'시스템 장애는 왜 두 번 일어났을까?'을 읽고

작 성 일 : 20.06.08
작 성 자 : 도 원 진

1. "미즈호 은행" 두번째 시스템 장애

1.1. ''미즈호은행''의 계정계시스템 마비

일시: 2011년 3월 14일

1.1.1. 표면적 원인

- **데이터의 상한값 설정오류 (송금 데이터 처리건수 설정의 오류)**
  - 23년간 유지된 배치처리 설정
  - 온라인처리 : 데이터 1건씩 처리 (현금 인출과 출금)
  - 배치처리 : 데이터 처리요청을 간직하고 있다가 업무시간 이후에 데이터 처리 진행
- **2개의 구조 병행**
  - 온라인 처리와 배치처리
  - 23년 전 설계구조를 방치하며 개선하지 않은 점
- **상급자에게 에러 상황에 대한 늦은 보고**
  - 혼자 처리를 감행하려는 담당자가 끝내 해결을 못하고 늦은 보고를 진행
- **부서간 소통부재**
  - 미즈호은행의 시스템부서, 정보종합연구소간의 소통부재
- **늦은 결단력**
  - 문제상황으로 부터 4일이 지난 18일 부터 서비스 정지후 점검진행
  - 실제로 24일에 모든 시스템장애를 해결함
  - 시간이 걸리더라도 운영을 중지하고 제대로 해결하는 방법을 택하지 않음

1.1.2. 근본적 원인

- **계정계시스템 내용의 복잡화(블랙박스화)**
  - 1억 행의 소스코드 (10년간 천명의 엔지니어가 개발하는 양)
  - 시스템 사양을 자세하게 파악할 수 없는 양
- **형식적인 감사**
- **비용과 리스크에 대한 두려움으로 시스템개선을 이루지 못한 점**
- **경영진의 IT업무 중요성, 역할 인지 부족**

1.1.3.해결책

- **경영진의 IT 경시문화 개선**
- **시스템 담당 CIO 배정**

- **이사회 멤버로 시스템 담당 임원 배정**
- **정보를 더 공개할 것**
    - 제 3자를 투입하여 시스템장애의 원인을 분석
    - 외부의 지적을 받아 프로젝트에 반영할 것

2. "미즈호 은행" 첫 번째 시스템 장애

2.1. 시간 순서

- 1999년 8월
    - 3개 은행의 통합 발표
        - 다이치간교 은행
        - 후지 은행
        - 니혼코교 은행
- 1999년 8월 20일 기자회견
- 2002년 4월 1일 장애발생

2.2. 장애의 근본원인

- 접속계 시스템의 장애
    - 구 다이치간교은행과 구 후지은행이 사용하는 대외 접속계시스템에서 구 후지은행을 외부시스템으로 간주
    - 접속계시스템에서 후지은행이 고립되는 상황 발생

3. 그 외 금융기관의 대규모 장애

3.1. 도쿄 증권거래소

- 일시 : 2005년 12월 8일
- 원인
    - 오발주로 인한 4백억엔 손실
- 개선책
    - 스즈키CIO 새로 영입
    - 과거의 거래규정이나 관례에 사로잡히지 않고 이상적인 업무프로세스 정비
    - 처리속도 향상 도모

3.2. 도쿄공업품거래소

- 일시 : 2009년 5월 12일
- 원인

    - 백업용 라우터 과부하 및 다운
- 근본원인
    - '하트비트 신호'의 송신간격 : 표준보다 5배 짧은 시간설정
    - 대기용 장비 구동중 실 가동용 장비의 사용률 상승

3.3. 도쿄소방청

- 일시 : 2011년 1월
- 원인
    - LAN케이블 설치오류로 통신 무한로프 발생

3.4. 하네다 공항 관제시스템 다운

- 일시 : 2010년 1월 14일
- 원인
    - 기상 데이터 저장과정에서 메모리 overflow 발생
    - 서버내부 회로의 SCF 고장

4. 동작하지 않는 컴퓨터를 없애는 십계명

4.1. 경영진 시스템 도입을 지휘

- 회사나 사업을 어떤 식으로 개혁시킬지 방침을 정해야 한다.
- 방침이 정해지면 필요한 정보를 정의할수 있고 정보시스템의 기능을 정의할 수 있다.

4.2. 여러 개발회사 비교, 자사 업무에 정통한 업체

- 고객 기업의 업무에 정통한 시스템 개발회사는 거의 없다.
- 따라서, 업무 프로그램을 잘 사용하여 정보시스템을 제대로 개발하는 회사를 알고있는 컨설팅회사를 잘 선별해야함.

4.3. 개발회사를 하청취급하거나 개발비를 함부로 깎지 않는다

- 의욕적인 중견 시스템 개발 회사와 직접 계약시 제조업체를 경유할 때보다 저비용으로 개발할 수 있다.

4.4. 자사의 시스템 구축능력 파악. 무리가 없는 계획수립

4.4.1. 프로젝트 계획단계에서 성패가 결정된다

- 성공의 판단요인

    - 빈틈없는 계획
    - 빠른 구현

4.4.2. 개념공유

- 두 기업이 합병이 됐을 때, 두 은행의 기존 시스템을 비교, 평가한다.
- 모든 구성원들이 이 정보를 공유한다.

4.5. 사내 책임 체제

- 프로젝트를 책임 총괄하는 관리자가 반드시 있어야 한다.
- 위탁 기업이 정해준 업무만이 시스템 개발회사에서 진행하므로 빠른 처리를 위해 일을 결정할 수 있는 사람이 필요함.

4.6. 요구사항에 많은 시간투자, 요구사항이 결정되면 함부로 변경하지 않을 것

4.7. 개발 진척은 자사에서 파악, 테스트와 검사에 많은 시간을 쏟기

4.8. 시스템이 가동될 때까지 포기하지 않고, 모든 수단과 방법을 도입

- 프로젝트 관리를 기업에 정착시킨다.
    - 개인의 능력에만 의존했던 프로젝트 관리를 표준체계를 기반으로 한 통합관리시스템으로 대체한다.
    - 사람에 따라 기술을 익히지 말고, 기술자를 대체가능한 업무표준을 만든다.
- 관리시스템을 둔다
    - 세계표준인 PMBOK 활용
    - 범위, 일정, 비용, 품질, 인적자원, 의사소통, 리스크, 조달로 나누어 9가지 영역에서 효과를 볼 것.

4.9. 시스템 개발회사와 유상A/S 계약을 맺는 등의 방법으로 유지보수 체제 확립

4.10. '부주의로 인한 ' 오류를 경시하지 말고 근본적 대책을 수립한다.

- **수 많은 설정값에 대한 주의 필요**
- **오류의 근본적 원인을 분석**
- **다음의 관행을 주의할 것**
    - 단순한 '작업실수'라고 여긴다
    - 오류를 꾸짖고 처벌한다
    - 뿌끄럽다고 숨긴다
    - 룰이라고 우긴다
    - 점검 강화로 끝낸다
    - 운용은 단순 작업이라고 생각

- 경영과 품질부서가 인솔

5. 느낀점

IT서비스에 장애는 없을 수 없다. 있어도 얼마나 신속한 대응을 하느냐에 따라 그 서비스의 평판이 달라진다. 그러기 위해서는 만반의 준비를 해야한다. 위기대응 메뉴얼을 만들고 전문가의 조언을 구하고 부서간의 비상연락망을 구축하는 등. 그런면에서 미즈호은행은 구 3사 은행의 통합부터, 2011년의 대형사고 까지 안일한 준비를 한 것이다.

특히 3개 은행의 시스템 통합과정이 무리한 방법으로 진행되었다는 점이 가장 안타깝게 다가왔다. 개발업무를 하는 이들은 고객의 요구사항을 IT기술을 통해 해소해주는 일을 한다. 그러나 미즈호은행 통합과정에서 필요한 새로운 경영방침, 전략, 조직개편, 영업점 통폐합을 정립하지 못한 채 정보시스템 통합을 진행했다. 이는 개발자에게 애매모호한 요구사항을 전달하는 요인이 될 뿐더러 시스템 결함을 가져오게 만든다. '호미로 막을 것을 가래로 막는 격'인 셈이다.

시스템가동은 개발과정과 별개로 또 다른 시작이다. 경영진의 IT개발인력에 대한 인식의 개선이 필요하며, 부주의를 줄여나가도록 메뉴얼을 필수로 숙지하고 "시간이 걸려도 제대로" 라는 모토로 두 번의 같은 시스템 장애가 일어나는 일을 막아야 할 것이다.