제127회 정보관리기술사 해설집

2022.04.16

국가기술자격 기술사 시험문제

기술사 제 127 회 제 3 교시(시험시간: 100 분)

분야	정보통신	자격종목	정보관리기술사	수검번호		성명	

※ 다음 문제 중 4 문제를 선택하여 설명 하십시오. (각 25 점)

1. 정보전략계획(Information Strategy Planning)에 대하여 아래의 사항을 설명하시오.

 가. 단계별 활동 및 산출물

 나. ISMP(Information System Master Plan)와 비교

2. 리팩토링(Refactoring)에 대한 아래의 사항을 설명하시오.

 가. 정의, 목적, 리팩토링 순서, 리팩토링 주요기법

 나. 코드스멜(Code Smell)의 정의와 특징

 다. 코드스멜의 종류를 3 개이상 기술하고 각각의 리팩토링 방법

3. A 기업에서는 비지니스 수행과정에서 수집된 많은 양의 빅데이터(Bigdata)를 통합 관리하고자 한다. 데이터 관리에 대한 아래의 사항을 설명하시오.

 가. 데이터 거버넌스(Data Governance)의 개념 및 주요 기능

 나. 마스터 데이터(Master Data)의 개념과 필요성

 다. 마스터 데이터 관리(Master Data Management)의 구성요소와 구축 시 고려사항

4. 데이터베이스 옵티마이저(Optimizer)에 대한 아래의 사항을 설명하시오.

가. 옵티마이저의 개념

나. RBO(Rule Based Optimizer)와 CBO(Cost Based Optimizer) 비교

다. 옵티마이저의 적용 시 고려사항

5. 소프트웨어 정의 네트워크(SDN)에 대한 아래의 사항을 설명하시오.

가. SDN 제어 평면의 개요 및 구조의 특징

나. 오픈플로우(OpenFlow) 프로토콜

6. SOAR(Security Orchestration, Automation and Response)의 개념 및 등장 배경, 구성 요소, 주요 기능, 기대효과, 도입시 고려사항에 대하여 설명하시오.

01	ISP(Information Strategy Planning)		
문제	정보전략계획(Information Strategy Planning)에 대하여 아래의 사항을 설명하시오. 가. 단계별 활동 및 산출물 나. ISMP(Information System Master Plan)와 비교		
도메인	경영전략	난이도	하 (상/중/하)
키워드	환경분석, 현황분석, 정보화 비전 및 전략수립, 목표모델 설계, 통합 이행 계획		
출제배경	123회, 125회 연속 출제에 따른 내용 확인		
참고문헌	ITPE 123회, 125회 기출풀이		
해설자	안응원 기술사(제119회 정보관리기술사 / tino1999@naver.com)		

I. 정보전략계획(Information Strategy Planning)의 개요

구분	설명
개념	- 정보시스템 구축의 출발점인 계획 단계로 조직의 정보시스템 구축에 대한 전반적인 상황의 인식과 지향해야 할 목표를 조명하는 작업
규정사항	- ISP 수립 절차 및 준수사항 등
적용대상	- 정보시스템 구축·재구축 사업을 추진하기 위해 수립하는 각 중앙관서의 모든 ISP - 정보화 외에 일반재정, R&D 등 모든 분야 내역 정보화 ISP 해당
결과 활용	- ISP 최종산출물에 대한 사업 타당성, 실현 가능성, 규모 적정성을 검토하여 해당 결과를 신규 정보시스템 구축사업의 예산안 편성시 활용

II. ISP의 단계별 활동 및 산출물

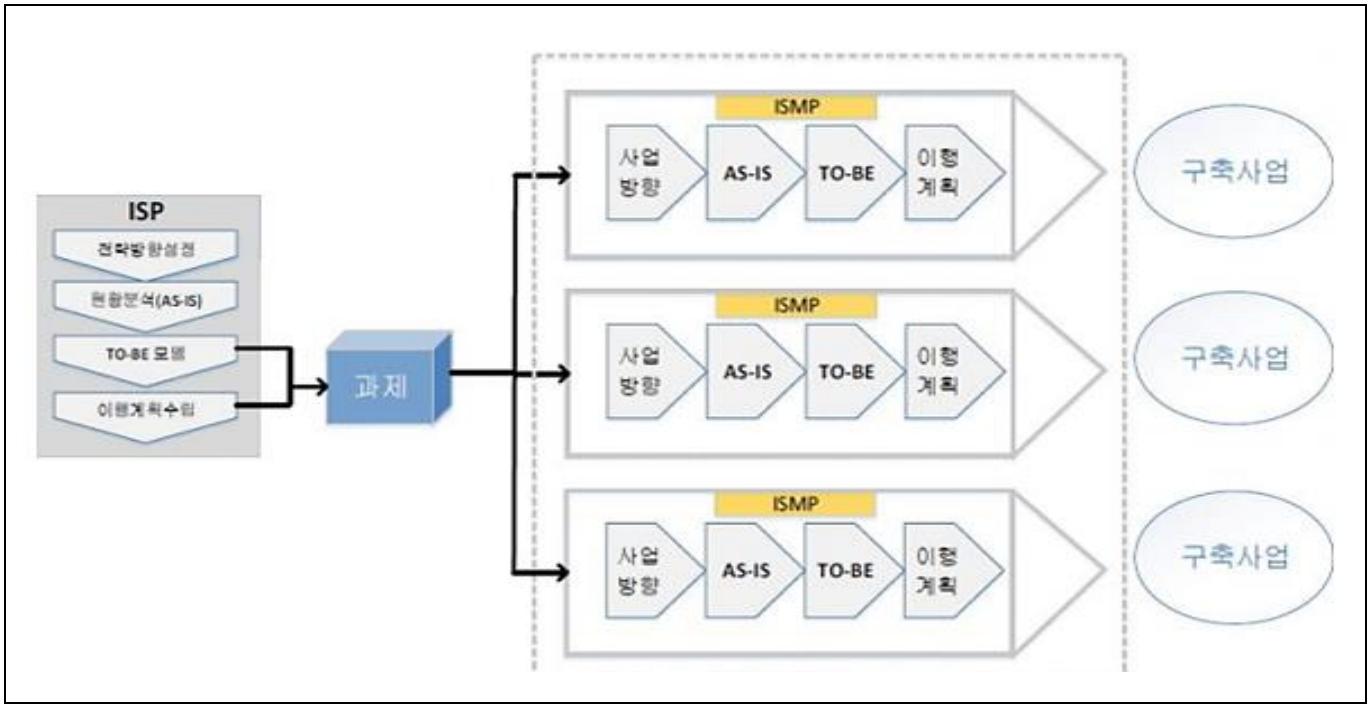
대상업무		세부내용	산출물
단계	활동		
환경분석	경영환경분석	- 외부환경 요인과 경영전략 분석을 통해 변화를 유발하는 요인에 대응하기 위한 시사점 도출	경영환경 분석서
	법령·제도분석	- 관련 법·제도 분석을 통해 사업에 영향을 미칠 수 있는 요구사항을 도출하여 목표모델 설계 시 반영	법·제도 분석서
	정보기술(IT) 환경분석	- 최신 정보기술 추세와 기술환경 변화를 검토하여 최신 정보기술의 적용가능성 및 적용 사례 분석	정보기술 동향 분석서
현황분석 (As-Is 분석)	업무현황 분석	- 조직의 역할 및 업무체계를 분석한 후, 업무절차맵(Process Modeling), 업무기능(Activity) 정의서 등을 작성하여 현행 조직과 업무체계상의 문제점 및 개선 요구사항을 도출	업무현황 분석서 (인터뷰 결과 포함)
	정보기술(IT) 현황 분석	- 업무시스템 분석, 데이터 분석, 인프라 분석, IT거버넌스 분석	정보기술 업무현황 분석서
	벤치마킹	- 현황분석(업무&정보기술)을 통해 도출된 문제점 및 개	선진사례 동향

		선요구사항을 바탕으로 벤치마킹 대상(항목)을 선정한 후, 선진사례 조사·분석을 진행	파악서
	차이(Gap) 분석	- 선진사례의 업무절차 및 정보기술 요건을 도출한 후, 기도출된 정보화 요건과의 차이를 분석하여 과제의 보완작업 및 개선방향을 설정	차이 분석서
	이슈통합 및 개선과제 도출	- 현황분석을 통해 도출된 이슈(문제점 및 개선요구사항)를 종합하여 연관성이 높은 이슈사항들을 그룹화 - 그룹화한 이슈에 대해 근본원인을 분석한 후, 개선과제를 도출(선진사례 조사·분석을 통해 도출된 시사점 적용)	요구사항 및 개선과제 분석서
정보화 비전 및 전략 수립		- 환경분석과 현황분석 결과를 연계하여 정보화 비전, 목표, 단계별 실행 전략 등을 수립하고 정보시스템 구축 원칙과 정보시스템에 적용할 기술 요건 및 정보관리 전략을 수립	정보화 전략 정의서
목표모델 설계 (To-Be 분석)	To-Be 개선과제 상세화	- 현황분석에서 도출된 개선과제들의 상세화 작업 수행 (과제 개요, 추진 범위, To-Be 개선방향, 적용사례 등)	To-Be 과제 상세 정의서
	To-Be 업무프로세스 설계	- 개선과제 내역, 선진사례, IT 개선방향을 종합적으로 고려하여 최적화된 To-Be 업무프로세스 재설계 - To-Be 업무프로세스 내 IT 지원 업무기능(Activity) 단위의 시스템 개발을 위한 기능(Function)요건 상세 정의	To-Be 업무프로세스 설계서
	To-Be 정보시스템 구조 설계	- 전략적 정보시스템 구축을 위한 이상적인 응용서비스(Application) 구조를 정립	To-Be 정보시스템 구조 설계서
	To-Be 데이터 구조 설계	- 정립된 정보시스템을 효율적으로 운용할 수 있는 정보자원(데이터) 관리 체계를 정리	To-Be 데이터 구조 설계서
	To-Be 기술 및 보안 구조 설계	- 전략적 정보시스템 구축을 위한 필요 기술 요소 및 기반(인프라) 구조를 정립	To-Be 기술 및 보안 구조 설계서
통합 이행계획	통합 이행계획 수립	- 과제별 우선순위 평가 및 전략적 특성, 시스템 간 연관성을 바탕으로 개선(이행)과제 간의 선후관계를 고려하여 추진체계 및 실행일정 수립	통합 이행계획 수립서
	총사업비 산출	- SW 개발비, 장비비, 운영·유지보수비	
	효과분석	- 타당한 기대효과 분석	

- ISP 최종산출물에는 ISP 기본 구성 내용의 결과물이 포함되어야 하며, 기본 구성 내용 간의 연관성을 기술

III. ISP와 ISMP의 비교

가. ISP와 ISMP의 관계 비교



- ISMP는 조직에 적합한 정보화 사업을 도출한다는 측면에서는 ISP와 유사한 면이 있지만, 목표와 역할에서 근본적인 차이점 존재

나. ISP와 ISMP의 상세 비교

구분	ISMP	ISP
목적	- 특정 정보시스템 기능적·기술적·비기능적 요구사항 상세화	- 경영전략과 정보화 전략 연계 및 새로운 정보기술 반영
범위	- 단위 프로젝트 또는 단위 프로젝트의 묶음	- 전사, 서비스 또는 부서대상정보화 전략
설계 대상	- SW 사업 범위 내 업무 및 정보시스템 현황 파악	- 조직 경영 목표 전략 기준 분석
상세화 수준	- 기능점수 도출 가능 레벨까지 상세화 - 객관적 지표로 측정 가능하도록 요구사항 기술 또는 검증 요건 기술	- 이행과제의 구축 대상 및 적용 기술을 제안요청서에 정의
주요활동	- 정보시스템 구축 범위 및 방향 수립 - 정보시스템에 대한 기능적/기술적(데이터 및 트랜잭션 기능, 성능, 테스트 등) 요건 도출 - 정보시스템 구조 및 요건 상세 기술 - 정보시스템 구축 계획 수립 - 정보시스템 예산 산정 및 업체 선정·평가 지원	- 경영환경 분석 - 최근 정보기술 동향분석 - 업무 분석(조직 내부 활동과 현행 프로세스 분석) - 정보 시스템 구조 분석 정보전략 및 정보관리체계 수립 - 미래업무 프로세스 및 정보시스템 구조 설계 - TO-BE 로드맵 수립

주요 산출물	- RFP(제안요청서) - 정보시스템 예산	- 경영환경분석 및 정보기술동향 분석 보고서 - 업무/정보시스템 분석 보고서 - IT 비전 및 전략 - 이행 과제 및 로드맵

"끝"

02	리펙토링(Refactoring)		
문제	리팩토링(Refactoring)에 대한 아래의 사항을 설명하시오. 가. 정의, 목적, 리팩토링 순서, 리팩토링 주요기법 나. 코드스멜(Code Smell)의 정의와 특징 다. 코드스멜의 종류를 3개이상 기술하고 각각의 리팩토링 방법		
도메인	소프트웨어 공학	난이도	중(상/중/하)
키워드	Extract Method, Pull Up Method, 중복된 코드 등		
출제배경	소프트웨어 개발시 품질 향상을 위한 기본개념 확인		
참고문헌	ITPE 서브노트		
해설자	안응원 기술사(제119회 정보관리기술사 / tino1999@naver.com)		

I. 리팩토링의 정의 및 목적

가. 리팩토링의 정의

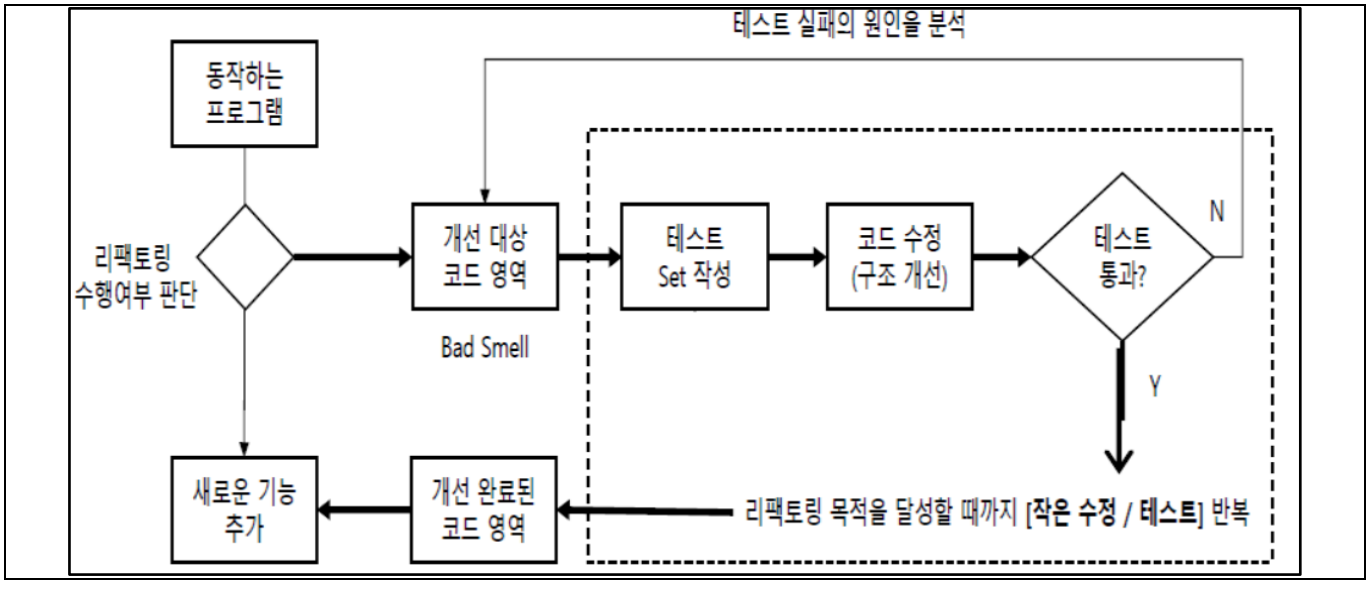
- 소프트웨어 모듈의 외부적 기능은 수정하지 않고 내부적인 구조, 관계등을 단순화하여 소프트웨어의 유지보수성을 향상시키는 기법

나. 리팩토링의 목적

소프트웨어 디자인 개선	- 설계 의도와 구현 코드의 일관성을 유지하여 설계 변경 용이
소프트웨어 이해도 향상	- 이해하기 쉬운 코드는 개발자의 작업시간 단축
오류발견 용이성 확보	- 소스 구조를 명확히 함으로써 버그 원인 쉽게 발견
전체 개발 생산성 유지	- "좋은 디자인 유지 -> 개발자 이해 향상 -> 오류감소" 개발 가속화

II. 리팩토링 순서, 리팩토링 주요기법

가. 리팩토링 순서



나. 리팩토링 주요기법

구분	설명
Extract Method	- 그룹으로 함께 묶을 수 있는 코드 조각이 있으면, 코드의 목적이 잘 드러나도록 메소드의 이름을 지어 별도의 메소드를 추출
Replace Temp With Query	- 어떤 수식의 결과값을 저장하기 위해서 임시변수를 사용하고 있다면, 수식을 추출해서 메소드로 만들고, 인시변수를 참조하는 곳을 찾아 모두 메소드 호출로 교체
Move Method	- 메소드가 자신이 정의된 클래스보다 다른 클래스의 기능을 더 많이 사용하고 있다면, 이 메소드를 가장 많이 사용하고 잇는 클래스에 비슷한 몸체를 가진 새로운 메소드 생성
Extract Class	- 두 개의 클래스가 해야 할 일을 하나의 클래스가 하고 있는 경우 새로운 클래스를 만들어 관련 있는 필드와 메소드를 예전 클래스에서 새로운 클래스로 이동
Rename Method	- 메소드의 이름이 그 목적을 드러내지 못하고 있다면 메소드의 이름 변경
Pull Up Field	- 두 서브 클래스가 동일한 필드를 가지고 있다면, 해당 필드를 슈퍼 클래스로 이동
Pull Up Method	- 동일한 기능을 하는 메소드를 여러 서브클래스에서 가지고 있다면 이 슈퍼클래스로 이동
Encapsulation Field	- Public 필드가 있는 경우, 그 필드를 Private으로 하고 접근자 제공
Inline Temp	- 간단한 수식의 결과값을 가지는 임시변수가 있고, 그 임시변수가 다른 리팩토링을 하는데 방해가 된다면, 이 임시변수를 참조하는 부분을 모두 원래의 수식으로 변경
Introduce Explaing Variable	- 복잡한 수식이 있는 경우에는, 수식의 결과나 또는 수식의 일부에 자신의 목적을 잘 설명하는 이름으로 된 임시변수를 사용
Split Temporary Variable	- 루프안에 있는 변수나 collecting temporary variable도 아닌 임시변수에 값을 여러 번 대입하는 경우에는, 각각의 대입에 대해서 따로따로 임시변수를 작성
Remove Assignments to Parameters	- 파라미터에 값을 대입하는 코드가 있으면, 대신 임시변수를 사용하도록 하라
Substitute Algorithm	- 알고리즘을 보다 명확한 것으로 바꾸고 싶을 때는 메소드의 몸체를 새로운 알고리즘으로 변경
Replace Magic Number with Symbolic Constant	- 특별한 의미를 가지는 숫자 리터럴이 있으면, 상수를 만들고, 의미를 잘 나타내도록 이름을 지은 다음, 숫자를 상수로 변경
Decompose Conditional	- 복잡한 조건문(if-then-else)이 있는 경우, 조건, then 부분, 그리고 else부분에서 메소드를 추출
Consolidate Duplicate Conditional Fragments	- 동일한 코드 조각이 조건문의 모든 분기 안에 있는 경우, 동일한 코드를 조건문 밖으로 이동
Remove Control Flag	- 일련의 boolean식에서 컨트롤 플래그 역할을 하는 변수가 있는 경우, break 또는 return을 대신 사용

Replace Nested Conditional with Guard Clauses	- 메소드가 정상적인 실행경로를 불명확하게 하는 조건 동작을 가지고 있는 경우, 모든 특별한 경우에 대해서 보호절(guard clause)을 사용
Add Parameter	- 어떤 메소드가 그 메소드를 호출하는 부분으로부터 더 많은 정보를 필요로 한다면, 이 정보를 넘길 수 있는 파라미터를 추가
Remove Parameter	- 파라미터가 메소드 몸체에서 더 이상 사용되지 않는다면, 그 파라미터를 제거하라
Parameterize Method	- 몇몇 메소드가 메소드 몸체에 다른 값을 포함하고 있는 것을 제외하고는 비슷한 일을 하고 있다면, 다른 값을 파라미터로 넘겨 받는 하나의 메소드를 작성
Replace Parameter with Explicit Methods	- 파라미터의 값에 따라서 다른 코드를 실행하는 메소드가 있다면, 각각의 파라미터 값에 대한 별도의 메소드를 작성
Replace Parameter with Methods	- 메소드를 호출한 다음, 결과를 다른 메소드에 대한 파라미터로 넘기고 있다. 수신자(파라미터를 넘겨 받는 메소드) 또한 이 메소드를 호출할 수 있다면, 그 파라미터를 제거하고 수신자가 그 메소드를 호출

- 리팩토링을 통해 코드스멜을 줄이며 클린코드 생성

III. 코드스멜(Code Smell)의 정의와 특징, 코드스멜의 종류별 리팩토링 방법

가. 코드스멜(Code Smell)의 정의와 특징

구분	설명
정의	프로그램 내에서 이해하기 어렵고 수정이 힘들며 확장이 어려운 코드를 의미하며, 프로그래머의 육감으로 찾아 리팩토링이 필요한 코드
특징	- Code Smell은 객관적이지 않으며 개발 환경에 따라 틀릴 수 있음 - 팀이나 회사에서 중요하게 생각하는 가치에 따라 틀릴 수 있음 - 어떤 언어를 사용하느냐에 따라 틀릴 수 있음

나. 코드스멜의 종류별 리팩토링 방법(3개이상)

코드스멜	설명	리팩토링 방법
중복된 코드	- 기능이나 데이터 중복	- 중복제거
긴 메소드	- 메소드 내부가 너무 긴 경우	- 메소드를 적정 크기로 나눔
큰 클래스	- 한 클래스에 너무 많은 속성과 메소드 존재	- 클래스 몸집 줄임
긴 파라미터 리스트	- 메소드 파라미터가 너무 많음	- 파라미터 개수 줄임
두 가지 이유로 수정되는 클래스	- 한 클래스의 메소드가 두 가지 이상의 이유로 수정이 되면 그 클래스는 한가지 종류의 책임만을 수행하지 않게 됨(SRP위반)	- 한 가지 이유만으로 수정되도록 변경

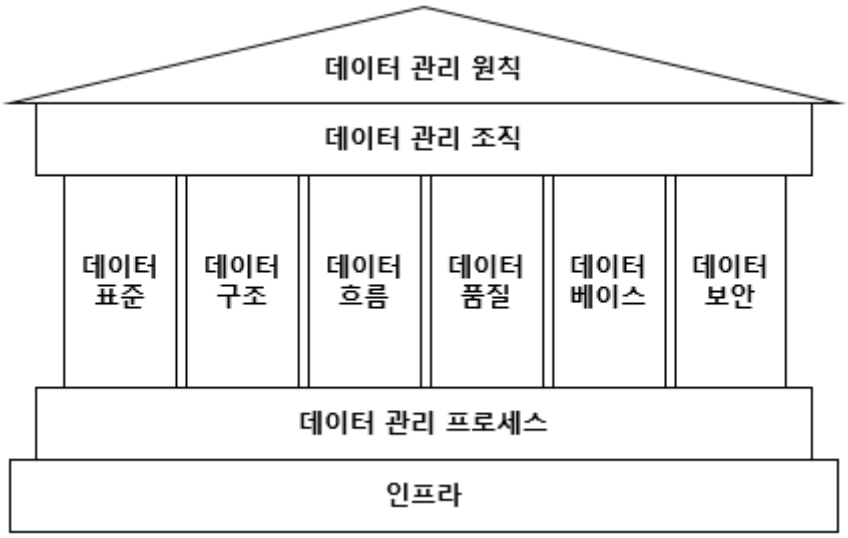
여러 클래스 동시수정 (Shotgun Surgery)	- 특정 클래스를 수정하면 그때마다 관련된 여러 클래스에서 자잘한 변경을 해야 함	- 여러 클래스에 흩어진 유사 기능을 한 곳으로 모음
다른 클래스를 지나치게 애용 (Feature Envy)	- 빈번히 다른 클래스로부터 데이터를 얻어와서 기능 수행	- 메소드를 데이터가 빈번히 쓰이는 클래스로 이동
유사 데이터들의 그룹 중복 (Data Clumps)	- 3개 이상의 데이터 항목이 여러 곳에 중복되어 나타남	- 해당 데이터를 독립 클래스로 정의
기본 데이터 타입 선호 (Prime Obsession)	- 객체 형태의 그룹을 만들지 않고, 기본 데이터 타입만 사용	- 같은 작업을 수행하는 기본 데이터의 그룹을 별도 클래스로 만듦
주석(Comments)	- 프로그램 코드가 단순성과 간결성을 담보로 하고 있다면, 주석이 불필요	- 간결한 주석으로 대체

끝"

03	데이터 관리		
문제	A기업에서는 비지니스 수행과정에서 수집된 많은 양의 빅데이터(Bigdata)를 통합 관리하고자 한다. 데이터 관리에 대한 아래의 사항을 설명하시오. 가. 데이터 거버넌스(Data Governance)의 개념 및 주요 기능 나. 마스터 데이터(Master Data)의 개념과 필요성 다. 마스터 데이터 관리(Master Data Management)의 구성요소와 구축 시 고려사항		
도메인	데이터베이스	난이도	중 (상/중/하)
키워드	MDM, DQM, MRM, 데이터 주기 관리		
출제배경	최근 기업 데이터 증가에 따른 MDM 구축 필요성 증대로 인한 데이터 관리 이해		
참고문헌	https://newsroom.koscom.co.kr/17346 ITPE Final Round		
해설자	정상반 이상헌 기술사(제 118회 정보관리기술사 / bluesanta97@naver.com)		

I. 기업 데이터 관리 지침, 데이터 거버넌스(Data Governance)의 개념 및 주요 기능

가. 데이터 거버넌스(Data Governance)의 개념



개념	- 전사 차원의 모든 데이터에 대한 정책, 지침, 표준화, 전략을 수립하고 데이터를 관리하는 조직과 프로세스를 구축함으로써 고품질의 데이터를 활용하여 기업의 가치 창출을 지원하는 체계

나. 데이터 거버넌스의 주요 기능

데이터 품질 관리 (DQM)	- 데이터 프로파일링 및 데이터 정제와 같은 작업을 포함하여 데이터 사용방법에 따라 실행
메타 데이터 관리	- 데이터 검색 중 데이터를 찾고, 분석 도구가 빅데이터를 정확하게 해석하고 사용할 수 있도록 실행.
데이터 주기 관리	- 데이터 생성 및 초기 저장에서부터 데이터가 폐기될 때까지 시스템의 데이터 흐름을 관리하는 정책 수립 필요

데이터 보안 및 프라이버시	- 데이터 요구 사항 및 정책은 사용자 역할을 기반으로 필요한 데이터 보호 수준을 정의

- 기업이 데이터 거버넌스를 구현하기 위해서는 데이터의 기반이 되는 마스터 데이터 선정이 중요함

II. 마스터 데이터(Master Data)의 개념과 필요성

가. 마스터 데이터(Master Data)의 개념

구분	설명	
정의	- 기업의 모든 비즈니스 활동 및 경영진의 비즈니스 의사결정에 근간이 되는 데이터 관련 시스템들의 기준이 정의된 데이터	
구성요소	마스터 기준정보	- 전사 업무에 동일한 기준으로 사용되는 핵심 업무 데이터
	컨트롤 기준정보	- 데이터의 입력/집계/분석 시 편의를 위해 설계된 코드
	운영 기준정보	- 업무 프로세스 실행 결과 또는 산출식에 의해 생성, 변경, 폐기되는 데이터로 참조되거나 입력 값으로 활용
선정 기준	관리범위 대상 여부	- 마스터 관리 범위 내에 포함되는 지 여부
	활용도	- 전사적으로 활용하는 정보인지 여부
	중요도	- 업무적, 전략적 중요 정보인지 여부
	데이터 정확도 보장	- 업무에서 활용 가치가 있는 정보로 제공 가능 여부
	지속 관리 여부	- 장기적으로 유지관리 가능한 속성인지 여부

나. 마스터 데이터의 필요성

필요성	설명
- 기준 정보 통합	- 기준 정보 간 존재하는 업무 규칙을 관계 연결을 통해 통합 구조 표현
- 정보 연관성 확인	- 기준 정보 간의 관계 분석을 통한 중복 제거 및 효율적 기준 정보 정제
- 업무 공유성 확장	- 다양한 업무 관점의 기준 정보 확인을 통한 업무간 기준 정보의 활용도 확장
- 데이터 양 증가	- 기업에서 수집하는 정보의 양이 증가함

- 마스터 데이터 중요도가 점점 증가함에 따라 마스터 데이터를 관리하는 MDM이 요구되어 짐

III. 마스터 데이터 관리(Master Data Management)의 구성요소

가. 마스터 데이터 관리의 정의 및 필요성

구분	설명	
정의	- 비즈니스 트랜잭션의 표준 데이터 정보인 Master Data를 분산된 시스템 들로부터 통합 및 공유하여 하나의 뷰를 제공하는 관리 기법	
필요성	효율적 관리	- 표준 프로세스 및 분류체계 부재, 정보의 품질 유지 필요
	무결성 확보	- 정보 변경절차의 표준 절차 부재로 데이터 신뢰성 저하 방지
	관리기준 제시	- 동일 정보에 대한 각 이해 관계자의 정보해석 관점 차이 극복

나. 마스터 데이터 관리의 구성요소

구분	항목	설명
기술	- EAI	- 다수의 이기종 시스템 어플리케이션 통합을 위한 및 연동 솔루션
	- Repository	- 트랜잭션/마스터/메타/스테이징 등의 데이터 저장을 위한 저장소
	- ETL	- Source DB로부터 데이터를 추출, 변환, 적재하기 위한 기술
	- Enterprise Portal	- 기준 정보 및 데이터 관리 편의성 확보를 위한 전사 통합 포털
관리	- DQM	- 데이터 관리의 효율성 확보를 위한 데이터 품질 관리 체계
	- Dashboard	- 데이터 관리 기준, 권한 관리 규칙, 관련 KPI 공지 등으로 활용
	- MRM	- 업무 규칙, 메타 데이터 관리 규정, 저장소 관리 기준 등을 관리
	- Integration	- 기존에 분산되어 있던 기준 정보 통합을 통한 일관성 향상

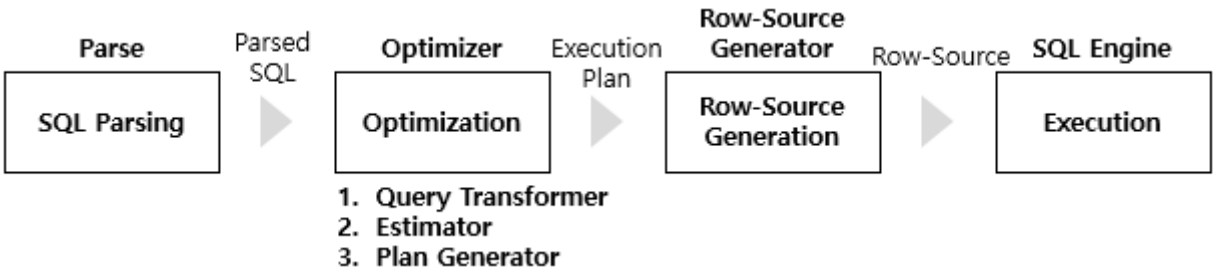
IV. 마스터 데이터 관리의 구축 시 고려사항

구분	설명
범위 확정	- 마스터 데이터 관리에 필요한 데이터 범위에 대한 명확한 정의 필요
적극적 참여	- 전사 차원에서 모든 시스템 담당자들의 적극적 참여 유발
데이터 거버넌스 고려	- 고품질, 명확한 마스터 데이터 관리를 위한 데이터 거버넌스를 고려
Top-down 방식	- C-Level 부터 인식 개선 후 하향식 방식을 통한 전사적 MDM 구축

"끝"

04	옵티마이저(Optimizer)		
문제	데이터베이스 옵티마이저(Optimizer)에 대한 아래의 사항을 설명하시오. 가. 옵티마이저의 개념 나. RBO(Rule Based Optimizer)와 CBO(Cost Based Optimizer) 비교 다. 옵티마이저의 적용 시 고려사항		
도메인	데이터베이스	난이도	중 (상/중/하)
키워드	실행계획, Rule 기반, 비용산정, Query Rewrite, Query Optimization, QEP Generation		
출제배경	DB 쿼리 처리의 기본이 되는 옵티마이저에 대한 이해 확인		
참고문헌	ITPE 서브노트		
해설자	정상반 이상헌 기술사(제 118회 정보관리기술사 / bluesanta97@naver.com)		

I. DBMS SQL 쿼리 수행 절차



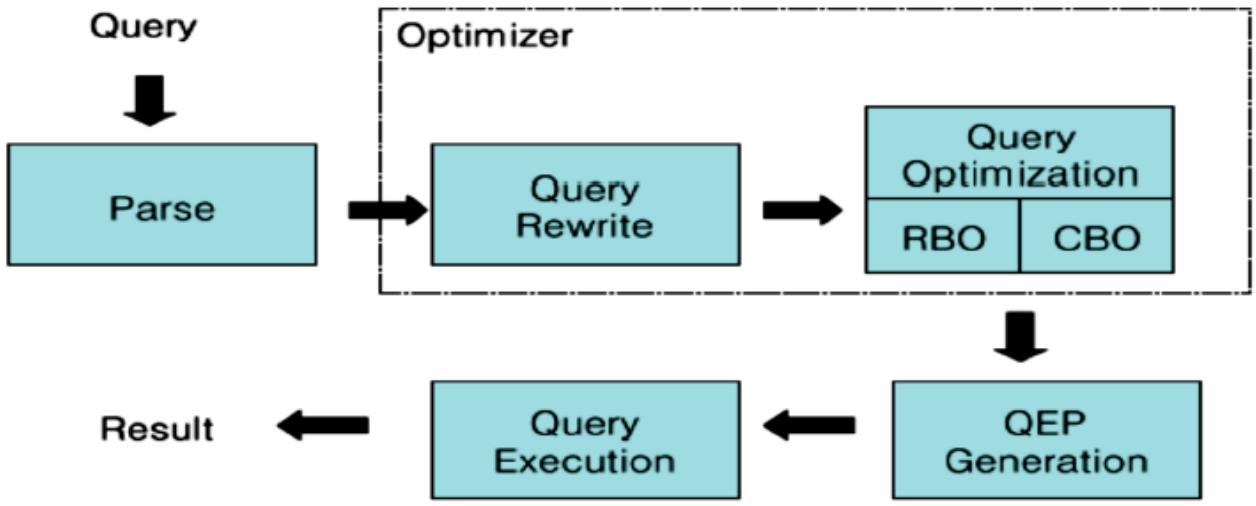
- DBMS에서 SQL 쿼리 수행 단계 중 옵티마이저는 최적의 실행계획을 도출하는 핵심 역할을 담당

II. DBMS 성능 구현의 핵심 구성요소, 옵티마이저(Optimizer)의 개념

가. 옵티마이저(Optimizer)의 정의 및 기능

구분	설명	
정의	- 사용자가 질의한 SQL문을 처리 가능한 실행계획을 탐색하고 각 실행계획에 대한 비용을 추정하여 최적의 실행계획을 수립하는 DBMS의 핵심 엔진	
핵심 기능	실행 계획 탐색	주어진 SQL 질의를 처리할 수 있는 실행 계획들을 나열(P1, .., Pn)
	비용 산정	각 실행계획의 예상비용을 계산 많은 실행계획들 중에서 최종적으로 가장 비용이 적게 드는 실행계획 Pi를 선택해서 SQL을 실행하고 결과를 사용자에게 제공.

나. 옵티마이저의 처리 절차



질의 처리 단계	핵심 기능	설명
Query Rewrite	질의 변환기	- 서브 질의와 뷰의 병합을 수행하고, OR Expansion 작업을 수행, - 서브질의와 뷰 병합: 옵티마이저가 더욱 효과적인 QEP를 찾기 위하여 더 효과적인 플랜이 있는지 그 가능성을 확인하는 과정
Query Optimization	비용 산정기	- 질의에 대한 엑세스 경로를 결정
QEP Generation	실행 계획 생성기	- 질의실행계획(QEP/Query Execution Plan) : 질의를 실행하는데 필요한 상세한 정보를 생성

- 옵티마이저는 룰 기반의 RBO와 비용기반의 CBO가 존재.

III. RBO(Rule Based Optimizer)와 CBO(Cost Based Optimizer) 비교

가. RBO(Rule Based Optimizer)와 CBO(Cost Based Optimizer) 개념 비교

구분	RBO	CBO
정의	- 인덱스구조나 비교연산자에 따른 순위부여를 기준으로 최적의 경로를 설정하는 옵티마이저	- 데이터 건수, 블록 수, 데이터 분포도 등 데이터 통계 정보를 기반으로 하여 처리에 대한 최적의 비용이 들어가는 실행 계획을 수립하는 옵티마이저
특징	- 사전에 정의된 규칙에 따라 실행 - 사후에 RBO 규칙을 변경하기 어려움	- 최적화된 결정을 위해 정기적 통계정보 갱신 필요함 - 실행계획을 미리 예측하기 힘듬

- RBO의 규칙 준수에 따른 성능 저하 발생하는 단점을 극복하고자 CBO가 등장함
- 현재 대부분의 상용 DB에서는 CBO 기반으로 운영되고 있음

나. RBO(Rule Based Optimizer)와 CBO(Cost Based Optimizer) 상세 비교

구분	RBO	CBO
경로선택	- 인덱스 구조나 비교 연산자에 따른 순서 여부를 기준으로 최적 경로 설정	- 처리 방법에 대한 비용을 산정한 후 최소 비용이 소요되는 방법 선택
인덱스	- 인덱스 존재 시 항상 사용	- Cost에 의한 결정
기준	- 실행 우선 순위(Ranking)	- 액세스 비용(Cost)
최적화 기준	- 개발자의 SQL 숙련도	- 옵티마이저의 예측 성능
동작 방식	- 15개 RULE 기반으로 처리	- 시스템 통계정보에 따른 비용 산정 후 처리
장점	- 예측 가능하여 사용자가 원하는 처리 경로 유도가 용이함	- 현실을 감안한 판단, 통계정보의 관리를 통한 최적화 제어
단점	- 통계정보라는 현실 요소 무시하여 판단의 오차가 크게 날 수 있음	- 실행 계획을 미리 예측, 제어가 어려움

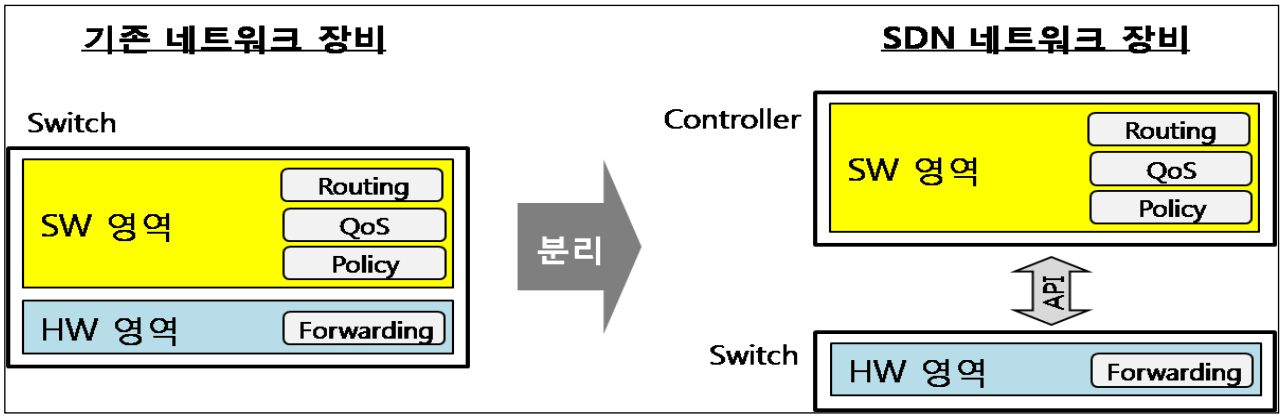
IV. 옵티마이저의 적용 시 고려사항

구분	설명
통계정보의 정확성	- 적절한 통계 정보의 생성 및 주기적인 갱신을 통한 통계정보 정확성 보정
효율적 인덱스 구성	- 데이터 카디널리티등을 관리하여 가장 효율적인 인덱스 생성
주기적 통계정보 갱신	- 주기적인 통계정보 갱신을 통한 최신 통계정보 유지
DBMS 튜닝	- 인덱스 조정 및 Table / Index 재 구성 수행

"끝"

05	SDN		
문제	소프트웨어 정의 네트워크(SDN)에 대한 아래의 사항을 설명하시오. 가. SDN 제어 평면의 개요 및 구조의 특징 나. 오픈플로우(OpenFlow) 프로토콜		
도메인	NW	난이도	상 (상/중/하)
키워드	Control Plane, Data Plane, OpenFlow, Network OS, NFV		
출제배경	5G 네트워크 기술 발전에 따른 활용도 증가로 연관 기술 지식 점검을 위한 출제		
참고문헌	ITPE 기술사회 서브노트 OpenFlow 네트워크에서의 플로우 라우팅 기술 개발 (https://scienceon.kisti.re.kr/srch/selectPORSrchReport.do?cn=TRKO201500007760)		
해설자	서경석 기술사(제119회 정보관리기술사 / akslemf@naver.com)		

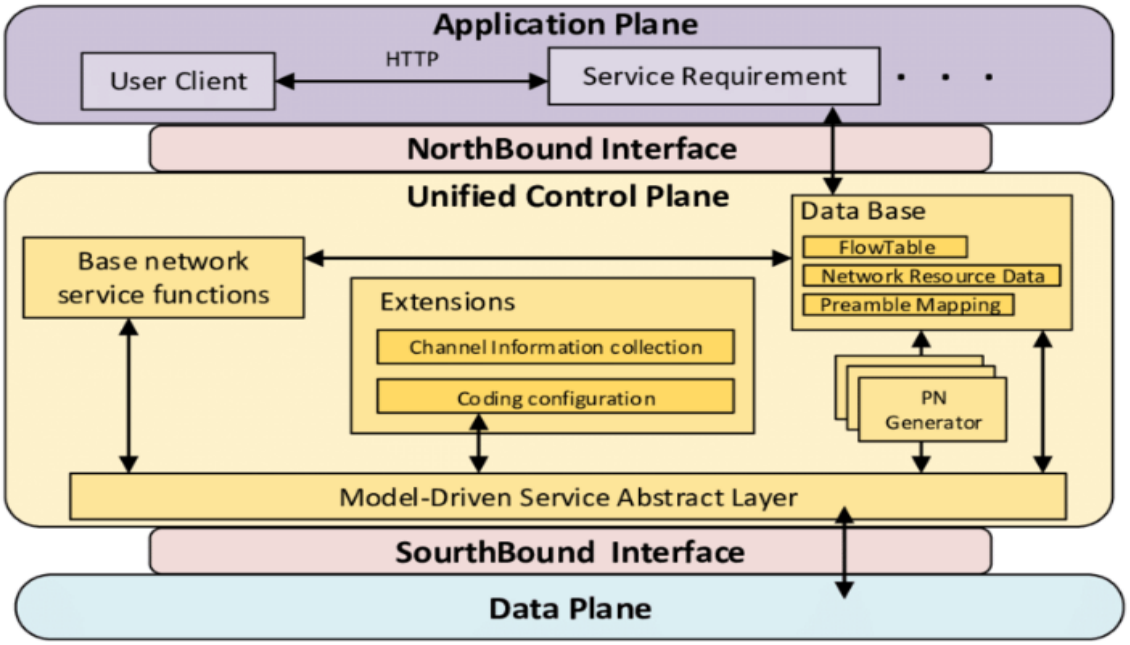
I. 네트워크의 추상화를 통한 효율적 네트워크 트래픽 관리, SDN의 개요



- 개방형 API인 OpenFlow를 통해 네트워크의 트래픽 전달 동작을 프로그래밍하듯 SW기반으로 컨트롤러에서 제어하는 네트워크 인프라

II. SDN 제어 평면의 개요 및 구조의 특징

가. SDN 제어 평면의 개요

구분	핵심 기술	설명
개념도		
개념	- 네트워크 제어기능(ACL, 라우팅 프로토콜, 인증 등)에 대한 중앙집중화 구현을 위한 계층	

- Application plane과 Data plane의 연계를 위해 제어 평면 활용

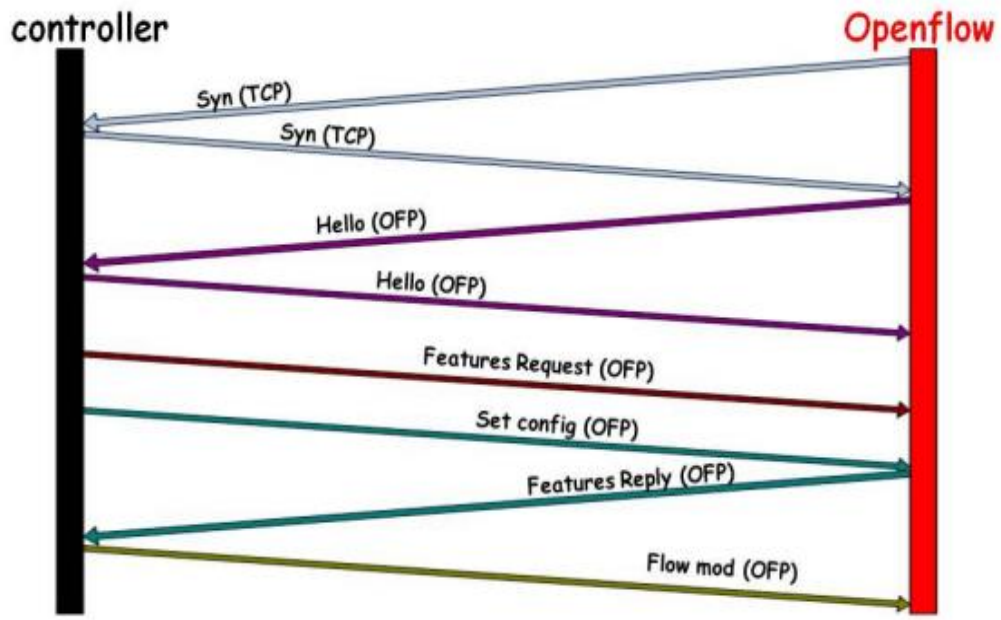
나. SDN 제어 평면 구조의 특징

구분	설명
플로우 기반 포워딩	- 오픈플로우를 통한 네트워크 포워딩 진행
데이터 평면과 제어 평면의 분리	- 데이터 평면과 제어 평면의 분리 통한 기능 단순화 및 성능 향상
제어기능 스위치 외부 존재	- 제어 평면의 네트워크 제어를 위한 스위치가 외부에 존재
프로그램 가능	- 프로그래밍 통한 제어 평면의 기능 및 추가 제어 가능
비종속성	- 제어 평면 타스크 수행 시 비종속성 보장
자가 학습	- 패킷이나 프레임 전송 이전 자가 학습 프로세스 진행
결과 반영	- 제어 평면 프로토콜 수행 결과를 RIB(Routing Information Base)와 FIB(Forwarding Information Base)에 입력
IP 테이블 관리	- IP 라우팅 테이블의 생성 및 유지 관리 담당
라우팅 테이블 업데이트 지원	- 제어 평면 패킷 전송 후 라우팅 테이블 업데이트 지원
다양한 프로토콜 지원	- STP, ARP, RIP, DHCP 등 다양한 프로토콜 지원
자체 저장	- 제어 평면 패킷은 기본적으로 라우터 내부에 로컬 저장

- SDN의 제어 평면과 데이터 평면의 통신을 위한 표준 프로토콜로 오픈플로우 프로토콜 사용

III. 오픈플로우 프로토콜의 개요 및 상세 설명

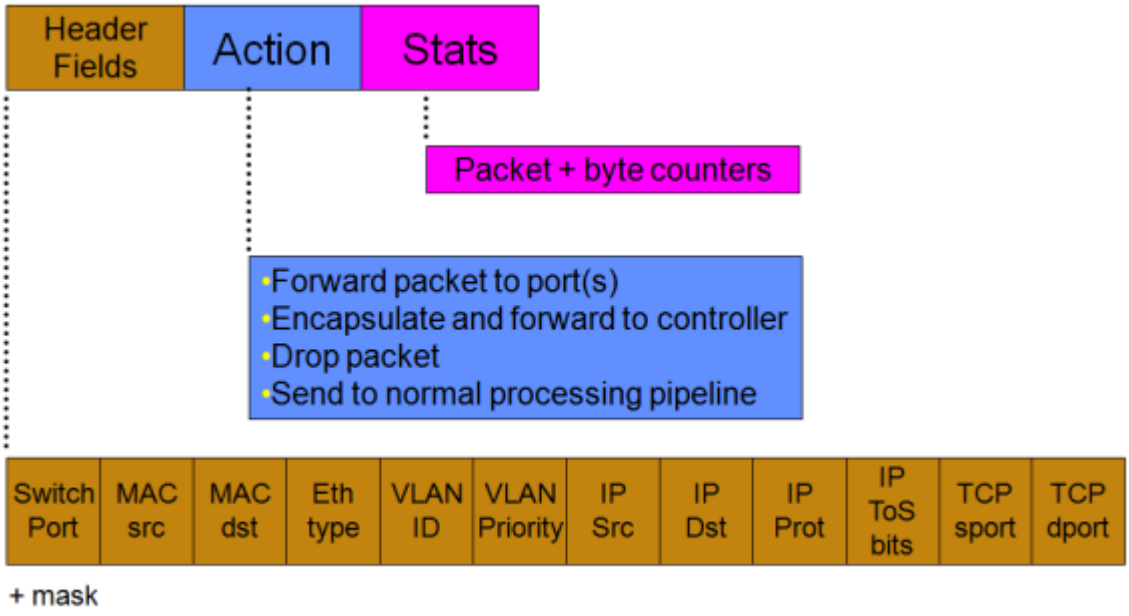
가. 오픈플로우 프로토콜의 개요

<table>
<tr><th>구분</th><th colspan="2">설명</th></tr>
<tr><td>개념</td><td colspan="2">- 스위치와 스위치를 관리하는 컨트롤러가 통신하기 위한 개방형 표준 인터페이스</td></tr>
<tr><td rowspan="5">특징</td><td>설치 용이</td><td>- 기존 PC에 리눅스 기반 OS 설치 후 오픈플로우 사용 및 테스트베드 구축 가능</td></tr>
<tr><td>범용성</td><td>- 일반 이더넷 네트워크 카드나 네트워크 전용의 FPGA 카드(NetFPGA), 혹은 OpenFlow 용 스위치에 설치 가능</td></tr>
<tr><td>독립성 유지</td><td>- 실험적 트래픽과 일반 트래픽을 독립적으로 유지</td></tr>
<tr><td>영향 최소화</td><td>- OpenFlow 프로토콜을 설치한다 하더라도 일반 트래픽 처리 방식에 영향 없음</td></tr>
<tr><td>단계적 변경</td><td>- 네트워크 장비 기능 급격한 변화 없이 적응 기간을 갖고 단계적 기능변화 가능</td></tr>
<tr><td rowspan="2">Secure Channel 연결 절차</td><td>Secure Channel 연결 개념도</td><td> 

- OpenFlow와 OpenFlow를 관리 및 제어하는 controller와의 명령어 교환</td></tr>
<tr><td>Secure Channel 연결 상세</td><td>1. TCP로 syn 패킷을 보내 상호 연결 상태 확인
2. 'Hello' 패킷 전송, 상호 버전 및 오픈플로우 프로토콜 연결 준비 확인
3. 컨트롤러에서 오픈플로우 스위치로 'Features Request' 패킷 전송, 스위치 특성 요청
(응답으로 스위치의 datapath ID, 버퍼에 저장할 수 있는 최대 패킷 수, 최대 플로우 테이블 수, 지원하는 오픈플로우 프로토콜 기능, 가능한 action,물리 포트에 대한 정의 수신)
4. Controller에서 오픈플로우 스위치로 'Set config' 패킷 전송, IP fragment에 대한 처리 및 controller에 보낼 수 있는 최대 패킷 크기 정의
5. Controller에서 오픈플로우 스위치에 초기화 명령을 담은 'Flow_mod' 패킷을 보내 모든 플로우 테이블 삭제</td></tr>
</table>

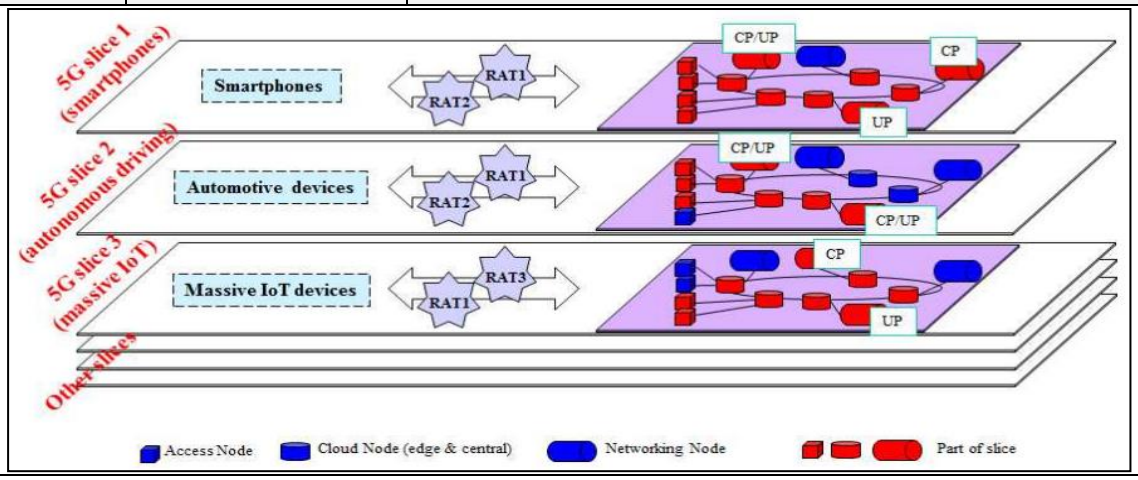
- 오픈플로우 프로토콜에 의해 스위치 내부의 플로우 테이블 작성

나. OpenFlow 프로토콜의 플로우 테이블 상세 설명

구분	설명	
개념	- 플로우 테이블 항목(필드, 카운터, 패킷 매칭 명령집합 등)과 동작을 연결하여 각 패킷 룩업과 포워딩 정보를 저장하고 있는 테이블	
구조		
세부	Switch Port	- 네트워크 카드의 포트 번호를 나타내며 패킷이 들어온 물리적 포트 번호
	MAC src/dst	- 패킷의 송수신 MAC 주소
	Eth type	- 이더넷 타입
	VLAN ID/Priority'	- Vlan ID와 우선순위, 패킷 VLAN 필드 값 있는 경우 표현, 없는 경우 무시
	IP Src/Dst	- 송수신 IP 주소
	IP Prot	- IP 프로토콜의 종류
	IP ToS bits	- IP프로토콜의 ToS(Type of Service) 필드
	TCP sport/dport	- 송수신 전송계층 포트 번호

- 오픈플로우 프로토콜은 Header, Action, Stats으로 구성되며, 오픈플로우 스위치 별 지원하는 Action과 Stats 이 다르므로 구축 시 적용 대상 스위치에 대한 충분한 검토 필요

IV. SDN과 OpenFlow를 활용한 네트워크 성능 향상 기술, 네트워크 슬라이스

<table>
<tr><th>구분</th><th colspan="2">세부</th><th>핵심 기술</th><th>설명</th></tr>
<tr><td>개념도</td><td colspan="4"> 
</td></tr>
<tr><td>개념</td><td colspan="4">- 물리적으로 하나의 네트워크를 통해 Device, Access, Transport, Core를 포함하여 End-to-End로 논리적으로 분리된 네트워크를 만들어 서로 다른 특성을 갖는 다양한 서비스들에 대해 서비스에 특화된 전용 네트워크를 제공하는 기술</td></tr>
<tr><td rowspan="5">핵심기술</td><td rowspan="3">SDN</td><td>Application</td><td>- Network OS 상에 사용자 서비스 지원 프로그램</td></tr>
<tr><td>Network OS</td><td>- 전체 망에 대한 Global view를 갖고 전체 망을 제어</td></tr>
<tr><td>Data Plane</td><td>- 단순 패킷 포워딩, 스위칭 기능만 구현</td></tr>
<tr><td rowspan="2">NFV</td><td>NFVI</td><td>- 컴퓨팅, 저장소, 네트워크 기능 지원 가상화 기능 인프라</td></tr>
<tr><td>NFVs</td><td>- 여러 응용프로그램 지원 위한 SW개발 네트워크 기능 집합</td></tr>
</table>

- 5G 네트워크 인프라 확충 및 연계 기술 발전에 따른 네트워크 슬라이싱 활성화 기대

"끝"

[참고 1] Header Field의 상세 설명

Field	Bits	When applicable	Notes
Ingress Port	(Implementation dependent)	All packets	Numerical representation of incoming port, starting at 1.
Ethernet source address	48	All packets on enabled ports	
Ethernet destination address	48	All packets on enabled ports	
Ethernet type	16	All packets on enabled ports	An OpenFlow switch is required to match the type in both standard Ethernet and 802.2 with a SNAP header and OUI of 0x000000. The special value of 0x05FF is used to match all 802.3 packets without SNAP headers.
VLAN id	12	All packets of Ethernet type 0x8100	
VLAN priority	3	All packets of Ethernet type 0x8100	VLAN PCP field
IP source address	32	All IP and ARP packets	Can be subnet masked
IP destination address	32	All IP and ARP packets	Can be subnet masked
IP protocol	8	All IP and IP over Ethernet, ARP packets	Only the lower 8 bits of the ARP opcode are used
IP ToS bits	6	All IP packets	Specify as 8-bit value and place ToS in upper 6 bits.
Transport source port / ICMP Type	16	All TCP, UDP, and ICMP packets	Only lower 8 bits used for ICMP Type
Transport destination port / ICMP Code	16	All TCP, UDP, and ICMP packets	Only lower 8 bits used for ICMP Code

[참고 2] Action의 상세 설명

Action	Associated Data	Description
Set VLAN ID	12 bits	If no VLAN is present, a new header is added with the specified VLAN ID and priority of zero. If a VLAN header already exists, the VLAN ID is replaced with the specified value.
Set VLAN priority	3 bits	If no VLAN is present, a new header is added with the specified priority and a VLAN ID of zero. If a VLAN header already exists, the priority field is replaced with the specified value.
Strip VLAN header	-	Strip VLAN header if present.
Modify Ethernet source MAC address	48 bits: Value with which to replace existing source MAC address	Replace the existing Ethernet source MAC address with the new value
Modify Ethernet destination MAC address	48 bits: Value with which to replace existing destination MAC address	Replace the existing Ethernet destination MAC address with the new value.
Modify IPv4 source address	32 bits: Value with which to replace existing IPv4 source address	Replace the existing IP source address with new value and update the IP checksum (and TCP/UDP checksum if applicable). This action is only applicable to IPv4 packets.
Modify IPv4 destination address	32 bits: Value with which to replace existing IPv4 destination address	Replace the existing IP destination address with new value and update the IP checksum (and TCP/UDP checksum if applicable). This action is only applied to IPv4 packets.
Modify IPv4 ToS bits	6 bits: Value with which to replace existing IPv4 ToS field	Replace the existing IP ToS field. This action is only applied to IPv4 packets.
Modify transport source port	16 bits: Value with which to replace existing TCP or UDP source port	Replace the existing TCP/UDP source port with new value and update the TCP/UDP checksum. This action is only applicable to TCP and UDP packets.
Modify transport destination port	16 bits: Value with which to replace existing TCP or UDP destination port	Replace the existing TCP/UDP destination port with new value and update the TCP/UDP checksum This action is only applied to TCP and UDP packets.

[참고 3] Stats의 상세 설명

- 개념 : 통계치를 나타내며 주로 전송된 패킷의 크기나 수 등
- 주로 사용되는 통계 메시지로는 'Aggregate flow statistics', 'Flow table statistics', 'Physical port statistics', 'Individual flow statistics

Counter	Bits
Per Table	
Active Entries	32
Packet Lookups	64
Packet Matches	64
Per Flow	
Received Packets	64
Received Bytes	64
Duration (seconds)	32
Duration (nanoseconds)	32
Per Port	
Received Packets	64
Transmitted Packets	64
Received Bytes	64
Transmitted Bytes	64
Receive Drops	64
Transmit Drops	64
Receive Errors	64
Transmit Errors	64
Receive Frame Alignment Errors	64
Receive Overrun Errors	64
Receive CRC Errors	64
Collisions	64
Per Queue	
Transmit Packets	64
Transmit Bytes	64
Transmit Overrun Errors	64

06	SOAR		
문제	SOAR(Security Orchestration, Automation and Response)의 개념 및 등장 배경, 구성 요소, 주요 기능, 기대효과, 도입 시 고려사항에 대하여 설명하시오		
도메인	보안	난이도	하 (상/중/하)
키워드	SOA , SIRP , TIP ,지능형 관제, 보안오케스트레이션, SOC 자동화		
출제배경	최근 보안 위협 자동 대응 및 보안 관제 프레임워크 기술 활성화에 따른 관련 지식 점검		
참고문헌	ITPE 기술사회 서브노트		
해설자	서경석 기술사(제119회 정보관리기술사 / akslemf@naver.com)		

I. SOC(Security Operation Center) 업무의 자동화, SOAR의 개요

가. SOAR(Security Orchestration, Automation and Response)의 개념

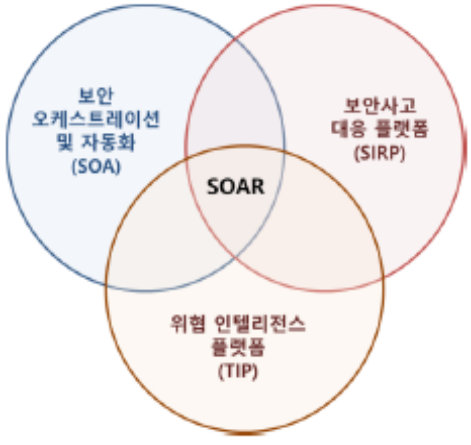
- 다양한 사이버위협에 대해 대응수준을 자동으로 분류하고 표준화된 업무 프로세스에 따라 보안업무 담당자와 솔루션이 유기적으로 협력할 수 있도록 지원하는 새로운 보안 플랫폼

나. SOAR의 등장배경

사이버 공격의 진화	- 랜섬웨어, APT 등 사이버 공격의 진화 및 고도화 - 클라우드, IoT 등 기업의 도입 IT시스템 증가로 범위 확대, 공격대상 급증
기존 보안관제 한계	- 다양한 이기종 보안장비로부터 보안데이터 수집으로 분석에 한계 - 탐지된 이벤트를 분석하고 원인과 대응책을 마련하는 데 많은 시간 소요

II. SOAR의 아키텍처와 주요 기능

가. SOAR의 아키텍처

아키텍처	설 명
	- SOA(Security Orchestration and Automation) 보안조직이 보유한 여러 개의 Workflow 관리 - SIRP(Security Incident Response Platform) SIEM에서 탐지된 위협대응을 자동화하도록 지원 - TIP(Threat Intelligence Platform) 위협 인텔리전스 중 관련 데이터를 찾아 자동분석하여 환경에 맞는 최적의 대응 솔루션 제시

- SOAR는 SOA, SIRP, TIP 3가지 플랫폼의 조합으로 구성됨

나. SOAR의 주요 기능

구 분	기 능	설 명
Orchestration	- 보안솔루션 연동 기능	- 다양한 보안솔루션의 연동, 탐지된 이벤트 자동 분석 - 하나의 화면에서 현재의 보안상황 확인 및 운영
	- 가시성 제공	- 대시보드 제공 - 특정 액션의 자동화, 사이버킬체인 적용, 대응절차 시각화
Automation	- 업무 자동화 및 집중도 향상	- 단순 반복되던 업무는 자동화하여 편의성 제공 - 보안담당자는 분석 및 공격시나리오 설계 등 가치 높은 업무에 집중하도록 환경 제공
	- 동적 플레이북 제공	- 사전 정의된 플레이북으로 일관된 프로세스로 작업을 처리하여 품질 편차 최소화
	- 작업 및 스크립트	- 워크플로우에서 스크립트 기능을 추가해 플랫폼 기능 자동화 운영
Response	- 사고대응 및 협업	- 사고대응 내역과 대응방식 등 의사결정에 대한 기록관리 - SOC 관리자 간 협업체계 지원
	- 리포팅	- 사고 대응에 대한 지표 관리로 의사결정 지원

- SOAR 도입 시 다양한 보안업무에 활용은 가능하나 환경분석 등 다양한 측면을 고려한 후 도입 필요

III. SOAR 도입 시 고려사항

고려사항	설 명
업무프로세스의 명확한 정의	- 정해진 업무프로세스에 대한 오케스트레이션 제품이므로 존재하지 않는 업무프로세스 처리 불가 - 세부적인 업무 프로세스까지 정의하여 SOAR 도입 후 적용
자동화 RISK 고려	- 모든 업무의 자동화 적용은 불가하며 최종 판단은 보안전문인력이 수행 - 연계하는 다양한 보안시스템들의 API 기능오류 등의 예상 못한 오동작을 고려하여 자동화 설계
도입 후 운영방식 충분한 사전준비	- 기업의 업무프로세스의 지속적인 변화로 SOAR 도입 후 지속적인 유지관리 필요 - 연계된 보안솔루션 제품 또는 기능 변경 시 API 수정 개발 필요

- 국내에서는 안랩이 'Sefinity AIR'라는 자체 개발 솔루션으로 가장 먼저 선보였으며, 해외는 'IBM 리질리언트', 팔로알토의 '데미스토' 솔루션을 출시함

IV. SOAR 적용 시 기대 효과 및 고려 사항

구분	세부	설명
기대 효과	전사적 관점	- 다양한 보안 기술 통합 관리 및 운영 통한 보안 스택의 ROI 향상
		- 개인 정보 침해 규제, 의무 이행 복잡성 제거 통한 정보 대응 관리 간소화
	실무 관점	- 3rd 보안 솔루션 연동 통한 위협 정보 분석, 정형화 사고 자동 대응
		- 히스토리 통합 관리를 통해 향후 유사 공격에 대한 대응력 확보 가능
	관리자 관점	- 조직 내 전체 보안 사고에 대한 과거/현재 사고 대응 현황 파악, 관리
		- 보고 시스템 일원화 통한 사고 발생 시 혼란 감소, 타 부서 협업 환경 구축
고려 사항	조직 관점	- 보안 사고 발생 시 조치 및 대응 방안에 대한 사고 대응 프로세스 정의
		- 사고 대응 프로세스 분석 통한 자동화 가능 영역 확인
	업체 선정	- 유연성 : 사고 대응 플랫폼에서 다양한 사고 유형에 대한 대응 가능성
		- 가시성 : 보안 사고 발생 시 법무팀, 임원진 공유 가능 여부
		- 통합성 : 기존 보안 IT 툴과 통합 운영 가능 여부 및 편의성 확인
		- 민감 정보 보호 : 개인 정보 보호 규정 및 침해 통보 기능 포함 여부

"끝

ITPE 기술사회
제127회 정보관리기술사 기출문제 해설집

대 상 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사, 정보시스템감리사 시험
발행일 2022년 04월 16일
집 필 강정배PE, 안응원PE, 서경석PE, 이상헌PE
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