제130회 정보관리기술사 해설집

2023.05.20

국가기술자격 기술사 시험문제

기술사 제 130 회 제 3 교시 (시험시간: 100 분)

분야	정보통신	자격종목	정보관리기술사	수검번호		성명	

※ 다음 문제 중 4 문제를 선택하여 설명하시오. (각 25 점)

1. 머신 러닝(Machine Learning)에서 활용되는 의사결정나무(Decision Tree)모델을 설명하시오.

2. 데이터저장 측면에서 파일, 데이터베이스, 블록체인을 비교하시오.

3. TCP(Transmission Control Protocol)는 네트워크에 혼잡(Congestion)이 발생한 경우 이를 해소하기 위한 다양한 메커니즘을 사용한다. 이와 관련하여 아래 사항들에 대해 설명하시오.

   1) TCP 혼잡제어 메커니즘의 구성요소

   2) 혼잡상황 감지

   3) 혼잡상황 제어

   4) 혼잡 윈도우 크기

4. 최근 인공지능 기술 활용이 증가하면서 다양한 보안 위협이 증가하고 있다. 이와 관련하여 아래 사항들에 대하여 설명하시오.

   1) 머신러닝 학습과정에서의 적대적 공격 4 가지와 방어기법

   2) 생성형 언어모델 기반의 인공지능 기술 활용 시 발생할 수 있는 보안취약점

5. 인공지능 등 지능정보 기술에 비현실적인 감리기준을 해결하기 위해 지능정보기술 감리 실무 가이드(한국지능정보사회진흥원, 2023 년)를 발간했다. 그 중 빅데이터 정보화 사업의 분석, 설계 단계별, 영역별 점검 항목에 대하여 설명하시오

6. 금융 클라우드 서비스를 받는 금융회사의 데이터는 가장 중요한 자산이며 민감정보를 다룬다. 금융 클라우드 SLA (Service Level Agreement)에 대하여 설명하시오.

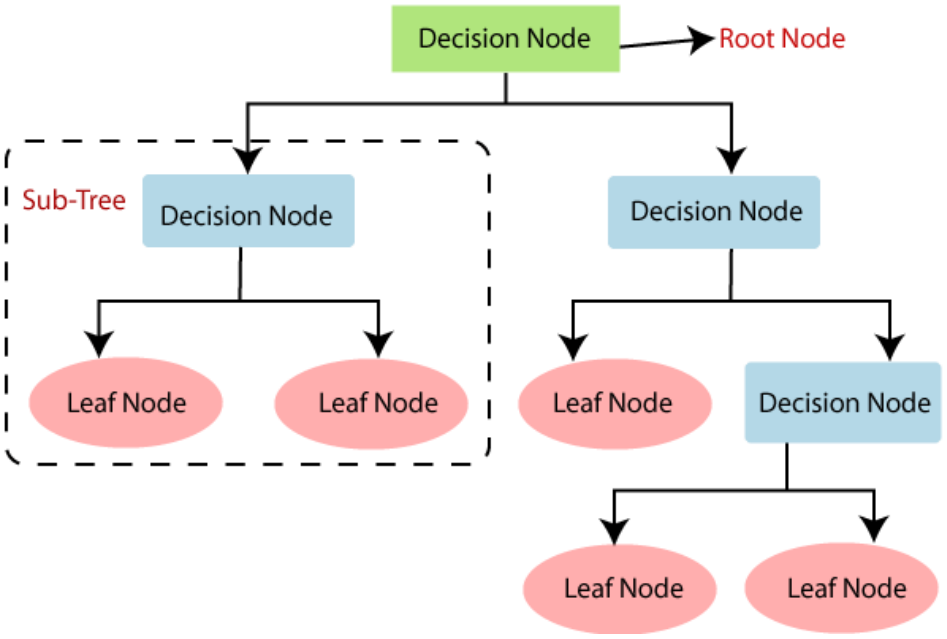
   1) SLA 개념

   2) 클라우드 SLA 가이드

   3) 금융 클라우드 SLA 가이드

01	의사결정나무(Decision Tree)		
문제	머신 러닝(Machine Learning)에서 활용되는 의사결정나무(Decision Tree)모델을 설명하시오.		
도메인	인공지능	난이도	상 (상/중/하)
키워드	성장(Tree Growing), 가치치기(pruning), 평균 제곱 오차(MSE, Mean Squared Error), 평균 절대 오차(MAE, Mean Absolute Error), 지니 지수(Gini Index), 엔트로피 지수(Entropy Index)		
출제배경	데이터 마이닝, 머신 러닝에서 자주 사용되는 의사결정나무(Decision Tree)에 대한 이해 확인		
참고문헌	IT기술사회 자료 http://bigdata.dongguk.ac.kr/lectures/datascience/_book/의사결정나무tree-model.html https://heytech.tistory.com/145		
출제자	단합반 안경환 기술사(제 110회 정보관리기술사 / akh.itpe@gmail.com)		

I. 스무고개 놀이, 의사결정나무(Decision Tree)모델의 개념



정의	- 의사결정 규칙을 나무 구조로 나타내어 전체 자료를 몇 개의 소집단으로 분류(classification)하거나 예측(prediction)을 수행하는 분석방법 - 설명변수(X) 간의 관계나 척도에 따라 목표변수(Y)를 예측하거나 분류하는 문제에 활용되는 나무 구조의 모델	
구성 요소	root node	- 의사결정 Tree가 시작되는 노드
	child node	- 하나의 마디로부터 분리되어 나간 2개 이상의 노드
	parent node	- 주어진 마디의 상위 노드
	terminal node	- 더 이상 분기가 되지 않아 자식 마디가 없는 최종 끝의 노드
	branch	- root node로부터 terminal node까지 연결된 node
	depth	- root node부터 terminal node 까지의 중간 node 들의 수

II. 의사결정나무(Decision Tree)모델의 절차

단계		설명
성장(Tree Growing)		- 최대 크기의 나무 모형 형성
	ASM(Attribute Selection Measure)	- 전체 데이터 세트에서 최상의 속성을 탐색
	분리 규칙	- 전체 데이터 세트에서 각 Node에서 적절한 최적의 분리 규칙 검색
	child node 생성	- 분리 규칙에 따라 하위 집합을 생성
가치치기(pruning)		- 최대 크기 나무모형에서 불필요한 가지를 제거하여 부분 나무모형(subtrees)의 집합을 탐색
최적 나무 모형 선택		- 가지치기의 결과인 나무모형의 집합에서 최적 모형을 선택 - 검증오차가 가장 작은 의사결정나무를 평가
해석 & 예측		- 구축된 나무모형을 해석하고 예측모형을 설정한 후 예측에 적용

III. 의사결정나무(Decision Tree)모델의 분류 기준

가. 의사결정나무(Decision Tree) 모델 기반 예측 모델링

분류 기준	수식	설명
평균 제곱 오차(MSE, Mean Squared Error)	$\frac{1}{n}\sum_{i=1}^{n}(y_i - t_i)^2$	- 모델 예측 값과 실제 값 간의 제곱오차의 평균 - 부모 노드의 평균 제곱 오차를 가장 많이 감소시키는 설명변수와 분리 값을 기준으로 자식 노드를 생성 - MSE가 작을수록 오차가 적은 좋은 모델
평균 절대 오차(MAE, Mean Absolute Error)	$\frac{1}{n}\sum\lvert\hat{y} - y\rvert$	- 모델 예측 값과 실제 값 간의 절대오차의 평균 - 부모 노드의 평균 절대오차를 가장 많이 감소시키는 설명변수와 분리 값을 기준으로 자식 노드를 생성 - MAE가 작을수록 오차가 적은 좋은 모델

나. 의사결정나무(Decision Tree) 모델 기반 분류 모델링

분류 기준	수식	설명
지니 지수(Gini Index)	$I_G = 1 - \sum_{j=1}^{c} p_j^2$	- 불순도 측정 지수 - 얼마나 다양한 데이터가 잘 섞여 있는지 정도 - 반대의 순수도는 같은 클래스의 데이터가 얼마나 포함하는지를 의미

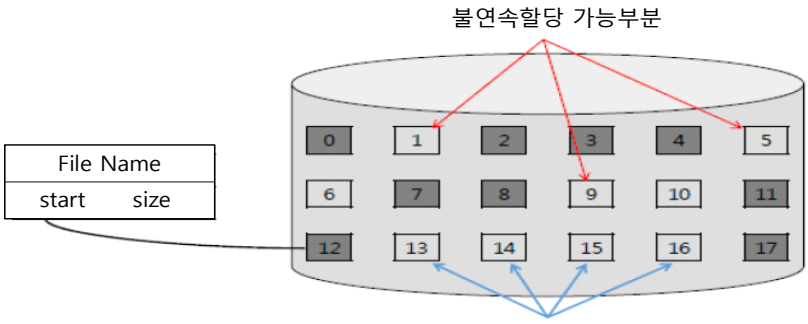
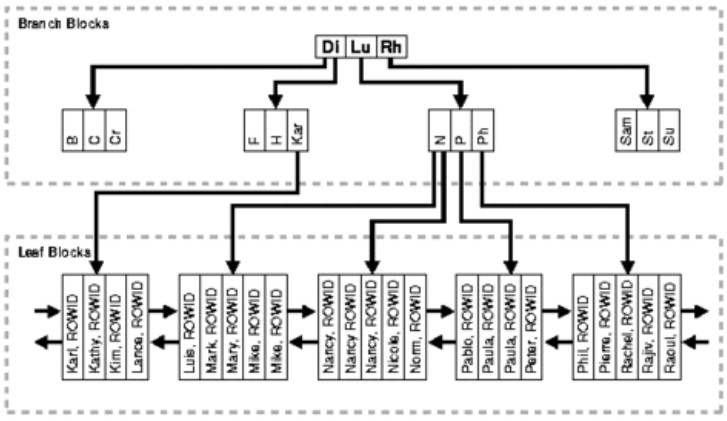
엔트로피 지수(Entropy Index)	$I_H = -\sum_{j=1}^{c} p_j log_2(p_j)$	- 모델 예측 값과 실제 값 간의 절대오차의 평균 - 부모 노드의 평균 절대오차를 가장 많이 감소시키는 설명변수와 분리 값을 기준으로 자식 노드를 생성 - MAE가 작을수록 오차가 적은 좋은 모델

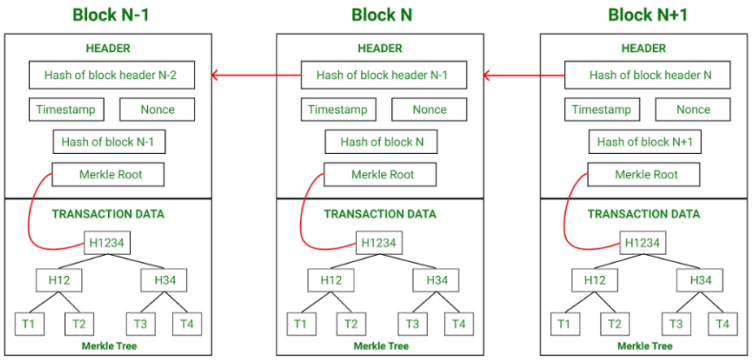
- c: 클래스의 개수, *Pj*: 전체 데이터 중 특정 클래스가 포함되어 있는 확률

"끝"

02	파일, 데이터베이스, 블록체인의 저장 측면 비교		
문제	데이터저장 측면에서 파일, 데이터베이스, 블록체인을 비교하시오.		
도메인	디지털 서비스	난이도	상 (상/중/하)
키워드	연속 할당 (Contiguous Allocation), 불연속 할당 (Non-Contiguous Allocation), B-Tree, 머클 트리 (Merkle tree), 데이터 공유, 데이터 중복, 비가역성		
출제배경	블록체인의 저장 관점의 활용 다양화에 따라 기존의 파일 시스템과 데이터베이스와 차이점 인지 확인		
참고문헌	IT기술사회 자료		
출제자	단합반 안경환 기술사(제 110회 정보관리기술사 / akh.itpe@gmail.com)		

I. 데이터의 저장 방식. 파일, 데이터베이스, 블록체인의 저장 측면 개념 비교

비교 대상	아키텍처	정의
파일		- 컴퓨터에서 파일이나 자료를 쉽게 발견 및 접근할 수 있도록 보관 또는 조직하는 체제
데이터베이스		- 여러 사람이 공유하여 사용할 목적으로 체계화해 통합, 관리하는 데이터의 집합

블록체인		- 트랜잭션을 기록하고, 자산을 추적하고, 신뢰를 구축하기 위한 불변 공유 원장

II. 데이터의 저장 방식. 파일, 데이터베이스, 블록체인의 저장 측면의 구조 비교

비교 항목	파일	데이터베이스	블록체인
저장 구조	- 컴퓨터에서 파일이나 자료를 쉽게 발견 및 접근할 수 있도록 보관 또는 조직하는 체제	- 이진 트리를 확장해 하나의 노드가 가질 수 있는 자식 노드의 최대 숫자가 2보다 큰 B-Tree 구조	- 모든 자식 노드들이 암호학적 해시로 이뤄진 데이터 블록을 갖는 트리 형태의 자료구조인 머클 트리
인프라 유형	- Local 구조	- 서버 클라이언트 구조	- 분산 저장 시스템
구성 요소	- 블록(Block), 데이터블록(DataBlock)	- Root, 브랜치(Branch), 리프(Leaf) 노드	- 모든 자식 노드들이 암호학적 해시로 이뤄진 데이터 블록을 갖는 트리 형태의 자료구조인 머클 트리
종류	- FAT32, NTFS, EXT, EXT2, EXT4, XFS, NFS	- MySQL, Oracle, MS-SQL 등	- 비트코인(bitcoin) - 이더리움(ethereum)
저장 데이터의 접근 제어	- 파일 또는 디렉토리 단위로 접근 권한 설정 - Linux의 경우 Owner, Group, Other로 읽기, 쓰기, 실행 단위 권한 제어	- 데이터베이스의 소유자와 접근 정책에 따라 접근 가능	- 블록체인 유형에 의존적 - Private의 경우 사전에 허가받은 참여자만 접근 가능하지만, Public형의 경우 누구나 참여 가능
저장 데이터 소유 및 관리 주체	- 파일 저장장치 소유자 - 파일시스템 소유자가 운영체제 통해서 관리	- 개인 혹은 기업 소유로 단일 관리자 존재 - 데이터베이스 관리자가 데이터베이스 엔진을 통해 관리	- 관리자가 여러 명이 존재하며 각자 원장의 사본을 보유하고 관리
데이터 처리 속도	- 매우 빠름	- 실제 하드디스크에 쓰는 시간과 데이터베이스의 처리 시간이 존재하나 상대적으로 빠름	- 합의 알고리즘을 위해 상대적으로 긴 시간이 필요

III. 데이터의 저장 방식. 파일, 데이터베이스, 블록체인의 저장 측면의 생성과 삭제 비교

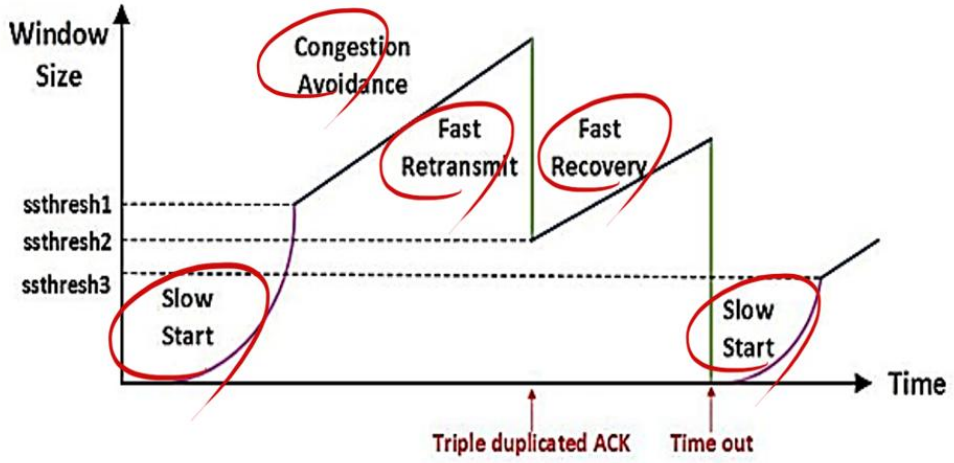
비교 항목	파일	데이터베이스	블록체인
저장 단위	- 파일 단위	- 컬럼(column), 테이블(table) 단위	- 원장에 저장 - 블록(block) 단위
데이터 생성 방식	- 파일 시스템 드라이버 통해 API 형식으로 지원 - 파일 시스템이 물리적 장치(device)의 유형을 지원 여부에 따라 생성	- DDL 언어를 이용하여 생성된 테이블에 DML 언어를 이용하여 insert query 통해 생성	- 합의 알고리즘(consensus algorithm)을 통해 노드 참여자의 승인하에 데이터 생성 후 연결 방식
저장 데이터의 공유	- 기본적으로 공유 미지원 - NFS(Network File System)으로 공유는 가능하나 매우 제한적	- 데이터베이스는 데이터를 여러 사용자에게 공유하기 위한 목적으로 사용	- 노드에 참여한 참여자는 공유된 정보를 자신의 체인에 추가함으로써 공유
생성 블록의 크기	- 운영체제와 파일시스템에 의존적 - 32bit Windows의 경우 최대 약 4G까지 가능	- 데이터베이스에 따라 의존적 - MySQL의 경우 LONGTEXT 유형으로 약 4G 가능	- 각 블록 체인에 의존적 - 비트코인(bit-coin)의 경우 약 1Mb로 제한, 이더리움은 평균적으로 20Kb에서 30Kb이며 최대 1Mb 가능
트랜잭션 처리	- 별도의 트랜잭션 미지원 - 저장 중 실패 발생 시 데이터 전체 손실	- 원자성(Atrocity), 일관성(Consistency), 고립성(Isolation), 지속성(Continuous) 보장	- 합의 알고리즘을 통해 트랜잭션이 처리되며 합의가 이뤄진 것만 원장에 저장
데이터 중복	- 중복으로 저장되지 않고 단일 데이터로 저장	- 데이터의 중복을 허용하지 않으나, 역정규화를 통해 일부 중복 허용	- 하나의 데이터가 여러 참여자에게 중복되어 저장 - 하나의 노드에는 데이터 중복이 최소가 되도록 저장
저장된 데이터의 공격	- 악의적 공격으로부터 접근 제어를 통해 일부 방어 가능	- 데이터베이스의 접근제어 정책을 통해 일부 방어 가능	- 악의적 데이터 조작 시도는 51% 공격을 통해 가능하며, 이 또한 다양한 방법으로 차단되어 현재는 사실상 불가능
데이터 삭제	- 파일 또는 디렉토리 단위 삭제 가능	- 테이블, 레코드 단위 삭제 가능	- 비가역성으로 인해 삭제 불가능 - 삭제가 필요한 경우 삭제가 되었다는 항목을 추가하여 삭제
데이터 복구	- 손실된 데이터는 일반적으로 복구가 곤란	- 장애 발생한 경우 데이터베이스 회복 메커니즘을 통해 데	- 손실된 데이터의 경우 복구가 불가능한 경우 발생

	- RAID 등의 부가적 구성을 통해 복구 가능	이터 복구 - 일부 데이터 손실 가능	- 비트코인 지갑 분실, 손상 발생 시 복구 난해

"끝"

03	TCP(Transmission Control Protocol)		
문제	TCP(Transmission Control Protocol)는 네트워크에 혼잡(Congestion)이 발생한 경우 이를 해소하기 위한 다양한 메커니즘을 사용한다. 이와 관련하여 아래 사항들에 대해 설명하시오. 1) TCP 혼잡제어 메커니즘의 구성요소 2) 혼잡상황 감지 3) 혼잡상황 제어 4) 혼잡 윈도우 크기		
도메인	네트워크	난이도	상 (상/중/하)
키워드	Slow Start, Congestion Avoidance, Fast Retransmit, Fast Recovery		
출제배경	최근 TCP 프로토콜에 대한 실전 문제가 빈번하게 출제되고 있으며, 그에 따른 TCP 심화 내용에 대한 이해 필요		
참고문헌	IT기술사회 자료		
출제자	TOP반 김민 기술사(제 120회 정보관리기술사 / itpe.min@naver.com)		

I. TCP 혼잡제어 메커니즘의 구성요소

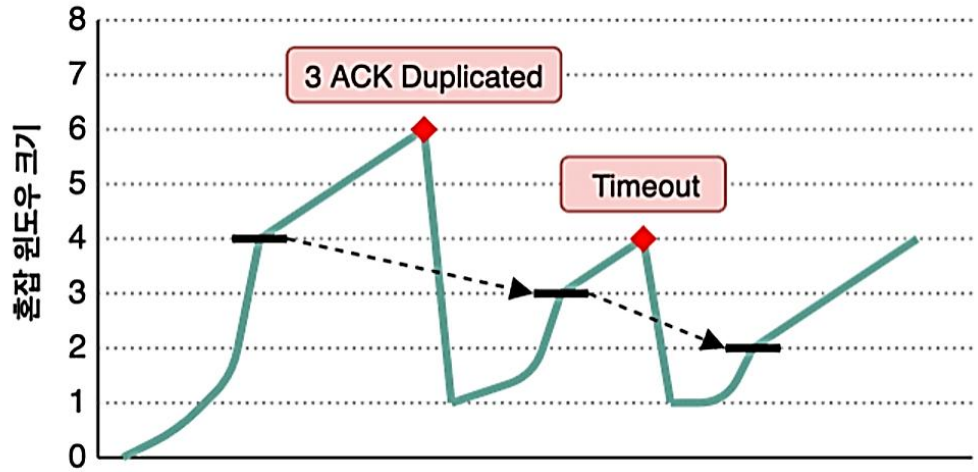
구분	상세 내용	
개념도		
정의	- 네트워크로 유입되는 사용자 트래픽의 양이 네트워크 용량을 초과하지 않도록 유지시키는 메커니즘	
TCP 혼잡제어 기본 메커니즘 구성요소	Slow Start	- 혼잡 윈도우를 한계치에 도달할 때까지 지수적으로 증가시키는 방법
	Congestion Avoidance	- 혼잡 윈도우의 크기를 혼잡 상태가 감지될 때까지 하나씩 증가시키는 방법
	Fast Retransmit	- 송신 측에서 Duplicate ACK를 받게 되면 패킷 손실로 간주하고 즉시 재전송
	Fast Recovery	- Fast Retransmit 후 Slow Start 아닌 Congestion Avoidance 상태에서 전송하는 기법

II. 혼잡상황 감지

구분	핵심 기술	설명
임계초과	- Timeout	- 송신지로부터 수신지까지 일정 시간내에 패킷이 도달하지 않아 최대 대기시간을 초과한 상황 - 패킷 유실로 혼잡상황 감지로 판단
중복 ACK	- 3 Duplicate ACK	- 송신지로부터 수신지까지 동일 패킷에 대하여 ACK를 3번 피드백 받은 상황 - 다른 패킷은 정상 전송되었으나 특정 패킷만 전달받지 못하는 경우 - Timeout 상황보다 3 Duplicate ACK이 혼잡도 높음

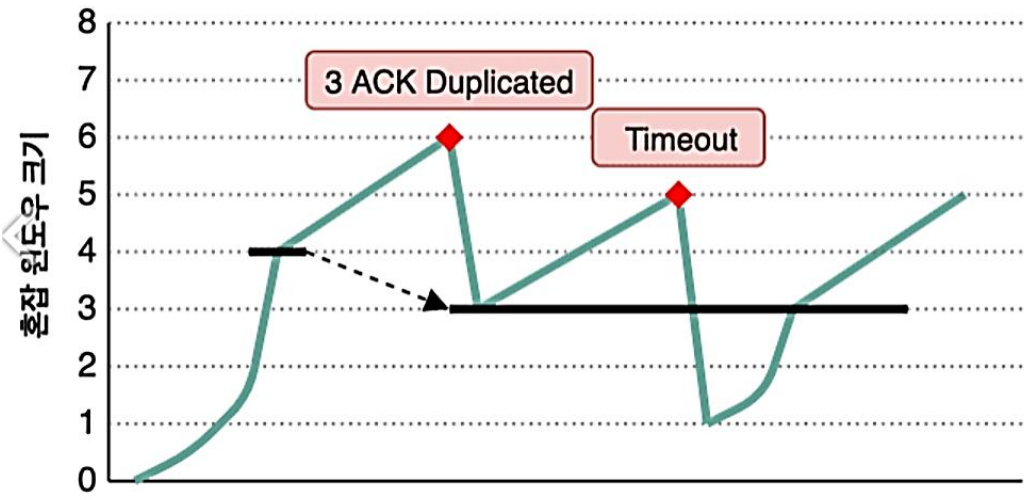
III. 혼잡상황 제어

가. TCP-Tahoe 기법 상세 설명

항목	상세 설명
동작 그래프	
동작 방식	- Slow Start → Congestion Avoidance → Fast Retransmit
동작 순서	- 3 Duplicate ACK 수신 시 즉시 재전송 ϒ 재 전송 - 시간 대기 미 수행하여 TCP 성능 향상(SS + CA 경우, 재전송 시간 만료 후 재전송) ① 재전송 직후 ssthresh = 1/2 Window 설정 ② Window 크기 1 MSS로 설정하고 SS로 천이
장점	- 패킷손실이 발생하지 않아 안전성 높음
단점	- 한 윈도우 내에 처음 발생한 손실된 패킷을 재전송한 후 차례로 slow start를 실행하면서 이후의 모든 패킷들을 재전송하므로 수신기가 이미 수신한 패킷을 다시 수신

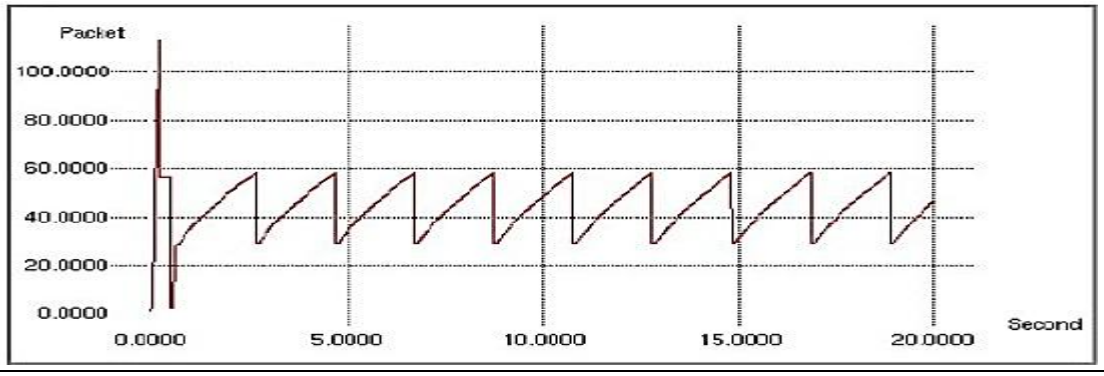
- ssthresh(slow start threshold): slow start 임계점
- cwnd(congestion window size): 혼잡 윈도우 크기

나. TCP-Reno 기법 상세 설명

항목	상세 설명
동작 그래프	
동작 방식	- Slow Start → Congestion Avoidance → Fast Recovery
동작 순서	- 3 Duplicate ACK 수신 시 즉시 재전송 ① 재 전송 후 ssthresh = 1/2 Window + 3 (ACK) ② cwnd = ssthresh 설정, ACK 수신 시 CA 천이
장점	- 한 윈도우 내에 하나의 패킷 손실이 발생한 경우에 가장 좋은 성능
단점	- 두 개 이상의 패킷 손실이 발생하면 첫 번째 패킷을 재전송하고 두 번째 패킷에 대한 Duplicate ACK 3개의 수신가능성이 적어지므로 타임아웃이 발생할 확률이 높아 Tahoe보다 성능이 낮음

- TCP Reno, TCP Tahoe에서는 패킷 손실이 발생할 때까지 창 크기가 계속 증가하고, 패킷 손실 시 인해 창 크기가 조절되면 연결 처리량이 저하
- 네트워크에서 패킷 손실이 발생하지 않도록 창 크기를 적절하게 제어하면 제한 창으로 인한 처리량 저하를 피할 수 있는 TCP Vegas 기법이 탄생

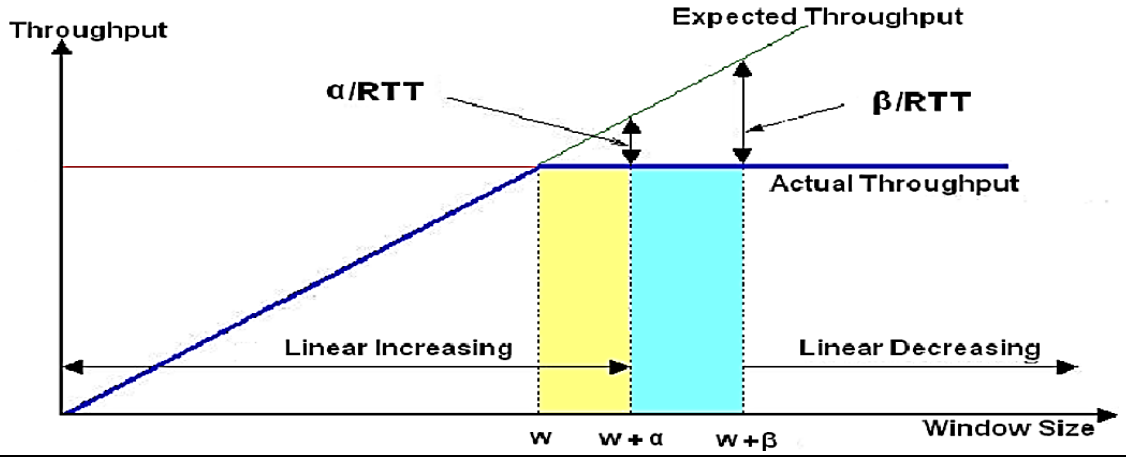
다. Reno 기법의 단점 보완, TCP-NewReno 제어 기법 설명

항목	상세 설명
동작 그래프	
TCP-Reno의 문제점	- 패킷 loss는 연속적으로 일어나는 경향이 매우 강함 - 따라서 연속적인 loss(중복 ack) 발생 시 window size를 계속해서 절반으로 줄이는 사태가 발생, 예를 들어 loss가 3번 연속으로 발생하면 window size는 기존 size의 1/8이 되어버리

	는 문제가 발생 - 위 문제를 해결하기 위해서 TCP Reno의 fast recovery방식을 개선한 방식이 TCP NewReno
동작 순서	1. 패킷 loss(중복 ACK)를 감지 2. fast recovery 상태에 들어감(window size는 절반이 됨) 3. 지금까지 보냈던 패킷들에 대한 ACK가 모두 도착할 때까지 fast recovery상태를 미 종료 4. 마지막에 보냈던 패킷에 대한 ACK가 오기 전에 패킷 loss가 한번 더 감지 5. window size는 절반이 되지않고 현재의 fast recovery 상태를 유지

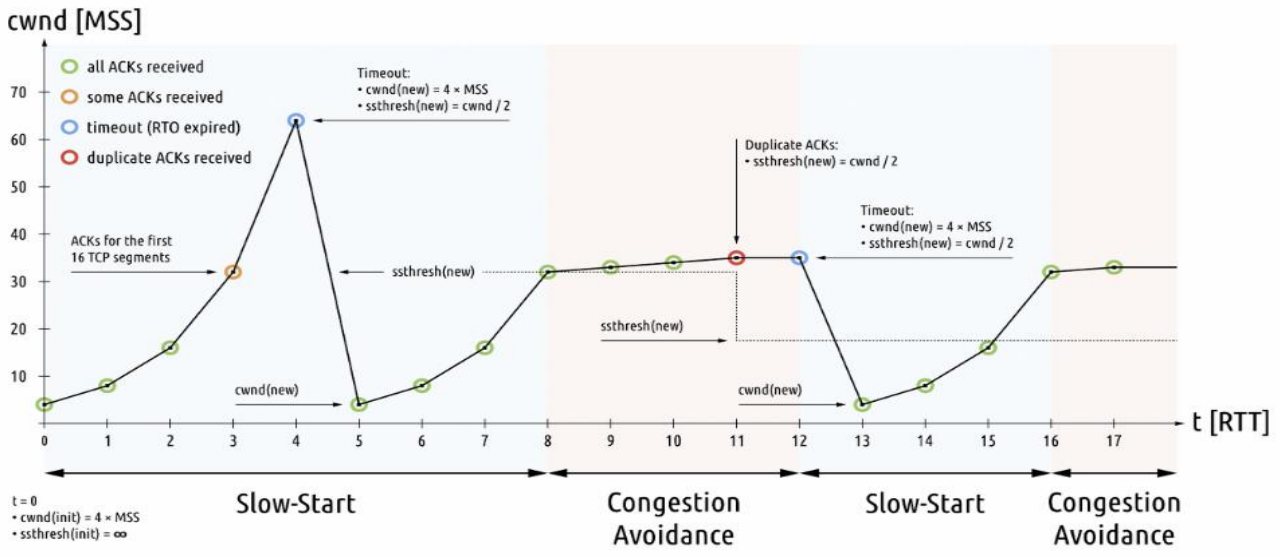
- 네트워크에서 패킷 손실이 발생하지 않도록 창 크기를 적절하게 제어하면 제한 창으로 인한 처리량 저하를 피할 수 있는 TCP Vegas 기법이 탄생

라. 창 크기를 적절한 값으로 수렴하는 TCP Vegas 제어 기법

항목	상세 설명
동작 그래프	
동작 방식	- Slow Start → Congestion Avoidance
동작 순서	- TCP Vegas는 보낸 호스트가 이전에 보낸 패킷의 RTT(왕복시간)를 관찰하여 창 크기 제어 - 관찰된 RTT가 커지면 TCP Vegas는 네트워크가 정체되기 시작함을 인식 후 창 크기를 조절하고, RTT가 작아지면 TCP Vegas의 발신자 호스트는 네트워크가 혼잡에서 해소되었다고 판단하고 창 크기를 다시 늘림 - 따라서 이상적인 상황에서 창 크기는 적절한 값으로 수렴

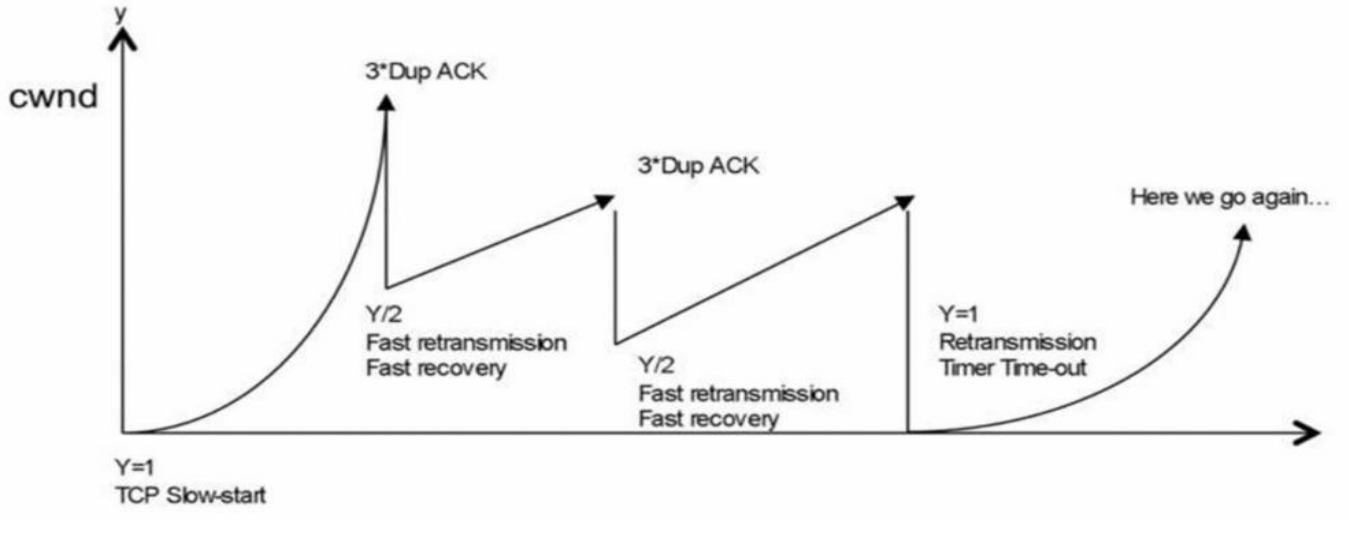
IV. 혼잡 윈도우 크기

가. Slow-Start, Congestion Avoidance 혼잡 윈도우 크기



구분	혼잡 윈도우 크기	설명
Slow-Start	- 1부터 2의 배수로 증가	- 처음에 한개씩 혼잡 윈도우의 디폴트 사이즈인 1 MSS로 패킷을 보내고 ACK 패킷 받으면 배로 증가하는 방식 - 타임 아웃 문제가 생긴다면 디폴트 사이즈로 회귀
Congestion Avoidance	- 임계점(ssthresh)부터 1씩 증가 - 타임아웃 문제 발생시 1/2로 변경	- 임계점(ssthresh)을 정하고 이때부터는 1개씩 증가하는 방식 - 타임 아웃 문제가 생긴다면 디폴트 사이즈로 돌아가며 임계점 사이즈의 1/2로 변경

나. Fast Retransmit, Fast Recovery 혼잡 윈도우 크기

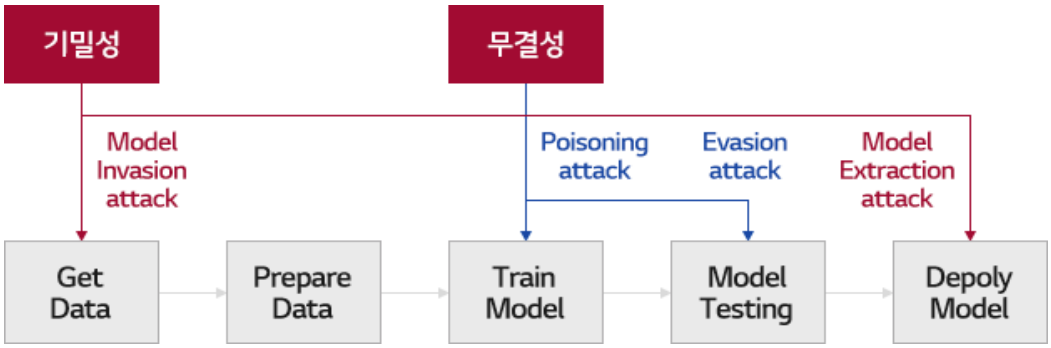


구분	혼잡 윈도우 크기	설명
Fast Retransmit	- 타임아웃 문제 발생시 1/2로 변경	- 3 Duplicate ACK 문제가 생긴다면 송신측은 즉시 패킷을 재전송하는 방식 - 혼잡한 상황이라 판단하고 혼잡 윈도우 사이즈는 디폴트 사이즈로 돌아가며 임계점은 해당 시점의 혼잡 윈도의 사이즈의 1/2로 변경
Fast Recovery	- 해당 시점의 혼잡 윈도우 사이즈의 1/2로 돌아간 후 ACK 패킷을 받으면 1개씩 증가	- 빠른 재전송과 유사하지만 3 Duplicate ACK 문제가 생긴다면 디폴트 사이즈로 돌아가지 않고 해당 시점의 혼잡 윈도우 사이즈의 1/2로 돌아간 후 ACK 패킷을 받으면 1개씩 증가하는 방식

"끝"

04	인공지능 보안위협		
문제	최근 인공지능 기술 활용이 증가하면서 다양한 보안 위협이 증가하고 있다. 이와 관련하여 아래 사항들에 대하여 설명하시오. 1) 머신러닝 학습과정에서의 적대적 공격 4가지와 방어기법 2) 생성형 언어모델 기반의 인공지능 기술 활용 시 발생할 수 있는 보안취약점		
도메인	인공지능(AI)	난이도	중 (상/중/하)
키워드	Poisoning attack, Evasion attack, Inversion attack, Model extraction attack Defense-GAN, 적대적 훈련(Adversarial training), 결과값 분석 차단, 쿼리 횟수 제한		
출제배경	최근 ChatGPT와 같은 생성형 언어모델 기반의 인공지능 활성화에 따른 보안취약점 출제		
참고문헌	IT기술사회 자료 ChatGPT 보안 위협과 시사점(한국인터넷진흥원, 2023)		
출제자	TOP반 김민 기술사(제 120회 정보관리기술사 / itpe.min@naver.com)		

I. 머신러닝의 적대적 공격 개요

정의	러닝의 심층신경망을 이용한 모델에 적대적 교란(Adversarial Perturbation)을 적용하여 오분류를 발생시키는 공격기술
유형	

- 적대적 공격은 AI를 활용하고 있는 다양한 분야에 위협이 되고 있음. 머신러닝 학습 과정에서 악의적인 학습 데이터를 주입해 머신러닝 모델을 망가뜨리는 중독 공격(Poisoning attack), 머신러닝 모델의 추론 과정에서 데이터를 교란해 머신러닝을 속이는 회피 공격(Evasion attack), 역공학을 이용해 머신러닝 모델이나 학습 데이터를 탈취하는 모델 추출 공격(Model extraction attack)과 학습 데이터 추출 공격(Inversion attack)이 있음.

II. 머신러닝 학습과정에서의 적대적 공격 4가지와 방어기법

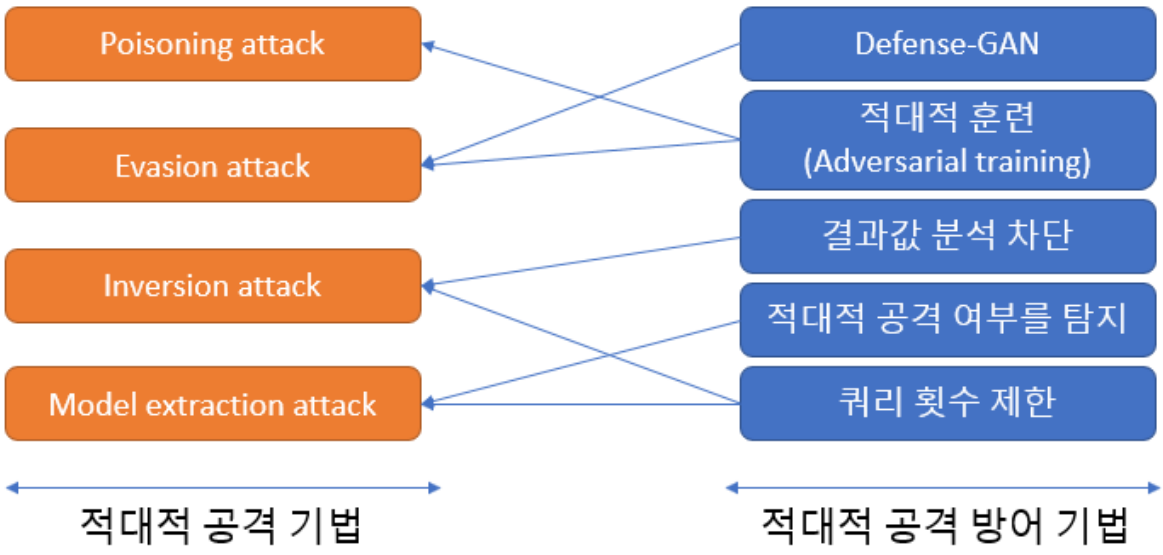
가. 머신러닝 학습과정에서의 적대적 공격 4가지

공격 기법	설명	사례
Poisoning attack (중독 공격, 오염 공격)	- 의도적으로 악의적인 학습 데이터를 주입해 머신러닝 모델을 망가뜨리는 공격 - 모델 자체를 공격해서 모델에게 영향 - 악의적인 데이터를 최소한으로 주입해 모델의 성능을 크게 떨어뜨리는 것이 공격의 평가 기준이 됨	- 마이크로소프트 사의 인공지능 채팅봇 '테이' - 스캐터랩 '이루다' - 의료 기계를 대상으로 한 연구 결과에서 대상 장비의 오작동 발생

Evasion attack (회피 공격)	- 입력 데이터에 최소한의 변조를 가해 머신러닝을 속이는 기법 - 이미지 분류 머신러닝인 경우, 사람의 눈으로는 식별하기 어려운 방식으로 이미지를 변조해 머신러닝 이미지 분류 모델이 착오를 일으키게 만드는 수법 - 적대적 스티커(Adversarial patch)는 쉽게 인쇄해 사용할 수 있고 악의적인 공격인지 쉽게 발견하기 어려워, 악용되는 경우 큰 위험을 가져올 수도 있음	- 도로 교통 표지판에 이미지 스티커를 부착해 자율주행 자동차의 표지판 인식 모듈을 교란 (자율주행차가 '정지' 표시를 '속도제한' 표시로 오인식)
Inversion attack (전도 공격, 학습 데이터 추출 공격)	- 머신러닝 모델에 수많은 쿼리를 던진 후, 산출된 결과값을 분석해 모델 학습을 위해 사용된 데이터를 추출하는 공격 - 데이터 분류를 위한 머신러닝은 주어진 입력에 대한 분류 결과와 신뢰도를 함께 출력하게 되는데, 이때 출력된 결괏값을 분석해 학습 과정에서 주입된 데이터를 복원하는 방식	- 얼굴인식 머신러닝 모델의 학습을 위해 사용한 얼굴 이미지 데이터를 복원 가능 - 머신러닝 모델을 훈련시키는 학습 데이터 안에 군사적으로 중요한 기밀정보나 개인정보, 민감정보 등이 포함되어 있는 경우라면, Inversion Attack을 이용한 공격에 의해 유출될 가능성이 존재
Model extraction attack (모델 추출 공격)	- 머신러닝 모델을 추출하는 공격 - 머신러닝 모델에 쿼리를 계속 던지면서 결과값을 분석하는 방식의 공격 - 유료 머신러닝 모델 서비스(MLaaS: Machine Learning as a Service)를 탈취하거나, Inversion attack, Evasion attack과 같은 2차 공격에 활용하기 위해 사용될 수 있음.	- 70초 동안 650번 쿼리만으로도 아마존 머신러닝 모델과 유사한 모델을 만들어 내는 것이 가능하다는 연구 결과가 발표

- 적대적 공격 기법의 대상과 각각의 특징에 따른 대응 방안이 지속적으로 연구되고 있음.

나. 머신러닝 학습과정에서의 적대적 공격 방어기법



방어 기법	설명
Defense-GAN	- 적대적 생성 신경망(GAN) 알고리즘을 이용하여 적대적 공격 방어 - 적대적 예제(Adversary Example)를 추가 학습 데이터로 활용하는 아이디어로 시작하여 변조된 이미지가 정상적인 이미지로 판단되도록 하는 것이 최종 목표
적대적 훈련(Adversarial training)	- 가능한 모든 적대적 사례를 학습 데이터에 포함해 머신러닝을 훈련시키는 방법 - 머신러닝을 훈련시키는 단계에서 예상 가능한 해킹된 데이터를 충분히 입력해 머신러닝의 저항성을 기르는 방식
결과값 분석 차단	- 학습모델의 결과값 분석을 통해 모델을 추론하는 방식의 공격을 차단하기 위해, 학습모델의 결과값이 노출되지 않도록 하거나, 결과값을 분석할 수 없게 변환하는 방식으로 공격을 차단
적대적 공격 여부를 탐지	- 원래의 모델과 별도로 적대적 공격 여부를 판단하기 위한 모델을 추가한 후, 두 모델의 추론 결과를 비교해 두 결과 간에 큰 차이가 발생하는 경우 적대적 공격으로 탐지하는 방식
쿼리 횟수 제한	- 모델에 반복적인 쿼리를 시도하는 Inversion attack이나 Model extraction attack을 방어하기 위해서 모델에 대한 쿼리 횟수를 제한하는 방식 - 학습 데이터에 포함된 기밀정보, 민감정보가 노출되지 않도록 암호화 등의 비식별 처리 방식도 연구

- 인공지능에 모든 프로세스를 전적으로 의지하는 것보다는 인간의 검증 단계를 통해 데이터가 오염되지 않았는지, 모델이 오작동하고 있는지 등 모니터링하고 점검하는 것이 필요.

III. 생성형 언어모델 기반의 인공지능 기술 활용 시 발생할 수 있는 보안취약점

보안 취약점	보안 취약점 상세	설명
피싱 메일 및 악성 코드 생성	- 생성형 언어모델의 결과물을 사이버 공격에 활용	- 대량의 피싱 메일 작성 및 언어적 한계 해소
	- 악성코드 생성 테스트	- 문서파일을 암호화하여 랜섬웨어 생성 - 국내 유명 포털사이트 사칭하여 계정정보 탈취 악성코드 생성 - CCTV 취약점 분석 및 공격 코드 생성
	- 텍스트, 소스코드 빠른 분석 및 지식 습득	- 보안 취약점이나 특정 포인트 검색 시간 단축 - 공격 사례, 기법 해킹 활용 정보 습득 가능
민감정보 유출과 결과물 오남용	- 무분별한 데이터 입력으로 인한 민감정보 유출 가능성	- 생성형 언어모델 서버 저장되는 회사의 기밀 유출 - 입력 데이터의 모델 개선 활용에 따른 보안 위협
	- 잘못된 결과물의 생산 및 활용	- 잘못된 정보의 오용 및 확산 가능성 - 보안 조치 없는 소스 코드 생성
인공지능에 대한 공격	- 인공지능에 대한 고유의 보안 위협 존재	- 악의적인 학습데이터 주입, 결과물 품질 저하 - 입력 데이터 변조, 복원, 모델 복제 공격

IV. 생성형 언어모델 기반의 인공지능 기술 활용 시 발생할 수 있는 보안취약점 대응방안

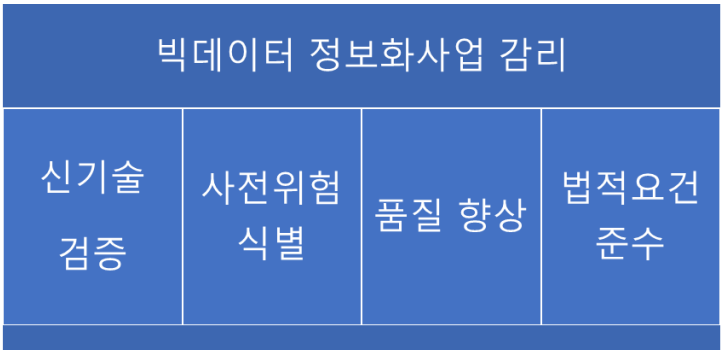
구분	대응방안	설명
대응	- 악용에 대한 선제적 대응	- 이메일 필터링 및 탐지 시스템 개선 - 생성형 언어모델로 생성 가능한 악성코드 지속적 테스트 및 위협수준 분석 - 생성형 언어모델의 결과물 식별 기술 개발 - 새로운 악용 사례의 즉각 대응할 수 있는 기반
활용	- 안전한 활용 및 도입 촉진	- 대국민 홍보, 교육, 안전 활용지침 마련 배포 - 기업의 생성형 언어모델 안전 도입 부작용 완화, 관련 보안사고 정보 공유, 간담회 개최
정책	- 인공지능 보안 정책 마련	- 인공지능 보안의 구체적인 방향성 확립 - 인공지능 모델 서비스 전과정 보안 프레임워크 필요 - 사용자의 권리 보호, 잠재적 위협 완화, 역기능 완화 정책 마련 시급 - 선진 국가 공동연구, 전문인력 양성, 국가 인공지능 기반 강화를 위한 노력 필요

"끝"

05	빅데이터 정보화사업 감리 점검가이드		
문제	인공지능 등 지능정보 기술에 비현실적인 감리기준을 해결하기 위해 지능정보기술 감리 실무 가이드(한국지능정보사회진흥원, 2023년)를 발간했다. 그 중 빅데이터 정보화 사업의 분석, 설계 단계별, 영역별 점검 항목에 대하여 설명하시오		
도메인	SW공학	난이도	상 (상/중/하)
키워드	시스템 구조, 응용시스템, 데이터베이스		
출제배경	지능정보 기술 발전에 따른 최신 감리 가이드 내용 출제		
참고문헌	IT기술사회 자료 https://www.nia.or.kr/site/nia_kor/ex/bbs/View.do?cbIdx=99860&bcIdx=25211 지능정보기술_감리_실무가이드(2023.2).pdf		
출제자	NS반 김민재 기술사(제 124회 정보관리기술사 / kmj_pe@naver.com)		

I. ICT신기술 검증과 사전위험을 식별하기 위한 빅데이터 정보화사업 감리의 개요

가. 빅데이터 정보화사업 감리 목적



- 빅데이터를 적용하는 사업에서도 타당성을 검증하고, 사전위험을 식별하여 품질을 향상시키는 것이 목적

나. 빅데이터 정보화사업 감리의 관련 근거

구분	관련 근거	주요 내용
법령	- 전자정부법 제57조 - 전자정부법 시행령 제71조	- 행정기관 등의 장은 정보시스템의 특성 및 사업규모 등이 일정 기준에 해당하는 정보시스템에 대하여 감리를 시행
고시	- 정보시스템 감리기준	- 정보시스템 감리 업무범위, 절차 및 준수사항 등 감리를 하기 위해 필요한 사항 등을 정함
가이드	- 정보시스템 감리발주 관리 가이드	- 정보시스템 감리용역을 효율적으로 발주하고 감리하기 위해 기획단계부터 종료단계까지 각 단계별 활동을 정의
	- 정보시스템 감리 수행 가이드	- 감리절차, 수행방법과 표준 점검항목, 계획서 및 보고서 등의 서식을 참고하기 위한 가이드
	- 정보시스템 감리점검 가이드	- 정보시스템 유형별로 감리점검 가이드를 제공

- 빅데이터 정보화사업 감리는 준거성을 기반으로 분석, 설계, 구축, 운영의 각 단계별로 점검을 수행

II. 분석단계 감리 점검 개요

가. 분석단계 감리 주요 점검 내용

- 빅데이터 시스템이 가져야 하는 데이터의 분석, 시각화, 사용자 인터페이스에 대한 요구사항이 제대로 정의되고 도출되었는지를 점검
- 시스템의 목표와 이를 달성하기 위한 필요 데이터의 정의를 점검하고, 분석을 위한 항목과 과정에 대해 점검
- 사용자의 활용을 위한 사용자 인터페이스와 시각화 유형과 도구에 대해서 점검
- 분석시스템의 기능, 성능, 품질에 대한 요구사항 정의에 대해 점검

나. 분석단계 상세 점검 항목

영역	항목구분	점검항목	주요 검토사항
응용 시스템	빅데이터 서비스 요구사항 정의 여부	- 사업의 목표와 구현 방안 등 사업 전반을 이해하고 있는가?	- 사업계획서, RFP 등에 제시된 목표 및 추진전략에 대한 이해 - 독립사업 또는 연도별 확산사업 여부에 따라서 데이터 확보 문제 - 편의성 높은 분석기술 제공 여부 - 시각화 기술의 제공 여부
		- 분석 목표 달성을 위한 분석항목을 정의했는가?	- 분석항목 정의 - 분석항목 간 상관관계 정의 - 분석결과의 품질 수준을 정의
		- 분석가 및 사용자 인터페이스 요구사항은 정의되었는가?	- 분석 과정 및 분석 결과 활용을 위한 사용자 인터페이스에 대한 요구사항 정의
		- 시각화 유형을 확인하고 적합한 도구를 선정하였는가?	- 데스크탑 어플리케이션, 웹 어플리케이션, 모바일 어플리케이션 등 의사결정 - 시각화 유형에 대한 구체적 검토 - 시각화 도구의 작동환경과 요구기능에 대한 분석 여부
		- 분석시스템의 운영과 관리를 위한 기능 요구사항이 도출되었는가?	- 분석시스템의 운영과 관리 요구사항분석 - 필요 운영 인력, 조직, 운영/관리프로세스, 운영 관리 시스템 요구사항 등
		- 빅데이터 분석 시스템의 기능과 성능 및 품질에 대한 요구사항을 정의하였는가?	- 빅데이터 수집, 정제, 범위 선택과 분석모델 - 분석모델의 학습 관련 - 시각화와 리포팅 관련 데이터 품질관리 절차 및 기준의 구체화 여부
데이터	빅데이터 데이터셋 수집 가능성 및 사용	- 분석 목표와 항목에 적합한 데이터에 대한 요구사항을 정의	- 데이터 종류, 양, 보관 방식, 수집 주기와 분석 주기 - 백업과 이중화 등 윈시데이터에 대한 요구사항 분석 - 수집 데이터 소스, 확보 비용, 데이터 이관 절차 등 조

	성 분석 여부	하였는가?	사 및 설계 반영
		- 빅데이터 구축을 위한 원시 데이터를 확보하였는가?	- 데이터 요구사항에 따라 원시 데이터가 확보 여부 - 확보되지 않은 원시 데이터에 대한 처리 방법의 확인 - 원시데이터 확보 가능성 판단 자료
		- 확보된 원시 데이터가 분석 목표 달성에 타당한가?	- 데이터가 분석 활용 목표에 부합되는 지 타당성 검토 - 요구사항 달성을 위해 필요한 데이터 추가 - 확보된 데이터에 기반하여 요구사항 및 목표 수준 변경 검토
	빅데이터 및 데이터 셋을 활용한 서비스 여부	- 데이터 연계를 위한 기관 내외부 서비스 운영 환경을 이해하고 있는가?	- 내부 및 외부 데이터를 활용한 서비스 - 서비스 운영을 위한 기능과 사용환경에 대한 구축 요구사항 분석

- 분석단계에서는 빅데이터 및 빅데이터 셋에 대한 분석항목과 요구사항을 중점적으로 점검

III. 설계단계 점검 개요

가. 설계단계 감리 주요 점검 내용

- 분석단계에서 정의된 요구사항이 설계에 잘 반영이 되었는지를 점검
- 응용시스템 측면에서는 데이터의 수집, 저장, 분석, 시각화에 이르는 과정이 처리되고 있는지를 점검
데이터 측면에서는 데이터가 표준화가 정의되어 있는지와 데이터가 표준을 잘 준수하고 있는지를 점검
- 시스템 측면에서는 데이터의 수집, 저장, 분석, 시각화를 위한 구성과 아키텍처를 점검
- 외부 시스템과 연계를 위한 인터페이스와 접근제어, 보안 등의 설계를 점검

나. 설계단계 상세 점검 항목

영역	항목구분	점검항목	주요 검토사항
응용 시스템	데이터 수집·정제 체계의 적정 설계 여부	- 데이터 수집·정제 체계가 마련되었는가?	- 수집 대상 데이터의 목록의 작성 - 수집 대상 데이터 현황 정의 (보유기관, 담당자, 데이터 제공형식 등) - 데이터 수집 및 정제 체계
		- 수집 대상 데이터에 대한 적절한 처리방안이 마련되었나?	- 데이터에 포함된 개인정보의 유출 문제를 처리하기 위한 방안 수립 여부 - 오류 데이터 제거, 길이 체크, 날짜 포맷 점검 등 데이터 정제 과정 점검
	데이터 저장 체계의 적정 설계 여부	- 데이터 추출, 변환, 탑재 기능이 정상 동작하나?	- 데이터 품질관리 절차 및 기준 유무 - 개인정보 탐색· 및 처리방법의 구체화 확인 (비식별화, 암호화 등)

		- 데이터 보유기관에서 주기적으로 수집 가능한 연계가 적용되었는가?	- 데이터 보유기관별 연계방법 및 주기 확인
	데이터 분석모델 설계	- 분석대상 및 범위가 요구사항과 일치하는가?	- 요구사항별 분석대상과 범위 지정
		- 분석대상별 분석모델이 지정되었는가?	- 분석대상별로 분석모델의 지정 여부 확인 (분류모델, 지수모델, 예측모델 등) - 분석모델의 설계 타당성 검증 (도메인별 데이터 분석 전문가의 검증) - 분석 알고리즘 모델의 설계 여부
	데이터 시각화 설계	- 분석 결과가 잘 반영되었나?	- 분석 화면 구성 설계 - 데이터 분석 시각화 설계 - 서비스를 위한 기능 설계
데이터	데이터 표준화 및 융합	- 수집된 데이터의 속성(칼럼명, 문자형, 숫자형, 크기 및 길이, 필수 여부 등) 정의되어 있는가?	- 코드 표준화 관련 명명규칙 - 사전관리(단어, 용어, 도메인 등), 통합코드 등 - 표준 항목 정의/적용 및 관리 체계
		- 분석에 필요한 데이터 목록과 유형이 정의되고 변환기준이 정의되었는가?	- 분석에 필요한 데이터 목록 - 데이터별 유형 설계 - 데이터 수집 시의 규칙 정의 (유효성 검증방안)
		- 수집된 데이터는 구조를 통일하고 병합하는 표준화 과정을 거쳤는가?	- 데이터 정제 및 변환 기준 - 데이터 변환 기준 및 변환 절차
시스템	시스템간 연계 설계	- 외부데이터 수집을 위한 연계가 명확히 정의되어 있는가?	- 데이터 소스 연결 관리 - 데이터 송/수신 연계 - 실시간/배치 연계
		- 시스템 구성요소에 대한 상세설계가 충분하게 이루어졌는가?	- HW, SW(분리발주 SW 포함) 등 구성 - 시스템 구성요소 검증 방법 및 절차 - 문제 발생 시 복구 및 업무처리 계획
		- 시스템 구성 및 아키텍처에 사용자 요구사항이 적용되고 명세화 되었는가?	- 시스템 성능/가용성 - 동시 사용자 접속 처리 용량 - 명세화된 항목별 검증 및 확인 방법

		- 시스템의 보안, 접근 권한 정책이 설계되었는가?	- 데이터에 대한 접근/통제 설계 - 시스템간 접근/통제 설계 - 암호화 전송 등

- 설계단계에서는 데이터 수집 및 정제 체계, 추출 및 변환 기능, 표준화 과정, 데이터 연계 등을 중점 점검

IV. 기존 감리가이드와 빅데이터 감리가이드 점검항목 비교

단계	기존 감리가이드	빅데이터 감리가이드
분석	- 현행 시스템 운영환경 분석 - 시스템 관련 사용자 요구사항 도출 - 업무프로세스, 이벤트 모델링, 보안관련 분석의 적정성 등	- 분석목표 달성을 위한 항목 정의 - UI 요구사항 정의 여부 - 시각화 유형 및 도구 사용 적정성 - 품질에 대한 요구사항 정의 - 빅데이터 구축 위한 원시 데이터 확보 여부 등
설계	- 시스템의 구조적 설계와 구성요소 간 상세설계 수행 - 시스템 설치, 검증 및 전환계획 적정성 - 업무기능, UI 등 구현 적정성 - 데이터분산, 무결성, 성능을 고려한 설계	- 데이터 수집 및 정제 체계 마련 - 데이터 추출, 변환, 탑재 기능의 적정성 - 분석대상 및 범위의 요구사항 일치 여부와 분석결과 적정성 - 데이터 표준화 및 융합 - 시스템 구성 및 아키텍처에 사용자 요구사항 적용 및 명세화
구축	- 설계에 따른 시험 및 검증 수행 - 기능의 충분성, 완전성, 무결성, 적정성, 편의성 확보여부 - 단위기능에 대한 검증 및 데이터 정합성	- 데이터 생애주기 관리 - 데이터 수집 및 변환 적정성 - 시각화 - 분석 및 로그 저장 적정성

- 빅데이터 감리는 빅데이터 구축을 위한 요구사항 정의, 데이터 수집 및 전처리, 분석모델링 및 구현, 시각화, 검증의 각 단계에서 필요한 사항들이 적절하게 이행되고 있는지를 확인하는 것이 중요

"끝"

06	SLA(Service Level Agreement)		
문제	금융 클라우드 서비스를 받는 금융회사의 데이터는 가장 중요한 자산이며 민감정보를 다룬다. 금융 클라우드 SLA(Service Level Agreement)에 대하여 설명하시오. 1) SLA 개념 2) 클라우드 SLA 가이드 3) 금융 클라우드 SLA 가이드		
도메인	IT경영전략	난이도	상 (상/중/하)
키워드	SOW, SLO, SLM, SLR, 가동률, 금융분야 클라우드 특수성		
출제배경	금융 기업의 클라우드 도입에 따른 SLA 이해도 점검		
참고문헌	IT기술사회 자료 클라우드+SLA가이드+및+개인정보보호수칙+자료(10.5).pdf 금융보안원-금융분야_클라우드컴퓨팅서비스_이용_가이드-fn.pdf		
출제자	NS반 김민재 기술사(제 124회 정보관리기술사 / kmj_pe@naver.com)		

I. SLA(Service Level Agreement)의 개념

가. SLA의 정의

- 정보시스템 사용자와 공급자 사이의 상호 동의에 의하여 서비스 수준을 명시적으로 정의하고 이를 문서화한 약정서

나. SLA의 구성요소

구분	구성요소	설명
업무 목표	- 서비스 정의, 목적, 범위	- 공급자가 제공하는 서비스 상세 내용 정의
	- 기본계약서	- 공급자와 서비스 사용자 간의 상호 계약서
	- 서비스 카탈로그	- 제공하는 서비스의 내역과 특성을 기술한 문서
성과 지표	- SOW(Statement of Work)	- SLA의 상세 항목 업무 기술
	- SLO(Service Level Object)	- SLA 관리 지표 별 목표
	- SLM(Service Level Measurement)	- SLA 정량적 측정 방법
	- SLR(Service Level Report)	- SLA 보고 형식 및 방법
조정 절차	- 약정의 변경 절차	- SLA 계약 수준 변경 절차
	- 서비스 유효 기간	- SLA 계약의 수행 기간 갱신

다. SLA의 주요지표

구분	주요지표	설명
하드웨어	- 서비스 가동률	- 서비스 시간 동안 제공 가용성 목표 비율 - 서비스 가동률(%) = (1 - 장애시간/서비스시간) * 100
	- 동일 장애 발생률	- 기존 발생된 하드웨어 장애가 재발생된 비율 - 동일 장애 발생률(%) = (동일장애발생건수/총장애발생건수)*100

소프트웨어	- 오류 건수	- 소프트웨어 버그, 오작동 등 오류 발생 건수
	- SR 적기 처리율	- SR(Service Request)의 요청한 완료일 이내 서비스 제공 비율 - SR 적기 처리율(%) = (적기 처리된 SR건수/전체 SR건수) * 100
네트워크	- 네트워크 가동률	- 서비스 시간 동안 제공 네트워크 가용성 목표 비율 - 네트워크 가동률(%) = (1 - 장애시간/네트워크 가동시간) * 100
	- 네트워크 장애건수	- 스위치, 라우터 등의 문제로 발생된 장애건수
고객 만족도	- 고객 만족도 점수	- 정보시스템 사용자(고객) 만족도 점수(100점 만점)

- SLA 관리 성과를 높이기 위한 Penalty/Incentive, SIP, Annual Reset 관리체계 존재

II. 클라우드 SLA 가이드

가. 클라우드 SLA 가이드 개요

- SLA 작성 시 서비스 제공자와 이용자가 고려해야 할 서비스 항목 (가용성, 백업고객 지원 등)과 목표 수준을 제시한 지침서
- 클라우드 SLA 가이드를 통해 서비스의 수준이 명확히 제시되면, 이용자의 경우 클라우드에 대한 막연한 불안감을 해소하고, 서비스 업체의 경우 품질에 기반한 경쟁을 유도할 수 있을 것으로 기대

나. 클라우드 SLA 가이드 주요 내용

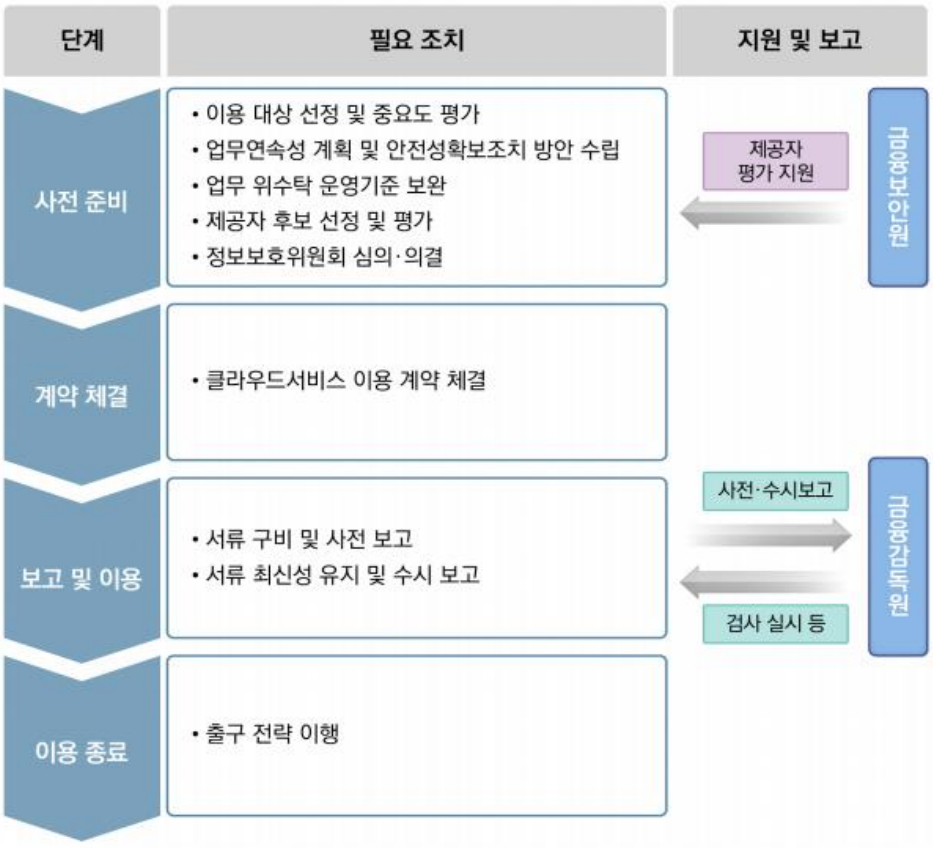
항목	설명
서비스 가용성	- 갑작스런 "클라우드 서비스 장애 로" 인해 서비스가 중단되는 우려를 최소화하기 위해, 서비스 가용성 기준 (99.5% 이상)을 제시 - 서비스 제공자가 통제하기 어려운 외부 N/W로 인한 장애는 제외하며 천재지변, 전쟁, 사변 그 밖의 불가 항력이나 이용자의 고의 또는 과실로 인하여 발생한 장애는 면책 - 가용성(%) = (클라우드 서비스에 접속이 가능한 시간 실제 (가동시간)/ 정해진 서비스 운영 시간 (예정 가동시간)) * 100 - 장애허용시간 월 3.6시간 이내 = 가용성 99.5% 이상
데이터 백업. 복구 및 보안	- 이용자의 데이터를 외부의 데이터 센터에 저장하는 만큼 데이터가 손상되거나 유실될 경우에 대비하여, 백업이 99% (계획 대비) 이상이 되도록 백업 준수율을 제시 - 실제 데이터가 손실될 경우 일정 시간 이내에 복구할 수 있도록 필요한 측정 항목들을 제시 - 백업준수율(%) = (실시된 백업건수 / 계획된 총 백업 건수) * 100 - 해킹악성 코드 감염 등 클라우드에서의 보안 위협에 대한 우려가 증가하고 있는 만큼 서비스 , 제공업체가 계약 시 보안 지침이나 인증 내역 예(. ISMS) 등을 사전에 제시하도록 하여 이용자의 신뢰를 높이도록 가이드
고객 지원	- 고객 지원에 대해서는 클라우드 서비스가 하드웨어소프트웨어 등 IT 자원을 빌려 쓰는 서비스이므로 상시적인 고객 지원이 중요한 만큼 서비스와 관련하여 고객 요청이 있는 경우 최대한 모든 요청을 조속히 처리하도록 제시 - 고객 요청 처리율 (99%이상), 서비스 요청 적기 처리율 (99% 이상) 등을 규정하여 고객 불만 등에 대한 처리 기준 제시

	- 고객요청처리율(%) = (고객요청 처리 건수/ 고객요청 접수 건수) *100 (99% 이상) - 서비스 요청 적기처리율(%) = (완료예정일 이내 처리한 서비스 요청 건수/ 측정기간 동안 완료예정인 서비스 요청 건수) * 100 (99% 이상)
위약금	- SLA에서 정한 서비스 목표 수준에 미달하는 경우 서비스 제공자가 고객에게 위약금을 지불하도록 명시 - 가용성의 경우 위약금에 대한 해외 클라우드 기업(구글, 아마존, MS 등)의 일반적 기준을 제시하여 글로벌 수준으로 유도
서비스 계약의 해지	- 원칙적으로 클라우드 이용자가 자유로이 계약을 해지할 수 있도록 하고 해지 후 데이터 처리 (일정기간 보관, 파기, 반환 등)에 대해 협의를 통해 규정하도록 함 - 계약 당사자가 계약상의 의무를 중대하게 위반하거나 반복적으로 불이행하는 경우, 위약금 없이 클라우드 서비스 계약을 해지 가능

- 많은 기업들이 클라우드 SLA 가이드에 따라 SLA를 마련하여 서비스를 제공할 수 있도록 이용 확산 추진중

III. 금융 클라우드 SLA 가이드

가. 금융 클라우드 SLA 가이드 개요 및 절차도

개요	- 금융회사 또는 전자금융업자(이하 '금융회사')가 「전자금융감독 규정」(이하 '감독규정') 제14조의2에 따라 클라우드 컴퓨팅서비스(이하 '클라우드 서비스')를 이용하고자 할 경우 요구되는 세부절차를 안내하고 금융시스템 안전성 및 금융소비자 보호를 위해 필요한 보안사항을 권고하는 것을 목적으로 하는 지침서. 본 가이드는 금융회사가 클라우드 서비스를 이용함에 있어 적절한 보안 대책을 수립·운영하기 위해 활용할 수 있다.
절차도	〈클라우드서비스 이용 절차도〉 

- 금융회사는 클라우드서비스 이용 시 절차에 따라 필요한 조치를 수행함으로써 감독규정 제14조의2(클라우드서비스 이용 절차)를 준수하고 적절한 보안수준을 확보하여야 한다.

나. 금융 클라우드 SLA 가이드 구성

단계		필요조치	설명
사전 준비	업무 선정 및 평가	이용 대상 정보처리업무 선정	- 금융회사는 정보처리 업무 중 정보처리의 규모, 클라우드서비스 이용에 따른 비용절감, 업무 효율성 증가 등을 종합적으로 검토하여 클라우드 서비스 이용 여부를 결정하여야 한다.
		이용 대상 정보처리업무 중요도 평가	- 금융회사는 해당 업무가 취급하는 정보의 중요도*, 클라우드서비스 이용이 전자금융거래의 안전성 및 신뢰성에 미치는 영향 등을 바탕으로 중요도 평가를 수행하여야 한다.
	계획 수립	업무연속성 계획 및 안전성 확보조치 방안 수립	- 금융회사는 클라우드서비스 이용에 따른 업무연속성 계획, 안전성 확보 조치 방안 등을 수립하여야 한다. : 특히, 업무연속성 계획에는 금융회사의 클라우드서비스 이용 중단 또는 종료 시 데이터의 반환 및 파기 절차, 위탁계약의 종료, 중단, 변경 시 데이터 반환·파기에 관한 사항 등(이하 '출구전략')이 반영되어야 한다
		업무 위수탁 기준 보완 (클라우드서비스 이용관련)	- 금융회사는 중요도가 높은 업무의 위탁을 추진하는 경우 감독규정 별표 2의3(업무위탁 운영기준 보완사항)의 내용을 내부 "업무 위수탁 기준"에 반영하고 준수하여야 한다
	계약준비	클라우드서비스 제공자의 건전성·안전성 등 평가	- 금융회사는 계약 준비단계에서 클라우드서비스 제공자의 건전성 및 안전성을 평가하여야 하며, : 평가결과에 따라 보완조치를 요구하거나 다른 클라우드서비스 제공자를 대상으로 신규 평가 실시 등을 추진할 수 있다.
		정보보호위원회 심의·의결	- 금융회사는 업무추진 과정의 객관성·공정성 제고, 책임인식 강화를 위해 다음 사항을 정보보호위원회에서 심의·의결하여야 한다. : 자사 정보처리업무의 중요도 평가결과 : 클라우드서비스 제공자의 건전성·안전성 등 평가결과 : 자체 업무 위수탁 운영기준
계약 체결		클라우드서비스 이용 계약 체결	- 금융회사는 클라우드서비스 이용 계약 체결 시 감독규정 별표2의3 중 '위수탁 계약서 주요 기재사항'을 반영하여야 한다. : 특히, 데이터 처리 위치, 훈련(비상대응, 침해사고대응) 및 취약점 분석 평가 등에 대한 협조, 위탁업무의 이전·반환 등에 관한 사항이 누락되지 않도록 하고, : 금융회사의 클라우드서비스 이용 관련 금융당국 검사·감독이 원활하게 수행될 수 있도록 금융당국의 조사·접근(데이터센터 등 현장방문 포함)에 협조할 의무를 반드시 명시하여야 한다.
보고 및 이용		관련 서류 구비	- 클라우드서비스를 이용하고자 하는 모든 금융회사는 클라우드

	및 금융당국 보고	서비스 이용과 관련하여 다음의 서류를 구비하여야 한다. :「금융회사의 정보처리 업무 위탁에 관한 규정」 제7조제1항 각 호의 서류 : 이용 대상 정보처리업무의 중요도 평가 기준 및 결과 : 클라우드서비스 이용 관련 업무연속성 계획 및 안전성 확보 조치 : 클라우드서비스 이용 관련 정보보호위원회 심의·의결 결과 -「이용 대상 정보처리업무 중요도 평가」 결과 중요도가 높은 업무에 대해서는 클라우드서비스를 실제 이용하려는 날의 7영업일 이전에 금융 감독원장에게 상기 서류를 보고하여야 한다.
	서류 최신성 유지 및 수시 보고	- 금융회사는 클라우드서비스 이용 관련 서류를 최신 상태로 유지하고, 금융감독원장 요청 시 지체 없이 제공하여야 한다. - 금융회사는 다음의 변경사항이 발생하는 경우, 발생일로부터 7영업일 이내에 발생 사유, 관련 자료 및 대응계획을 포함하여 금융감독원장에게 보고하여야 한다 : 클라우드서비스 제공자의 합병, 분할, 계약상 지위의 양도, 재위탁 등의 사유로 클라우드서비스 이용 계약에 중대한 변경사항이 발생한 경우 : 클라우드서비스 제공자가 서비스품질의 유지, 안전성 확보 등과 관련한 중요 계약사항을 이행하지 아니한 경우 : 이용 대상 정보처리업무의 중요도 평가 기준·결과, 업무연속성 계획 및 안전성 확보조치에 관한 중대한 변경사항이 발생한 경우
	리스크 관리	- 금융회사는 클라우드서비스 이용 시 사전에 수립한 업무연속성 계획 및 안전성 확보조치 등을 준수하여 리스크를 관리하고, 필요 시 클라우드 서비스 제공자에게 협조를 요청하여야 한다.
이용 종료	출구 전략 이행	- 금융회사는 클라우드서비스 이용이 종료(업무 장애·지연 등으로 인한 일시적 서비스 이전 등 포함)되는 경우 사전 수립된 출구 전략에 따라 적절한 조치를 취해야 한다.

- 금융 클라우드 서비스 사용시 본 가이드 활용 시 가이드 활용하여 진행 필요

"끝"

ITPE 기술사회
제130회 정보처리기술사 기출문제 해설집

대 상 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사, 정보시스템감리사 시험
발행일 2023년 05월 20일
집 필 강정배PE, 안경환PE, 김민PE, 김민재PE
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