[문서 번호: PM-2025-001]

[작성 일자: 2025. 12. 10]

주요 장애 처리 결과 보고서 (Major Incident Post-Mortem)

: 서비스 안정성 확보를 위한 장애 원인 분석 및 재발 방지 대책 리포트

---

1. 개요 (Overview)

1.1 목적

본 문서는 과거 발생했던 **Critical(심각)** 등급 이상의 주요 장애에 대하여 발생 경위, 근본 원인(Root Cause), 조치 결과, 재발 방지 대책을 기록합니다. 이를 통해 유사 장애 발생 시 신속한 참고 자료로 활용하고, AI 지식 베이스(Knowledge Base)에 학습시켜 장애 대응 역량을 강화합니다.

1.2 RAG(검색 증강 생성) 학습 가이드

- **학습 포인트:** 장애 발생 시점, 장애 현상(Symptom), 근본 원인(Cause), 해결 방법(Solution).
- **예상 질문:** "작년 5월 인터넷 장애 원인이 뭐였어?", "DB 데드락 발생 시 어떻게 조치했어?"

---

2. 장애 사례 분석 (Incident Case Study)

CASE 1. 대규모 인터넷 서비스 접속 지연 (DDoS)

항목	상세 내용
장애 ID	**INC-202405-001**
발생 일시	2024년 05월 15일 (14:10 ~ 15:40, 약 90분)
장애 등급	**Critical (서비스 중단)**

항목	상세 내용
장애 현상	수도권 지역 인터넷 가입자 접속 불가 및 속도 저하, 고객센터 민원 폭주 (3만 건 이상).
영향 범위	서울/경기 지역 일부 국사 하단 가입자 약 50만 회선.

2.1 타임라인 (Timeline)

- **14:10** NMS 트래픽 알람 발생 (평시 대비 500% 급증).
- **14:15** 보안관제센터(SOC) 유입 트래픽 분석 착수.
- **14:25** 특정 해외 IP 대역에서의 대규모 UDP Flooding 공격 확인 (DDoS).
- **14:40** 1차 대응: 공격 IP 대역 차단(ACL) 적용 $₩rightarrow$ 공격 IP 변조로 실패.
- **15:00** 2차 대응: **클린존(Scrubbing Center) 우회 경로 활성화** 및 Null-Routing 적용.
- **15:30** 트래픽 정상화 확인 및 서비스 순차 복구.
- **15:40** 상황 종료.

2.2 근본 원인 (Root Cause Analysis)

- **직접 원인:** 해외 해커 그룹에 의한 **DNS 증폭(Amplification) DDoS 공격** 발생.
- **기여 요인:** 당시 백본망의 예비 대역폭을 초과하는 1.2Tbps급 트래픽 유입으로 라우터 CPU 부하 발생.

2.3 재발 방지 대책 (Action Items)

1. **인프라 증설:** 백본망 용량을 기존 2Tbps에서 4Tbps로 증설 (완료: 2024.10).
2. **정책 강화:** 해외 유입 UDP 트래픽에 대한 Rate Limit 임계치 하향 조정.
3. **시스템 도입:** AI 기반 DDoS 자동 탐지 및 방어 솔루션 고도화.

CASE 2. AICC 상담 애플리케이션 로그인 불가 (DB)

항목	상세 내용
장애 ID	**INC-202408-012**
발생 일시	2024년 08월 20일 (09:00 ~ 09:45, 45분)
장애 등급	**Major (기능 마비)**
장애 현상	AICC 상담원 로그인 시도 시 "시스템 오류" 팝업 발생, 상담 업무 개시 불가.
영향 범위	AICC 이용 고객사 3곳 (약 200명 상담석).

2.1 타임라인 (Timeline)

- **09:00** 업무 개시와 동시에 로그인 불가 리포트 접수.
- **09:05** WAS 로그 확인: JDBC Connection Timeout 에러 다수 발견.
- **09:15** DB 모니터링 확인: Active Session 급증 및 Lock 발생 확인.
- **09:20** 원인 파악: 전날(8/19) 배포된 통계 쿼리가 **Table Full Scan**을 유발하여 **DB Deadlock(교착 상태)** 발생.
- **09:30** 긴급 조치: 해당 쿼리 세션 강제 Kill 및 전날 버전으로 애플리케이션 **롤백(Rollback)**.
- **09:45** 로그인 정상화 확인.

2.2 근본 원인 (Root Cause Analysis)

- **직접 원인:** 신규 배포된 '상담 이력 조회' SQL문에 인덱스(Index)가 누락되어 대량의 데이터를 조회하며 DB 자원을 독점함.
- **관리적 원인:** 배포 전 대용량 데이터 환경에서의 **성능 테스트(Load Test) 미비**.

2.3 재발 방지 대책 (Action Items)

1. **프로세스 개선:** SQL 성능 점검(Explain Plan 확인) 없이 배포 금지 프로세스 의무화.
2. **모니터링 강화:** DB Long Running Query(3초 이상) 실시간 알림 설정.
3. **인프라:** 읽기 전용(Read-Only) DB 복제본(Replica) 구성하여 조회 트래픽 분산.

CASE 3. 클라우드 스토리지 파일 업로드 실패 (Storage)

항목	상세 내용
장애 ID	**INC-202411-005**
발생 일시	2024년 11월 05일 (11:00 ~ 13:00, 2시간)
장애 등급	**Major (일부 기능 제한)**
장애 현상	고객사 앱에서 이미지/파일 업로드 시 실패, 다운로드는 정상.
영향 범위	Object Storage 이용 고객 전체.

2.1 타임라인 (Timeline)

- **11:00** 파일 업로드 실패 알람(500 Error) 수신.
- **11:10** 스토리지 노드 점검: 디스크 용량은 충분하나 Inode 고갈 확인.
- **11:30** 원인 분석: 특정 고객사가 수백만 개의 1KB 미만 초소형 파일(Tiny Files)을 생성하여 파일 시스템 메타데이터 공간(Inode) 소진.
- **12:00** 긴급 조치: 해당 버킷(Bucket)에 대한 쓰기 권한 임시 제한 및 Inode 증설 작업.
- **13:00** 서비스 정상화.

2.2 근본 원인 (Root Cause Analysis)

- **기술적 원인:** 파일 시스템 포맷 시 설정된 **Inode(파일 개수 제한)** 할당량이 실제 데이터 증가 패턴을 반영하지 못함.

- **정책적 원인:** 고객별 파일 개수 생성 제한(Quota) 정책 미적용.

2.3 재발 방지 대책 (Action Items)

1. **설정 변경:** 스토리지 포맷 방식을 XFS로 변경하고 동적 Inode 할당 기능 활성화.
2. **정책 적용:** 테넌트(Tenant)별 최대 객체 수 제한(Max Object Count) 정책 적용.

---

3. 종합 통계 및 교훈 (Lessons Learned)

3.1 2024년 장애 유형 통계

- **DDoS/보안:** 15%
- **소프트웨어 버그/배포:** 45% (가장 높음, QA 강화 필요)
- **하드웨어/인프라:** 20%
- **휴먼 에러:** 20%

3.2 총평

2024년 발생한 장애의 절반 가까이가 **변경 작업(배포, 설정 변경)** 직후 발생했습니다. 향후 모든 변경 작업에 대해 **'변경 관리 위원회(CAB)'의 승인 절차를 강화**하고, 자동화된 테스트 파이프라인(CI/CD)을 고도화하여 인적 오류를 줄이는 것이 2025년의 핵심 과제입니다.