가 평가보고서에 전혀 반영되지 않는 참고시험과 관련된 것은 설비에 포함되지 않는다.

14.4 신청사업자 및 공인시험기관에서 개발된 테스트 도구가 소프트웨어인 경우에는 해당 소프트웨어에 대해 KS Q ISO/IEC 17025:2017 7.11항을 만족시켜야 한다.

14.5 앞의 3항의 규정은 신청기관이 소유한 설비를 평가에 사용하는 경우에 준용한다. 이 경우에 있어 신청사업자 및 공인시험기관은 신청기관과 계약을 체결하는 것으로 KS Q ISO/IEC 17025:2017 6.4항과의 적합성을 확보함과 동시에 필요한 경우에는 그 설비를 심사의 대상이 될 수 있도록 확보하여야 한다.

15. 설비의 유지

15.1 신청사업자 및 공인시험기관은 IT 보안성 평가를 수행하기 위하여 사용하는 설비를 다음 사항에 따라 유지하여야 한다.

(1) 설비 제조업자의 권고사항
(2) 적용가능한 경우, 신청사업자 및 공인시험기관이 문서화한 매뉴얼

15.2 신청사업자 및 공인시험기관은 해당되는 설비에 대하여 평가대상 제품의 보안기능의 완전성을 훼손하지 않는지 검사하여야 한다.

16. 측정 소급성에 관련된 일반요구사항

16.1 신청사업자 및 공인시험기관은 평가 설비를 "교정"하여야 한다. IT 보안성 평가에 있어서 "교정"은 "정확도의 검증"의 다른 표현이다. 신청사업자 및 공인시험기관은 IT 보안성 평가를 행하기 위한 하드웨어장비 등 정확도를 요구하는 경우에 평가결과를 정확하게 표시하기 위하여 독립적으로 분리하여 정확도를 검증하여야 한다.

17. 측정 소급성에 관련된 특정요구사항

17.1 IT 보안성 평가에 있어서 KS Q ISO/IEC 17025:2017 6.5항은 적용하지 않는다.

17.2 IT 보안성 평가에 있어서 KS Q ISO/IEC 17025:2017 6.5항은 "IT 보안성 평가활동이 CC 및 CEM에서의 “시험요원(평가자) 활동”으로서 규정되어 있는 사항에 소급할 수 있어야 한다."라고 해석한다. 신청사업자 및 공인시험기관은 평가 도구를 사용하여 행하는 평가 및 평가결과가 CC 및 CEM에 소급 가능함을 증명하여야 한다. 또한 소급성은 해당 평가결과가 CC 및 CEM과 합치하고 있는가의 여부를 증명하는 정확한 증거의 일부가 되므로 반드시 필요하다.

18. 참조표준 및 표준물질

18.1 IT 보안성 평가에 있어 KS Q ISO/IEC 17025:2017 6.4.10항은 기본적으로 적용하지 않는다. 다만, 교정이 필요한 평가 도구에 대해서는 교정에 사용되는 참조표준의 교정기록 및 사용된 참조표준의 소급성에 대한 증거가 문서 또는 기록에 의하여 증명되어야 하고, 외부 기관에 교정을 의뢰할 경우 KOLAS 공인교정기관, 한국표준과학연구원,

ILAC-MRA를 체결한 인정기구에서 인정한 기관 등을 이용하여야 한다.

19. 샘플링

19.1 IT 보안성 평가에 있어 KS Q ISO/IEC 17025:2017 7.3항은 적용하지 않는다.

20. 결과보고

20.1 IT 보안성 평가에 있어 KS Q ISO/IEC 17025:2017 7.8.1항의 "시험성적서"는 "평가보고서"에 해당한다. 평가보고서의 양식은 인정기관에서 정한 공식적인 양식을 사용한다.

20.2 신청사업자 및 공인시험기관은 평가를 수행한 평가보고서를 발행한다. 신청기관에게 제출할 평가보고서는 신청기관과의 계약에서 정한 사항을 충족시키는 것이어야 한다. 신청사업자 및 공인시험기관은 CEM에서 정한 수준으로 평가보고서를 작성하여야 한다.

21. 시험성적서

21.1 신청사업자 및 공인시험기관은 평가보고서의 발행(승인)에 책임을 지는 자를 인정기관에 평가보고서 기술책임자로서 신고하여야 한다. 평가보고서 기술책임자는 평가보고서를 검토하고 평가보고서 기술책임자가 부재의 경우에 대비하여 대리자를 지명해야 한다. 평가보고서 기술책임자 및 대리인은 복수로 지명해도 무방하다.

21.2 평가대상 제품의 평가일자는 평가에 소요된 모든 기간 중 최종일을 기재하여야 한다.

21.3 평가보고서는 1건의 평가대상 제품에 대하여 복수를 발행해도 무방하다. 이 경우에는 각각의 보고서에 고유의 식별자를 부여해야 한다.

21.4 IT 보안성 평가에 있어 KS Q ISO/IEC 17025:2017 7.8.4항은 적용하지 않는다.

22. 재검토 기한

「훈령·예규 등의 발령 및 관리에 관한 규정」(대통령 훈령 제394호)에 따라 이 고시 발령한 후의 법령이나 현실 여건의 변화 등을 검토하여 이 고시의 폐지, 개정 등의 조치를 하여야 하는 기한은 2023년 09월 14일까지로 한다.

부 칙

제1조(시행일) 이 기준은 고시한 날로부터 시행한다.

제2조(일반적 경과조치) 종전의 「정보보호시스템 추가기술요건」(기술표준원 고시 제2012-0067호, 2012. 2. 17)에 의한 공인기관 인정 및 그 밖의 행위는 이 추가기술요건에 의하여 행한 것으로 본다.

<별표> 평가 보증컴포넌트 정의

(1) 인정범위가 EAL4 이하의 보증등급패키지인 시험기관의 경우

보증클래스	평가가능 보증컴포넌트
개발	ADV_ARC.1, ADV_FSP.1~5, ADV_IMP.1~2, ADV_TDS.1~5
설명서	AGD_OPE.1, AGD_OPE.1
생명주기지원	ALC_CMC.1~5, ALC_CMS.1~5, ALC_DEL.1, ALC_DVS.1~2, ALC_FLR.1~3, ALC_LCD.1~2, ALC_TAT.1~3
보안목표명세서 평가	ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.1~2, ASE_REQ.1~2, ASE_SPD.1, ASE_TSS.1
시험	ATE_COV.1~3, ATE_DPT.1~4, ATE_FUN.1~2, ATE_IND.1~3
취약성	AVA_VAN.1~3
보호프로파일 평가	APE_CCL.1, APE_ECD.1, APE_INT.1, APE_OBJ.1~2, APE_REQ.1~2, APE_SPD.1
합성	ACO_COR.1, ACO_CTT.1~2, ACO_DEV.1~3, ACO_REL.1~2, ACO_VUL.1~3

(2) 인정범위가 EAL5 이하의 보증등급패키지인 시험기관의 경우

보증클래스	평가가능 보증컴포넌트
개발	ADV_ARC.1, ADV_FSP.1~5, ADV_IMP.1~2, ADV_INT.2~3, ADV_TDS.1~5
설명서	AGD_OPE.1, AGD_OPE.1
생명주기지원	ALC_CMC.1~5, ALC_CMS.1~5, ALC_DEL.1, ALC_DVS.1~2, ALC_FLR.1~3, ALC_LCD.1~2, ALC_TAT.1~3
보안목표명세서 평가	ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.1~2, ASE_REQ.1~2, ASE_SPD.1, ASE_TSS.1
시험	ATE_COV.1~3, ATE_DPT.1~4, ATE_FUN.1~2, ATE_IND.1~3
취약성	AVA_VAN.1~4
보호프로파일 평가	APE_CCL.1, APE_ECD.1, APE_INT.1, APE_OBJ.1~2, APE_REQ.1~2, APE_SPD.1
합성	ACO_COR.1, ACO_CTT.1~2, ACO_DEV.1~3, ACO_REL.1~2, ACO_VUL.1~3

<참조> EAL4 승인기관이 EAL5 기관으로 업그레이드 할 경우 보증컴포넌트 평가 관련 예시

EAL4 보증컴포넌트	EAL5 이상 보증컴포넌트	EAL4 보증컴포넌트 vs. EAL5이상 보증컴포넌트 비교 설명	추가 평가
ADV_FSP.4	ADV_FSP.5	o 추가적인 오류메시지 서술, 준정형화된 방식(예 : Flow Chart)의 서술 추가	불필요
	ADV_FSP.6	o 추가적인 오류메시지 서술, 정형화된 방식의 서술 추가 ※ 정형기법에 대한 추가 기술 확보 필요	필요
ADV_IMP.1	ADV_IMP.2	o TOE설계와 구현표현간의 대응관계 범위 확대 (일부 -> 전체)	불필요
-	ADV_INT.2	o 전체 TSF의 구조화된 내부 설계 ※ 구조화 설계에 대한 추가 기술 확보 필요	필요
	ADV_INT.3	o 전체 TSF의 구조화되고 복잡하지 않은 내부 설계 ※ 구조화 설계 및 복잡도 최소화 방식에 대한 추가 기술 확보 필요	필요
-	ADV_SPM.1	o 정형화된 보안정책 모델 추가 ※ 정형기법에 대한 추가 기술 확보 필요	필요
ADV_TDS.3	ADV_TDS.4	o TSF 서브시스템의 준정형화된 방식(예 : Flow Chart)의 서술 추가	불필요
	ADV_TDS.5	o TSF 서브시스템 및 모듈의 준정형화된 방식(예 : Flow Chart)의 서술 추가	불필요
	ADV_TDS.6	o TSF 서브시스템의 정형화된 서술 및 모듈의 준정형화된 서술 ※ 정형기법에 대한 추가 기술 확보 필요	필요
ALC_CMC.4	ALC_CMC.5	o 형상관리 통제방법 강화	불필요
ALC_CMS.4	ALC_CMS.5	o 형상목록에 개발도구 및 관련 정보 추가	불필요
ALC_DVS.1	ALC_DVS.2	o TOE의 비밀성 및 무결성 유지를 위한 보호대책 정당화 서술 추가	불필요
ALC_LCD.1	ALC_LCD.2	o 측정 가능한 생명주기 모델 사용(국제표준에서 정의된 모델 사용 확인등)	불필요
ALC_TAT.1	ALC_TAT.2	o 개발자가 적용하는 구현표준 서술 추가(국제표준에서 정의된 구현표준 사용 확인 등)	불필요
	ALC_TAT.3	o 개발자 및 제3의 제공자가 적용하는 구현표준 서술 추가(국제표준에서 정의된 구현표준 사용 확인 등)	불필요
ATE_COV.2	ATE_COV.3	o 시험 범위 확대(일부 TSFI -> 모든 TSFI)	불필요
ATE_DPT.1	ATE_DPT.3	o 시험 범위 확대(일부 모듈 -> 모든 모듈)	불필요
	ATE_DPT.4	o 시험 범위 확대(모든 모듈, 구현 표현)	불필요
ATE_FUN.1	ATE_FUN.2	o 시험절차의 순서 종속관계에 대한 분석 추가	불필요
ATE_IND.2	ATE_IND.3	o 시험 범위 확대(표본 시험 -> 전수 시험)	불필요
AVA_VAN.3	AVA_VAN.4	o 중간 공격수준의 내성 검증 추가 ※ 중간의 공격성공가능성을 가지는 공격자가 수행할 수 있는 취약점 분석 및 침투시험 방법에 대한 추가 기술 확보 필요	필요
	AVA_VAN.5	o 높은 공격수준의 내성 검증 추가 ※ 높은 공격성공가능성을 가지는 공격자가 수행할 수 있는 취약점 분석 및 침투시험 방법에 대한 추가 기술 확보 필요	필요