제129회 정보관리기술사 해설집

2023.02.04

국가기술자격 기술사 시험문제

기술사 제 129 회 제 4 교시 (시험시간: 100 분)

분야	정보통신	자격종목	정보관리기술사	수검번호		성명	

※ 다음 문제 중 4 문제를 선택하여 설명하시오. (각 10 점)

1. 인포스틸러(InfoStealer) 개념을 설명하고 공격 절차와 공격에 대한 대응방안을 조직의 정보보안 담당자 입장에서 설명하시오.

2. 데이터베이스에서 정규화는 이상현상(Anomaly)이 있는 릴레이션(Relation)을 해결하기 위한 방법이다. 다음의 <수강테이블>을 활용하여 설명하시오.

   가. 이상현상 3 가지와 발생 이유

   나. 해결방안

   다. 테이블 재구성

3. 반도체 생태계를 차지하고자 하는 글로벌 기업들의 소리없는 전쟁이 계속되고 있다. 우리나라는 메모리 반도체의 강국이지만 비메로리 반도체 분야에서는 뒤쳐져 있다. 다음에 대하여 설명하시오.

   가. 메모리 반도체와 비메모리 반도체 비교

   나. 반도체 산업의 가치사슬(Value Chain)

   다. 비메모리 반도체 성장을 위한 비전과 전략

4. 정보시스템 개발 및 운영 단계에서 수행하는 소프트웨어 테스트와 관련하여 다음 사항에 대하여 설명하시오.

가. 몽키 테스트(Monkey Test)와 회귀 테스트(Regression Test) 비교 설명

나. 통합 테스트 계획서에 포함되어야 할 주요 사항

5. IT 투자분석의 프로세스, 프레임워크, 분석방법론에 대하여 설명하시오.

가. 프로세스

나. 프레임워크

다. 분석 방법론

6. 조직이 클라우드 컴퓨팅 서비스를 이용하고자 할 경우, 클라우드 서비스 제공자(CSP, Cloud Service Provider)에 대한 리스크를 관리하여야 한다. 다음을 설명하시오.

가. 클라우드 아웃소싱에 대한 요구사항

나. 리스크 관리 시 고려사항

다. 리스크 대응방안

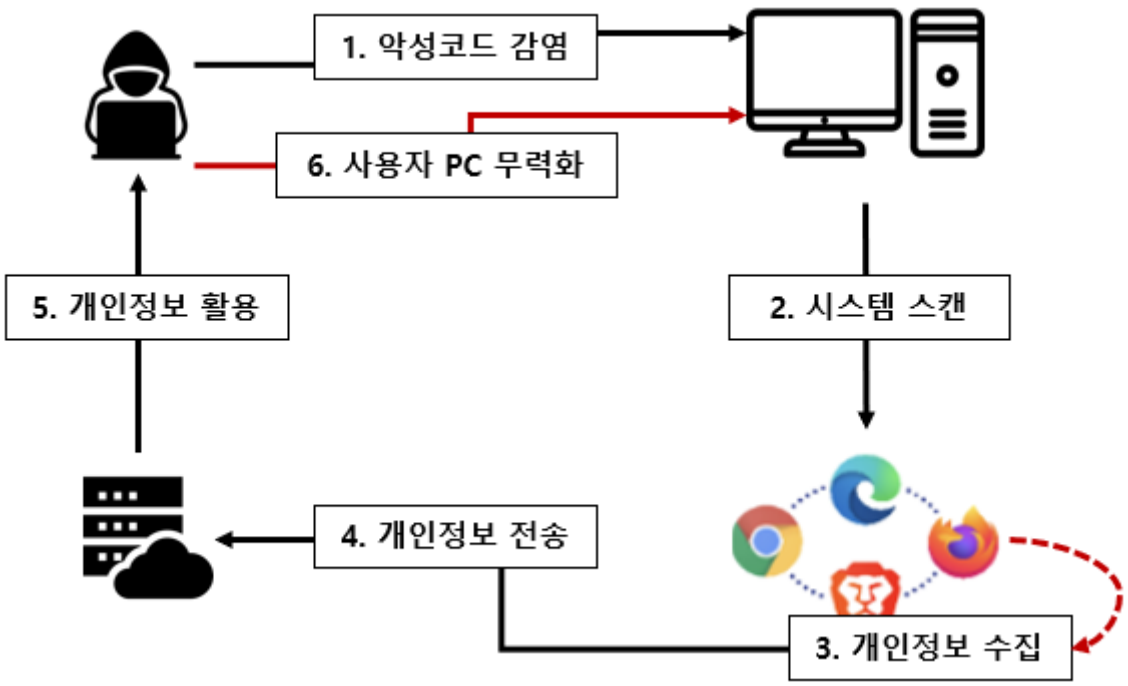
01	인포스틸러(InfoStealer)		
문제	인포스틸러(InfoStealer) 개념을 설명하고 공격 절차와 공격에 대한 대응방안을 조직의 정보보안 담당자 입장에서 설명하시오.		
도메인	정보보안	난이도	중(상/중/하)
키워드	Chromium, SQLite DB, AES Key Gecko, logins.json, NSS Library nss3.dll, PK11SDR_Decrypt		
출제배경	최근 전체 악성코드 중 절반이상을 차지하는 인포스틸러에 대한 출제		
참고문헌	안랩(https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=32320) 민간사이버안전매뉴얼(기업정보보호 담당자용) (KISA, 2006.02.28)		
해설자	소원반 소민호 기술사(제 119회 정보관리기술사 / mhsope@naver.com)		

I. 정보 탈취 악성코드, 인포스틸러(InfoStealer)의 개념 및 종류

구분	설명	
개념	- 정보 탈취형 악성코드로서 웹 브라우저나 이메일 클라이언트 같은 **프로그램에 저장되어 있는 사용자 계정 정보나 가상화폐 지갑 주소, 파일과 같은 사용자의 정보들을 탈취**하는 것이 목적인 악성코드 - 정보와 도둑이 합성어로 사용자의 컴퓨터에 침입해 웹브라우저, 암호화폐 지갑, 이메일 프로그램 등에 저장되어 있는 사용자 정보를 탈취하는 악성코드	
탈취 정보	- 사용자 계정 정보, 쿠키, 히스토리, 키로깅, 클립보드 탈취, 암호화폐 지갑주소, 인증서, 신용카드, 문서 파일, 설치 프로그램 등	
종류	비다르(VIDAR)	- 타 악성코드(랜섬웨어)를 다운로드하는 기능을 추가적으로 수행 - **이력서, 공공기관의 사칭 스팸메일**, 인증 툴, PUP를 위장해 유포
	레드라인 (RedLine)	- 정보를 탈취한 수 자신의 흔적을 지우고 타 악성코드를 심는 특징을 가짐 - **코로나19 악용 피싱메일**, 악성 프로젝트파일, **구글광고 악용, 정상프로그램 위장해** 유포
	크립트봇(CrytBot)	- 메일, 메신저, 게시판, 자료실을 통해 **크랙 파일로 위장하여 배포** - 특정 키워드 검색 시 피싱 사이트를 상위에 노출시켜 다운로드를 유도

II. 인포스틸러(InfoStealer) 공격 절차

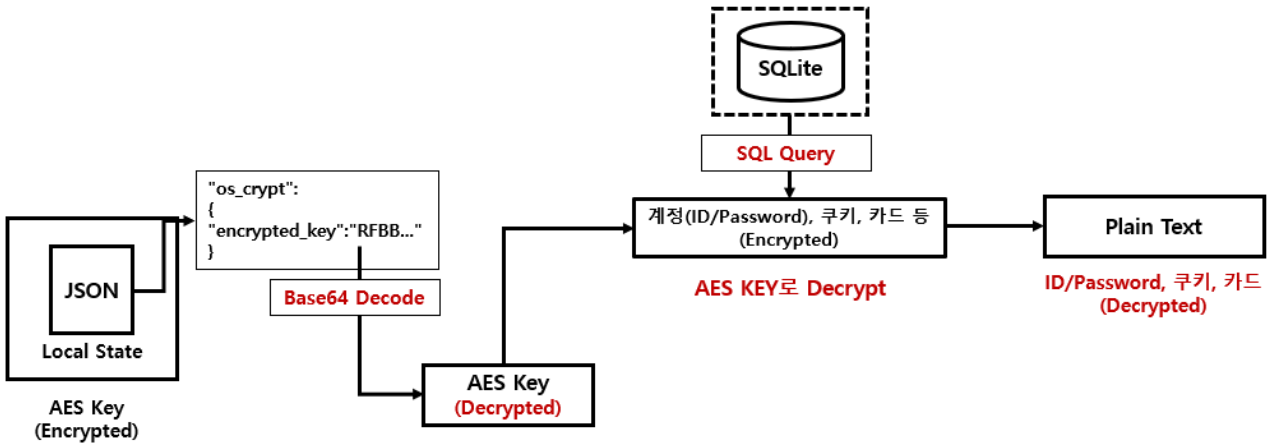
가. 일반적인 인포스틸러 공격 절차



순서	공격절차	설명
1	악성코드 감염	- 이메일, 첨부파일, 피싱사이트, 크랙파일 통한 악성코드 감염
2	시스템 스캔	- 개인정보가 있는 **브라우저 파일**, 이메일 프로그램, 파일 디렉토리 등 검색
3	개인정보 수집	- 파일, Database 파일에 접근해서 개인정보 추출 - 사용자 계정 정보, 쿠키, 히스토리, 키로깅, 클립보드 탈취, 암호화폐 지갑 주소, 인증서, 신용카드, 문서 파일, 설치 프로그램 등 다양한 정보 수집
4	개인정보 전송	- C&C 서버에 개인정보 전송
5	개인정보 활용	- 수집된 개인정보 다크웹 등에 판매 - 사이트에 로그인하여 악의적인 행위, 금전적 피해 유발
6	사용자 PC 무력화	- 사용자 PC를 다른 악성코드에 감염(랜섬웨어 등) 무력화, 2차 피해 발생

나. Chromium기반 브라우저 인포스틸러 공격 절차

- Chromium은 구글(Google)에서 개발 및 관리되는 오픈소스 웹 브라우저로, 현재 제일 많이 사용되고 있는 웹 브라우저 엔진
- 대표적으로 크롬(Chrome), 엣지(Edge), 오페라(Opera) 등이Chromium 코드를 베이스로 개발



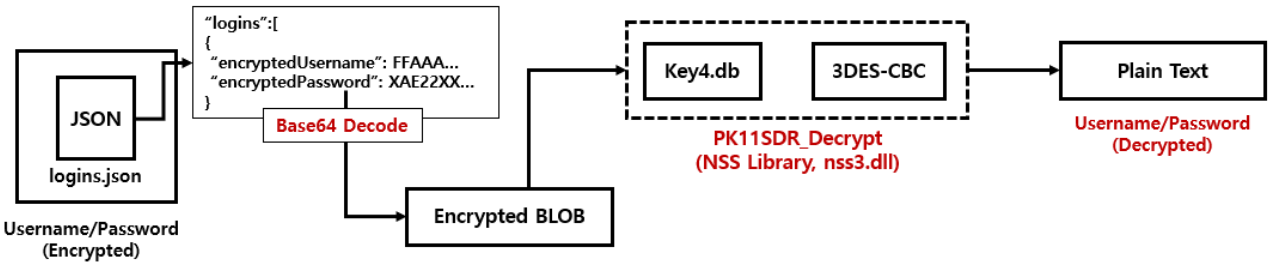
- Chromium 기반 웹 브라우저는 사용자가 웹 서핑을 하면서 저장하는 계정(아이디, 패스워드) 정보, 쿠키(Cookie) 데이터, 카드 정보, 히스토리, 자동 완성(Autofill) 등을 **로컬 시스템의 SQLite DB 파일에 저장**

순서	공격절차	설명
1	악성코드 감염	- 이메일, 첨부파일, 피싱사이트, 크랙파일 통한 악성코드 감염
2	시스템 스캔	- Chromium 기반 브라우저의 SQLite DB 파일 탐색
3	개인정보 수집	- SQL 쿼리문을 통해 개인정보 수집
4	개인정보 복호화	- Base64로 인코딩된 AES 키 추출 (키파일 위치 : (생략)...₩User Data₩Local State 파일의 "os_crypt" : {"encrypted_key"} 위치에 저장) **- Base64 디코딩을 통해 AES 키 획득** - 획득한 AES 키를 통해 암호화된 데이터를 평문화 시킴
5	개인정보 전송	- C&C 서버에 개인정보 전송

- 비밀번호 외 모든 암호화된 필드값도 동일한 방법을 활용해 평문으로 복호화 할 수 있음.
- Cookies 테이블의 encrypted_value, Credit_Card 테이블의 card_number_encrypted 필드 등

다. Gecko 기반 브라우저 인포스틸러 공격 절차

- 모질라(Mozilla) 재단에서 개발 및 관리하는 오픈소스 웹 브라우저 엔진
- 대표적으로 파이어폭스(Firefox), 썬더버드(Thunderbird), 아이스드래곤(IceDragon), 사이버폭스(Cyberfox) 등



- Gecko 브라우저에서 저장된 계정 정보는 logins.json 파일에 암호화된 상태로 저장
- Gecko 브라우저의 암호화 데이터 관리는 모질라에서 개발한 NSS 라이브러리의 PK11SDR_Encrypt / PK11SDR_Decrypt 함수를 이용

순서	공격절차	설명
1	악성코드 감염	- 이메일, 첨부파일, 피싱사이트, 크랙파일 통한 악성코드 감염
2	시스템 스캔	- 계정 정보를 담고있는 logins.json 파일 검색(**암호화 됨**) - 쿠키 정보 cookies.sqlite, 히스토리 places.sqlite DB 파일 검색(**암호화 안됨**)
3	개인정보 수집	- logins.json 파일에서 계정정보 수집 - SQL 쿼리문을 통해 쿠키정보, 히스토리 정보 수집
4	개인정보 복호화	- NSS Library nss3.dll의 PK11SDR_Decrypt 함수 동적 로드 - logins.json에서 추출한 암호화된 계정 정보를 평문으로 복호화
5	개인정보 전송	- C&C 서버에 개인정보 전송

- NSS 라이브러리의 PK11SDR_Encrypt / PK11SDR_Decrypt 함수를 이용 Username, Password 복호화 가능

III. 조직의 정보보안 담당자 입장측면 공격에 대한 대응방안

가. 정보보안 담당자의 기술적 및 예방활동 측면 대응방안

구분	대응방안	설명
기술적 대응방안	스팸메일차단 솔루션 도입	- 수신 메일을 대상으로 스캐닝을 통해 악의적인 의도를 가진 메일을 필터링
	멀티팩트인증	- N 가지 요소 인증 연결(지식+생체, 지식+소유, 소유+생체)
	비밀번호 업데이트	- 비밀번호를 주기적으로 변경
	자동로그인 해제	- 웹사이트 자동로그인 해제, 아이디, 비밀번호 저장 안함.
	히스토리 삭제	- 주기적으로 히스토리 삭제
	정품 소프트웨어 사용	- 정품 소프트웨어 구매 및 사용
	불분명한 이메일 삭제	- 발신자가 불분명한 이메일 삭제
	최신 백신 프로그램 사용	- 최신 소프트웨어 업데이트 및 백신 업데이트
	정기적 백업 수행	- 정기적으로 데이터 백업 및 분리보관
예방활동	서버의 점검	- 불필요한 네트워크 서비스 제거 - 서버소프트웨어 보안 패치 정보 확인/적용 - 불필요한 계정이 있는지 확인 및 삭제 - 최신 악성코드 정보 파악 및 보안 패치 - 주기적으로 중요한 시스템 및 데이터베이스 백업 - 로깅 실시 및 로그파일 매일 점검
	네트워크의 점검	- 로그기능 설정 및 로그 모니터링 - 네트워크 접근통제정책 확인 - 네트워크장비 보안 패치 실시 - 사용하지 않는 서비스 중지 - 네트워크 장비에 대한 이중화 및 백업체계 마련 - 관리계정에 대한 비밀번호 관리 - 보안도구 활용 내재된 취약점 점검
	보안장비의 점검	- 보안 도구 활용 침입차단시스템 설정 확인 - 침입탐지시스템의 탐지 규칙을 최신 규칙으로 업데이트 - 악성코드 필터링 규칙을 항상 최신의 상태로 업데이트 - 침입차단/탐지시스템의 로그를 주기적으로 모니터링 한다. - 각 서비스 포트는 반드시 필요한 포트만 허용
	보안정책	- 중요한 로그, 이벤트 메시지 발생시 관리자에게 통보되도록 설정 - 모든 컨텐츠 서버에 대하여 엄격한 접근통제리스트 유지 - 모든 사용자에 대하여 보안성이 있는 암호를 사용하도록 권고 - 관리 계정에는 보안성이 있는 암호 사용
	기타	- 모든 서버에 대하여 주기적으로 바이러스 검사 - 보안 패치 배포여부 모니터링

나. 정보보안 담당자의 정보보안사고관리 측면 대응방안

구분	대응방안	설명
보안사고 관리	보안사고 발생 확인	- 보안사고 발생 확인 즉시 사고 보고
	등급분류	- 보안사고의 등급 분류
	대응 팀 구성	- 자체 사고대응팀 구성, 사고대응 처리, 외부 침해사고대응기관 협조
	대응전략 체계화	- 최적의 전략을 결정하고 정보보안책임자의 승인 획득
	모니터링 및 재발방지 대책	- 데이터 수집 및 분석을 통해 사고 경유, 피해 확산 및 사고 재발을 어떻게 방지할 것인지를 결정
	적용및 사고처리 완료보고	- 사고에 대한 정확한 보고서를 작성하여 보고
	이력관리	- 유사 공격 예방위한 보안정책의 수립, 지침변경, 사건의 기록, 장기 보안정책 수립, 기술 수정 계획수립 등을 결정
보안사고 예방	불필요한 계정 삭제	- 불필요한 계정, 패스워드가 없는 계정에 대한 조치
	진단도구 활용	- 보안 진단도구를 이용하여 시스템을 수시로 점검
	접근통제	- 접근통제 시스템을 구축하여 불법 침입자의 접근을 차단
	사전 해킹 대비	- 최근 해킹방법 및 대처방안에 대한 자료를 입수하여 대비
	IDS, IPS 설치	- 침입자 탐지시스템을 설치하여 실시간으로 침입 식별
	백신 프로그램 배포	- 바이러스 백신 프로그램 배포, 바이러스 정보 게시판 게시
	취약점 분석 및 보호	- 취약점 분석 및 결과에 대한 보호대책을 이행
보안사고 대응 및 복구방안	보안사고 대응 조직	- 보안사고대응팀(CERT) 구성
	보안사고 보고체계	- 보안사고와 관련 이해관계자들에게 보고
	보안사고대응 처리방안	- 침투 자산 식별, 침입 흔적 등 보안 진단도구나 체크리스트를 이용하여 점검하고 보안사고 처리결과서를 작성하여 보고
	증거자료 수집, 보관	- 시스템이벤트, 접속기록 등 모든 관련 로그 수집, 별도 보관
	보안사고 처리및 재발방지	- 사고경위를 조사, 분석 수행, 보안사고의 재발방지에 노력
보안사고 사후대응	대응전략 수립	- 주어진 사건의 환경에서 가장 적절한 대응전략 결정 - 대응전략 수립 시 정책, 기술, 법, 업무 등 고려
	정보보안사고 상세 분석	- 탐지 및 접수된 이상 징후 분석, 외부 전문가 지원 활용 - 시스템, 주요 서비스 로그 파일, 프로세스 현황, 열려진 포트 현황, 사용자 디렉토리 점검, 최신 해킹 프로그램 점검 등
	보고서 작성	- 보안사고대응 결과보고서를 작성하여 관리
	사후 대응	- 재발방지 대책 수립/적용, 보안담당자 통보
	보안사고에 관한 교육 및 훈련	- 보안사고 대응방안, 정보보호 정책, 절차, 조직 등 보안사고대응 체계 교육 및 훈련 수행

IV. 인포스틸러 예방을 위한 정보보호 실천수칙

구분	정보보호 실천수칙	설명
기업	정보보호 교육	- 임직원 대상 정기적인 정보보호 교육 실시
	정보보호 정책 수립 및 담당자 지정	- 정보보호 정책·지침을 수립하고 책임자와 담당자를 지정하여 운영
	접근통제	- 정보시스템의 사용자계정 및 접근권한 관리하기
	정보자산 분류	- 기업의 정보자산 분류기준을 수립하고 목록 관리
	보안 정기점검	- 개인 및 공용 업무 환경의 PC, 노트북은 정기적으로 보안점검 (백신설치, 보안업데이트, 화면보호기 설정, 비밀번호 변경 등)
	주기적 취약점 분석, 시큐어코딩 적용	- 주기적인 취약점 점검·보완 및 홈페이지 제작시 시큐어 코딩 준수
	정기적 백업 수행	- 중요정보는 정기적으로 백업하고 안전하게 별도 관리
	중요문서 파쇄	- 사무실내 중요문서는 방치되지 않도록 하고 반드시 파쇄
	폐기시 데이터 삭제	- 시스템 및 소프트웨어 폐기 시에는 기록된 데이터 완전하게 삭제
	보안관련 준수여부 점검	- 기업이 지켜야할 보안관련 법적요구사항을 파악하고 준수여부 점검
사용자	최신 보안업데이트	- PC 운영체제 및 소프트웨어 최신 보안 업데이트
	자동 보안업데이트 설정	- PC 윈도우즈 운영체제 자동보안업데이트 설정
	백신프로그램 설치	- 백신프로그램을 설치하고 바이러스 검사
	비밀번호 주기적 변경	- PC 비밀번호 설정기능 사용하고 주기적으로 변경
	안전한 사이트 방문	- 언제 어디서든 신뢰할 수 없는 웹 사이트는 방문하지 않기
	인증서 안전 저장	- 공인인증서는 외장매체에 안전하게 저장
	스팸메일 삭제	- 출처가 불분명한 이메일은 열어보지 말고 삭제
	정품 OS, SW 사용	- 정품 OS(운영체제)를 사용하기(스마트폰 탈옥하지 않기)
	스팸문자 삭제	- 의심스러운 문자메세지는 열지 말고, 바로 삭제
	공유기 패스워드 설정	- 공유기 관리자/WiFi 패스워드 설정하기/WiFi 패스워드 설정

- 개인정보보호위원회는 평소 온라인 상에서 사용하는 계정정보(아이디, 패스워드)를 입력하면, 유출된 이력을 알려주는 '**털린 내정보 찾기 서비스**'를 제공, 해당 서비스를 통해 지속적으로 개인정보 관리가 필요

"끝"

02	정규화		
문제	데이터베이스에서 정규화는 이상현상(Anomaly)이 있는 릴레이션(Relation)을 해결하기 위한 방법이다. 다음의 <수강테이블>을 활용하여 설명하시오. 가. 이상현상 3가지와 발생 이유 나. 해결방안 다. 테이블 재구성		
도메인	데이터베이스	난이도	중(상/중/하)
키워드	2차 정규화 수행 후 3차 정규화 수행, 부분함수 종속성, 이행함수 종속성		
출제배경	데이터베이스 기본토픽(정규화) 이해 확인		
참고문헌	ITPE 기술사회 자료		
해설자	강남평일야간반 전일 기술사(제 114회 정보관리기술사 / nikki6@hanmail.net)		

I. 데이터 이상현상 제거, 정규화의 기본원칙

가. 데이터의 일관성과 정확성을 위한 정규화의 개념

- 이상현상을 발생시키는 속성 간의 종속성, 중복성을 제거하고 무결성을 보장하기 위해 릴레이션을 분해하는 과정

나. 정규화(Normalization)의 기본 원칙

구분	기본 원칙	세부 내용
일관성/ 정확성	정보의 무손실	- 분해된 릴레이션이 표현하는 정보는 분해되기 전의 정보를 모두 포함
	분리의 원칙	- 하나의 독립된 관계성은 하나의 독립된 릴레이션으로 분리하여 표현
	데이터 중복성 감소	- 최소의 중복으로 여러 이상현상 제거
사용성	구조 리팩토링	- 같은 의미의 정보를 유지하면서 더 바람직한 구조로 변환해야 함
	가용성 향상	- 자료검색과 추출의 효율성 추구

- 정규화는 이상현상을 제거, 관계 모델의 명확성 추구를 목적으로 함

II 수강테이블에서 이상현상 3가지와 발생 이유

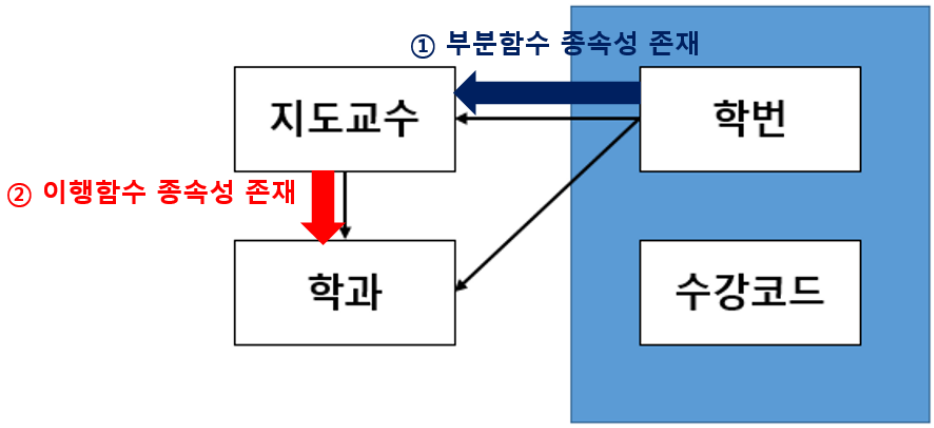
가. 수강테이블에서 이상현상 3가지

<수강테이블> 기본키: {학번, 수강코드}

학번	학과	지도교수	수강코드
221571	컴퓨터학과	K1	C412
221572	컴퓨터학과	M1	C412
211561	수학과	P2	C324
201511	전기과	C1	E123
201511	전기과	C1	C412

이상현상	세부 내용
삽입 이상	- 새로운 학과 발생 시 가짜 학번(999999)를 생성해야만 함
삭제 이상	- 학생 퇴원 시, 소속된 학과도 함께 삭제됨
갱신 이상	- 일부 학번의 학과 수정 시 다른 컬럼의 학과도 함께 수정해야 함

나. 이상현상 발생 이유

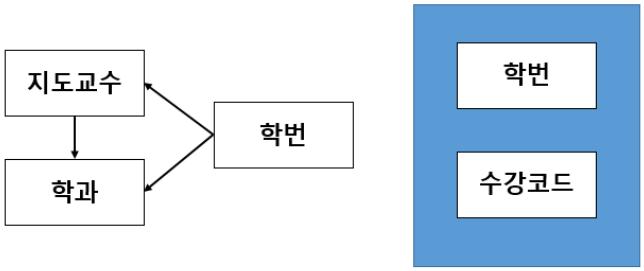
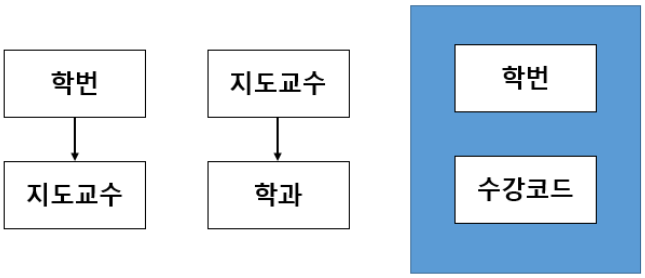


① 부분함수 종속성 존재	- 학번(부분집합)이 지도교수를 식별/결정 - X→Y에서 Y가 X의 부분집합에 대해서도 함수적으로 종속되는 경우
② 이행함수 종속성 존재	- 학번에 의해 지도교수가 식별/결정 - 일반 속성인 지도교수에 의해 학과가 FD(Functional Dependency) 관계 존재 - 결국, 릴레이션 R에서 A→X이고, X→Y 이면 A→Y 인 관계

- 해당 테이블에서 부분함수 종속성과 이행함수 종속성이 존재하므로, 2차 정규화와 3차 정규화 수행 필요

III. 수강테이블 이상현상 해결방안과 테이블 재구성

가. 수강테이블 이상현상 해결방안 (2차 정규화 → 3차 정규화)

해결 방안	정규화 수행 결과	상세 설명
1) 2차 정규화 수행		- 부분함수 종속성 제거해 모든 일반속성이 기본키에 완전 종속되도록 구성
2) 2차 정규화 후 3차 정규화 수행		- 이행함수 종속성을 제거하기 위해 학번-지도교수, 지도교수-학과 테이블로 분리

나. 수강테이블 재구성

<학번-지도교수 테이블>
기본키: {학번}

학번	지도교수
221571	K1
221572	M1
211561	P2
201511	C1

<지도교수-학과 테이블>
기본키: {지도교수}

지도교수	학과
K1	컴퓨터학과
M1	컴퓨터학과
P2	수학과
C1	전기과

<학번-수강 테이블>
기본키: {학번, 수강코드}

학번	수강코드
221571	C412
221572	C412
211561	C324
201511	E123
201511	C412

- 학번-지도교수의 학번 기본키는 학번-수강테이블의 학번 컬럼에 외래키로, 지도교수-학과 테이블의 지도교수 기본키는 학번-지도교수 테이블의 지도교수 컬럼에 외래키로 연결 구성 가능

IV. 정규화 진행 시 검토사항

검토사항	세부 내용
동료 검토	- 데이터 모델링 시 논리 모델 단계에서 물리 모델 진행에 따른 함수적 종속성 동료 검토 실시
Trade-off 관계 확인	- 업무가 익숙하고 시스템 규모가 작은 경우 세분화된 정규화는 오히려 속도 저하 비효율 발생 고려
전문가 참여	- 모델링 시 기술적 능력과 업무 프로세스에 충분한 지식을 베이스로 한 DA(Data Architect) 참여 필수

- 질의 성능 향상 및 모델의 복잡도 개선 위해 일부 비(반) 정규화 과정도 함께 고려

"끝"

03	반도체 산업 생태계		
문제	반도체 생태계를 차지하고자 하는 글로벌 기업들의 소리없는 전쟁이 계속되고 있다. 우리나라는 메모리 반도체의 강국이지만 비메로리 반도체 분야에서는 뒤쳐져 있다. 다음에 대하여 설명하시오. 가. 메모리 반도체와 비메모리 반도체 비교 나. 반도체 산업의 가치사슬(Value Chain) 다. 비메모리 반도체 성장을 위한 비전과 전략		
도메인	경영전략/CA	난이도	중(상/중/하)
키워드	정보저장, 정보처리, D램, S램, CPU, IDC, 팹리스, 칩리스, 전공정, 후공정		
출제배경	반도체 생태계 관련 국가 전략 인사이트 확인		
참고문헌	밸류체인 기반 산업경쟁력 진단시스템 구축사업-반도체산업편_산업통상자원부, 산업연구원_2021		
해설자	정상 기술사(제 12X회 정보관리기술사 / jeongsang_pe@naver.com)		

I. 메모리 반도체와 비메모리 반도체 비교

가. 메모리 반도체와 비메모리 반도체의 개념비교

메모리 반도체	비메모리 반도체
- 정보를 기억하는 목적으로 만들어진 반도체 - 정보를 저장하는 방식으로 휘발성의 RAM과 비휘발성의 ROM으로 구분되는 반도체	- 정보를 처리하는 목적으로 제작된 반도체 - 시스템 반도체로 전자제품의 두뇌 역할을 하는 칩으로 많이 사용되어 필수적인 반도체

- 정보에 대한 역할에 따라 반도체 종류 구분

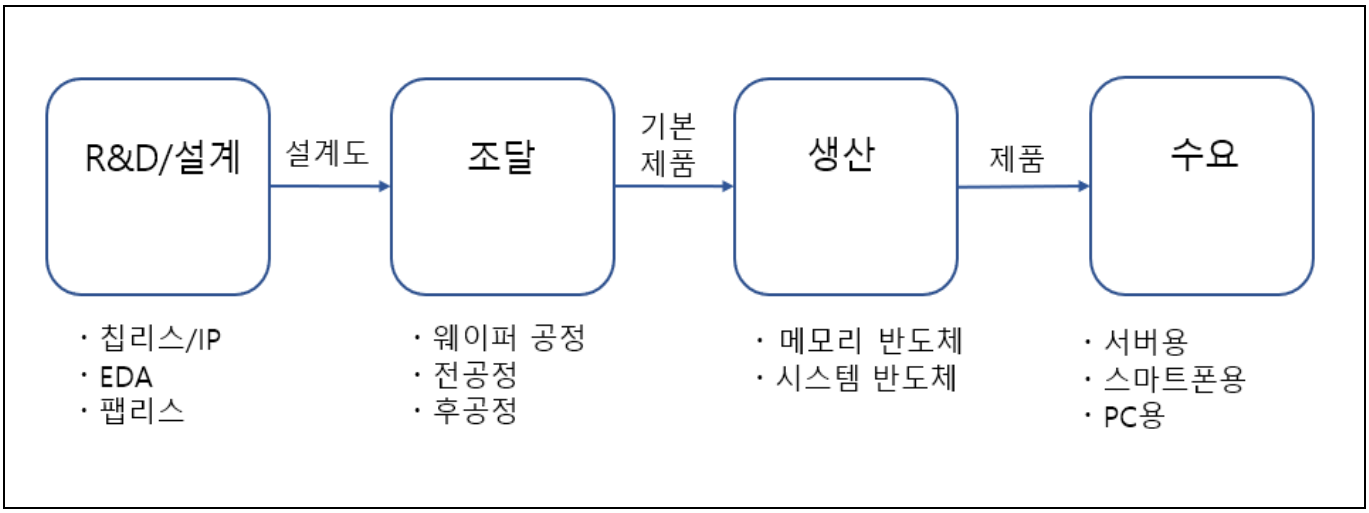
나. 메모리 반도체와 비메모리 반도체의 상세비교

구분	메모리 반도체	비메모리 반도체
목적	정보 저장	정보 처리, 연산, 추론
시장구조	소품종 대량양산	다품종 소량양산
시장 변동성	민감	둔감
생산구조	설계 업체가 대부분 양산	대부분 설계와 양산 업체 분리
경쟁력	자본력, 선행기술 개발, 설비투자	설계기술, 우수 설계인력
제품	D램, S램, V램, 롬 등	CPU, ASIC, MDL, 멀티미디어 반도체 파워반도체, 개별소자 등
주요업체	삼성전자, 하이닉스, Micron	Intel, Qualcomm, ST Micro

- 메모리 반도체 주도의 현 상황에서 비메모리 반도체 경쟁력 확보를 위한 전략 수립

II. 반도체 산업의 가치사슬(Value Chain) 및 상세 설명

반도체 산업의 가치사슬(Value Chain)



- 반도체 산업의 가치 사슬은 R&D 설계부터 조달까지의 전체 프로세스 영역에서 구성

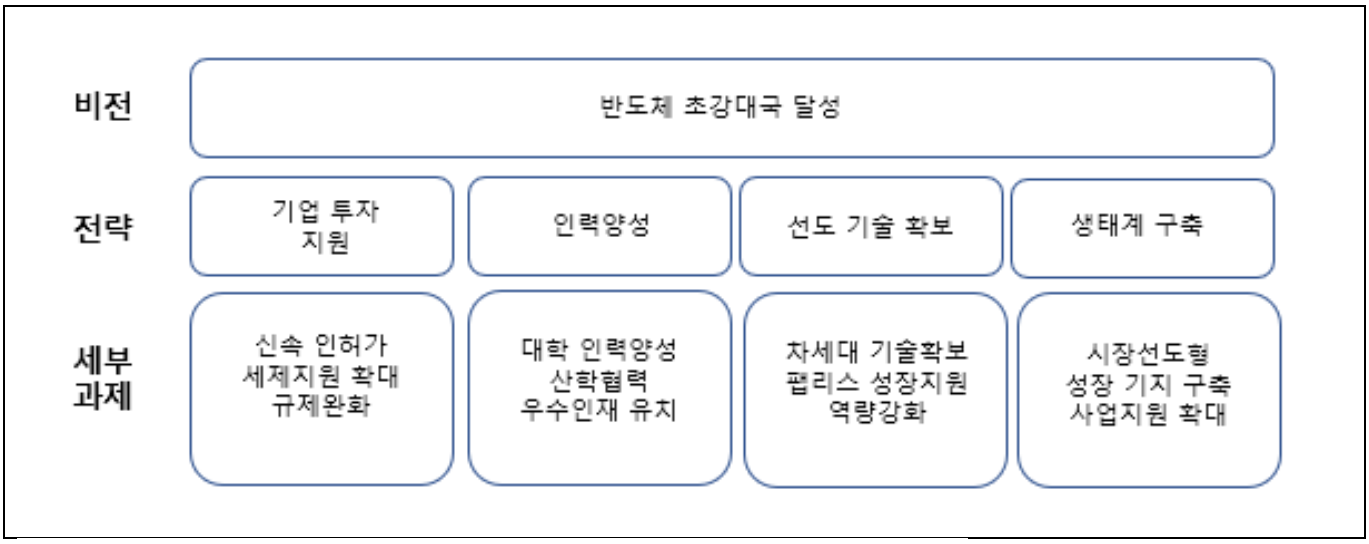
나. 반도체 산업의 가치사슬(Value Chain)의 상세 설명

구분	상세활동	설명
R&D/설계	칩리스/IP	- 팹리스와 파운드리 중간 역할을 하는 ODM
	EDA	- 반도체 제조에 사용되는 전문 소프트웨어
	팹리스	- 시스템 반도체의 설계와 개발만을 전문으로 수행
조달	웨이퍼 공정	- 원형의 판으로 생산되는 반도체 집적회로
	전공정	- 웨이퍼 위에 회로를 새겨 칩을 완성하는 공정 일체
	후공정	- 웨이퍼 상의 칩을 분리하여 패키징 및 테스트하는 공정
생산	메모리 반도체	- 정보를 기억하는 목적으로 만들어진 반도체
	시스템 반도체	- 정보를 처리하는 목적으로 만들어진 반도체
수요	서버용	- 특수한 목적으로 사용될 컴퓨터용 반도체
	스마트폰용	- 스마트 기기에 사용될 모바일용 반도체
	PC용	- 일반 PC에 사용될 목적으로 만들어진 반도체

- 각 가치 사슬을 기반으로 다른 활동으로 반도체 생산 진행

III. 비메모리 반도체 성장을 위한 비전과 전략 설명

가. 비메모리 반도체 성장을 위한 비전과 전략 구성도



- 국가적인 측면에서 메모리, 비메모리 반도체 경쟁력 확보를 위한 전략 수립

나. 비메모리 반도체 성장을 위한 비전과 전략 상세 설명

구분	설명	
비전	비메모리 반도체 산업 경쟁력 확보	- 메모리 중심의 산업 경쟁력을 비메모리 중심으로 옮겨 반도체 초강대국 달성
전략	기업 투자 총력 지원	- 기업의 산업 활성화를 위한 투자 지원
	민관 협력 인력양성	- 인재 양성을 위한 프로세스 구축, 관리 강화
	선도기술 확보	- 차세대 반도체 개발 관련 기술 개발
	소부장 생태계 구축	- 경쟁력 강화를 위한 생태계 구축
세부과제	기업 산업 활성화	- 인프라 지원 및 신속 인하가 진행 - 기업투자 세제지원 확대 - 노동/안전 등 규제 완화
	지속적인 인력 육성	- 대학/대학원 통한 인력 양성 - 산학협력 4대 인력양성 인프라 구축 - 시스템 반도체 생태계 역량강화
	선도적 신기술 확보	- 3대 차세대반도체 기술개발 - 유망 팹리스 성장 지원 - 시스템 반도체 생태계 역량 강화
	산업 생태계의 구축	- 시장 선도형 기술 개발로 전환 - 소부장 기업 성장 기지 구축 - 유망기술 사업 지원 확대

- 전략기반 세부 실행계획 수립으로 단계적 생태계 구축 진행

"끝"

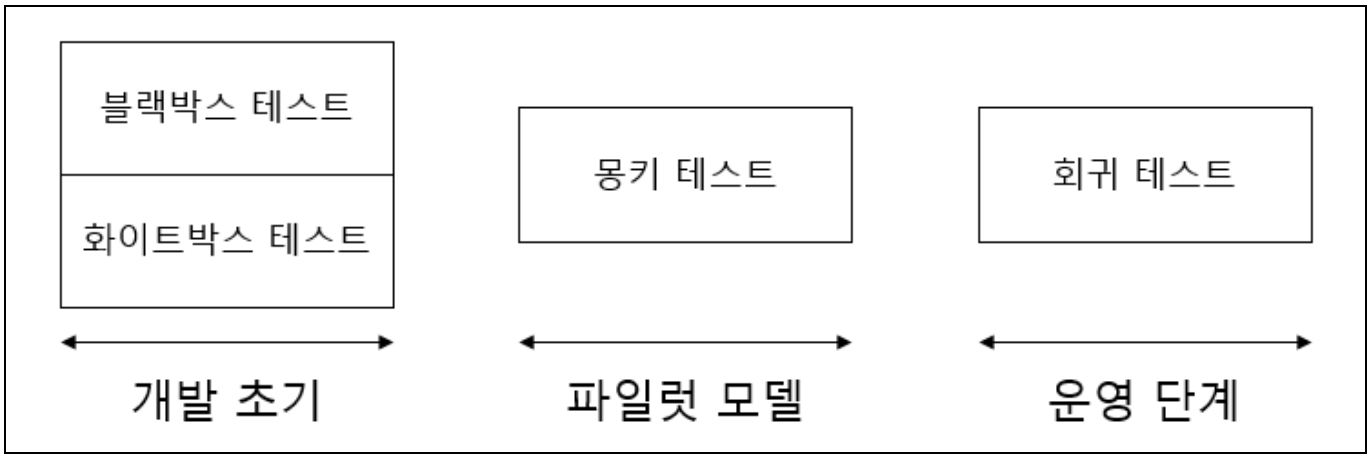
04	몽키테스트/회귀테스트/통합테스트		
문제	정보시스템 개발 및 운영 단계에서 수행하는 소프트웨어 테스트와 관련하여 다음 사항에 대하여 설명하시오. 가. 몽키 테스트(Monkey Test)와 회귀 테스트(Regression Test) 비교 설명 나. 통합 테스트 계획서에 포함되어야 할 주요 사항		
도메인	소프트웨어공학	난이도	중(상/중/하)
키워드	UI 테스팅, 랜덤, 스크립트, monkey runner, 수정 영향 확인, Selenium		
출제배경	모바일 환경 중요도 증가에 따라 다양한 테스트 기법이 활용되고 있어, 관련 지식을 위한 출제		
참고문헌	UI/Application Exerciser Monkey(https://developer.android.com/studio/test/monkey?hl=ko)		
해설자	서경석 기술사(제119회 정보관리기술사 / akslemf@naver.com)		

I. 소프트웨어의 완전성 확보, 소프트웨어 테스트의 개요

가. 소프트웨어 테스트의 정의

- 시스템이 정해진 요구를 만족하는지, 예상과 실제 결과가 어떤 차이를 보이는지 수동 또는 자동 방법을 동원하여 검사하고 평가하는 일련의 과정

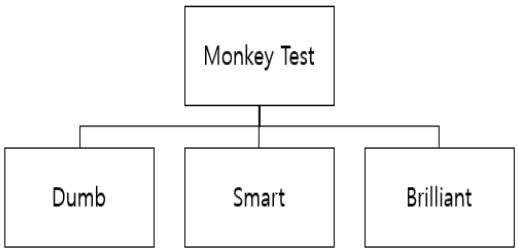
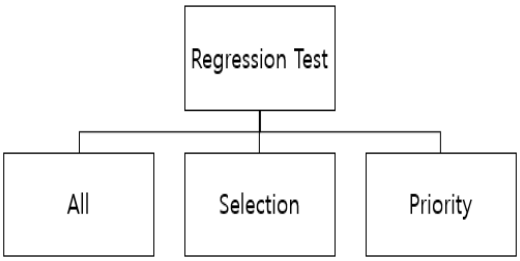
나. 소프트웨어 테스트의 유형



- 소프트웨어 개발, 운영, 유지 보수 전반에 걸쳐 지속적인 테스트를 통한 소프트웨어의 안정성 증가 추구

II. 몽키 테스트와 회귀 테스트 비교

가. 몽키 테스트와 회귀 테스트 개념 및 개념도 비교

구분	몽키 테스트	회귀 테스트
개념	- Android에서 지원하는 UI 테스팅 툴로 터치,제스쳐 등의 이벤트를 랜덤으로 발생시키거나, 스크립트 파일을 이용해서 원하는 UI Action을 수행하는 테스트	- 수정한 부분이 소프트웨어의 다른 부분에 영향을 미치는지 테스트 하여 소프트웨어 수정이 새로운 오류를 발생시키지 않았는지 확인을 위한 테스트
유형		

- 소프트웨어의 중요도, 성격, 단계에 따라 적합한 테스트 유형을 적용

나. 몽키 테스트와 회귀 테스트 상세 비교

구분	몽키 테스트	회귀 테스트
목적	- 사람이 예상하지 못한 오류 발견	- 수정에 따른 영향도 확인
대상	- 에뮬레이터, 디바이스	- 수정 대상 소프트웨어 전체
수행 시기	- 초기 모델 개발 단계	- 운영 환경 수정 발생 시
절차	- 스크립트 작성 -> 실행 -> 오류 검출	- 수정 발생 -> 영향도 분석 -> 실행
추적성	- 매우 빠르게 진행 되어 추적 불가	- 테스트 시나리오 기반 추적 가능
완료 시점	- 일정 시간 수행 후 종료	- 영향 받는 대상, 시스템 점검 완료 시
고려 사항	- 충분한 자원 확보 - 예상 되지 않은 출력 - 소프트웨어 신뢰성 확보	- Record & Replay - 유동적 계획 수립 - 결합도
특징	- 미확신 기반 테스트 - 시험 관점 누수 배제 - 개발자 의도와 무관	- 성능과 기능 Trade off - 정합성 테스트 - 결함 조치 확인
도구	- monkeyrunner	- Selenium, QTP, RFT

- 사람이 확인 하기 어려운 오류를 몽키 테스트를 통해 발견 하고 해당 부분에 대해 수정 진행 후 영향도 분석을 위한 회귀 테스트 추가 진행 완료 후에 소프트웨어 전반에 걸친 통합 테스트 진행 필요

III. 통합 테스트 개요 및 통합 테스트 계획서에 포함되어야 할 주요 사항

가. 통합 테스트 개요

구분	세부	설명
정의	- 컴포넌트간 인터페이스, H/W 시스템간 인터페이스와 같은 각기 다른 부분과 상호 연동 확인을 위해 모듈별 그룹 구성 후 진행하는 동작 테스트	
필요성	- 결속 동작 확인	- 다수의 개발자 참여, 기능별 분리 개발에 따른 정상 연계 확인
	- 요구 사항 변경	- 단위 테스트 이후 추가 발생된 요구 사항의 보완 테스트
	- 내외부 연계	- 내외부 I/F 발생 시 모듈간 정상 연계에 대한 확인 필요
	- 예외 처리 검증	- 부적절한 예외 처리로 인한 타 시스템 연계 오류 검증
방식	- 빅뱅 방식	- 모든 구성 요소 통합 완료 후 테스트 진행 - 구성 요소 통합 후 진행에 따른 테스트 시간 부족, 발생 위치 확인 어려움, 중요도에 따른 우선 순위 지정 불가
	- 상향식	- 하위 레벨의 테스트 모듈과 상향 레벨 모듈 동시 테스트 - 테스트 진행을 위해 테스트 드라이버 생성 필요
	- 하향식	- 테스트 진행 시 시스템의 제어 흐름을 상위에서 하위 레벨 진행 - 테스트 진행을 위해 테스트 스텁 생성 필요
	- 샌드위치 방식	- 상향식, 하향식 혼합 테스트 모델

- 통합 테스트의 성공적 수행을 위해 적절한 방식 결정 후 상세 수준 통합 테스트 계획서 작성 필요

나. 통합 테스트 계획서에 포함되어야 할 주요 사항

주요 사항	설명
차수 별 목표 이미지	- 목표 이미지는 작은 범위에서 큰 범위로 확장 - 처음부터 큰 범위로 확장할 경우에 문제를 찾는 것이 어려울 수 있음을 인지
진행 프로세스	- 통합 테스트의 단계별 진행 절차 및 방법론 정의
수행 주체와 R&R	- 테스트 시나리오 및 케이스 작성과 수행에 대한 R&R 수립 및 조직 구성
인프라 환경과 일정	- 통합 테스트는 일반적으로 운영 환경에서 진행되므로 데이터 이관 작업 필요 - 데이터 확보, I/F 장비, 인프라 환경 정상 구축 여부 확인 후 테스트 진행
테스트 시나리오	- 각 차수별 목표에 맞는 시나리오 선정, 시나리오 해당 테스트 케이스 정의
테스트 케이스	- 테스트 시나리오에 적합한 단계별 필요 부분 테스트 상황 정의
진척 관리 방법	- 테스트 시나리오 수행률, 성공률, 결함 처리율 등 현황 별 지표 관리 - 진척 집계 및 모니터링 도구 정의 필요
결함 처리 절차	- 결함 발생 시 반복 테스트, 결함 재등록 등 필요 활동 처리 순서 정의
합의 프로세스	- 통합 테스트 계획 수립 시 이해관계자 전체 참여 공식 회의 진행 - 이해 관계자가 모두 합의하는 프로세스 수립 및 공통 의견 도출 필요

- 각 역할별, 계층별 의사소통과 합의 기반 하 각 단계 완료 시 이해관계자 공유 통한 의사 소통 문제 발생 예방 및 통합 테스트 완성도 향상 가능

IV. 통합 테스트 계획서 목차 사례

제목 및 문서 번호	- ABC 시스템 고도화 통합 테스트 계획서(문-001)
테스트 항목	1. 통합 데이터베이스 정합성 확인 2. A, B, C 시스템 연계 I/F 3. 기능, 비기능 요구 사항 충족 여부
테스트 방식	상향식 선정 사유 : 다수 시스템 통합에 따른 개별 시스템 위험 요소 완화
테스트 Pass/Fail 기준	개별 테스트 시나리오 및 케이스에 상술
산출물	1. 통합 테스트 시나리오 2. 단위 테스트 시나리오/케이스 3. 단위 테스트 결과 보고서 4. 통합 테스트 결과 보고서
테스트 환경	서버, DB, I/F, Infra : 운영 환경과 동일 구축
테스트 일정	통합 테스트 계획 수립 : '23.01.01 ~ '23.01.31 1차 통합 테스트 : '23.02.01 ~ '23.02.28 1차 통합 테스트 결함 보완 : '23.03.01 ~ '23.03.15 2차 통합 테스트 : '23.03.16 ~ '23.03.31 통합 테스트 완료 보고 : '23.04.15
승인	ABC 시스템 고도화 PM(인)

"끝"

05	IT 투자분석		
문제	IT 투자분석의 프로세스, 프레임워크, 분석방법론에 대하여 설명하시오. 가. 프로세스 나. 프레임워크 다. 분석 방법론		
도메인	IT경영	난이도	하(상/중/하)
키워드	Real Option Valuation, Cost Benefit Analysis, Multi-Criteria Analysis		
출제배경	IT 투자와 성과의 프레임워크와 방법론 이해확인		
참고문헌	ITPE 기술사회 자료		
해설자	이상용 기술사(제 124회 정보관리기술사 / orangeday77@gmail.com)		

I. IT투자 효율 극대화, IT 투자분석의 개요

가. IT 투자분석의 정의

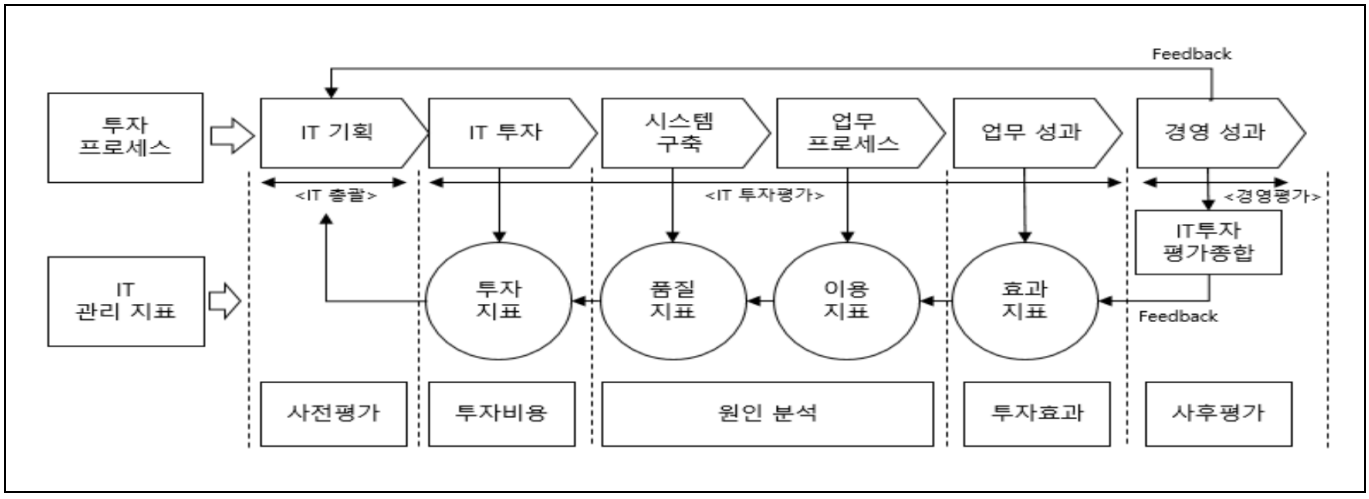
- IT가 기업의 목표 달성에 얼마나 기여를 하고 있으며, 경제적으로 얼마나 많은 공헌을 하고 있는 가를 사업적 관점에서 조사하고 분석하는 기법

나. IT 투자분석의 필요성

IT투자 형태의 복잡성	인프라, 플랫폼, 서비스 등 다양한 투자 형태가 존재
IT성과의 다양성	IT 투자를 통한 성과의 형태 다양성
IT투자의 객관화	IT 투자와 성과(가치)의 직접적인 연관성 객관화 난해

II. IT 투자분석의 프로세스 개념도와 단계

가. IT 투자분석의 프로세스 개념도



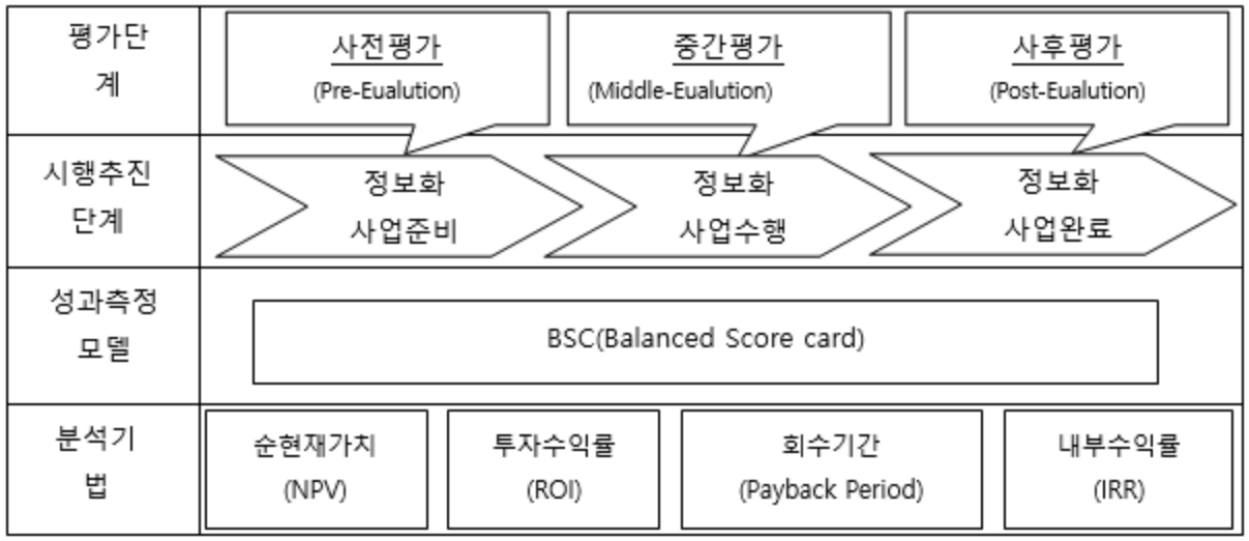
- 투자대비 성과에 대한 정확한 지표를 통해 해당 투자를 진행할 것인지에 대해 객관적인 지표로 활용
- 무형효과의 정량화 / 불확실성 파악 / 투자 타당성 파악 등의 효과 획득 가능

나. IT 투자분석의 프로세스 단계

추진 단계	세부 활동	설명
IT 기획	- 우선 순위 설정	- 법적, 전략적, 경제적 측면 등을 고려한 투자 우선 순위 설정
	- 타당성 검토	- Governance, Alliance 검토 및 예산, 시장 여건 고려
IT 투자	- KPI, CSF 점검	- IT 투자에 대한 기업의 중점 요소에 대한 점검 진행
	- 투자 여부 결정	- 비용 측면과 효과 측면을 고려하여 투자 여부 결정
시스템 구축	- 프로젝트 관리	- 비즈니스 부서의 요구 사항에 맞춘 프로젝트 진행 관리
	- 시스템 구현	- 명세서, 사양서 등에 적합한 형태의 IT 시스템 설계 및 구현
업무 프로세스	- 프로세스 점검	- 투자 관리 프로세스 준수 여부 및 적합도 평가
	- 프로세스 최적화	- 불필요 프로세스 제거 및 프로세스 보완 통한 업무 효율화
업무 성과	- 투자 효과 산출	- IT 투자 부분별 효과 정량적, 정성적 산출
	- KPI, CSF 수정	- 기획, 투자 단계에 수립 되었던 KPI, CSF 보완
경영 성과	- 투자 종합 평가	- 투자와 비즈니스 업무 성과 간 인과 관계 고려한 종합 평가
	- 의견 수렴 및 반영	- 평가 결과에 대한 기업 내부 의견 수렴 및 관리 기준 재반영

III. IT 투자분석의 프레임워크 개념도와 상세 설명

가. IT 투자분석의 프레임워크 개념도



나. IT 투자분석의 프레임워크 상세 설명

구분	세부 활동	설명
평가단계	- 사전평가	- 준비, 정의(전략과 위험요인), 추정(기대효과), 분석(전략과의 연계도), 결론도출(투자 우선순위)
	- 중간평가	- 검증(정보화 사업 추진비용), 분석(비용과 위험요인 수치화), 결론 도출(수정안 도출)
	- 사후평가	- 전략분석, 지표도출(CSF, KPI), 측정(KPI성과 측정), 분석(KPI수치 분석), 결론도출(정보화 사업 개선안 설계)
시행추진 단계	- 정보화 사업준비	- 내부조직 구성, 추진체계 수립
	- 정보화 사업수행	- 프로젝트 착수, 발주 및 계약, 실행 및 통제
	- 정보화 사업완료	- 프로젝트 종료, 사업관리 평가
성과추진 단계	- BSC (Balanced Score Card)	- 재무지표와 기업의 핵심성공요인(CSF, Critical Success Factor), 핵심성과지표(KPI, Key Performance Indicator)와 관련된 제반 운영상의 지표들을 결합하여 조직의 효과성 측정
분석 기법	- 순현재가치(NPV)	- 프로젝트의 예정 순이익을 현재의 화폐가치로 변환
	- 투자수익률(ROI)	- 자본 투자에 대비 수익 비율
	- 회수기간 (Payback Period)	- 프로젝트의 시작 시점부터 누적 흐름이 플러스로 돌아 서는 시점까지의 기간

IV. IT 투자분석의 분석방법론설명

분석방법론 유형	개념	유형 상세 기법
실물 옵션 가치 평가 (Real Option Valuation)	- 프로젝트에 대한 다양한 투자 옵션에 대한 가치를 평가하여 다음 단계의 투자를 결정하는 기법	- **블랙-숄즈(Black-Sholes) 모형:** 프로젝트 가치변화에 따른 IT투자옵션의 가치변화를 산식으로 도출
		- **이항모형:** 프로젝트 가치가 변화하는 경우의 수를 증가, 감소 2가지로 제한하는 이항옵션 모형 기반
		- **몬테카를로 평가 모델:** 확률 분포 근거하여 가치가 변화하는 모든 경로를 예측 산출 방법
비용편익분석 (Cost Benefit Analysis)	- 투입비용과 산출이익을 비교 분석하여 투자결정 및 타당성 확보기법	- **투자자본수익률(ROI, Return On Investment):** 내부 투자 대비 연평균 순이익의 비율
		- **투자회수기간(PP, Payback Period):** 손익분기점(BEP, Break Even Point)
		- **순현재가치(NPV, Net Present Value):** 프로젝트 비용과 이익 순현재가치로 산출(할인율) 예) NPV > 0 (투자가치 있음), NPV < 0 (없음)

		- **내부수익률(IRR, Internal Rate of Return):** 현금 수익의 현재가치가 현금 지출의 현재가치와 같도록 할인율을 정의 예) IRR > 0 (투자가치 있음), IRR < 0 (없음)
다중분석 (Multi-Criteria Analysis)	- 다양한 평가항목을 통해 최적안을 선정하는 기법	- **재무적관점:** RIO, NPM, PP, IRR 등 측정 결과 이용
		- **비즈니스 연계관점:** 비즈니스 필요성과 전략 연계성
		- **기술적 관점:** 시스템 성능과 운영 및 관리 측면 측정
		- **리스크 관점:** 리스크 발생가능성과 효과 측정

- 정성적 방식인 IO(Information Orientation, 정보화평가), IE(Information Economics, 정보경제학)함께 활용

"끝"

06	CSP (Cloud Service Provider)		
문제	조직이 클라우드 컴퓨팅 서비스를 이용하고자 할 경우, 클라우드 서비스 제공자(CSP, Cloud Service Provider)에 대한 리스크를 관리하여야 한다. 다음을 설명하시오. 가. 클라우드 아웃소싱에 대한 요구사항 나. 리스크 관리 시 고려사항 다. 리스크 대응방안		
도메인	디지털서비스	난이도	상(상/중/하)
키워드	데이터 보호, SRM		
출제배경	Cloud 서비스가 늘어남에 따라 요구되는 Cloud 서비스의 안전성과 보안에 대한 관심이 높아짐		
참고문헌	금융분야 클라우드 컴퓨팅 서비스 이용 가이드, 디지털서비스 심사·선정등에 관한 고시		
해설자	장건환 기술사(제 126회 정보관리기술사 / jkh556@naver.com)		

I. CSP(Cloud Service Provider)의 개념

- 권한이 있는 사용자가 클라우드를 통해 서비스를 이용할 수 있고, 사용량에 따라 컴퓨터 자원을 유동적으로 제공하는 클라우드 서비스 제공자

II. 클라우드 아웃소싱에 대한 요구사항

구분	요구사항	설명
계약	레지스터 등록	- 계약 관련 세부 정보 포함하여 아웃소싱 레지스터 등록
	적합성 평가	- CSP에 대한 평판 분석 등 적합성 평가 실시
	서면 계약	- 데이터 처리 및 저장 위치 등을 포함한 서면 계약 요건
	계약종료 가능 평가	- 클라우드 아웃소싱 계약의 종료 가능 여부 평가
	서브 아웃소싱 계약	- 서브 아웃소싱 허용여부를 고려한 아웃소싱 계약 체결
	계획 보고	- 관할 당국에 클라우드 아웃소싱 계획 보고
Biz 관리	Biz 관리 및 모니터링	- API 보안, 비즈니스 연속성 관리, 규정 준수 모니터링 수행
위험관리	아웃소싱 계약 위험평가	- 클라우드 아웃소싱 계약의 결과로 발생할 수 있는 위험 평가
	위험 발생 가능성 고려	- 동일한 CSP 사용으로 인한 집중 위험 발생 가능성 고려

- 집중위험이 확인될 경우 관할당국은 해당 위험을 모니터링하고 잠재적 영향을 평가

III. 클라우드 리스크 관리시 고려사항

구분	고려사항	설명
계획 및 평가	계획 및 모의훈련	- 클라우드 환경의 특수성을 고려한 업무지속성 확보방안 및 재해복구 계획을 수립하고 해당 계획의 실효성 제고한 다양한 모의훈련 실시
	주기적 위험평가 실시	- 클라우드를 통해 처리되는 정보 및 업무의 중요성 등을 감안하여 클라우드 이용부서 및 내부통제부서 등의 주기적인 위험평가 실시
	피해보상 대책의 적정성 검토	- CSP와의 이용계약 체결시 클라우드 전산센터의 전산사고 발생에 따른 피해보상대책의 적정성을 검토
Biz 관리	업무 집중 리스크 및 확장성 검토	- CSP에 대한 업무 집중 리스크를 정기적으로 분석하고 다중 공급업체 전략 적용(멀티 클라우드 등) 필요성 등을 검토
	업무연속성 확보 방안 마련	- 전산사고 등으로부터 데이터를 안전하게 보존하고, 업무연속성 확보를 위해 주 전산센터 및 재해복구센터 역할을 하는 클라우드 전산센터를 일정거리 이상 원격지에 분산 구축

- Cloud 서비스를 이용하는 기업에서는 재해 및 재난 등을 대비해 안정적인 시스템 운영을 위해 특정 CSP에 대한 집중 리스크를 고려할 필요 있음

IV. 클라우드 리스크 대응방안

구분	대응방안	설명
CSP의존성 리스크	제3자 관리시 집중 리스크 평가	- 제3자 계약의 중요성을 평가하여 중요 아웃소싱을 식별하고 의존 위험과 집중 위험 등을 주기적으로 평가
	아웃소싱 원칙 내 집중위험 대비	- SW취약점으로 인한 영향 전파나 재해복구시스템에 대한 복수기업 사용으로 자원 고갈 등을 대비하기 위한 기업 자체적인 방안을 마련
	클라우드 서비스의 제3자 의존성 분석	- 의존위험을 해소하기 위해 기업의 혁신과 복원력 사이의 균형을 따져 다중 공급업체 전략을 적용하는 등 조치를 검토
	운영위험 관리 및 제3자 위험방지 요건	- 비례성 원칙에 따라 중요 아웃소싱인 경우 보안조치 등을 강화하고 규모 및 복잡성이 적은 기업은 완화된 조치를 적용
보안	기존 보안 위협대응	- 암호화, 해싱, 디지털 서명, 중복 모니터링 등 강화 - 주기적 백업 및 백신관리, MFA 인증 관리
	가상화 따른 위험대응	- 자원사용량 제한, 로그이력 관리 등 VM간 독립성 보장 - Hypervisor & Agent 기반의 VM 모니터링, 보안 프로그램 설계
	관리측면 대응방안	- 이해관계자들에 대한 교육 및 전문인력 채용 - 국제 클라우드 보안 표준을 준수하는 인증 획득 및 보험 가입
	법/제도적 대응방안	- 법적인 쟁점을 사전 점검하여 시스템 설계 및 도입 - 국제 표준을 준수

"끝"

[참고] 클라우드 리스크 관리 6가지 가이드라인

가이드라인	설명
실패에 대한 계획	- 클라우드에 문제 생길시를 감안한 시나리오 세부적 개발
내부 전문가 확보	- 문제 발생시 대응 가능한 전무가의 노하우가 필요함
계획을 점검	- 클라우드 이슈가 발생 가능한 과정을 단계화하여 점검
내부적인 백업 방안 수립	- 데이터센터 문제 발생시 대비를 위해 사전 백업 중요
소싱 전략 재평가	- 멀티소싱 환경을 책임지도록 해 문제 발생시 해결을 일원화
싼게 비지떡	- 특정 데이터센터가 붕괴되더라도 지역을 바꿀 수 있는 역량을 확보할 수 있도록 전 지역에 걸쳐 백업, 복제 상태를 유지

ITPE 기술사회
제129회 정보처리기술사 기출문제 해설집

대 상 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사, 정보시스템감리사 시험
발행일 2023년 02월 04일
집 필 강정배PE, 소민호PE, 전일PE, 정상PE, 석PE, 이상용PE, 장건환PE
출 판 **ITPE(Information Technology Professional Engineer)**
주 소 ITPE 대치점 서울시 강남구 선릉로 86길 17 선릉엠티빌딩 7층
ITPE 선릉점 서울시 강남구 선릉로 86길 15, 3층 IT교육센터 아이티피이
ITPE 강남점 서울시 강남구 테헤란로 52길 21 파라다이스벤처타워 3층 303호
ITPE 영등포점 서울시 영등포구 당산동2가 하나비즈타워 7층 ITPE
연락처 070-4077-1267 / itpe@itpe.co.kr