

행정·공공기관 응용프로그램 표준운영절차서

< 목 차 >

[적 용 기 준]

◆ 정보시스템의 등급에 따라 표준운영절차 도입 수준을 차등 적용

- 1~2등급 : 9개 응용프로그램 표준운영절차 적용 및 도입 의무

- 응용프로그램 표준운영절차
 - * (예방) 변경, 배포, 테스트, 연계, 형상, 운영상태
- 범정부 정보시스템 표준운영절차 준용
 - * (예방) 요청, (대응) 장애, (사후관리) 문제관리

- 3~4등급 : 6개 응용프로그램 표준운영절차 적용 및 기록관리 권고

- 응용프로그램 표준운영절차
 - * (예방) 변경, 배포, 테스트, 형상
- 범정부 정보시스템 표준운영절차 준용
 - * (대응) 장애, (사후관리) 문제관리

[적 용 가 이 드]

- ◆ 행정공공기관 응용프로그램의 안정적 운영을 위한 표준운영절차와 기준을 제공하며, IT 운영관리에 널리 활용되는 ITIL과 ISO20000 국제 표준을 기반으로 함
- ◆ 정보시스템을 운영하는 행정·공공기관은 본 응용프로그램 표준운영절차 적용기준에 따라 표준운영절차를 도입/운영하여야 하며, 기관 및 서비스의 특성에 따라 추가적인 절차를 운영할 수 있음
- ◆ 정보시스템의 인프라와 응용프로그램을 모두 운영하는 기관은 「정보시스템 표준운영절차(24.10.)」와 응용프로그램 표준운영절차를 병행 적용

◆ 개요	1
1. 요청 관리 절차서(범정부 정보시스템 표준운영절차 준용)	4
2. 변경 관리 절차서	14
3. 배포 관리 절차서	27
4. 테스트 관리 절차서	38
5. 연계 관리 절차서	48
6. 형상 관리 절차서	58
7. 운영상태 관리 절차서	68
8. 장애 관리 절차서(범정부 정보시스템 표준운영절차 준용)	78
9. 문제 관리 절차서(범정부 정보시스템 표준운영절차 준용)	97

개요

가. 목적

- 행정-공공기관에서 운영하는 정보시스템 응용프로그램(AP) 운영 효율화와 장애 발생 요소 최소화를 위해 개별 기관에서 활용 및 적용 가능한 AP 표준운영절차를 제공한다.
- AP 표준운영절차는 IT 서비스관리의 글로벌 표준인 ITIL, ISO/IEC 20000 등을 기반으로 하여 개별 기관의 AP 운영관리 역량 향상을 도모한다.

나. 적용 범위

- 행정-공공기관의 정보시스템 응용프로그램의 운영관리 활동에 적용

다. 역할 분담 기준

- 응용프로그램 표준운영절차의 운영에 있어 주요 역할에 대한 기준을 제공한다.
- 역할에 따라 표준운영절차별 상세 역할과 책임을 정의한다.
- 역할과 책임의 상세항목은 각 행정-공공기관의 조직구조/운영환경에 따라 개별 정의할 수 있다.

구분		내용
운영기관 (응용프로그램의 운영관리에 최종 책임지는 기관)	관리자	행정-공공기관 내 정보시스템 운영 담당 공무원의 상위 책임자 또는 부서장
	담당자	행정-공공기관 내 정보시스템 운영 담당자로 응용프로그램 운영관리의 책임을 가지며, 운영 사업자를 통해 응용프로그램의 실제적 운영을 관리·담당
운영자 (위탁기관 또는 운영 사업자)	운영관리	운영기관과의 계약을 통해 응용프로그램 운영 관리를 지원하는 위탁기관 또는 운영사업자
	유지보수	운영기관 또는 운영 사업자와의 계약을 통해 응용프로그램 관련 기능 변경 및 개선 등의 유지보수를 지원하는 사업자
	테스트	정보시스템 기능 요구사항을 완전히 구현하여 배포하는지 검증하고, 성능 요구사항을 충족하여 서비스가 안정적으로 제공되는지 확인하는 담당자

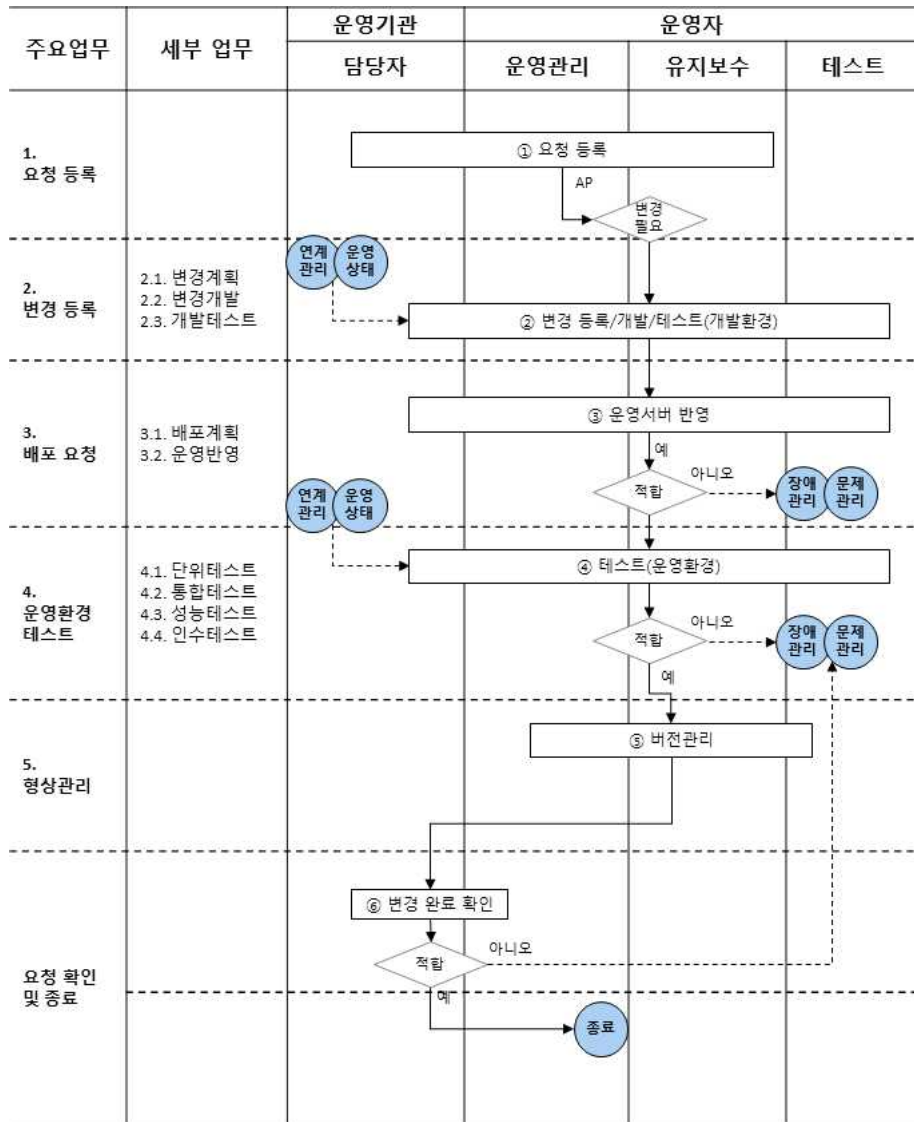
라. 표준운영절차

- 9개 응용프로그램(AP) 표준운영절차 설명

표준운영절차	설명
요청 관리 Customer Service Request Management	<ul style="list-style-type: none"> 서비스 요청 관리 범위와 절차 정립 요청등록, 분류, 처리, 고객 만족도 조사, 단계 승인 절차
변경관리 Change Management	<ul style="list-style-type: none"> 응용프로그램 변경 관리 범위와 운영 절차 정립 - 변경 관리 범위와 운영 절차 정립 - 변경 요청 접수 및 검토(CAB), 승인 - 변경 계획 수립 - 변경 종료 및 변경 평가
배포관리 Release & Deployment Management	<ul style="list-style-type: none"> 배포 관리 기준과 절차 정립 - 배포 계획 수립 및 검토, 승인 - 배포 수행 및 검증(테스트) - 배포 결과 검토 및 종료
테스트관리 Validation & Testing Management	<ul style="list-style-type: none"> 테스트 환경 구축 기준 및 테스트 관리 절차, 기준 정립 - 테스트 수행 기준 정의 - 테스트 계획 수립 및 설계 - 개발환경 및 운영환경 테스트 절차 정의 - 테스트 결과 분석 및 개선
연계관리 Integration Management	<ul style="list-style-type: none"> 연계관리 기준과 절차 정립 - 연계 요청 및 검토(사전 연계 협의) - 연계 계획 수립 및 검토, 검토결과 회신 - 연계 결과 검토
형상관리 Operational Configuration Management	<ul style="list-style-type: none"> 형상항목의 식별과 감사, 이력관리 절차 정립 - 형상 항목 식별 및 형상 관리 시스템 구축 - 형상 변경 승인 및 통제(Control) - 형상 감사(Audit) 및 기록
운영상태관리 Monitoring & Event Management	<ul style="list-style-type: none"> 운영시스템 상태관리 정책 및 운영이벤트 사후관리 기준 정립 - 운영상태관리 정책과 계획 수립 - 운영상태 모니터링 및 운영이벤트 조치 - 사후관리(예방점검, 최적화, 개선 등)
장애 관리 Incident Management	<ul style="list-style-type: none"> 장애 관리 기준과 처리 절차 정립 장애 식별 및 접수, 조사 및 진단, 해결 및 복구 절차
문제 관리 Problem Management	<ul style="list-style-type: none"> 문제 관리 기준과 절차 정립 문제 등록 및 검토, 조사 및 진단, 해결 및 복구 절차

마. 표준운영절차 흐름도

○ 응용프로그램(AP) 표준운영절차는 아래와 같은 순서로 구성된다.



1. 요청 관리 절차서

(범정부 정보시스템 표준운영절차 준용)

가. 개요

1) 목적

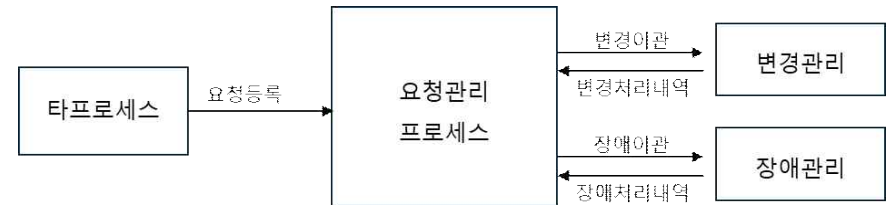
○ 정보시스템 운영 과정에서 발생하는 사용자의 다양한 요청사항(CSR: Customer Service Request)을 처리하기 위하여 유형별 처리 기준을 명시하고, 신속한 응대 및 처리를 위한 표준 절차를 제공함으로써 서비스 사용자의 요청사항을 누락없이 요구된 시간 내에 효과적으로 처리하는 것을 목적으로 한다.

2) 적용 범위

○ 요청 관리 절차는 행정-공공기관의 정보시스템을 운영하는 기관의 정보시스템 운영관리에 적용

3) 관련 업무 절차

○ 연관 선/후행 업무



○ 시작/종료/증적(Output) 조건

주요 업무	수행 업무
프로세스 시작 조건	사용자 요청(SR) 사항
프로세스 종료 조건	사용자 요청 처리
증적(Output)	요청 관리 대장 만족도 조사 결과 ※ ITSM 시스템을 사용하는 경우 시스템 내 이력으로 대체

나. 관리 정책

1) 정의

- 정보시스템 표준운영절차의 운영에 있어서 필히 준수해야 할 정책 기준을 제공

2) 정책 기준

정책	설명	
정책 1	기준	IT 서비스 사용자를 지원하기 위하여 표준화된 요청관리 프로세스가 존재하여야 한다.
	설명	○ 통합된 하나의 프로세스로 요청사항에 대해 신속하게 응대하고 처리 할 수 있어야 한다. ○ 하나의 최적화된 프로세스는 지원 비용 감소, 자원의 일관성 및 만족도 향상, IT 담당자의 생산성 향상을 목적으로 한다.
정책 2	기준	서비스요청은 ITSM 등의 표준운영절차 운영시스템을 통해 객관적인 정보로 관리되고 추적되어야 한다.
	설명	○ 모든 서비스요청은 유형 별로 기록, 관리 및 진행 상태가 추적 가능해야 한다. ○ 모든 서비스요청의 처리과정과 해결방법/결과정보는 시스템으로 관리한다. - 지원하는 시스템이 없는 경우 표준화된 절차를 기반으로 관련 이력이 수기 데이터로도 기록/관리되어야 한다.

다. 용어 정의

용어	설명
서비스 데스크	○ 사용자 지원을 위한 단일 접촉 창구로서 사용자로부터의 문의, 사용자 장비의 장애, 응용시스템 기능개선 요청 등에 대한 최초 접수창구로서 요청에 대한 진행사항 등을 관리하고, 사용자와의 커뮤니케이션을 진행한다.
서비스 요청	○ 사용자로부터 접수되는 IT 서비스에 대한 요청사항으로 문의사항, 변경요청, 응용시스템에 대한 기능개선요청, 일반적인 작업요청 등을 말한다.
이관 (Escalation)	○ 작업의 처리를 위해 관리자나 전문가 집단에게 처리를 넘겨거나, 타 프로세스 적 활동을 위해 프로세스로 작업을 넘기는 활동 - 프로세스 내에서 처리를 위해 상위 또는 차선 담당자에게 작업을 이관하는 활동

라. 역할 및 책임

- 요청관리 절차를 수행하는 역할자의 책임은 다음과 같다.

주요 업무	수행 업무	비고	
운영기관 (정보시스템의 최종운영관리를 책임지는 기관)	관리자	○ 정보시스템 관련 담당자의 상위 책임자 또는 부서장 ○ 요청 처리 관련 의사결정	
	담당자	○ 서비스요청 작업 대상 정보시스템의 담당자가 역할 수행 ○ 사용자의 요청사항에 대해 사전검토 등의 활동을 수행하고 필요 시 사용자의 서비스요청 내용을 운영 사업자에게 대행 요청하는 등의 활동 수행 ○ 요청건에 대한 이해당사자간 조율 및 의사소통 창구 ○ 서비스 요청의 적합 여부 검토 ○ 서비스 요청 처리 결과의 적합성 검토	
운영자 (위탁기관 또는 운영사업자)	운영관리	○ 운영기관과의 계약을 통해 정보시스템의 운영과 요청의 처리를 담당하는 위탁기관 또는 운영 사업자 ○ 서비스 데스크 역할 : 서비스 요청 작업의 접수 및 분류 ○ 서비스 요청에 대한 처리 수행 - 응대, 답변, 자료 제공 등	
	유지보수	○ 정보시스템을 구성하는 HW, SW, 미들웨어 등의 제조사 또는 유지보수를 담당하는 사업자 ○ 인프라 관련 서비스 요청에 대한 작업 수행	
	MSP	○ 운영관리 사업자 역할과 유사하며, 운영기관과의 계약을 통해 클라우드 환경에서의 정보시스템 운영관리를 지원하는 클라우드 운영 사업자 ○ 서비스 데스크 역할 : 서비스 요청 작업의 접수 및 분류 ○ 서비스 요청에 대한 처리 수행 - 응대, 답변, 자료 제공 등	
	CSP	○ 유지보수 사업자 역할과 유사하며, 운영기관 또는 MSP와 계약을 통해 클라우드 환경에서 제공되는 정보시스템 인프라에 대한 운영 사업자 ○ 클라우드 인프라 환경에서 발생하는 서비스 요청 작업 활동 수행	

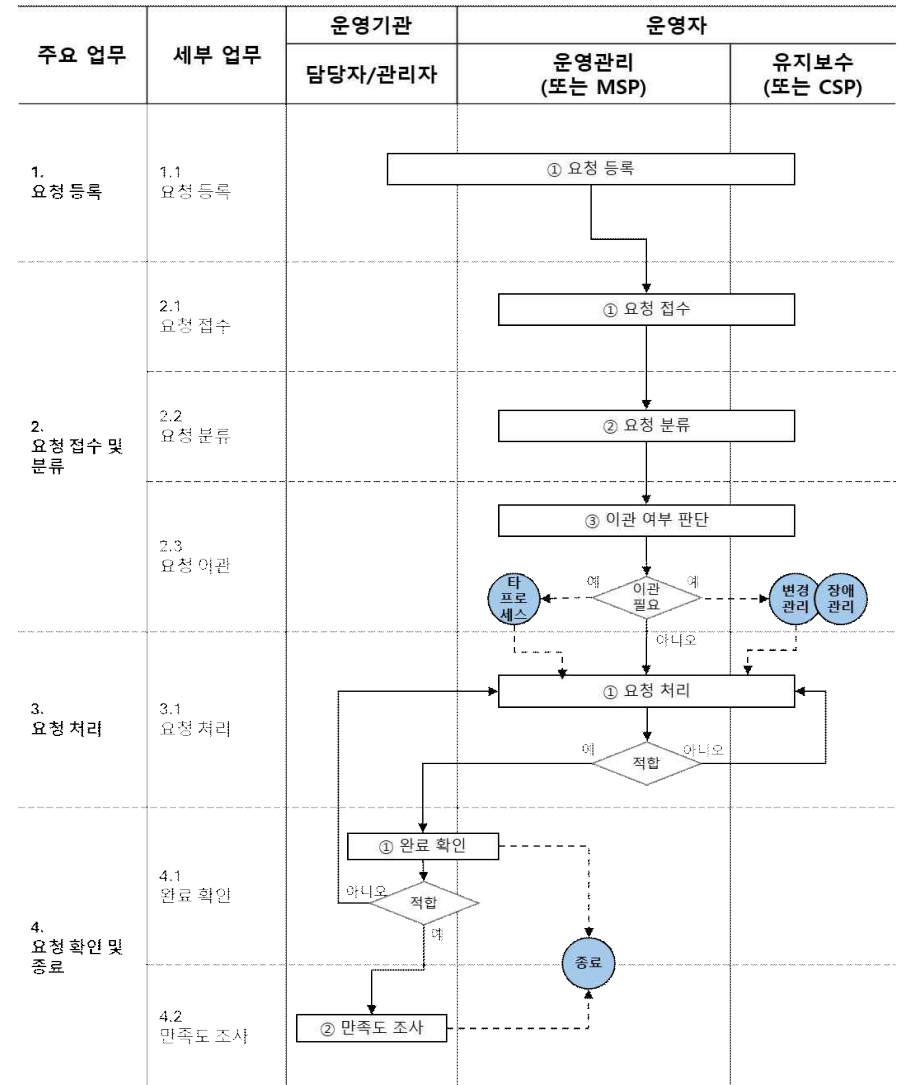
마. 표준절차 흐름도

○ 요청관리 절차는 아래와 같은 주요 업무와 수행절차들로 구성된다.

1) 주요 업무

주요 업무	세부 업무	수행 업무
1. 요청 등록	1.1 요청 등록	○ 사용자/요청자는 서비스 요청을 등록한다. ○ 메일 혹은 대면 등으로 접수된 사항은 운영기관 담당자 또는 운영자가 대행 등록을 수행한다.
2. 요청 접수 및 분류	1.2 요청 접수	○ 서비스 요청 사항을 접수하고 필요시 요청자에게 추가 정보를 요청하여 보완한다.
	2.1 요청 분류	○ 서비스 요청을 유형별로 분류하고, 담당자에게 배정한다. ○ 담당자 재배정이 필요한 경우는 다른 담당자에게 재배정한다.
3. 요청 처리	2.2 요청 이관	○ 서비스 요청 내역이 장애인 경우 장애 관리 프로세스로, 변경작업인 경우 변경 관리 프로세스로 이관 등 관련 프로세스로 이관한다.
	3.1 요청 처리	○ 서비스 요청 처리 담당자는 서비스 요청을 처리하고 결과를 기록한다.
4. 요청 확인 및 종료	4.1 완료 확인	○ 요청자는 처리 결과를 확인하여 적합 여부를 검토한다.
	4.2 만족도 조사	○ 만족도 조사를 수행해야 하는 경우 요청자는 요청 처리 결과 및 진행 상태에 대한 만족도 평가를 실시한다.

2) 수행주체별 표준절차 흐름도



바. 세부 수행 절차

1) 절차 및 역할과 책임(R&R : Role and Responsibility)

(●: 정, ○: 부)

세부 절차	수행 내용	운영기관		
		담당자/관리자	운영관리 (MSP)	유지보수 (CSP)
1.1- ① 요청 등록	<ul style="list-style-type: none"> - 사용자는 ITSM 혹은 메일 등(ITSM 시스템으로 Contact Point 일원화 권고)을 통하여 업무 요청, 변경 요청, 서비스 개선 요청 등 필요한 서비스를 요청한다. - ITSM 시스템을 활용하는 경우 ITSM을 통해 요청의 등록에서 처리까지 관련 이력을 관리한다. 	●	●	●
2.1- ① 요청 접수	<ul style="list-style-type: none"> - 메일 혹은 대면 등으로 접수된 사항은 ITSM 시스템에 요청을 받은 담당자가 대행 기록(등록)한다. ITSM 시스템이 없는 기관은 요청 이력의 관리가 누락되지 않도록 관련 사항을 기록/이력관리 하여야 한다. - IT 서비스데스크가 있는 기관의 경우는 서비스데스크를 통해서 접수하며, 아닌 경우는 운영자(운영관리 또는 MSP)가 서비스 요청 사항을 접수한다. - 접수된 서비스 요청의 정보가 충분하지 않으면 요청자에게 추가 정보를 요청하여 보완한다. - 정책 혹은 기타 사유로 서비스 요청을 처리할 수 없는 경우 반려사유를 안내하고 종료 처리한다. 		●	●
2.2- ② 요청 분류	<ul style="list-style-type: none"> - 서비스데스크 담당자는 서비스 요청을 사전 정의된 유형별로 분류한다. (ITSM 시스템을 활용하는 경우에는 사전 정의된 분류 유형에 따라 처리, 이관 등의 절차가 수행될 수 있도록 관리한다.) - 서비스 요청을 영향도, 해결의 시급함 등에 따라 우선 순위를 결정하고 담당자에게 배정한다. - 요청 처리를 위해 담당자 재 배정이 필요한 경우는 적절한 다른 담당자에게 배정 한다. 		●	●
2.3- ③ 이관 여부 판단	<ul style="list-style-type: none"> - 서비스 요청건의 처리를 위해 타 프로세스로의 이관이 필요한 경우 해당 프로세스로 작업을 이관한다. ※ 장애 관리 프로세스, 변경 관리 프로세스 등 		●	●

(●: 정, ○: 부)

세부 절차	수행 내용	운영기관		
		담당자/관리자	운영관리 (MSP)	유지보수 (CSP)
3.1- ① 요청 처리	<ul style="list-style-type: none"> - 배정받은 담당자는 서비스 요청 내용을 확인 검토한다. - 검토 내용을 기반으로 처리 작업을 수행한다. - 처리된 내역을 검토하여 적합한 경우 요청자에게 처리 내용의 확인을 요청한다. - 처리된 내역을 검토하였으나 부적합한 경우 처리작업을 재수행하거나 다른 담당자에게 이관할 수 있다. - 배정된 요청의 처리를 위해 다른 담당자에게 이관이 필요한 경우 처리 담당자를 지정하여 요청 작업건을 이관한다. (필요시 요청 분류단계로 이관하여 재분류 작업의 수행 절차로 진행할 수 있다.) - 장애(혹은 변경) 관리 프로세스로 이관된 건의 경우 처리 결과 확인 후 서비스 요청 건의 해결 여부를 확인한다. 		●	●
4.1- ① 완료 확인	<ul style="list-style-type: none"> - 서비스요청의 요청자는 처리 결과를 확인하여 적합 여부를 검토한다. - 적합한 경우 해당 요청건은 종료되며, 해당 요청건이 만족도 조사 활동이 필요한 경우 만족도 조사 단계를 진행한다. - 재작업이나 추가 작업이 필요한 경우에는 재작업을 요청 한다. 	●	○	
4.2- ② 만족도 조사	<ul style="list-style-type: none"> - 만족도 조사를 수행해야 하는 서비스 요청건에 대해서 요청자는 처리 결과에 대한 만족도를 평가한다. - 해당 만족도 조사는 이를 지원할 수 있는 ITSM 시스템 등이 있는 경우에 실시한다(지원시스템이 없는 경우 서비스요청 처리의 품질 관리를 위해 년 1회이상 수기 사용자 만족도 조사를 권고). - 만족도 조사에 응한 경우 해당 서비스 요청 건은 종료되며, 만족도 조사에 응하지 않은 경우 특정기간 (예시: 1주일)이 지나면 자동 종료처리할 수 있다. 	●		

사. 핵심성과지표 (KPI : Key Performance Indicator)

프로세스 운영 품질 관리를 위해 프로세스별 관리지표를 도출하여 관리함을 목표로 하며, 본 절차서에서는 관리가능한 KPI를 제시하고 개별기관별 운영 상황에 맞추어 최적화하여 지표 관리

측정지표	측정방법	측정목적	측정주기
서비스 요청 납기 준수율	(요청된 서비스 건수 ÷ 납기내 서비스 처리 건수) X 100	서비스 요청 일정 준수 (운영시스템이 없는 경우에도 최소한의 납기일정은 준수 권고)	월간

※ ITSM 등의 운영시스템 미사용시에는 서비스 품질 향상을 위해 만족도 평가 KPI를 연간 관리 지표로 권고

측정지표	측정방법	측정목적	측정주기
만족도 점수	만족도 점수 총합 ÷ 만족도 답변 건수	서비스 만족도 확인	월간

아. 수행 검증

1) 검증 방법

- 검증 체크리스트의 체크항목 기준(ITIL 표준 준용)으로 표준운영절차의 준수여부와 이행점검을 수행한다.
- 개별기관 내 자체 프로세스 검증자는 내부 감사자의 자격 또는 ITIL에 대한 충분한 이해를 가진자가 수행한다. (ITIL 관련 자격 권고)
- 점검 결과는 대외 감사/진단 시 내부 점검 활동의 결과물로 활용할 수 있다.

2) 검증 항목

세부 절차	체크 항목	정성 평가	증적 체크
요청 등록	- 모든 서비스요청은 기록되고 관리되고 있습니까?	적합/ 부적합	<ul style="list-style-type: none"> • ITSM 내 요청기록 • 요청관리대장 (ITSM 미사용시)
요청 접수 및 분류	- 접수되는 서비스요청은 적절히 분류되어 담당자에게 할당되고 있습니까?		<ul style="list-style-type: none"> • ITSM 내 처리이력 • 요청관리대장 (ITSM 미사용시)
요청 처리	- 서비스요청을 처리하기 위해 장애, 변경관리 등의 타 프로세스 작업이 필요한 경우 해당 프로세스로 적절하게 이관하여 처리하고 있습니까?		<ul style="list-style-type: none"> • ITSM 내 처리이력 또는 관리이력
	- 서비스요청의 진행사항 및 처리결과에 대해 요청자에게 적절하게 정보가 제공되고 있습니까?		<ul style="list-style-type: none"> • ITSM 내 처리이력 또는 관리이력
요청 확인 및 종료	- 만족도 조사가 필요한 요청건은 요청 처리 후 만족도 조사를 진행하고 확인이 되고 있습니까?		<ul style="list-style-type: none"> • ITSM 내 만족도 평가 이력 • 또는 만족도 관리이력
	- 만족도 조사를 통해 불만족 사항등이 파악되는 경우 해결을 위한 활동이 진행되고 있습니까?		<ul style="list-style-type: none"> • 불만족에 대한 관리 이력

자. 관리기준 및 예시

1) 서비스 요청 분류 (예시)

(하기 항목은 예시 유형으로 참고용이며, 각 기관별 적용가능한 유형으로 구분하여 적용)

범주	구분	비고
일반 요청	단순/사용법 문의	
	단순 데이터 확인	
	업무/작업 검토	
	불만	
	기타	
장애	기능 불가	
	단순 오류/결함	
	기타	
변경	신규 개발	
	기능 수정/개발	
	UI/UX 변경	
	데이터 변경	
	정보/자료 요청	
	서버 작업 요청	
	네트워크 작업 요청	
	보안 작업 요청	
	DB 작업 요청	
	기타	
	백업	백업/복구 요청
구성	구성정보 변경요청	
	구성정보 추가요청(신규)	

2) 만족도 기준 (예시)

점수	기준	설문항목(예시)
5점	매우 만족	<ul style="list-style-type: none"> 서비스 요청에 전반적으로 만족하십니까? 서비스 요청에 대한 일정이 잘 준수 되었습니까? 서비스 요청에 대한 처리가 요구사항에 맞게 정확히 처리 되었습니까?
4점	만족	
3점	불만	
2점	불만족	
1점	매우 불만족	

2. 변경 관리 절차서

가. 개요

1) 목적

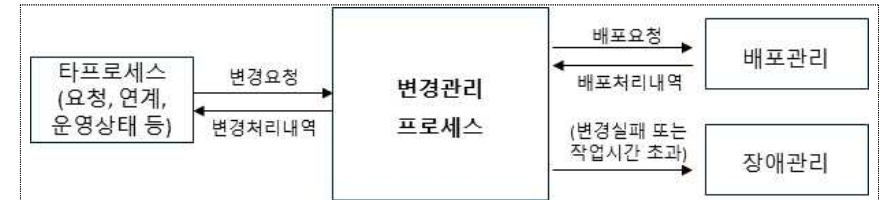
- 응용프로그램 변경작업으로 인한 서비스 영향과 위험 발생을 최소화하고, 효율적인 변경 처리를 위한 방법과 절차를 표준화하여 이를 준수할 수 있도록 보장한다.

2) 적용 범위

- 변경관리 절차는 서비스요청 중 응용프로그램 변경이 이루어지는 변경 요청을 대상으로 한다.

3) 관련 업무 절차

- 연관 선/후행 업무



- 시작/종료/증적(Output) 조건

주요 업무	수행 업무
프로세스 시작 조건	응용프로그램 구성의 추가, 수정, 제거 등 변경이 발생하는 일체의 요청
프로세스 종료 조건	변경처리 종료 변경요청(RFC)의 반려
증적(Output)	변경요청서(RFC) 변경계획서 변경결과서 변경이력 관리대장 ※ 변경관리 절차 및 증적을 ITSM 시스템에 반영하여 관리

나. 관리 정책

1) 정의

- 응용프로그램 변경관리 절차의 운영에 있어서 필히 준수해야 할 정책 기준을 제공

2) 정책 기준

정책	설명	
정책 1	기준	응용프로그램에 발생하는 모든 변경은 표준화된 변경관리 절차를 통하여 수행·관리 되어야 한다.
	설명	<ul style="list-style-type: none"> ○ 응용프로그램 구성의 추가, 수정, 제거 등 모든 변경요청은 반드시 변경관리 절차를 통하여 수행해야 한다. ○ 변경관리는 변경으로 인한 서비스 영향 검토, 변경작업을 위한 필요 자원 정의 및 변경에 대한 승인 등의 활동이 포함되어야 한다. ○ 변경관리 절차는 다양한 유형의 변경을 수용할 수 있어야 한다. ○ 변경관리 절차는 일반, 단순, 긴급 변경 절차를 구분한다. ※ 단순, 긴급 변경은 작업 특성을 고려하여 간소화된 작업절차를 정의할 수 있다.
정책 2	기준	모든 변경작업의 상태 및 이력은 문서로 기록하고 관리해야 한다.
	설명	<ul style="list-style-type: none"> ○ 1~2등급 정보시스템은 응용프로그램 표준운영절차의 체계적인 관리를 위하여 변경정보를 시스템으로 관리해야 한다. ○ 3~4등급 정보시스템은 표준운영절차로 운영하며, 이를 지원하는 ITSM 시스템이 없는 경우 변경정보를 관리대장 등에 기록·관리 해야한다. ○ 변경작업 이력(작업 실패 포함)은 AP 운영현황관리 항목에 포함되어 통계 관리해야 한다. - ITSM 변경작업 이력 관리 또는 변경이력 관리대장 작성
정책 3	기준	1~2등급 정보시스템은 서비스의 중요성을 고려하여 강화된 변경관리 절차(변경관리위원회 운영, 2단계 승인, 이행 후 검토, 업무시간 배포 금지 등)의 기준을 준수해야 한다. ※ 변경관리위원회 및 2단계 승인 (1등급 필수, 2등급 권고)
	설명	<ul style="list-style-type: none"> ○ 변경관리위원회를 통해 변경영향을 검토해야 한다. ○ 변경계획은 담당자와 관리자의 2단계 승인을 수행한다. ○ 변경처리 종료 시 이행 후 검토(변경 결과가 초기 목적 및 예상 효과를 적절하게 달성하였는지에 대한 검토) 활동을 수행한다. ○ 1~2등급 정보시스템의 일반 변경작업은 업무시간(09~18) 배포 작업을 금지하고(필수), 3~4등급 정보시스템은 가급적 상기 시간을 준수(권고)
정책 4	기준	모든 변경작업은 원상복구계획을 변경계획에 포함하여 관리해야 한다.
	설명	<ul style="list-style-type: none"> ○ 변경실패 발생 시 작업 결과를 상세히 기록하고, 장애관리로 이관한다. ○ 원상복구계획의 절차에 따라 복구를 수행한다.

다. 용어 정의

용어	설명
변경 요청 (RFC: Request For Change)	○ 응용프로그램의 서비스나 기능 변경을 제안하는 방법으로 제안된 변경의 특성이나 세부 사항, 타당성이 기술되고 승인이 적용된 문서나 기록을 의미한다.
일반 변경	○ 단순, 긴급 변경을 제외한 정기 및 비정기적으로 발생하는 변경 요청으로 변경 처리 절차를 준수해야 하며 시스템 등급에 따른 승인 절차를 준수하여야 한다.
단순 변경	○ 위험이 낮고 정형화된 변경으로 담당자가 작업의 진행여부를 결정하고 결과를 승인자에게 보고하는 변경을 의미한다.
긴급 변경	○ 처리가 가능한 신속하게 이루어져야 하는 변경작업을 의미한다. - (예) 장애 및 중요 이벤트 해결을 위한 긴급 조치로 인한 변경 등
변경 관리 위원회 (CAB: Change Advisory Board)	<ul style="list-style-type: none"> ○ 파급 효과가 높은 변경요청을 평가하는 책임과 대표성을 가진 인력 그룹(협의체)으로 구성원은 개별기관에 따라 달라질 수 있다. ○ 위원회는 변경 요청에 대한 진행여부, 우선순위 등을 검토하며, 변경을 구현하기 위한 자원의 할당 등을 제안한다. ※ 변경 관리 위원회(CAB)의 소집은 정보시스템 운영 환경에 따라 대면, 서면, 영상회의 등으로 개최할 수 있으며, 1등급 정보시스템은 필수 운영
이행 후 검토 (PIR: Post Implementation Review)	<ul style="list-style-type: none"> ○ 변경 완료 이후 검토 활동으로 변경 결과에 대한 검토 및 예상 효과 달성 여부를 검토한다. ○ 변경관리위원회 심의를 거친 1등급 정보시스템의 일반 변경은 의무적으로 이행 후 검토과정을 수행한다.
원상복구계획	○ 변경작업이 전체 또는 부분적으로 실패한 경우, 서비스를 원래 상태로 복구하기 위해 취해야 할 모든 활동들을 포함한 계획으로, 전체 복구 또는 일부 복구가 포함될 수 있다.

라. 역할 및 책임

○ 변경관리를 수행하는 역할과 책임은 다음과 같다.

구분		내용
운영기관 (응용프로그램의 운영관리에 최종 책임지는 기관)	관리자	○ 정보시스템 관련 담당자의 상위 책임자 또는 부서장 ○ 변경요청의 적합성 판단 ○ 변경계획 검토 및 승인 등 의사결정
	담당자	○ 변경작업 대상 정보시스템 업무 담당자가 역할 수행 ○ 변경계획의 적정성 검토 ○ 변경관리위원회(CAB) 소집 및 진행 ○ 변경작업 관련 이해당사자간 조율 및 의사소통 창구 - 위탁기관 및 운영사업자 간 유기적 협조체계 관리 포함 ○ 변경작업 관련 테스트 결과 및 이행 결과 검토 ○ 변경완료 후 PIR 수행
운영자 (위탁기관 또는 운영 사업자)	운영관리	○ 운영기관과의 계약을 통해 정보시스템의 운영과 변경작업을 담당하는 위탁기관 또는 운영 사업자 ○ 변경작업 관련 이해당사자(운영기관/운영사업자)간 조율 - 위탁기관 및 운영사업자 간 유기적 협조체계 관리 포함 ○ 변경계획의 적정성 검토 ○ 변경계획 수립과 변경관련 준비작업 - 변경사유, 작업 일정, 상세 작업계획, 변경영향, 테스트 계획, 복구 계획 등의 준비 ○ 변경작업 수행 - 변경계획에 따라 작업을 수행하고 완료 후 테스트 및 서비스 확인 ○ 변경작업 이후 형상정보에 대한 현행화 작업
	유지보수	○ 정보시스템의 응용프로그램 유지보수를 담당하는 사업자 ○ 변경계획 수립과 변경관련 준비작업 - 변경사유, 작업 일정, 상세 작업계획, 변경영향, 테스트 계획, 복구 계획 등의 준비 ○ 변경작업 수행과 결과 보고 ○ 변경작업 이후 형상정보에 대한 현행화 작업

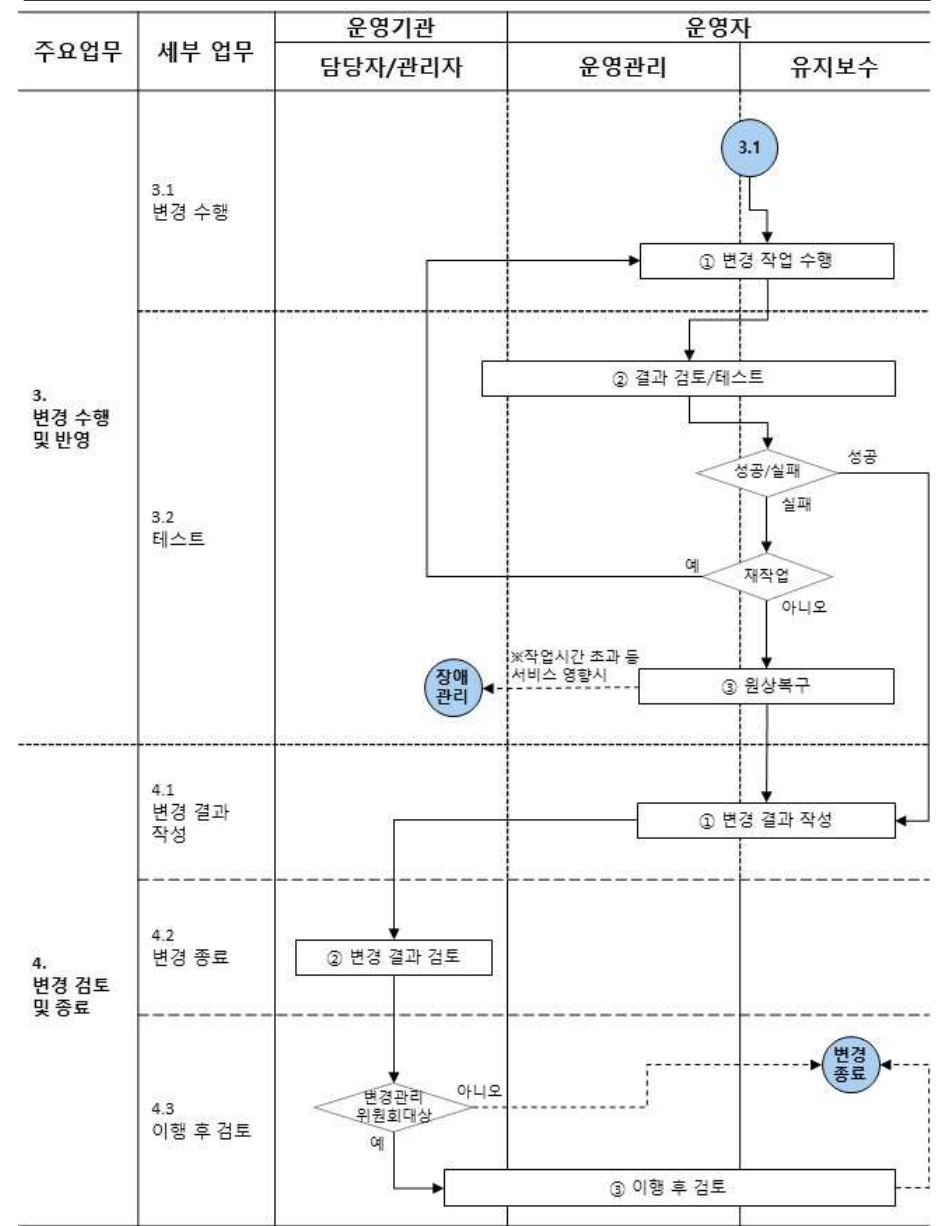
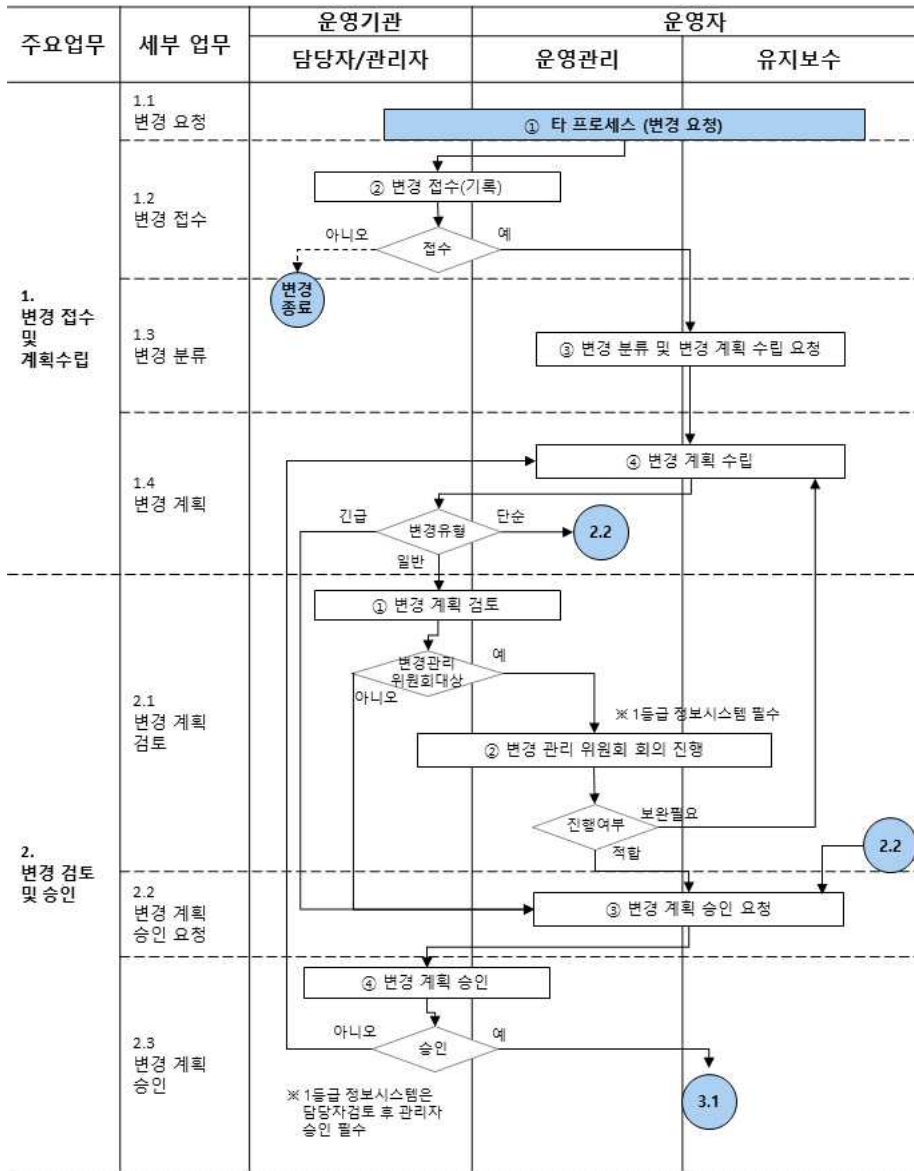
마. 표준절차 흐름도

○ 변경관리 절차는 아래와 같은 주요 업무와 수행 활동으로 구성된다.

1) 주요 업무

주요 업무	세부 업무	수행 활동
1. 변경 접수 및 계획 수립	1.1 변경 요청	○ 서비스 요청 프로세스나 타 프로세스에서 변경을 요청한다.
	1.2 변경 접수	○ 운영기관 담당자 또는 운영관리자는 변경 요청을 접수하고 진행 여부를 판단하여, 변경요청서를 작성한다.
	1.3 변경 분류	○ 운영관리자는 기준에 따라 변경 유형을 분류하고, 관련자들과 협의 하며 작업계획을 수립할 변경 작업자를 지명한다.
	1.4 변경 계획	○ 운영관리자는 변경 계획서(아래 내용 포함)를 작성한다. - 변경 요청 근거 및 내용, 변경 작업자, 변경 사유, 변경 일시 - 변경 대상, 변경 영향(타 시스템, 타 기관 등), 작업 계획 - 운영 반영 계획, 원복 계획, 첨부 자료 등
2. 변경 검토 및 승인	2.1 변경 계획 검토	○ 운영기관 담당자는 수립된 변경 계획의 적합성을 검토한다. ○ 정보시스템이 1,2 등급일 경우 변경관리위원회를 개최하여 변경 계획에 대한 심의 및 변경 작업의 진행 여부를 결정한다. ※ 변경관리위원회 (1등급 정보시스템 필수, 2등급 정보시스템 권고)
	2.2 변경 계획 승인 요청	○ 운영관리자는 검토된 변경계획을 운영기관 담당자에게 승인 요청 한다.
	2.3 변경 계획 승인	○ 운영기관 담당자는 변경계획을 검토하고 승인을 진행한다.
3. 변경 수행 및 테스트	3.1 변경 작업	○ 운영자는 변경계획에 따라 변경 작업을 수행한다. - 변경작업 수행 중 장애가 발생하지 않도록 변경작업계획을 지속적으로 확인하고 작업의 진행상태를 확인한다.
	3.2 테스트	○ 변경 작업 완료 후 운영환경 반영 전 변경에 대한 테스트를 진행 하고 이상 여부를 확인한다. - 테스트는 개별기관의 운영환경 및 인력구성에 따라 다르게 적용 될 수 있다
	3.3 변경 반영	○ 운영자는 승인된 운영환경 반영계획에 따라 운영환경에 반영작업 을 진행한다. ○ 반영작업 실패 시에는 원상복구계획에 따라 복구를 진행한다.
4. 변경 검토 및 종료	4.1 변경 결과 작성	○ 운영자는 변경완료 보고서를 작성하고 운영기관 담당자에게 보고한다. ○ 운영자는 형상항목 업데이트를 실시한다.
	4.2 변경 종료	○ 운영기관 담당자는 변경이력을 확인하여 변경작업 정상 여부를 확인하고, 변경을 종료한다. ○ 변경관리위원회 심의를 거친 변경은 이행 후 검토 단계를 진행한다.
	4.3 이행 후 검토	○ 변경관리위원회는 변경작업의 초기 목적 달성 여부 및 변경 수행 과정에서 발생했던 기술적인 이슈 사항이나 변경 지연 및 실패 등에 대해 검토를 수행한다.

2) 수행주체별 표준절차 흐름도



바. 세부 수행 절차

1) 절차 및 역할과 책임(R&R : Role and Responsibility)

(●: 정, ○: 부)

세부 절차	수행 내용	운영기관		
		운영기관	운영자	
		담당자/관리자	운영관리	유지보수
1.1- ① 변경 요청	<ul style="list-style-type: none"> - 요청자는 정보시스템의 변경 필요 시(변경작업 요구사항, 환경 변경, 법규의 변경 등) 서비스 요청 관리 프로세스에 의거 관련 사항을 운영기관 담당자에게 요청하거나, ITSM 시스템을 통하여 요청을 등록한다. - 타 프로세스에서 개선을 위하여 변경이 필요할 경우 관련 사항을 운영기관 담당자에게 전달하거나 ITSM 시스템에 변경 요청을 등록한다. 	●	●	○
1.2- ② 변경 접수 (기록)	<ul style="list-style-type: none"> - 운영기관 담당자 또는 운영자는 서비스 요청 및 타 프로세스에서 등록된 변경 요청의 필요성 및 요청 내용이 기준에 적합한지 검토하고 접수 여부를 결정한다. - 요청 진행 시 담당자는 요청된 내역에 대하여 변경 요청서(RFC: Request For Change)를 작성한다. 	●	●	
1.3- ③ 변경 분류 및 변경 계획 수립 요청	<ul style="list-style-type: none"> - 운영자는 변경작업의 유형에 따라 변경을 분류(긴급, 일반, 단순)한다. - 운영자는 요청자, 운영기관 담당자, 작업자, 유지보수 업체 등 관련자들과 협의하고, 작업계획을 수립할 변경 작업자를 지정한다. - 운영자는 지정된 변경 작업자에게 변경 작업 계획 수립을 요청 한다. 		●	●
1.4- ④ 변경 계획 수립	<ul style="list-style-type: none"> - 운영자는 변경 요청을 근거로 관련 담당자와 일정, 작업 내용 등 전반적인 변경 작업에 대하여 협의를 진행하고, 변경으로 인한 영향 등을 고려하여 변경 계획서를 작성 한다. - 변경 계획서는 아래와 같은 내용을 포함한다. <ul style="list-style-type: none"> ※ 변경 요청 근거, 변경 내용, 작업자, 변경 사유, 희망일 변경 일시, 변경 대상, 변경 영향(타 시스템 타 기관 등) 작업 계획, 운영 반영 계획, 원복 계획 등 ※ 소프트웨어 변경일 경우 테스트 계획 필수 포함 (프로그램 패치, 수정 및 배포, 환경변수 변경 등 일체의 소프트웨어적인 변경을 포함하며, 특히 다수의 시스템에 일괄배포되는 경우에는 순차적 배포를 권고) - 단순 변경의 경우 일상적이고 반복된 변경으로, 사전 정의된 변경 작업 계획에 의거 변경 승인 및 작업절차를 간소화하여 진행할 수 있다. 		●	●

(●: 정, ○: 부)

세부 절차	수행 내용	운영기관		
		운영기관	운영자	
		담당자/관리자	운영관리	유지보수
2.1- ① 변경 계획 검토	<ul style="list-style-type: none"> - 운영기관 담당자는 수립된 변경 계획을 검토한다. - 긴급 변경일 경우는 변경 계획을 구두로 확인하고 검토 단계를 생략할 수 있다. - 운영기관 담당자는 변경 관리 위원회(CAB) 대상(1 등급 정보시스템의 일반변경)의 여부를 파악하고 대상인 경우 변경 관리 위원회를 소집한다. - 변경 관리 위원회(CAB)의 주관 및 참석 대상 등 개최 기준은 "변경 관리 위원회 기준"을 참조한다. 	●	○	
2.1- ② 변경 관리 위원회 회의 진행	<ul style="list-style-type: none"> - 변경 관리 위원회(CAB)에서는 변경 요구 사항 (변경수준, 범위, 분류) 및 변경이 미치는 영향 등 기술 검토와 영향도를 검토하여 심의한다. - 변경 심의 내용은 회의록 등을 통해 이력으로 관리되어야 한다. - 위원회의 심의 결과가 변경에 적합하지 않은 경우 운영자를 통해 변경계획을 보완하여 절차를 재수행하거나 해당 변경 건을 요청자에게 사유 통보하고 프로세스를 종료할 수 있다. - 반려 및 조건부 승인이 될 경우, 운영기관 담당자는 관련 당사자와 추가 협의가 진행되도록 주관한다. 	●	○	○
2.2- ③ 변경 계획 승인 요청	<ul style="list-style-type: none"> - 운영자는 검토된 변경 계획을 운영기관 담당자에게 승인 요청한다. - 승인 단계 및 승인자는 각 운영기관 및 변경 등급에 따라 사전에 정의한다. 		●	●
2.3- ④ 변경 계획 승인	<ul style="list-style-type: none"> - 운영기관 담당자는 변경계획을 검토하여 변경작업에 대해 승인여부를 결정한다. - 변경계획서의 작성 오류 또는 미흡한 사항으로 승인이 불가할 경우 해당 계획서를 운영자에게 반려하여 수정/보완하도록 한다 - 1등급 정보시스템은 담당자 검토 후 관리자 승인을 필수로 진행한다. ※ 단순변경, 긴급변경은 관리자 승인을 제외할 수 있다. 	●	○	

(●: 정 ○: 부)

세부 절차	수행 내용	운영기관		
		운영기관 담당자/관리자	운영자 운영관리	운영자 유지보수
3.1- ① 변경 작업 수행	- 운영자는 변경계획에 따라 변경작업을 수행하고 결과를 기록한다. ※ 변경작업 수행의 시작과 종료는 관련된 이해관계자에게 전파/공유하여야 한다. - 운영자는 변경작업 수행 중 장애가 발생하지 않도록 변경작업 계획을 지속적으로 확인한다. - 운영자는 변경 작업이 초기 계획을 초과하여 서비스에 영향이 발생할 경우 서비스 영향이 발생되지 않도록 신속하게 원상복구를 수행한다.		●	●
3.2- ② 결과 검토 /테스트	- 운영자는 변경작업 후 테스트를 통해 정상 여부를 확인한다. - 테스트 실패 시 원인을 파악하고 원인이 불명할 경우는 문제 관리로 이관하고 재작업이 필요할 경우 재작업을 실시 한다.		●	●
3.2- ③ 원상복구	- 원상 복구가 필요할 경우는 원상 복구 계획에 의거하여 원상 복구를 실시한다. - 변경 작업 중 변경 실패나 작업시간 초과 등으로 서비스에 영향이 발생 시 장애 관리로 이관하여 처리한다	○	●	●
4.1- ① 변경 결과 작성	- 운영자는 변경 작업 완료 후 서비스 이상유무에 대한 점검 결과와 변경작업의 효율성 등을 모니터링하여, 특이사항 또는 이슈사항 등의 결과를 확인한다. - 운영자는 변경에 대한 완료 보고서를 작성하고 운영기관 담당자에게 보고한다. - 운영자는 구성 항목에 반영이 필요할 경우 구성 항목에 대한 업데이트를 실시한다. ※ CMDDB를 관리하는 기관에 해당		●	●
4.2- ② 변경 결과 검토	- 운영기관 담당자는 변경 기록을 확인하여 변경작업 정상유무를 확인하고, 변경을 종료한다. - 변경 관리 위원회(CAB) 심의를 거친 변경에 대해서는 운영기관 담당자가 변경 관리 위원회 소집을 요청하여 이행 후 검토(PIR) 활동을 수행한다.	●	○	○
4.3- ③ 이행 후 검토	- 변경 적용 사항 및 변경 수행 과정에서 발생했던 기술적인 이슈 사항이나 변경 지연 및 실패 등에 대해 검토를 수행한다. - 주요 검토 사항은 아래와 같다. ※ 변경작업의 목적 달성 여부 목적 미달성 시 검토/분석을 통해 개선 활동이 수행될 수 있도록 관리 ※ 변경 이후 일정 시간의 경과 후 변경에 따른 영향이나 오류 발생 등의 상태 점검	●	●	○

사. 핵심성과지표 (KPI : Key Performance Indicator)

프로세스 운영 품질 관리를 위해 프로세스 별 관리지표를 도출하여 관리함을 목표로 하며, 본 절차서에 서는 관리가능한 KPI를 제시하고 개별기관 별 운영 상황에 맞추어 조정하여 지표 관리

측정지표	측정방법	측정목적	측정주기
변경처리 목표시간 준수율	(목표시간내 변경 건수 ÷ 변경 요청 건수) X 100	변경 일정 준수	월간

아. 수행 검증

1) 검증 방법

- 검증 체크리스트의 체크항목 기준(ITIL 표준 준용)으로 표준운영절차의 준수여부와 이행점검을 수행한다.
- 개별기관 내 자체 프로세스 검증자는 내부 감사자의 자격 또는 ITIL에 대한 충분한 이해를 가진자가 수행한다. (ITIL 관련 자격 권고)
- 점검 결과는 대외 감사/진단 시 내부 점검 활동의 결과물로 활용할 수 있다.

2) 검증 항목

세부 절차	체크 항목	정성 평가	증적 체크
1. 변경 접수 및 계획수립	- 변경요청은 서비스요청 등의 타프로세스로부터 정상적으로 요청/등록되어지고 있습니까?	적합/ 부적합	• 변경요청 이력 - ITSM 내 변경요청 이력 또는 주기 변경이력 관리대장
	- 변경요청의 유형(일반/긴급/단순)은 사전정의되어 있으며, 해당 절차를 구분하고 있습니까?		• 변경유형 기준 • 유형별 처리절차
	- 변경계획에는 변경작업의 적합성을 검토하고 수행하기 위한 충분한 내용을 포함하고 있습니까? *변경요청근거, 변경사유, 변경대상, 변경영향, 작업계획 등 - 변경계획에는 작업 실패에 대비한 원복계획/절차를 수립하여 포함하고 있습니까?		• 변경계획서 - ITSM 내 변경계획 이력 또는 주기 변경계획서 • 원복계획서 - 변경계획서 내 포함 가능
2. 변경 검토 및 승인	- 1등급 정보시스템의 일반변경은 변경 수행전 변경심의위원회(CAB)를 통한 변경심의를 수행하고 있습니까?		• 변경심의 수행이력 - 회의록 또는 ITSM 내 변경작업이력
	- 1등급 정보시스템의 일반변경은 변경작업에 대해 2단계 승인(담당자검토 > 관리자승인)단계를 수행하고 있습니까? - 정보시스템의 변경작업은 검토, 승인단계를 수행하고 있습니까?		• 변경작업 승인이력 - 승인이력 또는 ITSM 내 검토/승인이력
3. 변경 수행 및 반영	- 변경 작업 후 실환경 적용전에 충분한 테스트가 진행되고 있습니까? * 개발계/검증계 테스트, 테스트케이스 활용여부		• 테스트케이스 및 테스트결과
	- 테스트시 발견된 결함은 등록되고 있으며, 이에 대한 처리이력이 관리되고 있습니까?		• 결함관리이력
4. 변경 검토 및 종료	- 변경작업 이후 PIR과 같은 검토활동이 수행되고 관련 이력이 관리되고 있습니까?		• 변경결과서 또는 PIR 활동 이력
	- 변경작업으로 구성정보가 변경된 경우 CMDB의 업데이트가 진행되고 있습니까?		• CMDB 업데이트 이력 - ITSM 이력 또는 CMDB 관리대장

자. 관리기준 및 예시

1) 변경 유형

구분	설명
일반 변경	• 단순, 긴급 변경을 제외한 정기 및 비정기적으로 발생하는 변경 요청으로 변경 처리 절차(변경계획, CAB, 검토 및 승인 단계 등)를 준수해야 하며 시스템 등급에 따른 승인 절차를 준수해야하는 변경
단순 변경	• 정기적으로 반복되어 수행되거나, 수행 경험으로 변경작업의 내용이 검증된 경우 간소화된 절차를 적용해 효과적인 작업을 수행하는 변경으로 위험성 및 업무서비스 영향도가 매우 낮은 변경 • 단순 변경(기관별 사전 정의에 따라 변경 가능) - 사용자 계정관리, 방화벽 정책 변경, 기타 파급 영향도가 낮은 작업으로 사전에 절차서에 단순변경으로 정의된 변경
긴급 변경	• 중대한 장애 혹은 문제로 인해 업무에 영향을 받는 경우, 또는 운영기관의 요구에 긴급하게 대응하여 처리되는 변경 - 정보시스템의 중대한 오류 등으로 서비스의 중단을 초래하거나, 다수의 사용자에게 심각한 영향을 미치는 장애에 대해서 빠른 작업처리를 위한 변경

2) 변경 관리 위원회(CAB)

가. 변경 관리 위원회는 접수된 변경요청에 대해 다양한 검토를 실시하여 그 수행여부에 대해 승인하고, 변경의 영향, 위험성, 우선순위의 평가 등을 통해 효율적이고 안정적인 변경관리가 되도록 하는 역할을 담당한다.

나. 변경 관리 위원회에 참여하여야 하는 구성원은 변경요청을 평가하는 책임과 대표성을 가진 인력을 포함하며, 역할 상 필요한 모든 이해관계자가 포함될 수 있도록 운영기관에 따라 사전에 정의가 필요하다.

다. 변경관리위원회 심의대상의 중요성에 따라 중점심의, 간소화심으로 구분하여 심의할 수 있으며, 개최기준에 해당되지 않는 변경 작업에 대해서도 운영기관 담당자가 판단하여 변경관리위원회 안건으로 상정할 수 있다.

3. 배포 관리 절차서

가. 개요

1) 목적

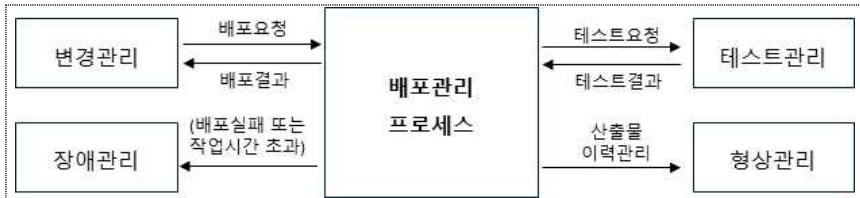
- 응용프로그램 변경요청을 운영환경에 반영하기 위한 배포 절차를 표준화하여 체계적으로 관리하고, 배포관리 기준을 제공하여 배포과정의 위험을 최소화하고 시스템의 무결성을 확보한다.

2) 적용 범위

- 배포관리 절차는 응용프로그램의 변경을 운영환경에 반영하는 활동에 적용된다.
 - 배포대상 시스템 : 시스템 운영서버
 - 배포대상 모듈 : 응용S/W, DB Schema, DB 스크립트 등

3) 관련 업무 절차

- 연관 선/후행 업무



- 시작/종료/증적(Output) 조건

주요 업무	수행 업무
프로세스 시작 조건	응용프로그램 기능 변경/신규 개발, 타 시스템(데이터 포함) 연계 변경/신규 연계 등의 다양한 이유로 응용프로그램 변경사항에 대한 배포를 위해 수행하는 일체의 요청
프로세스 종료 조건	배포 요청의 반려 배포 처리 종료
증적(Output)	배포 계획서, 배포 승인서, 배포 요청서, 배포 완료 보고서, 개선 사항 보고서 ※ ITSM 시스템을 사용하는 경우 시스템내 이력으로 대체

나. 관리 정책

1) 정의

- 응용프로그램 배포관리 절차의 운영에 있어서 필히 준수해야 할 정책 기준을 제공

2) 정책 기준

정책	설명	
정책 1	기준	모든 배포계획은 테스트환경(검증계)에서 테스트를 완료한 후 운영서버에 반영을 요청할 수 있다.
	설명	<ul style="list-style-type: none"> ○ 운영자는 개발 완료된 릴리스의 테스트 활동을 포함하여 배포계획을 수립한다. ○ 배포계획은 운영관리자와 운영기관 담당자(변경요청자)의 2단계 승인을 수행한다(긴급배포의 경우 예외적으로 생략 가능). <ul style="list-style-type: none"> - 운영자는 테스트 시나리오에 따라 테스트환경에서 사전검증 통합테스트를 수행하고 배포계획을 1차 검토 - 운영기관 담당자(변경요청자)는 1차 배포계획 검토 결과에 따라 보완요청 또는 운영서버 배포 승인
정책 2	기준	모든 배포작업의 상태 및 이력은 문서로 기록하고 관리해야 한다.
	설명	<ul style="list-style-type: none"> ○ 1~2등급 정보시스템은 배포작업의 이력 관리를 위하여 형상관리시스템(SVN 등 형상관리도구, ITSM 등)을 활용하여 체계적으로 관리한다. ○ 3~4등급 정보시스템은 표준운영절차로 운영하며, 이를 지원하는 시스템이 없는 경우 배포정보를 관리대장 등에 기록·관리한다(권고).
정책 3	기준	모든 배포 작업은 정상 동작 여부를 검증하는 테스트를 수행해야 한다.
	설명	<ul style="list-style-type: none"> ○ 변경 관련 주요 기능을 테스트하고 변경 사항이 시스템에 미치는 영향을 최소화하여 안정적인 서비스를 제공한다. <ul style="list-style-type: none"> - 기능 검증을 위한 단위테스트, 통합테스트, 성능테스트 등을 수행 - 운영서버 배포 후 운영기관 담당자(변경요청자)의 인수테스트 수행
정책 4	기준	모든 배포작업은 원상복구계획을 배포계획에 포함하여 관리해야 한다.
	설명	<ul style="list-style-type: none"> ○ 배포실패 발생 시 작업 결과를 상세히 기록하고, 장애관리로 이관한다. ○ 원상복구계획의 절차에 따라 복구를 수행한다. <ul style="list-style-type: none"> - 배포 실패 또는 문제 발생 시 사전 정의된 원상복구절차를 통해 즉시 복구 - 원상복구 시 시스템 및 데이터 정합성을 보장할 수 있도록 검증 절차 포함

다. 용어 정의

용어	설명
배포 승인	변경 관리 위원회(CAB) 또는 관련 부서에서 배포를 승인하는 절차
배포 요청	변경 사항을 운영 서버에 반영하기 위한 요청 문서
개발 환경	변경 작업자가 소스코드를 작성하고 단위테스트를 수행하는 로컬 또는 서버 환경
테스트 환경	개발 완료된 릴리즈의 기능과 성능을 검증하기 위한 별도의 환경
배포 검증	배포 후 정상 작동 여부를 확인하는 절차
롤백 (Rollback)	배포 실패 시 기존 상태로 복구하는 절차
사전 검증 테스트	배포 전 변경 요청사항 구현의 완전성을 검토하는 과정

라. 역할 및 책임

○ 배포관리 절차를 수행하는 역할과 책임은 다음과 같다.

구분	내용	
운영기관 (응용프로그램의 운영관리에 최종 책임지는 기관)	관리자	<ul style="list-style-type: none"> ○ 정보시스템 관련 담당자의 상위 책임자 또는 부서장 ○ 배포관리 정책 결정 ○ 배포 리스크 평가 등 관리 감독 ○ 배포 후 검증 결과 검토 및 최종 승인 ○ 배포 후 운영 안정화 방안 수립
	담당자	<ul style="list-style-type: none"> ○ 배포작업 대상 정보시스템 업무 담당자가 역할 수행 ○ 배포계획의 적정성 검토 <ul style="list-style-type: none"> - 배포계획 이관 승인 포함 ○ 배포 결과 검토 및 이슈 보고 ○ 배포 후 서비스 상태 점검 및 문제 발생 시 보고
운영자 (위탁기관 또는 운영 사업자)	운영관리	<ul style="list-style-type: none"> ○ 운영기관과의 계약을 통해 정보시스템의 운영과 배포작업을 담당하는 위탁기관 또는 운영 사업자 ○ 배포 요청에 따른 세부 계획 수립 및 일정 관리 ○ 배포 대상 시스템 및 애플리케이션 검토 및 준비 ○ 배포계획의 적정성 검토 ○ 배포계획 수립과 배포관련 준비작업 <ul style="list-style-type: none"> - 배포 자동화 도구(Jenkins 등) 설정 및 관리 ○ 배포 전 시스템 백업 및 복구 계획 수립 ○ 배포작업 수행 <ul style="list-style-type: none"> - 배포계획에 따라 작업 수행 완료 후 테스트 및 서비스 확인 ○ 배포 진행 상황 모니터링 ○ 배포 후 시스템 성능 점검 ○ 배포 후 형상정보에 대한 현행화 작업
	유지보수	<ul style="list-style-type: none"> ○ 배포계획 수립과 배포관련 준비작업 <ul style="list-style-type: none"> - 배포 스크립트 작성 및 검증 - 배포 파일 및 스크립트 무결성 검증 및 오류 수정 ○ 배포작업 수행과 결과 보고 ○ 배포 후 시스템 장애 발생 시 긴급 복구 및 롤백 수행 ○ 배포 후 시스템 성능 저하 및 오류 수정 ○ 배포 후 형상정보에 대한 현행화 작업
	테스트	<ul style="list-style-type: none"> ○ 배포 전/후 기능 테스트 및 성능 검증 ○ 배포 후 서비스의 정상 작동 여부 확인 ○ 테스트 결과 보고서 작성 및 이슈 보고

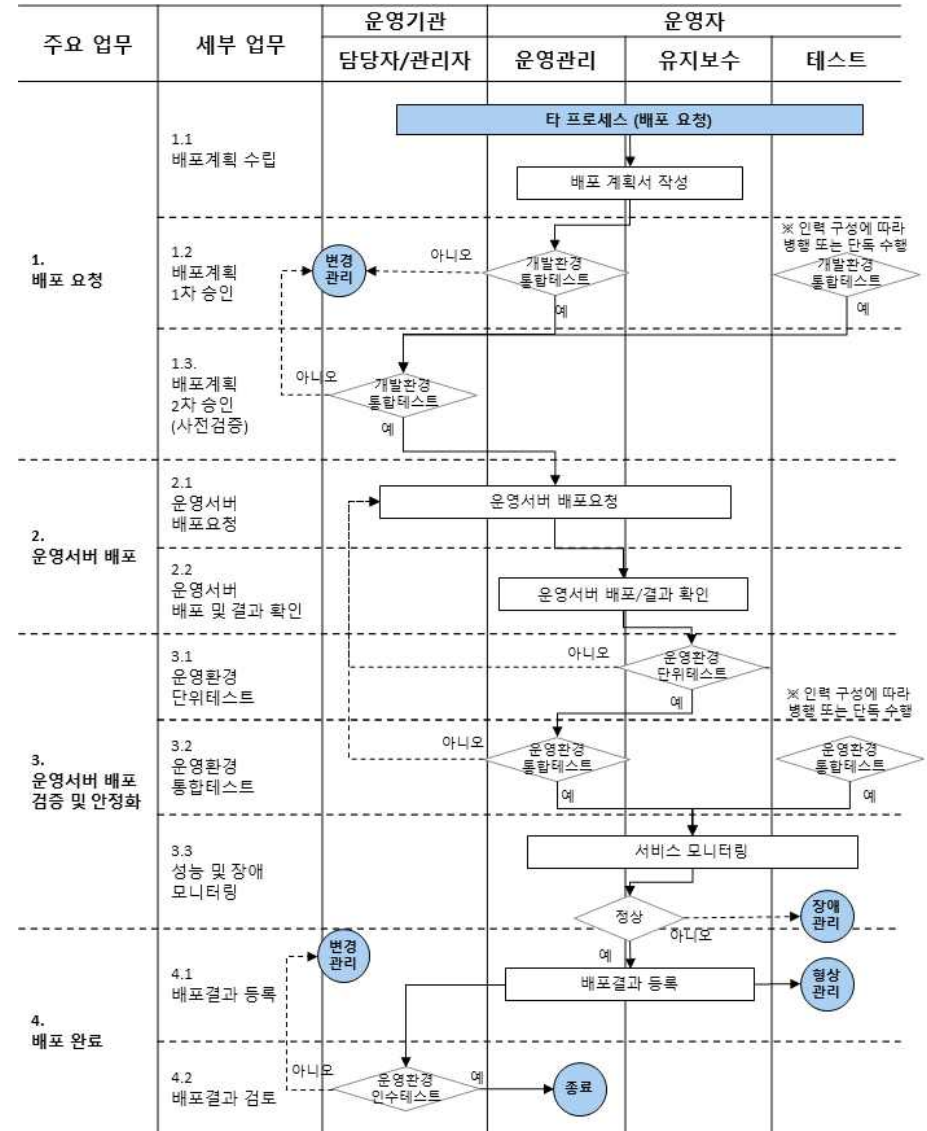
마. 표준절차 흐름도

○ 배포관리 절차는 아래와 같은 주요 업무와 수행 활동으로 구성된다.

1) 주요 업무

주요 업무	세부 업무	수행 활동
1. 배포요청	1.1. 배포계획 수립	○ 운영자는 변경된 릴리스의 서비스 영향을 분석하고 테스트 시나리오를 포함하여 배포계획을 수립한다.
	1.2. 배포계획 1차 승인	○ 운영관리자는 테스트환경에서 개발 완료된 릴리스의 통합테스트를 수행하고 배포계획을 1차 검토한다. ※ 테스트 전문 인력이 있는 기관에서는 테스트 관리자가 테스트 시나리오를 기반으로 테스트 수행
	1.3. 배포계획 2차 승인 (사전검증)	○ 운영기관 담당자(변경요청자)는 1차 배포계획 검토 결과를 확인하고 테스트환경에서 사전검증 통합테스트를 수행 후 보완요청 또는 운영 배포계획을 승인한다.
2. 운영서버 배포	2.1. 운영서버 배포요청	○ 승인된 배포계획에 따라 운영서버 배포를 요청한다.
	2.2. 운영서버 배포 및 결과 확인	○ 운영자(배포담당자)는 개발된 릴리스를 운영서버에 반영한다. ○ 배포 중 오류 발생 등 배포작업 결과를 확인한다.
3. 운영서버 배포검증 및 안정화	3.1. 운영환경 단위테스트	○ 유지보수 담당자는 단위테스트를 수행한다. - 배포된 릴리스 기능의 정상동작여부를 운영환경에서 확인
	3.2. 운영환경 통합테스트	○ 운영관리자는 통합테스트를 수행한다. - 변경 요구사항 구현의 완전성을 운영환경에서 검증 ※ 테스트 전문 인력이 있는 기관에서는 테스트 관리자가 테스트 시나리오를 기반으로 테스트 수행
	3.3. 성능 및 장애 모니터링	○ 운영자는 배포 후 시스템 성능을 모니터링하고 장애 발생 여부를 점검한다. - 장애 발생 시 신속히 대응하고 장애관리 절차로 이관 ○ 배포작업 실패 시에는 롤백을 실행하여 시스템을 복구한다. ○ 운영자는 현상항목 업데이트를 실시하고 배포완료 보고서를 작성한다.
4. 배포 완료	4.1. 배포 결과 등록	○ 운영관리자는 배포결과를 검토하고 ITSM에 등록한다.
	4.2. 배포결과 검토 (인수테스트)	○ 운영기관 담당자(변경요청자)는 배포작업 완료 여부를 확인하고, 인수테스트를 수행한 후 배포결과를 승인한다.
	4.3. 배포 종료	○ 배포 과정에서 도출된 개선 사항을 분석하고 문서화하여 향후 배포작업에 반영한다.

2) 수행주체별 표준절차 흐름도



바. 세부 수행 절차

1) 절차 및 역할과 책임(R&R : Role and Responsibility)

(●: 정, ○: 부)

단계	세부 절차	세부 수행 내용	운영 기관	운영 관리	유지 보수	테스트
1. 배포 계획 수립	1.1. 배포 계획 수립	- 운영자(운영관리 또는 유지보수 담당자)는 배포 계획서를 작성하여 ITSM 시스템에 등록한다. - 계획서에는 배포 대상 시스템, 배포 일정 및 서비스 영향도, 테스트 시나리오, 원복 계획 등을 상세히 기술한다.		●	●	
	1.2. 배포 계획 1차 승인	- 운영관리자는 테스트환경에서 개발된 릴리스의 통합테스트를 수행한다. - 테스트 시나리오에 따라 통합테스트를 수행하고 보완요청 또는 배포계획을 승인한다.		●	○	●
	1.3. 배포 계획 2차 승인 (사전검증)	- 운영기관 담당자(변경요청자)는 1차 배포계획 검토 결과를 확인한다. - 테스트 시나리오에 따라 사전검증 통합테스트를 수행하고 보완요청 또는 배포계획을 승인한다. - 연계시스템에 서비스 영향이 발생할 것으로 예상되는 경우 배포계획을 관련기관에 공지한다.	●	●		
2. 운영서버 배포	2.1. 운영서버 배포 요청	- 승인된 배포계획에 따라 운영서버 배포를 요청한다. ※ 배포 작업을 타기관에서 하는 경우(예. 국정자원) 배포계획서를 이관하고 운영서버 반영 작업을 요청한다.	●	●	●	
	2.2. 운영서버 배포 및 결과확인	- 배포 중 오류 발생 등 진행 상황을 모니터링하고 배포 작업 결과를 확인한다. - 배포 작업 중 오류(Incident) 발생 시 배포계획에 명시된 원복계획에 따라 복구를 수행한다.		●	●	

단계	세부 절차	세부 수행 내용	운영 기관	운영 관리	유지 보수	테스트
3. 운영서버 배포검증 및 안정화	3.1. 운영환경 단위테스트	- 유지보수 담당자는 운영환경 단위테스트를 수행한다. - 단위테스트를 통해 배포된 릴리스 기능의 정상동작여부를 확인한다.		○	●	
	3.2. 운영환경 통합테스트	- 운영관리자는 테스트 시나리오를 기반으로 운영환경 통합테스트를 수행한다. - 실제 운영환경과 유사한 테스트 데이터를 활용하여 운영환경 통합테스트를 수행한다. - 통합테스트를 통해 변경 요구사항 구현의 완전성을 검증한다.	○	●	○	●
	3.3. 성능 모니터링 및 장애점검	- 운영자는 배포 후 시스템 성능을 모니터링하고 장애 발생 여부를 점검한다. - 장애 발생 시 신속히 대응하고 장애관리 절차로 이관한다. - 장애 등으로 배포 작업이 실패할 경우 롤백을 실행하여 시스템을 복구하고 진행 상황을 모니터링 한다.		●	●	●
4. 배포 완료	4.1. 배포 결과 등록	- 유지보수 담당자는 형상관리도구에 형상항목 업데이트를 실시하고 배포완료 보고서를 작성한다. - 운영관리자는 변경계획, 배포계획, 배포결과 등이 일치하는지 검토하고 ITSM에 등록한다.		●	●	
	4.2. 배포 결과 검토 (인수테스트)	- 운영기관 담당자(변경요청자)는 배포작업 완료 여부를 확인하고, 인수테스트를 수행한다. - 인수테스트 결과에 따라 배포결과를 승인 또는 변경관리 절차로 이관한다. - 변경계획의 수정이 필요한 경우 변경계획 수립 절차로 이동한다.	●	●	○	○
	4.3. 배포 종료	- 운영관리자는 운영환경 인수테스트 결과를 확인하고 배포 종료를 승인한다. - 배포 과정에서 도출된 개선 사항을 분석하고 문서화하여 향후 배포작업에 반영한다.		●	●	

2) 고려사항

○ N/A

사. 핵심성과지표 (KPI : Key Performance Indicator)

- 배포 프로세스 관리지표를 도출하여 운영 품질 관리를 목표로 하며, 본 절차서에서는 KPI 표준안을 제시하고 개별기관별 운영 상황에 맞추어 조정하여 지표 관리한다.

KPI 항목	설명	측정 방법	목표 기준
배포 성공률 (Deployment Success Rate)	배포가 장애 없이 정상적으로 완료된 비율	(성공한 배포 수 / 전체 배포 수) × 100	≥ 98%
배포 장애율 (Deployment Failure Rate)	배포 후 장애가 발생한 비율	(장애 발생 배포 수 / 전체 배포 수) × 100	≤ 2%
배포 롤백 발생률 (Rollback Rate)	배포 후 롤백이 수행된 비율	(롤백 배포 수 / 전체 배포 수) × 100	≤ 1%
배포 후 결함 발생률 (Post-Deployment Defect Rate)	배포 후 발견된 기능적 결함 비율	(배포 후 발견된 결함 수 / 전체 배포 수) × 100	≤ 3%
배포 후 평균 복구 시간 (Mean Time to Recover, MTTR)	배포 중 장애 발생 시 정상 복구까지 소요된 평균 시간	장애 발생 시간 ~ 정상화 시간 측정	≤ 60분

아. 수행 검증

1) 검증 방법

- 검증 체크리스트의 기준 항목으로 표준운영절차의 준수여부와 이행점검을 수행한다.
- 개별기관 내 자체 프로세스 검증자는 내부 감사자의 자격 또는 ITIL에 대한 충분한 이해를 가진자가 수행한다. (ITIL 관련 자격 권고)
- 점검 결과는 대외 감사/진단 시 내부 점검 활동의 결과물로 활용할 수 있다.

2) 검증 항목

세부 절차	체크 항목	정성 평가	증적 체크
배포 계획 수립	- 배포계획은 서비스 영향 분석을 수행한 결과를 포함하고 있습니까?	적합/ 부적합	• 배포계획서 - 서비스 영향 분석 결과
	- 배포계획은 테스트 계획을 포함하고 있습니까?		• 배포계획서 - 테스트계획서
	- 배포계획은 2단계(운영관리자→운영기관담당자) 승인을 수행하고 있습니까?		• ITSM 내 승인 이력
	- 배포계획에는 작업 실패에 대비한 원복계획/절차를 수립하여 포함하고 있습니까?		• 원복계획서 - 배포계획서 내 포함 가능
운영서버 배포	- 배포계획은 테스트환경에서 테스트 완료 후 운영서버에 반영하도록 관리되고 있습니까?		• ITSM 프로세스 - 테스트결과서
	- 모든 배포작업의 상태 및 이력은 문서로 기록하고 관리되고 있습니까?		• ITSM 프로세스 - 배포이력
운영서버 배포검증	- 배포 후 기능의 정상동작 여부를 확인하기 위한 테스트를 수행하고 있습니까?		• 테스트계획 및 테스트결과
	- 배포 후 성능 및 장애 모니터링을 수행하고 장애 발생 시 장애관리 절차로 이관하여 관리하고 있습니까?		• 모니터링이력 • 장애관리이력

자. 관리기준 및 예시

1) 배포관리 산출물 예시

배포계획			
변경ID		작성자	
배포유형		서비스영향도	
배포계획			
테스트시나리오			
원상복구계획			

배포승인			
승인자		승인상태	
승인의견			

배포요청			
변경ID		요청자	
배포대상		배포요청일시	
긴급여부		서비스중단여부	
배포요청 항목	형상ID	경로	파일명
비 고			

배포결과			
작업시작일시		작업종료일시	
작업결과		작업자	
테스트결과		검증자	
오류발생사항			
모니터링결과			

개선사항	
내용	

4. 테스트 관리 절차서

가. 개요

1) 목적

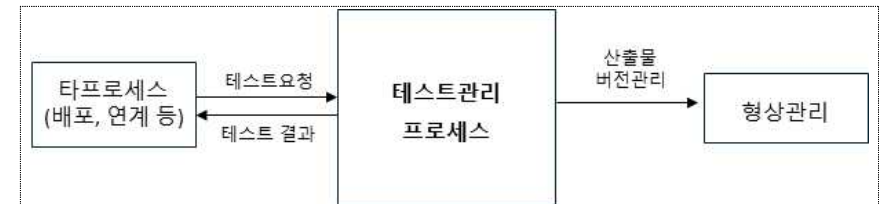
- 응용프로그램의 변경 기능이 정상적으로 동작하는지 확인하고, 응용프로그램 운영관리 요구 사항에 부합하는 서비스가 제공되는지 검증하기 위한 절차를 표준화하여 정보시스템의 품질을 보증한다.

2) 적용 범위

- 테스트관리 절차는 서비스에 영향을 미치는 변경이 일어나는 운영관리에 적용된다.

3) 관련 업무 절차

- 연관 선/후행 업무



- 시작/종료/증적(Output) 조건

주요 업무	수행 업무
프로세스 시작 조건	응용프로그램 기능 변경/신규 개발, 타 시스템(데이터 포함) 연계 변경/신규 연계 등의 테스트를 위해 수행하는 일체의 요청
프로세스 종료 조건	테스트 요청의 반려 테스트 처리 종료
증적(Output)	테스트 요청서, 테스트 계획서, 테스트 결과서(단위/통합/성능/인수 등) ※ ITSM 시스템을 사용하는 경우 시스템내 이력으로 대체

나. 관리 정책

1) 정의

○ 응용프로그램 테스트 관리 절차의 운영에 있어서 필히 준수해야 할 정책 기준을 제공

2) 정책 기준

정책	설명	
정책 1	기준	테스트환경은 실제 운영환경과 최대한 유사하게 구축해야 한다.
	설명	○ 테스트환경은 운영환경에서 발생할 수 있는 문제를 사전에 식별하고 대응할 수 있도록 시스템 구성, 설정 등 최대한 유사하게 구성해야 한다. - 유사환경 : OS버전, DB버전, WAS버전 등 운영환경과 동일하게 구성 - 물리적 자원 확보에 제약이 있을 경우, 동일 서버 내 파티션 분리를 통한 테스트/운영환경 구성 ※ 1등급 시스템 테스트환경 구성 필수, 2등급 시스템 권고
정책 2	기준	모든 테스트계획은 테스트 케이스와 시나리오를 포함하여 관리해야 한다.
	설명	○ 요구사항 구현의 완전성과 서비스 품질의 적합성을 보증하기 위한 테스트 케이스와 시나리오를 포함한다. ○ 단위테스트는 테스트가 가능한 최소 기능 단위로 작성한다. ○ 통합테스트는 인터페이스 단위로 작성한다. ※ 테스트 수행을 위한 테스트 데이터 사전 확보 필요
정책 3	기준	응용프로그램 기능개선으로 소스코드에 변경이 발생하는 경우 제3자에 의한 테스트를 수행해야 한다.
	설명	○ 단위테스트 : 변경작업자가 구현한 기능의 정상 동작 여부를 운영관리자가 검증 ○ 통합테스트 : 단위테스트를 통과한 릴리스를 테스트환경에 반영해서 운영기관 담당자가 서비스 품질 기준 충족 여부를 검증 ○ 인수테스트 : 운영기관 담당자와 변경요청자가 상이한 경우 변경요청자가 변경요구사항 구현 여부를 검증
정책 4	기준	모든 테스트 활동의 상태 및 이력은 문서로 기록하고 관리해야 한다.
	설명	○ 1~2등급 정보시스템은 응용프로그램 표준운영절차의 체계적인 관리를 위하여 테스트정보를 시스템으로 관리해야 한다. - 관리 정보: 테스트 절차별 수행자 및 테스트 결과 ○ 3~4등급 정보시스템은 표준운영절차로 운영하며, 이를 지원하는 시스템이 없는 경우 테스트정보를 관리대장 등에 기록·관리해야한다.
정책 5	기준	연계서비스에 영향을 미치는 변경이 발생하는 경우 연관된 시스템의 서비스 영향을 고려한 테스트활동을 수행해야 한다.
	설명	○ 변경작업자는 연계서비스 영향도를 파악하여 운영관리자와 운영기관 담당자에게 연계서비스 테스트계획서를 제공한다. ○ 운영관리자는 운영서버 배포 후 연계서비스 테스트를 수행하고, 정상 동작 여부를 확인하여 결과 기록 및 운영기관 담당자에게 보고한다.

다. 용어 정의

용어	설명
테스트관리 (Test Management)	시스템 변경 사항이 운영 환경에서 정상적으로 동작하는지 확인하고 품질을 유지하는 활동
단위 테스트 (Unit Test)	개별 모듈 또는 기능 단위로 정상 동작 여부를 검증하는 테스트
통합 테스트 (Integration Test)	여러 모듈 또는 시스템 간 연계를 검증하는 테스트
성능 테스트 (Performance Test)	응용프로그램이 예측된 사용 조건에서 정의된 성능 요건(응답 속도, 처리량, 자원 사용량 등)을 충족하는지 확인하는 테스트
부하 테스트 (Load Test)	일반적인 사용자 부하에서 시스템의 성능을 측정하는 테스트
스트레스 테스트 (Stress Test)	최대 부하를 초과하는 상황에서 시스템의 안정성을 확인하는 테스트
인수 테스트 (UAT, User Acceptance Test)	최종 사용자가 직접 시스템을 사용하면서 기능을 검증하는 테스트
배포 전 검증 테스트 (Pre-Deployment Testing)	운영 환경에서 변경 사항을 반영하기 전 수행하는 최종 검증
배포 후 검증 테스트 (Post-Deployment Testing)	운영 환경에서 변경 사항이 정상적으로 작동하는지 확인하는 테스트
테스트 보고서 (Test Report)	테스트 수행 결과, 오류 발생 내역, 개선 사항을 기록하는 문서

라. 역할 및 책임

○ 테스트관리 절차를 수행하는 역할과 책임은 다음과 같다.

구분	내용	
운영기관 (응용프로그램의 운영관리에 최종 책임지는 기관)	관리자	○ 정보시스템 관련 담당자의 상위 책임자 또는 부서장 ○ 테스트 결과 최종 검토 및 승인
	담당자	○ 변경작업 대상 정보시스템 업무 담당자가 역할 수행 ○ 테스트계획의 적정성 검토 - 테스트 시나리오 및 케이스 포함 ○ 배포 전 테스트환경 통합테스트 수행 ○ 배포 후 운영환경 인수테스트 수행 ○ 테스트 수행 결과 검토
운영자 (위탁기관 또는 운영 사업자)	운영관리	○ 운영기관과의 계약을 통해 정보시스템의 운영과 테스트 작업을 담당하는 위탁기관 또는 운영 사업자 ○ 테스트계획서 작성 ○ 테스트 시나리오 및 케이스 작성 ○ 테스트 환경 구성 및 테스트 데이터 준비 ○ 테스트 도구 설정 및 관리 ○ 테스트 일정 수립 및 진행 상황 보고 ○ 통합테스트 수행 ○ 통합테스트 결과 보고서 작성 ○ 테스트 수행 중 발생한 이슈 모니터링 및 대응 ○ 단위테스트 수행 결과 검토
	유지보수	○ 단위테스트 수행 ○ 단위테스트 결과 보고서 작성 ○ 테스트 중 발견된 결함 분석 및 수정
	테스트	○ 배포 전/후 기능 테스트 및 성능 검증 ○ 배포 후 서비스의 정상 작동 여부 확인 ○ 테스트 결과 보고서 작성 및 이슈 보고

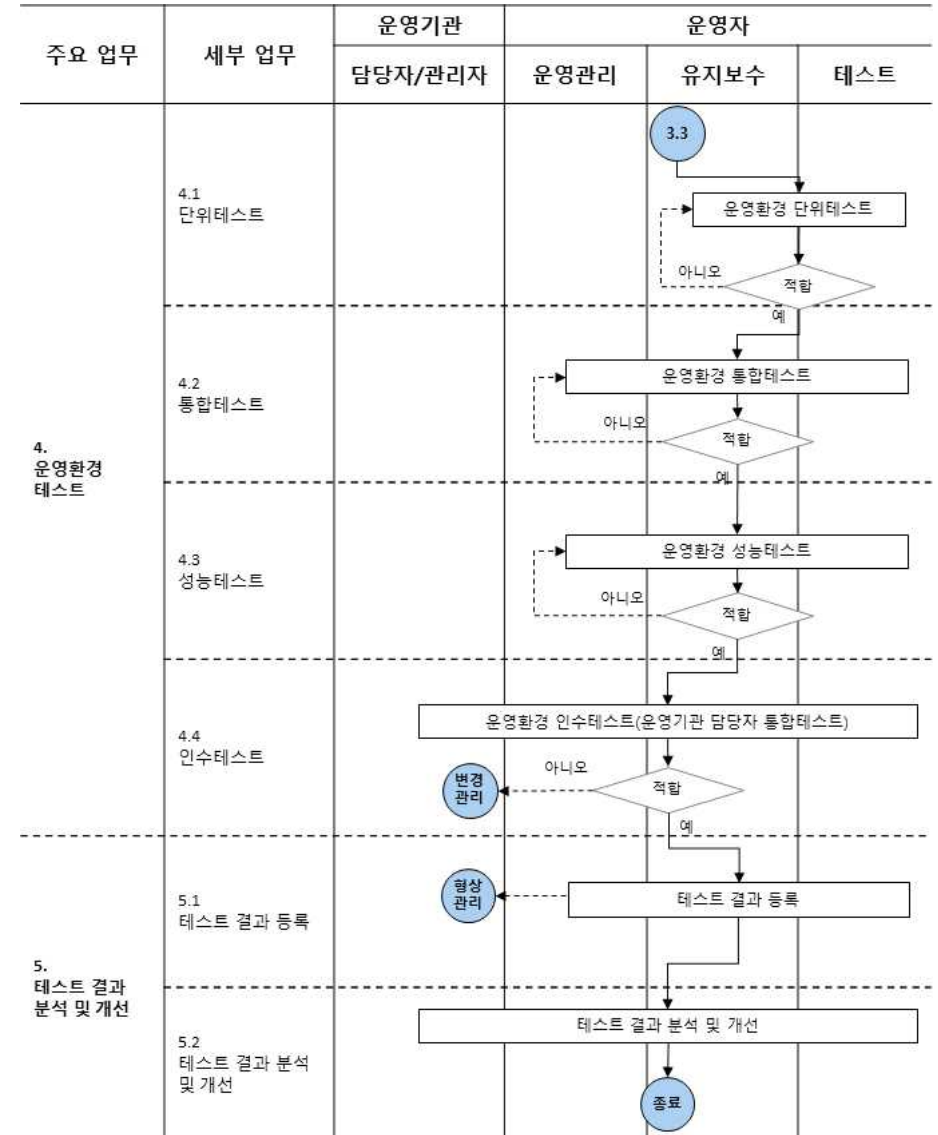
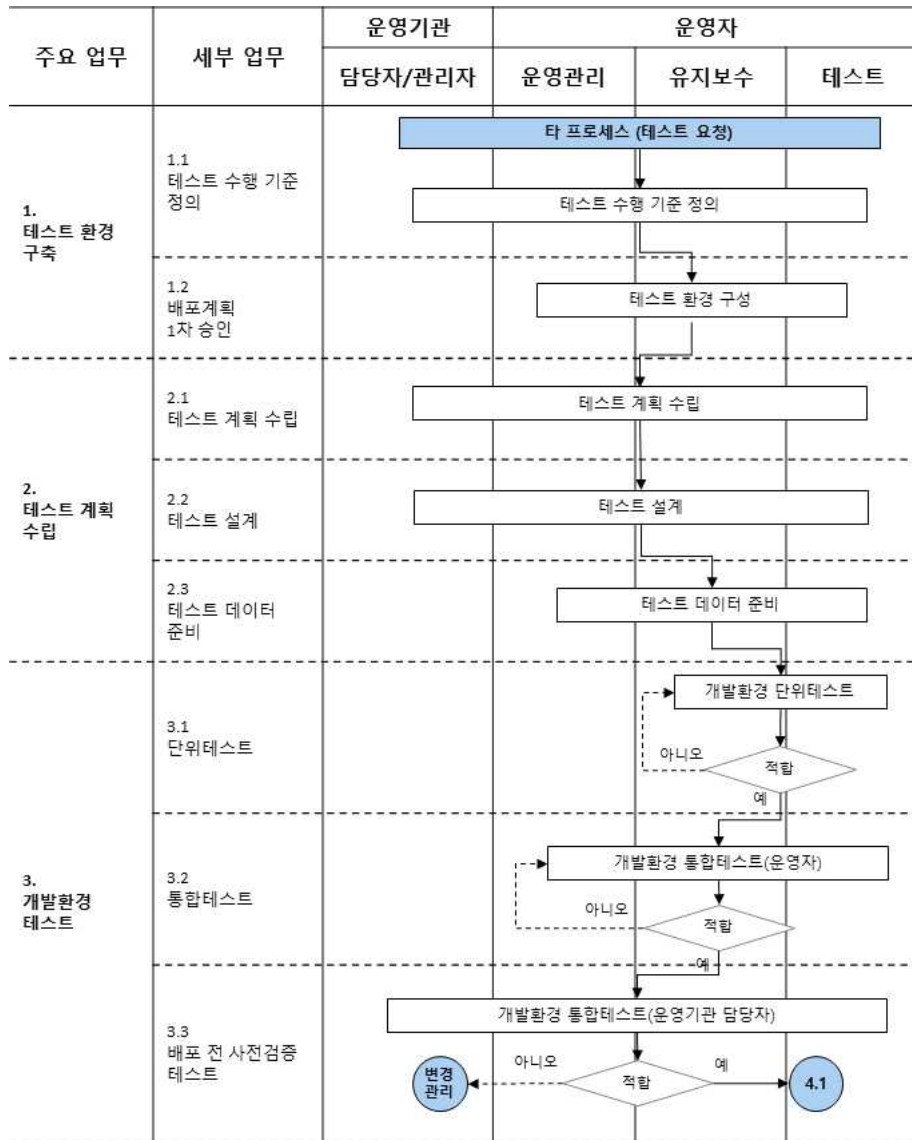
마. 표준절차 흐름도

○ 테스트관리 절차는 아래와 같은 주요 업무와 수행절차들로 구성된다.

1) 주요 업무

주요 업무	세부 업무	수행 업무
1. 테스트 환경 구축	1.1. 테스트 수행 기준 정의	○ 테스트 대상 및 범위, 수행인력 등 변경 사항의 품질 기준 충족여부를 검증하기 위한 기준을 정의한다.
	1.2. 테스트 환경 구성	○ 테스트 환경은 실제 운영환경과 최대한 유사하게 구성한다.
2. 테스트 계획 수립	2.1. 테스트 계획 수립	○ 테스트 수행 기준에 따라 테스트 유형을 결정하고 테스트 일정 계획을 수립한다.
	2.2. 테스트 설계	○ 변경 기능이 정상 동작하는지 확인하기 위한 테스트 케이스를 작성하고, 서비스의 정상화 등을 검증하기 위한 테스트 시나리오를 설계한다.
	2.2. 테스트 데이터 준비	○ 테스트 시나리오에 기반하여 실제 운영환경과 유사한 상황을 가정하고 테스트 수행에 필요한 테스트 데이터를 준비한다.
3. 개발환경 테스트	3.1. 단위테스트	○ 응용프로그램의 소스코드가 변경되는 경우 유지보수 담당자나 운영관리자, 또는 제3자(테스터 등)가 단위 테스트를 수행한다.
	3.2. 통합테스트	○ 기능 변경이 타 시스템이나 서비스에 영향을 미치는 경우 운영관리자 또는 제3자(테스터 등)가 통합테스트를 수행한다.
	3.3. 배포 전 사전검증 테스트	○ 운영서버에 배포 전 운영기관 담당자(변경요청자)는 테스트환경에서 배포 전 사전검증 테스트(통합테스트)를 수행한다. ※ 연계서비스에 변경이 발생하는 경우 배포 전 사전검증 테스트에 연계 관련 시스템 담당자 참여
4. 운영환경 테스트	4.1. 단위테스트	○ 유지보수 담당자는 변경된 릴리즈가 운영서버에 배포된 후 단위테스트를 수행하고 테스트 케이스별 테스트 결과를 작성한다.
	4.2. 통합테스트	○ 운영환경에서 테스트 시나리오에 따라 통합테스트를 수행하고 결과를 작성한다.
	4.3. 성능테스트	○ 시스템 성능에 영향을 미치는 변경작업은 업무집중기간 최대부하치를 기준으로 성능테스트(스트레스 테스트)를 수행하고 결과가 성능 기준에 부합하는지 평가한다.
	4.4. 인수테스트	○ 운영기관 담당자(변경요청자)는 운영환경에서 인수테스트를 수행하고, 변경요구사항 구현의 완전성을 평가한다.
5. 테스트 결과 분석 및 개선	5.1. 테스트 결과 등록	○ 변경 요구사항 구현결과가 서비스 품질기준에 부합하는지 확인하고 테스트 결과서를 작성한다.
	5.2. 테스트 결과 분석 및 개선	○ 테스트 결과를 분석하고 향후 테스트 작업에 반영한다.

2) 수행주체별 표준절차 흐름도



바. 세부 수행 절차

1) 절차 및 역할과 책임(R&R : Role and Responsibility)

(●: 정, ○: 부)

단계	세부 절차	세부 수행 내용	운영 기관	운영 관리	유지 보수	테스트
1. 테스트 환경 구축	1.1. 테스트 수행 기준 정의	- 운영관리자(또는 테스트관리자)는 변경요청서, 변경계획서, 배포계획서 등을 분석하여 테스트 요구사항을 도출한다. - 운영관리자는 프로그램 소스코드, DB 스크립트, 시스템 성능 등 테스트 대상 및 범위, 테스트 수행 인력 등을 결정한다.	○	●	●	●
	1.2. 테스트 환경 구성	- 운영관리자는 OS, DB, WAS 버전 등을 최대한 운영 환경과 유사하게 테스트 환경을 구성한다. - 운영관리자는 테스트 자동화 도구(Unit 등) 활용을 위한 환경 설정을 지원한다.		●	●	○
2. 테스트 계획 수립	2.1. 테스트 계획 수립	- 운영관리자는 테스트 수행기준에 따라 테스트 유형(단위, 통합, 성능 등)을 결정한다. - 테스트 일정 계획을 수립하고, 담당자를 지정한다.	○	●	●	●
	2.2. 테스트 설계	- 운영자(운영관리자 또는 유지보수 담당자)는 테스트 케이스와 테스트 시나리오를 작성한다. - 단위테스트는 예상 출력값을 포함하여 테스트가 가능한 최소 단위로 작성한다. - 통합테스트는 서비스 영향 검토 범위를 포함하는 인터페이스 단위로 작성한다. - 운영기관 담당자(변경요청자)는 테스트 시나리오 검토 후 테스트 계획을 승인한다.	○	●	●	●
	2.3. 테스트 데이터 준비	- 테스트 계획에 따라 테스트 수행에 필요한 테스트 데이터를 준비한다.		●	●	●

단계	세부 절차	세부 수행 내용	운영 기관	운영 관리	유지 보수	테스트
3. 개발환경 테스트	3.1. 단위테스트	- 유지보수 담당자(또는 운영관리자, 제3자, 테스터 등)는 개발환경에서 변경 기능의 단위테스트를 수행한다. - 테스트 케이스의 예상 결과값과 테스트 수행 결과값을 비교하여 정상동작여부를 확인한다.			●	●
	3.2. 통합테스트	- 운영관리자(또는 제3자, 테스터 등)는 테스트환경에서 테스트 시나리오에 따라 통합테스트를 수행한다. - 변경 범위가 다른 기능에 영향을 미치는 경우 영향받는 트랜잭션 단위의 정상 완료 여부를 확인한다.		●	○	●
	3.3. 배포 전 사전검증 테스트	- 운영기관 담당자(변경요청자)는 테스트환경에서 배포 전 사전검증 테스트(통합테스트)를 수행하여 주요 기능의 정상동작 여부를 확인한다. - 변경 범위가 연계시스템에 영향을 미치는 경우 연계시스템 담당자가 연계서비스의 정상동작 및 데이터 정합성을 검증한다.	●	●	○	●
4. 운영환경 테스트	4.1. 단위테스트	- 유지보수 담당자(또는 제3자, 테스터 등)는 배포 후 운영환경에서 단위테스트를 수행하고 테스트 결과를 작성한다.			●	●
	4.2. 통합테스트	- 운영관리자(또는 제3자, 테스터 등)는 운영환경에서 테스트 시나리오에 따라 통합테스트를 수행하고 결과를 작성한다.		●	●	●
	4.3. 성능테스트	- 시스템 성능에 영향을 미치는 변경작업은 배포 후 성능테스트를 수행하고 결과가 성능 기준에 부합하는지 평가한다. - 성능테스트(스트레스 테스트) 임계치는 업무집중기간 최대부하치를 기준으로 한다.		●	○	●
	4.4. 인수테스트	- 운영기관 담당자(변경요청자)는 운영환경에서 인수테스트를 수행하고, 변경요구사항 구현의 완전성을 평가한다.	●	○		○
5. 테스트 결과 분석 및 개선	5.1. 테스트 결과 등록	- 운영관리자는 테스트 수행 내역 및 오류 발생 사항을 ITSM에 등록한다. - 테스트 결과 산출물을 형상관리시스템에 등록한다.		●	●	●
	5.2. 테스트 결과 분석 및 개선	- 테스트 결과를 검토하고 분석하여 향후 테스트 작업에 반영한다.	○	●		●

2) 고려사항

○ N/A

사. 핵심성과지표 (KPI : Key Performance Indicator)

- 테스트관리 프로세스 관리지표를 도출하여 운영 품질 관리를 목표로 하며, 본 절차서에서는 KPI 표준안을 제시하고 개별기관별 운영 상황에 맞추어 조정하여 지표 관리한다.

KPI 항목	설명	측정 방법	목표 기준
테스트 성공률 (Test Success Rate)	테스트 수행 중 오류 없이 성공한 비율	(성공 테스트 수 / 전체 테스트 수) × 100	≥ 95%
테스트 커버리지 (Test Coverage Rate)	테스트 수행이 전체 기능 대비 차지하는 비율	(테스트 수행 가능 수 / 전체 기능 수) × 100	≥ 90%

아. 수행 검증

1) 검증 방법

- 검증 체크리스트의 기준 항목으로 표준운영절차의 준수여부와 이행점검을 수행한다.
- 개별기관 내 자체 프로세스 검증자는 내부 감사자의 자격 또는 ITIL에 대한 충분한 이해를 가진자가 수행한다. (ITIL 관련 자격 권고)
- 점검 결과는 대외 감사/진단 시 내부 점검 활동의 결과물로 활용할 수 있다.

2) 검증 항목

세부 절차	체크 항목	정성 평가	증적 체크
테스트 환경 구축	- 테스트 대상 및 범위, 인력 등 테스트 관리 기준을 정의하고 있습니까?	적합/ 부적합	• 테스트관리 기준
	- 테스트 환경은 실제 운영 환경과 유사하게 구성하고 있습니까?		
테스트 계획 수립	- 테스트계획은 테스트 케이스 및 시나리오를 포함하고 있습니까?		• 테스트계획서 - 테스트 케이스, 테스트 시나리오
	- 실제 운영환경과 유사한 상황을 가정하여 테스트를 수행할 수 있도록 테스트 데이터를 준비하고 있습니까?		
테스트 결과 분석 및 개선	- 테스트 결과 산출물은 형상관리시스템에 등록하여 관리하고 있습니까?		• ITSM내 테스트결과 - 테스트결과서
	- 결과를 검토하고 분석하여 개선하기 위한 활동이 수행되고 있습니까?		

5. 연계 관리 절차서

가. 개요

1) 목적

- 연계 시스템 간 원활한 데이터 흐름과 상호운영성(Interoperability)을 보장하여 서비스의 연속성과 데이터 정합성을 확보하고 변경작업으로 인한 서비스 영향을 최소화하기 위해 표준화된 절차를 정의하여 정보시스템의 품질을 보증한다.

2) 적용 범위

- 연계관리 절차는 행정-공공기관 정보시스템의 연계 서비스를 포함하는 모든 프로세스와 데이터에 적용된다.
 - API 연계 : RESTful, SOAP, UDDI 등
 - 데이터 연계 : CDC(Change Data Capture), DB 링크, ETL 연계, 배치 처리 등
 - 메시지 기반 연계 : AMQP, JMS, Kafka 등

3) 관련 업무 절차

- 연관 선/후행 업무



- 시작/종료/증적(Output) 조건

주요 업무	수행 업무
프로세스 시작 조건	응용프로그램 기능 변경/신규 개발, 타 시스템(데이터 포함) 연계 변경/신규 연계 등의 다양한 이유로 서비스 연계를 위해 수행하는 일체의 요청
프로세스 종료 조건	연계 요청의 반려 연계 처리 종료
증적(Output)	연계 요청서, 테스트 계획서, 연계 완료 보고서, 개선 사항 보고서 ※ ITSM 시스템을 사용하는 경우 시스템내 이력으로 대체

나. 관리 정책

1) 정의

- 응용프로그램 연계 관리 절차의 운영에 있어서 필히 준수해야 할 정책 기준을 제공

2) 정책 기준

정책	설명	
정책 1	기준	표준화된 연계관리 정책을 수립하여 정보보유기관 간 일관성 있는 관리체계를 기반으로 효율적인 연계관리 환경을 지원해야 한다.
	설명	<ul style="list-style-type: none"> ○ 연계정보, 인터페이스 목록 등을 관련기관과 공유하고 변경사항 발생 시 현행화한다. ○ 연계서비스 중단 시 관련 시스템에 공지(공문 등)하고, 관련 시스템의 중단 검토결과 내역을 ITSM에 등록하여 이력을 관리한다. ○ 연계서버 인증서 등 서비스 유효성에 영향을 미치는 라이선스 등의 관리 대장을 관련기관과 공유하고 현행화한다.
정책 2	기준	연계표준을 적용하여 정보보유기관 간 원활한 서비스가 제공될 수 있도록 지원해야 한다.
	설명	<ul style="list-style-type: none"> ○ 응용프로그램 변경작업 시 연계표준 적용, 테스트, 배포 및 모니터링 등 연계시스템을 고려한 표준운영절차를 마련한다. ○ 데이터의 교환, 처리, 저장 및 접근 방식에 대하여 데이터 포맷, 프로토콜, 인터페이스, 데이터 모델 등 표준화된 기술을 제공한다. - 연계서비스는 실시간 전문 방식(SOAP XML, JSON 등)이나 배치방식 등 표준 프로토콜에 기반한 기술을 활용하여 제공한다.
정책 3	기준	연계서비스에 영향을 미치는 점검이나 작업 발생 시 작업계획을 연계관련 기관에 사전 공지해야 한다.
	설명	<ul style="list-style-type: none"> ○ 변경작업자는 연계서비스 영향도를 파악하여 운영관리자와 운영기관 담당자에게 변경 작업계획서를 제공해야 한다. - 연계시스템 변경작업으로 인한 서비스 점검요청 시 작업계획서를 제공하고, 연계 서비스 점검 결과서를 변경작업 결과 산출물에 포함하여 관리 ○ 운영기관 담당자는 관련기관에 변경 작업계획을 공문 등으로 사전 공지한다.
정책 4	기준	연계서비스는 데이터 송수신 양방향에서 모니터링한다.
	설명	<ul style="list-style-type: none"> ○ 연계 송수신 양방향 교차검증 체계를 운영한다. - 데이터 수신기관은 정상 수신 여부를 모니터링하여 이벤트 감지 시 송신측에 알리고 재송신 요청 - 데이터 송신기관에 이벤트 발생 시 수신 서비스 영향도 파악하여 수신 측에 알림

다. 용어 정의

용어	설명
연계 (Integration)	서로 다른 시스템이나 기관 간에 데이터를 효과적으로 공유하고 통합하는 과정으로, 상호작용이 가능한 기술적 방법과 표준이 적용된 연계 모듈(허브, 에이전트, 어댑터 등)을 제공하여, 응용애플리케이션 시스템 간 데이터 송수신이 가능하도록 지원
API (Application Programming Interface)	서로 다른 시스템이 데이터를 교환하기 위한 인터페이스
RESTful API	HTTP 기반의 경량화된 웹 서비스 연계 방식
SOAP (Simple Object Access Protocol)	XML 기반의 표준화된 웹 서비스 프로토콜
ETL (Extract, Transform, Load)	데이터 추출, 변환, 적재를 수행하는 연계 방식
CDC (Change Data Capture)	데이터베이스 변경 사항을 실시간으로 감지하고 연계하는 방식

라. 역할 및 책임

○ 연계관리 절차를 수행하는 역할자의 책임은 다음과 같다.

구분		내용
운영기관 (응용프로그램의 운영관리에 최종 책임지는 기관)	관리자	○ 정보시스템 관련 담당자의 상위 책임자 또는 부서장 ○ 연계 요청의 적합성 판단 ○ 연계 계획 검토 및 승인 등 의사결정
	담당자	○ 연계 작업 대상 정보시스템 업무 담당자가 역할 수행 ○ 연계 계획의 적정성 검토 ○ 연계 시스템 변경에 따른 리스크 평가 및 관리 ○ 연계작업 관련 이해당사자간 조율 및 의사소통 창구 - 정보보유기관 간 유기적 협조체계 관리 포함
운영자 (위탁기관 또는 운영 사업자)	운영관리	○ 운영기관과의 계약을 통해 정보시스템의 운영과 연계작업을 담당하는 위탁기관 또는 운영 사업자 ○ 연계 요구사항 수집 및 세부 분석 - 연계 기술 및 데이터 흐름 설계 ○ 연계 시스템 인터페이스 구성 및 관리 ○ 연계 환경의 정기적 점검 및 성능 최적화 ○ 연계 데이터 흐름 및 프로세스 모니터링 ○ 연계 테스트 및 변경작업 결과 검토 및 승인
	유지보수	○ 연계 개발 후 단위 테스트 수행 ○ 연계 후 시스템 로그 분석 및 성능 점검 ○ 연계 프로세스 변경 및 데이터 오류 수정 ○ 테스트 중 발견된 결함 분석 및 수정
	테스트	○ 연계 후 서비스의 정상 작동 및 성능 확인 ○ 연계 프로세스 성능 및 부하 테스트 수행 ○ 테스트 결과 보고서 작성 및 이슈 보고

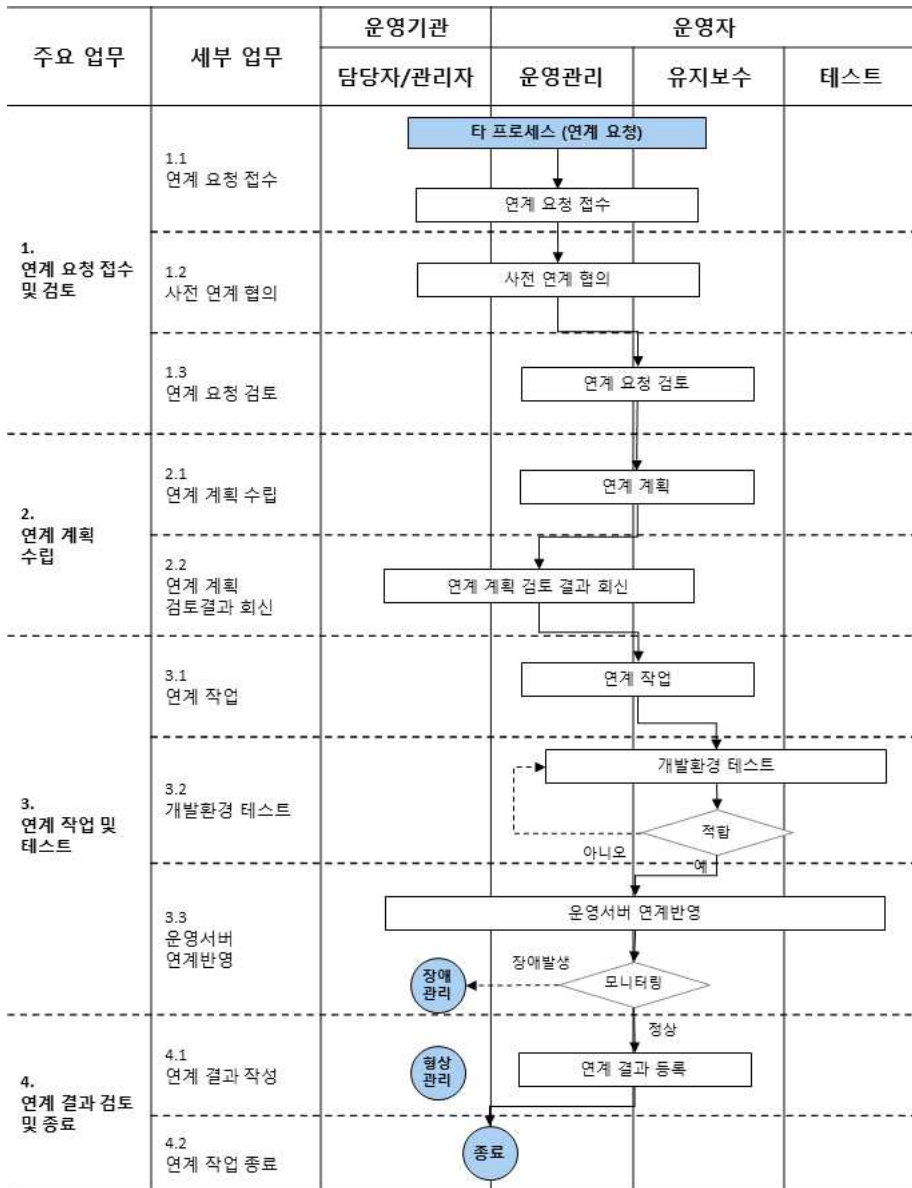
마. 표준절차 흐름도

○ 연계관리 절차는 아래와 같은 주요 업무와 수행절차들로 구성된다.

1) 주요 업무

주요 업무	세부 업무	수행 업무
1. 연계 요청 및 검토	1.1. 연계 요청 접수	○ 변경요청 프로세스나 타 프로세스에서 연계를 요청한다.
	1.2. 사전 연계 협의	○ 연계 요청기관과 사전 연계 협의를 통해 연계 요청 세부 사항을 확인한다.
	1.3. 연계 요청 검토	○ 연계기관 간 환경 및 제약사항을 확인하고 연계 가능 여부를 검토한다.
2. 연계 계획 수립	2.1. 연계 계획	○ 연계 요청기관은 연계 계획서(아래 내용 포함)를 작성하고 연계 대상기관에 검토요청한다. - 연계 계획에는 연계 근거, 연계 정보, 연계 방법 및 주기, 송수신 구분 등
	2.2. 연계 계획 검토결과 회신	○ 연계 대상기관은 연계 계획에 대한 검토결과서를 작성하여 회신한다.
3. 연계 작업 및 테스트	3.1. 연계 작업	○ 운영자는 연계 계획에 따라 연계 작업을 수행한다. ○ 연계 작업은 변경관리 절차(연계 기능 개발, 테스트, 운영서버 반영 등)를 따른다.
	3.2. 개발환경 테스트	○ 연계 시스템 간 테스트를 수행하여 데이터 흐름 및 상호작용이 올바르게 작동하는지 검증한다.
	3.3. 운영서버 연계 반영	○ 개발환경에서 테스트 완료된 연계기능을 운영서버에 반영하고 장애 발생여부를 모니터링한다.
4. 연계 결과 검토 및 종료	4.1. 연계 결과 등록	○ 운영자는 연계 완료 보고서를 작성하고 운영기관 담당자에게 보고한다. ○ 운영자는 변경된 연계정보의 현행화를 실시한다.
	4.2. 연계 작업 종료	○ 운영기관 담당자는 연계 작업이력을 확인하여 작업 정상 여부를 확인하고 연계 작업 종료를 승인한다.

2) 수행주체별 표준절차 흐름도



바. 세부 수행 절차

1) 절차 및 역할과 책임(R&R : Role and Responsibility)

(●: 정, ○: 부)

단계	세부 절차	세부 수행 내용	운영기관	운영관리	유지보수	테스트
1. 연계 요청 접수 및 검토	1.1. 연계 요청 접수	- 연계 요청기관은 연계 요청서를 작성하고 ITSM 시스템에 등록한다. - 연계요청서에는 연계 근거, 연계 목적, 연계 항목, 연계 일정 등 연계 요구 사항을 상세히 기술한다.	●	●	●	
	1.2. 사전 연계 협의	- 연계 요청기관과 연계 대상기관 간 사전 연계 협의를 통해 연계 요청 세부 사항을 확인한다.	●	●	●	
	1.3. 연계 요청 검토	- 운영자는 연계 요청서를 검토하고 연계 환경 및 제약사항을 검토한다. - 연계 목적 적합 여부 및 예상 트래픽의 서비스 영향도 등 연계 가능성을 고려하여 연계 진행 여부를 결정한다.	○	●	●	
2. 연계 계획 수립	2.1. 연계 계획	- 운영자는 연계 정보, 연계 방식 및 주기, 송수신 구분 등을 포함한 연계 계획서를 작성한다. - 연계 요청기관 담당자는 연계 대상기관 담당자에게 연계 계획 검토를 요청한다.		●	●	
	2.2. 연계 계획 검토결과 회신	- 연계 대상기관은 연계 요청기관의 연계 계획을 검토한다. - 운영자는 연계작업이 시스템에 미치는 영향을 평가하고, 연계작업 진행 여부를 포함한 검토결과서를 작성하여 회신한다.	○	●	●	

단계	세부 절차	세부 수행 내용	운영 기관	운영 관리	유지 보수	테스트
3. 연계 작업 및 테스트	3.1. 연계 작업	- 연계 요청기관의 운영자는 연계 계획 검토 의견 승인 이후 연계 작업을 수행한다. - 연계 작업은 연계 기능 개발, 테스트, 운영 서버 반영 등 변경요청관리 절차를 준용하여 수행한다.		●	●	
	3.2. 개발환경 테스트	- 유지보수 담당자(또는 테스터)는 개발환경에서 연계 기능의 단위테스트를 수행한다. - 운영관리자(또는 테스터)는 테스트환경에서 연계 서비스의 통합테스트를 수행한다. - 연계 시스템 간 데이터 흐름 및 상호작용이 올바르게 작동하는지 검증한다.		●	●	●
	3.3. 운영서버 연계 반영	- 운영자는 테스트환경에서 테스트 완료된 연계기능을 운영서버에 반영한다. - 유지보수 담당자는 운영환경에서 연계기능의 단위테스트를 수행한다. - 운영관리자는 운영환경에서 연계 서비스의 통합테스트를 수행한다. - 연계 요청기관과 대상기관 및 관련기관의 운영자는 연계서비스 통합테스트를 수행하고 장애 발생여부를 모니터링한다. ※ 관련기관과 연계기능 테스트가 불가능한 경우 자체 검증기능(루프백 등)을 제공하여 통합테스트 진행	●	●	●	●
4. 연계 결과 검토 및 종료	4.1. 연계 결과 등록	- 운영자는 테스트 결과를 확인하고 연계 완료 보고서를 작성하고 운영기관 담당자에게 보고한다. - 운영자는 변경된 연계정보의 현행화를 실시한다.		●	●	
	4.2. 연계 작업 종료	- 운영기관 담당자는 연계 완료 보고서를 검토하고 연계 작업 종료를 승인한다.	●	●		

2) 고려사항

○ N/A

사. 핵심성과지표 (KPI : Key Performance Indicator)

○ 연계 프로세스 관리지표를 도출하여 운영 품질 관리를 목표로 하며, 본 절차서에서는 KPI 표준안을 제시하고 개별기관별 운영 상황에 맞추어 조정하여 지표 관리한다.

KPI 항목	설명	측정 방법	목표 기준
연계 응답 속도 (Integration Response Time)	연계 처리 요청 후 응답까지 걸린 평균 시간	API 및 데이터 연계 응답 시간 측정	≤ 200ms
연계 장애 발생률 (Integration Failure Rate)	연계 오류가 발생한 비율	(장애 발생 연계 수 / 전체 연계 요청 수) × 100	≤ 1%
연계 장애 대응 시간 (Mean Time to Recover, MTTR)	연계 장애 발생 시 정상 복구까지 걸린 평균 시간	장애 발생 시간 ~ 정상화 시간 측정	≤ 30분
연계 데이터 무결성 오류율 (Data Integrity Failure Rate)	연계 데이터 정합성 오류 발생 비율	데이터 비교 및 무결성 점검 결과	≤ 0.5%

아. 수행 검증

1) 검증 방법

- 검증 체크리스트의 기준 항목으로 표준운영절차의 준수여부와 이행점검을 수행한다.
- 개별기관 내 자체 프로세스 검증자는 내부 감사자의 자격 또는 ITIL에 대한 충분한 이해를 가진자가 수행한다. (ITIL 관련 자격 권고)
- 점검 결과는 대외 감사/진단 시 내부 점검 활동의 결과물로 활용할 수 있다.

2) 검증 항목

세부 절차	체크 항목	정성 평가	증적 체크
연계 요청 검토	- 연계요청은 연계 요청기관과 연계 대상기관 담당자들이 사전 협의를 통해 검토하는 절차를 수행하고 있습니까?	적합/ 부적합	<ul style="list-style-type: none"> • ITSM내 회의록 • 연계요청서 • 사전 연계 협의 결과
	- 연계 환경 및 제약사항을 확인하고 연계가능 여부를 검토하고 있습니까?		
연계 계획 수립	- 연계 계획은 연계 근거, 정보, 방법 및 송수신 구분 등 구체적인 사항을 포함하고 있습니까?		<ul style="list-style-type: none"> • ITSM내 연계요청 - 연계 계획서
	- 연계 작업 대상 기관은 연계 계획을 기반으로 연계 요청에 대한 검토 후 검토결과서를 회신하고 있습니까?		
연계 테스트	- 연계 관련기관이 모두 참여하여 연계 테스트를 수행하고 운영 서버 반영 후 장애 발생 여부를 모니터링하고 있습니까? ※ 관련기관과 연계기능 테스트가 불가능한 경우 자체 검증기능을 제공하여 통합테스트를 진행한 경우 적합 판정		<ul style="list-style-type: none"> • ITSM내 연계요청 - 연계 테스트 계획서
연계 결과 검토	- 운영기관 담당자는 연계 작업 결과를 확인하고 연계 완료 여부를 검토하여 작업종료를 승인하고 있습니까?		<ul style="list-style-type: none"> • ITSM내 연계요청 - 연계 결과서
	- 변경된 연계정보의 현행화를 수행하고 있습니까?		

6. 형상 관리 절차서

가. 개요

1) 목적

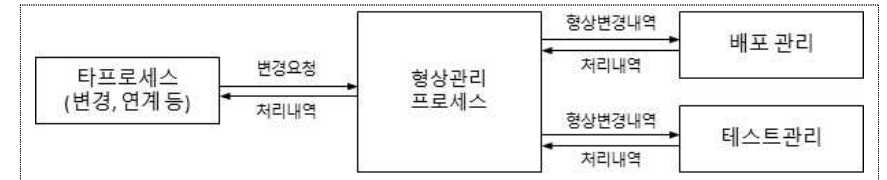
- 응용프로그램 변경요청과 관련된 소스코드, 산출물 등의 형상항목 변경이력을 체계적으로 관리하여 추적가능성과 최신성을 확보하고, 형상항목의 변경을 통제하여 무결성과 일관성을 유지한다.

2) 적용 범위

- 형상관리 절차는 행정·공공기관 응용프로그램 변경이 발생하는 운영관리에 적용한다.
- 형상관리 대상 : 응용프로그램 소스코드 버전관리 및 산출물 현행화

3) 관련 업무 절차

- 연관 선/후행 업무



- 시작/종료/증적(Output) 조건

주요 업무	수행 업무
프로세스 시작 조건	응용프로그램 기능 변경/신규 개발, 타 시스템(데이터 포함) 연계 변경/신규 연계 등으로 현상 변경 필요한 일체의 요청
프로세스 종료 조건	관리 대상 형상 식별에 따른 요청의 반력 형상 변경 처리 종료
증적(Output)	형상 관리 계획서, 형상 항목 목록, 변경 이력 기록, 형상 변경 완료 보고서 ※ ITSM 시스템을 사용하는 경우 시스템내 이력으로 대체

나. 관리 정책

1) 정의

- 응용프로그램 형상 관리 절차의 운영에 있어서 필히 준수해야 할 정책 기준을 제공

2) 정책 기준

정책	설명	
정책 1	기준	응용프로그램에 영향을 미치는 항목을 식별하여 형상정보를 정의하고, 현재 상태를 기준으로 현행화 및 유지관리해야 한다.
	설명	○ 형상항목은 식별 가능하고 고유한 버전 관리체계에 따라 관리한다. ○ 운영사업 착수(인수인계) 시점에 유지관리를 위한 베이스라인(Baseline)을 정의한다. ※ 연속사업으로 진행 시 이전의 형상버전 유지 가능
정책 2	기준	형상항목은 응용프로그램 소스코드와 산출물 등으로 구분하고 형상관리 도구를 이용하여 관리한다.
	설명	○ 형상관리 대상항목별 적합한 형상관리 도구를 활용하여 체계적으로 관리한다. - 버전관리가 필요한 소스코드 및 산출물의 제출은 형상관리도구(SVN 등)를 활용 - 표준운영절차별 계획서 및 결과서 등 이력관리가 불필요한 보고서는 ITSM 시스템을 활용
정책 3	기준	변경요청작업의 소스코드 및 산출물의 무결성 및 신뢰성을 유지하기 위한 관리정책을 정의한다.
	설명	○ 형상관리 도구에 변경 전 Check out, 변경 후 Check in ○ 형상변경이력관리를 위해 Check in 시 상세 사유를 기록한다. ○ 산출물 제출 시 변경요청ID를 입력하여 추적 가능하도록 관리한다. ○ 형상 항목의 변경 사항은 운영관리자 검토 후 승인 여부를 결정한다. - 관련 산출물의 미제출, 변경내용 누락, 형상버전 불일치 등 미흡 사항 발견 시 반려 처리하여 보완 ○ eGovFrame 개발도구(PMD)을 활용한 Code inspection 등 소스코드 결함 검출 및 산출물의 품질관리 활동을 포함하는 형상감사를 수행한다.

다. 용어 정의

용어	설명
형상관리 (Configuration Management)	소프트웨어 및 시스템의 변경 사항을 관리하고, 변경 이력을 추적하는 프로세스
형상 항목 (Configuration Item)	소프트웨어 및 시스템을 구성하는 모든 요소(코드, 문서, DB, 환경설정 등)
형상 베이스라인 (Baseline)	특정 시점에서 검증된 형상 항목의 상태로, 이후 변경 사항의 기준점
형상 변경 요청 (Configuration Change Request, CCR)	형상 항목 변경을 요청하는 공식 문서
버전 관리 (Version Control)	소프트웨어의 변경 이력을 추적하고 특정 버전으로 복구할 수 있도록 관리하는 방식
Git / SVN / CMDB	형상 관리를 위해 사용되는 대표적인 도구
형상 감사 (Configuration Audit)	형상 항목의 변경이 요구사항에 맞게 이루어졌는지, 변경에 대한 형상항목이 잘 관리되는지 검토하고 정책 준수 여부를 점검하는 활동

라. 역할 및 책임

○ 형상관리 절차를 수행하는 역할자의 책임은 다음과

구분		내용
운영기관 (응용프로그램의 운영관리에 최종 책임지는 기관)	관리자	○ 정보시스템 관련 담당자의 상위 책임자 또는 부서장 ○ 형상관리 관련 의사결정
	담당자	○ 형상정보 작업 대상 정보시스템 업무 담당자가 역할 수행 ○ 형상관리 계획 검토 및 승인 ○ 형상관리 항목 변경의 적정성 검토 및 승인 ○ 변경작업으로 인해 형상정보가 변경되는 경우 해당 형상항목 감사 활동 확인
운영자 (위탁기관 또는 운영 사업자)	운영관리	○ 운영기관과의 계약을 통해 정보시스템의 운영과 변경작업을 담당하는 위탁기관 또는 운영 사업자 ○ 형상관리 항목 식별 및 형상관리 계획 수립 ○ 형상관리 도구 및 환경 구축 - 형상관리도구(SVN, CMDB 등) 구성 및 환경설정 ○ 형상항목 베이스라인 설정 및 관리 ○ 형상 항목 변경 관리 - 변경작업 이후 형상정보 현행화 및 변경이력 관리 작업 ○ 형상 감사를 수행하고 시정조치 요청 및 개선 확인
	유지보수	○ 형상관리 항목 식별 및 형상관리 계획 수립 ○ 형상항목 베이스라인 설정 ○ 형상 항목 변경 작업 수행 - 소스코드 변경 전 Check out, 변경 후 Check in 수행 ○ 형상 데이터 백업 및 복구 절차 수행 ○ 형상감사 시 발견된 부적합 사항의 시정조치 계획 수립 ○ 시정조치 계획에 따른 조치이행
	테스트	○ 운영관리자와 협의하여 형상감사 계획 수립 ○ 형상감사를 수행하고 부적합 사항 보고 ○ 시정조치계획을 점검하고 시정조치 내역 확인 ○ 형상감사 결과 보고서 작성 ※ 품질관리자(QA)나 테스트관리자가 없는 경우 운영관리자가 형상감사 수행

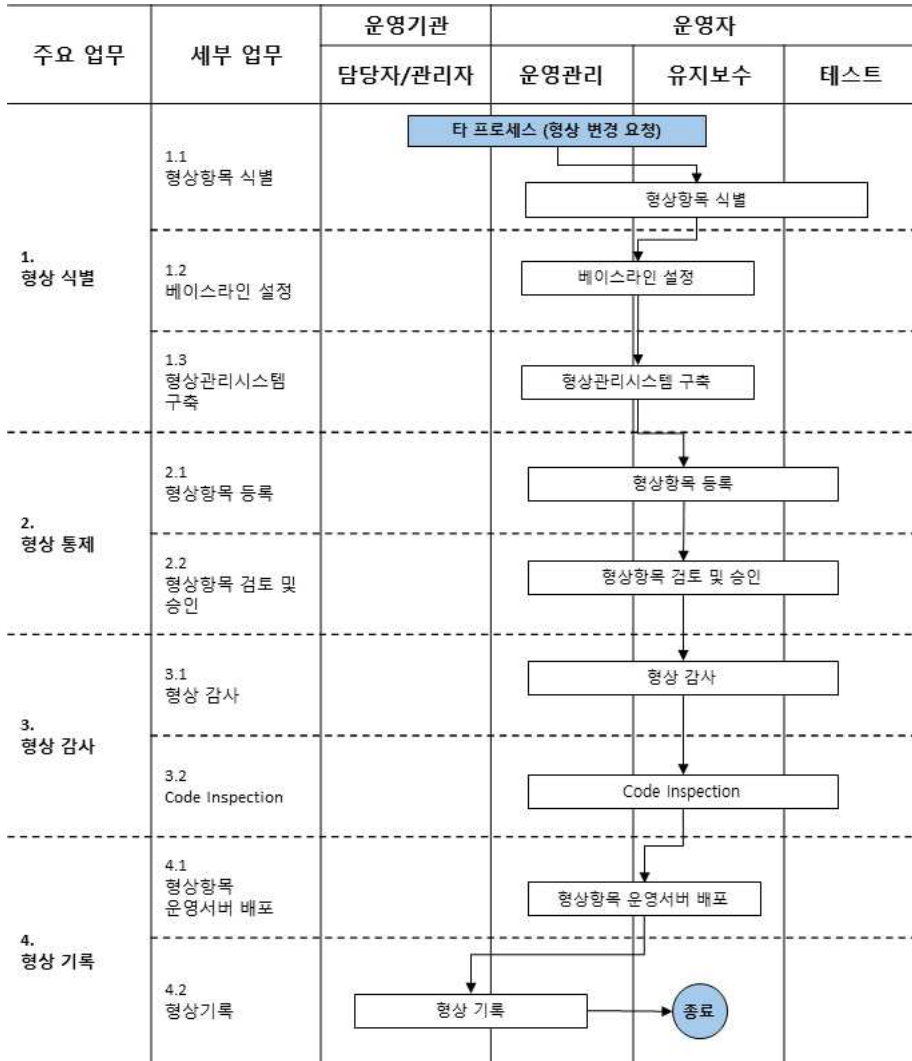
마. 표준절차 흐름도

○ 형상관리 절차는 아래와 같은 주요 업무와 수행절차들로 구성된다.

1) 주요 업무

주요 업무	세부 업무	수행 업무
1. 형상 식별	1.1. 형상항목 식별	○ 응용프로그램 소스코드, 산출물 등 형상관리 대상 항목을 정의하고, 항목별 관리 조직을 구성한다. ○ 형상 항목을 식별하고 버전관리 정책을 수립 및 표준화 한다.
	1.2. 베이스라인 (Baseline) 설정	○ 정보시스템 신규 구축 후 운영관리로 인수인계하는 시점 또는 운영사업자 변경 시 이전 사업자로부터 인수인계 받는 시점에 베이스라인을 설정한다.
	1.3. 형상관리 시스템 구축	○ 형상관리 도구를 구성하고 접근권한을 관리한다.
2. 형상 통제	2.1. 형상항목 등록	○ 변경작업 시 소스코드를 변경한 후 형상관리도구에 반영 (Check in) 한다. ○ 변경작업 관련 산출물 변경 후 형상관리시스템(ITSM 등)에 반영한다. ※ 소스코드 및 산출물 반영 시 변경작업 사항을 상세히 작성하고 변경요청ID를 반드시 입력하여 추적가능성을 확보
	2.1. 형상항목 검토 및 승인	○ Check in 된 산출물을 검토하고 승인여부를 결정한다. - 필수 산출물의 미제출, 변경사항 누락, 형상항목 버전 불일치 등 미흡사항 발견 시 반려 처리
3. 형상 감사	3.1. 형상 감사	○ 형상관리도구에 반영된 소스코드와 산출물의 형상감사를 수행한다. - 개발완료된 릴리스가 운영서버에 반영되기 전 변경요구 사항이 구현된 형상과 일치하는지 감사를 통해 검증 - 변경작업과정에서 수행된 테스트와 산출물 결과등을 점검하여 누락된 요구사항이나 잘못된 반영 등을 확인 ○ 부적합 사항 발견 시 시정조치를 요청한다.
	3.2. Code Inspection	○ 형상관리도구에 반영된 소스코드의 개발표준 위배 여부, 소스코드 규칙 검증 등을 수행하여 결함 검출 등 품질 감사를 수행한다. ※ eGovFrame 개발도구 PMD Plug in 활용 등
4. 형상 기록	4.1. 형상항목 운영서버 배포	○ 변경된 형상 항목을 운영서버에 배포한다.
	4.2. 형상기록	○ 배포 후 형상항목의 변경이력을 최종확인 후 검토 승인 한다.

2) 수행주체별 표준절차 흐름도



바. 세부 수행 절차

1) 절차 및 역할과 책임(R&R : Role and Responsibility)

(●: 정, ○: 부)

단계	세부 절차	세부 수행 내용	운영 기관	운영 관리	유지 보수	테스트
1. 형상 식별	1.1. 형상항목 식별	- 운영관리자는 형상관리 대상항목을 정의하고 항목별 관리조직을 구성한다. - 형상 항목을 식별하고 버전관리 정책을 수립하여 유지보수 담당자 및 테스트 관리자 등 관련조직에 전파한다.		●	●	○
	1.2. 베이스라인(Baseline) 설정	- 운영관리자는 인수인계 시점에 형상관리 베이스라인 1.0을 정의한다. - 유지보수 담당자는 설정된 베이스라인에 따라 개발환경을 구성한다.		●	○	
	1.3. 형상관리 시스템 구축	- 운영자는 형상관리 시스템(소스코드, 산출물 등)의 디렉토리를 구성하고 형상관리도구의 접근권한을 등록 및 관리한다. - 운영관리자는 형상감사를 위한 전자정부 표준 Inspection 룰셋 등 개발 표준이나 소스코드 규칙 등을 형상관리도구에 등록한다.		●	●	
2. 형상 통제	2.1. 형상항목 등록	- 유지보수 담당자는 프로그램 소스코드를 변경한 후 형상관리도구에 반영(Check in)한다. - 운영관리자(또는 품질관리자, 테스트관리자 등)는 변경작업 관련 산출물 변경 후 형상관리도구 또는 ITSM에 등록한다.		●	●	●
	2.1. 형상항목 검토 및 승인	- 유지보수 담당자는 소스코드 반영 시 충돌 여부를 반드시 확인하고 소스코드 병합(Merge) 후 통합테스트를 수행하여 정상동작 여부를 검증한다. ※ 소스코드 및 산출물 반영 시 변경작업 사항을 상세히 작성하고 변경요청ID를 반드시 입력하여 이력관리		●	●	●
	2.1. 형상항목 검토 및 승인	- 운영관리자는 형상관리 시스템에 반영된 소스코드 및 산출물을 검토하고 승인여부를 결정한다. - 미흡사항(필수 산출물의 미제출, 변경사항 누락, 형상항목 버전 불일치 등) 발견 시 반려 처리하고 보완요청 한다.		●	●	●

단계	세부 절차	세부 수행 내용	운영 기관	운영 관리	유지 보수	테스트
3. 형상 검사	3.1. 형상 검사	- 운영관리자(또는 품질관리자, 테스트관리자 등)는 개발완료된 릴리스가 운영서버에 반영되기 전, 소스코드와 산출물 등의 형상검사를 수행한다. - 구현된 형상과 변경요구사항이 일치하는지 형상검사를 통해 검증한다. - 변경작업과정에서 수행된 테스트 결과 등 산출물을 점검하여 누락된 요구사항이나 잘못된 반영 등 부적합 사항 발견 시 시정 조치를 요청한다.		●	●	●
	3.2. Code Inspection	- 운영관리자(또는 품질관리자, 테스트관리자 등)는 소스코드의 개발표준 위배 여부, 소스코드 규칙 검증 등 품질점검을 수행한다. - 미흡사항 발견 시 시정조치를 요청한다.		●	●	●
4. 형상 기록	4.1. 형상항목 운영서버 배포	- 운영관리자는 형상검사 결과를 검토하고 변경된 형상 항목을 운영서버에 배포한다.		●	●	
	4.2. 형상기록	- 운영기관 담당자는 형상항목의 변경이력을 최종확인 후 검토 승인한다.	●	●		

2) 고려사항

○ N/A

사. 핵심성과지표 (KPI : Key Performance Indicator)

○ 형상관리지표를 도출하여 운영 품질 관리를 목표로 하며, 본 절차서에서는 KPI 표준안을 제시하고 개별기관별 운영 상황에 맞추어 조정하여 지표 관리한다.

KPI 항목	설명	측정 방법	목표 기준
형상 검사 수행율 (Configuration Audit Execution Rate)	정기적으로 수행된 형상 검사 비율	(실제 수행된 검사 횟수 / 계획된 검사 횟수) × 100	100%
형상 항목 무결성 유지율 (Configuration Integrity Maintenance Rate)	형상 변경 후 변경 이력이 정상적으로 관리되는 비율	(무결성이 확인된 형상 수 / 전체 변경 형상 수) × 100	≥ 99%
형상 오류 탐지율 (Configuration Error Detection Rate)	형상 변경 후 발생한 오류 탐지 비율	(탐지된 오류 수 / 전체 변경 항목 수) × 100	≥ 90%

아. 수행 검증

1) 검증 방법

- 검증 체크리스트의 기준 항목으로 표준운영절차의 준수여부와 이행점검을 수행한다.
- 개별기관 내 자체 프로세스 검증자는 내부 감사자의 자격 또는 ITIL에 대한 충분한 이해를 가진자가 수행한다. (ITIL 관련 자격 권고)
- 점검 결과는 대외 감사/진단 시 내부 점검 활동의 결과물로 활용할 수 있다.

2) 검증 항목

세부 절차	체크 항목	정성 평가	증적 체크
형상 식별	- 형상관리를 위한 형상항목 식별체계 및 버전 관리 정책이 정의되고 관리되고 있습니까?	적합/ 부적합	• 형상관리계획 및 형상항목 관리대장
	- 형상항목 베이스라인을 설정 및 관리하고 있습니까?		• 형상관리도구(SVN) 버전관리 이력
형상 통제	- 형상항목을 형상관리도구에 등록하고 형상항목의 변경은 변경관리 프로세스와 연계하여 관리하고 있습니까?		• ITSM 기록 또는 형상항목 변경이력
	- 형상 항목의 변경은 추적 가능하고, 감사가 가능합니까?		• ITSM 기록 또는 형상감사 이력
	- 형상항목의 무결성과 신뢰성을 보증하기 위한 검토 및 승인 활동이 진행되고 있습니까?		• ITSM 기록 또는 형상항목 변경이력
형상 감사	- 형상감사가 계획되고 수행되고 있습니까?		• ITSM 기록 또는 형상감사 이력
	- 감사의 결과는 기록/관리되고 발견된 부적합 사항은 적절한 절차를 통해서 반영되고 있습니까?		• 형상감사 조치이력
형상 기록	- 형상정보의 현행화/업데이트는 적절한 절차와 기준에 맞추어 관리되고 있습니까?		• ITSM 기록 또는 형상항목 변경이력

7. 운영상태 관리 절차서

가. 개요

1) 목적

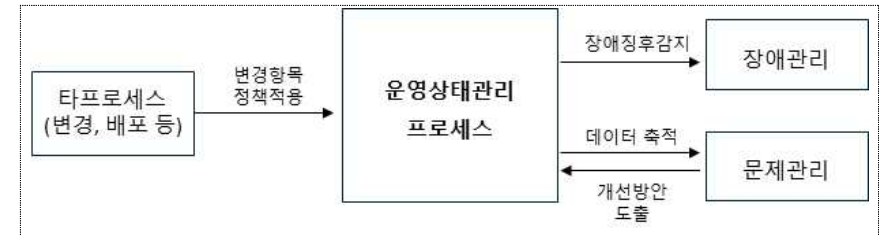
- 운영 시스템의 상태와 성능을 지속적으로 모니터링하고 이벤트를 감지하여 장애를 사전 예방하고, 장애 발생 시 신속히 대응하는 것을 목적으로 한다.

2) 적용 범위

- 운영상태관리 절차는 행정-공공기관 정보시스템의 응용프로그램 운영관리에 적용한다.
- 운영상태관리 대상 : 정보의 수집 및 상태 점검이 가능한 서버, DBMS, 미들웨어 등

3) 관련 업무 절차

- 연관 선/후행 업무



- 시작/종료/증적(Output) 조건

주요 업무	수행 업무
프로세스 시작 조건	운영 시스템의 이벤트(변경, 연계, 테스트, 장애, 성능 최적화 등) 발생
프로세스 종료 조건	이벤트 처리
증적(Output)	이벤트 처리 결과

나. 관리 정책

1) 정의

- 응용프로그램 운영상태관리 절차의 운영에 있어서 필히 준수해야 할 정책 기준을 제공

2) 정책 기준

정책	설명	
정책 1	기준	운영시스템의 지속적인 모니터링이 가능하도록 운영상태관리 계획을 수립하고 이행관리 한다.
	설명	<ul style="list-style-type: none"> ○ 운영상태관리 정책 수립 및 수립된 정책의 반영, 변경, 통제를 수행한다. - 운영상태 관리 주기 계획 수립 - 운영상태관리에 필요한 자원 및 인력 계획 수립
정책 2	기준	운영상태관리 대상별 상태 데이터를 수집하고, 수집된 데이터를 분석한다.
	설명	<ul style="list-style-type: none"> ○ 운영시스템 환경에 따라 관리 항목을 개별 또는 통합 수집·축적 ○ 운영상태 데이터는 기관의 특성을 반영하여 분석 및 관리 주기를 설정 - 상태 데이터 분석 결과는 사후관리(예방점검, 최적화, 개선 등)에 활용
정책 3	기준	운영상태 모니터링 결과는 운영기관 담당자 또는 관리자에게 수시 및 정기 보고한다.
	설명	<ul style="list-style-type: none"> ○ 특정 시스템에 변경이나 장애·오류 등 발생 시, 장애관리절차를 준수하여 처리하고, 운영기관 담당자에게 즉시 보고한다. - 장애발생 상태 데이터를 분석하여 문서화하고 개선 조치 수행 ○ 운영시스템 구성 환경에 따라 주별 또는 월별 운영상태 데이터 분석 결과를 운영기관 담당자에게 보고한다. ○ 운영상태관리 대상별 비상연락체계를 구성하여 관리한다. - 연계시스템을 포함하여 관리
정책 4	기준	업무부하 기간 서비스 지연에 대비한 운영상태 집중 모니터링 및 긴급 대응 방안을 마련한다.
	설명	<ul style="list-style-type: none"> ○ 운영상태를 지속적으로 모니터링하여 이용자 폭증 대비 시스템 지연 최소화를 위한 예방점검 및 시스템 최적화를 수행한다. - 운영상태관리 대상에 대해 분기별 예방 정기점검을 수행하고 발견된 문제점 및 개선방안을 지속적으로 관리 - 성능점검 후 DB튜닝, 응용프로그램 구조 개선 등 최적의 서비스 제공을 위한 활동 수행

다. 용어 정의

용어	설명
운영상태관리 (Operations State Management)	시스템 및 서비스의 상태를 모니터링하고, 이상 상태를 감지하며, 장애 발생 시 신속하게 대응하는 활동
가용성 (Availability)	서비스 및 시스템이 정상적으로 운영될 수 있는 시간의 비율
부하 분산 (Load Balancing)	다수의 서버에 트래픽을 분산하여 성능 및 가용성을 유지하는 기법
로그 분석 (Log Analysis)	시스템 로그를 분석하여 장애 원인 및 성능 문제를 식별하는 과정
이벤트 관리 (Event Management)	시스템 운영 중 발생하는 이벤트를 분석하여 이상 상태를 감지하는 프로세스

라. 역할 및 책임

○ 운영상태관리 절차를 수행하는 역할과 책임은 다음과 같다.

구분		내용
운영기관 (응용프로그램의 운영관리에 최종 책임지는 기관)	관리자	<ul style="list-style-type: none"> ○ 정보시스템 관련 담당자의 상위 책임자 또는 부서장 ○ 운영상태관리 관련 의사결정 ○ 시스템 운영 현황 및 성능 보고서 검토 및 승인 ○ 성능 개선 및 운영 최적화 계획 검토 및 승인
	담당자	<ul style="list-style-type: none"> ○ 운영상태관리 대상 정보시스템 업무 담당자가 역할 수행 ○ 운영상태관리 계획 검토 및 승인
운영자 (위탁기관 또는 운영 사업자)	운영관리	<ul style="list-style-type: none"> ○ 운영기관과의 계약을 통해 정보시스템의 운영과 변경작업을 담당하는 위탁기관 또는 운영 사업자 ○ 운영상태관리 계획 수립 및 관리 <ul style="list-style-type: none"> - 운영상태관리 대상 선정, 정책 수립, 수립된 정책 반영·통제 - 운영상태관리 조직 구성 및 도구·자원 구성 ○ 시스템 운영 현황 모니터링 ○ 시스템 점검 보고서 작성 및 운영기관 보고 ○ 시스템 성능 및 장애 모니터링 도구 구성 및 관리 ○ 시스템 성능 최적화 및 장애 예방 ○ 운영 상태 데이터 수집 및 분석을 통한 이상 징후 탐지
	유지보수	<ul style="list-style-type: none"> ○ 시스템 운영 현황 모니터링 및 일일 점검 수행 ○ 시스템 자원(서버, 네트워크, 스토리지 등) 상태 점검 ○ 시스템 성능 저하 시 문제점 분석 및 개선 수행 ○ 서비스 상태 분석 및 문제 발생 시 초기 대응 ○ 장애 발생 시 장애 원인 분석 및 긴급 복구 ○ 시스템 운영 상태 점검을 위한 성능 테스트 및 부하 테스트 수행 ○ 모니터링 및 알람 시스템의 정상 작동 여부 검증

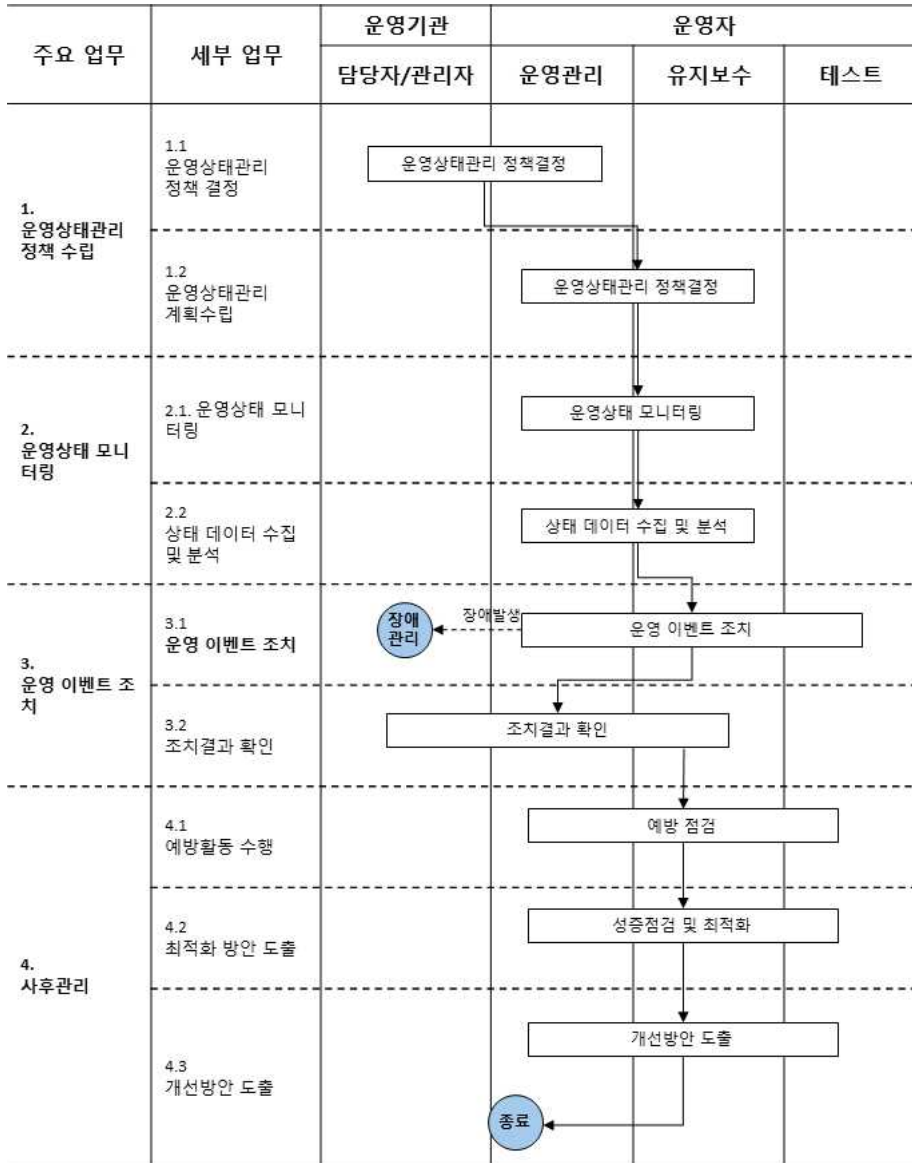
마. 표준절차 흐름도

○ 운영상태관리 절차는 아래와 같은 주요 업무와 수행절차들로 구성된다.

1) 주요 업무

주요 업무	세부 업무	수행 업무
1. 운영상태관리 정책 수립	1.1. 운영상태관리 정책 결정	○ 운영상태 관리 대상, 관리 항목, 관리 주기 등 운영상태 관리 정책을 결정한다.
	1.2. 운영상태관리 계획 수립	<ul style="list-style-type: none"> ○ 운영상태관리 정책에 따라 관리 계획을 수립한다. - 운영상태관리 조직 구성 및 역할과 책임 정의 - 운영상태 점검 및 테스트 등의 작업 일정 계획
2. 운영 상태 모니터링	2.1. 운영상태 모니터링	<ul style="list-style-type: none"> ○ 시스템 모니터링 도구 등을 통해 운영 시스템 자원의 상태(CPU, 메모리, 디스크 사용량 등)를 모니터링한다. - 모니터링 대상인 서버, DB 및 미들웨어 등에 대해 관리 계획을 세워 운영상태를 모니터링한다.
	2.2. 상태 데이터 수집 및 분석	<ul style="list-style-type: none"> ○ 운영상태관리 대상별 관리항목에 대해 상태 데이터를 수집하고, 수집된 데이터는 분석이 가능하도록 축적한다. ○ 운영상태 데이터는 용도에 맞게 분석하여 이상징후를 탐지하거나 성능 개선을 위한 최적화 등을 수행한다. ○ 모니터링 중 장애가 탐지되거나, 변경작업이 필요한 경우 해당 프로세스로 이관한다.
3. 운영 이벤트 조치	3.1. 운영 이벤트 조치	<ul style="list-style-type: none"> ○ 시스템 자원의 임계치 도달 등 장애 발생이 예상되는 경우 자원 추가 할당 및 최적화 등의 조치를 수행한다. ○ 장애가 발생한 경우 신속한 복구작업을 수행하고 원인을 분석하여 문제를 해결한다. ○ 조치 내역을 기록하고 운영기관 담당자에게 보고한다.
	3.2. 조치결과 확인	○ 운영기관 담당자는 조치 결과를 확인한다.
4. 사후관리	4.1. 예방활동 수행	○ 예방 정기점검을 수행하고 발견된 문제점에 대한 개선 방안을 지속적으로 관리하여 잠재적 문제를 예방한다.
	4.2. 최적화방안 도출	○ 성능점검 후 DB튜닝, 응용프로그램 구조 개선 등 최적의 서비스 제공을 위한 활동을 수행한다.
	4.3. 개선방안 도출	<ul style="list-style-type: none"> ○ 수집된 운영 상태 데이터를 분석하여 성능 개선 방안을 도출한다. - 개선을 위해 변경관리, 문제관리 프로세스 등으로 이관할 수 있다. ○ 개선 방안을 문서화하고 운영기관 담당자에게 보고한다.

2) 수행주체별 표준절차 흐름도



바. 세부 수행 절차

1) 절차 및 역할과 책임(R&R : Role and Responsibility)

(●: 정, ○: 부)

단계	세부 절차	세부 수행 내용	운영 기관	운영 관리	유지 보수	테스트
1. 운영상태 관리 정책 수립	1.1. 운영상태관리 정책 결정	○ 운영기관 담당자와 운영관리자는 운영 시스템 환경을 고려하여 운영상태관리 정책을 결정한다. - 운영상태 관리 대상, 관리 항목, 관리 주기 등을 포함	●	●		
	1.2. 운영상태관리 계획 수립	○ 운영자는 운영상태관리 정책에 따라 운영상태관리 계획을 수립한다. - 운영상태관리 조직 구성 및 역할과 책임 정의 - 운영상태 점검 및 테스트 등의 작업 일정 계획		●	●	
2. 운영 상태 모니터링	2.1. 운영 상태 모니터링	- 운영자는 모니터링 도구 등을 통해 서버 CPU, 메모리, 디스크 사용량 및 네트워크 트래픽 등 운영시스템 자원을 모니터링한다. - 운영자는 운영상태관리 대상별 임계치(Threshold)를 설정하고, 성능 저하 사전 감지 및 알림 시스템을 구성한다.		●	●	
	2.2. 상태 데이터 수집 및 분석	- 운영자는 애플리케이션 응답 속도, 처리량, 세션 상태, 오류 로그 등 상태 데이터를 수집한다. - 주요 운영상태 이벤트의 분석이 가능하도록 축적하고 관리한다. ※ 오류 발생 빈도, 특정 시간대의 트래픽 집중 현상 등 파악		●	●	

단계	세부 절차	세부 수행 내용	운영 기관	운영 관리	유지 보수	테스트
3. 운영 이벤트 조치	3.1. 운영 이벤트 조치	- 운영자는 CPU/메모리 성능 임계치 초과 등 장애 징후를 모니터링하고 이벤트 발생 시 신속히 대응한다. - 장애 발생 시 로그 및 시스템 상태 데이터 분석을 통해 원인을 파악한다. - 장애 원인에 따라 서버 및 네트워크 자원 최적화 및 데이터베이스 성능 최적화 등을 수행한다. ※ 장애 발생 시 장애관리 프로세스 적용		●	●	○
	3.2. 조치결과 확인	- 운영기관 담당자는 운영 이벤트 조치 후 모니터링 및 로그 분석을 통해 조치 완료 여부를 확인한다.	●	●	●	
4. 사후관리	4.1. 예방 활동 수행	- 운영자는 시스템 주요 구성 요소(서버, 네트워크, DB)에 대한 예방 점검을 수행한다. - 자동화 도구나 스크립트를 활용하여 주기적인 점검 및 자동 리포트를 생성한다. - 예방 점검을 통해 발견된 문제점을 지속적으로 개선하고 잠재적인 문제를 예방한다.		●	●	●
	4.2. 최적화 방안 도출	- 운영자는 성능 점검을 통해 DB튜닝, 응용프로그램 구조 개선 등 최적의 서비스 제공을 위한 활동을 수행한다. ※ 애플리케이션 성능 개선: 코드 최적화, GC(가비지 컬렉션), 메모리 누수 제거 등 ※ 네트워크 최적화: 트래픽 라우팅 조정, 패킷 손실 분석 및 대응 등 ※ DB 성능 튜닝: 인덱스 추가, 쿼리 최적화 등 검토		●	●	●
	4.3. 개선 방안 도출	- 운영관리자는 장애 발생 빈도, 성능 저하 추이 등을 분석하여 개선방안을 도출한다. - 운영기관 담당자는 운영상태 최적화 관리 계획을 수립하고 지속적인 개선 활동을 수행한다.	●	●	●	○

2) 고려사항

○ N/A

사. 핵심성과지표 (KPI : Key Performance Indicator)

○ 운영상태관리지표를 도출하여 운영 품질 관리를 목표로 하며, 본 절차서에서는 KPI 표준안을 제시하고 개별기관별 운영 상황에 맞추어 조정하여 지표 관리한다.

KPI 항목	설명	측정 방법	목표 기준
운영상태 모니터링 커버리지 (Monitoring Coverage)	주요 시스템, 네트워크, 어플리케이션의 모니터링 비율	전체 운영 자산 중 모니터링 적용 비율	≥ 95%
평균 응답 시간 (Average Response Time)	주요 서비스 응답 속도	어플리케이션 및 API 응답 시간 측정	≤ 200ms
평균 장애 탐지 시간 (Mean Time to Detect, MTTD)	장애 발생 후 감지까지 걸린 평균 시간	장애 발생 로그 분석	≤ 5분
운영 장애 발생률 (Incident Rate per Month)	월간 운영 장애 발생 빈도	(월간 장애 발생 수 / 전체 연계 수) × 100	≤ 2%

아. 수행 검증

1) 검증 방법

- 검증 체크리스트의 체크항목 기준(ITIL 표준 준용)으로 표준운영절차의 준수여부와 이행점검을 수행한다.
- 개별기관 내 자체 프로세스 검증자는 내부 감사자의 자격 또는 ITIL에 대한 충분한 이해를 가진자가 수행한다. (ITIL 관련 자격 권고)
- 점검 결과는 대외 감사/진단 시 내부 점검 활동의 결과물로 활용할 수 있다.

2) 검증 항목

세부 절차	체크 항목	정성 평가	증적 체크
운영상태 모니터링	- 시스템의 안정적 운영을 위해 운영상태관리 대상을 정의하고 모니터링하고 있습니까?	적합/ 부적합	• 운영상태관리대상
	- 운영상태 데이터를 수집하고, 분석 및 개선을 위한 제반 활동을 수행하고 있습니까?		• 모니터링 이력
운영 이벤트 조치	- 운영 이벤트 조치를 위해 프로세스 이관이 필요한 경우 적절하게 이관 및 처리가 진행되고 있습니까?		• 조치이력 (ITSM내 조치 및 이관이력)
	- 운영기관 담당자는 운영 이벤트 조치결과와 검토/확인을 수행하고 있습니까?		• 조치이력 확인결과
사후 관리	- 잠재적 장애/문제 예방을 위해 이벤트에 대한 예방점검 활동이 진행되고 있습니까?		• 예방점검이력
	- 성능점검을 수행하여 최적화 방안을 도출하는 등 성능관리가 수행되고 있습니까?		• 성능관리이력
	- 잠재적 위험요소가 있는 문제 등에 대해서는 개선방안을 도출하는 등 관리가 수행되고 있습니까?		• 개선계획 수립

8. 장애 관리 절차서

(법정부 정보시스템 표준운영절차 준용)

가. 개요

1) 목적

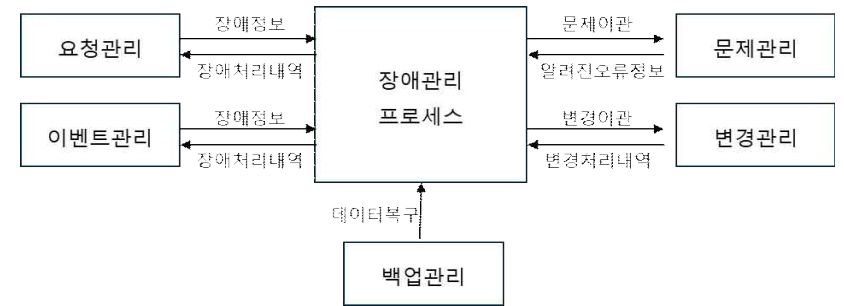
- 응용프로그램의 오류나 오작동으로 서비스 중단 등의 장애가 발생한 경우, 신속하게 대응하고 복구하여 정상적인 서비스를 제공하기 위한 표준 절차를 정의한다.

2) 적용 범위

- 장애관리 절차는 행정-공공기관 정보시스템의 응용프로그램 운영관리에 적용

3) 관련 업무 절차

- 연관 선/후행 업무



- 시작/종료/증적(Output) 조건

주요 업무	수행 업무
프로세스 시작 조건	장애신고 또는 장애인지
프로세스 종료 조건	장애조치완료 또는 신고된 장애가 비장애로 판단된 경우
증적(Output)	장애보고서 장애관리대장 ※ ITSM 시스템을 사용하는 경우 시스템내 이력으로 대체

나. 관리 정책

1) 정의

- 정보시스템 표준운영절차의 운영에 있어서 준수해야 할 정책 기준을 제공

2) 정책 기준

정책	설명	
정책 1	기준	정보시스템에서 발생하는 장애는 신속 정확하게 보고 및 전파되어야 한다.
	설명	○ 장애 정보는 전파 기준에 따라 적절한 대상자에게 전달되어야 한다. ○ 장애 등급에 따라 보고방법/대상/시점에 대한 기준이 수립되어야 한다.
정책 2	기준	발생된 모든 장애는 정상적인 서비스 운영을 위해 신속하게 복구되어야 한다.
	설명	○ 장애는 정상적인 서비스의 신속한 복구에 초점을 둔다. - 정상적인 서비스의 복구가 장애관리의 최우선 과제이며, 근본원인 분석을 위한 문제관리 이관 및 후속 조치 등 정상 서비스 복구 후 순차적으로 처리 수행
정책 3	기준	발생된 모든 장애는 ITSM 등의 관련 시스템을 통해 객관적인 정보로 관리되고 추적되어야 한다.
	설명	○ 발생된 모든 장애는 ITSM 시스템 또는 장애관리대장을 통해 누락없이 기록하고 관리되어야 한다. - 장애의 처리과정과 해결방법, 처리결과 ○ 기록된 장애 이력(해결방법)은 다른 장애 조치에 참조할 수 있어야 하며 추이 분석 등의 예방적 활동의 자료로도 활용되어야 한다.

다. 용어 정의

용어	설명
장애 (Incident)	○ 정보시스템의 전부 또는 일부 기능이 계획되지 않은 정치 상태에 이르거나 오동작, 기능저하 등으로 정상기능을 수행하지 못하여 정상적인 서비스를 제공하지 못하는 것
이벤트 (Event)	○ 정보시스템의 운영 중 식별 가능하거나 감지할 수 있는 것으로 IT인프라 관리나 IT서비스 제공에 있어서 중요한 영향을 미치는 모든 상태(파일 시스템의 용량 초과, CPU 사용율의 임계치 초과 상태, 서비스 프로세스의 다운, 메모리 사용율의 임계치 초과 상태 등)
임시 해결책 (Work-Around)	○ 정보시스템에 발생한 장애의 근본적인 해결을 목적으로 하지 않고, 빠른 서비스 복구를 위해서 임시적으로 장애를 처리하기 위한 방법
근본 해결책 (Root-Cause)	○ 정보시스템에 발생한 장애의 근본적인 원인에 대한 조치를 수행하는 방법 (영구 해결책)
장애 시간	○ 장애 발생시간부터 조치완료(서비스 정상운영) 시간까지의 기간으로 서비스에 영향이 발생한 시간
장애 협의체	○ 조치된 장애의 장애원인과 파급 영향을 검토하고 장애처리 과정에서의 문제점, 시사점 등을 도출 및 재발방지 대책에 대한 적합성 등을 검토하는 협의체
이관 (Escalation)	○ 장애조치를 위해 관리자나 전문가 집단에게 처리를 넘기거나, 장애 조치 후 근본 원인 분석을 위해 문제관리 프로세스 등으로 프로세스를 넘기는 활동 - 프로세스 내에서 처리를 위해 상위 또는 차선 담당자에게 작업을 이관하는 활동 포함
내부감사자	○ 프로세스가 사전 정의된 절차/기준으로 적합하게 운영/준수되고 있는지를 검증하는 내부검증자 역할로 각 프로세스 별 정의된 검증 기준에 따라 정기적(반기 또는 년간)으로 프로세스 감사 활동을 수행

라. 역할 및 책임

○ 장애관리절차를 수행하는 역할자의 책임은 다음과 같다.

주요 업무		수행 업무	비고
운영기관 (정보시스템의 최종운영관리를 책임지는 기관)	관리자	<ul style="list-style-type: none"> ○ 정보시스템 관련 담당자의 상위 책임자 또는 부서장 ○ 장애 처리 관련 의사결정 ○ 장애보고서/장애등급 적합성 판단 	
	담당자	<ul style="list-style-type: none"> ○ 장애조치 대상 정보시스템의 담당자가 역할 수행 ○ 장애상황 상태확인 및 전파/보고 ○ 실 장애처리자 또는 유지보수조직의 장애조치 활동 통제 <ul style="list-style-type: none"> - 장애원인분석 및 조치 참여 ○ 장애보고서 작성/검토(기록관리) ○ 장애 조치건의 문제관리절차 이관여부 결정 <ul style="list-style-type: none"> - 장애 근본원인 미도출 또는 근본원인이 도출되었으나 바로 적용이 어려운 경우 등에 대한 후속관리 	
운영자 (위탁기관 또는 운영사업자)	운영관리	<ul style="list-style-type: none"> ○ 운영기관과의 계약을 통해 정보시스템의 운영과 장애조치를 담당하는 위탁기관 또는 운영 사업자 ○ 실 장애처리자 또는 유지보수조직의 장애조치 활동 통제 <ul style="list-style-type: none"> - 장애 조치를 위한 변경관리 절차 연계 활동 ○ AP 관련기관 협조요청 및 서비스 정상 확인 ○ 장애상황 및 조치상황 보고 ○ 조치/종료 내역 기반 장애보고서 작성 	
	유지보수	<ul style="list-style-type: none"> ○ 정보시스템을 구성하는 HW, SW, 미들웨어 등의 제조사 또는 유지보수를 담당하는 사업자 ○ 장애 분석을 통한 진단과 해결책 도출 및 조치 활동 <ul style="list-style-type: none"> - 장애 조치를 위한 변경관리 절차 연계 활동 ○ 장애상황 및 조치상황 보고 ○ 조치/종료 내역 기반 장애보고서 작성 	
	MSP	<ul style="list-style-type: none"> ○ 운영관리 사업자 역할과 유사하며, 운영기관과의 계약을 통해 클라우드 환경에서의 정보시스템 운영 관리를 지원하는 클라우드 운영 사업자 ○ 장애 분석을 통한 진단과 해결책 도출 및 조치 활동 <ul style="list-style-type: none"> - 장애 조치를 위한 변경관리 절차 연계 활동 ○ 장애상황 및 조치상황 보고 ○ 조치/종료 내역 기반 장애보고서 작성 	
	CSP	<ul style="list-style-type: none"> ○ 유지보수 사업자 역할과 유사하며, 운영기관 또는 MSP와 계약을 통해 클라우드 환경에서 제공되는 정보시스템 인프라에 대한 운영 사업자 ○ 클라우드 인프라 환경에서 발생한 장애 조치 활동 	

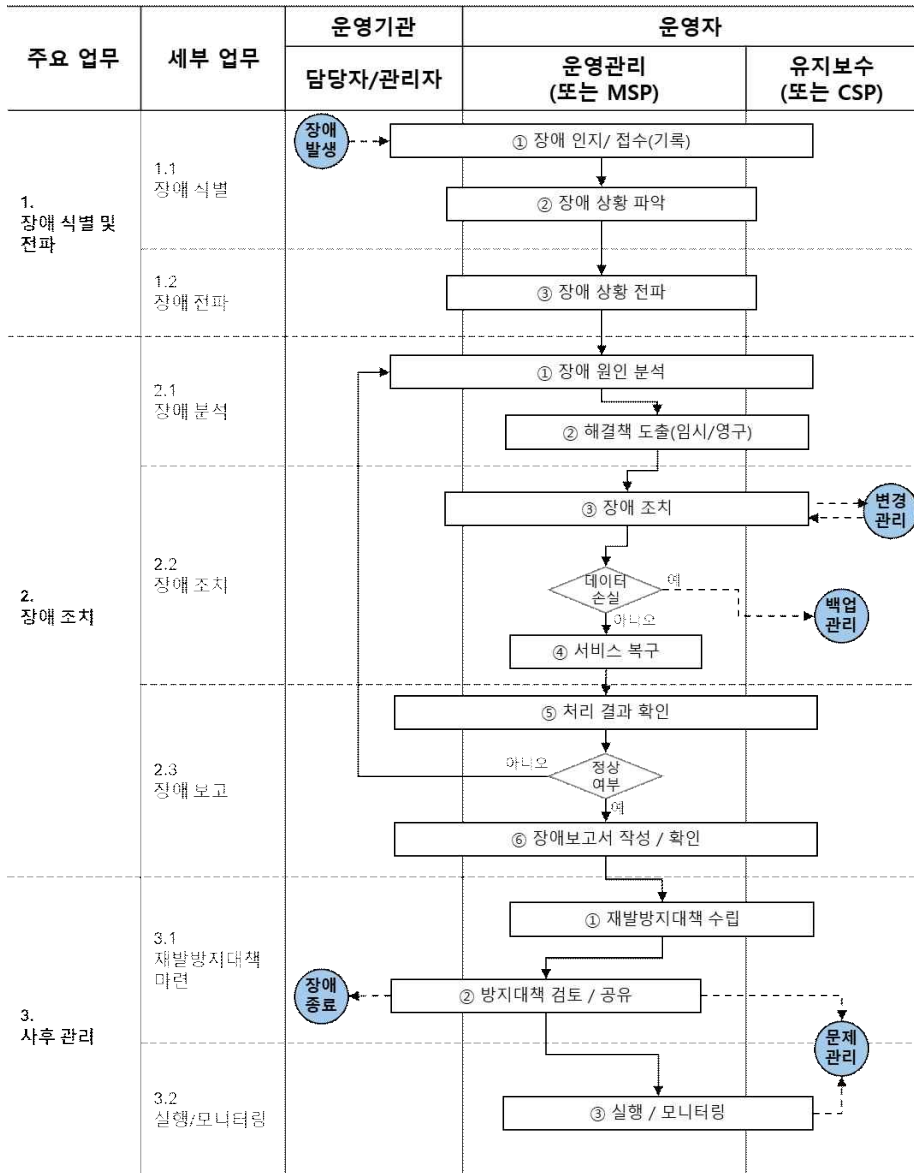
마. 표준절차 흐름도

○ 장애관리 절차는 아래와 같은 주요 업무와 수행절차들로 구성된다.

1) 주요 업무

주요 업무	세부 업무	수행 업무
1. 장애 식별 및 전파	1.1 장애 식별	○ 발생 장애의 인지 후 장애 상황에 대한 기본정보 파악
	1.2 장애 전파	○ 파악된 장애 상황정보를 이해관계자에게 전파 (장애전파기준)
2. 장애 조치	2.1 장애 분석	○ 장애 현상의 분석과 진단을 통해 원인과 해결책을 도출하여 대응방법을 확인
	2.2 장애 조치	○ 도출된 해결책을 기반으로 장애 조치 수행 <ul style="list-style-type: none"> - 시스템 변경작업이 필요한 경우 변경관리 프로세스로 연계 수행 - 데이터 복구 필요한 경우 백업관리 프로세스로 연계 수행
	2.3 장애 보고	○ 장애 조치 결과에 대해 이해관계자 확인 및 서비스 재개 공지
3. 사후 관리	3.1 재발방지대책 마련	○ 장애 재발방지와 예방을 위한 대책 수립 <ul style="list-style-type: none"> - 근본 원인 도출 등의 활동은 문제관리 프로세스로 연계 수행 ○ 재발방지 대책 적합성에 대해 이해관계자 검토
	3.2 실행/모니터링	○ 재발방지 대책에 따른 실행과 모니터링 수행

2) 수행주체별 표준절차 흐름도



바. 세부 수행 절차

1) 절차 및 역할과 책임(R&R : Role and Responsibility)

세부 절차	수행 내용	(●: 정, ○: 부) 운영기관		
		담당자/관리자	운영관리 (MSP)	유지보수 (CSP)
1.1- ① 장애 인지 /접수(기록)	- 사용자의 장애신고 또는 모니터링 시스템을 통해 장애 발생 상황을 인지한다. - 인지된 장애는 장애관리시스템(ITSM 등)에 발생 장애에 대한 기본정보(발생시간, 대상시스템, 관련서비스 등)를 등록한다. ※ 관리시스템이 없는 경우 장애관리대장에 수기 기록 - 운영자는 장애 인지 후 즉시 장애전파체계에 따른 전파 등 장애관리절차에 따라 관련 활동을 수행한다. - Output: 장애기록	○	●	●
1.1- ② 장애 상황 파악	- 운영자는 발생 장애에 대한 상황 정보(대상 정보시스템, 관련서비스, 발생시간, 인지시간 등)를 파악한다.		●	○
1.2- ③ 장애 상황 전파	- 파악된 장애 상황 정보를 이해관계자에게 전파한다. ※ 장애전파 기준은 핵심정보시스템(1등급, 2등급)에 대해서는 "핵심정보시스템 장애 상황관리 체계"에서 정의된 대응체계 기준으로 대응해야 하며, 3등급, 4등급 정보시스템의 경우 개별 기관별 전파기준을 수립하여 관리하도록 한다. (본 절차내 예시 기준 참조) - 장애 상황 전파는 필요에 따라 발생시점/조치시점/조치 완료시점에 상황정보를 전파한다. - Output: 장애 전파 이력	○	●	
2.1- ① 장애 원인 분석	- 운영자는 장애 조치를 위한 담당자를 지정한다. ※ 장애조치담당자 : 장애 발생 위치에 따라 MSP, CSP 또는 운영기관(AP 유지관리업체)이 될 수 있음 - 장애조치 담당자는 발생한 장애 현상을 분석하여 발생 원인을 도출한다. ※ ITSM시스템을 보유한 경우 원인 분석시 기존 장애이력 또는 알려진 오류 등이 기록된 KEDB(Known Error DB)를 활용한다(클라우드 운영사업자 MSP, CSP는 자체 운영중인 KEDB(Known Error DB)를 활용하여 원인분석을 수행한다).		●	●
2.1- ② 해결책 도출	- 장애 원인 분석을 통해 장애 조치를 위한 해결책을 도출한다. - 근본원인 조치를 위한 영구해결책 도출을 목표로 수행하나, 서비스의 빠른 복구를 위한 임시해결책이 먼저 도출되는 경우 해당 해결책 적용을 검토한다. ※ 영구해결책이 바로 도출되지 않는 경우 문제관리 프로세스와 연계하여 관련작업을 수행할 수 있다.		●	●

세부 절차	수행 내용	운영기관		운영자	
		담당자/관리자	운영관리 (MSP)	유지보수 (CSP)	유지보수 (CSP)
2.2- ③ 장애 조치	<ul style="list-style-type: none"> - 장애 조치는 서비스의 빠른 복구를 목표로 활동해야 하며, 도출된 해결책 중 바로 적용이 가능한 해결책을 적용한다. - 장애 조치를 위해 정보시스템의 변경작업이 필요한 경우 변경관리 프로세스와 연계하여 변경작업을 수행한다. ※ 변경관리 표준운영절차 참조 - 장애가 발생한 시스템의 데이터가 손실된 경우에는 백업 관리 프로세스와 연계하여 백업된 데이터의 복구작업을 수행한다. - 장애조치를 위하여 필요한 대응조직은 사전에 정의되고 구성되어야 한다. (붙임3 참조) 	●	●	●	
2.2- ④ 서비스 복구	<ul style="list-style-type: none"> - 장애 조치 활동을 수행하여 장애발생된 서비스를 정상 운영 상태로 복구한다. 		●	●	
2.3- ⑤ 처리 결과 확인	<ul style="list-style-type: none"> - 서비스가 복구되면 운영자 및 운영기관 담당자는 서비스 정상 여부를 확인한다. ※ 장애조치 미해결 시 장애원인분석 단계의 활동을 재 수행한다. - 장애 조치로 서비스의 정상 여부를 확인한 경우 서비스가 복구되었음을 이해관계자에게 전파한다. 	●	●	●	
2.3- ⑥ 장애보고서 작성 확인	<ul style="list-style-type: none"> - 운영자는 아래항목 등을 포함하여 장애보고서를 작성(ITS M시스템 또는 수기 기록)하여 운영기관에 제출한다. ※ 장애시간, 장애원인, 처리내역, 해결책 등 - 운영기관 담당자는 장애보고서를 확인하여 장애 처리내역의 적합성을 검토한다. ※ 개별기관별 장애협의체가 있는 경우 해당 협의체를 통해 장애보고서의 내용을 검토한다. (문제이관여부 포함) - Output: 장애보고서 	●	●	●	
3.1- ① 재발방지 대책 수립	<ul style="list-style-type: none"> - 운영자는 장애원인 및 처리내역을 기반으로 재발방지를 위한 대책과 이행방안을 수립한다. ※ 방지대책의 수립 활동은 개별기관별 상황에 따라 장애보고서 작성 단계의 활동과 병행할 수 있다. ※ 클라우드 운영사업자 MSP, CSP는 동일한 서비스를 이용중인 사용자에게 장애 및 조치 내역을 전파하여 장애 예방 활동을 지원한다. 		●	●	
3.1- ② 방지대책 검토/공유	<ul style="list-style-type: none"> - 운영기관 담당자 또는 장애협의체는 수립된 방지대책에 대해 적합성을 검토하고, 이행관리 방안에 대해 운영사업자와 협의한다. 	●	●	●	

세부 절차	수행 내용	운영기관		운영자	
		담당자/관리자	운영관리 (MSP)	유지보수 (CSP)	유지보수 (CSP)
3.2- ③ 실행/모니터링	<ul style="list-style-type: none"> - 운영자는 방지대책의 내용에 따라 실행 활동을 수행하고 관련 결과를 운영기관에 제공한다. - 운영기관 담당자는 방지대책의 실행 활동에 대해 모니터링을 수행하고 운영자와 지속적인 개선활동을 수행한다. - 재발방지대책의 실행은 필요에 따라 변경관리/문제관리 프로세스와 연계하여 실행할 수 있다. 	●	●	●	

사. 핵심성과지표 (KPI : Key Performance Indicator)

프로세스 운영 품질 관리를 위해 프로세스 별 관리지표를 도출하여 관리함을 목표로 하며, 본 절차서에서 사용하는 관리가능한 KPI를 제시하고 개별기관 별 운영 상황에 맞추어 조정하여 지표 관리

측정지표	측정방법	측정목적	측정주기
장애 적기 처리율	$\left(\frac{\text{목표 시간내 처리된 장애 건수}}{\text{당월 종료 처리된 장애건수}} \right) \times 100$	장애조치의 적기여부 관리(상호 합의된 장애처리시간 준수)	월간

아. 수행 검증

1) 검증 방법

- 검증 체크리스트의 체크항목 기준(ITIL 표준 준용)으로 표준운영절차의 준수여부와 이행점점을 수행한다.
- 개별기관 내 자체 프로세스 검증자는 내부 감사자의 자격 또는 ITIL에 대한 충분한 이해를 가진자가 수행한다. (ITIL 관련 자격 권고)
- 점검 결과는 대외 감사/진단 시 내부 점검 활동의 결과물로 활용할 수 있다.

2) 검증 항목

세부 절차	체크 항목	정성 평가	증적 체크
장애 식별 및 전파	- 모든 장애는 기록되고 있습니까?	적합/ 부적합	<ul style="list-style-type: none"> • 장애기록 - ITSM 내 장애기록 또는 수기 장애관리대장 • 장애전파기준 • 장애전파이력(ITSM 내 전파이력 또는 메일/SMS등의 이력)
	- 장애 인지 시 관련 이해관계자들에게 장애 전파 기준에 따라 공유되고 있습니까?		
장애 조치	- 장애 처리를 위해 유사 장애, 관련 구성항목의 정보 /이력 등을 활용하고 있습니까?		<ul style="list-style-type: none"> • ITSM 장애기록, 구성정보(CMDB) • 수기 장애관리대장 (ITSM 미사용시)
	- 장애발생 구성항목 정보와 연관 구성항목 정보를 파악하고 있습니까?		
	- 장애를 조치하기 위해 정보시스템의 변경작업이 필요한 경우 변경프로세스와 연계하여 작업이 진행되고 있습니까?		<ul style="list-style-type: none"> • 장애기록 및 변경작업이력
	- 장애 조치 후 장애보고서는 적절하게 작성하고 이해 관계자에게 보고/공유하고 있습니까?		
사후 관리	- 장애의 재발방지를 위한 대책과 이행방안이 수립되고 있습니까?		<ul style="list-style-type: none"> • 장애기록(또는 재발방지대책 내용)
	- 장애의 근본원인이 미도출되었거나, 도출되었으나 바로 조치가 어려운 경우 문제관리 프로세스와 연계하여 작업이 진행되고 있습니까?		<ul style="list-style-type: none"> • 장애기록 (장애발생정보와 문제이력 연관정보)
	- 재발방지대책의 실제 활동이 수행되고 이에대한 모니터링을 통한 개선활동이 진행되고 있습니까?		<ul style="list-style-type: none"> • 재발방지대책의 이행결과 이력

자. 관리기준 및 예시

1) 기준 상세

- 각 기관은 업무등급 별 발생장애의 전파체계를 갖추어야 하며, 하기 예시를 참조하여 보고 대상과 보고시점을 정의하고 관리한다.
 - 정보시스템 1~2등급의 경우 "핵심정보시스템 장애 상황관리 체계" 기준에 따라 관련 활동을 수행한다. (붙임2 참조)
- 발생한 장애는 모두 기록관리하여야 한다.
 - 정보시스템 1~2등급에 발생한 장애는 ITSM 등의 관리시스템을 통해 기록 및 유지관리한다.
 - 정보시스템 3~4등급에 발생한 장애는 ITSM 등의 관리시스템이 없는 경우 수기 관리가 가능하다.

2) 장애 전파 예시

<업무등급별 장애 전파 체계>

정보시스템 장애등급	보고 및 전파	
	보고 대상	보고 시점
1등급	각급기관 책임자 디지털안전상황실 (행안부 본부 / 대통령실, 국무조정실 등)	<ul style="list-style-type: none"> • 장애 발생 즉시 • 조치단계 중간보고 • 장애 복구 완료 후 즉시
2등급	각급기관 책임자 디지털안전상황실 (행안부 본부)	<ul style="list-style-type: none"> • 장애 발생 즉시 • 조치단계 중간보고 • 장애 복구 완료 후 즉시
3등급	각급기관 책임자 또는 부서장	<ul style="list-style-type: none"> • 장애 발생 즉시 • 조치단계 중간보고 • 장애 복구 완료 후 즉시
4등급	각급기관 책임자 또는 부서장	<ul style="list-style-type: none"> • 장애 발생 즉시 • 조치단계 중간보고 • 장애 복구 완료 후 즉시

※ 참조사항

- 다수 개별업무 장애 시 최고 업무 등급에 준해 전파한다.
- 장애 보고 절차(계통)는 각 기관별 특성에 맞추어 사전 정의한다.
- 중간보고: 장애 발생 후 30분 이상 장애가 지속되거나, 초기 보고내용과 달리진 상황이 있는 경우에는 관련 내용에 기반하여 중간보고를 진행한다.
- 장애 조치 후 완료보고는 장애보고서를 기반으로 하며, 장애 기록은 ITSM 시스템 또는 문서형태의 기록관리를 수행한다.

3) 장애보고서 (예시)

장애 내역			
시스템명		발생 일시	
접수 일시		접수자	
복구 일시		서비스 중단시간(분)	
장애 증상 및 범위			
서비스 영향도			
시간대 별 경과 사항	시 간	피해상황 및 대응조치(요약)	담당자
비 고			
반복 장애 이력	일 자	처리 내역	중단시간(분)
원인 분석			
진행 여부	<input type="checkbox"/> 완료	<input type="checkbox"/> 미완료	<input type="checkbox"/> 기타 (사유)
원인 유형	<input type="checkbox"/> 인적	<input type="checkbox"/> H/W	<input type="checkbox"/> S/W
	<input type="checkbox"/> O/S	<input type="checkbox"/> N/W	<input type="checkbox"/> 기술
분석 결과			
처리 결과			
처리내역	※ 장애 원인 해소를 목적으로 기술적 관리, 관리적 관리, 물리적 관리 관점에서 처리 업무 세부내용을 작성할 것.		
이행점검	※ 위 처리내역의 각 사항별에 대해 이행 유무 및 적합성 여부를 확인, 점검하고 결과를 작성할 것.		
Action Plan			
시정 및 예방조치	※ 처리 결과와 별도로 재발 방지를 위해 추가적으로 보완 또는 필요한 감쇄정책(Mitigation Plan) 등 실시한 내용을 작성할 것.		

4) 장애관리대장 (예시)

장애 관리대장 (예시)															
장애ID	장애유형	장애시스템	제목(장애명)	현재단계(상태)	장애인지일시	장애발생일시	조치완료일시	장애시간	장애등급	업무담당자	처리자	장애원인	조치내용	향후대책	비고

■ 불임1 정보시스템 장애등급 산정기준

- ▶(기본 원칙) 기본 장애등급은 정보시스템 등급과 동일
 - ※ 기반시설·공동장비 장애 등 동일 원인으로 복수의 정보시스템이 영향을 받는 경우 해당 정보시스템 중 가장 높은 등급을 기준으로 장애등급 지정
- ▶(등급 보정) 발생시간, 대상지역, 서비스 중요도에 따라 하향 보정
 - ※ 장애의 파급 효과를 고려하여 최대 2개 등급 하향 가능

- (정의) 정보시스템 사용자 관점에서 서비스 이용이 불가능하거나, 불편이 발생한 경우
 - ※ 사전에 공지한 변경작업 등 예정된 서비스 중단은 장애에 포함되지 않음
- (장애 발생일시) 아래 순서에 따라 지정
 - (1) 정보시스템 로그에서 식별된 시점(사용이 중단된 시점) / (2) 모니터링 자동화 도구로 장애가 감지된 시점 / (3) 장애신고 접수 시점 또는 장애상황 최초 인지 시점
- (장애 종료일시) 정보시스템 복구 완료 및 서비스 정상 가동을 확인한 시점
 - ※ 장애 관리자(공무원, 공공기관 직원) 또는 장애 조치자(운영 사업자 등)가 확인한 시점 포함
 - ※ 동일증상 당일내 재발 시 기존 장애 지속으로 간주, 최종 정상화 시점을 종료일시로 함
- (유형) 아래의 표와 같이 유형 분류

구분	유형	내 용	
장애 증상에 따른 구분	서비스 중단	·시스템 접속 불가, 무응답 등으로 서비스 이용이 10분 이상 중단 (변경작업 등 사전공지된 작업에 따른 중단은 제외)	
	서비스 지연	·서비스 지연 10분 이상 지속 (순번 대기후 정상 서비스는 지연으로 보지 않음)	
	서비스 오작동	·서비스는 작동하나 사용자가 받는 결과물이 정상적이지 않은 경우 ※ 예시) 증명서 오발급, 민원신청 불가, 화면 표시 정보 오류 등	
장애 원인에 따른 구분	내부요인 장애	·HW-SW-AP 등 시스템 구성요소의 고장 또는 과부하 등으로 인한 장애	
	외부요인 장애	단말 장애	·정보시스템에 접속하여 사용하는 PC 등 단말 영역의 문제로 다수 업무 담당자의 민원 접수처리 등 정보시스템 기반 업무 수행이 불가능한 경우
		기반시설 장애	·전원공급장치(UPS 등), 향온향습기 고장 등 기반시설에 문제가 생겨서 정보시스템의 장애가 발생한 경우
		사이버 침해 장애	·DDoS, 해킹, 랜섬웨어 등 사이버 침해로 인해 장애가 발생한 경우 ※ 단순 정보 유출이나 위변조는 장애가 아닌 보안 침해사고로 대응

- (등급보정 기준) 아래와 같이 등급 조정 가능

기준	1개 등급 하향	2개 등급 하향	비고
발생시간 보정	<ul style="list-style-type: none"> ▣ 평일 09시~18시 이외 시간대 내부업무 서비스 장애 ▣ 평일 09시~21시 이외 시간대 대국민 서비스 장애 	-	▣ 다음 평일 09시까지 정상화 미완료시 원래 장애등급 부여
지역 보정	<ul style="list-style-type: none"> ▣ 전국 대상 서비스 제공 정보시스템에 광역 또는 기초 지자체(주민 전체 영향) 장애 발생시 	<ul style="list-style-type: none"> ▣ 전국 대상 서비스 제공 정보시스템에 광역 또는 기초 지자체(주민 일부 영향) 장애 발생시 	-
서비스 중요도 보정	▣ 서비스 중요도 2순위 이하에 대해서만 장애가 발생한 경우	▣ 서비스 중요도 3순위 이하에 대해서만 장애가 발생한 경우	-

※ 복수 기준을 동시 적용 가능한 경우 합산해서 최대 2개 등급까지 하향 가능

■ 불임2

핵심정보시스템 장애 상황관리 체계

□ 개요

- 최근 잇따라 발생하는 행정정보시스템 장애에 효율적으로 대처하기 위해 각 기관과 상시 연락체계를 구축하여 장애 상황 발생 시 관련 정보를 초기에 신속하게 파악하고 적시 대응

□ 장애 상황관리 대상 정보시스템

- 대국민서비스 중심의 핵심정보시스템(1등급, 2등급)

□ 정보시스템 장애발생 대응체계

- (상황보고) 각 기관의 핵심정보시스템 운영 담당자*는 보고체계에 따라 정보시스템 장애발생 상황을 디지털안전상황실에 즉시 보고
 - * 데이터센터 관계자 및 인프라담당, AP담당 등 누구든 장애지연 인지 즉시 보고
- (보고기준) 핵심정보시스템 접속이 불가하거나 지연되는 경우, 일부 기능 불가로 국민 불편이 예상되는 경우 및 언론에 보도된 장애 등
- (보고채널) 디지털안전상황실 대표전화-문자(042-250-5777) 또는 대표메일(digital119@korea.kr) 및 SNS 소통방을 통해 장애발생 보고
- (상황전파) 업무등급 및 국민 불편 경중에 따라 단계별 상황전파

< 장애상황 전파 체계 >



9. 문제 관리 절차서

(법정부 정보시스템 표준운영절차 준용)

가. 개요

1) 목적

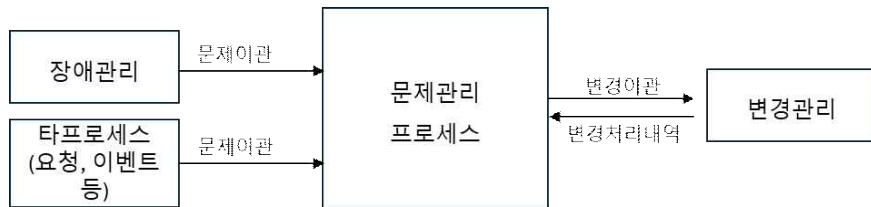
- 정보시스템에 발생한 장애 중 근본원인이 파악되지 않은 문제에 대하여 근본원인 도출과 해결 방안을 제시하고, 문제나 장애의 분석과 예방활동에 필요한 절차를 제공하여 동일 장애의 재발을 방지하고, 장애 발생을 예방하는데 목적이 있다.

2) 적용 범위

- 문제관리 절차는 행정·공공기관의 정보시스템을 운영하는 기관의 정보시스템 운영관리에 적용

3) 관련 업무 절차

- 연관 선/후행 업무



- 시작/종료/증적(Output) 조건

주요 업무	수행 업무
프로세스 시작 조건	장애 프로세스에서 문제 이관 또는 타프로세스(요청, 이벤트 등)에서 문제 등록 요청 사전 예방활동(경향분석 등)을 위한 개선 사항(잠재적 문제 등)의 등록
프로세스 종료 조건	근본원인 도출 또는 등록된 문제의 해결
증적(Output)	문제 관리대장(문제처리 이력) ※ ITSM 시스템을 사용하는 경우 시스템 내 이력으로 대체

나. 관리 정책

1) 정의

- 정보시스템 표준운영절차의 운영에 있어서 필히 준수해야 할 정책 기준을 제공

2) 정책 기준

정책	설명
정책 1	기준 문제관리 프로세스의 목적을 이해하고 장애관리 프로세스에서 수집/이관된 데이터에 대한 근본원인도출과 경향분석 등의 활동을 수행한다.
	설명 ○ 문제관리 프로세스의 목적은 장애의 근본원인을 식별/분석하여 향후 서비스에 영향을 미치는 장애가 발생하지 않도록 하는 것이다. ○ 장애관리 프로세스는 서비스의 빠른 복구에 초점을 두어 진행하며, 근본 원인 미도출, 재발가능성 등의 장애 요인은 문제관리를 통해 관리한다.
정책 2	기준 문제관리는 알려진 오류(Known Error) 관리 및 제시된 해결책 정보에 대한 관리 책임을 가진다.
	설명 ○ 알려진 오류나 해결책은 ITSM시스템을 사용하는 경우 KEDB에 등록하고 관리하여야 한다. ○ 발생한 장애이력 및 장애/문제에 대한 경향분석의 내용은 관리되고 참조될 수 있어야 한다.

다. 용어 정의

용어	설명
임시 해결책 (Work-Around)	○ 정보시스템에 발생된 장애의 근본적인 해결을 목적으로 하지 않고, 빠른 서비스 복구를 위해서 임시적으로 장애를 처리하기 위한 방법
근본 해결책 (Root-Cause)	○ 정보시스템에 발생된 장애의 근본적인 원인에 대한 조치를 수행하는 방법 (영구 해결책)
알려진 오류 (Known-Error)	○ 발생된 문제의 근본원인과 임시해결책 등이 사전 도출되어 문서화 또는 KEDB에 등록되어 있는 오류 .
알려진 오류 DB (KEDB)	○ 장애발생 원인과 해결 방안을 등록/관리하여 이후 발생장애의 조치나 예방활동에 활용할 수 있도록 알려진 오류 등을 관리하는 것으로, ITSM 시스템 내 지식 DB 형태로 구성하며, ITSM 시스템 미사용시에는 관리대장이나 기록 형태로 관리할 수 있음
사전예방적 문제관리 (Proactive Problem Management)	○ 기 발생된 장애 유형이나 추세 분석을 통해 중대한 문제를 식별하거나 발생할 수 있는 장애를 사전 예방하기 위한 활동
이관 (Escalation)	○ 장애나 작업의 조치를 위해 관리자나 전문가 집단에게 처리를 넘기거나, 조치 후 근본 원인 분석을 위해 문제관리 프로세스 등으로 프로세스를 넘기는 활동 - 프로세스 내에서 처리를 위해 상위 또는 차선 담당자에게 작업을 이관 하는 활동 포함
내부감사자	○ 프로세스가 사전 정의된 절차/기준으로 적합하게 운영/준수되고 있는지를 검증하는 내부검증자 역할로 각 프로세스 별 정의된 검증 기준에 따라 정기적(반기 또는 년간)으로 프로세스 감사 활동을 수행

라. 역할 및 책임

○ 문제관리절차를 수행하는 역할자의 책임은 다음과 같다.

주요 업무	수행 업무	비고	
운영기관 (정보시스템의 최종운영관리를 책임지는 기관)	관리자	○ 정보시스템 관련 담당자의 상위 책임자 또는 부서장 ○ 문제 처리 관련 의사결정 ○ 등록된 문제의 적합성 판단 ○ 문제관리 현황, 분석내용, 보고서 등에 대한 검토	
	담당자	○ 문제조치 대상 정보시스템의 담당자가 역할 수행 ○ 문제관리 정책 및 절차 수립 ○ 문제관리 수행과 관련된 조치 참여 ○ 실 문제처리자 또는 유지보수조직의 조치 활동 통제 ○ 접수된 문제의 진행여부 검토/승인 ○ 문제 경향분석 내용에 대한 검토	
운영자 (위탁기관 또는 운영사업자)	운영관리	○ 운영기관과의 계약을 통해 정보시스템의 운영과 문제조치를 담당하는 위탁기관 또는 운영 사업자 ○ 실 문제처리자 또는 유지보수조직의 문제조치 활동 통제 ○ 문제의 근본원인 분석을 통한 진단과 해결책 도출 및 조치 활동 - 문제 조치를 위한 변경관리 절차 연계 활동 ○ AP 관련기관 협조요청 및 서비스 정상 확인 ○ 문제상황 및 조치상황 보고 ○ 장애/문제 경향 분석과 모니터링을 통한 예방 활동	
	유지보수	○ 정보시스템을 구성하는 HW, SW, 미들웨어 등의 제조사 또는 유지보수를 담당하는 사업자 ○ 문제의 근본원인 분석을 통한 진단과 해결책 도출 및 조치 활동 - 문제 조치를 위한 변경관리 절차 연계 활동 ○ 문제상황 및 조치상황 보고	
	MSP	○ 운영관리 사업자 역할과 유사하며, 운영기관과의 계약을 통해 클라우드 환경에서의 정보시스템 운영 관리를 지원하는 클라우드 운영 사업자 ○ 문제의 근본원인 분석을 통한 진단과 해결책 도출 및 조치 활동 - 문제 조치를 위한 변경관리 절차 연계 활동 ○ 문제상황 및 조치상황 보고 ○ 장애/문제 경향 분석과 모니터링을 통한 예방 활동	
	CSP	○ 유지보수 사업자 역할과 유사하며, 운영기관 또는 MSP와 계약을 통해 클라우드 환경에서 제공되는 정보시스템 인 프라에 대한 운영 사업자 ○ 클라우드 인프라 환경에서 발생한 문제의 근본원인 분석 및 관련 조치 활동	

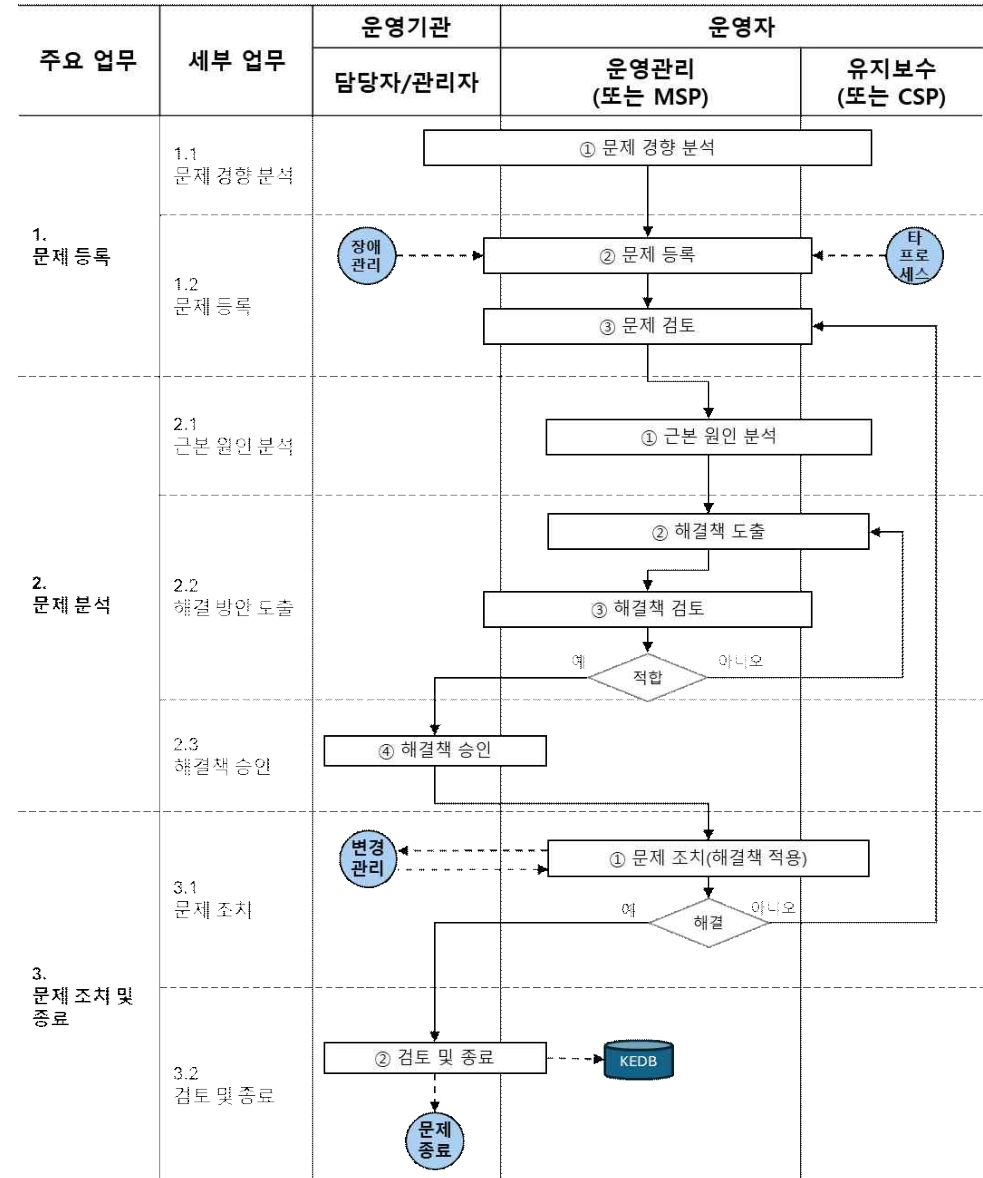
마. 표준절차 흐름도

○ 문제관리 절차는 아래와 같은 주요 업무와 수행절차들로 구성된다.

1) 주요 업무

주요 업무	세부 업무	수행 업무
1. 문제 등록	1.1 문제 경향 분석	○ 장애이력, 운영상황에 대한 분석/모니터링을 통해 잠재적 문제 또는 개선 필요건에 대한 도출 활동
	1.2 문제 등록	○ 장애로부터 이관된 근본원인 미 해결 건을 문제관리 프로세스에 등록 ○ 도출된 개선건 또는 타 프로세스 (변경, 이벤트 등)로부터 잠재적 문제나 관리가 필요한 문제를 등록
2. 문제 분석	2.1 근본 원인 분석	○ 등록된 문제의 분석과 진단을 통해 근본원인을 도출
	2.2 해결 방안 도출	○ 도출된 근본원인을 해결할 복수의 해결방안을 도출 - 근본원인에 대한 영구해결책을 도출 - 해결책에 대해 비즈니스 측면, 재정적인 측면, 기술적인 측면 등 다각적인 측면에서 적용 가능여부를 검토
	2.3 해결책 승인	○ 검토된 해결책의 적용을 위한 운영기관 담당자의 작업 검토/승인
3. 문제 조치 및 종료	3.1 문제 조치	○ 승인된 해결책을 적용하여 문제를 해결 - 조치를 위해 변경작업 필요시 변경관리 프로세스로 연계 수행
	3.2 검토 및 종료	○ 해결책을 통해 문제 조치 결과 검토 ○ 정상적으로 조치된 것을 확인 후 문제 종료

2) 수행주체별 표준절차 흐름도



바. 세부 수행 절차

1) 절차 및 역할과 책임(R&R : Role and Responsibility)

(●: 정, ○: 부)

세부 절차	수행 내용	운영기관		운영자	
		담당자/관리자	운영관리 (MSP)	유지보수 (CSP)	유지보수 (CSP)
1.1- ① 문제경향 분석	<ul style="list-style-type: none"> - 기 발생 장애기록을 분석하여 발생 빈도가 잦거나 잠재적인 장애 발생 가능성이 있는 문제를 도출한다. - IT 운영상황의 모니터링을 통해 잠재적인 문제/이슈 가능성이 있는 문제를 도출한다. - 도출된 문제/이슈는 문제관리 프로세스에 등록하여 집중 관리 및 개선활동을 수행하도록 한다. 	○	●	●	
1.2- ② 문제 등록	<ul style="list-style-type: none"> - 장애로부터 이관된 근본원인 미해결 건을 문제관리 프로세스에 등록한다. - 타프로세스(변경, 이벤트 등)의 운영관리 중 잠재적 문제 발생 가능성이 있어 지속적 관리가 필요한 경우 문제관리 프로세스에 등록한다. - Output: 문제기록 	○	●	○	
1.2- ③ 문제 검토	<ul style="list-style-type: none"> - 등록된 문제의 적합성에 대해서는 문제관리 담당자가 적합여부를 판단한다. ※ 적합여부의 판단을 위해 협의가 필요한 경우 관련 이해관계자를 소집하여 등록된 문제의 적합여부를 검토한다. - 문제 검토를 통해 적합하지 않은 문제의 경우 해당건을 종료한다. 	○	●	○	
2.1- ① 근본 원인 분석	<ul style="list-style-type: none"> - 운영자는 문제분석과 해결책 도출을 위한 담당자를 지정한다. ※ 문제조치담당자: 문제가 발생한 서비스의 상황에 따라 MSP, CSP 또는 운영기관(AP 유지관리업체)이 될 수 있음 - 문제조치 담당자는 등록된 문제의 현상과 관련 기록을 분석하여 문제의 근본 원인을 도출한다. ※ ITSM시스템을 보유한 경우 원인 분석시 기존 장애이력 또는 알려진 오류 등이 기록된 KEDB(Known Error DB)를 활용한다(클라우드 운영사업자 MSP, CSP는 자체 운영중인 KE DB(Known Error DB)를 활용하여 원인분석을 수행한다). 		●	●	
2.2- ② 해결책 도출	<ul style="list-style-type: none"> - 문제 원인 분석을 통해 조치를 위한 해결책을 도출한다. - 근본원인 조치를 위한 영구해결책 도출을 목표로 수행하며, 해결책은 여러개의 해결책으로 도출될 수 있다. ※ 도출되는 해결책은 비즈니스 측면, 재정적인 측면, 기술적인 측면 등 다각적인 측면에서 적용 가능여부를 검토 하도록 한다. 		●	●	

(●: 정, ○: 부)

세부 절차	수행 내용	운영기관		운영자	
		담당자/관리자	운영관리 (MSP)	유지보수 (CSP)	유지보수 (CSP)
2.2- ③ 해결책 검토	<ul style="list-style-type: none"> - 도출된 해결책은 관련 이해관계자 검토를 통해 적합한 해결책인지 검토한다. (적합하지 않은 경우 해결책 도출 작업을 재 수행한다.) - 해결책은 도출되었으나 이해관계자가 조직의 상황, 비용적 문제 등으로 해결책을 적용할 수 없거나, 해결책 미적용으로 발생할 수 있는 리스크를 수용할 경우 해당 문제건은 해결책을 적용하지 않고 종료할 수 있다. 		○	●	○
2.3- ④ 해결책 승인	<ul style="list-style-type: none"> - 운영기관 또는 위탁기관의 담당자는 검토된 해결책의 적용 여부에 대해 검토/승인 활동을 수행한다. 	●	○		
3.1- ① 문제 조치	<ul style="list-style-type: none"> - 문제조치담당자는 승인된 해결책 적용을 위한 관련 활동을 수행한다. - 조치를 위해 변경작업이 필요한 경우 변경관리 프로세스를 통해 해당 작업이 진행되도록 요청/관리한다. - 조치 활동 이후 적합한 조치가 되었는지에 대한 검토를 수행하며, 부적합하다고 판단된 경우 문제검토 단계 활동을 재수행한다. - 조치의 적합성이 확인된 경우 운영기관 또는 위탁기관의 담당자에게 조치건의 검토를 요청한다. 			●	●
3.2- ③ 검토 및 종료	<ul style="list-style-type: none"> - 운영기관 또는 위탁기관의 담당자는 조치된 문제건을 검토/확인하고 해당 문제건을 종료한다. - 검토 단계에 부적합 사항이 발견된 경우 문제조치 단계를 재수행할 수 있다. - 해당 문제활동 이력은 관리되어야 하며 이후 경향분석 및 유사 장애 검토, 장애의 원인/해결책 검토 등에 활용 가능하도록 관리하여야 한다. - Output: 문제기록(영구해결책 포함): ITSM 활용시 KEDB 		●	○	

사. 핵심성과지표 (KPI : Key Performance Indicator)

프로세스 운영 품질 관리를 위해 프로세스 별 관리지표를 도출하여 관리함을 목표로 하며, 본 절차서에서 관리가능한 KPI를 제시하고 개별기관 별 운영 상황에 맞추어 조정하여 지표 관리

측정지표	측정방법	측정목적	측정주기
문제 적기 처리율	(목표 시간내 처리된 문제 건수 ÷ 당월 종료 처리된 문제건수) X 100	문제조치의 적기여부 관리(상호 합의된 처리시간 준수)	월간

아. 수행 검증

1) 검증 방법

- 검증 체크리스트의 체크항목 기준(ITIL 표준 준용)으로 표준운영절차의 준수여부와 이행점검을 수행한다.
- 개별기관 내 자체 프로세스 검증자는 내부 감사자의 자격 또는 ITIL에 대한 충분한 이해를 가진자가 수행한다. (ITIL 관련 자격 권고)
- 점검 결과는 대외 감사/진단 시 내부 점검 활동의 결과물로 활용할 수 있다.

2) 검증 항목

세부 절차	체크 항목	정성 평가	증적 체크
문제 등록	- 장애관리에서 임시해결 또는 근본원인이 미도출된 장애건에 대해서 문제관리로 이관되어 등록/관리되고 있습니까?	적합/부적합	<ul style="list-style-type: none"> • ITSM내 문제기록 • 문제관리대장(ITSM 미사용시)
	- 사전예방활동이나 타프로세스의 수행중 도출되는 잠재적 문제 등이 문제로 등록/관리되고 있습니까?		
	- 문제의 등록 기준이 정의되고 이해관계자에게 공유되어 있습니까?		<ul style="list-style-type: none"> • 문제등록기준
문제 분석	- 접수된 문제의 경우 문제의 적합성 여부를 검토/판단하여 접수 또는 반려하고 있습니까?		<ul style="list-style-type: none"> • ITSM내 문제기록 • 문제관리대장
	- 문제 분석시 임시해결책, 영구해결책으로 구분하여 관리하고 있습니까?		<ul style="list-style-type: none"> • ITSM내 문제기록 • 문제관리대장
	- 원인파악불가 또는 해결책 미도출로 처리해야되는 경우 해당 문제에 대한 처리/관리 기준을 정의하고 있습니까?		<ul style="list-style-type: none"> • 문제처리기준
문제 조치 및 종료	- 문제의 근본원인 조치를 위해 변경 프로세스와 연계하여 조치작업을 진행하고 있습니까?		<ul style="list-style-type: none"> • ITSM내 문제기록 • 문제관리대장
	- 잠재적 문제를 줄이기 위한 예방 활동(문제경향분석, 장애추이 등)이 수행되고 있습니까?		<ul style="list-style-type: none"> • 문제경향분석 이력

자. 관리 기준

1) 문제 등록(이관) 기준

구분	정의
근본원인 불명 및 임시조치 장애	○ 장애 조치 중 장애의 근본 원인이 도출되지 않은 경우나 임시해결책(재기동 등)을 통해 긴급히 장애 조치를 수행한 경우
원인 불명의 이벤트	○ 발생된 이벤트의 원인을 파악할 수 없는 경우
원인 불명의 변경실패	○ 변경작업이 실패하여 원복하였으나 실패의 원인을 알수 없는 경우나 기타 분석 활동이 필요한 경우
관리자의 판단	○ 타 프로세스의 관리자가 운영 활동중에 나타나는 잠재적 문제나 이슈 등에 대해 문제관리로 등록이 필요하다고 판단하는 경우
장애 경향 분석	○ 사전예방적 문제관리 활동으로 기 발생 장애에 대한 경향 분석이나 운영 모니터링 활동을 통해 도출되는 반복적 오류 등에 대해 근본적인 해결책이 필요하다고 판단되는 경우
이벤트 로그 분석	○ 반복적으로 발생하는 이벤트에 대해 장애예방 차원의 근본원인분석과 해결책이 필요하다고 판단되는 경우

2) 문제 종료 기준

구분	정의
문제 해결 종료	○ 근본 원인과 영구 해결책이 도출된 경우
문제 합의 종료	아래와 같은 상황 또는 기관 내 관계자 합의를 통해 문제를 합의 종료할 수 있음 ○ 문제 해결을 위해 시간 및 비용이 과도하게 소요되는 경우 ○ 기술적으로 해결이 불가능한 경우 ○ 문제 등록 후 3개월이 경과하였으나 기관 내 상황으로 해당 문제를 지속 관리할 수 없는 경우

3) 문제 관리대장 (예시)

문제 관리대장 (예시)													
문제ID	문제유형	문제시스템	제목	현재단계(상태)	문제등록일시	완료예정일	조치완료일시	업무담당자	처리자	임시해결책	영구해결책	조치내역	비고