정보시스템

장애관리 지침

Guideline
for Incident & Problem Management
of Information System

국무조정실 정보통신부

정보시스템 장애관리 지침

Guideline for Incident & Problem Management of Information System

1. 정보시스템 운영관리 지침 개요서
2. 정보시스템 운영관리 지침

관리요소별 세부 지침

관리요소별 세부 지침	해당 10대 관리요소
3. 정보시스템 구성 및 변경관리 지침	구성 및 변경관리
4. 정보시스템 운영상태관리 지침	운영상태관리
5. 정보시스템 성능관리 지침	성능관리
6. 정보시스템 장애관리 지침	장애관리
7. 정보시스템 재해복구 지침	백업관리
8. 정보시스템 백업 지침	
9. 서비스데스크 운영관리 지침	사용자지원관리
10. 전산실 관리 지침	전산실관리
11. 정보시스템 운영 아웃소싱 관리 지침	운영아웃소싱관리
12. SLA를 강화한 정보시스템 운영계약 참조모델	

2005. 12

제 · 개정 이력표

버전	제 · 개정 내용	일자
V1.0	정보시스템 장애관리 지침 제정	2004. 10
V1.1	정보시스템 장애관리 지침 개정(본문수정)	2005. 12

Contents

1. 개요 01

2. 지침의 구성 및 범위 02

3. 정보시스템 장애 03

3.1 장애의 개념 03

3.1.1 본 지침서에서 장애의 개념 정의 03

3.1.2 정보기술서비스관리에서의 장애관리 03

3.1.3 정보보호관리와 장애관리 07

3.1.4 정보기술서비스관리의 주요 구성요소(BS 15000) 10

3.1.5 통제 가능성 관점에서 재해와 장애의 개념구분 13

3.1.6 프로세스 관점에서 장애의 개념 14

3.1.7 발생원인 관점에서 장애의 개념 15

3.1.8 복구시간 관점에서 장애의 개념 16

3.2 용어정의 18

3.3 정보시스템 장애의 요인과 유형 20

3.3.1 장애의 범위 및 유형 분류 20

3.3.2 장애등급의 분류 22

4. 장애관리 체계 32

4.1 장애관리 조직체계 32

4.2 장애관리 프로세스 38

5. 장애관리 세부 프로세스 41

5.1 장애관리 세부 프로세스 42

5.1.1 장애 식별 / 접수 42

5.1.2 장애 등록 및 등급지정 44

5.1.3 1차 해결 45

5.1.4 장애배정 46

5.1.5 2차 해결 47

5.1.6 문제관리 48

5.1.7 장애종료 49

5.1.8 프로세스 점검 50

5.2 문제관리 세부 프로세스 52
5.2.1 문제등록 52
5.2.2 근본원인 도출 53
5.2.3 해결방안선택 55
5.2.4 해결방안 모니터 56
5.2.5 해결방안 실행 57
5.2.6 해결방안 점검 58
5.2.7 문제종료 59
6. 장애관리에서의 비상 계획 61
6.1. 비상상황 대응을 위한 조직 구성 62
6.1.1 정보기술비상상황 관리위원회 62
6.1.2 비상 조직 64
6.2 비상 계획 프로세스 65
6.2.1 비상상황에 대한 판단 65
6.2.2 비상상황 선언 및 보고 66
6.2.3 비상상황 운영 및 복구 68

7. 모의훈련 및 조직학습 70

7.1 모의 훈련 70

7.1.1 세부 훈련 절차 71

7.1.2 장애조치 절차 74

7.1.3 비상연락 체계 및 의사소통 절차 76

7.2 조직 학습 77

7.2.1 조직 학습 활동 77

7.2.2 정기 장애 회의 79

부록 Ⅰ. 장애조치 훈련 지침 81

부록 Ⅱ. 정보시스템 자원별 장애처리 절차 93

부록 Ⅲ. 장애관리 시나리오 99

부록 Ⅳ. 장애관리 양식 111

표차례

〈표 3-1〉 ITIL 과 eSCM의 관점 비교 ····· 06

〈표 3-2〉 ISO 13335와 ITIL의 위험평가 비교 ····· 09

〈표 3-3〉 금융기관별 복구시간 ····· 17

〈표 3-4〉 정보시스템 재해 및 장애의 분류와 대응방안 ····· 20

〈표 3-5〉 장애 5등급의 영향도와 긴급도 ····· 31

〈표 6-1〉 비상상황 발생시 대응단계 ····· 62

〈표 6-2〉 정보기술비상상황 관리위원회 역할 ····· 63

〈표 6-3〉 정보기술비상상황 관리위원회 담당별 역할 ····· 63

〈표 6-4〉 비상조직 팀별 역할 및 구성 ····· 65

〈표 6-5〉 비상상황 선언시 참고 요소 ····· 66

〈표 6-6〉 초기 장애 상황 발생시 보고자와 보고 접수자의 역할 ····· 67

〈표 6-7〉 비상상황 발생시 1,2차 보고 내용 ····· 67

〈표 6-8〉 비상상황 발생시 대내 · 외 공지 내용과 방법 ····· 68

〈표 6-9〉 비상상황 문제 해결 프로세스 ····· 69

그림차례

(그림 3-1) 조직 시스템의 위험계층구조 04

(그림 3-2) ITIL과 eSCM의 관리영역 비교 06

(그림 3-3) 정보기술서비스관리 참조모형(ITSM Reference Model) 사례 12

(그림 3-4) 장애, 문제, 알려진 오류의 개념도 14

(그림 3-5) 장애등급을 5등급으로 구분하는 경우 27

(그림 4-1) 장애관리를 위한 조직도 예 32

(그림 4-2) 장애관리 및 문제관리 프로세스 관계도 39

(그림 4-3) 장애관리 프로세스 흐름도 39

(그림 4-4) 문제관리 프로세스 흐름도 40

(그림 5-1) IDEFØ 표기법 41

(그림 5-2) 장애식별/접수 43

(그림 5-3) 장애등록 및 등급지정 44

(그림 5-4) 1차 해결 45

(그림 5-5) 장애배정 46

(그림 5-6) 2차 해결 47

(그림 5-7) 문제관리 48

(그림 5-8) 장애종료 50

(그림 5-9) 프로세스 점검 51

(그림 5-10) 문제등록 53

(그림 5-11) 근본원인 도출 54

(그림 5-12) 해결방안 선택 55

(그림 5-13) 해결방안 모니터 57

(그림 5-14) 해결방안 실행 58

(그림 5-15) 해결방안 점검 59

(그림 5-16) 문제종료 60

(그림 6-1) 일반적인 장애와 비상상황의 연결 61

(그림 6-2) 비상 조직도 예시 64

1 개요

최근 공공부문 정보화에 대한 예산투자가 증가함에 따라, 업무 편의의 증진과 공공부문 대국민 서비스의 확대를 위한 공공기관의 정보시스템 도입이 점차 확산되고 있다. 이에 따라, 오늘날 공공기관에서 사용되는 대부분의 정보들이 정보시스템을 통해 저장, 관리, 활용되고 있다.

정보시스템 도입의 양적 증대가 기본 수준 이상 이루어짐에 따라, 과거 시스템 구축 및 도입에 강조되었던 정보화의 영역은 도입된 정보시스템의 운영관리 측면으로 새롭게 확장되고 있다. 정보시스템 장애관리는 정보시스템 운영관리를 위한 세부 요소 중의 하나로서, 최근 다양한 위험요소들이 존재하고 있는 시스템 운영환경에서 그 필요성이 증대되고 있다.

정보시스템 장애가 미치는 영향은 경우에 따라서는 매우 심각할 수 있다. 시스템이 제공하고 있는 서비스가 다수의 인원에 의해 사용되어 있는 경우, 시스템이 보안상 매우 민감한 데이터를 다루고 있는 경우, 단시간동안 서비스가 제공이 되지 않으면 업무상 혹은 재정상 치명적인 손상을 입게 되는 경우가 그 예이다.

정보시스템 장애를 유발하는 위험요소들은 다양한 원인을 통해 제공되고 있으며, 그 발생시점 또한 예측하기 어려운 특성이 있다. 이런 이유로, 장애가 절대로 발생하지 않는 무장애 시스템의 운영은 사실상 불가능하다. 따라서 장애관리의 주 목적은 발생된 장애에 대해 신속한 복구 작업을 수행하여 정상적으로 서비스를 제공할 수 있게 하는 것, 그리고 장애복구 결과에 대한 지속적인 관리를 통해 자주 반복되는 장애에 대한 예방조치를 사전에 취함으로써, 발생 가능한 장애를 미연에 방지하는 것이라 할 수 있다.

본 지침에서는 정보시스템 장애관리에 대한 기술적, 관리적인 이슈를 제공하고, 체계적으로 정보시스템 장애를 관리하기 위한 절차 및 방법에 대해 설명한다. 또한 정보시스템 장애관리를 위한 각종 양식들과 예제를 제공함으로써, 실무자들의 이해를 증진시키고자 한다.

본 지침은 정보시스템 운영관리를 수행하는 업무 담당자들에게 참고될 수 있다. 각 기관의 특성과 운영되고 있는 정보시스템의 성격이 각각 다르기 때문에, 각 기관들은 본 지침에서 제공하는 내용들을 참고하여 각 기관에 맞는 장애관리 절차와 방법을 수립해야 한다.

자연 재해, 인적 재해 등 통제 불가능한 재해, 재난에 대한 정보시스템 관리방법은 본 지침의 범위에서 제외하였다. 이 부분은 별도의 지침을 통해 설명할 예정이다.

2 지침의 구성 및 범위

본 지침에서 제공하는 내용은 다음과 같다. 3장에서는 정보시스템 장애의 개념에 대해 살펴본다. 다양한 관점에서 장애관리의 개념을 고찰해보고, 본 지침에서 전반적으로 사용되고 있는 용어의 의미를 정리한다. 또한 다양한 원인에 의해 발생하는 장애의 요인과 유형에 대해 설명하고, 장애등급을 분류하는 기준과 이에 대한 예시를 제공한다.

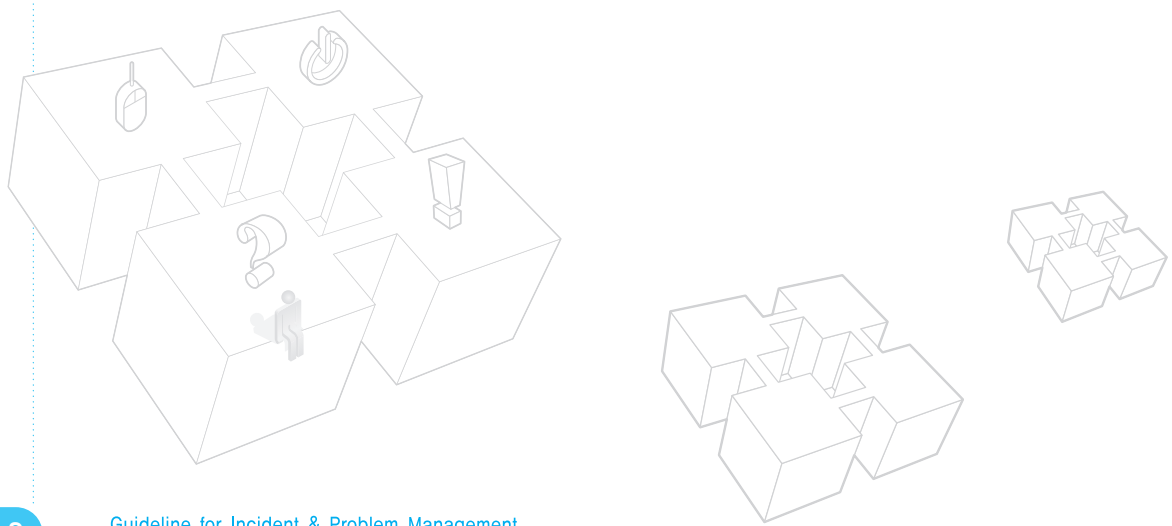
4장에서는 장애관리 체계에 대한 내용으로서, 장애관리 조직의 역할과 책임에 대해 설명하고, 장애관리 프로세스의 전체적인 흐름도를 제시한다.

5장에서는 4장에서 제시한 장애관리 프로세스 흐름도의 세부 프로세스에 대해 각각의 주요 역할, 수행 업무, 주요 관리 항목, 조직의 역할과 책임에 대해 설명한다. 이 중 문제관리 프로세스는 별도의 절로 분리하여 세부 절차에 대해 설명한다.

6장에서는 장애관리에서의 비상 계획에 대해 설명한다. 비상상황으로 선언하는 판단기준과, 이때의 조직체계 구성방법, 그리고 비상상황시 대응 프로세스를 제시한다.

7장에서는 장애발생시 신속하게 대응하기 위한 장애복구 모의훈련 절차와 장애조치 결과 및 예방활동을 통해 얻어지는 성과들의 지속적인 관리를 위한 조직학습에 대해 설명한다.

부록에서는 본 장애관리 지침에서 제시하고 있는 프로세스에 맞도록 작성된 장애관리 모의훈련 시나리오 예제를 제공하고 있으며, 각종 정보시스템 장애관리를 위한 양식들을 첨부한다.



3 정보시스템 장애

3 1 장애의 개념

3 1.1 본 지침서에서 장애의 개념 정의

정보기술서비스관리의 통제 가능성 관점에서 협의의 장애 개념으로서, '정보시스템의 통제 가능한 요인들로 인한 기능저하, 오류, 고장'을 의미한다. 구체적으로 '통제 불가능한 재해(자연 재해와 인적 재해)를 제외한 발생원인 관점에서 직접적으로 영향을 미치는 인적 장애, 시스템 장애, 기반구조 장애(운영 장애, 설비 장애 등 포함) 등과 같은 통제 가능한 요인들에 의한 정보시스템의 기능저하, 오류, 고장'을 의미한다.

3 1.2 정보기술서비스관리에서의 장애관리

조직 시스템의 위험은 계층별로 전략적 관점에서 전략적 위험, 프로세스 관점에서 업무 위험, 자원복구 관점에서 운영적 위험으로 구분할 수 있다. 위험관리(Risk Management)는 조직의 재해, 장애 등 손실을 최소화시키기 위한 절차 혹은 연속적인 행위(위험의 분석, 평가, 대책 등)이다. 이러한 조직의 일반적인 위험을 통제할 수 있는 위험관리는 조직 내의 모든 업무가 정보기술에 의존되어 있으므로, 크게 업무연속성관리와 정보기술 서비스관리로 구분할 수 있다.

업무연속성관리(BCM: Business Continuity Management)란 업무연속성계획(BCP: Business Contingency Planning)의 수립 및 유지보수를 위한 일련의 관리 과정이며, 조직이 재해 혹은 장애로 인한 위험에도 불구하고, 조직의 업무를 사전에 결정한 최소한의 수준으로 영위하기 위한 일련의 통제행위이다. 그러나 업무중단의 원인이 되는 위험에는 통제 가능한 위험인 장애

(그림 3-1) 조직 시스템의 위험계층구조

와 통제 불가능한 위험인 재해가 있다. 이에 대해서 장애는 정보기술서비스관리 내에 장애관리에서, 재해에 대해서는 업무연속성관리 내에서 위기관리 차원에서 관리한다. 위기관리(Crisis Management)에는 예방(Prevention), 대비(Preparedness), 긴급대응(Emergency Response), 재해복구(Disaster Recovery), 업무복구(Business Recovery), 업무재개(Business Resumption) 등이 포함된다. 이러한 업무연속성관리의 절차는 개시단계, 전략수립단계, 구현단계로 구분되며, 이중에서 특히 전략수립단계는 위험평가, 업무 영향분석, 업무연속성전략 수립으로 구성된다. 여기서 업무영향분석이란 조직의 주요 업무 프로세스를 파악하고, 업무기능의 지속적인 운영을 보장하기 위한 최소한의 요구사항을 결정하는 일련의 통제방법이다.

업무의 연속성을 유지시키기 위한 인프라로서 정보기술서비스관리(ITSM : Information Technology Service Management)는 조직의 위험 중 특히 운영적 위험을 최소화시키기 위한 관리이다. 정보기술서비스관리의 기본 목적은 정보시스템 사용자에 초점을 맞춘 정보기술서비스를 제공하고, 조직 목적에 맞는 정보기술서비스를 배치하고, 비용효과적인 서비스수준협약(SLA: Service Level Agreement)을 구현하는 것이다. 이와 같이 정보기술서비스관리에서는 정보기술의 연속적인 서비스 제공 프로세스와 서비스 중단에 대비한 해결 프로세스가 중요시되고 있으며, 서비스 중단에 대응하는 장애관리는 해결 프로세스 내에 존재하게 된다.

정보기술서비스관리는 정보기술관리 환경의 복잡 다양화, 표준관리 체계의 미흡, 불안정한

시스템 운영으로 인한 정보시스템 사용자 서비스의 품질저하를 방지하고, 서비스 품질 경쟁력을 확보하는 최선의 실무방법을 기초로 표준적인 정보기술 서비스관리 프로세스 체계를 관리하는 것으로, 주된 접근방법으로는 ITIL(IT Infrastructure Library)과 eSCM(e-Sourcing Capability Model)이 있다. 이 외에 접근방법에는 MNM(Munich Network Management) 서비스 모형, TINA(Telecommunication Information Networking Architecture) 서비스 모형, TOM(Telecom Operations Map), CIM(Common Information Model) 등이 있다.

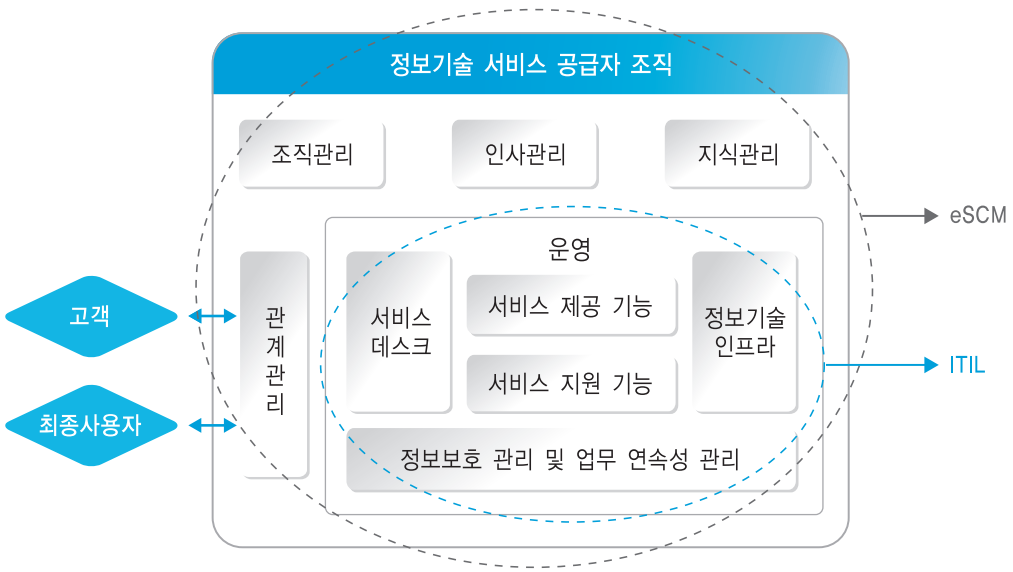
정보기술서비스 프로세스 관점에서 장애의 개념은 1989년에 영국 정부에서 ITIL의 정보기술 영역인 서비스 지원(Service Support), 서비스 제공(Service Delivery) 등 핵심 프로세스에 관한 최선의 실무방법(best practice processes and procedures)을 제시하면서 시작되었다. 1991년에 개선된 최선의 실무방법을 만들기 위해 정보기술서비스관리 포럼(ITSMF: IT Service Management Forum)이 결성되었고, ITSMF는 표준을 만들기 위해 BSI(the British Standards Institution)에 협의를 요청했다. 2000년에 BS 15000 규격이 최초로 제정되었고, 현재 버전은 2002년에 개정된 것이다.

eSCM은 정보기술서비스 제공자의 아웃소싱 서비스품질에 대한 성숙도(Maturity)를 사용자 관점에서 5단계 – (1) 수준 1 : 단순한 서비스 제공, (2) 수준 2 : 일관성 있는 사용자 요구사항 대응, (3) 수준 3 : 조직적 성과관리, (4) 수준 4 : 적극적으로 가치 제고, (5) 수준 5 : 지속적으로 우수성 유지 –로 정의하고 있다. ITIL과 eSCM을 관점에 따라서 비교한 것이 〈표 3-1〉이다.

ITIL은 서비스 설계와 서비스 제공에 대한 정보기술서비스관리 체계이고, eSCM은 소싱 서비스 공급자에 대한 정보기술서비스관리 체계이다. 그러므로 서비스 설계 및 서비스 제공 프로세스의 개선이 필요하면 ITIL 접근방법을 선택하고, 소싱 프로세스의 개선이 필요하면 eSCM 접근방법을 선택하면 된다. ITIL에서 출발된 BS 15000은 서비스 제공 프로세스에 대한 최선의 실무방법을 제시하고 있고, eSCM은 소싱의 품질을 향상시키는 새로운 표준으로 대두되고 있다. ITIL과 eSCM의 관리영역을 비교한 것이 (그림 3-2)이다.

〈표 3-1〉 ITIL과 eSCM의 관점 비교

관점	ITIL	eSCM
내 용	정보기술서비스관리를 위한 최선의 실무방법들의 집합	소싱(sourcing)관계를 형성, 관리, 확장시키는 서비스 공급업자의 능력 개발 및 향상
프로세스 개선	조직의 정보기술 프로세스 개선	아웃소싱 업무를 지원하는 조직 프로세스 개선
성과관리	정보기술서비스성과	조직성과
실무수준	실무자 수준의 지침	실무별 행위형태의 지침, 해석 필요
능력향상	능력향상 지침 없음, 준수사항	능력향상을 위한 지침
평 가	BS 15000-1: 2002 준수, PD 0015 외부감사 이용한 자체 평가	서비스 공급자 능력에 대한 독립적인 평가 및 인증
인 증	BS 15000-1: 2002 준수에 대해서 감사자가 인증	수준 2 – 수준 5에 대해서 Carnegie Mellon Univ.가 인증



(그림 3-2) ITIL과 eSCM의 관리영역 비교

BS 15000은 정보기술서비스 경영활동에 대한 요건을 정의한 영국국가표준(British Standard)이며, 2005년 12월 ISO 국제표준(ISO 20000)으로 제정된 표준이기도 하다. BS 15000은 업무와 사용자의 요구사항을 만족하는 정보기술서비스를 효과적으로 제공하기 위해 통합화된 접근방법을 적용한 심사체계 및 규격을 정의하고 있다. 향후, 정보기술서비스 시장에서 협력업체 또는 파트너 기관의 선택에 있어서 해당 기관의 BS 15000 인증 여부가 선택의 핵심적이고 중추적인 기준이 될 것으로 예상된다. 요약해서 BS 15000은 정보기술서비스관리 방법론으로서, 기본 목적은 정보시스템 사용자에 초점을 맞춘 정보기술서비스를 제공하고, 조직 목적에 맞는 정보기술서비스를 배치하고, 비용 효과적인 서비스수준협약을 구현하는 것이다.

3 1.3 정보보호관리와 장애관리

정보보호는 데이터 및 시스템을 고의적 혹은 실수에 의한 불법적인 공개(노출), 변조, 파괴, 지체 등으로부터의 보호하는 것이라 할 수 있다. 대부분의 정보가 정보기술에 의존되어 있기 때문에, 전자적인 형태의 정보를 처리, 저장 및 통신하는 모든 단계에 걸쳐서 보호하는 것이다. 정보보호란 위험 중 특히 정보보호위험(security risk)으로부터의 안전을 의미하며, 이러한 정보보호의 목표는 (1) 정보의 비 인가된 공개에 대한 비밀성(confidentiality), (2) 정보의 불법적인 변조 및 파괴에 대한 무결성(integrity), (3) 정보서비스 이용불가에 대한 가용성(availability)을 확보하는 것이다. 정보보호관리(SM: Security Management)는 정보의 비밀성, 무결성, 가용성을 확보하기 위해서 정보보호위험을 관리하는 것이다. 조직시스템의 일반적인 위험 중에서 비밀성, 무결성, 가용성 등과 관련된 정보보호위험은 물리적 정보보호위험, 논리적 정보보호위험, 관리적 정보보호위험으로 구분할 수 있다. 여기서 물리적 정보보호위험에는 환경, 물리적 접근, 물리적 가용성 등에 관한 정보보호위험이 있고, 논리적 정보보호위험에는 소프트웨어, 데이터, 통신 등에 관한 정보보호위험이 있으며, 관리적 정보보호위험에는 행정적, 조직적, 인적 정보보호위험이 있다.

모든 조직의 업무내용과 프로세스가 물리적이고 정태적인 것이 디지털과 모바일에 의해서 가상적이고 동태적인 것으로 급격하게 변화하고 있는 최근에, 정보보호관리를 위해서 비밀성 및 무

결성 보다는 가용성 확보가 중요하다. 왜냐하면, 가용성이 확보되지 않으면 정보서비스 이용이 불가능하므로, 비밀성 및 무결성도 의미가 없기 때문이다. 이와 같이 정보기술에 대한 가용성을 확보하기 위해서 정보보호위험을 관리하는 것이 가장 중요시되고 있는 이유는 정보기술서비스의 중단(downtime)에 의한 업무영향이 너무 커지고 있기 때문이다. 미국의 경우 정보기술서비스 중단으로 인한 시간당 평균 손실액이 약 1,000,000달러에 이르고 있다. 서비스 중단의 원인은 한국의 경우, 통신시설 고장 30%, 하드웨어 고장 26%, 소프트웨어 오류 23%, 인간의 오류 16%, 환경적 원인 4%, 원인을 모르는 경우 1%이다. 이러한 정보기술서비스 중단에 의한 업무영향은 매출감소, 사용자불만족 증가, 직원들의 생산성 감소 등과 같은 위험으로 나타나고 있다.

ISO의 정보보호관리표준으로 대표적인 것이 ISO 13335 MICTS (Management of Information and Communication Technology Security)와 ISO 17799 표준이다. ISO 13335는 정보보호관리와 관련된 국제표준으로서, Part 1 정보보호관리 모형 및 Part 2 정보보호위험관리 기술표준이 있다.

Part 1은 정보보호관리 프로세스를 (1) 전사적 정보기술 정보보호정책 수립, (2) 조직차원에서 정보기술 정보보호정책 수립, (3) 위험관리 프로세스, (4) 보안대책 실행 및 보안의식 제고, (5) 사후관리 활동으로 구분하고 있다. 여기서 위험관리 프로세스는 세부적으로 (1) 전사적 위험분석전략의 선택, (2) 정보기술 정보보호 대책 선택, (3) 정보기술 시스템 정보보호 정책 수립, (4) 정보기술 정보보호 계획 수립으로 되어 있다. 이와 같이 정보보호관리 내의 한 영역으로서 협의의 개념의 위험관리가 있고, 위험관리 활동 내에 위험분석이 있으며, 전사적 위험분석전략에는 네 가지 방법, (1) 기준선 접근방법(Baseline Approach), (2) 비공식적 접근방법(Informal Approach), (3) 상세 위험분석(Detailed Risk Analysis), (4) 혼합 접근방법(Combined Approach) 이 있다.

Part 2는 정보보호 위험분석기술에 대한 표준으로, (1) 정보보호위험의 식별, (2) 정보보호위험 분석, (3) 정보보호위험 평가, (4) 정보보호위험 처리 등 일련의 위험관리활동을 기술적인 측면에서 기술하고 있다. 정보보호관리와 장애관리의 위험평가를 비교하기 위해서, ISO 13335와 ITIL을 비교한 것이 〈표 3-2〉이다.

〈표 3-2〉 ISO 13335와 ITIL의 위험평가 비교

	정보보호관리	장애관리
표준	ISO 13335	ITIL
목표	비밀성, 무결성, 가용성 확보	가용성 확보
관점	위험분석	정보기술서비스
평가 대상	정보보호위험(security risk)	장애(incident)
평가 방법	비공식적 접근방법, 기준선 접근방법, 혼합접근방법, 세부 위험분석	영향도와 긴급도 측정
평가 절차	1) 정보보호위험의 식별 2) 정보보호위험 분석(자산, 위협, 취약성 분석) 3) 정보보호위험 평가(정보보호대책 선택) 4) 정보보호위험 처리(정보보호대책 실행)	1) 장애의 식별 2) 영향도의 측정 3) 긴급도의 측정 4) 장애복구 우선순위 결정
평가 결과	정보보호대책(통제) 선택 및 실행	장애등급(장애복구 우선순위) 결정

ISO 17799는 영국의 정보보호 표준인 BS 7799 Part 1의 정보보호관리 실무규정을 2000년 ISO에서 국제표준으로 채택한 것으로, 전 세계로부터 정보보호관리의 최선 실무방법을 수집해서 11개 분야 127개의 통제항목을 정보보호관리 표준으로 제시한 것이다. 위험평가방법 관점에서는 ISO 17799는 ISO 13335의 기준선 접근방법에 해당된다고 할 수 있다. ISO 17799는 정보보호관리 프로세스를 제시하고 있지 않으나, 정보보호 관리체계(ISMS)는 현재 2008년을 목표로 국제표준화 작업 중이다. ISO 17799의 정보보호 관리체계(ISMS)는 (1) 정보보호 관리체계(ISMS) 수립, (2) 실행 및 운영, (3) 모니터링 및 검토, (4) 유지관리 및 개선, 등 4단계가 PDCA(Plan, Do, Check, Act)를 반영한 체계로 구성되어 있다. 세부적으로 정보보호 관리체계(ISMS)는 (1) 정보보호 정책 수립, (2) 관리체계 범위 설정, (3) 위험관리, (4) 구현, (5) 사후관리 등 5단계로 구성되어 있다. ISO SC 27에서는 정보보호관리 표준이 현재 ISO 17799와 ISO 13335에 혼재되어 있어서, 정보보호관리 모형, 정보보호 관리체계(ISMS), 위험관리 방법, 통제지침 등 4가지 측면에서 통일된 체제를 만들려는 작업이 진행되고 있다.

3 1.4 정보기술서비스관리의 주요 구성요소(BS 15000)

1) BS 15000의 목적

- 정보시스템 사용자의 요구사항을 만족하는 정보기술서비스 경영을 개발하고 구현할 수 있는 방법이나 표준을 제공
- 운영 중인 정보기술시스템의 품질을 통제하고 관리하기 위한 방법론을 평가
- 정보기술서비스를 정보시스템 사용자에게 제공하는 방법의 효과성을 평가

2) BS 15000의 구성체계

BS 15000은 2000년에 최초로 제정되었으며, 다음의 두 개 부분으로 구성되어 있다.

- BS 15000-1 : 2002 정보기술서비스 경영 Part 1 : 정보기술서비스 경영을 위한 규격으로 인증 심사에 사용된다. 인증을 준비하는 서비스 제공자는 이 규격을 준수해야 한다.
- BS 15000-2 : 2003 정보기술서비스 경영 Part 2 : 정보기술서비스 경영을 위한 실무 지침으로 Part 1의 요건에 대한 가이드와 최선의 실행지침(Best Practices)을 제공한다.

3) 서비스제공 프로세스(Service Delivery Processes)

정보기술서비스의 수준을 정의, 합의, 기록 및 관리하기 위한 서비스수준관리, 정보기술서비스에 대한 보고절차 및 시기, 가용성과 지속적인 서비스를 보장하기 위한 절차, 예산 및 회계 관리, 용량계획 및 정보보호관리 등을 정의한 프로세스이다.

- 정보기술서비스수준관리(ITSLM : IT Service Level Management)
- 재무관리(Financial Management) : 정보기술서비스를 위한 예산 및 회계
- 용량관리(Capacity Management)
- 정보기술서비스 연속성관리(IT Service Continuity Management)
- 가용성관리(Availability Management)
- 정보보호관리(Information Security Management)

4) 관계 프로세스 (Relationship Processes)

정보기술서비스를 제공받는 사용자의 업무를 이해하고, 서비스 제공자, 협력업체(Supplier) 및 정보시스템 사용자 3자간의 좋은 관계를 수립하고 이를 유지 · 관리하기 위한 프로세스이다.

- 업무관계관리(Business Relationship Management)
- 협력업체관리(Supplier Management)

5) 해결 프로세스(Resolution Processes)

정보기술서비스에서 발생할 수 있는 장애에 대해서 신속하게 합의된 서비스를 복구하거나 또는 서비스 요구에 대응하고, 장애의 근본 원인 분석, 사전 정의 활동 및 문제 종결 관리를 통해 업무중지를 최소화하기 위한 프로세스이다.

- 장애관리(Incident Management)
- 문제관리(Problem Management)

장애관리는 정보기술서비스관리의 해결 프로세스(Resolution Processes)의 일부로서, 장애관리(Incident Management)와 문제관리(Problem Management)로 구분된다. 장애관리의 목적은 신속하게 업무(Business)에 대해서 사용자와 합의된 서비스를 복구하거나 또는 정보시스템 사용자의 서비스 요구에 대응하기 위한 것이다. 장애관리 절차를 위해서 장애에 대한 기록, 우선순위, 업무 영향, 등급, 상부 보고, 종료 등을 정의하고 있다. 문제관리(Problem Management)의 목적은 정보기술서비스 사고의 근본 원인 분석, 사전 정의 활동 및 문제 종결관리를 통해 업무중지를 최소화하는 것이다. 문제관리 절차는 문제의 정의, 문제에 대한 기록, 분류, 갱신, 상부보고, 종료, 잠재적인 문제를 줄이기 위한 예방활동, 문제의 근본 원인을 수정 변경하기 위한 기존 변경 절차 준수, 알려진 오류에 대한 상시 갱신 책임 할당 등이다.

6) 통제 프로세스(Control Processes)

전체 정보기술서비스 프로세스 중에서도 구심점이 되는 프로세스로서, 정보기술서비스와 인프

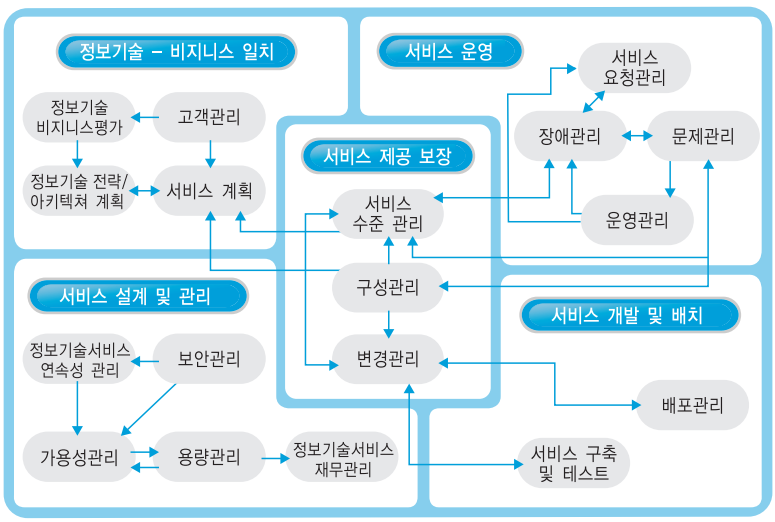
라의 구성 요소를 정의 및 통제하고 정확한 구성 정보를 유지하는 구성관리와 통제된 방식을 통해 모든 변경 사항이 평가, 승인, 구현 및 검토하는 변경관리를 위한 프로세스이다.

- ▶ 변경관리(Change Management)
- ▶ 구성관리(Configuration Management)

7) 배포 프로세스(Release Processes)

배포할 변경 사항을 운영환경으로 전환, 배포하며 기록 관리하기 위한 프로세스이다.

이와 같이 정보보호관리와 가용성관리는 서비스 제공 프로세스에 있으며, 이러한 서비스 제공에 장애가 발생되는 경우에는 해결 프로세스의 장애관리에서 장애에 대한 해결을 시도하고, 해결이 되지 않는 경우에만 문제관리로 이관되어서 장애의 근본원인에 대한 도출을 시도하게 된다. 장애관리란 정보기술서비스관리의 해결 프로세스의 일부로서, 장애관리와 문제관리로 구분되며, 자원복구관점에서 운영적 위험, 특히 정보기술 관련 운영적 위험에 대응해서 신속하게 사용자와 합의된 서비스를 복구해서 서비스 요구를 충족시키려는 일련의 통제행위이다. ITIL 및 BS 15000을 근간으로 해서 설계된 정보기술서비스관리 참조모형의 사례가 (그림 3-3)이다.



(그림 3-3) 정보기술서비스관리 참조모형(ITSM Reference Model) 사례

3 1.5 통제 가능성 관점에서 재해와 장애의 개념구분

정보시스템의 장애에 관한 광의의 개념은 정보시스템의 정상적인 운영을 방해하는 자연 재해, 시스템 장애와 기반구조 장애(혹은 운영 장애와 설비 장애 등)를 모두 포함한다. 광의의 개념은 정보시스템에 직·간접적으로 영향을 미치는 모든 요인들을 포함한다. 협의의 개념에서는 광의의 개념에서 포함한 자연 재해를 제외한 직접적으로 정보시스템에 영향을 미치는 요인들 즉, 시스템 장애와 기반구조 장애(혹은 운영 장애와 설비 장애 등)와 같은 요인들만을 포함한다.

정보시스템의 장애에 관한 광의와 협의의 개념은 그 직접적인 통제가능성으로 나눌 수 있다. 광의는 직접적인 요인뿐만 아니라 간접적인 요인까지도 포함한다. 반면 협의는 직접적인 요인 즉 통제 가능한 요인들만 포함한다. 이러한 개념에 대해 일반적인 시각에서는 협의의 개념을 선호한다. 광의의 개념은 정보시스템 관리부서가 직접 통제할 수 있는 문제가 아니기 때문이다. 특히 지진이나 홍수 혹은 파업 등은 전사적(全社的) 차원에서 취급해야 할 문제이기 때문이다. 그러므로 재해와 장애의 개념구분은 정보시스템 조직 관점에서의 통제가능성에 따라서, 통제 가능한 요인에 의한 기능저하, 오류, 고장을 장애라고 하고, 그 외에 통제 불가능한 경우는 재해라고 한다.

자연 재해는 일반적인 지진이나 태풍, 홍수 등 통제 불가능한 요인에 의한 것이고, 인적 재해는 화재, 폭동, 폭발, 테러 등 통제 불가능한 요인에 의한 것이다. 그러나 운영 장애는 정보시스템을 구성하는 각종 기기의 운영상의 오류나 고장 및 소프트웨어의 장애나 바이러스 및 해킹에 의한 시스템 파괴 등 통제 가능한 요인에 의한 것이고, 설비 장애도 각종 전산 설비 및 통신 장애 그리고 정전 및 화재 등 통제 가능한 요인에 의한 것이다. 정보시스템의 운영에 있어서 자연 재해 및 인적 재해와 관련된 요인들은 아주 특별한 경우를 제외하고는 직접적으로 관련되어 있지 않는데, 운영 장애와 설비 장애 등은 직접적으로 정보시스템의 전산 장애와 관련되어 있다. 한 예로, 네트워크 장애의 경우 회선불량이나 트래픽의 과부하로 시스템의 성능이 저하되는 경우가 있는데 이러한 예는 일상적인 정보시스템을 관리하는 측면에서 자주 부딪히는 문제이다. 즉, 협의의 개념에서의 정보시스템 장애는 정보시스템을 관리하는 부분에서 직접 통제 가능한 경우이다. 자연 재해

나 인적 재해는 정보시스템 관리자가 직접 통제할 수 있는 범위가 아니다. 그러나 설비 장애나 운영 장애 부분은 시스템 관리자가 직접 통제할 수 있다.

3 1.6 프로세스 관점에서 장애의 개념

1) 장애(Incident)

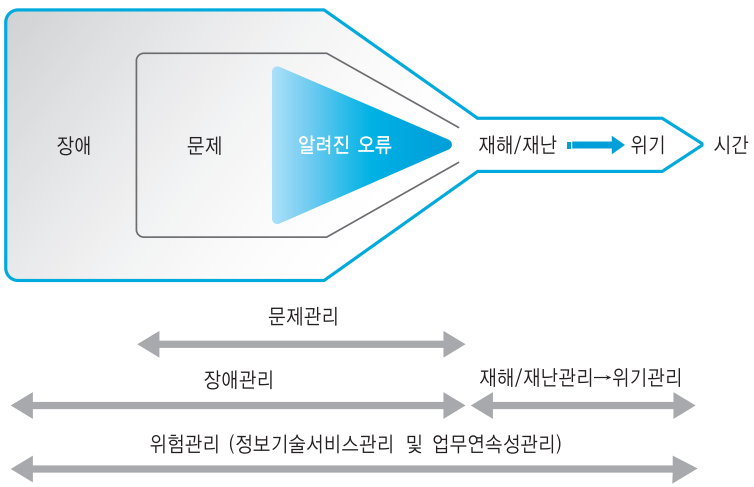
'장애(사고)는 정보기술 운영서비스에 영향을 주는 예상치 못한 사건' 이라고 정의한다.

2) 문제(Problem)

'문제는 단순한 사고가 원인이 되어 발생하지만 근본원인(Root Cause)을 파악 할 수 없는 사건' 이라고 정의한다.

3) 알려진 오류(Known Error)

'알려진 오류는 문제에 대한 근본원인이 밝혀져서 향후 재발생시 참조 가능한 상태의 사건' 이라고 정의한다.



(그림 3-4) 장애, 문제, 알려진 오류의 개념도

프로세스 관점에서 '장애'는 정보시스템 운영상에서 발생되는 사건이므로, 미약하더라도 정보기술서비스에 영향을 주게 된다. '문제'는 단순한 장애가 원인이 되어 다발적으로 발생되는 사고로써, 장애의 근본원인을 파악할 수 없는 경우에 해당한다. '알려진 오류'란 문제에 대한 근본원인이 밝혀져서 향후 재발생시 참조 가능한 상태에 있는 오류를 의미한다. 그러므로 근본원인이 계속 밝혀지지 않은 문제에 대한 잠재적 손실은 시간이 지날수록 지수적으로 증가되어 재난으로 진화되고 위기로 발전될 가능성이 매우 커지게 된다. 장애등급이 높고 허용 시간 내 복구가 불가능해서 심각한 결과를 초래할 것으로 예상되는 경우에는 비상 계획에 따라 대응하여 단순한 문제가 재해로 전환될 가능성을 최소화시켜야 한다.

3 1.7 발생원인 관점에서 장애의 개념

정보시스템에 치명적인 손상을 주는 장애 및 재해에는 여러 가지 다양한 종류들이 있으나 크게 자연 재해, 인적 재해, 시스템 장애, 기반구조 위협 등으로 분류해 볼 수 있다. 발생원인 관점에서 정보시스템 장애의 개념은 다음과 같이 정의할 수 있다.

1) 시스템 장애

'운영체제(OS) 결함, 응용프로그램의 결함, 통신프로토콜의 결함, 통신 소프트웨어의 결함, 하드웨어의 손상 등 통제 가능한 시스템 요인에 의한 기능저하, 오류, 고장'이라고 정의한다.

2) 기반구조 장애

'정전사고, 단수, 설비 장애(항온항습, 공기정화시설, 통신시설, 발전기, 공조기 등), 건물의 손상 등 통제 가능한 기반구조 요인에 의한 기능저하, 오류, 고장(설비 장애 포함)'이라고 정의한다.

3) 기술적 장애

'시스템 및 기반구조 등 통제 가능한 기술적 요인에 의한 기능저하, 오류, 고장'이라고 정의한다.

4) 운영 장애

'시스템 운영과 관련된 통제 가능한 기술적 및 인적 요인에 의한 기능저하, 오류, 고장'이라고

정의한다.

5) 인적 장애

'시스템운영 실수, 단말기 및 디스켓 등의 파괴 및 절취, 해커의 침입, 컴퓨터 바이러스의 피해, 자료누출 등 통제 가능한 인적 요인에 의한 기능저하, 오류, 고장' 이라고 정의한다.

3 1.8 복구시간 관점에서 장애의 개념

'정보시스템 구성요소의 부분적인 기능저하, 오류, 고장으로 인한 서비스 중단에 대한 복구를 위해서 허용 가능한 시간(예로써 24시간) 이내인 경우' 를 장애라고 정의한다. '허용 가능한 시간(예로써 24시간)을 초과한 경우' 는 재해라고 정의한다.

정보시스템 장애는 일반적으로 '하드웨어(주전산기, 디스크, 테이프, 통신장비 등)나 소프트웨어(운영체제, 응용 소프트웨어, 데이터베이스)의 오류로 발생한 시스템 불능 상태로서 대개 수분에서 수 시간 내에 복구가 가능한 경우' 라고 하여 복구의 용이성과 복구시간 면에서 서로 구분하고 있다.

정보시스템 재해는 일반적으로 '정보시스템 내의 하드웨어, 소프트웨어, 설비 및 인력 등이 자연 재해 혹은 인적 재해 등으로 인해 정상적인 기능을 발휘할 수 없을 정도로 훼손되어 이를 복구하는데 허용 가능한 시간 이상이 소요되는 경우' 라고 정의한다. 일반적으로 정보시스템 재해란 '정보시스템에 천재(天災) 또는 인재(人災)로 인하여 예상하지 못한 돌발 상황이 생겨 시스템의 가동이 전면 중단되고 허용 가능한 시스템 중단시간을 초과한 경우' 를 말한다.

각 산업별, 기관별 시스템 중단의 '허용 가능한 시간' 또한 천차만별인 가운데 국가 · 사회적으로 막대한 영향력을 미치는 중요한 전산센터일수록 단 몇 시간의 장애라 하더라도 재해와 동일한 막대한 손실이 발생할 수 있어 백업대책에 있어서 장애와 재해를 엄밀히 구분할 필요성은 적어지고 있다. 최근 각 기관들의 백업시스템을 통한 장애 및 재해 대책에서는 장애와 재해를 구분하지 않고 포괄적으로 대처하는 경향이 두드러지고 있다.

정보시스템의 상태는 평상상태와 비상상태로 구분되며, 비상상태는 또 다시 장애상태와 재해상태로 구분할 수 있고, 장애 및 재해 상태로부터 평상상태로 전환되는 것을 복구(recovery)라고

한다. 여기서 정보시스템의 평상상태란 정보시스템의 본래 요구대로 기능을 충분히 발휘하는 상태를 말한다.

□ 공공기관 정보시스템의 목표복구시간

목표복구시간(RTO: Recovery Time Objective)이란 '비상사태 또는 업무중단 시점부터 업무가 복구되어 다시 정상가동 될 때까지의 시간'을 말한다. 이와 유사한 개념으로 목표복구수준(RPO: Recovery Point Objective)이란 '비상사태 또는 업무 중단 시점부터 데이터가 복구되어 다시 정상가동 될 때까지의 시간(즉 데이터가 복구되어야 하는 시점)'을 말한다.

본 지침에서 공공기관 정보시스템 장애 복구시간에 대해 특정 시간을 정의하지는 않을 것이다. 왜냐하면, 각 기관에서 운영하는 정보시스템의 업무 중요도에 따라 시스템별 복구 요구 시간이 달라지기 때문이다. 따라서, 각 기관은 시스템의 특성과 장애시 복구 중요도를 계산하여, 목표복구시간을 각각 정의하도록 해야 한다.

참고로, 금융감독원은 재해복구센터 구축방법 및 복구시간은 비용, 파급효과 등을 고려하여 금융권역별로 차등 적용하고 있으나 대체로 은행, 증권, 신용카드사 등 주요 금융기관 및 금융공

〈표 3-3〉 금융기관별 복구시간

기 관	복구시간	비 고
은행 및 증권	3시간 이내	
금융공동망 운영기관, 공인인증센터	3시간 이내	금융결제원, 코스콤(구 증권전산)
증권유관기관, 통합시스템 운영기관	3시간 이내	증권거래소, 선물거래소, 코스닥 시장증권, 증권예탁원, 금고연합회
보험	24시간 이내	외국보험사 포함
외국계 금융기관	자 율	복구시간공개, 비상사태대응방안 제출
기타 금융기관	자 율	비상사태대응방안 제출

동망을 운영하는 기관, 공인증센터 등에 대하여 재해 발생시로부터 3시간 이내 완전 복구가 가능한 수준인 HOT사이트 수준의 백업센터를 구축하도록 권고하고 있다.

그러나 금융감독원은 직접 감독권이 없는 금융결제원과 코스콤(구 증권전산) 등에 대해서는 금융공동망 운영기관 및 공인인증센터의 재해 발생시 금융망 및 인증 업무 마비로 인하여 타행환, 차액결제, CD공동망, 해외 지급결제업무(SWIFT), 인터넷 뱅킹, 사이버 증권거래 등의 업무수행이 불가능하므로 은행, 증권사와 동일한 기준의 적용이 필요하다고 판단, 직접 권고가 아닌 협조요청 형태로 백업센터 구축을 촉구하고 있다.

3 2 용어정의

1) 목표복구수준(RPO : Recovery Point Objective)

비상사태 또는 업무중단 시점부터 데이터가 복구되어 다시 정상가동 될 때까지의 시간(즉 데이터가 복구되어야 하는 시점)

2) 목표복구시간(RTO : Recovery Time Objective)

비상사태 또는 업무중단 시점부터 업무가 복구되어 다시 정상가동 될 때까지의 시간

3) 문제(Problem)

단순한 사고가 원인이 되어 발생하지만 근본원인(Root Cause)을 파악할 수 없는 사건

4) 서비스데스크(Service Desk)

정보시스템 사용자와의 접점으로써 사용자에게 최선의 서비스를 제공하는 창구의 역할을 수행. 즉 서비스 사용자로부터 서비스 개선에 대한 요청을 받아 해결하거나 또는 새로운 서비스를 제공하는 조직

5) 서비스수준협약(Service Level Agreement)

서비스 제공자와 서비스 사용자가 제공될 서비스 및 그와 연관된 여러 조건들에 대한 서로의 책임과 의무사항을 기술해 놓은 협약서

6) 알려진 오류(Known Error)

문제에 대한 근본원인이 밝혀져서 향후 재발생시 참조 가능한 상태의 사건

7) 업무연속성관리(BCM : Business Continuity Management)

업무연속성계획의 개발 및 유지보수를 위한 일련의 관리 과정이며, 조직이 재해로 인한 위험에도 불구하고, 조직의 업무를 사전에 결정한 최소한의 수준으로 영위하기 위한 일련의 통제행위

8) 에스컬레이션(Escalation) 절차

장애 등급에 따라 1, 2차 지원그룹에서 해결을 시도할 수 있는 제한시간 및 보고단계를 미리 정해두고, 정보시스템 사용자가 장애 해결을 요청하였을 때, 해당 장애의 우선순위와 시간 경과에 따라 자동 또는 수동으로 장애를 다음 단계로 이관 및 보고하는 절차

9) 위험관리(Risk Management)

조직의 손실, 재해, 개인적 피해 등을 최소화시키기 위한 절차 혹은 연속적인 행위(위험의 분석, 평가, 대책 등)

10) 장애(Incident)

정보기술서비스관리의 통제 가능성 관점에서 협의의 장애 개념으로서, 통제 불가능한 재해(자연 재해와 인적 재해)를 제외한 발생원인 관점에서 직접적으로 영향을 미치는 인적장애, 시스템 장애, 기반구조 장애(운영 장애, 설비 장애 등 포함) 등과 같은 통제 가능한 요인들에 의한 정보시스템의 기능저하, 오류, 고장

11) 장애지식 데이터베이스

정보시스템 운영 중 발생된 장애의 등급, 상세내용, 요청자 정보 및 해결 결과 등 관련된 정보를 모아 놓은 데이터베이스

3 3 정보시스템 장애의 요인과 유형

3 3.1 장애의 범위 및 유형 분류

금융감독원에서는 재해의 종류를 자연 재해, 기술적 재해, 인적 재해 등으로 분류하고 있다. 그러므로 정보시스템 장애는 재해와 마찬가지로 몇 가지 기준(발생원인, 발생과정의 시간적 차이, 발생장소, 장애대상, 피해의 직 · 간접성 등)에 의해서 분류할 수가 있다.

가. 발생원인 관점에서 장애의 분류

- ▶ 자연 장애
- ▶ 인적 장애
- ▶ 기술적 장애
  - – 시스템 장애
  - – 기반구조 장애

〈표 3-4〉 정보시스템 재해 및 장애의 분류와 대응방안

통제	재해 및 장애			재해 및 장애의 요인	장애 대응방안
통제 불가능 요인	자연 재해			화재(전산실, 사무실), 지진 및 지반침하, 장마 및 폭우 등의 수재, 태풍 등	재해복구센터 구축을 통한 기기 및 프로그램의 이중화, 데이터 백업 및 소산 철저
	인적 재해			노조파업, 시민폭동, 폭탄테러 등	백업 또는 대체요원 확보
통제 가능 요인	인적 장애		운영장애	시스템운영실수, 단말기 및 디스켓 등의 파괴 및 절취, 해커의 침입, 컴퓨터 바이러스의 피해, 자료누출 등	
	기술적 장애	시스템 장애		운영체제 결함, 응용프로그램의 결함, 통신프로토콜의 결함, 통신소프트웨어의 결함, 하드웨어의 손상 등	전산기기 이중화 및 프로그램 변경 통제 강화, 재해복구 센터 구축을 통한 기기 및 프로그램의 이중화, 통신망 이중화, 전력공급 중단에 대비한 무정전설비(UPS) 및 발전설비 구축
		기반구조 장애		정전사고, 단수, 설비 장애(항온항습, 공기정화시설, 통신시설, 발전기, 공조기등), 건물의 손상 등	

나. 프로세스 관점에서 장애의 분류

- 장애(Incident)
- 문제(Problem)
- 알려진 오류(Known Error)

다. 정보시스템의 위협요인(Threat Agents) 관점에서 장애의 분류

사람이 원인이 아닌 경우와 사람이 원인인 경우로 크게 두 가지로 구분할 수 있다.

1) 사람이 원인이 아닌 요인으로 발생하는 장애

사람이 원인이 아닌 장애도 불규칙적인 경우와 규칙적인 경우로 크게 두 가지로 구분할 수 있다.

- 불규칙적 장애 : 정보시스템에서 발생(소프트웨어 자체 결함, 컴퓨터 구성요소의 결함, 네트워크 결함, 하드웨어 결함), 자연에서 발생(지진, 물의 범람(강의 범람, 제방의 범람, 댐의 범람, 홍수), 번개(정전, 화재), 바람(태풍)), 물리적인 환경에서 발생(전기합선으로 인한 화재, 정전, 절전, 예고되지 않은 전기합선, 지역의 정전), 자연 발생(화재), 물(스플링쿨러의 오작동, 상수도 파괴, 상수도 동파), 공기(먼지로 인한 오염, 위해 물질)
- 규칙적 장애(예상된 사고) : 악성 프로그램 및 코드(해킹 프로그램, 바이러스, 매크로 바이러스, 응용프로그램의 오류), 폭발 위험물 (폭탄, 지뢰), 통신(전파)방해, 방화(화재), 경보기 고장

2) 사람이 원인이 되어 발생하는 장애

사람의 원인에 의한 장애도 조직 내부인 경우와 조직 외부인 경우로 크게 두 가지로 구분할 수 있다.

- 조직 내부인의 장애 : 관리(기업관리자, 운영자 등의 문제), 기술부분(컴퓨터 운영자, 시스템 분석가, 소프트웨어 개발자, 소프트웨어 유지보수자, C/S 기술자, 하드웨어 유지보수자, 네트워크 관리자 등의 장애), 비기술부분(비서실, 인사부, 자금부, 회계부 등의 문제), 정보보호(정보보호부서, 정보보호관리자, 보안경비 등의 장애), 업무 담당자(법률업무자, 감사자, 회계업무자 등의 장애), 환경통제 부문(전기기술자, 상수도담당자, 공기정화담당

자, 소방담당자 등의 장애), 건물관리(청소원, 전기담당자, 상수도담당자, 공기정화 담당자, 집기담당자, 보일러 담당자, 건물관리인, 통신담당자 등의 장애)

- 조직 외부인의 장애 : 외국정부요원, 산업/협회요원, 해커, 범죄자 혹은 범죄단체, 테러리스트, 언론 매체(기자 등)

라. 장애발생 위치(정보시스템 자산) 관점에서 장애의 분류

- 정보 : 소프트웨어, 사람, 정보시스템 사용자, 재무, 법률, 연구, 계획, 보안, 서류, 이메일, 데이터 등과 관련되어서 전자적으로 저장되는 자산
- 과정(처리) : 운영시스템 프로그램, 응용 프로그램, 통신 프로그램, 관리 프로그램, 사용자, 관리, 계획, 보안 등 정보자산의 기본적인 처리절차와 관련된 자산
- 플랫폼 : 처리장치, 통신(네트워크) 기기 등
- 인터페이스 : 네트워크 연결장치, 디스크 및 테이프, 종이 등
- 사람 : 조직구성원, 계약직원 등
- 환경 : 건물, 데이터 센터, 사무실 등
- 기타 유형자산 : 상기 유형자산 분류체계이외의 유형자산
- 무형자산 : 공공신뢰, 사용자서비스, 사용자의 충성심, 상품권, 생산성, 경쟁적 우위, 윤리 등

3.2 장애등급의 분류

3.2.1 장애등급의 측정절차

ITIL에는 구체적인 장애관리 프로세스가 제시되어 있지 않다. 본 지침서에서는 장애관리 프로세스를 (1) 장애 식별 및 접수, (2) 장애등록 및 등급지정, (3) 1차 해결, (4) 장애배정, (5) 2차 해결, (6) 문제관리, (7) 장애종료, (8) 프로세스 점검 등 8단계로 제시했다. 여기서 장애관리의 위험평가는 단계 1과 단계 2에서 이루어진다. ITIL에서 장애등급은 업무 프로세스를 지원하는 정보시

스템의 장애복구의 우선순위를 의미하며, 이러한 장애등급은 장애의 영향도(Impact)와 긴급도(Urgency)에 따라서 측정된다.

▶ 장애등급 = 장애복구 우선순위 = 영향도 × 긴급도
= 잠재적 손실의 영향 × 해결 시간의 중요성

'장애복구 우선순위 = 영향도 × 긴급도 = 잠재적 손실의 영향 × 해결 시간의 중요성' 이라는 개념적 관계식이 성립된다. 왜냐하면, 장애발생 시점 이후에 위험의 크기는 장애해결 시간에 비례해서 지수적으로 증가하는 경향이 있기 때문에, 영향도는 물론 긴급도도 동시에 고려해야 한다. 장애등급의 측정절차는 다음과 같은 순서로 이루어진다.

▶ 장애의 식별
▶ 영향도의 측정
▶ 긴급도의 측정
▶ 장애복구의 우선순위 결정

이러한 장애 등급은 정보시스템의 구성, 업무 프로세스, 조직 시스템의 상황 등에 따라서 여러 가지로 측정되어서 적용될 수 있다. 궁극적으로는 장애등급의 측정을 보다 엄밀하게 적용시키기 위해서는 업무영향분석 (BIA: Business Impact Analysis)과 목표복구시간(RTO)에 관한 자료들이 분석될 필요가 있다. 여기서 업무영향분석의 목적은 중요한 업무 프로세스를 파악해서, 장애 때문에 발생하는 잠재적인 손실(혹은 손해)을 파악하는 것이다. 여기서 업무 프로세스는 특정 조직에서의 업무활동의 집합으로서, 업무기능(예로써, 과 혹은 부)과 업무지원기능(정보기술, 인력자원, 사무서비스 등)에 의존되어 있다.

가. 장애의 식별

장애는 정보시스템 운영상 발생하는 사건으로서, 미약하더라도 업무 프로세스에 영향을 줄

수 있으므로, 다음과 같이 형태(type)와 서비스 두 가지 관점에서 식별해야 한다.

- 형태
- 서비스

식별된 장애는 분류체계상 어떤 분류 영역(예로써, 하드웨어에 관련이 있는지, 소프트웨어에 관련이 있는지 혹은 문서와 관련이 있는지 등)에 속하는지 파악해야 한다. 또한, 장애와 관련된 어떤 서비스 영역(예로써, 정보기술에 대한 요청, 정보시스템 환경에 대한 구성변경, 혹은 업무서비스 복구 등)에 속하는지 파악해야 한다. 여기서 정보기술에 대한 요청이란 정보기술서비스에 대한 일반적인 문의, 비밀번호 변경, 정보시스템 상태에 대한 질문 등이 포함된다. 구성변경에 대한 요청은 하드웨어, 소프트웨어, 절차 등의 변경을 포함한 업무환경에 대한 어떤 변경을 의미한다. 업무서비스 복구에 대한 요청은 하드웨어, 소프트웨어, 네트워크, 절차 등의 기능저하, 오류, 고장 때문에 발생한 정보서비스를 정상상태로 복구하는 것을 의미한다.

서비스 데스크에서는 발생에 대해서 기록할 때, 이와 같은 장애의 형태 및 서비스의 영역을 기록해야 한다. 예로써, 작동되지 않는 프린터에 대한 고장수리 요청이 들어왔을 경우에, 형태의 영역은 '하드웨어', 서비스의 영역은 '서비스 복구' 라고 분류할 수 있다. 서비스 데스크에서 장애의 형태와 서비스를 보다 더 정확하게 식별할수록, 장애에 대한 해결대책을 보다 더 효과적으로 강구해나갈 수 있다.

나. 영향도의 측정

장애의 영향도란 '조직의 중요한 업무 프로세스를 지원하는 정보시스템의 장애 때문에 발생되는 위험으로 인한 잠재적 손실의 영향' 이라고 정의한다. 장애에 대한 잠재적인 영향의 영역에는 화폐가치로 측정되는 재무적 영역(매출감소, 영업권 혹은 신용 손실, 이자 증가, 계약위약금 등)과 화폐가치로 측정할 수 없는 비재무적 영역(기관에 대한 공공의 부정적 이미지, 외부 사용자들의 신뢰감 추락, 내부 종업원들의 사기 저하, 법규위반 등)이 있다. 장애가 업무 프로세스에 미치는

영향을 즉각적으로 평가하기 위해서는 단위 업무 및 이를 지원하는 정보시스템에 관한 기존 장애 데이터베이스로부터 다음과 같은 척도들을 분석하게 된다.

- 장애관련 데이터의 량
- 영향을 받은 업무프로세스 및 정보시스템의 구성부분
- 영향을 받은 시스템의 수
- 영향을 받은 사용자들의 수
- 영향을 받은 사이트의 수

특정 장애가 업무 프로세스의 정보시스템에 미치는 영향을 3점 혹은 4점 등간척도(interval scale)로 측정할 수 있다. 예를 들면, 4점 등간척도로 측정하는 경우 다음과 같이 분류할 수 있다. 조직 내 업무 프로세스에 대한 영향의 범위 관점에서, 개인적인 업무 → 일반 업무 프로세스의 기능 → 특정 부서의 특정 업무 → 전체 조직과 관련된 업무 프로세스로 영향도가 증가한다.

- 낮음 : 어떤 사용자가 새로운 컴퓨터 모뎀이 필요한 경우, 특정의 '개인적인 업무'에 부분적인 영향을 미치는 것이므로, 단순한 조치로 해결이 가능한 장애가 발생한 경우이다.
- 중간 : 특정의 사용자 집단이 일부 데이터베이스를 연결해서 사용할 수 없는 경우, 전체 네트워크 장비와는 관련은 없지만, 데이터베이스와 개인 PC의 연결장애 때문에, '일반 업무 프로세스의 기능'이 부분적으로 중단되거나 혹은 처리가 지연된다.
- 높음 : 전체 조직 중 특정 부서에서 LAN에 연결되지 않는 경우, 조직의 '특정 부서의 특정 업무' 기능이 부분적으로 중단되거나 혹은 처리가 지연된다.
- 매우 높음 : 전체 조직의 이메일 송·수신에 이상이 생긴 경우, 장애가 '전체 조직과 관련된 업무 프로세스'의 광범위한 영역에 걸쳐 비교적 심각한 영향을 미친다.

다. 긴급도의 측정

장애의 긴급도란 '정상적인 업무로 복구시키기 위해서 정보시스템의 장애를 해결해야 하는

시간의 중요성' 이라고 정의한다. 긴급도는 조직의 업무 프로세스에 미치는 영향을 최소화하기 위해서 장애를 얼마나 빨리 해결해야 하는지를 나타낸 것이며, 장애의 발생 시점에서 주요 업무에 미치는 영향 및 업무 프로세스 상의 중요성에 따라 결정된다. 영향도는 영향을 받은 시스템 및 사용자의 수(즉, 장애관련 데이터의 량)를 분석하지만, 이와 같은 장애가 조직의 업무 프로세스에 어떻게 영향을 미치는지에 대해서는 고려하지 않는다. 그러나 긴급도는 업무 프로세스에 미치는 부작용을 최소화시키기 위해서, 장애를 얼마나 빠르게 해결해야 하는지를 나타내는 시간적인 척도를 나타낸다.

영향도와 마찬가지로 특정 장애가 업무 프로세스의 정보시스템에 미치는 장애의 긴급도는 3점 혹은 4점 등간척도로 측정할 수 있다. 예를 들면, 4점 등간척도로 측정하는 경우 다음과 같이 분류할 수 있다. 조직 내 업무 프로세스에 대한 긴급도의 관점에서, 단순한 관리적 조치 → 어느 정도 대응시간을 가지고 해결 → 가능한 신속한 해결 → 즉각적인 해결로 정상 업무에 대한 허용된 복구 시간에 따라 긴급도를 결정한다.

- 낮음 : 어떤 사용자가 새로운 컴퓨터 모뎀이 필요한 경우, 특정의 개인적인 업무에 부분적인 영향을 미치므로, '단순한 관리적 조치로 해결' 이 가능하다.
- 중간 : 특정의 사용자 집단이 일부 데이터베이스를 연결해서 사용할 수 없는 경우, 전체 네트워크 장비와는 관련은 없지만, 데이터베이스와 개인 PC의 연결 장애 때문에, 일반 업무 프로세스의 기능이 부분적으로 중단되므로, '어느 정도 대응 시간을 가지고 해결' 을 해나갈 수 있다.
- 높음 : 전체 조직 중 특정 부서에서 LAN에 연결되지 않는 경우, 조직의 특정 부서의 특정 업무 기능이 부분적으로 중단되므로, '가능한 신속한 해결' 이 필요하다.
- 매우 높음 : 전체 조직의 이메일 송 · 수신에 이상이 생긴 경우, 장애가 전체 조직과 관련된 업무 프로세스에 걸쳐 비교적 심각한 영향을 미치므로, '즉각적인 해결' 이 필요하다.

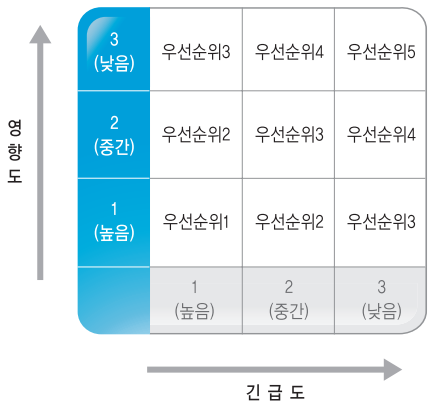
이러한 분류체계에서 영향도 혹은 긴급도는 상황에 따라서 측정치가 바뀔 수 있다. 예를 들어, 어떤 사용자가 작업 집단 디렉터리에 접근할 수 없어서 '일상' 업무가 아닌, '매우 중요한' 업

무를 수행할 수 없다면, 긴급도는 한 단계 상향조정되어서 '높음' 에서 '매우 높음' 으로 측정될 수 있다. 이와 같이 긴급도는 일반적으로 장애를 해결해야 하는 시간의 중요성을 의미한다. 어떤 장애가 아주 긴급한 것으로 분류되었으나, SLA에 설정된 날짜까지 장애가 해결되지 않은 경우에는, 이 장애는 매우 긴급한 문제로 상향조정되어서 상향조정된 수준에서 처리되도록 한다. 이러한 상향조정과정은 자동적으로 진행되도록 해야 한다.

라. 장애복구의 우선순위 결정

장애의 우선순위를 결정하는 중요한 두 가지 요소는 장애가 주요 업무 프로세스에 미치는 잠재적 손실의 영향과 장애해결 시간의 중요성이다. 즉 장애복구의 우선순위는 영향도와 긴급도의 척도에 의해서 결정된다. 장애의 영향도와 긴급도를 각각 3등급(높음, 중간, 낮음)으로 측정해서, 3×3 표로 작성하는 경우에 (영향도 2, 긴급도 1)과 (영향도 1, 긴급도 2)를 동일한 우선순위로 부여한다면, 장애등급을 우선순위 1부터 우선순위 5까지 5등급으로 구분할 수 있다. 이와 같이 정상업무 복귀를 위한 장애복구 우선순위는 영향도와 긴급도를 모두 절충해서 결정하는 것이 합리적이다. 또한, 장애의 영향도와 긴급도를 각각 4등급(매우높음, 높음, 중간, 낮음)으로 측정하여, 4×4 표로 작성하는 경우에, 위와 같은 방법으로 우선순위를 부여한다면, 장애등급을 우선순위 1부터 우선순위 7까지 7등급으로 구분할 수도 있다.

본 지침서에서는 장애등급 우선순위를 (그림 3-5)와 같이 5등급으로 구분한 예를 제공한다.



(그림 3-5) 장애등급을 5등급으로 구분하는 경우

3 3.2.2 장애등급을 5등급으로 구분하였을 때 영향도와 긴급도

가. 우선순위 1

영향도와 긴급도가 각각 '높음' 으로 측정된(영향도 1, 긴급도 1) 경우로서, 내외부의 정보시스템 사용자에 대한 서비스수준에 심각한 영향을 미치는 장애가 발생한 경우이다. 핵심 업무 프로세스의 기능중단으로 막대한 손실을 초래할 잠재적 가능성이 있는 장애가 발생된 경우로서, 잠재적 손실 및 해결시간의 추정에 따라서 비상대책 조직을 가동할 수 있다.

- ▶ 영향도 : 장애가 전체 조직과 관련된 중요한 업무 프로세스의 광범위한 영역에 걸쳐 매우 심각한 영향을 미친다. 메인프레임, 서버, 네트워크 등 주요 시스템(노드) 장애로서, 핵심 업무 프로세스의 기능이 중단되고, 주요 데이터의 손실(혹은 손상)로 인해 경제적 손실이 매우 심각하게 발생한다.
- ▶ 긴급도 : 즉각적인 해결이 필요하다.
- ▶ 보고체계 : 장애발생 즉시 또는 10분 이내에, 상위 조직에 보고하고, 장애발생 이후 30분 단위로 관련 조직에 경과 내용을 전파한다. 장애의 원인을 파악할 수 없거나 장시간 조치가 필요한 경우에는 즉시 비상대책 조직을 가동한다. 장애조치 후 장애보고서를 작성하고, 예방대책을 보고한다.

나. 우선순위 2

영향도와 긴급도가 각각 (영향도 1, 긴급도 2) 및 (영향도 2, 긴급도 1)로 측정된 경우로서, 내외부의 정보시스템 사용자에 대한 서비스수준에 중대한 영향을 미치는 장애가 발생된 경우이다. 우선순위 1의 장애와 유사하지만 좀 더 낮은 영향도와 긴급도를 가진 위험성이 높은 장애를 말한다. 잠재적 손실 및 해결시간의 추정에 따라서, 우선순위 1 등급으로 상향될 수도 있으며, 이에 따른 비상대책 조직을 가동할 수 있다.

- 영향도 : 장애가 전체 조직과 관련된 중요한 업무 프로세스의 부분적인 영역에 걸쳐 비교적 심각한 영향을 미친다. 메인프레임, 서버, 네트워크 등 주요 시스템(노드) 장애로서, 핵심 업무 프로세스의 기능이 부분적으로 중단되거나 혹은 처리가 지연된다. 일반 업무 기능이 중단되고, 주요 데이터의 손실(혹은 손상)로 인해 경제적 손실이 어느 정도 심각하게 발생한다.
- 긴급도 : 가능한 신속한 해결이 필요하다.
- 보고체계 : 장애발생 이후 20분 이내, 상위 조직에 보고하고, 장애발생 이후 30분 단위로 관련 조직에 경과 내용을 전파한다. 장애원인을 파악할 수 없거나 장시간 조치가 필요한 경우에는 우선순위를 상향조정하거나 경우에 따라서는 비상대책 조직을 가동한다. 장애조치 후 장애보고서를 작성하고, 예방대책을 보고한다.

다. 우선순위 3

영향도와 긴급도가 각각 (영향도 1, 긴급도 3), (영향도 2, 긴급도 2), (영향도 3, 긴급도 1) 로 측정된 경우로서, 내외부의 정보시스템 사용자에 대한 서비스수준에 미미한 영향을 미치는 장애가 발생된 경우이다. 조직 내에 작은 부서, 혹은 특정 개인과 관련된 소규모 지역에 국한된 장애로 위험성이 비교적 낮은 장애를 말한다. 잠재적 손실 및 해결시간의 추정에 따라서, 우선순위 2 등급으로 상향조정될 수도 있다.

- 영향도 : 장애가 전체 조직과 관련된 중요한 업무 프로세스가 아니고, 조직의 중간규모 부서의 특정 업무에 심각한 영향을 미친다. 소규모 부서의 네트워크 장비 및 이와 관련된 개인 PC의 장애 때문에, 일반 업무 프로세스의 기능이 부분적으로 중단되거나 혹은 처리가 지연된다.
- 긴급도 : 어느 정도 대응시간을 가지고 해결을 해나간다.
- 보고체계 : 장애발생 이후 1시간 내에 해결이 되지 않는 경우에, 상위 조직에 보고하고, 장애발생 이후 1시간 단위로 관련 조직에 경과 내용을 전파한다. 장애원인을 파악할 수 없거

나 장시간 조치가 필요한 경우라도 우선순위를 상향조정하거나 비상대책 조직을 가동할 필요성은 미미하다.

라. 우선순위 4

영향도와 긴급도가 각각 (영향도 2, 긴급도 3) 및 (영향도 3, 긴급도 2) 로 측정된 경우로서, 내외부의 정보시스템 사용자에 대한 서비스수준에 거의 영향을 미치지 않는 장애가 발생된 경우이다.

- 영향도 : 장애가 전체 조직과 관련된 중요한 업무 프로세스가 아니고, 조직의 소규모 부서의 특정 업무에 미미한 영향을 미친다. 전체 부서의 네트워크 장비와 관련은 없지만 부분적으로 데이터베이스 등과 개인 PC의 연결장애 때문에, 일반 업무 프로세스의 기능이 부분적으로 중단되거나 혹은 처리가 지연된다.
- 긴급도 : 관리적 조치로 해결이 가능하다.
- 보고체계 : 장애처리조직에서 별도로 관리하고, 우선순위 등급이 상향조정 될 때는 상향조정된 등급의 보고 절차에 따른다.

마. 우선순위 5

영향도와 긴급도가 각각 (영향도 3, 긴급도 3) 으로 측정된 경우로서, 내외부의 정보시스템 사용자에 대한 서비스수준에 전혀 영향을 미치지 않는 장애가 발생된 경우이다.

- 영향도 : 장애가 일부 조직의 소규모 부서 내에 특정의 개인적인 업무에 부분적으로 아주 미미한 영향을 미친다. 네트워크 장비와는 전혀 관계없이, 오직 개인 PC 장애로서, 일반 업무 프로세스에 영향을 미치지 않으므로, 단순한 조치로 해결이 가능한 장애가 발생한 경우이다.
- 긴급도 : 관리적 해결이 거의 필요 없다.
- 보고체계 : 장애처리조직에서 별도로 관리하고, 우선순위 등급이 상향조정 될 가능성과 보

고 절차의 필요성이 거의 없다.

〈표 3-5〉 장애 5등급의 영향도와 긴급도

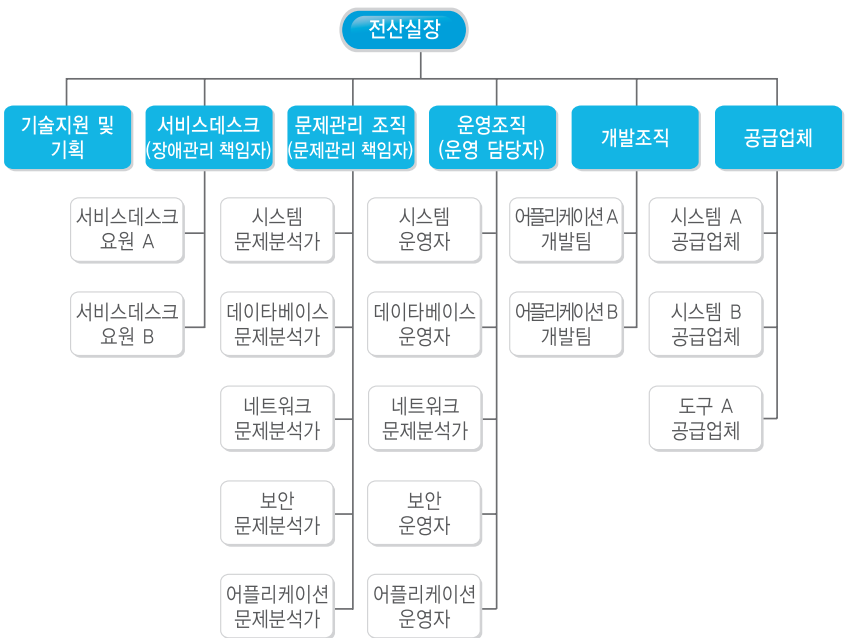
	영향도	긴급도	보고체계
우선순위 1	전체 조직과 관련된 중요한 업무 프로세스에 심각한 영향	즉각적으로 해결	장애발생 즉시 또는 10분 이내 상부 보고
우선순위 2	중요한 업무 프로세스의 부분적인 영역에 비교적 심각한 영향	가능한 신속히 해결	장애발생 20분 이내 상부 보고
우선순위 3	조직의 중간규모 부서의 특정 업무에 심각한 영향	어느 정도 대응시간을 가지고 해결	장애발생 1시간 이내 상부 보고
우선순위 4	조직의 소규모 부서의 특정 업무에 미미한 영향	관리적 조치로 해결 가능	장애처리 조직에서 별도 관리
우선순위 5	특정의 개인적인 업무에 부분적으로 아주 미미한 영향	관리적 해결이 거의 필요 없음	보고 필요 없음

4 장애관리 체계

체계적인 장애관리를 위해서는 장애관리를 수행하는 조직체계와 업무 절차들이 사전에 정의되어야 한다. 본 장에서는 장애관리 업무를 담당하는 조직의 역할과 책임을 살펴보고, 장애관리 절차에 대한 전체적인 흐름에 대해 살펴본다.

4 1 장애관리 조직체계

장애관리의 근본적인 목적은 정보시스템 사용자에게 중단 없는 서비스를 제공하고 장애가 발생하였을 경우 신속한 복구를 수행하는 것이다. 따라서 각종 장애요청을 신속하게 접수 · 해결할 수 있는 서비스 데스크 조직이 필요하며 장애관리 프로세스 관점에서 효율적인 정보시스템 운영을 수행하기 위한 각 담당조직의 명확한 역할 및 책임 설정이 필요하다.



(그림 4-1) 장애관리를 위한 조직도 예

(그림 4-1)은 이해를 돕기 위해 단순화한 조직도의 예이다. 정보시스템의 규모가 크다면 더욱 상세하게 역할을 나눌 수 있고, 정보시스템 규모가 작다면 한 사람이 다른 역할을 중복으로 맡아서 수행할 수도 있다. 여기서 주의해야할 점은 반드시 역할은 철저하게 명시되어 동일한 인물이 여러 가지 역할을 중복해서 맡는다 해도 각각의 역할을 독립적으로 유지해야 한다는 것이다. 또 한 가지 주의해야 할 점은 장애관리 책임자와 문제관리 책임자는 반드시 각각 다른 사람이 맡아야 한다. 문제관리 프로세스의 목적이 근본원인의 해결과 장애의 사전관리에 있기 때문에 신속하게 장애를 해결하려는 장애관리 프로세스와 충돌되는 부분이 존재하기 때문이다.

서비스 데스크(Service Desk)는 정보시스템 사용자와의 접점으로서 사용자에게 서비스를 제공하는 창구역할을 한다. 즉 서비스 사용자로부터 서비스 개선에 대한 요청을 받아 해결하거나 또는 새로운 서비스를 제공하는 역할을 한다. 서비스 데스크에서 가장 주의해야할 점은 사용자의 접점이 분산되지 않도록 하나의 접점(SPOC : Single Point of Contact)을 제공해야 한다는 것이다. 사용자의 입장에서는 사용자에게 필요한 서비스 요청을 하기 위해 서비스별로 다양한 부서의 담당자에게 서비스 요청을 하는 것보다는 하나의 단일 창구에서 전체 서비스 요청을 접수해서 1차적으로 해결하고 그 다음 해당 부서에 연계하는 것이 편의성과 만족도를 높일 수 있기 때문이다.

서비스 데스크는 사용자의 서비스 요청을 1차로 접수 및 해결을 하는 서비스 데스크 요원과 전체적인 프로세스를 감독하는 장애관리 책임자로 기본적으로 구성된다. 규모가 크거나 신속한 서비스 해결이 최우선일 경우에는 2차 지원 그룹도 서비스 데스크에 포함될 수 있다.

정보시스템 사용자는 서비스 요청을 전화, 이메일, 인터넷, 팩스, 또는 모니터링 도구와의 자동 연결 등 다양한 수단을 통해 서비스 데스크에 요청할 수 있다.

가. 장애관리 책임자(Incident Manager)

1) 책임

▶ 1차 지원선에서 발생되는 장애에 대해 신속한 서비스 복구의 책임을 갖는다. 장애에 대응하

여 할 수 있는 모든 작업을 수행하며 아울러 접수된 장애에 대해 기록하고 관리해야 할 의무도 갖는다.

- 사용자가 정보를 찾고자 할 경우나 보고를 원할 경우 사용자와의 창구를 지원한다. 이때 서비스 데스크는 정보기술 조직이 시스템 운영정보를 사용자에게 전달해주기 위한 접점이 된다.
- 장애관리 프로세스에서 관리되는 정보에 대한 1차 정보원 역할을 수행한다.
- 정보시스템 운영을 이끌며 구성원들의 기술 숙련도 수준 향상 및 문제관리 지원, 시스템 제공자, 서비스 지원 그룹과의 효율적인 협력관계를 유지하는 책임을 갖는다.

2) 역할

- 장애발생 빈도를 감소시키면서 안정적인 정보시스템 운영 환경을 구축한다.
- 장애에 대한 신속한 해결을 시도한다.
- 문제관리 책임자, 시스템 제공자, 서비스 지원 그룹에 대한 적절한 통제 및 협의를 통해 보다 나은 서비스 가용율 및 생산성을 보장한다.
- 장애 데이터에 대한 정확한 분석을 통해 문제관리 영역으로의 전이에 대한 판단을 하며 정보기술 조직과 사용자 조직과의 유연한 조화를 유지한다.
- 사용자 만족에 기여한다.
- 품질 높은 정보기술서비스 및 정보시스템 사용자 지원을 위한 정확한 관리 정보를 제공한다.
- 내 · 외부적으로 필요한 지원 조직 간에 유연한 관계를 유지한다.

나. 문제관리 책임자(Problem Manager)

1) 책임

- 장애관리 데이터 분석을 통해 서비스수준에 영향을 미치는 잠재적인 장애에 대한 분석과 이에 연관된 모든 활동을 관리한다.
- 장애의 근본원인에 대한 확인, 해결책 분석, 향후 장애 재발 방지를 위한 해결 및 변경요청에 연관된 모든 활동에 대해 조정 및 관리를 한다.

- 문제관리를 위한 조직을 이끌며 지정된 담당자에 대한 기술력 및 성과에 대한 책임을 갖는다.
- 문제관리 보고에 대한 책임을 갖는다.
- 장애에 대한 에스컬레이션관리 및 해결을 위해 적절한 자원들을 공급하는데 대한 책임을 갖는다.

2) 역할

- 모든 장애에 대한 근본원인을 알아낸다.
- 장애 및 문제에 대한 근본 원인을 제거하기 위해 시스템 변경을 요청한다.
- 한번 해결된 장애에 대한 재발 방지에 노력한다.
- 문제를 최대한 신속하게 처리하고, 근본적인 해결을 통해 장애 위험노출을 최소화한다.
- 내 · 외부의 모든 필요한 지원 조직 간에 유연한 관계를 유지한다.
- 명확하고 효과적인 문제관리 업무 절차를 확립한다.

다. 서비스 데스크 요원(Service Desk Agent)

1) 책임

- 사용자로부터 장애를 접수한다.
- 접수받은 장애를 자체 해결 하거나 문제관리, 시스템 공급자 등 서비스 지원 그룹으로 이관한다.
- 접수되는 모든 장애를 기록한다.
- 장애에 대한 상태나 서비스 요청에 대한 내용을 사용자에게 통보한다.

2) 역할

- 장애로 인한 영향력을 최소화한다.
- 서비스의 신속한 복구를 수행한다.
- 장애의 신속한 해결을 도모한다.
- 1차 지원에서 해결하지 못하는 장애에 대해 신속하고 정확한 대응 방법을 설정한다.
- 장애분류 작업을 수행하고, 장애 관련 정보를 등록 · 관리한다.

- 성실한 태도 및 지원을 통해 사용자만족을 높이도록 노력한다.
- 품질 높은 정보기술서비스 및 사용자지원을 위한 정확한 정보를 제공한다.

라. 문제 분석가(Problem Analyst)

1) 책임

- 서비스 데스크 요원 및 문제관리 책임자를 지원한다.
- 특정 도메인에 대한 축적된 지식경험을 통해 장애의 신속한 해결에 도움을 준다.
- 정보기술 문제 분석가로서의 기술력을 배양한다.
- 장애의 근본원인을 분석한다.

2) 역할

- 장애에 대한 영향력을 최소화한다.
- 장애가 신속하게 복구되도록 노력한다.
- 문제에 대한 근본원인을 분석한다.
- 영구적인 해결책을 위해 다른 전문가와 협력한다.
- 해결책을 실현하기 위해 변경 요청을 한다.
- 품질 높은 정보기술서비스 및 정보시스템 사용자 지원을 위해 정확한 정보를 제공한다.

마. 시스템/서비스 공급자(System/Service Provider)

1) 책임

- 시스템/서비스 공급자는 기관 내 정보시스템을 개발, 공급, 지원하는 누구나 해당될 수 있다. 여기에는 응용 소프트웨어 개발, 데이터베이스 및 기반 시설이 포함될 수 있다.
- 시스템/서비스 공급자는 공급된 시스템/서비스의 원천 정보에 대해 개발 · 변경의 책임이 있다.

2) 역할

- 요구된 변경 요청에 대해 점검한다.
- 완성도 및 정확성을 위한 변경 요청에 대해 점검한다.
- 업무에 미치는 영향에 대해 점검한다.
- 평가, 문서에 대해 기록을 갱신한다.
- 변경 구현을 위한 자원 요구사항을 인지한다.
- 변경이 효율적으로 수행되기 위한 일정을 엄수한다.
- 시스템 구성에 대한 유지보수를 한다.
- 업무 요구 분석으로부터 산출되는 결과를 근거로 요구되는 테스트를 수행한다.
- 변경을 위해 지원되는 항목에 대한 사용자 교육을 실시한다.

바. 운영조직

운영조직은 사용자와의 서비스수준협약에 따라 기관 내 정보시스템의 운영을 담당한다. 운영조직은 운영되는 시스템 자원에 따라 다음과 같은 세부 관리자로 구분될 수 있다. 정보시스템의 규모에 따라 개인이 2개 이상의 역할을 중복하여 맡을 수도 있다.

- 네트워크 운영자
- 시스템 운영자
- 데이터베이스 운영자
- 보안 운영자
- 백업 운영자

1) 책임

- 장애에 대한 2차 지원을 수행하며 문제 해결에도 관여한다.
- 해결된 장애, 문제 및 알려진 오류에 대해 문서화한다.
- 상급자에게 주기적으로 운영결과 보고서를 제출한다.

- 서비스수준에 위배되는 모든 서비스 중단사건 및 돌발사항에 대해 보고한다.
- 하드웨어, 응용시스템 및 운영체제의 장애 예방 활동에 적극적으로 참여한다.

2) 역할

- 시스템 커널 구성, 응용시스템 구성파일, 프린트 스풀링 관리를 담당한다.
- 디스크 사용현황 , 파일 위치를 관리한다.
- 사용자 및 암호를 관리한다.
- 시스템 로그파일을 관리한다.
- 주요 시스템 파라미터 및 성능지표를 관리한다(하드웨어, 네트워크, 응용시스템, 데이터베이스, 운영체제 및 기타 도구 등).
- 하드웨어, 응용시스템 및 운영체제의 유지보수를 담당한다.
- 시스템의 장애를 진단, 해결한다.
- 필요시 시스템 복구를 수행한다.

4.2 장애관리 프로세스

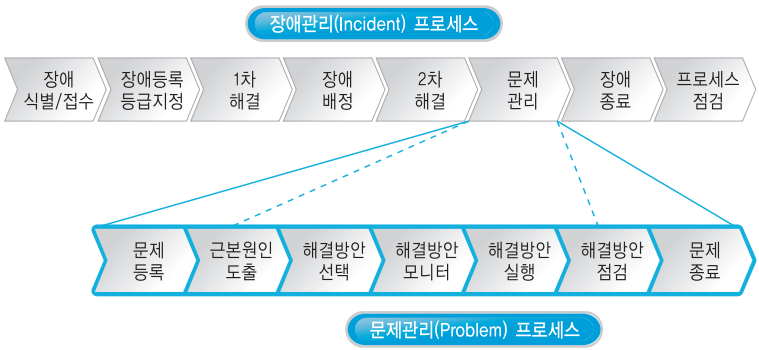
장애관리 프로세스는 다음과 같이 8개의 세부 프로세스로 구성된다.

장애식별/접수 → 장애등록 및 등급 지정 → 1차 해결 → 장애 배정 → 2차 해결 → 문제관리 → 장애 종료 → 프로세스 점검

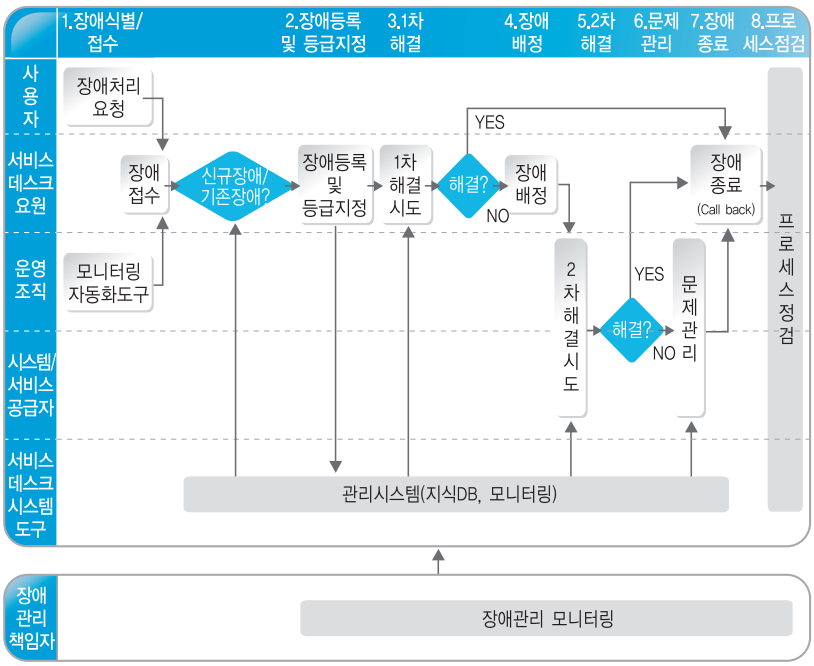
위의 세부 프로세스 중에서 2차 해결 시도에도 풀리지 않은 장애의 근본적인 해결을 처리하는 문제관리 세부 프로세스는 매우 중요하다. 같은 장애가 반복되지 않도록 하기 위한 사전 예방적인 성격을 내포하고 있으며, 다음과 같은 7개의 세부 프로세스로 이루어진다.

문제 등록 → 근본원인 도출 → 해결 방안 선택 → 해결 방안 모니터 → 해결 방안 실행 → 해결 방안 점검 → 문제 종료

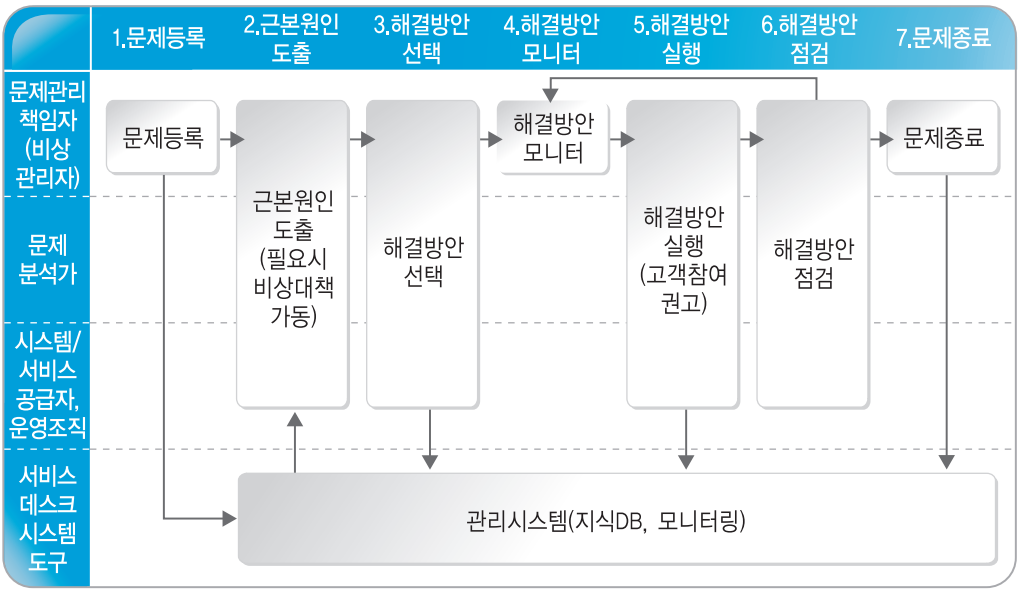
장애관리 프로세스와 문제관리 프로세스 관계는 (그림 4-2)와 같다. 즉, 문제관리 프로세스는 전체 장애관리 프로세스의 일부이며 보다 사전 예방적 관리에 집중하기 위해 별도의 프로세스 관리자와 세부 프로세스를 갖는다.



(그림 4-2) 장애관리 및 문제관리 프로세스 관계도



(그림 4-3) 장애관리 프로세스 흐름도

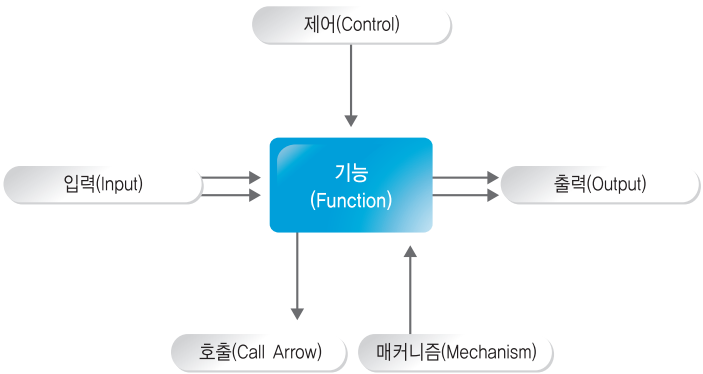


(그림 4-4) 문제관리 프로세스 흐름도

5 장애관리 세부 프로세스

4장에서는 장애 및 문제관리 프로세스를 전체적인 시각에서 살펴보았다. 5장에서는 좀 더 상세하게 접근해서 각 프로세스를 이루고 있는 세부 프로세스의 기능과 역할에 대해 살펴보겠다. 장애관리의 각 세부 프로세스는 IDEFØ(Integrated Computer-Aided Manufacturing (ICAM) DEFinition Ø)의 표기법을 이용하여 도식화 하였으며 각 세부 프로세스에서 주로 수행하는 활동들과 주요 관리 항목, 관련자들의 책임과 역할에 대해 설명한다.

IDEFØ 기능모델은 조직에서 수행되어지고 있거나 수행되어야 할 기능, 또는 기능과 기능간의 관계를 그림과 문자로서 표현해 놓은 표기법이다. IDEFØ는 모델을 박스와 화살표로서 표현하며 기본적 구성은 (그림 5-1)과 같다.



(그림 5-1) IDEFØ 표기법

1) 기능(Function)

기능은 박스형태로 표현되며 활동, 행동, 프로세스, 혹은 운영을 표현하는데 어떠한 상황에서 무엇이 일어나는지에 관한 서술로 사람이나, 기계, 컴퓨터 등에 의해 수행되는 기능을 표현한다.

2) 입력(Inputs)

기능박스의 왼쪽으로부터 들어가는 화살표로 표현되며 기능을 수행하는데 필요한 개체 혹은

데이터로서, 기능이 수행됨에 의하여 소모되거나 변형되는 것을 표현한다.

3) 출력(Outputs)

기능박스의 오른쪽으로 나오는 화살표로 표현되며 기능이나 활동의 결과로 생성되는 산출물을 말한다.

4) 제어(Controls)

기능박스의 위쪽에서부터 들어가는 형태로 표현되며 기능을 통제, 제어하는 제약조건, 지침 혹은 산출물을 결정하는데 필요한 제약조건 등으로 기능의 수행을 통제하거나 시작하게 한다.

5) 메커니즘(Mechanisms)

기능박스의 밑에서부터 들어가는 형태로 표현되며 기능을 수행하는 사람 또는 개체로서, 무엇에 의해 그 기능이 수행되는가 혹은 기능의 수행에 어떠한 자원이 사용되는가를 나타낸다.

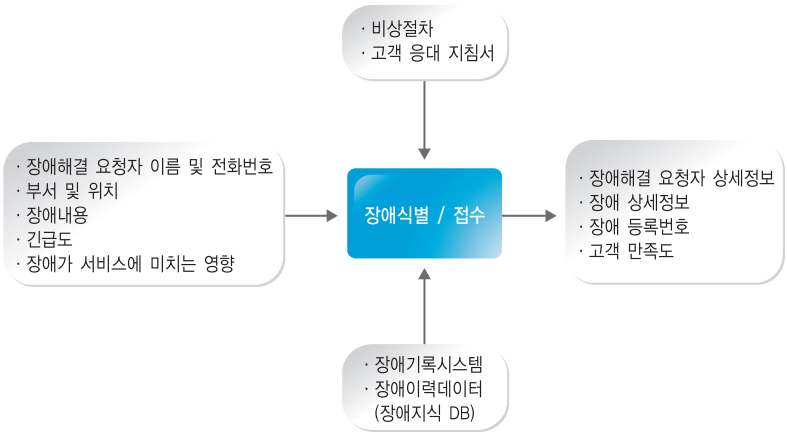
6) 호출(Call Arrow)

기능박스의 밑으로 나오는 형태로 표현되며 활동의 수행과 관련된 보다 상세한 기술을 위하여 관련된 다이어그램을 호출하기 위하여 사용한다. 호출은 동일한 리포지토리(repository)에 있는 모델에서 일어나는 다른 활동을 참조하게 한다.

5 1 장애관리 세부 프로세스

5 1.1 장애 식별/접수

장애는 사용자로부터 유·무선 전화, 이메일 및 인터넷, 방문 등 다양한 방법을 통해 접수될 수 있다. 또한 장애는 모니터링 도구에 의해 감지되어 서비스 데스크 요원에게 자동으로 통보될 수 있다. 접수받은 모든 장애는 향후 관리 및 추적을 위해 기록 되어야 한다.



(그림 5-2) 장애식별/접수

가. 주요 관리 항목

▶ 사용자의 장애 등록 요청 수 대비 장애 등록 수

나. 세부 프로세스 주요 참여자 역할

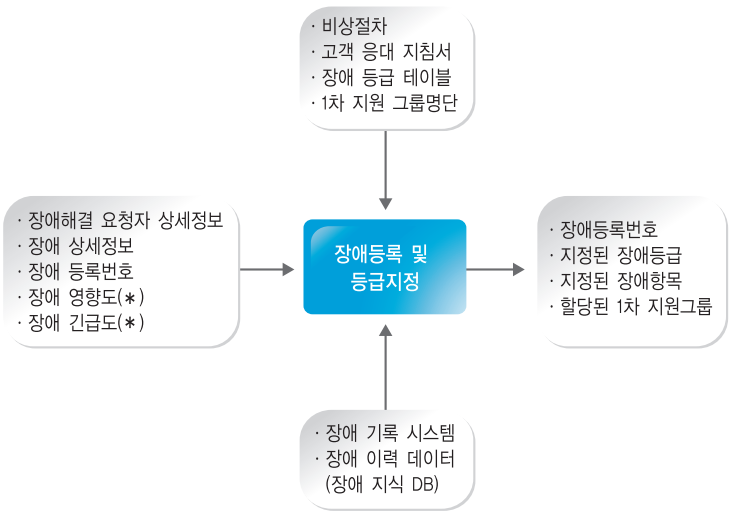
▶ 사용자 : 장애해결 요청

▶ 서비스 데스크 요원 : 장애접수

▶ 모니터링 자동화 도구 : 장애 자동식별

5 1.2 장애 등록 및 등급지정

서비스 데스크를 통해 접수된 정보는 장애 지식 데이터베이스에 기록되어야 한다. 이때 기록되어야 할 사항으로는 장애해결 요청자 정보, 장애내역, 장애의 영향, 장애등급 등이 있다. 장애등급 지정은 업무 프로세스를 지원하는 정보시스템의 장애복구의 우선순위를 의미하며, 이러한 우선순위는 장애의 영향도와 긴급도에 따라 측정된다. 장애등급 지정은 사용자와의 협의를 통해 서비스 데스크 요원이 할당하도록 한다.



(*) : 이전 단계의 세부 프로세스의 출력물과 연계되지 않고 이 단계에서 새롭게 입력된 정보

(그림 5-3) 장애등록 및 등급지정

가. 주요 관리 항목

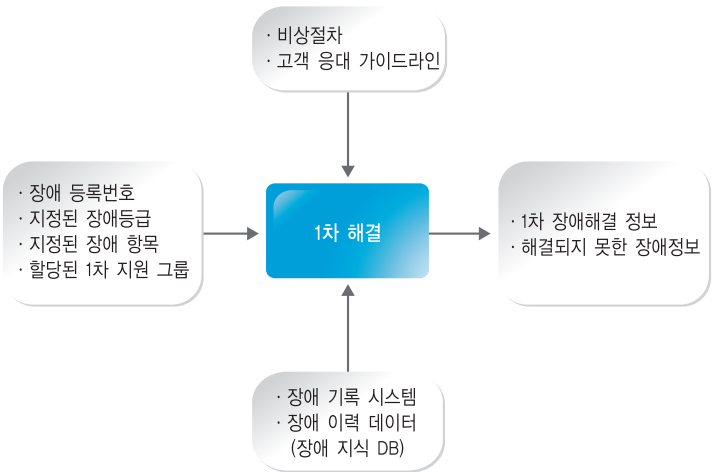
- ▶ 등록된 장애의 수
- ▶ 등록된 장애의 오류 정보 확인 수

나. 세부 프로세스 주요 참여자 역할

- ▶ 사용자 : 장애 상세정보 제공
- ▶ 서비스 데스크 요원 : 장애등록 및 장애등급 지정

5 1.3 1차 해결

서비스 데스크 요원은 정보시스템 사용자의 요청을 접수하여 해당 장애를 해결하려고 시도한다. 이러한 시도에는 관련된 정보를 장애 지식 데이터베이스 검색을 통해 찾는 과정이 포함되며, 해결책이 존재하면 즉시 사용자에게 해결책을 통보하여 해당 장애를 종료하도록 한다. 해당 장애는 해결을 위해 사전에 정의된 시간 범위 내에서 해결하는 것을 원칙으로 한다. 만일 정해진 시간 내에 해결하지 못하거나 정보시스템 사용자가 해결책에 만족하지 못하는 경우, 장애는 2차 지원 그룹(운영조직, 개발조직 및 시스템 공급업체)으로 전달되어 해결하도록 한다.



(그림 5-4) 1차 해결

가. 주요관리 항목

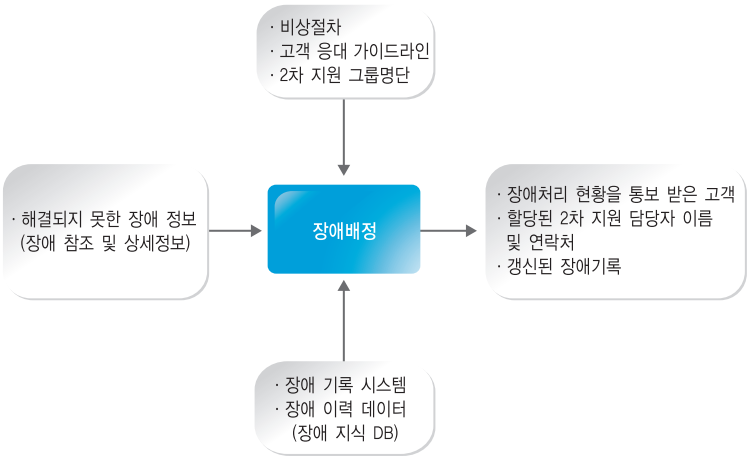
- ▶ 총 등록 장애 수 대비 해결된 장애 수
- ▶ 1차 해결 담당자가 장애해결에 할당한 시간
- ▶ 사용자 만족도

나. 세부 프로세스 주요 참여자 역할

- ▶ 사용자 : 해결책에 대한 의견제시
- ▶ 서비스 데스크 요원 : 장애 1차 해결

5 1.4 장애배정

장애가 1차 지원선에서 해결되지 못한 경우, 장애등급 및 장애와 연관된 에스컬레이션 상태에 따라 장애해결 과정이 실행된다. 서비스 데스크 요원은 장애해결 과정에 대해 최종 해결시까지 지속적으로 관리할 책임을 가지며 해당 장애에 대한 진행 상황을 정보시스템 사용자에게 알릴 수 있는 체계를 갖추고 있어야 한다. 서비스 데스크 요원이 해결하지 못하는 장애는 2차 지원 그룹에게로 재 할당된다.



(그림 5-5) 장애배정

가. 주요관리 항목

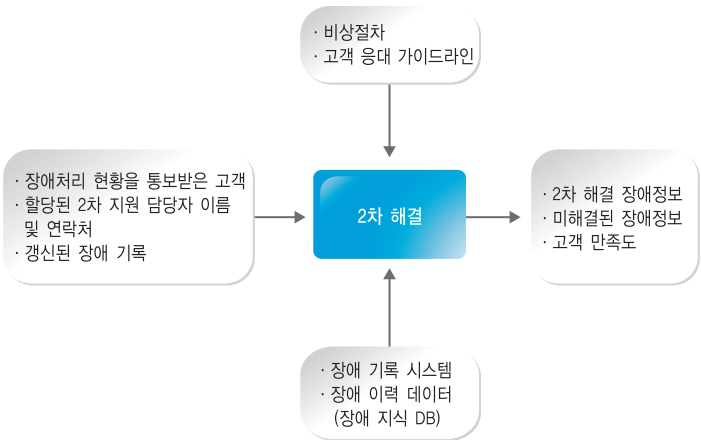
- ▶ 등록된 장애 수 대비 2차 배정된 장애 수
- ▶ 2차 배정된 장애의 재배정 수

나. 세부 프로세스 주요 참여자 역할

▶ 서비스 데스크 요원 : 1차 시도로 해결되지 못한 장애의 2차 해결 배정

5 1.5 2차 해결

장애를 할당 받은 2차 지원 담당자는 장애번호, 장애등급, 장애 상세정보, 과거 장애해결 이력에 대한 정보를 넘겨받아 해결책을 찾는데 참조한다. 이러한 행위는 자동화된 도구를 이용하거나 수작업형태로 진행 가능하다.



(그림 5-6) 2차 해결

가. 주요관리 항목

▶ 총 등록 장애 수 대비 해결된 장애 수

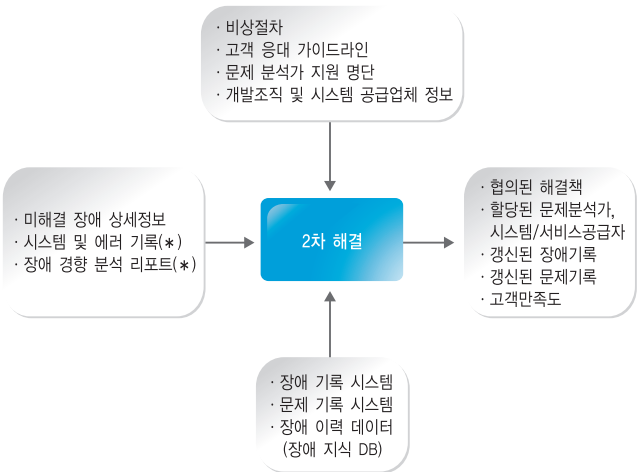
▶ 해결 담당자가 해결에 노력한 시간

나. 세부 프로세스 주요 참여자 역할

- ▶ 사용자 : 해결책에 대한 의견 제시
- ▶ 서비스 데스크 요원 : 장애 해결 상태 점검
- ▶ 운영조직 : 장애가 배정된 경우 해결 시도
- ▶ 시스템/서비스 공급자 : 장애가 배정된 경우 해결 시도

5 1.6 문제관리

장애가 2차 지원그룹에서도 해결되지 못할 경우에는 장애의 근본적인 해결 및 복구를 위해 장애에 대한 조사 및 분석이 뒤따라야 한다. 이러한 장애는 '문제'로 별도로 분류하여 등록되며, 문제 해결을 위한 담당자는 서비스 지원 그룹뿐만 아니라 외부의 협력업체로부터 적절한 인력을 제공하도록 요청해야 한다. 사용자가 해결책이나 복구에 대해 만족하지 않는 경우 해당 문제는 언제라도 에스컬레이션한다. 만일 미리 정의된 시간 범위를 벗어날 경우 장애해결 담당자는 장애등급 변경을 위한 협의를 수행한다. 문제관리의 세부 프로세스에 대해서는 5.2절에서 자세히 설명한다.



(*) : 이전 단계의 세부 프로세스의 출력물과 연계되지 않고 이 단계에서 새롭게 입력된 정보

(그림 5-7) 문제관리

가. 주요관리 항목

- 해결된 장애 수
- 해결에 걸린 시간
- 사용자 만족도

나. 세부 프로세스 주요 참여자 역할

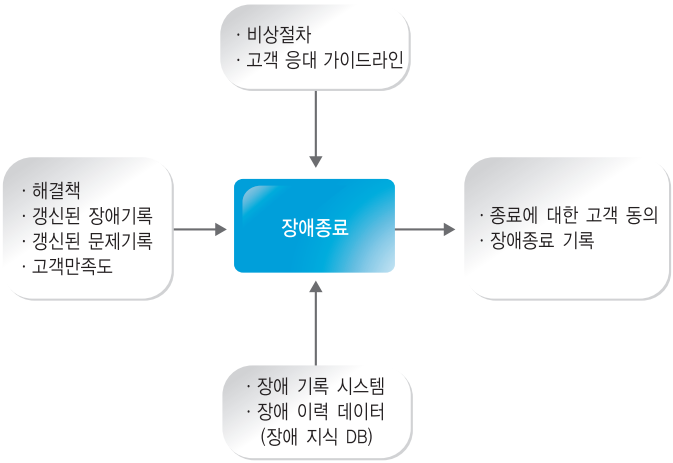
- 사용자 : 해결책에 대한 의견 제시
- 서비스 데스크 요원 : 장애해결 상태 점검
- 운영조직 : 할당된 문제해결
- 시스템/서비스 공급자 : 할당된 문제해결
- 문제 분석가 : 할당된 문제 해결
- 문제관리 책임자 : 문제등록 및 문제 점검

5 1.7 장애종료

장애에 대한 해결책을 성공적으로 찾은 경우 서비스 데스크 요원은 사용자와의 협의를 거쳐서 해당 장애를 종료한다. 장애가 다수의 사용자들로부터 발생한 내용일 경우 그룹 메시지를 보내어 해결 결과를 통보할 수도 있다.

가. 주요관리 항목

- 전체 장애 수 대비 종료된 장애 수
- 사용자 만족도



(그림 5-8) 장애종료

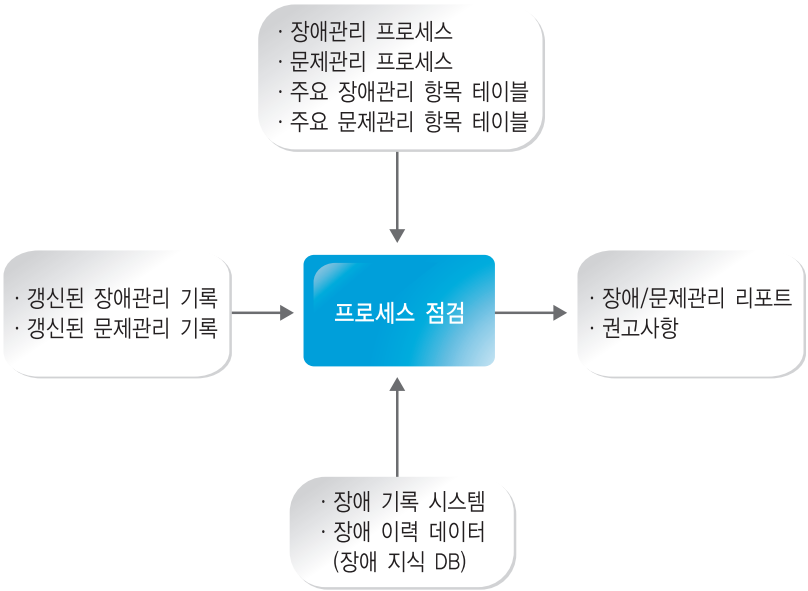
나. 세부 프로세스 주요 참여자 역할

- ▶ 사용자 : 장애종료에 의견 제시
- ▶ 서비스 데스크 요원 : 장애종료
- ▶ 장애관리 책임자 : 장애종료 점검

5 1.8 프로세스 점검

장애관리 책임자는 주기적으로 장애처리 데이터를 보고할 책임이 있다. 이 프로세스의 목적은 보고된 정보에 대해 검토하고, 이를 통한 장애관리 프로세스 전반에 걸친 향상을 도모하는 것이다. 장애관리 책임자 및 문제관리 책임자는 장애 및 문제의 이력 데이터가 일치 하는지에 대해 지속적으로 점검을 해야 한다. 만일 사실과 이력 데이터 간에 차이가 있다면 일치하도록 조정하여야 한다. 장애 프로세스 점검은 주기적으로 반드시 시행하여야 하며, 권고 주기는 월 1회이다.

또한, 장애 발생에 대비하여, 신속하고 정확한 대응을 위한 장애 모의훈련과 장애관리 업무에 대한 담당자의 마인드 교육과 기술 훈련을 위한 조직학습을 수시로 시행하여, 장애관리 프로세스를 견고하게 운영할 수 있도록 해야 한다. 장애관리 모의훈련과 조직학습은 본 지침의 7장을 참고한다.



(그림 5-9) 프로세스 점검

가. 주요관리 항목

- 장애관리 프로세스
- 문제관리 프로세스
- 주요 장애관리 항목
- 주요 문제관리 항목

나. 세부 프로세스 주요 참여자 역할

- 사용자 : 장애관리 프로세스에 대한 의견 제시
- 서비스 데스크 요원 : 장애 기록 점검
- 문제관리 책임자 : 문제 경향 분석 보고 및 프로세스 점검
- 장애관리 책임자 : 장애 경향 분석 보고 및 프로세스 점검

5 2 문제관리 세부 프로세스

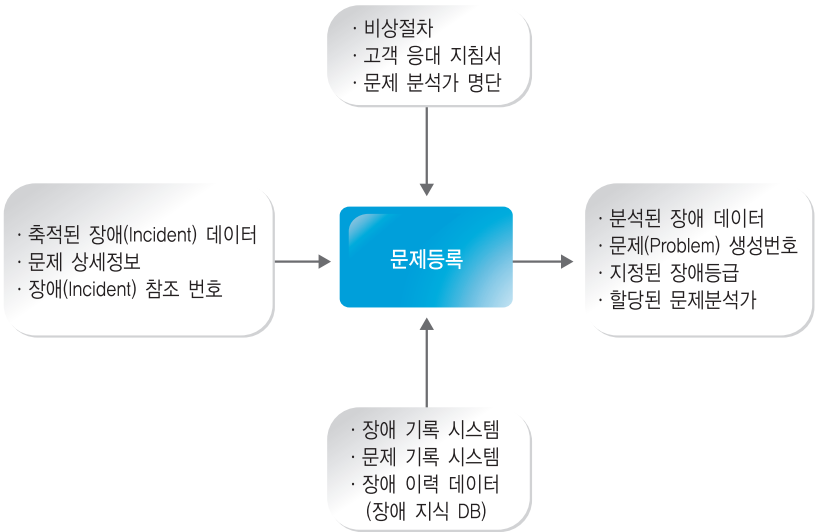
5 2.1 문제등록

장애관리 시스템 및 장애 데이터는 문제관리 프로세스를 위한 초기 정보원으로서 역할을 한다. 장애 정보는 장애 모니터링 시스템 및 타 정보시스템의 지원시스템을 통해 문제관리 책임자가 수집한다. 장애 데이터는 경향 분석을 위해 용이하게 사용되며 근본원인 분석을 위해 다양한 분석방법을 자체적으로 적용하도록 한다. 문제관리 책임자는 이러한 업무를 관장하는 역할을 수행한다.

문제관리 책임자는 문제에 대한 고유 번호 및 장애등급을 지정하고 이 단계 동안의 모든 문제에 대한 상세정보를 문제관리 시스템에 기록한다. 또한 문제관리 책임자는 문제가 해결되어 종료될 때까지 추이를 모니터링 하는데 대한 책임이 있으며 근본원인파악에 대한 책임은 장애가 할당된 해당 분야의 전문가인 문제 분석가에게 있다. 문제를 할당 받는 담당자에게는 문제참조 번호, 장애등급, 문제 상세정보 등과 같은 정보가 넘겨진다. 이러한 일들은 자동화 도구를 이용하거나 인적자원을 이용한 수작업에 의해 이루어진다.

가. 주요관리 항목

- 주간/월간 발생한 장애 수 대비 분석된 장애 수
- 한 주간 축적된 장애 데이터 수
- 생성된 문제 수
- 기록된 문제의 정보 중 오류 정보 기록 회수
- 전체 문제 수 대비 할당된 문제 수



(그림 5-10) 문제등록

나. 세부 프로세스 주요 참여자 역할

▶ 문제관리 책임자 : 문제등록 및 문제 분석가, 운영조직, 시스템/서비스 공급자 중 관련 조직에게 문제 배정

5 2.2 근본원인 도출

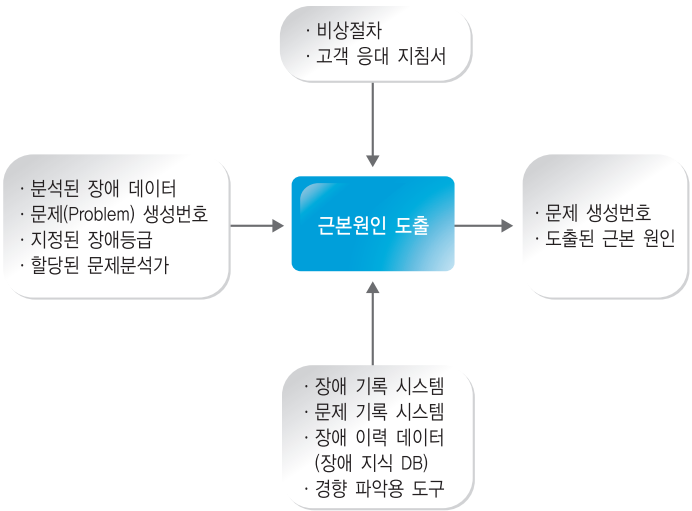
장애관리 프로세스가 신속한 장애해결에 주안점을 두는 반면 문제관리는 장애에 대한 근본원인을 도출하는데 초기 목적을 두고 있다. 심각한 장애 및 재발성 장애는 장애의 발생 빈도가 증가하면서 점진적으로 드러나게 된다. 경향 파악을 위한 도구 및 분석은 주간 단위나 월간 단위를 통해 이루어지며 표준화된 분석 기법을 보유하여 보다 체계적이고 효율적인 분석이 되도록 한다.

발생되는 장애에 대한 근본원인 분석이 기본적으로 이루어져야 하나 모든 경우에 다 해당되는 것은 아니다. 특히 업무나 조직에 심각한 영향을 끼치는 장애를 집중적으로 분석하고 관리하여야 한다. 일반적으로 등급이 가장 상위로 지정되는 장애는 근본원인을 분석하고 해결책을 도출하

여 향후에는 다시 재발하지 않도록 하는 것이 문제관리에서 해야 하는 주요한 역할이라 할 수 있다. 참고로 어떠한 장애를 분석할 것인가에 대한 최종 결정은 문제관리 책임자가 책임을 갖고 실행하도록 한다.

문제해결을 위해서는 조직으로부터 최대의 지원을 받아 해결을 위한 전문가를 할당한다. 기본적으로 근본원인 도출 단계 동안에 장애해결을 위해 할당된 지원 인력은 타 업무로부터 벗어나서 전적으로 장애해결을 위해 시간을 투입하는 것이 조직적으로 뒷받침되어야 한다. 표준화된 장애해결 기법을 위해서는 다음과 같은 단계가 필요하다.

- 예상 원인 파악
- 원인 파악을 위한 테스트 수행
- 원인 검증



(그림 5-11) 근본원인 도출

가. 주요관리 항목

- 높은 장애등급으로 할당된 문제의 수
- 전체 문제 수 대비 근본원인이 도출된 문제 수

▶ 한번 만에 근본원인이 도출된 문제 수

나. 세부 프로세스 주요 참여자 역할

▶ 운영조직 : 할당된 문제 근본원인 도출

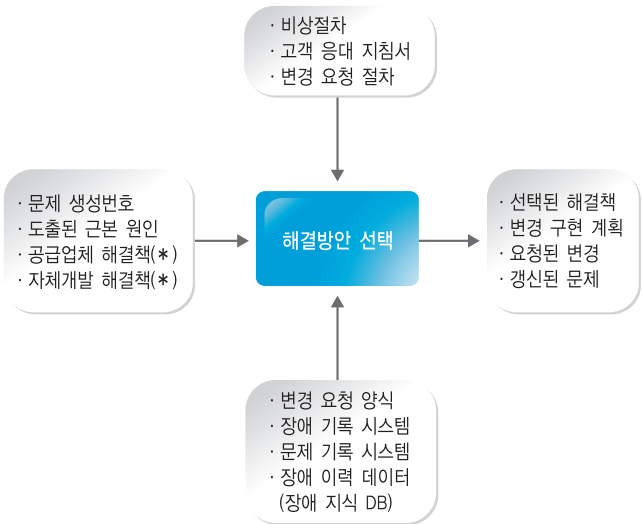
▶ 시스템/서비스 공급자 : 할당된 문제 근본원인 도출

▶ 문제 분석가 : 할당된 문제 근본원인 도출

▶ 문제관리 책임자 : 문제 근본원인 도출 상태 점검

5 2.3 해결방안선택

문제 분석가, 개발 조직, 시스템/서비스 공급자 및 운영조직에 의해 제공된 해결책 후보들 중에서 논의를 통해 해당 문제에 가장 적합한 해결책을 선정하여 문제 해결을 시도한다. 이때 변경절차가 필요할 경우에는 변경절차서를 작성하여 변경절차를 밟아야 한다.



(*) : 이전 단계의 세부 프로세스의 출력물과 연계되지 않고 이 단계에서 새롭게 입력된 정보

(그림 5-12) 해결방안 선택

가. 주요관리 항목

- 개발조직, 시스템/서비스 공급자가 제공한 해결책 수
- 자체 개발한 해결책 수

나. 세부 프로세스 주요 참여자 역할

- 운영조직 : 할당된 문제의 해결책 선택
- 시스템/서비스 공급자 : 할당된 문제의 해결책 선택
- 문제 분석가 : 할당된 문제의 해결책 선택
- 문제관리 책임자 : 선택된 해결책 점검

5 2.4 해결방안 모니터

문제 모니터링에 대한 책임은 문제관리 책임자에게 있다. 해결방안 모니터 프로세스에서는 사용자 문의에 대한 응답, 문제분석 및 해결 동안에 제기된 논쟁점을 다룬다. 장애등급에 따라 부여된 특정 시간을 초과하는 문제에 대해서는 문제관리 책임자가 해당 장애에 대한 현황을 파악하고 필요시 에스컬레이션 하도록 한다.

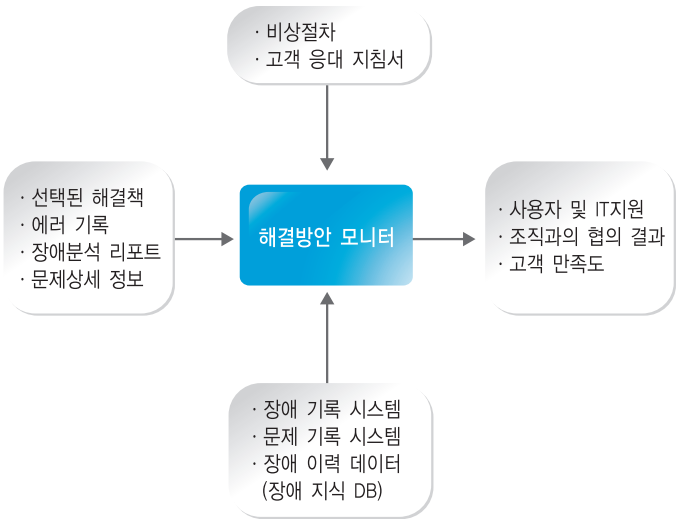
가. 주요관리 항목

- 지정된 시간에 따라 에스컬레이션된 문제의 수

나. 세부 프로세스 주요 참여자 역할

- 사용자 : 해결방안에 대한 의견 제시
- 운영조직 : 해결방안에 대한 의견 제시
- 시스템/서비스 공급자 : 해결방안에 대한 의견 제시
- 문제분석가 : 해결방안에 대한 의견 제시

▶ 문제관리 책임자 : 해결방안 모니터



(그림 5-13) 해결방안 모니터

5 2.5 해결방안 실행

향후에 발생되는 장애나 문제를 감소하기 위해 해결책을 마련하여 이를 구현하는 프로세스이다. 이 프로세스에서는 권고된 해결책을 구현하는데 주안점을 둔다.

가. 주요관리 항목

▶ 권고된 해결책 수 대비 구현된 해결책 수

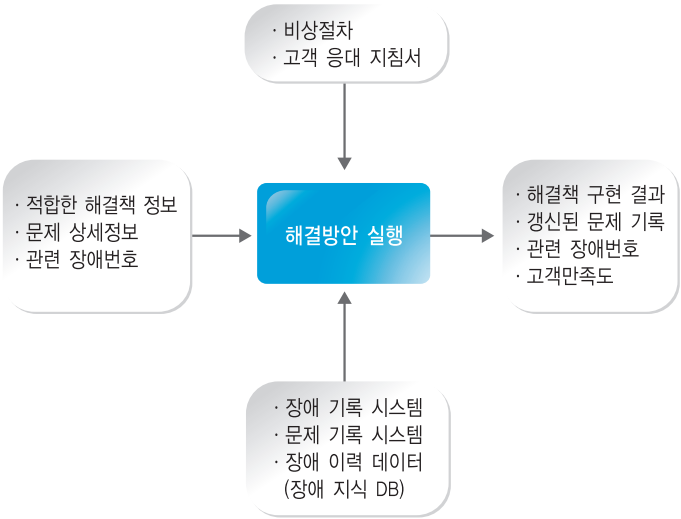
나. 세부 프로세스 주요 참여자 역할

▶ 사용자 : 해결방안에 대한 의견제시

▶ 운영조직 : 할당된 문제의 해결책 시도

▶ 시스템/서비스 공급자 : 할당된 문제의 해결책 시도

▶ 문제 분석가 : 할당된 문제의 해결책 시도



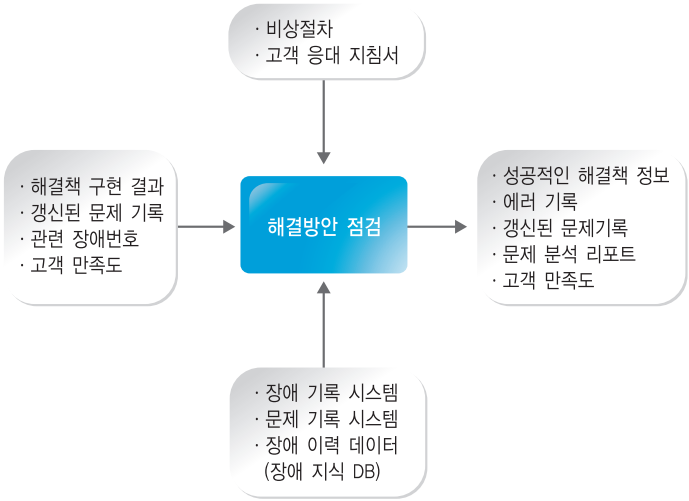
(그림 5-14) 해결방안 실행

5 2.6 해결방안 점검

구현된 문제 해결책이 목적대로 작동하는지 또는 제 2의 장애를 발생시키고 있지 않는지를 점검하는 프로세스이다. 해결방안에 대해 정보시스템 사용자가 만족하는지 여부를 먼저 문의하는 것이 좋다.

가. 주요관리 항목

▶ 구현된 해결책 수 대비 실패 수



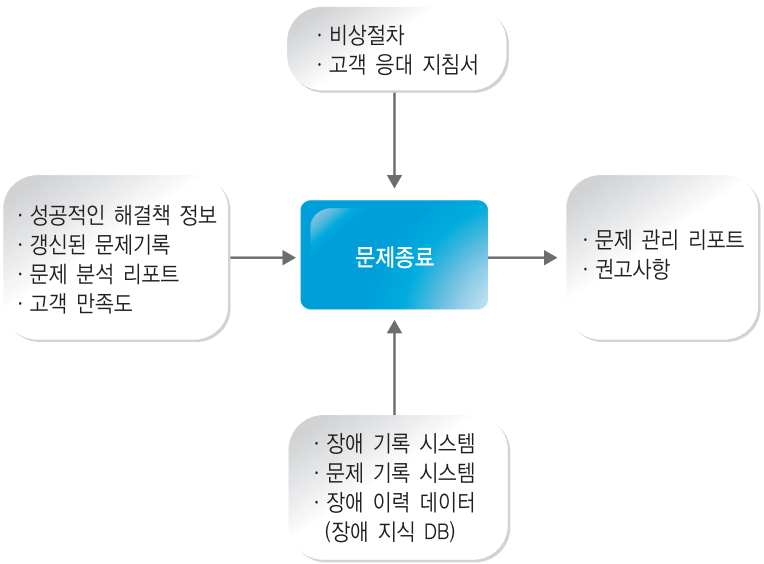
(그림 5-15) 해결방안 점검

나. 세부 프로세스 주요 참여자 역할

- ▶ 사용자 : 해결방안에 대한 의견제시
- ▶ 운영조직 : 시도된 해결방안 점검
- ▶ 시스템/서비스 공급자 : 시도된 해결방안 점검
- ▶ 문제 분석가 : 시도된 해결방안 점검

5 2.7 문제종료

문제가 해결되어 해결책을 성공적으로 찾은 경우, 문제관리 책임자는 해당 문제요청을 종료한다. 참고사항으로, 문제관리 책임자는 주기적으로 상부에 문제 데이터를 보고할 책임이 있다. 이 프로세스의 목적은 조직이 가지고 있는 잠재적 문제에 대해 공유하고, 전반적인 프로세스 향상을 위해 해결책을 권고하는 데 있다. 문제관리 책임자는 문제 이력 데이터가 일치하는지에 대해 관심을 가져야 한다. 만일 불일치가 있다면 이에 대한 수정이 요구된다.



(그림 5-16) 문제종료

가. 주요관리 항목

- 등록된 문제 수 대비 종료된 문제 수
- 보고된 문제 수

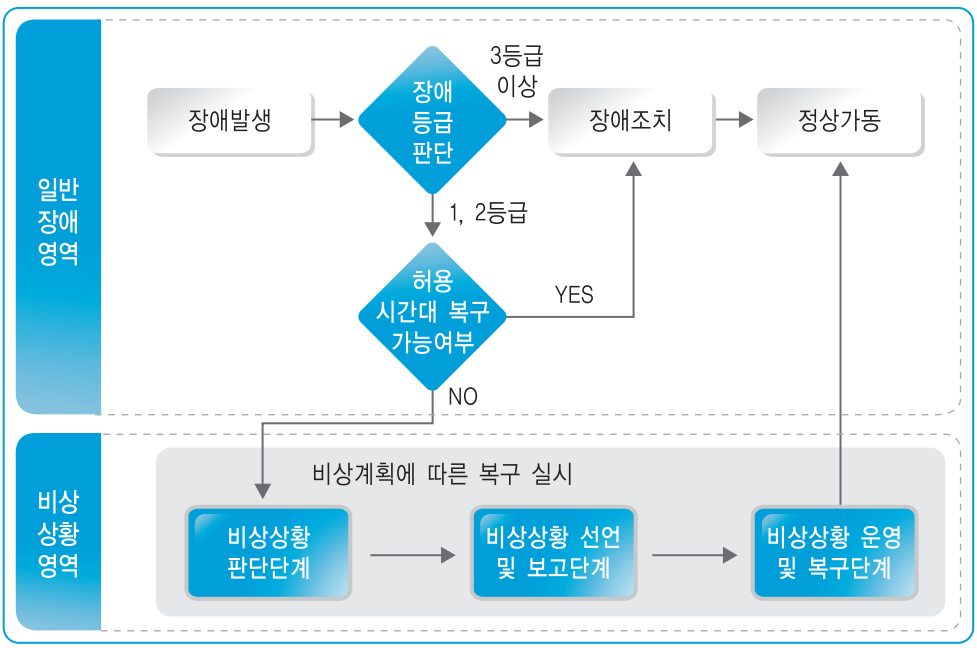
나. 세부 프로세스 주요 참여자 역할

- 사용자 : 문제종료에 대한 의견 제시
- 문제관리 책임자 : 문제종료 및 문제관리 리포트 작성

6 장애관리에서의 비상 계획

다양한 유형의 장애 중 일부는 단시간 내에 정상으로 복구되거나, 중요 업무가 아닌 사소한 업무에 발생하여 시급한 복구를 필요치 않는 경우가 있다. 그러나 일부 장애의 경우에는 대민 서비스 등 중요 업무를 대상으로 발생할 뿐만 아니라, 장시간의 장애로 인하여 금전적인 손해 및 기관의 대외적인 이미지에 치명적인 손상을 줄 수도 있다. 따라서 이런 경우의 장애에 대해서는 일반적인 장애관리 절차 이외에 추가적인 집중관리 및 대응 절차가 필요하다.

장애관리에 있어서의 비상상황이란 업무의 파급 영향 범위가 넓고, 신속한 복구가 필요한 시스템에 대한 장애가 허용 시간 내에 복구가 불가능하여 통제 불가능한 재해가 예상되는 상황을 의미하며, 이러한 비상상황을 효과적으로 해결하기 위해서는 비상상황 발생시 대처방안을 미리 수립하여야 한다.



(그림 6-1) 일반적인 장애와 비상상황의 연결

이러한 비상상황 대처방안에는 비상상황의 판단을 위한 의사결정 방법, 비상상황 선언 및 보고 방법, 비상 운영 및 복구 방법, 필요 조직체계 구성 등에 대한 지침이 포함되어야만 한다.

〈표 6-1〉 비상상황 발생시 대응단계

비상상황 발생시 대응단계	주요 내용
비상상황 대응을 위한 조직 구성	비상상황을 위한 조직 체계 구성과 비상시 구성되어야 할 위원회 인적 구성 및 역할에 대한 정의
비상상황에 대한 판단	장애 영향도와 긴급도를 고려한 장애 등급 판단과 복구 가능성 및 복구 예상시간 추정
비상상황 선언 및 보고	비상상황 선언, 경영진 보고 및 내외부 공지수행
비상상황 운영 및 복구	장애 상황 분석과 관련한 인원 소집, 장애 원인 분석, 예상 해결안 적용, 장애 상황 종료 확인, 비상상황 해제 및 보고/공지

6 1 비상상황 대응을 위한 조직 구성

정보시스템 비상상황과 관련한 조직은 크게 정보기술비상상황 관리위원회와 비상 조직으로 나눌 수 있으며, 비상 조직은 비상시에만 운영되는 조직인 반면 정보기술비상상황 관리위원회는 비상시뿐만 아니라 평상시에도 운영되는 조직으로 구성한다.

6 1.1 정보기술비상상황 관리위원회

정보기술비상상황 관리위원회의 역할은 평소 정보기술 부문 비상 계획의 수립과 유지정비를 수행하며, 적절한 장애복구 전략을 수립한다. 아울러 비상시에는 비상 계획에 의거 중요 의사결정 및 복구 활동을 지휘 · 조정하는 역할을 수행한다〈표 6-2〉. 위원회의 구성은 위원장, 부위원장, 사무국장, 운영위원으로 구성하며 역할은 〈표 6-3〉과 같다.

〈표 6-2〉 정보기술비상상황 관리위원회 역할

구 분	주요 역할
비상상황 발생 전	비상 계획을 수립하고 유지 정비하고 비상상황 발생시 필요한 조직 체계에 대한 계획안을 수립하며 복구절차에 대한 교육과 모의 훈련을 주관
비상상황 발생시	신속하고 정확한 비상상황 선언이 되도록 하고 상황실을 감독하고 대내 · 외 공지를 총괄함. 또한, 비상상황 선언 및 시스템 복구 등에 대한 주요 의사결정을 수행하고, 복구 작업 전반에 대해 지휘 · 감독함

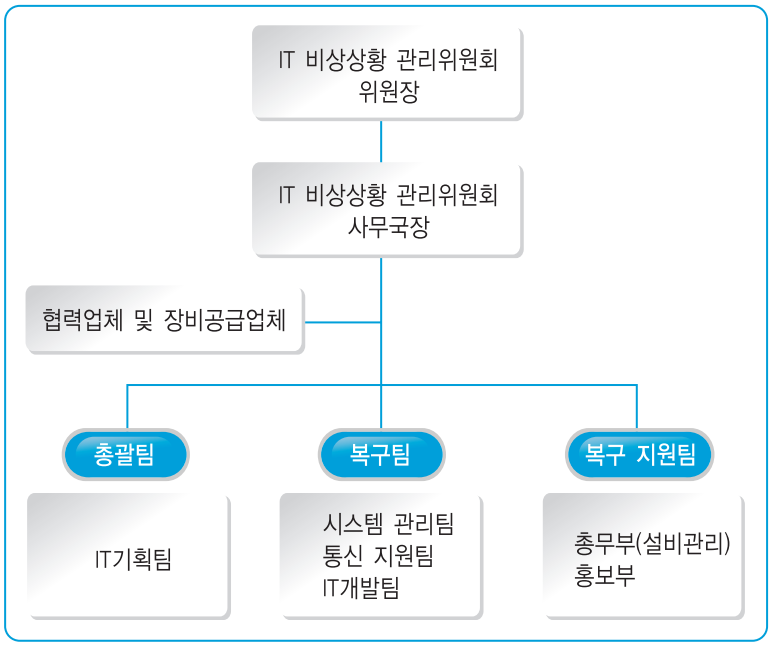
〈표 6-3〉 정보기술비상상황 관리위원회 담당별 역할

구 분	주요 역할	비 고[1)]
위원장	평상시 비상상황 대비 활동은 물론 초기 대응 단계에서 복구 활동까지 전 작업을 총괄, 비상 계획의 수립과 조직 구성원에 대한 교육 및 테스트 총괄, 실제 상황 발생시 정보기술비상상황 관리위원회 소집, 복구팀의 활동 조정 등의 책임이 있음	CIO
부위원장	위원장 및 다른 위원들과 협의하여 주요 의사결정을 수행하며, 위원장 부재 시 위원장의 역할을 대행함	기획실장
사무국장	비상 계획을 유지정비하고, 위원장을 보좌하여 비상상황 복구 활동 관련 교육과 테스트를 실시하며, 비상상황 발생시 복구반의 활동을 조정하는 책임이 있음	전산실장
운영위원	비상 계획 수립단계와 비상시 복구 단계에서 주요 의사결정(비상 계획의 범위와 내용, 비상 계획 관련 교육과 테스트, 업무복구 우선순위 및 목표 복구시간, 장애 등급 분류, 비상상황 선언 여부, 서비스 재개 결정)에 참여함	현업실장

*주) 1. 표시된 직급은 각 기관 조직 구성에 따라 달라질 수 있음

6 1.2 비상 조직

비상 조직을 구성할 때에는 가급적 평상시 조직과 큰 차이가 없도록 해야 한다. 비상 조직은 복구 수행을 위한 복구팀과 복구 지원팀 및 비상상황을 총괄하는 총괄팀으로 구분하며, 인원 구성은 평상시 각 담당자들의 업무 내용을 참고하여 비상상황 발생시 필요한 최소 인원으로 구성한다. 이때 총괄팀은 비상 관리자가 팀장의 역할을 수행한다.



(그림 6-2) 비상 조직도 예시

〈표 6-4〉 비상조직 팀별 역할 및 구성

팀 구분	시점 구분	책임 사항	평상시 관련조직
총괄팀	비상상황 발생시	– 비상상황실 운영 – 복구에 필요한 인원/자원 지원 – 장애 손실내용 평가 – 내외 공지 및 언론기관 초기 대응	정보기술 기획팀
	비상체제 운영시	– 비상운영 계획과 지원 – 복구 계획 수립과 복구 업무 총괄 – 비상 계획 보완대책 강구	
복구팀	비상상황 발생시	– 피해정도 파악 및 상황실에 피해 상황 보고 – 상황실 지시에 따라 협력업체 및 시스템 공급 업체와의 협의로 시스템 복구(시스템, 네트워크, 데이터베이스 등) 수행 – 복구진행상황 모니터링 및 상황실 보고 – 필요시 유실 데이터 추정 및 보고	정보기술 개발팀, 협력업체, 시스템/서비스 공급업체
	비상체제 운영시	– 장애 복구에 소요되는 시간 추정 및 보고	
복구 지원팀	비상상황 발생시/후	– 대표전화 안내(사용자 응대) – 외부 사용자 응대와 내부 직원에 대한 상황 공지 – 대외 공지 예 경영층 기자회견 준비(필요시) – 민원 처리 – 상황실의 대외 공지 안내에 따라 사용자 응대	총무부, 홍보부

6 2 비상 계획 프로세스

6 2.1 비상상황에 대한 판단

장애가 발생하면 일단 이에 대한 장애등급부터 파악해야 한다. 장애등급은 장애발생시 주요 업무에 미치는 영향도와 장애발생시 신속한 복구의 필요성에 대한 긴급도를 판단하여 결정한다. 이때 장애 1등급과 2등급에 해당하는 장애가 발생하면 복구 가능성 및 복구 예상 시간을 추정하여

비상상황의 선언 여부를 결정하도록 한다. 이러한 장애등급의 분류는 장애 상황 공유와 적절한 상황 대처를 위해 사용되도록 객관적으로 도출하여야 한다. 장애등급 분류와 관련해서는 3장을 참조한다.

6 2.2 비상상황 선언 및 보고

비상상황에 대한 판단은 업무의 파급 영향 범위가 넓고, 신속한 복구가 필요한 시스템에 대한 장애가 허용 시간 내에 복구가 불가능해서 통제 불가능한 재해가 예상되는 경우에 이루어진다. 다음은 비상상황 선언시 참고해야 할 내용들을 정리한 것이다.

〈표 6-5〉 비상상황 선언시 참고 요소

구 분	내 용
비상상황 선언시 참고자료	- 1차 담당자 보고자료 - 2차 경영진 보고자료 - 장애 등급(비상 계획서 내) 등
비상상황 선언권자	장애의 규모와 피해 정도에 따라 사전에 정의된 등급에 따라 결정함
비상상황 선언 목표시간	대형 장애시 최초 경영진 보고 후 권고시간 이내
비상상황 선언 방법	- 유무선 전화사용 - 대내외 메일 - 대내외 공지(기자회견 등)
비상상황 선언 내용	비상상황 선언시에는 장애 등급과 관련된 기본적인 내용만을 선언하도록 하되, 필요한 지시사항을 추가함
비상상황 선언 직후 정보기술비상상황 관리위원회 또는 상황실에서 해야 할 일	정보기술비상상황 관리위원회 소집과 주요 의사결정 수행

비상상황 발생시 보고 체계는 보고에 필요한 모든 단계나 상황에 대해서 기술되어야 하며, 각 상황(또는 단계)별로 보고자와 보고의 접수자가 명시되어 있어서 해당 상황에서 누가 어떠한 내용

의 보고를 누구에게 해야 하는지를 알 수 있어야 한다. 또한 보고 및 전파체계와 관련한 비상연락망을 작성하여 관리해야 하며, 이는 부록의 비상연락망을 참조하도록 한다. 〈표 6-6〉은 초기 장애 상황 발생시 보고자와 보고 접수자의 역할에 대하여 정의한 것이다.

〈표 6-6〉 초기 장애 상황 발생시 보고자와 보고 접수자의 역할

구 분	역 할
보고자	초기 감지에 대한 최초 보고 실행(자신이 감지한 사실에 대해서만 간략하고 신속하게 보고를 해야 함)하며 비상 계획 실시 여부 및 장애 분류를 위해서 장애 진행 상황을 살펴 추가 보고
접수자	상황의 정황에 따라 해당 업무 · 관련시스템 · 외부업체 담당자에게 비상 연락을 취하고 큰 피해가 예상되는 경우 정보기술 비상상황 관리위원회를 비상소집하며 상황실 준비(상황실의 물리적인 위치 선정, 상황판 · 전화 · 안내 방송시설 등 점검 및 준비) 및 경영진 보고 준비

〈표 6-7〉은 1차 보고 및 경영진에 대한 2차 보고시 구체적으로 보고해야 할 내용을 정리한 것이다. 부록Ⅳ의 '장애관리 양식' 을 참조한다.

〈표 6-7〉 비상상황 발생시 1,2차 보고 내용

구 분	보고 내용
1차 보고	장애발생 내용, 장애발생 시간과 위치, 피해 영향과 범위, 임시 조치내역, 추가 예상 위험, 보고자 이름과 직급, 보고자 연락처 등
2차 보고	1차 담당자 보고 항목과 예상 장애 등급, 지시사항, 요청사항, 외부 영향(타 기관 영향, 언론 노출 등), 상황 변화로 인한 추가 보고, 보고 내용의 수정 보고 등

이외에도 비상상황이 발생하면 이에 대한 대내외적인 공지가 필요하며, 이때 공지할 내용은 〈표 6-8〉과 같다.

〈표 6-8〉 비상상황 발생시 대내 · 외 공지 내용과 방법

구 분	공지 내용
대내 공지	– 공지 내용 : 간략한 피해 상황, 서비스 불가 내역, 복구 예상 시간, 비상상황실 연락처, 지시 및 협조사항(사용자 응대 요령 포함) 등 – 공지 방법 : 조직내 방송, 게시판, 이메일, 유무선 전화 등
대외 공지	– 공지 대상 : 정보시스템 사용자, 관련 기관 등 – 공지 내용 : 비상상황 선언 내용, 간략한 피해 상황, 서비스 불가 내역, 복구 예상 시간, 협조 요청 사항 등 – 공지 방법 : 대표전화 안내, 콜 센터 안내, 홈페이지 안내, 기자회견, 관련 기관 공지 등

6 2.3 비상상황 운영 및 복구

비상상황이 발생하게 되면 이에 따른 관련 조직(정보기술기획팀, 시스템 운영팀, 정보기술개발팀, 협력업체, 시스템/서비스 공급자 등)의 긴급 소집이 이루어지며, 이때부터 장애원인에 대한 세밀한 분석 및 해결 작업이 시작된다. 〈표 6-9〉는 이러한 장애원인 분석 및 해결과 관련한 문제 해결 프로세스의 예시이다.

〈표 6-9〉 비상상황 문제 해결 프로세스

단 계	주요 활동 내용
1. 문제의 정의	– 해결해야 할 문제 혹은 의사결정이 이루어져야 하는 이슈를 명확히 정의함 – 상기 문제는 일반적인 표현이 아니라 아주 구체적인 형태로 제시되어야 함
2. 문제의 분해	– 문제를 아래와 같이 몇 개의 요소로 분해 • 문제를 몇 가지의 집합으로 분리 • 문제 집합간의 우선순위 설정 • 개별 집합에 대한 책임자 선정 – 문제 해결의 완벽성을 유지하기 위해서는 문제의 분해를 MECE[1] 원칙에 입각해서 수행 – 이러한 문제의 분해를 위해서 Logic Tree와 같은 기법을 적용함
3. 중요하지 않은 내용의 제거	– 2단계에서 분해된 내용 중 중요하지 않은 문제 집합에 대해서는 검토 대상에서 제외함 – 80/20의 법칙에 입각하여 사고함
4. 작업계획 수립	– 각각의 문제 집합에 대해서 문제 발생의 원인에 대한 가설을 수립함 – 그리고 이렇게 예측된 원인을 해결하기 위한 방법 및 이에 대한 검증을 위한 방법까지 준비함 – 작업 수행의 담당자에 대해서 선정함
5. 분석 수행	– 상기 수립된 각 가설별로 실제 해결 작업을 수행하고 이것이 문제의 원인을 해결하는지 검증함 – 만일 상기 방법으로 문제 원인의 제거가 되지 않으며 추가적인 정보 등을 이용하여 새로운 가설을 수립하고 분석 작업을 반복함
6. 결과 종합	– 상기 작업을 통해 장애원인을 제거하고, 비상 상황을 해제하게 됨 – 이 후 대내외 공지 및 경영진 보고 등의 추가적인 조치를 취함

* 주) 1. MECE(Mutually Exclusive Collectively Exhaustive) : 특정 사안에 대한 내용을 분류/정리할 때 상호 배타적이면서 모든 내용이 다 포함될 수 있도록 분류해야 한다는 것을 정의한 컨설팅 기법중 하나임.

7 모의훈련 및 조직학습

7 1 모의훈련

모의훈련은 시스템 운영의 지속성과 효과적인 장애관리 프로세스의 중요한 부분이며 장애조치 계획, 업무복구 계획 및 절차가 실제 상황에서 유용하다는 것을 보장하는 방법이다. 또한 비계획적으로 발생하는 시스템 장애에 대비하여 주기적인 반복 훈련을 통해 응급조치 요령을 습득하고 신속히 장애원인을 파악하여 복구함으로써 장애시간을 최소화하기 위한 것이다.

정보시스템 운영 관리자는 주요 업무 및 시스템에 대한 문서화된 모의훈련 절차를 수립해야 하며, 운영자들이 숙지할 수 있도록 지속적이고 반복적인 훈련을 수행해야 한다. 또한, 모든 훈련 성과에 대한 내용은 문서로 작성되어 관리되어야 한다.

모의훈련 프로세스는 다음과 같은 항목을 포함해야 한다.

1) 훈련 목적

훈련을 실시하는 이유와 훈련을 통해 얻을 수 있는 성과를 포함한다.

2) 훈련 주기

시스템 운영환경에 적합한 훈련 주기를 설정한다. 초기에 훈련에 포함되는 대상자들과 사전에 협의하여 결정하며 적어도 연간 2회 이상은 실시하는 것이 좋다.

3) 훈련 책임자

훈련을 지휘하여 훈련 목적에 부합하는 성과를 이끌어 내기 위한 책임자를 말하며 해당 팀장 또는 정보시스템 관리자가 선임된다.

4) 훈련 대상

정보시스템 운영 요원 및 관리자가 참여하며 시스템 담당자, 네트워크 담당자, 데이터베이스 담당자, 설비 담당자, 서비스 데스크 요원, 장애관리 책임자, 문제관리 책임자, 문제 분석가 등이 포함된다. 또한 필요에 따라 협력업체, 시스템 공급자가 참여할 수 있다.

5) 훈련 내용

훈련의 방법과 절차, 점검 사항을 포함한다. 훈련 내용에는 다음과 같은 내용을 포함해야 한다.

- 장애발생 예상 요인을 선택하여 모의로 시스템 장애를 유발시킴
- 팀별, 개인별 역할, 의사소통, 임무 숙지 등을 점검함
- 응급조치 방법, 장애원인 분석, 업무복구 절차 등을 점검함
- 비상연락망, 상황전파, 보고절차 등을 점검함

6) 훈련 절차

훈련의 절차는 순차적으로 수행되며 다음과 같은 단계가 있다.

- 환경구성 및 장애발생
- 장애전파
- 장애요인 분석
- 장애조치 및 비상 계획
- 장애처리 결과보고
- 훈련 결과보고

7 1.1 세부 훈련 절차

가. 환경구성 및 장애발생 단계

훈련을 수행하기 위해 미리 시스템 환경을 구성해 놓아야 한다. 별도의 테스트 환경을 구성할 수 있는 경우에는 테스트 환경에서 장애처리 훈련을 수행할 수 있도록 구성한다. 예를 들면, 테스트 환경을 모니터링 도구에 사전 등록하여 진행할 수도 있다. 별도의 테스트 환경을 구성할 수 없는 경우에는 온라인 서비스 시간을 피하여 실제 운영 환경에서 장애처리 훈련을 진행한다. 미리 결정한 장애, 즉 특정 시스템 파일을 삭제하거나 데이터베이스 프로세스를 다운시키는 등의 장애를 고의로 발생시킨다. 그리고 장애요인에 대해서는 특정한 사람들만 사전에 알 수 있도록 하며 장애원인 파악 및 장애 복구에 참여하는 다른 사람들은 알 수 없도록 해야 한다. 세부 훈련 절차서

의 예는 부록 I 의 '장애조치 훈련 지침' 을 참조한다.

이 단계에서는 다음과 같은 사항을 점검한다.

- ▶ 장애발생 시스템 및 서비스는 적절한가?
- ▶ 장애훈련을 수행하기 위한 시스템 환경은 적절히 구성되었는가?
- ▶ 장애훈련으로 인하여 실 운영 서비스에 영향을 주지는 않았는가?

나. 장애 전파 단계

장애를 최초로 발견한 운영원 또는 장애를 접수한 서비스 데스크 요원은 비상연락망을 참고하여 관련 담당자에게 신속히 연락을 취한다. 관련 담당자는 장애상황을 점검하고 장애서비스 내용, 영향범위 등을 파악하여 보고절차에 따라 상부에 보고하고, 응급조치 및 장애조치를 수행한다. 장애처리 담당자는 상황에 따라 관련 조직 및 시스템 공급자에게 지원을 요청할 수 있다.

이 단계에서는 다음과 같은 사항을 점검한다.

- ▶ 모니터링 도구를 통해 장애를 사전에 감지하였는가?
- ▶ 목표 시간 내에 담당자에게 연락되었는가?
- ▶ 상부보고 및 연락이 필요한 모든 담당자에게 연락되었는가?

다. 장애요인 분석 단계

장애복구절차에 규정된 점검절차에 따라 장애요인을 분석한다. 이때, 관련 부서의 담당자들이 모두 참여하여 협의하거나, 장애 지식 데이터베이스를 검색하여 장애요인을 분석할 수도 있다. 필요시 시스템 공급자에게 지원을 요청하여 장애요인을 분석한다.

이 단계에서는 다음과 같은 사항을 점검한다.

- ▶ 장애조치 절차서에 규정된 점검 절차에 따라 점검이 이루어졌는가?
- ▶ 장애조치 절차서에 규정된 점검 절차가 적절한가?
- ▶ 장애요인이 예상하지 못한 발생 현상에 해당하는가?
- ▶ 장애요인 분석을 위해 필요시 장애 지식 데이터베이스를 적절히 활용하였는가?

라. 장애조치 및 비상계획 단계

장애요인이 쉽게 파악되지 않는 경우 또는 장애요인이 복합적으로 연관되어 있는 경우에는 장애관리 책임자는 비상관리자를 선임하여 장애해결을 시도한다. 장애요인을 발견하거나 조치 방안이 수립되면 적절한 장애조치 방법을 선택한 후 해당 팀장 또는 비상관리자에 보고하고 장애를 조치한다. 필요시 장애 지식 데이터베이스를 참고하거나 시스템 공급자의 지원 하에 장애를 조치한다.

이 단계에서는 다음과 같은 사항을 점검한다.

- 예비품이 적절히 확보되었는가?
- 비상 계획 관리가 적절한 시간 내에 수행되었는가?
- 비상 계획의 대응 방법 또는 관련 부서와의 의사소통은 적절하였는가?
- 장애요인별 장애조치 절차서에 정의된 장애조치 목표시간 내에 조치가 정상적으로 이루어졌는가?
- 장애조치 절차서에 정의된 장애조치 목표시간은 적절한가?
- 시스템 공급자에 대한 연락은 적시에 되었는가?
- 시스템 공급자로부터 적절한 지원을 적시에 받았는가?
- 장애조치를 위해 필요시 장애 지식 데이터베이스를 적절히 활용하였는가?

마. 장애처리 결과보고 단계

장애조치가 완료된 후, 장애 유발 원인과 관련된 부서의 담당자는 장애원인 및 조치경과에 대해 정리하여 장애보고서를 작성하고, 보고 절차에 따라 해당 팀장 및 상부에 보고한다. 장애관리 지침에 명시된 주요 장애인 경우 장애예방 및 재발방지를 위한 향후대책을 수립하여 장애보고서에 명시한다. 필요시 추가적으로 별도의 장애분석 보고서를 작성하여 보고할 수도 있다.

이 단계에서는 다음과 같은 사항을 점검한다.

- 장애보고서가 규정된 시간 내에 작성되었는가?
- 장애보고서의 내용은 적절히 이해할 수 있도록 작성되었는가?

▶ 장애복구 우선순위가 적절히 판단되었는가?

▶ 장애조치 내용 및 향후 대책은 정확히 명시되었는가?

바. 훈련 결과 보고 단계

장애훈련이 종료된 후, 장애훈련 결과보고서를 작성하여 훈련 책임자의 승인을 받는다. 장애를 발견, 접수, 전파, 조치, 보고 과정의 적시성, 신속성, 적정성을 기준으로 훈련결과를 평가한다.

훈련의 결과에 따라 장애요인 점검 절차 또는 장애조치 절차에 대한 변경이 필요하다고 판단된 경우에는 해당 내용을 변경하여 현행화하고, 실제 장애발생시 활용할 수 있도록 한다. 훈련 진행시 발견된 문제점에 대하여 관련 직원에게 공지하거나 교육을 실시한다. 이 단계에서는 이전 각 단계의 점검 내용이 정확히 수행되었는지 점검한다.

7 1.2 장애조치 절차

장애조치 절차는 운영중인 주요 시스템에 대해 발생할 수 있는 여러 장애유형에 대한 원인파악, 조치, 훈련을 위한 절차 및 내용을 기술한 것이다. 장애조치 절차서를 활용하여 장애발생시 주요 시스템에 대해 사전에 정의된 절차에 따른 신속한 장애원인 파악 및 시스템 운영을 담당하는 여러 부서 간에 원활한 의사소통을 할 수 있다. 또한 장애에 대비한 훈련을 수행함으로써 장애 해결시간을 단축할 수 있다.

장애조치 절차는 주요 시스템 운영을 담당하는 여러 관련 부서간의 협조에 의해 작성되어야 하며, 시스템 변경에 따라 현행화될 수 있도록 관리되어야 한다. 장애조치 절차서의 예는 부록 Ⅰ의 '장애조치 훈련 지침'을 참조한다.

가. 시스템 개요

주요 시스템의 개요, 서비스 내용, 업무범위 등에 대한 설명을 기술한다.

나. 시스템 구성도

주요 시스템의 모든 하드웨어 구성요소 및 네트워크 연결 체계가 포함된 구성도를 명시한다. 구성도는 전체 구성을 볼 수 있는 개념도와 세부 시스템 구성을 볼 수 있는 세부 구성도로 구분된다. 시스템 구성도는 소프트웨어 구성도와 더불어 시스템을 쉽게 이해할 수 있도록 명시되어야 한다.

다. 시스템 구성요소

주요 시스템을 구성하는 세부 구성요소를 명시하고 각 구성요소별 명칭과 용도, 서비스 업무 등을 기술한다. 그리고 시스템이 복수일 경우 각각에 대해 모두 기술한다. 다음과 같은 항목이 포함된다.

▶ 서버의 구성요소

서버의 명칭, 용도, 모델, 운영체제, CPU 개수 및 용량, 메모리 형식 및 용량, 디스크 형식 및 용량, IP 주소, 설치된 주요 소프트웨어 등을 기술한다.

▶ 네트워크 구성요소

네트워크를 구성하는 라우터, 스위치, 허브, 회선에 대해 각각의 명칭, 용도, 모델, 용량, 운영체제 등을 기술한다.

▶ 방화벽 구성요소

방화벽을 구성하는 시스템 사양, 소프트웨어, 처리 방식 등을 기술한다.

라. 소프트웨어 구성도

주요 시스템의 모든 소프트웨어 구성요소 및 업무처리 절차가 포함된 구성도를 명시한다. 구성도는 전체 구성을 볼 수 있는 개념도와 세부 업무 절차가 포함된 세부 구성도로 구분된다. 소프트웨어 구성도는 시스템 구성도와 더불어 시스템을 쉽게 이해할 수 있도록 명시되어야 한다.

마. 구성 요소별 세부 내용

주요 시스템에서 발생할 수 있는 각 단위 시스템의 주요 장애현상 및 원인, 대응 절차에 대한 내용을 포함한다. 관련조직 및 시스템 공급자의 지원을 받아 모든 가능한 시나리오를 상세히 기술해야 하며, 시스템 운영자가 쉽게 참조할 수 있어야 한다. 다음과 같은 항목이 포함된다. 구체적인 사항은 부록 Ⅱ의 '정보시스템 자원별 장애처리 절차'와 부록 Ⅲ의 '장애관리 시나리오'를 참조한다.

- ▶ 서버의 기능
- ▶ 서버의 프로세스 구성 및 기능
- ▶ 주요 장애현상 및 원인
- ▶ 주요 장애의 대응 및 복구 절차

7 1.3 비상연락 체계 및 의사소통 절차

훈련 계획서에는 시스템에 대한 고유한 담당자 및 시스템 공급자의 비상연락 체계를 명시해야 한다. 비상연락 체계에는 시스템별, 소프트웨어별, 응용 시스템별 담당자와 연락처가 포함되어야 하며 각 담당자의 성명, 소속, 직급, 연락처, 상주 여부 등을 명시한다.

또한, 서비스 데스크, 시스템 담당자, 장애관리 책임자, 시스템 공급자 등 장애관리지침에 명시된 각 담당자간의 의사소통 프로세스 및 통지 방법이 명시되어야 한다. 의사소통 프로세스에는 가능한 이벤트(시나리오), 통지책임자, 장애복구 우선순위, 의사소통 순서, 다음단계, 시간 등에 대한 항목이 포함된다. 구체적인 사항은 부록 Ⅰ의 '장애조치 훈련 지침'을 참조한다.

7 2 조직 학습

조직 학습은 정보시스템 운영과 관련하여 시스템 운영자, 시스템 관리자, 서비스 사용자 등의 구성원들이 장애조치 및 예방활동으로부터 얻어지는 유무형의 성과물을 통해 지속적인 협의와 학습을 하여 장애 대응 능력을 향상하기 위한 활동이다. 장애관리 책임자는 장애이력관리, 장애분석, 정기적인 협의 및 교육을 통해 구성원들의 장애 대응 능력을 향상하기 위한 업무를 수행해야 한다.

7 2.1 조직 학습 활동

가. 장애 이력 관리

주요 시스템의 장애발생 이력은 장애관리시스템에 저장되어 관리되어야 한다. 장애 이력자료는 객관적이고 신뢰성 있는 근본자료(Raw Data)로서 다양한 방법의 취약점 분석을 통해 동일 장애의 재발을 방지하는 예방활동 및 대응능력 향상을 위해 활용될 수 있다. 장애관리 책임자는 장애 이력자료의 유출을 방지하기 위한 적절한 보안 절차를 적용해야 한다. 장애 이력자료에는 다음과 같은 항목이 포함된다.

- 발생일자
- 정보시스템 사용 조직 또는 업무명
- 장애내용
- 장애번호
- 발생 및 해결 시간(분)
- 장애복구 우선순위
- 장애처리 조직
- 장애유형 분류

나. 장애 분석

장애관리 책임자는 장애 이력자료를 활용하여 주요 시스템의 취약점을 분석하고, 안정적인 서비스 제공을 위해 지속적인 개선활동을 수행해야 한다. 장애 분석은 월, 분기, 반기, 연간 주기로 필요에 따라 수행할 수 있다. 장애 분석에는 다음과 같은 항목이 포함된다.

- 장애발생 건수 분석
- 장애 평균 조치 시간 분석
- 정보시스템 사용 조직 또는 업무별 영향 분석
- 장애처리 조직별 영향 분석
- 장애 유형별 영향 분석
- 취약점(Weak Point) 분석
- 중점 개선사항

다. 장애관리 교육

장애관리 책임자는 지속적으로 장애처리 조직 구성원들의 장애관리 프로세스 준수 및 대응 능력 향상을 위해 장애관리 교육을 수행해야 한다. 교육 자료에는 다음과 같은 항목이 포함된다.

- 장애관리 개념
- 장애관리 지침
- 장애관리 프로세스 설명
- 장애관리 조직의 역할과 책임
- 장애복구 우선순위 기준
- 장애관리시스템 사용자 화면(GUI) 및 사용법

7 2.2 정기 장애 회의

가. 주간 장애 검토 회의

장애관리 책임자는 주요 서비스의 장애발생 및 조치 활동에 대해 매주 검토 회의를 진행하여 장애처리 조직 구성원들의 대응 능력 향상과 안정적인 시스템 운영을 보장하기 위한 활동을 수행하여야 한다. 주간 장애 검토 회의는 매주 발생한 주요 장애에 대해 발생원인, 조치내용, 예방대책 등에 대해 점검하고 장애관리 프로세스 상의 개선점을 협의한다. 주간 장애 검토 회의에는 다음과 같은 항목이 포함된다.

▶ 회의 주관
- 장애관리 책임자

▶ 검토 대상
- 주간 단위 주요 장애

▶ 회의 참석자
- 전산실장 또는 팀장
- 각 운영시스템 관리자
- 서비스 사용자 대표(필요시)
- 시스템 공급업체의 담당자(필요시)

▶ 회의 안건
- 주요 장애의 발생 현황 점검
- 장애조치 프로세스의 개선점 협의
- 복합장애, 반복장애, 원인 불명 장애의 점검
- 장애조치에 대한 서비스 사용자 불만사항 점검

▶ 회의 성과물
- 주간 장애 검토 회의 자료
- 주간 장애 검토 회의록

나. 월간 서비스 개선 회의

장애관리 책임자는 주요 서비스의 향상을 위해 월간 서비스 개선 회의를 진행한다. 월간 서비스 개선 회의는 시스템 장애뿐만 아니라 시스템 운영과 관련된 모니터링, 백업, 운영현황 등에 대해 점검한다. 검토 대상 및 안건은 관련 담당자들의 협의를 통해 조정할 수 있다. 월간 서비스 개선 회의는 다음과 같은 항목이 포함된다.

▶ 회의 주관

- 전산실장 또는 팀장

▶ 검토 대상

- 월간 단위 주요 장애 및 시스템 운영 현황

▶ 회의 참석자

- 시스템 운영조직 임원(필요시)
- 서비스 사용자 임원(필요시)
- 전산실장 또는 팀장
- 각 운영시스템 관리자
- 서비스 사용자 대표
- 시스템 공급업체의 담당자

▶ 회의 안건

- 주요 시스템 운영 현황 점검
- 주요 장애의 발생 현황 점검
- 서비스 사용 조직의 불만사항 점검

▶ 회의 성과물

- 월간 서비스 개선 회의 자료
- 월간 서비스 개선 회의록

부 록 I 장애조치 훈련 지침

1 개요

장애조치 훈련 지침은 정보시스템을 운영하는 조직에서 주기적인 장애조치 모의 훈련을 실시하기 위한 문서화된 절차 작성을 돕기 위해 만들어진 자료이다. 정보시스템 담당자는 장애조치 훈련 지침을 문서화하여 주기적으로 훈련함으로써 실제 운영 환경에서 발생하는 정보시스템 장애에 대해 적절히 대응할 수 있는 능력을 향상해야 한다.

장애조치 훈련 지침은 실제 운영 환경에 적용하면서 개선사항이 있으면 수시로 보완되어 관련자에게 배포되고 숙지되도록 하여야 한다. 장애조치 훈련 지침은 부록 Ⅱ의 '정보시스템 자원별 장애처리 절차'와 부록 Ⅲ의 '장애관리 시나리오'와 함께 활용되어질 때 효율적인 자료가 될 수 있다.

1 1 훈련 목적

시스템 장애발생에 대비하여 장애조치 훈련을 정기적으로 실시하여, 장애발생시 신속히 원인을 파악하고 조치함으로써 장애조치 시간을 단축하기 위한 것이다.

1 2 훈련 주기

예시 분기별 1회

1 3 훈련 책임자

예시 전산실장

1 4 훈련 대상

예시 서비스 데스크, 서버관리팀, 데이터베이스관리팀, 네트워크관리팀, 장애관리 책임자, 문제관리 책임자, 외부 시스템 공급자

1 5 훈련 내용

- ▶ 장애발생 예상 요인을 선택하여 모의로 장애를 발생시킴
- ▶ 팀별/개인별 의사소통, 임무 숙지 및 조치방법 점검
- ▶ 비상연락체계, 상황전파, 장애원인파악, 조치절차, 장애결과보고 등 훈련

1 6 훈련 절차

환경구성 및 장애발생 → 장애 및 상황전파 → 장애요인 분석 → 장애조치 및 비상 계획 → 장애처리 결과보고 → 훈련 결과보고

가. 환경 구성 및 장애발생

- ▶ 장애를 훈련하기 위해 미리 환경을 구성해 놓아야 한다. 별도의 테스트 환경을 구성할 수 있는 경우에는 테스트 환경에서 장애를 훈련할 수 있도록 구성한다. (예를 들면, 테스트 환경을 모니터링 도구에 등록함) 별도의 테스트 환경을 구성할 수 없는 경우에는 온라인 서비스 시간을 피하여 실 운영 환경에서 장애를 훈련한다.
- ▶ 미리 결정한 장애요인을 바탕으로 고의로 장애를 발생시킨다. (예를 들면, 특정 시스템 파일을 삭제하거나, 데이터베이스 프로세스를 다운시킴)

▶ 장애요인에 대해서는 특정한 사람들만 사전에 알 수 있도록 하며, 장애원인 파악 및 장애조치에 참여하는 다른 사람들은 알 수 없도록 해야 한다.

나. 장애 및 상황전파

▶ 장애를 최초 발견한 운영원 또는 장애를 접수한 서비스 데스크 요원은 비상연락망을 참고하여 관련 담당자에게 신속히 연락을 취한다.

▶ 운영원 또는 관련 담당자는 장애상황에 따라 시스템 공급자에게 지원을 요청한다.

다. 장애요인 분석

▶ 1차로 장애조치절차에 규정된 점검절차에 따라 장애요인을 분석한다. 이때, 관련 부서의 담당자들이 모두 참여하게 된다.

▶ 필요시 장애 지식 데이터베이스를 검색하여 장애요인을 분석한다. 또는 시스템 공급자에게 지원을 요청하여 장애요인을 분석한다.

라. 장애조치 및 비상 계획

▶ 장애요인이 쉽게 파악되지 않는 경우 또는 장애가 쉽게 조치되지 않는 경우에는 장애관리 책임자는 비상 계획 관리자를 선임하여 장애해결을 시도한다.

▶ 장애요인을 발견하면 적절한 장애조치방법을 선택한 후, 해당 팀장 또는 비상 계획 관리자에 보고하고 장애를 조치한다.

▶ 1차로 장애요인별 장애조치절차에 규정된 내용에 따라 장애를 조치한다.

▶ 필요시 장애 지식 데이터베이스를 참고하여 장애를 조치한다. 또는 시스템 공급자의 지원하에 장애를 조치한다.

마. 장애처리 결과보고

▶ 장애조치가 완료된 후, 장애의 (잠재적) 원인이 된 부서의 담당자는 장애원인 및 재발 방지 대책 등을 분석하여 장애보고서를 작성하고, 해당 팀장에게 보고한다.

바. 훈련 결과보고

▶ 장애훈련이 종료된 후, 장애훈련결과보고서를 작성하여 훈련 책임자의 승인을 받는다.

▶ 장애발견, 장애전파, 장애조치, 장애보고 등의 적시성, 신속성, 적정성을 기준으로 훈련결과를 평가한다.

▶ 훈련의 결과, 장애요인 점검절차 또는 장애조치절차에 변경이 필요하다고 판단된 경우에는 해당 내용을 변경하여 현행화하고, 실제 장애발생시 활용할 수 있도록 한다.

▶ 훈련의 결과, 발견된 문제점에 대하여 관련 직원에게 공지하고, 교육한다.

1 7 훈련 결과

훈련 결과 보고서에는 훈련 시나리오 별로 아래와 같은 양식이 포함된다.

훈련 단계	주요 점검 항목	훈련 결과	개선점
1. 환경구성 및 장애발생	– 장애훈련을 위한 환경이 적절히 구성되었는가? – 장애훈련으로 인하여 실 운영 환경 서비스에 영향을 주지 않았는가?		
2. 장애 및 상황전파	– 모니터링 도구를 통해 장애를 사전에 발견하였는가? – 목표 시간 내에 담당자에게 연락되었는가? – 연락이 필요한 모든 담당자에게 연락되었는가?		
3. 장애요인 분석	– 장애조치 절차서에 정의된 점검절차에 따라 점검이 이루어 졌는가? – 장애조치 절차서에 정의된 점검절차가 적절한가? – 장애요인이 예상하지 못한 장애발생 현상에 해당하는가? – 장애요인분석을 위해 필요시 장애 지식 데이터베이스를 적절히 활용하였는가?		
4. 장애조치 및 비상계획	– 예비품이 적절히 확보되었는가? – 상황실이 적절한 시간 내에 구성되었는가? – 상황실의 대응 방법 및 관련 부서와 의사소통이 적절하였는가? – 장애요인별 장애조치 절차서에 정의된 장애조치 목표시간 내에 조치가 이루어 졌는가? – 정의된 조치 목표시간이 적절한가? – 시스템 공급자에 대한 연락이 적시에 되었는가? – 시스템 공급자로부터 적절한 지원을 적시에 받았는가? – 장애조치를 위해 필요시 장애 지식 데이터베이스를 적절히 활용하였는가?		
5. 장애처리 결과보고	– 장애보고서가 규정된 시간 내에 작성되었는가? – 장애복구 우선순위가 적절히 판단되었는가?		
6. 훈련결과 보고	N/A		N/A

2 훈련시스템 개요

본 장에서는 주요 시스템에 대해 발생할 수 있는 여러 장애유형에 대한 원인파악, 조치, 훈련을 위해 주요 시스템을 구성하는 각 구성요소간의 관계 및 서비스 개요를 기술한다.

본 문서를 활용하여 평상시 시스템의 구성 및 역할을 이해하여 장애발생시 장애처리 절차에 따른 신속한 장애원인 파악 및 시스템 운영을 담당하는 여러 부서간의 원활한 의사소통을 할 수 있다. 또한 장애에 대한 훈련을 반복 수행함으로써 실제 환경에서의 주요 시스템에 대한 장애의 해결시간을 단축할 수 있다.

장애조치 훈련지침은 시스템 운영을 담당하는 여러 관련 부서간의 협조에 의해 작성되어야 하며, 시스템 변경에 따라 현행화될 수 있도록 관리되어야 한다. 본 장에서는 장애조치 훈련 대상이 되는 주요 시스템을 서술함에 있어 반드시 포함되어야 하는 개략적인 항목만을 언급하였으며, 각 정보시스템 담당자는 이를 참고로 실제 운영중인 주요 시스템의 현황을 문서화해야 한다.

2 1 시스템 개요

주요 시스템에 대한 업무 개요, 서비스 등을 설명한다. 어떤 목적의 서비스를 제공하는 시스템이며, 시스템명, 설치위치, 담당자(정 · 부) 등을 설명한다. 또한 연관된 주요 시스템을 설명해 놓음으로써 전체 시스템 구성을 이해하는데 도움이 된다.

2 2 시스템 구성요소

다음은 주요 시스템을 구성하는 구성요소들이며 본 장에서 설명해야 하는 일반적인 시스템 구성요소들이다. 아래 항목들 중에서 누락되거나 관련이 없는 사항들은 정보시스템 담당자가 판단하여 가감할 수 있다.

1) 서버 List

- 웹(Web) 서버
- Primary 파일서버
- Secondary 파일서버
- MS Exchange 서버
- Primary 데이터베이스 서버
- Secondary 데이터베이스 서버

2) 소프트웨어 List

- 모니터링 소프트웨어
- 바이러스 백신 소프트웨어

3) 방화벽

- Firewall 1
- Firewall 2

4) 네트워크 장비

- Router 1
- Router 2
- 메인 Switch
- 서브 Switch
- Local Hub 1
- Local Hub 2

2 3 시스템 및 네트워크 구성도

(주요 시스템의 모든 구성요소 및 연관관계가 그려진 구성도를 첨부함)

2 4 소프트웨어 구성도

(주요 시스템의 소프트웨어 구성요소 및 연관관계가 그려진 구성도를 첨부함)

2 5 구성요소별 세부 내용

본 장에서는 주요 시스템을 구성하는 세부 구성요소들에 대한 설명을 기술하고 주요 서버, 네트워크 장비 등에 대해 각 구성요소별로 각각의 상세한 속성을 설명한다. 주요 서버별로 모델, CPU 타입 및 개수, 운영체제, 메모리 타입 및 용량, 디스크 타입 및 용량, IP 주소, 설치된 소프트웨어 등을 설명한다. 또한 주요 시스템에서 발생가능한 주요 장애에 대해 사전에 문서화하여 훈련함으로써 신속한 대응 및 분석이 가능할 수 있다. 다음은 시스템 설명에 대한 예시이다.

예시 웹(Web) 서버

구성 요소
• 모델 : HP Proliant 7000 • CPU : Intel Xeon 프로세서 3.06 GHz (Dual) • 운영체제 : HPUX 7.0 (UNIX Type) • 메모리 : PC2100 DDR SDRAM– 1 GB (512MB x 2) • 디스크 : 내장형 100 GB HDD, 외장형 500 GB HDD • IP 주소 : 210.235.230.25
기 능
Internet information/Transaction 서버로서, 사용자들이 인터넷을 통하여 웹사이트에 접속하여 사용할 수 있는 HTML Front End를 제공하며 SQL 서버와 데이터베이스 트랜잭션을 처리한다. 세대의 서버가 클러스터 환경으로 구성되어 있으며, Windows load balancing 서비스가 사용되어 특정 서버에 장애가 발생하면 사용자 요청을 자동으로 다른 정상적인 온라인 서버로 경로를 재설정한다.

프로세스 구성

- usr/HTTPServer/bin/httpd (웹서버 프로세스)
- haemd HACMP 1nmapp1_nmapp2 SECNOSUPPORT (HACMP)

주요 장애 현상 및 원인

- 하나의 서버가 다운되었고, Windows Load Balancing 서비스 장애로 re-direct가 안됨
- 하나의 서버가 다운되었고, Load Balancing이 작동하나, 과중한 부하로 웹사이트 접속이 매우 느려, 사용자가 접속하지 못하는 것으로 인지함
- 세대의 Cluster 서버가 모두 다운됨. 서버 다운 원인은 다음과 같음
  - 하드웨어 구성요소 불량(LAN Card, 하드디스크 등)
  - 응용 소프트웨어 장애
  - 운영체제 Crash

  (발생 가능한 장애 현상 및 원인 기술한다.)

3 장애 대응 절차

비상연락체계는 유사시에는 매우 중요한 자료이다. 모의훈련을 수행함에 있어 실제 환경에서처럼 비상연락체계를 활용하여 장애 대응 능력을 점검해야 한다. 비상연락체계는 주기적으로 갱신되어야 하며 주요 담당자에게 공유되어야 한다. 다음은 일반적인 비상연락체계 샘플이다. 비상연락체계는 각 조직에 맞게 수정될 수 있지만 아래 항목은 반드시 포함되어야 한다. 또한 주요 시스템에 대하여 고유한 비상연락 프로세스가 있으면 프로세스 흐름도를 아래에 삽입할 수도 있다.

구 분	담당자	소속사	연락처	지원형태
웹 서버	홍길동	A사	010-XXXX-XXXX	상 주
데이터베이스 서버	홍길동	A사	010-XXXX-XXXX	상 주
데이터베이스	박문수	A사	011-XXXX-XXXX	상 주
미들웨어	박문수	A사	011-XXXX-XXXX	상 주
네트워크	이순신	A사	016-XXXX-XXXX	상 주
방화벽	김철수	A사	017-XXXX-XXXX	상 주
응용 소프트웨어	이영희	A사	019-XXXX-XXXX	상 주
웹서버 시스템 공급자	김영호	B사	010-XXXX-XXXX	비상주
DBMS 시스템 공급자	홍두깨	C사	011-XXXX-XXXX	비상주
네트워크 시스템 공급자	장길산	D사	016-XXXX-XXXX	비상주
외부 컨설팅	박남수	E사	017-XXXX-XXXX	비상주

부 록 II 정보시스템 자원별 장애처리 절차

1 개 요

정보시스템 자원별 장애처리 절차는 정보시스템을 구성하는 주요 자원에 대해 발생할 수 있는 시스템 장애를 사전에 문서화함으로써 시스템 운영조직 간의 의사소통을 원활히 하고, 주요 장애의 예상 장애원인 및 복구시간 등을 추정하는데 참고 될 수 있도록 해야 한다. 그리고 정보시스템 담당자는 자원별 장애처리 절차를 주기적으로 검토하고 훈련함으로써 실제 운영환경에서 발생하는 정보시스템 장애에 대해 적절히 대응할 수 있는 능력을 향상해야 한다.

자원별 장애처리 절차는 실제 운영 환경에 적용하면서 개선사항이 있으면 수시로 보완되어 관련자에게 배포되고 숙지되도록 하여야 하며 또한, 장애요인 파악을 위한 점검순서는 해당 장애현상에 대해 장애원인을 제공할 가능성이 높은 부분에 대해 우선적으로 점검하도록 작성된다. 정보시스템 자원별 장애처리 절차는 부록 Ⅰ의 '장애조치 훈련 지침'과 부록 Ⅲ의 '장애관리 시나리오'와 함께 활용되어질 때 효율적인 자료가 될 수 있다.

본 문서에서는 일반적인 정보시스템 자원에 대해 언급하였으며, 정보시스템 운영조직의 담당자는 해당 조직에서 운영중인 정보시스템 자원에 대해 아래와 같은 문서를 작성하여 활용하여야 한다. 아래의 장애처리 절차와 목표복구시간은 하나의 예제를 제시한 것으로, 각 기관에서 자원별 장애처리시에는 운영하는 시스템 자원의 특성에 따라 적절한 절차와 복구시간을 지정해야 한다.

2 자원별 장애처리 절차

자원별 장애처리 절차는 주요 자원에 대해 장애원인 점검에 의해 장애요인을 파악한 후, 그 장애를 조치하기 위한 작업절차를 기술한 것이다. 정보시스템 자원이라 함은 각종 서버, 응용 소프트웨어, 네트워크 장비, 데이터베이스 등을 일컫는다. 여기에는 장애를 근본적으로 해결하기 위한 절차 및 그러한 여유가 없는 경우에 사용할 수 있는 응급조치가 모두 포함된다. 장애조치 목표시간은 장애요인 파악 후 장애조치 완료시까지의 시간을 의미한다.

2 1 웹 서버 장애

장애 원인	장애 조치 순서	연락처	목표복구시간
웹 서버 디스크 한 개 불량	1) 교체해야 할 디스크를 파악 2) 서버를 정지 3) 새로운 디스크로 교체 4) 서버를 기동 5) Parity data를 바탕으로 데이터를 조치 6) 서비스 정상 가동 여부를 확인	서버관리팀, 홍길동	1시간
웹 서버 디스크 두 개이상 불량	1) 교체해야 할 디스크를 파악 2) 서버를 정지 3) 새로운 디스크로 교체 4) Ghost 디스크 이미지가 저장된 Swappable 디스크를 삽입한 후, Boot Disk를 사용하여 서버를 부팅 5) Ghost 응용소프트웨어를 실행하여 디스크 이미지를 로컬 디스크로 조치 6) 작업이 완료되면, 부팅 디스크 및 Swappable 디스크를 제거 후 재부팅 7) 서비스 정상 가동 여부를 확인	서버관리팀, 홍길동	2시간
프로세스별 리소스 (CPU, Memory, Disk) 점유율 과다	1) Resource 과다 점유 프로세스 kill 2) 오류 원인 제거 3) 프로세스 재실행	서버관리팀, 홍길동	5분

장애 원인	장애 조치 순서	연락처	목표복구시간
운영체제 손상	• 운영체제 백업이 있는 경우 1) 백업 데이터 복원 2) 시스템 재부팅 3) 데이터베이스 프로세스 기동 • 운영체제 백업이 없는 경우 1) 시스템 CD로 부팅 2) 운영체제 재설치 및 패치 적용 3) 시스템 재부팅	서버관리팀, 홍길동	5분
LAN card 불량	1) 교체해야 할 LAN 카드를 파악 2) LAN 카드 드라이버를 제거 3) 서버를 정지 4) 새로운 LAN 카드로 교체 5) 서버를 기동 6) 서비스 정상 가동 여부를 확인	서버관리팀, 홍길동	30분

2 2 응용 소프트웨어 관련 장애

장애 원인	장애 조치 순서	담당자	목표복구시간
응용 소프트웨어 오류	1) 변경전 원 프로그램으로 복원 2) 응용 소프트웨어 수정 후 재적용	데이터베이스 관리팀, 박문수	1시간
데이터 오류	1) 오류 데이터 확인 2) 오류 데이터 수정	데이터베이스 관리팀, 박문수	1시간
Batch 작업 오류	1) Batch 작업 kill 2) 오류 원인 제거 3) Batch 작업 성격에 따라 즉시 재실행 또는 온라인 마감 후 재실행	데이터베이스 관리팀, 박문수	

2 3 데이터베이스 또는 미들웨어 장애

장애 원인	장애 조치 순서	담당자	목표복구시간
Oracle 프로세스 정지/이상	1) Oracle DB rebooting	데이터베이스 관리팀, 박문수	10분
Oracle Archive 파일 Full	1) 백업 수행 후 Archive 파일 삭제	데이터베이스 관리팀, 박문수	10분
Oracle Listener 정지/이상	1) Listener 재시작	데이터베이스 관리팀, 박문수	10분
Oracle Home Directory Full	1) 파일 정리 또는 삭제	데이터베이스 관리팀, 박문수	10분
Oracle Block 손상	1) 최근 백업 테이프로 복원	데이터베이스 관리팀, 박문수	1시간
MQ 프로세스 정지/이상	1) MQ rebooting	데이터베이스 관리팀, 박문수	10분
MQ config. 파일 변경 이상	1) 변경 전 상태로 복원 및 수정 후 재적용	데이터베이스 관리팀, 박문수	10분

부 록 III 장애관리 시나리오

1 개요

장애관리 시나리오는 장애가 발생할 수 있는 예상 현상을 기술하고, 각 현상별로 장애요인을 파악하기 위한 점검순서 및 담당자를 기술한다. 장애발생시 2차 지원 그룹의 담당자는 아래 장애현상 가운데 유사한 것을 찾아서 해당 현상에 대한 대응 절차에 따라 장애요인을 파악하고 대응하며, 장애요인 파악을 위한 점검순서는 해당 장애현상에 대해 장애원인을 제공할 가능성이 높은 부분에 대해 우선적으로 점검하도록 작성된다.

장애관리 시나리오는 실제 운영 환경에 적용하면서 개선사항이 있으면 수시로 보완되어 관련자에게 배포되고 숙지되도록 하여야 한다. 장애관리 시나리오는 부록 Ⅰ의 '장애조치 훈련 지침'과 부록 Ⅱ의 '정보시스템 자원별 장애처리 절차'와 함께 활용되어질 때 효율적인 자료가 될 수 있다.

2 장애발생 시나리오

장애발생 시나리오는 크게 3가지로 내용이 설명되며, 일반적인 장애발생, 문제 관리 대상의 주요 장애발생, 비상상황 대상의 주요 장애발생 등이다. 정보시스템 담당자는 본 문서를 참고로 하여 각 조직에서 운영하는 주요 시스템의 장애에 대해 문서화함으로써 장애 대응능력을 향상시킬 수 있도록 해야 한다. 아래 설명된 장애발생 시나리오는 장애관리지침 및 각 운영조직의 정보시스템 운영규정을 따른다.

2 1 시나리오 상황 설정

본 문서에 서술된 장애 시나리오는 가상의 정보시스템 회사에서 발생할 수 있는 상황을 가정하여 설정하였다. 이 회사는 전국적인 조직을 가지고 있으며 전용 네트워크 구성망을 활용하여 일반 사용자 및 법인사용자를 대상으로 무선 이동통신 서비스를 제공하는 업체이다. 이 업체는 내부 사용자를 위한 인트라넷 서비스와 일반 사용자를 대상으로 하는 웹서비스를 제공하고 있다. 또한, 일반 사용자 및 내부 사용자를 위한 전용 서비스 데스크 조직을 운영하고 있으며 전용 전화를 통해 24시간 서비스 장애접수 및 해결을 시도한다.

2 2 일반적인 장애발생 시나리오

장애등급 3 또는 4에 해당하는 일반적인 장애에 대한 시나리오를 서술한다. 낮은 등급의 일반적인 장애는 서비스 영향력이 크지 않고 1차 또는 2차 장애해결을 시도함으로써 장애가 종료된다.

가. 장애식별/접수

사용자가 웹사이트에 접속하였는데, 본인의 개인정보 조회시 데이터가 뜨지 않는다. 사용자

는 유선을 통해 서비스데스크 요원에게 장애 상황을 접수하고 조치를 요청한다.

나. 장애등록 및 등급지정

서비스 데스크 요원은 접수받은 장애를 등록하고 장애관리시스템에서 동일 유형의 장애 접수 건수를 점검한다. 동일 유형의 장애접수 건수가 없음을 확인한 후 요원은 직접 웹 서버에 접속하여 장애접수 내용을 테스트한다. 테스트 결과 특정 사용자에 국한된 장애임을 확인하고 장애등급 3을 책정한다.

다. 1차 해결

서비스 데스크 요원은 장애관리시스템의 지식 데이터베이스를 검색하여 조치 이력을 검토한 후 접수된 장애의 1차 해결을 시도한다.

라. 장애 배정

서비스 데스크 요원은 1차 해결 과정을 통해 장애가 조치되지 않음을 확인하고 2차 지원 그룹인 서버관리팀의 홍길동 대리에게 장애를 배정한다.

마. 2차 해결

서버관리팀 홍길동 대리는 장애 통보(Notify) 기능을 통해 장애 배정을 확인한 후 장애내용을 점검하기 위해 장애관리시스템에 접속하여 해당 장애의 내용을 확인한다. 웹사이트에서 특정 사용자의 정보 조회가 안 되는 것을 확인하고 다음 사항을 점검한다. 신속한 조치를 위해 데이터베이스 관리자인 서버관리팀 박문수 대리에게 해당 테이블 점검을 요청한다.

예상발생지점	장애요인 파악을 위한 점검 순서	관련팀 및 담당자
웹 서버	1) 최근 서버/응용 소프트웨어 변경사항 점검 2) 메모리, 디스크 등 하드웨어 자원 점검 3) 인터페이스 프로세스 점검	서버관리팀 홍길동
데이터베이스	1) Background 프로세스 점검 2) Oracle Listener 점검 3) 해당 테이블 이상 유무 점검	데이터베이스관리팀 박문수

서버관리팀 홍길동 대리는 웹서버에서 데이터베이스와 인터페이스 하는 특정 프로세스의 홀딩(Hang-up) 상황을 확인하고 강제로 해당 프로세스를 종료 후 재시작 함으로써 장애를 해결한다.

바. 장애종료

홍길동 대리는 장애의 처리상태를 해결(Resolved) 상태로 변경한다. 장애관리 시스템의 장애 통보 도구는 자동적으로 해당 서비스 데스크 요원에게 장애해결 상태를 알린다. 서비스 데스크 요원은 장애접수 사용자에게 유선으로 통화(Call-Back)하여 서비스의 정상 유무를 확인한 후 장애의 처리상태를 장애종료(Closed) 상태로 변경한다.

2.3 문제관리 대상의 주요 장애발생 시나리오

장애등급 1 또는 2에 해당하는 주요 서비스 장애에 대한 시나리오를 서술한다. 높은 등급의 주요 장애는 서비스에 미치는 영향이 큼으로 경우에 따라서는 문제관리 단계로 진행되어 장애해결을 시도함으로써 장애가 종료된다.

가. 장애식별/접수

대전지역 사무소 직원이 사내 인트라넷에 접속하였으나 접속이 되지 않고, 옆의 동료도 접속

이 되지 않음을 확인한 후 유선을 통해 서비스 데스크 요원에게 장애 상황을 접수하고 조치를 요청한다.

나. 장애등록 및 등급지정

서비스 데스크 요원은 접수받은 장애를 등록하고 장애관리시스템에서 동일 유형의 장애 접수 건수를 점검한다. 동일 유형의 장애가 다수 접수되었고, 현재도 계속해서 장애가 접수되고 있다. 요원은 서비스 데스크 관리자에게 보고하고 장애등급 1을 책정한다.

다. 1차 해결

서비스 데스크 요원은 중앙시스템의 장애로 판단하고 1차 해결 시도를 생략한다.

라. 장애 배정

서비스 데스크 요원은 2차 지원그룹의 데이터베이스 관리팀 박문수 대리에게 장애를 배정한다. 동시에 미리 설정된 장애 통보(SMS) 기능을 통해 장애관리 책임자 및 시스템 담당자에게 장애등급 1의 주요 장애가 발생했음이 전파된다.

마. 2차 해결

데이터베이스 관리팀의 박문수 대리는 장애 통보(Notify, SMS) 기능을 통해 장애 배정을 확인한 후 장애내용을 점검하기 위해 장애관리시스템에 접속하여 해당 장애의 내용을 확인한다. 인트라넷 관련 시스템 이상으로 추정하고 다음 사항을 점검한다. 동시에 장애관리 책임자는 네트워크관리팀 및 서버관리팀 담당자에게 시스템 이상 유무 점검을 요청한다.

예상발생지점	장애요인 파악을 위한 점검 순서	관련팀 및 담당자
데이터베이스	1) 최근 서버/응용 소프트웨어 변경사항 점검 2) Background 프로세스 점검 3) Archive 파일 Full 여부 점검 4) Oracle Listener 점검 5) Oracle Home Directory Full 여부 점검 6) Block 손상 여부 점검 7) 데이터베이스 점검 중 서버 장애로 의심되면 서버 담당자에게 점검을 의뢰	데이터베이스 관리팀, 박문수
데이터베이스 서버	1) 최근 서버/응용 소프트웨어 변경사항 점검 2) 메모리, 디스크 등 하드웨어 자원 점검 2) 인터페이스 프로세스 점검 3) 인터페이스 소스코드 점검 4) 데이터 오류 확인 5) 데이터 처리 소스코드 점검 6) 데이터 디스플레이 소스코드 점검 7) 이상이 없는 경우, 데이터베이스 담당자 또는 네트워크 담당자에게 점검을 의뢰	서버관리팀, 홍길동
네트워크	• 방화벽 담당자 (김철수) 1) Firewall-1 점검 2) Firewall-2 점검 • 네트워크 장비 담당자 (이순신) 1) Router 점검 2) Switch 점검 3) Hub 점검	네트워크 관리팀, 김철수, 이순신

바. 문제등록

장애관리 책임자는 장애원인이 명확하지 않아 장애시간이 길어짐에 따라 문제관리 책임자와 협의하여 문제관리 등록을 한다.

사. 근본원인 도출 및 해결방안 선택

문제관리 책임자는 2차 지원그룹의 관리자를 소집하여 장애의 원인 및 해결 방안에 대해 협의한다. 근본원인 도출 협의시에도 담당자는 계속해서 장애조치를 위한 활동을 수행한다. 2차 지원그룹의 관리자는 회의 소집에 앞서 관련 시스템 공급자에 장애지원을 요청한다.

문제관리 책임자는 협의를 통해 장애원인을 추정하고, 다음과 같은 3단계의 조치 방안을 수립한다.

- ▶ 1단계 : 데이터베이스 관련 프로세스를 재실행한다. (30분 소요)
- ▶ 2단계 : 데이터베이스 서버를 재실행한다. (1시간 소요)
- ▶ 3단계 : 데이터베이스, 데이터베이스 서버, 네트워크 장비 등 모든 관련 시스템을 재실행한다.

아. 해결방안 실행 및 점검

데이터베이스 관리팀의 박문수 대리는 관리자의 지시에 따라 1단계 해결방안인 데이터베이스 엔진을 재실행한다. 재실행 전에 관련 덤프 및 로그를 별도 디렉토리에 저장한다.

데이터베이스를 재실행하였으나 서비스 장애는 지속된다. 서버관리팀의 관리자는 2단계 데이터베이스 서버 재실행을 서버담당자인 홍길동 대리에게 지시한다.

문제관리 책임자는 모든 과정에 참여하여 조치과정을 모니터링하고 해당 관리자와 의사결정을 협의한다. 또한 전산실장(경영층)에게 장애 현황을 보고한다.

서버관리팀의 홍길동 대리는 데이터베이스 서버 재실행이 정상적으로 처리되지 않음을 확인하고 시스템 공급자에게 세부 점검을 요청한다. 대기 중이던 시스템 공급자는 점검 후 디스크 장애를 추정하고 해당 디스크를 논리적으로 분리하고 재실행한다. 데이터베이스 서버는 정상적으로 재실행되고 데이터베이스 담당자는 백업 데이터를 활용해 깨진 데이터를 복구한다.

자. 문제종료

데이터베이스 서버 및 데이터베이스가 정상 재실행되고 서비스는 정상화되었다. 문제관리 책임자는 문제종료를 선언하고 전산실장(경영층)에게 장애해결을 보고한다.

차. 장애종료

데이터베이스 관리팀의 박문수 대리는 배정된 장애처리상태를 해결(Resolved) 상태로 변경한 후 장애를 서버관리팀의 홍길동 대리에게 재배정할 것을 요청한다. 장애관리시스템의 장애 통보 도구는 자동적으로 해당 서비스 데스크 요원에게 장애해결 상태를 알린다.

서비스 데스크 요원은 장애접수 사용자에게 유선으로 통화(Call-Back)하여 서비스의 정상 유무를 확인한 후 장애의 처리상태를 장애종료(Closed) 상태로 변경한다.

카. 프로세스 점검

서버관리팀의 홍길동 대리는 장애관리시스템에 장애보고서를 작성하여 팀장의 승인을 받는다. 또한 시스템 공급자와 협의하여 문제가 된 디스크의 교체를 야간에 작업하기로 하고 긴급변경 작업 등록을 한다.

장애관리 책임자 및 문제관리 책임자는 장애조치 과정에서의 문제점을 점검하고 필요시 장애처리 절차를 보완한다. 또한 장애관리 책임자는 승인된 서버관리팀 장애보고서를 점검하고 향후 이행 방안 및 변경작업 내용을 확인한다.

2.4 비상상황 대상의 주요 장애발생 시나리오

장애등급 1 또는 2에 해당하는 주요 서비스 장애에 대한 시나리오를 서술한다. 높은 등급의 주요 장애는 서비스 영향이 큼으로 경우에 따라서는 문제관리 및 비상상황 관리 단계로 진행되어 장애해결을 시도함으로써 장애가 종료된다.

가. 장애식별/접수

본사 근무 직원이 인터넷 및 사내 인트라넷 접속이 안 됨을 확인하고 유선을 통해 서비스 데스크 요원에게 장애 상황을 접수하고 조치를 요청한다.

나. 장애등록 및 등급지정

서비스데스크 요원은 접수받은 장애를 등록하고 장애관리시스템에서 동일 유형의 장애 접수 건수를 점검한다. 동일 유형의 장애가 다수 접수되었고, 현재도 계속해서 장애가 접수되고 있다. 요원은 서비스 데스크 관리자에게 보고하고 장애등급 1을 책정한다.

다. 1차 해결

서비스 데스크 요원은 네트워크 백본 시스템의 장애로 판단하고 1차 해결 시도를 생략한다.

라. 장애 배정

서비스 데스크 요원은 2차 지원그룹의 네트워크관리팀 이순신 대리에게 장애를 배정한다. 동시에 미리 설정된 장애 통보(SMS) 기능을 통해 장애관리 책임자 및 시스템 담당자에게 장애등급 1의 주요 장애가 발생했음이 전파된다.

마. 2차 해결

네트워크관리팀 이순신 대리는 장애 통보(Notify, SMS) 기능을 통해 장애 배정을 확인한다. 장애가 배정되기 전부터 이순신 대리는 자체 네트워크 모니터링 기능에 의해 백본에 이상 트래픽이 대량 발생되어 회선 사용량이 100%를 유지하고 있음을 인지하고, 방화벽 및 침입감지시스템 담당자와 점검하고 있는 중이었다. 동시에 네트워크 관리팀의 관리자는 장애관리 책임자 및 문제관리 책임자에게 네트워크 장애의 현황을 유선 통보한다.

장애관리 책임자는 데이터베이스 및 서버 담당자에게 유선으로 장애상황을 통보하고 모니터링 강화를 요청한다.

예상발생지점	장애요인 파악을 위한 점검 순서	관련팀 및 담당자
네트워크	1) Firewall의 이상 트래픽 점검 2) 백본 Router 및 Switch의 사용량 점검 3) 이상 트래픽의 패턴을 점검 4) 트래픽의 유입경로 및 영향 범위를 파악 5) 바이러스 감염 여부 및 백신업체 확인	네트워크관리팀
데이터베이스	1) 데이터베이스의 서비스 상태를 모니터링	데이터베이스 관리팀, 박문수
웹 서버, 데이터베이스 서버	1) 운영중인 서버의 상태를 모니터링	서버관리팀, 홍길동

바. 비상상황 관리

네트워크관리팀의 관리자는 이상 트래픽의 패턴이 전국적인 영향을 미치고 있는 신종 바이러스 감염에 의한 영향으로 파악하고, 장애관리 책임자 및 문제관리 책임자에게 현황을 통보한다. 장애관리 책임자는 문제관리 책임자와 협의하여 비상상황 관리위원회를 소집한다.

사. 장애 영향 파악 및 해결방안 선택

비상상황 관리자는 관련 2차 지원그룹의 관리자를 소집하여 장애의 해결 방안에 대해 협의한다. 또한 사전에 정해진 역할에 따라 경영층 보고 및 피해정도를 집계한다. 네트워크 관리자는 바이러스 백신 업체와의 채널을 유지하고 상황을 점검한다.

비상상황 관리자는 피해 및 영향 범위에 따른 다음과 같은 2단계의 조치 방안을 수립한다.

▶ 1단계 : 이상 트래픽이 유입되는 네트워크 포트를 일시 차단하여 내부 망 복구

▶ 2단계 : 바이러스 감염 PC의 네트워크 물리적 차단 및 바이러스 치료 백신 배포

아. 해결방안 실행 및 점검

네트워크 관리팀의 이순신 대리는 관리자의 지시에 따라 1단계 해결방안인 이상 트래픽 유입

포트를 차단하여 회선 사용량을 감소시킨다. 네트워크관리팀은 실시간으로 관련 로그 및 데이터를 별도 저장하고 관리한다.

1단계 작업으로 특정 업무를 제외한 내부 네트워크 망이 임시 복구되었다. 비상상황 관리자의 지시로 관련팀들의 협조 하에 바이러스 치료 백신을 모든 PC에 설치한다. 이때 중앙 배포서버에 의한 온라인 배포 및 설치는 네트워크 회선 사용량을 증가시킴으로 CD 및 이동디스크에 의한 수동 설치를 시도한다.

장애관리 책임자 및 문제관리 책임자는 모든 과정에 참여하여 조치과정을 모니터링 하고 비상상황 관리자의 의사결정을 지원하고 관련 회의록을 문서화한다.

자. 비상상황 관리 종료

비상상황 관리자는 바이러스 치료 및 백신프로그램 배포가 완료되면서 네트워크 회선이 정상 복구됨에 따라 비상상황 관리 종료를 선언하고 경영자에게 장애피해 상황 및 조치 경과를 최종 보고한다.

차. 장애종료

네트워크 관리팀의 이순신 대리는 배정된 장애의 처리상태를 해결 상태로 변경한다. 장애관리시스템의 장애 통보 도구는 자동적으로 해당 서비스 데스크 요원에게 장애해결 상태를 알린다.

서비스 데스크 요원은 장애접수 사용자에게 유선으로 통화하여 서비스의 정상 유무를 확인한 후 장애의 처리상태를 장애종료 상태로 변경한다.

카. 프로세스 점검

네트워크 관리팀의 이순신 대리는 장애관리시스템에 장애보고서를 작성하여 팀장의 승인을 받는다. 장애관리 책임자 및 문제관리 책임자는 장애조치 과정에서의 문제점을 점검하고 필요시 장애처리 절차를 보완한다.

장애관리 책임자는 승인된 서버관리팀 장애보고서를 점검하고 향후 이행 방안 확인한다.

부록 Ⅳ 장애관리 양식

- □ 장애접수보고서
- □ 장애결과보고서
- □ 일일 시스템 업무보고
- □ 장애관리대장
- □ 장애관리 비상연락망
- □ 장애현황보고 (임원보고양식)
- □ 장애현황보고 (언론대응양식)

장 애 접 수 보 고 서

담 당	검 토	승 인

협조 1	협조 2

장애요청번호		장애발생일시	
요청부서		요청자	
연락처		조치기한일자	
접수자		접수 일자	

발생시스템			
장애 현상			
장애영향도			
장애 유형	☐ 조작 미숙, 실수	☐ S/W 상의 문제 [요구변경 : Y/N]	☐ H/W, N/W 등 기타
조치긴급도	☐ 긴급 조치	☐ 사후 조치	
조치자		연락처	
응급조치내용			

조치 시간	일 시	소요 M/D	조치 현황
합 계			
조치내용 요약			
해결 내용			
향후 대책			

장 애 결 과 보 고 서

담 당	검 토	승 인

협조 1	협조 2

장애 제목	
내용/현상	
장애 원인	
영향 범위	

발생 일시		해결 일시		장애 시간	분
장애 번호		장애 유형		장애 등급	
작성 일자		작성 부서		작성자	

조치 시간	조치 내용 및 결과	조치자

향 후 이 행 대 책	완료일	이행 담당자

일 일　시 스 템　업 무 보 고

1. 일　　시	(2004. 1. 16 (금) 00:00 ~ 24:00)
2. 보　고　자	(전산실 운영담당 홍길동 과장)
3. 주 요　장 애	(장애등급 1, 2, 3 위주로 내용 보고) – 장애제목 : – 장애일시 : – 장애등급 : – 장애현상 : – 장애원인 : – 영향범위 : – 비　　고 :
4. 주 요　작 업	(주요 변경작업 위주로 내용 보고) – 작업내용 : – 담 당 자 : – 작업등급 : (Risk 1, 2, 3, 4) – 업무영향 : – 작업상태 : (정상완료, 부분완료, 원상복귀, 장애유발 등) – 비　　고 :
5. 특 이　사 항	(주요 장애 또는 변경작업 이외의 특이사항 내용 보고) – 태풍 '민들레' 영향으로 인해 09:00 현재 전남지역 한전 전원 공급 불안정. – 웜 바이러스(Welchia)로 인해 09:00 현재 수도권 지역 네트워크 속도 지연.

장 애 관 리 대 장

요청번호	발생일시	접수일자	조치기한일자	조치일자	조치 내용	조치자	장애 유형

장 애 관 리　비 상 연 락 망

소　속	이　름	직　위	업　　무	사무실 전화	이동 전화	자택 전화

장 애 현 황 보 고 (임원보고양식)

1. 장 애 일 시	(2004. 1. 16 (금) 14:00 ~ 16:00 (120분))
2. 장 애 내 용	(시스템의 장애내용 서술)
3. 장 애 원 인	(시스템의 장애발생 원인 서술)
4. 영 향 범 위	
- 관련 지역	(장애로 인해 영향을 받는 관련 회사 및 지역)
- 업무 영향	(구체적인 고객사 업무 영향)
5. 조 치 경 과	(시간대별 조치경과 (주요 Action별))
6. 복구 예정 시간	(복구 예정 시간 서술)
7. 여 론 동 향	
- 고 객	(장애로 인한 응대 내용 및 불만 내용, 규모 등)
- 언 론	(언론 동향 및 대응 상황)
8. 기타보고사항	

장 애 현 황 보 고 (언론대응양식)

1. 장 애 일 시	(2004. 1. 16 (금) 14:00 ~ 16:00 (120분))
2. 장 애 내 용	(시스템의 장애내용 서술)
3. 장 애 원 인	(시스템의 장애발생 원인 서술)
4. 영 향 범 위	
– 관련 지역	(장애로 인해 영향을 받는 관련 회사 및 지역)
– 업무 영향	(구체적인 고객사 업무 영향)
5. 조 치 경 과	(시간대별 조치경과 (주요 Action별))
6. 복구 예정 시간	(복구 예정 시간 서술)
7. 기타보고사항	

정보시스템 장애관리 지침

인쇄 : 2005년 12월
발행 : 2005년 12월

발행처 : 국무조정실 · 정보통신부

〈지침 개발 참여위원〉

· 한국전산원 이헌중 팀장
· 한국전산원 안현수 선임
· 한국전산원 김은영 선임
· 광운대학교 김기윤 교수
· LG CNS 민성기 책임
· (주)베니트 박남수 팀장
· 동국대학교 이영재 교수
· SK C&C 전한수 과장

본 자료는 제22차 정보화추진위원회(2004.2.25)에 보고된 '국가기간전산망 운영실태 점검 결과'에 따른 개선대책 후속조치로 한국전산원에서 작성된 지침입니다. 본 지침과 관련된 문의는 다음을 이용하여 주시기 바랍니다.

■ **우편문의**

(우)100-170 서울특별시 중구 무교동 77번지 NCA 빌딩
한국전산원 ITA팀 정보시스템 장애관리 지침 담당자 앞

■ **전화문의 : 02-2131-0114**

- 한국전산원 ITA팀 이헌중 팀장
- 한국전산원 ITA팀 김은영 선임연구원

Guideline for Incident & Problem
Management of Information System

문의처

한국전산원
100-775 서울시 중구 무교동 77번지 NCA빌딩
www.nca.or.kr Tel | 02.2131.0114 Fax | 02.2131.0409