제132회 정보관리기술사 해설집

2024.01.27

국가기술자격 기술사 시험문제

기술사 제 132 회 제 1 교시 (시험시간: 100 분)

분야	정보통신	자격종목	정보관리기술사	수검번호		성명	

※ 다음 문제 중 10 문제를 선택하여 설명하시오. (각 10 점)

1. ISO 31000

2. 데이터 거래소

3. 베이지안 최적화(Bayesian Optimization)

4. 대칭 암호화와 비대칭 암호화

5. ISA/IEC 62443

6. 큐싱(Qshing)

7. ELK(Elasticsearch/Logstash/Kibana) 스택

8. TPM(Trusted Platform Module)

9. 좋은 소프트웨어가 갖추어야 할 4 가지 특징

10. 모집단의 특성을 추론하는 점추정과 구간추정 비교

11. 다중공선성(Multicollinearity)

12. 블록 스토리지, 파일 스토리지, 오브젝트 스토리지의 데이터 접근 방식

13. 분산 데이터베이스의 5 가지 투명성

01	ISO 31000		
문제	ISO 31000		
도메인	IT경영전략	난이도	중(상/중/하)
키워드	리스크관리 국제표준, 8개의 기본원칙, 의사소통 및 협의, 맥락의 이해, 위험식별, 위험분석, 위험평가, 위험대응, 감독 및 보고		
출제배경	기업의 리스크 관리를 위한 거버넌스 측면에서의 대응 방안 및 전략 검토		
참고문헌	IT 기술사회 자료, https://demingcert.com/iso-31000-risk-management		
해설자	강남평일야간반 전일 기술사(제 114회 정보관리기술사 /nikki6@hanmail.net)		

I. 기업운영의 비즈니스 관리를 위한 ISO 31000 개요

가. ISO 31000 정의

- 모든 비즈니스 활동에서 발생하는 모든 종류의 리스크를 관리하기 위한 가이드라인을 제공하는 국제 표준

나. ISO 31000 기본 원칙

8 원칙	세부 내용
통합	- 위험 관리는 조직의 거버넌스, 관리 및 문화의 필수적인 부분
체계적이고 포괄적	- 조직은 위험 관리에 체계적이고 포괄적인 접근 방식을 채택
맞춤형	- 위험 관리 프로세스는 조직의 특정 상황과 요구 사항에 맞게 조정
종합적	- 모든 수준의 이해관계자가 참여해야 하며 포괄적이고 투명해야 함
동적	- 조직의 내부 및 외부 상황 변화에 적응하는 반복적이고 역동적인 프로세스
유용성	- 위험 관리의 목적은 정보에 입각한 의사 결정을 지원하는 것
인간과 문화적 요소	- 위험 관리에는 인적, 문화적 요인을 고려
지속적 개선	- 조직은 위험 관리 프레임워크와 프로세스를 발전 시켜야 함

- ISO 31000 2022년 11월 마지막 업데이트부터는 11개의 기본원칙이 8개로 축소

II. ISO 31000 프로세스

가. ISO 31000 프로세스 흐름도

나. ISO 31000 프로세스 상세 설명

절차	내용
의사소통 및 협의 (communicate & consult)	- 조직의 위협 인식에 대한 공유 및 협의
맥락의 이해 (establish context)	- 조직의 운영 현황과 주변 환경에 대한 이해
위험식별 (risk identification)	- 조직의 목적에 위험한 영향을 줄 수 있는 내, 외부 사건의 파악
위험분석(risk analysis)	- 위험사건이 어떻게 발생하고 어떻게 영향을 줄 것인가에 대한 분석
위험평가 (risk evaluation)	- 위험사건의 확률과 피해에 대한 예측 및 위험수요(risk tolerable) 및 정책 대응 여부 판단(risk register, risk profiling)
위험대응 (risk treatment)	- 위험평가를 바탕으로 직접적 위험 대응 - 종료(terminate): 위험이 발생할 수 있는 행위 자체를 자제 - 대응(treat): 위험확률 혹은 피해를 줄일 수 있는 대책을 마련 - 이전(transfer): 보험의 가입 등을 통한 위험의 분산 및 이전 - 수용(tolerate): 평가된 위험이 작다고 판단하고 감내함(수용함)
감독 및 보고(monitor & review)	- 보고 및 평가를 통한 조직 학습

III. ISO 31000 관련 추가 표준 제안 활동

표준	제안 활동
ISO/TR 31004	- 위험관리 > ISO 31000 구현 지침
IEC 31010	- 위험 관리 > 위험 평가 기술
ISO 31022	- 위험 관리 > 법적 위험 관리 지침

- ISO 31000 은 업계, 주제, 지역별로 다른 수많은 기존 표준, 방법론 및 패러다임을 대체하기 위해 위험 관리 프로세스를 사용하는 실무자와 기업에 보편적으로 인정되는 패러다임을 제공

"끝"

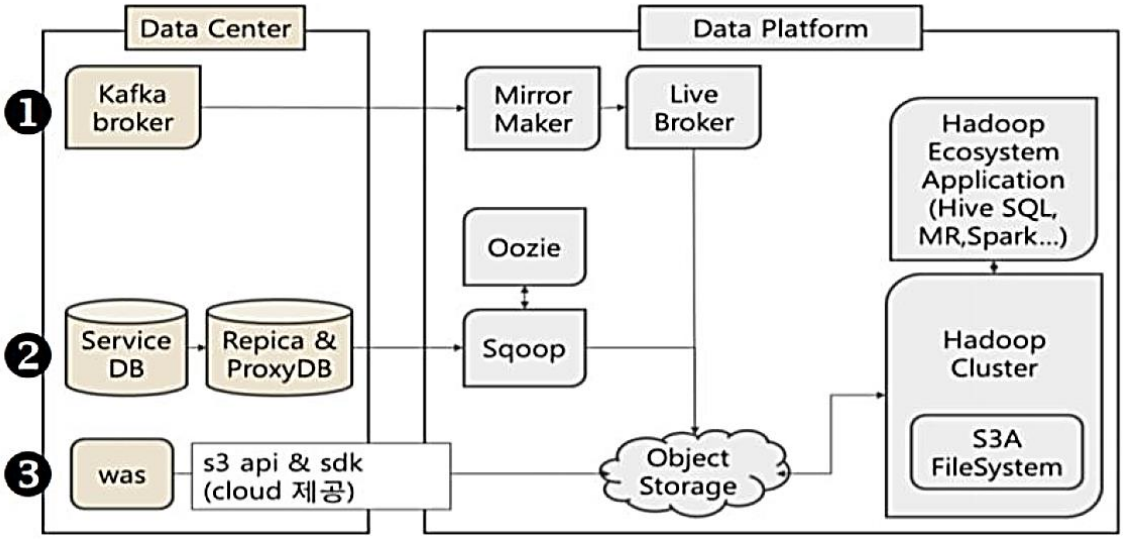
02	데이터 거래소		
문제	데이터 거래소		
도메인	데이터베이스	난이도	중 (상/중/하)
키워드	마이데이터, 데이터 브로커, Data Center, Data Platform, Kafka, Hadoop		
출제배경	데이터 3법 개정과 더불어 19년 12월 국내 최초 한국 데이터 거래소 출범으로 인한 개념 확인		
참고문헌	ITPE 서브노트		
해설자	강남평일야간반 전일 기술사(제 114회 정보관리기술사 /nikki6@hanmail.net)		

I. 자원 지원 빈국에서 데이터 자원 부국으로 도약, 데이터 거래소의 개념

- ICT를 통해 개인기업, 공공기관, 정부 등에서 확보한 데이터를 수집, 가공해 부가가치를 높여 필요한 소비자에게 공급하는 대규모 플랫폼
- (제안 배경) 표준 품질 보증, 다양한 데이터 통합 분석, 데이터를 활용한 경제 활성화

II. 데이터 거래소의 아키텍처 구성도와 구성요소

가. 데이터 거래소의 아키텍처 구성도



데이터 입수 방식	① Kafka 연동: 실시간 데이터 입수 지원 ② DB 복제 : 1일 Batch로 입수 지원 ③ S/W 설치하여 Object Storage에 직접 적재

- 개인정보나 민감정보의 필터링을 위해 Data Platform 내부에 Screen을 장착하고 있으며, Buyer는 무료 및 유료 데이터를 이용할 수 있음

나. 데이터 거래소의 구성요소

구분	구성요소	설명
Data Center	Kafka broker	- 대용량 실시간 로그 처리에 특화
	Replica & Proxy DB	- DB Scale-out 제공을 위한 읽기 처리량 향상
	S3(Simple Storage Service) API	- HTTPS형태의 API로 데이터를 저장하거나 추출
Data Platform	Hadoop Ecosystem	- Data Lake에 최적화된 오픈소스 프레임워크
	Object Storage	- 키 값과 데이터만 저장할 수 있는 확장성과 속도 우수
	Sqoop	- 대량의 RDB를 HDFS로전송 후 분석 용이

- 현재 KDX(Korea Data Exchange) 데이터 제공은 CSV등의 파일 형태와 Dash Board 형태의 리포트 방식으로 제공.

III. 해외 주요국의 데이터 거래 제도 동향

성숙도	해외 주요국	설명
활성화 단계	미국	- 데이터 브로커 제도 활성화 - 브로커 업체 수는 약 650개 정도이며, 연 매출 규모는 1560억달러 추정
	중국	- 지난해부터 개설된 빅데이터 거래소 7개 운영
초기 단계	영국	- 마이 데이터(MyData) 프로그램 운영을 통해 기계가 개인데이터 제공

"끝"

03	베이지안 최적화(Bayesian Optimization)		
문제	베이지안 최적화(Bayesian Optimization)		
도메인	인공지능	난이도	상(상/중/하)
키워드	Surrogate model, Acquisition function		
출제배경	최근 하이퍼파라메터 튜닝방법의 중요성에 따른 다양한 기법 검토		
참고문헌	ITPE 서브노트, https://gils-lab.tistory.com/61		
해설자	강남평일야간반 전일 기술사(제 114회 정보관리기술사 /nikki6@hanmail.net)		

I. Random Search 와 통계적 기법을 활용한 베이지안 최적화 개요

가. 베이지안 최적화(Bayesian Optimization) 정의

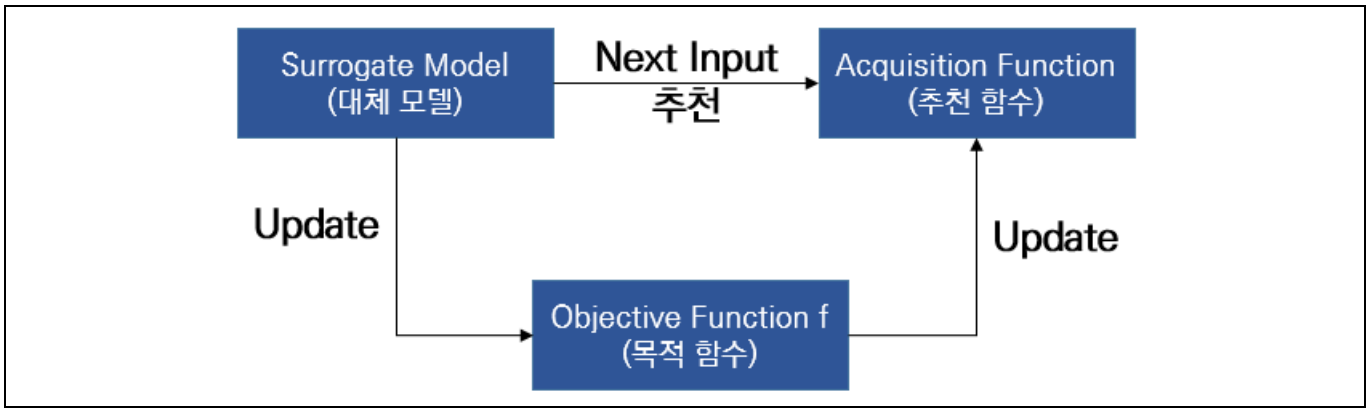
- 알려져 있지 않은 목적함수를 최대화(혹은 최소화)로 하는 최적 해를 찾는 기법으로 지금까지 확보된 데이터화 평가지표의 숨겨진 관계를 모델

나. 베이지안 최적화 특징

특징	설명
확률론적 모델	- 모델 성능의 예상되는 개선을 기반으로 시도할 다음 하이퍼 매개변수 세트를 예측하는 데 사용
최적의 하이퍼파라메터 조합 선정	- 모델 성능에 대한 이전 평가 및 하이퍼파라미터 값에 대한 제약 조건을 포함하여 목적 함수에 대해 사용 가능한 모든 정보를 활용

II. 베이지안 최적화 프로세스

가. 베이지안 최적화 흐름도



나. 베이지안 최적화 프로세스

구분	항목	세부내용
필수 구성요소	Surrogate Model	- 목적 함수를 추정하는 머신러닝 모델(주로 가우시안 프로세스 활용)
	Acquisition Function	- 다음 테스트 시 데이터 포인트 추천하는데 활용하는 함수
절차	1. 임의로 n_0개의 데이터 포인트 $x=\{x^1,\ldots, x^{n0}\}$생성 및 평가	

	2. 평가를 결과로 f에 대한 사후 확률 $Pr(f\|X^{1:n0})$ 업데이트
	3. 현재 f로 계산한 Acquisition Function을 최대화하는 x^* 탐색
	4. x^*평가 및 x에 추가

- Bayesian Optimization 방법은 좋은 성능을 보여주지만 느리다는 단점 존재

III. Bayesian Optimization의 단점을 극복한 Hyperband

특징	설명
개념	- 하이퍼파라미터 공간을 효율적으로 탐색하기 위해 새로운 적응형 리소스 할당 전략을 사용하는 최신 하이퍼파라미터 최적화 알고리즘
원리	- 랜덤 서치 기반 방법을 사용하여 여러 라운드로 이루어진 반복적인 과정을 거침 - 각 라운드에서는 먼저 랜덤한 하이퍼파라미터 설정으로 모델을 훈련시키고, 그 중 일부는 성능이 좋은 것만 선택하여 다음 라운드에 사용

- 하이퍼밴드는 CNN(Convolutional Neural Network), RNN(Recurrent Neural Network), DBN(Deep Belief Network)을 비롯한 다양한 딥 러닝 모델에 사용

"끝"

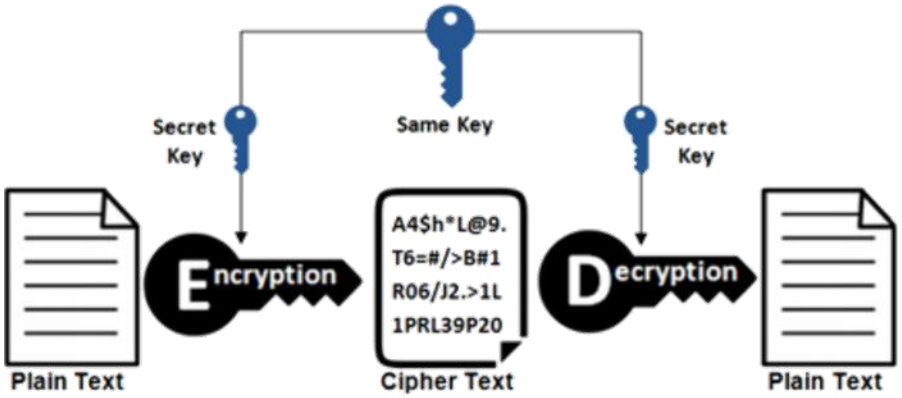
04	대칭 암호화와 비대칭 암호화		
문제	대칭 암호화와 비대칭 암호화		
도메인	정보보안	난이도	하 (상/중/하)
키워드	암호키와 복호화키, 동일, 불일치, 대칭키 – 비밀키, 비대칭키 – 공개키, 개인키		
출제배경	정보보안의 기본에 대한 지식 확인		
참고문헌	ITPE 기술사회 자료		
해설자	단합반멘토 안경환 기술사(제 110회 정보관리기술사 / akh.itpe@gmail.com)		

I. 암호와 복호의 ONE KEY. 대칭(Symmetric) 암호화

가. 대칭(Symmetric) 암호화의 개념

정의	- 암호문(Cyphertext)을 생성(암호화)할 때 사용하는 키와 암호문(Cyphertext)으로부터 평문(Plaintext)을 복원할 때 사용하는 키가 동일한 암호화 알고리즘	
특징	- 빠른 암호 연산	- 암호화 방식에 속도가 빠르므로 대용량 data 암호화에 적합
	- 키 교환 문제	- 암호화와 복호화에 동일한 키가 사용되므로 키의 교환 시 키 탈취에 대한 문제 발생
	- 키 관리 문제	- 관련된 사람이 증가될수록 키 관리의 문제 발생
	- 기밀성 제공	- 기밀성을 제공하나, 무결성, 인증, 부인 방지는 보장 불가

나. 대칭(Symmetric) 암호화의 개념도와 종류



종류	설명	
블록 암호화(Block cipher)	- 데이터를 고정된 길이의 입력 블록을 고정된 길이의 출력 블록으로 변환하는 알고리즘 - 암호화한 방식을 그대로 역으로 수행하면 복호화 할 수 있는 Feistel 구조와 역으로 복호화 할 수 없는 SPN(Substitution Permutation Network) 구조로 분류	
	- 운영 모드	- ESB(Electronic Code Book) Mode, CBC(Cipher Block Chaining), CFB(Cipher FeedBack), OFB(Output

		FeedBack), CTR(CounTeR)
스트림 암호화(Stream cipher)	- 유사 난수를 연속적(스트림)으로 생성하여 암호화하려는 자료와 결합하는 대칭키 암호화	
	- 암호화 종류	- 동기식 스트림 암호, 비동기식 스트림 암호

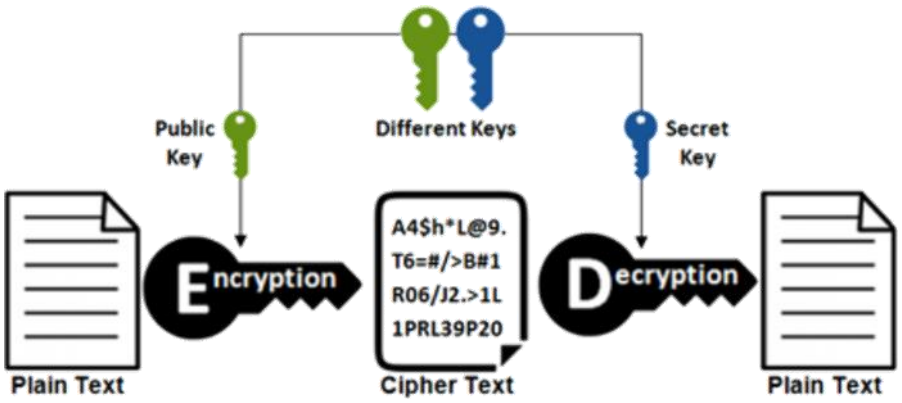
- 대칭 암호화 방식의 종류로 DES(Data Encryption Standard), AES(Advanced Encryption Standard), SEED 알고리즘, ARIA 알고리즘 등이 존재

II. 암호와 복호화 키의 분리. 비대칭(Asymmetric) 암호화

가. 비대칭(Asymmetric) 암호화의 개념

정의	- 암호문(Cyphertext)을 생성(암호화)할 때 사용하는 키와 암호문(Cyphertext)으로부터 평문(Plaintext)을 복원할 때 사용하는 키가 서로 다른 암호화 알고리즘	
특징	- 늦은 암호 연산	- 암호화 방식에 속도가 늦음
	- 키 교환 불필요	- 암호화한 키는 분배할 필요가 없고 공개키는 자유롭게 공개 및 배포
	- 기밀성 외 추가 기능 제공	- 기밀성, 인증과 부인 방지 기능을 제공

나. 비대칭(Symmetric) 암호화의 개념도와 동작 모드와 대표 알고리즘



종류	설명	
모드	- 암호 모드	- 송신자의 공개키로 송신하려는 메시지를 암호화하고, 송신자의 개인키로 복호화
	- 인증 모드	- 송신자의 개인키로 암호화하고 송신자의 공개키로 복호화하여 메시지 인증(부인방지)
대표 알고리즘	- Diffie–Hellman	- 이산대수의 난해함에 그 안전성을 둔 비밀키 교환 알고리즘
	- RSA	- 큰 숫자를 소인수 분해가 어렵다는 것에 기반을 둔 대표적 공개키 알고리즘
	- DSA(Digital Signature Algorithm)	- 미국 국립 표준·기술 연구소(NIST)가 공포한 서명 알고리즘 표준

	- ECC(Elliptic Curve Cryptography)	- 닐 코블리츠와 빅터 밀러가 타원곡선 이론에 기반한 공개 키 암호 방식

III. 대칭(Symmetric) 암호화와 비대칭(Asymmetric) 암호화의 비교

비교	대칭(Symmetric) 암호화	비대칭(Asymmetric) 암호화
키의 관계	- 암호키 = 복호키	- 암호키 ≠ 복호키
키의 수	- 두 사람 이상이 한 개의 동일한 비밀키 공유	- 전송 당사자간에 각각 키 쌍 (Private Key, Public Key) 공유
키의 종류	- 비밀키(Secret Key)	- 공개키(Public Key) - 개인키(Private Key)
키의 관리	- 복잡 (거래 당사자 전부 관리)	- 인증기관을 통해 전송 당사자 별 Private Key 발급 (상대적 단순)
부인방지 여부	- 대칭키로 인하여 부인방지 불가	- 키의 이원화로 부인방지 가능
속도	- 비트 단위 암호화로 상대적으로 빠른 속도 제공	- 큰 소수를 찾거나, 곡률 방정식 등의 연산으로 속도가 느림
용도	- 개인파일암호화, 특정그룹 내의 파일 등의 통신에 사용	- 다수의 사용자에 주로 사용
장점	- 키의 분배가 용이함 - 사용자의 증가에 따라 관리할 키의 개수가 상대적으로 적음 - 키 변화의 빈도가 적음 - 여러 가지 분야에서 응용이 가능함	- 암호화/복호화 속도가 빠름 - 키의 길이가 짧음 - 구현이 빠름 - 대칭키로 인하여 부인방지 불가
단점	- 암호화 / 복호화 속도가 느림 - 키의 길이가 김	- 사용자의 증가에 따라 관리해야 할 키의 수가 상대적으로 많음 - 키 변화의 빈도가 많음
대표 알고리즘	- AES, SEED, DES	- RSA, ECC

"끝"

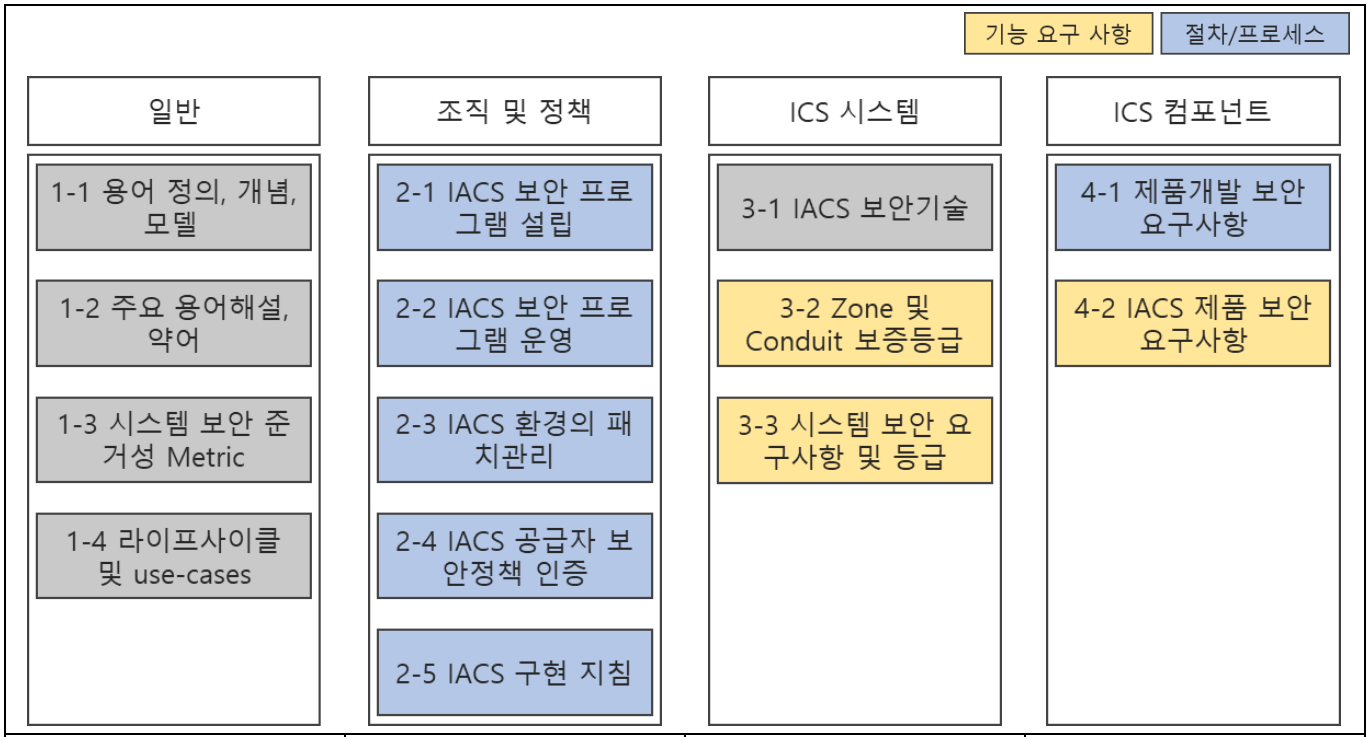
05	ISA/IEC 62443		
문제	ISA/IEC 62443		
도메인	정보보안	난이도	중 (상/중/하)
키워드	General, Policy & Procedure, System, Component		
출제배경	최근 ICS(Industrial Control System), IACS(Industrial Automation and Control Systems)의 스마트 팩토리 전환에 따른 네트워크 연결로 보안관리 요구 사항 부각에 따라 관련 표준 숙지 필요		
참고문헌	단합반-NS반 500제 핵심 노트, ITPE 기술사회 자료		
해설자	단합반멘토 안경환 기술사(제 110회 정보관리기술사 / akh.itpe@gmail.com)		

I. 산업 제어 시스템의 통합 보안 프레임워크, IEC 62443의 개념

- 산업제어시스템(IACS) 보안관리 요구사항과 보안기술, 제품의 개발 요구사항 및 구성요소에 대한 기술적 보안 요구사항 등이 정의되어 있는 산업제어시스템 보안 국제 표준

II. IEC 62443의 구성도와 구성요소

가. IEC 62443의 구성도



- 개념 모델, 용어 등 일반적인 사항 규정	- 산업제어시스템을 보유하는 조직의 보안 정책과 절차에 대해 규정	- 시스템 통합을 위한 ICS 시스템의 보안기능 요구사항 규정과 위험 감소 위해 필요한 강도를 가진 기본적인 요구사항(FR1 ~ FR7)을 선	- 산업제어시스템을 구성하는 제어기기, 장비, 애플리케이션의 보안을 취급하는 장비 업체를 위한 보증 요구사항과 기능 요구사항 규정

		택하여 설계 및 구현 실시	

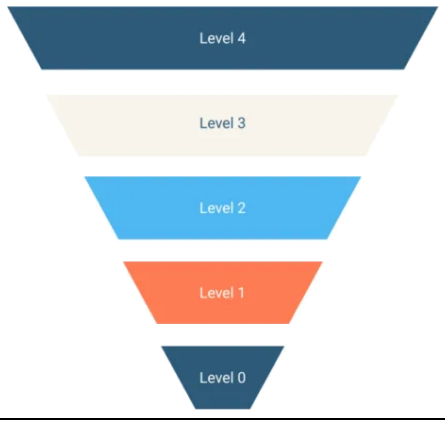
- General, Policy & Procedure, System, Component 총 4개의 Part로 구성되어 있음.

나. IEC 62443의 구성요소 설명

구분	세부	설명
General (Part 1)	- 용어 정의, 컨셉, 모델	- 7개 FR(Foundational requirements) 정의 - 식별 및 인증(FR1), 사용제어(FR2), 시스템 무결성(FR3), 데이터 기밀성(FR4), 데이터 제한성(FR5), 응답성(FR6), 자원가용성(FR7)
	- 용어, 약어 사전	- 사용하는 용어와 약어의 마스터 용어집 정의
	- 시스템 보안 적합 Metric	- IACS에 대한 우선 순위가 높은 시스템 사이버 보안 적합성 측정 기준 정의
	- 라이프사이클 및 유즈케이스	- IACS 보안 라이프사이클을 정의하고 실증 사례 설명
Policy & Procedure (Part 2)	- IACS 보안 프로그램 수립	- IACS 사이버 보안 관리 시스템 구축 필요 요소 정의
	- IACS 보안 관리 가이드 작성	- 설계 및 구현 후 보안관리시스템 운영 방안 기술
	- IACS 환경 패치 관리	- IT 기반과 다른 IACS 보안 환경 패치 관리 요구 사항
	- IACS 공급 업체 준수 요구사항	- IACS 공급 업체의 설치 및 유지관리 요구사항
System (Part 3)	- IACS 보안 기술	- 적용가능한 사이버보안 도구, 완화 대응책, 기술 제공
	- 영역, 전송에 대한 보안 수준	- IACS 시스템 및 네트워크 경로 보안 수준 목표 수립
	- 시스템 보안 요구 사항 및 수준	- 위험 평가 단계에서 필요한 서비스 및 기능을 식별
Component (Part 4)	- 제품 개발 요구 사항	- 보안개발생명주기 정의 및 그에 따른 요구사항 기술
	- IACS 컴포넌트 요구 사항	- 1-1에 기술된 7개 FR 관련 상세 컴포넌트 요구사항

- Part 3-3에 IACS 시스템의 보안 요구 사항 및 보장을 위한 Security Assurance Level이 정의됨

III. IACS의 보안 안전성 기준, Security Assurance Level

Security Level		설명
	Level 4	- 의도적 위협에 대한 광범위한 자원, 특정 기술 및 정교한 보호 수단 필요
	Level 3	- 의도적 위협에 대한 적합한 자원, 특정 기술 및 일반적 보호 수단 필요
	Level 2	- 의도적 위협에 대한 낮은 자원, 일반적 기술 및 간단한 보호 수단 필요
	Level 1	- 우연한 위반, 위협에 대한 보호 필요
	Level 0	- 특정 요구 사항 또는 보안 보호 요구 사항 없음

"끝"

06	큐싱(Qshing)		
문제	큐싱(Qshing)		
도메인	정보보안	난이도	하 (상/중/하)
키워드	QRCode, 피싱(fishing)		
출제배경	감리와 전통적 비교 대상인 PMO 비교 사항 이해 확인		
참고문헌	ITPE 기술사회 자료		
해설자	단합반멘토 안경환 기술사(제 110회 정보관리기술사 / akh.itpe@gmail.com)		

I. QR코드 스캔하고 보니 금융사기, 큐싱(Qshing)의 개념

정의

- 스미싱(Smishing)에서 한 단계 더 진화된 금융사기 기법으로 폰뱅킹 사용자에게 인증 등이 필요한 것처럼 속여 QR코드(Quick Response Code)를 통해 악성 앱을 내려 받도록 유도하는 공격 기법

II. 큐싱(Qshing)의 공격 메커니즘(mechanism)

가. 큐싱(Qshing)의 공격 순서도

나. 큐싱(Qshing)의 공격 과정

공격 과정	사용 기술	설명
스팸 문자 발송	- 피싱(fishing) - URL Shortening Service	- QR 코드를 생성하고 피해자(victim)에게 무료, 할인 쿠폰 제공과 함께 악성 링크가 포함된 스팸 문자(SMS)를 발송
QR 코드 촬영	- 카메라, 영상 처리	- 피해자는 스팸 문자의 내용을 확인 후 QR 코드를 스캔(scan)하여 해커(hacker)가 유도한 앱 설치 사이트로 이동

악성 앱 다운 및 설치	- 앱 설치 관리자	- 해커가 의도한 사이트에서 출처를 알 수 없는 앱(app)을 다운로드 후 설치
해커 명령 수신, 정보 유출	- 원격 제어	- 다양한 원격 제어 도구들을 이용하여 피해자의 디바이스에 있는 정보 등을 유출

- QR 코드는 2차원적 구성으로 가로, 세로를 활용하여 문자는 최대 4,296자, 한자는 최대 1,817자, 숫자도 최대 7,089자를 기록 가능

III. 큐싱(Qshing) 공격의 대응 방안

대응 방안	대응 주체	설명
URL 검증 사이트	- 국가 및 기업	- 접속 유도 URL에 대한 검증 사이트 운영으로 사용자에게 사전 검증 정보 제공
SMS 발송 주체 제공	- 기업	- 대량 SMS 발송 주체의 경우 발송 주체의 정보를 추가 제공
2차인증 유도 설치금지	- 2차인증 유도 설치금지	- QR 코드로 이동 후 2차인증 유도로 추가 정보 필요시 정보 제공 및 설치 금지
디바이스 앱 설정	- 디바이스 앱 설정	- '알 수 없는 출처(미인증) 앱 설치' 기능 설정 및 유지
미 확인 문자 URL 접속 금지	- 미 확인 문자 URL 접속 금지	- 출처가 불분명한 SITE 접속 금지

"끝"

07	ELK(Elasticsearch/Logstash/Kibana) 스택		
문제	ELK(Elasticsearch/Logstash/Kibana) 스택		
도메인	디지털서비스	난이도	상(상/중/하)
키워드	수집, 분석, 시각화		
출제배경	빅데이터 분석 및 활용에 대한 오픈소스 프로젝트 이해		
참고문헌	https://www.elastic.co/kr/elastic-stack https://aws.amazon.com/ko/what-is/elk-stack/		
해설자	모멘텀 안수현 기술사(제119회 정보관리기술사/tino1999@naver.com)		

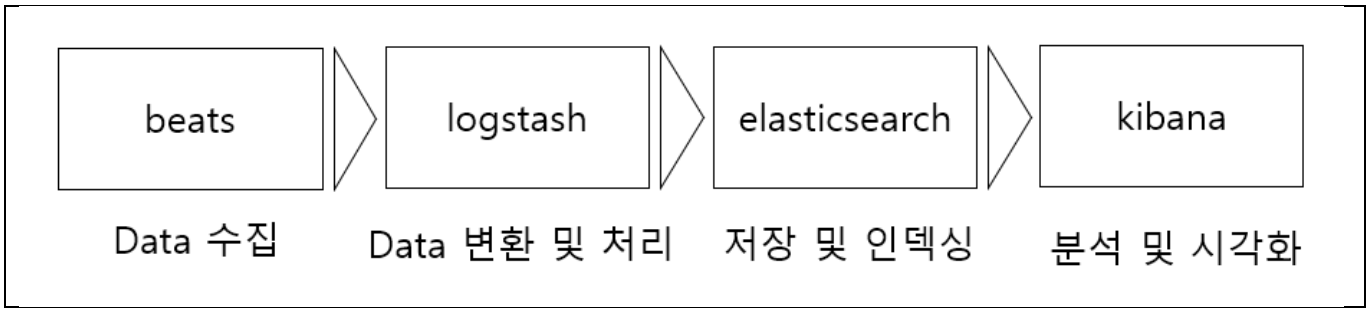
1. 데이터 수집 및 분석을 위한 오픈소스 프로젝트, ELK(Elasticsearch/Logstash/Kibana)의 개념

항목	설명
Elasticsearch	수집된 데이터를 저장소에 저장하고 관리하는 오픈소스 기반 검색 및 분산 엔진
Logstash	다양한 소스로부터 데이터를 수집하고 전환하여, 원하는 대상에 전송할 수 있는 오픈소스 도구
Kibana	데이터를 시작적으로 탐색하고 실시간으로 분석하는 오픈소스 도구

- 세가지 오픈소스 프로젝트와 추가적인 기술을 조합하여, 효율적인 데이터의 수집 및 분석을 제공하는 기술

2. ELK 스택의 설명

가. ELK 스택의 Data Flow



- 적용할 상황에 따라 추가적인 프로젝트 적용 및 제외가 가능한 유연성 보유

나. ELK 스택의 설명

구분	설명	세부 내용
Data Flow	데이터 수집	- 수집대상 서버에서 beats가 특정 트리거에 의해 logstash로 데이터 전송
	데이터 변환 및 처리	- 전달된 데이터를 커스터마이징 및 가공하여 elasticsearch로 전달
	저장 및 인덱싱	- 전달 받은 데이터를 저장 및 인덱싱, 검색
	분석 및 시각화	- kibana는 데이터를 분석하고, 결과를 시각화
기능	분석 및 검색	- 로그 분석, 문서 검색 등의 기능 제공
	보안 및 이벤트 관리	- SIEM 등을 통한 빅데이터 보안 기능 제공

- ELK 스택은 사용자에게 모든 시스템과 애플리케이션에서 로그를 집계하고 이를 분석하며 애플리케이션과 인프라 모니터링 시각화를 생성하고, 빠르게 문제를 해결하며 보안 분석할 수 있는 능력을 제공.

"끝"

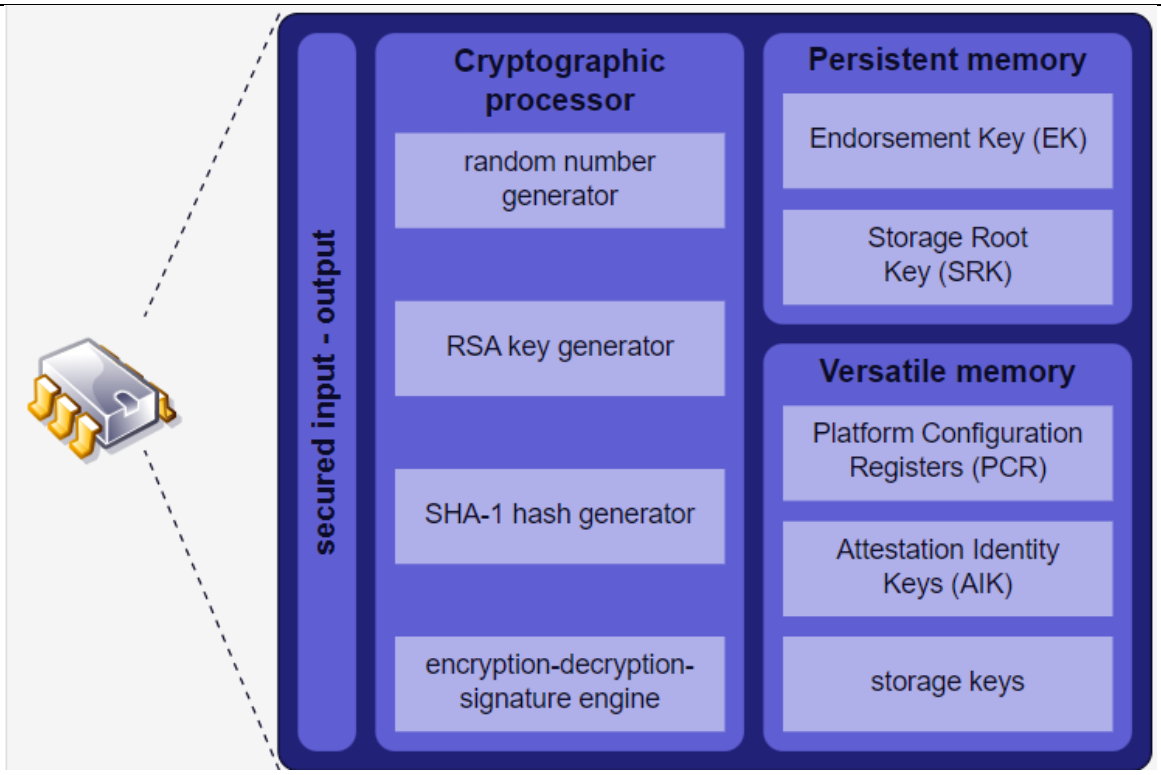
08	TPM(Trusted Platform Module)		
문제	TPM(Trusted Platform Module)		
도메인	CA/OS, 보안	난이도	중(상/중/하)
키워드	보증계층, 저장계층, 플랫폼 계층		
출제배경	보안위협 늘어감에 따른, 하드웨어 기반의 보안 기술에 대한 이해		
참고문헌	https://learn.microsoft.com/ko-kr/windows/security/hardware-security/tpm/trusted-platform-module-overview https://namu.wiki/w/TPM		
해설자	모멘텀 안수현 기술사(제119회 정보관리기술사/tino1999@naver.com)		

I. TPM (Trusted Platform Module)의 개요

- 키와 패스워드, 디지털 인증서를 저장하고, 암호화 작업을 수행하도록 설계된 보안 암호화 프로세서

II. TPM의 구성도 및 세부설명

가. TPM의 구성도



(그림출처 : 나무위키)

- TPM 2.0에서 암호화 알고리즘에 ECC가 추가되고 SHA-2가 추가됨

나. TPM의 세부설명

구분	항목	세부 내용
암호 알고리즘	ECC	공개키 암호화 알고리즘인 기존 RSA에 ECC가 추가
	SHA-2	대칭키 암호화 방식인 AES와 SHA-2 추가
Storage 관리	보증계층과 저장계층	제품 출하 시에 정해진 보증키를 저장하는 계층 (Endorsement Hierarchy, EH, Storage Hierarchy, SH)
	플랫폼 계층	제조업체나 운영제체가 별도로 사용가능한 저장 계층 (Platform Hierarchy, PH)
종류	Discrete TPM	별도 IC칩으로 추가 장착하는 형식
	Integrated TPM	칩셋에 통합되어 기능이 제공
	Firmware TPM	메인보드 UEFI 펌웨어에서 지원

- TPM은 소프트웨어적인 복호화에서 그치지 않고 하드웨어적으로도 보안성을 한층 강화하는 방법

"끝"

09	좋은 소프트웨어가 갖추어야 할 4가지 특징		
문제	좋은 소프트웨어가 갖추어야 할 4가지 특징		
도메인	소프트웨어공학	난이도	중(상/중/하)
키워드	신뢰성, 유지보수성, 사용용이성, 정확성		
출제배경	소프트웨어의 기본적인 지식 점검		
참고문헌	쉽게 배우는 소프트웨어 공학(김치수 저, 한빛아카데미) 새로 쓴 소프트웨어 공학(최은만 저, 정익사)		
해설자	모멘텀 안수현 기술사(제119회 정보관리기술사/tino1999@naver.com)		

I. 소프트웨어 공학의 개요

가. 소프트웨어 공학의 개념

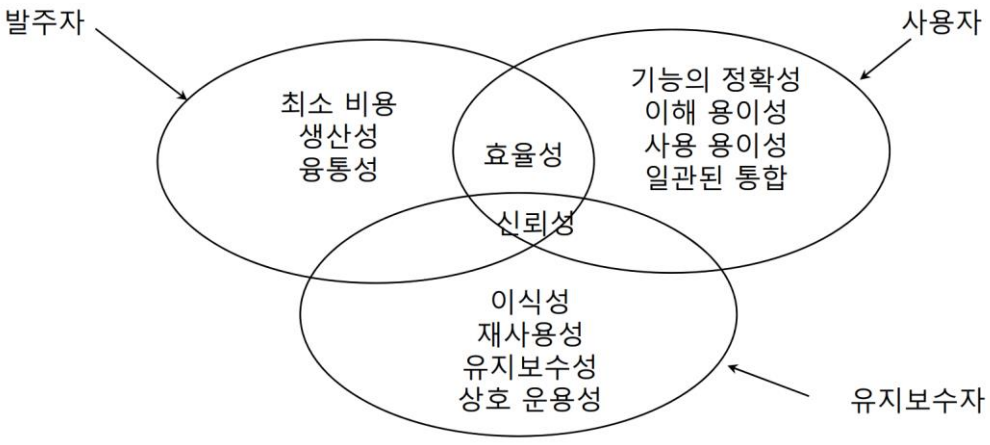
- 소프트웨어의 개발, 운용, 유지보수 등의 생명 주기 전반을 체계적이고 서술적이며 정량적으로 다루는 학문

나. 소프트웨어 공학의 목표

목표	필요 기법
고품질(Quality) 소프트웨어의 생산	요구사항 관리, 품질관리
사용자 만족도 증진	요구사항 관리, 품질관리
정해진 비용, 기간, 자원으로 소프트웨어 생산	정해진 비용, 기간, 자원으로 소프트웨어 생산
소프트웨어 생산 프로세스 수행능력 개선	요구사항 관리, 적정한 SDLC
생산성(Productivity) 향상	요구사항 관리, 부품화, 모듈화, 패턴화 기법

- 소프트웨어 공학의 목표는 좋은 품질과 생산성의 향상

II. 좋은 소프트웨어가 갖추어야 할 4가지 특징



좋은 소프트웨어 조건	설명
정확성(Correctness)	- 기능적으로 맞게 동작하는가, 표준에 적합한가 - 요구 분석서의 기능과 일치하는지 점검

신뢰성(Reliability)	- 소프트웨어가 주어진 기간 동안 바르게 작동할 확률 - 오류 발생 확률에 반비례 - 정확성 제공하기 위한 필요조건
강인성(Robustness)	- 요구 명세에 표시하지 않은 상황(오류 입력)에서도 제대로 작동하는 성질
성능(Performance)	- 수행 속도, 데이터/트랜잭션 처리량 - 알고리즘의 시간 복잡도 - 시뮬레이션, 스트레스 테스트
사용 용이성(Usability)	- 시스템을 친근하게 느낄 수 있는 성질 - 사용 대상에 따라 달라질 수 있음 - 사용자 인터페이스, Human factor
유지보수성(Maintainability)	- 보수성: 정해진 기간에 소프트웨어 결함을 해결할 수 있는 성질 - 진화성: 잠재적 발전 가능성 (추가 요구사항에 따라 기능이 진화할 수 있어야 함)
재사용성(Reusability)	- 소프트웨어 부품(라이브러리, 클래스 등)의 성질 - 확장 가능성(openness) - 적응성(adaptability) - 이용 용이성(closeness)

- 좋은 소프트웨어는 '사용자의 요구사항을 만족'하고 '정확하게 동작'하며 '쉬운 사용방법'과 '좋은 코드'로 개발된 소프트웨어.

"끝"

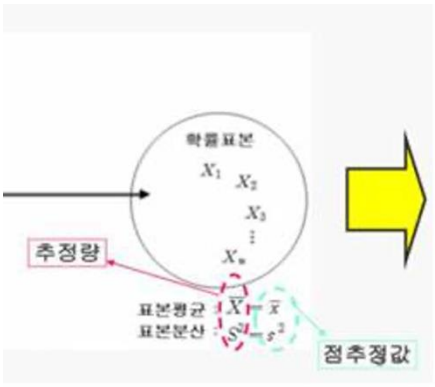
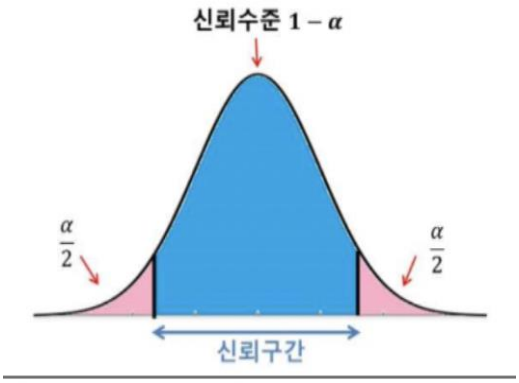
10	모집단의 특성을 추론하는 점추정과 구간추정 비교		
문제	모집단의 특성을 추론하는 점추정과 구간추정 비교		
도메인	확률통계	난이도	중(상/중/하)
키워드	추정이론, 불편성, 유효성, 일치성, 충분성, 신뢰구간, 신뢰수준, 가설검정		
출제배경	매회차 통계 관련 출제 및 기본적인 추정 이론에 관련된 지식 확인		
참고문헌	ITPE 기술사회		
해설자	BP반 김찬일 기술사(제 130회 정보관리기술사 /s2carey@naver.com)		

I. 모집단의 특성을 추론하는, 점추정과 구간추정 개념 비교

점추정	구간추정
추정이론 중 모수에서 추출된 표본으로 모수의 값에 가까울 것이라 예상되는 하나의 값을 제시하는 추정 방법	추정이론 중 모수에서 추출된 표본으로 모수의 값에 가까울 것이라 예상되는 특정 구간 안에 있을 것이라는 것을 나타내는 추정방법

II. 점추정과 구간추정의 상세 비교

가. 점추정과 구간 구간추정의 개념도 비교

점추정	구간추정
	

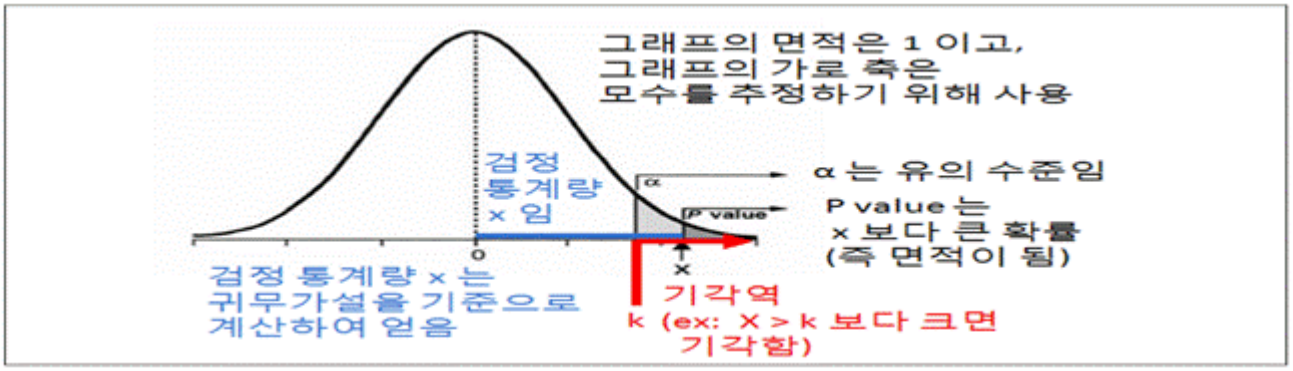
- 추정이론 중 점추정은 하나의 값, 구간추정은 신뢰구간을 추정하여 도출 방식과 제공에 따른 차이점 존재

나. 점추정과 구간추정 상세 비교

구분	점추정	구간추정
추정값	단일 수치 값	하한값과 상한값 범위
표현	직접 표현하지 않음	신뢰구간 통해 표현
신뢰수준	없음	신뢰수준 설정 표현
정보의 양	제한된 정보 (단일 추정치)	추가 정보 제공
사용 용이성	간단하고 해석 용이	계산 복잡, 해석 어려움의 가능성
정확성 정보	제공하지 않음	제공함

- 점추정이나 구간추정을 통해 얻은 결과를 사용하여 특정 가설이 참인지 거짓인지 판단이 가능함.

III. 추정 후 가설검정을 통한 통계적 유의성 확인



- 점추정이나 구간추정을 통해 얻은 결과를 사용하여 특정 가설이 참인지 거짓인지 판단, 어떤 처리가 효과가 있는지 없는지, 두 집단 간의 평균에 차이가 있는지 없는지 등을 검정

"끝"

11	다중공선성 (Multicolinearity)		
문제	다중공선성 (Multicolinearity)		
도메인	확률통계	난이도	상(상/중/하)
키워드	다중회귀분석, 분산팽창요인 (VIF), 결정계수, 상관관계, 변수제거, 주성분 분석		
출제배경	최근 통계문제 다수 출제, 다중 회귀 분석에서 가장 중요한 토픽 지식 이해 점검		
참고문헌	ITPE 기술사회		
해설자	BP반 김찬일 기술사(제 130회 정보관리기술사 /s2carey@naver.com)		

I. 강한 상관관계에 따른 문제, 다중공선성의 개요

가. 다중공선성의 정의

- 다중 회귀분석에서 사용된 모형의 일부 독립 변수가 다른 독립 변수와 상관 정도가 높아 데이터 분석 시 부정적인 영향을 미치는 현상

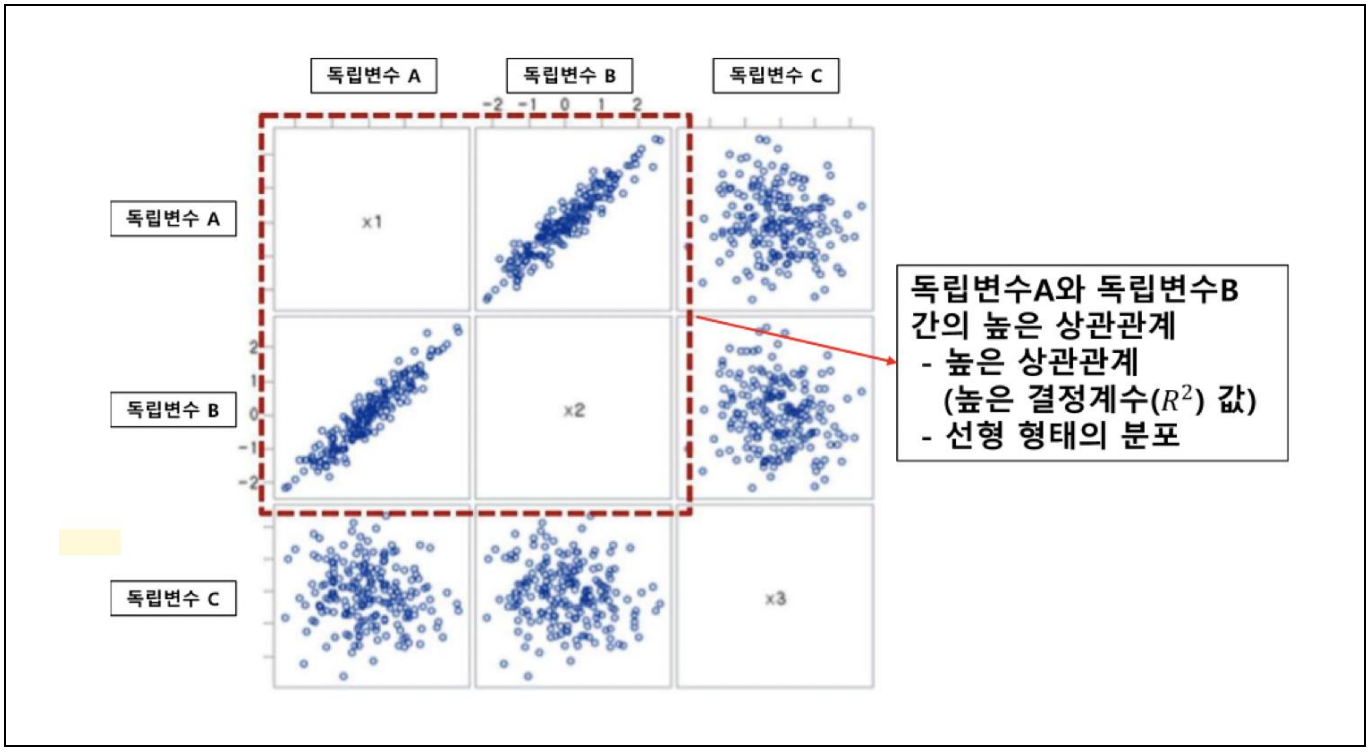
나. 다중공선성 특징

상관관계	- 다중회귀분석에서 두개 이상의 독립변수 간에 높은 상관관계
예측력 저하	- 다중공선성이 높은 모델은 데이터에 대한 예측력이 저하

- 독립변수간 높은 상관관계로 인하여 모델의 예측력이 저하되는 특징을 가짐.

II. 다중공선성 개념도 및 상세 설명

가. 다중공선성 개념도



- 독립변수 간의 상관관계가 강하여 결정계수(R^2) 값이 높아 과적합 발생

나. 다중공선성의 상세 설명

구분	항목	내용
판단기준	결정계수	- 피어슨 상관 계수 r^2, 0~1사이에 있으며, 종속변인과 독립 변인 사이에 상관 관계가 높을수록 1에 가까워 짐
	상관계수	- 독립변수들 간의 상관계수 도출 보통 0.7이상일 경우 상관관계가 높다고 판단
	분산팽창요인(VIF)	- VIF = 1/1-r 이 값이 10을 넘는다면 보통 다중공선성의 문제가 있다고 판단
해결방법	변수 제거	- 상관 관계를 가지는 두 변수 중 하나를 제거
	주성분 분석(PCA)	- 주성분 변수는 서로 독립이므로 주성분 변수를 독립변수로 사용하면 문제 발생 소지 감소
	다른 모델 사용	- MSE 최소화 추정 방법을 사용하여 다중공선성 문제해결

- 다중 회귀 분석 모델에서 다중공선성 문제 사전 예방을 위해 모델 설계 과성에서 독립변수 선택 중요.

III. 다중 회귀 분석 모델에서 독립변수 선택 방법

방법	설명
전진선택법 (Forward Selection)	- Y절편만 있는 상수모형부터 시작해 독립변수를 추가
후진소거법 (Backward Selection)	- 독립변수를 모두 포함한 상태에서 가장 적은 영향을 주는 변수를 하나씩 제거
단계적 선택법 (Stepwise Selection)	- 전진 선택법과 후진 제거법의 조합, 변수를 추가하거나 제거할 때, 미리 정해진 기준을 만족할 때까지 변수를 추가하거나 제거

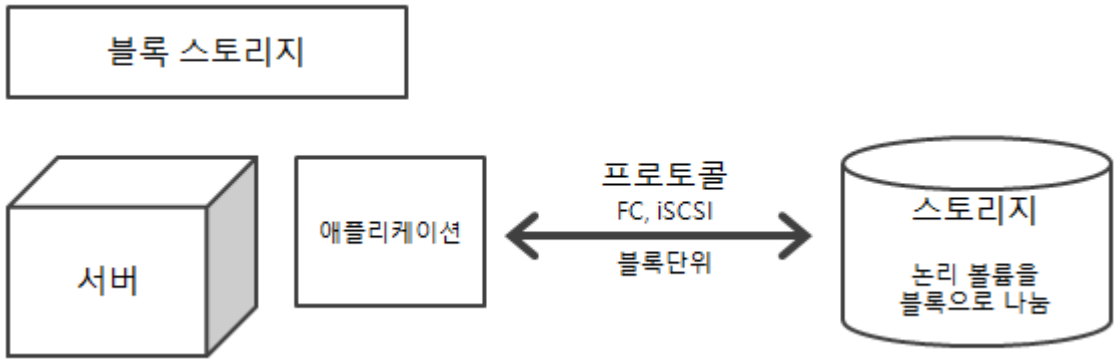
- 독립변수간 높은 상관관계로 인하여 모델의 예측력이 저하되는 특징을 가짐.

"끝"

12	블록 스토리지, 파일 스토리지, 오브젝트 스토리지		
문제	블록 스토리지, 파일 스토리지, 오브젝트 스토리지의 데이터 접근 방식		
도메인	디지털서비스	난이도	중 (상/중/하)
키워드	FC(Fibre Channel), iSCSI (Internet Small Computer System Interface), SMB(Server Message Block), CIFS(Common Internet File Sharing), NFS(Network File System), HTTP(HyperText Transfer Protocol), HTTPS(HyperText Transfer Protocol over Secure Socket Layer), RESTful API, 블록, 파일, 오브젝트		
출제배경	온프레미스 및 클라우드와 같이 다양한 환경에서 사용되는 스토리지 기술에 대한 이해도 확인		
참고문헌	그림으로 배우는 클라우드 2nd Edition (영진닷컴) ITPE 기술사회 자료집		
출제자	정상반 정상 기술사(제 124회 정보관리기술사 / itpe_peak@naver.com)		

I. 빠른 데이터 전송이 가능한, 블록 스토리지

가. 블록 스토리지의 개념

개념	- 일정한 크기의 블록으로 나누어진 스토리지의 논리 볼륨을 블록 단위로 액세스할 수 있는 스토리지
개념도	

- 애플리케이션 지정 블록의 주소로 액세스 하는 경우와, 파일 시스템 통해 블록의 주소로 액세스 가능.

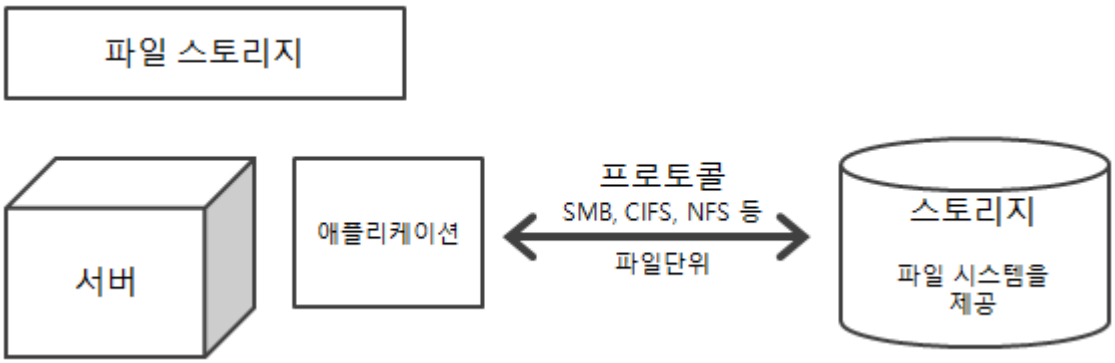
나. 블록 스토리지의 접근방식 및 장단점

구분	설명
접근방식	- 단일 스토리지 볼륨을 '블록'이라는 개별 단위로 분할하여 저장 - 각 블록은 저장된 위치에 대한 고유주소 보유 - 서버에서 파일 요청 시 블록들 재구성하여 하나의 데이터로 서버에 전달
특징	- SAN(Storage Area Network) 또는 가상 머신의 디스크로 사용됨 - 데이터가 블록 단위의 일정한 크기의 조각으로 나뉘어 저장됨
장점	- 데이터 블록이 운영체제와 무관하게 가장 효율적인 곳에 저장 - 파일 스토리지와 달리 접근방식이 단일경로에 국한되지 않아 탐색이 유연, 신속 - 대규모 트랜잭션, 대용량 데이터베이스 운영에 유리 - 하드웨어로부터 가상화하기 쉬워 컨테이너 기술과 호환 가능

단점	- 상대적으로 고비용 소모 - 메타데이터 처리 기능제한적으로 효율적인 데이터 정리 난해함

II. 파일의 접근제어, 속성정보 관리가 편리한, 파일 스토리지

가. 파일 스토리지의 개념

개념	- SMB, CIFS, NFS등의 프로토콜을 사용하여 파일 기준으로 읽고 쓸 수 있으며 공유 가능한 스토리지
개념도	

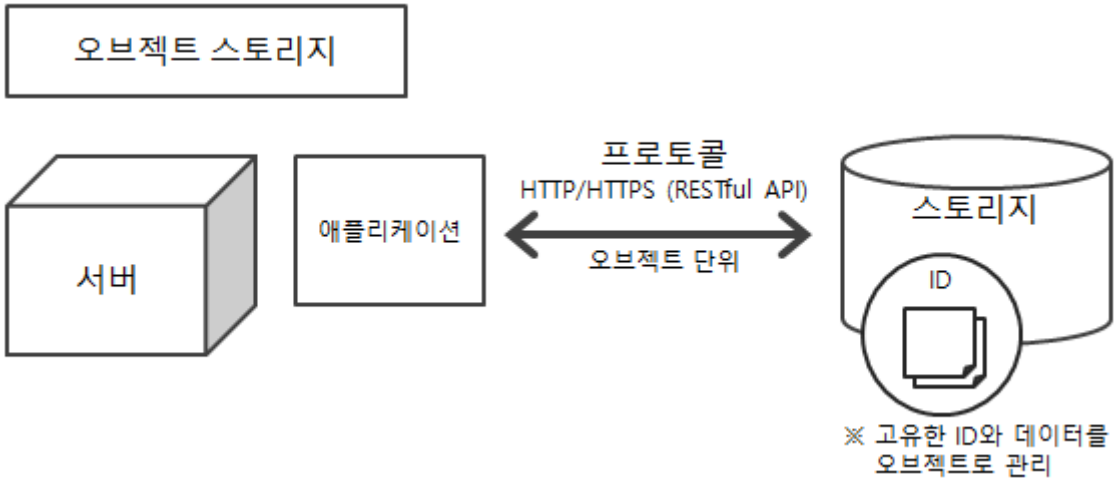
- 파일 시스템을 네트워크 통해 연결하여, 스토리지의 파일 시스템을 제공 가능.

나. 파일 스토리지의 접근 방식 및 장단점

구분	설명
접근방식	- 계층적 트리구조로 데이터를 저장하고 디렉토리에 접근하는 방식 - 일상적인 컴퓨터 사용시 볼 수 있는 윈도 탐색기, 맥 OS의 파인더 형태
특징	- 종이 파일 및 폴더가 캐비닛에 정리되는 방식을 모방한 계층적 구조 - 일반적으로 NAS(Network Attached Storage)에 사용됨
장점	- 논리적이고 직관적인 계층구조로 인하여 탐색이 직관적이고 간편함 - 수십년간 사용된 방식이며 많은 저장소가 파일 스토리지 기반으로 구축됨 - 다양한 매체 저장가능
단점	- 저장 구조 변경시 트리구조 변경하거나 시스템 변경 필요하여 확장성 낮음 - 데이터 접근이 단일 경로를 통해서만 이루어짐 - 파일수량 및 디렉토리 구조 복잡할수록 성능저하 - 운영체제간 호환성 낮음

III. 가용성과 비용 효율적인 저장 스토리지, 오브젝트 스토리지

가. 오브젝트 스토리지의 개념

개념	- HTTP 프로토콜 기반 REST API를 사용하여 고유한 ID 통해 데이터를 객체 단위로 처리하는 스토리지
개념도	

- 오브젝트의 ID(URI)를 지정하여 RESTful API 인터페이스 통해 액세스 가능.

나. 오브젝트 스토리지의 접근 방식 및 장단점

구분	설명
접근방식	- 오브젝트 ID 지정으로 API 인터페이스를 통해 액세스 - HTTP/HTTPS (Restful API)를 통해 액세스 오프젝트 스토리지에 접근
특징	- 파티션을 나눌 필요 없으며, 용량과 관계없이 데이터 수용 가능 - 계층구조가 아니므로 복잡한 디렉토리 구조가 없어 병목현상 미발생 - 자동 데이터 복제, 다운타임 미발생으로 데이터 일관성 보장 - 비정형 데이터에 작동
장점	- 데이터 검색 및 읽기 속도가 매우 빠름 - 맞춤작성 가능한 메타데이터 제공(상세한 검색 및 데이터 분석 수행가능) - 대용량 데이터 저장 가능
단점	- 메타데이터로 인한 입출력 오버헤드 발생 - 데이터 수정 발생시 오브젝트 전체 수정 필요 - 성능의 일관성 미보장

"끝"

13	분산 데이터베이스		
문제	분산 데이터베이스의 5가지 투명성		
도메인	데이터베이스	난이도	하(상/중/하)
키워드	위치 투명성, 복제 투명성, 병행 투명성, 분할 투명성, 장애 투명성		
출제배경	대규모 시스템에 구성되는 분산 데이터베이스에 대한 개념 이해 확인		
참고문헌	ITPE 서브노트 전담강의 데이터베이스 http://www.gurubee.net/lecture/2364		
해설자	정상반 정상 기술사(제 124회 정보관리기술사 / itpe_peak@naver.com)		

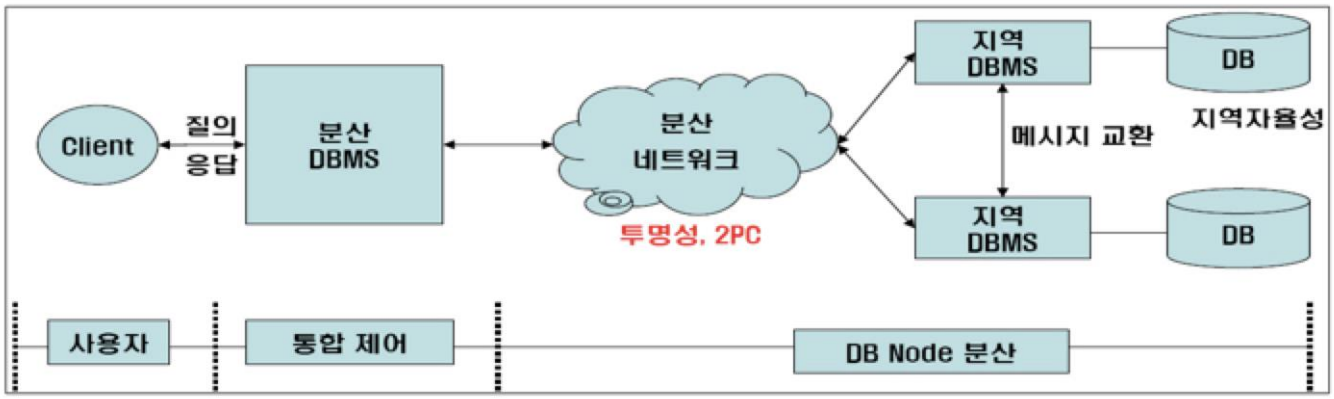
I. 데이터베이스, 분산 데이터베이스의 개요

- 논리적으로는 하나의 시스템으로 구성이 되어 있지만 물리적으로는 여러 사이트로 분산되어 있어 네트워크로 연결된 데이터베이스

II. 분산 데이터베이스의 투명성과 분산방법

투명성	주요개념	장점	단점
위치 투명성	- 사용자나 응용프로그램이 접근할 **데이터의 물리적 위치**를 알아야 할 필요가 없는 성질. 이를 보장하기 위해 DBMS는 Distributed Data Dictionary Directory가 필요	- Application 단순화 - 자유로운 Data의 접근	- 이중처리로 속도 저하 - 저장공간 낭비
복제 투명성	- 사용자가 응용프로그램이 접근할 데이터가 물리적으로 여러 곳에 **복제되어 있는지 여부**에 대해 알 필요가 없는 성질	- 상향식 점진적 확장 제공	- 이질형 시스템 구현 시 복잡
병행 투명성	- 여러 사용자나 응용프로그램이 동시에 **분산 데이터**베이스에 대한 트랜잭션을 수행하는 경우에도 결과에 이상이 발생하지 않는 성질 (Locking, Time Stamp 기법 이용)	- 자원사용 극대화	- 복잡한 Locking
분할 투명성	- 사용자가 하나의 논리적 릴레이션이 여러 **단편으로 분할**되어 각 단편의 사본이 여러 Site에 저장되어 있음을 알 필요가 없는 성질, 성능향상, Fragmentation을 위한 설계 필요	- Bottle neck 방지 - 시스템 성능향상	- 충분한 설계기술 필요
장애 투명성	- 데이터베이스가 분산되어 있는 각 지역의 시스템이나 통신망에 이상이 생기더라도 데이터의 무결성을 보존할 수 있는 성질 - 2PC 활용	- 장애처리 구현 단순	- 장애원인규명 복잡

III. 분산 데이터 베이스의 구축 방법



- 분산 DB의 설계 전략은 분산 DBMS에서의 통합제어, 지역 DBMS 모듈로 ACID 지원 방식으로 구축

"끝"

ITPE 기술사회
제132회 정보처리기술사 기출문제 해설집

대 상 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사, 정보시스템감리사 시험
발행일 2024년 01월 27일
집 필 강정배PE, 전일PE, 안경환PE, 안수현PE, 오준식PE, 김훈찬PE
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