

개방형 OS 도입 가이드



개방형OS 도입 가이드



CONTENTS

개방형OS 도입 가이드

서 문

제1장	개방형OS 개요	5
	1. 추진배경 및 목적	6
	2. 개방형OS의 종류	8
	3. 개방형OS의 특징	9
제2장	개방형OS 도입 사례	11
	1. 국내 개방형OS 도입 사례	12
	2. 해외 개방형OS 도입 사례	13
제3장	개방형OS 도입 사전 검토사항	15
	1. 기존 업무환경 분석	17
	2. 도입 모델 검토	18
	2.1. 개별 설치 구성	18
	2.2. DaaS / VDI 구성	18
	3. 호환성 검토	22
	3.1. 하드웨어 호환성 검토	22
	3.2. 소프트웨어 호환성 검토	23
	3.3. 주요 웹서비스 호환성 검토	26
	4. 보안성 검토	28
	4.1. 검증 절차	28
	4.2. 제출 서류 및 제출물	29
	4.3. 제품 유형별 도입 기준	29
	5. 유지관리 검토	32

제4장	개방형OS 도입 사업추진 절차	33
	1. 사업계획.....	35
	1.1. 소요예산 산정.....	35
	1.2. 사업계획서 작성.....	36
	1.3. 사업자 선정·계약.....	36
	2. 사업수행.....	37
	3. 사업검사.....	38
	3.1. 업무 적합성 검사.....	38
	3.2. 라이선스 규정 준수 검사.....	38
	4. 사용자 교육.....	39
제5장	개방형OS 유지관리 프로세스	41
	1. 개방형OS 유지관리 서비스 개요.....	43
	2. 개방형OS 유지관리 서비스 내용.....	44
	3. 개방형OS 유지관리 서비스 적용방안.....	46
제6장	개방형OS 도입 가이드 활용	49
	1. 개방형OS 도입 시나리오.....	50
	2. 개방형OS 도입 가이드 활용.....	52



서 문

공개소프트웨어(FOSS: Free Open Source Software, 오픈소스 소프트웨어)는 낮은 획득비용, 개방형 표준 준수, 특정 기업에의 의존성 감소 등 다양한 사용자의 요구를 충족시키고 전 세계적으로 최신 기술을 선도하며 급격하게 성장하고 있다. 또한, 최근 국내에도 공개소프트웨어를 산업 전반에 효율적으로 수용하기 위한 다양한 정책이 시행되고 있다.

본 가이드에서는 공개소프트웨어 관련 정책 중 최근 국내에서 활발하게 논의되고 있는 개방형OS 확산 정책과 관련하여 개방형OS를 도입하고자 하는 기관의 이해를 높이고, 도입의 절차와 고려사항을 제시하였다.

전 세계적으로 국가 주도의 개방형OS의 도입 사례가 증가하고 있으며, 정책적 관점, 기술적 관점, 경제적 관점에서 다양한 연구가 진행되고 있지만, 국내에는 아직 개방형OS 도입을 위한 참고자료가 거의 없는 실정이다.

본 가이드가 개방형OS에 대한 이해를 돕고 개방형OS 도입의 검토 및 실행 과정에 유용한 자료로 활용될 수 있기를 희망한다.



제1장 개방형OS 개요

- 01 추진배경 및 목적
- 02 개방형OS의 종류
- 03 개방형OS의 특징



01 추진배경 및 목적

4차 산업혁명의 흐름과 함께 산업에서 소프트웨어의 중요성은 날이 갈수록 커지고 있으며 그 중에서도 공개소프트웨어의 중요성은 더욱 강조되고 있다. 최근의 한 보고에 의하면 90% 이상의 소프트웨어에서 공개소프트웨어가 사용되고 있으며 세계적으로 공개소프트웨어 개발자와 활용 조직은 연평균 80% 이상 성장하고 있다¹⁾.

이러한 흐름 속에서 정부에서도 국내 공개소프트웨어 산업의 활성화를 위한 정책을 추진 중이다. 특히 과학기술정보통신부와 정보통신산업진흥원은 공개소프트웨어 활성화 계획을 수립하고 공개소프트웨어 활성화를 위한 다양한 사업을 추진 중이다.

사업 초기에는 공개 소프트웨어의 산업기반을 마련하는 것부터 시작하였으나 최근 공개 소프트웨어 활성화 4차 기본계획에서는 국내 공개 소프트웨어 생태계 조성을 위한 사업을 진행 중이다.



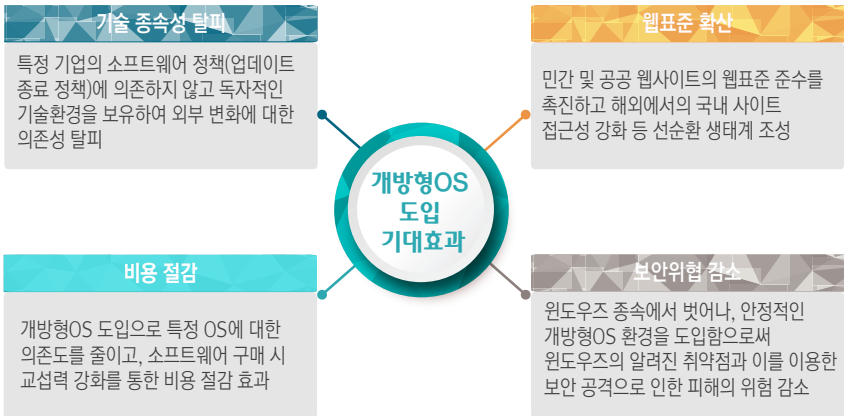
[과학기술정보통신부 공개SW 활성화 계획(1~4차) 요약(정보통신산업진흥원, 2018)]

1) 글로벌 오픈소스(공개SW) 생태계와 주요국 정책 (소프트웨어정책연구소, 2020.11)

다양한 산업 분야에서 공개소프트웨어는 널리 활용되고 있으나 그 중에서도 운영체제 분야의 공개소프트웨어는 성숙 단계로 리눅스 기반의 다양한 운영체제가 세계적으로 이미 널리 사용되고 있다. 그러나 국내에서는 특정 제품의 비율이 과도하게 높아 소프트웨어 시장 전체가 특정 기업에 종속되어 있는 실정이다.

이에 정부는 디지털 정부혁신추진계획('19, 관계부처합동) 발표 및 개방형OS 개발 및 확산을 위한 사업추진 등을 통하여 특정 운영체제의 종속을 탈피하고 개방형OS를 확산하는 정책을 추진 중이다. 특히 공공기관 개방형OS 선도 도입을 위한 사업을 과학기술정보통신부 및 행정안전부 중심으로 추진 중이다.

공공기관을 시작으로 국내 운영체제 시장에 개방형OS가 확산되면 특정 기업에의 기술 종속성을 탈피하고 비용을 절감할 수 있을 뿐 아니라 웹표준 기반의 생태계 조성, 보안 위협 감소 등의 효과가 기대된다.



[개방형OS 도입 기대효과]

02 개방형OS의 종류

개방형OS의 종류는 매우 많아 본 문서에서 모두 나열할 수는 없으나 지금까지 국내 공공기관에서 주로 도입된 개방형OS에는 하모니카OS, 한컴구름OS, 티맥스OS가 있다.

하모니카OS

하모니카OS는 리눅스 민트 배포판을 기반으로 2014년 미래창조과학부(現 과학기술정보통신부)와 정보통신산업진흥원(NIPA)의 지원사업을 통해 개발되었으며 현재는 (주)인베숨에 의해 개발 및 관리되고 있다.



한컴구름OS

과학기술정보통신부와 국가보안기술연구소는 2015년부터 보안을 강화한 개방형 OS인 구름OS를 개발하였다. 한컴구름OS는 이러한 구름OS를 기반으로 한글과컴퓨터의 오피스 제품과 개발 노하우를 더해 만들어진 OS이다.



티맥스OS

하모니카OS, 한컴구름OS와 달리 민간주도의 티맥스OS를 개발하고 기업용의 EE 버전과 개방형인 OE버전을 구분하여 운영하였으나 최근에는(2021년 6월) 구름플랫폼 활성화 포럼에 가입하고 구름OS 기반의 티맥스구름OS 개발을 발표하였다.

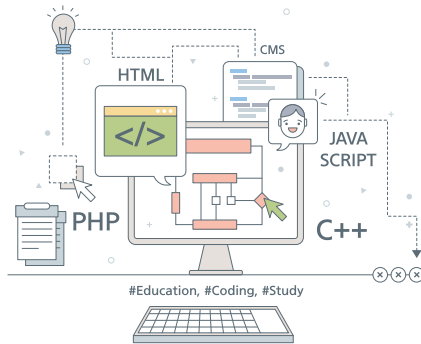


03 개방형OS의 특징

OS는 크게 소스코드가 공개되어 있지 않은 MS윈도우와 같은 폐쇄형OS와 소스코드가 공개된 개방형OS로 구분할 수 있다. 이 중 개방형OS는 소스 코드가 공개 되어 있어 누구나 원하는대로 소프트웨어의 개작과 파생 저작물의 생성이 가능하다는 특징이 있다.

[폐쇄형OS와 개방형OS의 비교]

구분	폐쇄형OS	개방형OS
소스 코드	바이너리 형태로 소프트웨어를 공급하므로 소스 코드 확인 불가능	소스 코드를 공개하여 누구나 확인 가능
라이선스 비용	사용 시 라이선스 비용 부과 (라이선스+서비스 비용)	라이선스 비용 부과 없음 (필요시 서비스 비용 부과)
지속성	최초 공급사의 정책 변경 또는 문제 발생 시 도입 고객에게 심각한 영향 미침	동일 솔루션에 대한 다수의 업체로부터 지원 및 공급이 가능하고 사용자의 선택권이 넓음





제2장 개방형OS 도입 사례

- 01 국내 개방형OS 도입 사례
- 02 해외 개방형OS 도입 사례



01 국내 개방형OS 도입 사례

국내에서는 윈도우XP 기술지원 종료와 함께 정부 주도로 개방형OS의 도입이 추진되면서 다년간 개방형OS의 보급 가능성이 검토되었다. 최근에는 행정안전부, 과학기술정보통신부, 우정사업본부, 국방부 등 여러 공공기관을 중심으로 개방형OS를 도입하기 시작하였다.

[국내 개방형OS 도입 사례]

대상기관	구축 내용
과학기술 정보통신부	<ul style="list-style-type: none"> · 사업명 : 과기정통부 개방형OS 시범 적용 · 수행 기간 : 2020년 06월 ~ 2020년 12월 · 도입OS : 한컴구름OS, 하모니카OS, 티맥스OS · 주요내용 : 디지털정부혁신 추진계획 및 5G 정부업무망 시범적용 등에 따라 인터넷PC의 개방형OS 도입 시범 운영
우정사업 본부	<ul style="list-style-type: none"> · 사업명 : 클라우드 기반 인터넷 망분리 서비스 도입 · 수행 기간 : 2019년 6월 1일 ~ 2019년 11월 30일 (서비스 환경 구축 및 시범 운영), 2019년 12월 1일 ~ 2024년 11월 30일 (서비스 기간 5년) · 도입OS : 한컴구름OS, 티맥스OS · 주요내용 : 별도 인터넷PC 없이 업무용PC에서 DaaS 기반 가상화 솔루션을 통해 외부 인터넷 접속이 가능하도록 구현
경찰청	<ul style="list-style-type: none"> · 사업명 : 재난안전통신망 전환을 위한 치안 업무용 무선시스템 구축 · 수행 기간 : 2019년 8월 ~ 2020년 12월 · 도입OS : 한컴구름OS · 주요내용 : 재난안전통신망 단말기에 개방형OS 구름플랫폼 적용하여 3,000여대 운용
국방전산 정보원	<ul style="list-style-type: none"> · 사업명 : 사이버지식정보방 클라우드 컴퓨팅 환경개선 사업 · 수행 기간 : 2019년 05월 ~ 2019년 12월 (구축 사업) 2020년 (무상하자보수), 2021년(연단위 유지관리 계약) · 도입OS : 하모니카OS · 주요내용 : 육, 해, 공 각 군부대 사이버지식정보방 약 3,000개소 인터넷용 PC 12,500대 대상 하모니카OS 도입
건강보험 공단	<ul style="list-style-type: none"> · 사업명 : 건강보험공단 재택근무 등 클라우드 기반환경 확대 구축 사업 · 수행기간 : 2021.06.30 ~ 2021.10.30 · 도입 OS : 티맥스구름OS V2.3 · 주요내용 : 가상 인터넷PC 환경 클라우드 확대구축으로 멀티OS 환경의 인터넷 서비스 구성 및 개방형OS 추가도입

02 해외 개방형OS 도입 사례

글로벌 동향을 보면 많은 국가에서 개방형OS 도입을 위한 노력 중이며, 현재 많은 국가에서 다양한 개방형OS를 사용하고 있다.²⁾ 이 중 주목할 만한 사례들은 다음과 같다.

[해외 개방형OS 도입 사례]

국가	구축 기관	구축 내용
영국	런던 구위원회 (Hackney)	· COVID-19 전염병 기간 동안 재택 근무 환경을 위해 4,000명의 직원이 리눅스 노트북 사용
스페인	바르셀로나 시	· 2018년 시 의회 컴퓨터 1,000대에 우분투를 설치하여 시범운영을 통해 안정성 등을 평가 · 2019년 모든 데스크톱 소프트웨어를 오픈소스로 대체하기로 하여 독점 운영체제에서 리눅스로 점진적으로 전환 추진
네덜란드	경찰	· 인터넷 조사/조사 네트워크(iRN)는 203년부터 감시 목적을 위해 인터넷에서 공개된 소스코드를 사용하여 2003년부터 공개적으로 개발된 개방형 표준 기반의 오픈소스를 사용하여 2,200대 우분투 워크스테이션을 사용
프랑스	경찰	· 2007년 윈도우 비스타 전환에 따른 추가 비용 문제로 인해 9만 대의 윈도우 XP PC를 우분투로 전환하여 2004년 ~ 2008년 동안 라이선스 비용을 약 5천만 유로 절감
마케도니아	교육과학부	· 2007년, 18만 대 이상의 우분투 기반 교실 데스크톱을 배치 · 북마케도니아 공화국의 모든 학생들에게 우분투 컴퓨터 워크스테이션을 사용하도록 권장
러시아	보건부, 국방부	· 2014년 크림반도 합병으로 인한 대 러시아 제재에 맞춰, 마이크로소프트 (MS) 등 미국 기업을 견제하는 수단으로 자국 보건부 시스템을 리눅스로 전환하는 계획 발표 · 2018년 “특별한 중요성”으로 분류된 데이터를 처리할 수 있는 인증된 운영체제인 아스트라 리눅스를 군사용 컴퓨터 시스템에 채택

2) https://en.wikipedia.org/wiki/List_of_Linux_adopters 참고

국가	구축 기관	구축 내용
스위스	교육기관	<ul style="list-style-type: none"> • 제네바에 있는 모든 초등학교와 중학교는 2013년 - 2014년에 교사와 학생이 사용하는 PC를 우분투로 전환 계획 • 2014년 70개의 공립 초등학교의 2,000대 이상 컴퓨터 전환 완료
중국	정부	<ul style="list-style-type: none"> • 2006년 자국 산업 지원 계획의 일환으로 150만 대의 리눅스PC 구입 • 2009년부터 론슨 프로세서를 이용한 리눅스PC를 시골 학교에 15만대 설치 • 2018년 중국 “정부 구매 PC, 중국산 리눅스 탑재 의무화“
인도	정부	<ul style="list-style-type: none"> • 2010년, 학생용 태블릿 1500루피(한화 약 3만원)이하의 태블릿 PC를 생산하기 위해 리눅스를 운영체제로 채택 • 2008년 타밀나두주는 리눅스 노트북 10만 대를 학생들에게 보급하였고, 2650개 공공기관과 정부가 지원하는 고등학교를 시작으로 리눅스 플랫폼에서 실행되는 무료 소프트웨어만을 사용할 것이라고 발표 • 2014년 윈도우 XP 지원 중단으로 지방 정부와 각 부처에서 오픈소스로 전환 추진





제3장 개방형OS 도입 사전 검토사항

- 01 기존 업무환경 분석
- 02 도입 모델 검토
- 03 호환성 검토
- 04 보안성 검토
- 05 유지관리 검토



개방형 OS의 성공적 도입을 위해서는 해당 기관의 개방형 OS 도입 가능 여부 및 개방형 OS 도입에 따른 리스크를 사전에 파악하는 것이 중요하다. 따라서 본 장에서는 개방형 OS의 도입 이전에 검토해야 할 사항에 대하여 기술한다.

본 장에서 기술된 사항은 개방형 OS를 도입하고자 하는 기관에서 자체적으로 수행할 수도 있으나 ISP를 위한 별도 컨설팅 기업에서 수행하는 것이 일반적이다.



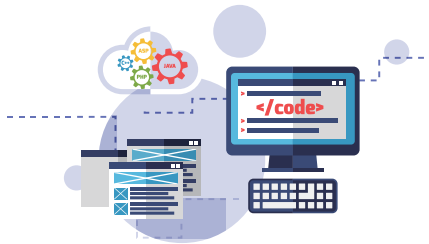
01 기존 업무환경 분석

기존 업무환경 분석은 대상 시스템의 소프트웨어 사용 현황, 기능 및 품질, 서비스 특성, 기타 요구 사항 등에 대한 현황 파악을 위한 과정이다.

파악 대상 항목은 시스템을 구성하고 있는 어플리케이션과 서비스뿐 아니라 관련 OA장비 등의 하드웨어까지 포함하며 이는 자산 관리 현황, 프로그램 내역서, 유지보수 비용 분석 등을 통하여 파악할 수 있다.

[기존 업무환경 분석 예시]

구 분	주요내용
소프트웨어	<ul style="list-style-type: none">• 기존 윈도우 환경에서 사용되던 주요 소프트웨어 목록• 기능, 품질, 서비스 등 업무 필수 요구사항• 주요 웹사이트 및 필수 웹서비스 웹호환성 검토
하드웨어	<ul style="list-style-type: none">• 설치될 단말기 사양 및 리눅스 드라이버 지원 여부• OA 장비 등 주변기기 분석 및 드라이버 지원 여부
기타	<ul style="list-style-type: none">• 자산 관리 현황, 프로그램 내역서, 유지관리계약



02 도입 모델 검토

개방형OS 도입 모델은 기관의 사용 현황에 따라 달라질 수 있다. 각 모델 별 기능 항목과 도입 기관의 요건에 따른 커스터마이징 가능 범위 등을 고려하여 안을 제공하고 선정 모델별 예산안에 반영한다. 다음과 같이 개방형OS 도입 모델을 구분할 수 있다.

2.1 PC 운영체제 전환

개방형OS 도입 시 가장 우선적으로 고려할 수 있는 모델은 사용 중인 PC의 운영체제를 개방형OS로 전환하는 것이다.

현재 공공기관의 경우 보안 목적에 따라 내부망과 외부망이 구분되어 운영 중인 경우가 많다. 따라서 개방형OS 도입 기관의 현황에 따라 내부망과 외부망 PC의 운영체제 전부 또는 일부를 개방형OS로 전환 가능할 것이다.

[PC 운영체제 전환 구성 시 고려사항 및 장단점]

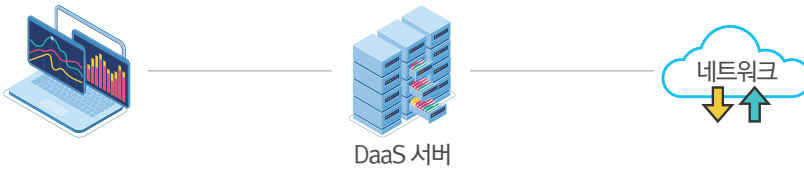
구 분	주요내용
주요 고려 사항	· 기존 윈도우 환경에서 사용되던 주요 소프트웨어의 개방형 OS와의 호환성 확보
장점	· 소프트웨어 호환성 확보이외 네트워크 구성 등 추가 고려사항이 적은 편 · 도입 구성 계획이 비교적 간단하다.
단점	· 개별 PC별 개방형OS 관리 필요 · 사용자 측면에서의 변화가 가장 큰 모델로 환경 변화에 따른 적응에 어려움이 있을 수 있음

2.2 DaaS / VDI³⁾

DaaS(Desktop as a Service)는 클라우드 구성 모델의 하나로 DaaS 자체는 개방형OS와 직접적 관련이 없다. 그러나 기관에서 개방형OS를 도입 시 DaaS를 활용하는 경우가 많으므로 본 절에서는 DaaS에 대하여 우선 기술한다.

3) 중앙행정기관 인터넷망 DaaS도입 가이드라인(2021.5, 행정안전부) 참고

DaaS 환경에서 PC는 사용자 작업을 위한 단말의 역할만을 수행하며 대부분의 작업은 DaaS 서버에서 수행된다. 따라서 사용자 입장에서는 단말의 운영체제 종류 및 단말의 성능에 따른 영향이 적으며 운영자의 입장에서는 운영 효율성이 높다.



[DaaS 모델 구성도]

DaaS 구성의 경우 Dedicated 방식과 Pooled 방식으로 구분된다. Dedicated 방식은 사용자별 단독 Desktop 환경을 제공하는 방식이며, Pooled 방식은 사용자가 접속할 때마다 초기 세션을 제공하는 방식이다. 따라서 Dedicated 방식의 경우 사용자 수 만큼의 자원 할당이 필요하며 Pooled 방식의 경우 사용자 수 보다 적은 수의 자원 할당으로 운영이 가능하다.

그러나 동시 접속자 수의 제한이 있을 수 있으며 DaaS 서버의 개인화 환경을 유지할 수 없다는 측면에서는 Dedicated 방식에 비해 단점이 존재한다. 따라서 기관의 상황에 따라 적절한 방식의 선택이 필요하다.

[DaaS 모델 고려사항 및 장단점]

구 분	주요내용
주요 고려사항	<ul style="list-style-type: none"> · DaaS 서버 직접 구축 여부, DaaS 서비스 방식(Dedicated, Pooled) 및 개방형OS 도입 범위(PC, 서버) 등
장점	<ul style="list-style-type: none"> · 구축 완료 이후 기관 내 개방형OS 확산(기관 내 미도입 부서 등)이 용이함 · 도입범위를 PC로 제한하는 경우 사용자의 작업 환경 변화가 매우 적음
단점	<ul style="list-style-type: none"> · 초기 도입 계획 수립 시 고려사항이 많음 · 서버구축 등에 따른 추가 비용이 발생할 수 있음

DaaS 모델을 이용하여 개방형OS를 도입하고자 하는 경우 우선적으로 고려하여야 하는 사항은 DaaS서버를 직접 구축할 것인지 여부이다. DaaS 서버를 직접 구축하는 경우 기관의 필요에 따라 구성이 가능하다는 장점이 있으나 서버를 직접 운영해야 한다는 단점이 있다. DaaS 서버의 직접 운영이 어려운 경우 DaaS 서비스를 제공하는 별도 클라우드 서비스를 이용할 수 있다. 일반적으로 서버를 직접 구축하여 운영하는 경우 DaaS와 구분하여 VDI로 칭한다.

내부 보안 정책 및 운영 프로세스에 따라 Public 클라우드 환경을 활용한 DaaS 서비스 제공과 Private한 내부 VDI 환경 구축을 통한 서비스 제공을 고려할 수 있다.

또한 DaaS 모델을 이용하는 경우, 개방형OS 도입 범위의 결정이 필요하다. 개방형OS가 도입될 수 있는 영역은 사용자 단말로 사용되는 PC와 DaaS 서버에서 제공되는 작업환경 두 가지가 있으며, 기관의 현황에 따라 둘 다 또는 하나에만 개방형OS를 도입할 수 있다.

[DaaS모델 개방형OS 도입범위별 특성]

도입범위	특 성
PC	<ul style="list-style-type: none"> 실제 사용자 작업 대부분은 DaaS서버에서 이루어지므로 개방형 OS 도입에 따라 사용자가 체감하는 영향이 매우 적음
개인별 작업환경 (DaaS)	<ul style="list-style-type: none"> 사용자 체감 영향은 개별 설치 구성과 동일하나 운영 측면에서 개별 설치 구성과 상이

참고 : 공공기관 개방형OS 도입모델 예시

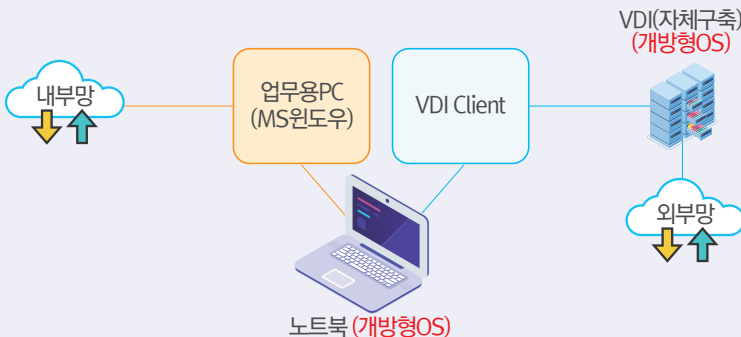
PC의 운영체제 전환 구성

기존 대부분의 공공기관은 1인 2PC(업무용, 인터넷용)를 운영 중이다. 업무용PC의 경우 MS윈도우와 호환성이 반드시 필요한 업무가 많으며 인터넷용PC의 경우 웹 작업이 주작업인 경우가 많으므로 호환성 이슈가 적은 인터넷PC에 한해 개방형OS를 우선 도입할 수 있다.



DaaS 구성

기존 1인 2PC 환경을 1인 1노트북 환경으로 전환함과 동시에 노트북에는 개방형OS를 설치하는 모델이다. 업무용은 윈도우VM을 활용하여 윈도우와 동일한 환경에서 업무를 수행할 수 있으며, 외부망 접속 시에는 자체구축한 VDI를 통하여 외부망에 접속할 수 있다.



03 호환성 검토

호환성 검토는 기존 업무환경 분석을 통해 파악된 소프트웨어, 서비스 및 주변기기 등이 개방형OS 환경에서 정상적으로 동작할 수 있는가를 여부를 검토하는 단계이다.

호환성 검토가 필요한 항목은 기관 마다 차이가 있지만 일반적으로 하드웨어, 소프트웨어, 웹사이트에 대한 호환성 검증이 필요하다.

3.1 하드웨어 호환성 검토

윈도우와 동일하게 개방형OS의 경우도 CPU, 기타 장치 드라이버(그래픽, NIC, USB, 모니터, 디스크, 프린터 등) 등에 따라 지원되지 않는 항목이 있을 수 있으며 각 업데이트(하드웨어, OS) 간에 호환성 충돌 이슈가 발생할 수 있다.

따라서 도입할 개방형OS 선정 시 하드웨어(PC 및 주변기기 등), 도입 모델(DaaS, VDI 모델 등)에 따라 개방형OS와의 호환성 문제에 대한 사전 검토가 필요하다.

[하드웨어 호환성 검토 예시]

- **(PC-OS 간 호환성)** 개방형OS와 일부 CPU는 서로 호환되지 않을 수 있다. 따라서 사전 검토 없이 PC를 구매 후 임의의 개방형OS 설치를 시도하는 경우 정상적인 설치가 불가능할 수 있다.
- **(OS-프린터 간 호환성)** 특정 기업의 특정 프린터 제품의 경우 개방형 OS 버전의 드라이버를 지원하지 않는 경우도 있다. 일반적으로 리눅스용 드라이버를 지원하는 경우 해당 드라이버가 정상적으로 동작하는지 검토해야 하며, 정상적으로 동작하지 않거나 리눅스용 드라이버를 지원하지 않는 경우 프린터 교체 등의 대안 마련이 필요하다.

3.2 소프트웨어 호환성 검토

기존 윈도우 환경에서 업무를 위해 사용되던 소프트웨어들이 있을 것이다. 윈도우에서 개방형OS로 전환 시 업무를 위해 사용되던 소프트웨어가 개방형OS 상에서도 정상적으로 사용이 되어야 한다.

만약 조직 내 소프트웨어 표준이 존재하는 경우에는 사용 중인 개별 소프트웨어 요구사항을 식별하고 개별 사용자의 소프트웨어 요구사항에 대한 기능 적합성 검토를 수행해야 한다. 일반적으로 대부분의 사용자 불만은 개별 사용자의 요구사항에 대한 불만족에서 출발하게 되므로 개방형OS 도입 시 새 운영체제에서 기존 사용자 환경의 프로그램이 지원되는지 확인하기 위해 제공되는 모든 소프트웨어 제품을 검증해야 한다.

검증 결과 주요 응용 프로그램이 개방형OS에서 지원되지 않는 경우 호환성 확보를 위한 방안을 마련해야 한다.

호환성 확보를 위한 첫 번째 방법은 유사한 서비스를 제공하는 타 소프트웨어로 변경하는 것이다. 만약 개방형OS를 지원하지 않는 특정 오피스 소프트웨어를 사용 중인 경우 개방형OS를 지원하는 리브레오피스, 오픈오피스 등으로 변경하거나 클라우드 버전을 사용하는 등의 대안을 선택할 수 있다.

두 번째 방법은 기존에 사용 중인 소프트웨어가 개방형OS를 지원하도록 개방형OS 또는 해당 어플리케이션 공급사 측에 변경을 요청하는 것이다. 관련 부분은 정보통신산업진흥원에서 운영 중인 OpenUp (오픈소스 소프트웨어 통합지원센터)에서 지원을 받을 수 있다.

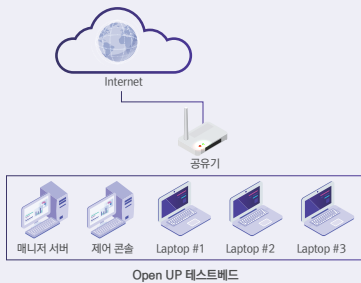
[소프트웨어 호환성 검토 예시]

① 필수 보안SW 분석 및 개방형OS 지원버전 검토

#	보안SW 현황 분석	개방형OS 지원 확인	개방형OS 지원 확인	개방형OS 지원 확인
1	백신	X	O	O
2	내PC지킴이	O	O	
3	매체제어	X	△	공급사 협의
4	접근제어	O	O	
5	출력물 보안	X	O	O
6	자료저장 방지	O	O	
7	망간 파일전송	O	O	

* 대체 가능 SW에 대한 호환성 검토는 NIPA의 OpenUp을 통해 지원 가능(www.oss.kr/open_oss)

② 호환성 검토 시스템 구성



③ 주요 기능 검증 목록 및 테스트

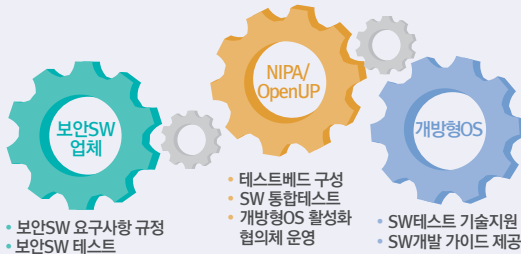
검증 기능	검증 항목
설치 및 삭제	명령어로 간단히 설치 및 삭제
업데이트	다양한 업데이트 조건 확인
백신 관리	실시간 관리 기능 제공
	제품 패치 제공
	다양한 검사 기능 제공
중앙관리	EPP를 통한 공통 정책 관리
편의 기능	다양한 편의 기능 제공
악성코드 탐지	다양한 형태의 악성코드를 탐지 삭제
성능	설치 후 성능 측정
안정성	재부팅 여부, 프로그램 간섭 여부
호환성	사내 프로그램 호환성 확인

* 시스템 구성 및 기능 검증 내용은 제품에 따라 다름

참고 : 오픈소스 소프트웨어 통합지원센터를 통한 개방형OS 호환성 확보

과학기술정보통신부와 정보통신산업진흥원은 오픈소스 소프트웨어 통합지원센터 운영을 통하여 개방형OS를 비롯한 공개SW의 활성화를 위한 서비스 정보 제공 및 커뮤니티 운영 등을 추진 중이다. 또한 개방형OS 공급사와 주요 공공 보안 소프트웨어 기업이 참여하는 개방형OS 활성화 커뮤니티를 운영 중으로, 개방형OS 및 공개SW 도입을 희망하는 기업/기관은 신청을 하면 관련 지원을 받을 수 있다.

- 오픈소스 소프트웨어 통합지원센터 : <https://www.oss.kr>
- 개방형OS 활성화 커뮤니티 : <https://github.com/Opensource-OS/ommunity>



1) 보안·응용 소프트웨어 기업

- 국정원 보안 요구 지침 사항을 기준으로 소프트웨어 품질 특성 및 이용 가능한 하부 특성들을 사용하여 요구사항을 규정한다.
- 보안SW의 기능성, 신뢰성, 사용성, 효율성, 유지보수성, 이식성 등의 테스트를 수행한다.

2) 오픈소스 소프트웨어 통합지원센터

- 개방형OS의 도입이 필요한 사이트의 보안소프트웨어 현황을 파악하여 테스트베드를 구성한다.
- 개발된 소프트웨어를 테스트베드에 순차적으로 설치하여 통합테스트를 수행한다.
- 이슈 발견 시 개방형OS 활성화 협의체를 통하여 해결한다.

3) 개방형OS 업체

- 각각의 소프트웨어의 테스트 및 통합테스트에 대한 기술을 지원한다.
- 개방형OS 호환을 위한 보안SW 개발 가이드를 제공한다.
- 신규 보안 취약점 및 호환성에 대한 패치를 지원한다.

3.3 주요 웹서비스 호환성 검토

내부 업무 및 외부 기관과의 업무 협업 기타 업무 등을 수행하기 위하여 필요한 주요 웹사이트 접속이 가능해야 하며, 관련 기능의 정상적 사용이 가능해야 한다.

따라서 우선 기관에서 내 외부 업무를 위하여 필수적으로 사용되는 웹사이트가 확인되어야 하며, 다음으로 해당 웹사이트에서 필수적으로 사용되는 서비스를 확인해야 한다.

확인된 웹사이트 및 서비스에 대하여 개방형OS 환경에서 정상 동작 여부가 확인되어야 하며, 정상 동작하지 않는 경우 그에 대한 대안이 필요하다.

웹사이트가 정상적으로 동작하지 않는 경우는 웹사이트 자체에서 개방형OS를 지원하지 않는 경우, 개방형OS에서 해당 웹사이트를 지원하지 않는 경우, 브라우저에서 해당 웹사이트를 지원하지 않는 경우가 있을 수 있다.

첫 번째로, 웹사이트에서 개방형OS를 지원하지 않는 경우는 해당 웹사이트가 윈도우 기반 플러그인으로 동작하는 경우가 대부분이다. 이에 대하여 정부는 공공 웹사이트에서 플러그인을 제거하는 정책을 꾸준히 추진 중이며, 지속적으로 상기한 문제를 개선하는 중이다.

차별 없는 공공 대민서비스의 관점에서도 주요 웹서비스의 호환성 확보는 매우 중요한 요소이므로 사업 담당자는 현재 호환성이 확보되지 않은 웹사이트에 대해 지속적으로 개선을 요청하고, 직접 구축하는 대민서비스 웹사이트에 대해서는 '공공 웹사이트 플러그인 제거 가이드라인(행정안전부, 2018)'을 참고하여 웹사이트 호환성을 확보하는 노력을 지속해야 한다.

두 번째로 개방형OS에서 해당 웹사이트를 지원하지 않는 경우라면 개방형OS 공급사를 통해 해당 문제를 검토해야 한다.

마지막으로 윈도우 환경에서도 브라우저에 따라 동작이 다른 웹사이트가 존재할 수 있듯이, 개방형OS에서도 브라우저에 따라 동작이 다를 수 있다. 자체 브라우저가 탑재된 개방형OS도 있으나 별도의 브라우저를 설치하여 동작을 확인하는 등의 절차가 필요하다.

[행정기관 홈페이지 및 인터넷뱅킹 호환성 검토 예시]

* 중앙행정기관 웹사이트 접속 가능 여부

부처명	접속사이트	접속 (O,X)	부처명	접속사이트	접속 (O,X)
고용노동부	www.moel.go.kr	O	법제처	www.moleg.go.kr	O
과학기술정보통신부	www.msit.go.kr	O	식품의약품안전처	www.mfds.go.kr	O
교육부	www.moe.go.kr	O	인사혁신처	www.mpm.go.kr	O
국방부	www.mnd.go.kr	O	검찰청	www.spo.go.kr	O
국토교통부	www.molit.go.kr	O	경찰청	www.police.go.kr	O
기획재정부	www.moef.go.kr	O	관세청	www.customs.go.kr	O
농림축산식품부	www.mafra.go.kr	O	국세청	www.hometax.go.kr	O
문화체육관광부	www.mcst.go.kr	O	기상청	www.weather.go.kr	O
법무부	www.moj.go.kr	O	농촌진흥청	www.rda.go.kr	O
보건복지부	www.mohw.go.kr	O	문화재청	www.cha.go.kr	O
산업통상자원부	www.motie.go.kr	O	방위사업청	www.dapa.go.kr	O
여성가족부	www.mogef.go.kr	O	병무청	www.mma.go.kr	O
외교부	www.mofa.go.kr	O	산림청	www.forest.go.kr	O
중소벤처기업부	www.mss.go.kr	O	새만금개발청	www.saemangeum.go.kr	O
통일부	www.unikorea.go.kr	O	소방청	www.nfa.go.kr	O
해양수산부	www.mof.go.kr	O	조달청	www.pps.go.kr	O
행정안전부	www.mois.go.kr	O	질병관리청	www.cdc.go.kr	O
환경부	www.me.go.kr	O	통계청	kostat.go.kr	O
국가보훈처	www.mpva.go.kr	O	특허청	www.kipo.go.kr	O
대통령경호처	www.pss.go.kr	O	해양경찰청	www.kcg.go.kr	O
민주평화통일자문회의사무처	www.nuac.go.kr	O	행정중심복합도시건설청	www.naacc.go.kr	O

* 국내 주요 은행 인터넷뱅킹 이용 가능 여부

은행명	접속사이트	보안프로그램	공인인증서 로그인
국민은행	www.kbstar.com	O	O
신한은행	www.shinhan.com	O	O
우리은행	www.wooribank.com	O	O
하나은행	www.kebhana.com	O	O

04 보안성 검토

보안성 검토는 각 기관에서 정보시스템, 소프트웨어 등을 도입하고 개발하는 사업을 진행할 시 보안취약점을 사전에 제거하고 보다 체계적인 보안 관리를 하기 위해 수행하는 일련의 과정을 뜻한다.

따라서 각 기관에서는 자체적인 보안대책을 수립하는 한편, 보안성이 중요한 정보시스템을 개발 및 구축할 경우, 보안성 검토 대상 여부를 확인한 후, 검토 대상일 경우 자체적으로 수립한 보안대책을 검증받기 위하여 검증기관에 검토를 요청해야 한다.

보안성 검토는 도입하고자 하는 시스템에 따라 세부내용에 차이가 있어 본 가이드에서는 개략적인 내용에 대해서만 언급하였으며, 세부적인 내용은 국가정보보호백서(2021, 국정원 등) 및 국가정보원 사이트의 보안 적합성 검증 관련 내용(https://www.nis.go.kr:4016/AF/1_7_2_2/list.do)을 참조할 수 있다.

4.1 검증 절차

국가·공공기관은 보안기능이 있는 도입 대상제품이 CC인증, 보안기능 확인서 등 사전 도입 요건을 만족했는지 확인한 후, 검증이 필요한 제품에 대해 국가정보원 또는 국가정보원이 지정한 검증기관(중앙행정기관 및 광역시·도, 광역시·도 교육청)에 보안적합성 검증을 신청한다.

검증기관은 국가보안기술연구소 또는 국가정보원장이 인정한 시험기관을 통하여 보안기능을 검증하고 그 결과를 신청기관에 통보한다. 신청기관은 검증과정에서 발견된 취약점에 대하여 개선 및 보안대책을 적용하고 미비점을 보완한 후 제품을 운용한다.

다만 아래의 경우에는 도입 후 보안적합성 검증 신청을 생략하고 운용 점검사항과 도입확인서, 인증서 사본 등을 제출하여 운용할 수 있다.

- ① 국가용 보안요구사항을 준수하여 국내용 CC인증을 받은 제품
- ② 국가정보원장이 승인한 국가용 보호프로파일(PP, Protection Profile)을 적용하여 국제용 CC인증을 받은 제품
- ③ 국가용 보안요구사항을 준용하여 보안기능 확인서를 받은 제품
- ④ 국가용 보안요구사항을 준수하여 성능평가 결과 확인서를 받은 제품
- ⑤ 국가용 보안요구사항을 준수하여 GS인증을 받은 제품

4.2 제출 서류 및 제출물

보안적합성 검증 신청은 최초 신청, 현상변경 등으로 인한 재검증 신청, 검증 생략제품 도입의 경우에 따라 아래의 서류를 검증 신청 공문과 함께 제출하여야 하며 개발 업체는 국가보안기술연구소가 안전성 시험을 위해 검증 대상 제품의 제출을 요청할 경우 5일(근무 일수 기준) 이내에 검증 신청제품과 동일한 제품을 국가보안기술연구소에 제출하여야 한다.

	최초 신청	재검증 신청 (형상변경 등)	검증 생략제품	비 고
보안적합성 검증신청서	0	0		
도입확인서	0	0	0	
기술 제안요청서	0			
보안기능 점검표	0	0		
운용점검사항	0	0	0	
변경내용 분석서		0		
CC인증서 사본	0		0	개발사
보안기능 운영 설명서	0		0	개발사
기본 및 상세 설계서	0			개발사
개발완료 보고서	0			개발사

4.3 제품 유형별 도입 기준

정보보호시스템 중 침입차단시스템·침입방지시스템 등 23종은 CC인증을 획득한 제품을 도입하여야 하며, CC인증 필수 제품 유형 중 가상사설망, 호스트기반 자료류출방지 제품은 국가정보원장이 승인한 검증필 암호모듈이 탑재되어야 한다.

국가용 보안요구사항 또는 국가용 보호프로파일을 준수한 경우 보안적합성 검증 신청 절차를 생략하여 도입하고 운용할 수 있다. 이를 준수하지 않은 경우 도입은 가능하지만 도입 후 보안적합성 검증 신청을 하여야 한다.

[CCC인증서를 보유해야만 도입이 가능한 제품]

제품유형	도입 요건	비 고
<ul style="list-style-type: none"> · 침입차단 시스템 · 침입방지 시스템(침입탐지 시스템 포함) · 통합보안관리 제품 · 웹 응용프로그램 침입차단 제품 · 서버 접근통제 제품 · 데이터베이스 접근통제 제품 · 네트워크 접근통제 제품 · 인터넷전화 보안 제품 · 무선 침입방지 시스템 · 무선랜 인증제품 · 가상화 제품 · 네트워크 자료유출 방지 제품 · 디지털 복합기(완전삭제 또는 데이터 암호화) · 스마트폰 보안관리 제품 · 디도스 대응장비 · 안티바이러스 제품 · 소스코드 보안약점 분석도구 · 스팸메일 차단 시스템 · 패치관리 시스템 · 망간 자료전송 제품 	CC인증	EAL 1 이상
<ul style="list-style-type: none"> · 가상사설망 제품 · 호스트 자료유출 방지 제품(매체제어 제품 포함) 	CC인증 및 검증필 암호모듈 탑재	EAL 1 이상
<ul style="list-style-type: none"> · 스마트카드 	CC인증	EAL 4 이상

출처 : 2021 국가정보보호백서

다만, 아래의 경우 검증 절차를 생략하고 도입 및 운용이 가능하다.

구 분	제품유형	비 고
GS인증	스팸메일 차단 시스템	한시적 (2021년 까지)
	팸메일 차단 시스템	
	팸메일 차단 시스템	
성능평가 결과 확인서	디도스 대응장비	
	안티바이러스 제품	
	소스코드 보안약점 분석도구	
보안기능 확인서	네트워크 장비	
	보안USB	
	가상화 관리	

출처 : 2021 국가정보보호백서

05 유지관리 검토

개방형OS 도입 시 도입 기관의 내부 인프라 운영 및 관리 현황을 고려하여 별도의 유지관리 서비스 계약을 검토하여야 한다.

기존의 내부 인프라 운영관리 부서의 경우 윈도우OS 기반의 소프트웨어에 대한 유지관리 프로세스로 업무가 이루어졌다고 한다면, 기존 유지관리 수준과 동일하게 개방형OS 기반의 각종 소프트웨어에 대한 유지관리 프로세스로 서비스 개선, 기술 지원 등의 유지관리 프로세스 정립이 필요하다.

개방형OS를 사용함에 있어 이후 발생할 수 있는 취약점, 버그, 장애 이슈에 대한 업데이트 등 인프라 운영 및 관리 업무 중의 발생 이슈에 대한 조치 프로세스 등을 고려하지 않는 경우 관련 이슈 대응에 어려움을 겪을 수 있다. 따라서 필수적으로 내부 관리 인력, 관련 제품 기술 지원 등의 별도 유지관리 서비스 계약을 검토하여야 한다.



제4장 개방형OS 도입 사업추진 절차

- 01 사업계획
- 02 사업수행
- 03 사업 검사
- 04 사업자 교육



개방형OS 도입 사업추진 절차는 일반적인 정보화사업 추진 절차와 크게 다르지 않다. 다만, 대부분의 구성원이 윈도우OS 환경에 익숙한 현실을 고려하여 개방형OS에 대한 사용자 교육 절차가 반드시 필요하다.

본 문서에서는 사업계획-사업수행-사업검사-사용자교육 단계로 구분하여 고려해야 할 주요한 사항에 대하여 기술하였다.



그림 2 개방형OS 도입 사업추진 절차



01 사업계획

1.1 소요예산 산정

개방형OS 도입의 총비용(TCO, Total Cost of Ownership)은 사전 검토 결과로 계획할 수 있는 도입 규모, 도입 모델 등의 구분과 도입 범위에 따라 기능적 요구사항, 시스템 환경, 기술지원 수준 등의 항목으로 다양한 유형의 예산안을 제공한다.

이 때 개방형OS, 보안소프트웨어, 업무용 소프트웨어 기준으로 호환성 확보에 필요한 추가 개발 비용을 고려해야 하며, As-Is 시스템에서 운영 중인 장비가 To-Be 시스템에서 활용 가능한지의 여부, 라이선스 정책, 유지보수 비용 등을 추가로 고려한 비용 산정이 필요하다.

[개방형OS 도입 비용 산정 항목]

		PC운영체제 전환	DaaS(클라우드)	VDI(구축)
서버구매		○ (매니저서버)	-	○ (VDI, 매니저서버)
라이선스	OS	○	○	○
	DaaS/VDI	-	○ (DaaS 서비스)	○ (VDI개발 포함)
	보안·응용 소프트웨어	○	○	○
설치, 교육, 유지보수		○	○	○

1.2 사업계획서 작성

사업계획서의 작성 시에는 본 가이드 3장 개방형OS 도입 사전 검토사항에 따른 검토 결과를 참고하여 사업계획서를 작성하여야 하며 사업목적 및 사업범위에 대한 정의가 필요하다.

우선 상호운용성 개선, 기술적용 계획, 예산절감 목적 등 개방형OS 활용 및 도입에 대한 목적에 따라 사업목적을 정의하고 개방형OS 도입 기관의 현황에 따라 도입하고자 하는 개방형OS 모델, 규모, 사업기간, 예산 등을 포함한 사업범위를 결정하여야 한다.

1.3 사업자 선정·계약

사업자 선정/계약을 위한 현황 진단을 통해 도출된 검토 항목, 도입 규모 및 범위에 따른 예산, 업무 프로세스 변경에 따른 리스크에 대한 기술 지원 수준 등을 고려하여 공급사와 공급 제품을 선정하여야 한다.

이 때 각 공급사별 검토 항목에 대한 증적 자료와 함께 개선 가능 범위 및 계획이 포함된 사업계획안을 각 사업 선정/계약 대상 공급사에 요청하여야 한다. 이를 통해 공급사와 공급 제품에 대한 평가를 실시하여 사업을 공정하게 수행할 수 있다.

02 사업수행

개방형OS 도입 검토가 완료되어 도입 규모, 도입 가능 여부가 확정되면 실 구축에 필요한 구축 계획 및 관련 협의가 필요하다.

선정된 개방형OS 기업, 소프트웨어 기업 등 관련 업무 담당자들 간에 실제 사전 검토 결과에 따른 실 구축 계획을 위한 협의를 주최한 후, 협의 결과에 따라 도입 규모를 확정한다.

또한 사용자 환경, 네트워크 환경 등의 도입 환경을 고려하여 일정 계획을 수립하고, 설치 프로세스를 정립한다.

도입 기업의 환경에 따라 계획 일정 및 설치 프로세스가 큰 차이가 있어 사업 수행 중 실무 담당자와의 협의회가 원활하게 이루어질 수 있도록 하여 발생하는 이슈에 대해 즉각적인 조치가 필요하다.

다음은 사업 수행 절차의 예로 실구축 계획-설치검증-연동검증-실구축-운영지원의 단계로 도입 환경 및 규모 등의 내용에 따라 일정을 관리하고 실구축 프로세스를 정립하여 사업 수행 중 이슈 발생을 최소화하여야 한다.

[사업 수행 절차 예시]

주요내용	일정	세부내용	비고
실구축 계획	0주	<ul style="list-style-type: none"> · 도입 규모 확정 · 대상 사용자, 사용자 계정, 네트워크 정보 확인 · 환경에 따른 설치 계획(회수, 설치, 배포) · 개방형OS, 보안소프트웨어 매니저 서버 구축 필요 여부 확인(반입 절차) 	
설치검증	0주	<ul style="list-style-type: none"> · 개방형OS 및 보안소프트웨어 설치 검증 · 설치 절차 매뉴얼 작업 	공급사/O대
연동검증	0주	<ul style="list-style-type: none"> · 실구축환경 네트워크 및 OS기기 연동 검증 · 매니저서버 통신 검증(매니저 서버 사전 구축 완료) 	실구축환경/ O대
실 구축	0주	<ul style="list-style-type: none"> · 주별00대 실구축(00주, 총000대) · 주차별 계획 	설치 및 운영 지원인력 상주 (0개사 00명, 0개월)
사전운영 지원	0주	<ul style="list-style-type: none"> · 개방형OS 및 보안소프트웨어 운영 기술지원(적합성 검사) · 관리 및 사용 교육 지원 	

03 사업 검수

개방형OS 도입 사업에서 필요한 검사항목은 현황 진단 단계에서 검토되었던 하드웨어 호환성, 소프트웨어 호환성, 주요 웹서비스 호환성 검사 등이 사용 환경 변경에 따른 업무 적합성을 충족 하는지 여부와 라이선스 규정 준수로 구분할 수 있다.

3.1 호환성 검사

개방형OS 도입 후 주요업무에 사용되는 응용 프로그램과 웹서비스 및 OA 기기 연동에 대한 검사를 수행한다. 다음은 도입 검토 기관의 보안 소프트웨어 및 업무용 소프트웨어 검사 리스트 예시이다.

[보안소프트웨어 및 업무용 소프트웨어항목 예시]

구분	소프트웨어 명
보안 분야	백신(PMS 포함), 내PC지키미, 매체제어(저장장치) 접근제어, 출력물 DRM, 인터넷 저장방지, 파일전송관리
장비 분야	PC-OFF
업무 분야	프린터 드라이버, GPKI 인증, NPKI 인증, 공직자 통합메일, 한글 뷰어, MS Office 뷰어, 리브레 오피스
웹사이트 접근	나라e음 영상회의, 국회방송, 연말정산(홈텍스), 일반 웹 접근

3.2 라이선스 규정 준수 검사

라이선스 규정에 따라 도입되는 개방형OS의 공개 소프트웨어 라이선스 준수 상태를 확인해야 한다. 이에 개방형OS 도입 사업 완료 시 공개소프트웨어 라이선스 검증보고서를 포함하여 제출하도록 개방형OS를 배포한 사업자에게 요구해야 한다. 라이선스 검증보고서 발급의 경우 오픈소스 소프트웨어 통합지원센터에서 무료로 지원하고 있다.

04 사용자 교육

개방형OS 도입 시 기존의 윈도우 사용자에게 익숙하지 않은 환경으로 업무를 함에 있어 해당 SW 및 서비스를 사용하는데 어려움이 있을 수 있다. 이에 업무 영향도를 고려하여 개방형OS 시스템 배포 절차를 진행하여야 하며 사용자 매뉴얼을 제공하고 관련 교육을 실시하여야 한다.





제5장 개방형OS 유지관리 프로세스

- 01 개방형OS 유지관리 서비스 개요
- 02 개방형OS 유지관리 서비스 내용
- 03 개방형OS 유지관리 서비스 적용 방안





도입이 완료되면 실제 사용자가 개방형OS를 사용하면서 정보시스템 담당자는 개방형OS 도입 시스템을 운영하게 된다.


기존 시스템과 동일하게 이슈를 해결할 수 있는 프로세스를 정립하고 관련 기술지원을 받을 수 있도록 하여야 한다. 또한 각 소프트웨어, 웹서비스 업데이트 등의 사용 환경적인 요소로 인한 이슈가 발생할 수 있음을 고려해야 한다.

01 개방형OS 유지관리 서비스 개요

개방형OS 도입 시 도입 기관의 내부 인프라 운영 및 관리 현황을 고려하여 별도의 유지관리 서비스 계약을 검토하여야 한다. 현재 개방형OS 유지관리 서비스를 위한 공공부문의 지침은 '소프트웨어사업 대가산정 가이드'이며, 다음과 같이 개방형OS의 유지관리 서비스를 정의한다.

 “공개소프트웨어 유지관리 서비스”는 공개 소프트웨어를 최적의 상태로 활용·유지하기 위한 기술지원 서비스를 의미한다.

 공개소프트웨어 도입 이후 운영에 필요한 기술지원 서비스를 제공하는 것으로 제품지원 (기능향상, 제품수정 및 업데이트), 유지관리(장애 지원, 예방지원 등), 컨설팅 등의 서비스가 포함한다.

 계약 기간과 유지관리 서비스 레벨(Service Level)의 조합에 의한 정액제 방식으로 계약을 체결하며, 공개소프트웨어 유지관리 서비스는 계약 기간 내에서 도입된 공개소프트웨어가 폐기 또는 변경되기 전까지 제공한다.(계약 기간과 시스템 수명주기의 불일치에 의한 기간 및 대가의 조정은 별도 약정)



02 개방형OS 유지관리 서비스 내용



개방형OS 유지관리비 대가 산정은 공개 소프트웨어의 특징을 고려하여, 공급받는 서비스에 대해 일정 금액을 대가로 지급하는 정액제 방식을 적용한다.



개방형OS는 대상의 유지관리 서비스 형태에 따라 아래와 같이 구분한다.

- **제품지원** : 특정 기업에서 공개 소프트웨어를 재구성하고, 일부 서비스를 추가하여 제품 형태로 제공하며, 구독료(subscription) 방식이 일반적이다.
- **기술지원** : 제품지원만 제공하거나, 커뮤니티 등에서 개발되는 공개 소프트웨어에 대해 기술지원(설치, 장애복구, 예방점검 등)을 전문으로 제공하는 기업의 서비스 형태이다.
- **제품 및 기술지원** : 제품지원 및 기술지원을 통합 일괄 제공하는 형태이다.



소프트웨어 사업 대가 산정 가이드 내 공개 소프트웨어 공급사 및 서비스 기업들이 제공하는 유지관리 서비스의 내용은 다음과 같다.

[공개SW 유지관리 서비스 항목]

구분	유지관리 서비스 항목		유지관리 서비스 내용
제품 지원	기능향상	메이저 기능향상	메이저 업그레이드 제품 제공 (예 : ver1.0 → ver2.0)
		마이너 기능향상	마이너 업그레이드 제품 제공 (예 : ver1.0 → ver1.1)
	제품 수정 및 업데이트	패치	보안 패치와 SW 제품의 버그 등 오류를 수정하는 업데이트 제공
	공개소프트웨어 라이선스 보증		공급한 제품의 계약기간 동안 공개소프트웨어 라이선스 (GPL, LGPL 등) 관련 법적 문제가 없다는 것을 보증
기술 지원	설치지원		설치 및 환경설정
	온라인 지원		고객지원 사이트 접속, 전화/이메일 등 원격 일상지원
	긴급 장애지원		사용자가 긴급한 문제를 해결하기 위해 장애처리 및 정비 서비스를 요청한 경우 고객을 지원
	예방지원		시스템 장애를 사전에 예방하기 위해 정기적으로 지원하는 정기점검 서비스
	교육		제품 운영 및 사용을 위한 운영자/사용자 교육
	성능 개선 및 튜닝		운영시스템의 성능 개선과 튜닝을 위한 전문 서비스

03 개방형OS 유지관리 서비스 적용 방안

개방형OS 유지관리 서비스는 계약 기간과 유지관리 서비스 수준(Service Level)에 따른 정액제 방식으로 대가를 산정하며, 대상 개방형OS 유지관리 유사거래 실제가격, 견적이 순으로 우선 적용한다. 공개소프트웨어 유지관리비 산정 절차는 다음과 같다.

[공개SW 유지관리비 산정 절차]

절차	주요내용	산출물
1. 사전준비	<ul style="list-style-type: none"> 유지관리 대상 공개소프트웨어를 식별한다. 	유지관리 대상 공개소프트웨어
↓		
2. 유지관리 서비스 수준 선택	<ul style="list-style-type: none"> 유지관리 대상 공개소프트웨어의 유지관리 서비스 항목을 참고하여, 서비스 수준을 선택한다. 	유지관리 서비스 수준
↓		
3. 유지관리 대가 산정방법 선택	<ul style="list-style-type: none"> 유지관리 대상 공개소프트웨어의 유사거래 실제가격, 견적이 순으로 우선 적용한다. 	유지관리 서비스 대가
↓		
4. 공개SW 유지관리비 산정	<ul style="list-style-type: none"> 공개소프트웨어 유지관리비를 산정한다. - 유지관리 서비스 적정가를 산정한다. 	공개소프트웨어 유지관리비

사전준비

유지관리 대상 공개 소프트웨어를 식별한다.

유지관리 서비스 항목 및 수준 선택

공개소프트웨어 유지관리 서비스 항목을 참고하여 개방형OS 서비스 기반으로 항목을 선정하고 유지관리 대상의 서비스 수준을 선택한다. 공개SW 유지관리 서비스 수준 등급 항목은 다음과 같다.

- **제품지원**: 선택 가능한 서비스 세부 항목 및 수준의 구분이 없으므로, 제품지원 서비스 여부만 선택한다.

- **기술지원**: 유지관리 서비스 항목과 아래 수준을 참고하여 기본, 표준, 고급 중 원하는 서비스 수준을 선택한다.
- **기본서비스**: 공개소프트웨어 제품을 도입해서 운영하기 위한 가장 기본적인 서비스 수준이다.
- **표준서비스**: 상시적 운영 이외 예방항목을 추가하여 보다 안정적인 서비스를 수행하기 위한 서비스 수준이다.
- **고급서비스**: 현장 방문을 통한 보다 질 높은 서비스 수준이다.

[공개SW 유지관리 서비스 수준 등급 항목]

구분	유지관리 서비스 항목		유지관리 서비스 수준*		
			기본	표준	고급
제품지원	기능향상	메이저	○	○	◎
		마이너	○	○	◎
	제품 수정 및 업데이트	패치	○	○	◎
	공개소프트웨어 라이선스 보증		○	○	○
기술지원	설치 및 환경설정		○	○	○
	온라인 지원		○	○	○
	긴급 장애지원		○	◎	◎
	예방지원		-	○	◎
	교육		-	◎	◎
	성능 개선 및 튜닝		-	-	◎

유지관리 대가 산정방법 선택

이전 단계의 유지관리 서비스 항목 및 수준 선택절차에 따라 유지관리 서비스 항목 및 수준을 참고하여, 해당 공개 소프트웨어에 대한 유지관리 서비스의 유사거래 실례가격, 3개 이상의 기업으로부터의 견적가 순으로 우선 적용하여 대가를 산정한다.



제6장 개방형OS 도입 가이드 활용

01. 개방형OS 도입 시나리오

02. 개방형OS 도입 가이드 활용



01 개방형OS 도입 시나리오

개방형OS 도입을 계획함에 있어 예산, 실무 사용환경 등을 고려한 실질적인 구축 계획의 수립이 중요하다.

다음 내용은 PC 운영체제 전환 모델 기준 개방형OS 도입 예시이다.

[개방형OS 도입 계획(예시)]

주요내용	일 정	세부내용
환경조사	2주	· 시범도입 규모 확정 · 사용자, 네트워크 등 환경조사
설치검증	2주	· 개방형OS 및 보안소프트웨어 설치 검증 · 설치 절차 매뉴얼 작업
연동검증	3주	· 실구축환경 네트워크 및 OS기기 연동 검증 · 매니저서버 통신 검증
실구축	14주	· 주별00대 실구축(총000대)
운영지원	6주	· 개방형OS 및 보안소프트웨어 운영 기술지원

[개방형OS 도입 월별 세부계획(예시)]

구분	세부항목	D+1월				D+2월				D+3월				D+4월				D+5월				D+6월				D+7월			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
환경 조사	도입 규모 확정	■																											
	환경 조사		■																										
설치 검증	설치			■																									
	설치 절차 매뉴얼 작업				■																								
연동 검증	매니저 서버					■																							
	개방형OS 설치						■																						
	보안소프트웨어 설치							■																					
	연동 검증								■																				
실 구축	개방형OS									■																			
	보안 소프트웨어										■																		
	사용자 통합 테스트(검사)																				■								
	사용자 교육																						■						
운영 지원																													
	운영 기술 지원																												

02 개방형OS 도입 가이드 활용

본 가이드에서 개방형OS 도입을 검토함에 있어 다양한 레퍼런스 모델 및 사례 등의 내용과 전체적인 사업 계획에 대한 가이드를 제시하였다. 이처럼 개방형OS 도입 확산을 위해 여러 기관 및 기업에서 다양한 레퍼런스 모델을 연구하여 시도 중이다.

본 가이드가 개방형OS를 도입하고자 하는 공공기관에 도움이 될 수 있기를 기대한다.

또한 과학기술정보통신부와 정보통신산업진흥원이 운영하는 오픈소스 소프트웨어 통합지원센터 (<https://www.oss.kr/>)에서는 개방형OS 도입을 위한 다양한 지원을 추진 중으로 본 가이드에서 미처 설명하지 못한 여러 사항에 대하여 다양한 지원을 받을 수 있다.

개방형OS 도입가이드

디자인 천세커뮤니케이션



공개소프트웨어 라이선스 가이드는 크리에이티브 커먼즈 저작자표시-비영리-변경금지 2.0 대한민국 라이선스에 따라 이용할 수 있습니다.
