

## 데이터베이스

여러 사람에 의해 공유되어 사용될 목적으로 통합하여 관리되는 데이터의 집합

통합된 정보들을 저장하여 운영할 수 있는 공용 데이터들의 묶음

- 자료구조 vs 데이터베이스

자료구조: 대부분 주기억장치에서 이루어질 내용

데이터베이스: 대부분 보조기억장치에서 이루어질 내용

관계형, 키-값형, 객체형, 문서형, 컬럼형

저장된 자료들을 어떤 형태로 모식화 할 수 있느냐 에 따라 나누게 된다.

관계형 구조: RDB라고 부르며 기업에서 많이 사용하나 처음 설계하기가 복잡함. 테이블과 컬럼이 추가 될 때마다 마이그레이션 작업을 해야 한다. 생성된 품에 맞게 변경, 추가, 삭제를 해야 한다.

- DBMS

DataBase Management System

데이터베이스에 접근할 수 있는 기능을 제공하는 소프트웨어. 즉, 데이터베이스계의 운영 체제

MySQL, PostgreSQL, SQLite, mariaDB 등

- SQL

Strucure Query Language

DBMS를 통해 데이터를 관리하기 위한 구조화된 질의문을 작성하기 위한 언어(질의어)

관계형 데이터베이스 관리 시스템에서 주로 사용

## 네트워크

- LAN (Local Area Network) 근거리통신망. 랜선랜선하는 케이블 이름이 아님

라우터: LAN과 LAN을 연결하거나 LAN과 WAN을 연결하기 위한 인터넷 네트워크

크

- MAN (Metropolitan Area Network) 도시권통신망, WAN (Wide Area Network) 광역통신망
- 인터넷

컴퓨터로 연결하여 TCP/IP 프로토콜을 이용해 정보를 주고받는 컴퓨터 네트워크

- TCP/IP (Transmission Control protocol) 전송 제어 규약. 속도와 데이터를 완벽하게 보내는 것이 문제. 신뢰성이 있는 방식임

(Internet Protocol)인터넷 사용규약

- WWW (World Wide Web) 문서들이 있는 정보의 저장소, 분산과 연결
- URL (Uniform Resource Locator

[Protocol]:// [host] : [port] / [path]

- Protocol : 통신 규약 , 장비사이에서 메시지를 주고 받는 양식과 규칙의 체계. 즉 통신 할 때 정해진 메시지 규칙

- HTTP – Hyper Text Transfer Protocol

HTTP Method

GET (주소에 정보를 실어서 보내는 방법. 빠르지만 최신정보는 아닐 수 있음)

POST (내부 몸통에 정보를 실어서 보내는 방법. 항상 최신)

(GET과 POST에 대한 부가설명 <https://blog.outsider.ne.kr/312> )

PUT 자료에 바디, 파라미터에 넣어서 서버에 올림

DELETE 자료에 바디, 파라미터에 넣어서 서버에서 지움

- FTP: File Transfer Protocol. 파일을 보내는것에 특화가 되어있고 HTTP로도 할수있음, 보안이 취약하고 암호화가 없어서 흔히 사용을 안한다.
- SFTP: Secure File Transfer Protocol
- TELNET: Terminal Network 원격 로그인을 위한 프로토콜. 원격으로 다른 컴퓨터 접속. 보안이 안됨
- SSH: Secure Shell Telnet 의 대응 목적으로 설계 되었으며 네트워크상의 다른 컴퓨터에 로그인하거나 원격 시스템에서 명령을 실행하고 다른 시스템으로 파일을 복사할 수 있도록 해 주는 응용 프로그램 또는 그 프로토콜. TELNET 대응 목적으로 설계함

■ SSL: Secure Socket Layer 웹 서버와 브라우저 사이의 보안을 위한 프로토콜

■ SMTL: Simple Mail Transfer Protocol 전자메일 보낼 때 사용하는 프로토콜

- Host: 네트워크에 연결된 장치

호스트 이름: 네트워크에 연결된 자치에 부여되는 고유한 이름

예) IP주소, 도메인주소, MAC주소

- IP Address

컴퓨터 네트워크에서 장치들이 서로를 인식하고 통신을 하기 위해 사용하는 번호

192.168.0.50 – 가 현재 강의를 듣는 나의 IP인데 192로 시작하는 IP는 대부분 공유기에서 할당되는 IP이다.

유동아이피 – 개인 사용자들이 사용할 때 대부분 유동아이피를 사용하게 된다. 사용하지 않으면 회수되며 다시 사용할 때 할당된다.

고정아이피 – 지속적으로 접근 해야 할 필요가 있는 서버의 경우 고정아이피를 할당 받아서 사용한다. 주로 웹 서비스들이 해당된다.

- Domain Address

네트워크상에서 컴퓨터를 식별하는 호스트이름

- DNS (Domain name system)

호스트의 도메인 이름을 호스트의 네트워크 주소로 바꾸거나 그 반대의 변환을 수행

- MAC Adress (Media Access Control Address) 네트워크 어댑터에 부착된 고유한 식별자

- Port: 가상의 논리적 통신 연결. 단, 번호로 구분

OSI 7 계층 모형 - 이런 게 있다는 것만

## 암호화

- 대칭키

암호화와 복호화에 같은 암호 키를 쓰는 알고리즘.

DES, AED, SEED

고전적인 방식으로는 pasAswAord - 비밀번호에 A 를 추가하여 암호화하고 A를 제거하면 비밀번호가 됨

SEED는 공인인증서관련 암호화방식이다.

- 공개키(비대칭키): 공개키로 암호화된 데이터를 비밀키로 사용하여 복호화 할 수 있는 암호화 알고리즘

RSA방식: HTTPS 통신에 사용되는 방식이다.

- 암호화 해시 함수

임의의 데이터를 고정된 길이의 데이터로 매핑하여 원래의 입력 값과의 관계를 찾기 어렵게 만든 것 - 고정된 길이의 값이기 때문에 실제로 MD5의 경우 이미 전부다 해독되어서 안 쓴다고 함.

자주 보게되는 용어들을 한번 찾아보면 더 많이 알아갈 수 있을 것이다.