국가용 보안요구사항 V3.0 기반의

국내용 보안목표명세서 작성 가이드 V1.0

2025. 4. 11.

과학기술정보통신부

IT보안인증사무국

• 제·개정 이력

버전	일 자	변경 내용
1.0	2025. 4. 11.	ㅇ 국가용 보안요구사항 V3.0 기반의 국내용 보안 목표명세서 작성 가이드 제정

서 문

2024년 과학기술정보통신부는
정보보호제품 평가·인증 제도의 개선을 통해 기업의 참여 확대와 평가·인증 준비의 실효성을 제고하고자
다양한 정책적 노력을 추진하였습니다.

이에 발맞춰 IT보안인증사무국은
기업이 정보보호제품 평가를 준비하는 과정에서 겪는 어려움을 덜어주기 위해
제출문서에 대한 가이드와 템플릿을 제공하고, 작성 샘플을 마련하여 실질적인 지원을 제공하고자 합니다.

본 가이드는 정보보호제품 CC 평가 시 요구되는 중요 제출문서인 보안목표명세서 평가에서의
복잡한 절차와 기술적 요건을 명확히 이해할 수 있도록 구체적인 지침과 사례를 제시하여,
문서의 구성별(세부목차별) 작성 방향에 대한 안내와 함께 실무적인 작성 예시를 포함하고 있습니다.

본 가이드를 통해 기업이 평가를 준비하는 과정에서부터 체계적이고 효율적으로
평가·인증에 대한 사전 역량을 강화할 수 있을 것으로 기대합니다.

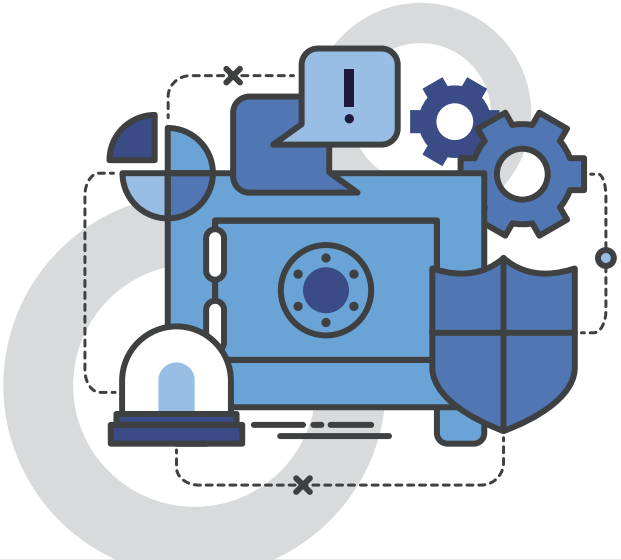
CONTENTS

06 보안요구사항

07 TOE 요약명세

08 참고자료

09 용어 및 약어



01

보안목표명세서 소개

1. 보안목표명세서 소개

1.1. 보안목표명세서 참조

제 목	OOO 보안목표명세서
버 전	X.X
작성자	(주) XXX
발간일	20XX.XX.XX

1.2. TOE 참조

☞ TOE 식별을 명확하게 할 수 있게 TOE 명칭, 세부 버전, TOE 구성요소 등 TOE에 대한 식별정보 서술

☞ TOE 버전 및 TOE 구성요소 식별 및 서술 방법은 최신의 '정보보호제품 평가·인증 해설서(이하 해설서)' 참조하여 서술

☞ 특히, 하드웨어 일체형 장비의 경우 해설서 '2.1 TOE 범위 산정 및 식별자 부여 방법' 확인 필요

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

작성요령	▸ ST 참조체계의 요건 : 고유성/유일성 ▸ ST 참조 작성원칙 : 다른 ST와 구별할 수 있어야 하고 동일 TOE를 다루는 ST의 다른 버전과도 구별 가능해야 함
	▸ TOE 참조체계의 요건 : 명확성 TOE(Target of Evaluation) : 보호프로파일 또는 보안목표명세서에 정의된 보안요구사항을 만족하는 소프트웨어, 펌웨어 및/또는 하드웨어 집합이며 가능한 설명서를 포함 ▸ TOE 참조 작성원칙 : TOE 평가범위에 대해 소비자가 혼동을 하지 않도록 제품명과 구분하여 명확하게 TOE 명칭을 사용해야 함 ☑ 다만, TOE 평가범위가 제품 전체인 경우 제품명을 그대로 사용할 수 있음

1.3. TOE 개요

☞ TOE 유형, TOE 용도 및 주요 보안특성을 요약하여 서술

예 : TOE는 네트워크 간 전송되는 패킷들을 정해진 규칙에 따라 차단하거나 통과시켜 공격자로부터 내부 자산을 보호하는 침입차단시스템(Firewall)이다.

1.3.1. TOE의 용도 및 주요 보안 특성

☞ TOE가 보안과 관련하여 어떤 기능을 제공하며 어떠한 운영환경에서 어떠한 목적으로 사용할 수 있는지에 대해 전반적인 사항을 간단 명료하게 서술

예 : TOE는 내부망에 연결되어 있는 자산을 외부로부터 보호하기 위해 인가된 관리자가 설정한 규칙에 따라 트래픽을 제어하는 기능을 기본으로 제공한다. TOE는 인가된 관리자가 설정한 IP 주소나 포트를 통해 송수신되는 네트워크 트래픽에 대해 패킷 필터링, 상태기반 검사, 세션 임계값에 따른 트래픽 필터링 등 상태기반 트래픽 필터링 기능을 제공한다. TOE를 통과하여 외부 네트워크로부터 내부로 유입되는 트래픽을 제어하고 내부 IT 자산에 대한 외부 사용자의 침입을 차단한다. 또한, 내부 네트워크로부터 외부 네트워크로 나가는 트래픽을 제어하여 내부 사용자의 비인가된 정보 유출을 방지한다.

☞ TOE를 포함한 제품이 제공하는 모든 보안특징을 서술하고 평가범위와 평가범위 이외의 부분을 명확하게 식별

☞ ST의 나머지 부분(TOE 유형, TOE 논리적 범위, TOE 물리적 범위, TOE 요약명세)과 일관성 유지

☞ 몇 개 단락으로 간단 명료하게 서술

작성요령	▸ 제품의 보안특징까지 모두 포함하여 작성할 수 있으나 평가범위 여부를 명확하게 구분할 수 있어야 함 ☑ TOE 소개절의 TOE 설명 부분에서 TOE 보안특징과 TOE 범위에는 제외되나 제품에서 제공하는 보안특성을 좀 더 세부적으로 서술할 수 있음 ☑ 평가되지 않은 제품의 보안특징이 ST 소개 절 이외에 부분(보안문제정의, TOE 보안목적, 보안요구사항, TOE 요약명세)에 서술할 수 없음

1.3.2. TOE 유형

☞ 국내용 평가제품인 경우 국가용 보안요구사항에 해당하는 제품 유형을 식별하고 핵심 기능 및 운영환경을 요약 서술

예 : TOE는 OSI 3~4계층(IP, 포트, 프로토콜 기반)에서 동작하는 상태기반 트래픽 필터링 기능을 제공하는 침입차단시스템으로 하드웨어 일체형 장비 형태로 제공된다. 하드웨어 사양은 “TOE 물리적 범위”에 명시하였다. TOE는 감사기능, 보안관리, 자체보호 기능 등 TOE의 핵심 기능을 지원하는 보안기능도 함께 제공된다.

작성요령	▸ TOE 유형(Type) : 제품이 일반적으로 제공하는 공통적인 보안특징을 최소 기본 보안요건으로 정의하고 이에 대해 개발그룹 및 사용자 그룹에서 TOE 유형으로 인정할 수 있어야 함 ▸ TOE 유형 작성원칙 : 일반적인 상식에서 기대할 수 있는 보안기능성 및 운영환경을 고려하여 TOE가 포함될 수 있는 제품 유형을 서술 ☑ TOE 유형에서 일반적으로 제공되는 핵심 기능을 TOE가 제공해야 함. 예를 들어, TOE 유형이 방화벽임에도 불구하고 잘 알려진 서비스 포트(원격접속, DB접속 등)를 접근통제(정보흐름통제)를 지원하지 못하는 경우 TOE는 방화벽 유형에 포함될 수 없음 ☑ TOE 유형이 설치되는 일반적인 운영환경에서 TOE가 동작해야 함. 예를 들어, 방화벽임에도 불구하고 TOE를 통과하는 모든 패킷 발생지에서는 악의를 가진 공격자가 존재하지 않는 운영환경에서만 동작한다면 TOE는 방화벽 유형에 포함될 수 없음 ☑ TOE 용도 및 보안특징을 한 문장으로 요약하여 서술하되 일반적으로 통용되는 제품유형을 명시적으로 표현

1.3.3. 비-TOE 식별(하드웨어/소프트웨어/펌웨어)

☞ TOE 범위에 포함되지 않은 IT 자원이나 TOE의 정상 동작을 위해 필요한 최소한의 IT자원을 식별
☞ TOE가 SW 형태인 경우 TOE를 설치할 수 있는 운영체제 및 NIC 등 하드웨어 사양을 식별
☞ TOE를 포함하는 제품 설치매뉴얼에 명시되어 있는 IT자원을 식별
☞ TOE가 외부 IT실체와 상호작용을 통해 동작을 수행하는 경우 외부 IT실체를 식별
☞ TOE가 외부 IT 실체와 상호작용을 통해 동작을 수행하는 경우, 아래와 같이 외부 IT 실체와 관련된 사항을 작성, 외부 IT 실체의 예로는 NTP, SYSLOG, SNMP, SMTP 등이 있음

TOE 구성요소	하드웨어 플랫폼	운영체제	기타 SW

외부 IT 실체	용도
Syslog 서버	
NTP 서버	

1.4. TOE 설명

1.4.1. TOE 물리적 범위

(가) TOE 구성요소 및 배포 방법

☞ TOE를 구성하는 모든 하드웨어, 펌웨어, 소프트웨어, 설명서 등을 식별(파일명 포함)하여 목록 작성
☞ TOE 구성요소마다 배포형태와 배포방법을 서술
☞ TOE 범위에 포함되는 물리적인 요소와 포함되지 않은 요소를 명확하게 식별할 수 있을 정도의 충분한 정보를 상세하게 서술
☞ TOE 용도 및 보안특성에 서술한 내용보다 상세하게 서술하되 일관성을 유지하도록 서술
☞ TOE가 물리적으로 여러 개체로 구성되는 경우 개별 요소에 대해 간략하게 핵심 보안특성을 서술

예: TOE는 하드웨어 일체형 장비 및 문서(설치매뉴얼, 운영매뉴얼)로 구성된다. 하드웨어 일체형 장비에는 “1.5.3 TOE 논리적 범위”에 서술된 기능을 소프트웨어로 구현되어 있다.
TOE는 다양한 하드웨어 플랫폼에 설치될 수 있으며 하드웨어 플랫폼 사양에 따라 제품의 모델명이 상이할 수 있다.

TOE 구성요소	버전정보	배포 형태	배포 방식

☞ TOE 보안기능이 제3자가 제공한 요소에서 구현된 경우에는 다음과 같이 제3자 제공 요소를 명시해야 한다.

제3자 요소(버전 포함)	보안기능 세부 설명

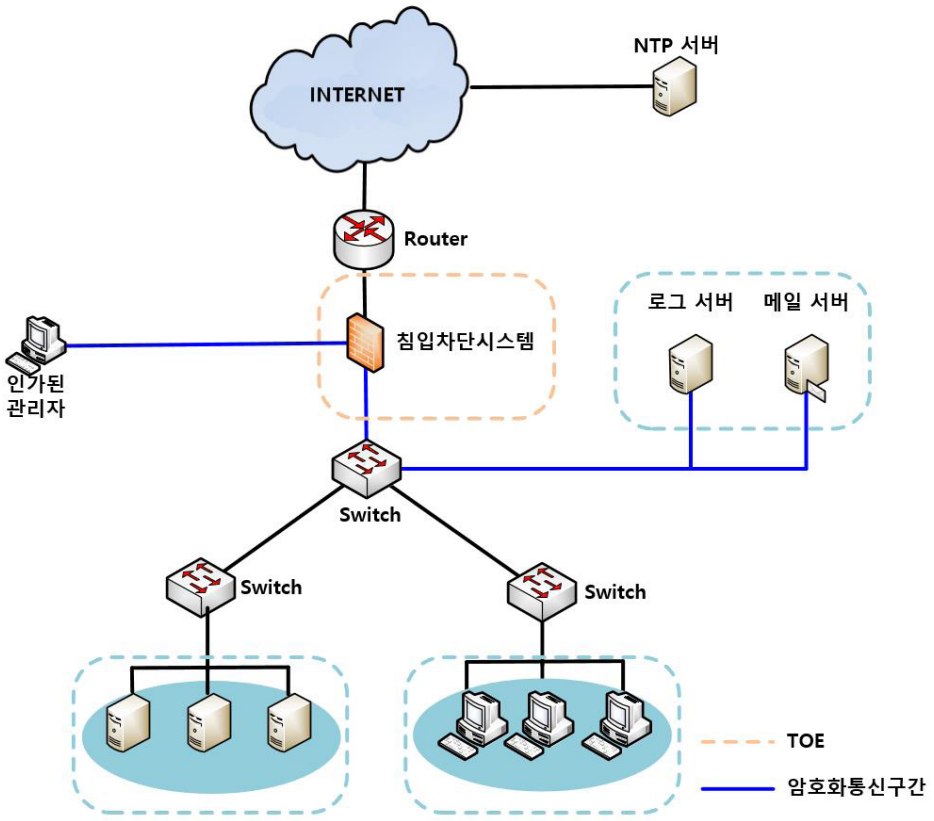
☞ 하드웨어 모델 사양과 관련된 사항은 최신 ‘정보보호제품 평가·인증 해설서’의 ‘하드웨어 일체형 장비의 확장 모델 서술 및 평가 방안’을 참고, 또한 TOE가 하드웨어 일체형 장비 형태의 제품인 경우, NIC, HDD, Memory, 보안기능 수행 하드웨어(예: 암호가속기 등)는 확장할 수 있으며 그 밖의 하드웨어(예: CPU)는 확장 구성이 허용되지 않음에 유의

모델명	CPU	HDD	RAM	NIC	기타

(나) TOE 운영환경

☞ 일반적인 TOE 설치 및 운영환경을 고려하여 시스템 구성 및 네트워크 구성도 작성
☞ 시스템 구성 및 네트워크 구성도에 Non-TOE로 식별된 외부 IT실체와의 상호관계를 포함
☞ TOE 구성요소, 외부 IT 실체, 관리자 단말 간의 네트워크 연결을 명시
☞ TOE의 핵심 보안특징이 표현되도록 TOE 구조도를 시스템 구성 및 네트워크 구성도에 내포
☞ TOE가 물리적으로 여러 개 분산된 경우 TOE 범위를 표현

TOE 운영환경



1.4.2. TOE 논리적 범위

☞ TOE 구성요소별로 제공하는 보안특징을 국가용 보안요구사항의 대분류 또는 CC 제2부의 보안기능 클래스 단위로 구분하여 서술

☞ TOE가 제공하는 보안기능에 매핑되는 보안기능요구사항(SFR)을 1차적으로 식별하여 해당 SFR의 핵심 사항을 요약하여 서술

☞ TOE에 포함된 암호 알고리즘, 암호키 길이, 암호 연산의 목적, 제3자 제공 암호 라이브러리 사용 여부에 대해 서술

☞ TOE를 서브시스템 단위로 TSF 경계를 구분하였을 때 SFR 수행에 직접적으로 관련되어 있는 기능을 상세하게 서술

☞ TOE 유형이라면 반드시 제공해야 하는 기본 핵심 보안특징을 상세하게 서술하고 표준문서가 존재하는 경우 해당하는 표준문서 참조 표기

☞ 앞 절(TOE 용도 및 보안특성)에서 서술한 보안특징을 보다 상세하게 서술하되 TOE 범위에 일관성을 유지하여 서술

(가) 보안감사

예: TOE는 침입차단 메커니즘에서 처리된 트래픽 로그는 감사데이터로 수집 및 저장되어 관리수단을 통해 관리자가 트래픽 로그를 조회할 수 있도록 한다. 트래픽 로그 외에도 관리자 행위, 시스템 동작 등 관리자가 설정한 감사대상사건에 대해 감사데이터를 생성하여 저장한다.
감사 저장소의 용량이 임계치의 80%에 도달하면 관리자에게 경고메일을 발송하고 임계치에 도달하면 오래된 감사레코드를 덮어쓰기 한다.

(나) 암호지원

예: TOE는 암호키 생성에 필요한 난수는 XXX 표준을 준수하고 암호키 생성 함수는 XXX 표준을 준수하여 생성한다. 암호연산이 수행되는 동안에 암호키는 메모리에 상주하게 되며 암호연산이 종료되면 즉시 메모리에서 완전 파기("0"으로 3회 덮어쓰기)한다. 암호연산이 수행되는 동안에는 다른 동작이 진행되지 못한다. TOE는 사전 공유키 방식과 RSA 공개키 방식이 적용되는 SSHv2를 지원하며 서버 인증서 기반의 TLS 1.2 이상을 지원한다.

(다) 사용자 데이터 보호

예: TOE의 침입차단 메커니즘은 TCP/IP 스택에서 패킷의 헤더 정보를 분석하여 정보흐름통제규칙에 일치하는지를 검사한다. 침입차단 메커니즘은 정보흐름통제규칙에 일치하고 Action이 허용한 경우에만 해당 패킷을 내부망으로 전달하거나 내부망에서 외부망으로 전달한다. 또한 상태기반 패킷 필터링 기능도 제공하므로 TOE가 처리할 수 있는 트래픽은 IP 패킷, TCP/UDP 패킷, ICMP 패킷이다.

(라) 식별 및 인증

예: 관리자가 관리수단에 접속하려는 경우 패스워드 기반 인증방식이 적용된다. 연속인증에 실패하는 경우 일정시간 동안 인증을 지연시킨다. 관리자가 입력한 패스워드는 화면에 노출되지 않도록 마스킹 처리한다. 패스워드가 초기 설정 또는 변경될 때 마다 패스워드 길이 및 조합규칙에 따라 패스워드를 검증한다.

(마) 보안관리

예: 관리자는 관리수단을 통해 보안정책 및 TSF 데이터를 관리할 수 있으며 TOE의 보안기능 동작을 변경할 수 있다. CLI 형태의 관리수단은 SSH 연결이 선행되어야 하고 GUI 형태의 관리수단은 HTTPS 연결이 선행되어야 한다. 3가지 보안역할이 정해져 있으며 관리자는 모든 관리기능을 사용하며, 서비스 관리자는 TOE의 중요 데몬 상태를 조회할 수 있으나 TOE 운영에 관한 환경설정을 변경할 수 없으며 모니터링 담당자는 트래픽 로그만 조회 가능하다.

(바) TSF 보호

예: 관리자 패스워드는 SHA 256 이상의 안전한 해시알고리즘을 적용하여 저장하고 환경설정 파일은 접근권한을 설정하여 비인가된 자의 접근을 제한한다. 감사레코드에 정확한 시간정보를 기록할 수 있도록 외부 NTP 서버로부터 시간정보를 수신하여 동기화시킨다. TOE의 정상적인 운영을 위해 중요 TSF 및 TSF 데이터에 대한 무결성 검증 수단을 관리자에게 제공하여 TOE의 정상여부를 확인할 수 있도록 한다.

(사) TOE 접근

예: 관리자가 로그인 후 일정시간 활동이 없으면 세션잠금을 수행하고 세션잠금 해제 전에 재인증을 하도록 요청한다. 관리자가 로그아웃 하는 경우 세션유지에 필요한 모든 정보를 파기한 후 세션종료 처리를 한다. 동시로그인을 제한하고 동일 관리자 역할에 대해서는 최대 1개의 세션만 유지한다.

(아) 안전한 경로/채널

예: TOE는 외부 Syslog 서버가 TLS 연결요청을 하면 TLS 기반의 Syslog 프로토콜을 이용하여 로그를 Syslog 메시지 형식으로 전송한다. 관리자가 관리접속을 하여 GUI 또는 CLI에 접속하려는 경우 안전한 암호통신프로토콜(HTTPS, SSHv2 등)을 이용하여 관리자와 TOE 간의 안전한 경로를 형성한다.

작성요령	▶ 제품이 구현되어 있지 않고 개발 계획 단계에 있는 경우 기획팀, 개발팀 등 제품 개발에 관련된 자들이 협의하여 TOE 용도에 부합하는 보안요구사항을 정의한 후 CC 제2부의 클래스에 따라 분류하여 논리적 흐름을 갖도록 서술 ▶ 제품이 구현되어 있는 경우 TOE 요약명세를 먼저 서술하고 TOE 요약명세에 따라 SFR을 명세한 후에 클래스 단위로 SFR의 핵심사항을 요약하는 방식으로 TOE 논리적 범위를 작성하면 일관성 유지 관점에서 효율적일 수 있음 ▶ 개인정보 관련 법령에 따라 개인정보 보호 목적의 정보보호시스템인 경우 관련 고시에 서술된 기술적 보호조치가 TOE 논리적 범위에 포함될 수 있도록 서술 ▶ ST 작성의 마무리 단계에서 TOE 요약명세→ SFR→ TOE 논리적 범위→ TOE 개요 및 용도에 서술된 내용에 대해 일관성을 유지하는 지 검토

02

준수 선언

2. 준수 선언

2.1. 공통평가기준 준수 선언

공통평가기준		정보보호시스템 공통평가기준 버전 3.1 개정 2판 •정보보호시스템 공통평가기준 1부 : 소개 및 일반모델, 버전 3.1R1, 2006. 9., CCMB-2006-09-001 •정보보호시스템 공통평가기준 2부 : 보안기능요구사항, 버전 3.1R2, 2007. 9., CCMB-2007-09-002 •정보보호시스템 공통평가기준 3부 : 보증요구사항, 버전 3.1R2, 2007. 9., CCMB-2007-09-003
준수 형태	2부 보안기능요구사항	(☞ 준수 또는 확장 중에서 선택하여 명시. 확장 시 5장에서 정의한 확장컴포넌트 식별)
	3부 보증요구사항	(☞ 준수 또는 확장 중에서 선택하여 명시. 확장 시 5장에서 정의한 확장컴포넌트 식별)
	패키지	(☞ 평가보증등급을 명시. EAL 패키지에서 추가한 경우 해당 보증컴포넌트 식별)

2.2. 보호프로파일(보안요구사항), 패키지 준수 선언

(☞ 국가용 보안요구사항 및 버전을 식별하여 명기)

☞ 최신 국가용 보안요구사항 및 사전 인증이 필요한 제품 유형은 국가정보원(nis.go.kr) 또는 국가사이버안보센터(ncsc.go.kr) 웹사이트를 참고

보호프로파일(보안요구사항)	-
보증등급	-
TOE 유형	-

2.3. 준수 선언의 이론적 근거

본 보안목표명세서에서는 보호프로파일을 준수선언하지 않았으므로 해당사항이 없다.

03

보안문제정의

3. 보안문제정의

3.1. 위협

예: 위협원은 보호하고자 하는 자산에 비인가 된 접근 또는 비정상적인 방법으로 위해를 가하는 IT실체 및 사용인이며, 다음과 같은 다양한 위협을 발생시킬 수 있다. 이때 TOE에 대한 위협원은 강화된-기본 수준의 전문지식, 자원, 동기를 가진다.

☞ 2장에서 준수선언한 평가보증등급의 AVA_VAN.# 컴포넌트에 따라 위협원의 수준을 명시. 예를 들어 EAL4를 선언한 경우 AVA_VAN.3에서 강화된-기본 수준의 위협원에 대해 내성을 갖는지 취약성 분석을 하게 되므로 위협원이 수준은 강화된-기본이 된다.

☞ TOE 용도, TOE 운영환경, TOE 논리적 범위를 고려하여 TOE가 대응해야 하는 위협과 더불어 TOE 자체에 대한 위협을 모두 고려하여 명세

☞ 위협 문장은 위협원, 자산, 악의적인 행동 등으로 표현하며 위협원은 전문지식, 자원, 동기 관점으로 명세

☞ 위협 유형에 따라 공격대상이 되는 자산 유을 식별하고 공격목표 달성을 위해 공격자가 수행할 수 있는 공격방법과 공격 성공 시 결과를 한 문장으로 명세. 즉, “위협원은 ooo 자산에 대해 ooo 공격방법으로 ooo 공격목표를 이룰 수 있다.” 형식으로 위협 문장을 명세

☞ 아래에 명세된 “비인가된 접속” 및 “정보 유출” 위협 유형에 대해 일반적으로 공통사항을 명세한 것이므로 활용하고 TOE 유형 및 용도를 고려할 때 위협 유형 및 위협을 추가 명세

3.1.1. 비인가 된 접속

T.REPLAY	(T.재사용)

위협원은 인증정보 또는 세션정보를 복사하여 재사용함으로써 TOE에 접속하거나 내부망에 접속할 수 있다.

T.WEAK_PASSWORD	(T.취약한 패스워드)

위협원은 패스워드의 디폴트값 이용 등 관리가 미흡한 패스워드를 획득하여 인가된 관리자로 위장한 후 TOE에 접근할 수 있고, 낮은 수준의 패스워드 규칙이 적용된 경우 인가된 관리자로 위장하여 TOE에 접근할 수 있다.

T.ADMIN_SESSION_HIJACK	(T.관리자 세션 탈취)

위협원은 로그인된 채로 방치된 관리자 화면에 접근하거나 로그아웃 상태이나 유지되고 있는 관리자 세션정보를 이용한 인증우회를 통해 관리자 권한을 탈취할 수 있다.

T.RETRY_AUTH_ATTEMPT	(T.연속 인증시도)

위협원은 연속적으로 인증을 시도하여 획득한 정보를 이용해 인증에 성공한 후 인가된 관리자로 위장하여 TOE에 접근할 수 있다.

T.IMPERSONATION	(T.위장)

위협원은 인가된 관리자나 통신상대로 가장하여 TOE 또는 내부망에 접근할 수 있다.

3.1.2. 정보유출

T.UNTRUSTED_PATH	(T.안전하지 않은 통신경로)

위협원은 관리자 관리접속 과정에서 발생된 트래픽을 스니핑하여 TOE 보안설정 등 미흡한 취약점을 발견하고 이를 악용하여 내부망에 불법접근하거나 중요정보를 유출시킬 수 있다.

T.WEAK_CRYPTO_PROTOCOLS	(T.취약한 암호 프로토콜)

위협원은 취약한 암호통신 프로토콜 또는 낮은 암호강도를 사용하는 트래픽을 분석하여 키정보를 유추하거나 통신암호문의 내용을 알아낼 수 있다.

3.1.3. ooo

☞ 일반적인 “비인가된 접속” 및 “정보유출” 위협 유형 이외에 TOE 유형 및 용도를 고려하여 추가 위협 유형에 대해 서술

T.	(T.)

T.	(T.)

T.	(T.)

※ 위험관리모델에 기반한 위협 도출 및 작성 절차

1단계 TOE 범위산정 과정을 통해 TOE 유형을 식별하고 TOE 운영환경을 설정한다.

- 위협 분류에서 해당하는 위협을 판별해내기 위해 TOE 유형이 필요함
- TOE 설명에서 서술한 물리적 범위 및 논리적 범위를 참조하여 TOE 운영환경을 설정
  - ▷ TOE 운영환경에 따라 위험 심사 대상 범위가 결정됨
  - ▷ 위험이란, 자산에 대해 악영향을 미치게 하는 기회(Opportunity)이며 기회란 어떤 원인으로 인해 발생한 사건을 의미함
  - ▷ 위협원이 취약점을 악용하여 자산에 악영향을 미칠 수 있는 공격을 수행하는 것을 위협이라 하며 이러한 위협이 많이 존재할수록 위험이 증가됨
  - ▷ 결론적으로 위험을 식별하고 자산 가치에 따른 위험도를 평가해야 정확한 위협을 식별하는 것이 가능해짐

2단계 TOE 운영환경에서 위험을 증가시키는 위협을 파악하기 위해 위협 후보목록을 작성한다.

- TOE 유형과 동일하거나 유사한 TOE에 대해 정의하고 있는 PP 및 ST를 CCRA 포털에서 검색하여 위협 목록 작성
- ST에서 준수선언한 PP의 보안문제정의에서 설명된 위협에 대해 목록 작성
- TOE 유형에 해당하는 알려진 취약점을 공개사이트(CVE 등)에서 검색하여 취약점 목록 작성
- 사이버 공격유형을 정의하는 표준문서, 기술문서, 가이드 등을 참조하여 TOE 유형에 해당하는 공격유형을 식별
- 각각 작성된 목록을 종합적으로 분석하여 중복내용을 제거하여 위협 후보목록을 작성

3단계 TOE에 실제 적용 가능한 위협목록을 작성하고 위협을 분류한다.

- 위협 후보목록 중에서 TOE 운영환경 및 보안특징을 고려하였을 때 적용되지 않는 위협을 후보목록에서 제거
- 위협분류 체계(참조 : ENISA 위협분류 맵)에서 TOE 유형에 적용 가능한 위협유형 및 세부위협 사항을 선별
- 위협유형 및 세부위협에 따른 위협원(참조 : ENISA 위협원 종류)을 식별
- 해당 위협에서 공격의 대상이 되는 자산 유형(참조 : ENISA 자산분류 맵)을 식별
  - ▷ 자산은 TOE가 보호해야 하는 대상일 수도 있고 TOE 자신(TSF, TSF 데이터 등)이 될 수도 있음
- 해당 위협에서 공격을 통해 이루고자 하는 공격목표를 식별
- 해당 위협에서 공격목표를 이루기 위해 취약점을 악용하는 행동을 서술

위협유형	세부위협	위협원	공격대상 (자산 유형)	공격목표	악의적 행동	위협 출처
Abuse	주소영역 하이재킹	외부해커	라우팅 테이블의 Prefixes	route BGP peer가 희생지의 prefixes를 발표하게 함	트래픽을 원하는 곳이 아닌 다른 곳으로 보내도록 재라우팅시킴	ENISA IITL

4단계 위협원, 공격대상, 공격목표, 악의적 행동 등을 토대로 형식을 갖춰 위협을 명세한다.

▧ 3단계에서 작성한 표로부터 위협원, 공격대상, 공격목표, 악의적 행동 등으로 문장형식을 구성함으로써 위협을 명세

▷ {위협원}은 {공격목표}를 이루기 위해 {공격대상}에 {악의적인 행동}을 한다.

▷ (예시) 외부 해커(공격자는)는 route BGP peer가 희생지의 prefixes를 발표하도록 라우팅 테이블의 Prefixes에 대해 하이재킹 공격을 한다.

5단계 TOE가 대응해야 하는 위협인지 TOE 운영환경에서 처리해야 하는 위협인지를 판단하여 도출된 위협의 유효성을 검증한다.

▧ 위협을 명세한 후 해당 위협을 위험대응 전략(제거/감소/완화/회피/이전)에 따른 대응방안을 제시하고 이러한 대응방안을 구현하는 경우 보호되는 자산 유형 식별

▧ 위험대응 전략에 따른 보호대책의 효과를 점검하여 잔여위험이 존재하는지 분석

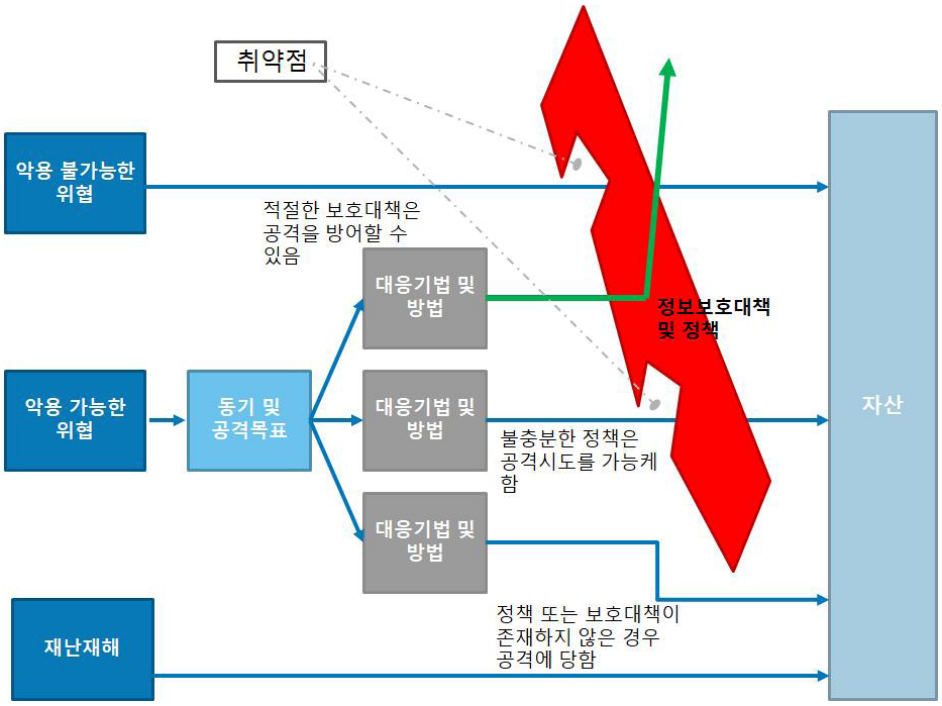
위협유형	위협	위협원	공격대상 (자산 유형)	공격목표	악의적 행동	대응방안 (보호대책)	보호되는 자산 유형	잔여위험

▧ 위험대응 전략에 따른 보호대책의 효과를 점검하여 잔여위험이 존재하는지 분석

▷ {보호대책 또는 조직의 보안정책이 존재하지 않으면 위협에 대응하지 못하므로 자산손실을 초래함

▷ {적절한 보호대책은 위협에 대응함으로써 자산을 보호할 수 있음

▷ {불충분한 보호대책은 위협에 일부만 대응함으로써 잔여 취약점을 악용한 공격에 자산손실을 초래함



3.2. 조직의 보안정책

☞ 아래에 명세된 조직의 보안정책은 일반적인 공통사항이므로 예제로 활용하고, 추가적인 사항이 존재하는 경우 추가 명세

☞ 위협으로 명세하기 어려운 TOE의 보안특성에 대해 조직의 보안정책으로 명세

☞ 조직의 보안정책이란 TOE에서 다루고자 하는 보안특성 및 범위를 정의한 것으로 TOE 및 TOE 운영환경에서 준수해야 하는 보안정책을 의미함

☞ 법령에 근거하는 정보보호제품의 경우 해당 법령의 조항에서 요구하는 바를 조직의 보안정책으로 표현

P.CORRECT_OPERATION	(P.안전한운영)

관리자는 조직의 침입차단시스템 보안정책을 준수하도록 TOE를 안전하게 설정하고 TOE 운영매뉴얼에 따라 정확하게 운영할 수 있도록 관리 수단을 제공해야 한다.

P.AUDIT	(P.감사)

보안과 관련된 행동에 대한 책임을 추적하기 위해 보안관련 사건은 기록 및 유지되어야 하며, 기록된 데이터는 검토되어야 한다. 또한, 감사데이터 저장용 디스크의 사용 가능한 공간을 정기적으로 점검하여 감사데이터가 소실되는 것을 예방하고, 저장된 감사데이터에 대한 비인가된 변경 및 삭제가 발생하지 않도록 보호해야 한다.

P.CRYPTO_STRENGTH	(P.암호강도)

조직은 패스워드 등과 같은 중요정보의 저장 및 전송 구간에 대한 암호화 조치를 적용해야 하며 안전한 암호알고리즘을 사용해야 한다.

P.	(P.)

3.3. TOE 운영환경에 관한 가정사항

☞ 아래 명세된 TOE 운영환경에 관한 가정사항은 일반적인 공통사항이므로 활용하고 추가적인 사항이 존재하는 경우 추가 명세

☞ TOE 운영환경에 관한 가정사항은 TOE 범위와 연관있으며 TOE가 직접적으로 대응할 수 없는 사항에 대해 명세하거나 TOE가 설치 운영되는 일반적인 운영환경을 명세

A.PHYSICAL_PROTECTION	(A.물리적보안)

TOE는 인가된 관리자만이 접근 가능한 물리적으로 안전한 환경에 위치한다.

A.TRUSTED_ADMIN	(A.신뢰된관리자)

TOE의 인가된 관리자는 악의가 없으며, TOE 관리 기능에 대하여 적절히 교육받았고, 관리자 지침에 따라 정확하게 의무를 수행한다.

A.SECURE_MAINTANANCE	(A.보안유지)

네트워크 구성 변경, 호스트의 증감, 서비스의 증감 등으로 내부 네트워크 환경이 변화될 때, 변화된 환경과 보안정책을 즉시 TOE 운영정책에 반영하여 이전과 동일한 수준의 보안을 유지한다.

A.SINGLE_POINT_OF_CONNECTION	(A.유일한연결점)

모든 외부 네트워크와 내부 네트워크간의 통신은 TOE를 통해서만 이루어진다.

A.	(A.)

04

보안목적

4. 보안목적

TOE에 대한 보안목적은 TOE에 의해서 직접적으로 다루어지는 보안목적이고, 운영환경에 대한 보안목적은 TOE가 보안기능성을 정확히 제공할 수 있도록 운영환경에서 지원하는 기술적/절차적 수단에 의해 다루어야하는 보안목적이다.

4.1. TOE 보안목적

☞ TOE 보안목적이란, 보안문제정의(위협, 조직의 보안정책)와 SFR 사이의 연결고리를 만들도록 SFR을 자연어로 표현한 것임

☞ 위협에 대응(제거, 감소, 피해 완화 등) 하고 조직의 보안정책을 수행할 수 있도록 TOE가 제공해야 하는 사항을 명세. 가정사항에 대해서는 TOE 보안목적으로 명세할 수 없음

☞ 어떠한 목적을 달성하기 위해 TOE가 제공하는 보안기능성이 무엇인지 관점에서 명료하게 한 문장으로 서술

☞ 여러 개의 위협/조직의 보안정책에 대해 동일 보안기능성으로 해결할 수 있는 경우 하나의 보안목적으로 명세

O.TRAFFICE_CONTROL	O.정보흐름통제

TOE는 패킷의 출발지 정보와 목적지 정보를 식별하여 외부망과 내부망 사이의 트래픽 흐름을 통제하여야 한다.

O.ABNORMAL_PACKET_BLOCK	O.비정상패킷차단

TOE는 TOE를 통과하는 패킷 중 비정상적인 구조를 가지는 패킷을 차단해야 한다.

O.	O.

O.	O.

4.2. 운영환경에 대한 보안목적

☞ 아래 명세된 TOE 운영환경에 관한 보안목적은 앞 절에서 명세된 가정사항에 대응하는 공통사항이므로 활용하고 추가적인 사항이 존재하는 경우 추가 명세

☞ 위협, 조직의 보안정책, 가정사항에 대응되나 TOE에서 제공하지 못하는 사항에 대해 명세

☞ TOE 유형에 따른 핵심 사항에 대해서는 운영환경에 대한 보안목적으로 명세할 수 없음

☞ 물리적 범위 및 논리적 범위에서 식별된 비-TOE, 비-TSF에 대해 TOE 운영환경에 대한 보안목적으로 명세

OE.PHYSICAL_CONTROL	OE.물리적보안

TOE는 인가된 관리자만이 접근하도록 출입을 통제하며 보호설비가 갖추어진 장소에 위치해야 한다.

OE.TRUSTED_ADMIN	OE.신뢰된관리자

TOE의 인가된 관리자는 악의가 없으며, TOE 관리 기능에 대하여 적절히 교육받았고 관리자 지침에 따라 정확하게 의무를 수행해야 한다.

OE.LOG_BACKUP	OE.로그백업

관리자는 감사기록 유실에 대비하여 감사데이터 저장소의 여유 공간을 주기적으로 확인하고 감사기록이 소진되지 않도록 감사기록 백업(외부 로그서버, 별도 저장장치 등) 등을 수행해야 한다.

OE.SECURITY_MAINTANANCE	OE.보안유지

네트워크 구성 변경, 호스트의 증감, 서비스의 증감 등으로 내부 네트워크 환경이 변화될 때, 변화된 환경과 보안정책을 즉시 TOE 운영정책에 반영하여, 이전과 동일한 수준의 보안을 유지해야 한다.

OE	OE.

4.3. 보안목적의 이론적 근거

4.3.1. TOE 보안목적의 이론적 근거

(가) TOE 보안목적과 SPD 간 일치성 분석

☞ 일치성 분석 표에서 매핑되지 않는 SPD 또는 TOE 보안목적이 존재하는 경우 일치성이 결여된 것이므로 SPD 또는 TOE 보안목적을 추가 식별하여 명세하거나 기존의 내용을 보완해야 함

	O.정보흐름통제	O.비정상패킷차단	O.서비스거부공격차단	O.정보흐름중재	O.식별및인증	O.패스워드관리	O.세션통제	O.	O.	O.	O.	O.	O.	O.
T.재사용					X		X							
T.취약한패스워드					X	X								
T.관리자세션탈취							X							
T.연속인증시도					X									
T.위장					X									
T.														
T.														
T.														
T.														
P.														
P.														
P.														
P.														

[TOE 보안문제정의와 TOE 보안목적 대응]

(나) TOE 보안목적과 SPD 간 추적성 입증

☞ TOE 보안목적과 위협 및 조직의 보안정책 사이의 매핑관계 정확성을 비정형화된 방식으로 분석

☞ 각 TOE 보안목적 최소 1개 이상의 위협 또는 조직의 보안정책으로 추적되어야 함

☞ 추적성이란, TOE 보안목적의 어떤 보안기능성이 위협의 어떤 부분을 대응(제거, 감소, 완화)하는지 관점에서 ST 작성자/개발자의 의도를 표현한 것임

T.재사용	O.식별및인증, O.세션통제

T.재사용은 O.식별및인증, O.세션통제에 의해 대응된다.

O.식별및인증은 관리자 패스워드 인증과정에서 전송되는 인증정보 또는 세션정보의 재사용 방지기술을 갖춘 안전한 인증수단을 제공하도록 하여 본 위협에 대응한다.

O.세션통제는 관리접속 시 인증데이터 재사용 공격에 방지할 수 있는 안전한 암호통신 프로토콜을 적용하고 관리자 로그아웃 시 세션종료를 통해 인증정보 또는 세션정보를 재사용한 인증우회에 대응한다.

T.취약한패스워드	O.패스워드관리, O.식별및인증

T.취약한패스워드는 O.패스워드관리, O.식별및인증에 의해 대응된다.

O.식별및인증은 관리자 패스워드 인증과정에서 전송되는 인증정보 또는 세션정보의 재사용 방지기술을 갖춘 안전한 인증수단을 제공하도록 하여 본 위협에 대응한다.

O.세션통제는 관리접속 시 인증데이터 재사용 공격에 방지할 수 있는 안전한 암호통신 프로토콜을 적용하고 관리자 로그아웃 시 세션종료를 통해 인증정보 또는 세션정보를 재사용한 인증우회에 대응한다.

T.관리자세션탈취	O.세션통제

T.관리자세션탈취는 O.세션통제에 의해 대응된다.

O.세션통제는 관리자 로그아웃 시 세션을 종료하고, 비활동 기간 초과 시 세션잠금/세션종료 등을 통해 관리자 세션을 통제하므로 관리자 세션을 이용한 권한 탈취 위협에 대응한다.

T.	O.

T.	O.

4.3.2. 운영환경에 대한 보안목적의 이론적 근거

(가) 운영환경에 대한 보안목적과 SPD 간 일치성 분석

☞ 일치성 분석 표에서 매핑되지 않는 SPD 또는 운영환경에 대한 보안목적이 존재하는 경우 일치성이 결여된 것이므로 SPD 또는 운영환경에 대한 보안목적을 을 추가 식별하여 명세하거나 기존의 내용을 보완해야 함

	OE. 물리적 보안	OE. 신뢰된관리자	OE. 로그백업	OE. 운영체제보강	OE. 보안유지	OE.	OE.
P.안전한운영		X					
P.감사			X				
A.물리적보안	X						
A.신뢰된관리자		X	X				
A.운영체제보강				X			
A.보안유지					X		

[TOE 보안문제정의와 운영환경에 대한 보안목적 대응]

(나) 운영환경에 대한 보안목적과 SPD 간 추적성 입증

☞ 각 운영환경에 대한 보안목적은 최소 1개 이상의 위협, 조직의 보안정책 또는 가정사항으로 추적됨을 입증

☞ TOE 보안목적에서 가정사항으로 추적될 수 없고 오로지 운영환경에 대한 보안목적에서만 가정사항을 추적될 수 있음

☞ 아래에 명세된 추적성 입증에 관한 내용은 공통사항이므로 활용하고 SPD 정의에서 추가한 가정사항 및 조직의 보안정책으로 인해 운영환경에 대한 보안목적을 추가 명세한 경우 이에 대해 추적성을 입증하는 주장을 서술

A.PHYSICAL_PROTECTION	OE.물리적보안

A.물리적보안은 OE.물리적보안에 의해 지원된다.

OE.물리적보안은 보호설비가 갖추어진 장소에 TOE를 배치하고 인가된 관리자만이 접근하도록 출입을 통제한다.

P.CORRECT_OPERATION	OE.신뢰된관리자

P.안전한운영은 OE.신뢰된관리자에 의해 이행된다.

OE.신뢰된관리자는 조직의 가상사설망 보안정책 및 운영매뉴얼에 따라 관리자가 TOE를 정확하게 운영하게 한다.

P.AUDIT	OE.로그백업

A.물리적보안은 OE.물리적보안에 의해 지원된다.

OE.물리적보안은 보호설비가 갖추어진 장소에 TOE를 배치하고 인가된 관리자만이 접근하도록 출입을 통제한다.

A.TRUSTED_ADMIN	OE.신뢰된관리자, OE.로그백업

A.신뢰된관리자는 OE.신뢰된관리자, OE.로그백업에 의해 지원된다.

OE.신뢰된관리자는 조직의 정보보호교육을 이수하고 정보보호시스템 관리지침을 숙지하여 조직 보안정책에 부합하도록 네트워크를 안정적으로 운영할 수 있는 능력을 갖추고 있으며 패치절차에 따라 TOE의 취약점이 없도록 최신 보안패치를 적용한다.

OE.로그백업은 인가된 관리자가 감사기록 유실에 대비하여 감사데이터 저장소의 여유 공간을 주기적으로 확인하고 감사기록이 소진되지 않도록 감사기록 백업(외부 로그서버, 별도 저장장치 등) 등을 수행하도록 보장한다.

A.PHYSICAL_PROTECTION	OE.물리적보안

A.보안유지는 OE.보안유지에 의해 지원된다.

OE.보안유지는 내부 네트워크 구성 변경, 호스트의 증감, 서비스의 증감 등으로 내부 네트워크 환경이 변화될 때, 변화된 환경과 보안정책을 즉시 TOE 운영정책에 반영하여 이전과 동일한 수준의 보안을 유지하도록 보장한다.

05

확장 컴포넌트 정의

5. 확장 컴포넌트 정의

본 보안목표명세서에서 확장한 컴포넌트의 정의는 다음과 같다.

☞ 확장컴포넌트가 존재하지 않은 경우 “본 보안목표명세서에서 확장한 컴포넌트는 없다.”로 서술

☞ 가능한 CC 제2부 및 CC 제3부에서 선택하여 요구사항을 명세하고, 그럼에도 불구하고 적절한 요구사항이 존재하지 않은 경우 필요한 단위(클래스, 패밀리, 컴포넌트)에 따라 CC 제2부 또는 CC 제3부의 표현형식에 따라 추가 정의

☞ 확장 대상의 최소 단위는 컴포넌트이므로 기존의 컴포넌트에 엘리먼트만 추가하는 방식으로 확장컴포넌트를 정의할 수 없음

5.1. (FCS, Cryptographic support)

5.1.1. 난수 생성

패밀리 개요

난수 생성(FCS_RBG, Random Bit Generation) 패밀리는 TOE 암호 연산 시 필요한 랜덤 값을 생성하는 기능을 요구하도록 정의한다.

컴포넌트 계층관계 및 설명

FCS_RBG 난수 생성	1

FCS_RBG.1 난수 생성은 TSF가 TOE 암호 연산 시 필요한 랜덤 값을 생성하는 기능을 요구한다.
예상되는 관리 요구사항은 없다.
예상되는 감사 대상 행동은 없다.

(가) FCS_RBG.1 난수 생성

계층관계	없음
종속관계	없음
FCS_RBG.1.1	TSF는 다음의 [할당 : 표준 목록]에 부합하는 명세된 난수 발생기를 이용해서 암호 키 생성에 필요한 난수를 생성해야 한다.

5.2. (FXX, XXXXXX)

5.2.1. 패밀리 명

패밀리 개요

컴포넌트 계층관계 및 설명

관리 : 컴포넌트 1, 컴포넌트 2

FMT에서 다음과 같은 관리 기능이 고려될 수 있다.

a)

감사 : 컴포넌트 1

FAU_GEN 보안감사 생성 데이터 생성 패밀리가 보호프로파일/보안목표명세서에 포함되면 다음 행동을 감사기록할 것을 권고한다.

a)감사수준 :

b)최소 :

(가) 컴포넌트 .X 컴포넌트 명

계층관계	없음
종속관계	없음
엘리먼트.X.1	TSF는 ~~해야 한다.
엘리먼트.X.2	TSF는 ~~해야 한다.
엘리먼트.X.3	TSF는 ~~해야 한다.
엘리먼트.X.4	TSF는 ~~해야 한다.
엘리먼트.X.5	TSF는 ~~해야 한다.

작성요령	▶ CC 제2부 SFR로 표현될 수 없는 TOE 보안목적이 존재하는 경우 확장컴포넌트 정의 ▶ TOE의 개발방법론에 따라 CC 제3부 SAR로 표현될 수 없는 경우 확장컴포넌트 정의 ▶ 확장 컴포넌트와 다른 CC 컴포넌트들 사이의 종속관계를 식별 ▶ 확장 컴포넌트를 구성하는 엘리먼트 정의 시 기능시험을 통한 검증이 가능하도록 기능요구사항을 정의 ▶ 확장컴포넌트를 정의하는 경우 CC 제1부의 “8.1 오퍼레이션”, CC 제2부의 “7.1.3 컴포넌트 구조”, “7.2.1 컴포넌트 변경 시 강조” 내용을 준수 ▶ 컴포넌트 단위로 확장하는 경우 컴포넌트가 속하는 패밀리를 선택하고 패밀리를 구성하는 컴포넌트와 유사 수준으로 정의하고 기존 패밀리가 어떻게 변경되는지를 명세 ▶ 패밀리 단위로 확장하는 경우 패밀리가 속하는 클래스를 선택하고 클래스를 선택한 이유가 정당화될 수 있도록 클래스를 구성하는 패밀리 및 컴포넌트들과 유사 수준으로 정의 ▶ 기존 클래스에 포함시키기 어려운 경우 클래스 단위부터 정의를 시작하여 패밀리, 컴포넌트를 모두 정의

06

보안요구사항

6. 보안요구사항

본 보안목표명세서는 일부 약어 및 명확한 의미 전달을 위해 영어를 혼용한다. 사용된 표기법, 형태, 작성 규칙은 공통평가기준을 따른다.

공통평가기준은 보안기능요구사항에서 수행될 수 있는 반복, 할당, 선택, 정교화 오퍼레이션을 허용한다. 각 오퍼레이션은 본 보안목표명세서에서 사용된다.

반복

오퍼레이션을 다양하게 적용하여 하나의 컴포넌트를 여러 번 반복할 경우 사용된다. 반복 오퍼레이션의 결과는 컴포넌트 식별자 뒤에 괄호 안의 반복번호, 즉. (반복 번호)로 표시한다.

할당

명세되지 않은 매개변수에 특정 값을 할당하는데 사용된다(예 : 패스워드 길이). 할당 오퍼레이션의 결과는 대괄호, 즉. [할당 값]으로 표시된다.

선택

요구사항 서술시 정보보호시스템 공통평가기준에서 제공되는 선택사항 중 하나 이상을 선택하는데 사용된다. 선택 오퍼레이션의 결과는 *밑줄 그은 이탤릭체*로 표시된다.

정교화

요구사항에 상세사항을 추가함으로써 요구사항을 더욱 제한하는데 사용된다. 정교화 오퍼레이션의 결과는 굵은 글씨로 표시된다.

본 보안목표명세서는 요구사항의 의미를 명확히 하고, CC 컴포넌트 오퍼레이션 적용에 대한 ST 작성자의 의도를 전달하기 위해 “ST 작성자 **註**”가 제공된다.

6.1. 보안기능요구사항

TOE가 만족하는 보안기능요구사항은 다음과 같다. '정교화', '반복' 오퍼레이션이 적용된 컴포넌트에 대해 비고란에 해당 사항을 기재한다.

보안기능 클래스	보안기능 컴포넌트		비고 (정교화, 반복 구분)
보안감사 (FAU)	FAU_GEN.1	감사데이터 생성	
암호지원 (FCS)	FCS_CKM.1(1)	암호키 생성(SSH 관리접속)	
사용자 데이터보호 (FDP)	FDP_IFC.2(1)	완전한 정보흐름 통제(침입차단)	
식별 및 인증 (FIA)	FIA_AFL.1(1)	인증 실패 처리(패스워드 기반 관리자 인증)	
보안관리 (FMT)	FMT_MOF.1	보안기능 관리	
TSF 보호 (FPT)	FPT_STM.1	신뢰할 수 있는 타임스탬프	
TOE 접근 (FTA)	FTA_MCS.2	사용자 속성별 동시 세션 수의 제한	
안전한 경로/ 채널 (FTP)	FTP_ITC.1	안전한 채널	

[표 2] 도출된 SFR 목록

☞ CC 제2부 <부록 C> ~ <부록 M>에서 설명하고 있는 “사용자 주의사항” 및 “오퍼레이션” 적용 지침을 참고하여 기능컴포넌트의 엘리먼트에 정의된 오퍼레이션을 적용하여 SFR을 명세

☞ 엘리먼트에 정의된 오퍼레이션에 대해 모두 적용하여 완성시켜야 함

☞ 반복, 정교화 오퍼레이션은 모든 컴포넌트에 적용 가능하나 동일 목적에 대해 적용가능한 다양한 방식이 존재하는 경우 반복 오퍼레이션을 적용하여 정의할 수 있으나 이로 인한 기능 사이의 상충성이 없어야 함

☞ 원문의 의도를 변경하지 않는 범위 내에서 문장의 가독성이나 문법에 따른 편집상의 정교화는 허용됨

6.1.1. 보안감사(FAU)

(가) FAU_GEN.1 감사데이터 생성

계층관계	없음
종속관계	없음
FAU_GEN.1.1	TSF는 다음 감사대상 사건에 대해 감사레코드를 생성할 수 있어야 한다. a) 감사 기능의 시동(start-up)과 종료(shut-down) b) *지정되지 않음* 감사 수준에 따른 모든 감사대상 사건 c) [[표 3] 감사대상 사건의 “감사대상 사건” 참조]
FAU_GEN.1.2	TSF는 최소한 다음 정보를 각 감사 레코드 내에 기록해야 한다. a) 사건 일시, 사건 유형, 주체의 신원(가능한 경우), 사건 결과(성공 또는 실패) b) 각 감사 사건 유형에 대하여, 보호프로파일/보안목표명세서에 포함된 기능 컴포넌트의 감사대상 사건 정의에 기반한 [[표 3] 필수 기록되어야 할 주요 감사 사건]

☞ [표 3] 필수 기록되어야 할 주요 감사 사건은 국가용 보안요구사항 서버 공통보안요구사항에 명시되어 있는 내용이며 ST 작성자는 제품 유형에 적합한 국가용 보안요구사항을 참고하여 TOE의 보안기능에 적합하게 필수로 기록되어야 할 주요 감사 사건을 명세해야함

소분류	감사사건	추가적인 감사정보
식별 및 인증	사용자의 로그인, 로그아웃	
	사용자 등록, 변경, 삭제	
	사용자 인증 시도의 한계치 도달 시 대응행동	
	패스워드에 대한 모든 변경	
보안 관리	관리용 단말기의 IP 등록, 삭제, 수정	
	보안관리 기능의 수행과 보안속성값의 모든 변경, 삭제 ** 다만, 보안관리 기능 중 ‘감사기록 조회’ 및 ‘TOE 버전 정보 조회’ 기능은 제외	변경된 보안속성 데이터
	기본 계정(ID)•패스워드 변경	
	관리용 단말 접속 IP 차단	

소분류	감사사건	추가적인 감사정보
안전한 세션관리	사용자의 세션 잠금 또는 종료	
	동일 계정의 중복 로그인 시도 탐지 시 대응 행동	
	동시 세션 수 제한에 기반한 새로운 세션 거부	
암호키 생성	암호 키 생성 실패	
암호 사용	암호연산 실패(암호 연산 유형 포함)	
감사기록	하드웨어 일체형 TOE의 감사기능 시작과 종료	

[표 3] 필수 기록되어야 할 주요 감사 사건

6.1.2. 암호지원(FCS)

(가) FCS_CKM.1 암호키 생성

계층관계 없음

종속관계 [FCS_CKM.2 암호키 분배 또는 FCS_COP.1 암호 연산]
FCS_CKM.4 암호키 파기

FCS_CKM.1.1 TSF는 다음의 [다음 표준]에 부합하는 명세된 암호키 생성 알고리즘 [다음 암호키 생성 알고리즘]과 명세된 암호키 길이 [다음 암호키 길이]에 따라 암호키를 생성해야 한다.

키생성 표준	암호키 생성 알고리즘	암호키 길이
RFC 4253	SSHv2 Transport Layer Protocol의 HASH 함수	AES용 128/256 비트
RFC 4253	SSHv2 Transport Layer Protocol의 HASH 함수	HMAC용 160 비트
RFC 3526	diffie-hellman-group14	2048 비트
RFC 8268	diffie-hellman-group14	2048 비트
RFC 8268	diffie-hellman-group15	3072 비트

ST 작성자 註

○ 본 SFR은 관리자가 원격에서 안전한 경로(SSH)로 TOE 관리수단(CLI)에 접속하여 데이터를 전송하는 경우 이들 데이터에 대한 암호화 및 MAC값 생성에 사용할 세션키 생성에 관한 것이다.

○ SSHv2(RFC4253)에서 정의한 Transport Layer Protocol에서 생성하는 세션키(클라이언트의 초기벡터, AES 암호키, HMAC 키와 서버의 초기벡터, AES 암호키, HMAC 키)에 관한 사항을 정의한 것이며 키생성 알고리즘은 HASH 함수를 사용하되 RFC4253에서 특정하고 있지 않으므로 HASH 함수로 명세하였다.

○ SSHv2(RFC4253)에서 정의한 Trasnport Layer Protocol에서 세션키 생성에 필요한 비밀정보 공유에 사용할 D-H 공개키 생성에 관한 것이다.

○ SSHv2(RFC4253)에서 정의한 Trasnport Layer Protocol에서 서버인증을 위한 공개키는 TOE에서 생성하지 않고 외부에서 생성한 공개키를 TOE에 등록하는 방식을 적용하고 있으므로 본 요구사항에서는 비대칭키 생성에 관한 사항은 해당사항이 없다.

6.1.3. 사용자 데이터 보호(FDP)

(가) FDP_IFC.2 완전한 정보흐름 통제

계층관계 FDP_IFC.1 부분적인 정보흐름 통제

종속관계 FDP_IFF.1 단일 계층 보안속성

FDP_IFC.2.1 TSF는 [다음의 주체 목록 및 정보 목록]과 SFP에 의하여 다루어지는 통제된 주체로/주체로부터의 정보흐름을 유발하는 모든 오퍼레이션에 대하여 [상태기반 트래픽 필터링 SFP]를 강제해야 한다.

침입차단 방식	주체	정보
상태기반 트래픽 필터링	패킷 송신자	패킷 필터링에 의해 통과된 트래픽

FDP_IFC.2.2 TSF는 TOE 내의 모든 주체로/주체로부터 TOE내의 모든 정보흐름을 유발하는 모든 오퍼레이션들이 정보흐름 통제 SFP에 의하여 다루어짐을 보장해야 한다.

6.1.4. 식별 및 인증(FIA)

(가) FIA_AFL.1(1) 인증 실패 처리(패스워드 기반 관리자 인증)

계층관계	없음
종속관계	FIA_UAU.1 인증
FIA_AFL.1.1	TSF는 [WebGUI 로그인, SSH 접속을 통한 CLI 로그인, 로컬콘솔을 통한 CLI 로그인] 에 관련된 *[3]*번의 실패한 인증 시도가 발생한 경우 이를 탐지해야 한다.
FIA_AFL.1.2	실패한 인증 시도가 정의된 횟수에 도달하면, TSF는 [5분 ~ 30분 범위에서 관리자가 설정한 인증지연 시간을 경과할 때 까지 관리접속 중단]을 수행해야 한다.

6.1.5. 보안 관리(FMT)

(가) FMT_MOF.1 보안기능 관리

☞ FMT_MOF.1.1의 표는 국가용 보안요구사항 서버 공통보안요구사항에 명시되어 있는 내용이며 ST 작성자는 보안관리 기능에 적합한 TOE의 보안기능을 명세해야함

계층관계	없음
종속관계	FMT_SMF.1 관리기능 명세 FMT_SMR.1 보안 역할
FMT_MOF.1.1	TSF는 [다음 표]의 기능에 대해 *관리 행동*을 하는 능력을 [인가된 관리자]로 제한해야 한다.

소분류	보안관리
식별 및 인증	사용자의 등록, 삭제, 수정, 권한 부여
	사용자의 패스워드 조합·길이 정책 설정
	사용자의 인증 실패 허용 횟수 설정
	사용자의 인증 실패 대응방법 설정
	사용자의 인증기능 비활성화된 후 활성화 까지의 시간 설정
	TOE가 인증하는 외부 IT 실체 인증정보 설정
보안 관리	관리용 단말기의 IP 등록, 삭제, 수정
	중요 데이터, 설정정보, 감사기록 등의 백업
	중요 데이터, 설정정보, 감사기록 등의 복구
	관리접속 서비스 활성화, 비활성화
	외부 IT 실체 접근을 위한 인증정보 설정

소분류	보안관리
자체 보호	관리자 요청에 의한 TOE의 보안기능 자체시험 수행
	자체시험 실패 시 대응행동 설정
	관리자 요청에 의한 TOE의 설정값 및 TOE 자체의 무결성 검사 수행
	무결성 검사 실패 시 대응행동 설정
업데이트 보호	관리자에 의한 업데이트 파일 유효성 수동 검증
	관리자에 의한 업데이트 파일 설치 실패 수동 복구
	TOE 버전정보 조회
안전한 세션 관리	사용자 세션 잠금, 종료시간 설정
	(세션 잠금의 경우)세션의 잠금 해제시 관리자 또는 개별 사용자 인증
	사용자 동시 접속 세션 수 설정
감사기록	감사기록의 조회
	감사기록 손실 대응 관련 설정

[표 4] 보안관리 기능 목록

ST 작성자 註

○ 정교화 오퍼레이션을 적용한 “관리 행동”은 일부 TSF 기능에 대해 행동을 결정(determine the behavior), 중지(disable), 개시(enable), 행동을 변경(modify the behaviour of)하는 능력을 모두 포함한다.

6.1.6. TSF 보호(FPT)

(가) FPT_STM.1 신뢰할 수 있는 타임스탬프

계층관계	없음
종속관계	없음
FPT_STM.1.1	TSF는 신뢰할 수 있는 타임스탬프를 제공할 수 있어야 한다.

6.1.7. TOE 접근(FTA)

(가) FTA_MCS.2 사용자 속성별 동시 세션 수의 제한

계층관계	FTA_MCS.1 기본적인 동시 세션 수의 제한
종속관계	FIA_UID.1 식별
FTA_MCS.2.1	TSF는 [동일 권한을 갖는 관리자 및 동일 관리자 동시 세션의 최대 수는 1로 제한, 동시 세션 연결금지] 규칙에 따라서 동일 **관리자**에 속하는 동시 세션의 최대 수를 제한해야 한다.
FTA_MCS.2.2	TSF는 기본적으로 **관리자**별로 [1] 개의 세션 한계치를 강제해야 한다.

※ SFR 식별 및 오퍼레이션 수행 절차

1단계 TOE 범위산정 과정을 통해 TOE 유형을 식별하고 TOE 운영환경을 설정한다.

- TOE의 보안기능을 국가용 보안요구사항 기능명 또는 보안기능성으로 열거한다.
- CC 2부의 클래스 분류에 따라 1차 분류하고 패밀리 분류에 따라 2차 분류한다.

보안기능에 연관된 클래스 및 패밀리	
국가용 보안요구사항 기능명 또는 보안기능성	국가용 보안요구사항 기능명 또는 보안기능성
로깅 및 감사 기능	FAU
식별 및 인증	FIA
암호연산	FCS
접근통제	FDP_ACC, FDP_ACF
정보흐름통제	FDP_IFC, FDP_IFF
관리기능	FMT
사용자 데이터 보호	FDP_RIP, FDP_ITT, FDP_ROL
TSF 데이터 보호	FPT
외부 전송시 데이터 보호	FDP_ETC, FDP_ITC, FDP_UCT, FDP_UIT, FDP_DAU
	FTP
	FCO
TOE 접속시 보호	FTA

- 보안기능성을 SFR로 표현하기에 가장 적합한 컴포넌트를 선택한다.
  - ▷ 동일 보안기능성에 대해 2개 이상 컴포넌트가 선택되어 있는 경우 CC 2부 부록을 참조하여 가장 적합한 컴포넌트를 선택한다.
  - ▷ 선택한 컴포넌트에 대해 계층관계가 있는 컴포넌트를 조사하여 어느 것이 더 적합한가를 판단하여 최종 선택한다.
  - ▷ 컴포넌트가 선택되면 해당 컴포넌트의 종속관계가 있는 컴포넌트를 추가 식별한다.
- 선택한 컴포넌트와 TOE 보안목적에 대한 일치성을 조사하여 완전성 및 충분성을 검증한다.
  - ▷ 선택한 컴포넌트에 유사한 TOE에 관한 보안목적을 식별하여 컴포넌트와 TOE 보안목적 사이의 매핑표를 작성한다.
  - ▷ TOE 보안목적에 매핑되지 않은 컴포넌트가 존재하는 경우 해당 컴포넌트에 해당하는 보안기능성이 TOE 범위에 포함되어 있는지 여부를 판단한다.
    - TOE 범위에 포함되어 있지 않은 경우 “TOE 범위 산정 가이드”를 참조하여 비-TOE 또는 Non-TSF가 될 수 있는지 확인한 후 컴포넌트를 제거한다.
    - TOE 범위에 포함되어야 하는 경우 ST “TOE 설명”의 물리적 범위 및 논리적 범위를 재조정한다.
    - TOE 범위 재조정 후에 TOE 보안목적을 추가로 정의하고 이에 대응할 수 있는 보안문제정의가 존재하는지 확인한 후 존재하지 않으면 위협 또는 조직의 보안정책을 추가 정의한다.
  - ▷ 컴포넌트에 매핑되지 않은 TOE 보안목적이 존재하는 경우 TOE 보안목적에 매핑되는 컴포넌트를 추가 식별한다.

[예시] 방화벽에 대한 SFR 식별하기

1 방화벽 핵심기능을 나타내는 보안목적에 매핑되는 패밀리 및 컴포넌트 식별

1-1. TOE 논리적 범위에 연관되는 클래스 및 패밀리 식별

TOE 논리적 범위	패밀리
TOE는 방화벽 정책에 정의된 범위에서 ACL에 따라 네트워크 트래픽을 통제한다.	FDP_IFC, FDP_IFF
TOE는 인가된 운영자만이 방화벽의 ACL를 변경할 수 있도록 관리자 권한을 통제한다.	FIA_UAU, FIA_UID FMT_MSA

1-2. 선택된 패밀리에서 TOE 보안기능성에 가장 적합한 컴포넌트 1차 식별

TOE 보안기능성	컴포넌트
TOE는 인터페이스마다 영역(Zone)을 설정하고 영역마다 아웃바운드 트래픽과 인바운드 트래픽으로 구분하여 규칙을 적용한다. 따라서 영역(Zone)을 벗어나는 경우 규칙이 적용되지 못한다. 아웃바운드 트래픽에 대한 기본규칙은 any any deny이며 다만 80포트에 대해서는 모두 허용이다. 인바운트 트래픽에 대한 기본규칙은 any any deny이다.	FDP_IFC.1, FDP_IFF.1
방화벽 규칙을 변경하는 기능에 접근을 허용하기 전에 반드시 관리자 식별 및 인증을 과정을 수행한다. 인증연속 실패시 관리자가 지정한 일정시간 동안 인증 시도를 차단한다. 식별 및 인증에 성공한 관리자는 방화벽 규칙을 변경, 삭제, 추가할 수 있다.	FIA_UID.1 FIA_UAU.1, FIA_AFL.1 FMT_MSA.1

1-3. 1차 식별 컴포넌트와 종속관계에 있는 컴포넌트 2차 식별

보안기능성에 따라 식별된 컴포넌트	종속관계
FDP_IFC.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1
	FMT_MSA.3
FIA_UID.1	없음
FIA_UAU.1	FIA_UID.1
FIA_AFL.1	FIA_UAU.1
FMT_MSA.1	FDP_IFC.1 FMT_SMF.1, FMT_SMR.1

1-4 보안목적과 컴포넌트 매핑표 작성

보안목적	컴포넌트
O.OUT_TRAFFIC : TOE는 방화벽 정책에 따라 LAN에서 WAN으로 나가는 네트워크 트래픽을 차단할 수 있어야 한다.	FDP_IFC.1, FDP_IFC.1
O.IN_TRAFFIC : TOE는 방화벽 정책에 따라 WAN에서 LAN으로 유입되는 네트워크 트래픽을 차단할 수 있어야 한다.	FDP_IFC.1, FDP_IFC.1
O.OPERATOR : TOE는 방화벽 정책 변경을 인가된 운영자에게만 허용해야 한다.	FMT_MSA.1, FMT_MSA.3
O.LOGON : 운영자 역할을 사용하려는 자에 대해 식별 및 인증을 수행해야 한다. 연속 인증 실패시 일정기간 동안 인증 시도를 차단해야 한다.	FIA_UAU.1, FIA_UID.1, FIA_AFL.1 FMT_SMF.1, FMT_SMR.1

2 방화벽 부가기능(예: 감사기능)에 연관된 컴포넌트 식별	
2-1. 방화벽 감사기능의 핵심 요소에 대해 컴포넌트 1차 식별	
로깅할 대상(이벤트) 정의	FAU_SEL.1
로깅시 기록할 정보유형 식별	FAU_GEN.1
감사기록을 생성하는 기능	FAU_GEN.1
생성된 감사기록을 저장하는 기능	FAU_STG.1
사전에 정의된 사건이 발생하는 경우 알람을 발생하는 기능	FAU_ARP.1
저장된 감사기록을 조회하는 기능	FAU_SAR.1
2-2. 1차 식별한 컴포넌트와 종속관계에 있는 컴포넌트 2차 식별	
감사기능에 매핑되는 컴포넌트 종속관계	패밀리
FAU_SEL.1	FAU_GEN.1 FMT_MTD.1
FAU_GEN.1	FPT_STM.1
FAU_STG.1	FAU_GEN.1
FAU_ARP.1	FAU_SAA.1
FAU_SAR.1	FAU_GEN.1
2-3. 1 단계에서 식별된 컴포넌트에 대해 FAU_GEN.1에 감사수준별 감사대상 사건 식별	
TOE 논리적 범위	패밀리
FDP_IFF.1	기본 : 정보흐름 요청에 대한 모든 결정
FIA_UAU.1	기본 : 인증 메커니즘의 모든 사용
FAU_ARP.1	최소 : 실패한 인증 시도의 한계치 도달과 취해진 행동

2단계 1단계에서 식별한 컴포넌트의 엘리먼트에 대해 오퍼레이션을 적용한다.

- ST에서는 미완성 상태의 오퍼레이션을 갖는 엘리먼트를 허용하지 않는다.
- 오퍼레이션 적용의 정확성을 위해 CC 2부의 부록을 반드시 참조 한다.

  ▷ CC 2부 부록 F에서 FDP_ACF.1.1 할당 오퍼레이션 적용시 주의사항

[예시] 방화벽 보안정책 정의 및 이에 따른 FDP_IFC 및 FDP_IFF 오퍼레이션 적용

1 방화벽 보안정책 “Firewall SFP” 정의

Type	약칭	정의
주체	S_LAN	내부망에 연결되는 방화벽 인터페이스
	S_WAN	외부망에 연결되는 방화벽 인터페이스
정보	I_Network	방화벽 인터페이스(S_LAN, W_LAN)를 통과하는 모든 네트워크 트래픽
오퍼레이션	차단	네트워크 데이터그램을 차단하여 방화벽 인터페이스로 전송하지 않음
	라우팅	네트워크 데이터그램을 차단하지 않고 방화벽 인터페이스로 전송함
주체의 보안속성	IP주소	방화벽 인터페이스에 할당된 IP주소(공인 IP주소, 사설 IP주소, NAC 주소)
정보의 보안속성	출발지 IP/포트 목적지 IP/포트 패킷 유형	관련 표준(RFC xxx)에 따름
규칙	R_Incoming	WAN 인터페이스를 경유하여 TOE로 유입되는 모든 네트워크 트래픽을 Traffic_Policy에 따라 라우팅하거나 차단한다.
	R_Outgoing	LAN 인터페이스를 경유하여 TOE로 유입되는 모든 네트워크 트래픽을 Traffic_Policy에 따라 라우팅하거나 차단한다.
TSF 데이터	Traffic_Policy	TOE 운영역할을 가진 자에 의해 정의된 네트워크 트래픽 보안정책

2 FDP_IFC.1 및 FDP_IFF.1 오퍼레이션 적용

컴포넌트	엘리먼트	오퍼레이션	수행 내용
FDP_IFC.1	FDP_IFC.1.1	[할당 : 정보흐름통제 SFP]	Firewall SFP
		[할당 : 정보흐름통제 SFP에 따라 통제되는 주체, 정보 및 오퍼레이션 목록]	주체 : S_LAN, S_WAN 정보 : I_Network 오퍼레이션 : 차단, 라우팅
FDP_IFF.1	FDP_IFF.1.1	[할당 : 정보흐름통제 SFP]	Firewall SFP
		[할당 : 정보흐름통제 SFP에 따라 통제 되는 주체 및 해당 주체의 보안속성]	S_LAN : 사설 IP주소 W_LAN : 공인 IP주소
	FDP_IFF.1.2	[할당 : 오퍼레이션 마다 주체 보안속성과 정보 보안속성 사이에 유지되어야 하는 관계]	R_Incoming R_Outgoing
	FDP_IFF.1.3	[정보흐름통제 SFP의 추가적인 규칙]	추가 규칙 없음
	FDP_IFF.1.4	[명시적으로 보안속성에 기반한 정보흐름을 허용하는 규칙]	없음
	FDP_IFF.1.5	[명시적으로 보안속성에 기반한 정보흐름을 허용하는 규칙]	없음

3단계 TOE의 보안기능성을 정확하게 표현하기에 오퍼레이션 적용이 어려운 경우 확장 컴포넌트를 정의한다.

- 확장 컴포넌트 정의 방법은 본 가이드의 2.5.2절 참조

4단계 컴포넌트의 엘리먼트에 오퍼레이션을 수행하면서 사용한 용어를 정의한다.

- FDP_ACC 또는 FDP_IFC에서 정의한 보안정책의 적용범위를 참조하여 해당 범위에 포함되는 모든 주체, 객체, 오퍼레이션, 정보 유형을 식별하고 이들이 가질 수 있는 값의 범위를 조사한다.
- FDP_ACC 또는 FDP_IFC에서 식별된 용어 이외에 다른 컴포넌트의 엘리먼트에서 사용된 용어를 모두 식별한다.
- TOE의 보안기능성을 수행하는데 외부 IT 실체가 필요한 경우 이에 대해 식별한다.
- CC 1부에서 정의한 용어정의는 반복 정의할 필요 없이 생략한다.
- 식별된 용어를 정의하는 경우 관련 표준에서 규정한 용어정의를 가능한 인용한다.
- CC 2부 부록의 컴포넌트 마다 서술되어 있는 “사용자 응용 시 주의사항”을 참고하여 용어정의를 보완한다.
- 일반 IT지식수준에서 벗어나 ST 내에서 특별히 다르게 사용되는 용어의 경우 반드시 용어정의에 포함시킨다.

6.2. 보증요구사항

☞ 국내용 평가보증등급(EAL2~EAL4)에 따른 제출문서는 '정보보호제품 평가 · 인증 안내서'의 국내용 평가 인증 절차 중 최초평가 및 재평가 부분을 참고

본 보안목표명세서의 보증요구사항은 공통평가기준 3부의 보증 컴포넌트로 구성되었고, 평가보증등급은 국내용 EAL4이다. 다음 표는 CC Part 3에서 정의한 EAL4 보증 컴포넌트와 국내용 평가보증등급 EAL4를 요약하여 보여준다.

보증클래스	CC Part3 보증 컴포넌트		국내용 평가보증등급
보안목표 명세서	ASE_INT.1	보안목표명세서 소개	좌동
	ASE_CCL.1	준수 선언	좌동
	ASE_SPD.1	보안문제 정의	좌동
	ASE_OBJ.1	운영환경에 대한 보안목적	좌동
	ASE_ECD.1	확장 컴포넌트 정의	좌동
	ASE_REQ.2	도출된 보안요구사항	좌동
	ASE_TSS.1	TOE 요약명세	좌동
개발	ADV_ARC.1	보안 아키텍처 설명	개발자 취약성 분석서로 대체
	ADV_FSP.4	완전한 기능명세	생략
	ADV_IMP.1	TSF에 대한 구현의 표현	소스코드 취약점 분석서로 대체
	ADV_TDS.3	기본적인 모듈화 설계	업체 자체 개발문서로 대체
설명서	AGD_OPE.1	사용자 운영 설명서	좌동
	AGD_PRE.1	준비 절차	좌동
생명주기지원	ALC_CMC.4	생산지원, 수용절차 및 자동화	내규/지침으로 대체 가능
	ALC_CMS.4	문제추적 형상관리 범위	
	ALC_DEL.1	배포 절차	
	ALC_DVS.1	보안대책의 식별	
	ALC_LCD.1	개발자가 정의한 생명주기 모델	
	ALC_TAT.1	잘 정의된 개발 도구	
시험	ATE_COV.2	시험범위의 분석	개발자 전체 기능시험서로 대체
	ATE_DPT.1	기본설계 시험	
	ATE_FUN.1	기능 시험	좌동
	ATE_IND.2	독립적인 시험 : 표본 시험	평가자 전체 기능시험 수행
취약성 평가	AVA_VAN.3	집중화된 취약성 분석	좌동

[표 6] EAL4 보증패키지와 국내용 EAL4 평가보증등급

본 ST는 국내용 EAL4 평가보증등급 준수를 선언하였으며 이에 따른 보증요구사항은 다음과 같다.

6.2.1. 보안목표명세서 평가

(가) ASE_INT.1 보안목표명세서 소개

종속관계	없음

개발자 요구사항

ASE_INT.1.1D	개발자는 보안목표명세서 소개를 제공해야 한다.

증거 요구사항

ASE_INT.1.1C	보안목표명세서 소개는 보안목표명세서 참조, TOE 참조, TOE 개요, TOE 설명을 포함해야 한다.
ASE_INT.1.2C	보안목표명세서 참조는 유일하게 보안목표명세서를 식별해야 한다.
ASE_INT.1.3C	TOE 참조는 TOE를 식별해야 한다.
ASE_INT.1.4C	TOE 개요는 TOE의 용도와 주요 보안 특성을 요약해야 한다.
ASE_INT.1.5C	TOE 개요는 TOE 유형을 식별해야 한다.
ASE_INT.1.6C	TOE 개요는 TOE에서 요구되는 비-TOE에 해당하는 하드웨어/소프트웨어/펌웨어를 식별해야 한다.
ASE_INT.1.7C	TOE 설명은 TOE의 물리적인 범위를 서술해야 한다.
ASE_INT.1.8C	TOE 설명은 TOE의 논리적인 범위를 서술해야 한다.

평가자 요구사항

ASE_INT.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.
ASE_INT.1.2E	평가자는 TOE 참조, TOE 개요, TOE 설명이 서로 일관성이 있음을 확인해야 한다.

(나) ASE_CCL.1 준수선언

종속관계	ASE_INT.1 보안목표명세서 소개 ASE_ECD.1 확장 컴포넌트 정의 ASE_REQ.1 명시된 보안요구사항

개발자 요구사항

ASE_CCL.1.1D	개발자는 준수 선언을 제공해야 한다.
ASE_CCL.1.2D	개발자는 준수 선언의 이론적 근거를 제공해야 한다.

증거 요구사항

ASE_CCL.1.1C	준수 선언은 보안목표명세서 및 TOE가 준수하는 공통평가기준의 버전을 식별하기 위해 공통평가기준 준수 선언을 포함해야 한다.
ASE_CCL.1.2C	공통평가기준 준수 선언은 보안목표명세서의 공통평가기준 2부에 대한 준수 선언을 “2부 준수” 또는 “2부 확장”으로 서술해야 한다.
ASE_CCL.1.3C	공통평가기준 준수 선언은 보안목표명세서의 공통평가기준 3부에 대한 준수 선언을 “3부 준수” 또는 “3부 확장”으로 서술해야 한다.
ASE_CCL.1.4C	공통평가기준 준수 선언은 확장 컴포넌트 정의와 일관성이 있어야 한다.
ASE_CCL.1.5C	준수 선언은 보안목표명세서가 준수하는 모든 보호프로파일 및 보안요구사항 패키지를 식별해야 한다.
ASE_CCL.1.6C	준수 선언은 보안목표명세서의 패키지에 대한 준수 선언을 '패키지 준수' 또는 '패키지 추가'로 서술해야 한다.
ASE_CCL.1.7C	준수 선언의 이론적 근거는 보안목표명세서의 TOE 유형이 그 보안목표명세서가 준수하는 보호프로파일의 TOE 유형과 일관성이 있음을 입증해야 한다.
ASE_CCL.1.8C	준수 선언의 이론적 근거는 보안목표명세서의 보안문제정의에 대한 설명이 그 보안목표명세서가 준수하는 보호프로파일의 보안문제정의 설명과 일관성이 있음을 입증해야 한다.
ASE_CCL.1.9C	준수 선언의 이론적 근거는 보안목표명세서의 보안목적에 대한 설명이 그 보안목표명세서가 준수하는 보호프로파일의 보안목적 설명과 일관성이 있음을 입증해야 한다.
ASE_CCL.1.10C	준수 선언의 이론적 근거는 보안목표명세서의 보안요구사항에 대한 설명이 그 보안목표명세서가 준수하는 보호프로파일의 보안요구사항 설명과 일관성이 있음을 입증해야 한다.

평가자 요구사항

ASE_CCL.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(다) ASE_SPD.1 보안문제정의

종속관계 없음

개발자 요구사항

ASE_SPD.1.1D	개발자는 보안문제정의를 제공해야 한다.

증거 요구사항

ASE_SPD.1.1C	보안문제정의는 위협을 서술해야 한다.
ASE_SPD.1.2C	모든 위협은 위협원, 자산, 악의적 행동의 관점에서 서술되어야 한다.
ASE_SPD.1.3C	보안문제정의는 조직의 보안정책(OSP)을 서술해야 한다.
ASE_SPD.1.4C	보안문제정의는 TOE 운영환경에 관한 가정사항을 서술해야 한다.

평가자 요구사항

ASE_SPD.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(라) ASE_OBJ.2 보안목적

종속관계	ASE_SPD.1 보안문제정의

개발자 요구사항

ASE_OBJ.1.1D	개발자는 보안목적에 대한 설명을 제공해야 한다.

증거 요구사항

ASE_OBJ.2.1C	보안목적에 대한 설명은 TOE 보안목적과 운영환경에 대한 보안목적을 서술해야 한다.
ASE_OBJ.2.2C	보안목적의 이론적 근거는 TOE에 대한 각 보안목적을 보안목적에 의해 대응되는 위협과 보안목적에 의해 수행되는 조직의 보안으로 추적해야 한다.
ASE_OBJ.2.3C	보안목적의 이론적 근거는 운영환경에 대한 각 보안목적을 보안목적에 의해 대응되는 위협, 보안목적에 의해 수행되는 조직의 보안정책, 보안목적에 의해 지원되는 가정사항으로 추적해야 한다.
ASE_OBJ.2.4C	보안목적의 이론적 근거는 보안목적이 모든 위협에 대응함을 입증해야 한다.
ASE_OBJ.2.5C	보안목적의 이론적 근거는 보안목적이 모든 조직의 보안정책을 수행함을 입증해야 한다.
ASE_OBJ.2.6C	보안목적의 이론적 근거는 운영환경에 대한 보안목적이 모든 가정사항을 지원함을 입증해야 한다.

평가자 요구사항

ASE_OBJ.2.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(마) ASE_ECD.1 확장 컴포넌트 정의

종속관계 없음

개발자 요구사항

ASE_ECD.1.1D 개발자는 보안요구사항에 대한 설명을 제공해야 한다.

ASE_ECD.1.2D 개발자는 확장 컴포넌트 정의를 제공해야 한다.

증거 요구사항

ASE_ECD.1.1C 보안요구사항에 대한 설명은 확장된 모든 보안요구사항을 식별해야 한다.

ASE_ECD.1.2C 확장 컴포넌트 정의는 각각 확장된 보안요구사항에 대한 확장 컴포넌트를 정의해야 한다.

ASE_ECD.1.3C 확장 컴포넌트 정의는 각 확장 컴포넌트가 기존의 공통평가기준 컴포넌트, 패밀리, 클래스와 어떻게 연관되는지를 서술해야 한다.

ASE_ECD.1.4C 확장 컴포넌트 정의는 기존의 공통평가기준 컴포넌트, 패밀리, 클래스와 방법론을 모델로 하여 표현해야 한다.

ASE_ECD.1.5C 확장 컴포넌트는 각 엘리먼트에 대한 준수 여부를 입증할 수 있도록 측정 가능하고 객관적인 엘리먼트로 구성되어야 한다.

평가자 요구사항

ASE_ECD.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

ASE_ECD.1.2E 평가자는 확장된 컴포넌트가 기존의 컴포넌트를 이용하여 명확히 표현할 수 없음을 확인해야 한다.

(바) ASE_REQ.2 도출된 보안요구사항

종속관계 ASE_OBJ.2 보안목적
ASE_ECD.1 확장 컴포넌트 정의

개발자 요구사항

ASE_REQ.1.1D 개발자는 보안요구사항에 대한 설명을 제공해야 한다.

ASE_REQ.1.2D 개발자는 보안요구사항의 이론적 근거를 제공해야 한다.

증거 요구사항

ASE_REQ.2.1C	보안요구사항에 대한 설명은 보안기능요구사항과 보증요구사항을 서술해야 한다.
ASE_REQ.2.2C	보안기능요구사항 및 보증요구사항에서 사용되는 모든 주체, 객체, 오퍼레이션, 보안 속성, 외부 실체, 기타 용어들은 정의되어야 한다.
ASE_REQ.2.3C	보안요구사항에 대한 설명은 보안요구사항에 대한 모든 오퍼레이션을 식별해야 한다.
ASE_REQ.2.4C	모든 오퍼레이션은 정확히 수행되어야 한다.
ASE_REQ.2.5C	보안요구사항의 각 종속관계는 만족되어야 하며, 그렇지 않을 경우에는 보안요구사항의 이론적 근거에 그에 대한 정당화가 제공되어야 한다.
ASE_REQ.2.6C	보안요구사항의 이론적 근거는 각 보안기능요구사항을 TOE에 대한 보안목적으로 추적해야 한다.
ASE_REQ.2.7C	보안요구사항의 이론적 근거는 보안기능요구사항이 TOE에 대한 모든 보안목적을 만족한다는 것을 입증해야 한다. 보안요구사항의 이론적 근거는 보증요구사항이 선택된 이유를 설명해야 한다.
ASE_REQ.2.8C	보안요구사항에 대한 설명은 내부적으로 일관성이 있어야 한다.

평가자 요구사항

ASE_REQ.2.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(사) ASE_TSS.1 TOE 요약명세

종속관계	ASE_INT.1 보안목표명세서 소개 ASE_REQ.1 명시된 보안요구사항 ADV_FSP.1 기본적인 기능명세

개발자 요구사항

ASE_TSS.1.1D	개발자는 TOE 요약명세를 제공해야 한다.

증거 요구사항

ASE_TSS.1.1C	TOE 요약명세는 TOE가 어떻게 각각의 보안기능요구사항을 만족시키는지 서술해야 한다.

평가자 요구사항

ASE_TSS.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.
ASE_TSS.1.2E	평가자는 TOE 요약명세가 TOE 개요 및 TOE 설명과 일관성이 있음을 확인해야 한다.

6.2.2. 개발

(가) ADV_ARC.1 기본적인 기능명세

종속관계 ADV_FSP.1 기본적인 기능명세
ADV_TDS.1 기본적인 설계

개발자 요구사항

ADV_ARC.1.1D 개발자는 TSF의 보안특성이 우회되지 않도록 TOE를 설계하고 구현해야 한다.

ADV_ARC.1.2D 개발자는 신뢰되지 않은 능동적 실체에 의한 침해로부터 TSF 자체를 보호할 수 있도록 TSF를 설계하고 구현해야 한다.

ADV_ARC.1.3D 개발자는 TSF의 보안 아키텍쳐 설명을 제공해야 한다.

증거 요구사항

ADV_ARC.1.1C 보안 아키텍쳐 설명은 TOE 설계문서에 서술된 SFR-수행 추상화 설명에 알맞은 상세 수준으로 서술되어야 한다.

ADV_ARC.1.2C 보안 아키텍쳐 설명은 TSF에 의해서 SFR과 일관성 있게 유지되어야 하는 보안영역을 서술해야 한다.

ADV_ARC.1.3C 보안 아키텍쳐 설명은 TSF 초기화 과정이 어떻게 안전한지 서술해야 한다.

ADV_ARC.1.4C 보안 아키텍쳐 설명은 TSF가 침해로부터 자신을 보호함을 입증해야 한다.

ADV_ARC.1.5C 보안 아키텍쳐 설명은 TSF가 SFR-수행 기능성의 우회를 방지함을 입증해야 한다.

평가자 요구사항

ADV_ARC.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(나) ADV_FSP.4 완전한 기능명세

종속관계 없음

개발자 요구사항

ADV_FSP.4.1D 개발자는 기능명세를 제공해야 한다.

ADV_FSP.4.2D 개발자는 기능명세에서 SFR로의 추적성을 제공해야 한다.

증거 요구사항

ADV_FSP.4.1C	기능명세는 TSF를 완전하게 표현해야 한다.
ADV_FSP.4.2C	기능명세는 모든 TSFI에 대한 목적과 사용 방법을 서술해야 한다.
ADV_FSP.4.3C	기능명세는 각 TSFI와 관련된 모든 매개변수를 식별 및 서술해야 한다.
ADV_FSP.4.4C	기능명세는 각 TSFI에 관련된 모든 행동을 서술해야 한다.
ADV_FSP.4.5C	기능명세는 각 TSFI 호출 결과로 발생하는 모든 직접적인 오류메시지를 서술해야 한다.
ADV_FSP.4.6C	추적성은 SFR이 기능명세 내의 TSFI로 추적됨을 입증해야 한다.

평가자 요구사항

ADV_FSP.4.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.
ADV_FSP.4.2E	평가자는 기능명세가 SFR을 정확하고 완전하게 실체화하는지 결정해야 한다.

(다) ADV_IMP.1 TSF에 대한 구현의 표현

종속관계	ADV_TDS.3 기본적인 모듈화 설계 ALC_TAT.1 잘 정의된 개발 도구

개발자 요구사항

ADV_IMP.1.1D	개발자는 전체 TSF에 대한 구현의 표현을 가용하게 해야 한다.
ADV_IMP.1.2D	개발자는 TOE 설계 설명과 구현의 표현 표본간의 대응관계를 제공해야 한다.

증거 요구사항

ADV_IMP.1.1C	구현의 표현은 더 이상의 설계과정 없이 TSF가 생성될 수 있는 상세수준으로 TSF를 정의해야 한다.
ADV_IMP.1.2C	구현의 표현은 개발 인력이 사용한 형태이어야 한다.
ADV_IMP.1.3C	TOE 설계 설명과 구현의 표현 표본간의 대응관계는 이들의 일치성을 입증해야 한다.

평가자 요구사항

ADV_IMP.1.1E	평가자는 선택된 구현의 표현 표본에 대해 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(라) ADV_TDS.3 기본적인 모듈화 설계

종속관계 ADV_FSP.4 완전한 기능명세

개발자 요구사항

ADV_TDS.3.1D 개발자는 TOE 설계를 제공해야 한다.

ADV_TDS.3.2D 개발자는 기능명세의 TSFI와 TOE 설계에 사용 가능한 가장 상세수준 분해간의 대응관계를 제공해야 한다.

증거 요구사항

ADV_TDS.3.1C 설계는 TOE의 구조를 서브시스템 측면에서 서술해야 한다.

ADV_TDS.3.2C 설계는 TSF를 모듈 측면에서 서술해야 한다.

ADV_TDS.3.3C 설계는 TSF의 모든 서브시스템을 식별해야 한다.

ADV_TDS.3.4C 설계는 TSF의 각 서브시스템에 대한 설명을 제공해야 한다.

ADV_TDS.3.5C 설계는 TSF의 모든 서브시스템들 간의 상호작용에 대한 설명을 제공해야 한다.

ADV_TDS.3.6C 설계는 TSF 서브시스템과 TSF 모듈간의 대응관계를 제공해야 한다.

ADV_TDS.3.7C 설계는 각 SFR-수행 모듈을 그 목적 및 다른 모듈 간의 상관관계 측면에서 서술해야 한다.

ADV_TDS.3.8C 설계는 각 SFR-수행 모듈을 SFR-관련 인터페이스, 인터페이스로부터의 반환 값, 다른 모듈과의 상호작용 및 다른 SFR-수행 모듈에서 호출된 SFR-관련 인터페이스 측면에서 서술해야 한다.

ADV_TDS.3.9C 설계는 각 SFR-지원 또는 SFR-비-간섭 모듈을 목적 및 다른 모듈과의 상호작용 측면에서 서술해야 한다.

ADV_TDS.3.10C 대응관계는 모든 TSFI가 자신이 호출하는 TOE 설계 내에 서술된 행동으로 추적됨을 입증해야 한다.

평가자 요구사항

ADV_TDS.31E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

ADV_TDS.32E 평가자는 설계가 모든 보안기능요구사항을 정확하고 완전하게 실체화하는지 결정해야 한다.

6.2.3. 설명서

(가) AGD_OPE.1 사용자 운영 설명서

종속관계 ADV_FSP.1 기본적인 기능명세

개발자 요구사항

AGD_OPE.1.1D 개발자는 사용자 운영 설명서를 제공해야 한다.

증거 요구사항

AGD_OPE.1.1C 사용자 운영 설명서는 각각의 사용자 역할에 대해 안전한 처리환경 내에서 통제되어야 하는 사용자가 접근 가능한 기능 및 특권에 대해 적절한 경고를 포함해서 서술해야 한다.

AGD_OPE.1.2C 사용자 운영 설명서는 각각의 사용자 역할에 대해 TOE에 의해 안전한 방식으로 제공되는 인터페이스의 사용 방법을 서술해야 한다.

AGD_OPE.1.3C 사용자 운영 설명서는 각각의 사용자 역할에 대해 사용 가능한 기능 및 인터페이스를 서술해야 한다. 특히 사용자의 통제 하에 있는 모든 보안 매개변수에 대해 안전한 값을 적절하게 표시해야 한다.

AGD_OPE.1.4C 사용자 운영 설명서는 각각의 사용자 역할에 대해, 수행되어야 할 사용자가 접근할 수 있는 기능과 연관된 보안-관련 사건의 각 유형을 명확히 제시해야 한다. 여기에는 TSF의 통제 하에 있는 실체에 대한 보안 특성의 변경도 포함되어야 한다.

AGD_OPE.1.5C 사용자 운영 설명서는 (장애 후의 운영 또는 운영상의 오류 후의 운영을 포함한) TOE의 모든 가능한 운영 모드, 그 영향 및 안전한 운영 유지를 위한 관련사항들을 식별해야 한다.

AGD_OPE.1.6C 사용자 운영 설명서는 각각의 사용자 역할에 대해 보안목표명세서에 기술된 대로 운영환경에 대한 보안목적을 만족시키기 위해 준수해야 하는 보안대책을 서술해야 한다

AGD_OPE.1.7C 사용자 운영 설명서는 명확하고 타당해야 한다.

평가자 요구사항

AGD_OPE.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(나) AGD_PRE.1 준비 절차

종속관계 없음

개발자 요구사항

AGD_PRE.1.1D 개발자는 준비 절차를 포함하여 TOE를 제공해야 한다.

증거 요구사항

AGD_PRE1.1C 준비 절차는 배포된 TOE의 안전한 인수를 위해 필요한 모든 단계를 개발자의 배포 절차와 일관되게 서술해야 한다.

AGD_PRE1.2C 준비 절차는 TOE의 안전한 설치 및 운영환경의 안전한 준비를 위해 필요한 모든 단계를 보안목표명세서에 기술된 운영환경에 대한 보안목적과 일관되게 서술해야 한다.

평가자 요구사항

AGD_PRE.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

AGD_PRE.1.2E 평가자는 TOE가 운영을 위해 안전하게 준비될 수 있음을 확인하기 위해 준비 절차를 적용해야 한다.

6.2.4. 생명주기 지원

(가) ALC_CMC.4 생산지원, 수용절차 및 자동화

종속관계 ALC_CMS.1 TOE 형상관리 범위
ALC_DVS.1 보안대책의 식별
ALC_LCD.1 개발자가 정의한 생명주기 모델

개발자 요구사항

ALC_CMC.4.1D 개발자는 TOE 및 그에 대한 참조를 제공해야 한다.

ALC_CMC.4.2D 개발자는 형상관리 문서를 제공해야 한다.

ALC_CMC.4.3D 개발자는 형상관리 시스템을 사용해야 한다.

증거 요구사항

ALC_CMC.4.1C TOE는 유일한 참조를 위한 레이블을 붙여야 한다.

ALC_CMC.4.2C 형상관리 문서는 형상항목을 유일하게 식별하는 데 사용된 방법을 서술해야 한다.

ALC_CMC.4.3C	형상관리 시스템은 모든 형상항목을 유일하게 식별해야 한다.
ALC_CMC.4.4C	형상관리 시스템은 형상항목에 인가된 변경만을 허용하는 자동화된 수단을 제공해야 한다.
ALC_CMC.4.5C	형상관리 시스템은 자동화된 수단을 이용하여 TOE의 생산을 지원해야 한다.
ALC_CMC.4.6C	형상관리 문서는 형상관리 계획을 포함해야 한다.
ALC_CMC.4.7C	형상관리 계획은 형상관리 시스템이 TOE 개발에 사용되는 방법을 서술해야 한다.
ALC_CMC.4.8C	형상관리 계획은 변경되거나 새로 생성된 형상항목을 TOE의 일부로 수용하는데 사용된 절차를 서술해야 한다.
ALC_CMC.4.9C	증거는 모든 형상항목이 형상관리 시스템 하에 유지되고 있음을 입증해야 한다.
ALC_CMC.4.10C	증거는 형상관리 시스템이 형상관리 계획에 따라 운영되고 있음을 입증해야 한다.

평가자 요구사항

ALC_CMC.4.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(나) ALC_CMS.4 문제추적 형상관리 범위

종속관계	없음

개발자 요구사항

ALC_CMS.4.1D	개발자는 TOE에 대한 형상목록을 제공해야 한다.

증거 요구사항

ALC_CMS.4.1C	형상목록은 TOE, 보증요구사항에서 요구하는 평가증거, TOE를 구성하는 부분, 구현 표현, 보안 결함 보고서 및 해결 상태를 포함해야 한다.
ALC_CMS.4.2C	형상목록은 형상항목을 유일하게 식별해야 한다.
ALC_CMS.4.3C	형상목록은 각 TSF 관련 형상항목의 개발자를 표시해야 한다.

평가자 요구사항

ALC_CMS.4.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(다) ALC_DEL.1 배포 절차

종속관계 없음

개발자 요구사항

ALC_DEL.1.1D 개발자는 소비자에게 TOE나 TOE 일부를 배포하는 절차를 문서화하여 제공해야 한다.

ALC_DEL.1.2D 개발자는 배포 절차를 사용해야 한다.

증거 요구사항

ALC_DEL.1.1C 배포 문서는 TOE를 소비자에게 배포할 때 보안을 유지하기 위해 필요한 모든 절차를 서술해야 한다.

평가자 요구사항

ALC_DEL.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(라) ALC_DVS.1 보안대책의 식별

종속관계 없음

개발자 요구사항

ALC_DVS.1.1D 개발자는 개발보안 문서를 작성하여 제공해야 한다.

증거 요구사항

ALC_DVS.1.1C 개발보안 문서는 개발환경 내에서 TOE 설계 및 구현 과정의 비밀성과 무결성을 보호하기 위하여 필요한 물리적, 절차적, 기술적 및 기타 보안대책을 서술해야 한다.

평가자 요구사항

ALC_DVS.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

ALC_DVS.1.2E 평가자는 보안대책이 적용되고 있는지 확인해야 한다.

(마) ALC_LCD.1 개발자가 정의한 생명주기 모델

종속관계 없음

개발자 요구사항

ALC_LCD.1.1D 개발자는 TOE의 개발과 유지에 사용되는 생명주기 모델을 수립해야 한다.

ALC_LCD.1.2D 개발자는 생명주기 정의 문서를 제공해야 한다.

증거 요구사항

ALC_LCD.1.1C	생명주기 정의 문서는 TOE의 개발과 유지에 사용되는 모델을 서술해야 한다.
ALC_LCD.1.2C	생명주기 모델은 TOE의 개발과 유지에 필요한 통제를 제공해야 한다.

평가자 요구사항

ALC_LCD.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(바) ALC_TAT.1 잘 정의된 개발 도구

종속관계	ADV_IMP.1 TSF에 대한 구현의 표현

개발자 요구사항

ALC_TAT.1.1D	개발자는 TOE에 사용된 각 개발 도구를 식별한 문서를 제공해야 한다.
ALC_TAT.1.2D	개발자는 각 개발 도구에 대해 구현-종속적인 선택사항을 문서화하여 제공해야 한다.

증거 요구사항

ALC_TAT.1.1C	구현에 사용된 각 개발 도구는 잘 정의된 것이어야 한다.
ALC_TAT.1.2C	각 개발 도구 문서는 구현에 사용된 모든 규정과 지시어 뿐만 아니라 모든 명령문의 의미를 모호하지 않게 정의해야 한다.
ALC_TAT.1.3C	각 개발 도구 문서는 모든 구현-종속적인 선택사항의 의미를 모호하지 않게 정의해야 한다.

평가자 요구사항

ALC_TAT.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

6.2.5. 시험

(가) ATE_COV.2 시험범위의 분석

종속관계	ADV_FSP.2 보안-수행 기능명세 ATE_FUN.1 기능 시험

개발자 요구사항

ATE_COV.2.1D	개발자는 시험범위의 분석을 제공해야 한다.

증거 요구사항

ATE_COV.2.1C	시험범위의 분석은 시험 문서 내의 시험항목과 기능명세 내의 TSFI간의 일치성을 입증해야 한다.
ATE_COV.2.2C	시험범위의 분석은 기능명세 내의 모든 TSFI가 시험되었음을 입증해야 한다.

평가자 요구사항

ATE_COV.2.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(나) ATE_DPT.1 기본설계 시험

종속관계	ADV_ARC.1 보안 아키텍쳐 설명 ADV_TDS.2 아키텍쳐 설계 ATE_FUN.1 기능 시험

개발자 요구사항

ATE_DPT.1.1D	개발자는 시험의 상세수준 분석을 제공해야 한다.

증거 요구사항

ATE_DPT.1.1C	시험의 상세수준 분석은 시험 문서 내의 시험항목과 TOE 설계 내의 TSF 서브시스템 간의 일치성을 입증해야 한다.
ATE_DPT.1.2C	시험의 상세수준 분석은 TOE 설계 내의 모든 TSF 서브시스템이 시험되었음을 입증해야 한다.

평가자 요구사항

ATE_DPT.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(다) ATE_FUN.1 기능 시험

종속관계	ATE_COV.1 시험범위의 증거

개발자 요구사항

ATE_FUN.1.1D	개발자는 TSF를 시험하고 그 결과를 문서화해야 한다.
ATE_FUN.1.2D	개발자는 시험 문서를 제공해야 한다.

증거 요구사항

ATE_FUN.1.1C	시험 문서는 시험계획, 예상 시험결과, 실제 시험결과로 구성되어야 한다.
ATE_FUN.1.2C	시험계획은 수행되어야 할 시험항목을 식별하고 각 시험 수행의 시나리오를 서술해야 한다. 이러한 시나리오는 다른 시험결과에 대한 순서 종속관계를 포함해야 한다.
ATE_FUN.1.3C	예상 시험결과는 시험의 성공적인 수행으로 기대되는 결과를 제시해야 한다.
ATE_FUN.1.4C	실제 시험결과는 예상 시험결과와 일관성이 있어야 한다.

평가자 요구사항

ATE_FUN.1.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.

(라) ATE_IND.2 독립적인 시험 : 표본 시험

종속관계	ADV_FSP.2 보안-수행 기능명세 기능명세 AGD_OPE.1 사용자 운영 설명서 AGD_PRE.1 준비 절차 ATE_COV.1 시험범위의 증거 ATE_FUN.1 기능 시험

개발자 요구사항

ATE_IND.2.1D	개발자는 시험할 TOE를 제공해야 한다.

증거 요구사항

ATE_IND.2.1C	TOE는 시험하기에 적합해야 한다.
ATE_IND.2.2C	개발자는 개발자의 TSF 기능 시험에 사용된 자원과 동등한 자원을 제공해야 한다.

평가자 요구사항

ATE_IND.2.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.
ATE_IND.2.2E	평가자는 개발자 시험 결과를 검증하기 위하여 시험문서 내의 시험항목에 대한 표본 시험을 수행해야 한다.
ATE_IND.2.3E	평가자는 TSF가 명세된대로 동작함을 확인하기 위하여 TSF의 일부를 시험해야 한다.

6.2.6. 취약성 평가

(가) AVA_VAN.3 집중화된 취약성 분석

종속관계

ADV_ARC.1 보안 아키텍쳐 설명
ADV_FSP.4 완전한 기능명세
ADV_TDS.3 기본적인 모듈화 설계
ADV_IMP.1 TSF에 대한 구현의 표현
AGD_OPE.1 사용자 운영 설명서
AGD_PRE.1 준비 절차
ATE_DPT.1 기본설계 시험

개발자 요구사항

AVA_VAN.3.1D	개발자는 시험할 TOE를 제공해야 한다.

증거 요구사항

AVA_VAN.3.1C	TOE는 시험하기에 적합해야 한다.

평가자 요구사항

AVA_VAN.3.1E	평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.
AVA_VAN.3.2E	평가자는 TOE의 잠재적 취약성을 식별하기 위해 공개 영역에 대한 조사를 수행해야 한다.
AVA_VAN.3.3E	평가자는 TOE의 잠재적 취약성을 식별하기 위해 설명서, 기능명세, TOE 설계 및 보안 아키텍쳐 설명, 구현의 표현을 이용하여 집중화된 독립적인 취약성 분석을 수행해야 한다.
AVA_VAN.3.4E	평가자는 TOE가 강화된-기본 공격 성공 가능성을 가진 공격자에 의해 행해지는 공격에 내성이 있음을 결정하기 위해, 식별된 잠재적 취약성에 근거하여 침투시험을 수행해야 한다.

6.3. 보안요구사항의 이론적 근거

6.3.1. 보안기능요구사항의 이론적 근거

☞ 보안기능요구사항으로 만족시킬 수 있는 TOE 보안목적을 모두 식별하여 매핑표에 표시

☞ TOE 보안목적에 대응되는 보안기능요구사항이 존재하지 않는 경우 보안기능요구사항을 추가 도출하거나 기존의 도출된 보안기능요구사항에 오퍼레이션을 보완

☞ 보안기능요구사항에서 매핑되는 TOE 보안목적이 존재하지 않지만 해당 보안기능요구사항이 TOE 보안 특징 및 논리적 범위에 해당하는 경우 TOE 보안목적을 추가하거나 기존에 정의된 보안목적을 보완

☞ 오퍼레이션이 적용된 보안기능요구사항이 왜/어떻게 보안목적을 달성할 수 있는지에 대한 관점으로 ST 작성자의 정당성을 주장하는 바에 대해 서술

☞ 하나의 보안목적은 1개 이상의 보안기능요구사의 조합을 통해 달성될 수 있으므로 보안목적 마다 관련되는 모든 SFR을 식별한 후 각각의 SFR에 대해 정당을 제시. 단, 기능요구사항이들이 논리적으로 밀접한 관계를 가지는 경우 종합적인 관점에서 서술할 수 있음

보안기능요구사항의 이론적 근거는 다음을 입증한다.

▷ 각 TOE 보안목적은 적어도 하나의 TOE 보안기능요구사항에 의해 다루어진다.

▷ 각 보안기능요구사항은 적어도 하나의 TOE 보안목적을 다룬다.

보안기능 요구사항	O. 감사	O.	O.	O.	O.	O.	O.	O.	O.	O.	O.	O.	O.	O.
FAU_ARP.1	X													
FAU_GEN.1	X													
FAU_SAA.1	X													
FAU_SAR.1	X													
FAU_SAR.3	X													

[보안목적과 보안기능요구사항 대응]

O.감사	FAU_GEN.1, FPT_STM.1, FAU_SAA.1, FAU_ARP.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.1, FAU_STG.3, FAU_STG.4

FAU_GEN.1은 보안과 관련된 모든 행동에 대해 책임추적이 가능하도록 감사정보를 감사레코드에 기록하여 생성하는 기능을 제공함을 보장하므로 책임추적이 가능한 보안관련 사건 기록 및 유지에 대한 본 보안목적을 만족시킨다.

FPT_STM.1은 감사정보에 저장될 사건 일시를 신뢰된 NTP 서버로부터 수신한 시간정보로 기록함을 보장하므로 책임추적이 가능한 사건 기록을 요구하는 본 보안목적을 만족시킨다.

FAU_SAA.1 및 FAU_ARP.1은 검사 규칙에 따라 감사된 사건을 분석하여 잠재적 보안 위반으로 탐지하는 경우 관리자가 설정한 이메일로 관련 내용을 통보하는 기능을 제공하도록 보장하므로 보안관련 모든 행동의 책임추적을 요구하는 본 보안목적을 만족시킨다.

FAU_SAR.1 및 FAU_SAR.3은 감사레코드 조회기능을 제공하고 특히 검색어 기준으로 특정 사건을 검색하여 정렬할 수 있는 감사기능 제공을 보장하므로 감사데이터 검토 수단 제공을 요구하는 본 보안목적을 만족시킨다.

FAU_STG.1은 인가되지 않은 삭제로부터 감사레코드를 보호하고 비인가된 변경을 방지하도록 보장하므로 감사데이터 위변조 방지를 요구하는 본 보안목적을 만족시킨다.

FAU_STG.3 및 FAU_STG.4는 감사 증적이 감사레코드 총 용량의 80%를 초과하는 경우 관리자가 설정한 메일로 통보하고 syslog 서버 로그전송 기능 자동 활성화를 보장하며, 감사 증적이 포화인 경우 자동 백업을 수행한 후 오래된 감사 레코드 덮어쓰기를 수행함을 보장하므로 감사저장 공간 초과시 적절한 대응행동을 요구하는 본 보안목적을 만족시킨다.

O.	**컴포넌트1, 컴포넌트2,**

O.	**컴포넌트1, 컴포넌트2,**

6.3.2. 보증요구사항의 이론적 근거

☞ 평가보증등급을 선택한 이유를 서술 : 평가범위, 상세수준, 엄밀성 등 보증수준을 측정하는 척도를 고려하여 선택한 평가보증등급의 적절성을 서술하되 CC 제3부 “8. 평가보증등급”에 서술되어 있는 목적을 참조하여 서술

☞ 법령, 수요기관의 내부 규정 등 미리 정해진 평가보증등급이 존재하는 경우 해당 규정을 언급함으로써 평가보증등급을 선택한 이유를 대체할 수 있음

☞ 평가보증 패키지에서 ST 작성자가 보증컴포넌트를 추가한 경우 추가한 이유를 서술

본 보안목표명세서의 평가보증등급은 국내용 평가보증등급 EAL4로 선정하였다.

EAL4는 기존의 생산공정을 변경하지 않고 일반적으로 사용되고 있는 개발 방법론을 적용하여 얻을 수 있는 최대한의 보증 수준이다. 따라서 완전한 인터페이스 명세, 기본적인 모듈 설계, 일부 TSF 구현명세서 등 일부 개발과정에서 추가적인 문서화 작업이 요구된다. 또한 개발환경 보안, TOE 형상관리 자동화, TOE 배포절차 등 일부 개발프로세스 개선이 요구된다. 생산공정을 변경하지 않는 범위 내애서 개발프로세스를 개선하여 이에 따라 추가적인 개발문서를 작성하고 이를 토대로 본 보안목표명세서에서 정의한 보안기능요구사항을 분석함으로써 제한적 범위에서 최대 수준의 보증을 제공한다.

보안기능요구사항의 분석에 대한 정확성, 객관성 확보를 위해 개발자시험 표본결과 확인, 설계문서(기능명세, TOE 모듈설계)에 기반한 평가자 독립시험, 강화된-기본 공격 성공 가능성을 가진 공격자의 침투 공격에 대한 내성을 입증하는 취약성 분석과 침투시험이 수행되며 이는 평가기관에서 수행된다.

6.4. 종속관계에 대한 이론적 근거

6.4.1. 보안기능요구사항의 종속관계

☞ ST에서 도출한 모든 SFR에 대해 일련번호를 부여하고, SFR 마다 CC 제2부에 정의된 종속관계를 식별 한 후 종속관계를 갖는 컴포넌트에 해당 하는 일련번호를 기재

☞ CC 제2부에 정의된 종속관계에 해당하는 컴포넌트가 ST에서 도출되지 않은 경우 종속관계를 만족시키지 않는 이유를 서술

다음 표는 보안기능요구사항의 종속관계를 보여준다.

번호	ST 보안기능요구사항	CC 제2부 보안기능요구사항 종속관계	본 표에서 SFR 식별을 위해 부여한 번호
1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT.STM.1	33
3	FAU_SAA.1	FAU_GEN.1	2
4	FAU_SAR.1	FAU_GEN.1	2
5	FAU_SAR.3	FAU_SAR.1	5
6	FAU_STG.1	FAU_GEN.1	2
7	FAU_STG.3	FAU_STG.1	6
8	FAU_STG.4	FAU_STG.1	6

[표 7] 종속관계 이론적 근거

6.4.2. 보증요구사항의 종속관계

정보보호시스템 공통평가기준에서 제공하는 EAL4 보증 패키지의 종속관계는 이미 만족되어 있으므로 이에 대한 이론적 근거는 생략한다.

07

TOE 요약명세

7. TOE 요약명세

☞ 보안기능요구사항을 만족시키기 위해 TOE에서 구현한 메커니즘, 기능 등을 설명하되 CC 제2부의 클래스 단위로 분류하여 유사 기능을 설명하거나 TOE 서브시스템/모듈 등 TOE 구조를 고려하여 구분하여 서술

☞ CC 제2부의 클래스 단위로 분류하여 서술하는 경우 오퍼레이션이 적용된 SFR을 만족시키는 TOE의 기능을 그룹핑하고 이들 사이의 상호관계를 논리적인 기능흐름에 따라 작성

☞ 보안메커니즘을 설명하는 기술문서(White Paper, Technical Document, Manual 등) 수준으로 작성

7.1. 사용자 데이터보호

7.2. TOE 접근

7.3. 식별 및 인증

7.4. 안전한 경로/채널

7.5. 보안감사

7.6. 보안관리

7.7. TSF 보호

7.8. 암호지원

08

참고자료

8. 참고자료

자료 명	저 자	비 고
정보보호시스템 공통평가기준 버전 3.1 개정 2판 •정보보호시스템 공통평가기준 1부 : 소개 및 일반모델, 버전 3.1R1, 2006. 9., CCMB-2006-09-001 •정보보호시스템 공통평가기준 2부 : 보안기능요구사항, 버전 3.1R2, 2007. 9., CCMB-2007-09-002 •정보보호시스템 공통평가기준 3부 : 보증요구사항, 버전 3.1R2, 2007. 9., CCMB-2007-09-003	CCRA	2007. 9

09

용어 및 약어

9. 용어 및 약어

CC	Common Criteria
CCMB	Common Criteria Maintenance Board
EAL	Evaluation Assurance Level
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
IT	Information Technology
NTP	Network Time Protocol
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
VPN	Virtual Private Network
SSH	Secure Shell
TLS	Transport Layer Security