문혜영 교수

# 제5과목 정보시스템 구축 관리

## 01 소프트웨어 개발 방법론 활용 A

# 소프트웨어 개발 방법론

## 소프트웨어 개발 방법론의 개요

- 소프트웨어 개발, 유지보수 등에 필요한 여러 가지 일들의 수행 방법과 각종 기법 및 도구를 체계적으로 정리하여 표준화한 것이다.

## 구조적 방법론

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

## 정보공학 방법론

- 정보 시스템의 개발을 위해 상호 연관성 있게 통합 및 적용하는 자료 중심의 방법론
- 개발 주기를 이용하여 대규모 정보 시스템을 구축하는데 적합

# 소프트웨어 개발 방법론

## 객체지향 방법론

- 기계의 부품을 조립하듯이 객체들을 조립해서 필요한 소프트웨어를 구현하는 방법론
- 구성 요소:(객체, 클래스, 메시지),기본 원칙:(캡슐화, 정보은닉, 추상화, 상속성, 다형성)

## 컴포넌트 기반(CBD; Component Based Design) 방법론

- 컴포넌트를 조합하여 하나의 새로운 애플리케이션을 만드는 방법론

## 애자일(Agile) 방법론

- 일정한 주기를 반복하면서 개발 과정을 진행하는 방법론

## 제품 계열 방법론

- 특정 제품에 적용하고 싶은 공통된 기능을 정의하여 개발하는 방법론

# 문제

- 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

정답 1

# 비용 산정 기법

## ➢ 소프트웨어 비용 산정의 개요

- 소프트웨어의 개발 규모를 소요하는 인원, 자원, 기간 등으로 확인하여 필요한 비용을 산정하는 것
- 하향식 비용 산정 기법과 상향식 비용 산정 기법이 있다.

## ➢ 소프트웨어 비용 결정 요소

- 프로젝트 요소 : 제품 복잡도, 시스템 크기, 요구되는 신뢰도
- 자원 요소 : 인적 자원, 하드웨어 자원, 소프트웨어 자원
- 생산성 요소 : 개발자 능력, 개발 기간

# 비용 산정 기법-하향식

## 하향식 비용 산정 기법의 개요

- 과거의 유사한 경험을 바탕으로 전문 지식이 많은 개발자들이 참여한 회의를 통해 비용을 산정

## 전문가 감정 기법

- 조직 내에 있는 경험이 많은 두 명 이상의 전문가에게 비용 산정을 의뢰하는 기법

## 델파이 기법

- 전문가의 감정 기법의 주관적인 편견을 보완하기 위해 많은 전문가의 의견을 종합하여 산정하는 기법

# 비용 산정 기법-상향식

## ➢ 상향식 비용 산정 기법의 개요

- 프로젝트의 세부적인 작업 단위별로 비용을 산정한 후 집계하여 전체 비용을 산정

## ➢ LOC(원시 코드 라인 수; Source Line Of Code) 기법

- 소프트웨어 각 기능의 원시 코드 라인 수의 비관치, 낙관치, 기대치를 측정하여 예측치를 구하고 이를 이용하여 비용을 산정
- 산정 공식
  - 노력(인원) = 개발 기간 × 투입 인원 = LOC / 1인당 월평균 생산 코드 라인수

# 문제

- 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

정답 3

문혜영 교수

# 제5과목 정보시스템 구축 관리

## 02 소프트웨어 개발 방법론 활용 B

# 수학적 산정 기법

## ➢ 수학적 산정 기법의 개요

- COCOCMO 모형, Putnam 모형, 기능 점수(FP) 모형이 있다.

## ➢ COCOMO 모형 개요

- 보헴(Boehm)이 제안, LOC(원시 코드 라인 수)에 의한 비용 산정

## ➢ COCOMO의 소프트웨어 개발 유형

- 조직형(Organic Mode) :  5만 라인 이하의 소프트웨어를 개발하는 유형
- 반분리형(Semi-Detached Mode) : 30만 라인 이하의 소프트웨어를 개발하는 유형
- 내장형(Embedded Mode) : 30만 라인 이상의 소프트웨어를 개발하는 유형

# 수학적 산정 기법

## COCOMO 모형의 종류

- 기본(Basic)형 : 소프트웨어 크기와 개발 유형만을 이용하여 비용을 산정
- 중간(Intermediate)형 : 기본형의 공식을 토대로 사용하나, 4가지 특성의 15가지 요인
- 발전(Detailed)형 COCOMO : 개발 공정별로 보다 자세하고 정확하게 노력을 산출

## Putnam 모형

- 소프트웨어 생명 주기의 전 과정 동안에 사용될 노력의 분포를 가정해 주는 모형

## 기능 점수(FP) 모형

- 총 기능 점수를 산출하며 총 기능 점수와 영향도를 이용하여 기능 점수(FP)를 구한 후 이를 이용해서 비용을 산정하는 기법

# 문제

## ➢ COCOMO의 프로젝트 모드가 아닌 것은?

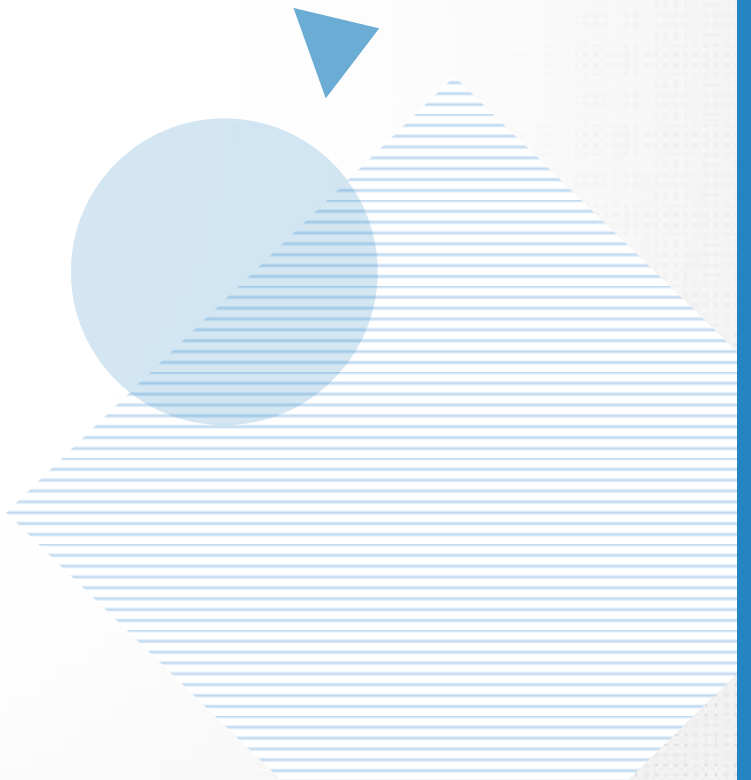
① Organic Mode

② Semi-detached Mode

③ Medium Mode

④ Embedded Mode

정답 3



# 소프트웨어 개발 방법론 결정

## 소프트웨어 개발 방법론 결정의 개요

- 프로젝트 관리와 재사용 현황을 소프트웨어 개발 방법론에 반영하고, 확정된 소프트웨어 생명 주기와 개발 방법론에 맞춰 소프트웨어 개발 단계, 활동, 작업, 절차 등을 정의
- 프로젝트 관리 유형 : 일정 관리, 비용 관리, 인력 관리, 위험 관리, 품질 관리

## 소프트웨어 개발 방법론 결정 절차

- 프로젝트 관리와 재사용 현황을 소프트웨어 개발 방법론에 반영한다.
- 개발단계별 작업 및 절차를 소프트웨어 생명 주기에 맞춰 수립한다.
- 매뉴얼을 작성

# 소프트웨어 개발 표준

## ➢ 소프트웨어 개발 표준의 개요

- 소프트웨어 개발 단계에서 수행하는 품질 관리에 사용되는 국제 표준을 의미
- 종류 : ISO/IEC 12207, CMMI, SPICE

## ➢ ISO/IEC 12207

- ISO(국제표준화기구)에서 만든 표준 소프트웨어 생명 주기 프로세스
- 기본 생명 주기 프로세스, 지원 생명 주기 프로세스, 조직 생명 주기 프로세서로 구분

## ➢ CMMI(Capability Maturity Model Integration)

- CMMI(능력 성숙도 통합 모델)는 소프트웨어 개발 조직의 업무 능력 및 조직의 성숙도를 평가하는 모델
- CMMI의 소프트웨어 프로세스 성숙도는 초기, 관리, 정의, 정량적 관리, 최적화로 구분

# 소프트웨어 개발 표준

## SPICE(Software Process Improvement and Capability Determination)

- SPICE(소프트웨어 처리 개선 및 능력 평가 기준)는 소프트웨어 프로세스를 평가 및 개선하는 국제 표준
- 프로세스 범주 5가지 : 고객-공급자, 공학, 지원, 관리, 조직 프로세스
- SPICE의 프로세스 수행 능력 단계 : 불완전, 수행, 관리, 확립, 예측, 최적화

# 소프트웨어 개발 방법론 테일러링

## ➢ 소프트웨어 개발 방법론 테일러링의 개요

- 프로젝트 상황 및 특성에 맞도록 정의된 소프트웨어 개발 방법론의 절차, 사용기법 등을 수정 및 보완하는 작업

## ➢ 소프트웨어 개발 방법론 테일러링 고려사항

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

## ➢ 소프트웨어 개발 방법론 테일러링 기법(4가지)

- 프로젝트 규모와 복잡도, 프로젝트 구성원, 팀내 방법론 지원, 자동화에 따른 테일러링 기법

# 소프트웨어 개발 프레임워크

## 소프트웨어 개발 프레임워크의 개요

- 여러 가지 기능들을 제공해주는 반제품 형태의 소프트웨어 시스템

## 스프링 프레임워크

- 자바 플랫폼을 위한 오픈 소스 경량형 애플리케이션 프레임워크

## 전자정부 프레임워크

- 우리나라의 공공부문 정보화 사업 시 필요한 기능 및 아키텍퍼를 제공하는 프레임워크
- 응용 소프트웨어의 표준화, 품질 및 재사용성의 향상이 목적

## 닷넷 프레임워크

- Windows 프로그램의 개발 및 실행 환경을 제공하는 프레임워크

# 문제

- 소프트웨어 개발 표준 중 조직의 개발 프로세스 역량 성숙도를 평가하는 표준은?

① CMMI

② SPICE

③ ISO 26262

④ ISO/IEC 12207

정답 1

문혜영 교수

# 제5과목 정보시스템 구축 관리

## 03 IT 프로젝트 정보시스템 구축 관리 A

# 네트워크 관련 신기술

## IoT(Internet of Things, 사물 인터넷)

- 다양한 사물들을 인터넷으로 서로 연결하여 진보된 서비스를 제공하기 위한 서비스 기반 기술

## M2M(Machine to Machine,사물 통신)

- 무선 통신을 이용한 기계와 기계 사이의 통신

## 모바일 컴퓨팅(Mobile Computing)

- 휴대용 기기로 이동하면서 자유로이 네트워크에 접속하여 업무를 처리할 수 있는 환경

## 클라우드 컴퓨팅(Cloud Computing)

- 각종 컴퓨팅 자원을 중앙 컴퓨터에 두고 인터넷 기능을 갖는 단말기로 언제 어디서나 인터넷을 통해 컴퓨터 작업을 수행할 수 있는 환경

# 네트워크 관련 신기술

## ➢ 모바일 클라우드 컴퓨팅(MCC; Mobile Cloud Computing)

- 소비자와 소비자의 파트너가 모바일 기기로 클라우드 컴퓨팅 인프라를 구성하여 여러 가지 정보와 자원을 공유하는 ICT 기술

## ➢ 인터클라우드 컴퓨팅(Inter-Cloud Computing)

- 각기 다른 클라우드 서비스를 연동하거나 컴퓨팅 자원의 동적 할당이 가능하도록 여러 클라우드 서비스 제공자들이 제공하는 클라우드 서비스나 자원을 연결하는 기술

## ➢ 메시 네트워크(Mesh Network)

- 특수 목적을 위한 새로운 방식의 네트워크 기술로, 대규모 디바이스의 네트워크 생성에 최적화되어 있다.

# 네트워크 관련 신기술

## 와이선(Wi-SUN)

- 장거리 무선 통신을 필요로 하는 사물 인터넷 서비스를 위한 저전력 장거리 통신 기술

## NDN(Named Data Networking)

- 콘텐츠 자체의 정보와 라우터 기능만으로 데이터 전송을 수행하는 기술

## NGN(Next Generation Network, 차세대 통신망)

- 유선망뿐만 아니라 이동 사용자를 목표로하며, 이동통신에서 제공하는 완전한 이동성 제공을 목표로 개발

## SDN(Software Defined Networking, 소프트웨어 정의 네트워킹)

- 네트워크를 컴퓨터처럼 모델링하여 여러 사용자가 각각의 소프트웨어들로 네트워킹을 가상화하여 제어하고 관리하는 네트워크

# 네트워크 관련 신기술

## NFC(Near Field Communication, 근거리 무선 통신)

- 고주파(HF)를 이용한 근거리 무선 통신

## UWB(Ultra WideBand, 초광대역)

- 짧은 거리에서 많은 양의 디지털 데이터를 낮은 전력으로 전송하기 위한 무선 기술

## 피코넷(Piconet)

- 여러 개의 독립된 통신장치가 블루투스 기술이나 UWB 통신 기술을 사용하여 통신망을 형성하는 무선 네트워크 기술

## WBAN(Wireless Body Area Network)

- 웨어러블(Wearable) 또는 몸에 심는(Implant) 형태의 센서나 기기를 무선으로 연결하는 개인 영역 네트워킹 기술

# 네트워크 관련 신기술

## GIS(Geographic Information System, 지리 정보 시스템)

- 위성을 이용해 모든 사물의 위치 정보를 제공해 주는 것

## USN(Ubiquitous Sensor Network, 유비쿼터스 센서 네트워크)

- 각종 센서로 수집한 정보를 무선으로 수집할 수 있도록 구성한 네트워크
- RFID 태그를 부착하여 사물의 인식정보는 물론 주변의 환경정보까지 탐지하여 이를 네트워크에 연결하여 정보를 관리하는 것

## SON(Self Organizing Network, 자동 구성 네트워크)

- 주변 상황에 맞추어 스스로 망을 구성하는 네트워크

## 애드 혹 네트워크(Ad-hoc Network)

- 별도의 고정된 유선망을 구축할 수 없는 장소에서 모바일 호스트만을 이용하여 구성한 네트워크

# 네트워크 관련 신기술

## ➢ 네트워크 슬라이싱(Network Slicing)

- 네트워크에서 하나의 물리적인 코어 네트워크 인프라를 독립된 다수의 가상 네트워크로 분리하여 각각의 네트워크를 통한 다양한 고객 맞춤형 서비스를 제공하는 것을 목적으로 하는 네트워크 기술

## ➢ 저전력 블루투스 기술(BLE; Bluetooth Low Energe)

- 일반 블루투스와 동일한 2.4GHz 주파수 대역을 사용하지만 연결되지 않은 대기 상태에서는 절전 모드를 유지하는 기술

## ➢ 지능형 초연결망

- 4차 산업혁명 시대를 맞아 새로운 변화에 따라 급격하게 증가하는 데이터 트래픽을 효과적으로 수용하기 위해 시행되는 정부 주관 사업

# 네트워크 구축

## 네트워크(Network) 설치 구조

- 성형(Star, 중앙 집중형)
- 링형(Ring, 루프형)
- 버스형(Bus)
- 계층형(Tree, 분산형)
- 망형(Mesh)
- 네트워크 분류
  - 근거리 통신망(LAN)
  - 광대역 통신망(WAN)

# 문제

- 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)

정답 3

문혜영 교수

# 제5과목 정보시스템 구축 관리

## 04 IT 프로젝트 정보시스템 구축 관리 B

# 스위치

## 스위치(Switch) 분류

- LAN과 LAN을 연결하여 훨씬 더 큰 LAN을 만드는 장치
- OSI 7 계층의 Layer에 따라 L2, L3, L4, L7으로 분류

## 스위칭(Switch) 방식

- 스위치가 프레임을 전달하는 방식에 다라 Store and Forwarding, Cut-throegh, Fragment Free가 있다.

## 백본 스위치(Backbone Switch)

- 백본에서 스위칭 역할을 하는 장비

## Hierarchical 3 Layer 모델

- 네트워크 구성 시 사용되는 모델의 한 종류로, 액세스, 디스트리뷰션, 코어 계층으로 나뉨

# 경로 제어 / 트래픽 제어

## 경로 제어 프로토콜(Routing Protocol)

- IGP(RIP , OSPF ), EGP , BGP

## 트래픽 제어(Traffic Control)의 개요

- 전송되는 패킷의 흐름 또는 그 양을 조절

## 흐름 제어 (Flow Control)

- 송 · 수신 측 사이에 전송되는 패킷의 양이나 속도를 규제, 정지-대기, 슬라이딩 윈도우

## 폭주(혼잡) 제어(Congesting Control)

- 네트워크 내의 패킷 수를 조절하여 네트워크의 오버플로(Overflow)를 방지하는 기능

## 교착상태(Dead Lock) 방지

- 교착상태란 무한정 기다리는 현상

# 문제

- 흐름 제어에서 한 번에 여러 개의 프레임을 나누어 전송할 경우 효율적인 방법은?

① 정지 및 대기

② 슬라이딩 윈도우

③ 다중 전송

④ 적응적 ARQ

정답 2

# SW 관련 신기술

## 인공지능(AI; Artificial Intelligence)

- 인간의 두뇌와 같이 컴퓨터 스스로 추론, 학습, 판단 등 인간지능적인 작업을 수행하는 시스템

## 뉴럴링크(Neuralink)

- 사람의 뇌와 컴퓨터를 결합하는 기술을 개발하기 위해 설립한 회사

## 딥 러닝(Deep Learning)

- 인간의 두뇌를 모델로 만들어진 인공 신경망을 기반으로 하는 기계 학습 기술

## 전문가 시스템(Expert System)

- 의료 진단 등과 같은 특정 분야의 전문가가 수행하는 고도의 업무를 지원하기 위한 컴퓨터 응용 프로그램

# SW 관련 신기술

## 증강현실(AR; Augmented Reality)

- 실제 촬영한 화면에 가상의 정보를 부가하여 보여주는 기술

## 블록체인(Blockchain)

- P2P 네트워크를 이용하여 온라인 금융 거래 정보를 온라인 네트워크 참여자의 디지털 장비에 분산 저장하는 기술

## 분산 원장 기술(DLT; Distributed Ledger Technology)

- 중앙 관리자나 중앙 데이터 저장소가 존재하지 않고 P2P 망 내의 참여자들에게 모든 거래 목록이 분산 저장되어 거래가 발생할 때마다 지속적으로 갱신되는 디지털 원장

## 해시(Hash)

- 임의의 길이의 입력 데이터나 메시지를 고정된 길이의 값이나 키로 변환

# SW 관련 신기술

## ➢ 양자 암호키 분배(QKD; Qeantum Key Distribution)

- 양자 통신을 위해 비밀키를 분배하여 관리하는 기술

## ➢ 프라이버시 강화 기술(PET; Privacy Enhancing Technology)

- 개인정보 위험 관리 기술

## ➢ 디지털 저작권 관리(DRM; Digital Rights Management)

- 데이터의 저작권 보호를 위해 데이터의 안전한 배포를 활성화하거나 불법 배포를 방지하기 위한 시스템

## ➢ 공통 평가 기준(CC; Common Criterial)

- ISO 15408 표준으로 채택된 정보 보호 제품 평가 기준

# SW 관련 신기술

## 개인정보 영향평가 제도(pia; Privacy Impact Assessment)

- 시스템의 구축·운영이 기업의 고객은 물론 국민의 사생활에 미칠 영향에 대해 미리 조사·분석·평가하는 제도

## 그레이웨어(Grayware)

- 소프트웨어를 제공하는 입장에서는 악의적이지 않은 유용한 소프트웨어라고 주장할 수 있지만 사용자 입장에서는 유용할 수도 있고 악의적일 수도 있는 소프트웨어

## 매시업(Mashup)

- 웹에서 제공하는 정보 및 서비스를 이용하여 새로운 소프트웨어나 서비스, 데이터베이스 등을 만드는 기술

# SW 관련 신기술

## ➢ 리치 인터넷 애플리케이션(RIA; Rich Internet Application)

- 플래시 애니메이션 기술과 웹 서버 애플리케이션 기술을 통합하여 기존 HTML보다 역동적이고 인터랙티브한 웹페이지를 제공하는 신개념의 플래시 웹페이지 제작 기술

## ➢ 시맨틱 웹(Semantic Web)

- 컴퓨터가 사람을 대신하여 정보를 읽고 이해하고 가공하여 새로운 정보를 만들어 낼 수 있도록 이해하기 쉬운 의미를 가진 차세대 지능형 웹

## ➢ 증발품(Vaporware)

- 판매 계획 또는 배포 계획은 발표되었으나 실제로 고객에게 판매되거나 배포되지 않고 있는 소프트웨어

## ➢ 오픈 그리드 서비스 아키텍처(OGSA)

- 애플리케이션 공유를 위한 웹 서비스를 그리드 상에서 제공하기 위해 만든 개방형 표준

문혜영 교수

# 제5과목 정보시스템 구축 관리

## 05 IT 프로젝트 정보시스템 구축 관리 C

# SW 관련 신기술

## ➢ 서비스 지향 아키텍처( SOA; Service Oriented Architecture)

- 기업의 소프트웨어 인프라인 정보시스템을 공유와 재사용이 가능한 서비스 단위나 컴포넌트 중심으로 구축하는 정보기술 아키텍처

## ➢ 서비스형 소프트웨어(SaaS; Software as a Service)

- 소프트웨어의 여러 기능 중에서 사용자가 필요로 하는 서비스만 이용할 수 있도록 한 소프트웨어

## ➢ 소프트웨어 에스크로(임치)(Software Escrow)

- 소프트웨어 개발자의 지식재산권을 보호하고 사용자는 저렴한 비용으로 소프트웨어를 안정적으로 사용 및 유지보수 받을 수 있도록 소스 프로그램과 기술 정보 등을 제3의 기관에 보관하는 것

# SW 관련 신기술

## ➢ 복잡 이벤트 처리(CEP; Complex Event Processing)

- 실시간으로 발생하는 많은 사건들 중 의미가 있는 것만을 추출할 수 있도록 사건 발생 조건을 정의하는 데이터 처리 방법

## ➢ 디지털 트윈(Digital Twin)

- 현실속의 사물을 소프트웨어로 가상화한 모델

# 문제

- 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)

정답 3

# 소프트웨어 개발 보안

## 소프트웨어 개발 보안의 개요

- 보안 위협으로부터 안전한 소프트웨어를 개발하기 위함
- 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)
- 소프트웨어 보안 취약점이 발생하는 경우
  - 보안 요구사항이 정의되지 않은 경우, 소프트웨어 설계 시 논리적 오류가 포함된 경우

# 소프트웨어 개발 직무별 보안 활동

- 프로젝트 관리자(Project Manager)
- 요구사항 분석가(Requirement Specifier):
- 아키텍트(Architect) :
- 설계자(Designer):
- 구현 개발자(Implementer):
- 테스트 분석가(Test Analyst):
- 보안 감사자(Security Auditor)

# 문제

- 아키텍트가 고려해야 할 보안 관련 비즈니스 요구사항을 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)

정답 3

# 소프트웨어 개발 보안 활동 관련 법령 및 규정

## 개인정보 보호 관련 법령

- 개인정보 보호법 , 정보통신망 이용촉진 및 정보보호 등에 관한 법률
- 신용정보의 이용 및 보호에 관한 법률, 위치정보의 보호 및 이용 등에 관한 법률
- 표준 개인정보 보호 지침, 개인정보의 안전성 확보 조치 기준

## IT 기술 관련 규정

- RFID 프라이버시 보호 가이드라인, 위치정보의 보호 및 이용 등에 관한 법률
- 위치정보의 관리적, 기술적 보호조치 권고 해설서
- 바이오정보 보호 가이드라인, 뉴미디어 서비스 개인정보 보호 가이드라인

# HW 관련 신기술

## 고가용성(HA; High Availability)

- 장애 발생 시 즉시 다른 시스템으로 대체 가능한 환경을 구축하는 메커니즘

## 3D Printing(Three Dimension Printing)

- 손으로 만질 수 있는 실제 물체로 만들어내는 것

## 4D Printing(Fourth Dimension Printing)

- 특정 시간이아 환경 조건이 갖추어지면 스스로 형태를 변화시키거나 제조되는 자가 조립(Self-Assembly) 기술이 적용된 제품을 3D Prinring하는 기술

## RAID(Redundant Array of Inexpensive Disk)

- 데이커 블록들을 서로 다른 디스크들에 분산 저장할 경우 그 블록들을 여러 디스크에서 동시에 읽거나 쓸 수 있으므로 디스크의 속도가 매우 향상

문혜영 교수

# 제5과목 정보시스템 구축 관리

## 06 IT 프로젝트 정보시스템 구축 관리 D

# HW 관련 신기술

## 4K 해상도

- 차세대 고화질 모니터의 해상도

## 앤 스크린(N-Screen)

- N개의 서로 다른 단말기에서 동일한 콘텐츠를 자유롭게 이용
- PC, TV, 휴대폰에서 동일한 콘텐츠를 끊김없이 이용할 수 있고, 여러 개의 단말기에서도 동일한 콘텐츠를 끊김없이 이용

## 컴패니언 스크린(Companion Screen)

- TV 방송 시청 시 방송 내용을 공유하여 추가적인 기능을 수행할 수 있는 스마트폰, 태블릿PC 등

# HW 관련 신기술

## 신 클라이언트 PC(Thin Client PC)

- 하드디스크나 주변 장치 없이 기본적인 메모리만 갖추고 서버와 네트워크로 운용되는 개인용 컴퓨터

## 패블릿(Phablet)

- 테블릿 기능을 포함한 5인치 이상의 대화면 스마트폰

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

- 기존 A형에 비하여 크기가 작고, 24핀으로 위아래 구분없이 어느 방향으로든 연결 가능

## 멤스(MEMS; Micro-Electro Machanical Systems)

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

# HW 관련 신기술

## ➢ 트러스트존 기술(TrustZone Technology)

- 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 기술

## ➢ 엠디스크(M-DISC, Millennial DISC)

- 한 번의 기록만으로 자료를 영구 보관할 수 있는 광 저장 장치

## ➢ 멤리스터(Memristor)

- 전류의 방향과 양 등 기존의 경험을 모두 기억하는 특별한 소자..

# 문제

➢ 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

정답 4

# Secure OS

## Secure OS의 개요

- 기존의 운영체제(OS)에 내제된 보안 취약점을 해소하기 위해 보안 기능을 갖춘 커널을 이식하여 외부의 침입으로부터 시스템 자원을 보호하는 운영체제
- 참조 모니터와 보안 커널의 3가지 특징
  - 격리성(Isolation) : 부정 조작이 불가능해야 함.
  - 검증가능성(Verifiability) : 적절히 구현되었다는 것을 확인할 수 있어야 함
  - 완전성(Completeness) : 우회가 불가능해야 함.

## Secure OS 보안 기능

- 식별 및 인증, 임의적/강제적 접근통제, 객체 재사용 보호, 완전한 조정, 신뢰 경로, 감사 및 감사기록 축소 등

# DB 관련 신기술

## 빅데이터(Big Data)

- 기존의 관리 방법이나 분석 체게로는 처리하기 어려운 막대한 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 데이터나 기존 데이터에 새로운 가치가 더해진 데이터

## 메타 데이터(Meta Data)

- 일련의 데이터를 정의하고 설명해 주는 데이터

# DB 관련 신기술

## 디지털 아카이빙(Digital Archiving)

- 디지털 정보 자원을 장기적으로 보존하기 위한 작업

## 하둡(Hadoop)

- 오픈 소스를 기반으로 한 분산 컴퓨팅 플랫폼

## 타조(Tajo)

- 오픈 소스 기반 분산 컴퓨팅 플롯폼인 아파치 하둡(Apache Hadoop) 기반의 분산 데이터 웨어하우스 프로젝트

## 데이터 다이어트(Data Diet)

- 데이터를 압축하고, 중복을 배제하고, 새로운 기준에 따라 나누어 저장하는 작업

# 회복 / 병행제어

## 회복(Recovery)

- 트랜잭션을 수행하는 도중 장애가 발생하여 데이터베이스가 손상되었을 때 손상되기 이전의 정상 상태로 복구하는 작업
- 장애의 유형
  - 트랜잭션 장애
  - 시스템 장애
  - 미디어 장애
- 회복 관리기(Recovery Management)
  - 트랜잭션 실행이 성공적으로 완료되지 못하면 트랜잭션이 데이터베이스에 생성했던 모든 변화를 취소(Undo)시키고, 트랜잭션 수행 이전의 원래 상태로 복구하는 역할

# 회복 / 병행제어

## 병행제어(Concurrency Control)

- 동시에 실행되는 트랜잭션들이 데이터베이스의 일관성을 파괴하지 않도록 트랜잭션 간의 상호 작용을 제어하는 것
- 병행제어의 목적
  - 데이터베이스의 공유를 최대화
  - 시스템 활용도를 최대화
  - 데이터베이스의 일관성 유지
  - 사용자에 대한 응답 시간을 최소화

## 병행수행의 문제점

- 갱신 분실, 비완료 의존성, 모순성, 연쇄 복귀 등의 문제점 발생

# 데이터 표준화

## 데이터 표준화의 정의

- 시스템을 구성하는 데이터 요소의 명칭, 정의, 형식, 규칙에 대한 원칙을 수립하고 적용하는 것

## 데이터 표준

- 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 단어
  - 표준 도메인 : 문자형, 숫자형, 날짜형, 시간형과 같이 컬럼을 성질에 따라 그룹핑한 개념
  - 표준 코드 : 선택할 수 있는 값을 정형화하기 위해 기준에 맞게 이미 정의된 코드 값
  - 표준 용어

# 데이터 표준화

## 데이터 관리 조직

- 데이터 표준 원칙이나 데이터 표준의 준수 여부 등을 관리하는 사람들(데이터 관리자)
- 데이터 관리자와 데이터베이스 관리자 비교

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

## 데이터 표준화 절차

- 데이터 표준화 요구사항 수집, 데이터 표준 정의, 데이터 표준 확정, 데이터 표준 관리 순

# 데이터 표준화

## ➢ 데이터 표준화 대상

- 데이터 명칭, 데이터 정의, 데이터 형식, 데이터 규칙

## ➢ 데이터 표준화 기대 효과

- 동일한 데이터에 대해 동일한 명칭을 지정하면 명확한 의사소통이 가능
- 데이터 표준에 다라 데이터 형식 및 규칙을 적용하면 데이터 품질을 향상시킬 수 있다.
- 데이터를 전사적으로 관리하면 시스템 간 데이터 공유 시 데이터 변환이나 정제 작업을 수행하지 않아도 된다.

# 문제

➢ 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

정답 4

문혜영 교수

# 제5과목 정보시스템 구축 관리

## 07 소프트웨어 개발 보안 구축 A

# Secure SDLC

## Secure SDLC의 개요

- 보안상 안전한 소프트웨어를 개발하기 위해 SDLC에 보안 강화를 위한 프로세스를 포함한 것

## 요구사항 분석 단계에서의 보안 활동

- 보안항목에 해당하는 요구사항을 식별하는 작업을 수행

## 보안 요소

- 기밀성, 무결성, 가용성, 인증, 부인 방지

# Secure SDLC

## 설계 단계에서의 보안 활동

- 식별된 보안 요구사항들을 소프트웨어 설계서에 반영하고, 보안 설계서를 작성

## 구현 단계에서의 보안 활동

- 표준 코딩 정의서 및 소프트웨어 개발 보안 가이드를 준수하며, 설계서에 따라 보안 요구사항들을 구현

## 테스트 단계에서의 보안 활동

- 설계 단계에서 작성한 보안 설계서를 바탕으로 보안 사항들이 정확히 반영되고 동작되는지 점검

## 유지보수 단계에서의 보안 활동

- 보안 사고들을 식별하고, 사고 발생 시 이를 해결하고 보안 패치를 설치

# 문제

- 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

정답 1

# 세션 통제

## 세션 통제의 개요

- 세션 : 서버와 클라이언트의 연결
- 세션 통제 : 세션의 연결과 연결로 인해 발생하는 정보를 관리하는 것
  - 세션 통제는 요구사항 분석 및 설계 단계에서 진단해야 하는 보안 점검 내용
  - 보안 약점 : 불충분한 세션 관리, 잘못된 세션에 의한 정보 노출

## 불충분한 세션 관리

- 일정한 규칙이 존재하는 세션ID가 발급되거나 타임아웃이 너무 길게 설정되어 있는 경우 발생할 수 있는 보안 약점

## 잘못된 세션에 의한 정보 노출

- 다중 스레드(Multi-Thread) 환경에서 멤버 변수에 정보를 저장할 때 발생하는 보안 약점

# 세션 통제

## 세션 설계 고려사항

- 시스템의 모든 페이지에서 로그아웃이 가능하도록 UI(User Interface)를 구성
- 로그아웃 요청 시 할당된 세션이 완전히 제거되도록 한다.

## 세션ID의 관리

- 안전한 서버에서 최소 128비트의 길이로 새성
- 세션ID의 예측이 불가능하도록 안전한 난수 알고리즘을 제공

# 입력 데이터 검증 및 표현

## 입력 데이터 검증 및 표현의 개요

- 입력 데이터로 인해 발생하는 문제들을 예방하기 위해 구현 단계에서 검증해야 하는 보안 점검 항목들

## 입력 데이터 검증 및 표현의 보안 약점

- 점검을 수행하지 않은 경우 SQL 삽입, 자원 삽입, 크로스사이트 스크립팅(XSS), 운영체제 명령어 삽입 등의 공격에 취약해진다.
- 보안 약점의 종류 : SQL  삽입, 경로 조작 및 자원 삽입, 크로스사이트 스크립팅(XSS), 운영체제 명령어 삽입, 위험한 형식 파일 업로드, 신뢰되지 않는 URL 주소로 자동접속 연결

문혜영 교수

# 제5과목 정보시스템 구축 관리

## 08 소프트웨어 개발 보안 구축 B

# 보안 기능

## 보안 기능의 개요

- 소프트웨어 개발의 구현 단계에서 코딩하는 기능인 인증, 접근제어, 기밀성, 암호화 등을 올바르게 구현하기 위한 보안 점검 항목들

## 보안 기능의 보안 약점

- 적절한 인증 없이 중요기능 허용
- 부적절한 인가

# 문제

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

① 종료되지 않는 반복문 또는 재귀함수

② 부적절한 인가

③ 중요한 자원에 대한 잘못된 권한 설정

④ 적절한 인증없이 중요기능 허용

정답 1

# 시간 및 상태

## 시간 및 상태의 개요

- 병렬처리 시스템이나 다수의 프로세스가 동작하는 환경에서 시스템이 원활하게 동작되도록 하기 위한 보안 검증 항목

## TOCTOU 경쟁 조건

- 검사 시점(Time Of Check)과 사용 시점(Time Of Use)을 고려하지 않고 코딩하는 경우 발생하는 보안 약점

# 에러처리

## 에러처리의 개요

- 소프트웨어 실행 중 발생할 수 있는 오류(Error)들을 사전에 정의하여 오류로 인해 발생할 수 있는 문제들을 예방하기 위한 보안 점검 항목들이다.

## 오류 메시지를 통한 정보 노출

- 오류 발생으로 실행 환경, 사용자 정보, 디버깅 정보 등의 중요 정보를 소프트웨어가 메시지로 외부에 노출하는 보안 약점

## 오류 상황 대응 부재

- 소프트웨어 개발 중 예외처리를 하지 않았거나 미비로 인해 발생하는 보안 약점

## 부적절한 예외처리

- 함수의 반환값 또는 오류들을 세분화하여 처리하지 않고 광범위하게 묶어 한 번에 처리하거나 누락된 에외가 존재할 때 발생하는 보안 약점

# 코드 오류

## 코드 오류의 개요

- 개발자들이 코딩 중 실수하기 쉬운 형(Type) 변환, 자원 반환 등의 오류를 예방하기 위한 보안 점검 항목들

## 널 포인터(Null Pointer) 역참조

- 널 포인터가 가리키는 메모리에 어떠한 값을 저장할 때 발생하는 보안 약점

## 부적절한 자원 해제

- 자원을 반환하는 코드를 누락하거나 프로그램 오류로 할당된 자원을 반환하지 못했을 때 발생하는 보안 약점

## 해제된 자원 사용

- 이미 사용이 종료되어 반환된 메모리를 참조하는 경우 발생하는 보안 약점

# 문제

➢ 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.

정답 2

문혜영 교수

# 제5과목 정보시스템 구축 관리

## 09 소프트웨어 개발 보안 구축 C

# 캡슐화

## 캡슐화의 개요

- 정보 은닉이 필요한 중요한 데이터와 기능을 불충분하게 캡슐화하거나 잘못 사용함으로써 발생할 수 있는 문제를 예방하기 위한 보안 점검 항목들
- 캡슐화로 인해 발생할 수 있는 보안 약점
  1. 잘못된 세션에 의한 정보 노출 : 다중 스레드(Multi-Thread) 환경에서 멤버 변수에 정보를 저장할 때 발생
  2. 제거되지 않고  남은 디버그 코드 : 개발 중에 버그 수정이나 결과값 확인을 위해 남겨둔 코드들로 인해 발생
  3. 시스템 데이터 정보 노출
  4. Public 메소드로부터 반환된 Private 배열
  5. Public 배열에 Private 데이터 할당

# API 오용

## API 오용의 개요

- API를 잘못 사용하거나 보안에 취약한 API를 사용하지 않도록 하기 위한 보안 검증 항목

### DNS Lookup

- 보안 결정을 내리는 경우 발생하는 보안 약점

### 취약한 API 사용

- 보안 문제로 사용이 금지된 API를 사용하거나 잘못된 방식으로 API를 사용했을 때 발생

# 암호 알고리즘

## 암호 알고리즘의 개요

- 중요 정보를 보호하기 위해 평문을 암호화된 문장으로 만드는 절차 또는 방법
  - 단방향 암호화 방식 : 해시(Hash)
  - 양방향 암호화 방식 : 개인키(Stream 방식, Block 방식), 공개키

## 개인키 암호화(Private Key Encryption) 기법

- 동일한 키로 데이터를 암호화하고 복호화한다.
  - 블록(Block) 암호화 방식 : 한 번에 하나의 데이터 블록을 암호화(DES, SEED, AES, ARIA)
  - 스트림(Stream) 암호화 방식 : 평문과 동일한 길이의 스트림을 생성하여 비트 단위로 암호화 (LFSR, RC4)
- 장점 : 암호화/복호화 속도가 빠름, 알고리즘이 단순, 파일의 크기가 작다.

# 암호 알고리즘

## 공개키 암호화(Public Key Encryption) 기법

- 암호화 할 때 사용하는 공개키(Public Key)는 데이터베이스 사용자에게 공개하고, 복호화할 때의 비밀키(Secrey Key)는 관리자가 비밀리에 관리
  - 비대칭 암호 기법이라고도 하며, 대표적으로 RSA(Rivest Shamir Adleman)기법이 있다.
- 장점 : 키의 분배가 용이, 관리해야 할 키의 개수가 적다.

## 양방향 알고리즘의 종류

- SEED, ARIA, DES, AES, RSA

## 해시(Hash)

- 임의의 길이의 입력 데이터나 메시지를 고정된 길이의 값이나 키로 변환
- 데이터의 암호화, 무결성 검증을 위해 사용

# 문제

➢ 데이터를 암호화하는데 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.

정답 4

문혜영 교수

# 제5과목 정보시스템 구축 관리

## 10 시스템 보안 구축 A

# 서비스 공격 유형

## ➢ 서비스 거부(Dos; Denial of Service) 공격의 개념

- 서버의 정상적인 기능을 방해하기 위한 공격기법.

- SYN Flooding
- Ping of Death(죽음의 핑)
- TearDrop
- Land attack
- SMURFING(스머핑)

# 서비스 공격 유형

## DDoS(Distributed Denial of Service, 분산 서비스 거부) 공격

- 여러 곳에 분산된 공격 지점에서 한 곳의 서버에 대해 분산 서비스 공격을 수행하는 것

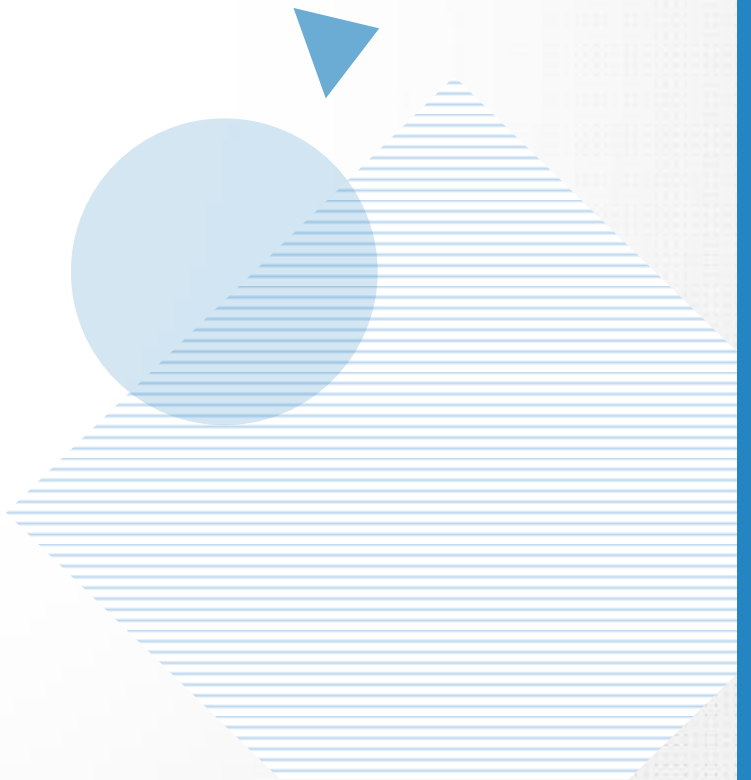
## 네트워크 침해 공격 관련 용어

- 스미싱(Smishing)
- 스피어 피싱(Spear Phishing)
- APT(Advanced Persistent Threats, 지능형 지속 위협)
- 무작위 대입 공격(Brute Force Attack)
- 큐싱(Qshing)
- SQL 삽입(Injection)
- 크로스 사이트 스크립팅(XSS; Cross Site Scripting)

# 서비스 공격 유형

## 정보 보안 침해 공격 관련 용어

- 좀비(Zombie) PC
- C&C 서버
- 봇넷(Botnet)
- 웜(Worm)
- 제로 데이 공격(Zero Day Attack)
- 키로거 공격(Key Logger Attack)
- 랜섬웨어(Ransomware)
- 백도어(Back Door, Trap Door)
- 트로이 목마(Trojan Horse)



# 서버 인증

## 보안 서버의 개념

- 인터넷을 통해 개인 정보를 암호화하여 송·수신할 수 있는 기능을 갖춘 서버

## 인증(Authentication)의 개념

- 접근 권한을 검증하는 보안 절차

## 지식 기반 인증(Something You Know)

- 사용자가 기억하고 있는 정보를 기반으로 인증을 수행하는 것

## 소유 기반 인증(Something You Have)

- 사용자가 소유하고 있는 것을 기반으로 인증을 수행하는 것

## 생체 기반 인증(Something You Are)

- 사용자의 고유한 생체 정보를 기반으로 인증을 수행하는 것

# 문제

## ➢ 다음 중 보안 서버에 대한 설명으로 잘못된 것은?

① 보안 서버란 인터넷을 통해 개인과 개인이 직접 연결되어 파일을 공유할 수 있도록 해 주는 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.

정답 1

문혜영 교수

# 제5과목 정보시스템 구축 관리

## 11 시스템 보안 구축 B

# 보안 아키텍처 / 보안 프레임워크

## ➢ 보안 아키텍처(Security Architecture)

- 정보 시스템의 무결성(Integrity), 가용성(Availability), 기밀성(Confidentiality)을 확보하기 위해 보안 요소 및 보안 체계를 식별하고 이들 간의 관계를 정의한 구조

## ➢ 보안 프레임워크(Securuty Framework)

- 안전한 정보 시스템 환경을 유지하고 보안 수준을 향상시키기 위한 체계
  - ISO 27001은 정보보안 관리를 위한 국제 표준으로 일종의 보안 인증

# 로그 분석

## 로그(Log)의 개념

- 시스템 사용에 대한 모든 내역을 기록해 놓은 것

## 리눅스(LINUX)로그

- 시스템의 모든 로그를 var/log 디렉토리에서 기록하고 관리
  - 로그 파일을 관리하는 syslogd 데몬은 로그 관련 파일들의 위치를 파악한 후 로그 작업을 시작
  - Syslog.conf 파일을 수정하여 로그 관련 파일들의 저장 위치와 파일명을 변경

## 리눅스의 주요 로그 파일

- 커널 로그, 부팅 로그, 크론 로그, 시스템 로그, 보안 로그, FTP 로그, 메일 로그

## Windows 이벤트 뷰어의 로그

- 응용 프로그램 로그, 보안 로그, 시스템 로그, Setup 로그, Forwarded Events

# 보안 솔루션

## 보안 솔루션의 개념

- 접근 통제, 침입 차단 및 탐지 등을 수행하여 외부로부터의 불법적인 침입을 막는 기술 및 시스템

## 방화벽(Firewall)

- 기업이나 조직 내부의 네트워크와 인터넷 간에 전송되는 정보를 선별하여 수용·거부·수정하는 기능을 가진 침입 차단 시스템이다.

## 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 것

# 보안 솔루션

## ➢ 데이터 유출 방지(DLP; Data Leakage/Loss Prevention)

- 내부 정보의 외부 유출을 방지하는 보안 솔루션

## ➢ 웹 방화벽(Web Firewall)

- 일반 방화벽이 탐지하지 못하는 SQL 삽입 공격, Cross-Site Sacripting(XSS) 등의 웹 기반 공격을 방어할 목적으로 만들어진 웹 서버에 특화된 방화벽

# 보안 솔루션

## VPN(Virtual Private Network, 가상 사설 통신망)

- 통신 사업자의 공중 네트워크와 암호화 기술을 이용하여 사용자가 마치 자신의 전용 회선을 사용하는 것처럼 해주는 보안 솔루션

## NAC(Network Access Control)

- 네트워크에 접속하는 내부 PC의 MAC 주소를 IP 관리 시스템에 등록한 후 일관된 보안 관리 기능을 제공하는 보안 솔루션

## ESM(Enterprise Security Management)

- 다양한 장비에서 발생하는 로그 및 보안 이벤트를 통합하여 관리하는 보안 솔루션

# 취약점 분석·평가

## 취약점 분석·평가의 개요

- 사이버 위협으로부터 정보 시스템의 취약점을 분석 및 평가한 후 개선하는 일련의 과정

## 취약점 분석·평가 범위

- 정보 시스템과 정보 시스템 자산에 직·간접적으로 관여된 물리적, 관리적, 기술적 분야를 포함한다.

## 수행 절차 및 방법

- 취약점 분석·평가 계획 수립
- 취약점 분석·평가 대상 선별
- 취약점 분석 수행
- 취약점 평가 수행

# 문제

➢ 다음 중 리눅스(Linux)의 주요 로그 파일이 아닌 것은?

① Console

② Cron

③ Secure

④ Syslogd

정답 4