국가용 보안요구사항 V3.0 기반의

국내용 사용자 운영 설명서 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**
1.1. 사용자 운영 설명서 참조 1
1.2. 목적 1
1.3. 사용자 운영 설명서 구성 1
1.4. 용어 정의 2
1.5. 참조 문서 3

2. 제품 소개 **4**
2.1. 제품 구성요소 4
2.2. 운용 시 주의사항 4

3. 000 V1.0 접속 **6**
3.1. 000 V1.0 접속 6

4. 정책 설정 **8**
4.1. 방화벽 정책 추가 8
4.2. 네트워크 객체 추가 8

5. 고객 지원 **10**

6. 부록 **11**
6.1. 제품 오류 메시지 11
6.2. FAQ 11

1. 개요

1.1. 사용자 운영 설명서 참조

☞ *사용자 운영 설명서 식별을 명확하게 할 수 있도록 문서명, 형상관리 번호 등 식별정보 서술*

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

참고사항	▶ 신규로 제출물을 작성하는 경우 사용자 운영 설명서 작성자는 본 가이드를 참고하여 사용자 운영 설명서를 작성할 수 있다.

1.2. 목적

☞ *사용자 운영 설명서는 사용자가 TOE 보안 기능 사용을 위한 모든 절차를 기술해야 한다. TOE 운영을 위한 사용자 역할, 인터페이스, 운영 모드 등 TOE의 보안 기능 사용을 위한 운영 절차 및 지침을 완전하게 기술해야 한다.*

예: 사용자 운영 설명서는 사용자가

운영과정에서 숙지하여야할 사항에 대하여 기술하고 있다.

1.3. 사용자 운영 설명서 구성

사용자 운영 설명서는 다음과 같이 구성되어 있다.

1장은 사용자 운영 설명서 개요로 설명서의 목적, 구성 등을 기술한다.

2장은 제품의 제품 주요 기능 및 구성요소에 대하여 기술한다.

3장에서 제4장까지는 제품에서 제공하는 000 기능에 대하여 기술한다.

5장은 고객지원 사항에 대한 내용을 기술한다.

부록은 제품에서 발생되는 오류메시지에 대하여 기술한다.

1.4. 용어 정의

☞ *사용자 운영 설명서에서 사용되는 용어를 중점적으로 추가하여 기술한다.*

예:

관리자(administrator)

제품의 보안기능에 의해 구현된 모든 정책에 관해서 신뢰 등급을 가진 실체

보증(assurance)

제품이 보안기능요구사항을 만족한다는 신뢰성의 근거

인가된 사용자(authorised user)

보안기능요구사항에 따라서 제품에서 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 제품 내의 수동적인 실체

주체(Subject)

객체에 대한 오퍼레이션을 수행하는 제품 내의 실체

사용자 데이터(user data)

일부 외부 실체에게는 의미가 있지만 제품의 보안기능 운영에 영향을 미치지 않는, 제품이 수신 또는 생성한 데이터

2. 제품 소개

☞ *TOE에 대한 간략한 소개 및 주요 기능을 기술한다.*

☞ *제품 소개는 보안목표명세서 및 TOE 설계서의 내용과 일관되게 기술하여야 한다.*

예 : 000 V1.0은 내부망에 연결되어 있는 자산을 외부로부터 보호하기 위해 인가된 관리자가 설정한 규칙에 따라 트래픽을 제어하는 기능을 제공하는 침입차단시스템이다. 000 V1.0은 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.

2.1. 제품 구성요소

☞ TOE, TOE 버전, TOE 구성요소 등 TOE 식별 정보를 기술합니다.

예: 000 V1.0의 구성요소는 다음과 같습니다.

제품명		*000 V1.0*
제품 버전		*V1.0.0*
제품 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*

2.2. 운용 시 주의사항

☞ *보안목표명세서에 서술된 운영환경에 대한 보안목적을 만족시키기 위해 준수해야 하는 보안대책을 기술한다.*

☞ *TOE 운영과 관련된 절차적, 물리적, 인적, 연결 대책 등을 포함하도록 기술한다.*

예:

물리적 보안

인가된 관리자만이 접근 가능한 물리적으로 안전한 환경에 위치해야 한다.

신뢰된 관리자

인가된 관리자는 악의가 없으며, 제품의 관리 기능에 대하여 적절히 교육을 받았고, 모든 관리 지침 및 행동 절차에 따라 정확하게 의무를 수행해야 한다.

로그백업

인가된 관리자는 감사기록 유실에 대비하여 감사 데이터 저장소의 여유 공간을 주기적으로 확인하고 감사기록이 소진되지 않도록 감사기록 백업(외부 로그 서버, 별도 저장장치 등) 등을 수행해야 한다.

운영체제보강

제품의 인가된 관리자는 제품이 설치되어 운영되는 운영체제의 최신 취약점에 대한 보강작업을 수행하여 운영체제에 대한 신뢰성과 안전성을 보장해야 한다.

타임스탬프

IT 환경에서 RFC1305를 따르는 NTP 서버 또는 OS는 신뢰 할 만한 타임스탬프를 제공해야 한다.

3. 000 V1.0 접속

☞ *TOE 운영 중 사용자가 접근 가능한 모든 인터페이스 및 기능에 대해 사용방법 및 절차 등 설명을 기술해야 한다.*

☞ *보안기능 운용을 위한 인터페이스 호출 방법, 사용자가 설정하는 매개변수에 대한 설명이 매개변수의 범위, 기본값 등을 포함하여 기술해야 한다.*

3.1. 000 V1.0 접속

예:

1. 웹 브라우저에 다음의 주소를 입력하여 웹 콘솔에 액세스합니다.

- https://000.000.000.000

2. 로그인 화면에서 사용자 이름(ID)과 비밀번호(PW)를 입력합니다.

필드명	필드 설명
사용자 이름(ID)	관리자의 아이디를 입력합니다. 해당 필드는 영문 기준 20자까지 입력할 수 있습니다.
비밀번호(PW)	관리자의 비밀번호를 입력합니다. 해당 필드는 영문기준 15자까지 입력할 수 있습니다.

3. Login(로그인)을 클릭합니다.
4. 인증에 성공하면 000 V1.0 인터페이스가 열립니다.

4. 정책 설정

4.1. 방화벽 정책 추가

예:

1. [방화벽 정책 설정]을 클릭합니다.

※ [방화벽 정책 설정]이 활성화되지 않으면 정책 설정 권한이 부여된 사용자 계정으로 접속합니다.

2. [정책 추가]를 클릭합니다.

3. 방화벽 정책 설정을 위한 항목을 입력합니다.

필드명	필드 설명
방향	방화벽 정책 방향을 선택합니다.
서비스	서비스 객체를 선택합니다.
네트워크-출발지	출발지 네트워크 객체를 선택합니다.
네트워크-목적지	목적지 네트워크 객체를 선택합니다.
설정	해당 Traffic의 허용/차단 여부 및, 허용/차단시에 로그 기록 여부를 선택합니다.
인터페이스	Inbound/Outbound Network Interface를 선택합니다.
설명	해당 IP Filter 정책에 대한 설명을 입력합니다. 해당 필드는 영문,숫자,한글,특수문자, 기준 80자까지 입력할 수 있습니다.

4. [확인]을 클릭하여 정책을 추가합니다.

4.2. 네트워크 객체 추가

예:

1. [방화벽 정책 설정]을 클릭합니다.

※ [방화벽 정책 설정]이 활성화되지 않으면 정책 설정 권한이 부여된 사용자 계정으로 접속합니다.

2. [네트워크 객체] 추가를 클릭합니다.

3. *방화벽 정책 설정을 위한 항목을 입력합니다.*

<table>
<tr><th>필드명</th><th>필드 설명</th></tr>
<tr><td>네트워크 명</td><td>네트워크 객체의 이름를 입력합니다. 해당 필드는 영문, 숫자 기준 32자까지 입력할 수 있습니다.</td></tr>
<tr><td>설명</td><td>네트워크 객체에 대한 설명을 입력합니다. 해당 필드는 영문,숫자,한글,특수문자, 기준 80자까지 입력할 수 있습니다.</td></tr>
<tr><td>네트워크 타입</td><td>네트워크 타입을 선택합니다. 해당 필드는 아래 표와 같이 입력할 수 있습니다.
<table>
<tr><th>유형</th><th>내용</th></tr>
<tr><td>Any</td><td>모든 IP address를 나타냅니다.</td></tr>
<tr><td>IP 주소 선택</td><td>특정 IP address 범위를 나타냅니다. 시작/끝 주소를 입력합니다. 해당 필드는 IP 주소 형식의 1~255 사이의 숫자를 입력 할 수 있습니다.</td></tr>
<tr><td>CIDR 방식</td><td>Netmask를 이용하여 IP address를 입력합니다. 해당 필드는 1~32 사이의 숫자를 입력할 수 있습니다.</td></tr>
</table></td></tr>
</table>

4. [확인]을 클릭하여 객체를 추가합니다.

5. 고객 지원

예: 기술지원이 필요하거나 제품에 대한 문의 사항은 아래 연락처로 문의하시기 바랍니다..

고객지원센터 02.xxx.xxxx

aaa@bbb.com

서울시 ~~~~~

대표 전화: 02.xxx.xxxx

팩스: 02.xxx.xxxx

홈페이지: http://aaa.bbb.com

6. 부록

6.1. 제품 오류 메시지

- **"ID 또는 패스워드가 올바르지 않습니다."**
  1. 해당 입력 항목을 입력하지 않았을 경우 표시되는 ~~~~~.
- **"~~~~~~~~~~~~."**
  1. ~~~~.

6.2. FAQ

9.1.5 사용자/부서/그룹등 권한이 중복 설정된 경우의 동작 방식

1. 해결 방법
2. 권한을 부여한 xxxx.
3. 사용자 권한 : xxxx