ITPE기술사회

제 138 회 대비 ITPE Final Round 해설집 (2일차)

2026.02.01

ITPE 제 138 회 대비 Final Round

[2 일차] – 2026. 02.01(일) 제 1 교시(시험시간: 100 분)

분야	정보통신	자격종목	정보관리	수검번호		성명	

※ 다음 문제 중 10 문제를 선택하여 설명 하십시오. (각 10 점)

1. 개인정보의 안전성 확보조치 기준

2. 포아송 분포(Poisson Distribution)

3. KCMVP(Korea Cryptographic Module Validation Program)

4. HBF(High Bandwidth Flash)와 HBS(High Bandwidth Storage)

5. OECD AI 10개 원칙

6. 합성 데이터(Synthetic Data) 생성 기술

7. AI 기본법 주요 내용

8. AI-RAN

9. PromptLock

10. 데브옵스(DevOps)와 노옵스(NoOps) 비교

11. ISO/IEC 21500에 대하여 설명하시오.

12. 기밀 컴퓨팅 (CC, Confidential Computing)

[정보관리기술사 선택 문제]

13. 가명처리(Pseudonymization) 기법에 대하여 설명하시오.

[컴퓨터시스템응용기술사 선택 문제]

13. 6G 이동통신 특징과 주파수 동향에 대해 설명하시오.

01	개인정보의 안전성 확보조치 기준		
문제	개인정보의 안전성 확보조치 기준		
도메인	보안	난이도	상 (상/중/하)
키워드	개인정보보호법 제29조		
출제배경	개인정보의 안전성 확보조치 기준 일부개정('25.10.)에 따른 내용 이해 확인		
참고문헌	개인정보의 안전성 확보조치 기준 안내서 – 개인정보보호위원회(2025.11)		
출제자	정상반멘토 이상헌 기술사(제 118회 정보관리기술사 / bluesanta97@naver.com)		

I. 개인정보의 안전성 확보조치 기준 개요

구분	설명
법적근거	- 개인정보 보호법 제29조(안전조치의무) - 개인정보 보호법 시행령 제16조제2항(개인정보의 파기방법), 제30조(개인정보의 안전성 확보 조치), 제30조의2(공공시스템 운영기관 등의 개인정보 안전성 확보 조치 등)
적용 대상	- 개인정보처리자 - 개인정보처리자로부터 개인정보를 제공받은 자 - 개인정보처리자로부터 개인정보 처리를 위탁받은 자(이하 '수탁자', 준용)
목적	- 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 기준을 정함
성격	- 반드시 준수해야 하는 최소한의 기준
과징금 및 과태료	- 개인정보가 분실·도난·유출·위조·변조·훼손된 경우 전체 매출액의 100분의 3을 초과하지 아니하는 범위에서 과징금(법 제64조의2제1항제9호) - 3천만원 이하의 과태료(법 제75조제2항제5호)

- '25년 10월 개인정보의 안전성 확보조치 기준 일부개정

II. 개인정보의 안전성 확보조치 기준 주요 내용 설명

가. 개인정보의 안전성 확보조치 상세설명

구분	설명
내부 관리계획의 수립·시행 및 점검	- 개인정보처리자는 개인정보의 분실·도난·유출· 위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다.
접근 권한의 관리	- 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 차등 부여한다. - 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.
접근통제	- 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 안전조치를 하여야 한다.

	1. 개인정보처리시스템에 대한 접속 권한을 인터넷 프로토콜(IP) 주소 등으로 제한하여 인가받지 않은 접근을 제한 2. 개인정보처리시스템에 접속한 인터넷 프로토콜(IP) 주소 등을 분석하여 개인정보 유출 시도 탐지 및 대응
개인정보의 암호화	- 개인정보처리자는 비밀번호, 생체인식정보 등 인증정보를 저장 또는 정보통신망을 통하여 송·수신하는 경우에 이를 안전한 암호 알고리즘으로 암호화하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다. - 암호화 대상 : 1. 주민등록번호 2. 여권번호 3. 운전면허번호 4. 외국인등록번호 5. 신용카드번호 6. 계좌번호 7. 생체인식정보 - 10만명 이상의 정보주체에 관하여 개인정보를 처리하는 대기업·중견기업·공공기관 또는 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 중소기업·단체에 해당하는 개인정보 처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.
접속기록의 보관 및 점검	- 개인정보처리자는 개인정보처리시스템에 접속한 자(다만, 정보주체는 제외한다)의 접속기록을 1년 이상 보관·관리하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 2년 이상 보관·관리하여야 한다. 1. 5만명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리시스템에 해당하는 경우 2. 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템에 해당하는 경우 3. 개인정보처리자로서 「전기통신사업법」제6조제1항에 따라 등록을 하거나 같은 항 단서에 따라 신고한 기간통신사업자에 해당하는 경우
악성프로그램 등 방지	- 개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다. 1. 프로그램의 자동 업데이트 기능을 사용하거나, 정당한 사유가 없는 한 일 1회 이상 업데이트를 실시하는 등 최신의 상태로 유지 2. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치
물리적 안전조치	- 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다. - 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다
재해·재난 대비 안전조치	- 10만명 이상의 정보주체에 관하여 개인정보를 처리하는 대기업·중견기업·공공기관 또는 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 중소기업·단체에 해당하는 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 다음 각 호의 조치를 하여야 한다. 1. 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검 2. 개인정보처리시스템 백업 및 복구를 위한 계획을 마련
출력·복사시 안전조치	- 개인정보처리자는 개인정보처리시스템에서 개인정보의 출력시 (인쇄, 화면표시,

	파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화하여야 한다. - 개인정보처리자는 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 필요한 안전조치를 하여야 한다.
개인정보의 파기	- 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다. 1. 완전파괴(소각·파쇄 등) 2. 전용 소자장비(자기장을 이용해 저장장치의 데이터를 삭제하는 장비)를 이용하여 삭제 3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

나. 공공시스템운영기관 등의 개인정보 안전성 확보조치 상세설명

구분	설명
공공시스템운영기관의 안전조치 기준 적용	- 2개 이상 기관의 단일 시스템 가. 100만명 이상의 정보주체에 관한 개인정보를 처리하는 시스템 나. 개인정보처리시스템에 대한 개인정보취급자의 수가 200명 이상인 시스템 다. 정보주체의 사생활을 현저히 침해할 우려가 있는 민감한 개인정보를 처리하는 시스템 - 2개 이상 기관의 다른 기관이 운영할 수 있도록 배포한 표준배포 시스템 - 기관별로 운영하는 개별 시스템 가. 100만명 이상의 정보주체에 관한 개인정보를 처리하는 시스템 나. 개인정보처리시스템에 대한 개인정보취급자의 수가 200명 이상인 시스템 다.「주민등록법」에 따른 주민등록정보시스템과 연계하여 운영되는 시스템 라. 총 사업비가 100억원 이상인 시스템
공공시스템운영기관의 접근 권한의 관리	- 공공시스템운영기관은 공공시스템 별로 다음 각 호의 사항을 포함하여 내부 관리계획을 수립하여야 한다. 1. 영 제30조의2제4항에 따른 관리책임자(이하 "관리책임자"라 한다)의 지정에 관한 사항 2. 관리책임자의 역할 및 책임에 관한 사항 3. 제4조제1항제3호에 관한 사항 중 개인정보취급자의 역할 및 책임에 관한 사항 4. 제4조제1항제4호부터 제6호까지 및 제8호에 관한 사항 5. 제16조 및 제17조에 관한 사항
공공시스템운영기관의 접속기록의 보관 및 점검 등	- 공공시스템운영기관은 공공시스템에 대한 접근 권한을 부여, 변경 또는 말소하려는 때에는 인사정보와 연계하여야 한다. - 공공시스템운영기관은 제5조제4항에 따른 계정을 발급할 때에는 개인정보 보호 교육을 실시하고, 보안 서약을 받아야 한다.

- 안전성 확보조치를 하지 아니한 자 등에게는 관련 법률에 따라 과징금, 과태료를 부과할 수 있음

"끝"

02	포아송 분포(Poisson Distribution)		
문제	포아송 분포(Poisson Distribution)		
도메인	확률/통계	난이도	중 (상/중/하)
키워드	평균=분산, 독립성, 비례성, 비중복성, 확률밀도함수		
출제배경	135회 출제 및 최근 확률분포 문제 다수 출제로 포아송 분포 이해 확인		
참고문헌	ITPE 서브노트		
출제자	정상반멘토 이상헌 기술사(제 118회 정보관리기술사 / bluesanta97@naver.com)		

I. 정해진 시공간 또는 단위구간 내의 사건 발생 확률, 포아송 분포(Poisson Distribution)의 개요

가. 포아송 분포(Poisson Distribution) 의 정의

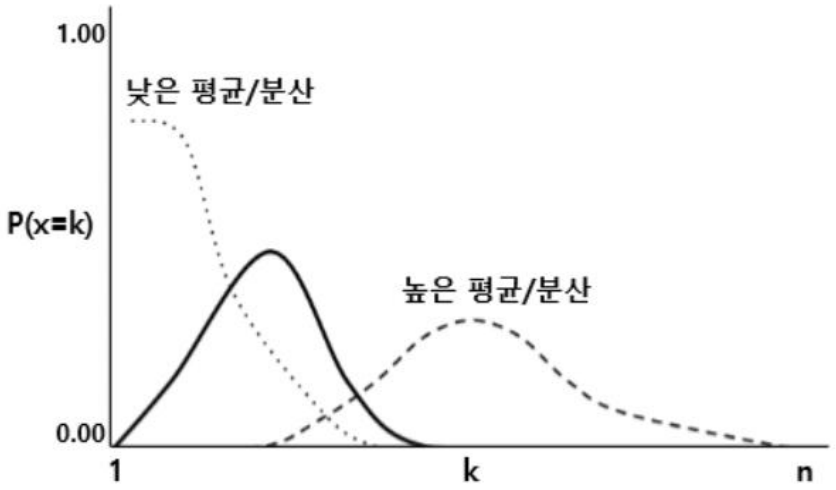
- 단위 시간이나 단위 공간에서 평균 λ 번 발생하는 사건이 정확히 x번 발생할 확률

나. 포아송 분포(Poisson Distribution)의 특징

독립성	- 특정 시간/공간에서 발생한 사건은 다른 구간에서 발생하는 사건에 영향을 주지 않음
비례성	- 사건이 발생할 확률은 해당 구간의 길이에 비례
비중복성	- 아주 짧은 시간 동안 두 번 이상의 사건이 동시에 일어날 확률은 0에 가까움

II. 포아송 분포(Poisson Distribution)의 형태와 상세 설명

가. 포아송 분포(Poisson Distribution)의 형태



나. 포아송 분포(Poisson Distribution)의 상세설명

구분	설명	
확률변수	- 0,1,2,3,4... (발생 횟수이므로 0 이상의 정수)	
확률밀도함수	$f(n;\lambda)=\frac{\lambda^n e^{-\lambda}}{n!}$	
기대값	$E(X)=\lambda$ - 평균적으로 발생하는 횟수	
분산	$E(X)=\lambda$ - 평균과 분산이 같다는 점이 특징	
그래프 형태	$\lambda<1$	- 오른쪽으로 긴 꼬리를 가진 형태
	$1\le\lambda<10$	- 왼쪽으로 치우쳐 있으나 점차 가운데로 이동
	$\lambda\ge10$	- 점차 좌우 대칭에 가까워짐

- 포아송 분포에서 λ 가 충분히 커지면(보통 30 이상), 정규분포에 가까워지는 특성을 가짐

III. 이항 분포와 포아송 분포 상세 비교

구분	이항 분포	포아송 분포
목적	- 고정된 시행 횟수 중 특정 사건이 발생하는 횟수를 모델링	- 일정 시간 또는 공간에서 사건이 발생하는 횟수를 모델링
적용 조건	- 고정된 시행 횟수 (nnn), 각 시행이 독립적, 사건 발생 확률 (ppp) 일정	- 사건 발생이 독립적, 사건 발생률 (λ) 일정, 단위 시간 또는 공간에서 발생
확률 변수	- 성공 횟수	- 사건 발생 횟수
파라미터	- n: 시행 횟수, p: 사건 발생 확률	- λ: 평균 사건 발생 횟수
특징	- 고정된 시행 횟수 필요, n이 크고 p가 작을 때 포아송 근사 가능	- 시행 횟수가 고정되지 않음, 사건 발생이 독립적으로 발생
기대값	- E(X)=n·p	- E(X)=λ
분산	- Var(X)=n·p·(1−p)	- Var(X)=λ
사례	- 동전 던지기 성공 횟수, 품질 검사(결함 여부), 선거 지지율 측정	- 콜센터 전화 횟수, 교통사고 발생 횟수, 공장 결함 개수

- 이항 분포는 성공·실패가 명확한 반복 시행에 사용, 포아송 분포는 특정 구간(시간·공간)에서 발생 사건 개수 다룰 때 적합

"끝"

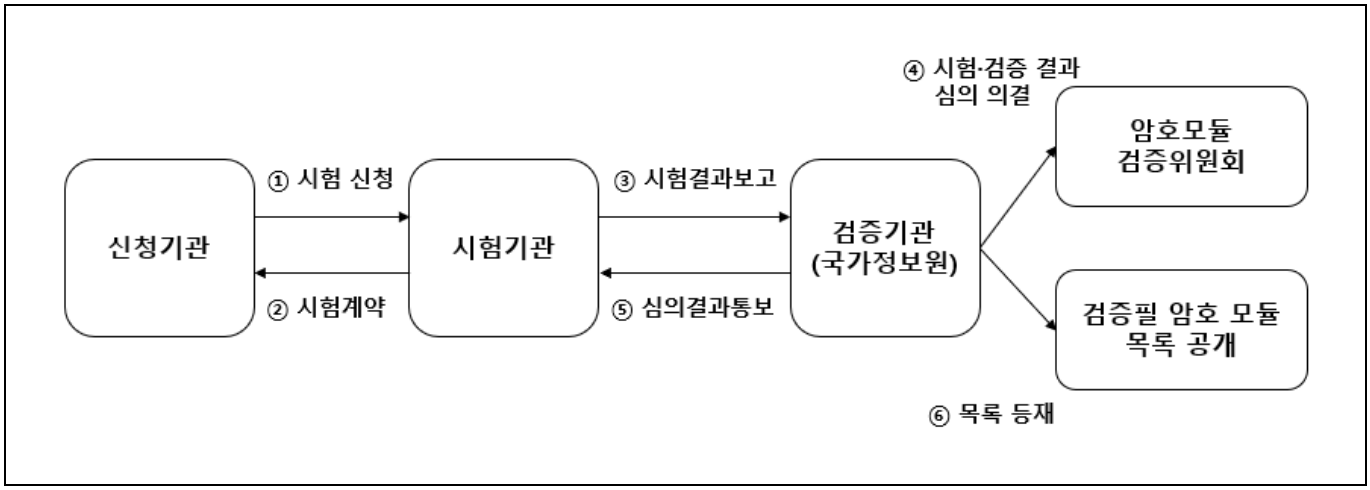
03	KCMVP(Korea Cryptographic Module Validation Program)		
문제	KCMVP(Korea Cryptographic Module Validation Program)		
도메인	보안	난이도	중 (상/중/하)
키워드	사이버안보 업무규정 제9조, 전자정부 시행령 제69조, 신청기관, 시험기관, 검증기관, 국정원		
출제배경	보안의 중요성에 따른 암호모듈 검증제도에 대한 이해 확인		
참고문헌	https://www.boannews.com/media/view.asp?idx=117358 https://defcon.tistory.com/11		
출제자	정상반멘토 이상헌 기술사(제 118회 정보관리기술사 / bluesanta97@naver.com)		

I. 암호모듈에 대한 안전성을 검증하는 제도, KCMVP(Korea Cryptographic Module Validation Program) 개요

개념	- 비밀로 분류되지 않은 중요 자료를 보호하기 위해 국가·공공기관에서 도입하는 암호모듈의 안전성과 구현 적합성을 검증하는 제도
관련 법적 근거	-「사이버안보 업무규정」제9조,「전자정부 시행령」제69조 등

II. KCMVP(Korea Cryptographic Module Validation Program) 상세 설명

가. KCMVP(Korea Cryptographic Module Validation Program) 보안적합성 시험·검증 절차



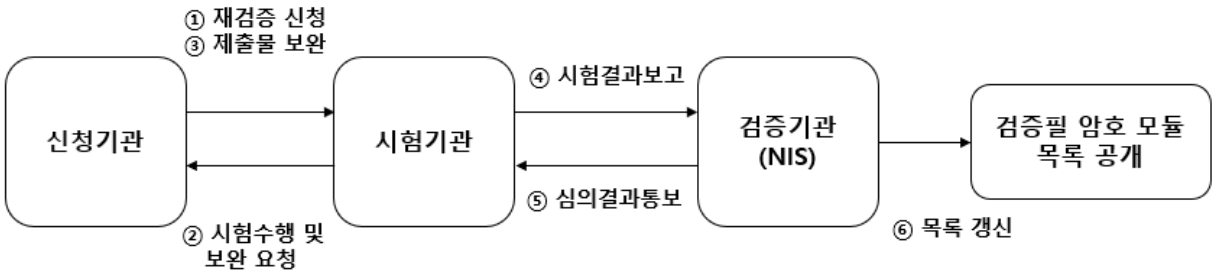
나. KCMVP(Korea Cryptographic Module Validation Program) 상세 설명

구분	항목	설명
시험·검증 절차	1. 시험 신청	- 암호모듈의 적절한 보안수준을 결정한 후, 제출물을 준비하여 시험기관에 시험 신청
	2. 시험 계약	- 시험기관은 신청서 및 제출물 검토 후 신청기관과 시험계약체결 - 암호모듈 시험요구사항에 따라 시험 수행
	3. 시험결과보고	- 시험 완료 후 검증기관에 시험결과 보고
	4. 시험·검증 결과 심의 의결	- 암호모듈 시험결과를 검토하여, 검증기준에 부합한지 여부와 시험결과의 타당성과 공정성 확인

	5. 심의결과 통보	- 검증기관은 암호모듈 검증 결과를 시험기관에 통보
	6. 목록 등재	- 검증이 완료된 암호모듈을 검증필 암호모듈 목록에 등재
검증 대상 암호 알고리즘	블록암호, 공개키 암호	- ARIA, SEED, LEA, HIGHT, RSAES
	해시함수	- SHA2, SHA3, LSH
	메시지 인증	- CMAC, GMAC, HMAC
	난수발생기	- CRT-DRBG, HASH-DRBG, HMAC-DRBG
	키설정, 키유도	- DH, ECDH, KBKDR, PKBKDF
	전자서명	- RSAPSS, KCDSA, EC-KCDSA, ECDSA

- 등재된 암호모듈의 검증 효력 만료되거나 형상 변경 시 별도 추가 조치가 필요함

III. 검증효력 만료 도래 시 및 형상 변경 시 조치 사항

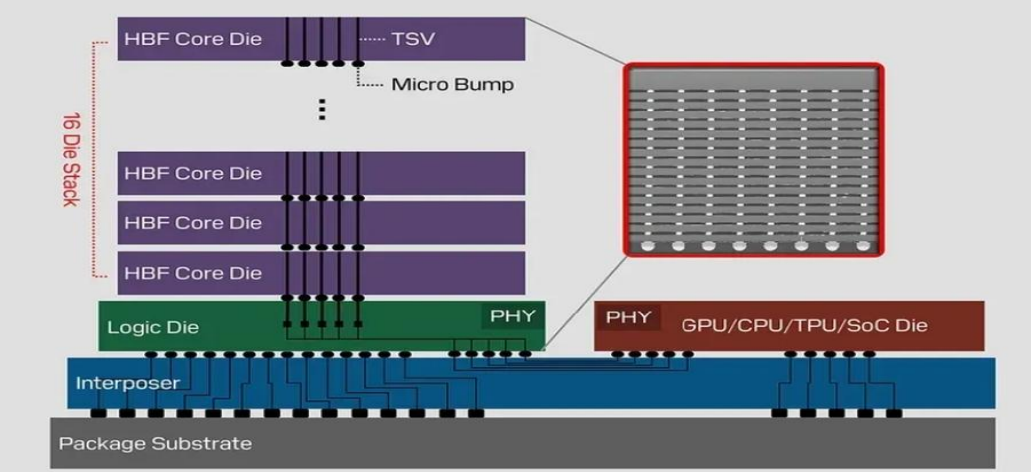


- 신청기간은 암호모듈 검증효력 연장을 위해 재검증을 신청할 경우 검증효력 만료 6개월 이전에 신청해야 함

"끝"

04	HBF(High Bandwidth Flash), HBS(High Bandwidth Storage)		
문제	HBF(High Bandwidth Flash)와 HBS(High Bandwidth Storage)		
도메인	컴퓨터구조	난이도	상 (상/중/하)
키워드	BiCS, TSV, 적층, VFO, TSV-Less		
출제배경	HBM 기출에 따른 추가 개발 진행중인 HBF, HBS 이해 확인		
참고문헌	ITPE 모의고사 https://www.trendforce.com/news/2025/11/11/news-sk-hynix-reportedly-explores-high-bandwidth-storage-stacking-nand-and-dram/		
출제자	정상반멘토 이상헌 기술사(제 118회 정보관리기술사 / bluesanta97@naver.com)		

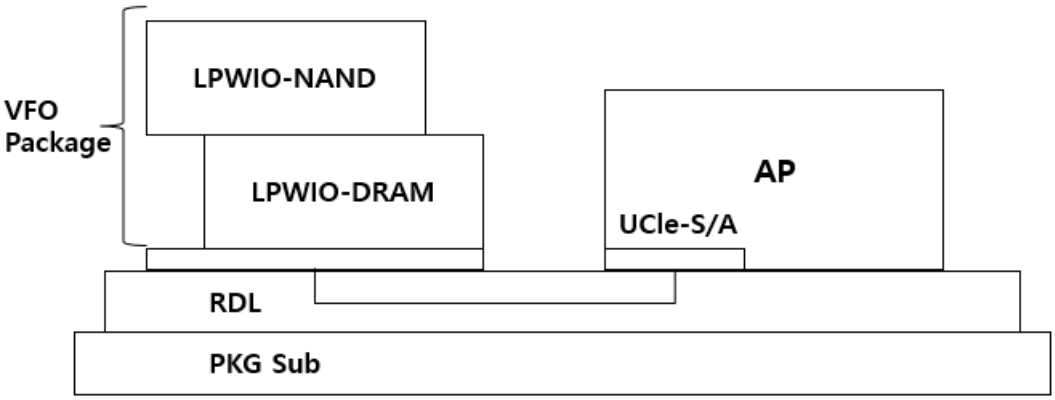
I. Flash Memory 적층, HBF(High Bandwidth Flash)의 개요



개념	- NAND Flash 메모리를 HBM과 유사한 3D 스택 구조로 패키징하여 높은 대역폭과 대용량, 비휘발성 특성을 동시에 제공하는 차세대 메모리 기술	
기술요소	- NAND 플래시 기반 및 BiCS 기술	- NAND 메모리 기술을 기반으로 개발되었으며, Sandisk의 BiCS 기술 위에 구축되어 용량 확장에 대한 명확한 경로 제공
	- CBA (CMOS directly bonded to Array)	- HBF에 초고밀도, 고속, 저전력 회로를 구현하게 하는 획기적인 기술로, 고대역폭 메모리 성능에 새로운 기준 설정
	- 고도화된 다이 적층 기술	- 다이의 뒤틀림/스트레스를 줄이고 열 전도성을 개선하며, 16개의 다이(die) 적층을 가능하게 함
	- TSV (Through-Silicon Vias) 및 로직 레이어	- HBM과 유사하게 3D 스택 구조로 패키징되며, TSV를 통해 층간 연결을 수행하며, 스택 하단에 특수 로직 레이어를 배치

- HBM은 높은 대역폭을 제공하는 기존의 3D 스택 DRAM 기술인 반면, HBF는 HBM의 한계를 보완하기 위해 Sandisk가 AI 추론(inferencing)에 맞추어 처음부터 개발한 NAND 플래시 기반의 혁신적인 메모리 기술

II. 이종 메모리 결합, HBS(High Bandwidth Storage)의 개요



개념	- 저전력 D램(LPWIO)과 낸드플래시를 수직으로 적층하여 하나로 만든 고대역폭 저장장치	
구성요소	- LPWIO-DRAM	- 입출력(I/O) 단자를 늘려 데이터 대역폭을 극대화한 저전력 와이드 I/O D램
	- LPWIO-NAND	- 대역폭을 극대화한 저전력 NAND Flash 메모리
기술요소	- VFO(Vertical Wire Fan-Out)	- 기존의 휘어진 와이어 본딩 대신 칩 사이를 직선으로 연결하는 기술
	- TSV-Less 공정	- 칩에 구멍을 뚫지 않고도 수직 연결을 구현하는 방식

- HBS는 최대 16개 D램과 NAND 칩을 수직으로 적층하여 구성하며, 모바일 기기에 탑재할 예정임

III. HBM, HBF, HBS의 비교

구분	HBM	HBF	HBS
주요 매체	- DRAM(휘발성)	- NAND Flash(비휘발성)	- DRAN + NAND 결합
수직적층방식	- TSV	- Parallel I/O	- VFO
핵심 역할	- GPU연산 데이터 즉시 처리	- 대용량 데이터 공급	- 온디바이스 AI 통합 가속
장점	- 최대 대역폭/속도	- 대용량 저장+고속 전송	- 메모리/저장장치 경계 해소
주요 타겟	- AI서버, GPU 가속기	- 대규모 AI 학습 서버	- 스마트폰, 온디바이스

- HBM은 연산중심, HBF는 저장 중심, 두가지 기능을 합친 HBS는 효율 중심의 기술로 발전 중

"끝"

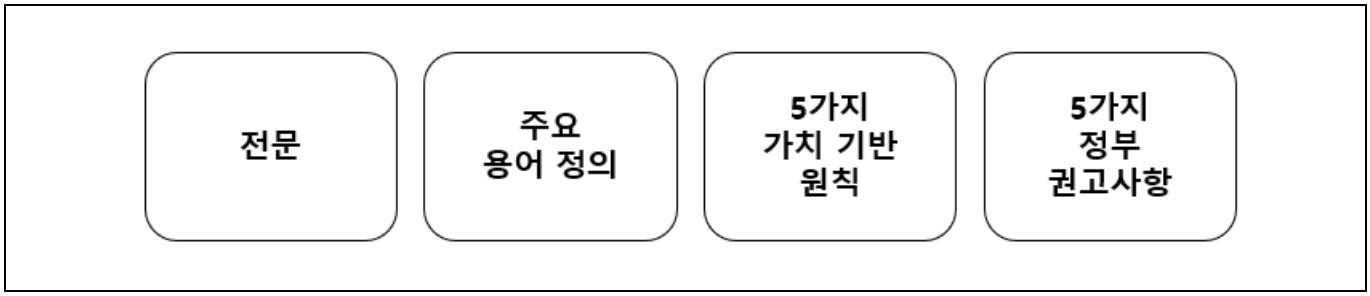
05	OECD AI 10개 원칙		
문제	OECD AI 10개 원칙		
도메인	인공지능	난이도	상 (상/중/하)
키워드	5가지 가치 기반 원칙, 5가지 정부 권고사항		
출제배경	OECD에서 채택한 AI 원칙에 대한 이해 확인		
참고문헌	한국 AI 정책 현황 및 발전 방안 : OECD AI 원칙을 중심으로-KISDI Perspectives(2025.9)		
출제자	정상반멘토 이상헌 기술사(제 118회 정보관리기술사 / bluesanta97@naver.com)		

I. 최초의 정부간 기구에서 채택된 원칙, OECD AI 10개 원칙의 개요

- 인공지능(AI) 기술이 인권과 민주주의 가치를 존중하며, 사회 전반에 신뢰받는 방식으로 개발·운영되어야 한다는 국제 기준

II. OECD AI 10개 원칙의 상세 설명

가. OECD AI 10개 원칙의 구성



- '23년부터 검토를 진행하였고, 검토 결과를 반영한 개정안을 '24년 OECD 각료이사회(MCM)에서 채택

나. OECD AI 10개 원칙 별 주요 내용

구분	원칙	주요 내용
5가지 가치 기반 원칙	1.1 포용적 성장, 지속가능한 개발 및 웰빙	- 인적 역량 증대, 창의력 향상, 과소 대표된 집단의 포용 증진, 불평등 감소, 자연환경의 보호 등 이로운 결과를 추구
	1.2 공정성 및 프라이버시를 포함한 법치, 인권 및 민주주의적 가치 존중	- 평등, 자유, 존엄성, 개인의 자율성, 개인정보 및 데이터 보호, 다양성, 공정성, 사회 정의, 노동권, 표현의 자유 등을 존중하고 오정보 및 허위 정보에 대처
	1.3 투명성 및 설명 가능성	- AI 시스템에 대한 이해 증진을 위한 정보, AI 시스템과의 상호작용에 관한 정보, 데이터/인풋의 출처, 요인, 프로세스 및/또는 논리에 관한 정보제공
	1.4 견고성, 보안성 및 안전성	- 위험이 있는 경우, 안전하게 시스템을 재정의, 수리 및/또는 폐기할 수 있는 메커니즘을 마련
	1.5 책임성	- 데이터 세트, 프로세스 및 의사결정과 관련하여 추적 가능성을 보장

5가지 정부 권고사항	2.1 AI 연구 개발에 투자	- 연구·개발 및 오픈 사이언스, 학제 간 노력을 포함하여 장기적인 공공 투자를 고려하고 민간 투자를 장려
	2.2 포용적인 AI 지원 생태계 조성	- 데이터, AI 기술, 컴퓨팅 및 연결 인프라, AI 지식 공유 메커니즘 등이 포함된 디지털 생태계의 개발과 접근을 촉진
	2.3 AI를 위한 지원 및 상호 운용 가능한 거버넌스 및 정책 환경 구축	- 민첩한 정책 환경을 장려하고, 규제실험을 고려하며, 유연성을 제공하는 성과 기반 접근방식을 채택하고, 상호 운용 가능한 거버넌스 및 정책 환경을 촉진하기 위해 관할권 내부 및 관할권 간 협력
	2.4 인적 역량 구축 및 노동 시장 변혁 대비	- 사람들이 AI 시스템을 사용하고 상호작용할 수 있도록 지원해야 하며, 필요한 역량(skill)을 제공
	2.5 신뢰할 수 있는 AI를 위한 국제 협력	- AI 지식 공유를 촉진하기 위해 협력하고, AI에 대한 전문 지식 축적을 위해 국가간, 부문간, 다자간 이니셔티브를 장려

- OECD의 법률 문서(legal instrument)는 법적 구속력이 없지만 동료 압박(peer pressure) 등으로 인해 회원국들이 이를 지키고자 하므로, OECD AI 원칙도 OECD 회원국들에 사실상 영향력을 미침

III. OECD AI 원칙의 활용

활용	설명
OECD AI 정책저장소	- OECD AI 10가지 원칙 관련 주요 블로그 및 보고서, 실시간 뉴스, 국가 정책 및 이니셔티브 등을 확인할 수 있음
OECD AI 국가 검토	- AI 국가 검토 시리즈는 OECD AI 원칙을 바탕으로 해당국이 각 원칙을 어떻게 이행하고 있는지 정책 및 국가 간 비교 통계를 통해 살펴보고 이를 토대로 권고사항을 도출
OECD AI 지수 (OECD AI Index)	- 현재 OECD AI 지수는 OECD AI 원칙 가운데 5가지 정부 권고사항만을 활용하고 있으나, 1차 지수 완성('25.11월 예정) 이후, 5가지 가치 기반 원칙을 기준으로도 세부 지표를 마련할 예정
OECD AI 원칙 이행 툴킷	- 자체 평가를 진행할 수 있도록 10개의 OECD AI 원칙에 따른 체크리스트를 제공하고, 원칙별로 이행 지침을 제공

- 국가 AI 정책을 점검하고 검토해야 하는 상황에서 OECD AI 원칙은 기준점으로 활용할 수 있음

"끝"

06	합성 데이터(Synthetic Data)		
문제	합성 데이터(Synthetic Data) 생성 기술		
도메인	데이터베이스	난이도	중 (상/중/하)
키워드	비모수 베이즈 방법, 연쇄 조건부 분포 방법, 변분오토인코더 방법, 생성적 적대 신경망, 디퓨전 모델		
출제배경	합성데이터 활용 안내서 발간으로 인한 출제 예상		
참고문헌	ITPE 서브노트 합성 데이터의 기술 동향과 향후 과제 - 주간기술동향 2201호(25.12)		
출제자	정상반멘토 이상헌 기술사(제 118회 정보관리기술사 / bluesanta97@naver.com)		

I. 실제 데이터 기반 모의데이터, 합성 데이터(Synthetic Data)의 개요

가. 합성 데이터(Synthetic Data)의 정의

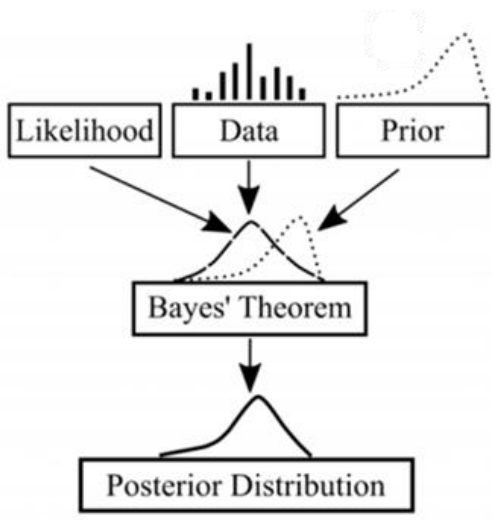
- 특정 목적을 위해 원본데이터의 형식과 구조 및 통계적 분포 특성과 패턴을 학습하여 생성한 모의(simulated) 또는 가상(artificial) 데이터

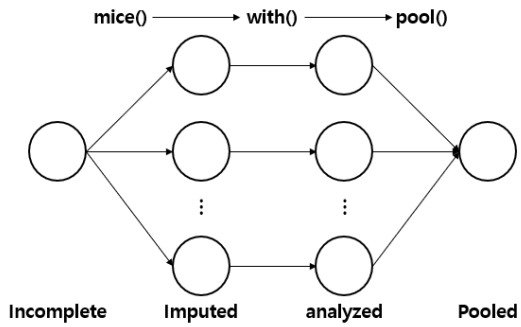
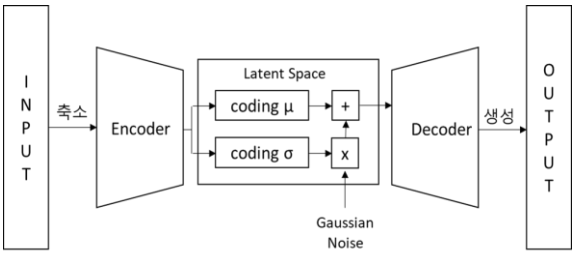
나. 합성 데이터의 필요성

안전한 데이터 사용	- 데이터의 개인정보와 기밀성을 보호하고, 데이터를 양적, 질적으로 고도화 목적 - 민감정보를 포함하고 있는 각종 데이터를 대체 가능
시간 및 비용 절감	- 소량의 원 데이터(Original Data)로 필요한 만큼의 데이터를 빠르게 생성 - 라벨링 작업을 별도로 하지 않더라도 정확하게 라벨링된 데이터셋 확보

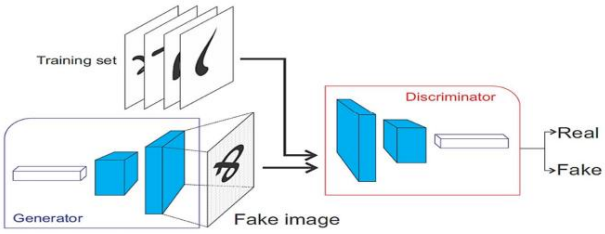
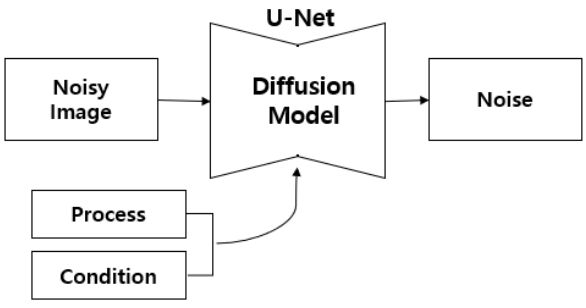
II. 합성 데이터(Synthetic Data) 생성 기술

가. 분포 추정 기반의 합성데이터 생성 기술

기술	개념도	설명
비모수 베이즈 방법		- 모수에 대한 사전 분포를 설정하고, 이를 실제 관측된 데이터를 통해 업데이트하여 사후 분포를 추론하는 통계적 원리에 기반 - DPMM: 비모수적 기법 - CDPMMN: 연산효율 높음 - HCMM-LD: 연속변수는 CDPMMN, 이산형 변수는 DPMPM 활용

연쇄 조건부 분포 방법		- 각 변수를 나머지 변수들에 대한 조건부 분포의 연쇄로 분해하여 모델링하는 접근법 - 장점: 선형 회귀부터 의사결정나무 같은 머신러닝 알고리즘 사용 가능 - 대표 알고리즘: MICE
변분 오토인코더 방법		- 평균(μ)과 표준편차(σ)를 학습하여 사후 확률을 최대화 하여 입력 데이터와 유사한 새로운 데이터를 생성하는 AI 기술

나. 분포 근사 기반의 합성데이터 생성 기법

기술	개념도	설명
생성적 적대 신경망		- 원본 데이터의 복잡한 잠재 분포를 학습하여 새로운 샘플을 생성하는 핵심적인 합성데이터 생성 방법론 - Table-GAN, CTGAN, CTAB-GAN 등
디퓨전 모델		- 점진적인 잡음 주입(noise addition)과 복원(denoising) 과 정을 통해 원본 데이터의 복잡한 분포를 정교하게 학습하는 최신 생성 방법론

- 합성 데이터 생성 시 개인정보가 포함될 수 있어 안정성 기준 및 비식별 처리가 중요하여 안전 기준 설정이 필요

III. 합성 데이터 안정성 유용성 평가 지표

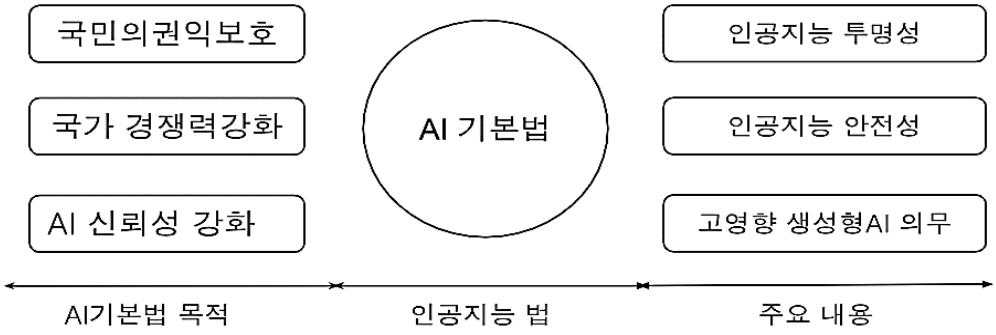
구분	데이터 유형	검증지표
유용성	비정형 합성데이터	- 모델 성능, Visual Turing Test, 이미지 품질
	정형 합성데이터	- 일차원 분포 유사성, 2차원 관계 유사성, 구별 불가능성, 모형성능 유사성
안전성	비정형 합성데이터	- 생성절차평가, 구조적 유사성, 지각적 유사성, 주관적 평가
	정형 합성데이터	- 구별 위험도, 연결 위험도, 추론 위험도

"끝"

07	AI 기본법		
문제	AI 기본법 주요 내용		
도메인	인공지능	난이도	중 (상/중/하)
키워드	고영향 생성형 AI, 국가 인공지능 위원회, 국내 대리인 지정 제도, 투명성 확보, 안정성 확보		
출제배경	AI 기본법 국회 본회의 통과 시행 예정		
참고문헌	인공지능 육성 및 신뢰 기반 조성 등에 관한 법률		
출제자	강북심화 이제이 기술사(제130회 정보관리기술사 / bwmslove@naver.com)		

I. 인공지능 신뢰 확보를 위한 법, AI기본법 개념 및 목적

가. AI기본법 개념



개념	- AI기술의 건전한 발전과 산업 국가의 경쟁력 강화 위한 AI 개념 규정, AI산업 발전 지원의 근거 및 기준을 명시한 인공지능 신뢰 기반 조성에 대한 규정 법안.

나. AI기본법 목적

구분	목적	설명
사회 측면	- 국민의 권익 보호	- 국민의 기본 권리와 자유를 적극 보호
	- 국민의 삶의 질 향상	- 국민 개개인의 삶의 질을 높이는 혁신적 서비스 제공
	- 국가 경쟁력 강화	- 기술력 확보 및 AI 산업 육성을 통한 경쟁력 강화
기술 측면	- AI 기술의 발전	- AI 기술의 혁신적 발전과 사회적 수용성을 함께 촉진
	- 신뢰 가능한 AI환경 조성	- 예측 결과와 의사결정 과정에 대한 투명성 확보, 윤리적·법적 책임 체계 마련

- AI 기본법의 핵심 주제는 금지 AI 제외 고영향 AI 책임 부분에 대한 신설

II. AI 기본법 주요 내용

가. 인공지능 건전한 발전 및 신뢰 기반 추진 체계 및 산업 활성화 설명

구분	주요 내용	설명
추진 체계	제6조 (인공지능 기본계획의 수립)	- 인공지능 등에 관한 정책의 기본 방향과 전략에 관한 사항
	제7조 (국가인공지능위원회)	- 대통령 소속으로 국가인공지능위원회를 관리
	제8조 (위원회의 기능)	- 계획 수립, 정책 , 연구 개발 사항, 고영향 AI 규율
산업 활성화	**제21조 (전문인력의 확보)**	- 인공지능기술 관련 해외 전문인력에 관한 조사・분석
	제22조 (국제협력 및 해외시장 진출의 지원)	- 인공지능산업 관련 해외진출에 관한 정보의 수집・분석 및 제공
	제23조 (인공지능집적단지 지정 등)	- 업무를 종합적으로 지원하는 전담기관을 설치하거나 지정

나. 인공지능 기술 개발과 산업 육성 및 윤리와 신뢰성 확보 설명

구분	주요 내용	설명
인공 지능 윤리	**제27조 (인공지능 윤리원칙)**	- 인공지능기술이 적용된 제품・서비스의 사용 가능한 접근성
	제28조 (민간자율인공지능윤리위원회의 설치)	- 인공지능기술 연구 및 개발을 수행하는 사람이 소속된 교육기관・연구기관
	제29조 (인공지능 신뢰 기반 조성을 위한 시책의 마련)	- 안전하고 신뢰할 수 있는 인공지능 이용환경 조성
	제30조 (인공지능안전성・신뢰성검・인증등 지원)	- 과학기술정보통신부장관이 지정한 자율적으로 추진하는 검증・인증 활동
	제31조 (인공지능 투명성 확보 의무)	- 인공지능사업자는 운용된다는 사실을 이용자에게 사전에 고지
	제32조 (인공지능 안전성 확보 의무)	- 수명주기 전반에 걸친 위험의 식별・평가 및 완화
고영향 인공지능	**제33조 (고영향 인공지능의 확인)**	- 기술정보통신부장관에게 확인
	제34조 (고영향 인공지능과 관련한 사업자의 책무)	- 위험관리방안의 수립・운영
	제35조 (고영향 인공지능 영향평가)	- 영향평가를 실시한 서비스를 우선적으로 고려
	제36조 (국내대리인 지정)	- 과학기술정보통신부장관에게 사전 신고

- 인공지능 법은 25년 1월 21일 제정하여 약칭 인공지능 기본법으로 2026년 1월 26일 시행 예정

III. AI기본법과 AI ACT의 차이점

구분	AI 기본법	AI ACT
신뢰성 확보	- 신뢰·윤리 기반 조성, 기술 촉진	- 시장 내 AI 위험 관리, 소비자 보호
인권 가치	- 사람 중심 AI 원칙 강조	- 기본권 보호 구체 명시
거버넌스	- 국가 AI 위원회 중심의 국가 전략	- 집행위원회(EU Commission) 중심 감독
법의 목적	- 자율성 확보	- 시장 안전성 확보

- AI 기본법은 산업 진흥·원칙 중심 접근이며, EU AI ACT는 위험 기반·강제적 규율로 공공 안전과 기본권 보호를 강화한 점이 주요 차이

"끝"

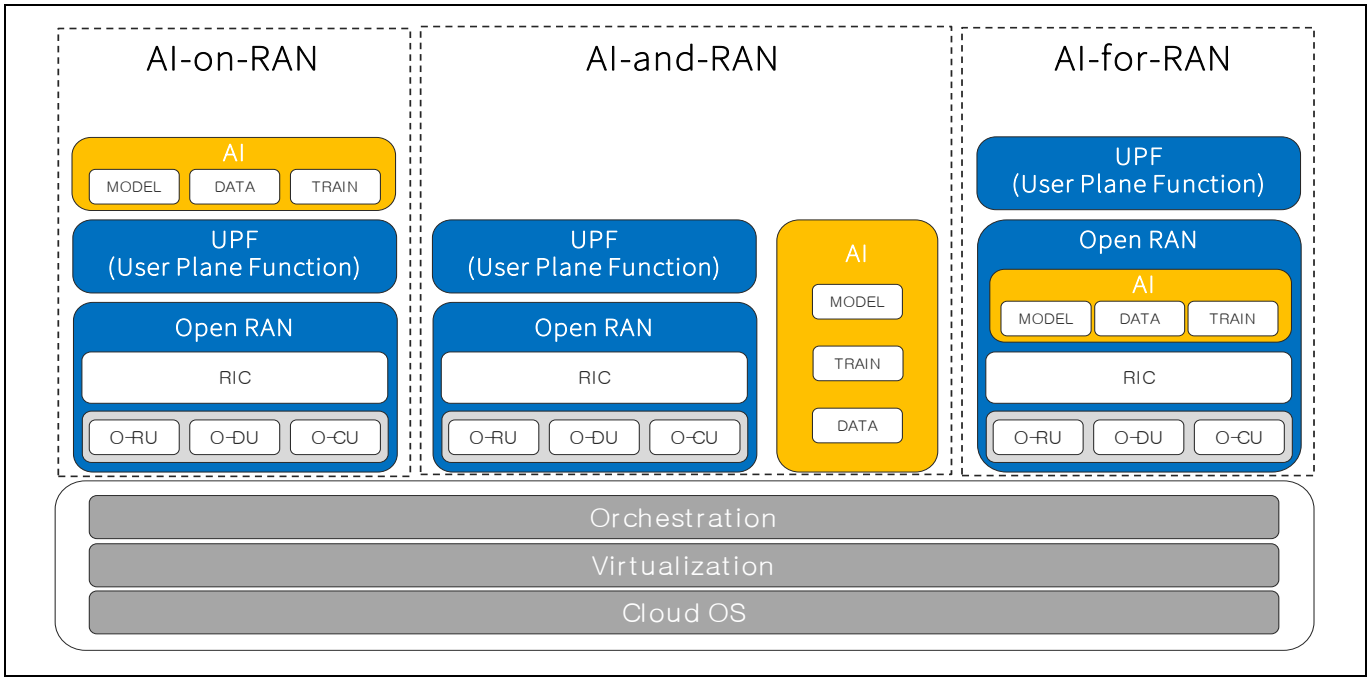
08	AI-RAN(Radio Access Network)		
문제	AI-RAN(Radio Access Network)		
도메인	NW	난이도	중 (상/중/하)
키워드	AI-on-RAN, AI-and-RAN, AI-for-RAN		
출제배경	6G 시대 핵심 기술		
참고문헌	ITPE 서브노트		
출제자	강북심화 이제이 기술사(제130회 정보관리기술사 / bwmslove@naver.com)		

I. NW와 AI의 접목, AI-RAN(Radio Access Network)의 개념

- 무선 접속망(RAN)에 인공지능 기술을 접목하여 네트워크 운영, 자원 관리, 장애 대응 등을 지능적으로 최적화하는 차세대 통신 기술

II. AI-RAN(Radio Access Network)의 구조와 기술 요소

가. AI-RAN(Radio Access Network)의 구조



- AI RAN 얼라이언스는 AI for RAN, AI and RAN, AI on RAN 3개 워킹 그룹을 구성

나. AI-RAN(Radio Access Network)의 기술요소

분류	기술 요소	설명
AI (Artificial Intelligence)	- 자율 치유 (Self-healing)	- 네트워크 문제를 자동으로 감지, 진단 및 해결하여 인력을 통하지 않고도 중단 없는 서비스를 보장하는 고급 네트워크 관리 시스템
	- 자가 최적화 (Self-optimizing)	- 토폴로지, 전파, 간섭 등의 상황을 인식(Context-aware)하여 스스로 네트워크 구성을 최적화

	- 자가 구성 (Self-configuring)	- 물리적 설치 이후 주변 환경 인식과 스스로 코어 네트워크에 접속하며 신규 기지국 추가 시 네트워크를 스스로 재구성
RAN (Radio Access Network)	- RIC (RAN 지능형 컨트롤러)	- RAN의 기능 제어 및 최적화, 다중 벤더의 상호 운용성 제공 - Non-RT RIC와 Near-RT RIC로 구성
	- RU (Radio Unit)	- 기지국의 무선 신호를 처리해 DU로부터 수신한 디지털 신호를 주파수 대역에 따라 신호로 변환
	- DU (Distributed Unit)	- 기지국의 디지털 신호를 처리해 무선 디지털 신호를 암호화
	- CU (Central Unit)	- 네트워크 소프트웨어 업무를 처리하고 통신 지연을 감소

- 워킹 그룹은 AI·머신러닝을 활용한 무선통신 최적화 기술, 효율적인 자원 관리와 인프라 활용 극대화를 위한 AI와 무선망 융합기술, AI무선망에서의 신규 AI 애플리케이션과 서비스 발굴을 주제로 본격적인 연구 진행

III. RAN(Radio Access Network)과 AI-RAN(Artificial Intelligence-enabled Radio Access Network)의 비교

비교 항목	RAN	AI-RAN
정의	- 이동통신 시스템에서 단말기와 코어 네트워크를 연결하는 무선 접속망	- 무선 접속 네트워크(RAN)에 자동화된 인공지능(AI)을 적용하여 효율성과 안전성을 향상한 무선 접속망
구조	- 안테나, 무선 장치(RU), 분산 장치(DU), 중앙집중식 장치(CU)	- 기존 RAN 구조에 AI 알고리즘과 머신러닝 모델 추가
네트워크 관리	- 사전 정의된 규칙과 수동 구성	- AI 알고리즘을 사용하여 네트워크를 동적으로 최적화와 AI 모델을 통해 발생 가능 문제를 사전 감지하고 예방
성능 최적화	- 정적인 리소스 할당 방식 - 네트워크 상황 변화에 대한 적응력이 제한적	- 실시간 네트워크 분석으로 동적 자원 할당과 지속적 성능 개선 진행
에너지 효율	- 트래픽 부하와 관계없이 일정한 전력 소비를 유지	- 트래픽 부하에 따라 전력 소비를 동적으로 조절

- AI-RAN은 기존 RAN의 한계를 극복하고 더 효율적이고 지능적인 네트워크 운영 가능

"끝"

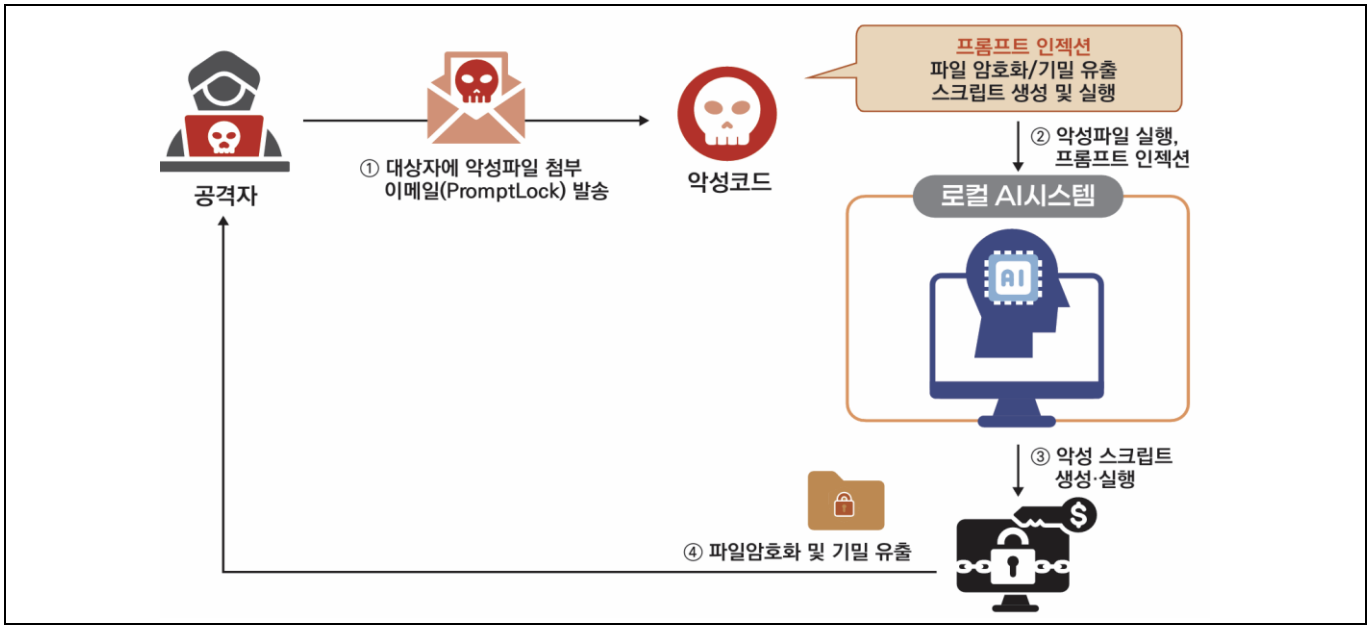
09	PromptLock		
문제	PromptLock		
도메인	보안	난이도	중 (상/중/하)
키워드	랜섬웨어, 악성파일 전달, 프롬프트 인젝션 유발, 악성 스크립트 생성·실행, 파일암호화 및 기밀 유출, AI-BOM, 가드레일, 레드팀 테스트		
출제배경	랜섬웨어 3.0 유형에 대한 이해도 확인		
참고문헌	국가정보원 AI 보안 가이드라인		
해설자	강북심화 이제이 기술사(제 130회 정보관리기술사 / bwmslove@naver.com)		

I. 최초의 AI기반 랜섬웨어, PromptLock의 개념

- 로컬에 접근 가능한 LLM을 통해 악성 Lua 스크립트를 실시간 생성하여 파일 열람·유출·암호화를 수행하는 적응형 랜섬웨어

II. PromptLock 공격절차 및 상세설명

가. PromptLock 공격절차



나. PromptLock 상세설명

절차	세부	설명
①	- 악성파일 전달	- 공격자가 악성 파일이 첨부된 이메일 등을 대상자에게 발송
②	- 프롬프트 인젝션 유발	- 대상자가 파일 실행 시 Ollama 기반 로컬 AI 모델 호출 및 프롬프트 인젝션 발생
③	- 악성 스크립트 생성·실행	- AI가 파일 암호화·정보 유출을 위한 악성 스크립트를 동적으로 생성·실행
④	- 파일암호화 및 기밀 유출	- 파일 암호화 및 기밀 데이터 외부 유출 발생

III. PromptLock 대응방안

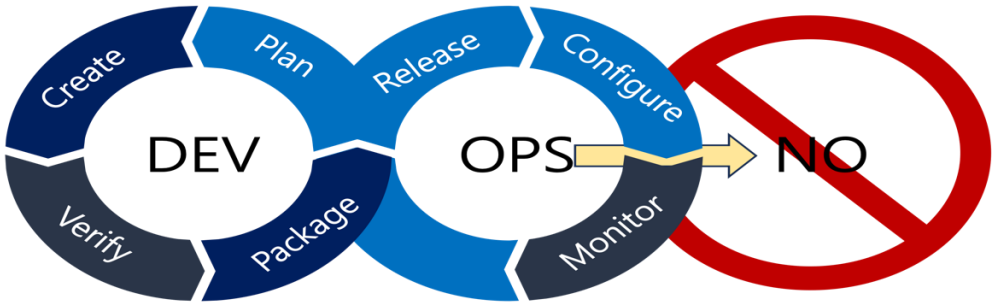
구분	핵심 기술	설명
기술적 측면	- AI-BOM	- AI 시스템의 구성요소(모델, 라이브러리 등)를 식별·관리하고 보안 취약점을 지속적으로 모니터링 및 업데이트
	- 필터링 및 가드레일 강화	- 프롬프트 인젝션 차단을 위한 입력 필터링, 악의적 요청 차단 로직 강화
관리적 측면	- 실행 제어 및 결과 검증	- AI 생성 결과(스크립트 등)에 대한 실행 제한, 코드 실행 여부를 사용자 승인 하에 제한
	- 적대적 모의공격 및 학습 강화	- 공격 시나리오 기반 Red Teaming 수행, AI 공격 유형 시뮬레이션 학습으로 사전 인지

- Promptware는 AI 오용 기반의 신종 보안 공격으로, AI-BOM 기반 구성관리와 Prompt 통제가 핵심

"끝"

10	데브옵스(DevOps)와 노옵스(NoOps)		
문제	데브옵스(DevOps)와 노옵스(NoOps) 비교		
도메인	소프트웨어공학	난이도	중 (상/중/하)
키워드	소통, 협업, 자동화, 가상화, 컨테이너, CI/CD, IAC, MSA		
출제배경	빅데이터와 머신러닝 결합한 AIOps 플랫폼을 통해 NoOps 도입하는 조직 증가에 따른 이해 확인		
참고문헌	TechTarget(https://www.techtarget.com/searchitoperations/definition/NoOps)		
출제자	강북심화 이제이 기술사(제 130회 정보관리기술사 / bwmslove@naver.com)		

I. 사라진 운영자, 데스옵스(DevOps)와 노옵스(NoOps)의 개념 비교



데스옵스(DevOps)	노옵스(NoOps)
- 시스템 개발자와 운영을 담당하는 정보기술 전문가 사이에서 소통, 협업 통합 및 자동화를 통해 어플리케이션과 서비스를 빠른 속도를 제공할 수 있도록 조직의 역량을 향상시키는 문화, 방식 및 도구의 조합	- 운영에 필요한 인프라를 가상화로 미리 구현하여 개발자는 H/W 인프라를 이해없이 어플리케이션의 배포, 모니터링, 관리 프로세스를 개선 및 자동화 하여 시스템 운영자 없이도 효율적이고 빠르게 장애대응 및 요구사항을 처리방식

- NoOps는 운영에 필요한 인프라를 미리 가상화로 구현하여 DevOps에 비해 효율적인 장애대응 및 요구사항 처리가능

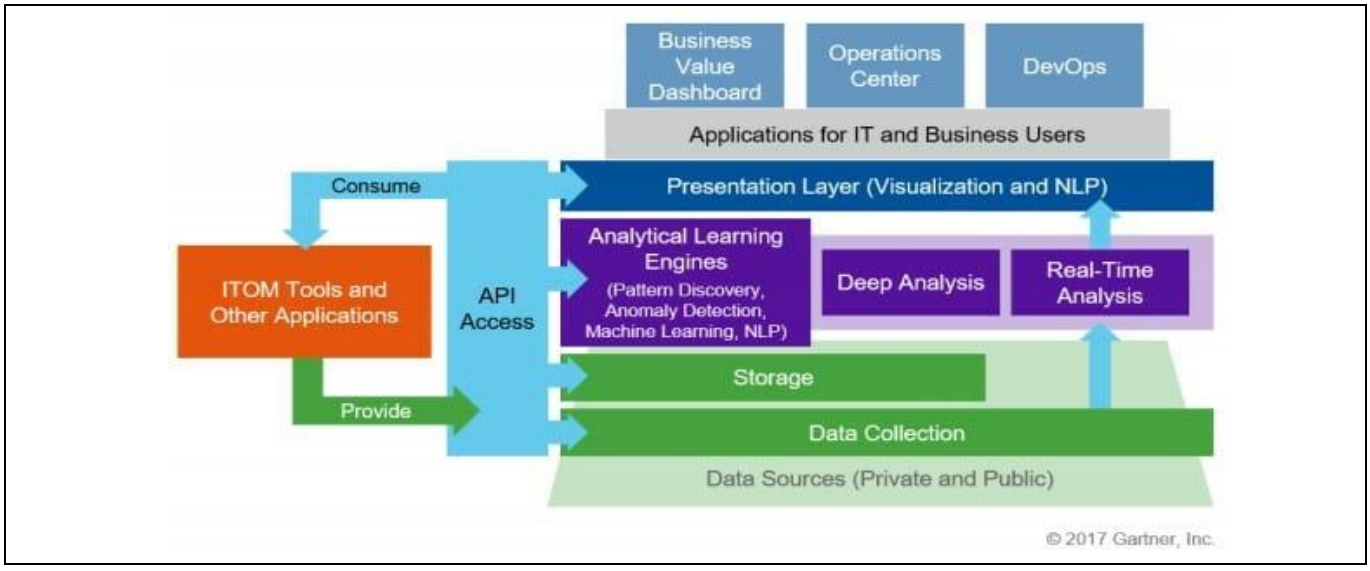
II. 데스옵스(DevOps)와 노옵스(NoOps)의 상세 비교

비교 항목	데스옵스(DevOps)	노옵스(NoOps)
관점	- 지속적인 피드백과 업데이트 중점	- 프로세스 최적화와 비즈니스에 집중
주요도구	- CI/CD - Provisioning - 테스트 자동화	- IAC(InfraStucture as Code) - MSA(Micro Service Architecture) - 컨테이너 관리 및 오케스트레이션 도구
개발생명주기 (SDLC)	- 요구사항 수립 - 분석, 설계, 개발 - 빌드, 테스트 - 배포 - 운영	- 개발 - 빌드, 테스트 - 배포 - 운영

운영 방식	- CI/CD, IaC(Infrastructure as Code), 모니터링, 협업 툴 등을 활용해 개발-운영 간 긴밀한 협력 필요.	- 클라우드 기반 PaaS, Serverless, 컨테이너 관리 서비스 등을 활용
한계/제약	- 문화적 변화(개발-운영 협업) 정착이 어려움	- 특정 클라우드/플랫폼에 종속 위험
적합한 환경	- 대규모 조직, 복잡한 인프라 운영 - 운영팀과 개발팀의 협업이 중요한 기업	- 스타트업, 빠른 개발 주기 필요 조직 - 운영 리소스를 최소화하려는 기업

- DevOps는 개발과 운영을 함께 하는 협업 기반 접근이고, NoOps는 운영 자체를 플랫폼/자동화에 맡겨서 개발자만 집중하는 접근
- DevOps로 CI/CD와 Deploy까지 자동화가 진행되면 배포 주기가 짧아져 이벤트·로그·티켓 데이터가 폭증하며, NoOps는 자동화가 미흡할 경우 알람·로그 분석과 조치를 사람이 떠안음으로서 병목 현상 발생

III. DevOps와 NoOps 문제 해결을 위한 AIOps 설명

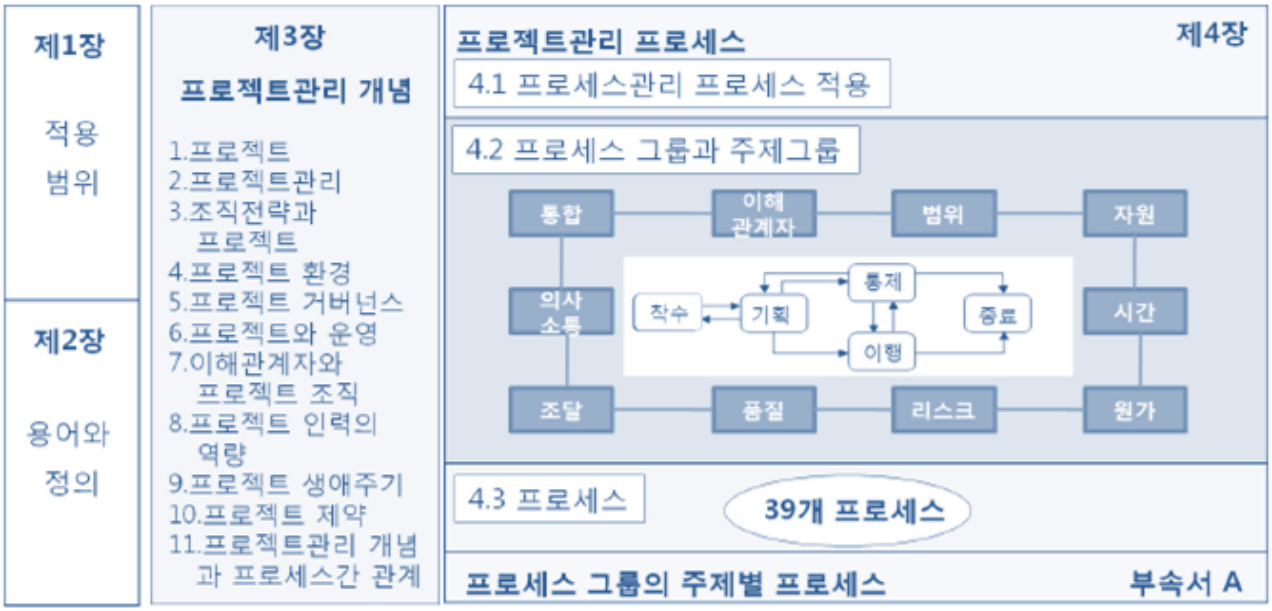


- AIOps를 통해 운영 데이터를 수집한 뒤 상관분석·이상탐지·근본원인분석(RCA)을 수행하고 API/Trigger 기반 자동조치와 시각화까지 연결해 자율 운영 현실화 가능

"끝"

11	ISO 21500		
문제	ISO 21500 구성모델		
도메인	프로젝트 관리	난이도	하 (상/중/하)
키워드	통합, 이해관리자, 범위, 자원, 일정, 원가, 리스크, 품질, 조달, 의사소통, 착수/기획/통제/이행/종료		
출제배경	130회 정보관리기술사 기출문제		
참고문헌	IT기술사회 자료		
출제자	강북심화 이제이 기술사(제 130회 정보관리기술사 / bwmslove@naver.com)		

I. 프로젝트 관리를 위한 지침 표준, ISO 21500의 개요



개념	- 국제적인 "프로젝트 관리에 대한 원칙과 절차"를 정립하기 위해 국제 표준화 기구 (ISO)에 제안한 프로젝트 관리에 대한 국제 표준

II. ISO 21500의 구성모델의 프로세스 그룹과 주제 그룹

가. ISO 21500 프로세스 그룹

프로세스 그룹	개념	주요 프로세스
착수	- 프로젝트 단계 또는 프로젝트 시작할 때 사용 - 프로젝트 단계 또는 프로젝트 목적을 정의 - 프로젝트 관리자 임명하여 프로젝트 작업 진행	- 프로젝트 헌장 개발 - 이해관계자 식별 - 프로젝트 팀 편성
기획	- 세부 계획 수립에 사용 - 세부 계획은 프로젝트 시행 관리가 가능해야 함 - 프로젝트 성과를 측정, 통제할 수 있는 기준선 수립 가능하도록	- 프로젝트 계획 수립 - 범위 정의 - 일정 개발

	충분히 구체적이어야 함	- 예산 편성
이행/실행	- 프로젝트 관리 활동 수행 - 프로젝트 계획에 따른 프로젝트 인도물 제공을 지원	- 프로젝트 작업 지시 - 품질 보증 수행
통제	- 프로젝트 계획 대비 실적을 모니터링, 측정, 통제 - 프로젝트 목표 달성을 위하여 예방 및 시정조치를 취하거나 변경 요청	- 프로젝트 작업 통제 - 변경 통제 - 범위 통제
종료	- 프로젝트 단계 또는 프로젝트의 완료를 공식화 - 필요할 경우 검토, 시행을 위한 교훈을 제공	- 프로젝트 종료 - 교훈 수집

나. ISO 21500 주제그룹

주제그룹	개념	주요 산출물
통합	- 프로젝트와 관련된 다양한 활동과 프로세스를 도출, 정의 결합, 단일화, 조정, 통제, 종료에 필요한 프로세스	- 프로젝트 헌장 - 프로젝트관리 계획서
이해관계자	- 프로젝트 스폰서, 고객사, 기타 이해관계자를 식별하고 관리	- 이해관계자 등록대장
범위	- 작업과 인도물을 식별하고 정의	- 작업분류체계
자원	- 인력, 시설, 장비, 자재, 기반 기설, 도구와 같은 적절한 프로젝트 자원을 식별하고 확보	- 자원계획 - 프로젝트 조직도
시간	- 프로젝트 활동의 일정을 수립하고 일정 통제의 진척상황을 관찰	- 활동기간산정, 일정표
원가	- 예산 개발과 원가통제의 진척상황을 관찰	- 원가산정, 예상
리스크	- 위험과 기회를 식별하고 관리	- 리스크 관리 대장
품질	- 품질보증과 품질통제를 계획하고 확립	- 품질계획, 시정조치
조달	- 계획에 요구된 프로세스를 포함하여 제품 및 서비스 또는 인도물을 인수하고 공급자와의 관계를 관리	- 조달 계획 - RFI, RFP
의사소통	- 프로젝트와 관련된 정보를 계획, 관리, 배포	- 의사소통 계획, 정보배포

III. ISO 21500과 PMBOK와의 비교

구분	ISO 21500	PMBOK
표준화 기관	ISO(국제표준기구)	미국 PMI
표준 구분	De jure Std. 법에 따른	De facto Std. 사실상의
목적	프로젝트 관리 지침 제공	
프로세스 그룹	5개 프로세스 그룹	
프로세스 수	39개	49개
주제/지식 그룹	10개 주제 영역	10개 지식 영역
특징	입력물과 산출물만 규정 도구 및 기법은 사용자 자율	입력물과 산출물 + 도구 및 기법 규정

- ISO 21500은 PMBOK의 프로세스와 지식영역을 수용하여, 최소한의 지침(상위수준에서의 개념과 프로세스에 대한 설명)을 제공

"끝"

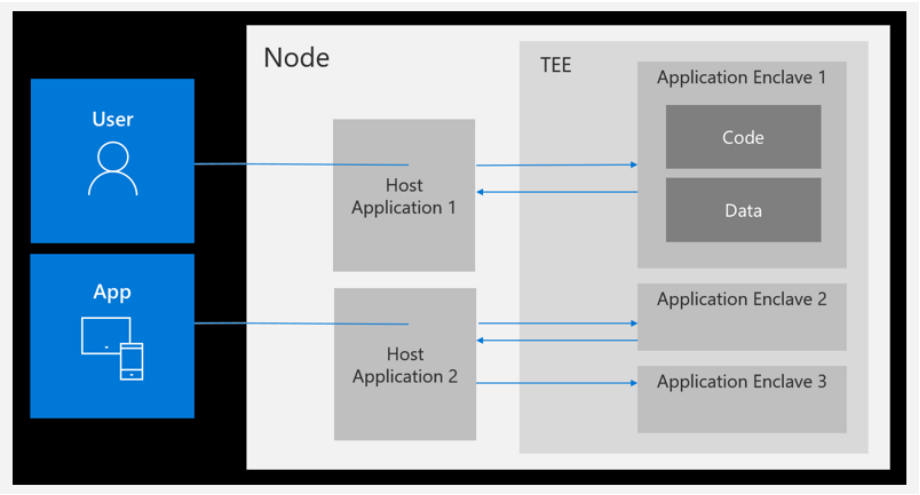
12	CC(Confidential Computing)		
문제	CC(Confidential Computing)		
도메인	보안	난이도	중(상/중/하)
키워드	Data-in-use, TEE, Confidential VM, Enclave, TPM/vTPM, 메모리 암호화, 원격 증명, Remote Attestation		
출제배경	한국정보공학기술사회 2026년 10대 전략 기술 트렌드 선정		
참고문헌	Confidential Computing Consortium		
해설자	강북심화 이제이 기술사(제130회 정보관리기술사/bwmslove@naver.com)		

I. Data-in-use 보안 기술, CC(Confidential Computing) 개념

- 데이터가 처리(Data-in-use)되는 동안에도 하드웨어 기반의 보안 기술(TEE 등)을 통해 데이터를 보호하는 컴퓨팅 기술

II. CC(Confidential Computing) 아키텍처 및 기술요소

가. CC(Confidential Computing)의 아키텍처



(출처: Confidential Computing Consortium)

- 하드웨어 기반 TEE의 Enclave에서 코드를 격리 실행하거나, 메모리 영역을 자체 암호화하는 Enclave에서 코드를 실행함으로써 데이터 사용 중(In-use) 기밀성을 보장

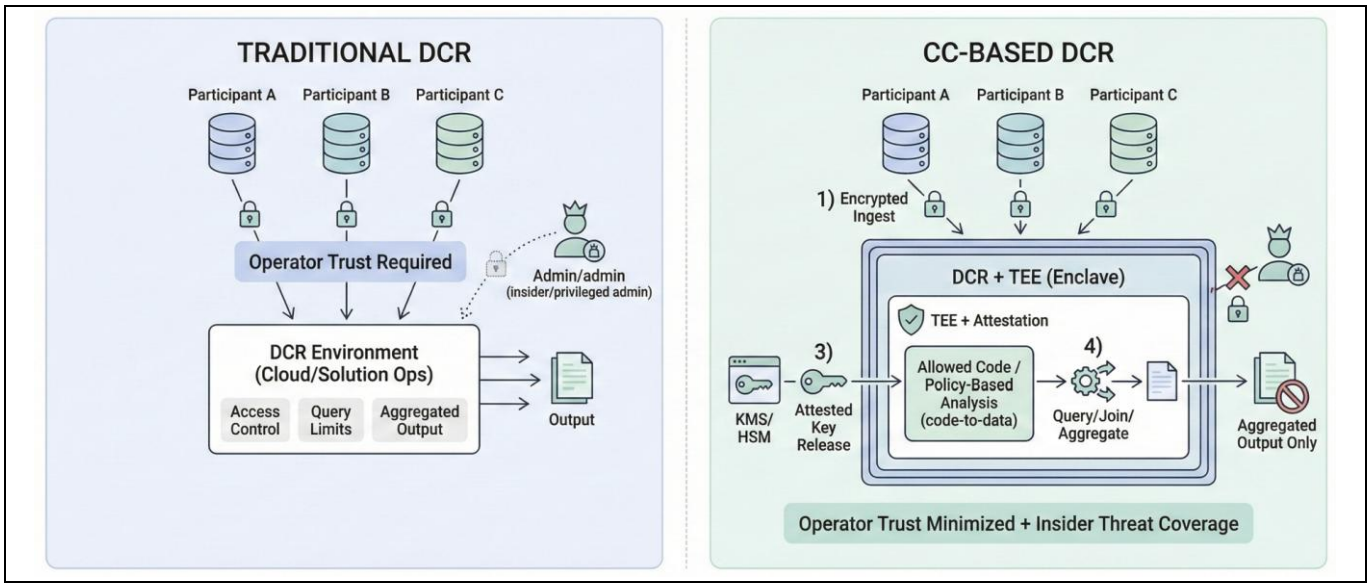
나. CC(Confidential Computing)의 기술요소

구분	기술요소	설명
환경	- TEE	- CPU 보호 영역에서 코드를 격리 실행해 OS·하이퍼바이저·관리자 접근을 차단
	- Confidential VM	- VM 단위로 실행환경을 하드웨어로 격리해 멀티테넌트 환경에서 Data-In-use 보호 강화
보호	- Enclave 방식	- 민감 연산을 Enclave로 캡슐화해 애플리케이션 단위 Data-In-

		use 보호 강화
	- TPM/vTPM	- 부팅~런타임 상태를 측정·저장·검증해 신뢰 체인을 구성
암호화	- 메모리 암호화	- 처리 중 데이터가 메모리에 존재하는 동안 암호화로 덤프/스니핑 공격 완화
인증	- 원격 증명 (Remote Attestation)	- "지금 이 워크로드가 검증된 TEE에서 실행 중"임을 서명된 증거로 검증

- CC의 핵심은 TEE와 원격증명으로 실행환경의 무결성과 신뢰성을 보장하는 것이며, 이를 DCR과 같은 데이터 협업 분석 플랫폼에 결합해 운영자(특권 관리자) 레벨까지 위협 범위를 최소화하는 방식으로 활용가능

III. 운영자 신뢰 확보, CC-based DCR 개요



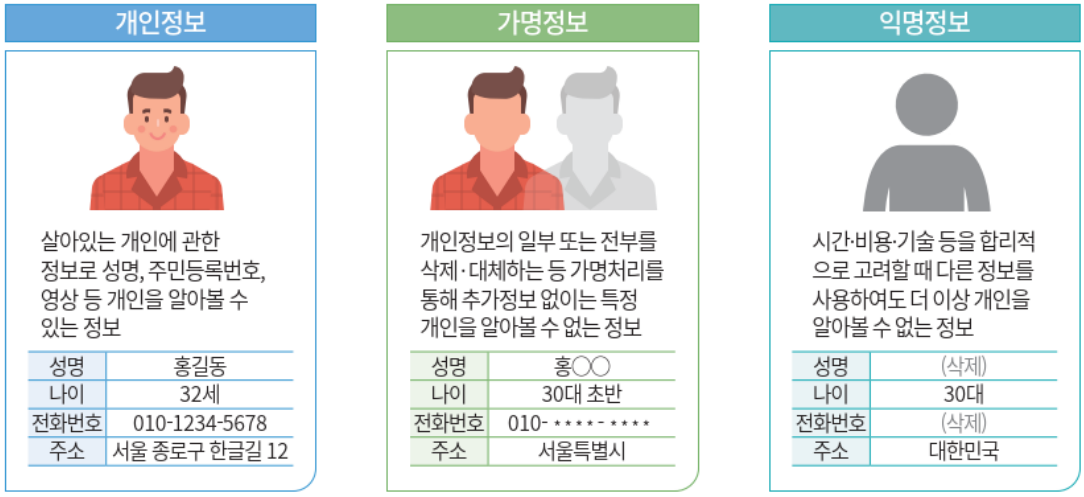
- CC-based DCR은 "쿼리/출력 통제형 DCR"에 "TEE+원격증명+키 릴리즈"를 결합해, 운영자 신뢰까지 확보하는 다자간 데이터 협업 보안 아키텍처

"끝

13	가명처리(Pseudonymization)		
문제	가명처리(Pseudonymization) 기법에 대하여 설명하시오.		
도메인	보안	난이도	중 (상/중/하)
키워드	통계(총계), 일반화(랜덤/제어/일반 라운딩, 범주화), 암호화(동형, 순서보존, 형태보존, 다형성), 무작위화(잡음, 치환, 토큰화), 기타(차분 프라이버시, 샘플링), **ISO/IEC 20889, 이미지 필터링 기술, 이미지 암호화, 얼굴 합성, 인페인팅**		
참고문헌	ITPE 기술사회		
풀이기술사	강북심화 이제이 기술사(제 130회 정보관리기술사 / bwmslove@naver.com)		

I. 임의의 다른 이름으로 대체, 가명처리 개념

가. 가명처리의 개념



가명 처리 개념	- 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 기술(개인정보보호법 제2조1의2)

II. 가명처리 기법

가. 정형 데이터 가명처리 기법

구분	기술	설명
삭제기술	삭제	- 원본정보에서 개인정보를 단순 삭제 - 부분삭제, 로컬삭제, 행 항목 삭제 등 다양한 기법 존재
	마스킹	- 특정 항목의 일부 또는 전부를 공백 또는 문자로 대체
통계도구	총계처리	- 평균값, 최댓값, 최솟값, 최빈값, 중간값 등으로 처리
	부분 총계	- 다른 정보에 비하여 오차 범위가 큰 항목을 평균값 등으로 대체
일반화	일반 라운딩	- 올림, 내림, 반올림 등의 기준을 적용하여 집계 처리하는 방법
	랜덤 라운딩 (Random rounding)	- 수치 데이터를 임의의 수인 자리 수, 실제 수 기준으로 올림(round up) 또는 내림(round down)하는 기법
	제어 라운딩	- 라운딩 적용 시 값의 변경에 따라 행이나 열의 합이 원본의 행이나 열

	(Controlled rounding)	의 합과 일치하지 않는 단점을 해결하기 위해 원본과 결과가 동일하도록 라운딩을 적용하는 기법
	상하단코딩 (Top and bottom coding)	- 정규분포의 특성을 가진 데이터에서 양쪽 끝에 치우친 정보는 적은 수의 분포를 가지게 되어 식별성을 가질 수 있음 - 이를 해결하기 위해 적은 수의 분포를 가진 양 끝단의 정보를 범주화 등의 기법을 적용하여 식별성을 낮추는 기법
	로컬 일반화	- 전체 정보집합물 중 특정 열 항목(들)에서 특이한 값을 가지거나 분포상 의 특이성으로 인해 식별성이 높아지는 경우 해당 부분만 일반화를 적용하여 식별성을 낮추는 기법
	범위 방법 (Data range)	- 수치 데이터를 임의의 수 기준의 범위(range)로 설정하는 기법으로, 해당 값의 범위 또는 구간(interval)으로 표현
	문자데이터 범주화	- 문자로 저장된 정보에 대해 보다 상위의 개념으로 범주화하는 기법
암호화	양방향 암호화	- 특정 정보에 대해 암호화와 암호화된 정보에 대한 복호화가 가능한 암호화 기법 (대칭키, 비대칭키 방식으로 구분)
	암호학적 해쉬함수	- 원문에 대한 암호화의 적용만 가능하고 암호문에 대한 복호화 적용이 불가능한 암호화 기법(MDC, MAC로 구분)
	순서보존 암호화	- 원본정보의 순서와 암호값의 순서가 동일하게 유지되는 암호화 방식
	형태보존 암호화	- 원본 정보의 형태와 암호화된 값의 형태가 동일하게 유지되는 암호화 방식
	동형암호화	- 암호화된 상태의 연산값을 복호화 하면 원래의 값을 연산한 것과 동일한 결과를 얻을 수 있는 4세대 암호화 기법
무작위화 기술	잡음 추가	- 개인정보에 임의의 숫자 등 잡음을 추가하는 방법
	치환	- 분석 시 가치가 적고 식별성이 높은 열 항목에 대해 대상 열 항목의 모든 값을 열 항목 내에서 무작위로 순서를 변경하여 식별성을 낮추는 기법
	토큰화	- 개인을 식별할 수 있는 정보를 토큰으로 변환 후 대체함으로써 개인정보를 직접 사용하여 발생하는 식별 위험을 제거하여 개인정보를 보호하는 기술
	(의사)난수생성기 ((P)RNG, (Pseudo) Random Number Generator)	- 주어진 입력값에 대해 예측이 불가능하고 패턴이 없는 값을 생성하는 메커니즘으로 임의의 숫자를 개인정보와 대체
기타 기술	표본추출 (Sampling)	- 데이터 주체별로 전체 모집단이 아닌 표본에 대해 무작위 레코드 추출 등의 기법을 통해 모집단의 일부를 분석하여 전체에 대한 분석을 대신하는 기법
	재현데이터 (Synthetic data)	- 원본과 최대한 유사한 통계적 성질을 보이는 가상의 데이터를 생성하기 위해 개인정보의 특성을 분석하여 새로운 데이터를 생성하는 기법
	차분 프라이버시 (Differential privacy)	- 특정 개인에 대한 사전지식이 있는 상태에서 데이터베이스 질의(Query)에 대한 응답 값으로 개인을 알 수 없도록 응답 값에 임의의

		숫자 잡음(Noise)을 추가하여 특정 개인의 존재 여부를 알 수 없도록 하는 기법 - 1개 항목이 차이나는 두 데이터베이스간의 차이(확률분포)를 기준으로 하는 프라이버시 보호 모델

- **개인정보 비식별조치 가이드라인, ISO/IEC 20889**를 활용한 가명, 익명화 처리

나. 비정형데이터 가명처리 기술

구분	기술	세부기술
영상정보	- 이미지 필터링 기술	- 블러링, 픽셀화, 마스킹
	- 이미지 암호화	- 픽셀 위치 기반 암호화
	- 얼굴 합성	- K-same 모델, K-Same-Select 모델
	- 인페인팅	- 패치 기반 인페이팅, 객체 기반 인페인팅 기술
	- AI 이용 가명처리	- GAN, 얼굴 보존형 가명처리 기술, AnonymousNet 프레임워크
음성정보	- 음성정보 자체 가명처리	- 음성 변형, 음성 변환, GMM, HMM, 평균값, 최댓값, 최솟값, 최빈값, 중간값 등으로 처리
	- 음성을 텍스트로 변환 (STT, Speech To Text)	- 개인식별정보가 포함된 음성을 텍스트로 변환 후 변환한 텍스트에서 개인정보를 가명처리하고 다시 음성으로 변환
텍스트 정보	- 규칙기반 삭제, 마스킹	- 정의된 형태에 기반하여 해당 정보 삭제하거나 마스킹
	- 스크러빙	- 원 텍스트의 내용과 구조를 보존하면서 개인식별정보만을 제거하는 기술
	- 정규표현식	- 문자나 혹은 문자열의 일정한 패턴을 표현하는 형식 언어
	- Annotation	- 주어진 텍스트를 논리적으로 분할후 단어 주석 첨가 기법
	- AI 기반 텍스트정보 가명처리	- 딥러닝 기술 등을 적용한 자연어 처리 언어 모델을 활용
	- 텍스트를 테이블 형식으로 변환	- 텍스트를 구문 문법의 규칙에 따라 파싱한 다음 테이블 형태로 정렬한 후 나머지 데이터 삭제

III. 가명·익명 처리의 평가 기법

평가 기법	취약점	설명
k-익명성	- 연결 공격(linking attack)	- 주어진 데이터 집합에서 준식별자 속성값들이 동일한 레코드가 적어도 K개 존재하도록 하는 연결 공격 방어형 프라이버시 보호 모델
l-다양성	- 동질성 공격	- 주어진 데이터 집합에서 함께 익명화되는 레코드들(동일 집합)은 적어도 L개의 서로 다른 민감 정도를 가져야 한다는 프라이버시 보호 모델
t-근접성	- 분포도	- 동질 집합에서 민감 정보의 분포와 전체 데이터 집합에서 민감정보의 분포가 유사한 차이를 보이게 하는 프라이버시 보호 모델

"끝"

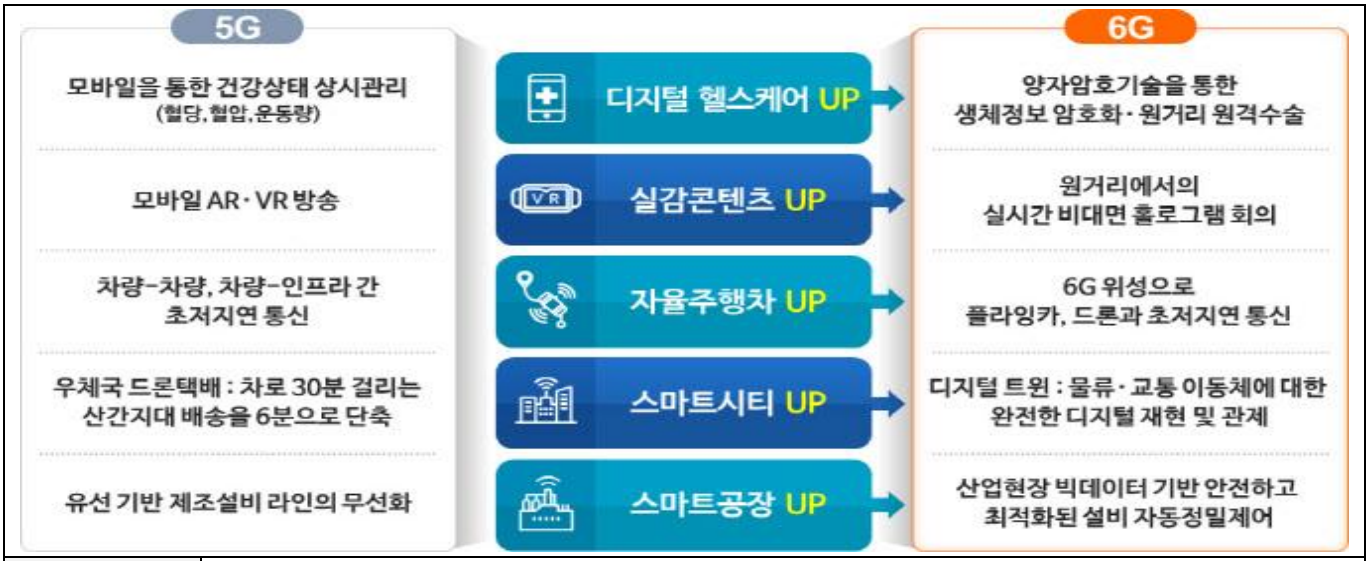
13	6G이동통신기술		
문제	6G 이동통신 특징과 주파수 동향에 대해 설명하시오.		
도메인	네트워크	난이도	중(상/중/하)
키워드	초성능, 초대역, 초현실, 초지능, 초정밀, 초공간, , Novel Antenna, 1Tbps, 10Km, 1000Km/h, 1Gbps, 저궤도 위성 mmWAVE, 테라헤르츠		
출제배경	135회 관리 2교시 출제		
참고문헌	ITPE 서브노트		
해설자	강북심화 이제이 기술사(제 130회 정보관리기술사 / bwmslove@naver.com)		

I. 차세대 이동통신, 6G의 기술적 의미

- 100 Gbps 이상의 최대 전송 속도, 1ms 이하의 지연 시간, 1000억개의 기기 연결, 10cm 이하의 위치 초정밀, 정확도, 초신뢰성의 이동통신기술

II. 6G이동통신 특징 및 주파수 동향

가. 6G이동통신 특징



초성능	- Tbps급무선통신기술, Tbps급광통신인프라기술
초대역	- 6G 이동통신지원RF 기술, 6G 주파수확보기술
초현실	- 초실감3차원공간미디어, 텐저블미디어서비스기술 - 6G방송통신융합미디어 기반 전송 기술
초지능	- 지능형무선엑세스네트워크기술, 초유연 6G 모바일코어 - 멀티도메인/멀티스페이스6G 네트워크자동화
초정밀	- Tbps급무선통신기술 - 6G 네트워크 종단간 초저지연 고정밀 고가용 네트워크 기술
초공간	- 3 차원 공간 이동체 브로드 밴드 무선 통신 기술 - 천 음속 급 이동통신기술, 6G우주 인프라 및 액세스

나. 6G이동통신 주파수 동향

구분	주파수 동향	설명
테라헤르츠 대역	100GHz~10THz	- 초고속 데이터 전송에 유리 - 전파 감쇠가 심하고 도달 거리가 짧음
Sub-THz 대역	7~24GHz	- 전파 도달 거리가 길고 건물 투과율이 높음
리미터파(mmWave) 대역	30~100GHz 대역	- 5G에서도 사용되는 대역으로 재활용 가능

- 6G 이동통신은 테라헤르츠(THz) 대역을 포함한 광대역 주파수를 활용할 것으로 예상

III. 6G이동통신기술 성능 요구사항

항목		6G 요구사항	비교를 위한 5G 요구사항
초성능	최대 전송률	- 1Tbps	- 20Gbps
	체감 전송 속도	- 1Gbps	-100Mbps
	광 액세스	- Tbps 급	-최대20Gbps
초대역	주파수 대역	- 100Ghz 대역 이상	-100Ghz 대역이하
	대역폭	- 수십 Ghz 대역폭	-수Ghz 대역폭
초공간	지원 고도	- 지상 10Km 이하	-지상120m 이하
	지원 속도	-1000km/h 이하	-500km/h 이하
	무선 구간 지연	-0.1ms	-1mc 이하
	종단간 지연	-수ms	-N/A
초지능		-학습기반의 이동통신(연결지능)	-해석적기반의 이동통신
초현실		-5감인지실감미디어(6DoF)	-시청각3D 미디어(3DoF)

"끝"

제136회 대비 ITPE
Final Round 해설집 (2일차)

대 상 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사, 정보시스템감리사 시험
발행일 2026년 02월 01일
집 필 강정배 PE, 서O욱 PE, 조재원 PE, 이상헌 PE, 이제이 PE, 전일 PE, 김찬일 PE, 강진우 PE
장O호 PE, 백현 PE, 정상 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
연락처 070-4077-1267 / itpe@itpe.co.kr