1	이해관계자 관리(Stakeholder Management)를 위한 절차와 현저성 모델(Salience model)
문제	프로젝트 이해관계자 관리(Stakeholder Management)를 위한 절차와 현저성 모델(Salience model)에 대해 설명하시오.
도메인	소프트웨어 공학(프로젝트 관리),
정의	현저성 모델: Mitchell, Agle and Wood 이 만든 이해관계자 분석을 통합 분류 모델
키워드	Power (권력, 권한), Legitimacy(합법성, 합리성), Urgency(긴급성) 속성 3 가지
출제의도분석	이해관계자 절차는 주요 프로세스로 이해, 단, 현저성 모델은 상식 및 많은 모델 중으로 하나로, 출제 의도 분석 없음. 우선순위 떨어짐
답안작성 전략	1 교시형 2 가지 지문에 대한 병렬 작성
참고문헌	주소: http://virk.wordpress.com/2010/03/23/salience-model-stakeholder-analysis/
풀이 기술사님	강정배 PE (제 78 회 정보관리/ kangjungbae@naver.com)

■ **프로젝트의 성공과 실패의 결정자 관리, 이해관계자 관리 개요**

이해관계자 관리(Project Stakeholder Management) 의 정의

- 프로젝트에 영향을 주거나 받을 수 있는 사람, 그룹, 조직을 식별하고 이해관계자의 기대사항과 영향력을 파악하며 프로젝트의 의사결정과 실행에 영향력 있는 이해관계자에 대한 적절한 관리전략을 포함한 프로세스

■ **이해관계자 관리(Stakeholder Management)를 위한 절차**

핵심역량	설명	주요 산출물
이해관계자 식별	프로젝트 결과에 영향을 미치는 개인이나 그룹 또는 조직	이해관계자 관리대장
이해관계자 관리 계획	이해관계자를 효과적으로 참여시키기 위한 적절한 관리계획 개발	이해관계자 관리계획
이해관계자 참여 관리	이해관계자의 기대 및 요구사항, 이슈 등에 대해 소통하는 프로세스	이슈로그, 변경 요청(CR)
이해관계자 참여 통제	이해관계자 참여 계획과 관계에 대한 전반적인 모니터링	WPI(Work Performance Index), 변경 요청(CR)

■ **현저성 모델**

- 이해관계자를 분석한 후에, 프로젝트 관리자가 이해관계자를 잘 관리하기 위해, 권력, 합법성, 긴급성의 3 가지 속성으로 분류하여 이해관계자를 분류하고, 그들의 등급을 부여해서 관리하는 모델

[그림] 현저성 모델을 적용한 분류 사례(7 등급으로 구분함)

"끝"

2	V2V(Vehicle to Vehicle)
문제	**V2V(Vehicle to Vehicle)의 개념과 적용 시 고려사항에 대해 설명하시오.**
도메인	디지털서비스
정의	차량 안전서비스를 위한 차량간 멀티홉 통신 기술
키워드	VANET, 차량간 멀티홉 통신 기술, WAVE, 브로드캐스팅
출제의도분석	ISO26262(93 응), AUTOSAR(96 정)와 더불어 자동차관련 문제의 증가추세 (IoT 의 메가트랜드의 일환으로 Smart Car, Connected Car 시장의 급성장 기반)
답안작성 전략	V2V 의 개념과, 적용 시 고려사항에 집중하여 답안 작성 필요 (WAVE 등의 연관토픽에 대한 설명이 많아지는 답안작성은 금물)
참고문헌	- 차량밀집환경에서 안전하고 효율적인 V2V 메시지인증기법-정보보호학회논문 - 프라이버시를 보호하며 안전하고 효율적인 차량간 통신프로토콜 정보보호학회논문 (2010.12)
풀이 기술사님	박상욱 PE (제 99 회 정보관리/ studygosu@gmail.com)

■ **V2V(Vehicle to Vehicle)의 개념**

가. V2V 의 정의

- VANET((Vehicular Ad-hoc NETwork)의 요소기술로, 차량 안전서비스를 위한 **차량간 멀티홉 통신 기술**

나. V2V 의 요구사항

요구사항	설명
호환성	- WAVE 를 기반으로 한 V2X 기술들과의 호환되는 성질
자체구성	- 주기적 안전주행 메시지 브로드캐스팅을 통한 홉(차량)통신 지원
보안성	- V2X 기술과의 호환, 내부 참여자 통신시 메시지는 보안성 만족
프라이버시	- 차량 위치 및 차량 정보 등 프라이버시의 불필요한 공개 금지

- 운전자의 신원은 보호되야 하나, 타 차량 신원은 인증되어야 하며, 프라이버시는 보호 되어야 하나, 긴급 상황 시 추적이 가능해야 하는 등, 적용 시 상충되는 고려사항 존재

■ **V2V(Vehicle to Vehicle) 적용 시 고려사항**

고려사항	항목	설명
보안성	**인증 (Authentication)**	- 전송된 메시지가 정당한 사용자로부터 생성된 메시지임을 검증해야 함 (무결성, 부인방지 기밀성)
	재생공격(replay attack) 방지	- 메시지를 탈취하여 재전송하는 네트워크 혼란을 야기하는 재생공격을 방지해야 함
프라이버시	**추적성(Traceability)**	- 사고등 분쟁발생 시 차량의 실제 ID 추적가능
	익명성(Anonymity)	- 차량통신시스템은 개인정보에 접근하면 안됨
네트워크	**가용성(Availability)**	- 암호연산 및 통신 오버헤드가 정상적인 V2V 서비스를 저해하면 안됨
	다이버시티 (Diversity)	- 신뢰성 있는 통신링크를 제공하기 위해서 다이버시티 기법의 적용

- V2 의 성공적 적용을 위해서는 보안과 프라이버시측면 이외에도 아래와 같은 선결과제가 존재함
- 폐지목록(Revocation List) 관리로 인해 불필요한 많은 자원을 소모하는 문제점 해결
- 상호인증 및 메시지의 서명과 검증에 많은 시간이 소모되어 효율성 저하되는 부분에 대한 해결

"끝"

■ [참고] 프라이버시를 보장하는 V2V 인증기법 비교

구분	V2V 인증		N/W Infra 기반 V2V인증		
인증기법	GSIS	Calandriello 등의 기법	TSVC	IBV	RAISE
내용	-그룹서명 사용	-그룹서명 사용 -Pseudonym 사용 -Pseudonym 최적화	-변형된 TESLA사용	-익명 ID-기반 서명 -Batch Verification -익명 ID를 RSU가 발급	-RSU가 인증대행
장점	-RSU와의 추가적인 통신이 필요 없음	-RSU와의 추가적인 통신이 필요 없음 -Pseudonym 최적화로 최소의 그룹서명 사용	-연산 및 패킷 오버헤드 적음	-Batch Verification을 통해 연산효율 높임	-연산 오버헤드 거의 없음
단점	-높은 연산 오버헤드 -큰 메시지 크기	-비교적 높은 연산 오버헤드 -비교적 큰 메시지 크기	-추가적인 통신 필요 -인증 지연 문제 -RSU 공격에 취약	-추가적인 통신 필요 -RSU 공격에 취약	-추가적인 통신필요 -RSU 공격에 매우 취약

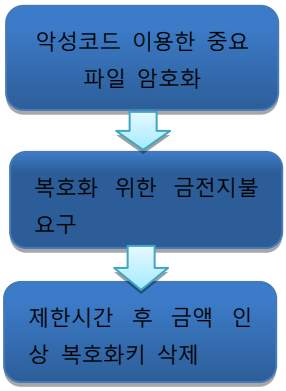
3	랜섬웨어, 파밍
문제	랜섬웨어(Ransom ware)와 파밍(Pharming)에 대해 설명하시오.
도메인	정보보안
정의	랜섬웨어: ransom(몸값)과 ware(제품)의 합성어로 컴퓨터 사용자의 문서를 '인질'로 잡고 돈을 요구한다는 악성코드 파밍: 합법적으로 소유하고 있던 사용자의 도메인을 탈취하거나 DNS 이름을 속여 사용자들이 진짜 사이트로 오인하도록 유도하여 개인 정보를 훔치는 해킹 기법
키워드	랜섬웨어: 악성코드, RSA-2048 알고리즘 암호화, 금전요구 파밍: 로컬 해킹(Host File), 도메인 탈취, DNS 서버 해킹
출제의도분석	최근 랜섬웨어, 파밍을 이용한 보안 사고 다수 발생
답안작성 전략	랜섬웨어와 파밍의 정의와 공격형태를 설명, 예방방법을 명시하여 고득점취득
참고문헌	KPC 모의고사(응용 44 회-1), [안랩][보안포커스]랜섬웨어 (2014.06)
풀이 기술사님	정상미 PE (제 101 회 정보관리/ jsm1111111@naver.com)

■ **랜섬웨어의 정의와 공격 형태**

가. 랜섬웨어(Ransom ware)의 정의

ransom(몸값)과 ware(제품)의 합성어로 컴퓨터 사용자의 문서를 RSA-2048 알고리즘으로 암호화하여 '인질'로 잡고 복호화키를 이용해 금전을 요구하는 형태의 악성코드

나. 랜섬웨어의 공격형태

공격 절차	설명
	1. 악성코드를 통한 DOC, PDF, JPG 등 다양한 확장자 파일을 RSA-2048 알고리즘으로 암호화. 2. 공격자는 파일을 정상화하기 위해 어떻게 해야 하는지 설명하고 돈을 지불하라고 유도 3. 제한시간을 정해두고 시간 내에 돈을 지불하지 않으면 금액을 인상하고. 복호화 키를 삭제해 영영 복구할 수 없게 한다는 메시지를 띄운다. 제한시간을 둬 사용자 불안감을 높임

■ **파밍의 정의와 공격 유형**

가. 파밍(Pharming)의 정의

합법적으로 소유하고 있던 사용자의 도메인을 탈취하거나 도메인 네임 시스템(DNS) 이름을 속여 사용자들이 진짜 사이트로 오인하도록 유도하여 개인 정보를 훔치는 해킹 기법

나. 파밍(Pharming)의 공격유형

구분	유형	설명
사용자 측면	로컬 해킹	사용자 PC 해킹, Host File 또는 DNS 서버 IP주소를 변경하여 파밍 사이트로 유도
공급자 측면	도메인 탈취	합법적으로 소요하고 있던 고객사의 도메인을 탈취하여 파밍 사이트로 유도
	DNS서버 해킹	DNS서버를 해킹, DNS 이름을 속여서 사용자들이 진짜 사이트로 오인하도록 유도

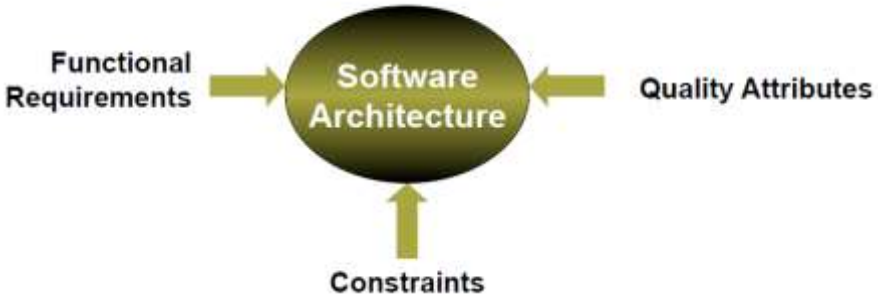
"끝"

4	소프트웨어 아키텍처 드라이버(Architecture Driver)
문제	소프트웨어 아키텍처 드라이버(Architecture Driver)에 대해 설명하시오.
도메인	소프트웨어 공학
정의	기능적 요구사항, 비 기능적 요구사항 중에서, SW 아키텍처에 영향을 주는 요구사항
키워드	아키텍처에 포함될 Functional Requirements, Constraints, Quality Attributes
출제의도분석	소프트웨어 아키텍처에서 유일하게 출제가 안된 항목
답안작성 전략	1 교시형 전형적인 답안 작성
참고문헌	http://www.nasa.gov/pdf/637608main_day_2-david_garlan.pdf http://www.ivifoundation.org
풀이 기술사님	강정배 PE (제 78 회 정보관리/ kangjungbae@naver.com)

■ **소프트웨어 아키텍처 드라이버(Architecture Driver) 정의**

소프트웨어 요구사항을 수행하는 기능적(functional), 품질적, 성능에 영향을 주는 속성(quality attributes, 서비스(업무적) 요구사항 중에서, 아키텍처 구성에 영향을 주는 항목 혹은 요구사항을 말함.

■ **소프트웨어 아키텍처 드라이버(Architecture Driver) 개념도**

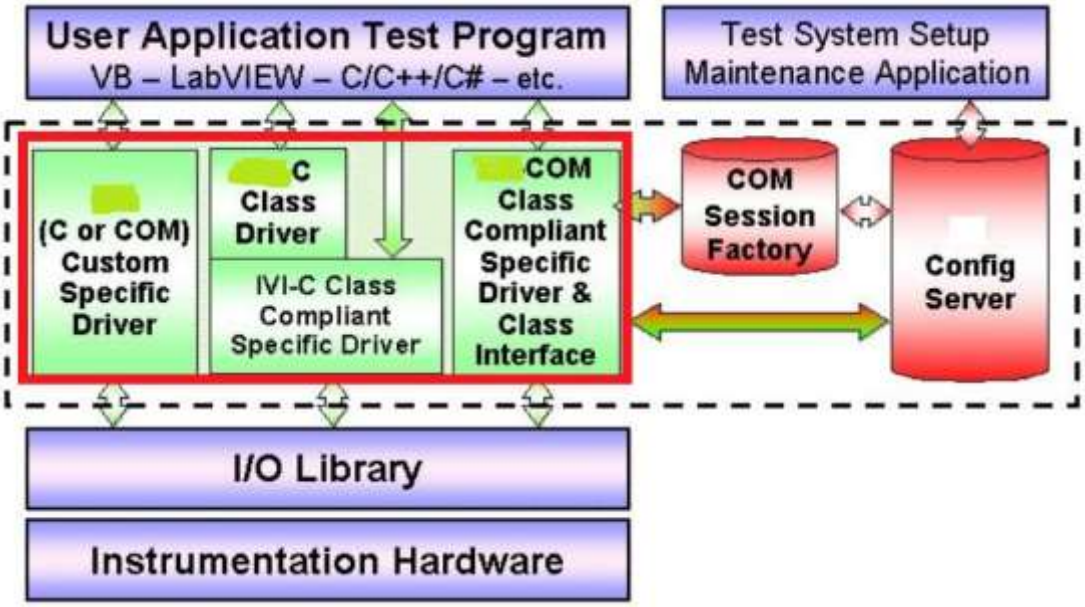


- 소프트웨어 아키텍처를 만드는데, 영향을 주는 요구사항을 소프트웨어 아키텍처 드라이버라고 함.

■ **아키텍처 드라이버 목록**

드라이브 목록	설명
Functional Requirements	시스템이 수행해야 하는 기능을 말함 보통 기능적 요구사항을 말하지만, 비기능적 요구사항도 같이 포함됨
Constraints	제약사항 – 시스템과 레거시(Legacy) 시스템에 영향을 주는 즉, 사전에 고려해야 되는 제약적인 요구사항
Quality Attributes	품질속성 – 기능적 요구사항 외에 품질 및 성능, 안정성 등 수행해야 하는 품질적 고려사항

■ **아키텍처 드라이버 구성 사례**



- 프로젝트, SW 의 품질, 기능적 요구사항 처리를 위한 소프트웨어 아키텍처 드라이버를 아키텍처에 반영한 개념도

[그림] SW 아키텍처 드라이버 위치 사례(위 붉은선 부분 참조)

"끝"

5	데브옵스(DevOps)
문제	데브옵스(DevOps)의 최근동향과 전망에 대해 설명하시오.
도메인	소프트웨어 공학
정의	개발과 운영 간의 상호 작용을 원활하게 하는 개발 방법론
키워드	프로세스 흐름(flow), 지속적인 피드백(Feedback), 끊임없는 학습(Learning)
출제의도분석	최근 애자일과 함께 급부상하고 있는 데브옵스에 대한 수험자의 지식을 알아보고 최근 동향에 대한 인지를 알아보기 위하여 출제
답안작성 전략	데브옵스의 간략한 개념을 설명의 최근동향과 앞으로의 전망을 기술사적 관점에서 제시하여 서술
참고문헌	스마트 기업의 DevOps 활용 (http://www.pinterest.com/pin/339178034176333360/) 엔터프라이즈 데브옵스(DevOps) (http://devopskr.blogspot.kr/2013/09/devops.html) 동향 브리핑 DevOps 관련 (정보통신산업진흥센터, NIPA)
풀이 기술사님	임항섭 PE (제 102 회 정보관리/ reo_dica@naver.com)

■ 데브옵스(DevOps)의 개념

- 소프트웨어 개발자들과 IT 종사자들 사이의 의사소통 , 협업 , 융합을 강조한 소프트웨어 개발 방법론이며 , 소프트웨어 개발과 IT 운영간의 상호 의존관계에 대한 산물
- 조직에서 소프트웨어 상품과 서비스를 신속히 생산하는 개발 방법론

■ 데브옵스(DevOps)의 최근 동향

가. 데브옵스의 변화 동향

- 별도로 분리된 채 Release 로 연결되어 온 DevOps 가 하나로 융화되어 지속적인 딜리버리와 지속적인 피드백을 통해 진화하고 있으며, 전체를 하나의 프로세스로 인식해 가고 있음.

나. 데브옵스와 주변 기술의 융합 동향

측면	설명
클라우드컴퓨팅과 DevOps	-고객에게 빠른 서비스 제공 및 변화 관리를 위하여 DevOps 가 도입되고 있으며 안정적이고 빠른 배포를 위한 자동화 솔루션이 도입중
모바일과 DevOps	-모바일 어플리케이션의 생명주기가 짧아지고 있음에 따라 빠른 어플리케이션 출시 및 배포를 위해 어플리케이션과 DevOps 를 결합한 앱옵스(AppOps)라는 방법론이 등장하고 있음
애자일과 DevOps 공존	-신속하고 빠르게 고객의 요구사항을 수렴하여 개발하는 애자일 방법론에 DevOps 가 결합되어 빠른 배포 및 지속적 릴리즈를 가능하게 하고 상호 보완적으로 결합되어 고 품질의 서비스 제공이 가능함
보안과	-빠른 배포 및 지속적 릴리즈를 목표로 하는 DevOps 에서 보안적인 요

DevOps	소가 상대적으로 간과되고 있으므로 이를 보완하기 위한 보안 자동화 툴의 적용이 고려되고 있음

■ **데브옵스(DevOps)의 전망**

구분	설명
기술적 측면	-지속적인 배포와 릴리즈를 위한 자동화 솔루션의 도입이 필요 -어플리케이션 개발 시 보안적 취약점에 대한 자동화 툴 도입 필요
관리적 측면	-효율적인 DevOps 도입 위한 정량적 측정 지표 개발 -지표에 대한 평가 및 보완할 수 있는 방안의 모색 필요
정책적 측면	-개발팀과 운영팀을 유기적으로 연계하여 프로세스를 실행할 수 있는 기업 전략이 요구되며, 이를 개발하고 구성원에게 교육이 필요함

- 어플리케이션의 생명주기가 짧아짐에 따른 빠른 배포를 위한 데브옵스가 확산될 전망
- 데브옵스는 프로세스 측면을 강조하므로 이를 지원할 도구와 체계확립이 필요함

"끝"

6	보안위협
문제	기관 내부자에 의해 행해지는 보안위협의 주요 행동적 특성을 설명하시오.
도메인	정보보안
정의	조직 내 정규직원, 계약직원, 아웃소싱 직원 등이 현재 또는 과거에 있었던 조직 내의 시스템, 네트워크, 데이터 등에 대한 접근권한을 의도적으로 오남용하여 조직 내 정보시스템의 기밀성, 무결성, 가용성을 해치는 위협
키워드	IT Sabotage, 금전취득을 노린 절취/변조, 사업이득을 노린 절취/변조
출제의도분석	정보침해원인에 내부자 위협이 높은 순위를 차지하고 있음
답안작성 전략	행동적 유형과 특징을 구체적 접근, 통제 방안을 추가
참고문헌	KPC 모의고사(관리 35 회-3)
풀이 기술사님	정상미 PE (제 101 회 정보관리/ jsm1111111@naver.com)

■ **내부자 위협에 의한 보안위협**

- 조직 내 정규직원, 계약직원, 아웃소싱 직원 등이 현재 또는 과거에 있었던 조직 내의 시스템, 네트워크, 데이터 등에 대한 접근권한을 의도적으로 오남용하여 조직 내 정보시스템의 기밀성, 무결성, 가용성을 해치는 위협

■ **내부자에 의한 보안 위협의 행동적 특징**

가. 내부자에 의한 보안 위협의 행동적 유형

구분	설명
IT Sabotage	- 내부자가 자신의 권한을 오남용하여 조직 내 시스템, 데이터 등에 위해를 가하는 행위
금전취득을 노린 절취 또는 변조	- 내부자가 자신의 권한을 오남용하여 금전취득이 가능한 고객정보 등을 절취하거나 변조 하는 행위
사업이득을 노린 절취 또는 변조	- 내부자가 자신의 권한을 오남용하여 사업적 이득을 위해 지적 재산 정보 등을 절취하거나 변조하는 행위

나. 내부자에 의한 보안 위협의 행동적 특징

구분	IT Sabotage	금전취득을 노린 절취 또는 변조	사업이득을 노린 절취 또는 변조
전, 현직	전직	현직	현직
직책	시스템/ DB 관리자	현업 담당자	영업 직원
방법	임의의 불법 계정을 통해 원격 접근 방식	적법한 시스템 접근 방식(인가된 방식)	적법한 시스템 접근 방식(인가된 방식)
목표	시스템, 네트워크, 데이터	고객정보	지적 재산 정보
장소/시간	근무 시간 외 원격접근	근무 시간 직장	근무 시간 직장
피해	시스템, 네트워크 다운, 중요 정보 삭제	금전적 배상, 대외 신뢰도 하락	사업 경쟁력 약화

■ **내부자에 의한 보안 위협 통제 방안**

- 기술적 방안: DRM, DLP 시스템 통한 내부 정보 유출 방지 강화, 내부자 행위 모니터링 강화
- 물리적 방안: 전산실 출입 통제 강화, 노트북 이동장비 반/출입 통제 강화, 전산실 CCTV 설치
- 관리적 방안: 비밀번호 공유 정책 강화, 내부 감사, 상시 점검 강화, 보안 대응 계획 수립, 훈련

"끝"

7	UNIX 파일 접근제어(Access control) 메커니즘
문제	UNIX 에서 적용되고 있는 파일 접근제어(Access Control) 메커니즘을 설명하시오.
도메인	컴퓨터구조/운영체제
정의	UNIX 파일 접근 제어를 위한 접근 권한 유형과 접근 모드
키워드	접근 권한 유형 user, group, other 와 접근 모드 read(r), write(w), execute(x)
출제의도분석	UNIX 계열의 파일 접근제어를 위한 접근 권한 유형과 접근 모드에대해 알고 있는지에 대한 기본 문제
답안작성 전략	UNIX 기반 파일시스템에 대한 기본 개요, 파일의 유형, 접근 제어 페커니즘 (접근 권한 유형과 접근 모드), 접근제어 변경 및 설정 메커니즘
참고문헌	Understanding Linux Kernel (O'Reilly)
풀이 기술사님	송영호 PE (제 102 회 컴퓨터시스템응용/ songyoungho@hanmail.net)

■ **UNIX 파일 시스템의 개요**

- UNIX 파일시스템은 트리로 구성되어 루트디렉토리(/)로 부터 각 하위 노드에 dev, home, bin, usr 등 시스템에 필요한 디렉토리와 일련의 바이트로 구성된 정보를 지닌 파일로 구성되어 있다.

■ **UNIX 파일의 유형**

유형	설명
정규파일	모든 UNIX 파일시스템의 구성요소로 일반적인 파일을 명시
심볼릭링크	실제 파일에대한 소프트링크나 하드링크로 구성된 링크파일
장치파일	블록 장치나, 문자 장치등에 해당하는 장치 파일
파이프	파이프(pipe)와 지정파이프(namedpipe 또는 FIFO 라고도 함)
소켓	프로세스간 통시을 위해 사용하는 특별한 파일

■ **UNIX 파일 접근 제어 메커니즘**

- 접근 권한 유형 (`설정 명령어: chown, chgrp)

접근권한	설명
User	파일을 사용하고있는 사용자 (owner)
Group	소유자를 제외하고 파일과 같은 그룹에 속해있는 모든 사용자 모임
Other	그밖의 사용자

- 파일 접근 모드 (설정 명령어: chmod)

Owner			Group			Other		
4	2	1	4	2	1	4	2	1
r	w	x	r	w	x	r	w	x

[파일 접근 권한 유형과 접근 모드]

- Read, Write, eXcute 로 파일을 읽거나(`r), 쓰거나(w), 실행(x) 할 수 있는 3 가지 모드로 구분함.
즉 파일이 'rwx' 모드를 지원한다면 그 파일을 읽고, 쓰고, 실행할 수 있다는 것을 의미.

■ **UNIX 파일 접근제어 변경 및 설정 메커니즘**

- r, w, x 세가지 권한은 각각 고유한 숫자값을 가지고 있으며, 2 진수로 각 사용자 유형에 해당하는 비트를 변경하여 파일 접근을 제어할 수 있다.

r : 4 (2 진수로 100), w: 2 (2 진수로 10), x: 1 (2 진수로 1) 즉, rwx 는 r+w+x = 4+2+1 = 7 (111)이 된다.

777 은, user, group, other 의 퍼미션을 모두 rwx rwx rwx 로 설정한다는 의미이다.

예를 들어, "#chmod 755 files" 라는 명령은 해당 파일에 대해 rwxr-xr-x 접근제어 권한을 설정한다.

"끝"

8	subnet 및 subnet mask
문제	subnet 및 subnet mask 인터넷에서 subnet 개념이 적용된 배경을 설명하고, subnet mask 255.255.255.224 인 네트워크를 예로 들어 subnet 을 설명하시오.
도메인	디지털네트워크
정의	Sub-network 의 줄인 말로, 그룹에 속한 네트워크를 분리하여 독립 네트워크로 인식될 수 있는 네트워크
키워드	서브넷(subnet), 서브넷 마스크(subnet mask)
출제의도분석	Subnet 의 기본 개념 및 적용된 배경에 대한 이해와 실제 subnet mask 를 이용한 네트워크 망을 분리할 수 있는지에 대한 출제
답안작성 전략	서브넷과 서브넷 마스크의 개요, 배경을 설명하고, 제시된 서브넷 마스크를 이용하여 망을 분리한 후 할당 가능한 호스트의 숫자를 제시한다.
참고문헌	UNIX Network Programming (W. Richard Stevens)
풀이 기술사님	송영호 PE (제 102 회 컴퓨터시스템응용/ songyoungho@hanmail.net)

■ 서브넷(subnet)과 서브넷 마스크(subnet mask)의 개요

- 서브넷은 sub-network 의 줄인 말로 동일 그룹에 소속된 네트웍이지만 분리된 하나의 독립 네트워크로 인식될 수 있는 네트워크를 의미함.
- 일반적으로 하나의 서브넷은 하나의 지역, 하나의 조직내에 있는 모든 컴퓨터들을 나타내고, 여러 개의 서브넷으로 나뉘어진 특정 그룹이나 기관은 하나의 동일한 공유된 주소로 접속 될 수 있다.
- 한 기관의 고유 네트웍에 도착한 패킷은 서브넷 번호를 이용하여 조직 내부의 게이트웨이에서 다시 라우팅 될 수 있다. 이때 라우터는 서브넷 마스크라는 2 진 비트 마스크를 참조하여 선택된 비트를 통해 패킷을 하위 네트워크 그룹에 좀 더 빠르게 이동시킬 수 있다.

■ 서브넷 적용의 배경설명

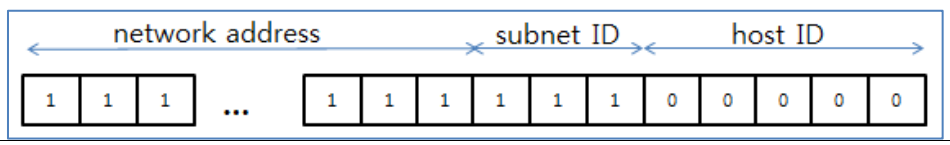
- 서브넷이 없다면, 전체 조직은 물리적으로 분리된 하위 조직의 서브네트웍마다 하나씩 여러곳에 인터넷 접속을 가지게 될 것이고 이로인해 한정된 량의 인터넷 주소가 낭비 될 수도 있게된다.

인터넷주소 절약	서브넷 마스크를 통한 하위 네트워크 구분, 인터넷 주소의 낭비를 억제
라우팅 속도개선	2 진 서브넷 마스크 비트를 참조한 빠른 패킷 전달

■ Subnet mask 255.255.255.224 인 네트워크의 subnet 설명

- IP 주소의 일부는 네트워크 번호를 나타내고, 일부는 호스트 주소를 나타낸다. 예를 들어 C 클래스의 경우 총 32 비트 중 24 비트가 네트워크 번호이고 8 비트가 호스트 주소이며 10 진수로 255.255.255.0 로 표기된다. 이것을 C 클래스의 기본 서브넷 마스크라 한다.
- 서브넷 마스크가 C 클래스의 255.255.255.224 라고 가정할 경우,

서브넷 마스크의 2 진수 값은 X.X.X.11100000 으로 모두 8 개(000, 001, 010, 011, 100, 101, 110, 111)의 서브네트워크로 구성되며, 각 서브 네트워크의 IP 주소 수는 32 개이다. 이때 네트워크 주소(0)와 브로드캐스트 주소(255)는 제외됨으로 서브 네트워크당 할당 가능한 호스트 수는 30 개가 된다.



[24-bit network address with 3-bit subnet ID and 5-bit host ID]

- 서브넷 마스크에 따른 서브넷 수 와 Host 수

이진수								십진수				
128	64	32	16	8	4	2	1	서브넷 마스크	서브넷 수	총 IP 수	제외 주소	Host 수
0	0	0	0	0	0	0	0	0	없음	256	2	254
1	0	0	0	0	0	0	0	128	2	128	2	126
1	1	1	0	0	0	0	0	224	8	32	2	30
:												
1	1	1	1	1	1	1	0	254	128	2	2	0
1	1	1	1	1	1	1	1	255	256	1	2	0

[subnet mask & number of hosts]

"끝"

9	기능성 게임(Serious Game)
문제	기능성 게임(Serious Game)의 개념과 응용분야에 대해 설명하시오.
도메인	디지털 서비스
정의	게임이 가진 순기능을 다양한 분야에 상호유기적으로 결합하여 상승효과를 기대하도록 디자인된 게임
키워드	순기능, 흥미유발, 재미, 과정 중시
출제의도분석	최근 다양한 분야에서 활용되고 있는 기능성 게임에 대한 개념과 각 분야에서의 실제 사례를 알고 있는지 검토하고자 출제
답안작성 전략	기능성 게임을 일반적인 게임과 다르게 충분히 개념 설명을 하고 다양한 응용분야에 대해서 충분히 설명
참고문헌	위키피디아(http://ko.wikipedia.org/wiki/기능성게임) 기능성게임 포탈(http://seriousgame.kocca.kr/seriousgame/main.do) 기능성게임 현황 및 활성화 방안 연구(한국콘텐츠진흥원, 2013 년 1 월)
풀이 기술사님	임항섭 PE (제 102 회 정보관리/ reo_dica@naver.com)

■ **기능성 게임(Serious)의 개념**

- 게임의 주요 목적인 오락성보다는 특정 목적성과 게임의 재미요소가 상호유기적으로 결합하여 상승효과를 기대하는 목적으로 디자인 된 게임

(클라크 앱트(Clark Abt)의 1977 년 저서 'Serious Game'에서 유래)

■ **기능성 게임(Serious)의 특징**

특징	설명
재미	게임이 가지고 있는 즐거움에 대한 효과를 학습에 접목
효과	다양한 사회적, 공공적 이익을 증진시키는 효과
과정 중시	결과만이 아닌 과정에서 얻게 되는 장점을 중시함

■ **기능성 게임의 응용분야**

분야	유형	설명	사례
의료	건강 관리	운동용 기구에 컴퓨터 게임요소를 더하여 운동과정의 성과를 게임으로 표현함으로써 운동의 효과를 높임	3DITeams
	질병 예방	질병의 중요성과 응급 대처방법을 알게 하는 예방용 게임	Re-Mission
교육	에듀게임	게임의 순기능을 이용하여 학습 향상을 도와주는 게임	한자마루
스포츠	스포츠게임	시간적, 공간적 제약을 벗어나 언제, 어디서나 스포츠를 즐길 수 있도록 제작된 기능성 게임	닌텐도 Wii 스포츠
교통	안전운전	안전운전에 대한 중요성을 강조하고 올바른 운전습관 효과	어린이 교통안전교육
공공	환경보호	다양한 사회적 의미를 갖춘 주제들과 국제분쟁이슈들을 게임을 통해 대중들에게 널리 알리고자 제작된 게임	에코프렌즈 푸드포스
국방	군사훈련	가상의 군사훈련을 통해 시뮬레이션을 통한 전략 습득	America's

		효과	Army

- 분야별로 다양한 기능성 게임이 존재하며 이중에서도 교육 분야에서 활용빈도가 가장 높음

■ **기능성 게임의 발전 방향**

방향	설명
인식 전환	게임이 단순 여가용의 기능에만 머물지 않고 교육, 스포츠, 의료, 국방, 공공의 분야에서 기능적으로 작용할 수 있다는 인식의 전환을 통해 게임의 순기능을 알리고 사회에도 발전적 효과를 이끌어 냄
부가가치 창출	미국에서는 2010 년에만 3 억 6,000 만 달러의 상업적 성공을 기록 국내에서도 2012 년 5,000 억 원 규모의 성장 가능성이 예상되면서 향후 10 년간 게임산업 중 가장 잠재력이 큰 분야로 예상

- 기능성 게임에 대한 긍정적 효과를 통해 인식 전환이 되며, 이를 통해 다양한 부가가치 창출

"끝"

10	드론(Drone)

문제	**드론(Drone)의 장점과 상용화 시 문제점에 대해 설명하시오.**
도메인	디지털서비스
정의	조종사 없이 무선전파로 유도하거나, 지상에서 원격으로 조정하는 무인항공기(UAV, Unmanned Aerial Vehicle)시스템
키워드	**UAV, 이동성, 확산성, 대체 노동성**
출제의도분석	미 연방항공청(FAA)가 무인기의 상업적 활용을 승인(2013)하는 등, 국제적인 무인기 상용화 적용사례가 증가하고 있고, 국내에서도 혁신 연구과제로 선정됨
답안작성 전략	드론의 정의 및 구성요소가 아닌, 드론의 장점과, 상용화 시 문제점에 집중하여 답안을 작성해야 함
참고문헌	- 드론(무인기, UAV) -KB 투자증권 - 신무기기술의 사용 및 국제인도법의 적용문제-이장희(한국외대)
풀이 기술사님	박상욱 PE (제 99 회 정보관리/ studygosu@gmail.com)

■ **드론(Drone)의 장점**

장점	설명	사례
이동성	- 교통 체증, 험한 지형등 사람이 접근하기 어려운 지역에 접근이 용이하여 임무수행 가능	항공촬영, 조난자 수색, 국경 및 우범지역 감시
확산성	- 다양한 센서를 활용한 다양한 산업 적용가능 - 군사용, 통신중계용, 배달용, 정보용 등 확산지속	3D(Dangerous, Dirty, Difficult) 분야 응용적용
대체 노동성	- 인간의 노동력 대체하는 방향으로 활용도 높음	저렴한 비용

- 국내: 산업기술혁신계획('14~'18)에서 4 대분야 13 개 대형융합 R&D 과제 중 6 개분야에 드론이 포함됨
- 국외: 구글의 '에어로스페이스', 아마존의 '프라임에어'등 산업 전반의 드론활용이 가속화됨
- 이러한 드론의 산업 전반의 상용화 시 해결해야 할 문제점 존재

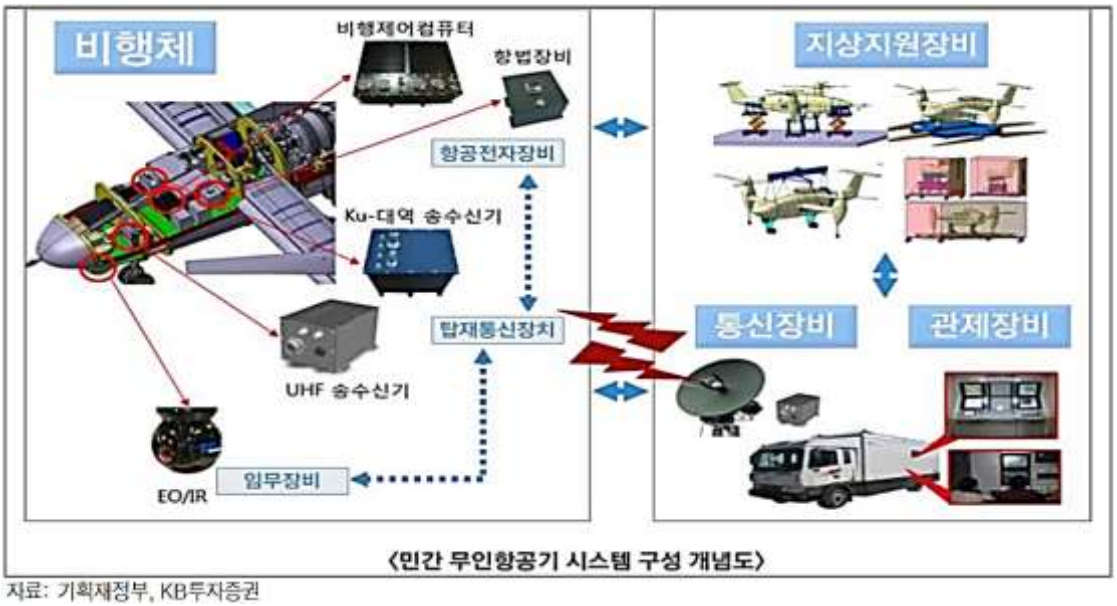
■ **드론(Drone)의 상용화 시 문제점**

문제점	설명	해결책 제안
법적 규제문제	- 미국의 경우 리모컨 기반 드론을 400 피트 상공에서만 비행하도록 제한하고 있음 - 국내의 경우 일부(산림, 측량, 농업 및 대여업)에만 사용을 허가하고 있음	- 가이드라인 마련 - 전용 주파수 분할
충돌, 추락 감시문제	- 드론의 충돌 및 추락에 따른 위험성 존재함	- TCAS(Traffic Collision Avoidance System) 의무탑재
사생활 침해문제	- 항공촬영을 통한 사생활 및 주요 정보 유출의 2 차피해 사례 속출	- 공역 규정 - 법적 장치 마련
해킹,보안 문제	- 드론의 GPS 를 조작하여 악의적 목적에 사용될 보안 위험 존재	- 비행 SW 에 특화된 보안기술 적용

- 미 연방항공청(FAA)는 2015 년 9 월까지 관련 규정개정 및 상업용 무인기 가이드라인 마련준비
- 한국 미래창조과학부는 2013~2022 까지 민간 무인항공기 실용화 기술 개발계획 수립

"끝"

■ **[참고] 드론의 구성도**



〈민간 무인항공기 시스템 구성 개념도〉

자료: 기획재정부, KB투자증권

■ [참고] 드론의 구성요소

구성 요소	내용
비행체	- 무인항공기의 기체(platform)를 말하며 기체에 실리는 추진 장치, 연료 장치, 전기 장치, 항법 전자 장치, 전기 장치 및 통신 장비 등을 포함
지상 통제 장치	- 임무 계획 수립과 비행체 및 임무 탑재체의 조종 명령, 통제 그리고 영상 및 데이터의 수신 등 무인항공기 운용을 위한 주 통제 장치
임무 탑재체	- 카메라, 합성구경 레이더(SAR), 통신 중계기, 무장 등의 임무 수행을 위해 비행체에 탑재되는 임무 장비
데이터 링크	- 비행체 상태의 정보, 비행체의 조종 통제, 임무 탑재체가 획득하거나 수행한 정보 등의 전달에 요구되는 비행체와 지상간의 무선 통신 요소
이착륙 장치	- 무인항공기가 지상으로부터 발사 및 이륙하고 착륙 및 회수하는 데 필요한 장치
지상 지원	- 무인항공기 시스템의 운용과 유지를 위해 소요되는 일련의 지상 지원 설비 및 인력 등을 총칭하는 말이며 무인항공기의 효율적인 운용에 필요한 분석, 정비, 교육 장비 시스템을 포함

자료: 월간로봇, KB투자증권

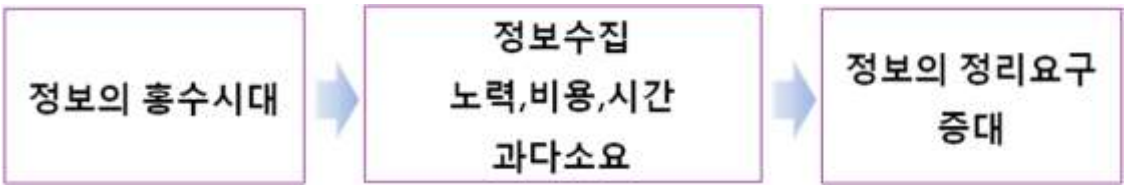
11 디지털 큐레이션(Digital Curation)

문제	디지털 큐레이션(Digital Curation)의 개념과 서비스 동향에 대해 설명하시오.
도메인	IT 경영전략 / Database
정의	데이터 홍수로부터 '선택적으로 골라서 사용자에 맞게 제공하는 행위'를 지칭하는 디지털 분야
키워드	정보 정리, 활용가치, 데이터 수집, 데이터 가공, 소셜 큐레이션 비교 등
출제의도분석	최근 디지털 큐레이션(Digital Curation) 동향 파악 문제
답안작성 전략	1 교시형 목차에 개념과 서비스 동향 타이틀로 답안 작성
참고문헌	http://cafe.naver.com/81th/29474 권갑진예비기술사님 자료
풀이 기술사님	강정배 PE (제 78 회 정보관리/ kangjungbae@naver.com)

■ **디지털 큐레이션(Digital Curation) 개념**

- 디지털 자원을 제공, 보존, 유지, 수집, 아카이빙하는 것을 지칭하며. 넓게 보면 현재와 장래에 이용될 신뢰할 수 있는 디지털 정보를 유지하고, 가치를 부여하는 행위.

■ **디지털 큐레이션(Digital Curation) 필요성**



- 소프트웨어 아키텍처를 만드는데, 영향을 주는 요구사항을 소프트웨어 아키텍처 드라이버라고 함.

■ **디지털 큐레이션(Digital Curation) 서비스 동향**

드라이브 목록	설명
핀터레스트 http://www.pinterest.com	- 미국에서 서비스를 시작하여 전세계로 서비스가 확대되고 있는 소셜 큐레이션 서비스이다. 액티브 유저가 2,000 만명이 넘는 서비스로서 웹서핑 중에 마음에 드는 이미지를 큐레이션해서 정리하여 다른 사람과 공유하고 전달 - 서비스로 장르적으론 스크랩류의 형태로 분석 할 수 있음
모바일 뉴스 신디케이션 서비스 (플립보드)	 SNS 계정을 연동하여 제공 받은 데이터를 모바일 매거진처럼 예쁘게 전환하는 서비스
아이엠데이 (Iamday)	IT 블로거들이 선별해 제공하는 큐레이션 뉴스 서비스와 SNS, URL, 동영상 큐레이션 기능을 이용해 대화하는 신개념 커뮤니티 서비스, 초심자도 외부에 널려있는 정보를 URL 과 다양한 큐레이션 기능을 이용해 제공 할 수 있고, 댓글도 URL 기반으로 작성 할 수 있음

12	BaaS(Backend as a Service)

문제	BaaS(Backend as a Service)의 개념과 기능에 대해 설명하시오.
도메인	디지털서비스
정의	모바일 응용 프로그램에서 API 를 써 호출하는 서버 측 코드를 작성하지 않고도 클라우드와 연동해 모바일 응용 프로그램을 효율적으로 개발할 수 있는 환경을 제공하는 서비스
키워드	API, 데이터저장소, 사용자관리, Location, 소셜인증, 빌링
출제의도분석	관심도가 높은 클라우드 서비스의 하나 가트너에서 Cloud Moblie Back-End Services 확대 전망
답안작성 전략	Baas 의 구조와 제공 서비스를 도식화, 표로 기술
참고문헌	모바일 앱개발자를 위한 클라우드서비스(2013 스마트앱 개발자포럼)
풀이 기술사님	유용희 PE (제 98 회 컴퓨터시스템응용/ yhinfuture@gmail.com)

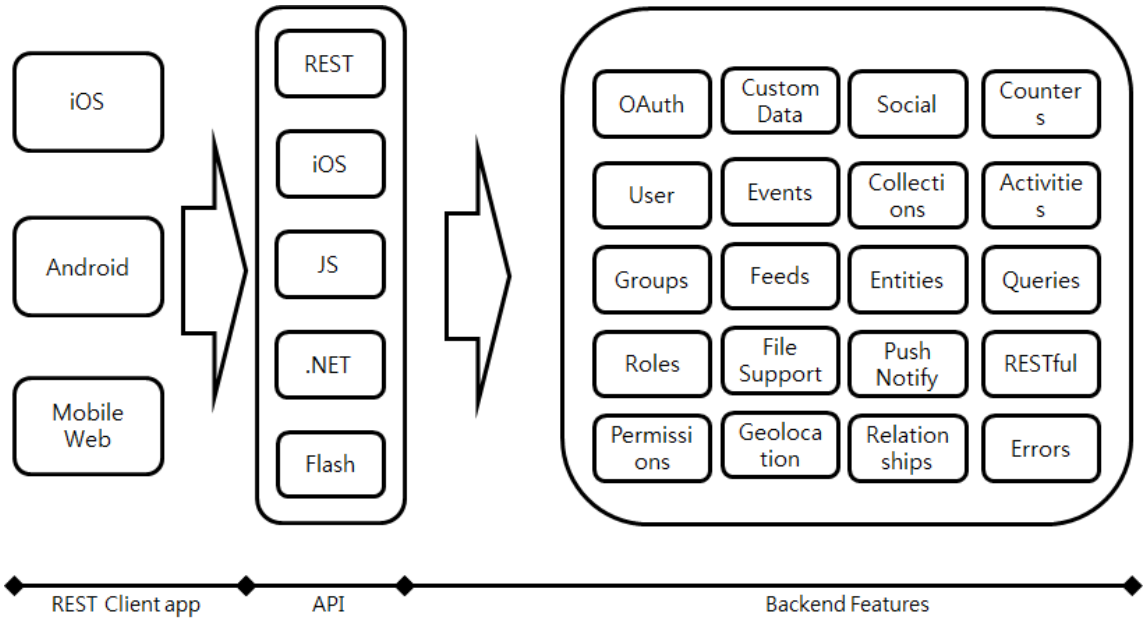
■ **BaaS 의 정의**

- 모바일 앱 개발시 자주 사용하는 백엔드 기능을 표준화(추상화)하여 API 로 제공
- 모바일 응용 프로그램에서 API 를 써 호출하는 서버 측 코드를 작성하지 않고도 클라우드와 연동해 모바일 응용 프로그램을 효율적으로 개발할 수 있는 환경을 제공하는 서비스

■ **BaaS 의 특징**

- 모바일 서비스 기반: 다양한 서비스가 이루어지는 모바일 앱, 웹에 특화된 클라우드 서비스
- 확장성: IaaS 기반, NoSql 채택
- 공유(Multi-Tenant): 여러 백엔드 앱이 같은 리소스 활용
- 과금: API 호출수, User 수, 용량에 따라 사용한 만큼 과금

■ **BaaS 개념도**



■ **BaaS 의 주요 기능**

기능	설명
데이터 저장소	API 방식으로 데이터 저장 인프라를 활용할 수 있으며, 다양한 유형의 데이터를 관리, 저장, 활용할 수 있는 기반 제공
푸시	특정 디바이스에 메시지를 전송하는 기능, Notification 애플의 APNS, 구글의 GCM 연계 인프라 제공
사용자관리	OAuth 기반의 사용자 인증, 등록, 권한 관리하는 기법 제공 역할과 권한 기반의 보안 체계 제공, 엑세스 제어, 자체인증 제공
소셜인증	회원간의 소셜 서비스 연계, 콘텐츠의 소셜 배포, 공유 지원
Location 연계	모바일 기기의 위치 정보와 이른 연계하는 GIS 정보 및 응용 기술 제공
빌링	API 요청 수, 파일 용량, 푸시 등 사용한 용량을 관리하고 과금 할 수 있는 정산 시스템 구성

"끝"

13 커넥티드카(Connected Car)

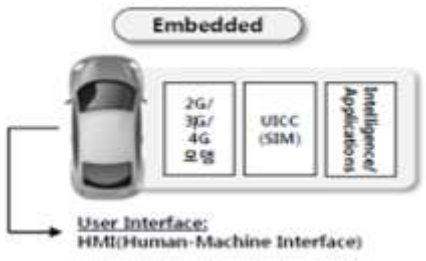
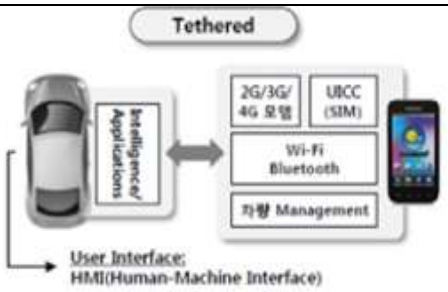
문제	커넥티드카(Connected Car)의 개념과 분류에 대해 설명하시오.
도메인	디지털 서비스
정의	통신망을 연결하여 차량을 정보화 기기로 활용할 수 있도록 제공하는 자동차
키워드	연결성(Connectivity), 임베디드, 테더드, 통합 방식
출제의도분석	차량을 통해 다양한 서비스를 제공하는 커넥티드 카가 주목되고 있으며, 이에 대한 명확한 개념과 연결방식 별 유형에 대해 학습 여부를 확인하고자 출제
답안작성 전략	커텍티드 카의 개념을 그림을 통해 명확하게 설명하고 연결방식 별 유형에 대해 명확한 차이점을 중심으로 충분하게 설명, 업체별 주요 동향을 3 단락에 제시한다면 가산점 예상
참고문헌	'커넥티드 카' 차세대 자동차 핵심 부상(http://www.etnews.com/20140220000039) 커넥티드 카의 서비스 동향 분석(ICT 기획 시리즈, 김선영 KT 경제연구소 연구원)
풀이 기술사님	임항섭 PE (제 102 회 정보관리/ reo_dica@naver.com)

■ **커넥티드 카(Connected Car)의 개념**

개념도	개념
	-통신망을 연결해 차량 자체를 정보기술(IT) 기기처럼 활용할 수 있는 자동차 -차량 연결성을 기반으로 자동차에 네트워크 기능을 탑재하여 실시간 네비게이션, 원격 차량제어 및 관리 서비스 뿐만 아니라 이메일, 멀티미이디어 스트리밍 등 엔터테인먼트 서비스를 지원하는 자동차

- 자동차가 커넥티드 디바이스로 진화하는 것으로 '바퀴달린 스마트폰'이라 불림

■ **커넥티드 카의 분류**

분류	구성도	설명
임베디드 (Embedded)		-정보처리와 통신 접속 기능을 모두 차량에 설치한 방식 초기하드웨어와 솔루션 비용이 -높지만, 끊김없는(Seamless) 사용자 경험을 제공 -안전성과 보안성이 높음
테더드 (Tethered)		-정보처리 기능을 갖춘 자동차로 휴대전화 테더링을 통해 네트워크에 접속하는 방식 -끊김없는 서비스 제공에 한계가 있을 수 있으나, 서비스 요금 부과가 용이함

통합 (Integrated)		-자동차에 스마트폰을 도킹(Docking)해 통신 접속과 정보처리 기능을 스마트폰에 의존하는 방식 -개인화된 컨텐츠를 제공함으로써 운전자에게 다양한 인포테인먼트 옵션을 제공함

- 커넥티드 카는 네트워크 연결방식에 따라 3 가지의 유형으로 분류됨

■ 커넥티드 카 서비스 업체별 주요 동향

업체 및 서비스		설명
GM	OnStar	-음성 통화, 네비게이션, 도난차량 소재파악 기능 제공
Ford	Sync AppLink	-블루투스나 USB 를 통해 스마트폰이나 MP3 플레이어 등을 연결하고 음성을 통해 조작하는 인터페이스 제공
Chrysler	U-Connect Touch	-911call, 원격 시동 및 도어락/언락, Wifi 핫스팟, 음성인식 기능을 탑재하고 터치스크린 인터페이스 제공
현대차	BlueLink	-운전자에게 실시간으로 날씨 정보, 음성으로 문자메시지 전송 및 차량 문 개폐, 시동 서비스 제공
기아차	UVO	음성인식으로 라디오오디오 기기 작동(MS 공동개발)
르노 삼성	모바일 텔레메틱스	-SKT 와 모바일 텔레메틱스 공동 개발, 네비게이션과 원격 제어, 도난방지 및 긴급 구조 서비스 제공

- 자동차 제조사 및 각 통신사에서 다양한 커넥티드 카 서비스를 운전자에게 제공

"끝"

1	전산통합센터
문제	A 기업 전국 단위 전산통합센터 구축/운영 시 업무중단 최소화를 위해, 전국 전산실 현황을 고려한 환경변수 사전 처리 방안
도메인	경영전략
정의	정보시스템의 효율적 관리 운영을 위한 산재된 정보시스템을 통합관리하는 통합전산센터
키워드	환경변수 사전 처리 방안, 단계별 이전, 테스트베드 활용, 데이터검증 체계
출제의도분석	공공기관의 지방이전 등과 맞물려 효과적인 전산통합센터 구축/운영과 관련된 이슈에 대한 문제해결 역량 요구
답안작성 전략	전산통합센터 구축/운영에 대한 실무적 문제해결 능력 표현
참고문헌	정부통합전산센터 구축사업 사업개요서
모범목차	1. 전산통합센터 구축/운영을 위한 A 기업의 전산실 현황 분석 2. 산재된 정보자원의 전산통합센터 이전 시 업무중단 최소화 방안 가. 전국단위 전산통합센터의 구축/운영을 위한 요구사항 나. 전산통합센터로의 전산실 이전 시 업무중단 최소화 방안 - 각 지점의 전산실 현황을 고려한 환경변수의 사전 처리가 가장 중요 3. 전국 전산실 현황을 고려한 환경변수 사전 처리 방안 가. 전국 전산실 현황을 고려한 환경변수 도출 나. 도출 된 환경변수 별 세부 처리 방안
풀이 기술사님	권혁재 PE (제 102 회 정보관리/ star10ve@naver.com)

■ **A 기업 전산실 현황**

- 전국 지점의 전산실 별로 다른 유지보수 사업자가 운영 및 관리하고 있음
- 서버는 UNIX, Windows, Linux 등 다양한 OS 및 H/W 로 구성되어 있음
- 이전 시 전산통합센터에서 제공하는 환경변수를 적용하여야 함
- 이전은 하드웨어, 시스템 소프트웨어, 응용어플리케이션, 데이터를 대상으로 함

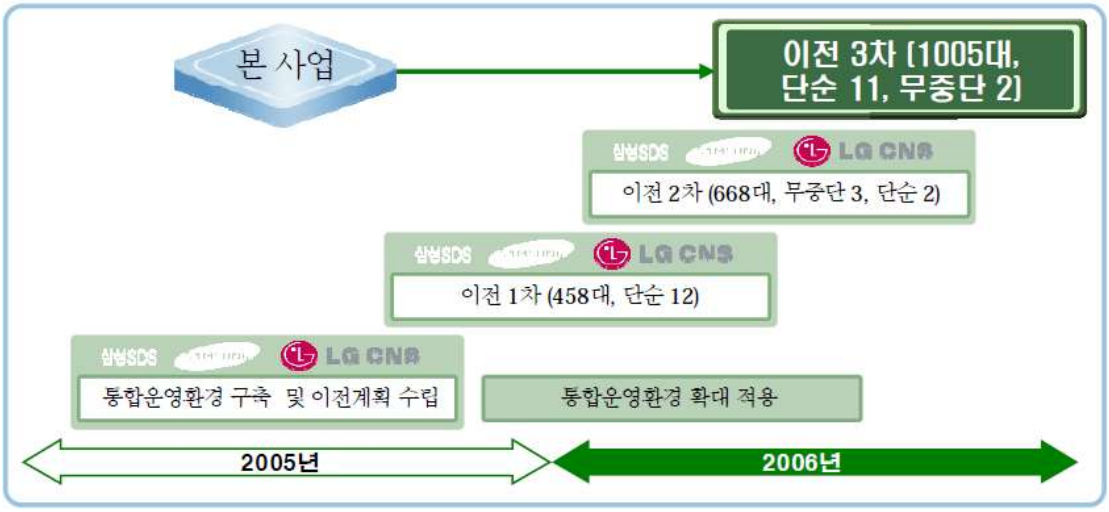
■ **전산통합센터 주요기능**

기능	내용	특징
시스템운영	서버, 스토리지, 네트워크, 보안장비 등 정보자원을 통합운영/관리	- ITIL 기반의 표준화/자동화된 시스템 통합운영 툴 개발/활용 - ISO20000 인증 획득
정보보호	외부의 물리적/사이버적 위협으로부터 정보시스템을 보호	ISMS 인증 획득
IT 자원관리	필요한 HW, 시스템 SW 등 IT 자원의 효과적 활용	클라우드 컴퓨팅 서비스 환경으로 전환
통합전산망	전용통신망 구성을 통한 각 지점 서비스 제공	SLA 에 기반한 서비스품질(QoS) 보장
IT 기반환경제공	시스템의 안정적인 가동을 보장하는 최적의 인프라 제공	지능형빌딩시스템, 출입보안시스템, 전력관리 시스템 등
업무연속성관리	재난 상황에 대비한 대비 체계 구축	BS25999 인증 획득

공통플랫폼관리	각 지점에서 공통으로 활용할 수 있는 모듈화된 공유 플랫폼 제공	검증된 표준환경 제공으로 효과적 서비스 개발을 지원
모바일지원	모든 지점에 일관된 모바일 업무 서비스 환경 제공	Mobile Service Life Cycle 관리

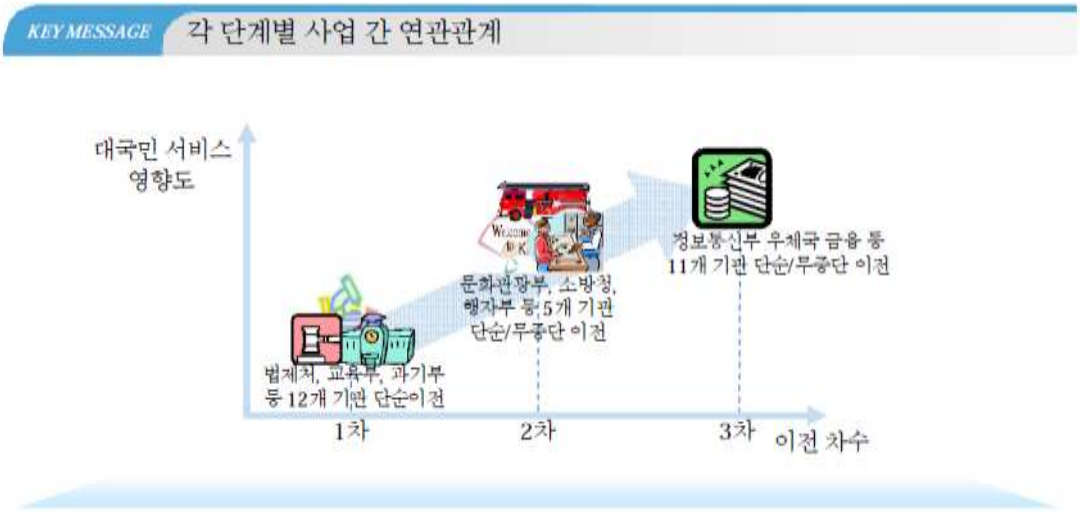
■ **전산센터 이전 시 업무중단 최소화 방안**

[참고 1] 정부 통합전산센터 단계별 이전 방안



- 이전 우선순위에 따라 1 차/2 차/3 차로, 업무 중단 시 영향도에 따라 단순이전/무중단이전으로 구분하여 단계별 이전

[참고 2] 정부 통합전산센터 단계별 이전 방안



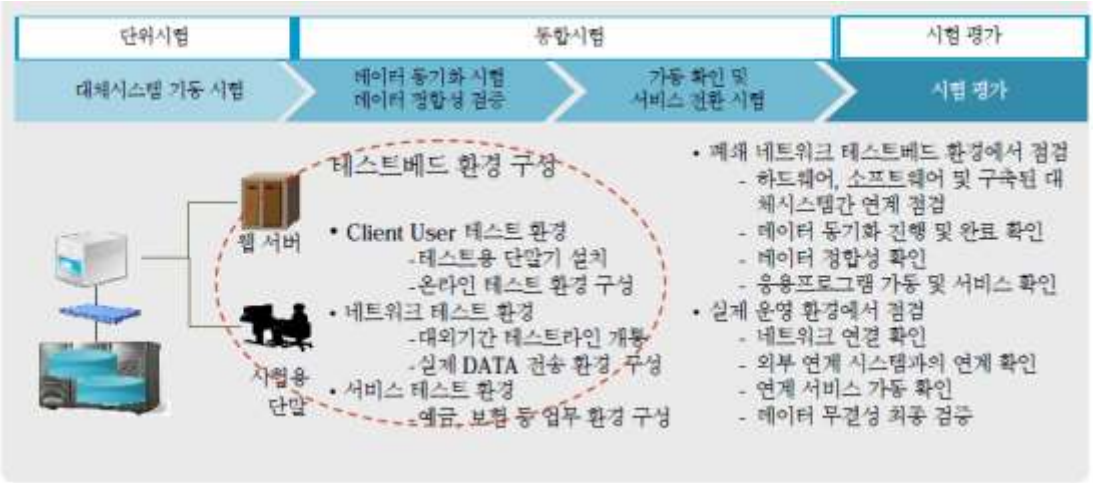
- 산재되어 있는 전산실(기관) 별 단계 및 이전 방향을 명확히 결정

■ **환경변수 사전 처리 방안**

구분	환경변수 내용	사례
하드웨어	- 서버(VM) Type, HA Group, 서버 용량 등	- WAS 서버/WEB 서버/DB 서버 - 함께 HA 구조로 묶일 VM 지정 - CPU 수/메모리 용량 등
시스템 소프트웨어	- OS Type, Middleware Type, 시스템 소프트웨어 세부 설정 등	- OS 형태(Windows/Linux 등) - 설치되어야 할 시스템 SW 지정 등
응용 어플리케이션	- 응용 어플리케이션 세부 설정 등	- 각 응용 어플리케이션의 세부 설정 사항
데이터	- 데이터 형태, 동기화 구조, 데이터 Size 등	- DB Type 등 데이터 관련 세부 설정 사항

- 산재되어 있는 모든 자원 형태 및 특성을 환경변수화 하여 전산통합센터의 시스템운영 및 IT 자원관리 기능 등을 통해 구축/운영 될 수 있도록 하는 것이 중요

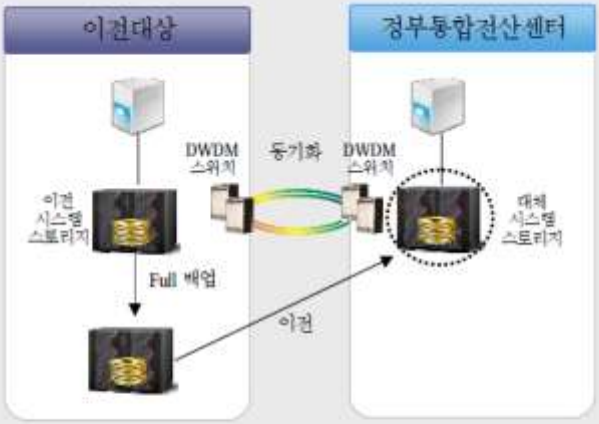
[참고 3] 테스트베드 활용 방안



- 데이터 센터 이전 단계별로 테스트 베드를 구축하여 충분한 테스트 진행 후 이전 수행

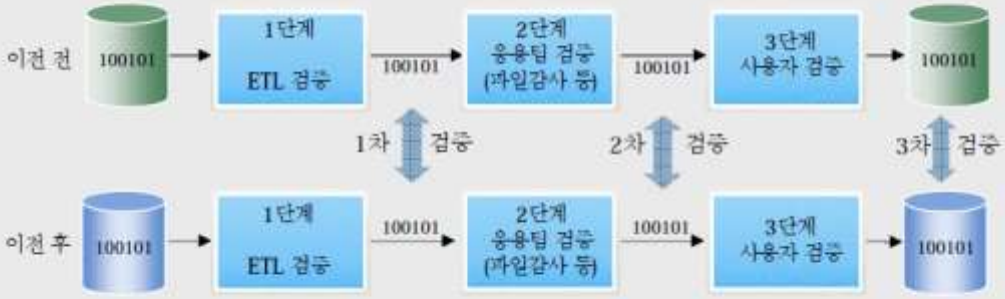
[참고 4] 데이터 무결성 보장을 위한 안정적 동기화와 3 중 검증체계

수행방안 직접 연결을 통한 안정적 데이터 동기화



- 이전대상 시스템에 스토리지를 직접 연결하여 데이터를 동기화 함으로써 기존의 네트워크를 통한 동기화에 비해
  - 동기화 시간을 단축
  - 동기화시에 오류 발생을 방지하여 안정적인 데이터 동기화 가능

수행방안 데이터 3중 검증 체계

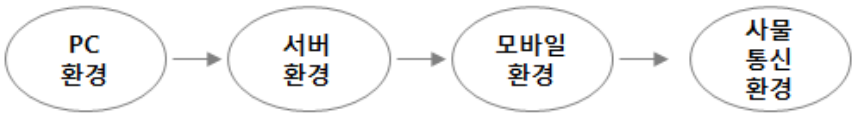


단계	1단계	2단계	3단계
확인방법	• 파일 개수 확인 • 볼륨사이즈 확인 • SQL 문 Query	• 배치 프로그램을 활용한 파일 감사 수행	• 온라인 화면을 통한 검증

2 스마트 데이터

문제	2. 스마트 데이터(Smart Data)에 대한 출현 배경, 3A, 빅 데이터와 스마트 데이터의 구분기준에 대해 설명하고, CQL(Continuous Query Language)에 대한 주요 기능, CQL 과 스마트 데이터와의 관계에 대해 설명하시오.
도메인	디지털 서비스
정의	스마트 데이터는 3A(Accurate, Actionable, Agile) 특성을 가진 품질이 확보된 데이터
키워드	3A(Accurate, Actionable, Agile)
출제의도분석	빅데이터와 공공데이터의 현 문제를 해결할 수 있는 스마트 데이터 개념 및 관련 기술을 알고 있는지 여부의 확인
답안작성 전략	빅데이터와 스마트 데이터의 정확한 개념 비교 및 CQL 에 대한 풍부한 기술
참고문헌	빅데이터의 진화: 스마트 데이터(2013,NIA) 초연결시대의 창조경제를 위한 스마트 데이터 전략(2013,NIA)
모범목차	1. 스마트 데이터에 대한 출현 배경 2. 스마트 데이터의 3A 특성 및 빅데이터와의 구분 기준 3. CQL 에 대한 주요기능 및 스마트데이터와의 관계
풀이 기술사님	김지영 PE (제 102 회 정보관리/ sayno9@naver.com)

■ **스마트 데이터에 대한 출현배경**

출현배경	설명
비즈니스 환경의 변화	- 기존의 전통산업과 공공영역이 ICT 융합을 통해 새로운 서비스, 솔루션, 서비스 창출이 빈번해 지는 사회로 전환
컴퓨팅 환경의 변화	 - 컴퓨팅 환경이 변화하면서 웹 환경, 네트워킹, 이동통신 환경 등 기술환경의 변화로 데이터 속성도 함께 변화
웹 환경의 변화	 - 사물통신 환경의 Web 4.0 의 지능형 웹을 기반으로 초연결 사회로 진화됨에 따라 스마트 데이터의 필요성 증대
데이터 환경의 변화	 - 현재의 빅데이터 보다 빠르고 민첩하게 실시간으로 데이터 분석이 필요하고 고품질의 분석 결과를 제공해야 하는 데이터 요구의 증대 - 3V 의 물리적 특징을 강조한 빅데이터에서 품질적 측면으로써 3A 특징을 가진 스마트한 데이터 필요함

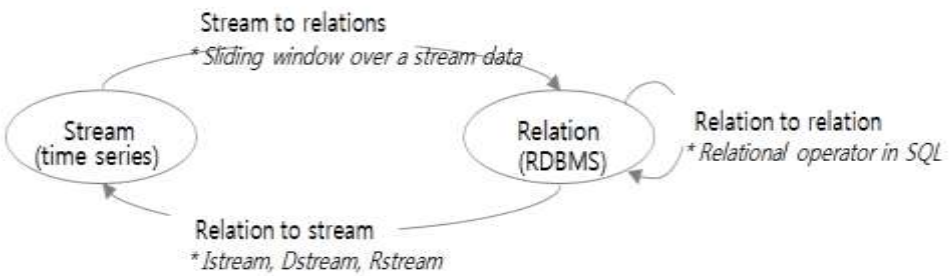
■ **스마트 데이터의 3A 특성**

3A 특성	개념	필수 조건
Accurate	데이터 분석의 정확성	빅데이터의 노이즈로부터 정확하고 양질의 정보를 전달할 수 있어야 함 지속적으로 유효성을 입증하여야 하며, 효과를 검증할 수 있는 사례 제공 필요
Actionable	데이터의 즉시 행동성	데이터를 활용해 의사결정이나 서비스를 마련 할 수 있는 정도의 행동성을 보유 해야 함
Agile	환경에 대한 데이터의 민첩성	급변하는 대내외적인 환경의 변화와 사회의 현안, 사물의 위험, 사람의 행동 변화등을 신속히 감지하고 정확히 분석하여 민첩하게 대응할 수 있어야 함

■ **빅데이터와 스마트 데이터의 구분기준**

구분기준	빅데이터	스마트데이터
관점	데이터의 물리적 특성 측면	데이터의 품질 측면
특징	3V 데이터 Volume-Velocity-Variety	3A 데이터 Accurate-Actionable-Agile
데이터 품질평가	빅 노이즈 발생에 대한 후속 프로세스 미흡	데이터 정확도에 관한 지속적 평가
데이터 활용	다양한 데이터의 수집, 축적, 공유, 분석	데이터의 통합, 사용의 편의성, 시맨틱 기반의 서비스 지향
기반 기술	Hadoop Eco System(HDFS, MapReduce, R .etc), NoSQL	LOD(Linked Open Data), 시맨틱 웹, 인공지능, IoT 기술
분석 기술	평판 분석, 소셜 네트워크 분석, Opinion Mining	상황인식 분석, 신경망 컴퓨팅, 인공지능, 자율학습
컴퓨팅 환경	모바일, 클라우드 환경 - 네트워크는 단순히 연결을 위한 수단	사물통신 환경 - 인터넷 전체가 하나의 거대한 지능형 컴퓨터
사회	정보화 사회, 지식사회, 모바일 사회	초연결 사회, 지능화 사회

■ **CQL(Continuous Query Language)에 대한 주요 기능**

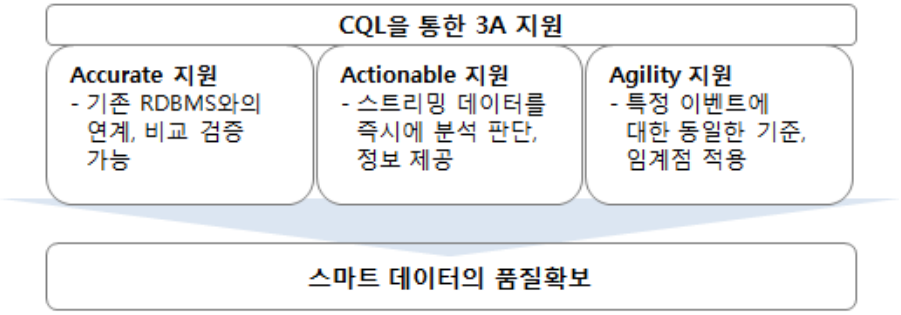


개념	SQL'99 를 기반한 언어로 테이블과는 다른 스트림 데이터에 질의할 수 있는 Continuous Query 확장이 추가된 언어로 스탠포드 대학 연구를 기초로 하고 있는 대용량 스트리밍 프로세싱 언어 예시) Highway System 에서 특정 구간에 최근 10 초간 지나간 차량의 평균 속도를 구하라

주요 기능	SQL 에서 스트림 질의, 지속적으로 입력되는 데이터에 대한 윈도우 단위처리, 스트림 패턴 분석	
Operation 기능	Relation to relation	릴레이션을 input 으로 릴레이션이 ouput 으로 나오는 연산 기능 기존 SQL 언어의 관계 연산자 사용
	Relation to stream	릴레이션을 input 으로 Stream 이 output 으로 나오는 연산 기능 Istream: Inserted, Dstream: Deleted, Rstream: updated
	Stream to relation	Stream 이 input 으로 릴레이션이 output 으로 나오는 연산 기능 스트림에 Sliding Window 사이즈 만큼의 데이터 튜플 집합 개념으로 연산

(참조) http://www.mathcs.emory.edu/~cheung/Courses/584-StreamDB/Syllabus/02-Systems/CQL.html

■ **CQL(Continuous Query Language)과 스마트 데이터와의 관계**



- CQL 을 통해 스마트 데이터의 주요 특성인 3A 를 지원함으로써 스마트 데이터의 품질확보 가능.

빅데이터에서 발생한 빅노이즈를 제거하고 데이터의 품질이 확보된 스마트 데이터로 이행하는 과정에서 CQL 은 필수적인 Query Language 로 사용될 것으로 예상됨.

"끝"

3 IPSec, VPN(Virtual Private Network) 구축

문제	범용적인 인터넷 보안 방법론인 IPSec 을 보안기능 중심으로 설명하고, VPN(Virtual Private Network) 구축에 IPSec 이 어떻게 사용되는지 설명하시오.
도메인	정보보안
정의	TCP/IP 프로토콜의 IP 계층에서 송신자의 인증을 허용하는 인증 헤더(AH, Authentication Header)와 기밀성(캡슐화를 통해)을 보장하는 ESP(Encapsulating Security Payload)를 이용한 IP 보안 프로토콜
키워드	터널링, 공중망, 가상 사설망, 전용회선 효과, 이동근무 지원, 암호화, IKE, AH, ESP
출제의도분석	현재까지 SSL VPN 으로 대부분 출제가 되었고, 시장은 IPSec 기반으로 많이 발전을 했기 때문에 출제될 가능성은 이미 있었음(뒤늦은 감 있는 필수 문제)
답안작성 전략	IPSec 기술과 VPN 서비스 연동
참고문헌	KPC 모의고사, 2013. 6 월 참조
모범목차	I. VPN 의 개념 및 특징 II. 보안기능 설명 주요 기술 III. VPN 구축에 IPSec 사용 절차 각각 목차 구성 적용 설명 IV. SSL VPN 과 IPSec VPN 비교
풀이 기술사님	강정배 PE (제 78 회 정보관리/ kangjungbae@naver.com)

■ **공중망에 보안과 QoS 를 제공하여 마치 사설망처럼 사용하는 VPN 개요**

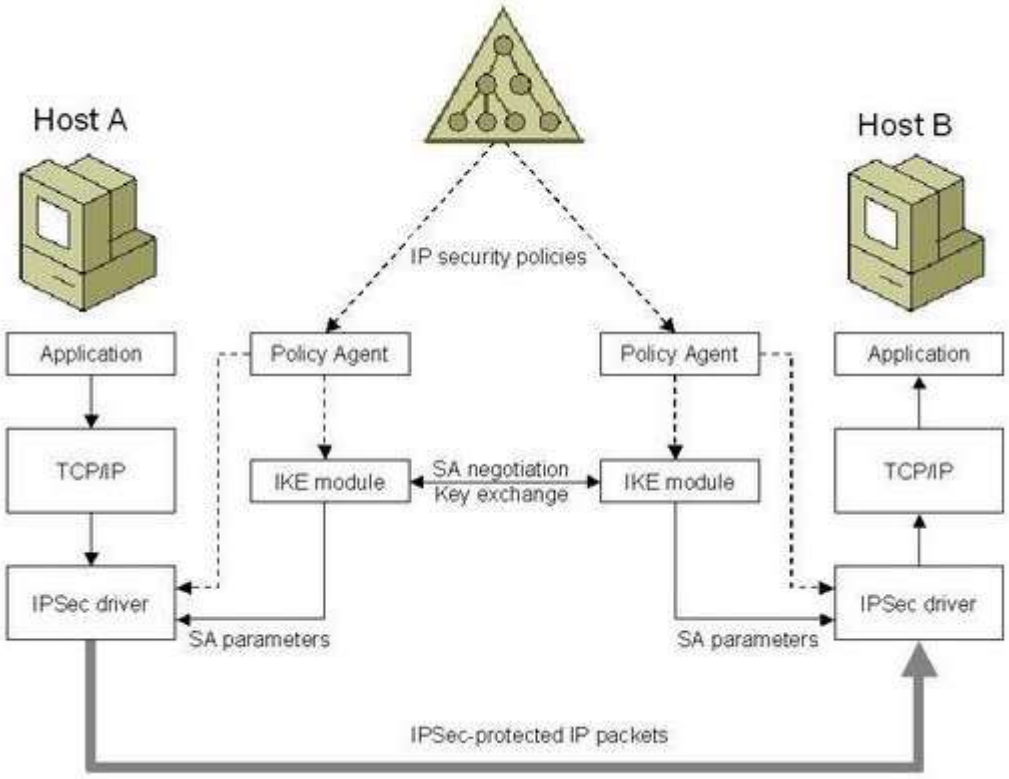
터널링(Tunneling) 기법을 사용해 공중망에 접속해 있는 두 네트워크 사이의 연결을 마치 전용회선을 이용해 연결한 것과 같은 효과를 내는 가상 네트워크.

■ **VPN 의 특징**

특징	설명
뛰어난 안정성	- IPSec VPN, SSL VPN 터널링 구성으로 안정성 제공 - Load-Balancing 기능 제공(회선장애 시 백업 기능 제공)
유연한 확장성	- 네트워크 증설 및 감속의 용이성 - 통합구성으로 인한 관리의 편리성
저렴한 구축비용	- 초고속망 기본 구성으로 인한 비용절감 - 본/지사 구축시 비용절감

■ **IPSec 를 통한 VPN 적용 개념도**

최근에는 SSL VPN 서비스와 거의 시장 점유율이 비슷할 정도로 상승하고 있는 추세를 가짐

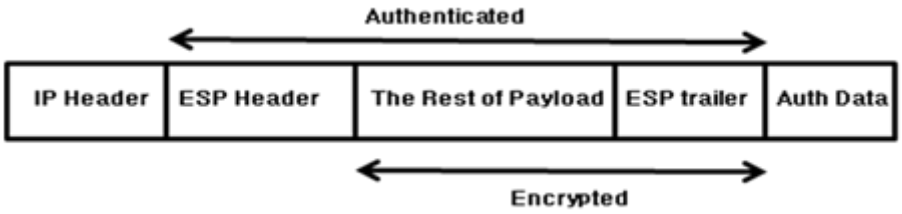


[그림] IPSec 를 통한 Host 사이의 VPN 적용 흐름도

- TCP/IP 프로토콜의 IP 계층에서 송신자의 인증을 허용하는 인증 헤더(AH, Authentication Header)와 기밀성(캡슐화를 통해)을 보장하는 ESP(Encapsulating Security Payload)를 이용한 IP 보안 서비스

■ **IPSec 보안 기능 중심 설명**

기능	설명
키 관리 메커니즘	- 보안 연관(SA, SA(Security Association) – 송, 수신자간 키교환, 인증, 암호화를 통한 협상 - Inbound 와 Outbounding 보안 연관을 생성하기 위하여 설계된 프로토콜로 IPSec 을 위한 SA(Security Association) 생성
보안 프로토콜	AH(Authentication Header) - IP 패킷을 인증하기 위해 필요한 정보를 포함하는 방법으로 데이터의 인증과 무결성을 보장해 주는 매커니즘 Original Frame: L2 | IP | L4 Payload Transport Mode: L2 | IP | ESP AH | L4 Payload Tunnel Mode: L2 | New IP | ESP AH | IP | L4 Payload

	 - 데이터의 기밀성과 무결성을 제공, IP 패킷의 인증, 프라이버시 제공 AH 프로토콜을 사용한 후에 설계되어 AH 기능에 추가 기능이 포함
IPSec 정책	**SPD(Security Policy Database)** 패킷에 대한 보안 정책을 적용하며, 모든 트래픽 처리 시에 참조 - SAD 를 이용하기 전에, 호스트 패킷에 대해 규정된 정책을 결정 **- 종류 : Drop(폐기), 통과(Bypass), 적용(Apply) 등** - SPD specifies the policies that determine the disposition of all IP traffic inbound or outbound from a host or a security gateway. **SAD(Security Authentication Database)** - 양단간의 비밀 데이터 교환을 위해 미리 설정되어야 할 보안 요소들에 대한 데이터 관리(-> AH, ESP 에 의해 서비스 됨) - SAD is a security association table, containing parameters that are associated with each security association.

■ **VPN(Virtual Private Network) 구축에 IPSec 이 어떻게 사용**

구축 절차	설명
IKE(Internet Key Exchange) Phase 정책 설정 (ISAKMP- Internet security association & key management protocol) **(준비 단계)**	**VPN 장비 간 인증 키 설정** - inbound 와 outbound 보안 연관을 생성하기 위하여 설계된 프로토콜로 IPSec 을 위한 **SA(Security Association)** 생성 - Key 를 주고 받는 알고리즘, 공개된 네트워크를 통하여 Key 를 어떻게 할 것 인가를 정의, IKE 교환을 위한 메시지를 전달하는 프로토콜 설정 **- ISAKMP(키교환, 인증을 위한 프레임워크, 메시지포멧),** SKEME(인증을 위한 공개키 암호화 기법), Oakley(Mode-based 메커니즘) 3 가지 방식 중 Oakley, SKEME 를 다포함하는 ISAKMP 를 주로 사용 - 통신 당사자가 서로 인증해서 암호 키를 교환하기 위한 통신 규약. IPSEC 의 일부로서 RFC 2408 에 규정되어 있으며, 구체적으로는 어떠한 인증 알고리즘, 암호화 기술, 암호 키 교환 규약을 사용할 것인지 등의 보안 수단을 상대방에게 알리기 위한 메시지 형식. **암호화 방식 지정** - 암호화를 설정하기 위한 AES 방식, SPN 방식, Hash 등 정책 설정
IPSec 정책 설정 (=IPSec 를 통한 접속 단계)	**VPN 으로 적용할 트래픽 지정 -> AH, ESP 방식 등 결정** **인증(AH)프로토콜** 데이터 무결성과 IP 패킷의 인증을 지원, 재생방지(anti-reply)

	서비스를 제공, 기밀성을 제공해 주지는 않음 **암호화(ESP)프로토콜** - 암호화 기법을 사용하여 데이터의 무결성, 비밀성의 기능을 제공 하는 프로토콜, 프라이버시 제공 **암호화 방식 및 무결성 확인 작업**
IPSec 적용 **활성화 단계**	장비, 인터페이스에 IPSec VPN 적용을 통한 활성화 작업 활성화를 통한 Host 간 연동 진행

"끝"

4	인터넷 프로토콜 주소체계 및 단계별 주소 변환 과정
문제	인터넷 프로토콜에서 3 단계 주소체계(Domain name, IP address, Physical address)를 사용하는 이유를 제시하고, 데이터 전송 과정에서 각 단계별로 주소가 변환되는 과정을 설명하시오.
도메인	디지털네트워크
정의	인터텟 프로토콜 3 단계 주소체계, 사용자 관점의 호스트 이름, 인터넷 주소 IP, 물리적 하드웨어 주소.
키워드	Domain name, Internet Address, Physical Address, Encapsulation & Decapsulation, OSI 7 계층, TCP/IP 5 계층. DNS 서버, ARP 프로토콜
출제의도분석	인터넷 프로토콜에서 사용하고 있는 3 단계의 주소체계에 대해 알고있는지 여부와 사용되는 이유, 각 주소별 대응 계층 및 데이터 전송 과정에서의 주소 변환 과정에 대한 이해 문제.
답안작성 전략	인터넷 프로토콜 각 주소체계에 대한 개요, 특징을 기술하고, 네트워크 모델에서의 각 계층에서 사용되는 주소체계를 설명, 데이터 전송과정에서의 주소 변환 순서를 기술
참고문헌	인터넷으로 본 정보통신개론 (조국현외, 인터넷교보문고)
모범목차	주소체계의 개요 (3 단계 주소체계 설명), 3 단계 주소체계 사용 이유, 각 단계별 변환 과정
풀이 기술사님	송영호 PE (제 102 회 컴퓨터시스템응용/ songyoungho@hanmail.net)

■ **인터넷 프로토콜 주소체계(Domain name, IP address, Physical address)의 개요**

- 인터넷에 연결된 여러 망들의 구성요소들을 각각 식별하기위한 체계로, 인터넷에 연결된 특정 호스트는 TCP/IP 인터넷 식별자 체계에 의해서 식별된다.

- 인터넷에서 사용하는 3 단계 주소 식별자들

식별자	설명
호스트이름(Host/Domain Name)	사용자 관점의 이름 체계, 도메인 네임서버 사용 (DNS)
인터넷주소(Internet Address)	일반적으로 IP 주소, 특정 망에 연결된 특정 호스트가 다른망과 인터네트워킹 될 때 형성된 가상 망인 인턴넷 내에서 유일하게 식별될 수 있도록 하는 주소
물리주소(Physical Address)	물리적 망에 접속된 각 장치에 대한 유일한 물리적 하드웨어 주소, 이더넷 주소 또는 하드웨어 주소

- Domain name 의 개념 및 특징

TCP/IP 사용자 호스트와 응용프로그램을 위한 식별자로 사용자 관점에서 알파벳과 숫자등의 조합으로 구성하여 사용자가 이해하기 쉬운구조.

일련의 도메인이름(domain name)들을 포함하는 트리구조의 이름 체계를 사용.

- IP Address 의 개념 및 특징

인터넷 상에서 라우팅을 효율적으로 하기 위해 물리적인 네트워크 주소와 일치하는 개념으로 부여된 32 비트(IPv4) 혹은 128 비트(IPv6) 주소로, IP 를 이용하면 네트웍상의 유일한 호스트를 식별하는 것 뿐만 아니라, 호스트가 있는 네트웍을 식별할 수 있다. IP 주소는 클래스로 나뉘어 있으며 하나의 네트워크에서

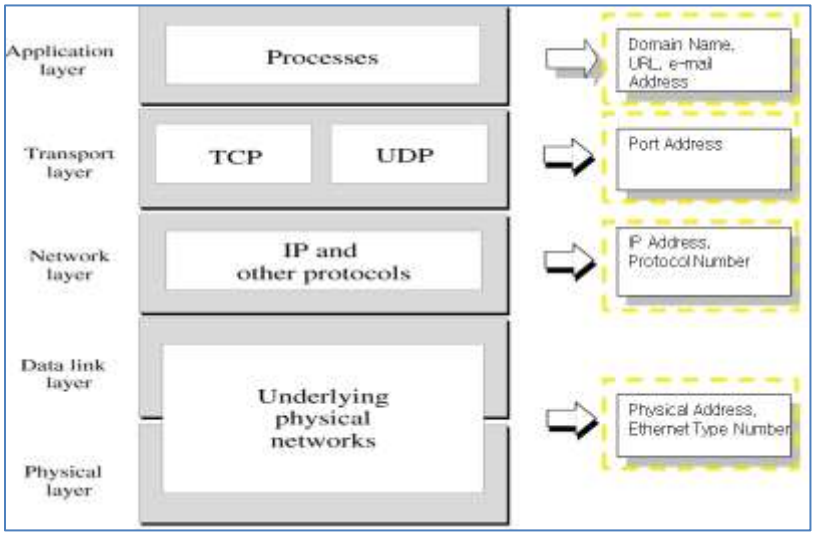
모든 호스트는 동일한 Prefix 를 공유하게 된다.

- Physical Address 의 개념 및 특징

이더넷(Ethernet) 망에 각 접속된다는 의미에서 "이더넷 주소" 또는 "하드웨어 주소"라고하며, 근거리 통신망에 특정 호스트 접속 시 사용되는 호스트의 망접속 카드(NIC: Network Internet Card) 생산업자가 이 장치를 생산할 때 세계적으로 유일하게 할당되는 주소. 근거리 통신망의 데이터 링크는 48 비트의 주소체계를 사용, 각 호스트를 유일하게 식별할 수 있도록 하는 하드웨어 주소

■ **3 단계 주소체계(Domain name, IP address, Physical address) 사용 이유**

- 인터넷 TCP/IP 는 데이터 전송과 인터넷을 사용하기 위해 각 계층별 각기 다른 주소체계를 사용하고 있음으로, 각 계층에 맞는 주소를 사용하여 효율적인 식별이 가능하다. 5 계층에서는 어플리케이션이나 사용자가 이해할 수 있는 주소체계 Domain name 을 사용하고, 3 계층에서는 IP 주소를 사용하고, 1,2 계층에서는 Physical 주소를 사용하여 각 계층별 주소 변환과정이 필요하게 된다.



[TCP/IP 각 계층과 주소체계의 연관성]

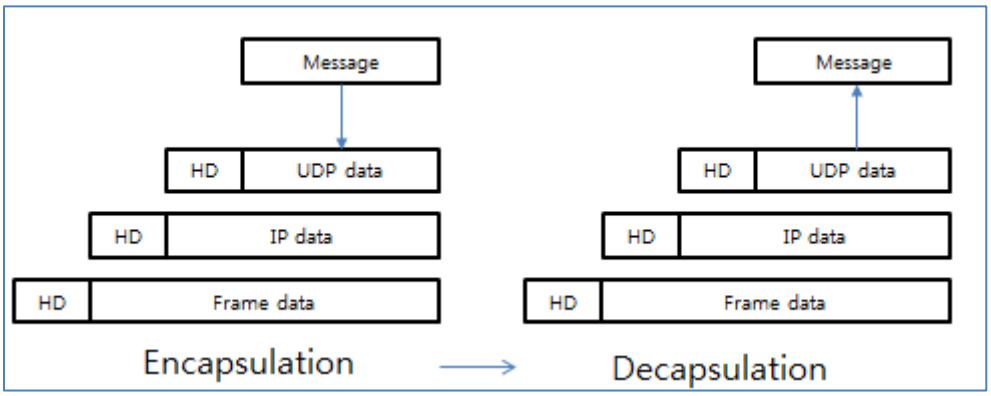
- 인터넷 프로토콜에서 3 단계 주소체계를 사용하는 각 단계별 이유

주소체계	사용계층 및 이유	주소 체계
Domain Name	- 5 계층에서 사용하는 컴퓨터 식별 주소 - 인터넷에서 특정호스트를 식별하는 IP 주소는 숫자로만 되어있어, 사람이 기억하기도 어렵고, 사용하기도 어렵다. - 도메인 네임은 문자로 이루어져 있기 때문에 기억하기도 쉽고 사용하기도 편리한 장점이있다.	- www.kpcpe.or.kr<호스트이름.기관이름.기관의성격.나라표시> - 일반 최상위 도메인 최상위 도메인 / 구 분 COM / 일반 기업체, 영리 기관 (Company) NET / 네트워크 관리 기관 (Network) ORG / 비영리 기관 또는 각종 조직 (Organization) EDU / 4년제 단과 대학/종합 대학 (Education) GOV / 미국 연방 정부 기관 (Goverment) MIL / 미국 연방 군사 기관 (Military) INT / 국제적인 기구, 기관 (UN, NATO 등) -국가별 최상위 도메인 코드 / 국 가 명 KR / 한국 KP / 북한 JP / 일본 CA / 캐나다

IP Address	- 3 계층에서 사용가능 - 인터넷상에서 라우팅을 효율적으로 하기위하여 물리적인 네트워크 주소와 일치하는 주소 사용 - 클래스로 나뉘어 있으며 하나의 네트웍에서 모든 호스트는 동일한 Prefix 를 공유가능하게 함	-32/128 비트 주소 체계 -바이트 단위로 4 개의 10 진수로 표시 -범위는 0.0.0.0 에서 255.255.255.255 의 값을 가짐 - 현재는 IPv4 에서 IPv6 체계로 변화됨
Physical Address	- 1,2 계층에서 사용가능 하드웨어주소 - 물리적 하드웨어에대한 유일한 식별 주소로 사용	- 48 비트 LAN 카드 식별번호, MAC 주소, 어뎁터 주소, 채널 번호 - 회사식별코드와 관리코드 등으로 구분됨

■ **데이터 전송과정에서 각 단계별 주소 변환 과정**

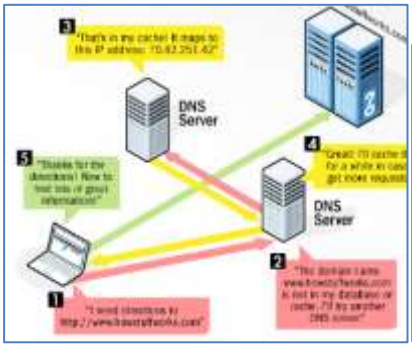
- 데이터 전송 전 캡슐화 과정을 중 수신자(Receiver) 식별절차로 먼저 DNS 서비스를 이용하여 수신자 도메인 네임을 IP 주소로 변환 하고, ARP 를 이용하여 수신자 IP 주소를 물리주소(Physical Address)로 변환한다.



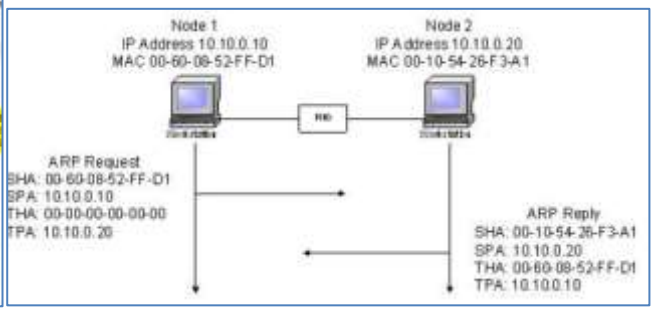
[Encapsulation 과 Decapsulation 과정]

- 각 단계별 주소 변환 과정

단계	과정 설명
도메인네임	응용계층에서 문자열 "Hello"를 수신자 도메인 네임을 사용하여 전송
IP 주소 획득	DNS 서버 또는 캐쉬된 주소를 이용하여 수신자의 도메인 네임에 해당하는 IP 주소를 획득하여, 네트워크계층 IP 헤더의 수신자 주소에 삽입
물리주소 획득	물리 주소는 동일 망 내에서, ARP 프로토콜을 이용하여 LAN 카드의 Physical 주소를 획득하고, 프레임 헤더의 수신자 주소에 삽입



[DNS Service to get IP Address]



[Address Resolution Protocol: to get Physical Address]

"끝"

5	사물인터넷(IoT : Internet of Things)
문제	**사물인터넷(IoT : Internet of Things)의 주요 핵심기술 및 국내외 서비스 개발현황에 대해 설명하시오.**
도메인	디지털서비스
정의	모든 사물에 네트워크 연결을 제공하는 네트워크의 네트워크 (ITU-T)
키워드	-핵심기술: **플랫폼 기술, 단말 인터렉션 기술, 통신기술, 에너지 하베스팅/센서 기술**
출제의도분석	99 회 IoT 특성 및 기본 구성요소 1 교시 문제에 대한 심화출제
답안작성 전략	플랫폼 기술, 단말 인터렉션 기술, 통신기술, 에너지 하베스팅을 핵심기술로 기술하고, 국내외 서비스 현황에 대한 풍부한 사례제시가 핵심
참고문헌	- IoT(M2M) 기술 동향 및 발전 전망-한국전자통신연구원 - IoT 플랫폼 개발동향 및 발전방향-전자부품연구원
모범목차	1. 사물인터넷의 개요 가. [도] D2D, M2M, IoT, IoE 의 기술범주 개념도 나. 사물인터넷(IoT)의 개념(혹은 정의) 2. 사물인터넷의 주요 핵심기술 - [표] 플랫폼/단말 인터랙션/통신/에너지 기술 3. 사물인터넷의 국내외 서비스 개발현황 가. [표] 국외 사물인터넷 개발현황 나. [표] 국내 사물인터넷 개발현황 4. (선택) 국내 IoT 시장 활성화를 위한 제언 - [도] 국내 IoT 산업 SWOT 분석도 및 의견제시
풀이 기술사님	박상욱 PE (제 99 회 정보관리/ studygosu@gmail.com)

■ **사물인터넷의 주요 핵심기술 설명**

가. 사물인터넷의 주요 핵심기술 개요

핵심기술	설명
(개방형 시맨틱) **IoT 플랫폼 기술**	- 개발자들이 쉽게 데이터를 찾고 적용할 수 있는 개방형 데이터 플랫폼이 기술
(센서-스마트) **단말 인터렉션 기술**	- 센서 및 스마트 기기 모두가 인터넷 연결 대신 내장된 네트워크 인터페이스를 이용해서 직접 통신이 가능한 기술
(고신뢰, 저전력) **통신 및 네트워크 기술**	- 통신거리 및 전송속도의 한계, 장애물/간섭에 의한 통신품질 저하, 저전력화의 어려움 등 기존 기술의 문제점을 극복기술
에너지 하베스팅 및 센서 기술	- IoT 사물 종류를 제한하는 원인인, 사물전원 공급을 위한 에너지 생성및 수집기술

나. 사물인터넷의 주요 핵심기술 상세설명

핵심기술	상세설명		기술 발전방향
(개방형 시맨틱) **IoT 플랫폼 기술**	M2M 플랫폼	- 단말의 연결성 기반	- 시맨틱, 서비스 mash-up,상황인식 및 예측 기술 추가
	USN 플랫폼	- 센서를 통한 서비스 기반	
	WOT 플랫폼	- 단말간 협업과 웹 서비스 기반	
(센서-스마트) **단말 인터렉션 기술**	유선방식	- USB, IEEE1394	- 비 인터넷 연결 구조로 보안강화
	무선방식	- 블루투스, IEEE 802.15.4	

		(Zigbee), RFID/NFC, Wi-Fi	- 독립적인 네트워크 구축
(고신뢰, 저전력) **통신 및 네트워크 기술**	HART 진영	- WirelessHART	- 1Km 이상의 통신거리, 음영지역 신뢰성 있는 통신 - 저전력화, 최소 인프라 기술
	ISA 진영	- ISA-100.11a	
	IEEE802.15	- 15.4e/g/k/m, 15.8	
에너지 하베스팅 및 센서 기술	태양광 기반	- 작은 표면용 (10mW-15mW)	- 사람, 동물 움직임에서 에너지를 하베스팅하는 기술 (압전소자 기반)
	온도 기반	- 작은 온도차를 이용 (15mW)	
	진동 기반	- 진동 변동성 (1mW-200mW)	

■ **사물인터넷의 국내외 서비스 개발현황**

가. 국외 사물인터넷 서비스 개발현황

구분	회사	서비스 개발현황
IT 기업	시스코	- Community+Exchange (스마트한 연결된 커뮤니티 제공)
	IBM	- Smart Planet (모든 자연과 사람을 연결하여 지능화 및 기능화)
헬스케어	버라이즌	- 디지털 케어 매니지먼트 플랫폼 (만성질환 관리 솔루션)
	보다폰	- 심장질환관리솔루션 (심장질환관리용 M2M 플랫폼)
	소프트뱅크	- Activity Tracker (핏빗(Fitbit)과 연동)
물류 및 자동차	페덱스	- 센스어웨어(SenseAware) (물류배송과정 파악)
	포드사	- Evos (차량의 부품들이 인터넷으로 연결되어 보험사 등과 연동)
	벤츠	- 자율 주행(Autonomous Driving) 자동차
에너지, 생활	필립스	- 휴(hue) (스마트으로 가정조명을 제어)
	밸킨	- 위모(Wemo) (스마트폰 기반 조명제어)
	디즈니랜드	- 미키마우스 (센서를 탑재하여 놀이기구 위치정보 제공)

나. 국내 사물인터넷 서비스 개발현황

구분	회사	서비스 개발현황
IT 업체	삼성전자	- 홈싱크 NFC 기능을 가진 안드로이드 기반의 모바일기기(스마트폰, CCTV, 카메라 등)와 연결하여 콘텐츠를 공유
	LG 전자	- 올조인(AllJoyn) (퀄컴과 제휴하여 가전제품 제어)
헬스케어	서울대학교 병원	- 서울대학교병원 (손목이나 허리에 착용한 활동량 측정기를 통한 개인 맞춤형 건강관리)
	텔릿	- 원격 의료 데이터 서비스 (원격 건강진단)
자동차	현대자동차	- BlueLink (스마트폰이을 통해 원격으로 차량 주차 위치 확인, 차량 내비게이션으로 목적지 전송등 차량 정보 관리가 가능)
	기아자동차	- UVO (M2M 기반 텔레메틱스 서비스)
이통사	KT	- 스마트홈(Smart Home) (스마트폰을 이용하여 원격으로 댁내 방범, 검침 및 전력제어 등 실시간으로 집안환경을 파악하고 제어)

	LGU+	- 음식물쓰레기 관리시스템 (음식물 쓰레기 처리기 연동) - 차량관제시스템 (물류업체, 버스 및 택시 등 차량 관리)
	SKT	- 스마트팜(Smart farm) (경작지, 축사 등에 센서를 장착하여 원격으로 내부습온도 등의 환경을 측정하고, 급배수 조정, 사료공급)

- 국내외 주요 서비스 사례를 통하여 알 수 있는 것은 기존 재난, 재해 등 공공 분야와 공장 자동화 등 기업 중심의 사례가 이제는 개인에 직접적으로 영향을 미치는 B2C 서비스가 확산
- 아직은 시장을 선도할 수 있는 서비스와 글로벌 시장을 창출할 수 있는 국제 표준과 킬러 어플리케이션의 부재 등으로 인해 시장이 느리게 확대되고 있음
- 국내 시장의 활성화를 모색하고 글로벌 기술 경쟁력 제고와 시장 선도를 위한 핵심 기술개발 및 서비스 발굴이 현시점에서는 무엇보다도 필요함 "끝"

■ **[참고] M2M, IoT, IoE and D2D**

구분	설명
M2M	- 인간의 직접적인 개입이 꼭 필요하지 않은 둘 혹은 그 이상의 객체 간에 일어나는 통신 (ETSI, 유럽통신표준협회)
IoT	- 모든 사물에 네트워크 연결을 제공하는 네트워크의 네트워크 (ITU-T) - 인간과 사물, 서비스 등 분산된 구성 요소들 간에 인위적인 개입없이 상호 협력적으로 센싱, 네트워킹, 정보 교환 및 처리 등의 지능적 관계를 형성하는 사물 공간 연결망
IoE	- M2M, IoT, 빅데이터, 클라우드, 공간인터넷 등을 기반으로 한 사람-사물-공간이라는 이질적 요소들의 초연결 생태계

- D2D(Device to Device)기술은 네트워크를 거치지 않고 근접거리에서 서로 다른 기기와 기기 간에 통신하는 기술. (Bluethooth, UPnP(Universal Plug and Play)와 DPWS(Device Profile forWeb Services), WiFi Direct 등)
- D2D 는 'M2M/IoT/IoE' 기술에 포함되지만 범위가 무선 통신이 가능한 기기 간의 통신에 국한됨.

■ [참고] 국내 IoT SWOT 분석

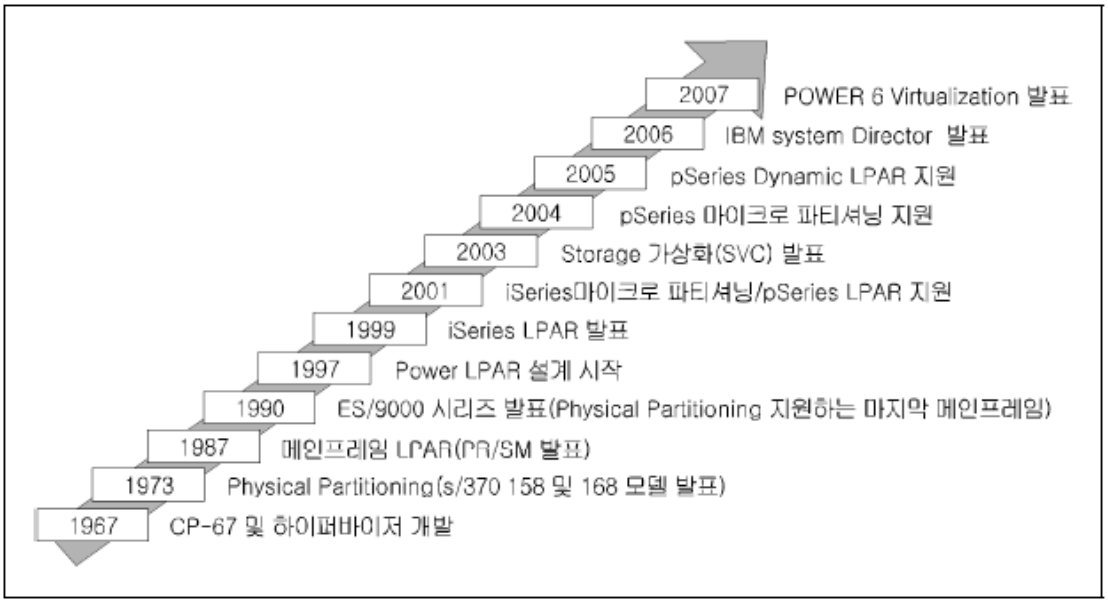
강점 요인	약점 요인
- 세계 최고의 IT 및 네트워크 인프라 - 최고 수준 이동통신기술(LTE-A 등) 확보 - 세계적인 IT 선도업체 보유 - 세계 1위의 스마트폰 제조국 - 반도체, 디스플레이 등 핵심부품 경쟁력 보유	- 플랫폼·SW 경쟁력 미흡 - 센서, 보안 등 핵심분야 경쟁력 부족 - 미래지향적 혁신 및 R&D 투자 부족 - 창의 전문인력 부족 - 주도적 중소기업 성장 환경 미흡 - 사물인터넷 시장 활성화 여건 및 생태계 조성 미흡
기회 요인	**위협 요인**
- 세계 사물인터넷 분야 수요 확대 - 사물인터넷 관련 표준화 추진 활발 - 사물인터넷 시장은 성장 초기로 대등한 경쟁 가능 - 정부의 적극적인 산업 육성 의지	- 글로벌 선도업체들의 기술 잠식 우려 - 기술 및 표준화 주도 경쟁 확대 - 중국 등 후발주자의 급부상 - 주요국들의 국가차원에서 집중 지원

"끝"

Notes

6	가상화
문제	**가상화 기술의 발전추이, 최근 가상화 기술의 특징인 1)동적배분, 2)ICT 하드웨어 자원 통합, 3)통합화된 가상화**
도메인	최신기술/동향
정의	물리적으로 다른 시스템을 논리적으로 통합하거나 하나의 시스템을 논리적으로 분할해 자원을 효율적으로 사용하게 하는 기술
키워드	동적배분, ICT 하드웨어자원 통합, 통합화된 가상화, 인포메이션 가상화, 워크로드 가상화
출제의도분석	효과적 ICT 자원활용 및 클라우드 컴퓨팅을 위한 핵심기술인 가상화 기술의 발전추이 및 최근의 기술적 특징에 대한 이해
답안작성 전략	문제에서 요구하는 기술에 대한 정확한 이해 및 표현
참고문헌	KISDI [방송통신정책] (제 25 권 5 호) 초점 - 가상화 기술의 동향 및 주요 이슈
모범목차	1. 가상화 기술의 발전 추이 및 최근 가상화 기술의 특징 가. 가상화 기술의 발전 추이 - 대규모 분산 개방형 구조 (x86 서버 가상화 도입) - 서비스/비즈니스 관점의 가상화 필요성 확대 나. 가상화 기술의 특징 - HW 효율성 관점(동적배분, ICT 하드웨어자원 통합), - 서비스 아키텍처관점(통합화된 가상화) **2. HW 자원 효율성 극대화 동적배분과 ICT 하드웨어 자원 통합** **3. 서비스 관점의 자원관리, 통합화된 가상화** 4. 가상화 기술의 효과
풀이 기술사님	권혁재 PE (제 102 회 정보관리/ star10ve@naver.com)

■ **가상화 기술의 발전 추이**



- 초기에는 Virtual Machine Monitor(VMM)를 통해 모든 하드웨어 인터페이스를 가상화. 이를 통해 메인프레임은 여러 애플리케이션과 프로세스를 동시에 실행할 수 있게 됨.
- 1980 년대 들어 클라이언트-서버 애플리케이션이 증가하고, x86 서버와 데스크톱을 통한 분산 컴퓨팅이 가능해짐. 기하급수적으로 늘어난 서버 자원의 효과적 활용을 위해 x86 서버에 가상화 도입.

컴퓨터 리소스의 추상화

가상화는 1960 년대부터 나온 개념. 초기 가상화는 메인프레임을 논리적으로 여러 개의 가상머신으로 분리하는 데 초점

1980 년대 이후 서버 가격이 낮아짐에 따라 ICT 인프라는 중앙 집중형에서 분산 개방형 구조로 변화함.

가상환경 구축/운영 비용

Notes

의 감소와 클라우드 컴퓨팅의 확산은 가상환경으로의 전환을 촉진하고 있음

1) 메인프레임 서버/하드웨어 인터페이스 가상화
2) 가상 스토리지
3) 물리적 파티셔닝
4) 다이내믹 파티션을 지원하는 하이퍼바이저
5) x86 서버 가상화 (분산 개방형 구조)

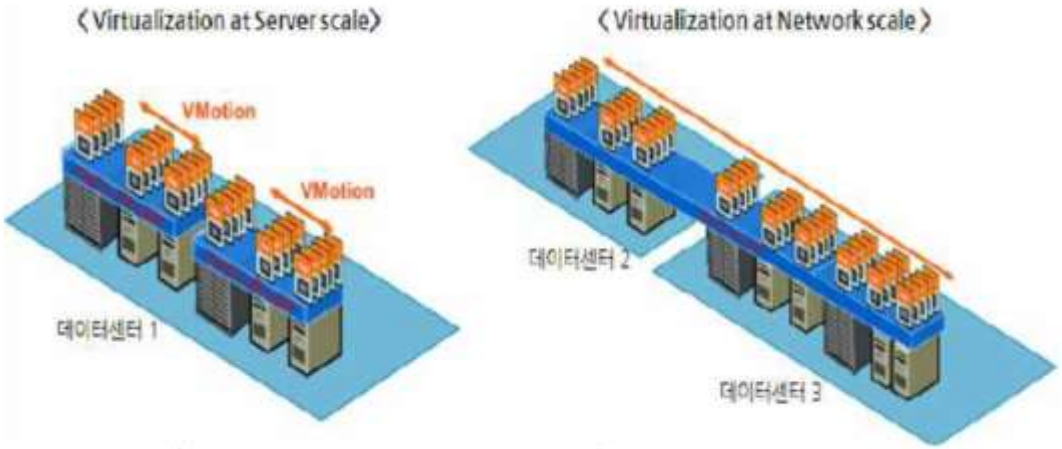
■ **최근 가상화 기술의 기술적 특징**

핵심역량	설명
동적 배분(dynamic allocation) 기술의 강화	- 사용자의 ICT 자원 요구가 늘어나면 이에 대응하여 자동적으로 가상자원을 재조정하는 것이 핵심. 1) 파티션 무빙 기술 - 개별 가상머신들이 서로 다른 서버간 이동 2) 애플리케이션 재배치 기술 – 가상머신 내에 존재하는 애플리케이션을 다른 가상머신으로 이동
ICT 하드웨어 자원의 통합 가상화 움직임 강화	- 복잡한 ICT 구조를 모듈 형태로 전환 - 가상화의 범위가 서버, 스토리지 등 단일 자원에서 총체적인 ICT 자원 전반으로 변화 - 자원 공유에서 나아가 ICT 자원의 통합(consolidation)의 방향으로 발전.
단절화된 가상화에서 **통합화된 가상화**로 이동	- 분산, 개방된 ICT 자원의 효율적 활용을 위해서는 전사적 워크로드 관리가 중요 - 워크로드 관리의 관점을 서비스 중심, 업무 중심으로 전환하는 서비스 지향적 ICT 인프라스트럭처 관리 필요 - 인포메이션 가상화, 워크로드 가상화

- 하드웨어관점의 가상화(동정배분, ICT 하드웨어 자원 통합)와 서비스 관점의 가상화(통합화된 가상화)로 구분 가능

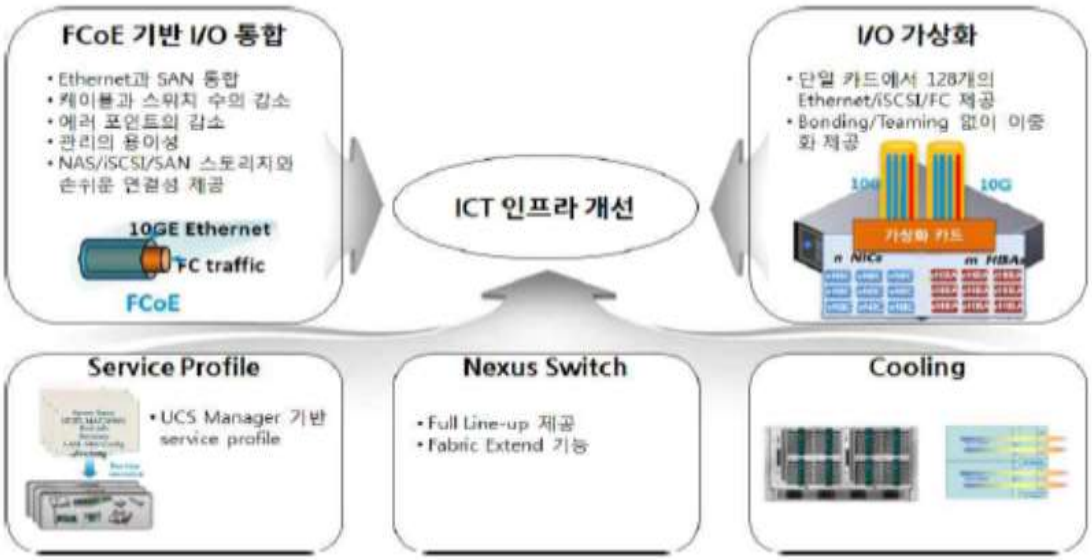
하드웨어 가상화라고 해서 데이터나 인포메이션, 그리고 워크로드에 무관하지 않으며, 인포메이션, 워크로드 가상화도 기본적으로 서버, 네트워크, 스토리지 등 하드웨어 가상화에 기반함

■ **동적배분(Dynamic allocation technology)**



- (Live Migration: 가상머신을 다른 서버로 이동시키는 기술, VMWare 의 vMotion 이 대표적 사례)
- ESX 서버 위에서 작동 중인 가상 머신을 power off 하거나 shutdown 하지 않고 다른 ESX 서버로 이동시키는 기술(서로 다른 데이터 센터간 동적 배분 가능)

■ **ICT 하드웨어 자원의 통합**



- 서버, 스토리지, 네트워킹을 하나의 장비에 통합하고, 기존의 랙 마운트 방식 서버에서 블레이드 서버로의 전환
- 메모리 확장, 10 gigabit Ethernet 기반의 FCoE(Fiber Channel over Ethernet) 기술 기반 I/O 통합, I/O 가상화 기술을 통한 다량의 I/O Card 생성 등

■ **인포메이션 가상화**

- 관리하는 데이터가 대용량화되고, 필요한 정보를 생성하기 위해 ***다양한 데이터***가 요구되고 있으며, 이를 적절히 처리하기 위한 대안으로 인포메이션 가상화가 대두
- 데이터 가상화를 통해 데이터 또는 데이터가 지닌 가치를 비즈니스에 쉽게 적용할 수 있는 단계로 발전시킨 형태로 **<u>파일 시스템 가상화와 데이터 가상화가 있음</u>**

이기종 데이터베이스에 존재하는

■ **파일시스템 가상화**

- 파일 시스템은 컴퓨터 파일에 이름을 붙이고, 저장이나 검색을 위해 논리적으로 그것들을 어디에 위치시켜야 하는지 등을 나타내는 방법.

- 파일 시스템의 종류

구분	특징	종류
단일 파일 시스템	저널링, 보안 등 단일 플랫폼 및 OS를 위해 특화된 파일 시스템	JFS, NTFS, ext2
네트워크 공유파일 시스템	특정한 프로토콜로 네트워크 상에서의 데이터 공유	NFS, CIFS, APS
클러스터 파일 시스템	동일 서버들로 이루어진 클러스터 사이에 고속으로 데이터를 공유	GPFS, GFS, Luster, ISVs
SAN 파일 시스템	SAN 환경에서 이기종의 서버들끼리 데이터를 공유	CXFS, SANergy
글로벌 그리드 파일 시스템	네트워크 공유 파일 시스템의 확장으로 독립적인 네트워크 파일 시스템이 모여서 계층적인 구조를 형성	Global GPFS, NFSv4

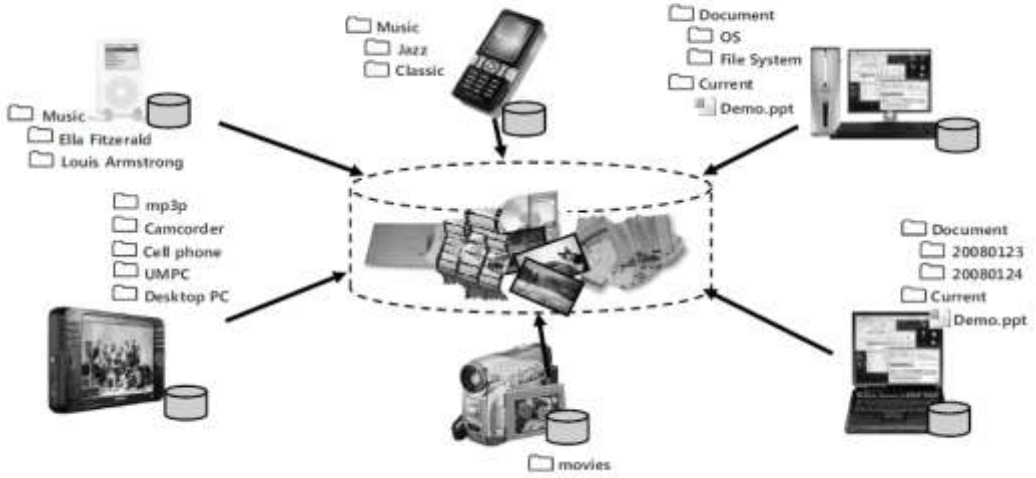
- 파일 시스템 가상화는 실제 파일레벨의 가상화를 의미
- 사례) 통합 파일 시스템에서의 파일 시스템 가상화

Notes

* 파일시스템 가상화

파일서버와 해당 파일을 사용하는 클라이언트 사이의 가상화

다양한 파일시스템을 하나의 가상 파일 시스템으로 통합하고 사용자의 엑세스를 지원하는 인터페이스를 제공



- 사용자는 자신이 사용하는 디바이스/OS 의 파일시스템을 사용한다고 인식

■ **데이터 가상화**

- 인포메이션 가상화 구현을 위한 근간으로, 단순히 데이터를 모으는 데서 나아가 의미 있는 정보로의 전환까지를 통합적으로 지원하는 가상화 기술

구분	내용	비고
데이터 콘솔리데이션	• 장소의 단일 지점화와 자원의 대규모화를 통한 물리적 단순화 • 대용량의 서버 및 스토리지를 이용해 구성 및 관리상의 단순함을 얻음 • 하지만 데이터 크기가 커짐에 따라 데이터 검색 시간, 성능 및 가용성 저하 노출 → 데이터베이스 파티셔닝, 데이터베이스 간 클러스터링 활용 • 데이터베이스 파티셔닝의 장점: 파티션간 병렬처리를 통한 빠른 데이터 검색 및 처리, 성능의 선형적 증가 효과, 고가용성(HA) 확보	물리적 통합
데이터 연합	• 장소와 자원을 그대로 둔 채 관계의 단순화를 통한 논리적 단순화 • 다양하게 분산되어 있는 데이터의 위치, 형태, 접근 언어에 무관하게 마치 단일 데이터 소스인 것 같은 접근을 가능하게 하는 미들웨어 기술 • 구축 시간과 유지비용 감소, 최신 데이터에 접근 용이, 다양한 포맷을 가진 데이터를 이용한 새로운 데이터 생성 용이 • 하지만 데이터 접근 속도는 데이터 콘솔리데이션 방식보다 느림	논리적 통합

데이터 자원의 중복을 최소화하며 가용성을 극대화 가능

물리적 자원을 단일화하여 재구성

- 물리적 통합인 데이터 콘솔리데이션과, 논리적 통합인 데이터 연합 크게 두 가지가 있음.

■ **워크로드 가상화**

- 현실적으로 물리적 ICT 자원의 완전한 가상화가 곤란한 상황에서 가용 수준의 가상화를 통해 애플리케이션의 성능을 최대한 끌어낼 수 있는 ICT 구조

외부 데이터를 논리적으로 가상화하여 통합

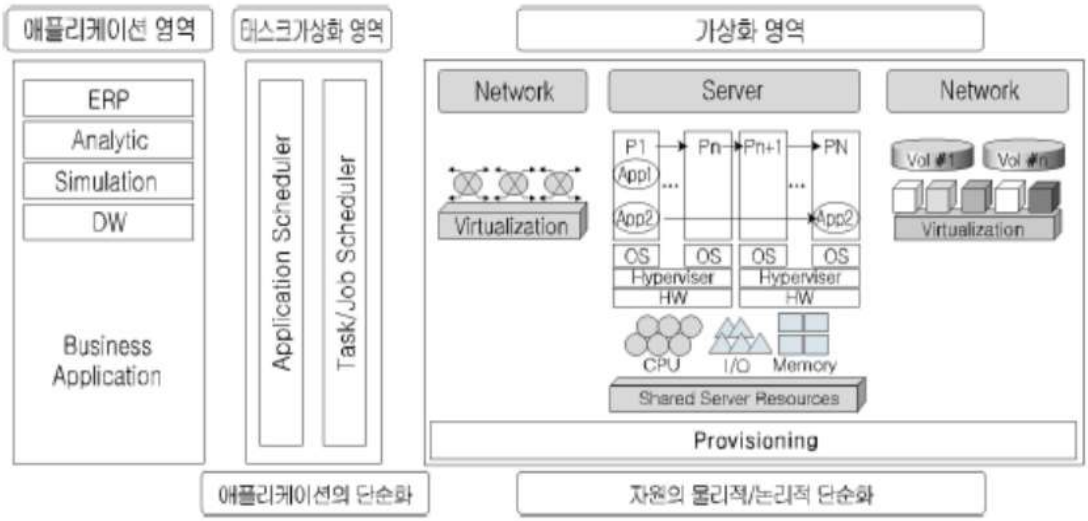
	내용
트랜잭션 가상화	JVM(Java virtual machine)과 같은 가상 머신을 이용하는 미들웨어 애플리케이션을 활용해 애플리케이션 자체적으로 적절한 워크로드 관리를 바탕으로 새로운 인스턴스를 생성하거나 워크로드가 낮은 서버 쪽으로 작업량을 배분
태스크 가상화	그리드 미들웨어를 사용해서 다른 기종 서버 환경에 대한 제약을 극복하며, 업무 스케줄러를 이용한 워크로드의 분산처리를 통해 다른 기종의 서버 자원들이 모인 환경에서도 대규모 컴퓨팅 파워를 제공. 컴퓨팅 그리드라고도 함
프리젠테이션 가상화	최종 사용자 측면에서 애플리케이션이 없더라도 애플리케이션이 수행될 수 있는 환경을 제공. 서버기반 컴퓨팅(server-based computing; SBC)이 대표적 기술임

1) **트랜잭션 가상화**

- 다수의 서버를 자원 풀로 관리하여, 관리자는 **가상화된 하나의 큰 서버에 애플리케이션을 설치하고, 각 애플리케이션이 어떤 물리적 서버에서 구동될 것인가는 트랜잭션을 전체적으로 관리하는 레이어가** 각 애플리케이션에 실시간으로 가해지는 부하량과 서버의 자원 사용량을 분석하여 **동적으로 결정**하는 방식

2) 태스크 가상화

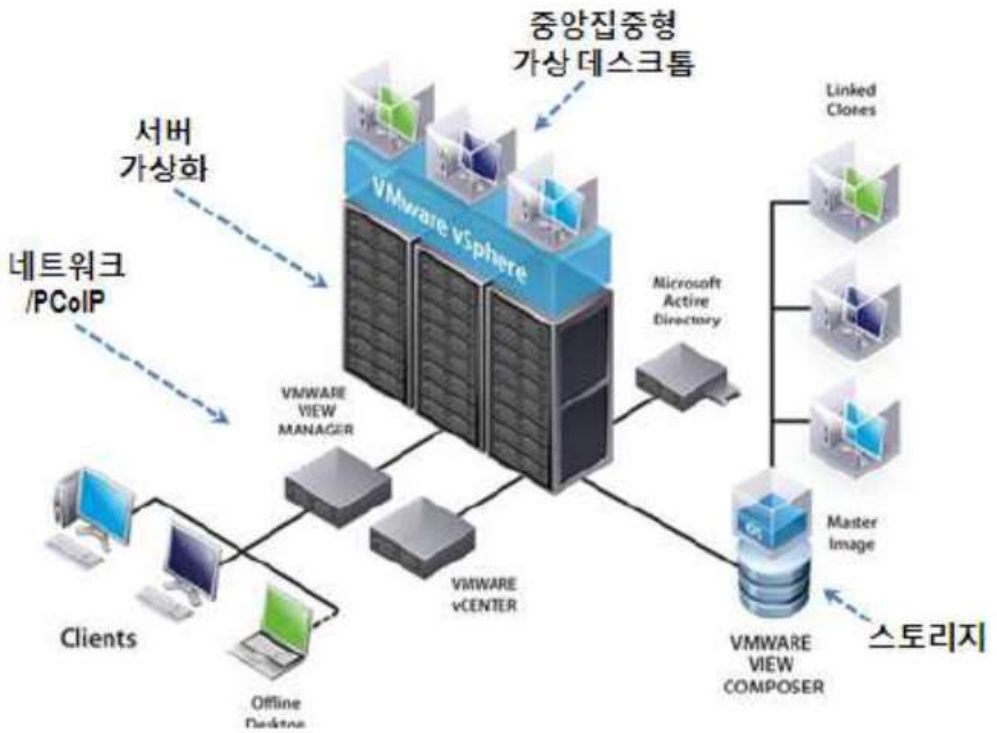
- **중간 매개체 역할을 하는 서버(task scheduler 혹은 job scheduler)에 작업(task 혹은 job)을 요청하고, 서버는 가용한 컴퓨팅 자원 풀에 작업을 분배하여 요청사항을 처리하게 한 다음, 처리가 끝난 후 이를 수집해서 다시 작업 요청자에게 돌려보내는 방식**



3) 프리젠테이션 가상화

- **클라이언트-서버 구조는 유지하면서, 클라이언트 레벨을 가상화하는 방식**.
- 즉 프리젠테이션(웹 서버)-프로세싱(애플리케이션 서버)-데이터(데이터베이스 서버)로 구성된 **3-tier 구조에서 웹 서버 단을 가상화하여 최종 사용자로 하여금 특정 클라이언트의 단말에 해당 애플리케이션이 없더라도 서비스를 수행할 수 있게 하는 방법**.

씬 클라이언트(thin client), 네트워크 컴퓨팅(network computing), 서버 기반 컴퓨팅 (server-based computing; SBC) 등을 통해 구현



- 높은 보안성이 요구되거나, 모바일 오피스와 같이 업무의 이동성이 중시되거나, 콜센터와 같이 표준화된 업무 프로세스가 일반적인 경우, 혹은 다수의 공용 PC 로 구성되어 클라이언트 관리가 어려운 경우 등에 적합

■ **가상화의 효과**

구분	가상화의 효과	내용
총소유비용 절감	자원 활용률 증가	물리적 자원과 자원 풀에 대한 동적 공유
	관리비용 절감	관리의 자동화, 정보화, 중앙화를 통한 관리 기능 단순화 및 관리 인력의 생산성 증가
유연성 증가	사용의 유연성	빠르게 변하는 비즈니스 요구사항에 대응한 자원의 동적 재구성 및 활용
	보안의 향상	분리, 격리 등을 통한 안전한 접근 제공
공유된 인프라 스트럭처 활용	가용성 증가	사용자에 영향을 주지 않으면서 물리적 자원의 변경
	확장성 증가	물리적 자원의 변경 없이 가상화된 자원의 확장
	상호운영성 및 투자의 보호	기존 물리적 자원간 불가능한 인터페이스와 프로토콜 레벨의 호환성 제공
	향상된 프로비저닝	ICT 자원의 물리적 단위에 상관없이 가상화된 자원을 빠르게 할당, 제공

ICT 자원을 안정적이면서도 수요에 맞춰 유연하고 빠르게, 자동적으로 제공

- 기업의 의사결정 방식을 기존 인프라스트럭처 중심 사고에서 서비스 중심 사고로 전환할 수 있도록 지원.

■ **[참고] 가상화를 통해 구현되는 클라우드 컴퓨팅의 기능**

클라우드 컴퓨팅의 요구사항	가상화를 통해 구현하는 내용
효율성 및 자동화	pooling, zero-touch infrastructure
민첩성	self service(automated provisioning), contol
선택의 자유	open, inter-operatability

- 서버를 가상화한다는 것은 컴퓨팅을 서비스로 바꿔놓는 의미이며, 결국 클라우드 컴퓨팅을 구현한다는 의미

"끝"

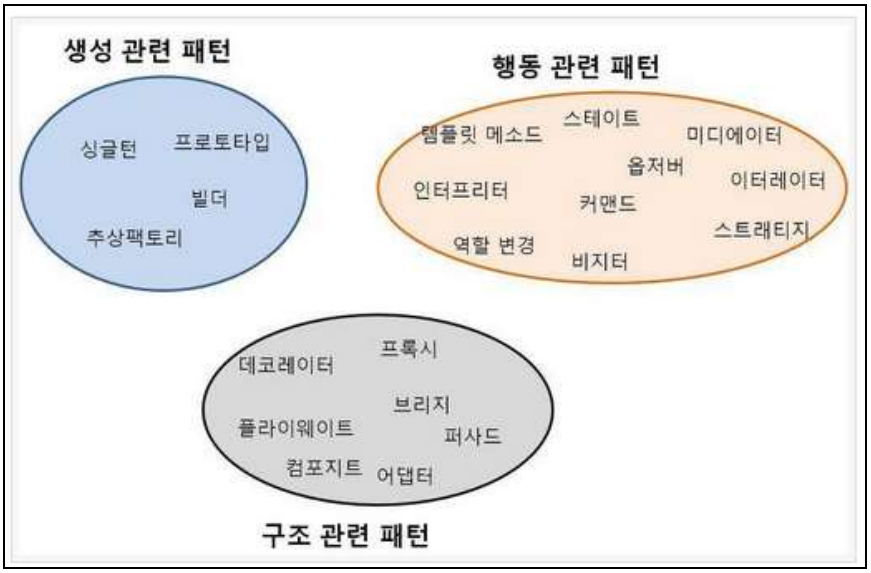
1	GoF 의 디자인 패턴(Design Pattern)
문제	객체지향 소프트웨어 설계에 많은 도움을 주는 GoF 의 디자인 패턴(Design Pattern)영역을 목적과 범위에 따라 분류하고, 분류 별 특성을 설명하시오. 또한, 객체지향시스템에서 개발된 기능의 재사용을 위해 사용되는 대표적 기법인 화이트박스 재사용(White-box Reuse), 블랙박스 재사용(Black-box Reuse) 및 위임(Delegation)이 패턴과 어떤 관계가 있는 지 설명하시오.
도메인	소프트웨어 공학
정의	프로그램을 개발하는 과정에서 빈번하게 발생하는 디자인 상의 문제를 정리하여 상황에 따라 간편하게 적용해서 쓸 수 있는 패턴 형태로 만든 해결 방법
키워드	생성/구조/행위, 클래스/객체, 상속(화이트박스)/합성(블랙박스)/위임 재사용 기법
출제의도분석	디자인 패턴에 대한 목적과 범위 별 분류를 이해하고 기능의 재사용을 위한 대표적 기법인 3 가지에 대해 디자인 패턴과의 연관성을 이해하는지에 대해 출제
답안작성 전략	-디자인 패턴에 대해 명확한 기준을 근거로 분류를 수행하고 각 분류 별 특성을 상세하게 작성 -화이트박스 재사용, 블랙박스 재사용, 위임 과 디자인 패턴과의 관계를 상술
참고문헌	디자인 패턴의 분류(인터넷 자료, http://hyeonstorage.tistory.com/100)
모범목차	1. 디자인 패턴의 목적과 범위에 따른 분류 2. 디자인 패턴의 분류 별 특성 가. 디자인 패턴의 목적에 따른 분류 별 특성 나. 디자인 패턴의 범위에 따른 분류 별 특성 3. 화이트 박스 재사용, 블랙박스 재사용, 위임과 디자인 패턴과의 관계 가. 화이트 박스 재사용, 블랙박스 재사용, 위임의 개념 나. 화이트 박스 재사용, 블랙박스 재사용, 위임과 디자인 패턴과의 관계
풀이 기술사님	임항섭 PE (제 102 회 정보관리/ reo_dica@naver.com)

■ **GoF 의 디자인 패턴 영역의 목적과 범위에 따른 분류**

분류기준	유형	설명
목적	생성	-객체 인스턴스 생성에 관여, 클래스 정의와 객체 생성 방식을 구조화, 캡슐화를 수행하는 패턴
	구조	-더 큰 구조 형성 목적으로 클래스나 객체의 조합을 다루는 패턴
	행위	-클래스나 객체들이 상호작용하는 방법과 역할 분담을 다루는 패턴
범위	클래스	-클래스 간 관련성 즉, 상속관계를 다루는 패턴 -컴파일 타임(Compile Time)에 정적으로 결정
	객체	-객체 간 관련성을 다루는 패턴 -런 타임(Run Time)에 동적으로 결정

- 디자인 패턴은 패턴의 목적과 범위에 따라 각각 분류됨

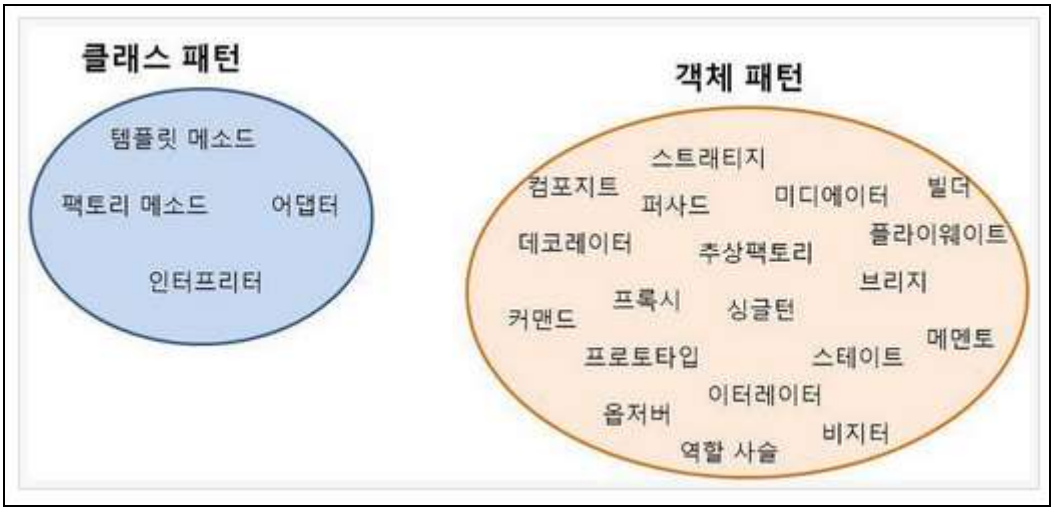
■ **GoF 의 디자인 패턴 영역의 목적에 따른 분류 별 특성**



분류	특성	패턴 종류
생성 패턴	-시스템이 어떤 구체 클래스를 사용하는 지에 대한 정보를 캡슐화 -이들 클래스의 인스턴스들이 어떻게 만들고 어떻게 서로 맞붙는지에 대한 부분을 완전히 숨김	-Singletone, Factory Method, Abstract Factory, Prototype, Builder 패턴
구조 패턴	-다른 기능을 가진 객체가 협력을 통해 어떤 역할을 수행할 때, 객체를 조직화시키는 일반적인 방식을 제시 -클래스와 객체가 보다 대규모 구조로 구성되는 방법에 대한 해결안을 제시 - 별도로 구성된 클래스 라이브러리를 통합하는데 유용	Decorator, Adaptor, Composite, Façade, Proxy, Bridge, Flyweight 패턴
행위 패턴	-객체의 행위를 조직화(organize), 관리(manage), 연합(combine) 하는 데 사용되는 패턴 - 객체간의 기능을 배분하는 일과 같은 알고리즘 수행에 주로 이용 - 런타임에 따르기 어려운 복잡한 제어 흐름을 결정짓는데 사용 가능	Strategy, Observer, State, Command, Iterator, Template Method, Interpreter 패턴

- 패턴이 수행하는 목적에 따라서 3 가지 유형으로 분류되며 각각의 특성을 지님

■ GoF 의 디자인 패턴 영역의 범위에 따른 분류 별 특성



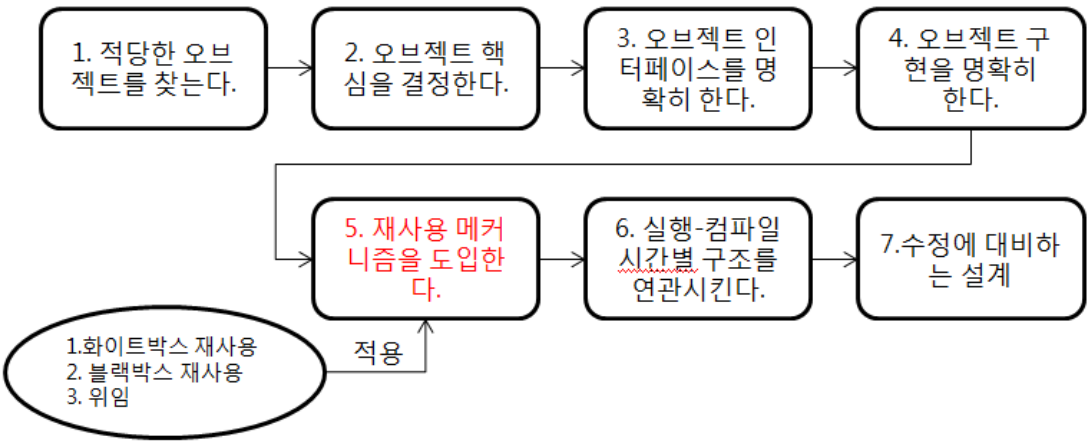
분류	특성	패턴 종류
클래스 패턴	-클래스 간 상속 관계에 대한 정의를 수행하는 패턴 -컴파일 타임에 정적으로 결정됨	Template Method, Factory method, Adaptor, Interpreter
객체 패턴	-객체 사이의 관계를 다루며, 객체 사이의 관계는 보통 구성을 통해서 정의된다. 객체 패턴에서는 일반적으로 실행 중에 관계가 생성되기 때문에 더 동적이고 유연하다.	Strategy, Observer, Decorator, Proxy, Composite, Iterator, State 패턴 등

- 패턴에서 다루고자 하는 영역의 범위에 따라 클래스 패턴과 객체 패턴으로 분류됨

■ 화이트박스 재사용과 블랙 박스 재사용 및 위임의 개념

구분	설명
화이트박스 재사용	-객체 지향 프로그래밍에서 일반화/상세화의 관계나 상속 구조를 통해 클래스의 구현 사항을 재사용하는 기법 -클래스 내부의 내용을 알고 이를 재사용한다는 데에서 화이트박스 재사용이라 함 -재사용한 클래스가 변경이 일어난 경우 이를 이용한 객체에 영향이 큼
블랙 박스 재사용	-객체 인터페이스를 이용하여 객체를 조립하고 결합하여 시스템을 구성하는 방법 -객체 내의 구현은 모른 체 외부적 기능만을 활용하여 재사용한다는 데에서 블랙박스 재사용이라 함 -재사용된 클래스에 변경이 일어난 경우 객체에게 미치는 영향이 상대적으로 작음
위임	-어떤 객체의 조작 일부를 다른 객체에게 넘김(위탁자 -> 수탁자) -상속보다는 위임을 통해 객체간 결합도를 낮추는데 이용됨 -한 객체의 변경이 다른 객체에 미치는 영향이 작아짐

■ **화이트박스 재사용과 블랙 박스 재사용 및 위임과 패턴과의 관계**



<디자인 패턴에서 문제 해결 과정>

- 디자인 패턴의 문제 해결 방법 중 재사용 메커니즘 도입 시에 화이트 박스 재사용과 블랙박스 재사용 및 위임을 적용한다.

기법	적용 방식	적용 패턴
화이트 박스 재사용	-일반화 또는 상세화 및 상속을 통해 객체 재사용 -내부적 메소드 또는 변수를 이용하여 재사용	Adaptor, Decorator 패턴
블랙 박스 재사용	-객체 합성(Composition)을 통해 객체 재사용 -객체 자체의 외부적 기능을 합성하여 재사용	Proxy, Composite 패턴
위임	-객체의 조작 일부를 다른 객체에게 넘겨 수행하도록 함	Adaptor, State, Strategy, Template Method 패턴

"끝"

■ **참고(목적과 범위 별 디자인 패턴 종류)**

		목적		
		생성(Creational)	구조(Structual)	행동(Behavioral)
범위	클래스	Factory Method	Adapter	Interpreter Template Method
	객체	Abstract Factory Builder Prototype Singletone	Adapter Bridge Composite Decorator Façade Flyweight Proxy	Chain of Responsibility Command Iterator Mediator Memento Observer State Strategy Visitor

2	통계 데이터베이스(Statistical Database)
문제	통계 데이터베이스(Statistical Database)에서 통계 질의문(Statistic Query)에 대해 설명하시오. 그리고 다음의 데이터베이스에서 개별추적자(Individual Tracker) 역할을 하는 Query 문을 예를 들어 작성하고, 이러한 개별추적자가 통계 데이터베이스에 미치는 영향에 대해 설명하시오.
도메인	데이터베이스, 보안
정의	데이터베이스 내부의 민감 정보가 보호되고 있음에도 불구하고, 보호되지 않는 다른 데이터에서 추측할 수 있는 데이터를 포함한 데이터 베이스
키워드	SUM, AVG 등 통계함수, 추론
출제의도분석	최근 금융기관의 개인정보 유출 등의 보안 이슈로 인하여 DB 보안의 주요 요구사항인 추론방지에 관하여 출제
답안작성 전략	-통계데이터베이스에 대한 명확한 개념 제시와 질의문 설명 -개별추적자에 대한 사례를 통한 설명과 데이터베이스에 미치는 영향 상세 설명
참고문헌	DB 가이드넷(http://www.dbguide.net) Technical Report - 데이터베이스보안(7) (통계적 DB 보안과 객체중심 DB 보안.pdf)
모범목차	1. 집합과 추론으로의 데이터 접근, 통계 데이터베이스의 개요 가. 통계 데이터베이스의 정의 나. 통계 데이터베이스의 보안 2. 통계 데이터베이스에서의 통계 질의문 가. 통계 질의문에 사용되는 통계 함수 나. 통계 질의문에 사용되는 집합 질의문 3. 개별추적자 Query 문과 개별추적자가 통계 데이터베이스에 미치는 영향 가. 개별추적자의 정의 나. 개별추적자 Query 문 다. 개별추적자가 통계 데이터베이스에 미치는 영향
풀이 기술사님	임항섭 PE (제 102 회 정보관리/ reo_dica@naver.com)

■ 집합과 추론으로의 데이터 접근, 통계 데이터베이스의 개요

가. 통계 데이터베이스의 정의

- 데이터베이스 내부의 민감 정보가 보호되고 있음에도 불구하고, 보호되지 않는 다른 데이터에서 추측할 수 있는 데이터를 포함한 데이터 베이스
- 통계 데이터베이스는 매개변수데이터와 이러한 매개변수에 대한 측정데이터를 포함하여, 매개변수 데이터는 각각 다른 값으로 구성되어 있고, 측정데이터의 다양한 조건하에서 측정 값을 추출할 수 있는 데이터 베이스

나. 통계 데이터베이스의 보안

구분	설명
집합 (Aggregation)	-집합(합계, 횟수)의 보안등급은 통계적 DB 의 낮은 등급에 사용된 기본요소들과 다른 등급에서 정해짐 -보안 등급의 차이에 의하여 집합 질의문을 통해 데이터 식별이 가능

추론 (Inference)	-중요하지 않은 데이터로부터 민감한 정보를 추출 -직접 공격, 간접 공격, 추적 공격, 선형 시스템 취약점 공격 등이 있음

- 정보에 접근을 허용하는 것이 아닌 데이터로 접근제어를 서술하는 메커니즘 때문에 보안문제로 발생됨

■ **통계 데이터베이스에서의 통계 질의문**

가. 통계 질의문에 사용되는 통계 함수

통계 함수	설명	함수 적용 사례
COUNT	-테이블에서 열의 수 또는 행의 수를 결정 -함수 괄호 내부에 * 또는 컬럼을 지정	-COUNT(*) -COUNT(컬럼 명)
MIN/MAX	- 열에서 최소, 최대 값을 결정	-MAX(급여)
SUM	-열에 있는 값들의 합을 결정 -오직 열과 수치 자료형의 수식에만 적용 -행에 있는 열이 오직 NULL 값만을 가지면 결과 값은 NULL	-SUM(성적) -SUM(급여)
AVG	-열에 있는 값들의 산술평균을 결정 -오직 열과 수치 자료형의 수식에만 적용	-AVG(급여)
STDDEV VARRIANCE	-STDDEV 함수는 열의 NULL 값을 제외한 표준편차를 계산하여 값을 결정 -VARIANCE 함수는 열의 NULL 값을 제외한 분산을 계산하여 값을 결정	-STDDEV(급여) -VARRIANCE(성적)

- NULL 값을 가지는 Tuple 은 함수의 계산에 포함되지 않음

나. 통계 질의문에 사용되는 집합 질의문

통계 집합 질의문	설명	질의 적용 사례
GROUP BY	-동일성을 기초하여 여러 개의 행을 그룹화	SELECT SUBSTRING(emp_no,1,4), COUNT(*) FROM EMPLOYEE GROUP BY SUBSTRING(emp _no,1,4)
HAVING	-WHERE 절과 유사한 기능을 가지며, 그룹의 조건을 지정	SELECT emp_no, COUNT(*) FROM EMPLOYEE_EFFORT GROUP BY emp_no HAVING COUNT(*) > 2

- 통계 함수와 집합 질의문을 이용하여 통계 데이터베이스의 민감한 정보를 추론이 가능함.

■ **개별추적자 Query 문과 개별추적자가 통계 데이터베이스에 미치는 영향**

가. 개별추적자(Individual Tracker) 정의

- 단일 Tuple 에 대한 정보를 추적하는 것을 허용하는 주체
- 테이블 내에서 단일 Tuple 에 대한 접근을 허용하는 컬럼 혹은 컬럼 집합(PK, Composite Key)

나. 문제에서의 개별추적자(Individual Tracker) Query 문 예시

Query 문	설명
SELECT SUM(성적) FROM 성적 WHERE 지역 = 'C'	지역 = 'C' 는 학과 전기라는 단일 Tuple 에 대한 정보를 추적하는 것을 허용하는 개별적인 트랙커이며, 학년 4 는 일반적인 트랙커로 정의
SELECT SUM(성적) FROM 성적 WHERE 지역 = 'B' AND 제외(학년='4')	지역 = 'B' AND 제외(학년 = '4')는 전자라는 학과를 추론할 수 있는 개별적인 트랙커로 정의할 수 있으며, 단일 Tuple 에 대한 정보를 추적할 수 있고, 학년 4 를 제외 함으로서 3 학년 중 전자학과의 성적을 추론 가능

- 통계 질의문과 개별 추적자를 이용하여 통계 정보에서 개인의 민감 정보를 추출 가능함.

다. 개별추적자(Individual Tracker 가 통계 데이터베이스에 미치는 영향

영향도	설명
비가용 데이터 간접접근	비인가 사용자가 자신에게 가용한 데이터 X 에 대한 질의로 자신에게 가용하지 않은 데이터 Y 를 추론
상호연관 데이터 접근	사용자에게 가용한 데이터 X 가 가용하지 않은 데이터 Y 와 연관되어 있을 때 상호연관데이터는 전형적인 추론채널
누락데이터 접근	사용자에게 값을 알려주지는 않았지만 데이터의 존재를 암시하는 누락데이터는 추론채널

- 기밀성이 없는 데이터로부터 기밀 정보를 얻어내는 가능성을 이끌어내어 데이터 추론 제공
- 통계적 집계 정보에서 시작하여 개개의 개체에 대한 정보를 추적하지 못하도록 방지

■ 개별추적자에 의한 통계 데이터베이스추론에 대한 대응방안

대응방안	설명
분명하게 민감한 정보에 대한 제한	민감한 정보가 무엇이며 민감한 정보가 어떻게 추론가능한지에 대한 사전 분석을 수행하여 이에 대한 제한을 수행
사용자가 알고 있는 것을 추적	사용자의 행동들은 감사로그로 기록되어지고, 사용자가 누구인지 어떤 그룹에 속하는지 알 수 있도록 고려해야 함
데이터 위장	임의로 치환반복, 교환함으로써 정확성과 용이성 혼란
적절한 데이터 디자인에 적용	속성들 사이의 민감한 관계에 대해 수용하고 DB 구조에 대한 통계적 분석 수행

- 사용자의 의심스러운 행동에 대해 사전에 인식하고 이를 모니터링하여 분석을 수행해야 함

"끝"

3	순방향 에러 발견(Forward Error Detection), CRC 계산
문제	패킷 데이터의 송수신 과정에서 순방향 에러 발견(Forward Error Detection) 절차를 다이어그램을 이용하여 제시하고, 전송 데이터가 1011010, 디바이더(divider)가 1101 인 경우 CRC(Cyclic Redundancy Check) 값을 구하는 과정을 설명하시오.
도메인	디지털네트워크
정의	전송 중 발생한 오류 검출/발견을 위해 에러 검출 코드를 함께 송신측에 보내는 순방향 에러 발견기술 FED, 파일이 전송되는 도중에 손상되었는지를 검사하는 CRC(순환잉여검사).
키워드	FED, FEC, BEC, CRC, divider, party check, check sum, ARQ
출제의도분석	Forward Error Correction, Forward Error Detection, Backward Error Correction 의 차이를 이해하고 CRC 값을 divider 로 부터 계산할 수 있는지의 여부
답안작성 전략	순방향 에러 발견에 대한 정의와 주요 에러 발견 방식을 기술하고, 발견 절차를 다이어 그램으로 제시한다. 주어진 전송 데이터와 디바이더를 이용해 CRC 값을 계산하고 계산된 CRC 값을 검증한다.
참고문헌	http://wikipedia.org
모범목차	순방향 에러 발견의 개요, 주요 발견/검출 방식, 절차 다이어그램, FEC (BEC 와 비교), CRC 계산 값 구하기 과정
풀이 기술사님	송영호 PE (제 102 회 컴퓨터시스템응용/ songyoungho@hanmail.net)

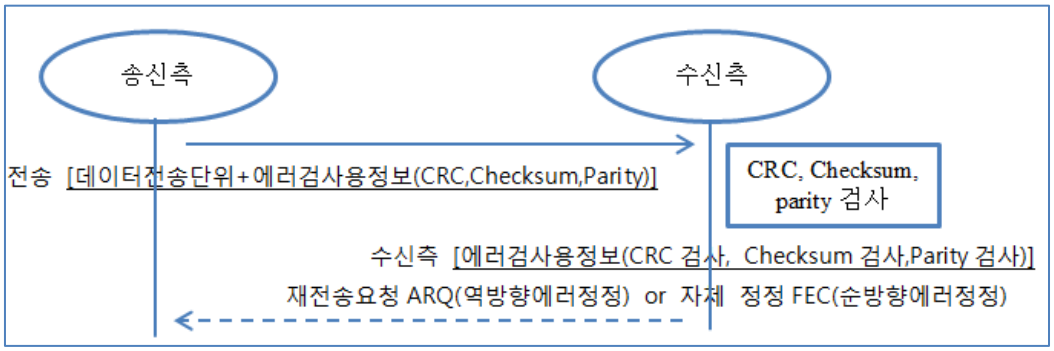
■ **순방향 에러 발견(Forward Error Detection)의 개요**

- 순방향 에러 발견/검출은 단지 전송 중에 발생한 오류의 존재 여부만을 수신측에 알수있도록 하는 기술로 에러를 검출하는 기능을 내재시킨 에러검출 코드를 송신측이 함께 보내는 기술,
- 재전송이 가능한 시스템에서는 오류정정 체계를 갖추지 못하였더라도, 단지 오류의 검출만으로도 오류제어가 충분한 경우가 많음.
- 오류의 정정이 필요 시 에러정정부호화 FEC(순방향에러정정)를 사용함.

■ **주요 에러 발견/검출 방식**

주요방식	설명
패리티검사	- Parity Check, 정보비트수가 적고 에러발생 확률이 낮은 경우 가장 많이 사용하는 에러 검출 방식. - 어느 비트에 오류가 발생하였는지 알 수 없고, 짝수 개의 오류가 발생하면 오류검출이 불가능한 단점. 구현이 간단하여 비동기 통신에 많이 이용.
검사합	- Checksum, 간단하게 에러감출을 하는 방식. -송신측에서 전송할 모든 데이터를 1 비트 워드 단위로 구분하고, 1 의 보수를 취하고 그 합에 대한 결과를 전송하면, 수신측에서 같은 합을 해보아 오류를 검출하는 방식
순환중복검사	- CRC, 송신측에서 데이터로부터 다항식에 의해 나온 결과를 여분의 오류검사필드에 덧붙여 보내면, 수신측에서는 동일한 방법으로 추출한 결과와의 일치성으로 오류룰 검사하는 기술

■ **순방향 에러 발견 절차 다이어그램**



[순방향 에러 발견 절차 다이어그램]

- 절차

1) 송신측에서 데이터 전송단위만큼의 데이터와 에러 검사용 정보(CRC, Check sum, Parity bit 값 등)를 함께 전송

2) 수신측에서는 전송 받은 데이터의 CRC 검사, Check sum 검사, Parity bit 검사 등을 통해 비트의 오류를 검출

3) FEC(순방향 에러 정정)의 경우 추가된 정보를 기반으로 수신 받은 데이터의 오류를 직접 정정할 수도 있고, ARQ(역방향 에러정정)의 경우 재 전송요청을 통해 송신지로 부터 새로운 데이터를 수신 받게 됨

■ **순방향 오류 정정 (FEC: Forward Error Correction)**

- 수신측에서 에러의 검출 및 수정을 담당하는 방법으로 에러검출 후 수정을 위해 특별히 추가된 코드(error correct code)를 계산하여 추가 전송하는 기법.
- 수신측에서 부가된 비트를 이용하여 오류검사 및 정정을 담당하게됨.
- FEC 와 BEC 간의 차이

비고	FEC (전진/순방향 에러수정)	BEC(후진/역방향 에러수정)
정의	- 송신측의 부가정보를 기반으로 수신측에서 에러를 검출하고 자체 정정하는 방식	- 송신측이 에러를 검출할 수 있을 정도의 부가적인 정보를 문자나 프레임에 첨가시켜 전송하고 수신측이 에러 발견시 재전송을 송신측에 요구하는 방식
종류	- Hamming Code, CRC Code BCH Code, Reed0Solomon Code, Convolutional Code, Turbo Code 등	- ARQ(검출 후 재전송방식), Stop-and-wait ARQ, Go-Back-N ARQ, Selective Repeat ARQ 등

■ **전송 데이터가 1011010, 디바이더(divider)가 1101 인 경우 CRC(Cyclic Redundancy Check)값 구하는 과정**

- *n*-bit 이진 CRC 계산을 위한 (*n*+1)-bit divider 가 1101(4bit)인 다항식은 $1x^3 + 1x^2 + 0x + 1$ 로, 다음과 같은 CRC 계산을 위한 테이블을 만들 수 있다.

다항식	제수	비트수	CRC
$1x^3 + 1x^2 + 0x + 1$	1101	4bit	3bit

즉, 3-bit 이진 CRC 를 계산하기 위해 divider 로 나누는 과정을 반복하면,

전송데이터:

1011010 000
1101 ← 제수(divider) 4bit

0110010 000 ← 결과
1101 ← 제수(divider) 4bit

0000110 000 ← 결과
110 1 ← 제수(divider) 4bit

0000000 **100** ← 나머지 3bit, 앞에있는 데이터가 모두 0 이되고 뒤에 3bit 가 최종 CRC 값.

- CRC 값 계산 검증
계산 결과의 검증을 위해 입력 전송데이터 다음에 CRC 결과를 붙여 divider 로 나누어 0 이 되는지 확인.

1011010 100
1101

0110010 100
1101

0000110 100
110 1
---
0 ← 나머지 0

"끝"

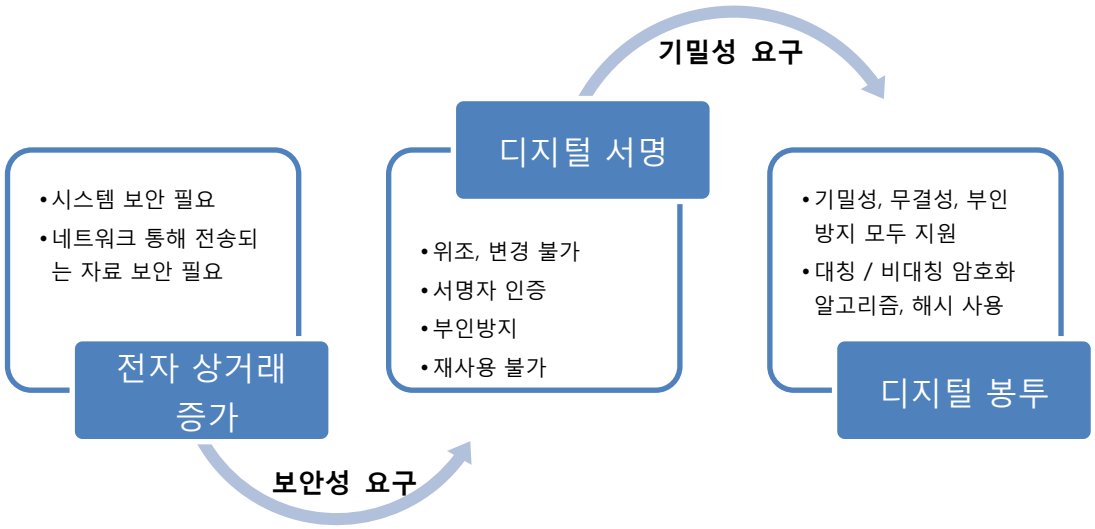
4	디지털봉투

문제	디지털봉투(Digital Envelopes) 출현 배경을 설명하고, 디지털봉투를 생성하고 개봉하는 과정을 그림을 이용하여 구체적으로 설명하시오.
도메인	정보보안
정의	송신자의 키(비밀)로 전자 서명된 메시지를 비밀키로 암호화 하여 기밀성을 보장하기 위한 기법.
키워드	디지털 서명, 비밀키, 공개키, 사설키
출제의도분석	암호화 알고리즘을 이용한 전자 상거래 정보 보호 기법의 기본 이론
답안작성 전략	디지털 봉투 출현 배경과 디지털 봉투 생성, 개봉 과정을 상세하고 정확하게 작성
참고문헌	KPC 모의고사(8 회-4), IT CookBook, 정보 보안 개론(한빛미디어)
모범목차	1. 디지털봉투 출현배경 2. 디지털봉투 생성과정 3. 디지털봉투 개봉과정 4. 디지털봉투 사용시 고려사항
풀이 기술사님	정상미 PE (제 101 회 정보관리/ jsm1111111@naver.com)

■ **디지털 봉투 출현 배경**

가. 디지털 봉투의 출현 배경

- 암호화를 이용한 전자상거래의 전자 서명의 기밀성 보완한 디지털 봉투 출현



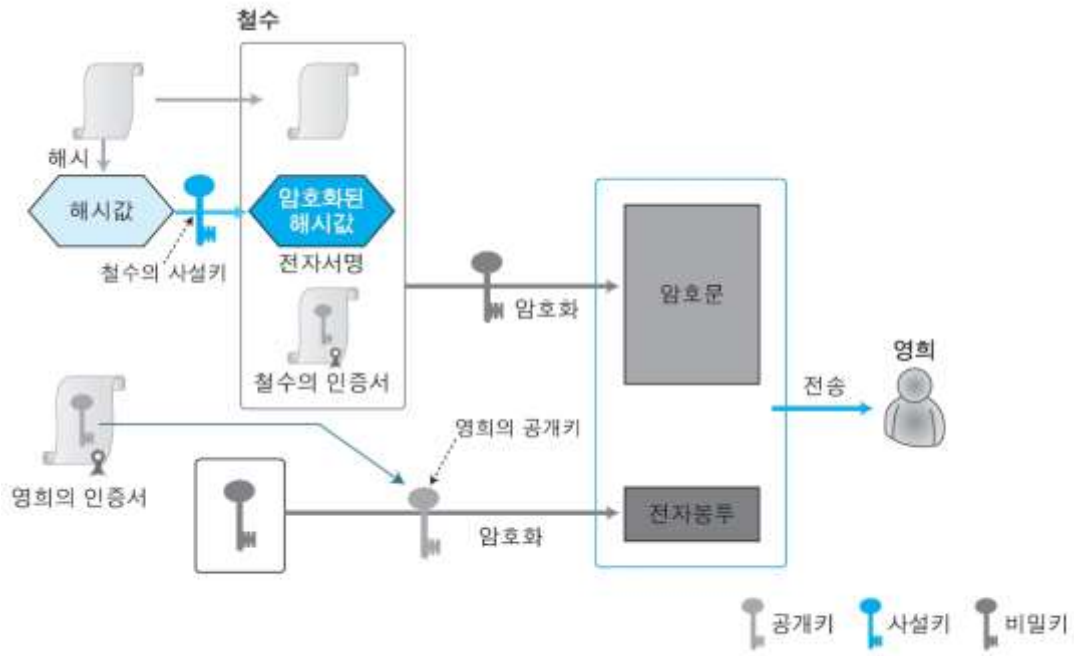
나. 디지털 봉투의 정의

- 송신자의 키(비밀)로 전자 서명된 메시지를 비밀키로 암호화 하여 기밀성을 보장하기 기법.
- 전달하고자 하는 메시지를 암호화하여 한 사람을 통해서 보내고, 암호화 키는 다른 사람에게 가져가게 하는 것을 암호학적으로 구현한 것.

■ **디지털 봉투 생성 과정**

가. 디지털 봉투 생성 과정 구성도

- 철수가 영희에게 데이터를 전송하면서 디지털 봉투를 생성하는 암호화 과정.



[그림 8-10] 전자봉투를 이용한 암호화 전송

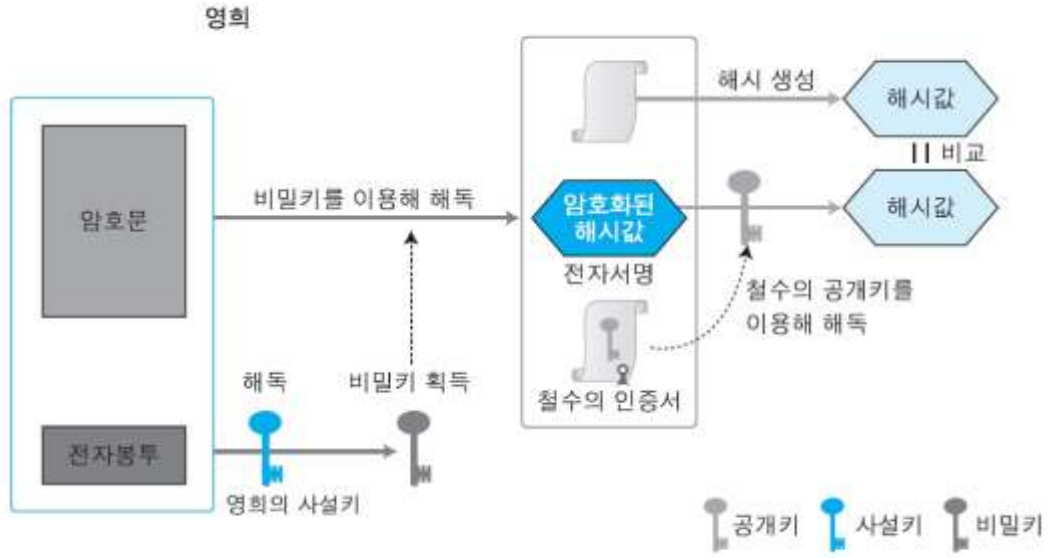
나. 디지털 봉투 생성 과정

과정	설명
1. 전자 서명 생성	전자봉투를 사용하기 위해 우선 해시값을 이용하여 전자서명을 생성하고.
2. 비밀키로 암호화	전자서명과 원문, 그리고 자신의 공개키가 들어있는 인증서(철수의 인증서)를 비밀키(DES 알고리즘 등에 사용되는 대칭키)를 사용하여 암호화
3. 수신자의 공개키로 암호화 (디지털 봉투 생성)	전자서명 세트와 인증서를 암호화한 비밀키를 영희의 공개키로 암호화하는데, 이것이 전자봉투가 됨
4. 암호문과 디지털 봉투 전송	철수는 최종적으로 비밀키로 암호화한 결과와 비밀키가 암호화된 전자봉투를 영희에게 보냄.

■ **디지털 봉투 개봉 과정**

가. 디지털 봉투 개봉 과정 구성도

- 영희가 철수에게서 받은 데이터를 디지털 봉투에서 개봉하는 복호화 과정.



[그림 8-11] 전자봉투의 복호화

나. 디지털 봉투 개봉 과정

과정	설명
1. 송신자 사설키로 디지털 봉투 복호화	전달받은 영희(수신자)는 우선 디지털봉투를 자신의 사설키로 복호화하여 비밀키를 획득.
2. 비밀키로 암호문 복호화	비밀키를 이용하여 전자서명과 평문, 철수의 인증서를 복호화 (해독).
3. 철수의 공개키로 해시값 비교	복호화한 인증서에서 철수의 공개키를 얻어 전자서명을 복호화한 후 이를 원문 해시 결과와 비교

"끝"

5	개인정보 보호
문제	개인정보의 개념과 국내 개인정보 법률을 설명하고, 빅데이터 등 신 산업 육성 시 규제측면의 고려 사항에 대해 제시하시오.
도메인	정보보안
정의	개인정보: 성명, 주민번호 등을 통하여 살아있는 개인을 알아볼 수 있는 정보와 다른 정보와 용이하게 결합하여 개인을 알아볼 수 있는 정보
키워드	정보보호 개인정보보호 법률, 주요 위협사례와 대응전략
출제의도분석	2014 년 8 월 개인정보보 보호법 개정안 시행과 더불어 전자정부법 개정안에서 정부 3.0 의 빅데이터 활용을 두고 있음
답안작성 전략	개인정보 개념을 법률에서 정의한 내용으로 작성하고 국내 개인 정보 관련 법률들과 상호간의 관계 설명 마지막으로 신사업 육성 시 규제 측면의 고려사항을 다양한 각도에서 제시
참고문헌	개인정보보호 종합지원 포탈(privacy.go.kr) 개인정보보호 관련 규제체계와 주요 이슈(정보통신방송정책 25 권)
모범목차	1. 개인정보 개념 2. 국내 개인정보 법률 3. 신사업 육성에 따른 개인정보 규제 고려사항
풀이 기술사님	정상미 PE (제 101 회 정보관리/ jsm1111111@naver.com)

■ 개인정보의 개념

가. 개인 정보의 정의

- 성명, 주민번호 등을 통하여 살아있는 개인을 알아볼 수 있는 정보와 컴퓨터 IP 주소, e-mail 등 다른 정보와 용이하게 결합하여 개인을 알아볼 수 있는 정보

나. 법률상 개인정보의 정의

구분	내용
개인정보 보호법	(제 2 조 1) "개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다).
정보통신망 이용촉진 및 정보보호 등에 관한 법률	(제 2 조 6) "개인정보"란 생존하는 개인에 관한 정보로서 성명 . 주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호 . 문자 . 음성 . 음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)
신용정보의 이용 및 보호에 관한 법률	(제 2 조 1) "신용정보"란 금융거래 등 상거래에 있어서 거래 상대방의 신용을 판 단할 때 필요한 다음 각 목의 정보로서 대통령령으로 정하는 정보. 가. 특정 신용정보주체를 식별할 수 있는 정보 나. 신용정보주체의 거래내용을 판단할 수 있는 정보 다. 신용정보주체의 신용도를 판단할 수 있는 정보 라. 신용정보주체의 신용거래능력을 판단할 수 있는 정보 마. 그 밖에 가목부터 라목까지와 유사한 정보

위치정보의 정호 및 이용 등에 관한 법률	(제 2 조 2) "개인위치정보"라 함은 특정 개인의 위치정보(위치정보만으로는 특정 개인의 위치를 알 수 없는 경우에도 다른 정보와 용이하게 결합하여 특정 개인의 위치를 알 수 있는 것을 포함한다)

■ **개인정보 법률**

가. 국내 개인정보 보호 관련 법률

- 소관부처에 따라 개인정보에 관한 법률을 대상과 기관에 따라 제정

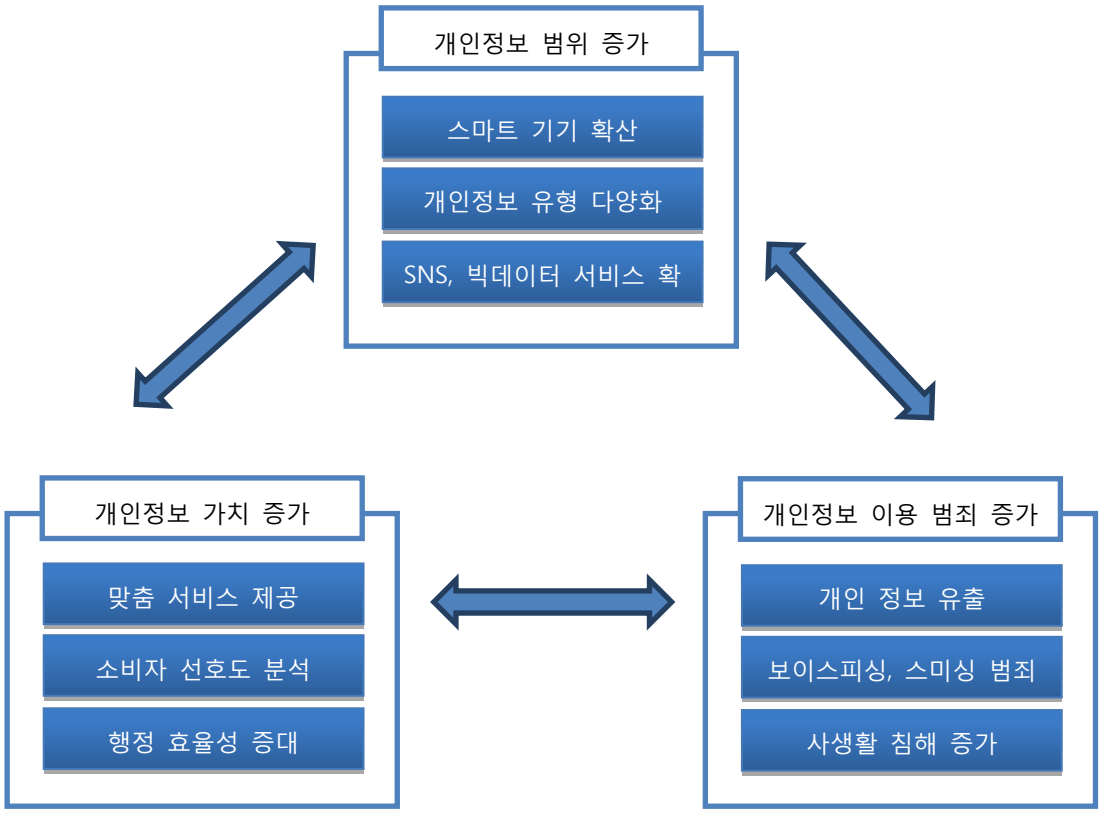
소관부처	법률	설명
안전행정부	개인정보 보호법	개인정보의 수집·유출·오용·남용으로부터 사생활의 비밀 등을 보호함으로써 국민의 권리와 이익을 증진하고, 나아가 개인의 존엄과 가치를 구현하기 위하여 개인정보 처리에 관한 사항을 규정함 목적
	전자정부법	행정업무의 전자적 처리를 위한 기본원칙, 절차 및 추진방법 등을 규정함으로써 전자정부를 효율적으로 구현하고, 행정의 생산성, 투명성 및 민주성을 높여 국민의 삶의 질을 향상시키는 것을 목적
	전자서명법	전자문서의 안전성과 신뢰성을 확보하고 그 이용을 활성화하기 위하여 전자서명에 관한 기본적인 사항을 정함으로써 국가사회의 정보화를 촉진하고 국민생활의 편익을 증진함을 목적
	주민등록법	시·군 또는 구의 주민을 등록하게 함으로써 주민의 거주관계 등 인구의 동태(動態)를 항상 명확하게 파악하여 주민생활의 편익을 증진시키고 행정사무를 적정하게 처리하도록 하는 것을 목적
	지방공기업법	지방자치단체가 직접 설치/경영하거나, 법인을 설립하여 경영하는 기업의 운영에 필요한 사항을 정하여 그 경영을 합리화함으로써 지방자치의 발전과 주민복리의 증진에 이바지함을 목적
	공공기관의 정보공개에 관한 법률	공공기관이 보유·관리하는 정보에 대한 국민의 공개 청구 및 공공기관의 공개 의무에 관하여 필요한 사항을 정함으로써 국민의 알 권리를 보장하고 국정(國政)에 대한 국민의 참여와 국정 운영의 투명성을 확보함을 목적
방송통신위원회	정보통신망 이용 촉진 및 정보보호에 관한 법률	보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함을 목적
	위치정보의 정호 및 이용 등에 관한 법률	위치정보의 유출·오용 및 남용으로부터 사생활의 비밀 등을 보호하고 위치정보의 안전한 이용환경을 조성하여 위치정보의 이용을 활성화함으로써 국민생활의 향상과 공공복리의 증진에 이바지함 목적
금융위원회	신용정보의 이용 및 보호에	신용정보업을 건전하게 육성하고 신용정보의 효율적 이용과 체계적 관리를 도모하며 신용정보의 오용·남용으로부터 사생

	관한 법률	활의 비밀 등을 적절히 보호함으로써 건전한 신용질서의 확립에 이바지함 목적
국가인권위원회	국가인권위원회 법	국가인권위원회를 설립하여 모든 개인이 가지는 불가침의 기본적 인권을 보호하고 그 수준을 향상시킴으로써 인간으로서의 존엄과 가치를 실현하고 민주적 기본질서의 확립에 이바지함을 목적
기획재정부	공공기관의 운영에 관한 법률	공공기관의 운영에 관한 기본적인 사항과 자율경영 및 책임경영체제의 확립에 관하여 필요한 사항을 정하여 경영을 합리화하고 운영의 투명성을 제고함으로써 공공기관의 대국민 서비스 증진에 기여함을 목적
교육부	초·중등교육법	「교육기본법」 제 9 조에 따라 초·중등교육에 관한 사항 정함을 목적
	고등교육법	「교육기본법」 제 9 조에 따라 고등교육에 관한 사항을 정함을 목적

나. 개인정보 법과 개별법과 관계

- 개인정보보호 관련 다른 법률에 특별한 규정이 있는 경우, 해당 조항을 우선적으로 적용

■ **신사업 육성에 따른 개인정보 규제의 고려사항**



가. 개인정보 규제측면에서 필요성

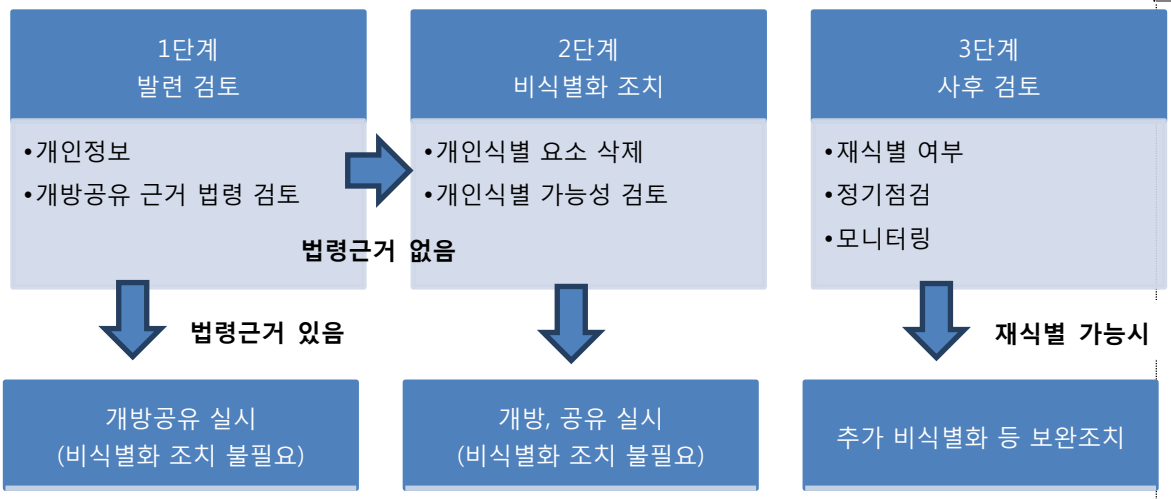
- 신사업 육성에 따라 기존의 개인 정보 범위가 증가하고 개인 정보를 이용한 서비스와 범죄가 동시에 증가 하는 현상 발생

나. 신사업 육성시 규제 측면의 단계별 고려사항

단계	설명
수집이용	-법령 근거 또는 정보주체 동의에 의해 수집 . 이용 -인터넷, 언론 등에 공개된 개인정보는 사회 통념상 공개된 목적 범위 내 수집 . 이용
분석	-개인 식별 가능한 정보는 삭제 또는 비식별화 후 분석(빅데이터 등) -개인정보 활용이 불가피한 경우 당초 수집 목적 범위 내에서 분석
제공(공유)	-목적 내 제 3 자 제공(공유)시에는 필요 최소한으로 제한 -목적 외 제 3 자 제공(공유)시에는 법률 근거 또는 별도 동의 필요
개방(공개)	-원칙적으로 개인정보는 배제, 비식별화 처리 후 개방 -법률 근거 또는 정보주체 동의하에 제한적으로 개방 가능
관리	-주민등록번호 등 중요정보는 암호화 -개인정보 필터링, 재식별 여부 모니터링 등 안전조치

다. 개인정보 비식별화 기준 관련 규제

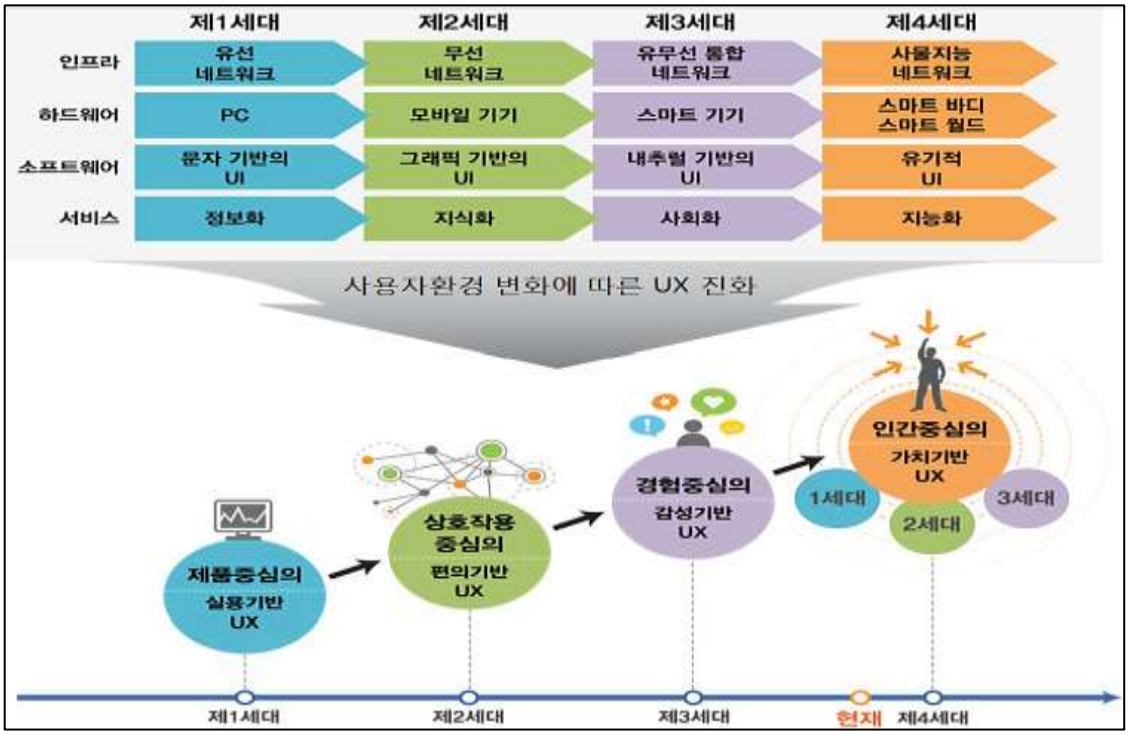
- 클라우드 컴퓨팅을 기반한 SNS, 빅데이터 등의 기술에 의한 개인정보 식별 기준이 변경이 될 수 있음.


1단계
발련 검토
•개인정보
•개방공유 근거 법령 검토
2단계
비식별화 조치
•개인식별 요소 삭제
•개인식별 가능성 검토
3단계
사후 검토
•재식별 여부
•정기점검
•모니터링
법령근거 없음
법령근거 있음
재식별 가능시
개방공유 실시
(비식별화 조치 불필요)
개방, 공유 실시
(비식별화 조치 불필요)
추가 비식별화 등 보완조치

"끝"

6	사용자경험(User Experience)
문제	**사용자경험(User Experience) 패러다임의 진화를 4 세대로 나누어 각 세대별 특징 및 내용을 설명하고, 주요 이슈를 제시하시오.**
도메인	소프트웨어
정의	제품, 시스템, 서비스 등을 사용자가 직간접적으로 경험하면서 느끼고 생각하는 총체적 경험
키워드	**CLI, GUI, NUI, OUI**
출제의도분석	ICT 융합이 보편화 되면서 UX 가 창출하는 부가가치가 모든 산업에서 더욱더 증대되고 있고, 차세대 경쟁의 핵심으로 부상, 관련 배경지식을 물어보는 문제임
답안작성 전략	세대별 UX 키워드를 제시 및 3 가지 질문에 대해 집중한 목차 및 답안작성
참고문헌	-IT 발달에 따른 사용자경험(UX)패러다임 변화와 발전방향-NIA(2012) -고객중심 경영의 요체, 사용자경험(UX)-삼성경제연구소(2013)
모범목차	1. 제 1 세대~제 4 세대 사용자경험(UX) 패러다임의 진화 개념도 - [도] 세대별 진화 개념도 2. 사용자경험(UX) 패러다임의 세대별 특징 - [표] 1 세대(CLI), 2 세대(GUI), 3 세대(NUI), 4 세대(OUI) 3. 사용자경험(UX) 패러다임의 세대별 주요내용 - [표] 세대별 인프라, H/W, S/W, 서비스관점의 사용자 경험 진화 4. 사용자경험(UX) 패러다임의 진화에 따른 주요 이슈 및 해결방안 가. [표] 사용자경험(UX) 주요 이슈 제기 나. [표 or 도] 사용자경험(UX) 주요 이슈 해결을 위한 실천과제 제안
풀이 기술사님	박상욱 PE (제 99 회 정보관리/ studygosu@gmail.com)

■ **제 1 세대~제 4 세대 사용자경험(UX) 패러다임의 진화 개념도**



- IT 발달(인프라, 하드웨어, 소프트웨어, 서비스)과 경제,사회 변화에 따른 사용자 환경에서 사용자의 수요와 행태를 반영하는 방향으로 세대별 UX 패러다임은 진화해 옴

■ **사용자경험(UX) 패러다임의 세대별 특징**

세대	특징 진화	설명
제 1 세대	**- CLI (Command line Interface)** - 제품 중심의 실용기반	- 사용자가 제공자의 의도대로 제품을 효과적으로 사용하고 얻게 되는 실용기반의 경험이 중시
제 2 세대	**- GUI (Graphical user interface)** - 상호작용 중심의 편의기반	- 사용자가 제품과의 일대일 관계에서 벗어나, 연결이 확장된 환경에서 원활한 상호작용을 통해 얻게 되는 편의기반의 경험이 중시
제 3 세대	**- NUI (Natural User Interface)** - 경험 중심의 감성기반	- 사용자가 자신의 수요와 개인적 특성, 이용목적 등에 따라 즐겁고 행복하게 제품을 사용하면서 얻게 되는 감성기반의 경험이 중시
제 4 세대	**- OUI (Organic User Interface)** - 인간 중심의 가치기반	- 사용자가 고도로 지능화된 세상에서 라이프스타일에 따라 의식하지 않아도 저절로 제공되는 제품을 통해 얻게되는 가치기반의 경험이 중시

- 사용자경험(UX) 패러다임의 세대별 특징은 인프라, H/W, S/W, 서비스 측면의 진화내용이 존재함

■ **사용자경험(UX) 패러다임의 세대별 내용**

세대	구분	사용자경험 진화	사용자환경 예
제 1 세대	인프라	- **제한된 사용자경험**	유선 네트워크
	H/W	- **한정된 사용자경험**	PC
	S/W	- **어렵고 낯선 사용자경험**	**CLI 인터페이스**
	서비스	- **유익한 사용자경험**	정보화 진행
제 2 세대	인프라	- **확장된 사용자경험**	무선 네트워크
	H/W	- **동적인 사용자경험**	모바일 기기
	S/W	- **쉽고 편리한 사용자경험**	**GUI 인터페이스**
	서비스	- **지적인 사용자경험**	지식화
제 3 세대	인프라	- **풍부한 사용자경험**	유무선 통합 네트워크
	H/W	- **향상된 사용자경험**	스마트 기기
	S/W	- **직관적인 사용자경험**	**NUI 인터페이스**
	서비스	- **사회적인 사용자경험**	사회화
제 4 세대	인프라	- **수고스럽지 않은 사용자경험**	M2M, IoT 네트워크
	H/W	- **스마트한 사용자경험**	스마트바디, 스마트월드
	S/W	- **실재감 있는 사용자경험**	**OUI 인터페이스**
	서비스	- **개인화된 사용자경험**	지능화

■ **사용자경험(UX) 패러다임의 진화에 따른 주요 이슈**

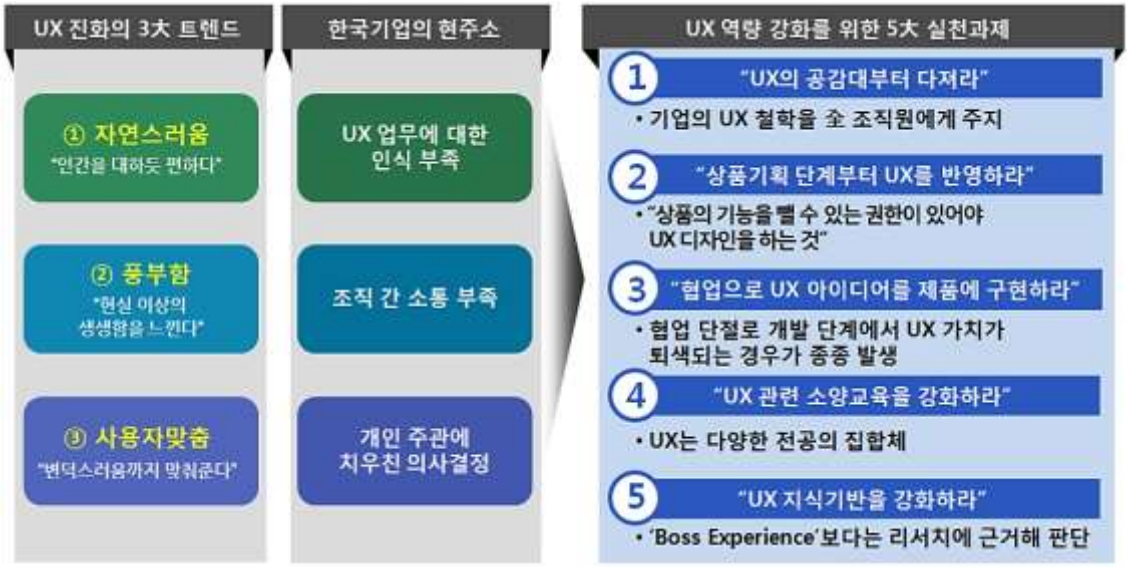
가. 사용자경험(UX) 주요 이슈 제기

주요이슈	설명
공공분야 UX 활용 미비	- 민간부문, 학계등에 비해 공공서비스 분야의 UX 도입과 활용은 미비 - 인지도 높은 민간포털, 서비스와의 품질격차가 심화되면서 정책효과

	감소에 영향
법제도적 전략마련 시급	- 중소기업과 UX 전문기업의 기술력과 역량 육성, 지적재산권 등 부재 - 법제도적 차원의 시의적절한 정비등에 대한 전략마련이 필요
선제적 산업 육성전략 필요	- 지속가능한 성장을 위한 선제적 산업 육성 전략 필요 - 지속가능한 상생을 위한 UX 산업 생태계 구축 - 기초 연구와 UX 기술 고도화를 위한 R&D 필요
전문가 육성책 마련	- 디자인, 심리학, 인문학, 인지공학 등의 융합 현상 강화 전망으로 학계간 협업 및 해당 전문가 육성

- 공급자 중심의 서비스 제공방식의 한계가 드러나면서, 사용자의 요구와 행동을 이해하고 즐거운 경험과 가치를 줄 수 있는 UX에 대한 고민이 이슈의 핵심으로 부상함

나. 사용자경험(UX) 주요 이슈 해결을 위한 실천과제 제안



- 최고 경영자 주도의 UX 리더십하에 가치있는 UX 발굴, 구현 및 UX 중심의 조직운영체계 정비
- 실천과제를 통해 사용자관점에서 제품을 기획, 출시하는 'UX 기반 경영' 구사가 가능해 질 수 있음

"끝"

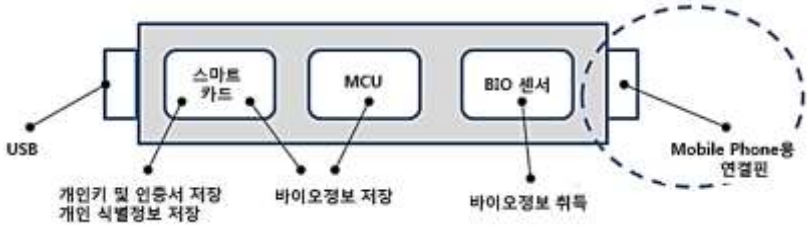
1	모바일 바이오인식(Mobile Biometrics)
문제	**모바일 바이오인식(Mobile Biometrics) 기법의 하나인 바이오(Bio) 보안 토큰에 대해 설명하고, 국제 표준에 따른 모바일 기반 바이오 인식기술 사용 서비스를 위한 인증 모델 및 보안 위협에 대해 설명하시오.**
도메인	정보보안
정의	모바일 환경을 기반으로, 사람의 고유한 바이오정보를 이용하여 신원 확인 시, 그 사람의 ID 에 해당하는 저장된 특징과 입력된 특징을 비교(1:1 비교)하는 기술
키워드	-바이오토큰: **구성(BIO 센서, MCU, 보안토큰, USB, 연결핀), 표준(ITU-T X.1085/X.bhsm)** -모바일 바이오 인증모델: **모델(1~12), 표준(ITU-T X.1087/X.tam)**
출제의도분석	바이오인증(89 응) 1 교시형 문제에 대한 심화로, 국내(TTA)주관 국제표준 이해배경
답안작성 전략	바이오 인식으로 일반화하여 작성하는 것은 금물이고, 모바일 바이오 인식의 국제표준(ITU-T X.1087/X.tam)에서 제시하는 주요 모델기반 답안작성이 필요함
참고문헌	- 바이오 보안토큰을 이용한 프라이버시 보호형 사용자 인증기법- 정보보호학회논문집(2012,신용녀) - 텔레바이오인식 보안기술 국제표준화 동향 분석-KISA(2013,한양사이버대학) - 스마트폰 환경에서의 바이오인식 보안-KISA(2011,한양사이버대학)
모범목차	1. 바이오 보안토큰(BHSM: Biometric Hardware Security Module) 설명 가. [도] 바이오 보안토큰의 개념도 - 개념도 아래 간글로 바이오 보안토큰 개념 설명 나. 바이오 보안토큰의 구성요소 2. 국제표준(ITU-T X.1087/X.tam)에 따른 모바일 바이오 인증모델 - [표] ITU-T X.1087/X.tam 에서 제시하는 인증모델 1~12 중 주요모델 (도 + 설명) 3. 모바일 바이오 인증모델 보안위협 및 대응방안 - [표] 2 단락에서 제시한 모델별 보안위협 대응방안 (3 단표) 4. (선택) 바이오 보안토큰(BHSM)의 운영요구사항 및 보안요구사항
풀이 기술사님	박상욱 PE (제 99 회 정보관리/ studygosu@gmail.com)

■ **바이오(Bio) 보안토큰 설명**

가. 바이오 보안토큰(BHSM: Biometric Hardware Security Module)의 개념

- 바이오 인식 센서와 바이오인식 정보를 처리할 수 있는 MCU(Microcontroller Unit), 스마트카드로 구성된 USB 형태의 하드웨어 기기
- 기기내부의 바이오인식 센서로 가입자의 바이오인식 정보를 추출하여 보안토큰에 안전하게 저장하며, 사용자 인증 시 바이오인식 센서로 부터 취득된 바이오인식 정보와 저장되어 있는 바이오 인식 정보를 기기내부 MCU 에서 매칭하여 사용자를 인증하는 독립된 하드웨어 보안모듈

나. 바이오 보안토큰의 구성도 및 구성요소

구분	내용
구성도	

구성 요소	BIO 센서	- 생체정보 인식
	MCU	- 바이오 정보 처리
	보안토큰	- 개인키, 공인인증서, 개인 식별정보 저장
	USB	- PC 단말에 연결하기 위한 부가장치
	연결핀	- 모바일용 바이오 보안토큰에만 적용됨

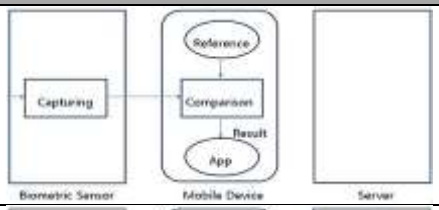
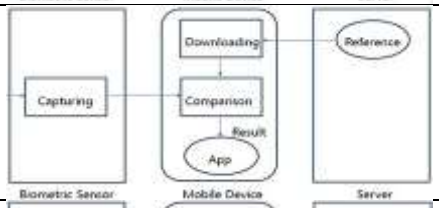
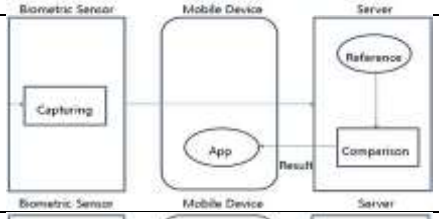
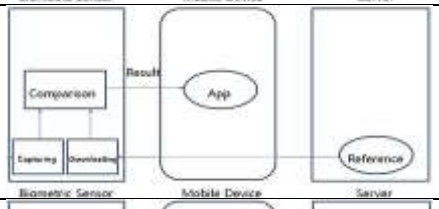
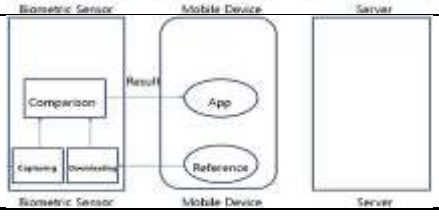
- **ITU-T X.1085/X.bhsm** (ITU-T SG17 Q.9 X.1085/X.bhsm)에서 기존 공인인증서와 바이오 보안토큰과의 프로토콜 및 인증 프레임워크를 개발중이며, ISO/IEC 17922 (ISO/IEC JTC1 SC27 17922)와 공동으로 국제표준화 진행 중임
- X.bhsm: Telebiometric authentication framework using biometric hardware security module

■ **국제 표준기반 모바일 바이오 인식 인증 모델 설명**

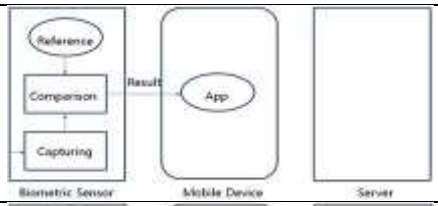
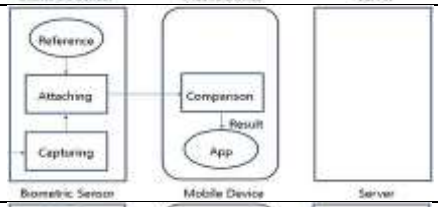
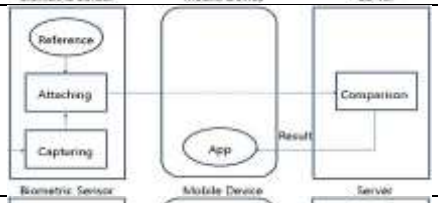
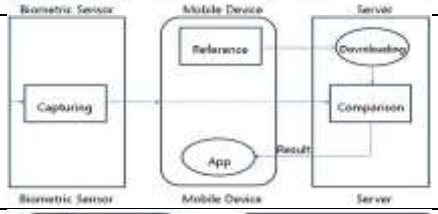
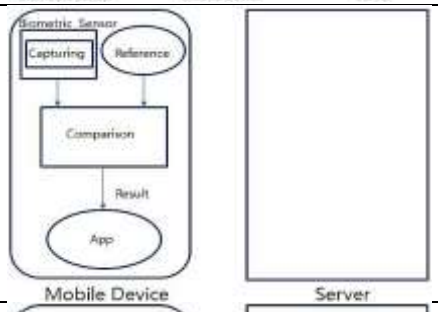
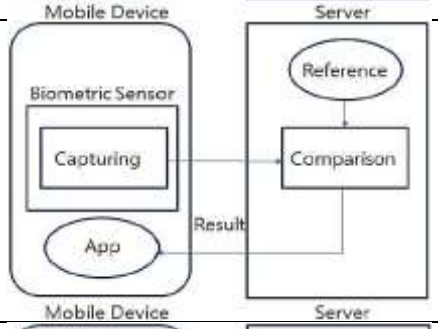
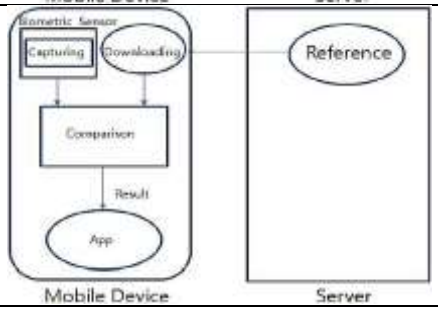
가. ITU-T X.1087/X.tam (ITU-T SG17 Q.9 X.1087/X.tam) 개요

- **모바일 기반 바이오 인식기술 사용 서비스를 위한 인증 모델** 및 보안 위협, 대응방안을 제시하는 기술적 관리적 가이드라인을 제시하는 국제표준
- X.tam: A guideline to technical and operational countermeasures for telebiometric applications using mobile devices (2014.08 현재 5th Draft of Recomm. 임)

나. X.tam 인증 12 개 모델 설명

모델	개념도	Layer 별 기능		
		바이오센서	모바일디바이스	서버
Model1		Capturing	Comparison Store*	
Model2		Capturing	Comparison	Store
Model3		Capturing		Comparison Store
Model4		Capturing Comparison		Store
Model5		Capturing Comparison	Store	

실제 답안 작성시는 주요 모델 3~4 개 위주로 작성
(예: 모델 1,3,8,11)

Model6		Capturing Comparison Store	Comparison	
Model7		Capturing Store		
Model8		Capturing Store		Compariso n
Model9		Capturing	Store	Compariso n
Model1 0			Capturing Comparison Store	
Model1 1			Capturing	Compariso n Store
Model1 2			Capturing Comparison	Store

- Store: Biometric reference template location
- 모바일 기반 바이오인식 인증 모델별 보안위협을 고려하여 적용해야 함

■ 모바일 바이오 인식 인증 모델의 보안위협 및 대응방안

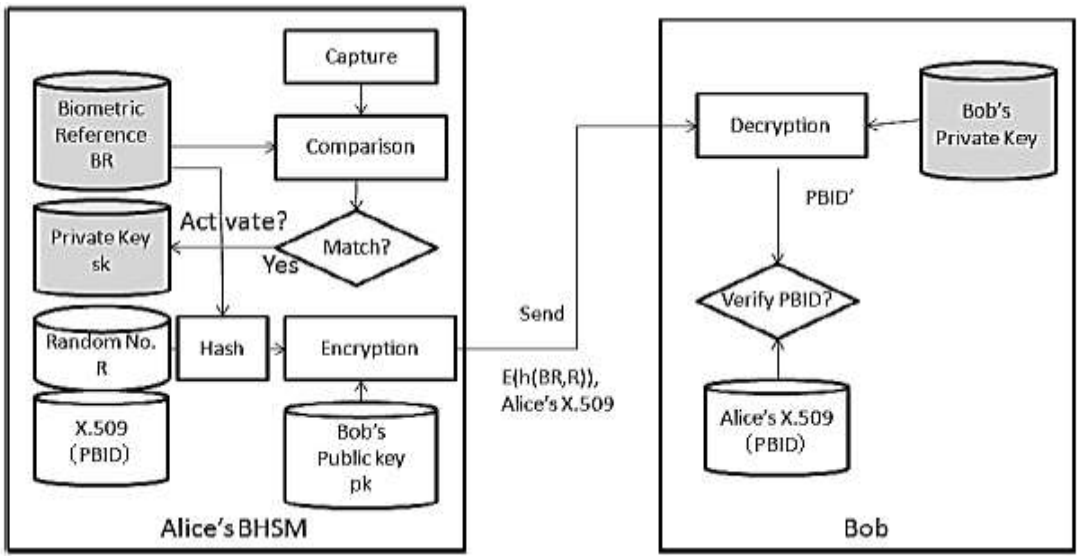
인증모델	보안위협	대응방안
Model1	- 허용되지 않은 센서를 통한 자료 수집 - 바이오 DB 자료의 오용 - 오염된 바이오 DB 자료를 통한 잘못된 비교 - 모바일 장치의 분실 등을 통한 바이오 DB 정보의 유출	- 센서와 모바일장치 상호 인증 - 바이오 DB 의 암호화
Model2	- 허용되지 않은 센서를 통한 자료 수집 - 잘못된 캡쳐 바이오 정보의 전송 - 바이오 DB 자료의 오용 - 오염된 바이오 DB 자료를 통한 잘못된 비교 - 바이오 DB 정보의 유출 - 잘못된 서버 사용 - 모바일 장치의 분실 등을 통한 바이오 DB 정보의 유출 - 캡쳐 후 수집되는 바이오 정보에 대한 서버 집중화로 대량의 바이오 정보 유출 가능	- 센서, 모바일 장치, 서버에 대한 인증 - 전송 채널 암호화 - 바이오 DB 의 암호화 - 전송된 자료 암호화
Model3	- 허용되지 않은 센서를 통한 자료 수집 - 잘못된 캡쳐 바이오 정보의 전송 - 전송 채널에 대한 공격 - 잘못된 서버 사용 - 캡쳐 후 수집되는 바이오 정보에 대한 서버 집중화로 대량의 바이오 정보 유출가능	- 센서, 서버에 대한 인증 - 전송 채널 암호화 - 전송된 자료 암호화
Model4	- 허용되지 않는 센서를 통한 자료 수집 - 바이오 DB 자료의 오용 - 오염된 바이오 DB 자료를 통한 잘못된 비교 - 센서의 분실을 통한 바이오 DB 자료의 유출 - 전송 채널에 대한 공격 - 캡쳐 후 수집되는 바이오 정보에 대한 서버 집중화로 대량의 바이오 정보 유출 가능	- 센서, 서버에 대한 인증 - 바이오 DB 의 암호화 - 전송 채널 암호화 - 전송된 자료 암호화
Model5	- 허용되지 않는 센서를 통한 자료 수집 - 바이오 DB 자료의 오용 - 오염된 바이오 DB 자료를 통한 잘못된 비교 - 센서의 분실을 통한 바이오 DB 자료의 유출	- 센서와 모바일 장치에 대한 인증 - 바이오 DB 의 암호화
Model6	- 허용되지 않는 센서를 통한 자료 수집 - 바이오 DB 자료의 오용 - 오염된 바이오 DB 자료를 통한 잘못된 비교 - 센서의 분실을 통한 바이오 DB 자료의 유출	- 바이오 DB 의 암호화
Model7	- 허용되지 않은 센서를 통한 자료 수집 - 잘못된 캡쳐 바이오 정보의 전송 - 바이오 DB 자료의 오용 - 오염된 바이오 DB 자료를 통한 잘못된 비교 - 모바일 장치의 분실 등을 통한 바이오 DB	- 센서와 모바일 장치에 대한 인증 - 바이오 DB 의 암호화

	정보의유출	
Model8	- 허용되지 않은 센서를 통한 자료 수집 - 잘못된 캡쳐 바이오 정보의 전송 - 전송 채널에 대한 공격 - 잘못된 서버 사용	- 센서와 서버에 대한 인증 - 전송 채널 암호화
Model9	- 센서에 대한 오용(관계없는 모바일앱이 센서 사용) - 캡쳐되는 바이오 정보에 대한 탈취 (다른 모바일앱이 센서에 MTM 공격을 통한 탈취 가능) - 바이오 DB 자료의 오용 - 오염된 바이오 DB 자료를 통한 잘못된 비교 - 모바일 장치의 분실등을 통한 바이오 DB 정보의유출	- 센서와 애플리케이션에 대한 인증 - 바이오 DB 의 암호화
Model10	- 센서에 대한 오용 (관계없는 모바일앱이 센서사용) - 캡쳐되는 바이오 정보에 대한 탈취 (다른 모바일앱이 센서에 MTM 공격을 통한 탈취 가능) - 전송 채널에 대한 공격 - 잘못된 서버 사용 - 캡쳐 후 수집되는 바이오 정보에 대한 서버 집중화로 대량의 바이오 정보 유출 가능	- 센서와 애플리케이션에 대한 인증 - 애플리케이션과 서버에 대한 인증 - 전송채널 암호화 - 전송 자료 암호화
Model11	- 센서에 대한 오용 (관계없는 모바일앱이 센서사용) - 캡쳐되는 바이오 정보에 대한 탈취 (다른 모바일앱이 센서에 MTM 공격을 통한 탈취가능) - 바이오 DB 자료의 오용 - 오염된 바이오 DB 자료를 통한 잘못된 비교 - 모바일 장치의 분실등을 통한 바이오 DB 정보의 유출 - 전송 채널에 대한 공격 - 잘못된 서버 사용 - 캡쳐 후 수집되는 바이오 정보에 대한 서버 집중화로 대량의 바이오 정보 유출 가능	- 센서와 애플리케이션에 대한 인증 - 애플리케이션과 서버에 대한 인증 - 바이오 DB 암호화 - 전송 채녈 암호화 - 전송 자료 암호화
Model12	- 센서에 대한 오용 (관계없는 모바일앱이 센서사용) - 캡쳐되는 바이오 정보에 대한 탈취 (다른 모바일앱이 센서에 MTM 공격을 통한 탈취 가능) - 전송 채널에 대한 공격 - 잘못된 서버 사용	- 센서와 애플리케이션에 대한 인증 - 애플리케이션과 서버에 대한 인증 - 전송 채널 암호화

- 서버는 일반적인 보안 위협에는 충분히 대응하고 있다는 전제하에 서버의 위협은 주로 오랜 기간 모아진 전송된 바이오 정보의 대량 유출 정도로만 생각할 수 있음
- 각 장치들에 대한 역할 분담을 통한 정확한 위협대응을 위해서는 Model 8 의 방식이 권장됨

"끝"

■ **[참고] 바이오 보안토큰(BHSM)의 운영요구사항 및 보안요구사항**



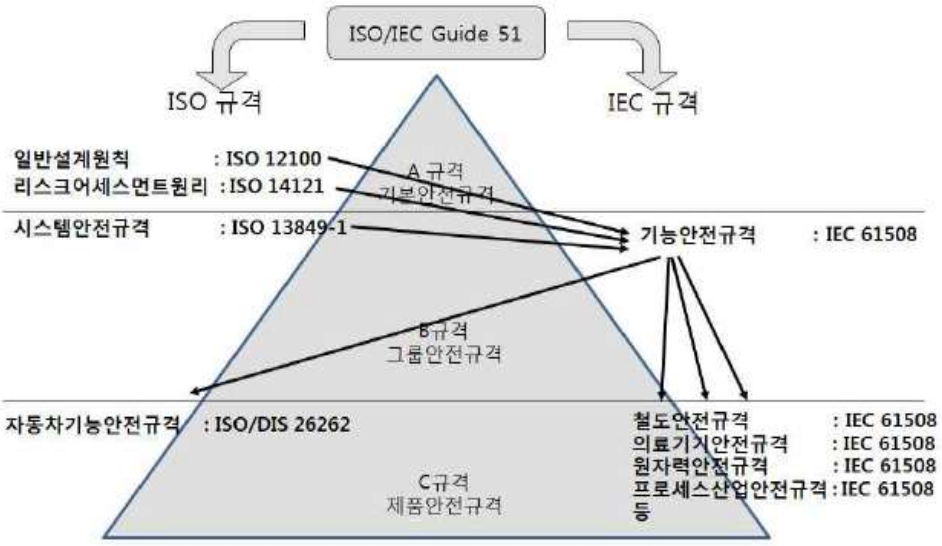
구분	설명
운영요구사항	1. CA 는 기존의 PKI 를 이용하여 바이오보안 토큰을 운용함에 있어서 X.509 확장 필드를 이용함으로서 기존의 X.509 에 대해서 별도의 수정을 요구하지 않는다.
	2. 사용자 확인을 위한 X.509 확장필드를 사용함에 있어서 사용자의 프라이버시 보호를 위하여 Alice 의 개인식별 정보 IR 을 직접적으로 사용하지 않아야 한다.
	3. 바이오인식정보를 이용함에 있어서 ISO 24745 국제표준에서 제시한 바이오 프라이버시 보호를 위한비가역성(irreversibility), 비연결성(Unlinkability), 기밀성(confidentiality)를 만족해야 한다.
	4. 바이오인식 프라이버시 보호를 바이오인식 정보 BR 은 운영중에 오직바이오보안 토큰내에서만 사용됨으로서 바이오정보에 대한 자기 통제가보장되어야 한다.
보안요구사항	1. Alice 는 Bob 에게 자신의 바이오보안토큰을 이용하여 RA 에 등록된 사용자가 본인 임을 증명할 수 있다.
	2. Eve 가 Alice 의 인증서로부터 바이오인식 정보 BR 을 알아내기 위해서는 막대한 양의 작업 시간을 요구한다.

- CA: Alice 의 바이오 보안 토큰을 발급하는 인증기관(Certificate Authority)
- RA: Alice 가 자신의 바이오정보를 최초 한번 공개하여 BR 을 등록해야만 하는 등록기관 (Register Authority)
- IR: ISO 24745 국제표준에 정의된 주민등록번호, 신용카드번호 같은 개인식별정보(Identity Reference).
- BR: ISO 24745 국제 표준에 정의된 지문이나 얼굴인식을 위한 템플릿 등과 같은 바이오인식 정보(Biometric Reference)

2 소프트웨어의 안정성(Safety)

문제	소프트웨어 산업과 건설, 자동차, 의료 등 타 산업과의 융합이 확대됨에 따라 소프트웨어가 우리 생활 전 분야에 활용되고 있으며, 안전한 소프트웨어의 구축에 대한 요구가 급증하고 있다. 소프트웨어의 안정성(Safety) 확보를 위한 국제 표준 규격, 소프트웨어 안정성 평가 기법에 대해 설명하고, 안전한 소프트웨어 개발을 보증하는 방법에 대해 설명하시오.
도메인	소프트웨어 공학
정의	안전성은 사람 또는 환경을 위협하지 않고 정상적 또는 비정상적으로 동작하는 시스템의 능력을 나타내는 시스템 요소
키워드	IEC 61508(구성요소, SIL), ISO26262(구성요소, ASIL), SW 안전성 테스트 방법 (테스트 주도 개발, 요구사항 추적성 확보, 모델기반 테스트, 신뢰성 입증된 도구 사용)
출제의도분석	소프트웨어 안전성 보증 필요성 대두
답안작성 전략	- IEC 61508, ISO 26262 표준에 대한 정확한 이해를 기반으로 소프트웨어 안전성 평가 방법을 다양하게 제시하고 소프트웨어 개발 보증 방법 기술
참고문헌	KPC 모의고사(28 회-2) 전자신문 "[이슈분석]ISO 26262 전면 도입, 車 산업 선진화 계기"(2014.03.18) RMS 기반으로 한 소프트웨어 품질의 안전성 평가 개선방안 연구(2010)
모범목차	1. 소프트웨어 안전성 확보의 중요성 2. 국제 표준 규격 - IEC 61508 와 ISO 26262 3. 소프트웨어의 안정성(Safety) 평가 기법 4. 안전한 소프트웨어 개발을 보증하는 방법
풀이 기술사님	정상미 PE (제 101 회 정보관리/ jsm1111111@naver.com)

■ **소프트웨어의 안정성(Safety) 확보를 위한 국제 표준 규격**



국제표준	내용	
ISO/IEC Guide 51	- 제품 규격에 안전에 관한 규정을 도입하기 위한 기본적인 가이드라인	
	A 규격	광범위한 제품, 프로세스 및 서비스에 대해서 적용하는 일반적인 안전측면에 관한 기본 개념과 원칙, 요구사항을 포함
	B 규격	- 몇 개 또는 한 무리의 유사한 제품, 프로세스 및 서비스에 적용할

		수 있는 안전측면을 포함하는 규격- IEC61508 규격이 해당
	C 규격	- 특정 또는 한 무리의 제품, 프로세스 또는 서비스의 안전 측면을 포함하는 규격 - ISO 26262 IEC 62278, 60601, 61511 등

■ **IEC 61508 와 ISO 26262**

가. 기능 안전성 관련 국제표준 IEC 61508

- 전기, 전자, 프로그램 가능한 전자시스템의 기능안전(Functional safety of electrical/ electronic/ programmable electronic safety-related systems) 표준으로 안전생명주기, 하드웨어, 소프트웨어 안전성 구현방법 및 검증방법 제시

- 안전수명주기에 따라 위험분석 및 평가, 안전무결성수준(SIL: Safety Integrity Level)을 설정하고, 하드웨어와 소프트웨어를 목표된 수준(SIL 수준)에 충족하도록 구현하며, 설치, 운영, 유지보수, 변경, 폐기까지 관리

Part	구성	설명
Part 1	General requirements(required for compliance)	일반적 요구사항
Part 2	Requirements for electrical/electronic/programmable electronic safety-related systems(required for compliance)	전기적/전자적/프로그램 가능한 전자 안전 관련 시스템에 대한 요구사항
Part 3	Software requirements (required for compliance)	소프트웨어 요구사항
Part 4	Definitions and abbreviations (supporting information)	정의와 약어
Part 5	Examples of methods for the determination of safety integrity levels (supporting information)	안전도 수준의 결정 방법의 예
Part 6	Guidelines on the application of parts 2 and 3 (supporting information)	IEC 61508-2와 IEC 61508-3의 적용 가이드 라인
Part 7	Overview of techniques and measures (supporting information)	기술과 측정의 개관

나. 차량용 기능 안전규격, ISO 26262

- 자동차에 탑재되는 SW 의 오류로 인한 사고를 미연에 방지하기 위해 제정된 기능안전 규격

- 기존 차량용 품질관리 기준인 IEC 61508 의 핵심 개념인 안전성보전등급(SIL)과 하드웨어 중심의 안전 생명주기(Safety lifecycle)를 개선한 차량의 전기전자장치의 기능 안전성에 관한 요건을 정의한 국제표준

- 10 개 파트 43 개 요구사항으로 구성됨, 제품 개발 시스템, 하드웨어, 소프트웨어 수준에서의 개발은 V 모델을 따름

Part	구성	설명
Part 1.	Vocabulary (용어)	-관련 용어를 정의
Part 2.	Management of Functional Safety (기능안전관리)	-기능 안전성에 관련된 개발활동을 계획, 조정, 추적하는 요건 등 전반적인 안전성 관리 요구사항 정의
Part 3.	Concept Phase (컨셉트 단계)	-아이템 정의, HARA 분석, 안전 목표와 안전메커니즘정의 -개발 품목 정의를 기반으로 위험요인 분석 및 위험심사로 ASIL 판정
Part 4.	Product development: System level (시스템 수준 개발)	-기능 안전 요구사항을 시스템으로 설계하고 검증하는 것을 정의 -시스템 수준에서의 개발은 V모델을 따름, 기술적

		요구사항, 시스템디자인, 테스트(왼쪽), 검증, 확인과 심사(오른쪽)
Part 5.	Product development: Hardware level (하드웨어 수준 개발)	-시스템에서 할당 받은 요구사항을 하드웨어로 개발하고 검증하는 것을 정의, V모델의 개념에 따라 하드웨어의 개발, 통합, 검증 등에 대한 요구사항정의
Part 6.	Product development: Software level (소프트웨어 수준 개발)	-시스템에서 할당 받은 요구사항을 소프트웨어로 개발하고 검증하는 것을 정의, V모델의 개념에 따라 개발, 통합, 검증 등에 대한 요구사항 정의
Part 7.	Production and operation (생산과 운영)	-품목 생산을 위한 계획, 샘플 생산, 양산, 서비스 등에 관한 요구사항 표준 정의
Part 8.	Supporting process (지원 프로세스)	-안정요구사항, 명세방법, 형상관리, 변경관리, 검증, 문서화, 지원 도구의 자격검증, 재사용 소프트웨어의 자격검증, 하드웨어자격검증, 실제 사용을 통해서 입증된 안전성에 대한 요구사항정의
Part 9.	ASIL-oriented and safety-oriented analysis(ASIL 및 안전 관련 분석)	- ASIL(Automotive safety integrity level) 안정요구사항을 분해하는 방법, 안전 관련 구성요소 사이의 공존의 조건인 상호간섭정도, 위험 분석방법 등 기술
Part 10.	Guidelines on ISO26262 (가이드라인)	-주요개념, 안전케이스, ASIL 분해 등 ISO 26262 이해에 도움이 되는 가이드라인 정의

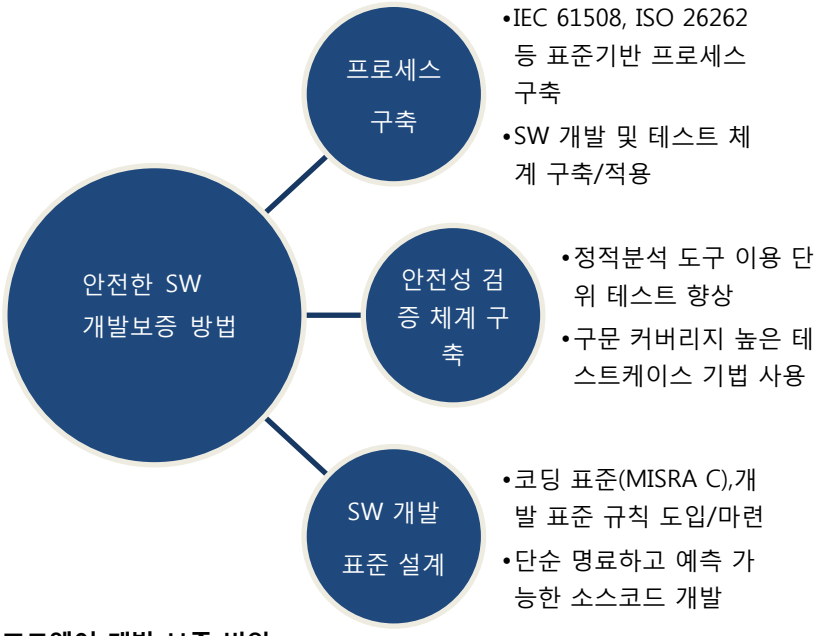
■ **소프트웨어의 안정성(Safety) 평가 기법**

기법	정의	특징
결함수 분석 (Fault Tree Analysis: **FTA**)	- 하나의 특정한 사고의 원인이 무엇인가를 연역적 기법으로 찾아가는 위험성 평가 기법 - 시스템의 고장이나 사고를 장치나 운전자의 실수 등 사고 원인들의 관계를 논리 게이트로 표현-	- 도해적으로 분석하여 고장이나 사고 기본적 원인을 찾아내고 원인으로 인한 사고의 가능성을 정량적으로 평가 - 항공우주, 전자공학, 핵산업 등에 폭넓게 사용
위험과 운영 가능성 분석 (Hazard & Operability study: **HAZOP**)	- 시스템 안전성 분석을 위해 요구사항 명세단계에서 안전성 분석을 수행 - 사고가 설계 또는 운용상에서 의도한 것에서 벗어났을 때 발생함을 가정하고 설계에서 예상한 운용시 일어날 수 있는 모든 가능한 일탈 상황과 관련 위해 요소 발견	- 시스템을 구성하는 각 단위에 대하여 Guide Phrase 를 사용하여 의도된 동작에서 일탈이 일어났을 때, 발생 가능한 모든 위해도에 대하여 HAZOP 조직이 설계에 대한 의문을 제기하는 형식으로 수행. - 화학공장과 같은 산업에서 사용
고장모드 및 영향분석(Failure Mode & Effect Analysis: **FMEA**)	- 기계부품(시스템요소)의 고장이 기계(시스템) 전체에 미치는 영향을 예측하는 해석방법 - 기계부품 등의 기계요소가 고장을 일으킨 경우에 기계 전체가 받는 영	- 예상되는 고장 빈도, 고장의 영향도, 피해도 등에 평가기준을 설정해 두고, 개개의 구성요소에 대하여 고장 평가를 하고 종합하여 치명도 구함.

	향을 규명	- 치명도가 높을수록 집중적인 관리 필요
예비위험 분석 (Preliminary Hazard Analysis)	- 예비 위험 분석은 시스템 내의 위험한 요소가 어떤 위험한 상황에 있는가를 정성적으로 평가하는 기법	- 공정의 설계 초기 단계에서 일차적으로 위험을 찾아내어 효과적이고 경제적으로 안전성을 확보 - 예비위험분석은 다른 위험 분석 방법에 선행

■ **안전한 소프트웨어 개발 보증 방안**

가. 소프트웨어 안전성 향상을 위한 개발 보증 전략



나. 안전한 소프트웨어 개발 보증 방안

구분	내용	도구
프로세스 구축	표준 기반 프로세스 구축	IEC 61508, ISO 26262 국제 표준의 소프트웨어 안전성 프로세스를 CMMI 와 함께 적용하여 조직의 수준 및 특성에 맞는 프로세스 구축하고 적용
	SW 개발 및 테스트 체계 구축	Reverse engineering 과 Forward Engineering 통해 체계적인 소프트웨어 개발 체계를 도입하고 요구사항 관리, 개발 절차, 산출물, 테스트 결과에 대한 SW Audit 구축
안전성 검증 도구 및 기법 도입	정적 분석 도구 이용	- 소스코드 기반 분석 도구: 언어의 기본적인 규칙을 위반하거나 API 를 부정확하게 사용 등 일관성이 없거나 모순적인 가정을 하는 코드 부분을 발견 (McCabe, peframe) - Rule 기반 분석 도구: 코딩 표준에 부합하는지 여부를 검사하는 Programming Research 도구(QAC++) - 의미기반 분석 도구: 버퍼 오버런(buffer overrun), 널 포인터 역참조, 경쟁 조건(race condition), 리소스 누설(resource leak) 처럼 코드에 있는 심각한 오류 발견 도구(CodeSonar)

	테스트케이스 기법 사용	-MC/DC 등의 구문 커버리지가 높은 기법을 적용한 테스트케이스 설계하고 FTA, FMEA 등에 수치를 이용하여 중요도 파악
SW 개발 표준 설계	개발 표준 도입	- MISRA C 등의 코딩 표준 도입하여 소스코드 수준에서 취약점이 발견되지 않도록 예방하고 UML profile 을 정의하여 특정 기술이나 특정 플랫폼에 맞는 개발 수행하도록 테일러링
	개발 규칙 도입	코드의 배치, 변수나 상수(또는 identifier)와 같은 이름의 선택, 구문 구조(syntactic construct)와 같은 주로 코드의 외관적인 측면으로 프로그래머가 프로그램을 작성하는 방식을 제한하는 규칙 도입하여 단순 명료하고 예측 가능한 소스코드 개발

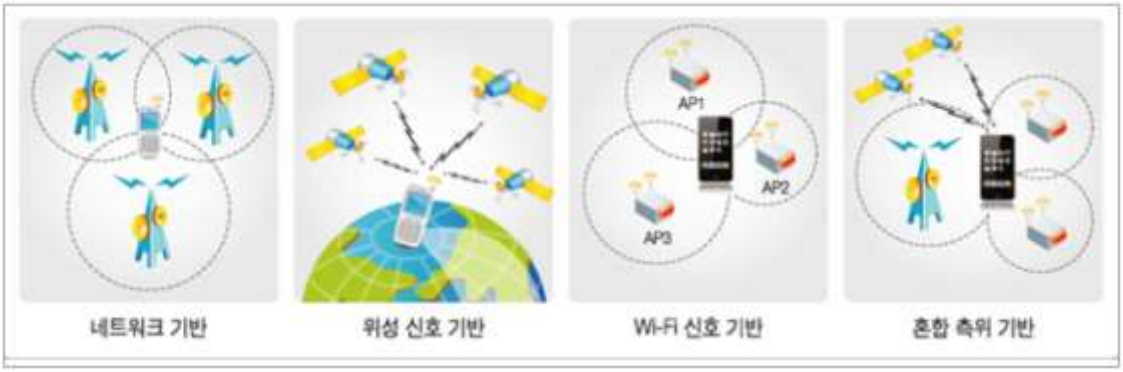
"끝"

3 실내 위치 설정

Notes

문제	실내에서 WLAN 과 같은 상용 통신장치의 전파특성을 이용한 이동 단말의 위치 설정 방안
도메인	네트워크
정의	WiFi 이동 단말에서 주변 AP 의 신호 세기를 측정 한 후, 이를 사전에 구축한 AP 들의 수신 패턴 DB 와 비교하여 가장 유사한 패턴을 갖는 위치를 선택하는 방식
키워드	삼각측량, 핑거프린트
출제의도분석	위치기반 서비스가 실내공간으로 확대 되고 있으며, 특히 무선랜은 현재 가장 널리 쓰이고 있는 무선 통신 방식이고 여러 분야에서 안정성이 검증됨
답안작성 전략	이동 단말의 실내 측위 기술들과 해당 기술들을 활용한 효과적인 위치 서비스 제공 방법 제시
참고문헌	KPC 모의고사 해설집(51 회 정보관리 3 교시)
모범목차	1. 이동 단말의 실내 위치 설정 기술의 개요 2. 실내에서 상용 통신장치 전파특성 이용한 이동 단말 위치 설정 방안 3. WLAN 기반 이동 단말의 실내 위치 설정 방안 4. 이동 단말의 실내 위치 설정 활용 사례
풀이 기술사님	권혁재 PE (제 102 회 정보관리/ star10ve@naver.com)

■ **위치 정보 측위 기술의 개요**



- 위치정보를 측위하는 기술은 측위에 사용하는 인프라의 유형에 따라 네트워크 기반, 위성신호 기반, Wi-Fi 신호 기반, 혼합측위 기반의 4 가지로 분류 가능

■ **실내 위치 정보 측위 기술**

구분	작동방식	정확도	특징
WLAN	- Wi-Fi 단말이 자신의 위치를 요청할 경우 단말은 주변에 설치된 Wi-Fi AP 의 MAC 과 전계강도를 검색하여 서버로 전송 - 사전에 구축한 Wi-Fi AP 의 위치정보 DB 에서 해당 AP 의 MAC 주소를 찾아 위치 파악	10~30m (층단위 구분)	- 도심지역에서 저비용으로 비교적 정확한 측위 가능 - 전파 맵 작성 및 지속 갱신 필요
ZigBee/ Bluetooth	- ZigBee/Bluetooth 탑재 단말이 AP 를 통해 단말의 위치를 주기적으로 위치 서버로 등록 - 이통망 LBS 서버에서	10~30m (층단위 구분)	- 건물의 층단위까지 정확한 위치정보 제공 - 모든 건물에 AP 구축 필 요

** 장면 분석 어떠한 시간을 기준으로 장면을 비교 분석하여 유사도에 의해 결과를 판단하는 방법*

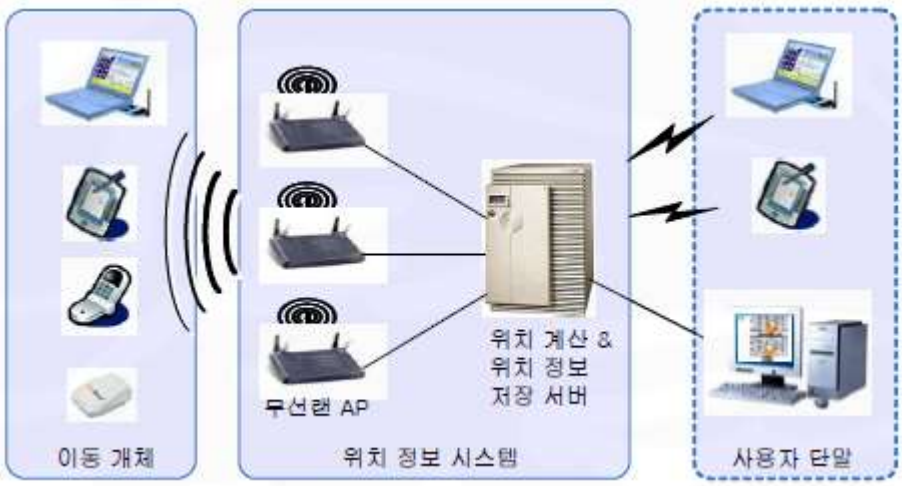
	ZigBee/Bluetooth 위치서버와 연동하여 위치정보를 제공		- 정확한 위치를 위해 서버와 연동 필요
UWB	- UWB 단말기에 자신의 고유 ID 를 32bit 로 송출 - 건물 내에 설치된 여러 UWB AP 가 이를 수신 위치 계산	10cm (층단위 구분)	- 투과성이 우수, 건물내 음영지역에서도 위치 파악 가능 - 건물 내 다수의 AP 설치 필요
기지국	- 기지국들로부터 위상, 전계강도 정보를 받아 측위서버에 전송 - 도심지를 약 60mX60m 격자구조로 전파를 측정하여 구축한 DB 에서 가장 적합한 패턴을 검색해 위치 파악	200~300m (층단위 구분 불가)	- 도심지역 대비 외곽지역에서의 기지국 커버리지가 넓고, 다수의 기지국 정보 수신 불가

- 이외에 적외선 기반, 초음파 기반, RFID 기반, LED 조명기반 등 다양한 실내측위 기술 활용 가능

■ **무선랜 기반 실내 위치 측위 기술**

구분	작동방식	특징
삼각측량	- AP 에서 수신된 신호의 지연 시간 및 감쇠 정도를 이용	- 기본적인 무선 측위 기술
핑거 프린트	- 측위 지역을 셀로 나누어 장면 분석을 통해 위치를 측위 높은 측위 정확도로 인해 실내 위치 - AP 의 Mac address 와 수신신호세기 정보를 이용하여 위치를 결정	- 위치측위 전에 측위 공간에 대해데이터베이스를 미리 구축해야 함 - 실내 환경이 바뀌면 재작업 필요

■ **무선랜 기술을 이용한 위치 정보 시스템**



- 무선랜 기술을 이용한 위치 정보 시스템 (측위 기술과 더불어 위치 정보 저장/관리 서버 이용)

■ **WLAN 기반 실내 위치 측위 기술의 장점**

- 높은 위치 추정 정확도를 제공.
- 위치정보 서비스와 함께 고속 데이터 통신이 가능
- 이미 성숙한 기술을 이용하기 때문에 안정적
- 기 설치된 하드웨어의 재활용이 가능

- 신규 설치 및 구조 변경이 용이.
- 별도의 이용료를 지불하지 않아도 됨
- 자체 인프라를 사용하기 때문에 중요 자원 정보에 대한 대외 기밀성을 유지 용이
- ERP, MIS 등과 같은 기존 업무 시스템과 연동해서 사용할 수 있으며, 이를 통해 다양한 부가 서비스 개발이 가능
- 무선 인터넷 전화(WVoIP)와 연계해서 사용 가능

■ **WLAN 기반 실내 위치 측위 사례**

구분	작동방식	설명
국내사례	주차 위치 제공 서비스 (신세계 백화점)	- GPS 가 닿지 않는 빌딩 내 실내 주차장의 주차 위치 확인 서비스 시행 - 반경 5m 정보의 정확성으로 주차구역과 번호를 알려주고 주차위치까지 길안내 제공 - Wi-Fi 측위 기반
	myCoex (코엑스)	- 코엑스 내부에서의 위치 검색 및 목적지 안내 서비스 - 실내 매장 등과 같은 POI 정보와 전시, 회의 및 이벤트, 행사 안내 등 제공 - Wi-Fi Fingerprinting 측위 기반
	다음 스토어 뷰	- 기존의 다음 맵과 연동하여 상점에 대한 실내공간의 이미지 및 정보 서비스 - 사용자의 위치를 기반으로 근처 매장에서 즉시 사용할 수 있는 할인쿠폰을 실시간으로 제공
	네이버 실내지도	- 코엑스, 강남역, 부평역 등 전국 78 개 주요 지하상가의 실내지도(2D) 서비스 제공
해외사례	Google Maps	- Bluetooth 태그가 탑재된 기기를 추적하는 Bluetooth 안테나들을 천정에 설치 - 삼각측위 방법을 이용 위치 측정 - Wi-Fi/3G 측위 기반
	실내 위치찾기 서비스 (노키아)	- Bluetooth 태그가 탑재된 기기를 추적하는 Bluetooth 안테나들을 천정에 설치 - 삼각 측위 방법을 이용 위치 측정 - Bluetooth 측위 기반
	가시광 LBS 측위 서비스 (e-Space Kansai)	- LED 조명을 이용한 가시광 통신의 특성 활용 - 자신의 위치와 주변 지역의 정보를 제공 - LED 조명 측위 기반

"끝"

4	정적해싱 오버플로우 처리기법
문제	정적해싱(Static Hashing) 과정에서 발생하는 오버플로우(Overflow)를 처리하기 위한 전형적인 기법 2 가지를 제시하고, 성능 관점에서 비교하여 설명하시오.
도메인	컴퓨터구조/운영체제
정의	고정 크기의 테이블을 이용하는 해싱 기법
키워드	정적해싱, 동적해싱, 확장성 해싱, 단방향 특성, 강한 충돌저항, 해시함수, 동거자, 개방 주소법(선형, 2 차 탐색), 폐쇄 주소법 (합병, 분리 체인법)
출제의도분석	해싱기법과 정적해싱 과정에서 발생하는 오버플로우를 처리하기 위한 전형적인 기법, 개방 주소법과 폐쇄 주소법에 대한 이해와 성능관점의 비교 문제로, 실제 두 기법의 기능적 차이뿐 아니라 성능적인 비교를 할 수 있는지 여부의 문제
답안작성 전략	정적해싱의 개요, 구성도, 구성요소를 보이고, 정적해싱에 대한 오버플로우 해결 기법의 일반적인 기법을 개방 주소법과 폐쇄 주소법으로 크게 둘로 나누어 제시한다. 이후 성능 관점에서 두 기법을 비교 설명한다.
참고문헌	www.nhu.edu.tw/~chun/DS(II)-Ch08-Hashing.pdf C++ 자료 구조론(Horowitz, Ellis, 교보문고)
모범목차	정적해싱의 개요 (필요성, 특성, 종류), 구성도 구성요소, 오버플로우 처리기법, 성능 관점의 비교
풀이 기술사님	송영호 PE (제 102 회 컴퓨터시스템응용/ songyoungho@hanmail.net)

■ **정적해싱(Static Hashing)의 개요**

- 해싱은 데이터의 신속한 탐색을 위해 데이터를 해시테이블이라는 배열에 저장하고, 데이터의 키값을 주면 이를 적절한 해시 함수를 이용하여 테이블의 주소로 변환 후 원하는 데이터를 찾아내는 기법으로 고정 크기의 테이블을 이용하여 한 번 저장된 데이터의 상대적 위치가 변경되지 않는 정적 해싱(Static hashing)과, 삽입 삭제가 빈번히 발생하는 응용에 적합하도록 고안된 동적 해싱(Dynamic hashing) 또는 확장성 해싱(extensible hashing)으로 구분된다.

■ **해싱의 필요성 및 특성**

- 테이블에서 키 값과 일치하는 데이터를 차례로 비교하는 방식은 최악의 경우 n 회의 비교가 필요하나, 해쉬를 이용하면 해수함수의 키 값으로 해당 주소를 최소 한번에 변환해 가능함으로 매우 빠른 검색이 가능하다.

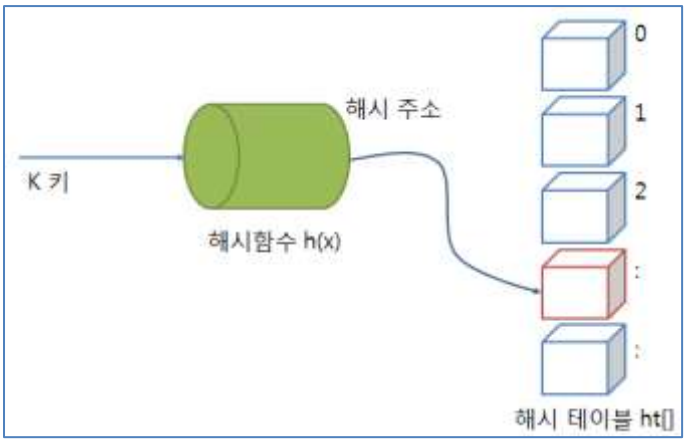
특성	설명
단방향 특성 (one-way property)	- h(k) = c 를 만족하는 c 가 주어졌을 때, k 를 찾는 것을 계산적으로 어렵게 하는 성질
강한 충돌저항 (strong collision resistance)	- h(x) = h(y)를 만족 시키는 (x, y)쌍을 계산적으로 찾기 어렵게 만드는 성질.
암호화 해시 함수의 추가적 특징	- h 는 데이터 블록 크기에 상관없이 적용가능해야 함 - h 는 고정 길이의 해시 코드를 만들어야 함 - h(k)는 어떤 k 가 주어져도 계산이 비교적 쉬워서 하드웨어와 소프트웨어의 구현이 실용적이어야 함

■ **해싱의 종류**

종류	설명
정적해싱 (Static Hashing)	- 고정크기의 테이블을 이용하여 해싱하는 방법으로 한 번 저장된 데이터의 상대적 위치가 변경되지 않는다.
동적해싱 (Dynamic Hashing)	- 확장성 해싱(extensible hashing)이라고도 함, - 재조정을 한 번 할 때마다 오직 하나의 버킷 안에 있는 엔트리들에 대해서만 홈 버킷을 변경하게 하여 재조정 시간을 줄임 - 하나의 연산에대해 좋은 성능을 유지할 수 있게한다.

■ **정적해싱의 구성도 및 구성요소**

- 정적해싱의 구성도



- 정적해싱의 구성요소

구성요소	설명
해싱테이블	- 식별자들의 저장장소
버킷	- 데이터들의 저장장소
슬롯	- 하나의 주소에 여러 데이터가 저장 가능하도록 버켓을 나눔
오버플로우	- 가득찬 버킷에 새로운 식별자를 추가하려고 할 때 발생되는 현상
동거자(synonym)	- 한 버킷에 두 개 이상의 식별자를 사상시킴 (슬롯)

■ **정적해싱과정에서 발생하는 오버플로우(Overflow)를 처리하기 위한 전형적인 기법**

- 정적해싱을 하는 경우 서로 다른 두 개 이상의 키 값들이 해시 함수에 의해 동일한 주소로 변환되는 경우 충돌이 발생될 수 있다.

- 충돌의 발생이 빈번하면 처리 시간이 길어지는 등 성능이 저하되므로 해시 함수의 수정이나 해시 테이블의 크기가 적절히 조절되어야 한다.

- 일반적으로 충돌이 발생할 경우 버킷이 여러 슬롯으로 구성되어 있다면 다른 슬롯으로 저장하면 된다. 그러나 모든 슬롯이 채워지면 오버플로우가 발생한다.

- 정적해싱 과정에서 발생하는 오버플로우 처리를 위한 전형적인 기법들

기법	설명	
개방 주소법	- 생성된 버킷 주소에서 충돌이 발생하면 생성된 버킷의 주소로 부터 비이있는 버킷이 발견될 때까지 찾는다.	- 선형 탐색법 (Linear probing): 충돌이 발생하면 다음버킷부터 차례로 빈 버킷을 찾는 기법, 간단하나 집중현상이 발생.

	- 만일 해시 테이블의 끝까지 빈 버킷을 찾지 못한다면 테이블의 처음부터 빈 버킷을 찾아 저장한다.	- 2 차 탐색법(quadratic probing): 선형 탐색법에서 발생하는 집중문제 해결을 위한 방법으로, 특정한 수 만큼 떨어진 곳을 순환적으로 뒤져서 빈 공간을 찾아 저장하는 기법
		- 재해싱: 집중문제 해결위한 방법으로, 키 값에 대하여 두 번의 해싱이 이루어지는 기법
폐쇄 주소법 (Closed Addressing) / 체인법 (chaining)	충돌이 발생하는 동거자 별로 연결 리스트에 저장하는 기법	- 합병 체인법(coalesced chaining): 충돌이 발생하면 빈 버킷을 찾아 삽입하고 삽입된 위치를 포인터 부분에 기억시키는 기법
		- 분리체인법(separate chaining): 충돌이 발생한 키 값들을 연결리스트로 처리, 동거자들은 같은 버킷에 연결구조로 저장

■ **개방 주소법과 폐쇄 주소법의 성능 관점에서의 비교**

- 비고	개방주소법	폐쇄 주소법
복잡도	알고리즘이 비교적 단순	알고리즘이 비교적 복잡함
평균 비교횟수 기대치	α 가 적재 밀도일 때 키를 찾기 위한 평균 키 비교 횟수의 기대 값은 (2-α)/(2-2α)	검색이 성공했을 경우 키의 비교 횟수 기대치는 α 가 적재 밀도일때 평균적으로 약 1 + α/2
속도	처리 속도가 빠르나 집중 문제 발생시 전체 성능이 떨어지는 단점	충돌이 발생한 것들만 연결 리스트에서 검색해 주면 되므로 속도가 빠름
기억 소모량	기억 소모량이 비교적 적음	기억 소모량이 많음.
테이블 크기	해쉬 테이블의 크기에 영향받음	해쉬 테이블의 크기에 영향 받지않음
이론적 평가 (참고자료)	폐쇄 주소법의 예상 성능에 대한 확률적 분석 시, a=n/b 가 균일 해시 함수를 사용한 해시 테이블의 적재 밀로라 가정하면 (n 개의 키, b 는 버킷, U_n 은 해시테이블에 없는 키를 찾는데 필요한 예상 비교 횟수, S_n 는 임의로 선택된 주소 확인에 필요한 예상 키 비교횟수 인 경우). (1) 선형 개발 주소법에 대해 • $U_n = ½[1 + 1/(1-a)^2]$ • $S_n = ½[1 + 1/(1-a)]$ (2) 재해싱 및 임의 조사법과 이차 조사법에 대해 • $U_n \approx 1/(1-a)$ • $S_n \approx -[1/a]\log_e(1-a)$ (3) 체인법에 대해 • $U_n \approx a$ • $S_n \approx 1 + a/2$	

"끝"

5	빅데이터 분석도구 R
문제	빅데이터 분석 도구인 R 의 역사와 주요 기능 3 가지에 대해 설명하시오.
도메인	디지털 서비스
정의	통계분석 및 그래프 분석 프로그램을 포함하는 개방형 소프트웨어 기반 패키지
키워드	빅데이터 분석도구
출제의도분석	빅데이터와 관련된 기술의 꾸준한 출제
답안작성 전략	R 의 역사를 태동, 전파, 확산의 단계로 구분 설명하고, R 의 주요기능을 분석측면에서 빅데이터 기술환경측면에서 구분지어 상세하게 설명함.
참고문헌	KPC 모의고사, http://www.r-project.org/
모범목차	1. 빅데이터 분석 도구인 R 의 역사 2. 통계적 분석 측면에서의 R 의 주요기능 3. 빅데이터 기술환경 측면에서의 R 의 주요기능
풀이 기술사님	김지영 PE (제 102 회 정보관리/ sayno9@naver.com)

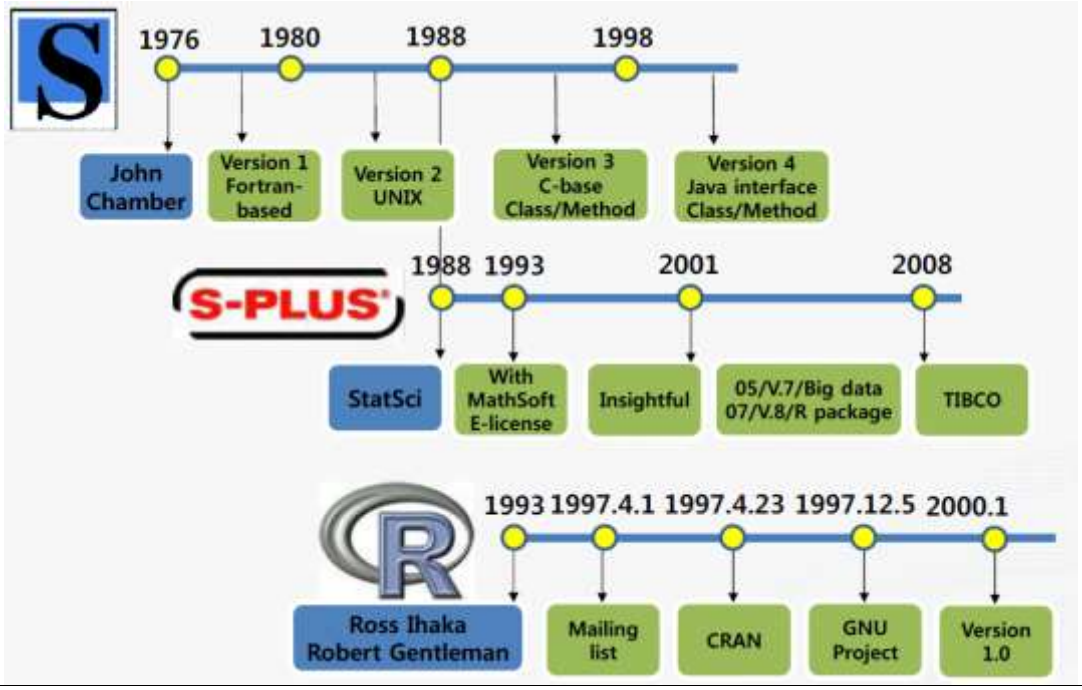
■ **빅데이터 분석도구인 R 의 개념**

- 통계분석 및 그래프 분석 프로그램을 포함하는 개방형 소프트웨어 기반 패키지

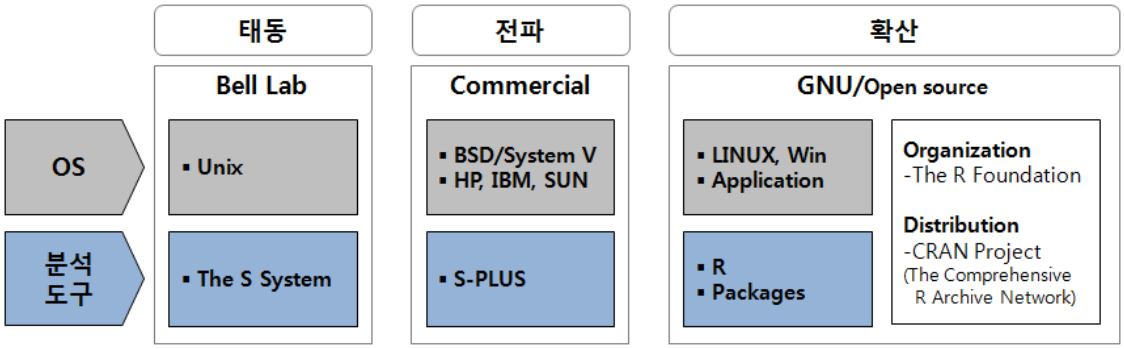
■ **R 의 특징**

특징	설명
In Memory Computing	모든 데이터를 메모리에 로딩 후 처리하는 작업방식
Object-oriented	데이터, 함수가 Object 로 관리 됨
Statistical Package	다양한 함수 및 데이터 내장, 최신 알고리즘 적용 통계 분석에 최적화 된 자료구조 제공(Matrix, Vector)
Visualization	그래픽 지원, 차트, 히스토그램, 지도 연계 등을 R 에서 바로 사용
Connectivity	다른 언어, 어플리케이션, DB 등 통합이 용이함

■ **R 의 역사**



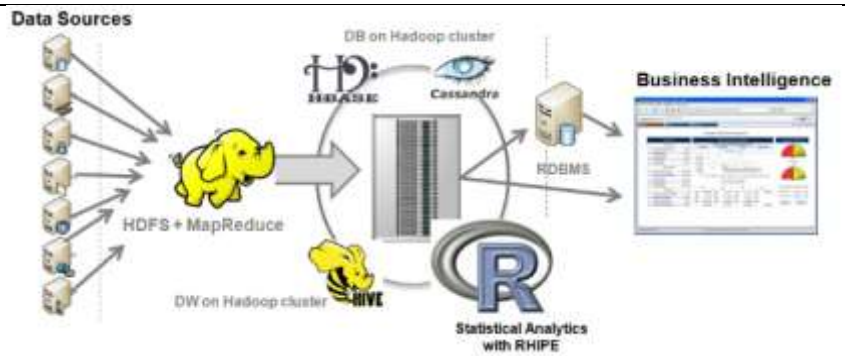
(출처) 넥스알, 빅데이터 애널리틱스 인사이드 2011

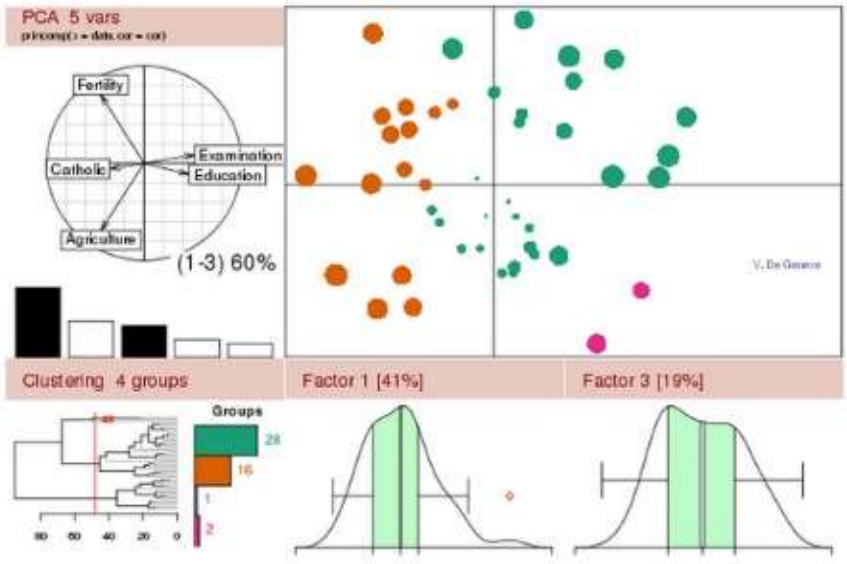


구분	R 의 역사 설명
태동 1980 년대	미국 Bell Lab 에서 데이터 분석용 객체지향 언어인 S 개발 cf) SAS 와 SPSS
R 의 개발 1990 년대	S 언어에 뿌리를 두고 뉴질랜드 오클랜드 대학의 통계학과 교수 Ross Ihaka 와 Robert Gentleman 에 의해 개발 (R 로 시작하는 두명의 교수)
전파 및 확산 2000 년대 이후	R Foundation 의 비영리 단체를 기반으로 R 의 배포와 수정은 Contributor 들에 의해 이루어지고 있음(http://cran.r-project.org) - 현재는 R 3.1.1 버전까지 Release(7.10) 되어있음 빅데이터 분석을 위한 플랫폼으로써 활용

- R 의 탄생 및 발전과정을 살펴보면 R 이 왜 빅데이터 시대의 통계 분석 도구 및 플랫폼으로 부상할 수 밖에 없음을 알 수 있음

■ **R 의 주요기능 3 가지**

주요기능	설명
분산처리	 - 빅데이터 Hadoop 에서 통계분석을 위한 엔진으로써의 기능 - 특히 Package RHipe(R and Hadoop Integrated Processing Environment)를 통해 Hadoop eco-System 에서 통계 분석을 위한 엔진으로써 자리매김
Dynamic Visualization	- 분석결과를 직관적으로 이해할 수 있는 환경, 소프트웨어 기능 제공 - 이차원 평면 상에서의 데이터의 다차원 구조를 이해할 수 있는 다이나믹

	그래프 제공 - GIS, 차트, 산점도, 그라데이션 등 다양한 응용 시각화가 가능함 Ex) Vendor 사에서 in memory 혹은 in database 분석엔진으로 R 을 적용함 
통계분석엔진 기반의 분석	- Data in rest 방식: 생성되는 데이터를 DB 에 기록 한후 분석 - Event-captured/data in motion 방식: DB 기록전에 분석이나, 의사결정에 활용 고성능 컴퓨팅(HPC: High Performance Computing)에 유리한 아키텍처로써 고성능 분석에 용이함 Ex) Google Prediction API

"끝"

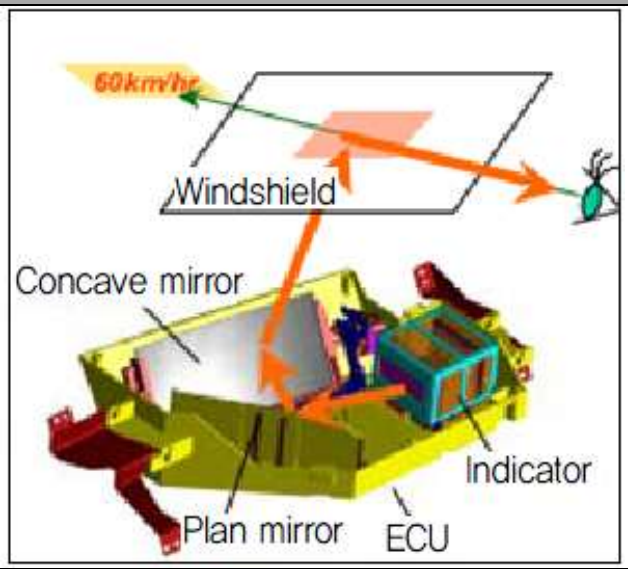
6	**차량용 증강현실**
문제	차량용 증강현실 기술 실현을 위한 HUD(Head Up Display) 및 AR(Augmented Reality) 기술 개발 동향과 적용 시 고려사항에 대해 설명하시오.
도메인	최신기술/동향
정의	운전자의 신체적 인지적 부하를 최소화함으로써 운전자의 안전과 편의를 달성하기 위한 목적으로 차량에서 제공되는 정보를 운전자의 시야에 맞게 운전자 전방 실세계에 정합하여 제공하는 기술
키워드	프로젝션 방식, 후방투영, 전방투영, 레이저방식, 마이크로디스플레이
출제의도분석	자동차의 고급화, 지능화 추세로 사용자 인터랙션 기술에 관심이 높아짐
답안작성 전략	HUD 의 프로젝션 및 레이저방식에 대해 명확히 제시하고 AR 기술적인 부분이 아닌 동향 부분에 대한 제시가 중요함
참고문헌	차량용 증강현실 기술개발 동향(전자통신동향분석 제 28 권 제 4 호 2013 년 8 월)
모범목차	1. 차량용 증강현실의 등장 배경 및 개요 2. 차량용 HUD 기술 개발 동향 3. AR(Augmented Reality) 기술 개발 동향

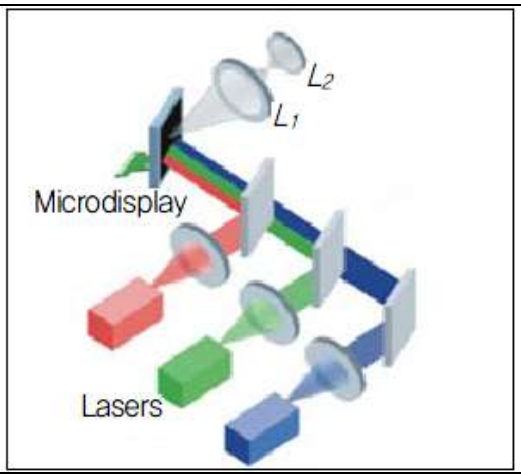
	4. HUD 및 AR 기술 적용 시 고려사항
풀이 기술사님	유용희 PE (제 98 회 컴퓨터시스템응용/ yhinfuture@naver.com)

■ **차량용 증강현실 개요**

- 운전자의 신체적 인지적 부하를 최소화함으로써 운전자의 안전과 편의를 달성하기 위한 목적으로 차량에서 제공되는 정보를 운전자의 시야에 맞게 운전자 전방 실 세계에 정합하여 제공하는 기술
- 최근 차량의 지능화와 증강현실기술 접목의 다양화 및 디스플레이 기술의 발전으로 HUD 개발이 활발히 이루어지고 있음

■ **차량용 HUD(Head Up Display) 기술 개발 동향**

방식	구분	설명
프로젝션 방식	개념도	
	구성요소	- 광원: HUD 에 정보를 표시 - 광학장치: 광원을 투사하기 위한 장치 - 투명스크린: 정보가 투사되는 스크린 - 투영: VFD(Vacuum Fluorescent Display), CRT(Cathode-Ray Tubes), LCD(Liquid Crystal Display), LED(Light-Emitting Diode)등의 디스플레이 형태에 따라 전방투영 또는 후방 투영
	동작방식	1. 하나 또는 여러 개의 프로젝터가 유리판을 향하도록 구성 2. 빔은 스크린에 닿은 후 기록된 렌즈의 배열에 따라 다시 정렬됨 3. 모아진 영상은 원래 영상에 대한 허상(Virtual Point)를 만듦 ※ 후방 투영방식: 영상이 유리판을 통과하면서 보임 ※ 전방 투영방식: 영상이 스크린에 반사되어 나타남

레이저 방식	개념도	
	구성요소	레이저: 영상을 나타내는 각색의 레이저 빔 렌즈: 레이저 빔을 모아서 영상을 구성 Micro display: 모아진 레이저 빔을 스크린에 투사하는 기능
	동작방식	레이저 빔을 렌즈에 비추어 주시 공간 상에 이미지가 나타나게 해주는 직접 투사 방식

■ **AR(Augmented Reality) 기술 개발 동향**

구분	동향
모바일 증강현실 내비게이션 개발	스마트폰 앱을 이용한 차량용 증강현실 내비게이션 기술 개발 차선정보, 경로정보, 전방 주행 차량정보 등 운전자의 안전과 편의를 위한 다양한 정보를 카메라에서 획득하여 제공
단말기 기반 증강현실 내비게이션	기존의 그래픽기반 내비게이션 기술과 접목하여 차량에 장착된 카메라를 통해 획득된 도로 영상 위에 3 차원 형태로 경로정보 제공 내비게이션 경로의 입체 선형 표시, 좌/우회전 화살표 제공 경로정보, 교차로까지의 거리, POI(Point of Interest)정보, 신호등에 따른 경고 알람, 전방 주행 차량과의 거리 등 색깔변이를 이용한 정보 제공
증강현실기술 /HUD	차량 전방위치에 출력하여 머리 움직임이나 시선 이동 등 운전자의 신체적 주의 분산을 줄임으로 써 안전운전 도모 HUD 로 출력되는 정보와 운전자가 눈으로 획득하고 인지하는 실 세계 정보와의 부정합을 감소시키기 위해 증강현실 기술 접목, 활발히 연구 중

■ **AR(Augmented Reality) 사용화 동향**

구분	동향
Autoglass 2020 vision	차량의 고장, 연료, 선행차량, POI, 속도 등의 정보를 full-windshield 기반 AR-HUD 기술 개발 및 상용화 예정(미국)
Windows to the World	자동차의 모든 유리창이 정보제공 디스플레이로 사용, 자동차 앞, 뒤 좌석을 포함한 모든 유리창에 증강현실 접목(일본)
Pioneer	MEMS 기반 레이저 프로젝션 기술 사용, 소형 레이저 프로젝터로 투사, 투명 디스플레이형 HUD 개발(일본)
GM	Full windshield 기반 차량용 증강현실 기술 2016 년 상용화 예정, 비나 안개와 같은 악천후 시 운전자 전방시야 보조 디스플레이
국내	운전 안전성 및 편의성 향상을 위한 운전자 시야 중심 차량용 증강현실 정

	보제공 시스템 기술 개발 중, 주/야간, 악천후 시 전방 보행자, 차량, 교통 안내판, 차선 등을 검출/인식한 후 HUD 에 정보제공

■ **HUD 및 AR 기술 적용 시 고려사항**

- 인지부하 축소: 운전자의 상황인식을 위한 인지부하를 줄일 수 있도록 제공되는 정보를 쉽고 빠르게 이해할 수 있도록 표현해야 함
- 정보제공 효용성 사전 분석: 제공되는 정보의 형태, 배치, 색상과 크기, 개수, 위치, 정보 제공 시점 등 정보제공 효용성에 대한 사전 분석 필요
- 빠른 직관력 제공: HVI(Human Vehicle Interaction) 측면의 연구 진행으로 주의 분산을 최소화하고 빠른 직관력을 제공(GM, BMW)
- 안정성, 만족도 확인: 다양한 정보제공 방법을 적용한 실제 테스트 차량을 이용 실험하여 인지 반응 시간과 실제 운전 조작 행위에 대한 안전 운전 수행도 분석 필요
- 효용성 검증: 정보의 특성과 종류 및 운전 상황에 맞는 정보 표현을 정의, 분류, 분석하고 각 정보표현에 대한 운전 수행 효율 및 주관적 운전자 만족에 대한 효용성 검증 필요

"끝"