119 회 정보처리기술사 합격을 위한

118 회 정보관리기술사

기출풀이

- KPC 기술사회-

SMART KPC
한국생산성본부

교육 문의 및 상담 : 한 승 연

- Tel : 02) 724-1831/1223
- Fax : 02) 724-1875
- Email : syhan@kpc.or.kr
- Web Site : www.kpc.or.kr
cafe.naver.com/81th

kpc 기술사회

119 회 합격대비 심화반 신청 안내

[토요일 명품심화반] 5.25.(토) 개강

- O 열정반(박상욱/KPC): cafe.naver.com/81th/134354
- O 공감반(공수재/KPC): cafe.naver.com/81th/134329
- O MP 필통반(구환회/KPC): cafe.naver.com/81th/134384
- O ITPE Makers(박제일/KPC): cafe.naver.com/81th/134386
- O 단합반(SPP 반)(안경환/KPC): cafe.naver.com/81th/134412
- O FB(Future Builders)(강희석/KPC): cafe.naver.com/81th/134330
- O 정주행(서정훈/KPC): cafe.naver.com/81th/134299

[일요일 명품심화반] 5.19.(일) 개강

- O T.O.P 반 (유술사/KPC): https://cafe.naver.com/81th/137407
- O NS 반 (강정배/박주형/강남아지트): https://cafe.naver.com/81th/134237

[유일한 평일 명품심화반] 5.17.(금) 개강

- O 강남평일야간반 (강정배/전일/강남아지트/화,금):

  https://cafe.naver.com/81th/133950

※ 신 청 : KPC 홈페이지에서 신청 가능합니다.

※ 교육비: 9 주 91 만원

국가기술자격 기술사 시험문제

기술사 제 118 회 제 3 교시 (시험시간: 100분)

분야	정보통신	종목	정보관리기술사	수험번호		성명	

※ 다음 문제 중 4문제를 선택하여 설명하시오. (각25점)

1. 데이터 웨어하우스에 적용되는 온라인 분석처리(OLAP, On-Line Analytical Processing)를 온라인 트랜잭션처리(OLTP, On-Line Transaction Processing)와 비교하여 설명하고, 분석정보 데이터베이스(데이터 웨어하우스)와 운영정보 데이터베이스(운영 데이터베이스)가 분리 운영되어야 하는 이유에 대하여 설명하시오.

2. 패스워드 없는 인증기술인 FIDO(Fast IDentity Online)에 대하여 다음을 설명하시오.
   가. FIDO의 개념
   나. 표준 프로토콜인 UAF와 U2F
   다. 유니버설 인증 프레임워크 (UAF) 총 11개 기술표준 구성요소

3. 클라우드 컴퓨팅 환경에서 클라우드 서비스 제공자가 이용자에게 안전한 서비스 제공을 위하여 다음을 설명하시오.
   가. 정보보호 정책의 관리적 측면과 기술적 측면으로 구분한 보호 조치분야
   나. 클라우드 컴퓨팅의 보안위협
   다. 클라우드 컴퓨팅의 프라이버시(Privacy) 이슈

4. 소프트웨어 기능안전(Functional Safety)에 대하여 다음을 설명하시오.
   가. 소프트웨어 안전과 소프트웨어 보안의 차이점
   나. IEC 61508에서 정의한 안전기능 요구사항의 도출과정
   다. IEC 61508과 의료기기, 항공기, 자동차 분야의 기능안전 표준들 간 비교

국가기술자격 기술사 시험문제

기술사 제 118 회 제 3 교시 (시험시간: 100분)

분야	정보통신	종목	정보관리기술사	수험번호		성명	

5. 정보시스템 감리와 사업관리위탁(PMO, Project Management Office)을 비교 설명하시오.

6. 당신은 어느 한 프로젝트의 PM이다. 아래 사항을 참조하여 다음을 설명하시오.

1. 프로젝트 수행기간의 목표는 25일이다.
2. A 액티비티는 소요기간이 10일이다.
3. B 액티비티는 A 액티비티가 완료된 후에 시작할 수 있으며, 소요기간이 13일이다.
4. C 액티비티는 소요기간이 12일이다.
5. D 액티비티는 C 액티비티 완료된 후에 시작할 수 있으며, 소요기간이 15일이다.

가. 네트워크 다이어그램을 작성하시오.

나. 주경로의 수행기간을 계산하시오.

다. 목표 수행기간을 맞추기 위해서 수행기간을 단축할 수 있는 방법을 설명하시오.

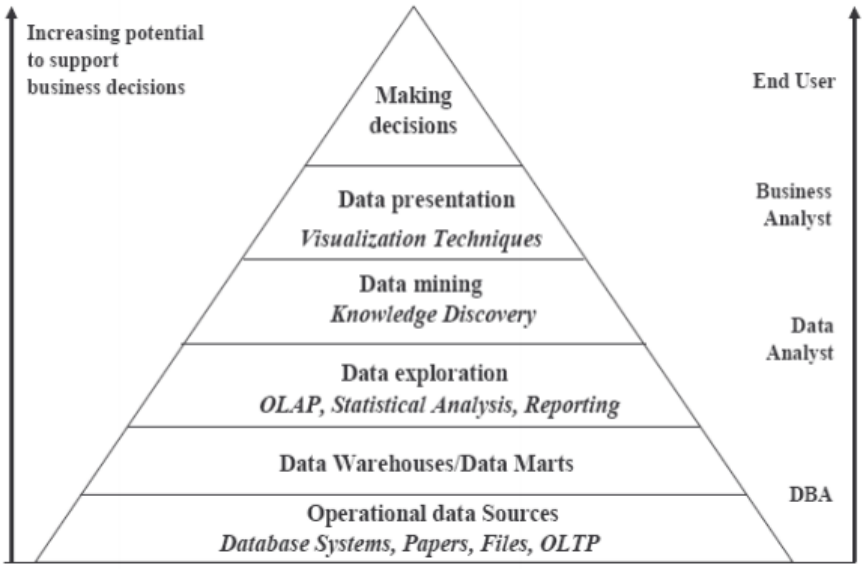
라. 일정을 단축하기 위해 기존팀원 5명에 더해 팀원 1명을 추가로 투입하였다. 의사소통 수(커뮤니케이션 통로의 수)가 기존보다 얼마나 더 늘어나는지 계산하시오.

마. 프로젝트 획득가치관리(Earned Value Management)보고서에 EV=95 백만원, PV=110 백만원, AC=100 백만원, BAC=950 백만원이다. CV와 CPI를 구하고 현재까지의 작업효율이 유지될 경우의 EAC를 계산하고 설명하시오.

(단, EV : Earned Value, PV : Planned Value, AC : Actual Cost, BAC : Budget At Completion, CV : Cost Variance, CPI : Cost Performance Index, EAC : Estimate At Completion이다.)

1	(OLAP, On-Line Analytical Processing), (OLTP, On-Line Transaction Processing)
문제	1. 데이터 웨어하우스에 적용되는 온라인 분석처리(OLAP, On-Line Analytical Processing)를 온라인 트랜잭션처리(OLTP, On-Line Transaction Processing)와 비교하여 설명하고, 분석정보 데이터베이스(데이터 웨어하우스)와 운영정보 데이터베이스(운영 데이터베이스)가 분리 운영되어야 하는 이유에 대하여 설명하시오.
도메인	경영
정의	OLAP: 사용자가 다차원 정보에 직접 접근하여 대화 형태로 정보를 분석하고 의사결정에 활용하는 과정 OLTP: 데이터 기입 및 트랜잭션 처리를 위해 시스템이 사용자 요청에 즉각 반응하는 처리
키워드	정형업무/비정형 업무, 데이터 조회/데이터 분석, 트랜잭션 처리량/데이터 처리량
출제의도분석	온라인 처리 중심인 OLTP 와 데이터 분석 중심인 OLAP 비교 분석
답안작성 전략	OLTP/OLAP 관계, OLAP, OLTP 개념 및 상세 비교, 분석정보와 운영정보를 분리 운영하는 이유 설명
참고문헌	contents.kocw.or.kr/document/region/2010/04/02/04_02_09_su01.pdf contents.kocw.or.kr/KOCW/document/2015/chungbuk/chowanseop/8.pdf https://d1.awsstatic.com/whitepapers/ko_KR/enterprise-data-warehousing-on-aws.pdf Wikipedia 참조
풀이 기술사	박부기 PE (제 117 회 컴퓨터시스템응용기술사 / arrgon7@gmail.com)

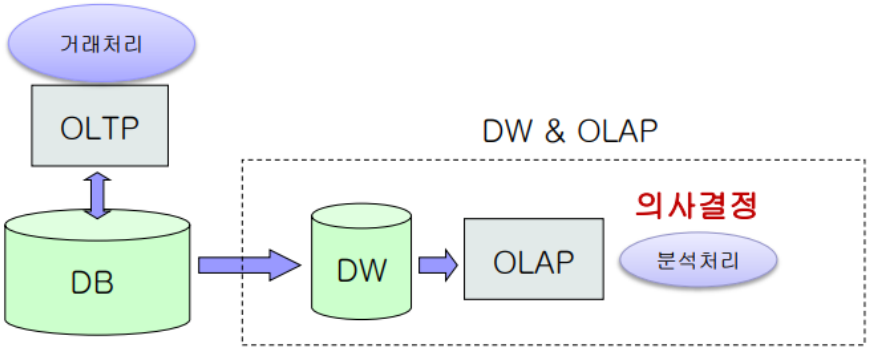
1. 정보 이용 환경 개선, OLTP 와 OLAP 관계



- 정형에서 비정형 업무로, 데이터 조회 중심에서 데이터 분석으로, 2 차원 DB 에서 다차원 DB 로 정보 이용 형태 및 IT 환경 변화

2. OLTP 와 OLAP 비교 설명

가. OLTP 와 OLAP 의 개념 비교

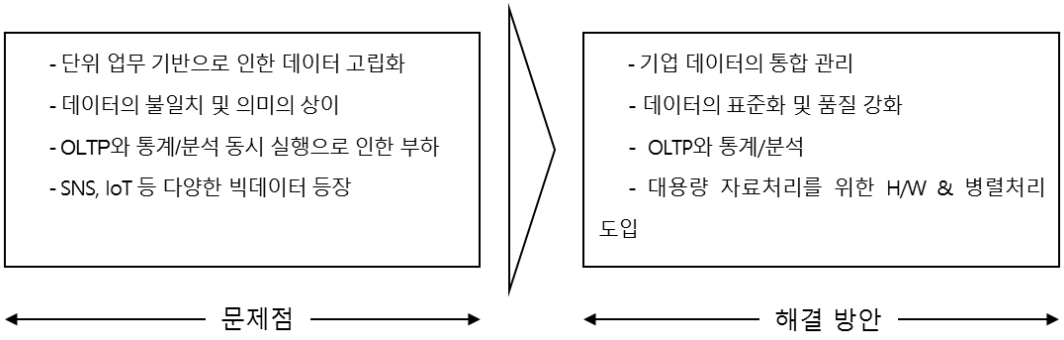
비교 항목	OLTP	OLAP
개념	데이터 기입 및 트랜잭션 처리를 위해 시스템이 사용자 요청에 즉각 반응하는 처리	사용자가 다차원 정보에 직접 접근하여 대화 형태로 정보를 분석하고 의사결정에 활용하는 과정
개념도		
목적	기업운영을 위한 거래처리 트랜잭션 처리가 주요 목적	최종사용자가 상황을 이해하고 의사결정을 지원하기 위해 데이터의 분석과 관리
특징	- "WHAT" 에 초점 - 처리시스템의 정확한 기록과 갱신에 초점	- "WHY" 에 초점 - 다차원분석을 통한 추이, 비교, 예측에 초점

나. OLTP 와 OLAP 세부 비교

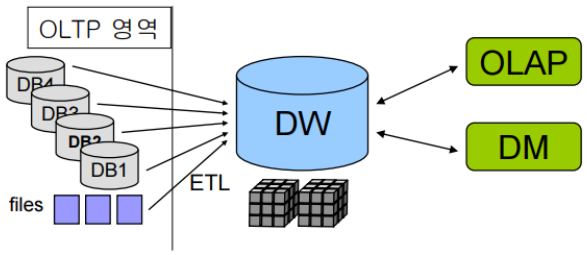
비교 항목	OLTP	OLAP
정보구성	업무 처리 중심	주제 중심
사용자층	운영자 계층	분석가/의사결정자 계층
사용 DB	관계형 DB(2 차원)	다차원 DB
구축 정보	세부거래 정보 Raw data	요약집계 정보 Summarized, consolidated data
주요 용도	거래 처리	분석, 계획, 보고서
적용 업무	정형 업무	비정형 업무
데이터 크기	Mb-Tb of data	Gb-Tb of data
SQL 유형	다수의 짧은 단순 SQL	복잡한 장시간 수행되는 SQL

3. 분석정보 데이터베이스와 운영정보 데이터베이스가 분리 운영되어야 하는 이유

가. 분석정보 데이터베이스와 운영정보 데이터베이스 통합 운영 문제점

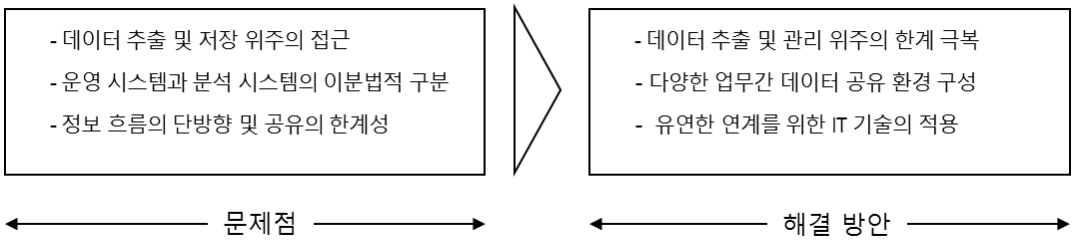


나. 분석정보 데이터베이스와 운영정보 데이터베이스 분리 운영 사례

항목	해결방안
개념도	
주요 기법	다양한 데이터 소스로부터 통합 구성 대부분 operational data 의 복사본 (운영 DB, DW DB 분리) non-volatile data 주제 중심적(subject-oriented), 다차원적 data ETL 을 통합 일괄배치, CDC 를 통한 준실시간 처리

- OLTP 중심인 운영정보 데이터베이스와 OLAP 울 위한 분석정보 데이터베이스 분리를 통해 시스템의 안정적인 운영과 대량의 사용자 데이터 분석환경 제공

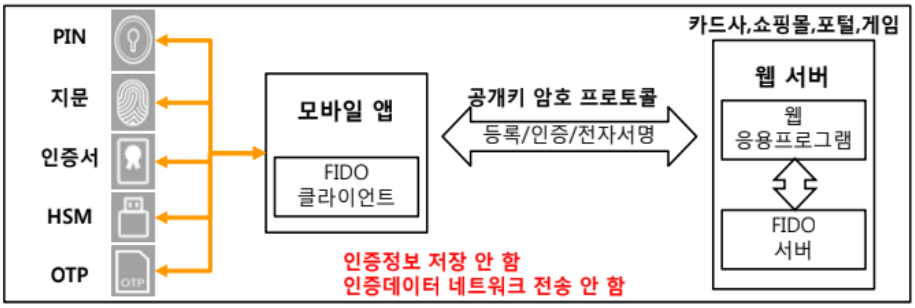
4. 분석정보 데이터베이스와 운영정보 데이터베이스 발전 방향



- Kafka 등 스트리밍 처리 기술 기반의 최신 IT 기술 적용을 통해 다양한 데이터 공유 및 추출 환경 개선 검토

2	FIDO(Fast IDentity Online)
문제	2. 패스워드 없는 인증기술인 FIDO(Fast IDentity Online)에 대하여 다음을 설명하시오. 가. FIDO 의 개념 나. 표준 프로토콜인 UAF 와 U2F 다. 유니버셜 인증 프레임워크 (UAF) 총 11 개 기술표준 구성요소.
도메인	보안
정의	비밀번호의 문제점을 해결하기 위한 목적으로 FIDO 얼라이언스에 의해 제안된 사용자 인증 프레임워크
키워드	UAF/U2F, FIDO 서버/클라이언트,
출제의도분석	기출 문제인 FIDO(Fast Identity Online)에 대한 세부 프로토콜 및 기술표준에 대한 심화 질문
답안작성 전략	목차는 물어본 순서대로 1.FIDO 의 개념, 2.표준 프로토콜인 UAF 와 U2F, 3. 유니버셜 인증 프레임워크 (UAF) 총 11 개 기술표준 구성요소에 대한 질문에 대한 충실한 답안 작성
참고문헌	wikipedia. – FIDO 서브노트 https://www.tta.or.kr/data/reportDown.jsp?news_num=4488 https://www.fsec.or.kr/common/proc/fsec/bbs/42/fileDownLoad/249.do
풀이 기술사	박부기 PE (제 117 회 컴퓨터시스템응용기술사 / arrgon7@gmail.com)

1. Multi-Factor 인증체계 보안강화, FIDO 의 개념

항목	세부 내용	
정의	현재의 ID/PW 방식 대신 지문, 홍채, 얼굴 인식 등 다양한 생체 인식 기반의 새로운 인증 시스템	
개념도		
처리 FLOW	생체 인증 등으로 사용자를 사용자 단말에서 로컬 인증하고 서버에서의 원격 인증을 위한 공개키/개인키 쌍을 생성하여 개인키를 이용해 전자서명을 수행	
구성요소	FIDO Client	- FIDO 인증 토큰과 인증 토큰 API 라는 인증 토큰 추상화 단계에서 연동하는 역할 - API 만 준용하면 어떤 종류의 인증 토큰이라도 FIDO 클라이언트

		에서 사용가능 - 역할: FIDO 서버와 프로토콜을 송수신하며 등록, 인증, 조회 서비스를 제공
	FIDO Server	- 클라이언트와 인증 프로토콜을 주고받아 서비스를 제공하는 것이 주역할 - 클라이언트가 제시하는 인증 토큰을 검증하고 등록 및 요청에 대해 평가하는 과정 수행
	FIDO Protocol	- 등록 메시지: 사용자가 디바이스에 있는 인증 토큰을 조회, 검증, 등록 - 인증 메시지: Challenge & Response 형태의 프로토콜을 수행하여 사용자를 인증 - 안전거래 메시지: 특정 거래에 대해 서버가 클라이언트에게 전자서명을 확인

- 비밀번호 없이 인증을 하기 위한 Universal Authentication Framework (UAF) 프로토콜과 비밀번호를 보완해서 인증을 하기 위한 Universal 2nd Factor (U2F) 프로토콜로 구성

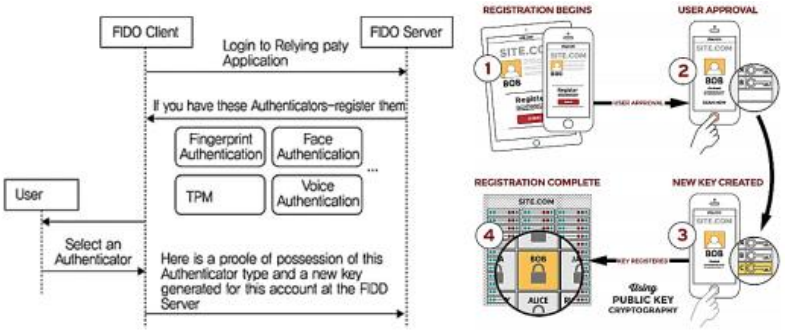
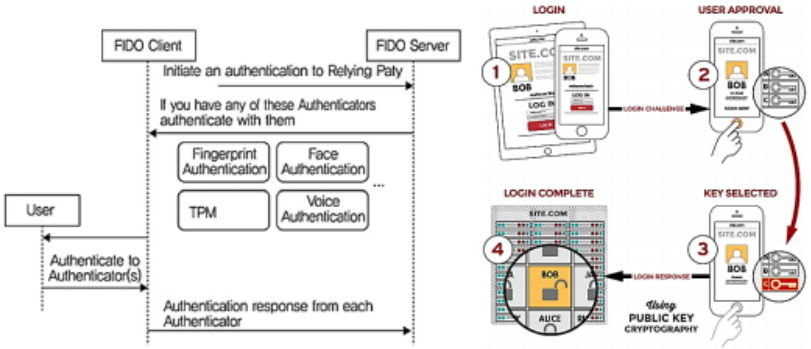
2. 표준 프로토콜인 UAF 와 U2F

가. FIDO 프로토콜

구분	절차	설명
UAF 프로토콜		-Universal Authentication Framework -비(非)비밀번호 인증표준으로 비밀번호 입력 없이 지문 등의 생체 인식이나 핀(PIN)으로 인증하는 방법 -사용자 클라이언트 디바이스에 UAF 정보를 인스톨 수행 -지문, 목소리, 얼굴인식 이용한 사용자 인증
U2F 프로토콜		-Universal Second Factor -UAF 방식으로 1 차 인증한 뒤 별도로 인증이 가능한 USB 단말기로 2 차 인증을 받는 방식

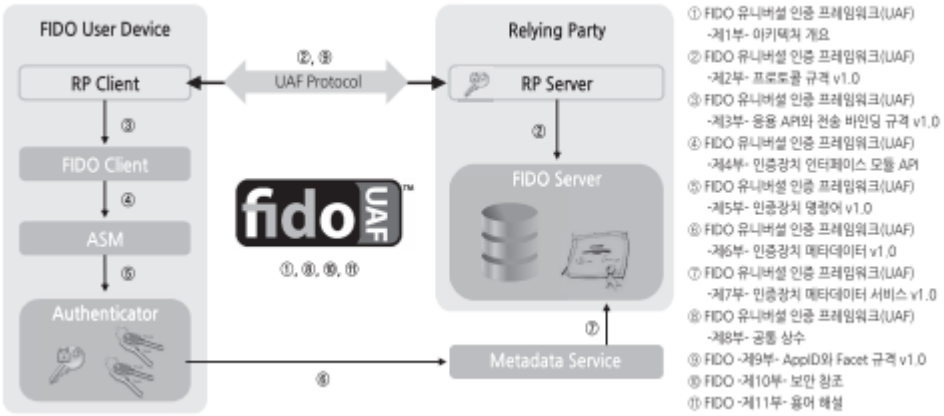
- 국제 온라인 인증 컨소시엄 얼라이언스에서는 FIDO 인증 표준으로 UAF, U2F 기술을 이용한 인증규격 선정

나. FIDO 처리과정

구분	처리절차
1. 등록 (Registration)	-사용자의 인증 토큰과 공개키를 등록하는 과정 ①FIDO 클라이언트가 FIDO 서버에 로그인 시도 ②FIDO 서버는 클라이언트에게 로그인 시에 사용 가능한 인증 토큰 리스트 보냄 ③사용자화면은 원하는 인증 토큰을 선택, 본인인증 수행 후 키 쌍을 생성 서명 후 서버전송 ④FIDO 서버는 사용자가 선택한 인증 토큰과 공개키를 등록, 향후 인증/전자서명 검증 
2. FIDO 인증 (Authentication)	-사용자의 인증 토큰과 공개키를 등록하는 과정 ①FIDO 서버는 인증에 필요한 Challenge 값인 난수와 인증 토큰을 보내 인증 요청 ②클라이언트에서는 디바이스에서 등록된 인증 토큰으로 사용자를 인증 ③비밀키를 이용, 서버에서 보내온 요청 메시지에 대한 응답으로 전자서명을 생성하여 전송 ④서버는 클라이언트가 보내온 전자서명을 등록된 공개키로 검증하여 사용자 인증 
3. 확인 (Validation)	전자서명기반 안전거래 확인 메시지 전송

3. 유니버셜 인증 프레임워크 (UAF) 총 11 개 기술표준 구성요소

가. 유니버셜 인증 프레임워크 (UAF) 구성도



나. 가. 유니버셜 인증 프레임워크 (UAF) 구성 요소

대구분	구성 요소	설명
FIDO 공통	(1) 아키텍처 개요 규격	- 배경 설명, 아키텍처, 사용시나리오 등 기본사항 - 대상: 엔지니어, 정책/의사 결정권자 대상
	(8) 공통 상수 규격	- 공통 사용 상수 정의 - 사용자 인증 방법, 서명 알고리즘, 고유 특성, 데이터 타입
	(10) 보안 참조 규격	- FIDO 표준의 보안성 분석 내용 기술 - 공격 대응 방법, 보안 환경 설명
	(11) 용어 해설 규격	- 기술용어, 약어
UAF 프로토콜	(2) 프로토콜 규격	- 프로토콜 메시지 규격, 세부 절차 설명 - 등록, 인증, 탈퇴 프로토콜로 3 개로 구성 - 대상: 엔지니어, 기술 활용 업체
	(9) AppID 와 Facet 규격	- 서비스 기관이 제공하는 어플리케이션 ID - AppID 는 서비스 기관 대표 id - Facet ID 는 서비스 기관이 제공하는 어플리케이션 각각에 부여한 ID
FIDO User Device	(3) 응용 API 와 전송 규격	- 응용 앱에서 FIDO 기술 이용하기 위한 방법 - 안드로이드 앱은 Intent API, iOS 는 Custom URL API 사용
	(4) 인증장치 인터페이스 모듈 API 규격	- FIDO 인증 장치에 접근할 수 있는 표준화된 방법 - FIDO 인증장치 배포는 FIDO ASM (표준화된 소프트웨어 인터페이스) 제공 - FIDO Client 는 FIDO ASM 통해 인증장치 검색
	(5) 인증장치 명령어 규격	- 다양한 형태 인증장치 구현 (SW/HW 방식, 지문/홍채/얼굴/카드 터치 등) - 인증장치가 공통으로 제공하는 명령어, 명령어 구조, 처리 절차 정의
인증장치	(6) 인증장치	- 사용자 인증 방법, 인증 성능, 보안 알고리즘, 인증 키

메타 데이터	메타데이터 규격	보호 메커니즘 등 인증장치 메타데이터 정의
	(7) 인증장치 메타데이터 서비스 규격	- FIDO 인증장치를 사용하는 서비스 기관(RP, Relying Party)이 메타데이터에 접근하는 방법 기술 - 인증 장치 신뢰성 확인 정보(Trust Anchor) 포함

- FIDO 기술은 다양한 분야에서 사업화가 진행되고 있으며, 금융 분야의 FIDO 기반 지문 인증 서비스, 기존 본인 확인 수단 대체, 출입통제 등에 활용되고 있음

3	클라우드 보안
문제	3. 클라우드 컴퓨팅 환경에서 클라우드 서비스 제공자가 이용자에게 안전한 서비스 제공을 위하여 다음을 설명하시오. 가. 정보보호 정책의 관리적 측면과 기술적 측면으로 구분한 보호 조치분야 나. 클라우드 컴퓨팅의 보안위협 다. 클라우드 컴퓨팅의 프라이버시(Privacy) 이슈
도메인	보안
정의	인터넷 상에 자료를 저장해 두고, 사용자가 필요한 자료나 프로그램을 자신의 컴퓨터에 설치하지 않고도 인터넷 접속을 통해 언제 어디서나 이용할 수 있는 서비스
키워드	하이퍼바이저, 가상화, 개인정보 위탁
출제의도분석	기업들의 퍼블릭 클라우드 활용 증가에 따라 클라우드 환경에서의 정보보호 조치, 보안위협 및 프라이버시 이슈 확인
답안작성 전략	클라우드 환경에서 다양한 관점의 보안이슈, 보안위협 및 대응방안 제시
참고문헌	20111011_클라우드_서비스_정보보호_안내서_원본(최종) – KISA 클라우드_정보보호_안내서 – KISA 클라우드 서비스환경 내 개인정보보호 측면에서의 국내외 동향분석 - INTERNET & SECURITY FOCUS December 2014
풀이 기술사	박부기 PE (제 117 회 컴퓨터시스템응용기술사 / arrgon7@gmail.com)

1. . 정보보호 정책의 관리적 측면과 기술적 측면으로 구분한 보호 조치분야

가. 관리적 측면의 보호 조치분야

보호조치 분야	주요 내용
정보보호조직, 인력보안	내·외부 업무수행 관련 인력의 역할 및 권리, 보안책임 등
정보자산 분류 및 통제	소유 및 관리 책임을 갖는 자산 목록, 정의 및 통제 방안 등
비상대응체계 및 사고관리	비상대응체계 구성원 및 운영체계 정의, 서비스 복구 계획 등
서비스 가용성 및 연속성	신규 보안대책 및 기술 도입에 따른 절차, 규정 등
법제도적 준거성 확보	서비스 제공 근거법령 및 규정 준수

- 정보의 외부 위탁, 클라우드 서비스 유형(XaaS) 등을 고려하여 관리적 보호조치 적용

나. 기술적 측면의 보호 조치분야

보호조치 분야	주요 내용
네트워크 보안	네트워크 접속, 이용 단말의 제한, IP 접근통제 등
시스템 및 가상화 보안	사용자 세션 관리 방안, 하이퍼바이저 취약점 관리 등
물리적 보안	데이터 센터 및 처리서버의 지리적 위치, 입출입 통제 방안 등
데이터 저장, 관리	개인정보처리방침, 데이터 암호화 적용절차 및 방법 등
사용자 인증 및 접근관리	사용자 계정 및 접근 관리정책, 특정 정보 및 상황을 위한 사용자 권한 관리 등

- 하이퍼바이저, 자원 공유, 다양한 단말기 접속 등 클라우드 특성을 고려한 기술적 보호조치 적용

2. 클라우드 컴퓨팅의 보안위협

가. 클라우드 서비스의 보안위협 현황

- 불충분한 인증 및 접근관리, APT, 시스템 취약점 등 증가하는 보안 위협에 대한 대응방안 마련 필요

나. 클라우드 서비스 보안위협의 대응방안

구분	위협	대응방안
관리적 보안위협	클라우드 컴퓨팅 남용	- 사용자 신원 검증 절차 수립 및 이행 - 주기적 이용자 모니터링
	악의적인 내부자들	- 특정 사용자에 대한 권한 분산 - 사용자별 권한 차등 부여 - 퇴직자, 전배자 권한 회수 절차 수립 및 이행
	클라우드서비스 이해부족	- 가상화 환경에서 HW, NW 직접 제어가 불가능 - 업무시스템의 가상화 환경에서의 안전성 확보 방안 검토
	불충분한 인증 및 접근관리	- SSO, MFA, EAM, IP 접근제어, 권한 차등 부여 등 적용
	APT	- 방화벽, IPS, WIPS, 보안관제, EDR(Endpoint Detection Response)
기술적 보안위협	안전하지 않은 API	- 안전한 API 설계(Security by Design), 클라우드 적용
	가상화 취약점	- 하이퍼바이저 취약점 패치 - 서버 인스턴스간 접근통제
	계정, 서비스 &트래픽 탈취	- 입출력값 검증, Two-Factor 인증, 보안 라이브러리(AntiXss 등) 사용
	데이터 유출	- 암호화, 키와 데이터 분리보관, HSM, KMS
	데이터 손실	- 백업, 무결성 검증, 최소 권한의 원칙(Write 권한 제한)
	서비스 거부(DoS)	DoS 공격 차단 솔루션, 비정상 트래픽 유발 IP 차단
	시스템 취약점	- 시스템 취약점 패치, 패스워드 관리 강화, 불필요 서비스(FTP, SSH 등) 비활성화

- 자원 오남용, 가상화 기술에 대한 이해를 기반으로 대응방안 마련
- 클라우드에 개인 정보 위탁 운영에 따른 프라이버시 이슈 존재

3. 클라우드 컴퓨팅의 프라이버시(Privacy) 이슈

구분	주요 이슈	대응방안
법 규제 측면	거버넌스 차이	클라우드의 어플리케이션 개발 및 서비스 조항에 적용되는 정책, 절차 및 표준 수립 시스템 생명주기에 걸쳐 해당 사례가 지켜지는지 감사 메커니즘 및 도구 마련

	준거성	조직의 요구사항 및 계약 조건 충족 확인
	신뢰성	개인정보보호 통제 절차의 투명성과 관련한 매커니즘을 SLA 에 포함
	사고대응	개인정보 침해사고대응에 대한 계약 조항 및 절차를 이해
아키텍쳐 측면	**ID 및 접근관리**	인증, 권한부여, ID 및 접근관련 기능을 위한 적절한 보호 장치 확립
	소트트웨어 격리	클라우드 제공자가 사용하는 가상화 및 기타 소프트웨어 격리 기술에 대한 이해
	가용성	장기적인 분열 및 심각한 재해 발생 시 운영의 즉각적인 복구 방법 확립
	공유기술의 취약점	공유자원의 접근통제, 인증 절차 수립 및 이행
	공급자 의존	클라우드 서비스에 대한 호환성을 보장할 수 있는 도구나 표준 수립
데이터 측면	**데이터 통제권 양도**	위험평가, 데이터 중요도에 따른 퍼블릭 클라우드에 선별적 활용 및 데이터 이관
	데이터 보호	클라우드 제공자의 데이터 관리 솔루션에 대한 적합성 평가
	불완전한 데이터 삭제	개인정보 파기절차 수립 및 이행, 복구 불가능한 삭제
	데이터 손실	DLP(Data Loss Prevention), 데이터 백업

- 클라우드 컴퓨팅은 서비스유형, 배치형태에 따라 다양한 기술모델이 존재

4. 클라우드 컴퓨팅 도입 시 보안 고려사항

구분	핵심요소	상세 내용
조직측면	**조직 및 조직원 역할 수립**	기존의 IT 시스템 구축 및 운영 중심에서 서비스 운영 및 공급자 역할과 책임을 가지는 조직으로 변화
	변화 관리	선행팀 운영, 모범사례 공유, 전문가 세미나, 내부 연구모임, 전문 교육
정책측면	**표준 운영 모델 수립**	네트워크 구성, IP 통제 및 모니터링, 침해방지 및 모니터링, 암호화 등 보안운영모델 수립
	정책 식별 및 개정	법규, 지침, 절차 검토 및 개정
기술측면	**보안 아키텍쳐 수립**	서비스 도입 시 영향받는 통제항목 식별
	보안 솔루션 검증	- 현재 솔루션의 클라우드환경 적용 가능성 - 클라우드 제공 솔루션이 표준에 부합하는지 확인

- 클라우드 도입을 고려한 기업은 기업의 필요와 목적에 따라 클라우드 컴퓨팅 기술 모델을 선정하고 관련 기술, 비용, 보안을 고려한 전략적인 결정을 통해 시행착오 최소화

4	소프트웨어 기능안전
문제	4. 소프트웨어 기능안전(Functional Safety)에 대하여 다음을 설명하시오. 가. 소프트웨어 안전과 소프트웨어 보안의 차이점 나. IEC 61508 에서 정의한 안전기능 요구사항의 도출과정 다. IEC 61508 과 의료기기, 항공기, 자동차 분야의 기능안전 표준들 간 비교
도메인	디지털 서비스
정의	위험을 감지하고 안전하게 조치(제거, 회피, 경감, 복구 등)하기 위한 SW 기능
키워드	DO-178B(C), ISO26262, ISO62304, ISO6061, SIL, ASIL
출제의도분석	4 차 산업혁명시대에 소프트웨어의 활용도 및 영향력 증가에 따라 소프트웨어 안전성 및 표준에 대한 이해 확인
답안작성 전략	물어본 내용을 목차로 하여 충실하게 내용 작성
참고문헌	- 소프트웨어 안전(Safety) 산업 동향 조사, SPRi, 2017. 8. - 소프트웨어 안전성 확보 체계에 관한 연구, SPRi, 2016. 1. - SW 안전성 안전성 공통 개발 가이드 가이드, NIPA, 2016. 11. - 항공안전을 위한 소프트웨어 인증 기술 발전 동향, 항공우주산업 기술동향, 2013 - KPC 심화반 강의교재, 기출풀이, 모의고사
풀이 기술사	박부기 PE (제 117 회 컴퓨터시스템응용기술사 / arrgon7@gmail.com)

1. 소프트웨어 안전과 소프트웨어 보안의 차이점

가. 소프트웨어 안전과 소프트웨어 보안 정의

구분	정의
소프트웨어 안전	- 소프트웨어로 인한 사람의 생명이나 신체에 대한 위험의 발생을 방지하거나 이에 대한 충분한 대비가 되어 있는 상태 - 인명 피해나 시스템, 장비, 재산 등의 손실을 가져올 수 있는 위험요소를 확인 및 관리하여 위험이 수용 가능한 수준 이하로 유지되는 상태
소프트웨어 보안	안전한 소프트웨어 개발을 위해 소스 코드 등에 존재할 수 있는 잠재적인 보안 취약점을 제거하고, 보안을 고려하여 기능을 설계 및 구현하는 등 소프트웨어 개발 과정에서 지켜야 할 일련의 보안 활동

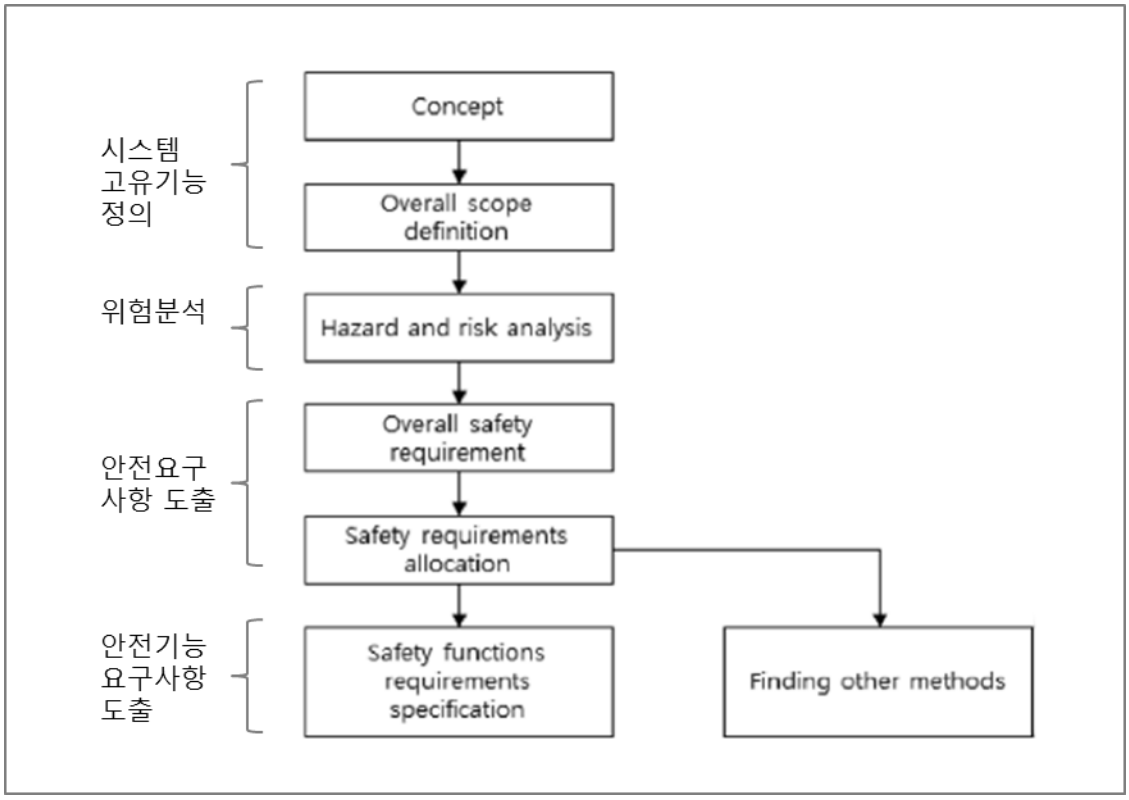
나. 소프트웨어의 안전과 소프트웨어 보안의 차이점

구분	소프트웨어 안전	소프트웨어 보안
목적	소프트웨어 오류로 인한 수용 불가능한 위험을 제거	외부로부터의 보안위협에 대응하기 위한 취약점 제거
범위	기능 단위의 국소적 범위	시스템 단위
요구분석	기능 요구 안전 분석	SDLC 보안 요구 분석
분석기법	정형기법(정형명세, 정형개발, 정형검증)	정성적 분석, 정량적 분석
표준	IEC61508, ISO26262, IEC60601, IEC 62304, DO178B/C	OWASP Top 10, 시큐어 코딩 가이드라인, CWE

영향	사람의 생명이나 신체에 직접적 영향	- 시스템 기능 마비, 시스템 침해를 통한 금전요구, 정보유출
평가수준	ASIL, SIL	EAL

2. IEC 61508 에서 정의한 안전기능 요구사항의 도출과정

가. IEC 61508 의 요구사항 도출 절차



- 위험원 및 위해사건에 대한 식별과 위험분석이 중요

나. IEC61508 의 요구사항 도출 과정 설명

구분	도출 과정	설명
시스템 고유 기능정의	**Concept (개념)**	- 필요한 제어기능 및 물리적 환경 정의 - 유해사건 원인 결정, 위험원 정보, 안전규정 파악
	Overall Scope Definition (범위 정의)	- 위험원과 리스크 분석 적용 범위(프로세스, 환경) 결정 - 외부 사건, 연관된 장비/시스템, 고려할 사건 유발 유형 결정
위험분석	**Hazard & Risk Analysis (위험원 및 위험분석)**	- 위험원 식별 : 위험원, 위해사건 식별(위험원 제거/감소 고려 - 위험성 계산 : 결과 확인(심각도), 정량적/정성적 위험원 및 리스크 분석 기법 적용 - 위험한 사건과 관련된 위험 결정(평가/추정)
안전요구 사항 도출	**Overall safety requirement**	- 안전 기능 요구사항 명세 - 안전 무결성 요구사항 명세

	(안전 요구사항 명세)	
	Safety requirements allocation (안전 요구사항 할당)	- 안전기능 → 안전관련 시스템, 위험감소 수단에 할당 - 안전 무결성 수준(SIL) → 각 안전 기능에 할당
안전기능 요구사항 도출	**Safety functions requirements specification (안전 요구사항 명세)**	- 안전 기능 요구사항들의 명세화

- 산업군 특성에 맞는 기능안전 등급, 분석절차 필요성으로 표준 세분화

3. IEC 61508 과 의료기기, 항공기, 자동차 분야의 기능안전 표준들 간 비교

가. 의료기기, 항공기, 자동차 분야의 기능안전 표준

구분	표준	설명
의료기기	IEC 60601	- 의료기기에 대한 안전 요구사항을 도출하여 안전성 분석 수행
	IEC 62304	- 의료기기 개발 및 유지보수의 개발 생명주기 정의, 각 단계별 수행해야 하는 활동과 지표 및 산출물 정의
	ISO 14971	의료기기 개발 시 필요한 위험분석방법의 규정 및 SW 개발 단계 적용
항공기	DO-178B	1992 년 상용 항공 산업 내 사용되는 SW 의 인증 표준
	DO-178C	DO-178B 의 SW 안전성에 대한 부족성, 신기술에 대해 보완 개정으로 2011 년부터 현재까지 항공 산업내 사용되는 SW 인증 표준 상해에 대한 등급 및 안전 테스트 방법 기술
자동차	ISO26262	IEC61508 을 바탕으로 자동차 분야 적용 위해 발표된 표준 자동차 ECU 의 오작동으로 인한 사고 및 인명손실 최소화 목적

- 기능안전표준인 IEC 61508 을 근간으로 의료기기, 항공기, 자동차 등의 제품안전규격으로 세분화

나. IEC 61508 과 의료기기, 항공기, 자동차 분야의 기능안전 표준들 간 비교

. 구분	산업 전기/전자 IEC61508	항공 DO-178C	의료 IEC62304	자동차 ISO26262
개요	전기/전자 고신뢰 시스템 기능 안전 표준	항공시스템 및 장비에 대한 안전 표준	의료 기기 및 SW 에 대한 위험 표준	자동차 전기/전자 시스템의 기능 안전 표준
목적	안전성과 경제적 성능 및 효율을 향상	항공기에 탑재되는 SW 의 FAA 인증	의료기기의 위험 판단 및 사고 방지	자동차 SW 오류로 인한 사고 방지
구성	7 개 파트	9 개 파트	2 개 파트	10 개 파트 (2^{nd} 13 개 파트)

생명주기 목표	계획, 구축, 문서화, 실행 계획 만족 여부 문서화	시스템 생명주기에 포함된 안전성 평가	개발 및 유지보수 생명 주기로 정의	개발 및 생성 시작 후의 안전 활동을 위한 관리
안전무결성 레벨	SIL 1,2,3,4(최고등급)	DAL E-A(최고등급)	CLASS A, B, C(최고등급)	ASIL A~D(최고등급)

- 이외에도 철도 IEC62279, 원자력 IEC61513 등의 표준이 존재

5	감리/PMO
문제	정보시스템 감리와 사업관리위탁(PMO, Project Management Office)을 비교 설명하시오
도메인	소프트웨어 공학
정의	- 감리는 이해관계자로부터 독립된 자가 제 3 자적 관점에서 정보시스템 품질향상을 위해 종합적인 점검을 하고 문제점을 개선하도록 하는 제도 - PMO 는 전자정부사업을 효율적으로 수행하기 위해 전자정부사업을 전문지식과 기술능력을 갖춘 자에게 위탁하는 제도
키워드	발주자 관점, 제 3 자 관점, 법적근거, 투입시점, 주요 산출물 등 비교
출제의도분석	빈출 문제로 PMO 와 정보시스템 감리의 정확한 이해 여부 확인
답안작성 전략	정보시스템 감리와 PMO 를 다양한 관점으로 풍부하게 비교 설명하고 제도의 문제점에 대한 해결방안을 제시
참고문헌	한국정보진흥원(NIA) PMO 도입 가이드 행정안전부 "상주감리 및 PMO 제도화 방안 정보화사업 PMO 운영관리메뉴얼 (NIA) 정보시스템 감리 수행 가이드 (NIA) [전문가기고] 정보시스템 감리와 PMO 논쟁, 해결책은?
풀이 기술사	박부기 PE (제 117 회 컴퓨터시스템응용기술사 / arrgon7@gmail.com)

1. 정보시스템 감리와 PMO 의 필요성

구분	필요성
프로젝트 기간	대규모의 장기 프로젝트는 다양한 위험요소(일정, 이슈, 자원 등) 존재
대규모 인력 및 예산	대규모 인력관리 누수 발생, 초기 예측하지 못한 변수 발생으로 프로젝트 예산 초과
다양한 이해관계자	이해관계자의 기대수준이 상이, 이해관계자들간의 커뮤니케이션 문제 발생
대기업 참여제한 및 신기술	대기업 참여제한 및 신기술의 적용으로 현업과 IT 인력에 대한 지속적인 변화문제 발생 위험

- 정보시스템의 위험 최소화, 품질 향상을 위해 감리와 PMO 제도 필요
- 감리는 프로젝트의 진행 중 사후진단, 투자목적에 부합한 기능/비기능적 목적, 목표의 달성과 최종품질확보를 위하여 절차, 산출물, 성과관점에서 다각적이고 전문적인 점검을 수행
- PMO 는 사전진단, 철저한 프로젝트 단계별 계획수립, 정량적 공정관리, 주기적 의사소통과 산출물 품질 확보 등을 위해 필요

2. 정보시스템 감리와 PMO 의 설명

가. 정보시스템 감리 설명

구분	감리
정의	정보시스템 감리는 "전자정부법 57 조 행정기관등의 정보시스템 감리"

	법령에 따라 이해관계로부터 독립된 자가 제 3 자적 관점에서 정보시스템 품질향상을 위해 종합적인 점검을 하고 문제점을 개선하도록 하는 제도
배경	공공정보화 시장은 국내 SW 산업 발전의 토양이 될 수 있도록 중소기업 중심으로 전면 개편 - 11.07 월부터 3 단계 감리 제도 본격 시행. 단계별 감리의 한계로 인해 자율적으로 상주감리를 실시
역할	사업관리 및 품질보증, 응용시스템, 데이터베이스, 시스템 구조 및 보안 등 기능 및 과업이행여부 점검 및 조치 확인
유형	- 정기감리 : 정보시스템 구축사업을 제외한 EA 수립, ISP 컨설팅, DB 구축, 유지보수사업, 운영사업에 대하여 특정단계에 정기적으로 실시하는 감리 - 3 단계 감리 : 감리기준 제 3 조제 1 항에 따라 정보시스템 구축 사업에 대하여 감리시점을 3 단계로 나누어 요구정의, 설계, 종료단계 감리를 실시하는 감리 - 상주감리 : 감리 대상사업 전기간 또는 특정기간 동안 감리원이 현장에 직접 상주하며 감리 활동을 수행하는 감리

나. PMO 설명

구분	PMO
정의	PMO(프로젝트 관리 조직)는 "전자정부법 64 조의 전자정부사업관리의 위탁" 법령에 따라 전자정부사업을 효율적으로 수행하기 위해 전자정부사업을 전문지식과 기술능력을 갖춘 자에게 위탁하는 제도
배경	「소프트웨어산업진흥법」의 개정 2013 년부터 국가기관 등이 발주하는 소프트웨어사업에서 대기업의 참여제한에 따라, 공공정보화 관련 사업이 중소기업 중심으로 전환되어 정보화사업의 품질 및 원활한 사업수행을 위한 전문성 확보 필요
역할	- 일정, 인력, 위험, 품질관리 등 사업관리 전체 모니터링 및 지원 - 과업이행여부 점검 및 조치지원 - 발주기관 요구사항 지원 등
유형	- R&R 구분 : 기상대, 지도, 관제탑 모델 - 조직위치 구분 ; 내부조직, 외부조직, 하이브리드 조직 구성 - Skill 구분 : 프로젝트 통합관리, 범위관리, 일정관리, 원가관리, 품질관리, 자원관리, 이해관계자관리, 의사소통관리, 위험관리, 조달관리 - 투여시간 및 직위 구분 : part time, Full time, PMO Directior

3. 정보시스템 감리와 PMO 의 비교

가. 제도 도입 측면의 비교

구분	감리	PMO
제도 도입 취지	사업시행자가 국가정보화사업을 수행함에 있어 발주기관의 요구대로 수행하였는지를 점검하여 정보시스템의 품질을	국가정보화사업에 대기업집단의 참여가 전면 제한됨에 따라 발주기관과 중소기업의 사업관리 전문성 부족 문제를 보완

	보장	
관점	제 3 자 관점 (독립적)	발주자 관점
투입시점	발주 후의 프로젝트 단계별 감리	발주 전과 프로젝트 중 단계별 지원
법적근거	전자정부법 제 57 조 1 항에 따른 의무사항	전자정부법 제 64 조 2 에따른 권고사항
기대효과	- 사업관리에 대한 점검 지원 - 위험요소의 대응방안 제시 - 정보시스템 및 산출물 품질 향상	- 잠재적인 프로젝트 위험 조기 식별 - 조직의 목적과 IT 연계하여 관리 - 효고적인 자원배분을 통한 비용절감

나. 수행 측면의 비교

구분	감리	PMO
수행역할	- 계약서와 실체 진행 내용의 차이에 대해서 확인하고, 원인을 파악해 적절한 조치권고 - 단계별 검증 및 테스트 - 산출물 검증 및 추적	발주 전: RFP작성, 프로젝트 원칙수립, 초기위험 도출, 발주처 선정지원 발주 후: 발주지원조직운영(PMO), 사업관리계획수립, 업무표준 프로세스 수립
수행조직	감리법인	컨설팅업체, 회계법인, 대형 SI
주요산출물	- 감리계획서 - 감리수행결과보고서 - 시정조치확인보고서	- 요구사항 정의서(RFP) - 사업자 선정 기준서 - 사업자 관리 계획서 - 아키텍처 정의서 - 영역별 관리 계획서
사업관리측면	직접 사업관리업무 수행하지 않음.	사업관리 수행

- 감리는 기술적 측면의 평가 성격이며 PMO 는 프로젝트 전 과정에 개입하는 관리적 성격이 강함

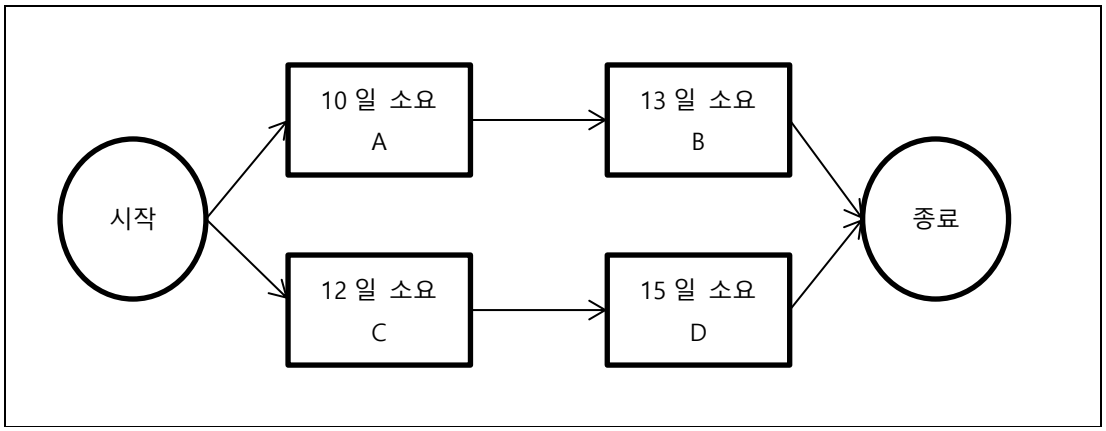
4. 정보시스템 감리와 PMO 문제점 및 개선방안

구분	문제점	개선방안
감리	- 도메인에 대한 이해 부족 - 실질적 도움보다는 문서에 의존한 형식적인 점검	- 품질제고를 위한 감리지침 연구 - 정보기술 및 환경에 맞춰 도구 개선
PMO	- 담당인력의 개인 역량에 의존 - 모호한 도입기준 - 예산부족	- 전문교육을 통한 역량 향상, - 조직측면의 체계적인 지원 - 적용대상 기준 명문화

- 감리 및 PMO 제도는 상반되는 관점에서 서로 상호보완적 관계도 있음을 인식하고 복잡도(Complexity)가 높아지는 IT 상황에 맞게 탄력적으로 활용하여 사업성과에 기여.

6	CPM / EVM
문제	6. 당신은 어느 한 프로젝트의 PM 이다. 아래 사항을 참조하여 다음을 설명하시오. --- 1. 프로젝트 수행기간의 목표는 25 일이다. 2. A 액티비티는 소요기간이 10 일이다. 3. B 액티비티는 A 액티비티가 완료된 후에 시작할 수 있으며, 소요기간이 13 일이다. 4. C 액티비티는 소요기간이 12 일이다. 5. D 액티비티는 C 액티비티 완료된 후에 시작할 수 있으며, 소요기간이 15 일이다. --- 가. 네트워크 다이어그램을 작성하시오. 나. 주경로의 수행기간을 계산하시오. 다. 목표 수행기간을 맞추기 위해서 수행기간을 단축할 수 있는 방법을 설명하시오. 라. 일정을 단축하기 위해 기존팀원 5 명에 더해 팀원 1 명을 추가로 투입하였다. 의사 소통 수(커뮤니케이션 통로의 수)가 기존보다 얼마나 더 늘어나는지 계산하시오. 마. 프로젝트 획득가치관리(Earned Value Management)보고서에 EV=95 백만원, PV=110 백만원, AC=100 백만원, BAC=950 백만원이다. CV 와 CPI 를 구하고 현재까지의 작업효율이 유지될 경우의 EAC 를 계산하고 설명하시오. (단, EV : Earned Value, PV : Planned Value, AC : Actual Cost, BAC : Budget At Completion, CV : Cost Variance, CPI : Cost Performance Index, EAC : Estimate At Completion 이다.)
도메인	소프트웨어 공학
정의	CPM : Activity 간 의존관계 파악, 임계경로 선정, 일정 계산 EVM : 원가와 일정을 종합적으로 고려하여 프로젝트 관리하는 기법
키워드	CPM : Forward/Backward Scheduling, 주경로, Crashing, Fast Tracking EVM : 측정요소(PV, EV, AC, BAC), 분석요소(SV, CV, SPI, CPI), 예측요소(ETC, EAC)
출제의도분석	CPM 과 EVM 이해 확인
답안작성 전략	CPM 과 EVM 에 대한 정확한 풀이보기 쉽게 표현
참고문헌	서브노트, KPC 기출문제 풀이집
풀이 기술사	박부기 PE (제 117 회 컴퓨터시스템응용기술사 / arrgon7@gmail.com)

1. 네트워크 다이어그램을 작성하시오.



2. 주경로의 수행기간을 계산하시오.

- 프로젝트의 활동 경로 중 가장 긴 시간이 소요되는 경로를 계산

주경로	주경로 수행기간
C → D (12 + 15)	27

3. 목표 수행기간을 맞추기 위해서 수행기간을 단축할 수 있는 방법을 설명하시오.

기법	핵심	설명
공정 압축법 (Crashing)	자원 추가	- 비용과 시간 사이의 상충 관계를 분석하여 최소한의 자원 추가로 최대한 시간을 단축할 방법을 결정하는 기법 - 단점 : 비용 증가
공정중첩 단축법 (Fast Tracking)	작업 병행 추진	- 일정계획상의 Activity 간의 Dependency 를 조정해서 순서상의 활동을 중첩 진행하여 일정을 단축하는 기법 - 단점 : 활동 중첩 가능 경우에만 적용, 재작업 위험 증가

- 자원 추가하는 Crashing 기법과 병행 추진의 Fast Tracking 으로, 필요 시 일정 단축 수행

4. 일정을 단축하기 위해 기존 팀원 5 명에 더해 팀원 1 명을 추가로 투입 시 의사 소통 수(커뮤니케이션 통로의 수)가 기존보다 얼마나 더 늘어나는지 계산 하시오.

- 의사소통 채널수는 프로젝트 의사소통의 복잡성을 나타내는 척도.

  의사소통 채널수 = N*(N-1) /2

  (N은 전체 이해관계자 수를 나타냄)

구분	인원 수	의사소통 채널 수	채널 증가 수
현재(기존)	6 명 (PM 1 명 + 팀원 5 명)	- 6 * (6 -1) = 30/2 = 15	기존보다 6 만큼 증가
팀원 1 명 추가 시	7 명 (PM 1 명 + 팀원 6 명)	- 7 * (7 -1) = 42/2 = 21	

5. 프로젝트 획득가치관리(Earned Value Management)보고서에 EV=95 백만원, PV=110 백만원, AC=100 백만원, BAC=950 백만원이다. CV 와 CPI 를 구하고 현재까지의 작업효율이 유지될 경우의 EAC 를 계산하고 설명하시오.

구분	지표	풀이
측정요소	PV	110 백만원
	EV	95 백만원
	AC	100 백만원
	BAC	950 백만원
분석요소	CV	EV-AC = 95 백만원 – 100 백만원 = -5 백만원 (예산 초과)
	CPI	EV/AC = 95 백만원 / 100 백만원 = 0.95 (예산 초과)
예측요소	ETC	- 정형 : (BAC-EV)/CPI = 855 백만원 / 0.95 = 900 백만원
	EAC	- 정형 : (AC+ETC) = 100 백만원 + 900 백만원 = 1000 백만원