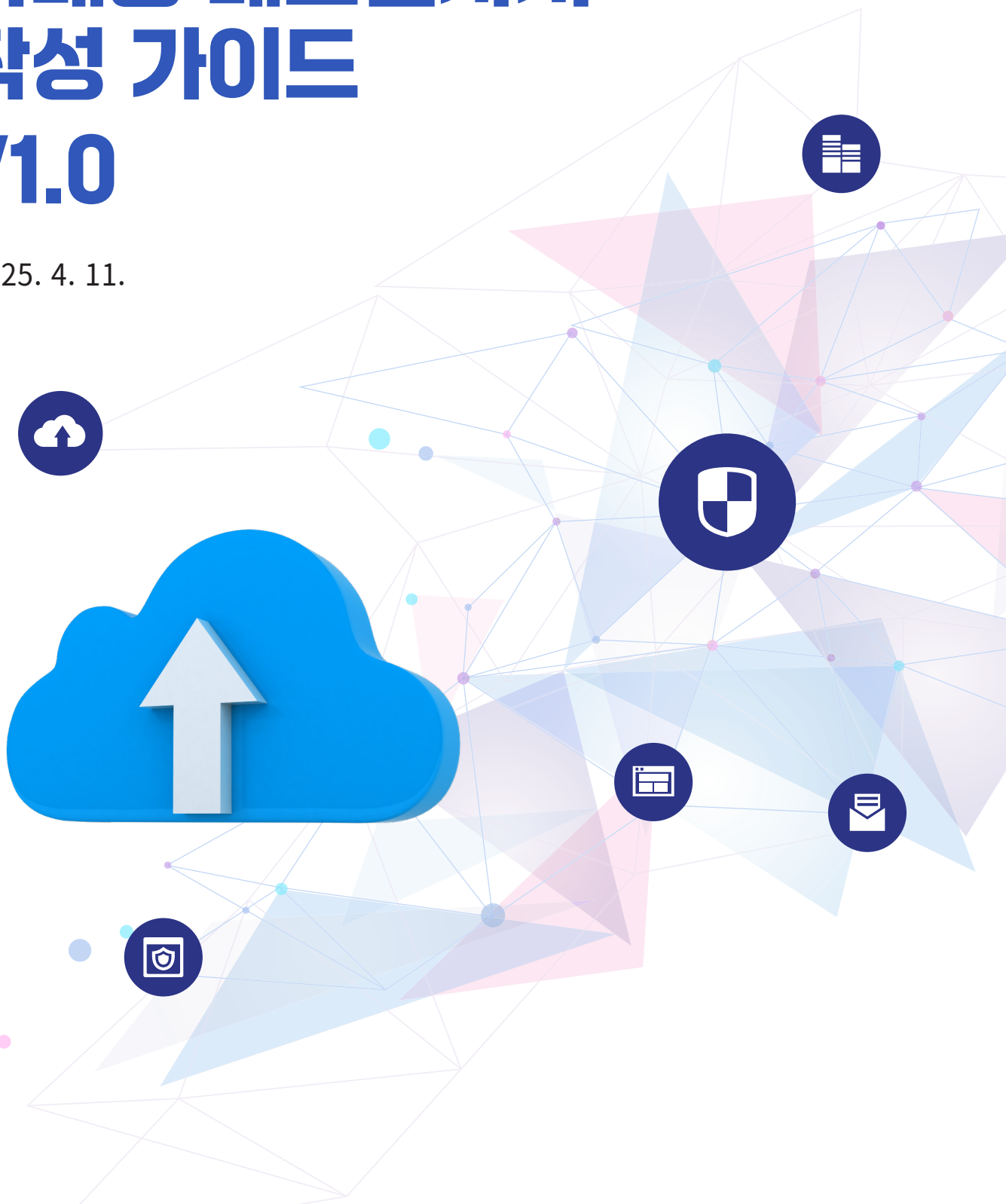


국가용 보안요구사항 V3.0 기반의 국내용 배포절차서 작성 가이드 V1.0

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	4
1.1. 배포절차서의 정의	4
1.2. 배포절차서의 주요 내용	4
1.3. 개발환경 보안점검 항목	5
2. 배포절차서의 구성	6
2.1. 문서의 구성	6
2.2. 배포절차서 작성 시 고려사항	8
2.3. 개발환경 보안점검 목록을 고려하여 작성	8
3. 배포절차서 작성방법 및 예시	10
3.1. 배포절차서 참조	10
3.2. 배포절차서 목적	10
3.3. 배포절차서 구성	11
3.4. 용어 정의	11
3.5. 참조문서	11
3.6. TOE 배포 방법	11
3.7. 배포 인력 체계	12
3.8. TOE 배포 절차별 분석 및 도식화	12
3.9. TOE 배포 절차별 보안 유지 방안	13
3.10. TOE 배포 버전 추적 방법	14
[부록 1] 배포절차서 작성 템플릿	17
[부록 2] 배포절차서의 주요 관찰사항	26

1. 개요

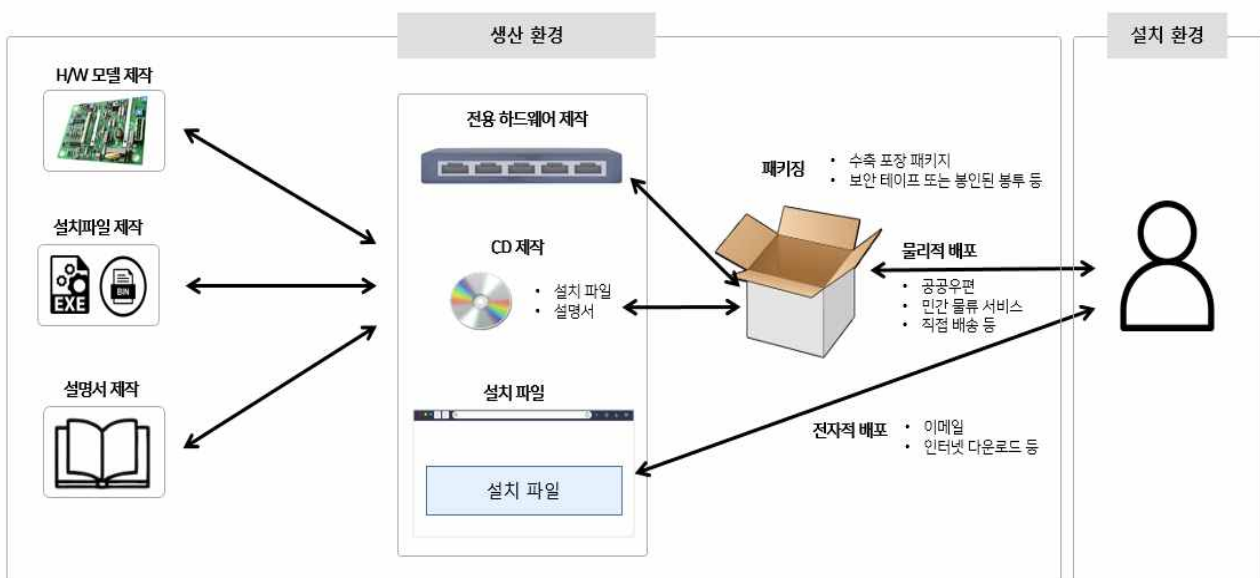
TOE 생명주기 지원과 관련된 보증요구사항은 TOE 개발 및 유지하는 동안 TOE 상세화 과정에서 규칙과 통제 수립을 요구한다. 이와 관련하여 생명주기 지원에서는 생명주기정의, 형상관리 능력, 형상관리 범위, 개발보안, 도구 및 기법, 결함교정, 배포에 대해 다루고 있으며, 본 문서에서는 그 중에서 배포절차에 대한 작성 방법을 다룬다.

1.1. 배포절차서의 정의

배포절차서는 완료된 TOE를 개발환경으로부터 변경되지 않고 소비자에게 배포(안전하게 전송)된다는 것을 보증하기 위해 사용하는 적절한 절차를 서술하는 문서이다.

1.2. 배포절차서의 주요 내용

배포절차서에는 시스템 통제, 배포 시설, TOE가 사용자에게 배포되는 동안 보안이 유지된다는 것을 보증하는데 필요한 방법을 서술해야 한다. TOE를 정확하게 배포하기 위해 TOE배포 절차는 TOE를 배포하는 동안 보안과 관련된 보안목표명세서에서 확인된 내재적 또는 식별된 목표를 다룬다.



하도급자(subcontractor)로부터 개발자로의 전송 또는 서로 다른 개발 장소간의 이동은 개발 보안(ALC_DVS) 문서에서 다루어진다.

배포의 마지막 단계는 TOE가 하위 사용자(= 최종 소비자, 최종 사용자)의 책임하에 들어가게 되는 전송의 수락 시점으로 한다. 전송의 수락 시점은 TOE가 하위 사용자 측에 도착하는 시점과 반드시 일치할 필요는 없다.

배포절차는 다음과 같은 사항을 적용가능하다면 고려하도록 권고된다.

- 1) 하위 사용자에게 전달된 TOE가 평가된 TOE버전과 정확하게 일치함을 보장
- 2) 현재 버전의 TOE에 대한 무단변경 예방 또는 탐지
- 3) 가짜 버전의 TOE제출을 방지
- 4) TOE를 하위 사용자에게 배포할 때 불필요한 정보 차단하고 잠재적인 공격자들이 배포 시기와 방법을 알아서는 안 되는 상황이 있을 수 있음
- 5) TOE가 배포되는 동안 가로채기 되는 것을 차단 또는 탐지
- 6) TOE 배포가 지연되거나 중단되는 상황을 차단

배포절차는 위와 같은 문제로부터 예상되는 수신자(하위 사용자)의 행동을 포함하도록 권고된다. 예상되는 행동에 대한 설명의 일치성은 준비절차서에서도 확인된다.

1.3. 개발환경 보안점검 항목

국내용 인증 시 ALC(생명주기지원 클래스) 일부 보증요구사항 평가를 개발환경보안점검으로 대체하고 있으며 배포 절차도 그중 하나로 평가 과정 중 평가자가 배포절차를 실질적으로 수행하는 배포과정에 대해 개발사의 현장 실사를 통하여 배포 과정의 보안성을 확인하는 과정이 포함된다.

개발환경 보안점검 목록은 인증기관 홈페이지(<http://www.itsec.kr>) 게시판> 자료실에서 「정보보호제품 평가인증 해설서」를 통해 확인 가능하며 배포와 관련된 개발환경 보안점검 항목은 다음과 같다.

점검 항목
1. 배포하는 동안 TOE의 보안을 유지하기 위한 절차는 무엇인가?
2. TOE 배포 시 고려해야 하는 보안성은 무엇인가?
3. TOE를 배포하는 동안 TOE 무결성을 유지하기 위한 기술적인 방법은 무엇인가?
4. 배포되어야 하는 버전의 TOE 만이 배포됨을 보장하는 방법은 무엇인가?
5. 개발자의 마스터 복사본과 사용자 측에서 수령한 버전간의 불일치를 탐지하는 방법은 무엇인가?

배포(ALC_DEL.1)의 개발환경 보안점검 목록은 국제용/국내용 평가 시에는 일부 항목에서 차이점이 있으나 보증등급(EAL2, EAL3, EAL4)에 따라 개발환경 보안점검 항목의 차이점은 존재하지 않는다.

2. 배포절차서의 구성

2.1. 문서의 구성

(1) 표지 예시

문서의 표지에는 해당 문서를 식별할 수 있도록 보안목표명세서의 TOE참조와 일치하도록 TOE의 명칭(제품명)과 문서의 명칭 및 버전, 업체명, 문서 작성 일자등을 기재한다.

Secure Product V1.0 (제품명)

배포절차서

V1.0 또는 Rev.0 (문서버전)

20〇〇 . 〇〇 . 〇〇

XXXX (회사명)

(2) 제·개정 이력 예시

배포절차서의 제·개정 이력을 작성하여 배포절차서의 형상을 관리할 수 있도록 한다. 제·개정이력에는 문서 버전, 일자, 주요 개정 내용 등이 포함되도록 한다.

<제·개정 이력>		
버 전	일 자	개정 내용
1.0	24-12-10	o Secure Product V1.0 배포절차서 V1.0 작성
1.1	24-12-30	o 관찰보고서 EOR-01 반영

(3) 배포절차서 권장 목차

배포절차서의 목차는 아래 예시와 같이 구성될 수 있다. 권장 목차는 단순 예시로 반드시 권장 목차와 같이 구성할 필요는 없다. 제품의 특성 및 개발사의 배포 절차와 특성을 고려하여 목차를 구성할 수 있으며 새로운 항목을 추가하거나 제외하여 구성할 수 있다. 특히 2장 배포업무 규정 및 인력체계 부분은 권장목표에서와 같이 별도의 장으로 구분하여 설명할 수 있으나 3장 배포절차 설명 시 관련 내용을 포함하여 서술 가능하다.

배포절차서 전체 : 권장 목차

1. 개요
 - 1.1 배포절차서 참조
 - 1.2 배포절차서 목적
 - 1.3 배포절차서 구성
 - 1.4 용어 정의
 - 1.5 참조 문서
2. 배포 업무 규정 및 인력체계
 - 2.1 TOE 배포 방법
 - 2.2 배포 인력 체계
3. 배포 절차 및 보안유지 방안
 - 3.1 TOE 배포 절차 분석 및 도식화
 - 3.2 배포 단계별 설명
 - 3.2.1 배포본 제작
 - 3.2.2 제품 보관
 - 3.2.3 제품 패키징 및 포장
 - 3.2.4 제품 배송
 - 3.3 TOE 배포절차 별 보안 유지 방안
 - 3.4 TOE 배포 버전 추적 방법
4. 기술지원

2.2. 배포절차서 작성 시 고려사항

배포절차서는 TOE를 사용자에게 배포할 때 TOE 보안유지를 위한 모든 절차를 포함한다. TOE 또는 TOE 일부 구성요소의 전달 과정 중 TOE의 보안을 유지하고 TOE를 식별하기 위한 적절한 절차를 서술하며 전체 TOE를 다루도록 권고되지만 TOE의 서로 다른 부분에 대해서 서로 다른 배포 절차를 포함할 수 있다. 즉 제품의 버그 수정 등을 통해 온라인 업데이트 하는 등 TOE일부에 대한 배포절차도 본 배포절차서에 기술되어야 하며 안전한 배포절차 수립이 필요하다.

배포 절차는 생산 환경에서 설치 환경(예 : 패키지, 저장 및 배포)까지 모든 배포 단계에 걸쳐 적용되어야 한다. 패키지와 배포에 대한 표준적인 상용 방식이 수용될 수 있다. 상용 방식으로 수축포장 패키지, 보안테이프 또는 봉인된 봉투 등이 있다. 배포를 위해서는 물리적(예 : 공공 우편 또는 민간 물류 서비스) 또는 전자적(예 : 이메일 또는 인터넷으로부터 다운로드) 절차가 사용될 수 있다.

변조나 위장을 탐지하기 위하여 개발자는 암호학적 체크섬이나 소프트웨어 서명을 사용할 수 있다. 변조 방지 봉인은 부가적으로 비밀성의 손상 여부를 알려준다. 소프트웨어 TOE의 경우 암호화 방법을 사용하여 비밀성을 보장할 수 있다. 가용성이 주요 관심 대상인 경우 보안 전송이 요구될 수 있다.

“보안 유지에 필요한”이라는 요구를 만족하기 위해서는 다음과 같은 사항을 고려할 필요가 있다.

- TOE의 특성(예 : TOE가 소프트웨어 또는 하드웨어인지 여부)
- 선택된 취약성 평가 수준에 따라 TOE에 요구되는 전반적인 보안 수준. TOE가 의도된 환경에서 특정 잠재적 공격에 대한 내성이 요구되는 경우 이는 또한 TOE의 배포에도 적용되도록 권고된다.
- 보안목표명세서에 의해 제공되는 보안 목적. 특히 실제 TOE와 연관되는 보안 관점(무결성, 비밀성, 가용성)은 보안목표명세서상에 정의된 개발환경에 대한 보안 목적에서 유도되도록 권고된다. TOE의 무결성을 유지하는 것은 항상 중요하기 때문에 무결성과 관련된 대책이 배포 문서에서 강조될 수 있다. 하지만 일부 TOE의 배포에 있어서는 비밀성과 가용성이 주요 관심의 대상이 될 수 있다. 안전한 배포의 이런 측면들과 관련된 절차 또한 배포 절차 내에서 논의되도록 권고된다.

2.3. 개발환경 보안점검 목록을 고려하여 작성

다음은 평가자가 국내용 EAL2 개발환경 보안 점검을 실시할 때 배포 측면에서 점검해야 하는 개발환경 보안점검 목록이다. 배포절차서에서는 다음 개발환경 보안점검 목록을 고려하여 해당 내용에 대한 절차와 기술적 방안이 배포절차서에 포함되도록 작성하는 것을 권고한다.

- ① 배포하는 동안 TOE의 보안을 유지하기 위한 절차는 무엇인가?
- ② TOE 배포 시 고려해야 하는 보안성은 무엇인가?

- ③ TOE를 배포하는 동안 TOE 무결성을 유지하기 위한 기술적인 방법은 무엇인가?
- ④ 배포되어야 하는 버전의 TOE 만이 배포됨을 보장하는 방법은 무엇인가?
- ⑤ 개발자의 마스트 복사본과 사용자 측에서 수령한 버전간의 불일치를 탐지하는 방법은 무엇인가?

3. 배포절차서 작성방법 및 예시

배포절차서는 작성 시 필요 사항은 다음과 같으며 작성 완료시 다음 내용이 준비절차서 내에 모두 포함되어야 한다.

☞ 배포 문서는 전체 TOE를 다루도록 권고되지만 TOE의 서로 다른 부분에 대해서 서로 다른 배포 절차를 포함

구분	작성 내용
1	배포문서는 TOE를 소비자에게 배포할 때 보안을 유지하기 위해 필요한 모든 절차를 서술한다.

3.1. 배포절차서 참조

☞ 배포절차서식별을 명확하게 할 수 있도록 문서명, 문서 버전 등 배포절차서에 대한 식별정보 서술

문서명	OOO 배포절차서
문서버전	XX
파일명	신청대상제품명-문서명-버전-날짜(세부버전 등).hwp
작성자	(주) XXX
발간일	20XX.XX.XX

참고사항

- ▶ 정보보호제품 평가인증(CC인증) 제도의 국내용 정보보호제품 평가·인증 스킴에 따라 배포절차서는 신청인 자체문서(내규, 보안지침 등)로 대체 제출 가능하다.
- ▶ 신규로 제출물을 작성하는 경우 배포절차서 작성자는 본 가이드를 참고하여 배포절차서를 작성할 수 있다.

3.2. 배포절차서 목적

☞ 배포절차서는 TOE를 사용자에게 배포할 때 TOE 보안 유지를 위한 모든 절차가 서술

예: 배포절차서는 사용자에게 TOE가 변경 없는 상태로 전달되는 것을 보증하기 위한 시스템 통제와 배포 시설 및 절차를 기술한다. 사용자가 수령한 버전이 TOE 원본과 정확하게 일치할 수 있도록, 실제 버전이 변경되거나 잘못된 버전으로 대치되는 것을 방지하기 위해 TOE 전달 과정에서 필요한 모든 절차를 서술한다.

3.3. 배포절차서 구성

☞ 배포절차서 전체 구성에 대해 서술

본 배포절차서는 다음과 같이 구성되어 있다.

1장은 배포절차서 개요로 참조, 목적, 구성, 용어 정의 등을 기술한다.

2장은 배포 환경 및 인력에 대하여 기술한다.

3장은 배포절차 및 보안유지 방안에 대하여 기술한다.

3.4. 용어 정의

☞ 배포절차서상에서 사용되는 용어에 대한 설명을 기술한다.

용어 설명에서는 배포절차서에서 사용된 전문용어나 특정용어에 대하여 설명한다.

예/:

- 매뉴얼 : 제품에 설치, 운영, 사용을 위한 설명 자료로 제품 설명서가 있음
- 매뉴얼 CD : 설치지침서, 관리자 설명서가 포함된 CD를 말함.
- 제품 CD : Security Product V1.0을 설치하기 위해 고객에게 전달되는 CD로 Manager와 Agent 설치 프로그램이 포함되어 있음.
- 라이선서 서버 : 고객에게 TOE 배포 시 제품 사용을 위한 라이선서를 발급하기 위한 시스템

3.5. 참조 문서

☞ 일반적으로 준비절차서 평가(ALC_DEL.1)에서 요구되는 입력문서를 참조로 한다.

- OOO V1.0 보안목표명세서 vX.X

3.6. TOE 배포 방법

☞ TOE 또는 TOE 구성요소에 대하여 생산환경에서 설치환경까지 배포 방식에 대하여 기술한다. 패키지화 배포에 대한 표준적인 상요 방식이 수용될 수 있다. 상용 방식으로 수축포장 패키지, 보안 테이크 또는 봉인된 봉투 등이 있다. 배포를 위해서는 물리적(예: 공공 우편 또는 민간 물류 서비스) 또는 전자적(예: 이메일 또는 인터넷으로부터 다운로드) 절차가 사용될 수 있다.

TOE 구성요소	형태	배포 방식
구성요소 명칭1	펌웨어	물리적 방식 : 전용 하드웨어 탑재 후 보안테이프로 박스 포장하여 엔지니어가 고객사로 직접 배송
구성요소 명칭2	소프트웨어	물리적 방식 : CD형태로 제작 후 보안테이프로 박스 포장하여 엔지니어가 고객사로 직접 배포
구성요소 명칭3	소프트웨어	전자적 방식 : 홈페이지를 통해 다운로드 형태로 배포(HTTPS)
설명서	운영설명서	물리적 방식 : CD형태로 제작 후 보안테이프로 박스 포장하여 엔지니어가 고객사로 직접 배포
	준비 절차서	물리적 방식 : CD형태로 제작 후 보안테이프로 박스 포장하여 엔지니어가 고객사로 직접 배포

3.7. 배포 인력 체계(옵션)

☞ 배포 단계에서 담당자를 명시하는 것은 필수 사항은 아니나 전반적으로 배포 단계를 명확하게 규정하고 운영하기 위해서는 배포 단계별 담당자를 배정할 필요가 있음.

구분	세부 절차	담당자
구매요청	영업담당자	
생산	배포본 제작	
	설치 이미지 제작	
	매뉴얼 제작	
	설치 CD 제작	
납품		기술지원 배포담당자
보관		

3.8. TOE 배포 절차 분석 및 도식화

☞ 배포절차를 작성하기 위해서는 우선 현재 개발사에서 제품을 개발하여 고객에서 인수되는 전체 과정에 대한 분석이 필요하다.

☞ 다음은 제품 개발 완료 시점부터 TOE 제작에서 하위 사용자에게 인수하는 과정까지의 배포 과정을 도식화 한 예이다. 개발사의 제작 환경, 제품의 특성 등에 따라 배포 과정은 상이할 수 있으며 개발사 배포 절차를 단계별로 서술하면 되며 배포절차 도식화도 배포 절차를 설명하기 위한 하나의 수단으로 필수적으로 요구되는 사항은 아니다.

다음은 TOE를 생산환경에서 설치환경(고객)까지 모든 배포 단계를 설명한다.



배포절차에 대한 상세 설명은 다음과 같다.

<배포 절차별 상세 설명 기술>

1) 배포본 제작

구분	세부 절차	단계 설명
제품 제작		

3.9. TOE 배포 절차별 보안 유지 방안

☞ TOE 배포 절차가 식별되면 배포 절차 세부 단계별 제품의 이동 경로를 따라 이동 또는 해당 단계에서 TOE와 연관되는 보안 관점(무결성, 비밀성, 가용성)을 식별하고 식별된 보안성을 유지하기 위한 방안과 절차를 기술한다.

☞ TOE를 배포하는 동안 TOE 무결성을 유지하기 위한 기술적이 방법이 있다면 기술한다. 기술적인 방법에는 암호화적 체크섬이나 소프트웨어 서명 기법 등이 사용될 수 있다.

구분	세부 절차	배포방법	보안을 유지하기 위한 방법
구매요청	영업담당자		

구분	세부 절차	배포방법	보안을 유지하기 위한 방법
생산	배포본 제작		
	설치 이미지 제작		
	매뉴얼 제작		
	설치 CD 제작		
납품			담당자는 제품 BOX의 봉인상태를 확인하고 납품확인서와 함께 직접 고객에게 전달
보관			

3.10. TOE 배포 버전 추적 방법

- ☞ 배포와 관련된 개발환경 보안점검 항목에는 1) 배포되어야 하는 버전의 TOE만이 배포됨을 보장하는 방법이 무엇인지 2) 개발자의 마스터 복사본과 사용자 측에서 수령한 버전간의 불일치를 탐지하는 방법에 대한 항목이 존재한다. 따라서, 해당 내용에 대한 배포하는 동안 TOE 보안유지 방법에 함께 포함되어 있다면 본 내용은 기술할 필요가 없다.
- ☞ 다음 내용은 배포 버전 관리 및 버전 불일치 탐지 방법의 예이며 다양한 방법이 존재할 수 있으며 제품의 특성 및 개발사 환경 등을 고려하여 관련 내용이 작성될 필요가 있다.

1) 배포되어야 하는 버전의 TOE만이 배포됨을 보장하는 방법

배포되어야 하는 버전의 TOE만이 배포됨을 보장하기 위해서 고객으로부터 제품 발주가 있는 경우 제품 납품 계약서상에 제공해야 하는 TOE명을 명확하게 기술한다.

<납품 계약서 예시>

납품계약서		
[매수인명](이하 "갑"이라 칭함)와 [매도인명](이하 "을"이라 칭함)는 "을"이 공급하는 제품(이하 "제품"이라 칭함)을 "갑"을 구매자로 하고 "을"이 공급자로 하여 아래와 같은 조건과 방법으로 거래할 것을 합의한다.		
제1조(발주내역)		
구분	내역	비고
품명	TOE 명칭과 버전을 정확하게 기술	
SPEC		
STYLE NO		
단가		
수량		
금액	[] (원)	
납기	20__년__월__일	
특기사항		
단, 상기 내역을 기본으로 하고 제품의 품종, 수량, 납기 등은 "갑"과 "을"의 상호 합의 하에 변경할 수 있다.		
제2조(원·부자재)		
["을"은 제품을 제조함에 있어서 "갑"의 생산지시서에 의한 원·부자재를 <u>자체 조달, 사용</u> 함을 원칙으로 하며, 포장자재 및 LABEL, TAG은 "갑"이 공급한다.]		
["을"이 제품을 제조함에 있어서 "갑"의 생산지시서에 의한 원·부자재는 " <u>갑"이 조달</u> 함을 원칙으로 하며, 포장자재 및 LABEL, TAG도 "갑"이 공급한다.]		
제3조(결판순위)		

패키지 담당자는 납품계약서 상에 명시된 TOE 버전만이 배포됨을 보장하기 위해 제조기록서를 작성하여 납품을 위해 제작된 TOE의 버전을 기록한다.

[illegible]

고객에게 직접 배포를 수행할 엔지니어는 고객사에 배포 전 납품계약서와 납품 될 제품의 버전을 확인한다. 직접 배송 업무를 수행하는 엔지니어에 의해 고객사에게 제품을 납품하고 납품 계약서에 명시된 TOE 버전과 같은 버전의 TOE가 고객에게 배송되었음을 확인하고 납품확인서에 고객의 서명을 진행한다.

납 품 확 인 서		DELIVERY CONFIRMATION	
상 호 명		상 호 명	
대표자명		대표자명	
사업자등록번호		연 락 처	
공 급		발	

납품계약서 번호 및

제작된 TOE 명칭과 버전을 기술

연 기	0	0
읍 · 도		

TOE 명칭/버전 확인 후

고객사 서명

일련자 : _____ (인)

2) 개발자의 마스터 복사본과 사용자 측에서 수령한 버전간의 불일치를 탐지하는 방법

개발자는 마스터 복사본 생성 시 마스터 복사본에 대하여 해시값을 생성하여 같이 제품을 등록한다. 개발사는 제품의 버전과 제품에 대한 해시값을 개발사 홈페이지를 통해 항상 공개하여 사용자 측에서 수령한 버전의 해시값을 확인하여 개발자의 마스터 복사본과 수령한 버전간의 불일치 여부를 탐지할 수 있다.



[부록 1] 배포절차서 작성 템플릿

Secure Product V1.0 (제품명)

배포절차서

V1.0 또는 Rev.0 (문서버전)

20○○ . ○○ . ○○

XXXX (회사명)

<제·개정 이력>

버 전	일 자	개정 내용
1.0	24-12-10	o Secure Product V1.0 배포절차서 V1.0 작성
1.1	24-12-30	o 관찰보고서 EOR-01 반영

1. 배포절차서 개요

☞ 개요부분에는 배포 문서에 대한 목적, 문서 식별정보, 문서 구성 정보 등을 기술한다.

- 목적, 배포문서 식별, 배포문서 구성, 작성 규칙, 용어 정의

1) 배포절차서 식별

☞ 배포절차서 식별정보 서술

배포절차서의 식별 정보는 다음과 같다.

문서명	000 배포절차서
문서버전	X.X
파일명	신청대상제품명-문서명-버전-날짜(세부버전 등).hwp
작성자	(주) XXX
발간일	20XX.XX.XX

2) 배포절차서 참조

☞ 배포절차서 목적 서술

배포절차서는 사용자에게 TOE가 변경 없는 상태로 전달되는 것을 보증하기 위한 시스템 통제와 배포 시설 및 절차를 기술한다. 사용자가 수령한 버전이 TOE 원본과 정확하게 일치할 수 있도록, 실제 버전이 변경되거나 잘못된 버전으로 대치되는 것을 방지하기 위해 TOE 전달 과정에서 필요한 모든 절차를 서술한다.

3) 배포절차서 구성

☞ 배포절차서 전체 구성에 대해 서술

본 배포절차서는 다음과 같이 구성되어 있다.

1장은 배포절차서 개요로 참조, 목적, 구성, 용어 정의 등을 기술한다.

2장은 배포 환경 및 인력에 대하여 기술한다.

3장은 배포절차 및 보안유지 방안에 대하여 기술한다.

4) 용어 정의

☞ 배포절차서상에서 사용되는 용어에 대한 설명을 기술

용어 설명에서는 배포절차서에서 사용된 전문용어나 특정용어에 대하여 설명한다.

- 매뉴얼 : 제품에 설치, 운영, 사용을 위한 설명 자료로 제품 설명서가 있음
- 제품 CD : Security Product V1.0을 설치하기 위해 고객에게 전달되는 CD로 Manager와 Agent 설치 프로그램이 포함되어 있음.
- 배포 서버

5) 참조 문서

☞ 일반적으로 준비절차서 평가(ALC_DEL.1)에서 요구되는 입력문서를 참조로 한다.

- OOO V1.0” 보안목표명세서 VX.X

2. TOE 배포 방법 및 인력체계

1) 배포 업무 규정

제품 관련 업무는 제품별로 구분되며 제품별 관리 업무는 제품 제작, 제품 배포, 기술지원 등의 업무로 나누어진다.

..... [중략].....

2) 배포 인력 체계

배포 단계 별 관리 책임자를 임명하고 제품배포 책임자는 제작, 배포, 기술지원 등에 대한 책임자 및 담당자를 임명한다.

기술지원본부 제품 관련 업무는 다음과 같이 직무를 분리·운영한다.

구분	역할	담당자	직무
구매요청	영업담당자	영업팀원	
제작	배포본 제작 담당자		
	설치 이미지 담당자		
	매뉴얼 담당자		
	설치 CD 제작	'~~'(외부조직)	
납품		기술지원 배포담당자	
보관			

..... [중략].....

3. TOE 배포절차 및 보안 유지 방안

☞ 배포 절차는

- 개발자에 의해 만들어진 Master CD/매뉴얼 등이 공장으로 전달되어 대량 생산되고,
- 생산된 TOE 및 TOE의 일부가 사용자에게 전달되는 모든 과정이 실제 적용 가능해야 한다.

3.1 TOE 배포 절차 분석 및 도식화



3.2 배포 단계별 설명

1) 배포본 제작

가) 제품 제작 체계

☞ 설치 이미지를 외부 CD 제작 업체로 전달할 경우 보안 수단을 서술해야 함

설치 이미지는 마스터 CD로 제작되며 배포본 제작 담당자가 직접 외부 CD 제작 업체로 전달하여 불법적인 노출 및 변경으로부터 방지한다. 외부 제작 업체에 대해서는 보안서약서를 작성하고 보안서약서 내에는 보안유지에 대한 항목을 포함한다.

..... [중략].....

나) 지침서 인쇄

☞ 매뉴얼 파일을 외부 제작 업체로 전달할 경우 보안 수단을 서술해야 함

매뉴얼 파일을 전송 시 암호화 한 후 e-mail로 전송한다. 암호는 유선상으로 공유한다.

..... [중략].....

다) 배포 TOE 포장

☞ 최종 제품 패키지가 고객에게 전송될 때 불법적인 변경 및 노출로부터 보호하는 방법

- 보안 테이핑, 봉인, 수출포장 패키징

배포본 제작 담당자는 설치 CD와 매뉴얼을 제품 박스에 담은 후 보안테이프를 붙인다.

납품확인서와 제품 박스를 배포 담당자에게 전달한다.

[보안테이프 예시]

[패키지 박스 예시]

..... [중략].....

2) 재고 관리

☞ 재고 관리

- 시건 장치가 있는 장소에 보관
- 담당자만 접근 가능해야 함

3.3 TOE 배포 절차별 보안 유지 방안

TOE 배포 절차가 식별되면 배포 절차 세부 단계별 제품의 이동 경로를 따라 이동 또는 해당 단계에서 TOE와 연관되는 보안 관점(무결성, 비밀성, 가용성)을 식별하고 식별된 보안성을 유지하기 위한 방안과 절차를 기술한다.

구분	세부 절차	배포방법	보안을 유지하기 위한 방법
구매요청	영업담당자		
생산	배포본 제작		
	설치 이미지 제작		
	매뉴얼 제작		
	설치 CD 제작		
납품			담당자는 제품 BOX의 봉인상태를 확인하고 납품확인서와 함께 직접 고객에게 전달
보관			

3.4 TOE 배포 버전 추적 방법

1) 배포되어야 하는 버전의 TOE만이 배포됨을 보장하는 방법

배포되어야 하는 버전의 TOE만이 배포됨을 보장하기 위해서 고객으로부터 제품 발주가 있는 경우 제품 납품 계약서상에 제공해야 하는 TOE명을 명확하게 기술한다.

<납품 계약서 예시>

납품계약서		
[매수인명][이하 "갑"이라 칭함]와 [매도인명][이하 "을"이라 칭함]는 "을"이 공급하는 제품(이하 "제품"이라 칭함)을 "갑"을 구매자로 하고 "을"이 공급자로 하여 아래와 같은 조건과 방법으로 거래할 것을 합의한다.		
제1조(발주내역)		
구분	내역	비고
품명	TOE 명칭과 버전을 정확하게 기술	
SPEC		
STYLE		
단가		
수량		
금액	[] (원)	
납기	20__년 __월 __일	
특기사항		
단, 상기 내역을 기본으로 하고 제품의 품종, 수량, 납기 등은 "갑"과 "을"의 상호 합의 하에 변경할 수 있다.		
제2조(원-부자재)		
["을"은 제품을 제조함에 있어서 "갑"의 생산지시서에 의한 원-부자재를 자체 조달, 사용함을 원칙으로 하며, 포장지재 및 LABEL, TAG은 "갑"이 공급한다.]		
["을"이 제품을 제조함에 있어서 "갑"의 생산지시서에 의한 원-부자재는 "갑"이 조달함을 원칙으로 하며, 포장지재 및 LABEL, TAG도 "갑"이 공급한다.]		
제3조(계좌입금)		

패키지 담당자는 납품계약서 상에 명시된 TOE 버전만이 배포됨을 보장하기 위해 제조기록서를 작성하여 납품을 위해 제작된 TOE의 버전을 기록한다.

[illegible]

고객에게 직접 배포를 수행할 엔지니어는 고객사에 배포 전 납품계약서와 납품 될 제품의 버전을 확인한다. 직접 배송 업무를 수행하는 엔지니어에 의해 고객사에게 제품을 납품하고 납품 계약서에 명시된 TOE 버전과 같은 버전의 TOE가 고객에게 배송되었음을 확인하고 납품확인서에 고객의 서명을 진행한다.

납 품 확 인 서 DELIVERY CONFIRMATION			
영 주 법 대표자명 공 사일지출금입금		상 호 법 대표자명 금 입 격 서	
납품계약서에 명시된 TOE명칭/버전 과 납품된 TOE 명칭/버전을 확인한 후 작성			
총 계		0	0
합 도			
위와 같이 납품확인서를 제출합니다.			
TOE 명칭/버전 확인 후 고객사 서명		담당자 : _____ (인)	

2) 개발자의 마스터 복사본과 사용자 측에서 수령한 버전간의 불일치를 탐지하는 방법

개발자는 마스터 복사본 생성 시 마스터 복사본에 대하여 해시값을 생성하여 같이 제품을 등록한다. 개발사는 제품의 버전과 제품에 대한 해시값을 개발사 홈페이지를 통해 항상 공개하여 사용자 측에서 수령한 버전의 해시값을 확인하여 개발자의 마스터 복사본과 수령한 버전간의 불일치 여부를 탐지할 수 있다.



[부록 2] 배포절차서의 주요 관찰사항

1

평가자가 TOE 또는 TOE 일부를 소비자에게 배포할 때 보안을 유지하기 위해 필요한 모든 보안 유지 절차가 배포문서에 서술되어 있는지 확인하는 과정에서 다음과 같은 관찰사항이 주로 발견됨

- 1) TOE에 대한 구성요소 중 일부 구성요소에 대한 전달 과정에 대한 보안유지 절차가 누락되는 경우
- 2) 배포절차에는 생산환경에서 설치 환경까지 모든 배포 단계에 걸쳐 보안을 유지하는 방안이 고려되어야 하는 일부 단계(예: 외부 위탁 생산 과정)에 대한 절차가 누락되는 경우

2

평가자가 TOE 또는 TOE 일부에 대한 배포를 위해 고려되어야 하는 보안성을 확인하는 과정에서 다음과 같은 관찰사항이 발견됨.

- 1) 배포되는 TOE 구성요소의 특성 및 선택된 취약성 평가 수준에 따라 TOE에 요구되는 전반적인 보안 수준이 결정되어야 하나 보안특성 중 일부만 적용되어 보안 수준이 적절하게 적용되고 있지 않은 경우(예를 들어, 제품을 온라인 배포하는 경우 무결성에 대한 부분만 적용되고 비밀성에 대한 대책은 마련되지 않은 경우)

3

개발환경보안점검을 통해 배포절차서와 실제 배포과정의 동일성을 확인하는 과정에서 실제 이행이 절차서와 상이한 경우가 다수 발견됨

- 1) 배포과정에서 소비자에게 전달된 TOE가 평가된 TOE 버전과 정확하게 일치하는지 확인하기 위해 납품확인서를 이용하고 있으나 실제 납품확인서에 기록된 제품의 버전이 실제 납품된 TOE 버전과 상이한 경우
- 2) 제품 배포 과정에서 하드웨어 모델을 패키징하는 과정에서 제품의 훼손을 방지하기 위해 배포절차서 상에는 보안 라이선스 Seal을 부착한다고 되어 있으나 실제 제품을 확인한 결과 보안 라인선스 Seal이 부착되지 않은 경우