국가용 보안요구사항 V3.0 기반의

국내용 시험서 작성 가이드 V1.0

2025. 4. 11.

과학기술정보통신부

kisia 한국정보보호산업협회

[문서 변경이력]

버전	일 자	변경 내용
1.0	2025. 4. 11.	o v1.0 문서 배포

목 차

1. 개요

1.1. 시험서 참조

☞ *시험서 식별을 명확하게 할 수 있도록 문서명, 문서버전 등 취약성 분석서에 대한 식별정보 서술*

문서명	*OOO 시험서*
문서버전	*X.X*
파일명	*신청대상제품명-문서명-버전-날짜(세부버전 등).hwp*
보증컴포넌트	*ATE_IND.2*
작성자	*(주) XXX*
발간일	*20XX.XX.XX*
주요용어	*침입차단시스템, 방화벽, FW, Firewall 등*

참고사항	▶ 시험서는 TOE의 모든 보안기능이 시험되었음을 입증하기 위한 내용을 기술해야 한다. ▶ 시험서는 작성기관의 자체 양식을 이용하여 작성 될 수 있으며, 각 시험항목을 시험하기 위한 시험환경, 시험조건, 시험절차 등 시험계획 및 시험 수행결과를 제공해야 한다. ▶ 신규로 제출물을 작성하는 경우 시험서 작성자는 본 가이드를 참고하여 시험서를 작성할 수 있다.

1.2. 목적

☞ *시험서는 국가용 보안요구사항 따라 구현된 기능을 수행하기 위한 시험항목 식별하고, 각 시험항목을 시험하기 위한 시험환경, 시험조건, 시험 절차 등 시험계획을 기술해야 한다. 또한, 시험계획에 따라 수행된 시험결과를 제공하여 개발자 시험에 대한 증거를 제공하기 위한 자료로 사용된다.*

예) 본 문서는 [000 V1.0]에 대한 시험서로, TOE에서 제공하는 모든 보안기능을 시험하기 위한 시험항목을 식별하고 보안기능이 정확하게 구현됨을 입증하기 위해 작성되었습니다.
또한, 국가용 보안요구사항을 만족하고 있음을 입증하기 시험항목과의 대응관계를 제공합니다.

1.3. 시험서 구성

시험서는 다음과 같이 구성되어 있다.

1장은 시험서 개요로 시험서의 목적, 구성, 참조문서 등을 기술한다.

2장은 시험환경, 시험범위, 시험 항목 및 결과에 대한 내용을 기술한다.

3장은 각 시험항목에 대한 시험 절차 및 시험 결과에 대한 상세 내역을 기술한다.

1.4. 참조 문서

☞ *일반적으로 시험(ATE_IND.2)에서 요구되는 입력문서를 참조로 한다.*

- OOO V1.0” 보안목표명세서 VX.X
- OOO V1.0” 사용자 운영설명서 VX.X

2. 시험계획

본 장에서는 TOE에서 제공하는 시험환경, 시험범위, 시험항목 및 결과 등 시험 계획에 대한 내용을 기술한다.

2.1. 시험환경

☞ TOE에 대한 설명 및 시험환경, 시험에 사용된 시험도구 등을 기술하고, 시험범위 및 시험 항목 및 시험결과에 대한 요약 정보를 제공한다.

2.1.1 TOE

☞ 시험에 사용된 TOE 정보를 기술한다.

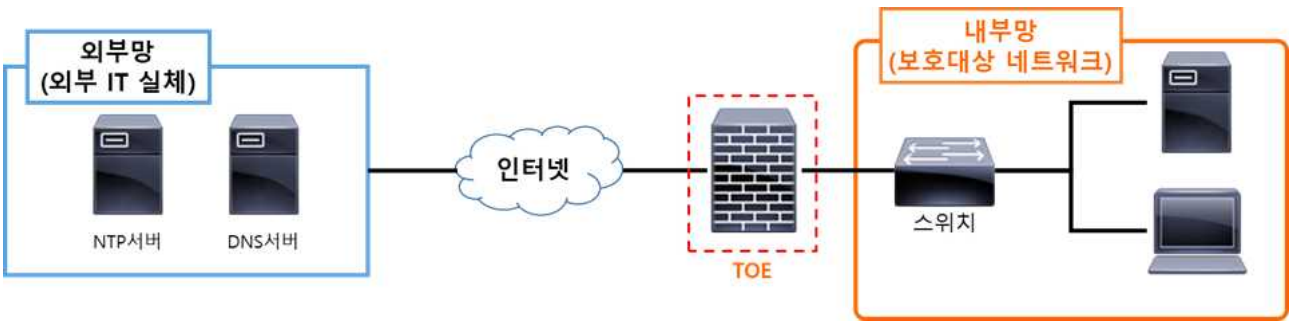
시험에 사용되는 TOE는 다음과 같이 식별된다.

TOE 명칭		*OOO*
TOE 버전		*Vx.x*
TOE 구성요소	HW	*XXX (☞ TOE 유형이 하드웨어 일체형인 경우 SW가 설치되는 플랫폼 명)*
	SW	*XXX Vx.x (빌드버전 : x.x.xxxx.x)*
	문서	*XXX 설치매뉴얼 Vx.x* *XXX 운영매뉴얼 Vx.x*

2.1.2 시험환경 구성

☞ TOE 시험을 위해 사용된 시험환경을 기술한다.

예) TOE는 네트워크간 전송되는 패킷들을 정해진 규칙에 따라 차단하거나 통과시켜 공격자로부터 내부 자산을 보호하는 목적으로 사용되는 침입차단 시스템으로, TOE의 시험환경은 다음과 같다.



- TOE

구 분	내 용
TOE	000 V1.0
하드웨어 모델	000 FW_001 000 FW_002

- 관리자 PC

구 분	내 용
CPU	Intel i5-10400 2.90 GHz
Memory	16 GB
HDD	1 TB
SSD	256 GB
NIC	100/1000 Base-T Ethernet 1 개
OS	Windows 11 Pro, 64 bit
시험도구	Chrome 113.0

2.1.3 시험 도구

☞ TOE 시험에 사용된 시험 도구를 기술한다.

예) TOE에서 제공하는 기능을 시험하는데 사용된 시험도구는 다음과 같다.

도구명	기능	버전
Wireshark	네트워크 패킷 확인 도구	4.4.13
tcpreplay	네트워크 패킷 전송 도구	-
hping3	네트워크 패킷 전송 도구	-

2.2. 시험범위

본 장에서는 TOE에서 제공되는 모든 기능이 시험되었음을 입증하기 위한 시험범위를 분석한다.

☞ TOE의 모든 기능이 시험되었음을 입증하기 위한 시험범위를 기술한다.

예) 다음의 표는 TOE에서 제공되는 기능 목록을 제공하며, 해당 기능에 대한 시험 항목의 대응관계를 제공한다.

구분	보안기능	시험항목
식별 및 인증	관리자 로그인	T_FIA_01 관리자 식별 및 인증
	사용자 로그인	T_FIA_02 사용자 식별 및 인증
보안관리	환경설정 – 계정 관리	T_FMT_01 계정 관리 – 계정 생성
		T_FMT_02 계정 관리 – 계정 변경
…	…	…

2.3. 시험 항목 및 시험 결과

2.3.1 시험 결과

☞ 시험범위에 식별된 보안기능에 대한 시험항목이 모두 시험되었음을 기술한다.

예) 다음의 표는 TOE에서 제공하는 시험항목에 대한 시험 목적 및 시험결과의 요약정보를 나타낸다.

구분	시험항목	시험목적	시험결과
식별 및 인증	T_FIA_01 관리자 식별 및 인증	관리자에 대한 식별 및 인증 기능을 수행한다.	통과
	T_FIA_02 사용자 식별 및 인증	사용자에 대한 식별 및 인증 기능을 수행한다.	통과
보안관리	T_FMT_01 계정 관리 – 계정 생성	관리자 및 사용자 계정 생성 기능을 시험하고, 계정 생성시 계정 역할 및 권한 설정 및 중복 ID 방지 기능을 시험한다.	통과
	T_FMT_02 계정 관리 – 계정 변경	관리자 및 사용자 계정에 대한 수정 및 삭제 기능을 시험한다.	통과
…	…	…	…

2.3.2 국가용 보안요구사항 대응결과

☞ 국가용 보안요구사항과 시험항목에 대한 만족 여부를 기술한다.

예) 다음의 표는 국가용 보안요구사항에 대한 시험항목 및 관련 SFR에 대한 대응관계를 나타낸다.

- 서버 공통 보안요구사항 V3.0 R1

보안요구사항			시험항목	국가용 보안요구사항 만족여부	SFR
1. 식별 및 인증	1.1 사용자 등 식별 및 인증	1.1.1	T_FIA_01 관리자 식별 및 인증	만족	FIA_UAU.1 FIA_UID.1 ....
			T_FIA_02 사용자 식별 및 인증	만족	
			T_FMT_01 계정 관리 – 계정 생성	만족	....
			T_FMT_02 계정 관리 – 계정 변경	만족	
		1.1.2	...	...	...
		1.1.3	...	...	...
	1.2 인증실패 대응	1.2.1	...	...	...
		1.2.2	...	...	...
	1.3 패스워드 등 민감정보 생성 및 안전성 검증				
...	...	...	...		...

3. 세부 시험 내용

본 장에서는 시험계획에 작성된 시험 항목에 대한 시험 목적, 시험 환경, 시험 절차 및 시험 결과에 대한 세부 시험 내용을 기술한다.

☞ *각 시험항목에 대한 세부 내용의 작성 양식은 문서 작성자가 자유 형식으로 작성할 수 있으나, 시험목적, 시험환경, 시험 절차 및 결과를 포함해야한다.*

예) 3.1 식별 및 인증

3.1.1 T_FIA_01 관리자 식별 및 인증

시험 보안기능
☞ *각 시험항목에 대응하는 국가용 보안요구사항 항목을 기술한다.* 서버 공통 보안요구사항 1.1.1, 7.1.1, 7.2.1
시험 목적
☞ *각 시험항목에 대한 시험 목적을 기술한다.* TOE에서 제공하는 관리자에 대한 식별 및 인증 기능을 시험한다.
시험 환경
☞ *각 시험 항목이 수행된 시험환경을 기술한다.* ☞ *시험환경이 여러개로 구성된 경우 해당되는 시험환경만 기술한다.* 2.1 시험환경에 기술된 내용에 따라 시험환경을 구성한다.
시험도구
☞ *각 시험항목에 사용된 시험 도구를 기술한다.* - Chrome 113.0
선행조건
☞ *각 시험항목을 시험하기 전 사전에 필요한 준비 내용을 기술한다.* 최초 설치 후 TOE에 관리자 계정이 설정되어 있어야 한다.
시험절차 및 결과
☞ *시험항목을 수행하기 위한 각 단계별 절차 및 시험결과를 기술한다.* 1. 관리자 PC에서 웹브라우저를 통해 관리자로 GUI 접속을 시도한다. - 웹브라우저에서 관리자 식별 및 인증 페이지로 접속된다. 2. 관리자 계정 정보를 입력하여 식별 및 인증을 수행한다. - 계정명 : admin - 비밀번호 : password - 관리자 계정을 이용한 로그인이 성공하고, GUI에 접속된다. 3. GUI에서 GUI에서 '감사기록 – 사용자 로그' 메뉴를 선택한다. - 관리자에 대한 식별 및 인증 로그가 화면에 출력된다.

[부록] 국가용 보안요구사항 V3.0 관련 SFR 대응표 예시

- 서버 공통 보안요구사항 V3.0 R1

보안요구사항			관련 SFR
1. 식별 및 인증	1.1 사용자 등 식별 및 인증	1.1.1	FIA_UAU.1 FIA_UID.1 FIA_ATD.1
		1.1.2	FIA_UAU.1 FIA_UAU.5 FIA_UID.1 FIA_ATD.1
		1.1.3	FDP_IFC.1 FDP_IFF.1
	1.2 인증실패 대응	1.2.1	FIA_AFL.1
		1.2.2	FIA_AFL.1 FAU_ARP.1
	1.3 패스워드 등 민감정보 생성 및 안전성 검증	1.3.1	FIA_SOS.1
		1.3.2	FIA_SOS.1
		1.3.3	FIA_SOS.1
	1.4 인증 정보 재사용 방지	1.4.1	FIA_UAU.4
	1.5 인증피드백 보호	1.5.1	FIA_UAU.7
		1.5.2	FIA_UAU.7
2. 보안관리	2.1 보안관리 기능	2.1.1	FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_SMF.1 FMT_SMR.1
	2.2.관리접속 기능	2.2.1	FMT_MTD.1
	2.3 보안관리용 IP 제한	2.3.1	FTA_MCS.1 FTA_TSE.1
	2.4 기본(default) 패스워드 등의 관리	2.4.1	FMT_PWD.1 FIA_SOS.1
		2.4.2	FMT_PWD.1 FIA_SOS.1
		2.4.3	FMT_PWD.1 FIA_SOS.1
	2.5 에이전트 관리	2.5.1	FMT_MTD.1
		2.5.2	FMT_MOF.1
		2.5.3	FMT_MTD.1

3.데이터 보호	3.1 전송 데이터 보호	3.1.1	FPT_ITT.1 FCS_CKM.1 FCS_CKM.2 FCS_CKM.4 FCS_COP.1
		3.1.2	FTP_TRP.1 FCS_CKM.1 FCS_CKM.2 FCS_CKM.4 FCS_COP.1
		3.1.3	FPT_ITT.1 FTP_ITC.1 FTP_TRP.1 FCS_CKM.1 FCS_CKM.2 FCS_CKM.4 FCS_COP.1 FCS_TLS.1
	3.2 저장 데이터 보호	3.2.1	FPT_PST.1(확장) FCS_CKM.1 FCS_CKM.2 FCS_CKM.4 FCS_COP.1
		3.2.2	FMT_MOF.1 FMT_MSA.1 FMT_MTD.1 FMT_PWD.1 FPT_PST.1(확장) FCS_CKM.1 FCS_CKM.2 FCS_CKM.4 FCS_COP.1
4. 자체보호	4.1 보안기능 자체 시험	4.1.1	FPT_TST.1
		4.1.2	FPT_TST.1 FAU_ARP.1
	4.2 무결성 검증	4.2.1	FPT_TST.1
		4.2.2	FPT_TST.1
		4.2.3	FAU_GEN.1 FAU_SAA.1 FAU_SAR.1 FAU_SAR.3
		4.2.4	FPT_TST.1 FAU_ARP.1

5.업데이트 보호	5.1 안전한 업데이트	5.1.1	FPT_TUD.1(확장)
		5.1.2	FPT_TUD.1(확장)
		5.1.3	FPT_TUD.1(확장)
6. 안전한 세션 관리	6.1 세션 잠금・종료 기능	6.1.1	FTA_SSL.1 FTA_SSL.3
	6.2 동시접속 세션 제한	6.2.1	FTA_MCS.1 FTA_MCS.2
7. 감사기록	7.1 감사기록 생성	7.1.1	FAU_GEN.1
		7.1.2	FAU_GEN.1
		7.1.3	FPT_STM.1
	7.2 감사기록 조회	7.2.1	FAU_SAA.1 FAU_SAR.1
		7.2.2	FAU_SAR.3
		7.2.3	FAU_GEN.1
	7.3 감사기록 보호	7.3.1	FAU_STG.1
		7.3.2	FPT_PST.1(확장) FCS_CKM.1 FCS_CKM.2 FCS_CKM.4 FCS_COP.1
	7.4 감사기록 손실 예측시 대응행동	7.4.1	FAU_STG.3
	7.5 감사기록 손실 방지	7.5.1	FAU_STG.4
8. 암호지원	8.1 암호사용	8.1.1	FCS_CKM.1 FCS_CKM.2 FCS_CKM.4 FCS_COP.1
	8.2 암호키 생성	8.2.1	FCS_CKM.1 FCS_CKM.2 FCS_CKM.4 FCS_COP.1 FCS_RBG.1(확장)
	8.3 암호키 저장	8.3.1	FCS_CKM.1 FCS_CKM.2 FCS_CKM.4 FCS_COP.1
	8.4 암호키 파기	8.4.1	FCS_CKM.1 FCS_CKM.2 FCS_CKM.4 FCS_COP.1
9. 취약성 대응	9.1 소스코드 보안약점 제거	9.1.1	취약점 분석서로 대체
	9.2 알려진 취약점 제거	9.2.1	
	9.3 불필요한 서비스 제거	9.3.1	

- 앤드포인트 공통 보안요구사항 V3.0 R1

보안요구사항			관련 SFR
1. 식별 및 인증	1.1 서버 식별 및 인증	1.1.1	FIA_IIA.1(확장)
	1.2 인증 피드백 보호	1.2.1	FIA_UAU.7
2. 보안관리	2.1 보안관리 기능	2.1.1	FMT_MOF.1 FMT_MSA.1 FMT_MTD.1 FIA_UID.1 FIA_UAU.1
3. 데이터 보호	3.1 저장 데이터 보호	3.1.1	FPT_PST.1(확장) FCS_CKM.1 FCS_CKM.2 FCS_CKM.4 FCS_COP.1 FCS_RBG.1(확장)
		3.1.2	FAU_STG.1 FPT_PST.1(확장) FCS_CKM.1 FCS_CKM.2 FCS_CKM.4 FCS_COP.1
4. 자체 보호	4.1 무결성 확보	4.1.1	FPT_TST.1
		4.1.2	FPT_TST.1
	4.2 가용성 확보	4.2.1	FPT_PST.2(확장)
		4.2.2	FPT_TST.1 FPT_RCV.1 FPT_RCV.2
		4.2.3	FPT_PST.2(확장)
	4.3 에이전트 제거	4.3.1	FPT_PST.2(확장)
5. 감사기록	5.1 감사기록 생성	5.1.1	FAU_GEN.1
		5.1.2	FAU_GEN.1
	5.2 감사기록 전송	5.2.1	FAU_GEN.1 FPT_ITT.1
6. 안전한 업데이트 및 파일 배포	6.1 온라인 업데이트 및 파일 배포	6.1.1	FPT_TUD.1(확장)
		6.1.2	FPT_TUD.1(확장)
		6.1.3	FPT_TUD.1(확장)