<부록7. 개발보안 문서>

CHAOS ver1.0
개발보안 문서 ver1.0

(ALC_DVS.2)

- 고등급 보안 마이크로커널 개발 -

<목 차>

1. 개요

본 문서는 TOE에 해당하는 CHAOS(Chibi-based High Assurance Operating System)의 보안대책에 대한 적절성 및 충분성을 설명하는 개발보안 문서(ALC_DVS.2)이다. 공통평가기준(CC, Common Criteria)의 ALC_DVS 패밀리는 TOE와 TOE의 부분을 보호하기 위해 개발 환경에서 사용될 수 있는 물리적, 절차적, 인적, 기타 보안대책에 관한 설명을 제시하도록 요구한다. 해당 설명에는 개발 장소의 물리적 보안과 개발 인력을 선발할 때 사용되는 절차를 포함해야 한다. 따라서 본 문서에서는 해당 패밀리 내의 컨포넌트들에 따라 CHAOS 개발환경의 보안대책이 충분한지 근거를 기술한다.

1.1. 문서의 목적

본 문서의 목적은 CHAOS의 안전한 운영이 손상되지 않도록 보장하기 위해 CHAOS 설계 및 구현에 대한 비밀성과 무결성을 제공하는 것이며, 이 과정에서 개발자가 개발환경에 적용한 보안통제가 적절한지, 적용한 보안대책이 충분한지를 입증하는 것이다.

1.2. 문서의 구성

본 문서는 아래와 같이 구성되어 있다. 1장은 본 문서의 개요를 보여주며 2장은 평가받고자 하는 개발 환경의 물리적 위치와 수행활동에 대한 전반적인 개요를 제시한다. 3장에서는 보안대책을 수립하기 위한 근거인 자산, 위협, 조직의 보안정책 등을 제시함으로써, 개발 환경 내 적용된 보안대책이 적절하고 충분한지에 대해 서술한다.

2. 개발환경

TOE를 구현하기 위한 개발환경은 아래 기입된 주소 내 연구실에서 구축되었다. 고등급 보안 및 보증 수준을 만족하는 TOE를 구현하기 위해 해당 장소에서는 요구사항 도출, 설계, 테스팅 관련 개발 활동이 수행되었다.

개발 환경의 물리적 위치는 아래와 같다.

◦ 고려대학교 자연계캠퍼스 로봇융합관 401호 보안공학연구실
(지번: 서울특별시 성북구 안암동5가 126-16)

3. 보안대책

본 장에서는 개발환경 내 적용된 보안대책의 적절성 및 충분성을 어떻게 만족하는지 설명하기 위한 근거에 대해 제시한다. 이를 위해 먼저 개발 환경 내 산출물 중 TOE에 영향을 줄 수 있는 것을 자산으로 식별해야 한다. 이후 식별된 자산에 대해 발생할 수 있는 보안 위협을 도출한 후, 이를 완화하기 위해 만족해야 하는 개발 환경에 대한 보안 목적을 서술한다. 마지막으로 본장 말미 서술한 보안대책이 앞서 서술한 모든 보안목적을 만족함을 표 형태로 도식화함으로써 TOE 개발 시, 적용된 물리적, 절차적, 인적 보안대책이 개발 환경 내 발생할 수 있는 보안 위협으로부터 자산을 보호하는데 적절함과 동시에 충분함을 입증할 예정이다.

3.1. 자산

개발 환경 내 산출물 중 구현물(TOE)에 영향을 줄 수 있는 자산은 형태와 그 목적에 따라 크게 3가지로 구분된다.

번호	자산 명	상세 설명
1	Development Data	개발 과정 중 도출되는 모든 산출물(가이드라인, 지침, 소스 코드 등)로 IT 장비에서 사용할 수 있는 전자 형태의 파일
2	Development Tools	개발 활동(요구사항 도출, 설계, 테스팅, 구현 등)을 수행할 때, 활용되는 모든 도구(이때, ALC_CMC, ALC_CMS 보증 컴포넌트와 별개로 형상관리 도구도 보호해야 하는 자산으로 식별됨)
3	Physical object	개발자들이 편의 또는 팀 내 기술회의 등과 같은 부수적인 이유로 제작하는 것으로 회의 자료, 의사 코드, 테스트 결과 샘플 등 TOE에 대한 내부 정보가 포함된 모든 종이 문서

[표 1] 개발 환경 내 보호해야 하는 자산

3.2. 위협

개발 환경 내 자산에 대해 악영향을 줄 수 있는 보안 위협은 그 형태에 따라 아래와 같이 7 가지로 구분된다.

번호	위협 명	상세 설명
1	T. Smart Theft	접근이 인가된 개발 환경 내 물리적 공간이나 접근이 통제되어야 하는 영역을 통해 공격자가 자산에 접근하는 위협
2	T. Rugged Theft	접근이 모두에게 허용되는 물리적 공간이나 접근이 통제되어야 하는 영역을 통해 공격자가 자산에 접근하는 위협. 해당 위협은 외부의 제 3자가 전문적인 장비(Specialized Equipment)를 활용함
3	T. Computer Net	자산 중 Development Data가 네트워크 상의 비인가된 접근으로 인해 접근되는 위협. 해당 위협은 보안에 대한 전문 지식을 함양한 해커(Experts)가 표준 장비(Standard Equipment)를 활용함
4	T. Unauthorised Staff	접근이 허용되지 않은 개인(내부 직원, 타부처 계약 담당자 등)이 자산이 위치한 영역에 접근하는 위협
5	T. Staff Collusion	외부의 제 3자가 개발 환경에 접근할 수 있는 직원에게 뇌물을 제공하거나 협박하여 자산에 접근하는 위협
6	T. Accident Change	교육을 받지 않은 개발 직원이나 계약 담당자에 의해 기존 TOE나 형상관리 시스템의 설정이 우발적으로 변경됨에 따라 발생할 수 있는 위협
7	T. Attack Transport	업무적 이유로 인해 조직 내부 구성원 간 데이터나 제품을 전달하는 과정 중 자산이 수정 또는 외부로 유출되는 위협

[표 2] 개발 환경 내 발생할 수 있는 위협

3.3. 조직의 보안정책

개발 환경을 유지하는데 필요한 조직의 보안 정책은 아래와 같이 6 가지로 구분된다.

번호	조직의 보안정책 명	상세 설명
1	P. Config Item	형상 관리 시스템은 형상 항목을 식별할 수 있어야 함
2	P. Config Control	개발 환경 내 생산 공정 절차나 제품에 대한 초기 설정은 적절한 절차에 따라 승인된 담당자에 의해서 변경이 승인될 수 있음
3	P. Config Process	개발 환경 내 개발 활동과 프로세스는 관련 절차에 따라 진행되어야 함

4	P. Data Transfer	업무 목적의 조직 내부 연구원 간 데이터 전송이 요구되는 경우, 보안 수준이 요구되는 전자 형태의 데이터는 암호화되어야 함
5	P. Serve Guidance	개발 환경 내 구축된 장비나 인프라를 활용할 수 있도록 충분한 설명 및 가이드를 제공
6	P. Secure Scrap	개발 시, 발생된 산출물에 대한 별도의 점검 및 파기 프로세스가 구축되어 있어야 함 - 생산된 제품의 불량 여부를 점검해야 함. 불량품의 경우 고객 요청에 따라 처리되어야 함(현장 파기 또는 고객 반환). 이때 모든 작업은 보안 구역에서 CCTV 로 모니터링되어야 함 - 산출물 중 TOE 내부 정보가 포함된 전자 기기는 별도 프로세스에 따라 적절히 파기되어야 함 - 산출물 중 일반 문서는 파쇄기를 통해 문서 내용이 식별되지 않게 완벽히 파쇄되어야 함

[표 3] 개발 환경에 대한 조직의 보안정책

3.4. 보안 목적

개발 환경 내 자산에 대해 악영향을 줄 수 있는 보안 위협을 완화하기 위해 만족해야 하는 보안 목적 아래와 같이 15 가지로 구분된다.

번호	보안목적 명	상세 설명
1	O. Physical Access	개발 환경 내 방문자에 대한 접근 권한을 영역별로 할당함으로써, 방문자들이 최소권한의 법칙에 맞게 자산에 접근할 수 있도록 접근통제를 수행함
2	O. Security Guard	개발 환경에 대한 비인가된 접근을 방지하거나 방문자들을 적절히 안내하기 위해, 방문자들에 대해 출입통제 및 감시 수행을 위한 현장 인력 배정
3	O. Alarm Response	보안 사고를 성공적으로 예방하기 위해, 자산에 대해 비인가된 접근이 발생하기 전에 경보가 발생해야 함
4	O. Internal Monitor	기존 보안대책의 유효성 여부에 대해 평가를 수행하기 위해 6개월마다 주기적으로 내부 감사 및 관련 회의를 수행해야 함
5	O. Maintain Security	개발 환경 내 주요 인프라가 정상적으로 동작하는지 확인하기 위해, 주요 시스템에 대한 감사를 수행해야 함

6	O. Network Separation	방화벽을 통해 개발 환경 내 네트워크와 외부망(인터넷)을 논리적으로 분리함. 이때, 방화벽은 화이트리스트 기반의 접근통제 정책을 기반으로 사전에 허용한 서비스와 네트워크 연결만을 허용
7	O. Up-to-date Ver	최신 사이버 보안위협에 대응할 수 있도록 IT 장비 및 인프라에는 최신 버전의 암호 및 백신 프로그램이 설치되어야 함
8	O. Control Scrap	시스템 운용 시, TOE 대한 기밀성 및 무결성을 보호하기 위해 TOE에 대한 주요 기밀 정보가 포함된 문서 및 관련 전자 매체를 파기할 수 있는 방안이 마련되어야 함
9	O. Staff Engagement	자산에 접근할 수 있는 모든 직원들에 의해 발생할 수 있는 보안 문제를 방지하기 위해 보안 서약서를 서명해야 함. 또한 직원들이 올바르게 업무를 수행할 수 있도록 관련 교육 과정을 제공해야 함
10	O. Config Item	형상 관리 시스템은 고유 식별자를 기반으로 형상 항목을 식별할 수 있어야 함
11	O. Config Control	개발 환경 내 생산 공정 절차나 제품에 대한 초기 설정은 적절한 절차에 따라 승인된 담당자에 의해서 변경이 승인될 수 있음
12	O. Config Process	개발 환경 내 개발 활동과 프로세스는 관련 절차에 따라 진행되어야 함
13	O. Data Transfer	업무 목적의 조직 내부 연구원 간 데이터 전송이 요구되는 경우, 보안 수준이 요구되는 전자 형태의 데이터는 암호화되어야 함
14	O. Serve Guidance	개발 환경 내 구축된 장비나 인프라를 활용할 수 있도록 충분한 설명 및 가이드를 제공

[표 2] 개발 환경이 만족해야 하는 보안 목적

4. 보안대책

본 장에서는 본 문서에서 다루고 있는 모든 유형의 보안대책에 대해 상세히 서술한다. 이때 보안대책의 유형에는 물리적, 절차적, 인적 및 기타 보안대책이 포함된다. 해당 보안 대책은 개발 환경 내 자산을 보호함으로써, TOE의 기밀성 및 무결성을 확보하는데 간접적으로 영향을 끼친다.

4.1. 물리적 보안대책

본 절에서는 개발 환경에 적용된 보안대책 중 물리적 보안대책을 서술한다. 그에 대한 상세내용은 [표 1]과 같다. 본 문서에서는 총 5 가지의 물리적 보안대책을 제시한다.

번호	분류	보안대책
1	CCTV 설치	경비를 피해 개발 환경에 대한 비 인가된 접근을 방지하기 위해 건물 입구와 연구실 입구/내부에 CCTV를 설치하여 그런 시도가 발생하는지 여부를 감시
2	열화상 방범시스템 구축	개발 환경에 대한 비 인가된 접근을 방지하기 위해 업무시간(9:00-16:00) 외의 시간은 열화상 방법시스템을 연구실 내에 구축하여 비인가된 접근을 방지한다. 업무시간 외의 접근이 요구되는 경우, 야간 상주하는 경비를 통해 인증 절차를 거쳐 개발 환경이 구축된 연구실에 대한 접근 허가 여부를 결정
3	문 잠금 장치 설치	자산에 대한 비 인가된 접근을 방지하기 위해 개발 서버 및 관련 PC가 위치한 공간(예: 사무실, 서버실 등)에 대한 접근을 확인할 수 있는 별도의 잠금(예: 생체 인증)장치로 보호함
4	백업 시스템 구축	업무 종료 시, 자동으로 동작하는 백업 시스템을 개발 환경에 구축함으로써 재난이나 재해가 발생했을 경우, TOE 내부 정보와 관련 개발용 소프트웨어가 완전히 손실되는 것을 방지

[표 3] 개발 환경 내 물리적 보안대책

4.2. 절차적 보안대책

본 절에서는 개발 환경에 적용된 보안대책 중 절차적 보안대책을 서술한다. 그에 대한 상세내용은 [표 2]와 같다. 본 문서에서는 총 11 가지 절차적 보안대책을 제시한다.

번호	분류	보안대책
1	자료 공유	TOE 개발 시, 생성되는 자료 중 원할 한 업무 수행을 위해 공유되는 자료의 경우, 상급 담당자에게 점검된 후, 수행되어야 함
2	방문자 별 권한 부여	최소권한 법칙에 따라 개발자, 계약 담당자, 하청업체 직원 별로 자산에 대한 서로 다른 권한을 부여함. 이때 프로젝트를 수행하는 개발자는 입사기간에 따라 자산에 대한 접근 권한을 차등적으로 배분함

3	자료 파기	TOE 개발 시, 프로젝트 참여자 간 원활한 협업을 수행하기 위해 제작된 다양한 회의 문서 및 공유 자료에 대해 안전한 파기 정책을 수립 - TOE 내부 정보가 포함된 일반 문서는 협업 종료 후, 파쇄기를 활용하여 해당 문서 파기 - NIST와 같은 공인된 기관에서 권유하는 파기 방법을 준수하여 TOE 내부 정보가 포함된 전자 문서를 파기
4	보안대책의 역할 및 책임	지속적으로 보안대책의 적용과 보안 위배에 대한 탐지를 보장하기 위해 담당자에 따른 역할과 책임을 부여하고 이를 주기적으로 관리
5	형상 관리체계	Private Git을 기반으로 형상관리를 수행함으로써 중요정보에 대한 접근 및 추가/수정/삭제 권한을 통제
6	복구	복구 절차를 사전에 구축하여 개발환경이 구축된 연구실에 재난이나 재해가 발생했을 경우, TOE 내부 정보와 관련 개발용 소프트웨어가 복구될 수 있도록 관리함
6	개발관련 장비 반출입 통제	TOE 개발에 소요되는 각 개발 장비의 반출입 대한 통제를 수행함. 이때 개발 장비를 제3자를 통해 구매하는 경우, 계약 내 보안 조건이 준수되는지 점검함
7	외부인에 대한 출입통제	프로젝트 참여 인원과 동행한 외부인이 TOE 개발 환경에 출입하고자 할 경우 해당 외부인의 신분을 동행한 프로젝트 참여 인원의 방문객으로 등록해야 함
8	내부인에 대한 출입통제	연구실의 구성인원이지만 본 TOE 개발 프로젝트 참여 인원이 아닐 경우 관련 개발 영역에 대해 출입이 제한되어야 한다.
9	연구소 퇴근 시, 휴대용 기기 점검	연구소 퇴근 시 주요 기밀 정보 소장여부에 관한 확인 절차를 구축하여, TOE 내부 정보가 외부로 유출되는 것을 방지함 - 전자 문서를 저장할 수 있는 휴대용 데이터 스토리지(USB)의 경우, 반출입 불허
10	퇴실 보안점검	퇴근 시, 프로젝트 참여인원이 연구 자산을 보호하기 위한 행동 수칙을 수립하고, 이를 준수해야 함
11	내부 회의	보안 담당자와 연구실 책임자는 주기적인 회의를 거쳐 현재 보안대책이 적절한지 의논함

[표 4] 개발 환경 내 절차적 보안대책

4.3. 인적 보안대책

본 절에서는 개발 환경에 적용된 보안대책 중 인적 보안대책을 서술한다. 그에 대한 상세내용은 [표 3]과 같다. 본 문서에서는 총 5 가지의 인적 보안대책을 제시한다.

번호	분류	보안대책
1	신규 개발인력 관리	프로젝트 내 신규 개발인력 투입 시, 일정 기간 동안 TOE 내부 정보에 접근할 수 있는 업무를 최소화함
2	내부 개발인력 개발 정보/자료 비밀유지 대책	프로젝트 내 개발인력들은 프로젝트 투입 시, 보안 서약서를 작성한 후 제출
3	보안 교육	외부 초청 강사나 인터넷 강의를 통해 TOE 개발 시 활용할 수 있는 보안 지식을 관련 프로젝트에 참여하는 연구원들에게 전달함
4	개발인력 퇴사 및 직무 변경 관리	TOE 개발 프로젝트에서 제외된 인력은 관련 인프라(개발 서버)에 대한 접근 권한을 회수함
5	개발 활동 모니터링	프로젝트 참여 인력이 개발 환경 내 저장된 TOE 내부 정보를 무단으로 유출시키는 것을 방지하기 위해, 모든 개발 활동과 관련하여 사용한 IT 장비 및 인프라 활용 내역은 모니터링 되어야 함

[표 5] 개발 환경 내 인적 보안대책

4.4. 기타 보안대책

본 절에서는 앞서 서술한 물리적/절차적/인적 보안대책에 속하지 않는 기타 보안대책에 대해 서술한다. 해당 보안대책은 [표 3]과 같다. 본 문서에서는 총 5 가지의 기타 보안대책을 제시한다.

번호	분류	보안대책
1	논리적 망분리	방화벽을 활용하여, 외부에서 시도되는 인가되지 않은 서비스 요청이나 사이버 보안 위협으로부터 개발 환경 내 IT 인프라와 자산을 보호해야 함
2	암호화	TOE 내부 정보가 포함된 전자 파일을 저장하거나 외부로 전송하는 경우, 해당 파일은 암호화되어야 함
3	최신 업데이트 유지	개발 환경 내 구축된 IT 장비와 인프라는 항상 최신 업데이트 버전이 설치되어야 함
4	시스템 보안	연구원들은 개인 PC에 안전한 개발 환경을 확보할 수 있도록 알약, 백신과 같은 보안 프로그램이 설치되어 있어야 함
5	경비 인력 배치	방문록을 관리하고 실험실이 위치한 건물의 방문객에 대한 접근 통제 및 안내를 수행하기 위한 별도의 인력이 건물 입구에 상주해야 함

[표 1] 개발 환경 내 기타 보안대책

5. 보안대책의 종속 관계

본 장에서는 2장에서 서술한 보안대책에 대해 적절성 및 충분성을 어떻게 만족하는지 그 근거에 관해 설명한다. TOE와 TOE에 관련된 정보를 대상으로 한 공격은 각각 다른 설계 및 생산 단계에서 이루어지므로 해당 공격을 방지하기 위한 보안대책을 가져야 한다.

본 장에서는 앞서 4장에서 식별된 보안대책이 충분하다는 것을 입증하기 위해 서술한 보안대책이 본장에서 서술한 모든 보안목적을 만족함을 표 형태로 도식화한다. 이를 통해 TOE 개발 시, 적용된 물리적, 절차적, 인적 보안대책이 개발 환경 내 발생할 수 있는 보안 위협을 완화하는데 적절함과 동시에 충분함을 입증할 예정이다.

위협 및 조직의 보안정책	보안목적	보안 대책
T. Smart Theft	O.Physical Access O.Security Guard O.Alarm Response O.Internal Monitor O.Maintain Security	(물리적 보안대책) - CCTV 설치 - 열화상 방범시스템 구축 - 개폐 장치 설치 (절차적 보안대책) - 연구소 퇴근 시, 휴대용 기기 점검 - 내부인(외부인)에 대한 접근통제 - 방문자 별 권한 부여 - 자료 파기 - 내부 회의 (기타 보안대책) - 경비 인력 배치
T. Rugged Theft		

이유・근거 (Rationale)

권한이 없는 건물 방문객이 개발 환경이 구축된 연구실에 무단으로 침입하는 것을 방지하기 위해, 연구실이 위치한 건물 입구에는 연구실 업무 시간과 관련 없이 항시 **“경비 인력”** 이 상주하고 있다. 해당 인력은 **“내부인(외부인)에 대한 접근통제 절차”** 와 **“연구소 퇴근 시, 휴대용 기기 점검”** 를 통해 연구실 내 자산에 비허가된 인원이 접근하는 것을 방지한다. 업무 시간 내 건물 출입객은 신분 및 TOE 개발 프로젝트 참여 여부에 따라 **“방문자 별 다른 접근 권한이 부여”** 된다. 이때 방문객이 조직 내 인력이 아닌 경우 별도의 방명록 작성이 요구된다. 모든 건물 입구와 연구실 출입은 **“출입구와 연구실 내 설치된 CCTV”** 를 통해 상황실에서 모니터링되어, 현장 경비 인력이 미처 확인하지 못한 출입자들을 관리한다. 업무시간 이외에는 연구실 내 설치된 **“열화상 방범시스템”** 과 **“연구실 출입문에 설치된 개폐 장치”** 를 활용하여 비인가된 접근을 방지한다. 만약 상기 보안대책을 통해 비인가된 접근이 발견되는 경우, 알람을 통해 별도의 보안 조치를 취한다. 이외에도 외부인이 우연히 TOE 내부 정보가 포함된 일반 문서를 획득하는 것을 방지하기 위해 업무 종료 후, 모든 자료는 **“자료 파기 절차”** 에 따라 파쇄되도록 조치한다. 또한 현재 보안대책이 여전히 상기 위협을 완화할 수 있는지 여부를 판단하기 위해 6개월마다 주기적인 회의를 수행한다. 만약 부족하다고 판단되는 경우, 이를 해결하기 위해 공통평가기준에서 제공하는 보조 문서인 “Minimum Site Requirements” 문서를 참고하여 추가 보안대책을 수립한다.

위협 및 조직의 보안정책	보안목적	보안 대책
T. Computer Net	O.Internal Monitor O.Maintain Security O.Network Separation O.Data Transfer	(절차적 보안대책) - 보안대책의 역할 및 책임 - 내부 회의 (인적 보안대책) - 개발활동 모니터링 (기타 보안대책) - 논리적 망분리 - 암호화 - 최신 업데이트 유지 - 시스템 보안

이유・근거 (Rationale)

외부 해커가 개발 환경 내 구축된 IT 기기와 인프라에 무단으로 침입하는 것을 방지하기 위해, **"논리적 망분리"** 를 통해 연구실을 포함한 건물 내 사설망을 구축한다. 만약 해커가 건물 내 사설망에 침투하여 연구실 내 설치된 IT 기기와 인프라에 접근할 수 있기 때문에, 백신 프로그램이나 스파이웨어 등의 보안 프로그램을 통해 **"시스템 보안"** 을 구축한다. 또한 설치된 보안 프로그램이 최신 바이러스를 탐지할 수 있도록 항상 **"최신 업데이트를 유지"** 하도록 한다. 해커가 상기 서술한 보안대책을 우회하여 TOE 개발 프로젝트 참여 연구원 권한으로 개발 환경 내 인프라에 저장된 전자 파일에 접근하는 경우, **"개발활동 모니터링"** 을 기반으로 모든 행위를 수행한다. 향후 해당 내용을 기반으로 **"보안대책 역할 및 책임"** 을 재수립한 후, **"내부 회의"** 를 거쳐 추가 보안대책을 수립한다.

이외에도 해커는 TOE 개발 프로젝트 참여 연구원 간 메일 송・수신 시, 중간자 공격을 통해 건물 출입에 필요한 인증 정보(관련 위협: T. Smart Theft, T. Rugged Theft) 또는 TOE 내부 정보 등을 탈취할 수 있다. 이를 완화하기 위해 상기 정보가 포함된 자료 전송 시, 별도로 자료를 **"암호화"** 한다.

위협 및 조직의 보안정책	보안목적	보안 대책
T. Unauthorised Staff	O.Physical Access O.Security Guard O.Alarm Response O.Internal Monitor O.Maintain Security O.Staff Engagement O.Config Control O.Control Scrap	(물리적 보안대책) - CCTV 설치 - 개폐 장치 설치 (절차적 보안대책) - 자료 공유, 파기 - 내부 개발인력 개발 정보/자료 비밀유지 대책 - 연구소 퇴근 시, 휴대용 기기 점검 - 내부인에 대한 출입통제 - 내부 회의 (인적 보안대책) - 개발인력 퇴사 및 직무 변경 관리

		- 개발 활동 모니터링 (기타 보안대책) - 경비 인력 배치

이유・근거 (Rationale)

TOE 개발 프로젝트 참여인원이 자신에게 허용된 권한 이상의 행위를 수행하여 자산에 접근하는 것을 방지하기 위해, 모든 프로젝트 참여 인원은 초기에 **"보안대책의 역할 및 책임"** 에 따라 권한을 부여 받는다. 건물 입구에 배치된 **"경비 인력"** 은 상기 부여된 권한에 따라 건물에 방문하는 **"내부인에 대한 출입통제"** 를 수행한다. 건물에 입장이 허가된 인원은 자신의 권한이 부여된 신분증을 **"연구실 문에 설치된 개폐 장치"** 에 태그하고 연구실에 입장한다. 이때 모든 건물 입구와 연구실 출입은 **"출입구와 연구실 내 설치된 CCTV"** 를 통해 상황실에서 모니터링되어, 현장 경비 인력이 미처 확인하지 못한 출입자들을 관리한다. 상기 서술한 보안대책을 우회하여 TOE 개발 프로젝트 참여 연구원 권한으로 개발 환경 내 인프라에 저장된 전자 파일에 접근하는 경우, **"개발활동 모니터링"** 을 기반으로 모든 행위를 수행한다. 향후 해당 내용을 기반으로 **"보안대책 역할 및 책임"** 을 재수립한 후, **"내부 회의"** 를 거쳐 추가 보안대책을 수립한다.

이외에도 TOE 개발 프로젝트에 중도 하차한 연구원이나 협력 기관 소속 연구원에게 TOE에 대한 내부 정보가 유출되는 것을 방지하기 위한 별도의 보안대책이 필요하다. TOE 개발 프로젝트에 중도 하차한 연구원에게 TOE 내부 정보가 유출되는 것을 방지하기 위해 중간에 프로젝트에서 제외된 연구원들은 **"개발인력 퇴사 및 직무 변경 관리"** 절차에 따라 부여된 모든 권한이 회수된다. 또한 TOE 개발 시, 타 기관 소속 연구원과 회의를 목적으로 만드는 자료는 공유되기 전 **"자료 공유"** 절차에 따라 상급자의 승인이 선행되어야 하며 회의 종료 후 모든 자료는 **"자료 파기"** 절차에 따라 안전하게 파기되어야 한다.

위협 및 조직의 보안정책	보안목적	보안 대책
T. Staff Collusion	O.Staff Engagement O.Internal Monitor O.Maintain Security O.Control Scrap	(물리적 보안대책) - CCTV 설치 (절차적 보안대책) - 자료 공유, 파기 - 연구소 퇴근 시, 휴대용 기기 점검 - 퇴실 보안점검 (인적 보안대책) - 내부 개발인력 개발 정보/자료 비밀유지 대책 - 개발 활동 모니터링

이유・근거 (Rationale)

뇌물이나 협박으로 인해 TOE 개발 프로젝트 참여인원이 무단으로 자산에 접근하는 것을 방지하기 위해, 모든 프로젝트 참여 인원은 초기에 **"내부 개발인력 개발 정보/자료 비밀유지 대책"** 에 따라 보안 서약을 받는다. 보안 서약에도 불구하고 자산에 대한 비허가된 접근을 수행하려는 행위를 방지하기 위해 건물에 출입하는 모든 인원의 행동은 **"CCTV" 와 "개발 활동 모니터링"** 에 의해 실시간으로

모니터링된다. 또한 TOE 내부 정보가 포함된 자료가 무단으로 유출되는 것을 방지하기 위해, 모든 자료는 **“자료 공유”**와 **“자료 파기”** 절차에 따라 관리된다. 이외에도 임의의 TOE 개발 프로젝트 참여인원이 업무시간 이외에 연구실에 입장하여, 타 인원의 자료를 반출하는 것을 방지하기 위해 모든 연구실 퇴실자는 퇴근 시, **“퇴실 보안점검”** 절차에 따라 연구 자료를 관리한다.

위협 및 조직의 보안정책	보안목적	보안 대책
T. Accident Change	O.Config Items O.Config Control O.Config Process O.Maintain Security O.Serve Guidance	(물리적 보안대책) - 백업 시스템 구축 (절차적 보안대책) - 개발 활동 모니터링 - 복구 - 형상관리 체계 (인적 보안대책) - 보안 교육 - 신규 개발인력 관리

이유・근거 (Rationale)

TOE 개발 프로젝트 신규 참여인원이 의도치 않게 자산에 접근하여 TOE의 기밀성 및 무결성을 훼손하는 것을 방지하기 위해, 모든 프로젝트 참여 인원은 초기에 **“신규 개발 인력 관리”, “보안 교육”**을 수행한다. 그럼에도 불구하고 신규 참여인원이 의도치 않게 TOE 설정을 변경하는 것을 방지하기 위해 개발 환경에는 각 수행인원의 행동을 “개발 활동 모니터링” 한다. 이후 사고가 발생하는 경우, **“백업 시스템”** 기반의 **“형상 관리 체계”** 및 **“복구”** 절차에 따라 사고 이전의 설정으로 복구되어야 한다.

위협 및 조직의 보안정책	보안목적	보안 대책
T. Attack Transport	O.Config Process O.Up-to-date Ver O.Data Transfer	(절차적 보안대책) - 개발 활동 모니터링 - 보안대책의 역할 및 책임 - 외부인에 대한 접근통제 - 개발관련 장비 반출입 통제 (기타 보안대책) - 암호화 - 최신 업데이트 유지 - 시스템 보안 - 경비 인력 배치

이유・근거 (Rationale)

TOE 개발 프로젝트 진행 시, 개발 산출물이 전달 과정 중에 훼손되는 것을 방지하기 위해, 다양한 보안대책이 적용되어야 한다. 개발 산출물이 특정 하드웨어와 같은 유형의 형태를 가지는 경우, **“보안대책의 역할 및 책임”**에 따라 등록된 배송원에 의해서만 개발 산출물이 운송되어야 한다. 이때 건물 내 **“경비 인력”**은 사전에 정의된 “보안대책의

역할 및 책임" 에 따라 **"외부인에 대한 접근통제"** 를 수행한다. 이후 프로젝트 참여 인원은 운송된 개발 산출물이 사전에 합의한 보안조건을 만족하는 지 여부에 따라 **"개발관련 장비 반출입 통제"** 한다.

만약 개발 산출물이 전자 형태의 문서일 경우, 최신 사이버보안 위협에 대응하기 위해 **"암호화", "최신 업데이트 유지", "시스템 보안"** 이 개발 환경에 적용되어야 한다.

P. Config Item	O.Config Item	-
P. Config Control	O. Config Control	-
P. Config Process	O. Config Process	-
P. Data Transfer	O.Data Transfer O. Up-to-date Ver	-
P. Serve Guidance	O. Serve Guidance	-
P. Secure Scrap	O. Control Scrap	-

[표 1] 보안대책의 종속관계