

## 11주차 3차시 시스템 평가와 최적화

### 【학습목표】

1. 시스템에 대한 정확한 수행기준들을 설명할 수 있다.
2. 시스템 최적화를 추진하기 위해서 기존 개발 운용되는 시스템을 평가해야할 측면을 파악할 수 있다.

### 학습내용1 : 시스템 평가 및 최적화의 개념

#### 1. 시스템 평가 (system evaluation)

- 1) 시스템의 목표가 성취되었다고 생각될 경우 그 시스템의 수행능력을 측정하기 위한 조직적인 임무를 의미
- 2) 실행단계에서 중요한 것으로서 시스템의 수행능력과 출력에 대한 것을 정량적으로 나타내고 그들을 설계단계에서 설정한 목표와 비교하는 것을 목적으로 실시함
- 3) 이 과정에서 시스템의 수행능력이나 출력의 설계단계에서 설정한 목표와 합치할 경우에는 그 시스템은 적합한 것으로 판정하여 계속적으로 사용될 것이고 그렇지 않다면 시스템 분석가는 그 원인을 규명하여 재설계해야 함.

#### 2. 시스템 최적화 (system optimization)

- 1) 변화된 요인을 적합하게 고려하여 최대의 능력을 발휘할 수 있도록 조화된 설계를 해야 함
- 2) 시스템의 수행능력을 개선하기 위한 시스템 구성요소들의 재설계이며 세련된 방안임

### 학습내용2 : 수행기준

#### 1. 시스템에 대한 정확한 수행기준(performance criteria)들

- 1) 변화된 요인을 적합하게 고려하여 최대의 능력을 발휘할 수 있도록 조화된 설계를 해야 함.
- 2) 시스템의 수행능력을 개선하기 위한 시스템 구성요소들의 재설계이며 세련된 방안임

#### 2. 수행능력의 측정기준

- 1) 하드웨어 및 소프트웨어의 수행능력, 시간, 비용, 생산성, 정확도, 보안성, 사기(morale), 사용자와 고객의 반응 등을 이용함.

### 3. 시간적 요소

#### 1) 시계

- 시스템 평가 도구로서 중요한 역할을 하는데 특정한 행위를 수행하기 위해서 요구되는 시간 단위(time unit)를 기록하는데 이용

#### 2) 시간 개념은 시스템의 수행능력을 평가하는데 반드시 고려되어야 할 요소

#### 3) 응답시간 (response time)

- 컴퓨터 시스템이 주어지는 입력에 대해서 반응할 때까지에 드는 시간을 의미
- 어떤 시스템에서는 처리시작으로부터 몇 시간 혹은 며칠이 들 수도 있으며, 시스템에 따라서는 지연 없이 즉시 처리되는 경우도 있음

#### 4) 반환시간(turn around time)

- 사용자가 수집한 데이터를 컴퓨터 센터로 보낸 시점에서부터 컴퓨터에서 데이터를 처리하여 그 결과를 사용자에게 되돌려 줄 때까지 드는 시간

### 4. 비용요소

#### 1) 시스템 가동비용

- 수행능력을 정량적으로 측정하는 척도

#### 2) 비용

- 시스템의 모든 부분을 수행하기 위한 예산을 확정하는데 이용

#### 3) 노무비(labor cost)

- 직원들에게 반드시 지급해야 할 비용
- 월급, 급여율, 커미션과 같은 것들은 노무비의 정량적 측정 요소들임

#### 4) 고정비용 (overhead cost)

- 변화되지 않는 시스템 비용
- 기계, 설비, 물리적 장치, 컴퓨터 및 조명 등에 드는 비용들을 포괄적으로 지칭하는 것

#### 5) 가변비(variable cost)

- 출력의 크기에 따라서 변화되는 비용

#### 6) 유지관리비(maintenance cost)

- 물리적 장치, 사무실 설비, 통신회선, 컴퓨터 하드웨어 및 소프트웨어 등의 관리 및 유지에 드는 비용
- 시스템이 설치된 이후부터 평가하여 산출할 수 있음
- 시스템이 설치 운영되는 동안에 처리능력을 평가하는 요소가 됨

#### 7) 확장변경비(expansion modification)

- 시스템을 수정 보완하거나 변경시키는 경우에 발생하는 비용

8) 교육훈련비(training cost)

- 시스템을 평가하는 기간 동안에 부과되는 관계 요원들의 교육과 훈련에 드는 비용

9) 데이터 입력비(data entry cost)

- 출력, 처리, 설비비 등과 같은 다른 요소들과 관련시켜서 측정해야 함
- 자동화된 데이터 입력시스템(data entrysystem)에서 OCR, MICR, OMR, POS(point of sales)에 사용되는 바코드(bar code)와 같은 것들을 사용함으로써 데이터 입력비는 낮아지지만 설비비는 높아짐

10) 데이터 저장비(data storage cost)

- 매우 다양한 형태를 보임
- 액세스 능력, 저장장치의 유형, 파일의 시큐리티(security) 등과 같은 요소들과 관련시켜서 평가해야 함

11) 기타비용(other cost)

- 통신 회선비, 중복 서비스비, 컨설팅비, 백업장치의 임차비 등과 같은 잡다한 비용
- 시스템 평가에서 반드시 하나의 요소로서 취급하고 포함시켜야 함

## 5. 하드웨어 능력

1) 하드웨어 능력(hardware performance)을 평가하는 요소로서 반드시 포함해야 할 항목

- 속도, 신뢰도, 서비스, 유지관리, 운영비, 요구수준 등

2) 컴퓨터 시스템(computer system)

- 비즈니스 시스템에서 중요한 비용요소 부분으로서 그 작동은 전체 수행에 중대한 영향을 미침
- 비즈니스 시스템에 중요한 비용부문을 점유하는 컴퓨터 시스템에 대해서 평가해야 할 측면
  - 컴퓨터 시스템의 중요한 요소들은 초기의 기대치에 대하여 평가되고 비교 검토되어야 함
    - 포함되어야 할 요소 : 처리시간,장비의신뢰도,유지관리비, 입출력 장치의 속도 및 보조기억장치의 실행능력과 같은 항목들
  - 컴퓨터 시스템은 오퍼레이터와 사용자의 교육훈련 기간에 대해서도 평가되어야 함

3) 기타 하드웨어 시스템

- 시스템에서 사용되는 기타 장치와 설비들에 대해서도 수행능력의 평가와 비교되어야 함
- 이 범주에 속하는 사항들
  - 컴퓨터, 워드프로세싱 기계, 복사기, 마이크로 필름장치와 같은 것들
  - 시스템의 확장, 변경 등의 경우에 대체 수단이나 방안이 될 수 있기 때문임

## 6. 소프트웨어

- 수행능력(software performance)

1) 사용자가 작성한 소프트웨어

2) 구입한 프로그램 패키지 등을 포함해서 실시

3) 평가에 포함되어야 할 요소

- 처리속도
- 출력에 대한 질과 양적인 문제
- 정확도
- 신뢰도
- 유지관리비

## 7. 생산성(productivity)

1) 입출력 사이의 관계나 비율에 대해서 시스템의 수행능력을 측정

2) 일반적으로 전체 시스템이나 부분 시스템의 생산성은 시스템의 수행능력을 측정할 수 있는 기준의 하나가 됨

## 8. 정확도(accuracy)

1) 에러가 포함되지 않도록 하거나 혹은 사실에 합치하도록 하여 시스템에 의한 성취의 정도를 측정

## 9. 컴퓨터 시큐리티(computer security)

1) 시스템에서 처리 및 관리되는 정보들이 시스템의 통제 하에 안전하게 유지 및 기록되는지 여부를 평가하는데 중요한 개념

2) 컴퓨터 시스템에서 취약성을 가지고 있는 측면

- 기술적 측면의 취약성

- 업무처리의 고도화로 새로운 매체 등이 복합적으로 사용되기 때문에 에러 또는 장애의 발생원인이 복잡해서 그 원인의 추적이나 방지대책 수립이 어려움
- 매체의 극소화로 부정확한 반출이나 파괴(소실)가 간단히 이루어질 수 있음
- 매체의 불가시성(不可視性) 및 개인적 특징이 없어져 시큐리티의 문제가 제기됨
- 정보 통신이 일반화됨에 따라서 원격지에서 액세스하는 경우가 많아지고 이에 따라서 해커(hacker)나 컴퓨터 범죄자들의 시큐리티 위협에 대해서 기술적으로 대처하기가 어려움

- 사회적 측면의 취약성

- 정보통신망을 일상적으로 활용함에 따라서 대형사고가 발생할 가능성은 상존하고 있으며, 만일 이러한 대형사고가 발생할 경우 사회적으로 많은 문제가 일어남

- 실제로 대형사고가 발생했던 대표적인 예
  - 1977년에 발생했던 뉴욕의 대정전사고
  - 1984년에 발생했던 일본의 世田谷 전화국 화재
- 조직적 측면의 취약성
  - 컴퓨터에서 데이터 처리의 핵심적인 과정은 시스템 내부에서 이루어지기 때문에 블랙박스(black box)화한 상황으로 처리되므로 눈으로 확인하거나 다른 검증 절차를 거치기 어려움
  - 일반적으로 컴퓨터 처리는 단위 업무를 담당하는 개인에 의해서 일괄적으로 처리되기 때문에 내부 견제기능의 붕괴로 인한 위험성이 증가되고 있음
  - 컴퓨터 시큐리티(computer security)는 대책이 수립되고 운용되어야 할 측면
    - 기술적 측면의 시큐리티
    - 설비적 측면의 시큐리티
    - 운용관리적 측면의 시큐리티
    - 시스템 감사 제도

## 10. 기술적 시큐리티

### 1) 기술적인 측면에서 시큐리티를 높이는 방안

- 신뢰성 제고
- 데이터 보호와 부정방지
- 암호화에 의한 통제
- 데이터베이스 통제

### 2) 신뢰성 제고

- 소프트웨어 기술의 관점
  - 시큐리티 제고는 장애억제, 장애영향의 최소화, 장애회복 등과 같은 사항이 고려되어야 함.
  - 장애억제
    - 소프트웨어의 장애발생을 억제하고 신뢰성을 향상시키기 위해서는 IPT(improved programming technologies)나 객체지향 프로그래밍(object oriented programming), 칩프 프로그래머(chief programmer) 제도의 도입, 워크스루(walkthrough) 등의 개선된 개발기법들을 적용하는 것이 효과적임
  - 장애영향의 최소화
    - 장애부분을 분리시키고 시스템을 재구성하여 운용 또는 처리하는 방안
    - 파일을 백업시스템에 의해서 운용하는 방안
  - 장애회복
    - 컴퓨터 시스템에 일단 장애가 발생했을 경우에 신속하게 정상으로 회복할 수 있는 소프트웨어적 대응 방안은 필수적으로 요구되는 사항임
- 하드웨어 기술의 관점
  - 시큐리티 제고 방안은 다중화 시스템, 듀플렉스 시스템, 로드공유 시스템, 이중 시스템, 케이블관련설비의 이중화 등과 같은 관점에서 고려되어야 함

- 다중화 시스템(multi system)
  - 시스템을 구성하는 장치 사이에는 말할 것도 없고 장치 사이의 결합으로도 다중화되어 있기 때문에 시스템을 구성하는 어느 장치가 장애를 일으켜도 그 장치를 시스템으로부터 분리할 수 있음
- 듀플렉스 시스템(duplex system)
  - 사용자가 요구하는 처리능력을 가진 컴퓨터 2대를 설치하고, 그 중에서 한 대는 예비 컴퓨터로 대기시켜 놓고 평상시 사용하던 컴퓨터에 장애가 발생할 경우에 즉시 예비 컴퓨터를 활용하는 방법
- 로드공유 시스템(load share system)
  - 처리할 업무량이 많기 때문에 한 대의 컴퓨터로 처리가 불가능할 때 같은 규모의 컴퓨터 2대를 설치하고 부하를 두 대의 컴퓨터에 분산시켜 처리하는 방법
- 이중 시스템(dual system)
  - 높은 신뢰도가 요구되는 특수한 업무의 경우에는 그 내용을 2대의 컴퓨터가 병행으로 처리함으로써 어느 하나의 컴퓨터에서 장애가 발생하더라도 업무처리 기능에 지장을 가져오는 것을 막을 수 있는 방법
  - 듀플렉스 시스템이 어느 한 시스템에서 다른 시스템으로 전환하는 과정에 동작중단이 되는 단점을 보완함
- 케이블 · 관련설비의 이중시설
  - 대형화재와 같은 재해에 대응하기 위하여 케이블이나 관련설비를 이중으로 설비해서 장애 발생 시에 즉시 대처 토록하여 피해를 최소화시키려는 방안

### 3) 데이터 보호와 부정방지

- 액세스 통제와 사용자 확인
- 분리에 의한 액세스 통제
- 기타 액세스 통제 등의 측면에서 방안이 마련되어야 함
- 액세스 통제와 사용자 확인
  - 컴퓨터 시스템의 운영방식이 개방 서비스(open service)형태로 전환되고 사용자가 대폭적으로 증가되며 정보통신의 일상화로 분산처리 시스템의 보편화는 시큐리티에 많은 문제점을 제기하고 있음
  - 이러한 환경의 변화에 대응하여 부정한 액세스를 방지하고 시큐리티를 높이기 위해서 사용자의 소유물에 의한 식별, 사용자의 개인정보에 의한 식별, 사용자의 특징에 의한 식별 등의 방안이 고려됨

- 사용자의 소유물에 의한 식별
  - 사용자 개개인에게 터미널 보호용 자물쇠, 자기카드, 광학식 카드 등을 교부하여 이들을 교부 받은 유자격자를 식별(identification)하여 인증(authentication)된 경우에 한해서 시스템을 액세스할 수 있도록 통제하는 방법
  - 무자격자의 액세스를 배제할 수 있음
  - 사용자 개인정보에 의한 식별
    - 사용자에게 부여된 패스워드(password)로 시스템 액세스 통제를 함으로써 안전성을 확보하는 방법
  - 사용자 특징에 의한 식별
    - 사용자가 본인의 성명이나 식별번호(identification number)를 입력시키고 나서 다시 다음과 같은 사용자에게 개인적 특성을 확인하는 과정을 거쳐서 유자격자 여부를 판정함으로써 시큐리티를 높이는 방법
      - 손의 형태(손가락 길이 및 굵기)
      - 성문(voice print)
      - 지문(finger print)
      - 서명분석(서명속도, 가속도, 필압)
      - 뇌파의 패턴(brain wave pattern)
      - 기타의 유전적 특징(발의 형태, 귀의 형태, 치아의 형태)
- 분리에 의한 액세스 통제
  - 분리(isolation)는 사용자가 자신의 업무 이외에는 액세스할 수 없도록 시스템 구성을 분리시켜서 시큐리티를 확보하는 방안
  - 시간분리
    - 이 방안은 몇 가지 형태로 구분할 수 있음
    - 특정한 장치는 특정한 업무를 수행하는 시간대에 한정하여 시스템에 접속시키는 방안
    - 특정한 업무는 특정한 시간대에만 수행하는 방안
    - 중요한 업무와 일반업무는 시간대를 달리하여 수행시킴으로써 시큐리티를 높이는 방법
  - 공간분리
    - 물리적 메모리의 공간을 분리시켜서 데이터를 기억시키고 허락된 유자격자만이 시스템을 액세스 함으로써 시큐리티를 높이는 방안
  - 특권제한(restriction of privilege)
    - 사용자가 시스템을 사용할 경우 허용된 범위 내로 액세스 권한을 제한시킴으로써 시스템 액세스를 통제하는 방안
- 기타의 액세스 통제
  - 탐지·감시(surveillance)
    - 시스템 액세스를 위하여 수립된 여러 가지 규칙을 철저히 준수하는지 여부를 확인하여 시큐리티를 확보하는 방안
    - 컴퓨터 시스템 운용 시에 액세스에 관련되는 데이터를 수집해 두었다가 정기적으로 분석하여 현저한 변화가 나타난 사용자를 찾아내서 부정한 액세스 여부를 판정하는 경향분석(trend analysis) 방법
  - 위협로그 파일
    - 시스템에 위협을 가하는 경우가 발생하면 그 상황을 위협감시 로그파일(threat attempt log files)에 기록시켜 두었다가 시스템 감사(system audit)나 통제의 톨로 사용하여 시큐리티를 확보하는 방안
    - 시스템 위협 : 시스템에 대한 로그인(log-on)의 실패,비밀 파일에 대한 액세스 시도, 특권명령 세트의 부정사용, 업무처리의 이상종료, 시스템의 이상종료, 하드웨어 및 소프트웨어의 기밀보호기구 고장
  - 자동로킹(automatic Locking)

- 시스템의 로그인(log-on)을 일정한 횟수이상 실패했을 경우에는 해당 터미널을 로그아웃(log-out) 및 자동로그 시킴으로써 시큐리티를 높이는 방안

#### 4) 암호에 의한 통제

- 정보통신에서 일반적인 평문(plaintext or cleartext)을 해독하기 어려운 형태로 변환시키거나 암호화한 통신문을 해독 가능한 형태로 변환시키기 위한 원리, 수단 및 방법 등을 내용으로 하는 기술을 이용하여 시큐리티를 높이는 방안

#### 5) 데이터베이스 통제

- 데이터베이스를 지원하는 데이터베이스 관리 시스템(DBMS : database management system)에서의 시큐리티 문제에 어려움의 요소
  - 데이터의 저장기능을 가짐
  - 데이터의 생산 및 합성기능을 함
  - 터미널이나 다른 DBMS와 통신기능
- 데이터 저장기능이라는 측면에서 데이터베이스의 시큐리티 문제 대책
  - 사용자에게 의한 부정 이용으로부터 보호
  - 하드웨어 고장 시의 보호
  - 바이러스로부터 보호
  - 보조기억장치의 재난이나 도난으로부터 보호
- 데이터 전송의 측면에서 고려될 사항
  - 안전한 데이터 통신의 실현
  - 고속과 병행처리가 가능한 효율적 알고리즘 개발
- 데이터베이스 사용권의 종류
  - 데이터 판독권리
  - 데이터 변경권리
  - 데이터 삭제권리
- 데이터베이스 사용권을 통제하는 대표적인 방식
  - 집중형 사용권 통제
    - 모든 데이터는 작성단계에서 데이터베이스 관리자(database administrator)가 그 사용권을 관리하도록 규정
  - 계층형 사용권 통제
    - 이는 데이터베이스에 관련되는 사람을 데이터베이스 관리자, 데이터베이스 소유자, 데이터베이스 비소유 사용자 등의 계층으로 구분하여 각 계층에 합당한 사용권을 부여하여 통제하는 방식
  - 동적 사용권 통제
    - 데이터 양이 증가되어 집중형 관리가 어려운 경우나 데이터 내용의 변화로 인해서 비교적 자유로 공유자나 사용자를 변경할 수 있다는 점에서 채택하는 방안



## 11. 설비적 시큐리티

- 1) 자연재해(화재, 지진, 홍수)로부터 보호대책
- 2) 무자격자나 불법침입자에 의한 파괴와 같은 물리적 보호대책
- 3) 문제에 대한 대책 요약
  - 시스템 고장에 대한 설비적 대책
    - 자연재해로부터 시스템을 안전하게 보호하기 위해서는 건물의 구조를 강화하고 방재설비를 확충하여 환경을 개선
  - 안전운용을 위한 설비적 대책
    - 우선 데이터의 누설, 파괴, 변경 등과 같은 부정을 방지하기 위해서 방법대책(입퇴실 기록, 식별장치, 모니터 카메라 설치)을 수립함.
    - 인적재해를 방지하기 위해서는 컴퓨터 시스템의 주변통제, 데이터 처리부문의 액세스 통제 대책 수립

## 12. 운용관리의 시큐리티

- 1) 운용관리 부문에서 시큐리티를 높이기 위한 대책
  - 조직체제 개선
    - 직무분담의 명확화, 액세스의 명확한 통제, 책임과 권한의 명확화 등으로 내부건제 기능이 효율적으로 이루어지도록 체제를 구축해야 함
    - 교육훈련과 인사관리를 철저히 하여 시스템의 원활한 운용유지를 꾀해야 함
    - 시스템의 운용관리 규정을 확정하고 준수함

## 13. 시스템 감사제도

- 1) 시스템 감사
  - 시스템의 신뢰성, 안전성, 효율성을 높여서 정보화 사회의 건전화에 기여함을 목적으로 실시되는 것
  - 시스템의 시큐리티 제고에 커다란 기여를 할 수 있는 방안

## 14. 사기(moral)

- 1) 관계되는 요원들이 자신의 업무에 대하여 만족하는 정도를 반영함
- 2) 사기 진작은 직접 측정하기 어려움

## 15. 사용자와 고객의 반응

- 1) 시스템을 사용하는 사람이나 또는 그 시스템에 영향을 받게 될 사람(예를 들면 고객)들의 반응은 시스템 수행능력을 측정할 수 있는 또 다른 요소가 됨

## 학습내용3 : 시스템 최적화

### 1. 시스템 최적화(system optimization)

- 계획된 목표와 실제 성취 사이에 차이점이 존재하는 경우 해결을 위한 대안으로서 새로운 기계, 기술, 소프트웨어 등을 외부로부터 구입하는 것

## 학습내용4 : 요약

### 1. 시스템 평가

1) 대상 시스템의 목표 달성 여부를 판정하기 위하여 시스템의 수행능력을 평가하는 것

### 2. 시스템 최적화

1) 시스템의 수행능력을 개선시키기 위하여 재설계하거나 개선하는 방안을 포함

### 3. 시스템에 수행능력

1) 시간적 요인을 측정하는 평가기준 : 응답시간, 반환시간 등

2) 비용적인 측면 : 중요한 평가기준은 노무비, 고정비, 가변비, 유지관리비 등

3) 부가적인 고려 사항 : 교육훈련, 데이터 입력비, 데이터 저장비 등

### 4. 하드웨어의 수행능력에 관련되는 요소

1) 속도, 신뢰도, 서비스, 유지관리, 운영비, 요구능력 등

### 5. 소프트웨어 수행능력

1) 신뢰도, 유지관리, 유지관리를 위한 갱신 등

### 6. 시스템 최적화를 추진하기 위해서 기존 개발 운용되는 시스템을 평가해야 할 측면

1) 실제로 시스템이 목적인 바와 같이 적합성(effectiveness)을 발휘하는지 여부

2) 시스템이 어느 정도 정확한 결과를 제공하는지에 대한 신뢰성(reliability)의 수준

3) 시스템이 어느 정도의 유용성(usefulness)있게 사용되기 쉽고 합리성을 구비하고 있는지에 대한 평가

4) 변화 대응의 용이성 및 에러의 발견 용이성과 같은 유지보수성(maintainability)의 정도

5) 시스템이 사용하는 메모리의 양, 자원의 구성 및 사용의 적정성, 처리시간의 단축 등과 같은 효율성(efficiency)의 수준

## 7. 최적화 추진 원칙

- 1) 시스템을 구성하고 있는 부문 중에서 최적화할 필요성이 존재하는 부문을 선정하여 실시
- 2) 가능한 한 기존 시스템의 골격을 유지하면서 필요한 부문의 효율을 개선하는데 목표를 둬
- 3) 시스템의 최적화를 위해서 수정 보완된 시스템은 가능한 한 단순 명료성을 가지도록 배려해야 함

## 【학습정리】

1. 시스템 평가 및 최적화의 개념을 알아본다.
2. 수행기준을 파악한다.
3. 시스템 최적화를 이해한다.