ITPE기술사회

제39회 ITPE 실전 명품 모의고사 해설집

2025.12.21

ICT 기술사, 감리사, PMP, SW No1.

ITPE기술사회

기술사 포탈 http://itpe.co.kr | 국내최대 1위 커뮤니티 http://cafe.naver.com/81th

제 39 회 ITPE 실전 명품 모의고사

일시 : 2025 년 12 월 21 일 제 2 교시(시험시간: 100 분)

분야	정보통신	자격종목	정보관리 컴퓨터 시스템 응용	수검 번호		성 명	

※ 다음 문제 중 4 문제를 선택하여 설명 하십시오. (각 25 점)

1. 25 년 4 월 소프트웨어 진흥법이 개정되었다. 다음을 설명하시오

가. 소프트웨어 진흥법의 정의 및 목적

나. 소프트웨어 진흥법의 구성 내용

다. 25 년 4 월 개정판의 주요내용 및 의미

2. AI 시스템 구축 시 데이터 저장소로서 데이터 레이크(Data Lake)가 사용되고 있다. 다음을 설명하시오.

가. 데이터 레이크의 개념 및 필요성

나. 데이터 레이크를 포함한 AI 시스템 구축 아키텍처

다. AI 시스템의 데이터 레이크 구축 시 고려사항

3. HTTP 3.0 에 대하여 다음을 설명하시오.

가. HTTP 3.0 개념 및 프로토콜 스택 구조

나. HTTP 3.0 주요 기능

다. HTTP 3.0 1-RTT 와 0-RTT 연결 과정

4. ARP(Address Resolution Protocol)에 대하여 다음을 설명하시오.

가. ARP(Address Resolution Protocol), RARP(Reverse Address Resolution Protocol) 동작방식

나. ARP Spoofing 공격방식 및 대응방안

5. 최근 지정학적 리스크 증가와 각국의 데이터 규제 강화로 인해 글로벌 퍼블릭 클라우드에서 자국 또는 지역 기반 클라우드로의 데이터 이전이 가속화되고 있다. 이러한 환경 변화 속에서 '소버린(Sovereign) 클라우드'의 도입이 주목받고 있다. 다음에 대해 설명하시오.

가. 소버린 클라우드의 개념 및 특징

나. 소버린 클라우드와 퍼블릭 클라우드 비교

다. 소버린 클라우드의 주요 기술

[정보관리기술사 선택문제]

6. 최근 랜섬웨어 공격으로 인한 기업 피해가 증가함에 따라 공공기관 및 기업에서는 랜섬웨어 공격에 대한 대응방안 마련의 필요성이 증가하고 있다. 다음에 대해 설명하시오.

가. 랜섬웨어의 유형 및 감염 증상

나. 랜섬웨어의 분석 방법

다. 랜섬웨어 대응방안

[컴퓨터시스템응용기술사 선택문제]

6. 가상 메모리 관리 기법에 대해 다음을 설명하시오.

가. 가상 메모리 관리기법

나. 페이징(Paging) 기법과 세그멘테이션(Segmentation) 기법

다. 메모리 단편화

01	소프트웨어진흥법		
문제	25년 4월 소프트웨어 진흥법이 개정되었다. 다음을 설명하시오. 가. 소프트웨어 진흥법의 정의 및 목적 나. 소프트웨어 진흥법의 구성내용 다. 25년 4월 개정판의 주요내용 및 의미		
도메인	법. 가이드	난이도	중 (상/중/하)
키워드	소프트웨어 중심사회 전략 , SW산업 확장, SW 융합, 전면개정, 8장 78개조		
출제배경	20년만에 전면 개정된 소프트웨어 진흥법의 내용, 의도, 주요 개정내용 숙지 필요		
참고문헌	국가법령정보센터 , 소프트웨어정책연구소 연구자료 (https://spri.kr/posts/view/22961?code=data_all&study_type=industry_trend)		
출제자	배미경 기술사(제 135 정보관리기술사 / hjmom0727@daum.net)		

I. 소프트웨어 진흥법의 정의 및 목적

가. 소프트웨어 진흥법의 정의

- 디지털 전환 시대에 대응하여 SW산업의 성장, 공정한 사업환경, 기술·인력·안전 기반 강화를 국가 차원에서 체계적으로 추진하기 위해 제정된 법

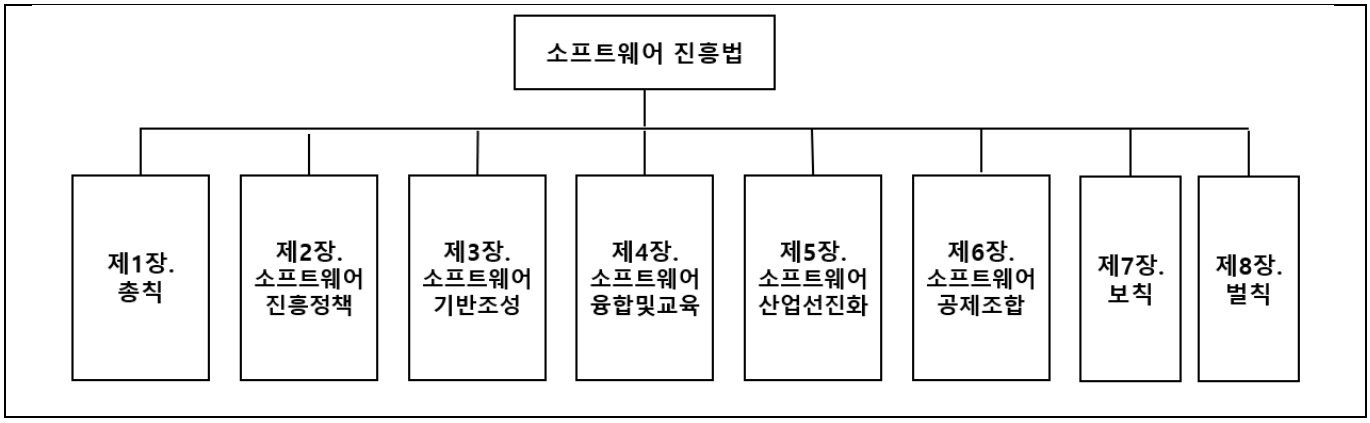
나. 소프트웨어 진흥법의 목적 (법 제1조 기반)

국가 소프트웨어 역량 강화	- 국가경쟁력을 좌우하는 핵심 산업으로서 SW의 전략적 중요성 강화
SW산업기반 조성 및 구조적 진흥	- 기술개발, 인력양성, 창업·융합, 표준화 등 산업 생태계 전반 지원
국민경제·국민생활 기여	- 산업·공공서비스·생활전반의 디지털 전환 가속화
SW 안전·보안·품질 확보	- 안전하고 신뢰할 수 있는 SW 개발·운영 환경 구축
공정한 SW사업 환경 조성	- 발주·입찰·계약·대가체계 개선을 통한 산업 구조 선진화

- SW를 국가 핵심 자원으로 육성하고, 공정· 안전· 혁신 기반 생태계를 만들기 위한 종합 법률

II. 소프트웨어 진흥법의 구성내용

가. 소프트웨어 진흥법의 구성



- 25년 4월 개정된 소프트웨어 진흥법은 총8장으로 구성되어 향후 대통령 재가와 국무회의 심의를 거쳐 공포

나. 소프트웨어 진흥법의 구성 상세

구분	항목	세부 내용
제 1 장 (총칙)	- 1조.목적	- 소프트웨어 진흥을 통해 국가 경쟁력 및 국민생활 향상 도모
	- 2조.정의	- 소프트웨어 관련 주요 용어를 규정
	- 3조.국가 및 지자체 의무	- 국가·지자체는 소프트웨어 산업 진흥을 위한 시책을 수립·시행
	- 4조.다른 법률과의 관계	- 다른 법에 특별 규정이 없으면 이 법을 우선 적용
제 2 장 (소프트웨어 진흥정책)	- 5조.기본계획의 수립	- 관계 부처 협의하여 소프트웨어 진흥 기본·시행계획을 수립
	- **6조.실태조사**	- 정부는 산업·기술자·사업자현황 등 SW산업정보 조사·공표가능
	- 7조.소프트웨어산업 정보 관리	- 정부는 소프트웨어 산업정보를 종합적으로 관리하고 공개 가능
제 3 장 (소프트웨어 기반조성)	제1절.소프트웨어 산업지원 (제8조~제18조)	- 전담기관 지정 및 연구소 운영(NIPA, 소프트웨어정책연구소) - 지역별 소프트웨어산업 육성 및 지원기관 지정 - 한국소프트웨어산업협회 설립 및 역할 규정 - 진흥시설·진흥단지 지정 및 지원 - 소프트웨어 창업 지원(기술사업화, 금융, M&A 등) - 국유재산 무상사용 허용(창업 지원 목적) - 국제협력·해외진출 촉진(표준·전시·공동연구 등) - 지식재산권 보호 시책 마련 - 세제·금융 등 산업 활성화를 위한 지원
	제2절.**표준화와 품질인증** (제19조~제21조)	- 소프트웨어 표준화 추진 및 권고 - 소프트웨어 품질인증 제도 운영 및 인증기관 지정 - 공공기관 우선구매 지원 - 소프트웨어프로세스 품질인증(PM·개발절차 품질 인증)
	제3절.**인력양성과 기술진흥** (제22조~제27조)	- 소프트웨어 전문 인력 양성 정책(교육·경력개발·협력) - 전문교육기관 설치·운영 - 소프트웨어기술자 경력관리 및 증명서 발급 - 기초연구 진흥 및 공개SW 중심 R&D 확산 - 연구자 지원(활동비·성과평가) - 소프트웨어공학 기술 연구·보급
제 4 장 (소프트웨어 융합및교육)	제1절.소프트웨어 **융합촉진** 및 소프트웨어 **안전확보** (제28조~제31조)	- 산업 간 소프트웨어 융합 촉진(시범사업·수출·R&D) - 소프트웨어 개발보안 활성화(기반 조성·중소기업 지원) - 소프트웨어안전 확보 지침 마련(위험분석·설계·검증 등) - 소프트웨어안전 산업 육성 및 사고 대응 지원
	제2절.소프트웨어 교육 및 소프트웨어 문화조성 (제32조~제37조)	- 국민 SW교육 활성화(콘텐츠·지역·강사 양성) - 초·중등 SW교육 지원 - SW 영재 발굴·육성 - SW 역량검정 제도 운영 - SW 문화 확산(개방·공유·협력 개발문화) - SW 기술자 사회적 우대

제 5 장 (소프트웨어 산업선진화)	제1절.통칙 (제38조~제42조)	- 공정하고 대등한 소프트웨어사업 계약 원칙 확립 - 요구사항 명확화, 계약서 기재사항 규정, 발주자 책무 제시 - 사전협의, 과업심의위원회 등 발주·계약의 기본 절차 마련
	제2절.소프트웨어 사업추진 (제43조~제52조)	- 요구사항 작성·변경 절차 명확화 및 적정 사업기간·대가 산정 - 중소기업 참여 확대, 부당 하도급 제한, 인력변동 관리 강화 - 주요 사업의 사전협의 의무화 및 제안서 보상 등 절차 개선
	제3절.상용소프트웨어 활용촉진 (제53조~제55조)	- 국가기관의 정품 상용SW 구매 의무화 및 직접 구매 원칙 - 필요 시 SaaS 우선 검토 등 효율적 구매 방식 허용 - 상용SW 품질·성능 평가시험을 통해 구매 전 품질 검증
	제4절.소프트웨어 사업관리 (제56조~제60조)	- 유지관리기준 정립,계약변경 절차,자산(산출물)관리 체계 마련 - 산출물 반출 승인 기준 규정 및 하자담보 책임 명확화 - 사업 전 생애주기(착수~종료) 전체의 관리·책임체계 정비
제 6 장 (소프트웨어 공제조합)	제61조.소프트웨어공제조합의 설립 ~ 제71조.배상책임 등	- **소프트웨어공제조합 제도화를** 통해 **소프트웨어 기업의 자금 조달, 보증, 성능보험, 이행보증 등을 종합적으로 지원하는 제도적 기반을** 마련
제 7 장 (보칙)	제72조.업무의 위탁 ~ 제76조.비밀누설의 금지	- **법 집행을 위한 행정적 규정으로** 업무 위탁·청문·환수·비밀보호 등 행정·절차적 보완 규정
제 8 장 (벌칙)	제77조.벌칙 ~ 제79조.과태료	- **법 위반 시 형사·행정 처벌 규정**으로 비밀누설·부정 표시 등에 대한 형사·행정 처벌 규정

- 총칙부터 벌칙까지 총 8장, 79조의 내용으로 구성된 소프트웨어 진흥법은 시대적 변화에 부응하기 위해 20년만의 전면개정 법안

III. 25년 4월 개정판의 주요내용 및 의미

가. 25년 4월 개정판의 주요내용

구분	항목	상세
기존법 비교	- 명칭 변경	- 소프트웨어산업 진흥법->소프트웨어 진흥법
	- 항목 변경	- 5장 48개조 -> 8장 78개조, 부칙
	- 제정, 개정 시기	- 2000년 제정, 28번 개정-> 25년4월 전면개정
	- 전면 개정 이유	- 공공 소프트웨어 사업을 위한 산업법 -> 소프트웨어 중심사회 실천 전략
개정판 주요내용	2장 – SW 진흥 정책	- SW융합, SW안전, 지역SW진흥 부문 적시 - 실태조사 실시 근거 마련
	3장 – SW 기반 조성	- SW 산업기반 내용 보강 (9,17,23,26조) - 품질인증 강화 (20,21조) - SW창업 활성화
	4장 – SW 융합 및 교육	- SW 융합 촉진 규정 - SW 안전확보 위한 지침 고시 - 초등SW 교육진흥 예산근거 마련 - SW 역량 검정 규정

		- SW 기술자 우대 조항
	5장 – SW 산업 선진화	- 공공 SW 시장 불공정 관행 개선 - 민간에 공정거래 원칙 확산 - 민간자본활용 공공SW 사업 추진
	6장 – SW 공제조합	- SW 공제조합 설립
	7장 – 보칙	- 업무 위탁과 청문, 출연금 환수 조항을 규정
	8장 – 벌칙	- 비밀누설 원칙 위반시 벌금 및 벌칙

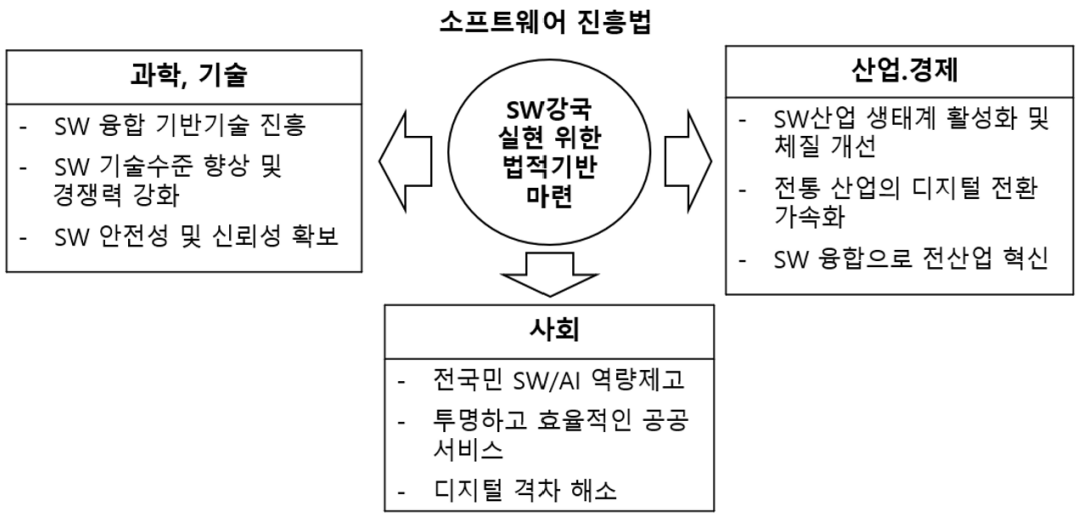
- SW 중요성을 인식하여 소프트웨어를 국가 경제를 발전시키는 지랫대로 삼기 위해 전면개정 진행

나. 25년 4월 개정판의 의미

구분	의미	설명
변화 대응	- 디지털 전환과 SW 중심사회 대응	- 디지털 시대의 SW 중요성 인식하여 SW 중심사회의 실천 전략으로 자리매김
	- SW 확장 및 융합 대처 용이	- 공공 소프트웨어 뿐 아니라, 상용SW, 지역SW로 확장 및 융합
통합, 정책강화	- 정책, 규제 통합적 접근	- SW 정책, 산업 지원, R&D 지원의 통합적 관점의 접근이 가능
	- 산업, 경제적 관점 강화	- **중소·벤처 소프트웨어 기업 지원, 공공·민간 소프트웨어 수요 촉진, SW 품질·신뢰성 확보** 등 산업 경쟁력 확보를 위한 법적 장치를 강화
	- 인력 및 교육중심 정책강화	- **소프트웨어 전문 인력 양성, 디지털 역량 강화 교육** 지원 근거를 명확히 하여, 인력 부족 문제와 기술 격차를 해소

- 소프트웨어를 **국가 경쟁력, 기술 신뢰성, 인력 양성, 산업 혁신의 핵심 수단으로** 규정하고, 정책적·제도적 기반을 전면적으로 재정비

IV. 소프트웨어 진흥법 개정의 기대효과



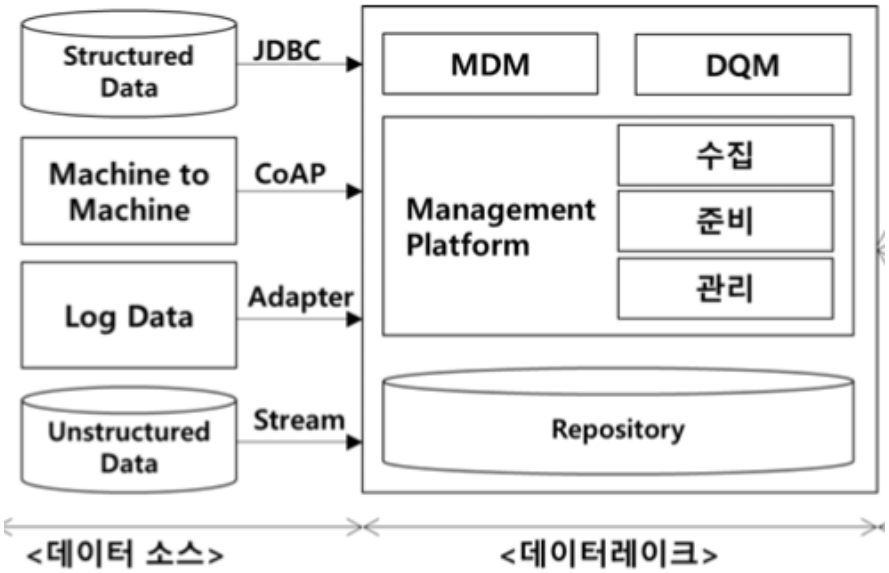
- 소프트웨어 진흥법 전면개정을 통해 대한민국은 SW 강국으로서의 입지를 다지고, 디지털 대전환 시대를 선도하는 기반을 구축할 것으로 기대

"끝"

02	데이터 레이크		
문제	AI 시스템 구축 시 데이터 저장소로서 데이터 레이크(Data Lake)가 사용되고 있다. 다음을 설명하시오 가. 데이터 레이크의 개념 및 필요성 나. 데이터 레이크를 포함한 AI시스템 구축 아키텍처 다. AI시스템의 데이터 레이크 구축 시 고려사항		
도메인	데이터베이스	난이도	중 (상/중/하)
키워드	대용량 데이터 저장소, 정형, 반정형, 비정형 데이터, Schemaless, 확장성, 데이터 카탈로그, 메타데이터		
출제배경	AI시스템 구축이 늘어남에 따라 데이터 저장소로서 데이터 레이크가 필수적으로 활용, 그 의미와 개념을 재 검토.		
참고문헌	ITPE 서브노트, 디지털서비스 이용지원시스템 자료실 , https://www.ibm.com/kr-ko/think/topics/data-lake		
출제자	배미경 기술사(제 135회 정보관리기술사 / hjmom0727@daum.net)		

I. AI시스템의 데이터 저장소, 데이터 레이크(Data Lake)의 개념 및 필요성

가. 데이터 레이크(Data Lake)의 개념

구분	설 명
개념도	
개념	- **정형, 반정형, 비정형** 데이터를 **원본** 그대로 저장해 사용시 필요한 형태로 제공하는 **대용량 데이터 저장소**

- 다양한 종류의 데이터 소스를 스키마 없이(Schemaless) 원시형태로 저장하는 대용량 데이터 저장소

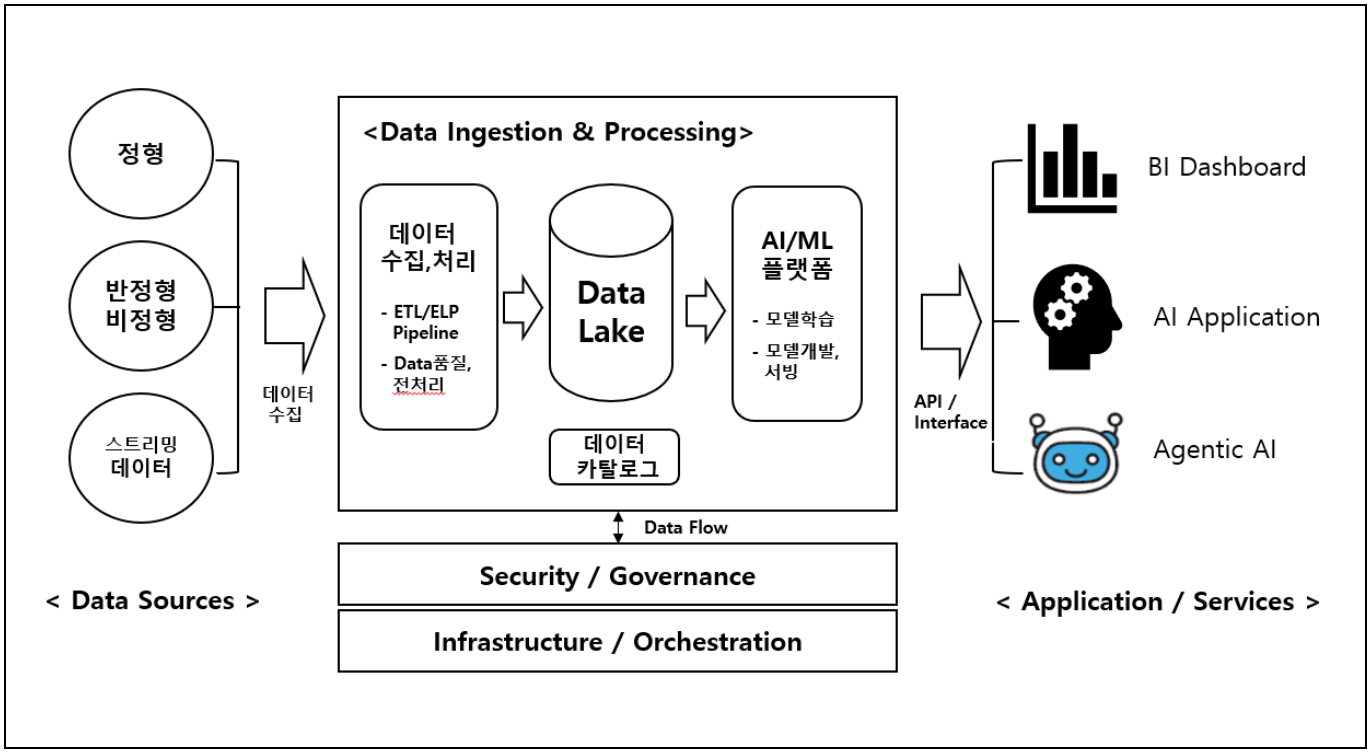
나. 데이터 레이크(Data Lake)의 필요성

구분	필요성	설명
기술적 관점	- 모든 형태의 데이터 저장가능	- 정형· 반정형· 비정형 데이터를 원본 그대로 저장
	- AI/ML 분석을 위한 고성능 처리 기반 확보	- Spark, Hadoop, GPU 기반 처리 등 다양한 엔진 사용이 가능
	- ELT기반 유연한 변환, 실험 가능	- 스키마를 사전에 강제하지 않아 빠르게 분석 시도 가능
	- 스트리밍 + 배치 데이터 통합 처리	- 수집된 데이터 추출과 로드를 위하여 스케줄링 잡과 실시간 스트리밍 처리가 모두 가능
	- 확장성 용이	- 오브젝트 스토리지 기반 → 무제한 확장 가능
비즈니스 관점	- 데이터 사일로 해소	- 분산되어 있는 전사 데이터 통합 가능
	- 데이터 기반 의사결정 고도화	- 다양한 데이터 조합 → 더 정확한 인사이트 도출
	- AI·예측모델·자동화 기반 마련	- 원천 데이터 수집이 AI 경쟁력의 핵심
	- 데이터 자산화,재사용성 증가	- 동일한 데이터를 여러 조직·부서에서 활용 가능
	- 비용 효율성	- 낮은 스토리지 가격

- 다양한 형태의 데이터 통합 및 대용량 데이터 저장소로서 낮은 가격과 높은 확장성 등의 특징으로 AI시스템 구축 시 데이터 저장소로서 활용

II. 데이터 레이크를 포함한 AI시스템 구축 아키텍처

가. 데이터 레이크를 포함한 AI시스템 아키텍처



- 데이터 소스, 데이터 수집 및 처리, **데이터 레이크**, AI/ML 플랫폼, 애플리케이션 및 서비스의 5가지 핵심 레이어로 구성

나. 데이터 레이크를 포함한 AI시스템 아키텍처의 기술요소

레이어	기술 요소	설명
데이터 소스	- 관계형 데이터베이스(RDB)	- 정형 데이터를 저장하며, 트랜잭션 처리에 주로 사용 (MySQL, Oracle)
	- 비정형 데이터	- 구조화되지 않은 대량의 데이터. AI 모델 학습에 필수적 (이미지, 텍스트, 소셜 미디어)
	- 스트리밍 데이터	- 실시간으로 지속적으로 발생하는 데이터 흐름 (IoT 센서, 클릭 스트림)
데이터 수집 및 처리	- Apache Kafka / Pub/Sub	- 실시간 스트리밍 데이터를 안정적으로 수집, 분산 처리하기 위한 메시징 시스템
	- Apache Spark / Flink	- 대규모 데이터의 **배치(Batch) 처리**와 **스트림(Stream) 처리**를 위한 고속 분산 처리 엔진
	- ETL/ELT 파이프라인	- 데이터 추출(Extract), 변환(Transform), 적재(Load) 과정을 자동화하여 데이터 품질을 확보
데이터 레이크	- S3 / ADLS / HDFS	- 모든 형태의 원시 데이터(Raw Data)를 저장하는 **저비용의 대규모 분산 저장소**
	- Parquet / ORC	- 데이터 레이크에서 분석 효율성을 높이기 위한 **컬럼 기반**의 압축 파일 형식
	- 데이터 카탈로그	- 저장된 데이터의 **메타데이터** (위치, 스키마, 소유자 등)를 관리하여 검색을 용이하게 함
AI/ML 플랫폼	- TensorFlow / PyTorch	- 머신러닝 및 딥러닝 모델을 구축하고 학습시키기 위한 핵심 **프레임워크**
	- Feature Engineering	- 모델 학습 성능 향상을 위해 원시 데이터로부터 **유의미한 예측 변수(Feature)를 생성**하는 과정
	- MLOps 도구 (MLflow, Kubeflow)	- 모델 개발부터 **배포, 모니터링, 재학습**에 이르는 전체 수명 주기를 자동화하고 관리
AI 서비스, Application	- REST API / gRPC	- 학습된 AI 모델의 **추론 결과**를 다른 시스템이나 서비스에 제공하기 위한 인터페이스
	- BI/대시보드	- AI 분석 결과나 데이터 기반의 통찰력을 시각화, 비즈니스 의사결정을 도움
	- AI 서비스	- AI 모델이 직접 작동하여 사용자에게 가치를 제공하는 애플리케이션. (추천 시스템, 이미지 인식 서비스)

- AI시스템 구축 시, 5가지 레이어 외에 인프라 및 오케스트레이션 (클라우드,컨테이너, GPU/TPU, 쿠버네티스) 과 보안 및 거버넌스의 요소도 필요

III. AI시스템의 데이터 레이크 구축 시 고려사항

가. 기술적 관점의 고려사항

구분	고려사항	설명
확장성	- 데이터 수집 파이프라인 설계	- 다양한 소스(정형/비정형/스트리밍)의 데이터를 안정적으로 수집하고 처리할 수 있는 유연하고 확장 가능한 파이프라인을 구축
	- 확장성 및 탄력성 확보	- AI 프로젝트의 성장에 따라 데이터 용량이 기하급수적으로 증가할 수 있으므로, 무한한 확장성을 제공하는 클라우드 기반 아키텍처를 선택하고, 수요에 따라 자원을 조절하는 탄력성을 확보
성능	- 저장소 및 데이터 형식 최적화	- 비용 효율성과 분석 성능을 동시에 고려 - 대용량 데이터는 클라우드 스토리지 (S3, ADLS)에 저장, 쿼리 속도를 높이기 위해 Parquet이나 ORC와 같은 컬럼 기반 파일 형식을 사용
	- 고성능 컴퓨팅 엔진 선택	- 데이터 레이크의 데이터를 분석하고 ML 모델 학습에 활용할 수 있도록 Apache Spark와 같이 대규모 병렬 처리가 가능한 고성능 분석 엔진을 선택

- AI 시스템의 성능보장과 데이터 용량의 증가에 대한 확장성 있는 데이터 레이크의 선택을 고려

나. 운영 및 거버넌스 관점의 고려사항

구분	고려사항	설명
운영	- 비용 관리 및 최적화	- 데이터 레이크는 저장 비용은 저렴하지만, **쿼리 비용**이 발생할 수 있으므로 수명 주기 정책을 적용, 오래된 데이터를 계층적으로 관리 및 불필요한 컴퓨팅 자원 낭비를 방지
	- 기술 조직의 역량 확보	- 데이터 레이크 및 관련 기술 스택(Spark, Lakehouse 기술 등)의 구축과 운영을 위해서 **데이터 엔지니어링 및 MLOps 역량**을 갖춘 전담 조직의 확보가 필수적
거버넌스	- 데이터 품질 및 거버넌스	- AI 모델의 성능은 데이터 품질에 직접적으로 영향을 받으므로, **데이터 계보(Lineage)** 추적, **데이터 오너십** 정의, **메타데이터 관리**를 통해 데이터의 신뢰성을 보장
	- 보안 및 접근 제어	- 개인정보 등 민감한 데이터를 포함할 수 있으므로, 저장소 및 데이터 접근에 대한 **강력한 인증 및 권한 관리(IAM)** 체계를 구축 필요. 개인정보 비식별화 및 데이터 암호화(Encryption)도 필수 고려사항

- 데이터 레이크가 단순히 데이터를 담아두는 저장소가 아니라, AI/ML 및 비즈니스 분석을 위한 **신뢰할 수 있는 기반**이 되므로 데이터 품질, 보안 및 거버넌스를 고려하여 데이터 늪(Data Swamp)이 되지 않도록 고려
- AI/ML 워크로드와 전통적인 BI분석 워크로드를 하나의 플랫폼에서 통합하기 위해 데이터 레이크 하우스의 사용으로 진화되고 있음

IV. 데이터 레이크와 데이터 레이크 하우스의 비교

구분	데이터 레이크	데이터 레이크 하우스
개념	- 모든 형태(정형·비정형·반정형)의 데이터를 원천 그대로 저장하는 대규모 저장소	- 데이터 레이크 계층 위에 데이터 웨어하우스 역할을 하는 계층을 통합하여 구현한 아키텍처
목적	- 모든 데이터를 있는 그대로 저장하여 향후 분석에 활용 (Schema-on-Read)	- 데이터 레이크의 유연성과 데이터 웨어하우스의 신뢰성 통합
데이터품질	- 낮음 - 원시데이터 그대로 저장 사용시 가공	- 높음 - 데이터 웨어하우스의 기능(ACID 트랜잭션, 스키마 적용)을 도입하여 데이터 일관성 보장
스키마 관리	- 읽을 때 스키마 적용 (Schema-on-Read)	- 쓰거나 읽을 때 스키마 적용
비용효율성	- 매우 높음. 클라우드 오브젝트 스토리지를 활용, 저렴한 비용으로 대규모 저장	- 데이터 레이크보다 비용이 높아 비용효율이 낮음
장점	- 원시 데이터를 무한 확장으로 저장 가능 - 비용이 매우 저렴함 - 모든 유형 데이터를 저장 가능 - AI/ML용 장기 데이터 아카이브에 적합	- ACID 트랜잭션 지원으로 **데이터 품질 보장** - BI + ML 분석을 하나의 저장소에서 수행 - 스키마 관리, 거버넌스 강화 - 웨어하우스 대비 비용 절감 가능 - 성능 높은 SQL 엔진 지원
단점	- 스키마가 없어 **데이터 품질 관리 어려움** - BI 분석에 부적합 - Governance/보안 통합 어려움 - 관리 비용 증가	- 기존 레이크 대비 구현 복잡성 증가 - ACID/메타데이터 레이어 관리 필요 - 플랫폼 락인 우려(Delta, Databricks 등) - 구축 비용이 레이크보다 큼
AI시스템 적합성	- 데이터 저장·ML 학습용 대용량 데이터 수집에 적합	- AI+BI 통합 환경, 대규모 ML 실험·데이터 품질 관리에 특히 적합

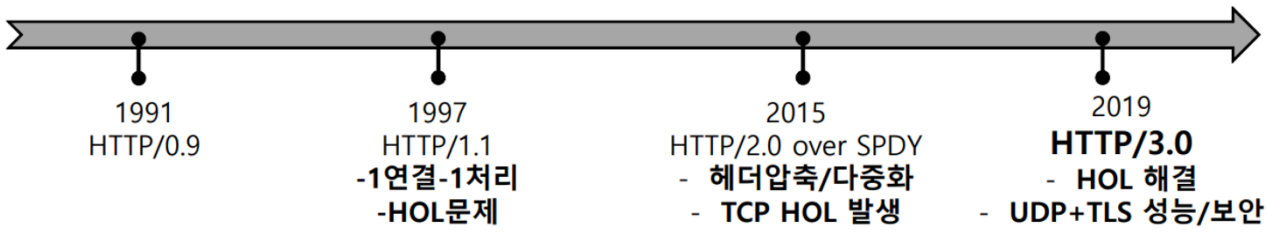
- 구축하려는 AI시스템의 모델과 목적에 따라 데이터 레이크와 데이터 레이크 하우스를 선택하여 사용

"끝"

03	HTTP 3.0		
문제	HTTP 3.0에 대하여 다음을 설명하시오. 가. HTTP 3.0 개념 및 프로토콜 스택 구조 나. HTTP 3.0 주요 기능 다. HTTP 3.0 1-RTT와 0-RTT 연결 과정		
도메인	디지털서비스	난이도	중 (상/중/하)
키워드	UDP, TLS 1.3, QUIC, 0-RTT, 멀티플렉싱, TCP HOL Blocking, Connection ID, QPACK		
출제배경	2022년 IETF에서 국제 표준으로 채택, 이후 꾸준히 점유율 증가		
참고문헌	ITPE 기술사회 서브노트		
출제자	박서현 기술사(제 131회 정보관리기술사 / mondaysss@naver.com)		

I. HTTP 차세대 표준, HTTP 3.0 개념 및 프로토콜 스택 구조

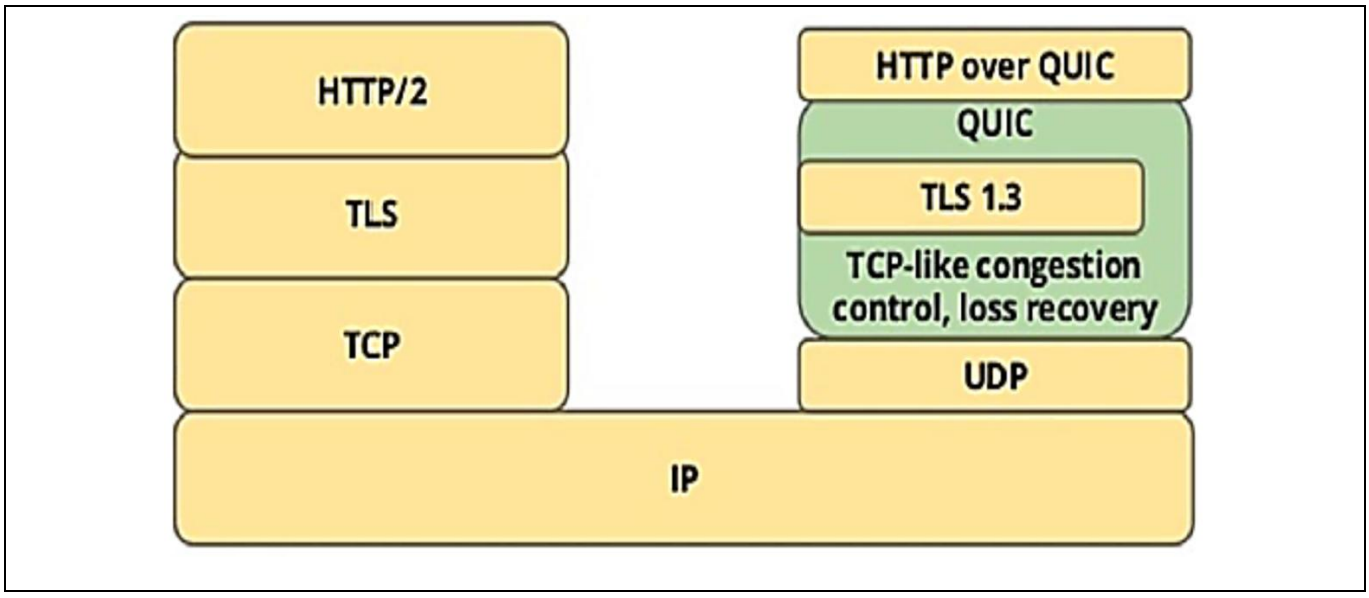
가. HTTP 3.0 개념



정의	- HTTP 연결 및 전송 지연을 최소화 하기 위해, TCP+TLS 조합 대신 UDP+TLS 조합을 이용하는 보안 및 향상된 성능을 제공하는 UDP 기반 전송 계층 프로토콜

- HTTP over QUIC이 HTTP 3.0으로 이름을 변경

나. HTTP 3.0 프로토콜 스택 구조

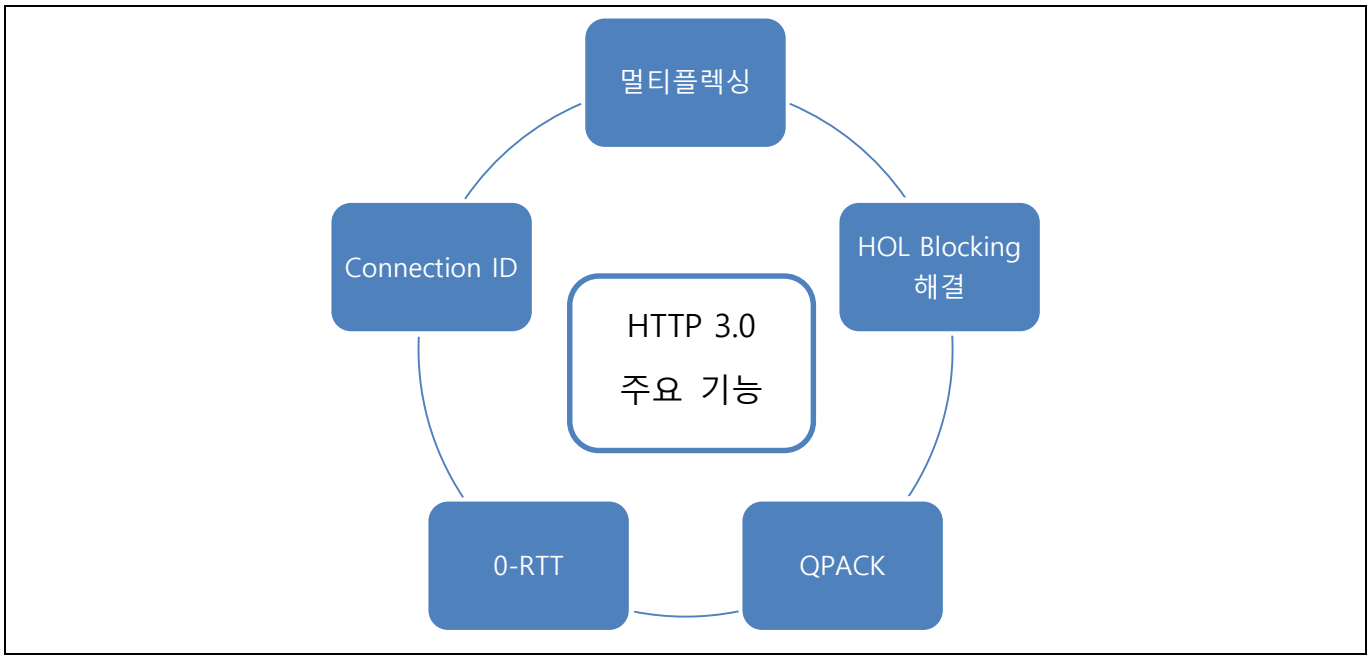


OSI 계층	스택 구성요소	설명
네트워크 계층(3계층)	IP	- 패킷 주소 지정 및 경로 설정을 담당
전송계층 (4계층)	UDP	- TCP보다 더 가볍고 빠른 통신 제공 - 단, 신뢰성을 보장할 수 없는 단점 존재
	QUIC (Quick UDP Internet Connection)	- UDP 기반으로 신뢰성 있는 전송을 수행하기 위해 구글에서 개발한 전송 계층(Transfer Layer) 프로토콜 - UDP의 비연결성을 QUIC이 보완하여 속도와 안정성을 개선
세션계층 (5계층)	TLS 1.3	- 데이터 암호화 송수신 및 속도 개선 - UDP 443 Port 사용

- UDP와 TLS 1.3를 통해 성능과 보안성 향상 및 QUIC 통한 연결 및 전송 지연 최소화

II. HTTP 3.0 주요기능

가. HTTP 3.0 주요기능 개념도



나. HTTP 3.0 주요기능 설명

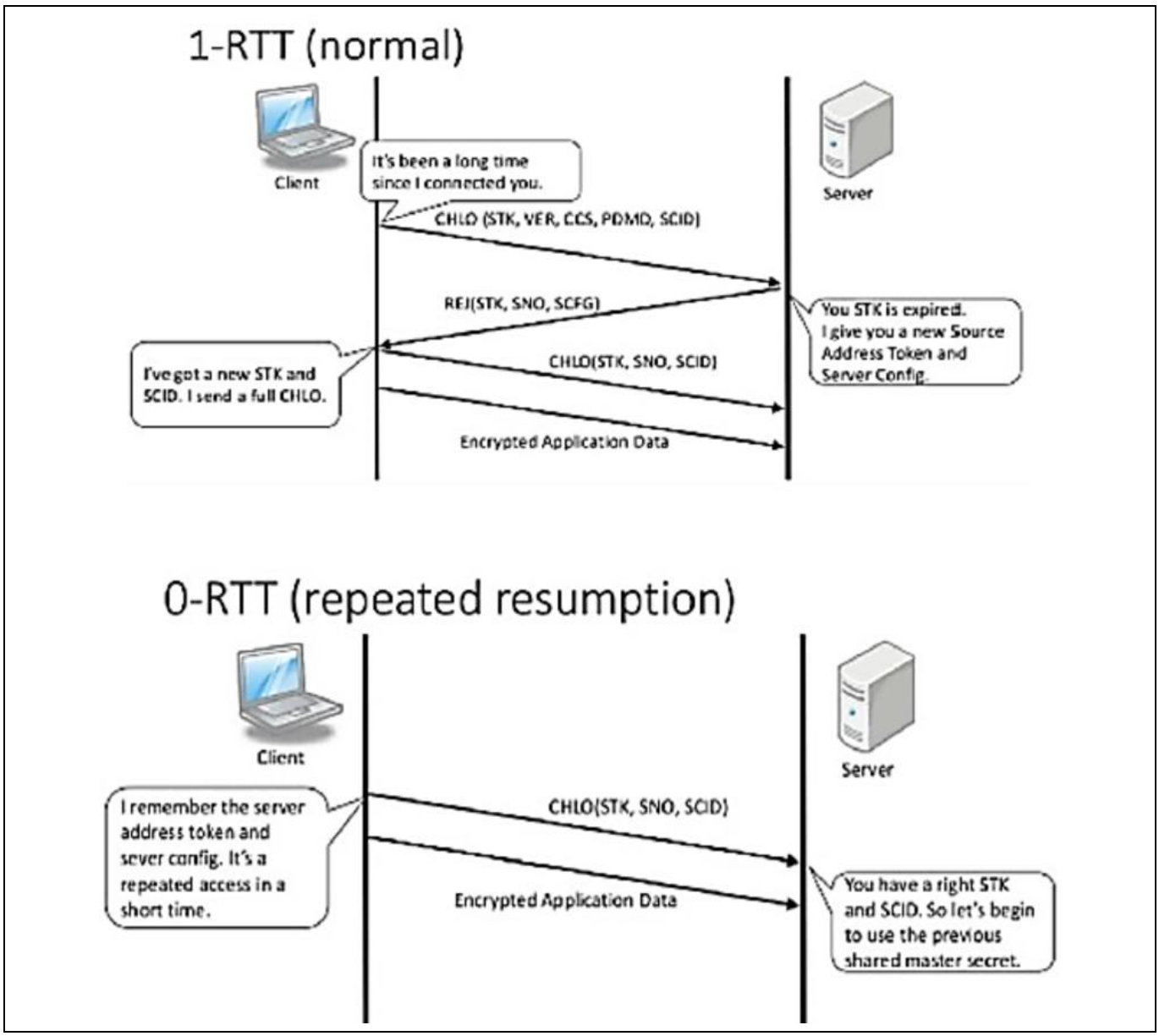
구분	주요기능	설명
전송 속도 개선	- 멀티플렉싱	- 하나의 연결 내에서 여러 요청을 동시에 전송 가능 - 웹 응답 속도 개선
	- TCP HOL(Head-of-line) Blocking 해결	- HTTP 2.0은 HTTP HOL Blocking 문제는 해결했으나 TCP HOL Blocking 문제는 여전히 존재함 - HTTP 3.0은 요청 다중화를 통해 TCP HOL Blocking까지 해결 - 병렬 데이터 전송 속도 향상
대역폭 최적화	- QPACK	- 무손실 헤더압축 기능 - 전송 오버헤드 감소

빠른 재연결	- 0-RTT 연결 수립	- 이전 연결 시 캐싱된 자격증명을 사용하기 때문에 두번째 연결 시 0-RTT 소요 - 전송 오버헤드 감소
	- Connection ID	- Connection ID를 사용하여 연결을 유지하므로 IP가 변경되어도 연결 끊김 없음 - 모바일 환경에서 안정적 통신 지원

- TCP+TLS 1.3 조합은 연결 시 기본 2-RTT가 소요되는 것에 반해 HTTP 3.0은 최초 연결에 1-RTT, 재연결 시 0-RTT(Round Trip Time) 연결을 통해 빠른 연결 수립

III. HTTP 3.0 1-RTT와 0-RTT 연결 과정

가. HTTP 3.0 1-RTT와 0-RTT 연결 과정도



- 최초에는 1-RTT 수행, 이후 0-RTT 연결을 수립하여 빠른 연결이 가능하여 IoT, 모바일 환경에 최적화

나. HTTP 3.0 1-RTT와 0-RTT 연결 과정 설명

구분	연결 과정	상세 설명
Initial 1-RTT Handshake	- Inchoate CHLO(Client Hello) : 암호화되지 않은 CHLO 패킷 전송 - Rejection : 서버 설정, 암호화된 토큰을 포함한 패킷(토큰을 이용해 서버로 보내는 요청 암호화) - Complete CHLO : 연결 완료	- 토큰, 서버 인증서를 gzip 압축 파일 형태로 Client에 전달
Successful 0-RTT Handshake	- Complete CHLO : 이전 연결 시 캐싱된 자격증명을 사용해서 Encrypted Request를 서버로 바로 전송 가능	- 캐시된 자격증명 사용해서 핸드쉐이크를 스킵하고 암호화된 요청을 즉시 서버로 전송
Rejected 0-RTT Handshake	- 1-RTT Handshake 재수행 - 캐싱된 정보가 오래된 경우 수행	- 클라이언트의 캐싱된 정보가 오래된 경우 1-RTT를 재수행

- 향상된 보안성, 빠른 연결을 수행하는 HTTP 3.0을 5G 기술과 결합하면 모바일, 엣지, 실시간 서비스의 품질을 획기적으로 개선 가능할 것으로 보임

IV. HTTP 3.0과 5G 연계 시사점

구분	시사점	설명
속도	초저지연 실현	- 5G의 짧은 RTT와 0-RTT 핸드쉐이크를 결합하여 실시간 스트리밍, AR/VR에 최적
	엣지 컴퓨팅 최적화	- 다중 스트림, HOL Blocking 문제 해결하여 엣지 단의 응답 속도 향상
보안성	보안 및 신뢰성 향상	- TLS 1.3 기반이므로 5G 네트워크 슬라이스 간 보안 경계 유지
이동성	연결 유지성 향상	- IP 기반이 아닌 Connection ID 기반이므로 단말기가 셀 간 이동 시에도 세션 유지되어 5G 네트워크 슬라이싱 환경에 적합

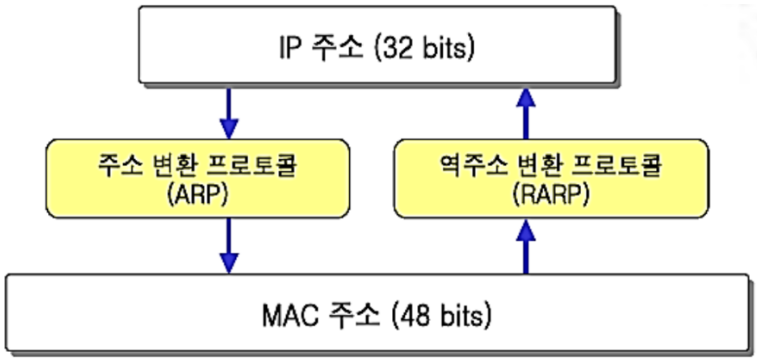
- 5G 네트워크는 낮은 지연 시간과 높은 대역폭을 제공하지만, 모바일 환경에서는 여전히 패킷 손실이 다수 발생하므로 HTTP 3.0의 빠른 복원력이 5G의 빠른 속도 잠재력을 최대한 활용 가능

"끝"

04	ARP(Address Resolution Protocol)		
문제	ARP(Address Resolution Protocol)에 대하여 다음을 설명하시오. 가. ARP(Address Resolution Protocol), RARP(Reverse Address Resolution Protocol) 동작방식 설명 나. ARP Spoofing 공격방식 및 대응방안		
도메인	보안	난이도	상 (상/중/하)
키워드	논리주소(IP), 물리주소(MAC), 주소변환, Broadcast, Unicast, ARP Cache, static ARP, 암호화		
출제배경	134회 컴시응 출제로 인한 교차 출제 가능성, 기본 토픽인 ARP와 관련 보안 취약점 숙지 확인		
참고문헌	ITPE 기술사회 서브노트		
출제자	박서현 기술사(제 131회 정보관리기술사 / mondaysss@naver.com)		

I. 논리주소와 물리주소 변환 프로토콜, ARP와 RARP 개요

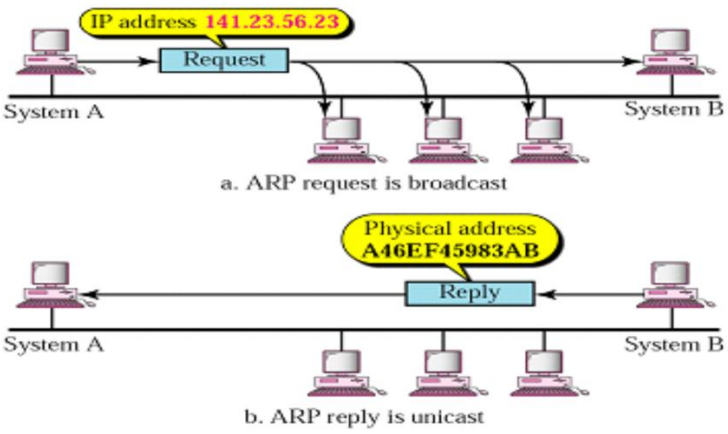
가. ARP(Address Resolution Protocol)와 RARP(Reverse Address Resolution Protocol) 개념



ARP	- LAN 환경에서 논리적인 주소인 IP주소를 물리적인 주소인 MAC 주소로 변환해 주는 네트워크 계층의 프로토콜
RARP	- 라우터 등 특정 시스템이 MAC 주소는 알고 있으나 IP주소를 모를 경우 MAC 주소를 IP주소로 변환해주는 프로토콜 (RFC 903)

II. ARP(Address Resolution Protocol), RARP(Reverse Address Resolution Protocol) 동작방식 설명

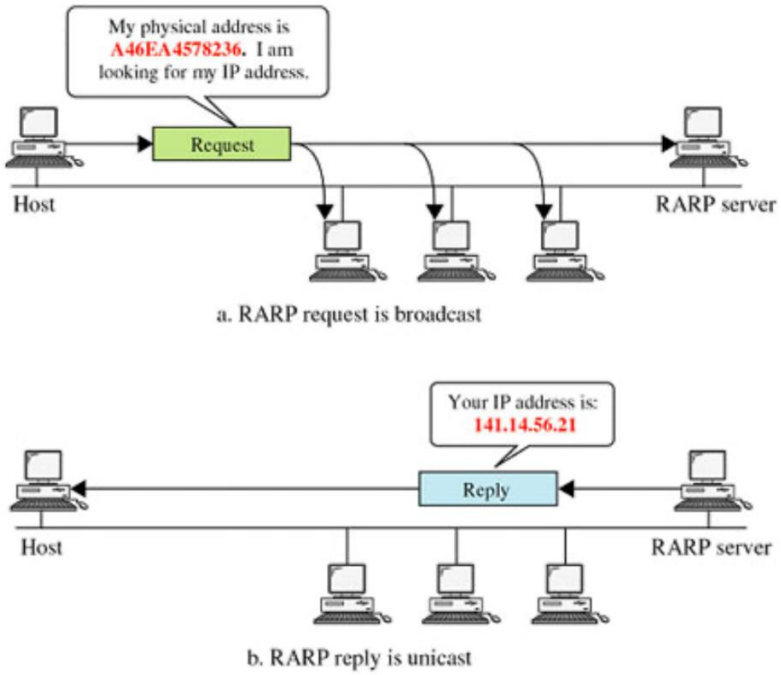
가. ARP 동작방식 설명



동작주체	동작방식	설명
Host A	(1) ARP Cache 확인	- Host A(그림의 System A) 가 자신의 네트워크 어댑터 내의 ARP Cache 테이블을 확인 - Cache 테이블에 질의 대상 IP에 해당하는 MAC주소가 없음을 확인(이미 존재하는 경우에는 ARP Reques 생략)
Host A	(2) ARP Request Broadcast	- ARP Request 패킷을 같은 대역에 Broadcast - 질의 대상 IP 주소를 Request
Host B	(3) ARP Reply	- 전송받은 IP에 해당하는 Host B가 ARP Reply 패킷에 본인의 MAC주소를 담아 Host A로 전송
Host A	(4) ARP Cache 저장	- Host A는 ARP Reply 패킷을 확인하고 자신의 ARP Cache 테이블을 수정

- 논리주소(IP)를 기반으로 물리주소(MAC)을 찾기 위해 ARP 프로토콜을 이용
- RARP는 IP주소 이외의 추가정보를 얻을 수 없어 잘 사용하지 않으며, 대신 DHCP, BOOTP를 많이 사용

나. RARP 동작방식 설명

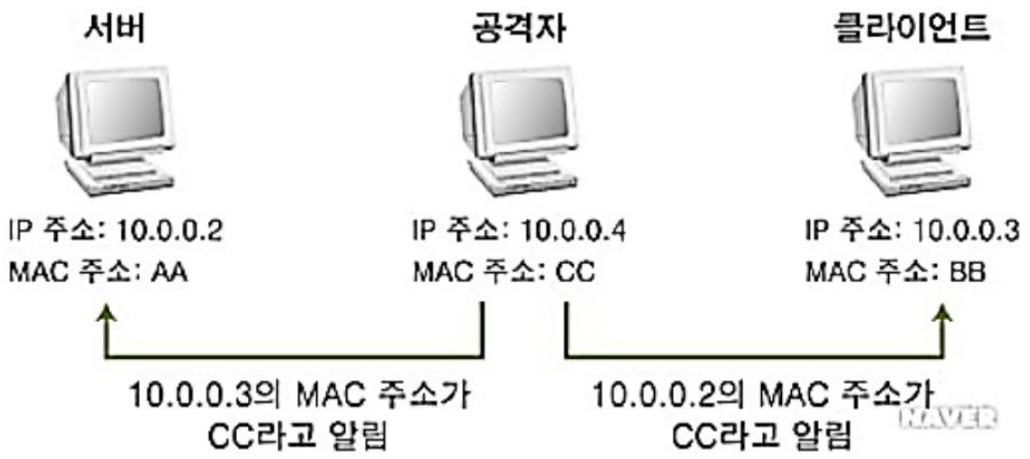


구분	동작방식	설명
Host	(1) RARP Request Broadcast	- Host가 최초 자신의 IP를 모를 때 MAC 주소를 담고있는 RARP Request를 Broadcast
RARP Server	(2) RARP Reply Unicast	- 연결된 호스트들의 IP:MAC 정보는 RARP Server에 유지 - RARP Server는 요청받은 RARP Request에 해당하는 IP주소를 담아 RARP Reply를 요청 Host에 전송
Host	(3) IP 주소 저장	- 응답받은 IP 주소를 저장

- ARP 프로토콜 동작 시 악의적 의도를 가진 Host의 MAC주소를 응답함으로써 다른 Host에 전달되어야 하는 정보를 가로채는 MITM 공격 방식인 ARP Spoofing 취약점 존재

III. ARP Spoofing 공격방식 및 대응방안

가. ARP Spoofing 공격방식



구분	공격방식	설명
준비단계	(1) IP Forward 활성화	- 일반적인 컴퓨터는 자신에게 온 패킷만 처리하지만 IP Forward 기능이 활성화된 시스템은 자신을 거쳐가는 패킷을 다른 네트워크로 전달 가능 - 공격 대상이 되는 호스트 간 정상통신(스니핑을 눈치채지 못하게) 하기 위해 IP Forward 기능 활성화 * 2계층 주소인 MAC 주소를 속이는 공격, 2계층에서 동작하므로 동일 네트워크 대역에 있어야 함
수행단계	(2) 위조 ARP Reply 전송	- 송수신자 사이에서 위조된 ARP Reply를 두 희생자에게 지속적으로 전송
	(3) ARP Cache Table 변조	- ARP Cache Table의 MAC 정보를 공격자의 MAC 정보로 변경
	(4) 패킷 가로채기	- 공격자는 정상 송수신 호스트 간의 주고 받는 패킷을 중간에서 가로채어 데이터 확인 가능

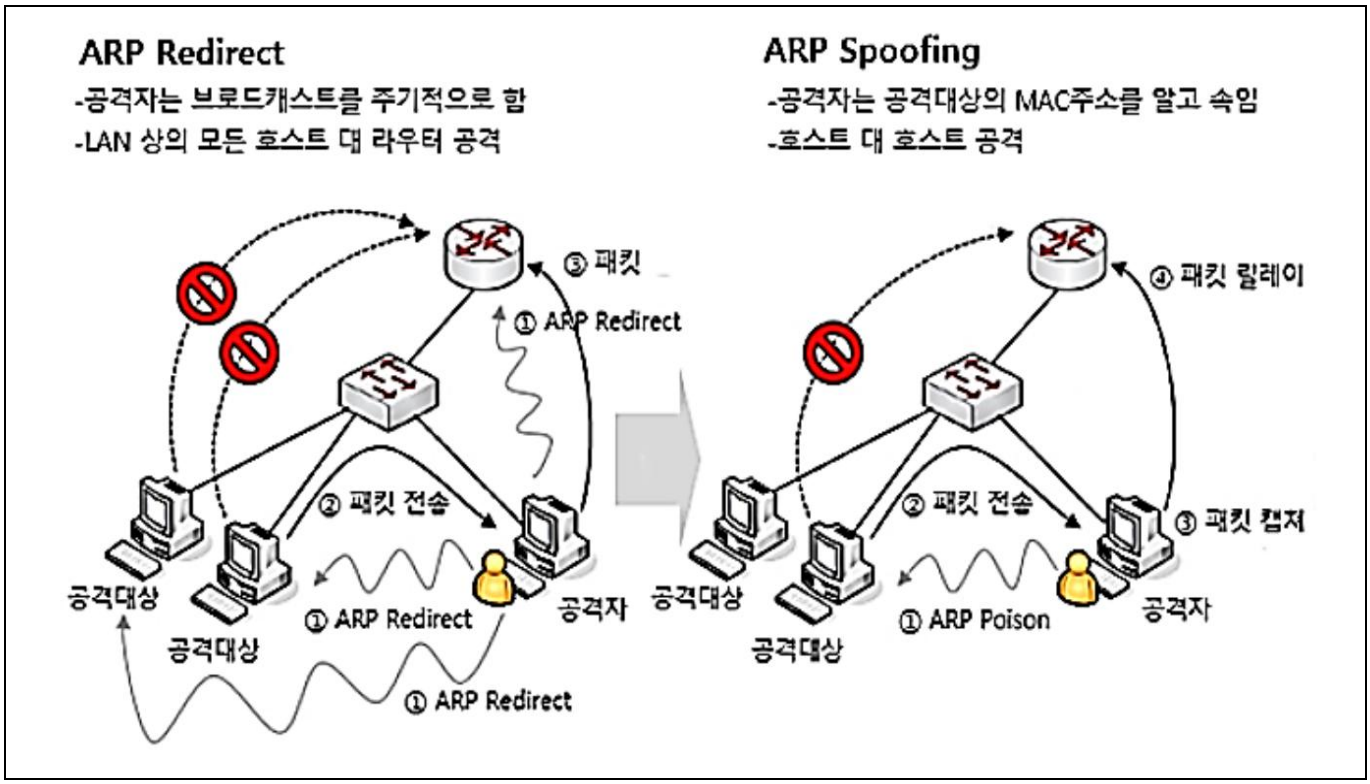
나. ARP Spoofing 대응방안

구분	대응방안	설명
시스템 관리	정적 ARP 테이블 관리	- ARP Table의 정보를 정적으로 설정하여 비정상 변경 방지 - 명령어 : arp -s 192.168.10.100 a9:12:12:aa:bb:99
	중요 패킷 암호화	- 안전한 서버도 동일 서브넷 내 스푸핑된 서버에 의해 패킷 스니핑이 가능하기 때문에 민감정보 암호화
	서버 보안수준 강화	- 침입자가 설치한 프로그램으로 인해 네트워크 트래픽 변조 서버로 악용되지 않도록 서버보안 수준 강화
네트워크 관리	MAC Flooding 관리	- MAC 주소의 개수나 특정 MAC 주소 지정 네트워크 장비와 Host 시스템 양측에서 모두 정적 ARP 관리
	ARP 트래픽 모니터링	- 네트워크 상의 ARP 트래픽을 실시간으로 모니터링 하는 프로

		그램(ARP Watch 등)을 통해 IP와 MAC 주소 매핑 감시, 변경 사항 발생 시 확인
	사설 VLAN 기능 활용	- 같은 서브넷의 서버도 통신 불필요 시 제외하고 동일 서브넷에서 지정 호스트만 통신

- ARP Spoofing과 유사한 취약점 중 ARP 프로토콜을 이용한 ARP Redirect 공격 기법도 존재

IV. ARP Spoofing과 ARP Redirect 관계



- ARP Spoofing은 호스트 대 호스트 공격, ARP Redirect는 LAN의 모든 호스트 대 라우터라는 점 외에는 큰 차이가 없는 취약점

"끝"

05	소버린(Sovereign) 클라우드		
문제	최근 지정학적 리스크 증가와 각국의 데이터 규제 강화로 인해 글로벌 퍼블릭 클라우드에서 자국 또는 지역 기반 클라우드로의 데이터 이전이 가속화되고 있다. 이러한 환경 변화 속에서 '소버린(Sovereign) 클라우드'의 도입이 주목받고 있다. 다음에 대해 설명하시오. 가. 소버린 클라우드의 개념 및 특징 나. 소버린 클라우드와 퍼블릭 클라우드 비교 다. 소버린 클라우드의 주요 기술		
도메인	디지털서비스	난이도	중 (상/중/하)
키워드	의무적 기업 규칙(BCR), 개인정보보호강화기술(PET), 접근 통제/서명, 암호화, 보안 모니터링, EDR/XDR, Micro Segmentation, 제로 트러스트		
출제배경	가트너 2026년 10대 전략 기술 '지오패트리에이션' 발표에 따른 관련 토픽 출제예상		
참고문헌	금융 분야 클라우드 도입 및 소버린 클라우드 필요성(주기동, 2025.08)		
출제자	소민호 기술사(제 119회 정보관리기술사 / mhsope@naver.com)		

I. 데이터 주권 유지, 소버린 클라우드(Sovereign Cloud)의 개념 및 특징

가. 소버린 클라우드(Sovereign Cloud)의 개념

- 특정 국가의 법률, 규정, 정책을 엄격하게 준수하고 데이터 주권(data sovereignty)을 보장하기 위해 설계된 클라우드 컴퓨팅 환경
- 데이터 주권, 데이터 상주, 운영 주권, 디지털 주권을 바탕으로 특정 국가 또는 지역의 법률, 규제의 정책을 엄격하게 준수하도록 설계되고 운영되는 클라우드 컴퓨팅 환경

나. 소버린 클라우드의 특징

특징	설명
국가별 법·규제 준수	- 각국의 데이터 보호법과 규제에 따라 데이터의 저장·처리·전송이 이루어지며, 데이터의 물리적 위치와 관리 주체가 해당 국가 내에 한정됨
데이터 주권 확보	- 자국 내에서 데이터의 저장과 통제를 수행함으로써 외국 정부나 제3자의 접근 위험을 차단하고 자국민 데이터의 주권을 보장함
퍼블릭 클라우드 한계 보완	- 글로벌 퍼블릭 클라우드의 구조적 한계(국경 간 데이터 이동, 외국 법률 적용 등)를 보완하기 위해 등장
법적 안정성 확보	- 자국 법체계 하에서 데이터가 관리되어 법적 불확실성과 해외 법률 적용 위험을 최소화함
고보안·고규제 산업 중심 도입	- 정부, 금융, 국방 등 보안성과 규제 준수가 필수적인 산업 분야에서 우선적으로 채택됨
핵심 가치	- 데이터 주권(Data Sovereignty)과 규제 준수(Compliance)를 보장하는 국가 중심의 클라우드 인프라 모델

- 소버린 클라우드는 국가가 요구하는 보안·규제 기준을 충족하며 데이터 주권을 강화하는 클라우드 모델

II. 소버린 클라우드와 퍼블릭 클라우드의 비교

가. 소버린 클라우드와 퍼블릭 클라우드의 운영 방식 비교

구분	소버린 클라우드	퍼블릭 클라우드
개념	- 특정 국가의 법·규제·데이터 주권을 준수하도록 설계된 국가별 전용 클라우드	- 전 세계 누구나 이용할 수 있는 글로벌 범용 클라우드 서비스
초점	- 데이터 주권, 규제 준수, 보안, 국가 통제	- 확장성과 비용 효율성, 전 세계적 접근성
운영 방식	- 특정 국가 내 인가된 사업자/국가기구 중심 운영	- 글로벌 사업자가 전 세계에서 일괄 운영
데이터 주권	- 특정 국가 및 지역 내 데이터 저장 및 처리	- 데이터 저장에 국가 간 경계 없음
물리적 측면	- 데이터센터의 물리적 위치를 특정 국가로 제한	- 데이터센터의 물리적 위치 제한 없음
운영·관리 주체	- 보안 허가·시민권·거주 요건 등으로 제한	- 글로벌 클라우드 서비스 공급업체가 전담 운영
장점	- 높은 보안 수준 - 데이터 저장 위치·운영자·접근 권한을 국가가 직접 통제	- 글로벌 확장성, 높은 유연성 - 다양한 서비스·최신 기술 활용 가능 - 저렴한 비용·기반 인프라 자동 확장
단점	- 구축·운영 비용 증가 - 글로벌 확장성 제한 - 서비스 다양성 부족, 보안 인가 필요	- 데이터 주권 및 규제 준수 어려움 - 물리적 데이터 경계 불명확 - 특정 국가 정책·법령 적용 시 운영 복잡성 증가
활용분야	- 정부, 국방, 금융, 헬스케어 등 민감 영역	- 제조, 물류, 유통 등 범용 민간 분야

- 소버린 클라우드가 국가 통제와 주권 보장을 중심으로 설계되는 반면, 퍼블릭 클라우드는 글로벌 확장성과 효율성을 우선하는 구조적 차이가 존재

나. 소버린 클라우드와 퍼블릭 클라우드의 보안·규제 준수 체계 비교

구분	소버린 클라우드	퍼블릭 클라우드
암호화 키 관리	- BYOK/HYOK 등 사용자가 통제하거나 국가가 관리 가능	- CSP가 키를 관리하거나 해외 거점에서 운영 가능
접근 통제	- 보안 허가, 국적·거주 요건 등 강화된 접근 통제 적용	- 접근자 국적·거주지 제한 거의 없음
네트워크 보안	- 전용 네트워크를 통해 기밀성·무결성 보장	- 전용망 의무 없음(일반 인터넷 기반도 가능)
규제 준수	- 국가 법률·산업 규제에 맞춰 아키텍처·운영 정책 설계	- 규제 준수는 계약·설정 과정에 의존
보안 측면 장점	- 고보안 요구 충족, 국가 기준 보안 정책 직접 적용	- 최신 보안 기능 활용 가능, 글로벌 표준 준수
보안 측면 한계	- 높은 비용·관리 부담, 기술 다양성 제한	- 데이터 주권 확보 어려움, 규제 충돌 발생 가능

- 소버린 클라우드는 국가 규제와 데이터 주권을 우선하는 반면, 퍼블릭 클라우드는 글로벌 확장성과 비용 효율성을 중점으로 하는 클라우드 모델

III. 소버린 클라우드 주요 기술

가. 소버린 클라우드의 주요 원칙 관련 핵심 기술

주요 원칙	핵심 기술	설명
데이터 주권 및 관할권	- 의무적 기업 규칙(BCR) - 개인정보보호강화기술(PET)	- 모든 데이터는 관할권 내 수집 및 통제, 독점적 운영/관리 - 데이터 레지던시, 레이턴시, 보안 요건 준수
데이터 액세스 및 무결성	- 접근 통제/서명 - 암호화	- 관할 구역 내 최소 2 개 이상의 데이터 센터 구성 - 클라우드 복원력 증가 , 안전한 연결
데이터 보안 및 규정 준수	- 보안 모니터링 - EDR/XDR	- 산업 및 지역 규제(법규 및 표준)의 특수성 반영 가능 - 주기적 감사(Audit)
데이터 독립성 및 이동성	- Micro Segmentation - 제로 트러스트	- 벤더 클라우드 종속성 방지 - 애플리케이션 이식성 및 독립성 제공

- 소버린 클라우드는 데이터 주권·보안·무결성·독립성을 보장하기 위해 고보안 기술을 기반으로 운영

나. 소버린 클라우드의 세부 기술

구분	기술	설명
데이터 보안 및 암호화	고급 암호화 표준	- AES-256 등 전송·저장 시 암호화 적용, KISA 승인 암호 기술 사용 적합성 검증 필요
	고객 키 관리(BYOK/HYOK)	- 고객이 직접 키를 생성·관리(BYOK), 전용 HSM·보안 HW에서 키 유지(HYOK)
	기밀 컴퓨팅(Confidential Computing)	- CPU·메모리 처리 중에도 데이터를 암호화된 상태로 유지(TEE, SGX 등)
	데이터 주권	- 데이터가 특정 국가 밖으로 유출되지 않도록 저장 위치·암호화 정책을 강제
	데이터 사용 제어	- 암호 해제 후에도 데이터 복제·전송 제한(ABE·DRM·정책 기반 제어)
접근제어 및 ID 관리	다단계 인증(MFA)	- 생체·OTP·SMS·하드웨어 토큰 기반 2단계 이상 인증
	RBAC(역할 기반 접근)	- 사용자 역할 기반 리소스·데이터 접근 통제
	지리·국적 기반 접근제어	- IP·GPS·국가 식별 기반 허용 국가만 접근 가능
	제로트러스트(Zero Trust) 적용	- 사용자·기기·네트워크 모든 요청에 연속적 검증 수행
	ID 연계·국가 인증체계 연동	- DID, FIDO2 기반 국가 신원 인증체계와 연계하여 주권적 접근 강화
물리적 격리	단일 테넌트(Single Tenant)	- 특정 고객 전용 하드웨어·네트워크 제공으로 논리·물리적 분리
	에어갭(Air-Gapped)	- 인터넷과 완전 분리된 고보안 환경 제공

	국가 지정 영역 내 위치 (Locality Zone)	- 데이터 저장·처리를 특정 국가·특정 IDC 내에서만 실행하도록 보장
	보안운영물리센터	- 국가 승인된 장소에서만 운영·접근 가능한 보안운영 구역 구성
컴플라이언스	규제준수 모니터링	- 데이터 보호법·전송규제 준수 현황 자동 모니터링
	투명 로깅·감사	- 모든 접근·처리 활동을 국가 감사 기준에 맞게 기록
	디지털 주권 규제 준수 엔진	- 국가·산업별 규제(K-ISMS, GDPR, 금융 규정 등)를 자동 점검·보고
	데이터 검증 불변성 (Immutable Audit)	- 감사 로그를 삭제·위변조 불가하도록 Blockchain·WORM 적용
운영 및 인력 통제	현지 인력 운영	- 운영·보안 담당자를 해당 국가 시민권으로 구성
	국가 내 데이터센터 위치	- 데이터 저장·백업 모두 국가 지정 영역 내 배치
	운영행위 통제	- 외국 인력·MSP의 원격 접속 제한, 모든 행위 기록·승인
	보안 운영 자동화	- 규제준수·보안정책을 자동 배포 및 강제(AIOps·SOAR)

- 소버린 클라우드는 국가 규제 중심의 보안·통제 기술로 데이터를 보호하고 주권을 보장하는 인프라

IV. 소버린 클라우드의 고려사항

구분	고려사항	설명
데이터 주권·규제 준수	국가별 데이터 주권 준수	- 데이터 생성·저장·처리가 해당 국가 내에서만 이루어지도록 법·규제 충족 필요
	지역·산업 규제 반영	- 금융, 국방, 의료 등 산업별 컴플라이언스 규정(금융보안원, HIPAA 등)을 아키텍처에 반영
	데이터 경계 설정	- 물리적·논리적 데이터 경계를 국가 단위로 분리해 해외 유출 가능성 차단
보안·접근 통제	접근 주체 제한	- 운영 인력을 시민권 보유자, 보안 인가자 등으로 제한하여 내부 위협 감소
	암호화·키 관리 체계 강화	- 고객 또는 국가기관 주도의 KMS/HSM 운영, 키 해외 반출 금지
	물리적 보안 강화	- 국가 내 소재 데이터센터의 물리 보안 수준(출입통제·CCTV·보안인증) 확보
아키텍처·네트워크 디자인	전용 네트워크 구축	- 공용 인터넷이 아닌 전용선 기반 통신으로 기밀성·무결성 확보
	멀티존·재해복구 구성	- 동일 국가 내 이중화·DR 센터 구성으로 가용성 확보
	글로벌 클라우드와의 분리	- 퍼블릭 클라우드 리전과 네트워크/관리 영역 완전 분리 설계 필요
운영·관리 체계	인가된 운영 인력	- 국가 보안요건을 충족하는 인력으로 운영 인원을 제한
	투명한 로그 및 모니터링	- 접근 로그·API 호출·보안 이벤트를 중앙에서 기록·감사
	업데이트·패치 절차 통제	- 공급업체 패치가 국가 규제를 위배하지 않는지 검증 후 적용

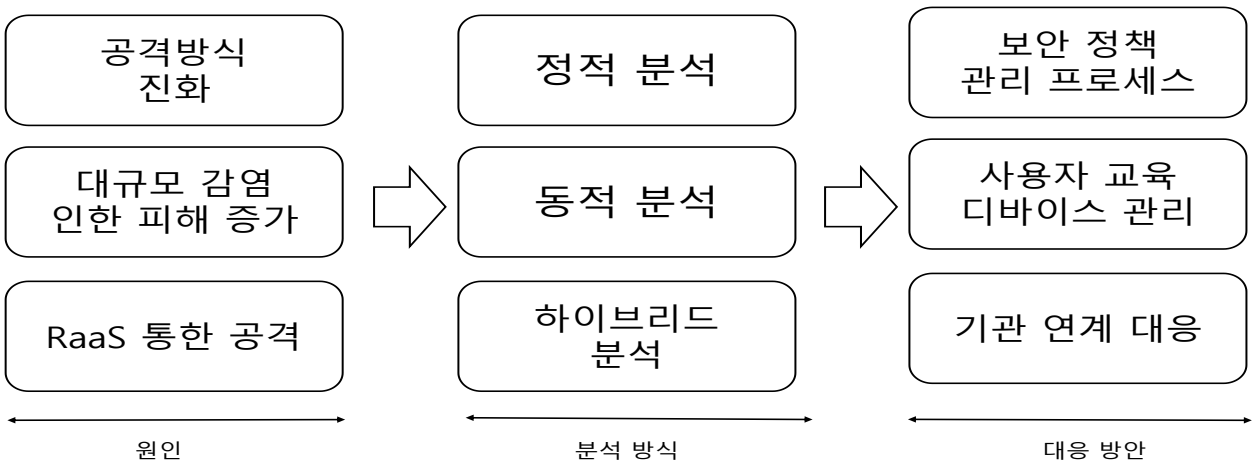
서비스·거버넌스	SLA 및 규제 준수 보장	- 데이터 주권·보안·가용성에 대한 SLA를 국가 규제와 일치하도록 설정
	공공·민감 서비스 우선 적용	- 국방·정부·금융·의료 등 민감 데이터 활용 영역에 우선 적용 필요
	공급망(Supply Chain) 검증	- 하드웨어·소프트웨어 공급망에 대한 위조·취약점 검증 필수

- 소버린 클라우드는 국가 규제 준수, 강력한 보안·접근 통제, 물리·논리적 분리, 현지 운영 체계 등 국가 수준의 통제 요구사항을 충족하도록 설계·운영되어야 함.

"끝"

06	랜섬웨어		
문제	최근 랜섬웨어 공격으로 인한 기업 피해가 증가함에 따라 공공기관 및 기업에서는 랜섬웨어 공격에 대한 대응방안 마련의 필요성이 증가하고 있다. 다음에 대해 설명하시오. 가. 랜섬웨어의 유형 및 감염 증상 나. 랜섬웨어의 분석 방법 다. 랜섬웨어 대응방안		
도메인	보안	난이도	중 (상/중/하)
키워드	백업, 정적분석, 동적분석, 암호화형, RaaS		
출제배경	최근 대규모 랜섬웨어로 인한 기업 피해 확산 사례 관련 랜섬웨어에 대한 전반적인 지식 확인		
참고문헌	ITPE 기술사회 서브노트		
출제자	이다연 기술사(제 135회 정보관리기술사 / dlekdusz@naver.com)		

I. 데이터 인질 이용 금전 요구 공격 방식, 랜섬웨어의 개념



개념	- 사용자의 중요 데이터를 암호화거나 시스템 사용을 불가능하게 만든 후, 복호화의 대가로 금전(몸값)을 요구하는 악성 소프트웨어

- 최근 대기업에 대한 랜섬웨어 공격 증가로 인해 대규모 개인정보 유출 및 금전적 피해가 기하급수적으로 증가

II. 랜섬웨어의 유형 및 감염 증상

가. 랜섬웨어의 유형

구분	유형	설명	사례
감염 방식	- 암호화형 (Crypto)	- 파일 암호화하여 접근 불가	- CryptoLocker - WannaCry
	- 잠금형 (Locked)	- OS 화면을 잠가서 기기 사용 불가	- Police Locker

	- 공포형(Scareware)	- 가짜 감염 메시지로 불안조성하여 금전 결제 유도	- WinFixer
행위 기반	- 정보유출 협박형 (Doxware/Leakware)	- 민감 정보 탈취 후 금전 요구	- DoppelPaymer
	- 복합형(Hybrid)	- 정보 유출+시스템 파괴 등 복합 공격	- Ryuk
공급방식 기반	- RaaS (Ransomware-as-a Service)	- 공격자가 랜섬웨어 제작을 의뢰 - 서비스 구매자가 공격 가능	- Cerber

나. 랜섬웨어의 감염 증상

구분	감염 증상	설명
데이터 접근 문제	- 파일 암호화	- 사용자 주요 파일 사용 불가 상태로 변환
	- 파일 삭제/이름변경	- 랜섬웨어 흔적 제거 위한 원본 파일 삭제
시스템 동작 오류	- 화면 잠금	- 사용자의 전자기기 화면 잠금
	- 부트영역 암호화	- 운영체제 시작 위한 영역 암호화하여 기기 사용 불가
	- 시스템 파괴	- 주요 메모리영역 데이터 삭제하여 오류 유발

- 랜섬웨어 감염 대응 위해 공격에 대한 사전 분석 필요

III. 랜섬웨어의 분석 방법

가. 정적분석(static Analysis) 설명

구분	설명	
개념	- 랜섬웨어를 실행하지 않고 외형을 분석하여 구조 및 기능, 예상되는 감염 증상을 찾아내는 분석 기법	
장점	- 높은 안전성	- 비실행 방식으로 분석 - 샌드박스 불필요
	- 정책 수립 효율성	- 요구메시지, 암호화 루틴 사전 분석하여 대응 가능
단점	- 동작 행위 분석 불가	- 비실행 방식 분석으로 실제 동작에 대한 예측 부정확 - 오탐 가능성 존재
	- 분석 불가 랜섬웨어 존재	- 난독화된 랜섬웨어는 분석 불가

- 정적 분석방식으로는 랜섬웨어의 정확한 분석이 어렵기 때문에 동적 분석 방식을 이용하여 추가 분석 수행

나. 동적분석(Dynamic Analysis) 설명

구분	설명	
개념	- 랜섬웨어를 실행 가능한 환경에서 실행시킨 후 동작 행위 및 공격 방식을 분석하는 기법	
장점	- 실제 증상 확인 가능	- 실제 실행 통한 동작 방식 분석 - 공격 흐름 분석 가능

	- 대응 방안 도출 용이	- 공격 패턴 및 감염 증상을 확인하여 실제 대응방안 마련
단점	- 격리 환경 필요	- 샌드박스와 같은 격리 환경 필수 - 격리 환경 안전성 추가 확인 필요
	- 분석 회피 (Anti-sandbox) 기술에 취약	- 분석 환경 감지 시 정상 코드처럼 실행하는 기술이 이용된 경우 분석 불가

- 정적분석과 동적분석의 한계점 보완하기 위한 하이브리드 분석 방식으로 랜섬웨어 분석 가능

다. 하이브리드 분석(Hybrid Analysis) 설명

구분	설명	
개념	- 정적 분석과 동적 분석의 결과를 서로 상관시켜 랜섬웨어를 분석하는 기법	
장점	- 분석 정확도 증가	- 정적 방식으로 구조, 특징 파악 - 동적 방식으로 실제 행위 추적
	- 높은 재현성, 정확성	- 대규모 보안 대응방안 수립에 적합
단점	- 분석 시간 증가	- 정적/동적 분석 방식 전체 수행 후 상관관계 파악 - 분석 시간 증가 따른 추가 비용 증가 가능성
	- 전문 지식 필요	- 고도화된 분석 환경 이용 위한 분석 전문지식 요구

- 랜섬웨어 분석과 함께 감염 및 확산 방지 위한 관리적/기술적 대응방안 마련 필요

IV. 랜섬웨어 대응방안

가. 관리적 관점 랜섬웨어 대응방안

구분	대응방안	설명
설비	- 백업체계 수립	- 공격 시 백업 데이터 이용 데이터 복구 체계 마련
	- 대응 계획 수립	- 감염 시 대응시간 최소화하여 시스템 복구
	- 접근통제 체계 마련	- 이용자들 기기 통한 랜섬웨어 감염 최소화
정책	- 주기적 교육 수행	- 상시, 주기적 랜섬웨어 위험성 전파
	- 버그바운티 활용	- 제품 취약점 조기발견, 대응방안 수립
외부	- 침해 사례 전파	- 다양한 사례 기반 대응방안 다각도 마련
	- 전문 기관 상담	- 피해신고, 대응방안, 점검 수행
사용자	- 중요 자료 분리 보관	- 중요 파일에 대한 감염 피해 최소화
	- SW 최신 패치	- 취약점 패치 통한 최신 보안 상태 유지
	- EoS 제품 미사용	- 보안 취약점 패치 불가한 SW 사용 지양
	- 신뢰 사이트 이용	- 관심 키워드 악용 사이트, 악성 메일 경로 접속 금지

- 백업 체계를 수립하여 감염 시 데이터 유실 최소화 및 신속한 복구를 하는 것이 중요

나. 기술적 관점 랜섬웨어 대응방안

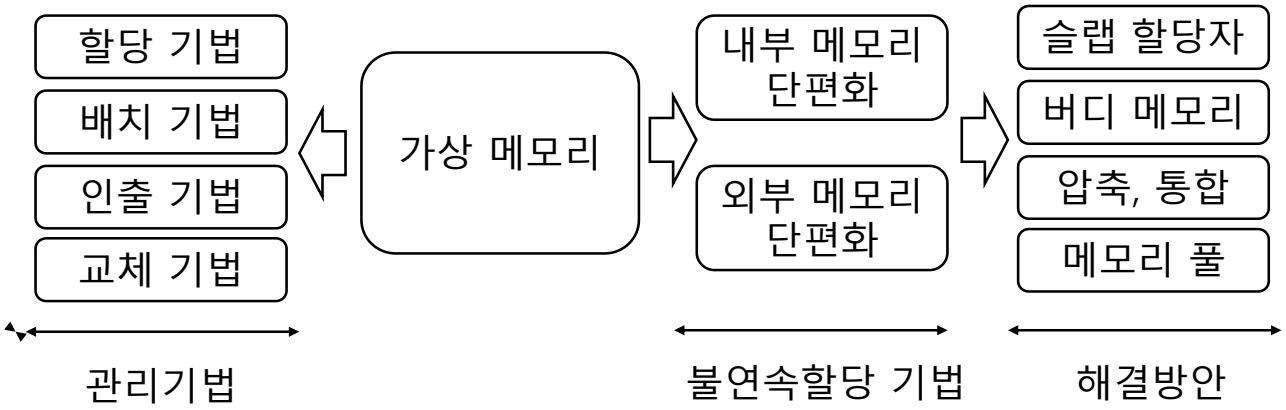
구분	대응방안	설명
N/W 보안	- 방화벽, IDS/IPS	- 악성IP 및 네트워크 공격 차단
	- WAF, 웹 관제	- 상시 네트워크 모니터링 통한 감염 사전 예방
	- 샌드박스, APT	- 악성 코드 분석 위한 환경 마련
Device	- EDR	- IoC, 머신러닝 통해 랜섬웨어 초기 발견/대응
	- WhiteList 적용	- 검증된 인터넷 사이트만 접속 허용하여 감염 경로 차단
Platform	- SIEM, SOAR	- 통합 관제 시스템 이용하여 감염 경로 확인
	- Zero Trust	- 모든 접근에 대한 권한 부여 전 인증 통해 접근 차단
사용자	- 스마트 필터링	- 브라우저 이용 시 악성 코드 차단
	- 백업 프로그램	- 중요 자료 백업 통한 감염 피해 최소화
	- 공용 백신 프로그램	- 개인 디바이스의 감염 여부 상시 모니터링
	- OS 업데이트	- 최신 보안 취약점 패치 통해 사용자 디바이스 통한 랜섬웨어 감염 차단

- 랜섬웨어 대응 가이드라인 기반 랜섬웨어 사전 예방 방안 마련 통해 랜섬웨어 감염 피해 최소화 가능.

"끝"

06	가상 메모리 관리		
문제	가상 메모리 관리 기법에 대해 다음을 설명하시오. 가. 가상 메모리 관리기법 나. 페이징(Paging) 기법과 세그멘테이션(Segmentation) 기법 다. 메모리 단편화		
도메인	CA	난이도	하 (상/중/하)
키워드	할당, 배치, 인출, 교환, 페이징, 세그멘테이션, 외부단편화, 내부단편화		
출제배경	가상 메모리 관리기법의 기본적 이해		
참고문헌	ITPE 기술사회 서브노트		
출제자	이다연 기술사(제 135회 정보관리기술사 / dlekdusz@naver.com)		

I. 메모리의 확장적 사용 위한, 가상 메모리 관리의 개념

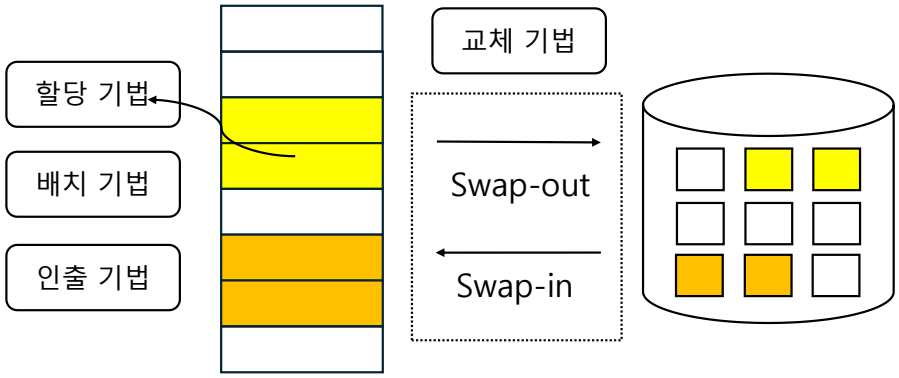


개념	- 물리적 메모리의 한계를 극복하고 다수의 사용자에 의한 메모리 공유를 위해 가상 메모리를 할당, 배치, 인출, 교체 기법을 사용하여 관리하는 기법

- 메모리를 프로세스에 효율적으로 할당하고 단편화 문제를 최소화하여 성능을 향상시킬 수 있도록 가상 메모리 관리 기법 활용

II. 가상 메모리 관리 기법 설명

가. 가상 메모리 관리 기법 개념도



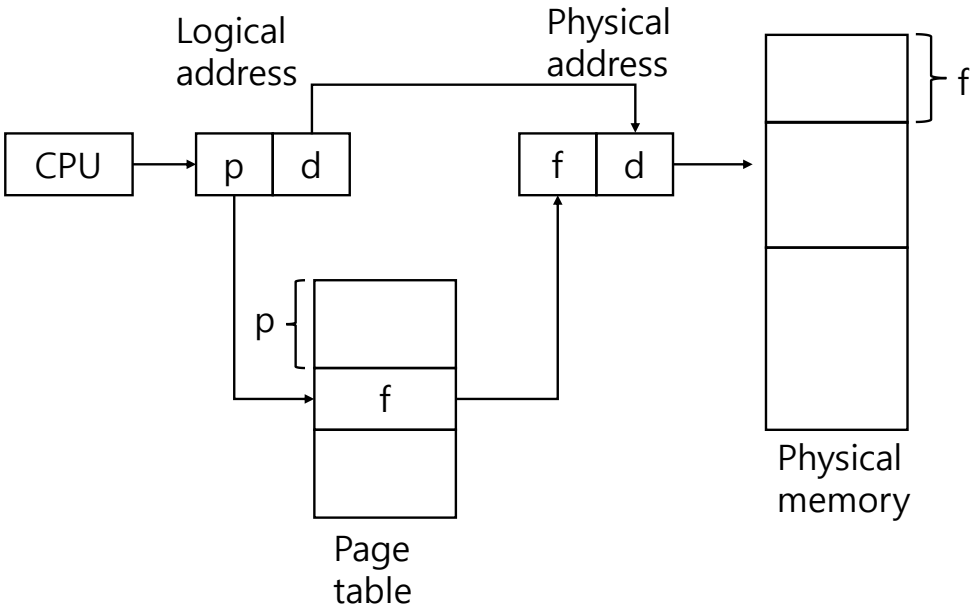
- 할당, 배치, 인출, 교체의 4가지 방법을 통해 가상 메모리를 효율적 관리 가능

나. 가상 메모리 관리 기법 상세 설명

구분	관리 기법	설명
할당 기법 (Allocation)	- 연속 할당 기법	- 고정할당(정적) 기법, 가변할당(동적) 기법
	- 불연속 할당 기법	- 페이징(Paging), 세그멘테이션(Segmentation), 페이지드 세그멘테이션(Paged-Segmentation) 기법
배치기법 (Placement)	- First-Fit	- 가장 처음에 남는 공간에 할당하는 기법
	- Best-Fit	- 전체 스캔 후 가장 적합한 공간에 할당하는 기법
	- Next-Fit	- 최근 할당 블록의 다음 위치에 할당하는 기법
	- Worst-FIt	- 가장 적합하지 않은 공간에 할당하는 기법
인출기법 (Fetch)	- 요구 인출(Demand Fetch)	- 실행 프로그램이 메모리 요구 시 참조된 페이지나 세그먼트를 주기억장치로 옮기는 기법
	- 예측 인출(Pre Fetch)	- 실행 프로그램에 의해 참조될 것을 예측하여 미리 주기억장치로 옮기는 기법
교체기법 (Replacement)	- FIFO(First In First Out)	- 가장 먼저 들어온 페이지 교체
	- LFU(Least Frequently Used)	- 현재 기준 사용 횟수가 가장 낮은 페이지 교체
	- LRU(Least Recently Used)	- 현재 기준 가장 오랫동안 사용되지 않은 페이지 교체
	- OPT(Optimal Page)	- 가장 오랫동안 사용되지 않을 페이지 교체
	- NUR(Not Used Recently)	- 최근 사용되지 않은 페이지를 2bit 이용하여 교체

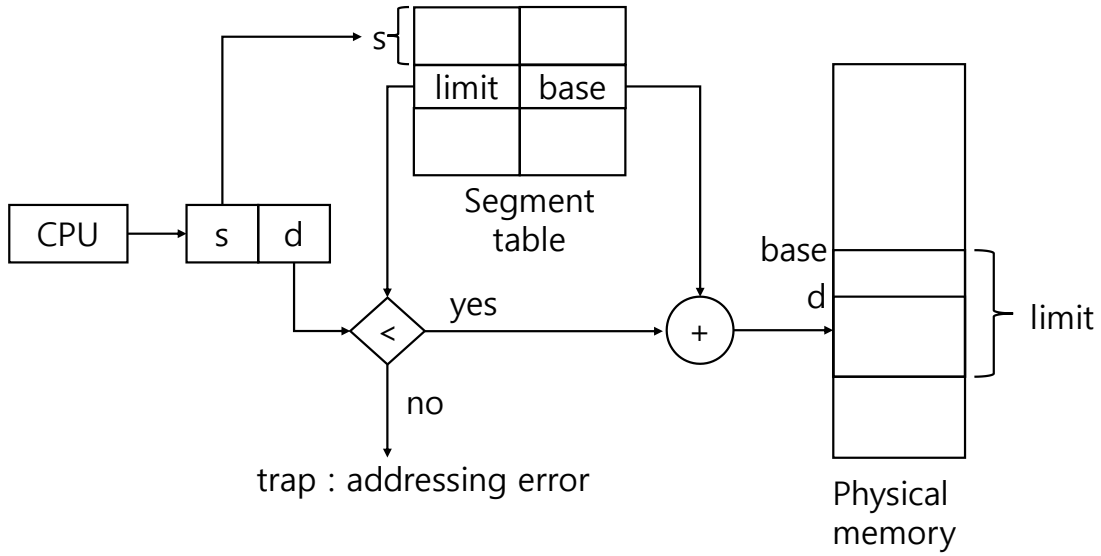
III. 페이징(Paging) 기법과 세그멘테이션(Segmentation) 기법 설명

가. 고정 분할 기법, 페이징(Paging) 기법 설명

구분	설명	
개념	- 메모리를 고정된 크기의 프레임/페이지로 나누어 페이지 번호와 프레임 번호를 매핑하여 할당하는 메모리 관리 기법	
개념도		
구성요소	- 가상주소	- 가상 페이지 번호와 오프셋으로 구성
	- VPN	- 가상 페이지 번호(Virtual Page Number)
	- PPN	- 물리적 페이지 번호(Physical Page Number)
	- 제어 부분	- 페이지에 대한 접근권한 필드와 페이지가 메모리에 존재하는지 나타내는 비트
동작방식	P : page number , f : frame number(Physical address), d : page offset ① logical address 의 주소 이용 page number 확보 ② page table에서 해당 page에 있는 frame number 확보 ③ frame number + page offset으로 물리 메모리 주소 확인	

나. 동적 분할 기법, 세그멘테이션(Dynamic Analysis) 기법 설명

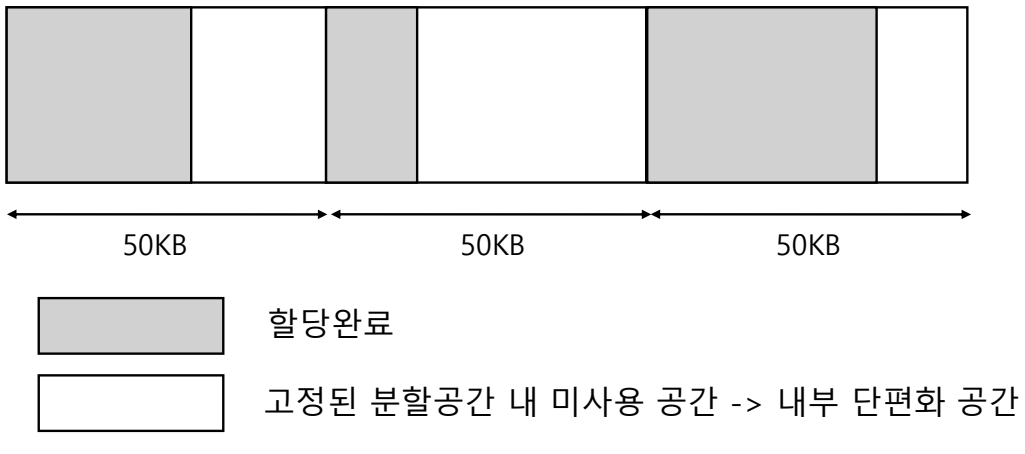
구분	설명
개념	- 메모리를 필요한 크기만큼 가변적으로 분할하여 논리적 블록 단위인 세그먼트로 할당하는 메모리 관리 기법

개념도		
구성요소	- 세그먼트 테이블	- 가상 페이지 번호와 오프셋으로 구성
	- Limit	- 세그먼트마다 제한된 크기를 사용하여 가변적으로 할당
	- Based address	- 각 세그먼트의 기준이 되는 주소
동작방식	S : segment number, d : page offset ① segment address의 주소 이용 segment number 확보 ② segment table에서 시작 주소(base)와 길이(limit) 확보 ③ segment + offset으로 물리 메모리 주소 확인	

- 페이징 기법과 세그멘테이션 기법 사용 시 메모리 단편화 문제 발생 가능성 존재

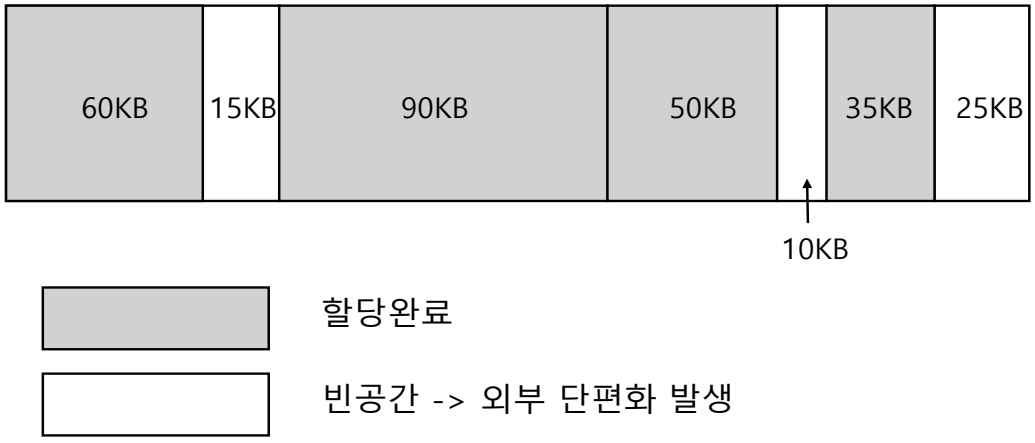
IV. 메모리 단편화 설명

가. 내부 단편화 설명

구분	설명	
개념	- 가상 메모리 할당 시 프로세스가 필요한 크기보다 큰 메모리가 할당되어 메모리 공간이 낭비되는 문제	
개념도		
발생원인	- 할당 영역과의 크기 차이	- 분할된 영역 > 프로그램 크기

	- 고정 분할 기법 사용	- 고정 분할 기법 사용 시 프로그램 크기와 상관없이 메모리를 분할, 할당하기 때문에 낭비 영역 발생
해결방안	- 슬랩할당자(Slab Allocator) 기법	- 페이지 프레임을 할당 받아 작은 크기로 분할, 메모리 요청시 작은 크기로 메모리 할당을 해제하는 기법 - 할당 받은 프레임을 미리 작은 크기로 분할하여 자주 할당되고 해제되는 크기의 캐시 구성 (Cache -> slab -> object로 구성)

나. 외부 단편화 설명

구분	설명	
개념	- 할당 가능한 가상 메모리 위치가 불연속적이기 때문에 사용 가능한 공간이 남아있는 경우에도 할당이 불가능하여 낭비되는 상태	
개념도		
발생원인	- 불연속 할당	- 빈 공간의 합산은 프로그램 크기보다 크거나 같지만 위치가 불연속적이기 때문에 할당 불가
	- 가변 분할 기법 사용	- 메모리를 필요한 크기만큼 가변적으로 분할하여 불연속적 메모리 낭비 공간 발생 가능
해결방안	- 버디 메모리 시스템 (Buddy Memory System)	- 요청 프로그램 크기에 맞게 메모리를 할당하기 위해 2의 거듭제곱 크기로 분할하여 할당하는 방식 - 메모리 해제 시 인접 메모리가 비어있으면 free 버디를 합치는 방식을 반복 수행

- 통합, 압축, 재배치, 메모리풀 과 같은 방식으로 내/외부 단편화 해결 가능

"끝"

제 39 회 ITPE
실전 명품 모의고사 해설집

대 상 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사, 정보시스템감리사 시험
발행일 2025년 12월 21일
집 필 강정배 PE, 전일 PE, 이상헌 PE, 소민호 PE, 현수 PE, 박서현 PE, 배미경 PE
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
ITPE 을지로점 서울시 중구 삼일대로 363, 2615호(장교동 장교빌딩)
ITPE 강북점 서울 종로구 수표로 96, 7층 (관수동,국일관드림팰리스)
연락처 070-4077-1267 / itpe@itpe.co.kr