백석대학교
BAEKSEOK UNIVERSITY

정보시스템 재난 대비
위기관리 대응절차

2025. 10.

전산정보원

■ 문서 변경 이력

개정 번호	제정	개정	문서명
9.0	2017.03.02	2025.10.01	정보시스템 재난 대비 위기관리 대응절차

버전 번호	일자	변경 항목	변경 내용	작성자	검토자	승인자
1.0	2017.03.02	-	▪ 최초 제정	김대용	이문재	임중수
1.1	2017.07.17	장애관리	▪ SLA 협약에 따른 장애관리 등급 및 기준 갱신	김대용	이문재	임중수
2.0	2018.05.27	장애관리 기본사항	▪ SLA 협약에 따른 변경 갱신 ▪ 조직도 갱신	김대용	이문재	임중수
3.0	2019.09.16	장애관리 기본사항	▪ SLA 협약에 따른 변경 갱신 ▪ 조직도/비상 연락망 갱신 ▪ 장애 감지 프로세스 수정 ▪ 보고서 샘플 추가	김대용	이문재	임중수
4.0	2020.12.01	장애관리 기본사항	▪ SLA 협약에 따른 변경 갱신 ▪ 조직도/비상연락 갱신 ▪ 장애 처리방안 수정 ▪ 보안장비 관리매뉴얼 추가	김대용	이문재	임중수
5.0	2021.11.10	문서명 변경 재난대비 절차 추가	▪ 문서명 변경: 장애복구 매뉴얼 → 재난대비 위기관리 대응절차 ▪ 위기대응 절차항목 추가 ▪ 업무 영향도 분석방안 추가	김대용	이문재	이성진
6.0	2022.12.02	재난복구 내용 보완	▪ 조직도/비상연락 갱신 ▪ 재난복구 수준별 유형 갱신	김대용	이문재	이성진
7.0	2023.03.27	조직도 비상연락 갱신	▪ 조직도/비상연락 갱신	이문재	이문재	홍경호
8.0	2024.08.14	시스템 개인정보 보유량 정보자산 관리대상 복구 우선순위 조직도 비상연락 갱신	▪ 문서변경이력 ▪ 시스템 개인정보 보유량 갱신 ▪ 정보자산 관리대상 갱신 ▪ 복구 우선순위 갱신 ▪ 조직도/비상연락 갱신	홍승우	노남철	홍경호
9.0	2025.10.01.	시스템 개인정보보유량 대응조직 최신화 비상연락망 갱신 유지보수 대응팀 갱신	▪ 시스템 개인정보 보유량 갱신 ▪ 조직도/비상연락 갱신	신서호	노남철	홍경호

목 차

1. 개요 ····· 1
1.1. 목적 ····· 1
1.2. 적용 범위 ····· 1
1.3. 재난 · 재해 · 위기 · 장애 정의 ····· 1
1.3.1. 재난 · 재해 정의 ····· 1
1.3.2. 위기 정의 ····· 2
1.3.3. 장애 정의 ····· 2
1.3.4. 정보자산 관리 대상 ····· 3

2. 재난위기 대응절차 ····· 6
2.1. 절차 개요 ····· 6
2.2. 단계별 정의 ····· 6
2.2.1. 1단계 : 예방 ····· 6
2.2.2. 2단계 : 대응 ····· 6
2.2.3. 3단계 : 복구 및 복원 ····· 6
2.2.4. 재해 복구 수준별 유형 ····· 6
2.3. 장애 대응 ····· 7
2.3.1. 목적 ····· 7
2.3.2. 전체 흐름도 ····· 7
2.3.3. 장애 감지 ····· 8
2.3.4. 장애 전파 ····· 8
2.3.5. 장애 분석 ····· 8
2.3.6. 장애 대응 절차 ····· 8
2.3.7. 장애 복구 ····· 9
2.3.8. 장애 복구절차 ····· 9
2.4 대응 조직 및 역할 ····· 10
2.4.1. 대응조직 개요 ····· 10
2.4.2. 대응조직 역할 ····· 10
2.4.3. 대응 조직도 ····· 11
2.4.4. 개인정보처리시스템 위기 발생시 ····· 12
2.4.5. 유관기관 현황 ····· 12
2.5. 재난 등에 따른 파급효과(정보 유출, 손실, 훼손 등) 및 초기 대응방안 ····· 12
2.5.1. 위기의 정의 ····· 12
2.5.2. 위기 등급의 분류 ····· 13
2.5.3. 위기 등급별 대응 계획 ····· 13
2.6. 정보시스템 백업 및 복구 우선순위, 목표시점 · 시간 ····· 13
2.6.1. RTO와 RPO의 정의 ····· 13
2.6.2. 위기 등급별 복구 소요시간 ····· 14
2.6.3. 장애 단계별 판단기준 (목표 시점 · 시간) ····· 14
2.6.4. 업무 영향도 분석 ····· 14
2.6.5. 복구 우선순위 ····· 15

2.7. 정보시스템 백업 및 복구방안 (복구센터마련, 백업계약체결, 비상가동 등) ····18
2.7.1. 정보시스템 장애 복구 흐름도 ····18
2.7.2. 백업관리 ····18
2.7.3. 백업시스템 운영 현황 ····18
2.8. 실제 발생 가능한 사고에 대한 정기적 점검, 지속관리 및 사후처리 ····19
2.8.1. 정기적 점검 ····19
2.8.2. 지속관리 절차 ····19
2.8.3. 사후처리 및 운영방안 ····19
2.9. 표준화된 유형별 장애처리 방안 ····20
2.9.1. 유형별 효과적인 장애처리 방안(예시) ····20
- 서버 장애 ····20
- 스토리지 장애 ····21
- 백업 장애 ····21
- DBMS 장애 ····22
- 소프트웨어 장애 ····23
- 네트워크 회선 장애 ····23
- 네트워크/보안 장애 ····24

3 모의훈련 ····25
3.1. 장애 대응 모의훈련 ····25
3.1.1. 목적 ····25
3.1.2. 훈련 조직도 ····25
3.1.3. 훈련 주기 ····25
3.1.4. 훈련 결과 공유 ····25
3.1.5. 비상연락망 ····26

1. 개요

본 "정보시스템 재난대비 위기관리 대응절차" 는 백석대학교/백석문화대학교 정보시스템 운영 중 발생하는 화재, 홍수, 단전 등의 재해·재난으로 인한 서비스 영향을 최소화하기 위해 필요한 절차 및 흐름과 각 절차에서 수행되는 내용 및 기준을 관리한다.

1.1. 목적

위기관리 대응절차는 빠른 위기 사항의 인지 및 의사소통, 장애복구, 근본원인 분석 및 개선을 통한 재발방지 등 장애상황 발생시 신속하게 합의한 서비스 수준으로의 복귀를 목적으로 한다.

1.2. 적용 범위

- 정보시스템의 재난방지 위기대응 매뉴얼 및 대응절차 마련
- 정보처리시스템 등 백업 및 복구를 위한 조치사항

1.3. 재난 · 재해 · 위기 · 장애 정의

o 서비스시간 정의

2023년 3월에 ㈜인성정보와 체결한 서비스수준협약서에 근거하여 서비스 시간, 정보자산 중요도, 영향도, 심각도를 종합적으로 고려하여 장애등급을 정의하고 등급별 처리시간을 관리하고 있으며, 아래와 같이 그 수준과 관리기준을 정의하고 있다.

구분	대상 시간
서비스 시간	24시간 X 365일

구 분	판 단 기 준	비 고
관심 (Blue)	**◦ 장애 발생 직후 S/W 및 H/W 적인 FAIL OVER 등의 처리로 중단 없이 서비스가 제공되는 경우** ◦ 파일시스템이 RAID1으로 구성되어 디스크 하나에 장애 발생시 자동으로 FAIL OVER 되는 경우, 서버의 한쪽 Power Supply에 장애 발생으로 다른 한쪽으로 FAIL - OVER 되는 경우 ◦ 평상 시 운영절차에 의거 수행	징후감시 활동
주의 (Yellow)	**◦ 장애 발생 후 인지/접수 즉시 간단한 조치로 서비스 재개가 가능한 경우** ◦ 네트워크 라인의 절단, 비정격 전류 인입으로 일시적인 서버 중지, WEB/WAS, DBMS 등 주요 프로세스 일시장애 ◦ 임의 백업 수행, DATA 복구 계획 재점검 ◦ 비상연락망에 의해 연락체계 수립	협조체계 가동
경계 (Orange)	**◦ 장애 발생 인지 즉시 필요 사항 조치 후 1시간 내 서비스 재개가 가능한 경우** ◦ 응용 S/W의 오류로 서비스가 중지되어 해당 개발자가 조치해야 할 경우 ◦ 긴급 백업 수행, 대피 우선순위에 의거 장비 및 내역확인 ◦ 비상 연락망 가동 및 장비 반출계획 수립	대비계획 점검
심각 (Red)	**◦ 재난 발생으로 시스템실에 직접적인 피해가 발생한 경우** **◦ 교체에 많은 시간이 걸리는 H/W 부품 등의 파손이 대량 발생하여 2시간 이상 서비스가 불가능 한 경우** ◦ 대피 우선순위에 의거 장비 및 DATA미디어 반출	즉각 대응태세 돌입

1.3.1. 재난 · 재해 정의

전산시스템 구성요소(H/W, S/W, 설비, 인력)가 자연재난 · 재해, 인적재해 및 기타 원인에 의해 그 물리적 구성형태가 파괴되거나 정상적인 기능을 발휘할 수 없을 정도로 훼손되어 이를 복구하는데 상당한 시간이 소요되거나 또는 불가능하여 서비스를 제공할 수 없는 경우를 모두 재난 · 재해라고 한다

1.3.2. 위기 정의

전산시스템 구성요소(H/W, S/W, 설비, 인력)가 악성코드공격, 서비스 거부공격, 비인가접근공격, 복합구성공격 또는 인적 위해 및 기타원인에 의해 그 물리적 구성형태가 파괴되거나 정상적인 기능을 발휘할 수 없을 정도로 훼손되어 이를 복구하는데 상당한 시간이 소요되거나 또는 불가능하여 서비스를 제공할 수 없는 사안으로 예견될 때 이를 위기라 칭한다

1.3.3. 장애 정의

- 장애는 서비스 대상의 기능성 문제로 인해 정보서비스의 업무가 중단된 현상을 말하며, 장애등급 판정기준은 정보자산 중요도와 영향도에 따라 심각도를 판단한다.
- 장애로 관리되지 않는 의사 장애는 다음의 사항을 말한다.
  서비스 대상의 기능성에 문제가 없으나 사용자가 장애로 인식하여, 상주직원, PM 또는 관리조직(전산정보원)에 문의·접수되는 경우 (단순 사용법의 오류, 시스템 성능의 현저한 저하 등)
- 서비스 대상의 기능성에 문제가 있으나, 업무가 중단되지 않은 경우(이중화된 시스템의 장애 등)는 “등급별 가동률”, “장비별 가동률” 지표 측정 시 제외하고 평가한다.
- 합의된 시간 내 장애가 해결되지 못했다면, 그러한 장애들은 서비스 관리조직으로 회부된다.
- 장애발생 시, 우리 대학과 유지보수 업체 간의 장애에 대한 인지와 초점을 동일하게 유지해야 한다.
- 장애 이력관리 : 발생된 모든 장애에 대하여 발생부터 처리 완료 시점까지의 내용을 관리

o 서비스시간 정의

2023년 3월에 ㈜인성정보와 체결한 정보통신자원 통합유지보수에 근거하여 서비스 시간, 정보자산 중요도, 영향도, 심각도를 종합적으로 고려하여 장애등급을 정의하고 등급별 처리시간을 관리하고 있으며, 아래와 같이 그 수준과 관리기준을 정의하고 있다.

구분	대상 시간
서비스 시간	24시간 X 365일

o 핵심 업무별 중요도 구분

등급	등급분류 기준
A등급 (핵심 시스템)	- 업무 중요도가 매우 높은 핵심 시스템 - 장애 발생 즉시 학생 및 학교 전 직원에게 영향을 미치는 시스템 (학사 지원 서비스, 학교 직원 실시간 사용 서비스) - 지속적인 장애 시 민원 발생을 초래하는 시스템 - 장애 발생 시 개인정보 유출 위험소지 존재
B등급 (주요 시스템)	- 업무 중요도가 높은 시스템 - 업무시간 중에는 반드시 가동되어야 하는 시스템 - 학생지원 업무를 직/간접 지원하는 시스템 - 장애발생 시, 학교 일부 부서에 영향을 미치는 시스템
C등급 (기타 시스템)	- 업무 중요도가 보통 또는 낮은 시스템 - 일반 학생민원과 관련된 정보나 관련 자료를 제공하는 시스템

※. 시스템 개인정보 보유량(기준일: 2023.12.31.)

개인정보처리시스템명	연관 개인정보 파일명	정보주체수	항목
종합정보시스템	학생정보파일	131,018	일반/민감/ 고유실별정보
입학관리시스템	신입생정보파일	179,277	일반/민감/ 고유실별정보

1.3.4. 핵심 업무별 관리 대상

등급	등급분류 기준	등급별 관리 대상
A등급 (핵심 시스템)	o 업무 중요도가 매우 높은 핵심 시스템 o 장애발생 즉시 학생 및 학교 전 직원에게 영향을 미치는 시스템(학사 지원 서비스, 학교 직원 실시간 사용 서비스) o 지속적인 장애 시 민원 발생을 초래하는 시스템 o 장애 발생 시 개인정보 유출 위험소지 존재	o 서버 - 서버: 개발 및 테스트서버(R740), 종합정보테스트서버(R740), S2DDS DNS 관리-A(S2DDS 2500), S2DDS DNS 관리-S(S2DDS 2500), S2 DHCP 관리(Active)(X4150), S2 DHCP 관리(Stanby)(X4150), AhnLab V3 및 EPM 관리(R440), 통합블레이드서버(BL460c), 통합이력관리서버-문화대 TBCS(BL460c), 백석대 학생이력관리(백석대 BEST)(BL460c), 도서관 DB서버(R730), (신)_백업마스터서버(LC4000), 체육관 원격지 백업 서버(LC4000), TCMS 통합ODA DB1 19C, TCMS 통합ODA DB2 19C, 유무선 통합인증 시스템(R740), NTP 서버, 종합정보시스템 SVN - 가상화 서버: Prism 뉴타닉스 서버(DX2200 DX170r Gen10) [TCMS 수강신청 SUKANG#1, TCMS 수강신청 SUKANG#2, TCMS 전자출결 BUATT#1, TCMS 전자출결 BSCUATT#1, TCMS 신규 TCWAS#1,TCMS 신규 TCWAS#2, TCMS 신규 TCWAS#3, TCMS 신규 TCWAS#4, TCMS 신규 TCWEB#1, TCMS 신규 TCWEB#2, TCMS 신규 TCWEB#3, TCMS 신규 TCWEB#4, 신규 BSWAS1, 신규 BSWAS2, 신규 BSWEB1, 신규 BSWEB2, 접근통제솔루션(MACS), NMS(PRTG NMS)] o 스토리지 - 학사/행정통합 DB스토리지(HP 3PAR 7200), TCMS 통합NAS TCNAS(DX2200 170r Gen10) o 네트워크 - 라우터(NCS5001), 서버팜 스위치 2EA(Nexus 9372), 백본 스위치 2EA(Nexus 7706), Cisco SAN 스위치 2EA(MDS 9148 FC), 체육관 메인 스위치(9300-24S), L4 스위치 2EA(Application Switch 5224), L4 스위치-사이버캠퍼스 2EA(MPX 5905), LMS 스위치(Nexus 3172T), 10G_HCI스위치 2EA(Nexus 3172T), 네트워크 트래픽 관리시스템(TaskQoS N500-B10G) o 정보보호시스템 - 통합보안시스템#1(Axgate-20000), 통합보안시스템#2(Axgate-10000), DDoS 보안장비(one-d 5000), 서버팜 방화벽 2EA(TrusGuard 10000B), 모니터랩 웹방화벽(WIWAF 2000), TMS 위협탐지 관리(TESS TAS 2000), ChakraMax DB접근제어(Warevalley W-L8), 접근통제솔루션(MACS), 백석대 Secuve Tos Manager(RNC 115), 개인정보 접속기록관리(백석대), 개인정보 접속기록관리(문화대), 개인정보필터링-A(EU-4000), 개인정보필터링(EU-3000), AhnLab V3 및 EPM 관리 o 웹 서비스 - 대표홈페이지, 대표홈페이지 관리자, 통합인증로그인, 포털시스템, 종합정보시스템, 출결, 행정정보시스템, 수강신청시스템, 입시홈페이지, 정보시스템 접근제어 솔루션, 학생역량관리시스템, 교직과정, 백석톡 관리자, 백석대학교 스마트 출결 학생용(Android/iOS), 백석대학교 스마트 출결 교수용(Android/iOS), 백석대학교/백석문화대학교 도서관(Android/iOS), 클리커(Android/iOS) o 소프트웨어 - 전자결재시스템, eXSignOn SSO(SSO 3.0), WAS 미들웨어(WebtoB, JEUS Standard), 전자결재시스템, 백석대 학생이력관리, 유무선 통합인증 시스템, U-Check+ 전자출결, 백석문화대학교 홈페이지(Wizard 7), 클립리포트(CLIP Report 5.0), 학사/행정개발 Mybulider, eXPortal, eXBuilder 6, TCMS TCWEB#1, TCMS TCWEB#2, TCMS TCWEB#3, TCMS TCWEB#4, TCMS TCWAS#1, TCMS TCWAS#2, TCMS TCWAS#3, TCMS TCWAS#4 신규 BSWEB1, 신규 BSWEB2, 신규 BSWAS1, 신규 BSWAS

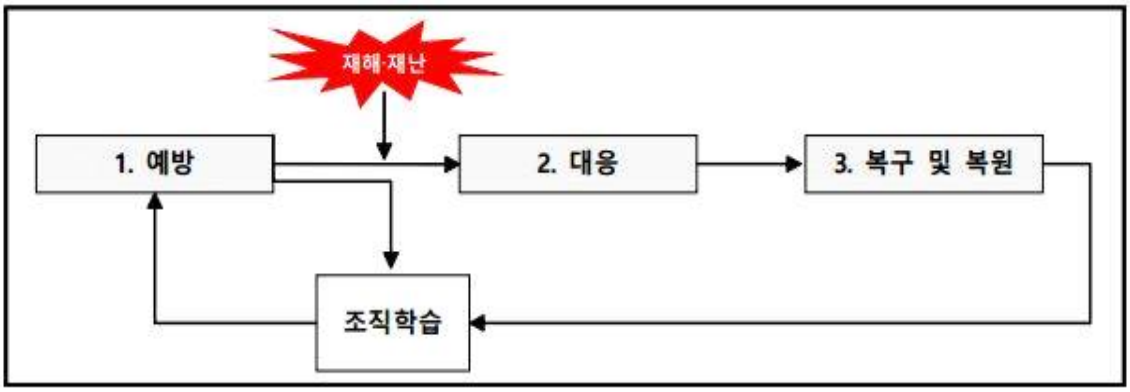
등급	등급분류 기준	등급별 관리 대상
B등급 (주요 시스템)	o 업무 중요도가 높은 시스템 o 업무시간 중에는 반드시 가동되어야 하는 시스템 o 학생지원 업무를 직/간접 지원하는 시스템 o 장애발생 시, 학교 일부 부서에 영향을 미치는 시스템	o 서버 - 신한은행 헤이영 중계서버(백석대)(DL380), 백석대 GSL 관리(R730), 백석 TALK 백석대(DL360), AD서버(DL320), NAS Gateway 2EA(3par SFC), 백석대 증명 발급 중계 서버 PC(Ncore), (구)DB서버#1(BL870c), (구)DB서버#2(BL870c), (구)WAS서버#1(BL870c), (구)WAS서버#2(BL870c), (구)WEB서버#1(BL870c), (구)WEB서버#2(BL870c), 한국어교육원 관리시스템(Bu_Global)(DX170r), 연말정산서버)(Rockey)(DX170r), 버스승차권 어플 관리서버(Bu_Ticket)(DX170r), 멀티미디어 서버(도서관) 2EA(BL380), 도서관 WEB서버(R730), 기숙사(생활관) 기존(R440), 기숙사(생활관) 신규(R440), 콘텐츠 제작용(R710), 문화대 GSL 관리(R720), 문화대 산단 직무교육 e-디딤돌 웹서버(R450), 백석 TALK 문화대(DL360), 백석대 사이버캠퍼스 WEB서버 4EA(R740), 교수학습개발원 CMS 컨텐츠 관리 시스템(R940), 문화대 자체원서접수(SMS전송관리)(R720), 예산서버(2950), 신한은행 헤이영 중계서버(문화대)(DL380), 교수학습개발원 장비 2EA, 연구비 관리서버(백석대 산학협력단)(R740), 연구비 관리서버(VM)(R740), RemoteCall 6.0, BSCC(BL380) o 스토리지 - 백석·문화 통합 NAS, (구)웹메일 2EA, 도서관 NAS 스토리지, CYBER LMS 스토리지 2EA, 콘텐츠 및 백업 스토리지, VM-LMS 8EA(Resin), VM-CMS 2EA(Resin) o 네트워크 - 메인 스위치: 글로벌 외식산업관(WS-C3650-24TD), 은혜관(HP-A5500 48G), 자유관(WS-C3650X-24T-S), 창조관 2EA(C9200L-24T-4X), 인성관(WS-C3560X-24T-S), 목양관(C9200L-24T-4X), 본부동 우측 2EA(WS-C3650-24TD), 본부동 좌측(WS-C3650-24), 예술동(C9200L-24T-4X), 조형관(9300-48S), 진리관(WS-C3560X-24T-S), 지혜관(WS-C3560X-24T-S), 승리관(WS-C3560X-24T-S), 학생복지동(WS-C3560X-24T-S), 음악관(C9200L-24T-4X), 교수회관(HP-1920-POE- 24g), 백석홀(HP-A5500 48G) - 스위치: 자유관(Cisco-9200L-24T) - 무선장비: PoE 스위치 81EA, AP 1389EA, APC 6EA o 정보보호시스템 - 블루엑스레이 매체제어-DLP(R230), COMVOY 컴보이(X3650) o 웹서비스 - 통계, 구글계정생성 관리자 화면, 구매자산관리 시스템, 도서관, 현대시 100년관, 백석목회지원센터, 백석역사관, 교수학습개발원 사이버캠퍼스, (구)교수학습개발원 사이버캠퍼스, 백석생활관, 평생교육원, 사회봉사센터, 장애학생지원센터, 산학협력단, LINC+ 사업단, 디지털 사업단, 무인항공센터, 실버센터, 국제교육센터, 온라인 디자인 공유 캠퍼스(한국, 중국, 일본) 발전기금, 설문, 백석대학교 부속기관, 도서관(서울), 백석톡(Android/iOS), 백석대 버스(Android/iOS), 백석대학교 도서관(서울)(Android/iOS) o 소프트웨어 - eXSurvey 설문조사시스템(eXSurvey), 웹방식 원격지원시스템, 교육통계솔루션(i-DAS), 백석 TALK 유지보수(Mthink), Google Gsuite, (구)WEB서버#1, (구)WEB서버#2, 백석대 사이버캠퍼스 WEB서버 4EA, 도서관 WEB서버, (구)WAS서버#1, (구)WAS서버#2

등급	등급분류 기준	등급별 관리 대상
C등급 (기타 시스템)	o 업무 중요도가 보통 이하 o 일반 학생 민원과 관련된 정보나 관련 자료를 제공	o 서버 - DSC 공유대학 서버(RC124-P4), 재해 DB 복구서버(DBBKTEMP)(DX170r) o 스토리지 - DSC 공유대학 NAS, TCMS 통합 Oracle Database o 정보보호시스템 - 망분리용 방화벽(TrusGuard 100B)

2. 재난위기 대응절차

2.1. 절차 개요

정보시스템 위기 발생 시 예방, 대응, 복구 및 복원으로 이루어지는 3단계를 체계적으로 구조화해야 함



2.2. 단계별 정의

2.2.1. 1단계 : 예방

- o 위기상황이 발생하기 전 예상되는 문제들을 미리 보완하고 대비
- o 위기대응 조직, 위기등급, 복구목표 등 위기대응 체계 검토
- o 주기적 백업 실시 및 위기대응 훈련 실시를 통해 위기대응 준비

2.2.2. 2단계 : 대응

- o 재난으로 위기상황이 발생하여 위기대응 체계에 따라 대응 실시
- o 위기대응 조직을 소집하고 위기등급을 정의하여 위기상황 선포
- o 비상연락체계를 가동하고 위기대응 조직의 역할에 따라 대응 실시

2.2.3. 3단계 : 복구 및 복원

- o 복구목표에 따라 우선순위가 높은 업무부터 복구 및 복원 실시
- o 복구 및 복원이 완료되면 위기상황의 종료를 선언하고 위기대응 시 이슈사항을 위기대응 체계에 반영하여 개선
- o 위기상황으로 인한 피해를 수습하고 위기내용 학습

2.2.4. 재해 복구 수준별 유형

유형	특징	장점	단점
미러 사이트 (Active-Active)	주센터와 동일한 수준의 정보기술자원을 원격지에 구축하여 두고 실시간에 동시 서비스를 하는 방식	복구시간 0 시간 데이터 유실(X)	고비용
핫 사이트 (Active-Standby)	주센터와 동일한 수준의 정보기술자원을 대기상태(Standby)로 원격지 구축 보유	실 전환 시간 필요 데이터 유실(X)	고비용
웜 사이트	핫사이트와 유사하나, 재해복구센터에 주센터와 동일한 수준의 정보기술자원을 보유하는 대신, 중요성이 높은 정보기술자원만 부분적으로 보유	상대적 저비용	데이터 유실(○)
콜드 사이트	데이터만 원격지에 보관하고, 이외 서비스를 위한 정보자원은 확보하지 않거나 장소 등 최소한으로만 확보하고 있다가, 재해 시에 데이터를 근간으로 하여 필요한 정보자원을 조달하여 정보시스템을 복구	최저비용	데이터 유실(○) 복구 장기화 낮은 신뢰성

2.3. 장애대응

2.3.1. 목적

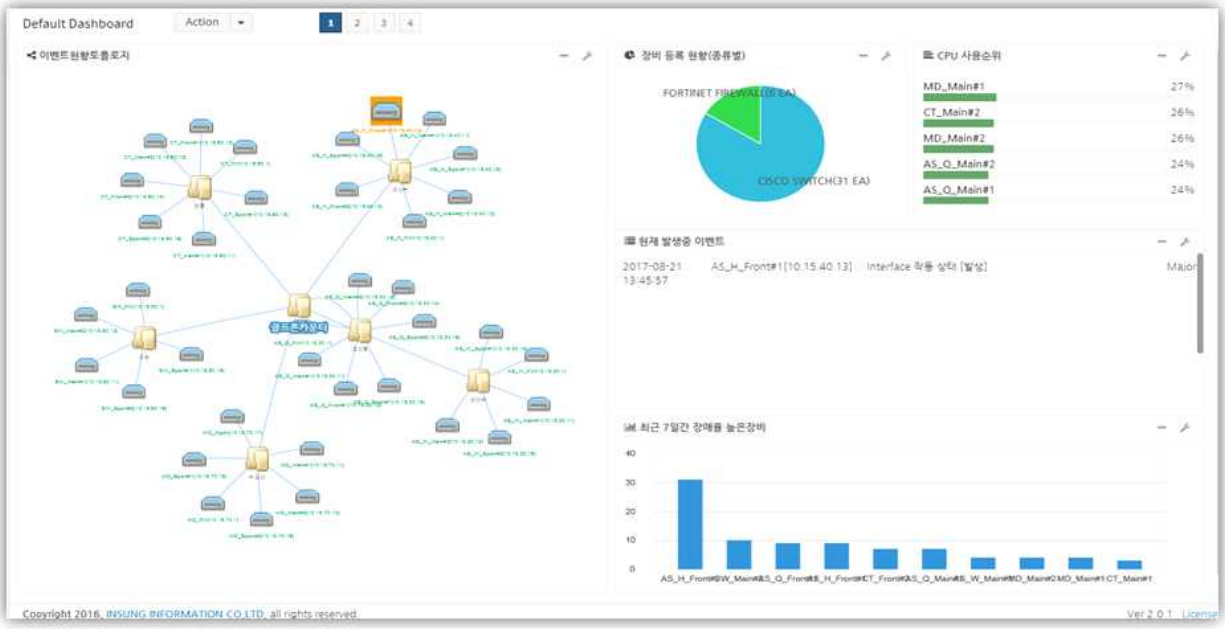
재난 위기 가운데에서도 서비스의 지연 및 중단을 직접 유발할 수 있는 장애를 별도분리하여 관리한다. 장애 대응은 장애가 발생하였을 때 신속한 상황 파악 및 판단을 통하여 장애원인을 분석하고 조치하여 장애로 인한 서비스 영향도를 최소화하는 것을 목적으로 한다.

2.3.2. 전체 흐름도

2.3.3. 장애 감지

IT Helpdesk 운영인력 및 상주운영 인력이 장애를 인지하거나, 통합관제 대시보드에서 자동 송부하는 장애경보를 확인하여 장애접수 즉시 초동 대응을 수행한다.

1. 통합관제 대시보드를 통하여 장애 이벤트 발생정보, 주요서버, DB, 회선 및 트래픽 현황이 실시간으로 모니터링되고 있다.
2. 문제 시 대시보드에서 경보가 발생하고 자동SMS 발송을 통하여 담당자에게 장애 상황이 전파된다.



2.3.4. 장애 전파

장애발생 인지 후 즉시(30분 이내) 장애 보고 프로세스에 따라 보고 및 상황 전파가 이루어 질 수 있도록 하며 유관사업자와 관련이 있는 사안일 경우 PM은 즉시 상황전파 및 협조요청을 한다.

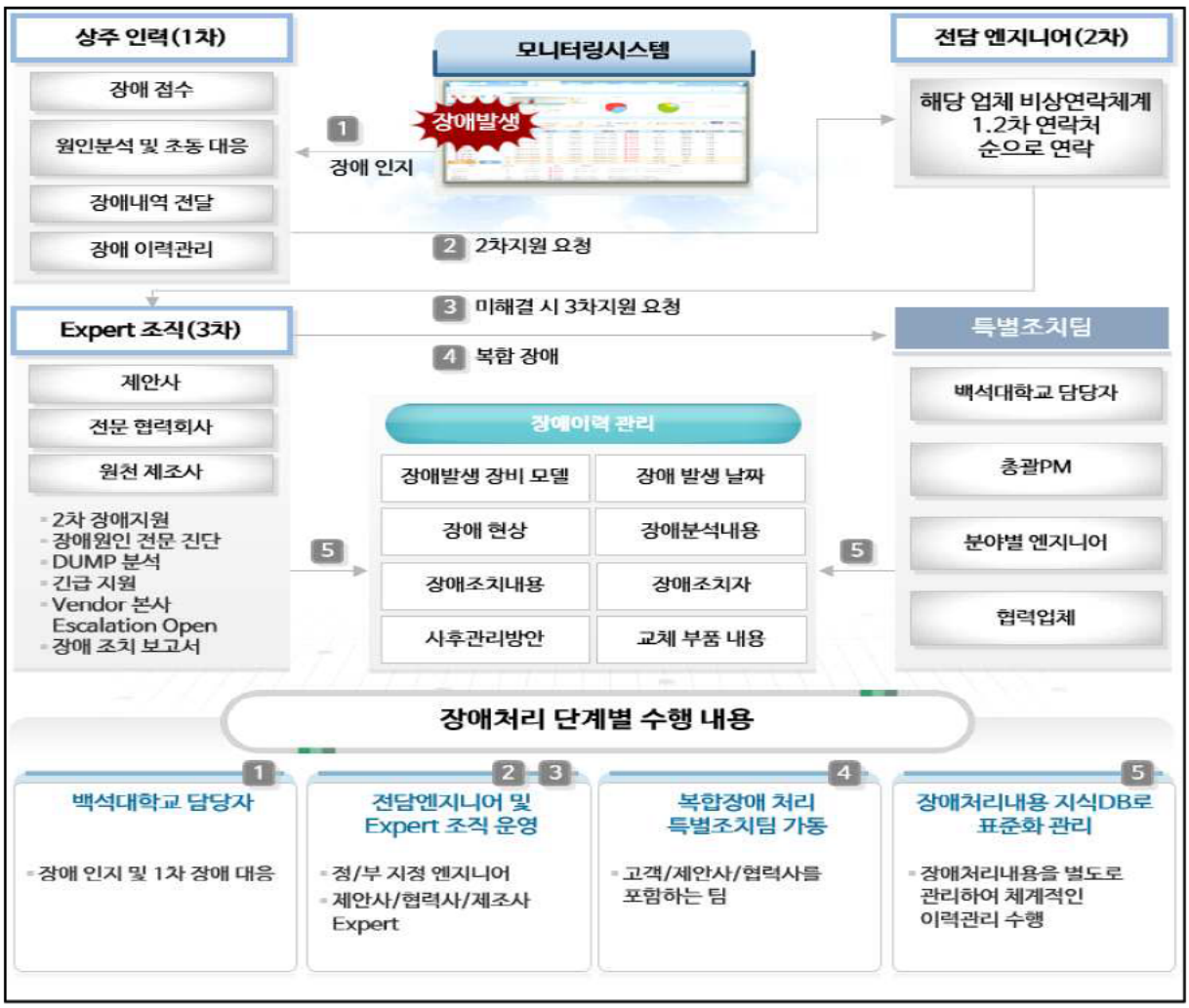
1. PM은 장애 현상 및 업무 영향도를 확인하여 장애등급을 분류하고 담당자에게 보고한다.
2. PM은 필요 시 유관사업자에 장애 상황을 전파한다.

2.3.5. 장애 분석

다음 절차에 따라 장애 분석을 수행한다.

1. IT Helpdesk/상주인력은 유사 장애 이력을 확인하여 장애조치 이력에 따라 초동/1차 지원한다.
2. 장애해결이 되지 않을 경우 유지보수 전담엔지니어 및 2차, 3차 지원 인력을 즉시 호출한다.
3. 유지보수 전담엔지니어는 SLA 기준 내 현장 도착 및 장애 원인 분석에 착수한다.
4. 현장도착 유지보수 전담엔지니어는 수집 가능한 로그 및 상황을 분석하여 원인을 파악한다.
5. 장애 유형 분류 및 근본원인을 분석하여 장애를 신속히 복구한다.
6. 원인 파악이 지연되는 경우 우선 장애 복구를 진행하고 원인분석 절차에 따라 분석을 수행한다.

2.3.6. 장애 대응 절차

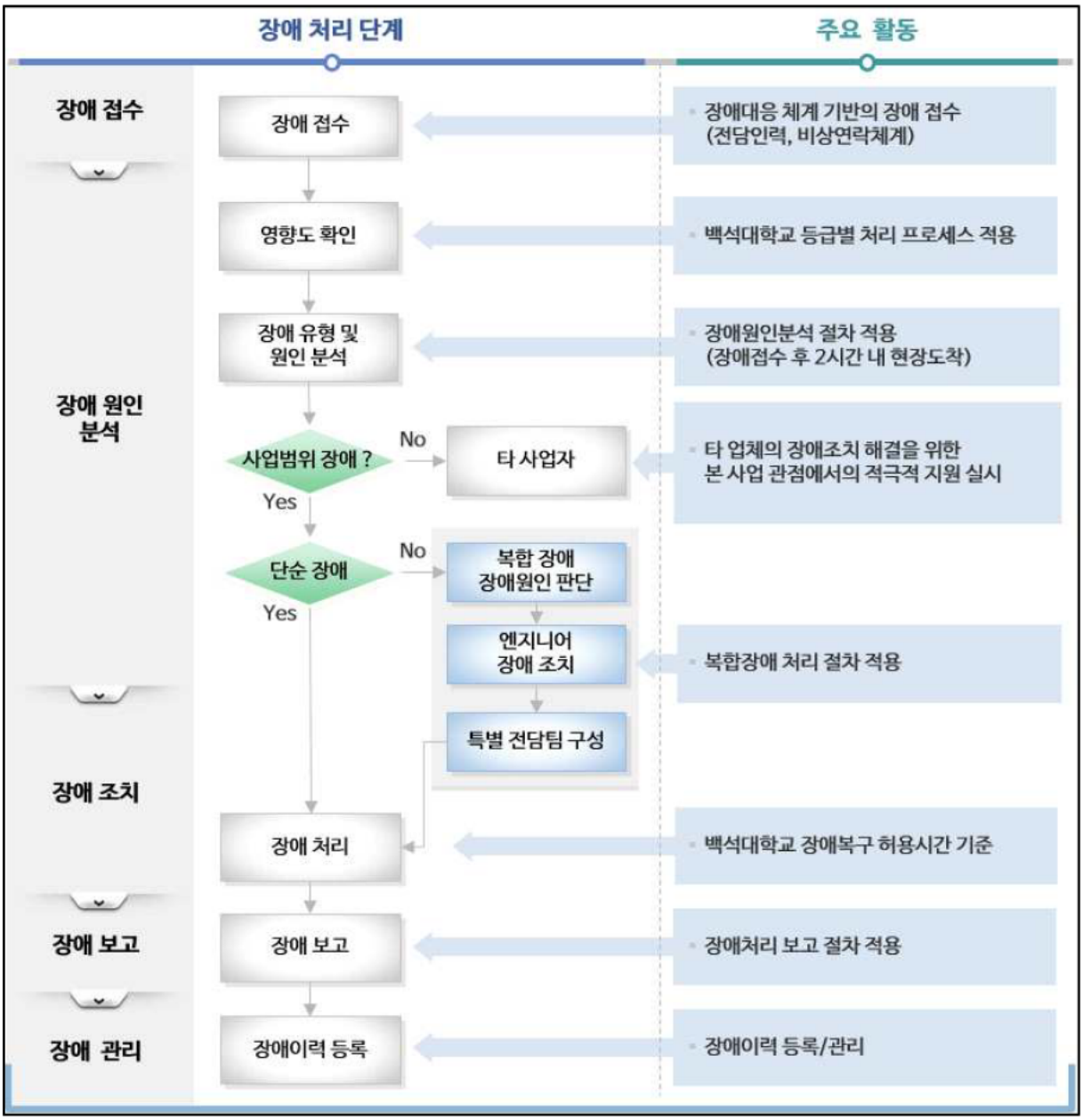


2.3.7. 장애 복구

다음 절차에 따라 장애 복구를 수행한다

1. 유지보수 전담엔지니어는 장애 복구방안에 대해서 PM에게 즉시 보고한다.
2. 필요할 경우 PM은 유관 사업자의 전담엔지니어와 복구방안에 대한 협의를 진행한다.
3. PM은 검토 후 복구 수행을 지시하며, 장애 복구방안에 대해 담당자에게 보고한다.
4. 유지보수 전담 엔지니어는 복구방안에 따라 장애 상황을 복구하고, PM에게 결과보고를 한다.
5. PM은 보고 접수 후 서비스 이상유무 확인 및 연관서비스 확인을 하며, 이상이 없음을 확인 후 1일 이내 담당자에게 장애 복구 완료 보고를 한다.
6. 복구 완료 보고 후 장애 이력 등록을 수행한다.

2.3.8. 장애 복구절차



2.4. 대응조직 및 역할

2.4.1. 대응조직 개요

o 정보시스템담당자는 대응조직원, 유관기관, 관련업체 등으로 이뤄진 비상연락망을 기록관리 해야 함

o 정보시스템담당자는 비상연락망을 주기적으로 검토하고 평시에도 연락 체계로 정보를 공유해야 함

o 위기상황 발생 시 위기상황 종료 시까지 비상연락망을 가동하여 신속한 대응을 지원해야 함

2.4.2. 대응조직 역할

o 개인정보처리시스템 책임자

- 위기대응 업무의 총괄
- 위기선포 및 위기대응 조직 구성원에게 업무를 지시
- 위기대응 상황 종료 시 결과 공유 등

o 전산정보원장(정보보안담당관)

- 정보시스템 위기대응 업무의 총괄
- 위기 선포 및 위기대응 조직 구성원에게 업무 지시
- 위기대응 상황 종료 시 결과를 공유 및 사후 조치 승인

o 전산개발운영팀장

- 위기상황 발생 시 각 업무기능의 복구 총괄
- 책임자의 위기선포에 따라 위기상황 전파
- 유관 기관과 연락망 가동 및 정보공유
- 평상 시 위기대응 절차 및 계획의 검토
- 위기 발생 시 사고분석, 대응, 복구 등의 처리와 재발방지에 대한 책임

o 개인정보처리시스템 담당자

- 위기상황 발생 시 각 업무기능의 현황 파악 및 복구 총괄
- 위기대응 절차 및 계획 수립 및 책임자의 위기 선포에 따라 위기상황 전파
- 비상연락망 및 유관기관과의 연락망 가동·정보공유
- 개인정보처리시스템 상시·정기점검 및 후속조치 실시

o 장애대응 기술 담당자(영역별 유지보수 업체)

- 정보시스템의 기술적 복구 및 운용 담당
- 개인정보처리시스템의 기술적 보안·복구 및 운용 담당
- 책임자 및 담당자 지시에 따라 필요한 활동 지원

2.4.3. 대응 조직도

o 백석대학교 장애보고 조직도

2.4.4. 개인정보처리시스템 위기 발생시

구분	주요 역할
개인정보처리시스템 책임자	· 위기대응 업무의 총괄 · 위기선포 및 위기대응 조직 구성원에게 업무를 지시 · 위기대응 상황 종료 시 결과 공유 등
개인정보처리시스템 담당자	· 위기상황 발생 시 각 업무기능의 현황 파악 및 복구 총괄 · 책임자의 위기 선포에 따라 위기상황 전파 · 비상연락망 및 유관기관과의 연락망 가동·정보공유 · 위기대응 절차 및 계획 수립 · 개인정보처리시스템 상시·정기점검 및 후속조치 실시
개인정보처리시스템 기술 담당자	· 개인정보처리시스템의 기술적 보안·복구 및 운용 담당 · 책임자 및 담당자 지시에 따라 필요한 활동 지원

2.4.5. 유관기관 현황

기관명	신고전화	비고
국가정보원	☎ 111	
교육사이버안전센터	☎ 053-714-0777	
KISA 보호나라/ 개인정보침해신고센터	☎ 118	

2.5. 재난 등에 따른 파급효과(정보 유출, 손실, 훼손 등) 및 초기 대응방안

2.5.1. 위기의 정의

o 재난으로 인한 정보시스템 위기는 아래와 같이 손실, 유출 및 훼손, 중단으로 구분됨

영역	위기	재해·재난 발생시 파급효과	초기대응방안
정보	유출	재해·재난으로 인해 개인정보가 유출된 경우	개인정보 침해사고 대응절차의 긴급대응 조치 방법의 개인정보 유출에 따라 대응
	손실 및 훼손	재해·재난으로 인해 정보가 유출되지는 않았으나 전부 또는 일부가 사용할 수 없게 된 경우	o 손실범위 확인(25%, 50%, 75%) o 긴급 복구 진행
서비스	중단	재해·재난으로 인해 정보 자체는 안전하게 보관되고 있지만 서버 또는 네트워크 장애 등으로 인해 서비스가 제공되지 못하는 경우	o 장애 위치 확인 o 긴급 절체로 서비스 제공 o 장애 복구 진행

2.5.2. 위기 등급의 분류

위기등급	내용
A등급	· 정보시스템 장애시간이 지정시간 이상 지속되는 경우 · 정보시스템 운용의 전면 중단 · 데이터의 중대한 손상으로 복구 불가 · 정보시스템 장비의 전원공급 단절
B등급	· 정보시스템 장애시간이 지정시간 이하로 지속되는 경우 · 정보시스템 운용 시 일부 기능 작동 중단 · 데이터의 일부 손상으로 복구 필요 · 정보시스템 장비의 전원공급 이상
C등급	· 정보시스템 장애가 일시적으로 발생한 경우 · 정보시스템의 운용이 일시적 작동 중단 · 데이터의 경미한 손상이나 운영에 지장 없음

2.5.3. 위기 등급별 대응 계획

위기등급	내용
A등급	· 발생 즉시 원장 또는 개인정보책임자에게 보고 · 원장 공식적인 위기 상황 선포 및 대응 총괄 · 필요시 외부 전문가 포함 위기 대응팀 구성 · 위기 종료 후 사후 조치 계획 수립 및 이행
B등급	· 전산정보팀장(정보보호) 수준에서 대응, 필요한 경우 원장, 개인정보책임자 또는 정보보안담당관에게 보고 · 위기대응팀 구성 · 위기 종료 후 원장 또는 개인정보책임자에게 공식 보고
C등급	· 담당자 수준에서 대응 · 해당 정보시스템 담당자로 위기대응팀 구성 · 위기 종료 후 원장(정보보안담당관) 또는 개인정보책임자에게 보고 · 정보시스템 담당자는 즉각적 조치가 가능한 경우 재발방지 조치 수행

2.6. 정보시스템 백업 및 복구 우선순위, 목표시점 · 시간

o 정보시스템의 위기 상황 발생 시 신속한 대응 및 복구를 위해 복구목표시간(RTO) 및 복구목표시점

(RPO)을 정의해야 함

o 복구목표는 정보시스템별 업무 영향도를 고려하여 우선 순위를 정해야 하며 위기선포 시부터 적용

2.6.1. RTO와 RPO의 정의

구분	세부사항
복구목표시간 [RTO] (Recovery Time Objective)	서비스 또는 사업 감내 목표를 초과하여 영향을 미치기 전 시점까지의 최고 중단 허용시간
	정보시스템의 책임자는 업무 영향도를 고려하여 복구목표 시간에 대한 정의 필요
복구목표시점 [RPO] (Recovery Point Objective)	업무를 수행하기 위해 손실된 데이터에 대한 유실 허용시점
	복구목표시점은 재해발생 직전까지 이며 재해복구시스템이 준비되어 있지 않은 시스템은 최종 백업 시점까지 복구목표

2.6.2. 위기 등급별 복구 소요시간

유형	RPO	RTO	내용
위기등급 C	24시간 이내	1시간 이내	정보시스템의 순단(대다수가 인지못함) 데이터의 경미한 손상으로 운영 지장없음
위기등급 B	24시간 이내	4시간 이내	장애시간이 지정시간(4시간) 이하 지속 데이터 일부 손실로 백업본 활용 복구 일부 시스템의 기능 동작 불가
위기등급 A	48시간 이내	24시간 이내	장애시간이 지정시간 이상 지속되는 경우 정보시스템 전면 중단에 따른 사용자 공지 필요
완전 장애 시 (주 전산센터 소멸)	5달 이내	4달 이내	현재 백업센터는 DB데이터 소산기능만 수행 인터넷 전용회선 포설, 장비 수급 및 설치 진행 인터넷 전용회선 포설 후 장비 셋업 및 보안 시스템 설정 (1개월)

2.6.3. 장애 단계별 판단기준(목표 시점 · 시간)

구분	판단기준	비고
관심 (Blue)	◦ 장애 발생 직후 S/W 및 H/W 적인 FAIL OVER 등의 처리로 중단 없이 서비스가 제공되는 경우 ◦ 파일시스템이 RAID 1으로 구성되어 디스크 하나에 장애 발생시 자동으로 FAIL OVER 되는 경우, 서버의 한쪽 Power Supply에 장애 발생으로 다른 한쪽으로 FAIL OVER 되는 경우 ◦ 평상 시 운영절차에 의거 수행	징후감시 활동
주의 (Yellow)	◦ 장애 발생 후 인지/접수 즉시 간단한 조치로 서비스 재개가 가능한 경우 ◦ 네트워크 라인의 절단, 비정격 전류 인입으로 일시적인 서버 중지, WEB/WAS, DBMS 등 주요 프로세스 일시장애 ◦ 임의 백업 수행, DATA 복구 계획 재점검 ◦ 비상연락망에 의해 연락체계 수립	협조체계 가동
경계 (Orange)	◦ 장애 발생 후 인지/접수 즉시 해당 필요 사항 조치 후 1시간 이내 서비스 재개가 가능한 경우 ◦ 응용 S/W의 오류로 인해 서비스가 중지되어 해당 업무 개발자가 조치해야 할 경우 ◦ 긴급 백업 수행, 대피 우선순위에 의거 장비 및 내역확인 ◦ 비상 연락망 가동 및 장비 반출계획 수립	대비계획 점검
심각 (Red)	◦ 재난 발생으로 시스템실에 직접적인 피해가 발생한 경우 ◦ 교체에 많은 시간이 걸리는 H/W 부품 등의 파손이 대량 발생하여 2시간 이상 서비스가 불가능 한 경우 ◦ 대피 우선순위에 의거 장비 및 DATA미디어 반출	즉각 대응태세 돌입

2.6.4. 업무 영향도 분석

o 변경관리, 릴리즈, 장애 대응 처리 활동 등 정보시스템의 변경을 수반하는 작업이 진행되는 경우 사전 유관 응용업무 및 인프라 영역에 대한 영향도 분석을 진행하여 장애 예방 및 성능저하를 방지

o 정보시스템 변경관리 계획서 상의 " 서비스 영향도 검토" 영역에서 유관 시스템 담당자와 변경 영향도 및 장애 위험 요소를 사전에 검토하여 장애 위험을 최소화 함

o 작성 예시

■ 서비스 영향도 검토

Example

서비스 영향 범위	장비 교체 시 Fail-over로 인하여 네트워크 순단 발생			
타업무 영향 범위	네트워크 순단으로 인하여 방화벽 인접 장비나 통과하는 트래픽에 영향이 있음			
영향도 검토여부	서버	무	업무 협의자	
	네트워크	유		한승훈(인성): 장비 교체, 패치시 발생될 문제 없음
	스토리지	무		
	백업	유		이정민(그루젠): 백업 스케줄을 고려한 일정 수립필요
	보안	유		양현순(서버보안): 발생될 문제 없음 전일환(UTM) : 외부 접근 데이터 차단이 아니라 영향 없음. 방화벽과 직연결 구간 아님 이승현(개인정보필터링): 발생될 문제 없음 이철희(웹방화벽): 발생될 문제 없음
	부대장비	무		
	관리용 SW	무		
협의결과 (특이사항)				

o 작업관련 영역별 업무 영향도 주요 확인 사항

업무 영역	주요 영향도 분석 사항
서버/스토리지	o 작업으로 인한 서비스 중단 발생 위험 파악 o 중단이 필요한 경우 사전 공지여부 및 다운타임 검증여부 o 디스크 교체 작업 시 RAid에 따른 무중단 Fail-over 여부 확인 o 스토리지 마운트 영역 확인 및 응용 서비스 연계 확인 o 통합관제 솔루션(SMEV)와 연동성 확인
네트워크/보안	o 작업으로 인한 서비스 중단 발생 위험 파악 o 보안 솔루션/시스템과의 영향도 사전 파악 o 보안 솔루션 변경에 따른 개인정보 필터링/접속이력관리 정상 동작확인 o 계정, 설정 변경 시 주요 서비스 영향 CAB으로 파악 o 특화된 시스템, 방화벽 정책 등 변경 시 반드시 유관 담당자 협의 필요
솔루션	o 전자결재, 수강신청 연계 등 주요업무 관련 요소 사전 분석결과 제시 o 미들웨어(Jeus), DBMS 등 서비스 직접 연계하는 솔루션 작업 시 o 업무 담당자 입회하에 CAB 분석으로 영향도 파악
부대장비	o 부대장비 중단에 따른 전산시스템 다운여부 사전 확인 o 전원점검 , 항온항습기 중단 등 전산실 중단 위험에 대한 CAB 회의 필수

2.6.5. 백업 데이터 표

o 시스템 장애 시, 백석대학교 서비스 품질관리(SLA Ver11.0)에서 정한 정보시스템 자산 1,2,3 등급을 기준하여 아래와 같이 우선순위가 정해지며, 동시에 동일 등급의 장애가 경우 아래와 같은 기준을 적용한다.

1) 학사 행정, 학교직원 실시간 사용 서비스 등 업무 중요도가 매우 높은 핵심 시스템 우선
2) 지속적인 장애 시 민원 발생을 초래하거나 개인정보 유출 위험 소지가 큰 시스템 우선

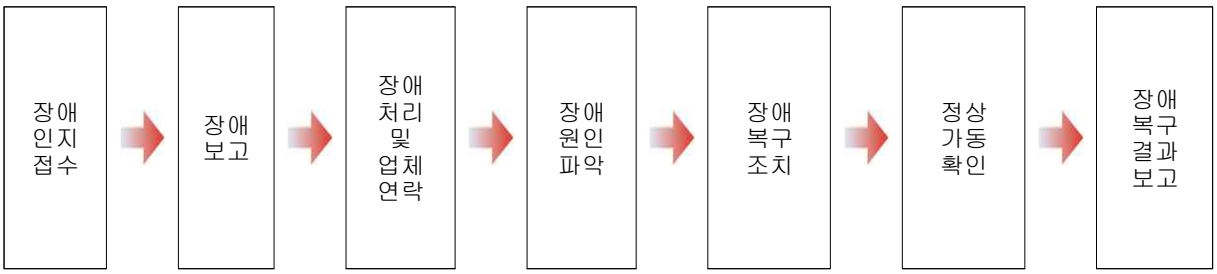
등급	등급별 복구 우선순위	
A등급 (핵심 시스템)	A-1	o 서버 - 서버: 개발 및 테스트서버(R740), 종합정보테스트서버(R740), S2DDS DNS 관리-A(S2DDS 2500), S2DDS DNS 관리-S(S2DDS 2500), S2 DHCP 관리(Active)(X4150), S2 DHCP 관리(Stanby)(X4150), AhnLab V3 및 EPM 관리(R440), 통합블레이드서버(BL460c), 통합이력관리서버-문화대 TBCS(BL460c), 백석대 학생이력관리(백석대 BEST)(BL460c), 도서관 DB서버(R730), (신)_백업마스터서버(LC4000), 체육관 원격지 백업 서버(LC4000), TCMS 통합ODA DB1 19C, TCMS 통합ODA DB2 19C, 유무선 통합인증 시스템(R740), NTP 서버, 종합정보시스템 SVN - 가상화 서버: Prism 뉴타닉스 서버(DX2200 DX170r Gen10) [TCMS 수강신청 SUKANG#1, TCMS 수강신청 SUKANG#2, TCMS 전자출결 BUATT#1, TCMS 전자출결 BSCUATT#1, TCMS 신규 TCWAS#1,TCMS 신규 TCWAS#2, TCMS 신규 TCWAS#3, TCMS 신규 TCWAS#4, TCMS 신규 TCWEB#1, TCMS 신규 TCWEB#2, TCMS 신규 TCWEB#3, TCMS 신규 TCWEB#4, 신규 BSWAS1, 신규 BSWAS2, 신규 BSWEB1, 신규 BSWEB2, 접근통제솔루션(MACS), NMS(PRTG NMS)] o 스토리지 - 학사/행정통합 DB스토리지(HP 3PAR 7200), TCMS 통합NAS TCNAS(DX2200 170r Gen10)
	A-2	o 웹 서비스 - 대표홈페이지, 대표홈페이지 관리자, 통합인증로그인, 포털시스템, 종합정보시스템, 출결, 행정정보시스템, 수강신청시스템, 입시홈페이지, 정보시스템 접근제어 솔루션, 학생역량관리시스템, 교직과정, 백석톡 관리자, 백석대학교 스마트 출결 학생용(Android/iOS), 백석대학교 스마트 출결 교수용(Android/iOS), 백석대학교/백석문화대학교 도서관(Android/iOS), 클리커(Android/iOS) o 소프트웨어 - 전자결재시스템, eXSignOn SSO(SSO 3.0), WAS 미들웨어(WebtoB, JEUS Standard), 전자결재시스템, 백석대 학생이력관리, 유무선 통합인증 시스템, U-Check+ 전자출결, 백석문화대학교 홈페이지(Wizard 7), 클립리포트(CLIP Report 5.0), 학사/행정개발 Mybulider, eXPortal, eXBuilder 6, TCMS TCWEB#1, TCMS TCWEB#2, TCMS TCWEB#3, TCMS TCWEB#4, TCMS TCWAS#1, TCMS TCWAS#2, TCMS TCWAS#3, TCMS TCWAS#4 신규 BSWEB1, 신규 BSWEB2, 신규 BSWAS1, 신규 BSWAS
	A-3	o 네트워크 - 라우터(NCS5001), 서버팜 스위치 2EA(Nexus 9372), 백본 스위치 2EA(Nexus 7706), Cisco SAN 스위치 2EA(MDS 9148 FC), 체육관 메인 스위치(9300-24S), L4 스위치 2EA(Application Switch 5224), L4 스위치-사이버캠퍼스 2EA(MPX 5905), LMS 스위치(Nexus 3172T), 10G_HCI스위치 2EA(Nexus 3172T), 네트워크 트래픽 관리시스템(TaskQoS N500-B10G) o 정보보호시스템 - 통합보안시스템#1(Axgate-20000), 통합보안시스템#2(Axgate-10000), DDoS 보안장비(one-d 5000), 서버팜 방화벽 2EA(TrusGuard 10000B), 모니터랩 웹방화벽(WIWAF 2000), TMS 위협탐지 관리(TESS TAS 2000), ChakraMax DB접근제어(Warevalley W-L8), 접근통제솔루션(MACS), 백석대 Secuve Tos Manager(RNC 115), 개인정보 접속기록관리(백석대), 개인정보 접속기록관리(문화대), 개인정보필터링-A(EU-4000), 개인정보필터링(EU-3000), AhnLab V3 및 EPM 관리

등급	등급별 복구 우선순위	
B등급 (주요 시스템)	B-1	o 서버 - 신한은행 헤이영 중계서버(백석대)(DL380), 백석대 GSL 관리(R730), 백석 TALK 백석대(DL360), AD서버(DL320), NAS Gateway 2EA(3par SFC), 백석대 증명 발급 중계 서버 PC(Ncore), (구)DB서버#1(BL870c), (구)DB서버#2(BL870c), (구)WAS서버#1(BL870c), (구)WAS서버#2(BL870c), (구)WEB서버#1(BL870c), (구)WEB서버#2(BL870c), 한국어교육원 관리시스템(Bu_Global)(DX170r), 연말정산서버)(Rockey)(DX170r), 버스승차권 어플 관리서버(Bu_Ticket)(DX170r), 멀티미디어 서버(도서관) 2EA(BL380), 도서관 WEB서버(R730), 기숙사(생활관) 기존(R440), 기숙사(생활관) 신규(R440), 콘텐츠 제작용(R710), 문화대 GSL 관리(R720), 문화대 산단 직무교육 e-디딤돌 웹서버(R450), 백석 TALK 문화대(DL360), 백석대 사이버캠퍼스 WEB서버 4EA(R740), 교수학습개발원 CMS 컨텐츠 관리 시스템(R940), 문화대 자체원서접수(SMS전송관리)(R720), 예산서버(2950), 신한은행 헤이영 중계서버(문화대)(DL380), 교수학습개발원 장비 2EA, 연구비 관리서버(백석대 산학협력단)(R740), 연구비 관리서버(VM)(R740), RemoteCall 6.0, BSCC(BL380) o 스토리지 - 백석·문화 통합 NAS, (구)웹메일 2EA, 도서관 NAS 스토리지, CYBER LMS 스토리지 2EA, 콘텐츠 및 백업 스토리지, VM-LMS 8EA(Resin), VM-CMS 2EA(Resin)
	B-2	o 웹서비스 - 통계, 구글계정생성 관리자 화면, 구매자산관리 시스템, 도서관, 현대시 100년관, 백석목회지원센터, 백석역사관, 교수학습개발원 사이버캠퍼스, (구)교수학습개발원 사이버캠퍼스, 백석생활관, 평생교육원, 사회봉사센터, 장애학생지원센터, 산학협력단, LINC+ 사업단, 디지털 사업단, 무인항공센터, 실버센터, 국제교육센터, 온라인 디자인 공유 캠퍼스(한국, 중국, 일본) 발전기금, 설문, 백석대학교 부속기관, 도서관(서울), 백석톡(Android/iOS), 백석대 버스(Android/iOS), 백석대학교 도서관(서울)(Android/iOS) o 소프트웨어 - eXSurvey 설문조사시스템(eXSurvey), 웹방식 원격지원시스템, 교육통계솔루션(i-DAS), 백석 TALK 유지보수(Mthink), Google Gsuite, (구)WEB서버#1, (구)WEB서버#2, 백석대 사이버캠퍼스 WEB서버 4EA, 도서관 WEB서버, (구)WAS서버#1, (구)WAS서버#2
	B-3	o 네트워크 - 메인 스위치: 글로벌 외식산업관(WS-C3650-24TD), 은혜관(HP-A5500 48G), 자유관(WS-C3650X-24T-S), 창조관 2EA(C9200L-24T-4X), 인성관(WS-C3560X-24T-S), 목양관(C9200L-24T-4X), 본부동 우측 2EA(WS-C3650-24TD), 본부동 좌측(WS-C3650-24), 예술동(C9200L-24T-4X), 조형관(9300-48S), 진리관(WS-C3560X-24T-S), 지혜관(WS-C3560X-24T-S), 승리관(WS-C3560X-24T-S), 학생복지동(WS-C3560X-24T-S), 음악관(C9200L-24T-4X), 교수회관(HP-1920-POE- 24g), 백석홀(HP-A5500 48G) - 스위치: 자유관(Cisco-9200L-24T) - 무선장비: PoE 스위치 81EA, AP 1389EA, APC 6EA o 정보보호시스템 - 블루엑스레이 매체제어-DLP(R230), COMVOY 컴보이(X3650)

등급	등급별 복구 우선순위	
C등급 (기타 시스템)	C-1	o 서버 - DSC 공유대학 서버(RC124-P4), 재해 DB 복구서버(DBBKTEMP)(DX170r) o 스토리지 - DSC 공유대학 NAS, TCMS 통합 Oracle Database
	C-2	o 정보보호시스템 - 망분리용 방화벽(TrusGuard 100B)

2.7. 정보시스템 백업 및 복구방안

2.7.1. 정보시스템 장애 복구 흐름도



2.7.2. 백업관리

1) 정보시스템 담당자는 신속한 업무 복구를 위해 백업 대상을 선정하고 필요한 내용을 주기적으로 백업해야 함
2) 백업 대상은 DB, 개발소스 및 메일 데이터, 로그, 서버OS 그리고 기타 중요도 가 높다고 판단되는 데이터를 대상으로 함
3) 정보시스템 담당자는 안전한 백업매체를 선정하고 백업의 주기 및 소산 유무를 결정해야 함
4) 백업매체는 비인가자가 접근할 수 없는 격리된 곳에 보관하여 비인가자에 의한 백업정보 유출이 일어나지 않도록 해야 함

2.7.3. 백업시스템 및 부대장비 운영현황

구분	유지관리 현황	비고
백업시스템	정기 점검 및 유지보수관리	
항온항습기	정기 점검 및 유지보수관리	
UPS 및 전기	정기 점검 및 유지보수관리	
소방설비	시설관리처 반기 및 매월	

2.8. 실제 발생 가능한 사고에 대한 정기적 점검, 지속관리 및 사후 처리

2.8.1. 정기적 점검

구분	세부사항	비고
교육	외부용역 유지관리 업체	매년
보안점검	통합UTM장비	유지관리 / 매월 점검
	방화벽시스템, 웹방화벽	
	DDOS장비	
	DB 접근제어	
	DB 암호화	
	개인정보이력관리시스템	
	백신, 서버 보안 등	
시스템	서버시스템	
	네트워크 시스템	
	백업시스템	
	항온항습기	
	UPS 시스템	
소방설비	가스 소화설비	시설관리처 / 반기 및 매월
회선(망)	데이터 및 인터넷회선	회선관리(통신사)

2.8.2. 지속관리 절차

구분	세부사항	비고
안전, 재해, 재난 운영 관리 절차	재난 유형별 대응대책 수립	풍수해 발생 / 폭설 / 지진
	재난 상황 시 조치요령	정전사고 및 전기시설 파손 / 폭설
	시기별 안전관리	해빙기 / 장마철 / 태풍기 / 동절기 / 명절
침해사고 대응절차	업무과실로 인한 유출 점검	
	외부 침투에 의한 유출 점검	
	오남용으로 인한 유출 점검	

2.8.3. 사후처리 및 운영방안

o 장단기 계획에 따라 단계적 노후 장비교체, 이중화로 재난을 최소화 운영

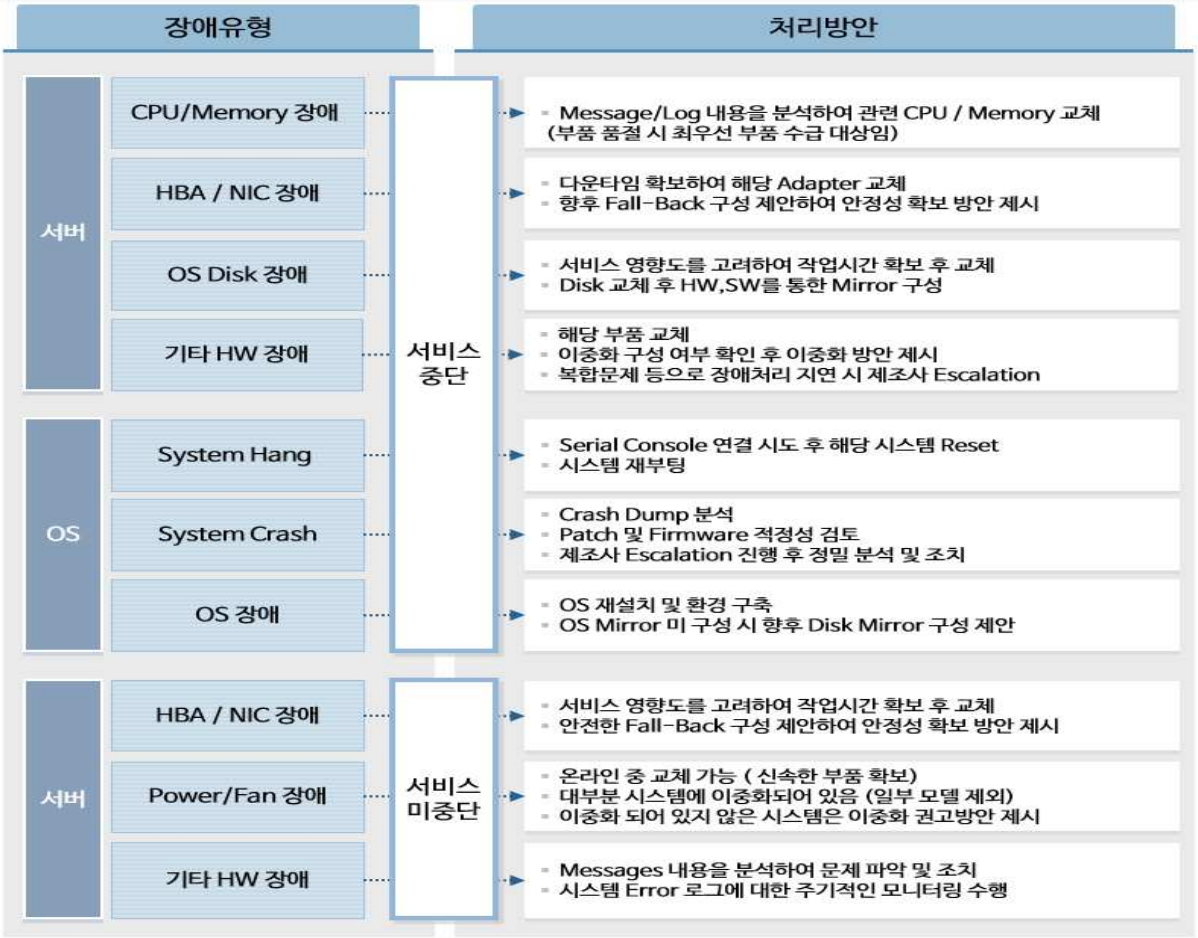
o 유형별 장애처리 방안을 표준화하여 처리의 신속성을 제고

2.9. 표준화된 유형별 장애처리 방안

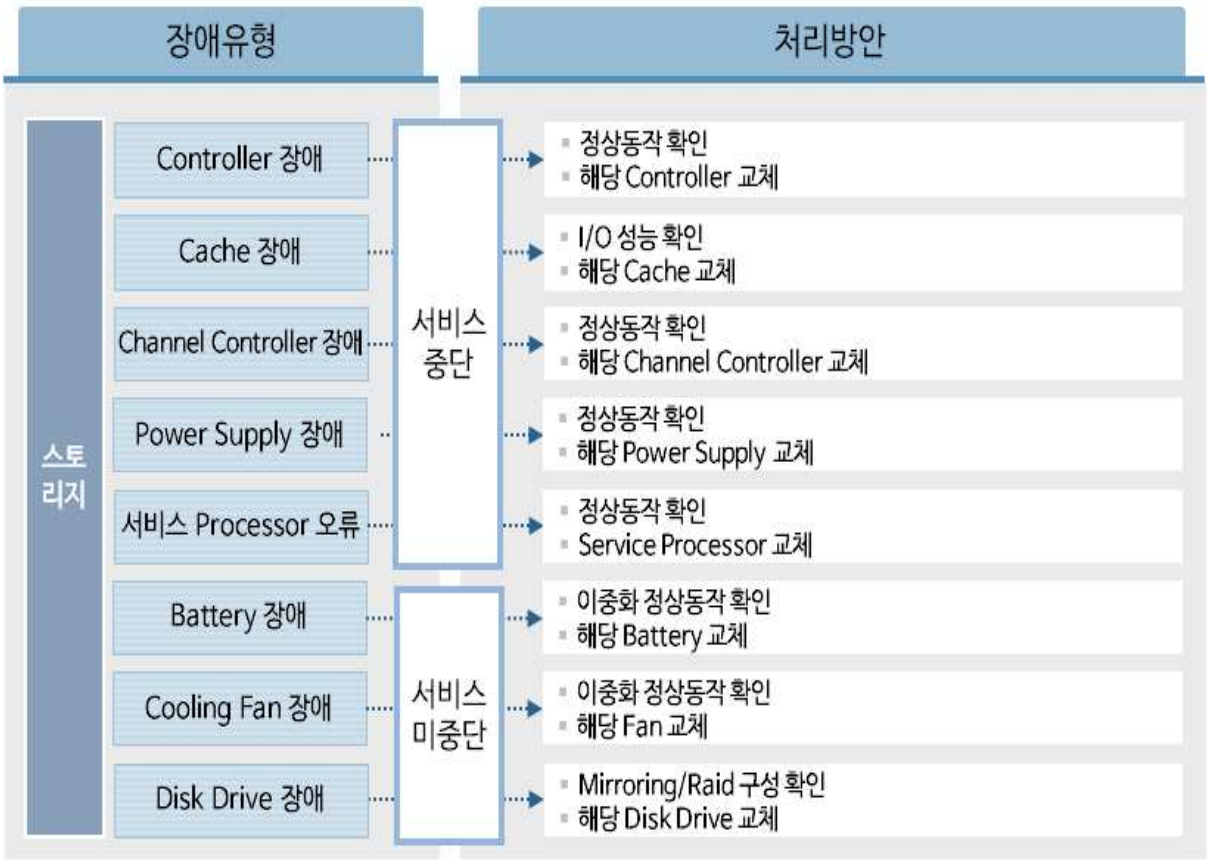
o 표준화된 유형별 장애처리 방안을 적용하여 장애를 신속하게 처리함으로써 안정적이고 효율적인 시스템 운영을 보장한다.

2.9.1. 유형별 효과적인 장애처리 방안(예시)

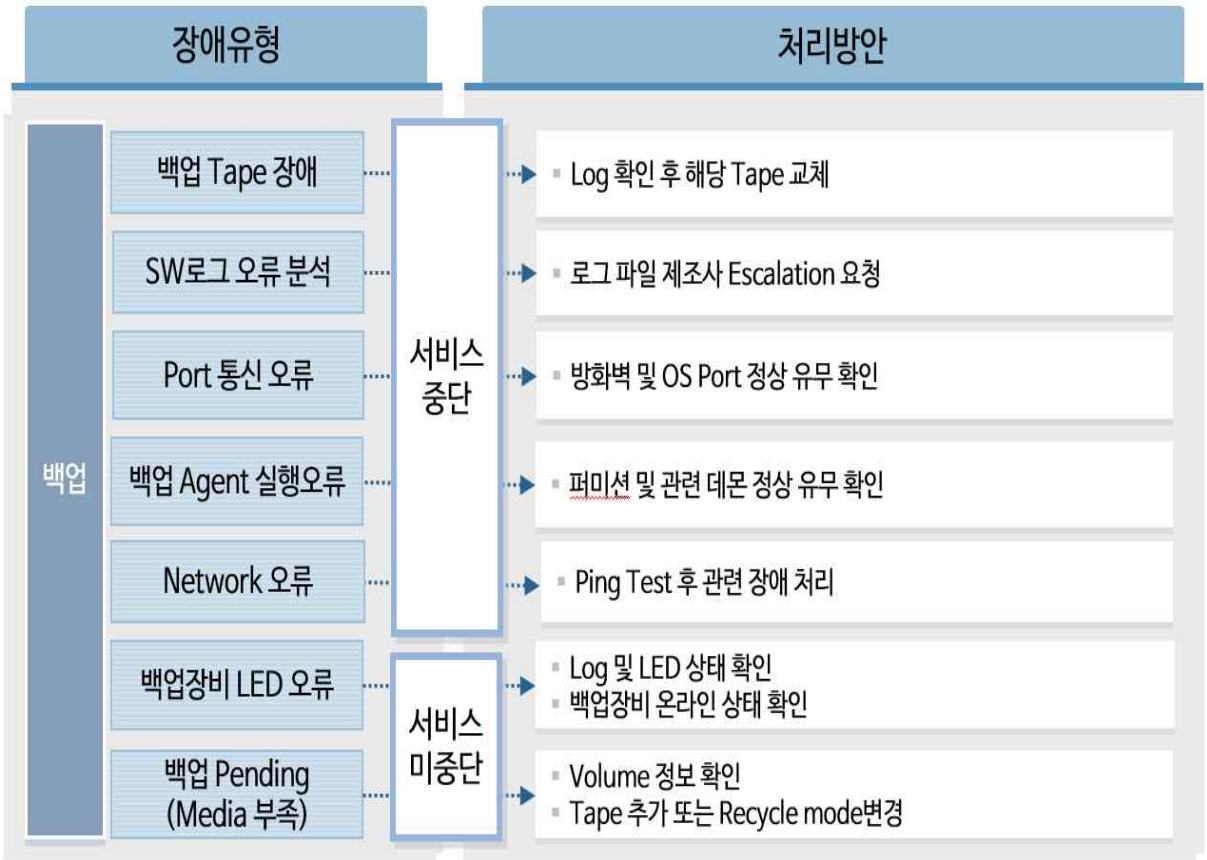
- 서버 장애



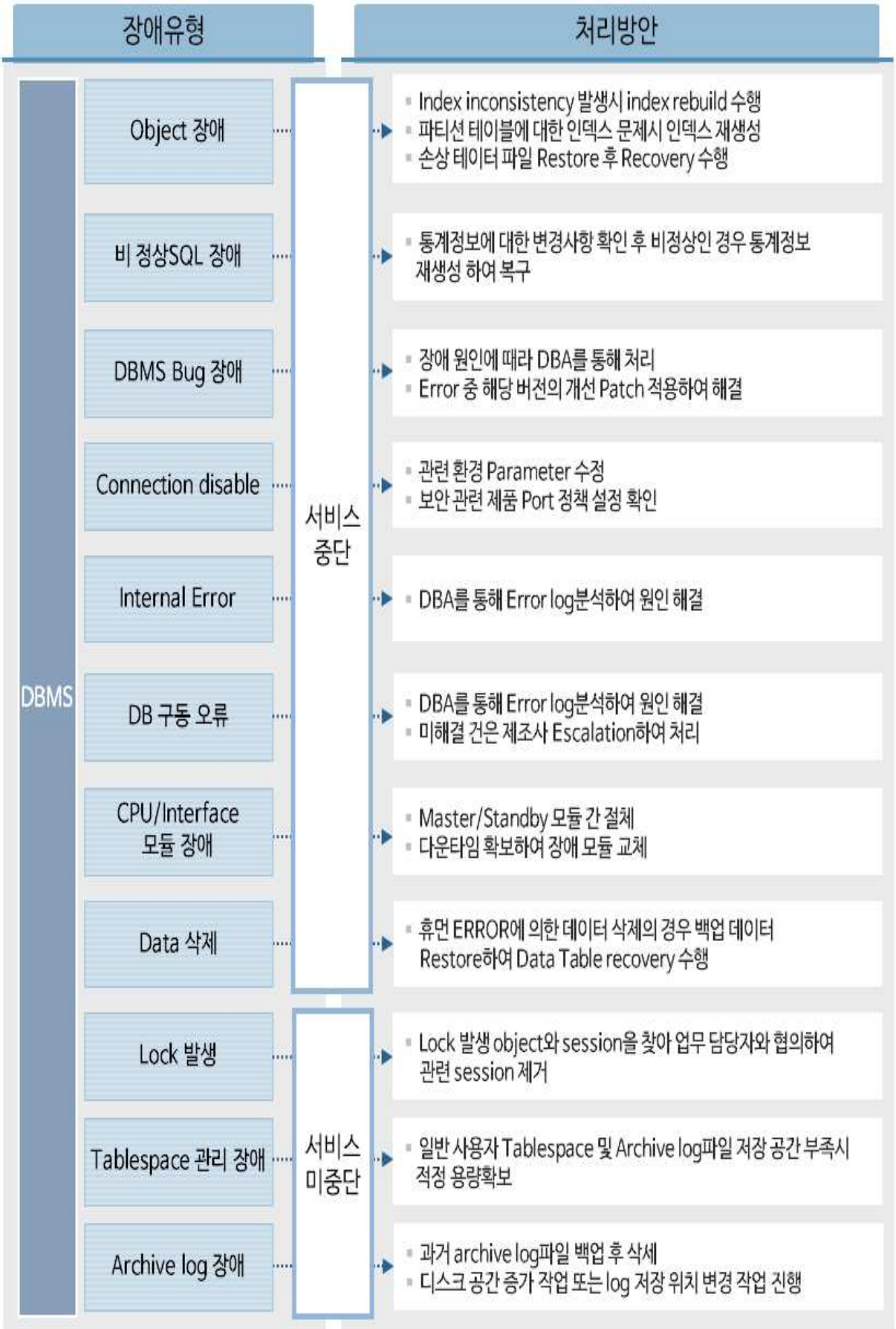
- 스토리지 장애


장애유형
처리방안
스토리지
Controller 장애
Cache 장애
Channel Controller 장애
Power Supply 장애
서비스 Processor 오류
서비스 중단
정상동작 확인
해당 Controller 교체
I/O 성능 확인
해당 Cache 교체
정상동작 확인
해당 Channel Controller 교체
정상동작 확인
해당 Power Supply 교체
정상동작 확인
Service Processor 교체
Battery 장애
Cooling Fan 장애
Disk Drive 장애
서비스 미중단
이중화 정상동작 확인
해당 Battery 교체
이중화 정상동작 확인
해당 Fan 교체
Mirroring/Raid 구성 확인
해당 Disk Drive 교체

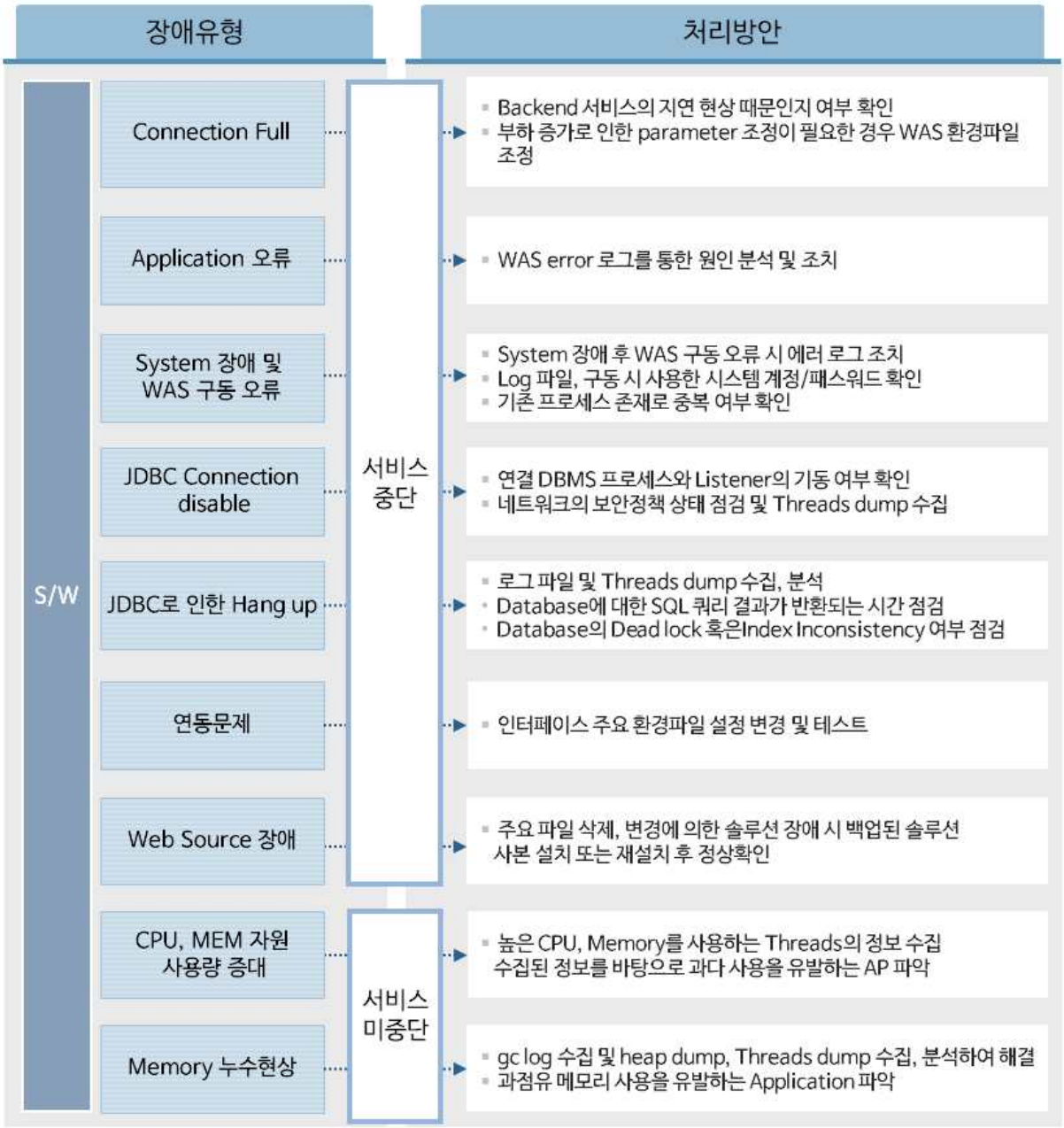
- 백업 장애


장애유형
처리방안
백업
백업 Tape 장애
SW로그 오류 분석
Port 통신 오류
백업 Agent 실행오류
Network 오류
서비스 중단
Log 확인 후 해당 Tape 교체
로그 파일 제조사 Escalation 요청
방화벽 및 OS Port 정상 유무 확인
퍼미션 및 관련 데몬 정상 유무 확인
Ping Test 후 관련 장애 처리
백업장비 LED 오류
백업 Pending (Media 부족)
서비스 미중단
Log 및 LED 상태 확인
백업장비 온라인 상태 확인
Volume 정보 확인
Tape 추가 또는 Recycle mode변경

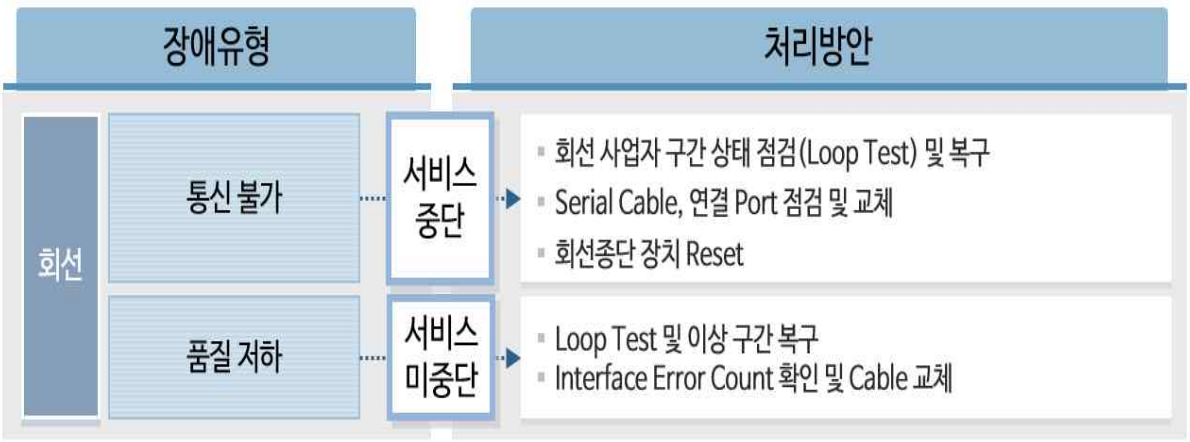
- DBMS 장애


장애유형
처리방안
DBMS
Object 장애
비 정상SQL 장애
DBMS Bug 장애
Connection disable
Internal Error
DB 구동 오류
CPU/Interface 모듈 장애
Data 삭제
Lock 발생
Tablespace 관리 장애
Archive log 장애
서비스 중단
서비스 미중단
Index inconsistency 발생시 index rebuild 수행
파티션 테이블에 대한 인덱스 문제시 인덱스 재생성
손상 테이터 파일 Restore 후 Recovery 수행
통계정보에 대한 변경사항 확인 후 비정상인 경우 통계정보 재생성 하여 복구
장애 원인에 때라 DBA를 통해 처리
Error 중 해당 버전의 개선 Patch 적용하여 해결
관련 환경 Parameter 수정
보안 관련 제품 Port 정책 설정 확인
DBA를 통해 Error log분석하여 원인 해결
DBA를 통해 Error log분석하여 원인 해결
미해결 건은 제조사 Escalation하여 처리
Master/Standby 모듈 간 절체
다운타임 확보하여 장애 모듈 교체
휴먼 ERROR에 의한 데이터 삭제의 경우 백업 데이터 Restore하여 Data Table recovery 수행
Lock 발생 object와 session을 찾아 업무 담당자와 협의하여 관련 session 제거
일반 사용자 Tablespace 및 Archive log파일 저장 공간 부족시 적정 용량확보
과거 archive log파일 백업 후 삭제
디스크 공간 증가 작업 또는 log 저장 위치 변경 작업 진행

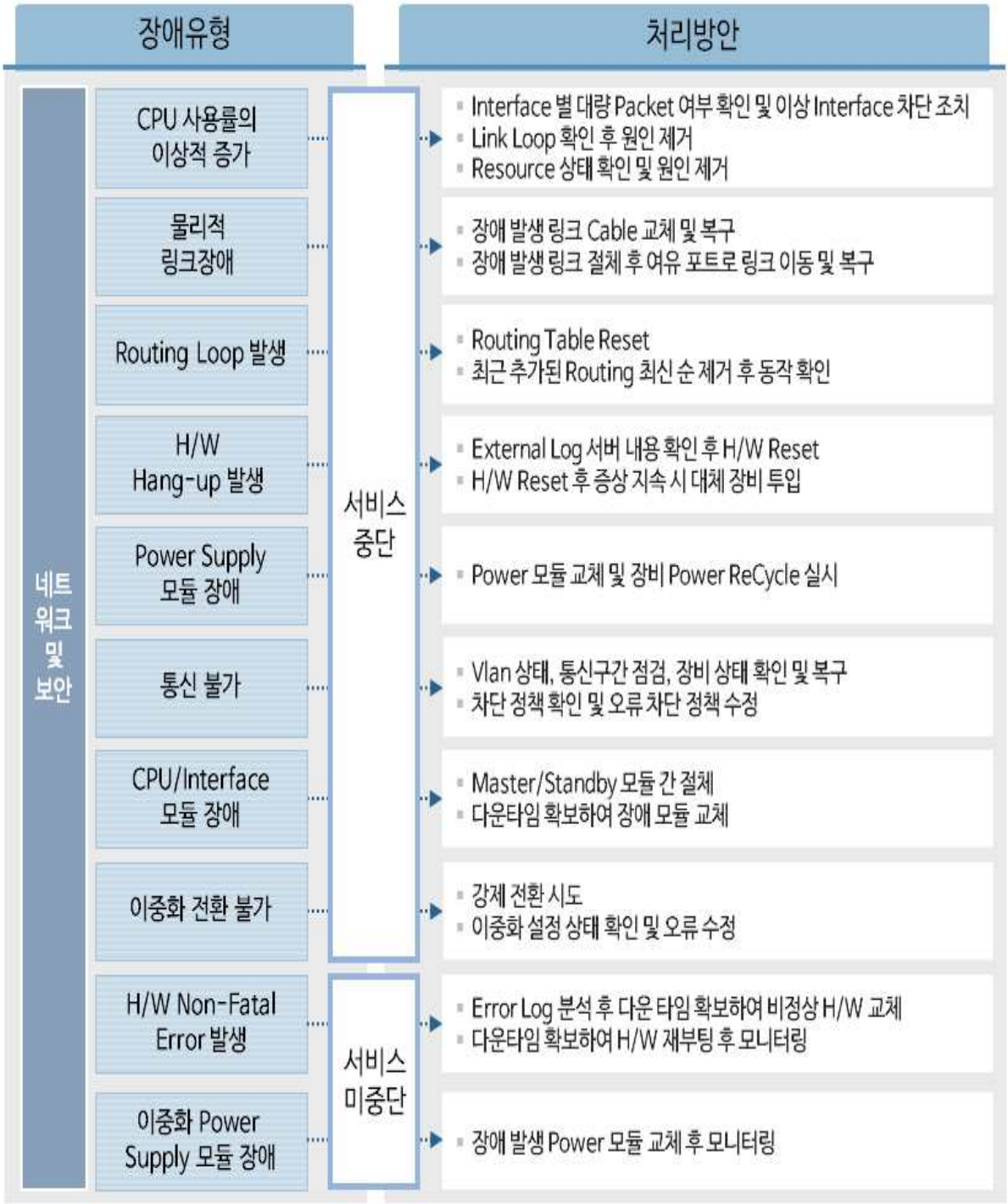
- 소프트웨어 장애



- 네트워크 회선 장애



- 네트워크/보안 장애



※. 보안장비 장애의 경우 장비별 세부 장애 대응은 “보안장비별 매뉴얼” 참고

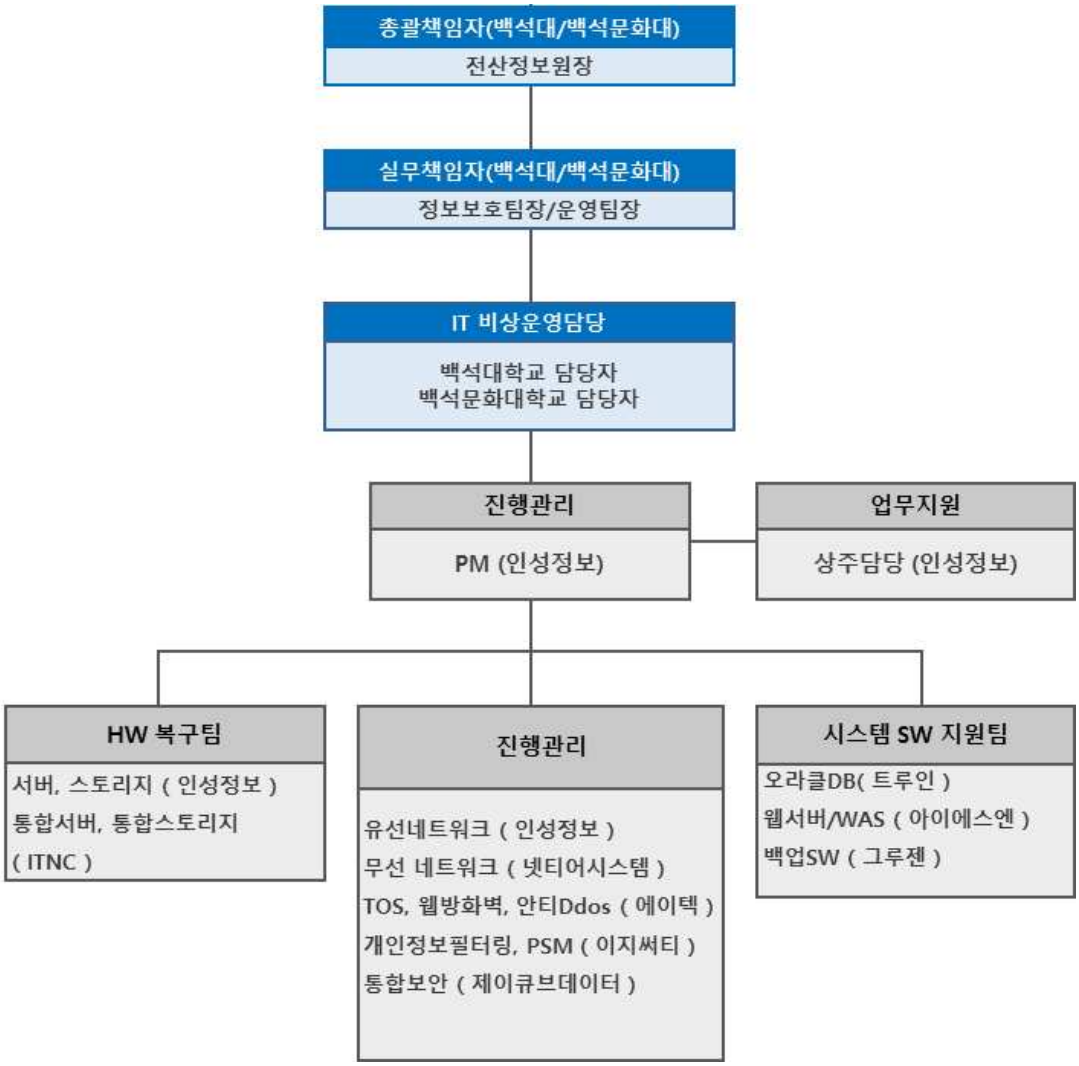
3. 모의훈련

3.1. 장애 대응 모의훈련

3.1.1. 목적

o 장애 대응 모의훈련은 전산장비 장애나 사이버침해사고가 발생하였을 때를 가정하여 훈련 시나리오를 계획하고 이를 토대로 실질적인 훈련을 수행하여 비상시 대응태세 견지 및 신속한 장애처리를 수행할 수 있는 역량 강화를 그 목적으로 한다.

3.1.2. 훈련 조직도



3.1.3. 훈련 주기

o 장애 대응 모의훈련은 연 1회 실시하고 그 결과를 본 매뉴얼에 이력 관리한다.

3.1.4. 훈련 결과 공유

o 훈련 종료 시 모의훈련 결과 설명회 및 강평회를 실시한다.

3.1.5. 비상연락망

o 교내 대응팀

직급명	담당자	연락처	email
원장 정보보안담당관	홍	[redacted]	
팀장	노		
팀원	홍		
“	김		
“	심		
“	김		
“	유		
“	최		
“	신		
“	이		
총무처			
개인정보책임자	임		
개인정보담당자	김		
시설관리처			
처장	전		
전기통신	김		
소방담당	이		

o 유지보수 대응팀

No	지원분야	회사명	구분	성명	핸드폰	이메일
1	사업총괄	인성정보	PM	최		
2	담당영업	인성정보	영업	이		
3	상주(백석대학교)	인성정보	상주	오		
4	상주(백석문화대학교)	인성정보	상주	김		
5	HP Blade 서버, HP 스토리지	ITNC	정	민		
6			부	박		
7	통합백업소프트웨어	그루젠	정	최		
8			부	권		
9	팀웹하드(웹메일)	나무기술	정	김		
10			부	조		
11	뉴타닉스 (HP무선랜,삼성무선랜)	넷티어	정	이		
12			부	이		
13	HIWARE (접근통제관리시스템)	셈스티씨에스	정	차		
14			부	강		
15	Google G-suite	시소아이티	정	김		
16			부	노		
17	U-check 전자출결	씨딘	정			
18			부			
19	WAS 미들웨어	아이에스엔	정	한		
20			부	박		
21	보안DNS(iDHCP)	아이엔아이맥스	정	김		
22			부	최		
23	교육통계솔루션	아이플랜비즈	정	김		
24			부	이		
25	학사/행정개발My bulder	액티브소프트	정	김		
26			부	한		
27	Comvoy (PC보안취약점점검시스템)	에이텍정보기술	정	김		
28			부	박		
29	서버보안, SSL웹방화벽	에이텍정보기술	정	박		
30			부	박		
31	DDoS 대응시스템	에이텍정보기술	정	최		
32			부	정		
33	QoS 장비	엔에스텍	정	이		
34			부	하		
35	전자결재시스템(그룹웨어)	엔엔소프트	정	한		
36			부	도		

No	지원분야	회사명	구분	성명	핸드폰	이메일
37	V3, 웹방식원격지원 시스템	위포	정	이		
38			부	최		
39	개인정보 상시모니터링	이지서티	정	배		
40	개인정보필터링	이지서티	정	박		
41			부	조		
42	HP, Dell 서버, 스토리지	인성정보	정	김		
43			부	심		
44	네트워크, L4, SAN sw, Aruba PoE	인성정보	정	김		
45			부	심		
46	Server WAS(Resin), Jeniffer APM	제스트정보기술	정	문		
47			부	이		
48	개인정보암호화	조은아이앤에스	정			
49			부	박		
50	홈페이지	케이투웹테크	정	장		
51			부	김		
52	clip report	클립소프트	정	양		
53			부	정		
54	eXBuilde6, eXPortal, eXSignOn,eXSurvey	토마토시스템	정	김		
55			부	박		
56	Oracle DB	트루인	정	장		
57			부	황		
58	Oracle ODA	트루인	정	임		
59			부	황		
60	UPS, 항온항습기	한강기전	정	김		
61			부	안		
62	BEST백석인재개발, TBCS학생이력관리	휴노	정	김		
63			부	임		
64	샤크라 맥스	ITNC	정	백		
65	서버팜 방화벽	한성아이티엘	정	한		
66			부	서		

o 유관기관

기관명	신고전화	비고
국가정보원	☎ 111	
교육사이버안전센터	☎ 053-714-0777	
KISA 보호나라/ 개인정보침해신고센터	☎ 118	