보안기능 확인서

발급절차 안내

V2.3

제 · 개정 이력

일 자	변경 내용	문서 버전
2020. 05. 15.	o '보안기능 확인서 발급절차 안내' 제정	V1.0
2020. 05. 21.	o 제출물 작성방법, 보안기능 시험, 발급절차 설명 등	V1.1
2021. 05. 25.	o 제도 개선 사항(△유효기간 △일반 보안요구사항 등) 반영 o 제출물 작성 방법 등 보완	V1.5
2021. 07. 02.	o 발급가능 제품 유형중 誤記 정정 o 발급 제한 기준 · 간소화된 발급절차에 대한 설명 추가	V1.6
2021. 08. 26.	o 국내용 CC인증제품에 대한 발급절차 추가	V1.7
2021. 12. 27.	o 다음 사항에 대한 상세 설명 추가 - 표준 · 간소화 · CC인증 수용 발급 절차 - 시험기관 · 시험원 및 '보증 시험' 등 o 신설된 절차에 대한 설명 추가 - 국가용 PP(Protection Profile)를 준수한 국제용 CC인증제품에 대한 발급절차 신설 -「보안기능 구현명세서」 기반 시험 · 발급 절차 신설 - '착수검토회의' 및 시험중 제출물(제품 포함) 보완 절차 신설 - 탑재된 암호모듈 만료시 추가 시험을 통한 효력연장 절차 신설 등	V2.0
2022. 06. 22.	o 다음 사항에 대한 상세 설명 추가 - 양자암호통신장비 제품군에 적용되는 추가 기재 사항 o 제품유형 제한 해제 - '[별표 1]'에 기재된 발급가능 제품유형을 '예시'로 변경 - 신종 융 · 복합 제품은 'OOO 제품군 기타'로 표기하지 않고 신청업체가 제품유형을 자율 기재하도록 허용 o 권장 시험기간 기재 o 발급가능 제품유형 추가 - 양자암호통신장비 제품군 추가	V2.1
2022. 10. 28.	o 원격시험 허용 o 구현명세서 기반 시험의 횟수 제한 해제 o '〈부록〉 보완요청이 빈번한 항목' 추가	V2.2
2025. 05. 20.	o 다음 사항에 대한 상세 설명 보완 - '추가 시험', '보안기능 확인서 유효기간 부여 원칙', '보안기능 시험 신청서' 보완 - '클라우드 환경 또는 운영체제 추가' 추가 - '발급된 제품의 하드웨어 모델 추가', 시험결과 요약서 관련 절차 · 별지 보완 o '파생 제품에 대한 보안기능 확인서 발급', '제품 명칭 변경 등' 삭제	V2.3

1 보안기능 시험 제도 개요

Ⅰ 제도 소개

'보안기능 시험' 제도(Security Function Test Program)는 정보보호시스템 · 네트워크 장비 등 IT보안제품의 안전성을 사전에 검증[1]하여 **사이버안보 위해 제품**과 **부실제품**의 **공공분야 유입**을 막고 **주요 국가기관**의 **사이버보안**을 **강화**하기위해 국가정보원이 운영하는 제도입니다.

시험기관은 국가용 보안요구사항을 만족한 제품에 대해 보안기능 확인서[2](Verification of Security Function Test)를 발급합니다.

국가정보원은 정책기관, 국가보안기술연구소는 검증기관이며 한국정보통신기술협회(TTA) 등 6개 기관이 공인시험기관으로 지정되어 관련 업무를 수행하고 있습니다.

2 '보안기능 확인서' 발급 대상 제품

보안기능 확인서는 국가정보원법 제4조 · 사이버안보업무규정 제9조 및 전자정부법 제56조 · 전자정부법 시행령 제69조에 따른 안전성 검증의 대상인 보안기능이 있는 정보통신기기[3]에 대해 발급이 가능합니다.

---

1) '보안기능 확인서' 발급과 관련된 모든 절차는 국내 · 외 제품에 동일하게 적용됩니다.

2) '보안기능 확인서'란 발급기준을 만족한 제품에 대해 시험기관이 발급하는 증서를 말합니다.

3) '보안기능이 있는 정보통신기기'란 △정보보호시스템 및 △네트워크 장비(L3 이상 스위치, 라우터, SDN 장비 등) △제품의 유형이 정해지지 않은 신기술 · 신종 융복합 제품 등을 말합니다.

(1) 보안기능 확인서 발급 제품 유형

침입차단제품군, 침입방지제품군 등 9개 제품군에 속하는 제품에 대해 발급됩니다. 신종 제품의 경우, 제품군을 선택한 후 제품 유형을 자율적으로 기재하여 발급될 수 있습니다.(별표 1. 참조)

(2) 보안기능 확인서 발급 제품에 대한 정의

국가정보원은 보안기능 확인서가 발급된 제품에 대해 아래와 같이 정의합니다.

〈 발급제품 정의 〉

❶ 보안기능 확인서 발급 제품은 2022.11.1.부터 시행되는 '新 보안적합성 검증체계'에 규정된 모든 그룹의 보안기준을 만족합니다.

❷ 보안기능 확인서 발급 제품은 개발업체에 의해 발급일까지 발견된 취약점이 제거되었지만 발급일 이후, 미래에 발견될 수 있는 취약점은 제거되지 않았습니다.

❸ 보안기능 확인서 발급 제품은 보안기능 시험을 위해 제출된 문서와 형상에 따라 시험되었습니다. 발급 제품의 운용중 기능 개선 · 취약점 제거 등으로 인한 형상변경은 불가피 하지만, 이로 인해 보안기능이 저하되거나 새로운 취약점이 발생되는 상황은 보안기능 확인서 발급 과정에서 전제되지 않았습니다.

여 백

2 제출문서 작성

Ⅰ 제출문서 작성시 유의사항

모든 제출문서는 한국어(한글)로 작성되어야 합니다. 다만 제품 또는 보안기능 명칭 등의 고유명사는 외국어로 표기할 수 있습니다. 제출문서에 기재되는 내용을 바탕으로 보안기능 시험이 수행되므로 허위 · 과장 · 축소 · 누락없이 사실 그대로 기재해야 합니다. 고의로 제출문서에 사실이 아닌 내용을 기재할 경우, 시험이 중단될 수 있으며 보안기능 확인서가 발급되었더라도 효력이 무효화될 수 있습니다.

2 제출문서 작성 방법

(1) 제품 설명서

「제품 설명서」는 관리자 · 사용자가 신청 제품을 목적에 맞게 활용할 수 있도록 운용 방법을 기술한 문서 입니다. 「제품 설명서」에 필수로 기재되어야 하는 항목은 다음과 같습니다.

□ H/W 사양

신청 제품의 CPU · RAM · 저장 장치 · 인터페이스 등 하드웨어 구성요소를 기술합니다. 파생모델이 있을 경우 각 모델별로 하드웨어 사양을 식별, 기재해야 하지만, ‘Capacitor’ · ‘Power Module’ 등 보안기능과 관련없는 구성요소는 기재하지 않아도 됩니다.

□ 운용 환경

신청 제품의 운용에 필요한 ‘S/W적 요소’를 기술합니다. 운영체제(O/S)와 같이 제품이 설치되는 S/W 뿐 아니라, DB · Web 서버 등 제품에 연동되는 외부 IT실체도 포함됩니다.

운용 환경은 명확하게 식별되야 합니다. 단순히 'Redhat® Linux' · 'Windows® Server' 등 제품 명칭만 기재하지 않고, S/W의 특정 형상을 지정하는 버전도 기재해야 합니다.

〈 표 1. 운용 환경 기재 예시〉

잘못된 표기	올바른 표기
Windows 10	Windows 10 pro 20H2 19042.928
Linux	Release : Redhat linux x.x Kernel : Linux version 3.16.0-30-generic (이하 생략)
Apache Server	Apache/2.4.6 (Cent OS)

운용 환경 버전은 S/W(OS)에서 제공되는 명령어(예 : grep . /etc/*-release, httpd -v 등) 또는 버전 확인 기능을 사용하여 출력된 값을 기재합니다.

□ **설치 · 사용법**

신청 제품의 설치 · 배포 및 준비 · 일반적인 운용방법 · 관리 등을 기술합니다. 최초 설치 또는 업데이트시 배포되는 방식(예 : CD, USB, 온라인 등)도 기재되야 합니다.

□ **문제 해결 방법**

예정되지 않은 작동 중단 · 불완전한 시동 또는 종료 등 운용 과정에서 문제가 발생할 경우, 이를 해결할 수 있는 방법을 기재합니다.

(2) 보안기능 구현명세서

「보안기능 구현명세서」는 시험기관이 신청 제품에 구현된 보안기능을 최대한 이해할 수 있도록 구현 방법 · 동작 절차 등의 상세한 사항을 기술한 문서입니다.

그리고 일반 보안요구사항(35페이지 참조)의 작성이 어려울 경우,「보안기능 구현명세서」가 시험항목을 식별 · 시험하기 위해 활용될 수 있습니다.「보안기능 구현명세서」는 최대한 시험원이 이해할 수 있는 방식으로 기술되야 하며 이를 보조하기 위해 도표 · 그림 등을 첨부할 수 있습니다.「보안기능 구현명세서」에 필수로 기재되어야 하는 항목은 다음과 같습니다.

□ 보안기능 식별

제품에 구현된 보안기능은 최소한의 단위로 나누어 식별되고 수행하는 역할이 기재되어야 합니다. 각 보안기능은 타 보안기능과의 연관 · 종속관계가 기재될 수 있습니다. 식별된 보안기능의 기재 예시는 아래와 같습니다.

〈 예시 : 보안기능의 식별〉

1. 패스워드 암호화

관리자 및 사용자 패스워드는 OOO 으로 암호화되며 Rounds 값은 OOOO 으로 범위는 OOOO ~ OOOO 입니다. Salt 값은 OOOO 함수를 이용하여 생성됩니다.

- 중 략 -

1.1 마스터 패스워드

마스터 패스워드는 OOOO에 대한 입력으로 암호화되며 OOOO 알고리즘을 사용...

□ 접속 방법 · 인터페이스 중요

사람 또는 외부 IT실체의 제품 접속을 위해 제품이 제공(구현)하는 인터페이스[1] · 계정을 빠짐없이 기재해야 합니다. △기본 설정된 관리자 계정 △유지보수용 인터페이스 · 계정 △전원 인가시 또는 운용중 특정 조건 · 외부 신호 · 키보드 입력의 조합[2] 등에 의해 활성화되는 인터페이스 · 계정이 해당됩니다. 제공(구현)되는 모든 인터페이스 또는 계정은 사용 목적을 만족해야 하며 목적을 특정하지 않고 제공(구현)될 수 없습니다. 기재되지 않은 인터페이스 · 계정은 '백도어'로 간주되어 발급이 거부되거나 보안기능 확인서의 효력이 무효화될 수 있습니다.

□ 보안기능 구현 명세

식별된 보안기능에 대해 △기능 구현 방식 △동작 방식 등을 기재합니다. 시험원의 이해를 돕기 위해 표 · 그림 · 순서도 등을 추가할 수 있습니다.

---

1) '인터페이스'란, 접속을 위해 실행(준비)되는 포트 · 서비스 · 프로세스 등을 포함하는 의미입니다.

2) 예를 들어 키보드의 특정 입력값에 의해 활성화되는 엔지니어 모드 등이 있습니다.

□ 양자암호통신 제품군에 적용되는 추가 기재 사항

양자암호통신 제품군(양자키관리장비, 양자키분배장비, 양자통신암호화장비 등)의 경우, 양자키의 안전한 생성 · 분배 · 관리 등 구현된 보안기능에 대한 시험과 검증이 필요합니다.

이를 위해 다음의 표에 기재된 내용을 상세하게 서술해야 합니다.

〈 표 2. 양자암호제품군에 적용되는 추가 기재사항 〉

제품 유형	보안기능	항목
양자통신 암호화장비	하이브리드 키 조합	1.3.2 검증필 암호모듈이 제공하는 조합키 생성 기능 사용 방식 1.3.2 검증필 암호모듈에서 조합키 생성 기능을 제공하지 않는 경우 제품 자체에서 조합키 생성 과정
	암호화 통신용 비밀키 생성	1.4.1 검증필 암호모듈이 제공하는 암호화 통신용 비밀키 생성 기능 사용 방식 1.4.1 검증필 암호모듈에서 암호화 비밀키 생성 기능을 제공하지 않는 경우 제품 자체에서 암호화 비밀키 생성 과정
양자키 관리장비	키 파기	1.6.1 모든 키 및 그와 관련된 정보가 삭제되는 시기와 파기하는 매커니즘에 대한 설명
양자키 분배장비	비밀키 생성	1.1.1 제품에 적용된 비밀키 생성을 위한 양자키분배 매커니즘에 대한 설명
	광학계 기능	2.2.1 QKD 매커니즘 동작 절차와 관련 요구사항의 만족 여부 설명
		2.2.2 광학계 동작이 QKD 매커니즘을 정확히 구현하였는지 여부 2.2.2 광학계 불완전 동작시 혹은 실시간 도청 판정의 경고 메시지와의 연계방법 설명
		2.2.3 QKD 광학계가 양자성을 가지고 있음을 설명
	양자상태 생성	2.3.1 양자상태가 생성되는지 시험한 자체 평가 내용
	후처리 동작 보호	2.5.2 후처리 동작의 절차별 보안기능에 대한 요구항목 만족여부 설명

제품 유형	보안기능	항목
양자키 분배장비	후처리 동작 보호	2.5.3 후처리 알고리즘의 안전성 증명에 대한 요구항목 만족여부 설명(선택)
	알려진 공격에 대한 보호	2.6.1 QKD 장비의 알려진 공격 및 그 대응책에 대한 설명을 제품 설명서나 구현명세서에 기술(선택)
공통	인증데이터 보호	o 비밀번호를 저장하는 방법(사용 암호 알고리즘 포함) o 최소 128bit 이상의 난수를 발생시켜 salt값을 사용하는 방법
	암호 사용	o 제품에서 사용하는 검증필 암호모듈의 명칭 o 사용하는 검증대상 암호알고리즘 o 검증필 암호모듈이 제공하는 암호기능(예 : API 등) 사용 여부 o 블록암호 사용 요구사항 준수 여부
	암호키 생성	o 제품에서 생성하는 암호키와 난수의 종류 및 생성 방식에 대한 설명
	암호키 유도	o 제품에서 키 유도 방식으로 생성하는 암호키 종류 및 유도 방식에 대한 설명
	암호키 저장	o 제품에 저장되는 암호키의 종류 및 저장 방식에 대한 설명
	암호키 파기	o 제품의 암호키 파기 시점 및 파기 방식에 대한 설명
	보안기능 자체시험	o 제품 구동시 하드웨어 오류에 대한 자체 시험기능의 상세한 설명 o 제품 구동시 프로세스 오류에 대한 자체 시험기능의 상세한 설명
	무결성 검사 기능	o 제품 구동시 펌웨어 및 주요소프트웨어에 대한 무결성 검사 기능의 상세한 설명 o 운용중 주요 소프트웨어에 대한 무결성 검사기능의 상세한 설명(선택)

(3) 보안기능 운용 설명서

「보안기능 운용 설명서」는 「보안기능 구현명세서」에 기재된 모든 보안기능의 △설정 △운용 절차 · 방법 등을 기재한 문서입니다. 제품의 특징에 따라 「보안기능 구현명세서」에 해당 내용을 통합, 기재할 수 있습니다.

(4) 시험결과서

「시험결과서」는 신청 업체가 사전에 '국가용 보안요구사항'(Security Requirement for Government)또는 '일반 보안요구사항'에 따라 제품의 보안기능을 시험하고, 그 결과를 기재한 문서입니다. 각 보안요구사항별로 △시험 환경 △시험 절차 △시험 결과를 기재합니다. 시험 결과는 요구사항 만족 여부에 따라 〈표 3〉의 기준을 준수하여 기재해야 합니다. 적용 가능한 보안요구사항이 없는 경우, 구현명세서에 기재된 보안기능에 대해 자체 시험합니다.

〈 표 3. 시험결과 기재 〉

구현 강도	시험 결과
'필수' 항목	'만족', '불만족'으로 기재
'조건부 필수' 항목	'만족', '불만족', '기능 미제공'으로 기재
'선택' 항목	'만족', '불만족', '기능 미제공', '해당사항 없음'으로 기재

(5) 취약점[1] 개선내역서

「취약점 개선내역서」는 신청 제품의 취약점 개선 이력과 그 내용을 기술한 문서입니다. 「취약점 개선내역서」를 제출받는 이유는 사전에 제품의 보안성을 제고하고 시험중 발견된 취약점 보완으로 인한 시험 · 발급 지체를 방지하기 위함입니다.

「취약점 개선내역서」의 기재 대상은 △CVE △개발사 △KISA 홈페이지에 공개된 취약점중 신청 제품에 해당하는 취약점이며, 신청일 3년전(변경 승인의 경우 발급일)으로부터 신청 전일(前日)까지 개선이 완료된 내역을 기재해야 합니다.

다만, 리눅스 커널 2.x 와 같이 반드시 보완해야 하는 특정 취약점의 경우, 출시일로부터 신청 전일(前日)까지 개선 내역을 기재해야 합니다.

---

1) '취약점'이란, 사이버 공격에 악용되어 관리자가 설정한 접근권한外 정보를 열람 · 취득하게 하거나 보안기능을 회피 가능하게 하는 정보통신망 · 정보시스템의 결함을 말합니다.

「취약점 개선내역서」는 ‘취약점 리스트’와 ‘세부 개선내용’으로 구성됩니다. ‘취약점 리스트’란 식별되어 개선된 취약점을 기재한 목록이며 ‘취약점 리스트’에 기재된 취약점의 개선 내용을 ‘세부 개선내용’에 기재합니다. ‘세부 개선내용’에 기재되어야 할 항목은 〈표 4〉와 같습니다.

〈 표 4. ‘세부 개선내용’에 기재되어야 하는 항목 〉

항목	기재가 필요한 내용
취약점 설명	△취약점의 영향을 받는 보안기능 △위협 정도 △취약점이 발견된 부분(S/W의 경우, 파일 이름도 명기)
취약점 개선 내용	취약점에 대한 기술적 조치 (화면 · 동영상 캡쳐 등 증빙자료 포함)

3 제출물의 관리

신청 업체로부터 제출물(제출 문서와 신청 제품)을 인수한 시험기관은 제출문서가 신청 업체의 동의나 법원의 명령없이 정책기관 및 검증기관을 제외한 제3자에게 제공되거나 공개되지 않도록 관리해야 합니다.

이를 위해 시험기관은 자체적으로 제출물 관리체계와 절차를 수립하여 제출물을 관리해야 하며 신청 업체는 시험기관에 비밀유지계약 체결 등 제출물에 대한 제3자 유출 제한 조치를 요청할 수 있습니다.

여 백

3 보안기능 시험 신청 단계

1 신청 업체 준수 사항

신청 업체는 ①제출물 작성 · 제출, ②시험에 필요한 기술 지원, ③발급 제품의 보안기능 및 취약점 개선결과 보증, ④발급 제품의 사후 관리 등의 역할을 수행하며 다음 사항을 준수해야 합니다.

① 보안기능 확인서 발급 절차를 준수해야 하며 시험 진행과 관련된 문서를 제3자에게 유출해서는 안됩니다.

② 보안기능 확인서 발급과 관련된 모든 사항을 국가 · 공공기관 납품 이외 용도로 활용해서는 안됩니다.

③ 제출물과 신청 제품에 대한 정당한 법적 권한[1]을 가지고 있어야 하며 제출문서 기재 내용의 허위 · 과장 · 축소 · 누락없이 사실대로 작성해야 합니다.

2 보안기능 시험 신청

(1) 신청 업체 작성 제출문서

신청 업체는 ❶제품 설명서, ❷보안기능 구현명세서, ❸보안기능 운용 설명서, ❹자체 시험결과서, ❺취약점 개선내역서 등 5종의 제출문서와 신청에 필요한 서식을 작성하여 시험기관에 제출해야 합니다. 다만, 관련 법률 · 정책에 의하여 제출이 불가할 경우, 시험기관에 사유를 서면으로 제출하고 대체 방안(예: 열람 등)을 제공해야 합니다.

---

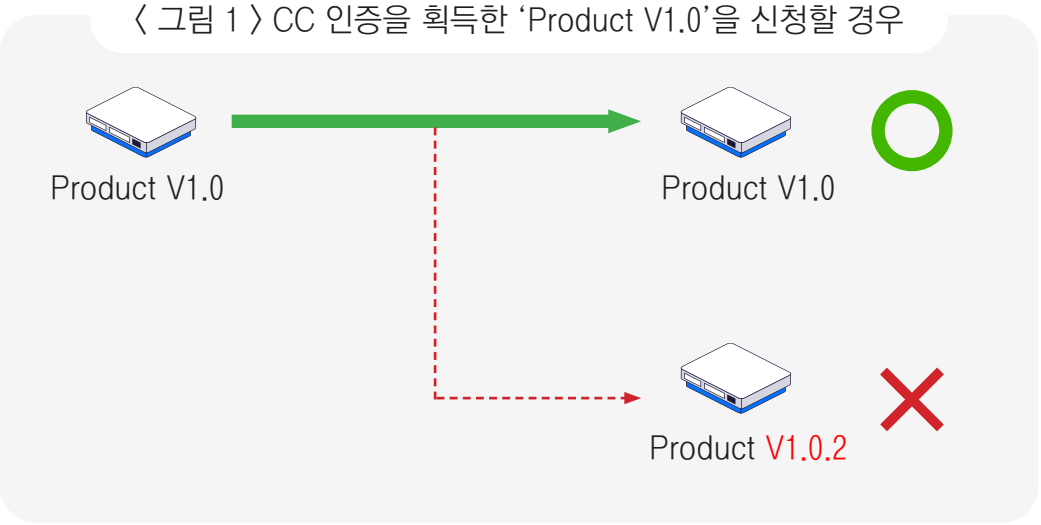
1) '정당한 법적 권한'이란, 신청(개발)업체가 제품에 대한 지적 재산권을 소유해야 하며, 타인의 지적 재산권을 침해하지 않아야 한다는 의미입니다.
특히, 오픈소스를 활용한 제품은 관련 라이센스(예 : GPLv2, 2-clause BSD license 등)의 준수를 적극 권고합니다.

신청 업체가 제출한 문서 등은 시험 결과 검토 및 발급 심의를 위해 정책기관 · 검증기관에 제출되어 열람될 수 있습니다.

(2) CC인증 제품의 신청

국내용 CC인증 또는 국가정보원장이 인정한 보호프로파일[1]을 준수하여 국제 CC인증을 획득한 제품은 제출 문서와 보안기능 시험의 생략이 가능합니다. 이에 해당되는 제품은 인증 형상 그대로 보안기능 시험을 신청해야 합니다. 예를 들어 '침입차단시스템'으로 CC인증을 받은 'Product V1.0' 제품의 경우, 인증 유형(침입차단시스템)과 형상(V1.0)으로 신청해야 합니다. 업데이트 버전(예 : V1.0.2 등)은 신청이 불가합니다.

〈 그림 1 〉 CC 인증을 획득한 'Product V1.0'을 신청할 경우



(3) 신종 제품의 유형 분류

신종 제품[2]은 국가용 보안요구사항과 일반 보안요구사항이 복합적용[3]되므로 9개의 제품군 중 어느 하나에 해당하는지 선택하여 신청해야 합니다. 국가용 보안요구사항 중에서 '침입차단시스템 보안요구사항'과 업체가 작성한 일반 보안요구사항이 복합적용된 제품은 신청 업체가 제품 유형을 자율적으로 기재, 신청할 수 있습니다.

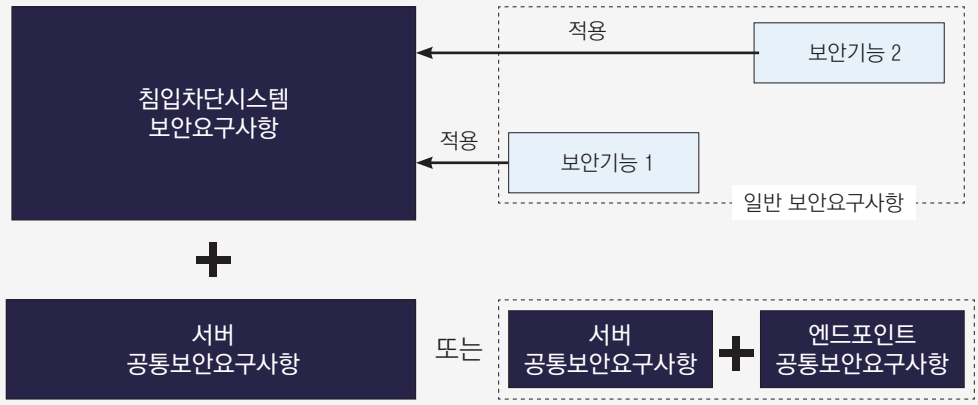
---

1) 국가용 보호프로파일 등 국가용 보안요구사항이 반영되었다고 인정한 보호프로파일을 의미합니다.

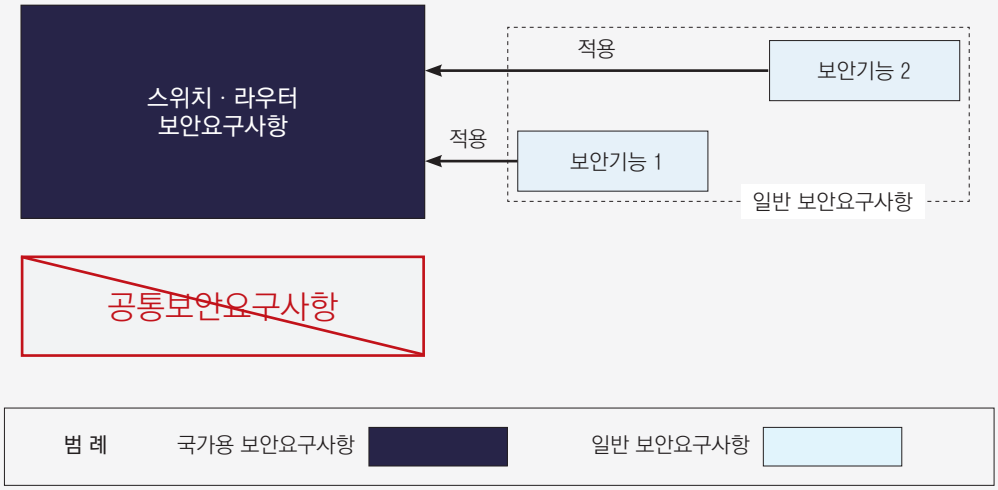
2) 신종 제품이란, 〈표 1〉의 발급 제품 유형(예시)에 해당되지 않는 정보보호제품 · 네트워크 장비를 의미합니다.

3) 국가용과 일반 보안요구사항의 복합적용은 「국가용 보안요구사항」 1편을 참고하시기 바랍니다.

〈 그림 2 〉 '침입차단제품군 기타' 유형의 예시



〈 그림 3 〉 '네트워크장비 기타' 유형의 예시



예시에 언급되지 않은 보안요구사항의 조합도 상기의 원칙이 동일하게 적용됩니다.

3 '보안기능 시험 신청서' 작성 방법

(1) '보안기능 시험 신청서' 서식

'보안기능 시험 신청서'는 신청 제품의 보안기능 시험을 위해 신청 업체가 작성, 시험기관에 제출하는 문서입니다. 아래 설명을 참고하여 '보안기능 시험 신청서'를 작성하시기 바랍니다.

보안기능 시험 신청서

<table>
<tr><td>접 수 번 호</td><td colspan="5">❶ 호</td></tr>
<tr><td rowspan="3">개발(생산)
업체</td><td>업 체 명</td><td colspan="2"></td><td>소재국</td><td></td></tr>
<tr><td>대 표 자
성 명</td><td colspan="4"></td></tr>
<tr><td>주 소</td><td colspan="4">□□□□□ ❷</td></tr>
<tr><td rowspan="5">신청기관</td><td>업 체 명</td><td colspan="2"></td><td>소재국</td><td></td></tr>
<tr><td>대 표 자
성 명</td><td></td><td>사업자등록번호</td><td colspan="2">❸</td></tr>
<tr><td>주 소</td><td colspan="4">□□□□□ ❹</td></tr>
<tr><td rowspan="2">담당자
성 명</td><td rowspan="2"></td><td>전화 번호</td><td colspan="2"></td></tr>
<tr><td>이메일 주소</td><td colspan="2"></td></tr>
<tr><td rowspan="9">신청제품</td><td>제 품 군</td><td>❺</td><td>제품 유형</td><td colspan="2">❻</td></tr>
<tr><td>제 품 명</td><td colspan="4"></td></tr>
<tr><td>운영 체제</td><td colspan="4">❼</td></tr>
<tr><td>펌 웨 어</td><td colspan="4">기본 : ❽ 사용자 설치 : ❾</td></tr>
<tr><td>해시값</td><td colspan="4"></td></tr>
<tr><td rowspan="3">CC인증
(해당시)</td><td>인증서 번호</td><td></td><td>인증 등급</td><td></td></tr>
<tr><td>인증 기관</td><td></td><td>만 료 일</td><td></td></tr>
<tr><td>준수한 PP</td><td colspan="3"></td></tr>
<tr><td rowspan="2">검증필
암호모듈
(해당시)</td><td>검증 번호</td><td>CM -</td><td>검증 등급</td><td></td></tr>
<tr><td>유효 기간</td><td colspan="3"></td></tr>
<tr><td rowspan="2">추가 시험
(해당시)</td><td colspan="2">최초 신청 또는 발급 제품
정보(제품명 및 발급번호)</td><td colspan="3">❿</td></tr>
<tr><td colspan="2">신청 사유</td><td colspan="3">⓫</td></tr>
</table>

개발 및 생산	⑫ 개 발 방 식	□ 독자 개발 □ 공동 · 위탁 개발(전체) □ 공동 · 위탁 개발(일부)	
		공동 · 위탁 개발(ODM)일 경우 기재	
		계약 업체명	
		계약업체 소재지	
	⑬ 생 산 방 식	□ 자체 생산(본사 생산) □ OEM(H/W) □ OEM(전체) □ 기 타	
		위탁 생산(OEM)일 경우 기재	
		계약 업체명	
		계약업체 소재지	
탑재 모델명 (복수 기재 가능)			

※ 신청 제품이 공동(위탁) 개발 · 생산에 해당할 경우, 신청 업체는 해당 사실을 증명하는 계약서 사본 1부를 첨부해야 합니다.(다만, 계약서 내용에 쌍방 또는 일방에 의해 기밀로 취급되는 사항은 검증기관과 협의하여 해당 내용을 삭제하고 제출할 수 있습니다.)

※ 추가 시험의 경우 신청 사유에 따라 제한적으로 형상 변경이 가능하나 신청 사유와 무관한 변경은 허용되지 않으며 이를 위반시 허위사실로 간주합니다.

※ 이 신청서에 기재한 내용중 허위사실이 확인될 경우, 시험이 중단되거나 확인서의 효력이 정지(취소)될 수 있습니다.

상기 제품에 대한 보안기능 시험을 신청합니다.

20 년 월 일

(직인)

귀하

(2) '보안기능 시험 신청서' 서식 설명

□ '❶' 접수 번호

시험기관이 사전검토를 완료한 후, 부여하는 번호입니다.

□ '❷, ❹' 개발(생산)업체 및 신청업체 우편번호

작성시 선택한 개발(생산)업체의 '소재국'에 맞게 자동으로 우편번호 입력란이 조정됩니다. 만약, 선택 가능한 소재국이 없다면 우편번호는 공란으로 비워놓으십시오. 선택 가능한 소재국은 대한민국, 독일, 미국, 스웨덴, 영국, 일본, 중국, 프랑스, 핀란드 9개국이며 그 외는 직접 국가이름을 입력할 수 있습니다.

□ ‘❸’ 사업자등록번호

해외 소재 업체가 직접 신청할 경우 미국(EIN), 영국(UTR), 독일(Handelsregister) 등 소재국의 세무당국이 발행한 번호를 기재합니다.

□ ‘❺’ 제품군

침입차단제품군, 침입방지제품군 등 9개의 제품군 중에서 하나를 선택합니다. 선택 가능한 제품군은 〈별표 1. 보안기능 확인서 발급 가능 유형(예시)〉를 참고하십시오.

□ ‘❻’ 제품 유형

〈별표 1. 보안기능 확인서 발급 가능 유형(예시)〉에 따라 신청 제품에 해당되는 제품 유형을 선택합니다. 일반 보안요구사항이 적용된 제품은 〈그림 2〉와 〈그림 3〉을 참고하여 제품 유형을 선택하십시오. 새로운 제품유형은 해당 유형을 자율적으로 기재합니다.

□ ‘❼’ 운영 체제

〈표 5〉의 기재 방법에 따라 신청 제품이 운용되거나 제품에 설치되는 OS · 펌웨어를 기재합니다.

〈 표 5. 운영체제 기재 방법 〉

제품 형태	기재 내용	유의 사항
S/W	제품이 운용되는 OS를 기재	〈 표 3. 운용 환경 기재 예시〉 준수
H/W	펌웨어의 기저OS를 기재 (예 : Linux kernel 3.x.x 등) * 자체 개발 펌웨어는 업체의 표기방식을 수용	

□ ‘❽, ❾’ 펌웨어

네트워크 장비 등 하드웨어 일체형 제품만 기재합니다. S/W제품은 공란으로 남겨 두십시오. ‘기본’란에는 기저 펌웨어의 파일 명칭을 기재하고, ‘사용자 설치’란에는 기저 펌웨어 파일에 추가 설치되는 파일 명칭을 기재합니다.

□ ‘❿, ⓫’ 추가 시험 2025.05.20.

추가 시험의 기반이 되는 최초 시험 또는 발급제품의 제품명과 발급번호를 기재하고, 추가 시험 절차의 〈추가 시험 신청 제품〉을 참고하여 해당하는 신청 사유를 기재합니다.

□ '⑫' 개발 방식

개발 업체가 신청 제품을 단독으로 개발하였는지, 공동 · 위탁 개발하였는지를 기재합니다. 공동 · 위탁 개발한 경우, 수탁(하청) 업체의 명칭과 소재국을 기재합니다.

□ '⑬' 생산 방식

신청 업체는 OEM[1] 생산 업체의 명칭과 소재국가를 기재합니다.

□ 국제사회의 제재를 받는 국가(단체) 및 업체에 대한 제한

공동 · 위탁 개발하거나 OEM 생산의 경우, 신청 업체는 개발(생산)에 참여한 업체가 국제사회로부터 다자간 · 일방적 제재를 받고 있는지 확인해야 합니다.

만약, 개발 · 생산 · 유통 과정에 국제사회의 제재를 받는 국가(단체) · 업체가 있을 경우, 보안기능 시험 신청은 반려되고 이미 진행중인 시험 및 발급된 보안기능 확인서는 확인된 날부터 즉시 중지되거나 효력을 상실합니다.

국제사회의 제재를 받는 국가(단체) · 업체에 대한 사항은 '전략물자관리원' 홈페이지에서 확인하십시오.

1) 신청(개발) 업체와 계약에 의해 타 업체가 제품의 전부 또는 일부를 생산하고 신청(개발) 업체의 상호 · 상표 등의 표식을 사용하여 국가 · 공공기관에 판매되는 경우, OEM 생산에 해당됩니다. 다만, 신청 업체가 일부 H/W를 구입하여 제품을 구성하는 경우는 해당되지 않습니다.

4 보안기능 시험 단계

Ⅰ 제출물 사전 검토 및 착수검토회의

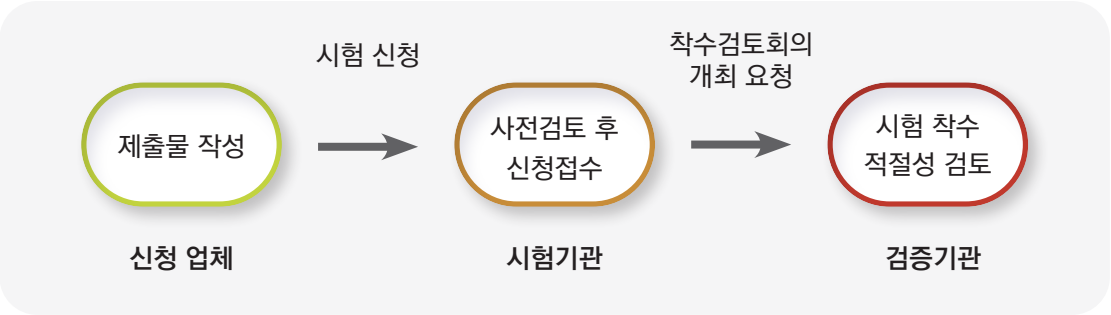
(1) 시험기관에 의한 제출물 사전 검토

신청 업체로부터 보안기능 시험 신청을 받은 시험기관은 업체가 작성한 제출물(제출문서 및 신청 제품)에 대한 사전검토를 실시하여 검토 기준을 만족한다고 판단될 경우, '**보안기능 시험 신청 접수증**'을 작성, 신청 업체에 배부합니다.

(2) 착수검토회의

시험기관은 접수증을 배부한 날로부터 3일 이내에 '착수검토회의'[1] 개최를 검증기관에 요청합니다. 검증기관은 신청 제품에 대한 시험착수의 적절성을 심사하기 위해 신청을 받은 날로부터 5일 이내에 '착수검토회의'를 개최[2]합니다.

〈 그림 4. 신청 및 착수검토회의 〉



1) '착수검토회의'란, 신청 제품의 보안기능 시험 착수 가능 여부를 심사하는 회의를 말합니다.

2) 5일 이내 개최가 곤란할 경우, 시험기관과 검증기관이 협의하여 개최일정을 조정할 수 있습니다.

'착수검토회의'는 해당 시험기관과 검증기관이 참석하며 필요시 검증기관의 요청에 의해 △정책기관 △신청기관(신청 업체) △관련 전문가가 참석할 수 있습니다.

검증기관은 신청 제품이 △사이버 안보 위해 △개발 주체 또는 취약점 개선주체의 불분명 △'**취약점 개선 내역서**'의 부실 작성 △구현된 보안 · 비보안 기능의 신뢰성 부재 등에 해당된다고 판단될 경우, 표준 발급절차를 따르도록 시험기관에 통보할 수 있습니다.(〈별지 2. 신규 신청 및 착수검토 절차〉) 시험기관은 검증기관의 착수 승인 이후, 신청 업체와 시험계약을 체결하고 사안 발생 순서대로 시험에 착수 합니다.

(3) 신청내용의 정정(訂正)

신청 업체는 이미 제출한 '**보안기능 시험 신청서**' 등의 서식에 기재된 오기(誤記)[1]를 올바르게 수정해야할 경우 '**신청내용 정정 신청서**'를 작성, 시험기관에 제출하여 잘못 기재된 내용을 고칠 수 있습니다.

2 보안기능 시험 수행

(1) 시험기관이 반드시 확인해야하는 사항

시험기관은 신청 제품에 구현된 모든 보안기능과 접속 방법 · 인터페이스[2]를 시험하고 확인해야 합니다. 가능한 일부 항목에 대해 외부의 별도공간에서 시험기관으로 연결하여 원격 시험할 수 있습니다.

(2) 시험 범위

최초 신청 제품은 구현된 모든 보안기능이 시험 범위에 속합니다. 그러나, 시험 과정 또는 발급 후 제품의 효력 유지를 위해 일부 보안기능에 대해 시험을 수행할 수 있습니다.

△검증필 암호모듈 만료로 인한 효력 연장 △취약점 패치의 안전성 확인 △하드웨어 모델의 추가 등의 경우가 해당됩니다.

---

1) 오기(誤記)란, 신청된 제품명의 표기방식 변경(△전체표기↔축약표기 △대문자↔소문자 △한글↔한자의 병기 · 전환)이 필요한 경우를 의미합니다.

2) 이 문서의 7 페이지에 기재된 '**사람 또는 외부 IT실체의 제품 접속을 위해 제품이 제공(구현)하는 인터페이스 · 계정**'을 의미합니다.

(3) 시험 기준에 따른 시험의 분류

보안기능 시험은 적용되는 시험 기준에 따라 △‘보안요구사항 기반 시험’과 △‘구현명세서 기반 시험’으로 구분됩니다.

□ 보안요구사항 기반 시험

‘보안요구사항 기반 시험’이란 신청 제품에 국가용 · 일반 보안요구사항[1]을 적용하여 수행하는 시험 절차를 의미합니다. 시험기관은 제품에 해당하는 국가용 · 일반 보안요구사항의 만족여부를 시험합니다. 보안요구사항 기반 시험을 거쳐 발급된 보안기능 확인서는 5년의 효력을 부여합니다.

□ 구현명세서 기반 시험

‘구현명세서 기반 시험’이란 적용 가능한 국가용 보안요구사항이 없어 일반 보안요구사항 작성이 불가피하지만 신청 업체의 사정상 작성이 곤란한 제품에 대해 시험기관이 신청 업체가 제출한 「보안기능 구현명세서」에서 시험 항목을 식별하여 수행하는 시험 절차를 의미합니다.

구현명세서 기반 시험의 횟수 제한은 없으며 이 절차를 거쳐 발급된 보안기능 확인서는 2년의 효력을 부여합니다.

(4) 시험 수행을 위한 신청 업체와 시험기관의 협조

시험기관은 시험중 필요시 신청 업체에 추가 자료제출 또는 시험 환경에 대한 기술적인 지원을 요청할 수 있습니다. 신청 업체는 시험기관의 요청시 합의된 기한 내에 해당 자료를 제출해야 하며 제출 문서의 보완을 요청받은 경우 이에 응해야 합니다.

(5) 제출물(제출문서 및 제품)의 보완

시험 과정에서 제출물의 수정 · 보완이 필요할 경우 시험을 잠시 중단하고 제출물을 보완한 후, 중단된 항목부터 시험을 재개할 수 있습니다. 〈별지 3. 시험중 제출물 보완 절차〉를 참조하십시오.

---

1) 일반 보안요구사항의 적용 원칙은 「국가용 보안요구사항」 제1편의 ‘4. 국가용 보안요구사항의 적용’을 참고하시기 바랍니다.

□ 수정 · 보완이 필요한 항목의 식별

시험기관이 시험중 제출물에서 수정 · 보완이 필요한 항목을 식별할 경우, 시험을 중단하고 신청 업체에 식별된 항목에 대한 보완을 요청합니다. 시험기관에 의한 보완요청은 2회로 제한되므로 시험기관은 시험중 식별된 보완항목을 최대한 취합하여 신청 업체에 전달해야 합니다.

또한, 신청 업체도 시험중 제출물에서 수정 · 보완이 필요한 항목을 식별한 경우 시험기관에 제출물의 수정 · 보완을 위한 시험 중단을 요청할 수 있습니다. 신청 업체에 의한 보완요청의 횟수는 제한이 없습니다.

□ 수정 · 보완 사항에 대한 시험

신청 업체는 특별한 사유가 없는 한, 시험기관과 협의한 기한 이내에 제출물을 보완하여 시험기관에 제출하고 시험기관은 이에 대한 시험을 수행합니다. 보완 기간은 총 3개월을 초과할 수 없습니다. 시험기관은 제출물의 수정 · 보완에 3개월이 초과된다면 시험을 취소할 수 있습니다.

(6) 시험 소요기간

□ 권장 시험기간

신청 제품에 대한 보안기능 시험은 보안요구사항 또는 보안기능 구현 명세서를 기반으로 진행됩니다. 시험기간은 구현된 보안 · 비보안(경우에 따라) 기능을 시험하는데 소요되는 기간이며 각 신청 제품마다 구현된 보안기능이 획일적이지 않고 매우 다양하기 때문에 소요되는 시험기간이 다를 수 있습니다.

신청 업체가 제출한 제출문서의 사전검토가 완료되고 신청 제품에 보완사항이 없다고 가정할 경우, 국가용 보안요구사항 V3.0 기준으로 권장되는 시험기간은 다음과 같습니다.

〈 표 6. 권장 시험기간 〉

구분	적용되는 보안요구사항	시험일수
정보보호시스템	공통보안요구사항(서버 · 엔드포인트)	35일~40일
	제품 단위 보안요구사항	5일~10일
네트워크 장비	라우터 · 스위치 보안요구사항	10일~15일
	SDN 스위치 · 컨트롤러 보안요구사항	15일~20일

이 밖에 국가용 보안요구사항과 일반 보안요구사항을 복합적용하거나 구현명세서 기반의 시험일 경우, 신청 업체와 시험기관이 협의하여 필요한 시험기간을 산정할 수 있습니다.

□ 시험기간 연장 신청

시험기관 또는 신청 업체에 의해 제출물의 수정 · 보완이 요청될 경우, 신청 업체는 시험기관과 수정 · 보완 및 시험을 위해 추가로 필요한 기간을 협의한 다음 시험기관에 '**시험기간 연장 신청서**'를 제출하여 시험기간을 연장합니다.

(7) 시험 중단

시험기관은 시험중 제출물의 수정 · 보완 사항이 식별될 경우뿐 아니라 다음의 사항에 해당될 경우, 시험을 중단할 수 있습니다. 시험기관은 신청 업체와 검증기관에 이를 통보합니다.

〈 시험 중단 사유 〉

1. 제출된 제품과 보안기능 시험 신청서에 기재된 제품이 상이할 경우
2. 신청 업체가 요청하거나 시험기관과 신청 업체간의 계약에 의할 경우
3. 신청 업체가 시험기관과 협의한 보완기간내에 제출물의 보완을 이행하지 못한 경우
4. 신청 업체가 정당한 사유 없이 보안기능 시험을 신청한 날로부터 10일 이내에 신청 제품을 제공하지 않는 경우

(8) 시험 취소

□ 검증기관과 협의에 의한 시험 취소결정

시험기관은 △제출물의 수정 · 보완에 3개월이 초과되는 경우 △신청 업체가 시험 · 검증기관 등을 기망할 목적으로 제출물을 허위로 작성, 제출한 경우 △시험기관이 2회차 보완요청 이후에도 보완 사유를 발견한 경우 검증기관과 협의하여 시험을 취소할 수 있습니다.

□ 검증기관과 협의가 필요하지 않은 시험 취소결정

△신청 업체가 요청하거나 신청 업체와의 계약에 의할 경우 △신청 업체가 제출물의 보완을 거부하는 경우 △신청 업체가 정당한 사유없이 시험기관의 시험 수행을 위한

협조 요청에 불응하거나 발급 절차를 위반하여 처리하도록 강요할 경우 △신청 업체가 '보증 시험'[1]에 필요한 제출물의 제출을 거부할 경우는 검증기관과 협의없이 시험을 취소할 수 있습니다.

(8) 시험의 완료

시험기관은 신청 제품에 대한 시험이 완료될 경우, '**시험결과 보고서**'와 '**시험결과 요약서**[2]'를 작성합니다. 〈별지 5. 시험결과 요약서〉를 참조하십시오. 신청 제품이 표준 발급절차의 대상인 경우, 검증기관에 시험결과의 검토를 요청하고 간소화 발급절차의 대상인 경우, 시험기관이 자체적으로 시험결과를 검토합니다.

3 보증 시험

(1) 보증 시험 대상

검증기관은 정책기관과 협의하여 다음에 해당하는 신청 제품에 대해 시험기간 중 언제라도 보증 시험의 수행을 시험기관에 요구할 수 있습니다.

〈 보증 시험 대상 〉

1. 신청 제품의 개발 · 배포 · 운용 과정에서 사이버안보 위해 우려가 있는 경우
2. 신청 제품에 구현된 보안 · 비보안 기능의 신뢰성에 대한 보증이 필요한 경우
3. 기타 신청 제품의 개발과정에 대한 신청 업체의 보증이 필요한 경우

(2) 보증 시험의 적용기준 및 제출물

보증 시험 수행 적용기준 및 제출물에 대한 사항은 시험기관이 신청 업체에 서면으로 통보합니다.

---

1) '보증 시험'이란 신청 업체 또는 신청 제품의 △신뢰성 △안전성 △보안기능 등에 대한 신청 업체의 보증을 확인하는 별도의 시험절차 입니다.

2) 시험결과 요약서란, 신청 제품에 대한 △요약된 시험 결과 △적용된 시험기준에 대한 사항이 기재된 문서이며 보안기능 확인서 발급시 대외에 공개됩니다.

4 추가 시험 2025.05.20.

(1) 추가 시험 대상

추가 시험은 신청 제품 또는 발급 제품에 대해 추가적인 시험을 수행하는 것으로 추가 시험 대상은 모든 보안기능을 시험 범위로 시험을 수행한 제품을 전제로 합니다.

(2) 추가 시험 신청 제품

다음에 해당하는 제품은 추가 시험을 신청할 수 있습니다.

〈 추가 시험 신청 제품 〉

1. 제품의 안전성 확인이 필요할 경우
2. 검증필 암호모듈 탑재가 필수인 제품의 보안기능 확인서 효력을 발급일로부터 5년까지 연장할 경우
3. 제품의 운용환경으로 클라우드 환경 또는 운영체제를 추가할 경우
4. 제품의 하드웨어 모델을 추가할 경우
5. 시험 절차 중에 형상변경이 불가피할 경우
6. 그 외 정책 · 검증기관이 제품의 추가 시험을 요청할 경우

추가 시험 신청 제품은 추가 시험 신청 사유에 따라 제한적으로 최초 신청 제품 또는 발급 제품을 기반으로 형상 변경이 가능합니다. 다만, 신청한 사유와 무관한 변경은 허용되지 않습니다.

(3) 추가 시험 신청 절차

신청기관은 추가 시험 신청 제품에 해당하는 경우 보안기능 시험 신청서의 추가 시험 신청 항목을 작성하여 시험기관에 제출합니다.

다만, 〈추가 시험 신청 제품〉의 1과 6은 정책기관 · 검증기관이 시험기관, 신청기관 또는 확인서 보유기관에 추가 시험 신청을 요청해야 추가 시험이 진행될 수 있습니다.

(4) 추가 시험 범위

추가 시험의 범위는 추가 시험 대상에 따라 신청기관, 시험기관 및 검증기관이 협의하여 정합니다.

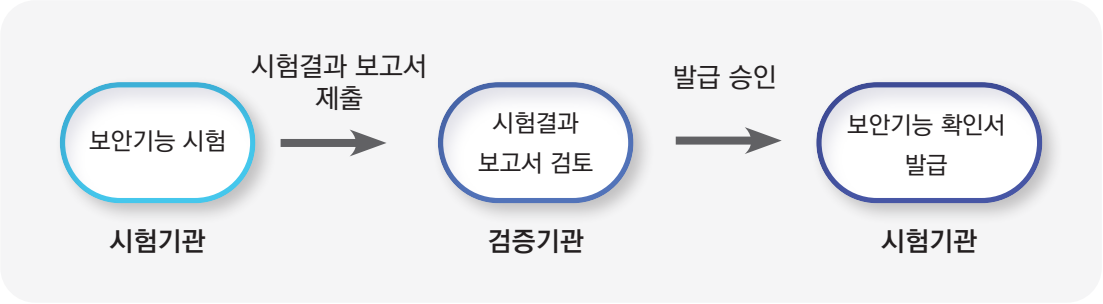
5 보안기능 확인서 발급 단계

Ⅰ 발급 절차

(1) 표준 발급절차

시험기관이 검증기관에 제출한 '**시험결과 보고서**'의 검토가 완료되면 발급 절차가 진행됩니다.

검증기관은 시험의 적절성 등을 검토한 후, 발급 여부를 결정합니다. 발급 승인時 시험기관은 신청 제품에 발급 번호를 부여하고 이를 검증기관에 통보한 후, 신청 업체에 발급번호가 기재된 '**보안기능 확인서**'를 발급하고 '**시험결과 요약서**'를 정책기관에 제출합니다.



(2) 간소화 발급절차

표준 발급절차와 별개로, 정책기관의 역량평가 결과 간소화 발급이 허용된 시험기관은 검증기관의 시험결과 검토를 받지 않고 자체 검토한 후, 신청 업체에 보안기능 확인서를 발급합니다.

(3) CC인증 수용 발급절차

국내용 CC인증[1] 또는 국가정보원장이 인정한 보호프로파일[2]을 준수하여 국제 CC 인증을 획득한 제품은 보안기능 확인서 발급에 필요한 보안기능 시험과 제출문서 제출이 생략됩니다. 평가 · 인증결과의 인정 또는 대체 가능 범위는 〈표 7〉과 같습니다.

〈 표 7. CC인증결과 인정범위 〉

구분	보안기능 시험 제도	인정되는 문서 · 평가
제출문서	제품 설명서	사용자운영 설명서 및 준비절차서
	보안기능 운용설명서	
	보안기능 구현명세서	TOE 설계서 또는 기능명세서
	자체 시험결과서	시험서
	취약점 개선내역서	취약점 분석서 또는 시험기관이 수행한 취약점 분석 결과 문서
보안기능 시험	국가용 보안요구사항에 따른 시험	보안기능 평가

해당되는 CC인증서를 보유한 기관(업체)은 동일 제품에 대한 보안기능 확인서를 발급받고자 할 경우, 신청 제품을 평가한 CC평가기관에 보안기능 시험을 신청합니다.

만약, 신청 제품을 평가한 평가기관이 보안기능 시험 제도의 시험기관 자격이 없거나 정지되어 있다면 검증기관과 협의할 수 있습니다.

시험기관은 신청 업체가 CC 평가 · 인증을 위해 제출한 제출문서의 보안기능 시험 활용에 대한 동의를 받아 해시값 비교 등을 통해 동일 제품 여부를 확인한 후, 보안기능 확인서를 발급[3]할 수 있습니다.

---

1) 「정보보호제품 평가 · 인증 수행규정」 (과학기술정보통신부, 2017.9.12.)의 '정보보호제품 국내용 평가 · 인증 세부 수행절차'에 규정된 절차에 따라 발급된 인증서를 말합니다.

2) 국가용 보호프로파일 등 국가용 보안요구사항이 반영되었다고 인정한 보호프로파일을 의미합니다.

3) CC평가 · 인증 과정에서 국가용 보안요구사항의 만족이 확인되었으므로 별도의 제출문서 검토나 보안기능 시험이 필요하지 않으며 시험결과의 검토도 필요하지 않습니다.

(4) 발급 제한 기준

다음의 '발급 제한기준'에 해당되는 제품에 대해서는 발급이 제한되며, 이미 발급되었더라도 효력이 무효화 됩니다.

〈 발급 제한 기준 〉

1. 반국가단체 · 테러단체 · 대한민국 정부 전산망에 사이버 침해행위를 가할 목적으로 조직되었거나 침해행위를 한 사실이 있는 단체(또는 국가의 정부)로부터 기술 · 자금지원을 받거나, 공동 · 위탁 개발을 통해 개발된 경우
2. 신청 제품이 저작권법에 규정된 지적재산권자의 권리를 침해하거나 신청업체가 제출문서 허위 작성 등의 행위로 시험 · 검증 · 정책 기관을 기망, 정상적인 업무수행을 방해한 경우
3. 대한민국에 수입 · 판매되기 위해 사전에 준수해야할 법적 요건 · 절차를 지키지 않았거나 위계로써 이에 부합한 경우
4. 국제사회로부터 다자간 · 일방적 제재를 받는 국가 · 단체 · 기업이 개발 · 유통에 참여한 경우

검증기관은 신청 제품이 보안요구사항의 필수 항목을 만족하였더라도 국가 전산망의 안전성을 저해하는 취약점 등 보안위해 요인에 대한 보증 시험을 요청할 수 있습니다. 또한, 신청 업체가 보안기능 확인서 발급이 승인되지 않았음에도 발급되었다고 허위로 공표 · 홍보할 경우에는 발급을 즉시 불허할 수 있습니다.

2 보안기능 확인서의 유효 기간

(1) 유효 기간 부여 원칙

신규 발급되는 보안기능 확인서에 대한 효력 부여 원칙은 다음과 같습니다.

〈 효력 부여 원칙 〉

1. 국가용 보안요구사항을 만족하면 일반 보안요구사항이 복합적용 되더라도 효력연장이 없는 5년을 부여합니다.
2. 'CC인증 수용 발급'을 받은 제품과 검증필 암호모듈 탑재가 필수인 제품의 만료일은 해당 CC인증 · 암호모듈검증의 만료일을 초과하지 않습니다.
3. 추가 시험을 통해 신규로 발급되는 보안기능 확인서는 최초 발급된 확인서의 만료일과 동일한 만료일로 발급됩니다. 2025.05.20.

다만, 각 제품 유형의 특성에 따라 국가용 또는 일반 보안요구사항 복합적용 방식이 다양하기 때문에 기본 원칙에 따른 세부적인 효력부여 기준을 마련, 적용하고 있습니다. 적용된 보안요구사항에 따른 유효 기간 부여 원칙의 세부 내용은 〈표 8〉과 같습니다.

〈 표 8. 유효 기간 부여 세부 내용 〉

적용된 보안요구사항		유효 기간
공통 보안요구사항	제품 단위 보안요구사항	
적용 대상이 아님[1]	국가용 보안요구사항	5년
공통보안요구사항(V3.0)	국가용 보안요구사항	
공통보안요구사항(V3.0)	일반 보안요구사항	
공통보안요구사항(V3.0)	국가용 + 일반 복합적용[2]	
기본 보안요구사항(V2.0)	국가용 보안요구사항	
기본 보안요구사항(V2.0)	일반 보안요구사항	2년
적용 대상이 아님	일반 보안요구사항	
구현명세서 적용[3]		

공통 보안요구사항을 배제하고 △제품 단위의 일반 보안요구사항만 준수 △구현명세서 기반 시험 등에 해당된 제품은 효력연장이 없는 2년을 부여합니다.

공통 보안요구사항을 배제하고 일반 보안요구사항만 적용이 가능한 제품 유형은 가상 인프라 관리제품[4]만 허용됩니다. 부여된 효력은 효력 정지 · 취소 사유가 발생하지 않는 이상, 만료일까지 유지됩니다.

---

1) 공통보안요구사항의 적용 대상이 아닌 제품유형 입니다.(예 : 네트워크 장비, 패스워드 관리제품 등)

2) 제품 단위끼리의 복합적용뿐아니라 제품 단위 + 기능 단위, 기능 단위 + 기능 단위 복합 적용이 모두 포함됩니다.

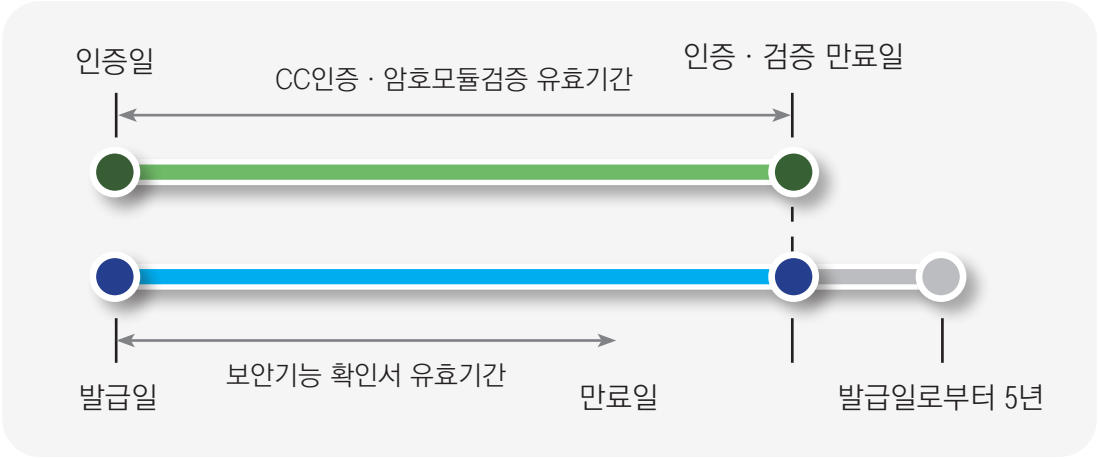
3) 이 문서의 21페이지를 참고하십시오.

4) '가상 인프라 관리'란, 가상 서버를 관리하는 제품유형을 의미합니다. (가상 데스크톱 관리는 '가상화 관리제품' 국가용 보안요구사항이 적용되므로 해당되지 않습니다.)

(2) 사전 인증 제품의 유효기간 부여

'CC인증 수용 발급'절차에 따라 발급되거나, 검증필 암호모듈의 탑재가 필수인 제품은 다음 〈그림 6〉과 같은 방식으로 유효기간이 부여됩니다.

〈 그림 6. 사전 인증 제품에 대한 유효 기간 부여 〉



'CC인증 수용 발급'을 받은 제품중 검증필 암호모듈 탑재가 필수인 제품은 CC인증과 검증필 암호모듈의 만료일 중에서 가장 먼저 도래하는 날이 보안기능 확인서의 만료일이 됩니다.

'표준 발급' 또는 '간소화 발급'절차를 거쳐 발급된 제품중 검증필 암호모듈 탑재가 필수인 제품은 발급일로부터 5년째 되는날과 검증필 암호모듈의 만료일 중에서 가장 먼저 도래하는 날이 보안기능 확인서의 만료일 입니다.

3 보안기능 확인서의 유효성 인정

보안기능 확인서의 효력은 발급 당시의 형상에 한정되며 아래 사항에 해당된 경우, 발급된 보안기능 확인서의 유효성을 인정하지 않습니다.

〈 효력 부여 원칙 〉

1. 발급 당시의 제품 명칭 또는 버전이 변경된 경우(소수점 이하의 변경도 포함)
2. 보안기능이 변경되거나 추가 · 제거된 경우
3. 보안기능에 중대한 영향을 미치는 비보안기능 · 운영환경이 변경된 경우
4. 발급 제한 기준[1]에 해당된 경우

1) 이 문서의 27페이지를 참고하십시오.

6 발급 제품 사후 관리

1 보안기능 확인서 재발급

신청 업체는 ❶보안기능 확인서의 분실 · 훼손, ❷보안기능 확인서 보유기관 명칭 변경, ❸보안기능 확인서 권리의 양도 · 양수 등의 경우, 시험기관에 '**보안기능 확인서 재발급 신청서**'를 제출하여 재발급을 신청할 수 있습니다. 재발급된 보안기능 확인서의 유효기간은 이전(以前)에 발급된 보안기능 확인서의 유효기간과 동일하게 부여합니다.

2 발급 제품의 운용 환경을 추가할 경우

(1) 클라우드 환경 또는 운영체제 추가 2025.05.20.

보안기능 확인서 보유 업체가 발급 제품의 운용 환경에 클라우드 환경 또는 운영체제를 추가하고자 할 경우, 추가 시험을 요청할 수 있습니다.

클라우드 환경을 추가하기 위해서는 「클라우드 운영환경 공통보안요구사항」를 준수해야 합니다. 제품이 클라우드 환경에서 설치 및 동작하기 위해서 일부 형상을 제한적으로 변경하는 것을 허용합니다. 다만 제품의 기능 개선, 취약점 패치 등에 이유로 형상을 변경하는 것은 불가합니다.

운영체제를 추가하기 위해서는 제품의 형상이 발급 제품과 같고 추가할 운영체제가 발급 제품의 운영체제와 동일한 계열의 범용 운영체제여야 하며 보안패치 서비스가 종료된 운영체제만 단독으로 추가할 수 없습니다.

(2) 발급된 제품의 하드웨어 모델 추가

보안기능 확인서 보유 업체는 보안기능 확인서가 발급된 제품과 동일한 시리즈에 하드웨어 모델이 추가될 경우, 보안기능 확인서에 하드웨어 모델의 추가 기재를 요청할 수 있습니다.

〈별지 4. 하드웨어 모델 추가〉 절차를 참고하십시오.

하드웨어 모델의 추가를 위해 보안기능 확인서 보유 업체는 추가 시험을 요청할 수 있습니다. 시험기관은 추가된 하드웨어 모델에 대한 시험이 필요한 경우 시험 범위를 검증기관과 협의한 후, 시험을 수행하고 그 결과에 따라 보안기능 확인서를 신청 업체에 발급합니다.

〈 하드웨어 모델 추가 기재 허용기준 〉

1 보안기능 확인서에 기재된 하드웨어 모델과 동일한 CPU 제조사(또는 아키텍쳐)인 경우

2 보안기능 확인서에 기재된 하드웨어 모델에 공통으로 탑재된 NIC(네트워크 인터페이스 카드)에 비해 동일하거나 유사한 기능의 NIC를 탑재한 경우

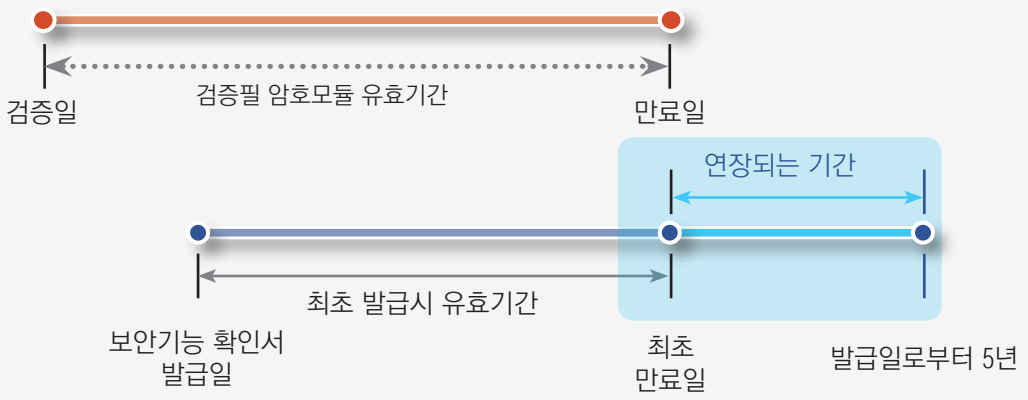
3 그 외 정책 · 검증기관이 승인한 경우

3 검증필 암호모듈 효력 만료 제품의 유효기간 연장

(1) 표준 · 간소화 발급절차에 따른 발급 제품

검증필 암호모듈 탑재가 필수인 제품에 해당하는 제품으로서 탑재된 검증필 암호모듈이 만료된 제품은 암호모듈을 교체하지 않더라도 일부 암호 기능에 대한 추가 시험을 통해 보안기능 확인서의 효력을 발급일로부터 5년까지 연장할 수 있습니다.

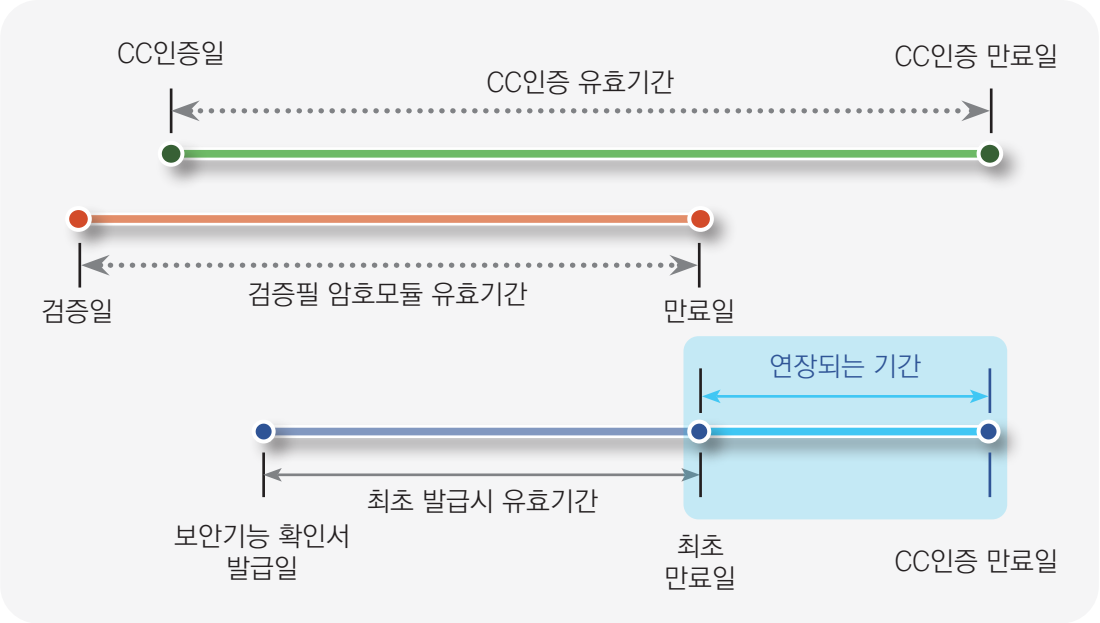
〈 그림 7. 표준 · 간소화 발급 제품의 유효기간 연장 〉



(2) CC인증 수용 발급절차에 따른 발급 제품

검증필 암호모듈 탑재가 필수인 제품 유형으로서 검증필 암호모듈을 탑재하고 CC인증을 받은 제품은 만료된 암호모듈을 교체하지 않더라도 일부 암호 기능에 대한 추가 시험을 통해 보안기능 확인서의 효력을 원래 CC인증의 만료일까지 연장할 수 있습니다.

〈 그림 8. CC인증 수용 발급 제품의 유효기간 연장 〉



4 권리의 양도(양수) · 이전 및 종료

보안기능 확인서 보유 업체가 소유한 보안기능 확인서의 권리를 계약에 의해 양도 또는 이전(移轉)하였을 경우, 양수업체(인수업체)는 '**보안기능 확인서 재발급 신청서**'와 양방의 '**사업자등록증**' 사본 각 1부 및 권리의 양도 또는 이전(移轉) 사실이 기재된 '**계약서**'[1] 사본 1부를 시험기관에 제출합니다.

보유 업체의 해산, 폐업, 사업종료 등의 사유가 발생한 경우, 근무일수 기준 5일 이내에 시험기관에 보유한 보안기능 확인서의 효력 종료를 신청해야 합니다.

5 효력 정지

검증기관은 다음 사항에 해당할 경우 발급 제품의 보안기능 확인서 효력을 정지할 수

1) 계약서에 양방 또는 일방의 영업기밀이 포함된 경우, 양수(인수)기관은 시험기관과 협의 후, 해당 해당 부분을 삭제하여 제출할 수 있습니다. 이 경우, 양수(인수)기관은 계약서 사본이 원본과 동일함을 보증해야 합니다.

있습니다. 이와 별개로 정책기관은 중대한 취약점이 발견되어 신속한 대응이 필요한 경우, 검증기관에 해당 제품의 보안기능 확인서 효력 정지를 요청할 수 있습니다.

보유 업체는 효력 정지 결정이 있을 경우, 지체없이 보안기능 확인서를 시험기관에 반납해야 하며 효력 정지가 만료되면 시험기관은 효력 정지 만료일의 다음날에 해당 보안기능 확인서를 보유 업체에 반환합니다.

다만, 반환일이 휴일인 경우 도래하는 첫 근무일에 반환합니다. 효력 정지 기간은 연장될 수 있으나 정지 기간의 총 합은 1년을 초과하지 않습니다.

〈 효력 정지 기준 〉

1 보유 업체가 정책기관 또는 검증기관으로부터 취약점 개선을 요청받고 합의된 시일(예 : 15일) 이내 개발을 완료하지 않은 경우

2 보유 업체가 정책기관과 합의된 기간 내에 국가 · 공공기관에 납품된 제품의 취약점을 개선하지 않은 경우

3 보유 업체가 보안기능 확인서를 국가 · 공공기관 납품 이외의 용도로 활용하는 등 준수 사항을 위반하였을 경우

4 보유 업체의 요청이 있는 경우

6 효력 취소

검증기관은 발급 제한 기준 또는 다음 사항에 해당하는 제품에 대해 보안기능 확인서 효력을 취소할 수 있습니다. 보유 업체는 효력 취소 결정이 있을 경우, 지체없이 보안기능 확인서를 시험기관에 반납해야 합니다.

〈 효력 취소 기준 〉

1 보유 업체가 제출물을 허위로 제출하여 보안기능 확인서를 발급받은 사실이 확인된 경우

2 보유 업체가 정책 · 검증기관의 취약점에 대한 개선 요청을 거부하는 경우

3 보유 업체가 보안기능 확인서를 위 · 변조 등 임의 조작한 경우

4 보유 업체가 발급 제품의 형상 또는 탑재되는 H/W 모델이 변경되었음에도 기존 발급된 보안기능 확인서를 임의로 행사하는 등 오 · 남용할 경우

5 시험기관이 간소화 발급 절차를 준수하지 않고 부실하게 발급한 경우

7 일반 보안요구사항의 작성 및 활용

1 일반 보안요구사항 개요

'일반 보안요구사항'이란, '보안기능 시험'을 신청한 제품중에서 적용 가능한 국가용 보안요구사항이 제정되지 않았거나 제품의 보안기능이 현행 국가용 보안요구사항과 현저히 다를 경우, 해당 제품의 시험을 위해 개발업체 등이 직접 작성하는 보안요구사항입니다.

2 일반 보안요구사항의 활용

(1) 일반 보안요구사항 제안

일반 보안요구사항은 개발업체, 시험기관, 관련 전문가 등 누구나 작성할 수 있습니다. 작성인(개발 업체)은 '국가용 보안요구사항'의 구조를 참고하여 일반 보안요구사항을 작성합니다.

작성인(개발 업체)은 작성이 완료된 '**일반 보안요구사항**'과 '**일반 보안요구사항 제안서**' 각 1부를 시험기관을 통해 검증기관에 제안합니다. 정책기관은 제안된 일반 보안요구사항을 검증기관과 검토, 승인 여부를 결정합니다. 일반 보안요구사항은 승인된 날로부터 신청 제품의 시험에 적용될 수 있습니다.

여 백

8 시험기관 및 시험원

Ⅰ 시험기관

(1) 시험기관 자격 요건

시험기관이 갖추어야 할 자격요건은 다음과 같습니다.

〈 자격 요건 〉

1. 국내 법인으로서 국가기술표준원의 '한국인정기구'(KOLAS)로부터 '3.008 유/무선 통신기기' · '3.012 소프트웨어 시험' 등 관련 분야의 시험기관 인정서를 교부받고 홈페이지에 그 사실이 공지된 기관
2. 보안요구사항에 따라 발급 신청 제품을 시험할 수 있는 설비와 4인 이상의 시험인력이 상시 근무하는 시험부서를 국내에서 운영하는 기관
3. 출입 통제 및 망 분리 등에 대한 명문화된 자체 보안정책을 수립 · 시행하고 있는 기관
4. 국제표준규격(ISO/IEC 17025)에 규정된 공정성을 확보하며 자체 품질 가이드 및 절차서를 구비한 기관
5. 정책기관이 제도 운영상 시험기관으로 지정이 필요하다고 인정한 기관

시험기관 지정을 희망하는 기관은 검증기관에 관련 절차와 제출 문서를 문의하고 시험기관 지정을 신청할 수 있습니다. 검증기관은 시험기관에 대한 역량 평가를 통해 간소화 발급 기관을 지정할 수 있으며 그외 시험기관 관리 업무를 수행합니다.

2 시험원

(1) 시험원 자격 요건

시험원은 시험기관에 소속되어 보안기능 시험을 수행할 수 있는 자격을 지닌 사람으로서 다음 요건 중의 어느 하나를 충족해야 합니다.

〈 자격 요건 〉

1. IT분야 학사 이상의 학위를 보유
2. 정보보호제품 · 네트워크 장비의 개발 · 시험 · 품질보증 등 유관업무 수행 경력 3년 이상
3. 국내 · 외 전문기관 또는 업체에서 발급한 신청 제품의 시험 · 운용 등과 관련된 IT 자격증 보유

(2) 시험원 자격 부여

검증기관은 시험기관에 소속 직원 중에서 시험원 자격 요건을 만족한 사람을 '수습 시험원'으로 임명할 수 있습니다.

수습 시험원은 분야에 따라 '정보보호제품 시험원'과 '네트워크 장비 시험원'으로 임명될 수 있으며 이를 위해 정보보호제품과 네트워크 장비에 대한 시험을 각 3회 이상 참여하고 2회 이상 직접 수행[1]하여 독립적으로 '**시험결과보고서**'를 작성해야 합니다.

끝.

1) CC평가자로서 수행한 시험경력도 인정됩니다.

[별표 1]

보안기능 확인서 발급 가능 유형(예시)

연번	제품군	제품 유형	비고
1	침입차단제품군	침입차단시스템	
2		웹 방화벽	
3		DDoS 대응장비	
4		인터넷전화 보안제품	
5		*제품유형 자율 기재*	제품군에 속한 새로운 제품유형
6	침입방지제품군	침입방지시스템	
7		무선 침입방지시스템	
8		*제품유형 자율 기재*	제품군에 속한 새로운 제품유형
9	구간보안제품군	가상사설망제품	
10		네트워크 접근통제제품	
11		망간 자료전송제품	
12		무선랜 인증제품	
13		구간암호화제품	
14		*제품유형 자율 기재*	제품군에 속한 새로운 제품유형
15	전송자료보안 제품군	스팸메일차단시스템	
16		소프트웨어 기반 보안USB제품	
17		호스트 자료유출방지제품	
18		네트워크 자료유출방지제품	
19		메일암호화제품	
20		*제품유형 자율 기재*	제품군에 속한 새로운 제품유형
21	보안관리제품군	스마트카드(COS 포함)	
22		통합보안관리제품	
23		소스코드 보안약점 분석도구	
24		통합로그관리제품	
25		패치관리시스템	
26		DB접근통제제품	

연번	제품군	제품 유형	비고
27	보안관리제품군	시스템접근관리제품	
28		패스워드관리제품	
29		통합인증제품(SSO)	
30		*제품유형 자율 기재*	제품군에 속한 새로운 제품유형
31	가상화제품군	가상화관리제품	
32		*제품유형 자율 기재*	제품군에 속한 새로운 제품유형
33	엔드포인트보안 제품군	디지털 복합기	
34		안티바이러스제품	
35		스마트폰 보안관리제품	
36		운영체제(서버) 접근통제제품	
37		엔드포인트 위협탐지 및 대응제품	EDR 제품
38		APT 공격 대응 제품	
39		문서암호화제품(DRM)	
40		DB 암호화제품	
41		*제품유형 자율 기재*	제품군에 속한 새로운 제품유형
42	네트워크 장비 제품군	L3 스위치	
43		L4 스위치	
44		L7 스위치	
45		라우터	
46		SDN 컨트롤러	
47		SDN 스위치	
48		*제품유형 자율 기재*	제품군에 속한 새로운 제품유형
49	양자암호통신장비 제품군	양자키 분배장비(QKD)	
50		양자키 관리장비(QKMS)	
51		양자통신 암호화장비(QENC)	
52		*제품유형 자율 기재*	제품군에 속한 새로운 제품유형

※ 제품군에 속한 새로운 제품유형은 「보안기능 시험 신청서」에 해당 유형을 자율 기재합니다.

끝.

[별지 1]

일반 보안요구사항 서식

〈 제품 명칭 〉

일반 보안요구사항

V 0.0

202x년 0월 0일

〈 작성 기관(작성 업체) 명칭 〉

[문서 정보]

작성 기관	*〈작성 기관 명칭〉 작성자 1, 작성자 2 . . .*
시험 기관	*〈시험 기관 명칭〉 검토한 시험원 1, 검토한 시험원 2 . . .*

[문서 이력 관리]

문서 버전	개정 내용	날 짜

– 하 략 –

목 차

– 하 략 –

1. 제품 소개

1.1 제품 개요

가. 제품 개요에는 제품이 제공하는 보안기능을 상위 수준으로 분류하여 서술한다.

- 작성기관이 분류한 보안기능 단위로 '2 보안요구사항'을 서술한다.

나. 제품에 국가용 보안요구사항의 '제품 보안요구사항'을 적용할 수 없는 이유를 서술한다.

- 국가용 보안요구사항에 정의되지 않은 새로운 제품군/제품유형인 경우 기존 제품군(제품 유형)에 속하지 않는다는 타당한 근거를 함께 제시한다.

다. 제품과 관련된 일반적인 정보를 찾을 수 있는 공개된 자료에 대한 참조정보를 서술한다.

- 작성기관 홈페이지, 공개된 브로셔 등에 대한 정보가 제공되어야 하며, 공개된 정보가 없는 경우 이유를 서술한다.

1.2 운용 환경

가. 제품이 설치 및 운용되는 환경을 간략히 서술한다.

나. 제품의 보안기능을 사용하기 위해 식별 및 인증이 필요한 사용자(예: 인가된 관리자, 일반사용자 등) 역할을 정의한다.

- 제품과 연동하는 외부 IT 실체 중 제품으로부터 인증을 받아야 하는 실체가 존재하는 경우 포함하여 서술한다.

1.3 가정 사항

제품을 안전하게 설치 및 운용하기 위해 반드시 준수되어야 하는 전제조건을 서술한다.

1.4 국가용 보안요구사항의 적용

제품에 적용할 수 있는 △공통보안요구사항 △제품 보안요구사항 △기능 보안요구사항을 식별한다.

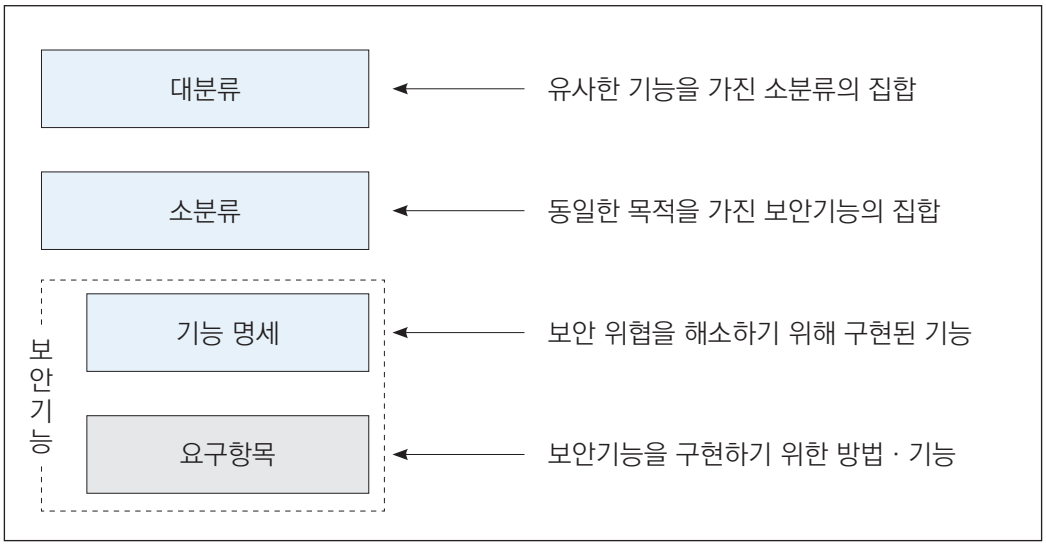
1.5 일반 보안요구사항 참조

제품과 유사한 다른 제품의 일반 보안요구사항이 이미 존재하는 경우 이를 식별한다.

- 기존 일반 보안요구사항과 비교하여 동일한 보안요구사항, 유사하나 일부 다른 보안요구사항, 새롭게 정의한 보안요구사항 등을 서술해야 한다.

2. 보안요구사항

가. 아래 '국가용 보안요구사항'의 구조를 참고하여 제품의 보안요구사항을 서술한다.



(* 위 그림은 일반 보안요구사항의 구조에 대한 이해를 돕기위해 첨부한 그림이기 때문에 일반 보안요구사항의 본문에 포함할 필요가 없음.)

나. 대분류 보안기능으로 '보안관리' 및 '감사기록'은 반드시 포함해야 하며, 포함하지 않는 경우 타당한 이유를 설명해야 한다.

다. 일반 보안요구사항은 구현된 제품을 기반으로 정의하므로 '조건부 필수' 또는 '선택' 보안요구사항은 도출하거나 기재하지 않는다.

라. '기능 명세' 작성시 제품이 구현한 보안기능만을 서술한다.

– 제품의 운영환경 또는 제품과 연동하는 외부 IT 실체가 제공하는 보안기능을 서술하지 않아야 한다.

마. '기능 명세'에 대한 세부 구현 방법이나 기능으로 '요구항목'을 서술한다.

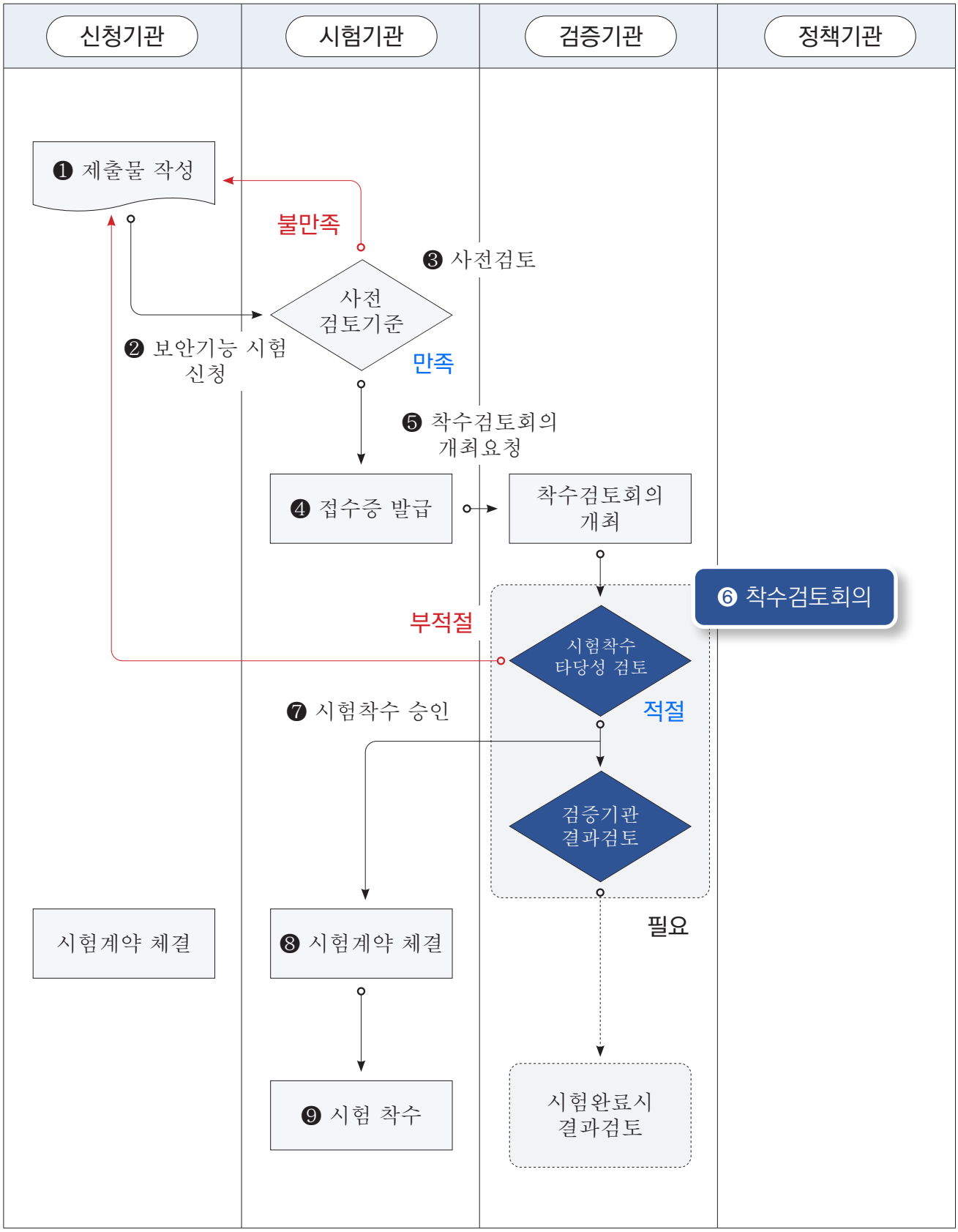
– '기능 명세'만으로 세구 구현 방법이나 기능에 대한 설명이 충분한 경우 '요구항목'을 생략할 수 있다.

바. '기능 명세' 및 '요구항목'에 대한 해석으로 '점검시 유의사항'을 서술할 수 있다.

– 작성기관과 시험기관은 '기능 명세' 및 '요구항목'을 일관되게 해석하고 시험에 적용하기 위한 유의사항을 서술할 수 있다.

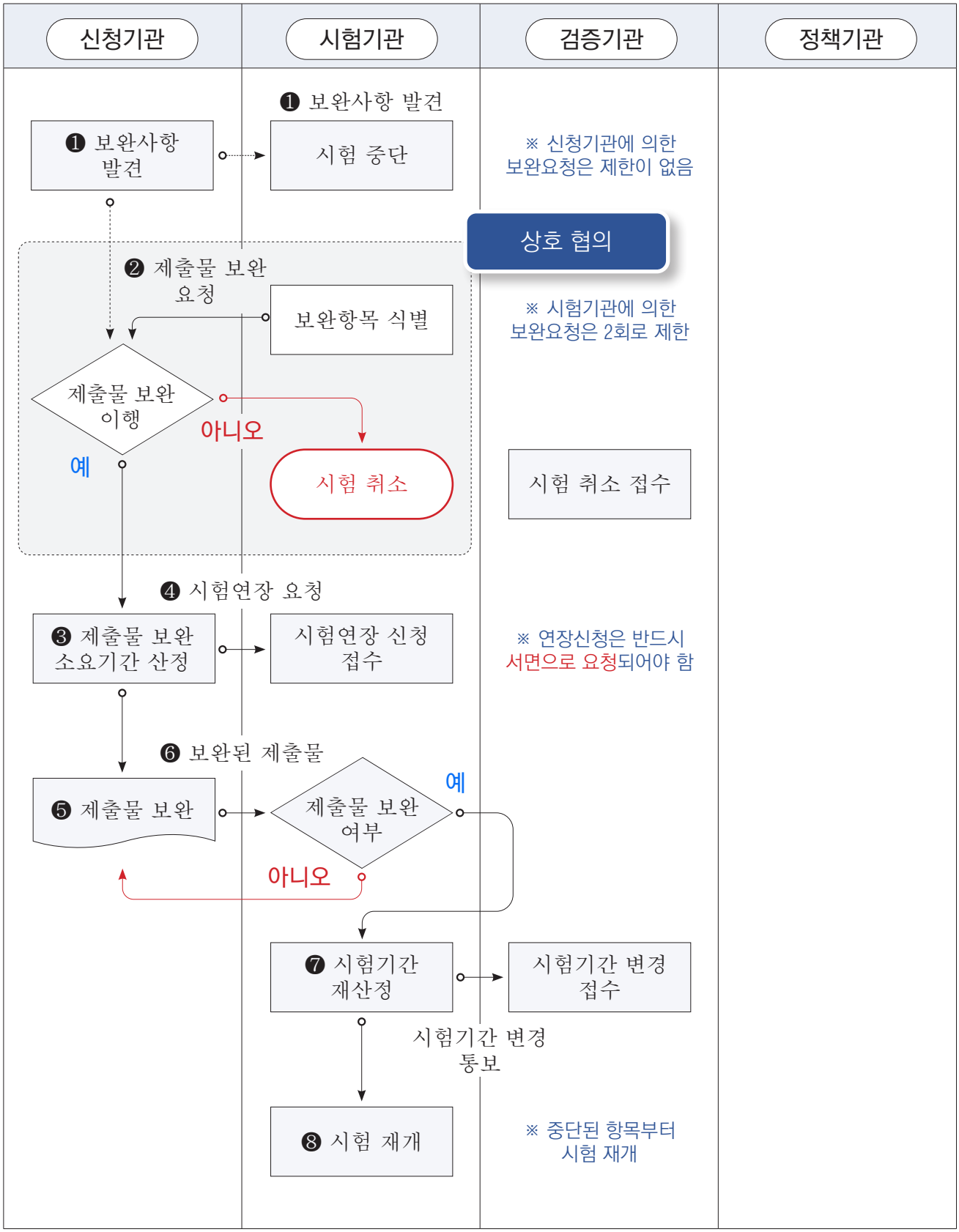
[별지 2]

신규 시험신청 및 착수검토 절차



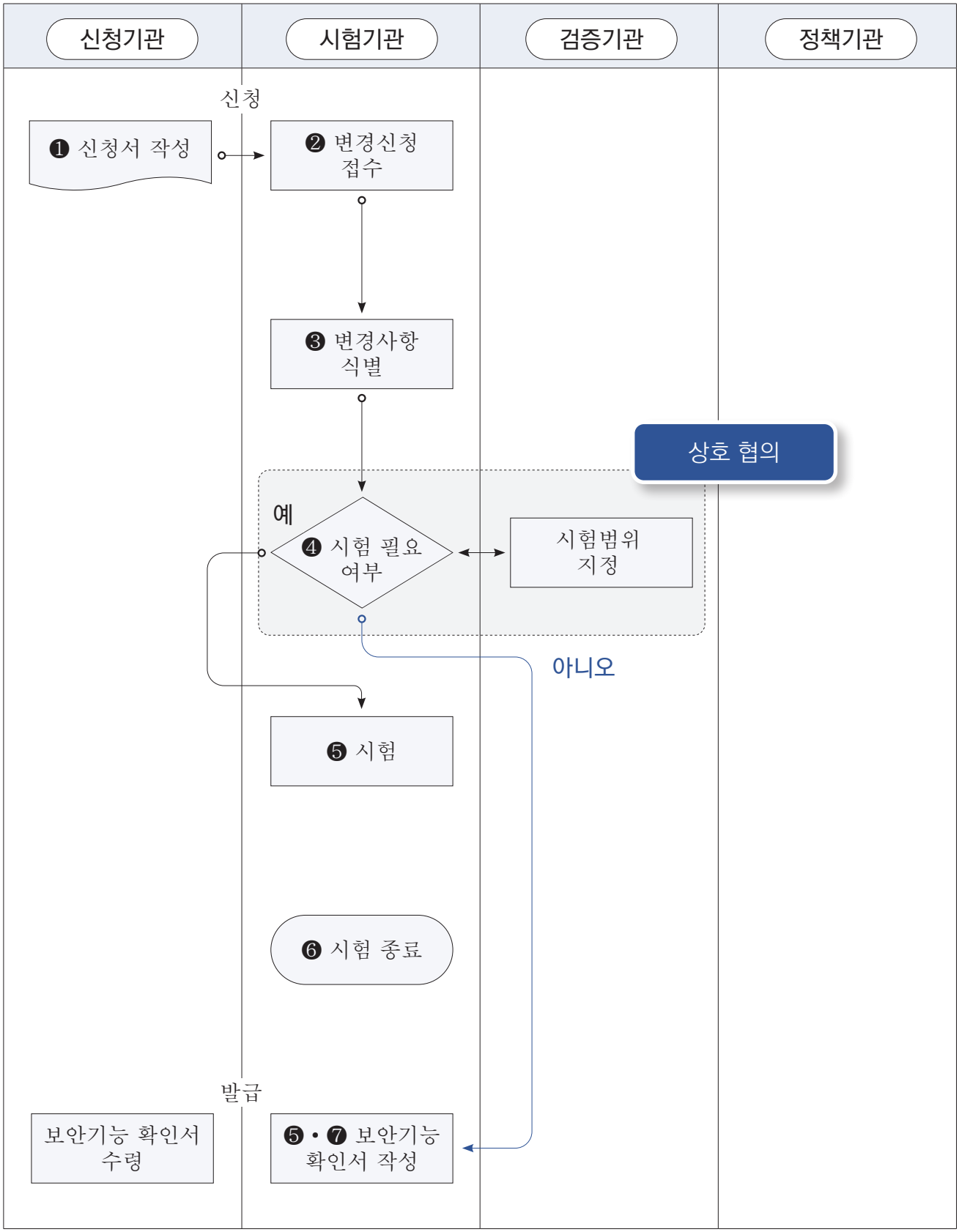
[별지 3]

시험중 제출물 보완 절차



[별지 4]

하드웨어 모델 추가 절차



[별지 5]

시험결과 요약서

이 문서는 YYYY년 MM월 DD일에 발급된 보안기능확인서(VSFT-OOO-00000000)의 부속문서로 △발급 제품의 정보 △시험의 내용 · 결과 △ (국가용 보안요구사항 만족 여부 및/또는 일반 보안요구사항/구현명세서 기반 시험기준 사용 여부)을/를 도입 기관에 제공하기 위해 작성되었습니다.

(추가 시험 시 다음 문구 추가)※ 본 시험은 旣 발급된 보안기능확인서(VSFT-OOO-00000000) '발급제품명'의 시험 결과를 수용하고 추가 시험을 수행한 결과입니다.

[발급제품 식별정보]

제품군	
제품유형	
제품명	
시험기준	
시험결과 보고서	
제품 설명서	
보안기능 구현명세서	
신청기관	
제 조 사	
개발방식	
생산방식	
시험기관	
만료일	

상기와 같이 보안기능 시험이 완료되었음을 확인합니다.

〈시험기관 명칭〉

☐ 식별정보

발급제품의 상세 버전, 구성요소, 유형 및 배포 방법은 다음과 같습니다.

구분		식별정보(물리적 범위)	유형	배포 방법
제품				
세부버전				
구성 요소	구성요소 A			
	구성요소 B			
	제품 설명서			

☐ 해시값

발급제품의 해시값은 다음과 같습니다.

구성요소	해시값(SHA 512)
구성요소 A 식별정보 (물리적 범위)	
구성요소 A 식별정보 (물리적범위)	
제품 설명서 식별정보 (물리적범위)	

☐ 운용 환경

발급제품의 운용 환경은 다음과 같습니다.

- 하드웨어 모델
- 구성요소 운용 환경
- 관리자 PC 운용 환경

☐ 시험기준

발급제품이 준수한 시험기준과 제공하는 보안기능은 다음과 같습니다.

구분	분류	기능명세 항목

※ 국가용 보안요구사항을 준수한 발급제품은 '필수' 기능명세를 모두 만족합니다. 다만, 제품의 구현 형태 등의 이유로 상기 기능명세 항목에 포함되지 않을 수 있습니다.

□ 비고

발급제품 및 시험기준과 관련된 참고사항입니다.

- 검증필 암호모듈

구성요소	암호모듈명	세부정보	
		검증번호	
		개 발 사	
		모듈형태	
		검 증 일	
		효력만료일	
		보안수준	

부 록 시험중 보완요청이 빈번한 항목

이 부록에 수록된 내용은 신청 제품들의 완성도에 따라 변경되거나 삭제될 수 있습니다.

Ⅰ 보안기능 구현명세서

(1) 하드웨어 · 소프트웨어 자체 검사 방법에 대해 미흡한 서술

□ 해당하는 국가용 보안요구사항

일부 네트워크 장비 신청 업체의 「보안기능 구현명세서」에서 '하드웨어 · 소프트웨어 자체 검사'에 대한 서술이 미흡하여 보완요청이 빈번하게 발생합니다. 해당하는 보안요구사항은 〈표 1〉과 같습니다.

〈 표 1. 보안기능 구현명세서에 서술이 미흡한 보안요구사항 〉

보안요구사항	보안기능
스위치 · 라우터	5.1.1 장비 구동(Power On)시 주요 하드웨어의 오류를 확인하는 자체검사 기능을 제공해야 한다.
	5.1.2 장비 구동(Power On)시 펌웨어 로딩 후 주요 프로세스의 오류를 확인하는 자체검사 기능을 제공해야 한다.
	5.2.1 장비 구동(Power On)시 펌웨어 이미지 또는 주요 소프트웨어에 대한 무결성 검사 기능을 제공해야 한다.
SDN 스위치	5.1.1 장비 구동(Power On)시 주요 하드웨어의 오류를 확인하는 자체검사 기능을 제공해야 한다.
	5.1.2 장비 구동(Power On)시 펌웨어 로딩 후 주요 프로세스의 오류를 확인하는 자체검사 기능을 제공해야 한다.
	5.2.1 장비 구동(Power On)시 펌웨어 이미지 또는 주요 소프트웨어에 대한 무결성 검사 기능을 제공해야 한다.

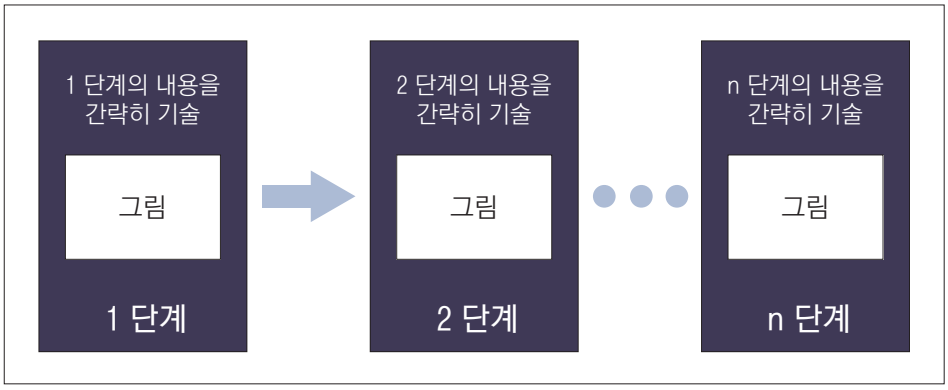
〈 표 1. 보안기능 구현명세서에 서술이 미흡한 보안요구사항 〉

보안요구사항	보안기능
SDN컨트롤러	5.1.1 컨트롤러 주요 프로세스에 대한 오류를 확인하는 자체검사 기능을 제공해야 한다.
	5.2.1 컨트롤러 실행 또는 구동시 소프트웨어에 대한 무결성 검사 기능을 제공해야 한다.

□ **서술되어야 하는 항목**

하드웨어의 경우, 제품의 구동(Power On) · 부팅 절차를 단계별로 나누어 상세하게 서술합니다. 소프트웨어의 경우, 펌웨어 이미지 또는 프로세스(사용자 식별 · 인증, 보안 관리, 주요 서비스, 감사기록 등)에 대한 무결성 확인방법 및 절차를 단계별로 나누어 상세하게 서술합니다. 무결성 확인 방법으로는 전자서명 또는 해시값 비교 등이 있습니다. 시험원의 이해를 돕기위해 아래와 같은 그림을 첨부할 수 있습니다.

〈그림 1. (예시) OOO에 대한 절차도 〉



(2) **구현된 보안기능에 대해 전체적으로 미흡한 서술**

제품에 구현된 보안기능에 대해 구현의 결과만을 간략하게 서술하는 것이 아닌, 보안기능이 어떻게 구현되었고, 어떤 메커니즘으로 작동하는지를 서술해야 합니다.

예를 들어 '인증정보 재사용 방지'의 경우, '제품이 인증정보 재사용을 하지 않는다.'고 서술할 뿐 인증정보 재사용 방지가 어떤 메커니즘으로 작동하는지 서술하지 않는다면 시험원이 제품을 이해하는데 도움이 되지 않습니다.

아래 〈표 2〉를 참고하십시오.

〈표 2. (예시) 보안기능에 대한 서술 〉

구분	서술 내용
부실한 서술	“제품이 난수를 사용하여 인증정보의 재사용을 막습니다.”
올바른 서술	o △세션키 생성 · 관리 방식 △재사용 방지 프로세스의 시퀀스 △난수발생기의 명칭 등을 서술 o 식별 · 인증 프로세스가 작동하는 절차를 단계적으로 설명하고 필요한 경우, 절차도를 그려서 첨부

2 제품의 보안기능

(1) 주요 보안기능의 구현 미흡

□ 국가용 보안요구사항을 고려하지 않은 제품 설계

보안기능 확인서 발급 소요기간을 줄이는 가장 효과적인 방법은 △시험기준인 국가용 보안요구사항에 대한 이해 △국가용 보안요구사항[1]을 만족하는 보안기능 구현입니다.

구현된 보안기능 중에서 국가용 보안요구사항을 만족하는 기능의 비중이 높을수록 보안기능 확인서가 신속하게 발급되지만, 제품 설계시 국가용 보안요구사항을 고려하지 않고 설계되는 경우가 많아, 보완요청이 빈번하게 발생합니다.

아래 〈표 3〉을 참고하십시오.

〈표 3. (예시) 보완요청이 빈번한 보안기능 〉

보안기능	미흡한 사항
식별 · 인증 기능	△n회 인증실패시 계정잠금 기능 부실 △인증정보 재사용 방지 기능 부실 △인증실패 사유 노출 등
비밀번호 생성 · 저장	△연속된 문자 · 숫자 입력 제한(1234, qwer 등) 미준수 △비밀번호 암호화 미흡 △salt 이용시 난수발생기 미적용 등
감사기능	△보안관리 기능 수행시 감사기록 미생성 △암호연산 관련 감사기록 미생성 등

끝.

1) 국가용 보안요구사항에 정의되지 않은 새로운 보안기능(신기술)일지라도 정책 · 검증기관과 협의를 통해 시험을 진행할 수 있습니다.