국가용 보안요구사항 V3.0 기반의

국내용 TOE 설계서 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. TOE 설계서 참조

☞ TOE 설계서 식별을 명확하게 할 수 있도록 문서명, 형상관리 번호 등 TOE 설계서에 대한 식별정보 서술

문서명	*OOO TOE 설계서*
문서버전	*X.X*
파일명	*신청대상제품명-문서명-버전-날짜(세부버전 등).hwp*
보증컴포넌트	*ADV_TDS.1*
작성자	*(주) XXX*
발간일	*20XX.XX.XX*
주요용어	*침입차단시스템, 방화벽, FW, Firewall 등*

참고사항	▶ 정보보호제품 평가인증(CC인증) 제도의 국내용 정보보호제품 평가·인증 스킴에 따라 TOE 설계서는 신청기관 자체 설계서 등 개발문서 제출로 인정된다. ▶ 신규로 제출물을 작성하는 경우 TOE 설계서 작성자는 본 가이드를 참고하여 TOE 설계서를 작성할 수 있다.

1.2. 목적

☞ TOE설계서는 TOE의 모든 서브시스템이 식별되어야 하고, 보안기능(TSF)을 구성하는 TOE의 부분들을 식별하는 작업으로 사용된다.

예: TOE 설계서(TDS, TOE Design)는 TSF 설명을 위한 배경 및 전체 TSF 설명을 제공한다. 서브시스템은 TOE 설계에 대한 설명으로, TOE의 부분이 어떤 역할을 어떻게 수행하는지에 대한 상위수준의 설명을 제공하며, 서브시스템은 더 상세수준의 하부시스템 또는 모듈 등 보안기능을 세분화될 수 있다.

1.3. TOE 설계서 구성

TOE 설계서는 다음과 같이 구성되어 있다.

1장은 TOE 설계서 개요로 TOE 설계서의 목적, 구성, 용어 정의 등을 기술한다.

2장은 TOE의 서브시스템 식별내용을 기술한다.

3장에서 제4장까지는 식별된 서브시스템과 보안기능에 대하여 각각 기술하며, 시스템의 전체적인 구조와 구성요소와의 상호작용에 대하여 설명한다.

5장은 이론적 근거로 TOE 설계서에 대하여 서브시스템 및 보안기능이 적절히 다루어지고 적합함을 입증한다.

1.4. 용어 정의

☞ *TOE 설계서에서 사용되는 용어를 중점적으로 추가하여 기술한다.*

예:

관리자(administrator)

TOE 보안기능성(TSF)에 의해 구현된 모든 정책에 관해서 신뢰 등급을 가진 실체

보증(assurance)

평가대상(TOE)이 보안기능요구사항(SFR)(3.78)에 부합한다는 신뢰성의 근거

인가된 사용자(authorised user)

보안기능요구사항(SFR)에 따라서 평가대상(TOE)(3.90)에서 오퍼레이션을 실행할 수 있는 실체

실체(entity)

속성의 집합 또는 모음으로 설명되는 식별가능한 항목

평가보증등급(evaluation assurance level)

미리 정의된 보증 수준의 지표를 나타내는 보증요구사항의 잘 구성된 패키지

객체(object)

주체의 오퍼레이션 대상이며 정보를 포함하거나 수신하는 평가대상(TOE) 내의 수동적인 실체

주체(Subject)

객체에 대한 오퍼레이션을 수행하는 평가대상(TOE) 내의 실체

평가대상(target of evaluation), TOE

가능한 경우 설명서가 수반되는 소프트웨어, 펌웨어 및/또는 하드웨어 집합으로, 평가의 대상이 됨

TOE 보안기능성 (TSF, TOE Security Functionality), TSF

보안기능요구사항(SFR)의 정확한 수행을 위해 의존하는 평가대상(TOE)의 모든 하드웨어, 소프트웨어, 펌웨어로 결합된 기능성

TOE 보안정책 (TSP, TOE Security Policy)

TOE내에서 자산의 관리, 보호, 분배를 규제하는 규칙의 집합

보안목표명세서(ST, Security Target)

TOE 평가를 위한 근거로써 사용되는 보안요구사항과 기능 명세의 집합

TSF 데이터(TSF Data)

보안기능요구사항(SFR) 수행을 위해 의존하는 평가대상(TOE) 오퍼레이션을 위한 데이터

사용자 데이터(user data)

일부 외부 실체에게는 의미가 있지만 TOE 보안기능성(TSF)의 운영에 영향을 미치지 않는, 평가대상(TOE)이 수신 또는 생성한 데이터

1.5. 참조 문서

☞ *일반적으로 기본적인 설계 평가(ADV_TDS.1)에서 요구되는 입력문서를 참조로 한다.*

- OOO V1.0” 보안목표명세서 VX.X
- OOO V1.0” 기능명세서 VX.X
- OOO V1.0” 보안구조설명서 VX.X

2. TOE 기본구조

본 장은 TOE인 OOO V1.0에 대한 TOE 기본구조를 기술한다. 각 서브시스템을 식별하고 TSF(TOE Security Functionality)에 해당하는 부분을 정의한다. TSF는 보안감사, 식별 및 인증, 사용자 데이터보호, 암호지원, 보안관리, TSF 보호, TOE 접근, 안전한 경로/채널 서브시스템이 포함된다.

2.1. 서브시스템 구조

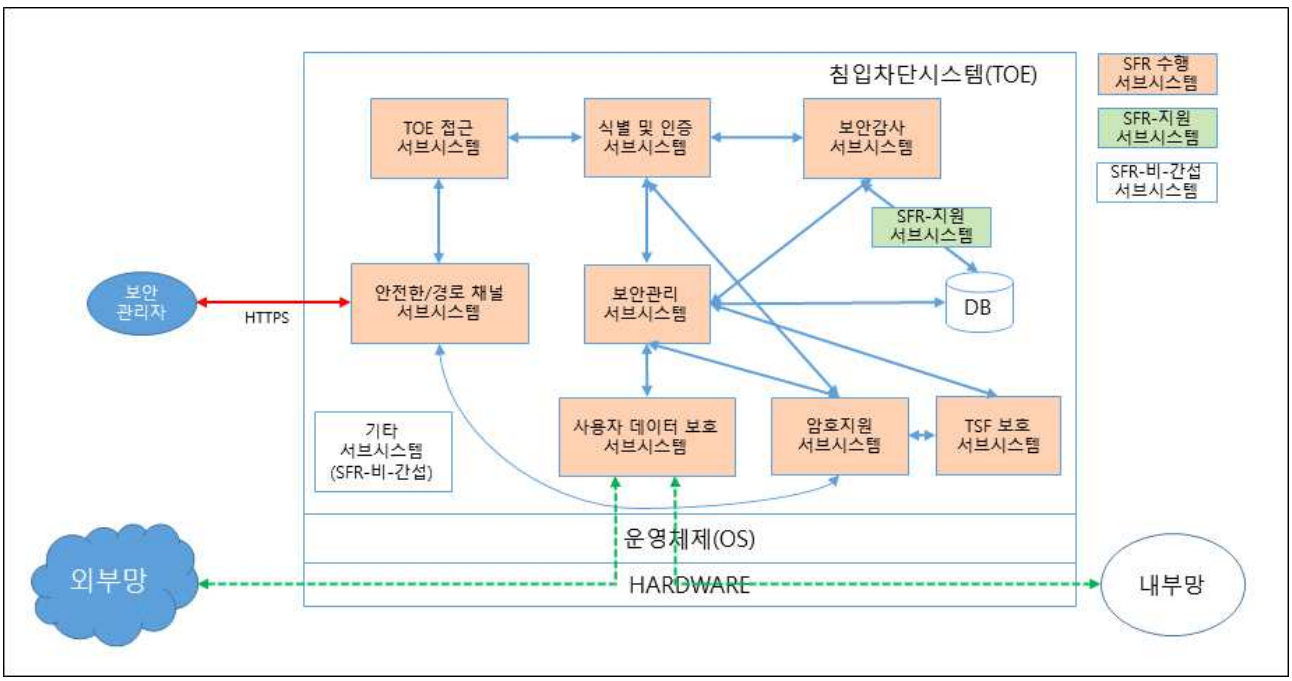
☞ *TOE 설계서(TDS, TOE Design)는 TSF 설명을 위한 배경 및 전체 TSF 설명을 제공한다. TOE 설계는 서브시스템과 모듈이라는 두 가지 수준의 분해를 사용할 수 있다. 모듈은 기능성에 대한 가장 상세한 서술로써, 구현에 대한 설명이다. 서브시스템은 TOE 설계에 대한 설명으로, TOE의 부분이 어떤 역할을 어떻게 수행하는지에 대한 상위수준의 설명을 제공할 수 있다.*

☞ *TOE(및 TSF)는 여러 계층으로 추상화 되어 설명되며, 복잡도에 따라 서브시스템 또는 모듈로 설명될 수 있으며, 공통평가기준 3부 "부록 A.4 ADV_TDS: 서브시스템 및 모듈"에 따라 EAL2 보증 수준에서는 ADV_TDS.1에서 요구사항에 따라 최소한 서브시스템 수준에서 작성이 필요하다.*

☞ *즉, 각 서브시스템을 모듈화 하여 상세히 표현하는 것도 가능하다.*

☞ *TOE 설계서 작성자는 제품의 구성 및 서브시스템, 모듈의 구성에 따라 적절히 구조를 도식화한다.*

예: 다음 그림은 TOE의 전체 서브시스템의 구성도를 도식화한 것이다.



[그림 1] TOE 서브시스템 구성도(예시)

(전체 TSF에 대해 non-TSF 서브시스템, TSF 서브시스템 또는 모듈 간 포함 관계를 그림/표로 기술)

☞ *TOE 서브시스템 구성도에 따라 TOE가 수행하는 보안기능에 대해 상위 수준에서 설명한다.*

예: TOE는 침입차단 시스템 제품유형으로 하드웨어 일체형 장비에 해당한다. 인가된 관리자를 통한 보안관리를 수행하는 관리접속 인터페이스와 내·외부망의 접점에 위치하여 네트워크 트래픽을 모니터링하고 침입차단 규칙에 따라 트래픽 정보의 흐름을 탐지·차단하는 기능을 수행한다.

2.2. SFR-수행 서브시스템

☞ *시험대상 제품 유형 및 구조에 따라 서브시스템 구조는 다를 수 있으며 제품에 적합하게 표현되어야 함*

☞ TOE의 모든 서브시스템을 식별하고 TOE 보안기능(TSF)과의 관계를 설명한다.

☞ *상위수준 설명은 특정 데이터 구조체를 포함할 필요는 없으며(가능하더라도), 대신에 서브시스템 내에서 일반적인 데이터 흐름, 메시지 흐름, 통제 관계를 다룰 수 있다.*

서브시스템	SFR-수행 행동
보안감사 서브시스템 (S_FAU)	☞ *보안감사 서브시스템에서 SFR-수행과 관련한 기능을 설명한다.* 예: 보안감사 서브시스템은 감사로그 생성, 보안경보, 잠재적인 위반 분석, 검사검토, 감사 증적 저장소 보호, 감사 데이터 손실 예측 시 대응 행동, 감사 데이터의 손실 방지와 관련한 보안 기능을 수행한다. *1. S_FAU.1 : 감사데이터 수집 및 저장* *TOE는 TSF를 실행하는 주요 기능(침입차단, 암호연산, 관리자 행위, 잠재작 보안탐지)의 실행 결과와 감사기능 시동 및 종료에 대해 감사데이터를 생성한다. 감사데이터에는 사건 발생 일시, 사건 유형, 사건을 발생시킨 주체의 신원, 작업 내역 및 결과(성공/실패) 등이 포함된다. 외부 NTP 서버로부터 수신한 시각 정보를 동기화하여 이를 감사데이터의 사건 발생 일시로 기록한다.* *2. S_FAU.2 : 감사로그 조회 및 알람* *관리자는 관리자 웹페이지에 로그인하여 감사기록을 정렬 조회하거나 고급검색 기능을 이용하여 다양한 검색어(단어, 구문, 정규표현식 등)로 감사기록을 조회한다. CLI에 접속하여 감사기록이 저장된 clog 파일을 읽을 수는 있으나 다만, 트래픽 로그(정보흐름통제규칙에 적용된 패킷 처리결과)는 CLI로 접속하여 읽을 수는 있으나 사람이 이해할 수 없는 형태로 제공된다. 로컬 하드디스크에 저장된 clog 파일은 관리자라도 수정/삭제가 불가능하다. 또한, 감사된 사건에 대해 위반규칙에 따른 잠재적 보안 위반을 탐지하고 관리자가 지정한 이메일로 경고메시지를 발송한다.* *3. S_FAU.3 : 감사 저장소 보호* *생성된 감사데이터는 TOE 로컬디스크에 파일형태로 저장되고 감사 저장공간이 임계치에 도달하는 경우 감사기록을 원격 syslog 서버로 전송하며 감사 저장공간이 부족한 경우 관리자가 지정한 이메일로 경고메시지를 발송하고 자동백업을 수행한 후 감사기록을 덮어쓰기 한다.*

사용자 데이터보호 서브시스템 (S_FDP)	*☞ 사용자 데이터 보호 서브시스템에서 SFR-수행과 관련한 기능을 설명한다.* 예: 사용자 데이터 보호 서브시스템은 설정된 침입차단시스템 보안정책에 따라 외부망/내부망으로부터 유입되는 네트워크 트래픽의 차단 유무를 결정하고 정보의 흐름을 통제하는 보안기능을 수행한다. *1. S_FDP.1 : 침입차단 정책* *TOE의 침입차단 기능은 TCP/IP 기반 네트워크 트래픽의 정보흐름를 통제하기 위해 IP 주소 및 포트를 기반으로하는 패킷 필터링 메커니즘과 TCP/UDP 세그먼트의 Flag 값을 기반으로 트래픽 흐름을 통제하는 상태기반 감시 메커니즘으로 구성된다.* *2. S_FDP.2 : 패킷 필터링 정책* *패킷 필터링 메커니즘은 내외부 네트워크간 IPv4 출발지/목적지 IP주소, 서비스(프로토콜, 포트) 정보에 기반하여 관리자가 설정한 정보흐름통제규칙에 따라 트래픽을 처리(거부/차단/허용)한다. 패킷 필터링 메커니즘은 tcpudp dump로부터 받은 네트워크 패킷에 대해 우선적용 거부규칙을 적용한 후 정보흐름통제규칙에서 정한 처리방식에 따라 정보흐름을 통제하고 일치하는 규칙이 존재하지 않는 패킷에 대해서는 무조건 차단하는 화이트리스트 방식을 적용한다.* *3. S_FDP.3 : 상태기반 감시 정책* *상태기반 감시 메커니즘은 패킷 필터링 메커니즘을 통해 통과된 패킷의 상태 값을 상태 표에 기록하고 이 후 동일 상태 값을 갖는 패킷에 대해 정보흐름통제규칙을 적용하지 않고 TOE를 통과시키게 된다. TCP/UDP 세그먼트의 Flag 값을 확인하여 해당 패킷에 대한 상태 값(State)을 상태 표에 기록하여 세션이 유지되는 동안 유지하며 패킷을 처리한다. 상태 표에 기록된 정보를 기반으로 조각난 패킷을 탐지하여 TTL이 만료되어도 조각난 패킷들이 모두 도착하지 못하면 이전에 수신한 관련 패킷들까지 모두 폐기한다. 또한 Half-open TCP 세션에 대해서도 임계치에 도달하면 세션을 종료하고 연결을 끊는다.*
식별 및 인증 서브시스템 (S_FIA)	*☞ 식별 및 인증 서브시스템에서 SFR-수행과 관련한 기능을 설명한다.* 예: 로그인(예: ID/PW 기반) 인터페이스를 통해 인가된 사용자 여부를 판단하기 위한 식별 및 인증과 인증실패처리, 인증 피드백 보호 등을 통한 인증데이터를 보호하기 위한 식별 및 인증과 관련한 보안기능을 수행한다. 1. S_FIA.1 : 관리자 식별 및 인증 2. S_FIA.2 : 인증 실패 처리 3. S_FIA.3 : 비밀정보의 검증 4. S_FIA.4 : 재사용 방지 매커니즘
암호지원 서브시스템 (S_FCS)	*☞ 암호지원 서브시스템에서 SFR-수행과 관련한 기능을 설명한다.* 예: 암호지원 서브시스템은 각 서브시스템들이 암호연산 등을 수행할 때 필요한 암호키 관리(암호키 생성, 분배, 파기 등), 암호연산, 난수 생성 등과 관련한 기능을 수행한다. 1. S_FCS.1 : 암호키 생성 2. S_FCS.2 : 암호키 분배

	3. S_FCS.3 : 암호키 파기 4. S_FCS.4 : 암호 연산 5. S_FCS.5 : 난수 생성
보안관리 서브시스템 (S_FMT)	☞ *보안관리 서브시스템에서 SFR-수행과 관련한 기능을 설명한다.*
TSF 보호 서브시스템 (S_FPT)	☞ *TSF 보호 서브시스템에서 SFR-수행과 관련한 기능을 설명한다.*
TOE 접근 서브시스템 (S_FTA)	☞ *TOE 접근 서브시스템에서 SFR-수행과 관련한 기능을 설명한다.*
안전한 경로/채널 서브시스템 (S_FTP)	☞ *안전한 경로/채널 서브시스템 SFR-수행과 관련한 기능을 설명한다.*

[표 2] 서브시스템의 보안기능(예시)

2.3. SFR-지원 및 SFR-비간섭 서브시스템

☞ *SFR-지원 또는 SFR-비-간섭 서브시스템은 시스템에서 어떻게 기능 하는지 상세하게 서술될 필요는 없으며, SFR-지원, SFR-비-간섭 TSF 서브시스템 행동이 SFR-수행 행동이 아님을 결정할 수 있도록 서술되어야 함*

서브시스템	수행 행동
지원 서브시스템 (S_SPT)	☞ *지원 서브시스템에서 SFR-지원과 관련하여 제공되는 기능을 설명한다.*
기타 서브시스템 (S_ETC)	☞ *기타 서브시스템에서 SFR-비-간섭과 관련한 일반 기능에 대해 설명한다.*

2.4. 서브시스템 구분

☞ *TOE의 모든 서브시스템을 식별하고, 각 서브시스템들은 SFR-수행, SFR-지원, SFR-비간섭으로 적절하게 분류됨을 입증해야 한다.*

☞ *본 절에서는 서브시스템 및 하부시스템/보안기능을 식별하고 각 하부시스템/보안기능을 SFR-수행, SFR-지원, SFR-비-간섭으로 분류하여 표를 완성한다.*

예: 본 평가대상 시스템의 서브시스템들은 다음과 같이 하부시스템(또는 모듈)으로 세분화하고 그 하부시스템들은 SFR-수행, SFR-지원, SFR-비-간섭 서브시스템으로 범주화될 수 있다.

분류	하부시스템/보안기능	서브시스템 구분
보안감사 서브시스템(S_FAU)	S_FAU.1 : 감사데이터 수집 및 저장	SFR-수행
	S_FAU.2 : 감사로그 조회 및 알람	SFR-수행
	S_FAU.3 : 감사 저장소 보호	SFR-수행
사용자 데이터보호 서브시스템(S_FDP)	S_FDP.1 : 침입차단 정책	SFR-수행
	S_FDP.2 : 패킷 필터링 정책	SFR-수행
	S_FDP.3 : 상태기반 감시 정책	SFR-수행
식별 및 인증 서브시스템(S_FIA)	S_FIA.1 : 관리자 식별 및 인증	SFR-수행
	S_FIA.2 : 인증 실패 처리	SFR-수행
	S_FIA.3 : 비밀정보의 검증	SFR-수행
	S_FIA.4 : 재사용 방지 매커니즘	SFR-수행
암호지원 서브시스템(S_FCS)	S_FCS.1 : 암호키 생성	SFR-수행
	S_FCS.2 : 암호키 분배	SFR-수행
	S_FCS.3 : 암호키 파기	SFR-수행
	S_FCS.4 : 암호 연산	SFR-수행
	S_FCS.5 : 난수 생성	SFR-수행
보안관리 서브시스템(S_FMT)	S_FMD.1 : 보안기능 관리	SFR-수행
	S_FMT.2 : 보안속성 및 데이터 관리	SFR-수행
TSF 보호 서브시스템(S_FPT)	S_FDP.1 : 저장데이터 보호	SFR-수행
	S_FDP.2 : 전송데이터 보호	SFR-수행
	S_FPT.3 : TSF 자체 시험	SFR-수행
TOE 접근 서브시스템(S_FTA)	S_FTA.1 : 사용자 세션 관리	SFR-수행
안전한 경로/채널 서브시스템(S_FTP)	S_FTP.1 : 안전한 경로	SFR-수행
지원 서브시스템(S_SPT)	S_SPT.1 : 감사저장 지원	SFR-지원
	S_SPT.2 : 암호가속기	SFR-지원
기타 서브시스템(S_ETC)	S_ETC.1 : 도움말 기능	SFR-비-간섭
	S_ETC.2 : 기타 비-보안 관련 기능	SFR-비-간섭

[표 4] TOE의 보안기능(예시)

3. TOE 서브시스템

본 장에서는 TOE의 서브시스템에 대한 동작을 기술한다. 각 서브시스템 및 보안기능의 설계내용에 대하여 자세하게 기술하며, 각 서브시스템간의 상호작용에 대해서도 기술한다.

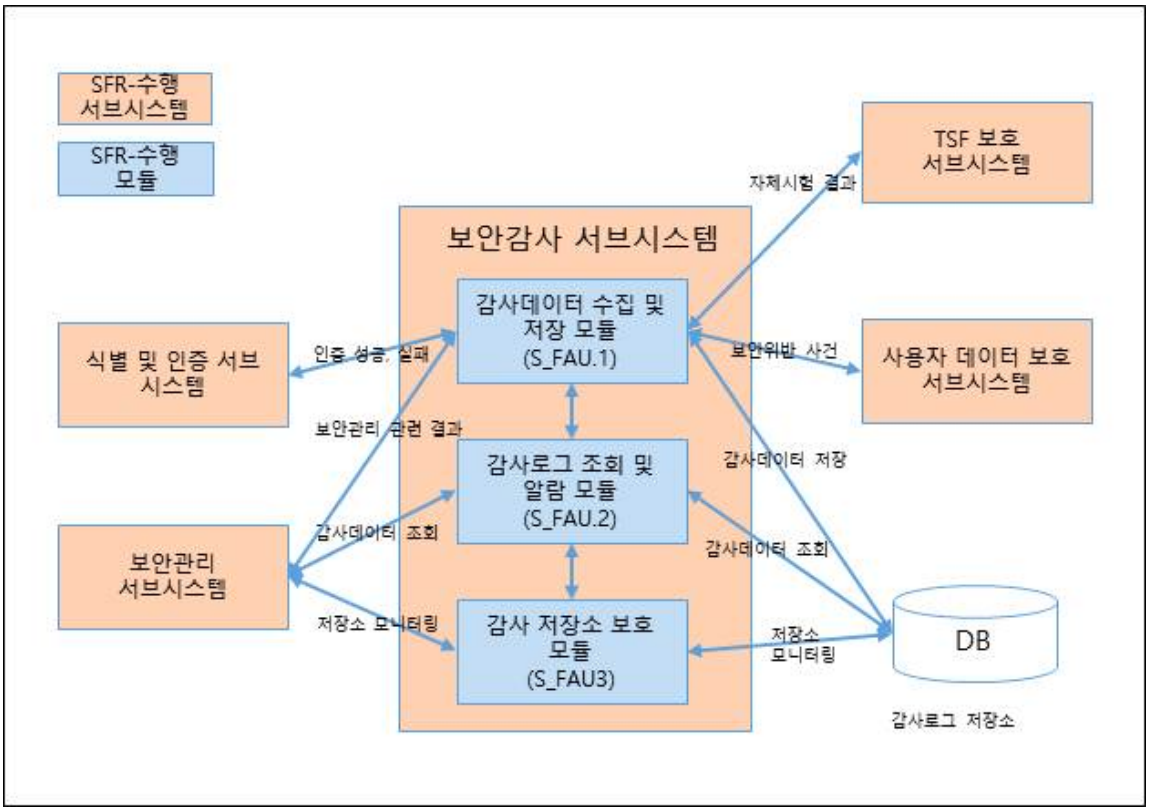
3.1. 보안감사(FAU) 서브시스템

3.1.1 목적

☞ *모든 SFR-수행 서브시스템의 목적, 기능을 상세하게 기술하고 TSF 외부 인터페이스를 식별한다.*

☞ *서브시스템 간의 모든 상호작용을 기술하고, SFR-수행 행동에 관련된 결과를 기술한다.*

예: 보안감사(S_FAU)서브시스템은 보안관리 및 침입차단 결과 등 제품 내부에서 발생한 모든 보안관련 이벤트에 대해 감사데이터로 수집 및 생성하여 DB에 저장하고, 인가된 관리자 조회 요청시 관리자가 해석하기 적합한 형태로 조회 기능을 제공한다. 또한 감사데이터의 보호 조치를 위해 감사 저장소 관리 등 보안기능을 수행한다.



[그림 2] 보안감사 서브시스템 및 상호작용(예시)

☞ *위와 같이 데이터 흐름을 표시한 기본구조 형태의 그림으로 표현해도 되고, 순서도를 이용한 도식화도 가능함.*

☞ *보안감사 서브시스템은 보안목표명세서(ST) 작성자에 의해 도출된 보안감사(FAU) 클래스의 보안요구사항을 달성하는데 필요한 서브시스템이며 SFR-수행 서브시스템으로 분류된다.*

예: 보안감사(FAU) 서브시스템은 감사데이터 수집 및 저장 모듈(S_FAU.1), 감사로그 조회 및 알람 모듈(S_FAU.2), 감사 저장소 보호 모듈(S_FAU.3)로 구성된다.

3.1.2 상호작용 설명

☞ *SFR-수행 서브시스템들 간의 상호작용 및 SFR-수 행 서브시스템과 다른 서브시스템 간의 상호작용에 대한 설명한다.*

☞ *상호작용은 구현 수준(예 : 한 서브시스템의 한 루틴으로부터 다른 서브시스템의 루틴으로 전송되는 매개변수들, 전역 변수들, 하나의 하드웨어 서브시스템에서 인터럽트를 처리하는 서브시스템으로의 하드웨어 신호(예 : 인터럽트))에서 특징지어질 필요는 없다.*

☞ *다른 서브시스템에서 사용되어야 할 특정 서브시스템에 대해 식별된 데이터 요소들은 여기서 논의될 필요는 있음*

☞ *또한 서브시스템 간의 통제 관계(예 : 침입차단시스템에서 기본 규칙을 구성할 책임이 있는 서브시스템과 실제로 이러한 규칙들을 구현하는 서브시스템의 관계)도 서술되도록 권고한다.*

☞ *TOE 설계서 작성자는 상세한 정보 제공을 위해 필요한 경우 모듈간의 내부 인터페이스, 매개변수, 흐름도 등을 포함하여 작성 할 수 있다.*

예: 보안감사 서브시스템은 식별 및 인증 서브시스템으로부터 사용자 식별 및 인증과 관련한 인증 실패, 연속인증 실패 한계횟수 초과 등 보안관련 사건을 감사데이터 수집 및 저장 모듈을 통해 수집하여 감사로그 저장소(DB)에 저장한다.

인가된 관리자는 보안관리 서브시스템을 통해 보안감사기록 조회를 요청하는 경우 보안감사 서브시스템의 감사데이터 조회 모듈(S_FAU.2)은 감사데이터 저장소(DB)를 조회하여 관리자 접속 UI를 통해 감사기록이 출력된다.

인가된 관리자는 보안관리(S_FMT) 서브시스템의 보안기능 관리, TSF 데이터 관리 등 보안관리 기능으로부터 보안 관련 정책 및 환경 설정 등 설정 수행 결과를 보안감사 서브시스템의 감사데이터 수집 및 저장 모듈이 수신하여 감사저정소(DB)에 저장한다.

사용자데이터 보호시스템(S_FDP)으로부터 ACL 정책에 기반한 차단/허용 로그(주체, 객체, 주체의 보안속성, 객체의 보안속성 등을 포함한) 등을 보안감사 서브시스템의 감사데이터 수집 및 저장 모듈이 수신하여 감사저장소(DB) 저장한다.

작성요령	▶ 설계서 작성자는 서브시스템이 SFR 관련 기능을 어떻게 구현하였는지 설계 관점에서 설명을 제공해야 함 ☑ 서브시스템은 상위수준에 대한 설명을 포함하여야 하며 특정 데이터 구조체를 포함할 필요는 없으며, 서브시스템 내에서 일반적인 데이터 흐름, 메시지 흐름, 통제 관계를 포함하여 서술해야 함 ☑ SFR-수행 행동이 어떻게 달성되는지 이해할 수 있도록 충분한 정보를 제공해야 함 ☑ TOE의 복잡도에 따라 “공통평가기준 3부 부록 A.4 ADV_TDS: 서브시스템 및 모듈”을 참조하여 모듈 수준까지 서술 할 수 있으나 EAL2 보증수준(ADV_TDS.1)에서는 강제사항이 아님을 유의 ☑ 완전성 및 정확성을 위해 다른 정보(예 : 기능명세서, 보안 구조 설명, 구현의 표현)의 정보와 일치하도록 작성해야 함

3.2. 식별 및 인증 서브시스템(FIA)

3.2.1 목적

☞ *3.1.1 항 보안감사 서브시스템(S_FAU) 작성 내용을 참조하여 작성한다.*

3.2.2 상호작용 설명

☞ *3.1.2 항 보안감사 서브시스템(S_FAU) 작성 내용을 참조하여 작성한다.*

3.3. 보안감사 서브시스템(S_FAU)

3.3.1 목적

☞ *3.1.1 항 보안감사 서브시스템(S_FAU) 작성 내용을 참조하여 작성한다.*

3.3.2 상호작용 설명

☞ *3.1.2 항 보안감사 서브시스템(S_FAU) 작성 내용을 참조하여 작성한다.*

3.4. 사용자 데이터보호 서브시스템(S_FDP)

3.4.1 목적

☞ *3.1.1 항 보안감사 서브시스템(S_FAU) 작성 내용을 참조하여 작성한다.*

3.6.2 상호작용 설명

☞ *3.1.2 항 보안감사 서브시스템(S_FAU) 작성 내용을 참조하여 작성한다.*

3.5. 식별 및 인증 서브시스템(S_FIA)

3.5.1 목적

☞ *3.1.1 항 보안감사 서브시스템(S_FAU) 작성 내용을 참조하여 작성한다.*

3.5.2 상호작용 설명

☞ *3.1.2 항 보안감사 서브시스템(S_FAU) 작성 내용을 참조하여 작성한다.*

3.6. 암호지원 서브시스템(S_FCS)

3.6.1 목적

☞ *3.1.1 항 보안감사 서브시스템(S_FAU) 작성 내용을 참조하여 작성한다.*

3.6.2 상호작용 설명

☞ *3.1.2 항 보안감사 서브시스템(S_FAU) 작성 내용을 참조하여 작성한다.*

3.7. 보안관리 서브시스템(S_FMT)

3.7.1 목적

☞ *3.1.1 항 보안감사 서브시스템(S_FAU) 작성 내용을 참조하여 작성한다.*

3.7.2 상호작용 설명

☞ *3.1.2 항 보안감사 서브시스템(S_FAU) 작성 내용을 참조하여 작성한다.*

3.8. TSF 보호 서브시스템(S_FPT)

3.8.1 목적

☞ *3.1.1 항 보안감사 서브시스템(S_FAU) 작성 내용을 참조하여 작성한다.*

3.8.2 상호작용 설명

☞ *3.1.2 항 보안감사 서브시스템(S_FAU) 작성 내용을 참조하여 작성한다.*

3.9. TOE 접근 서브시스템(S_FTA)

3.9.1 목적

☞ *3.1.1 항 보안감사 서브시스템(S_FAU) 작성 내용을 참조하여 작성한다.*

3.9.2 상호작용 설명

☞ *3.1.2 항 보안감사 서브시스템(S_FAU) 작성 내용을 참조하여 작성한다.*

3.10. 안전한 경로/채널 서브시스템(S_FTP)

3.10.1 목적

☞ *3.1.1 항 보안감사 서브시스템(S_FAU) 작성 내용을 참조하여 작성한다.*

3.10.2 상호작용 설명

☞ *3.1.2 항 보안감사 서브시스템(S_FAU) 작성 내용을 참조하여 작성한다.*

4. 이론적 근거

4.1. 보안기능 상관 분석

보안기능요구사항에 따른 TSF 인터페이스의 상관관계를 보여준다.

☞ *기능명세서에 기술된 모든 TSFI와 서브시스템 사이의 대응관계를 통해 모든 기능이 설계서 반영 되었음을 입증 할 수 있다.*

TOE 보안기능 요구사항 (컴포넌트)	하부시스템 or 모듈	OOO 기능명세서 TSFI (TSF 인터페이스)
FAU_ARP.1	S_FAU.2	☞ *ST의 SFR 중 FAU_SAA.1에서 도출된 다음의 잠재적 보안위반으로 식별한 사건을 발생시키는 TSFI를 서술 한다.* *FIA_UAU.1의 감사대상 사건 중 동일 계정의 인증 실패* *FAU_STG.3의 감사 대상 사건 중 대응 행동 실패* *FAU_STG.4의 감사대상 사건 중 대응 행동 실패* *FDP_IFF.1의 감사대상 사건 중 상태 표 메모리 임계치 초과* *FDP_IFF.1의 감사대상 사건 중 관리자가 설정한 정보흐름 통제규칙 적용 결과* *FMT_MTD.1(1)의 감사대상 사건 중 SSH Authorized Key 설정 변경* *FMT_SMF.1의 감사대상 사건 중 관리자가 설정한 관리메뉴* *FPT_TST.1의 감사대상 사건 중 무결성 위반 감사 사건* *예)* *EI_GUI_FMT_Alert(경보 정책 설정)* *EI_MGT_Login_fail (연속인증 실패 처리)*
FAU_GEN.1	S_FAU.1	☞ *ST의 SFR 중 FAU_GEN.1에서 도출된 감사대상 사건을 발생시키는 모든 TSFI를 서술 한다.* *예:* *EI_GUI_Login(식별 및 인증 인터페이스)* *EI_GUI_TST_Selftest(자체시험 수행 인터페이스)*

FAU_SAA.1	S_FAU.2	*EI_analysis_audit_event(잠재적 위반 분석 인터페이스)*
FAU_SAR.1	S_FAU.2	*EI_GUI_Audit_review(감사기록조회 화면인터페이스)*
FAU_SAR.3	S_FAU.2	*EI_GUI_Audit_review(감사기록조회 화면인터페이스)*
FAU_STG.1	S_FAU.3	*EI_AC_DB(감사저장소 접근통제 인터페이스)*
FAU_STG.3	S_FAU.3	*EI_AC_Monitoring(감사저장소 모니터링 인터페이스)*
FAU_STG.4	S_FAU.3	*EI_AC_Monitoring(감사저장소 모니터링 인터페이스)*
FCS_CKM.1	S_FCS.1	*EI_Generate_KEY_API (암호키 생성 인터페이스 호출)*
FCS_CKM.2	S_FCS.2	*EI_GUI_LOGIN_TLS (관리자 로그인 인터페이스-암호통신)*
FCS_CKM.4	S_FCS.3	*EI_GUI_FMT_DEK (암호키 관리 인터페이스-암호키 파기)*
FCS_COP.1	S_FCS.4	*EI_GUI_LOGIN_TLS (관리자 로그인 인터페이스-암호통신)*
FCS_RBG.1 (확장)	S_FCS.5	*EI_Generate_DRBG_API (암호키 생성 인터페이스)*
FCS_IFC.2	S_FDP.1	*EI_FMT_Firewall (방화벽 정책 설정 인터페이스)* *EI_FMT_ACL (방화벽 ACL 정책 설정 인터페이스)* *EI_OS_SCALL_inbound (OS시스템콜호출 인터페이스-수집)* *EI_OS_SCALL_oubound (OS시스템콜호출 인터페이스-차단)*
FDP_IFF.1	S_FDP.2	*EI_FMT_Firewall (방화벽 정책 설정 인터페이스)* *EI_FMT_ACL (방화벽 ACL 정책 설정 인터페이스)* *EI_OS_SCALL_inbound (OS시스템콜호출 인터페이스-수집)* *EI_OS_SCALL_oubound (OS시스템콜호출 인터페이스-차단)*

FIA_AFL.1	S_FIA.2	*EI_Login_fail (식별 및 인증 실패 인터페이스)*
FIA_SOS.1	S_FIA.1	*EI_GUI_Login (사용자 식별 및 인증 인터페이스)*
FIA_UAU.1	S_FIA.1	*EI_GUI_Login (사용자 식별 및 인증 인터페이스)*
FIA_UAU.4	S_FIA.4	*EI_GUI_Login (사용자 식별 및 인증 인터페이스)*
FIA_UAU.7	S_FIA.1	*EI_GUI_Login (사용자 식별 및 인증 인터페이스)*
FIA_UID.1	S_FIA.1	*EI_GUI_Login (사용자 식별 및 인증 인터페이스)*
FMT_MOF.1	S_FMD.1	*EI_GUI_FMT_Function (보안 기능 관리 인터페이스)*
FMT_MSA.1	S_FMT.2	*EI_GUI_FMT_data_atrrirbute (보안 속성 및 데이터 관리 인터페이스)*
FMT_MSA.3	S_FMT.2	*EI_GUI_FMT_data_atrrirbute (보안 속성 및 데이터 관리 인터페이스)*
FMT_MTD.1 (1)	S_FMT.2	*EI_GUI_FMT_data_atrrirbute (보안 속성 및 데이터 관리 인터페이스)*
FMT_MTD.1 (2)	S_FMT.2	*EI_GUI_FMT_data_atrrirbute (보안 속성 및 데이터 관리 인터페이스)*
FMT_PWD.1 (확장)	S_FMT.2	*EI_GUI_FMT_data_atrrirbute (보안 속성 및 데이터 관리 인터페이스)*
FMT_SMF.1	S_FMT.2	*EI_GUI_FMT_data_atrrirbute (보안 속성 및 데이터 관리 인터페이스)*

FMT_SMR.1	S_FMT.2	*EI_GUI_Login (사용자 식별 및 인증 인터페이스)*
FPT_PST.1 (확장)	S_FDP.1	*EI_Internal_protect_data (저장된 데이터 보호 인터페이스)* *EI_Generate_DRBG_API (암호키 생성 인터페이스)* *EI_Generate_KEY_API (암호키 생성 인터페이스 호출)*
FPT_STM.1	S_FPT.4	*EI_GUI_Timestamp (신뢰된 시간 생성 인터페이스)*
FPT_TST.1	S_FPT.3	*EI_initial (제품 시동)* *EI_GUI_Selftest (곽자체시험 인터페이스)*
FTA_MCS.2	S_FTA.1	*EI_GUI_Login(식별 및 인증 인터페이스)*
FTA_SSL.5 (확장)	S_FTA.1	*EI_GUI_Login(식별 및 인증 인터페이스)*
FTA_TSE.1	S_FTA.1	*EI_GUI_Login(식별 및 인증 인터페이스)*
FTP_TRP.1	S_FTP.1	*EI_GUI_Login(식별 및 인증 인터페이스)*

[표 6] SFR-서브시스템-TSFI 간 대응관계(예시)

작성요령

▶ 설계서 작성자는 오퍼레이션이 TSFI에서 요청되는 경우 초기에 호출되는 서브시스템을 식별하고 해당 기능성을 우선적으로 구현할 책임이 있는 다양한 서브시스템을 식별해야 함

☑ 각 TSFI에 대한 완전한 '호출 트리'는 요구되지 않음을 주의

☑ 모든 TSFI가 최소한 하나의 서브시스템으로 대응되는지 보장함으로써 대응관계의 완전성을 입증할 수 있음

☑ 부적합 대응관계 예시로는 정보흐름통제를 다루는 TSFI를 패스워드 검사에 대한 서브시스템에 대응시키는 것은 정확하지 않은 내용이므로 작성에 유의 필요함

☑ ST 작성자가 기능요구사항에서 수행한 오퍼레이션(할당, 정교화, 선택)으로 인하여 요구사항의 엘리먼트 수준의 상세수준이 될 수 있음을 유의해야 함

예) FDP_IFF.1.2 엘리먼트의 할당에 a) 규칙은 방화벽 정책에 모듈에 대응되고 b) 규칙은 ACL 정책 모듈에 대응되는 대응관계를 명확하게 서술해야 함

☑ ST에서 도출된 모든 SFR이 하나 이상의 서브시스템과 대응되고, 모든 TSFI가 하나 이상의 서브시스템과 대응됨을 통해 모든 보안기능요구사항을 정확하게 실체화 했음을 입증

5. 비-보안 서브시스템

5.1. 비-보안 서브시스템(Non-TSF)

☞ *보안목표명세서(ST)의 보인기능요구사항(SFR)과 관련이 없으며 상호작용과 연관이 없는 서브시스템이 있는 경우 작성한다.*

예:

본 절에서는 TSF 데이터를 사용하지 않는 비보안 서브시스템에 대한 내용을 서술한다. 비보안 서브시스템(Non-TSF)을 구성하는 하부시스템은 다음과 같다.

o HELP.1: 도움말 기능

... 추가작성

5.1.1 도움말 기능

인가된 관리자가 TOE의 보안기능 설정에 대한 정보가 필요할 경우 이를 위해 도움말 기능을 제공한다.

... 기능에 대한 요약설명 위주로 추가작성

2) 상호작용

도움말 기능은 관리자의 편의를 위해 제공되는 기능이므로 보안기능과 관계가 없으며, TSF 데이터를 사용하지 않는다.

... 다른 기능과 관련이 있는 경우에 요약설명 위주로 추가 작성