ICT의 가치를 이끄는 사람들!!

125회

컴퓨터시스템응용기술사 기출풀이 2교시

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

국가기술자격 기술사 시험문제

기술사 제125회 제 2 교시 (시험시간: 100분)

분야	정보통신	종목	컴퓨터 시스템응용기술사	수험번호		성명	

※ 다음 문제 중 4문제를 선택하여 설명하시오. (각25점)

1. 내부망과 외부망을 분리하는 망분리시스템에 대하여 다음을 설명하시오.
   가. 망분리 개념 및 망분리 원칙
   나. 망분리 구축 유형의 특징 비교
   다. 망분리 방식의 장·단점

2. 코드 전송 시 발생하는 오류를 검출(Detection)할 수 있을 뿐만 아니라 오류 코드의 정정(Correction)이 가능한 해밍코드(Hamming Code)에 대하여 다음을 설명하시오. (단, Data는 4Bit로 가정하고 짝수 패리티를 사용한다.)
   가. 해밍코드의 구성
   나. 해밍코드의 정정과정 및 정정방법
   다. 해밍코드의 활용 사례

국가기술자격 기술사 시험문제

기술사 제125회 제 2 교시 (시험시간: 100분)

분야	정보통신	종목	컴퓨터 시스템응용기술사	수험번호		성명	

3. 정보시스템 마스터 플랜(ISMP, Information System Master Plan) 방법론에 대하여 다음을 설명하시오.

가. ISMP 정의

나. ISMP 수행 단계

다. ISP(Information Strategy Planning) 방법론과의 차이점

4. 사업유형이 정보시스템 개발인 경우 정보시스템 감리 점검 프레임워크 V3.0에 따라 다음 두 모델에 대하여 감리시점과 감리영역을 설명하시오.

가. 구조적/정보공학적 개발 모델

나. 객체지향/컴포넌트기반 개발 모델

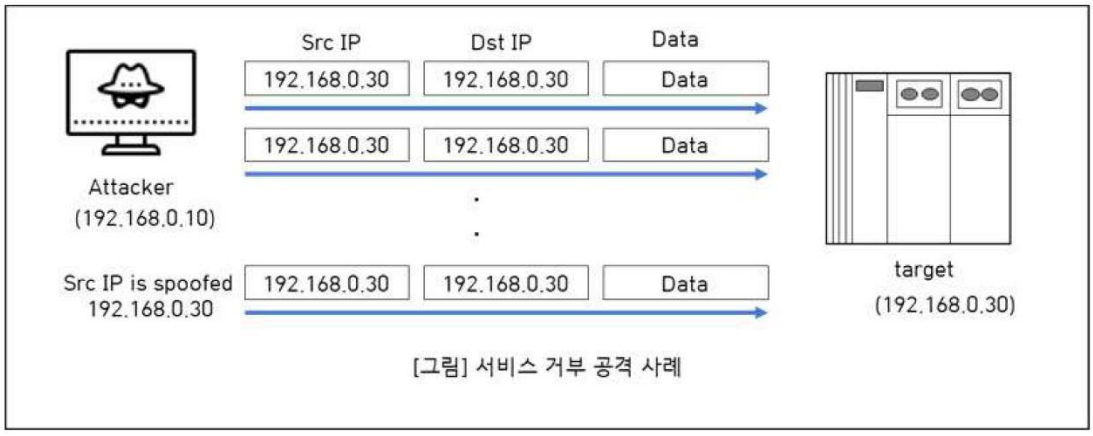
5. 공공안전망에 구현된 RAN-Sharing 목적과 기술방식을 각각 설명하시오.

국가기술자격 기술사 시험문제

기술사 제125회 제 2 교시 (시험시간: 100분)

분야	정보통신	종목	컴퓨터 시스템응용기술사	수험번호		성명	

6. 다음의 그림은 서비스 거부(DDoS, Distributed Denial of Service) 공격 사례이다. DDoS에 대하여 다음 내용을 설명하시오.



[그림] 서비스 거부 공격 사례

가. 위 사례의 공격기법 개념

나. 위 사례의 공격기법

다. 공격기법에 대한 보안 대책

문 제	**1. 내부망과 외부망을 분리하는 망분리시스템에 대하여 다음을 설명하시오.** **가. 망분리 개념 및 망분리 원칙** **나. 망분리 구축 유형의 특징 비교** **다. 망분리 방식의 장·단점**
출 제 영 역	디지털 보안 / 난 이 도 ★★★☆☆
출 제 배 경	- 금융권, 핀테크 업계에서 주장하는 망분리 규제 완화 - 코로나 19 로 비대면, 재택근무 활성화로 인한 망분리 규제 완화 의견 증가
출 제 빈 도	99 회 컴시응
참 고 자 료	- 알기쉬운 망분리 가이드(https://m.blog.naver.com/gojump0713/220433591216)
Keyword	망분리, 차단조치, 내부업무망, 외부 인터넷망, 보안관리, PMS, 논리적, 물리적, SBC, CBC
풀 이	임호용 기술사(123 회 정보관리기술사)

1. 외부 침입방지, 망분리의 개념 및 망분리 원칙 설명

가. 망분리의 개념

- 외부 인터넷 망을 통한 불법적인 접근과 내부 정보 유출을 차단하기 위해 내부 업무 망과 외부 인터넷 망을 분리하는 망 차단 조치

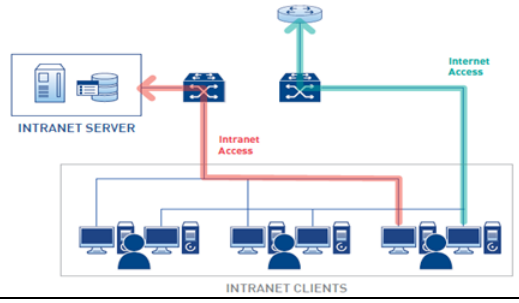
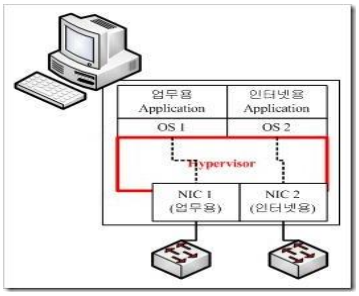
나. 망분리의 원칙

구분	원칙	설 명
단말기	PC 보안관리	- 인터넷망, 업무망에 접근하는 PC 를 분리, 인터넷 PC, 업무 PC 에 대한 보안관리 각각 수행하여야 한다
	보조기억장치 관리	- 인가된 보조기억장치(USB 메모리, CD, 이동식 하드디스크 등)만 사용하도록 통제되어야 한다.
통신	패치관리 시스템	- 패치관리시스템은 보안성 강화를 위하여 외부 인터넷 연결을 차단하고 인터넷망과 업무망에 각각 설치 운영 하여야 한다
	N/W 접근제어	- 비인가된 기기는 인터넷망과 업무망에 접속할 수 없도록 통제되어야 한다.
	프린터 등 주변기기운영	- 프린터 등 주변기기는 인터넷용 또는 업무용으로 분리 운영 되어야 한다. (VDI 는 논리적 분리 가능)
	무선 랜 사용 시 보안대책 강구	- 업무망과 인터넷간 망분리 효과를 와해시킬 수 있는 무선랜 등 무선 통신 관련 취약요소는 WIPS 설치, 통신차단 등 보안대책을 강구해야 한다.
데이터	인터넷 메일 사용	- 외부 이메일 송수신을 위한 메일 서버는 업무망과 분리하고 인터넷 PC 에서만 접근 가능하도록 한다.
	망간 자료전송	- 인터넷 PC 와 업무 PC 간의 자료 전송 또는 공개 서버와 업무 서버간 실시간 업무 연계 시 망간 자료전송 시스템 등을 운영할 수 있다.

- 망분리 원칙에 의거하여 구축 유형은 크게 물리적, 논리적, SBC, CBC 로 구분됨

2. 망분리 구축 유형 특징 비교 설명

가. 물리적, 논리적 망분리의 구축 특징 비교 설명

구 분	물리적 망분리	논리적 망분리
정의	2 대 이상의 PC 또는 네트워크 회선을 달리하여 내부망과 외부망을 분리하는 방식	가상화 기술을 이용해 내부 업무 전산망과 외부 인터넷망을 분리하는 방식
구성도		
구성요소	방화벽, DMZ, 네트워크 전환장치	가상화 서버팜, 침입차단시스템, 하이퍼바이저
구성방법	복수 PC, 네트워크 전환	서버방식, 클라이언트 방식
장점	- 완벽한 망 분리 구현 - 외부 해킹/악성코드로부터 보안 강화	- 별도 LAN 회선 추가/PC 확보 불필요 - 사용자 접근 용이
단점	- 망 사이 데이터 교환문제 발생, 생산성 저하 - 망전환 스위치 사용 또는 2 대 이상 PC 필요 - 사용자별 2 개 네트워크 회선 제공 필요	- 일부프로그램 경우 가상머신 환경 지원못함 - 가상환경에서 동작하도록 프로그램 일부 수정 필요 발생가능

- 논리적 망분리는 서버, 클라이언트 방식으로 구분됨

나. SBC, CBC 의 구축 특징 비교 설명

구 분	SBC(Server Based Computing)	CBC(Client Based Computing)
개념	서버에 가상영역을 두어 업무는 서버에서 수행, 사용자 PC 는 입/출력만 수행	기존에 사용하던 PC 에서 가상화를 시켜 망을 분리
구성도		
가상화수준	프레젠테이션, 어플리케이션, 데스크탑 가상화	하드웨어, 소프트웨어(커널/유저레벨) 가상화
장점	- 관리 편의성 증대(중앙관리, 패치, 배포 등) - 사용자별 개인화 환경 제공	- 관리 서버만 필요, 서버구매비용 절감 - 클라이언트 자원활용 가능
단점	- 고사양 서버, 서버팜 구축 필요 - N/W 대역폭 확장 필요	- 상이한 PC 환경으로 많은 문제 발생 가능 - 구축사례 부족으로 인한 낮은 신뢰성

- 이러한 물리적/논리적, SBC/CBC 망분리 방식은 각각 장, 단점 존재

3. 망분리 방식의 장·단점 설명

가. 망분리 방식의 장점 설명

방식	장점	설명
물리적	완벽한 망분리	- 물리적으로 네트워크망 분리로 인한 완벽한 망분리 수행
	보안 강화	- 외부망 PC, 내부망 PC 분리로 인한 외부 해킹, 악성코드로부터 보안강화
논리적	추가 자원 불필요	- 추가적인 네트워크 회선, PC 확보 불필요로 자원, 비용절약 효과
	사용자 접근 용이	- 개인 PC 에서 망분리 수행, 접근성 및 활용성 용이
SBC	관리 편의성 증대	- 중앙관리, 패치관리, 배포관리 등으로 유지/관리 비용 감소
	개인화 환경 제공	- 서버 내 사용자별 VM 할당, 개인화된 가상화 데스크탑 환경 제공
CBC	구매비용 절감	- 업무자 PC 사용으로 고사양 서버 구매 비용 절감
	자원활용	- 클라이언트 PC 자원(CPU, GPU, 메모리 등) 활용, 유휴 자원 활용

- 보안성, 편의성 측면에서 망분리의 장점이 있으나, 단점도 존재

나. 망분리 방식의 단점 설명

방식	단점	설명
물리적	회선 증설	- PC 2 대 사용으로 인한 2 개의 네트워크 회선 증설로 추가 비용 발생
	데이터 교환 문제	- 망 교환 체계를 통한 데이터 교환 어려움, 업무 효율 저하 발생
논리적	가상머신 환경	- 사용자 PC 마다 가상머신 환경 운용 불가능 경우 발생 가능
	프로그램 수정	- 가상머신 사용 시 해당 환경에서 운용되도록 프로그램 수정 발생 가능
SBC	높은 구매비용	- 고사양 서버팜 구축으로 인한 초기 높은 구매비용 발생
	N/W 대역폭 확장	- 사용자 가상환경의 I/O 데이터 안정적 전송을 위한 N/W 고대역폭 필요
CBC	상이한 PC 환경	- 사용자 PC 환경(H/W, S/W, OS 등)의 상이함으로 인한 문제 발생 가능
	저 신뢰성	- 구축사례 부족으로 인한 해당 망분리의 낮은 신뢰성 문제

- 망분리 구축 유형 특징과 장, 단점을 충분히 숙지하여 망분리 시 올바른 기술을 도입해야 함

4. 망분리 기술 도입 시 고려사항 설명

유형	고려사항	설명
물리적	충분한 사례	- 기술적 난이도가 높지 않고, 기존에 충분히 검토된 기술 사용 시 선택
논리적	높은 보안성	- 외부접속 단말 통합 관리, 적은 도입비용으로 높은 보안성 필요 시 선택

- 내부인의 고의적인 정보유출, 악성코드 유입에도 철저한 관리 필요 **"끝"**

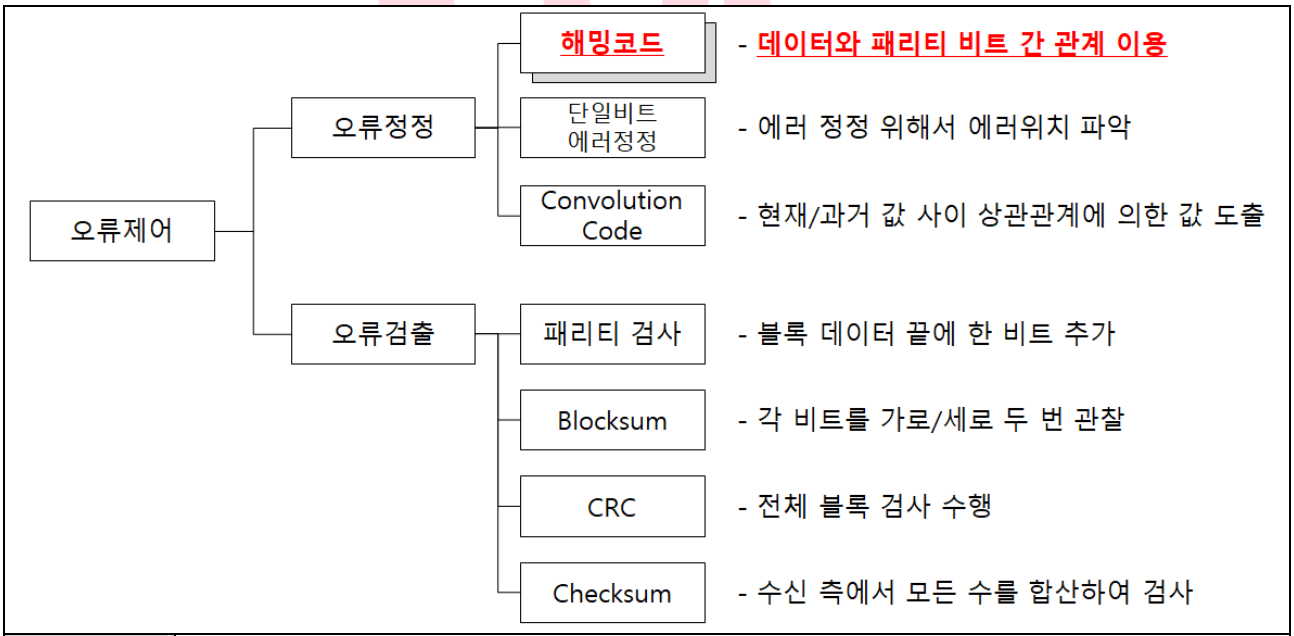
기출풀이 의견

1. 망 분리의 정확한 정의, 원칙, 수행근거를 자세하게 작성하시고, 구축 유형 비교를 도식화를 포함하여 상세 작성, 장/단점으로 차별화하여 작성하시면 고득점을 기대할 수 있겠습니다.

문 제	**2. 코드 전송 시 발생하는 오류를 검출(Detection)할 수 있을 뿐만 아니라 오류 코드의 정정(Correction)이 가능한 해밍코드(Hamming Code)에 대하여 다음을 설명하시오.** **(단, Data 는 4Bit 로 가정하고 짝수 패리티를 사용한다.)** **가. 해밍코드의 구성** **나. 해밍코드의 정정과정 및 정정방법** **다. 해밍코드의 활용 사례**

출 제 영 역	디지털 네트워크	난 이 도	★★★☆☆
출 제 배 경	122 회 컴시응, 해밍거리 확장		
출 제 빈 도	미출제		
참 고 자 료	- 정보통신기술용어해설(http://www.ktword.co.kr/test/view/view.php?m_temp1=1212) - 데이터 통신 개정 3 판(생능출판) - 해밍코드(https://blog.naver.com/vanpelt/100138087430)		
Keyword	선형부호, 패리티 비트, 해밍코드, 오류검출, 오류정정, 신드롬, 신드롬 테이블, XOR 연산		
풀 이	임호용 기술사(123 회 정보관리기술사)		

1. 신뢰성 있는 데이터 전송, 오류제어의 개요



해밍코드 정의	- 선형 부호방법으로 수신 측에서 오류가 발생한 Bit 를 찾아 직접 오류를 수정하는 오류정정 기법

- 원본 데이터들을 이용, 연산 결과를 덧붙여 수신 측에서 에러 검출, 해당 비트를 정정 가능

2. 해밍코드의 구성 설명

가. 해밍코드의 구성

구 분	구성	설 명
해밍 코드	데이터 비트	- 문제에서 제시한 **4Bit 는 1001 로 가정**.
	XOR 연산	- 패리티 비트를 구하기 위한 연산 수행
	패리티 비트 수 조건	- $2^P \geq m + P + 1$, (**m** : 데이터 비트 수, **P** : 패리티 비트 수)
	최소해밍거리	- 임의 두 부호어(코드) 쌍 간에 항상 N 비트만 상이함
패리티	패리티 비트	- m = 4(데이터 비트 수 4, 문제 제시) 일 때, P 는 $2^P - P \geq 5$. - P = 3 일 때, $2^3 - 3 \geq 5$, 8 - 3 = 5, 따라서 **패리티 비트 수는 3 개, 총 비트는 7 개**
	패리티 비트 위치	<table><tr><td>**비트**</td><td>7</td><td>6</td><td>5</td><td>**4**</td><td>3</td><td>**2**</td><td>**1**</td></tr><tr><td>**해밍 코드**</td><td>D7</td><td>D6</td><td>D5</td><td>**P4**</td><td>D3</td><td>**P2**</td><td>**P1**</td></tr></table> - 패리티 비트 위치는 2^N 으로 위치 결정(N ≥ 0, N 은 **3-1 = 2** 까지)
	홀수/짝수 패리티	- **홀수 패리티** : 전체 비트에서 1 의 개수가 홀수가 되도록 하는 비트 - **짝수 패리티** : 전체 비트에서 1 의 개수가 짝수가 되도록 하는 비트

- 문제에서 주어진 조건에 맞게 해밍코드 변환 시 **짝수 패리티** 사용

나. 주어진 조건에 따른 해밍코드의 변환과정

구 분	변환과정	설 명
위치	패리티 비트 위치	<table><tr><td>**비트**</td><td>7</td><td>6</td><td>5</td><td>**4**</td><td>3</td><td>**2**</td><td>**1**</td></tr><tr><td>**해밍 코드**</td><td>D7</td><td>D6</td><td>D5</td><td>**P4**</td><td>D3</td><td>**P2**</td><td>**P1**</td></tr></table> - 패리티 비트 위치는 2^N 으로 위치 결정(N ≥ 0, N 은 **3-1 = 2** 까지)
규칙	패리티 비트 규칙 결정	① 비트 번호가 **3, 5, 7** 인 비트 검사, 짝수 패리티가 되도록 P1 비트 값 결정 ② 비트 번호가 **3, 6, 7** 인 비트 검사, 짝수 패리티가 되도록 P2 비트 값 결정 ③ 비트 번호가 **5, 6, 7** 인 비트 검사, 짝수 패리티가 되도록 P3 비트 값 결정
계산/ 할당	데이터 비트 할당	<table><tr><td>**비트**</td><td>**7**</td><td>**6**</td><td>**5**</td><td>4</td><td>**3**</td><td>2</td><td>1</td></tr><tr><td>**해밍 코드**</td><td>**1**</td><td>**0**</td><td>**0**</td><td>P4</td><td>**1**</td><td>P2</td><td>P1</td></tr></table> - 비트 3, 5, 6, 7 순으로 4 Bit 인 1, 0, 0, 1 각각 할당
	패리티 비트 계산	- 문제 조건에 맞도록 **짝수 패리티** 사용, 패리티 비트 연산은 **XOR 연산** 사용 ① **3, 5, 7** 번 비트가 각각 1, 0, 1 이므로 **P1 = 0** ② **3, 6, 7** 번 비트가 각각 1, 0, 1 이므로 **P2 = 0** ③ **5, 6, 7** 번 비트가 각각 0, 0, 1 이므로 **P4 = 1**
	패리티 비트 할당	<table><tr><td>**비트**</td><td>7</td><td>6</td><td>5</td><td>**4**</td><td>3</td><td>**2**</td><td>**1**</td></tr><tr><td>**해밍 코드**</td><td>1</td><td>0</td><td>0</td><td>**1**</td><td>1</td><td>**0**</td><td>**0**</td></tr></table>

- 패리티 비트 수 조건에 따른 패리티 비트 갯수 도출을 통한 전체 해밍코드는 **1001100**

3. 해밍코드의 정정과정 및 정정방법 설명

가. 해밍코드의 정정과정

구분	정정과정	설명
변화	해밍코드 변화	- 전송 시 노이즈 등으로 인하여 데이터 오류 발생, 송/수신 데이터 무결성 위배
확인/수정	신드롬 생성	- 데이터, 패리티 비트를 XOR 연산한 값 생성
	오류위치 확인	- 신드롬 표를 사용하여 변화가 발생한 패리티 비트, 오류 비트 위치 확인
	오류 수정	- 확인된 오류 비트 위치를 확인하여 비트 정정

- 오류가 발생한 해밍코드에 대해 신드롬 표를 사용하여 오류 위치 검출하여 정정 수행

나. 해밍코드의 정정방법

<table>
<tr><th>구분</th><th>정정방법</th><th>설명</th></tr>
<tr><td>변화</td><td>해밍코드 변화</td><td>- 송신 측 코드 : 1001100 데이터 송신
- 수신 측 코드 : 1101100 으로 데이터 수신
- 전송 시 데이터 변화로 인한 수신 오류로 판단</td></tr>
<tr><td rowspan="3">확인/수정</td><td>신드롬 생성</td><td>- 신드롬표 생성규칙을 따른 신드롬 생성
- 데이터 비트는 1001(m_4, m_3, m_2, m_1 순),
- 패리티 비트는 001(p_3, p_2, p_1 순)임
<table>
<tr><th>신드롬</th><th>계산식</th><th>계산</th><th>결과</th></tr>
<tr><td>s_1</td><td>$m_1 \oplus m_2 \oplus m_3 \oplus p_1$</td><td>$1 \oplus 0 \oplus 0 \oplus 0$</td><td>1</td></tr>
<tr><td>s_2</td><td>$m_2 \oplus m_3 \oplus m_4 \oplus p_2$</td><td>$0 \oplus 0 \oplus 1 \oplus 0$</td><td>1</td></tr>
<tr><td>s_3</td><td>$m_1 \oplus m_2 \oplus m_4 \oplus p_3$</td><td>$1 \oplus 0 \oplus 1 \oplus 1$</td><td>1</td></tr>
</table>
- $s_1 = 1, s_2 = 1, s_3 = 1$ 이므로 신드롬 표에서 매치되는 오류 패턴, 위치 확인</td></tr>
<tr><td>신드롬 표를 통한 오류위치 확인</td><td>
<table>
<tr><th colspan="3">신드롬</th><th colspan="7">오류 패턴</th><th>오류위치</th></tr>
<tr><th>S_3</th><th>S_2</th><th>S_1</th><th>E_7</th><th>E_6</th><th>E_5</th><th>E_4</th><th>E_3</th><th>E_2</th><th>E_1</th><th>-</th></tr>
<tr><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>오류없음</td></tr>
<tr><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td><td>P1</td></tr>
<tr><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td>P2</td></tr>
<tr><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td><td>D3</td></tr>
<tr><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>P4</td></tr>
<tr><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>D5</td></tr>
<tr><td>1</td><td>1</td><td>1</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>D6</td></tr>
<tr><td>1</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>D7</td></tr>
<tr><td colspan="3">송신비트 : 1001100</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>-</td></tr>
<tr><td colspan="3">수신비트 : 1101100</td><td>1</td><td>1</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>6 번 비트</td></tr>
</table>
</td></tr>
<tr><td>오류 정정</td><td>- 신드롬 표를 통해 파악된 오류위치 6 번 비트에 대해 오류 정정
- <u>수신한 6 번째 비트인 1 을 0 으로 정정</u></td></tr>
</table>

- 오류 위치를 확인 후 정정하는 메커니즘을 다양한 분야에서 활용하고 있음

4. 해밍코드의 활용사례 설명

구분	활용사례	설명
디스크	SSD	- SSD 컨트롤러 내 탑재, 잡음마진 감소에 따른 오류 보완
	RAID-2	- 에러체크, 수정을 위해 해밍코드 사용
메모리	ECC Memory	- 싱글 비트 오류에 메모리 시스템 면역 관리.(*일반 DIMM 대비 +1 개 메모리 칩)

- 이외 데이터 은닉 등 다양한 분야에서 오류수정 위한 해밍코드 활용 **"끝"**

기출풀이 의견

2. 해밍코드가 어느 기법으로 분류되는지, 변환과정을 포함한 정정과정과 정정방법을 정확하고 가독성 있게 작성해 주시면 좋겠습니다.

문 제	3. 정보시스템 마스터 플랜(ISMP, Information System Master Plan) 방법론에 대하여 다음을 설명하시오. 가. ISMP 정의 나. ISMP 수행 단계 다. ISP(Information Strategy Planning) 방법론과의 차이점
출 제 영 역	IT 경영전략 / 난 이 도 ★★★☆☆
출 제 배 경	- 빅데이터 플랫폼 구축 등 신규사업 컨설팅 발생 증가
출 제 빈 도	125 회 관리, 119 회 관리
참 고 자 료	- 위키피디아-정보시스템 마스터플랜(https://ko.wikipedia.org/wiki/정보시스템_마스터플랜) - 정보시스템 마스터플랜(ISMP) 방법론
K e y w o r d	현황, 요구사항 분석, 기능점수 도출, 상세기술, 착수, 방향성, 요건분석, 요건정의, 이행방안
풀 이	임호용 기술사(123 회 정보관리기술사)

1. 정보시스템 구축의 마스터 플랜, ISMP 의 정의 설명

가. ISMP 의 정의

- SW 개발사업의 상세분석, RFP 마련을 위해 현황과 요구사항을 분석, 기능점수 도출 수준까지 상세히 기술하며, 구축전략 및 이행계획을 수립하는 활동

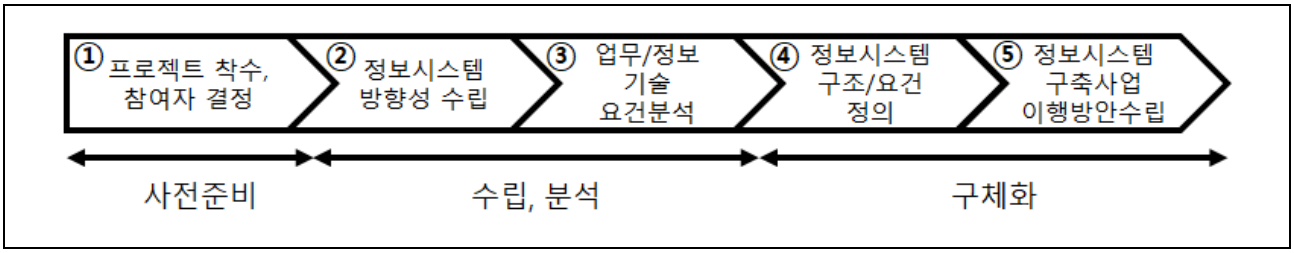
나. ISMP 의 참조모델 특징

구 분	참조모델 특징	설 명
계획	FSAM 기반	- EA 와 연계된 업무라인의 효율적인 정보화 계획 및 아키텍처 수립
	MBT 방법론	- 업무 전략 재 정의, 목표 아키텍처 계획 및 구현을 수행하기 위한 일련의 활동, 과업, 관리 체크 포인트, 커뮤니케이션 방안
프로세스	ISO 12207	- S/W 의 도입을 위한 준비, 특정 SW 제안 요청서(RFP) 작성 및 선정, 그리고 도입 준비단계 연계
상세화	IFPUG 활용	- 정보시스템의 규모 및 예산을 측정하는 활동을 상세화

- 참조모델들의 자료 분석을 통해 충분한 이해 후 목적과 실제 정보시스템 구축에 적합한 정교한 모델 개발

2. ISMP 의 수행 단계 설명

가. ISMP 의 수행단계



- 각 단계는 세부 수행 활동으로 구성, 필수 활동과 선택 활동으로 구분

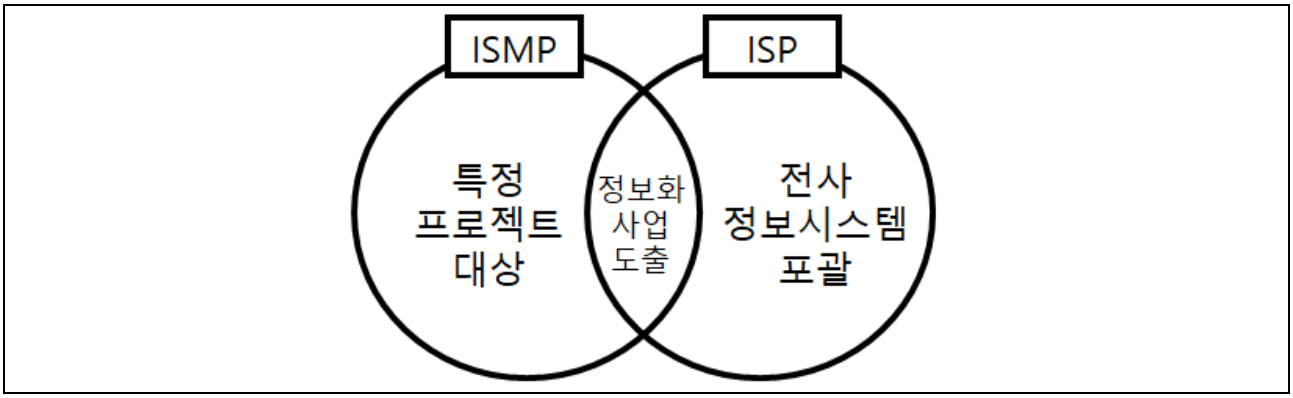
나. ISMP 의 수행단계 상세 설명

수행활동	수행활동	설 명
①프로젝트 착수, 참여자 결정	경영진 지원조직 형성	- 프로젝트 관련 조직 파악, 경영진 지원조직 확립
	프로젝트 수행 조직편성	- 프로젝트 수행 역할 정의, 인력 결정, 리더쉽 확보
	프로젝트 계획 수립	- 프로젝트 수행, 의사소통계획 수립, 계획 검토
②정보시스템 방향성 수립	정보화 전략 검토	- 정보화전략/방향검토, 정보시스템 사업이해/과제식별
	벤치마킹 분석	- 벤치마킹 조사대산 선정, 준비, 실시 등
	정보시스템 추진범위/방향 정의	- 정보시스템 구축범위, 사용자 그룹, 추진방향/목표 정의
	정보시스템 범위/방향 검토	- 정보화 전략과 방향일치, 추진범위 검토
③업무/ 정보기술 요건분석	업무/정보기술 현황 분석	- 업무프로세스, 응용/데이터/기술기반 아키텍처 분석
	업무요건 분석	- 업무요건 분석준비, 최종사용자 요구사항 도출
	정보기술 요건 분석	- 도입대상장비/데이터/표준화요건/보안요건 분석 등
	업무/정보기술 요건 검토	- 업무/정보기술 요건 최종검토, 우선순위 평가
④정보시스템 구조/요건 정의	정보시스템 아키텍처 정의	- 정보시스템 To-Be 아키텍처 정의, 재사용 가능요소 파악
	요건 간 이행 연관성 분석	- 정보시스템 연관성 분석, 이행연관성 고려 등
	정보시스템 요건 기술서 작성	- 요건 기술표준 정의, 경계식별, 기능/비기능 요건기술 등
	정보시스템 요건 기술서 검토	- 정보시스템 요건 기술서 점검 및 최종 검토
⑤정보시스템 구축사업 이행방안 수립	정보시스템 구축사업 계획수립	- 정보시스템 구축범위 확정, 기대효과/추진전략 수립 등
	분리발주 가능성 평가	- 관련 패키지 조사, 분리발주 가능성 분석 등
	정보시스템 예산 수립	- 정보시스템 기능점수 산정, 예산 검토
	RFP 작성	- RFP 목차수립, 세부내용 작성, 제안안내서 작성, 검토
	구축업체 선정/평가 지원	- 정보시스템 구축업체 선정/평가 준비, 수행

- 구성 단계가 반복적으로 여러 번 수행되는 것이 아닌, 하나의 사업으로 마무리될 수 있도록 한 사이클만 수행

3. ISP 방법론과의 차이점 설명

가. ISMP 와 ISP 의 관계



- 정보화 사업 도출 관점에서 ISP 와 ISMP 유사. ISP 는 전사 정보시스템 포괄, ISMP 는 특정 프로젝트를 대상

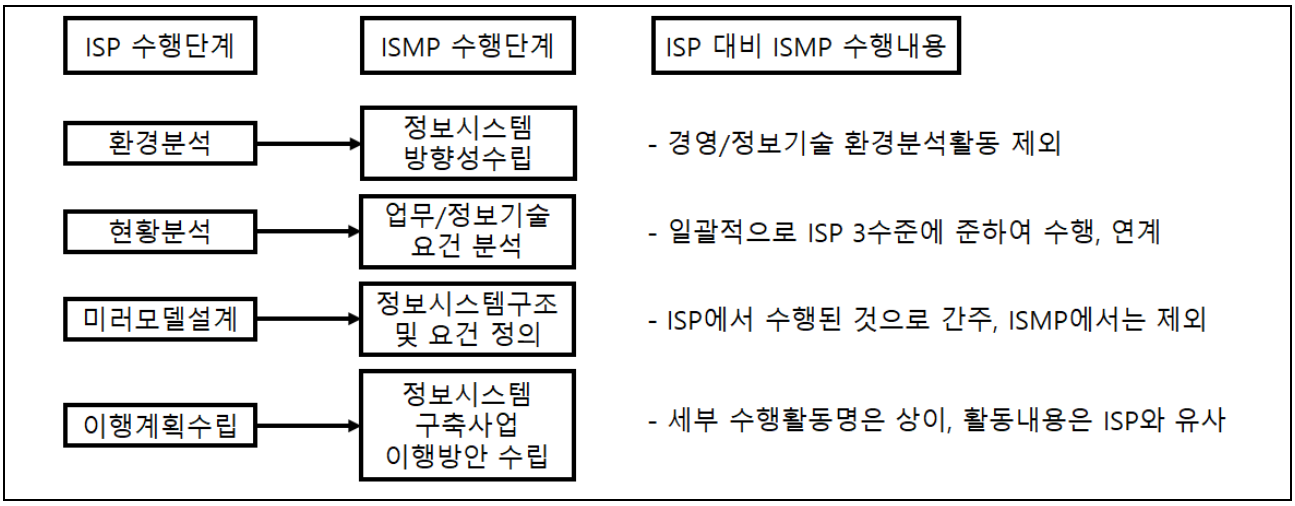
나. ISMP 와 ISP 차이점 설명

구분	ISMP	ISP
목적	시스템 기능적 요구사항 상세화	경영전략과 정보화 전략 연계
범위	단위 프로젝트, 프로젝트 묶음	전사, 서비스, 부서 정보화전략

주요활동	구축 범위/방향, 기능 요건 도출, 요건 상세기술, 이행 계획 수립, 예산 산정 업체 선정, 평가 지원	경영환경 분석, 기술 동향 분석, 업무 분석, 시스템구조 분석, 정보화전략 수립, 시스템구조 설계, To-Be 로드맵
주요산출물	RFP, 정보시스템 예산	경영환경/기술동향 분석서, 정보시스템 분석, IT 비전/전략, 이행과제 및 로드맵
환경분석활동	환경분석활동 불필요	환경분석활동 필요
업무/정보 시스템 분석	S/W 사업 범위 내 업무/정보시스템 현황 파악, 사용자 요구사항 도출	경영목표 전략 기준 정보시스템 문제점/개선 방향 분석
설계대상	특정 S/W 사업 사용자/비즈니스 기능/기술/ 비기능/프로젝트지원 요구사항 상세설계	정보화전략, 업무프로세스, 정보시스템 구조/ 정보관리 조직체계. 개선방향/이행과제 정의
제안요청서 상세화 수준	구축기능의 입출력정보/절차, 기능검증 요건 까지 기술. 기능점수도출 가능 레벨 상세화	이행과제의 구축대상, 적용 기술을 제안 요청서에 정의하는 정도 수준

- ISMP 와 ISP 는 각 사업 간 수행단계에서도 차이 발생, 단계간 대응위한 노력 필요

4. ISMP 와 ISP 사업 간 수행단계 대응을 통한 차이점 설명



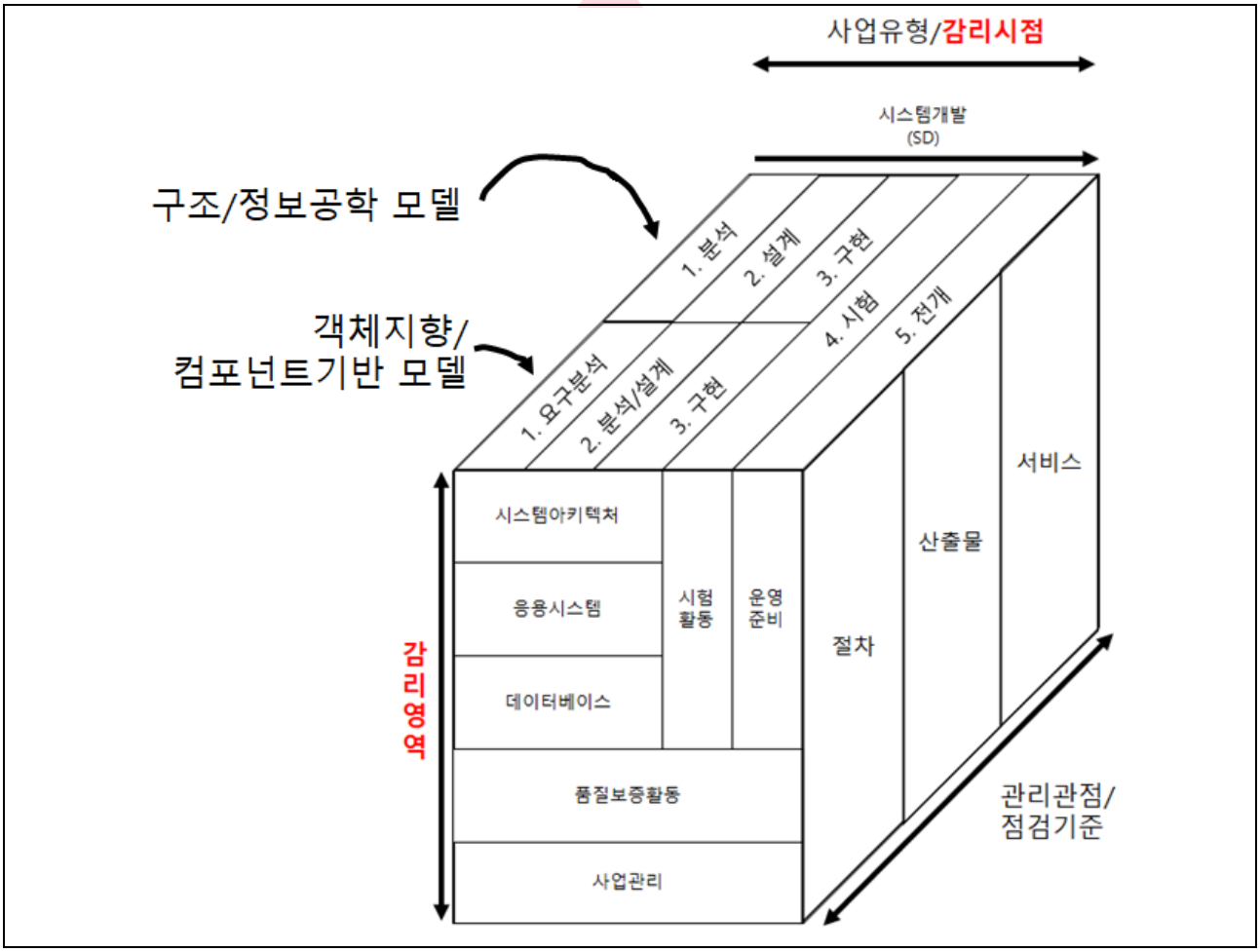
- 이외 수행활동 가중치, 난이도 보정계수 등을 통해 보다 정교한 마스터 플랜 수립 가능 **"끝"**

기출풀이 의견

3. ISMP의 수행 단계와 각 세부 수행활동, ISP와 비교했을 때 명확한 구분으로 차이점을 작성하시면 고득점을 노릴 수 있을 것 같습니다.

문 제	4. 사업유형이 정보시스템 개발인 경우 정보시스템 감리 점검 프레임워크 V3.0 에 따라 다음 두 모델에 대하여 감리시점과 감리영역을 설명하시오. 가. 구조적/정보공학적 개발 모델 나. 객체지향/컴포넌트기반 개발 모델		
출 제 영 역	소프트웨어 공학	난 이 도	★★★☆☆
출 제 배 경	정보시스템 감리기준 개정에 따른 정보시스템 감리 학습 내용 점검		
출 제 빈 도	92 회 관리, 98 회 컴시응		
참 고 자 료	- 정보시스템 감리점검 해설서 V3.0		
Keyword	감리시점, 감리영역, 구조적, 정보공학적, 객체지향, 컴포넌트기반, 요구분석, 설계, 구현, 시험, 전개		
풀 이	임호용 기술사(123 회 정보관리기술사)		

1. 정보시스템 감리점검 프레임워크 V3.0 의 개요



- 사업유형이 정보시스템 개발은 크게 구조/정보공학 개발모델과 객체지향/컴포넌트기반 개발모델로 구분

2. 구조적/정보공학적 개발 모델의 감리시점과 감리영역 설명

감리시점	감리영역	설 명
분석	시스템 아키텍처	- 현행 시스템 운영환경 분석, 시스템 관련 사용자 요구사항 충분히 도출 - 요구사항을 만족하는 기술 아키텍처 구성, 용량 등 분석여부 점검
	응용시스템	- 현행업무/시스템 분석, 사용자 요구사항의 충분한 도출 - 업무 프로세스, 이벤트 모델링 보안관련 분석 적정수행여부 점검
	데이터베이스	- 현행 업무/시스템 데이터베이스 관련 현황 분석 - 사용자 요구사항 충분한 도출 및 데이터 모델링 적정 도출여부 점검
설계	시스템 아키텍처	- 사용자 요구사항/분석결과로 시스템 구조적/구성요소들 상세설계 수행 - 시스템 설치, 검증/전환계획 등 적정 수립여부 점검
	응용시스템	- 사용자 요구사항/분석결과로 업무기능, 사용자 UI, 내/외부 UI 등을 구현 가능 수준으로 적정 설계하였는지 여부 점검
	데이터베이스	- 사용자 요구사항/분석결과로 데이터 분산, 무결성/성능 등을 고려한 데이터베이스 상세설계 수행 - 초기 데이터 구축/전환 위한 계획 적정 수립여부 점검
구현	시스템 아키텍처	- 설계에 따라 시스템 도입/설치위한 시험/검증 수행 - 시스템 시험계획 적정수립여부 점검
	응용시스템	- 설계에 따라 응용시스템 기능 충분성/완전성/무결성/편의성/적정성 확보할 수 있도록 구현 - 단위 기능에 대한 검증을 수행했는지 여부 점검
	데이터베이스	- 설계에 따라 데이터 무결성, 성능, 보안성을 확보할 수 있도록 구현 - 응용시스템 기능에 따른 데이터 정합성 검증여부 점검
시험	시험활동	- 통합시험, 시스템 시험을 통하여 구현된 시스템이 통합적 관점에서 기능 완전성, 성능, 안전성, 보안성 확보 여부를 검증했는지 점검
전개	운영준비	- 시스템 운영을 위한 시스템 설치/배포/초기데이터 구축 등 준비 완료 - 시스템이 사용자에게 이관/운영될 수 있도록 준비여부 점검

- 객체지향/컴포넌트기반 개발모델은 시험활동/운영준비의 감리시점, 영역과 상이한 점이 존재

3. 객체지향/컴포넌트기반 개발 모델의 감리시점과 감리영역 설명

감리시점	감리영역	설 명
요구분석	시스템 아키텍처	- 현행 시스템 운영환경 분석, 시스템 관련 사용자 요구사항 **도출/분석** - **상위 수준** 시스템 아키텍처 정의, 기술여부 점검
	응용시스템	- 업무영역 분석, 사용자 요구사항 도출/분석 수행 - 시스템 기능에 대한 **유스케이스 모형 정의, 분석 클래스 도출** 적정 수행여부 점검
	데이터베이스	- 현행 업무/시스템 데이터베이스 관련 현황 분석 - 사용자 요구사항 충분한 도출 확인 및 **개념적 수준 엔티티 클래스를 충분하게 도출**하였는지 점검
분석/설계	시스템 아키텍처	- **프로토타이핑 등 기술 검증** 통한 **최종적 시스템 아키텍처 적정 설계** - 전반적 시스템 전환계획 수립여부 점검

	응용시스템	- 요구분석 결과, 업무/사용자 요구사항에 대한 상세분석에 따라 **시스템 기능에 대한 유스케이스 모형/클래스를 충분히 정제** - 시스템을 **구현 가능한 수준**으로 설계하였는지 점검
	데이터베이스	- 요구분석 결과/상세 분석에 따라 **엔티티 클래스 충분히 정제** - 데이터의 분산, 무결성, 성능, 백업/복구 등을 고려한 **상세설계**, 초기데이터 구축/전환 **계획수립** 적정 수행여부 점검
구현	**시스템 아키텍처**	- 설계에 따라 시스템 도입/설치위한 시험/검증 수행 - 시스템 시험계획 적정수립여부 점검
	응용시스템	- 설계에 따라 응용시스템 기능 완전성, 무결성, 편의성, 적정성 등 확보할 수 있도록 **컴포넌트 도입/개발에 의해 구현** - 단위 기능에 대한 검증을 수행했는지 여부 점검
	데이터베이스	- 설계에 따라 데이터의 무결성, 성능, 보안성을 확보할 수 있도록 구현 - 기능에 따른 데이터 **정합성을 확보**하였는지 점검

- 각 개발모델 별 공통적인 활동에 대한 품질보증활동 및 사업관리 활동 설명

4. 품질보증활동 및 사업관리의 감리시점 및 감리영역 설명

감리시점	감리영역	설 명
분석(요구분석)	**품질보증활동**	- 사업 추진을 위한 방법론, 절차, 표준, 품질보증계획 수립 - 관련 산출물을 적정하게 작성했는지 점검
설계(분석/설계)		- 기 수립된 방법론, 절차, 표준, 품질보증계획에 의거, 각 활동 수행, 관련 산출물을 적정하게 작성했는지 점검
구현		
시험		- 기 수립된 방법론, 절차, 표준, 품질보증계획에 의거, 각 활동 수행, 관련 산출물을 적정하게 작성했는지 점검 - 초기 사업의 목표달성여부, 교육계획 등의 적정성 점검
전개		- 사업 마감, 구축된 시스템을 운영환경으로 이관하기 위한 준비, 각종 절차/계획 적정 수행여부 점검
착수/계획	**사업관리**	- 계획을 구체적, 실행가능 수준으로 수립했는지 여부, 실행결과가 요구사항을 충족시킬 수 있는지 점검
실행/통제		- 사업관리 계획에 따라 적절히 실행/통제하고 있는지 점검
종료		- 계획된 일정 내 사용자 요구사항 만족, 사업을 정상적으로 완료할 수 있는지 점검

- 각 감리영역들은 일련의 절차, 산출물, 서비스의 기준으로 점검되고 관리되어야 함 **"끝"**

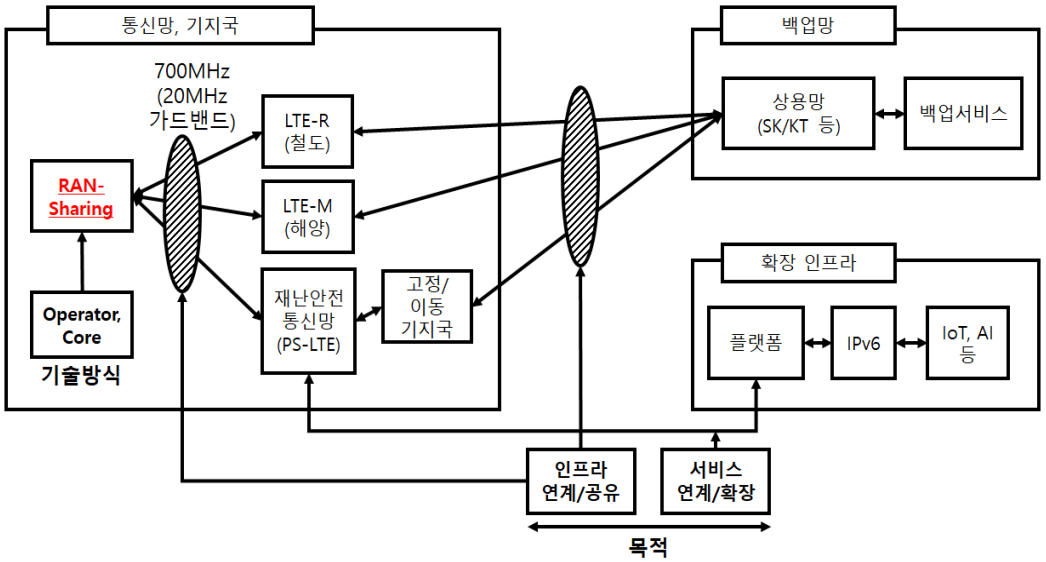
기출풀이 의견

4. 정보시스템 개발의 사업영역 감리 프레임워크를 정확히 작성하신 후, 감리시점/감리영역 및 각 모델의 차이가 발생하는 부분에 대해서 구체적인 활동을 작성해야 합니다.

문 제	5. 공공안전망에 구현된 RAN-Sharing 목적과 기술방식을 각각 설명하시오.		
출 제 영 역	디지털 네트워크	난 이 도	★★★☆☆
출 제 배 경	- 통합공공망 상호운영성 확보, 전국단일재난통신망 핵심기술, 커버리지 확대		
출 제 빈 도	미출제		
참 고 자 료	- 국내 공공망에서의 네트워크 공유방안 - TTA 저널-통합공공망 주파수 공유 및 상호연동 요구사항(https://www.tta.or.kr/data/androReport/ttaJnal/181-2-2.pdf) - How MOCN RAN-Sharing Works(https://blog.3g4g.co.uk/search/label/MOCN)		
K e y w o r d	RAN-Sharing, Operator, Core, EPC, eNB, Gateway, MORAN, MOCN, GWCN, 700MHz, Guard Band		
풀 이	임호용 기술사(123 회 정보관리기술사)		

1. 통합 공공안전망의 핵심기술, RAN-Sharing 의 개요

가. RAN-Sharing 의 정의



정의	- 서비스 커버리지 확장의 제약을 극복하기 위해 사업자 간 무선 Access 자원을 공유하는 기술

- 각기 다른 LTE 망 사용으로 인한 인프라와 서비스의 연계, 공유, 확장의 필요성 증가

나. RAN-Sharing 의 필요성

구 분	필요성	설 명
서비스 측면	서비스 연계	- 인프라-서비스 간 효율적인 이용을 위한 연계 필요
	서비스 확장	- 공공 통신망에서 ICBAM 기반 서비스로 확장 필요
인프라 측면	인프라 연계	- LTE-R, LTE-M, PS-LTE 장애 대비를 위한 백업 망 연계 필요
	인프라 공유	- 700MHz 주파수의 효율적인 사용과 주파수 간섭 감소를 위한 통신망 인프라 공유 필요

- 다양한 측면의 RAN-Sharing 필요성을 통한 RAN-Sharing 목적 도출

2. RAN-Sharing 의 목적 설명

가. 서비스 측면의 목적 설명

구 분	목적	설 명
연계	서비스 효율적 사용	- LTE-R, LTE-M, PS-LTE 등 기반의 간섭 없는 응용 서비스의 효율적 사용
	인프라 연계	- OpenRAN, SDN 등 서비스-인프라의 융/복합을 통한 상호 연계
	백업서비스 연계	- 인프라 백업망 서비스 연계로 재난 발생 시 상용망 전환 정책 등 관리
확장	타 서비스 확장	- 확장 플랫폼 통한 IPv6 전환으로 ICBAM 기반 서비스 확장
	운영/관제 확장	- 통합 공공안전망 운영센터의 인프라 관리/관제 서비스로 확장
	공공망 통합	- 전국 단일재난안전통신망의 핵심기술, 통합운영 서비스로 일괄 관리

- 다양한 재난안전 응용서비스 제공을 위해서는 인프라 측면의 목적과 부합해야 함

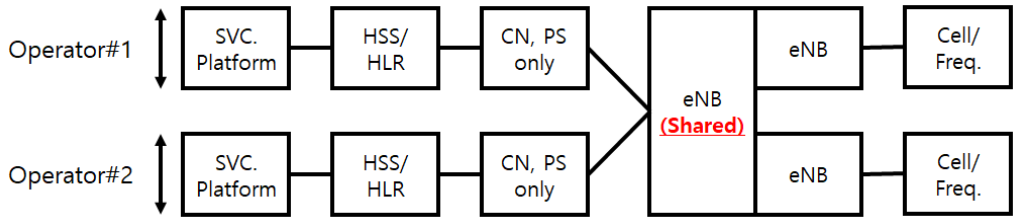
나. 인프라 측면의 목적 설명

구 분	목적	설 명
연계	서비스 연속성	- PS-LTE/LTE-M/LTE-R 등의 망 연계를 통한 통신 서비스 지연 최소화
	주파수 간섭 최소화	- Guard Band(20MHz) 확보로 통신망 주파수 간 간섭 최소화
	백업망 연계	- 인프라 장애 대응 Fail-over 를 위한 상용망을 백업망으로 사용, 연계
공유	주파수 공유	- 700MHz 대역의 LTE 기반 인프라 주파수 공유
	공공기관 활용	- 코로나 19 백신 수송 시 군부대 등의 기관에서 연락체계 구축, 사용 등
	재난 실시간 대응	- 각종 재난 상황에서 광범위한 지역 상황을 실시간으로 공유하고 대응

- 네트워크 공유방식 유형은 Site, Mast, RAN, Core N/W Sharing 이 존재함

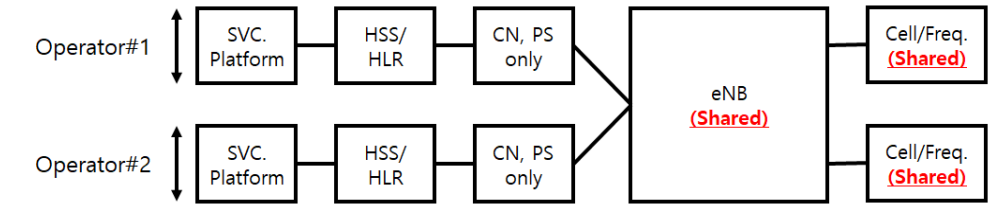
3. RAN-Sharing 의 기술방식 설명

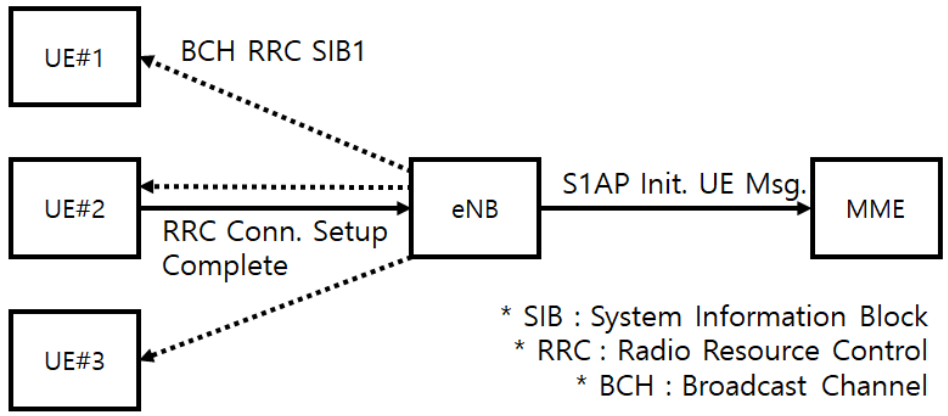
가. MORAN(Multiple Operator RAN) 설명

구분	설명	
정의	- 무선 캐리어를 제외한 RAN(안테나, 타워, 사이트, 전원)의 모든 것이 둘 이상의 사업자 간에 공유되는 RAN-Sharing 기술	
구성도		
특징	고유 주파수 사용	- Operator 들은 고유 주파수 대역을 계속 사용

- MORAN 은 3GPP Standard 에 정의되지 않은 기술방식

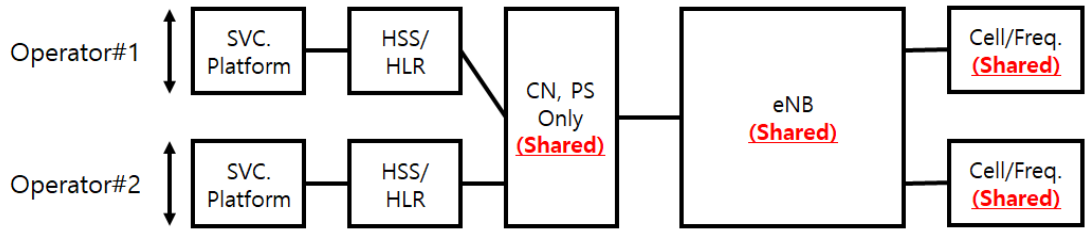
나. MOCN(Multiple Operator Core N/W) 설명

구분	설명
정의	- 둘 이상의 코어 네트워크가 동일한 RAN 과 캐리어를 공유하는 RAN-Sharing 기술
구성도	

동작 절차	

- MOCN 은 연동 인터페이스 간단, 장애처리 같은 망 운용 관점에서 유리

다. GWCN(Gateway Core N/W) 설명

구분	설명
정의	- MOCN 에 더하여 핵심 네트워크인 MME, S-GW 까지 공유하는 RAN-Sharing 기술
구성도	
특징	- MOCN 대비 추가 비용절감 가능하지만 유연성이 떨어짐

- MOCN, GWCN 은 3GPP 표준 TS 23.251 로 정의되어 있음

4. MORAN, MOCN, GWCN 의 비교 설명

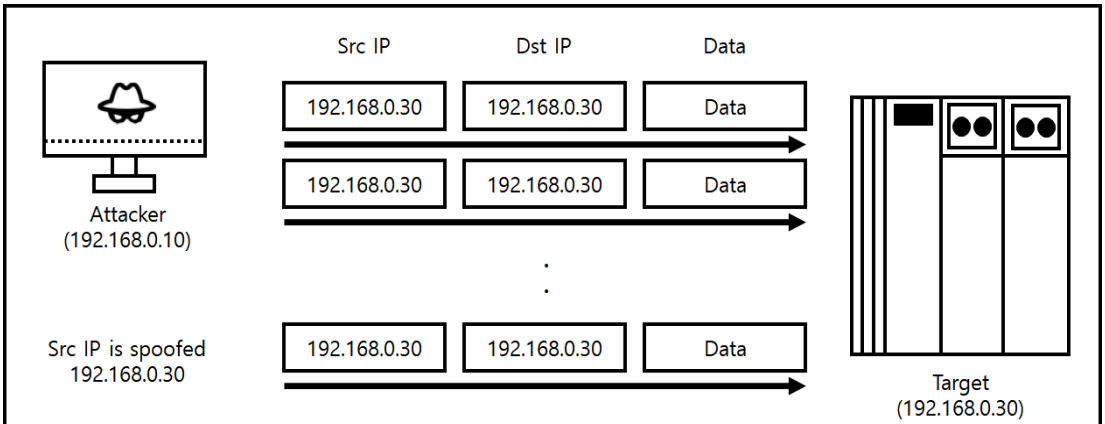
구분	MORAN	MOCN	GWCN
공유범위	Site, 안테나, RAN, 전송	MORAN + 스펙트럼	MOCN + Core N/W(일부)
캐리어	독립	공유	공유
MME 공유	독립	독립	개별

- 공공망에서 사용 시 PLMN 등록 및 변경 발생 시 즉시 설정할 수 있어야 함 **"끝"**

※ PLMN : Public Land Mobile Network

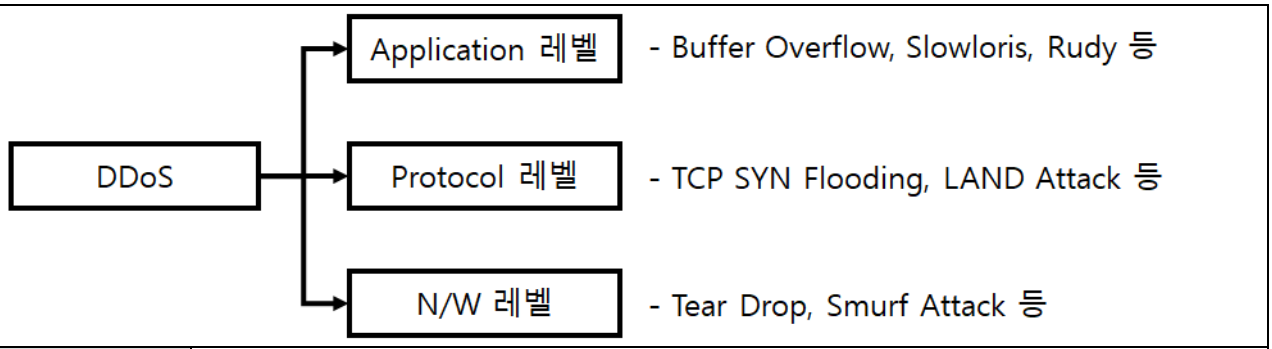
기출풀이 의견

5. RAN-Sharing 목적에 다양한 분야에서 사용되는 것과 구체적인 기술방식의 도식화가 필요하며, 각 기술방식의 풍부한 비교 작성 시 고득점을 기대할 수 있겠습니다.

문 제	6. 다음의 그림은 서비스 거부(DDoS, Distributed Denial of Service) 공격 사례이다. DDoS 에 대하여 다음 내용을 설명하시오.  [그림] 서비스 거부 공격 사례 가. 위 사례의 공격기법 개념 나. 위 사례의 공격기법 다. 공격기법에 대한 보안 대책

출 제 영 역	디지털 보안	난 이 도	★★★☆☆
출 제 배 경	- 국내 : 네이버, 금융권 등 DDoS 공격, 서비스 다운 - 국외 : Github, 유럽은행 등 지속적인 DDoS 공격, 서비스 다운		
출 제 빈 도	114 회 컴시응		
참 고 자 료	- 신기록 수립한 디도스 공격.... (https://www.boannews.com/media/view.asp?idx=89014)		
K e y w o r d	IP Spoofing, 타겟 주소 변조, Land Attack, Source IP, Destination IP, 루프 응답, 세션 생성, DDoS		
풀 이	임호용 기술사(123 회 정보관리기술사)		

1. 서비스 거부 공격(DDoS)의 개요

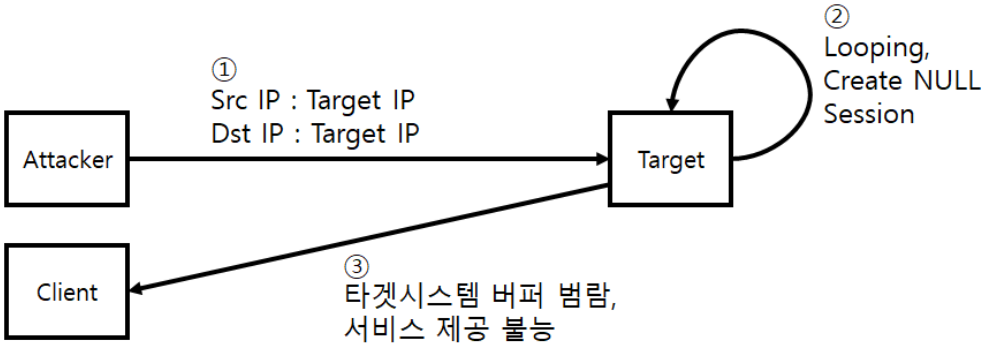


정의	- C&C 서버와 N/W 에 분산되어 있는 많은 에이전트를 점령하여 공격대상에 동시에 과도한 서비스 요청을 발생시키는 공격
특징	- 가용성 저해, 추적/대응 어려움, 사전공격 성격 강함

- 최근 다양한 트래픽(프로토콜), 고용량 트래픽, 트래픽 진원지가 불특정 다수인 DDoS 공격 증가 추세

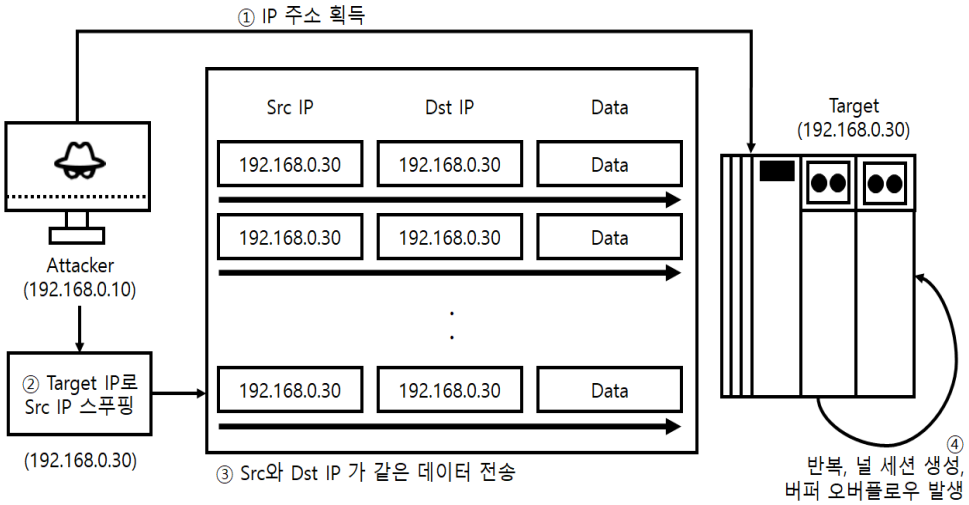
2. 위 사례의 공격기법 개념 및 공격기법 설명

가. 위 사례의 공격기법의 개념

구분	설명
개념	- 공격자가 타겟의 IP 주소를 변경한 TCP SYN 패킷을 보내 타겟 시스템이 응답을 무한반복 하면서 NULL Session 을 생성하여 서비스를 거부상태로 만드는 공격 기법
개념도	
사례의 공격기법 명칭	- **LAND(Local Area Network Denial) Attack** - **판단이유 :** 위 그림에서 Src IP is spoofed 를 보고 판단. spoofed 된 IP 주소가 타겟 IP 주소

- LAND Attack 은 IP Spoofing 을 이용한 SYN 공격

나. 위 사례의 공격기법 설명

구 분	공격단계	설 명
		
Attacker	**① IP 주소 획득**	- ping 명령어 등을 통해 타겟 IP 주소 획득
	② Src IP 스푸핑	- 획득한 IP 주소로 공격자의 IP 변조 수행
	③ Src/Dst IP 가 같은 패킷 전송	- 타겟 IP 를 Dst IP 로 하여 Src/Dst IP 가 동일한 패킷 전송 - 이 때 타겟은 Response 를 자기자신한테 수행
Target	**④ 반복, 널 세션 생성,**	- Src IP 가 타겟 IP 이므로 자기 자신한테 계속해서 반복 응답 - 혹은 새로운 연결 생성 위한 널 세션 생성
	④ 버퍼 오버플로우 발생	- 루핑, 세션이 계속 저장, 할당된 버퍼 메모리를 초과하는 현상 발생
	⑤ 서비스 마비	- 버퍼 오버플로우로 인한 시스템 마비, 서비스 제공 불가

- 다양한 Device 를 이용해 영상을 전송하고, 실시간으로 분석하여 빠른 대응이 가능

3. 공격기법에 대한 보안 대책 설명

가. 관리적 측면의 보안 대책

구분	보안대책	설명
시스템	주기적 모니터링	- 주기적인 모니터링으로 네트워크 현황 분석 수행
조직/정책	전담조직 구성	- DDoS 발생 시 대응 가능한 TFT(Task Force Team) 구성 - CERT 구축 등 정보보호 위원회, 실무협의체 등 구성
	보안계획수립	- 보안활동 계획, 정책/지침 수립, 보안성 검토, 성과관리 방법 정의
	주기적 활동	- 보안감사, 컴플라이언스 준수, 모의훈련, 침투테스트 등 DDoS 공격 대응 위한 활동 수행

- DDoS 공격 대응을 위한 조직 내/외부 가이드라인 및 체계 수립

나. 물리적 측면의 보안 대책

구분	보안대책	설명
장비	장비 교체	- 구형 장비의 경우, Land Attack 에 대응 가능한 장비로 교체
네트워크	스크러빙센터 활용	- SECaaS 형태로 구성된 스크러빙 센터를 통한 DDoS 공격 대응

- 주기적인 네트워크 트래픽 감시 필요, ISP/IDC 와 적극적인 협력 필요

다. 기술적 측면의 보안 대책

구분	보안대책	설명
인증	트러스트인증해제	- Source IP 기반 인증 방법 해제
	접근제어목록 활용	- ACL 규칙 기반 네트워크 접근 가능한 목록 관리
데이터	패킷 차단	- Source IP 와 Destination IP 가 동일한 패킷은 차단
	다른 계층 방어	- OSI 7 Layer 의 1, 2, 4, 7 계층 등 응용되는 공격에 대해서 방어대책 수립
	임계치 설정	- Packet Threshold 설정 통한 일정 패킷 수 이상 수신 시 차단 - Buffer 사이즈 조절 통한 시스템의 일시적 대응도 고려

- 초대용량(100Gbps ~ 1Tbps 이상) 공격이 들어올 시 임계치/규칙기반/인증 기능으로 방어 불가능함

4. 위 사례의 공격기법과 TCP SYN Flooding, Smurf Attack 의 비교 설명

구분	위 사례의 공격기법	TCP SYN Flooding	Smurf Attack
변조방법	IP Spoofing	없음	ICMP Direct Broadcast
프로토콜	IP(3 계층)	TCP(4 계층)	ICMP(3 계층)
공격방법	IP Spoofing 통한 타겟시스템 응답 증폭	세션 과다 통한 시스템 큐 오버플로우	ICMP direct broadcasting 통한 메시지 타겟 전송
대응방법	Src IP, Dst IP 같은 패킷 차단	Backlog Queue 크기 확장 등	ICMP Direct Broadcast 차단

- 고용량, 융복합 DDoS 공격 대응을 위해 SIEM, SOAR 등의 시스템으로 대응의 자동화 필요 **"끝"**

기출풀이 의견

6. 해당 그림에서 제시한 공격기법이 무엇인지 아는 것이 중요합니다. ICMP 기반인 Smurf Attack과 혼동이 올 수 있으므로 주의가 필요합니다.