제133회 정보관리기술사 해설집

2024.05.18

국가기술자격 기술사 시험문제

기술사 제 133 회 제 4 교시 (시험시간: 100 분)

분야	정보통신	자격종목	정보관리기술사	수검번호		성명	

※ 다음 문제 중 4 문제를 선택하여 설명하시오. (각 10 점)

1. 데이터 중심 사회에서 데이터의 프라이버시와 보안은 매우 중요한 이슈로 부상하고 있고, 이를 해결하기 위한 다양한 기술적 접근이 시도되고 있다. 그러한 시도 중에서 다자간 계산(Multi-Party Computation; MPC)에 대하여 다음을 설명하시오.

   가. MPC 개념, 원리, 특징

   나. MPC 기술 종류

   다. MPC 기반 인증서비스

2. 정보시스템 개발과 운영 단계에서 수행되는 소프트웨어 테스트의 종류를 쓰고, 이 중 신뢰성 테스트와 이식성 테스트의 세부 활동에 대하여 각각 설명하시오.

3. 정보보호 방법을 암호화와 접근제어로 크게 분류할 때, 접근제어에 대하여 그 개념과 정책, 절차, 그리고 이를 구현하는 매커니즘에 대하여 설명하시오

4. DBMS 를 적용하기 위한 데이터 모델링에 대하여 다음을 설명하시오.

가. 데이터 모델링의 개념 및 모델링 단계별 수행내용

나. 데이터 관계 모델링 시 식별(Identification)과 비식별(Non Icentification)에 대하여 비교

다. 데이터 모델링 시 고려사항

5. 5G 특화망을 위한 네트워크를 구축할 때 고려되어야 할 사항에 대하여 다음을 설명하시오.

가. 안정성 및 신뢰성 확보 방안

나. 간섭회피 방안

6. VPN (Virtual Private Network)에 대하여 다음을 설명하시오.

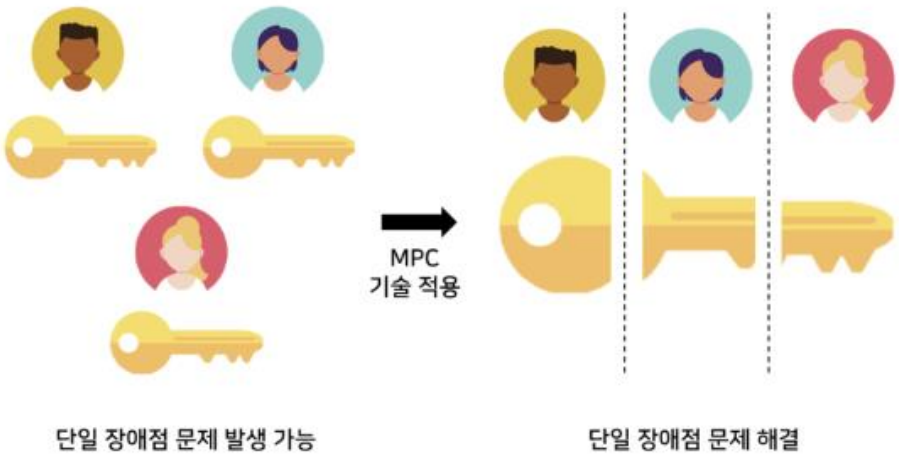
가. VPN 의 개념 및 특징

나. IPSec (Internet Protocol Security) VPN 과 SSL(Secure Socket Layer) VPN

다. VPN 의 기술요소

01	다자간 계산(Multi-Party Computation; MPC)		
문제	데이터 중심 사회에서 데이터의 프라이버시와 보안은 매우 중요한 이슈로 부상하고 있고, 이를 해결하기 위한 다양한 기술적 접근이 시도되고 있다. 그러한 시도 중에서 다자간 계산(Multi-Party Computation; MPC)에 대하여 다음을 설명하시오. 가. MPC 개념, 원리, 특징 나. MPC 기술 종류 다. MPC 기반 인증서비스		
도메인	보안	난이도	상(상/중/하)
키워드	비밀 분할, 베이버 트리플, Garbled Circuits, Oblivious Transfer		
출제배경	분산 환경이 확산됨에 따라, 분산 기술을 이용한 암호 기술 확인		
참고문헌	Fintech를 위한 다자간 컴퓨팅 암호기술, 디지털산업정보학회 논문 (박찬길 외 2인) 생체인증, 디지털 자산을 보호하는 다자간 컴퓨팅 기술(MPC) (펜타 시큐리티 블로그) "신뢰할 수 없는 환경에서 신뢰를 확보한다" SMPC란 무엇인가" (https://www.itworld.co.kr/news/203304) MPC 기술의 이해와 적용 사례 (최대선 / 전자금융과 금융보안 2024-1Q)		
해설자	모멘텀 안수현 기술사(제119회 정보관리기술사 / tino1999@naver.com)		

I. MPC 개념, 원리, 특징

구분	설명	
개념	- 둘 이상의 참여자가 각자의 비밀 데이터를 보유한 채로 공동의 계산 목표를 달성할 수 있도록 하는 암호학적 기법	
원리	 (그림출처 : 펜타시큐리티 블로그)	
	- 데이터를 암호화한 상태로 처리하고, 최종 결과만이 복호화 - 참가자는 자신의 데이터를 직접적으로 공개하지 않고, 암호화된 형태로만 참여하여 연산을 수행	
특징	비밀 유지	각 참여자의 데이터는 다른 참여자에게 노출되지 않음
	결과의 정확성	모든 참여자가 동의한 규칙에 따라 처리된 정확한 결과를 도출
	탄력성	일부 참여자가 비협조적이거나 공격을 시도하더라도 시스템의 안정성을 유지

II. MPC 기술 종류

구분	기술	설명
비밀 분할 기반	비밀 분할 (Secret Sharing)	- 데이터 또는 비밀을 여러 조각으로 나누고, 이 중 일정 수 이상의 조각이 모여야만 비밀을 복원할 수 있도록 하는 기술
	베이버 트리플 (Beaver Triples)	- 사전 계산된 값들로, 특히 곱셈 연산을 보다 효율적으로 수행할 수 있게 해주는 기술 - MPC의 핵심 문제 중 하나인, 데이터 공개 없이 여러 참가자가 공동으로 데이터를 계산하는 과정을 최적화 하는 기술
	동형 암호	- 암호화된 데이터에 대해 연산을 수행할 수 있으며, 연산 결과도 암호화된 형태로 출력되는 암호 기술
회로 기반	Garbled Circuits	- Yao's Garbled Circuits 프로토콜이라고 하며, Boolean 회로를 기반으로 함 - Boolean 회로를 암호화하여, 입력값을 숨긴 채 계산을 수행할 수 있게하는 기술
	Oblivious Transfer	- 송신자가 어떤 정보를 수신자에게 전달했는지 수신자만 알 수 있게 하는 프로토콜 - Garbled Circuits과 함께 사용되며, 보다 복잡한 계산에서 입력값의 비밀을 유지하면서 처리 될 수 있도록 함

- 동형 암호는 엄밀히 MPC의 기술은 아니지만, 데이터를 암호화한 상태로 연산을 수행 할 수 있는 기술

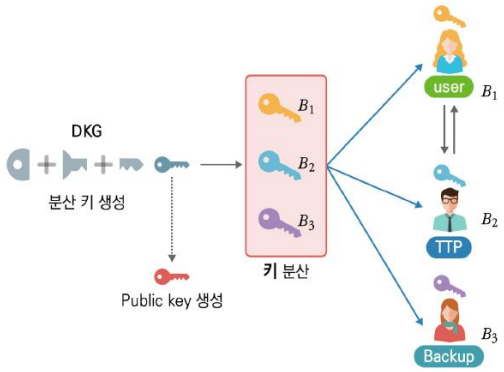
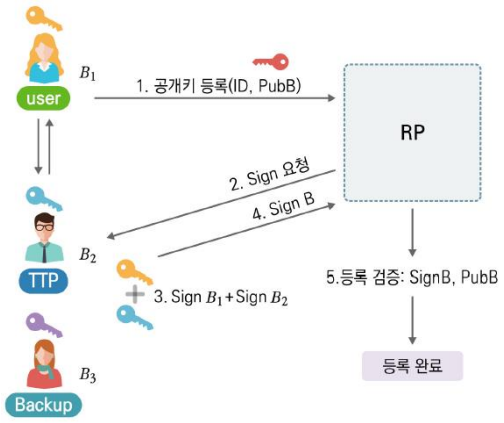
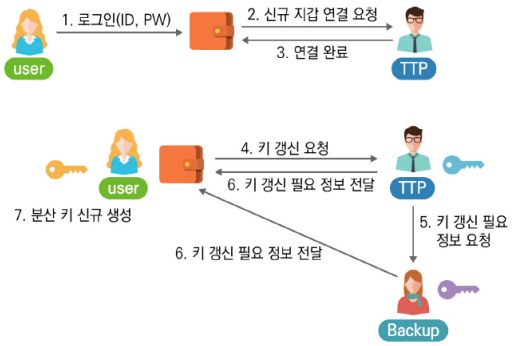
III. MPC 기반 인증서비스

가. MPC 기반 인증서비스 구성 요소

구성요소	설명
User	- 분산 키 생성 및 저장, 배포와 검증, 분산 서명 생성을 할 수 있는 지갑 형태의 애플리케이션을 보유한 통상의 사용자
TTP (Trusted Third Party)	- 분산 키 생성 및 저장, 배포와 검증, 분산 서명 생성을 할 수 있는 서버 형태의 신뢰 서비스
Backup	- 분산 키 생성 및 저장, 배포와 검증, 분산 서명 생성을 할 수 있는 서버 형태의 서비스로, 통상의 백업서버와 달리, user의 키를 보관하는 것이 아닌 분산 서명에 참여하는 형태로 백업을 달성
RP (Relying Party)	- 사용자를 인증하려는 통상의 서비스

- 인증서비스를 구현하기 위해 비밀 공유 기술과 임계값 서명 기술을 활용

나. MPC 기반 인증 시스템의 동작 흐름

구분	개념도	설명
분산키 생성		- user와 TTP, Backup은 공동으로 임계값 서명을 위한 키 쌍을 생성 1) 각각은 자신의 개인 키 생성 2) 개인키에 부합하는 공개 파트와, 여기에 해상하는 개인 키 소유 증명을 모두에게 브로드캐스트 3) 각각은 수신된 공개 파트와 소유 증명을 검증 4) 자신의 부분 공개 파트와 수신된 공개 파트를 조합 후 공통 공개 키 생성 - 이 절차 이후 각각은 자신의 개인 키와 공통 공개키를 갖게 됨
RP 등록		- user는 RP에 사용자 등록을 하며 인증 크리덴셜로 공개 키를 제출한다. 1) user는 ID와 함께 공개 키를 RP에 제출 2) RP는 공개 키에 대한 소유 증명을 user에게 요청. 이 과정은 보통 챌린지 값에 대한 서명 요구 포함 3) user는 자신의 개인 키로 챌린지 값에 대해 부분 서명을 생성해 TTP로 전송. TTP도 자신의 부분 서명을 생성. TTP는 user의 서명 값과 자신의 서명값을 결합하여 결합 서명 생성 4) TTP가 결합 서명을 RP에 제출 5) RP는 1번에서 제출된 공개 키로 4번에서 제출된 결합 서명을 검증하고 서명 검증을 통과하면, 1번에서 user가 제출한 공개 키에 대한 개인 키 검증을 완료하고 이를 저장하여 등록 완료
로그인	- 로그인 절차는 RP등로 절차와 유사 - RP는 로그인하려는 user에게 챌린지 값에 대한 서명을 요구하고 user는 TTP와 함께 결합 서명을 생성하여 RP로 전송하면, RP가 기 등록된 공통 공개 키로 이 결합 서명을 검증하여 통과하면 로그인 수행 됨	
키 복구		- 사용자가 개인 키가 저장된 지갑 어플리케이션을 손망실 했을 때, RP에 등록된 공개 키를 갱신하지 않고 새로운 키를 획득하는 절차(FROST 알고리즘 사용) 1) user는 TTP에 로그인. 이를 위해 TTP는 자신에 등록된 user를 인증할 수 있는 별도의 메커니즘 필요 2) 새로운 지갑 생성하여 TTP내 기존 계정과의 연결 요청 3) TTP는 새로운 지갑을 등록하여 연결 완료

		4) user가 TTP에 키 갱신 요청 5) TTP는 Bsckup에 분산 키 생성을 위한 정보를 user에게 전달할 것을 요청 6) TTP와 Backup은 분산 키 생성을 위한 정보를 user에게 전달 7) user는 전달받은 키 갱신 정보를 바탕으로 분산 키를 신규로 생성

IV. MPC 기술의 적용 분야

구분	설명
금융 서비스	- 리스크 평가, 신용 평가, 사기 탐지 등에 중요한 역할을 수행 - 데이터 프라이버시를 보호하면서 정확하고 포괄적인 리스크 평가 수행 가능
보건 의료	- 환자의 프라이버시를 보호하면서도 공동으로 의료 연구를 진행 가능
공급망 관리	- 공급망 데이터를 공유하면서도 각 기업의 민감한 정보를 보호할 수 있음
데이터 마케팅	- 자신의 고객 데이터를 공재하지 않으면서 공동의 분석 결과를 도출할 수 있음
암호화폐	- 안전하게 개인 키를 관리하고, 여러 당사자가 공동으로 지갑을 제어할 수 있는 방식으로 사용 - 예를 들어, 비트코인 지갑에 대한 액세스 권한을 여러 당사자 간에 분할하여, 거래 승인을 위해 다수의 승인이 필요한 멀티시그(Multi-Sig) 지갑과 같은 기능을 향상
계약 협상	- 최소 입찰 가격 또는 최대 판매 가격과 같은 민감한 정보를 포함한 협상등에서 활용
데이터 수집	- 응답자의 개인정보를 보호하면서도 중요한 통계적 데이터를 수집하고 분석 - 의료, 금융, 교육 등의 분야에서 개인 데이터 보호가 중요한 연구에 활용. - 다양한 데이터를 수집하면서도 개인의 프라이버시를 침해하지 않음.
자동화된 시장	- 다양한 투자자들이 자신의 투자 전략이나 포지션을 공개하지 않고도 공동의 투자 결정을 내릴 수 있도록 하며, 여러 자산 관리자가 공동의 투자 펀드를 운영하면서 각자의 전략을 비밀로 유지 가능.

- 다양한 분야에서 프라이버시를 보호하면서도 필요한 계산과 의사 결정을 가능하게 하는 기술로 활용

"끝"

02	소프트웨어 테스트		
문제	정보시스템 개발과 운영 단계에서 수행되는 소프트웨어 테스트의 종류를 쓰고, 이 중 신뢰성 테스트와 이식성 테스트의 세부 활동에 대하여 각각 설명하시오.		
도메인	소프트웨어 공학	난이도	중(상/중/하)
키워드	단통시인설, 부하테스트, 성능테스트		
출제배경	기본 토픽에 대한 지식 확장		
참고문헌	ITPE 기술사회 자료		
해설자	모멘텀 안수현 기술사(제119회 정보관리기술사 / tino1999@naver.com)		

I. 소프트웨어 테스트의 개요

가. 소프트웨어 테스트의 정의

- 소프트웨어가 설계된 요구사항을 충족하는지 확인하고, 소프트웨어 내 잠재적인 결함을 식별하는 과정

나. 소프트웨어 테스트의 유형

구분	유형	특징
테스트 정보 획득 대상	화이트박스 테스트 (White Box Test)	프로그램 내부 로직을 보면서 테스트(구조 테스트) - 구조테스트 : 프로그램의 논리적 복잡도 측정 후 수행경로들의 집합을 정의 - 루프테스트 : 프로그램의 루프 구조에 국한해서 실시
	블랙박스 테스트 (Black Box Test)	프로그램 외부 명세를 보면서 테스트(기능 테스트) - 동등분할/경계값분석/Cause-Effect 그래프/오류예측기법 - Data Driven Test
프로그램 실행 여부	동적 테스트	프로그램 실행을 요구하는 테스트 (화이트박스, 블랙박스)
	정적 테스트	프로그램 실행 없이 구조를 분석하여 논리성 검증 - 코드검사(Code Review): 오류 유형 체크리스트 및 역할에 의한 formal한 검사 방법(fagan) - 워크스루(Walk Through): 역할/체크리스트가 없는 비공식적 검사 방법 - Inspection : 공식적 검사
테스트 목적	기능 테스트 (Functional)	- 시스템이 수행하는 기능을 단독으로 또는 상호 운용 성을 고려하여 테스트 - 모든 테스트레벨에서 수행 가능 - 명세 기반 기법, Black Box Test로 접근 (IEEE 610)
	비기능 테스트 (Nonfunctional)	- 성능 테스트, 사용성 테스트 등 비 기능적 요구 사항 또는 품질 목표에 대한 검증 - 시스템이 어떻게 동작하는가에 대한 검증
	구조 테스트 (Structure)	내부논리경로, 복잡도 평가 - 특정 유형의 구조 커버리지를 평가하여 테스트 보장성 또는 충분함을 측정 - 코드 구조의 커버리지 측정이 대표적

		- 자동화 툴을 이용하여 평가 가능 - White Box Test 로 접근

II. 개발과 운영 단계에서 수행되는 소프트웨어 테스트의 종류

가. 개발 단계에서 수행되는 소프트웨어 테스트의 종류

유형	특징
단위 테스트	모듈의 독립성 평가, White Box 테스트 - 구현 단계에서 프로그램 개발자에 의해 수행 - 테스트 가능한 최소 단위로 분리된 클래스, 컴포넌트, 모듈을 대상으로 결함식별, 기능을 검증 - 코드 중심으로 수행하며, 코드를 작성한 개발자가 테스트 주도 - 개별 모듈 테스트를 위해 모듈의 단독 실행 환경 필요
통합 테스트	모듈 간의 인터페이스 테스트(결함 테스트) - 모듈을 결합하여 하나의 시스템으로 구성 시 수행 - 빅뱅 통합 : 한꺼번에 테스트하므로 오류발생 시 원인 규명 어려움 - 하향식 통합 : 상위 모듈 테스트 시 다수의 하위 스텁(stub) 필요 - 상향식 통합 : 하위 모듈 호출하는 테스트 드라이버(Driver) 필요 - 상,하향식 통합을 결합한 샌드위치 통합방식 사용 권장 - 컴포넌트 또는 모듈 간의 상호 연동 부분 (Interface) 를 테스트 - 단위테스트의 완전성 확보 필요
시스템 테스트	통합 모듈에 대한 시스템적 테스트 - 기능적/비기능적 시스템 상위 레벨 요구 사항 검증 - 신뢰성, 견고성, 성능, 안전성 등 비기능적 요구사항 - 회복, 안전, 강도, 성능, 구조 등 - 통합된 시스템에 대해 실제 사용 환경과 유사한 환경에서 다양한 기법의 테스트 수행

나. 운영 단계에서 수행되는 소프트웨어 테스트의 종류

유형	특징
인수 테스트	사용자 요구사항 만족도 평가(알파,베타,감마) - 알파 : 개발자 환경에서 사용자가 수행 - 베타 : 일정 수의 사용자가 테스트 후 피드백 - 감마 : 베타버전 배포 이후 다수의 사용자 테스트 - 시스템에 대한 '확신'을 얻기 위해 사용자가 주체가 되어 전체 시스템을 검증 - 일반적으로 최종 단계의 테스트
설치 테스트	시스템을 설치하면서 수행 - HW체계, SW연결성 등 테스트
회귀 테스트	변경 또는 교정이 새로운 오류를 발생시키지 않음을 확인 - 결함 수정 이후 변경의 결과로 도입되었거나 발견되지 않았던 또 다른 결함을 발

	견하기 위한 테스트 - 조치의 결과로 시스템이 퇴행 되었는지 여부 확인
성능 테스트	응답시간, 처리량, 속도에 대한 점검 테스트
신뢰성 테스트	소프트웨어의 오류 없는 운영 시간(또는 사이클)을 측정하여 제품의 신뢰도를 평가
이식성 테스트	소프트웨어가 다른 환경(하드웨어, 운영체제, 네트워크 환경 등)에서도 기능을 유지할 수 있는지 확인

- 신뢰성 테스트와 이식성 테스트는 개발 및 운영단계에서 수행되며, 소프트웨어 품질 향상을 위해 수행

III. 신뢰성 테스트와 이식성 테스트의 세부 활동

가. 신뢰성 테스트의 세부 활동

활동	설명
오류 주입 (Fault Injection)	- 시스템의 내구성과 오류 처리 능력 확인 - 소프트웨어의 다양한 컴포넌트에 인위적으로 오류를 생성하여 시스템이 이를 어떻게 감지하고 대응하는지 확인 - 일반적으로 소프트웨어 코드 내에 예외 상황을 생성하거나, 데이터베이스 연결을 중단하는 등의 방법으로 수행
회복 테스트 (Recovery Testing)	- 시스템 장애 또는 오류 상황 후 복구 능력 확인 - 시스템의 중요 컴포넌트를 의도적으로 실패시킨 후, 시스템이 얼마나 빠르게 그리고 완전하게 기능을 회복하는지 평가 - 백업 시스템의 자동화된 복원 절차와, 데이터 일관성 및 무결성의 유지확인
부하/스트레스 테스트 (Load/Stress Testing)	- 시스템의 성능 한계를 정의하고, 고부하 상황에서의 처리 능력을 확인 - 시스템에 정상 범위를 초과하는 요청을 발생시켜 처리 능력을 확인. - 다양한 리소스(서버 CPU, 메모리, 네트워크 등)에 대한 부하를 점진적으로 증가시키면서 수행

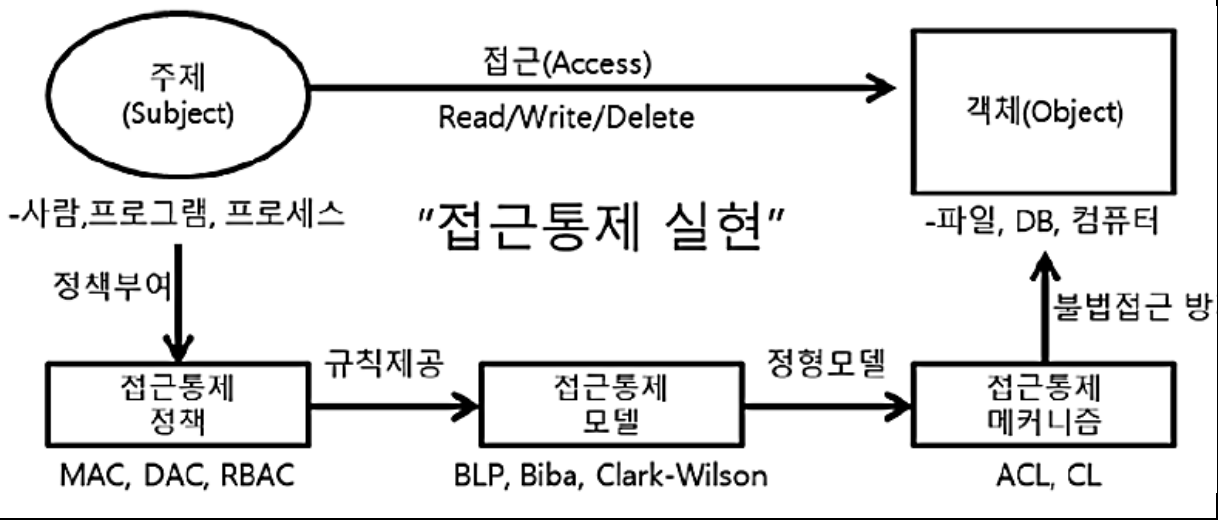
나. 이식성 테스트의 세부 활동

활동	설명
환경 테스트	- 다양한 운영 체제와 하드웨어 플랫폼에서 소프트웨어의 호환성을 확인 - 소프트웨어를 다양한 운영 체제에 설치하고 실행하여 확인 - 다른 CPU 아키텍처나 메모리 구성을 가진 하드웨어에서 테스트 수행
컴파일러 호환성 테스트	- 소프트웨어가 다른 컴파일러 및 개발 도구와 호환되는지 확인 - 다양한 컴파일러를 사용하여 소프트웨어 소스 코드를 컴파일하고, 발생하는 오류나 경고를 분석
사용자 인터페이스 일관성 테스트	- 다양한 플랫폼에서의 사용자 인터페이스(UI)가 일관되게 유지되고 사용자 UI가 동일한지 확인 - 소프트웨어의 UI를 다양한 화면 해상도, 입력 장치, 및 사용자 인터페이스 표준에 맞추어 테스트

"끝"

03	접근제어		
문제	정보보호 방법을 암호화와 접근제어로 크게 분류할 때, 접근제어에 대하여 그 개념과 정책, 절차, 그리고 이를 구현하는 매커니즘에 대하여 설명하시오		
도메인	보안	난이도	중(상/중/하)
키워드	MAC, DAC, RBAC, 식별, 인증, 인가, 책임추적성, ACL, CL		
출제배경	접근제어 전반에 대한 이해도 파악		
참고문헌	ITPE 기술사회 자료 https://it-life.tistory.com/192		
해설자	NS반 김민재 기술사(제124회 정보관리기술사 / kmj_pe@naver.com)		

I. 인가된 주체만이 객체 접근, 접근 제어 개념

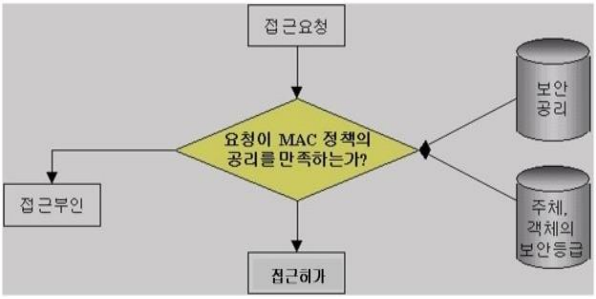
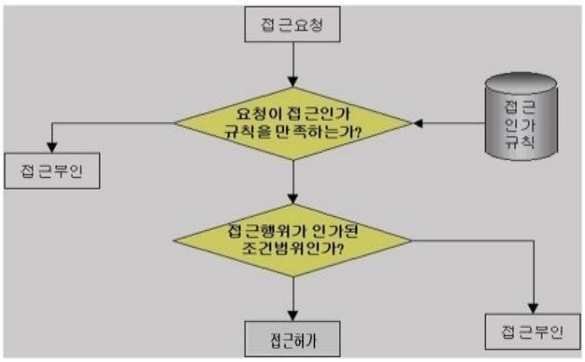
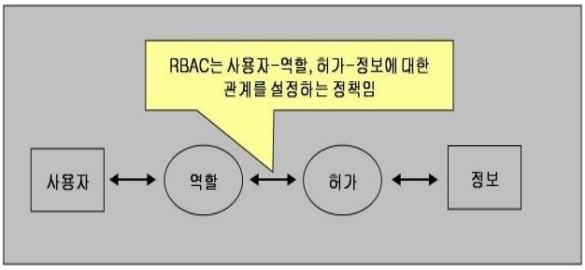
개념	- 사용자(주체)의 신원을 식별/인증하여 대상정보(객체)의 접근, 사용수준을 인가(Authorization)하는 기법으로 접근 제어 정책, 매커니즘, 모델로 구성
개념도	

II. 접근 제어 정책 설명

가. 접근 제어 정책의 원칙

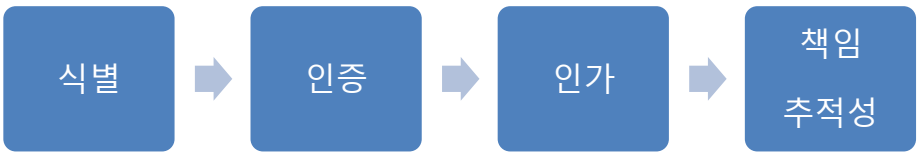
원칙	내용
최소 권한 부여	사용자들이 업무를 수행하기 위하여 꼭 필요한 권한만을 가지도록 접근 권한을 부여
직무 분리의 원칙	보안/감사, 개발/생산, 암호키 관리/변경 등 직무에 따라 접근 권한 분리

나. 접근 제어 정책 유형

유형	개념도	설명	주체
MAC (Mandatory Access Control)		- 강제적 접근통제, 규칙 기반 접근 통제, 관리자 - 사전 정의된 규칙(Rule)을 기반으로 주제(Subject)에게 허용된 접근 권한과 객체에 부여된 허용 등급을 비교하여 접근 통제	시스템
DAC (Discretionary Access Control)		- 임의적 접근통제, ACL(Access Control List), 사용자 소유권과 권한 - 주체의 신분에 근거하여 객체에 대한 접근 통제, 주체가 자신이 소유한 객체에 대해 다른 주체의 접근 권한 임의 설정 가능	사용자
RBAC (Role-Based Access Control)		- 역할 기반(임무 기반) 접근통제 - 사용자의 역할에 기반을 두고 접근을 통제하는 정책, 주체가 역할이라는 추상화 단계를 거쳐 객체의 접근 권한을 부여	사용자 역할

III. 접근 제어 절차 설명

가. 접근 제어 절차도



- 4단계를 통하여 접근 제어 수행

나. 접근 제어 절차 설명

절차	특징	설명
식별	사용자 식별	- 사용자를 식별하는 것으로 책임 추적성 분석에 유용
인증	식별 검증	- 식별에 대한 검증하기 위한 활동 - 메시지 인증, 사용자 인증, Type별 인증, SSO 인증 등 존재
인가	권한 부여	- 인증된 주체에게 허가된 권한을 부여하는 과정
책임 추적성	책임 소재 파악	- 문제 발생시에 원인 및 책임 소재 파악

- 책임 추적성은 최근에 추가된 절차임

IV. 접근 제어 매커니즘 설명

가. CL (Capability List)

개요	**- 행 중심의 표현형태** - 한 주체에 대해 접근 가능한 객체와 허가 받은 접근 종류 목록 - 비교적 객체가 적은 경우 적합
개념도	• Rows of access control matrix *file1* / *file2* / *file3* *Andy*: rx, r, rwo *Betty*: rwxo, r *Charlie*: rx, rwo, w C-Lists: • Andy: { (file1, rx) (file2, r) (file3, rwo) } • Betty: { (file1, rwxo) (file2, r) } • Charlie: { (file1, rx) (file2, rwo) (file3, w) }

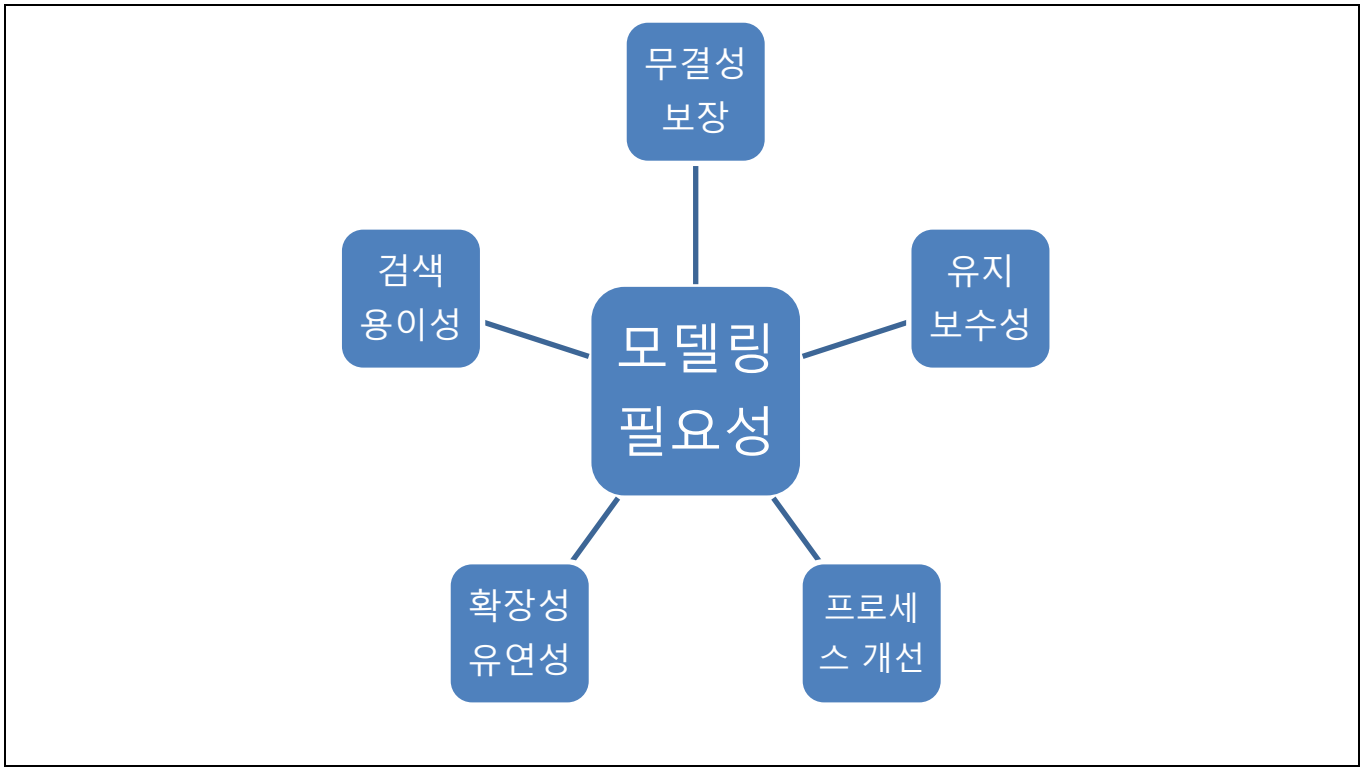
나. ACL (Access Control List) 객체

개요	- 객체관점에서 접근이 허용된 주체들에 대한 접근 권한을 테이블형태로 기술하여 이를 기반으로 접근제어 - 구분될 필요가 있는 사용자(개인, 그룹, 또는 직무)가 비교적 소수일 때와 그러한 사용자의 분포가 안정적일 대 가장 적합 **- 열 중심의 표현형태** - 현재 가장 널리 쓰이는 Access Matrix의 형태 - Resource(object)에 허용권한과 대상을 기록하는 방식 - 지속적으로 변화하는 환경에는 부적합
개념도	• Columns of access control matrix *file1* / *file2* / *file3* *Andy*: rx, r, rwo *Betty*: rwxo, r *Charlie*: rx, rwo, w ACLs: • file1: { (Andy, rx) (Betty, rwxo) (Charlie, rx) } • file2: { (Andy, r) (Betty, r) (Charlie, rwo) } • file3: { (Andy, rwo) (Charlie, w) }

"끝"

04	데이터 모델링		
문제	RDBMS를 적용하기 위한 데이터 모델링에 대하여 다음을 설명하시오. 가. 데이터 모델링의 개념 및 모델링 단계별 수행내용 나. 데이터 관계 모델링 시 식별(Identification)과 비식별(Non-Identification)에 대하여 비교 다. 데이터 모델링 시 고려사항		
도메인	데이터 베이스	난이도	중(상/중/하)
키워드	요구사항, 개념적/논리적/물리적 모델링, 주식별자 상속관계, Trade-off, 연결함정		
출제배경	데이터 모델링 개념, 절차 이해 파악		
참고문헌	ITPE 기술사회 자료		
해설자	NS반 김민재 기술사(제124회 정보관리기술사 / kmj_pe@naver.com)		

I. 데이터 베이스 모델링 필요성

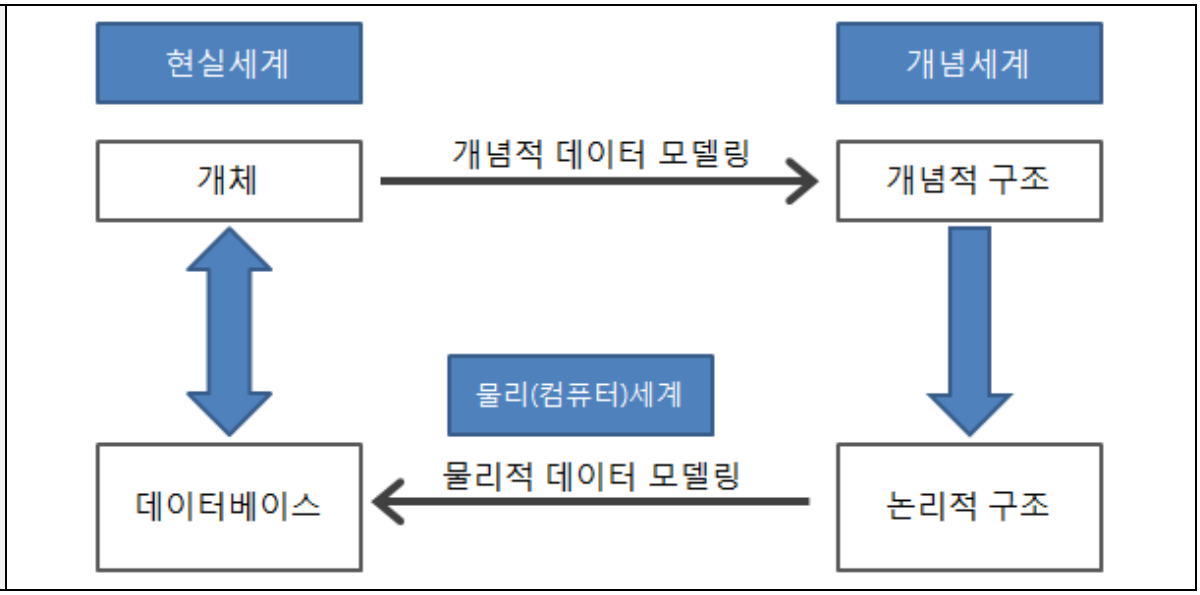


- 데이터 베이스의 효율적 관리를 위하여 모델링 필요

II. 현실세계를 추상화 하여 데이터베이스화 하는 데이터 모델링 개념

가. 데이터 모델링 개념

개념	- 요구사항 분석, 개념적/논리적/물리적 모델링의 절차에 따라 현실세계를 추상화하여 일정한 표기법에 의해 표현하는 작업

개념도	

- 데이터 베이스 모델링은 요구사항 분석 -> 개념 모델링 -> 논리 모델링 -> 물리 모델링 순서로 진행

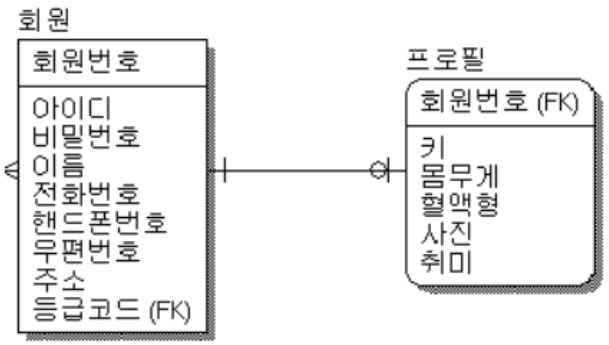
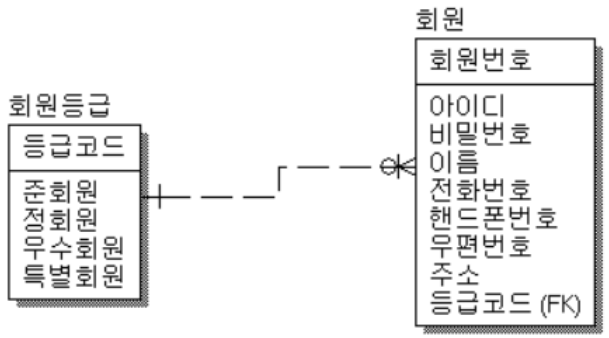
나. 데이터 모델링 단계별 수행내용

단계	수행 내용	주요활동	산출물
요구사항 수집 및 분석	- 사용자가 요구하는 업무 요구사항 수집 분석 - 사용자/데이터/프로세스 요구사항 분석 - 정적 구조, 동적 구조 요구사항 파악	- 정적 구조 요구사항: 엔터티(entity), 속성, 관계, 제약조건 등 - 동적 구조 요구사항: 트랜잭션의 유형, 빈도 등	- 요구사항 명세서 - 업무 기술서
개념적 모델링	- 추상화 수준 높고, 업무중심적 포괄적 수준의 모델링 - 정보의 구조를 추상적으로 개념화	- 데이터 중요성 판단, 데이터 형태 유지 결정 - 핵심 엔터티 발견, 관계정의, ERD 표현	- 개념 데이터 모델 - ERD (Entity Relationship Diagram)
논리적 모델링	- 시스템으로 구축하고자 하는 업무를 Key, 속성, 관계 등으로 표현 - 데이터 모델링 과정 중 핵심부분 - 비즈니스 정보의 논리적 구조, 규칙을 명확히 표현	- 개념적 설계 결과, DB 저장 위해 논리적 구조로 변환 - 정규화 수행 - ERD 기반으로 테이블 구조로 변환	- 논리 스키마
물리적 모델링	- 물리적 DB에 이식 가능하도록 성능향상, 저장 효율화 위해 물리적 성격을 고려하여 설계 - 관계형 테이블 전환 및 테이블 설계	- 데이터 타입 설계 - 인덱스 설계 - 뷰 설계	- 물리 스키마 - 테이블 정의서

- 모델링 진행 시 Trade-off 관계, 연결 함정에 유의하여 실행 필요

III. 데이터 관계 모델링 시 식별(Identification)과 비식별(Non-Identification)에 대하여 비교

가. 데이터 모델링의 식별관계, 비식별관계 정의 및 개념도 비교

식별관계	비식별관계
상위 엔티티의 주식별자를 하위 엔티티로 상속할 때, 주 식별자에 포함시키는 관계	상위 엔티티의 주식별자가 하위 엔티티로 상속될 때, 일반 속성에 포함되는 관계
	

- 주 식별자를 하위(자식)엔티티에 어떻게 상속하느냐에 따라 식별/비식별 관계로 분류.
- 부모, 자식 엔티티 간 표기 시 실선/점선으로 식별 관계를 표기함.

나. 식별관계, 비식별관계 상세 비교

구분	식별관계	비식별관계
목적	- 강한 연결관계 표현	- 약한 연결관계 표현
자식 주식별자 영향	- 자식 주식별자의 구성에 포함	- 자식 일반 속성에 포함
표기법	- 실선 표현	- 점선 표현
연결 고려사항	- 반드시 부모 엔티티 종속 - 자식 주식별자 구성에 부모 주식별자 포함 필요	- 약한 종속 관계 - 자식 주식별자 구성을 독립적으로 구성 - 부모 쪽의 관계 참여가 선택 관계

- 두 엔티티간 종속 관계라면 식별관계를 사용하고, 참조관계라면 비식별관계를 사용하는 것이 원칙.

IV. 데이터 모델링 시 고려사항

고려사항	설명
Trade-off 관계	- 정규화 및 반정규화 시 Trade-off 관계를 고려하여 진행 필요 - 조회성능 향상, 삽입성능 하락 등
연결함정	- 데이터 모델에서 관계 형성되어 있으나 실제로는 연결된 데이터를 찾을 수 없는 현상 고려 필요(부채꼴 함정, 균열함정)

- 데이터 모델링 기본 원칙(커뮤니케이션 원칙, 모델링 상세화 원칙, 논리적 표현 원칙) 고려하여 모델링 수행

"끝"

(추가)

데이터 모델링 기본원칙

기본원칙	설명	고려사항
커뮤니케이션 원칙 Communication Principle	모든 사람들의 이해와 분명한 파악이 가능한 모델 제시 최종사용자와 모든 이해관계자들을 최대한 고려 **(대상)** 최종사용자, 시스템분석가, DB관리자, 타 전문가	이해를 돕기 위한 비즈니스지향적 모델과 기술적 상세모델 두가지 버전 관리
모델링상세화 원칙 Granularity Principle	조직 정부구조의 최소 공통 분모 제시 **(분할)** 복잡한 구조 및 프로세스는 요소단위로 분할 **(제거)** 불필요한 구조와 중복은 협의통해 제거	물리모델 단계가 아닌 논리모델 단계에서 선행
논리적표현 원칙 Logical Representation Principle	조직의 비즈니스를 그대로 논리적으로 반영 **(분석)** 경험에의한 섣부른 판단 보다는 절차 준수 **(구체화)** 단기간의 솔루션을 구체화 시도는 지양	데이터 모델링 시 물리적인 제약조건은 배제 원칙

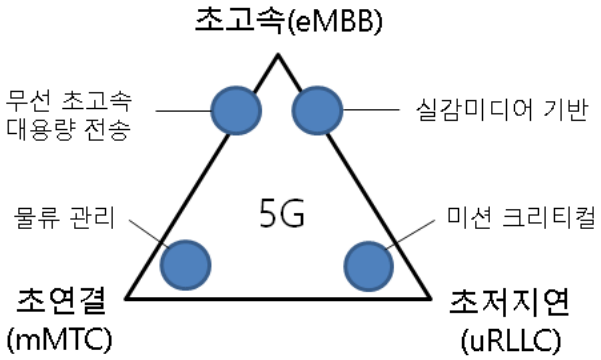
05	5G 특화망		
문제	5G 특화망을 위한 네트워크를 구축할 때 고려되어야 할 사항에 대하여 다음을 설명하시오. 가. 안정성 및 신뢰성 확보 방안 나. 간섭회피 방안		
도메인	네트워크	난이도	상(상/중/하)
키워드	네트워크 보안 인증, 전송망 이중화, 주파수 대역, 대역폭		
출제배경	5G 특화망은 125회, 126회 연속으로 출제된 토픽으로 구축 방안 및 고려사항 모두 학습 필요		
참고문헌	5G 특화망 가이드라인(21.10, 과학기술정보통신부/한국방송통신전파진흥원)		
출제자	강북심화 이제이 기술사(제 130회 정보관리기술사 / bwmslove@naver.com)		

I. 전용 주파수를 통한 맞춤형 네트워크, 5G 특화망 개요

가. 5G 특화망 개념

- 기존 이동통신 상용망이 아닌 전용 주파수를 통해 특정공간(건물, 시설, 장소 등)에서 수요기업이 도입하고자 하는 최첨단 서비스를 구현할 수 있는 맞춤형 네트워크
- 수요기업 또는 사업자가 건물·시설·토지 등 제한된 범위 내에서 5G 서비스를 적용하기 위해 기업 맞춤형으로 무선 네트워크 구축

나. 5G 특화망 네트워크 구축 목표



- 특화망을 통해 사업장 내 적용하려는 서비스를 정의할 때 서비스 별 속도(Throughput), 지연(Latency) 등의 5G 특화망 요구성능을 산정하고 정의함
- 단일장비의 일시 장애, 상용전원 공급중단 등 비상상황에 따른 안정성 및 신뢰성 확보 필요
- 인접지역 셀 경계구간에서 특화망간의 간섭영향이 발생 할 수 있어서 간섭회피 방안에 대한 고려 필요

II. 네트워크 구축단계 안정성 및 신뢰성 확보 방안

가. 네트워크 보안 인증

대상	인증	담당부처, 기관	관계 법률
보안제품·솔루션 (방화벽, IPS, DDOS대응장비,	CC인증	과기부, ITSCC	국가정보화법

접근통제 등 20종)			
국제CC인증 제품 및 L3이상 네트워크 장비, 가상화(SDN) 제품 (국가·지자체·공공기관 한)	보안적합성검증	국정원, 국가보안기술연구소	전자정부법
암호화 모듈 (국가·지자체·공공기관 한)	KCMVP	국정원, 국가보안기술연구소	전자정부법

- 특화망을 구축하고 외부 인터넷과의 연동이 필요할 경우 CC인증을 받은 보안제품·솔루션을 도입함으로써 해킹 등의 보안위협으로부터 특화망을 보호
- 국가 및 지자체의 경우 5G코어장비 등 가상화 장비에 대한 보안적합성 검증 및 단말-서버간의 암호화를 적용할 때 KCMVP인증을 받은 암호모듈 적용이 요구됨

나. 이중화 기술 적용

방안	적용 기술	설명
기지국 이중화	- 셀 중첩 설계를 통한 가상셀(Virtual Cell) 적용	- 다수의 물리적 기지국을 하나의 논리적 기지국으로 구성하는 가상셀(Virtual Cell)로 구성 - 커버리지 이중화를 통해서 RU간 커버리지가 중첩되도록 구성하여 서비스 연속성 확보
	- RU교번배치	- RU장비와 CU/DU장비간 교번 배치를 통해 프론트홀 링크를 이중으로 구성
	- 주요 장비 Active/Standby 운용	- 5G코어 등 주요 장비에 대한 이중화 및 Active/Standby모드 적용
전송망 이중화	- 백홀(Backhaul)구간 전송망 이중화	- 특정 지역 내 특화망을 공동으로 구축하는 경우 개별 사업장 내 액세스망을 구성하는 기지국과 코어망을 연결하는 백홀구간에서 광 전송장비를 활용한 전송망 이중화 - 지역의 생산공장, 발전소 등에 특화망을 구축하고 본사에 코어망을 구축 - 특화망 기간통신사업자의 코어망을 공유할 경우 백홀 구간의 전송망을 이중화시켜 네트워크의 안정성을 확보
	- 링형 토폴로지 등을 통한 물리적 이중화	- 전송망 구간에서의 국지적 화재·재난 등의 비상상황 발생시 회선 절체로 서비스 중단 없는 5G특화망 이용

- 5G특화망 네트워크 구축 단계에서 기지국과 전송망을 이중화하여 안정성 및 신뢰성 확보

III. 네트워크 구축단계 간섭회피 방안

가. 특화망 기획 및 설계단계 간섭회피 방안

단계	방안	설명
기획	- 최적 주파수 대역, 대역폭 선정	- 서비스에 적합한 주파수 대역과 대역폭 산출 - 특화망지원센터(KCA)로 인접지역 특화망 검토 - 적정 가드밴드를 확보하면 4.7GHz, 28GHz 대역 인접채널 사용 가능

설계	- 설계 결과 기술검토	- 5G무선망 설계 도구(Tool)를 활용하여 기술 검토 - RU 위치 및 수량 조정 - RF 출력 등의 파라미터 조정

- 5G특화망은 기획 및 설계 단계부터 간섭회피 방안을 고려하여 네트워크를 구축함

나. 시공 및 운영 단계 간섭회피 방안

단계	방안	설명
시공	- 준공신고서 제출	- 특화망지원센터(KCA)에 준공신고서 제출
	- 네트워크 성능 검사	- 인접채널 누설, 대역 외 발사, 스퓨리어스(Spurious), 주파수 편차, 점유주파수 대역폭 등에 대한 성능 검사
운영	- 상/하향 슬롯 비율 조정	- 인접지역 또는 인접대역의 상하향 링크를 동일하게 설정 - KCA의 중재로 RF출력세기 축소 등의 조정 과정 진행

- 시공 및 운영 단계에서는 준공신고서를 제출하고 인접지역 간섭에 대한 설정을 확인함

IV. 5G 특화망 네트워크 운영단계 고려사항

항목	고려사항	설명
품질 관리	- OSS를 통한 성능 개선 (Operation Support System)	- 운영 및 유지보수 기능을 지원하는 시스템을 액세스망과 코어망에 연동 예) 5G장비 구성, 알람 관측, 원격 파라미터 설정
	- 기능추가를 통한 성능 개선	- TSN, CoMP, IAB 등 성능강화 솔루션 적용
보안 강화	- 보안 운영 절차 수립	- 업무 분리, 최소 권한 사용 및 로깅
	- 보안 성능 모니터링, 감지	- 보안 취약점 관리 및 공격 감지
	- 침해 대응	- 보안 침해 후 대응 및 복구

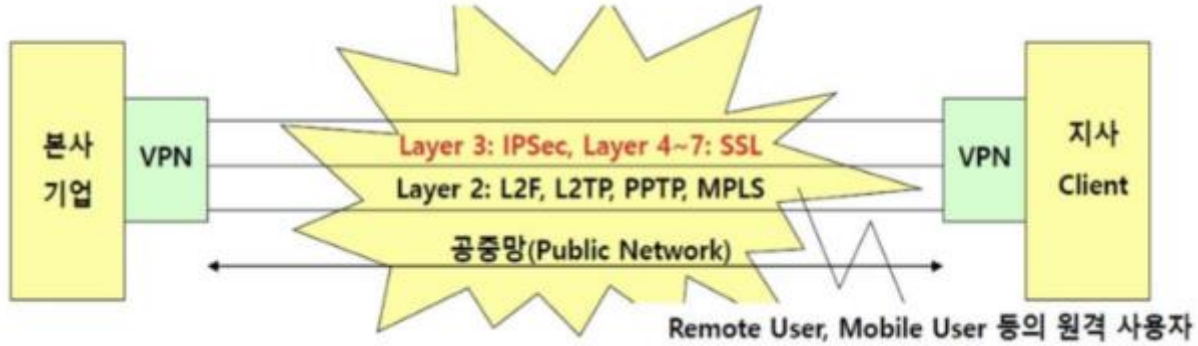
- 5G 특화망은 네트워크 설계, 제조사 제품 개발, 설치, 운영 단계별 보안 강화를 위해 방안 수립 필요

"끝"

06	VPN의 구축 종류		
문제	VPN(Virtual Private Network)에 대하여 다음을 설명하시오. 가. VPN의 개념 및 특징 나. IPSec (Internet Protocol Security) VPN과 SSL(Secure Socket Layer) VPN 다. VPN의 기술요소		
도메인	네트워크	난이도	중(상/중/하)
키워드	SSLVPN, IPsecVPN, MPLS, 기밀성, 무결성, 터널링 기법		
출제배경	VPN의 개념과 OSI 계층 별 VPN 구축 종류에 대한 숙지 여부 확인		
참고문헌	ITPE 기술사회		
출제자	강북심화 이제이 기술사(제 130회 정보관리기술사 / bwmslove@naver.com)		

I. 가상 사설 네트워크, VPN의 개념 및 특징

가. VPN의 개념



개념	- 인터넷 같은 공중망에서 터널링 기법을 통해 사용자가 사설망에 연결된 것처럼 기밀성, 무결성을 보장하는 네트워크 통신 기술

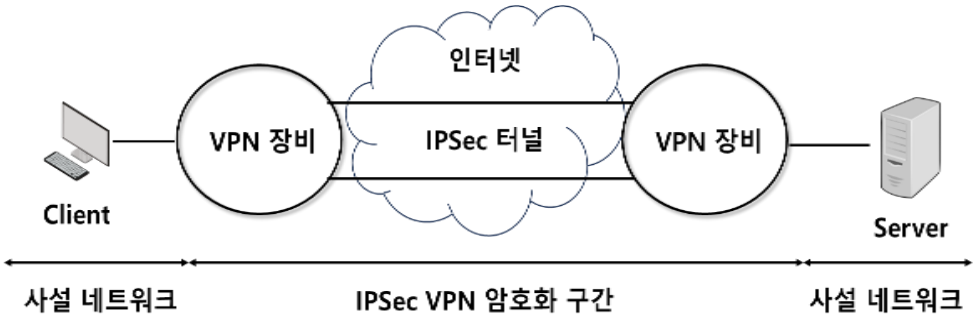
나. VPN의 특징

구분	특징	설명
보안 측면	- 데이터 기밀성	- 암호화를 이용하여 메시지의 내용을 은폐
	- 데이터 무결성	- 데이터 전송 중 제3자에 의해 변환되지 않았음을 보장
	- 데이터 원본 인증	- 요청한 수신인에 의해 각 데이터가 원본인지 확인
	- 재전송 공격 방지	- 인증헤더에 일련번호를 부여하여 재전송 공격 방지
비즈니스 측면	- 비용 절감	- 가상화를 통해 전용망과 같은 효과 기대
	- QoS 보장	- 네트워크 사용자 품질 보증 기술로 활용

- VPN 기술은 OSI 7Layer에 계층에 따라 IpsecVPN과 SSLVPN 분류

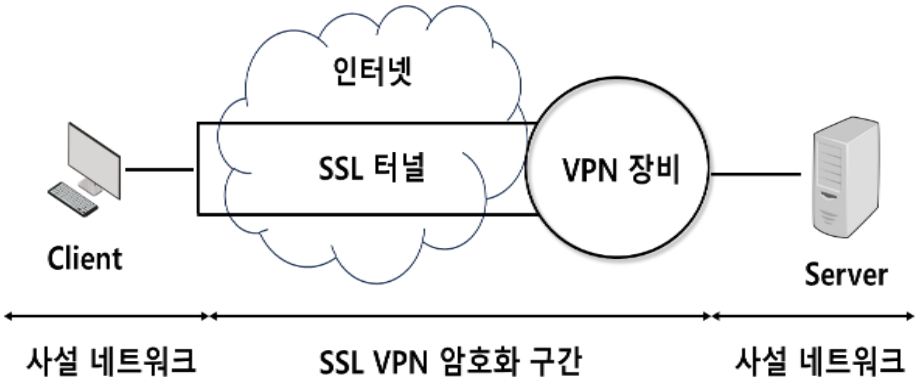
II. IPSec (Internet Protocol Security) VPN과 SSL(Secure Socket Layer) VPN

가. 3계층 VPN기술, IPSec (Internet Protocol Security) VPN

정의	- 단말간 안전한 통신망 연결을 위해 IPSec Tunneling 기술 이용하는 OSI 3계층 사설 네트워크 보안 기술	
개념도		
구성요소	- AH, ESP	- 인증헤더, 데이터 인증, 무결성 보장, 재전송 공격 방지
	- IKE	- 인터넷 키 교환 알고리즘 및 키 교환 관련 SA 생성

- IPSecVPN 기술은 주로 지사와 본사간 통신에 활용

나. 4~7계층 VPN기술, SSL(Secure Socket Layer) VPN

정의	- OSI 4~7계층에서 웹 브라우저를 통해 원격 액세스를 제공하며, 사용자 인증, 데이터 암호화 및 데이터 무결성을 보장하는 사설 네트워크 보안 기술	
개념도		
구성요소	- Change Cipher Spec Protocol	- Handshake 프로토콜에 의해 협상된 압축, MAC, 암호화에 쓰는 방식이 이후부터 적용됨을 수신자에게 알리는 목적
	- Alert Protocol	- 암호 오류, 압축 오류, 메시지 인증 오류, 인증 실패 등의 에러 발생을 수신자에게 알리는 역할
	- Handshake Protocol	- 서버와 클라이언트 간 상호 인증과 암호 키 교환 및 암호화 알고리즘/MAC 방식/압축 방식 협상 그리고 세션키 생성
	- Record Protocol	- 응용 데이터나 제어 메세지를 레코드 단위로 TCP 계층으로 안전하게 전달하는 역할 (기밀성, 무결성 제공)

- SSLVPN 기술은 주로 브라우저를 통한 기업 내부망 접속을 위한 재택근무, 원격근무에 활용

III. VPN의 기술요소

구분	기술요소	설명
인증 및 보안	- 인증	- VPN에 접속하기 위한 사용자나 장치의 신원을 확인하는 과정
	- 암호화	- 데이터를 안전하게 전송하기 위해 데이터 암호화
	- 키 관리	- 암호화 및 복호화를 위한 키를 안전하게 생성, 저장 및 교환하는 방법
통신 및 프로토콜	- 터널링	- 데이터를 캡슐화하여 안전한 통신 채널을 구축합니다.
	- 암호화 프로토콜	- VPN에서 사용되는 IPsec, SSL 등
	- 인터넷 프로토콜	- 인터넷 프로토콜(IP) 기반

- OSI 7 layer 계층별 VPN 기술의 차이점 존재

IV. IPSec VPN과 SSL VPN과 상세 비교

비교 항목	IPSec VPN	SSL VPN
OSI Layer	- Layer 3	- Layer 4 ~ 7
표준	- RFC 4301 (IPSec 기준)	- RFC 5246 (TLS 1.2 기준)
프로토콜	- IP	- TCP
인증방식	- 비밀키 공유	- X.509 인증서
구현방식	- Site to Site (Lan to Lan)	- Client to Site
장점	- 높은 안정성	- 브라우저 및 Agent 방식 구현
단점	- 고비용(전용 장비 설치 양단 설치)	- 저비용(전용 장비 서버측 설치)
사례	- 본사와 지사의 VPN 연결	- 브라우저를 통한 기업 내부망 접속 (재택근무)

- 그 외에 PPTP, L2F, L2TP, MPLS VPN 등 다양한 VPN 연결 방식 존재

"끝"

ITPE 기술사회
제133회 정보처리기술사 기출문제 해설집

대 상 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사, 정보시스템감리사 시험
발행일 2024년 05월 18일
집 필 강정배PE, 안수현PE, 이제이PE, 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