

제134회 컴퓨터시스템응용기술사 해설집

2024.07.27



기술사 포털 <http://itpe.co.kr> | 국내최대 1위 커뮤니티 <http://cafe.naver.com/81th>

국가기술자격 기술사 시험문제

기술사 제 134 회

제 1 교시 (시험시간: 100 분)

분야	정보통신	자격 종목	컴퓨터시스템응용기술사	수검 번호		성 명	
----	------	----------	-------------	----------	--	--------	--

※ 다음 문제 중 10 문제를 선택하여 설명하시오. (각 10 점)

1. Wi-Fi 7
2. 제로데이(Zero Day) 취약점
3. 온디바이스 AI
4. 촉각 인터넷(Tactile Internet)
5. 제로 트러스트(Zero Trust)
6. 동적 WEP 키(Dynamic WEP Key)
7. SBOM(Software Bill of Materials)
8. 신경망 처리장치(NPU : Neural Processing Unit)
9. 플랫폼 엔지니어링(Platform Engineering))
10. 「행정기관 및 공공기관의 클라우드 컴퓨팅 서비스 이용 기준 및 안전성 확보 등에 관한 고시」의 서비스 운영 분야 안전성 검토 항목
11. 애자일(Agile) 소프트웨어 개발의 장점 및 단점
12. 전자정부 정보시스템 성과 측정지표
13. 소프트웨어 품질성능 평가시험.

01	Wi-Fi 7		
문제	Wi-Fi 7		
도메인	네트워크	난이도	하(상/중/하)
키워드	IEEE 802.11be, 다중 AP 조정, 16개 공간 스트림, MIMO 프로토콜, 혼합 빔포밍, HARQ, 4096-QAM		
출제배경	Wi-Fi 얼라이언스에서 Wi-Fi 7 인증 출시에 따른 출제예상		
참고문헌	제133회 대비 FR(4일차)		
해설자	강남평일야간반 전일 기술사(제 114회 정보관리기술사 / rosemachine@naver.com)		

I. IEEE 802.11be 무선통신표준, Wi-Fi 7의 개요

가. Wi-Fi 7의 개념

- 30Gbps의 최대 전송률과 2.4GHz, 5GHz, 6GHz 무선 주파수에서의 초실감 미디어 콘텐츠를 안정적으로 전송하는 차세대 무선통신 기술

나. Wi-Fi 7의 특징

3대역 운영	- 2.4 GHz, 5 GHz, 6 GHz 주파수 대역 운영, 채널 증설, 혼잡 감소
변조 속도 증가	- 변조 속도 4096 QAM적용, 기존 1024 QAM대비 20% 향상.
확장된 대역폭	- 최대 320MHz 대역폭 정의, 전송 속도 2배 향상, 다양한 채널 결합 옵션 정의

- Wi-Fi 7 얼라이언스는 'IEEE 802.11be' 기술을 기반으로 **Wi-Fi CERTIFIED 7**을 출시함

II. Wi-Fi 7의 성능 Spec 및 기술요소

가. Wi-Fi 7의 성능 Spec

구분	성능 Spec	설명
최대 속도	30Gbps 이상	- 실감형 콘텐츠 지원 위한 전송속도 확보(3배 증가)
최대 대역폭	320Mhz 이상	- 30Gbps 달성 위한 최대 대역폭 허용
지원 주파수	2.4Ghz, 5Ghz, 6Ghz	- 비면허 대역인 6Ghz 추가로 운영 주파수 확대
하위 호환성	기존 IEEE 802.11 장비 지원	- 2.4, 5GHz 대역의 IEEE 802.11 장비 지원
기술명	IEEE 802.11 be	- IEEE 801.11be (EHT, Extremely High Throughput)
멀티플렉싱	In-Band Full-Duplex Multiplexing	- AP와 클라이언트 간의 송/수신 동시 통신 가능
지연시간	5ms 이하	- 클라우드 기반 어플리케이션(게임, 원격사무실) 등 지원

- '19년 5월부터 무선 랜의 MAC(Media Access Control) 및 PHY(physical layer)의 주요 후보 기능 사양을 정의.

나. Wi-Fi 7의 기술 요소

구분	기술 요소	설명
MAC (Media Access Control)	MLO(Multi-Link Operation)	- 처리량 증가, 대기 시간 감소, 신뢰성 향상을 위해 장치가 여러 링크를 통해 동시에 데이터를 전송하고 수신할 수 있도록 함
	무선공유기(AP)간 다중협력통신	- 시간, 주파수 및 공간 자원 유연성 개선을 위해 AP 간 데이터 공유 및 제어 정보 지원
	채널당 최대 320MHz 대역폭	- 320MHz 대역폭 및 비연속 스펙트럼의 효율적인 이용
	16x16 MIMO	- 최대 16개의 공간 스트림 네트워크 용량 증대 및 늘어난 스트림 오버헤드 개선
	하이브리드 ARQ	- 향상된 복호화 수행을 위한 추가 패리티를 통한 재전송 프로토콜 이용
PHY (Physical layer)	혼합 빔포밍	- 320MHz 광대역을 여러 개의 협대역으로 나누어 프리코딩을 수행
	4096 QAM	- 12bit 반송파 변조를 통해 기존 1024 QAM 보다 20% 향상

- Wi-Fi 6보다 3배 빠른 전송 속도 보장을 통해 AR, VR등의 콘텐츠 전송을 위해 추진 중.

III. Wi-Fi 6와 Wi-Fi 7의 비교

항목	IEEE 802.11ax (Wifi 6)	IEEE 802.11be (Wifi 7)
관련 표준	- IEEE 802.11ax	- IEEE 802.11be
최대 속도	- 9.6 Gbps	- 30 Gbps 이상
대역폭	- 20 ~ 160 MHz	- 320 MHz 이상
주파수 대역	- 2.4 GHz, 5 GHz	- 2.4 GHz, 5 GHz, 6 GHz
서비스 대상	- 밀집환경 고효율 무선 통신 서비스	- 4K, 8K 영상 스트리밍, VR/AR 등 초고속, 초저지연 무선통신 서비스
표준 기술명	- IEEE 802.11ax, HEW	- IEEE 802.11be, EHT
Antenna	- MU-MIMO(8 x 8)	- MU-MIMO(16 x 16)
Modulation	- 1024 QAM	- 4096 QAM
적용기술	- OFDMA, MU-MIMO	- Hybrid ARQ, 인밴드 전이중 멀티플렉싱
목표	- 2.4~5GHz 대역과 함께 작동	- 저지연성(낮은 지연시간)과 광활한 전송 속도

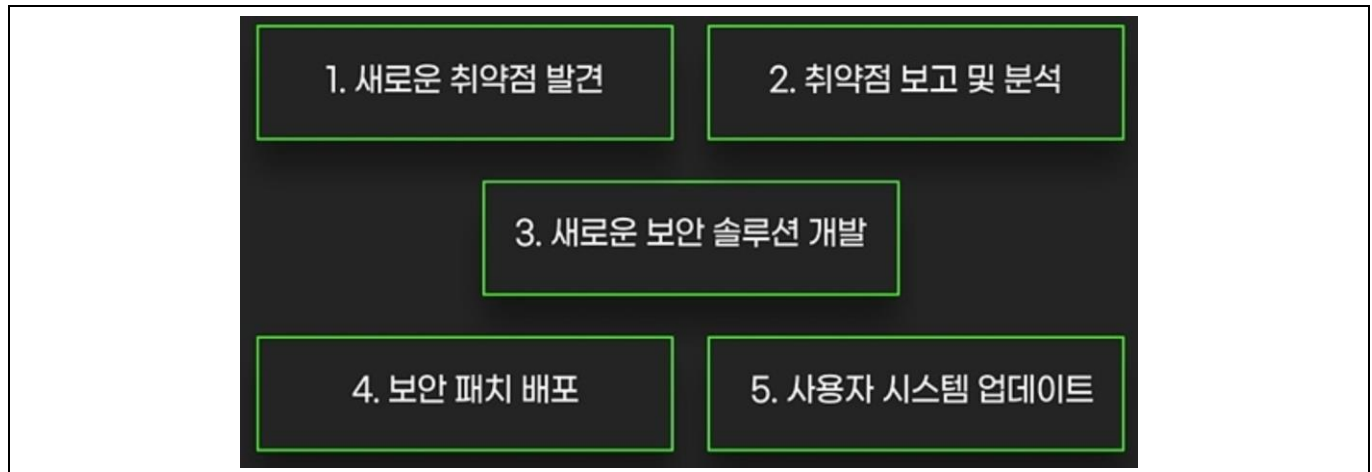
“끝”

02	제로데이(Zero Day) 취약점		
문제	제로데이(Zero Day) 취약점		
도메인	보안	난이도	중(상/중/하)
키워드	멀티코어, 파이프라인, 면적대비, 전력소비		
출제배경	기본 보안 지식 확인		
참고문헌	ITPE 서브노트		
해설자	강남평일야간반 전일 기술사(제 114회 정보관리기술사 / nikki6@hanmail.net)		

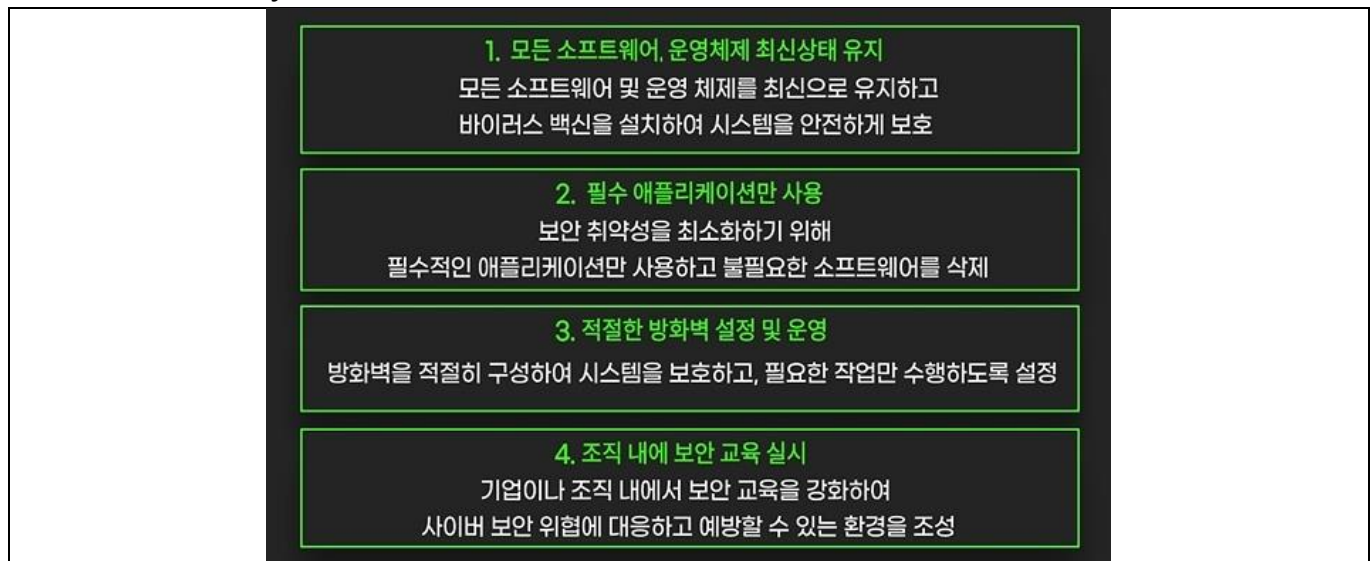
I. 제로데이(Zero Day) 취약점 개념

- 특정 소프트웨어의 아직까지 공표되지 않은, 혹은 공표되었지만 아직까지 패치 되지 않은 보안 취약점을 이용한 해킹의 통칭

II. 제로데이(Zero Day) 취약점 대응 프로세스



III. 제로데이(Zero Day) 취약점 예방 방법



“끝”

03	온디바이스 AI		
문제	온디바이스 AI		
도메인	인공지능	난이도	중(상/중/하)
키워드	인공지능 가속기, NPU, 경량 AI 모델, 클라우드 AI		
출제배경	IoT 기술에 인공지능 기술을 더한 온디바이스 AI 기술에 대한 현황 확인		
참고문헌	온디바이스 AI 하드웨어 및 소프트웨어 기술개발 동향-(주간기술동향 2028호) https://dbr.donga.com/article/view/1203/article_no/9635		
해설자	강남평일야간반 전일 기술사(제 114회 정보관리기술사 / nikki6@hanmail.net)		

I. 디바이스 내 AI 탑재, 온디바이스 AI(Artificial Intelligence)의 개념

<div><div>AS-IS</div><div><div><div>Service</div><div> Smart Home Smart Energy Smart Factory</div></div><div><div>Platform</div><div>서버, 엣지 고속지능 중심 대규모 처리</div><div></div><div></div></div><div><div>Network</div><div>4G LTE</div></div><div><div>Device</div><div>디바이스 단순 처리 / 고정적 대응</div><div></div><div></div></div></div></div> <div><div>TO-BE</div><div><div><div>Service</div><div> 스쿨존 위험상황 신속대응 주차단속 등 도시교통 지원 노후시설 모니터링 및 보수 지원</div></div><div><div>Platform</div><div>단말 가공/처리 데이터 기반 지능 보조</div><div></div><div></div></div><div><div>Network</div><div>5G</div></div><div><div>Device</div><div>디바이스 고속지능 처리 / 자체 판단능동 대응</div><div></div><div></div></div></div></div>		
정의	- 멀리 떨어진 클라우드 서버를 거치지 않고 스마트기기 자체적으로 정보를 수집하고 연산할 수 있는 AI 기술	
특징	빠른 응답 속도	- 데이터 이동 없이 단말 자체 처리를 통한 빠른 서비스 제공 가능
	개인정보 보호	- 데이터를 단말 중심으로 운영하여 이동 중 발생하는 공격 대응 가능
	저전력/저비용	- 중앙집중식 처리 방식에서 일부 영역을 단말기에서 직접 처리함으로써 클라우드 컴퓨터의 에너지 과부하 해결 가능

II. 온디바이스 AI의 하드웨어 및 소프트웨어 기술

가. 온디바이스 AI의 하드웨어 기술

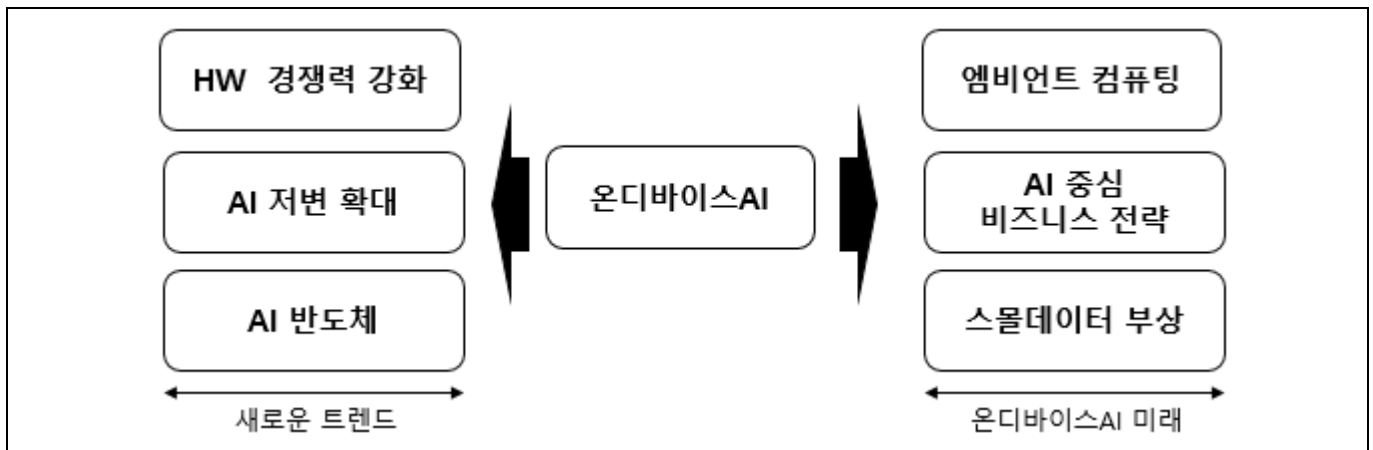
구분	기술	설명
국내	인공지능 가속기	- 뉴로모픽 기술에 집중하여 엣지 및 디바이스에서 사용 가능한 인공지능 가속기 기술
	NeuroMem 기술	- 에너지 효율적 소형 폼팩터 구성을 위한 기술
	NPU(Neural Processing Unit)	- 인공지능 네트워크 연산에 사용되던 GPU와 유사한 구조이나 인공지능 기술에 특화하여 연산 효율을 높이거나 에너지 효율을 증가시키기 위해 개발한 칩
	AI SoC 솔루션	- 비전 관련 작업 가속기 및 음성 관련 작업 가속기를 탑재하여 가전에서 필요한 영상 및 음성 AI 분석을 지원
국외	뉴럴 엔진	- Apple의 인공지능 서비스 품질 향상을 위해 개발된 NPU
	Volta GPU	- 엔디비아는 AI 가속을 위한 GPGPU를 개발
	NVDLA	- AI 추론 가속기 아키텍처를 통한 디바이스에서 클라우드까지 확장성 제공
	NNP	- 인텔에서 구현한 NPU 하드웨어 기술
	엣지 TPU	- 구글이 개발한 엣지 디바이스 환경의 온디바이스 AI 수행을 위한 기술

나. 온디바이스 AI의 소프트웨어 기술

구분	기술	설명
경량 AI 모델	모델 구조 변경	- 잔여 블록, 병목 구조, 밀집 블록 등 다양한 신규 계층 구조를 이용하여 파라미터 축소 및 모델 성능을 개선(ResNet, DenseNet, SqueezeNet)
	합성곱 필터 변경	- 합성곱 신경망의 가장 큰 계산량을 요구하는 합성곱 필터의 연산을 효율적으로 감소(MobileNet, ShuffleNet)
	자동 모델 탐색	- 특정 요소(지연시간, 에너지 소모 등)가 주어진 경우, 강화 학습을 통해 최적 모델을 자동 탐색(NetAdapt, MNasNet)
AI 모델 경량화 기술	모델 압축	- 가중치 가지치기, 양자화/이진화, 가중치 공유 기법을 통해 파라미터의 불필요한 표현력을 감소(Deep Compression, XNOR-Net)
	모델 압축 자동 탐색	- 알고리즘 경량화 연구 중 일반적인 모델 압축 기법을 적용한 강화 학습 기반의 최적 모델 자동 탐색 연구(PocketFlow, AMC)

- 온디바이스 AI에 대한 활용성이 점점 증가하면서 온디바이스 AI 기술은 점점 발전되고 있음.

III. 온디바이스 AI의 시사점



“끝”

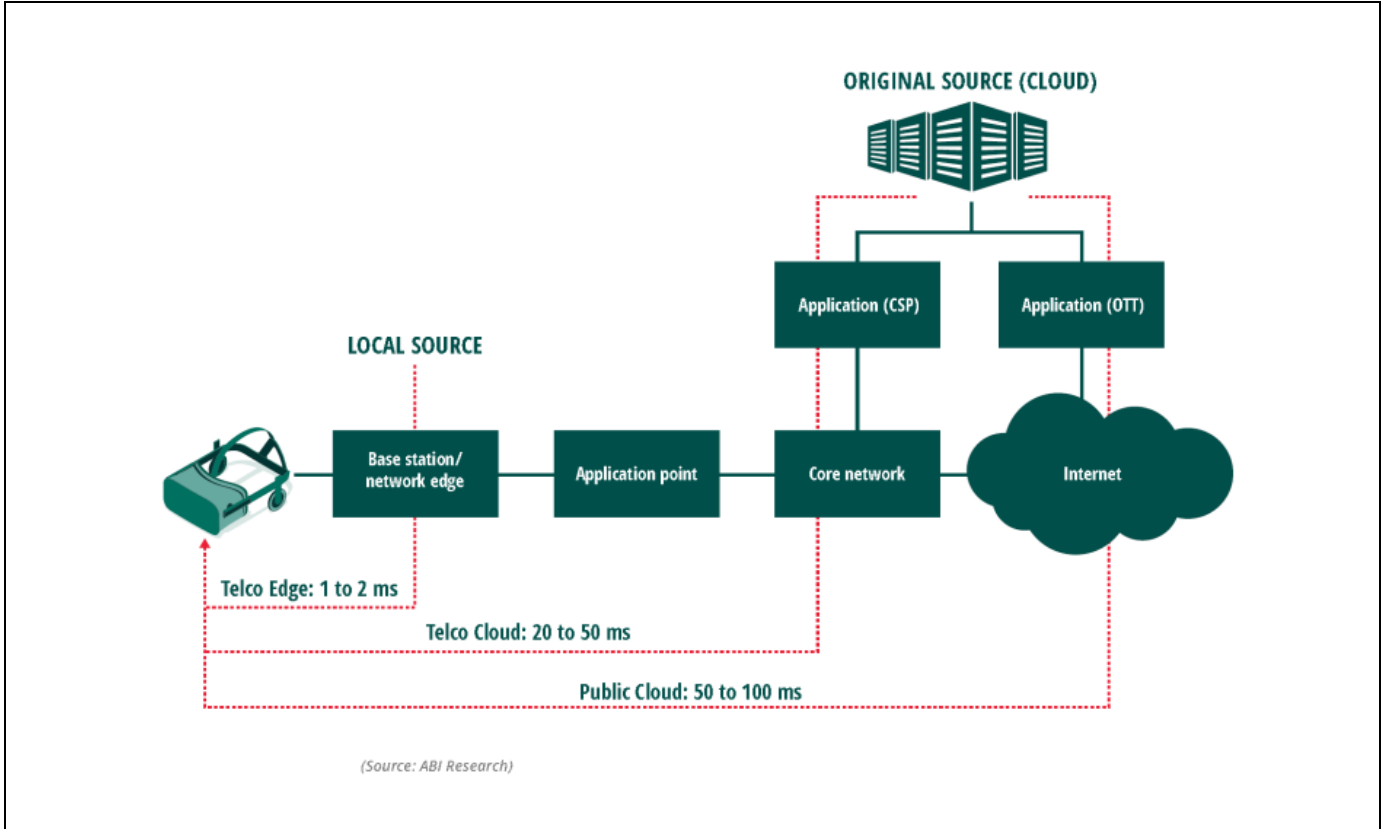
04	촉각 인터넷(Tactile Internet)		
문제	촉각 인터넷(Tactile Internet)		
도메인	디지털서비스	난이도	중 (상/중/하)
키워드	초저지연(1 ms 이내) 인터넷 서비스, 가용성, 신뢰성, 보안성		
출제배경	5G/6G 출시로 인한 촉각 인터넷 개념 이해 확인		
참고문헌	ITPE 기술사회 자료		
해설자	NS반 멘토 백현 기술사(제 122회 정보관리기술사 / snuoo@naver.com)		

I. 초고속 인터넷 서비스, 촉각 인터넷(Tactile Internet) 개념

- 사람의 촉각(촉감)이 느낄 만큼 정보를 매우 빠른 속도로 전송하는 인터넷 서비스

II. 촉각 인터넷 실현을 위한 기술

가. 촉각 인터넷 실현을 위한 아키텍처



- 촉각 인터넷 실현을 위해서는 MEC(Mobile Edge Cloud)기반 1~2ms 이내의 end-to-end latency 구현이 필수

나. 촉각 인터넷 활용 서비스

구간	기술	설명
기지국/응용서버간 유무선구간	모바일 에지 클라우드	<ul style="list-style-type: none"> - 모바일 에지 클라우드(Mobile Edge Cloud) - 응용 서버를 기지국 가장 가까운 위치에 둬으로써 전체 단-대-단(End-to-end) 서비스 지연 또한 2ms 내외로 감소

단말/기지국간 무선구간	TTI 단축	<ul style="list-style-type: none"> - TTI : Transmission Time Interval Shortening (전송시간주기) 단축 - 데이터 전송단위를 기존 1ms 주기였던 4G LTE 방식 대비 1/7 수준($143\mu s$)으로 감소 시킴 - 단말에서 기지국까지의 무선 구간에서 데이터 전송 주기 단축
	역호환 무선 프레임 구조	<ul style="list-style-type: none"> - 역호환 무선 프레임(Backward-compatible Radio Frame) 구조 - 4G 호환 2-symbol 전송 단위 기술 - 기존의 4G용 단말과 5G 저지연 단말을 동시에 수용
	빠른 데이터 수신	<ul style="list-style-type: none"> - 고속 채널 추정 및 디코딩 (On-the-fly 개념) - 수신 데이터 인식 시간을 최소화
	오버헤드 최소화 신호설계	<ul style="list-style-type: none"> - 제어신호와 참조 신호(추정신호)를 최적으로 배치
	기타	<ul style="list-style-type: none"> - 슬롯단위 데이터 전송 기술 - 슬롯단위 주파수 호핑 기술 : seamless 전송 - 4G 호환 1/4 전송단위 축소기술 : 선별적 자원 할당 - 제로지연 핸드오버 기술 : 기지국 이용 연결 지원) - 경쟁기반 데이터 전송 방식 : 빠른 액세스

- 5G 이동통신 핵심기술로 초각인터넷 구현

III. 초각 인터넷의 활용 서비스

분야	서비스	지연 한계 요구사항
로보틱스	위험한 지역(원자력발전소 등)의 건설, 철거 및 유지보수, 해양구조물에 로봇을 이용한 원격 조정 서비스	수 ms 이하
증강현실	도시 및 박물관 가이드, 차량 보조 시스템	수 ms 이하
기능성 게임	유선기반의 기능성 게임(오락성과 특별한 목적을 가진 게임-건강, 교육, 치료, 군사훈련)을 이동 통신망을 이혼해도 가능하도록 확대	10 ~ 20 ms 이하
헬스케어	원격 수술, 원격 재활 서비스	수 ms 이하 (고 신뢰성)
도로 교통	V2V 및 V2I의 차량 안전 시스템	수 ms 이하 (고 신뢰성)
스마트 그리드	무효전력의 양을 줄이고 전력공급의 안전성을 위한 지능형 파워 그리드 시스템	1 ~ 100ms 이하 (고 신뢰성 및 보안성)

- 다양한 분야에 활용되어 4차 산업혁명을 이끌 것으로 예상됨

“끝”

05	제로 트러스트(Zero Trust)		
문제	제로 트러스트(Zero Trust)		
도메인	보안	난이도	중 (상/중/하)
키워드	멀티코어, 파이프라인, 면적대비, 전력소비		
출제배경	기존 경계기반 보안 모델의 취약점 개선을 위한 개념으로 출제 가능		
참고문헌	https://gusdnd852.tistory.com/143		
해설자	NS반 멘토 백현 기술사(제 122회 정보관리기술사 / snuoo@naver.com)		

I. 절대 신뢰하지 말고 항상 검증하라(Never Trust, Always Verity), 제로트러스트(Zero Trust) 개념

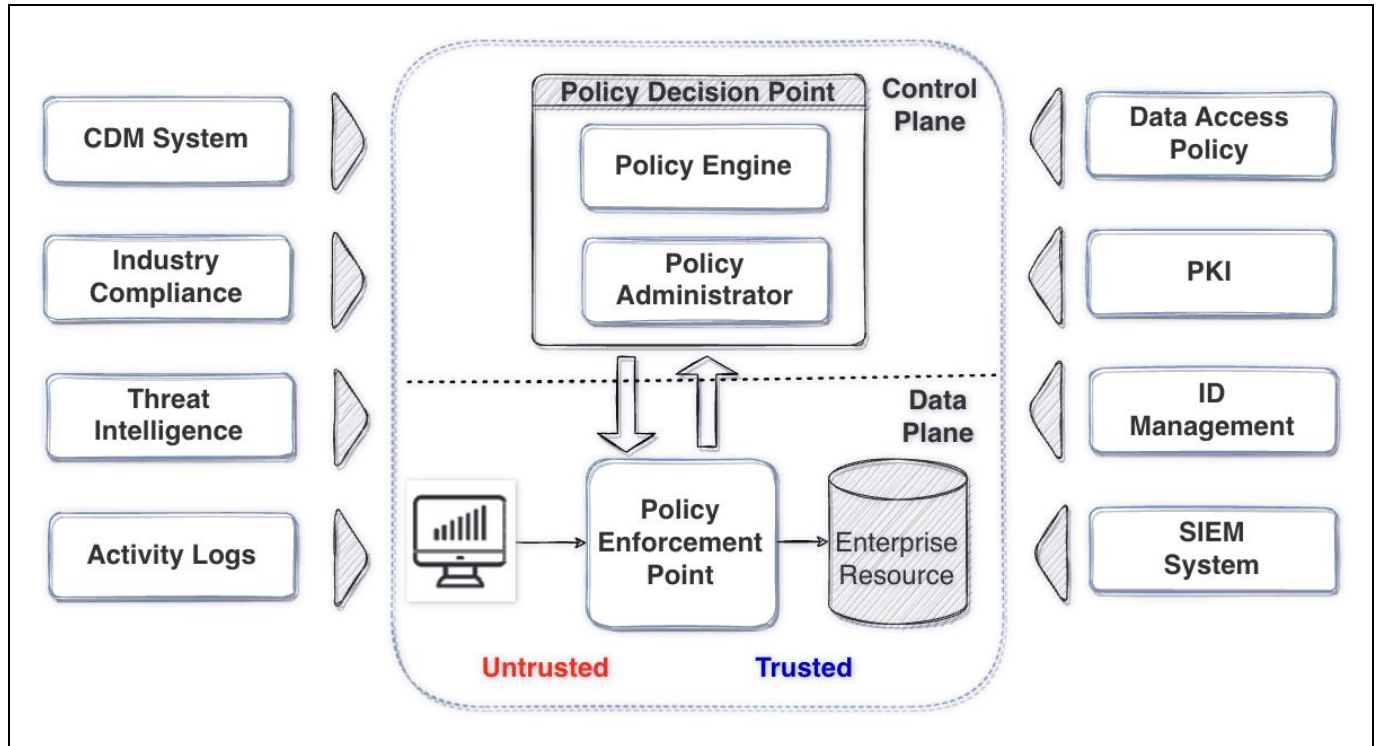
가. 제로트러스트(Zero Trust) 개념

구분	내용	
개념도	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;"> <p>Traditional Single Perimeter Defense</p> </div> <div style="text-align: center;"> <p>Zero Trust Defense Focuses on Resource Protection</p> </div> </div>	
개념	2020 NIST SP 800-207	- 항상 네트워크가 침해되었다 가정하고, 보호해야 할 데이터 및 컴퓨팅 서비스 등에 대한 접근 요구에 대해 정확하고 최소한의 권한(Least Privilege)을 부여하는 아이디어와 개념의 모음
	2022 MIT Lincoln Laboratory	- 악의적인 상대에 의해 지속적으로 노출되고 잠재적으로 침해될 수 있는 시스템의 구성요소, 서비스 및 사용자를 다루는 일련의 원칙

- 제로트러스트 기반의 보안 구조는 기업망 내외부 언제나 공격자가 존재할 수 있다는 것을 상정
- 기존의 기업망을 신뢰하지 않고 기업 내 자산에 접근하는 모든 주체에 대해 "지속적으로 인증"하고, 위험성을 평가하여 정보 자산을 보호

II. 제로트러스트 구현을 위한 아키텍처

가. 제로트러스트 아키텍처 개념도



나. 제로트러스트 아키텍처 구성요소

구분	핵심 구성요소	설명
플레인	- 제어 플레인	- 경로 계산이나 패킷의 전송 정책, 우선 제어, 부하 분산 등의 복잡한 처리
	- 데이터 플레인	- 제어 플레인에 따라서 결정된 경로와 정책에 따라서 데이터 패킷을 전송
정책	- 정책 결정 포인트	- PDP(Policy Decision Point) - 이용자(주체)로부터의 액세스 허가의 평가 및 판단 컴포넌트
	- 정책 엔진	- PE(Policy Engine) - 액세스 허가를 결정하는 컴포넌트
	- 정책 관리자	- PA(Policy Administrator) - PEP 명령어를 통해 사용자와 리소스의 통신 및 차단 컴포넌트
	- 정책 실시 포인트	- PEP(Policy Enforcement Point) - 사용자의 리소스 액세스 시 접속, 감시, 종료 컴포넌트
기술	- 마이크로 세그멘테이션	- VLAN, VxLAN을 통해 서비스 논리적 그룹으로 분류
	- 소프트웨어 정의 경계 (Software Defined Perimeter)	- 애플리케이션과 사용자 간 IP터널 설정(IP-Sec, TLS's VPN) - SDDC(Software Defined Data Center)와 오버레이 NW 사용
	- 제로 트러스트 프록시	- 인증된 사용자와 애플리케이션의 주문형 경계 설정, 분석 - 향상된 ID 거버넌스 IAP(Identity Aware Proxy)

- 제로 트러스트 아키텍처(Zero Trust Architecture)는 네트워크 보안과 접근 제어에 대한 현대적인 접근 방법으

로 "신뢰하지 않는 것으로 가정하고 검증"하는 철학을 기반

III. 제로트러스트(Zero Trust) 실현을 위한 7 원칙

구분	내용
Resources	- 모든 데이터와 컴퓨팅 서비스는 자원으로 간주하며, SaaS(Software as a Service)나 소형기기도 사내 시스템에 접근할 수 있다면 자원임
Communication	- 모든 통신은 환경에 관계 없이 동일한 보안 요구가 충족되어야 하며, 기업 내 네트워크에 대해서도 예외는 없음
Per-session Access	- 조직의 리소스에 대한 접근은 개별 세션마다 허가를 받아야 함
Dynamic Policy	- 클라이언트 식별자, 응용, 요청을 보낸 자산 상태, 행동 및 환경 속성 등에 따라 동적 정책이 결정
Monitoring	- 기본적으로 자산을 신뢰하지 않고, 리소스에 대한 접근을 판단 시 자산의 상태를 감시하고, 보안 조치를 하기 위한 모니터링을 수행
Authentication and Authorization	- 모든 리소스에 대해 정형화된 사이클로 접근하며, ICAM, 자산관리 시스템, 다중 인증 사용을 권장
Continuous Improvement	- 자산의 보안 상태, 네트워크 트래픽, 접근 요청에 대해 가능한 많은 정보를 수집하고, 이를 활용해 지속적으로 보안 상태를 개선

- 제로트러스트는 개별 세션마다 허가를 받아야 한다는 "Per-session Access"의 요구사항을 충족시키기 위해 서라도 무자각 지속 인증 기술은 유의미

“끝”

06	동적 WEP 키(Dynamic WEP Key)		
문제	동적 WEP 키(Dynamic WEP Key)		
도메인	보안	난이도	중(상/중/하)
키워드	무선, 암호화, IEEE 802.1aa, 키, 사용자 인증, 인증 서버, 주기적으로 키 변경		
출제배경	웹 기반 서비스 증가로 웹 방화벽 기능에 대한 고전 토픽 출제		
참고문헌	https://peemangit.tistory.com/208		
해설자	NS반 멘토 백현 기술사(제 122회 정보관리기술사 / snuoo@naver.com)		

I. 무선 랜 보안성 향상을 위한, 동적 WEP 키(Dynamic WEP Key)의 개요

가. 동적 WEP 키 개념

- 무선 단말기와 AP 간의 WEP 키를 주기적으로 자동 변경함으로써 무선 랜(WLAN)의 보안성을 향상시킨 방식. 정적 WEP 키 방식은 공유된 해킹 툴로도 간단하게 해킹이 가능해져 이를 보완하기 위해 동적 WEP 키 방식

나. 동적 WEP 키 특징

특징	설명
보안 강화	- 키를 주기적으로 변경함으로써 키가 유출되더라도 잠깐 동안만 유효해 보안 강화
중앙 관리	- 네트워크 관리자가 중앙에서 키를 관리하고 배포할 수 있어 관리 효율성 증가
사용자 인증	- IEEE 802.1aa 프로토콜을 통해 사용자 인증을 강화하여 네트워크 접근을 제어

II. 동적 WEP 키를 사용한 암호화 과정 및 구성요소

가. 동적 WEP 키를 사용한 암호화 과정

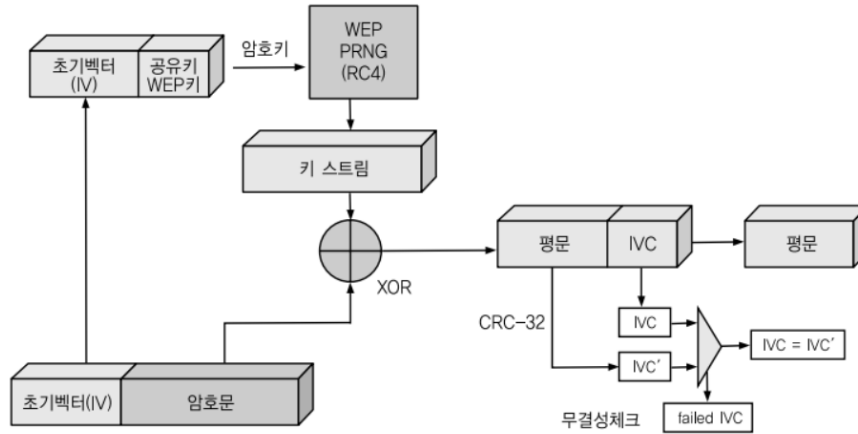
암호화 과정

```

graph TD
    IV[초기벡터 IV] --> RC4[WEP PRNG RC4]
    Key[공유키 WEP키] --> RC4
    RC4 --> KS[키 스트림]
    P[평문] --> XOR((XOR))
    KS --> XOR
    XOR --> C[암호문]
    C --> E[초기벡터 IV | 암호문]
    P --> CRC[CRC-32]
    CRC --> ICV[ICV]
    ICV --> E
    
```

- 1) 공유키와 난수 발생기를 이용하여 RC4 알고리즘을 통한 키스트림을 생성 (데이터 암호화 지원)
- 2) 무결성을 보장하기 위해 CRC-32 알고리즘으로 구성되는 ICV 를 사용
- 3) 키스트림과 평문과 ICV 값이 합해진 데이터를 XOR 연산 수행하여 암호문 생성
- 4) 생성된 암호문에 IV 값 추가
- 5) 완성된 암호문에 프레임 헤더와 FCS 를 붙여 전송

복호화 과정

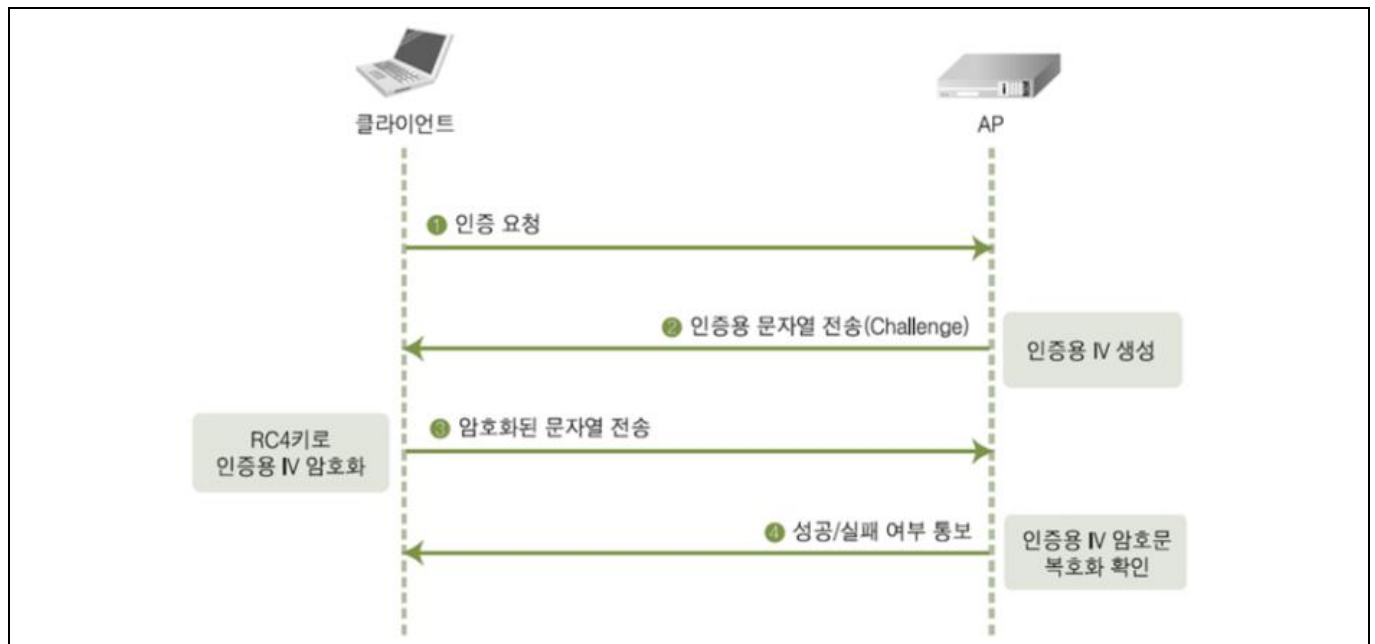


- 1) 송신자가 보낸 패킷에서 IV 값 추출
- 2) 추출해낸 IV 값과 WEP 키로 난수발생기에서 난수를 생성하여 키스트림 구성
- 3) 키스트림과 암호문을 XOR 연산 수행을 통한 복호화수행
- 4) 복호화된 평문을 CRC-32 연산을 통한 IVC와 IVC를 비교하여 무결성 체크
- 5) 무결성 확인이 완료되면 평문 수신

나. 동적 WEP 키 구성요소

구성요소	설명
키 관리 프로토콜	- IEEE 802.1aa 인증 프로토콜로 키관리에 사용
키 갱신 주기	- 네트워크 관리자가 설정한 주기(예: 매 30분)마다 키를 자동으로 갱신
키 분배	- 인증 서버는 클라이언트 장치와 액세스 포인트(AP) 간에 새로운 WEP 키를 안전하게 분배

III. 동적 WEP 키를 사용한 인증절차



- 인증 요청, 인증용 문자열 전송, 암호화된 문자열 전송, 성공실패 여부 단계로 인증 진행

“끝”

07	SBOM (Software Bill of Materials)		
문제	SBOM(Software Bill of Materials)		
도메인	소프트웨어공학	난이도	하(상/중/하)
키워드	Author Name, Timestamp, Version String, SPDX, CycloneDX, SWID		
출제배경	SW 공급망 관리의 중요성에 따른 출제 예상		
참고문헌	미국 NTIA(https://www.ntia.gov/SBOM)		
해설자	정상반멘토 정상 기술사(제 124회 정보관리기술사 / itpe_peak@naver.com)		

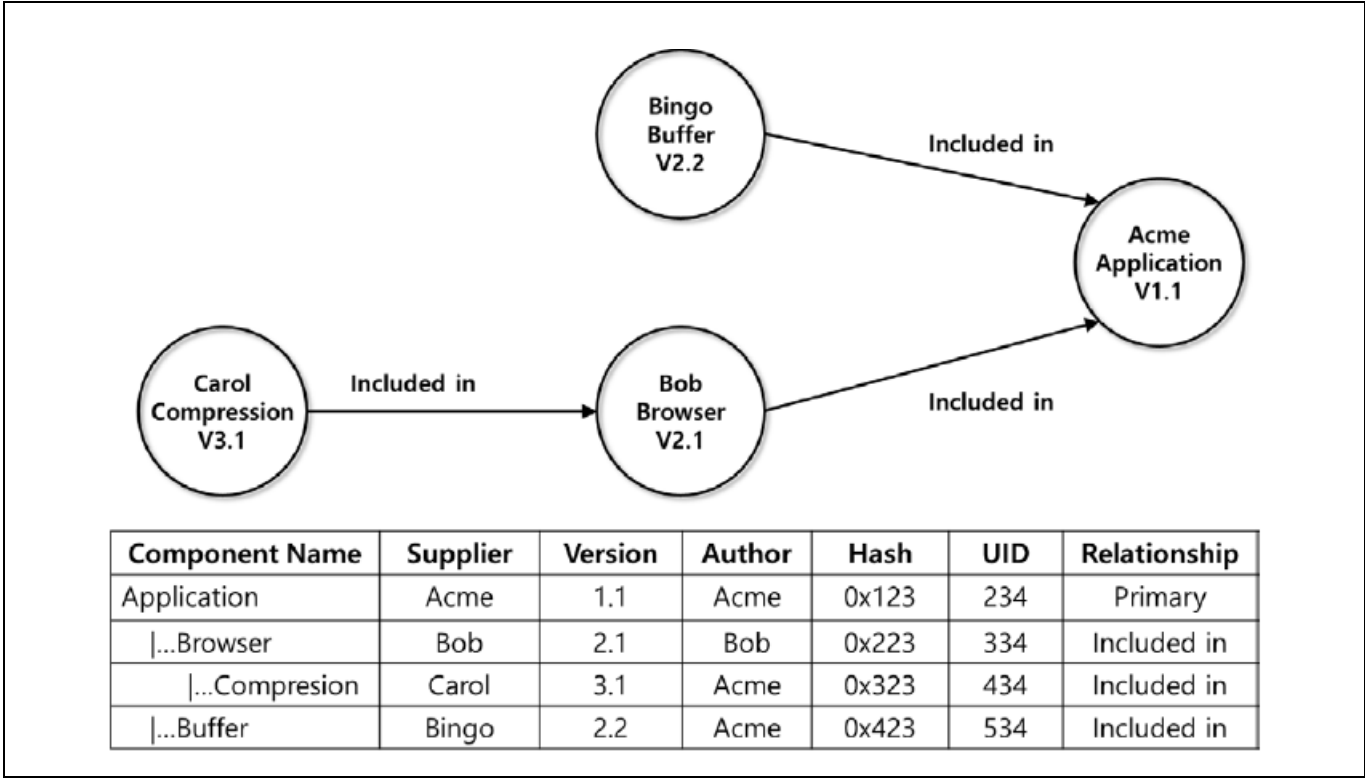
I. SW 공급망 공격 대응, SBOM의 정의

가. SBOM의 정의

- 소프트웨어 컴포넌트 및 구성 요소를 식별할 수 있는 메타데이터와 저작권 및 라이선스 등으로 소프트웨어 콘텐츠에 대한 정보를 포함하는 공식 SW 자재 명세서

II. SBOM의 개념도 및 기술요소

가. SBOM의 개념도



나. SBOM의 기술요소

구분	핵심 기술	설명
Baseline Attributes	- Author Name	- SW 작성자 정보
	- Timestamp	- SBOM이 마지막으로 업데이트된 날짜 및 시간(ISO 8601)
	- Supplier Name	- SW 공급업체의 이름 또는 기타 식별자

	- Component Name	- SW 구성요소 이름 또는 식별자
	- Version String	- SW Version 정보(Semantic Versioning)
	- Component Hash	- SW 컴포넌트 해시 값을 통한 무결성 증빙
	- Unique Identifier	- 고유한 Namespace 및 고유 식별자 생성
	- Relationship	- SBOM 구성 요소 간의 종속성 및 연관 관계 표현
Formats	- SPDX	- Software Package Data Exchange - 리눅스 재단 오픈소스 저작권 및 라이선스 정보 교환 표준
	- CycloneDX	- OWASP 재단 공급망 구성요소 보안 및 경량 SBOM 표준
	- SWID	- Software Identification - SW 정보에 대한 Tag 생성 및 오픈소스 SW 인벤토리 지원

- 성공적인 SBOM 적용을 위한 관리적, 기술적 고려사항 필요

III. SBOM의 고려사항

구분	고려사항	내용
관리적	- SBOM 관리요소 설정	- 미국 국가표준기술연구소 SBOM 최소 관리 요소 가이드 - 데이터 필드, 자동화 지원, 지침 절차
	- SW 공급망 위험 평가 정기 수행	- SW 공급망 취약점, 악성코드 유입 위험 정기적 평가 - 잠재적 취약성 식별 및 공격 사전 대응
기술적	- SBOM 자동화 구현	- SBOM 자동 생성 및 기계 가독성 고려한 자동화 기술 - SPDX, CyclonDX, SWID 이용한 표준 양식 적용
	- SBOM 오픈 플랫폼	- IoTcube 등 SBOM 자료생성 및 보안취약점 분석 수행

- SW 제품에 대한 SBOM 제출 의무화('21년 미국)로 글로벌 시장 진출을 위해 SBOM 적용 활성화 필요

“끝”

08	NPU(Neural Processing Unit)		
문제	NPU(Neural Processing Unit)		
도메인	AI/CA	난이도	중(상/중/하)
키워드	Accumulator, weights		
출제배경	인공지능 반도체의 기본 이해		
참고문헌	ITPE 기술사회 자료집		
해설자	정상반멘토 정상 기술사(제 124회 정보관리기술사 /itpe_peak@naver.com)		

1. 머신러닝 전용 칩, NPU(Neural Processing Unit)의 개념

가. NPU의 정의

- 딥러닝 알고리즘 연산을 수행하는데 필요한 모든 제어 및 산술 논리를 구현하는 머신러닝 기반의 차세대 반도체

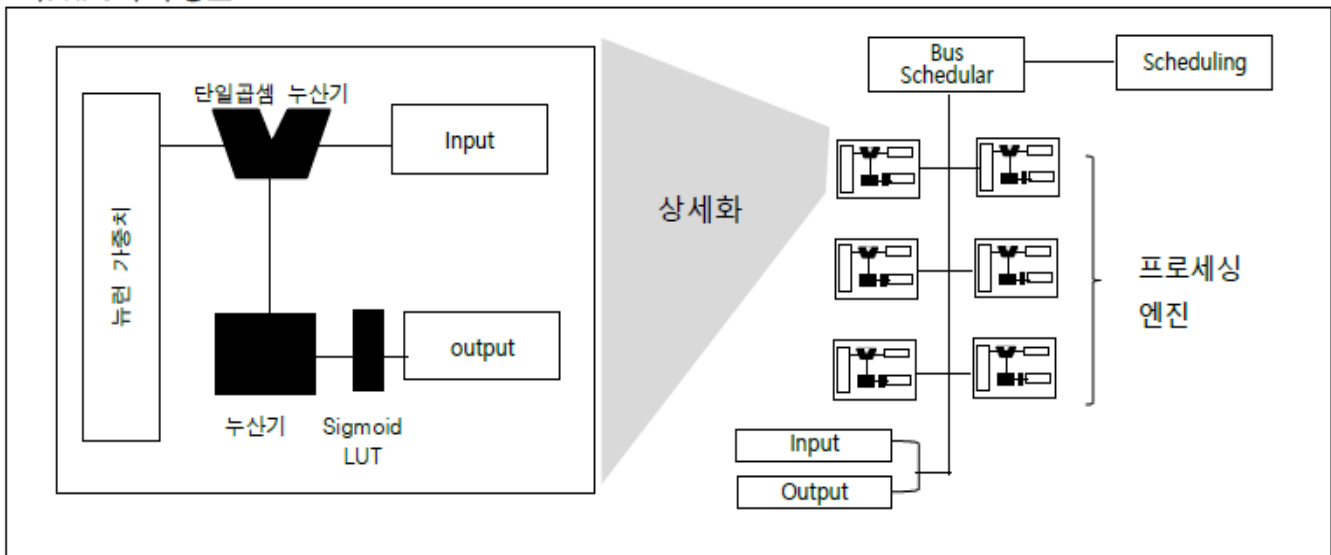
나. NPU의 특징

특징	설명
저전력/고성능	머신러닝 처리에 특화된 프로세서로 최소전력으로 CPU/GPU 처리 성능 개선
기계학습 모델	DNN, CNN, RNN 등을 활용한 대용량 데이터 처리 및 고신뢰성 제공
머신러닝 소프트웨어 프레임워크 지원	TensorFlow, Caffe2, Theano, CNTK, MXNet, Torch 등의 머신러닝 소프트웨어 프레임워크 지원

- 구글의 TPU(Tensor Processing Unit)보다 개선된 인공지능 구현에 최적화된 하드웨어 프로세서

2. NPU의 구성도 및 구성요소

가. NPU의 구성도



- 입력데이터는 누산기, 시그모이드 룩업 테이블 등 하드웨어 장치를 활용하여 딥러닝 고속 연산 수행

나. NPU의 구성요소

구성요소	기술요소	설명
Processing Engine	Sigmoid LUT, Accumulator, Neuron Weights	머신러닝 데이터 입출력/연산을 처리하는 H/W
데이터 전송	Bus Scheduler	Processing Engine간 데이터 통신 및 병렬 처리
딥러닝 알고리즘	DNN, CNN, RNN	입력데이터를 딥러닝 알고리즘 활용하여 출력값 처리

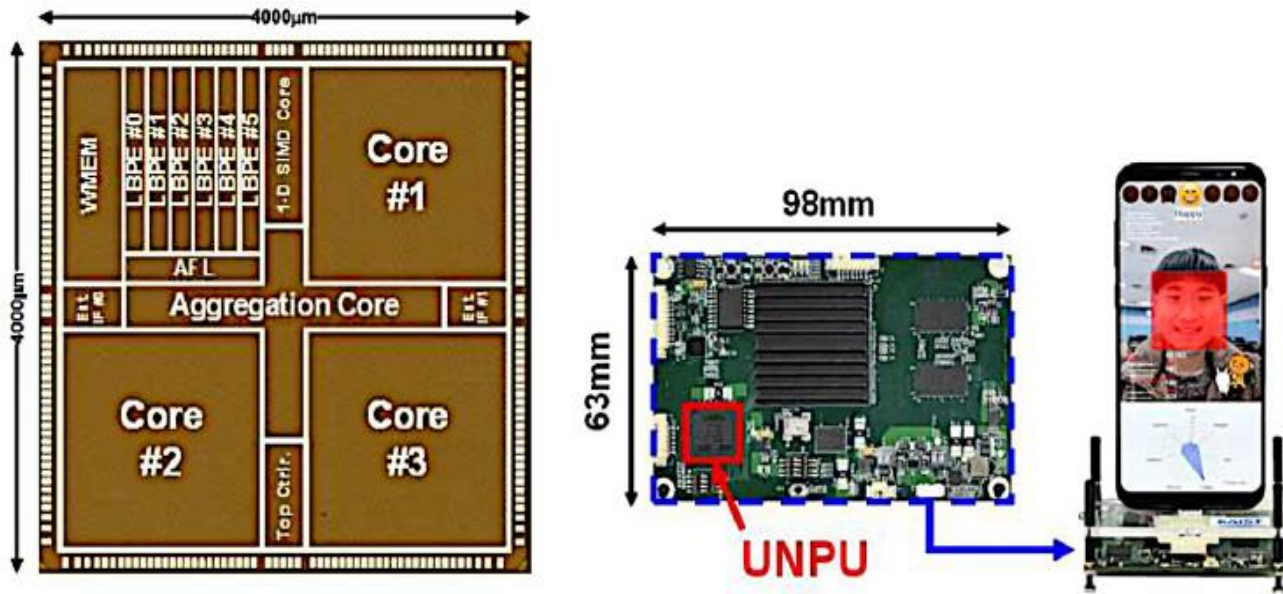
- 딥러닝을 처리하는 소프트웨어 알고리즘을 전용 하드웨어 방식으로 구현하여 GPU처리방식의 성능개선

3. GPU와 NPU 비교

항목	GPU	NPU
개념	고속 그래픽 렌더링 처리위한 그래픽 칩	딥러닝 기반의 인간 두뇌 모방 칩
특징	고속 그래픽연산, 병렬처리	저전력, AI 전용 H/W
핵심기술	SM(Stream Multiprocessor), SIMD, SP(Streaming Processor), PCI Express Bus	Accumulator, sigmoid LUT, neuron Weight, DNN, CNN, RNN
활용사례	구글 - TPU	삼성 - 엑시노스9820 애플 - A12 Bionic

- NPU는 엣지컴퓨팅을 위한 핵심기술로, 엣지 디바이스에 탑재되어 딥러닝 기반의 고속 AI 서비스 제공

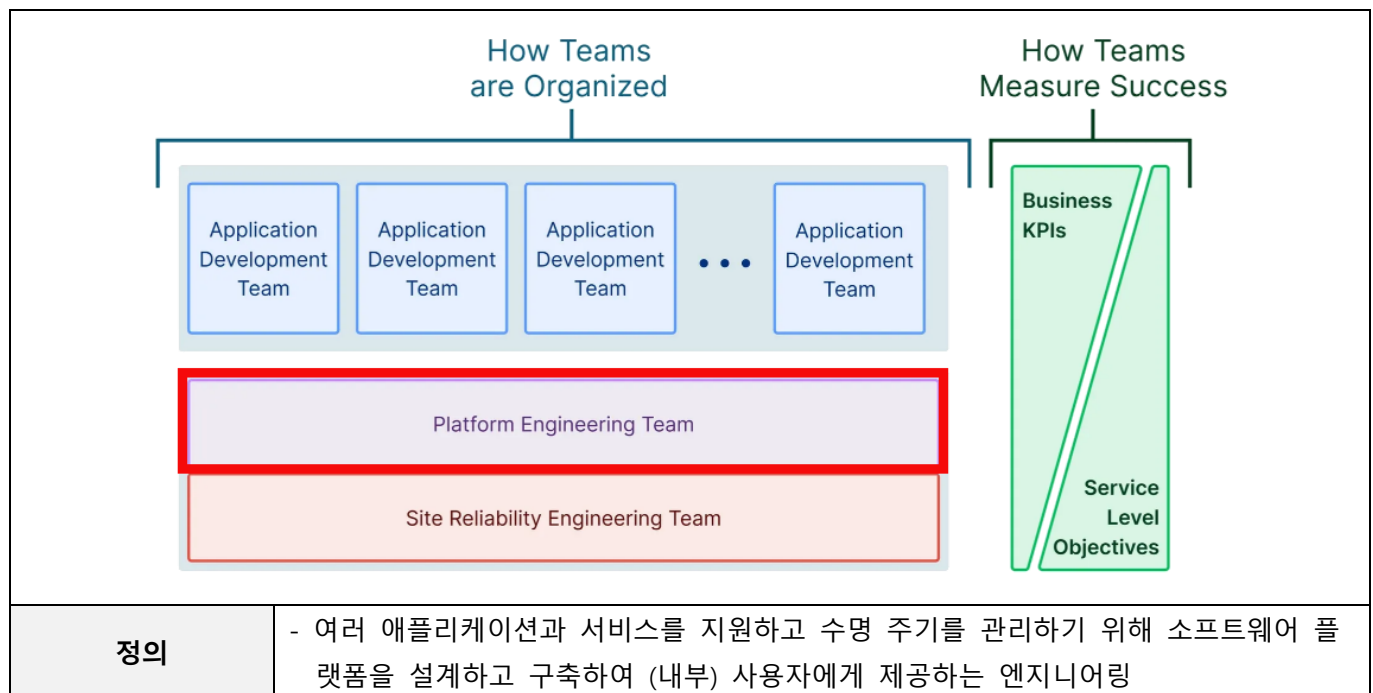
[기타자료]



09	플랫폼 엔지니어링(Platform Engineering)		
문제	플랫폼 엔지니어링(Platform Engineering)		
도메인	디지털서비스	난이도	중 (상/중/하)
키워드	소프트웨어 수명 주기 관리 위한 플랫폼, Cross Functional Team		
출제배경	가트너 선정 2023년 10대 전략 기술 트렌드 중 일부로 출제 가능성 대비		
참고문헌	가트너 선정 2023년 10대 전략 기술 트렌드 분석 - 플랫폼 엔지니어링 (https://www.joinc.co.kr/w/platform_engineering) SRE vs. Platform Engineering(https://www.getambassador.io/resources/rise-of-cloud-native-engineering-organizations)		
출제자	유술사 (제 113회 컴퓨터시스템응용기술사 / itpe_you@naver.com)		

I. 데브옵스(DevOps)의 또 다른 진화. 플랫폼 엔지니어링(Platform Engineering)의 개념

가. 플랫폼 엔지니어링(Platform Engineering)의 정의

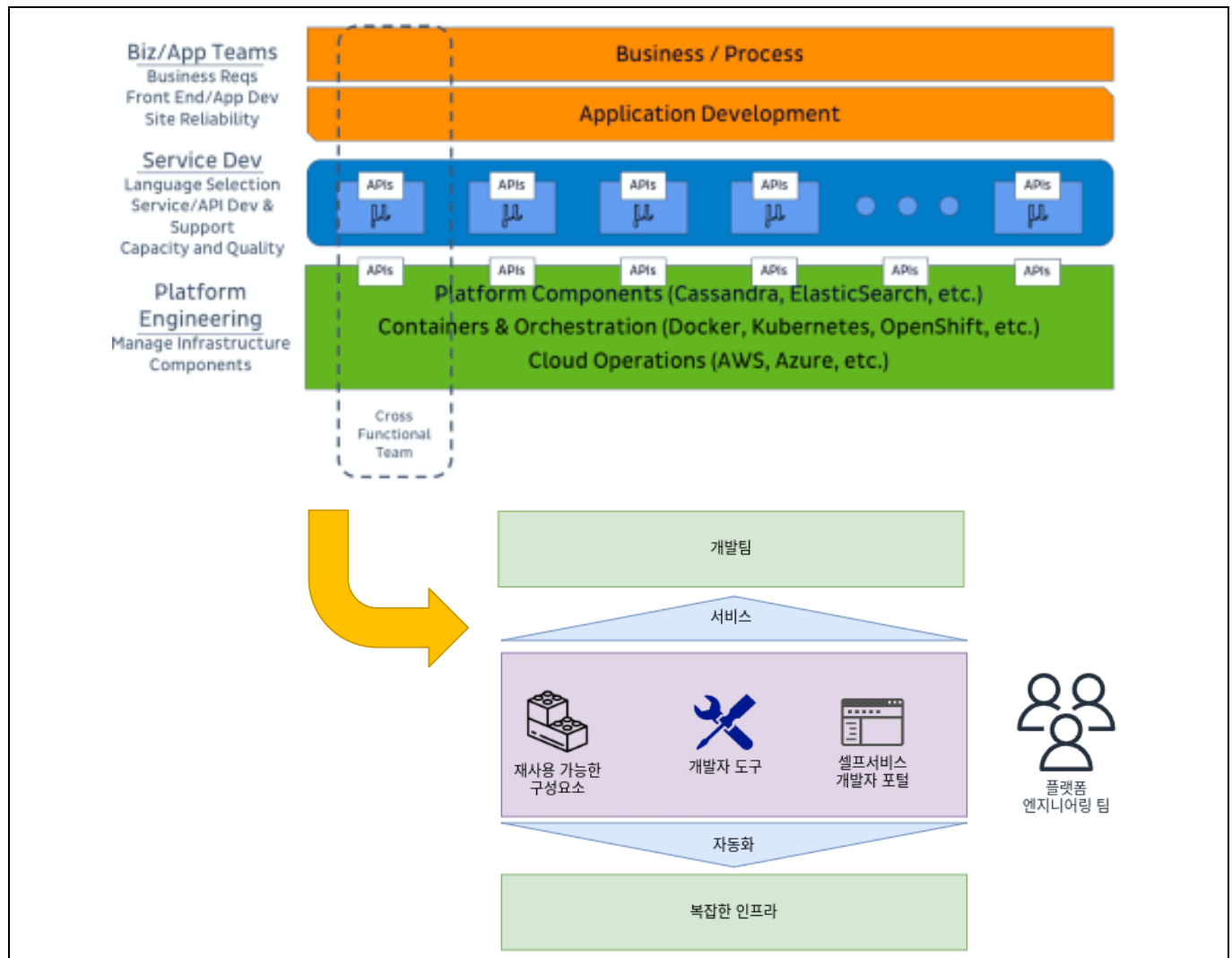


나. 플랫폼 엔지니어링(Platform Engineering)의 등장 배경

등장 배경	설명
소프트웨어 다양성과 복잡성의 증가	- 효율적으로 애플리케이션의 빠른 배포가 필요하지만 소프트웨어 복잡성의 증가로 수행 과정에서의 마찰 감소 필요
개발 생산성 향상	- 개발자와 다른 이해관계자가 전체 개발 주기에서 가능한 최소의 오버헤드(overhead)를 통해 가치 있는 소프트웨어 생산할 수 있도록 지원
일관되고 자동화된 워크로드(workload)	- 리포지토리(repository)와 같은 인프라 요소를 유지 관리하고 단위 테스트에서 생산까지 전 CI/CD 파이프라인의 일관성 유지

II. 플랫폼 엔지니어링(Platform Engineering)의 구성과 역할

가. 플랫폼 엔지니어링(Platform Engineering)의 구성도



- 플랫폼 엔지니어링(Platform Engineering)은 Cross Functional Team으로 구성하여 각 계층의 커뮤니케이션이 원활하게 이루어지는 조정자 역할을 수행

나. 플랫폼 엔지니어링(Platform Engineering)의 역할

역할	설명
인프라 자동화	- Terraform, Ansible등의 도구를 이용하여 IaC(Infra as a Code)를 적용하여 인프라 관리의 자동화 구현
분산 시스템 설계	- MSA(Micro Service Architecture), 분산 시스템 등의 기술과 원칙을 이해하고 이를 지원할 수 있는 인프라, 소프트웨어 플랫폼의 설계
확장성과 성능 최적화	- Caching, Load balancing, Sharding과 같은 기술 이해하고 설계 반영
모니터링 및 로깅	- 로깅, 모니터링 및 경고 시스템을 구축하여 실시간으로 시스템을 모니터링하고 디버깅 진행
보안	- Best Practices에 해당하는 보안 사례를 발굴 및 이해하고 네트워크 분할, 방화벽, 적절한 보안 솔루션 도입과 조치 실현

III. DevOps와 Platform Engineering과 Site Reliability Engineering의 개념과 목적 비교

구분	개념도	목적
DevOps		<ul style="list-style-type: none"> - 개발 및 운영 팀을 통합하고 도구, 시스템 및 반복 프로세스를 사용하여 피드백 주기를 단축하는데 중점
Platform Engineering		<ul style="list-style-type: none"> - 플랫폼 엔지니어링 팀은 개발자의 생산성을 높이는 데 도움이 되는 도구와 프로세스를 구축하는 일을 담당 - 플랫폼 엔지니어링 팀은 소프트웨어 엔지니어링 원칙을 적용해 소프트웨어 제공을 가속화
Site Reliability Engineering		<ul style="list-style-type: none"> - SLO, SLA 및 오류 예산과 같은 비즈니스 수준 목표를 사용하여 서비스가 사용자 기대에 충족되고 안정되도록 하는데 중점

“끝”

10	공공기관 클라우드 컴퓨팅 서비스 이용		
문제	「행정기관 및 공공기관의 클라우드 컴퓨팅 서비스 이용 기준 및 안전성 확보 등에 관한 고시」의 서비스 운영 분야 안전성 검토 항목		
도메인	법, 가이드	난이도	상 (상/중/하)
키워드	자체 관제체계, 비상연락체계, 실시간 모니터링, 장애 대응 및 위험관리, 계정 및 보안관리		
출제배경	행정안전부고시 제2023-23호, 2023. 4. 12., 일부개정에 따른 안전성 항목 확인		
참고문헌	https://www.law.go.kr/LSW/main.html (법제처 국가법령정보센터)		
해설자	BP반 김찬일 기술사(제 130회 정보관리기술사 / s2carey@naver.com)		

I. 행정기관 및 공공기관의 클라우드 컴퓨팅 서비스 이용 기준 및 안전성 확보 등에 관한 고시

근거법령	제정이유
전자정부법 제 54 조의 2	- 행정기관 및 공공기관에서 클라우드컴퓨팅서비스를 안전하게 이용할 수 있도록 이용 기준 및 안전성 확보 등에 필요한 세부사항을 정하기 위함.

- 안전성 검토 항목(제 10 조, 제 12 조 관련) 서비스 운영 분야 안전성 검토 항목 존재

II. 서비스 운영 분야 안전성 검토 항목

1. 자체 관제체계	운영 현황	- 24시간 운영 방안, 관제 인력 및 휴일·야간 관제·모니터 요원 상주 등 현황
	환경 구성	- 자체 연중 24시간 관제를 위한 별도 장소 및 환경 구성
2. 비상 연락 체계	전파 대상	- 장애 시 운영서비스 제공자의 자체 전파 및 전파대상에 이용기관 담당자 포함
	비상연락망	- 기관 유지보수·협력업체 및 기술지원 엔지니어 등 명단 및 연락처 확보 현행화
3. 실시간 모니터링	툴 보유	- MSP 자체 주요 리소스에 대한 모니터링 툴 운영
	외부 지원	- URL, Port 같은 서비스 모니터링
	내부 지원	- Apache, Tomcat, Mysql 등 모니터링
	관제 항목	- CPU 및 Memoery 사용률, Disk 가용량, Network Traffice, URL Check, Process, Log 관제 등 항목구성
	애플리케이션	- JAVA, PHP, Node.js 등 애플리케이션 성능 관리 모니터링 ※APM 도입(웹서비스 동작 상태 및 성능, 미들웨어 트랜잭션 사용시간 분석 등)
	CSP	- CSP별 인프라, WAF, VPN, 전용회선, CDB 등 CSP 제공사품 모니터링
	안내 주기 및 임계치 설정	- 주기 설정(실시간, 1~5분 등) 및 등록된 담당자에 안내, 임계치 설정 후 초과 시 알람 가능 여부 및 수단(SMS, 메일 등)
4. 장애 대응 및 위험 관리	현황 보고	- 운영 현황 보고서 작성 및 보고
	조직 구성	- 실시간 고객 요구 수렴 접수 및 처리 등 고객 대응 관리체계 운영
	사전 예방 교육	- 서비스 문제 발생 사전 확인 및 장애 방지대책 운영
	백업 및 복구	- 장애 대응 모의훈련, 시나리오 수립 및 이용자 교육
5. 계정 및 보안관리	장애 발생 시 신속한 복구를 위한 장애 대응 체계 및 복구 후 서비스 개선	- 장애 발생 시 신속한 복구를 위한 장애 대응 체계 및 복구 후 서비스 개선
	서버	- 서버 접속정보를 열람 권한 정책 및 사용기록, 계정 관리솔루션 이용
	인프라 서비스 제공자	- 업무 및 역할에 따른 클라우드 관리 콘솔 계정 부여
	접근통제	- UTM, F/W, VPN, IPS 등의 보안시스템 구축
	PC 보안	- P2P 프로그램, 웹하드 등 비인가프로그램, 유해사이트에 대한 접속 차단 및 백신설치 운영
	인력 보안	- 업무에 관한 비밀 유지 및 내부 인력 보안 교육

“끝”

11	Agile		
문제	애자일(Agile) 소프트웨어 개발의 장점 및 단점		
도메인	소프트웨어공학	난이도	하 (상/중/하)
키워드	Manifesto, Principles, 개변동고, 고요배의 동대소지 중단자호		
출제배경	소프트웨어 개발 방법론인 Agile의 장점 및 단점에 대한 이해 점검		
참고문헌	ITPE 서브노트		
해설자	BP반 김찬일 기술사(제 130회 정보관리기술사 / s2carey@naver.com)		

I. 점진적 상세화, Agile의 개념

- 효율적인 제품, SW 개발을 위해 절차보다는 사람과 제품에 집중하여 낭비를 제거하고 고객의 요구사항을 보다 유연하고 신속하게 반영하기 위한 방법론

II. 애자일(Agile) 소프트웨어 개발의 장점 및 단점

가. 애자일(Agile) 소프트웨어 개발의 장점

장점	설명
ROI 증대	- 고객들에게 가치 있는 기능들을 빠르고 안정적으로 전달
Delivery Time 감소	- 요구사항의 변화를 유연하게 수용함으로써 Time to Market 실현
창의성 향상	- 팀 자율성 강화를 통한 업무만족도와 창의성 향상
생산성 향상	- 불필요한 산출물 제거 및 팀 협업 강화
제품 품질 향상	- 고객의 주기적 피드백 및 빈번한 테스트

- 이러한 장점이 있지만, 단점도 존재하기에 소프트웨어 개발에 적합한 방법론을 적용하여 완수하는것이 중요

나. 애자일(Agile) 소프트웨어 개발의 단점

단점	내용
체계적인 문서화 및 지침 부족	- Agile 프로세스 적용을 지원하는 문서화나 구체적인 지침 부족 - 전체 제품에 대한 통합과 테스트에 대한 가이드가 부족
요구사항 변경에 의한 오버헤드	- 비기능적인 요구사항에 대한 고려가 부족 - 요구사항의 잦은 변경에 따른 테스트 수행노력 증가
사업 관리 부분 미흡	- 측정지표가 개발자 위주로 상위관리자의 요구를 충족하기 어려움 - 프로젝트 리스크 관리 (Risk management)에 대한 고려 부족
감리 대응 문제	- 기존 방법론에 비해 적은 문서량, 감리 기준에 부합되지 않는 산출물로 이슈 발생

- 애자일 기법 세부 유형도 존재하며 각각의 장단점이 존재함.

III. 주요 애자일(Agile) 유형 장단점 설명

구분	장점	단점
----	----	----

스크럼 (Scrum)	- 짧은 스프린트로 빠른 피드백	- 고정된 스프린트로 유연성 부족
칸반 (Kanban)	- 작업 흐름 시각적 관리	- 장기 계획 수립 어려움
XP	- 유연한 계획 수립	- 높은 고객 참여 요구

- 각각의 유형에 따라 적절한 기법 선택 필요

“끝”

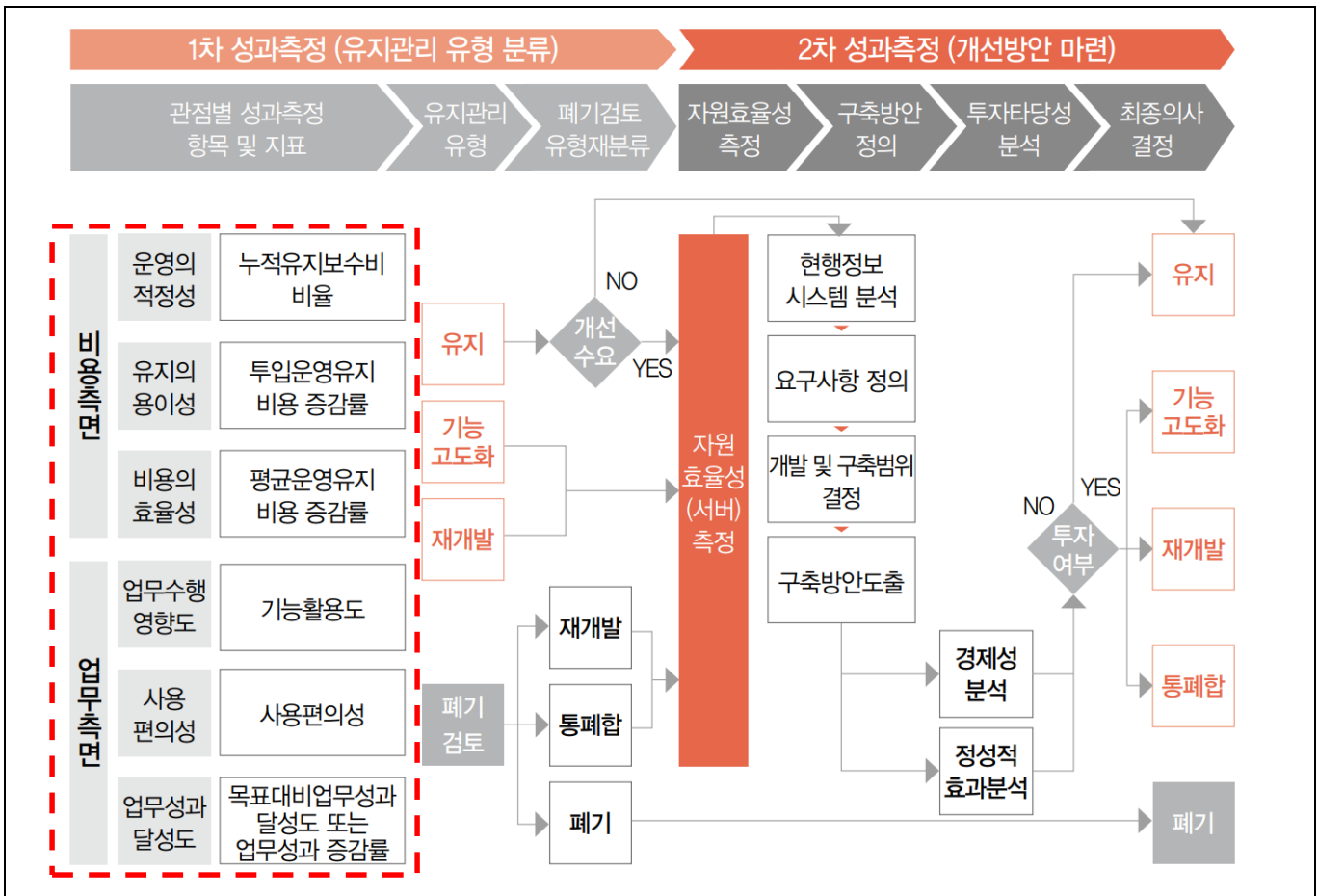
12	전자정부 정보시스템 성과 측정지표		
문제	전자정부 정보시스템 성과 측정지표		
도메인	사업관리	난이도	상(상/중/하)
키워드	비용측면, 업무측면		
출제배경	정보시스템 운영 성과를 측정하기 위한 구체적인 기준과 절차, 방법 등을 상세 내용 이해		
참고문헌	정보시스템 운영 성과측정 매뉴얼(2017.04)		
해설자	정주행 조종흥 기술사(제127회 정보관리기술사 / choheung@naver.com)		

I. 전자정부 정보시스템 성과 측정지표의 목적

- 비용과 업무 관점 별 성과측정을 통해 정보시스템의 유지관리 유형을 분류하고 폐기검토 대상 정보시스템에 대한 유형 재분류를 통하여 상세 유형을 식별을 할 수 있음
- 이를 통해 정보시스템의 운영성과를 객관적으로 판단하고 그 결과에 따라 정보시스템의 운영 및 개선과 관련하여 합리적 의사결정을 지원하는데 목적이 있음

II. 정보시스템 운영 성과측정 모델 및 측정을 위한 기초데이터 확보

가. 정보시스템 운영 성과측정 모델



- 비용측면과 업무측면 성과측정 항목 및 지표로 구성됨

나. 측정을 위한 기초데이터 확보 방안

측정 관점	측정항목	측정지표	기초데이터
비용	운영의 적정성	누적 유지보수비 비율	초기개발비
	유지의 용이성	투입 운영유지비용 증감률	추가개발비
	비용의 효율성	평균 운영유지비용 증감률	유지보수비
업무	업무수행 영향도	기능 활용도	운영비
	사용상의 편의성	사용 편의성	시스템 유형
	업무성과 달성도	업무성과 증감률	접속자 수
		목표대비 업무성과달성도	데이터 업데이트 수
			응용기능
			응용기능 활용현황(접속건수, 데이터량)
			사용자 만족도(편의성)
			업무성과목표, 지표별 결과

- 비용 측면의 기초데이터를 범정부 EA포털(GEAP)에 입력하여 관리하고 GEAP내 정보시스템 운영 성과측정 기능을 사용하여 측정하는 경우 비용측면의 기초데이터는 운영 성과측정 시 자동 반영됨.

“끝”

13	소프트웨어 품질성능 평가시험		
문제	소프트웨어 품질성능 평가시험		
도메인	소프트웨어공학	난이도	중(상/중/하)
키워드	소프트웨어진흥법 제55조		
출제배경	소프트웨어 품질 성능 평가 개념 확인		
참고문헌	ITPE 기술사회 자료집, 127회 Final Round		
해설자	정주행 조종흥 기술사(제127회 정보관리기술사 / choheung@naver.com)		

I. 소프트웨어 품질성능 평가시험 개념

개념	소프트웨어 품질성능 평가시험이란 동종의 경쟁 제품간 기능 및 성능 비교 평가를 통해 사용자의 요구사항을 만족하고 품질 및 성능이 우수한 제품을 가려내는 시험
법적근거	<ul style="list-style-type: none"> - 소프트웨어 진흥법 제55조(상용소프트웨어 품질성능 평가시험) - 국가기관등의 장은 상용SW를 직접 구매하려는 경우 품질성능 평가시험을 직접 하거나 지정시험기관에 대행하게 하여 그 결과를 제품구매에 반영해야 함
시행목적	<ul style="list-style-type: none"> - 구매자에게는 우수제품 선택 기회를 제공하고, 개발자에게는 자사 제품 강점 파악 및 취약점 보완 기회를 제공 - 가격, 인지도, 영업력 또는 특정 제품 선호 풍토 등 제품 품질 이외의 요소로 제품을 평가하는 것을 방지하고 발주기관의 요구사항을 만족하는 품질과 성능이 우수한 제품을 선택할 수 있도록 하기 위함

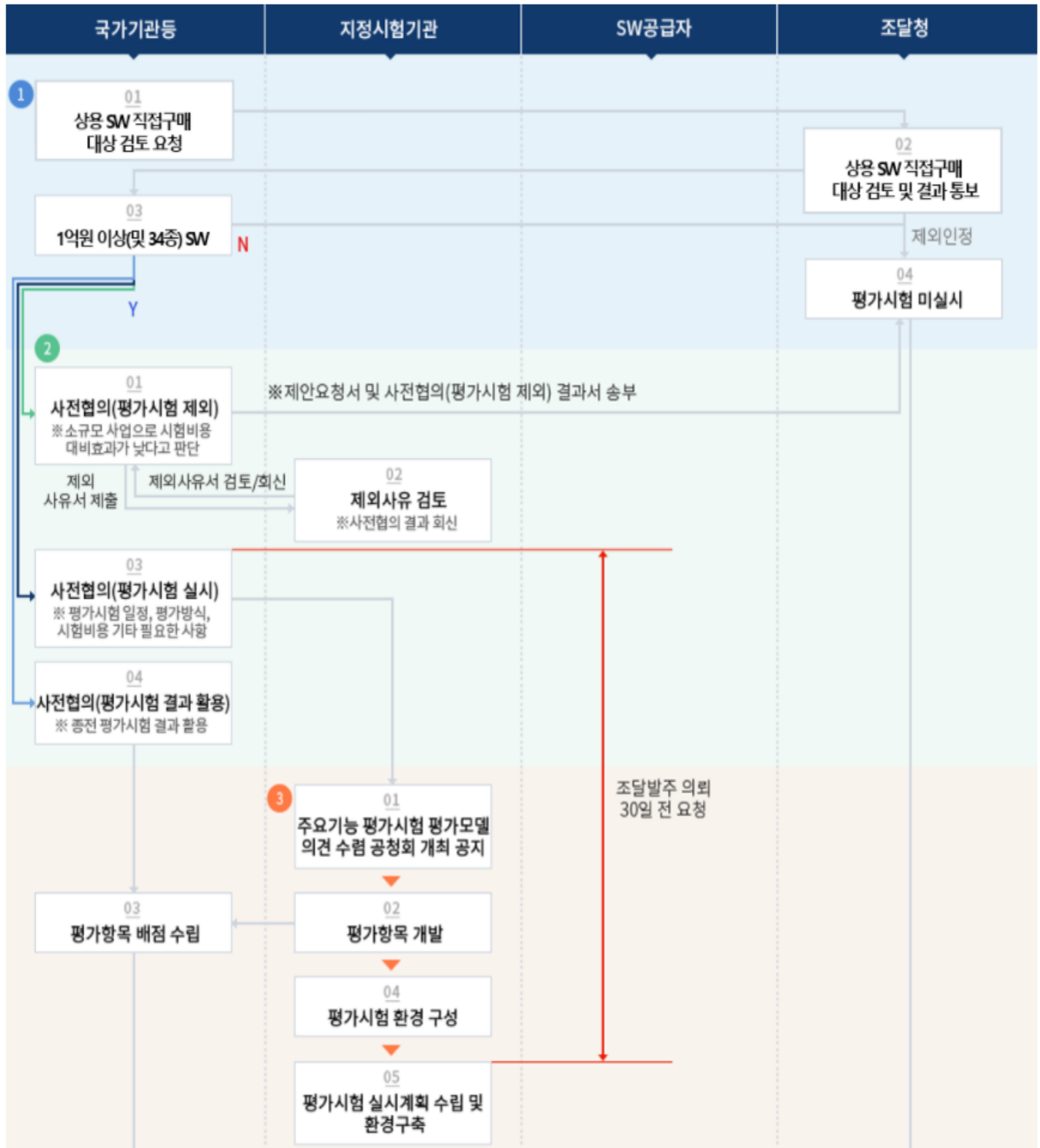
II. 상용소프트웨어 품질 성능 평가 시험 적용 대상

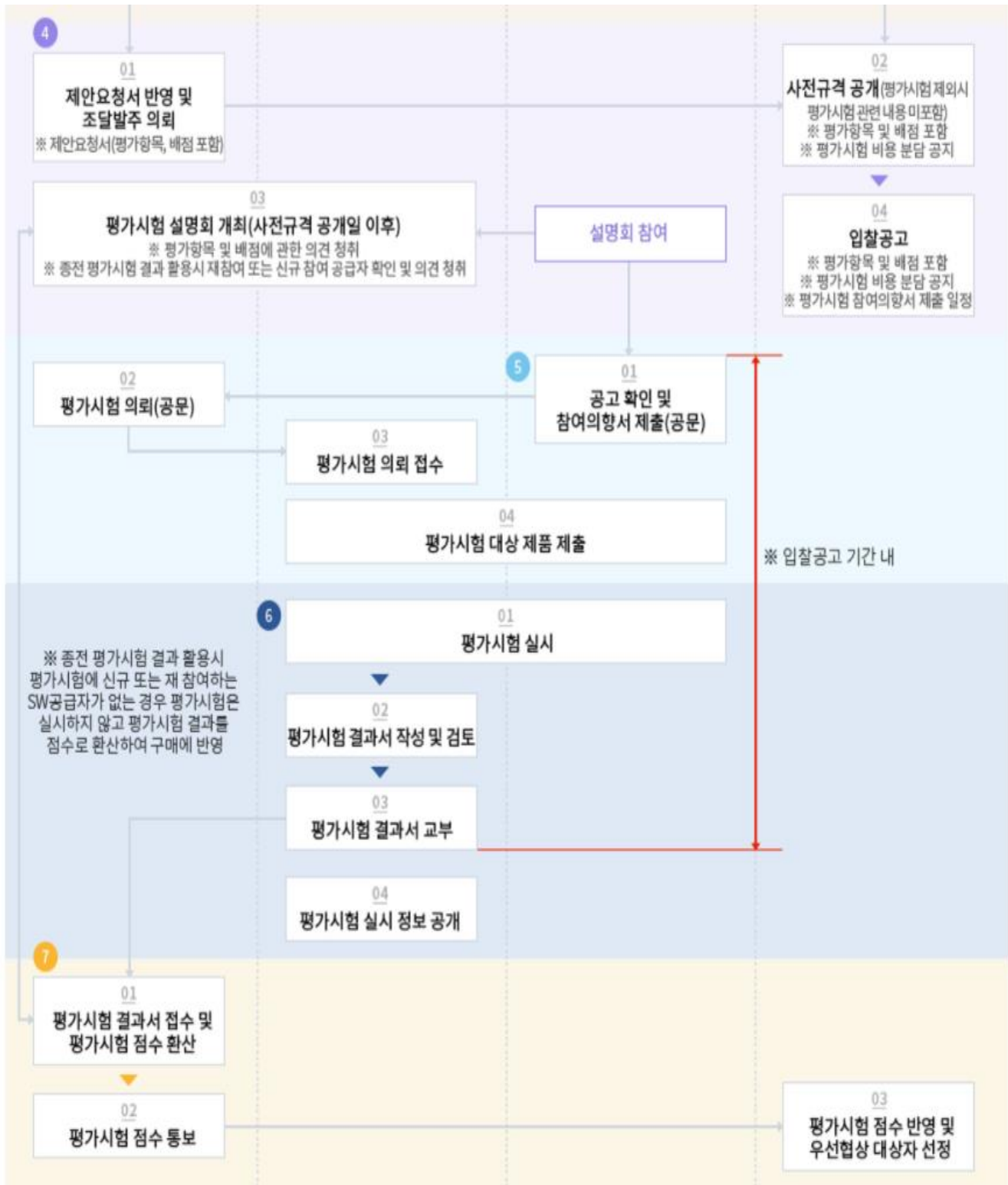
평가시험 대상	<ul style="list-style-type: none"> - 법적근거: 소프트웨어 품질성능 평가시험 운영에 관한 지침(제7조) 1. 경쟁입찰을 통한 직접구매 대상 상용SW 제품 중 구매금액 1억원 이상(부가가치세 포함)으로서 별표3(대상분야 34종)에 해당하는 SW 제품 다만, 2. 「소프트웨어사업 계약 및 관리감독에 관한 지침」 제8조제3항의 경우 SW 구매금액 2억원 이상으로서 별표3에 해당하는 해당하는 소프트웨어 제품만을 대상으로 함 * 제8조3항 (SW사업 총3억이상(부가가치세 포함)이고 5천이상(부가가치세 포함)인 다음 SW제품. - 국가종합전자조달시스템 종합쇼핑몰 등록(5천만 미만도 포함) SW, GS, CC, NET, NEP, 5천미만인 경우 총금액 5천 초과인 경우) 3. 제7조에서 정한 평가시험 대상에 해당하지 않는 경우에도 국가기관등이 필요하다고 판단하는 경우에는 평가시험을 수행할 수 있다.
---------	---

- 대상 소프트웨어 분야로는 시스템 SW, 개발용 SW, 응용 SW로 구분하여 적용

III. 평가시험 절차

가. 평가시험 절차 흐름도





나. 평가시험 절차 상세설명

절차	설명
1. 평가시험 대상 검토 단계	01. 상용 소프트웨어 직접구매 대상 검토 요청 (국가기관등) 02. 상용 소프트웨어 직접구매 대상 검토 결과 송부 (조달청) 03. 평가시험 의무화 대상 검토 (국가기관등) 04. 평가시험 미실시.
2. 사전협의 단계	01. 평가시험 사전협의 요청 - 평가시험 제외 (국가기관등 → 지정시험기관) 02. 평가시험 제외 사유 검토 (지정시험기관) 03. 평가시험 사전 협의 요청 - 평가시험 실시 (국가기관등 → 지정시험기관) 04. 평가시험 사전 협의 요청 - 종전 평가시험 결과 활용 (국가기관등 → 지정시험기관)
3. 평가시험 설계 단계	01. 국가기관등의 요구사항 및 운영 시스템 분석 (지정시험기관) 02. 평가항목 개발 (지정시험기관) 03. 평가항목 배점 수립 (국가기관등) 04. 평가시험 환경 구성 (지정시험기관) 05. 평가시험 실시 계획 수립 및 평가시험 환경 구축 (지정시험기관)
4. 조달발주 단계	01. 제안요청서에 평가항목 및 배점 반영 (국가기관등) 02. 사전규격 공개 (조달청) 03. 평가시험 설명회 개최 (지정시험기관, 국가기관등) 04. 입찰공고 게재 (조달청)
5. 평가시험 의뢰 단계	01. 평가시험 참여 의향서 제출 (SW공급자) 02. 평가시험 실시 의뢰 (국가기관등) ※ 평가시험 의뢰공문(의뢰서) 03. 평가시험 의뢰 접수 및 평가시험 실시 준비 (지정시험기관) 04. 평가시험 대상 제품 제출 (SW공급자 → 지정시험기관)
6. 평가시험 실시 단계	01. 평가시험 실시 (지정시험기관/SW공급자) 02. 평가시험 결과서 작성 및 검토 (지정시험기관) 03. 평가시험 결과서 교부 (지정시험기관 → 국가기관등) 04. 평가시험 실시 정보 공개 (지정시험기관)
7. 평가시험 결과 반영 단계	01. 평가시험 결과서 접수 및 평가시험 점수 환산 (국가기관등) 02. 평가시험 점수 통보 (국가기관등 → 조달청) 03. 평가시험 결과를 기술성평가에 반영 및 우선협상대상자 선정 (조달청)

- 7단계 절차를 기반으로 상용 소프트웨어 평가시험 진행

“끝”



ITPE 기술사회

제134회 정보처리기술사 기출문제 해설집

대 상	정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사, 정보시스템감리사 시험
발행일	2024년 07월 27일
집 필	강정배PE, 전일PE, 백현PE, 조종흥PE, 정상PE, 김찬일PE
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

본 저작물은 [ITPE\(아이티피이\)](#)에 저작권이 있습니다.

저작권자의 허락없이 **본 저작물을 불법적인 복제 및 유통, 배포**하는 경우
법적인 처벌을 받을 수 있습니다.