ICT의 가치를 이끄는 사람들!!

123회

컴퓨터시스템응용기술사 기출풀이 4교시

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

국가기술자격 기술사 시험문제

정보처리기술사 제 123 회 제 4 교시

분야	정보처리	종목	컴퓨터시스템응용기술사	수험번호		성명	

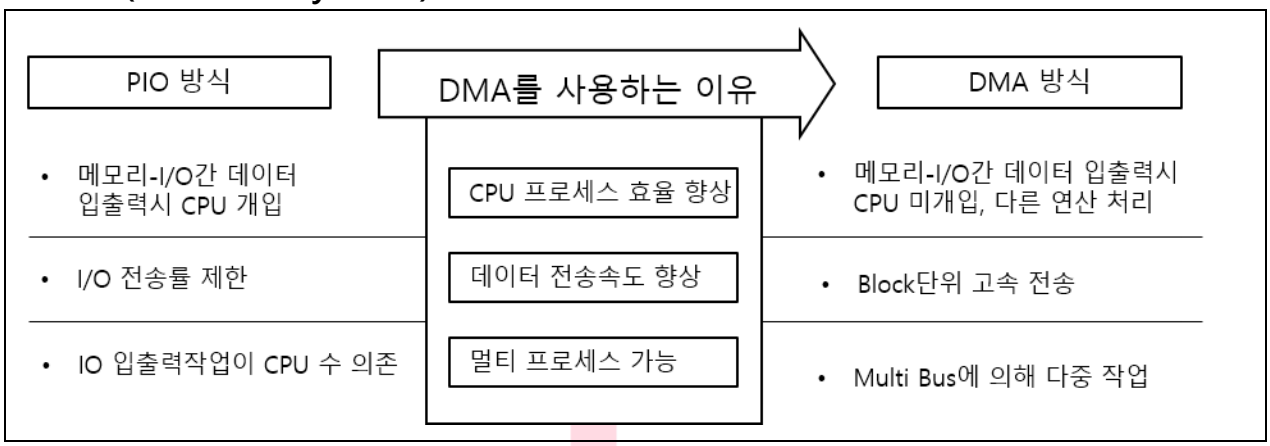
※ 다음 문제 중 4 문제를 선택하여 설명하시오. (각 25 점)

1. DMA(Dirent Memory Access)에 대하여 다음을 설명하시오.
   가. DMA 를 사용하는 이유
   나. 입출력장치에서 주기억장치로 정보 전송 시 DMA 를 이용한 정보전송
   다. Burst Mode, Cycle Stealing Mode, Demand Trandsfer Mode
2. 버퍼 오버플로우(buffer overflow)를 이용한 사이버 공격을 설명하고, 이를 해결하기 위한 소프트웨어 방안(실행 시간 방어, 컴파일 시간 방어)들을 설명하시오.
3. 물리적으로 안전한 가상현실 서비스를 위한 주변감지 및 경고시스템 표준(TTAK.KO-10.1116, 2018)을 설명하시오.
4. 드론(Drone) 서비스 관련 보안 위협과 대응방안에 대하여 다음 각 사항을 반영하여 설명하시오.
   가. 자산 별 보안위협
   나. 4 가지 이상의 위협 시나리오
5. 최근 각 분야에서 개인정보유출이 잇따르면서 경제협력개발기구(OECD)의 '프라이버시 8 원칙'이 새삼 주목받고 있다. 이 8 원칙은 개인정보의 수집 및 관리에 대한 국제사회의 합의를 반영한 국제기준으로 법적인 구속력은 없지만 일반원칙으로 인정받고 있다. 경제협력개발기구(OECD) 프라이버시(privacy) 8 원칙을 설명하시오.
6. 공공기관의 정보기술 투자성과에 대한 성과관리를 평가체계 관점에서 설명하시오.

*

문 제	4-1 DMA(Direct Memory Access)		
출 제 영 역	CA	난 이 도	★★★☆☆
출 제 배 경	CA 기본		
출 제 빈 도	80 회 응용 2 교시, 86 회, 89 회		
참 고 자 료	- 위키백과 - 쉽게 배우는 운영체제(조성호, 한빛아카데미)		
K e y w o r d	Burst Mode, Cycle Steeling, Demand Transfer Mode, PIO, Block 단위, Interrupt		
풀 이	신지선 (122 회 정보관리기술사)		
감 수	채명희 (92 회 컴퓨터시스템응용기술사)		

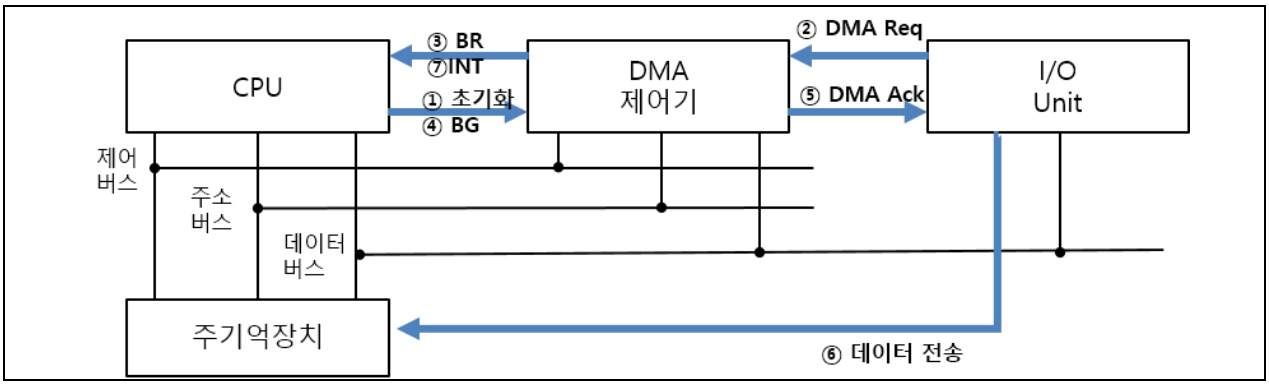
1. DMA(Direct Memory Access)를 사용하는 이유



- DMA 는 PIO 의 단점을 보완하고 CPU 의 효율성을 높이기 위해 고안된 장치

2. 입출력 장치에서 주기억 장치로 정보 전송시 DMA 를 이용한 정보전송 흐름도 및 설명

가. DMA 를 이용한 정보 전송 흐름도



- DMA 제어기가 BUS Request 획득 후 I/O 인터페이스가 직접 주기억장치에 정보 전송

나. DMA 를 이용한 정보 전송 흐름 상세설명

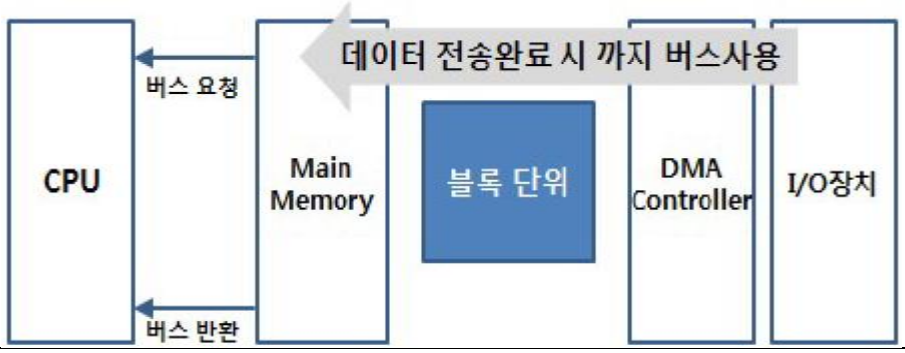
전송 동작	제어 흐름	설 명
①DMA 초기화	CPU -> DMA	- 데이터 처리를 위한 초기화 명령 전송

		- 초기화 항목) IO 장치 주소, 연산(읽기/쓰기) 지정자, 데이터 읽거나 쓰여질 주기억장치 영역의 시작 주소
② DMA Req	I/O -> DMA	- I/O 인터페이스가 DMA 서비스 요청
③ BR	DMA -> CPU	- DMA 는 CPU 로 시스템 버스 제어권을 요청
④ BG	CPU -> DMA	- CPU 는 시스템 버스 허가 신호 응답
⑤ DMA Ack	DMA -> I/O	- DMA 는 I/O 인터페이스에 DMA 서비스 응답
⑥ 데이터 전송	I/O -> 주기억장치	- 중앙 처리 장치의 개입없이 버스제어권을 사용 - 입출력 장치에서 주기억장치에 데이터 전송
⑦ INT	DMA ->CPU	- 전송완료시 CPU 에 Interrupt 신호 전송

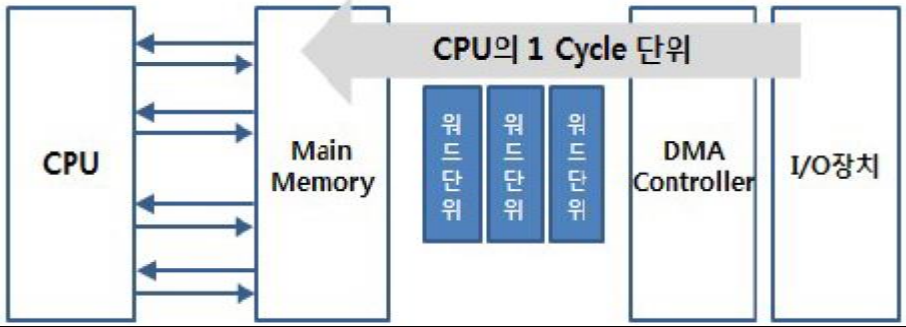
- DMA 가 버스제어권을 이용하여 데이터를 전송하는 방식에 따라 Burst Mode, Cycle Steeling Mode, Demand Transfer Mode 분류

3. DMA 의 3 가지 동작모드(Burst Mode, Cycle Stealing Mode, Demand Transfer)

가. Burst Mode(Block Mode)

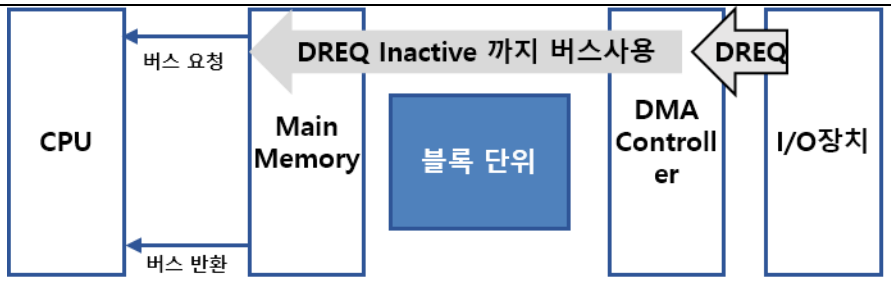
개 념	DMA 컨트롤러가 버스 제어권을 획득시 데이터 전송이 완료될때까지 시스템 버스 사이클을 독점하는 전송 방식
동작방식	
특 징	블록 단위 전송, 고속 입출력 장치에 사용

나. Cycle Steeling Mode

개 념	한번의 버스 제어권 요청당 1Byte 씩 데이터 전송하는 전송방식
동작방식	
특 징	워드 단위 전송, 저속 입출력 장치, 데이터 실시간 모니터링 입출력 장치에 유리

다. Demand Transfer Mode

개 념	Burst Mode 와 유사하며 DREQ 신호 비활성시 전송을 중지하고 활성시 재시작하는 전송 방식

동작방식	
특 징	프로그램 로딩/데이터 파일 로딩에 유용, 상대적으로 긴 CPU Idle Time

"끝"

기출풀이 의견

1. CA영역의 기본 토픽을 이해하고 질문에 대해 깊이 있는 답을 제시하는 것이 유효합니다.
2. 모의고사에도 자주 출제된 기본적이고 원론적인 질문입니다. 기본에 대한 학습이 필요합니다.

문 제	4-2 버퍼 오버플로우 (Buffer Overflow) 공격		
출 제 영 역	보안	난 이 도	★★★☆☆
출 제 배 경	IoT 기기에 대한 버퍼 오버플로우 공격 지속		
출 제 빈 도	미출제		
참 고 자 료	- 위키백과 - 정보 보안 개론 개정 3 판(양대일, 한빛미디어)		
K e y w o r d	스택, 힙, 실행시간방어, 컴파일시간 방어		
풀 이	신지선 (122 회 정보관리기술사)		
감 수	채명희 (92 회 컴퓨터시스템응용기술사)		

1. 메모리 구조를 이용한 조작, 버퍼 오버플로우(Buffer Overflow) 공격의 개념

가. 버퍼 오버플로우 공격의 정의

- 프로그램 작성시 모호한 데이터 길이 정의를 이용하여 버퍼에 할당된 크기를 벗어나 다른 영역의 정보를 변경하는 공격 방식

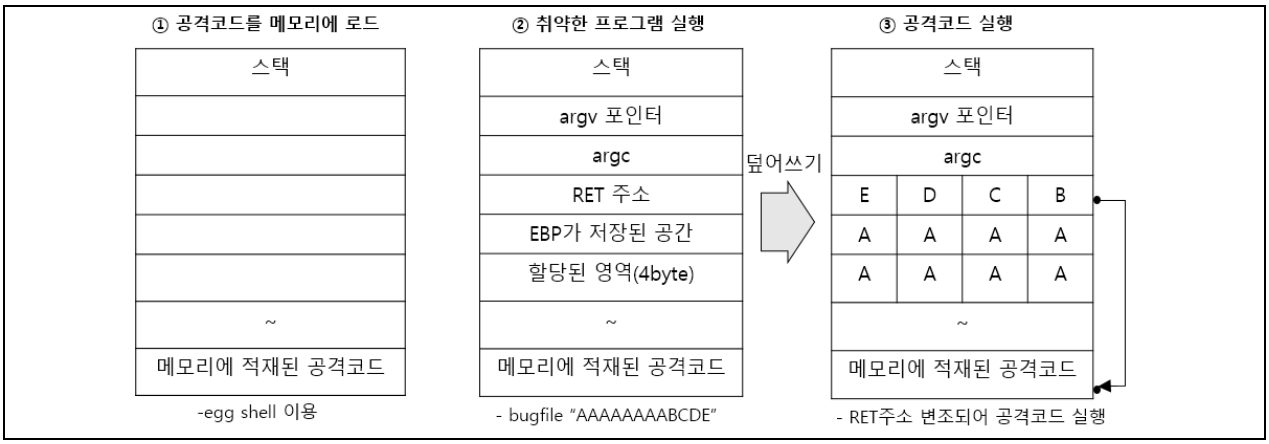
나. 버퍼 오버플로우 공격의 특징

구분	특징	설명
취약점	C 언어의 무결성 문제	- C 언어의 입력 데이터 무결성 검증 취약점 활용 - scanf(), sscanf(), vscanf(), strcpy()
공격 메커니즘	메모리 값 변조	- 시스템의 메모리 구조, 주소지정방식을 활용한 공격 - 허용된 길이 이상의 값을 주입하여 데이터 변조 공격
공격 현황	공격 방식 다변화	- 코드 품질이 낮은 임베디드 시스템에 대한 공격 증가

- 버퍼오버플로우의 유형은 스택버퍼오버플로우, 힙버퍼오버플로우로 세분화 가능

2. 버퍼 오버플로우 공격 원리

가. 버퍼 오버플로우 공격시 스택의 구조



- 4byte 할당된 여역을 넘어서는 데이터(12byte)를 입력시 RET 주소 정보 변경됨

나. 버퍼 오버플로우 공격시 스택 상태

공격순서	스택 상태	설명
① 공격코드 로드	공격코드 메모리 로드	- 관리자 권한 탈취등 공격코드를 egg shell 등을 이용한 특정 메모리상에 로드 - 코드는 실행되지 않도 메모리상의 특정위치에 로드됨
② 취약한 프로그램 실행	RET 주소 덮어쓰기	- 버퍼 오버플로우 취약한 프로그램 실행(예, strcmp) - 할당된 영역(4 byte) 보다 큰 12byte 의 인자값에 공격코드의 메모리 주소를 입력
③ 공격코드 실행	RET 주소 위치로 이동	- RET 주소가 가리키는 공격 코드 실행

- 버퍼오버플로우 취약점을 이용하는 공격은 구조, 운영체제, 메모리 영역에 따라 다름

3. 버퍼 오버플로우 공격 대응을 위한 소프트웨어적 방안

가. 실행 시간 방어

개 념	기존 프로그램을 실행시에 공격을 발견하고 중지시키는 방어기법	
상세기법	주소공간 임의추출	- 실행시 스택공간을 임의적으로 배치해 공격자가 실행코드의 주소를 예측할수 없도록 함
	가드페이지	- 프로세스 주소공간 내에 메모리 임계영역 사이에 가드페이즈를 둠 - 가드페이즈에 접근하는 프로세스 강제종료
	실행가능 주소공간 보호	- 실행코드가 프로세스 메모리상의 특정 위치에서만 실행될 수 있게 함

나. 컴파일 시간 방어

개 념	새 프로그램에서 공격을 저지하도록 프로그램을 강화하는 방어 기법	
상세기법	고수준 프로그램 언어 사용	- java, python 같은 버퍼오버플로우를 허용하지 않는 언어 사용
	안전한 함수 사용	- 안전한 함수 : strncpy(), fgets() - 안전하지 않은 함수 : scanf(), sscanf(), vscanf(), strcpy(), gets()
	스택보호 매커니즘	- 함수의 스택프레임에 손상이 있는지 확인하고 문제시 종료 - 지역변수 할당시 canary 값 기록, 종료시 canary 값 변경되면 프로그램 종료
	스택 쉴드	- 함수 시작시 복귀주소를 Global RET 에 저장해 두었다가 반환시 특수 스택의 값과 비교해 다를 경우 프로그램 종료

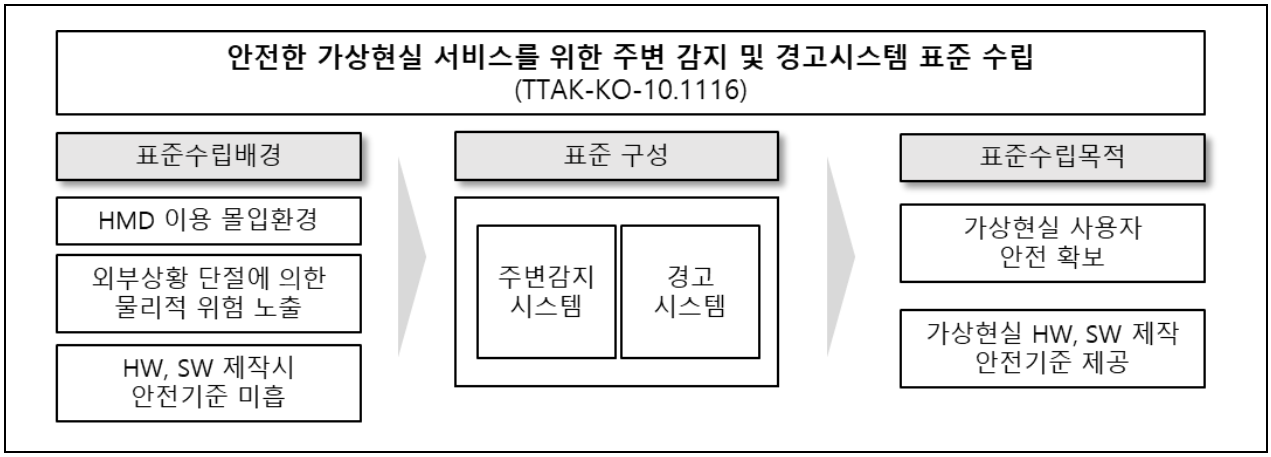
- 소프트웨어적 방법 이외 심층패킷조사(DPI)를 이용한 방어기법이 있음 "끝"

기출풀이 의견

1. 보안영역의 기본토픽이면서 OS영역과 겹치는 토픽으로 기본원리를 이해하고 심도있는 답변으로 차별화가 필요합니다.

문 제	4-3 안전한 가상현실 서비스를 위한 주변 감지 및 경고시스템 표준 (TTAK.KO-10.1116, 2018)		
출 제 영 역	디지털서비스	난 이 도	★★☆☆☆
출 제 배 경	언택트 사회 도래에 따른 가상현실 서비스 활성화와 이에 따른 안전성 문제 대응		
출 제 빈 도	미출제		
참 고 자 료	- 안전한 가상현실 서비스를 위한 주변감지와 경고시스템_TTAK.KO-10.1116 - 안전한 가상현실 서비스를 위한 주변감지와 경고시스템_표준해설서		
Keyword	HMD, 깊이 카메라, 감지 시스템, 경고 시스템, 절대적 안전거리, 상대적 안전거리		
풀 이	신지선 (122 회 정보관리기술사)		
감 수	채명희 (92 회 컴퓨터시스템응용기술사)		

1. 안전한 가상현실 서비스를 위한 주변감시 및 경고시스템 표준 개요



- HMD(Head Mounted Display)를 통해 가상현실 콘텐츠 서비스를 제공할 때, 사용자의 안전성 보장을 위해 표준 수립

2. 주변감지 시스템 표준

가. 주변감지 시스템 개요

구 분	설 명	
개 념	사용자와 주변 물체의 추돌 사고를 예방하기 위해 위부 위험 요소에 대한 안전거리 확보에 대한 감지하는 시스템	
물리적 안전 확보 항목	절대적 안전 거리	사용자로부터 반경 1m 이상
	상대적 안전 거리	주변 물체와 사용자 간의 상대 속도에 의해서 가까워지는 거리가 초당 1m 이상일 때, 5 미터 이상
	절대적 위험 물체	곡률이 2mm 이하인 날카로운 물체
	상대적 위험 물체	사용자를 중심으로 반경 2m 이내에서 2m/sec 이상의 속도로 접근하는 물체

- 위험물체와 사용자와 주변 물체간의 안전거리에 대해 정의하고 감지 및 경고시스템의 기준 제시

나. 주변감지 시스템 표준 상세

구 분	표준 항목	설 명
시 스 템 구 성	깊이 카메라 모듈 배열	- 사용자 주변 물체에 대한 상대적 거리 측정, HMD 에 장착
	감지 기준	- 깊이 카메라 모듈은 '절대적 안전거리'와 '상대적 안전거리' 이내에 '절대적 위험 물체' 또는 '상대적 위험 물체' 감지
	시야각 기준	- 수평 시야각(FOV, Field of View) 90 도 이상, - 수직 시야각 120 도 이상
시 스 템 활 성 화	활성화 기준	- 깊이 카메라 모듈은 사용자가 HMD 구동시 자동적으로 활성화
	안전대처시간	- '상대적 안전거리'는 사용자가 위험을 인지하고 대처할 수 있는 최소한의 시간인 5 초 확보
	비활성화 기준	- 사용자의 의지에 따라 비활성 가능 -단, 비활성시 경고메시지를 음성신호와 문자등의 영상신호로 출력
위 험 의 판 단	잠재적 위험	- 사용자 중심 물체가 '절대적 안전거리' 또는 '상대적 안전거리'내에 있는 경우
	심각한 위험	- 절대적 안전거리' 또는 '상대적 안전거리'내에 '절대적 위험 물체' 또는 '상대적 위험 물체'가 접근하는 경우

3. 경고시스템 표준

가. 경고시스템 개요

구 분	설 명	
개 념	음성 신호 또는 영상 신호를 이용하여 사용자가 인지할 수 있도록 구성한 시스템	
경고시스템 활 성 기 준	잠재적 위험	- '잠재적 위험'으로 판단될 경우 경고시스템 활성화 - 음성 신호 또는 양상 신호중 콘텐츠 사용에 지장을 주지 않는 방식
	심각한 위험	- '심각한 위험'으로 판단되는 경우 음성 신호와 영상신호 모두 사용

- 감지시스템에 의해 감지된 위험상황을 사용자에게 적절하게 알리는 경고 시스템 표준 정의

나. 경고시스템 표시 유형

유형	항목	설명
영 상 신 호	표시방식	-문자 신호, 이미지 신호, 영상 신호, 객체 윤곽 신호
	표시기준	-콘텐츠의 특성에 따라 위의 영상 신호 방식 중 사용자가 상황을 인지할 수 있는 방식 선택
음 성 신 호	표시방식	-비프 신호, 사람의 목소리 신호, 사운드 신호
	표시기준	-콘텐츠의 특성에 따라 위의 음성 신호 방식 중 사용자가 상황을 인지할 수 있는 방식 선택
심각한 위험	영상신호+음성신호	- '심각한 위험'으로 판단되는 경우 음성 신호와 영상신호 모두 사용

- 경고시스템 표시 유형을 영상신호, 음성신호로 구분하고 위험의 정도에 따라 표시 기준을 제시함

4. 표준의 적용

구 분	적용 방법	적용 항목
HMD 장치	감지 시스템	- HMD 에 구조물 형태로 깊이 카메라 장착 - 깊이 카메라 지속적 주면 감지를 위해 기능 활성화
	경고 시스템	- HMD 디스플레이, 스피커 이용
콘 텐 츠	경고 시스템 구체적 표현	- HMD 의 감지시스템과 경고 시스템을 사용 - 경고시스템의 구체적 표현 방식은 컨텐츠가 사용될 때의 목적, 사용환경을 해치지 않는 범위에서 표준의 의도를 감안하여 표현

- 안전한 가상환경 서비스를 위해 콘텐츠 장르별, 서비스 활용 분야별 특화된 기준 필요

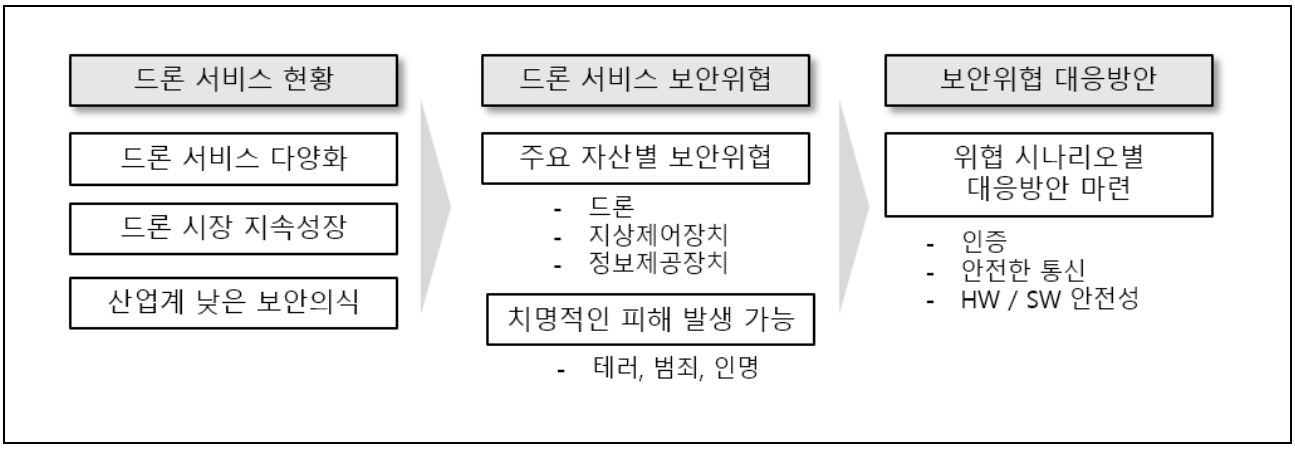
"끝"

기출풀이 의견

1. 표준번호까지 명시해서 질문이 나왔기 때문에 정확하게 해당 내용을 답해야 합니다.

문 제	4-4 드론 서비스 관련 보안위협과 대응방안		
출 제 영 역	보안	난 이 도	★★☆☆☆
출 제 배 경	드론 기반 서비스 증가에 따라 보안 취약점에 대한 위협 증가 보안 취약점에 대한 이해 및 대응방안 요구		
출 제 빈 도	미출제		
참 고 자 료	- 드론 사이버보안 가이드(2020.12. 한국인터넷진흥원)		
K e y w o r d	드론, 지상제어장치, 정보제공장치, GPS 재밍, 제어신호 전파방해		
풀 이	신지선 (122 회 정보관리기술사)		
감 수	채명희 (92 회 컴퓨터시스템응용기술사)		

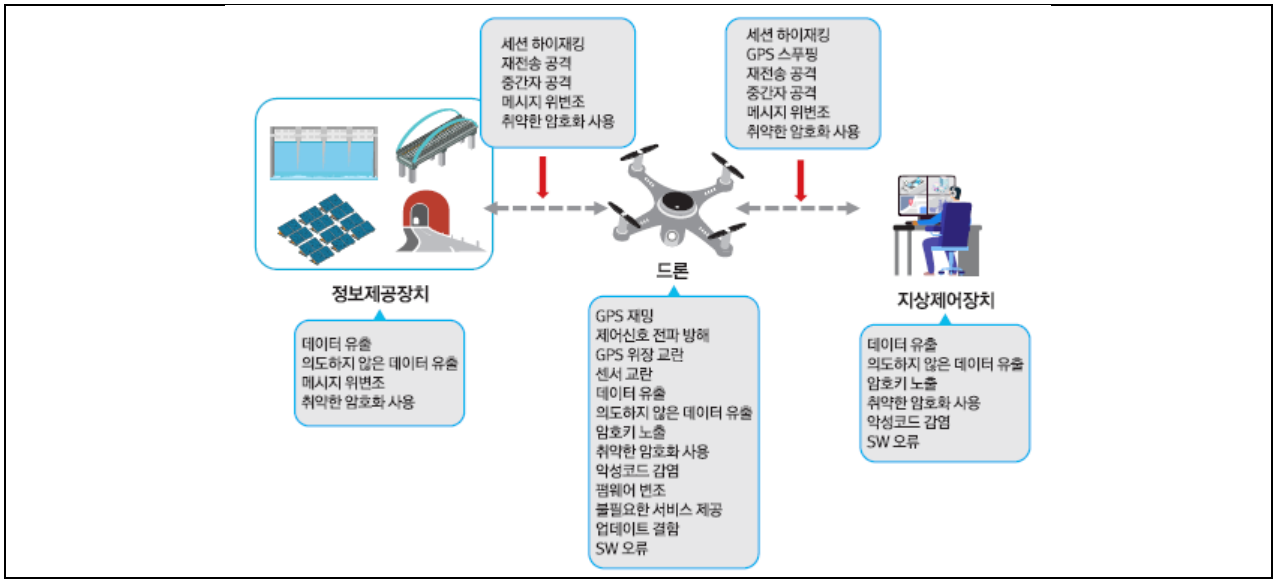
1. 성장하는 서비스와 함께 확대되는 보안위협, 드론 서비스 관련 보안위협 개요



- 드론은 조종사가 직접 탑승하지 않고 무선으로 원격 조정, 또는 프로그램에 의해 비행하는 비행체
- 드론 서비스의 성장으로 신규 비즈니스 모델이 창출되고 있으며 이와 함께 치명적인 인명피해를 줄 수 있는 보안위협이 발생 가능

2. 드론시스템 구성 및 자산별 보안위협

가. 드론시스템 구성에 따른 주요 보안위협

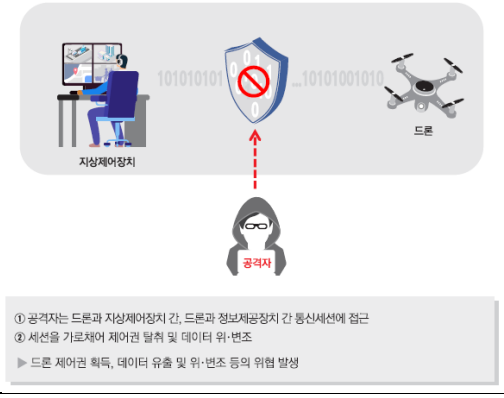


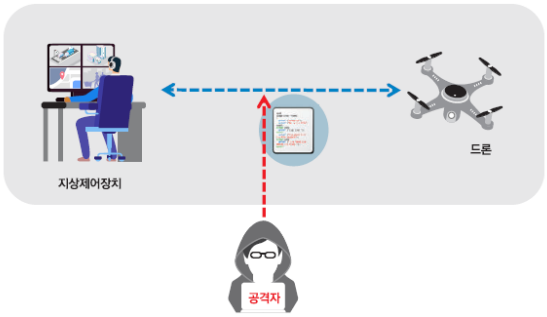
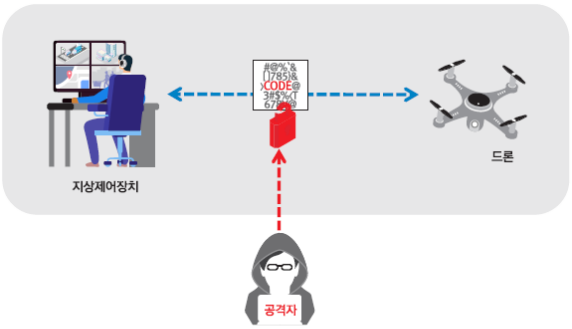
나. 드론시스템 자산별 보안 위협 상세설명

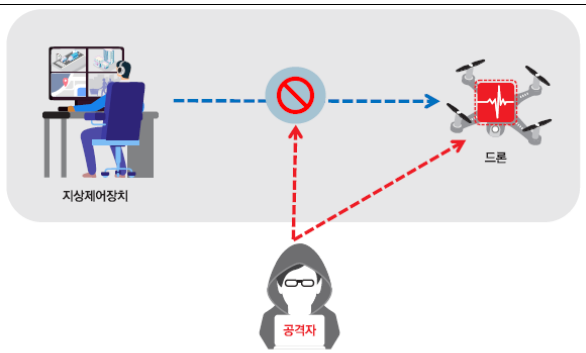
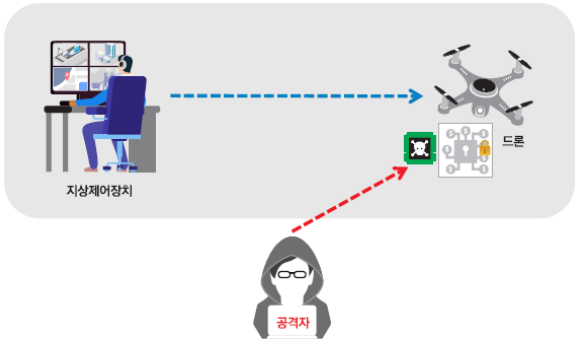
자산	보안위협	설명
정보제공장치	데이터 유출	- 개인정보, 주요시설 기밀정보 유출, 서비스 장애 및 불능
	메시지 위변조	- 세션 하이재킹, 재전송 공격, 중간자 공격 이용한 메시지 위변조
	취약한 암호화	- 암호키 노출, 취약한 암호 알고리즘 사용
드 론	GPS 재밍	- 강한 GPS 신호 발생, 드론 경로 이탈 및 서비스 장애
	제어신호 전파 방해	- 지상제어장치와 드론간 무선통신주파수 해킹, 드론 제어 무력화
	센서 교란	- 거리계, 기압계, GPS 센서 교란을 통한 무력화
	펌웨어 변조	- 드론 임베디드 시스템 변조된 펌웨어 업데이트 및 시스템 변조 - 악성코드 실행, 백도어 설치, 시스템 권한 탈취
지상제어장치	데이터 유출	- 개인정보, 인증정보, 기기정보 등 기밀정보 유출
	취약한 암호화	- 암호키 노출, 취약한 암호 알고리즘 사용으로 제어권 탈취 - MAVLink 프로토콜
	SW 오류	- 잘못된 설계 및 구현

- 드론시스템 자산의 보안위협은 다양한 보안위협 시나리오로 재구성 되며 이에 대한 대응방안 제시 필요함

3. 드론서비스 보안위협 시나리오 및 대응방안

구분	위협 시나리오	대응방안
중간자 공격		- 인증 - 안전한 통신 - 암호 - 중요데이터 보호

가용성 방해	 ① 공격자는 GPS Jammer를 이용하여 조작된 GPS 신호를 송신 ② GPS 수신기 및 센서를 장착한 드론은 정상 GPS 신호를 받지 못하고 조작된 GPS 신호를 계속 수신 ③ 조작된 GPS 신호를 정상 GPS 신호로 수신하여 정상 비행 경로 이탈 ▶ 드론 탈취, 무력화, 서비스 장애 등의 위협 발생	- HW 및 SW 안정성 - 인증 - 안전한 통신 - 안전한 비행
데이터 손실	 ① 공격자는 드론-지상제어장치 간, 드론-정보제공장치 간의 통신 세션에 접근 ② 세션을 가로채어 송·수신 메시지를 분석하고 위·변조 ③ 위·변조된 메시지를 지상제어장치, 정보제공장치에 전송 ▶ 데이터 유출, 허위 정보 제공, 서비스 장애 등의 위협 발생	- HW 및 SW 안정성 - 인증 - 중요 데이터 보호 - 보안감사
부적절한 암호사용	 ① 공격자는 드론-지상제어장치 간, 드론-정보제공장치 간의 통신 세션에 접근 ② 암호를 해제하고 중요한 정보를 추출 ▶ 데이터 유출, 서비스 장애 등의 위협 발생	- HW 및 SW 안정성 - 안전한 통신 - 암호 - 중요 데이터 보호

악 의 적 인 프로그램 실행	 ① 공격자는 드론의 펌웨어 구조와 프로토콜을 분석하여 펌웨어 변조 및 악성코드를 삽입 ② 펌웨어 변조를 통한 조작된 명령어 전송 및 제어권 탈취 ▶ 드론 탈취, 제어권 탈취, 중요정보 유출, 서비스 장애 등의 위협 발생	- HW 및 SW 안정성 - 인증 - 암호 - 중요데이터 보호
잘못된 설계 및 구현	 ① 공격자는 드론, 지상제어장치, 정보제공장치에 물리적으로 접근 ② 드론, 지상제어장치, 정보제공장치에 악성 메시지 전송 및 펌웨어 변조 ▶ 드론 탈취, 제어권 탈취, 중요정보 유출, 서비스 장애 등의 위협 발생	- HW 및 SW 안정성 - 안전한 통신 - 안전한 비행 - 중요 데이터 보호 - 보안감사

- 보안위협 시나리오별 취약점을 분석한 후 이에 대한 대응기술 적용

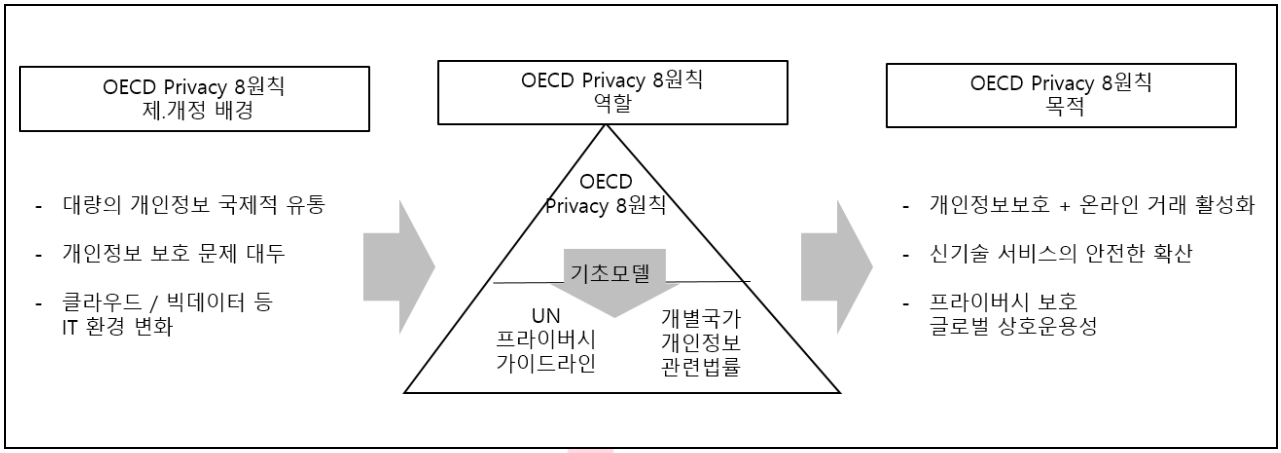
"끝"

기출풀이 의견

1. 가이드라인에 따라 전문적으로 답변하면 고득점이 가능합니다.
2. IoT 기기 보안과 드론의 특성을 결합하여 좋은 답안구성이 가능합니다.

문 제	4-5 경제협력개발협력기구(OECD) 프라이버시(privacy) 8 원칙		
출 제 영 역	보안	난 이 도	★★★☆☆
출 제 배 경	2020 년 데이터 3 법 개정과 마이데이터 사업 활성화로 개인정보 처리 중요성 부각		
출 제 빈 도	미출제		
참 고 자 료	- 개정 OECD 프라이버시 가이드라인 주요내용 및 향후 전망(주간기술동향 2014.6.4)		
K e y w o r d	기초모델, 수집제한, 정보 정확성, 목적명시, 이용제한, 안전성 확보, 공개, 개인참가, 책임		
풀 이	신지선 (122 회 정보관리기술사)		
감 수	채명희 (92 회 컴퓨터시스템응용기술사)		

1. 개인정보 관련 법안의 기초 모델, 경제협력개발기구(OECD) Privacy 8 원칙 개요



- OECD Privacy 8 원칙은 OECD Privacy 가이드라인에서 기본원칙으로 규정
- OECD Privacy 8 원칙은 UN 프라아버시 가이드라인, EU 개인정보 치침, 세계 각국의 개인정보 보호에 관한 법안과 규정 개발을 위한 기초 모델을 제공

2. 경제협력개발기구(OECD) Privacy 8 원칙

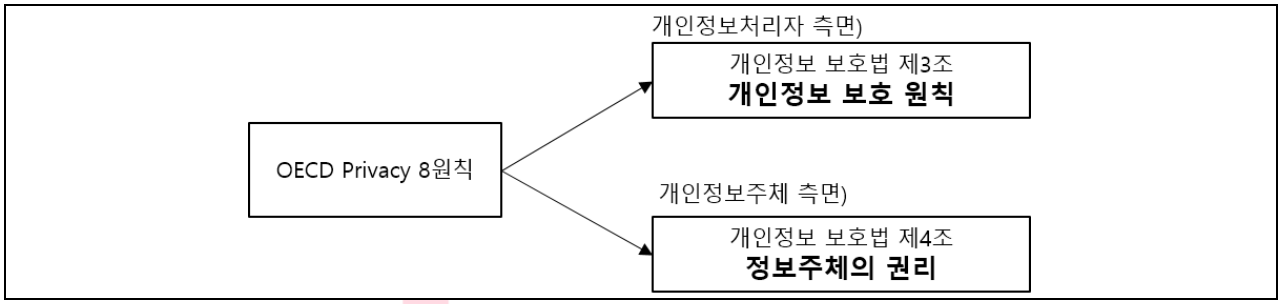
No.	원칙	주요내용
1	수집 제한의 원칙	- 적법하고 공정한 방법을 통한 개인정보의 수집 - 정보주체의 인지 또는 동의를 얻어 개인정보 수집
2	정보 정확성의 원칙	- 이용목적과의 관련성 요구 - 이용 목적상 필요한 범위 내에서 개인정보의 정확성, 완전성 확보
3	목적 명시의 원칙	- 수집 이전 또는 당시에 수집목적 명시 - 명시된 목적에 적합한 개인정보의 이용
4	이용제한의 원칙	- 정보주체의 동의가 있거나 법규정이 있는 경우를 제외하고는 목적 외 이용 및 공개 금지
5	안전성 확보의 원칙	- 개인정보의 침해, 누설, 도용 등을 방지하기 위한 물리적, 조직적, 기술적 안전조치 확보

6	공개의 원칙	- 개인정보의 처리 및 보호를 위한 정책의 공개 - 개인정보관리자의 신원 및 연락처, 개인정보의 존재 사실, 이용목적 등에 대한 접근 용이성 확보
7	개인 참가의 원칙	- 정보주체의 개인정보 열람, 정정, 삭제청구권 보장 - 정보주체가 합리적 시간과 방법에 의해 개인정보에 접근할 수 있도록 보장
8	책임의 원칙	- 개인정보관리자에게 원칙 준수 의무 및 책임 부과

- 향후 기술 발전을 수용할 수 있도록 기술 중립적인 원칙 반영
- 세계 각국의 개인 정보 관련 법안과 규정 개발을 위한 기초자료로 활용

3. OECD Privacy 8 원칙과 개인정보 보호법 비교

가. OECD Privacy 8 원칙과 개인정보 보호법 관계



- OECD Privacy 8 원칙을 반영하여 개인정보 처리 관련 원칙, 정보주체의 권리 정의

나. OECD Privacy 8 원칙과 개인정보 보호법 항목 비교

No.	OECD 8 원칙	개인정보 보호법
1	수집 제한의 원칙	-(제 3 조 1 항)목적에 필요한 최소정보의 수집 -(제 3 조 6 항)사생활 침해를 최소화하는 방법으로 처리 -(제 3 조 7 항)익명처리의 원칙
2	정보 정확성의 원칙	-(제 3 조 3 항)처리목적 내에서 정확성. 완전성. 최신성 보장
3	목적 명시의 원칙	-(제3조1항)처리목적의 명확화
4	이용제한의 원칙	-(제3조2항)목적 범위 내에서 적법하게 처리, 목적외 활용금지
5	안전성 확보의 원칙	-(제3조4항)권리침해 가능성 등을 고려하여 안전하게 관리
6	공개의 원칙	-(제3조5항)개인정보 처리방침 등 공개 -(제4조1항)개인정보 처리에 관한 정보를 제공받을 권리
7	개인 참가의 원칙	-(제3조5항)열람청구권 등 정보주체의 권리보장 -(제4조2항, 3항,4항) 개인정보 처리 정지.정정.삭제권
8	책임의 원칙	-(제3조8항)개인정보처리자의 책임준수. 신뢰확보 노력

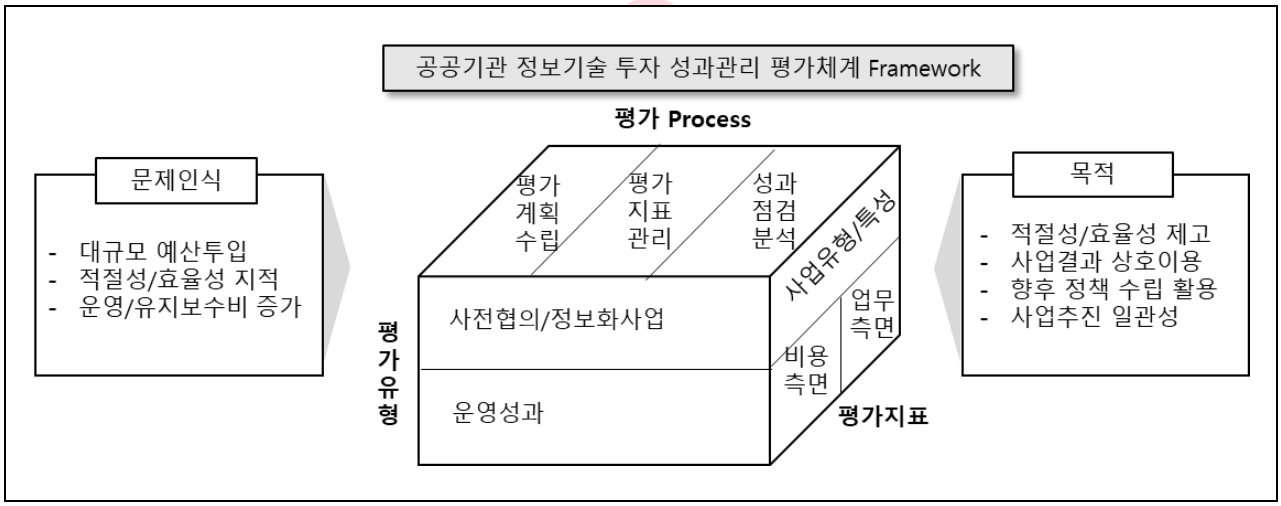
기출풀이 의견

1. OECD 프라이버시 8원칙 항목은 정확하게 표기하고 국내법과의 연관성을 설명합니다.

문 제	4-6 공공기관 정보기술 투자성과 성과관리를 평가체계 관점에서 설명		
출 제 영 역	경영전략	난 이 도	★★★☆☆
출 제 배 경	공공기관 전자정부 성과관리 시행 이후 성과와 한계점 도출		
출 제 빈 도	121 회 관리 3 교시, 116 회 컴시응 2 교시, 110 회 관리 3 교시		
참 고 자 료	- 전자정부 성과관리 평가로서 정보시스템 성과지표의 적정성 분석 (국회입법조사처 [입법과 정책] 제 12 권 제 2 호) - 전자정부 성과관리 매뉴얼		
Keyword	사전협의, 사전협의, 운영성과 측정, 성과관리 결과 환류		
풀 이	신지선 (122 회 정보관리기술사)		
감 수	채명희 (92 회 컴퓨터시스템응용기술사)		

1. 공공기관 정보기술 투자 성과관리 평가체계 Framework

가. 공공기관 정보기술 투자 성과관리 평가체계 Framework



- 공공기관 정보화사업의 투자성과 관리에 대한 문제를 인식하고 이를 해결하기위해 투자성과 평가체계 Framework 구성
- 평가체계를 수립함으로써 정보기술 투자성과에 대한 적절성/효율성을 제고하고 사업의 성과를 공유하여 거시적인 정부정책과의 일관성 수립

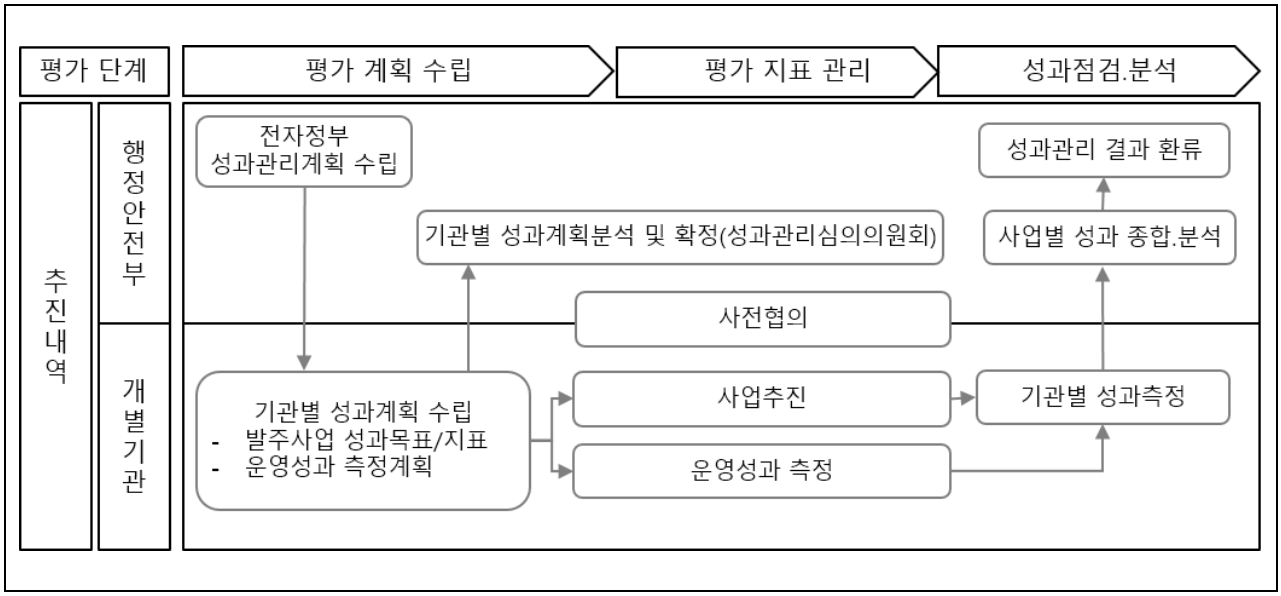
나. 성과관리 평가체계 평가유형

평가유형	설명	평가대상
사 전 협 의 / 정 보 화 사 업	- 신규 정보화사업에 대해 중복투자, 상호연계여부를 검토하고 사업내용을 조정, 성과관리 지표를 협의하여 관리하는 평가 유형	신규사업 계속사업
운 영 성 과	- 시스템 효율적 운영을 위해 성과를 측정하고 유지관리유형을 분류하여 관리하는 평가유형	3 년이상 정보시스템 1 년이상 모바일앱

- 근거법률) 전자정부법 제 67 조, 68 조에 의한 행정안전부 고시 "전자정부 성과관리지침"

2. 성과관리 평가체계 프로세스

가. 성과관리 평가체계 프로세스 절차도



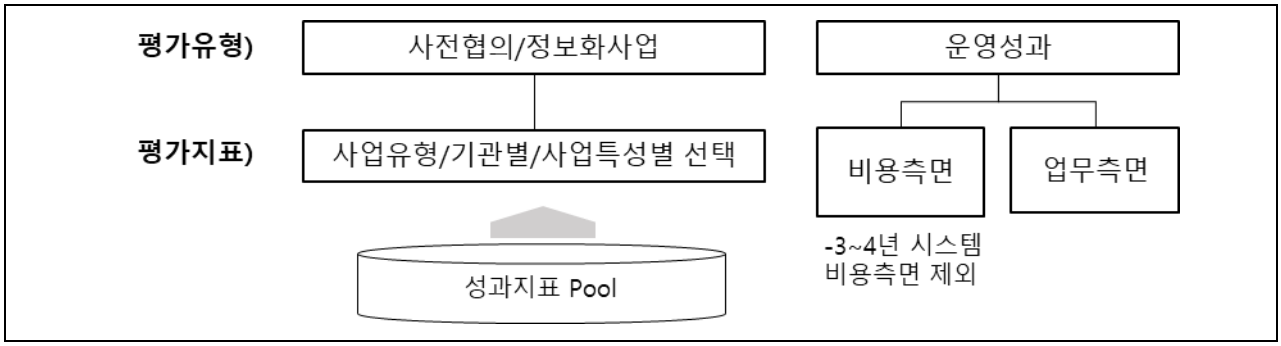
나. 성과관리 평가체계 프로세스 추진내역 상세설명

평가단계	추진내역	상세설명	수행주체
평가계획수립	1) 전자정부 성과관리계획수립	- 범정부 차원의 성과관리 목표를 수립	행정안전부
	2) 기관별 성과계획수립	- 발주사업에 대한 성과목표/ 성과지표 수립 - 운영성과 측정계획(대상,일정) 수립	개별기관
	3) 성과계획 분석 및 확정	- 성과관리심의위원회를 구성하여 성과계획 의적정성, 타당성 분석 및 확정	행정안전부
평가지표관리	4) 사업추진	- 사전협의 신청 및 검토결과 이행 - 성과계획시 수립한 목표. 지표관리	개별기관 행정안전부
	5) 운영성과측정	- 정보화사업/공공앱 운영 성과측정 및 후속조치 실실행	개별기관
성과점검/분석	6) 기관별 성과측정	- 정보화사업 성과측정 및 기관별 지표 측정	개별기관
	7) 사업별 성과 종합/분석	- 사전협의시 제출한 사업성과 관리 - 분석, 통계 작성	행정안전부
	8) 성과관리 결과 환류	- 성과결과를 차기 성과관리계획수립에 환류	행정안전부

- 개별기관에서 성과목표, 지표를 수립/수행/측정하고 행정안전부에서 이를 관리

3. 성과관리 평가체계 평가지표

가. 성과관리 평가체계 평가지표 구성



- 평가유형에 따라 평가지표 구성이 상이함

나. 사전협의/정보화사업 성과지표 Pool

정보화사업 유형	성과지표
기 획 . 구 축	업무처리건수증감률, 업무처리시간 개선율
구 축	데이터입력시간 절감률, DB 구축비율,
구 축 . 운 영	사이버침해 조기차단율, 서비스 재방문율, 시스템 응답속도 변동율, 문서 전자화율, 민원서비스 온라인 비율 등
운 영	사용자만족도, 신규 고객수, 고객증가율, 일일 평균 이용자 수, 서비스 이용 증가율, 시스템 접속 건수, 온라인 서비스 이용자 비율 등

- 사전협의시 사업형, 기관, 사업의 특성과 목적에 맞게 성과지표 Pool 에서 선택

다. 운영성과 측정지표

측정관점	측정지표	설명	측정항목
비용측면	누적 유지보수비 비율	정보시스템 개발에 소요된 총 금액 대비 연간 정보시스템 유지보수비 누계의 비율	운영의 적성성
	투입 운영유지비 증감율	정보시스템 우영과 유지보수를 위하여 요구되는 비용의 증감률	유지의 용이성
	평균 운영유지비 증감율	활용규모 당 평균 운영유지비의 증감률	비용의 효율성
업무측면	기능 활용도	업무지원 및 서비스 제공을 위해 구현된 기능의 활용 수준 측정	업무수행 영향도
	사용편의성	정보시스템 활용시 사용자가 느끼는 편의성 측정	사용상의 편의성
	목표대비업무성과달성도	직전 연도 성과 목표 대비 업무성과의 달성수준을 측정	업무성과 달성도
	업무성과 증감률	최근 3년 평균 업무성과의 증감률 측정	

"끝"

기출풀이 의견

1. 전자정부 성과관리 지침을 숙지하고 성과관리 체계를 기준으로 작성합니다.
2. IT 투자 성과관리 모델을 기반으로 공공기관을 특성을 가미하여 작성합니다.