ICT의 가치를 이끄는 사람들!!

126회

컴퓨터시스템응용기술사 기출풀이 3교시

T 02.724.1831 E kpcitpe@kpc.or.kr H www.kpc.or.kr C cafe.naver.com/kpcitpe

국가기술자격 기술사 시험문제

정보처리기술사 제 126 회 제 3 교시

분야	정보처리	종목	컴퓨터시스템응용	수험번호	.	성명	

※ 다음 문제 중 4 문제를 선택하여 설명하시오. (각 25 점)

1. 행정안전부에서는 공공기관 등이 정보시스템 사업을 추진할 때 SW 보안약점을 제거하기 위해 사용하는 "소프트웨어 개발 보안 가이드"를 개정(2021 년 11 월) 하였다. 이와 관련하여 다음을 설명하시오.
   가. 소프트웨어 개발 보안의 정의, 대상 및 범위
   나. 소프트웨어 설계 단계 보안 기준 중"보안기능 입력값 검증"과 "업로드·다운로드 파일 검증"의 개념 및 보안 대책

2. 최근 개인정보를 활용하는 서비스들이 증가하면서 개인정보에 대한 보호가 중요해지고 있다. 이와 관련하여 ISO/IEC 29100 프라이버시 11 개 원칙과 ISO/IEC 27701 개인정보 보호 시스템에 대한 인증 및 평가에 대하여 각각 설명하시오.

3. 드론과 사용자간의 무선통신을 위해 신호다중화 기술 중 FHSS(Frequency Hopping Spread Spectrum)와 DSSS(Direct Sequence Spread Spectrum) 통신방식을 활용하고 있다. 이와 관련하여 다음을 설명하시오.
   가. 드론 무선통신을 위한 신호 다중화의 개요와 필요성
   나. FHSS
   다. DSSS

4. 플래시 메모리(Flash Memory)에 대하여 다음을 설명하시오
   가. 플래시 메모리의 개요와 구조
   나. 스케일다운 한계와 대응방법
   다. 3D-Vertical NAND Flash Memory

5. 마이데이터 서비스에 대하여 다음을 설명하시오
   가. 서비스절차
   나. 마이데이터 인증 방식
   다. 보안 문제점 및 개선 방안

6. 휴대용 전자기기 및 전기자동차 등의 확대로 인해 무선으로 전력을 전송하여 배터리를 충전하는 무선 충전기술이 주목받고있다. 이와 관련하여 다음을 설명하시오.
   가. 무선충전기술의 개요
   나. 무선충전기술 유형별 사용 주파수, 전송거리 및 효율, 인체 유해성, 주요 사용분야 측면에서 비교
   다. 무선충전기술 사용에서 발생 가능한 보안 문제점

문 제	1. 행정안전부에서는 공공기관 등이 정보시스템 사업을 추진할 때 SW 보안약점을 제거 하기 위해 사용하는 "소프트웨어 개발 보안 가이드"를 개정(2021 년 11 월) 하였다. 이와 관련하여 다음을 설명하시오. 가. 소프트웨어 개발 보안의 정의, 대상 및 범위 나. 소프트웨어 설계 단계 보안 기준 중 "보안기능 입력값 검증"과 "업로드・다운로드 파일 검증"의 개념 및 보안 대책		
출 제 영 역	보안	난 이 도	★★★★☆
출 제 배 경	- 소프트웨어 보안약점 기준(제 57 조) 개정에 따른 소프트웨어 개발 보안 가이드 개정		
출 제 빈 도	- 관리(114 회 2 교시), 응용(101 회 2 교시), 모의고사/합숙 빈출		
참 고 자 료	- 소프트웨어 개발보안 가이드 (2021.11)		
Keyword	- 시큐어코딩, 감리대상 사업(전자정부법 71 조 1 항), 신규개약, 유지보수, log4j		
풀 이	이정현(125 회 정보관리기술사)		

1. 소프트웨어 개발 보안의 정의, 대상 및 범위

가. 소프트웨어 개발 보안의 정의

필요성	개발 측면 - 시큐어코딩 표준 확립 - 보안 라이브러리 재사용	안전 측면 - 생명주기 전반 보안활동 수행 - SW 보안 교육
	공공 측면 - 개인정보, 민감정보 탈취 방지 - 민원인 만족도 향상	민간 측면 - 주요 기밀정보 유출방지 - 보안약점, 취약점 사전대응
정의	- SW 개발과정에서 개발자의 실수・논리적오류로 발생가능한 보안 취약점, 보안 약점들을 최소화하여 사이버 보안 위협에 대응 할 수 있는 안전한 SW 를 개발하기 위한 보안 활동	

- 행정기관/공공기관 정보시스템 구축 운영 지침에서 안전 SW 개발을 위해 개발보안 대상 및 범위를 지정

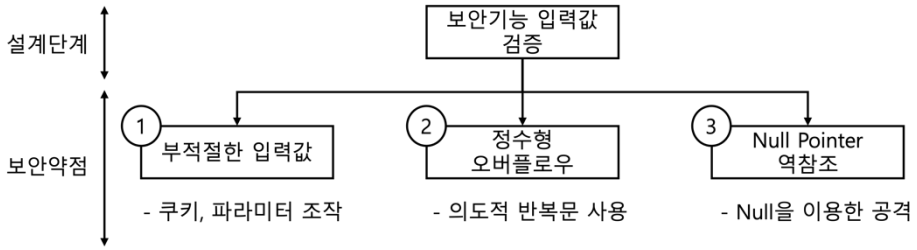
나. 소프트웨어 개발 보안의 대상 및 범위

구분	주요사항	법적근거
대상	- SW 개발자・운영자 - 정보시스템 감리대상 사업 - 자체 SW 개발 보안 적용	- 전자정부법 시행령 71 조 1 항
범위	- 신규개발의 경우 - 유지보수의 경우 - 상용 소프트웨어 제외	- 행정기관 및 공공기관 정보시스템 구축・운영 지침 제 50 조, 57 조

- 분석단계에서 식별된 요구사항 정의서를 기반으로 설계단계에 적용, 입력데이터 유효성 체계와 처리방법을 설계
- 설계단계에서 보안항목 반영하지 못한 경우 구현단계에서 5 배, 제품 출시 이후 30 배의 추가비용 발생 예측

2. 보안기능 입력값 검증의 개념 및 보안대책

가. 보안기능 입력값 검증의 개념 및 보안대책

개념도	
개념	- 보안기능 입력값과 함수의 외부 입력 값 및 수행결과에 대한 유효성 검증 및 유효하지 않은 값에 대한 처리방법을 설계하는 개발보안활동

- 보안기능은 인증 대상 방식, 비밀번호, 접근통제, 암호키, 중요정보에 활용되는 사용자 입력값을 의미

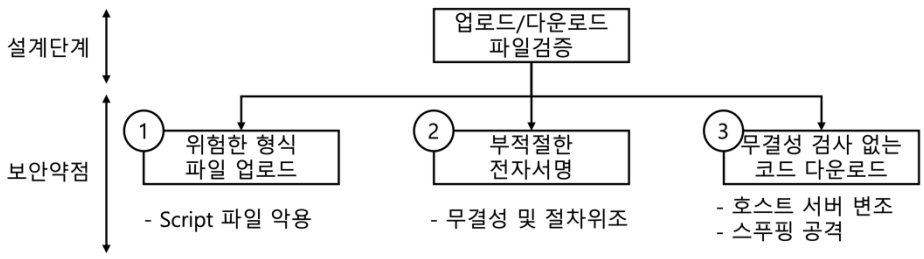
나. 보안기능 입력값 검증의 개념 및 보안대책

보안약점	보안대책	설 명
1. 부적절한 입력값	**- 사용자 중요정보 관리방안**	- 상태, 인증, 권한정보 서버측 DB 저장 사용 설계
	- 보안기능 매개변수 제한	- 쿠키, 환경변수, 파라미터 검증 작업 수행 설계
	- 주요정보 암호화 전송	- 개인정보, 권한정보에 대한 보호대책 수립
2. 정수형 오버플로우	**- 시스템 오류 페이지 숨김처리**	- 오류스택, 로그 통한 침투경로 사전차단
	- 데이터 값 범위 검증	- 극단치 및 무의미 값 제거, 시큐어코딩 적용
	- 반복문 제어 및 메모리 보호방안	- while 문 사용금지, 스택가드, 스택쉴드, ASLR 도입
3. Null Pointer 역참조	**- 객체 Null 예외방안 수립**	- 공격자가 예외상황 이용, 별도오류페이지로 변경
	- 모의해킹 및 취약점 테스트 수행	- 사내 주기적 모의침투공격 통한 취약점 도출
	- 예외상황 악용 대응방안 수립	- 설계 초기부터 시큐어코딩 표준화 방안 수립

- 공격자는 사용자 및 접근용이성이 높은 업로드/다운로드 파일을 악용하므로, 보안대책 필요

3. 업로드・다운로드 파일 검증의 개념 및 보안대책

가. 업로드・다운로드 파일 검증의 개념

개념도	
개념	- 파일의 무결성, 실행권한 등에 관한 유효성 검증방법 및 부적합한 파일에 대한 처리방 방법을 설계하는 개발보안활동

- 파일 검증 미비시 공격자는 변조파일을 이용해 서버권한을 탈취하여 공격 가능
- 최근 발생한 Log4j 쉘 취약점도 같은 맥락으로 보안 취약점을 악용하는 점을 염두하여, 초기 설계부터 집중 필요.

나. 업로드 · 다운로드 파일 검증의 보안대책

보안약점	보안대책	설 명
1. 위험한 형식 파일 업로드	- 서버 스크립트 파일 제한	- asp, jsp, php 파일 업로드 불가토록 설계
	- 업로드 파일 필터링 방안	- 사전 현업/고객과 업로드 파일 선정
	- 다운로드 파일 취약점 검증	- 다운로드 요청시 파일명에 대한 검증 수행
2. 부적절한 전자 서명	- 사용자 인증 및 이중화 대책	- Token 인증과 탈취 방지위한 사이버디셉션 도입
	- 전자서명 위변조 판별	- 전자서명 사용시 파일의 출저 확인
	- 전자서명 주체 신뢰여부 판단	- 객체(jar, dll)등의 전자서명 여부 판단을 고려
3. 무결성 검사 없는 코드	- 코드 검사 솔루션 대응	- 악성코드 탐지 정적/동적도구 사용방안
	- 무결성 확보대책 마련	- 파일 생성일, 크기, 권한, 타입 통한 무결성 확인
	- 캡처 기반 코드 검증 도구	- 코드 변경사항 사전 확인 및 취약점 제거

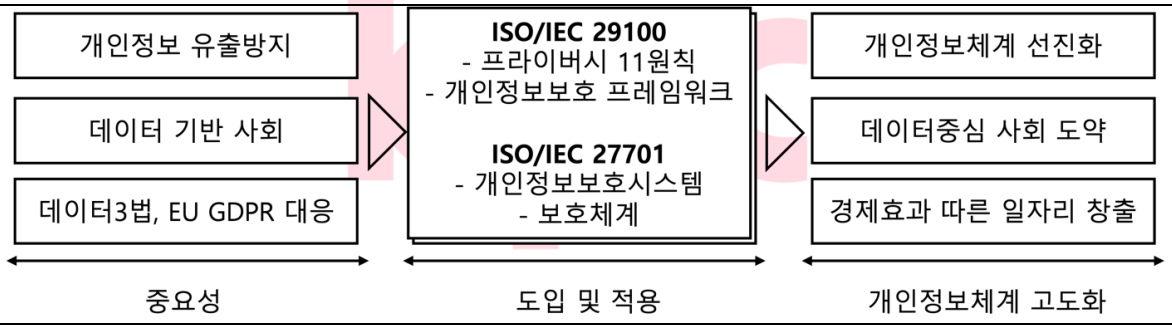
- 공격자 측면에서 접근성이 쉬운 보안기능 입력값과 업로드 파운로드 파일 취약점을 악용
- 초기 개발보안 설계 기준(20 개)을 만족시 구현 기준(49 개)의 대한 보안 취약점 제거 가능. "끝"

기출풀이 의견

1. "소프트웨어 개발보안 가이드 개정" 이란 문구로 혼란을 준 함정문제로 보입니다. 그러나 개정내용이 아닌, 기존 가이드에서 문제를 출제한 것으로 보아, 충실하게 가이드를 숙지하신 응시자는 고득점을 예상합니다.

문 제	**2. 최근 개인정보를 활용하는 서비스들이 증가하면서 개인정보에 대한 보호가 중요해지고 있다. 이와 관련하여 ISO/IEC 29100 프라이버시 11 개 원칙과 ISO/IEC 27701 개 인정보 보호 시스템에 대한 인증 및 평가에 대하여 각각 설명하시오.**		
출 제 영 역	보안	난 이 도	★★★☆☆
출 제 배 경	- EU GDPR 2021.6 적용으로 ICT 제품 및 서비스 프로세스에 대한 개인정보체계 중요성 대두		
출 제 빈 도	- 관리(125 회 3 교시, 121 회 3 교시, 120 회 4 교시)		
참 고 자 료	- 국제 개인정보보호 표준화 동향 https://www.koreascience.or.kr/article/JAKO202025551105303.pdf - EU-GDPR 을 대비한 개인정보보호 인증제도의 개선방안		
Keyword	- EU GDPR, 데이터 3 법, ISMS-P, ISMS, PIM, 프라이버시 보호원칙, ISO/IEC 27001 확장판		
풀 이	이정현(125 회 정보관리기술사)		

1. 개인정보 활용 서비스 증가, 개인정보보호의 중요성



- 최근 메타버스, 블록체인, AIoT 등 신기술과 개인정보의 관계는 상호융합 통한 폭발적 시너지로 작용
- ISO/IEC 29100 은 프라이버시 프레임워크를 제시, 특히 프라이버시 보호 11 원칙 통해 사전 설계 마련가능

2. ISO/IEC 29100 프라이버시 11 원칙

가. ISO/IEC 29100 프라이버시 프레임워크

프레임워크	
개념	- 프라이버시 관련 용어, 개인정보처리 주체 역할, 보호 요구사항과 프라이버시 보호 원칙을 포함한 프라이버시 프레임워크

- 초기 프라이버시 프레임워크 구축시 프라이버시 11 원칙을 기반으로 보호체계를 마련

나. ISO/IEC 29100 프라이버시 11 원칙 상세

구분	프라이버시 11 원칙	설명
이용자 보호 측면	1. 동의와 선택	- 서비스 선택의 자율권 보장 관련 원칙
	2. 합법성과 명세성	- 개인정보 이용 목적 합법성과 구체적 제시
	3. 수집 제한의 원칙	- 서비스 이용자 동의하의 수집 수행
무결성 보장 측면	4. 데이터 최소화	- 무결성 보장을 위한 프라이버시 정보 최소화
	5. 이용 및 공개 제한	- 서비스 이용시 최소 개인정보만으로 인증 및 암호화
	6. 정확성과 품질	- 데이터 정확성과 최소 품질 준수 활동 제시
투명성 보장 측면	7 공개성, 투명성	- 안전한 서비스보안 위한 공개성,투명성 확보 원칙
	8. 개별 참여와 접근	- 개인별로 중복치 않고, 접근성의 용이성을 보장
	9. 책임성	- 서비스 및 시스템의 권한에 따른 책임의 따른 원칙
서비스 보호 측면	10. 정보보호	- 안전한 정보보안 정책 및 거버넌스 통한 안전성 확보
	11. 프라이버시 준수	- 비식별 기법 기반 프라이버시 준수 체계 마련

- 초기 프라이버시 11 원칙 기반 프레임워크 적용, 이후 개인정보시스템의 처리체계의 따른 인증 및 평가 필요
- ISO/IEC 27701 은 ISO/IEC 27001 과 27002 의 확장표준이며, KISA 의 ISMS-P(ISMS, PIMS)에서 참조 표준으로 사용

3. ISO/IEC 27701 개인정보보호시스템의 인증 및 평가

가. ISO/IEC 27701 개인정보보호시스템의 인증

구분	인증항목	설명
적법성, 투명성, 공정성	- 법률적 근거 파악	- 데이터 3 법, 개인정보보호법, 정보통신망법등 근거 제시
	- 조직 목적 제시	- ISO/IEC 27001 선행된 상태에서 조직 목적 제시
목적 제한	- 정보 수집 제한	- 최소 개인식별정보 수집하여 목적을 제한
	- 조직 목적 제한	- 전사적 또는 일부조직 목표에 따라 목적을 제한
데이터 최소화	- PII 최소화 목표	- 모든 조직에서 개인식별정보처리(PII) 처리, 최소화 필요
	- PII 비식별화 및 삭제	- 인증시 PII 비식별화 및 삭제 방안의 선행 필요

- ISO/IEC 27701 은 ISO/IEC 27001 과 27002 에 대한 인증이 선행되야 하며 평가항목 만족시 인증 획득

나. ISO/IEC 27701 개인정보보호시스템의 평가

구분	평가항목	설명
개인정보 처리 원칙	- 적법성	- 서비스 선택의 자율권 보장 관련 원칙
	- 투명성	- 개인정보 이용 목적 합법성과 구체적 제시
처리의 적법성	- 타당성	- 무결성 보장을 위한 프라이버시 정보 최소화
	- 안전성	- 서비스 이용시 최소 개인정보만으로 인증 및 암호화
PII (개인식별정보 처리)	- 기록 보호	- 안전한 암호화 또는 비식별 조치로 기록물 보호
	- PII 계약 및 기록	- 개인식별정보 처리 계약 및 사용내역 기록 필수

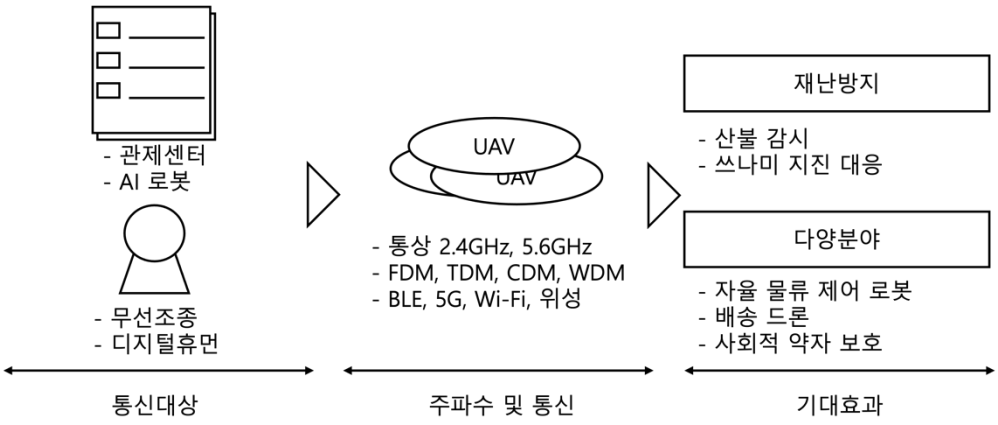
- 최근 서비스 폭발적 증가 및 다양성으로 개인정보보호는 기본활동으로 인지되고 있는 상황
- ISO/IEC 29100, 27701 과 ISMS-P(ISMS, PIMS)와 상호보완적으로 활용하여 MECE 한 개인정보보호체계 구성 "끝"

기출풀이 의견

1. 개인정보 자율점검표, AI 개인정보보호, 데이터 3 법 등에서 표현할 수 있는 키워드로 차별화 유도. 인증 / 평가 부분에선 실무적 관점에서 접근하시면 고득점 예상합니다.

문 제	**3. 드론과 사용자간의 무선통신을 위해 신호다중화 기술 중 FHSS(Frequency Hopping Spread Spectrum)와 DSSS(Direct Sequence Spread Spectrum) 통 신방식을 활용하고 있다. 이와 관련하여 다음을 설명하시오.** **가. 드론 무선통신을 위한 신호 다중화의 개요와 필요성** **나. FHSS** **다. DSSS**
출 제 영 역	네트워크 / 난 이 도 ★★★☆☆
출 제 배 경	- 한국판 뉴딜 2.0 무인항공기, 무인물류제어로봇 지원 확대에 의한 출제 예상
출 제 빈 도	- 응용(125 회 1 교시, 123 회 4 교시)
참 고 자 료	- 드론에서 사용되는 무선기술 https://sharehobby.tistory.com/ - 드론무선통신의 개요 및 이슈 https://csi.dgist.ac.kr/uploads/Publications/Jan2016-KICS.pdf
Keyword	- FHSS(23 개 독립채널, 23 개 시스템채널, Hopping) - DSSS(확산코드, XOR)
풀 이	이정현(125 회 정보관리기술사)

1. 드론 무선통신을 위한 신호 다중화의 개요와 필요성

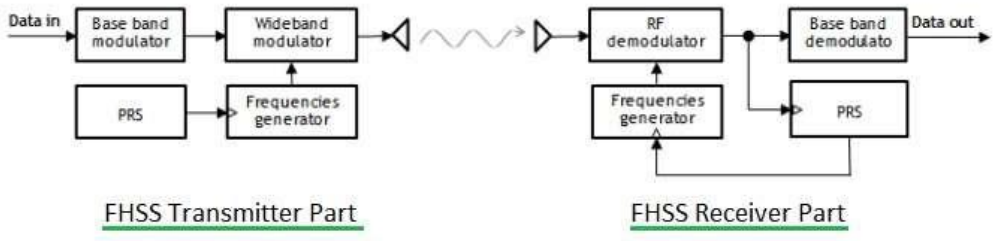
개요	
필요성	- 한국 뉴딜 2.0 디지털뉴딜 중 5G+AI 영역 차지와 새로운 드론 활용방안 모색 - VR, MR, XR 기반 몰입감있는 컨텐츠 제공으로 메타버스 기술 선점 - 사회적 약자, 재난방지, 도시문제 해결등 긍정적 효과 발휘

- 과거 인간이 원격환경 또는 주변에서 컨트롤했다면 현재 5G, LTE + FHSS, DSSS 통해 최대 2km 까지 조종 가능
- 특히 최근 드론의 거점 충전소 마련 및 구축으로 24 시간 운행하는 것이 가능해져 관심이 증가

-드론에서 보편적으로 활용하는 신호다중화 기술로서 FHSS(Frequency Hopping Spread Spectrum)와 DSSS(Direct Sequence Spread Spectrum)을 주로 사용.

2. FHSS 의 개념과 동작원리

가. FHSS 의 개념

개념도	
개념	- 23 개의 독립채널과 시스템 자동할당 채널 23 개 채널 전체에 걸쳐 Hopping 으로 무작위 주파수로 데이터를 송수신하는 대역확산 변조 기술

- FHSS 는 잡음 및 전파간섭이 적고, 약 18dB 의 SNR(Signal to Noise Ratio)로 작동

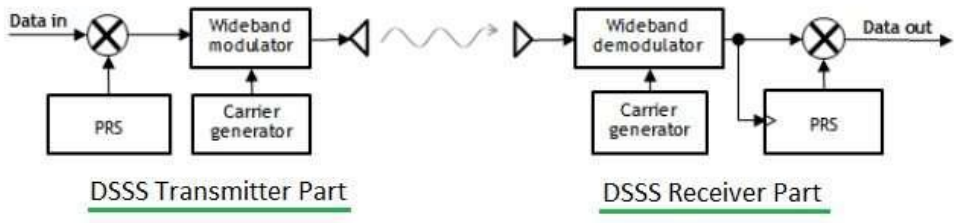
나. FHSS 의 동작원리

구분	동작원리	설 명
1. 채널 스캐닝	- 할당 채널 검색	- 23 개 독립채널, 23 개의 시스템채널 검색
	- 채널 연결	- 잡음간섭 없을 경우 채널 연결 수행
2. Noise 확인	- 잡음간섭 여부	- Hopping 전 잡음시 채널 변경 수행
	- 잡음 존재시 채널 변경	- 반복하며 잡음 없는 채널을 탐색 및 변경 수행
3. 데이터 전송	- 데이터 전송	- Wideband Modulator 로 데이터 전송 시작
	- 데이터 수신	- RF Demodulator 로 데이터 수신 시작

- PSK 위상변조 기술을 사용하여 12dB 보다 낮은 SNR 로 동작

3. DSSS 의 개념과 동작원리

가. DSSS 의 개념

개념도	
개념	- 기존 신호에 주파수가 높은 확산코드를 XOR 하여 기존 신호 대역폭을 확산 시키는 대역확산 변조 기술

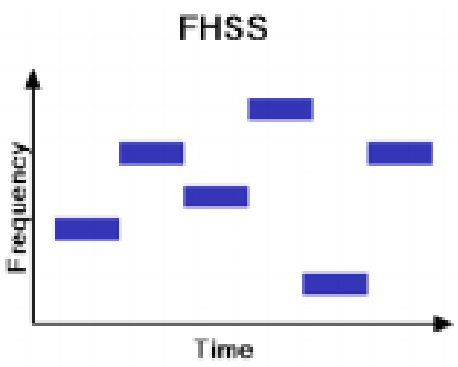
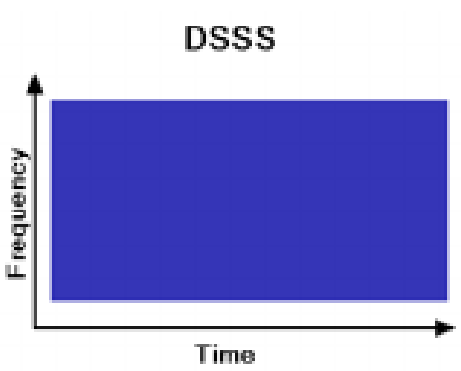
- FHSS 대비 모듈이 적어 전송이 용이하며, 이론상 FHSS 보다 넓은 커버리지를 지님.
- 국내의 경우 일반인이 사용할 경우 고저제한, 제한구역이 존재하므로 드론 통신으로 적합

나. DSSS 의 동작원리

구분	동작원리	설 명
1. 클라이언트 연결	- 독립채널과 시스템채널 고정	- 클라이언트 채널 고정 할당 수행
	- 채널 변경	- 클라이언트 채널 변동시 시스템 채널 변경
2. Noise 여부	- XOR 변조	- 데이터 전송시 XOR 처리 수행
	- XOR 복조	- 데이터 수신시 XOR 통해 기존 신호 복구
3. 전파간섭	- 채널변경 메뉴얼 처리	- 자동채널변경 기능 부재로 수동 처리
	- 전파간섭, 잡음으로 차단시 변경	- Case by Case 로 변경 반복하며 안정 채널 확정

- FHSS 와 DSSS 는 동일한 대역확산 기술이지만, 세부사양 상이.

4. FHSS 와 DSSS 비교

비교	FHSS	DSSS
주파수와 시간의 관계		
전체 주파수 간섭	- sub ISM 대역 23Mhz	- master ISM 대역 83.5Mhz
	- 낮은 신호레벨 대비 넓은 커버리지	- 높은 신호레벨 대비 적은 커버리지
Near/Par 문제	- DSSS 의 고질적 문제	- FHSS 경우 발생하지 않음
	- 과도한 전력 신호로 무선신호 파괴	- 낮은 전력신호로 간섭문제 해결
전파 투과력	- 10mW	- 10mW
	- 투과력이 높아 안정적 무선신호 송수신	-확산대역 밀도로 통신불능 지역 발생

- 안정성 있는 경우 FHSS 기반 드론을 사용, 협소적인 경우 DSSS 대역확산 기술 사용. "끝"

기출풀이 의견

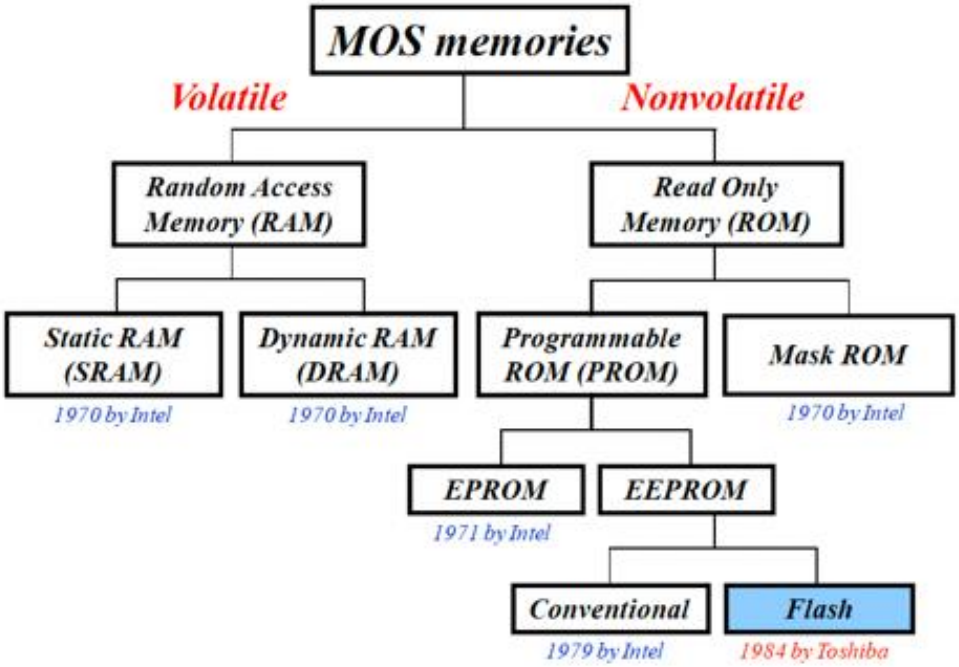
1. 드론이 보편적 기술이 되고, 상용화되었기 때문에 드론 키워드와 네트워크 신호다중화 기술 키워드로 풀고, 자신감 있게 풀어주시고, 정확한 수치와 단락간 연계 간글로 풀어주시면 좋은 점수 기대합니다.

문 제	**4. 플래시 메모리(Flash Memory)에 대하여 다음을 설명하시오.** **가. 플래시 메모리의 개요와 구조** **나. 스케일다운 한계와 대응방법** **다. 3D-Vertical NAND Flash Memory**
출 제 영 역	컴퓨터구조 / 난 이 도 ★★☆☆☆
출 제 배 경	- 반도체 호황과 수급부족에 따른 해결방안 제시 및 신기술 동향
출 제 빈 도	- 응용(86 회 4 교시)
참 고 자 료	- Flash memory 의 기술동향 https://www.koreascience.or.kr/article/JAKO201216238707699.pdf
Keyword	- 비휘발성, 저장장치, Program, Erase
풀 이	이정현(125 회 정보관리기술사)

1. 플래시 메모리의 개요와 구조

가. 플래시 메모리의 개요

개요

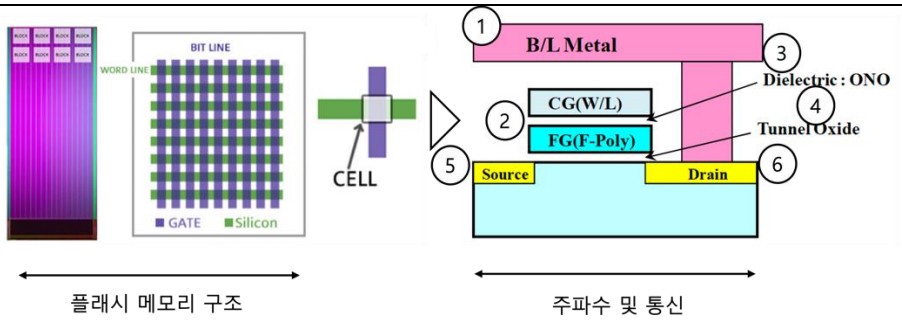


개념

- NAND, NOR 에서 사용하며, Program(쓰기), Erase(삭제) 매커니즘을 통해 전기적으로 데이터를 지우고 다시 기록할 수 있는 비휘발성 메모리(Nonvolatile Memory)

- 플래시 메모리는 셀이라 불리는 기본 저장 단위의 배열로 이루어지며, 각각의 셀은 Program, Erase 동작을 수행

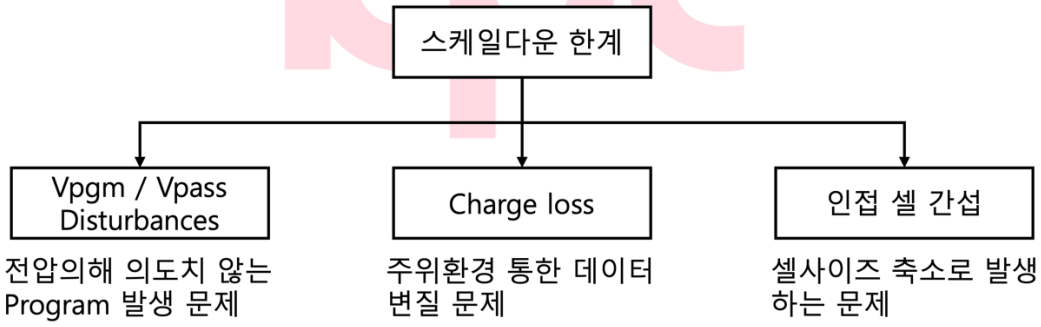
나. 플래시 메모리의 구조

구조	 플래시 메모리 구조 주파수 및 통신	
설명	① Control Gate(CG) ② Floating Gate(FG) ③ Dielectric(ONO) ④ Tuunel Oxide ⑤ Source ⑥ Drain	① Charge Storage Node 와 2 개의 게이트를 지님. ② 전자를 채우면 Program , 비우면 Erase 작업 ③ CG, FG 사이에 배치 ④ FG 와 셀 사이를 연결 ⑤ Drain 직렬로 연결하여 옆의 셀과 공유 ⑥ Source 직렬로 연결하여 옆의 셀과 공유

- 대표적으로 NAND 와 NOR 메리가 존재하며, 고집적화 용이한 NAND 고용량 저장용으로 사용되며 NOR 는 Byte 단위의 고속 Sensing 이 가능하여 저용량 데이터 저장용으로 사용.
- 한정된 영역에서 고집적화를 위해 스케일다운을 이용, 셀사이즈가 작아질 수록 Disturbance, Charge Loss, 인접셀 간섭현상 이슈 발생

2. 스케일다운 한계와 대응방법

가. 스케일다운 한계



- chipset 집적도 증대화 위해 스케일다운을 진행시 전압, 환경, 축소 문제 발생. 대응방법 필요.

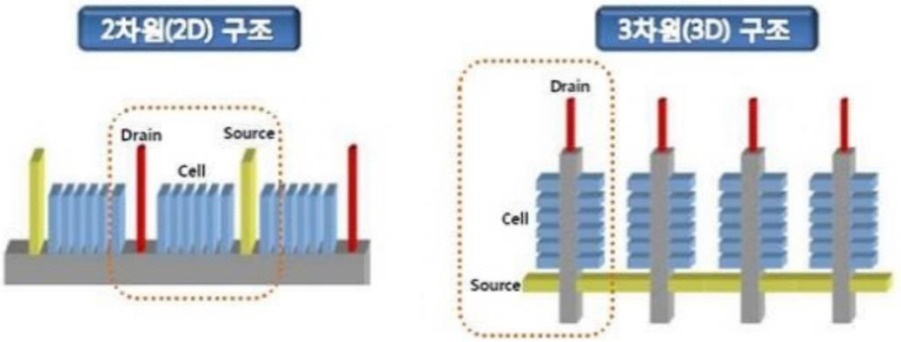
나. 스케일다운 한계 대응방법

주요한계점	주요원인	대응방법
Vpgm / Vpass	- 셀 사이즈 축소로 인해 저장된 데이터 왜곡이 발생	- 적절한 Vpss Window 설정
		- Vpgm,Vpass 의 Trade Off 유도
Charge Loss	- 주위환경(온도, 접근빈도, 사용자 습관)따라 데이터 변질이 발생	- 시간적 차이 최소화 또는 축소
		- 셀 Program 구동방식 변경
인접셀 간섭	- 메모리의 대용량화를 위해 셀사이즈 축소시 가장 먼저 발생하는 간섭현상	- All-bit Line 아키텍처 사용
		- 공정시 FG 간 Capacitive Coupling 감소

- NAND, NOR 플레시의 스케일다운 한계성을 해결한 3D Flash Memory 존재.

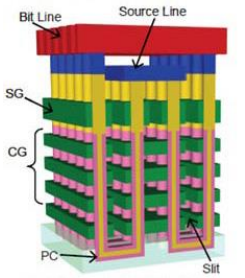
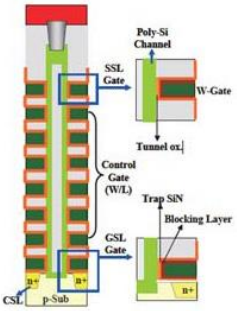
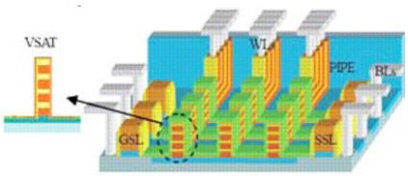
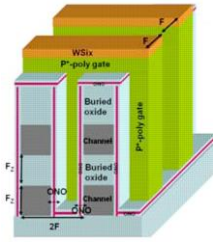
3. 3D-Vertical NAND Flash Memory

가. 3D-Vertical NAND Flash Memory 필요성



- 스케일다운 문제 Vpgm, Vpass, Charage Loss, 인접셀 간섭 을 해결한 대용량 고집적 비메모리

나. 3D-Vertical NAND Flash Memory 아키텍처

구분	아키텍처 구성도	설명
P-BiCS (Pipe-Shaped-Bit-Cost Scalable)		- 3D NAND BiCS 개선 버전 - Tunnel Oxid Damage 해결
TCAT (Terabit Cell Array Transistor)		- 삼성에서 최초로 구현된 3D NAND - Metal GATE 공정으로 구현
VSAT (Vertical Stacked Array Transistor)		- 게이트에 대한 채널 확보 최대화 - Twisted-Channel 사용
VG (Vertical gate)		- 전류를 수평방향으로 흐르도록 구현 - 적층 용이성과 안전성 보장

- 공정 분야 노드 발전에 발전에 맞춰 '게이트올어라운드(GAA)'와 같은 트랜지스터 구조변화와 함께 시스템 반도체에서도 적층 기술이 공정 한계를 극복할 대안으로 떠오를 것으로 전망 "끝"

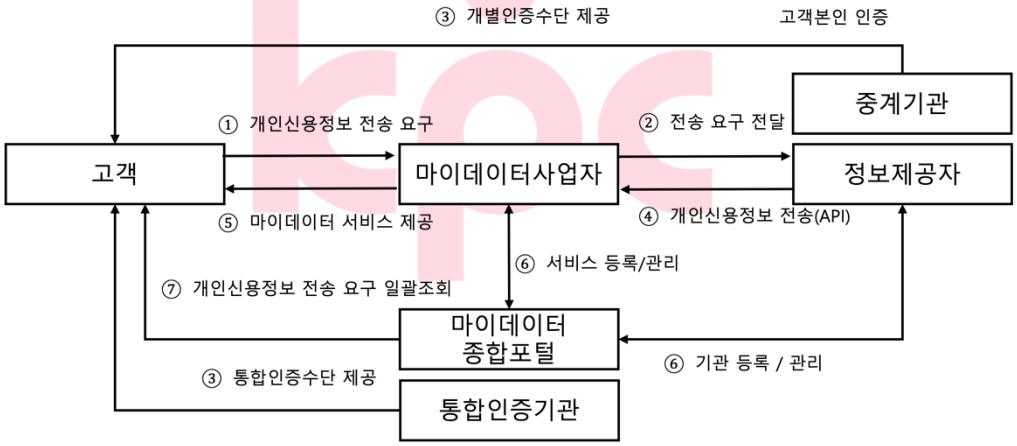
기출풀이 의견

4. 현재 전기자동차의 급성장, 자율주행, GPU 으로 반도체 부족현상이 나타나고 있습니다. 해당 배경을 가지고, 적절한 키워드 배치와 정확한 표현이 필요하며, 도식화가 필요한 문제입니다.

문 제	5. 마이데이터 서비스에 대하여 다음을 설명하시오. 가. 서비스 절차 나. 마이데이터 인증 방식 다. 보안문제점 및 개선방안		
출 제 영 역	보안	난 이 도	★★☆☆☆
출 제 배 경	- 마이데이터 가이드라인 개정 및 마이데이터 보안 이슈 인한 출제		
출 제 빈 도	- 관리(120 회 2 교시), KPC 모의고사, KPC 합숙 다수 출제		
참 고 자 료	- 마이데이터 가이드라인 https://www.fsc.go.kr/no010101/76323?srchCtgry=&curPage=&srchKey=&srchText=&srchBeginDt=&srchEndDt=		
Keyword	- 사업자 시행착오 최소화, 알고하는 동의		
풀 이	이정현(125 회 정보관리기술사)		

1. 마이데이터 서비스 절차

가. 마이데이터 서비스 절차도



- 고객의 개인신용정보 전송요구 및 마이데이터서비스 제공과 관련 세부절차, 기준을 제공하여, 이해관계자들의 편리성과 시행착오 최소화를 위해 2021.2. 마이데이터 서비스/기술 가이드라인 개정

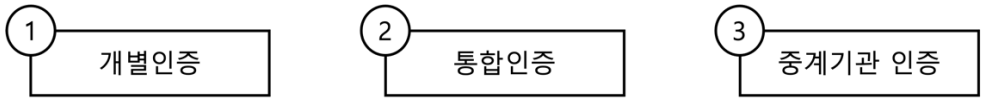
나. 마이데이터 서비스 절차

구분	절차	설명
전송요구	1. 개인신용정보 전송 요구	- 사업자가 제공하는 서비스 이용
	2. 전송 요구 전달	- API 규격에 따라 개인신용정보 전송
전송	3. 통합인증수단 제공	- 정보제공자의 인증수단 통해 고객 인증
	4. 개인신용정보 전송(API)	- 마이데이터 사업자에 개인신용정보 전송
서비스 제공	5. 마이데이터 서비스 제공	- 수집된 정보로 통합조회 및 서비스 제공
	6. 서비스/기관 등록 및 관리	- 정보제공자와 사업자 등록 관리 제공
종합포털지원업무	7. 개인신용정보 전송 요구 일괄조회	- 고객에게 전송요구 이력 등 서비스 제공

- 정보제공자는 안전한 개인신용정보 전송을 위해 해당 고객의 인증이 필요. 개별, 통합, 중계기관 인증 존재

2. 마이데이터 인증 방식

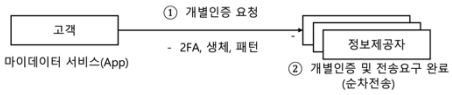
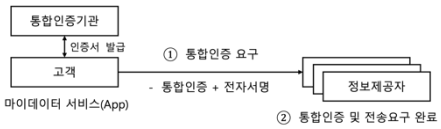
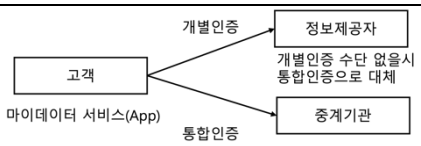
가. 마이데이터 인증 방식의 유형



- 고객이 개별인증 요청
- 1회인증으로 다수인증
- 정보제공자가 전송

- 개인신용정보의 전송요구(신용정보법 제 33 조 2)에 따라 본인여부 확인 불가시 전송요구를 거절, 중단 가능

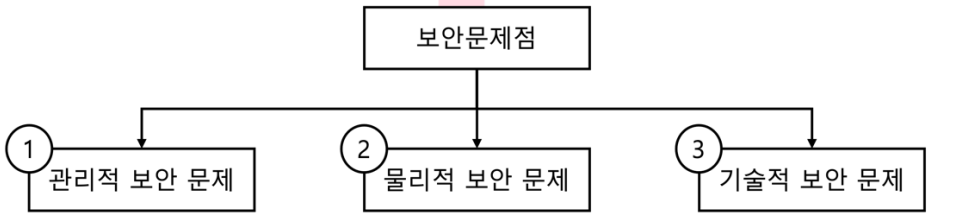
나. 마이데이터 인증 방식 상세

방식	인증순서	설명
개별인증		- 각 정보 제공자가 인증수행 - 정보제공자 수만큼 반복수행 - 표준 API 제공 및 다중인증 수행
통합인증		- 통합인증기관이 발급한 인증수단 이용 - 정보제공자 수와 무관하게 1 회 수행 - CI 제공 및 다중요소 공개키인증서 발급
중계기관인증		- 개별인증 정보제공자가 수행 - 통합인증 중계기관이 수행 - 개별인증 불가시 통합인증으로 대체

- 마이데이터 서비스를 구축함에 따라 관리적, 물리적, 기술적 보안 문제가 발생

2. 보안문제점 및 개선방안

가. 보안문제점의 유형



- 개인정보 침해
- 직무분리 부족
- 시스템 불법 접근

- 접근통제 문제
- 물리적 보안 미비

- 비밀번호 및 암호 탈취
- 약한 암호화 수준
- 시스템 개발보안 미준수

- 서비스 개발 및 다수의 이해관계자간 협의를 통해 기관 및 업체별로 서비스를 제공하므로, 보안 문제점이 발생

나. 보안문제점의 개선방안

구분	개선방안	기술요소
관리적 보안 문제	- 개인신용 정보보호 교육, 직무분리	- 사용자보안, 내부보안, 프라이버시 체계
	- API 시스템 관리 및 이용자 보호	- 2FA, Token, 다중인증, 다중요소 공개키
물리적 보안 문제	- 서비스 별 접근통제 방안	- MAC, DAC, RBAC, ACL, SL, CL
	- 내부중심 물리적 보안 수행	- 보안관리자, 보안요원, EDR, IDS, IPS
기술적 보안 문제	- 비밀번호, 암호통제 마련	- 숫자, 문자, 특수문자 혼용
	- 시스템보안, 개발보안 준수	- 계정, 권한, 로그 관리 및 시큐어코딩

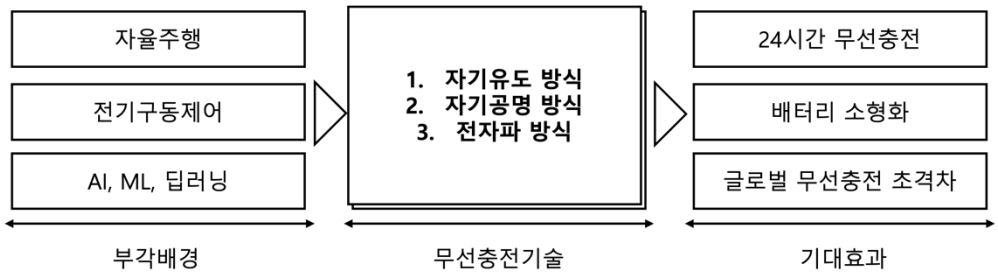
- 보안중심 서비스 개발 통해 안전성 확보와 TF 구성 운영, 가이드 지속개선으로 마이데이터 사업 활성화 "끝"

기출풀이 의견

1. 최근 꾸준히 마이데이터 관련 문제가 기출되고 있습니다. 1 단락 절차 정도 외워주시면 앞으로 문제가 기출되더라도 대응 및 답안 작성이 가능합니다. 또한 해당 문제는 누구나 아는 문제이므로 자신만의 생각 / 차별화 요소로 승부하셨다면 고득점 예상합니다.

문 제	6. 휴대용 전자기기 및 전기자동차 등의 확대로 인해 무선으로 전력을 전송하여 배터리를 충전하는 무선 충전기술이 주목받고있다. 이와 관련하여 다음을 설명하시오. 가. 무선충전기술의 개요 나. 무선충전기술 유형별 사용 주파수, 전송거리 및 효율, 인체 유해성, 주요 사용분야 측면에서 비교 다. 무선충전기술 사용에서 발생 가능한 보안 문제점
출 제 영 역	보안 / 난 이 도 ★★☆☆☆
출 제 배 경	- 휴대용 전자기기 및 전기자동차의 활성화로 인한 출제
출 제 빈 도	- 응용(125 회 4 교시, 111 회 2 교시)
참 고 자 료	- 무선충전기술 동향 및 보안위협 https://scienceon.kisti.re.kr/srch/selectPORSrchArticle.do?cn=NPAP12685145&dbt=NPAP
Keyword	- 자기유도, 자기공명, 전자파
풀 이	이정현(125 회 정보관리기술사)

1. 무선충전기술의 개요

개요	
개념	- 물리적 전력선없이 전력을 무선으로 전파하여 사용자의 디바이스를 충전하는 기술

- 과거 충전시 전력 소모량, 충전 범위, 사용기기가 부족했으나, 현재 개인디바이스 및 전기차, 드론까지 활용

2. 무선충전기술 유형별 비교

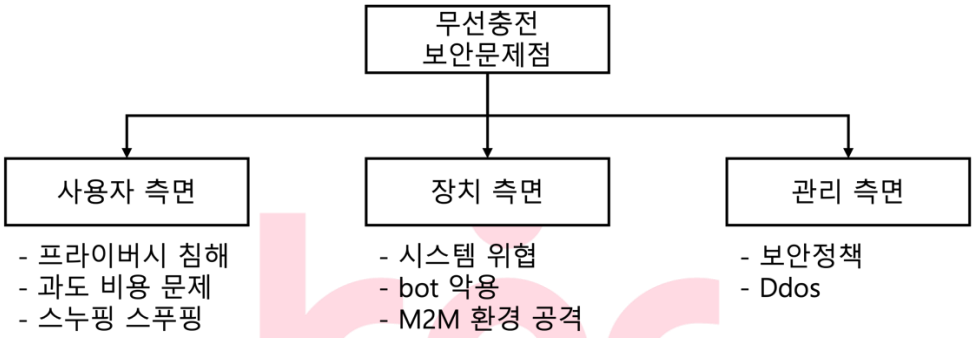
구분	자기유도 방식	자기공명 방식	전자파 방식
원리	- 변압기 1~2 차 코일간 유도현상 이용	- 송수신 안테나 간의 공명현상 이용	- 안테나를 통해 전자파를 직접 송수신
주파수	- 125 kHz, 13.56 MHz	- 수십 kHz ~ 수 MHz	- 2.45 GHz ~ 5.8 GHz
전송 거리 및 효율	- 수 mm 이내 - 90% 이상 효율	- 1m ~ 90% 효율 - 2m ~ 40% 효율	- 최대 수십 km - 최대 10 ~ 50% 효율

인체 유해성	- 거의 무해	- 거의 무해	- 유해
특성	- 대전력 전송에 유리	- 대전력 전송 부적합 - 안테나 크기 문제	- 인체 및 장애물 영향 - 생체리듬 영향 문제
응용	- 휴대폰, 노트북, 전기차	- 가전기기 전원	- 항공위성
표준화	- WPC 표준	- A4WP	- ITU-R SG1

- 스마트폰 및 전기차 무선충전시 BLE, Wi-Fi 등 무선통신 기술로 데이터 송수신 가능
- 상대적으로 편리성은 높아졌으나, 보안성은 낮아지는 문제가 존재

3. 무선충전기술 사용에서 발생 가능한 보안 문제점

가. 무선충전기술 사용시 발생 가능한 보안 문제점



- 무선충전시 데이터를 무선통신으로 송수신하므로 사용자, 장치, 관리 측면의 대응방법 필요

다. 무선충전기술 사용시 발생 가능한 보안 문제점 해결방안

비교	문제점	해결방안
사용자 측면	- 무선통신 데이터 탈취 문제	- 평문통신 방지, 경량암호화, 2FA 인증
	- 프라이버시 침해 문제	- 비식별조치, 익명화, 가명화, 사용자 종속
	- 인증되지 않은 무선충전 장치	- 전파 인증 및 사용자 경각심 필요
장치 측면	- 시스템 위협	- IDS, IPS WIPS, Firewall 이용해 대응
	- Bot 악용	- 신뢰된 정보만 검증, 보안 솔루션
	- M2M 환경 공격	- 기계간 통신시 서로 IP 및 통신규약
관리 측면	- 사용자 및 사내 보안정책 문제	- 개인무선충전기기 사용금지
	- 폐쇄형 환경에서 반입정책 문제	- 허가된 경우만 무선충전 사용
	- 무선통신 표준화 및 보안기준 수립	- WPC, A4WP, ITU-R 준수

- 무선충전은 편리성을 높여주므로 경제성장에 큰 도움. 수평적 보안 인식 고려 및 관련 시스템 및 장치에 대한 SW 개발시, SW 개발 보안을 준수하여 안전성 확보 "끝"

기출풀이 의견

1. 많은 키워드보다 스토리텔링 중심으로 왜? 지금 화자 되었나. 와 출제자가 보고 싶은 답안은 무엇인가를 고민하며 작성하면 좋겠습니다.