제124회 정보관리기술사 해설집

2021.05.28

국가기술자격 기술사 시험문제

기술사 제 124 회 제 2 교시 (시험시간: 100 분)

분야	정보통신	자격종목	정보관리기술사	수검번호		성명	

※ 다음 문제 중 4 문제를 선택하여 설명하시오. (각 10 점)

1. 코로나-19(Covid-19)로 인한 언택트 시대의 데이터 주권 이슈와 데이터 거버넌스 전략 방향에 대하여 설명하시오.

2. 디자인 싱킹(Design Thinking)에서 요구분석을 위한 공감(Empathize) 방법의 중요성을 설명하시오.

3. 사용자 요구사항 도출 기법 4 가지 및 요구사항 도출 시 유의사항을 설명하시오.

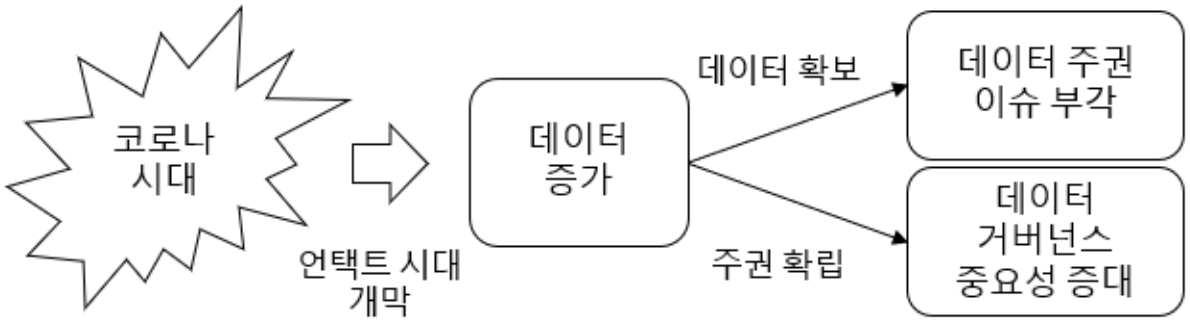
4. 소프트웨어 신뢰성 성장 모델(Software Reliability Growth Model, SRGM)을 2 가지 설명하시오.

5. DA(Data Architect)와 DBA(Database Administrator)의 역할을 비교하여 설명하시오.

6. OWASP 에서 발표한 보안 위협 인젝션(Injection)의 개념과 대응 방안을 설명하시오.

01	데이터 거버넌스		
문제	코로나-19(Covid-19)로 인한 언택트 시대의 데이터 주권 이슈와 데이터 거버넌스 전략 방향에 대하여 설명하시오.		
도메인	데이터베이스	난이도	중 (상/중/하)
키워드	데이터 거버넌스, 데이터 주권, 통계, 빅데이터, 법·제도 개선		
출제배경	코로나19로 인한 데이터 증가로 데이터의 확보가 중요해지고 있고 데이터 거버넌스 전략 부각		
참고문헌	포스트 코로나19 시대의 데이터 주권과 데이터 거버넌스, (정보통신정책연구원, 2020.12.14)		
해설자	NS반 백기현 기술사(제 122회 정보관리기술사 / onlyride@naver.com)		

I. 코로나-19 시대 데이터 주권 확립을 위한 데이터 거버넌스 전략의 필요성

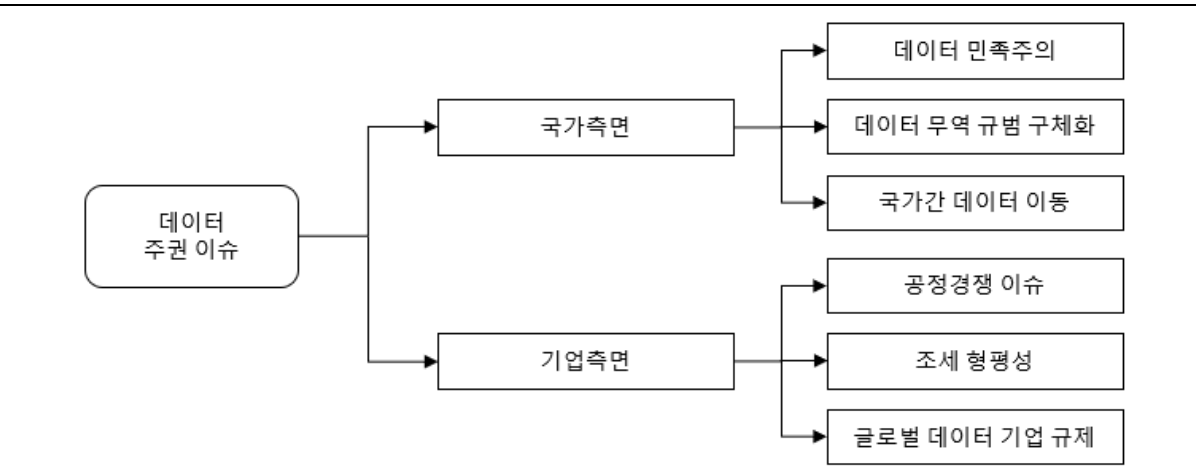


필요성	- 코로나19의 영향이 장기화되면서 언택트 문화가 일상화되고 있고 데이터 자원의 폭발적 증가를 의미하며 데이터 확보를 위한 데이터 주권 확보 차원으로 진화되고 있고 확립 차원에서 데이터 거버넌스 전략이 필요

- 데이터 주권이란 데이터가 수집된 국가 내의 법률 및 거버넌스 구조에 종속되는 것으로 언택트 시대에 이슈로 부각되는 중

II. 코로나-19로 인한 언택트 시대의 데이터 주권 이슈

가. 언택트 시대의 데이터 주권 이슈 분류



- 언택트 문화가 장기화되면서 디지털 경제로 전환이 가속화되고 있으며, 데이터 자원의 폭발적 증가됨
- 새로운 자원인 데이터 확보를 위한 경쟁은 기업 차원을 넘어 국가 간의 경쟁, 데이터 주권 확보 차원 전개

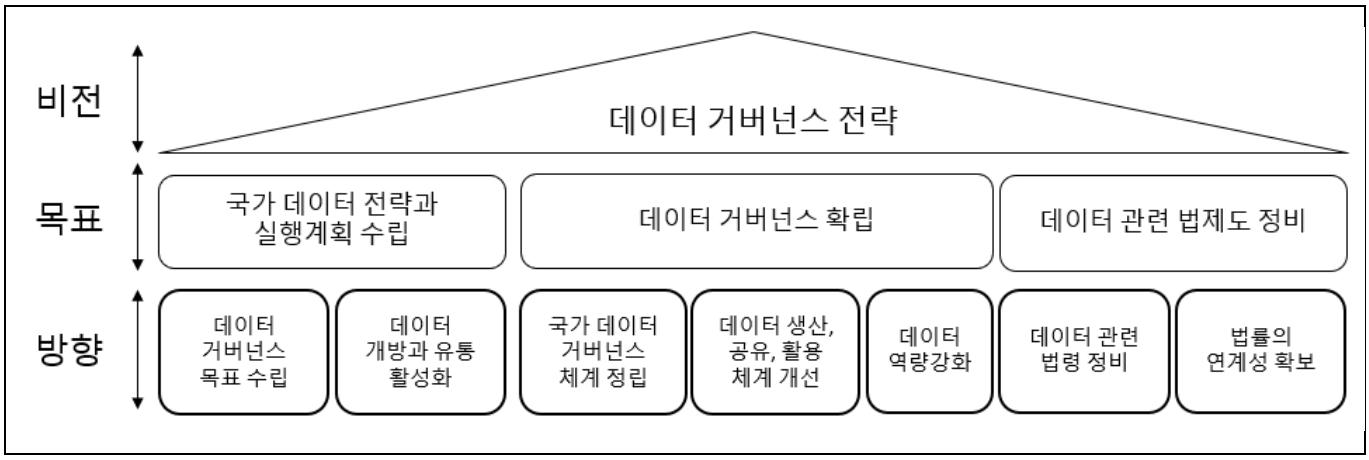
나. 언택트 시대의 데이터 주권 이슈 설명

구분	이슈	설명
국가측면	데이터 민족주의 (Data Nationalism)	- 국경간 데이터 이동과 글로벌 데이터 기업의 조세 형평성 등 데이터를 매개로 한 국가간 무역 분쟁으로 '데이터 민족주의'를 촉발
	무역 협상에서 데이터 관련 무역 규범의 구체화	- TPP는 국경 간 데이터 이동 보장, 컴퓨터 설비의 지역화 요구 금지, 소스코드 공개 요구 금지를 규정하고 있으며 USMCA의 경우 국경 간 데이터 이동 보장, 컴퓨터 설비의 지역화 요구 금지, 소스코드 공개 요구 금지, 공공데이터 접근 촉진을 명문화
	국가간 데이터이동	- 미국의 '클린 네트워크' 정책과 중국의 '데이터 안보에 관한 글로벌 이니셔티브' 정책의 대립으로 국가간 데이터 접근에 관한 이슈 발생
기업측면	고객 데이터 독점에 따른 공정경쟁 이슈	- 거대 글로벌 데이터 기업의 고객 데이터 독점에 따른 시정조치 명령 - 빅데이터, AI 시대에 데이터 경쟁우위 이슈가 중요해짐으로써 개인 데이터 이동성 강화와 기업 데이터 개방 등 새로운 규제 마련이 필요 - 인터넷 경제 활성화 과정에서 일정한 역할을 담당한 망중립성 원칙과 유사하게 데이터 경제 촉진을 위한 데이터 중립성 개념 정립 필요
	조세 형평성 (Digital Tax)	- 기존 법인세 체계에 디지털 비즈니스 모델이 적용될 수 있도록 '주요 디지털 사업장(significant digital presence)' 개념을 추가 - EU 회원국 중 영국, 프랑스 등 6개국이 매출의 2%에서 7.5%에 해당하는 디지털서비스세(DST: Digital Service Tax)를 부과
	글로벌 데이터 기업에 대한 규제	- 글로벌 데이터 기업에 대한 시정조치 명령과 과징금 부과는 새롭게 형성되는 데이터 경제 체제에서 공정경쟁 규제 이슈가 현안으로 부상하고 있음을 의미

- 포스트 코로나 시대의 최우선 국가전략은 국가 데이터 거버넌스 확보에서 출발해야 함

III. 코로나19 이후의 데이터 주권 확보를 위한 데이터 거버넌스 전략 방향

가. 데이터 거버넌스 전략 방향

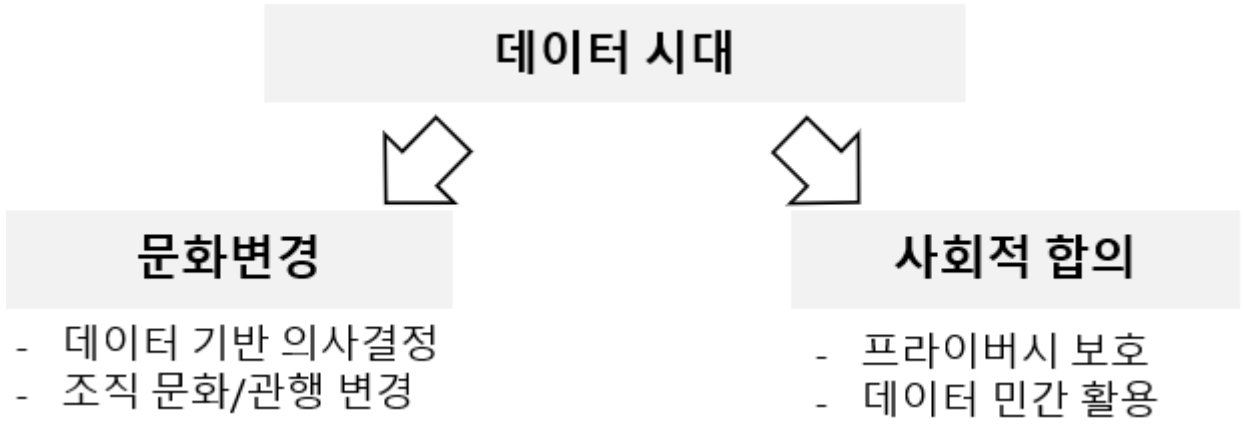


- 국가적인 데이터 거버넌스의 전략 목표 수립 후 증거기반 정책 확립이 필요

나. 데이터 거버넌스 전략 방향 상세

구분	거버넌스 전략	설명
국가 데이터 전략과 실행 계획 수립	데이터 거버넌스 목표 수립	- 국가 데이터 전략의 목표는 공공 서비스를 위한 국가 데이터의 충분한 활용과 함께 세계를 선도하는 데이터 경제 구축 지향으로 설정
	데이터 개방과 유통 활성화	- 데이터 개방, 유통 활성화에 역점을 두고 공공부문의 데이터 공유와 활용 관련 세부 목표와 구체적인 실천 계획 수립
데이터 거버넌스 확립	국가 데이터 거버넌스 체계 정립	- 국가 데이터 전략, 시행계획 수립 - 통계 거버넌스를 포괄한 데이터 거버넌스 설계 - 통계 및 데이터 관련 법령 재정비 - 통계 및 데이터 관련 전담 조직, 인력 재정비 - 지방분권 지원을 위한 데이터 거버넌스 확립
	데이터 생산, 공유, 활용 체계 개선	- 행정데이터와 통계 생산의 유기적 연계 - 공정정책 지원을 위한 공데이터 공유, 활용 강화 - 공공데이터 민간개방 확대, 민간데이터의 공유, 활용 활성화
	데이터 역량강화	- 데이터 공유 활용을 위한 공감대 형성 - 개인정보호와 데이터 활용의 조화 - 공공의 데이터 분석 역량 강화 - 정책지원을 위한 데이터 공유 활성화
데이터 관련 법제도 정비	데이터 관련 법령 정비	- 데이터담당관과 통계담당관 등 관련 담당자와 증거 구축을 위한 데이터자문위원회, 최고 데이터 책임관위원회 등 유관 위원회의 역할과 협력 관계를 명시한 미국의 증거기반정책법을 벤치마킹하여 데이터와 통계의 유기적인 연계 필요
	법률의 연계성 확보	- 통계법과 데이터기반 행정활성화에 관한 법률 등 연계성 확보를 ₩ 위한 개정 작업과 함께 상위 차원의 데이터법 제정

IV. 데이터 시대 국가 경쟁력을 갖추기 위한 시사점



- 데이터가 중심이 되는 미래 사회를 대비하기 위해서는 산업사회에서 통용되던 낡은 틀을 깨는 패러다임의 변화가 필요

"끝"

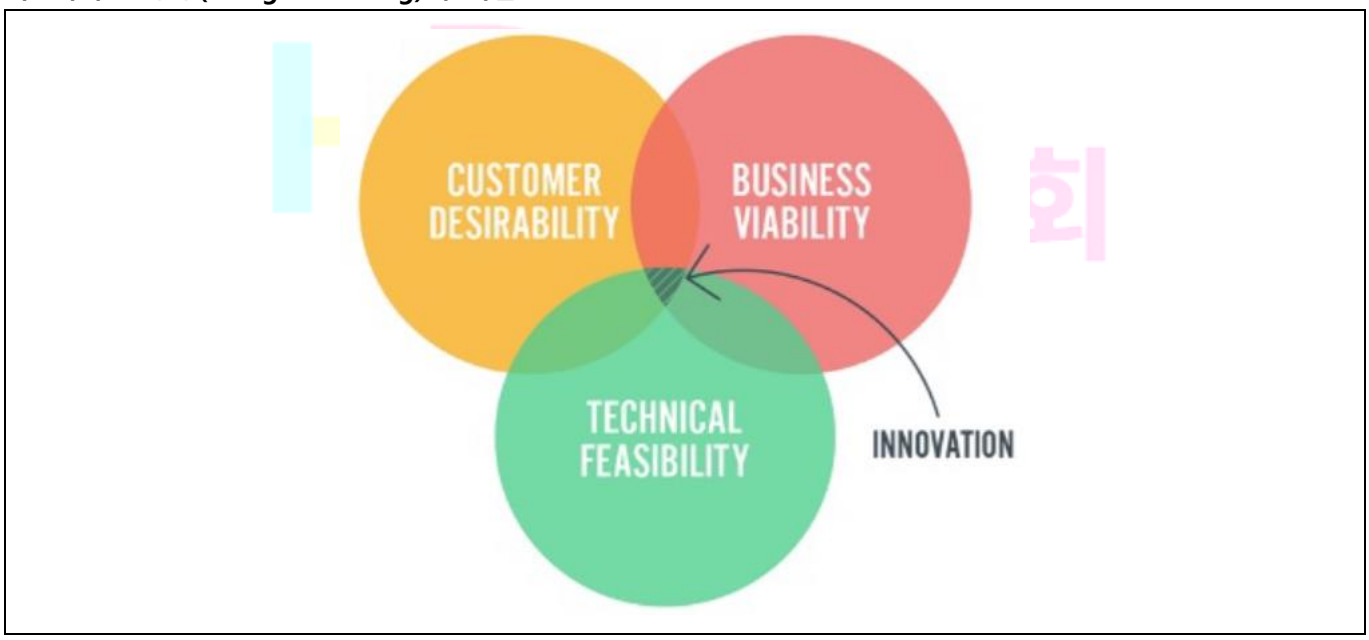
02	디자인 씽킹(Design Thinking)		
문제	디자인 씽킹(Design Thinking)에서 요구분석을 위한 공감(Empathize) 방법의 중요성을 설명하시오.		
도메인	디지털서비스	난이도	중(상/중/하)
키워드	속도보다 방향, 사용자 중심, 고객의 니즈 사전 파악		
출제배경	암기보다 토픽의 이해력 확인		
참고문헌	https://www.ceopartners.co.kr/news/articleView.html?idxno=1336		
해설자	강남평일야간반 전일 기술사(제 104회 정보관리기술사 / nikki6@hanmail.net)		

I. 공감적 관찰 통한 창의적 문제해결, 디자인 씽킹(Design Thinking) 개요

- '사람과 사물'에 대한 공감적 관찰(Empathic Observation) 통해 문제 재해석(Reframing Issues)하고, 시각적 아이디어 도출, 프로토타입 제작 통해 문제 솔루션 도출하는 통합적, 사용자 중심 문제 해결 방법론.
- (특징) 인간 중심 디자인 방법론, 공감 통한 문제 맥락 접근, 감수성과 비즈니스 전략적 사고의 통합

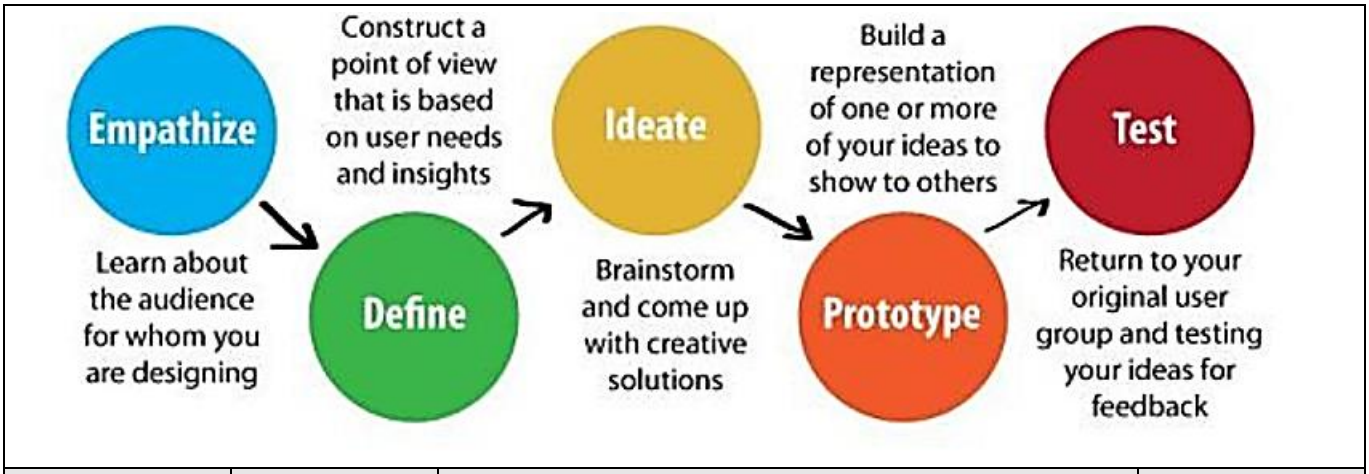
II. 디자인 씽킹(Design Thinking)의 핵심요소 및 프로세스

가. 디자인 씽킹(Design Thinking)의 핵심요소



- 사람들이 진정 원하는 것(Desirability), 기술적 & 조직적으로 가능한 것(Feasibility), 사업 가치가 있는 것(Viability)을 기본 3 대 핵심요소로 활용해 혁신 위한 전략(Strategy) 도출이 중요.

나. 디자인 씽킹(Design Thinking)의 적용 프로세스



구분	프로세스	설명	기법
Inspiration (영감)	공감 (Empathize)	- 사용자 식별 - 사용자 관찰, 인터뷰 통한 공감 - 사용자 Needs 파악	설문조사, 인터뷰, 관찰, Shadowing
	문제 정의 (Define)	- 공감한 결과 바탕 문제점 파악 및 문제 우선순위화 - 문제 인식 및 공유	요구사항 정의, 페르소나,
Ideation (아이디어 도출)	아이디어 도출 (Ideate)	- 파악된 문제점 해결 위한 다양한 아이디어 발산 - 아이디어 우선순위화, 개선 방향 도출 - Divergence(확장적 사고), Convergence(집중적 사고)	브레인스토밍, 아이디어 스케치, 시각화
Implementation (실행)	프로토타이핑 (Prototype)	- 도출된 아이디어의 시각화, 실체화 - 아이디어 구현하기	스토리보드, 3D 프린팅
	테스트 (Test)	- 제작된 프로토타입 테스트 - 피드백 통한 아이디어 개선 및 회고	사용성 테스트, Role play

- 디자인 씽킹 프로세스는 공감, 문제 정의, 아이디어 도출, 프로토타입, 테스트 5단계로 이루어지며, 필요에 따라서 거꾸로 가기도 하며 전체 과정이 반복되기도 함

III. 요구분석을 위한 공감(Empathize) 방법의 중요성

가. 디자인씽킹의 핵심, 공감(Empathize) 상세설명

구분	내용
정의	- 실제로 내가 만든 물건이나 서비스를 사용하는 사람(사용자)의 속마음을 알아보는 단계
프로세스	1) 감정이입 2) 민족지학적 탐색 3) 맥락적 종합

나. 다양한 관점에서 공감(Empathize) 방법의 중요성

구분	주요 내용	상세 설명
개념적 뷰	속도보다는 방향	- 잘못된 완성품을 만들어 수정하기 보다 처음부터 올바른 제

		품의 구현
	사용자 중심	- 유지보수성 및 기능성 보다 사용자 친숙성 강화
	문제의 사전 발견	- Snowball Effect 의 사전 차단
	현상 파악	- 전체적인 관점에서 다수의 뷰를 종합적으로 구현
구체화 뷰	사용자 식별	- 주요 고객의 대상 파악
	기능적 요구사항 파악	- 사용 시 필요한 기능 구현의 사전 진단

- 공감을 통해 소비자의 문제를 정의하고 아이디어를 도출한 뒤 프로토타입을 만들고 테스트를 통해 소비자가 불편해하는 점을 개선하기에 디자인씽킹 프로세스 중 가장 중요

IV. 디자인 씽킹(Design Thinking) 적용 시 유의사항

고려사항	설명
"Yes, BUT..." 보다는 "Yes, AND..."을 사용	- 전자는 상대방의 의견에 대해 부정적·비판적으로 반응하는 것이고, 반면에 후자는 긍정적·건설적으로 반응하는 것
아이디어는 질보다 양	- 아이디어 개수는 창의성과 연관
말이 많은 사람의 아이디어가 꼭 좋은 것은 아님	- 좋은 아이디어를 공정하게 고르기 위해서 스티커를 붙여서 투표하는 방법을 사용

- 디자인 씽킹(Design Thinking)의 성공적 적용 위해서 경계 허물기, 믹스하기, 연관, 대조, 조합, 파괴하기 등 경계 없는 창의적 발상이 중요.

"끝"

03	요구사항 관리		
문제	사용자 요구사항 도출 기법 4가지 및 요구사항 도출 시 유의사항을 설명하시오.		
도메인	소프트웨어공학	난이도	중(상/중/하)
키워드	인터뷰, 포커스 그룹, 집단창의적 기법, 집단의사결정 기법		
출제배경	소프트웨어공학 기본 토픽 이해 및 실무에서의 활용(유의사항)확인		
참고문헌	ITPE 기술사회		
해설자	강남평일야간반 전일 기술사(제 104회 정보관리기술사 / nikki6@hanmail.net)		

I. 요구사항 추적을 통한 범위 확인 기법, 요구사항관리의 필요성

필요성	내용
추적성 제공	- 요구사항과 개발 산출물간의 관계와 단계별 개발 산출물 간의 관계를 파악하는 능력으로, 요구사항이라는 추상적 개념에서 실질적으로 동작하는 시스템으로 구현되는 과정과 구현된 기능이 요구사항을 만족하는지를 파악하고 검증할 수 있도록 해주는 속성 제공
범위기준선 제공	- 요구사항을 수집하여, 범위를 정의하고. WBS 를 작성하게 됨 - 이를 통해, 고객, 이해관계자와 프로젝트 및 제품을 만드는 기준선 제공
일정과 원가에 영향	- 요구사항의 통합은 결국 Core 의 프로젝트 일정과 원가 및 예산 산정의 기준이 되며, 품질 속성을 만족시키는 Rework 및 낮은 품질 사전 제거 - 요구사항명세서, 범위기술서를 작성하는 입력물로서, 프로젝트 및 SW 의 가시화(Visualization) 제공

II. 요구사항 수집을 위한 도출 기법 4 가지 이상 도출 기법

가. 요구사항 수집 프로세스의 ITO

수집 입력물	도구 및 기법	산출물
범위관리계획서 요구사항 관리계획서 이해관계자 관리계획서 이해관계자 관리대장	전문가 판단 데이터 수집(Data Gathering) 데이터 분석(Data Analysis) 의사 결정(Decision Making) 데이터 표현 (Data Representation) 대인관계와 팀 스킬 (Interpersonal and team skills) 컨텍스트 다이어그램 (Context Diagrams) 프로토타입(Prototypes)	요구사항 문서 (Requirement Documentation) 요구사항 추적 매트릭스 (Requirement Traceability Matrix)

나. 도출기법 상세 설명

기법	항목	세부내용
전문가 판단	- 비즈니스에 대한 전문가 및 도메인에 대한 전문가가 판단	
	브레인스토밍	- 아이디어 생성 및 수집 기법

데이터 수집(Data Gathering)	인터뷰(Interview)	- 이해관계자와 직접 대화를 통해 정보를 구하는 공식적 또는 비 공식적 정보 수집 방법
	핵심전문가 그룹 (Focus Group)	- 제안된 제품, 서비스에 대한 기대 사항과 의견을 교환하기 위해 선별된 전문가 집단으로 대화식 토론으로 요구사항을 수집하는 방법
	설문조사(Questionnaires and Surveys)	- 다수의 대상자에게 신속하게 정보를 수집할 수 있도록 구성된 질 문지로 조사 대상자가 많거나 광범위 할 경우, 신속한 자료 수집 이 필요한 경우 효과적인 방법
	벤치마킹(Benchmarking)	- 경쟁사, 선진 업체의 사례 및 업무 절차를 참조하여 유사한 수준 의 효과를 낼 수 있는 기능 요구 사항 정의
데이터 분석(Data Analysis)	문서분석	- 고객의 RFP 나 현행 시스템 혹은 프로세스 문서를 참고하여 요구사항 도출에 활용
의사 결정(Decision Making)	투표(Voting)	- 만장일치(Unanimity) 등을 통하여, 평가 및 단체 의사결정기법
데이터 표현	친화도(Affinity diagram)	- 효과적인 검토 및 분석을 위하여 수많은 아이디어를 몇 개의 그룹으로 분류 하는 기법

- 이외 대인관계와 팀 스킬, 컨텍스트 다이어그램, 프로토타입 기법 등이 존재

III. 요구사항 도출 시 유의사항

가. 요구사항 도출 시 유의사항

구분	핵심 기술	설명
사전 준비	목표, 범위, 제약사항	- 시스템의 목표, 범위, 사용자, 제약사항 등을 가장 먼저 파악하고 결정하여 요구사항 도출, 실행
다양화	최신 자료 확보	- 고객, 마케팅, 개발자, 기타 이해관계자, 기존 시스템, RFD 등
의사소통	구체화	- 추상적 요구(Need)를 구체적 요구(Candidate Requirements)로 변환

나. 요구사항 도출 시 기법 별 상세 유의사항

기법	항목	유의사항
전문가 판단	- 맹목적인 전문가의 판단만으로 진행 하지 말고 적절한 분석 필요	
데이터 수집(Data Gathering)	브레인스토밍	- 소극적인 분위기일 경우 브레인라이팅 기법 변환 시도
	인터뷰(Interview)	- 다양한 관점과 다양한 이해관계자와의 인터뷰 시도
	핵심전문가 그룹 (Focus Group)	- 전문가의 이론적 지식이 조직 프로세스에 적합한지 사전 확인/분석 필요
	설문조사(Questionnaires and Surveys)	- 설문조사를 위한 문항이 적절하지 않거나 복잡할 경우 신뢰성 없는 데이터 추출 가능

	벤치마킹(Benchmarking)	- 업체의 선진 사례가 조직의 문화 및 프로세스와 적절한지 확인
데이터 분석(Data Analysis)	문서분석	- 문석의 최근 버전 확인 및 이해 불가 시 관련자와의 인터뷰 필요
의사 결정(Decision Making)	투표(Voting)	- 만장일치(Unanimity) 불가 시 다수결에 의한 결정 변환

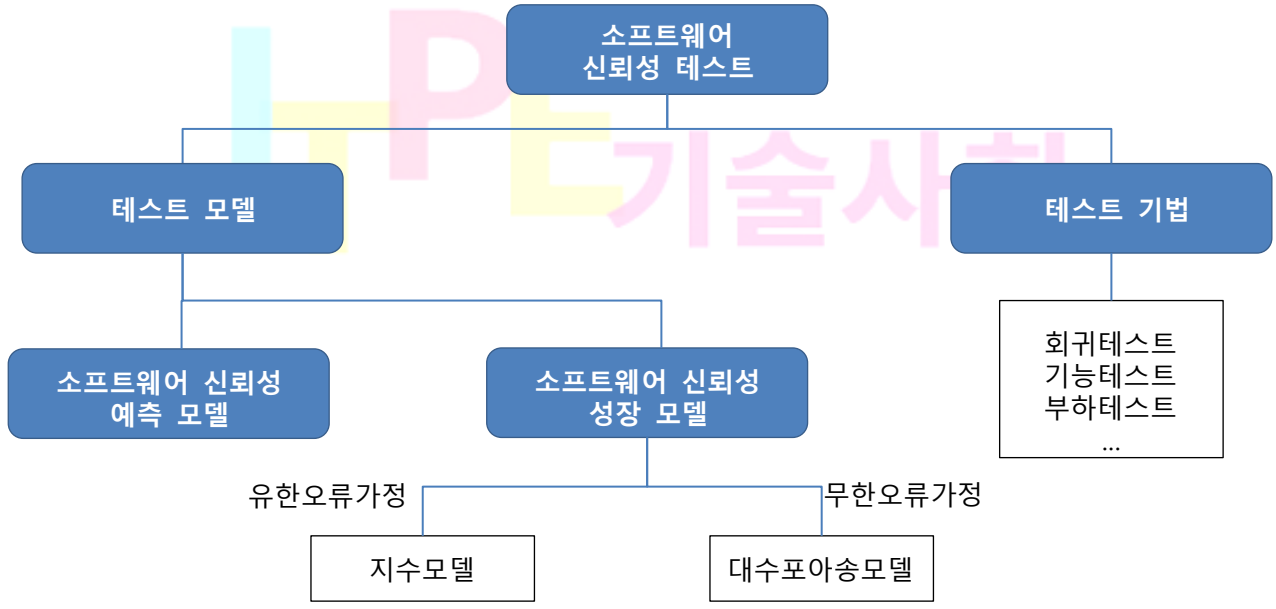
- 잘못된 요구사항 도출은 서비스 및 제품의 품질에 많은 변경을 필요로 하기에 초기 대처 중요

"끝"

04	SRGM(Software Reliability Growth Model)		
문제	소프트웨어 신뢰성 성장 모델(Software Reliability Growth Model, SRGM)을 2가지 설명하시오		
도메인	소프트웨어공학	난이도	상(상/중/하)
키워드	지수모델, 대수 포아송 모델, NHPP, S-shaped		
출제배경	소프트웨어 안전성 문제 중요도 증가와 관련된 신뢰성에 대한 이해 여부 확인		
참고문헌	소프트웨어 신뢰성에 대한 정량적인 평가(이창희) Software Reliability & Testing ('2002, University of Calgary) Software Reliability Modeling ('2012, Steven J Zeil) https://www.semanticscholar.org/paper/Software-Reliability-Growth-Models-Exposing-Field-Siok-Whittaker/416bf08c8179ea128723c89904c951985724a991 https://www.javatpoint.com/software-engineering-basic-execution-time-model		
해설자	단합반 안경환 기술사(제 110회 정보관리기술사 / akh.itpe@gmail.com)		

I. 소프트웨어 신뢰성 성장 모델(SRGM)의 개요

가. 소프트웨어 신뢰성 성장 모델(SRGM)의 정의



정의	- 소프트웨어의 시험 기간 중에 발생되어지는 고장데이터에 대해서 고장 시간이나 고장 수를 중심으로 소프트웨어의 신뢰성을 평가하기 위한 확률적 모델

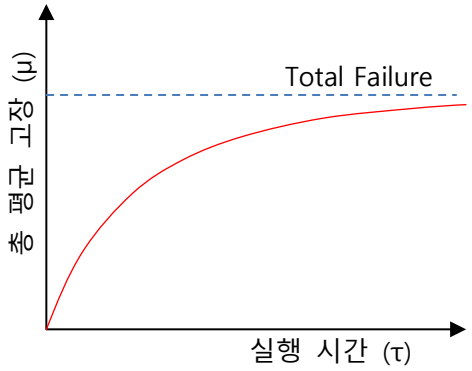
- 각 모델은 소프트웨어 전체 Life Cycle이 아닌 한번의 수정 기간 동안에만 적합

나. 소프트웨어 신뢰성 성장 모델(SRGM) 측정을 위한 매개변수

매개변수	설명
고장 강도 (λ)	- 단위시간당 고장이 발생한(실패) 횟수
실행 시간 (τ)	- 프로그램이 실행된 이후의 시간
경험한 평균 고장 (μ)	- 특정 시간 동안 발생한 평균 고장 수($\mu = \sum_{i=1}^{n} i \times p_i$, p: *발생 확률*, i: *실패 회수*)

II. 소프트웨어 신뢰성 성장 모델(SRGM)의 지수모델(Basic Exponential model)

가. 지수모델(Basic Exponential model)의 개념

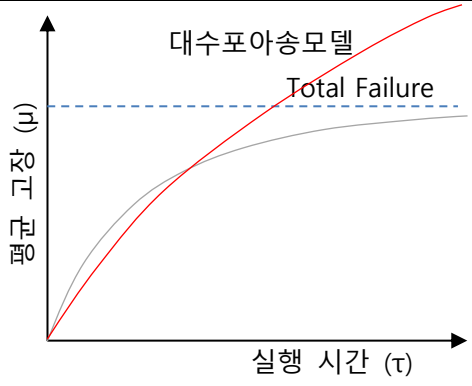
수식	실행 시간과 경험한 평균 고장의 관계
$\lambda(\tau) = \lambda_0 e^{\left(-\frac{\lambda_0}{\nu_0}\right)\tau}$ λ_0 : *실행 시작시 초기 실패 강도* ν_0 : *총 실패 횟수*	
정의	- 무한한 시간에 유한 오류를 가정하는 소프트웨어 신뢰성 성장 모델

나. 지수모델(Basic Exponential model)의 상세 유형

모델 유형	설명
Jelinski-Moranda 모델	- 가장 초기의 소프트웨어 안정성 모델 중 하나이며, 기존의 많은 소프트웨어 신뢰성 성장 모델에 참조 모델을 제공
Musa-Basic 모델	- 관찰된 고장 수에 따른 고장 강도의 감소는 일정하다는 가정과 실행 시간에 기반한 모델 - 모든 결함이 똑같이 발생할 가능성이 있고 서로 독립적이라고 가정
NHPP 모델	- 발생한 소프트웨어 고장수 혹은 발견된 소프트웨어 결함수에 기초한 확률통계 모델

III. 소프트웨어 신뢰성 성장 모델(SRGM)의 대수 포아송 모델(Logarithmic Poisson model)

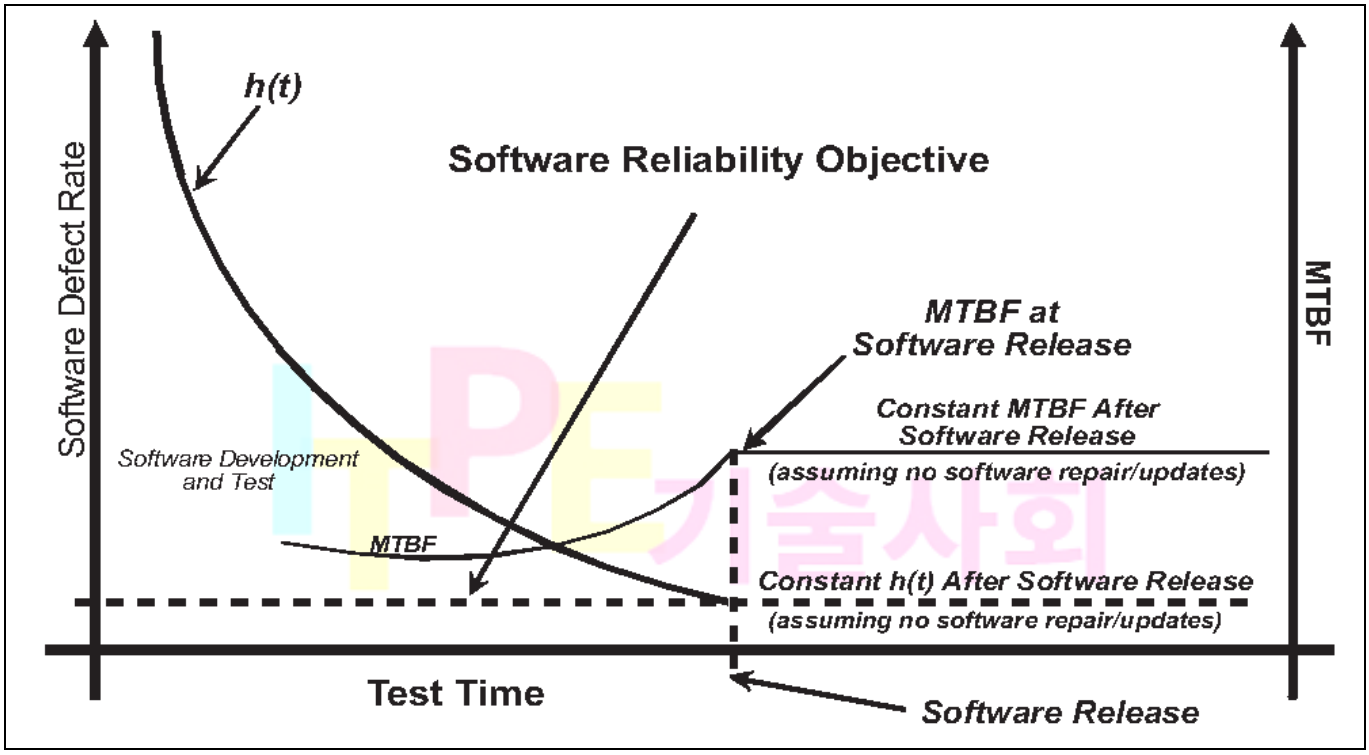
가. 대수 포아송 모델(Logarithmic Poisson model)의 개념

수식	실행 시간과 경험한 평균 고장의 관계
$\lambda(\tau) = \frac{\lambda_0}{\lambda_0\theta\tau + 1}$ λ_0: *초기 실패 강도,* θ : *감쇠 매개 변수*	
정의	- 무한 오류를 가정하는 소프트웨어 신뢰성 성장 모델

나. 대수 포아송 모델(Logarithmic Poisson model)의 상세 유형

모델 유형	설명
Gompertz 모델	- 소프트웨어 내에 잠재하는 총 결함수를 회귀 분석에 의해 추정하는 모델
Musa-Okumoto logarithmic Poisson 모델	- Musa-basic 모델과 마찬가지로 실행 시간으로 측정 된 오류 데이터를 기반으로 소프트웨어 신뢰성 측정
Yamada S-shaped 모델	- Yamada 에 의해 제안된 모델로써, 소프트웨어 고장발생시간에서부터 그 고장의 원인인 에러를 제거하는 시간까지의 시간지연을 고려한 모델

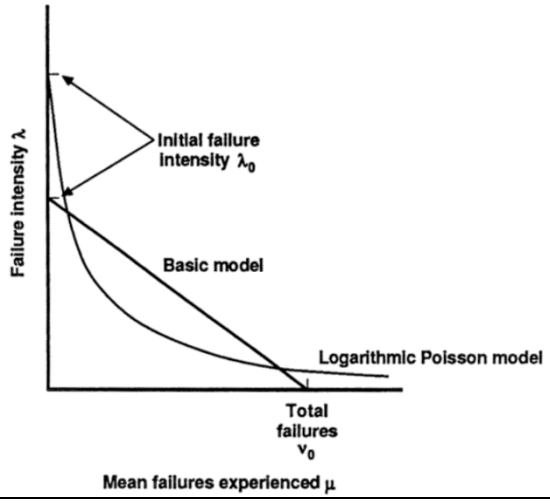
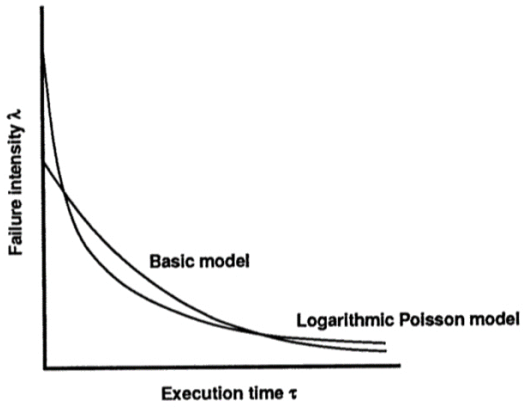
IV. SRGM의 활용방안

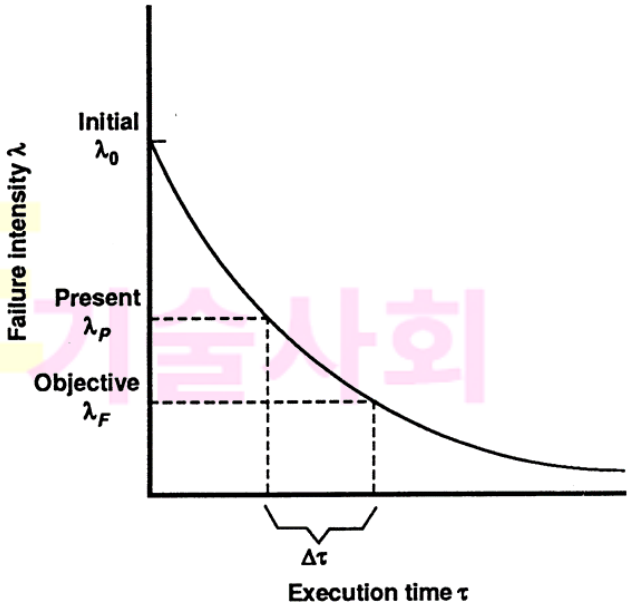


- 신뢰성 평가 척도를 중심으로 소프트웨어의 최적의 배포 시기 결정

"끝"

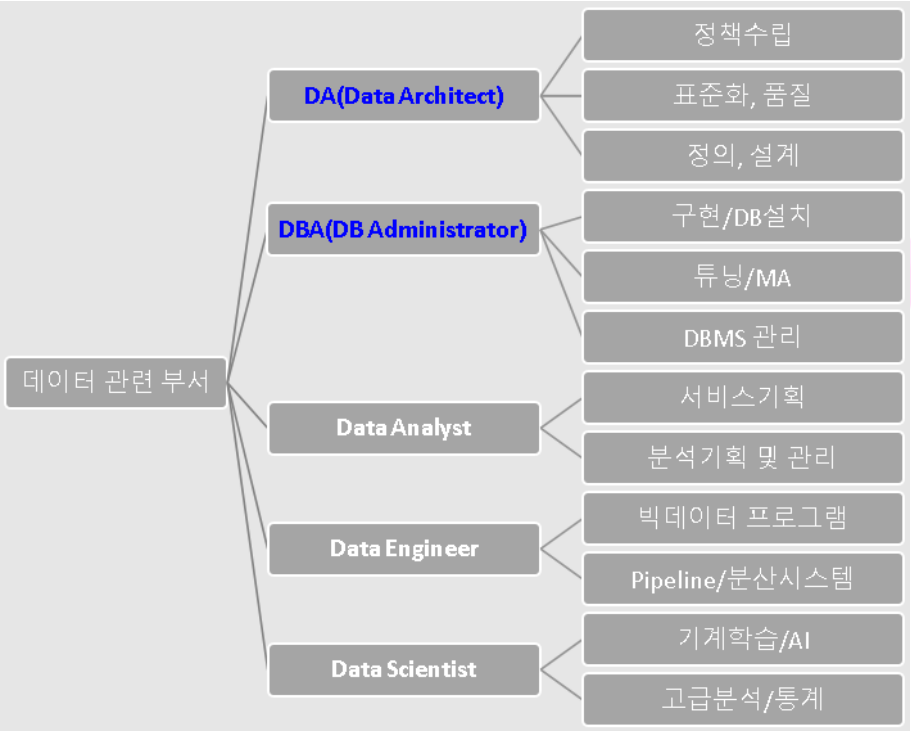
[참고 자료]

고장 강도와 경험한 평균 고장	고장 강도와 실행 시간의 관계
	

배포 기준	
- 목표 고장 강도에 도달하기 위해 시스템을 테스트하는 데 필요한 시간	

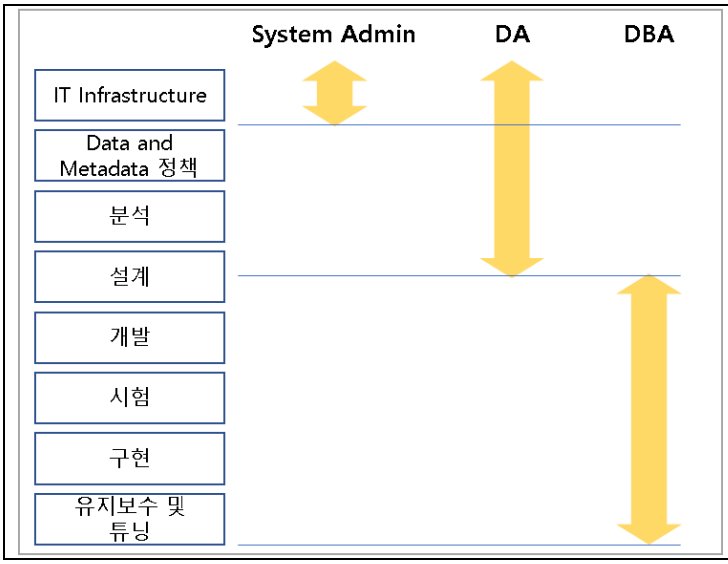
05	DA와 DBA		
문제	DA(Data Architect)와 DBA(Database Administrator)의 역할을 비교하여 설명하시오.		
도메인	데이터베이스	난이도	중(상/중/하)
키워드	표준화, 거버넌스, 도메인, 단어, 용어, 표준항목, 개념, 논리, 물리		
출제배경	데이터베이스 구축에 따른 기본 지식 확인		
참고문헌	데이터아키텍처 전문가 가이드(2020)교재 (한국데이터산업진흥원, 2020.05) 데이터 품질관리 지침(Ver.2.0) - 한국데이터산업진흥원 https://lovedb.tistory.com/116 https://www.mygreatlearning.com/blog/business-analytics-jobs/		
해설자	TOP반 유술사 (제 113회 컴퓨터시스템응용기술사 / itpe_you@naver.com)		

I. 효율적인 데이터 관리를 위한 조직 구성



- 기업 비즈니스를 성장시키기 위한 핵심으로 역량으로 효율적인 데이터 관리 및 분석이 중요함
- 대표적으로 DA(Data Architect)와 DBA(Database Administrator), Data Analyst, Data Engineer, Data Scientist로 조직을 구성

II. 시스템 구축단계별 DA와 DBA의 역할 개념비교



DA	- 데이터 기반으로 정책, 표준화, 아키텍처, 설계 업무를 수행하는 자 - 데이터 관점에서 구축하려고 하는 업무를 사용자/현업 담당자와 협의 및 분석하여 개체(entity)와 속성(attribute) 추출 및 정의하는 담당자
DBA	- 개발에 필요한 DB를 설치하고, DA로 받은 논리분석(ERD) 결과를 기반으로 물리적 테이블을 생성 및 SQL튜닝하는 담당자

III. DA(Data Architect)와 DBA(Database Administrator)의 역할 상세비교

구분	DA(Data Architect)	DBA(Database Administrator)
업무 범위	- 인프라 구축, 데이터/메타데이터 정책관리 - 데이터아키텍처 수립 및 모델링(분석/설계)	- 물리적 설계부터, 개발, 시험, DB구현 - 유지보수 및 튜닝 수행
관리 영역	- 데이터 관리(값/구조/프로세스) 정책 - 데이터 요구 사항을 반영한 데이터 모델 및 각종 표준 정의	- 데이터 모델을 특정 DBMS 제품 특성에 맞추어 구축한 데이터베이스
주 업무	- 데이터베이스 구축을 위한 분석 및 설계 - 업무에 필요한 데이터의 메타 데이터를 정의하고 신규 또는 변경된 요구 사항을 신속하게 데이터 모델에 반영	- 요구되는 성능 수준을 발휘하면서 안정적으로 운영되도록 데이터베이스를 관리
품질 수준 확보	- 정책 및 데이터 표준의 관리 및 적용을 통해 품질 수준을 확보	- 데이터의 정합성 관리를 통해 데이터 품질 수준을 확보
전문 기술	- 담당 업무 분야에 대한 업무 지식과 데이터 모델링에 대한 전문성이 필요	- 데이터 모델에 대한 해독 능력 및 특정 데이터베이스 제품에 대한 전문 지식이 필요

IV. 효율적인 데이터 관리를 위한 품질 프레임워크 및 관리 프로세스

조직 \ 대상	데이터 값	데이터 구조	데이터 관리 프로세스
CIO/EDA (개괄적 관점)	데이터 관리 정책		
DA (개념적 관점)	표준 데이터	개념 데이터 모델 데이터 참조 모델	데이터 표준 관리 요구사항 관리
Modeler (논리적 관점)	모델 데이터	논리 데이터 모델	데이터 모델 관리 데이터 흐름 관리
DBA (물리적 관점)	관리 데이터	물리 데이터 모델 데이터베이스	DB 관리 DB 보안 관리
User (운용적 관점)	업무 데이터	사용자 View	데이터 활용 관리

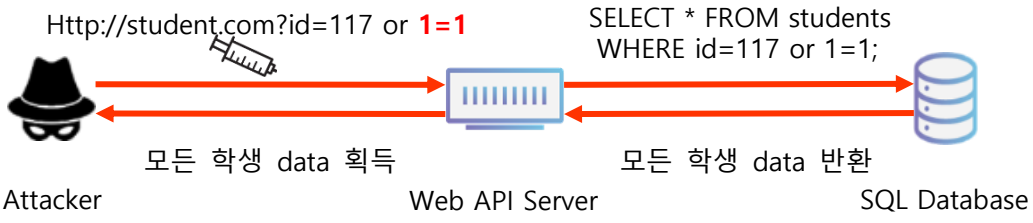
- 데이터 품질관리 요소는 크게 데이터 값(data value), 데이터 구조(data hierarchy), 데이터 관리 프로세스(data management process)로 구분
- 각 요소들은 상호 연계되어 정보시스템의 데이터 품질에 영향을 주고 있으므로 통합적이고 체계적인 관리 노력이 필요

번호	데이터 관리 프로세스	주요 절차	설명
1	데이터 품질기준 수립	- DQI, CTQ 선정	- 데이터 품질 기준정보 - DQI 등 업무영역 선정
2	프로파일링	- 대상선정 프로파일링	- 일반적 유형 현황 파악 - 컬럼, 관계, 패턴, 코드 등
3	BR(Business Rule) 선정	- BR 도출 및 확정	- 각종 업무 규칙 수집 - 측정 가능형태로 선정
4	데이터품질진단	- BR 측정 및 진단	- 확정 BR의 측정, 진단 - 결과에 따른 현상 분석
5	개선/정제	- 데이터 정제	- 저품질 BR 오류 분석 - 개선/정제 후 재측정

"끝"

06	인젝션(Injection)		
문제	OWASP에서 발표한 보안 위협 인젝션(Injection)의 개념과 대응 방안을 설명하시오.		
도메인	보안	난이도	하(상/중/하)
키워드	인터프리터, 입력값 유효성 검사, 화이트리스트(White List), 동적 쿼리 사용 제한, 백업		
출제배경	OWASP TOP 10 기출 문제 중 개별 취약점에 대한 이해와 대응 방안 확인 92회 정보관리기술사 4교시 SQL-Injection 취약점 문항 변형		
참고문헌	A1:2017-Injection(https://owasp.org/www-project-top-ten/2017/A1_2017-Injection) 자동화된 SQL Injection 공격을 통한 악성코드 대량 삽입 수법 분석(Mass SQL Injection) (한국정보보호진흥원, 2008.12) 웹 관리자를 위한 응급처치법-SQL Injection 해킹 보안(박상옥, 한국데이터산업진흥원) https://lifars.com/2020/04/injection-attacks-explained/ https://ko.wikipedia.org/wiki/SQL_삽입 https://ko.wikipedia.org/wiki/DLL_인젝션 https://m.mkexdev.net/427		
해설자	안경환 기술사(제 110회 정보관리기술사 / akh.itpe@gmail.com)		

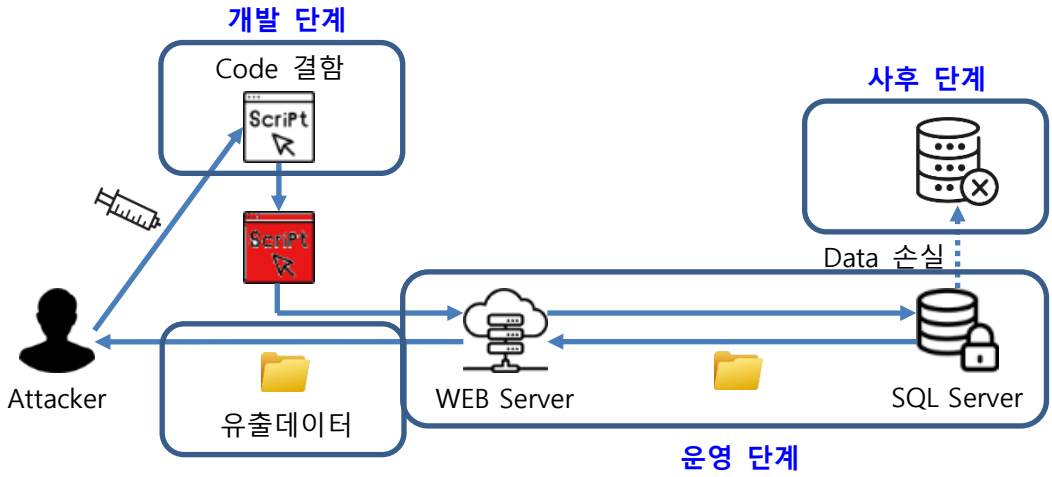
I. 악성코드 보안 위협. 인젝션(Injection)의 개념

개념	- 응용 프로그램 보안 상의 허점을 의도적으로 이용해, 악의적인 데이터(예: SQL문 등에 사용되는 데이터)를 인터프리터(Interpreter)에게 전송하여 정상적인 프로그램(예: Database)을 비정상적으로 조작하는 공격 기법	
공격 개념도		
유형	SQL Injection	- SQL Query문의 논리적 오류를 이용하여 공격
	Blind SQL Injection	- Query 결과에 따른 서버의 참과 거짓 결과를 이용하여 공격
	LDAP Injection	- 웹 어플리케이션의 악의적 LDAP 문법을 이용해 서버가 의도치 않는 동작을 실행
	DLL Injection	- 다른 프로세스의 주소 공간 내에서 DLL을 강제로 로드시킴으로써 코드를 실행

- 인젝션(Injection) 공격은 인터프리터(Interpreter)에게 악의적 데이터를 이용한 공격기법으로 이를 대응하기 위해 공격 경로와 피해 영역에 대한 분석 필요

II. 인젝션(Injection)의 대응 방안 – 대응 영역 분석과 대응 방안

가. 인젝션(Injection)의 공격 경로와 피해 영역



- 인젝션(Injection) 공격은 개발 단계에서 발생한 취약점을 이용하여 공격하며 운영 중인 Web Server 등의 경로를 통해 데이터 유출 혹은 손실 등의 피해를 발생하므로 각 공격 경로와 피해 영역에 대해 대응 방안 수립 필요

나. 인젝션(Injection)의 공격의 대응 방안

단계	대응 방안	설명
개발 단계	- 시큐어 코딩 - 보안 인프라 구축	- 개발 단계에서부터 인젝션(Injection) 공격의 경로가 될 수 있는 스크립트(Script) 언어(Language)에 대해 보안 개발 적용과 유출된 데이터에 대해 악용 소지 사전 제거
운영 단계	- 공격 탐지	- 인젝션(Injection) 공격의 특성상 수회 반복된 특정 페이지 호출이나 반복된 에러가 발생하는 등의 로그(Log)가 생성되므로 이에 대한 모니터링 수행
사후 단계	- 피해 복구 조치	- 손실이나 변경 등이 발생한 데이터를 이전 상태로 복구 조치 수행

III. 인젝션(Injection)의 세부 대응 방안

가. 시큐어 코딩과 보안 인프라 구축

대응 방안	세부 대응 방안	설명
입력값 유효성 검사	블랙 리스트 방식	- SQL 쿼리의 구조를 변경시키는 문자나 키워드를 제한하는 방식
	화이트 리스트 방식	- 블랙리스트 방식에서는 금지된 문자 외에는 모두 허용하지만 화이트리스트 방식에서는 허용된 문자를 제외하고는 모두 금지하는 방식
동적 쿼리 사용 제한	정적 쿼리 사용	- 웹 애플리케이션이 DB와 연동할 때 정적 쿼리 사용
	매개변수화된 쿼리(구조화	- 동적 쿼리를 정적 쿼리처럼 사용

	된 쿼리) 사용	- 쿼리 구문에서 외부 입력 값이 SQL 구문의 구조를 변경하지 못하도록 처리
오류 메시지 출력 제한	Database 오류 출력 제한	- Database 오류 정보에 표시되는 내부 정보가 외부에 그대로 노출되지 않도록 처리 - 사용자 오류 메시지(Custom Error Message)로 대체
	추상화된 메시지	- 자세한 안내 메시지를 제거하여 공격자에게 공격 범위 축소하지 못하도록 제한
보안 인프라 구축	방화벽(Firewall) 도입	- 웹 공격에 특화되어 있는 방화벽 도입 및 운영

나. 공격 탐지

대응 방안	세부 대응 방안	설명
SQL Injection 침입 확인	Database 확인	- 임시 테이블 혹은 이용자 계정 확인
	Web Log 점검	- 특정 웹 페이지의 반복된 접속 시도나 HTTP 500 error 지속 발생 확인 - SQL의 Query 구문의 존재 확인
SQL Injection 취약점 검검 툴	수동 점검	- GET 방식 SQL 주입 공격 탐색 - POST 방식 SQL 주입 공격 탐색
	자동 점검	- 자동으로 SQL Injection 주입 시도하는 공격 툴을 이용 - Paros Proxy를 이용한 자동 검색 - nikto web CGI스캐너 - SQL Injector

다. 피해 복구 조치

대응 방안	고려 사항	설명
백업본 이용한 복구	- 백업 시점 이후 자료 유실 발생	- 침해 사고 발생 이전 백업본이 있을 경우 백업본 이용 복구
컬럼 단위 복구	- 직접 적용하기 전에 문제가 없는지 사전 환경 구축 후 테스트 진행	- 발견한 악성 코드 문자열을 SQL Update 명령어를 적용하여 삽입된 악성 코드 제거
일괄 스크립트 사용 복구	- 직접 적용하기 전에 문제가 없는지 사전 환경 구축 후 테스트 진행	- 컬럼 단위 복구 스크립트는 복구 대상 컬럼이 많을 경우 많은 시간이 필요 - 일괄 스크립트 적용하여 빠르게 일괄 복구 수행 -

"끝"

ITPE 기술사회
제124회 정보처리기술사 기출문제 해설집

대 상 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사, 정보시스템감리사 시험
발행일 2021년 05월 28일
집 필 강정배PE, 안경환PE, 유술사PE, 전일PE, 백기현PE
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
연락처 070-4077-1267 / itpe@itpe.co.kr