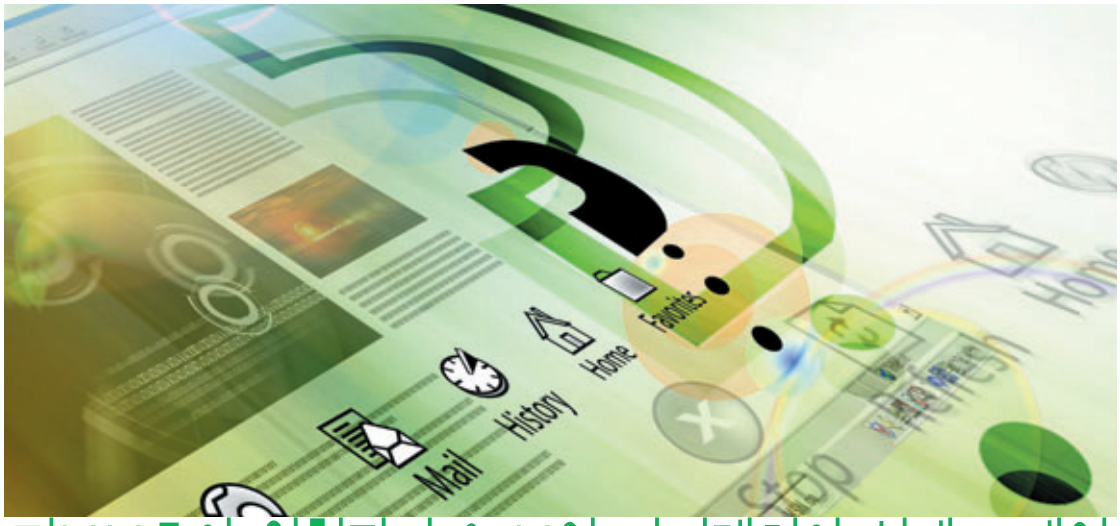
허종오 · 한국 CISSP협회 연구분과 이사, 전자계산기기술사

KBS + 허종오 · 한국 CISSP협회 연구분과 이사, 전자계산기기술사

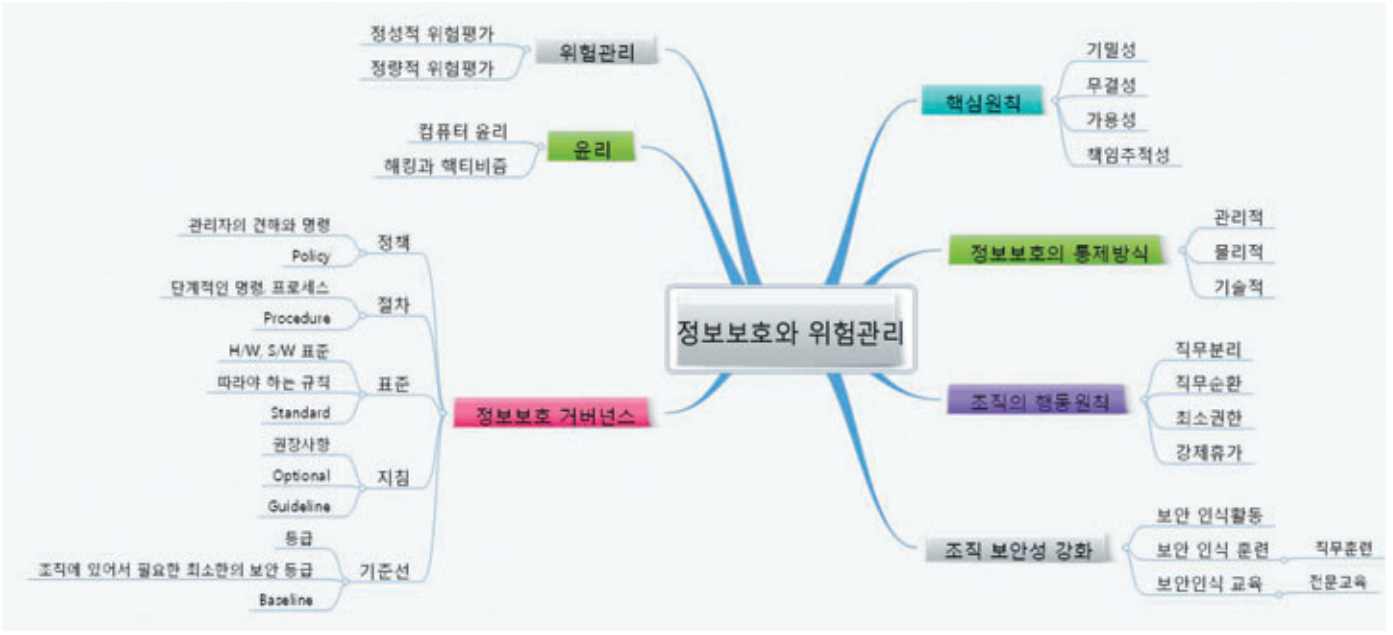


정보보호와 위험관리 & 보안 아키텍처와 설계 도메인

지난 호에서는 글로벌 공인 보안 자격증인 CISSP에 대한 소개와 취득방법에 대해서 알아보았다.
이번 호부터는 CISSP의 CBK(Common Body of Knowledge) 10개 도메인 중에서 매월 2개 도메인을 선정하여, 해당 도메인에서 학습해야 할 주요 요점과 함께 연습문제를 제공하고자 한다. 이를 통해, CISSP가 되기 위해서는 어떤 부분을 알아야 하며, 어떤 문제가 출제되는지를 독자들이 자연스럽게 알 수 있도록 하고자 한다. 첫 번째로 정보보호와 위험관리, 보안 아키텍처와 설계 도메인에 대해 알아보자.

1. 정보보호와 위험관리(Information Security and Risk Management) 요점 정리

이번 호에 소개하는 정보보호와 위험관리, 보안 아키텍처와 설계는 CISSP의 10개 도메인 중에서 정책부분을 언급하는 도메인이다. 특히, 정보보호와 위험관리는 CISSP가 조직에서 정보보호 활동을 수행 시에 가치판단 기준이 되는 정보보호 정책에 대한 가이드를 제공하고 있다. 최근의 CISSP 시험에서는 정책적인 지식을 기반으로 하여 실제 환경에서의 CISSP로서의 판단을 물어보는 문제가 많이 출제되므로, 꾸준한 반복학습이 필요한 분야이다. 한 가지 Tip을 제시하면, 회사의 정보보호 정책이 CBK에서 제공하는 정책과 다를 수도 있다. 따라서, 회사에서 일하는 방식을 항상 정답으로 선택하면 안 되며, CISSP CBK에서 제시한 내용이 판단기준이 되어야 한다. 간혹, 한국의 실정에 맞는 문제를 답으로 골라, 문제를 틀리는 수험생들이 있다. 하지만, 엄연히 이 시험은 미국에 있는 기관이 출제하는 미국 시험이라는 것에 주의해야 한다.
정보보호와 위험관리 도메인에서 학습해야 할 내용들은 다음 Domain Map을 통해 한 눈에 알 수 있다. 기본적으로 정보보호전문가가 되기 위해서는 Domain Map의 큰 가지들을 숙지하고, 큰 가지에서 작은 가지를 뽑아내는 일명 "가지치기" 능력을 가져야 한다. 지면상 Domain Map의 전체 내용을 설명하기보다는 꼭 알아야 할 주요 요점 위주로 설명하겠다.



[그림 1] 정보보호와 위험관리 Domain Map

[그림 2] 정보보호의 핵심원칙

1-1. 핵심 원칙

정보보호의 핵심원칙은 기밀성, 무결성, 가용성을 말하며, 다른 말로 정보보호의 목표이라고 표현한다. 정보보호의 대상들은 모두 기밀성, 무결성, 가용성이 충족할 때 비로소 정보보호를 이루었다고 볼 수 있다.

(1) 기밀성(Confidentiality)

오직 인가된 사람, 프로세스, 시스템만이 알 필요성(need-to-know)[1]에 근거하여 시스템에 접근해야 하는 원칙을 말한다.

(2) 무결성(Integrity)

정보는 고의적인 또는 비인가 된 우연한 변경으로부터 보호되어야 한다는 원칙을 말한다.

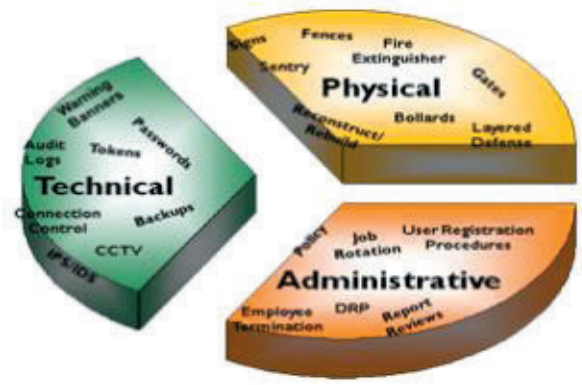
(3) 가용성(Availability)

정보는 사용자가 필요로 하는 시점에 접근 가능해야 한다는 원칙을 말한다.

1) 정보에 접근하는 사람은 자신이 알 필요가 있는 정보만을 습득해야 한다는 원칙

1-2. 정보보호의 통제 방식

정보보호의 핵심원칙 또는 목표를 이루기 위해서는 적절한 활동이 있어야 한다. 이것을 정보보호를 위한 통제 방식이라고 한다. 통제 방식은 관리적인 방식, 기술적인 방식, 물리적인 방식으로 구분된다.



[그림 3] 정보보호의 통제 방식

(1) 관리적 통제(Administrative Controls)

정보자원을 적절히 보호하기 위한 서류화된 관리, 혹은 인적 관리를 말한다. 조직의 정보보호 정책과 절차, 우발적 사고에 대한 대책, 조직의 윤리 지침서 등이 있다.

(2) 기술적 통제(Technical Controls)

논리적(Logical) 통제라고도 불리며, 정보자원을 권한 외의 접근을 제한하기 위해 사용하는 하드웨어, 소프트웨어 통제 방식을 말한다. 접근 관리 소프트웨어, 바이러스, 스팸, 스파이웨어 차단 소프트웨어 등이 있다.

(3) 물리적 통제(Physical Controls)

장비와 컴퓨터 연산 리소스에 대한 권한 외의 접근 혹은 자연재해 등으로부터 보호하기 위한 인공적, 구조적, 환경적 관리를 말한다. 잠금장치, 문 울타리, 경비원, CCTV 등이 있다.

1-3. 조직의 행동 원칙

조직에서 정보보호 통제 방식을 실행할 때 사용하는 행동 원칙을 말하며, 직무분리, 직무순환, 최소권한, 강제휴가 등이 있다.

(1) 직무분리(Segregation of Duties)

한 사람이 특정 프로세스의 모든 단계를 수행할 권한을 가져서는 안 된다는 원칙이다. 예를 들면, 최근에 발생하였던 장애우 복지 관련 공무원의 행정비리 사건에서 해당 공무원이 장애우 명단 관리, 사회 보조금 관리 등의 모든 관리 권한을 가지게 되어 비리를 저지르게 되는 경우를 예방하기 위해 업무 자체를 분리해야 한다는 원칙이다.

(2) 직무순환(Job Rotation)

한 직원이 오랫동안 같은 직무를 수행함으로써 발생할 수 있는 부정의 가능성을 예방하고, 전임 직원의 부정이나 실수를 후임 직원이 발견하기 위한 행동 원칙이다. 정부 중앙부처에서는 해당 직원의 부정을 막기 위해 3~5년에 한 번씩 근무지를 이동하는 예가 있다. 특히, 직무순환은 직무분리를 통해 권한이 분리되어 발생할 수 있는 공모를 예방하기 위한 예방 통제 방식이기도 하다.

(3) 최소권한(Least Privilege)

정보 접근자 또는 사용자는 해당 직무에 필요한 권한만을 받아야 한다는 원칙이다. 다른 말로는 'Need to Know' 라고 불리기도 한다.

(4) 강제휴가(Mandatory Vacations)

직원의 부정을 막기 위해 주기적으로 휴가를 강제적으로 보낸 후, 자유롭게 해당 직원의 부정을 조사하는 방식이다. 강제휴가는 직원을 직무순환 시키지 않더라도 해당 직원의 부정을 예방, 발견할 수 있는 효과를 발휘할 수 있다.

1-4. 조직의 보안성 강화를 위한 보안 인식 활동

조직 내의 보안에 대한 인식을 높이기 위한 활동으로 공식적인 교육과 포스터를 이용한 교육으로 구분된다. 공식적인 교육은 한 장소에 교육대상자들을 모아 교육을 하는 집체 교육과 온라인을 통해 교육을 하는 온라인 교육으로 구분된다. 그 외에 보안 전문가를 양성하기 위한 전문 교육들이 존재한다. 이러한 교육을 실시하는 이유는 직원에게 보안 교육을 투자 하지 않아 보안 사고가 발생한다면 경영진이 책임을 피할 수 없다는 강제조항에 근거하여 교육이 실시되고 있다.

1-5. 정보보호 거버넌스

지금까지 정보보호의 핵심 원칙, 통제 방식, 행동 원칙 등을 살펴보았다. 이러한 원칙과 행동들은 필히 조직에서 수행되어야 하는 활동들이다. 하지만, 이러한 원칙이 잘 실행되기 위해서는 조직의 상부의 정책이 하부까지 잘 전달되어야 하며, 이러한 통제 방식들이 제대로 수행되고 있는지 관리되어야 한다. 이를 위해서는 조직의 목표와 일치하는 정보보호 정책, 절차, 표준 등을 명시하고 실제적으로 잘 수행되도록 통제하는 정보보호 거버넌스가 조직 내에 자리 잡혀야 한다.

그럼, 정보보호 거버넌스는 무엇인지 좀 더 살펴보자. 정보보호 거버넌스는 한마디로 조직의 목표를 이룰 수 있도록 정보보호 체계를 수립하고, 이 체계가 잘 수행되도록 관리하는 활동을 말한다. 여기에는 정보보호 정책, 절차, 표준, 지침, 기준선 등이 명시되어 있어야 한다. 그 외에 통제를 위한 조직, 관리 시스템, 평가기준들이 있어야 하나, CISSP 시험에서는 이 부분이 중요한 부분으로 다루어지지 않고 있다. 따라서, 이 장에서는 정보보호 정책, 절차, 표준, 지침, 기준선 등에 대해 알아보자.

(1) 정책

조직의 목표를 이루기 위한 필요한 보안 목표를 명시하며, 임직원에게 가치판단 기준을 제공하고, 모든 직원들이 공유할 수 있는 내용이어야 한다.

(2) 절차

정책을 구현하기 위한 단계별 세부 지시사항이다.

(3) 표준

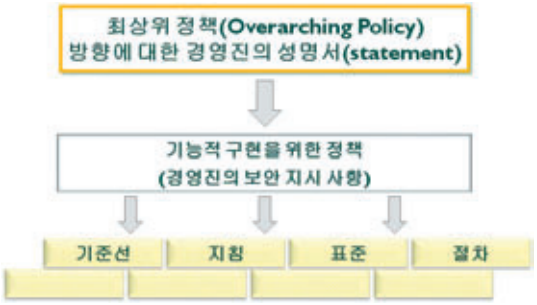
조직에 적용되는 하드웨어, 소프트웨어의 구체적 사양이다.

(4) 기준선

정보보호 정책의 일관성 있는 적용을 위해 기본적으로 준수해야 할 사항이다.

(5) 지침

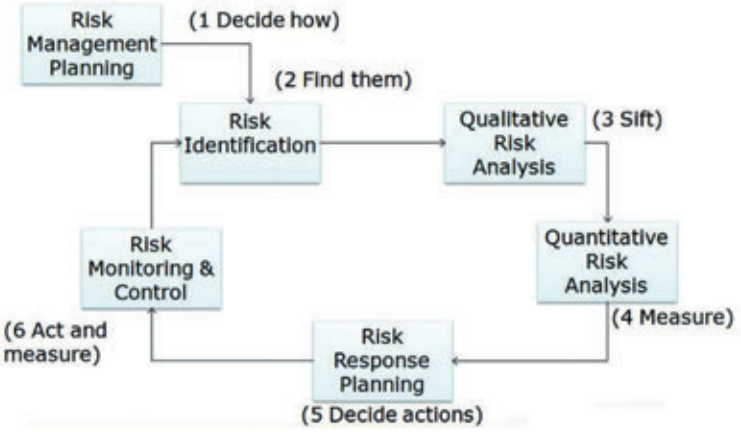
그 외에 추가적으로 권고할 사항으로 적용여부는 조직의 선택이다.



[그림 4] 정보보호 거버넌스

1-6. 정보보호 위험관리

정보보호를 함에 있어 발생할 수 있는 잠재적인 위험을 평가하고 그에 대한 대응책을 세워야 한다. 따라서, 이러한 위험을 발굴, 평가, 통제하는 정보보호 위험관리에 대해서 알아보자.



[그림 5] 위험관리 절차

구성 요소	설명
위험관리 계획 수립	– 조직에 발생할 위험에 대한 관리 목적 및 관리 방안에 대한 계획을 수립한다.
위험 식별	– 조직에 발생할 수 있는 노출된 또는 잠재적인 위험을 식별한다.
정성적 위험 분석	– 식별된 위험의 발생가능성, 영향도 등을 정성적 판단기준에 의해 위험 수준을 결정한다.
정량적 위험 분석	– 정성적 위험 분석에 의해 산출 된 위험수준을 참고하여, 위험으로 인한 피해액을 산출한다.
위험 대응	– 위험 피해액에 비해 위험 대응 소요비용을 비교하여, 위험에 대한 대응 여부와 대응 방안을 결정한다.
위험 모니터링과 통제	– 대응한 위험에 대한 효과를 확인하고, 추가적인 위험에 대한 식별을 전 단계에 걸쳐서 모니터링 한다.

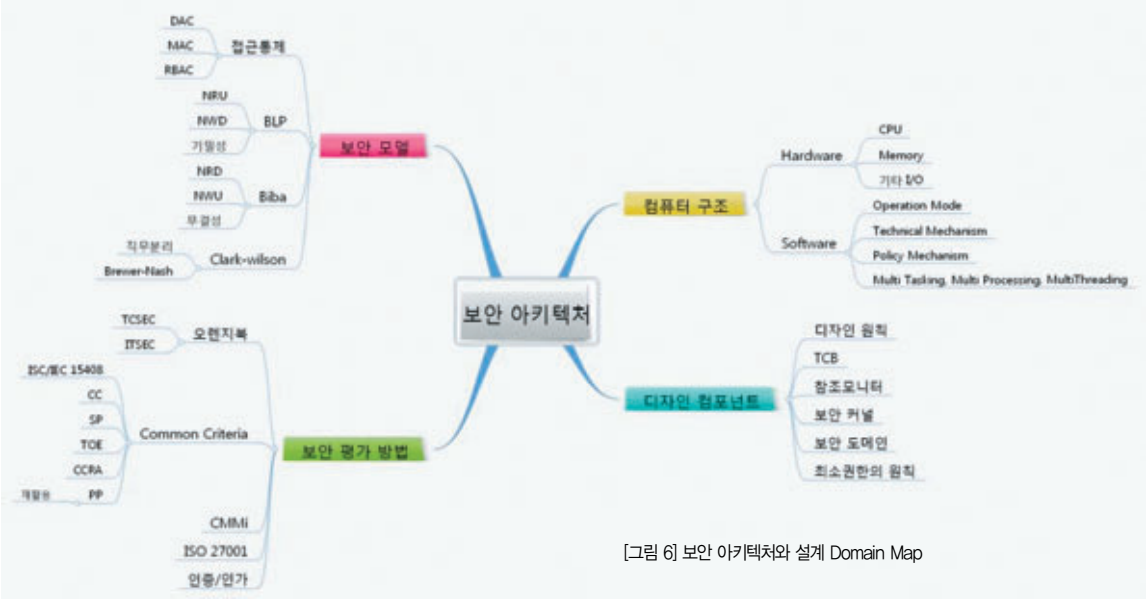
지금까지 정보보호와 위험관리에 대해서 살펴보았다. 두 가지 부분은 기업의 정보보호 정책에 대한 내용으로서 CISSP 합격을 위해서는 꼭 필요한 가치 기준이므로, 충분한 학습이 필요하다.

정리해보면, 정보보호와 위험관리 부분에 주로 출제되는 다음의 Key Factor와 같다. 그리고, 정보보호와 위험관리는 시나리오형 문제에서 판단근거가 되는 중요한 부분이다. 또한, 최근 시나리오형 문제 출제로 인해, 출제비중은 "높음"이니, 확실한 학습이 필요하다.

도메인	Key Factor	출제 비중
정보보호와 위험 관리	– 보안 정책, 절차, 표준, 그리고 지침에 대한 이해 – 위험 평가와 관리방법에 대한 이해 및 위험평가 계산 – 인적 보안, 훈련, 그리고 보안 인식 프로그램 학습	높음

2. 보안 아키텍처와 설계(Security Architecture and Design) 요점 정리

보안 아키텍처와 설계는 정보보호 정책을 조직에 어떻게 체계적으로 적용하는가에 대한 방법을 아키텍처 모델을 통해 안내한다. 또한, IT를 이루고 있는 기본적인 시스템 아키텍처도 함께 언급하고 있다.

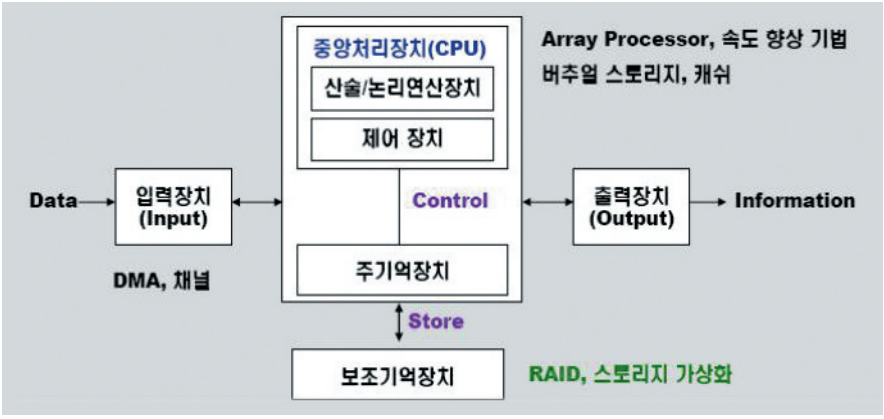


[그림 6] 보안 아키텍처와 설계 Domain Map

2-1. 컴퓨터 구조(Computer Architecture)

컴퓨터 시스템 아키텍처를 구성하는 Hardware와 Software를 설명한다. 먼저, 컴퓨터 아키텍처는 다음과 같다. 컴퓨터가 기능을 수행하기 위한 모든 H/W(CPU, Memory 등)와 S/W(Operating System) 요소를 총괄해서 컴퓨팅 시스템의 구성을 논리적 수준에서 다루는 엔지니어링 분야이다.

(1) 하드웨어



[그림 7] 하드웨어 구성

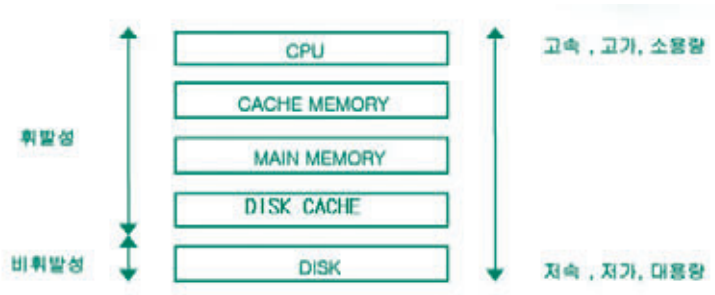
가) 중앙처리장치(CPU)

프로그램에 의해 기술된 명령어를 메모리에서 인출하여 해석하고 실행하는 장치로서 입력된 데이터를 사용하여 컴퓨터 내부에서 논리연산, 산술연산, 편집, 이동 등의 작업을 하여 목적한 값 출력한다.

구성 요소	설명
BUS	– 내부 버스(Internal Bus) : CPU 내부의 버스 – 외부 버스(External Bus) : CPU, Main Memory, 입출력 장치와 연결된 버스
ALU	– Arithmetic Logic Unit, 사칙연산, 논리연산, shift 연산 등을 수행함
레지스터	– 연산장치나 제어장치에서 실행 도중의 중간 데이터 값을 일시적으로 저장하는 장소 – 특수목적 레지스터, 메모리와 통신을 위한 레지스터, 범용 레지스터
제어장치	– 메모리로부터 명령어를 받아 해석함으로써 레지스터리에 마이크로 명령을 실행하는 일련의 제어함수를 발생시킴

나) 주기억장치(Memory)

실행 프로그램과 데이터의 임시적 또는 영구적 저장 기능을 수행하는 장치로서 용량, 속도, 휘발성에 따라 Cache Memory, Main Memory, Disk Cache, DISK 등이 있다.



[그림 8] 주기억 장치

다) 입 · 출력 기기

- Monitor
- Printers, Key Boards/Mice(마우스), Modem

(2) 소프트웨어

소프트웨어로는 시스템을 운영하는 운영체제 모드와 운영체제의 정책을 결정하는 기술적, 정책적 매커니즘 등으로 구성된다.

가) Operation Mode

운영체제 내의 중요한 시스템 자원을 보호하기 위하여, 각 사용자 프로그램과 프로세스에 각각의 권한(Rings)을 주어 그 권한에 따라 주어진 Mode에서 시스템 자원을 사용할 수 있는지 여부를 결정하는 Privileged Mode의 계층적 구조 중 하나이다. 여기에는 User Mode, Privileged Mode, Additional Mode 등이 있다.

나) Technical Mechanisms

- 계층화(Layering): Ring 모델과 유사한 구조로 각 운영 시스템 프로세스에 적용하여 특정한 기능이 시스템의 서로 다른 계층에서 발생하며, 프로세스와 자원을 분리하고 시스템에 모듈화를 추가하는 구조
- 추상화(Abstraction): 객체지향 프로그램의 원칙으로 객체(또는 운영 시스템 구성요소)의 사용자들은 객체가 동작하는 방법의 내역을 알아야 할 필요는 없다고 정의하는 "Black Box" 원칙

• 프로세스 격리(Process Isolation): 운영 시스템이 각 프로세스의 명령어와 데이터를 위하여 분리된 메모리 공간을 제공하도록 요구함으로써 허가 받지 않은 데이터의 접근을 방지하고 프로세스의 무결성을 보호함

다) Policy Mechanisms

• 최소권한(Least Privilege): 자원이나 프로세스가 그 자신의 기능을 수행할 수 있기 위해 필요한 권한만 가지는 것
• 책임추적성(Accountability): 모든 보안 디자인의 필수적 구성요소로 높은 보안 시스템들은 특권 기능에 대한 개인 책임을 추적하기 위해 물리적 장비를 사용하는 것

2-2. 보안 아키텍처 및 설계 원칙

(1) 설계 원칙

설계 원칙은 시스템의 보안성을 높이기 위한 기준을 말한다. 여기에는 보안 Domain, 보호 링, TCB 등이 있다.

• 보안 Domain: 동일한 보안 원칙이 적용되는 구간 또는 주체가 접근할 수 있는 일련의 객체들의 집합을 말한다.
• TCB(Trusted Computer Base): 시스템의 안전한 환경을 구성하기 위한 논리적인 환경을 말한다. TCB를 구성하기 위해서는 참조 모니터와 보안 커널이 필요하다.
• 참조 모니터(Reference Monitor): 승인되지 않는 접근이나 변경으로부터 객체를 보호하기 위해 객체에 대한 모든 주체의 접근을 통제하고 중재하는 개념이다.
• 보안 커널(Security Kernel): 참조 모니터를 구성하는 핵심 요소이며, 보안 커널은 부정조작을 방지하기 위한 격리성, 오류 여부를 확인하기 위한 작은 사이즈가 되어야 한다는 검증가능성, 공격자가 우회하지 못하게 하는 완전성을 가지고 있어야 한다는 설계 원칙이다.

(2) 보안 모델

정보의 기밀성과 무결성을 보호하기 위한 정책 중에서 가장 효과적이고 활용가능성이 높은 정책이다. 주로 많이 사용하는 보안 모델로는 BLP, Biba, Clark-Wilson 등이 있다.

• 기밀성 모델(Bell-LaPadula Confidentiality Model)
  – 허가된 비밀정보에 허가되지 않는 방식의 접근 방지(기밀성 위주)를 위한 군사적 모델
  – No Read Up: 낮은 등급의 주체가 높은 등급의 객체에 접근하지 못하는 원칙
  – No Write Down: 높은 등급의 주체가 낮은 등급의 객체를 변경하지 못하는 원칙
• 비바 무결성 모델(Biba Integrity Model)
  – 최초 데이터의 변경 방지(무결성)를 위한 상업용 모델
  – No Read Down: 높은 등급의 주체가 낮은 등급의 객체에 접근하지 못하는 원칙
  – No Write Up: 낮은 등급의 주체가 높은 등급의 객체를 변경하지 못하는 원칙
• Clark-Wilson Integrity Model
  – 비바 모델과 유사하게 무결성을 강조한 모델로 상업적 모델에 기반을 둔 모델
• Brewer-Nash(Chinese Wall)
  – 여러 회사들에 대한 자문서비스를 제공하는 환경에서 기업 컨설턴트들에 의해 이해가 충돌되는 회사간의 정보의 흐름이 발생하지 않도록 접근통제 기능을 제공하는 모델

  * 예) A은행을 마케팅 한 컨설팅 회사는 B은행을 마케팅 해서는 안 된다.

2-3. 보안 평가방법

보안 시스템을 평가하는 방법으로서 기존에는 오렌지북으로 불리든, 미국의 TCSEC이 있었으며, 유럽에서 사용하는 ITSEC 등이 있었다. 하지만, 최근에는 글로벌 표준으로 Common Criteria가 각광을 받고 있다.

(1) Common Criteria의 정의

• 국가마다 서로 다른 정보보호 시스템 평가 기준을 연동하고 평가 결과를 상호 인증하기 위해 제정된 국제 표준 평가 기준임
• 현존하는 평가 기준과 조화를 통해 평가 결과의 상호 인정(CCRA)
• 정보보호 시스템의 수출입에 소요되는 인증 비용절감으로 국제 유통 촉진, 정보보호 시스템의 보안 등급 평가에 신뢰성 부여
• 현존하는 평가 기준과 조화를 통해 평가 결과의 상호인정(CCRA: CC 상호인정협정)

(2) Common Criteria의 구성 요소

구성 요소	설명
패키지	– 부분적인 보안 목표를 만족시키기 위한 Component들의 집합으로 구성 – 유용한 요구사항의 모음으로 재사용 가능
EAL	– 보증요구에 관련된 Component들의 집합으로 구성된 패키지의 일종 – CC의 체계화된 보증수준이 보증 등급을 형성
PP	– Protection Profile: 보호 프로파일 – 정보제품이 갖추어야 할 공통적인 보안 요구사항들을 모아 놓은 것
ST	– Security Target: 보안 목표 명세서 – 벤더는 PP를 먼저 참조한 후 제품 명세서인 ST를 작성하여 제품을 개발

지금까지 보안 아키텍처와 설계에 대해서 알아보았다. 보안 아키텍처와 설계는 주요 출제분야가 보안 모델이 주로 출제되므로 보안 모델에 대한 확실한 개념 파악이 필요하다. 따라서, 학습 시 다음의 Key Factor를 참고하여 시험을 준비하기 바란다.

분야	Key Factor	출제 비중
보안 아키텍처와 설계	– 운영 상태, 커널 기능 이해 – 보안 모델, 아키텍처, 그리고 평가기준 학습 – 응용프로그램과 시스템 내의 일반적인 결함 이해	보통

이번 호에는 정보보호와 위험관리, 보안 아키텍처를 살펴보았다. 이 두 가지 도메인은 정보보호 정책을 어떻게 실무에 적용하는가에 대한 내용이었다. 보안은 가장 먼저 정립되어야 하는 것이 관리적 보안으로써, 이 두 가지 도메인이 관리적 보안의 핵심이다. 따라서, 이 부분은 앞으로 학습할 8가지 도메인의 기반임으로 철저한 학습이 필요하다.

다음 호에는 나머지 8가지 CISSP 도메인 중에서 기술적 보안에서 가장 중추적인 역할을 하는 통신 및 네트워크 보안, 접근통제 도메인에 대해서 알아보고자 한다.

3. 연습 문제

간단한 문제를 통해서 이번 호에 배운 도메인에 대한 이해능력을 키우자. 중요한 것은 실제 시험에서는 이보다 어려운 문제가 출제되나, 기본을 알면 충분히 풀 수 있는 문제이니 문제를 풀고 잘못 이해하는 부분은 요점 정리를 통해 복습을 하길 바란다.

▣ 정보보호와 위험관리

1. 사업장에서 정보보호에 관한 책임은 누구에게 있는가?
   ① Data 소유자 ② Data 관리자 ③ 사업 책임자 ④ 경영진

2. 직원의 해고 통보 시 가장 먼저 해야 할 것은 무엇인가?
   ① 해당직원의 계정삭제 ② 해당직원의 계정중지 ③ 해당직원의 모든 접근차단 ④ 퇴사자 면담

3. 해커들이 자신들의 행위를 정당화하기 위해 가장 보편적으로 사용하고 있는 주장은 무엇인가?
   ① 해킹은 예술이다. ② 기술은 인간을 위해 쓰여 져야 한다.
   ③ 정보는 공유되어야 한다. ④ 실력 있는 해커는 대우받을 수 있다.

4. 1주~2주간의 갑작스런 강제휴가를 통해 조직이 얻을 수 있는 가장 큰 장점은 무엇인가?
   ① 부정행위를 보다 자유롭게 조사할 수 있다. ② 공모자의 확인이 가능하다.
   ③ 직원을 강제퇴사 시킬 수 있다. ④ 직원들의 회사에 대한 충성심이 높아진다.

5. A회사는 직원들의 보안의식교육을 진행한 후 교육에 대한 성과를 측정하기를 원하고 있다.
   다음 보기 중 보안의식교육을 가장 성공적으로 진행했다고 볼 수 있는 것은 무엇인가?
   ① 신고 되는 사고건수(취약성 등)의 증가 ② 신고 되는 사고건수(취약성 등)의 감소
   ③ 교육을 받은 전체직원의 감소 ④ 접근 규칙 위반 전수 감소

▣ 보안 아키텍처 및 설계

1. 상태 머신 모델에 기반 한 보안 모델은 무엇인가?
   ① Bell-LaPadula, Take-Grant ② Biba, Clark-Wilson
   ③ Clark-Wilson, Bell-LaPadula ④ Bell-LaPadula, Biba

2. 데이터 기밀성을 언급하는 보안 모델은 무엇인가?
   ① Bell-LaPadula ② Biba ③ Clark-Wilson ④ Brewer and Nash

3. 낮은 수준의 주체가 높은 수준의 객체에 대해 접근하지 못하도록 하는 Bell-LaPadula의 속성은 무엇인가?
   ① *(star) Security Property ② No write up property
   ③ No read up property ④ No read down property

4. TCB란 무엇인가?
   ① 안전한 전송을 지원하는 당신의 네트워크상의 호스트 ② 운영체제 커널과 디바이스 드라이버
   ③ 보안정책을 집행하는 하드웨어, 소프트웨어, 통제의 조합 ④ 보안정책을 인증하는 소프트웨어와 통제

5. 보안목표명세서 ST(Security Target)과 관련 있는 것은 무엇인가?
   ① ISO27001 ② BS7799 ③ ISO9000 ④ CC(Common Cretaria)

정답 : ④, ③, ③, ①, ①, ④, ①, ③, ③, ④