제129회 컴퓨터시스템응용기술사 해설집

2023.02.04

국가기술자격 기술사 시험문제

기술사 제 129 회 제 1 교시 (시험시간: 100 분)

분야	정보통신	자격종목	컴퓨터시스템응용기술사	수검번호		성명	

※ 다음 문제 중 10 문제를 선택하여 설명하시오. (각 10 점)

1. PIM(Processing in Memory)

2. CSAP(Cloud Security Assurance Program)

3. 웹 애플리케이션 방화벽(WAF: Web Application Firewall)

4. 스마트양식장(Smart Fish Farm)

5. 페어 프로그래밍(Pair Programming) 기법과
   핑퐁 프로그래밍(Ping Pong Programming)기법에 대하여 각각 설명하시오

6. 3-상태 버퍼(Tier-State Buffer)

7. 소프트웨어 리팩토링(Refactoring)

8. 전송 부호화 기법의 소스코딩(Source Coding)과 채널코딩(Channel Coding)을
   비교하여 설명하시오.

9. HBM(High Bandwidth Memory)

10. 자동차 통신 등에 활용하는 CAN(Controller Area Network)

11. 튜링테스트

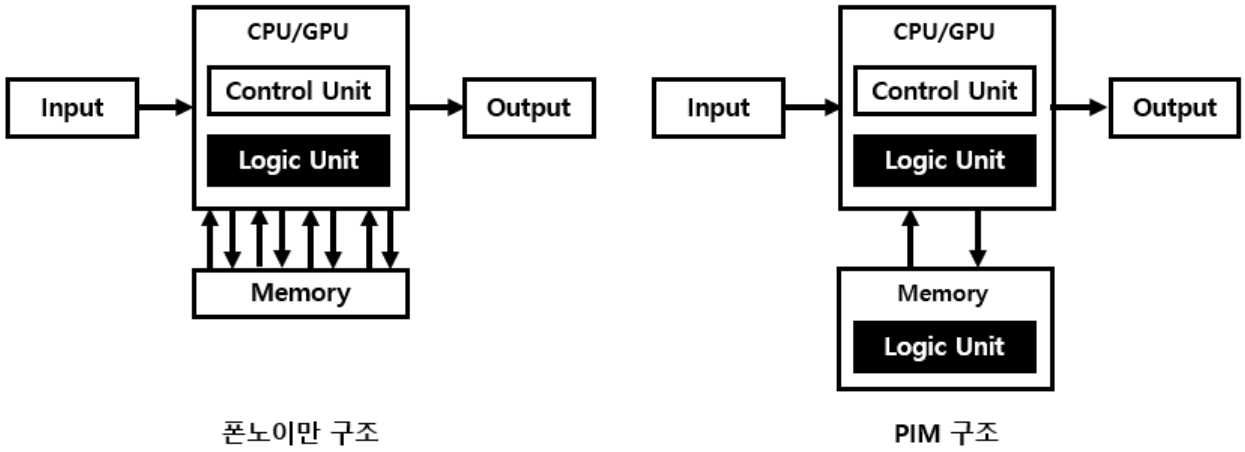
12. Cache Memory 의 쓰기 정책인 Write Through 방식과 Write Back 방식을 비교하여 설명하시오.

13. 상용 소프트웨어 직접구매 제도

01	PIM(Processing in Memory)		
문제	PIM(Processing in Memory)		
도메인	CA	난이도	중(상/중/하)
키워드	Logic DIE, 3D-packaged DRAM, Processor DIE Processing with memory, Processing in memory, Processing near memory		
출제배경	AI·종합반도체 강국 실현 3대 실행 과제 중 하나인 PIM에 대한 출제		
참고문헌	프로세싱 인 메모리시스템(안준환, 유승주, 최기영 저, 정보과학회지, 2016.07) A Processing-in-Memory Architecture Programming Paradigm for Wireless Internet-of-Things Applications ITPE 기술사회 자료		
해설자	소민호 기술사(제 119회 정보관리기술사 / mhsope@naver.com)		

I. 메모리 안에서 연산이 이루어지는, PIM(Processing In Memory) 개요

가. PIM의 개념



폰노이만 구조 PIM 구조

개념	- 데이터를 저장하는 **메모리 반도체 내부에 연산 작업에 필요한 프로세스 기능을 더한** 신개념의 메모리 반도체 - 메모리 안에서 혹은 메모리 근처에서 계산을 할 수 있도록 메모리 구조를 개선하는 기술

- PIM 구현 방법으로 Processing with memory, Processing in memory, Processing near memory 종류가 존재
- 메모리 안에서 혹은 메모리 근처에서 계산을 할 수 있도록 메모리 구조를 개선하는 기술

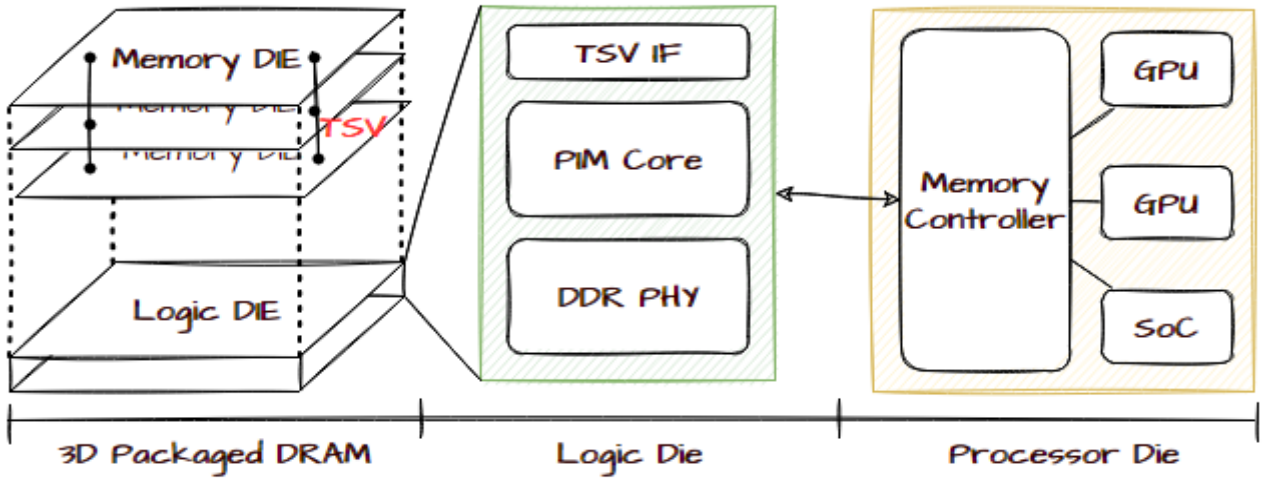
나. PIM의 특징

AI 가속화	- 메모리 내부 연산처리 기반 성능 극대화
병렬 프로세싱	- 메모리 내부 병렬 프로세싱 구현
전력 소모 감소	- 데이터 이동 감소에 의한 대량 데이터 처리, 에너지 효율성 향상
활용성/확장성 증가	- 기존 LPDDR, GDDR 메모리 적용, HBM 인터페이스 지원

- PIM의 메모리 내 연산처리 능력에 의한 AI, 빅데이터 처리 및 활용 가속화

II. PIM의 구조 및 구성요소

가. PIM의 구조



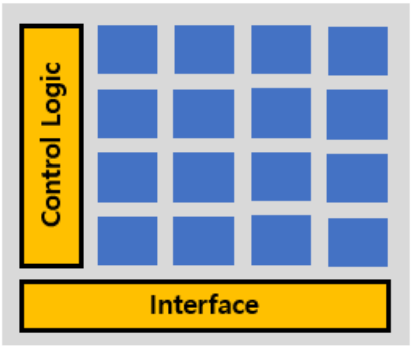
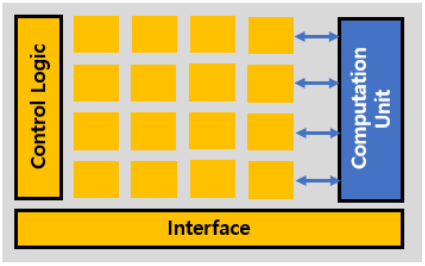
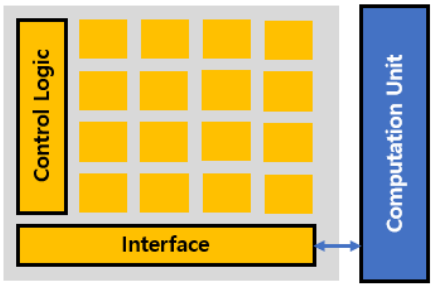
- Memory Package 기술에는 적층 방식, TSV 방식이 있으며, HBM과 TSV 방식 발전
- CPU와 메모리 사이 대역폭 제한 문제 해결 구조

나. PIM 구성요소

구분	구성요소	설명
Logic DIE	TSV Interface	- 실리콘 관통 전극 패키징 기술, Stack Layer 의 수천 연결 지원
	PIM Core	- DDR 에 고속 Access 지원, Data Intensive Processing
	DMA	- Physical, Logical Address 의 변환수행, 가상메모리 지원
	BUS	- 유기적 Data 전송위한 System Bus
	DDR PHY	- Uncacheable Memory Space 통한 PIM Core 연계
3D-packaged DRAM	Memory DIE	- 3D 적층 기술기반으로 물리적인 DRAM 의 결합
	Logic DIE	- PIM 구현을 위한 논리단위 처리
Processor DIE	Memory Controller	- Process in memory 처리를 위해 Unit 과의 연계 수행
	Unit	- 연산 수행을 위한 전통적인 Unit

- 메모리 내의 데이터 연산 기능을 제공함으로써 데이터 이동을 최소화하고, 전체적인 성능 극대화
- 기존 프로세서 기능 일부를 메모리가 담당하는 Memory Centric Computing구현 가능

III. PIM의 구현 방법의 분류

분류	구성도	상세 설명
Processing with memory		- 메모리 셀과 연산기가 한 몸으로 있어 **Memory Cell이 Processing logic과 같은 역할** - Bandwidth를 높이며, Data Transfer latency를 없앨 수 있음 - 연산에 적합한 형태로 저장하는 방법이나, 기능을 운용하는 방법이 잘 제시되지 않음
Processing in memory		- **메모리 다이(Memory Die)에 Processing Logic이 있는 형태** - With Memory 만큼의 성능은 내지 못하지만, 행렬을 이용하므로 좋은 병렬 처리가 가능
Processing near memory		- **Memory Device와 Process Logic이 가까이 있는 형태** - 기존 CPU에 적용하기 좋고 다양한 디자인 제시가 가능하나, CPU와 PIM간의 Memory에 데이터 쓰고 지우는 타이밍 충돌 가능

- With와 In은 Byte 접근성이 중요하여 NAND는 사용할 수 없고 현재 DRAM만 사용 가능

"끝"

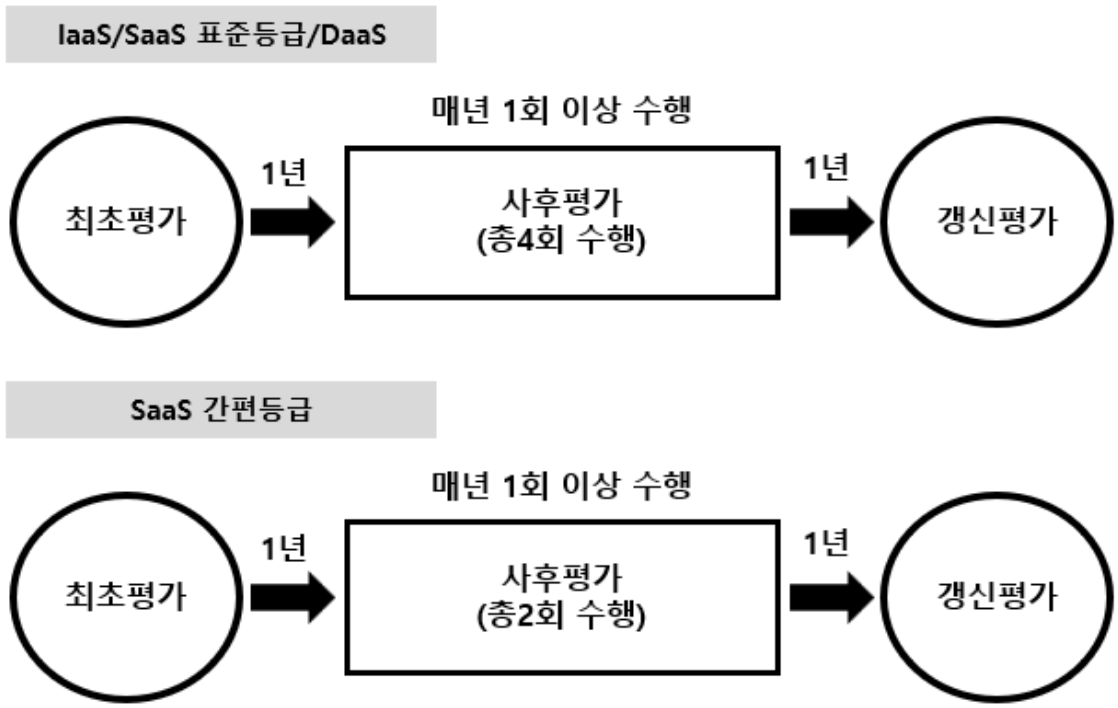
02	CSAP(Cloud Security Assurance Program)		
문제	CSAP(Cloud Security Assurance Program)		
도메인	정보보안	난이도	중(상/중/하)
키워드	최초평가, 사후평가, 갱신평가, 상/중/하 1. 정보보호 정책 및 조직 / 2. 인적보안 / 3. 자산관리 / 4. 서비스 공급망 관리 5. 침해사고 관리 / 6. 서비스 연속성 관리 / 7. 준거성 / 8. 물리적 보안 / 9. 가상화 보안 10. 접근통제 / 11. 네트워크 보안 / 12. 데이터 보호 및 암호화 13. 시스템 개발 및 도입 보안 / 14. 공공부문 추가 보안요구 사항		
출제배경	클라우드 컴퓨팅서비스 보안인증에 관한 고시 개정 및 등급제 변경에 따른 출제		
참고문헌	클라우드보안인증제(https://isms.kisa.or.kr/main/csap/intro/)		
해설자	소민호 기술사(제 119회 정보관리기술사 / mhsope@naver.com)		

I. 안전한 클라우드 컴퓨팅 서비스 정보보호 관리체계를 만들어가는, CSAP의 개요

가. CSAP의 개념

구분	설명
개념	- **클라우드 서비스 제공자**가 제공하는 서비스에 대해 **정보보호 기준의 준수여부 확인**을 인증기관이 평가·인증하여 이용자들이 안심하고 클라우드 서비스를 이용할 수 있도록 지원하는 제도
목적 및 필요성	- 공공기관에 안전성 및 신뢰성이 검증된 민간 클라우드 서비스 공급 - 객관적이고 공정한 클라우드 서비스 보안인증으로 이용자의 보안우려 해소, 클라우드 서비스 경쟁력 확보
추진근거	-『클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률』 제5조에 의한『제1차 클라우드 컴퓨팅 기본계획』(2015)의 클라우드 보안인증제 시행 -『클라우드 컴퓨팅 서비스 정보보호에 관한 기준 고시』 제7조에 따른 정보보호 기준의 준수여부 확인 (과학기술정보통신부 고시 제2017-7호)
평가·인증 범위 기준	- 공공기관의 업무를 위하여 제공하는 클라우드서비스의 모든 서비스를 포함하여 설정 (클라우드서비스 보안인증제는 클라우드컴퓨팅법 시행령 제3조의 서비스를 대상으로 시행 - 클라우드서비스에 포함되거나 관련 있는 자산(시스템, 설비, 시설 등), 조직, 지원서비스 등도 모두 포함하여 설정 (서비스 운영·관리를 위한 온·오프라인 자산 및 지원서비스, 안전성 및 신뢰성 확보를 위한(정보보호시스템, 로그관리시스템 등) - 식별된 자산 및 조직에 대해서는『클라우드컴퓨팅서비스 정보보호에 관한 기준 고시』의 관리적·물리적·기술적 보호조치 및 공공기관용 클라우드서비스 추가 보호조치를 준하여야 함

나. CSAP의 평가·인증 종류



구분	설명
인증 종류	- IaaS 분야 및 DaaS 분야 인증의 유효기간은 5년으로 운영 - SaaS 분야 인증은 표준등급에 대해서는 유효기간을 5년, 간편등급에 대해서는 유효기간을 3년으로 운영
최초평가	- 최초평가는 보안인증을 처음으로 취득할 때 진행하는 평가, 인증 취득기간 중 중요한 변경이 있을 경우 변경 사항에 대해 상시평가 가능
사후평가	- 보안인증을 취득한 이후 지속적으로 클라우드서비스 보안 평가·인증 기준을 준수하고 있는지 확인하기 위한 평가, 인증 유효기간(3~5년) 안에 매년 시행
갱신평가	- 보안인증 유효기간(3~5년)이 만료되기 전에 클라우드서비스에 대한 인증의 연장을 원하는 경우에 실시하는 평가

- 최초평가를 통해 인증을 취득하면, 5년(SaaS 간편등급은 3년)의 유효기간을 부여
- 갱신평가를 통과하는 경우, 3~5년의 유효기간을 다시 부여

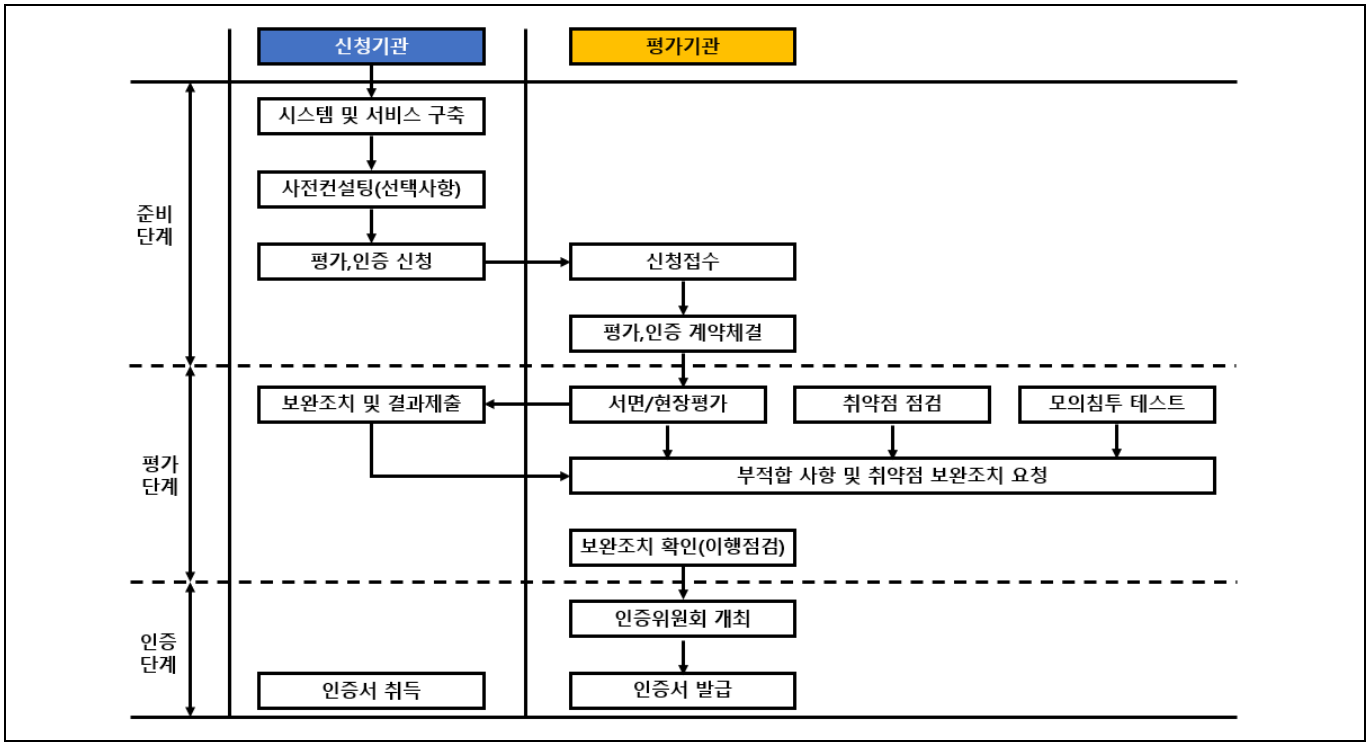
다. 클라우드 서비스 이용 '시스템 중요도' 등급 분류기준

분류등급	세부사항		영역분리
상	파급영향	- 해당 정보시스템에 대한 침해는 운영기관, 자산 및 개인에게 치명적 악영향을 미칠 수 있음	물리적 분리
	분류기준	- 국가 중대 이익(안보, 국가안전, 국방, 통일, 외교 등), 수사/재판 등 민간정보를 포함하거나 행정 내부 업무 등을 운영하는 시스템	
중	파급영향	- 해당 정보시스템에 대한 침해는 운영기관, 자산 및 개인에게 심각한 영향을 미칠 수 있음	물리적 분리
	분류기준	- 비공개 업무자료를 포함 또는 운영하는 시스템	
하	파급영향	- 해당 정보시스템에 대한 침해는 운영기관, 자산 및 개인에게 제한적인 영향을 미칠 수 있음	물리적 또는 논리적 분리
	분류기준	- 개인정보를 포함하지 않고 공개된 공공데이터를 포함 또는 운영하는 시스템	

- 클라우드컴퓨팅 서비스의 정보보호 수준에 따라 상·중·하 등급제로 나누고, 하등급은 논리적 분리를 허용
- **상등급은** 국가 중대 이익(안보, 국가안전, 국방, 통일, 외교 등), 수사·재판 등 민감정보를 포함하거나 행정 내부업무 등을 운영하는 시스템
- **중등급은** 비공개 업무자료를 포함 또는 운영하는 시스템
- **하등급은** 개인정보를 포함하지 않고 공개된 공공 데이터를 포함 또는 운영하는 시스템으로 분류

II. CSAP의 평가·인증 절차 및 인증기준

가. CSAP의 평가·인증 절차



- 최초평가를 기준으로 하였으며, 1년 단위로 실시하는 사후평가에서는 평가·인증신청 단계부터 수행

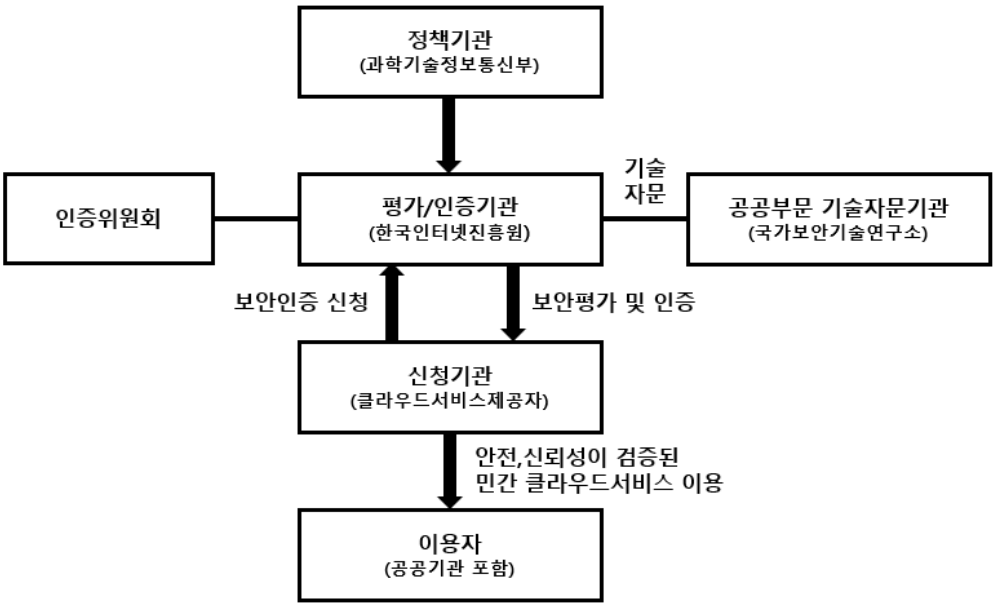
나. CSAP의 인증기준

통제분야	통제 항목	통제 항목 수			
		IaaS	SaaS(표준)	SaaS(간편)	DaaS
1. 정보보호 정책 및 조직	1.1. 정보보호 정책	3	3	-	3
	1.2. 정보보호 조직	2	2	2	2
2. 인적보안	2.1. 내부인력 보안	6	4	1	4
	2.2. 외부인력 보안	3	-	-	3
	2.3. 정보보호 교육	3	1	1	1
3. 자산관리	3.1. 자산 식별 및 분류	3	1	-	3
	3.2. 자산 변경관리	3	1	-	3
	3.3. 위험관리	4	1	-	4
4. 서비스 공급망 관리	4.1. 공급망 관리정책	2	2	-	2
	4.2. 공급망 변경관리	2	1	-	2
5. 침해사고 관리	5.1. 침해사고 절차 및 체계	3	3	1	3
	5.2. 침해사고 대응	2	2	1	2
	5.3. 사후관리	2	2	-	2
6. 서비스 연속성 관리	6.1. 장애대응	4	4	1	4
	6.2. 서비스 가용성	3	2	1	3
7. 준거성	7.1. 법 및 정책 준수	2	1	1	2
	7.2. 보안 감사	2	2	-	2
8. 물리적 보안	8.1. 물리적 보호구역	6	-	-	6
	8.2. 정보처리 시설 및 장비보호	6	-	-	6
9. 가상화 보안	9.1. 가상화 인프라	6	2	1	5
	9.2. 가상 환경	4	4	-	2
10. 접근통제	10.1. 접근통제 정책	2	2	1	2
	10.2. 접근권한 관리	3	3	-	3
	10.3. 사용자 식별 및 인증	5	5	4	5
11. 네트워크 보안		6	5	2	6
12. 데이터 보호 및 암호화	12.1. 데이터 보호	6	6	2	6
	12.2. 매체 보안	2	-	-	2
	12.3. 암호화	2	2	2	2
13. 시스템 개발 및 도입 보안	13.1. 시스템 분석 및 설계	5	5	1	5
	13.2. 구현 및 시험	4	4	1	4
	13.3. 외주 개발 보안	1	1	-	1
	13..4. 시스템 도입 보안	2	-	-	2
14. 공공부문 추가 보안요구 사항		8	7	7	8
총계		**117**	**78**	**30**	**110**

- IaaS 인증은 관리적·물리적·기술적 보호조치 및 공공기관용 추가 보호조치로 총 14개 분야 117개 통제항목으로 구성

- SaaS 표준등급 인증은 관리적·기술적 및 공공기관용 추가 보호조치로 총 13개 분야 78개 통제항목으로 구성
- SaaS 간편등급 인증은 관리적·기술적 및 공공기관용 추가 보호조치로 총 11개 분야 30개 통제항목으로 구성
- DaaS 인증은 관리적·물리적·기술적 및 공공기관용 추가 보호조치로 총 14개 분야 110개 통제항목으로 구성

III. CSAP의 보안 평가·인증 체계



구분	주관기관	주요역할
정책기관	과학기술정보통신부	- 평가·인증 관련 법·제도 개선 및 정책 수립 - 평가/인증기관의 지정 및 감독
평가/인증기관	한국인터넷진흥원	- 평가·인증 신청접수, 평가·인증기준, 지침 개발 - 평가를 통한 인증업무 수행 - 인증서 발급 및 인증된 클라우드서비스 관리
인증위원회	한국인터넷진흥원	- 평가결과를 통한 인증 심의·의결 - 인증취소의 타당성 심의 - 학계, 연구기관, 기술자문기관 등 클라우드 관련 전문가 5인 이상 10인 이내로 구성
기술자문기관	국가보안기술연구소	- 국가·공공기관 민간 클라우드서비스 이용 보안기준 마련 - 국가·공공 클라우드 안전성 강화 대책 수립
신청기관	클라우드서비스제공자	- IaaS, SaaS 등 클라우드서비스 제공 - 자체 보안활동 정기· 수시 수행

- 클라우드서비스 보안 평가·인증체계는 역할과 책임에 따라 정책기관, 평가/인증기관, 인증위원회, 기술자문기관, 신청기관, 이용자로 구분
- 정책기관은 과학기술정보통신부, 평가/인증기관은 한국인터넷진흥원, 기술자문기관은 국가보안기술연구소에서 각각 역할 수행

"끝"

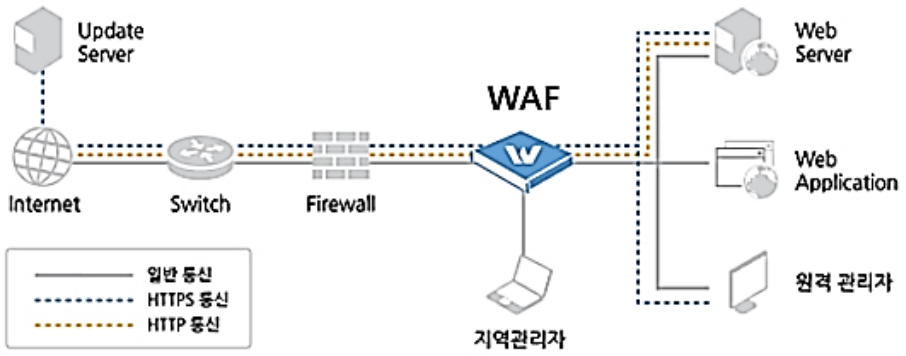
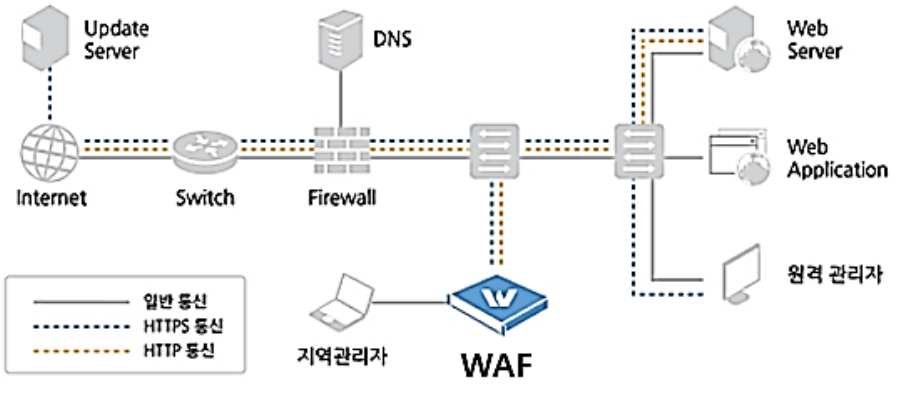
03	WAF(Web Application Firewall)		
문제	웹 애플리케이션 방화벽(WAF: Web Application Firewall)		
도메인	정보보안	난이도	중(상/중/하)
키워드	사용자 요청검사, 컨텐츠 보호, SSL/TLS 지원		
출제배경	웹 기반 서비스 증가로 웹 방화벽 기능에 대한 고전 토픽 출제		
참고문헌	ITPE 기술사회 자료		
해설자	강남평일야간반 전일 기술사(제 114회 정보관리기술사 / nikki6@hanmail.net)		

I. 웹 어플리케이션 특화 보안, 웹 방화벽 정의

- SQL Injection, XSS 와 같은 웹 공격 및 보안을 위협하거나 과도한 리소스 사용 공격을 탐지하고 차단하는 방화벽 기능
- **(공격유형)** 홈페이지 내용 위/변조, 거래 정보 변조, 중요 정보 유출, 악성 코드 유포, XSS, SQL Injection

II. 웹 방화벽 구성도 및 기능

가. 웹 방화벽 구성도

인라인 모드	
프록시 모드	

- XSS, SQL Injection 과 같은 웹 공격 패턴 인지, 특정 트래픽 차단 등을 통한 웹 어플리케이션 보안 효율적

나. 웹 방화벽 기능

분류	기능	설명
사용자 요청 검사	어플리케이션 접근 제어	- 서비스 사용 및 자원 접근 시, 사용자 권한 식별 기반 접근 제어
	Web Dos 제어	- 과도한 리소스 사용 차단
	업로드 파일/요청 형식 검사	- 바이러스 및 악성 파일 업로드 검사
	버퍼오버플로우/스크립트 차단	- XSS, SQL Injection 등의 웹 공격 차단
컨텐츠 보호	정보 유출 차단	- 신용카드, 주민등록번호 등 유출 차단
	웹 변조 방지	- 응답 형식 검사 및 코드 노출 차단 기반 변조 식별
보안	URL 및 서버 위장	- 사용자 제공 정보(URL/서버정보 등) 일부 변조
	SSL/TLS 지원	- HTTPS 웹 트래픽 암호화 기능 제공

- 접근제어, 사용자 요청 보안 기능 및 패턴 인식 통해 웹 공격 방지

III. 퍼블릭/프라이빗 클라우드 환경에서의 WAF 기능 제공

분류	기능	설명
퍼블릭 클라우드	AWS	- 사용자 등록 Rule 기반 WAF 서비스 기능 제공 - Default All-Deny, 사용자 규칙 기반 트래픽 허용
	Google Cloud	- 여러 보안 업체 솔루션(AlterLogic, CloudFlare, ETC)의 보안 솔루션 서비스 제공
	NCloud	- 보안 강화 인프라(Secure Zone)을 두어 중요 정보 보관 및 WAF 기능 제공
프라이빗 클라우드	어플라이언스 서버	- WAF 기능 포함 어플라이언스 서버 기반 증설
	WAF 솔루션 및 컨설팅	- CloudFlare, Akamai 등 WAF 솔루션 기반 구축

- 다양한 웹 공격에 대한 방어로 서비스 안전성 제고 및 AI 기반 다양한 웹 공격 패턴 인식

"끝"

04	스마트양식장(Smart Fish Farm)		
문제	스마트양식장(Smart Fish Farm)		
도메인	디지털서비스	난이도	중(상/중/하)
키워드	지능형 자동먹이공급장치, 어군탐지센서, 사육환경 제어장치, 수중 드론		
출제배경	해양 수산의 스마트화를 위한 최신기술 확인		
참고문헌	국내 스마트 양식 기술 동향(ETRI, 2021 한국전자통신연구원)		
해설자	강남평일야간반 전일 기술사(제 114회 정보관리기술사 / nikki6@hanmail.net)		

I. 고갈되고 있는 수산자원의 대안, 스마트양식장 개요

가. 스마트양식장(Smart Fish Farm)의 정의

- 양식수산물의 효율적·친환경적 생산을 위해 스마트 기술을 활용하여 양식산업 시스템을 자동화·지능화한 양식장

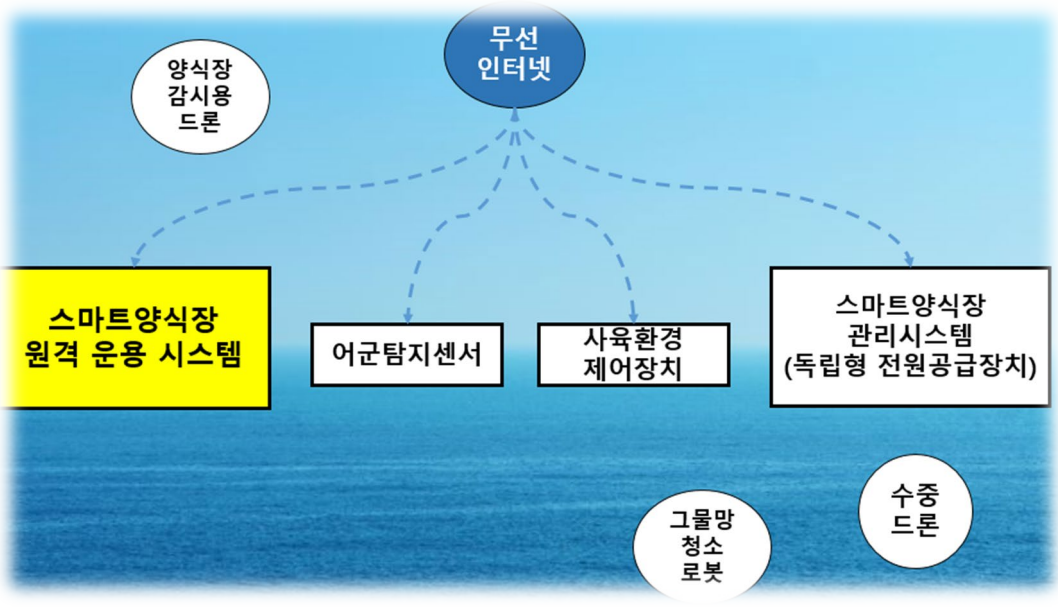
나. 기존 양식과 스마트 양식의 구분

구분	기존 양식		스마트 양식
	전통 양식	자동화 양식	
개념	인간판단→인간노동	인간판단→기계노동	기계판단→기계노동
생산관리	노동집약적 공정	서로 비(非)유기적 공정	각 공정 인공지능 연결
데이터관리	경험적 관리·운영	데이터의 개별적 수집	데이터간 연결·수집 분석

- 기술 개발 단계 기준으로 전통 양식을 1단계, 자동화 양식은 2·3단계, 스마트 양식은 4단계로 분류하기도 함

II. 스마트 양식장의 구성도와 구성요소

가. 스마트 양식장 구성도



나. 스마트 양식장 구성요소

구분	구성요소	세부 내용
통합관제	스마트양식장 원격 운영 시스템	- 무선 인터넷을 통해 어군 탐지 및 모니터링
DCS(Distributed Control System)	독립형 전원공급 장치	- 태양광 또는 풍력을 이용해 자체 전원 공급
	지능형 자동먹이 공급장치	- 사료의 자동 공급 및 시간대별 먹이 제공
	사육환경 제어장치	- 그물망 청소 및 수질 모니터링
센서	어군 탐지 센서	- 어군의 생육 과정 및 이동 상황에 따른 측정
	양식장 환경 측정 센서	- 수질, 환경오염, 해수온도, 탁도 측정
드론	양식장 감시용 드론	- 수중 외부의 침입 및 감시
	수중 드론	- 수중 내부의 부유물 및 폐사 제거

- 위 내용에서 제시되고 있는 스마트 양식장은 기술 개발 2단계(복합환경제어+자동제어)에 해당

III. 스마트양식장 기술 개발 단계

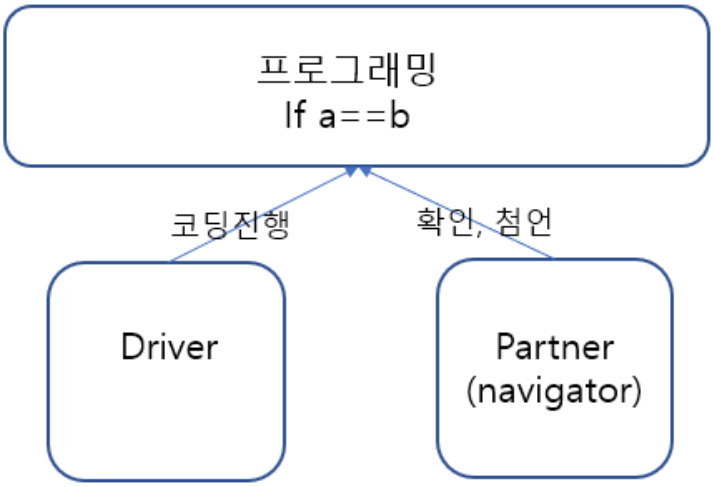
구분	1단계	2단계	3단계	4단계
개념	원격감시+원격제어	복합환경제어+자동제어	로봇자동화+자율제어	생산 자율관리+자율경영
	IoT기반 양식장 모니터링	데이터 기반 양식장 자동제어 시스템	AI 기반 양식장 자율제어 시스템	디지털트윈 기반 자율경영 시스템
	원격제어 기반	복합·자동제어 기반	지능화 기반	자율경영 기반
의사결정주체	인간	인간+컴퓨터	컴퓨터	컴퓨터
예시	무선 네트워크 기반 양식장 수조 감시 시스템(2016.12)	양식장 환경 자동	개체적응형 자동사료공급 (노르웨이 사료공급선)	양식생산 자율관리 및 경영지원시스템 (노르웨이 AM社)

- 향후 4단계에서 제시되고 있는 의사결정주체가 컴퓨터가 전적으로 진행할 수 있지만 주기적인 인간의 검토와 모니터링이 필요

"끝"

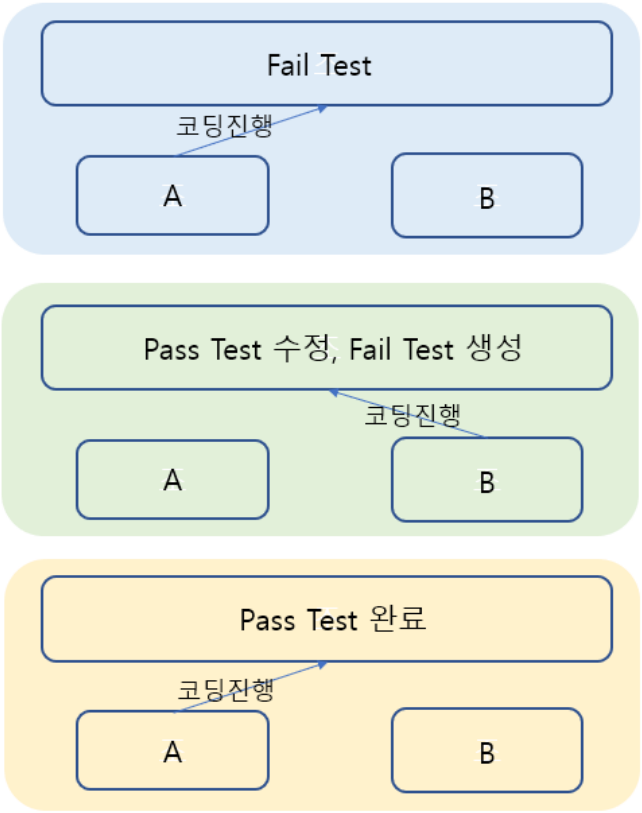
05	페어 프로그래밍, 핑퐁 프로그래밍		
문제	페어 프로그래밍(Pair Programming) 기법과 핑퐁 프로그래밍(Ping Pong Programming)기법에 대하여 각각 설명하시오		
도메인	소프웨어 공학	난이도	하(상/중/하)
키워드	Driver, Partner(navigator), Ping, Pong, Fail, Pass		
출제배경	TDD의 기본 개념 이해		
참고문헌	ITPE 기술사회 자료집 https://openpracticelibrary.com/practice/ping-pong-programming/		
해설자	정상 기술사(제 12X회 정보관리기술사 / jeongsang_pe@naver.com)		

I. 두 사람이 한 컴퓨터로 사용 프로그래밍, 페어 프로그래밍 기법 설명

구분	설명	
개념	- 두 사람이 한 컴퓨터를 사용해서 Pair work로 프로그래밍 하는 방법 - 애자일 개발 방법론 중의 하나로 하나의 컴퓨터에 두 사람의 프로그래머가 작업하는 방법	
개념도		
구성요소	Driver	- 실제 코딩 표준에 따라 코드를 작성하는 프로그래머
	Partner	- Driver에게 전략과의 일치 여부 등 모든 것을 상기시켜주는 역할을하는 프로그래머

- 한명은 직접 코딩을 하고 다른 한명은 옆에서 지켜보며 질문을 하고, 논의 하는 방식으로 진행, Driver와. Partner의 역할을 바꿔가며 수행하면 코드와 시스템에 대한 이해가 높아짐

II. 핑퐁 프로그래밍 기법 개요

구분	설명
개념	- 팀 내에서 지식 공유의 용도로 사용하기 위해 페어 프로그래밍과 TDD 방법의 결합한 프로그래밍 방법
개념도	
절차	1) Ping : A가 실패하는 새 테스트를 만들고, 키보드를 B에게 넘긴다
	2) B가 테스트를 통과하도록 코드를 작성한다.
	3) Pong : B가 실패하는 새 테스트를 만들고, 키보드를 A에게 넘긴다
	4) A가 테스트를 통과하도록 코드를 작성한다.

- 피드백 주기가 짧아 두 프로그래머가 지속적으로 집중할 수 있도록 하는 장점이 있음

"끝"

06	3-상태 버퍼		
문제	3-상태 버퍼(Tri-State Buffer)		
도메인	CA/OS	난이도	중(상/중/하)
키워드	High, Low, High-Impedance(Z:고저항 상태)		
출제배경	플립플롭, 3 상태 버퍼 등 기본 소자에 대해서는 동작에 대한 기본 이해가 필요		
참고문헌	ITPE 기술사회 자료집		
해설자	정상 기술사(제 12X회 정보관리기술사 / jeongsang_pe@naver.com)		

I. 3-상태 버퍼의 개요

가. 3-상태 버퍼의 개념

- Control 신호를 추가로 입력받아 Control 신호에 의해 3가지 출력 상태를 갖는 논리 소자

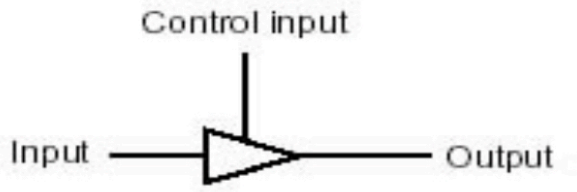
나. 3-상태 버퍼의 특징

3가지 출력	High, Low, High-Impedance(Z:고저항 상태)
방향성	입력 A 로부터 출력 Y 로 신호가 흐르는 반면 Y 에서 A 로는 흐르지 않음

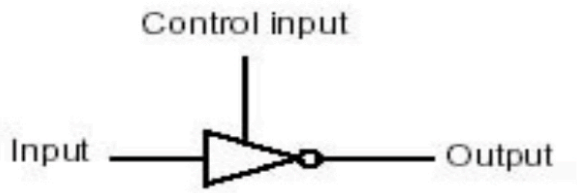
- 3-상태 버퍼를 2개 조합하여 양방향서의 신호를 제어하도록 만들 수 있음

II. 3-상태 버퍼의 동작 원리 및 설명

가. 3-상태 버퍼의 동작 원리 개념도



In	Control	Out
0	0	Hi Z
1	0	Hi Z
0	1	0
1	1	1



In	Control	Out
0	0	Hi Z
1	0	Hi Z
0	1	1
1	1	0

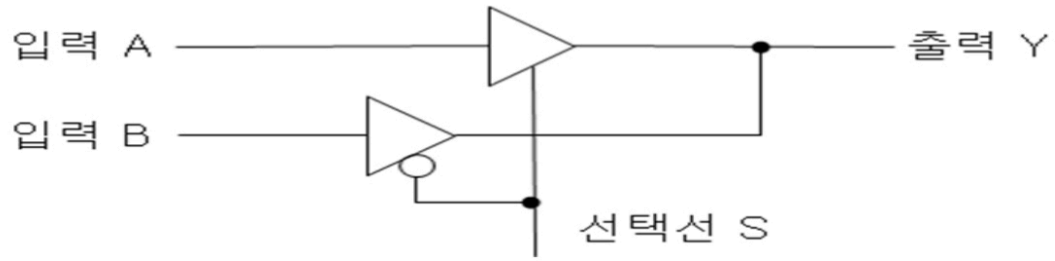
- 제어 입력의 1, 0의 경우에 따라 회로 동작이 차단, 증폭 됨

나. 3-상태 버퍼의 동작 상세 설명

구분	설명
제어입력(Control Input)	- 데이터 입력 단자 Input과 출력 단자 Output 사이 회로 개폐 역할
제어 입력이 1인 경우	- 상위 회로에서는 단순 증폭기 역할, 하위 회로에서는 Inverter 역할
제어 입력이 0인 경우	- 모두 고 임피던스(High Impedance) 상태로 입력 단자 차단된 상태

- 제어 입력의 동작에 따라 MUX 등 회로에 활용

III. 3-상태 버퍼의 활용



- 2가지 종류의 3-상태 버퍼와 선택선을 연결하여 2-to-1 MUX 회로구성
- 선택선(S)가 1인 경우에는 입력 A가 선택되고, 선택선(S)가 0 인 경우에는 입력 B가 선택됨

"끝"

07	소프트웨어 리팩토링(Refactoring)		
문제	소프트웨어 리팩토링(Refactoring)		
도메인	소프트웨어공학	난이도	하(상/중/하)
키워드	Extract, Replace, Move, Rename, Pull up, Encapsulation		
출제배경	시스템 내 소프트웨어 중요도 증가에 따라 소프트웨어의 효율적 관리를 위한 리팩토링 활용도가 증가 추세에 있어 관련 지식 점검을 위한 출제		
참고문헌	ITPE 기술사회 자료		
해설자	서경석 기술사(제119회 정보관리기술사 / akslemf@naver.com)		

I. 소프트웨어 코드의 정제를 통한 생산성 향상기법, 소프트웨어 리팩토링의 개요

가. 소프트웨어 리팩토링(Refactoring)의 정의

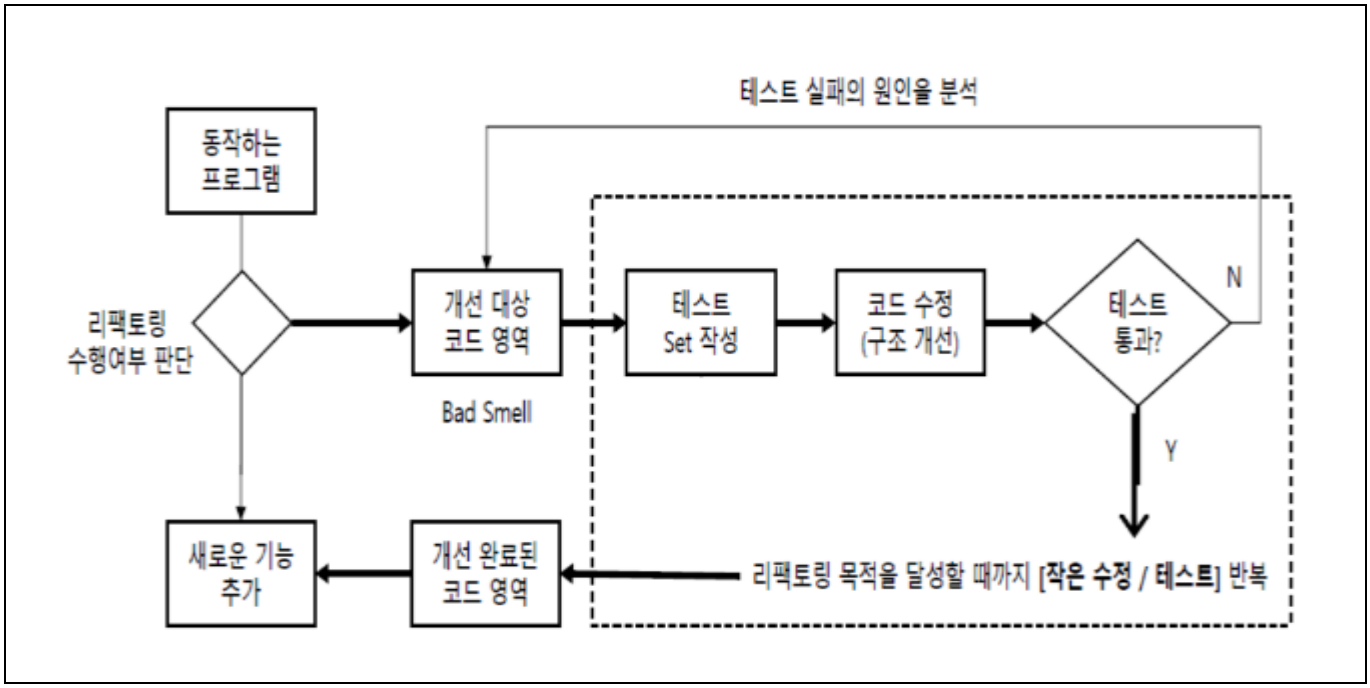
- 소프트웨어 모듈의 외부적 기능은 수정하지 않고 내부적인 구조, 관계등을 단순화하여 소프트웨어의 유지보수성을 향상시키는 기법

나. 소프트웨어 리팩토링의 목적

소프트웨어 디자인 개선	- 설계 의도와 구현 코드의 일관성을 유지하여 설계 변경 용이
소프트웨어 이해도 향상	- 이해하기 쉬운 코드는 개발자의 작업시간 단축
오류발견 용이성 확보	- 소스 구조를 명확히 함으로써 버그 원인 쉽게 발견
전체 개발 생산성 유지	- "좋은 디자인 유지 -> 개발자 이해 향상 -> 오류감소" 개발 가속화

II. 소프트웨어 리팩토링의 수행 절차와 기법

가. 소프트웨어 리팩토링의 수행 절차



나. 소프트웨어 리팩토링의 기법

기법	내용
Extract Method	- 그룹으로 함께 묶을 수 있는 코드 조각이 있으면, 코드의 목적이 잘 드러나도록 메소드의 이름을 지어 별도의 메소드를 추출
Replace Temp With Query	- 어떤 수식의 결과값을 저장하기 위해서 임시변수를 사용하고 있다면, 수식을 추출해서 메소드로 만들고, 임시변수를 참조하는 곳을 찾아 모두 메소드 호출로 교체
Move Method	- 메소드가 자신이 정의된 클래스보다 다른 클래스의 기능을 더 많이 사용하고 있다면, 이 메소드를 가장 많이 사용하고 잇는 클래스에 비슷한 몸체를 가진 새로운 메소드 생성
Extract Class	- 두 개의 클래스가 해야 할 일을 하나의 클래스가 하고 있는 경우 새로운 클래스를 만들어 관련 있는 필드와 메소드를 예전 클래스에서 새로운 클래스로 이동
Rename Method	- 메소드의 이름이 그 목적을 드러내지 못하고 있다면 메소드의 이름 변경
Pull Up Field	- 두 서브 클래스가 동일한 필드를 가지고 있다면, 해당 필드를 슈퍼 클래스로 이동
Pull Up Method	- 동일한 기능을 하는 메소드를 여러 서브클래스에서 가지고 있다면 이 슈퍼클래스로 이동
Encapsulation Field	- Public 필드가 있는 경우, 그 필드를 Private으로 하고 접근자 제공
Inline Temp	- 간단한 수식의 결과값을 가지는 임시변수가 있고, 그 임시변수가 다른 리팩토링을 하는데 방해가 된다면, 이 임시변수를 참조하는 부분을 모두 원래의 수식으로 변경
Introduce Explaing Variable	- 복잡한 수식이 있는 경우에는, 수식의 결과나 또는 수식의 일부에 자신의 목적을 잘 설명하는 이름으로 된 임시변수를 사용
Split Temporary Variable	- 루프안에 있는 변수나 collecting temporary variable도 아닌 임시변수에 값을 여러 번 대입하는 경우에는, 각각의 대입에 대해서 따로따로 임시변수를 작성
Remove Assignments to Parameters	- 파라미터에 값을 대입하는 코드가 있으면, 대신 임시변수를 사용하도록 하라
Substitute Algorithm	- 알고리즘을 보다 명확한 것으로 바꾸고 싶을 때는 메소드의 몸체를 새로운 알고리즘으로 변경
Replace Magic Number with Symbolic Constant	- 특별한 의미를 가지는 숫자 리터럴이 있으면, 상수를 만들고, 의미를 잘 나타내도록 이름을 지은 다음, 숫자를 상수로 변경
Decompose Conditional	- 복잡한 조건문(if-then-else)이 있는 경우, 조건, then 부분, 그리고 else부분에서 메소드를 추출
Consolidate Duplicate Conditional Fragments	- 동일한 코드 조각이 조건문의 모든 분기 안에 있는 경우, 동일한 코드를 조건문 밖으로 이동
Remove Control Flag	- 일련의 boolean식에서 컨트롤 플래그 역할을 하는 변수가 있는 경우, break 또는 return을 대신 사용

Replace Nested Conditional with Guard Clauses	- 메소드가 정상적인 실행경로를 불명확하게 하는 조건 동작을 가지고 있는 경우, 모든 특별한 경우에 대해서 보호절(guard clause)을 사용
Add Parameter	- 어떤 메소드가 그 메소드를 호출하는 부분으로부터 더 많은 정보를 필요로 한다면, 이 정보를 넘길 수 있는 파라미터를 추가
Remove Parameter	- 파라미터가 메소드 몸체에서 더 이상 사용되지 않는다면, 그 파라미터를 제거하라
Parameterize Method	- 몇몇 메소드가 메소드 몸체에 다른 값을 포함하고 있는 것을 제외하고는 비슷한 일을 하고 있다면, 다른 값을 파라미터로 넘겨 받는 하나의 메소드를 작성
Replace Parameter with Explicit Methods	- 파라미터의 값에 따라서 다른 코드를 실행하는 메소드가 있다면, 각각의 파라미터 값에 대한 별도의 메소드를 작성

III. 리팩토링의 적용을 위한 필요 기술 및 적용시점

가.리팩토링의 적용을 위한 필요 기술

항목	내용
나쁜 코드 식별	- 개발 경험 기반 문제가 될 수 있는 코드를 식별해 내는 능력
좋은 코드 식별	- 리팩토링의 방향성 수립 및 리팩토링 정상 적용 여부 확인
테스트	- 테스트 프레임워크 선택, 단위 테스트 구축 후 자동화 및 TDD 적용 고려
시간 확보	- 리팩토링을 할 수 있는 시간을 확보, 작은 규모의 리팩토링 수행

나. 리팩토링 적용시점

시점	적용 사유
삼진 규칙	- 비슷한 중복이 세번째 나타나는 경우 수행 -> 기본가이드제공
기능 추가 시	- 기존 코드의 구조를 개선으로 이해 향상 -> 기능추 가를 쉽고 빠르게 수행
버그 수정 시	- 버그 수정 전에 더 깊은 이해를 제공 -> 버그수정용이
코드 리뷰 중	- 코드의 명확성 유지,더 나은 설계 아이디어가 제안 -> 품질향상

"끝"

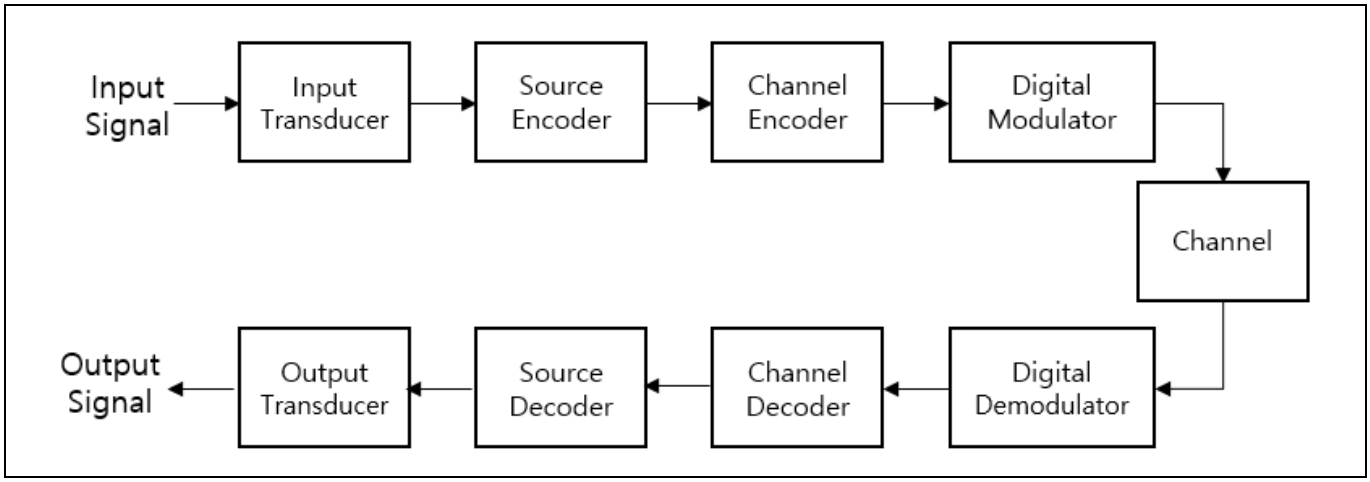
08	소스 코딩/채널 코딩		
문제	전송 부호화 기법의 소스 코딩(Source Coding)과 채널 코딩(Channel Coding)을 비교하여 설명하시오.		
도메인	네트워크	난이도	하(상/중/하)
키워드	데이터 중복 제거, 오류 검출 및 정정, 부호화, 검출/정정 코드		
출제 배경	아날로그 데이터 송수신 기본 프로세스인 소스 코딩과 채널 코딩에 대한 지식 점검을 위한 출제		
참고문헌	ITPE 기술사회 자료		
해설자	서경석 기술사(제119회 정보관리기술사 / akslemf@naver.com)		

I. 아날로그 데이터 전송 방식, 소스 코딩과 채널 코딩의 개념 비교

소스 코딩(Source Coding)	채널 코딩(Channel Coding)
통신 시스템 상에서 효율적 정보 전송을 위해 전송하려는 원천 데이터에서 불필요한 정보 및 중복 정보를 제거하여 전송 데이터를 줄이는 과정 및 기법	디지털 전송 채널 상의 잡음, 간섭 등에 의해 발생되는 오류를 검출 및 정정하기 위해 송수 양측에 의해 합의된 잉여 비트를 추가하고 복원하는 과정

II. 소스 코딩과 채널 코딩의 프로세스 및 상세 비교

가. 소스 코딩과 채널 코딩의 프로세스



- 소스 코딩을 통한 중복 제거 후 채널 코딩을 통해 데이터 전송 효율성 증가

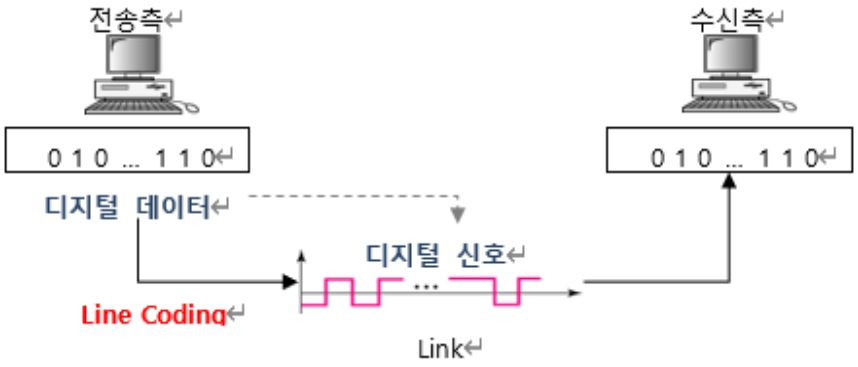
나. 소스 코딩과 채널 코딩의 상세 비교

구분	소스 코딩		채널 코딩	
목적	- 원 정보 신호를 디지털 신호로 변경 및 데이터 압축을 통해 제한된 통신 시스템의 대역폭에서 고속으로 전송		- 전송 단계에서 발생 가능한 오류 최소화	
기능	- 압축 부호화		- 에러 검출(패리티 검사 등), 에러 정정	
기법	영상 부호화	- 영상 정보를 부호화하는 기법 (JPEG, MPEG)	오류 검출 코드	- 전송 중에 발생한 오류만 검출 가능 (패리티 검사, 검사합, CRC)
	오디오 부호화	- 파원 부호화, 음성 파형 부호화(PCM, DM) 등	오류 정정 코드	- 오류 검출과 정정까지 가능 (FEC, Forward Error Correction)
	고정 길이 부호화	- 심볼 모두에 동일한 코드 길이를 부여한 부호 방식 (FLC(Fixed Length Coding), ASCII 코드)	파형 코딩	- 오류의 영향이 덜 받는 파형으로 변환 (직교 신호, 대척 신호)
	가변 길이 부호화	- 사용 빈도에 다른 코드 길이 가변 부호화 (모스 부호)	구조화 코딩	- 오류 탐지 및 정정에 필요한 여분의 비트 첨가 (Block Coding, Non Block Coding)
	무손실 압축 부호화	- 압축 데이터 복원 시 압축 전의 데이터와 일치 (허프만코딩, 런렝스 코딩)	블록 코드	- 오류 탐지 및 정정에 필요한 여분의 비트 첨가 (Block Coding, Non Block Coding)
	손실 압축 부호화	- 압축한 데이터 복원 시 압축 전의 데이터와 불일치(JPEG, MPEG)	비블록 코드	- 부호화기 메모리 존재, 코드화 시 과거 신호화 함께 활용 (Convolutional Code, Turbo Code)

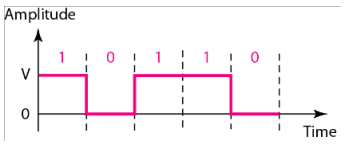
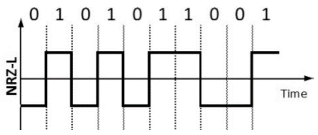
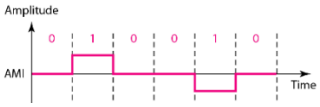
- 소스 코딩과 채널 코딩 후 라인 코딩을 통해 데이터 전송 진행

III. 디지털 신호 변환, 라인 코딩

가. 라인 코딩의 개념

구분	설명
정의	- 수신 측의 원활한 동기 재생과 오류 검출을 위해 2진 bit의 디지털 데이터를 신호 전달을 위한 의미 있는 디지털 신호(기저 대역 신호, 전기적 신호)로 변환하는 과정
목적	- 전송 제약의 극복 및 수신 측 동기 재생의 용이
특징	- 높은 대역 효율, 높은 전력 효율, 비트 동기 정보 포함, Zero DC component, Error Detection Capability
개념도	

나. 라인 코딩의 유형

구분	Unipolar	Polar	Bipolar
펄스 파형 (Pulse wave)			
극성	단극성	극성	양극성
Mark 정의 예	+ V	+ V	+ V와 - V 교대
Space 정의 예	0V	- V	0V
유형	NRZ	NRZ, RZ, 맨체스터 부호화	AMI
활용	일반적 부호	BPSK의 입력	AMI, T의 Encoding

"끝"

09	HBM		
문제	HBM(High Bandwidth Memory)		
도메인	CA/OS	난이도	상(상/중/하)
키워드	초절전, 초슬림, 초고속		
출제배경	차세대 초고성능 컴퓨팅 메모리 지원 지식 확인		
참고문헌	amd.com		
해설자	이상용 기술사(제 124회 정보관리기술사 / orangeday77@gmail.com)		

I. 차세대 초대역폭 메모리, HBM(High Bandwidth Memory)의 개요

가. HBM(High Bandwidth Memory)의 정의

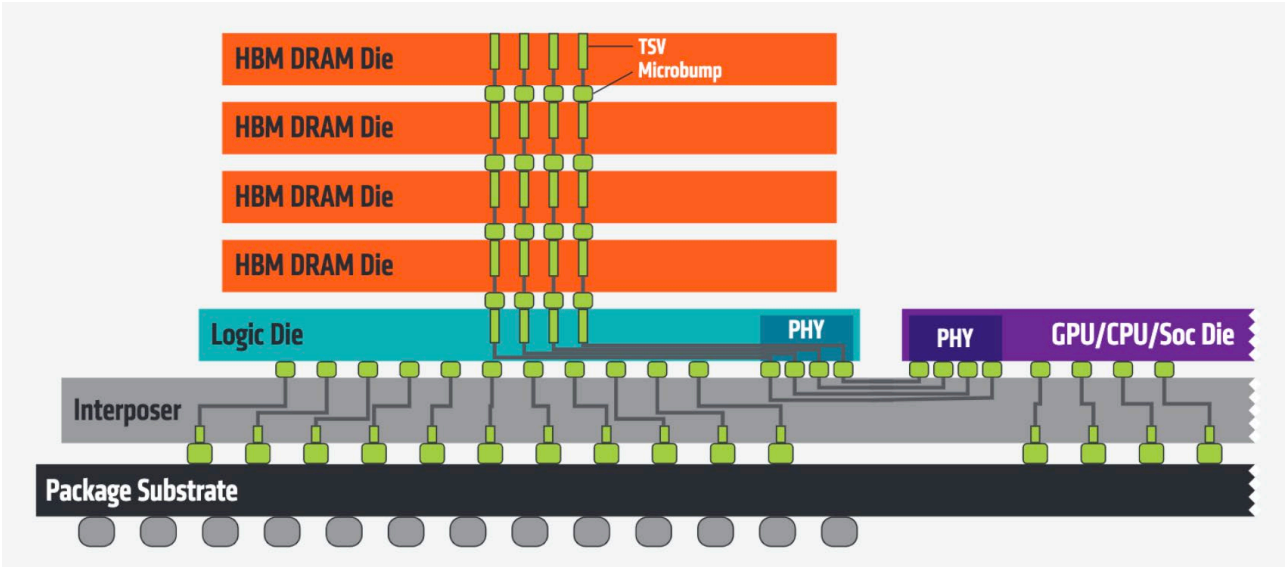
- 3D TSV기술을 적용해 D램 칩에 수천개의 홀을 뚫고 상하를 연결함으로써 데이터 처리속도를 혁신적으로 끌어올린 메모리 프로덕트

나. HBM(High Bandwidth Memory)의 등장 배경

GDDR의 한계	- GDDR 계열 SGRAM의 긴 레이턴시와 낮은 대역폭 D램의 한계
마이크로 한계	- GDDR 계열의 차지하는 공간의 한계
전력소비량/발열 문제	- 전력 소비량 문제와 발열 문제 존재

II. HBM(High Bandwidth Memory)의 아치텍처와 기술요소와 특징

가. HBM(High Bandwidth Memory)의 아키텍처



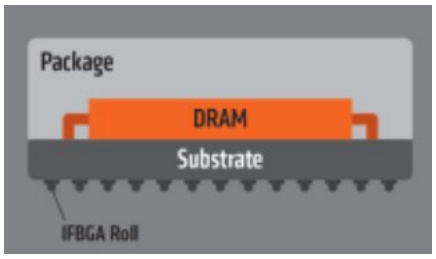
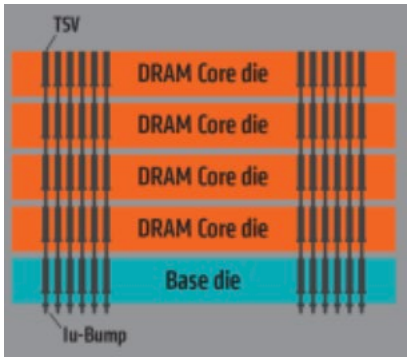
- HBM은 미국 칩 제조 업체 AMD와 한국의 메모리 칩 공급업체 SK 하이닉스가 함께 개발함

나. HBM(High Bandwidth Memory)의 기술과 특징

구분	내용	상세 설명
기술	- 실리콘관통전극 (TSV, Through Silicon Via)	- 메모리 다이를 적층하여 실리콘을 관통하는 통로를 만들어 주는 기술 - 최대 8개의 DRAM 다이를 적층 함
	- 인터페이스	- HBM(High Bandwidth Memory)2 - HBM(High Bandwidth Memory)3 - HBM(High Bandwidth Memory)4
	- DRAM	- DRAM(Dynamic Random Access Memory)은 커패시터에 데이터를 저장
특징	- 초절전	- 초당 256기가바이트의 데이터 전송하여 와트당 데이터 전송량 2배 높여 전력 소모 크게 줄어듦
	- 초슬림	- TSV 기술을 적용한 적층 형태의 초슬림
	- 초고속	- 적층칩을 수직연결하기 위해 수 천개 TSV Hole 연결

- 현장에서는 HBM은 HPC 작업용으로 설계된 ARM 기반프로세서와 함께 쓰이고 있음

III. HBM와 GDDR5의 비교

구분	HBM	GDDR5
개념도		
구현난이도	- 복잡	- HBM보다 유리
Bus Width	- 1024-bit	- 32-bit
Clock Speed	- Up to 500MHz(1GBps)	- Up to 1750MHz(7GBps)
Bandwidth	- > 100GB/s per stack	- Up to 28GB/s per chip
Voltage	- 1.3V	- 1.5V

- 현재 SK하이닉스는 19년과 21년 각각 HBM2E와 HBM3를 잇달아 선보인 데 이어, 엔비디아에 HBM3 출하를 공개하는 등 지난 몇 년간 성공적으로 HBM 출시 속도를 높이고 있음

"끝"

10	CAN		
문제	자동차 통신 등에 활용하는 CAN(Controller Area Network)		
도메인	네트워크	난이도	중(상/중/하)
키워드	ISO 11898, 저비용 경량 네트워크, 브로드캐스트 통신		
출제배경	차량 내부통신 기본지식 확인		
참고문헌	Introduction to the Controller Area Network (CAN) Steve Corrigan		
해설자	이상용 기술사(제 124회 정보관리기술사 / orangeday77@gmail.com)		

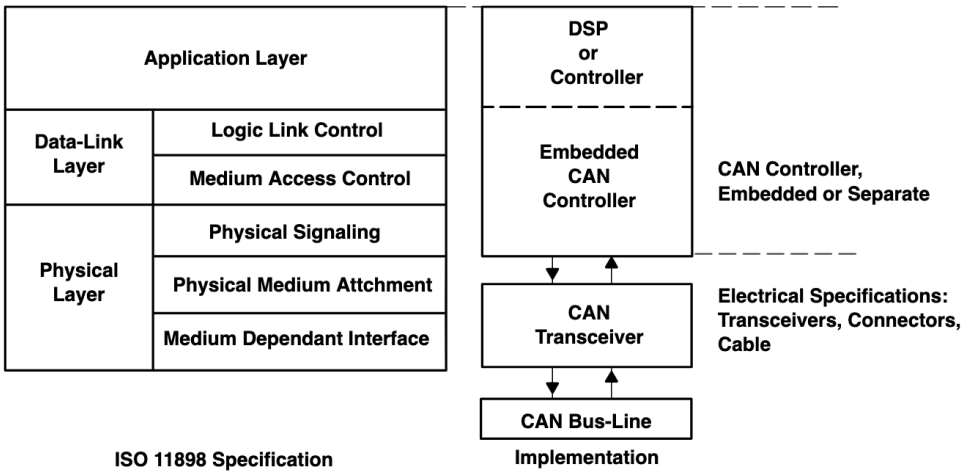
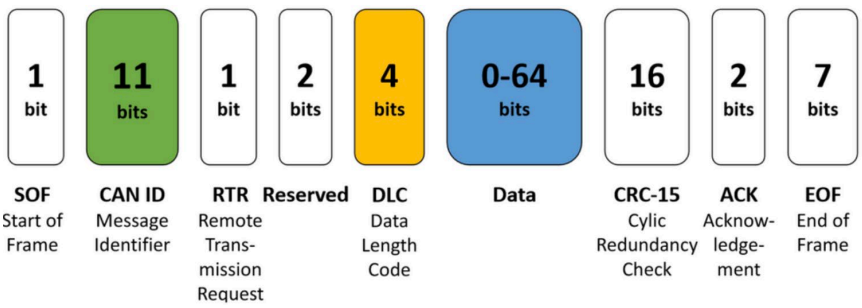
I. ISO 11898, CAN(Controller Area Network)의 개요

가. CAN(Controller Area Network)의 정의

- ISO 11898 표준 기반하여 컨트롤러 영역 네트워크(CAN) 버스는 지능형 디바이스를 네트워크로 연결하는 고정밀 시리얼 버스 시스템
- (역사) CAN은 Bosch가 1985년에 차량 내 네트워크를 위해 개발함

II. CAN(Controller Area Network)의 아키텍처와 기술요소

가. CAN(Controller Area Network)의 아키텍처

구분	개념도
아키텍처	 **Figure 1. The Layered ISO 11898 Standard Architecture**
프레임	

나. CAN(Controller Area Network)의 기술요소

구분	핵심 기술 요소	상세 설명
통신 방식	- Multi Master	- CAN 버스는 통신 버스를 여러 노드들이 공유
배선 구조	- CAN_High - CAN_Low	- 두 개의 신호로 통신하므로 단 2개의 선 필요 - 많은 모듈이 추가되어도 배선의 양이 적음
잡음 내성	- Twist Pair	- Twist Pair 2선으로 되어 있어 전기적 잡음이 강하여 메시지 보호
매커니즘	- Unique ID	- 자동차의 ECU들은 고유 ID값을 가짐 - ID 값이 낮을 수록 우선순위 높음 - ID 값 수신해 우선순위 결정
속도와 거리	- 최대 1Mbps - 최대 1,000m	- 고속 통신 제공 - 원거리 통신 가능
확장성	- Plug & Play	- CAN 제어기를 버스에 간편하게 연결 및 해제
에러 제어	- Error Active State - Error Passive State - Bus-off State	- 하드웨어 오류 보정

- 에러 카운터가 특정 임계를 넘어설 때마다 노드는 스스로를 네트워크로부터 3개의 state로 분리

III. CAN 통신의 보안 약점 및 대응 방안

취약점	설명
Broadcast	- CAN 네트워크 상에 패킷을 전체 수신자로 전송
No Encryption	- 패킷 암호화 하지 않고 원본 데이터 전송
No Authentication	- 인증이 안된 장치의 데이터 위조 가능
Weak Access Control	- CAN버스에 직접 접근이 가능하여 위조된 메시지를 전송하거나 재전송 가능

- (방안) 침입탐지시스템(IDS), HMAC 데이터 프레임 인증

"끝"

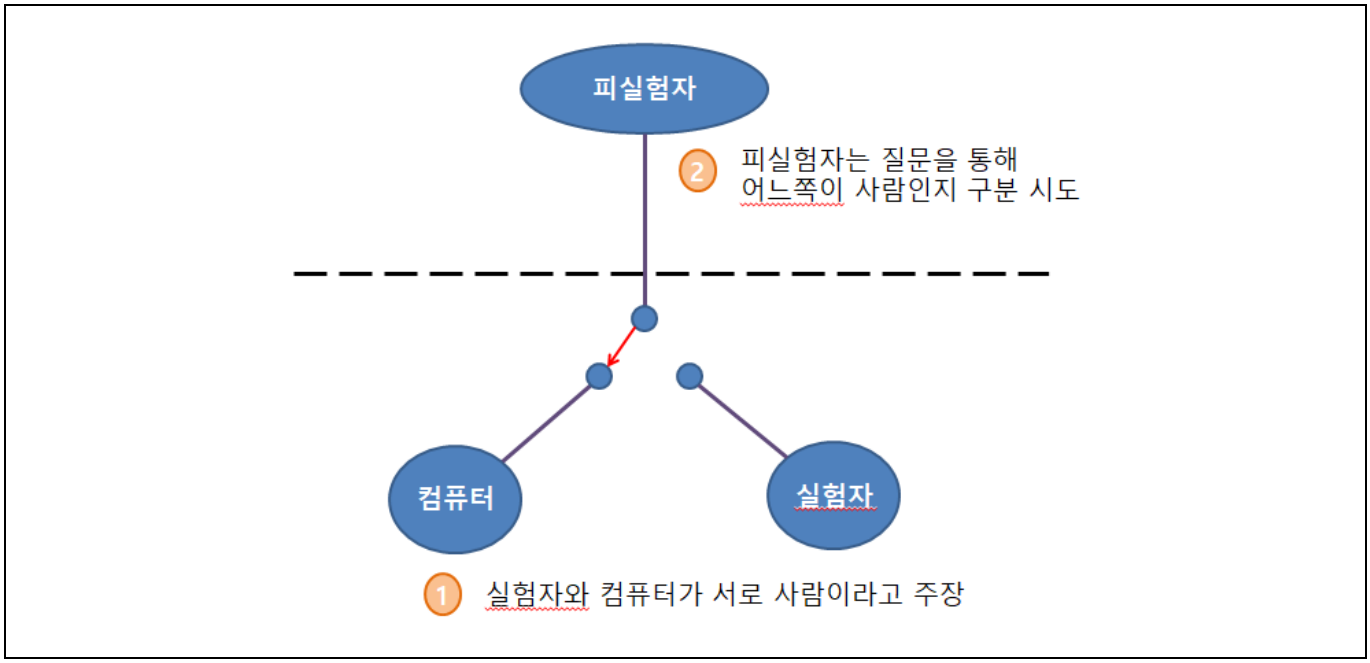
11	튜링 테스트		
문제	튜링 테스트 (Turing Test)		
도메인	인공지능	난이도	하(상/중/하)
키워드	지능적 행위, 추론, 패턴인식, 기계학습, 인공지능, 기계의 출력과 사람의 출력 구별		
출제배경	인공지능에 대한 이해, 튜링 테스트가 적용되는 방식에 대한 학습		
참고문헌	ITPE 기술사 자료		
해설자	장건환 기술사(제 126회 정보관리기술사 / jkh556@naver.com)		

I. 인간과 구분할 수 없는 기계능력 테스트, 튜링 테스트의 개념

- 주어진 문제 해결적 사고 상황에서 판단자가 기계의 출력과 사람의 출력을 구별할 수 없다면, 그 기계는 인간과 같은 사고를 하였다고 규정할 수 있다는 테스트
- 인공지능의 선구자인 앨런 튜링이 제안한 기계가 인간과 얼마나 비슷하게 대화할 수 있는지를 기준으로 기계의 사고 능력을 판별하는 테스트

II. 튜링 테스트의 절차도 및 절차

가. 튜링 테스트의 절차도



- 피실험자는 격리상태에서 누가 진짜 사람인지 판별하고 구분할 수 없는 경우 인간수준의 사고능력을 인정

나. 튜링 테스트의 절차

단계	핵심 기술	설명
1	테스트 환경 구성	- 차단된 2개의 방에서 한쪽 방에 실험자와 인공지능 컴퓨터를 두고 다른 방에는 피실험자를 위치
2	테스트 수행	- 피실험자의 질문에 실험자와 컴퓨터는 화면을 통해 대화를 수행
3	테스트 평가	- 피실험자는 누가 사람인지 판별을 하고 구분할 수 없다면 인공지능이 인간수준의 사고능력을 가진 것으로 평가

III. 튜링 테스트 방식의 활용 사례

구분	활용 사례	설명
이미지 인식분야	CAPTCHA	- 접근 사용자가 컴퓨터 프로그램인지 실제 사람인지 구별하기 위해 사용하는 방법 - 종류 : 텍스트 이미지 CAPTCHA, 오디오 CAPTCHA
	구텐베르크 프로젝트	- 인류 자산인 문학작품들을 전자화 및 배포하는 프로젝트, - 전자화 과정 중에 컴퓨터 인식이 어려운 부분을 CAPTCHA 형식으로 접속 사용자에게 인식하도록 활용
의료분야	엘리자(Eliza)	- 1966년 조셉 와이젠바움이 만든 인공지능 소프트웨어 - Doctor 모드에서 질문자의 진술을 키워드로 관련 질문을 만들어 심리 상담 프로그램 활용
	패리(Parry)	- 1972년 정신의학자 케네스 콜비가 만든 정신분열증 환자를 모사한 프로그램 - 실제 엘리자와 서로 대화 나는 기록

- 21세기에는 TV, Youtube 동영상 등을 보고 질문에 대답할 수 있는 정도의 인공지능 테스트 수준을 주장

"끝"

12	Write Through, Write Back		
문제	Cache Memory의 쓰기 정책인 Write Through 방식과 Write Back 방식을 비교하여 설명하시오.		
도메인	CA	난이도	중(상/중/하)
키워드	병렬컴퓨팅, 캐시-주기억장치간 내용 일관성, 일관성 유지의 용이성 및 비용, 성능		
출제배경	병렬컴퓨팅과 병렬컴퓨팅에서 캐시일관성 문제는 매우 중요하므로 재 출제 가능성 있음		
참고문헌	병렬 컴퓨터 구조론, ITPE 기술사회 자료		
해설자	장건환 기술사(제 126회 정보관리기술사 / jkh556@naver.com)		

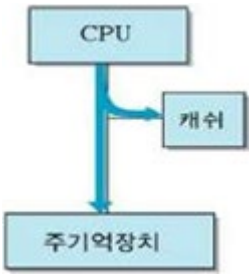
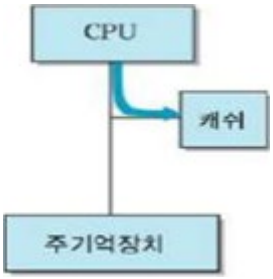
I. Cache Memory의 Write Through방식과 Write Back의 개념 비교

Write Through	Write Back
- 쓰기 동작 시 캐시메모리와 주기억장치에 데이터를 동시에 쓰는 방식	- 쓰기 동작 시 캐시메모리에만 쓰고 해당 데이터가 Swap-out 될 때 주기억장치에 복사하는 방식

- CPU의 Cache Memory의 일관성 문제를 해결하기 위한 방법

II. Write Through와 Write Back 상세비교

가. Write Through와 Write Back 동작 비교

구분	Write Through	Write Back
구성도		
동작원리	- 캐시와 주기억장치에 동시에 쓰기 수행	- 캐시에만 쓰기 수행 (추후 주기억장치에 복사)

- 일관성 유지와 성능간의 Trade-Off 관계가 있음

나. Write Through와 Write Back의 상세 비교

구분	Write Through	Write Back
일관성 유지방법	- VI Protocol (Valid-Invalid)	- MESI Protocol
장점	- 구조가 단순함 - 캐시와 주기억장치 간 일관성 유지	- 기억장치 쓰기 횟수 최소화 - 쓰기 시간 단축
단점	- 버스 트래픽 증가 - 쓰기 시간 증가	- 캐시 일관성 문제 발생 가능 - 일관성 위해 별도 확인 절차 구현 필요

- 성능, 일관성 모두 보장할 수 있는 최적의 방안 필요

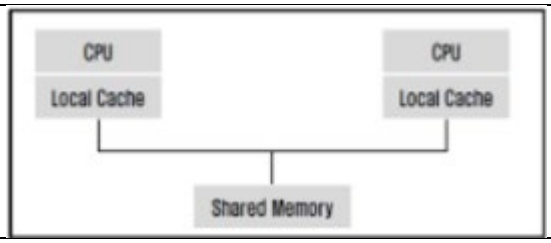
III. Write Through와 Write Back 정책의 캐시 일관성 유지 기법 설명

구분	캐시 일관성 유지 기법		설명
Write Through	VI Protocol	유효(V: Valid) 상태	- 캐쉬 내용 = 주기억장치 내용
		무효(I: Invalid) 상태	- 캐쉬 내용 =/ 주기억장치 내용
Write Back	MESI Protocol	수정(M: Modified) 상태	- 데이터가 수정(변경)된 상태
		배타(E: Exclusive) 상태	- 유일한 복사본, 주기억장치의 내용과 동일한 상태
		공유(S: Shared) 상태	- 데이터가 두 개 이상 프로세서 캐쉬에 적재 상태
		무효(I: Invalid) 상태	- 데이터가 다른 프로세서 의해 수정, 무효된 상태

- Cache coherence 유지를 위한 S/W(공유캐시 사용/미사용), H/W(디렉토리기반/버스감시 매커니즘) 적 기법 존재

"끝"

[참고] 다중 캐시메모리에 대한 쓰기정책 및 해결방안

	- 공유 캐시 사용 - 공유 데이터 캐시 저장 금지 - 잠금 변수 캐시 저장 금지 - 버스 감시 매커니즘 - 디렉터리 기반 캐시 프로토콜

13	상용 소프트웨어 직접구매 제도		
문제	상용 소프트웨어 직접구매 제도		
도메인	소프트웨어공학	난이도	중(상/중/하)
키워드	소프트웨어 진흥법, 소프트웨어사업 계약 및 관리감독에 관한 지침, 3억 이상, 조달 종합쇼핑몰, 5천만원 이상, 제외조건		
출제배경	(구) 분리발주에서 상용SW 직접구매 제도로 명칭 변경 및 직접구매 제도 학습여부 확인		
참고문헌	상용 소프트웨어 직접구매 가이드		
해설자	장건환 기술사(제 126회 정보관리기술사 / jkh556@naver.com)		

I. 상용SW 직접구매 제도 개념 및 법적근거

가. 상용SW 직접구매 제도 개념

- 발주기관이 공공 정보화사업 추진 시 HW, SW, 시스템 통합 구축사업에서 상용SW만을 별도로 발주, 평가, 선정 계약하는 방식으로 상용SW를 직접 구매하는 제도

나. 상용SW 직접구매 제도 법적 근거

구분	근거법령	조항	설명
구매 및 대상	SW진흥법	제54조	- 국가기관 등의 상용SW 구매
	SW사업 계약 및 관리감독에 관한 지침	제7조	- 상용SW 직접구매 대상
예외 대상		제8조	- 상용SW 직접구매 제외
	조달청 내자 구매업무 처리규정	제6조의 2	- SW 분리발주 제외사유 사전검토 요청

- SW 진흥법을 통해 상용SW 구매에 관한 근거를 제시하고 SW사업 계약관리 및 관리감독에 관한 지침을 통해 세부 대상을 정의

II. 상용SW 직접구매 대상사업 조건 및 제외 기준

가. 상용SW 직접구매 대상사업 조건

1차 조건	2차 조건	근거
총 사업규모 3억원이상 사업 (VAT 포함)	- 조달청 종합쇼핑몰에 등록된 SW를 포함한 경우	SW계약 및 관리감독에 관한 지침 제7조
	- 5천만원 이상 또는 동일 SW 다량 구매로 5천만원을 초과하는 경우에는 5천만원 이상인 SW로 간주 - SW 품질인증(GS), CC, NEP, NET 및 국가정보원 검증/지정 SW가 포함된 경우	

- 1차 조건 충족 시 2차 조건 중 어느 하나라도 해당하는 경우 상용SW 직접구매 대상사업
- 위 조건에 해당하지 않아도 국가기관 장의 판단에 따라 SW를 직접구매 가능

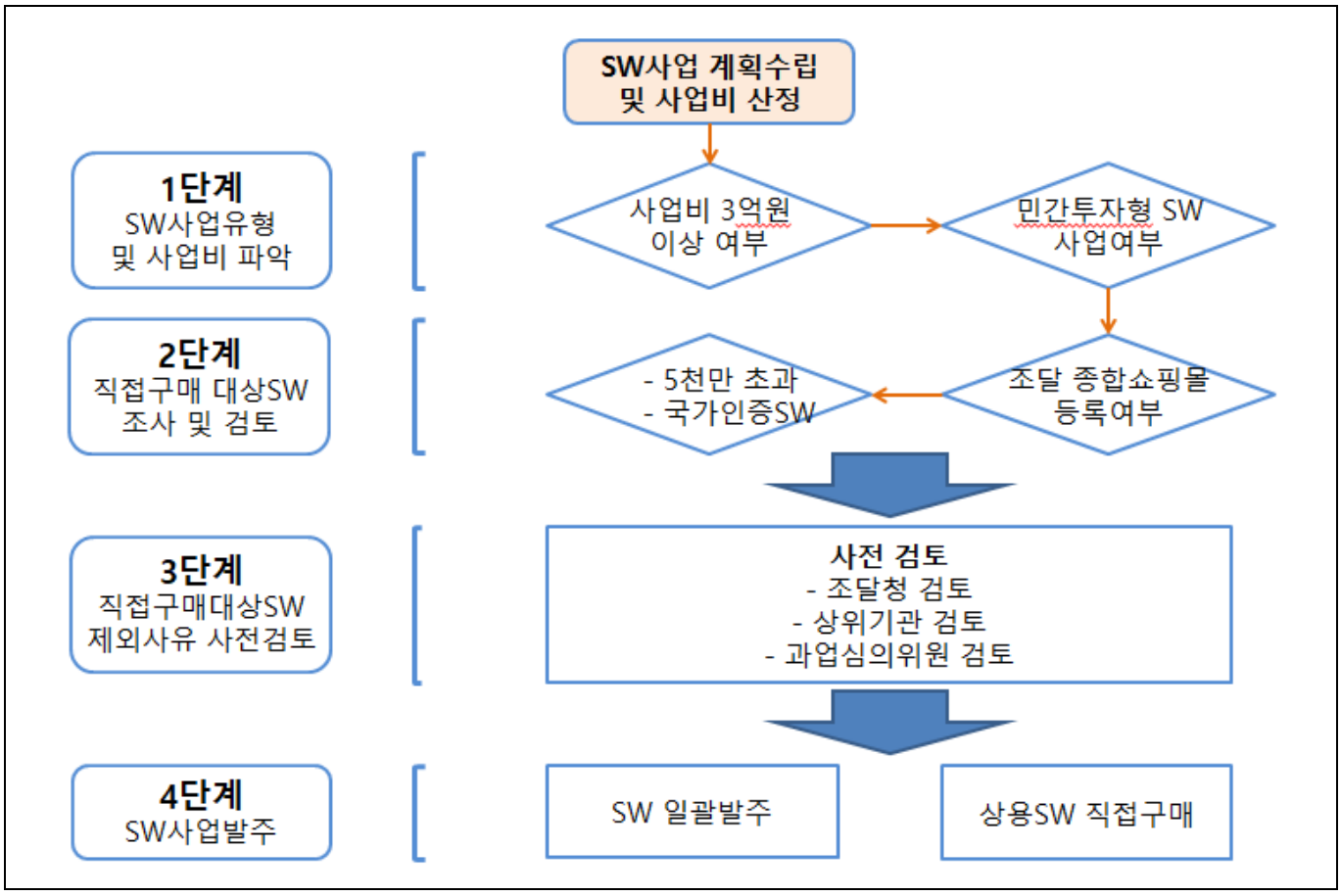
나. 상용SW 직접구매 제외기준

구분	예외 기준	세부 설명
대상 사업	민간투자형 SW사업	- 'SW진흥법' 제40조에 따른 민간투자형 SW사업에 해당하는 경우
대상 SW	현저한 비용상승 초래	- 직접 공급할 경우 비용이 현저하게 상승할 것으로 예상되는 경우
	정보시스템 통합 불가	- 기존 구축된 정보시스템과 연계 및 연동이 불가능할 경우
	현저한 사업기간 지연	- SW제품을 직접 공급하게 되면 해당 사업이 사업기간 내에 완성될 수 없을 정도로 현저하게 지연 될 우려가 있는 경우
	현저하게 비효율적이라고 판단되는 경우	- 상용SW 직접구매로 인한 행정업무 증가 외에 SW제품을 직접구매하여 공급하는 것이 현저하게 비효율적이라고 판단되는 경우

- 대상SW를 제외하고자 하는 경우 제외사유에 대하여 SW사업 계약 및 관리감독에 관한 지침 제8조2항에 따라 사전검토를 요청하여야 하며, 제외사유를 발주계획서 및 입찰공고문에 명시해야 함

III. 상용SW 직접구매 업무 프로세스

가. 상용SW 직접구매 업무 프로세스 절차도



- 상용SW 직접구매는 총4단계로 구성되며, 각 단계별 검토항목을 검토 후 마지막 단계에서 일괄발주 혹은 직접구매 방식을 선택

나. 상용SW 직접구매 업무 프로세스 상세

단계	처리 프로세스	설명
1단계 SW 사업유형 및 사업비 파악	사업비 3억원 이상	- SW사업 총사업규모(HW·SW 도입가격, 응용SW개발 비용 등) 산정 후 상용SW 직접구매 대상 사업 기준 확인
	민간투자형SW 사업	- 소프트웨어진흥법 40조에 해당하는지 기준 확인
2단계 직접구매대상SW 조사 및 검토	조달청 종합쇼핑몰 등록	- 도입 대상 SW품목이 조달청 종합쇼핑몰에 등록된 품목인지 확인
	SW 도입 가격 및 인증 여부 확인	- 단일 SW 5천만원 이상 또는 동종 구매 합산 5천만원 초과이면서 SW품목이 국가인증 획득 여부 조사
	구매계획 작성	- 소프트웨어사업 계약 및 관리감독에 관한 지침 별지 제2호 서식. 구매시기, 예산 규모등 명시 필요
3단계 직접구매대상 SW 제외사유 사전검토	제외사유 "미리검토"	- 조달 발주하는 사업의 경우 제외사유 적용 시 조달청에 미리검토 요청 - 자체발주 시 과업심의위원회 및 상위기관 등에 미리검토 요청
4단계 SW사업발주	발주 우선순위, 방법 선택	- 상용SW직접구매 사업 및 본 사업의 발주 우선순위 결정 - 상용SW직접구매 대상 SW 발주 방법(경쟁 입찰공고, 조달구매, 수의계약, GS우선구매 등) 결정

- 상용SW 직접구매 제도는 일괄발주 대비 추가적인 행정처리 증가와 통합사업 수행사와의 과업범위 불명확 등의 사유로 실제 공공SW발주 시장에서는 제외사유를 적용하여 일괄발주하는 사례 증가
- 경쟁 입찰공고(1억원 이상) 시 소프트웨어 품질성능 평가(BMT) 실시 및 평가를 반영해야 함.

IV. 상용SW 직접구매 제도 활성화 방안

현행 문제점	활성화 방안
직접구매를 위한 추가 업무가중으로 제외사유 증가	- 조달구매 시 BMT 절차 제외 및 계약 필요 절차 및 서류 간소화를 통한 제도 활성화 기여 - 과업심의 위원회 심의 시 해당내용 검토항목에 추가
통합사업자와 상용SW 납품 사업자 간 업무범위 불명확	- RFP에 통합사업자와의 명확한 업무정의 필수항목으로 포함

- SW 제값주기를 실현하기 위한 상용SW 직접구매 제도 개선 및 정착을 유도하여 발주자, SW사업자, 통합사업 간 선순환 생태계 구축 필요

"끝"

ITPE 기술사회
제129회 정보처리기술사 기출문제 해설집

대 상 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사, 정보시스템감리사 시험
발행일 2023년 02월 04일
집 필 강정배PE, 소민호PE, 전일PE, 정상PE, 석PE, 이상용PE, 장건환PE
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