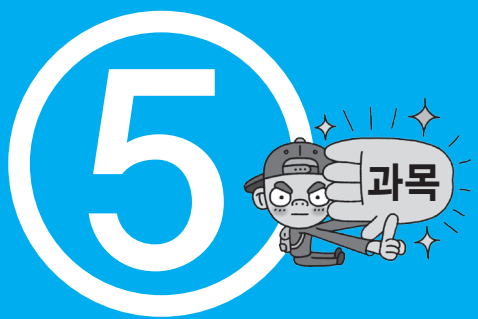


정보시스템 구축 관리

1장 / 소프트웨어 개발 방법론 활용

2장 / IT프로젝트 정보 시스템 구축 관리

3장 / 소프트웨어 개발 보안 구축

4장 / 시스템 보안 구축

베리나이쓰~
구독!

1장 소프트웨어 개발 방법론 활용

이 장에서 꼭 알아야 할 키워드 Best 10

1. 애자일 방법론 **2.** 소프트웨어 비용 결정 요소 **3.** 델파이 기법 **4.** LOC 기법 **5.** COCOMO 모형
6. 기능 점수 모형 **7.** 프로젝트 관리 **8.** CMMI **9.** SPICE **10.** 닷넷 프레임워크

SECTION
157
LIVE

소프트웨어 개발 방법론

전문가의 조언

소프트웨어 개발 방법론의 종류에는 어떤 것이 있으며, 종류별 특징과 절차를 구분할 수 있도록 정리하세요.

1 소프트웨어 개발 방법론의 개요

소프트웨어 개발 방법론은 소프트웨어 개발, 유지보수 등에 필요한 여러 가지 일들의 수행 방법과 이러한 일들을 효율적으로 수행하려는 과정에서 필요한 각종 기법 및 도구를 체계적으로 정리하여 표준화한 것이다.

- 소프트웨어 개발 방법론의 목적은 소프트웨어의 생산성과 품질 향상이다.
- 소프트웨어 개발 방법론의 종류에는 구조적 방법론, 정보공학 방법론, 객체지향 방법론, 컴포넌트 기반(CBD) 방법론, 애자일(Agile) 방법론, 제품 계열 방법론 등이 있다.

2 구조적 방법론

구조적 방법론은 정형화된 분석 절차에 따라 사용자 요구사항을 파악하여 문서화하는 처리(Precess) 중심의 방법론이다.

- 쉬운 이해 및 검증이 가능한 프로그램 코드를 생성하는 것이 목적이다.
- 복잡한 문제를 다루기 위해 분할과 정복(Divide and Conquer) 원리를 적용한다.
- **구조적 방법론의 절차**

타당성 검토 단계 → 계획 단계 → 요구사항 단계 → 설계 단계 → 구현 단계 → 시험 단계 → 운용/유지보수 단계

3 정보공학 방법론

정보공학 방법론은 정보 시스템의 개발을 위해 계획, 분석, 설계, 구축에 정형화된 기법들을 상호 연관성 있게 통합 및 적용하는 자료(Data) 중심의 방법론이다.

- 정보 시스템 개발 주기를 이용하여 대규모 정보 시스템을 구축하는데 적합하다.
- **정보공학 방법론의 절차**

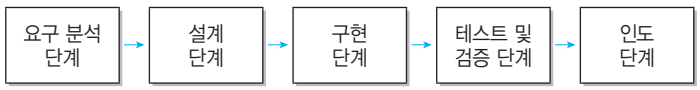
정보 전략 계획 수립 단계 → 업무 영역 분석 단계 → 업무 시스템 설계 단계 → 업무 시스템 구축 단계

4 객체지향 방법론

객체지향 방법론은 현실 세계의 개체(Entity)*를 기계의 부품처럼 하나의 객체(Object)로 만들어, 소프트웨어를 개발할 때 기계의 부품을 조립하듯이 객체들을 조립해서 필요한 소프트웨어를 구현하는 방법론이다.

현실 세계의 개체
사람, 자동차, 컴퓨터, 고양이 등과 같이 우리 주위에서 사용되는 물질적이거나 개념적인 것으로, 명사로 사용됩니다.

- 객체지향 방법론은 구조적 기법의 문제점으로 인한 소프트웨어 위기의 해결책으로 채택되었다.
- 객체지향 방법론의 구성 요소에는 객체(Object)*, 클래스(Class)*, 메시지(Message)* 등이 있다.
- 객체지향 방법론의 기본 원칙에는 캡슐화(Encapsulation)*, 정보 은닉(Information Hiding)*, 추상화(Abstraction)*, 상속성(Inheritance)*, 다형성(Polymorphism)* 등이 있다.
- **객체지향 방법론의 절차**



5 컴포넌트 기반(CBD; Component Based Design) 방법론

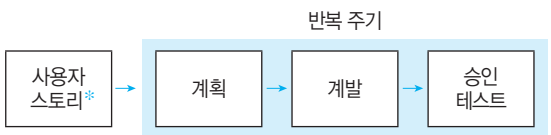
컴포넌트 기반 방법론은 기존의 시스템이나 소프트웨어를 구성하는 컴포넌트*를 조합하여 하나의 새로운 애플리케이션을 만드는 방법론이다.

- 컴포넌트의 재사용(Reusability)이 가능하여 시간과 노력을 절감할 수 있다.
- 유지 보수 비용을 최소화하고 생산성 및 품질을 향상시킬 수 있다.
- **컴포넌트 기반 방법론의 절차**

6 애자일(Agile) 방법론

애자일은 '민첩한', '기민한'이라는 의미로, 애자일 방법론은 고객의 요구사항 변화에 유연하게 대응할 수 있도록 일정한 주기를 반복하면서 개발 과정을 진행하는 방법론이다.

- 소규모 프로젝트, 고도로 숙달된 개발자, 급변하는 요구사항에 적합하다.
- 애자일 방법론의 대표적인 종류에는 익스트림 프로그래밍(XP; eXtreme Programming)*, 스크럼(Scrum)*, 칸반(Kanban), 크리스탈(Crytal) 등이 있다.
- **애자일 방법론의 절차**



- **객체(Object)** : 데이터와 데이터를 처리하는 함수를 묶어 놓은 하나의 소프트웨어 모듈
- **클래스(Class)** : 공통된 속성과 연산을 갖는 객체의 집합으로 객체의 일반적인 타입(Type)
- **메시지(Message)** : 객체들 간에 상호작용을 하는 데 사용되는 수단으로, 객체에게 어떤 행위를 하도록 지시하는 명령 또는 요구 사항
- **캡슐화(Encapsulation)** : 데이터와 데이터를 처리하는 함수를 하나로 묶는 것
- **정보 은닉(Information Hiding)** : 캡슐화에서 가장 중요한 개념으로, 다른 객체에게 자신의 정보를 숨기고 자신의 연산만을 통하여 접근을 허용하는 것
- **추상화(Abstraction)** : 불필요한 부분을 생략하고 객체의 속성 중 가장 중요한 것에 중점을 두어 개략화하는 것
- **상속성(Inheritance)** : 이미 정의된 상위 클래스의 모든 속성과 연산을 하위 클래스가 물려받는 것
- **다형성(Polymorphism)** : 메시지에 의해 객체가 연산을 수행하게 될 때 하나의 메시지에 대해 각 객체가 가지고 있는 고유한 방법으로 응답할 수 있는 능력

컴포넌트(Component)
문서, 소스코드, 파일, 라이브러리 등과 같은 모듈화된 자원으로, 재사용이 가능합니다.

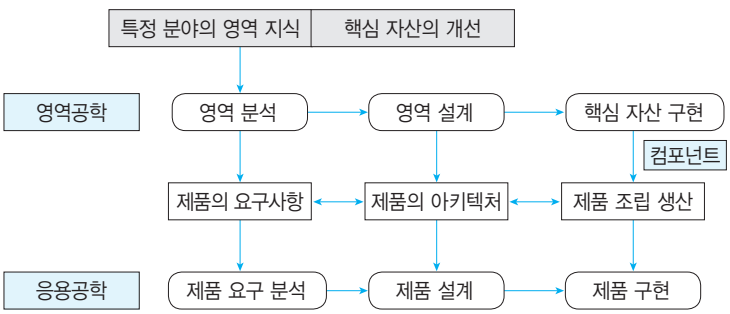
익스트림 프로그래밍에 대한 자세한 내용은 Section 003, 스크럼은 Section 002를 참조하세요.

사용자 스토리(User Story)
사용자 스토리는 사용자의 요구사항을 의미합니다.

7 제품 계열 방법론

제품 계열 방법론은 특정 제품에 적용하고 싶은 공통된 기능을 정의하여 개발하는 방법론이다.

- 임베디드 소프트웨어*를 만드는데 적합하다.
- 제품 계열 방법론은 영역공학과 응용공학으로 구분된다.
  - 영역공학 : 영역 분석, 영역 설계, 핵심 자산을 구현하는 영역이다.
  - 응용공학 : 제품 요구 분석, 제품 설계, 제품을 구현하는 영역이다.
- 영역공학과 응용공학의 연계를 위해 제품의 요구사항, 아키텍처, 조립 생산이 필요하다.
- **제품 계열 방법론의 절차**



임베디드 소프트웨어(Embedded Software)
임베디드 소프트웨어란 디지털 TV, 전기밥솥, 냉장고, PDA 등 해당 제품의 특정 기능에 맞게 특화되어서 제품 자체에 포함된 소프트웨어를 말합니다.

기출문제 따라잡기 Section 157

출제예상
1. 소프트웨어를 구성하는 컴포넌트를 조립해서 하나의 새로운 응용 프로그램을 작성하는 소프트웨어 개발 방법론은?

① Agile 방법론
② CBD 방법론
③ 구조적 방법론
④ 객체지향 방법론

이것은 **컴포넌트(Component)**를 **기반(Based)**으로 응용 프로그램을 **만드는(Design)** 방법론입니다.

출제예상
2. 다음 중 소프트웨어 개발 방법론 중 제품 계열 방법론에 대한 설명으로 가장 옳은 것은?

① 특정 제품에 적용하고 싶은 공통된 기능을 정의하여 개발하는 방법론이다.
② 소프트웨어를 구성하는 컴포넌트를 조립해서 하나의 새로운 응용 프로그램을 개발하는 방법론이다.
③ 고객의 요구사항을 바로바로 반영하고 상황에 따라 주어지는 문제를 풀어나가는 방법론이다.
④ 정보시스템 개발에 필요한 관리 절차와 작업 기법을 체계화한 방법론이다.

①번은 제품 계열 방법론, ②번은 컴포넌트 기반 방법론, ③번은 애자일 방법론, ④번은 정보공학 방법론에 해당합니다.

기출문제 따라잡기 Section 157

출제예상

3. 개체를 기계의 부품처럼 하나의 객체로 만들어, 기계적인 부품들을 조립하여 제품을 만들 듯이 소프트웨어를 개발할 때에도 객체들을 조립해서 작성할 수 있도록 하는 소프트웨어 개발 방법론은?

① 컴포넌트 기반(CBD) 방법론
② 애자일(Agile) 방법론
③ 제품 계열 방법론
④ 객체지향 방법론

객체지향은 각각의 객체로 프로그램이나 시스템을 구성하는 것을 의미합니다.

출제예상

4. 다음이 설명하고 있는 소프트웨어 개발 방법론은?

> 정형화된 분석 절차에 따라 사용자 요구사항을 파악하여 문서화하는 체계적인 분석 이론으로, 목적은 쉽게 이해할 수 있고 검증할 수 있는 프로그램 코드를 생성하는 것이다.

① Agile 방법론
② 구조적 방법론
③ CBD 방법론
④ 정보공학 방법론

이 방법론은 처리(Process)를 중심으로 쉽게 이해 및 검증 가능한 프로그램 코드를 생성하는 것이 목적입니다. 이제 답을 찾아보세요.

출제예상

5. 고객의 요구사항을 바로바로 반영하고 상황에 따라 주어지는 문제를 풀어나가는 소프트웨어 개발 방법론은?

① 애자일(Agile) 방법론
② 컴포넌트 기반(CBD) 방법론
③ 객체지향 방법론
④ 구조적 방법론

고객의 요구사항 변화에 유연하게 대응하는 방법론은 애자일 방법론입니다.

출제예상

6. 정보 시스템 개발에 필요한 관리 절차와 작업 기법을 체계화한 방법론으로, 개발 주기를 이용해 대형 프로젝트를 수행하는데 적합한 것은?

① 제품 계열 방법론
② 객체지향 방법론
③ 정보공학 방법론
④ 구조적 방법론

아직도 답을 못 찾겠으면 본문을 다시 한 번 공부하세요.

출제예상

7. 다음 중 애자일 방법론의 종류에 해당하지 않는 것은?

① 익스트림 프로그래밍(eXtreme Programming)
② 스크럼(Scrum)
③ 크리스탈(Crystal)
④ 짝 프로그래밍(Pair Programming)

짝 프로그래밍(Pair Programming)은 하나의 컴퓨터로 두 사람이 함께 프로그래밍 하는 것을 의미합니다.

▶ 정답 : 1. ② 2. ① 3. ④ 4. ② 5. ① 6. ③ 7. ④

SECTION
158
LIVE

비용 산정 기법

전문가의 조언

소프트웨어 비용 산정은 말 그대로 소프트웨어를 개발하는데 필요한 비용을 예측하는 것을 의미합니다. 비용 산정 기법은 그 방법에 따라 하향식 비용 산정 기법과 상향식 비용 산정 기법으로 분류할 수 있는데 이는 다음 섹션에서 공부할 예정이며, 여기서는 소프트웨어 비용 산정의 개요 및 비용 산정 시 고려사항에 대해서 학습하도록 하겠습니다.

전문가의 조언

소프트웨어 개발 비용은 시스템의 크기가 크고, 신뢰도가 높을수록 많이 들고, 개발 초기 보다 개발 후기로 갈수록 적게 듭니다.

1 소프트웨어 비용 산정의 개요

소프트웨어 비용 산정은 소프트웨어의 개발 규모를 소요되는 인원, 자원, 기간 등으로 확인하여 실행 가능한 계획을 수립하기 위해 필요한 비용을 산정하는 것이다.

- 소프트웨어 비용 산정을 너무 높게 산정할 경우 예산 낭비와 일의 효율성 저하를 초래할 수 있고, 너무 낮게 산정할 경우 개발자의 부담이 가중되고 품질문제가 발생할 수 있다.
- 소프트웨어 비용 산정 기법에는 하향식 비용 산정 기법과 상향식 비용 산정 기법이 있다.

2 소프트웨어 비용 결정 요소

소프트웨어 비용은 개발하는 소프트웨어, 소프트웨어 개발에 투입되는 자원, 소프트웨어 생산성에 따라 결정된다.

- 소프트웨어 비용을 결정하는 요소에는 프로젝트 요소, 자원 요소, 생산성 요소가 있다.

프로젝트 요소

- **제품 복잡도** : 소프트웨어의 종류에 따라 발생할 수 있는 문제점들의 난이도를 의미한다.
- **시스템 크기** : 소프트웨어의 규모에 따라 개발해야 할 시스템의 크기를 의미한다.
- **요구되는 신뢰도** : 일정 기간 내 주어진 조건하에서 프로그램이 필요한 기능을 수행하는 정도를 의미한다.

자원 요소

- **인적 자원** : 소프트웨어 개발 관련자들이 갖춘 능력 혹은 자질을 의미한다.
- **하드웨어 자원** : 소프트웨어 개발 시 필요한 장비와 워드프로세서, 프린터 등의 보조 장비를 의미한다.
- **소프트웨어 자원** : 소프트웨어 개발 시 필요한 언어 분석기, 문서화 도구 등의 개발 지원 도구를 의미한다.

생산성 요소

- **개발자 능력** : 개발자들이 갖춘 전문지식, 경험, 이해도, 책임감, 창의력 등을 의미한다.
- **개발 기간** : 소프트웨어를 개발하는 기간을 의미한다.

기출문제 따라잡기 Section 158

출제예상

1. 소프트웨어 비용 결정 요소 중 생산성 요소에 해당하는 것으로 올바르게 짝지어진 것은?

① 개발자 능력, 시스템 크기
② 신뢰도, 개발 기간
③ 개발자 능력, 개발 기간
④ 시스템 크기, 신뢰도

생산성 요소하면 '개발자 능력'과 '개발 기간'이라는 것을 기억해 두세요.

출제예상

2. 다음 중 소프트웨어 비용 산정에 대한 설명으로 가장 옳지 않은 것은?

① 소프트웨어의 규모를 기반으로 개발에 필요한 비용을 예측하는 것이다.
② 소프트웨어 비용을 낮게 산정할 경우 예산 낭비와 일의 효율성 저하를 초래할 수 있다.
③ 소프트웨어 비용 산정 기법에는 하향식 비용 산정 기법과 상향식 비용 산정 기법이 있다.
④ 소프트웨어 비용 결정 요소에는 프로젝트 요소, 자원 요소, 생산성 요소가 있다.

예산이 낭비되고 일의 효율성이 저하되는 경우는 예산이 많을 때일까요? 적을 때일까요?

출제예상

3. 소프트웨어 비용 결정 요소 중 자원 요소에 해당하지 않는 것은?

① 인적 ② 하드웨어
③ 소프트웨어 ④ 품질

자원은 소프트웨어 개발에 필요한 노동력, 프로그램, 장비 등을 의미합니다.

출제예상

4. 다음 중 소프트웨어 비용을 산정할 때 고려해야 할 요소가 아닌 것은?

① 프로젝트 요소 ② 자원 요소
③ 생산성 요소 ④ 위험 요소

벌써 잊었나요? 소프트웨어 비용을 결정하는 요소 3가지는 프로젝트 요소, 자원 요소, 생산성 요소입니다. 이젠 잊지마세요.

출제예상

5. 소프트웨어 비용 결정 요소 중 프로젝트 요소에 해당하지 않는 것은?

① 개발자 능력 ② 요구되는 신뢰도
③ 시스템 크기 ④ 제품 복잡도

개발자의 능력은 생산성 요소입니다.

▶ 정답 : 1. ③ 2. ② 3. ④ 4. ④ 5. ①

SECTION
159
LIVE

비용 산정 기법 – 하향식

전문가의 조언

비용 산정 기법은 그 방법에 따라 하향식 비용 산정 기법과 상향식 비용 산정 기법으로 분류할 수 있습니다. 하향식 비용 산정 기법에는 무엇이 있는지 정도만 구분할 수 있으면 됩니다.

1 하향식 비용 산정 기법의 개요

하향식 비용 산정 기법은 과거의 유사한 경험을 바탕으로 전문 지식이 많은 개발자들이 참여한 회의를 통해 비용을 산정하는 비과학적인 방법이다.

- 프로젝트의 전체 비용을 산정한 후 각 작업별로 비용을 세분화한다.
- 하향식 비용 산정 기법에는 전문가 감정 기법, 델파이 기법 등이 있다.

2 전문가 감정 기법

전문가 감정 기법은 조직 내에 있는 경험이 많은 두 명 이상의 전문가에게 비용 산정을 의뢰하는 기법이다.

- 가장 편리하고 신속하게 비용을 산정할 수 있으며, 의뢰자로부터 믿음을 얻을 수 있다.
- 새로운 프로젝트에는 과거의 프로젝트와 다른 요소들이 있다는 것을 간과할 수 있다.
- 새로운 프로젝트와 유사한 프로젝트에 대한 경험이 없을 수 있다.
- 개인적이고 주관적일 수 있다.

3 델파이 기법

델파이 기법은 전문가 감정 기법의 주관적인 편견을 보완하기 위해 많은 전문가의 의견을 종합하여 산정하는 기법이다.

- 전문가들의 편견이나 분위기에 지배되지 않도록 한 명의 조정자와 여러 전문가로 구성된다.
- **비용 산정 순서**
  1. 조정자는 각 비용 산정 요원에게 시스템 정의서와 산정한 비용 내역을 기록할 서식을 제공한다.
  2. 산정 요원들은 정의서를 분석하여 익명으로 그들 나름대로의 비용을 산정한다.
  3. 조정자는 산정 요원들의 반응을 요약하여 배포한다.
  4. 산정 요원들은 이전에 산정한 결과를 이용하여 다시 익명으로 산정한다.
  5. 요원들 간의 의견이 거의 일치할 때까지 이 과정을 반복한다.

기출문제 따라잡기 Section 159

출제예상

1. 과거의 유사한 경험을 바탕으로 전문 지식이 많은 개발자들이 참여한 회의를 통해 비용을 산정하는 비과학적인 방법은?

① 상향식 비용 산정 기법
② 하향식 비용 산정 기법
③ LOC 비용 산정 기법
④ 수학적 비용 산정 기법

'과거 경험', '비과학적 비용 산정 기법'하면 하향식 비용 산정 기법이란 것을 기억해 두세요.

출제예상

2. 하향식 비용 산정 기법 중 전문가 감정 기법에 대한 설명으로 가장 옳지 않은 것은?

① 조직 내에 있는 경험이 많은 두 명 이상의 전문가에게 비용 산정을 의뢰하는 기법이다.
② 가장 편리하고 신속하게 비용을 산정할 수 있는 기법이다.
③ 새로운 프로젝트와 유사한 프로젝트에 대한 경험이 없을 수 있다.
④ 집단적이고 객관적일 수 있다.

전문가 감정 기법은 개인적이고 주관적일 수 있습니다.

출제예상

3. 다음이 설명하는 비용 산정 기법은?

- 전문가 감정 기법의 주관적인 편견을 보완하기 위해 많은 전문가의 의견을 종합하여 산정하는 기법이다.
- 전문가들의 편견이나 분위기에 지배되지 않도록 한 명의 조정자와 여러 전문가로 구성된다.

① 델파이 기법
② 원시 코드 라인 수 기법
③ 개발 단계별 인원수 기법
④ 명목 집단 기법

전문가 감정 기법을 보완한 것은 델파이 기법입니다.

▶ 정답 : 1. ② 2. ④ 3. ①

SECTION 160 ● LIVE

비용 산정 기법 – 상향식

전문가의 조언

상향식 비용 산정 기법에서는 LOC 기법을 이용한 계산 문제가 중요합니다. 노력(인월), 개발 기간, 개발 비용 등을 구할 수 있도록 공식을 암기하고, 예제를 풀어 보세요.

1 상향식 비용 산정 기법의 개요

상향식 비용 산정 기법은 프로젝트의 세부적인 작업 단위별로 비용을 산정한 후 집계하여 전체 비용을 산정하는 방법이다.

- 상향식 비용 산정 기법에는 LOC(원시 코드 라인 수) 기법, 개발 단계별 인월수 기법, 수학적 산정 기법 등이 있다.

2 LOC(원시 코드 라인 수, source Line Of Code) 기법

LOC 기법은 소프트웨어 각 기능의 원시 코드 라인 수의 비관치*, 낙관치*, 기대치*를 측정하여 예측치를 구하고 이를 이용하여 비용을 산정하는 기법이다.

- 측정이 용이하고 이해하기 쉬워 가장 많이 사용된다.
- 예측치를 이용하여 생산성, 노력, 개발 기간 등의 비용을 산정한다.

$$\text{예측치} = \frac{a+4m+b}{6}$$ 단, a : 낙관치, b : 비관치, m : 기대치(중간치)

비관치, 낙관치, 기대치
- **비관치** : 가장 많이 측정된 코드 라인 수
- **낙관치** : 가장 적게 측정된 코드 라인 수
- **기대치** : 측정된 모든 코드 라인 수의 평균

- **산정 공식**
  - 노력(인월) = 개발 기간 × 투입 인원
    = LOC / 1인당 월평균 생산 코드 라인 수
  - 개발 비용 = 노력(인월) × 단위 비용(1인당 월평균 인건비)
  - 개발 기간 = 노력(인월) / 투입 인원
  - 생산성 = LOC / 노력(인월)

예제 LOC 기법에 의하여 예측된 총 라인 수가 30,000라인, 개발에 참여할 프로그래머가 5명, 프로그래머들의 평균 생산성이 월간 300라인일 때 개발에 소요되는 기간은?

- 노력(인월) = LOC/1인당 월평균 생산 코드 라인 수 = 30000/300 = 100명
- 개발 기간 = 노력(인월)/투입 인원 = 100/5 = 20개월

3 개발 단계별 인월수(Effort Per Task) 기법

개발 단계별 인원수 기법은 LOC 기법을 보완하기 위한 기법으로, 각 기능을 구현시키는 데 필요한 노력을 생명 주기의 각 단계별로 산정한다.

- LOC 기법보다 더 정확하다.

기출문제 따라잡기 Section 160

이전기출
1. 두 명의 개발자가 5개월에 걸쳐 10,000 라인의 코드를 개발하였을 때, 월별(Person Month) 생산성 측정을 위한 계산 방식으로 가장 적합한 것은?

① 10,000 / 2
② 10,000 / 5
③ 10,000 / (5 × 2)
④ (2 × 10,000) / 5

생산성은 '원시 코드 라인 수/노력'입니다. 노력은 소프트웨어를 한 달 간 개발하는 데 소요되는 총 인원 또는 한 사람을 기준으로 몇 개월에 걸쳐 개발했느냐를 나타내는데, 이를 계산하는 방법은 '투입 인원 × 개발 기간'입니다.

이전기출
2. 어떤 소프트웨어 개발을 위해 10명의 개발자가 10개월 동안 참여되었다. 그런데 그 중 7명은 10개월 동안 계속 참여했지만 3명은 3개월 동안만 부분적으로 참여했다. 이 소프트웨어 개발을 위한 인월(Man Month)은 얼마인가?

① 100 ② 70
③ 79 ④ 60

7명이 10개월 동안 개발한 것의 노력(인월)은 70이고, 3명이 3개월 동안 개발한 것의 노력은 9입니다. 이를 더하면 전체 노력(인월)이 됩니다.

이전기출
3. LOC 기법에 의하여 예측된 총 라인 수가 25000 라인일 경우 개발에 투입될 프로그래머의 수가 5명이고, 프로그래머들의 평균 생산성이 월당 500라인일 때, 개발에 소요되는 시간은?

① 8개월 ② 9개월
③ 10개월 ④ 11개월

쉽게 생각해 보세요. 25000라인을 5명이 개발하는 데 한 사람이 한 달에 500라인을 생산한다면, 25000 / (5×500) = 10, 즉 개발 기간은 10개월입니다. 물론 공식에 대입해서 풀어도 됩니다.

이전기출
4. COCOMO의 비용 산정에 의해 개발에 소요되는 노력이 40PM (Programmer-Month)으로 계산되었다. 개발에 소요되는 기간이 5개월이고, 1인당 인건비가 100만 원이라면 이 프로젝트에 소요되는 총 인건비는 얼마인가?

① 2억 원 ② 1억 원
③ 4천만 원 ④ 2천만 원

개발 비용(총 인건비)은 '노력(인월) × 단위 비용(1인당 월평균 인건비)'이므로 40PM × 1,000,000 = 40,000,000 즉 4천만 원이 됩니다.

이전기출
5. 비용 산정 기법 중 소프트웨어 각 기능의 원시 코드 라인 수의 비관치, 낙관치, 기대치를 측정하여 예측치를 구하고 이를 이용하여 비용을 산정하는 기법은?

① Effort Per Task 기법
② 전문가 감정 기법
③ LOC 기법
④ 델파이 기법

'코드 라인 수'가 영문 약어로 무엇인지 생각해 보세요.

▶ 정답 : 1. ③ 2. ③ 3. ③ 4. ③ 5. ③

SECTION 161 ● LIVE

수학적 산정 기법

전문가의 조언

소프트웨어 추정 모형의 종류를 구분할 수 있어야 합니다. 소프트웨어 추정 모형에는 COCOMO, Putnam 모형, 기능 점수(FP) 모형 등이 있다는 것을 기억하고, 각 모형의 특징을 구분할 수 있도록 학습하세요.

1 수학적 산정 기법의 개요

수학적 산정 기법은 상향식 비용 산정 기법으로, 경험적 추정 모형, 실험적 추정 모형 이라고도 하며, 개발 비용 산정의 자동화를 목표로 한다.

- 비용을 자동으로 산정하기 위해 사용되는 공식은 과거 유사한 프로젝트를 기반으로하여 경험적으로 유도된 것이다.
- 수학적 산정 기법에는 COCOMO 모형, Putnam 모형, 기능 점수(FP) 모형 등이 있으며 각 모형에서는 지정된 공식을 사용하여 비용을 산정한다.

2 COCOMO 모형 개요

COCOMO(COnstructive COst MOdel) 모형은 보헴(Boehm)이 제안한 것으로, 원시 프로그램의 규모인 LOC(원시 코드 라인 수)에 의한 비용 산정 기법이다.

- 개발할 소프트웨어의 규모(LOC)를 예측한 후 이를 소프트웨어 종류에 따라 다르게 책정되는 비용 산정 방정식에 대입하여 비용을 산정한다.
- 비용 견적의 강도 분석 및 비용 견적의 유연성이 높아 소프트웨어 개발비 견적에 널리 통용되고 있다.
- 같은 규모의 프로그램이라도 그 성격에 따라 비용이 다르게 산정된다.
- 비용 산정 결과는 프로젝트를 완성하는 데 필요한 노력(Man-Month)으로 나타난다.

전문가의 조언

소프트웨어 개발 유형을 구분하는 기준과 각 개발 유형의 특징을 구분할 수 있어야 합니다. 공식을 암기할 필요는 없습니다.

3 COCOMO의 소프트웨어 개발 유형

소프트웨어 개발 유형은 소프트웨어의 복잡도 혹은 원시 프로그램의 규모에 따라 조직형(Organic Mode), 반분리형(Semi-Detached Mode), 내장형(Embedded Mode)으로 분류할 수 있다.

조직형(Organic Mode)

조직형은 기관 내부에서 개발된 중 · 소 규모의 소프트웨어로 일괄 자료 처리나 과학 기술 계산용, 비즈니스 자료 처리용으로 5만(50KDSI*) 라인 이하의 소프트웨어를 개발하는 유형이다.

- 사무 처리용, 업무용, 과학용 응용 소프트웨어 개발에 적합하다.
- 비용을 산정하는 공식은 다음과 같다.

> - 노력(MM) = 2.4 × $(KDSI)^{1.05}$
> - 개발 기간(TDEV) = 2.5 × $(MM)^{0.38}$

KDSI(Kilo Delivered Source Instruction)
전체 라인 수를 1,000라인 단위로 묶은 것으로 KLOC(Kilo LOC)와 같은 의미입니다.

반분리형(Semi-Detached Mode)

반분리형은 조직형과 내장형의 중간형으로 트랜잭션 처리 시스템이나 운영체제, 데이터베이스 관리 시스템 등의 30만(300KDSI) 라인 이하의 소프트웨어를 개발하는 유형이다.

- 컴파일러, 인터프리터와 같은 유틸리티 개발에 적합하다.
- 비용을 산정하는 공식은 다음과 같다.

> - 노력(MM) = $3.0 \times (KDSI)^{1.12}$
> - 개발 기간(TDEV) = $2.5 \times (MM)^{0.35}$

내장형(Embedded Mode)

내장형은 최대형 규모의 트랜잭션 처리 시스템이나 운영체제 등의 30만(300KDSI) 라인 이상의 소프트웨어를 개발하는 유형이다.

- 신호기 제어 시스템, 미사일 유도 시스템, 실시간 처리 시스템 등의 시스템 프로그램 개발에 적합하다.
- 비용을 산정하는 공식은 다음과 같다.

> - 노력(MM) = $3.6 \times (KDSI)^{1.20}$
> - 개발 기간(TDEV) = $2.5 \times (MM)^{0.32}$

4 COCOMO 모형의 종류

COCOMO는 비용 산정 단계 및 적용 변수의 구체화 정도에 따라 기본(Basic), 중간(Intermediate), 발전(Detailed)형으로 구분할 수 있다.

기본(Basic)형 COCOMO

기본형 COCOMO는 소프트웨어의 크기(생산 코드 라인 수)와 개발 유형만을 이용하여 비용을 산정하는 모형이다.

- 산정 공식*
  - 개발 노력(Effort, MM, PM) = $a \times (KDSI)^{b}$
  - 개발 기간(TDEV) = $c \times (MM)^{d}$
  - 적정 투입 인원(FPS) = MM / TDEV
  - 인적 비용(COST) = MM × 1인당 월평균 급여

중간(Intermediate)형 COCOMO

중간형 COCOMO는 기본형 COCOMO의 공식을 토대로 사용하나, 다음 4가지 특성의 15가지 요인에 의해 비용을 산정하는 모형이다.

- **제품의 특성** : 요구되는 신뢰도, 데이터베이스 크기, 제품의 복잡도
- **컴퓨터의 특성** : 수행 시간의 제한, 기억장소의 제한, 가상 기계의 안정성, Turn Around Time

전문가의 조언

COCOMO 모형의 종류를 구분할 때의 기준과 각각의 특징 정도만 알아두세요. 물론 공식을 암기할 필요는 없습니다.

산정 공식

a, b, c, d는 소프트웨어 개발 유형, 즉 조직형이냐 반분리형이냐 내장형이냐에 따라 정해진 값을 사용합니다.

- **개발 요원의 특성** : 분석가의 능력, 개발 분야의 경험, 가상 기계의 경험, 프로그래머의 능력, 프로그래밍 언어의 경험
- **프로젝트 특성** : 소프트웨어 도구의 이용, 프로젝트 개발 일정, 최신 프로그래밍 기법의 이용
- 산정 공식
  - 개발 노력(MM) = 기본 COCOMO의 MM × 요인별 노력 승수*
  - 개발 기간(TDEV) = c × $(MM)^d$
  - 적정 투입 인원(FPS) = MM / TDEV
  - 인적 비용(COST) = MM × 1인당 월평균 급여

요인별 노력 승수
요인별 노력 승수는 15가지 요인의 높고 낮음에 따라 정해진 값을 사용합니다.

발전(Detailed)형 COCOMO

발전형 COCOMO는 중간(Intermediate)형 COCOMO를 보완하여 만들어진 방법으로 개발 공정별로 보다 자세하고 정확하게 노력을 산출하여 비용을 산정하는 모형이다.

- 소프트웨어 환경과 구성 요소가 사전에 정의되어 있어야 하며, 개발 과정의 후반부에 주로 적용한다.
- **산정 공식** : 중간형 COCOMO 산정 공식을 그대로 사용하되, 노력 승수를 다음과 같이 적용하여 산정한다.

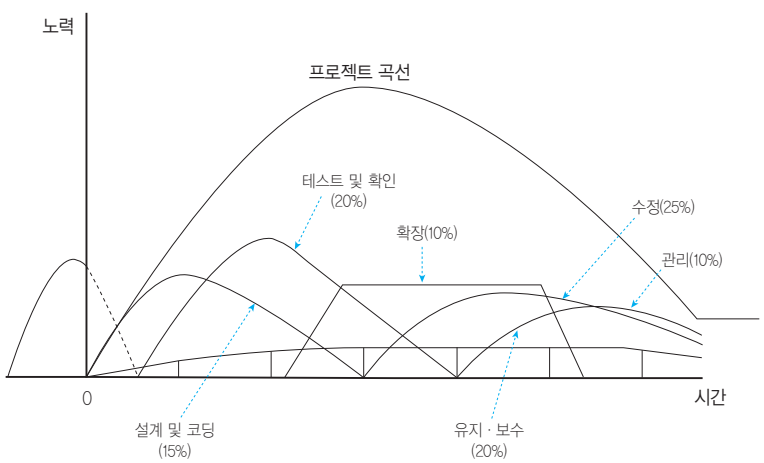
노력 승수 = 개발 공정별 노력 승수 × 개발 공정별 가중치

5 Putnam 모형

Putnam 모형은 소프트웨어 생명 주기의 전 과정 동안에 사용될 노력의 분포를 가정해 주는 모형이다.

- 푸트남(Putnam)이 제안한 것으로 생명 주기 예측 모형이라고도 한다.
- 시간에 따른 함수로 표현되는 Rayleigh-Norden 곡선*의 노력 분포도를 기초로 한다.

Rayleigh-Norden 곡선
노든(Norden)이 소프트웨어 개발에 관한 경험적 자료를 수집하여 이를 근거로 그린 곡선입니다.



- 대형 프로젝트의 노력 분포 산정에 이용되는 기법이다.
- 개발 기간이 늘어날수록 프로젝트 적용 인원의 노력이 감소한다.
- 산정 공식

$$\text{개발 노력(MM)} = \frac{L^3}{C_k^3 \cdot Td^4}$$

- L : 원시 코드 라인 수
- Td : 개발 기간
- C_k : 환경 상수(빈약 환경 = 2,000, 좋은 환경 = 8,000, 최적 환경 = 12,000)

6 기능 점수(FP) 모형

기능 점수(Function Point) 모형은 알브레히트(Albrecht)가 제안한 것으로, 소프트웨어의 기능을 증대시키는 요인별로 가중치를 부여하고, 요인별 가중치를 합산하여 총 기능 점수*를 산출하며 총 기능 점수와 영향도를 이용하여 기능 점수(FP)를 구한 후 이를 이용해서 비용을 산정하는 기법이다.

기능 점수(FP) = 총 기능 점수 × [0.65 + (0.1 × 총 영향도)]

- 발표 초기에는 관심을 받지 못하였으나 최근에는 그 유용성과 간편성으로 비용 산정 기법 가운데 최선의 평가를 받고 있다.
- 기능별 가중치

소프트웨어 기능 증대 요인	가중치		
	단순	보통	복잡
자료 입력(입력 양식)	3	4	6
정보 출력(출력 보고서)	4	5	7
명령어(사용자 질의수)	3	4	5
데이터 파일	7	10	15
필요한 외부 루틴과의 인터페이스	5	7	10

자동화 추정 도구

비용 산정의 자동화를 위해 개발된 도구로는 SLIM과 ESTIMACS가 있습니다.

- SLIM : Rayleigh-Norden 곡선과 Putnam 예측 모델을 기초로 하여 개발된 자동화 추정 도구입니다.
- ESTIMACS : 다양한 프로젝트와 개인별 요소를 수용하도록 FP 모형을 기초로 하여 개발된 자동화 추정 도구입니다.

전문가의 조언

COCOMO나 Putnam 모형은 LOC를 중심으로 비용을 산정하는데 반해 기능 점수 모형은 FP를 이용하여 비용을 산정한다는것 정도만 알아두세요.

총 기능 점수

소프트웨어 개발의 규모, 복잡도, 난이도 등을 하나의 수치로 집약시킨 것을 의미합니다.

이전기출
1. 소프트웨어 추정 모형(Estimation Model)이 아닌 것은?

① COCOMO ② Putnam
③ Function-Point ④ PERT

소프트웨어 추정 모형의 종류를 기억해야 한다고 했죠? PERT는 프로젝트에 필요한 전체 작업의 상호 관계를 표시하는 네트워크로, 일정 계획을 위한 도구입니다.

이전기출
2. COCOMO의 프로젝트 모드가 아닌 것은?

① Organic Mode
② Semi-detached Mode
③ Medium Mode
④ Embedded Mode

COCOMO의 소프트웨어 개발 유형과 특징을 구분할 수 있어야 합니다. COCOMO의 소프트웨어 개발 유형에는 조직형, 반분리형, 내장형이 있습니다. 물론 영문까지 정확하게 기억해야 합니다.

이전기출
3. COCOMO 기법에 의한 소프트웨어 모형에 속하지 않는 것은?

① Basic COCOMO
② Putnam COCOMO
③ Intermediate COCOMO
④ Detailed COCOMO

COCOMO 모형의 종류와 특징을 구분하라고 했죠? 기본(Basic), 중간(Intermediate), 발전(Detailed)형! COCOMO 소프트웨어 개발 유형과 COCOMO 모형의 종류를 혼동하지 마세요.

이전기출
4. COCOMO(COnstructive COst MOdel) 모형에 대한 설명으로 옳지 않은 것은?

① 산정 결과는 프로젝트를 완성하는 데 필요한 Man-Month로 나타난다.
② Boehm이 고안한 개발비 산정 모델로 프로젝트의 예상되는 크기와 유형에 관한 정보가 주로 사용된다.
③ 프로젝트 특성을 15개로 나누고 각각에 대한 승수값을 제시하였다.
④ 각 모델별로 개발되어지는 프로젝트 개발 유형에 따라 Object Mode, Dynamic Mode, Function Mode의 세 가지 모드로 구분한다.

COCOMO에 대한 다양한 특징을 알아야 풀 수 있는 문제이지만 COCOMO의 개발 유형만 알면 답을 바로 찾을 수 있습니다. COCOMO의 개발 유형 세 가지는 반드시 기억해야 합니다.

이전기출
5. COCOMO(COnstructive COst MOdel) 비용 예측 모델에 대한 설명으로 옳지 않은 것은?

① B. Boehm이 제안한 원시 프로그램의 규모에 의한 비용 예측 모형이다.
② 소프트웨어의 종류에 따라 다르게 책정되는 비용 산정 방정식을 이용한다.
③ COCOMO 방법은 가정과 제약 조건 없이 모든 시스템에 적용할 수 있다.
④ 같은 규모의 프로그램이라도 그 성격에 따라 비용이 다르게 생성된다.

COCOMO 방법은 소프트웨어의 규모와 복잡도, 종류 등에 따라 적용할 가정과 제약 조건이 있습니다.

이전기출
6. COCOMO Model 중 기관 내부에서 개발된 중소 규모의 소프트웨어로 일괄 자료 처리나 과학 기술 계산용, 비즈니스 자료 처리용으로 5만 라인 이하의 소프트웨어를 개발하는 유형은?

① Semi-Detached Model
② Organic Model
③ Semi-Embedded Model
④ Embedded Model

COCOMO 모형의 소프트웨어 개발 유형은 크기에 따라 분류한다고 했죠? Organic은 5만 라인 이하, Semi-Detached는 30만 라인 이하, Embedded는 30만 라인 이상의 최대형 규모에 사용합니다. 잊지마세요.

이전기출
7. 다음의 자동화 예측 도구들 중 Rayleigh-Norden 곡선과 Putnam의 예측 모델에 기반을 둔 것은?

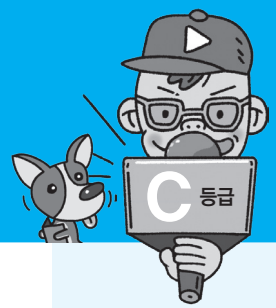
① SLIM ② ESTIMACS
③ SPQR/20 ④ WICOMO

Rayleigh-Norden 곡선과 Putnam의 예측 모델에 기반을 둔 자동화 예측 도구는 SLIM이라고 했죠? ESTIMACS는 FP 모형을 기초로 하여 만든 자동화 예측 도구입니다.

▶ 정답 : 1. ④ 2. ③ 3. ② 4. ④ 5. ③ 6. ② 7. ①

SECTION
162
LIVE

소프트웨어 개발 방법론 결정



1 소프트웨어 개발 방법론 결정의 개요

소프트웨어 개발 방법론의 결정은 프로젝트 관리와 재사용 현황을 소프트웨어 개발 방법론에 반영하고, 확정된 소프트웨어 생명 주기와 개발 방법론에 맞춰 소프트웨어 개발 단계, 활동, 작업, 절차 등을 정의하는 것이다.

프로젝트 관리

프로젝트 관리(Project Management)는 주어진 기간 내에 최소의 비용으로 사용자를 만족시키는 시스템을 개발하기 위한 전반적인 활동입니다.

관리 유형	주요 내용
일정 관리	작업 순서, 작업 기간 산정, 일정 개발, 일정 통제
비용 관리	비용 산정, 비용 예산 편성, 비용 통제
인력 관리	프로젝트 팀 편성, 자원 산정, 프로젝트 조직 정의, 프로젝트 팀 개발, 자원 통제, 프로젝트 팀 관리
위험 관리	위험 식별, 위험 평가, 위험 대처, 위험 통제
품질 관리	품질 계획, 품질 보증 수행, 품질 통제 수행

2 소프트웨어 개발 방법론 결정 절차

❶ 프로젝트 관리와 재사용 현황을 소프트웨어 개발 방법론에 반영한다.
- 소프트웨어 개발 방법론에 프로젝트 관리와 재사용 현황을 반영하는 방법을 프로젝트 관련자들에게 설명한다.
- 소프트웨어 개발 방법론에 프로젝트 관리와 재사용 현황을 반영하고 그 결과를 프로젝트 관련자들에게 설명한 후 결정한다.

❷ 개발 단계별 작업 및 절차를 소프트웨어 생명 주기에 맞춰 수립한다.
- 소프트웨어의 기본 생명 주기, 지원 생명 주기, 조직 생명 주기별로 주요 프로세스를 확인한다.
- 소프트웨어의 개발 프로세스*, 개발 생명 주기*, 프로세스 모형*을 정리한다.

❸ 결정된 소프트웨어 개발 방법론의 개발 단계별 활동 목적, 작업 내용, 산출물에 대한 매뉴얼을 작성한다.

전문가의 조언

소프트웨어 개발 방법론을 결정한다는 것은 투입 자원 및 일정, 비용, 품질, 위험 관리 등 여러 조건을 확인하여 어떤 방법론으로 소프트웨어를 개발할지를 결정하는 것을 의미합니다. 소프트웨어 개발 방법론을 결정하는 절차에 대해 알아두세요.

소프트웨어 개발 프로세스
소프트웨어 제품 생산을 위해 수행하는 작업으로, 소프트웨어 명세, 개발, 검토, 진화로 구분됩니다.

소프트웨어 개발 생명 주기
소프트웨어를 개발하기 위해 정의하고 운용, 유지보수 등의 과정을 각 단계별로 나눈 것입니다.

소프트웨어 프로세스 모형
소프트웨어 생명 주기를 표현하는 형태를 의미하며, 대표적인 모형에는 폭포수 모형(Waterfall Model), 나선형 모형(Spiral Model), 프로토타이핑 모형(Prototyping Model)이 있습니다.

기출문제 따라잡기 Section 162

출제예상

1. 다음 지문의 내용에 해당하는 프로세스 관리의 유형은?

> 프로젝트 팀 편성, 프로젝트 조직 정의, 프로젝트 팀 개발, 프로젝트 팀 관리

① 비용 관리 ② 일정 관리
③ 품질 관리 ④ 인력 관리

팀과 조직은 같은 일을 하는 사람으로 구성된 집단을 의미합니다.

출제예상

2. 다음 중 소프트웨어 개발 방법론을 결정하는 절차에 대한 설명으로 가장 옳지 않은 것은?

① 프로젝트 관리와 재사용 현황을 소프트웨어 개발 방법론에 반영한다.
② 소프트웨어의 기본 생명 주기, 단위 생명 주기, 통합 생명 주기별로 주요 프로세스를 확인한다.
③ 소프트웨어의 개발 프로세스, 개발 생명 주기, 프로세스 모형을 정리한다.
④ 확정된 소프트웨어 개발 방법론의 개발 단계별 활동 목적 등에 대한 매뉴얼을 작성한다.

소프트웨어 생명 주기는 기본, 지원, 조직 생명 주기로 구분합니다.

출제예상

3. 다음 중 프로젝트 관리의 유형에 해당하지 않는 것은?

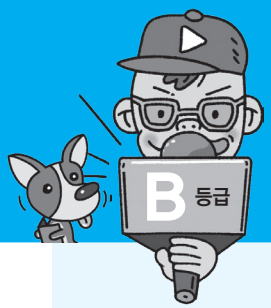
① 보안 관리 ② 위험 관리
③ 품질 관리 ④ 일정 관리

프로젝트 관리는 '일정, 비용, 인력, 위험, 품질'을 관리하는 것을 의미합니다.

▶ 정답 : 1. ④ 2. ② 3. ①

SECTION
163
LIVE

소프트웨어 개발 표준



1 소프트웨어 개발 표준의 개요

소프트웨어 개발 표준은 소프트웨어 개발 단계에서 수행하는 품질 관리에 사용되는 국제 표준을 의미한다.

- 대표적인 소프트웨어 개발 표준에는 ISO/IEC 12207, CMMI, SPICE 등이 있다.

전문가의 조언

소프트웨어 개발 표준의 종류에는 어떤 것들이 있는지 정확히 숙지하고, 어떤 종류의 특징을 말하는지 구분할 수 있도록 잘 정리하세요.

2 ISO/IEC 12207

ISO/IEC 12207은 ISO(International Organization for Standardization, 국제표준화기구)에서 만든 표준 소프트웨어 생명 주기 프로세스로, 소프트웨어의 개발, 운영, 유지보수 등을 체계적으로 관리하기 위한 소프트웨어 생명 주기 표준을 제공한다.

- ISO/IEC 12207은 기본 생명 주기 프로세스, 지원 생명 주기 프로세스, 조직 생명 주기 프로세스로 구분한다.

기본 생명 주기 프로세스	획득, 공급, 개발, 운영, 유지보수 프로세스
지원 생명 주기 프로세스	품질 보증, 검증, 확인, 활동 검토, 감사, 문서화, 형상 관리, 문제 해결 프로세스
조직 생명 주기 프로세스	관리, 기반 구조, 훈련, 개선 프로세스

3 CMMI(Capability Maturity Model Integration)

CMMI(능력 성숙도 통합 모델)는 소프트웨어 개발 조직의 업무 능력 및 조직의 성숙도를 평가하는 모델로, 미국 카네기멜론 대학교의 소프트웨어 공학연구소(SEI)에서 개발하였다.

- CMMI의 소프트웨어 프로세스 성숙도는 초기, 관리, 정의, 정량적 관리, 최적화의 5단계로 구분한다.

단계	프로세스	특징
초기(Initial)	정의된 프로세스 없음	작업자 능력에 따라 성공 여부 결정
관리(Managed)	규칙화된 프로세스	특정한 프로젝트 내의 프로세스 정의 및 수행
정의(Defined)	표준화된 프로세스	조직의 표준 프로세스를 활용하여 업무 수행
정량적 관리 (Quantitatively Managed)	예측 가능한 프로세스	프로젝트를 정량적으로 관리 및 통제
최적화(Optimizing)	지속적 개선 프로세스	프로세스 역량 향상을 위해 지속적인 프로세스 개선

4 SPICE(Software Process Improvement and Capability dEtermination)

SPICE(소프트웨어 처리 개선 및 능력 평가 기준)는 정보 시스템 분야에서 소프트웨어의 품질 및 생산성 향상을 위해 소프트웨어 프로세스를 평가 및 개선하는 국제 표준으로, 공식 명칭은 ISO/IEC 15504이다.

- **SPICE의 목적**
  - 프로세스 개선을 위해 개발 기관이 스스로 평가하는 것
  - 기관에서 지정한 요구조건의 만족여부를 개발 조직이 스스로 평가하는 것
  - 계약 체결을 위해 수탁 기관의 프로세스를 평가하는 것
- SPICE는 5개의 프로세스 범주와 40개의 세부 프로세스로 구성된다.

범주	특징
고객-공급자 (Customer-Supplier) 프로세스	• 소프트웨어를 개발하여 고객에게 전달하는 것을 지원하고, 소프트웨어의 정확한 운용 및 사용을 위한 프로세스로 구성된다. • 구성 요소 : 인수, 공급, 요구 도출, 운영 • 프로세스 수 : 10개
공학(Engineering) 프로세스	• 시스템과 소프트웨어 제품의 명세화, 구현, 유지보수를 하는데 사용되는 프로세스로 구성된다. • 구성 요소 : 개발, 소프트웨어 유지보수 • 프로세스 수 : 9개
지원(Support) 프로세스	• 소프트웨어 생명 주기에서 다른 프로세스에 의해 이용되는 프로세스로 구성된다. • 구성 요소 : 문서화, 형상, 품질 보증, 검증, 확인, 리뷰, 감사, 품질 문제 해결 • 프로세스 수 : 8개
관리(Management) 프로세스	• 소프트웨어 생명 주기에서 프로젝트 관리자에 의해 사용되는 프로세스로 구성된다. • 구성 요소 : 관리, 프로젝트 관리, 품질 및 위험 관리 • 프로세스 수 : 4개
조직(Organization) 프로세스	• 조직의 업무 목적 수립과 조직의 업무 목표 달성을 위한 프로세스로 구성된다. • 구성 요소 : 조직 배치, 개선 활동 프로세스, 인력 관리, 기반 관리, 측정 도구, 재사용 • 프로세스 수 : 9개

- SPICE는 프로세스 수행 능력 단계를 불완전, 수행, 관리, 확립, 예측, 최적화의 6단계로 구분한다.

단계	특징
불완전(Incomplete)	프로세스가 구현되지 않았거나 목적을 달성하지 못한 단계이다.
수행(Performed)	프로세스가 수행되고 목적이 달성된 단계이다.
관리(Managed)	정의된 자원의 한도 내에서 그 프로세스가 작업 산출물을 인도하는 단계이다.
확립(Established)	소프트웨어 공학 원칙에 기반하여 정의된 프로세스가 수행되는 단계이다.
예측(Predictable)	프로세스가 목적 달성을 위해 통제되고, 양적인 측정을 통해서 일관되게 수행되는 단계이다.
최적화(Optimizing)	프로세스 수행을 최적화하고, 지속적인 개선을 통해 업무 목적을 만족시키는 단계이다.

기출문제 따라잡기

출제예상

1. 다음 중 소프트웨어 개발 표준이 아닌 것은?

① SPICE ② CMMI
③ SCRUM ④ ISO/IEC 12207

소프트웨어 개발 표준 종류 3가지는 'SPICE, CMMI, ISO/IEC 12207'입니다.

출제예상

2. 다음이 설명하고 있는 소프트웨어 개발 표준은?

ISO에서 만든 소프트웨어 생명 주기 프로세스로, 소프트웨어와 관련된 조직과 사람, 소프트웨어 획득자, 공급자, 개발자, 운영자, 유지보수자, 품질보증 관리자, 사용자 등의 이해관계자들이 각자의 입장에서 수행해야 할 일을 정의하고 지속적으로 개선시키기 위한 소프트웨어 생명 주기 표준을 제공한다.

① ISO/IEC 12207 ② SPICE
③ CMMI ④ ISO 26262

소프트웨어 개발 표준의 종류별 개념을 숙지해야 한다고 했죠? 답을 찾지 못하겠으면 섹션 내용을 다시 한 번 공부하세요.

출제예상

3. 소프트웨어 개발 표준 중 조직의 개발 프로세스 역량 성숙도를 평가하는 표준은?

① CMMI ② SPICE
③ ISO 26262 ④ ISO/IEC 12207

이 표준은 조직의 개발 프로세스 **역량(Capability) 성숙도(Maturity)**를 **통합적(Integration)**으로 평가하는 **모델(Model)**입니다.

출제예상

4. 소프트웨어 개발 표준 중 소프트웨어 프로세스 평가를 위한 국제 표준을 제정하는 프로젝트는?

① ISO/IEC 12207 ② CMMI
③ SPICE ④ ISO 26262

이 표준은 **소프트웨어(Software) 프로세스(Process) 개선(Improvement)** 및 **능력(Capability)**을 **평가(dEtermination)**하는 것입니다.

출제예상

5. 다음 중 ISO/IEC 12207의 프로세스가 아닌 것은?

① 기본 생명 주기 프로세스
② 지원 생명 주기 프로세스
③ 조직 생명 주기 프로세스
④ 통합 생명 주기 프로세스

ISO/IEC 12207의 프로세스하면 '기본, 지원, 조직'! 잊지마세요.

출제예상

6. 다음 중 SPICE의 프로세스 수행 능력 단계에 대한 설명으로 가장 옳지 않은 것은?

① 불완전 단계는 프로세스가 구현되지 않았거나, 프로세스가 그 목적을 달성하지 못한 단계이다.
② 수행 단계는 프로세스의 목적이 전반적으로 이루어진 단계이다.
③ 확립 단계는 정의된 자원의 한도 내에서 그 프로세스가 작업 산출물을 인도하는 단계이다.
④ 최적화 단계는 프로세스 수행을 최적화하고, 지속적으로 업무 목적을 만족시키는 단계이다.

확립 단계는 소프트웨어 공학 원칙에 기반하여 정의된 프로세스가 수행되는 단계입니다.

출제예상

7. 다음 중 SPICE의 프로세스에 대한 설명으로 가장 옳지 않은 것은?

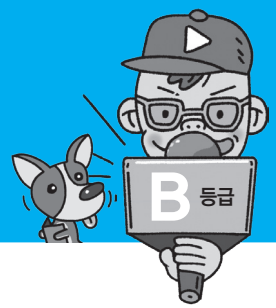
① Support 프로세스는 소프트웨어 생명 주기에서 다른 프로세스에 의해 이용되는 프로세스로 구성된다.
② Management 프로세스는 조직의 업무 목적 수립과 조직의 업무 목표 달성을 위한 프로세스로 구성된다.
③ Engineering 프로세스는 시스템과 소프트웨어 제품의 명세화, 구현, 유지보수를 하는데 사용되는 프로세스로 구성된다.
④ Customer-Supplier 프로세스는 소프트웨어를 개발하여 고객에게 전달하는 것을 지원하고, 소프트웨어의 정확한 운용 및 사용을 위한 프로세스로 구성된다.

Management 프로세스는 소프트웨어 생명 주기에서 프로젝트 관리자에 의해 사용되는 프로세스로 구성됩니다.

▶ 정답 : 1. ③ 2. ① 3. ① 4. ③ 5. ④ 6. ③ 7. ②

SECTION 164 ● LIVE

소프트웨어 개발 방법론 테일러링



전문가의 조언

테일러링(Tailoring)의 사전적 의미는 '재단, 양복업'으로, 표준을 기반으로 실제 업무에서 여건에 맞게 수정 · 보완하는 것을 의미합니다. 소프트웨어 개발 방법론 테일러링에서는 테일러링 작성 시 고려사항, 테일러링 기법을 중심으로 학습하세요.

1 소프트웨어 개발 방법론 테일러링의 개요

소프트웨어 개발 방법론 테일러링은 프로젝트 상황 및 특성에 맞도록 정의된 소프트웨어 개발 방법론의 절차, 사용기법 등을 수정 및 보완하는 작업이다.

- **소프트웨어 개발 방법론 테일러링 수행절차**

프로젝트 특징 정의 → 표준 프로세스 선정 및 검증 → 상위 수준의 커스터마이징 → 세부 커스터마이징 → 테일러링 문서화

2 소프트웨어 개발 방법론 테일러링 고려사항

소프트웨어 개발 방법론 테일러링 작업 시 고려해야 할 사항에는 내부적 요건과 외부적 요건이 있다.

내부적 요건

- **목표 환경** : 시스템의 개발 환경과 유형이 서로 다른 경우 테일러링이 필요하다.
- **요구사항** : 프로젝트의 생명 주기 활동에서 개발, 운영, 유지보수 등 프로젝트에서 우선적으로 고려할 요구사항이 서로 다른 경우 테일러링이 필요하다.
- **프로젝트 규모** : 비용, 인력, 기간 등 프로젝트의 규모가 서로 다른 경우 테일러링이 필요하다.
- **보유 기술** : 프로세스, 개발 방법론, 산출물 등이 서로 다른 경우 테일러링이 필요하다.

외부적 요건

- **법적 제약사항** : 프로젝트별로 적용될 IT Compliance*가 서로 다른 경우 테일러링이 필요하다.
- **표준 품질 기준** : 금융, 제도 등 분야별 표준 품질 기준이 서로 다른 경우 테일러링이 필요하다.

IT Compliance
기업 운영 시 IT 분야에서 내 · 외부적으로 반드시 지켜야 하는 법적 규제 사항이나 지침을 의미합니다.

3 소프트웨어 개발 방법론 테일러링 기법

- **프로젝트 규모와 복잡도에 따른 테일러링 기법** : 가장 일반적인 기법으로, 프로젝트 규모를 프로젝트 기간, 작업범위, 참여인원 등에 따라 대 · 중 · 소로 구분하고, 프로젝트 업무의 난이도에 따라 복잡도를 상 · 중 · 하로 구분하는 기법이다.
- **프로젝트 구성원에 따른 테일러링 기법** : 프로젝트에 참여하는 구성원들의 기술적 숙련도와 방법론의 이해 정도를 확인하여 테일러링 수준을 결정하는 기법이다.
- **팀내 방법론 지원에 따른 테일러링 기법** : 프로젝트 수행 시 각 팀별로 방법론 담당 인력을 배정하여 팀의 방법론 교육과 프로젝트 전체의 방법론 운영을 위한 의사소통을 담당하도록 인력을 구성하는 기법이다.
- **자동화에 따른 테일러링 기법** : 프로젝트 수행 시 작업 부하를 줄이기 위해 중간 단계에서의 산출물을 자동화 도구를 사용하여 산출할 수 있도록 지원하는 기법이다.

기출문제 따라잡기 Section 164

출제예상

1. 소프트웨어 개발 방법론 테일러링 작업 시 고려해야 할 내부적 요건에 대한 설명으로 가장 옳지 않은 것은?

① 요구사항 : 프로젝트에서 우선적으로 고려할 요구사항이 서로 다른 경우 테일러링이 필요하다.

② 보유 기술 : 프로세스, 개발 방법론, 산출물 등이 서로 다른 경우 테일러링이 필요하다.

③ 프로젝트 규모 : 비용, 인력, 기간 등 프로젝트의 규모가 서로 다른 경우 테일러링이 필요하다.

④ 표준 품질 기준 : 분야별 표준 품질 기준이 서로 다른 경우 테일러링이 필요하다.

테일러링의 고려사항에는 내부적 요건과 외부적 요건이 있는데, '법적 제약사항'과 '표준 품질 기준'은 외부적 요건에 해당합니다.

출제예상

2. 다음 중 소프트웨어 개발 방법론 테일러링 기법이 아닌 것은?

① 프로젝트 구성원에 따른 테일러링 기법

② 프로젝트 관리에 따른 테일러링 기법

③ 프로젝트 규모와 복잡도에 따른 테일러링 기법

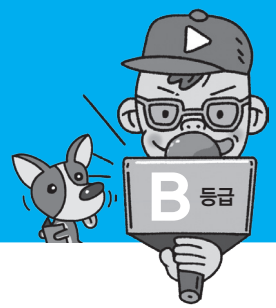
④ 팀내 방법론 지원에 따른 테일러링 기법

소프트웨어 개발 방법론 테일러링 기법 4가지는 '규모와 복잡도, 프로젝트 구성원, 팀내 방법론 지원, 자동화'입니다. 잊지마세요!

▶ 정답 : 1. ④ 2. ②

SECTION
165
LIVE

소프트웨어 개발 프레임워크



전문가의 조언

프레임워크(Framework)는 사전적으로 '뼈대', '골조'를 의미하며, 소프트웨어에서는 특정 기능을 수행하기 위해 필요한 클래스나 인터페이스 등을 모아둔 집합체를 가리킵니다. 소프트웨어 개발 프레임워크의 개념을 숙지하고, 프레임워크들의 개별적인 특징을 잘 구분해서 정리하세요.

반제품

완제품의 재료로 사용되기 위해 원료를 가공하여 만든 중간 제품을 의미합니다.

1 소프트웨어 개발 프레임워크의 개요

프레임워크(Framework)는 소프트웨어 개발에 공통적으로 사용되는 구성 요소와 아키텍처를 일반화하여 손쉽게 구현할 수 있도록 여러 가지 기능들을 제공해주는 반제품* 형태의 소프트웨어 시스템이다.

- 프레임워크의 주요 기능에는 예외 처리, 트랜잭션 처리, 메모리 공유, 데이터 소스 관리, 서비스 관리, 쿼리 서비스, 로깅 서비스, 사용자 인증 서비스 등이 있다.
- 프레임워크의 종류에는 스프링 프레임워크, 전자정부 프레임워크, 닷넷 프레임워크 등이 있다.

2 스프링 프레임워크(Spring Framework)

스프링 프레임워크는 자바 플랫폼을 위한 오픈 소스 경량형 애플리케이션 프레임워크이다.

- 동적인 웹 사이트의 개발을 위해 다양한 서비스를 제공한다.
- 전자정부 표준 프레임워크의 기반 기술로 사용되고 있다.

3 전자정부 프레임워크

전자정부 프레임워크는 우리나라의 공공부문 정보화 사업 시 효율적인 정보 시스템의 구축을 지원하기 위해 필요한 기능 및 아키텍처를 제공하는 프레임워크이다.

- 전자정부 프레임워크는 개발 프레임워크의 표준 정립으로 응용 소프트웨어의 표준화, 품질 및 재사용성의 향상을 목적으로 한다.
- 전자정부 프레임워크는 오픈 소스 기반의 범용화가 되고 공개된 기술을 활용함으로써 특정 업체의 종속성을 배제하고 사업별 공통 컴포넌트의 중복 개발을 방지한다.

4 닷넷 프레임워크(.NET Framework)

닷넷 프레임워크는 Windows 프로그램의 개발 및 실행 환경을 제공하는 프레임워크로, Microsoft 사에서 통합 인터넷 전략을 위해 개발하였다.

- 닷넷 프레임워크는 코드 실행을 관리하는 CLR(Common Language Runtime, 공용 언어 런타임)이라는 이름의 가상머신 상에서 작동한다.
- 닷넷 프레임워크는 메모리 관리, 유형 및 메모리 안전성, 보안, 네트워크 작업 등 여러 가지 서비스를 제공한다.

기출문제 따라잡기 Section 165

출제예상

1. 다음이 설명하고 있는 것은?

> EJB(Enterprise Java Beans) 기반의 복잡함과 무거움을 극복하고 개발 생산성 향상과 고품질의 시스템 개발을 위한 자바 플랫폼 상의 경량화된 오픈 소스 웹 애플리케이션 프레임워크이다.

① 닷넷 프레임워크
② 스프링 프레임워크
③ 전자정부 프레임워크
④ 장고 프레임워크

프레임워크들의 개별적인 특징을 잘 구분해두라고 했는데, 답을 못 찾겠으면 본문을 다시 한 번 공부하고 오세요.

출제예상

2. 다음 중 대한민국의 공공부문 정보화 사업 시 사용하는 플랫폼별 표준화된 개발 프레임워크로서, 응용 소프트웨어의 표준화, 품질 및 재사용성의 향상을 목표로 하는 것은?

① 스프링 프레임워크
② 닷넷 프레임워크
③ 플라스크 프레임워크
④ 전자정부 프레임워크

이 문제는 어렵지 않게 답을 찾을 수 있겠죠.

출제예상

3. 다음 중 마이크로소프트에서 개발한 윈도우 프로그램 개발 및 실행 환경으로, 네트워크 작업, 인터페이스 등의 많은 작업을 캡슐화하였고, 공통 언어 런타임(Common Language Runtime)이라는 이름의 가상머신 위에서 작동하는 프레임워크는?

① .NET Framework
② Django Framework
③ Sprin Framework
④ Flask Framework

마이크로소프트 사의 윈도우와 공통 언어 런타임(CLR)과 관련된 프레임워크하면 닷넷 프레임워크(.NET Framework)! 꼭 기억하세요.

▶ 정답 : 1. ② 2. ④ 3. ①

예·상·문·제·은·행

1. 다음 중 소프트웨어 비용 산정에 대한 설명으로 옳은 것은?

① 소프트웨어 비용을 너무 높게 산정하면 품질 문제가 발생할 수 있다.

② 소프트웨어 비용 산정 기법에는 상향식, 중향식, 하향식 기법이 있다.

③ 소프트웨어 비용 결정 요소에는 프로젝트 요소, 신뢰성 요소, 품질 요소가 있다.

④ 프로젝트 요소에는 제품 복잡도, 시스템 크기, 요구되는 신뢰도가 있다.

2. 다음 중 소프트웨어 비용을 결정할 때 사용되는 프로젝트 요소에 대한 설명으로 옳지 않은 것은?

① 시스템의 크기 : 대형, 소형 등 소프트웨어의 규모에 따라 개발할 시스템의 규모를 의미한다.

② 개발자 능력 : 전문 분야에 대한 지식, 유사 분야에 대한 경험, 응용 분야에 대한 이해도 등을 의미한다.

③ 요구되는 신뢰도 : 정확성, 견고성, 완전성, 일관성 등 프로그램이 일정한 기간 내에 주어진 조건하에서 필요한 기능을 수행하는 정도를 의미한다.

④ 제품의 복잡도 : 응용, 유틸리티, 시스템 소프트웨어 등 소프트웨어의 종류에 따라 달라지는 문제의 난이도를 의미한다.

3. 다음 중 소프트웨어 비용 결정 시 확인하는 자원 요소에 대한 설명으로 옳은 것은?

① 인적 자원은 관리자, 개발자 등의 능력이나 자질을 의미한다.

② 하드웨어 자원은 언어 분석기, 문서화 도구, 요구 분석기 등과 같은 개발 자원 도구를 의미한다.

③ 소프트웨어 자원은 개발 장비, 워드프로세서, 프린터와 같은 보조 장비를 의미한다.

④ 개발 기간은 소프트웨어를 개발하는 기간을 의미한다.

4. 소프트웨어를 개발하는 개발 기간은 소프트웨어 비용 결정 요소 중 어느 요소에 속하는가?

① 프로젝트 요소

② 생산성 요소

③ 자원 요소

④ 품질 요소

5. 다음 중 하향식 비용 산정 기법은?

① LOC 기법

② 개발 단계별 인월수 기법

③ 전문가 감정 기법

④ 수학적 산정 기법

6. 소프트웨어 비용 산정 기법 중 전문가의 감정에 의한 산정 기법에 대한 설명이 아닌 것은?

① 조직 내에 있는 두 명 이상의 핵심 요원으로부터 그의 경험, 배경, 업무 처리 센스에 의존하는 방법이다.

② 새로운 프로젝트와 유사한 프로젝트에 대한 경험이 없을 수 있다.

③ 새로운 프로젝트에는 과거의 것과 상당히 차이 있게 만드는 요소들이 있다는 것을 간과할 수 있다.

④ 객관적으로 산정할 수 있어서 의뢰자로부터 믿음을 얻을 수 있다.

7 소프트웨어 비용 산정 기법 중 산정 요원과 조정자에 의해 산정하는 방법은?

① 델파이 기법 ② 기능 점수 기법

③ LOC 기법 ④ COCOMO 기법

8 원시 코드 라인 수(LOC) 기법에 의하여 예측된 총 라인 수가 30,000라인, 개발에 참여할 프로그래머가 5명, 프로그래머들의 평균 생산성이 월간 300라인일 때 개발에 소요되는 기간은?

① 10개월 ② 15개월 ③ 20개월 ④ 30개월

9. 다음 중 소프트웨어 비용 산정에 이용되는 기법이 아닌 것은?

① COCOMO(COnstructive COst MOdel) 방정식

② 기능 점수(Function Point) 모형

③ 홀스테드 노력 방정식(Halstead Effort Equation)

④ 전문가의 감정과 델파이 기법

10. 비용 예측을 위한 기능 점수 방법에 대한 설명 중 가장 옳지 않은 것은?

① 입력, 출력, 질의, 파일, 인터페이스의 개수로 소프트웨어의 규모를 표현한다.

② 기능 점수는 원시코드의 구현에 이용되는 프로그래밍 언어에 종속적이다.

③ 경험을 바탕으로 단순, 보통, 복잡한 정도에 따라 가중치를 부여한다.

④ 프로젝트의 영향도와 가중치의 합을 이용하여 실질 기능 점수를 계산한다.

해설은 722쪽에 있습니다.

11. COCOMO 모델에 대한 설명으로 옳지 않은 것은?

① Boehm이 제시한 비용 추정 모델이다.

② 비용 추정 단계 및 적용 변수의 구체화 정도에 따라 기본(Basic), 중간(Intermediate), 진보(Advanced)형 모델로 구분할 수 있다.

③ 비용 견적의 강도 분석 및 비용 견적의 유연성이 높아 소프트웨어 개발비 견적에 널리 통용되고 있다.

④ 기본(Basic) 모형은 단순히 소프트웨어의 크기와 개발 모드에 의해서 구해진다.

12. 비용 예측 방법에서 원시 프로그램의 규모에 의한 방법(COCOMO Model) 중 최대형 규모의 트랜잭션 처리 시스템이나 운영체제 등의 소프트웨어를 개발하는 유형은?

① Organic 프로젝트

② Semi-Detached 프로젝트

③ Embedded 프로젝트

④ Sequential 프로젝트

13. 비용 예측 방법에서 원시 프로그램의 규모에 의한 방법 중 트랜잭션 처리 시스템이나 운영체제, 데이터베이스 관리 시스템 등의 30만 라인 이하의 소프트웨어를 개발하는 유형은?

① Organic 프로젝트

② Semi-Detached 프로젝트

③ Embedded 프로젝트

④ Organic, Embedded 프로젝트

14. COCOMO 모델에 의한 비용(Cost) 산정 과정에 해당하지 않는 것은?

① KDSI(or KLOC)를 측정한다.

② UFP(Unadjusted Function Point)를 계산한다.

③ 개발 노력 승수(Development Effort Multipliers)를 결정한다.

④ 비용 산정 유형으로 단순형, 중간형, 임베디드형이 있다.

15. 다음 중 CMMI의 소프트웨어 프로세스 성숙도를 1단계부터 5단계까지 올바르게 나열한 것은?

㉠ 관리	㉡ 최적화	㉢ 초기	㉣ 정량적 관리	㉤ 정의

① ㉠ → ㉡ → ㉢ → ㉣ → ㉤

② ㉢ → ㉤ → ㉠ → ㉡ → ㉣

③ ㉢ → ㉠ → ㉤ → ㉣ → ㉡

④ ㉤ → ㉢ → ㉠ → ㉣ → ㉡

16. 다음 중 CMMI의 소프트웨어 프로세스 성숙도에 대한 설명으로 옳지 않은 것은?

① 초기 단계에서는 작업자의 능력에 따라 성공 여부가 결정된다.

② 관리 단계에서는 조직의 표준 프로세스를 활용하여 업무를 수행한다.

③ 정량적 관리 단계에서는 프로젝트를 정략적으로 관리 및 통제한다.

④ 최적화 단계에서는 프로세스 역량 향상을 위해 지속적으로 프로세스를 개선한다.

17. 다음 중 SPICE의 프로세스 수행 능력 단계를 올바르게 나열한 것은?

㉠ 불완전	㉡ 수행	㉢ 관리
㉣ 확립	㉤ 예측	㉥ 최적화

① ㉠ → ㉡ → ㉢ → ㉣ → ㉤ → ㉥

② ㉠ → ㉤ → ㉡ → ㉢ → ㉥ → ㉣

③ ㉠ → ㉡ → ㉢ → ㉤ → ㉣ → ㉥

④ ㉠ → ㉢ → ㉡ → ㉤ → ㉥ → ㉣

18. 소프트웨어 개발 방법론 테일러링 작업 시 고려사항 중 외부적 요건에 해당하는 것은?

① 요구사항 ② 프로젝트 규모

③ 보유 기술 ④ 표준 품질 기준

19. 다음 중 닷넷 프레임워크에 대한 설명으로 옳지 않은 것은?

① Microsoft 사에서 통합 인터넷 전략을 위해 개발하였다.

② 전자정부 표준 프레임워크의 기반 기술로 사용되었다.

③ Windows 프로그램의 개발 및 실행 환경을 제공하는 프레임워크이다.

④ 코드 실행을 관리하는 CLR(가상머신) 상에서 작동한다.

▶ **정답 :** 1. ④ 2. ② 3. ① 4. ② 5. ③ 6. ④ 7. ① 8. ③ 9. ③ 10. ② 11. ② 12. ③ 13. ② 14. ② 15. ③ 16. ② 17. ① 18. ④ 19. ②

예·상·문·제·은·행·해·설

1. Section 158

① 소프트웨어 비용을 너무 높게 산정하면 예산 낭비와 일의 효율성 저하를 초래할 수 있고, 너무 낮게 선정하면 개발자의 부담이 가중되고 품질 문제가 발생할 수 있다.

② 소프트웨어 비용 산정 기법에는 상향식과 하향식 기법이 있다.

③ 소프트웨어 비용 결정 요소에는 프로젝트 요소, 자원 요소, 생산성 요소가 있다.

2. Section 158

개발자 능력은 소프트웨어 비용 결정 요소 중 생산성 요소에 해당한다.

3. Section 158

② 하드웨어 자원은 소프트웨어 개발 시 필요한 장비와 워드프로세서, 프린터 등의 보조 장비를 의미한다.

③ 소프트웨어 자원은 소프트웨어 개발 시 필요한 언어 분석기, 문서화 도구 등의 개발 지원 도구를 의미한다.

④ 개발 기간은 생산성 요소에 해당한다.

5. Section 159

①, ②, ④번은 상향식 비용 산정 기법에 해당한다.

6. Section 159

전문가의 감정에 의한 기법은 전문가의 주관이 많이 개입될 수 있다.

7 Section 159

- **기능 점수 기법** : 소프트웨어의 기능을 고려하는 FP를 사용하는 기법
- **LOC 기법** : 소프트웨어 각 기능의 원시 코드 라인 수의 비관치, 낙관치, 기대치를 측정하여 예측치를 구하고 이를 이용하여 비용을 산정하는 기법
- **COCOMO 기법** : 원시 프로그램의 규모(LOC, 원시 코드 라인수)에 의한 비용 예측 기법

8. Section 160

- 노력(PM) = LOC/1인당 월평균 생산 라인 수 = 30000/300 = 100
- 개발 기간 = 노력/투입인원 = 100/5명 = 20개월

9. Section 161

홀스테드(Halstead)의 노력 방정식은 코드 생성 후 피연산자와 연산자 수를 더하여 복잡도를 측정하는 데 사용되는 평가척도 중의 하나이다.

10. Section 161

기능 점수는 원시 코드의 구현에 이용되는 프로그래밍 언어에 독립적이다.

11. Section 161

COCOMO는 비용 산정 단계 및 적용 변수의 구체화 정도에 따라 기본(Basic), 중간(Intermediate), 발전(Detailed)형으로 구분할 수 있다.

12. Section 161

- **조직형(Organic Mode)** : 기관 내부에서 개발된 중·소 규모의 소프트웨어로 일괄 자료 처리나 과학 기술 계산용, 비즈니스 자료 처리용으로 5만(50KDSI) 라인 이하의 소프트웨어를 개발하는 유형
- **반분리형(Semi-Detached Mode)** : 조직형과 내장형의 중간형으로 트랜잭션 처리 시스템이나 운영체제, 데이터베이스 관리 시스템 등의 30만(300KDSI) 라인 이하의 소프트웨어를 개발하는 유형
- **내장형(Embedded Mode)** : 최대형 규모의 트랜잭션 처리 시스템이나 운영체제 등의 30만(300KDSI)라인 이상의 소프트웨어를 개발하는 유형

14. Section 161

UFP(Unadhusted Function Point)를 계산하는 것은 기능 점수(Function Point) 모델이다.

16. Section 163

관리 단계에서는 특정한 프로세스 내의 프로세스를 정의 및 수행한다. ②번은 정의 단계에 대한 설명이다.

18. Section 164

소프트웨어 개발 방법론 테일러링 작업 시 고려사항

- **내부적 요건** : 목표 환경, 요구사항, 프로젝트 규모, 보유기술
- **외부적 요건** : 법적 제약사항, 표준 품질 기준

19. Section 165

전자정부 표준 프레임워크의 기반 기술로 사용된 프레임워크는 스프링 프레임워크이다.

2장 IT프로젝트 정보시스템 구축 관리

이 장에서 꼭 알아야 할 키워드 Best 10

1. 네트워크 관련 신기술 **2.** 네트워크 설치 구조 **3.** 스위치 **4.** 경로 제어 프로토콜 **5.** SW 관련 신기술
6. 트래픽 제어 **7.** HW 관련 신기술 **8.** Secure OS **9.** 병행제어 **10.** 데이터 표준화

SECTION 166 ● LIVE

네트워크 관련 신기술

전문가의 조언

문제에 제시된 내용이 무슨 용어를 말하는지 맞힐 수 있을 정도로 학습하세요.

유비쿼터스(Ubiquitous)
유비쿼터스는 라틴어로 '편재하다(보편적으로 존재하다)'라는 의미로, 사용자가 컴퓨터나 네트워크를 의식하지 않고 장소에 상관없이 자유롭게 네트워크에 접속할 수 있는 환경을 의미합니다.

부호 분할 다중 접속(CDMA)
부호 분할 다중 접속이란 주파수나 시간을 모두 공유하면서 각 데이터에 특별한 코드를 부여하는 방식을 말합니다.

GSM(Global System for Mobile communication)
GSM은 유럽전기통신표준협회(ETSI)에서 제정한 디지털 셀룰러 이동통신 시스템의 표준 규격입니다.

1 IoT(Internet of Things, 사물 인터넷)

IoT는 정보 통신 기술을 기반으로 실세계(Physical World)와 가상 세계(Virtual World)의 다양한 사물들을 인터넷으로 서로 연결하여 진보된 서비스를 제공하기 위한 서비스 기반 기술이다.

- 유비쿼터스* 공간을 구현하기 위한 컴퓨팅 기기들이 환경과 사물에 심겨 환경이나 사물 그 자체가 지능화되는 것부터 사람과 사물, 사물과 사물 간에 지능 통신을 할 수 있는 엠투엠(M2M; Machine to Machine)의 개념을 인터넷으로 확장하여 사물은 물론, 현실과 가상 세계의 모든 정보와 상호 작용하는 IoT 개념으로 진화했다.
- IoT의 주요 기술로는 스마트 센싱 기술, 유무선 통신 및 네트워크 인프라 기술, 사물 인터넷 인터페이스 기술, 사물 인터넷을 통한 서비스 기술 등이 있다.
- IoT 기반 서비스는 개방형 아키텍처를 필요로 하기 때문에 정보 공유에 대한 부작용을 최소화하기 위한 정보 보안 기술의 적용이 중요하다.

2 M2M(Machine to Machine, 사물 통신)

M2M은 무선 통신을 이용한 기계와 기계 사이의 통신이다.

- M2M은 변압기 원격 감시, 전기, 가스 등의 원격 검침, 무선 신용카드 조회기, 무선 보안단말기, 버스 운행 시스템, 위치 추적 시스템, 시설물 관리 등을 무선으로 통합하여 상호 작용하는 통신이다.
- M2M은 부호 분할 다중 접속(CDMA)*, GSM*, 무선 데이터 통신 등 다양한 무선 통신망을 사용한다.

3 모바일 컴퓨팅(Mobile Computing)

모바일 컴퓨팅은 휴대형 기기로 이동하면서 자유로이 네트워크에 접속하여 업무를 처리할 수 있는 환경을 말한다.

- 휴대 기기는 소형 대용량화와 저전력화가 진행 중이고 네트워크 기술은 무선으로 고속/대용량의 정보를 처리할 수 있는 기술이 상용화되고 있으므로 모바일 컴퓨팅은 휴대 기기와 네트워크 기술의 진화로도 가능하다.
- 모바일 컴퓨팅의 진화로 기업은 비즈니스 효율을 극대화하여 경쟁력을 확보할 수 있고, 개인은 삶의 질을 향상시킬 수 있다.

4 클라우드* 컴퓨팅(Cloud Computing)

클라우드 컴퓨팅은 각종 컴퓨팅 자원을 중앙 컴퓨터에 두고 인터넷 기능을 갖는 단말기로 언제 어디서나 인터넷을 통해 컴퓨터 작업을 수행할 수 있는 환경을 의미한다.

- 중앙 컴퓨터는 복수의 데이터 센터를 가상화 기술로 통합한 대형 데이터 센터로, 각종 소프트웨어, 데이터, 보안 솔루션 기능 등 컴퓨팅 자원을 보유하고 있다.
- 사용자는 키보드와 모니터, 마우스를 갖추고 통신 포트만 연결하면 업무 수행이 가능하다.
- 클라우드 컴퓨팅이 그리드 컴퓨팅(Grid Computing)과 다른 점은 그리드 컴퓨팅이 수많은 컴퓨터를 하나의 컴퓨터처럼 묶어 분산 처리하는 방식으로 기상 예측이나 우주 문제 등 대규모 연산에 사용된다면, 클라우드 컴퓨팅은 중앙의 대형 데이터 센터의 컴퓨팅 자원을 필요한 이들에게 필요한 순간에 빌려주는 방식이다.

클라우드(구름, Cloud)
클라우드는 네트워크 상에 숨겨진 다양한 기기들이 공유되어 있는 인터넷 환경을 말합니다.

5 모바일 클라우드 컴퓨팅(MCC; Mobile Cloud Computing)

모바일 클라우드 컴퓨팅(MCC)은 클라우드 서비스를 이용하여 소비자와 소비자의 파트너가 모바일 기기로 클라우드 컴퓨팅 인프라를 구성하여 여러 가지 정보와 자원을 공유하는 ICT(Information and Communications Technologies)* 기술을 의미한다.

- 모바일 클라우드 컴퓨팅은 모바일 기기의 기종이나 운영체제(OS) 등과 같은 환경에 구애받지 않고 클라우드의 ICT 자원들을 제약 없이 이용하는 것이 가능하며, 모바일의 이동성과 클라우드 컴퓨팅의 경제성이 결합되어 사업상의 큰 시너지 효과를 불러일으킬 수 있다.

ICT(Information Communication Technology)
ICT는 정보기술과 통신기술을 합한 말로, 정보 · 통신기기의 운영 및 관리에 필요한 소프트웨어 기술과 하드웨어 기술을 이용하여 정보를 수집, 생산, 가공, 활용하는 모든 방법을 통틀어 일컫는 말입니다.

6 인터클라우드 컴퓨팅(Inter-Cloud Computing)

인터클라우드 컴퓨팅은 각기 다른 클라우드 서비스를 연동하거나 컴퓨팅 자원의 동적 할당이 가능하도록 여러 클라우드 서비스 제공자들이 제공하는 클라우드 서비스나 자원을 연결하는 기술을 말한다.

- 인터클라우드 컴퓨팅의 서비스 형태
  - 대등 접속(Peering) : 클라우드 서비스 제공자 간 직접 연계하는 형태
  - 연합(Federation) : 자원 공유를 기본으로 사용 요구량에 따른 동적 자원 할당을 지원함으로써 논리적으로 하나의 서비스를 제공하는 형태
  - 중개(Intermediary) : 서비스 제공자 간의 직간접적인 자원 연계 또는 단일 서비스 제공자를 통한 중개 서비스를 제공하는 형태

7 메시 네트워크(Mesh Network)

메시 네트워크는 차세대 이동통신, 홈네트워킹, 공공 안전 등 특수 목적을 위한 새로운 방식의 네트워크 기술로, 대규모 디바이스의 네트워크 생성에 최적화되어 있다.

블루투스 SIG
블루투스 SIG는 블루투스 기술 표준 개발을 위한 다국적 기업 연합체입니다.

- 2017년 7월 '블루투스 SIG*'에서 메시 네트워크를 지원한다고 발표하면서 주목을 받았다.
- 메시 네트워크는 무선 랜의 한계를 극복하기 위해 라우터들을 기지국으로 활용하여 모든 구간을 동일한 무선망처럼 구성한다. 이를 이용하면 사용자는 와이파이에 접속하는 것처럼 안정적인 네트워크를 사용할 수 있게 된다.
- 메시 네트워크는 수십에서 수천 개의 디바이스가 유기적으로 연결되어 있어야하는 건물 자동화, 센서 네트워크 등 IoT 솔루션에 적합한 기술이다.

8 와이선(Wi-SUN)

스마트 그리드(Smart Grid)
스마트 그리드는 전기의 생산부터 소비까지의 전 과정에 정보통신기술을 접목하여 에너지 효율성을 높이는 지능형 전력망 시스템입니다.

와이선은 스마트 그리드*와 같은 장거리 무선 통신을 필요로 하는 사물 인터넷(IoT) 서비스를 위한 저전력 장거리(LPWA; Low-Power Wide Area) 통신 기술이다.

- 와이선은 짧은 시간 동안 데이터 전송이 빈번한 검침 분야에 유용하며, 낮은 지연 속도, 메시 네트워크 기반 확장성, 펌웨어 업그레이드 용이성 면에서 다른 저전력 장거리 통신 기술에 비해 우월하다.
- 와이선은 2017년 3월 전남 고창군에 도입되면서 주목받았는데, 해당 와이선은 국제표준화단체 IEEE의 802.15.4g 표준을 준수하여 900MHz의 비면허 대역을 활용하였고, 최대 데이터 전송 속도 300kbps로 약 5km까지 전송이 가능하다.

9 NDN(Named Data Networking)

NDN은 콘텐츠 자체의 정보와 라우터 기능만으로 데이터 전송을 수행하는 기술로, 클라이언트와 서버가 패킷의 헤더에 내장되어 있는 주소 정보를 이용하여 연결되던 기존의 IP(Internet Protocol) 망을 대체할 새로운 인터넷 아키텍처로 떠오르고 있다.

- NDN은 콘텐츠 중심 네트워킹(CCN; Content Centric Networking)*과 같은 개념이며, 해시 테이블(Hash Table)*에 기반을 두는 P2P(Peer-to-Peer)* 시스템과 같이 콘텐츠에 담겨 있는 정보와 라우터 기능만으로 목적지를 확정한다.

- **콘텐츠 중심 네트워킹(CCN; Content Centric Networking)** : 인터넷에서 IP 주소에 따른 데이터 전송에서 벗어나 사용자가 요구하는 콘텐츠 중심의 데이터 전달이 가능한 네트워크
- **해시 테이블(Hash Table)** : 레코드를 한 개 이상 보관할 수 있는 Bucket들로 구성된 기억공간
- **P2P(Peer-to-Peer)** : 개인 대 개인이라는 의미를 가지며, 네트워크에서 개인 대 개인이 PC를 이용하여 서로 데이터를 공유하는 방식을 의미

10 NGN(Next Generation Network, 차세대 통신망)

NGN은 ITU-T에서 개발하고 있는 유선망 기반의 차세대 통신망으로, 유선망뿐만 아니라 이동 사용자를 목표로 하며, 이동통신에서 제공하는 완전한 이동성(Full Mobility) 제공을 목표로 개발되고 있다.

- NGN의 배경 개념은 하나의 망이 인터넷처럼 모든 정보와 서비스(음성, 데이터, 비디오와 같은 모든 형식의 미디어)를 패킷으로 압축하여 전송한다는 것이다.
- NGN은 보통 인터넷 프로토콜(Internet Protocol) 기반으로 구축되므로 때때로 '올(all)-IP*'라는 용어 또한 NGN을 향한 변화를 기술하는데 사용되기도 한다.

올(all)-IP
올-IP는 유선 전화망, 무선 망, 패킷 데이터 망 등 기존의 통신망을 모두 IP 기반의 망으로 통합한 차세대 네트워크입니다.

11 SDN(Software Defined Networking, 소프트웨어 정의 네트워킹)

SDN은 네트워크를 컴퓨터처럼 모델링하여 여러 사용자가 각각의 소프트웨어들로 네트워킹을 가상화하여 제어하고 관리하는 네트워크이다.

- SDN 기술은 네트워크 비용 및 복잡성을 해결할 수 있는 기술로 간주되어 기존 네트워킹 기술의 폐쇄형 하드웨어 및 소프트웨어 기술을 개방형으로 변화시키는 미래 인터넷 기술로 떠오르고 있다.

12 NFC(Near Field Communication, 근거리 무선 통신)

NFC는 고주파(HF)를 이용한 근거리 무선 통신 기술이다.

- NFC는 Ecma 340, ISO/IEC 18092 표준으로, 아주 가까운 거리에서 양방향 통신을 지원하는 RFID* 기술의 일종이다.
- NFC는 13.56MHz 주파수를 이용해 10cm 내에서 최고 424Kbps의 속도로 데이터 전송을 지원한다.
- NFC는 모바일 기기를 통한 결제뿐만 아니라 슈퍼마켓이나 일반 상점에서 물품 정보나 방문객을 위한 여행 정보 전송, 교통, 출입 통제, 잠금장치 따위에 광범위하게 활용된다.

RFID(Radio Frequency IDentification)
RFID는 사물에 전자 태그를 부착하고 무선 통신을 이용하여 사물의 정보 및 주변 정보를 감지하는 센서 기술입니다.

13 UWB(Ultra WideBand, 초광대역)

UWB는 짧은 거리에서 많은 양의 디지털 데이터를 낮은 전력으로 전송하기 위한 무선 기술로 무선 디지털 펄스라고도 하며, 블루투스*와 비교되는 기술이다.

- UWB는 0.5m/W 정도의 저전력으로 많은 양의 데이터를 1km의 거리까지 전송할 수 있을 뿐 아니라, 땅 속이나 벽면 뒤로도 전송이 가능하다. 이를 통해 지진 등 재해가 일어났을 때 전파 탐지기 기능으로 인명 구조를 할 수 있는 등 응용 범위도 광범위하다.
- UWB는 1950년대에 미국 국방부가 군사적 목적으로 개발하였으나, 미 연방통신위원회가 2002년 2월 14일 이 기술의 상업적 용도를 승인한 이후 여러 업체에서 제품 개발에 적극적으로 나서 상용화가 빨라지고 있다.

블루투스(Bluetooth)
블루투스는 근거리에서 데이터 통신을 무선으로 가능하게 해주는 기술입니다.

14 피코넷(PICONET)

피코넷은 여러 개의 독립된 통신장치가 블루투스 기술이나 UWB 통신 기술을 사용하여 통신망을 형성하는 무선 네트워크 기술이다.

- 피코넷은 네트워크를 구성하는 장비 간에 사전에 네트워크의 정의와 계획 없이 상황에 따라 조정 프로토콜에 의하여 마스터와 슬레이브의 역할을 하면서 네트워크를 형성한다.
- 피코넷은 주로 수십 미터 이내의 좁은 공간에서 네트워크를 형성하는 것과 정지 또는 이동 중에 있는 장치를 모두 포함한다는 특징을 가지고 있다.

15 WBAN(Wireless Body Area Network)

WBAN은 웨어러블(Wearable) 또는 몸에 심는(Implant) 형태의 센서나 기기를 무선으로 연결하는 개인 영역 네트워킹 기술이다.

- WBAN은 무선 센서나 기기로부터 수집한 정보를 휴대폰 또는 간이형 기지국(Base Station)을 통하여 병원이나 기타의 필요한 곳에 실시간으로 전송함으로써 uHealth 등의 서비스를 받는데 응용할 수 있다.

16 GIS(Geographic Information System, 지리 정보 시스템)

GIS는 지리적인 자료를 수집 · 저장 · 분석 · 출력할 수 있는 컴퓨터 응용 시스템으로, 위성을 이용해 모든 사물의 위치 정보를 제공해 주는 것을 말한다.

- GIS는 지도에서 사물을 확인하는 단계를 벗어나 인터넷, 인공위성 등 다양한 매체를 통해 지리 데이터를 수집 · 구축 · 분석 · 처리 과정을 거쳐 고품질의 공간 정보를 생성함으로써 보다 나은 공간 의사 결정에 도움을 주는 단계에까지 이르고 있다. 예를 들면 자동차에서 자신의 위치와 목적지를 지정하여 최단 거리를 찾을 수도 있다.

17 USN(Ubiquitous Sensor Network, 유비쿼터스 센서 네트워크)

USN은 각종 센서로 수집한 정보를 무선으로 수집할 수 있도록 구성한 네트워크를 말한다. 즉 필요한 모든 것(곳)에 RFID 태그를 부착하고, 이를 통하여 사물의 인식 정보는 물론 주변의 환경정보까지 탐지하여 이를 네트워크에 연결하여 정보를 관리하는 것을 의미한다.

- USN은 사람의 접근이 불가능한 취약지구에 수백 개의 센서 네트워크 노드를 설치하면 사람이 감시하는 것과 같은 효과를 얻을 수 있다.

18 SON(Self Organizing Network, 자동 구성 네트워크)

SON은 주변 상황에 맞추어 스스로 망을 구성하는 네트워크를 말한다.

- SON의 목적은 통신망 커버리지 및 전송 용량 확장의 경제성 문제를 해결하고, 망의 운영과 관리의 효율성을 높이는 것이다.
- SON은 갑작스러운 사용자의 증가나 감소 시에는 자동으로 주변 셀과의 협력을 통해 셀 용량을 변화시키며, 장애가 발생했을 때 자체적인 치유도 가능하다.

19 애드 혹 네트워크(Ad-hoc Network)

애드 혹 네트워크는 재난 현장과 같이 별도의 고정된 유선망을 구축할 수 없는 장소에서 모바일 호스트(Mobile Host)만을 이용하여 구성한 네트워크로, 망을 구성한 후 단기간 사용되는 경우나 유선망을 구성하기 어려운 경우에 적합하다.

- 애드 혹 네트워크는 유선망과 기지국이 필요 없고 호스트의 이동에 제약이 없어 빠른 망 구성과 저렴한 비용이 장점이다.

20 네트워크 슬라이싱(Network Slicing)

네트워크 슬라이싱은 3GPP*를 포함한 여러 글로벌 이동통신 표준화 단체가 선정한 5G(IMT-2020)의 핵심기술 중 하나로, 네트워크에서 하나의 물리적인 코어 네트워크 인프라(Infrastructure)를 독립된 다수의 가상 네트워크로 분리하여 각각의 네트워크를 통해 다양한 고객 맞춤형 서비스를 제공하는 것을 목적으로 하는 네트워크 기술이다.

- 네트워크 슬라이싱이 5G 네트워크에서는 주문형 비디오(VOD)*의 형태로 1인칭 미디어를 포함해 초고선명(UHD)의 동영상, 증강현실(AR) · 가상현실(VR) 콘텐츠, 홀로그램, 자율주행 자동차, 로봇 · 드론 원격 조정 등 다양한 서비스가 제공될 것으로 기대되는데, 이를 1개의 물리적 네트워크로 제공하는 것에는 한계가 있어 네트워크 슬라이싱 기술이 5G 네트워크를 구현하는데 중요한 핵심 기술이 되었다.
- 네트워크 슬라이싱 기술의 구현을 위해서는 소프트웨어 정의 네트워킹(SDN; Software-Defined Networking)*과 네트워크 기능 가상화(NFV; Network Functions Virtualization)* 구현이 선행되어야 한다.

3GPP(3rd Generation Partnership Project)
3GPP는 이동통신 관련 국제 표준을 위해 각국의 통신 관련 기관이 참여하는 기술협력 기구입니다.

주문형 비디오(VOD; Video On Demand)
주문형 비디오는 고객이 원하는 시간에 원하는 내용의 프로그램을 전송 및 재생해주는 시스템입니다.

소프트웨어 정의 네트워킹(SDN; Software-Defined Networking)
소프트웨어 정의 네트워킹은 네트워크에서 제어부와 데이터 전달부를 분리하여 관리자가 소프트웨어를 통해 네트워크를 효율적으로 제어 · 관리할 수 있게 하는 기술입니다.

네트워크 기능 가상화(NFV; Network Functions Virtualization)
네트워크 기능 가상화는 네트워크 구성에 필요한 하드웨어들을 소프트웨어적으로 구현하여 장비를 줄이는 기술입니다.

21 저전력 블루투스 기술(BLE; Bluetooth Low Energy)

저전력 블루투스 기술은 일반 블루투스와 동일한 2.4GHz 주파수 대역을 사용하지만 연결되지 않은 대기 상태에서는 절전 모드를 유지하는 기술이다.

- 저전력 블루투스 기술은 주로 낮은 전력으로 저용량 데이터를 처리하는 시계, 장난감, 비컨(Beacon), 그리고 착용 컴퓨터 등의 극소형 사물 인터넷에 매우 적합하다.
- 저전력 블루투스 기술은 전력 효율이 좋아 배터리 하나로 몇 년을 사용할 수 있으므로 비용면에서도 매우 효율적이다.

22 지능형 초연결망

지능형 초연결망은 과학기술정보통신부 주관으로 추진 중인 사업으로, 스마트 시티, 스마트 스테이션 등 4차 산업혁명 시대를 맞아 새로운 변화에 따라 급격하게 증가하는 데이터 트래픽을 효과적으로 수용하기 위해 시행되는 정부 주관 사업이다.

- 지능형 초연결망은 국가 전체 망에 소프트웨어 정의 기술(SDE)*을 적용하는 방법으로 네트워크의 데이터 트래픽 증가를 불러올 수 있는 사물 인터넷(IoT), 클라우드, 빅데이터, 5G 등을 효율적으로 수용할 수 있도록 한다.
- 지능형 초연결망은 기존의 초고속정보통신망, 광대역통합망(BcN), 광대역융합망(UBcN)을 잇는 중장기 네트워크 발전 전략이다.

소프트웨어 정의 기술(SDE, SDx, Software-Defined Everything)
소프트웨어 정의 기술은 네트워크, 데이터 센터 등에서 소유한 자원을 가상화하여 개별 사용자에게 제공하고, 중앙에서는 통합적으로 제어가 가능한 기술입니다.

출제예상

1. 다음 중 사물 인터넷에 대한 설명으로 옳지 않은 것은?

① IoT(Internet of Things)라고도 한다.
② 사람을 제외한 사물과 공간, 데이터 등을 인터넷으로 서로 연결시켜주는 무선 통신 기술을 의미한다.
③ 스마트 센싱 기술과 무선 통신 기술을 융합하여 실시간으로 데이터를 주고받는 기술이다.
④ 사물 인터넷 기반 서비스는 개방형 아키텍처를 필요로 하기 때문에 정보 공유에 대한 부작용을 최소화하기 위한 정보 보안 기술의 적용이 중요하다.

사물 인터넷은 사람, 사물, 공간, 데이터 등 세상에 존재하는 모든 사물을 인터넷으로 서로 연결시켜주는 무선 통신 기술입니다.

출제예상

2. 다음에서 설명하는 용어는 무엇인가?

- 인터넷 상에서 서버 및 회선, 플랫폼, 소프트웨어 등과 같은 정보기술 자원을 소유하지 않고 서비스 형태로 빌려 쓰는 방식이다.
- 매우 큰 가상화된 컴퓨팅 환경이다.

① 모바일 컴퓨팅(Mobile Computing)
② 분산 컴퓨팅(Distributed Computing)
③ 클라우드 컴퓨팅(Cloud Computing)
④ 그리드 컴퓨팅(Grid Computing)

'가상화된 컴퓨팅 환경, 빌려 쓰는 방식'하면 클라우드 컴퓨팅! 꼭 기억하세요.

출제예상

3. 다음 중 지리적으로 분산되어 있는 컴퓨터 자원을 초고속 인터넷 망을 통해 격자 구조로 연결하여 공유함으로써 하나의 고성능 컴퓨터처럼 사용하는 방법은 어느 것인가?

① 그리드 컴퓨팅(Grid Computing)
② 클라이언트/서버 컴퓨팅(Client/Server Computing)
③ 가상 컴퓨팅(Virtual Computing)
④ 유비쿼터스 컴퓨팅(Ubiquitous Computing)

'격자 무늬'를 'Grid'라고 합니다. 인터넷에 연결된 수많은 컴퓨터를 격자 구조로 모두 연결하여 하나의 컴퓨터처럼 사용할 수 있게 하는 것이 바로 그리드 컴퓨팅(Grid Computing)입니다.

출제예상

4. 다음에서 설명하는 용어로 적합한 것은?

모든 사물에 부착된 RFID 태그 또는 센서를 통해 탐지된 사물의 인식 정보는 물론 주변의 온도, 습도, 위치 정보, 압력, 오염 및 균열 정도 등과 같은 환경 정보를 실시간으로 네트워크와 연결하여 수집하고 관리하는 네트워크 시스템이다.

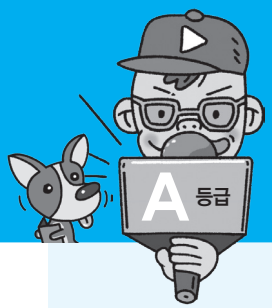
① BT
② VAN
③ USN
④ URI

USN, 벌써 잊은 건 아니죠? 불안하면 다시 한 번 공부하고 오세요.

▶ 정답 : 1. ② 2. ③ 3. ① 4. ③

SECTION 167 LIVE

네트워크 구축



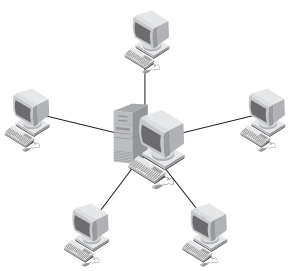
1 네트워크(Network) 설치 구조

통신망(Communication Network)은 정보를 전달하기 위해서 통신 규약에 의해 연결한 통신 설비의 집합이다. 네트워크 설치 구조는 통신망을 구성하는 요소들을 공간적으로 배치하는 방법, 즉 장치들의 물리적 위치에 따라서 성형, 링형, 버스형, 계층형, 망형으로 나누어진다.

2 성형(Star, 중앙 집중형)

성형은 중앙에 중앙 컴퓨터가 있고, 이를 중심으로 단말장치들이 연결되는 중앙 집중식의 네트워크 구성 형태이다.

- 포인트 투 포인트(Point-to-Point) 방식으로 회선을 연결한다.
- 각 단말장치들은 중앙 컴퓨터를 통하여 데이터를 교환한다.
- 단말장치의 추가와 제거가 쉽다.
- 하나의 단말장치가 고장나더라도 다른 단말장치에는 영향을 주지 않지만, 중앙 컴퓨터가 고장나면 전체 통신망의 기능이 정지된다.
- 중앙 집중식이므로 교환 노드의 수가 가장 적다.

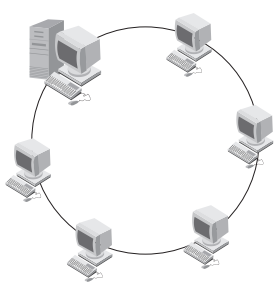


성형

3 링형(Ring, 루프형)

링형은 컴퓨터와 단말장치들을 서로 이웃하는 것끼리 포인트 투 포인트(Point-to-Point) 방식으로 연결시킨 형태이다.

- 분산 및 집중 제어 모두 가능하다.
- 단말장치의 추가/제거 및 기밀 보호가 어렵다.
- 각 단말장치에서 전송 지연이 발생할 수 있다.
- 중계기의 수가 많아진다.
- 데이터는 단방향 또는 양방향*으로 전송할 수 있으며, 단방향 링의 경우 컴퓨터, 단말장치, 통신 회선 중 어느 하나라도 고장나면 전체 통신망에 영향을 미친다.



링형

전문가의 조언

네트워크 설치 형태에 따른 망(Network)들의 개별적인 특징을 그림과 연관지어 확실히 알아두세요.

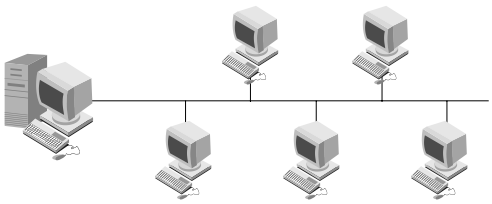
양방향 링

양방향 링은 노드에 이상이 생겼을 경우 다른 방향으로 우회할 수 있으므로, 정상적인 노드들끼리는 통신이 가능합니다.

4 버스형(Bus)

버스형은 한 개의 통신 회선에 여러 대의 단말장치가 연결되어 있는 형태이다.

- 물리적 구조가 간단하고, 단말장치의 추가와 제거가 용이하다.
- 단말장치가 고장나더라도 통신망 전체에 영향을 주지 않기 때문에 신뢰성을 높일 수 있다.
- 기밀 보장이 어렵고, 통신 회선의 길이에 제한이 있다.

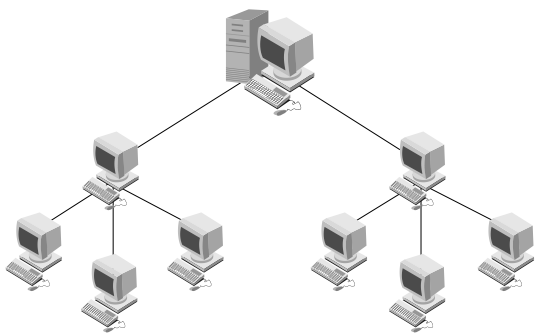


버스형

5 계층형(Tree, 분산형)

계층형은 중앙 컴퓨터와 일정 지역의 단말장치까지는 하나의 통신 회선으로 연결시키고, 이웃하는 단말장치는 일정 지역 내에 설치된 중간 단말장치로부터 다시 연결시키는 형태이다.

- 분산 처리 시스템을 구성하는 방식이다.



계층형

6 망형(Mesh)

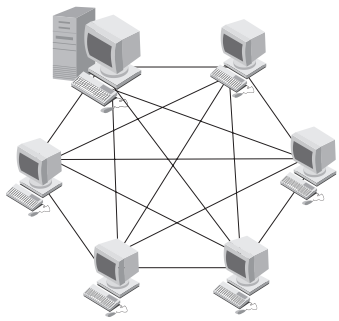
망형은 모든 지점의 컴퓨터와 단말장치를 서로 연결한 형태로, 노드의 연결성이 높다.

- 많은 단말장치로부터 많은 양의 통신을 필요로 하는 경우에 유리하다.
- 보통 공중 데이터 통신망에서 사용되며, 통신 회선의 총 경로가 가장 길다.
- 통신 회선 장애 시 다른 경로를 통하여 데이터를 전송할 수 있다.

• 모든 노드를 망형으로 연결하려면 노드의 수가 n개일 때, n(n−1)/2개의 회선이 필요하고 노드당 n−1개의 포트가 필요하다.

예제 25개의 노드를 망형으로 연결하려고 할 때 필요한 회선의 수와 노드당 필요한 포트의 수는?

회선 수 $= \frac{n(n-1)}{2} = \frac{25(25-1)}{2} = \frac{600}{2} = 300$(개), 포트 수 $= n-1 = 24$(개)



망형

7 네트워크 분류

네트워크는 각 사이트들이 분포되어 있는 지리적 범위에 따라 LAN과 WAN으로 분류된다.

근거리 통신망 (LAN; Local Area Network)	• 회사, 학교, 연구소 등에서 비교적 가까운 거리에 있는 컴퓨터, 프린터, 테이프 등과 같은 자원을 연결하여 구성한다. • 주로 자원 공유를 목적으로 사용한다. • 사이트 간의 거리가 짧아 데이터의 전송 속도가 빠르고, 에러 발생율이 낮다. • 근거리 통신망에서는 주로 버스형이나 링형 구조를 사용한다.
광대역 통신망 (WAN; Wide Area Network)	• 국가와 국가 혹은 대륙과 대륙 등과 같이 멀리 떨어진 사이트들을 연결하여 구성한다. • 사이트 간의 거리가 멀기 때문에 통신 속도가 느리고, 에러 발생률이 높다. • 일정한 지역에 있는 사이트들을 근거리 통신망으로 연결한 후 각 근거리 통신망을 연결하는 방식을 사용한다.

전문가의 조언

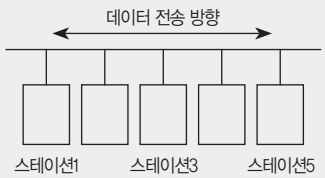
근거리 통신망과 광대역 통신망의 특징을 서로 비교하여 알아두세요.

이전기출
1. 망(Network) 구조의 기본 유형이 아닌 것은?

① 스타형 ② 링형
③ 트리형 ④ 십자형

통신망 구성 형태 5가지 다 외웠죠! 성형(Star), 링형(Ring), 버스형(Bus), 계층형(Tree), 망형(Mesh).

이전기출
2. 다음 LAN의 네트워크 토폴로지는 어떤 형인가?



① 버스형 ② 성형
③ 링형 ④ 트리형

네트워크 구조는 제시된 그림만 자세히 살펴봐도 답을 쉽게 찾을 수 있습니다. 그림이 버스 손잡이 같이 생기지 않았나요?

이전기출
3. 중앙에 호스트 컴퓨터가 있고 이를 중심으로 터미널들이 연결되는 네트워크 구성 형태(Topology)는?

① 버스형(Bus) ② 링형(Ring)
③ 성형(Star) ④ 그물형(Mesh)

중앙에 호스트 컴퓨터가 있고 이를 중심으로 터미널이 연결된 형태를 머릿속으로 그려보세요. 마치 별 모양 같지 않나요?

이전기출
4. 데이터는 한쪽 방향으로만 흐르고 병목 현상이 드물지만, 두 노드 사이의 채널이 고장나면 전체 네트워크가 손상될 수 있는 단점을 가지는 토폴로지는?

① 링형 토폴로지 ② 망형 토폴로지
③ 성형 토폴로지 ④ 계층형 토폴로지

링형에는 단방향 링형과 양방향 링형이 있으며, 데이터가 한쪽 방향으로만 흐르는 단방향 링형의 경우 두 노드 사이의 채널이 고장나면 전체 통신망에 영향을 줍니다.

출제예상
5. 근거리 네트워크의 특징이라고 할 수 없는 것은?

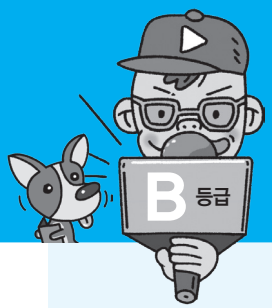
① 데이터의 전송 속도가 빠르다.
② 경영의 융통성을 향상시킬 수 있다.
③ 네트워크 구조는 Mesh형이 많이 사용된다.
④ 자료 및 장비의 공유가 용이하다.

근거리 통신망에서는 링형이나 버스형 구조가 많이 사용됩니다. 참고로 Mesh형은 망형을 의미합니다.

▶ 정답 : 1. ④ 2. ① 3. ③ 4. ① 5. ③

SECTION 168 LIVE

스위치



1 스위치(Switch) 분류

스위치는 브리지와 같이 LAN과 LAN을 연결하여 훨씬 더 큰 LAN을 만드는 장치로, OSI 7 계층의 Layer에 따라 L2, L3, L4, L7으로 분류된다.

L2 스위치	• OSI의 2계층에 속하는 장비이다. • 일반적으로 부르는 스위치는 L2 스위치를 의미한다. • MAC 주소*를 기반으로 프레임*을 전송한다. • 동일 네트워크 간의 연결만 가능하다.
L3 스위치	• OSI의 3계층에 속하는 장비이다. • L2 스위치에 라우터 기능이 추가된 것으로, IP 주소를 기반으로 패킷을 전송한다. • 서로 다른 네트워크 간의 연결이 가능하다.
L4 스위치	• OSI 4계층에 속하는 장비이다. • 로드밸런서*가 달린 L3 스위치로, IP 주소 및 TCP/UDP를 기반으로 사용자들의 요구를 서버의 부하가 적은 곳에 배분하는 로드밸런싱 기능을 제공한다.
L7 스위치	• OSI 7계층에 속하는 장비이다. • IP 주소, TCP/UDP 포트 정보에 패킷 내용까지 참조하여 세밀하게 로드밸런싱한다.

2 스위칭(Switch) 방식

스위치가 프레임을 전달하는 방식에 따라 Store and Forwarding, Cut-through, Fragment Free가 있다.

Store and Forwarding	데이터를 모두 받은 후 스위칭하는 방식
Cut-through	데이터의 목적지 주소만을 확인한 후 바로 스위칭하는 방식
Fragment Free	Store and Forwarding과 Cut-through 방식의 장점을 결합한 방식

3 백본 스위치(Backbone Switch)

여러 네트워크들을 연결할 때 중추적 역할을 하는 네트워크를 백본(Backbone)이라 하고, 백본에서 스위칭 역할을 하는 장비를 백본 스위치라고 한다.

- 백본 스위치는 모든 패킷이 지나가는 네트워크의 중심에 배치한다.
- 대규모 트래픽을 처리하려면 고성능의 백본 스위치를 사용해야 한다.
- 주로 L3 스위치가 백본 스위치의 역할을 한다.

전문가의 조언

이번 섹션에서는 4과목에서 공부한 네트워크 장비 중 스위치에 대해 좀 더 자세히 공부하도록 하겠습니다. 스위치의 기능을 바탕으로 스위치의 분류, 스위칭 방식 등을 숙지해 두세요.

전문가의 조언

상위 레이어의 스위치는 하위 레이어의 스위치의 기능들을 포함합니다. 즉 L4 스위치는 L2, L3의 기능을 갖고 있으며, L7 스위치는 L2~L4의 기능들을 갖고 있죠.

MAC 주소

MAC 주소는 네트워크 어댑터(NIC)의 고유 번호를 말합니다. 네트워크 어댑터는 전세계에 걸쳐 유일한 번호를 가지므로 NIC만으로도 인터넷 상의 컴퓨터를 구분할 수 있습니다.

프레임

L2 스위치에서는 패킷을 프레임이라고 부릅니다.

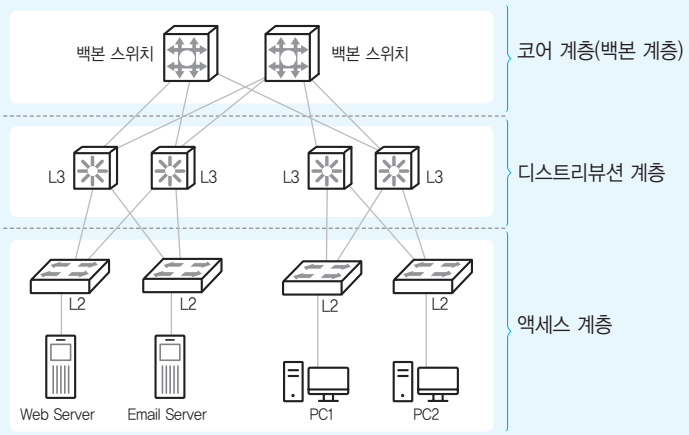
로드밸런서(Load Balancer)

로드밸런서는 특정 서버에만 부하가 발생하지 않도록 트래픽을 분산시켜 주는 장비입니다.

참깐만요 Hierarchical 3 Layer 모델

Hierarchical 3 Layer 모델은 네트워크 구성 시 사용되는 모델의 한 종류로, 액세스 계층, 디스트리뷰션 계층, 코어 계층으로 나뉩니다.

액세스 계층 (Access Layer)	• 사용자가 네트워크에 접속할 때 최초로 연결되는 지점으로, 사용자들로부터 오는 통신을 집약해서 디스트리뷰션 계층으로 전송합니다. • 액세스 계층에 배치되는 장비는 성능은 낮아도 되지만 포트수는 사용자수 만큼 있어야 합니다. • L2 스위치를 사용합니다.
디스트리뷰션 계층 (Distribution Layer)	• 액세스 계층의 장치들이 연결되는 지점으로, 액세스 계층에서 오는 통신을 집약해서 코어 계층으로 전송합니다. • LAN 간에 라우팅 기능을 수행합니다. • 라우터, L3 스위치를 사용합니다.
코어 계층 (Core Layer)	• 디스트리뷰션 계층에서 오는 통신을 집약해 인터넷에 연결하는 계층으로, 백본 계층이라고도 합니다. • 전자우편, 인터넷 접속, 화상 회의 등의 기능을 수행합니다. • 백본 스위치를 사용합니다.



따라잡기 기출문제 따라잡기 Section 168

출제예상

1. L4 스위치의 기능이 아닌 것은?

① 로드밸런싱 기능을 제공한다.
② TCP/UDP를 기반으로 트래픽을 분류한다.
③ 패킷 내용을 참조하여 트래픽을 분배한다.
④ 사용자 요구를 서버의 부하 분배 상태에 따라서 배분한다.

패킷 내용까지 참조할 수 있는 스위치는 L7 스위치입니다.

출제예상

2. Hierarchical 3 Layer 모델에 대한 설명으로 틀린 것은?

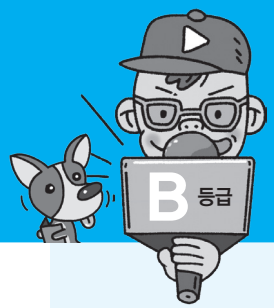
① 액세스 계층, 디스트리뷰션 계층, 코어 계층으로 분류된다.
② 액세스 계층은 사용자가 네트워크에 최초로 연결되는 지점이다.
③ 디스트리뷰션 계층은 백본 계층이라고도 한다.
④ 코어 계층은 인터넷에 연결하는 계층이다.

코어 계층을 백본 계층이라고도 합니다.

▶ 정답 : 1. ③ 2. ③

SECTION 169 ● LIVE

경로 제어 / 트래픽 제어



1 경로 제어(Routing)의 개요

경로 제어는 송 · 수신 측 간의 전송 경로 중에서 최적 패킷 교환 경로를 결정하는 기능이다.

- 최적 패킷 교환 경로란 어느 한 경로에 데이터의 양이 집중하는 것을 피하면서, 최저의 비용으로 최단 시간에 송신할 수 있는 경로를 의미한다.
- 경로 제어는 경로 제어표(Routing Table)*를 참조해서 이루어지며, 라우터*에 의해 수행된다.
- **경로 제어 요소** : 성능 기준, 경로의 결정 시간과 장소, 정보 발생지, 경로 정보의 갱신 시간

2 경로 제어 프로토콜(Routing Protocol)

경로 제어 프로토콜이란 효율적인 경로 제어를 위해 네트워크 정보를 생성, 교환, 제어하는 프로토콜을 총칭한다.

- 대표적인 경로 제어 프로토콜에는 IGP, EGP, BGP가 있다.

IGP(Interior Gateway Protocol, 내부 게이트웨이 프로토콜)	• 하나의 자율 시스템(AS)* 내의 라우팅에 사용되는 프로토콜이다. • RIP(Routing Information Protocol) – 현재 가장 널리 사용되는 라우팅 프로토콜이다. – 소규모 동종의 네트워크(자율 시스템, AS) 내에서 효율적인 방법이다. – 최대 홉(Hop)* 수를 15로 제한하므로 15 이상의 경우는 도달할 수 없는 네트워크를 의미하는데 이것은 대규모 네트워크에서는 RIP를 사용할 수 없음을 의미한다. – 라우팅 정보를 30초마다 네트워크 내의 모든 라우터에 알리며, 180초 이내에 새로운 라우팅 정보가 수신되지 않으면 해당 경로를 이상 상태로 간주한다. • OSPF(Open Shortest Path First protocol) – 대규모 네트워크에서 많이 사용되는 라우팅 프로토콜이다. – 라우팅 정보에 변화가 생길 경우, 변화된 정보만 네트워크 내의 모든 라우터에 알린다.
EGP(Exterior Gateway Protocol, 외부 게이트웨이 프로토콜)	자율 시스템(AS) 간의 라우팅, 즉 게이트웨이 간의 라우팅에 사용되는 프로토콜이다.
BGP(Border Gateway Protocol)	• 자율 시스템(AS) 간의 라우팅 프로토콜로, EGP의 단점을 보완하기 위해 만들어졌다. • 초기에 BGP 라우터들이 연결될 때에는 전체 경로 제어표(라우팅 테이블)를 교환하고, 이후에는 변화된 정보만을 교환한다.

전문가의 조언

인터넷이 확산되면서 네트워크 간 경로 제어의 중요성이 날로 커지고 있습니다. 경로 제어의 의미와 경로 제어 요소, 경로 설정 프로토콜을 기억하세요.

경로 제어표(Routing Table)
경로 제어표는 일반적으로 라우팅 테이블이라고 하며, 다음 홉 주소, 메트릭(Metric), 목적지(수신지) 주소가 저장됩니다.

라우터(Router)
라우터는 하나의 도메인에 속하는 네트워크와 네트워크를 연결하고, 데이터 전송의 최적 경로를 선택하는 기능을 하는 장치입니다.

자율 시스템(AS; Autonomous System)
자율 시스템은 하나의 도메인에 속하는 라우터들의 집합을 말합니다. 그러므로 하나의 자율 시스템에 속한다는 것은 하나의 도메인에 속한다는 것과 같은 의미입니다.

홉(Hop)
홉이란 데이터가 목적지까지 전달되는 과정에서 거치는 네트워크의 수를 의미합니다. 예를 들어, 어떤 목적지까지의 홉이 3이라면, 그 목적지까지 가기 위해서는 세 개의 네트워크를 경유함을 의미합니다.

전문가의 조언

트래픽 제어 방법에는 어떤 것들이 있는지 기억하고, 흐름 제어의 기능과 제어 방식은 자세히 알아두세요.

3 트래픽 제어(Traffic Control)의 개요

트래픽 제어는 네트워크의 보호, 성능 유지, 네트워크 자원의 효율적인 이용을 위해 전송되는 패킷의 흐름 또는 그 양을 조절하는 기능으로 흐름 제어, 폭주(혼합) 제어, 교착상태 방지 기법이 있다.

4 흐름 제어(Flow Control)

흐름 제어

수신 측에서는 수신된 데이터를 버퍼에 저장한 후 순차적으로 처리해서 상위 계층으로 전달하는데, 송신 측의 속도가 수신 측보다 빠르면 수신된 데이터양이 제한된 버퍼를 초과할 수 있으며, 이로 인해 이후 수신 데이터가 손실될 수 있습니다. 이러한 상황은 송신 측과 수신 측의 전송 속도를 적절히 조절하여 예방할 수 있는데 이것을 흐름 제어라고 합니다.

흐름 제어*란 네트워크 내의 원활한 흐름을 위해 송 · 수신 측 사이에 전송되는 패킷의 양이나 속도를 규제하는 기능이다.

- 송신 측과 수신 측 간의 처리 속도 또는 버퍼 크기의 차이에 의해 생길 수 있는 수신 측 버퍼의 오버플로(Overflow)를 방지하기 위한 기능이다.

정지-대기 (Stop-and-Wait)	• 수신 측의 확인 신호(ACK)를 받은 후에 다음 패킷을 전송하는 방식이다. • 한 번에 하나의 패킷만을 전송할 수 있다.
슬라이딩 윈도우 (Sliding Window)	• 확인 신호, 즉 수신 통지를 이용하여 송신 데이터의 양을 조절하는 방식이다. • 수신 측의 확인 신호를 받지 않더라도 미리 정해진 패킷의 수만큼 연속적으로 전송하는 방식으로, 한 번에 여러 개의 패킷을 전송할 수 있어 전송 효율이 좋다. • 송신 측은 수신 측으로부터 확인 신호(ACK) 없이도 보낼 수 있는 패킷의 최대치를 미리 약속받는데, 이 패킷의 최대치가 윈도우 크기(Window Size)를 의미한다. • 윈도우 크기(Window Size)는 상황에 따라 변한다. 즉, 수신 측으로부터 이전에 송신한 패킷에 대한 긍정 수신 응답(ACK)이 전달된 경우 윈도우 크기는 증가하고, 수신 측으로부터 이전에 송신한 패킷에 대한 부정 수신 응답(NAK)이 전달된 경우 윈도우 크기는 감소한다.

5 폭주(혼잡) 제어(Congestion Control)

폭주 제어

송신 측에서 전송한 데이터는 수신 측에 도착할 때까지 여러 개의 라우터를 거치는데, 데이터의 양이 라우터가 처리할 수 있는 양을 초과하면 초과된 데이터는 라우터가 처리하지 못합니다. 송신 측에서는 라우터가 처리하지 못한 데이터를 손실 데이터로 간주하고 계속 재전송하게 되므로 네트워크는 더욱 더 혼잡하게 됩니다. 이러한 상황은 송신 측의 전송 속도를 적절히 조절하여 예방할 수 있는데 이것을 폭주 제어라고 합니다.

흐름 제어(Flow Control)가 송 · 수신 측 사이의 패킷 수를 제어하는 기능이라면, 폭주 제어*는 네트워크 내의 패킷 수를 조절하여 네트워크의 오버플로(Overflow)를 방지하는 기능을 한다.

느린 시작 (Slow Start)	• 윈도우의 크기를 1, 2, 4, 8, …과 같이 2배씩 지수적으로 증가시켜 초기에는 느리지만 갈수록 빨라진다. • 전송 데이터의 크기가 임계 값에 도달하면 혼잡 회피 단계로 넘어간다.
혼잡 회피 (Congestion Avoidance)	느린 시작(Slow Start)의 지수적 증가가 임계 값에 도달되면 혼잡으로 간주하고 회피를 위해 윈도우의 크기를 1씩 선형적으로 증가시켜 혼잡을 예방하는 방식이다.

6 교착상태(Dead Lock) 방지

교착상태란 교환기 내에 패킷들을 축적하는 기억 공간이 꽉 차 있을 때 다음 패킷들이 기억 공간에 들어가기 위해 무한정 기다리는 현상을 말한다.

- 패킷이 같은 목적지를 갖지 않도록 할당하고, 교착상태 발생 시에는 교착상태에 있는 한 단말장치를 선택하여 패킷 버퍼를 폐기한다.

따라잡기

기출문제 따라잡기 Section 169

이전기출
1. 다음 중 IP의 라우팅 프로토콜이 아닌 것은?

① IGP ② RIP
③ EGP ④ HDLC

라우팅 프로토콜의 종류만 알면 풀 수 있는 문제네요. 각각의 기능도 다시 한 번 생각해 보세요.

이전기출
2. 흐름 제어에서 한 번에 여러 개의 프레임을 나누어 전송할 경우 효율적인 기법은?

① 정지 및 대기 ② 슬라이딩 윈도우
③ 다중 전송 ④ 적응적 ARQ

정지 및 대기는 한 번에 하나의 프레임(패킷)을 전송하고, 슬라이딩 윈도우는 한 번에 여러 개의 프레임을 전송할 수 있습니다.

이전기출
3. 외부 라우팅 프로토콜로서 AS(Autonomous System) 간의 라우팅 테이블을 전달하는데 주로 이용되는 것은?

① BGP(Border Gateway Protocol)
② RIP(Routing Information Protocol)
③ OSPF(Open Shortest Path First)
④ EGP(Exterior Gateway Protocol)

AS(Autonomous System), 즉 자율 시스템 간의 라우팅 프로토콜에는 EGP와 BGP가 있었죠. 이 중에서 라우팅 테이블을 전달하는데 주로 이용되는 것은?

이전기출
4. 다음이 설명하고 있는 라우팅 프로토콜은?

- 내부 라우팅 프로토콜이며 링크 상태 알고리즘을 사용하는 대규모 네트워크에 적합하다.
- IGP의 한계를 극복하기 위해 IETF에서 고안한 것으로 네트워크의 변화가 있을 때만 갱신하므로 대역을 효과적으로 사용할 수 있다.

① BGP ② IGP
③ OSPF ④ EGP

라우팅 프로토콜(~GP; ~ Gateway Protocol)은 크게 Interior(내부, IGP)와 Exterior(외부, EGP) 그리고 외부의 단점을 보완한 Border(경계, BGP)로 구분합니다. 그리고 내부에는 RIP과 OSPF가 있죠? 내부의 종류를 구분하는 기준은 규모인데, 혼동되면 글자 수를 규모와 연관지어서 기억해 보세요. RIP(소규모), OSPF(대규모).

▶ 정답 : 1. ④ 2. ② 3. ① 4. ③

SECTION 170 ● LIVE

SW 관련 신기술

전문가의 조언

문제에 제시된 내용이 무슨 용어를 말하는지 맞힐 수 있을 정도로 학습하세요.

1 인공지능(AI; Artificial Intelligence)

인공지능(AI)은 인간의 두뇌와 같이 컴퓨터 스스로 추론, 학습, 판단 등 인간지능적인 작업을 수행하는 시스템이다.

- 인공지능은 인간 상호 간의 지능적 인식을 기반으로 행동하도록 컴퓨터가 만들어질 수 있는 가능성을 추구하는 분야로, 기존의 프로그래밍 순서에 따라 작업하는 컴퓨터 시스템과는 달리 좀 더 유연한 문제 해결을 지원하는데 공헌하고 있다.
- 인공지능의 응용 분야에는 신경망, 퍼지, 패턴 인식, 전문가 시스템, 자연어 인식, 이미지 처리, 컴퓨터 시각, 로봇 공학 등이 있다.
- 인공지능의 개발 언어로는 리스프(LISP), 프롤로그(PROLOG) 등이 있다.

2 뉴럴링크(Neuralink)

뉴럴링크는 미국의 전기자동차 회사 테슬라(Tesla)의 CEO 일론 머스크(Elon Musk)가 사람의 뇌와 컴퓨터를 결합하는 기술을 개발하기 위해 2017년 3월 설립한 회사이다.

- 뉴럴링크가 개발하고 있는 기술은 '신경 레이스(Neural Lace)'로, 작은 전극을 뇌에 이식함으로써 생각을 업로드하고 다운로드하는 것을 목표로 삼고 있다. 또한 머스크는 '피질 직결 인터페이스(Direct Cortical Interface)'라는 개념을 제안했는데, 이는 사람이 인공지능(AI)에 대항할 수 있는 더 높은 수준의 기능에 도달하도록 컴퓨터와 뇌를 연결한다는 개념이다.

3 딥 러닝(Deep Learning)

딥 러닝은 인간의 두뇌를 모델로 만들어진 인공 신경망(ANN; Artificial Neural Network)을 기반으로 하는 기계 학습 기술이다.

- 딥 러닝은 많은 데이터를 이용한 컴퓨터가 마치 사람처럼 스스로 학습할 수 있어 특정 업무를 수행할 때 정형화된 데이터를 입력받지 않고 스스로 필요한 데이터를 수집 · 분석하여 고속으로 처리할 수 있다.

4 전문가 시스템(Expert System)

전문가 시스템은 의료 진단 등과 같은 특정 분야의 전문가가 수행하는 고도의 업무를 지원하기 위한 컴퓨터 응용 프로그램이다.

- 전문가 시스템은 인간의 지적 활동과 경험을 통해서 축적된 전문가의 지식과 전문가에 의해 정의된 추론 규칙을 활용하여 결정을 내리거나 문제를 해결한다.

- 인간 전문가가 사실에 근거한 지식과 추론 능력을 활용하여 문제를 해결하는 것과 같이, 전문가 시스템에는 지식 베이스(Knowledge Base)라는 데이터베이스와 지식 베이스에 기초하여 추론을 실행하는 추론 기구(Inference Engine)가 구성 요소에 포함되어 있다. 지식 베이스는 제목에 관한 구체적 사실과 규칙을 제공하고 추론 기구는 전문가 시스템이 결론을 도출할 수 있도록 하는 추론 능력을 제공한다.

5 증강현실(AR; Augmented Reality)

증강현실(AR)은 실제 촬영한 화면에 가상의 정보를 부가하여 보여주는 기술로, 혼합현실(MR; Mixed Reality)이라고도 부른다.

- 증강현실은 편리할 뿐만 아니라 감성적 측면에서의 만족도도 대단히 높기 때문에 방송은 물론 게임, 교육, 오락, 패션 등 다양한 분야에서 응용이 가능하다.*
- 모바일에서는 증강현실이 위치 기반 서비스(LBS)* 분야에 활발히 이용되고 있다.

6 블록체인(Blockchain)

블록체인은 P2P* 네트워크를 이용하여 온라인 금융 거래 정보를 온라인 네트워크 참여자(Peer)의 디지털 장비에 분산 저장하는 기술을 의미한다.

- 블록체인은 P2P 네트워크 환경을 기반으로 일정 시간 동안 반수 이상의 디지털 장비에 저장된 거래 내역을 서로 교환 · 확인 · 승인하는 과정을 거쳐 디지털 서명으로 동의한 금융 거래 내역만 하나의 블록으로 만든다. 이렇게 생성된 블록은 기존의 블록체인에 연결되고 다시 복사되어 각 사용자의 디지털 장비에 분산 저장된다.
- 블록체인은 기존 금융 회사들이 사용하고 있는 중앙 집중형 서버에 거래 정보를 저장할 필요가 없어 관리 비용이 절감되고, 분산 저장으로 인해 해킹이 어려워짐에 따라 보안 및 거래 안전성도 향상된다.
- 비트 코인(Bitcoin)이 블록체인의 가장 대표적인 예이며, 주식 · 부동산 거래 등 다양한 금융거래에 사용이 가능하고, 현관 키 등의 보안과 관련된 분야에도 활용될 수 있어 크게 주목받고 있다.

7 분산 원장 기술(DLT; Distributed Ledger Technology)

분산 원장 기술(DLT)은 중앙 관리자나 중앙 데이터 저장소가 존재하지 않고 P2P 망 내의 참여자들에게 모든 거래 목록이 분산 저장되어 거래가 발생할 때마다 지속적으로 갱신되는 디지털 원장을 의미한다.

- 대표적인 사례로 블록체인(Blockchain)이 있으며, 2016년부터 많은 은행과 금융회사들이 분산 원장 기술에 주목하여 투자하고 있다.
- DLT는 기존의 중앙 서버와 같이 집중화된 시스템을 유지 및 관리할 필요가 없고, 해킹 및 위변조의 위험도도 낮기 때문에 효율성과 보안성 면에서 크게 유리하다.

증강현실 사용 예

- 스포츠 중계 시 등장 선수의 소속 국가나 정보를 보여주거나, 화장한 자신의 모습을 미리 보고, 옷을 가상으로 입어보고 구매할 수 있습니다.
- 스마트폰으로 거리를 비추면 커피숍이나 약국 등의 정보가 화면에 부가적으로 표시됩니다.

위치 기반 서비스(LBS; Location Based Service)

위치 기반 서비스는 통신 기술과 GPS, 그리고 컴퓨터에 저장된 데이터베이스를 이용하여 주변의 위치와 부가 서비스를 제공하는 기술로, 위치 정보, 실시간 교통 정보 등 다양한 서비스를 제공합니다.

P2P(Peer-to-Peer)

P2P는 개인 대 개인이라는 의미를 가지며, 네트워크에서 개인 대 개인이 PC를 이용하여 서로 데이터를 공유하는 방식을 의미합니다.

8 해시(Hash)

해시는 임의의 길이의 입력 데이터나 메시지를 고정된 길이의 값이나 키로 변환하는 것을 말한다.

- 해시는 데이터의 암호화가 아닌 무결성을 검증하기 위한 방법으로 사용된다.
- 해시는 대칭 · 비대칭 암호화 기법과 함께 사용되어 전자화폐, 전자서명 등의 다양한 방면에서 활용되고 있다.

9 양자 암호키 분배(QKD; Quantum Key Distribution)

양자 암호키 분배(QKD)는 양자 통신을 위해 비밀키를 분배하여 관리하는 기술로, 두 시스템이 암호 알고리즘 동작을 위한 비밀키를 안전하게 공유하기 위해 양자 암호키 분배 시스템을 설치하여 운용하는 방식으로 활용된다.

- 양자 암호키 분배는 키 분배를 위해 얽힘(Entanglement) 상태* 광자 또는 단일 광자를 이용하는 방법을 사용한다.

얽힘(Entanglement) 상태
얽힘 상태란 광자나 원자 등이 양자역학적으로 상관관계를 맺고 있는 상태를 말합니다.

10 프라이버시 강화 기술(PET; Privacy Enhancing Technology)

프라이버시 강화 기술(PET)은 개인정보 위험 관리 기술이다.

- PET는 최근 심각한 위험으로 대두되고 있는 개인정보 침해 위험을 관리하기 위한 핵심 기술로, 암호화, 익명화 등 개인정보를 보호하는 기술에서 사용자가 직접 개인정보를 통제하기 위한 기술까지 다양한 사용자 프라이버시 보호 기술을 통칭한다.

11 디지털 저작권 관리(DRM; Digital Rights Management)

디지털 저작권 관리(DRM)는 인터넷이나 기타 디지털 매체를 통해 유통되는 데이터의 저작권을 보호를 위해 데이터의 안전한 배포를 활성화하거나 불법 배포를 방지하기 위한 시스템이다.

- DRM 시스템은 보통 데이터를 암호화하여 인증된 사용자만이 접속할 수 있게 하거나, 디지털 워터마크*의 사용 또는 이와 유사한 방식으로 콘텐츠를 제작하여 콘텐츠가 제한 없이 보급되지 않도록 한다.

디지털 워터마크 (Digital Watermark)
디지털 워터마크는 사진이나 동영상 등 디지털 데이터에 대해 저작권 정보를 식별할 수 있도록 만든 디지털 이미지나 비트 패턴을 말합니다.

12 공통 평가 기준(CC; Common Criteria)

공통 평가 기준(CC)은 1999년 6월 8일 ISO 15408 표준으로 채택된 정보 보호 제품 평가 기준이다.

- 공통 평가 기준은 정보화 순기능 역할을 보장하기 위해 정보화 제품의 정보보호 기능과 이에 대한 사용 환경 등급을 정한 기준이다.

- 정보 보호 시스템에 대한 공통 평가 기준은 나라마다 서로 다른 평가 기준으로 인해 발생하는 시간과 비용 낭비 등의 문제점을 없애기 위해 개발하기 시작하여 1998년에는 미국, 캐나다, 영국, 프랑스, 독일 간에 상호 인정 협정이 체결되었다.
- 공통 평가 기준은 제1부 시스템의 평가 원칙과 평가 모델, 제2부 시스템 보안 기능 요구사항(11개), 제3부 시스템의 7등급 평가를 위한 보증 요구사항(8개)으로 되어 있다.

13 개인정보 영향평가 제도(PIA; Privacy Impact Assessment)

개인정보 영향평가 제도(PIA)는 개인 정보를 활용하는 새로운 정보시스템의 도입 및 기존 정보시스템의 중요한 변경 시 시스템의 구축 · 운영이 기업의 고객은 물론 국민의 사생활에 미칠 영향에 대해 미리 조사 · 분석 · 평가하는 제도이다.

- PIA는 개인정보의 침해 위험성을 사전에 발견해 정보시스템 구축 및 운영에서 시행 착오를 예방하고 효과적인 대응책을 수립하기 위하여 도입되었으며, 개인정보보호법에 의하여 공공기관은 의무화되어 있다.

14 그레이웨어(Grayware)

그레이웨어는 소프트웨어를 제공하는 입장에서는 악의적이지 않은 유용한 소프트웨어라고 주장할 수 있지만 사용자 입장에서는 유용할 수도 있고 악의적일 수도 있는 애드웨어*, 트랙웨어*, 기타 악성 코드나 악성 공유웨어를 말한다.

- 그레이웨어는 정상적인 소프트웨어의 이미지인 백색과 악성 소프트웨어의 이미지인 흑색의 중간에 해당한다고 하여 이러한 명칭으로 불리게 되었다.

애드웨어(Adware)
애드웨어는 소프트웨어 자체에 광고를 포함하여 이를 보는 대가로 무료로 사용하는 소프트웨어입니다.

트랙웨어(Trackware)
트랙웨어는 적절한 사용자 동의 없이 사용자 정보를 수집하는 프로그램으로 스파이웨어(Spyware)라고도 불립니다.

15 매시업(Mashup)

매시업은 웹에서 제공하는 정보 및 서비스를 이용하여 새로운 소프트웨어나 서비스, 데이터베이스 등을 만드는 기술이다. 즉 다수의 정보원이 제공하는 콘텐츠를 조합하여 하나의 서비스로 제공하는 웹 사이트 또는 애플리케이션을 말한다.

- 구글 지도에 부동산 매물 정보를 결합한 구글의 하우징맵스(HousingMaps)가 대표적인 매시업이다.

16 리치 인터넷 애플리케이션(RIA; Rich Internet Application)

리치 인터넷 애플리케이션(RIA)은 플래시 애니메이션 기술과 웹 서버 애플리케이션 기술을 통합하여 기존 HTML 보다 역동적이고 인터랙티브한 웹페이지를 제공하는 신개념의 플래시 웹페이지 제작 기술이다.

- RIA는 다양한 컴포넌트가 추가된 플래시(Flash)와 플렉스(Flex) 같은 멀티미디어 도구와 데이터베이스가 연동되는 단일 인터페이스를 통해 기존의 웹에서는 볼 수 없었던 다이나믹하고 편리한 고객 중심의 웹페이지를 제공한다.

- RIA는 2001년 매크로 미디어사가 플래시 MX 저작툴을 통해 처음 선보인 이후 쇼핑몰이나 대고객 웹서비스, 포털 등을 중심으로 널리 확산되고 있다.
- MS의 원격스크립팅, SUN의 자바, 매크로미디어의 X-인터넷, AJAX 등도 RIA로 통칭되고 있다.

17 시맨틱 웹(Semantic Web)

시맨틱 웹은 컴퓨터가 사람을 대신하여 정보를 읽고 이해하고 가공하여 새로운 정보를 만들어 낼 수 있도록 이해하기 쉬운 의미를 가진 차세대 지능형 웹이다.

- 예를 들면, 휴가 계획을 짜기 위하여 웹상에 있는 여행 정보를 일일이 직접 찾아서 비행기와 호텔을 예약하는 대신에 자동화된 프로그램에 대략적 휴가 일정과 개인의 선호도를 알려주면 웹상의 정보를 해독하여 세부 일정과 여행에 필요한 예약이 이루어지는 것과 같은 원리이다.
- 시맨틱 웹을 구성하는 핵심 기술로는 웹 자원(Resource)을 서술하기 위한 자원 서술 기술, 온톨로지(Ontology)*를 통한 지식 서술 기술, 통합적으로 운영하기 위한 에이전트(Agent) 기술들을 들 수 있다.

온톨리지(Ontology)
온톨리지는 인간뿐만 아니라 컴퓨터도 정보를 이해할 수 있도록 해주는 개념화 명세로서, 단어와 관계들로 구성된 일종의 사전을 의미합니다.

18 증발품(Vaporware)

증발품은 판매 계획 또는 배포 계획은 발표되었으나 실제로 고객에게 판매되거나 배포되지 않고 있는 소프트웨어이다.

- 증발품은 새로운 소프트웨어의 판매나 배포 계획을 발표해 놓고 실제로 그 제품을 내놓지 못하거나 지연시키고 있는 것을 풍자하여 일컫는 말이다.

19 오픈 그리드 서비스 아키텍처(OGSA; Open Grid Service Architecture)

오픈 그리드 서비스 아키텍처(OGSA)는 애플리케이션 공유를 위한 웹 서비스를 그리드* 상에서 제공하기 위해 만든 개방형 표준이다.

- OGSA는 IBM을 비롯해 수백여 기업이 회원으로 가입해 있는 글로벌 그리드 포럼이 개발을 주도하고 있으며, 웹 서비스 표준을 적극적으로 따르고 기존의 웹 개발 툴들을 그대로 사용할 수 있다는 장점이 있다.

그리드(Grid)
그리드는 한 번에 한 곳만 연결할 수 있던 기존의 웹(WWW)과는 달리 동시에 여러 곳에 연결할 수 있는 인터넷 망 구조입니다.

20 서비스 지향 아키텍처(SOA; Service Oriented Architecture)

서비스 지향 아키텍처(SOA)는 기업의 소프트웨어 인프라인 정보시스템을 공유와 재사용이 가능한 서비스 단위나 컴포넌트 중심으로 구축하는 정보기술 아키텍처이다.

- SOA는 정보를 누구나 이용 가능한 서비스로 간주하고 연동과 통합을 전제로 아키텍처를 구축해 나간다.
- SOA의 대표적인 예인 단순 객체 접근 프로토콜(SOAP) 기반의 웹서비스에서는

서로 다른 이용자들이 서로 다른 방식으로 서비스와 의사소통을 하면서도 통합 관리되는 서비스들을 사용할 수 있다.

- 1996년 컨설팅 업체 가트너가 처음 소개한 것으로, 기업의 IT 시스템을 비즈니스에 맞춰 유연하게 사용할 수 있다는 것이 장점이다.
- SOA는 기존 개념에 이벤트 기반 아키텍처(EDA; Event Driven Architecture)를 더해 비즈니스에서 발생하는 각각의 상황을 실시간으로 처리하는 개념인 SOA 2.0을 도입하고 있다.

21 서비스형 소프트웨어(SaaS; Software as a Service)

서비스형 소프트웨어(SaaS)는 소프트웨어의 여러 기능 중에서 사용자가 필요로 하는 서비스만 이용할 수 있도록 한 소프트웨어이다.

- SaaS는 소프트웨어 유통 방식의 근본적인 변화를 설명하는 개념으로, 공급업체가 하나의 플랫폼을 이용해 다수의 고객에게 소프트웨어 서비스를 제공하고, 사용자는 이용한 만큼 돈을 지급한다.
- 전통적 소프트웨어 비즈니스 모델과 비교할 때 SaaS의 가장 큰 차이점은 제품 소유의 여부다. 기존 기업용 소프트웨어는 기업 내부의 서버 등 장비에 저장해 이용한다는 점에서 고객이 소유권을 갖고 있었지만, SaaS는 소프트웨어가 제품이 아닌 서비스, 즉 빌려 쓰는 모델이라는 점에서 기존 라이선스 모델과는 확연히 구분된다.
- SaaS는 기업이 새로운 소프트웨어 기능을 구매하는데 드는 비용을 대폭 줄여주며, 일정기간 동안 사용량 기반으로 비용을 지급함으로써 인프라 투자와 관리 부담을 피할 수 있게 한다.

22 소프트웨어 에스크로(임치)(Software Escrow)

소프트웨어 에스크로(임치)는 소프트웨어 개발자의 지식재산권을 보호하고 사용자는 저렴한 비용으로 소프트웨어를 안정적으로 사용 및 유지보수 받을 수 있도록 소스 프로그램과 기술 정보 등을 제3의 기관에 보관하는 것이다.

- 소프트웨어 에스크로의 목적은 소프트웨어 저작재산권자의 지식재산권을 보호하고, 저작재산권자의 폐업, 파산, 소프트웨어 개발 관련 정보 멸실 등의 사건이 발생할 경우 소프트웨어 사용 권한이 있는 사용자에게 보관된 자료를 제공하는 등 정당한 사용자의 권리를 보장하는 데 있다.

23 복잡 이벤트 처리(CEP; Complex Event Processing)

복잡 이벤트 처리(CEP)는 실시간으로 발생하는 많은 사건들 중 의미가 있는 것만을 추출할 수 있도록 사건 발생 조건을 정의하는 데이터 처리 방법이다.

- CEP는 금융, 통신, 전력, 물류, 국방 등에서 대용량 데이터 스트림에 대한 요구에 실시간으로 대응하기 위하여 개발된 기술이며, 미들웨어*에 접목시키면 기업이 독자적인 실시간 응용 애플리케이션을 개발할 수 있도록 도와준다.

미들웨어(Middleware)
미들웨어는 다양한 기종의 컴퓨팅 환경에서 응용 프로그램과 운영체제 사이 또는 종류가 다른 두 응용 프로그램 사이에서 보완해 주고 연결해 주는 소프트웨어입니다.

24 디지털 트윈(Digital Twin)

디지털 트윈은 현실속의 사물을 소프트웨어로 가상화한 모델로, 자동차, 항공, 에너지, 국방, 헬스케어 등 여러 분야에서 주목 받고 있다.

- 디지털 트윈은 현실속의 사물을 대신해 다양한 상황을 모의 실험하기 위한 용도로 사용한다.

기출문제 따라잡기 Section 170

출제예상

1. 다음 중 사용자가 눈으로 보는 현실 화면이나 실제 영상에 문자나 그래픽과 같은 가상의 3차원 정보를 실시간으로 겹쳐 보여주는 새로운 멀티미디어 기술을 의미하는 용어로 옳은 것은?

① 가상장치 인터페이스(VDI)
② 가상현실 모델언어(VRML)
③ 증강현실(AR)
④ 주문형 비디오(VOD)

가상현실은 컴퓨터로 만들어 낸 가상의 세계이고, 증강현실은 현실 세계에 가상의 정보를 더한 것임을 염두에 두고 답을 찾아보세요.

출제예상

2. 다음 중 아래의 보기에서 설명하는 최신 정보 기술로 옳은 것은?

- 정보들 사이의 연관성을 컴퓨터가 이해하고 처리할 수 있는 에이전트 프로그램을 통해 사용자가 원하는 정보를 찾아 제공한다.
- 컴퓨터들끼리 정보를 주고받으면서 자체적으로 필요한 일을 처리할 수 있다.
- 차세대 지능형 웹이다.

① AI(Artificial Intelligence)
② IoT(Internet of Things)
③ 시맨틱 웹(Semantic Web)
④ 서비스형 소프트웨어(SSoftware as a Service)

지문에서 '차세대 지능형 웹'이라고 했습니다. 보기 중에서 웹을 찾으면 되겠네요.

출제예상

3. 디지털 콘텐츠의 불법 복제와 유포를 막고 저작권 보유자의 이익과 권리를 보호해주는 기술과 서비스를 무엇이라고 하는가?

① PICS(Platform for Internet Contents Selection)
② DCRP(Digital Contents Rights Protection)
③ DRM(Digital Rights Management)
④ CRM(Customer Relationship Management)

이것은 **디지털**(Digital) 콘텐츠의 **저작권**(Right)을 **관리**(Management) 해주는 기술입니다.

출제예상

4. 소프트웨어를 제공하는 입장에서는 악의적이지 않은 유용한 소프트웨어라고 주장할 수 있지만 사용자 입장에서는 유용할 수도 있고 악의적일 수도 있는 소프트웨어는 무엇인가?

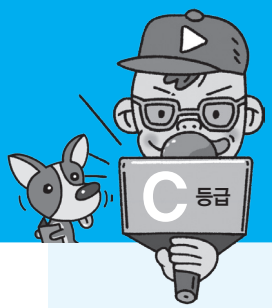
① 애드웨어 ② 그레이웨어
③ 트랙웨어 ④ 스파이웨어

정상적인 소프트웨어의 이미지인 백색과 악성 소프트웨어의 이미지인 흑색의 중간에 해당한다고 해서 붙여진 이름! 뭘까요?

▶ 정답 : 1. ③ 2. ③ 3. ③ 4. ②

SECTION
171
LIVE

소프트웨어 개발 보안



1 소프트웨어 개발 보안의 개요

소프트웨어 개발 보안은 소프트웨어 개발 과정에서 발생할 수 있는 보안 취약점을 최소화하여 보안 위협으로부터 안전한 소프트웨어를 개발하기 위한 일련의 보안 활동을 의미한다.

- 소프트웨어 개발 보안은 데이터의 기밀성(Contidentiality), 무결성(Integrity), 가용성(Availability)을 유지하는 것을 목표로 한다.
- 소프트웨어 보안 취약점이 발생하는 경우
  - 보안 요구사항이 정의되지 않은 경우
  - 소프트웨어 설계 시 논리적 오류가 포함된 경우
  - 기술 취약점을 갖고 있는 코딩 규칙을 적용한 경우
  - 소프트웨어의 배치가 적절하지 않은 경우
  - 보안 취약점 발견 시 적절하게 대응하지 못한 경우
- 안전한 소프트웨어 개발을 위한 수행 작업
  - 소프트웨어 개발 프로젝트에 참여하는 관련자들의 역할과 책임을 명확히 정의하고, 충분한 보안 교육을 실시한다.
  - 소프트웨어 개발 생명 주기(SDLC)*의 각 단계마다 보안 활동을 수행한다.
  - 소프트웨어 개발 보안을 위한 표준을 확립한다.
  - 재사용이 가능한 보안 모듈을 만들어 유사한 소프트웨어 개발에 사용될 수 있도록 한다.
  - 새로운 소프트웨어 개발 프로젝트에 사용될 수 있도록 보안 통제의 효과성 검증을 실시한다.

전문가의 조언

소프트웨어 개발 보안의 개념과 함께 보안 취약점이 발생하는 경우, 안전한 소프트웨어 개발을 위해 수행할 작업에 대해 알아두세요.

소프트웨어 개발 생명 주기

소프트웨어 생명 주기에 대한 자세한 내용은 Section 001을 참조하세요.

2 소프트웨어 개발 보안 관련 기관

소프트웨어 개발 보안과 관련된 활동 주체는 정책기관인 행정안전부, 발주기관인 행정기관, 전문기관인 한국인터넷진흥원(KISA), 개발기관인 사업자, 보안 약점을 진단하는 감리법인 등으로 구분한다.

- 활동 주체별 개발 보안 역할

활동 주체	역할
행정안전부	• 소프트웨어 개발 보안 정책을 총괄한다. • 소프트웨어 개발 보안 관련 법규, 지침, 제도를 정비한다. • 소프트웨어 보안 약점을 진단하는 사람의 양성 및 관련 업무를 수행한다.

전문가의 조언

문제에 제시된 소프트웨어 개발 보안 관련 활동이 어떤 기관의 역할인지 찾아낼 수 있도록 학습하세요.

한국인터넷진흥원(KISA)	• 소프트웨어 개발 보안 정책 및 가이드를 개발한다. • 소프트웨어 개발 보안에 대한 기술을 지원하고, 교육과정 및 자격제도를 운영한다.
발주기관	• 소프트웨어 개발 보안의 계획을 수립한다. • 소프트웨어 개발 보안 사업자 및 감리법인을 선정한다. • 소프트웨어 개발 보안의 준수 여부를 점검한다.
사업자	• 소프트웨어 개발 보안 관련 기술 수준 및 적용 계획을 명시한다. • 소프트웨어 개발 보안 관련 인력을 대상으로 교육을 실시한다. • 소프트웨어 개발 보안 가이드를 참조하여 개발한다. • 자체적으로 보안 약점을 진단하고 제거한다. • 소프트웨어 보안 약점과 관련된 시정 요구사항을 이행한다.
감리법인	• 감리 계획을 수립하고 협의한다. • 소프트웨어 보안 약점의 제거 여부 및 조치 결과를 확인한다.

기출문제 따라잡기 Section 171

출제예상

1. 다음 중 소프트웨어 개발 보안에 대한 설명으로 가장 옳지 않은 것은?

① 소프트웨어 개발 보안은 보안 위협으로부터 안전한 소프트웨어를 개발하기 위한 일련의 보안 활동이다.
② 소프트웨어 개발 보안의 목적은 데이터의 기밀성, 무결성, 가용성을 유지하는 것이다.
③ 소프트웨어의 배치가 적절하지 못한 경우 보안 취약점이 발생할 수 있다.
④ 보안 활동은 소프트웨어 개발 생명 주기(SDLC)의 개발 단계에서만 수행한다.

일반적으로 소프트웨어 개발 생명 주기는 정의, 개발, 유지보수 단계로 구분하는데, 개발 단계에서만 보안 취약점이 발생할까요?

출제예상

2. 다음 중 소프트웨어 보안 취약점이 발생하는 경우가 아닌 것은?

① 보안 요구사항이 정의되지 않은 경우
② 물리적인 오류를 가지는 설계를 수행한 경우
③ 기술 취약점을 가지는 코딩 규칙을 적용한 경우
④ 발견된 취약점에 대해 적절한 관리 또는 패치를 하지 않은 경우

소프트웨어 보안 취약점은 물리적이 아닌 논리적인 오류를 가지는 설계를 수행한 경우 발생합니다.

출제예상

3. 다음 중 소프트웨어 개발 보안과 관련된 활동 주체가 아닌 것은?

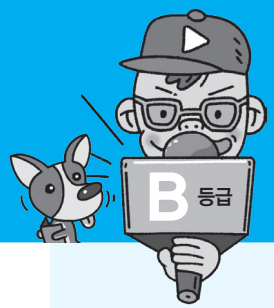
① 행정안전부 ② 산업통상자원부
③ 발주기관 ④ KISA

소프트웨어 개발 보안과 관련된 활동 주체는 앞글자만 따서 '**감**리법인, **사**업자, **한**국인터넷진흥원(KISA), **발**주기관, **행**정안전부'로 외워두세요.

▶ 정답 : 1. ④ 2. ② 3. ②

SECTION
172
LIVE

소프트웨어 개발 직무별 보안 활동



1 소프트웨어 개발 직무별 보안 활동

안전한 소프트웨어 개발을 위해서는 프로젝트 관련자들이 보안 활동을 수행할 수 있도록 각 직무(Role)별로 수행해야 할 보안 활동을 정의해야 한다.

- 소프트웨어 개발 참여자의 직무는 프로젝트 관리자, 요구사항 분석가, 아키텍트, 설계자, 구현 개발자, 테스트 분석가, 보안 감사자로 구분한다.

2 프로젝트 관리자(Project Manager)

- 응용 프로그램에 대한 보안 전략을 조직 구성원들에게 전달한다.
- 조직 구성원들에게 응용 프로그램 보안 영향을 이해시킨다.
- 조직의 상태를 모니터링 한다.

3 요구사항 분석가(Requirement Specifier)

- 아키텍트가 고려해야 할 보안 관련 비즈니스 요구사항을 설명한다.
- 프로젝트 팀이 고려해야 할 구조 정의 및 해당 구조에 존재하는 자원에 대한 보안 요구사항을 정의한다.

4 아키텍트(Architect)※

- 보안 오류가 발생하지 않도록 보안 기술 문제를 충분히 이해한다.
- 시스템에 사용되는 모든 리소스 정의 및 각 리소스별로 적절한 보안 요구사항을 적용한다.

5 설계자(Designer)

- 특정 기술에 대해 보안 요구사항의 만족성 여부를 확인한다.
- 문제 발생 시 최선의 문제 해결 방법을 결정한다.
- 애플리케이션 보안 수준에 대한 품질 측정을 지원한다.
- 많은 비용이 필요한 수정 요구사항을 최소화하기 위한 방법을 제공한다.
- 다른 소프트웨어와 통합할 때 발생할 수 있는 보안 위험에 대해 이해해야 한다.
- 소프트웨어에서 발견된 보안 위협에 대해 적절히 대응한다.

전문가의 조언

소프트웨어 개발 프로젝트에 참여하는 각 참여자들의 역할을 구분할 수 있도록 학습하세요.

아키텍트(Architect)

아키텍트는 아키텍처(Architecture)를 설계 및 구축하는 사람을 의미합니다.

※ **아키텍처(Architecture)** : 개발할 소프트웨어의 기본 틀을 만드는 것으로, 복잡한 소프트웨어 개발 과정을 체계적으로 접근하기 위한 밑그림을 의미합니다.

시큐어 코딩(Secure Coding)
시큐어 코딩은 개발하고 있는 소프트웨어의 보안상 취약점을 사전에 보완하면서 프로그래밍하는 것입니다.

6 구현 개발자(Implementer)

- 구조화된 소프트웨어 개발 환경에서 프로그램을 원활히 구현할 수 있도록 시큐어 코딩* 표준을 준수하여 개발한다.
- 다른 사람이 소프트웨어의 안전 여부를 쉽게 확인할 수 있도록 문서화 한다.

7 테스트 분석가(Test Analyst)

- 소프트웨어 개발 요구사항과 구현 결과를 반복적으로 확인한다.
- 테스트 분석가는 반드시 보안 전문가일 필요는 없지만 보안 위험에 대한 학습이나 툴(Tool) 사용법 정도는 숙지하고 있어야 한다.

8 보안 감사자(Security Auditor)

- 소프트웨어 개발 프로젝트의 현재 상태의 보안을 보장한다.
- 요구사항 검토 시 요구사항의 적합성과 완전성을 확인한다.
- 소프트웨어 개발 프로젝트의 전체 단계에서 활동한다.
- 설계 단계에서는 보안 문제로 이어질 수 있는 사항이 있는지 확인한다.
- 구현 단계에서는 보안 문제가 있는지 확인한다.

기출문제 따라잡기 Section 172

출제예상
1. 다음과 같은 직무를 수행하는 프로젝트 참여자는?

- 팀 구성원들에게 응용 프로그램 보안 전략을 전달한다.
- 프로젝트 일정 및 보안 위험의 상관관계 같은 응용 프로그램에 대한 보안 영향을 이해시킨다.
- 조직의 상태를 모니터링 한다.

① Project Manager ② Architect
③ Designer ④ Requirement Specifier

이 사람의 역할은 프로젝트(Project)를 전반적으로 관리(Management)하는 것입니다.

출제예상
2. 아키텍트가 고려해야 할 보안 관련 비즈니스 요구사항들을 자세히 설명하고, 프로젝트 팀이 고려해야 할 구조를 정의한 다음 해당 구조에 존재하는 자원에 대한 보안 요구사항을 결정하는 자는?

① 설계자(Designer)
② 테스트 분석가(Test Analyst)
③ 요구사항 분석가(Requirement Specifier)
④ 보안 감사자(Security Auditor)

문제에 답이 숨어 있네요. 요구사항들을 자세히 설명하고 ~ 요구사항을 결정하는 자!

출제예상
3. 다음은 소프트웨어 개발 프로젝트의 참여자 중 누구에 대한 설명인가?

- 고도로 구조화된 개발 환경에서 프로그램을 구현하기 위해 시큐어 코딩 표준을 준수하여 개발한다.
- 제 3자가 소프트웨어의 안전 여부를 쉽게 판단할 수 있도록 문서화 한다.

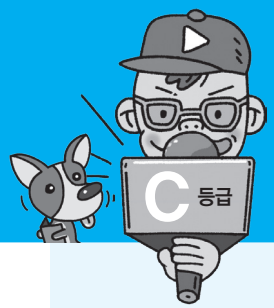
① 아키텍트 ② 설계자
③ 구현 개발자 ④ 보안 감사자

프로그램 구현을 위해 소프트웨어를 개발하는 사람은 누구일까요?

▶ 정답 : 1. ① 2. ③ 3. ③

SECTION 173 LIVE

소프트웨어 개발 보안 활동 관련 법령 및 규정



1 개인정보 보호 관련 법령

- **개인정보 보호법** : 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호한다.
- **정보통신망 이용촉진 및 정보보호 등에 관한 법률** : 정보통신망의 이용 촉진 및 정보통신 서비스를 이용하는 이용자들의 개인정보를 보호한다.
- **신용정보의 이용 및 보호에 관한 법률** : 개인 신용정보의 효율적 이용과 체계적인 관리를 통해 정보의 오남용을 방지한다.
- **위치정보의 보호 및 이용 등에 관한 법률** : 개인 위치정보의 안전한 이용 환경을 조성하여 정보의 유출이나 오남용을 방지한다.
- **표준 개인정보 보호 지침** : 개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등에 관한 세부사항을 규정한다.
- **개인정보의 안전성 확보 조치 기준** : 개인정보 처리자가 개인정보를 처리하는데 있어 개인정보가 분실, 도난, 유출, 위조, 변조, 훼손되지 않도록 안전성 확보에 필요한 기술적, 관리적, 물리적 안전조치에 관한 최소한의 기준을 규정한다.
- **개인정보 영향평가에 관한 고시** : 개인정보 영향평가를 위한 평가기관의 지정, 영향평가의 절차 등에 관한 세부기준을 규정한다.

2 IT 기술 관련 규정

- **RFID 프라이버시 보호 가이드라인** : RFID 시스템의 이용자들의 프라이버시를 보호하고 안전한 RFID 이용 환경을 조성하기 위한 가이드라인
- **위치정보의 보호 및 이용 등에 관한 법률** : 개인 위치정보의 유출 및 오남용을 방지하기 위한 법률
- **위치정보의 관리적, 기술적 보호조치 권고 해설서** : 개인 위치정보의 누출, 변조, 훼손 등을 방지하기 위해 위치정보 사업자 및 위치기반 서비스 사업자가 준수해야 하는 관리적, 기술적 보호조치의 구체적인 기준
- **바이오정보*** **보호 가이드라인** : 개인 바이오정보의 보호와 안전한 활용을 위한 원칙 및 조치사항
- **뉴미디어 서비스*** **개인정보 보호 가이드라인** : 뉴미디어 서비스 이용 및 제공 시 개인정보의 침해사고를 예방하기 위한 준수사항

전문가의 조언

개인정보 보호 관련 법령과 IT 기술 관련 규정에는 어떤 것들이 있는지 알아두고, 각각의 개념을 구분할 수 있도록 정리하세요. 각각의 명칭을 통해 어렵지 않게 특징을 알 수 있으니 편하게 학습하시면 됩니다.

바이오정보

바이오정보는 지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 의미합니다.

뉴미디어 서비스

뉴미디어 서비스는 클라우드 컴퓨팅 서비스, 소셜 네트워크 서비스, 소셜 커머스 서비스, 스마트폰 활용 서비스 등을 의미합니다.

기출문제 따라잡기 Section 173

출제예상

1. 다음이 설명하는 소프트웨어 개발 보안 활동 관련 법령은?

> 개인정보 처리자가 개인정보를 처리함에 있어서 개인정보가 분실, 도난, 유출, 위조, 변조 또는 훼손되지 않도록 안전성 확보에 필요한 기술적, 관리적, 물리적 안전조치에 관한 최소한의 기준을 정하는 것을 목적으로 한다.

① 개인정보 보호법
② 개인정보의 안전성 확보 조치 기준
③ 표준 개인정보 보호 지침
④ 개인정보 영향평가에 관한 고시

문제의 지문에 답이 숨어 있네요. 소프트웨어 개발 보안 활동 관련 법령이나 규정은 명칭으로 개념을 쉽게 유추할 수 있습니다.

출제예상

2. 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하는 것을 목적으로 하는 것은?

① 신용정보의 이용 및 보호에 관한 법률
② 표준 개인정보 보호 지침
③ 개인정보 영향평가에 관한 고시
④ 개인정보 보호법

개인정보를 보호하는 법은 무엇일까요?

출제예상

3. 다음이 설명하는 것은 무엇인가?

> 지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보의 보호와 안전한 활용을 위한 원칙 및 조치사항의 안내를 목적으로 한다.

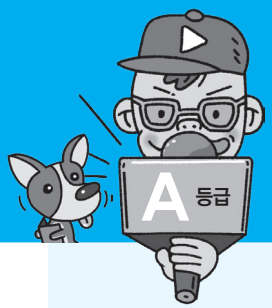
① RFID 프라이버시 보호 가이드라인
② 바이오정보 보호 가이드라인
③ 위치정보의 관리적, 기술적 보호조치 권고 해설서
④ 뉴미디어 서비스 개인정보보호 가이드라인

지문, 홍채 등 개인을 식별할 수 있는 신체 및 행동적 특징에 관한 정보를 바이오정보라고 합니다.

▶ 정답 : 1. ② 2. ④ 3. ②

SECTION 174 LIVE

HW 관련 신기술



1 고가용성(HA; High Availability)

고가용성은 긴 시간동안 안정적인 서비스 운영을 위해 장애 발생 시 즉시 다른 시스템으로 대체 가능한 환경을 구축하는 메커니즘을 의미한다.

- 가용성(Availability)을 극대화하는 방법으로는 클러스터*, 이중화* 등이 있다.

2 3D Printing(Three Dimension Printing)

3D Printing은 대상을 평면에 출력하는 것이 아니라 손으로 만질 수 있는 실제 물체로 만들어내는 것을 말한다.

- 3D Printing은 아주 얇은 두께로 한층한층 적층시켜 하나의 형태를 만들어내는 기술을 이용한다.
- 3D Printing은 건축가나 항공우주, 전자, 공구 제조, 자동차, 디자인, 의료 분야에서 사용되고 있다.

3 4D Printing(Fourth Dimension Printing)

4D Printing은 특정 시간이나 환경 조건이 갖추어지면 스스로 형태를 변화시키거나 제조되는 자가 조립(Self-Assembly) 기술이 적용된 제품을 3D Printing하는 기술을 의미한다.

- 4D Printing은 2013년 4월 TED(Technology, Entertainment, Design) 강연에서 미국 MIT 자가 조립 연구소(Self-Assembly Lab)의 스카일러 티빗츠(Skylar Tibbits) 교수에 의해 처음 공개되었다.
- 4D Printing을 위해서는 인간의 개입 없이 열 · 진동 · 습도 · 중력 등 다양한 환경이나 에너지원에 자극 받아 변화하는 스마트 소재가 필요하며, 이는 형상기억합금*이나 나노 기술*을 통해 전기회로를 내장하는 방법 등으로 제조된다.
- 4D Printing으로 제조된 제품에 전기로 열을 가하면 기존에 설정한 모양으로 접히는 종이접기 로봇이나, 접힌 상태에서 출력되어 완전한 형태로 변화하는 키네메틱스 드레스(Kinematics Dress) 등이 선보여진 바 있다.

전문가의 조언

문제에 제시된 내용이 무슨 용어를 말하는지 맞힐 수 있을 정도로 학습하세요.

클러스터 / 이중화

클러스터와 이중화에 대한 자세한 내용은 Section 094를 참조하세요.

형상기억합금

형상기억합금은 모양을 변형시켜도 일정한 온도가 주어지면 변형 전 모양으로 다시 되돌아오는 성질을 가진 합금입니다.

나노 기술(Nanotechnology)

나노(Nano)는 10억분의 1을 나타내는 단위로, 나노 기술은 나노미터 정도로 아주 작은 크기의 소자를 만들고 제어 하는 기술, 즉 분자와 원자를 다루는 초미세 기술을 의미합니다.

4 RAID(Redundant Array of Inexpensive Disk, Redundant Array of Independent Disk)

여러 개의 하드디스크로 디스크 배열을 구성하여 파일을 구성하고 있는 데이터 블록들을 서로 다른 디스크들에 분산 저장할 경우 그 블록들을 여러 디스크에서 동시에 읽거나 쓸 수 있으므로 디스크의 속도가 매우 향상되는데, 이 기술을 RAID라고 한다.

- RAID는 어느 한 디스크에만 결함이 발생해도 전체 데이터에 파일이 손상되는 문제가 발생한다. 이러한 문제점을 해결하기 위해 디스크 배열에 오류 검출 및 복구를 위한 여분의 디스크들을 추가하여 오류가 발생해도 원래의 데이터를 복구할 수 있게 했다.
- RAID는 오류 검출 및 정정 방법에 따라 RAID1 ~ RAID5까지 다섯 종류가 있다.

5 4K 해상도

4K 해상도는 차세대 고화질 모니터의 해상도를 지칭하는 용어이다.

- 4K 해상도는 가로 픽셀 수가 3840이고(1920×1080) 세로 픽셀 수가 2160인 영상의 해상도를 말하는데, 이는 Full HDTV의 가로 · 세로 2배, 총 4배에 해당하는 초고화질의 영상이다.
- UHDTV*는 차세대 TV 규격으로, HDTV 해상도의 4배에 해당하는 4K, 16배에 해당하는 8K 해상도를 채택하고 있다.

UHDTV
UHDTV는 'Ultra High Definition TV'의 줄임말로, 초고화질 TV를 의미합니다.

6 앤 스크린(N-Screen)

앤 스크린은 N개의 서로 다른 단말기에서 동일한 콘텐츠를 자유롭게 이용할 수 있는 서비스를 말한다.

- 앤 스크린은 PC, TV, 휴대폰에서 동일한 콘텐츠를 끊김 없이 이용할 수 있는 것은 물론 사용자가 가지고 있는 여러 개의 단말기에서도 동일한 콘텐츠를 끊김 없이 이용할 수 있다.

7 컴패니언 스크린(Companion Screen)

컴패니언 스크린은 앤 스크린(N Screen)의 한 종류로, TV 방송 시청 시 방송 내용을 공유하며 추가적인 기능을 수행할 수 있는 스마트폰, 태블릿PC 등을 의미한다. 세컨드 스크린(Second Screen)이라고도 불린다.

- 컴패니언 스크린 이용자는 IP(Internet Protocol)망을 통해 TV와 스마트폰, PC 등을 연결하여 시청 중인 방송 프로그램의 관련 정보, 가수의 영상(VOD), 음원(AOD) 등을 이용하는 것이 가능하며, 소셜TV와 같이 시청 중에 SNS를 통해 다른 사람들과 의견을 공유할 수도 있다.

8 신 클라이언트 PC(Thin Client PC)

신 클라이언트 PC는 하드디스크나 주변 장치 없이 기본적인 메모리만 갖추고 서버와 네트워크로 운용되는 개인용 컴퓨터를 말하는 것으로, 서버 기반 컴퓨팅과 관계가 깊다.

- 클라이언트는 프로그램이 필요할 때마다 서버에 접속하여 소프트웨어를 내려받기만 하면 되며, 기억장치가 없으므로 데이터는 서버 측에서 한꺼번에 관리한다.
- 신 클라이언트 PC는 기억장치를 따로 두지 않기 때문에 PC를 분실하더라도 정보가 유출될 우려가 없다.
- 신 클라이언트 PC는 원래 유지보수 등에 발생하는 비용을 절감하기 위해 고안되었지만, 정보 유출 방지를 위해 이용되면서 재택근무 도입을 검토하고 있는 기업들의 주목을 받고 있다.

9 패블릿(Phablet)

패블릿은 폰(Phone)과 태블릿(Tablet)의 합성어로, 태블릿 기능을 포함한 5인치 이상의 대화면 스마트폰을 말한다.

- 대화면 스마트폰은 동영상 시청, 웹 브라우징 등 각종 서비스가 월등하므로 대화면 기기를 한 번 사용해보면 작은 기기를 사용할 수 없다는 이른바 '톱니 효과(Ratchet Effect)'가 적용될 수 있다는 점에서 의미 있는 프리미엄 제품이다.

10 C형 유에스비(Universal Serial Bus Type-C, USB Type-C, USB-C)

C형 유에스비는 범용 인터페이스 규격인 유에스비(USB; Universal Serial Bus)의 표준 중 하나로, 2014년 8월 USB IF(Implementers Forum)에서 발표되었다.

- C형 유에스비는 기존 A형에 비하여 크기가 작고, 24핀으로 위아래의 구분이 없어 어느 방향으로든 연결이 가능하다.
- C형 유에스비의 데이터 전송 속도는 초당 10기가비트(Gbps)이며, 전력은 최대 100W까지 전송이 가능하다.
- 전력 전송량이 증대됨에 따라 전원 케이블을 필요로 하던 주변기기들을 C형 유에스비만으로 연결할 수 있게 되면서 기기 간 연결의 편의성이 증대되었다.

11 멤스(MEMS; Micro-Electro Mechanical Systems)

멤스는 초정밀 반도체 제조 기술을 바탕으로 센서, 액추에이터(Actuator) 등 기계 구조를 다양한 기술로 미세 가공하여 전기기계적 동작을 할 수 있도록 한 초미세 장치이다.

- 멤스는 일반적으로 작은 실리콘 칩 위에 마이크로 단위의 작은 부품과 이들을 입체적으로 연결하는 마이크로 회로들로 구성되며, 정보기기의 센서나 프린터 헤드, HDD 자기 헤드, 기타 환경, 의료 및 군사 용도로 이용된다.
- 최근의 초소형이면서 고도의 복잡한 동작을 하는 마이크로시스템이나 마이크로머신들은 대부분 멤스 기술을 사용한다.

12 트러스트존 기술(TrustZone Technology)

트러스트존 기술은 칩 설계회사인 ARM(Advanced RISC Machine)에서 개발한 기술로, 하나의 프로세서(Processor) 내에 일반 애플리케이션을 처리하는 일반 구역(Normal World)과 보안이 필요한 애플리케이션을 처리하는 보안 구역(Secure World)으로 분할하여 관리하는 하드웨어 기반의 보안 기술이다.

- 트러스트존 기술을 적용한 프로세서를 사용하면 결제, 인증서, 기밀문서 등과 같이 보안이 필요한 데이터들을 취급하는 애플리케이션을 외부 공격에 노출하지 않고 운영체제(OS) 수준에서 안전하게 보호하는 것이 가능하다.

13 엠디스크(M-DISC, Millennial DISC)

엠디스크는 한 번의 기록만으로 자료를 영구 보관할 수 있는 광 저장 장치이다.

- 엠디스크는 디스크 표면의 무기물층에 레이저를 이용해 자료를 조각해서 기록한다. 기존의 염료층에 표시하는 방식과 달리 물리적으로 조각하는 방식 덕분에 시간이 가도 변하지 않는 금속 활자처럼 빛, 열, 습기 등의 외부 요인에 영향을 받지 않는다.
- 엠디스크는 미국의 밀레니어터(Millenniata)사에서 개발되었으며, 디지털 비디오 디스크(DVD)와 블루레이 디스크(Blue-ray Disk)*에 적용된다.

블루레이 디스크(Blue-ray Disk)
블루레이 디스크는 고선명(HD) 비디오를 위한 디지털 데이터를 저장할 수 있도록 만든 광 기록 방식의 저장매체입니다.

14 멤리스터(Memristor)

멤리스터는 메모리(Memory)와 레지스터(Resister)의 합성어로, 전류의 방향과 양 등 기존의 경험을 모두 기억하는 특별한 소자이다.

- 멤리스터는 레지스터(Resister), 커패시터(Capacitor), 인덕터(Inductor)에 이어 네 번째 전자회로 구성 요소라 불리고 있다.
- 멤리스터는 전원 공급이 끊어졌을 때도 직전에 통과한 전류의 방향과 양을 기억하기 때문에 다시 전원이 공급되면 기존의 상태가 그대로 복원된다. 컴퓨터를 예로 들면, 문서 작업을 하다 전원을 끈 뒤 다시 켜면 작업했던 상태 그대로 남아 있는 것이다. 이를 이용하면 수분이 소요되는 부팅 시간이 몇 초로 줄어들 수 있다.

기출문제 따라잡기 Section 174

출제예상

1. 다음 보기는 무엇에 대한 설명인가?

> PC, TV, 휴대폰 등 여러 개의 서로 다른 단말기에서 동일한 콘텐츠를 자유롭게 이용할 수 있다.

① Companion Screen
② N-Screen
③ Phablet
④ Second Screen

지문의 내용과 보기의 영문 뜻을 연결해서 답을 찾아보세요.

출제예상

2. 다음 중 하드디스크나 주변 장치 없이 기본적인 메모리만 갖추고 서버와 네트워크로 운용되는 개인용 컴퓨터를 의미하는 것은?

① Mobile Computing
② Cloud Computing
③ MEMS
④ Thin Client PC

서버와 네트워크로 연결되어 운영되는 것! 서버 하면 항상 따라 오는 게 뭐죠?

출제예상

3. 다음은 하드웨어와 관련된 기술들을 설명한 것이다. 가장 옳지 않은 것은?

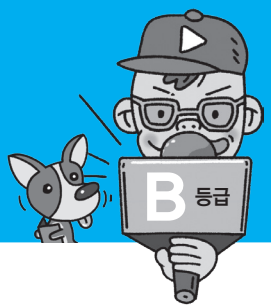
① MEMS : 초정밀 반도체 제조 기술을 바탕으로 센서, 액추에이터(Actuator) 등 기계 구조를 다양한 기술로 미세 가공하여 전기기계적 동작을 할 수 있도록 한 초미세 장치
② TrustZone Technology : 하나의 프로세서 내에 일반 애플리케이션을 처리하는 일반 구역(Normal World)과 보안이 필요한 애플리케이션을 처리하는 보안 구역(Secure World)으로 분할하여 관리하는 하드웨어 기반의 보안 기술
③ Phablet : 태블릿 기능을 포함한 10인치 이상의 대화면 스마트폰
④ M-DISC : 한 번의 기록만으로 자료를 영구 보관할 수 있는 광 저장 장치

패블릿은 10인치 이상이 아니라 5인치 이상의 대화면 스마트폰입니다.

▶ 정답 : 1. ② 2. ④ 3. ③

SECTION 175 ● LIVE

Secure OS



전문가의 조언

보안 커널의 개념과 구현 복잡도에 따른 분리 방법들을 기억하고, Secure OS의 각 기능들의 개별적인 의미를 확실히 파악해 두세요.

커널(Kernel)

커널은 컴퓨터가 부팅될 때 주기억장치에 적재된 후 실행된 상태로 상주하면서 하드웨어를 보호하고, 프로그램과 하드웨어 간의 인터페이스 역할을 담당합니다.

TCB(Trusted Computing Base)

TCB는 운영체제(OS), 하드웨어, 소프트웨어, 펌웨어 등 컴퓨터 시스템 내의 모든 장치가 보안 정책을 따르도록 설계한 보호 메커니즘입니다.

1 Secure OS의 개요

Secure OS는 기존의 운영체제(OS)에 내재된 보안 취약점을 해소하기 위해 보안 기능을 갖춘 커널*을 이식하여 외부의 침입으로부터 시스템 자원을 보호하는 운영체제를 의미한다.

- 보안 커널은 보안 기능을 갖춘 커널을 의미하며, TCB*를 기반으로 참조 모니터의 개념을 구현하고 집행한다.
- 보안 커널의 보호 대상에는 메모리와 보조기억장치, 그리고 그곳에 저장된 데이터, 하드웨어 장치, 자료 구조, 명령어, 각종 보호 메커니즘 등이 있다.
- 보호 방법을 구현하기 복잡한 것부터 차례로 분류하면 다음과 같다.
  - 암호적 분리(Cryptographic Separation) : 내부 정보를 암호화하는 방법
  - 논리적 분리(Logical Separation) : 프로세스의 논리적 구역을 지정하여 구역을 벗어나는 행위를 제한하는 방법
  - 시간적 분리(Temporal Separation) : 동일 시간에 하나의 프로세스만 수행되도록 하여 동시 실행으로 발생하는 보안 취약점을 제거하는 방법
  - 물리적 분리(Physical Separation) : 사용자별로 특정 장비만 사용하도록 제한하는 방법

참조 모니터(Reference Monitor)

참조 모니터는 보호대상의 객체에 대한 접근통제를 수행하는 추상머신이며, 이것을 실제로 구현한 것이 보안 커널입니다.

- 참조 모니터는 보안 커널 데이터베이스(SKDB; Security Kernel Database)를 참조하여 객체에 대한 접근 허가 여부를 결정합니다.
- 참조 모니터와 보안 커널은 다음의 3가지 특징을 갖습니다.
  - 격리성(Isolation) : 부정 조작이 불가능해야 합니다.
  - 검증가능성(Verifiability) : 적절히 구현되었다는 것을 확인할 수 있어야 합니다.
  - 완전성(Completeness) : 우회가 불가능해야 합니다.

2 Secure OS의 보안 기능

Secure OS의 보안 기능에는 식별 및 인증, 임의적/강제적 접근통제, 객체 재사용 보호, 완전한 조정, 신뢰 경로, 감사 및 감사기록 축소 등이 있다.

식별 및 인증	각 접근 주체에 대한 안전하고 고유한 식별 및 인증 기능
임의적 접근통제	• 소속 그룹 또는 개인에 따라 부여된 권한에 따라 접근을 통제하는 기능 • DAC(Discretionary Access Control) 또는 신분 기반 정책이라고도 한다.
강제적 접근통제	• 접속 단말 및 접속 방법, 권한, 요청 객체의 특성 등 여러 보안 속성이 고려된 규칙에 따라 강제적으로 접근을 통제하는 기능 • MAC(Mandatory Access Control) 또는 규칙 기반 정책이라고도 한다.
객체 재사용※ 보호	메모리에 기존 데이터가 남아있지 않도록 초기화하는 기능
완전한 조정	우회할 수 없도록 모든 접근 경로를 완전하게 통제하는 기능
신뢰 경로	비밀번호 변경 및 권한 설정 등과 같은 보안 작업을 위한 안전한 경로를 제공하는 기능
감사 및 감사기록 축소	• 모든 보안 관련 사건 및 작업을 기록(Log)한 후 보호하는 기능 • 막대한 양의 기록들을 분석하고 축소하는 기능

객체 재사용(Object Reuse)
객체 재사용은 객체가 사용한 후 해제한 메모리에 남아 있는 데이터를 탈취하는 공격 기법입니다.

기출문제 따라잡기 Section 175

출제예상
1. Secure OS에 대한 설명으로 거리가 먼 것은?

① Secure OS는 기존 OS에 내재된 보안 취약점을 해소하기 위해 개발되었다.
② 보안 커널을 이식하여 외부로부터의 접근을 분리하고 통제한다.
③ 보호 대상에는 메모리 및 보조기억장치의 데이터부터 하드웨어 장치까지 다양한 요소들을 보호한다.
④ 보호 방법 중 물리적 분리는 구현 방법이 가장 복잡하다.

물리적 분리(Physical Separation)는 사용자별로 특정 장비만 사용하도록 제한하는 방법으로, 구현 방법이 복잡하지 않습니다.

출제예상
2. 참조 모니터(Reference Monitor)의 특징에 속하지 않는 것은?

① Isolation ② Cohesion
③ Verifiability ④ Completeness

영문으로 나왔다고 당황하지 마세요. ①번은 격리성, ②번은 응집도, ③번은 검증 가능성, ④번은 완전성을 의미합니다. 이제 정답을 찾아보세요.

▶ 정답 : 1. ④ 2. ②

SECTION 176 ● LIVE

DB 관련 신기술

전문가의 조언

문제에 제시된 내용이 무슨 용어를 말하는지 맞힐 수 있을 정도로 학습하세요.

사물 네트워크

사물 네트워크는 인간과 사물, 서비스 등 분산되어 있는 요소들이 인간의 개입 없이 상호 협력적으로 감지, 통신, 정보 처리 등 지능적 관계를 형성하는 네트워크입니다.

1 빅데이터(Big Data)

빅데이터는 기존의 관리 방법이나 분석 체계로는 처리하기 어려운 막대한 양의 정형 또는 비정형 데이터 집합으로, 스마트 단말의 빠른 확산, 소셜 네트워크 서비스의 활성화, 사물 네트워크*의 확대로 데이터 폭발이 더욱 가속화되고 있다.

- 빅데이터가 주목받고 있는 이유는 기업이나 정부, 포털 등이 빅데이터를 효과적으로 분석함으로써 미래를 예측해 최적의 대응 방안을 찾고, 이를 수익으로 연결하여 새로운 가치를 창출하기 때문이다.

2 브로드 데이터(Broad Data)

브로드 데이터는 다양한 채널에서 소비자와 상호 작용을 통해 생성된, 기업 마케팅에 있어 효율적이고 다양한 데이터이며, 이전에 사용하지 않거나 알지 못했던 새로운 데이터나, 기존 데이터에 새로운 가치가 더해진 데이터를 말한다.

- 브로드 데이터는 대량의 자료를 뜻하는 빅데이터(Big Data)와는 달리 다양한 정보를 뜻하는 것으로, 소비자의 SNS 활동이나 위치 정보 등이 이에 속한다.
- IBM은 아시아 유통 데이터 분석 리포트를 통해 브로드 데이터의 중요성을 강조하기도 했다.

3 메타 데이터(Meta Data)

메타 데이터는 일련의 데이터를 정의하고 설명해 주는 데이터이다. 컴퓨터에서는 데이터 사전의 내용, 스키마 등을 의미하고, HTML 문서에서는 메타 태그 내의 내용이 메타 데이터이다. 방송에서는 방대한 분량의 저작물을 신속하게 검색하기 위한 촬영 일시, 장소, 작가, 출연자 등과 음원의 검색을 위한 작곡자나 가수명 등을 메타 데이터로 처리한다.

- 메타 데이터는 여러 용도로 사용되나 주로 빠르게 검색하거나 내용을 간략하고 체계적으로 하기 위해 많이 사용된다.

4 디지털 아카이빙(Digital Archiving)

디지털 아카이빙은 디지털 정보 자원을 장기적으로 보존하기 위한 작업을 말한다. 아날로그 콘텐츠는 디지털로 변환한 후 압축해서 저장하고, 디지털 콘텐츠도 체계적으로 분류하고 메타 데이터를 만들어 DB화하는 작업이다.

- 디지털 아카이빙은 늘어나는 정보 자원의 효율적인 관리와 이용을 위해 필요한 작업이다.

5 하둡(Hadoop)

하둡은 오픈 소스를 기반으로 한 분산 컴퓨팅 플랫폼이다.

- 하둡은 일반 PC급 컴퓨터들로 가상화된 대형 스토리지를 형성하고 그 안에 보관된 거대한 데이터 세트를 병렬로 처리할 수 있도록 개발된 자바 소프트웨어 프레임워크로, 구글, 야후 등에 적용되고 있다.

6 타조(Tajo)

타조는 오픈 소스 기반 분산 컴퓨팅 플랫폼인 아파치 하둡(Apache Hadoop) 기반의 분산 데이터 웨어하우스* 프로젝트로, 우리나라가 주도하여 개발하고 있다.

- 타조는 하둡(Hadoop)의 빅데이터를 분석할 때 맵리듀스(MapReduce)*를 사용하지 않고 구조화 질의 언어(SQL)를 사용하여 하둡 분산 파일 시스템(HDFS; Hadoop Distributed File System) 파일을 바로 읽어낼 수 있다.
- 타조는 대규모 데이터 처리와 실시간 상호 분석에 모두 사용할 수 있다.

7 데이터 다이어트(Data Diet)

데이터 다이어트는 데이터를 삭제하는 것이 아니라 압축하고, 중복된 정보는 중복을 배제하고, 새로운 기준에 따라 나누어 저장하는 작업이다.

- 데이터 다이어트는 인터넷과 이동통신 이용이 늘면서 각 기관 · 기업의 데이터베이스에 쌓인 방대한 정보를 효율적으로 관리하기 위해 대두된 방안으로, 같은 단어가 포함된 데이터들을 한 곳에 모아 두되 필요할 때 제대로 찾아내는 체계를 갖추는 것이 중요하다.

데이터 웨어하우스(Data Warehouse)
데이터 웨어하우스는 정보(Data)와 창고(Warehouse)의 합성어로, 기업의 의사결정 과정에 효과적으로 사용될 수 있도록 여러 시스템에 분산되어 있는 데이터를 주제별로 통합 · 축적해 놓은 데이터베이스입니다.

맵리듀스(MapReduce)
맵리듀스란 흩어져 있는 데이터를 연관성 있는 데이터 분류로 묶는 Map 작업을 수행한 후 중복 데이터를 제거하고 원하는 데이터를 추출하는 Reduce 직업을 수행하는 것을 의미합니다.

기출문제 따라잡기 Section 076

출제예상
1. 다음 중 각 용어에 대한 설명으로 틀린 것은?

① Tajo : 오픈 소스 기반 분산 컴퓨팅 플랫폼인 아파치 하둡(Apache Hadoop) 기반의 분산 데이터 웨어하우스 프로젝트

② Meta Data : 일련의 데이터를 정의하고 설명해 주는 데이터

③ Digital Archiving : 데이터를 압축하고, 겹친 정보는 중복을 배제하고, 새로운 기준에 따라 나누어 저장하는 작업

④ Hadoop : 오픈 소스를 기반으로 한 분산 컴퓨팅 플랫폼

데이터를 압축하고 중복을 배제하여 크기를 줄이는 것은 Data Diet입니다.

출제예상
2. 다음은 무엇에 대한 설명인가?

- 다양한 채널에서 소비자와 상호 작용을 통해 생성된 데이터
- 이전에 사용하지 않거나 알지 못했던 새로운 데이터
- 기존 데이터에 새로운 가치가 더해진 데이터

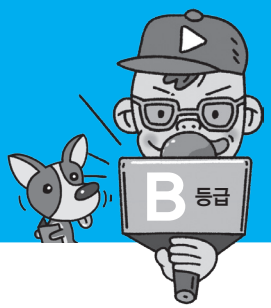
① 빅 데이터 ② 브로드 데이터
③ 메타 데이터 ④ 스마트 데이터

기존 데이터에 새로운 가치를 더해 넓어진 데이터! 뭘까요? 스마트 데이터는 실제로 가치를 창출할 수 있는 검증된 고품질의 데이터를 의미합니다.

▶ 정답 : 1. ③ 2. ②

SECTION 177 LIVE

회복 / 병행제어



전문가의 조언

회복은 말 그대로 원래의 상태로 복구하는 것입니다. 장애의 유형을 살펴보고, 회복 관리기의 역할에 대해 알아두세요.

1 회복(Recovery)

회복은 트랜잭션들을 수행하는 도중 장애가 발생하여 데이터베이스가 손상되었을 때 손상되기 이전의 정상 상태로 복구하는 작업이다.

장애의 유형

- **트랜잭션 장애** : 입력 데이터 오류, 불명확한 데이터, 시스템 자원 요구의 과다 등 트랜잭션 내부의 비정상적인 상황으로 인하여 프로그램 실행이 중지되는 현상
- **시스템 장애** : 데이터베이스에 손상을 입히지는 않으나 하드웨어 오동작, 소프트웨어의 손상, 교착상태 등에 의해 모든 트랜잭션의 연속적인 수행에 장애를 주는 현상
- **미디어 장애** : 저장장치인 디스크 블록의 손상이나 디스크 헤드의 충돌 등에 의해 데이터베이스의 일부 또는 전부가 물리적으로 손상된 상태

회복 관리기(Recovery Management)

- 회복 관리기는 DBMS의 구성 요소이다.
- 회복 관리기는 트랜잭션 실행이 성공적으로 완료되지 못하면 트랜잭션이 데이터베이스에 생성했던 모든 변화를 취소(Undo)*시키고, 트랜잭션 수행 이전의 원래 상태로 복구하는 역할을 담당한다.
- 메모리 덤프*, 로그(Log)*를 이용하여 회복을 수행한다.

취소(Undo)
로그(Log)에 보관한 정보를 이용하여 가장 최근에 변경된 내용부터 거슬러 올라가면서 트랜잭션 작업을 취소하여 원래의 데이터베이스로 복구합니다.

Dump와 Log
- **덤프(Dump)** : 주기적으로 데이터베이스 전체를 복사해 두는 것
- **로그(Log)** : 갱신되기 전후의 내용을 기록하는 별도의 파일로, 저널(Journal)이라고도 함

전문가의 조언

병행제어의 정의를 이해하고 목적을 암기하세요. 병행제어의 정의를 이해하면 목적은 어렵지 않게 기억할 수 있습니다.

다중 프로그래밍의 이점
- 프로세서의 이용률 증가
- 전체 트랜잭션의 작업 처리율 향상

2 병행제어(Concurrency Control)

병행제어란 다중 프로그램의 이점*을 활용하여 동시에 여러 개의 트랜잭션을 병행수행할 때, 동시에 실행되는 트랜잭션들이 데이터베이스의 일관성을 파괴하지 않도록 트랜잭션 간의 상호 작용을 제어하는 것이다.

- 병행제어의 목적
  - 데이터베이스의 공유를 최대화한다.
  - 시스템의 활용도를 최대화한다.
  - 데이터베이스의 일관성을 유지한다.
  - 사용자에 대한 응답 시간을 최소화한다.

3 병행수행의 문제점

병행제어 기법에 의한 제어 없이 트랜잭션들이 데이터베이스에 동시에 접근하도록 허용할 경우 갱신 분실, 비완료 의존성, 모순성, 연쇄 복귀 등의 문제점이 발생한다.

문제점	의미
갱신 분실 (Lost Update)	두 개 이상의 트랜잭션이 같은 자료를 공유하여 갱신할 때 갱신 결과의 일부가 없어지는 현상이다.
비완료 의존성 (Uncommitted Dependency)	• 하나의 트랜잭션 수행이 실패한 후 회복되기 전에 다른 트랜잭션이 실패한 갱신 결과를 참조하는 현상이다. • 임시 갱신이라고도 한다.
모순성 (Inconsistency)	• 두 개의 트랜잭션이 병행수행될 때 원치 않는 자료를 이용함으로써 발생하는 문제이다. • 불일치 분석(Inconsistent Analysis)이라고도 한다.
연쇄 복귀 (Cascading Rollback)	병행수행되던 트랜잭션들 중 어느 하나에 문제가 생겨 Rollback하는 경우 다른 트랜잭션도 함께 Rollback되는 현상이다.

전문가의 조언

병행수행 시 발생하는 문제점의 종류와 각각의 의미를 이해하세요.

기출문제 따라잡기 Section 177

이전기출

1. 트랜잭션들을 수행하는 도중 장애로 인해 손상된 데이터베이스를 손상되기 이전의 정상적인 상태로 복구시키는 작업은?

① Recovery ② Restart
③ Commit ④ Abort

회복은 말 그대로 원래의 상태로 복구하는 것이라 했죠!

이전기출

2. 트랜잭션의 병행제어 목적이 아닌 것은?

① 데이터베이스의 공유 최대화
② 시스템의 활용도 최대화
③ 데이터베이스의 일관성 최소화
④ 사용자에 대한 응답 시간 최소화

데이터베이스의 일관성 최소화가 아니고 일관성 유지입니다.

이전기출

3. 병행제어 기법을 적용하지 않을 경우 문제점 중 하나의 트랜잭션 수행이 실패한 후 회복되기 전에 다른 트랜잭션이 실패한 갱신 결과를 참조하는 현상은?

① Lost Update
② Inconsistency
③ Cascading Rollback
④ Uncommitted Dependency

비완료 의존성이란 말 그대로 무엇이 완료되기 전에 의존한다는 뜻이란 것을 염두에 두고 생각해 보세요.

▶ 정답 : 1. ① 2. ③ 3. ④

SECTION 178 ● LIVE

데이터 표준화

전문가의 조언

데이터 표준화는 업무에서 사용하는 일반 용어를 정보시스템에서 체계적으로 사용하려면 반드시 필요한 활동입니다. 데이터 표준화의 정의와 특징에 대해 알아두세요.

1 데이터 표준화의 정의

데이터 표준화는 시스템을 구성하는 데이터 요소의 명칭, 정의, 형식, 규칙에 대한 원칙을 수립하고 적용하는 것을 의미한다.

- 데이터 표준화 작업을 통해 사용자가 데이터를 정확히 이해하고 활용할 수 있도록 데이터 용어 및 항목 이름이 중복되지 않고 직관적이며 공통된 의미로 전달되도록 표준 항목명을 부여해야 한다.
- 데이터 표준화 작업을 통해 엔티티, 속성, 테이블, 컬럼 등 데이터 요소에서 사용되는 단어에 대해 일정한 규칙이 적용되도록 해야 한다.
- 데이터 표준화의 구성 요소에는 데이터 표준, 데이터 관리 조직, 데이터 표준화 절차가 있다.

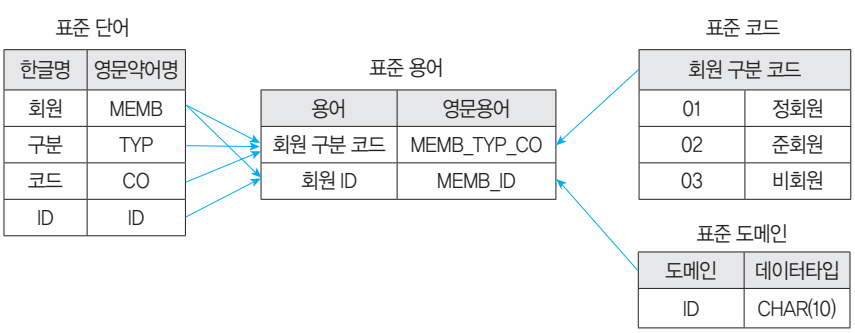
전문가의 조언

데이터 표준화의 구성 요소에는 어떤 것이 있는지 기억하고, 각각의 개념에 대해 알아두세요.

2 데이터 표준

데이터 표준은 데이터 모델이나 DB에서 정의할 수 있는 모든 오브젝트를 대상으로 데이터 표준화를 수행해야 한다.

- 데이터 표준의 종류
  - **표준 단어** : 업무에서 사용하고 일정한 의미를 갖고 있는 최소 단위의 단어를 의미한다.
  - **표준 도메인** : 문자형, 숫자형, 날짜형, 시간형과 같이 컬럼을 성질에 따라 그룹핑한 개념이다.
  - **표준 코드** : 선택할 수 있는 값을 정형화하기 위해 기준에 맞게 이미 정의된 코드 값으로, 도메인의 한 유형이다.
  - **표준 용어** : 단어, 도메인, 코드 표준이 정의되면 이를 바탕으로 표준 용어를 구성한다.



3 데이터 관리 조직

데이터 관리 조직은 데이터 표준 원칙이나 데이터 표준의 준수 여부 등을 관리하는 사람들로, 대표적으로 데이터 관리자가 있다.

- 데이터 관리자는 조직 내의 데이터에 대한 정의, 체계화, 감독 등의 업무를 담당한다.
- 데이터 관리자와 데이터베이스 관리자 비교

구분	데이터 관리자(DA)	데이터베이스 관리자(DBA)
관리 대상	데이터 모델, 각종 표준	데이터베이스
주요 업무	• 추가, 수정 등 사용자의 요구사항을 데이터에 반영 • 메타 데이터 정의	데이터베이스 관리
품질 관리	데이터 표준 관리 및 적용	데이터의 정합성 관리

4 데이터 표준화 절차

데이터 표준화는 데이터 표준화 요구사항 수집, 데이터 표준 정의, 데이터 표준 확정, 데이터 표준 관리 순으로 진행된다.

데이터 표준화 요구사항 수집	• 데이터 표준화와 관련된 요구사항 수집 • 시스템별 데이터 표준 수집 • 표준화 현황 진단
데이터 표준 정의	• 표준화 원칙 정의 • 표준 용어, 표준 단어, 표준 도메인, 표준 코드 등 데이터 표준 정의
데이터 표준 확정	데이터 표준 검토, 확정, 공표
데이터 표준 관리	• 데이터 표준 적용, 변경, 준수 검사 등 데이터 표준 관리 절차 수립 • 데이터 표준 이행

5 데이터 표준화의 대상

데이터 표준화의 대상으로는 데이터 명칭, 데이터 정의, 데이터 형식, 데이터 규칙이 있다.

데이터 명칭	데이터를 유일하게 구별할 수 있는 유일성, 의미 전달의 충분성, 그리고 업무적 보편성을 갖는 이름으로 정의해야 한다.
데이터 정의	데이터를 제3자의 입장에서도 쉽게 이해할 수 있도록 해당 데이터가 의미하는 범위 및 자격 요건 등을 규정한다.
데이터 형식	업무 규칙 및 사용 목적과 유사한 데이터에 대해 일관되게 데이터 형식을 정의함으로써 데이터 입력 오류, 통제 위험 등을 최소화한다.
데이터 규칙	기본 값, 허용 값, 허용 범위 등과 같이 발생할 수 있는 데이터 값을 사전에 지정함으로써 데이터의 정합성 및 완전성을 향상시킨다.

6 데이터 표준화의 기대 효과

- 동일한 데이터에 대해 동일한 명칭을 지정하면 명확한 의사소통이 가능하다.
- 표준화된 데이터를 사용하면 필요한 데이터의 의미나 위치 등을 쉽게 파악할 수 있다.
- 데이터 표준에 따라 데이터 형식 및 규칙을 적용하면 입력 오류를 방지하고 잘못된 데이터로 인한 의사 결정의 오류를 줄여 데이터 품질을 향상시킬 수 있다.
- 데이터 표준에 따라 데이터를 전사적으로 관리하면 시스템 간 데이터 공유 시 데이터 변환이나 정제 작업을 수행하지 않아도 된다.
- 향후 데이터 유지보수 및 운영의 효율성, 관리 비용을 절감할 수 있다.

기출문제 따라잡기 Section 178

출제예상

1. 다음 중 데이터 관리자(DA)의 역할에 대한 설명으로 틀린 것은?

① 사용자의 요구사항을 데이터에 반영
② 데이터 표준 정의
③ 데이터 모델 관리
④ 데이터베이스 관리

보기 중에 데이터베이스 관리자(DBA)의 역할이 있네요. 찾아보세요.

출제예상

2. 다음 중 데이터 표준화의 기대 효과로 가장 옳지 않은 것은?

① 명칭을 통일함으로 인해 의사소통이 증대된다.
② 필요한 데이터의 소재 파악에 소요되는 시간이 감소된다.
③ 일관된 데이터 형식 및 규칙을 적용함으로써 데이터 품질이 향상된다.
④ 시스템 간에 데이터 표준화 기준이 달라 데이터 변환 시간이 증대된다.

데이터 표준화는 시스템 간 실시되는 것이 아니라 전사적으로 실시되므로 시스템 간 데이터 변환 작업이 감소합니다.

출제예상

3. 다음 중 데이터 표준에 대한 설명으로 가장 거리가 먼 것은?

① 데이터 표준은 데이터 모델이나 DB에서 정의할 수 있는 모든 오브젝트를 대상으로 표준화를 수행해야 한다.
② 표준 도메인 : 문자형, 숫자형, 날짜형, 시간형과 같이 컬럼을 성질에 따라 그룹핑한 개념
③ 표준 코드 : 선택할 수 있는 값을 정형화하기 위해 기준에 따라 이미 정의된 코드 값
④ 표준 용어 : 업무에서 사용하고 일정한 의미를 갖고 있는 최소 단위의 단어

표준 단어와 표준 용어를 혼동하지 마세요. '회원', '구분', '코드', 'ID' 등과 같이 의미를 갖고 있는 최소 단위의 단어는 표준 단어, '회원구분코드', '회원ID' 등과 같이 단어를 조합해서 구성하는 것은 표준 용어입니다.

▶ 정답 : 1. ④ 2. ④ 3. ④

예·상·문·제·은·행

해설은 769쪽에 있습니다.

1. 다음은 무엇에 대한 설명인가?

- 인터넷을 기반으로 사람과 사물, 사물과 사물 간의 정보를 상호 소통하는 지능형 기술 및 서비스를 말한다.
- 인터넷에 연결된 기기가 사람의 개입 없이 상호간에 알아서 정보를 주고받아 처리한다.

① RFID(Radio Frequency Identification)
② IoT(Internet of Things)
③ SDN(Software Defined Networking)
④ M2M(Machine to Machine)

2. 다음 중 정보통신기술에 대한 설명으로 적당하지 않은 것은?

① 와이선(Wi-SUN)은 스마트 그리드와 같은 장거리 무선 통신을 필요로 하는 사물 인터넷(IoT) 서비스를 위한 저전력 장거리 통신기술이다.
② 클라우드 컴퓨팅(Cloud Computing)은 HW/SW 등의 자원을 자신이 필요한 만큼 빌려서 비용을 지불하는 방식의 서비스이다.
③ RFID는 모든 사물에 부착된 태그 또는 센서를 통해 탐지된 사물의 인식 정보는 물론 주변의 온도, 습도, 위치정보, 압력, 오염 및 균열 정도 등과 같은 환경 정보를 실시간으로 네트워크와 연결하여 수집하고 관리하는 네트워크 시스템이다.
④ 피코넷(PICONET)은 여러 개의 독립된 통신장치가 블루투스 기술이나 UWB 통신기술을 사용하여 통신망을 형성하는 무선 네트워크 기술이다.

3. 통신망(Communication Network)은 정보를 전달하기 위해서 통신 규약에 의해 연결한 통신 설비의 집합이다. 다음 중 통신망의 구성 형태에 대한 설명으로 틀린 것은?

① 성형(Star)은 중앙에 중앙 컴퓨터가 있고 이를 중심으로 단말장치들이 연결되는 중앙 집중식의 네트워크 구성 형태로, 각 단말장치들은 중앙 컴퓨터를 통하여 데이터를 교환한다.
② 링형(Ring)은 서로 이웃하는 컴퓨터 또는 단말장치들을 포인트 투 포인트(Point-to-Point) 방식으로 연결시킨 형태로, 양방향 링(Ring)의 경우 양쪽 방향으로 접근이 가능하여 통신 회선 장애에 대한 융통성이 있다.
③ 계층형(Tree)은 중앙 컴퓨터와 일정 지역의 단말장치까지는 하나의 통신 회선으로 연결하고, 이웃하는 단말장치는 일정 지역 내에 설치된 중간 단말장치로부터 다시 연결하는 형태이다.
④ 망형(Mesh)은 모든 지점의 컴퓨터와 단말장치를 서로 연결한 형태로, 많은 단말장치로부터 많은 양의 통신을 필요로 하는 경우에 유리하며, LAN에서 가장 많이 사용되는 방식이다.

4. LAN(Local Area Network)의 특징으로 옳지 않은 것은?

① 오류 발생률이 낮다.
② 통신 거리에 제한이 없다.
③ 경로 선택이 필요하지 않다.
④ 망에 포함된 자원을 공유한다.

5. 25개의 구간을 망형으로 연결하면 필요한 회선의 수는 몇 회선인가?

① 250 ② 300
③ 350 ④ 500

6. 흐름 제어란 통신망 내의 트래픽 제어의 원활한 흐름을 위해 망 내의 노드와 노드 사이에 전송하는 패킷의 양이나 속도를 규제하는 것이다. 흐름 제어를 위한 방식 중 슬라이딩 윈도우에 대한 설명으로 틀린 것은?

① 송신 측은 수신 측이 수신할 수 있는 최대 패킷의 수를 미리 통보받는다.
② 한 번에 여러 개의 패킷을 전송할 수 있다.
③ 전송 효율이 좋다.
④ 한 번에 하나의 패킷만을 전송할 수 있다.

7. 슬라이딩 윈도우 프로토콜에서 송신 윈도우가 증가하는 경우는 언제인가?

① 송신 측으로부터 이전에 송신한 프레임에 대한 긍정 수신 응답이 왔을 때
② 수신 측으로부터 이전에 송신한 프레임에 대한 긍정 수신 응답이 왔을 때
③ 수신 측으로부터 이전에 송신한 프레임에 대한 부정 수신 응답이 왔을 때
④ 증가되지 않는다.

8. 다음은 소프트웨어 관련 기술에 대한 설명이다. 가장 옳지 않은 것은?

① 블록체인(Blockchain) : P2P 네트워크를 이용하여 온라인 금융 거래 정보를 온라인 네트워크 참여자(Peer)의 디지털 장비에 분산 저장하는 기술
② CC(Common Criteria) : 정보화 순기능 역할을 보장하기 위해 정보화 제품의 정보보호 기능과 이에 대한 사용 환경 등급을 정한 기준

▶ **정답 :** 1. ② 2. ③ 3. ④ 4. ② 5. ② 6. ④ 7. ②

해설은 769쪽에 있습니다.

③ SOA(Service Oriented Architecture) : 애플리케이션 공유를 위한 웹 서비스를 그리드 상에서 제공하기 위해 만든 개방형 표준

④ 매시업(Mashup) : 웹에서 제공하는 정보 및 서비스를 이용하여 새로운 소프트웨어나 서비스, 데이터베이스 등을 만드는 기술

9. 다음 중 소프트웨어 개발에 참여하는 설계자(Designer)의 보안 활동으로 옳지 않은 것은?

① 특정 기술이 보안 요구사항을 만족하는지 확인하고 그 기술이 적절히 사용될 수 있도록 방법을 터득해야 한다.

② 다른 사람이 소프트웨어의 안전 여부를 쉽게 확인할 수 있도록 문서화 한다.

③ 문제 발생 시 최선의 문제 해결 방법을 결정한다.

④ 애플리케이션 보안 수준에 대한 품질 측정을 지원해야 한다.

10. 개인정보의 처리에 관한 기준과 개인정보 침해의 유형 및 예방조치 등에 관한 세부적인 사항을 규정하는 보안 활동과 관련된 법령은?

① 표준 개인 정보 보호 지침

② 개인정보 보호법

③ 개인정보의 안전성 확보 조치 기준

④ 정보통신망 이용촉진 및 정보보호 등에 관한 법률

11. 다음에서 설명하는 용어로 가장 옳은 것은?

- 한 번의 기록만으로 자료를 영구 보관할 수 있는 광 저장 장치이다.
- 디스크 표면의 무기물층에 레이저를 이용해 자료를 조각해서 기록한다.

① Blue-ray Disk ② M-DISC

③ Solid State Drive ④ Digital Video Disk

12. Secure OS의 보호 방법을 구현하기 복잡한 순서대로 옳게 나열된 것은?

① 암호적 분리 〉 논리적 분리 〉 시간적 분리 〉 물리적 분리

② 물리적 분리 〉 시간적 분리 〉 암호적 분리 〉 논리적 분리

③ 암호적 분리 〉 시간적 분리 〉 논리적 분리 〉 물리적 분리

④ 물리적 분리 〉 시간적 분리 〉 논리적 분리 〉 암호적 분리

13. Secure OS가 제공하는 보안 기능에 속하지 않는 것은?

① 객체 재사용 보호

② DAC 및 MAC

③ 네트워크 트래픽 제어

④ 신뢰 경로

14. 다음에서 설명하는 용어는 무엇인가?

- 일련의 데이터를 정의하고 설명해 주는 데이터이다.
- 컴퓨터에서는 데이터 사전의 내용, 스키마 등을 의미한다.

① 빅 데이터 ② 브로드 데이터

③ 메타 데이터 ④ 스마트 데이터

15. 많은 단말기로부터 많은 양의 통신을 필요로 하는 경우에 유리한 네트워크 형태는?

① 성형 망 ② 환형 망

③ 계층형 망 ④ 망형 망

16. 다음 중 소프트웨어 개발 보안 활동 주체별 역할로 옳지 않은 것은?

① 행전안전부 : 소프트웨어 개발 보안 정책 총괄, 법 · 지침 등 제도 정비

② 한국인터넷진흥원 : 소프트웨어 개발 보안 정책 및 가이드 개발

③ 발주기관 : 소프트웨어 개발 보안 능력을 갖춘 사업자 선정

④ 사업자 : 소프트웨어 개발 보안 계획 수립

17. 병행제어의 목적으로 옳지 않은 것은?

① 시스템 활용도 최대화

② 데이터베이스 공유도 최대화

③ 데이터베이스 일관성 유지

④ 사용자에 대한 응답시간 최대화

18. 다음 중 회복에 대한 설명이 아닌 것은?

① 장애를 일으켰을 때 일관적인 상태로 원상 복귀시켜 주는 기능

② 회복 관리기에 의해 수행

③ 덤프나 로그(저널)를 이용

④ 미디어의 모든 물리적 손상이 회복 가능

▶ **정답 :** 8. ③ 9. ② 10. ① 11. ② 12. ① 13. ③ 14. ③ 15. ④ 16. ④ 17. ④ 18. ④

예·상·문·제·은·행·해·설

1. Section 166

- RFID(Radio Frequency Identification) : 사물에 전자 태그를 부착하고 무선 통신을 이용하여 사물의 정보 및 주변 정보를 감지하는 센서 기술
- SDN(Software Defined Networking) : 네트워크를 컴퓨터처럼 모델링하여 여러 사용자가 각각의 소프트웨어 프로그램들로 네트워킹을 가상화하여 제어하고 관리하는 네트워크
- M2M(Machine to Machine) : 무선 통신을 이용한 기계와 기계 사이의 통신으로, 변압기 원격 감시, 전기, 가스 등의 원격 검침, 무선신용 카드 조회기, 무선 보안 단말기, 버스 운행 시스템, 위치 추적 시스템, 시설물 관리 등 무선으로 통합하여 상호 작용하는 통신

2. Section 166

- ③번의 내용은 USN(Ubiquitous Sensor Network)에 대한 설명이다.
- RFID(Radio Frequency Identification) : 사물에 전자 태그를 부착하고 무선 통신을 이용하여 사물의 정보 및 주변 정보를 감지하는 센서 기술

3. Section 167

- LAN에서는 주로 버스(Bus)형이나 링(Ring)형 구조를 사용한다.
- 망(Mesh)형은 공중 통신망에 사용되는 방식이다.

4. Section 167

LAN은 한 건물, 일정 지역 내 등으로 통신 거리가 제한되는 네트워크이다.

5. Section 167

망형 연결 시 필요 회선 수는

$$\frac{n(n-1)}{2} = \frac{25(25-1)}{2} = \frac{600}{2} = 300(\text{개})$$입니다.

6. Section 169

슬라이딩 윈도우(Sliding Window)

- 수신 측이 수신할 수 있는 최대 패킷의 수(윈도우 사이즈)를 정해서, 수신 측으로부터 확인 신호를 받지 않더라도 정해진 패킷의 수만큼은 연속적으로 전송할 수 있는 방식이다.
- 한 번에 여러 개의 패킷을 전송할 수 있으므로, 전송 효율이 좋다.

7. Section 169

송신 윈도우는 수신 측으로부터 확인 신호 없이도 수신 측으로 보낼 수 있는 패킷의 개수를 의미하는 것으로, 긍정 수신 응답이 있을 때 송신 윈도우를 증가시킬 수 있다.

8. Section 170

- ③번의 내용은 OGSA(Open Grid Service Architecture)에 대한 설명이다.
- SOA(Service Oriented Architecture) : 기업의 소프트웨어 인프라인 정보 시스템을 공유와 재사용이 가능한 서비스 단위나 컴포넌트 중심으로 구축하는 정보기술 아키텍처

9. Section 172

②번은 구현 개발자의 역할이다.

10. Section 173

- **개인정보 보호법** : 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호함
- **개인정보의 안전성 확보 조치 기준** : 개인정보 처리자가 개인정보를 처리하는데 개인정보가 분실, 도난, 유출, 위조, 변조, 훼손되지 않도록 안전성 확보에 필요한 기술적, 관리적, 물리적 안전조치에 관한 최소한의 기준을 규정함
- **정보통신망 이용촉진 및 정보보호 등에 관한 법률** : 정보통신망의 이용 촉진 및 정보통신 서비스를 이용하는 이용자들의 개인 정보를 보호함

11. Section 174

- **블루레이 디스크**(Blue-ray Disk) : 고선명(HD) 비디오를 위한 디지털 데이터를 저장할 수 있도록 만든 광 기록방식의 저장매체
- SSD(Solid State Drive) : 하드디스크 드라이브(HDD)와 비슷하게 동작하면서 HDD와는 달리 기계적 장치가 없는 반도체를 이용하여 정보를 저장하는 컴퓨터 보조기억장치
- DVD(Digital Video Disk) : 화질과 음질이 뛰어난 멀티미디어 데이터를 저장할 수 있는 대용량 저장 매체

12. Section 175

Secure OS의 보호 방법

- 암호적 분리(Cryptographic Separation) : 내부 정보를 암호화하는 방법
- 논리적 분리(Logical Separation) : 프로세스의 논리적 구역을 지정하여 구역을 벗어나는 행위를 제한하는 방법
- 시간적 분리(Temporal Separation) : 동일 시간에 하나의

예·상·문·제·은·행·해·설

프로세스만 수행되도록 하여 동시 실행으로 발생하는 보안 취약점을 제거하는 방법

- **물리적 분리(Physical Separation)** : 사용자별로 특정 장비만 사용하도록 제한하는 방법

13. Section 175

네트워크 트래픽을 제어하는 기능은 교환기나 스위치 등의 네트워크 장비가 수행해야 하는 기능이다. 네트워크 장비에 Secure OS가 설치될 수는 있겠지만 OS가 해당 기능을 제공한다고 보기는 어렵다.

14. Section 176

- **빅 데이터(Big Data)** : 기존의 관리 방법이나 분석 체계로는 처리하기 어려운 방대한 양의 정형 또는 비정형 데이터 집합
- **브로드 데이터(Broad Data)** : 다양한 채널에서 소비자와 상호 작용을 통해 생성된, 기업 마케팅에 있어 효율적이고 다양한 데이터이며, 이전에 사용하지 않거나 알지 못했던 새로운 데이터, 기존 데이터에 새로운 가치가 더해진 데이터
- **스마트 데이터((Smart Data)** : 실제로 가치를 창출할 수 있는 검증된 고품질의 데이터

15. Section 167

망형 망은 모든 지점의 컴퓨터와 단말기들이 포인트 투 포인트(Point-to-Point) 형식으로 연결된 형태이므로, 많은 단말기로부터 많은 양의 데이터를 전송할 때 유리하다.

16. Section 171

- 사업자의 역할에는 소프트웨어 개발 보안 관련 기술 수준 및 적용 계획 명시, 소프트웨어 개발 보안 관련 인력을 대상으로 교육 실시 등이 있다.
- 소프트웨어 개발 보안 계획 수립은 발주기관의 역할이다.

17. Section 177

병행제어(Concurrency Control)란 다중 프로그램의 이점을 활용하여 동시에 여러 개의 트랜잭션을 병행수행 할 때, 동시에 실행되는 트랜잭션들이 데이터베이스의 일관성을 파괴하지 않도록 트랜잭션 간의 상호작용을 제어하는 것으로 ①, ②, ③번의 목적과 사용자에 대한 응답시간을 최소화하기 위해 사용한다.

18. Section 177

DBMS의 구성 요소인 회복 관리기에 의해서 미디어의 물리적 손상을 회복시키는 것은 불가능하다. 이런 경우에 대비해 별도의 미디어에 수시로 Backup해 두는 것이 중요하다. 물리적 손상을 입으면 그 자체로는 회복시킬 수 없기 때문에 Backup해 둔 것을 재저장(Restore)시킴으로써 회복할 수 있다. 그러나 Backup한 내용까지만 회복이 가능하다.

3장 소프트웨어 개발 보안 구축

이 장에서 꼭 알아야 할 키워드 Best 10

1. 보안 요소 **2.** 시큐어 코딩 **3.** 세션 **4.** 레이스컨디션 **5.** SQL 삽입 **6.** 널 포인터 **7.** API **8.** 개인키 암호화 기법 **9.** 공개키 암호화 기법 **10.** 해시

SECTION 179 ● LIVE

Secure SDLC

전문가의 조언

SDLC는 소프트웨어를 개발하기 위한 모든 과정을 각 단계별로 나눈 것이며, Secure SDLC는 보안을 위해 SDLC의 전체 단계에 보안 강화를 위한 프로세스를 포함한 것입니다.

전문가의 조언

CLASP와 SDL은 서로 각기 다른 과정과 방법을 통해 Secure SDLC를 구성합니다. 먼저 이러한 종류의 방법론이 있다는 것을 기억해 두고, 기본적인 5단계에 적용되는 공통적인 사항을 머릿속에 잘 정리하세요.

소프트웨어 개발 생명주기(SDLC; Software Development Life Cycle)

소프트웨어 개발 생명주기는 소프트웨어 개발 방법론의 바탕이 되는 것으로, 소프트웨어를 개발하기 위해 정의하고 운용, 유지보수 등의 전 과정을 각 단계별로 나눈 것입니다. 자세한 설명은 Section 001을 참조하세요.

요구 수준

요구 수준은 해당 보안 정책 항목의 적용이 필수적인지 선택적인지를 의미합니다. 예를 들어, 주민번호는 정해진 수집 및 취급 방법이 법령에 있으므로 필수적으로 적용해야 합니다.

1 Secure SDLC의 개요

Secure SDLC는 보안상 안전한 소프트웨어를 개발하기 위해 SDLC*에 보안 강화를 위한 프로세스를 포함한 것을 의미한다.

- Secure SDLC는 소프트웨어의 유지 보수 단계에서 보안 이슈를 해결하기 위해 소모되는 많은 비용을 최소화하기 위해 등장하였다.
- Secure SDLC의 대표적인 방법론에는 Secure Software 사의 CLASP, Microsoft 사의 SDL이 있다.
- Secure SDLC는 요구사항 분석, 설계, 구현, 테스트, 유지 보수 등 SDLC 전체 단계에 걸쳐 수행되어야 할 보안 활동을 제시한다.

2 요구사항 분석 단계에서의 보안 활동

요구사항 분석 단계에서는 보안 항목에 해당하는 요구사항을 식별하는 작업을 수행한다.

- 전산화되는 정보가 가지고 있는 보안 수준을 보안 요소별로 등급을 구분하여 분류한다.
- 조직의 정보보호 관련 보안 정책을 참고하여 소프트웨어 개발에 적용할 수 있는 보안 정책 항목들의 출처, 요구 수준*, 세부 내용 등을 문서화한다.

보안 요소

보안 요소는 소프트웨어 개발에 있어 충족시켜야할 요소 및 요건을 의미합니다.

- 주요 보안 요소에는 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)이 있으며, 그 외에도 인증(Authentication), 부인 방지(NonRepudiation) 등이 있습니다.

기밀성	• 시스템 내의 정보와 자원은 인가된 사용자에게만 접근이 허용됩니다. • 정보가 전송 중에 노출되더라도 데이터를 읽을 수 없습니다.
무결성	시스템 내의 정보는 오직 인가된 사용자만 수정할 수 있습니다.
가용성	인가받은 사용자는 언제라도 사용할 수 있습니다.
인증	• 시스템 내의 정보와 자원을 사용하려는 사용자가 합법적인 사용자인지를 확인하는 모든 행위를 말합니다. • 대표적 방법으로는 패스워드, 인증용 카드, 지문 검사 등이 있습니다.
부인 방지	데이터를 송 · 수신한 자가 송 · 수신 사실을 부인할 수 없도록 송 · 수신 증거를 제공합니다.

3 설계 단계에서의 보안 활동

설계 단계에서는 식별된 보안 요구사항들을 소프트웨어 설계서에 반영하고, 보안 설계서를 작성한다.

- 소프트웨어에서 발생할 수 있는 위협*을 식별하여 보안대책, 소요예산, 사고 발생 시 영향 범위와 대응책 등을 수립한다.
- 네트워크, 서버, 물리적 보안, 개발 프로그램 등 환경에 대한 보안통제 기준을 수립하여 설계에 반영한다.
  - **네트워크** : 외부의 사이버 공격으로부터 개발 환경을 보호하기 위해 네트워크를 분리하거나 방화벽을 설치한다.
  - **서버** : 보안이 뛰어난 운영체제를 사용하고 보안 업데이트, 외부접속에 대한 접근통제 등을 실시한다.
  - **물리적 보안** : 출입통제, 개발 공간 제한, 폐쇄회로 등의 감시설비를 설치한다.
  - **개발 프로그램** : 허가되지 않은 프로그램을 통제하고 지속적인 데이터 무결성 검사를 실시한다.

위협(Threat)
위협이란 불법적인 유출, 위조, 변조, 삭제, 파손 등 소프트웨어에 발생할 수 있는 재산상의 손해를 말합니다.

4 구현 단계에서의 보안 활동

구현 단계에서는 표준 코딩 정의서* 및 소프트웨어 개발 보안 가이드*를 준수하며, 설계서에 따라 보안 요구사항들을 구현한다.

- 개발 과정 중에는 지속적인 단위 테스트*를 통해 소프트웨어에 발생할 수 있는 보안 취약점을 최소화해야 한다.
- 코드 점검 및 소스 코드 진단 작업을 통해 소스 코드의 안정성을 확보해야 한다.

시큐어 코딩(Secure Coding)

시큐어 코딩은 소프트웨어의 구현 단계에서 발생할 수 있는 보안 취약점들을 최소화하기 위해 보안 요소들을 고려하며 코딩하는 것을 의미합니다.

- 보안 취약점을 사전에 대응하여 안정성과 신뢰성을 확보하기 위해 사용됩니다.
- 보안 정책을 바탕으로 시큐어 코딩 가이드를 작성하고, 개발 참여자에게는 시큐어 코딩 교육을 실시해야 합니다.

표준 코딩 정의서
표준 코드 정의서는 코딩 시 다른 개발자나 운영자가 쉽게 접근할 수 있도록 클래스, 메소드 등의 네이밍 규칙, 주석 첨부 방식 등을 정의해 둔 문서입니다.

소프트웨어 개발 보안 가이드
소프트웨어 개발 보안 가이드는 안전한 소프트웨어 개발을 위해 정부에서 제작하여 배포하고 있는 지침입니다.

단위 테스트(Unit Test)
단위 테스트는 프로그램의 단위 기능을 구현하는 모듈이 정해진 기능을 정확히 수행하는지 검증하는 것입니다. 자세한 내용은 Section 039를 참조하세요.

5 테스트 단계에서의 보안 활동

테스트 단계에서는 설계 단계에서 작성한 보안 설계서를 바탕으로 보안 사항들이 정확히 반영되고 동작되는지 점검한다.

- 동적 분석 도구* 또는 모의 침투테스트를 통해 설계 단계에서 식별된 위협들의 해결여부를 검증한다.

동적 분석 도구
동적 분석 도구는 프로그램을 실제 또는 가상으로 실행시킨 상황에서 메모리 분석, 보안 취약점 검색, 오류 탐지 등의 다양한 기능을 수행하는 소프트웨어입니다.

- 설계 단계에서 식별된 위협들 외에도 구현 단계에서 추가로 제시된 위협들과 취약점들을 점검할 수 있도록 테스트 계획을 수립하고 시행한다.
- 테스트 단계에서 수행한 모든 결과는 문서화하여 보존하고, 개발자에게 피드백 되어야 한다.

6 유지보수 단계에서의 보안 활동

유지보수 단계에서는 이전 과정을 모두 수행하였음에도 발생할 수 있는 보안사고들을 식별하고, 사고 발생 시 이를 해결하고 보안 패치를 실시한다.

기출문제 따라잡기 Section 179

출제예상

1. 다음 중 Secure SDLC에 대한 설명으로 가장 옳지 않은 것은?

① 소프트웨어 개발 생명주기의 방법론에 보안 프로세스를 포함한 것이다.

② 보안 강화를 위한 유지 보수에 들어가는 비용을 최소화하기 위해 등장하였다.

③ Secure SDLC를 엄격히 준수하여 개발한 경우 보안으로 인한 유지보수 비용이 발생하지 않는다.

④ 소프트웨어 개발을 5단계로 구분하여 각 단계별로 수행해야할 프로세스를 분류하였다.

Secure SDLC를 통해 기존의 모든 보안 이슈들을 해결했어도 새로운 공격 방식에 의해 보안은 언제나 위협받을 수 있습니다. 새로운 보안 이슈가 생기면 업데이트를 해야 하는데 그러려면 무엇이 필요할까요?

출제예상

2. 시스템 내에 정보와 자원이 인가된 사용자에게만 허용되고, 전송 중에 노출되더라도 데이터를 읽을 수 없도록 하는 성질의 보안 요소를 무엇이라 하는가?

① 기밀성(Confidentiality)

② 무결성(Integrity)

③ 가용성(Availability)

④ 부인 방지(NonRepudiation)

무결성은 인가된 사용자만 데이터를 수정할 수 있도록 하는 것, 가용성은 인가받은 사용자는 언제든지 자원을 사용할 수 있도록 하는 것, 부인방지는 송 · 수신 사실의 부인을 막기 위해 증거를 제공하는 것입니다.

출제예상

3. Secure SDLC의 각 단계별로 수행할 내용으로 가장 잘못된 것은?

① 요구사항 분석 단계에서는 전산화되는 정보가 어느 정도의 보안등급을 가지고 있는지 분류한다.

② 요구사항 분석 단계에서는 보안 요구사항을 정의한다.

③ 설계 단계에서는 단위 테스트를 수행한다.

④ 구현 단계에서는 보안 요구사항들을 구현한다.

단위 테스트는 구현된 프로그램이 정상적으로 수행하는지 테스트 하는 것입니다. 단위 테스트는 어느 단계에서 수행할까요?

출제예상

4. 소프트웨어에서 발생할 수 있는 보안 취약점들을 최소화하기 위해 보안 위협 요소들을 고려하여 프로그래밍하는 것을 의미하는 용어는?

① Secure Coding

② Secure SDLC

③ Secure Architecture

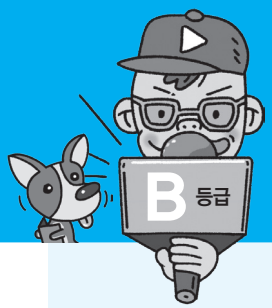
④ Secure Framework

Secure SDLC와 Secure Coding의 차이를 확실히 알아두세요. Secure SDLC가 소프트웨어 개발의 모든 과정에서 보안 위협 요소들을 고려한다면, Secure Coding은 소프트웨어 구현 단계에서 위협 요소들을 고려하며 코딩하는 것을 의미합니다.

▶ 정답 : 1. ③ 2. ① 3. ③ 4. ①

SECTION 180 LIVE

세션 통제



1 세션 통제의 개요

세션은 서버와 클라이언트의 연결을 의미하고, 세션 통제는 세션의 연결과 연결로 인해 발생하는 정보를 관리하는 것을 의미한다.

- 세션 통제는 소프트웨어 개발 과정 중 요구사항 분석 및 설계 단계에서 진단해야 하는 보안 점검 내용이다.
- 세션 통제의 보안 약점에는 불충분한 세션 관리, 잘못된 세션에 의한 정보 노출이 있다.

2 불충분한 세션 관리

불충분한 세션 관리는 일정한 규칙이 존재하는 세션ID*가 발급되거나 타임아웃이 너무 길게 설정되어 있는 경우 발생할 수 있는 보안 약점이다.

- 세션 관리가 충분하지 않으면 침입자는 세션 하이재킹*과 같은 공격을 통해 획득한 세션ID로 인가되지 않은 시스템의 기능을 이용하거나 중요한 정보에 접근할 수 있다.

3 잘못된 세션에 의한 정보 노출

잘못된 세션에 의한 정보 노출은 다중 스레드(Multi-Thread)* 환경에서 멤버 변수*에 정보를 저장할 때 발생하는 보안 약점이다.

- 싱글톤* 패턴에서 발생하는 레이스컨디션*으로 인해 동기화 오류가 발생하거나, 멤버 변수의 정보가 노출될 수 있다.
- 멤버 변수보다 지역 변수를 활용하여 변수의 범위를 제한함으로써 방지할 수 있다.

4 세션 설계시 고려 사항

- 시스템의 모든 페이지에서 로그아웃이 가능하도록 UI(User Interface)를 구성한다.
- 로그아웃 요청 시 할당된 세션이 완전히 제거되도록 한다.
- 세션 타임아웃은 중요도가 높으면 2~5분, 낮으면 15~30분으로 설정한다.
- 이전 세션이 종료되지 않으면 새 세션이 생성되지 못하도록 설계한다.
- 중복 로그인을 허용하지 않은 경우 클라이언트의 중복 접근에 대한 세션 관리 정책을 수립한다.
- 패스워드 변경 시 활성화된 세션을 삭제하고 재할당한다.

전문가의 조언

세션 통제의 정확한 의미를 이해하고, 세션 통제가 적절히 구현되지 않은 경우 발생할 수 있는 보안 약점들에 대해 알아두세요.

세션ID(SessionID)
세션ID는 서버가 클라이언트들을 구분하기 위해 부여하는 키(Key)로, 클라이언트가 서버에 요청을 보낼 때마다 세션ID를 통해 인증이 수행됩니다.

세션 하이재킹 (Session Hijacking)
세션 하이재킹은 서버에 접속하고 있는 클라이언트들의 세션 정보를 가로채는 공격 기법으로, 세션 가로채기라고도 합니다.

다중 스레드(Multi-Thread)
프로세스 내의 작업 단위로, 시스템의 자원을 할당받아 실행하는 프로그램의 단위를 스레드라고 하며, 두 개 이상의 스레드가 생성되어 동시 처리되는 다중 작업(Multitasking)을 다중 스레드 또는 멀티 스레드라고 부릅니다.

멤버 변수(Member Variable)
멤버 변수는 객체와 연결된 변수로, 클래스 내에 선언되어 클래스의 모든 메소드들이 접근 가능한 변수입니다. 멤버 필드라고도 부르며, 종류에는 클래스 변수, 인스턴스 변수가 있습니다.

싱글톤(Singleton)
싱글톤은 하나의 객체를 생성하면 생성된 객체를 어디서든 참조할 수 있지만, 여러 프로세스가 동시에 참조할 수는 없는 디자인 패턴입니다. 자세한 내용은 Section 026을 참조하세요.

레이스컨디션(Race Condition)
레이스컨디션은 두 개 이상의 프로세스가 공용 자원을 획득하기 위해 경쟁하고 있는 상태를 의미합니다.

5 세션ID의 관리 방법

- 세션ID는 안전한 서버에서 최소 128비트의 길이로 생성한다.
- 세션ID의 예측이 불가능하도록 안전한 난수 알고리즘을 적용한다.
- 세션ID가 노출되지 않도록 URL Rewrite* 기능을 사용하지 않는 방향으로 설계한다.
- 로그인 시 로그인 전의 세션ID를 삭제하고 재할당한다.
- 장기간 접속하고 있는 세션ID는 주기적으로 재할당되도록 설계한다.

URL Rewrite
URL Rewrite는 쿠키를 사용할 수 없는 환경에서 세션ID 전달을 위해 URL에 세션ID를 포함시키는 것입니다.

기출문제 따라잡기 Section 180

출제예상
1. 보안 점검과 관련하여 '세션 통제'에 대한 설명으로 가장 잘못된 것은?

① 서버와 클라이언트의 연결과 연결로 인해 발생하는 정보를 관리하는 것이다.
② 인가된 클라이언트만 시스템 자원에 접근할 수 있도록 통제하는 것을 말한다.
③ Secure SDLC의 요구사항 분석, 설계 단계에서 진단되어야 할 보안 점검 사항이다.
④ 보안 약점에는 불충분한 세션 관리, 잘못된 세션에 의한 정보 노출이 있다.

세션은 서버와 클라이언트의 연결만을 관리할 뿐, 각 세션이 가지고 있는 접근 권한을 통제하지는 않습니다.

출제예상
2. 다음 중 세션 설계 시 고려할 사항이 아닌 것은?

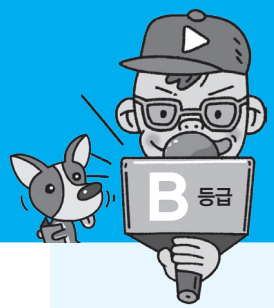
① 정해진 페이지에서만 로그아웃이 가능하도록 UI를 구성한다.
② 로그아웃 요청을 받으면 해당 세션이 완전히 삭제되도록 설계한다.
③ 이전 세션이 남아있는 경우 새 세션이 생성되지 못하도록 설계한다.
④ 패스워드 변경 시 활성화된 세션을 삭제한 후 재할당한다.

클라이언트가 언제든지 로그아웃을 할 수 있도록 모든 페이지에 로그아웃 버튼을 배치하는 것이 좋습니다.

▶ 정답 : 1. ② 2. ①

SECTION 181 ● LIVE

입력 데이터 검증 및 표현



1 입력 데이터 검증 및 표현의 개요

입력 데이터 검증 및 표현은 입력 데이터로 인해 발생하는 문제들을 예방하기 위해 구현 단계에서 검증해야 하는 보안 점검 항목들이다.

- 입력 데이터로 인해 발생하는 문제를 예방하기 위해서는 소프트웨어 개발의 구현 단계에서 유효성 검증 체계를 갖추고, 검증되지 않은 데이터가 입력되는 경우 이를 처리할 수 있도록 구현해야 한다.
- 입력 데이터를 처리하는 객체에 지정된 자료형이 올바른지 확인하고, 일관된 언어셋*을 사용하도록 코딩한다.

2 입력 데이터 검증 및 표현의 보안 약점

입력 데이터 검증 및 표현과 관련된 점검을 수행하지 않은 경우 SQL 삽입, 자원 삽입, 크로스사이트 스크립팅(XSS), 운영체제 명령어 삽입 등의 공격에 취약해진다.

- 보안 약점의 종류

SQL 삽입	• 입력란에 SQL을 삽입하여 무단으로 DB를 조회하거나 조작하는 보안 약점이다. • 동적 쿼리*에 사용되는 입력 데이터에 예약어 및 특수문자가 입력되지 않게 필터링 되도록 설정하여 방지할 수 있다.
경로 조작 및 자원 삽입	• 데이터 입출력 경로를 조작하여 서버 자원을 수정 · 삭제할 수 있는 보안 약점이다. • 사용자 입력값을 식별자로 사용하는 경우, 경로 순회* 공격을 막는 필터를 사용하여 방지할 수 있다.
크로스사이트 스크립팅(XSS)	• 웹페이지에 악의적인 스크립트*를 삽입하여 방문자들의 정보를 탈취하거나, 비정상적인 기능 수행을 유발하는 보안 약점이다. • HTML 태그의 사용을 제한하거나 스크립트에 삽입되지 않도록 '<', '>', '&' 등의 문자를 다른 문자로 치환함으로써 방지할 수 있다.
운영체제 명령어 삽입	• 외부 입력값을 통해 시스템 명령어의 실행을 유도함으로써 권한을 탈취하거나 시스템 장애를 유발하는 보안 약점이다. • 웹 인터페이스를 통해 시스템 명령어가 전달되지 않도록 하고, 외부 입력값을 검증 없이 내부 명령어로 사용하지 않음으로써 방지할 수 있다.
위험한 형식 파일 업로드	• 악의적인 명령어가 포함된 스크립트 파일을 업로드함으로써 시스템에 손상을 주거나, 시스템을 제어할 수 있는 보안 약점이다. • 업로드 되는 파일의 확장자 제한, 파일명의 암호화, 웹사이트와 파일 서버의 경로 분리, 실행 속성을 제거하는 등의 방법으로 방지할 수 있다.
신뢰되지 않는 URL 주소로 자동접속 연결	• 입력 값으로 사이트 주소를 받는 경우 이를 조작하여 방문자를 피싱 사이트로 유도하는 보안 약점이다. • 연결되는 외부 사이트의 주소를 화이트 리스트로 관리함으로써 방지할 수 있다.

전문가의 조언

- 소프트웨어 개발의 구현 단계에서 검증해야 하는 보안 점검 내용은 총 7가지로, 입력 데이터 검증 및 표현, 보안 기능, 시간 및 상태, 에러처리, 코드 오류, 캡슐화, API 오용으로 분류됩니다. 각 단계를 차례대로 살펴보도록 하겠습니다.
- 이번 섹션에서는 입력 데이터 및 표현과 관련된 보안 점검 내용과 이를 적절히 구현하지 않았을 경우 발생할 수 있는 보안 약점의 종류들에 대해 알아두세요.

언어셋(Character Set)
언어셋은 문자(Character)를 컴퓨터에서 처리하기 위해 사용하는 코드표를 의미하며, 종류에는 ASCII, UNICODE, UTF-8 등이 있습니다.

전문가의 조언

입력 데이터 검증 및 표현 미비로 발생하는 보안 약점에는 왼쪽의 6가지 이외에도 XQuery/XPath/LDAP/포맷 스트링 삽입, 크로스사이트 요청 위조, HTTP 응답 분할, 정수형/메모리 버퍼 오버플로우, 보안기능 결정에 사용되는 부적절한 입력값 등이 있습니다.

동적 쿼리(Dynamic Query)
동적 쿼리는 질의어 코드를 문자열 변수에 넣어 조건에 따라 질의를 동적으로 변경하여 처리하는 방식을 의미합니다. 자세한 내용은 Section 111을 참조하세요.

경로 순회(Directory Traversal)
경로를 탐색할 때 사용하는 '/', '\', '..' 등의 기호를 악용하여 허가되지 않은 파일에 접근하는 방식입니다.

스크립트(Script)
소프트웨어를 수행하는데 필요한 처리 절차가 기록된 텍스트로, 대표적인 스크립트 파일의 확장자에는 asp, jsp, php 등이 있습니다.

기출문제 따라잡기 Section 181

출제예상

1. 보안 점검 관련 내용 중 입력 데이터 검증 및 표현과 관련된 설명으로 가장 잘못된 것은?

① 잘못된 또는 악의적인 입력 데이터로 인해 프로그램의 권한 탈취, 오류 등을 방지하기 위함이다.

② 입력 데이터가 올바른 자료형으로 취급되는지 확인해야 한다.

③ 입력 데이터의 언어셋은 가능한 다양하게 활용하여 해독하기 어렵게 만들어야 한다.

④ 충분한 조치가 취해지지 않을 경우 SQL 삽입, 크로스사이트 스크립팅(XSS) 등의 외부 공격에 취약해진다.

언어셋은 하나로 통일하여 사용하지 않으면 코드 작성 시 혼동될 뿐만 아니라 필요치 않은 변환 과정이 추가되어 프로그램의 수행 능력을 떨어뜨릴 수 있습니다.

출제예상

2. 보안 점검 내용 중 '입력 데이터 검증 및 표현'과 관련된 보안 약점에 해당하지 않는 것은?

① SQL 삽입

② 경로 조작 및 자원 삽입

③ 크로스사이트 스크립팅(XSS)

④ 취약한 암호화 알고리즘

입력 데이터와 관계없는 사항을 찾아보세요. ①번은 입력 데이터로 SQL을, ②번은 경로를, ③번은 스크립트를 삽입하여 소프트웨어에 문제를 일으킵니다.

출제예상

3. 다음 중 웹페이지에 악의적인 스크립트를 삽입하여 방문자들의 정보를 탈취하거나 비정상적인 기능 수행을 유발하지 못하도록 방지하는 방법으로 가장 옳은 것은?

① 연결되는 외부 사이트의 주소를 화이트 리스트로 관리한다.

② 웹 인터페이스를 통해 시스템 명령어가 전달되지 않도록 한다.

③ HTML 태그의 사용을 제한하거나 '<', '>' 등의 문자를 다른 문자로 치환한다.

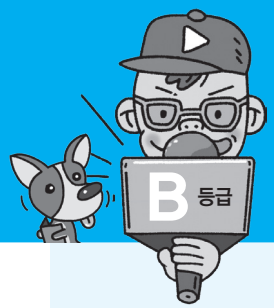
④ 동적 쿼리에 사용되는 입력 데이터에 예약어나 특수 문자가 입력되지 않도록 설정한다.

각각의 보안 약점에 대비하는 방법을 알아두어야 합니다. 답을 모르겠다면 다시 공부하고 오세요.

▶ 정답 : 1. ③ 2. ④ 3. ③

SECTION 182 LIVE

보안 기능



1 보안 기능의 개요

보안 기능은 소프트웨어 개발의 구현 단계에서 코딩하는 기능인 인증, 접근제어, 기밀성, 암호화 등을 올바르게 구현하기 위한 보안 점검 항목들이다.

- 각 보안 기능들은 서비스 환경이나 취급 데이터에 맞게 처리될 수 있도록 구현해야 한다.
- 소프트웨어의 기능 또는 데이터에 접근하려는 사용자별로 중요도를 구분하고, 차별화된 인증 방안을 적용한다.
- 인증된 사용자가 이용할 기능과 데이터에 대해 개별적으로 접근 권한을 부여하여 인가되지 않은 기능과 데이터로의 접근을 차단한다.
- 개인정보나 인증정보와 같은 중요한 정보의 변조 · 삭제 · 오남용 등을 방지하기 위해 안전한 암호화 기술을 적용한다.

2 보안 기능의 보안 약점

보안 기능에 대한 점검을 수행하지 않을 경우 인증 없이 중요한 기능을 허용하거나 비밀번호가 노출되는 등 다음과 같은 보안 약점이 발생할 수 있다.

적절한 인증 없이 중요기능 허용	• 보안검사를 우회하여 인증과정 없이 중요한 정보 또는 기능에 접근 및 변경이 가능하다. • 중요정보나 기능을 수행하는 페이지에서는 재인증 기능을 수행하도록 하여 방지할 수 있다.
부적절한 인가	• 접근제어 기능이 없는 실행경로를 통해 정보 또는 권한을 탈취할 수 있다. • 모든 실행경로에 대해 접근제어 검사를 수행하고, 사용자에게는 반드시 필요한 접근 권한만을 부여하여 방지할 수 있다.
중요한 자원에 대한 잘못된 권한 설정	• 권한 설정이 잘못된 자원에 접근하여 해당 자원을 임의로 사용할 수 있다. • 소프트웨어 관리자만 자원들을 읽고 쓸 수 있도록 설정하고, 인가되지 않은 사용자의 중요 자원에 대한 접근 여부를 검사함으로써 방지할 수 있다.
취약한 암호화 알고리즘 사용	• 암호화된 환경설정 파일을 해독하여 비밀번호 등의 중요정보를 탈취할 수 있다. • 안전한 암호화 알고리즘을 이용하고, 업무관련 내용이나 개인정보 등에 대해서는 IT 보안인증사무국*이 안정성을 확인한 암호모듈을 이용함으로써 방지할 수 있다.
중요정보 평문 저장 및 전송	• 암호화되지 않은 평문 데이터를 탈취하여 중요한 정보를 획득할 수 있다. • 중요한 정보를 저장하거나 전송할 때는 반드시 암호화 과정을 거치도록 하고, HTTPS* 또는 SSL*과 같은 보안 채널을 이용함으로써 방지할 수 있다.
하드코드*된 비밀번호	• 소스코드 유출 시 내부에 하드코드된 패스워드를 이용하여 관리자 권한을 탈취할 수 있다. • 패스워드는 암호화하여 별도의 파일에 저장하고, 디폴트 패스워드*나 디폴드 키의 사용을 피함으로써 방지할 수 있다.

전문가의 조언

보안 점검 내용 중 하나인 보안 기능의 정확한 의미를 이해하고, 보안 기능이 적절히 구현되지 않은 경우 발생할 수 있는 보안 약점과 이를 방지하기 위한 방법에 대해 알아두세요.

전문가의 조언

보안 기능과 관련된 내용을 점검하지 않아 발생하는 보안 약점에는 왼쪽의 6가지 이외에도 충분하지 않은 키 길이 사용, 적절하지 않은 난수값 사용, 하드코드된 암호화 키, 취약한 비밀번호 허용, 사용자 하드디스크에 저장되는 쿠키를 통한 정보 노출, 주석문 안에 포함된 시스템 주요정보, 솔트 없이 일방향 해시함수 사용, 무결성 검사 없는 코드 다운로드, 반복된 인증 시도 제한 기능 부재가 있습니다.

IT보안인증사무국
정보보호제품의 평가 · 인증을 수행하고 인증제품 목록을 공개 및 관리하는 국가보안기술연구소 산하의 인증기관입니다.

HTTPS(Hypertext Transfer Protocol Secure)
웹브라우저와 서버 간의 안전한 통신을 위해 HTTP와 암호통신규약을 결합한 것입니다.

SSL(Secure Sockets Layer)
데이터를 송 · 수신하는 두 컴퓨터 사이에 위치하여 인증, 암호화, 무결성을 보장하는 업계 표준 프로토콜입니다.

하드코드
데이터를 코드 내부에 직접 입력하여 프로그래밍하는 방식입니다.

디폴트 패스워드(Default Password)
사용자를 등록하기 전에 설치 권한을 획득하기 위해 사용되는 초기 설정 암호입니다.

기출문제 따라잡기 Section 182

출제예상

1. 보안 점검 내용 중 보안 기능과 관련된 설명으로 가장 옳지 않은 것은?

① 인증, 접근제어, 암호화 등이 올바르게 처리될 수 있도록 코딩 되었는지 확인하는 것을 의미한다.

② 기능과 사용자에 따라 차별화된 인증 방안을 적용해야 한다.

③ 잘못된 입력 데이터로 소프트웨어의 기능이 훼손되지 않도록 유효성 검증 체계를 갖춘다.

④ 중요 정보는 암호화 기술을 적용하여 취급해야 한다.

유효성 검증 체계를 갖추는 것은 보안 기능이 아닌 '입력 데이터 검증 및 표현'과 관련된 내용입니다.

출제예상

2. 소프트웨어 개발의 구현 단계에서 보안 기능의 점검 미비로 인해 발생할 수 있는 보안 약점에 해당하지 않는 것은?

① 종료되지 않은 반복문 또는 재귀함수

② 부적절한 인가

③ 중요한 자원에 대한 잘못된 권한 설정

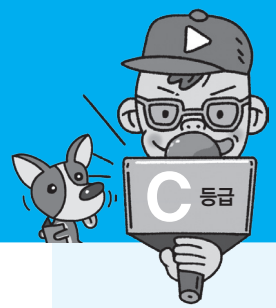
④ 적절한 인증 없이 중요기능 허용

'보안 기능'은 인증, 접근제어, 기밀성, 암호화와 관련이 있습니다. 이것과 관련 없는 보기를 찾아보세요.

▶ 정답 : 1. ③ 2. ①

SECTION 183 ● LIVE

시간 및 상태



1 시간 및 상태의 개요

시간 및 상태는 동시 수행을 지원하는 병렬 처리 시스템이나 다수의 프로세스가 동작하는 환경에서 시간과 실행 상태를 관리하여 시스템이 원활하게 동작되도록 하기 위한 보안 검증 항목들이다.

- 시간 및 상태를 점검하지 않은 코딩이 유발하는 보안 약점에는 TOCTOU 경쟁 조건, 잘못된 반복문 · 재귀함수 등이 있다.
- 시간 및 상태의 점검 미비로 발생하는 각종 오류들은 공격자에 의해 악용될 수 있다.

2 TOCTOU 경쟁 조건

TOCTOU 경쟁 조건은 검사 시점(Time Of Check)과 사용 시점(Time Of Use)을 고려하지 않고 코딩하는 경우 발생하는 보안 약점이다.

- 검사 시점에는 사용이 가능했던 자원이 사용 시점에는 사용할 수 없게 된 경우에 발생한다.
- 프로세스가 가진 자원 정보와 실제 자원 상태가 일치하지 않는 동기화 오류, 교착상태* 등이 발생할 수 있다.
- 코드 내에 동기화 구문*을 사용하여 해당 자원에는 한 번에 하나의 프로세스만 접근 가능하도록 구성함으로써 방지할 수 있다.
- 동기화 구문은 성능 감소를 동반하기 때문에 반드시 필요한 부분에 한정하여 사용해야 한다.

3 종료되지 않는 반복문 또는 재귀함수

반복문이나 재귀함수*에서 종료 조건을 정의하지 않았거나 논리 구조상 종료될 수 없는 경우 발생하는 보안 약점이다.

- 반복문이나 재귀함수가 종료되지 않을 경우 시스템 자원이 끊임없이 사용되어 자원고갈로 인한 서비스 장애 또는 시스템 장애가 발생한다.
- 모든 반복문이나 재귀함수의 수행 횟수를 제한하는 설정을 추가하거나, 종료 조건을 점검하여 반복 또는 호출의 종료 여부를 확인함으로써 방지할 수 있다.

전문가의 조언

보안 점검 내용 중 '시간 및 상태'와 관련된 내용입니다. 시간과 실행 상태 등으로 인해 발생할 수 있는 보안 약점에 대해 확실히 알아두세요.

전문가의 조언

경쟁 조건(Race Condition)은 두 개 이상의 프로세스가 공용 자원을 획득하기 위해 경쟁하고 있는 상태를 의미하며, 여기서는 검사 시점(TOC)과 사용 시점(TOU)의 차이로 발생하는 경쟁 조건을 가리킵니다. 예를 들어, 프로세스 A가 자원 X를 사용하기 위해 검사한 결과 X는 사용 가능한 자원임을 확인했습니다(TOC). 이제 사용하기 위해 X를 요청하였더니(TOU) 그 사이에 프로세스 B가 A보다 먼저 X에 대한 사용 요청을 내고 사용해 버림으로써 A는 X를 사용할 수 없는 상황이 여기에 해당합니다.

교착상태(Deadlock)

교착상태는 둘 이상의 프로세스들이 자원을 점유한 상태에서 서로 다른 프로세스가 점유하고 있는 자원을 요구하며 무한정 기다리는 현상입니다.

동기화 구문

동기화 구문은 공유 자원에 대해 둘 이상의 프로세스가 접근하는 것을 막는 구문으로, Synchronized, Mutex 등이 있습니다.

재귀 함수(Recursive Function)

재귀 함수는 자기가 자기를 호출하는 순환 프로그램입니다.

기출문제 따라잡기 Section 183

출제예상

1. 보안 점검 내용 중 시간 및 상태와 관련된 설명으로 가장 옳지 않은 것은?

① 병렬 처리 시스템이나 다수의 프로세스가 동작하는 환경에서 점검해야 하는 사항이다.

② 프로세스가 수행되는 시간 및 실행 상태를 점검하여 원활히 동작되도록 점검해야 한다.

③ 시간 및 상태를 고려하지 않고 코딩하는 경우 교착상태, 시스템 정지 등에 빠질 수 있다.

④ 코딩 시 접근 제어를 위한 구문을 추가하여 교착상태를 예방할 수 있다.

접근 제어는 사용자에 따라 데이터 또는 기능에 접근할 수 있는 권한을 제어하는 방법으로, 접근 제어를 통해 교착상태를 예방할 수는 없습니다.

출제예상

2. 다음 설명이 의미하는 것은?

- 시간 및 상태와 관련된 점검을 수행하지 않고 코딩했을 때 발생하는 보안 약점이다.
- 검사 시점과 사용 시점에 자원 상태가 서로 다른 경우 발생한다.
- 동기화 오류, 교착상태 등이 발생할 수 있으며, 코드 내 동기화 구문을 사용하여 방지할 수 있다.

① XSS

② 경쟁조건 : TOCTOU

③ 종료되지 않는 반복문 또는 재귀함수

④ 충분하지 않은 키 길이 사용

검사 시점(Time Of Check)과 사용 시점(Time Of Use)의 영문 앞 글자를 따라 읽어보세요.

출제예상

3. 하나의 프로그램에서 두 개 이상의 프로세스가 공용 자원을 사용하기 위해 동시에 경쟁하며 접근하는 상황을 가리키는 용어는 무엇인가?

① 레이스컨디션(Race Condition)

② 교착상태(Deadlock)

③ 병행제어(Concurrency Control)

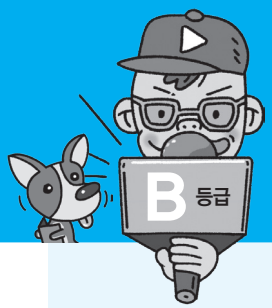
④ 동기화 오류(Synchronization Error)

문제에 답이 나와 있습니다. 경쟁(Race)하는 상황(Condition)이 무엇일까요?

▶ 정답 : 1. ④ 2. ② 3. ①

SECTION 184 LIVE

에러처리



1 에러처리의 개요

에러처리*는 소프트웨어 실행 중 발생할 수 있는 오류(Error)들을 사전에 정의하여 오류로 인해 발생할 수 있는 문제들을 예방하기 위한 보안 점검 항목들이다.

- 각 프로그래밍 언어의 예외처리 구문을 통해 오류에 대한 사항을 정의한다.
- 예외처리 구문으로 처리하지 못한 오류들은 중요정보를 노출시키거나, 소프트웨어의 실행이 중단되는 등 예기치 못한 문제를 발생시킬 수 있다.
- 에러처리의 미비로 인한 코딩이 유발하는 보안 약점에는 오류 메시지를 통한 정보 노출, 오류 상황 대응 부재, 부적절한 예외처리가 있다.

2 오류 메시지를 통한 정보노출

오류 메시지를 통한 정보노출은 오류 발생으로 실행 환경, 사용자 정보, 디버깅 정보 등의 중요 정보를 소프트웨어가 메시지로 외부에 노출하는 보안 약점이다.

- 오류 메시지를 통해 노출되는 경로 및 디버깅 정보는 해커의 악의적인 행위를 도울 수 있다.
- 예외처리 구문에 예외의 이름이나 스택 트레이스*를 출력하도록 코딩한 경우 해커는 소프트웨어의 내부구조를 쉽게 파악할 수 있다.
- 오류 발생 시 가능한 한 내부에서만 처리되도록 하거나 메시지를 출력할 경우 최소한의 정보 또는 사전에 준비된 메시지만 출력되도록 함으로써 방지할 수 있다.

3 오류 상황 대응 부재

오류 상황 대응 부재는 소프트웨어 개발 중 예외처리를 하지 않았거나 미비로 인해 발생하는 보안 약점이다.

- 예외처리를 하지 않은 오류들로 인해 소프트웨어의 실행이 중단되거나 의도를 벗어난 동작이 유도될 수 있다.
- 오류가 발생할 수 있는 부분에 예외처리 구문을 작성하고, 제어문을 활용하여 오류가 악용되지 않도록 코딩함으로써 방지할 수 있다.

전문가의 조언

보안 점검 내용 중 '에러처리'와 관련된 내용입니다. 에러처리로 인해 발생할 수 있는 보안 약점에 대해 확실히 알아두세요.

에러처리

에러는 오류의 영문명이며, 예외처리(Exception Handling)와 에러(오류)처리(Trouble Shooting)는 동일한 의미로 사용됩니다.

스택 트레이스(Stack Trace)

스택 트레이스는 오류가 발생한 위치를 추적하기 위해 소프트웨어가 실행 중에 호출한 메소드의 리스트를 기록한 것입니다.

전문가의 조언

메모리 부족, 잘못된 주소 참조 등 다양한 오류들이 발생할 수 있습니다. 이 때 오류들을 개별적으로 처리하지 않고 그저 '오류가 나면 이렇게 해라'라는 식으로 단순하게 예외처리를 해버리게 되면 작업이 조금만 복잡해져도 간단한 오류에 멈춰버리거나, 필요한 값이 할당되지 않는 등 예기치 못한 다양한 문제가 발생할 수 있습니다.

4 부적절한 예외처리

부적절한 예외처리는 함수의 반환값 또는 오류들을 세분화하여 처리하지 않고 광범위하게 묶어 한 번에 처리하거나, 누락된 예외가 존재할 때 발생하는 보안 약점이다.

- 모든 오류들을 세세하게 정의하여 처리할 필요는 없지만, 모든 오류들을 광범위한 예외처리 구문으로 정의해 버리면 예기치 않은 문제가 발생할 수 있다.
- 함수 등이 예상했던 결과와 다른 값을 반환하여 예외로 처리되지 않은 경우 잘못된 값으로 인해 다양한 문제가 발생할 수 있다.
- 모든 함수의 반환값이 의도대로 출력되는지 확인하고, 세분화된 예외처리를 수행함으로써 방지할 수 있다.

기출문제 따라잡기 Section 184

출제예상

1. 점검 내용 중 에러처리와 관련된 내용으로 잘못된 것은?

① 소프트웨어에서 발생할 수 있는 오류들을 사전에 정의하면 대비할 수 있다.

② 각 프로그래밍 언어의 예외처리 구문을 통해서 오류들을 정의할 수 있다.

③ 에러처리와 관련된 보안 약점에는 오류 메시지를 통한 정보노출, 오류 상황 대응 부재, 부적절한 예외처리가 있다.

④ 에러처리가 충분히 이루어지지 않는 경우 교착상태, 레이스컨디션 등이 발생할 수 있다.

교착상태나 레이스컨디션은 자원이나 데이터를 획득하기 위해 두 개 이상의 프로세스가 경쟁할 때 발생합니다.

출제예상

2. 보안 점검 내용 중 에러처리에서 발생할 수 있는 보안 약점에 해당하지 않는 것은?

① 부적절한 인가

② 부적절한 예외처리

③ 오류 메시지를 통한 정보노출

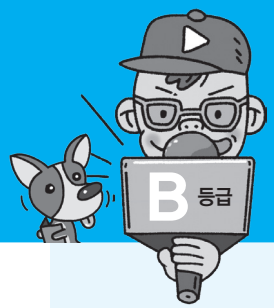
④ 오류 상황 대응 부재

부적절한 인가는 보안 기능과 관련된 보안 약점입니다.

▶ 정답 : 1. ④ 2. ①

SECTION 185 LIVE

코드 오류



1 코드 오류의 개요

코드 오류는 소프트웨어 구현 단계에서 개발자들이 코딩 중 실수하기 쉬운 형(Type) 변환, 자원 반환 등의 오류를 예방하기 위한 보안 점검 항목들이다.

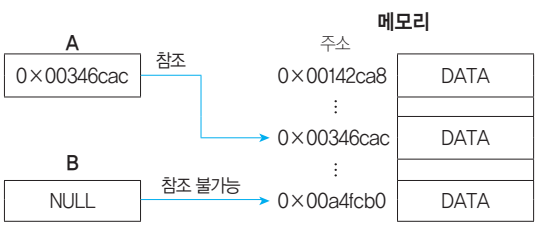
- 코드 오류로 발생할 수 있는 보안 약점에는 널 포인터* 역참조, 부적절한 자원 해제, 해제된 자원 사용, 초기화되지 않은 변수 사용이 있다.

2 널 포인터(Null Pointer) 역참조

널 포인터 역참조는 널 포인터가 가리키는 메모리에 어떠한 값을 저장할 때 발생하는 보안 약점이다.

- 많은 라이브러리 함수들이 오류가 발생할 경우 널 값을 반환하는데, 이 반환값을 포인터로 참조하는 경우 발생한다.
- 대부분의 운영체제에서 널 포인터는 메모리의 첫 주소를 가리키며, 해당 주소를 참조할 경우 소프트웨어가 비정상적으로 종료될 수 있다.
- 공격자가 널 포인터 역참조로 발생하는 예외 상황을 악용할 수 있다.
- 널이 될 수 있는 포인터를 이용하기 전에 널 값을 갖고 있는지 검사함으로써 방지할 수 있다.

예제 다음은 A와 B를 포인터로 해서 참조하는 메모리에 값을 저장하는 경우 발생하는 상황이다.



해설

- A를 포인터로 해서 참조하는 경우 A에는 정상적인 메모리 주소가 저장되어 있으므로 해당 위치의 메모리에 값을 저장할 수 있습니다.
- B를 포인터로 해서 참조하는 경우 B에는 NULL이 저장되어 있어 참조가 불가능하여 오류가 발생합니다. 공격자는 이러한 오류로 발생하는 예외 상황을 이용하여 추후 공격을 계획하는데 사용할 수 있습니다.

전문가의 조언

보안 점검 내용 중 '코드 오류'에 대한 내용입니다. 코드 오류와 관련된 보안 약점에 대해 확실히 알아두세요.

널 포인터(Null Pointer)

널(Null)은 값이 없음을 의미하며, 포인터(Pointer)는 메모리의 위치를 가리키는 요소입니다. 널 포인터(Null Pointer)는 포인터에 널이 저장되어 어떠한 곳도 가리키지 못하는 상태의 요소를 말합니다.

전문가의 조언

널 포인터 역참조로 오류가 발생하는 경우 "메모리 0×00000000을 참조하였습니다."라는 오류 메시지가 발생합니다.

3 부적절한 자원 해제

부적절한 자원 해제는 자원을 반환하는 코드를 누락하거나 프로그램 오류로 할당된 자원을 반환하지 못했을 때 발생하는 보안 약점이다.

- 힙 메모리(Heap Memory)*, 소켓(Socket)* 등의 유한한 시스템 자원이 계속 점유하고 있으면 자원 부족으로 인해 새로운 입력을 처리하지 못 할 수 있다.
- 프로그램 내에 자원 반환 코드가 누락되었는지 확인하고, 오류로 인해 함수가 중간에 종료되었을 때 예외처리에 관계없이 자원이 반환되도록 코딩함으로써 방지할 수 있다.

힙 메모리(Heap Memory)
힙 메모리는 소프트웨어가 자유롭게 사용할 수 있는 메모리 공간입니다.

소켓(Socket)
소켓은 데이터 교환을 위한 통로입니다.

4 해제된 자원 사용

해제된 자원 사용은 이미 사용이 종료되어 반환된 메모리를 참조하는 경우 발생하는 보안 약점이다.

- 반환된 메모리를 참조하는 경우 예상하지 못한 값 또는 코드를 수행하게 되어 의도하지 않은 결과가 발생할 수 있다.
- 반환된 메모리에 접근할 수 없도록 주소를 저장하고 있는 포인터를 초기화함으로써 방지할 수 있다.

5 초기화되지 않은 변수 사용

초기화되지 않은 변수 사용은 변수 선언 후 값이 부여되지 않은 변수를 사용할 때 발생하는 보안 약점이다.

- 변수가 선언되어 메모리가 할당되면 해당 메모리에 이전에 사용하던 내용이 계속 남아있어 변수가 외부에 노출되는 경우 중요정보가 악용될 수 있다.
- 변수 선언 시 할당된 메모리를 초기화함으로써 방지할 수 있다.

기출문제 따라잡기 Section 185

출제예상
1. 코드 오류로 인한 부적절한 자원 해제가 발생하지 않도록 방지하는 방법에 해당하는 것은?

① 포인터 사용 전에 널 값 확인
② 예외처리와 관계없이 자원 반환
③ 자원 반환 후 해당 자원을 참조하는 포인터 초기화
④ 변수 선언 시 할당된 메모리에 초기값 부여

①번은 널 포인터 역참조, ③번은 해제된 자원 사용, ④번은 초기화되지 않은 변수 사용을 방지하는 방법입니다.

출제예상
2. 다음 중 코드 오류와 관련된 보안 약점에 대한 설명으로 가장 옳지 않은 것은?

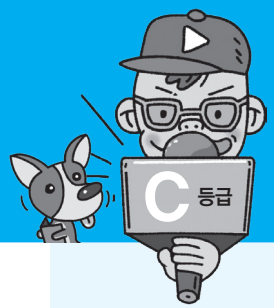
① 널 포인터가 가리키는 메모리에 값을 저장하면 오류가 발생한다.
② 널 포인터 역참조를 방지하려면 널 포인터를 초기화해야 한다.
③ 자원을 획득해서 사용한 다음에는 반드시 해제하여 반환해야 하는데, 그렇지 않을 경우 문제가 발생한다.
④ 이미 사용이 종료된 반환 메모리를 참조하지 않기 위해서는 주소를 저장하고 있는 포인터를 초기화한다.

널(Null)은 값이 없음을 의미합니다. 이미 값이 없는데 초기화 할 필요가 있을까요?

▶ 정답 : 1. ② 2. ②

SECTION
186
LIVE

캡슐화



1 캡슐화의 개요

캡슐화*는 정보 은닉이 필요한 중요한 데이터와 기능을 불충분하게 캡슐화하거나 잘못 사용함으로써 발생할 수 있는 문제를 예방하기 위한 보안 점검 항목들이다.

- 캡슐화로 인해 발생할 수 있는 보안 약점에는 잘못된 세션에 의한 정보 노출, 제거되지 않고 남은 디버그 코드, 시스템 데이터 정보 노출 등이 있다.

2 잘못된 세션에 의한 정보 노출

잘못된 세션에 의한 정보 노출은 다중 스레드(Multi-Thread)* 환경에서 멤버 변수*에 정보를 저장할 때 발생하는 보안 약점이다.

- 싱글톤* 패턴에서 발생하는 레이스컨디션으로 인해 동기화 오류가 발생하거나, 멤버 변수의 정보가 노출될 수 있다.
- 멤버 변수보다 지역 변수를 활용하여 변수의 범위를 제한함으로써 방지할 수 있다.

3 제거되지 않고 남은 디버그 코드

제거되지 않고 남은 디버그 코드는 개발 중에 버그 수정이나 결과값 확인을 위해 남겨둔 코드들로 인해 발생하는 보안 약점이다.

- 소프트웨어 제어에 사용되는 중요한 정보가 디버그 코드로 인해 노출될 수 있다.
- 디버그 코드에 인증 및 식별 절차를 생략하거나 우회하는 코드가 포함되어 있는 경우 공격자가 이를 악용할 수 있다.
- 소프트웨어를 배포하기 전에 코드 검사를 통해 남아있는 디버그 코드를 삭제함으로써 방지할 수 있다.

4 시스템 데이터 정보 노출

시스템 데이터 정보 노출은 시스템의 내부 정보를 시스템 메시지 등을 통해 외부로 출력하도록 코딩했을 때 발생하는 보안 약점이다.

- 시스템 메시지를 통해 노출되는 메시지는 최소한의 정보만을 제공함으로써 방지할 수 있다.

전문가의 조언

보안 점검 내용 중 '캡슐화'에 대한 내용입니다. 캡슐화의 개념을 숙지하고, 캡슐화로 인한 보안 약점에 대해 확실히 알아두세요.

캡슐화

캡슐화는 데이터(속성)와 데이터를 처리하는 함수를 하나로 묶는 것을 의미합니다. 자세한 내용은 Section 022를 참조하세요.

전문가의 조언

잘못된 세션에 의한 정보노출은 보안 점검 내용 중 '세션 통제' 항목에서도 다루어졌던 내용입니다. 세션 통제는 분석 · 설계 단계의 점검 내용이고 캡슐화는 구현 단계의 점검 내용이라는 것만 다를 뿐 나머지는 동일하니 확인한다는 느낌으로 읽어보세요.

다중 스레드(Multi-Thread)

프로세스 내의 작업 단위로, 시스템의 자원을 할당받아 실행하는 프로그램의 단위를 스레드라고 하며, 두 개 이상 스레드가 생성되어 동시 처리되는 다중 작업(Multitasking)을 다중 스레드 또는 멀티 스레드라고 부릅니다.

멤버 변수(Member Variable)

멤버 변수는 객체와 연결된 하나의 변수로, 클래스 내에 선언되어 클래스의 모든 메소드들이 접근 가능한 변수입니다. 멤버 필드라고도 부르며, 종류에는 클래스 변수, 인스턴스 변수가 있습니다.

싱글톤(Singleton)

싱글톤은 하나의 객체를 생성하면 생성된 객체를 어디서든 참조할 수 있지만, 여러 프로세스가 동시에 참조할 수는 없는 디자인 패턴입니다. 자세한 내용은 Section 026을 참조하세요.

5 Public 메소드로부터 반환된 Private 배열

선언된 클래스 내에서만 접근이 가능한 Private 배열을 모든 클래스에서 접근이 가능한 Public 메소드에서 반환할 때 발생하는 보안 약점이다.

- Public 메소드가 Private 배열을 반환하면 배열의 주소가 외부로 공개되어 외부에서 접근할 수 있게 된다.
- Private 배열을 별도의 메소드를 통해 조작하거나, 동일한 형태의 복제본으로 반환받은 후 값을 전달하는 방식으로 방지할 수 있다.

접근 지정자

접근 지정자는 프로그래밍 언어에서 특정 개체를 선언할 때 외부로부터의 접근을 제한하기 위해 사용되는 예약어입니다(접근 가능 : ○, 접근 불가능 : ×).

한정자	클래스 내부	패키지* 내부	하위 클래스	패키지 외부
Public	○	○	○	×
Default	○	○	×	×
Private	○	×	×	×

패키지(Package)
패키지는 관련 클래스나 인터페이스 등을 하나로 모아둔 것입니다.

6 Private 배열에 Public 데이터 할당

Private 배열에 Public으로 선언된 데이터 또는 메소드의 파라미터*를 저장할 때 발생하는 보안 약점이다.

- Private 배열에 Public 데이터를 저장하면 Private 배열을 외부에서 접근할 수 있게 된다.
- Public으로 선언된 데이터를 Private 배열에 저장할 때, 레퍼런스*가 아닌 값을 직접 저장함으로써 방지할 수 있다.

파라미터(Parameter)
파라미터는 메소드의 외부에서 전달된 값을 저장하는 변수로, 매개변수 또는 형식 매개변수라고도 합니다.

레퍼런스(Reference)
레퍼런스를 전달 또는 할당한다는 것은 메모리의 위치를 공유한다는 의미입니다. 예를 들어, 배열 A를 선언하여 값을 저장하고 배열 B 선언 시 B = A라고 했을 때, 배열 B는 배열 A와 동일한 메모리를 공유하게 됩니다. 즉, 배열 B에는 어떠한 값도 저장하지 않았지만 배열 A에 저장한 값들을 B를 통해 접근할 수 있게 되는 것입니다.

기출문제 따라잡기

출제예상

1. 보안 점검 내용에서 캡슐화의 정의로 가장 적합한 것은?

① 인터페이스를 제외한 세부 내용이 은폐되도록 데이터와 함수를 객체로 묶어 코딩하는 것

② 분석 자료들을 종합하여 보안 요구사항을 정의하고 개발 프로세스와의 관계를 분석하는 것

③ 시스템의 정보와 자원에 접근하려는 사용자가 합법적인 사용자인지 확인하는 것

④ 보안 요구사항들을 기술적, 관리적, 물리적 측면으로 분류하는 것

캡슐화는 서로 다른 약들을 조합하여 캡슐에 담아놓는 것과 같이 데이터와 함수를 객체로 묶어 은폐한 것입니다.

출제예상

2. 캡슐화에 대한 점검이 충분하지 않을 때 발생하는 보안 약점 중 제거되지 않고 남은 디버그 코드와 관련된 설명으로 가장 옳지 않은 것은?

① 개발 중 버그 수정이나 결과값 확인을 위해 남겨둔 코드로 인해 발생하는 보안 약점이다.

② 디버그 코드에 포함된 제어 정보가 노출될 수 있다.

③ 디버그 코드를 이용하여 인증 및 식별 절차를 우회할 수 있다.

④ 최소한의 정보만 노출되도록 제한하여 방지할 수 있다.

디버그 코드는 완전히 삭제해야지 조금이라도 남아 있으면 문제가 발생할 수 있습니다.

출제예상

3. 보안 점검 내용 중 캡슐화에서 Private 배열에 Public 데이터를 할당함으로써 발생하는 보안 약점에 대한 내용으로 가장 옳지 않은 것은?

① Private 배열에 Public 데이터 또는 메소드의 파라미터를 저장할 때 발생한다.

② Private 배열을 외부에서 접근할 수 있게 된다.

③ Public 메소드가 Private 배열을 반환하지 못하도록 코딩하여 방지할 수 있다.

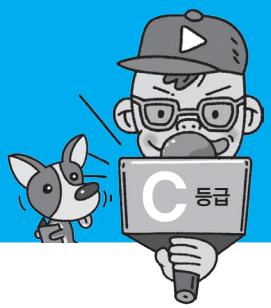
④ Private 배열에 레퍼런스가 아닌 값을 저장하여 방지할 수 있다.

'Public 메소드로부터 반환된 Private 배열'은 반환과 관련되어 있고, 'Private 배열에 Public 데이터 할당'은 할당과 관련되어 있다는 점에 주의하세요.

▶ 정답 : 1. ① 2. ④ 3. ③

SECTION 187 ● LIVE

API 오용



전문가의 조언

보안 점검 내용 중 'API 오용'과 관련된 내용입니다. API 오용으로 인해 발생할 수 있는 보안 약점에 대해 확실히 알아두세요.

API(Application Programming Interface)

API는 운영체제나 프로그래밍 언어 등에 있는 라이브러리를 응용 프로그램 개발 시 이용할 수 있도록 규칙 등에 대해 정의해 놓은 인터페이스입니다.

DNS(Domain Name System)

숫자로 된 IP 주소를 사람이 이해하기 쉬운 문자 형태로 표현한 것을 도메인 네임이라고 하며, 이러한 도메인 네임을 IP 주소로 바꾸어주는 역할을 하는 것이 DNS입니다.

DNS 엔트리

DNS 엔트리는 도메인 이름들과 도메인에 해당하는 IP들이 저장된 목록입니다.

C언어의 문자열 함수

- strcat( ) : 두 개의 문자열을 하나로 합치는 함수
- strcpy( ) : 문자열을 복사하는 함수
- sprintf( ) : 문자열에 서식지정자를 적용하는 함수

1 API 오용의 개요

API* 오용은 소프트웨어 구현 단계에서 API를 잘못 사용하거나 보안에 취약한 API를 사용하지 않도록 하기 위한 보안 검증 항목들이다.

- API 오용으로 발생할 수 있는 보안 약점에는 DNS* lookup에 의존한 보안 결정, 취약한 API 사용이 있다.

2 DNS Lookup에 의존한 보안 결정

도메인명에 의존하여 인증이나 접근 통제 등의 보안 결정을 내리는 경우 발생하는 보안 약점이다.

- DNS 엔트리*를 속여 동일한 도메인에 속한 서버인 것처럼 위장하거나, 사용자와 서버 간의 네트워크 트래픽을 유도하여 악성 사이트를 경유하도록 조작할 수 있다.
- 공격자는 DNS lookup을 악용하여 인증이나 접근 통제를 우회하는 수법으로 권한을 탈취한다.
- DNS 검색을 통해 도메인 이름을 비교하지 않고 IP 주소를 직접 입력하여 접근함으로써 방지할 수 있다.

3 취약한 API 사용

보안 문제로 사용이 금지된 API를 사용하거나, 잘못된 방식으로 API를 사용했을 때 발생하는 보안 약점이다.

- 보안 문제로 금지된 대표적인 API에는 C언어의 문자열 함수 strcat( )*, strcpy( )*, sprintf( )* 등이 있다.
- 보안 상 안전한 API라고 하더라도 자원에 대한 직접 연결이나, 네트워크 소켓을 통한 직접 호출과 같이 보안에 위협을 줄 수 있는 인터페이스를 사용하는 경우 보안 약점이 노출된다.
- 보안 문제로 금지된 함수는 안전한 함수로 대체하고, API의 매뉴얼을 참고하여 보안이 보장되는 인터페이스를 사용함으로써 방지할 수 있다.

기출문제 따라잡기 Section 187

출제예상

1. 보안 점검 내용 중 API 오용으로 발생할 수 있는 보안 약점에 대한 설명으로 가장 옳지 않은 것은?

① 보안에 취약한 API를 사용할 때 발생한다.

② 보안에 문제가 없는 API라도 잘못된 방식으로 사용하는 경우 발생한다.

③ 자신을 호출하는 함수의 종료 시점이 존재하지 않아 무한히 반복될 때 발생한다.

④ IP가 아닌 도메인명을 통해 보안 결정을 내릴 때 발생한다.

③번은 재귀함수로 인해 발생할 수 있는 보안 점검 내용 중 '시간 및 상태'와 관련된 보안 약점입니다.

출제예상

2. 보안 약점 중 취약한 API 사용으로 인한 보안 약점에 대한 설명으로 가장 옳지 않은 것은?

① 보안 문제로 사용이 금지된 API를 사용할 때 발생하는 보안 약점이다.

② 네트워크 소켓을 통한 직접 호출 등 인터페이스를 잘못 이용할 때 발생하는 보안 약점이다.

③ IP 주소를 직접 입력하지 않고 DNS 검색을 통해 도메인명을 비교하여 접근함으로써 방지할 수 있다.

④ 보안 상 사용이 금지된 API를 다른 안전한 API로 대체함으로써 방지할 수 있다.

API 오용은 도메인명이 아닌 IP 주소를 직접 입력함으로써 방지할 수 있습니다.

출제예상

3. 서버에서 도메인명에 의존하여 인증이나 접근 통제를 수행할 때 발생할 수 있는 문제점으로 가장 옳지 않은 것은?

① 도메인에 속한 서버인 것처럼 위장하여 인증을 우회할 수 있다.

② 네트워크 트래픽을 유도하여 악성 사이트를 방문하도록 만들 수 있다.

③ 도메인명보다는 IP 주소를 직접 입력하는 방식으로 예방할 수 있다.

④ 허용할 도메인명을 화이트리스트로 관리하여 예방할 수 있다.

화이트리스트란 허용 대상들만을 기록하여 나머지는 모두 허용하지 않는 것을 의미합니다. 도메인 엔트리를 속여서 접속하는 공격자가 화이트리스트는 공격 안 할까요? 화이트리스트로 막을 수 있을까요?

▶ 정답 : 1. ③ 2. ③ 3. ④

SECTION
188
LIVE

암호 알고리즘

전문가의 조언

암호 알고리즘에서는 각 암호 방식들이 어떻게 분류되는지 분류표를 확실히 기억하고, 암호 방식들의 개별적인 특징을 잘 알아두세요.

1 암호 알고리즘의 개요

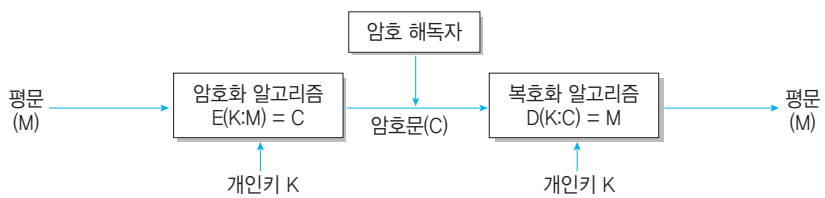
암호 알고리즘은 패스워드, 주민번호, 은행계좌와 같은 중요정보를 보호하기 위해 평문을 암호화된 문장으로 만드는 절차 또는 방법을 의미한다.

- 암호 알고리즘은 해시(Hash)를 사용하는 단방향 암호화 방식과, 개인키 및 공개키로 분류되는 양방향 암호화 방식이 있다.
- 암호 방식 분류

2 개인키 암호화(Private Key Encryption) 기법

개인키 암호화 기법은 동일한 키로 데이터를 암호화하고 복호화한다.

- 데이터베이스 사용자는 평문의 정보 M을 암호화 알고리즘 E와 개인키(Private Key) K를 이용하여 암호문 C로 바꾸어 저장시켜 놓으면 사용자는 그 데이터베이스에 접근하기 위해 복호화 알고리즘 D와 개인키 K를 이용하여 다시 평문의 정보 M으로 바꾸어 이용하는 방법이다.



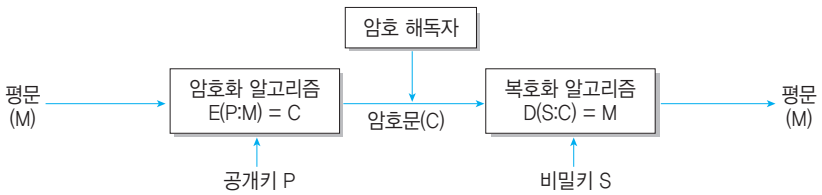
- 개인키 암호화 기법은 대칭 암호 기법 또는 단일키 암호화 기법이라고도 한다.
- 개인키 암호화 기법은 한 번에 하나의 데이터 블록을 암호화 하는 블록 암호화 방식과, 평문과 동일한 길이의 스트림을 생성하여 비트 단위로 암호화 하는 스트림 암호화 방식으로 분류된다.
- 종류
  - 블록 암호화 방식 : DES, SEED, AES, ARIA
  - 스트림 암호화 방식 : LFSR, RC4

- **장점** : 암호화/복호화 속도가 빠르며, 알고리즘이 단순하고, 공개키 암호 기법보다 파일의 크기가 작다.
- **단점** : 사용자의 증가에 따라 관리해야 할 키의 수가 상대적으로 많아진다.

3 공개키 암호화(Public Key Encryption) 기법

공개키 암호화 기법은 데이터를 암호화할 때 사용하는 공개키(Public Key)는 데이터베이스 사용자에게 공개하고, 복호화할 때의 비밀키(Secret Key)는 관리자가 비밀리에 관리한다.

- 데이터베이스 사용자는 평문의 정보 M을 암호화 알고리즘 E와 공개키(Public Key) P를 이용하여 암호문 C로 바꾸어 저장시켜 놓고, 이를 복호화하기 위해서는 비밀키와 복호화 알고리즘에 권한이 있는 사용자만이 복호화 알고리즘 D와 비밀키(Secret Key) S를 이용하여 다시 평문의 정보 M으로 바꿀 수 있는 기법이다.



- 공개키 암호화 기법은 비대칭 암호 기법이라고도 하며, 대표적으로는 RSA(Rivest Shamir Adleman) 기법이 있다.
- **장점** : 키의 분배가 용이하고, 관리해야 할 키의 개수가 적다.
- **단점** : 암호화/복호화 속도가 느리며, 알고리즘이 복잡하고, 개인키 암호화 기법보다 파일의 크기가 크다.

공개키 기반 구조(PKI; Public Key Infrastructure)

- 공개키 기반 구조는 공개키 암호 시스템을 안전하게 사용하고 관리하기 위한 정보 보호 표준 방식으로 ITU-T의 X.509 방식과 비X.509 방식으로 구분됩니다.
- **X.509 방식** : 인증기관에서 발생하는 인증서를 기반으로 상호 인증을 제공
- **비X.509 방식** : 국가별, 지역별로 맞게 보완 및 개발

잠깐만요

양방향 알고리즘 종류

개인키 암호화 방식과 공개키 암호화 방식에서 사용되는 주요 암호화 알고리즘에는 SEED, ARIA 등이 있습니다.

SEED	• 1999년 한국인터넷진흥원(KISA)에서 개발한 블록 암호화 알고리즘 • 블록 크기는 128비트이며, 키 길이에 따라 128, 256으로 분류됩니다.
ARIA(Academy, Research Institute, Agency)	• 2004년 국가정보원과 산학연협회가 개발한 블록 암호화 알고리즘 • ARIA는 학계(Academy), 연구기관(Research Institute), 정부(Agency)의 영문 앞 글자로 구성되었습니다. • 블록 크기는 128비트이며, 키 길이에 따라 128, 192, 256으로 분류됩니다.
DES(Data Encryption Standard)	• 1975년 미국 NBS☆에서 발표한 개인키 암호화 알고리즘 • DES를 3번 적용하여 보안을 더욱 강화한 3DES(Triple DES)도 있습니다. • 블록 크기는 64비트이며, 키 길이는 56비트입니다.
AES(Advanced Encryption Standard)	• 2001년 미국 표준 기술 연구소(NIST)에서 발표한 개인키 암호화 알고리즘 • DES의 한계를 느낀 NIST에서 공모한 후 발표하였습니다. • 블록 크기는 128비트이며, 키 길이에 따라 128, 192, 256으로 분류됩니다.
RSA(Rivest Shamir Adleman)	• 1978년 MIT의 라이베스트(Rivest), 샤미르(Shamir), 애들먼(Adelman)에 의해 제안된 공개키 암호화 알고리즘 • 큰 숫자를 소인수분해 하기 어렵다는 것에 기반하여 만들어졌습니다. • 공개키와 비밀키를 사용하는데, 여기서 키란 메시지를 열고 잠그는 상수(Constant)를 의미합니다.

NBS
(National Bureau of Standards)
NBS는 미국 표준 기술 연구소(NIST)의 과거 이름입니다.

4 해시(Hash)

해시는 임의의 길이의 입력 데이터나 메시지를 고정된 길이의 값이나 키로 변환하는 것을 의미한다.

- 해시 알고리즘을 해시 함수라고 부르며, 해시 함수로 변환된 값이나 키를 해시값 또는 해시키라고 부른다.
- 데이터의 암호화, 무결성 검증을 위해 사용될 뿐만 아니라 정보보호의 다양한 분야에서 활용된다.
- 해시 함수의 종류에는 SHA 시리즈, MD5, N-NASH, SNEFRU 등이 있다.

기출문제 따라잡기 Section 188

이전기출

1. 분산 데이터베이스의 불법적인 접근을 차단하기 위하여 데이터 암호화가 필요하다. DES 알고리즘에서는 평문을 (㉠)비트로 블록화를 하고, 실제 키의 길이는 (㉡)비트를 이용한다. 괄호의 내용으로 옳은 것은?

① ㉠ 64 ㉡ 56 ② ㉠ 64 ㉡ 32
③ ㉠ 32 ㉡ 16 ④ ㉠ 32 ㉡ 8

DES는 미 표준국에서 채택했던 기법으로, 시험에 등장할 수 있습니다. 특징을 잘 정리해 두세요.

이전기출

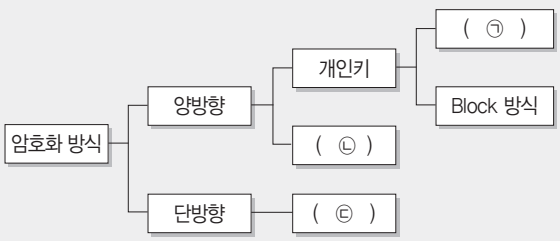
2. 데이터를 암호화하는 데 사용되는 RSA 기법에 대한 설명으로 가장 옳지 않은 것은?

① 암호화키와 해독키를 별도로 사용한다.
② 암호화키를 일반적으로 공중키라고도 한다.
③ 해독키는 반드시 비밀로 보호되어야 한다.
④ 암호화키를 사용하여 해독키를 유도할 수 있다.

RSA 기법은 공중키(Public Key) 기법으로 암호화와 복호화에 서로 다른 별도의 키를 사용하므로 암호화키를 사용하여 해독키를 유도하는 것은 절대 불가능합니다.

출제예상

3. 다음 그림에서 빈 칸에 들어갈 적합한 단어는?



① ㉠ Stream 방식, ㉡ 공개키, ㉢ 해시(Hash)
② ㉠ 비밀키, ㉡ 대칭키, ㉢ Stream 방식
③ ㉠ 비밀키, ㉡ 비대칭키, ㉢ 해시(Hash)
④ ㉠ Stream 방식, ㉡ 대칭키, ㉢ 공개키

바로 앞에서 배운 분류표를 떠올려 보세요!

출제예상

4. 해시(Hash)에 대한 설명으로 잘못된 것은?

① 임의의 길이의 입력 데이터를 받아 고정된 길이의 해시값으로 변환하는 것이다.
② 해시 함수는 해시값으로 변환하는 알고리즘을 의미한다.
③ 해시 함수의 종류에는 SHA-256, MD5 등이 있다.
④ 공개키 암호화 기법의 한 종류로 암호화와 무결성 검증을 위해 사용된다.

해시는 단방향, 공개키/개인키는 양방향 방식입니다.

출제예상

5. 다음에서 설명하는 암호화 알고리즘은?

- 한국인터넷진흥원(KISA; Korea Internet & Security Agency)에서 1999년 개발한 블록 암호화 알고리즘이다.
- 블록의 크기는 128비트이며, 키의 길이에 따라 128, 256 버전이 있다.

① DES ② AES
③ SEED ④ ARIA

국내에서 개발된 대표적인 암호화 알고리즘에는 SEED와 ARIA가 있습니다. 이제 정답을 찾아보세요.

▶ 정답 : 1. ① 2. ④ 3. ① 4. ④ 5. ③

예·상·문·제·은·행

1. 소프트웨어 개발 보안 중 다음 설명에 해당하는 것은?

> • 소프트웨어 개발 생명주기에 보안 프로세스를 포함하는 것이다.
> • 유지 보수 단계에서 보안 문제를 해결하는데 큰 비용이 소모되는 것을 예방하기 위해 등장하였다.
> • 대표적으로 CLASP, SDL이 있다.

① Secure Coding
② Secure SDLC
③ Secure Architecture
④ Secure Framework

2. Secure SDLC의 구현 단계에 대한 설명으로 가장 거리가 먼 것은?

① 보안 요구사항들을 구현하는 단계이다.
② 설계 단계에서 작성한 보안 설계서에 따라 소프트웨어를 구현한다.
③ 지속적인 점검 및 진단작업으로 코드의 안정성을 확보한다.
④ 동적 분석도구의 사용 또는 모의 침투테스트를 통해 보안 위협들의 해결 여부를 검증한다.

3. 시큐어 코딩(Secure Coding)에 대한 설명으로 가장 옳지 않은 것은?

① 소프트웨어 설계 시 보안 요소들을 고려하며 코딩하는 것을 말한다.
② 취약점을 유지 및 보수 단계가 아닌 개발 단계에서 대응하는 것이다.
③ 보안 약점을 사전에 대응하여 안전성과 신뢰성을 확보하기 위함이다.
④ 사내 보안 정책을 바탕으로 시큐어 코딩 가이드를 작성한 후 개발 참여자들에게 코딩 교육을 실시한다.

4. 세션이 안전하게 관리되도록 코딩되지 않았을 때 발생할 수 있는 문제점으로 옳은 것은?

① 교착상태나 동기화 오류 등이 발생할 수 있다.
② 세션ID를 탈취하여 시스템의 기능을 이용하거나 중요정보에 접근할 수 있다.
③ 자원고갈로 인해 서비스나 시스템에 장애가 발생할 수 있다.
④ 오류 메시지를 통해 시스템의 중요정보가 노출될 수 있다.

5. 보안을 고려하여 세션을 설계할 때 주의해야 할 점으로 잘못된 것은?

① 시스템의 모든 페이지에서 로그아웃이 가능해야 한다.
② 로그아웃 시 세션ID가 남아있으면 안된다.
③ 세션의 타임아웃은 중요도에 따라 2분에서 30분 사이로 설정한다.
④ 패스워드 변경 시 활성화된 세션이 제거되지 않도록 주의한다.

6. 세션ID를 관리하는 방법에 대한 설명으로 잘못된 것은?

① 안전한 서버에서 최소 길이 128bit의 세션ID를 사용하는 것이 좋다.
② HASH 함수 등의 난수 알고리즘을 사용하여 세션ID를 발급한다.
③ 쿠키를 사용할 수 없는 경우 URL Rewrite 기능을 사용하여 세션ID를 관리한다.
④ 오래된 세션ID는 주기적으로 재할당하도록 설계해야 한다.

7. 크로스사이트 스크립팅(XSS)과 관련된 내용으로 옳지 않은 것은?

① 악의적인 스크립트 파일을 업로드 함으로써 시스템에 손상을 주는 보안 약점이다.
② 게시판이나 메일 등에 HTML 태그 또는 스크립트 명령어를 삽입하는 방식을 이용한다.
③ 공격 대상 사이트의 장애를 유발하거나, 방문자들의 정보를 탈취하는 용도로 사용된다.
④ 입력 데이터에 대해 올바른 유효성 검증 체계를 갖추지 않은 경우 발생할 수 있다.

8. 신뢰되지 않은 URL 주소에 자동 접속으로 연결할 경우 발생할 수 있는 문제점으로 옳은 것은?

① 웹페이지에 악의적인 스크립트를 삽입하여 방문자들의 정보를 탈취할 수 있다.
② 외부 입력값을 통해 시스템 명령어의 실행을 유도함으로써 권한을 탈취할 수 있다.
③ 사이트 주소를 조작하여 방문자를 피싱 사이트로 유도할 수 있다.
④ 데이터 입·출력 경로를 조작하여 서버 자원을 무단으로 사용할 수 있다.

해설은 799쪽에 있습니다.

9. 소프트웨어 구현 단계에서 점검해야 하는 보안 점검 내용 중 보안 기능에 대한 설명으로 잘못된 것은?

① 보안 기능으로는 인증, 접근제어, 기밀성, 암호화 등이 있다.

② 중요 정보의 변조나 오남용을 막기 위해 접근제어 기능을 사용해야 한다.

③ 서비스 환경이나 취급 데이터에 맞게 보안 기능들을 구현해야 한다.

④ 인증된 사용자에게 개별적으로 권한을 부여하여 인가되지 않은 기능과 데이터의 사용을 제한한다.

10. 취약한 암호화 알고리즘 사용 시 발생하는 보안 약점에 대한 설명으로 가장 옳지 않은 것은?

① 충분히 오래 사용되어 검증된 암호화 알고리즘을 사용하여 예방할 수 있다.

② 암호화된 환경설정 파일을 해독하여 중요정보를 탈취할 수 있다.

③ IT보안인증사무국의 인증제품 목록을 참고하여 암호화 알고리즘을 선정한다.

④ 소프트웨어 개발의 구현 단계에서 검증해야 하는 보안 점검 항목이다.

11. 보안 약점 중 TOCTOU 경쟁 조건에 대한 설명으로 잘못된 것은?

① 자원의 상태가 검사 시점(TOC)과 사용 시점(TOU)의 사이에 변경되는 경우 발생한다.

② 동기화 오류, 교착 상태 등을 발생시킬 수 있다.

③ 동기화 구문을 사용하여 예방할 수 있으나, 성능이 감소하는 것은 감안해야 한다.

④ 주로 사용되는 동기화 구문에는 Strcpy, Strcat 등이 있다.

12. 소스 코드의 논리 구조 상 종료되지 않고 무한히 반복하는 경우 발생하는 결과로 가장 옳은 것은?

① 시스템 자원이 끊임없이 사용되어 결국 장애가 발생하게 된다.

② 피싱 사이트로 유도될 수 있다.

③ 메모리 0x00000000을 참조하였다는 오류가 발생한다.

④ 스택 트레이스가 노출되어 시스템의 내부 구조가 공격자에게 노출된다.

13. 예외처리(Exception Handling)가 미비한 경우 발생하는 보안 약점에 대한 설명으로 잘못된 것은?

① 오류 발생으로 인해 실행 환경, 사용자 정보 등이 외부로 노출될 수 있다.

② 오류로 인해 예기치 못한 동작이 발생할 수 있으며, 이러한 동작이 공격자에 의해 악용될 수도 있다.

③ 광범위한 예외처리 구문을 사용하여 예외처리에 누락되는 오류가 발생하지 않도록 함으로써 방지할 수 있다.

④ 제어문을 활용하여 오류가 악용되지 않도록 함으로써 방지할 수 있다.

14. 널 포인터가 가리키는 곳에 데이터를 저장하는 경우 발생하는 보안 약점에 대한 설명으로 가장 옳지 않은 것은?

① 값이 없는 포인터 변수를 참조하여 데이터를 저장할 때 발생한다.

② 널 포인터는 메모리의 마지막 주소인 FxFFF...F를 가리킨다.

③ 널 포인터를 참조하는 경우 소프트웨어는 비정상적으로 종료될 수 있다.

④ 널 값을 가질 가능성이 있는 포인터 변수를 확인하여 사용 전에 널 여부를 검사하여 예방할 수 있다.

15. 자원이 부적절하게 해제된 경우 발생하는 보안 약점에 대한 설명으로 잘못된 것은?

① 반환 코드를 누락하거나 오류로 자원 반환이 이루어지지 않은 경우 발생한다.

② 힙 메모리, 소켓 등의 한정된 자원이 반환되지 않고 계속 점유되면 시스템은 결국 어떤 처리도 하지 못하게 된다.

③ 프로그램 내 자원 반환 코드를 확인하여 코드 누락을 방지할 수 있다.

④ 자원을 점유하는 함수가 오류로 중간에 중단되어 반환이 이루어지지 않은 경우 예외처리를 통해 해당 함수를 재실행한다.

16. 소프트웨어 구현 과정에서 작성한 디버그 코드로 인해 발생하는 보안 약점에 대한 설명으로 잘못된 것은?

① 소프트웨어의 중요정보가 디버그 코드로 인해 노출될 수 있다.

② 디버그 코드에 식별절차를 생략할 수 있는 코드가 포함되어 있는 경우 공격자에 의해 악용될 수 있다.

③ 레이스컨디션으로 인한 동기화 오류가 발생할 수 있다.

④ 디버그 코드는 소프트웨어 배포 전 반드시 삭제해야 한다.

▶ **정답 :** 1. ② 2. ④ 3. ① 4. ② 5. ④ 6. ③ 7. ① 8. ③ 9. ② 10. ① 11. ④ 12. ① 13. ③ 14. ② 15. ④ 16. ③

예·상·문·제·은·행

해설은 799쪽에 있습니다.

17. 접근 지정자에 대한 설명으로 옳지 않은 것은?

① 특정 개체를 선언할 때 외부로부터 접근을 제한하기 위해 사용되는 예약어이다.

② Public 개체는 외부 패키지를 포함한 프로그램의 모든 위치에서 접근이 가능하다.

③ Default 개체는 하위 클래스와 외부 패키지에서는 접근이 불가능하다.

④ Private 개체는 클래스 내부에서만 접근이 가능하다.

18. 취약한 API를 사용했을 때 발생하는 보안 약점에 대한 설명으로 옳지 않은 것은?

① API를 잘못된 방식으로 사용하는 경우 발생한다.

② 보안에 문제가 있는 API를 사용하는 경우 발생한다.

③ 보안이 금지된 대표적인 API에는 C언어의 문자열 함수 strcat( ), strcpy( ) 등이 있다.

④ 예방을 위해 직접 연결이나 네트워크 소켓을 통한 호출을 통해 보안에 문제가 없는 API를 이용해야 한다.

19. 다음에서 설명하는 암호화 알고리즘은 무엇인가?

- 1975년 미국 표준 기술 연구소의 전신인 NBS에서 발표한 개인키 암호화 알고리즘이다.
- 블록 크기는 64비트이며, 키 길이는 56비트이다.
- 컴퓨터의 발달로 인해 최근에는 사용되지 않으며, 알고리즘을 3번 적용한 버전이 잠시 사용되기도 하였다.

① ARIA 암호화 알고리즘

② SEED 암호화 알고리즘

③ DES 암호화 알고리즘

④ AES 암호화 알고리즘

20. 임의의 길이의 입력 데이터나 메시지를 고정된 길이의 값이나 키로 변환하는 것으로 데이터 암호화부터 무결성 검증까지 정보보호의 다양한 분야에서 활용되는 것은?

① Private Key Encryption

② Public Key Encryption

③ Hash

④ SEED

21. 공개키 암호화(Public Key Encryption)에 대한 설명으로 옳지 않은 것은?

① 암호키는 사용자에게 공개하고, 복호키는 관리자가 비밀리에 관리한다.

② 암호화 및 복호화의 속도가 비교적 빠르고 관리해야 할 키의 수가 적다.

③ 알고리즘이 복잡하고, 파일의 크기가 비교적 크다.

④ 대표적으로 RSA, DSA 등이 있다.

▶ **정답 :** 17. ② 18. ④ 19. ③ 20. ③ 21. ②

예·상·문·제·은·행·해·설

1. Section 179

- Secure Coding : 소프트웨어 개발 생명주기 전체가 아닌 구현 단계에서 수행되는 보안 활동
- Secure Architecture : 설계 단계에서 사용되는 보안이 고려된 아키텍처

2. Section 179

④번은 테스트 단계에서 수행되어야 하는 보안 활동이다.

3. Section 179

시큐어 코딩은 개발 단계가 아닌 본격적인 코딩이 수행되는 구현 단계에서 이루어진다.

4. Section 180

①번은 TOCTOU 경쟁 조건, ③번은 종료되지 않는 반복문 또는 재귀함수, ④번은 오류 메시지를 통해 발생할 수 있는 문제점이다.

5. Section 180

활성화된 세션에서 패스워드 변경 작업이 발생한다면 세션을 삭제하고 재할당해야 한다.

6. Section 180

세션ID를 URL로 전달하는 URL Rewrite 기능을 사용하는 것은 오히려 보안을 위협하는 방법에 해당한다.

7. Section 181

①번은 입력 데이터 검증 및 표현과 관련된 보안 약점이다.

8. Section 181

입력 데이터 검증 및 표현의 보안 약점

- SQL 삽입 : 입력란에 SQL을 삽입하여 무단으로 DB를 조회하거나 조작하는 보안 약점
- 경로 조작 및 자원 삽입 : 데이터 입 · 출력 경로를 조작하여 서버 자원을 수정 · 삭제할 수 있는 보안 약점
- 크로스사이트 스크립팅(XSS) : 웹페이지에 악의적인 스크립트를 삽입하여 방문자들의 정보를 탈취하거나, 비정상적인 기능 수행을 유발하는 보안 약점
- 운영체제 명령어 삽입 : 외부 입력값을 통해 시스템 명령어의 실행을 유도함으로써 권한을 탈취하거나 시스템 장애를 유발하는 보안 약점
- 위험한 형식 파일 업로드 : 악의적인 명령어가 포함된 스크립트 파일을 업로드함으로써 시스템에 손상을 주거나, 시스템을 제어할 수 있는 보안 약점

9. Section 182

개인정보나 인증정보와 같은 중요 정보의 변조 · 삭제 · 오남용 등을 방지하기 위해서는 접근제어가 아닌 암호화 기술을 적용해야 한다.

10. Section 182

암호 알고리즘은 점점 보안성이 높아지고 있으므로 오래된 알고리즘 보다는 IT보안인증사무국이 안정성을 확인한 암호 모듈을 사용하는 것이 좋다.

11. Section 183

Strcpy는 문자열을 복사하는 함수, Strcat는 2개의 문자열을 합치는 함수의 명칭이다. 동기화에 사용되는 구문에는 Synchronized, Mutex 등이 있다.

12. Section 183

반복문이나 재귀함수가 종료되지 않는 경우 시스템 자원이 끊임없이 사용되어 자원 고갈로 인한 서비스 장애 또는 시스템 장애가 발생한다.

13. Section 184

모든 오류들을 세세하게 정의하여 처리할 필요는 없지만, 광범위한 예외처리 구문으로 모든 오류들을 정의해 버리는 경우 예기치 않은 문제를 발생시킬 수 있다.

14. Section 185

널 포인터는 일반적으로 메모리의 첫 주소를 가리키며, 0x00000000으로 표현된다.

15. Section 185

자원을 점유하는 함수가 오류로 중간에 중단되어 반환이 이루어지지 않은 경우 예외처리에 관계없이 자원이 반환되도록 코딩해야 한다.

16. Section 186

레이스컨디션으로 인한 동기화 오류는 잘못된 세션에 의해 발생한다.

17. Section 186

Public 개체는 패키지 외부에서는 접근이 불가능하고 나머지 다른 위치에서는 접근이 가능하다.

예·상·문·제·은·행·해·설

18. Section 187

보안 상 안전한 API라고 하더라도 자원에 대한 직접 연결이나, 네트워크 소켓을 통해 직접 호출하는 경우는 보안에 위협을 줄 수 있으므로 사용하지 않아야 한다.

19. Section 188

- ARIA(Academy, Research Institute, Agency) : 2004년 국가정보원과 산학연협회가 개발한 블록 암호화 알고리즘으로 블록 크기는 128비트이며, 키 길이에 따라 128, 192, 256으로 분류됨
- SEED : 1999년 한국인터넷진흥원(KISA)에서 개발한 블록 암호화 알고리즘으로 블록 크기는 128비트이며, 키 길이에 따라 128, 256으로 분류됨
- AES(Advanced Encryption Standard) : 2001년 미국 표준기술 연구소(NIST)에서 발표한 개인키 암호화 알고리즘으로 DES의 한계를 느낀 NIST에서 공모한 후 발표함

20. Section 188

- Private Key Encryption : 동일한 키로 데이터를 암호화 · 복호화 하는 개인키 암호화 기법
- Public Key Encryption : 공개키와 비밀키, 2개의 키로 데이터를 암호화 · 복호화 하는 공개키 암호화 기법
- SEED : 1999년 한국인터넷진흥원(KISA)에서 개발한 블록 암호화 알고리즘으로 블록 크기는 128비트이며, 키 길이에 따라 128, 256으로 분류됨

21. Section 188

공개키 암호화는 개인키 암호화에 비해 키의 분배가 용이하고 관리해야 할 키의 개수가 적다는 장점이 있지만, 암호화 및 복호화의 속도가 느리고 복잡하며 파일의 크기가 크다는 단점이 있다.

4장 시스템 보안 구축

이 장에서 꼭 알아야 할 키워드 Best 10

1. 서비스 거부(DoS) 공격 **2.** 분산 서비스 거부(DDoS) 공격 **3.** 인증 서버 **4.** 인증 **5.** 보안 아키텍처
6. 보안 프레임워크 **7.** 로그 **8.** 리눅스 로그 **9.** 윈도우 로그 **10.** 방화벽

SECTION 189 ● LIVE

서비스 공격 유형

전문가의 조언

안전한 정보 시스템 환경을 구축하기 위해서는 먼저 서비스 거부 공격의 개념과 주요 유형에 대한 이해가 필요합니다. 서비스 거부 공격의 개념을 기억하고 주요 서비스 거부 공격들의 개별적인 특징을 정리해 두세요.

1 서비스 거부(DoS; Denial of Service) 공격의 개념

서비스 거부 공격이란 표적이 되는 서버의 자원을 고갈시킬 목적으로 다수의 공격자 또는 시스템에서 대량의 데이터를 한 곳의 서버에 집중적으로 전송함으로써, 표적이 되는 서버의 정상적인 기능을 방해하는 것이다.

- 서비스 거부 공격의 유형에는 Ping of Death, SMURFING, SYN Flooding, TearDrop, Land, DDoS 등이 있다.

2 Ping of Death(죽음의 핑)

Ping of Death는 Ping 명령을 전송할 때 패킷의 크기를 인터넷 프로토콜 허용 범위(65,536 바이트) 이상으로 전송하여 공격 대상의 네트워크를 마비시키는 서비스 거부 공격 방법이다.

- 공격에 사용되는 큰 패킷은 수백 개의 패킷으로 분할되어 전송되는데, 공격 대상은 분할된 대량의 패킷을 수신함으로써 분할되어 전송된 패킷을 재조립해야 하는 부담과 분할되어 전송된 각각의 패킷들의 ICMP Ping 메시지*에 대한 응답을 처리하느라 시스템이 다운되게 된다.
- jolt, sPING, ICMP bug, IceNewk 등의 변종 공격에 대비하여 ICMP Ping 메시지가 전송되지 못하도록 방화벽에서 차단하는 기술이 개발되었다.

3 SMURFING(스머핑)

SMURFING은 IP나 ICMP의 특성을 악용하여 엄청난 양의 데이터를 한 사이트에 집중적으로 보냄으로써 네트워크를 불능 상태로 만드는 공격 방법이다.

- 공격자는 송신 주소를 공격 대상지의 IP 주소로 위장하고 해당 네트워크 라우터의 브로드캐스트 주소*를 수신지로 하여 패킷을 전송하면, 라우터의 브로드캐스트 주소로 수신된 패킷은 해당 네트워크 내의 모든 컴퓨터로 전송된다.
- 해당 네트워크 내의 모든 컴퓨터는 수신된 패킷에 대한 응답 메시지를 송신 주소인 공격 대상지로 집중적으로 전송하게 되는데, 이로 인해 공격 대상지는 네트워크 과부하로 인해 정상적인 서비스를 수행할 수 없게 된다.
- SMURFING 공격을 무력화하는 방법 중 하나는 각 네트워크 라우터에서 브로드캐스트 주소를 사용할 수 없게 미리 설정해 놓는 것이다.

ICMP Ping 메시지

ICMP Ping 메시지는 특정 IP로 패킷이 전송될 때 해당 IP의 노드가 현재 운영 중인지 확인을 요청하는 메시지로, 이를 수신한 노드가 운영 중이라면 Ping 메시지에 대한 응답으로 에코 응답 메시지를 전송합니다.

※ ICMP(인터넷 제어 메시지 프로토콜) : TCP/IP 기반의 인터넷 통신 서비스에서 인터넷 프로토콜(IP)에 결합되어 전송되는 프로토콜로, IP에 대해 통신 중에 발생하는 오류 처리와 전송 경로 변경, 에코 요청, 에코 응답 등을 제어하기 위한 메시지를 취급함

브로드캐스트 주소

브로드캐스트 주소는 네트워크 내의 특정 호스트를 대상으로 패킷을 전송하는 것이 아니라 네트워크 내의 전체 호스트를 대상으로 패킷을 전송할 때 사용하는 주소입니다.

4 SYN Flooding

TCP(Transmission Control Protocol)는 신뢰성 있는 전송을 위해 3-way-handshake*를 거친 후에 데이터를 전송하게 되는데, SYN Flooding은 공격자가 가상의 클라이언트로 위장하여 3-way-handshake 과정을 의도적으로 중단시킴으로써 공격 대상지인 서버가 대기 상태에 놓여 정상적인 서비스를 수행하지 못하게 하는 공격 방법이다.

- 공격자는 사용할 수 없는 IP 주소를 이용해 가상의 클라이언트로 위장하여 공격 대상지인 서버로 'SYN' 신호를 보내 3-way-handshake의 첫 번째 과정을 수행한다.
- 공격 대상지인 서버는 'SYN' 신호에 대한 응답으로 'SYN+ACK' 신호를 가상의 클라이언트로 보내면서 클라이언트의 접속을 받아들이기 위해 메모리의 일정 공간을 확보한다.
- 가상의 클라이언트는 본래 사용할 수 없는 주소였으므로 서버가 보낸 응답이 전송되지 않을 뿐만 아니라 가상의 클라이언트로부터 3-way-handshake의 마지막 과정인 'ACK' 신호도 전송되지 않으므로 공격 대상지인 서버는 메모리 공간을 확보한 상태에서 대기하게 된다.
- 공격자가 사용할 수 없는 IP 주소를 이용해 공격 대상지 서버로 반복적인 3-way-handshake 과정을 요청하면 공격 대상지 서버는 메모리 공간을 점점 더 많이 확보한 상태에서 대기하게 되며, 결국 서버에 설정된 동시 사용자 수가 모두 대기 상태로 채워지게 되어 더 이상 정상적인 서비스를 수행할 수 없게 된다.
- SYN Flooding에 대비하기 위해 수신지의 'SYN' 수신 대기 시간을 줄이거나 침입차단 시스템을 활용한다.

5 TearDrop

데이터의 송·수신 과정에서 패킷의 크기가 커 여러 개로 분할되어 전송될 때 분할 순서를 알 수 있도록 Fragment Offset 값을 함께 전송하는데, TearDrop은 이 Offset 값을 변경시켜 수신 측에서 패킷을 재조립할 때 오류로 인한 과부하를 발생시킴으로써 시스템이 다운되도록 하는 공격 방법이다.

- TearDrop에 대비하기 위해 Fragment Offset이 잘못된 경우 해당 패킷을 폐기하도록 설정한다.

6 Land

Land는 패킷을 전송할 때 송신 IP 주소와 수신 IP 주소를 모두 공격 대상의 IP 주소로 하여 공격 대상에게 전송하는 것으로, 이 패킷을 받은 공격 대상은 송신 IP 주소가 자신이므로 자신에게 응답을 수행하게 되는데, 이러한 패킷이 계속해서 전송될 경우 자신에 대해 무한히 응답하게 하는 공격이다.

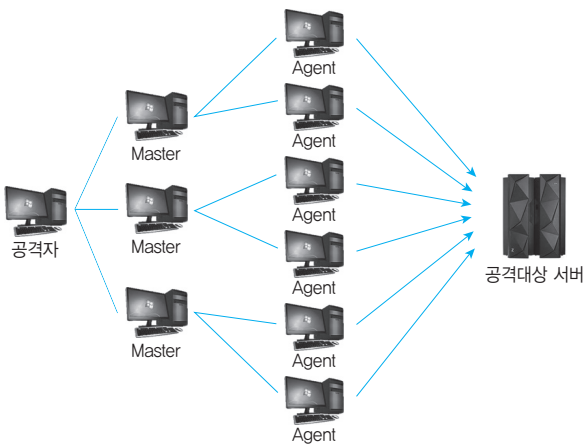
- Land에 대비하기 위해 송신 IP 주소와 수신 IP 주소의 적절성을 검사한다.

3-way-handshake
신뢰성 있는 연결을 위해 송신지와 수신지 간의 통신에 앞서 3단계에 걸친 확인 작업을 수행한 후 통신을 수행합니다.
- **1단계** : 송신지에서 수신지로 'SYN' 패킷을 전송
- **2단계** : 수신지에서 송신지로 'SYN + ACK' 패킷을 전송
- **3단계** : 송신지에서 수신지로 'ACK' 패킷을 전송

7 DDoS(Distributed Denial of Service, 분산 서비스 거부) 공격

DDoS 공격은 여러 곳에 분산된 공격 지점에서 한 곳의 서버에 대해 분산 서비스 공격을 수행하는 것으로, 네트워크에서 취약점이 있는 호스트들을 탐색한 후 이들 호스트들에 분산 서비스 공격용 툴*을 설치하여 에이전트(Agent)로 만든 후 DDoS 공격에 이용한다.

- 공격의 범위를 확대하기 위해 일부 호스트에 다수의 에이전트를 관리할 수 있는 핸들러(Handler) 프로그램을 설치하여 마스터(Master)로 지정한 후 공격에 이용하기도 한다.



DDoS 공격 예시

분산 서비스 공격용 툴
에이전트(Agent)의 역할을 수행하도록 설계된 프로그램으로 데몬(Daemon)이라고 부르며, 다음과 같은 종류가 있습니다.
- Trin00 : 가장 초기 형태의 데몬으로, 주로 UDP Flooding 공격을 수행함
- TFN(Tribe Flooding Network) : UDP Flooding 뿐만 아니라 TCP SYN Flood 공격, ICMP 응답 요청, 스머핑 공격등을 수행함
- TFN2K : TFN의 확장판
- Stacheldraht : 이전 툴들의 기능을 유지하면서, 공격자, 마스터, 에이전트가 쉽게 노출되지 않도록 암호화된 통신을 수행하며, 툴이 자동으로 업데이트되도록 설계됨

8 네트워크 침해 공격 관련 용어

용어	의미
스미싱(Smishing)	• 문자 메시지(SMS)를 이용해 사용자의 개인 신용 정보를 빼내는 수법 • 초기에는 문자 메시지를 이용해 개인 비밀정보나 소액 결제를 유도하는 형태로 시작되었다. • 현재는 각종 행사 안내, 경품 안내 등의 문자 메시지에 링크를 걸어 안드로이드 앱 설치 파일인 apk 파일을 설치하도록 유도하여 사용자 정보를 빼가는 수법으로 발전하고 있다.
스피어 피싱 (Spear Phishing)	사회 공학*의 한 기법으로, 특정 대상을 선정한 후 그 대상에게 일반적인 이메일로 위장한 메일을 지속적으로 발송하여, 발송 메일의 본문 링크나 첨부된 파일을 클릭하도록 유도해 사용자의 개인 정보를 탈취한다.
APT(Advanced Persistent Threats, 지능형 지속 위협)	• 다양한 IT 기술과 방식들을 이용해 조직적으로 특정 기업이나 조직 네트워크에 침투해 활동 거점을 마련한 뒤 때를 기다리면서 보안을 무력화시키고 정보를 수집한 다음 외부로 빼돌리는 형태의 공격 • 공격 방법 – 내부자에게 악성코드가 포함된 이메일을 오랜 기간 동안 꾸준히 발송해 한 번이라도 클릭되길 기다리는 형태 – 스턱스넷(Stuxnet)과 같이 악성코드가 담긴 이동식 디스크(USB) 등으로 전파하는 형태 – 악성코드에 감염된 P2P 사이트에 접속하면 악성코드에 감염되는 형태 등

사회 공학(Social Engineering)
사회 공학이란 컴퓨터 보안에 있어서, 인간 상호 작용의 깊은 신뢰를 바탕으로 사람들을 속여 정상 보안 절차를 깨트리기 위한 비기술적 시스템 침입 수단을 말합니다.

무작위 대입 공격 (Brute Force Attack)	암호화된 문서의 암호키를 찾아내기 위해 적용 가능한 모든 값을 대입하여 공격하는 방식
큐싱(Qshing)	QR코드(Quick Response Code)*를 통해 악성 앱의 다운로드를 유도하거나 악성 프로그램을 설치하도록 하는 금융사기 기법의 하나로, QR코드와 개인정보 및 금융정보를 낚는다(Fishing)는 의미의 합성 신조어이다.
SQL 삽입(Injection) 공격	전문 스캐너 프로그램* 혹은 봇넷 등을 이용해 웹사이트를 무차별적으로 공격하는 과정에서 취약한 사이트가 발견되면 데이터베이스 등의 데이터를 조작하는 일련의 공격 방식
크로스 사이트 스크립팅(XSS; Cross Site Scripting)	• 네트워크를 통한 컴퓨터 보안 공격의 하나로, 웹 페이지의 내용을 사용자 브라우저에 표현하기 위해 사용되는 스크립트의 취약점을 악용한 해킹 기법 • 사용자가 특정 게시물이나 이메일의 링크를 클릭하면 악성 스크립트가 실행되어 페이지가 깨지거나, 사용자의 컴퓨터에 있는 로그인 정보나 개인 정보, 내부 자료 등이 해커에게 전달된다.

9 정보 보안 침해 공격 관련 용어

용어	의미
좀비(Zombie) PC	악성코드에 감염되어 다른 프로그램이나 컴퓨터를 조종하도록 만들어진 컴퓨터로, C&C(Command & Control) 서버의 제어를 받아 주로 DDoS 공격 등에 이용된다.
C&C 서버	해커가 원격지에서 감염된 좀비 PC에 명령을 내리고 악성코드를 제어하기 위한 용도로 사용하는 서버를 말한다.
봇넷(Botnet)	악성 프로그램에 감염되어 악의적인 의도로 사용될 수 있는 다수의 컴퓨터들이 네트워크로 연결된 형태를 말한다.
웜(Worm)	네트워크를 통해 연속적으로 자신을 복제하여 시스템의 부하를 높임으로써 결국 시스템을 다운시키는 바이러스의 일종으로, 분산 서비스 거부 공격, 버퍼 오버플로 공격*, 슬래머* 등이 웜 공격의 한 형태이다.
제로 데이 공격 (Zero Day Attack)	보안 취약점이 발견되었을 때 발견된 취약점의 존재 자체가 널리 공표되기도 전에 해당 취약점을 통하여 이루어지는 보안 공격으로, 공격의 신속성을 의미한다.
키로거 공격 (Key Logger Attack)	컴퓨터 사용자의 키보드 움직임을 탐지해 ID, 패스워드, 계좌번호, 카드번호 등과 같은 개인의 중요한 정보를 몰래 빼가는 해킹 공격
랜섬웨어 (Ransomware)	인터넷 사용자의 컴퓨터에 잠입해 내부 문서나 파일 등을 암호화해 사용자가 열지 못하게 하는 프로그램으로, 암호 해독용 프로그램의 전달을 조건으로 사용자에게 돈을 요구하기도 한다.
백도어 (Back Door, Trap Door)	시스템 설계자가 서비스 기술자나 유지 보수 프로그램 작성자(Programmer)의 액세스 편의를 위해 시스템 보안을 제거하여 만들어놓은 비밀 통로로, 컴퓨터 범죄에 악용되기도 한다.
트로이 목마 (Trojan Horse)	정상적인 기능을 하는 프로그램으로 위장하여 프로그램 내에 숨어 있다가 해당 프로그램이 동작할 때 활성화되어 부작용을 일으키는 것으로, 자기 복제 능력은 없다.

QR코드
QR코드는 각종 정보나 프로그램을 담은 격자무늬의 2차원 코드로, 스마트폰 카메라로 스캔하면 관련된 정보가 바로 확인되는 편리한 시스템입니다.

스캐너 프로그램
스캐너 프로그램은 서비스를 제공하는 서버의 상태를 확인하는 프로그램으로, 네트워크 상의 서버들을 스캐닝하면서 서버의 열려있는 포트, 제공 서비스, OS, 취약점 등의 정보를 수집합니다.

버퍼 오버플로 공격
버퍼 오버플로 공격은 버퍼의 크기보다 많은 데이터를 입력하여 프로그램이 비정상적으로 동작하도록 만드는 것입니다.

슬래머(Slammer)
슬래머는 SQL의 허점을 이용하여 SQL 서버를 공격하는 웜 바이러스의 형태로, SQL 슬래머라고도 합니다.

출제예상

1. 다음 중 DDoS(Distributed Denial of Service)에 대한 설명으로 옳지 않은 것은?

① 여러 대의 장비를 이용하여 대량의 데이터를 한 곳의 서버에 집중적으로 전송한다.

② 특정 서버의 정상적인 기능을 방해할 목적으로 사용된다.

③ 표적이 되는 서버는 데이터의 범람으로 결국 시스템의 가동이 멈추게 된다.

④ DDoS 공격자들은 DDoS 공격 중지를 위한 암호 해독용 프로그램의 전달을 조건으로 돈을 요구하기도 한다.

보기 중 Ransomware의 특징이 설명된 것이 하나 있으니 찾아보세요.

출제예상

2. 다음 보기에서 설명하는 것은 무엇인가?

> 보안 취약점이 발견되었을 때 그 문제의 존재 자체가 널리 공표되기도 전에 해당 취약점을 악용하여 이루어지는 보안 공격으로, 공격의 신속성을 의미한다. 일반적으로 컴퓨터에서 취약점이 발견되면 제작자나 개발자가 취약점을 보완하는 패치를 배포하고 사용자가 이를 내려받아 대처하는 것이 관례이나, 이것은 대응책이 공표되기도 전에 공격이 이루어지기 때문에 대처 방법이 없다.

① 스피어 피싱(Spear Phishing)

② 제로 데이 공격(Zero Day Attack)

③ 트로이 목마(Trojan Horse)

④ 랜섬웨어(Ransomware)

이 용어의 핵심은 대응책이 공표되기도 전에 이뤄지는 공격이라는 것입니다. 특정일(D-Day) 이전에 진행되는 공격이 힌트입니다.

출제예상

3. 다음 중 다양한 IT 기술과 방식들을 이용해 조직적으로 특정 기업이나 조직 네트워크에 침투해 활동 거점을 마련한 뒤 때를 기다리면서 보안을 무력화시키고 정보를 수집한 다음 외부로 빼돌리는 APT(Advanced Persistent Threats)의 공격 방법 아닌 것은?

① 내부자에게 악성코드가 포함된 이메일을 오랜 기간 동안 꾸준히 발송해 한 번이라도 클릭하길 기다리는 형태

② 스턱스넷(Stuxnet)과 같이 악성코드가 담긴 이동식 디스크(USB) 등으로 전파하는 형태

③ 악성코드에 감염된 P2P 사이트에 접속하면 악성코드에 감염되는 형태

④ 통신망 보안 정보에 접근 권한이 있는 담당자와 신뢰를 쌓고 전화나 이메일을 통해 그들의 약점과 도움을 이용하는 형태

보기 중에 인간 상호 작용의 깊은 신뢰를 바탕으로 사람들을 속여 정상 보안 절차를 깨트리고 시스템에 침입하는 사회 공학(Social Engineering)과 관련된 내용이 있으니 찾아보세요.

출제예상

4. 다음과 같은 특징을 갖는 서비스 공격 유형은 무엇인가?

> QR코드(Quick Response Code)를 통해 악성 앱의 다운로드를 유도하거나 악성 프로그램을 설치하도록 하는 금융사기 기법의 하나로, QR코드와 개인정보 및 금융정보를 낚는다는 의미의 합성 신조어이다. 스마트폰의 대중화로 모바일 앱을 통한 금융거래가 증가하면서 스마트폰에 악성프로그램을 설치해 해킹하는 방식의 금융사기가 성행하는데, 그 중 QR코드를 이용한 최신 신용금융사기 방식인 이것에 의한 피해가 증가하고 있다.

① 무작위 공격(Brute Force Attack)

② 큐싱(Qshing)

③ SQL 삽입(injection) 공격

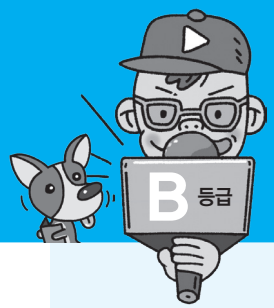
④ 스미싱(Smishing)

이 용어의 특징은 QR코드입니다. QR코드와 낚시를 의미하는 영문인 피싱(Fishing)을 결합해서 생각해 보세요.

▶ 정답 : 1. ④ 2. ② 3. ④ 4. ②

SECTION 190 LIVE

서버 인증



1 보안 서버의 개념

보안 서버란 인터넷을 통해 개인정보*를 암호화하여 송 · 수신할 수 있는 기능을 갖춘 서버를 말한다.

- '개인정보의 기술적 · 관리적 보호조치 기준'에 따르면 보안 서버는 다음과 같은 기능을 갖춰야 한다.
  - 서버에 SSL(Secure Socket Layer)* 인증서를 설치하여 전송 정보를 암호화하여 송 · 수신하는 기능
  - 서버에 암호화 응용 프로그램을 설치하고 전송 정보를 암호화하여 송 · 수신하는 기능
- 스니핑(Sniffing)을 이용한 정보 유출, 피싱(Phishing)을 이용한 위조 사이트 등에 대비하기 위해 보안 서버 구축이 필요하다.

2 인증(認證, Authentication)의 개념

인증은 다중 사용자 컴퓨터 시스템이나 네트워크 시스템에서 로그인을 요청한 사용자의 정보를 확인하고 접근 권한을 검증하는 보안 절차이다.

- 인증에는 네트워크를 통해 컴퓨터에 접속하는 사용자의 등록 여부를 확인하는 것과 전송된 메시지의 위·변조 여부를 확인하는 것이 있다.
- **인증의 주요 유형**
  - 지식 기반 인증(Something You Know)
  - 소유 기반 인증(Something You Have)
  - 생체 기반 인증(Something You Are)
  - 위치 기반 인증(Somewhere You Are)

3 지식 기반 인증(Something You Know)

지식 기반 인증(Something You Know)은 사용자가 기억하고 있는 정보를 기반으로 인증을 수행하는 것이다.

- 지식 기반 인증은 사용자의 기억을 기반으로 하므로 관리 비용이 저렴하다.
- 사용자가 인증 정보를 기억하지 못하면 본인이라도 인증 받지 못한다.
- **고정된 패스워드(Password)** : 사용자가 알고 있는 비밀번호를 접속할 때 마다 반복해서 입력한다.

전문가의 조언

보안 서버와 인증의 개념을 잘 이해하고 기억하세요. 그리고 인증 유형별로 사용되는 방법들에는 어떤 것들이 있는지 파악해 두세요.

인터넷 상에서 송 · 수신되는 개인정보

로그인 시 사용하는 사용자ID와 패스워드, 회원가입 시 등록한 이름, 전화번호, 인터넷 뱅킹 이용 시 등록한 계좌번호, 계좌 비밀번호 등이 있습니다.

SSL(Secure Socket Layer)

SSL은 데이터를 송 · 수신하는 두 컴퓨터 사이, 종단 간, 즉 TCP/IP 계층과 애플리케이션 계층(HTTP, TELNET, FTP 등) 사이에 위치하여 인증, 암호화, 무결성을 보장하는 업계 표준 프로토콜입니다.

- **패스 프레이즈(Passphrase)** : 'iloveyou'와 같이 일반 패스워드보다 길이가 길고 기억하기 쉬운 문장을 활용하여 비밀번호를 구성하는 방법
- **아이핀(i-PIN)** : 인터넷에서 주민등록번호 대신 쓸 수 있도록 만든 사이버 주민등록번호로, 사용자에 대한 신원확인을 완료한 후에 본인확인기관에서 온라인으로 발행한다.

4 소유 기반 인증(Something You Have)

소유 기반 인증은 사용자가 소유하고 있는 것을 기반으로 인증을 수행하는 것이다.

- 소유 기반 인증은 소유물이 쉽게 도용될 수 있으므로 지식 기반 인증 방식이나 생체 기반 인증 방식과 함께 사용된다.
- **신분증** : 사용자의 사진이 포함된 주민등록증, 운전면허증, 여권 등을 사용하여 사용자의 신분을 확인한다.
- **메모리 카드(토큰)** : 마그네틱 선에 보안 코드를 저장해서 사용하는 것으로, 카드 리더기를 통해서만 읽을 수 있다(예 일반 은행 입출금 카드).
- **스마트 카드** : 마이크로프로세서, 카드 운영체제, 메모리 등으로 구성되어 사용자의 정보뿐만 아니라 특정 업무를 처리할 수 있는 기능이 내장되어 있다(예 IC칩이 내장된 카드).
- OTP(One Time Password) : 사용자가 패스워드를 요청할 때마다 암호 알고리즘을 통해 새롭게 생성된 패스워드를 사용하는 것으로, 한 번 사용된 패스워드는 폐기된다.

전문가의 조언

신분증을 사용할 때 신분증의 사진과 사용자의 얼굴을 비교해 보거나 스마트카드 사용 시 추가 패스워드를 요구하는 것과 같이 소유 기반 인증은 지식 기반 인증이나 생체 기반 인증 방식과 함께 사용되는 경우가 많습니다.

5 생체 기반 인증(Something You Are)

생체 기반 인증은 사용자의 고유한 생체 정보를 기반으로 인증을 수행하는 것이다.

- 생채 기반 인증은 사용이 쉽고 도난의 위험도 적으며 위조가 어렵다.
- **생체 인증 대상** : 지문, 홍채/망막, 얼굴, 음성, 정맥 등

6 기타 인증 기법

이외의 기타 인증 기법에는 행위 기반 인증과 위치 기반 인증이 있다.

행위 기반 인증 (Something You Do)	사용자의 행동 정보를 이용해 인증 수행 예 서명, 동작
위치 기반 인증 (Somewhere You Are)	인증을 시도하는 위치의 적절성 확인 예 콜백*, GPS나 IP 주소를 이용한 위치 기반 인증

콜백(Call Back)

콜백은 상대방이 전화로 인증을 요청한 경우, 전화를 끊고 걸려온 번호로 다시 전화를 걸어 해당 전화번호가 유효한지 확인하는 방법입니다.

기출문제 따라잡기 Section 190

출제예상

1. 다음 중 보안 서버에 대한 설명으로 잘못된 것은?

① 보안 서버란 인터넷을 통해 개인과 개인이 직접 연결되어 파일을 공유할 수 있도록 해주는 서버를 말한다.

② 보안 서버는 SSL(Secure Socket Layer) 인증서를 설치하여 전송 정보를 암호화하여 송 · 수신하는 기능을 갖춰야 한다.

③ 보안 서버는 암호화 응용 프로그램을 설치하여 전송 정보를 암호화하여 송 · 수신하는 기능을 갖춰야 한다.

④ 스니핑(Sniffing)을 이용한 정보 유출, 피싱(Phishing)을 이용한 위조 사이트 등에 대비하기 위해 보안 서버 구축이 필요하다.

보안은 암호화와 관련이 있습니다. 보안 서버의 개념을 다시 한 번 생각해 보세요.

출제예상

2. 다음이 설명하는 것은 무엇인가?

- 다중 사용자 컴퓨터 시스템 또는 네트워크 시스템에서 로그인을 요청한 사용자의 정보를 확인하고 접근 권한을 검증하는 보안 절차이다.
- 망(Network)을 경유해서 컴퓨터에 접속해 오는 사용자가 등록된 사용자인지 확인하는 것과 전송된 메시지가 변조되거나 의미가 그릇되지 않고 송신자가 보낸 그대로의 것인지를 확인하는 것이 있다.

① 보안(Secure)

② 접근 통제(Access Control)

③ 인증(Authentication)

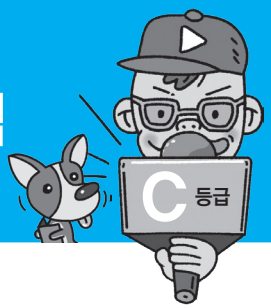
④ 암호화(Encryption)

사용자의 정보를 **확인**하고 **검증**하는 것은 무엇일까요?

▶ 정답 : 1. ① 2. ③

SECTION 191 ● LIVE

보안 아키텍처 / 보안 프레임워크



전문가의 조언

이번 섹션에서는 보안 아키텍처와 보안 프레임워크에 대해 학습합니다. 보안 아키텍처의 개념을 기억하고 대표적인 보안 프레임워크인 ISO 27001의 개념과 함께 보안 통제 항목의 종류를 잘 정리해 두세요.

관리적, 물리적, 기술적 보안 개념의 수립

- **관리적 보안** : 정보보호 정책, 정보보호 조직, 정보자산 분류, 정보보호 교육 및 훈련, 인적 보안, 업무 연속성 관리 등의 정의
- **물리적 보안** : 건물 및 사무실 출입 통제 지침, 전산실 관리 지침, 정보 시스템 보호 설치 및 관리 지침, 재해 복구 센터 운영 등의 정의
- **기술적 보안** : 사용자 인증, 접근 제어, PC, 서버, 네트워크, 응용 프로그램, 데이터(DB) 등의 보안 지침 정의

인프라(Infra)

인프라는 정보 시스템에서 사용되는 서버, 네트워크, 시설, 설비 등의 자원을 의미합니다.

감사 추적(Audit Trails)

감사 추적은 데이터 처리 과정에서의 오류나 외부의 불법적인 침입을 파악하기 위해 정보 시스템 내·외부의 모든 활동을 기록하고 분석하는 것을 의미합니다.

1 보안 아키텍처(Security Architecture)

보안 아키텍처란 정보 시스템의 무결성(Integrity), 가용성(Availability), 기밀성(Confidentiality)을 확보하기 위해 보안 요소 및 보안 체계를 식별하고 이들 간의 관계를 정의한 구조를 말한다.

- 보안 아키텍처를 통해 관리적, 물리적, 기술적 보안 개념의 수립*, 보안 관리 능력의 향상, 일관된 보안 수준의 유지를 기대할 수 있다.
- 보안 아키텍처는 보안 수준에 변화가 생겨도 기본 보안 아키텍처의 수정 없이 지원할 수 있어야 한다.
- 보안 아키텍처는 보안 요구사항의 변화나 추가를 수용할 수 있어야 한다.
- 다음 표는 ITU-T X.805의 보안 표준을 기준으로 구성한 보안 아키텍처 모델이다.

보안 계층 (Security Layers)	인프라* 시스템
	응용 프로그램
	데이터(DB)
	단말기(PC)
	인터페이스
보안 영역 (Security Areas)	정보 시스템
	제어 시스템
	클라우드
	무선
	사물인터넷(IoT; Internet of Things)
보안 요소 (Security Elements)	인증(Authentication)
	접근 통제(Access Control)
	데이터 처리 보호(Data Processing Protection)
	암호화(Encryption)
	감사 추적(Audit Trails)*
	위협 탐지(Threat Detection)

2 보안 프레임워크(Security Framework)

프레임워크는 '뼈대', '골조'를 의미하는 용어이며, 보안 프레임워크는 안전한 정보 시스템 환경을 유지하고 보안 수준을 향상시키기 위한 체계를 말한다.

- ISO 27001은 정보보안 관리를 위한 국제 표준으로, 일종의 보안 인증이자 가장 대표적인 보안 프레임워크이다.
- ISO 27001은 영국의 BSI(British Standards Institute)가 제정한 BS 7799를 기반으로 구성되어 있다.
- ISO 27001은 조직에 대한 정보보안 관리 규격이 정의되어 있어 실제 심사/인증용으로 사용된다.
- 다음은 ISO 27001의 보안 통제 항목이다.

요구사항	주요 내용	통제 항목수
보안 정책(Security Policy)	정보 보호 수행을 위한 경영 방침과 지원 사항	2
정보 보안 조직(Organization of Information Security)	효과적인 보안 관리를 위한 조직 내의 책임과 역할	7
자산 관리(Asset Management)	조직의 자산 보호를 위한 적절한 보호 프로세스	10
인적 자원 보안 (Human Resource Security)	사람의 실수, 절도, 사기, 시설의 오용으로 인한 위험을 줄이기 위한 대응책	6
접근 통제(Access Control)	부적절한 접근에 대한 통제	14
암호화(Cryptography)	무결성, 가용성, 기밀성을 확보하기 위한 암호화 사용	2
물리적 및 환경적 보안(Physical & Environmental Security)	비인가된 접근 및 방해요인 방지	15
통신 보안 (Communications Security)	네트워크 및 시스템 간의 안전한 정보 전송	7
운영 보안(Operations Security)	시스템 설비의 안전한 운영	14
시스템 획득, 개발 및 유지 보수 (System Acquisition, Development & Maintenance)	정보 시스템 내에 보안이 수립되어 있음을 보장하기 위한 대응 방안 확인	13
공급자 관계 (Supplier Relationships)	정보 시스템에 대한 협력 업체의 정보 접근 범위, 정보 보안 및 서비스 제공에 대한 사항	5
정보 보안 사고 관리(Information Security Incident Management)	정보 시스템과 관련된 보안 사고에 대한 대응책	7
정보 보호 측면 업무 연속성 관리 (Information Security Aspects of Business Continuity Management)	업무 활동에 대한 방해요소를 완화시키고 중대한 실패 및 재해로부터 중요 업무를 보호하기 위한 프로세스	4
준거성(Compliance)	범죄 및 민형사상의 법률, 법규, 규정 또는 계약 의무사항 및 보호요구사항의 불일치를 회피하기 위한 대응책	8

출제예상

1. 다음 중 보안 아키텍처에 대한 설명으로 잘못된 것은?

① 보안 아키텍처(Security Architecture)란 정보 시스템의 무결성, 가용성, 기밀성을 확보하기 위해 보안 요소 및 보안 체계를 식별하고 이들 간의 관계를 정의한 구조를 말한다.

② 보안 아키텍처를 통해 관리적, 물리적, 기술적 보안 개념의 수립, 보안 관리 능력의 향상, 일관된 보안 수준의 유지를 기대할 수 있다.

③ 보안 아키텍처는 보안 수준의 변화가 발생할 경우 기본 보안 아키텍처를 수정하여 변화에 빠르게 대응해야 한다.

④ 보안 아키텍처는 보안 요구사항의 변화나 추가를 수용할 수 있어야 한다.

보안 아키텍처는 기본 보안 아키텍처의 수정 없이 변화에 대응할 수 있어야 합니다.

출제예상

2. 다음 중 대표적인 보안 프레임워크인 ISO 27001에 대한 설명으로 잘못된 것은?

① 보안 프레임워크란 안전한 정보 시스템 환경을 유지하고 보안 수준을 향상시키기 위한 체계를 말한다.

② ISO 27001은 정보보호 관리를 위한 국제 표준으로, 일종의 보안 인증이다.

③ ISO 27001은 영국의 BSI(British Standards Institute)가 제정한 BS 7799를 기반으로 구성되어 있다.

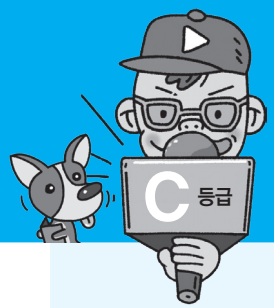
④ ISO 27001은 조직에 대한 정보보안 관리 규격은 제외되어 있어 심사/인증용으로는 사용할 수 없다.

ISO 27001은 현업에서 심사나 인증용으로 사용하고 있는 대표적인 보안 프레임워크입니다.

▶ 정답 : 1. ③ 2. ④

SECTION 192 LIVE

로그 분석



1 로그(Log)의 개념

로그란 시스템 사용에 대한 모든 내역을 기록해 놓은 것으로, 이러한 로그 정보를 이용하면 시스템 침해 사고 발생 시 해킹 흔적이나 공격 기법을 파악할 수 있다.

- 로그 정보를 정기적으로 분석하면 시스템에 대한 침입 흔적이나 취약점을 확인할 수 있다.

2 리눅스(LINUX) 로그

리눅스에서는 시스템의 모든 로그를 var/log 디렉터리에서 기록하고 관리한다.

- 로그 파일을 관리하는 syslogd 데몬*은 etc/syslog.conf 파일을 읽어 로그 관련 파일들의 위치를 파악한 후 로그 작업을 시작한다.
- syslog.conf 파일을 수정하여 로그 관련 파일들의 저장 위치와 파일명을 변경할 수 있다.

3 리눅스의 주요 로그 파일

리눅스에서는 커널 로그, 부팅 로그, 크론 로그, 시스템 로그, 보안 로그, FTP 로그, 메일 로그 등을 기록하고 관리한다.

로그	파일명	데몬	내용
커널* 로그	/dev/console	kernel	커널에 관련된 내용을 관리자에게 알리기 위해 파일로 저장하지 않고 지정된 장치에 표시한다.
부팅 로그	/var/log/boot.log	boot	부팅 시 나타나는 메시지들을 기록한다.
크론 로그	/var/log/cron	crond	작업 스케줄러인 crond의 작업 내역을 기록한다.
시스템 로그	/var/log/messages	syslogd	커널(kernel)에서 실시간으로 보내오는 메시지들을 기록한다.
보안 로그	/var/log/secure	xinetd	시스템의 접속에 대한 로그를 기록한다.
FTP 로그	/var/log/xferlog	ftpd	FTP로 접속하는 사용자에 대한 로그를 기록한다.
메일 로그	/var/log/maillog	sendmail popper	송수신 메일에 대한 로그를 기록한다.

전문가의 조언

시스템에 대한 보안 사고가 발생하면 시스템의 모든 활동이 기록되어 있는 로그 파일을 분석하여 그 원인을 찾을 수 있습니다. 또한 로그 데이터 분석을 통해 시스템의 취약점을 미리 파악하여 이를 관리할 수도 있습니다. 이번 섹션에서는 LINUX와 Windows에서 사용되는 로그 파일에 대해 학습합니다. LINUX와 Windows에서 사용되는 로그 파일을 종류를 파악해 두세요.

데몬(Daemon)

데몬은 사용자의 직접적인 개입 없이 특정 상태가 되면 자동으로 동작하는 시스템 프로그램으로, LINUX 계열에서는 데몬이라고 하며, Windows 계열에서는 서비스라고 부릅니다.

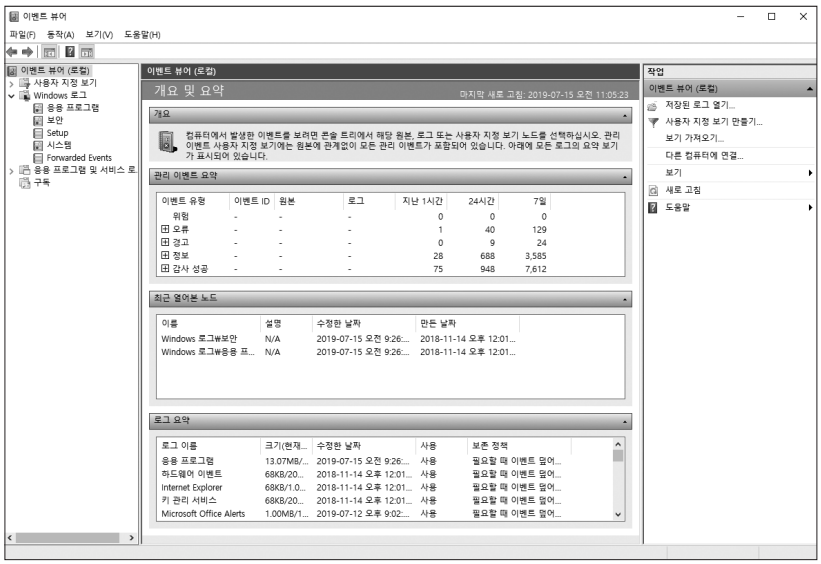
커널(Kernel)

커널은 운영체제의 가장 핵심적인 부분으로, 하드웨어를 보호하고, 프로그램과 하드웨어 간의 인터페이스 역할을 담당합니다. 프로세스 관리, 기억장치 관리, 파일 관리, 입·출력 관리, 프로세스 간 통신, 데이터 전송 및 변환 등 여러 가지 기능을 수행합니다.

4 윈도우(Windows) 로그

Windows 시스템에서는 이벤트 로그 형식으로 시스템의 로그를 관리한다.

- Windows의 이벤트 뷰어를 이용하여 이벤트 로그를 확인할 수 있다.
- Windows의 이벤트 뷰어는 [제어판] → [관리 도구] → [이벤트 뷰어]를 선택하여 실행한다.



Windows 10의 이벤트 뷰어

5 Windows 이벤트 뷰어의 로그

Windows 이벤트 뷰어에서는 응용 프로그램 로그, 보안 로그, 시스템 로그, Setup 로그, Forwarded Events 로그를 확인할 수 있다.

로그	내용
응용 프로그램	• 응용 프로그램에서 발생하는 이벤트가 기록된다. • 기록되는 이벤트는 응용 프로그램 개발자에 의해 결정된다.
보안	로그온 시도, 파일이나 객체 생성, 조회, 제거 등의 리소스 사용과 관련된 이벤트가 기록된다.
시스템	Windows 시스템 구성 요소에 의해 발생하는 이벤트가 기록된다.
Setup	프로그램 설치와 관련된 이벤트가 기록된다.
Forwarded Events	다른 컴퓨터와의 상호 작용으로 발생하는 이벤트가 기록된다.

기출문제 따라잡기

출제예상

1. 다음 중 리눅스(LINUX)의 주요 로그 파일이 아닌 것은?

① console ② cron
③ secure ④ syslogd

보기 중에 로그 파일이 아니라 로그 파일을 관리하는 데몬이 하나 포함되어 있으니 찾아보세요.

출제예상

2. 다음 중 윈도우(Windows)의 이벤트 뷰어를 통해 확인할 수 있는 로그 항목이 아닌 것은?

① 응용 프로그램 ② 보안
③ 시스템 ④ 로그인

로그인과 같이 시스템에 접근을 시도하는 것은 '보안' 로그 항목에서 기록하고 관리하는 내용입니다.

출제예상

3. 다음 중 리눅스(LINUX)의 로그 파일에 대한 설명으로 잘못된 것은?

① 시스템의 모든 로그를 'var/log' 디렉터리에서 기록하고 관리한다.
② 로그 파일 중 시스템 로그(/var/log/messages)는 커널(Kernel)에서 실시간으로 보내오는 메시지들을 기록하고 관리한다.
③ syslog.conf 파일에는 로그 관련 파일들의 위치가 기록되어 있으므로 수정되거나 삭제되지 않도록 관리해야 한다.
④ 로그 파일 중 메일 로그(/var/log/maillog)는 주고받는 메일에 대한 로그를 기록하고 관리한다.

로그 관련 파일들의 저장 위치와 파일명을 변경할 수 있다고 했죠? 로그 관련 파일들의 저장 위치와 파일명이 변경되었다면, 로그 관련 파일들에 대한 정보를 저장한 파일도 변경해야 겠네요.

▶ 정답 : 1. ④ 2. ④ 3. ③

SECTION 193 ● LIVE

보안 솔루션

전문가의 조언

이번 섹션에서는 외부의 불법적인 침입으로부터 시스템을 보호하기 위한 각종 솔루션의 기능과 특징을 학습합니다. 어떤 보안 솔루션을 말하는지 구분할 수 있도록 각각의 기능과 특징을 잘 정리해 두세요.

1 보안 솔루션의 개념

보안 솔루션이란 접근 통제, 침입 차단 및 탐지 등을 수행하여 외부로부터의 불법적인 침입을 막는 기술 및 시스템을 말한다.

- 주요 보안 솔루션에는 방화벽, 침입 탐지 시스템(IDS), 침입 방지 시스템(IPS), 데이터 유출 방지(DLP), 웹 방화벽, VPN, NAC 등이 있다.

2 방화벽(Firewall)

방화벽은 기업이나 조직 내부의 네트워크와 인터넷 간에 전송되는 정보를 선별하여 수용 · 거부 · 수정하는 기능을 가진 침입 차단 시스템이다.

- 내부 네트워크에서 외부로 나가는 패킷은 그대로 통과시키고, 외부에서 내부 네트워크로 들어오는 패킷은 내용을 엄밀히 체크하여 인증된 패킷만 통과시키는 구조이다.
- 해킹 등에 의한 외부로의 정보 유출을 막기 위해 사용한다.

3 침입 탐지 시스템(IDS; Intrusion Detection System)

침입 탐지 시스템은 컴퓨터 시스템의 비정상적인 사용, 오용, 남용 등을 실시간으로 탐지하는 시스템이다.

- 방화벽과 같은 침입 차단 시스템만으로는 내부 사용자의 불법적인 행동과 외부 해킹에 100% 완벽하게 대처할 수는 없다.
- 문제가 발생한 경우 모든 내 · 외부 정보의 흐름을 실시간으로 차단하기 위해 해커 침입 패턴에 대한 추적과 유해 정보 감시가 필요하다.
- **오용 탐지(Misuse Detection)** : 미리 입력해 둔 공격 패턴이 감지되면 이를 알려준다.
- **이상 탐지(Anomaly Detection)** : 평균적인 시스템의 상태를 기준으로 비정상적인 행위나 자원의 사용이 감지되면 이를 알려준다.
- 침입 탐지 시스템의 위치
  - 패킷이 라우터로 들어오기 전 : 네트워크에 시도되는 모든 공격을 탐지할 수 있다.
  - 라우터 뒤 : 라우터에 의해 패킷 필터링을 통과한 공격을 탐지할 수 있다.
  - 방화벽 뒤 : 내부에서 외부로 향하는 공격을 탐지할 수 있다.

- 내부 네트워크 : 내부에서 내부 네트워크의 해킹 공격을 탐지할 수 있다.
- DMZ : DMZ는 외부 인터넷에 서비스를 제공하는 서버가 위치하는 네트워크로, 강력한 외부 공격이나 내부 공격으로부터 중요 데이터를 보호하거나 서버의 서비스 중단을 방지할 수 있다.

4 침입 방지 시스템(IPS; Intrusion Prevention System)

침입 방지 시스템은 방화벽과 침입 탐지 시스템을 결합한 것이다.

- 비정상적인 트래픽을 능동적으로 차단하고 격리하는 등의 방어 조치를 취하는 보안 솔루션이다.
- 침입 탐지 기능으로 패킷을 하나씩 검사한 후 비정상적인 패킷이 탐지되면 방화벽 기능으로 해당 패킷을 차단한다.

5 데이터 유출 방지(DLP; Data Leakage/Loss Prevention)

데이터 유출 방지는 내부 정보의 외부 유출을 방지하는 보안 솔루션이다.

- 사내 직원이 사용하는 PC와 네트워크상의 모든 정보를 검색하고 메일, 메신저, 웹하드, 네트워크 프린터 등의 사용자 행위를 탐지 · 통제해 외부로의 유출을 사전에 막는다.

6 웹 방화벽(Web Firewall)

웹 방화벽은 일반 방화벽이 탐지하지 못하는 SQL 삽입 공격*, Cross-Site Scripting(XSS)* 등의 웹 기반 공격을 방어할 목적으로 만들어진 웹 서버에 특화된 방화벽이다.

- 웹 관련 공격을 감시하고 공격이 웹 서버에 도달하기 전에 이를 차단해 준다.

7 VPN(Virtual Private Network, 가상 사설 통신망)

VPN은 가상 사설 네트워크로서 인터넷 등 통신 사업자의 공중 네트워크와 암호화 기술을 이용하여 사용자가 마치 자신의 전용 회선을 사용하는 것처럼 해주는 보안 솔루션이다.

- VPN은 암호화된 규격을 통해 인터넷망을 전용선의 사설망을 구축한 것처럼 이용하므로 비용 부담을 줄일 뿐만 아니라 원격지의 지사, 영업소, 이동 근무자가 지역적인 제한 없이 업무를 수행할 수 있다.

8 NAC(Network Access Control)

NAC은 네트워크에 접속하는 내부 PC의 MAC 주소를 IP 관리 시스템에 등록한 후 일관된 보안 관리 기능을 제공하는 보안 솔루션이다.

SQL 삽입 공격
SQL 삽입 공격이란 전문 스캐너 프로그램 혹은 봇넷 등을 이용해 웹사이트를 무차별적으로 공격하는 과정에서 취약한 사이트가 발견되면 데이터베이스 등의 데이터를 조작하는 일련의 공격 방식을 말합니다.

Cross-Site Scripting(XSS)
Cross-Site Scripting이란 네트워크를 통한 컴퓨터 보안 공격의 하나로, 웹 페이지의 내용을 사용자 브라우저에 표현하기 위해 사용되는 스크립트의 취약점을 악용한 해킹 기법을 말합니다.

- 내부 PC의 소프트웨어 사용 현황을 관리하여 불법적인 소프트웨어 설치를 방지한다.
- 일괄적인 배포 관리 기능을 이용해 백신이나 보안 패치 등의 설치 및 업그레이드를 수행한다.
- 네트워크에 접속한 비인가된 시스템을 자동으로 검출하여 자산을 관리한다.

9 ESM(Enterprise Security Management)

ESM은 다양한 장비에서 발생하는 로그 및 보안 이벤트를 통합하여 관리하는 보안 솔루션이다.

- 방화벽, IDS, IPS, 웹 방화벽, VPN 등에서 발생한 로그 및 보안 이벤트를 통합하여 관리함으로써 비용 및 자원을 절약할 수 있다.
- 보안 솔루션 간의 상호 연동을 통해 종합적인 보완 관리 체계를 수립할 수 있다.

기출문제 따라잡기 Section 193

출제예상

1. 다음은 무엇에 대한 설명인가?

> 기업이나 조직 내부의 네트워크와 인터넷 간에 전송되는 정보를 선별하여 수용 · 거부 · 수정하는 기능을 가진 보안 시스템이다. 내부 네트워크에서 외부로 나가는 패킷은 그대로 통과시키고, 외부에서 내부 네트워크로 들어오는 패킷은 내용을 엄밀히 체크하여 인증된 패킷만 통과시키는 구조로, 해킹 등에 의한 외부로의 정보 유출을 막기 위해 사용한다.

① 침입 탐지 시스템(IDS; Intrusion Detection System)
② 침입 방지 시스템(IPS; Intrusion Prevention System)
③ 방화벽(Firewall)
④ 데이터 유출 방지(DLP; Data Leakage/Loss Prevention)

내부의 네트워크와 인터넷 사이에서 보호막의 역할을 수행하는 보안 솔루션은 무엇일까요?

출제예상

2. 다음 중 보안 솔루션에 대한 설명으로 옳지 않은 것은?

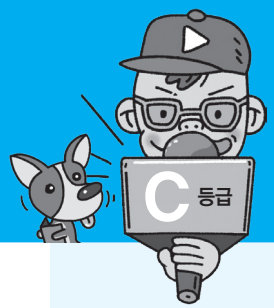
① 침입 탐지 시스템(IDS; Intrusion Detection System) : 컴퓨터 시스템의 비정상적인 사용, 오용, 남용 등을 실시간으로 탐지하는 시스템이다.
② 침입 방지 시스템(IPS; Intrusion Prevention System) : 방화벽과 침입 탐지 시스템(IDS)을 결합한 보안 솔루션이다.
③ 데이터 유출 방지(DLP; Data Leakage/Loss Prevention) : 사내 직원이 사용하는 PC와 네트워크상의 모든 정보를 검색하고 사용자 행위를 탐지 · 통제해 외부로의 유출을 사전에 막는다.
④ NAC(Network Access Control) : 일반 방화벽에서는 탐지하지 못하는 SQL 삽입 공격, Cross-Site Scripting(XSS) 등의 웹 기반 공격을 방어할 목적으로, 웹 서버에 특화된 방화벽이다.

NAC는 내부 네트워크를 관리하는 보안 솔루션입니다. 그럼 웹 서버에 특화된 보안 솔루션은 무엇인지 기억해 보세요.

▶ 정답 : 1. ③ 2. ④

SECTION 194 LIVE

취약점 분석 · 평가



1 취약점 분석 · 평가의 개요

취약점 분석 · 평가란 사이버 위협으로부터 정보 시스템의 취약점을 분석 및 평가한 후 개선하는 일련의 과정을 말한다.

- 안정적인 정보 시스템의 운영을 방해하는 사이버 위협에 대한 항목별 세부 점검항목을 파악하여 취약점 분석을 수행한다.
- 취약점이 발견되면, 위험 등급을 부여하고 개선 방향을 수립한다.

2 취약점 분석 · 평가 범위 및 항목

- 취약점 분석 · 평가의 범위는 정보 시스템과 정보 시스템 자산에 직 · 간접적으로 관여된 물리적, 관리적, 기술적 분야를 포함한다.
- 취약점 분석 · 평가의 기본 항목은 상, 중, 하 3단계로 중요도를 분리한다.
- 취약점 분석 · 평가의 기본 항목의 중요도가 '상'인 항목은 필수적으로 점검한다.
- 취약점 분석 · 평가의 기본 항목의 중요도가 '중', '하'인 항목은 회사의 사정에 따라 선택적으로 점검한다.

3 수행 절차 및 방법

❶ 취약점 분석 · 평가 계획 수립

취약점 분석 · 평가를 위한 수행 주체, 수행 절차, 소요 예산, 산출물 등의 세부 계획을 수립한다.

❷ 취약점 분석 · 평가 대상 선별

- 정보 시스템의 자산을 식별하고, 유형별로 그룹화하여 취약점 분석 · 평가 대상 목록을 작성한다.
- 식별된 대상 목록의 각 자산에 대해 중요도를 산정한다.

❸ 취약점 분석 수행

- 취약점 분석 평가를 위한 관리적, 물리적, 기술적 세부 점검 항목표를 작성한다.
- 관리적 점검은 정보보호 정책이나 지침 등 관련 문서 확인과 정보보호 담당자, 시스템 관리자, 사용자 등과의 면담을 통해 수행한다.
- 물리적 점검은 전산실, 발전실 등 통제구역을 직접 찾아가 현장 점검 형태로 수행한다.
- 기술적 점검은 점검 도구, 모의 해킹 등을 통해 수행한다.

전문가의 조언

이번 섹션에서는 '주요정보통신기반시설 취약점 분석 · 평가 기준' 행정규칙에 제시된 정보 통신 기반 시설에 대한 취약점 분석 · 평가에 대한 내용을 학습합니다.

❹ 취약점 평가 수행

- 취약점 분석 세부 결과를 작성한다.
- 파악된 취약점별로 위험등급을 상, 중, 하 3단계로 표시한다.
- 위험등급 '상'은 조기 개선, 위험등급 '중', '하'는 중기 또는 장기 개선으로 구분하여 개선 방향을 수립한다.

기출문제 따라잡기 Section 194

출제예상

1. 다음 중 취약점 분석 및 평가에 대한 설명으로 잘못된 것은?

① 취약점 분석 · 평가란 사이버 위협으로부터 정보 시스템의 취약점을 분석 및 평가한 후 개선하는 일련의 과정을 말한다.

② 취약점 분석 · 평가의 범위는 정보 시스템과 정보 시스템 자산에 직 · 간접적으로 관여된 물리적, 관리적, 기술적 분야를 포함한다.

③ 관리적 점검은 전산실, 발전실 등 통제구역을 직접 찾아가 현장 점검 형태로 수행한다.

④ 위험등급 '상'은 조기 개선, 위험등급 '중', '하'는 중기 또는 장기 개선으로 구분하여 개선 방향을 수립한다.

취약점 분석 수행 시 관리적, 물리적, 기술적 점검 방법 중 물리적으로 직접 현장을 찾아가 점검하는 방법이 무엇이었는지 생각해 보세요.

▶ 정답 : 1. ③

예·상·문·제·은·행

해설은 827쪽에 있습니다.

1. 다음 중 Ping of Death에 대한 설명으로 잘못된 것은?

① 공격자는 송신 주소를 공격 대상지의 IP 주소로 위장하고 해당 네트워크 라우터의 브로드캐스트 주소를 수신지로 하여 패킷을 전송하면, 라우터의 브로드캐스트 주소로 수신된 패킷은 해당 네트워크 내의 모든 컴퓨터로 전송된다.

② 공격 대상은 분할된 대량의 패킷을 수신함으로써 분할되어 전송된 패킷을 재조립해야 하는 부담을 갖는다.

③ 공격 대상은 분할되어 전송된 각각의 패킷들의 ICMP Ping 메시지에 대한 응답을 처리하느라 결국 다운되게 된다.

④ jolt, sPING, ICMP bug, IceNewk 등의 변종 공격에 대비하여 ICMP Ping 메시지가 전송되지 못하도록 방화벽에서 차단하는 기술이 개발되었다.

2. 다음 중 SMURFING(스머핑)에 대한 설명으로 잘못된 것은?

① SMURFING은 신뢰성 있는 전송을 위해 수행하는 3-way-handshake 과정을 의도적으로 중단시킴으로써 공격 대상지인 서버가 대기 상태에 놓여 정상적인 서비스를 수행하지 못하게 하는 공격 방법이다.

② 해당 네트워크 내의 모든 컴퓨터는 수신된 패킷에 대한 응답 메시지를 송신 주소인 공격 대상지로 집중적으로 전송하게 되는데, 이로 인해 공격 대상지는 네트워크 과부하로 인해 정상적인 서비스를 수행할 수 없게 된다.

③ SMURFING 공격을 무력화하는 방법 중 하나는 각 네트워크 라우터에서 브로드캐스트 주소를 사용할 수 없게 미리 설정해 놓는 것이다.

④ 브로드캐스트 주소란 네트워크 내의 특정 호스트를 대상으로 패킷을 전송하는 것이 아니라 네트워크 내의 전체 호스트를 대상으로 패킷을 전송할 때 사용하는 주소이다.

3. 다음에 제시된 내용은 무엇에 대한 설명인가?

> 패킷의 크기가 커 여러 개로 분할되어 전송될 때 분할 순서를 알 수 있도록 Fragment Offset 값을 함께 전송하는데, 이 Offset 값을 변경시켜 수신 측에서 패킷을 재조립할 때 오류로 인한 과부하를 발생시킴으로써 시스템이 다운되도록 하는 공격 방법이다.

① Ping of Death ② Land
③ TearDrop ④ DDoS

4. 다음 중 Land 공격에 대비하는 방법으로 옳은 것은?

① 송신 IP 주소와 수신 IP 주소의 적절성을 검사한다.

② Fragment Offset이 잘못된 경우 해당 패킷을 폐기하도록 설정한다.

③ 수신지의 'SYN' 수신 대기 시간을 줄이거나 침입 차단 시스템을 활용한다.

④ 각 네트워크 라우터에서 브로드캐스트 주소를 사용할 수 없게 미리 설정해 놓는다.

5. 다음의 분산 서비스 공격용 툴 중에서 공격자, 마스터, 에이전트가 쉽게 노출되지 않도록 암호화된 통신을 수행하며, 툴이 자동으로 업데이트되도록 설계된 것은?

① Trin00 ② TFN
③ TFN2K ④ Stacheldraht

6. 다음에 제시된 내용은 서비스 거부 공격 방법 중 무엇에 대한 설명인가?

> • 여러 곳에 분산된 공격 지점에서 한 곳의 서버에 대해 분산 서비스 공격을 수행하는 것으로, 네트워크에서 취약점이 있는 호스트들을 탐색한 후 이들 호스트들에 분산 서비스 공격용 툴을 설치하여 에이전트(Agent)로 만든 후 공격에 이용한다.
> • 공격의 범위를 확대하기 위해 일부 호스트에 다수의 에이전트를 관리할 수 있는 핸들러(Handler) 프로그램을 설치하여 마스터(Master)로 지정한 후 공격에 이용하기도 한다.

① SQL 삽입(injection) 공격

② DDoS(Distributed Denial of Service)

③ APT(Advanced Persistent Threats)

④ Smishing

7. 다음 중 정보 보안 침해 공격 관련 용어에 대한 설명이 잘못된 것은?

① 봇넷(Botnet) : 악성 프로그램에 감염되어 악의적인 의도로 사용될 수 있는 다수의 컴퓨터들이 네트워크로 연결된 형태를 말함

② C&C 서버 : 해커가 원격지에서 감염된 좀비 PC에 명령을 내리고 악성코드를 제어하기 위한 용도로 사용하는 서버를 말함

③ 백도어(Back Door, Trap Door) : 시스템 설계자가 서비스 기술자나 유지 보수 프로그램 작성자(Programmer)의 액세스 편의를 위해 시스템 보안을 제거하여 만들어놓은 비밀 통로로, 컴퓨터 범죄에 악용되기도 함

▶ **정답 :** 1. ① 2. ① 3. ③ 4. ① 5. ④ 6. ② 7. ④

예·상·문·제·은·행

해설은 827쪽에 있습니다.

④ 키로거 공격(Key Logger Attack) : 인터넷 사용자의 컴퓨터에 잠입해 내부 문서나 파일 등을 암호화해 사용자가 열지 못하게 하는 프로그램으로, 암호 해독용 프로그램의 전달을 조건으로 사용자에게 돈을 요구하기도 함

8. 다음은 네트워크 침해 공격 중 하나를 설명한 것이다. 지문에 제시된 내용에 해당하는 네트워크 침해 공격은 무엇인가?

- 다양한 IT 기술과 방식들을 이용해 조직적으로 특정 기업이나 조직 네트워크에 침투해 활동 거점을 마련한 뒤 때를 기다리면서 보안을 무력화시키고 정보를 수집한 다음 외부로 빼돌리는 형태의 공격이다.
- 공격 방법에는 내부자에게 악성코드가 포함된 이메일을 오랜 기간 동안 꾸준히 발송해 한 번이라도 클릭되길 기다리는 형태, 스턱스넷(Stuxnet)과 같이 악성코드가 담긴 이동식 디스크(USB) 등으로 전파하는 형태, 악성코드에 감염된 P2P 사이트에 접속하면 악성코드에 감염되는 형태 등이 있다.

① 무작위 대입 공격(brute force attack)
② 크로스 사이트 스크립팅(XSS; Cross Site Scripting)
③ 지능형 지속 위협(APT; Advanced Persistent Threats)
④ 스피어 피싱(Spear Phishing)

9. 지식 기반 인증 방법 중 하나로 'iloveyou'와 같이 일반 패스워드보다 길이가 길고 기억하기 쉬운 문장을 활용하여 비밀번호를 구성하는 방법은 무엇인가?

① 고정된 패스워드(Password)
② 패스 프레이즈(PassPhrase)
③ i-PIN
④ OTP(One Time Password)

10. 다음 중 인증의 유형과 그 대상이 잘못 연결된 것은?

① Something You Know(알고 있는 것) – 비밀번호
② Something You Have(가지고 있는 것) – 지문, 홍채
③ Somewhere You Are(위치하는 곳) – GPS 기반 인증
④ Something You Do(행동하는 것) – 서명, 동작

11. 다음에 제시된 내용과 관련된 보안 솔루션은 무엇인가?

- 방화벽만으로는 내부 사용자의 불법적인 행동과 외부 해킹에 100% 완벽하게 대처할 수는 없다.
- 문제가 발생한 경우 모든 내·외부 정보의 흐름을 실시간으로 차단하기 위해 해커 침입 패턴에 대한 추적과 유해 정보 감시가 필요하다.

① 방화벽(Firewall)
② 침입 방지 시스템(IPS; Intrusion Prevention System)
③ 침입 탐지 시스템(IDS; Intrusion Detection System)
④ 데이터 유출 방지(DLP; Data Leakage/Loss Prevention)

12. 다음 중 보안 솔루션인 ESM(Enterprise Security Management)에 대한 설명으로 잘못된 것은?

① 다양한 장비에서 발생하는 로그 및 보안 이벤트를 통합하여 관리하는 보안 솔루션이다.
② 방화벽, IDS, IPS, 웹 방화벽, VPN 등에서 발생한 로그 및 보안 이벤트를 통합하여 관리함으로써 비용 및 자원을 절약할 수 있다.
③ 보안 솔루션 간의 상호 연동을 통해 종합적인 보완 관리 체계를 수립할 수 있다.
④ 네트워크에 접속하는 내부 PC의 MAC 주소를 IP 관리 시스템에 등록한 후 일관된 보안 관리 기능을 제공한다.

13. 다음에 제시된 내용과 관련된 보안 솔루션은 무엇인가?

- SQL 삽입 공격, Cross-Site Scripting(XSS) 등의 웹 기반 공격을 방어할 목적으로 만들어진 웹 서버에 특화된 솔루션이다.
- 웹 관련 공격을 감시하고 공격이 웹 서버에 도달하기 전에 이를 차단해 준다.

① 웹 방화벽(Web Firewall)
② 웹 보안 시스템(Web Security System)
③ 침입 탐지 시스템(IDS; Intrusion Detection System)
④ 침입 방지 시스템(IPS; Intrusion Prevention System)

▶ **정답 :** 8. ③ 9. ② 10. ② 11. ③ 12. ④ 13. ①

예·상·문·제·은·행·해·설

1. Section 189

- ①번의 내용은 SMURFING에 대한 설명이다.
- Ping of Death는 Ping 명령을 전송할 때 패킷의 크기를 인터넷 프로토콜 허용 범위(65,536 바이트) 이상으로 전송하여 공격 대상의 네트워크를 마비시키는 서비스 거부 공격이다.

2. Section 189

- ①번의 내용은 SYN Flooding에 대한 설명이다.
- SMURFING은 IP나 ICMP의 특성을 악용하여 엄청난 양의 데이터를 한 사이트에 집중적으로 보냄으로써 네트워크를 불능 상태로 만드는 공격 방법이다.

3. Section 189

- Ping of Death : Ping 명령을 전송할 때 패킷의 크기를 인터넷 프로토콜 허용 범위(65,536 바이트) 이상으로 전송하여 공격 대상의 네트워크를 마비시키는 서비스 거부 공격
- Land : 패킷을 전송할 때 송신 IP 주소와 수신 IP 주소를 모두 공격 대상의 IP 주소로 하여 공격 대상에게 전송하는 것으로, 이 패킷을 받은 공격 대상은 송신 IP 주소가 자신이므로 자신에게 응답을 수행하게 되는데, 이러한 패킷이 계속해서 전송될 경우 자신에 대해 무한히 응답하게 하는 공격
- DDoS : 여러 곳에 분산된 공격 지점에서 한 곳의 서버에 대해 분산 서비스 공격을 수행하는 것으로, 네트워크에서 취약점이 있는 호스트들을 탐색한 후 이들 호스트들에 분산 서비스 공격용 툴을 설치하여 에이전트(Agent)로 만든 후 DDoS 공격에 이용함

4. Section 189

②번은 TearDrop, ③번은 SYN Flooding, ④번은 SMURFING 공격을 대비하는 방법이다.

5. Section 189

- Trin00 : 가장 초기 형태의 데몬으로, 주로 UDP Flooding 공격을 수행함
- TFN(Tribe Flooding Network) : UDP Flooding 뿐만 아니라 TCP SYN Flood 공격, ICMP 응답 요청, 스머핑 공격을 수행함
- TFN2K : TFN의 확장판

6. Section 189

- SQL 삽입(injection) 공격 : 전문 스캐너 프로그램 혹은 봇넷 등을 이용해 웹사이트를 무차별적으로 공격하는 과정에서 취약한 사이트가 발견되면 데이터베이스 등의 데이터를 조작하는 일련의 공격 방식
- APT(Advanced Persistent Threats) : 다양한 IT 기술과 방식들을 이용해 조직적으로 특정 기업이나 조직 네트워크에 침투해 활동 거점을 마련한 뒤 때를 기다리면서 보안을 무력화시키고 정보를 수집한 다음 외부로 빼돌리는 형태의 공격
- Smishing : 문자 메시지(SMS)를 이용해 사용자의 개인 신용 정보를 빼내는 수법

7. Section 189

- ④번의 내용은 랜섬웨어(Ransomware)에 대한 설명이다.
- 키로거 공격(Key Logger Attack) : 컴퓨터 사용자의 키보드 움직임을 탐지해 ID, 패스워드, 계좌번호, 카드번호 등과 같은 개인의 중요한 정보를 몰래 빼가는 해킹 공격

8. Section 189

- 무작위 대입 공격(Brute Force Attack) : 암호화된 문서의 암호키를 찾아내기 위해 적용 가능한 모든 값을 대입하여 공격하는 방법
- 크로스 사이트 스크립팅(XSS; Cross Site Scripting) : 네트워크를 통한 컴퓨터 보안 공격의 하나로, 웹 페이지의 내용을 사용자 브라우저에 표현하기 위해 사용되는 스크립트의 취약점을 악용한 해킹 기법
- 스피어 피싱(Spear Phishing) : 사회 공학의 한 기법으로, 특정 대상을 선정한 후 그 대상에게 일반적인 이메일로 위장한 메일을 지속적으로 발송하여, 발송 메일의 본문 링크나 첨부된 파일을 클릭하도록 유도해 사용자의 개인 정보를 탈취함

9. Section 190

- 고정된 패스워드(Password) : 사용자가 알고 있는 비밀번호를 접속할 때마다 반복해서 입력함
- 아이핀(i-PIN) : 인터넷에서 주민등록번호 대신 쓸 수 있도록 만든 사이버 주민등록번호로, 사용자에 대한 신원확인을 완료한 후에 본인확인기관에서 온라인으로 발행함
- OTP(One Time Password) : 사용자가 패스워드를 요청할 때마다 암호 알고리즘을 통해 새롭게 생성된 패스워드를 사용하는 것으로, 한 번 사용된 패스워드는 폐기됨

10. Section 190

- Something You Have(소유 기반 인증) : 신분증, 메모리 카드(토큰), 스마트 카드, OTP(One Time Password) 등

예·상·문·제·은·행·해·설

- Something You Are(생체 기반 인증) : 지문, 홍채/망막, 얼굴, 음성, 정맥, 키보드 입력 등

11. Section 193

- 방화벽(Firewall) : 기업이나 조직 내부의 네트워크와 인터넷 간에 전송되는 정보를 선별하여 수용 · 거부 · 수정하는 기능을 가진 침입 차단 시스템
- 침입 방지 시스템(IPS; Intrusion Prevention System) : 방화벽과 침입 탐지 시스템을 결합한 것으로 비정상적인 트래픽을 능동적으로 차단하고 격리하는 등의 방어 조치를 취하는 보안 솔루션
- 데이터 유출 방지(DLP; Data Leakage/Loss Prevention) : 내부 정보의 외부 유출을 방지하는 보안 솔루션으로 사내 직원이 사용하는 PC와 네트워크상의 모든 정보를 검색하고 메일, 메신저, 웹하드, 네트워크 프린터 등의 사용자 행위를 탐지 · 통제해 외부로의 유출을 사전에 막음

12. Section 193

④번의 내용은 NAC(Network Access Control)에 대한 설명이다.

13. Section 193

- 침입 탐지 시스템(IDS; Intrusion Detection System) : 컴퓨터 시스템의 비정상적인 사용, 오용, 남용 등을 실시간으로 탐지하는 시스템
- 침입 방지 시스템(IPS; Intrusion Prevention System) : 방화벽과 침입 탐지 시스템을 결합한 것으로 비정상적인 트래픽을 능동적으로 차단하고 격리하는 등의 방어 조치를 취하는 보안 솔루션