제130회 정보관리기술사 해설집

2023.05.20

국가기술자격 기술사 시험문제

기술사 제 130 회 제 4 교시 (시험시간: 100 분)

분야	정보통신	자격종목	정보관리기술사	수검번호		성명	

※ 다음 문제 중 4 문제를 선택하여 설명하시오. (각 25 점)

1. 음성데이터 마이닝의 정의, 목적, 주요 기술, 활용 가능 분야, 발전 방향에 대하여 기술하시오.

2. 최근 많은 범죄들이 지능화, 고도화 되면서 디지털 포렌식의 중요성이 증가하고 있다. 이러한 디지털 포렌식과 관련하여 아래 사항을 설명하시오.

   1) 디지털 포렌식의 개념

   2) 디지털 포렌식의 유형과 절차

   3) 디지털 포렌식 기술 및 활용분야

3. 최근 다수의 기업들이 클라우드 서비스를 도입하면서 다양한 보안 문제가 대두되고 있다. IT 담당자 입장에서 클라우드 서비스 도입 시 고려해야 할 보안 요소를 설명하시오.

4. IT 프로젝트를 성공적으로 수행하기 위해 요구사항이 체계적인 관리와 문서화가 매우 중요하다. 요구사항에 대하여 다음을 설명하시오.

1) 소프트웨어(SW) 요구사항 품질속성

2) 요구사항 도출기법

3) 요구사항 개발 프로세스

5. 웹 3.0 에 대하여 다음을 설명하시오.

1) 웹 3.0 의 도입배경 및 개념

2) 웹 3.0 의 주요특징 및 기술요소

3) 웹 3.0 기반의 서비스 활용 방안

6. 데이터옵스(DataOps)와 데브옵스(DevOps)에 대하여 다음을 설명하시오.

1) 데이터옵스와 데브옵스의 비교

2) 데이터옵스 아키텍처 및 주요 기술

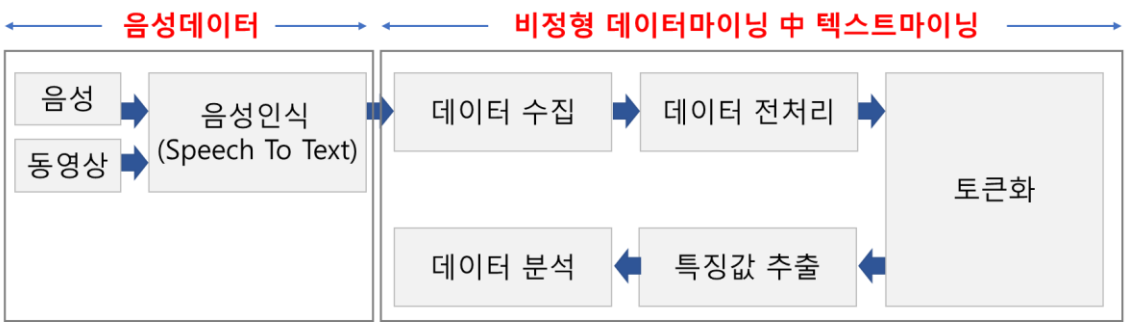
01	음성데이터 마이닝		
문제	음성데이터 마이닝의 정의, 목적, 주요 기술, 활용 가능 분야, 발전 방향에 대하여 기술하시오.		
도메인	인공지능	난이도	중 (상/중/하)
키워드	음성인식 STT, 의미분석, 형태소분석, 구문분석,		
출제배경	영상 데이터 다음으로 음성 데이터에 대한 분석 및 마이닝 부각		
참고문헌	IT기술사회 자료		
출제자	단합반 안경환 기술사(제 110회 정보관리기술사 / akh.itpe@gmail.com)		

I. 음성데이터 마이닝의 정의와 목적

정의

- 콜 센터 등의 비정형 데이터인 대량의 음성 데이터를 정련하여 정형 데이터로 변환하고 분류, 군집화, 회귀분석, 이상탐지 등의 기법으로 유의미한 정보를 추출하는 분석기법
- 음성데이터 마이닝을 음성인식을 통해 텍스트로 변환된 데이터를 수집하여 전처리를 통해 분석을 통해 의미 있는 결과도출을 하는 과정

구성도



목적

빅데이터 중 비정형 데이터 규모(volume) 증가	- 빅데이터 환경에서 거의 80% 이상이 비정형 데이터이므로, 빅데이터 분석 시 비정형 데이터 분석 요구 증가
대용량 실시간(velocity) 데이터 증가	- 동영상, 실시간 스트리밍 데이터 폭증에 따른 비정형 전용 데이터 분석 필요
다양한(variety) 비정형 유형 증가	- IoT, 음성인식, 상황인식 등 지능형 서비스 증가에 따른 다양한 비정형 데이터 분석 요구 증가

- 다양한 자연어 처리를 위해서는 음성데이터를 이용한 마이닝을 통한 학습 필요

II. 음성데이터 마이닝의 주요 기술

가. 음성인식(Speech To Text) 측면의 주요 기술

구분	항목	설 명
요소 기술	EPD (End-Point Detection)	음성신호만의 고유한 특성을 처리하기 위해서, 발화 음성의 시작과 끝을 자동으로 검출하는 끝점검출 기술
	전처리 기술	음성신호의 주파수 특성을 잡음환경에서도 뚜렷하게 분석 추출하는 기술
	후처리 기술	숫자나 영문, 문장부호를 복원하는 기술
인식 모델	음향모델	화자의 음성이 어떤 소리인지 분별 능력을 학습하는 모델
	발음사전	단어의 다양한 발음패턴을 기억하는 사전
	언어모델	단어 간의 관계 또는 문법을 학습하는 모델

나. 비정형데이터인 음성데이터의 텍스트 마이닝(Text Mining) 주요 기술

주요 기술	설명
데이터 수집	- 뉴스/동영상 공유 플랫폼/콜센테 음성녹취파일/블로그 등 음성 데이터 수집
데이터 전처리	- 컴퓨터 이해하기 쉽게 텍스트를 변환하는 과정 (오탈자 제거, 불용어 제거, 정제, 정규화)
토큰화	- 단어 단위로 나누는 과정으로 형태소 분석기 사용 (주어진 말뭉치에서 토큰이라는 단위로 나누는 작업)
특징값 추출	- 중요한 단어를 선별하는 과정
데이터 분석	- 데이터 마이닝, 머신러닝, 딥러닝 등 분석 모델 이용 (회귀분석, 랜덤포레스트, 선형분석, XGBoost, RNN, GRU 등)

III. 음성데이터 마이닝의 활용 가능 분야

분야	설명
범죄 예방	- 음성데이터를 이용하여 보안과 안전 강화를 목적으로 사람들을 감시
콘텐츠 분석	- 콘텐츠 내 음성데이터를 이용하여 분류
건강 모니터링	- 병원에 있는 환자의 건강 상태를 감지, 유아의 호흡 문제 감지
인구 통계 정보	- 성별, 나이, 감정과 감정, 언어 등을 포함하여 분류
고객의 의견	- 제품 및 서비스에 대한 고객의 정확하고 정확한 의미를 해석하는 데 도움

IV. 음성데이터 마이닝의 발전 방향

구분	항목	설 명
기술동향	종단형 음성인식	트랜스포머 기반 종단형 음성인식은 현재 SOTA 성능을 내는 최적 모델로 대부분 음성인식 시스템의 기반
	비지도 학습	- 종단형 음성인식의 경우, 학습에 소요되는 데이터가 기존 대비 몇 곱절 이상 필요함에 따라 데이터 증강(Data Augmentation), 자기 지도학습(Self-supervised) 기반 비지도 학습 등 새로운 방법론 도입 필요 - BERT 와 유사한 비지도 학습 방식인 Wav2Vec, HuBERT 방식 등 제안
	다국어 음성인식	- 자연어 음성인식 기술의 국제경쟁력 확보의 일환으로 주요 언어 외 주변국으로의 다국어 확장이 필요하며 이 경우 low resource 문제 발생 - 동남아어, 동유럽어, 아랍어권 등 주변국 언어의 경우, 현실적으로 대량의 데이터 확보가 매우 어려움.
국내외 산업계 현황	인공지능 스피커 대중화	구글, 애플, 마이크로소프트, 아마존 등 글로벌 기업의 인공지능 스피커를 경쟁적으로 출시 및 자사 플랫폼 기반 생태계 구축으로 대중화 추진
	개발플랫폼 지원 및 생태계 구축	B2B 차원의 인공지능 스피커 생태계 확장을 위한 개발플랫폼 지원
	가정 내 AI 허브 전략	인공지능 비서(스피커, 스마트 TV)를 가정내 모든 가전 기기를 연동할 수 있는 AI 허브로 만들려는 가전업체, 포털업체, 통신업체간 주도권 싸움이 치열

"끝"

02	디지털 포렌식		
문제	최근 많은 범죄들이 지능화, 고도화되면서 디지털 포렌식의 중요성이 증가하고 있다. 이러한 디지털 포렌식과 관련하여 아래 사항을 설명하시오. 1) 디지털 포렌식의 개념 2) 디지털 포렌식의 유형과 절차 3) 디지털 포렌식 기술 및 활용분야		
도메인	보안	난이도	하 (상/중/하)
키워드	정당성의 원칙, 재현의 원칙, 신속성의 원칙, 연계 보관성의 원칙, 무결성의 원칙 수사 준비, 증거 수집, 보관/이송, 증거 분석, 보고서 및 증거 제출		
출제배경	보안의 기본인 디지털 포렌식에 대한 기본 개념과 기반 기술들에 대한 인지 확인		
참고문헌	IT기술사회 자료		
출제자	단합반 안경환 기술사(제 110회 정보관리기술사 / akh.itpe@gmail.com)		

I. 사이버 공간에서의 범죄 증거 확보 기법, 디지털 포렌식의 개념

개념	- 컴퓨터를 이용하거나 활용해 이뤄지는 범죄 행위에 대한 법적 증거 자료 확보를 위해 컴퓨터 시스템, 네트워크 등 디지털 자료가 법적 증거물로 법원에 제출될 수 있도록 확보하는 일련의 절차와 방법
기본 원칙	**내용**
정당성의 원칙	- 증거가 적법 절차에 의해 수집되었는가? → 위법 수집 증거 배제 법칙. - 위법하게 수집된 증거에서 얻어진 2차 증거도 증거 능력이 없음 → 독수 독과(과실) 이론.
재현의 원칙	- 같은 조건과 상황하에서 항상 같은 결과가 나오는가? - 불법 해킹 용의자의 해킹 툴이 증거 능력을 가지기 위해서는 같은 상황의 피해 시스템에 툴을 적용할 경우 피해 결과와 일치하는 결과가 나와야 함.
신속성의 원칙	- 컴퓨터 포렌식의 전 과정이 신속하게 진행되었는가? - 휘발성 데이터의 특성 상 수사 진행의 신속성에 따라 증거 수집 가능 여부가 달라짐.
연계 보관성의 원칙 Chain of Custody	- 증거물의 수집, 이동, 보관, 분석, 법정 제출의 각 단계에서 담당자 및 책임자가 명확해야 함. - 수집된 저장 매체가 이동 단계에서 물리적 손상이 발생하였다면, 이동 담당자는 이를 확인하고 해당 내용을 정확히 인수 인계하여 이후의 단계에서 적절한 조치가 취해지도록 해야 함.
무결성의 원칙	- 수집된 증거가 위변조 되지 않았음을 증명. - 일반적으로 해쉬 값을 이용하여 수집 당시 저장 매체의 해쉬 값과 법정 제출 시 저장 매체의 해쉬 값을 비교하여 무결성 입증.

I. 디지털 포렌식의 유형과 절차

가. 디지털 포렌식의 유형

분류	구분	내용
분석 목적에 따른 분류	사고 대응 포렌식	* 침해 사고에 대응하여 범죄자 파악이 목적. * 해킹 등 침해 시스템의 로그, 백도어, 루트킷 등을 조사하여 침입자의 신원, 피해 내용, 침입 경로 등을 파악. * 네트워크 기술, 서버 로그 분석 기술, 유닉스/리눅스/윈도우 서버 등 운영 체제 기술 필요.
	정보 추출 포렌식	* 범행 입증에 필요한 증거물 획득이 목적. * 디지털 저장 매체에 기록되어 있는 데이터를 복구하거나 검색 하여 증거물 획득.
분석 대상에 따른 분류	디스크 (데이터 포렌식)	* 디스크의 증거(데이터) 식별 및 복구. * 각종 보조 기억 장치에서 삭제된 파일 복구, 증거 분석, 증거 훼손 방지를 위한 쓰기 방지 등 사후 조치. * 디렉터리 구조, 키워드 검색, MAC Time 및 시계열 분석 등의 기법 사용.
	시스템 포렌식	* 운영 체제, 응용 프로그램 및 프로세스 분석하여 증거를 확보.
	네트워크 포렌식	* 네트워크를 통한 데이터 및 로그 분석. * 방화벽 로그, 웹 프록시 캐시, ARP 테이블 * 스니핑된 트래픽 로깅 파일, IP 발신자 추적, 라우터 로그 분석 등을 통하여 증거 확보.
	인터넷 포렌식	* 인터넷(웹 등) 통신 히스토리 분석. * 웹 히스토리 분석, 전자 우편 헤더 분석, IP 추적 기술 이용.
	모바일 포렌식	* 휴대용 기기에서 필요한 정보를 입수하여 분석. * 휴대용 기기의 은닉 용이성으로 세심한 분석 필요.
	암호 포렌식	* 문서나 시스템에서 암호를 추출 * 증거 수집에서 비인가 접근을 막기 위해 문서나 시스템에 암호를 설정한 경우 암호 분석 필요.
	회계 포렌식	* 저장된 회계 데이터를 추출하고 회계 전문가가 분석할 수 있도록 데이터를 정제. * 기업의 부정과 관련된 수사 시 필요.
	이메일 포렌식	* 전자 메일, 메신저 등에서 증거 자료 확보, 분석. * 발신자 추적, 메일 검색, 삭제된 메일 복구 등의 기술 활용.
	소스 코드 포렌식	* 프로그램 소스 코드 유형을 보고 작성자를 구분(필적 감정과 유사한 형태). * 프로그램 개발 흔적을 조사하여 원시 코드와 실행 프로그램과의 상관 관계를 분석.
	데이터베이스 포렌식	* 데이터베이스에서 데이터 추출 및 분석. * 압수 수색이 현실적으로 어려운 대형 시스템에서 디지털 증거물 획

		득 및 분석. * 증거 획득 과정에서 관계자 입회 및 작업 과정 결과 파일에 대한 해쉬 값 계산, 문서화 후 서명 절차 등이 필요.
	멀티미디어 포렌식	* 디지털 형태의 그림, 음악, 비디오 파일에 관련된 저작권, 자료의 위변조 여부 분석 및 데이터 은닉 기술(Steganography) 등이 해당됨.

나. 디지털 포렌식의 절차

단계	설명	고려 사항
수사 준비	* 전문 인력과 포렌식 도구의 활용 방안 수립 * 보관의 연속성 방안 수립. * 데이터의 무결성 유지 방안 수립. * 수사 참조 라이브러리 준비: 잘 알려진 파일에 대해 쉽게 식별.	* 전 과정에 대한 기록 준비 * 하드디스크 복사 도구. * 자료 검사 도구. * 자료 무결성 도구. * 시스템 분석용 도구. * 암호용 도구.
증거 수집	* 증거 수집 및 수집 시간/과정 기록. * 디스크 이미징, 복제, 해싱(Hashing) 기법 활용. * 자료 삭제/파괴 행위 방지, 시스템 목록 작성, 하드디스크 이미징. * 시스템/네트워크/프로세스 상태 수집, 증거물 무결성 확보.	* 휘발성 증거 우선 수집 * 전원 차단 여부 결정 * 증거 수집 대상에 따른 대응(복제/원본/출력 등).
보관/ 이송	* 증거의 훼손, 변경, 유출 방지. * 라벨링 부착하여 이력 관리. * 증거 자료 이중화, 쓰기 방지/봉인, 증거물 담당자 목록 기록 관리. * 정전기 방지용 팩, 하드 케이스 등 안전한 포장, 접근 통제.	* 증거물의 이력 관리(Chain of Custody)
증거 분석	* 수집된 데이터 복구 및 증거 분석. * 암호 해제, 삭제 파일 복구, 고급 검색, 이메일 분석, 웹 히스토리 분석 기법 활용.	* 증거 무결성. * Slack Space 등 고려. * Time Line.

보고서 및 증거 제출	* 분석 과정 및 결과에 대한 보고서 작성. * 증거물과 보고서를 법정에 증거로 제출. * 6하 원칙에 따른 객관성 유지.	* 누구나 쉽게 이해할 수 있도록 쉽고 상세한 설명.

III. 디지털 포렌식 기술 및 활용분야

가. 디지털 포렌식 기술

구분	증거 복구	수집 및 보관	증거 분석
저장 매체	- 하드디스크 복구 - 메모리 복구	- 하드디스크 복제 기술 - 메모리 기반 복제 기술 저장 매체 복제 장비	- 저장 매체 사용 흔적 분석 - 메모리 정보 분석
시스템	- 삭제 파일 복구 - 파일시스템 복구 - 로그온 우회 기법	- 휘발성 데이터 수집 - 시스템 초기 대응 - 포렌식 라이브 CD/USB	- 윈도우 레지스트리 분석 - 시스템 로그 분석 - 프리 패치 분석
데이터 처리	- 언어 통계 기반 복구 - 암호해독/DB 구축 - 스테가노그래피 파일 조각 분석	- 디지털 저장 데이터 추출 - 디지털 증거 보존 - 디지털 증거 공증/인증	- 데이터 포맷 별 분석 - 영상 정보 분석 - 데이터베이스 정보 분석 - 데이터 마이닝
응용/네트워크	- 파일 포맷 기반 복구 - 암호통신 내용 해독	- 네트워크 정보 수집 - 네트워크 역추적	- 네트워크 로그 분석 - 해시 데이터베이스
기타 기술	- 개인 정보보호 기술, 범죄 유형 프로파일링 연구, 통합 타임라인 분석		

- 최근 IT기술이 발전함에 따라 디지털 데이터 형태의 대용량 정보를 이용한 디지털 범죄가 날로 증가 추세

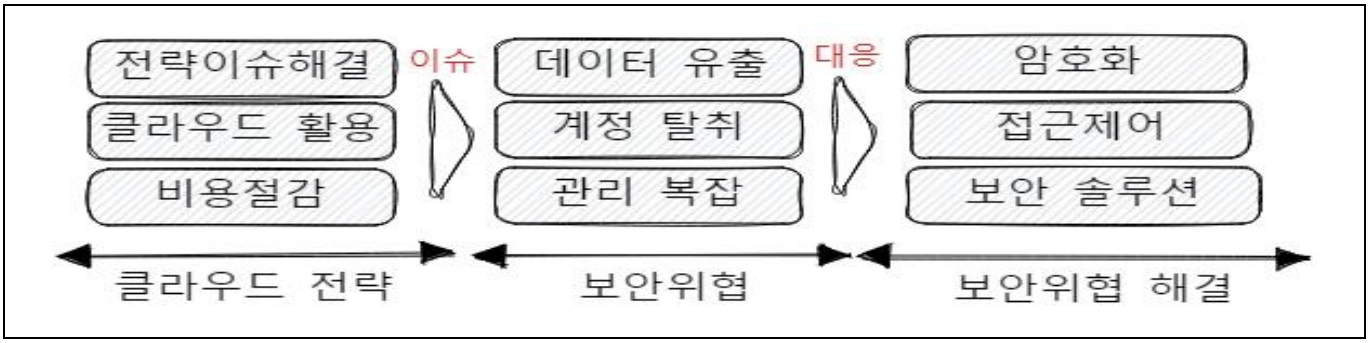
나. 디지털 포렌식 활용분야

활용 분야	설명
전자증거개시제도(E-Discovery)	- 정식 재판이 진행되기 전 소송 당사자 간 공소 제기된 사건과 관련된 정보를 서로의 요청에 의해 공개하는 제대로 재판 없이 합의를 이끌어내는 효과로 시간 낭비를 줄이고, 쟁점을 명확화
침해사고 대응	- 외부 해킹 공격 및 악성코드 유입 등에 따른 침해 사고 조사
내부 감사	- 퇴사자, 협력 업체 인원 등에 대한 감사, 내부 정보 유출 조사 등
포렌식 회계 감사	- 기업의 분식회계 조사, 재무 조작 검사, 상장사에 대한 재감사
민사 소송 대응	- 소비자에 의한 소송 대응, 기업 간 소송 대응

"끝"

03	클라우드 보안		
문제	최근 다수의 기업들이 클라우드 서비스를 도입하면서 다양한 보안 문제가 대두되고 있다. IT 담당자 입장에서 클라우드 서비스 도입 시 고려해야 할 보안 요소를 설명하시오.		
도메인	보안	난이도	중 (상/중/하)
키워드	클라우드 데이터 유출, 계정 탈취, 중간자 공격, 악성코드 유입		
출제배경	기업의 클라우드 도입 활성화에 따른 보안 문제 출제		
참고문헌	IT기술사회 자료		
출제자	TOP반 김민 기술사(제 120회 정보관리기술사 / itpe.min@naver.com)		

I. 클라우드 서비스의 보안 문제 개요



- 기업의 다양한 전략적 이슈 해결을 위해 클라우드 도입이 증가함에 따라 보안면적 확대로다양한 보안위협 요소들이 발생, 효과적인 대응을 위해서 영역별 및 통합적인 보안위협 대응에 대한 방안 필요

II. IT 담당자 입장에서 클라우드 서비스 도입 시 고려해야 할 보안 요소

구분	보안위협요소	설명
데이터	데이터 유출	- 하이브리드/멀티 클라우드 환경 데이터 이동 자주 발생 - 데이터 유출 위험이 증가 - 랜섬웨어, Ransomware-as-a-Service(RaaS)
	데이터 손실	- 하드웨어 결함 및 운영상 실수 인해 데이터 손실 - 인력 부족, 미숙한 데이터 백업
인증/인가	잘못된 권한 부여	- 복잡한 환경의 권한 관리 어려움 - 민감한 데이터 무단 접근 발생 - 과도한 권한 부여, 잘못 구성된 IAM 정책
	계정 탈취	- 약한 인증 절차나 공격자에 의해 계정 탈취 - 사회 공학, 피싱 공격
네트워크	중간자 공격	- 클라우드 서비스 간의 연결 시 중간자 공격 - ARP 스푸핑, SSL 스트립 공격
	분산 서비스 거부 공격 (DDoS)	- 클라우드 인프라에 대한 분산 서비스 거부 공격 - SYN 플러드, DNS 포이즈닝 공격
시스템	취약점 공격	- ISP의 시스템 및 기술에 대한 약점 공격

		- SQL 인젝션, 크로스 사이트 스크립팅(XSS)
	악성 코드 유입	- 클라우드 환경에 악성 코드 유입 및 시스템 손상, 데이터 침해 - 트로이 목마, 웜

III. IT 담당자 입장에서 클라우드 서비스 도입 시 고려해야 할 보안 대응방안

구분	해결방안	설명
데이터	데이터 암호화	- 데이터 저장, 전송 모든 과정 암호화 적용 - 정보 유출 위험 최소화 - AES, RSA, PKI, S/MIME, DH, DES
	데이터 백업 및 복구	- 데이터 손실 방지위해 정기적 백업, 필요 시 신속 복구 시스템 구축 - 스냅샷, 지역 간 복제, DB Replication, DRS, Storage
인증/인가	역할 기반 접근 제어 (RBAC)	- 역할 기반 접근 제어 도입 - 사용자 역할 기반 최소 권한 부여 - 무단 접근 방지 - AWS IAM, Azure AD, LDAP, Oauth2.0, SAML, OIDC
	다중 인증(MFA)	- 다중 인증 절차 도입 - 사용자 인증 과정 강화 - 계정 탈취 방지 - OTP 인증, 생체 인증, DID
네트워크	통신 경로 암호화	- 통신 암호화 - 중간자 공격 방지 - SSL/TLS, IPSec VPN
	DDoS 대응 솔루션	- 분산 서비스 거부 공격 방어위해 DDoS 공격 대응 솔루션 도입 - AWS Shield, Cloudflare, 사이버대피소
시스템	정기적 패치 및 업데이트	- 하이브리드/멀티 클라우드 시스템의 소프트웨어 및 하드웨어의 정기적 패치/업데이트 - 알려진 취약점 해결 - 보안 업데이트 자동화, 취약점 스캐너
	악성코드 방지 및 탐지	- 악성 코드 방지 및 탐지 솔루션 도입 - 클라우드 환경 악성 코드 위험 관리 - 침입탐지 시스템(IDS), 침입방지 시스템(IPS), 백신 소프트웨어
클라우드 보안	CASB	- 보안 중개 솔루션 - 클라우드 서비스 접근 통제, 데이터 보호, 위협 탐지와 대응
	ZTNA	- 클라우드 서비스 접근 시점부터 Zero Trust 기반 보안 정책 적용 - 통제 및 보안 강화 솔루션
	CSPM	- 클라우드 환경의 위협과 취약점 탐지 및 대응 솔루션 - 클라우드 보안 설정, 계정 권한 관리, 네트워크 보안, 데이터 보호 등 다양한 보안 요소 관리

보안 운영 및 관리	SIEM	- 로그 및 이벤트 수집, 분석, 보안이슈 탐지/대응 솔루션
	EDR	- 엔드 포인트 보안 이슈 탐지/대응 솔루션 - 위협 탐지, 탐지 결과 분석, 대응 기능 등 제공
	SOAR	- 보안 이벤트에 대한 자동화된 대응 및 조치 프로세스 구축/관리 솔루션
	SASE	- 클라우드 기반 네트워크 보안 솔루션 - Zero Trust 기반 접근 통제, 데이터 보호, 위협 탐지와 대응 등의 기능 제공
	SD-WAN	- 소프트웨어 기반 WAN 기술 - 여러 위치의 지사와 데이터 센터를 연결하는 네트워크 관리 - WAN 대역폭 확장, QoS(Quality of Service) 제어, VPN 등 다양한 기능 제공

"끝"

04	요구사항		
문제	IT프로젝트를 성공적으로 수행하기 위해 요구사항이 체계적인 관리와 문서화가 매우 중요하다. 요구사항에 대하여 다음을 설명하시오. 1) 소프트웨어(SW) 요구사항 품질속성 2) 요구사항 도출기법 3) 요구사항 개발 프로세스		
도메인	SW공학	난이도	중 (상/중/하)
키워드	완전성, 정확성, 인터뷰, 워크샵, 브레인스토밍, 추출, 분석, 명세, 검증		
출제배경	소프트웨어 품질 고도화를 위한 요구사항 관리체계 지식 점검		
참고문헌	IT기술사회 자료		
출제자	TOP반 김민 기술사(제 120회 정보관리기술사 / itpe.min@naver.com)		

I. 소프트웨어(SW) 요구사항 품질속성

완전성	- 소프트웨어 누락된 요구사항의 존재 여부
정확성	- 소프트웨어 요구사항을 논리적으로 정확하게 기술하였는지 여부
명확성	- 이해관계자가 명확하게 이해할 수 있도록 기술되었는지 여부
일관성	- 요구사항들 간의 연관 및 종속 관계의 불일치 존재 여부
특이성	- 중요도, 난이도, 변경 가능성을 표기하였는지 여부
검증 가능성	- 요구사항에 대한 검증 기준 및 방법을 제시하였는지 여부
수정 용이성	- 요구사항 항목의 식별, 수정, 영향도 분석이 용이한지 여부
추적성	- 관련된 산출물에서 요구사항을 추적할 수 있는지 여부
이해 가능성	- 요구사항을 표준 형식에 따라 기술하고 이해 가능한지 여부

II. 요구사항 도출기법

기법	설명	세부 기법
인터뷰	- 직접(대면) 대화를 통해 요구사항 도출	Close / Open 인터뷰
설문지	- 많은 인원으로부터 통계적 분석기법을 통해 요구사항 도출	사전 질문, 설문
브레인스토밍	- 자유롭게 생각을 도출하고 참여자들의 아이디어를 합병하여 새로운 아이디어 생성	Group Session Video conferencing
관찰	- 고객의 업무 작업 수행과정을 관찰하여 도출	관찰/질문, 비디오 촬영
위크샵	- 일정 주제에 대한 토론을 통하여 결론 도출	소그룹 집합 교육
유즈케이스	- 시스템 기능에 대한 명확하고 일관성 있게 표현	유즈케이스 다이어그램
프로토타이핑	- 일부 시스템의 기능에 대한 시연을 통해 고객의 피드백 또는 요구사항을 도출	데모, 시뮬레이션

- 요구사항 도출 시에는 다양한 고객, 마케팅, 개발자 등 이해관계자를 대상으로 구체적으로 요구사항 도출이 필요함

III. 요구사항 개발 프로세스

구성요소	대상	산출물/기법
요구사항 추출	- 요구사항 도출 대상 선정 - 제안서, 사업수행 계획서, 인터뷰, 프로토타이핑	- 인터뷰, 브레인스토밍 - 스토리보드, BPR
요구사항 분석	- 도출된 기능을 명확히 파악. - 정보공학 분석법, UML	- UML, ERD - 시나리오
요구사항 명세	- 시스템의 행동을 기술. 요구사항 명세서	- SRS - TTA 명세서 템플릿
요구사항 검증	- 요구사항과 요구사항 명세의 일치 확인 및 승인 - 타당성 검증, 일치성, 완전성, 현실성, 프로토타이핑	- 요구사항 문서 - V&V, 리뷰, 인스펙션

- 요구사항 프로세스는 요구사항 개발과 관리로 나누어 수행됨

IV. 요구사항 명세의 주요 평가기준

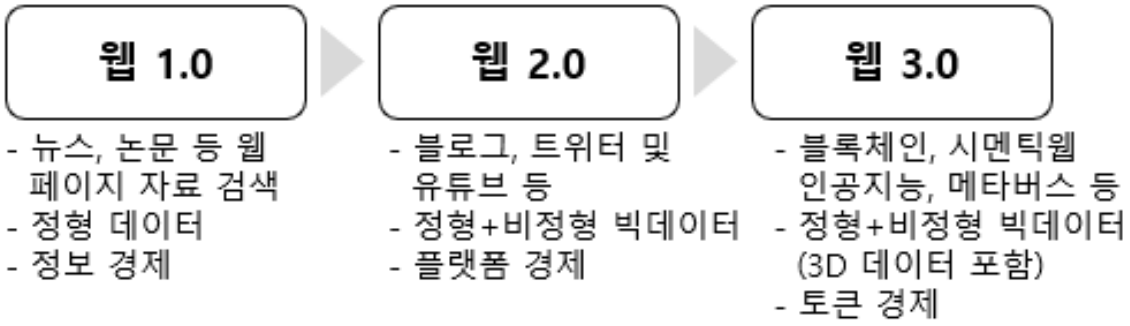
평가기준	설명
정확성	- 고객의 요구와 명시된 요구사항이 정확한지 확인이 필요
명확성	- 요구사항 명세 내용은 하나의 요구사항에 대한 의미만 포함하고 있는지 확인
일관성	- 명세 내용 간의 상호 모순이 없는지 확인
검토/수정/추적 가능성	- 요구사항 충족여부, 변경 용이성, 추적(순방향/역방향) 상호 참고 가능한지 확인이 필요

- 요구사항 명세의 다양한 평가기준을 기반으로 명확한 요구사항 도출 가능

"끝"

05	웹3.0		
문제	웹3.0에 대하여 다음을 설명하시오. 1) 웹3.0의 도입배경 및 개념 2) 웹3.0의 주요특징 및 기술요소 3) 웹3.0 기반의 서비스 활용 방안		
도메인	서비스	난이도	중 (상/중/하)
키워드	탈중앙화, 보안, 블록체인, AI/ML		
출제배경	블록체인, 시멘틱웹 발전에 따른 웹3.0 출제		
참고문헌	IT기술사회 자료 https://www.igloo.co.kr/security-information/web-3-0-시대를-위한-활성화-방안-및-도입-시-고려사항/		
출제자	NS반 김민재 기술사(제 124회 정보관리기술사 / kmj_pe@naver.com)		

I. 웹 3.0의 도입배경 및 개념



도입배경	- 비트코인, 이더리움 등의 가상자산과 NFT, 블록체인 게임 및 메타버스에 대한 인식이 확산되면서 가상자산이 모든 분야를 아우르는 새로운 인터넷 기반 "웹 3.0"이 급부상하고 있음.
개념	- 시맨틱 웹 기술을 이용하여 웹페이지에 담긴 내용을 이해하고 개인 맞춤형 정보를 제공하고, 인공지능, 빅데이터, 클라우드와 함께 탈중앙화된 블록체인 생태계와 결합하여 구현된 웹 기술

II. 웹 3.0의 주요특징과 기술요소

가. 웹 3.0의 주요특징

주요특징	설명	기술
컨텐츠의 소유권	- 웹에서 생산되고 소비되는 다양한 컨텐츠에 대해 본인이 소유(데이터를 사용자가 소유)	- NFT
창작자 중심의 플랫폼	- 데이터를 제공한 사용자가 정당한 보상을 받음(사용자가 수익 창출)	- NFT, DApp, P2E
탈중앙화 (중앙 의존성 탈피)	- 중앙 통제 기관(중개자) 없는 거래환경 제공 - 자율적·민주적 운영 규칙 결정	- 블록체인 - DAO

높은 보안성 (데이터 안정성)	- 중앙 서버가 필요 없는 데이터 분산 저장 - 프로토콜 기반 무보증·무허가 참여	- 블록체인
지능화 서비스	- 사용자에게 맞춤화 된 지능형 서비스 제공	- AI
확장된 미디어 인터페이스	- 현실세계와 가상세계가 융합된 공간 제공	- 메타버스

- 블록체인, NFT, AI, 메타버스 등의 기술을 활용하여 웹3.0 진화 진행중

나. 웹 3.0의 기술요소

구분	기술요소	설명
기반 기술	블록체인	- 분산데이터베이스의 한 형태로 분산 노드의 특정 사용자에 의한 임의 조작이 불가능하도록 고안되어 지속적으로 성장하는 데이터기록 리스트블록(block)을 잇따라 연결한 모음
	Semantic Web	- 인간이 사용하는 정보 체계를 기계가 인식하고 기계와 인간이 같이 웹 정보를 동일하게 인식하게 하기 위한 기술 표준
	AI/ML	- 상황에 따른 시맨틱 검색엔진 활성화와 사용자 맞춤 서비스, 여러 유형의 장비간 연결되어 실행
	NFT	- 블록 체인에 저장된 데이터 단위로 고유하면서 하나의 토큰을 다른 토큰으로 대체하는 것이 불가능한 토큰
	클라우드	- 많은 사람이 언제 어디서나 접근가능한 환경 제공
	5G/6G	- 초고속 인터넷 연결로 메타버스 이용 확산
	DApp	- 블록체인 기술 기반 탈중앙화 분산 어플리케이션
서비스 기술	AR/VR/XR	- 가상현실(VR)과 증강현실(AR)을 모두 구현하는 메타버스의 기본기술로 현실감 있는 영상 구현
	메타버스	- 가상세계가 전산업으로 확대 적용됨에 따라 비 대면 온라인 공간에서 실감나는 체험 제공
	HMD	- 360도 전면녹화, 상황인식, 주변정보에 대한 입력과 해석을 통해 판단하여 정보를 제공
	디지털 휴먼	- 가상공간에 실제 사람과 같은 움직임의 재현
	텔레햅틱	- 가상공간에 몰입감을 더하는 초감각 제공

- 'Web 3.0'에서는 탈중앙화 이외에도 인공지능, 블록체인, 메타버스, NFT 등의 기술이 활용되면서 보다 다양한 서비스와 생태계를 구축. 이와 같은 생태계의 변화는 △블록체인 기반의 탈중앙화, △ 사용자 중심의 데이터 활용 및 서비스 운영, △ 탈중앙화로 인한 데이터 유출 등 보안 이슈 감소 등의 효과를 가져옴.

III. 웹 3.0 기반의 서비스 활용 방안

가. 기술적, 산업적 측면의 활용 방안

구분	활용 방안
기술적 측면	- 차세대 폼팩터(Form Factor) 및 프레임 워크 기술 개발 - 가상 자산 활성화를 위한 응용 기술 개발

		- 블록체인 기반 데이터 분산 저장 기술 개발 - 만물 인터넷(Internet of Everything, IoE) 시대를 위한 5G, 6G 개발 및 상용화
보안기술 측면	인프라 및 네트워크	- DevSecOps를 통한 웹 3.0 플랫폼 개발 및 운영 - 분산 데이터 환경 보안을 위한 보안 액세스 서비스 에지(Secure Access Service Edge, SASE), 제로 트러스트 네트워크 액세스(ZTNA) 등의 네트워크 솔루션 도입 - 웹 3.0 플랫폼 오픈소스 보안 이슈 최소화를 위한 보안 테스트 강화
	개인정보 및 데이터	- 동형암호, 프라이버시 강화 기술(Privacy Enhancing Technology, PET) 이용한 데이터 보호 - 가상 자산 거래 및 개인정보보호를 위한 FIDO, DID 등의 차세대 인증기술 개발 - 어플리케이션 데이터 위변조 방지를 위한 Anti-Tempering 기술 적용
산업 측면	메타버스	- 실 세계에서 발생하는 유통, 금융, 교육 뿐만 아니라 정서적 유대관계를 디지털 기술을 사용하여 구현 - 증강현실, 라이프 로깅, 미러 월드, 버추얼 월드
	NFT	- 메타버스에서 실세계의 실물경제와 유사한 경제구조를 구성하기 위해서 블록체인 기술을 기반으로 구성 - 플랫폼을 구성하고 있는 데이터 및 서비스 등 컨텐츠의 소유권과 희소성을 부여함으로써 메타버스 생태계를 유지하도록 지원 - ERC-721 기반의 '스마트 계약(Smart Contract)'기술을 이용해 디지털 자산에 고유 아이디와 메타데이터 정보를 할당해 파일의 진위여부 및 소유권을 증명 - 소스코드에서 토큰 ID(Token-ID)와 소유자(Owner)를 토큰의 발행부터 토큰의 소멸까지 모든 거래단계에 적용하여 소유권과 대체불가능을 구현

- 기술, 산업적 준비 뿐만 아니라 법·제도적, 정부 측면에서도 준비 필요

나. 법, 제도적 및 정부 측면의 활용 방안

구분	활용 방안
법·제도적 측면	- 웹 3.0 플랫폼 및 기술 개발을 위한 MPEG-v, IEEE 2888 등의 표준 확립 - 웹 3.0 플랫폼 활성화를 위한 가이드 라인 마련 - 개인정보보호를 위한 마이데이터, 데이터 3법 등 법률 개선 - 가상세계에서의 디지털 성범죄 처벌 관련 법안 개선 - 가상 자산(암호화폐, NFT) 관련 법안 마련 및 개선
정부 측면	- 웹 3.0 주요 플랫폼 활성화를 위한 인력 양성 및 육성 - 웹 3.0 산업 육성을 위한 국내·외 시장 현황 모니터링 - 웹 3.0의 글로벌 기술선도를 위한 정책마련 및 예산지원 강화 - 가상 자산의 생성, 유통, 거래 등 프로세스 지원

- 웹3.0 기반 서비스 활성화를 위해서는 기술, 산업, 법·제도, 정부 등 다양한 부분에서 체계적이고 다각화된 준비가 필요

"끝"

06	데이터옵스, 데브옵스		
문제	데이터옵스(DataOps)와 데브옵스(DevOps)에 대하여 다음을 설명하시오. 1) 데이터옵스와 데브옵스의 비교 2) 데이터옵스 아키텍처 및 주요 기술		
도메인	서비스	난이도	중 (상/중/하)
키워드	CI/CD, Code, Deploy, Build, Test		
출제배경	기술과 운영의 합성 개념 출제		
참고문헌	IT기술사회 자료		
출제자	NS반 김민재 기술사(제 124회 정보관리기술사 / kmj_pe@naver.com)		

I. 자동화 프로세스를 지원하기 위한 x옵스 개요

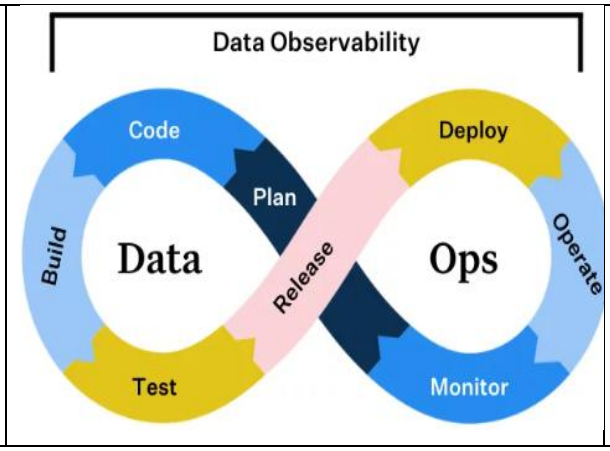
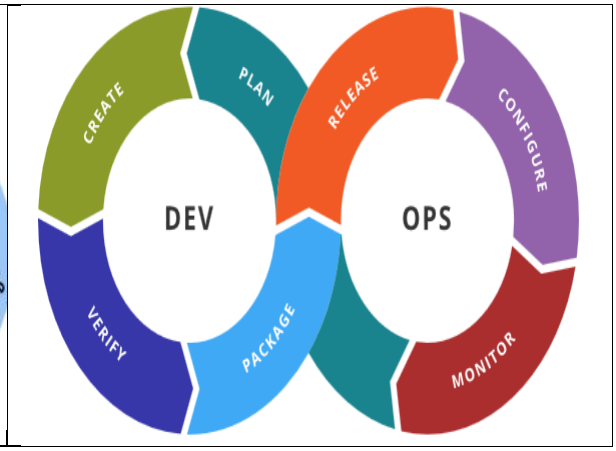
정의	- 자동화를 지원하고 기술 및 프로세서의 중복을 줄이는 엔터프라이즈 기술 스택을 구축을 목표로 실행하는 방법론

- x옵스중 데이터 관리와 소트프웨어 개발에 적용하여 DataOps와 DevOps 활용 증가

II. 데이터옵스(DataOps)와 데브옵스(DevOps) 비교

가. 데이터옵스와 데브옵스의 개념 비교

구분	데이터옵스 (DataOps)	데브옵스 (DevOps)
개념	- 조직 전체의 데이터 관리자와 데이터 소비자 간의 데이터 흐름의 커뮤니케이션, 통합 및 자동화를 개선하는 데 중점을 둔 협업 데이터 관리 방식 - 데이터를 분석해 애플리케이션을 형성한 후 최종 사용자에게 신뢰할 수 있는 고품질 데이터를 신속히 제공하기 위한 기본적인 데이터 운영/관리 방식	- 시스템 개발자와 운영을 담당하는 정보기술 전문가 사이의 소통, 협업, 통합 및 자동화를 강조하는 소프트웨어 개발론 - 소프트웨어 제품이나 서비스를 알맞은 시기에 출시하기 위해서 개발과 운영이 상호의존 대응 - 개발과 운영의 합성어 - 개발과 운영의 원활한 상호 작용을 하게 하는 모든 개발 방법론

프레임워크	 

- 파이프라인 활용한 자동화로 효율적인 프로세스 운영 가능

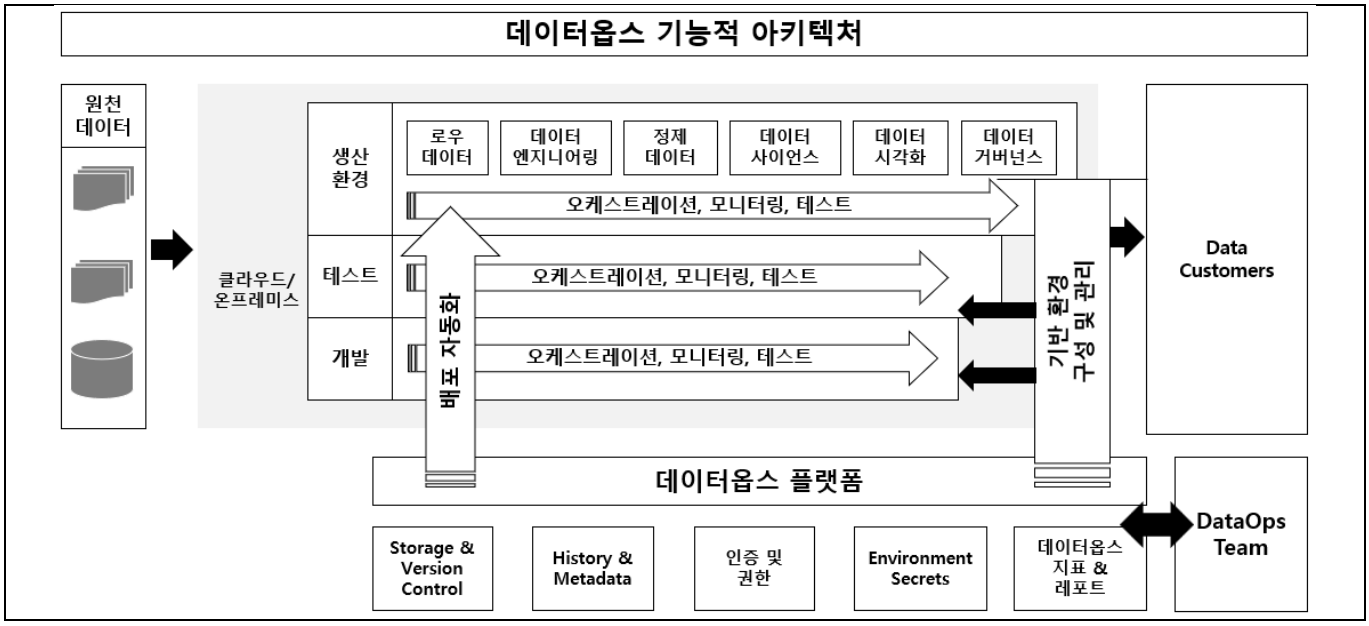
나. 데이터옵스와 데브옵스의 상세 비교

구분	데이터옵스	데브옵스
목적	- 데이터 파이프라인 자동화/모니터링 관리	- SW 개발 자동화 및 모니터링
조합	- 데이터 공학, 데이터 통합,	- SW 개발, 품질보증(QA), 기술운영
협력	- 데이터 품질, 데이터 보안, 개인정보	- SW 엔지니어(개발자),
기대효과	- 데이터 엔지니어, 데이터 과학자,	- 시스템관리자(운영 팀), 테스트

- 데이터옵스를 적용하기 위해서는 기술환경과 분석 전문가, 데이터 엔지니어 등의 역량 확보 필요

III. 데이터옵스 기능 아키텍처 및 주요기술

가. 데이터옵스 기능 아키텍처



- 데이터를 생산·수집·가공·분석하는 체계인 데이터 플랫폼를 통해 신속한 배포 및 부가가치가 높은 고품질의 가치를 창출할 수 있도록 지원하는 여러 가지 기능(스토리지·리비전 제어, 인증 및 권한 관리, 이력 및 메타데이터 등)이 통합

나. 데이터옵스의 접근방식 및 주요 기술

구분	접근방식 및 기술	설명
접근방식	데브옵스	- 지속적 통합/제공과 테스트 중심의 개발
	애자일 방식	- 단기 작업 수행이 가능한 자체 조직화된 팀 중심
	린 제조	- 비효율을 파악하여 프로세스를 단순화·자동화
주요기술	**스토리지/리비전 제어**	- 버전 제어는 인위적인 변경 사항을 관리. 거버넌스 및 반복 개발에 필수 (예, git, dockerhub)
	이력 및 메타 데이터	- 시스템 및 활동 로그 관리 (예, MongoDB)
	인증 및 권한	- 환경에 대한 액세스 제어 (예, Auth0)
	환경 비밀	- 환경 내 도구 및 리소스에 대한 역할 기반 액세스 (예, Vault)
	데이터옵스 지표 및 보고서	- 분석 및 데이터 팀의 상태에 평가에 대한 내부 분석 : CDO 대시보드 (예, Tableau)
	자동 배포	- 하나의 환경에서 프로덕션 환경으로 코드/구성을 이동하는 과정 (예, Jenkins, CircleCI)
	환경 생성 및 관리	- 하드웨어, 소프트웨어, 테스트 데이터 세트 등 필요한 모든 것을 가지고 작업할 수 있는 환경을 생성할 수 있는 코드와 같은 인프라 취급 (예, Chef, Puppet)
	오케스트레이션, 테스트, 모니터링	- 파이프라인이 실행되는 동안 관련된 모든 도구를 오케스트레이션하고 테스트 및 모니터링하며 문제가 발생 시 경고(예: Airflow, Great Expectations, Grafana).

"끝"

ITPE 기술사회
제130회 정보처리기술사 기출문제 해설집

대 상 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사, 정보시스템감리사 시험
발행일 2023년 05월 20일
집 필 강정배PE, 안경환PE, 김민PE, 김민재PE
출 판 **ITPE(Information Technology Professional Engineer)**
주 소 ITPE 대치점 서울시 강남구 선릉로 86길 17 선릉엠티빌딩 7층
ITPE 선릉점 서울시 강남구 선릉로 86길 15, 3층 IT교육센터 아이티피이
ITPE 강남점 서울시 강남구 테헤란로 52길 21 파라다이스벤처타워 3층 303호
ITPE 영등포점 서울시 영등포구 당산동2가 하나비즈타워 7층 ITPE
연락처 070-4077-1267 / itpe@itpe.co.kr