행정·공공기관 정보시스템
표준운영절차 가이드

2026. 6.

행정안전부

NIA 한국지능정보사회진흥원

1. 목적

○ 표준운영절차는 정보시스템의 표준적인 운영·관리 절차로, 정보시스템 운영 체계화 및 장애발생요소 최소화를 통해 디지털정부 서비스 품질 제고를 목적으로 함

2. 추진 근거

○ 행정기관 및 공공기관 정보시스템 안정성 고시(행정안전부 고시 제2026-23호, 2026. 4. 13.) 제10조(표준운영절차)

> 제10조(표준운영절차) ① 중앙행정기관등의 장은 정보시스템 운영의 체계화와 장애발생요소 최소화를 위해 표준운영절차를 마련하여 적용하여야 한다. 단, A4등급 정보시스템의 경우 중앙행정기관등의 장의 판단에 따라 적용하지 아니할 수 있다.
> ② 행정안전부장관은 제1항에 따른 표준운영절차 마련을 지원하기 위해 표준운영절차 수립 안내서를 작성하여 중앙행정기관등의 장에게 제공할 수 있으며, 정보시스템 표준운영절차의 주요내용은 별표 3과 같다.

3. 표준운영절차(SOP) 적용 기준

* SOP : Standard Operating Procedure의 약자

○ 대상 정보시스템 : A1~A3등급 정보시스템 의무 적용, A4등급 적용 권고

※ 재해복구시스템의 경우, 별도 표준운영절차 없이 주 시스템의 표준운영절차에 따름

○ 적용시기 : A1~A4등급 정보시스템으로 재분류·확정 통보일로부터 3개월 이내 표준운영절차 수립

○ 적용기준 : A1~A3등급은 13개 표준운영절차 적용 의무화, A4등급은 8개 표준운영절차 적용 및 기록관리 권고

- A1~A3등급 정보시스템 응용프로그램(AP) 운영 : 9개 절차 적용

  · 공통 표준운영절차 4개(요청, 변경, 장애, 문제관리)와 AP 표준운영절차 5개(배포, 테스트, 연계, 형상, 운영상태관리) 적용

- A1~A3등급 정보시스템 인프라 운영 : 8개 절차 적용
  · 공통 표준운영절차 4개(요청, 변경, 장애, 문제관리)와 인프라 표준운영절차 4개(구성, 이벤트, 서비스수준, 백업관리) 적용
- A1~A3등급 정보시스템 AP, 인프라 통합운영 : 13개 절차 적용
  · 공통 표준운영절차 4개(요청, 변경, 장애, 문제관리), AP 표준운영절차 5개(배포, 테스트, 연계, 형상, 운영상태관리)와 인프라 표준운영절차 4개(구성, 이벤트, 서비스수준, 백업관리) 적용
- A4등급 정보시스템 응용프로그램(AP) 운영 : 6개 절차 권고
  · 공통 표준운영절차 3개(변경, 장애, 문제관리)와 AP 표준운영절차 3개(배포, 테스트, 형상관리) 적용
- A4등급 정보시스템 인프라 운영 : 5개 절차 권고
  · 공통 표준운영절차 3개(변경, 장애, 문제관리)와 인프라 표준운영절차 2개(서비스수준, 백업관리) 적용
- A4등급 정보시스템 AP, 인프라 통합운영 : 8개 절차 권고
  · 공통 표준운영절차 3개(변경, 장애, 문제관리), AP 표준운영절차 3개(배포, 테스트, 형상관리)와 인프라 표준운영절차 2개(서비스수준, 백업관리) 적용

4. 표준운영절차 활용방법

○ 본 안내서는 행정·공공기관 정보시스템(인프라 및 응용프로그램)의 안정적·효율적 운영을 위한 통합 표준운영절차 기준을 제시함

○ 글로벌 IT 서비스 관리 표준인 ITIL v4 및 ISO/IEC 20000을 기반으로 하며, 행정·공공기관의 정보자원관리 정책 및 지침과 연계하여 수립됨

○ 기관은 본 안내서의 적용 기준에 따라 표준운영절차를 도입·운영하여야 하며, 기관의 정보시스템 규모·등급·서비스 특성에 따라 표준운영절차 세부사항을 선택적으로 추가·변경·삭제하여 운영할 수 있음

○ 기관별 IT서비스 관리체계(ITSM 등)와 연계하여 지속적으로 개선·보완되어야 함

5. 표준운영절차 주요내용

구분	절차명	절차별 주요내용
공통	요청관리	• 서비스 요청 관리 범위와 절차 정립 • 요청 등록, 분류, 처리, 고객 만족도 조사, 단계 승인 절차
	변경관리	• 인프라/응용프로그램 변경관리 범위와 운영 절차 정립 • 변경 접수 및 검토, 계획 수립, 변경작업, 원복 절차
	장애관리	• 장애 관리 기준과 처리 절차 정립 • 장애 식별 및 접수, 조사 및 진단, 해결 및 복구 절차
	문제관리	• 문제 관리 기준과 절차 정립 • 문제 등록 및 검토, 조사 및 진단, 해결 및 복구 절차
인프라	구성관리	• 구성항목의 식별과 분류 체계 정립 • 구성 통제, 구성관리데이터베이스(CMDB) 운영, 구성감사 절차
	이벤트관리	• 이벤트 정의와 관리 범위 정립 • 이벤트 접수 및 검토, 처리 절차
	서비스수준관리	• 서비스 수준 정의와 관리 방법 정립 • 서비스 수준 평가 지표
	백업관리	• 백업 정책의 수립과 이행 증적 관리 프로세스 정립
응용 프로그램 (AP)	배포관리	• 배포 계획 수립 및 검토, 승인, 배포 수행 및 검증(테스트), 배포 결과 검토 및 종료
	테스트관리	• 테스트 수행 기준 정의, 테스트 계획 수립 및 설계, 개발환경 및 운영환경 테스트 절차 정의, 테스트 결과 분석 및 개선
	연계관리	• 연계 요청 및 검토(사전 연계 협의), 연계 계획 수립 및 검토, 검토 결과 회신, 연계 결과 검토
	형상관리	• 형상 항목 식별 및 형상 관리 시스템 구축, 형상 변경 승인 및 통제 (Control), 형상 감사(Audit) 및 기록
	운영상태관리	• 운영상태관리 정책과 계획 수립, 운영상태 모니터링 및 운영이벤트 조치 • 사후관리(예방점검, 최적화, 개선 등) 기준 정립

【별첨】

정보시스템 표준운영절차서

(안내) 본 표준운영절차서는 행정·공공기관의 정보시스템 운영·관리를 위한 표준운영절차 마련을 지원하기 위해 마련한 표준안이며, 기관은 본 안내서의 적용기준에 따라 표준운영절차를 도입·운영하여야 하며, 기관의 정보시스템 운영·관리 유형(인프라, 응용프로그램), 정보시스템 규모·등급·서비스 특성에 따라 표준운영절차를 선택적으로 추가·변경·삭제하여 운영하여야 함

※ '26년 개편 등급 확정 통보일로부터 3개월 이내 표준운영절차서 마련

※ A1-A3등급 표준운영절차 적용 필수, A4 등급 적용 권고

2026. 0.

기관명

문서 개정 이력표				
버전	날짜	내용	작성자	승인자
1.0	*2026.07.*	*정보시스템 표준운영절차서*		

< 목 차 >

기관의 정보시스템 유형, 등급 등에 따라 표준운영절차 선택적으로 적용

◈ 개요 1

Ⅰ. 공통 7
1. 요청관리 절차서 7
2. 변경관리 절차서 19
3. 장애관리 절차서 39
4. 문제관리 절차서 58

Ⅱ. 인프라 71
5. 구성관리 절차서 71
6. 이벤트관리 절차서 89
7. 서비스수준관리 절차서 100
8. 백업관리 절차서 118

Ⅲ. 응용프로그램 136
9. 배포관리 절차서 136
10. 테스트관리 절차서 147
11. 연계관리 절차서 158
12. 형상관리 절차서 168
13. 운영상태관리 절차서 178

◈ 개요

가. 목적

○ 본 절차서는 행정·공공기관 정보시스템의 안정적·효율적 운영을 위한 표준운영절차 기준을 제공한다.

○ 글로벌 IT 서비스 관리 표준인 ITIL v4 및 ISO/IEC 20000을 기반으로 하며, 행정·공공기관의 정보자원관리 정책 및 지침과 연계하여 수립된다.

나. 적용 범위

○ 행정·공공기관 정보시스템의 운영관리 활동에 적용된다.

다. 역할 분담 기준

○ 표준운영절차의 운영에 있어 주요 역할에 대한 기준을 제공한다.

○ 표준운영절차별 상세 역할과 책임을 정의한다.

○ 역할과 책임의 상세 항목은 각 행정·공공기관의 조직구조/운영환경에 따라 개별 정의할 수 있다.

구분	주요 역할	세부 내용
운영기관 (정보시스템 운영의 최종 책임기관)	관리자	• 행정·공공기관 내 정보시스템 운영을 총괄하는 부서장 또는 상위 책임자 • 주요 운영관리 활동, 운영절차 점검·관리활동에 대한 의사결정 수행
	담당자	• 정보시스템 운영절차 준수 여부를 점검할 수 있는 내부 감사, 점검부서 또는 독립적인 점검 담당자 • 변경, 장애, 배포, 백업, 점검 등 주요 운영 활동에 대한 검토 및 승인 수행 • 운영기관, 운영자, 유관기관 간 협의 및 의사소통 창구 역할 수행 • 운영절차 점검 및 관리 업무 수행
수탁기관 또는 운영사업자	운영자	• 운영기관과의 계약에 따라 정보시스템 운영관리 업무 수행 • 시스템 모니터링, 배포, 백업, 장애대응, 문제관리 등 운영 전반의 실무 수행 • 정보시스템을 구성하는 하드웨어, 소프트웨어, 미들웨어 및 응용프로그램에 대한 기술지원 수행 • 장애 복구, 패치 적용, 성능 개선, 기능 보완 등 유지보수 활동 수행

※ 기관의 조직·인력 여건에 따라 역할과 책임은 조정할 수 있음..

라. 운영절차 점검 및 관리방안

○ 정보시스템 운영기관은 정보시스템 운영절차를 수립하고, 운영절차의 적용범위, 역할 및 책임 기준을 관리한다.

○ 관리자는 운영절차 이행현황을 감독하고, 미준수 사항 및 개선조치 결과를 확인한다.

○ 정보시스템 운영기관은 운영절차의 적정성, 현행화 필요사항 및 개정 필요사항을 연 1회 이상 정기 검토한다.

○ 정보시스템 운영기관은 법령·고시·지침 변경, 조직 및 역할 변경, 정보시스템 등급 변경, 중대한 장애 발생, 감사·점검 지적사항 발생 등 운영절차 변경이 필요한 경우 수시 검토한다.

○ 정보시스템 운영기관은 운영절차 개정 필요사항을 식별하고, 개정안을 작성·관리한다.

○ 운영절차 검토, 개정, 승인, 배포, 이행점검 및 모니터링 결과는 관련 이력으로 관리한다.

마. 용어 정의

용어	설명
표준운영절차	○ 정보시스템의 표준적인 운영·관리절차로, 운영 체계화 및 장애발생요소 최소화를 통해 디지털정부 서비스 품질 제고를 목적으로 한다.
정보시스템	○ 「전자정부법」 제2조 제13호에 따른 정보의 수집·가공·저장·검색·송신·수신 및 그 활용과 관련되는 기기와 소프트웨어의 조직화된 체계를 말한다.
응용프로그램	○ 정보시스템에서 운영체제 및 미들웨어 등 기반 소프트웨어 상에서 실행되어, 대국민 서비스 또는 행정업무 수행을 위한 업무처리 기능을 제공하는 소프트웨어를 말한다.
인프라	○ 응용프로그램이 작동할 수 있도록 환경을 제공하는 하드웨어 및 기반 소프트웨어를 말한다.

바. 표준운영절차

○ 13개 표준운영절차에 대한 기본 설명

구분	표준운영절차	설명
공통	1. 요청관리 (Customer Service Request Management)	• 서비스 요청 관리 범위와 절차 정립 • 요청 등록, 분류, 처리, 고객 만족도 조사, 단계 승인 절차
	2. 변경관리 (Change Management)	• 정보시스템 변경 관리 범위와 운영 절차 정립 - 변경 요청 접수 및 검토 - 변경 계획 수립 및 검토, 승인 - 변경 작업, 원복 절차 및 변경 평가
	3. 장애관리 (Incident Management)	• 장애 식별·접수·조사·진단 및 복구 절차 정립 • 장애 복구 결과 검증 및 보고 수행
	4. 문제관리 (Problem Management)	• 근본 원인 분석 수행 및 개선 절차 수립 • 재발방지대책 수립 및 개선 결과 검증
인프라	5. 구성관리 (Configuration Management)	• 구성항목의 식별과 분류 체계 정립 • 구성 통제, 구성관리데이터베이스 운영, 구성감사 절차
	6. 이벤트관리 (Event Management)	• 이벤트 정의와 관리 범위 정립 • 이벤트 접수 및 검토, 처리 절차
	7. 서비스수준관리 (Service Level Management)	• 서비스 수준 정의 및 관리 방법 정립 • 서비스 품질 지표 모니터링 및 개선 활동 수행
	8. 백업관리 (Backup Management)	• 백업 정책 수립·수행·검증·로그 관리 절차 정립 • 백업·복구 증적 관리 및 보고
응용	9. 배포관리 (Release and Deployment Management)	• 배포 관리 기준과 절차 정립 - 배포 계획 수립 및 검토, 승인 - 배포 검증(테스트) 및 수행 - 배포 결과 검토 및 종료
	10. 테스트관리 (Validation and Testing Management)	• 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
	11. 연계관리 (Integration Management)	• 연계관리 기준과 절차 정립 - 연계 요청 및 검토(사전 연계 협의) - 연계 계획 수립 및 검토, 검토 결과 회신 - 연계 결과 검토
	12. 형상관리 (Operational Configuration Management)	• 소스코드, 산출물, 문서 등 형상 식별·버전관리 • 형상 감사(Audit), 변경 통제 및 승인 수행 • 형상관리 도구 기반 이력 관리
	13. 운영상태관리 (Monitoring and Event Management)	• 운영시스템 상태관리 정책 및 운영이벤트 조치 기준 정립 - 운영상태관리 정책과 계획 수립 - 운영상태 모니터링 및 운영이벤트 조치 - 사후관리(예방점검, 최적화, 개선 등)

참고. ITIL v4 및 ISO/IEC 20000와 표준운영절차 비교표

1) 공통 표준운영절차

표준운영절차	표준운영절차 주요내용	ITIL v4	ITIL v4 주요내용	ISO/IEC 20000	ISO/IEC 20000 주요내용	비고
요청 관리	정보시스템 운영 중 발생하는 사용자의 다양한 요청사항을 신속하게 등록, 분류, 처리하고 고객 만족도를 조사하여 응대하는 절차임	요청 관리 (Request Fulfilment)	사용자가 빈번하게 요구하는 위험이 낮고 적은 비용이 소요되는 소규모 변경(패스워드 재설정 등), 정보/자문 등의 서비스 요청(Service Request)을 처리하는 프로세스임	서비스 요청 관리 (Service Request Management)	서비스 요청 관리는 사용자의 서비스 요청을 기록·분류하고, 우선순위를 결정한 후 이행 및 종료까지 관리하는 활동 요청 처리 과정에서 수행한 조치는 기록에 반영하여 최신화하고, 요청 이행에 필요한 지침을 관련 담당자에게 제공(8.6.2)	
변경 관리	인프라 및 애플리케이션의 구성 상태를 변경할 때 서비스 영향을 최소화하기 위해 계획 수립, 변경관리위원회(CAB) 심의, 2단계 승인, 테스트 및 원상복구 계획을 통제하는 절차임	변경 관리 (Change Enablement Management)	IT 서비스에 영향을 미칠 수 있는 모든 변경의 수명주기를 통제하며, 변경심의위원회(CAB)를 운영하고 최소한의 중단으로 유익한 변경이 이루어지도록 통제하는 프로세스임	변경 관리 (Change Management)	변경 관리는 서비스 및 서비스 구성요소에 대한 변경을 통제하기 위해 변경관리 정책을 수립하고, 변경요청을 기록·분류한 후 영향도, 위험, 사업적 이익, 실행 가능성 및 재정적 영향을 검토하여 승인·우선순위를 결정하는 활동(8.5.1)	
장애 관리	정보시스템 운영 중 장애 발생 시 최대한 신속하게 원인을 분석하고 임시/영구 해결책을 적용하여 정상적인 서비스를 복구하는 데 최우선 목적을 두는 절차임	인시던트 관리 (Incident Management)	서비스를 중단시키거나 품질을 감소시키는 모든 이벤트를 다루며, 사용자가 최대한 신속하게 정상 비즈니스 업무로 복귀할 수 있도록 서비스를 재개하는 데 초점을 맞추는 프로세스임	장애 관리 (Incident Management)	인시던트 관리는 서비스 중단 또는 품질 저하가 발생하거나 발생할 가능성이 있는 사항을 기록·분류하고, 영향도와 긴급도를 고려하여 우선순위를 정한 후 필요한 경우 에스컬레이션하여 해결·종료하는 활동(8.6.1)	
문제 관리	장애 처리 중 근본 원인이 파악되지 않은 문제에 대해 심층 분석으로 근본 원인과 해결 방안을 도출하고, 동일 장애 재발을 방지하기 위한 예방 활동을 수행하는 절차임	문제 관리 (Problem Management)	인시던트의 알려지지 않은 근본 원인을 진단하여 영구 해결책을 찾고, 장애 재발을 방지하며, 알려진 오류 데이터베이스(KEDB)를 구축 및 유지관리하는 프로세스임	문제 관리 (Problem Management)	문제 관리는 인시던트 데이터와 경향을 분석하여 문제를 식별하고, 근본 원인 분석을 통해 인시던트의 발생 또는 재발 방지 조치를 결정하는 활동 문제는 기록·분류·우선순위 결정·필요 시 이관·해결·종료 절차에 따라 관리하며, 변경이 필요한 경우 변경관리 정책에 따라 처리함 근본 원인이 확인되었으나 영구 해결되지 않은 경우 알려진 오류로 기록함(8.6.3)	

2) 인프라 표준운영절차

표준운영절차	표준운영절차 주요내용	ITIL v4	ITIL v4 주요내용	ISO/IEC 20000	ISO/IEC 20000 주요내용	비고
구성 관리	HW, SW, 네트워크 장비 등 구성항목의 등록, 변경, 재사용, 폐기 등 생명주기와 이력을 관리하며, 구성정보 데이터베이스(CMDB)를 최신으로 유지하고 구성 감사를 수행하는 절차임	서비스 구성 관리 (Service Configuration Management)	IT 서비스를 제공하는 구성항목(CI)의 생명주기 및 상호 의존성을 식별·제어하며, 구성관리 시스템(CMS)과 CMDB를 정확하게 현행화하여 타 프로세스에 제공하는 프로세스임	구성 관리 (Configuration Management)	구성 관리는 서비스를 포함한 구성항목(CI)의 유형을 정의하고, 서비스 중요도와 유형에 적합한 수준으로 구성정보를 기록·통제하는 활동임 각 CI는 식별자, 유형, 설명, 관계, 상태 정보를 포함하여 관리하며, 변경사항은 추적·감사 가능해야 함 변경 배치 후 구성정보를 현행화하고, 계획된 주기로 정확성을 검증하여 필요한 서비스관리 활동에 제공(8.2.6)	
이벤트 관리	모니터링 도구와 육안을 통해 시스템에서 발생하는 이벤트를 감지 및 분석하고 조치하며, 타 프로세스(장애, 변경, 문제 등)로 이관하여 잠재적 위험을 예방하는 절차임	이벤트 관리 (Event Management)	적극적/소극적 모니터링 툴을 활용해 IT 인프라/서비스의 상태를 파악하고, 정상 운영을 벗어나는 예외사항을 탐지 및 분석하여 경보를 생성하는 프로세스임	모니터링, 측정, 분석 및 평가 (Monitoring, measurement, analysis and evaluation)	모니터링, 측정, 분석 및 평가는 SMS 및 서비스의 성능과 효과성을 확인하기 위해 모니터링·측정 대상, 방법, 수행 시점 및 분석·평가 시점을 정하고 그 결과를 문서화된 정보로 유지하는 활동임 운영상태관리에서는 서비스 상태와 성능 정보를 모니터링하고, 측정 결과를 분석·평가하여 서비스 요구사항 충족 여부와 개선 필요사항을 확인하는 기준으로 활용함(9.1)	ISO 20000 직접절차 없음
서비스 수준 관리	제공하는 IT 서비스의 목표 수준을 상호 협의(SLA)하여 지표(KPI)를 선정하고, 월간 실적 수집, 평가, 보고 및 서비스 개선 활동을 수행하여 합의된 품질을 유지하는 절차임	서비스 수준 관리 (Service Level Management)	비즈니스 목적에 맞춰 제공할 IT 서비스의 목표 품질(SLA)을 협상 및 합의하고, 이를 모니터링, 측정, 보고, 검토하여 서비스 품질을 보장하는 프로세스임	서비스 수준 관리 (Service Level Management)	SLA에는 서비스 수준 목표, 업무부하 한계 및 예외사항을 포함하며, 계획된 주기로 서비스 수준 목표 대비 성과와 업무부하 변화를 모니터링·검토·보고함 서비스 수준 목표를 달성하지 못한 경우에는 원인을 확인하고 개선기회를 식별하여 서비스 개선 활동에 반영함(8.3.3)	
백업 관리	재해나 하드웨어 고장으로부터 데이터를 보호하고 업무 연속성을 보장하기 위해, 정기적인 백업 정책을 수립하고 매체 소산 및 복구 모의 훈련을 수행하는 절차임	가용성 / 연속성 관리 Availability / Service Continuity Management	IT 인프라를 일상적으로 실행하고 유지보수하는 기능을 뜻하며, 이 중 운영 통제 활동의 핵심 항목으로 데이터의 '백업 및 재개'를 명시하여 수행함	가용성 / 연속성 관리 Availability / Service Continuity Management	서비스 가용성 및 연속성 관리는 서비스 사용 가능 상태를 유지하고, 중대한 서비스 손실 발생 시 복구 요구사항에 따라 서비스를 복구하기 위한 위험평가, 목표관리, 모니터링, 복구계획 및 테스트 활동을 포함함 백업관리는 서비스 중단 또는 데이터 손실 시 복구 가능성을 확보하는 운영수단으로, 백업 수행·복구검증·테스트 결과를 통해 서비스 가용성 유지와 서비스 연속성 확보를 지원하는 활동으로 봄(가용성:8.7.1 연속성:8.7.2)	ITIL, ISO 20000 직접절차 없음

3) 응용 표준운영절차

표준운영절차	표준운영절차 주요내용	ITIL v4	ITIL v4 주요내용	ISO/IEC 20000	ISO/IEC 20000 주요내용	비고
배포 관리	응용프로그램 변경요청을 운영환경에 반영하기 위해 배포 계획 수립, 테스트 완료 및 반영 등 배포과정의 위험을 최소화하는 절차임	릴리스 및 배치 관리 (Release and Deployment Management)	릴리스를 패키지, 빌드, 테스트하여 실제 운영 환경에 성공적으로 배치하고 고객에게 가치를 제공할 수 있도록 통제하는 프로세스임	릴리스 및 배치 관리 (Release and Deployment Management)	릴리스 및 배치 관리는 신규 또는 변경된 서비스와 서비스 컴포넌트를 실제 환경에 안정적으로 배치하기 위해 릴리스 유형, 배치계획, 변경관리 연계, 인수기준 확인, CI 베이스라인 설정 및 실제 환경 배치를 관리하는 활동임 배치 후에는 릴리스의 성공·실패와 관련 인시던트를 모니터링·분석하고, 그 결과를 기록·검토하여 개선기회와 향후 릴리스 정보를 다른 서비스관리 활동에 제공함(8.5.3)	
테스트 관리	응용프로그램의 변경 기능이 정상적으로 동작하는지 확인하고 단위, 통합, 성능, 인수 테스트 등을 통해 요구사항 부합 여부를 검증하는 절차임	서비스 검증 및 테스트 (Service Validation and Testing)	신규 또는 변경된 IT 서비스가 설계 사양을 충족시키고 비즈니스 니즈를 충족시키는지 확인하고 테스트하는 프로세스임	서비스 설계 및 전환 (Service Design and Transition)	서비스 설계 및 전환은 신규·변경 서비스, 서비스 제거 또는 기존 서비스 이전이 서비스 요구사항을 충족하도록 계획·설계·구축·전환하는 활동임 조직은 권한과 책임, 일정, 자원, 종속성, 테스트, 서비스 인수 기준, 영향 및 의도된 결과를 정하고, 구축·테스트 후 인수 기준 충족 여부를 확인함 승인된 서비스는 릴리스 및 배치 관리를 통해 실제 환경에 배치하며, 전환 완료 후 의도된 결과 대비 성과를 이해관계자에게 보고함(8.5.2)	
연계 관리	연계 시스템 간 원활한 데이터 흐름과 상호운영성을 보장하여 데이터 정합성을 확보하고 연계 인터페이스를 구성, 검증(테스트), 모니터링하는 절차임	서비스 확인 및 릴리스 테스트 (Service Validation and Testing)	전체 시스템 및 다른 서비스 구성요소들과 통합된 상태에서 인터페이스 및 데이터 상호작용이 설계대로 동작하는지 확인하는 프로세스임	구성 관리 (Configuration Management)	외부망과의 연계 인터페이스에 변경이 발생했을 때, 이를 구성 정보에 즉각 반영하기 위한 내부 기준을 주체적으로 마련해야 함 연계 대상 시스템, API, 인터페이스, 송수신 항목, 연계 구성요소 및 관계정보를 구성항목(CI) 관점에서 관리하는 활동임(8.2.6)	ITIL, ISO/IEC 20000 직접절차 없음
형상 관리	응용프로그램의 소스코드, 산출물 등 형상항목의 변경이력을 체계적으로 추적하고 통제하여 무결성과 일관성을 유지하는 절차임	구성 관리 (Service Configuration Management)	IT 서비스를 제공하는 구성항목(CI)에 대한 정보를 수명주기 전반에 걸쳐 식별, 통제하고 구성관리 시스템(CMS)을 유지관리하는 프로세스임	구성 관리 (Configuration Management)	구성 관리는 서비스를 포함한 구성항목(CI)의 유형을 정의하고, 서비스 중요도와 유형에 적합한 수준으로 구성정보를 기록·통제하는 활동임 각 CI는 식별자, 유형, 설명, 관계, 상태 정보를 포함하여 관리하며, 변경사항은 추적·감사 가능해야 함 변경 배치 후 구성정보를 현행화하고, 계획된 주기로 정확성을 검증하여 필요한 서비스관리 활동에 제공.(8.2.6)	
운영상태 관리	응용프로그램 및 운영 시스템 자원의 상태와 성능을 지속적으로 모니터링하고 이벤트를 감지하여 이상 징후에 신속히 대응하고 최적화를 수행하는 절차임	이벤트 관리 (Monitoring Management)	모니터링 툴을 활용해 IT 인프라/서비스의 상태를 파악하고, 정상 운영을 벗어나는 예외사항을 탐지 및 분석하여 경보를 생성하는 프로세스임	모니터링, 측정, 분석 및 평가 (Monitoring, measurement, analysis and evaluation)	모니터링, 측정, 분석 및 평가는 SMS 및 서비스의 성능과 효과성을 확인하기 위해 모니터링·측정 대상, 방법, 수행 시점 및 분석·평가 시점을 정하고 그 결과를 문서화된 정보로 유지하는 활동임 운영상태관리에서는 서비스 상태와 성능 정보를 모니터링하고, 측정 결과를 분석·평가하여 서비스 요구사항 충족 여부와 개선 필요사항을 확인하는 기준으로 활용함(9.1)	ISO 20000 직접절차 없음

1. 요청관리 절차서

가. 개요

1) 목적

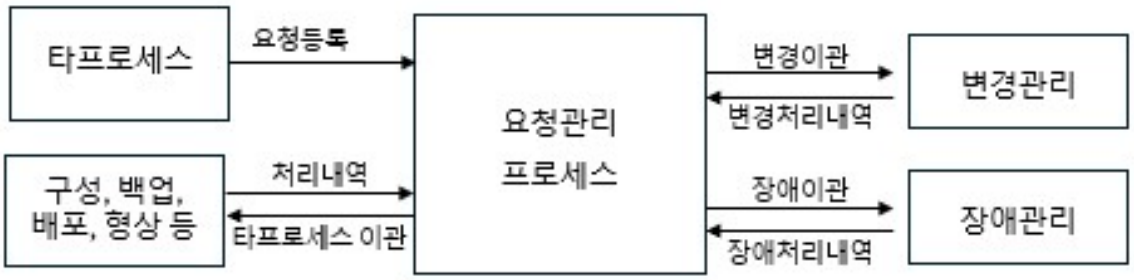
○ 정보시스템 운영 과정에서 발생하는 사용자의 다양한 요청사항(CSR: Customer Service Request)을 처리하기 위하여 유형별 처리 기준을 명시하고, 신속한 응대 및 처리를 위한 표준절차를 제공함으로써 서비스 사용자의 요청사항을 누락 없이 요구된 시간 내에 효과적으로 처리하는 것을 목적으로 한다.

2) 적용 범위

○ 요청관리 절차는 행정·공공기관 정보시스템의 요청관리에 적용한다.

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 관리대장 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	정보시스템 운영 과정에서 발생하는 서비스 요청은 표준화된 요청관리 절차에 따라 접수·분류·처리·이관·종료되어야 한다.
	설명	○ 요청관리 절차는 서비스 요청의 등록, 분류, 처리, 처리결과 확인, 만족도 조사 및 필요한 경우 단계별 승인 절차를 포함하여야 한다. ○ 요청사항은 정보시스템 운영관리 범위에서 발생하는 요청을 포함한다. ○ 요청사항이 장애, 변경, 백업, 구성, 배포 등 다른 표준운영절차의 수행이 필요한 사항인 경우 해당 절차로 이관하여 처리한다.
정책 2	기준	서비스 요청은 ITSM 등 표준운영절차 운영시스템 또는 요청관리대장을 통해 객관적으로 기록·관리되고 처리 이력이 추적되어야 한다.
	설명	○ 모든 요청관리는 표준운영절차 운영시스템을 통해 요청 등록, 접수, 분류, 처리, 승인, 결과 확인 등 처리과정과 이력을 관리하여야 한다. ○ 다만, 시스템이 없는 경우 표준화된 절차를 기반으로 관련 이력이 수기 데이터로도 기록·관리되어야 한다. ○ 요청 처리과정과 처리결과는 향후 장애관리, 변경관리, 문제관리 및 서비스 수준관리의 분석자료로 활용할 수 있도록 관리하여야 한다.

다. 용어 정의

용어	설명
서비스 데스크	○ 사용자로부터의 문의, 사용자 장비의 장애, 응용프로그램 기능 개선 요청 등에 대한 최초 접수 창구로서 요청에 대한 진행사항 등을 관리하고, 사용자와의 커뮤니케이션을 진행한다.
서비스 요청	○ 사용자로부터 접수되는 IT 서비스에 대한 요청사항으로 문의 사항, 변경 요청, 응용프로그램에 대한 기능 개선 요청, 일반적인 작업 요청 등을 말한다.
이관	○ 작업의 처리를 위해 관리자나 전문가 집단에게 처리를 넘기거나, 타 프로세스 처리가 필요한 작업을 해당 프로세스로 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	○ 서비스 요청 작업 대상 정보시스템의 담당자가 역할 수행 ○ 사용자의 요청사항에 대해 사전검토 등의 활동을 수행하고 필요시 사용자의 서비스 요청 내용을 운영사업자에게 대행 요청하는 등의 활동 수행 ○ 요청 건에 대한 이해당사자 간 조율 및 의사소통 창구 ○ 서비스 요청의 적합 여부 검토 ○ 서비스 요청 처리 결과의 적합성 검토	
수탁기관 또는 운영사업자	운영자	○ 운영기관과의 계약을 통해 정보시스템의 운영과 요청의 처리를 담당하는 수탁기관 또는 운영사업자 ○ 정보시스템을 구성하는 HW, SW, 미들웨어 등의 제조사 또는 유지보수를 담당하는 사업자 ○ 서비스 데스크 역할 : 서비스 요청 작업의 접수 및 분류 ○ 서비스 요청에 대한 처리 수행 - 응대, 답변, 자료 제공 등	

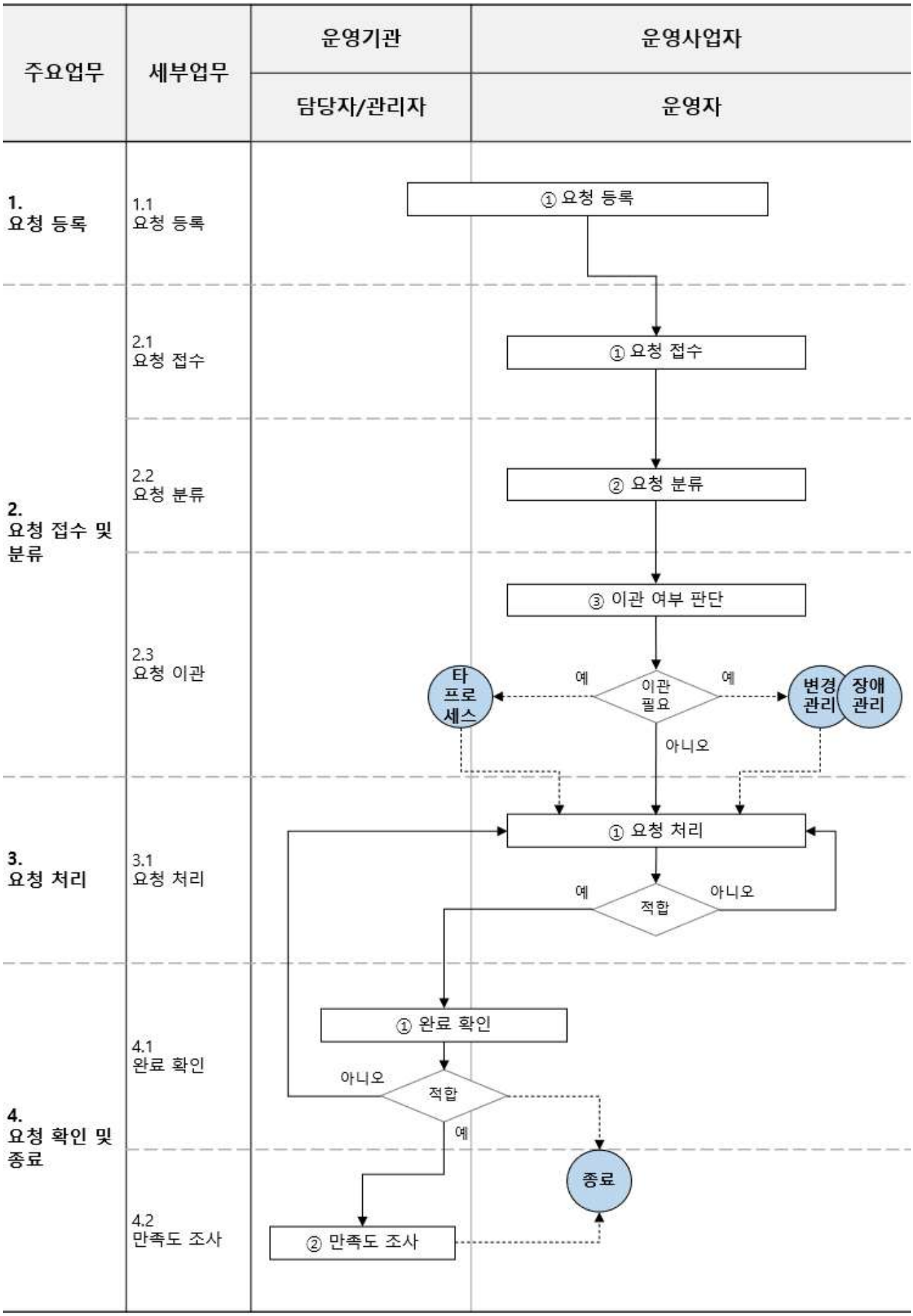
마. 표준절차 흐름도

○ 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 또는 요청자는 ITSM 등 표준운영절차 운영시스템을 통해 서비스 요청을 등록한다. ○ 메일 혹은 대면 등으로 접수된 사항은 운영기관 담당자 또는 운영자가 대행 등록을 수행한다. ○ ITSM 등 운영시스템이 없는 경우 요청관리대장 등 문서 형태로 기록·관리할 수 있다.
2. 요청 접수 및 분류	2.1 요청 접수	○ 서비스 요청 사항을 접수하고, 요청 내용이 불명확하거나 정보가 부족한 경우 요청자에게 추가 정보를 요청하여 보완한다.
	2.2 요청 분류	○ 서비스 요청을 유형별로 분류하고, 담당자에게 배정한다. ○ 담당자 재배정이 필요한 경우에는 다른 담당자에게 재배정한다.
	2.3 요청 이관	○ 서비스 요청 내용에 따라 장애관리, 변경관리, 백업관리, 구성관리, 배포관리, 테스트관리, 연계관리, 형상관리 등 관련 표준운영절차로 이관하여 처리할 수 있다.
3. 요청 처리	3.1 요청 처리	○ 서비스 요청 처리 담당자는 요청사항을 처리하고, 처리과정 및 처리 결과를 표준운영절차 운영시스템 또는 요청관리대장에 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	운영사업자
		관리자/담당자	운영자
1.1- ① 요청 등록	- 사용자는 ITSM 등 표준운영절차 운영시스템을 통해 업무 요청, 변경 요청, 서비스 개선 요청 등 필요한 서비스를 등록한다. - 전화, 메일, 대면 등으로 접수된 요청은 운영기관 담당자 또는 운영자가 표준운영절차 운영시스템에 대행 등록한다. - ITSM 등 운영시스템이 없는 경우 요청관리대장 등 문서 형태로 기록·관리할 수 있다.	●	●
2.1- ① 요청 접수	- 메일 혹은 대면 등으로 접수된 사항은 ITSM 시스템에 요청을 받은 담당자가 대행 기록(등록)한다. - ITSM 등 운영시스템이 없는 경우 요청관리대장 등 문서 형태로 기록·관리할 수 있다. - 서비스 데스크가 있는 기관은 서비스 데스크를 통해 요청을 접수하고, 서비스 데스크가 없는 경우 운영기관 담당자 또는 운영자가 요청을 접수한다. - 접수된 서비스 요청의 정보가 충분하지 않으면 요청자에게 추가 정보를 요청하여 보완한다. - 정책 혹은 기타 사유로 서비스 요청을 처리할 수 없는 경우 반려 사유를 안내하고 종료 처리한다.		●
2.2- ② 요청 분류	- 서비스 데스크 담당자는 서비스 요청을 사전 정의된 유형별로 분류한다. - ITSM 시스템을 활용하는 경우, 사전 정의된 분류 유형에 따라 처리, 이관 등의 절차가 수행될 수 있도록 관리한다. - 서비스 요청을 영향도, 해결의 시급함 등에 따라 우선순위를 결정하고 담당자에게 배정한다. - 요청 처리를 위해 담당자 재배정이 필요한 경우는 적합한 다른 담당자에게 배정한다.		●
2.3- ③ 이관 여부 판단	- 서비스 요청 건의 처리를 위해 타 프로세스로의 이관이 필요한 경우 해당 프로세스로 작업을 이관한다. ※ 장애, 변경, 백업, 구성, 배포, 테스트, 연계, 형상 등		●

(●: 정, ◑: 부)

세부 절차	수행 내용	운영기관	운영사업자
		관리자/담당자	운영자
3.1- ① 요청 처리	- 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 처리 작업을 재수행하거나 다른 담당자에게 이관할 수 있다. - 배정된 요청의 처리를 위해 다른 담당자에게 이관이 필요한 경우 처리 담당자를 지정하여 요청 작업 건을 이관한다. (필요시 요청 분류 단계로 이관하여 재분류 작업의 수행 절차로 진행할 수 있다.) - 관련 표준운영절차로 이관된 요청의 경우 해당 절차의 처리결과를 확인한 후 서비스 요청 건의 해결 여부를 확인한다.		●
4.1- ① 완료 확인	- 요청자는 처리 결과를 확인하고, 운영기관 담당자는 필요한 경우 처리 결과의 적합 여부를 검토한다. - 적합한 경우 해당 요청 건은 종료되며, 해당 요청 건이 만족도 조사 활동이 필요한 경우 만족도 조사 단계를 진행한다. - 처리결과가 부적합하거나 추가 조치가 필요한 경우 재작업 또는 관련 절차 이관을 요청할 수 있다.	●	◑
4.2- ② 만족도 조사	- 만족도 조사를 수행해야 하는 서비스 요청 건에 대해서 요청자는 처리 결과에 대한 만족도를 평가한다. - 해당 만족도 조사는 이를 지원할 수 있는 ITSM 시스템 등이 있는 경우에 실시한다. (ITSM 등 운영시스템이 없는 경우 서비스 요청 처리의 품질 관리를 위해 연 1회 이상 수기 사용자 만족도 조사를 권고) - 만족도 조사에 응한 경우 해당 서비스 요청 건은 종료되며, 만족도 조사에 응하지 않은 경우 특정 기간 (예시: 1주일)이 지나면 자동 종료 처리할 수 있다.	●	

사. 핵심성과지표 (KPI : Key Performance Indicator)

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

측정 지표	측정 방법(예시)	측정 목적	측정 주기
서비스 요청 일정 준수율	(납기 내 요청 처리 건수 / 당월 종료된 요청 건수) X 100	서비스 요청 일정 준수 (운영시스템이 없는 경우에도 최소한의 납기일정은 준수 권고)	당월

※ ITSM 등의 운영시스템 미사용 시에는 서비스 품질 향상을 위해 만족도 평가 KPI를 연간 관리지표로 권고

만족도 점수	만족도 점수 총합 / 만족도 답변 건수	서비스 만족도 확인	당월

아. 수행 검증

1) 검증 방법

○ 검증 체크리스트의 체크 항목 기준(ITIL 표준 준용)으로 표준운영절차의 준수 여부와 이행 점검을 수행한다.

○ 개별기관 내 자체 프로세스 검증자는 내부 감사자의 자격 또는 ITIL에 대한 충분한 이해를 가진 자가 수행한다. (ITIL 관련 자격 권고)

○ 점검 결과는 대외 감사/진단 시 내부 점검 활동의 결과물로 활용할 수 있다.

○ 표준운영절차 운영시스템을 통한 요청관리 이력관리 여부를 확인하고, ITSM 등 운영시스템이 없는 경우 요청관리대장 등 기록관리 여부를 확인한다.

2) 검증 항목

세부 절차	체크 항목	정성 평가	증적 체크
요청 등록	- 모든 서비스 요청 등록, 처리, 승인, 결과 확인 이력이 표준운영절차 운영시스템 또는 요청관리대장에 등록·관리되고 있습니까?	적합/ 부적합	• ITSM 요청등록 이력 • 요청관리대장
요청 접수 및 분류	- 접수되는 서비스 요청은 적절히 분류되어 담당자에게 할당되고 있습니까?		• 요청분류 이력 • 담당자 배정 이력
요청 처리	- 서비스 요청을 처리하기 위해 장애, 변경관리 등의 타 프로세스 작업이 필요한 경우 해당 프로세스로 적절하게 이관하여 처리하고 있습니까?		• 요청관리 이력 • 장애·변경·백업·구성·배포 등 처리 이력
	- 서비스 요청의 진행사항 및 처리 결과에 대해 요청자에게 적절하게 정보가 제공되고 있습니까?		• 처리결과 안내 이력
요청 확인 및 종료	- 만족도 조사가 필요한 요청 건은 요청 처리 후 만족도 조사를 진행하고 확인이 되고 있습니까?		• 만족도 평가 이력 • 만족도 관리 이력
	- 만족도 조사를 통해 불만족 사항 등이 파악되는 경우, 해결을 위한 활동이 진행되고 있습니까?		• 불만족에 대한 관리 이력

자. 관리 기준 및 예시

1) 서비스 요청 분류 (예시)

(하기 항목은 예시 유형으로 참고용이며, 각 기관별 적용 가능한 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 변경 요청	
	구성정보 추가 요청(신규)	

2) 만족도 기준 (예시)

점수	기준	설문항목(예시)
5점	매우 만족	• 서비스 요청에 전반적으로 만족하십니까? • 서비스 요청에 대한 일정이 잘 준수되었습니까? • 서비스 요청에 대한 처리가 요구사항에 맞게 정확히 처리되었습니까?
4점	만족	
3점	불만	
2점	불만족	
1점	매우 불만족	

3) 요청 관리대장 (예시)

SR관리대장

No.	Request ID	요청자	요청일시	요청내용	고객명	고객 연락처	업무담당자	Call-Back 일시	방문일자	방문자	방문지역	처리내용	처리완료일시
1													
2													
3													
4													
5													
6													
7													
8													

2. 변경관리 절차서

가. 개요

1) 목적

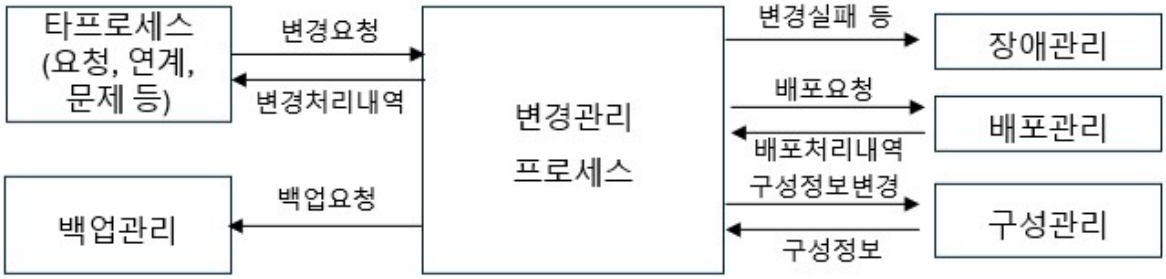
○ 정보시스템 운영 과정에서 발생하는 변경작업에 대하여 변경 절차를 표준화함으로써 서비스 영향과 위험을 최소화하고, 정보시스템 운영의 체계화와 장애발생요소 최소화를 목적으로 한다.

2) 적용 범위

○ 변경관리 절차는 행정·공공기관 정보시스템의 변경관리에 적용한다.

3) 관련 업무 절차

○ 연관 선/후행 업무



○ 시작/종료/증적(Output) 조건

주요 업무	수행 업무
프로세스 시작 조건	- 정보시스템의 도입, 구성, 기능 변경/신규 개발, 타 시스템 연계 등으로 인한 변경 요청(RFC)이 접수된 경우 - 장애관리·문제관리 등 절차에서 조치/해결 활동으로 변경작업이 필요한 경우
프로세스 종료 조건	변경처리 종료 변경요청(RFC)의 반려
증적(Output)	변경작업 관리대장 변경 요청서 변경 계획서 변경 결과 보고서 변경이력 관리대장 ※ 변경관리 절차 및 증적을 ITSM 시스템에 반영하여 관리

나. 관리 정책

1) 정의

○ 정보시스템 변경관리 절차의 운영에 있어서 필히 준수해야 할 정책 기준을 제공

2) 정책 기준

정책	설명	
정책 1	기준	정보시스템에 발생하는 모든 변경은 표준화된 변경관리 절차를 통하여 수행·관리되어야 한다.
	설명	○ 서비스에 영향을 미치는 정보시스템의 추가·수정·제거, 기능 변경, 신규 개발, 패치, 타 시스템 연계 변경 등 모든 변경 요청은 반드시 변경관리 절차를 통해 수행되어야 한다. ○ 변경관리 절차는 변경 접수 및 검토, 계획 수립, 변경작업, 원복 절차를 포함하여 운영하여야 한다. ○ 변경관리 절차는 다양한 변경의 유형을 수용할 수 있어야 한다. ○ 변경관리에는 변경으로 인한 서비스의 영향 검토, 변경작업을 위한 필요 자원 정의 및 변경에 대한 승인 등의 활동이 포함되어야 한다. ○ 변경관리 절차는 일반, 단순, 긴급 변경 절차를 구분한다. ※ 단순, 긴급 변경은 작업 특성을 고려하여 간소화된 작업 절차를 정의할 수 있다. ○ 운영체제, 상용소프트웨어 등의 업데이트 및 패치는 사전 영향도 검토 및 안정성 테스트 후 적용하고, 운영상태를 기록·관리하여야 한다.
정책 2	기준	모든 변경작업의 단계별 상태 및 이력은 정보시스템 등급에 따라 관리시스템 또는 기록관리 방식으로 객관적으로 관리되고 추적되어야 한다.
	설명	○ 변경 요청, 접수, 검토, 승인, 변경작업, 테스트, 결과 확인, 반려 및 종료 이력은 관리시스템을 통해 기록·관리되어야 하며, 변경 정보 및 변경이력을 관리하여야 한다. ○ A1등급은 관리시스템을 다중화하여 구축·운영하여야 한다. ○ 변경작업 이력은 작업 실패 이력을 포함하여 관리하여야 한다.
정책 3	기준	정보시스템 등급에 따라 변경계획의 적합성, 영향도 검토 및 변경작업 완료 후 이행 적정성 점검을 실시한다.
	설명	○ A1등급 정보시스템의 일반 변경은 변경관리위원회 개최, 변경계획 2단계 승인(담당자 검토 후 관리자 승인), 변경작업 이행 후 검토를 수행하여 변경 결과가 초기 목적 및 예상 효과를 달성하였는지 확인하여야 한다. ○ 정보시스템의 일반 변경작업은 업무 시간대(09~18) 작업을 금지하고 일과 후 작업을 수행한다.
정책 4	기준	모든 변경작업은 원상복구계획을 변경 계획에 포함하여 관리하여야 한다.
	설명	○ 변경 계획에는 변경 실패, 작업 지연, 서비스 영향 발생 등에 대비한 원상복구계획을 포함하여야 한다. ○ 원상복구계획은 명령어 수준의 상세 절차를 포함해야 한다. ○ 원상복구계획에 따라 복구를 수행한다. ○ 원상복구 수행 결과 및 변경 실패 이력은 변경 결과에 포함하여 기록·관리하여야 한다. ○ 변경 실패로 장애가 발생한 경우, 작업 결과를 기록하고 장애관리 절차로 이관한다.

다. 용어 정의

용어	설명
변경 요청 (RFC: Request For Change)	○ 서비스 요청의 해결, 서비스 품질 향상 또는 정보시스템의 구성항목 및 응용프로그램 서비스·기능 변경을 제안하는 방법으로, 제안된 변경의 특성이나 세부 사항, 타당성 및 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, 루틴화되어 정형화된 변경으로 담당자가 작업의 진행 여부를 결정하고 결과를 승인자에게 보고하는 변경을 의미한다.
긴급 변경	○ 변경의 목적이 업무 또는 서비스에 미치는 부정적인 영향을 완화하거나 회피하기 위해 가능한 신속하게 이루어져야 하는 변경작업을 의미한다. - 예: 장애 및 중요 이벤트 해결을 위한 긴급 조치로 인한 변경 등
변경관리위원회 (CAB: Change Advisory Board)	○ 파급효과가 높은 변경 요청을 평가하는 책임과 대표성을 가진 인력 그룹(협의체)으로, 구성원은 각 기관에 따라 달라질 수 있다. ○ 위원회는 변경 요청에 대한 진행 여부, 우선순위 등을 권고하며, 변경을 구현하기 위한 자원의 할당 등을 제안한다. ※ 변경관리위원회(CAB)의 소집은 정보시스템 운영환경에 따라 대면, 서면, 영상회의 등으로 개최할 수 있으며, A1등급 정보시스템은 필수 운영한다.
구성 정보	○ 정보시스템을 구성하는 각각의 구성요소를 구성항목이라고 하며, 이에 대한 정보, 관련 상세 내역 및 구성항목 간의 관계성을 담고 있는 데이터베이스를 CMDB라고 한다.
이행 후 검토 (Post Implementation Review)	○ 변경 완료 이후 검토 활동으로, 변경 결과에 대한 검토 및 예상 효과 달성 여부를 검토한다. ○ 변경관리위원회 심의를 거친 A1등급 정보시스템의 일반 변경은 의무적으로 이행 후 검토 과정을 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

○ 변경관리 절차를 수행하는 역할자의 책임은 다음과 같다.

주요 업무		수행 업무	비고
운영기관 (정보시스템의 최종 운영관리를 책임지는 기관)	관리자	○ 정보시스템 관련 담당자의 상위 책임자 또는 부서장 ○ 변경 검토, 처리 및 승인 관련 의사결정 ○ 변경 요청 및 계획의 적합성 판단	
	담당자	○ 변경작업 대상 정보시스템의 담당자가 역할 수행 ○ 변경 수행 관련 이해관계자 간 조율 및 의사소통 창구 - 수탁기관 및 운영사업자 간 유기적 협조 체계 관리 포함 ○ 변경 계획의 적정성 검토 ○ 변경관리위원회(CAB) 소집 및 진행 ○ 변경작업 관련 테스트 결과 및 이행 결과 검토 ○ 변경 구현 이후에 PIR 수행 ○ 변경 수행 관련 이해당사자 간 조율 - 수탁기관 및 운영사업자 간 유기적 협조 체제 관리 ○ 변경작업으로 인해 구성/형상정보가 변경되는 경우 해당 구성/형상정보에 대한 정합성 확인	
수탁기관 또는 운영사업자	운영자	○ 운영기관과의 계약을 통해 정보시스템의 운영·유지 및 변경 작업을 담당하는 수탁기관 또는 운영사업자 ○ 정보시스템 변경 및 유지보수 업무 수행 ○ 변경 수행 관련 이해관계자(운영기관/운영사업자) 간 조율 - 수탁기관 및 운영사업자 간 유기적 협조 체계 관리 포함 ○ 변경 계획의 적정성 검토 ○ 변경 계획 수립과 변경 관련 제반 준비 작업 - 변경작업 일정, 변경 사유, 상세 작업계획, 테스트 계획, 복구 계획, 변경 영향 등의 준비 작업과 계획 수립 활동 ○ 변경작업 수행 및 결과 보고 - 변경계획에 따라 변경작업을 수행하고 작업 이후 테스트 및 서비스 확인 - AP 변경의 경우 개별기관에서 관리하는 AP 변경관리 절차가 있고, 본 표준운영절차에서 요구하는 타스크를 포함하는 경우, 자체 보유한 관리 절차에 따라 관리 가능 ○ 변경작업 이후 구성/형상정보에 대한 현행화 작업	

마. 표준절차 흐름도

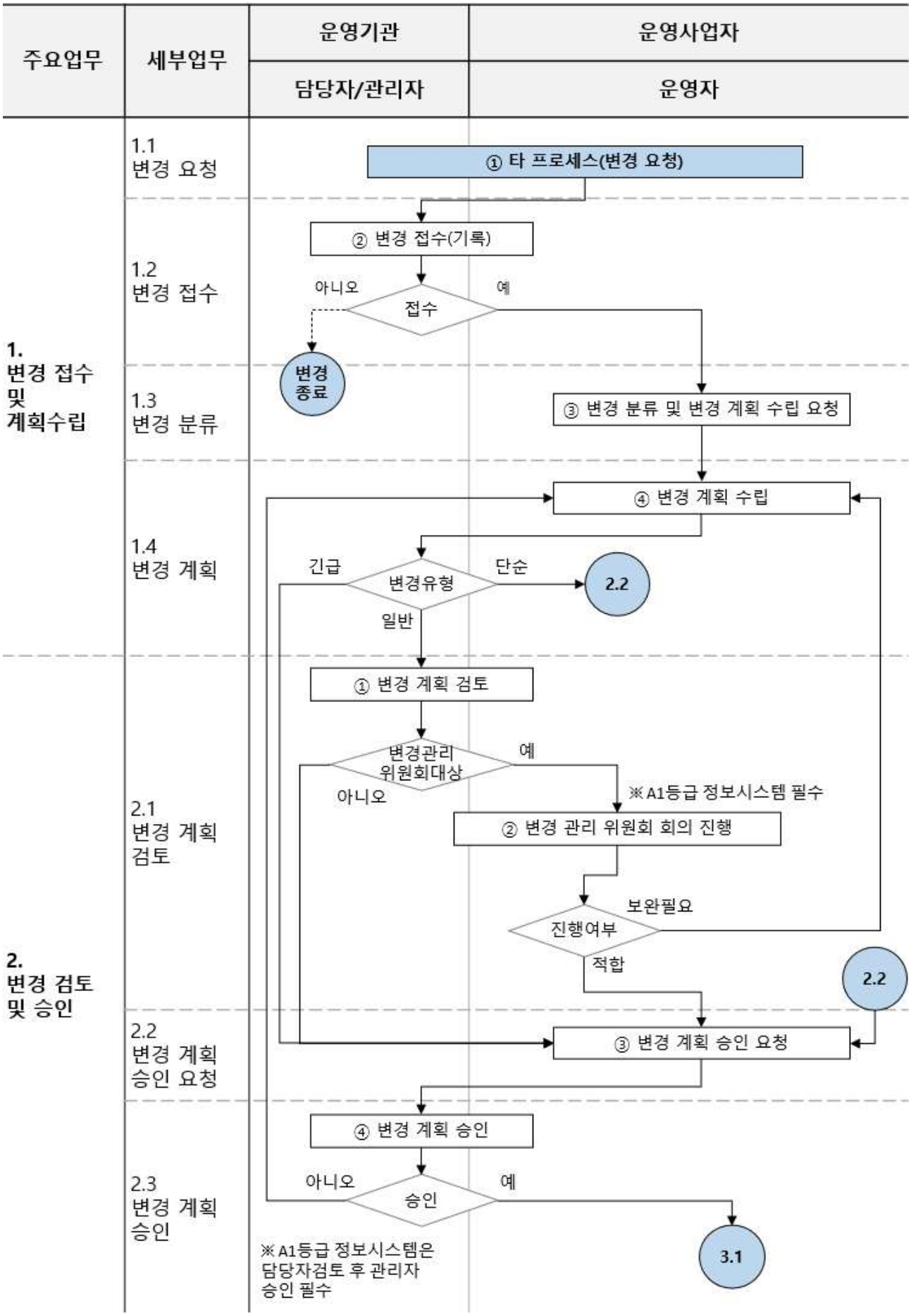
○ 변경관리 절차는 아래와 같은 주요 업무와 수행절차들로 구성된다.

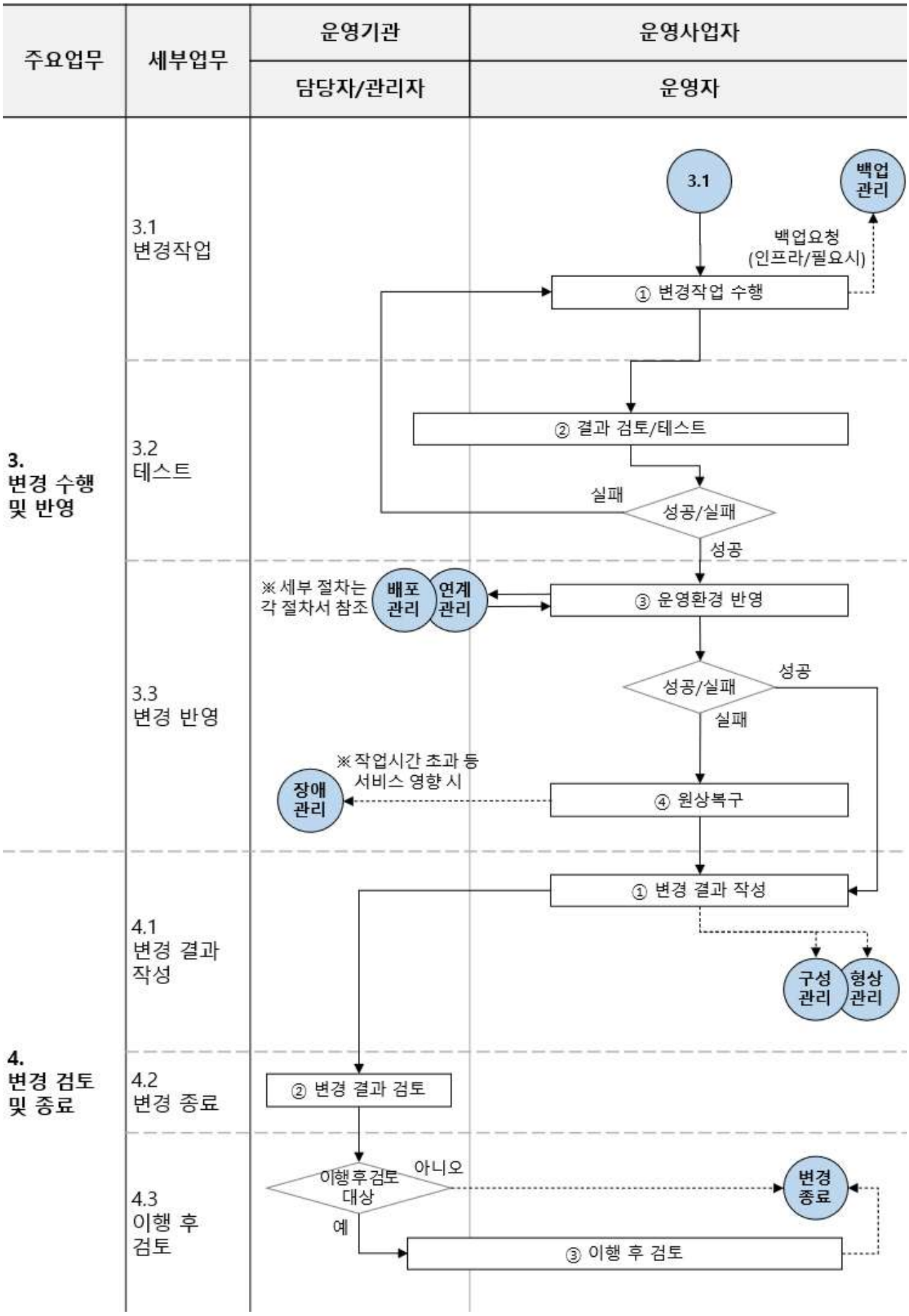
1) 주요 업무

주요 업무	세부 업무	수행 업무
1. 변경 접수 및 계획 수립	1.1 변경 요청	○ 서비스 요청 프로세스나 타 프로세스에서 변경 요청서를 작성하여 변경을 요청한다.
	1.2 변경 접수	○ 운영기관 담당자 또는 운영자는 변경 요청을 접수하고 진행 여부를 판단한다.
	1.3 변경 분류	○ 운영자(변경 담당자)는 변경 요청을 변경 유형 분류 기준에 따라 분류하고, 관련자들과 협의하며 작업계획을 수립할 변경작업자를 지정한다.
	1.4 변경 계획	○ 운영자(변경 담당자)는 변경 계획서(아래 내용 포함)를 작성한다. - 변경 요청 근거 및 내용, 변경작업자, 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 적합성 및 영향도를 검토한다. ○ 정보시스템의 등급이 A1등급일 경우 변경관리위원회(CAB)를 개최하여 변경 계획에 대한 심의 및 변경작업의 진행 여부를 결정한다. ※ 변경관리위원회: A1등급 필수
	2.2 변경 계획 승인 요청	○ 운영자(변경 담당자)는 검토된 변경 계획을 운영기관 담당자에게 승인을 요청한다.
	2.3 변경 계획 승인	○ 변경 승인자는 변경 계획을 검토하고 승인을 진행한다. ※ A1등급 정보시스템의 일반 변경은 2단계 승인(담당자 검토 후 관리자 승인)을 수행한다.
3. 변경 수행 및 테스트	3.1 변경작업	○ 변경작업자는 변경 계획을 토대로 변경작업 사전 준비를 수행한다. - 변경작업 수행 결과와 진행상태를 기록·관리한다.
	3.2 테스트	○ 변경작업 완료 후 실환경 적용 전 변경에 대한 테스트를 진행하고 이상 여부를 확인한다. - 테스트는 개별기관의 운영환경 및 인력 구성에 따라 다르게 적용될 수 있다.
	3.3 변경 반영	○ 운영자(변경 담당자)는 승인된 운영환경 반영 계획에 따라 운영환경에 반영 작업을 진행한다. ○ 반영 작업 실패 시에는 원상복구계획에 따라 원상복구를 진행한다.

4. 변경 검토 및 종료	4.1 변경 결과 작성	○ 운영자(변경 담당자)는 변경에 대한 완료 보고서를 작성하고 운영기관 담당자에게 보고한다. ○ 변경작업 완료 후 운영상태를 확인하고 기록·관리한다. ○ 운영자(변경 담당자)는 구성/형상항목 업데이트를 실시한다.
	4.2 변경 종료	○ 운영기관 담당자는 변경 기록을 확인하여 변경작업 정상 여부를 확인하고, 변경을 종료한다. ○ A1등급 정보시스템의 일반 변경 또는 변경관리위원회 심의를 거친 변경에 대해서는 이행 후 검토(PIR) 단계를 진행한다.
	4.3 이행 후 검토	○ 운영기관은 변경관리위원회 또는 별도 구성한 조직을 통해 변경 작업의 초기 목적을 달성하였는지 여부 및 변경 수행 과정에서 발생했던 기술적인 이슈 사항이나 변경 지연 및 실패 등에 대해 검토를 수행한다.

2) 수행주체별 표준절차 흐름도




주요업무
세부업무
운영기관
담당자/관리자
운영사업자
운영자
3. 변경 수행 및 반영
3.1 변경작업
3.2 테스트
3.3 변경 반영
4. 변경 검토 및 종료
4.1 변경 결과 작성
4.2 변경 종료
4.3 이행 후 검토
3.1
백업 관리
백업요청 (인프라/필요시)
① 변경작업 수행
② 결과 검토/테스트
실패
성공/실패
성공
※ 세부 절차는 각 절차서 참조
배포 관리
연계 관리
③ 운영환경 반영
성공/실패
성공
실패
※ 작업시간 초과 등 서비스 영향 시
장애 관리
④ 원상복구
① 변경 결과 작성
구성 관리
형상 관리
② 변경 결과 검토
이행 후 검토 대상
아니오
예
변경 종료
③ 이행 후 검토

바. 세부 수행 절차

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

(●: 정, ◑: 부)

세부 절차	수행 내용	운영기관	운영사업자
		관리자/담당자	운영자
1.1- ① 변경 요청	- 요청자는 정보시스템의 변경이 필요할 경우(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)	- 운영기관 담당자 또는 수탁기관 운영자는 서비스 요청 및 타 프로세스에서 등록된 변경 요청의 필요성 및 요청 내용이 기준에 적합한지 검토하고 접수 여부를 결정한다. - 접수된 변경 요청은 관리시스템에 등록한다. - 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	- 운영자(변경 담당자)는 변경 대상 및 변경 처리 유형에 따라 변경을 분류(긴급, 일반, 단순)한다. - 운영자는 요청자, 운영기관 담당자, 작업자, 유지보수 업체 등 관련자들과 협의하고, 작업계획을 수립할 변경작업자를 지정한다. - 운영자는 지정된 변경작업자에게 변경작업 계획 수립을 요청한다.		●
1.4- ④ 변경 계획 수립	- 변경작업자는 변경 요청을 근거로 관련 담당자와 일정, 작업 내용 등 전반적인 변경작업에 대하여 협의를 진행하고, 변경으로 인한 영향 등을 고려하여 변경 계획서를 작성한다. - 변경 계획서는 아래와 같은 내용을 포함한다. ※ 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 단순 변경의 경우 일상적이고 반복된 변경으로, 사전 정의된 변경작업 계획에 의거하여 변경 승인 및 작업 절차를 간소화하여 진행할 수 있다. 긴급히 수행할 보안 패치로 인한 긴급 변경의 경우 제조사 영향 검토로 변경 영향 검토를 대체하거나, 타 모듈, 타 시스템, 타 기관 등 간접 영향을 제외하고 직접 영향받는 대상으로 영향 검토를 간소화할 수 있다.		●

(●: 정, ◑: 부)

세부 절차	수행 내용	운영기관	운영사업자
		관리자/담당자	운영자
2.1- ① 변경 계획 검토	- 운영기관 담당자는 수립된 변경 계획을 검토한다. - 긴급 변경일 경우는 변경 계획을 확인하고 검토 단계를 생략할 수 있다. - 운영기관 담당자는 변경관리위원회(CAB) 대상 여부를 파악하고 대상인 경우 변경관리위원회를 소집한다. ※ A1등급 정보시스템 일반 변경 시 변경관리위원회 필수 단순, 긴급 변경일 경우 생략 가능 - 변경관리위원회(CAB)의 주관 및 참석 대상 등 개최 기준은 "변경관리위원회 기준"을 참조한다.	●	◑
2.1- ② 변경관리 위원회 회의 진행	- 변경관리위원회(CAB)는 변경 요구사항(변경 수준, 범위, 분류), 기술 검토 결과 및 영향도를 검토하여 심의한다. - 변경 심의 내용은 회의록 등을 통해 이력으로 관리되어야 한다. - 위원회의 심의 결과가 변경에 적합하지 않은 경우, 운영자를 통해 변경 계획을 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	- 운영자(변경 담당자)는 검토된 변경 계획을 운영기관 담당자에게 승인 요청한다. - 승인 단계 및 승인자는 정보시스템 등급, 변경 유형 및 각 기관 운영기준에 따라 사전에 정의한다.		●
2.3- ④ 변경 계획 승인	- 변경 승인자는 변경 계획을 검토하여 변경작업에 대해 승인 여부를 결정한다. - 변경계획서의 작성 오류 또는 미흡한 사항으로 승인이 불가할 경우 해당 계획서를 운영자(변경 담당자)에게 반려하여 수정·보완하도록 한다. - A1등급 정보시스템 일반 변경은 2단계 승인(담당자 검토 후 관리자 승인)을 필수로 진행한다. ※ 단순 변경, 긴급 변경은 관리자 승인을 제외할 수 있다.	●	◑

(●: 정, ◑: 부)

세부 절차	수행 내용	운영기관 관리자/담당자	운영사업자 운영자
3.1- ① 변경작업 수행	- 변경작업자는 변경 계획에 따라 변경작업 사전 준비를 수행한다. ※ 변경작업 수행의 시작과 종료는 관련된 이해관계자에게 전파·공유하여야 하며, 변경작업 수행 결과와 진행 상태를 기록·관리한다.		●
3.2- ② 결과 테스트	- 변경작업자는 변경작업 후 테스트를 통해 정상 여부를 확인한다. - 테스트 실패 시 원인을 파악하고, 원인이 불명확한 경우 문제관리로 이관하고 재작업이 필요할 경우 재작업을 실시한다.		●
3.3- ③ 운영환경 반영	- 운영자(변경 담당자)는 승인된 운영환경 반영계획에 따라 변경사항을 운영환경에 반영한다.	◑	●
3.3- ④ 원상복구	- 원상복구가 필요할 경우는 원상복구계획에 의거하여 원상복구를 실시한다. - 변경 작업 중 변경 실패나 작업 시간 초과 등으로 서비스에 영향 발생 시 장애관리로 이관하여 처리한다.	◑	●

(●: 정, ◑: 부)

세부 절차	수행 내용	운영기관	운영사업자
		관리자/담당자	운영자
4.1- ① 변경 결과 작성	- 운영자(변경 담당자)는 변경작업 완료 후 서비스 정상 여부, 운영상태 및 오류 발생 여부를 확인하고, 특이사항 또는 이슈 사항을 변경 결과에 포함하여 기록·관리한다. - 운영자(변경 담당자)는 변경에 대한 완료 보고서를 작성하고 운영기관 담당자에게 보고한다. - 운영자(변경 담당자)는 구성/형상정보에 반영이 필요할 경우 구성/형상항목에 대한 업데이트를 실시한다. ※ CMDB를 관리하는 기관에 해당		●
4.2- ② 변경 결과 검토	- 운영기관 담당자는 변경 기록을 확인하여 변경작업 정상 여부를 확인하고, 변경을 종료한다. - 변경관리위원회(CAB) 심의를 거친 변경에 대해서는 운영기관이 변경관리위원회 또는 별도로 구성한 조직을 통해 이행 후 검토(PIR) 활동을 수행한다. ※ A1등급 정보시스템 일반 변경은 이행 후 검토 필수	●	◑
4.3- ③ 이행 후 검토	- 운영기관은 변경관리위원회 또는 별도로 구성한 조직을 통해 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 및 분석을 통한 개선 활동 필요 여부 · 변경 이후 일정 시간 경과 후 변경에 따른 영향, 오류 발생 등 상태 점검	●	●

2) 고려사항

○ N/A

사. 핵심성과지표 (KPI : Key Performance Indicator)

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

측정 지표	측정 방법(예시)	측정 목적	측정 주기
변경 절차 준수율	((당월 종료된 변경작업 건수 – 변경절차 미준수 건수) / 당월 종료된 변경작업 건수) X 100	변경관리 절차 준수 여부 관리	당월
변경 작업 성공률	(변경작업 성공 건수 / 당월 종료된 변경작업 건수) X 100	변경작업 정상 완료 여부 관리	당월

아. 수행 검증

1) 검증 방법

○ 검증 체크리스트의 체크 항목 기준(ITIL 표준 준용)으로 표준운영절차의 준수 여부와 이행 점검을 수행한다.

○ 개별기관 내 자체 프로세스 검증자는 내부 감사자의 자격 또는 ITIL에 대한 충분한 이해를 가진 자가 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 계획 수립	- 변경 요청은 서비스 요청 등의 타 프로세스로부터 정상적으로 요청·등록되고 있습니까?	적합/ 부적합	• 변경 요청 이력 - ITSM 내 변경 요청 이력 또는 수기 변경이력 관리대장
	- 변경 요청의 유형(일반/긴급/단순)은 사전 정의되어 있으며, 해당 절차를 구분하고 있습니까?		• 변경유형 기준 • 유형별 처리 절차
	- 변경 계획에는 변경작업의 적합성을 검토하고 수행하기 위한 충분한 내용을 포함하고 있습니까? * 변경 요청 근거, 변경 사유, 변경 대상, 변경 영향, 작업계획 등		• 변경계획서 - ITSM 내 변경 계획 이력 또는 수기 변경계획서
	- 변경 계획에는 작업 실패에 대비한 원복계획 또는 절차를 수립하여 포함하고 있습니까?		• 원복계획서 - 변경계획서 내 포함 가능
	- 원복계획서에 명령어 수준의 상세한 원복 절차가 작성되어 있습니까?		• 원복계획서 - 변경계획서 내 포함 가능
변경 검토 및 승인	- A1등급 정보시스템의 일반 변경은 변경 수행 전 변경관리위원회(CAB)를 통한 변경 심의를 수행하고 있습니까?		• 변경 심의 수행 이력 - 회의록 또는 ITSM 내 변경작업 이력
	- A1등급 정보시스템의 일반 변경은 변경작업에 대해 2단계 승인(담당자 검토 > 관리자 승인) 단계를 수행하고 있습니까? - 정보시스템의 변경작업은 검토, 승인 단계를 수행하고 있습니까?		• 변경작업 승인 이력 - 승인 이력 또는 ITSM 내 검토·승인 이력
변경 수행 및 반영	- 변경작업 후 실환경 적용 전에 충분한 테스트가 진행되고 있습니까? * 개발계/검증계 테스트, 테스트케이스 활용 여부 등		• 테스트케이스 및 테스트 결과
	- 테스트 시 발견된 결함은 등록되고 있으며, 이에 대한 처리 이력이 관리되고 있습니까?		• 결함 관리 이력
	- 변경작업 완료 후 서비스 정상 여부 및 운영상태를 확인하고, 관련 이력을 기록·관리하고 있습니까?		• 변경결과서 • 운영상태 기록·관리 이력
변경 검토 및 종료	- A1등급 정보시스템의 일반 변경 또는 변경관리위원회(CAB) 심의를 거친 변경에 대해, 이행 후 검토(PIR)과 같은 검토 활동이 수행되고 관련 이력이 관리되고 있습니까?		• 변경 결과서 또는 PIR 활동 이력
	- 변경작업으로 구성정보 또는 형상정보가 변경된 경우 CMDB의 업데이트가 진행되고 있습니까?		• CMDB 업데이트 이력 - ITSM 이력 또는 CMDB 관리대장

자. 관리 기준 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 준수해야 하는 변경 • 일반 변경 예 - HW(서버, 스토리지, 네트워크, 보안 등) OS, 펌웨어, 보안패치 등 업데이트 - 응용프로그램 기능 변경, 신규 개발, 프로그램 수정 및 배포, 타 시스템 연계 변경 등
단순 변경	• 정기적으로 반복되어 수행되거나, 수행 경험으로 변경작업의 내용이 검증된 경우, 간소화된 절차를 적용해 효과적인 작업을 수행하는 사전에 정의된 변경으로, 위험성 및 업무서비스 영향도가 매우 낮은 변경 • 단순 변경 예(기관별 사전 정의에 따라 변경 가능) - 사용자 계정관리, 구성/형상정보 오류수정, 방화벽 정책 변경, 기타 파급 영향도가 낮은 루틴화된 작업으로 사전에 절차서에 단순변경으로 정의된 변경
긴급 변경	• 중대한 장애 혹은 문제로 인해 업무에 영향을 받는 경우, 또는 운영기관의 요구에 긴급하게 대응하여 처리되는 변경 • 긴급 변경 예 - 정보시스템의 중대한 오류 등으로 서비스의 중단을 초래하거나, 다수의 사용자에게 심각한 영향을 미치는 장애에 대해서 빠른 작업처리를 위한 변경

2) 변경관리위원회(CAB) 기준

가. 변경관리위원회는 접수된 변경 요청에 대해 다양한 검토를 실시하여 그 수행 여부에 대해 승인하고, 변경의 영향, 위험성, 우선순위의 평가 등을 통해 효율적이고 안정적인 변경관리가 되도록 하는 역할을 담당한다.

나. 변경관리위원회에 참여하여야 하는 구성원은 변경 요청을 평가하는 책임과 대표성을 가진 인력을 포함하며, 역할상 필요한 모든 이해관계자가 포함될 수 있도록 운영기관에 따라 사전에 정의가 필요하다.

다. 변경관리위원회 심의 대상의 중요성에 따라 중점 심의, 간소화 심의로 구분하여 심의할 수 있으며, 개최 기준에 해당하지 않는 변경작업에 대해서도 운영기관 담당자가 판단하여 변경관리위원회 안건으로 상정할 수 있다.

라. 가이드 구성안

<table>
<tr><th colspan="3" rowspan="2">구분</th><th colspan="3">변경관리위원회 구성(A1등급 정보시스템 필수)</th></tr>
<tr><th>위원장</th><th>필수</th><th>선택</th></tr>
<tr><td rowspan="3">단일</td><td rowspan="2">AP</td><td>단위
서비스</td><td>운영기관
관리자
(부서장)</td><td>운영기관
- 요청 업무 팀장
- 요청 업무 담당자
운영사업자
- 요청 업무 팀장
- 요청 업무 담당자</td><td>- 요청자</td></tr>
<tr><td>연계
서비스</td><td>운영기관
관리자
(부서장 이상)</td><td>운영기관
- 요청 업무 팀장 이상
- 요청 업무 담당자
운영사업자
- 요청 업무 팀장 이상
- 요청 업무 담당자</td><td>- 요청자
- 유관기관 팀장 이상</td></tr>
<tr><td colspan="2">인프라</td><td>운영기관
관리자
(부서장 이상)</td><td>운영기관
- 요청 업무 팀장 이상
- 요청 업무 담당자
운영사업자
- 요청 업무 팀장 이상
- 요청 업무 담당자</td><td>- 요청자
- 유관기관 팀장 이상</td></tr>
<tr><td>복합</td><td colspan="2">AP + 인프라</td><td>운영기관
관리자
(부서장 이상)</td><td>운영기관
- 요청 업무 팀장 이상
- 요청 업무 담당자
운영사업자
- 요청 업무 팀장 이상
- 요청 업무 담당자</td><td>- 요청자
- 유관기관 팀장 이상</td></tr>
</table>

3) 서식 예시 (수기 사용 시 참조용)

가. 변경계획서

변경작업 계획서 (예시)

***변경제목**				
***변경접수번호**			***접수일자**	
변경 요청자			**변경완료 희망일시**	
***위험수준(등급)**			***변경 승인 일자**	
***변경 담당자**			**CAB 수행 여부**	**Yes, No**
***대상 시스템**			**주 작업자**	
***작업계획**	**시작시간**		***영향받는서비스**	대분류 > 중분류 (N/A -> **서비스 영향 없음**)
	완료시간		**서비스 예상 중단시간**	0분 (MM.DD hh:mm ~ MM.DD hh:mm)
***변경 목적**				
***작업 계획**				
***테스트계획**				
***복구계획**				
***CAB 검토 의견**	(공란 시: **CAB 미 수행**) PIR 활동			
첨부 문서				

주) * : 필수 작성 필드

나. 변경결과서

변경작업 결과 보고서 (예시)

*변경제목				
*변경접수번호			접수일자	
변경 요청자			*수행결과	반영완료( ), 취소( ), 실패( )
*변경 담당자			주 작업자	
*대상 시스템			서비스 중단시간	0분
*작업계획	시작시간	MM.DD hh:mm	*실제 시작시간	
	완료시간		*실제 완료시간	
*변경 목적				
*변경 계획				
* 테스트 결과				
*작업 내역				
변경결과 검토				
첨부 문서				

주) * : 필수 작성 필드

다. 변경이력 관리대장

변경작업 관리대장 (예시)

변경ID	변경유형#1	변경유형#2	변경업무시스템	제목	현재단계(상태)	요청자	요청부서	요청일시	합의완료일	업무담당자	처리자	변경계획 승인 일자	변경작업 시작 일자	변경작업 종료 일자	처리내용	비고

3. 장애관리 절차서

가. 개요

1) 목적

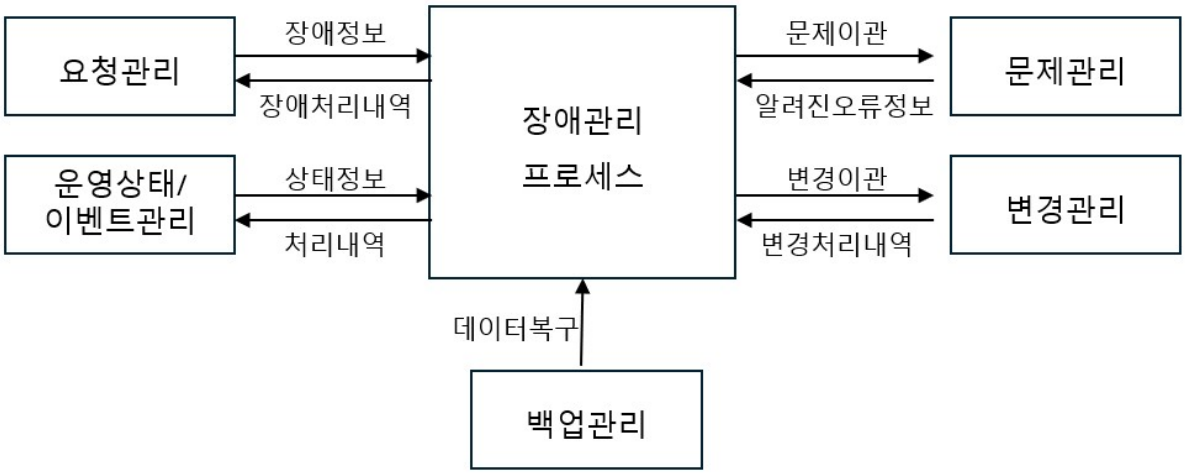
○ 정보시스템 운영 중 장애가 발생한 경우 장애상황을 신속하게 식별·전파하고, 원인 분석 및 조치를 통해 서비스를 조속히 복구하며, 재발방지대책을 수립·이행함으로써 정보시스템 서비스의 안정성과 연속성을 확보하는 것을 목적으로 한다.

2) 적용 범위

○ 장애관리 절차는 행정·공공기관 정보시스템에서 발생하는 장애의 대응·복구 및 사후관리에 적용한다.

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 시스템 내 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 보고 방법/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, 근본 원인 분석을 위한 문제관리 이관 및 후속 조치 등 정상 서비스 복구 후 순차적으로 처리 수행
정책 3	기준	발생된 모든 장애는 표준운영절차 운영시스템 또는 장애관리대장을 통해 객관적으로 기록·관리되고 처리 이력이 추적되어야 한다.
	설명	○ 정보시스템에서 발생한 장애는 표준운영절차 운영시스템을 통해 장애 접수, 장애등급 산정, 조치, 복구 확인, 보고 및 종료 이력을 관리하여야 한다. ○ ITSM 등 운영시스템이 없는 경우 장애관리대장 등 문서 형태로 관리할 수 있다. ○ 장애의 처리과정, 조치내용, 처리결과 및 재발방지대책은 누락 없이 기록하여야 하며, 기록된 장애 이력은 유사 장애 조치 및 예방활동에 활용할 수 있다.

정책	설명	
정책 4	기준	정보시스템 장애 발생 시 정보시스템 등급과 장애 정도 등을 고려하여 장애등급을 1등급부터 4등급까지 산정하고, 정보시스템에서 발생한 장애상황은 정보시스템 등급 및 장애상황 관리체계에 따라 신속하게 보고·전파하여야 한다.
	설명	○ 장애 발생 시 정보시스템 등급, 장애 정도, 발생시간, 대상지역 등을 고려하여 장애등급을 산정하여야 한다. ○ 기반시설·공통장비 장애 등 동일 원인으로 복수의 정보시스템이 영향을 받는 경우에는 해당 정보시스템 중 가장 높은 정보시스템 등급을 기준으로 장애등급을 산정하여야 한다. ○ 정보시스템에서 장애상황이 발생한 경우, 정보시스템 등급 및 장애상황 관리체계에 따라 행정안전부 디지털안전상황실장에게 즉시 통보하여야 한다. ○ 장애가 장기화되는 경우 1등급 장애는 매 2시간 경과 시마다, 2등급 장애는 매 4시간 경과 시마다 경과 시점으로부터 1시간 이내에 장애 조치 진행 상황을 통보하여야 한다.
정책 5	기준	1등급 또는 2등급 장애는 장애사후관리를 실시하고, 장애사후관리 결과 및 조치계획을 기록·관리하여야 한다.
	설명	○ 정보시스템 장애사후관리를 실시하여야 하며, 장애 사후관리 점검항목에 따라 장애 원인, 조치내용, 영향범위, 재발방지대책 등을 점검하여야 한다. ○ 장애사후관리 결과는 정보시스템 복구일로부터 1개월 이내에 정보자원관리 시스템(IRM)을 통해 행정안전부장관에게 제출하여야 한다. ○ 장애사후관리 결과 검토에 따라 조치계획 및 조치 결과 확인이 필요한 경우 관련 자료를 제출하고, 필요한 개선조치를 이행하여야 한다. ○ 장애사후관리 결과는 문제관리, 변경관리, 예방점검, 장애대응훈련 등 후속 개선활동과 연계하여 관리하여야 한다.

다. 용어 정의

용어	설명
장애 (Incident)	○ 정보시스템 사용자 관점에서 서비스 이용이 불가능하거나, 불편이 발생하여 정보시스템에서 제공하는 서비스의 정상적인 활용이 어려운 상태를 말한다.
이벤트 (Event)	○ 정보시스템의 운영 중 식별 가능하거나 감지할 수 있는 것으로 IT 인프라 관리나 IT 서비스 제공에 있어서 중요한 영향을 미치는 모든 상태(파일 시스템의 용량 초과, CPU 사용률의 임계치 초과 상태, 서비스 프로세스의 다운, 메모리 사용률의 임계치 초과 상태 등)
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)
장애등급	○ 장애 발생 시 정보시스템 등급, 장애 정도, 장애 발생시간, 대상지역 등을 고려하여 정한 등급을 말한다.
장애 발생일시	○ 정보시스템 로그에서 식별된 시점, 모니터링 자동화 도구로 장애가 감지된 시점, 장애신고 접수 또는 장애상황 최초 인지 시점 중 가장 빠른 시점
장애 종료일시	○ 장애 복구 후 정보시스템 서비스가 정상 가동됨을 확인한 시간
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	○ 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 내부 검증자 역할로 각 프로세스별 정의된 검증 기준에 따라 정기적(반기 또는 연간)으로 프로세스 감사 활동을 수행

라. 역할 및 책임

○ 장애관리 절차를 수행하는 역할자의 책임은 다음과 같다.

주요 업무		수행 업무	비고
운영기관 (정보시스템의 최종운영관리를 책임지는 기관)	관리자	○ 정보시스템 관련 담당자의 상위 책임자 또는 부서장 ○ 장애 처리 관련 의사결정 ○ 장애보고서, 장애등급 산정 결과 및 장애상황 보고 적정성 검토	
	담당자	○ 장애조치 대상 정보시스템의 담당자가 역할 수행 ○ 장애상황 확인, 장애등급 산정 지원 및 장애상황 보고·전파 ○ 실 장애처리자 또는 유지보수 조직의 장애조치 활동 통제 - 장애원인분석 및 조치 참여 ○ 장애보고서 작성/검토(기록관리) ○ 장애 조치 건의 문제관리 절차 이관 여부 결정 - 장애 근본원인 미도출 또는 근본원인이 도출되었으나 바로 적용이 어려운 경우 등에 대한 후속관리	
수탁기관 또는 운영사업자	운영자	○ 운영기관과의 계약을 통해 정보시스템의 운영과 장애조치를 담당하는 수탁기관 또는 운영사업자 ○ 정보시스템을 구성하는 하드웨어, 소프트웨어, 미들웨어 등의 제조사 또는 유지보수를 담당하는 사업자 ○ 실 장애처리자 또는 유지보수조직의 장애조치 활동 통제 ○ 장애 분석을 통한 진단과 해결책 도출 및 조치 활동 - 장애 조치를 위한 변경관리 절차 연계 활동 ○ 담당부서 및 연계기관 협조 요청 및 서비스 정상 확인 ○ 장애상황 및 조치상황 보고 ○ 조치/종료 내역 기반 장애보고서 작성	

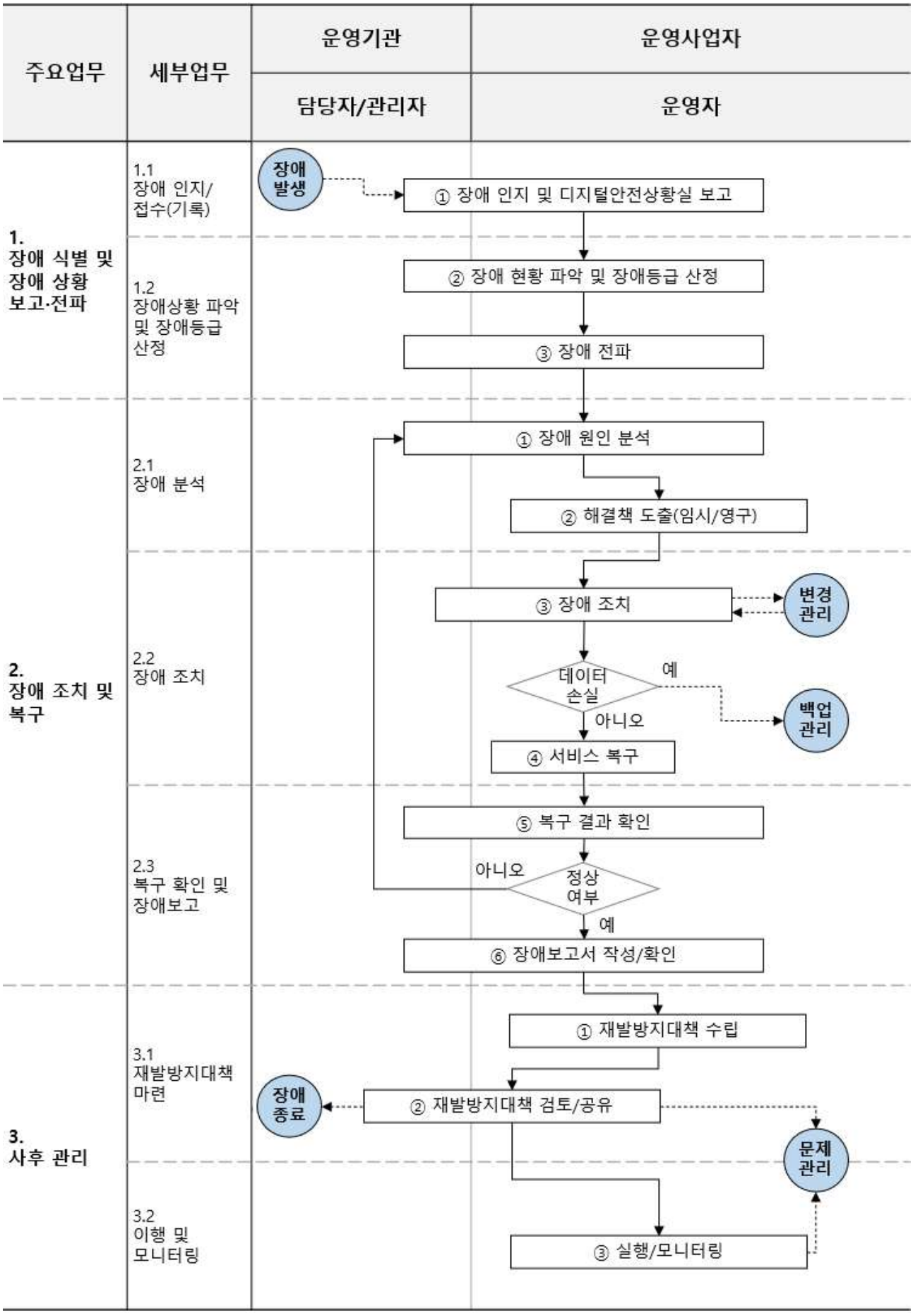
마. 표준절차 흐름도

○ 장애관리 절차는 아래와 같은 주요 업무와 수행절차들로 구성된다.

1) 주요 업무

주요 업무	세부 업무	수행 업무
1. 장애 식별 및 장애상황 보고·전파	1.1 장애 식별	○ 사용자 장애신고, 모니터링, 운영상태 점검 등을 통해 장애 발생 여부를 식별한다. ○ 장애 발생일시, 대상 정보시스템, 관련 서비스, 장애증상, 영향범위 등 장애상황 기본정보를 파악한다. ○ 장애 여부는 장애 판단기준에 따라 확인한다.
	1.2 장애등급 산정 및 장애 상황 보고·전파	○ 정보시스템 등급, 장애 정도, 발생시간, 대상지역 등을 고려하여 장애 등급을 산정한다. ○ 정보시스템에서 장애상황이 발생한 경우 정보시스템 등급 및 주요 정보시스템 장애상황 관리체계에 따라 디지털안전상황실장에게 즉시 통보한다. ○ 장애상황은 최초보고, 경과보고, 종료보고 기준에 따라 보고한다.
2. 장애 조치 및 복구	2.1 장애 분석	○ 장애 현상, 장애증상, 장애 원인 유형, 관련 로그, 구성정보, 변경이력 등을 분석하여 장애 원인과 해결방안을 도출한다.
	2.2 장애 조치	○ 도출된 해결책을 기반으로 장애 조치 수행 - 정보시스템 변경이 필요한 경우 변경관리 절차로 연계 - 데이터 복구가 필요한 경우 백업관리 절차로 연계
	2.3 복구 확인 및 장애보고	○ 장애 조치 후 서비스 정상 여부를 확인하고 장애상황 종료를 보고한다. ○ 장애시간, 장애원인, 피해내용, 조치 결과, 장애등급 등을 포함하여 장애 보고서를 작성한다.
3. 사후 관리	3.1 재발방지대책 마련	○ 장애 원인, 조치내용, 영향범위 및 재발방지대책을 마련한다. ○ 1~2등급 장애는 장애사후관리 점검항목에 따라 장애사후관리를 실시한다. ○ 근본원인 분석 또는 지속 관리가 필요한 경우 문제관리 절차로 이관한다.
	3.2 실행 및 모니터링	○ 재발방지대책의 이행 여부를 모니터링한다. ○ 필요 시 문제관리, 변경관리, 예방점검, 장애대응훈련 등 후속 개선 활동과 연계하여 관리한다.

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	운영사업자
		관리자/담당자	운영자
1.1- ① 장애 인지/접수(기록)	- 사용자의 장애신고, 모니터링 시스템, 운영상태 점검 등을 통해 장애 발생상황을 인지한다. - 인지된 장애는 장애 발생일시, 대상 정보시스템, 관련 서비스, 장애증상, 인지경로 등 기본정보를 포함하여 표준운영절차 운영시스템에 등록한다. - 정보시스템에서 발생한 장애는 표준운영절차 운영시스템을 통해 장애 접수부터 종료까지의 처리 이력을 관리하여야 한다. - ITSM 등 운영시스템이 없는 경우 장애관리대장 등 문서 형태로 기록·관리할 수 있다. - Output: 장애기록	◑	●
1.1- ② 장애상황 파악 및 장애등급 산정	- 운영자는 발생 장애에 대한 대상 정보시스템, 정보시스템 등급, 관련 서비스, 장애 발생일시, 인지일시, 장애증상, 영향범위, 대상지역 등 장애상황 정보를 파악한다. - 운영기관 담당자는 파악된 장애상황 정보를 확인하고, 정보시스템 등급과 장애 정도 등을 고려하여 장애등급 산정이 필요한 정보를 검토한다. - 기반시설·공통장비 장애 등 동일 원인으로 복수의 정보시스템이 영향을 받는 경우에는 해당 정보시스템 중 가장 높은 정보시스템 등급을 기준으로 장애등급을 산정한다.	●	●
1.2- ③ 장애상황 보고·전파	- 운영기관 담당자는 파악된 장애상황 정보를 장애상황 보고체계에 따라 보고·전파한다. - 정보시스템에서 장애상황이 발생한 경우 정보시스템 등급 및「주요 정보시스템 장애상황 관리체계」에 따라 행정안전부 디지털안전상황실장에게 즉시 통보한다. - 장애가 장기화되는 경우 1등급 장애는 매 2시간 경과 시마다, 2등급 장애는 매 4시간 경과 시마다 경과 시점으로부터 1시간 이내에 조치 진행상황을 통보한다. - 장애상황 전파는 장애 발생 시점, 조치 진행 시점, 복구 완료 시점 등 보고 기준에 따라 수행한다. - Output: 장애 전파 이력	●	●

세부 절차	수행 내용	운영기관	운영사업자
		관리자/담당자	운영자
2.1- ① 장애 원인 분석	- 운영자는 장애 조치를 위한 담당자를 지정한다. - 장애조치 담당자는 발생된 장애 현상을 분석하여 발생 원인을 도출한다. ※ ITSM 시스템을 보유한 경우 원인 분석 시 기존 장애이력 또는 알려진 오류 등이 기록된 KEDB(Known Error DB)를 활용한다. 클라우드 운영사업자는 자체 운영 중인 KEDB (Known Error DB)를 활용하여 원인 분석을 수행한다.		●
2.1- ② 해결책 도출	- 장애 원인 분석을 통해 장애 조치를 위한 해결책을 도출한다. - 근본 원인 조치를 위한 영구 해결책 도출을 목표로 수행하나, 서비스의 빠른 복구를 위한 임시 해결책이 먼저 도출되는 경우 해당 해결책 적용을 검토한다. ※ 영구 해결책이 바로 도출되지 않는 경우 문제관리 프로세스와 연계하여 관련 작업을 수행할 수 있다. - 해결책 적용 시 서비스 영향, 변경 필요 여부, 데이터 복구 필요 여부 및 관계기관 영향 여부를 함께 검토한다.	◑	●
2.2- ③ 장애 조치	- 장애 조치는 서비스의 빠른 복구를 목표로 활동해야 하며, 도출된 해결책 중 바로 적용이 가능한 해결책을 적용한다. - 장애 조치를 위해 정보시스템의 변경 작업이 필요한 경우 변경관리 절차와 연계하여 변경 작업을 수행한다. ※ 변경관리 표준운영절차 참조 - 장애가 발생한 시스템의 데이터가 손실된 경우에는 백업 관리 절차와 연계하여 백업된 데이터의 복구작업을 수행한다. - 장애조치를 위하여 필요한 대응조직은 사전에 정의·구성되어야 한다. (붙임4 참조)	◑	●
2.2- ④ 서비스 복구	- 장애 조치 활동을 수행하여 장애가 발생한 서비스를 정상 운영상태로 복구한다. - 장애 종료일시는 장애 복구 후 정보시스템 서비스가 정상 가동됨을 확인한 시점으로 기록한다.		●
2.3- ⑤ 복구 결과 확인	- 서비스가 복구되면 운영자 및 운영기관 담당자는 서비스 정상 여부를 확인한다. ※ 장애조치 미해결 시 장애 원인 분석 단계의 활동을 재수행한다. - 복구 결과 확인 시 주요 기능 정상 여부, 서비스 지연 여부, 데이터 정합성, 연계서비스 정상 여부 및 이용자 불편 해소 여부를 확인한다. - 장애 조치로 서비스의 정상 여부를 확인한 경우, 서비스가 복구되었음을 이해관계자에게 전파한다.	●	◑

세부 절차	수행 내용	운영기관 관리자/담당자	운영사업자 운영자
2.3- ⑥ 장애보고서 작성/확인 및 종료 보고	- 운영자는 장애시간, 피해내용, 장애원인, 조치내용, 조치결과, 장애등급, 재발방지대책 및 문제관리 이관 여부 등을 포함하여 장애보고서를 작성하고 운영기관에 제출한다. - 정보시스템 장애상황의 경우 장애상황 종료 시 「주요 정보시스템 장애상황 관리체계」에 따라 종료보고를 수행한다. - 종료보고에는 대상시스템명, 기관명, 장애시간, 서버 위치, 피해내용, 장애원인, 조치결과, 대국민 안내, 언론대응 방향 및 장애등급을 포함한다. - 운영기관 담당자는 장애보고서의 내용, 장애등급 산정, 조치내역, 복구 결과 및 문제관리 이관 여부의 적정성을 검토한다. - Output: 장애보고서, 종료보고 이력	◑	●
3.1- ① 재발방지 대책 수립	- 운영자는 장애원인 및 처리내역을 기반으로 재발 방지를 위한 대책과 이행방안을 수립한다. ※ 재발방지대책의 수립 활동은 개별기관별 상황에 따라 장애보고서 작성 단계의 활동과 병행할 수 있다. - 1등급 또는 2등급 장애는 정보시스템 장애사후관리 점검항목에 따라 장애사후관리를 실시한다. ※ 클라우드 운영사업자는 동일한 서비스를 이용 중인 사용자에게 장애 및 조치 내역을 전파하여 장애 예방 활동을 지원한다.		●
3.1- ② 재발방지 대책 검토/공유	- 운영기관 담당자 또는 장애협의체는 수립된 재발방지대책과 조치계획의 적정성을 검토한다. - 1등급 또는 2등급 장애의 장애사후관리 결과는 정보시스템 복구일로부터 1개월 이내에 정보자원관리시스템(IRM)을 통해 제출하여야 한다.	◑	●
3.2- ③ 실행/모니터링	- 운영자는 재발방지대책의 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 절차와 연계하여 실행할 수 있다.	◑	●

사. 핵심성과지표 (KPI : Key Performance Indicator)

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

측정 지표	측정 방법(예시)	측정 목적	측정 주기
장애 적기 처리율	(목표 시간 내 처리된 장애 건수 / 당월 종료된 장애 건수) X 100	장애조치의 적기 여부 관리(상호 합의된 장애처리시간 준수)	당월

아. 수행 검증

1) 검증 방법

○ 검증 체크리스트의 체크 항목 기준(ITIL 표준 준용)으로 표준운영절차의 준수 여부와 이행 점검을 수행한다.

○ 개별기관 내 자체 프로세스 검증자는 내부 감사자의 자격 또는 ITIL에 대한 충분한 이해를 가진 자가 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 장애가 표준운영절차 운영시스템 또는 장애관리대장에 등록·관리되고 있습니까?	적합/부적합	• ITSM 장애기록 또는 장애관리대장
	- 장애 발생일시, 대상 정보시스템, 정보시스템 등급, 장애 증상, 영향범위 및 장애등급 산정 정보가 기록되고 있습니까?		• 장애기록 • 장애등급 산정 이력
	- 정보시스템 장애상황을 주요 정보시스템 장애상황 관리체계에 따라 보고하고 있습니까?		• 최초 상황보고 이력 • 장애상황 보고 이력
	- 장기화된 1등급 또는 2등급 장애에 대해 경과보고를 수행하고 있습니까?		• 경과보고 이력
장애 조치	- 장애 처리를 위해 장애이력, 구성정보, 형상정보, 배포이력, 테스트결과, 연계이력 등 관련 정보를 확인하고 있습니까?		• 장애이력 • 구성정보 또는 CMDB • 형상·배포·테스트·연계 관련 이력
	- 장애 원인 분석 시 장애증상 및 장애 원인 유형을 기준에 따라 분류하고 있습니까?		• 장애보고서 • 장애 원인분석 결과
	- 장애 조치를 위해 변경, 배포, 백업·복구, 형상, 연계 등 관련 절차와 연계하고 있습니까?		• 장애기록 • 관련 절차 이관·처리 이력
	- 장애 조치 후 서비스 정상 여부, 데이터 정합성, 연계서비스 정상 여부 및 이용자 영향 해소 여부를 확인하고 있습니까?		• 복구 확인 이력 • 서비스 정상확인 결과
	- 장애의 재발방지를 위한 대책과 이행방안이 수립되고 있습니까?		• 장애보고서 • 재발방지대책 또는 조치계획
사후 관리	- 1등급 또는 2등급 장애의 장애사후관리, IRM 제출, 문제관리 이관 및 조치계획 이행관리가 수행되고 있습니까?	적합/부적합	• 장애사후관리 결과 • IRM 제출 이력 • 문제관리 이관 이력 • 조치계획 이행결과
	- 재발방지대책의 실제 활동이 수행되고 이에 대한 모니터링을 통한 개선활동이 진행되고 있습니까?		• 모니터링 결과

자. 관리 기준 및 예시

1) 기준 상세

○ 각 기관은 정보시스템 등급 및 장애등급에 따른 장애상황 보고체계를 갖추어야 하며, 아래 예시를 참조하여 보고대상과 보고시점을 정의하고 관리하여야 한다.

- 정보시스템에서 장애상황이 발생한 경우「주요 정보시스템 장애상황 관리체계」기준에 따라 관련 활동을 수행한다. (붙임2 참조)

○ 발생된 장애는 모두 기록관리하여야 한다.

- 정보시스템에 발생한 장애는 ITSM 등 관리시스템을 통해 장애 처리과정과 이력을 기록·관리하여야 한다.
- ITSM 등 운영시스템이 없는 경우 장애관리대장 등 문서 형태로 기록·관리할 수 있다.

2) 장애상황 보고체계

<주요 정보시스템 장애상황 관리체계>

구분	보고 및 전파		
	보고 전파 주체	보고 전파 대상	보고 전파 시점
정보시스템 장애	장애 발생기관	디지털안전상황실	• 장애 발생 확인 즉시
장애등급 결정 및 관계기관 전파	디지털안전상황실	국무조정실, 대통령비서실 등 관계기관	• 장애상황 접수 및 장애등급 결정 후
1등급 장애 경과보고	장애 발생기관	디지털안전상황실	• 매 2시간 경과 시마다 경과 시점으로부터 1시간 이내
2등급 장애 경과보고	장애 발생기관	디지털안전상황실	• 매 4시간 경과 시마다 경과 시점으로부터 1시간 이내
A4등급 정보시스템 장애	기관 자체 보고체계	기관 자체 보고체계	• 기관 자체 장애보고 기준에 따라 보고·전파
종료보고	장애 발생기관	디지털안전상황실	• 장애 발생 상황 종료 시

※ 참조사항

○ 기반시설·공통장비 장애 등 동일 원인으로 복수의 정보시스템이 영향을 받는 경우 해당 정보시스템 중 가장 높은 정보시스템 등급을 기준으로 장애등급을 지정한다.

○ 기관 내부의 세부 보고 절차와 전파 계통은 기관 특성에 맞게 사전 정의하며, 정보시스템 장애상황은 정보시스템 등급에 따라 주요 정보시스템 장애상황 관리체계를 우선 적용한다.

○ 장애상황 종료 시 종료보고를 실시하며, 장애 기록은 ITSM 등 관리시스템 또는 ITSM 등의 운영시스템이 없는 경우 장애관리대장 등 문서 형태로 기록·관리한다.

○ 디지털안전상황실장은 장애상황을 보고받은 경우 장애등급을 결정하고, 국무조정실, 대통령비서실 등 관계기관에 전파하여야 한다.

3) 장애보고서 (예시)

<table>
<tr><th colspan="6">장애 내역</th></tr>
<tr><td>시스템명</td><td colspan="2"></td><td>발생 일시</td><td colspan="2"></td></tr>
<tr><td>접수 일시</td><td colspan="2"></td><td>접수자</td><td colspan="2"></td></tr>
<tr><td>복구 일시</td><td colspan="2"></td><td>서비스 중단시간(분)</td><td colspan="2"></td></tr>
<tr><td>장애 증상 및 범위</td><td colspan="5"></td></tr>
<tr><td>서비스 영향도</td><td colspan="5"></td></tr>
<tr><td rowspan="6">시간대별
경과 사항</td><td>시 간</td><td colspan="3">피해상황 및 대응조치(요약)</td><td>담당자</td></tr>
<tr><td></td><td colspan="3"></td><td></td></tr>
<tr><td></td><td colspan="3"></td><td></td></tr>
<tr><td></td><td colspan="3"></td><td></td></tr>
<tr><td></td><td colspan="3"></td><td></td></tr>
<tr><td></td><td colspan="3"></td><td></td></tr>
<tr><td>비 고</td><td colspan="5"></td></tr>
<tr><td rowspan="2">반복 장애 이력</td><td>일 자</td><td colspan="3">처리 내역</td><td>중단시간(분)</td></tr>
<tr><td></td><td colspan="3"></td><td></td></tr>
<tr><th colspan="6">원인 분석</th></tr>
<tr><td>진행 여부</td><td colspan="5">☐ 완료 ☐ 미완료 ☐ 기타 (사유)</td></tr>
<tr><td>원인 유형</td><td colspan="5">☐ 인적 ☐ H/W ☐ S/W ☐ Application
☐ O/S ☐ N/W ☐ 기술 ☐ 구성</td></tr>
<tr><td>분석 결과</td><td colspan="5"></td></tr>
<tr><th colspan="6">처리 결과</th></tr>
<tr><td>처리내역</td><td colspan="4">※ 장애 원인 해소를 목적으로 기술적 관리, 관리적 관리, 물리적 관리 관점에서 처리 업무 세부내용을 작성할 것.</td><td></td></tr>
<tr><td>이행점검</td><td colspan="4">※ 위 처리내역의 각 사항에 대해 이행 유무 및 적합성 여부를 확인, 점검하고 결과를 작성할 것.</td><td></td></tr>
<tr><th colspan="6">Action Plan</th></tr>
<tr><td>시정 및
예방조치</td><td colspan="4">※ 처리 결과와 별도로 재발 방지를 위해 추가적으로 보완 또는 필요한 감쇄정책(Mitigation Plan) 등 실시한 내용을 작성할 것.</td><td></td></tr>
</table>

4) 장애관리대장 (예시)

장애 관리대장 (예시)

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

■ 붙임1 정보시스템 장애 유형

※ 행정기관 및 공공기관 정보시스템 안정성 고시 [별표 6]

정보시스템 장애 유형(제13조 관련)

구분	유형		내용
장애 증상에 따른 구분	서비스 중단		• 정보시스템의 예상하지 못한 원인으로 인해 시스템 접속 불가, 무응답 등 서비스 이용이 10분 이상 중단된 상태 • 10분 이내의 서비스 중단이 수차례 반복되는 상태 • 변경작업 등 사전공지된 작업에 따른 중단은 제외
	서비스 지연		• 정보시스템의 예상하지 못한 원인으로 인해 서비스가 지연되고, 10분 이상 경과한 후에도 계속 지연 현상이 발생하는 경우 • 이용자에게 접속 대기 순번을 안내하고 대기 종료 후 접속하여 정상적으로 서비스가 제공되는 경우는 지연으로 보지 않음
	서비스 오작동		• 정보시스템의 서비스가 작동하나 사용자에게 표출되는 결과물이 정상적이지 않은 경우 ※ (예시) 증명서 오발급, 화면 표시 정보 오류 등 • 단, 데이터가 정보시스템에 잘못 입력되어 잘못 입력된 대로 출력되는 경우 제외 ※ (예시) 홈페이지 담당자 연락처 오입력 정보 화면 표출 등
장애 원인에 따른 구분	내부 요인 장애		• HW·SW·AP 등 정보시스템을 구성하는 요소의 고장 또는 과부하 등으로 인한 장애
	외부 요인 장애	핵심 운영설비 장애	• 전원공급장치(UPS 등), 항온항습기 고장 등 핵심 운영설비에 문제가 생겨서 정보시스템의 장애가 발생한 경우
		사이버 침해 장애	• DDoS, 해킹, 랜섬웨어 등 사이버 침해가 정보시스템의 서비스 중단 또는 서비스 지연을 초래한 경우 • 정보시스템 기능에 직접적인 문제를 발생시키지 않는 정보 유출이나 위변조는 장애에 해당하지 않음 (⇨ 보안 침해사고로 분류·대응)
		연계 장애	• 외부 연계기관의 API 등 연계서비스에 의해 발생한 장애

■ 붙임2 정보시스템 장애등급 산정기준

※ 행정기관 및 공공기관 정보시스템 안정성 고시 [별표 7]

정보시스템 장애등급 산정기준(제14조 및 제15조 관련)

<table>
<tr><th>구분</th><th>주요내용</th></tr>
<tr><td>장애 정도 분류 기준</td><td>ㅇ 장애 정도는 중요, 일반, 경미한 장애로 구분
<table>
<tr><th>구분</th><th>내용</th></tr>
<tr><td>중요 장애</td><td>· 사용 빈도* 순으로 상위 10%에 속하는 핵심 기능 장애
· 기능 중단 시 실시간 연계된(데이터를 송신하는) 타 정보시스템의 서비스 제공에 차질을 초래하는 기능 장애</td></tr>
<tr><td>일반 장애</td><td>· 사용 빈도* 순으로 상위 50%에 속하는 기능 장애</td></tr>
<tr><td>경미한 장애</td><td>· 해당 기능이 중단되어도 정보시스템 본연의 업무를 처리하는 데 지장이 없는 부가 기능 장애 (게시판, 일반자료실, 조직도, 통계관리 등)
· 그 외 '중요', '일반'에 해당하지 않는 기능 장애</td></tr>
</table>
* 사용 빈도 산정 기준
① 전체 기능 수 산정: 시스템에서 제공하는 모든 기능을 메뉴 구조의 2단계(2레벨) 기준으로 나열
② 기능별 이용건수 산정: 모니터링 툴 또는 액세스 로그 등에 기록된 전체 데이터(최소 1개월 이상)를 기반으로 산정</td></tr>
<tr><td>장애 등급 보정 기준</td><td>
<table>
<tr><th>기준</th><th>1개 등급 하향</th><th>2개 등급 하향</th><th>비고</th></tr>
<tr><td>장애 정도</td><td>· 일반 장애 발생 시</td><td>· 경미한 장애 발생 시</td><td>· 전체 및 중요 장애 발생 시 원래 장애등급 부여</td></tr>
<tr><td>발생시간 보정</td><td>· 평일 09시~18시 이외 시간대 내부업무 서비스 장애
· 평일 09시~21시 이외 시간대 대국민 서비스 장애</td><td>-</td><td>· 다음 평일 09시까지 정상화 미완료 시 원래 장애등급 부여</td></tr>
<tr><td>지역 보정</td><td>· 전국 대상 서비스 제공 정보시스템에서 단일 광역 또는 기초 지자체 단위에 영향을 미치는 장애 발생 시</td><td>· 전국 대상 서비스 제공 정보시스템에서 단일 광역 또는 기초 지자체의 일부 지역에만 영향을 미치는 장애 발생 시</td><td>-</td></tr>
</table>
※ 복수 기준을 동시 적용 가능한 경우 합산해서 최대 2등급까지 하향 가능</td></tr>
<tr><td>장애 등급 산정표</td><td>
<table>
<tr><th rowspan="2">정보시스템 등급</th><th></th><th rowspan="2">장애등급</th><th colspan="2">등급보정</th></tr>
<tr><th>1개 등급 하향</th><th>2개 등급 하향</th></tr>
<tr><td>A1·A2등급</td><td>→</td><td>1등급</td><td>2등급</td><td>3등급</td></tr>
<tr><td>A3등급</td><td>→</td><td>2등급</td><td>3등급</td><td>4등급</td></tr>
<tr><td>A4등급</td><td>→</td><td>3등급</td><td>4등급</td><td>4등급</td></tr>
</table>
</td></tr>
</table>

■ 붙임3 주요 정보시스템 장애상황 관리체계

※ 행정기관 및 공공기관 정보시스템 안정성 고시 [별표 8]

주요 정보시스템 장애상황 관리체계(제15조 관련)

구분	주요내용	
보고 체계 (장애 발생기관)	보고 대상	A1, A2, A3등급 정보시스템 장애
	보고 주체	· 정보시스템 운영 담당자, 응용프로그램 담당자, 인프라 담당자, 데이터센터 관계자 등 · 정보시스템 운영 담당자뿐 아니라 API 연계 서비스 이용 기관도 관련 정보시스템 장애 인지 시 신속하게 신고
	보고 채널	· 디지털안전상황실 전화(대표번호 042-250-5777, 개별번호 042-250-5770~5775) · 문자메시지(대표번호 042-250-5777) 또는 SNS 소통방을 통해 장애발생 보고
보고내용 및 방법	최초 상황보고	· 대상시스템명 : ○○○ (○등급) ※ URL : · 기관(부서)명 : · 발생일시 : 00:00 ~ · 서버 위치 : · 피해내용 : · 장애원인 : · 조치사항 : · 장애등급 : ※ 장애원인, 조치사항 등 내용 확인에 장시간 소요되는 경우, 장애 발생일시 및 시스템명 등 기본적인 내용만 기입하여 우선 보고를 하고, 내용 파악 후 재보고 실시
	경과 보고	· 최초 상황보고 후, 장애 등급별 시간 경과*에 따라 피해내용, 원인, 조치사항을 작성하여 대표전화·문자메시지 또는 SNS 소통방을 통해 통보 * 민원 발생 또는 언론 보도 시, 1등급 장애가 2시간 이상 지속 시, 2등급 장애가 4시간 이상 지속 시 통보
	종료 보고	· 대상시스템명 : ○○○ (○등급) ※ URL : · 기관(부서)명 : · 장애시간 : 00:00 ~ 00:00 (oo분) · 서버 위치 : · 피해내용 : · 장애원인 : · 조치결과 : · 대국민 안내 : · 언론대응 방향 : · 장애등급 :

■ 붙임4 장애대응반 구성운영 (예시)

○ 장애대응반은 장애인지 즉시 장애를 조치할 수 있는 장소에 응소하여 장애를 조치한다.
- 장애대응반은 사전에 정의되고 구성되어야 하며, 비상연락체계를 현행화하여 유지한다.
- 공통장비 장애는 서비스 영향을 받은 최상위 업무등급 기준으로 각각 장애대응반을 구성한다.

○ 장애대응반 구성

장애등급	대응반장 (공무원)	대응반원 (공무원)	조치책임 (사업자)	조치반 (사업자)
1등급	담당과장	담당팀장 장애담당자	운영지원 및 유지관리 사업자 PM	장애조치자
2등급	담당팀장	장애담당자		장애조치자
3등급	담당팀장	장애담당자	운영지원 및 유지관리 사업자 PL	장애조치자
4등급	장애담당자	장애담당자		장애조치자

4. 문제관리 절차서

가. 개요

1) 목적

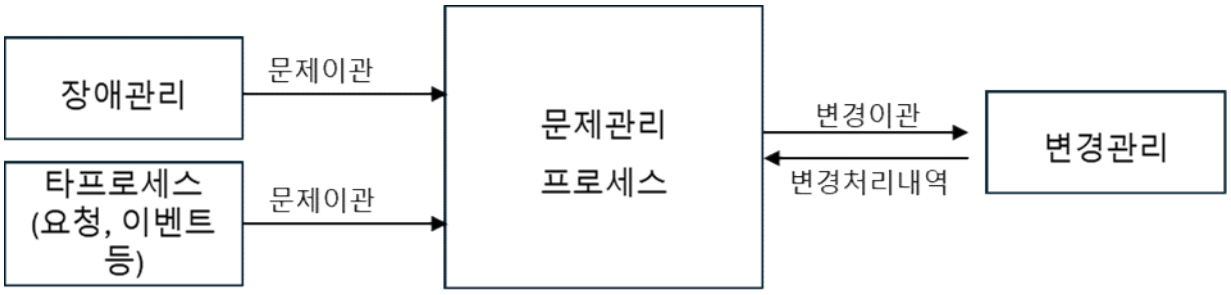
○ 정보시스템 운영 과정에서 발생한 장애, 운영 이벤트, 운영상태 모니터링, 변경·배포·테스트·연계·형상관리 활동 및 장애사후관리 결과 등에서 식별된 근본원인 미확인 사항 또는 반복 발생 가능성이 있는 문제에 대하여 근본원인을 분석하고, 임시해결책 및 영구해결책을 수립·관리하여 동일 또는 유사 장애의 재발을 방지하는 것을 목적으로 한다.

2) 적용 범위

○ 문제관리 절차는 행정·공공기관 정보시스템에 발생하거나 발생 가능성이 있는 문제의 등록, 분석, 조치, 종료 및 사전예방 활동에 적용한다.

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 타 프로세스(요청, 이벤트 등)에서 문제 등록 요청 사전 예방활동(경향 분석 등)을 위한 개선 사항(잠재적 문제 등)의 등록
프로세스 종료 조건	근본 원인 도출 또는 등록된 문제의 해결
증적(Output)	문제관리대장(문제처리 이력) ※ ITSM 시스템을 사용하는 경우 시스템 내 이력으로 대체

나. 관리 정책

1) 정의

○ 정보시스템 문제관리 절차의 운영에 있어 준수하여야 할 정책 기준을 제공.

2) 정책 기준

정책	설명	
정책 1	기준	문제관리는 장애, 이벤트, 운영상태, 변경, 배포, 테스트관리 및 장애사후관리 결과에서 식별된 문제에 대하여 근본원인 분석과 재발방지 활동을 수행한다.
	설명	○ 장애관리 절차는 서비스의 신속한 복구를 우선하고, 근본원인이 도출되지 않았거나 임시조치로 복구된 장애는 문제관리 절차로 이관하여 관리한다. ○ 장애사후관리 결과 근본원인 분석, 재발방지대책 수립 또는 조치계획 관리가 필요한 사항은 문제관리 절차와 연계하여 관리한다. ○ 운영상태 이상징후, 변경 실패, 배포 실패, 테스트 반복 결함, 연계 오류, 형상 불일치 등 잠재적 장애 요인은 문제로 등록하여 분석할 수 있다.
정책 2	기준	문제의 근본원인, 임시해결책, 영구해결책 및 조치결과는 기록·관리하고, 유사 장애 조치 및 예방활동에 활용한다.
	설명	○ 정보시스템의 문제관리 이력과 해결책 정보는 표준운영절차 운영시스템을 통해 관리한다. ○ ITSM 등 운영시스템이 없는 경우 문제관리대장 등 문서 형태로 기록·관리할 수 있다. ○ 등록된 문제 이력, 장애 이력, 알려진 오류 및 해결책 정보는 경향분석과 사전예방 활동에 활용한다.

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 Solution)	○ 정보시스템에 발생된 장애의 근본적인 원인에 대한 조치를 수행하는 방법 (영구 해결책)
근본원인 (Root Cause)	○ 장애 또는 문제가 발생하게 된 근본적인 원인으로, 제거하지 않을 경우 동일 또는 유사 장애가 반복 발생할 가능성이 있는 원인을 말한다.
알려진 오류 (Known-Error)	○ 발생된 문제의 근본원인과 임시해결책 등이 사전 도출되어 문서화 또는 KEDB에 등록되어 있는 오류
알려진 오류 DB (KEDB)	○ 장애 또는 문제의 발생 원인, 임시해결책, 영구해결책 및 조치 결과를 등록·관리하여 유사 장애 조치와 예방활동에 활용하는 지식 기반 정보를 말한다. - 표준운영절차 운영시스템으로 관리하고, ITSM 등 운영시스템이 없는 경우 문제관리대장 등 문서 형태로 관리할 수 있다.
사전예방적 문제관리 (Proactive Problem Management)	○ 기 발생 장애 유형이나 추세 분석을 통해 중대한 문제를 식별하거나 발생할 수 있는 장애를 사전 예방하기 위한 활동
이관	○ 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 이관하는 활동 포함
내부감사자	○ 프로세스가 사전 정의된 절차/기준으로 적합하게 운영/준수되고 있는지를 검증하는 내부 검증자 역할로, 각 프로세스별 정의된 검증 기준에 따라 정기적(반기 또는 연간)으로 프로세스 감사 활동을 수행

라. 역할 및 책임

○ 문제관리 절차를 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, 분석 내용, 보고서 등에 대한 검토	
	담당자	○ 문제조치 대상 정보시스템의 담당자가 역할 수행 ○ 문제관리 정책 및 절차 수립 ○ 문제관리 수행과 관련된 조치 참여 ○ 실 문제 처리자 또는 유지보수 조직의 조치 활동 통제 ○ 접수된 문제의 진행 여부 검토·승인 ○ 문제 경향분석 내용에 대한 검토	
수탁기관 또는 운영사업자	운영자	○ 운영기관과의 계약을 통해 정보시스템의 운영과 문제조치를 담당하는 수탁기관 또는 운영사업자 ○ 정보시스템을 구성하는 HW, SW, 미들웨어 등의 제조사 또는 유지보수를 담당하는 사업자 ○ 실 문제처리자 또는 유지보수 조직의 문제조치 활동 통제 ○ 문제의 근본 원인 분석을 통한 진단과 해결책 도출 및 조치 활동 - 문제 조치를 위한 변경관리 절차 연계 활동 ○ 담당 부서, 연계기관 등과 협조 요청 및 서비스 정상 확인 ○ 문제 등록, 분석, 조치 및 조치 계획 이행 상황 보고 ○ 장애/문제 경향 분석과 모니터링을 통한 예방 활동	

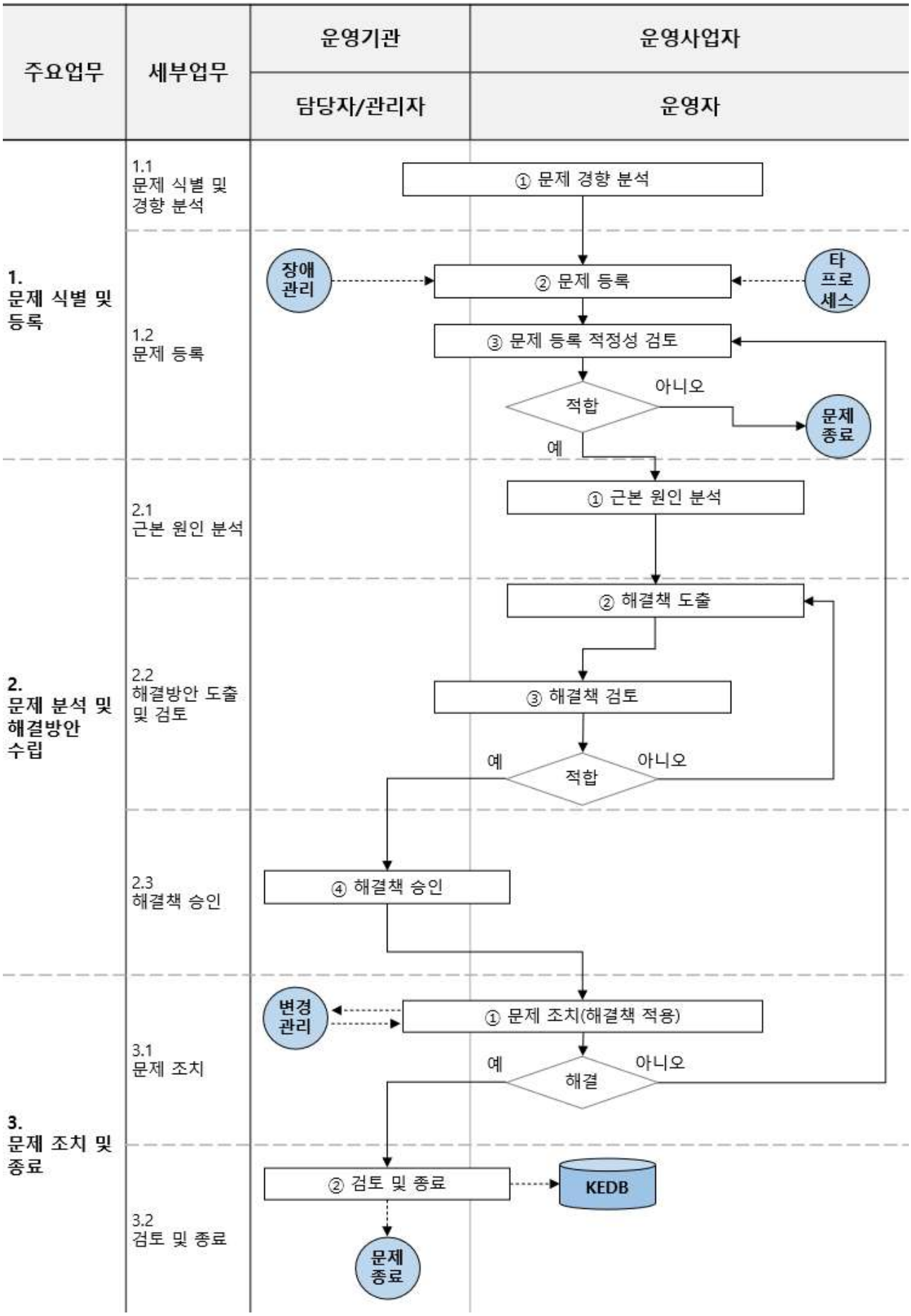
마. 표준절차 흐름도

○ 문제관리 절차는 아래와 같은 주요 업무와 수행절차들로 구성된다.

1) 주요 업무

주요 업무	세부 업무	수행 업무
1. 문제 식별 및 등록	1.1 문제 식별 및 경향 분석	○ 장애이력, 이벤트, 운영상태 모니터링 결과, 장애사후관리 결과 및 운영 활동 이력을 분석하여 잠재적 문제 또는 개선 필요사항을 식별한다. ○ 변경 실패, 배포 실패, 테스트 반복 결함, 연계 오류 등 반복 발생 가능성이 있는 사항을 문제관리 대상으로 검토한다.
	1.2 문제 등록	○ 장애관리 절차에서 이관된 근본원인 미도출 장애 또는 임시조치 장애를 문제관리 절차에 등록한다. ○ 장애사후관리 결과 근본원인 분석, 재발방지대책 수립 또는 조치계획 관리가 필요한 사항을 문제로 등록한다. ○ 도출된 개선사항 또는 타 프로세스 (변경, 이벤트 등)로부터 잠재적 문제나 관리가 필요한 문제를 등록
2. 문제 분석 및 해결방안 수립	2.1 근본원인 분석	○ 등록된 문제의 분석과 진단을 통해 근본 원인을 도출
	2.2 해결방안 도출 및 검토	○ 도출된 근본 원인을 해결할 복수의 해결방안을 도출 - 근본 원인에 대한 영구 해결책을 도출 - 해결책에 대해 비즈니스 측면, 재정적인 측면, 기술적인 측면 등 다각적인 측면에서 적용 가능 여부를 검토
	2.3 해결책 승인	○ 운영기관 담당자는 도출된 해결책의 적용 여부를 승인한다.
3. 문제 조치 및 종료	3.1 문제 조치	○ 승인된 해결책을 적용하여 문제를 조치한다. - 조치를 위해 정보시스템 변경이 필요한 경우 관련 절차와 연계하여 수행한다.
	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	운영사업자
		관리자/담당자	운영자
1.1- ① 문제 식별 및 경향 분석	- 장애이력, 이벤트, 운영상태 모니터링 결과, 장애사후관리 결과 및 운영활동 이력을 분석하여 잠재적 문제 또는 개선 필요사항을 식별한다. - 변경 실패, 배포 실패, 테스트 반복 결함, 연계 오류, 형상 불일치 등 반복 발생 가능성이 있는 사항을 문제관리 대상으로 검토한다. - 도출된 문제 또는 이슈는 문제관리 절차에 등록하여 집중 관리 및 개선활동을 수행하도록 한다.	◑	●
1.2- ② 문제 등록	- 장애관리 절차에서 이관된 근본 원인 미도출 장애 또는 임시조치 장애를 문제관리 절차에 등록한다. - 장애사후관리 결과 근본원인 분석, 재발방지대책 수립 또는 조치계획 관리가 필요한 사항을 문제로 등록한다. - 이벤트, 운영상태, 변경, 배포, 테스트관리 등 관련 절차에서 지속 관리가 필요한 사항을 문제로 등록한다. - Output: 문제기록	◑	●
1.2- ③ 문제 등록 적정성 검토	- 운영기관 담당자는 등록된 문제의 적합 여부를 검토한다. - 적합 여부 판단을 위해 필요한 경우 장애관리 담당자, 운영자, 정보시스템 담당자, 연계기관 등 관련 이해관계자와 협의한다. - 문제로 등록하기에 적합하지 않은 경우 사유를 기록하고 종료한다.	◑	●
2.1- ① 근본 원인 분석	- 운영자는 문제분석과 해결책 도출을 위한 담당자를 지정한다. - 문제조치 담당자는 등록된 문제의 현상과 관련 기록을 분석하여 문제의 근본 원인을 도출한다. - 표준운영절차 운영시스템을 보유한 경우 기존 장애 이력, 문제 이력 또는 알려진 오류 정보 등을 활용한다. - 클라우드 환경의 경우 운영자가 보유한 운영 로그, 장애 이력 및 조치 이력을 활용할 수 있다.		●

(●: 정, ◑: 부)

세부 절차	수행 내용	운영기관	운영사업자
		관리자/담당자	운영자
2.2- ② 해결책 도출	- 문제 원인 분석을 통해 조치를 위한 해결책을 도출한다. - 근본 원인 조치를 위한 영구 해결책 도출을 목표로 수행하며, 해결책은 여러 개의 해결책으로 도출될 수 있다. ※ 도출되는 해결책은 비즈니스 측면, 재정적인 측면, 기술적인 측면 등 다각적인 측면에서 적용 가능 여부를 검토하도록 한다.		●
2.2- ③ 해결책 검토	- 도출된 해결책은 관련 이해관계자 검토를 통해 적합한 해결책인지 검토한다. (적합하지 않은 경우, 해결책 도출 타스크를 재수행한다.) - 해결책은 도출되었으나 이해관계자가 조직의 상황 및 비용적 문제 등으로 해결책을 적용할 수 없거나, 해결책 미적용으로 발생할 수 있는 리스크를 수용할 경우, 해당 문제 건은 해결책을 적용하지 않고 종료할 수 있다.	◑	●
2.3- ④ 해결책 승인	- 운영기관 또는 수탁기관의 담당자는 검토된 해결책의 적용 여부에 대해 검토/승인 활동을 수행한다.	●	◑
3.1- ① 문제 조치	- 문제조치 담당자는 승인된 해결책 적용을 위한 관련 활동을 수행한다. - 조치를 위해 변경 작업이 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 수탁기관의 담당자에게 조치 건에 대한 검토를 요청한다.	◑	●
3.2- ③ 검토 및 종료	- 운영기관 또는 수탁기관의 담당자는 조치된 문제 건을 검토 및 확인하고 해당 문제 건을 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 활용 시 KEDB	●	◑

사. 핵심성과지표 (KPI : Key Performance Indicator)

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

측정 지표	측정 방법(예시)	측정 목적	측정 주기
문제 적기 처리율	(목표 시간 내 처리된 문제 건수 / 당월 종료된 문제 건수) X 100	문제조치의 적기 처리 건수 관리(상호 합의된 처리시간 준수)	당월

아. 수행 검증

1) 검증 방법

○ 검증 체크리스트의 체크 항목 기준(ITIL 표준 준용)으로 표준운영절차의 준수 여부와 이행 점검을 수행한다.

○ 개별기관 내 자체 프로세스 검증자는 내부 감사자의 자격 또는 ITIL에 대한 충분한 이해를 가진 자가 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 식별 및 등록	- 장애관리에서 임시 해결 또는 근본원인이 미도출된 장애 건에 대해서 문제관리로 이관되어 등록·관리되고 있습니까?	적합/ 부적합	• ITSM 등록 이력 또는 문제관리대장
	- 사전 예방활동이나 타 프로세스의 수행 중 도출되는 잠재적 문제 등이 문제로 등록·관리되고 있습니까?		
	- 문제의 등록 기준이 정의되고 이해관계자에게 공유되어 있습니까?		• 문제등록기준
문제 분석 및 해결방안 수립	- 접수된 문제의 경우 문제의 적합성 여부를 검토·판단하여 접수 또는 반려하고 있습니까?		• 문제등록 검토이력 • 문제관리대장
	- 임시 해결책, 영구 해결책 및 재발방지대책이 검토·수립되고 있습니까?		• 해결방안 검토 이력 • 재발방지대책
	- 원인 파악 불가 또는 해결책 미도출로 처리해야 하는 경우 해당 문제에 대한 처리·관리 기준을 정의하고 있습니까?		• 문제처리기준
문제 조치 및 종료	- 문제의 근본 원인 조치를 위해 변경 작업이 필요한 경우 변경 절차와 연계하여 조치작업을 진행하고 있습니까?		• 관련 절차 이관·처리 이력
	- 문제 조치결과, 근본원인, 해결책 및 재발방지대책 이행 여부를 확인한 후 문제를 종료하고 있습니까?		• 문제조치 결과, 종료 승인 이력
	- 알려진 오류 및 해결책이 운영시스템, KEDB 또는 문제관리대장에 등록되어 유사 장애 조치와 예방활동에 활용되고 있습니까?		• KEDB 등록 이력 • 문제관리대장

자. 관리 기준

1) 문제 등록(이관) 기준

구분	정의
원인 불명의 변경 실패	○ 변경 작업이 실패하여 원복하였으나 실패의 원인을 알 수 없는 경우나 기타 분석 활동이 필요한 경우
근본 원인 불명 및 임시조치 장애	○ 장애 조치 중 장애의 근본 원인이 도출되지 않은 경우나 임시 해결책(재기동 등)을 통해 긴급히 장애 조치를 수행한 경우
장애사후관리 결과	○ 장애사후관리 점검 결과 근본 원인 분석, 재발방지대책 수립 또는 조치 계획 관리가 필요한 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
관리자의 판단	○ 타 프로세스의 관리자가 운영 활동 중에 나타나는 잠재적 문제나 이슈 등에 대해 문제관리로 등록이 필요하다고 판단하는 경우
원인 불명의 이벤트	○ 발생된 이벤트의 원인이 확인되지 않거나 반복 발생하여 근본 원인 분석이 필요한 경우
이벤트 로그 분석	○ 반복적으로 발생하는 이벤트에 대해 장애 예방 차원의 근본 원인 분석과 해결책이 필요하다고 판단되는 경우
원인 불명의 배포 실패	○ 배포 작업 실패 또는 배포 후 롤백이 발생하였으나 명확한 원인이 확인되지 않은 경우
테스트 반복 결함	○ 테스트 과정에서 동일 또는 유사 결함이 반복 발생하거나 결함 원인이 명확하지 않은 경우
연계 오류	○ 대내외 연계 API, 전문 송수신, 데이터 연계 과정에서 반복 오류 또는 원인 불명의 오류가 발생한 경우
형상 불일치	○ 운영환경, 검증환경, 형상관리시스템 간 소스코드, 설정 파일, DB 스크립트, 배포 파일의 버전 또는 기준선이 불일치하는 경우
운영상태 이상징후	○ 운영상태 모니터링 결과 응답 지연, 오류 로그, 자원 사용량 증가 등 잠재적 장애로 발전할 가능성이 있는 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

5. 구성관리 절차서

가. 개요

1) 목적

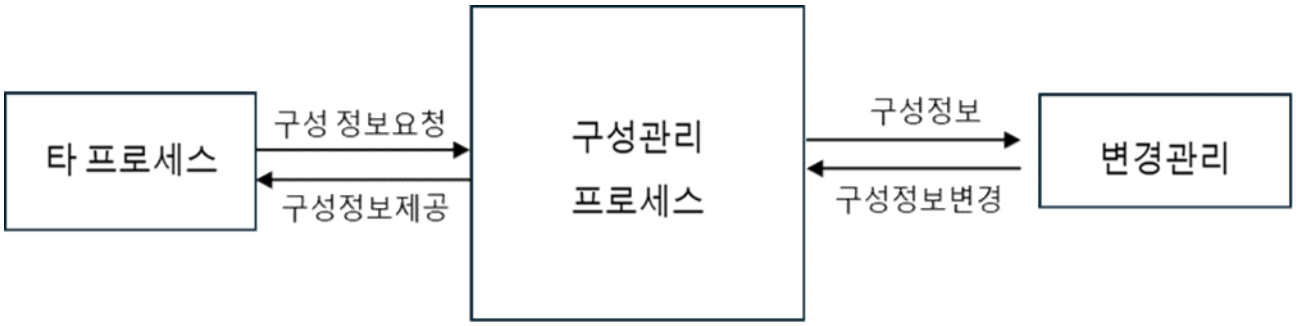
○ IT 서비스 제공에 관련된 하드웨어, 소프트웨어, 네트워크 등의 장비와 이를 구성하고 있는 정보에 대하여 등록, 변경, 재사용, 폐기 등의 생명주기(Life-Cycle) 및 이력 정보를 관리하여, 구성 정보를 최신 상태로 유지·관리하고 다른 서비스 관리 프로세스에 정확한 구성 현황 정보를 제공하는 것을 목적으로 한다.

2) 적용 범위

○ 구성관리 절차는 행정·공공기관 정보시스템 운영관리에 적용된다.

3) 관련 업무 절차

○ 연관 선/후행 업무



○ 시작/종료/증적(Output) 조건

주요 업무	수행 업무
프로세스 시작 조건	구성관리 범위 정의 및 구성 정보 식별 신규 CI 등록 요청 변경 작업에 의한 CI 정보(속성) 업데이트 요청
프로세스 종료 조건	구성 항목 업데이트
증적(Output)	구성 정보 관리대장 구성 정보 실사결과 ※ ITSM 시스템을 사용하는 경우 시스템 내 증적으로 대체

나. 관리 정책

1) 정의

○ 정보시스템 표준운영절차의 운영에 있어서 필히 준수해야 할 정책 기준을 제공

2) 정책 기준

정책	설명	
정책 1	기준	모든 구성 항목(CI)은 분류 체계와 명명 규칙에 따라 고유한 이름으로 구별할 수 있어야 한다.
	설명	○ 구성 항목은 관리 가능하도록 분류 체계와 명명 규칙이 정의되고 규칙에 따라 구별되어야 한다. ○ 관리의 효율성을 위해 명명 규칙은 중복이 발생하지 않도록 해야 한다. ○ 구성 항목별 고유 특성을 대표하는 특성 항목들로 정의되어야 한다.
정책 2	기준	구성 정보는 IT 환경의 현재 상태를 기준으로 현행화하고 유지 관리하여야 한다.
	설명	○ 구성 정보는 상호 연계되어 정확성과 최신성이 유지되도록 관리되어야 한다. ○ 구성 정보는 ITSM과 같은 관리시스템을 통해 적절하게 관리·통제되어야 하며 정보의 변경 이력과 같이 관리되어야 한다. ※ ITSM 시스템이 없는 경우 구성 정보에 대한 관리대장을 통해 관리하며, 지속적으로 변경에 대한 이력을 현행화하여야 한다. ○ 구성 항목별로 명확한 담당자가 규정되어 최신 정보 유지에 대한 책임을 지도록 한다. ○ 구성 항목에 대한 모든 변경은 승인 및 통제되어야 한다.
정책 3	기준	구성 정보는 신뢰성과 정확성을 보증할 수 있도록 검증되고 관리되어야 한다.
	설명	○ 구성 항목의 현황 및 이력 정보를 제공해야 한다. ○ 구성 실사 및 보고는 정기적으로 수행되어야 한다.(반기 1회 이상의 구성감사 권고) ○ 실사를 위한 조직은 필요시 독립적으로 구성할 수 있다.

다. 용어 정의

용어	설명
자산 정보	○ 정보시스템 자산의 식별, 추적 및 관리에 필요한 정보로서 하드웨어, 소프트웨어, 네트워크 장비 등 자산의 세부 사항과 재무 정보를 포함한다.
구성 항목(CI)	○ 정보 자산을 사용하여 운영에 필요한 정보를 구성 정보라 하며, 정보시스템 및 서비스를 구성하는 항목들에 대한 구체적인 데이터이면서 각각의 컴포넌트를 말한다.
클라우드 자산 정보	○ 클라우드 환경에서 사용되는 정보시스템 자산의 세부 정보로서 가상머신, 스토리지, 네트워크 장비, 데이터베이스 등 다양한 클라우드 리소스를 포함하며, 이들 자산의 식별, 추적, 관리에 필요한 정보를 제공한다.
클라우드 구성 정보	○ 클라우드 환경에서 사용하는 정보시스템 및 서비스의 구성 항목(CI)들에 대한 구체적인 데이터로, 클라우드 인프라와 서비스를 효과적으로 관리하고 최적화하기 위한 필수적인 데이터를 의미한다.
CMDB (Configuration Management Database)	○ 구성 항목에 대한 정보 및 상세 내역, 구성 항목 간의 관계성을 담고 있는 데이터베이스를 말한다.
속성	○ 구성관리를 통해 관리되는 구성 항목의 특정 정보 및 사양을 의미한다.
내부감사자	○ 프로세스가 사전에 정의된 절차 및 기준에 따라 적합하게 운영·준수되고 있는지를 검증하는 내부 검증자 역할로, 각 프로세스별 정의된 검증 기준에 따라 정기적(반기 또는 연간)으로 프로세스 감사 활동을 수행한다.

라. 역할 및 책임

○ 구성관리 절차를 수행하는 역할자의 책임은 다음과 같다.

주요 업무		수행 업무	비고
운영기관 (정보시스템의 최종운영관리를 책임지는 기관)	관리자	○ 정보시스템 관련 담당자의 상위 책임자 또는 부서장 ○ 구성 감사 승인 관련 의사결정	
	담당자	○ 구성 정보 작업 대상 정보시스템의 담당자가 역할 수행 ○ 구성관리 활동 관련 이해당사자 간 조율 및 의사소통 창구 ○ 구성관리 계획의 적정 여부 및 정보 변경 시 검토 ○ 변경 작업으로 인해 구성 정보가 변경되는 경우 해당 구성 정보에 대한 정합성 확인	
수탁기관 또는 운영사업자	운영자	○ 운영기관과의 계약을 통해 정보시스템의 운영, 유지보수 및 변경 작업을 담당하는 수탁기관 또는 운영사업자 ○ 정보시스템을 구성하는 HW, SW, 미들웨어 등의 제조사 또는 유지보수 사업자와 협력하여 구성관리 업무 수행 ○ 클라우드 인프라 환경에서 발생하는 구성 항목 관련 활동 ○ 구성관리 계획의 적정 여부 검토 ○ 구성관리 계획 수립과 관련 제반 준비작업 - 구성분류체계, 관리대상/범위, 관리속성 정의 등 ○ 구성 항목 변경 작업 수행 - 변경 작업 이후 구성 정보에 대한 현행화 작업 ○ 변경 작업으로 인해 구성 정보가 변경되는 경우 해당 구성 정보에 대한 정합성 확인	

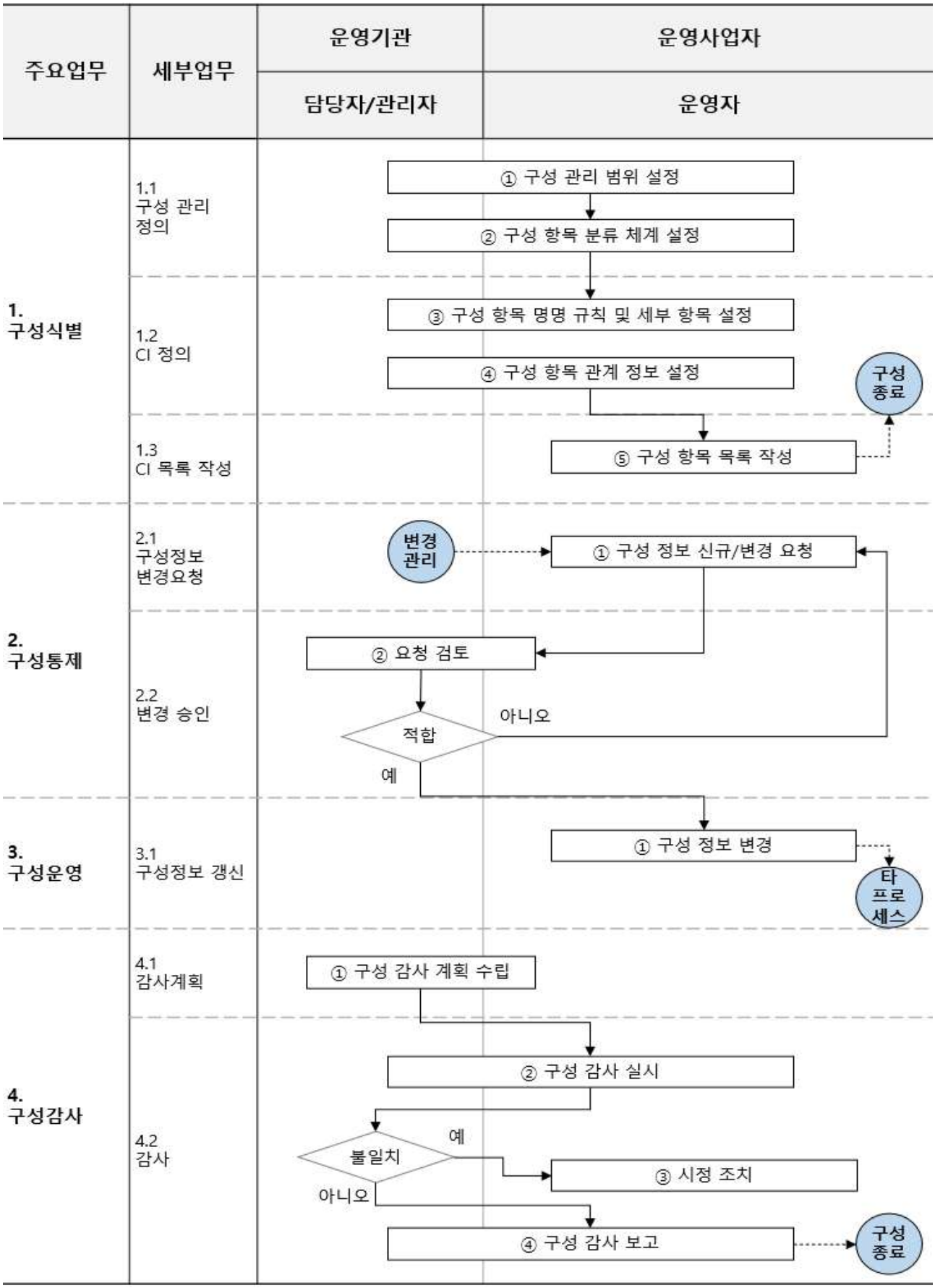
마. 표준절차 흐름도

○ 구성관리 절차는 아래와 같은 주요 업무와 수행절차들로 구성된다.

1) 주요 업무

주요 업무	세부 업무	수행 업무
1. 구성 식별	1.1 구성관리 정의	○ 운영기관 담당자와 운영자(구성 담당자)는 관리하고자 하는 구성 범위에 대하여 대상, 범위, 수집 방안, 구성 관리 DB(CMDB)에 대한 관리계획을 수립하고 작성한다.
	1.2 CI 정의	○ 구성 항목(CI)에 대한 명명 규칙 및 속성, 연관 기준 등을 정의한다.
	1.3 CI 목록 작성	○ 운영자(구성 담당자)는 정의된 CI에 대한 조사를 진행하여, CI 목록을 작성하고 이를 바탕으로 CMDB를 구축한다. (ITSM 시스템을 활용한 CMDB 구축을 권고하나, ITSM 미사용 기관은 별도의 방법을 활용하여 관련 목록을 정리한다.)
2. 구성 통제	2.1 변경 요청 관리	○ 운영자(구성 담당자)는 구성 항목의 추가, 삭제 등 변경이 필요한 경우, 변경된 내용에 대해 운영기관 담당자에게 변경 사항에 대한 검토를 요청한다.
	2.2 변경 승인	○ 운영기관 담당자는 구성 정보/관리체계의 변경 사항을 확인하고, 적합할 경우 변경을 승인한다.
3. 구성 운영 (CMDB)	3.1 구성 정보 갱신	○ 운영자(구성 담당자)는 변경 작업에서 의뢰된 구성 항목의 정보에 대한 변경 작업을 수행하여 정보의 현행화를 진행한다.
4. 구성 감사	4.1 감사계획	○ 운영기관 담당자는 구성 정보가 실제 환경과 일치하는지 확인하고 일관성을 유지하기 위한 방안으로 감사 계획을 수립한다.
	4.2 감사	○ 운영기관 담당자와 운영자(변경 담당자)는 계획된 감사 계획에 의거하여 구성 감사를 실시하고 보고한다. 운영자(구성 담당자)는 필요시 시정 조치를 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	운영사업자
		관리자/담당자	운영자
1.1- ① 구성 관리 범위 설정	- 운영기관 담당자는 운영자와 협업하여 구성관리 대상과 범위 및 관리 방안을 설정한다. 주요 내역은 아래와 같다. · 구성 관리 대상, 범위 · 구성 관리 계획 등 ※ 주기적으로 관리 대상과 범위, 계획 등을 업데이트하여 관리한다.	●	◑
1.1- ② 구성 항목 분류 체계 설정	- 운영기관 담당자는 운영자와 협업하여 정해진 범위 안에서 구성 항목의 분류를 위한 기준을 수립한다. - 기준의 예시는 "자. 관리 기준"을 참조한다.	●	◑
1.2- ③ 구성 항목 명명 규칙 및 세부 항목 설정	- 운영기관 담당자는 운영자와 협업하여 구성 항목에 대한 명명 규칙 및 세부 속성에 대한 기준을 수립한다. - 명명 규칙 및 세부 속성 예시는 "자. 관리 기준"을 참조한다.	●	◑
1.2- ④ 구성 항목 관계 정보 설정	- 구성 항목 간의 상호 관계 정보에 대한 관리범위를 정의하고 관련 정보를 파악한다. ※ 구성 항목 간 상호 연계 정보는 서비스의 영향도 파악이나 장애 발생 시 관련 시스템의 정보 파악을 위해 중요한 관리 정보이다.	●	◑
1.3- ⑤ 구성 항목 목록 작성	- 운영자(구성 담당자)는 정해진 기준에 따라 CI 정보를 확인하고, 목록을 작성한다. - ITSM 시스템을 사용하는 기관은 CMDB를 활용하여 CI, 속성, 연결 관계 등 관련 정보를 기록한다. ITSM 시스템 미사용 기관은 관련 정보를 Excel 등을 활용하여 문서로 관리한다. ※ ITSM 시스템을 활용한 CMDB 구축을 권고	◑	●

(●: 정, ◑: 부)

세부 절차	수행 내용	운영기관	운영사업자
		관리자/담당자	운영자
2.1- ① 구성 정보 신규/변경 요청	- 운영자는 구성 정보의 신규 등록 또는 인프라 작업 등을 통해 운영상의 구성 정보 변경 사항이 발생한 경우 구성 정보 변경 내용에 대하여 운영기관 담당자에게 검토를 요청한다. ※ ITSM 시스템을 활용하는 경우, 인프라 변경 작업 이후 해당 구성 정보에 대한 변경을 수행하고 운영기관 담당자의 검토를 통해 정보를 업데이트한다.		●
2.2- ② 요청 검토	- 운영기관 담당자는 구성 정보의 변경 내용을 검토하여 정보의 적합성에 대해 승인 여부를 결정한다.	●	◑
3.1- ① 구성 정보 변경	- 운영자는 구성 정보의 변경 작업을 수행하여 정보의 현행화를 진행한다.		●
4.1- ① 구성 감사 계획 수립	- 운영기관 또는 수탁기관의 담당자는 구성 정보가 실제 환경과 일치하는지 확인하고 일관성을 유지하기 위한 방안으로 감사 계획을 수립한다. - 감사는 정기/비정기 감사로 구분할 수 있으며, 정기 감사는 연 2회 정도의 감사를 권고한다. - 감사 계획 수립은 "자. 관리 기준"을 참조한다. - 감사를 위한 조직은 필요시 독립적으로 구성할 수 있으며, 자신의 업무에 대한 감사는 배제한다.	●	◑
4.2- ② 구성 감사 실시	- 운영기관 또는 수탁기관의 담당자는 감사를 실시하고, 관련 결과를 취합한다. (감사의 원활한 수행을 위해 운영자의 지원을 받아 진행할 수 있다.) - 취합된 실사 결과들을 검토하여 CMDB와의 불일치가 있는지 확인하며 불일치 정보가 있는 경우 관련 원인을 분석한다. - CMDB 불일치 원인 분석 결과를 바탕으로 CMDB를 갱신하여 해결할 것인지, 실물을 변경해야 해결할 것인지 판별하고 구체적인 계획을 수립한다.	●	◑
4.2- ③ 시정 조치	- 운영자는 시정 조치와 관련 계획에 따라 시정 조치를 수행한다.		●
4.2- ④ 구성감사 보고	- 운영자는 CMDB 불일치 원인 분석 결과, 시정 조치 등을 포함한 감사보고서를 작성한다. - 운영자는 구성 감사에 대한 감사보고서 및 시정 조치 결과를 운영기관 담당자에게 보고한다.	◑	●

사. 핵심성과지표 (KPI : Key Performance Indicator)

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

측정 지표	측정 방법(예시)	측정 목적	측정 주기
구성 정보 정합률	100 - ((불일치 CI 항목 수 / 감사대상 CI 항목 수)) X 100	CI 불일치 개선	반기

아. 수행 검증

1) 검증 방법

○ 검증 체크리스트의 체크 항목 기준(ITIL 표준 준용)으로 표준운영절차의 준수 여부와 이행 점검을 수행한다.

○ 개별기관 내 자체 프로세스 검증자는 내부 감사자의 자격 또는 ITIL에 대한 충분한 이해를 가진 자가 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
구성 식별	- 구성관리를 위한 구성 항목 분류 체계(유형, 관리 수준, 관리 속성, 관계 정보)가 정의되고 관리되고 있습니까?	적합/ 부적합	• ITSM 기록 또는 구성관리 계획(구성 분류 체계) 문서
	- 구성 항목 식별을 위한 정보 수집 시 IT서비스 기반 구성 항목 간 연관 관계 정보를 분석하고 있습니까?		• ITSM 기록 또는 구성 항목 관리대장
	- 모든 구성 항목은 고유하게 구분되고, 기록되고 있습니까?		• ITSM 기록 또는 구성 항목 관리대장
구성 통제	- CMDB는 구성 항목의 신뢰도와 정확도를 보증하기 위해 지속적인 모니터링 활동이 진행되고 있습니까?		-
	- 구성 정보를 CMDB에 등록 후 구성 항목의 신규 등록 및 구성 정보의 변경은 변경관리 프로세스를 통해 관리되고 있습니까?		• ITSM 기록 또는 구성 항목 변경이력
구성 운영	- 구성 정보의 현행화·업데이트는 적절한 절차와 기준에 맞추어 관리되고 있습니까?		• ITSM 기록 또는 구성 항목 변경이력
구성 감사	- 구성 항목의 변경은 추적 가능하고, 감사가 가능합니까?		• ITSM 기록 또는 구성감사 이력
	- 정기적인 구성감사가 계획되고 수행되고 있습니까?		• ITSM 기록 또는 구성감사 이력
	- 감사의 결과는 기록·관리되고 발견된 부적합 사항은 적절한 절차를 통해서 반영되고 있습니까?		• 구성감사 조치 이력

자. 관리 기준 및 예시

1) 구성 항목 분류 체계(예시)

○ 구성 항목 분류 체계 관리를 위한 참조(예시) 기준으로 개별기관의 운영환경에 맞추어 구성 항목의 분류 체계를 설정하고 관리하여야 한다.

※ 클라우드 서비스를 이용 시에는 제공받는 서비스 환경에 맞추어 운영자와 협의를 통해 분류 체계를 설정할 수 있다.

구분	대분류	중분류	소분류	중분류 약어
인프라	하드웨어	서버	단순서버	ISVR ※ 중분류 기준 CI 명명규칙 예시
			통합서버	
			NIRS x86서버	
			Unix서버	
			블레이드서버	
			메인서버	
			기타	
		네트워크	라우터	INET
			스위치	
			CSU/DSU/모뎀	
			기타	
		스토리지	NAS	ISTR
			SAN	
			SAN Switch	
			기타	
		백업장비	PTL백업	IBAC
			VTL백업	
			기타	
		기반설비	항온항습기	IINF
			UPS	
		보안시스템	방화벽(Firewall)	ISEC
			가상사설망(VPN)	
			침입탐지시스템(IDS)	
			침입방지시스템(IPS)	
			DDoS 대응 장비	
			UTM	
			기타	
	클라우드	컴퓨팅	가상머신	CCOM
			컨테이너	
			서버리스 컴퓨팅	
			기타	

구분	대분류	중분류	소분류	비고
인프라	클라우드	스토리지	객체 스토리지	CSTR
			블록 스토리지	
			NAS 스토리지	
			아카이브 스토리지	
			기타	
		네트워크	VPC	CNET
			로드밸런서	
			도메인	
			기타	
		데이터베이스	관계형 데이터베이스	CDBM
			비관계형 데이터베이스	
			데이터 웨어하우스	
			기타	
		보안	네트워크 ACL	CSEC
			Security Services	
			Secure Zone	
			기타	
	소프트웨어	운영체계	유닉스	SOPS
			리눅스	
			윈도우	
			메인프레임	
			임베디드	
			Hypervisor	
			클라우드	
			기타	
		미들웨어	WEB	SMDW
			WAS	
			기타	
		DBMS	DBMS	SDBM
			데이터 관리 도구	
			데이터 모델링	
			기타	

구분	대분류	중분류	소분류	비고
인프라	소프트웨어	시스템관리	SMS	SSYS
			NMS	
			APM	
			개발S/W	
			백업S/W	
			보안S/W	

2) 주요 속성 (예시)

구분	하위범주	속성	설명
공통	기본정보	CI명(구성 항목)	구성 항목을 고유하게 구분해 주는 구성 항목명
		범주	구성 항목 분류 체계 (예시) 참조
		상태	구성 항목의 상태정보: 운영, DR, 개발, 테스트, 유휴, 운영예정, 처분, 불용, 기타
		자산명	자산의 명칭을 기록
		제조사	구성 항목의 제조 및 개발회사
		공급사	구성 항목의 공급회사, 문서는 제외
		사용회사	구성 항목을 사용하고 있는 기관
		소유회사	구성 항목을 소유하고 있는 기관
	관리정보	관리번호	관리 번호
		구성 항목 위치	구성 항목의 위치 정보
		도입일자	도입 일자
		자산구분	기관자산/외주/임차/기타
		반입일	자산의 운영을 위해 반입한 날짜를 기록
		반출일	자산의 처분이나 불용을 위해 반출한 날짜를 기록
		관리 부서	구성 항목의 관리 부서
		관리 담당자	구성 항목 관리자
		관리 담당자 연락처	관리 담당자의 휴대전화 번호
		비고	자세한 설명, 운영상의 주의 사항, 특이 사항 등
	유지보수	유지보수 업체	해당 CI를 유지보수하는 업체
		유지보수 업체 담당자	유지보수 업체의 담당자
		유지보수 업체 담당자 연락처	유지보수 업체 담당자 연락처
		유지보수 유무	유지보수 수행 여부
		유지보수 기간	유지보수 시작일과 유지보수 종료일을 기록
하드웨어	서버	호스트명	호스트명
		제품명	서버의 모델 명칭
		제품번호(시리얼번호)	제품번호나 시리얼번호
		대표IP	IP주소
		NAS IP	
		DB IP	
		서비스 IP	
		HA 구성	예)HACMP
		Rack 번호	

구분	하위범주	속성	설명
하드웨어	서버	OS 버전	
		CPU 속도	CPU Clock 속도
		Core 개수	
		CPU 타입	CPU 타입
		Bandwidth	대역폭
		Memory	Memory 용량
		서버등급	대형, 중형, 소형
		Internal Disk	예) 146GB*4
		External Disk	예) 146GB*4
		업무명	대상업무명
		백업적용	백업적용 여부
		소산적용	소산적용 여부
		보안Tool설치	보안Tool설치유무
		백신설치	백신설치유무
	네트워크	호스트명	네트워크 호스트명
		모델명	네트워크 장비의 모델
		제품번호	제품번호
		대표 IP	
		서비스 IP	
		용도	
		Rack 번호	
		대역폭	네트워크 내부 Bus의 대역폭
		Interface 개수	
	스토리지/백업장비	제품번호	제품번호
		IP주소	IP주소
		용량	디스크 총용량
		업무	용도
	보안장비	호스트명	호스트명
		제품명	장비의 모델 명칭
		제품번호	제품번호
		대표IP	IP주소
		CPU 속도	CPU Clock 속도
		Core 개수	
		CPU 타입	CPU 타입

구분	하위범주	속성	설명
클라우드	컴퓨팅- 가상머신	인스턴스 ID	VM 식별을 위한 ID
		VM 이름	VM 이름
		인스턴스 유형	하드웨어 리소스
		CPU	할당된 가상 CPU의 수
		메모리	할당된 메모리의 크기
		디스크 크기	할당된 디스크의 크기
		운영체계	운영체계
		상태	실행 중, 중지됨, 일시 중단됨
	컴퓨팅- 컨테이너	컨테이너 ID	컨테이너 식별을 위한 ID
		이미지	컨테이너 생성 템플릿의 이름
		상태	실행 중, 중지됨, 일시 중단됨
		이름	컨테이너의 논리적 이름
		포트	외부 통신을 위한 네트워크 포트
		네트워크	컨테이너가 연결된 네트워크 설정 (브리지, 호스트 등)
		호스트이름	호스트이름
	컴퓨팅 - 서버리스	함수이름	서버리스 함수 이름
		트리거	서버리스 함수 실행 조건 혹은 이벤트
		메모리 할당량	함수 실행에 할당되는 메모리 크기
		실행 시간 제한	함수가 실행될 수 있는 최대 시간
	스토리지 - 볼륨	볼륨 ID	볼륨 식별 ID
		이름	볼륨 이름
		유형	SSD, HDD 등에서 선택
		크기	볼륨의 용량
		I/O 성능	볼륨의 입출력 성능
		스토리지 클래스	표준, 데이터용, 보관용 등에서 선택
	스토리지 - 오브젝트	버킷 이름	버킷 이름
		생성 일자	오브젝트 생성 일자
		KEY	버킷 내 오브젝트를 식별하는 고유 이름
		오브젝트 수	오브젝트 수
	스토리지 - 파일	파일시스템 ID	파일시스템 식별 ID
		이름	파일시스템 이름
		저장용량	파일시스템의 총 저장용량
		프로토콜	파일시스템에 접근하기 위한 네트워크 프로토콜(NFS, SMB 등)

구분	하위범주	속성	설명
클라우드	네트워크 - VPC	VPC ID	VPC 식별 ID
		이름	VPC 이름
		CIDR 블록	VPC 내 사용할 IP주소 범위
		서브넷	세그먼트 단위 (퍼블릭, 프라이빗 등)
		라우팅 테이블	네트워크 트래픽 경로
	네트워크 - 보안그룹	보안그룹 ID	보안그룹 식별 ID
		보안그룹 이름	보안 그룹 이름
		설명	보안 그룹의 목적과 용도 설명
		인바운드-프로토콜	트래픽 유형 지정 (TCP, UDP, ICMP 등)
		인바운드-포트범위	허용할 포트 번호 혹은 범위
		인바운드-소스	허용할 트래픽의 출발지 IP 주소 혹은 CIDR 블록
		아웃바운드-프로토콜	트래픽 유형 지정 (TCP, UDP, ICMP 등)
		아웃바운드-포트범위	허용할 포트 번호 혹은 범위
		아웃바운드-대상	허용할 트래픽의 목적지 IP 주소 혹은 CIDR 블록
	네트워크 – 로드밸런서	이름	로드밸런서 이름
		유형	로드밸런서 유형 (애플리케이션, 네트워크, 클래식 등)
		리스너 프로토콜	로드밸런서가 수신하는 프로토콜 (HTTP, HTTPS, TCP 등)
		리스너 포트	로드밸런서가 수신하는 포트 (80, 443 등)
		대상 그룹	대상유형 (인스턴스, IP주소, 함수 등)
기반 소프트웨어	운영체계, 미들웨어, DBMS, 시스템 관리	소프트웨어명	소프트웨어의 명칭
		라이선스 구분	라이선스 구분
		라이선스 수	소프트웨어 라이선스의 개수
		버전	설치 버전 정보
		Patch	Patch 정보

3) CI 명명 규칙 예시

○ 중분류 약어 - 도입년도 - 일련번호(시퀀스 5자리)

※ 예) ISVR-2024-00001

4) 구성 감사 계획

가. 구성 감사 계획(예시)

구분		시기	감사 대상
정기	반기	정기감사일	▪ 해당 기간 중 발생한 변경 사항 ▪ 그 외 샘플링 구성 항목
	연간	정기감사일	▪ 전체 구성 항목
비정기		CMDB 재구축	▪ 전체 구성 항목
		대규모 변경	▪ 해당 변경과 관련된 구성 항목

나. 감사 세부 내역(예시)

구분	내용
목적	▪ CMDB 정합성 향상
주기	▪ 반기별 (6월, 12월)
대상	▪ 각 업무별 관리 CI 샘플링 (5% 이상)
평가	▪ (불일치 CI 항목 수 ÷ 심사 대상 CI 항목 수) X 100
보고	▪ 운영기관 관리자, 담당자

5) 구성 관리대장(예시)

○ 구성 관리대장은 예시로 제시한 구성 분류 체계 및 관리 속성 범위를 기준으로 개별기관에서 관리 가능한 범위로 조정하여 사용한다.

6. 이벤트관리 절차서

가. 개요

1) 목적

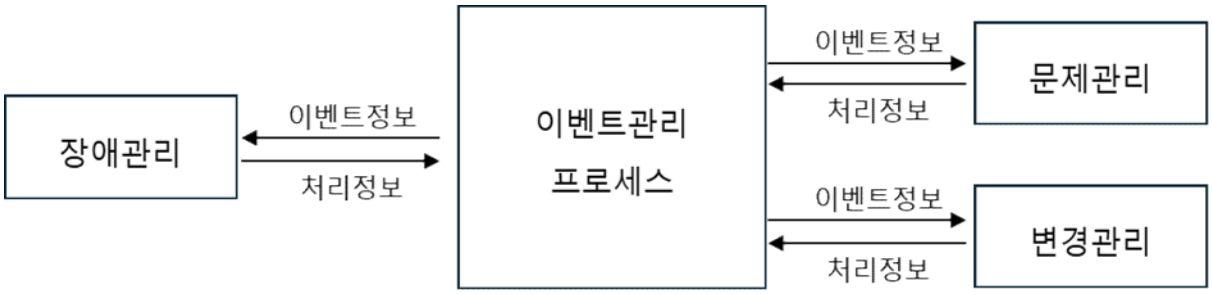
○ 이벤트관리는 정보시스템의 인프라, 클라우드 자원, 운영도구 등에서 발생하는 상태 변화, 임계치 초과, 오류 알림 등 운영 이벤트를 모니터링 도구 등을 통해 감지·분석하고, 조치 또는 관련 절차로 이관하여 장애 발생요소를 최소화하고 정보시스템의 안정적 운영을 지원하는 것을 목적으로 한다.

2) 적용 범위

○ 이벤트관리 절차는 행정·공공기관 정보시스템에서 발생하는 운영 이벤트의 감지, 접수, 검토, 분석, 조치 및 이관 업무에 적용한다.

3) 관련 업무 절차

○ 연관 선/후행 업무



○ 시작/종료/증적(Output) 조건

주요 업무	수행 업무
프로세스 시작 조건	이벤트 감지
프로세스 종료 조건	이벤트 이관 또는 처리
증적(Output)	이벤트 이력

나. 관리 정책

1) 정의

○ 정보시스템 표준운영절차의 운영에 있어서 필히 준수해야 할 정책 기준을 제공

2) 정책 기준

정책	설명	
정책 1	기준	정보시스템의 인프라에서 발생하는 운영 이벤트를 모니터링 자동화 도구 등을 통해 감지·관리하여야 한다.
	설명	○ 감지된 이벤트에 대해서 기록·점검 관리한다. ○ 이벤트 조치 사항은 그 완료 여부를 추적·확인하고, 관리시스템 또는 운영관리 도구를 통해 기록 관리한다.
정책 2	기준	감지된 이벤트의 처리를 위해 장애관리·변경관리·문제관리 등 관련 절차로 이관 필요시, 이벤트관리 프로세스는 이관 및 이관 이력관리의 책임을 가진다.
	설명	○ 발생 이벤트가 장애로 판단되는 경우 장애관리 프로세스로 이관 수행 ○ 발생 이벤트가 임계치 조정, 튜닝, 인프라 증설, 서비스 개선, 정책 변경 등 정보시스템의 변경 작업을 수행해야 하는 경우 변경관리 프로세스로 이관 수행 ○ 이벤트의 지속 모니터링이 필요하거나, 반복 발생, 원인불명, 잠재적 문제 위험이 식별되는 경우 문제관리 프로세스로 이관 수행

다. 용어 정의

용어	설명
이벤트	○ 정보시스템의 하드웨어 및 기반 소프트웨어, 클라우드 자원, 운영도구 등에서 발생하는 상태 변화, 임계치 초과, 오류 알림 등 감지 가능한 운영 상태를 말한다.
이관	○ 작업의 처리를 위해 관리자나 전문가 집단에게 처리를 넘기거나, 장애관리·변경관리·문제관리 등 관련 절차로 작업을 넘기는 활동 - 절차 내 처리를 위해 상위 또는 차선 담당자에게 작업을 이관하는 활동 포함
모니터링	○ 정보시스템의 하드웨어 및 기반 소프트웨어, 클라우드 자원, 운영도구 등의 운영 이벤트 발생 여부를 모니터링 도구 또는 육안 점검 등을 통해 확인하는 활동을 말한다.

라. 역할 및 책임

○ 이벤트관리 절차를 수행하는 역할자의 책임은 다음과 같다.

주요 업무		수행 업무	비고
운영기관 (정보시스템의 최종운영관리를 책임지는 기관)	관리자	○ 정보시스템 관련 담당자의 상위 책임자 또는 부서장 ○ 이벤트 처리 관련 의사결정	
	담당자	○ 이벤트 관련 대상 정보시스템의 담당자가 역할 수행 ○ 이벤트 처리 관련 이해당사자 간 조율 및 의사소통 창구 ○ 이벤트 조치의 적합 여부 검토 ○ 이벤트 분석(경향분석) 결과를 검토하여 문제관리, 변경관리 등의 활동에 대한 가이드	
수탁기관 또는 운영사업자	운영자	○ 운영기관과의 계약을 통해 정보시스템의 운영, 유지보수 및 요청 건의 처리 작업을 담당하는 수탁기관 또는 운영사업자 ○ 정보시스템을 구성하는 HW, SW, 미들웨어 등의 제조사 또는 유지보수 사업자와 협력하여 이벤트 분석 및 조치 수행 ○ 인프라, 운영도구 등에서 발생하는 운영 이벤트 모니터링 ○ 클라우드 인프라 환경 및 운영도구에서 발생하는 이벤트 모니터링 ○ 이벤트 분석 및 조치 수행 ○ 담당 구성요소에서 발생하는 이벤트의 기술 분석 및 조치 수행 ○ 이벤트 처리·조치·이관 이력 등록 및 관리 ○ 정기적 이벤트 경향분석 활동 수행	

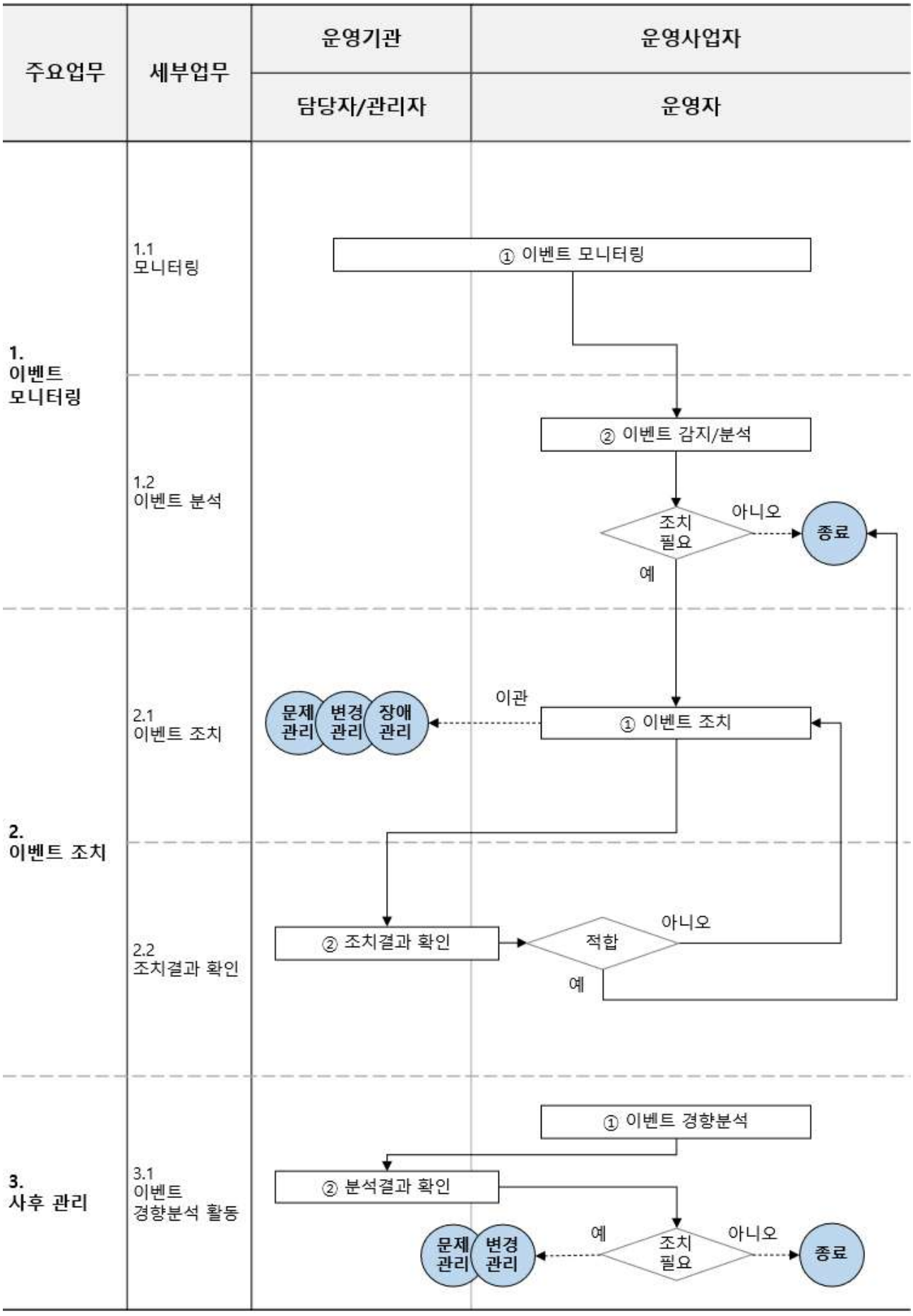
마. 표준절차 흐름도

○ 이벤트관리 절차는 아래와 같은 주요 업무와 수행절차들로 구성된다.

1) 주요 업무

주요 업무	세부 업무	수행 업무
1. 이벤트 모니터링	1.1 이벤트 모니터링	○ 정보시스템의 인프라, 클라우드 자원, 운영도구 등에서 발생하는 운영 이벤트를 모니터링 자동화 도구 및 육안 점검 등을 통해 감지·모니터링 한다. ○ 장애 징후 사전 감지를 위해 모니터링 도구의 임계치를 설정하고, 정보시스템 운영환경을 고려하여 최적화하여 관리한다.
	1.2 이벤트 분석	○ 감지된 이벤트는 관리시스템 또는 운영관리 도구에 접수·등록하고, 발생 원인, 영향도 및 장애 전환 가능성을 분석하여 장애, 오탐, 단순 이벤트 등으로 분류한다. ○ 오탐의 경우 이벤트를 종료할 수 있으며, 종료 사유를 기록·관리한다. ○ 이벤트가 장애로 판단되는 경우나, 변경 작업을 수행해야 하는 경우 해당 프로세스로 이관한다. - 타 프로세스 이관 시 해당 이벤트는 종료 처리 및 이벤트관리 절차에서 이관 이력을 기록하고, 이관된 프로세스에서 조치 또는 관련 작업을 수행한다.
2. 이벤트 조치	2.1 이벤트 조치	○ 조치가 가능한 이벤트에 대해 조치 작업을 수행한다. ○ 이벤트의 조치 내역을 기록하고 조치 결과에 대해 운영기관의 담당자에게 확인을 요청한다.
	2.2 조치 결과 확인	○ 운영기관 담당자는 이벤트의 조치 결과를 확인한다. - 조치 결과가 적합한 경우 해당 이벤트를 종료한다. - 조치 결과가 부적합한 경우 해당 이벤트에 대한 재조치를 요청한다.
3. 사후 관리	3.1 이벤트 경향분석 활동	○ 정기적인 이벤트 경향분석 활동을 통해 잠재적 문제 예방 활동을 수행한다. ○ 분석 활동을 통해 도출된 내용에 대해서는 운영기관 담당자 확인을 거쳐 조치를 위한 문제관리, 변경관리 프로세스 등으로 이관할 수 있다.

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	운영사업자
		관리자/담당자	운영자
1.1- ① 이벤트 모니터링	- 정보시스템의 인프라에서 발생하는 운영 이벤트를 모니터링 자동화 도구 및 육안 점검 등을 통해 감지·모니터링한다. - 모니터링 대상 이벤트는 기관별 운영하는 모니터링 툴 및 기관 환경에 따라 적용 가능하다. - 장애 징후 사전 감지를 위해 모니터링 도구의 임계치를 설정하고, 정보시스템 운영환경을 고려하여 연 1회 이상 최적화하여 관리한다. - 모니터링의 주 활동은 수탁기관 또는 운영자 측에서 진행하며, 필요시 운영기관 담당자도 모니터링 활동에 참여할 수 있다.	◑	●
1.2- ② 이벤트 감지/분석	- 모니터링을 통해 감지된 이벤트에 대해서 기록·분석하고, 조치를 위한 제반 활동을 수행한다. (관련 시스템 및 업무 담당자 협업) * 감지되는 이벤트의 등급 및 통보 기준은 각 기관별 관리 기준으로 정의하되, 이벤트의 중요도, 장애 유발 가능성 등을 기준으로 분류하여 관리한다. (Down, Critical, Major, Minor 등) - 이벤트가 사전 계획된 작업 또는 오탐으로 인한 경우 이벤트를 종료할 수 있으며, 종료 사유를 기록·관리한다. - 분석을 통해 조치가 필요한 이벤트는 담당자를 지정하여 조치 작업을 수행한다.		●

(●: 정, ◑: 부)

세부 절차	수행 내용	운영기관	운영사업자
		관리자/담당자	운영자
2.1- ① 이벤트 조치	- 이벤트 담당자는 발생 이벤트의 조치 활동을 수행하고, 조치 내역과 처리 결과를 관리시스템 또는 운영관리 도구에 기록·관리한다. - 이벤트의 조치를 위해 조치 담당자 재배정이 필요한 경우는 다른 담당자에게 이관하여 처리하고, 이관 내역을 기록·관리한다. (이벤트 조치 내역에 대해 운영기관 담당자 확인이 불필요하다고 판단되는 경우 해당 이벤트를 자체 검토 후 종료할 수 있다.) - 장애로 판단되는 이벤트는 장애관리로 이관하여 장애 프로세스에 따라 처리한다. - 이벤트 조치를 위해 정보시스템 구성요소의 변경이 필요한 경우에는 변경관리로 이관하여 처리한다. - 해당 이벤트가 반복 발생하거나 잠재적 문제 위험 또는 원인 불명이라고 판단되는 경우 문제관리로 이관하여 지속적인 관리를 수행한다. ※ 이벤트 처리 담당자 : 요청 내역에 따라 운영자 또는 운영기관이 될 수 있음		●
2.2- ② 조치 결과 확인	- 조치 결과 확인이 필요한 이벤트에 대해 운영기관 담당자는 이벤트 처리 결과를 확인한다. - 처리 결과가 적합한 경우 해당 이벤트를 종료하고, 적합하지 않은 경우 이벤트 조치 단계 활동을 재수행한다.	●	◑
3.1- ① 이벤트 경향분석	- 수탁기관 및 운영자는 발생한 이벤트에 대해 정기적으로 경향분석 활동을 수행하여 이벤트 추이 및 개선점을 도출하여 잠재적 문제에 대한 예방 활동을 수행한다. - 이벤트 경향분석의 결과는 운영기관 담당자의 검토를 통해 조치에 대한 방향을 결정한다.		●
3.1- ② 분석 결과 확인	- 운영기관 담당자는 이벤트 경향분석 결과를 확인한다. - 경향분석의 내용을 통해 잠재적 위험요소가 있는 문제 등에 대해서는 지속 관리를 수행하며, 해소 방안에 대해 수탁기관 및 운영자와 협의하여 관리를 수행한다. - 분석 활동을 통해 도출된 내용에 대해서는 운영기관의 담당자 확인을 거쳐 조치를 위한 문제관리, 변경관리 프로세스 등으로 이관할 수 있다.	●	◑

2) 고려사항

○ 모니터링 시스템의 필터링 기능을 사용할 경우 너무 많은 이벤트가 통보되거나 처리가 필요한 사항이 무시되지 않도록 사전 정의가 신중하게 이루어져야 한다.

○ 실시간 이벤트의 관리는 모니터링 시스템에 의해 대부분 자동으로 이루어지나, 문제가 발생할 경우 운영 담당자에 의해 수동으로 처리될 수 있다.

사. 핵심성과지표 (KPI : Key Performance Indicator)

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

※ 측정 주기는 기관의 운영환경 및 이벤트 발생 특성에 따라 조정할 수 있다.

측정 지표	측정 방법(예시)	측정 목적	측정 주기
이벤트 적기 처리율	(당일 처리된 이벤트 건수 / 당월 종료된 이벤트 건수) X 100	빠른 이벤트 처리	당월

※ 당일 기준: 이벤트 발생 시점에서 24시간(기관의 운영 정책 및 이벤트 유형에 따라서 적기 기준은 조정할 수 있음)

아. 수행 검증

1) 검증 방법

○ 검증 체크리스트의 체크 항목 기준(ITIL 표준 준용)으로 표준운영절차의 준수 여부와 이행 점검을 수행한다.

○ 개별기관 내 자체 프로세스 검증자는 내부 감사자의 자격 또는 ITIL에 대한 충분한 이해를 가진 자가 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
이벤트 모니터링	- 정보시스템의 안정적 운영을 위해 이벤트 모니터링 대상을 정의하고, 모니터링 자동화 도구를 적용하고 있습니까?	적합/ 부적합	• 이벤트 관리 대상/기준
	- 감지되는 이벤트에 대해서 기록·분석하고, 조치를 위한 제반 활동을 수행하고 있습니까?		• 모니터링 툴 또는 ITSM의 이벤트 관리 이력
	- 장애 징후 사전 감지를 위해 정보시스템별 모니터링 도구의 임계치를 설정하고, 최적화하여 관리하고 있습니까?		• 임계치 설정 기준 및 설정 내역 • 임계치 변경·최적화 이력 • 모니터링 도구 설정 증적
이벤트 조치	- 이벤트 조치를 위해 프로세스 이관이 필요한 경우 적절하게 이관 및 처리가 진행되고 있습니까?		• 이벤트 처리 이력 (ITSM 내 처리 이력 및 이관 이력)
	- 중요한 이벤트에 대해서 운영기관 담당자의 검토/확인을 수행하고 있습니까?		• 이벤트 처리 이력
사후 관리	- 잠재적 장애/문제 예방을 위해 이벤트에 대한 경향분석 등의 활동이 진행되고 있습니까?		• 경향 분석 이력
	- 경향분석의 내용을 통해 잠재적 위험요소가 있는 문제 등에 대해서는 문제관리 프로세스에 등록하여 지속적 관리가 수행되고 있습니까?		• 문제관리 이력

자. 관리 기준 및 예시

1) 장애 및 이벤트 판단 기준(예시)

(하기 항목은 예시 유형으로 참고용이며, 각 기관별 관리 가능한 기준으로 구분하여 적용)

구분	장애 관리	이벤트 관리
정의	- 정보시스템 서비스의 전부 또는 일부 기능이 계획되지 않은 정지 상태에 이르거나, 오동작, 기능 저하, 저장 정보의 손실 등으로 정상 기능을 수행하지 못하여 정상 서비스를 제공하지 못하는 상태	- 자동화 툴, 예방 점검 등을 통해 인프라에서 발생하는 상태 변화, 임계치 초과, 오류 알림 등 조치가 필요한 상황을 인지한 상태
상황	- 서비스 또는 HW·SW 기능 중단	- 인프라의 중단은 없으나 원활한 운영을 위해 신속한 증상 해소 필요
조치 절차	- 장애관리 절차로 수행	- 이벤트관리 절차로 수행

7. 서비스수준관리 절차서

가. 개요

1) 목적

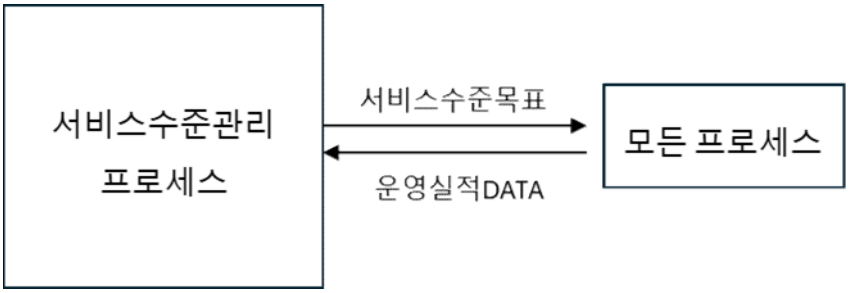
○ 서비스수준관리 절차는 행정·공공기관에서 제공하는 정보시스템 서비스를 대상으로 정보시스템 등급과 서비스 특성에 따른 서비스 목표수준 및 최소수준을 정의·합의하고, 정보시스템 운영사업자와 서비스수준협약을 체결하여 매월 서비스수준을 측정·평가·보고·개선함으로써 합의된 수준 이상의 IT 서비스 품질과 정보시스템 안정성을 확보하는 것을 목적으로 한다.

2) 적용 범위

○ 서비스수준관리 절차는 행정·공공기관 정보시스템을 대상으로 하며, 정보시스템 등급에 맞는 서비스 목표수준 설정, 서비스수준협약 체결, 서비스수준 측정·평가·보고, 개선조치 및 제재부과 관리에 적용한다.

3) 관련 업무 절차

○ 연관 선/후행 업무



○ 시작/종료/증적(Output) 조건

주요 업무	수행 업무
프로세스 시작 조건	서비스 수준 협약 작성 및 개정 시
프로세스 종료 조건	서비스 수준 협약 종료
증적(Output)	서비스 수준 협약서(SLA) 서비스 측정 항목(KPI) 정의서 서비스 운영실적보고서 월간 서비스수준 평가결과 서비스수준 미달 개선조치 내역 제재부과 기준 및 산정내역 종합평가 결과

나. 관리 정책

1) 정의

○ 정보시스템 표준운영절차의 운영에 있어서 필히 준수해야 할 정책 기준을 제공

2) 정책 기준

정책	설명	
정책 1	기준	서비스 수준 관리를 통하여 합의한 서비스 품질을 유지해야 한다.
	설명	○ SLA 적용 범위에 대해 운영기관과 운영자는 상호 합의하여야 한다. ○ 운영기관과 운영자는 제공되는 서비스의 품질 유지를 위해 상호 합의된 SLA를 체결하고 서비스 수준 관리 활동을 수행해야 한다. ○ 서비스 목표와 합의한 서비스 수준은 명확하게 정의되어야 한다. ○ 신규 서비스가 오픈되는 경우 서비스 수준에 대한 검토 및 평가가 수행되어야 한다.
정책 2	기준	서비스 품질 향상을 위한 지속적인 활동이 진행되어야 한다.
	설명	○ 서비스 목표 수준 및 SLA는 매년 실적 기반 재평가되어, 상호 협의 하에 변경되어야 한다. ○ SLA 변경을 통해 서비스 품질 향상을 위한 개선활동이 지속되어야 한다.
정책 3	기준	서비스 수준 관리 활동의 효과성 및 효율성을 검증하기 위하여 주기적인 평가가 수행되어야 한다.
	설명	○ SLA로 합의한 서비스는 계획된 주기(최소 1회/월)로 실제 실행 성과의 추이(trends) 분석 및 서비스 목표 대비 (달성)성과를 검토하여 부적합 또는 개선사항을 식별하고 합의된 서비스 목표를 지속적으로 달성할 수 있는 조치를 수행해야 한다. ○ SLA에 대한 모니터링 방법 및 성과 보고 주기 등은 명문화되어 관리되어야 한다.
정책 4	기준	서비스수준협약은「행정기관 및 공공기관 정보시스템 안정성 고시(행정안전부 고시 제2026-23호)」[별표 4]에 따라 정보시스템 등급에 맞는 서비스 목표수준과 최소수준을 포함하여 정보시스템 운영사업자와 체결·관리하여야 한다.
	설명	○ 운영기관은 정보시스템 등급과 서비스 특성을 고려하여 서비스수준 관리지표를 선정하여야 한다. ○ 서비스수준협약에는 서비스 대상 정보시스템, 서비스수준 측정 및 평가 방법, 목표수준, 최소수준, 보고주기, 역할과 책임, 위약사항 발생 시 조치방안이 포함되어야 한다. ○ 장애등급에 따른 가용률은 서비스수준협약에 반드시 포함하여야 할 필수지표로 관리하고 가중치는 30% 이상으로 설정, 그 외 선택지표는 정보시스템 운영 환경 및 서비스 특성에 따라 사업자와 협의하여 추가·변경 가능하다.

정책	설명	
정책 5	기준	서비스수준은 매월 평가·관리하고, 서비스수준 미달 및 장시간 장애 발생 시 위약금 기준을 마련·적용하여야 한다.
	설명	○ 운영자는 서비스수준협약에서 정한 관리지표별 실적을 월 단위로 측정하여 운영기관에 보고하여야 한다. ○ 운영기관은 월간평가 결과를 검토하고, 목표수준 또는 최소수준 미달 항목에 대하여 원인분석 및 개선조치를 요구하여야 한다. ○ 서비스수준 미달, 장시간 장애, 반복장애, 인적장애 등에 대해서는 서비스수준 협약에서 정한 위약금 기준에 따라 관리하여야 한다. ○ 종합평가는 평가기간의 월간평가 결과를 기준으로 산정하고, 평가등급에 따라 위약금 부과 여부를 검토하여야 한다.

다. 용어 정의

용어	설명
서비스 수준 협약서 (SLA: Service Level Agreement)	○ 정보시스템 서비스의 목표수준 관리를 위하여 운영기관과 정보시스템 운영사업자가 서비스 대상 정보시스템, 서비스수준 측정 및 평가, 목표수준, 최소수준, 위약사항 발생 시 조치방안 등에 관한 사항을 규정하여 체결하는 협약을 말한다.
서비스 카탈로그	○ 운영기관의 정보시스템을 통해 제공하는 서비스에 대한 목록과 특성을 기술한 문서이다. 서비스 목록에는 서비스의 범위와 종류가 포함되고 특성에는 해당 서비스의 속성과 특징 등을 포함한다.
서비스 수준 관리지표	○ 서비스 수준 협약서에서 정의된 서비스 항목의 품질 수준을 유지하고 측정·관리하기 위해 상호 협의된 관리지표(KPI)로 제공되는 서비스의 목표 수준 및 임계치 등으로 구성되어 있다.
임계치	○ 서비스의 측정 항목이 기준치 이하로 미달되는 것을 방지하기 위해 최저 수준 이상의 일정 값을 설정하는 것을 의미한다.
서비스 수준 검토 회의	○ IT서비스 수준에 대하여 주기별로 실적을 종합하여 보고하는 회의를 의미한다.
서비스 수준 관리 (SLM, Service Level Management)	○ 합의된 서비스 수준의 실행 및 유지를 담당하는 활동으로 서비스 수준 관리를 위한 항목 개발부터 운영, 리포팅, 개선에 이르는 일련의 서비스 수준 관리 행위를 말한다.
외부공급계약 (UC: Underpinning contract)	○ 운영자가 운영기관과 합의한 서비스 제공과 관련하여 외부 공급자와 체결한 계약을 의미한다.
목표수준	○ 서비스수준협약에서 정한 서비스 제공 목표값으로, 운영기관과 정보시스템 운영사업자가 달성하기로 합의한 서비스 품질 수준을 말한다.
최소수준	○ 서비스수준협약에서 정한 최소 허용 기준으로, 해당 기준 미달 시 개선조치 또는 제재부과 검토 대상이 되는 서비스 품질 수준을 말한다.
월간평가	○ 월 단위로 서비스수준 관리지표별 실적을 측정하고, 목표수준 및 최소수준 대비 달성 여부를 평가하는 활동을 말한다.
종합평가	○ 평가기간 전체의 월간평가 결과를 종합하여 서비스수준 달성 정도와 위약금 부과 여부 등을 판단하는 활동을 말한다.
위약금	○ 서비스수준 미달, 장시간 장애, 반복장애, 인적장애 등 서비스수준협약에서 정한 위약사항 발생 시 계약조건에 따라 부과하는 금액을 말한다.
장시간 장애	○ 장애등급별 장애조치 최대 허용시간을 초과한 장애를 말한다.

라. 역할 및 책임

○ 서비스수준관리 절차를 수행하는 역할자의 책임은 다음과 같다.

주요 업무		수행 업무	비고
운영기관 (정보시스템의 최종운영관리를 책임지는 기관)	관리자	○ 정보시스템 관련 담당자의 상위 책임자 또는 부서장, 기관장 ○ 서비스 수준 협약 관련 의사결정	
	담당자	○ 관리자가 지정한 정보시스템 관련 담당자가 역할 수행 ○ 서비스 수준 관리 제·개정을 위한 사용자 및 수탁기관, 운영사업자 간 조율과 의사소통 창구, 협상 관리 ○ 서비스 수준 관리 체계 구축 ○ 서비스 수준 월간 운영 실적에 대한 검토/평가 ○ 서비스 수준 개선 방안 검토 및 모니터링	
수탁기관 또는 운영사업자	운영자	○ 운영기관과의 계약을 통해 정보시스템 및 클라우드 환경에서의 정보시스템의 운영, 유지보수 및 서비스수준관리 업무를 담당하는 수탁기관 또는 운영사업자 ○ 정보시스템을 구성하는 HW, SW, 미들웨어 등의 제조사 또는 유지보수 사업자와 협력하여 서비스 운영 및 유지보수 업무 수행 ○ 서비스수준관리 제·개정을 위한 운영기관과의 조율 및 의사소통 창구 및 협상 관리 ○ 서비스 평가 기준에 따른 성과 측정 수행 ○ 외부공급업체가 제공하는 서비스에 대한 측정, 평가 및 관리 활동을 수행 ○ 월간 운영 현황·실적 보고서 작성, 검토 등 실무 수행 ○ 서비스 운영 성과에 대한 시정조치 활동 수행	

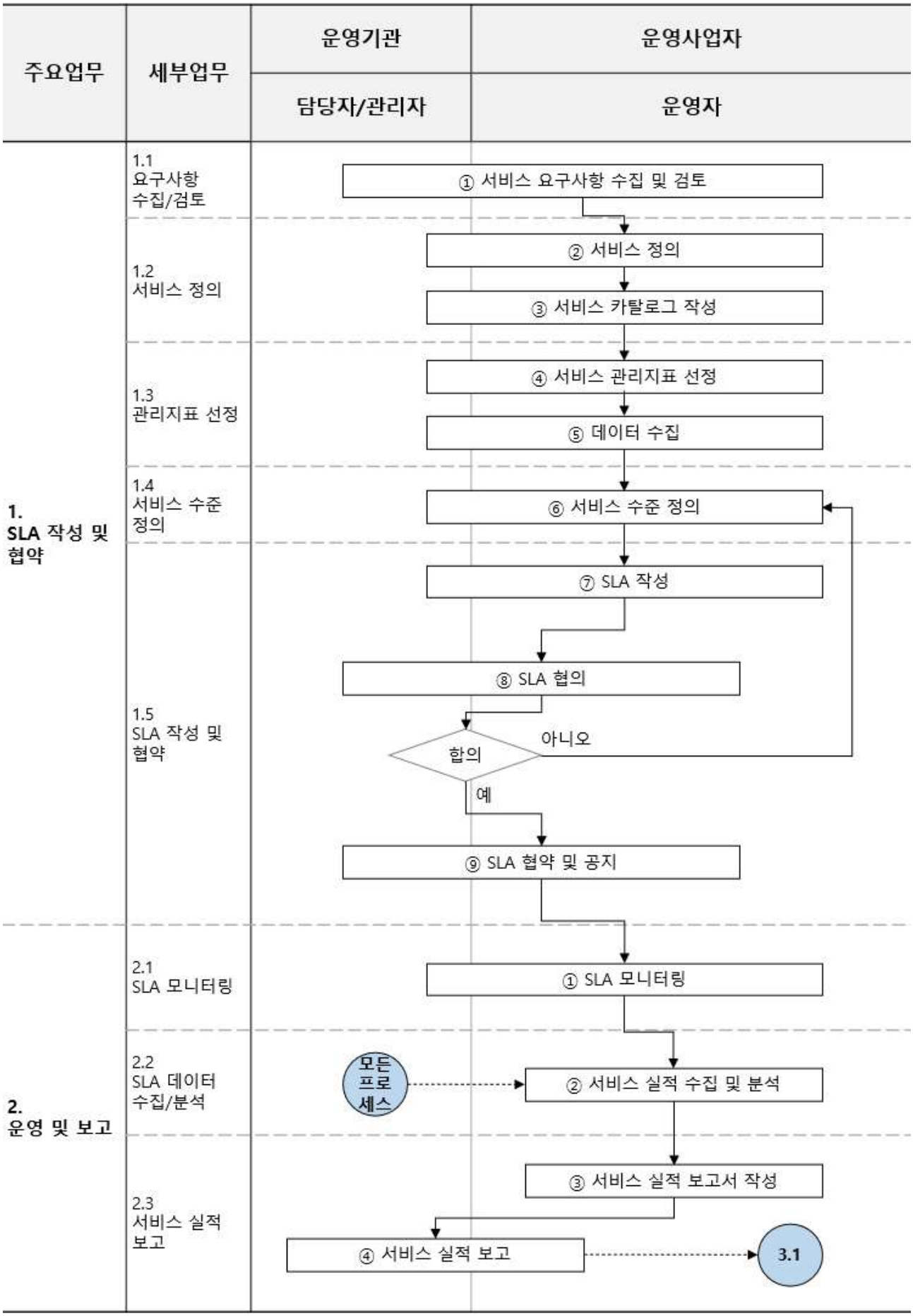
마. 표준절차 흐름도

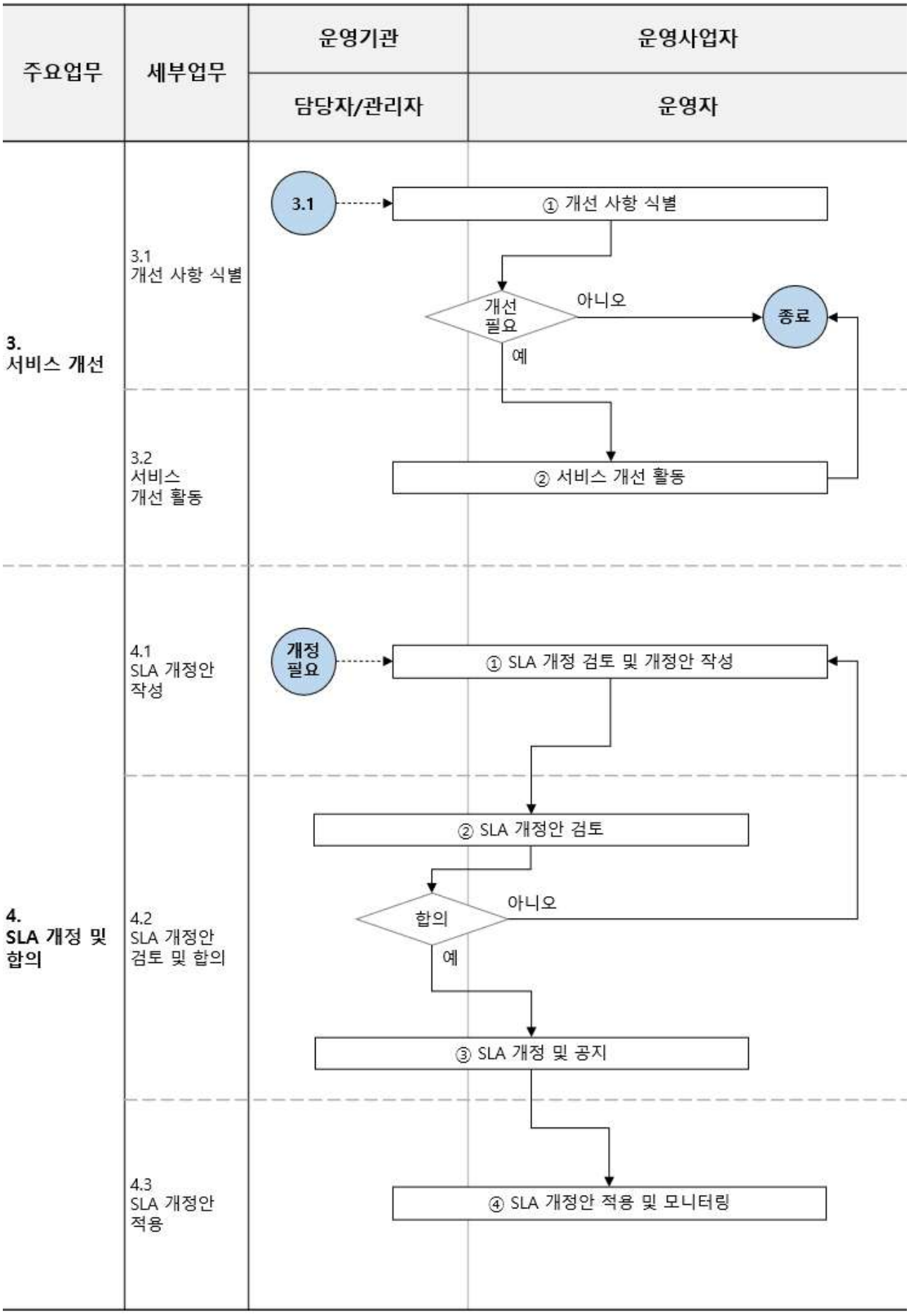
○ 서비스수준관리 절차는 아래와 같은 주요 업무와 수행절차들로 구성된다.

1) 주요 업무

주요 업무	세부 업무	수행 업무
1. SLA 작성 및 협약	1.1 요구사항 수집/검토	○ 행정·공공기관에서 제공하는 IT 서비스에 대한 특징, 서비스 시간 등을 조사하고, 사용자 및 운영부서의 서비스에 대한 요구사항을 수집하고 검토한다.
	1.2 서비스 정의	○ 운영기관 담당자는 운영자와 협업하여 적용대상 정보시스템 및 서비스 범위를 정의하고, 서비스 카탈로그를 작성한다.
	1.3 관리지표 선정	○ 서비스 수준을 객관적으로 측정할 수 있는 관리지표를 선정하고, 지표를 측정할 수 있는 데이터 수집 방안 등을 정의하여 실제 데이터를 수집한다. 이 경우 장애등급에 따른 가용률은 필수지표로 포함한다.
	1.4 서비스수준 정의서	○ 수집된 데이터 기반으로 정보시스템 등급, 운영환경 및 운영자의 역량, 요구수준 등을 고려하여 목표수준 및 최소수준을 협의·정의한다. (신규 지표일 경우 목표 수준은 상호 합의하에 임시로 설정하고 이후 축적된 데이터를 기반으로 최종 확정한다.)
	1.5. SLA 작성 및 협약	○ 협의를 통하여 정의된 적용대상, 적용기준, 관리지표, 목표수준, 최소수준, 평가주기, 역할 및 책임, 보상방안, 위약금 기준, 위약사항 발생 시 조치방안 등이 반영된 SLA를 작성하고 정보시스템 운영사업자와 협약을 진행한다.
2. 운영 및 보고	2.1 SLA 모니터링	○ 운영자는 체결된 SLA를 기반으로 제공하는 서비스에 대한 운영 수준을 모니터링한다.
	2.2 SLA 데이터 수집/분석	○ 운영자는 각 프로세스의 운영데이터 수집을 통해 서비스 수준 목표 대비 성과, 미준수 사항 및 이슈 등을 분석한다.
	2.3 서비스 실적 보고	○ 운영자는 제공된 서비스 실적에 대해 SLA 기준에 맞추어 월간 평가를 수행하고, 서비스 실적 보고서를 작성하고, 운영 보고 시 운영기관 담당자 및 이해관계자에게 보고한다.
3. 서비스 개선	3.1 개선 사항 식별	○ 운영기관 담당자와 운영자는 월간 서비스 성과 및 운영 보고회를 통하여 서비스 품질에 영향을 주는 문제나 이슈, 서비스수준 미달 항목 발견 시 이에 대한 개선 항목을 도출하고 정의한다. 서비스수준 미달 및 장시간 장애 등이 발생한 경우 SLA에서 정한 제재부과 기준에 따라 위약금 산정 여부를 검토하고, 제재부과 기준 및 산정 내역을 관리한다.
	3.2 서비스 개선 활동	○ 운영자는 개선 항목에 대한 개선 활동을 진행한다.
4. SLA 개정 및 합의	4.1 SLA 개정안 작성	○ 운영기관 담당자는 서비스 수준, 월간평가 결과, 종합평가 결과, 현실적 제약 사항 등으로 SLA의 개정이 필요한 경우 분석·검토를 통하여 개정안을 작성한다.
	4.2 SLA 개정안 검토 및 합의	○ 운영기관 담당자와 이해관계자 및 운영자는 작성된 SLA 개정안에 대하여 공식 절차를 통하여 검토 및 합의를 진행한다.
	4.3 SLA 개정안 적용	○ 운영기관과 운영자는 합의된 SLA 개정안을 준용하여 서비스수준관리 활동을 수행·모니터링한다.

2) 수행주체별 표준절차 흐름도




주요업무
세부업무
운영기관
운영사업자
담당자/관리자
운영자
3. 서비스 개선
3.1 개선 사항 식별
3.2 서비스 개선 활동
4. SLA 개정 및 합의
4.1 SLA 개정안 작성
4.2 SLA 개정안 검토 및 합의
4.3 SLA 개정안 적용
3.1
① 개선 사항 식별
개선 필요
아니오
종료
예
② 서비스 개선 활동
개정 필요
① SLA 개정 검토 및 개정안 작성
② SLA 개정안 검토
합의
아니오
예
③ SLA 개정 및 공지
④ SLA 개정안 적용 및 모니터링

바. 세부 수행 절차

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

(●: 정, ◑: 부)

세부 절차	수행 내용	운영기관	운영사업자
		관리자/담당자	운영자
1.1- ① 서비스 요구사항 수집 및 검토	- 운영기관 담당자는 운영자와 협업하여 사용자에게 제공되는 IT 서비스에 대하여 사용자 및 운영부서, 이해관계자와 회의, 인터뷰 등을 통하여 서비스에 대한 요구사항을 수집한다. - 요구사항은 제공하는 서비스와의 연관성, 서비스 품질 관련성, 실현 가능성 등을 검토하여 관리 가능한 범위로 선별한다.	●	◑
1.2- ② 서비스 정의	- 운영기관 담당자는 기관에서 제공하는 서비스에 대한 목록을 파악하고 해당 서비스 목록을 정의한다. 서비스 정의에는 적용대상 정보시스템, 서비스 대상, 업무명, 업무 중요도, 상세 내용, 제공 시간 등이 포함된다. - 서비스에 대한 정의 및 카탈로그 작성, 관리지표 선정 등의 작업은 운영자의 지원/협업을 통해 작업할 수 있다.	●	◑
1.2- ③ 서비스 카탈로그 작성	- 정의된 서비스를 토대로 서비스 카탈로그를 작성한다. 서비스 카탈로그는 서비스 정의 항목 외에 지원 연락처, 관련 조직, 주요 공급업체 및 연락처, 제약 사항, 기타 사항 등이 추가되어 리스트로 작성한다. ※ ITSM 시스템이 있을 경우는 ITSM 내 서비스 카탈로그 관리를 통하여 작성한다.	●	◑
1.3- ④ 서비스 관리지표 선정	- 운영기관 담당자는 기관에서 제공하는 서비스 수준을 객관적으로 측정할 수 있는 관리지표(KPI)를 도출한다. - 관리지표의 도출은 측정 가능한 지표로 도출되어야 하며, 장애등급에 따른 가용률은 필수지표로 포함하고 그 외 선택지표는 운영자와 협의를 통해 상호 관리 가능한 지표를 도출하도록 한다. - 관리지표 선정 시에는 지표에 대한 산출 공식, 데이터 수집 방법 및 측정 기준, 측정 주기 등을 명확히 정의한다.	●	◑
1.3- ⑤ 데이터 수집	- 운영기관 담당자는 운영자와 협업하여 선정된 관리지표의 적합성을 확인하기 위한 정량화된 데이터를 측정/수집한다. - 데이터의 수집은 운영자와 협업하여 특정 기간 및 실제 서비스 실적 데이터를 기반으로 수행한다.	●	◑

(●: 정, ◑: 부)

세부 절차	수행 내용	운영기관	운영사업자
		관리자/담당자	운영자
1.4- ⑥ 서비스 수준 정의	- 운영기관 담당자는 실측 결과를 바탕으로 정보시스템 등급, 운영환경, 운영자 역량, 사용자 요구수준 등을 고려하여 목표수준 및 최소수준을 정의한다. - 목표 수준에 대해서는 운영자와 상호 협의하여 적합하고 제공 가능한 수준으로 정의되어야 한다. - 신규 서비스의 경우는 실적 데이터 및 서비스 수준 측정 기간을 가지기 어려우므로 목표 수준과 최소 허용 수준을 운영기관과 운영자 간 상호 합의에 의하여 임시로 설정하고, 이후 축적된 데이터에 근거하여 변경 적용을 수행할 수 있다.	●	◑
1.5- ⑦ SLA 작성	- 운영기관 담당자는 적용대상, 적용기준, 서비스 제공범위, 서비스 시간, 서비스 내역, 관리지표, 목표수준, 최소수준, 역할 및 책임, 평가주기, 보고양식, 보상방안, 위약금 기준, 위약사항 발생 시 조치방안 등이 포함된 서비스 수준 관리(SLA) 문서를 작성한다.	●	◑
1.5- ⑧ SLA 협의	- 운영기관 담당자는 작성된 서비스 수준 관리(SLA) 문서에 대하여 이해관계자를 포함하여 운영자와 협의를 진행한다. - 협의 과정에서는 SLA에 포함된 적용대상, 적용기준, 서비스 제공범위, 관리지표, 목표수준, 최소수준, 측정·평가 방법, 평가주기, 역할 및 책임, 보상방안, 위약금 기준, 위약사항 발생 시 조치방안의 적정성을 검토한다. - 상호 협의 단계에 서비스수준 및 관리지표, 기타 조건 등에 대한 합의가 이루어져야 하며, 불일치되는 부분이 발생하는 경우 해당 부분의 상호 합의가 이루어질 수 있도록 이전 단계를 재수행하여 보완 및 합의 활동을 수행한다.	●	◑
1.5- ⑨ SLA 협약 및 공지	- SLA 문서에 대한 협의/검토를 통해 내용에 문제가 없을 경우 운영기관 관리자(기관장) 및 운영자 대표자의 서명을 통해 공식적인 협약을 진행한다. - 합의된 서비스 수준 관리(SLA) 문서에 변경이 필요할 경우는 '4.SLA 개정 및 합의' 프로세스에 따라 진행한다. - 협약 후 운영기관 담당자는 공식적으로 SLA가 체결되었음을 공지하여 관련 이해관계자들이 인지할 수 있도록 한다.	●	◑

(●: 정, ◑: 부)

세부 절차	수행 내용	운영기관	운영사업자
		관리자/담당자	운영자
2.1- ① SLA 모니터링	- 운영자는 체결된 SLA를 기반으로 서비스 수준을 모니터링하며 도출되는 이벤트/이슈 등에 대해서는 운영기관 담당자와 공유한다. - 운영기관 담당자도 SLA에 기반한 서비스의 운영 수준을 지속적으로 모니터링한다.	◑	●
2.2- ② 서비스 실적 수집 및 분석	- 운영자는 SLA를 기반으로 제공하는 서비스에 대한 운영 실적 산출에 필요한 데이터가 정해진 주기에 따라 산출되는지 확인하고, 산출된 데이터를 측정, 검토·분석하여 서비스 수준 현황을 분석한다. 이때 서비스수준협약에서 정한 장애등급에 따른 가용률 등 서비스수준 관리지표를 기준으로 목표수준 및 최소수준 대비 실적을 분석한다. - 운영자는 서비스 수준 현황 및 운영데이터(각 프로세스 이벤트, 이슈, 운영 실적, 성능/용량 분석, 가동률 등)의 수집을 통해 서비스 수준 목표 대비 성과, 미준수 사항, 이슈 등을 분석하고, 운영기관 담당자와 공유 및 협의한다.	◑	●
2.3- ③ 서비스 실적 보고서 작성	- 운영자는 분석된 데이터를 근간으로 서비스 수준에 대한 실적 보고서를 작성한다. - 보고서는 다음 내용을 포함한다. . 시스템 운영 현황 . 서비스 요청 현황 (요청, 변경 등) . 장애 현황 및 조치 결과 . 서비스 수준 측정 결과 · 관리지표별 목표수준 및 최소수준 대비 달성 여부 · 월간평가 결과(평가점수, 환산점수, 합산점수) · 서비스수준 미달 항목 및 개선 필요사항 . 주요 자원 분석 결과 (인프라, 클라우드 등) . 이슈 및 리스크 현황 . 만족도 결과 및 불만족 사항 등 - 작성된 보고서는 운영기관 담당자와 사전 검토를 통해 미흡한 사항에 대해서는 시정 조치를 하도록 한다.	◑	●

2.3- ④ 서비스 실적 보고	- 운영자는 작성된 서비스 실적 보고서를 운영기관 담당자/관리자 및 이해관계자에게 보고한다. 보고 방식은 개별기관의 상황에 따라 조정될 수 있다. - 운영기관 담당자는 서비스 실적보고를 통해 장애등급에 따른 가용률 등 필수지표와 SLA에서 선정한 선택지표 등 서비스수준협약 관리지표별 운영실적을 확인하고, 월간평가 결과와 목표수준·최소수준 달성 여부를 검토하여 미달사항 및 개선 필요사항을 서비스 개선 활동과 연계하여 관리한다. - 운영기관 담당자는 서비스 실적 보고를 통해 운영되는 서비스의 이슈/이벤트 및 주요 현황을 파악하고 운영상의 개선 포인트를 도출하여 지속적인 관리가 수행될 수 있도록 서비스 개선 활동과 연계하여 관리하여야 한다. - 합의된 SLA 수준 및 실제 운영되는 서비스 실적 등에 대해서 주기적으로(분기 혹은 반기) 서비스 수준 적합성에 대한 검토 회의를 진행한다. 서비스 검토 회의는 운영기관 담당자/관리자 및 실제 사용자와 이해관계자, 운영사업자 등이 참석하여 서비스 수준의 유지 및 개선에 필요한 활동을 도출하거나 목표수준 조정 등의 사항을 검토한다.	●	●

(●: 정, ◑: 부)

세부 절차	수행 내용	운영기관 관리자/담당자	운영사업자 운영자
3.1- ① 개선 사항 식별	- 운영자는 월간 서비스 성과, 서비스 검토회의 등을 통하여 확인된 문제점, 이슈사항 및 서비스수준 미달 항목에 대하여 개선 사항을 도출하고, 정리하여 운영기관 담당자에게 보고한다. - 개선사항은 서비스 실적보고에 포함되어 진행할 수 있다. - 운영기관 담당자는 운영자의 개선사항 식별 이외에도 운영 모니터링 및 사용자의 요구사항에 기반한 개선사항을 식별하여 운영자와 협의를 진행한다. - 주요 개선 대상은 아래와 같다. . 서비스 수준 미충족 항목 . 서비스 불만 사항 . 서비스 개선 요구 . 중복 장애 등 - 운영기관 담당자는 식별된 내용을 검토하고 개선 여부를 판단한다. - 서비스수준 미달, 장시간 장애, 반복장애, 인적장애 등 위약사항이 발생한 경우 운영기관 담당자는 서비스수준협약에서 정한 위약사항 조치기준에 따라 위약금 산정 여부를 검토하고, 위약금 산정 내역 및 조치 결과를 관리한다. - 운영자는 월간평가 결과, 장애시간, 지체시간, 장애등급 등 산정에 필요한 자료를 제공한다.	◑	●
3.2- ② 서비스 개선 활동	- 운영기관 담당자는 식별된 개선 활동이 적절하게 수행될 수 있도록 리소스, 스케줄 등을 고려하여 담당자를 선임하고, 개선에 대한 이행을 요청한다. - 운영자(개선담당자)는 개선 필요 항목에 대한 활동 계획을 수립하고 실행하며 서비스수준 미달 항목에 대한 원인분석 및 개선조치 결과를 운영기관 담당자에게 공유한다. - 운영기관 담당자는 서비스 개선 방안의 실행 결과가 의도했던 성과를 가져왔는지를 검토 및 분석하고, 성과 미달성 시 해당 원인을 분석한 후, 추가 개선 활동을 수행한다. - 서비스 개선 활동을 통하여 SLA 변경이 필요할 경우 '4.SLA 개정 및 합의' 프로세스를 수행한다.	●	●

(●: 정, ◑: 부)

세부 절차	수행 내용	운영기관	운영사업자
		관리자/담당자	운영자
4.1- ① SLA 개정 검토 및 개정안 작성	- 운영기관 담당자 및 운영자는 서비스 운영 및 모니터링을 통해 기정의된 서비스 수준 목표가 비합리적이거나 달성 과정에 심각한 문제가 발생한 경우 혹은 업무가 추가되거나, 업무 변경, IT 환경 변화 등이 발생했을 경우에 SLA 개정 필요에 대한 데이터를 수집하고 검토를 진행한다. - SLA 개정이 필요하다고 판단될 경우 이해관계자에게 개정의 필요성을 공유하고 개정안을 작성한다. - 개정안에는 아래와 같은 내용을 포함한다. · SLA 개정 필요 사유 (검토회의 결과, 분석 결과 등) · 신규·삭제되는 서비스 내역 · 변경되는 지표 및 목표값 · 제안 사항 및 의견 등	●	◑
4.2- ② SLA 개정안 검토	- 운영기관 담당자는 작성된 서비스 수준 관리(SLA) 개정안에 대하여 이해관계자 협의를 진행한다. - 협의 과정을 통해 변경될 서비스 수준 내용에 대하여 적절성, 타당성 등을 검토한다. - 개정되는 서비스 수준 관리(SLA) 문서에 상호 이슈가 없을 경우 운영기관 관리자 및 운영자 대표자의 서명을 날인한다. - 상호 협의 단계에 개정 내용, 기타 조건 등에 대한 합의가 이루어져야 하며, 불일치되는 부분이 발생하는 경우 해당 부분의 상호 합의가 이루어질 수 있도록 이전 단계를 재수행하여 보완 및 합의 활동을 수행한다.	●	◑
4.2- ③ SLA 개정 및 공지	- SLA 개정안에 대한 상호 합의가 진행된 경우 운영기관 담당자는 공식적으로 SLA가 개정되었음을 공지하여 관련 이해관계자들이 인지할 수 있도록 한다.	●	◑
4.3- ④ SLA 개정안 적용 및 모니터링	- 운영기관 담당자 및 운영자는 합의된 개정안에 따라 서비스 수준 관리 활동이 진행될 수 있도록 관리하며, 운영 상황에 대한 지속적인 모니터링을 수행한다.	●	●

사. 핵심성과지표 (KPI : Key Performance Indicator)

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

측정 지표	측정 방법(예시)	측정 목적	측정 주기
서비스 수준목표 달성률	∑(지표별 배점 X 지표별 달성도)	서비스 수준 달성	당월

아. 수행 검증

1) 검증 방법

○ 검증 체크리스트의 체크 항목 기준(ITIL 표준 준용)으로 표준운영절차의 준수 여부와 이행 점검을 수행한다.

○ 개별기관 내 자체 프로세스 검증자는 내부 감사자의 자격 또는 ITIL에 대한 충분한 이해를 가진 자가 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
SLA 작성 및 협약	- SLA에 대한 서비스 대상이 정의되어 있으며, 관리 정보가 서비스 목록(카탈로그)로 반영되어 있습니까?	적합/ 부적합	• SLA • 서비스 카탈로그
	- 평가지표는 서비스에 대한 목표수준, 최소수준의 적정성이 점검되었으며, 적절한 수준으로 설정되어 있습니까?		• SLA 평가지표
	- 서비스수준협약서(SLA)는 서비스 적용대상, 의무사항, 서비스 수준 기준, 서비스 수준 측정/평가/보고의 내용이 포함되어 있습니까?		• SLA
	- SLA에서 정의한 목표수준을 충족하기 위해 서비스 제공자는 서비스를 지원하는 협력업체/벤더와 SLA에 준하는 합의(UC)가 정의되고 운영되고 있습니까?		• UC
운영 및 보고	- SLA 실적에 대한 평가/보고가 주기적으로 평가되고 보고되고 있습니까?		• SLA 실적보고서
	- SLA 보고서에는 목표 대비 성과, 미준수 사항, 개선 필요사항 등이 분석되고 관리되고 있습니까?		• SLA 실적보고서
서비스 개선	- SLM 운영결과 서비스 개선활동이 필요하다고 판단되는 경우 개선 계획이 수립되고, 이행되고 있습니까?		• 개선활동 이력
	- SLM을 통하여 실질적으로 서비스 품질이 향상되고 있습니까?		-
SLA 개정 및 합의	- SLA 실적 데이터를 기반으로 서비스 품질 개선을 위한 SLA 개정 활동이 진행되고 합의되고 있습니까?		• SLA 개정 이력

자. 관리 기준 및 예시

1) 서비스 지표정의서 양식 (예시)

구 분	내 용
지표 명	도출된 지표명을 기재
정 의	지표에 대한 설명
측정산식	해당 지표의 측정값을 산출하기 위한 계산식으로 측정산식과 각 항목에 대한 정의가 포함되어야 함
평가점수	산출된 측정값이 사전 정의된 SLA 평가점수에 어떻게 대응되는지를 보여주는 기준 ※ 목표수준, 기대수준, 최소허용수준 등
측정방법	*예. ITSM 등의 측정시스템 또는 모니터링 시스템* ※ 이용기관과 사업자가 협의하여 측정방법 및 측정도구(시스템 또는 수기) 등을 기재한다.
특이사항	평가지표 관리/산출을 위한 고려사항, 예외사항 등을 기술

2) 서비스수준협약 개정요청서 (예시)

<table>
<tr><td>계 약 명</td><td colspan="2"></td><td>요청기관</td><td></td></tr>
<tr><td>요 청 인</td><td colspan="2">부서: 성명:</td><td>요청일자</td><td></td></tr>
<tr><td>개정
요청사유</td><td colspan="4"></td></tr>
<tr><td rowspan="2">개정요청
내용</td><td colspan="2">개 정 전</td><td colspan="2">개 정 후</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td>검토의견</td><td colspan="4"></td></tr>
<tr><td>검토결과</td><td colspan="2">□개정 □추가검토 □의견반려</td><td>개정일정</td><td></td></tr>
<tr><td>검토자</td><td colspan="4">부서 : 성명 :</td></tr>
</table>

8. 백업관리 절차서

가. 개요

1) 목적

○ 장애 또는 재해 상황 발생 시 정보시스템 운영 데이터의 복구 가능성을 확보하고, 재해복구 및 백업체계의 구축·운영을 통한 정보시스템의 안정성·신뢰성을 제고하는 것을 목적으로 한다. 이를 위해 정보시스템의 특성에 맞는 백업관리체계를 구축·운영하고, 백업 정책에 따라 운영 데이터를 정기적으로 백업하며, 백업 결과 확인 및 이행 증적 관리를 통하여 백업 관리 절차가 지속적으로 이행될 수 있도록 한다.

- 데이터 변조·손실 방지 : 장애 또는 재해 상황 발생 시 데이터 복구가 가능하도록 백업 관리체계를 구축·운영한다.
- 서비스 연속성 확보 : 데이터 손실 시 백업 데이터를 활용하여 정보시스템 운영 및 서비스 중단 영향을 최소화한다.
- 재해 상황 대응 : 재해 상황 발생 시에도 백업 데이터의 안정성을 확보할 수 있도록 백업 데이터를 원격지 저장소에 주기적으로 소산한다.
- 백업 결과 신뢰성 확보 : 백업 수행 후 백업 정상 완료 여부, 데이터 무결성 등 백업 결과를 점검·확인한다.
- 백업 복구 훈련 : 백업 데이터의 정상 여부 및 복구 역량 강화를 위해 백업 데이터 복구 훈련을 실시한다.

2) 적용 범위

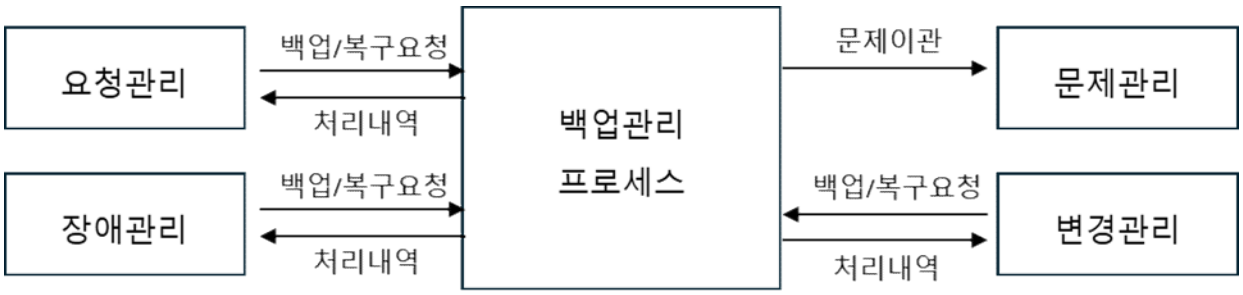
○ 백업관리 절차는 행정·공공기관의 정보시스템 운영관리에 적용한다.

구분	범위
서버	○ 운영체계(OS 데이터)와 애플리케이션 데이터 ○ 데이터베이스와 파일시스템 ○ 서버 구성 파일과 로그 파일
가상화 환경	○ 가상 머신(VM) 전체 ○ VM 설정과 구성 파일 ○ 가상화 호스트와 클러스터 구성
데이터베이스	○ 관계형 데이터베이스 (MS SQL, MySQL, Oracle, PostgreSQL 등) ○ NoSQL 데이터베이스 (MongoDB 등) ○ 트랜잭션 로그 및 데이터베이스 스키마

구분	범위
네트워크 장비	○ 라우터, 스위치, 방화벽 등 구성 데이터 ○ 네트워크 설정과 정책 데이터
사용자 계정	○ 사용자 프로필 및 계정 정보 데이터 ○ 사용자 환경 설정 데이터
기타	○ 중요 문서 및 파일 ○ 아카이브 데이터 ○ 시스템 로그 및 감사 로그

3) 관련 업무 절차

○ 연관 선/후행 업무



○ 시작/종료/증적(Output) 조건

주요 업무	수행 업무
프로세스 시작 조건	백업 대상 확인 및 정책 수립 백업/복구 요청
프로세스 종료 조건	정책 수립 완료 모의 훈련 완료 백업/복구 완료
증적(Output)	백업 정책 백업/복구 대장 복구 계획서 모의 훈련 계획 및 결과 보고서

나. 관리 정책

1) 정의

○ 정보시스템 표준운영절차의 운영에 있어서 필히 준수해야 할 정책 기준을 제공

2) 정책 기준

정책	설명	
정책 1	기준	정보시스템의 안정적 운영과 장애 또는 재해상황 발생 시 데이터 복구를 위하여 백업관리체계를 구축·운영하고, 백업 정책을 수립·관리하여야 한다.
	설명	○ 백업 정책에는 백업대상, 백업방법, 백업주기, 백업 데이터 보관기간, 데이터 복구 시점목표(RPO) 및 그 밖에 백업 정책 수립에 필요한 사항이 포함되어야 한다. 또한 백업 대상을 반기 1회 이상 현행화하여 관리하여야 하며, 백업정책 수립 시 "붙임 1. 백업 정책 기준"을 참조한다. ○ 백업시스템, 저장매체, 소산 복구 수행 환경 등 백업환경을 구축·관리하여야 한다.
정책 2	기준	백업 정책에 따라 정기적으로 백업이 수행되고, 그 결과가 확인되어야 한다.
	설명	○ 정보시스템의 운영 데이터는 백업 정책에 따라 정기적으로 백업하여야 한다. ○ 백업 수행 후 백업 정상 완료 여부, 데이터 무결성 등 결과를 점검 및 확인하여야 한다. ○ 백업 실패, 지연, 오류 등 이상사항이 확인된 경우 원인을 확인하고 필요한 조치를 수행하여야 한다. ○ 백업 결과 확인 내역은 일정 기간 보관하여야 한다.
정책 3	기준	백업 데이터는 재해상황에 대비하여 원격지에 소산되어야 한다.
	설명	○ 원격지 저장소는 정보시스템과 동일한 재해상황에 동시에 영향을 받지 않는 장소여야 한다. ○ 원격지 소산은 온라인 또는 오프라인 방식으로 수행할 수 있다. ○ 원격지 소산 수행 결과는 이력으로 기록·관리하여야 한다.
정책 4	기준	백업 데이터의 정상 여부 점검 및 백업 복구 역량 강화를 위하여 백업 데이터 복구 훈련을 연 1회 이상 실시하여야 한다.
	설명	○ 다수의 정보시스템을 동일 운영환경 및 백업환경에서 통합 관리하는 경우에는 운영환경 및 백업환경별 1개 이상 정보시스템을 대상으로 훈련을 실시할 수 있다. ○ 소산 데이터 복구 훈련을 실시한 경우에는 백업 복구 훈련을 실시한 것으로 갈음할 수 있다. ○ 훈련 결과는 기록하고, 개선이 필요한 사항은 개선계획을 수립하여 관리하여야 한다.
정책 5	기준	백업관리 이행 증적은 기록·관리되어야 한다.
	설명	○ 백업 결과 확인 내역, 백업관리체계 점검 결과, 개선계획 등을 기록하여 관리하여야 한다. ○ 백업관리 절차의 수행 결과는 이행 증적으로 관리하여야 한다.

다. 용어 정의

용어	설명
백업	○ 정보시스템 장애, 재해 또는 데이터 손상 등에 대비하여 운영 데이터를 별도의 저장매체 또는 저장소에 복사·보관하는 행위를 말한다.
복구	○ 장애, 사고, 재해 또는 데이터 훼손 등이 발생한 경우 백업 데이터를 활용하여 정보시스템 또는 데이터를 정상 상태로 되돌리는 행위를 말한다.
백업대상	○ 백업을 수행하여야 하는 정보시스템, 운영 데이터, 데이터베이스, 파일, 가상머신, 컨테이너, 설정 정보 등을 말한다.
백업환경	○ 백업 수행 및 복구를 위하여 구축·운영하는 백업시스템, 저장매체, 소산 복구 수행 환경 등을 말한다.
백업 정책	○ 백업대상, 백업방법, 백업주기, 백업 데이터 보관기간, 데이터 복구시점목표(RPO) 및 그 밖에 백업 수행에 필요한 기준을 정한 정책을 말한다.
백업관리체계	○ 장애 또는 재해상황 발생 시 데이터 복구를 위하여 백업 정책 수립, 백업 수행, 백업 결과 확인, 소산, 복구 훈련 및 이행 증적 관리를 체계적으로 수행하기 위한 관리체계를 말한다.
소산	○ 재해상황 발생 시에도 백업 데이터의 안정성을 확보하기 위하여 백업 데이터를 원격지 저장소에 주기적으로 이관·보관하는 행위를 말한다.
시스템 백업	○ 운영체제, 시스템 설정 파일, 시스템 로그 등 정보시스템 운영에 필요한 시스템 영역을 백업하는 것을 말한다.
데이터베이스 백업	○ 관계형 데이터베이스 및 관련 데이터 파일, 컨트롤 파일, 변경 로그 파일 등을 백업하는 것을 말한다.
데이터 백업	○ 시스템 백업 및 데이터베이스 백업을 제외한 개발자 소스 파일, 응용프로그램 파일, 데이터 관련 파일 등 모든 파일에 대한 백업을 의미한다.
백업 장비	○ 백업 수행을 위하여 필요한 백업시스템, 저장매체, 백업 라이브러리, 네트워크 및 기타 물리적·논리적 구성요소를 말한다.
백업 구성 방식	○ 백업시스템을 구성하는 방식으로, 백업 대상과 백업시스템 간 연결 구조 및 백업 데이터 전송 방식을 말한다. (백업 솔루션을 구분하기 위해 크게 로컬(다이렉트) 백업, 네트워크 백업, SAN(Storage Area Network)으로 나누어지며 백업 규모, 시간 및 특성에 따라 그 구성 방식이 결정된다.)
백업 데이터 복구 훈련	○ 백업 데이터의 정상 여부 점검 및 백업 복구 역량 강화를 위하여 백업 데이터를 활용하여 복구 가능 여부를 확인하는 훈련을 말한다.
소산 데이터 복구 훈련	○ 원격지 저장소에 소산된 백업 데이터를 활용하여 복구 가능 여부를 확인하는 훈련을 말한다.
복구시간목표 (Recovery Time Objective)	○ 재해, 장애 등으로 정보시스템 서비스가 중단된 시점부터 핵심 기능을 복구하여 정상 여부를 확인하기까지의 목표 시간을 말한다.
복구시점목표 (Recovery Point Objective)	○ 장애 또는 재해 발생 시 복구하여야 하는 데이터의 목표 시점을 말한다. (허용할 수 없는 데이터 시점이 있다면 반드시 그 시점마다 백업이 이루어져야 한다.)
백업 최대허용시간	○ 백업 수행으로 인한 운영 영향 및 백업 가능 시간을 고려하여 백업 작업이 완료되어야 하는 최대 허용시간을 말한다.

라. 역할 및 책임

○ 백업관리 절차를 수행하는 역할자의 책임은 다음과 같다.

주요 업무		수행 업무	비고
운영기관 (정보시스템의 최종운영관리를 책임지는 기관)	관리자	○ 정보시스템 관련 담당자의 상위 책임자 ○ 백업 정책 및 백업/복구 승인 관련 의사결정	
	담당자	○ 백업/복구 대상 정보시스템의 담당자가 역할 수행 ○ 백업/복구 대상 정보시스템 및 데이터 검토 ○ 백업 정책, 복구 모의훈련 계획, 백업/복구 관련 이해당사자 간 조율 및 의사소통 창구 ○ 백업/복구 정책, 복구 모의훈련 계획의 적정 여부 검토 ○ 백업/복구 활동 및 결과의 적정 여부 검토	
수탁기관 또는 운영사업자	운영자	○ 운영기관과의 계약을 통해 정보시스템 및 클라우드 환경에서의 정보시스템의 운영과 백업/복구 작업을 담당하는 수탁기관 또는 운영사업자 ○ 백업 정책, 복구 모의훈련 계획, 백업/복구 관련 이해당사자 간 조율 및 의사소통 창구 - 수탁기관 및 운영사업자 간 유기적 협조 체계 관리 ○ 백업 정책, 복구 모의훈련 계획의 적정 여부 검토 ○ 백업/복구 활동 및 결과의 적정 여부 검토 ○ 백업 정책 수립, 복구 모의 훈련, 백업, 복구 관련 제반 준비 작업 ○ 백업 모니터링, 모의 훈련, 백업 및 복구 작업 수행	

마. 표준절차 흐름도

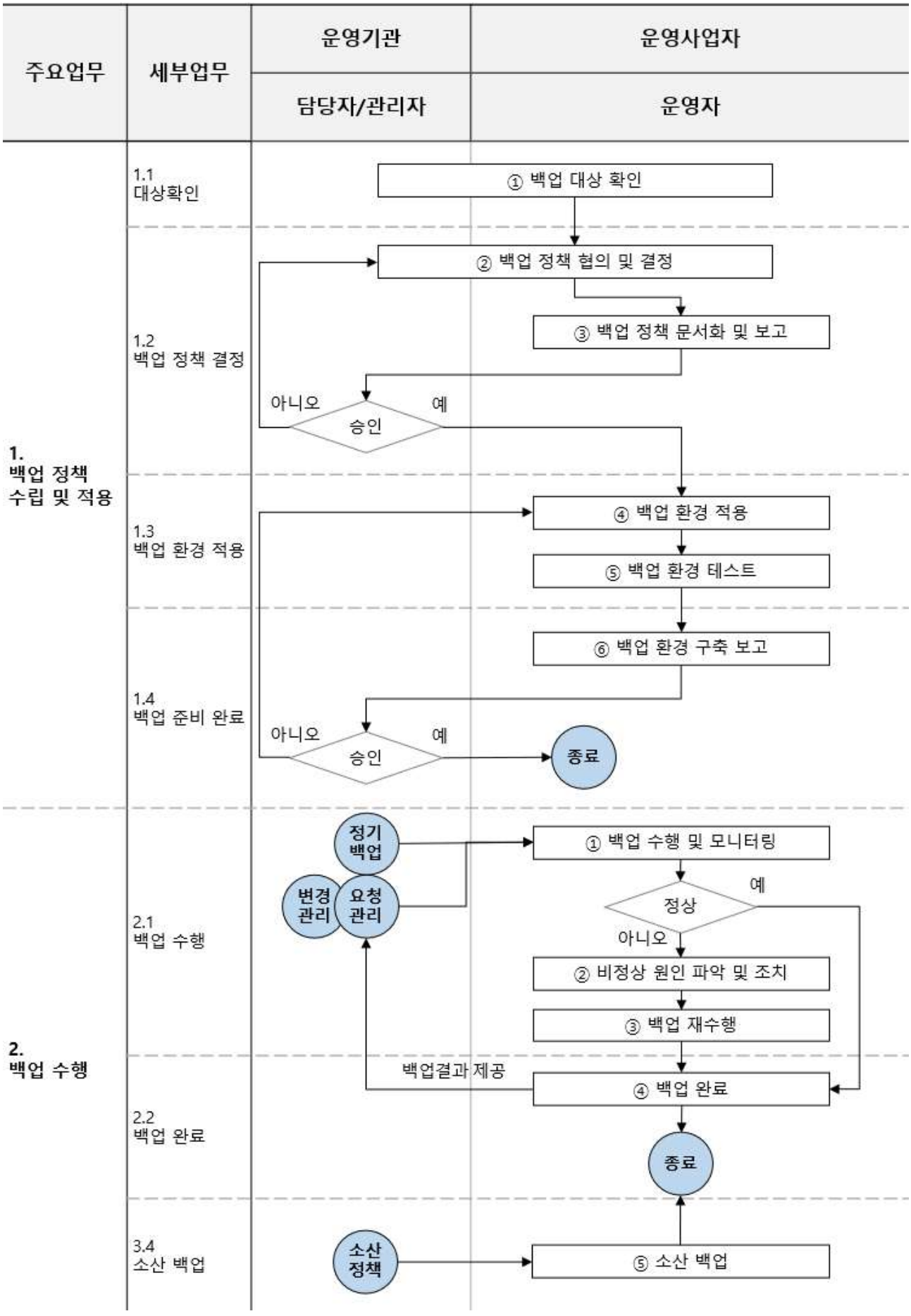
○ 백업관리 절차는 아래와 같은 주요 업무와 수행절차들로 구성된다.

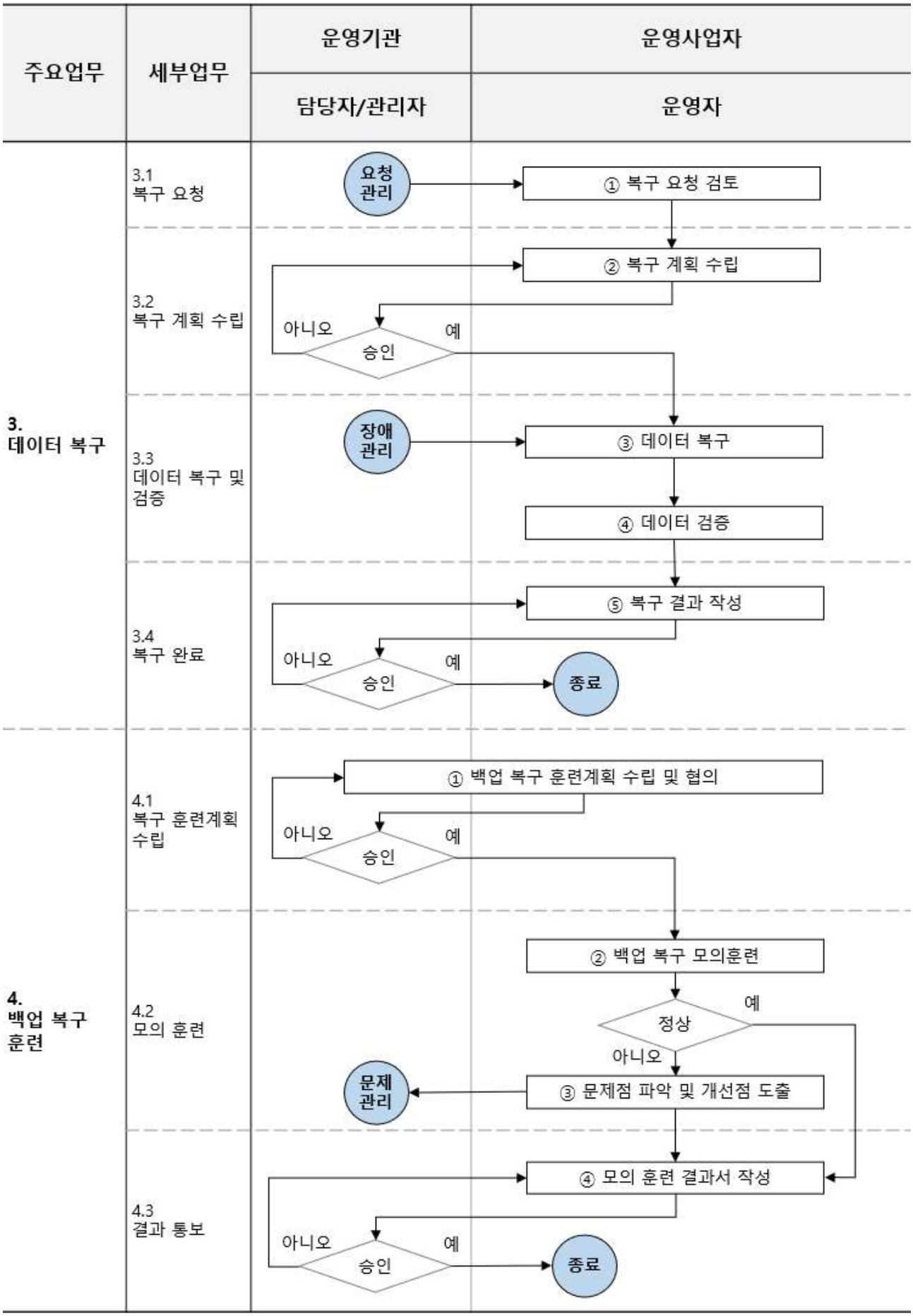
1) 주요 업무

주요 업무	세부 업무	수행 업무
1. 백업 정책 수립 및 적용	1.1 대상 확인	○ 운영기관 담당자와 운영자(백업 담당자)는 관리하고자 하는 백업 대상을 확인하고 정의한다. ○ 운영기관 담당자와 운영자(백업 담당자)는 데이터 유형별 백업대상을 반기 1회 이상 현행화하여 관리한다.
	1.2 백업 정책 결정	○ 운영기관 담당자와 운영자(백업 담당자)는 기관의 환경, 정보시스템 및 데이터 유형별 특성을 고려하여 백업 정책에 대한 협의를 진행하고, 적용할 정책에 대한 의사결정을 진행한다. ○ 백업 정책에는 백업대상, 백업방법, 백업주기, 백업 데이터 보관기간, 데이터 복구시점목표(RPO) 및 그 밖에 백업 정책 수립에 필요한 사항을 포함하며, "붙임 1. 백업 정책 기준"에 따라 수립·관리한다.
	1.3 백업 환경 적용	○ 운영자(백업 담당자)는 백업을 위한 제반 환경을 구성하고, 테스트를 진행한다.
	1.4. 백업 준비 완료	○ 운영자(백업 담당자)는 백업 환경 구축 결과에 대해 운영기관 담당자에게 보고한다. ○ 운영기관 담당자는 관련 내용을 검토하고 의사결정을 진행한다.
2. 백업 수행	2.1 백업 수행	○ 백업 정책에 기반하여 운영자(백업 담당자)는 백업 진행과 모니터링 활동을 수행한다. ○ 운영자(백업 담당자)는 정기 백업 및 백업 요청에 의한 백업 수행 결과를 확인하고, 백업 수행 후 백업 정상 완료 여부 및 데이터 무결성 등 백업 결과를 점검한다. ○ 백업 실패 또는 비정상 백업이 발생하는 경우 해당 원인을 파악하고 필요한 조치를 수행한다.
	2.2 백업 완료	○ 운영자(백업 담당자)는 정기 백업 및 요청 백업에 대하여 백업 결과 확인 내역을 기록·관리하고 일정 기간 보관한다.
	2.3 소산 백업	○ 운영자(백업 담당자)는 백업 데이터를 운영 중인 정보시스템과 동일한 재해상황에 동시에 영향을 받지 않는 원격지 저장소에 주기적으로 소산한다. ○ 원격지 소산은 온라인 또는 오프라인 방식으로 수행할 수 있으며, 소산 수행 결과는 기록·관리한다.

주요 업무	세부 업무	수행 업무
3. 데이터 복구	3.1 복구 요청	○ 정보시스템의 장애 또는 재해상황, 사용자 요청 등에 따라 복구가 필요할 경우 요청 관리 절차를 통하여 복구 요청을 진행하며 백업 담당자는 해당 요청의 적합성을 검토한다.
	3.2 복구 계획 수립	○ 운영자(백업 담당자)는 백업 복구를 위한 계획을 수립하여 보고한다. ○ 운영기관 담당자는 관련 내용을 검토하고 의사결정을 진행한다.
	3.3 데이터 복구 및 검증	○ 운영자(백업 담당자)는 백업 복구를 실시하고, 복구 데이터를 검증한다.
	3.4 복구 완료	○ 운영자(백업 담당자)는 백업 복구 결과에 대한 보고서를 작성하여 보고한다. ○ 운영기관 담당자는 관련 내용을 검토하고 의사결정을 진행한다.
4. 백업 복구 훈련	4.1 복구 훈련 계획 수립	○ 운영기관 담당자와 운영자(백업 담당자)는 백업 데이터 복구 훈련에 대한 대상, 범위, 일정 등에 대한 계획을 수립하고 적정 여부를 검토한다.
	4.2 모의훈련	○ 운영자(백업 담당자)는 훈련 계획 일정에 맞추어 백업 데이터 복구 훈련을 연 1회 이상 실시한다.
	4.3 결과 통보	○ 운영자(백업 담당자)는 백업 복구 훈련에 대한 보고서를 작성하여 보고한다. ○ 운영기관 담당자는 관련 내용을 검토하고, 개선이 필요한 사항에 대해 개선계획을 수립·관리한다.

2) 수행주체별 표준절차 흐름도




주요업무
세부업무
운영기관
운영사업자
담당자/관리자
운영자
3. 데이터 복구
3.1 복구 요청
요청 관리
① 복구 요청 검토
3.2 복구 계획 수립
② 복구 계획 수립
아니오
승인
예
3.3 데이터 복구 및 검증
장애 관리
③ 데이터 복구
④ 데이터 검증
3.4 복구 완료
⑤ 복구 결과 작성
아니오
승인
예
종료
4. 백업 복구 훈련
4.1 복구 훈련계획 수립
① 백업 복구 훈련계획 수립 및 협의
아니오
승인
예
4.2 모의 훈련
② 백업 복구 모의훈련
정상
예
아니오
문제 관리
③ 문제점 파악 및 개선점 도출
4.3 결과 통보
④ 모의 훈련 결과서 작성
아니오
승인
예
종료

바. 세부 수행 절차

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

(●: 정, ◑: 부)

세부 절차	수행 내용	운영기관	운영사업자
		관리자/담당자	운영자
1.1- ① 백업대상 확인	- 운영기관 담당자는 운영자와 협업하여 백업이 필요한 대상을 확인하고, 백업대상에 대하여 데이터, 복구 시 소요되는 목표시간, 백업주기 및 백업 데이터 보관기간에 관하여 분석한다. - 백업대상은 데이터 유형별로 백업 정책에 따라 관리한다. ※ "붙임1. 백업 정책 기준" 참조 ※ 데이터의 중요도와 서비스시간 등을 고려한 복구시간목표(RTO), 복구시점목표(RPO) 등을 분석한다. ※ 복구시간목표는 시스템의 중요도에 따라 달라질 수 있으며, 시스템 간의 우선순위가 고려되어야 한다.	●	◑
1.2- ② 백업 정책 협의 및 결정	- 운영기관 담당자는 운영자와 협업하여 분석된 대상을 상대로 백업 정책을 결정한다. · 데이터별 백업 방법을 선택한다. · 백업 수행 주기 및 백업 데이터 보관기간을 결정한다. · 데이터 복구 목표 시간에 대해 정의한다. · 원격지 소산 대상, 소산 주기, 소산 방식 및 원격지 저장소를 결정한다. (소산은 온라인 또는 오프라인으로 수행할 수 있다.) ※ "자. 관리 기준" 백업 정책(예시) 참조	●	◑
1.2- ③ 백업 정책 문서화 및 보고	- 운영자는 운영기관과 협의를 통해 결정된 백업 정책 및 절차 등을 문서화하고 운영기관 담당자에게 승인을 요청한다. - 운영기관 담당자는 내용을 검토하고, 미흡한 사항에 대해서는 시정 조치를 취한다. 미흡한 사항이 없을 경우 정책을 승인한다.		●
1.3- ④ 백업환경 적용	- 운영자(백업 담당자)는 백업 정책에 따른 백업환경을 구축한다. (예시: 백업관련 환경변수 설정, 정책적용, 스크립트 작업, 스케줄 등록, 백업시스템, 저장매체, 소산 복구 수행 환경 등) - 백업환경 구성을 위해 백업장비의 증설이 필요한 경우, 증설 작업 및 환경 구축을 수행한다.		●
1.3- ⑤ 백업환경 테스트	- 운영자(백업 담당자)는 백업환경 구축 후 정상 수행 여부를 확인하기 위하여 테스트를 수행한다. 업무에 지장을 주지 않는 한 간단한 백업/복구 테스트를 진행하여 백업환경의 적합성을 확인한다.		●

(●: 정, ◑: 부)

세부 절차	수행 내용	운영기관	운영사업자
		관리자/담당자	운영자
1.4- ⑥ 백업환경 구축보고	- 운영자(백업 담당자)는 백업환경 구축 및 테스트에 대한 결과를 작성 후 운영기관 담당자에게 보고한다. - 운영기관 담당자는 내용을 검토하고, 미흡한 사항에 대해서는 시정 조치를 취한다. 미흡한 사항이 없을 경우 승인한다.	◑	●
2.1- ① 백업 수행 및 모니터링	- 운영자(백업 담당자)는 백업 정책에 맞추어 백업의 진행 상태를 주기적으로 모니터링한다. - 백업 요청이 접수된 경우 운영자(백업 담당자)는 백업 작업을 수행한다. - 정기 백업은 사전 정의된 스케줄에 따라 실행되며, 백업 수행 중 진행 상태에 대한 모니터링을 수행한다. - 백업 수행 결과가 정상인 경우 해당 백업절차를 완료하며, 비정상인 경우 원인 파악 및 조치 작업을 수행한다. - 모니터링을 통해 동일한 에러가 반복되어 나타나는 등의 문제 현상이 도출되면 문제관리로 이관하여 문제를 해결한다.		●
2.1- ② 비정상 원인 파악 및 조치	- 백업 실패 또는 비정상 백업이 발생한 경우 오류 원인을 파악하여 조치 작업을 수행한다. - 백업 수행 중 나타나는 에러는 백업 소프트웨어에서 제공하는 매뉴얼을 참고하여 해결할 수 있다. - 비정상 백업이 빠르게 조치되지 않거나 장애에 해당될 경우 장애관리 절차에 따라 장애조치를 수행한다.		●
2.1- ③ 백업 재수행	- 비정상 백업에 대한 조치가 완료된 경우 재백업 또는 백업 스케줄을 고려하여 백업을 재수행한다.		●
2.2- ④ 백업 완료	- 운영자(백업 담당자)는 정기 백업, 예방 차원의 백업 수행 또는 요청에 의한 백업 작업을 완료한 경우 백업 정상 완료 여부 및 데이터 무결성 등 백업 결과를 점검·확인한다. - 운영자(백업 담당자)는 백업 이력, 수행 내역 및 백업 결과 확인 내역을 기록·관리하고 일정 기간 보관한다.		●
2.3- ⑤ 소산 백업	- 운영자(백업 담당자)는 백업 데이터를 운영 중인 정보시스템과 동일한 재해상황에 동시에 영향을 받지 않는 원격지 저장소에 주기적으로 소산한다. - 원격지 소산은 온라인 또는 오프라인 방식으로 수행할 수 있으며, 소산 수행 결과는 기록·관리한다. - 소산 구역 출입 권한은 기관의 정보보호 규정에 따른다. - 모든 정보시스템은 필수적으로 원격지 백업 소산을 수행한다.		●

(●: 정, ◑: 부)

세부 절차	수행 내용	운영기관	운영사업자
		관리자/담당자	운영자
3.1- ① 복구 요청 검토	- 데이터 관련 장애 또는 필요에 의한 복구 요청은 요청 프로세스에 의거하여 운영자(백업 담당자)에게 복구 요청을 할 수 있다. - 운영자(백업 담당자)는 접수된 복구요청서를 확인하고 데이터 복구 가능 여부를 확인한다. - 요청한 데이터가 보관기간에서 벗어나거나, 백업이 수행되지 않는 데이터인 경우 요청자에게 현재 백업 상황을 통보한다.		●
3.2- ② 복구 계획 수립	- 운영자(백업 담당자)는 긴급한 복구 상황의 경우 선조치 후 보고의 방법을 통하여 신속한 복구절차를 수행한다. - 운영자(백업 담당자)는 복구요청서의 내용과 데이터 확인을 바탕으로 복구 계획서를 작성하고 운영기관 담당자에게 승인을 요청한다. · 내용: 복구 시점, 복구 방법, 복구 절차, 미디어 위치 및 관련 정보 - 운영기관 담당자는 내용을 검토하고, 미흡한 사항에 대해서는 시정 조치를 취한다. 미흡한 사항이 없을 경우 복구 계획을 승인한다.	◑	●
3.3- ③ 데이터 복구	- 운영자(백업 담당자)는 승인된 복구 계획에 따라 데이터를 복구한다.		●
3.3- ④ 데이터 검증	- 운영자(백업 담당자)는 복구된 데이터의 정상 여부를 검증한다. 데이터 검증의 효율성을 위하여 업무 시스템 담당자도 함께 검증을 진행할 수 있다.		●
3.4- ⑤ 복구 결과 작성	- 운영자(백업 담당자)는 복구 결과에 대한 보고서를 작성하여 보고한다. 운영기관 담당자는 관련 내용을 검토하고 의사결정을 진행한다. · 내용: 복구 방법, 결과, 복구 시간, 문제점 및 개선점 - 운영기관 담당자는 내용을 검토하고, 미흡한 사항에 대해서는 시정 조치를 취한다. 미흡한 사항이 없을 경우 복구 결과를 승인한다.	◑	●

(●: 정, ◑: 부)

세부 절차	수행 내용	운영기관 관리자/담당자	운영사업자 운영자
4.1- ① 백업 복구 훈련 계획 수립 및 협의	- 운영자(백업 담당자)는 운영기관 담당자와 협의하여 백업 데이터 복구 훈련 계획서를 작성하고, 운영기관 담당자에게 승인을 요청한다. - 백업 데이터 복구 훈련은 연 1회 이상 실시한다. 단, 다수의 정보시스템을 동일 운영환경 및 백업환경에서 통합 관리할 경우, 운영환경 및 백업환경별 1개 이상 정보시스템을 대상으로 실시할 수 있다. - 복구 훈련 계획에는 다음 사항을 포함한다. · 복구 훈련 일정, 복구 범위, 복구 데이터 검증 방안, 복구 훈련 장비 등 - 복구는 안정성 및 서비스 중단의 최소화를 위해 대체 장비 활용을 원칙으로 하며, 정기적인 백업 스케줄에 영향을 주지 않는 범위에서 수행한다. - 운영기관 담당자는 내용을 검토하고, 미흡한 사항에 대해서는 시정 조치를 요구한다.	●	●
4.2- ② 백업 복구 모의훈련	- 운영자(백업 담당자)는 복구 훈련 계획에 따라 백업 데이터 복구 훈련을 실시한다. - 복구 훈련의 주요 사항은 아래와 같다. · 복구 후 백업된 데이터에 복구 대상 파일들이 모두 포함되어 있는지 확인한다. · 비정상적 복구 시 백업 방법의 문제인지 복구 방법의 문제인지 조사 후 수정 및 조치한다. - 복구시간 지연 시 백업시스템 및 솔루션의 설정, 매체 드라이브의 이상 유무, 백업 네트워크 속도 등을 점검한다. 필요시 솔루션 공급자의 지원을 받을 수 있다. - 소산 데이터 복구 훈련을 한 경우, 백업 복구 훈련을 한 것으로 갈음할 수 있다.		●
4.2- ③ 문제점 파악 및 개선점 도출	- 복구 데이터의 무결성에 이상이 있을 경우, 백업 매체의 이상이나 백업방식의 문제 등을 확인한다. - 문제점 파악 및 개선점을 도출한 이후, 지속적인 개선 관리가 필요한 경우 문제관리 프로세스로 이관하여 보완 조치 및 관리 활동을 수행한다.	◑	●
4.3- ④ 모의훈련 결과서 작성	- 운영자(백업 담당자)는 백업 데이터 복구 훈련에 대한 보고서를 작성하고 운영기관 담당자에게 승인을 요청한다. · 내용: 복구 방법·결과, 복구시간, 문제점, 개선점 등 - 운영기관 담당자는 내용을 검토하고, 개선이 필요한 사항에 대해서는 개선계획을 수립·관리한다. 미흡한 사항이 없을 경우, 훈련 결과를 승인한다.	◑	●

사. 핵심성과지표 (KPI : Key Performance Indicator)

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

측정 지표	측정 방법(예시)	측정 목적	측정 주기
백업 성공률	(백업 성공 건수 / 당월 총 백업 실행 건수) X 100	백업 성공 유무	당월

아. 수행 검증

1) 검증 방법

○ 검증 체크리스트의 체크 항목 기준(ITIL 표준 준용)으로 표준운영절차의 준수 여부와 이행 점검을 수행한다.

○ 개별기관 내 자체 프로세스 검증자는 내부 감사자의 자격 또는 ITIL에 대한 충분한 이해를 가진 자가 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
백업 정책 수립 및 적용	- 조직의 운영환경과 백업 정책 기준을 고려하여 데이터 유형별 백업 정책이 수립되어 있습니까?	적합/ 부적합	• 백업 관리 정책
	- 백업 대상은 반기 1회 이상 현행화되어 관리되고 있습니까?		• 백업 관리 정책 • 백업 대상 목록
백업 수행	- 백업 정책에 맞추어 백업활동의 진행상태를 주기적으로 모니터링하고 있습니까?		• 백업 관리대장
	- 정기 백업 이외의 요청은 요청관리 프로세스에 따라 요청되고 진행·관리되고 있습니까?		• 백업 관리대장
백업 복구 훈련	- 정보시스템의 안정적 운영을 고려하여 백업 복구 역량 강화를 위한 백업 데이터 복구 훈련을 연 1회 이상 실시하고 있습니까?		• 복구 훈련 계획, 결과
	- 훈련 결과 도출된 문제점 및 개선사항 등에 대해서 적절한 관리 또는 문제관리 프로세스에 의한 개선 관리가 수행되고 있습니까?		• 문제 관리 이력
데이터 복구	- 데이터 복구 요청 및 처리에 대한 이력은 기록·관리되고 있습니까?		• 백업 관리대장
	- 장애에 준하는 긴급한 복구 상황의 경우에 대처하기 위한 대응 절차를 운영하고 있습니까?		• 긴급 복구 절차

자. 관리 기준 및 예시

1) 백업 정책(예시)

구분	정책		정책에 대한 설명
데이터 백업 방법	전체 백업(Full Backup)		▪ 파일시스템으로 구성된 사용자파일에 대한 데이터 전체를 백업하는 방식
	증분 백업 (Incremental Backup)	차별 증분	▪ Full Backup 기준 변경된 데이터를 다음 Full Backup까지 매일 백업하는 방식
		누적 증분	▪ 전체 백업 이후로 다음 전체 백업이 실시되기 직전까지 전체 백업 이후의 변화된 데이터를 백업하는 방식
백업 수행 주기	일일 백업(Daily Backup)		▪ 요청 파일이나 데이터베이스 파일 등 주요 업무에 대해 매일 백업을 실시한다. 보관 기간은 정책에 따라 달라질 수 있다.
	주간 백업(Weekly Backup)		▪ 매주 지정된 요일에 데이터를 백업한다. 주로 시스템자원의 사용이 적은 주말에 백업하며, 일간 백업 시 수행하지 못했던 데이터에 대해서도 전체적으로 백업한다.
	월간 백업(Monthly Backup)		▪ 매월 지정된 날에 실시한다.
데이터 복구 목표시간	-		▪ 업무 시스템의 중요도, 긴급성, 데이터의 용량 등에 따라 복구 목표 시간을 다르게 설정할 수 있다.
매체 소산 여부 (분산백업)	-		▪ 정보시스템 운영장소(IDC 등)의 재해 및 장애에 대한 2차적인 복구방안으로 소산백업을 실시할 수 있다. 즉, 주요 데이터에 대한 전체 백업본을 적절한 원격지에 안전하게 보관함으로써 센터의 물리적 재해에 대비할 수 있다.

2) 소산 방법(예시)

구분	보관 장소	설명
내부 소산	내부 내화 금고	▪ 보안, 항온항습이 유지되는 공간으로 매체 소산 활동을 진행한다.
외부 소산	외부 소산 장소	▪ 정보시스템 운영 장소와 일정 거리 이격된 장소에 위치한 보안, 항온항습이 유지되는 공간으로 매체 소산 활동을 진행한다.

■ 붙임1 백업 정책 기준

※ 행정기관 및 공공기관 정보시스템 안정성 고시 [별표 11]

백업 정책 기준(제19조 관련)

데이터(정보) 유형	백업방법	백업주기	보관기간	백업 최대허용시간
OS 데이터 (OS 프로그램 파일, 시스템 구성 및 로그 파일 등)	전체 백업	분기 1회	반기	주중 12시간 주말 60시간 ※ 백업 최대허용시간을 초과하지 않도록 백업환경 개선, 분할 백업 등 조치 수행
DB 데이터 (DB의 데이터파일 및 컨트롤파일, 변경로그파일 등)	전체 백업	주 1회	4주	
	증분 백업	일 1회	4주	
파일 데이터 (소스파일, AP SW, 사용자 데이터 등)	전체 백업	주 1회	4주	
	증분 백업	일 1회	4주	
가상머신(VM)	이미지 백업	주 1회	4주	
컨테이너	이미지/설정 백업	일 1회 또는 변경 시	4주	
클라우드 관리 서버	전체 백업	일 1회	4주	

※ 세부 데이터 유형, 데이터 용량 등에 따라 백업 방법과 주기 등 조정 가능

9. 배포관리 절차서

가. 개요

1) 목적

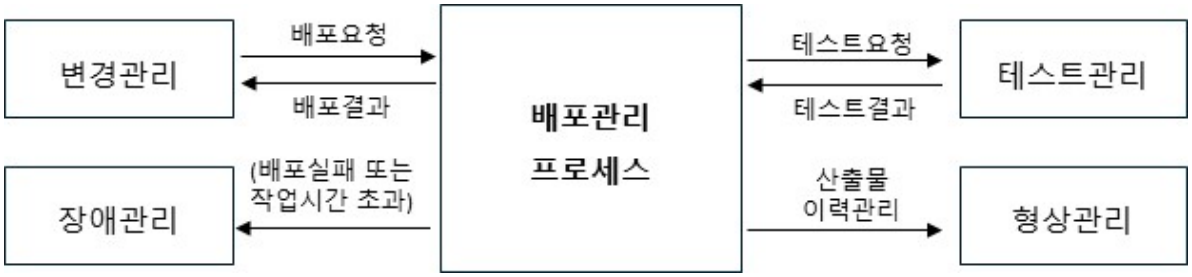
○ 응용프로그램 변경 요청을 운영환경에 반영하기 위한 배포 절차를 표준화하여 체계적으로 관리하고, 배포관리 기준을 제공하여 배포 과정의 위험을 최소화하고 시스템의 무결성을 확보한다.

2) 적용 범위

○ 배포관리 절차는 응용프로그램의 변경을 운영환경에 반영하기 위한 배포 계획 수립, 검토, 승인, 배포 수행, 검증, 배포결과 검토 및 종료 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 변경사항을 운영환경에 반영하기 위해 수행하는 배포 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 시스템 내 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 배포 계획은 테스트환경(검증계)에서 테스트를 완료한 후 운영서버에 반영을 요청할 수 있다.
	설명	○ 운영자는 개발 완료된 릴리스의 테스트 활동을 포함하여 배포 계획을 수립한다. ○ 배포 계획은 운영자와 운영기관 담당자(변경 요청자)의 2단계 승인을 수행한다. (긴급 배포의 경우 예외적으로 생략 가능) - 운영자는 테스트 시나리오에 따라 테스트환경에서 사전 검증 통합 테스트를 수행하고 배포 계획을 1차 검토 - 운영기관 담당자(변경 요청자)는 1차 배포 계획 검토 결과에 따라 보완 요청 또는 운영서버 배포 승인
정책 2	기준	모든 배포 작업의 상태 및 이력은 문서로 기록하고 관리해야 한다.
	설명	○ 배포 작업의 요청, 승인, 결과 확인 및 이력은 ITSM, 형상관리시스템 등 관리시스템을 통해 기록·관리한다. ○ ITSM 등 운영시스템이 없는 경우 배포 정보를 관리대장 등에 기록·관리할 수 있다. ※ A1등급은 관리시스템을 다중화하여 구축·운영한다.
정책 3	기준	모든 배포 작업은 정상 동작 여부를 검증하는 테스트를 수행해야 한다.
	설명	○ 변경 관련 주요 기능을 테스트하고 변경 사항이 시스템에 미치는 영향을 최소화하여 안정적인 서비스를 제공한다. - 기능 검증을 위한 단위 테스트, 통합 테스트, 성능 테스트 등을 수행 - 운영서버 배포 후 운영기관 담당자(변경 요청자)의 인수 테스트 수행
정책 4	기준	모든 배포 작업은 원상복구 계획을 배포 계획에 포함하여 관리해야 한다.
	설명	○ 배포 실패 발생 시 작업 결과를 상세히 기록하고, 장애관리로 이관한다. ○ 원상복구 계획의 절차에 따라 복구를 수행한다. - 배포 실패 또는 문제 발생 시 사전 정의된 원상복구 절차를 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 운영서버에 반영하기 위한 요청 문서
개발환경	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	○ 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	○ 배포 작업 대상 정보시스템 업무 담당자가 역할 수행 ○ 배포 계획의 적정성 검토 - 배포 계획 이관 승인 포함 ○ 배포 결과 검토 및 이슈 보고 ○ 배포 후 서비스 상태 점검 및 문제 발생 시 보고
수탁기관 또는 운영사업자	운영자	○ 운영기관과의 계약을 통해 정보시스템의 운영, 유지보수 및 배포 작업을 담당하는 수탁기관 또는 운영사업자 ○ 배포 요청에 따른 세부 계획 수립 및 일정 관리 ○ 배포 대상 시스템, 응용프로그램 검토 및 준비 ○ 배포 계획의 적정성 검토 ○ 배포 계획 수립과 배포 관련 준비 작업 - 배포 자동화 도구(Jenkins 등) 설정 및 관리 - 배포 스크립트 작성 및 검증 - 배포 파일 및 스크립트 무결성 검증 및 오류 수정 ○ 배포 전 시스템 백업 및 복구 계획 수립 ○ 배포 작업 수행 및 결과 보고 - 배포 계획에 따라 작업 수행 후 테스트 및 서비스 확인 ○ 배포 진행 상황 모니터링 ○ 배포 후 시스템 성능 점검 및 오류 수정 ○ 배포 후 시스템 장애 발생 시 긴급 복구 및 롤백 수행 ○ 배포 후 형상정보에 대한 현행화 작업 수행 ○ 배포 전/후 기능 테스트 및 성능 검증 ○ 배포 후 서비스의 정상 작동 여부 확인 ○ 테스트 결과보고서 작성 및 이슈 보고

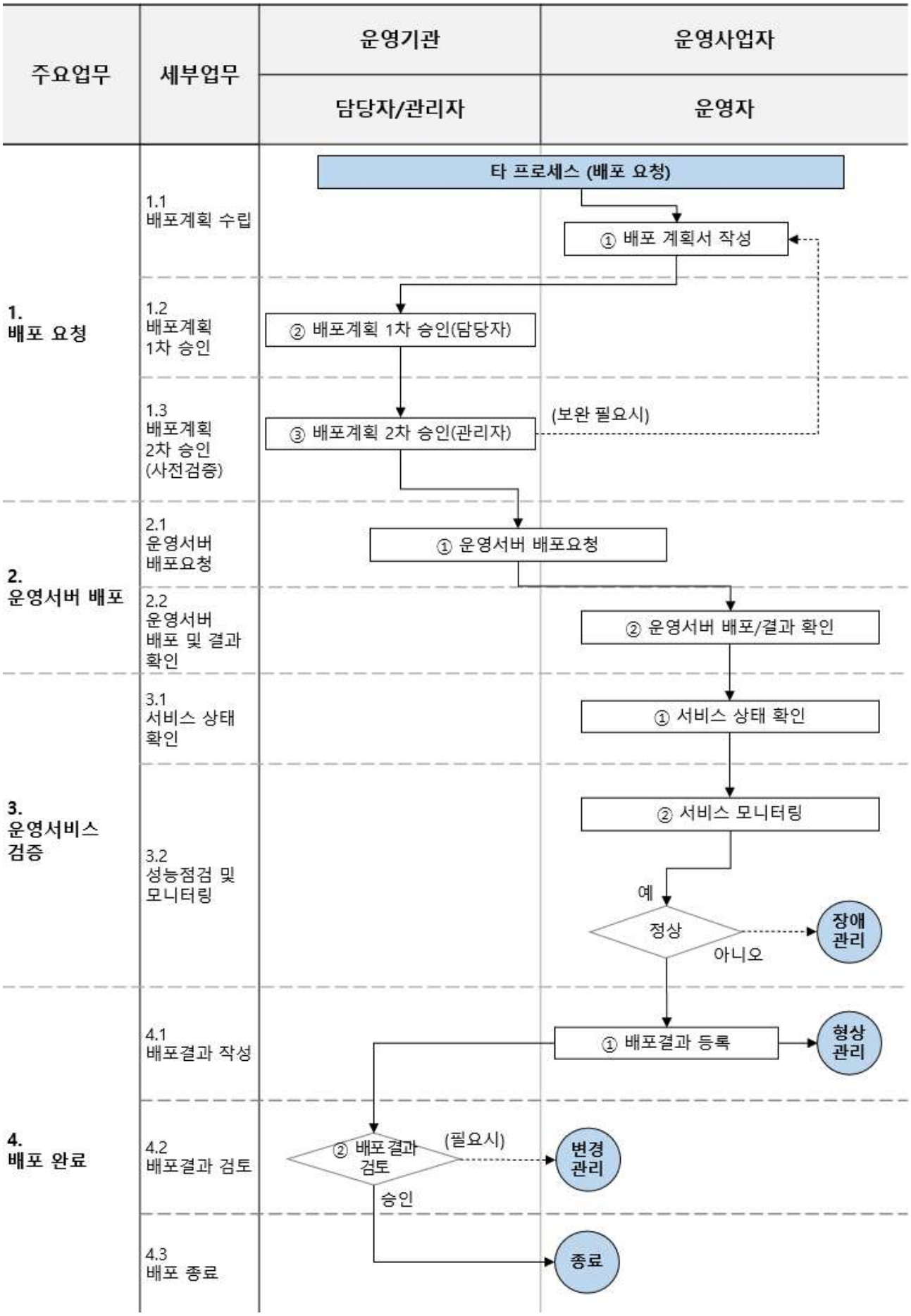
마. 표준절차 흐름도

○ 배포관리 절차는 아래와 같은 주요 업무와 수행 활동으로 구성된다.

1) 주요 업무

주요 업무	세부 업무	수행 활동
1. 배포 요청	1.1. 배포 계획 수립	○ 운영자는 변경된 릴리스의 서비스 영향을 분석하고 테스트 수행 후 테스트 시나리오 및 결과를 포함하여 배포 계획을 수립한다.
	1.2. 배포 계획 1차 승인	○ 담당자는 배포 계획을 검토하고, 1차 승인한다.
	1.3. 배포 계획 2차 승인 (사전 검증)	○ 관리자는 1차 배포 계획 검토 결과를 확인하고 보완 요청 또는 운영 배포 계획을 승인한다.
2. 운영서버 배포	2.1. 운영서버 배포 요청	○ 승인된 배포 계획에 따라 운영서버 배포를 요청한다.
	2.2. 운영서버 배포 및 결과 확인	○ 운영자(배포 담당자)는 개발된 릴리스를 운영서버에 반영한다. ○ 배포 중 오류 발생 등 배포작업 결과를 확인한다.
3. 운영 서비스 검증	3.1. 서비스 상태 확인	○ 운영자는 배포된 릴리즈가 서비스에 정상 반영되었는지 확인한다. - 주요 기능, 접속, 화면, 처리 결과 등 서비스 기본기능의 정상 동작 여부 확인
	3.2. 성능점검 및 모니터링	○ 운영자는 배포 후 시스템 성능을 모니터링하고 장애 발생 여부를 점검한다. ○ 서비스 응답 상태, 자원 사용률, 처리 속도, 서비스 지연 여부 등을 확인한다. - 장애 발생 시 신속히 대응하고 장애관리 절차로 이관한다. ○ 배포 작업 실패 또는 서비스 검증 실패 시에는 롤백을 실행하여 시스템을 복구한다.
4. 배포 완료	4.1. 배포 결과 작성	○ 운영자는 형상항목 업데이트를 실시하고 배포 완료 보고서를 작성한다. ○ 운영자는 배포 결과를 검토하고 ITSM에 등록한다.
	4.2. 배포 결과 검토	○ 운영기관 담당자(변경 요청자)는 배포 작업 완료 여부를 확인하고, 배포 결과를 승인한다.
	4.3. 배포 종료	○ 배포 과정에서 도출된 개선 사항을 분석하고 문서화하여 향후 배포 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	운영기관	운영사업자
			관리자/담당자	운영자
1. 배포 계획 수립	1.1.- ① 배포 계획 수립	- 운영자는 배포 계획서를 작성하여 ITSM 시스템에 등록한다. - 배포 계획서에는 배포 대상 시스템, 배포 일정 및 서비스 영향도, 테스트 시나리오 및 결과, 원복 계획 등을 상세히 기술한다.		●
	1.2.- ② 배포 계획 1차 승인	- 담당자는 배포 계획서를 검토하고, 1차 승인한다.		●
	1.3.- ③ 배포 계획 2차 승인 (사전 검증)	- 관리자는 1차 배포 계획 검토 결과를 확인하고, 보완 요청 또는 배포 계획을 승인한다. - 연계 시스템에 서비스 영향이 발생할 것으로 예상되는 경우 배포 계획을 관련 기관에 공지한다.	●	●
2. 운영서버 배포	2.1.- ① 운영서버 배포 요청	- 승인된 배포 계획에 따라 운영서버 배포를 요청한다. ※ 배포 작업을 타 기관에서 하는 경우 (예. 국정자원) 배포 계획서를 이관하고 운영서버 반영 작업을 요청한다.	●	●
	2.2.- ② 운영서버 배포 및 결과 확인	- 배포 중 오류 발생 등 진행 상황을 모니터링하고 배포 작업 결과를 확인한다. - 배포 작업 중 오류(Incident) 발생 시 배포 계획에 명시된 원복 계획에 따라 복구를 수행한다.		●

단계	세부 절차	세부 수행 내용	운영기관 관리자/담당자	운영사업자 운영자
3. 운영 서비스 검증	3.1.- ① 서비스 상태 확인	- 운영자는 배포 완료 후 배포된 릴리스가 서비스에 정상 반영되었는지 확인한다. - 운영자는 서비스 접속, 화면, 주요 기능, 업무 처리 결과 등 서비스 기본 기능의 정상 동작 여부를 확인한다. - 서비스 상태 확인 결과 오류 또는 이상 사항이 확인된 경우 배포 담당자 및 관련 담당자에게 조치를 요청하고 조치 결과를 확인한다.		●
	3.2.- ② 성능점검 및 모니터링	- 운영자는 서비스 응답 상태, 자원 사용률, 처리 속도, 서비스 지연 여부 등을 확인한다. - 성능 저하, 오류 또는 장애 징후가 확인된 경우 신속하게 대응하고, 필요 시 장애관리 절차로 이관한다. - 배포 작업 실패 또는 서비스 검증 실패 시에는 롤백을 실행하여 시스템을 복구한다. - 운영자는 롤백 수행 여부, 복구 결과 및 진행 상황을 확인하고 배포 결과에 기록한다.		●
4. 배포 완료	4.1.- ① 배포 결과 등록	- 운영자는 형상관리도구에 형상항목 업데이트를 실시하고 배포 완료 보고서를 작성한다. - 운영자는 변경 계획, 배포 계획, 배포 결과 등이 일치하는지 검토하고 ITSM에 등록한다.		●
	4.2.- ② 배포 결과 검토	- 운영기관 담당자(변경 요청자)는 배포 작업 완료 여부를 확인한다. - 배포 결과를 승인 또는 변경관리 절차로 이관한다. - 변경 계획의 수정이 필요한 경우 변경 계획 수립 절차로 이동한다.	●	●
	4.3.- ③ 배포 종료	- 운영자는 배포 결과를 확인하고 배포 종료를 승인한다. - 배포 과정에서 도출된 개선 사항을 분석하고 문서화하여 향후 배포 작업에 반영한다.		●

2) 고려사항

○ N/A

사. 핵심성과지표 (KPI : Key Performance Indicator)

○ 배포 프로세스 관리 지표를 도출하여 운영 품질 관리를 목표로 하며, 본 절차서에서는 KPI 표준안을 제시하고 개별기관별 운영 상황에 맞추어 조정하여 지표 관리

측정 지표	측정 방법(예시)	측정 목적	측정 주기
배포 성공률 (Deployment Success Rate)	(성공한 배포 건수 / 당월 수행된 배포 건수) X 100	배포가 장애 없이 정상적으로 완료된 비율 관리	당월
배포 후 결함 발생률 (Post-Deployment Defect Rate)	(배포 후 발견된 결함 건수 / 당월 수행된 배포 건수) X 100	배포 후 발견된 기능적 결함 비율 관리	당월
배포 후 평균 복구 시간 (Mean Time to Recover, MTTR)	장애 발생 시간 ~ 정상화 시간 측정	배포 중 장애 발생 시 정상 복구까지 소요된 평균 시간 관리	당월

아. 수행 검증

1) 검증 방법

○ 검증 체크리스트의 기준 항목으로 표준운영절차의 준수 여부와 이행 점검을 수행한다.

○ 개별기관 내 자체 프로세스 검증자는 내부 감사자의 자격 또는 ITIL에 대한 충분한 이해를 가진 자가 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	- 배포 계획은 서비스 영향 분석을 수행한 결과를 포함하고 있습니까?	적합/ 부적합	• 배포 계획서 - 서비스 영향 분석 결과
	- 배포 계획은 테스트 결과를 포함하고 있습니까?		• 배포 계획서 - 테스트계획서
	- 배포 계획은 2단계(운영자→운영기관 담당자) 승인을 수행하고 있습니까?		• ITSM 내 승인 이력
	- 배포 계획에는 작업 실패에 대비한 원복 계획/절차를 수립하여 포함하고 있습니까?		• 원복 계획서 - 배포 계획서 내 포함 가능
운영서버 배포	- 배포 계획은 테스트환경에서 테스트 완료 후 운영 서버에 반영하도록 관리되고 있습니까?		• ITSM 프로세스 - 테스트 결과서
	- 모든 배포 작업의 상태 및 이력은 문서로 기록하고 관리되고 있습니까?		• ITSM 프로세스 - 배포 이력
운영서비스 검증	- 배포 후 기능의 정상 동작 여부를 확인하기 위한 테스트를 수행하고 있습니까?		• 테스트 계획 및 테스트 결과
	- 배포 후 성능 및 장애 모니터링을 수행하고 장애 발생 시 장애관리 절차로 이관하여 관리하고 있습니까?		• 모니터링 이력 • 장애관리 이력

자. 관리 기준 및 예시

1) 배포관리 산출물(예시)

배포 계획			
변경ID		작성자	
배포유형		서비스 영향도	
배포 계획			
테스트 결과			
원상복구 계획			

배포 승인			
승인자		승인 상태	
승인의견			

배포 요청				
변경ID			요청자	
배포 대상			배포요청일시	
긴급 여부			서비스 중단 여부	
배포 요청 항목	형상ID	경로		파일명
비 고				

배포 결과			
작업시작일시		작업종료일시	
작업 결과		작업자	
모니터링 결과		검증자	
오류발생사항			

개선 사항	
내용	

10. 테스트관리 절차서

가. 개요

1) 목적

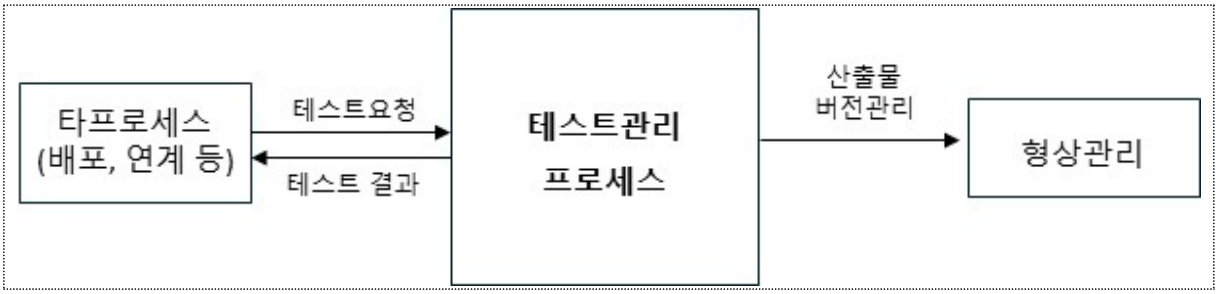
○ 응용프로그램 변경에 따른 서비스 영향과 장애발생요소를 최소화하기 위하여 테스트 수행 기준, 테스트 계획 수립 및 설계, 개발환경 및 운영환경 검증, 테스트 결과 분석 및 개선 절차를 표준화하여 정보시스템의 안정적 운영을 보장한다.

2) 적용 범위

○ 테스트관리 절차는 중앙행정기관등의 장이 관리하는 정보시스템 중 응용프로그램 변경, 신규 개발, 연계 변경 등 서비스에 영향을 미치는 운영관리 업무에 적용한다.

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 정보시스템 또는 데이터 연계 변경 등 서비스 영향 검토 및 테스트 수행이 필요한 요청
프로세스 종료 조건	테스트 요청의 반려 테스트 결과 등록 및 분석·개선사항 확인 완료
증적(Output)	테스트 요청서, 테스트 계획서, 테스트 결과서(단위/통합/성능/인수 등) ※ ITSM 시스템을 사용하는 경우 시스템 내 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	○ 테스트 수행 기준에는 테스트 대상, 범위, 수행환경, 수행주체 및 결과관리 기준을 포함하여야 한다. 개발환경 및 운영환경 검증은 테스트 절차에 따라 수행하며, 변경사항 적용 전 안정성에 대한 테스트를 수행하여야 한다. - 유사환경 : OS버전, DB버전, WAS버전 등 운영환경과 동일하게 구성 - 물리적 자원 확보에 제약이 있을 경우, 동일 서버 내 파티션 분리를 통한 테스트/운영환경 구성
정책 2	기준	테스트계획은 테스트 수행 기준에 따라 수립하고, 테스트 설계 산출물로 테스트 케이스 및 시나리오를 포함하여 관리하여야 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 변경, 소프트웨어 업데이트 및 패치 등 서비스에 영향을 미치는 변경사항은 사전 영향도 검토 및 안정성 테스트 후 적용하여야 하며, 테스트 결과를 기록·관리하여야 한다.
	설명	○ 단위테스트 : 변경작업자가 구현한 기능의 정상 동작 여부를 운영자가 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	테스트관리 절차의 요청, 승인, 결과 확인 등 모든 단계는 관리시스템을 통해 처리하고 이력을 관리한다.
	설명	○ 관리시스템을 통한 처리 및 이력관리를 적용한다.
정책 5	기준	연계서비스에 영향을 미치는 변경이 발생하는 경우 서비스 영향도 및 파급도를 검토하고, 연계 대상 정보시스템의 정상 동작 여부와 결과를 확인·기록하여야 한다.
	설명	○ 변경작업자는 연계서비스 영향도를 파악하여 운영자와 운영기관 담당자에게 연계서비스 테스트계획서를 제공한다. ○ 운영자는 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 개발환경 및 운영환경에서 정상적으로 동작하는지 확인하고 테스트 결과를 분석·개선하여 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 확인하고, 서비스 영향 여부를 검증하는 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 ○ 테스트 계획의 적정성 검토 - 테스트 시나리오 및 케이스 포함 ○ 배포 전 테스트환경 통합테스트 수행 ○ 배포 후 운영환경 인수테스트 수행 ○ 테스트 수행 결과 및 개선 필요사항 검토
수탁기관 또는 운영사업자	운영자	○ 운영기관과의 계약을 통해 정보시스템의 운영과 테스트 작업을 담당하는 수탁기관 또는 운영사업자 ○ 테스트 계획서 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 ○ 개발환경 및 운영환경 테스트 수행 지원 ○ 단위테스트 수행 ○ 단위테스트 수행 결과 검토 ○ 단위테스트 결과 보고서 작성 ○ 통합테스트 수행 ○ 통합테스트 결과 보고서 작성 ○ 테스트 수행 중 발생한 이슈 보고, 모니터링 및 대응 ○ 테스트 중 발견된 결함 분석 및 수정 ○ 테스트 요청, 승인, 결과 확인 등 단계별 이력관리 ○ 배포 전/후 기능 테스트 및 성능 검증 ○ 배포 후 운영환경에서 서비스의 정상 작동 및 서비스 영향 여부 확인

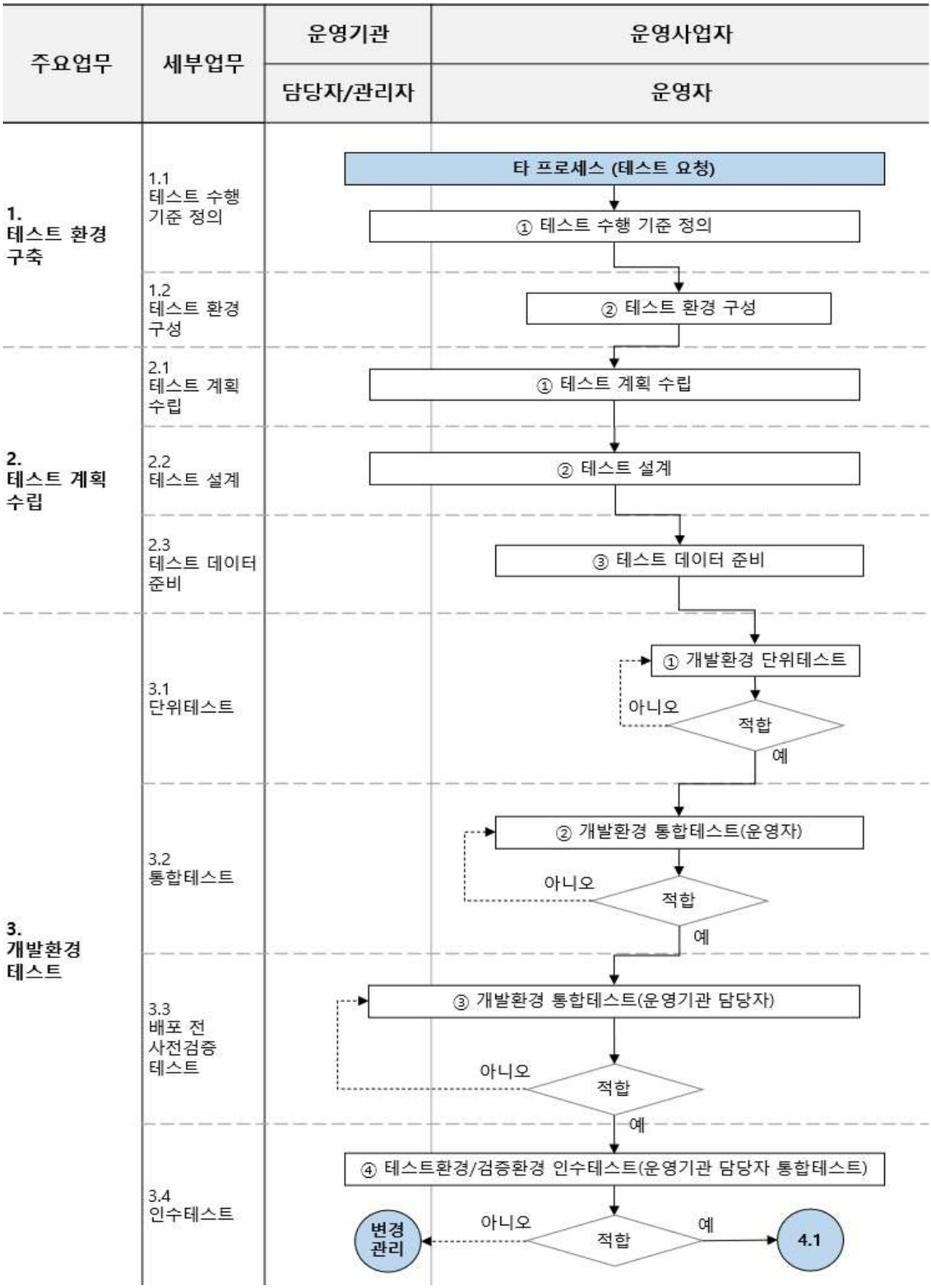
마. 표준절차 흐름도

○ 테스트관리 절차는 아래와 같은 주요 업무와 수행절차들로 구성된다.

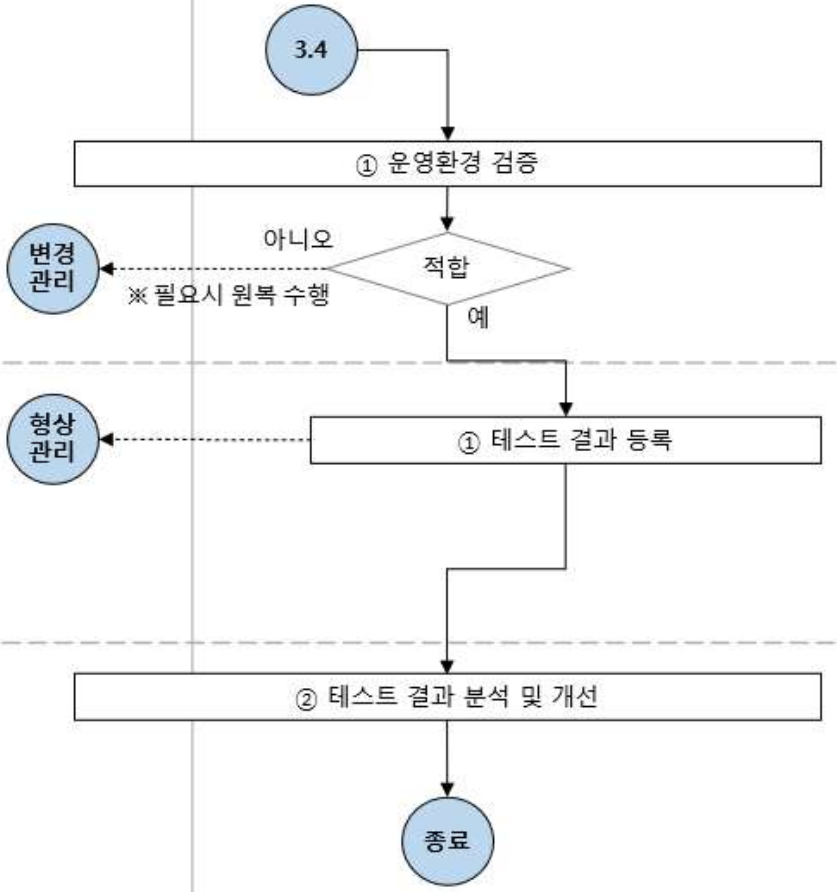
1) 주요 업무

주요 업무	세부 업무	수행 업무
1. 테스트 환경 구축	1.1. 테스트 수행 기준 정의	○ 테스트 대상 및 범위, 수행인력 등 변경 사항의 품질기준 충족 여부를 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.
	2.3. 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 운영자가 단위테스트를 수행한다.
	3.2. 통합테스트	○ 기능 변경이 타 시스템이나 서비스에 영향을 미치는 경우 운영자가 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
	3.4. 인수테스트	○ 운영기관 담당자(변경요청자)는 테스트환경 또는 검증환경에서 인수테스트를 수행하고, 변경 요구사항 구현의 완전성을 평가한다.
4. 운영환경 검증	4.1. 운영환경 검증	○ 운영환경에 배포된 변경사항에 대하여 서비스 정상 동작 여부와 핵심 기능을 중심으로 검증한다. ○ 운영환경 검증 결과 경미한 부적합이 확인된 경우 신규 변경요청을 등록하여 조치하고, 중대한 부적합이 확인된 경우 원복을 우선 수행한 후 신규 변경요청을 등록하여 개발환경 테스트 단계부터 재수행한다.
5. 테스트 결과 분석 및 개선	5.1. 테스트 결과 등록	○ 변경 요구사항 구현 결과가 서비스 품질기준에 부합하는지 확인하고 테스트 결과서를 작성하여 관리시스템에 등록·관리한다.
	5.2. 테스트 결과 분석 및 개선	○ 테스트 결과를 분석하고 향후 테스트 작업에 반영한다.

2) 수행주체별 표준절차 흐름도



주요업무	세부업무	운영기관	운영사업자
		담당자/관리자	운영자
4. 운영환경 검증	4.1 운영환경 검증		
5. 테스트 결과 분석 및 개선	5.1 테스트 결과 등록		
	5.2 테스트 결과 분석 및 개선		



바. 세부 수행 절차

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

(●: 정, ◑: 부)

단계	세부 절차	세부 수행 내용	운영기관 관리자/담당자	운영사업자 운영자
1. 테스트 환경 구축	1.1. 테스트 수행 기준 정의	- 운영자는 변경요청서, 변경계획서, 배포계획서 등을 분석하여 테스트 요구사항을 도출한다. - 운영자는 프로그램 소스코드, DB 스크립트, 시스템 성능 등 테스트 대상 및 범위, 테스트 수행 인력 등을 결정한다.	◑	●
	1.2. 테스트 환경 구성	- 운영자는 OS, DB, WAS 버전 등을 최대한 운영 환경과 유사하게 테스트 환경을 구성한다. - 운영자는 테스트 자동화 도구(JUnit 등) 활용을 위한 환경 설정을 지원한다.		●
2. 테스트 계획 수립	2.1. 테스트 계획 수립	- 운영자는 테스트 수행기준에 따라 테스트 유형(단위, 통합, 성능 등)을 결정한다. - 테스트 일정 계획을 수립하고, 담당자를 지정한다.	◑	●
	2.2. 테스트 설계	- 운영자는 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	운영기관 관리자/담당자	운영사업자 운영자
3. 개발환경 테스트	3.1. 단위 테스트	- 운영자는 개발환경에서 변경 기능의 단위 테스트를 수행한다. - 테스트 케이스의 예상 결과값과 테스트 수행 결과값을 비교하여 정상 동작 여부를 확인한다.		●
	3.2. 통합 테스트	- 운영자는 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 정상 동작 여부를 확인한다. - 변경 범위가 연계시스템에 영향을 미치는 경우 연계시스템 담당자가 연계서비스의 정상 동작 및 데이터 정합성을 검증한다.	●	●
	3.4. 인수 테스트	- 운영기관 담당자(변경요청자)는 테스트환경 또는 검증환경에서 인수테스트를 수행하고, 변경요구사항 구현의 완전성을 평가한다.	●	◑
4. 운영환경 검증	4.1. 운영환경 검증	- 운영자는 운영환경에 배포된 변경사항에 대하여 서비스 정상 동작 여부, 핵심 기능을 중심으로 검증하고, 변경요구사항 충족 여부를 검증한다. - 운영환경 검증 결과 경미한 부적합이 확인된 경우 신규 변경요청을 등록하여 조치한다. - 운영환경 검증 결과 중대한 부적합이 확인된 경우 원복을 우선 수행하고, 신규 변경요청을 등록하여 변경 범위에 따라 필요한 절차를 재수행한다.		●
5. 테스트 결과 분석 및 개선	5.1. 테스트 결과 등록	- 운영자는 테스트 수행 내역, 오류 발생 사항, 결과 확인 내역을 관리시스템에 등록·관리한다. - 테스트 결과 산출물은 ITSM 또는 형상관리 시스템에 등록할 수 있다.		●
	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 관리

측정 지표	측정 방법(예시)	측정 목적	측정 주기
테스트 성공률 (Test Success Rate)	(성공한 테스트 건수 / 당월 수행된 테스트 건수) X 100	테스트 수행 중 오류 없이 성공한 비율 관리	당월
테스트 커버리지 (Test Coverage Rate)	(테스트 수행 기능 수 / 당월 구현된 전체 기능 수) X 100	테스트 수행이 전체 기능 대비 차지하는 비율 관리	당월

아. 수행 검증

1) 검증 방법

○ 검증 체크리스트의 기준 항목으로 테스트관리 표준운영절차의 준수 여부와 이행 점검을 수행한다.

○ 개별기관 내 자체 프로세스 검증자는 내부 감사자의 자격 또는 ITIL에 대한 충분한 이해를 가진 자가 수행한다. (ITIL 관련 자격 권고)

○ 점검 결과는 자체 점검, 대외 감사 및 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	- 테스트 계획은 테스트 케이스 및 시나리오를 포함하고 있습니까?		• 테스트 계획서 - 테스트 케이스, 테스트 시나리오
	- 실제 운영환경과 유사한 상황을 가정하여 테스트를 수행할 수 있도록 테스트 데이터를 준비하고 있습니까?		• 테스트 계획서 - 테스트 데이터
테스트 결과 분석 및 개선	- 테스트 결과 산출물은 형상관리시스템에 등록하여 관리하고 있습니까?		• ITSM 내 테스트 결과 - 테스트 결과서
	- 결과를 검토하고 분석하여 개선하기 위한 활동이 수행되고 있습니까?		• 테스트 결과서

11. 연계관리 절차서

가. 개요

1) 목적

○ 연계 시스템 간 원활한 데이터 흐름과 상호운영성을 보장하고, 연계 요청 및 검토, 사전 연계 협의, 연계 계획 수립 및 검토, 검토결과 회신, 연계 결과 검토 절차를 표준화하여 서비스 연속성과 데이터 정합성을 확보한다.

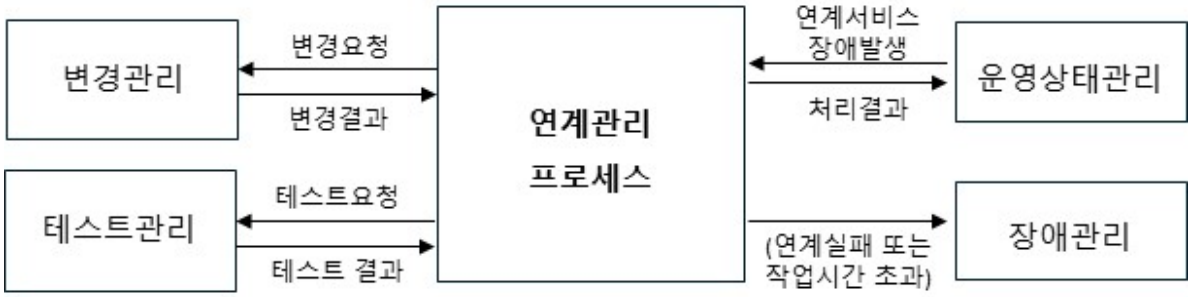
2) 적용 범위

○ 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, 사전 연계 협의 결과, 연계 계획서, 연계 계획 검토 결과서, 연계 결과 검토 내역, 연계 현황 등록·관리 내역을 관리한다. ※ ITSM 시스템을 사용하는 경우 시스템 내 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	○ 서비스 연계 현황 정보는 장애 발생 시 서비스 영향도·파급도 파악이 가능하도록 정보자원관리시스템(IRM)에 등록·관리하고, 변경사항 발생 시 현행화한다. ○ 연계서비스 중단 시 관련 시스템에 공지(공문 등)하고, 연계 요청, 승인, 검토 결과 및 결과 확인 등 연계관리 단계별 처리내역을 ITSM에 등록하여 이력을 관리한다. ○ 연계서버 인증서 등 서비스 유효성에 영향을 미치는 라이선스 등의 관리대장을 관련 기관과 공유하고 현행화한다.
정책 2	기준	연계표준을 적용하여 정보보유기관 간 원활한 서비스가 제공될 수 있도록 지원해야 한다.
	설명	○ 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 연계 관련 기관에 사전 공지해야 한다.
	설명	○ 변경작업자는 연계서비스 영향도를 파악하여 운영자와 운영기관 담당자에게 변경 작업계획서를 제공해야 한다. 연계서비스에 영향을 미치는 작업은 변경계획의 적합성, 영향도 검토 및 변경작업 완료 후 이행 적정성 점검을 수행하여야 한다. - 연계시스템 변경작업으로 인한 서비스 점검 요청 시 작업계획서를 제공하고, 연계 서비스 점검 결과서를 변경작업 결과 산출물에 포함하여 관리 ○ 운영기관 담당자는 관련 기관에 변경 작업계획을 공문 등으로 사전 공지한다.
정책 4	기준	연계서비스는 데이터 송수신 양방향에서 모니터링한다.
	설명	○ 연계 송수신 양방향 교차검증 체계를 운영한다. - 데이터 수신기관은 정상 수신 여부를 모니터링하여 이벤트 감지 시 송신 측에 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, 응용 애플리케이션 시스템 간 데이터 송·수신이 가능하도록 지원
연계 장애	외부 연계기관의 API 등 연계서비스에 의해 발생한 장애를 말한다.
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
정보자원관리시스템(IRM)	「전자정부법」 제47조제3항에 따라 행정안전부장관이 구축·운영하는 시스템을 말한다.

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, 연계 시스템 변경에 따른 영향도 및 서비스 연계 현황의 등록·현행화 여부를 확인 ○ 연계 계획의 적정성 검토 ○ 연계 시스템 변경에 따른 리스크 평가 및 관리 ○ 연계 작업 관련 이해당사자 간 조율 및 의사소통 창구 - 정보보유기관 간 유기적 협조체계 관리 포함
수탁기관 또는 운영사업자	운영자	○ 운영기관과의 계약을 통해 정보시스템의 운영, 유지보수 및 연계작업을 담당하는 수탁기관 또는 운영사업자 ○ 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 개발 후 단위 테스트 수행 ○ 연계 후 시스템 로그 분석 및 성능 점검 ○ 연계 프로세스 성능 및 부하 테스트 수행 ○ 연계 프로세스 변경 및 데이터 오류 수정 ○ 테스트 중 발견된 결함 분석 및 수정 ○ 연계 테스트 및 변경작업 결과 검토 및 승인 ○ 테스트 결과 보고서 작성 및 이슈 보고

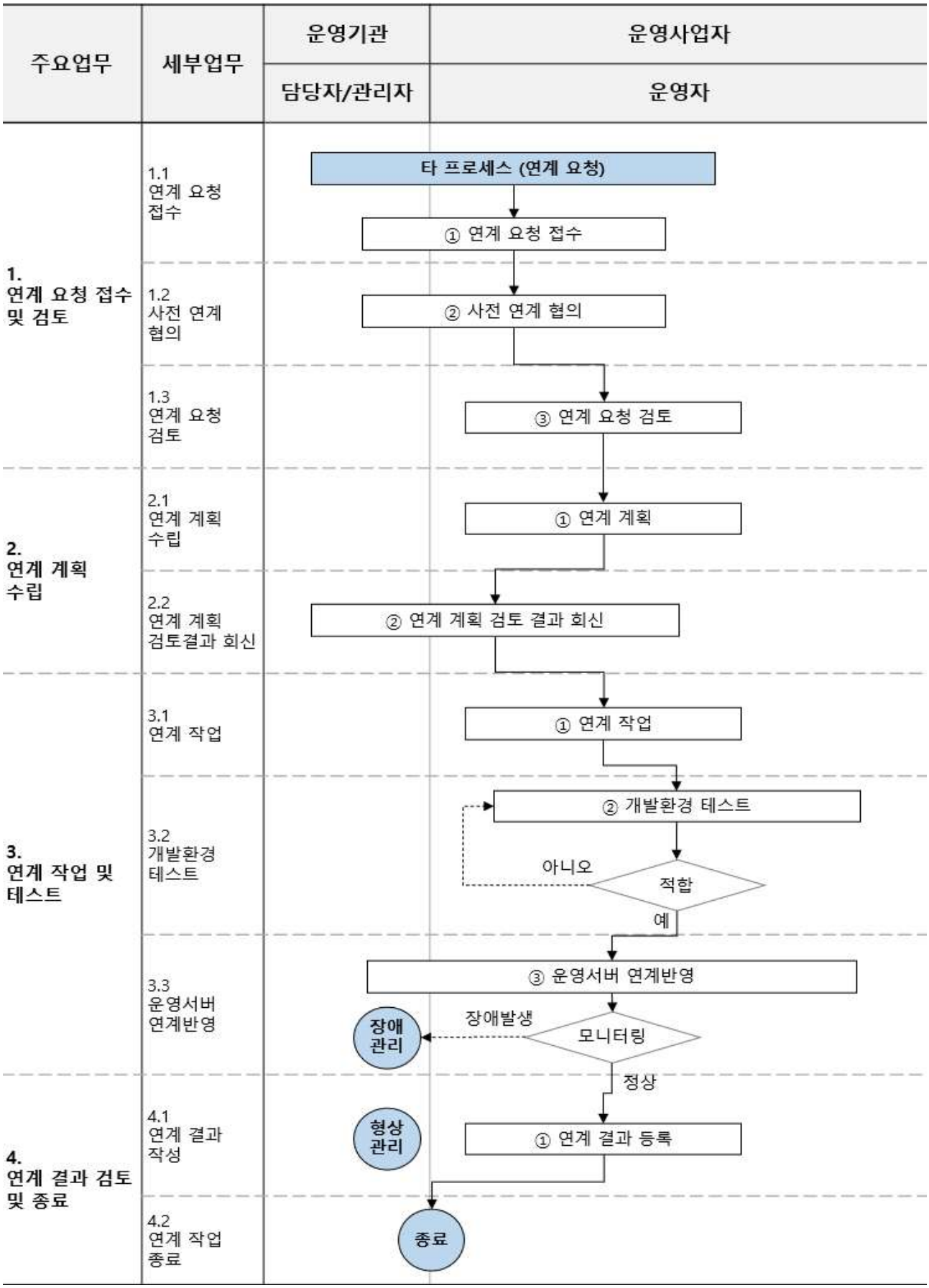
마. 표준절차 흐름도

○ 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	○ 연계 기관 간 환경 및 제약사항을 확인하고 연계 가능 여부를 검토한다.
2. 연계 계획 수립 및 검토	2.1. 연계 계획	○ 연계 요청기관은 연계 계획서(아래 내용 포함)를 작성하고 연계 대상 기관에 검토를 요청한다. - 연계 계획에는 연계 근거, 연계 정보, 연계 방법 및 주기, 송수신 구분 등
	2.2. 연계 계획 검토 결과 회신	○ 연계 대상 기관은 연계 계획에 대한 검토 결과서를 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 연계 기능을 운영서버에 반영하고 장애 발생 여부를 모니터링한다.
4. 연계 결과 검토 및 종료	4.1. 연계 결과 등록	○ 운영자는 연계 완료 보고서를 작성하고 운영기관 담당자에게 보고한다. ○ 운영자는 변경된 연계 정보의 현행화를 실시한다.
	4.2. 연계 작업 종료	○ 운영기관 담당자는 연계 작업 이력을 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 관리자/담당자	운영사업자 운영자
1. 연계 요청 접수 및 검토	1.1.- ① 연계 요청 접수	- 연계 요청기관은 연계 요청서를 작성한다. - 연계 요청서에는 연계 근거, 연계 목적, 연계 항목, 연계 일정 등 연계 요구사항을 상세히 기술한다.	●	●
	1.2.- ② 사전 연계 협의	- 연계 요청기관과 연계 대상 기관 간 사전 연계 협의를 통해 연계 요청 세부 사항을 확인한다.	●	●
	1.3.- 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.- ① 연계 계획	- 운영자는 연계 정보, 연계 방식 및 주기, 송수신 구분 등을 포함한 연계 계획서를 작성하고 연계 대상 기관에 검토를 요청한다. - 연계 요청기관 담당자는 연계 대상 기관 담당자에게 연계 계획 검토를 요청한다.		●
	2.2.- ② 연계 계획 검토 결과 회신	- 연계 대상 기관은 연계 요청기관의 연계 계획을 검토한다. - 운영자는 연계 작업이 시스템에 미치는 영향을 평가하고, 연계 작업 진행 여부를 포함한 검토 결과서를 작성하여 회신하고, 관리 시스템에 등록한다.	◑	●

단계	세부 절차	세부 수행 내용	운영기관 관리자/담당자	운영사업자 운영자
3. 연계 작업 및 테스트	3.1.- ① 연계 작업	- 연계 요청기관의 운영자는 연계 계획 검토 의견 승인 이후 연계 작업을 수행한다. - 연계 작업은 연계 기능 개발, 테스트, 운영서버 반영 등 변경요청관리 절차를 준용하여 수행한다.		●
	3.2.- ② 개발환경 테스트	- 운영자는 개발환경에서 연계 기능의 단위 테스트를 수행한다. - 운영자는 테스트환경에서 연계 서비스의 통합테스트를 수행한다. - 연계 시스템 간 데이터 흐름 및 상호작용이 올바르게 작동하는지 검증한다.		●
	3.3.- ③ 운영서버 연계 반영	- 운영자는 테스트환경에서 테스트 완료된 연계 기능을 운영서버에 반영한다. - 운영자는 운영환경에서 연계 기능의 단위 테스트를 수행한다. - 운영자는 운영환경에서 연계 서비스의 통합 테스트를 수행한다. - 연계 요청기관과 대상 기관 및 관련 기관의 운영자는 연계 서비스 통합테스트를 수행하고 장애 발생 여부를 모니터링한다. ※ 관련 기관과 연계 기능 테스트가 불가능한 경우 자체 검증 기능(루프백 등)을 제공하여 통합테스트 진행	●	●
4. 연계 결과 검토 및 종료	4.1.- ① 연계 결과 등록	- 운영자는 테스트 결과를 확인하고 연계 완료 보고서를 작성하고 운영기관 담당자에게 보고한다. - 운영자는 변경된 연계 정보의 현행화를 실시한다. - 운영자는 변경된 내용이 있으면 서비스 연계 현황 정보를 정보자원관리시스템(IRM)에 등록한다.		●
	4.2.- 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 관리

측정 지표	측정 방법(예시)	측정 목적	측정 주기
연계 응답 속도 (Integration Response Time)	API 및 데이터 연계 평균 응답 시간 측정	연계 처리 요청 후 응답까지 걸린 평균 시간 관리	당월
연계 장애 발생률 (Integration Failure Rate)	(연계 장애 발생 건수 / 당월 연계 요청 건수) X 100	연계 오류가 발생한 비율 관리	당월
연계 장애 대응 시간 (Mean Time to Recover, MTTR)	장애 발생 시간 ~ 정상화 시간 측정	연계 장애 발생 시 정상 복구까지 걸린 평균 시간 관리	당월

아. 수행 검증

1) 검증 방법

○ 검증 체크리스트의 기준 항목으로 표준운영절차의 준수 여부와 이행 점검을 수행한다.

○ 개별기관 내 자체 프로세스 검증자는 내부 감사자의 자격 또는 ITIL에 대한 충분한 이해를 가진 자가 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	- 연계 요청은 연계 요청기관과 연계 대상 기관 담당자들이 사전 협의를 통해 검토하는 절차를 수행하고 있습니까?	적합/ 부적합	• ITSM 내 회의록 • 연계 요청서 • 사전 연계 협의 결과
	- 연계 환경 및 제약사항을 확인하고 연계 가능 여부를 검토하고 있습니까?		
연계 계획 수립	- 연계 계획은 연계 근거, 정보, 방법 및 송수신 구분 등 구체적인 사항을 포함하고 있습니까?		• ITSM 내 연계 요청 - 연계 계획서
	- 연계 작업 대상 기관은 연계 계획을 기반으로 연계 요청에 대한 검토 후 검토 결과서를 회신하고 있습니까?		• ITSM 내 연계요청 - 연계 계획 검토 결과서
연계 테스트	- 연계 관련 기관이 모두 참여하여 연계 테스트를 수행하고 운영서버 반영 후 장애 발생 여부를 모니터링하고 있습니까? ※ 관련 기관과 연계 기능 테스트가 불가능한 경우 자체 검증 기능을 제공하여 통합테스트를 진행한 경우 적합 판정		• ITSM 내 연계요청 - 연계 테스트 계획서
연계 결과 검토	- 운영기관 담당자는 연계 작업 결과를 확인하고 연계 완료 여부를 검토하여 작업종료를 승인하고 있습니까?		• ITSM 내 연계 요청 - 연계 결과서
	- 변경된 연계정보의 현행화를 수행하고 있습니까?		• 연계 정보 관리대장

12. 형상관리 절차서

가. 개요

1) 목적

○ 응용프로그램 형상관리는 소스코드, 산출물 등 형상항목을 식별하고, 형상관리 시스템을 통해 형상 변경의 승인·통제, 형상 감사 및 기록을 체계적으로 수행하여 형상항목의 추적 가능성, 최신성, 무결성 및 일관성을 확보하는 것을 목적으로 한다.

2) 적용 범위

○ 형상관리 절차는 행정·공공기관 정보시스템의 응용프로그램 변경이 발생하는 운영관리에 적용한다.
- 형상관리 대상 : 응용프로그램 개발·테스트·배포 과정에서 발생하는 소스코드, 산출물, 버전 정보, 변경이력, 형상관리도구 등록정보 및 형상 감사 기록

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 형상 변경 필요한 일체의 요청
프로세스 종료 조건	관리 대상 형상 식별에 따른 요청의 반려 형상 변경 처리 종료
증적(Output)	형상 관리 계획서, 형상 항목 목록, 변경 이력 기록, 형상 변경 완료 보고서 ※ ITSM 시스템을 사용하는 경우 시스템 내 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 도구 또는 관리시스템을 이용하여 관리한다.
	설명	○ 형상관리 대상항목별 적합한 형상관리 도구 또는 관리시스템을 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 변경요청 ID를 입력하여 추적이 가능하도록 관리한다. ○ 형상 항목의 변경 사항은 운영자 검토 후 승인 여부를 결정한다. - 관련 산출물의 미제출, 변경 내용 누락, 형상 버전 불일치 등 미흡 사항 발견 시 반려 처리하여 보완 ○ eGovFrame 개발도구(PMD)를 활용한 Code Inspection 등 소스코드 결함 검출 및 산출물의 품질관리 활동을 포함하는 형상 감사를 수행한다. ○ 형상 감사 결과 및 부적합 사항에 대한 시정조치 이력은 기록·관리한다.

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, 변경된 형상 항목이 적절히 관리되는지 검토하고 정책 준수 여부를 점검하는 활동

라. 역할 및 책임

○ 형상관리 절차를 수행하는 역할자의 책임은 다음과 같다.

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·승인 및 통제 ○ 변경 작업으로 인해 형상정보가 변경되는 경우 형상 감사 결과 및 조치기록 확인
수탁기관 또는 운영사업자	운영자	○ 운영기관과의 계약을 통해 정보시스템의 운영, 유지보수 및 변경작업을 담당하는 수탁기관 또는 운영사업자 ○ 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 및 변경 작업 수행 - 소스코드 변경 전 Check out, 변경 후 Check in 수행 - 변경작업 이후 형상정보 현행화 및 변경이력 관리 ○ 형상 데이터 백업 및 복구 절차 수행 ○ 형상 감사 계획 수립 ○ 형상 감사를 수행하고 감사 결과, 시정조치 요청 및 개선 결과를 기록·관리, 부적합 사항 보고 ○ 형상 감사 시 발견된 부적합 사항의 시정조치 계획 수립 및 조치 이행 ○ 시정조치계획을 점검하고 시정조치 내역 확인 ○ 형상 감사 결과 보고서 작성 ※ 품질관리자(QA)가 없는 경우 운영자가 형상 감사 수행

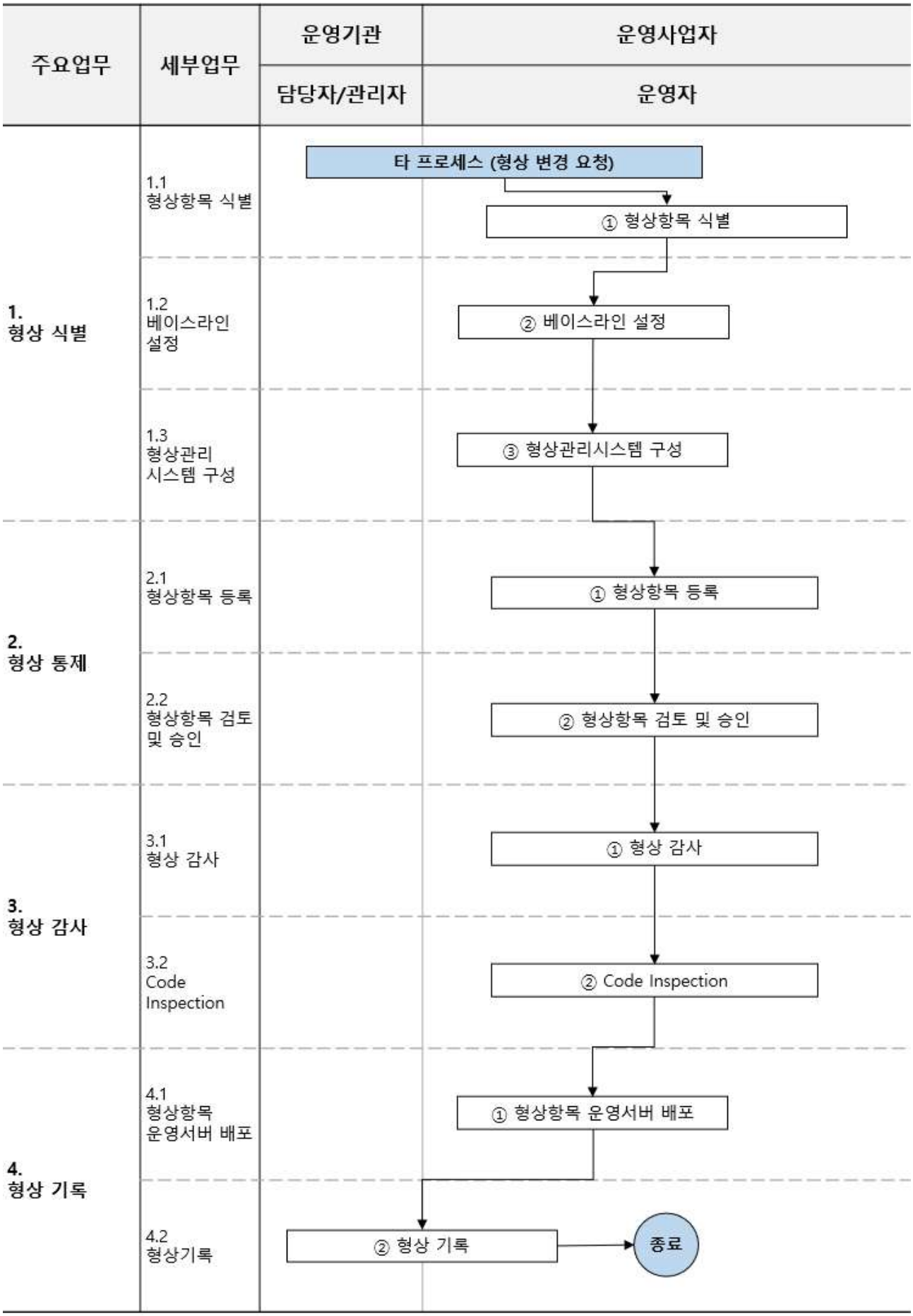
마. 표준절차 흐름도

○ 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 표준화한다.
	1.2. 베이스라인 (Baseline) 설정	○ 정보시스템 신규 구축 후 운영관리로 인수인계하는 시점, 주요 릴리스 및 정기 배포 완료 시점 또는 운영사업자 변경 시 이전 사업자로부터 인수인계 받는 시점에 베이스라인을 설정한다.
	1.3. 형상관리 시스템 구성	○ 형상관리도구를 구성하고 접근 권한을 관리한다.
2. 형상 통제	2.1. 형상항목 등록	○ 승인된 변경 작업에 따라 소스코드를 변경한 후 형상관리 도구에 반영(Check in)한다. ○ 변경 작업 관련 산출물 변경 후 형상관리시스템(ITSM 등)에 반영한다. ※ 소스코드 및 산출물 반영 시 변경 작업 사항을 상세히 작성하고 변경요청 ID를 반드시 입력하여 추적가능성을 확보
	2.2. 형상항목 검토 및 승인	○ Check in된 산출물을 검토하고 승인 여부를 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 형상 감사를 수행한다. - 개발 완료된 릴리스가 운영서버에 반영되기 전 변경 요구사항이 구현된 형상과 일치하는지 감사를 통해 검증 - 변경 작업 과정에서 수행된 테스트와 산출물 결과 등을 점검하여 누락된 요구사항이나 잘못된 반영 등을 확인 ○ 부적합 사항 발견 시 시정조치를 요청하고 감사 결과 및 조치 이력을 기록한다.
	3.2. Code Inspection	○ 형상관리도구에 반영된 소스코드의 개발표준 위배 여부, 소스코드 규칙 검증 등을 수행하여 결함 검출 등 품질 검사를 수행한다. ※ eGovFrame 개발도구 PMD Plug-in 활용 등
4. 형상 기록	4.1. 형상항목 운영서버 배포	○ 운영 반영 대상 형상항목의 승인 내역, 버전 및 반영 결과를 확인한다.
	4.2. 형상기록	○ 배포 후 형상항목의 변경이력을 최종 확인 후 검토 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	운영사업자
			관리자/담당자	운영자
1. 형상 식별	1.1.- ① 형상 항목 식별	- 운영자는 형상관리 대상항목을 정의하고 항목별 관리조직을 구성한다. - 형상 항목을 식별하고 버전관리 정책을 수립하여 관련조직에 전파한다.		●
	1.2.- ② 베이스라인 (Baseline) 설정	- 운영자는 인수인계 시점에 형상관리 베이스라인 1.0을 정의한다. - 운영자는 설정된 베이스라인에 따라 개발 환경을 구성한다.		●
	1.3.- ③ 형상 관리 시스템 구축	- 운영자는 형상관리 시스템(소스코드, 산출물 등)의 디렉토리를 구성하고 형상관리도구의 접근 권한을 등록 및 관리한다. - 운영자는 형상 감사를 위한 전자정부 표준 Inspection 룰셋 등 개발 표준이나 소스코드 규칙 등을 형상관리도구에 등록한다.		●
2. 형상 통제	2.1.- ① 형상 항목 등록	- 운영자는 승인된 변경 작업에 따라 프로그램 소스코드를 변경한 후 형상관리도구에 반영(Check-in)한다. - 운영자(또는 품질관리자 등)는 변경 작업 관련 산출물 변경 후 형상관리도구 또는 ITSM에 등록한다. - 운영자는 소스코드 반영 시 충돌 여부를 반드시 확인하고 소스코드 병합 (Merge) 후 통합테스트를 수행하여 정상 동작 여부를 검증한다. ※ 소스코드 및 산출물 반영 시 변경 작업 사항을 상세히 작성하고 변경요청 ID를 반드시 입력하여 이력 관리		●
	2.2.- ② 형상 항목 검토 및 승인	- 운영자는 형상관리 시스템에 반영된 소스코드 및 산출물을 검토하고 승인 여부를 결정한다. - 미흡사항(필수 산출물의 미제출, 변경사항 누락, 형상항목 버전 불일치 등) 발견 시 반려 처리하고 보완 요청을 수행한다.		●

단계	세부 절차	세부 수행 내용	운영기관	운영사업자
			관리자/담당자	운영자
3. 형상 감사	3.1.- ① 형상 감사	- 운영자(또는 품질관리자 등)는 개발 완료된 릴리스가 운영서버에 반영되기 전, 소스코드와 산출물 등의 형상 감사를 수행한다. - 구현된 형상과 변경 요구사항이 일치하는지 형상 감사를 통해 검증한다. - 변경 작업 과정에서 수행된 테스트 결과 등 산출물을 점검하여 누락된 요구사항이나 잘못된 반영 등 부적합 사항 발견 시 시정 조치를 요청하고 조치 이력을 기록·관리한다.		●
	3.2.- ② Code Inspection	- 운영자(또는 품질관리자 등)는 소스코드의 개발표준 위배 여부, 소스코드 규칙 검증 등 품질 점검을 수행한다. - 미흡사항 발견 시 시정조치를 요청하고 조치 이력을 기록·관리한다.		●
4. 형상 기록	4.1.- ① 형상 항목 운영서버 배포	- 운영자는 형상 감사 결과를 검토하고, 운영 반영 대상 형상항목의 승인내역, 버전 및 반영 결과를 확인한다.		●
	4.2.- ② 형상 기록	- 운영기관 담당자는 형상항목의 변경이력, 감사 결과 및 조치 이력을 최종 확인 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 관리

측정 지표	측정 방법(예시)	측정 목적	측정 주기
형상 감사 수행률 (Configuration Audit Execution Rate)	(실제 수행된 감사 횟수 / 계획된 감사 횟수) X 100	정기적으로 수행된 형상 감사 비율 관리	반기
형상 항목 무결성 유지율 (Configuration Integrity Maintenance Rate)	(무결성이 확인된 형상 수 / 당월 전체 변경 형상 수) X 100	형상 변경 후 변경 이력이 정상적으로 관리되는 비율 관리	당월
형상 오류 탐지율 (Configuration Error Detection Rate)	100 - ((탐지된 오류 수 / 당월 전체 변경 항목 수) X 100	형상 변경 후 발생한 오류 탐지 비율 관리	당월

아. 수행 검증

1) 검증 방법

○ 검증 체크리스트의 기준 항목으로 표준운영절차의 준수 여부와 이행 점검을 수행한다.

○ 개별기관 내 자체 프로세스 검증자는 내부 감사자의 자격 또는 ITIL에 대한 충분한 이해를 가진 자가 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 형상 감사 이력
	- 형상항목의 무결성과 신뢰성을 보증하기 위한 검토 및 승인 활동이 진행되고 있습니까?		• ITSM 기록 또는 형상항목 변경이력
형상 감사	- 형상 감사가 계획되고 수행되고 있습니까?		• ITSM 기록 또는 형상 감사 이력
	- 감사의 결과는 기록·관리되고 발견된 부적합 사항은 적절한 절차를 통해서 반영되고 있습니까?		• 형상 감사 조치 이력
형상 기록	- 형상 정보의 현행화·업데이트는 적절한 절차와 기준에 맞추어 관리되고 있습니까?		• ITSM 기록 또는 형상항목 변경이력

13. 운영상태관리 절차서

가. 개요

1) 목적

○ 정보시스템의 응용프로그램 기능 정상 여부, 배치 수행 상태, 로그, 응답 상태, API·연계 처리 상태 등 서비스 상태를 지속적으로 모니터링하고, 이상징후를 조치하거나 장애관리·문제관리 등 관련 절차로 이관하여 안정적인 응용프로그램 운영을 지원하는 것을 목적으로 한다.

2) 적용 범위

○ 운영상태관리 절차는 행정·공공기관 정보시스템의 응용프로그램 운영관리에 적용된다.
- 운영상태관리 대상 : 응용프로그램의 기능 정상 여부, 배치 수행 상태, 로그, 응답 상태, API·연계 처리 상태 등 서비스 상태 점검 및 이상징후 조치·이관 업무

3) 관련 업무 절차

○ 연관 선/후행 업무



○ 시작/종료/증적(Output) 조건

주요 업무	수행 업무
프로세스 시작 조건	응용프로그램 기능, 배치, 로그, 응답 상태, API·연계 처리 상태 등 서비스 상태에 대한 모니터링 또는 점검 필요사항 발생
프로세스 종료 조건	운영상태 점검·분석 및 조치 완료 또는 관련 절차 이관 완료
증적(Output)	운영상태 점검 결과, 조치 결과 및 관련 절차 이관 이력

나. 관리 정책

1) 정의

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

2) 정책 기준

정책	설명	
정책 1	기준	응용프로그램 및 서비스 상태의 지속적인 모니터링이 가능하도록 운영상태관리 계획을 수립하고 이행관리한다.
	설명	○ 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 분석하여 이상징후를 식별한다.
	설명	○ 운영시스템 환경에 따라 관리 항목을 개별 또는 통합 수집·축적 ○ 운영상태 데이터는 기관의 특성을 반영하여 분석 및 관리 주기를 설정한다. - 상태 데이터 분석 결과는 사후관리(예방점검, 최적화, 개선 등)에 활용한다.
정책 3	기준	운영상태 모니터링 결과는 운영기관 담당자 또는 관리자에게 수시 및 정기 보고한다.
	설명	○ 운영상태 모니터링 결과 장애, 반복 이상징후, 오류 등 발생 시, 장애관리·문제관리 등 관련 절차로 이관하여 처리하고, 운영기관 담당자에게 즉시 보고한다. - 운영상태 데이터를 분석하여 문서화하고 개선 조치를 수행한다. ○ 응용프로그램 운영환경에 따라 주별 또는 월별 운영상태 데이터 분석 결과를 운영기관 담당자에게 보고한다. ○ 운영상태관리 대상별 비상연락체계를 구성하여 관리한다. - 연계시스템을 포함하여 관리한다.
정책 4	기준	업무부하 기간 서비스 지연에 대비한 운영상태 집중 모니터링 및 긴급 대응 방안을 마련한다.
	설명	○ 운영상태를 지속적으로 모니터링하여 이용자 폭증에 따른 서비스 지연을 최소화하기 위한 예방점검 및 시스템 최적화 활동을 수행한다. - 운영상태관리 대상에 대해 예방점검 기준에 따라 정기점검을 수행하고, 발견된 문제점 및 개선방안을 지속적으로 관리한다. - 성능점검 후 응용프로그램 구조 개선 등 최적의 서비스 제공을 위한 활동을 수행한다.

다. 용어 정의

용어	설명
운영상태관리 (Operations State Management)	응용프로그램의 기능 정상 여부, 배치 수행 상태, 로그, 응답 상태, API·연계 처리 상태 등 서비스 상태를 모니터링하고, 이상징후를 식별하여 조치하거나 장애관리·문제관리·변경관리 등 관련 절차로 이관하는 활동
가용성 (Availability)	서비스 및 시스템이 정상적으로 운영될 수 있는 시간의 비율
부하 분산 (Load Balancing)	다수의 서버에 트래픽을 분산하여 서비스 성능 및 가용성을 유지하는 기법
로그 분석 (Log Analysis)	응용프로그램 및 서비스 로그를 분석하여 오류, 지연, 처리 실패 등 운영상태 이상징후와 성능 문제를 식별하는 과정
이벤트 관리 (Event Management)	정보시스템의 인프라, 클라우드 자원, 운영도구 등에서 발생하는 상태 변화, 임계치 초과, 오류 알림 등 운영 이벤트를 감지·분석·조치·이관하는 절차

라. 역할 및 책임

○ 운영상태관리 절차를 수행하는 역할과 책임은 다음과 같다.

구분		내용
운영기관 (응용프로그램의 운영관리에 최종 책임지는 기관)	관리자	○ 정보시스템 관련 담당자의 상위 책임자 또는 부서장 ○ 운영상태관리 관련 의사결정 ○ 응용프로그램 운영상태 및 성능 보고서 검토 및 승인 ○ 응용프로그램 성능 개선 및 운영 최적화 계획 검토 및 승인
	담당자	○ 운영상태관리 대상 응용프로그램 또는 서비스의 업무 담당자 역할 수행 ○ 운영상태관리 계획 검토 및 승인 ○ 운영상태 조치 결과 및 관련 절차 이관의 적정성 검토
수탁기관 또는 운영사업자	운영자	○ 운영기관과의 계약을 통해 응용프로그램 운영상태관리 업무를 담당하는 수탁기관 또는 운영사업자 ○ 운영상태관리 계획 수립 및 관리 - 운영상태관리 대상 선정, 정책 수립, 수립된 정책 반영·통제 - 운영상태관리 조직 구성 및 도구·자원 구성 ○ 응용프로그램 기능, 배치 수행상태, 로그, 응답 상태, API·연계 처리 상태 등 담당 영역의 상태 점검 ○ 응용프로그램 운영상태 모니터링 및 일일 점검 수행 ○ 운영상태 점검 보고서 작성 및 운영기관 보고 ○ 운영상태 모니터링 및 알림 시스템의 정상 작동 여부 검증 ○ 운영상태 데이터 수집 및 분석을 통한 이상징후 식별, 조치 및 관련 절차 이관 ○ 응용프로그램 또는 서비스 성능 저하 시 문제점 분석 및 개선 수행 ○ 응용프로그램 성능 최적화 및 장애 예방 ○ 서비스 상태 분석 및 문제 발생 시 초기 대응 수행 ○ 장애로 판단되는 경우 장애관리 절차에 따라 원인 분석 및 복구 지원 ○ 응용프로그램 운영상태 및 서비스 성능 점검을 위한 성능 테스트 및 부하 테스트 수행

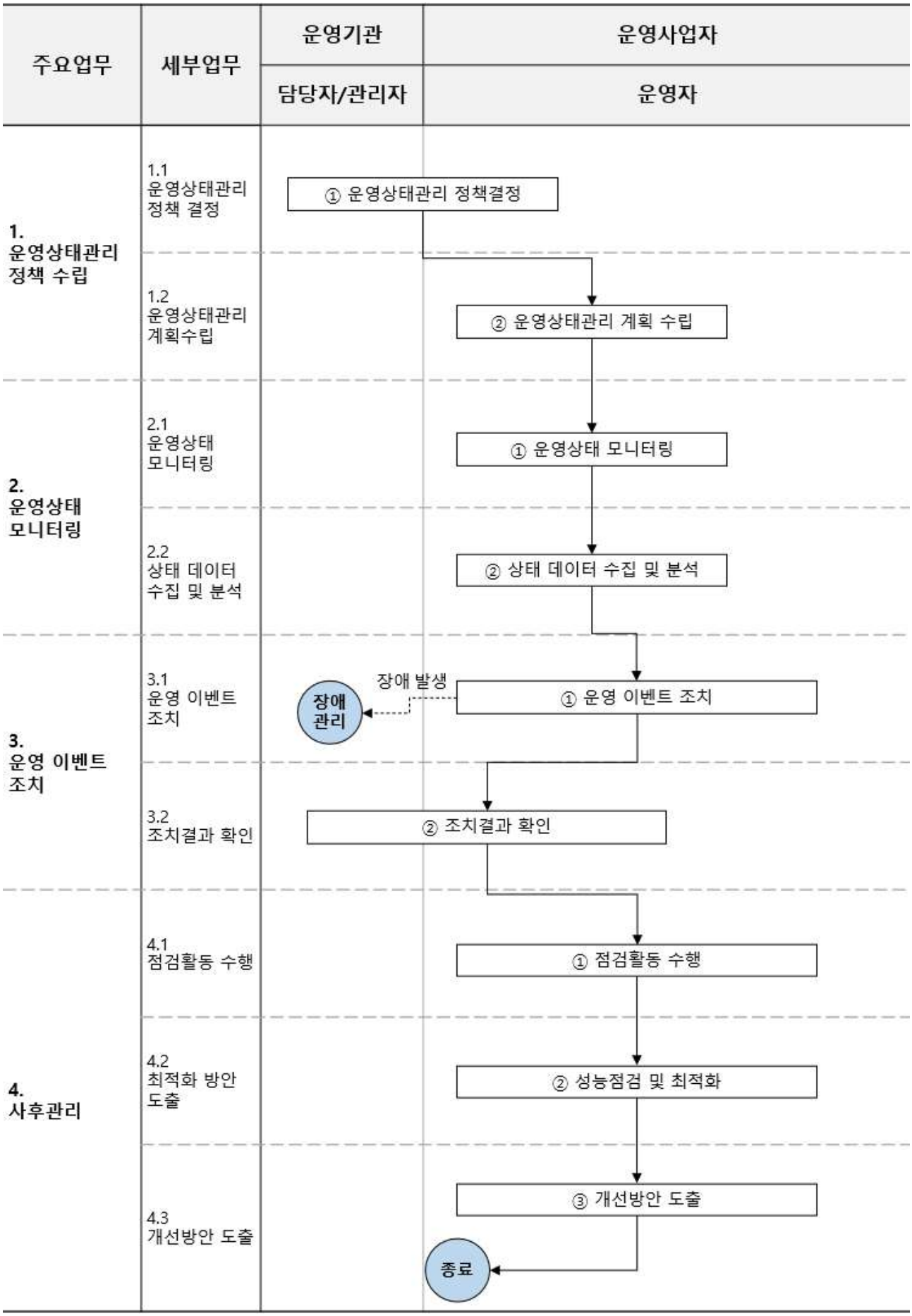
마. 표준절차 흐름도

○ 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	○ 운영상태관리 대상, 관리 항목, 관리 주기 등 운영상태관리 정책을 결정한다.
	1.2. 운영상태관리 계획 수립	○ 운영상태관리 정책에 따라 관리 계획을 수립한다. - 운영상태관리 조직 구성 및 역할과 책임 정의 - 운영상태 점검 및 테스트 등의 작업 일정 계획 ※ 성능점검의 경우 연 1회 이상 수행하도록 계획 수립 ※ 업무집중기간 전, 사전점검 수행하도록 계획 수립
2. 운영상태 모니터링	2.1. 운영상태 모니터링	○ 시스템 모니터링 도구 등을 통해 서비스 상태를 모니터링 한다. - 운영상태관리 대상인 응용프로그램, 배치, 로그, 응답 상태, API·연계 처리 상태 등에 대해 관리 계획을 수립하고 운영상태를 모니터링한다.
	2.2. 상태 데이터 수집 및 분석	○ 운영상태관리 대상별 관리항목에 대해 상태 데이터를 수집하고, 수집된 데이터는 분석이 가능하도록 축적·관리한다. ○ 운영상태 데이터는 용도에 맞게 분석하여 이상징후를 탐지하거나 성능 개선을 위한 최적화 등을 수행한다. ○ 모니터링 중 장애, 반복 이상징후 또는 변경 필요사항이 식별되는 경우 관련 절차로 이관한다.
3. 운영 이벤트 조치	3.1. 운영 이벤트 조치	○ 응용프로그램 응답 지연, 배치 실패, 로그 오류, API·연계 처리 오류 등 이상징후가 식별되는 경우 조치 또는 최적화 활동을 수행한다. ○ 장애로 판단되는 경우 장애관리 절차로 이관하고, 장애 원인 분석 및 신속한 복구를 지원한다. ○ 조치 내역 및 관련 절차 이관 이력을 기록하고 운영기관 담당자에게 보고한다.
	3.2. 조치 결과 확인	○ 운영기관 담당자는 조치 결과 및 관련 절차 이관 결과를 확인한다.
4. 사후관리	4.1. 점검활동 수행	○ 운영상태관리 대상에 대해 점검활동을 수행하고, 발견된 문제점에 대한 개선방안을 지속적으로 관리하여 잠재적 문제를 예방한다.
	4.2. 최적화방안 도출	○ 성능점검 후 응용프로그램 구조 개선, 응답성 개선 등 최적의 서비스 제공을 위한 활동을 수행한다.
	4.3. 개선방안 도출	○ 수집된 운영상태 데이터를 분석하여 성능 개선 방안을 도출한다. - 개선을 위해 변경관리, 문제관리 등 관련 절차로 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	운영기관 관리자/담당자	운영사업자 운영자
1. 운영상태 관리 정책 수립	1.1.- ① 운영상태 관리 정책 결정	- 운영기관 담당자와 운영자는 응용프로그램 환경을 고려하여 운영상태관리 정책을 결정한다. · 운영상태 관리 대상, 관리 항목, 관리 주기 등을 포함	●	●
	1.2.- ② 운영상태 관리 계획 수립	- 운영자는 운영상태관리 정책에 따라 운영상태관리 계획을 수립한다. · 운영상태관리 조직 구성 및 역할과 책임 정의 · 운영상태 점검 및 테스트 등의 작업 일정 계획 · 성능점검은 연 1회 이상 수행하도록 계획 수립 · 업무집중기간 전, 장애 위험요소에 대한 사전점검 수행 계획 수립		●
2. 운영상태 모니터링	2.1.- ① 운영상태 모니터링	- 운영자는 모니터링 도구 등을 통해 응용프로그램 응답 속도, 처리량, 세션 상태, 오류 로그 등 운영상태 데이터를 모니터링한다. - 운영자는 운영상태관리 대상별 임계치(Threshold)를 설정하고, 성능 저하 사전 감지 및 알림 시스템을 구성한다.		●
	2.2.- ② 상태 데이터 수집 및 분석	- 운영자는 애플리케이션 응답 속도, 처리량, 세션 상태, 오류 로그 등 상태 데이터를 수집한다. - 주요 운영상태 이상징후의 분석이 가능하도록 축적하고 관리한다. ※ 오류 발생 빈도, 특정 시간대의 트래픽 집중 현상 등 파악		●

단계	세부 절차	세부 수행 내용	운영기관 관리자/담당자	운영사업자 운영자
3. 운영 이벤트 조치	3.1.- ① 운영 이벤트 조치	- 운영자는 응용프로그램 응답 지연, 처리량 저하 등 운영상태를 모니터링하고, 이상 징후 발생 시 신속히 대응한다. - 장애로 판단되는 경우 장애관리 절차로 이관하고, 로그 및 운영상태 데이터 분석을 통해 원인을 파악한다. - 장애 원인에 따라 응용프로그램 구조 개선, 응답성 개선 등 최적화 활동을 수행한다. ※ 장애 발생 시 장애관리 프로세스 적용		●
	3.2.- ② 조치 결과 확인	- 운영기관 담당자는 운영 이벤트 조치 후 모니터링 및 로그 분석을 통해 조치 완료 여부를 확인한다.	●	●
4. 사후관리	4.1.- ① 점검 활동 수행	- 운영자는 응용프로그램 기능, 배치, 로그, 응답 상태, API·연계 처리 상태 등 운영상태관리 대상에 대한 점검활동을 수행한다. - 자동화 도구나 스크립트를 활용하여 주기적인 점검 및 자동 리포트를 생성한다. - 점검활동을 통해 발견된 문제점을 지속적으로 개선하고 잠재적인 문제를 예방한다.		●
	4.2.- ② 최적화 방안 도출	- 운영자는 성능 점검을 통해 응용프로그램 구조 개선, 응답성 개선 등 최적의 서비스 제공을 위한 활동을 수행한다. ※ 응용프로그램 성능 개선: 코드 최적화, GC(가비지 컬렉션), 메모리 누수 제거 등 ※ 네트워크 최적화: 트래픽 라우팅 조정, 패킷 손실 분석 및 대응 등 기반 인프라 개선이 필요한 경우 관련 절차로 이관 ※ DB 성능 튜닝: 인덱스 추가, 쿼리 최적화 등 검토		●
	4.3.- ③ 개선방안 도출	- 운영자는 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)

○ 운영상태 관리지표를 도출하여 운영 품질 관리를 목표로 하며, 본 절차서에서는 KPI 표준안을 제시하고 개별기관별 운영 상황에 맞추어 조정하여 지표 관리

측정 지표	측정 방법(예시)	측정 목적	측정 주기
운영상태 모니터링 커버리지 (Monitoring Coverage)	전체 운영 자산 중 모니터링 적용 비율	주요 시스템, 네트워크, 응용프로그램의 모니터링 비율	당월
평균 응답 시간 (Average Response Time)	애플리케이션 및 API 응답 시간 측정	주요 서비스 응답 속도	당월
평균 장애 탐지 시간 (Mean Time to Detect, MTTD)	장애 발생 로그 분석 (발생 시간 ~ 인지 시간)	장애 발생 후 감지까지 걸린 평균 시간	당월

아. 수행 검증

1) 검증 방법

○ 검증 체크리스트의 체크 항목 기준(ITIL 표준 준용)으로 표준운영절차의 준수 여부와 이행 점검을 수행한다.

○ 개별기관 내 자체 프로세스 검증자는 내부 감사자의 자격 또는 ITIL에 대한 충분한 이해를 가진 자가 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	- 응용프로그램 및 서비스 상태의 안정적 운영을 위해 운영상태관리 대상을 정의하고 모니터링하고 있습니까?	적합/ 부적합	• 운영상태관리 대상
	- 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?		• 조치 이력 (ITSM 내 조치 및 이관 이력)
	- 운영기관 담당자는 운영 이벤트 조치 결과의 검토·확인을 수행하고 있습니까?		• 조치 이력 확인 결과
사후 관리	- 잠재적 장애·문제 예방을 위해 운영상태관리 대상에 대한 예방점검 활동이 진행되고 있습니까?		• 점검 이력
	- 성능점검을 수행하여 최적화 방안을 도출하는 등 성능관리가 수행되고 있습니까?		• 성능관리 이력
	- 잠재적 위험요소가 있는 문제 등에 대해서는 개선방안을 도출하는 등 관리가 수행되고 있습니까?		• 개선계획 수립