해설과 함께 풀어 보는 최신 기출문제 | 2015년 9월 19일 시행

* 본 문제는 실제 시험지를 기준으로 작성된 것으로, 저자가 시험응시 후 복원한 문제입니다.

1과목 시스템 보안

상 중 하 시스템 보안 > 리눅스 서버 보안

01 트로이목마 프로그램인 루트킷에 대한 설명으로 틀린 것은?

① 시스템에 침입 후 다시 침입을 위해서 백도어를 설치한다.
② 주로 트로이목마, 원격접근, 로그삭제, 관리자 권한 획득 등의 불법적인 해킹에 사용되는 프로그램의 모임이다.
③ 트로이목마는 자기복제를 통하여 증식시킨다
④ 네트워크상에서 다른 사용자의 ID와 패스워드를 탐지하여 관리자 권한을 획득한다.

트로이목마의 특징은 특정 조건이 되면 실행되며 정보 유출을 목적으로 하지만, 자기복제는 하지 않는다.

정답 ③

상 중 하 시스템 보안 > 리눅스 서버 보안

02 유닉스(UNIX) 시스템에서 패스워드는 /etc/passwd 파일에 해시 값으로 보유하고 있다. 이러한 해시 값을 보유하기 위해서 임의적으로 필드를 늘려서 해시 값을 보이지 않게 한다. 이와 관련된 것은 무엇인가?

① /etc/passwd
② /etc/shadow
③ /etc/rhosts
④ /etc/hosts

Shadow 파일은 사용자 패스워드를 보관하는 파일로 md5를 사용한 해시 값을 가지고 있다. 이것은 salt 값을 포함하고 있고 첫 번째 $는 사용자가 만든 해시 값이고 두 번째 $는 salt 값이다.

정답 ②

상 중 하 시스템 보안 > 리눅스 서버 보안

03 다음의 도구 중 무결성을 검사하는 도구가 아닌 것은?

① fcheck
② tripwire
③ prstat
④ shmhain

prstat는 어떤 프로세스가 CPU 자원을 소모하는지 확인하는 프로그램이다.

prstat

```
limbest$ prstat -s cpu -n 5

PID USERNAME SIZE RSS STATE PRI NICE TIME CPU PROCESS/NLWP
13974 limbest 888K 432K run 40 0 36 : 14.51 69% cpuhog/1
27354 limbest 2216K 1928K run 31 0 314 : 48.51 23% server/5
14690 root 136M 46M sleep 59 0 0 : 00.59 2.3% Xsun/1
```

정답 ③

상 중 하 시스템 보안 > 리눅스 서버 보안

04 rlogin은 ID와 Password 없이도 로그인이 가능하다. 즉, 인증 없이 시스템에 접근할 수 있다. 이와 관련된 파일은 무엇인가?

① hosts
② hosts.equiv
③ .profile
④ service

r-command를 통해서 인증 없이 중요 정보 유출 및 시스템 공격 등을 수행할 수 있고 이때 사용되는 파일이 hosts.equiv와 .rhosts이다. 본 파일은 root 혹은 600으로 권한을 설정하고 파일 내에"+"설정이 없어야 한다.

- /etc/hosts.equiv 및 $HOME/.rhosts 파일 소유자가 root 또는, 해당 계정인 경우
- /etc/hosts.equiv 및 $HOME/.rhosts 파일 권한이 600 이하인 경우
- /etc/hosts.equiv 및 $HOME/.rhosts 파일 설정에'+'설정이 없는 경우

정답 ②

상 중 하 시스템 보안 > 윈도우 클라이언트 및 서버 보안

05 다음은 윈도우 서버 인증에 관련된 설명이다. 괄호 안에 알맞은 것은 무엇인가?

> 윈도우 서버 인증은 도메인 정보를 통해서 인증을 할 수 있고 (1)는 인증을 수행하고 그 다음 (2) 인증을 수행한다.

① (1) 도메인 컨트롤러 (2) 컴퓨터
② (1) 컴퓨터 (2) 도메인 컨트롤러
③ (1) 도메인 컨트롤러 (2) 부도메인 컨트롤러
④ (1) 부도메인 컨트롤러 (2) 컴퓨터

도메인(Domain)은 컴퓨터 계정과 사용자 계정 같은 객체들을 지역적으로 모아 놓은 것을 의미한다. 도메인 컨트롤러(Domain Controller)는 액티브 디렉터리(Active Directory) 정보의 복사본을 가지고 있는 컴퓨터로 액티브 디렉터리의 정보 요청에 응답하고 네트워크를 통한 사용자 인증, DNS 통합 등을 수행한다.

정답 ①

상 중 하 네트워크 보안 > 네트워크 기반 공격 기술의 이해 및 대응

06 아래의 공격 기법 중에서 TCP에 해당하는 공격 기법은?

① ARP Spoofing
② ICMP Redirect
③ SYN Flooding
④ IP Spoofing

SYN Flooding은 TCP 연결 시 사용되는 SYN 신호를 계속적으로 발생시켜서 서버를 공격하는 DDoS 공격 기법이다.

정답 ③

상 중 하 네트워크 보안 > 네트워크 기반 공격 기술의 이해 및 대응

07 아래에서 설명하는 것은 무엇인가?

> 32bit IP 주소는 48bit MAC 주소와 매핑되어 사용된다. IP 주소와 MAC 주소를 메모리 캐시에 보관하여 근거리 네트워크상에서 수신자 의MAC 주소를 알아낼 수 있다. 이때 이러한 캐시를 변조하여 의도하지 않은 단말로 통신하게 한다.

① DNS Spoofing
② Web Spoofing
③ ARP Spoofing
④ Land Attack

ARP Spoofing

- 로컬 통신 과정에서 서버와 클라이언트는 IP와 MAC 주소로 통신을 수행한다.
- 클라이언트의 MAC 주소를 중간에 공격자가 자신의 MAC 주소로 변조하여 마치 서버와 클라이언트가 통신하는 것처럼 속이는 공격이다. 이러한 공격은 Fragrouter를 통하여 연결이 끊어지지 않도록 Release를 해주어야 한다.

정답 ③

상 중 하 시스템 보안 > 운영체제 구조

08 다음 중 비선점 스케줄링 기법으로 올바르게 짝지은 것은 무엇인가?

① FCFS, SJF
② Round Robin, SJF
③ FSCF, Round Robin
④ SJF, SRT

비선점 스케줄링(Non-Preemptive)은 프로세스(Process)가 CPU를 해제할 때까지 다른 프로세스는 대기(Wait)해야 하는 스케줄링 기법으로 FCFS, SJF, HRN, 우선순위, 기한부 스케줄링이 있으며, 선점 스케줄링(Preemptive)은 라운드로빈, SRT, 다단계 큐, 다단계 피드백 큐 방법이 있다.

정답 ①

상 중 하 시스템 보안 > 윈도우 클라이언트 및 서버 보안

09 Windows NT File System은 EFS(Encrytion File System)를 지원한다. EFS에 대한 설명으로 올바르지 않은 것은?

① 암호화된 파일을 NTFS가 아닌 다른 파일 시스템에 복사해도 복호화되지 않는다.
② NTFS에서만 사용 가능하고 읽기 전용, 압축, 숨김과 같은 기능을 제공한다.
③ 파일에 대해서 암호화 특성을 설정하여 암호화 기능을 제공한다.
④ 모든 파일과 하위 폴더를 자동으로 암호화한다.

암호화된 파일을 NTFS가 아닌 다른 파일 시스템 파티션에 복사하면 암호화가 풀려버리기 때문에 잘 사용되지 않는다.

오답 피하기

EFS는 NTFS 파티션에서만 사용 가능하고, 읽기 전용, 압축 또는 숨김과 같은 다른 특성을 설정할 때와 마찬가지로 폴더와 파일에 암호화 특성을 설정함으로써 폴더나 파일을 암호화하거나 해독할 수 있다. 폴더를 암호화하면 암호화된 폴더에 만들어지는 모든 파일과 하위 폴더도 자동으로 암호화된다.

정답 ①

상 중 하 시스템 보안 > 운영체제 구조

10 다음은 가상기억장치에 대한 설명이다. 괄호 안에 알맞은 것은 무엇인가?

> • 가상기억장치를 관리하기 위해서 ( ) 고정된 크기를 사용한다.
> • 가상기억장치를 관리하기 위해서 ( ) 가변된 크기를 사용한다.

① Paging, Segmentation
② Segmentation, Paging
③ Block, Frame
④ Frame, Block

가상기억장치를 관리하기 위해서 고정길이 크기를 분할하여 관리하는 것은 페이지(page)이고 가변 길이로 관리하는 것은 세그먼트(Segment)이다.

구분	Paging 기법	Segmentation 기법
할당	고정(Static) 분할	가변(Dynamic) 분할
적재	요구 Page만 일부 적재(On-demand)	프로그램 전체 적재
관점	메모리 관리 측면	파일 관리 측면
장점	• 요구 Page만 온디맨드 Load • 외부 단편화 해결 • 교체시간 최소	• 사용자 관점에서 프로그래밍 용이 • 내부 단편화 해결 • 코드, 데이터 공유 용이
단점	• 내부 단편화(Fragmentation) 발생 • Thrashing, 잦은 디스크 I/O 유발	• 외부 단편화 심각 • 메인 메모리가 커야 함

정답 ①

상 중 하 정보보안 일반 > 보안 요소 기술

11 FDS에 대한 설명으로 올바르지 않은 것은?

① 사용자의 금전적 손실 및 정보유출을 탐지한다.
② 추론 알고리즘을 사용하여 정상 패턴을 데이터베이스화하고 탐지한다.
③ 속임수나 거짓말을 사용한 범죄 행위를 탐지한다.
④ 핀테크 서비스, Paypal 서비스 등의 간편 결제에 대한 이상 행위를 탐지한다.

FDS(Fraud Detection System)는 이상 행위 탐지 시스템으로 핀테크, Paypal 서비스의 간편 결제 시스템에서 거짓및 부정한 방법으로 금전적 손실과 정보 유출을 탐지한다. 본 문제는 정보보안기사의 시험 범위 내의 주제는 아니지만, 최신 보안 이슈 및 정보기술 관련 이슈는 실제 시험에서 두 문제 정도 출제된다. 이러한 문제는 간단한 용어만 학습하여도 충분하다.

정답 ②

상 중 하 시스템 보안 > 운영체제 구조

12 MDM(Mobile Device Management)의 기능 설명으로 올바르지 않은 것은?

① 분실, 도난관리
② 원격 강제잠금, 원격 백업과 복구
③ 디바이스 통제 및 차단, 화이트 리스트 기반 앱 관리
④ 설정, 네트워크 환경관리

MDM(Mobile Device Management)은 스마트 폰 분실 및 도난, 원격 강제 잠금, 사용자 통제, 원격 백업과 복구, 블루투스 및 카메라, GPS 등의 디바이스 통제, 화이트 리스트 및 블랙 리스트 기반의 앱(Application) 관리, 알 수 없는 소스 차단, 루팅 탐지 등을 수행하는 솔루션이다.

정답 ④

상 중 하 시스템 보안 > 리눅스 서버 보안

13 레이스컨디션(Race Condition)에 대한 설명으로 올바르지 않은 것은?

① 두 개 이상의 프로세스들이 공유 자원에 동시에 접근하여 읽기 및 쓰기를 못하게 해야 한다.
② 여러 번 실행되는 과정에서 실행 순서가 뒤바뀌어 실행자가 원하는 결과를 얻는다.
③ 하드 링크를 통해서 접근한다.
④ 임시파일을 사용하여 공격한다.

하드 링크(Hard Link)가 아니라 심볼 링크(Symbolic Link)를 통해서 접근한다. 심볼 링크는 원래 파일에 경로 정보만 가지고 있는 것으로 포인터(Pointer)만 가지는 것이다. 하드 링크는 원래 파일의 inode를 공유해서 사용하는 것으로 하드 링크가 수정되면 원본 파일도 변경된다. 즉, 이름이 다른 같은 파일을 만드는 것이다.

정답 ③

상 중 하 시스템 보안 > 운영체제 구조

14 다음 지문에서 설명하는 것은?

> 계수기나 카운터를 두어서 가장 최근에 참조하지 않은페이지를 교체하는 것으로 계수기 및 카운터는 하드웨어에 의해서 구현될 수 있다.

① HRN
② LFU
③ LRU
④ Round Robin

LRU(Least Recently Used) 알고리즘

가장 오래 참조되지 않은 페이지를 교체한다. 가장 보편적인 방법이나, Time Stamping에 의한 Overhead가 존재한다.

참조페이지	2	3	2	1	5	2	3	5
페이지 프레임	2	2	2	2	2	2	2	2
		3	3	3	5	5	5	5
			1	1	1	1	3	3
	●	●		●	●		●	

오답 피하기

- HRN은 서비스 시간과 대기 시간을 고려하여 우선순위를 산정한 후 가장 큰 작업에게 우선순위를 부여하는 방법이다.
- LFU는 사용한(참조된) 횟수가 가장 적은 페이지를 교체하는 방법이다.
- 라운드 로빈(Round Robin)은 시간을 할당하여 CPU를 사용하는 방법으로 시간 할당량이 적을 경우 문맥교환에 따른 오버헤드가 커진다.

정답 ③

상 중 하 시스템 보안 > 윈도우 클라이언트 및 서버 보안

15 윈도우 시스템 이벤트 관리 도구에 대한 설명으로 올바르지 않은 것은?

① 이벤트 로그는 응용, 보안, 시스템이 있다.
② C:₩Windows₩System32₩config₩system.evt 파일에 환경을 설정한다.
③ 기본적으로 저장되는 경로는 C:₩Windows₩System32₩winevt₩Logs이다.
④ 윈도우 시스템 로그를 실시간으로 기록하고 날짜, 시간, 사용자, 컴퓨터, 이벤트 ID, 이벤트 종류, 정보, 경고, 오류 등을 관리한다.

윈도우 시스템이 로그를 보관하는 방법은 로그파일 형식(.evt), 텍스트 파일 형식(.txt), 쉼표 구분 텍스트 파일 형식(.csv)이 있고, system.evt는 로그파일이다.

정답 ②

상 중 하 정보보안 일반 > 접근 통제

16 주체의 역할에 따라서 접근할 수 있는 객체를 지정하는 방법으로 그룹에 근거한 ID를 관리하며, 사용자의 역할에 권한이 부여되는 것은 무엇인가?

① Task-based
② DAC
③ RBAC
④ MAC

RBAC(Role-based Access Control)는 사용자의 역할(혹은 임무)에 의해서 권한을 부여하는 것으로 PM 권한, 개발자 권한, 디자이너 권한과 같이 관리한다.

정답 ③

상 중 하 시스템 보안 > 리눅스 서버 보안

17 아래에서 설명하는 것은 무엇인가?

> Syslogd.conf 파일을 사용하며 메시지를 표시하는 필드 및 기록위치를 표시하는 필드로 구성된다. 또 시스템 로그, 보안 로그, 부팅로그등을기록한다.

① Daemon
② Message
③ Syslogd
④ Service

Syslog는 로그에 대한 메시지 표준으로 다양한 프로그램들이 생성하는 메시지를 저장하고 이 메시지를 사용해서 분석기능을 제공하는 로그 메시지이다. Syslog는 프로그램, 장비(Device) 등의 문제점과 성능을 확인할 수 있다. 또한, 시스템 관리, 보안, 시스템 정보, 디버깅 메시지 등의 정보를 제공한다. 이러한 로그를 기록하는 프로세스의 이름은 Syslogd이다.

정답 ③

상 중 하 네트워크 보안 > 네트워크 기반 공격 기술의 이해 및 대응

18 HTTP 쿠키에 대한 설명으로 올바르지 않은 것은?

① 지속적인 클라이언트 측의 상태를 저장하기 위해서 사용된다.
② 서버는 클라이언트 브라우저에 쿠키를 설정하기 위해서 HTTP Header에 Set-Cookie를 포함시킨다.
③ 쿠키의 저장 공간에 제약이 없어서 편의성은 향상되지만, 보안에 취약하다.
④ 키와 값의 구조를 이룬다.

쿠키(Cookie)는 최대 4KB의 공간을 저장한다.

정답 ③

상 중 하 시스템 보안 > 리눅스 서버 보안

19 다음 내용 중 inode에 포함되지 않은 것은 무엇인가?

① 접근 모드
② 링크 수
③ 파일 수정 시간
④ 파일명

iNode가 보유하고 있는 데이터
- 파일 소유자의 사용자 ID
- 파일 소유자의 그룹 ID
- 파일 크기
- 파일이 생성된 시간
- 최근 파일이 사용된 시간
- 최근 파일이 변경된 시간
- 파일이 링크된 수
- 접근 모드
- 데이터 블록 주소

정답 ④

상 중 하 네트워크 보안 > 네트워크 기반 공격 기술의 이해 및 대응

20 DDoS 공격에 대한 설명으로 올바르지 않은 것은?

① CPU, Memory 등의 시스템 자원을 고갈시키는 공격이다.
② 시스템의 정보를 획득하는 수동적 공격이다.
③ C&C 서버로부터 명령을 받은 좀비 PC에 의해서 다량의 트래픽을 유발시킨다.
④ 네트워크 대역을 급속도로 소모시켜 서비스를 사용할 수 없게 한다.

정보 획득을 목적으로 공격하는 것을 수동적 공격(Passive Attack)이라고 하고 가장 대표적인 방법은 스니핑(Sniffing)이다.

정답 ④

2과목 네트워크 보안

상 중 하 네트워크 보안 > 네트워크 기반 공격 기술의 이해 및 대응

21 호스트 기반 IDS의 장점으로 올바른 것은 무엇인가?

① Promiscuous 모드로 동작하는 패킷을 모니터링할 수 있다.
② 네트워크 자원 손실 및 패킷의 변조를 유발하지 않는다.
③ 감시영역이 크고 실시간 탐지가 가능하다.
④ 내부자에 의한 공격, 바이러스, 웜, 트로이목마에 대해서 탐지한다.

HIDS(Host based IDS)는 시스템에 설치되어서 사용자가 시스템에 행하는 행위를 모니터링하여 침입 여부를 결정하는 것으로 내부자에 의한 공격, 바이러스, 웜, 트로이목마, 백도어에 대한 탐지가 가능하다.

정답 ④

상 중 하 네트워크 보안 > 네트워크 기반 공격 기술의 이해 및 대응

22 Snort의 탐지 Rule이다. 설명으로 올바른 것은 무엇인가?

```
alert tcp 210.1.1.1 20 -> 190.1.1.1 20
{msg : "Limbest", flow : established
```

① TCP 연결이 확립된 경우 모두 경고 메시지를 출력하게 한다.
② tcp와 udp 모두를 탐지하고 tcp만 경고 파일을 추가로 기록하게 한다.
③ IDS와 같은 탐지이며 실시간 및 배치 형태로 탐지가 가능하다.
④ 210.1.1.1에서 190.1.1.1로 전송되는 패킷 중에서 TCP 연결을 확립한 패킷은"Limbest"라는 경고 메시지를 출력한다.

Snort에서"->"는 방향을 의미하고 flow : established는 TCP 연결 확립을 의미하며 alert는 경고, msg는 출력할 메시지 내용을 의미한다. 따라서 210.1.1.1에서 190.1.1.1로 향하는 패킷 중에서 TCP 연결을 확립하면"Limbest"라는 메시지를 출력한다.

정답 ④

상 중 하 네트워크 보안 > 네트워크 기반 공격 기술의 이해 및 대응

23 VPN의 터널링에 대한 설명이다. 올바르지 않은 것은 무엇인가?

① 데이터를 IP 패킷화할 때의 통신규약으로 캡슐화와 동시에 안전성을 확보한다.
② Point to Point 터널링으로 PPTP와 L2TP, SSL이 있다.
③ 터널링은 공개된 네트워크를 사용하여 안정적으로 데이터 송수신할 때 사용한다.
④ 암호화를 통해서 스니핑으로 원본을 확인할 수 없게 된다.

터널링은 VPN의 핵심기술로 데이터를 암호화하여 전송한다. 터널링은 단순히 암호화하는 경우와 달리 내부 자원에 접속할 때만 암호화를 수행하여 터널링하고 외부 자원 즉, 인터넷에 접속할 때는 암호화를 수행하지 않는다. 기업 내부에서 안정적으로 통신하는 것과 동일한 효과를 얻으며 데이터 링크(Data Link) 계층의 터널링 기술은 PPTP, L2TP가 있다.

정답 ②

상 중 하 네트워크 보안 > 네트워크 기반 공격 기술의 이해 및 대응

24 다음 중 VPN의 종류로 올바른 것은 무엇인가?

① IPSEC, SET, SSL
② PPTP, L2TP, WAP
③ L2TP, IPSEC, SSL
④ PPTP, WAP, IPSEC.

L2TP, PPTP, SSL, IPSEC, MPLS VPN은 모두 VPN의 터널링 기술이다.

정답 ③

상 중 하 네트워크 보안 > 네트워크 기반 공격 기술의 이해 및 대응

25 다음은 봇넷(Bonet)에 대한 설명이다. 올바르지 않은 것은 무엇인가?

① 악성코드에 감염된 좀비 컴퓨터를 의미한다.
② 감염된 컴퓨터들이 네트워크를 형성한다.
③ 은닉된 함정으로 악성코드를 탐지하고 대응한다.
④ 피해를 줄이기 위해서는 보안 패치 적용, 불필요한 공유 삭제, 정기적 백신 업데이트를 수행한다.

봇넷(Bonet)은 악성코드에 감염된 컴퓨터들이 네트워크를 형성한 것으로 스팸메일 전송, 바이러스 유포, 컴퓨터 공격등에 악용된다. 이것은 보안패치 적용, 불필요한 공유 삭제, 정기적으로 백신을 업데이트해야 예방할 수 있다.

정답 ③

상 중 하 네트워크 보안 > 네트워크 기반 공격 기술의 이해 및 대응

26 다음 보기의 괄호 안에 올바른 것은?

감염된 컴퓨터들이 서로 네트워크를 형성하는 것을 ( )이라고 하며 이러한 좀비 PC를 조종하는 컴퓨터는 ( )이라고한다. ( )은/는 봇넷에 참여한 좀비 PC에서 명령을 전달한다.

① 봇넷 – C&C 서버 – 봇마스터
② 봇마스터 – 봇넷 – C&C 서버
③ 봇넷 – 봇마스터 – C&C 서버
④ C&C 서버 – 봇넷 – 봇마스터

봇(Bot)이란 컴퓨터 시스템의 보안 취약점을 이용하여 설치된 악성 프로그램을 의미하며 이들 간에 형성된 네트워크를 봇넷이라고 한다. 봇마스터는 이러한 좀비 PC를 조종하고 C&C 서버는 Command & Control 서버로 좀비 PC에서 명령을 전달한다.

정답 ③

상 중 하 네트워크 보안 > 최신 네트워크 위협 및 대응 기술

27 무선 LAN의 보안 규격을 사용하는 프로토콜은 무엇인가?

- IEEE 802.1x, IEEE 802.11i를 지원
- TKIP를 통한 임시 키 무결성 관리

① SSID
② IEEE 802.1x
③ EAP
④ WPA

WPA(Wi-Fi Protected Access)는 무선 LAN 보안 프로토콜로 WEP의 취약점을 해결하고 IEEE 802.11i 보안 표준을 구현했다. 즉, IEEE 802.11i가 완성되기 전에 일시적으로 사용하기 위해서 개발했다. WPA2는 해당 장치가 확장 프로 토콜 표준을 준수하고 있다는 것을 보장한다. 즉, WPA는 임시 키 무결성 프로토콜인 TKIP를 통해서 데이터 암호화를 향상하고 EAP를 사용한 사용자 인증 기능을 구현했다. WPA2는 고급 암호화 표준인 AES를 지원한다.

오답 피하기

EEE 802.1x는 무선 LAN 인증 구조로 EAP를 사용한 무선 LAN 인증을 지원한다.

정답 ④

상 중 하 네트워크 보안 > 네트워크 기반 공격 기술의 이해 및 대응

28 APT 공격의 유형으로 올바르지 않은 것은?

① 제로데이 공격 APT
② DDoS 공격 APT
③ MAIL APT
④ 백도어 APT

APT(Advanced Persistent Threat)는 사회관계망 서비스(Social Network Service)를 사용하여 정보수집, 악성코드 배포를 수행하고 공격표적을 선정하여 지속적으로 공격을 수행하는 것이다.

오답 피하기

Zero Day Attack은 소프트웨어 패치 취약점을 이용한 공격이며 MAIL APT는 악성코드를 메일에 첨부하여 발송하고 이를 통해서 정보를 획득한다. 백도어 APT는 표적에 침투 후 백도어를 설치하여 재침입 시 유입경로를 열어두는 것이다.

정답 ②

상 중 하 네트워크 보안 > 네트워크 기반 공격 기술의 이해 및 대응

29 허니팟(Honey Pot)에 대한 설명으로 올바르지 않은 것은 무엇인가?

① 컴퓨터 시스템에 침입한 스팸, 바이러스, 크랙커를 탐지하는 가상의 컴퓨터 시스템이다.
② 실제 공격을 당한 것처럼 보이도록 만든 함정이다.
③ 공격자가 허니팟으로 접근할 수 없도록 차단해야 한다.
④ 침입자가 오래 머물게 해야 한다.

허니팟(Honey Pot)은 일종의 함정으로 공격자가 오래 머물게 하여 공격자를 식별하고 대응한다. 그러므로 의도적으로 취약점을 공개하여 허니팟으로 유인해야 한다.

정답 ③

상 중 하 네트워크 보안 > 네트워크 기반 공격 기술의 이해 및 대응

30 다음 중 아래에서 설명하는 것은 무엇인가?

- 컴퓨터의 보안 취약점을 이용한 공격으로 대상 컴퓨터의 권한 획득, DoS 공격을 수행한다.
- 취약점을이용한공격의종류는 BOF, CSRF, XSS 등이존재한다.

① exploit 코드
② Web Shell
③ SQL Injection
④ Zero day Attack

exploit이란 컴퓨터의 보안 취약점을 이용한 공격으로 결함을 이용해서 의도된 동작을 수행하게 한다. 이것은 명령, 스 크립트, 데이터 조작과 같은 공격을 수행하고 BOF, CSRF, XSS 공격 등이 존재한다

정답 ①

상 중 하 네트워크 보안 > 네트워크 대응 기술 및 응용

31 배스천 호스트에 대한 설명으로 올바르지 않은 것은?

① 시스템 관리자가 중점적으로 관리해야 하는 시스템이다.
② 접근 제어, 응용 시스템, 게이트웨이로 가상 서버의 설치, 인증, 로그 등을 담당한다.
③ 주로 해킹의 대상이 되므로 취약점이 존재하지 않도록 해야 하며 배스천 호스트가 공격당하면 내부 네트워크도 침입이 가능하게 된다.
④ 로그 생성과 관리가 용이하지만 Screening Router보다는 불안전하다.

배스천 호스트(Bastion Host)는 일종의 요새라는 의미로 내부 네트워크와 외부 네트워크를 분리하여 응용 계층에서 동작하기 때문에 Screening Router보다 안전하고 접근 제어, 로그 기록과 같은 역할을 수행한다.

정답 ④

상 중 하 네트워크 보안 > 네트워크 기반 공격 기술의 이해 및 대응

32 VPN 계층에 대한 연결로 올바른 것은 무엇인가?

① IPSEC – Application
② PPTP – Network
③ L2TP – Data Link
④ SSL – Data Link

L2TP 및 PPTP 터널링 기술은 모두 Data Link 계층에서 동작한다.

정답 ③

상 중 하 네트워크 보안 > 네트워크 대응 기술 및 응용

33 UTM에 대한 설명으로 올바르지 않은 것은?

① 방화벽, VPN, IPS 등의 보안 기능을 하나로 통합한 통합 보안을 제공한다.
② 각각 다른 보안 정책을 수립하여 적용한다.
③ 보안 기능을 한꺼번에 해결하여 구축 시 비용이 절감된다.
④ 다양하고 복잡한 보안 위협에 대응하고 편의성이 향상된다.

UTM(Unified Threat Management)은 방화벽, VPN, IDS, IPS 등의 보안 기능을 하나로 통합한 보안 솔루션으로 구축 비용을 절감하고 유지보수의 편의성을 향상시킨다. 또한, 일관된 보안 정책을 적용할 수 있다.

정답 ②

상 중 하 네트워크 보안 > 네트워크 기반 공격 기술의 이해 및 대응

34 다음 지문에서 설명하는 포트 스캐닝 방법은 무엇인가?

가. TCP SYN 패킷을이용하여접속을시도하고포트가열려있는경우응답패킷인 SYN/ACK에대해접속을강제로종료 (RST)해정상적인 TCP 3-Way Handshaking 과정을맺지않는방법이다.
나. NULL Packet을전송하고응답이없으면 Port Open으로판단한다.
다. Stealth Scan이라고도부르며 TCP Flag의FIN을활성화하여전송한다.

① TCP Half Open, Null Scan, TCP FIN
② TCP Connection, XMAS,TCP FIN
③ TCP FIN, XMAS, TCP Half Open
④ TCP FIN, XMAS, NULL SCAN

NMAP을 사용한 포트스캔(Port Scan)

NMAP Port Scan	설명
TCP connect() scan	3-Way Handshaking을 수립하고 Target System에서 쉽게 탐지가 가능함
TCP SYN scan	• SYN 패킷을 대상 포트로 발송하여 SYN/ACK 패킷을 수신 받으면 Open 상태 • SYN 패킷을 대상 포트로 발송하여 RST/ACK을 수신 받으면 Close 상태 • Half Open 혹은 Stealth Scanning이라고 함
TCP FIN scan	• 대상 포트로 FIN 패킷을 전송하고 닫혀 있는 포트는 RST를 전송함 • 포트가 개방되어 있으면 패킷을 무시함
TCP Null	• 모든 플래그를 지움 • 대상 포트가 닫혀 있으면 RST를 돌려보내고 개방 상태이면 패킷을 무시함
TCP Xmas Tree SCAN	• 대상 포트로 FIN, URG, PUSH 패킷을 전송 • 대상 시스템에서 포트가 닫혀 있으면 RST를 되돌려 보냄 • 포트가 개방되어 있으면 패킷을 무시함

정답 ①

상 중 하 네트워크 보안 > 네트워크 기반 공격 기술의 이해 및 대응

35 다음 지문의 라우터 Access-list를 보고 올바르지 않은 것을 고르시오.

```
access-list 101 deny tcp 160.20.0.0 0.0.0.255 any eq 22
access-list 101 deny tcp 160.20.0.0 0.0.0.255 any eq 80
access-list 101 deny udp 160.20.0.0 0.0.0.255 any eq 53
access-list 101 permit icmp any any2
```

① 160.20.X.X에서 유입되는 telnet과 SSH 서비스를 모두 차단한다.
② 160.20.X.X로 유입되는 HTTP 서비스를 모두 차단한다.
③ DNS 서비스를 거부하고 있다.
④ 모든 ICMP를 허용한다.

22번 포트를 사용하는 SSH에 대해서 160.20.X.X로 연결을 모두 거부한다. telnet은 TCP 23번 포트를 사용한다.

정답 ①

상 중 하 네트워크 보안 > 네트워크 기반 공격 기술의 이해 및 대응

36 아래의 hping3 명령에 해당하는 공격 방법은 무엇인가?

hping3 210.10.10.255--icmp--flood -a 210.10.10.12

① LAND
② Ping of Death
③ SYN Flooding
④ Smurf

본 문제는 icmp 신호를 계속적으로 발생시키는 DDoS 공격 기법인 ICMP Flooding에 관한 문제이다. ICMP Flooding 기법은 다른 말로 Smurf라고도 한다.

정답 ④

상 중 하 네트워크 보안 > 네트워크 기반 공격 기술의 이해 및 대응

37 기업 내부의 정보시스템을 훔쳐보는지 확인하기 위해서 수행해야 할 것은 무엇인가?

① ICMP 트래픽을 추적한다.
② 특정 패킷을 분석한다.
③ 스니핑에 Promiscuous Mode가 가동 중인지 확인한다.
④ 네트워크 성능 저하를 확인한다.

Promiscuous Mode를 사용했다는 것은 유입되는 모든 패킷을 모니터링 하고 있다는 것으로 정상적인 경우 모니터링을 할 이유가 없는 것이다. 그러므로 Promiscuous Mode가 설정되어 있다면 스니핑을 하고 있다고 의심할 수 있다.

스니핑(Sniffing) 모드

- Normal Mode : 자신에게 들어오는 목적지 MAC 주소로 올릴 것인지 혹은 버릴 것인지를 판단하는 모드이다.
- Promiscuous Mode : LAN 카드에게 들어오는 모든 패킷을 목적지 MAC 주소와 상관없이 모두 올려 버리는 모이다.(LAN 카드는 자신의 주소로 온 패킷일 경우 상위계층으로 올려주지만, 자신의 주소로 오지 않는 패킷은 폐기한다. 하지만 Promiscuous Mode는 모든 패킷을 상위계층으로 올려준다.) Command 〉 ifconfig eth0 promisc

정답 ③

상 중 하 네트워크 보안 > 네트워크 대응 기술 및 응용

38 다음 IDS에 대한 설명 중 괄호 안에 올바른 것을 고르시오.

( )는 공격 패턴을 저장하고 있다가 공격 패턴과 동일한 패턴이 발견되면 공격으로 인식하는 것으로 ( )는 네트워크의 트래픽을 모니터링하여 식별한다.

① 시그니처, NIDS
② 시그니처, HIDS
③ 행위, NIDS
④ 행위, HIDS

오용탐지(Misuse)는 공격 패턴을 저장하고 이와 동일하면 공격을 식별하는 시그니처 기반 탐지 방법으로 False Positive는 낮지만, False Negative가 크다. NIDS는 네트워크 패킷을 모니터링하여 탐지를 수행한다.

정답 ①

상 중 하 네트워크 보안 > 네트워크 대응 기술 및 응용

39 IDS의 이상탐지와 오용탐지에 대한 설명으로 올바르지 않은 것은?

① 시그니처 기반, 지식기반 탐지 방법을 오용탐지(Misuse)라고 하며 일반적으로 가장 많이 사용되는 방법이다.
② 공격패턴을 미리 알 수 있을 때 효과적으로 False Negative가 크다는 문제점을 가지고 있는 것은 이상탐지이다.
③ 프로파일 기반, 행위기반, 통계기반 탐지 방법은 이상탐지(Anomaly)이다.
④ 이상탐지는 False Positive가 크지만 알려지지 않은 공격에 대응할 수 있다.

False Negative가 크다는 것은 공격인데 공격이 아니라고 오판하는 것으로 오용탐지(Misuse)의 단점이다. 그리고 False Positive가 크다는 것은 공격이 아닌데 공격으로 오판하는 것으로 이상탐지(Anomaly)의 단점이다.

정답 ②

상 중 하 네트워크 보안 > 네트워크 활용(TCP/IP 구조)

40 웹 서버와 웹 브라우저 간에 통신 프로토콜은 무엇인가?

① Web Service
② SSL
③ HTTP
④ XML

웹 브라우저와 웹 서버 간의 통신 프로토콜은 개방형 표준인 HTTP를 사용한다.

정답 ③

3과목 애플리케이션 보안

상 중 하 애플리케이션 보안 > 인터넷 응용 보안

41 FTP에 대한 공격 유형의 종류로 틀린 것은 무엇인가?

① 무작위 공격
② Bounce 공격
③ Port Scanning
④ XSS

FTP 공격은 ID/Password 인증에서 Password에 대한 무작위 공격과 익명의 사용자를 이용한 Bounce Attack, 포트스캐닝 공격이 있으며 XSS는 웹 취약점을 이용한 공격 중 하나이다.

정답 ④

상 중 하 애플리케이션 보안 > 인터넷 응용 보안

42 FTP 보안 대책에 대한 설명으로 올바르지 않은 것은?

① TFTP는 인증 과정이 없으므로 사용을 지양해야 한다.
② 익명(Anonymous) 사용자를 제거해야 하고 익명의 사용자에 대한 쓰기 권한을 제한해야 한다.
③ ftpusers 파일에 FTP로 접근 가능한 FTP 사용자 정보를 등록한다.
④ FTP 데몬 기동 시 -l 옵션을 주어서 xferlog를 기록한다.

FTP 설정 파일 ftpusers 파일은 FTP 사용을 제한할 사용자 ID를 등록하는 것이다.

정답 ③

상 중 하 애플리케이션 보안 > 전자상거래 보안

43 다음 전자화폐 중 그 성격이 다른 하나는 무엇인가?

① Mondex
② E-Cash
③ Proton
④ Net Cash

Proton은 유럽에서 가장 활발히 사용되는 전자화폐로 실물화폐의 성격과 상품 구입 시 최소단위까지 분할, 세계 어느 곳으로도 화폐가치를 이전할 수 있는 특징을 가지고 있다. 본 문제는 어떤 기준으로 문제를 바라보느냐에 따라 답에 차이가 날 수 있다. 그러므로 수험생 여러분은 Proton이라는 것의 의미만 학습하기 바란다.

정답 ③

상 중 하 애플리케이션 보안 > 전자상거래 보안

44 인터넷상거래 시 물품 지급 이후 안전한 거래를 위해서 구매자가 물품을 받기 전까지 대금 지급을 유예하는 것은 무엇인가?

① Key Management
② Payment Gateway
③ Escrow Service
④ SET

Escrow Service는 인터넷에서 상품(Internet Market Place)을 구매할 경우 상품이 소비자에게 인도된 후에 결제대금을 지급하는 시스템이다. Payment Gateway는 카드결제 시 카드사를 대신해서 결제를 처리 해주는 결제대행 업체이며 KCP, LGUplus와 같은 회사이다.

정답 ③

상 중 하 애플리케이션 보안 > 인터넷 응용 보안

45 IMAP에 대한 설명으로 올바르지 않은 것은?

① 전자우편을 위한 전자우편 보안 프로토콜이다.
② MBox에서 메일을 읽어 수신자에게 전송한다.
③ 메일을 읽어도 MBOX에 남아 있다.
④ IMAP 143 Port, IMAP3 220 Port를 사용한다.

전자우편 보안 프로토콜은 PGP, PEM, S/MIME가 있고 POP3와 IMAP은 메일을 내려받을 때 사용되는 MDA(Mail Delivery Agent) 프로그램이다.

정답 ①

상 중 하 애플리케이션 보안 > 인터넷 응용 보안

46 악성 메일 탐지 방법으로 올바르지 않은 것은?

① SPF를 적용한다.
② 라우터에서 Class Policy을 적용한다.
③ Inflex로 첨부 파일을 필터링한다.
④ MTA 패턴을 사용한다.

라우터에서 Class Map은 QoS(Quality of Service) 명령어로 특정 프로토콜의 속도를 조절할 때 사용된다.

오답 피하기

Pop3 프로토콜에 대해서 최대 5M의 대역을 할당

```
config)# class-map match-all pop3
(config-cmap)# match access-group 101

(config)# policy-map cisco
(config)# class pop3
(config)# police flow 5000000 3000 conform-action transmit exceed-action drop
```

정답 ②

상 중 하 애플리케이션 보안 > 전자상거래 보안

47 SET에 대한 설명으로 올바르지 않은 것은?

① 인터넷상에서 신용카드에 대한 결제 처리를 위해서 사용되는 프로토콜이다.
② VISA와 MASTER 社가 개발한 지불 처리 프로토콜이다.
③ 카드 소유자 정보와 가맹점 정보를 통합하여 서명하기 때문에 지불 처리의 편의성이 향상된다.
④ 전자상거래 보안 프로토콜로 지불 처리와 보안 기능을 제공한다.

SET의 가장 중요한 특징은 가맹점 정보와 카드 소유자 정보를 분리해서 서명하는 이중서명(Dual Signature)이다.

정답 ③

상 중 하 애플리케이션 보안 > 전자상거래 보안

48 서명자가 서명한 내용을 알지 못하고 서명하는 것은 무엇인가?

① 이중서명
② 대리인 서명
③ 은닉서명
④ 그룹서명

은닉서명(Blind Signature)

- D.Chaum에 의해서 제안된 서명 방식이다.
- 서명자가 서명문 내용을 알지 못하는 상태에서 서명하는 것을 수식으로 표현한다.
- 서명문의 내용을 서명자로부터 숨기는 서명 방식으로 서명을 받는 사람의 신원과 서명문을 연결할 수 없으므로 익명성을 유지한다.
- 전자화폐에 사용된다.

정답 ③

상 중 하 애플리케이션 보안 > 인터넷 응용 보안

49 세션 하이재킹에 대한 설명으로 올바르지 않은 것은?

① 클라이언트와 서버 사이에서 TCP의 Sequence Number를 제어할 때 발생하는 보안 취약점이다.
② UDP 및 TCP에서 RST 패킷(Packet)을 전송하여 Sequence Number를 새로 생성하고 세션을 빼앗는 방법이다.
③ Non Blind Attack와 Blind Attack이 있다.
④ 클라이언트와 서버 간에 Established 상태 시 Sequence Number를 획득해야 하고 이를 위해서 스니핑을 수행한다.

- 세션 하이재킹(Session Hijacking)은 TCP의 세션을 갈취하는 것으로 UDP에서는 발생하지 않는다. UDP는 세션 자체가 존재하지 않기 때문이다.
- 세션 하이재킹은 세션을 가로채기 위해서 Sequence Number를 스니핑하고 RST(RESET) 명령을 보내서Sequence Number를 초기화하여 갈취하는 것이다.

정답 ②

상 중 하 정보보안 일반 > 암호학

50 WPKI 구성요소가 아닌 것은?

① SLC
② OCSP
③ ECC
④ VPN

WPKI(Wireless Public Key Infrastructure)는 인증서 유효성 검사를 위해서 SLC, OCSP 방식을 가지고 있으며, 암호화는 무선의 특성을 고려하여 ECC 기법을 사용한다.

정답 ④

상 중 하 정보보안 일반 > 암호학

51 암호화에 대한 설명으로 올바르지 않은 것은?

① 패스워드는 일방향(One way) 함수를 지원하는 해시함수로 암호화를 수행한다.
② 대칭키는 128Bit 이상의 블록 암호화 방식을 사용한다.
③ 해시함수는 256Bit 이상을 사용한다.
④ 비대칭키는 1024Bit 이상의 암호화를 수행한다.

비대칭키(공개키) 암호화 기법은 2048Bit 이상의 키(Key)를 사용한다.

정답 ④

상 중 하 애플리케이션 보안 > 인터넷 응용 보안

52 SSL 계층에 대한 설명으로 올바르지 않은 것은?

① Alert Protocol은 비정상적인 세션 종료 및 에러 발생 시 경고 메시지를 전송한다.
② Record Protocol 계층은 송수신되는 데이터에 대해서 암호화 및 복호화를 수행한다.
③ Handshaking 계층은 세션을 생성하고 웹 브라우저와 웹 서버 간에 암호화 방식 등을 결정한다.
④ Change Cipher 키 관리 Protocol은 사용할 인증 정보를 공유한다.

Change Cipher 키 관리 Protocol은 Handshaking Protocol에서 협의된 암호 알고리즘, 키 교환 알고리즘, MAC 암호화, 해시 알고리즘이 사용될 것을 웹 브라우저와 웹 서버에게 공지하는 역할이다.

정답 ④

상 중 하 애플리케이션 보안 > 인터넷 응용 보안

53 다음의 역할을 수행하는 SSL 메시지는 무엇인가?

웹 브라우저가 지원하는 암호 알고리즘, 키 교환 알고리즘, MAC 암호화, 해시 알고리즘을 전송한다.

① Client Hello
② Server Hello
③ Server Hello Done
④ Client Hello Done

Client Hello는 웹 브라우저가 지원하는 암호 알고리즘, 키 교환 알고리즘, MAC 암호화, 해시 알고리즘을 전송한다.

정답 ①

상 중 하 애플리케이션 보안 > 전자상거래 보안

54 신용카드 사기를 방지하기 위한 보안 코드로 올바르지 않은 것은?

① CSS
② CSC
③ CVV
④ CVC

CSS(Credit Scoring System)는 누적된 고객의 거래정보를 통계적으로 분석해서 고객의 신용도를 예측하는 개인 신용 평가 기법이다.

오답 피하기

- CSC(Card Security Code)는 신용카드, 체크카드, 직불카드 및 선불카드에서 물리적 카드를 제시하지 않고 거래를 할 수 있는 보안 코드로 신용카드 사기를 예방한다. CSC는 다른 이름으로 CVV(Card Verification Value), CVC(Card Verification Code)라고도 한다.
- 보안 CID는 안전한 인증 문자 서비스 제공을 위해서 메시지 착신 전환 방지를 수행한다.

정답 ①

상 중 하 애플리케이션 보안 > 인터넷 응용 보안

55 버퍼 오버플로(Buffer Overflow)에 대한 설명으로 올바르지 않은 것은?

① 할당된 버퍼 크기 이상으로 데이터가 삽입되면 다른 영역의 데이터까지 침범하는 취약점이다.
② 버퍼 오버플로를 방지하기 위해서 길이 제한이 존재하는 strcpy( )와 같은 함수를 사용해야 한다.
③ 버퍼 오버플로는 데이터를 복사할 때 다른 영역에 침범하지 않도록 경계검사를 수행해야 한다.
④ /etc/system 혹은 /etc/sysctl 설정 파일에서 버퍼 오버플로를 예방하기 위한 경계 검사를 수행한다.

문자열 길이를 제한해서 복사하는 함수는 strncpy( ) 이다.

정답 ②

상 중 하 애플리케이션 보안 > 전자상거래 보안

56 인터넷 표준인 XML을 기반으로 Web에서 사용하는 기술이 아닌 것은?

① UDDI
② WSDL
③ OCSP
④ SOAP

W3C 웹 서비스(Web Service) 표준 기술

표준기술	세부 내용
WSDL(Web Service Description Language)	서비스 제공자와 서비스 사용자 간의 웹 서비스 파라미터의 이름, 서비스가 위치한 URL 및 웹 서비스 호출에 관한 정보를 기술하는 표준
UDDI(Universal Description, Discovery and Integration)	서비스 제공자가 웹 서비스를 등록하고 서비스 사용자가 웹 서비스를 검색하기 위한 레지스트리
SOAP(Simple Object Access Protocol)	XML을 기반으로 하는 메시지 표준으로 서비스 사용자가 서비스 제공자에 의해서 노출한 웹 서비스를 호출하고 결과를 받기 위한 표준 프로토콜

정답 ③

상 중 하 애플리케이션 보안 > 데이터베이스 보안

57 MySQL 데이터베이스에서 사용하는 두 가지 인증 방법에 대한 설명이다. 그 내용으로 틀린 것은?

① 기본 인증은 윈도우 인증을 수행하면 자동으로 데이터베이스 인증도 완료된다.
② 기본 인증은 ID와 Password를 입력하여 데이터베이스와 연결을 수행한다.
③ 윈도우 인증과 관계없이 데이터베이스 연결에 대해서 별도의 인증을 받아야 한다.
④ 인증을 자동화하면 데이터베이스 취약점이 발생한다.

데이터베이스 인증을 위한 기본 인증은 데이터베이스 사용자 ID와 Password를 입력하여 정당한 사용자인지를 확인하는 방법이다. 윈도우 인증은 윈도우 시스템에 대한 인증이고 데이터베이스와는 별도의 인증이다.

정답 ①

상 중 하 애플리케이션 보안 > 인터넷 응용 보안

58 SSH 기능에 대한 설명으로 틀린 것은?

① 보안 기능을 제공한다.
② 인증 기능을 제공한다.
③ 패킷 필터링을 수행한다.
④ 전송 구간 암호화를 수행한다.

SSH는 원격 터미널 접속 시 암호화를 수행해서 안전성을 확보하는 것으로 패킷 필터링을 수행하지는 않는다.

정답 ③

상 중 하 애플리케이션 보안 > 전자상거래 보안

59 전자입찰 시스템에 대한 설명으로 틀린 것은 무엇인가?

① 기업 내 입찰 업무를 인터넷을 사용하여 전자서명한 후 검증하는 방식으로 처리하는 시스템이다.
② 입찰 시 견적서에 대한 전자서명 검증을 수행한다.
③ Paperless를 실현하여 입찰 과정의 업무 효율성을 증대했다.
④ 마감 서버가 여러 대 일 때는 순차적으로 마감한다.

전자입찰 시스템은 오프라인 입찰 업무를 인터넷을 사용해서 처리하는 시스템으로 견적 제출 시 전자서명된 암호문서를 관리하고 전자서명에 대한 검증을 수행한다.

정답 ④

상 중 하 애플리케이션 보안 > 전자상거래 보안

60 능동형 공격과 수동형 공격의 분류로 올바른 것은?

① 능동형 – 스니핑, 삭제
② 능동형 – 트로이목마, 도청
③ 수동형 – 스니핑, 도청
④ 수동형 – DDoS, 서비스 거부 공격

수동형 공격은 직접적인 피해를 발생시키지 않고 도청과 같은 스니핑을 수행하는 공격이고 능동형 공격은 직접적인 공격과 피해를 유발하는 공격이다.

정답 ③

4과목 정보보안 일반

상 중 하 정보보안 일반 > 암호화

61 다음은 RSA 공개키 암호화 알고리즘에 대한 설명이다. 올바른 것을 모두 고르시오.

가. Diffie-Hellman이 제안한 공개키 암호화 알고리즘이다.
나. 소인수분해의 수학적 기반의 공개키이다.
다. 안정성을 보장받기 위해서 소수 p, q 조건과 공개키 암호화 키와 비밀 복호화 키의 조건들이 부가적으로 필요하다.
라. 전사적 공격, 수학적 공격, 시간적 공격으로 공격할 수 있다.

① 가
② 가, 나
③ 나, 다
④ 나, 다, 라

RSA 공개키 암호화 알고리즘은 소인수를 이용한 암호화 방법이다. 소인수라는 것은 어떤 수를 소수의 곱으로 표현할 때 각각의 소수를 소인수라고 한다. 즉, 6의 값을 보면 6의 소수는 2, 3이 되며 그것 2×3=6이기 때문이다.

정답 ④

상 중 하 정보보안 일반 > 접근 통제

62 다음 중 접근 통제 모델에 대한 설명으로 올바르지 않은 것은?

① 비바(Biba) 모델 : 무결성에 기반을 둔 상태 머신 모델이다.
② 벨라파듈라(Bell-Lapadula) 모델 : 객체 무결성과 가용성 유지에 중점을 두고, 기밀성 측면에서는 대처하지 않는다.
③ 비바(Biba) 모델 : 은닉채널(Covert Channels)을 방지하며, 내부와 외부간의 객체의 일관성을 보호한다.
④ 클락앤윌슨(Clark and Wilson) 모델 : 인가된 사용자가 허가받지 않은 데이터의 수정을 방지 한다.

접근 통제 보안 모델(Access Control Model)

종류	설명
Bell-Lapadula	기밀성에 중점을 둔 가장 대표적인 모델
Biba	무결성에 중점(무결성의 대표적 모델)
Clark and Wilson	상업용 무결성에 중점
만리장성 모델	서로 상충관계에 있는 객체 간의 정보 접근을 통제하는 모델, 상업적 기밀성

정답 ②

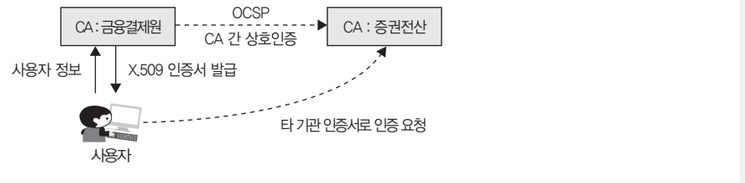
상 중 하 정보보안 일반 > 암호화

63 다음 중 OCSP(Online Certificate Status Protocol)에 대한 설명으로 틀린 것은?

① 실시간 인증서의 상태 프로토콜 인증서의 유효성을 검증할 수 있다.
② 비용 지불없이 사용할 수 있다.
③ OCSP 서버로부터 인증서 상태를 전달한다.
④ 인증서가 폐지되면 그 상태를 알 수 없다.

OCSP(Online Certificate Status Protocol)

은행에서 발급받은 인증서를 증권회사에 인증받기 위해서 인증기관 간의 상호인증을 수행하는 실시간 프로토콜이다.



정답 ④

상 중 하 정보보안 일반 > 암호학

64 다음 중 PKI(Public Key Infrastructure) 인증서 관리 구조 중 네트워크 구조에 대한 특징으로 옳지 않은 것은?

① 인증 경로 탐색이 쉽다.
② 상업적 상호 신뢰관계를 반영한다.
③ CA(Certification Authority) 개인키 손상에 대한 복구가 쉽다.
④ CA(Certification Authority)의 직접적 상호인증을 허용한다.

CA(Certification Authority)는 OCSP를 통해서 상호인증을 지원한다. 개인키 손상 시 복구가 아니라 재발급이 가능하다.

정답 ③

상 중 하 정보보안 일반 > 암호화

65 키 사전 분배에 대한 설명으로 옳지 않은 것은?

① TA(Trusted Authority)가 사전에 임의의 두 사용자(A, B)의 비밀 경로를 통하여 임의키를 선택하여 전달한다.
② TA(Trusted Authority)는 네트워크상에 모든 사용자와 필요할 때마다 사용하는 키 공유 방법이다.
③ TA(Trusted Authority)는 네트워크상에 모든 사용자 사이에 안전한 통로가 필요하다.
④ 사용자들이 많으면 많은 키 관리를 해야 하는 문제점이 발생한다.

키 분배(Key Distribution)는 암호화 키를 전송하는 과정으로 송신자와 수신자 간에 비밀키를 공유하기 위한 기술이다.
즉, 임의의 비밀 값을 생성하여 사용자에게 전송하고 전송된 데이터로 자신만의 공유키를 생성한다.

정답 ③

상 중 하 정보보안 일반 > 암호화

66 다음 괄호 안에 알맞은 것은?

공개키 알고리즘을 암호화 서비스와 전자서명 서비스에 제공할 때 암호화로 사용하는 키는 수신자의 ( )이고, 서명 검증에 사용하는 키는 송신자의 ( )이다.

① 개인키, 공개키
② 공개키, 공개키
③ 개인키, 개인키
④ 공개키, 개인키

전자서명에서 키 사용

구분	키(Key)	설명
송신자	개인키	전자서명
	공개키	전자서명 확인
수신자	개인키	복호화
	공개키	암호화

정답 ②

상 중 하 정보보안 일반 > 접근 권한

67 다음 중 접근 권한 관리에 대한 설명으로 틀린 것은?

① 최소한의 사람에게 유효기간을 명시한다.
② 유효기간의 자동연장을 허락하지 않는다.
③ 특별 권한은 need to know 원칙을 적용한다.
④ 원칙은 유효기간 전후 유예기간을 둘 수 없다.

접근 권한 관리에서 유효기간을 자동연장 할 수 있다.

정답 ②

상 중 하 정보보안 일반 > 암호화

68 다음 괄호 안에 들어갈 것을 나열한 것은?

전자상거래 등의 e-business 환경에서 유통되는 정보의 안전성과 신뢰성을 확보하기 위해 공개키 암호화 알고리즘과 인증서의 사용을 가능하게 해주는 새로운 기반 구조가 필요하 게되는데 이러한 공개키 암호화 기술을 지원하는 기반 구조인 ( )가있고, 이를 무선 환경으로 확장한 것이 ( )이다. 이 공개키 기반 구조에서 사용되는 인증서는 ITU-T에서 개발한 ( ) 형식을 사용한다.

① WPKI, PKI, X.500
② PKI, VPN, X.500
③ PKI, WPKI, X.501
④ PKI, WPKI, X.509

PKI, WPKI, X.509에 대한 설명이다.

정답 ②

상 중 하 정보보안 일반 > 접근 통제

69 물리적 접근 통제에 해당하지 않은 것은?

① 네트워크 장비들의 물리적 위치 분리
② 정보보안 정책 및 절차
③ 보안 구역의 분리
④ 도난, 파괴, 복제 금지

정보보안 정책 및 절차는 관리적 보안이다.

오답 피하기

물리적 접근 통제는 물리적 위치, 보안 구역, 도난, 파괴, 복제금지 등을 관리한다.

정답 ②

상 중 하 정보보안 일반 > 암호화

70 OTP(One Time Password) 시간 동기화에 대한 설명으로 옳지 않은 것은?

① 서버와 클라이언트 카운터 값은 동일하게 증가하며, 카운터 값과 입력 값은 OTP 생성 시 시간 동기화를 위하여 사용된다.
② 임의의 입력 값이 필요하지 않다.
③ 클라이언트가 현재 시각을 입력 값으로 OTP를 생성한다.
④ 클라이언트와 서버 시간 동기화가 정확하지 않을 시 인증에 실패한다.

시간 동기화 방식

- OTP 생성 매체가 매시간 비밀번호를 자동으로 생성하는 형태로 시간을 기준 값으로 하여 OTP 생성 매체와 OTP 인증 서버가 동기화된다.
- 시간을 입력 값으로 동기화하기 때문에 간편한 장점을 가지지만, 일정 시간 동안 은행에 OTP를 전송하지 못하면 다시 새로운 OTP가 생성될 때까지 기다려야 하는 문제점을 가진다.
- 이벤트 동기화 방식은 OTP 생성 매체와 인증 서버의 동기화된 인증 횟수를 기준 값으로 생성, OTP 생성 매체에서생성된 비밀번호 횟수와 인증 서버가 생성한 비밀번호 횟수가 자동으로 동기화되기 때문에 시간 동기화의 불편성을 완화한다.

오답 피하기

동기화 방식

- 사용자의 OTP 생성 매체와 은행의 OTP 인증 서버 사이에 동기화된 기준 값에 따라 OTP가 생성되는 방식이다.
- 동기화된 기준 값에 따라 시간 동기화(Time Synchronous) 방식과 이벤트 동기화(Event Synchronous) 방식으로 분류된다.

정답 ②

상 중 하 네트워크 보안 > 최신 네트워크 위협 및 대응 기술

71 다음이 설명하는 인증 기법에 해당하는 것은?

> IEEE 표준인증 기법으로 사용자 ID 인증 및 동적 키 관리 계정을 지원한다. PAP, CHAP, RAUDIUS, PEAP, WEP 등 프로토콜을 사용한다. 포트기반의 네트워크 접근 제어를 수행한다.

① IEEE 802.1x
② IEEE 802.11i
③ Wi-Fi Protected Access
④ Extensible Authentication Protocol

EAP(Extensible Authentication Protocol)는 WEP의 보안성을 높이기 위해서 사용자 인증 프로토콜로 스테이션 (Station)과 AP(Access Point) 간의 TK(Temporal Key)를 동적으로 생성하고 무선 구간에 암호화를 수행한다

정답 ④

상 중 하 정보보안 일반 > 암호화

72 다음 중 암호 부인방지 기능을 수행하지 않는 것은?

① RSA
② DSS
③ ECDH
④ ElGamal

ECDH(Elliptic curve Diffie-Hellman)는 대칭키 암호화 방법의 변종이며, 타원곡선 암호화 방법으로 키 교환을 위해서 사용한다.

정답 ③

73 BYOD(Bring Your Own Device)는 개인이 소유한 노트북, 스마트폰, 태블릿 등의 장비를 직장에서 업무용으로 사용하는 관리체계로 최근 확산되고 있다. 최근 인터넷상에 가상화된 개인 PC 환경을 구축하여 다양한 단말을 통해 언제 어디서나 업무 환경을 실현하는 가상 데스크톱 인프라 시스템의 도입이 증가하는 추세이다. 아래 보기에서 설명하는 기술에 해당하는 것은?

> 애플리케이션 데이터는 기업 데이터와 개인 데이터로 구분하여 관리할 수 있도록 애플리케이션 데이터를 패키징하는 기술이다.

① 모바일 가상화
② 컨테이너화
③ 하드웨어 가상화
④ MDM(Mobile Device Management)

컨테이너화는 업무용 앱과 개인용 앱을 분리하여 접속통제 등을 수행하고 데이터를 보호한다.

오답 피하기

모바일 가상화는 안드로이드 환경에서 보안, 취급성, 제어 능력을 향상시키기 위한 기능으로 운영체제를 이중으로 사용하는 방법이고 해커 및 악의적 공격에 보호하기 위해서 데이터 암호화를 기반으로 한 컨테이너화, 네트워크 보안 등의 기술이 필요하다.

정답 ②

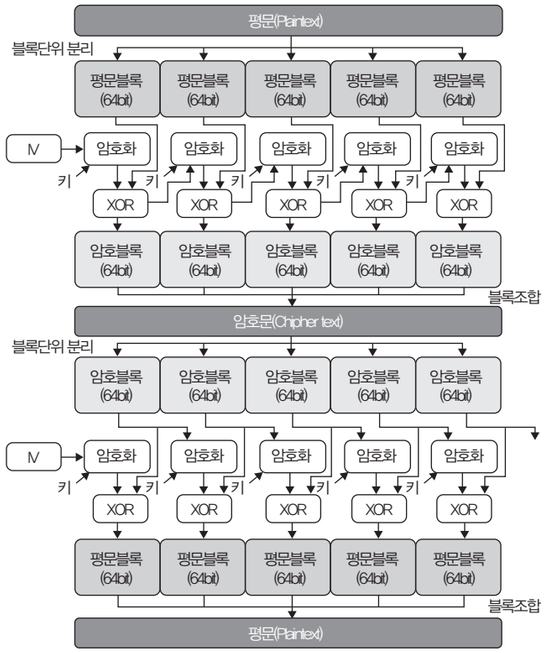
74 아래의 내용이 설명하는 블록 암호화 사용 방식에 해당하는 것은?

> • 초기화 벡터를 암호화한 값과 첫 번째 평문 블록을 XOR하여 암호문 블록을 생성한다. 다시 암호화한 값과 그 다음 평문블록을 XOR하여 암호문 블록을 반복 생성한다.
> • 암호화에서는 특정 입력이 이후에 영향을 미치게 되며, 복호화에서는 특정 암호문의 오류가 계속적으로 이후에 영향을 미치지 않는다는 특징을 가진다.

① 선택 평문 공격(Chosen Plaintext Attack)
② 암호화 피드백 모드(Cipher FeedBack Mode)
③ 출력 피드백 모드(Output FeedBack Mode)
④ 카운터 모드(CounTeR Mode)

암호화 피드백 모드(Cipher FeedBack Mode)

• CBC와 마찬가지로 IV가 사용되며, 암호화는 순차적으로 처리해야 하며 복호화는 병렬처리가 가능하다.
• CBC 모드, CFB 모드는 암호문 한 개의 블록에서 에러 발생 시 현재 복호화되는 평문블록과 다음 복호화되는 평문 블록에 영향을 준다.



정답 ②

상 중 하 정보보안 일반 > 보안 요소 기술

75 다음 중 Active Attack과 Passive Attack으로 올바르게 짝지어진 것은?

Active Attack	Passive Attack
① 트래픽 분석 공격	전송 파일 도청
② 재생 공격	메시지 변조
③ 삭제 공격	전송 파일 도청
④ 삽입 공격	삭제 공격

Passive Attack은 수동적 공격 혹은 소극적 공격이라고 하며 위변조와 같은 공격은 하지 않고 정보를 획득하기 위한 공격으로 스니핑이 가장 대표적이다. Active Attack은 적극적 공격 혹은 능동적 공격이라고 하고 위변조와 같은 직접 적인 공격을 수행한다.

정답 ③

상 중 하 정보보안 일반 > 암호학

76 블록 암호 알고리즘 구조에 대한 설명으로 적절한 것은?

① SPN 구조의 블록 암호 알고리즘은 암호호와 복호화 과정이 다르다.
② Feistel 구조의 블록 암호 알고리즘은 SPN보다 병렬성이 우수하다.
③ DES, RC5, AES는 SPN 구조를 대표한다.
④ Feistel 구조는 3라운드 이상이면 짝수 라운드로 구성한다.

SPN(Substitution Permutation Network)은 혼돈과 확산의 이론에 기반을 둔 구조로 암호화 과정과 복호화 과정이 다른 특성이 존재한다.

오답 피하기

Feistal 구조는 암호화와 복호화 과정이 동일한 것으로 역변환이 가능한 방법이며, 하드웨어 및 소프트웨어로 구현이 쉽다.

정답 ①

상 중 하 정보보안 일반 > 보안 요소 기술

77 다음 중 커버로스(Kerberose)에 대한 설명으로 옳지 않은 것은?

① 커버로스는 클라이언트와 서버의 응용 프로그램을 설계한다.
② 사용자 등록 과정에서 Kerberos 서버 사용자 사이에 키 협상 절차를 진행한다.
③ 무차별 대입 암호화 공격이 가능하다.
④ 서버를 사용자들의 비밀키와 아이디로 데이터베이스를 유지한다.

커버로스(Kerberos)는 클라이언트와 서버가 데이터를 암호화하기 위해 공유 대응키를 통해서 통신하고 키 협상 절차를 가지고 있다. 클라이언트는 두 개의 복제 세션키를 보내서 서버와 통신하는 클라이언트의 요청에 반응한다.

정답 ④

상 중 하 애플리케이션 보안 > 전자상거래 보안

78 다음 중 이중서명(Dual signature)에 대한 설명으로 틀린 것은?

① 카드 결제에서 계좌 정보 내 구매 프로필 목록을 방지하는 요소이다.
② 이중서명의 검증은 위변조 여부를 확인하지 않고 사용자 인증을 포함하지 않는다.
③ 판매자가 결제 정보를 위변조하는 것을 방지한다.
④ 이중서명의 검증은 판매자가 수행한다.

SET은 우리가 인터넷에서 물건을 구매할 때 사용하는 방법이다. 인터넷상에서 카드결제를 수행하면 LG uplus와 같은 PG(Payment Gateway)사가 Active X로 카드결제 프로그램을 기동시킨다. 그러면 사용자는 카드번호를 입력하고 결제를 의뢰한다. 그러면 SET은 이중서명 기능으로 카드 소유자 정보와 가맹점 정보를 분리해서 서명한 후 PG사에 보낸다. PG사는 신용카드 회사에 결제 승인을 요청하고 승인이 되면 결제는 완료된다. 이러한 구조에서 사용되는 보안 프로토콜이 바로 SET이다.

정답 ④

상 중 하 애플리케이션 보안 > 전자상거래 보안

79 다음이 설명하는 인증 기법은?

- 사용자가 ID를 서버 호스트에 전달하면, 서버 호스트는 난수를 생성하여 사용자에게 보낸다.
- 사용자는 서버 호스트에 등록된 사전 공유키를 사용하여 난수를 암호화해서 서버 호스트에 보낸다.
- 서버 호스트는 사용자 ID에 대응하는 사전 공유키를 사용하여 확인한다.

① OTP(One Time Password)
② Challenge Response
③ 시간 동기화(Time synchronization)
④ S/Key 일회용 패스워드

비동기 방식 : 질의응답(Challenge Response)

- 사용자의 OTP 생성 매체와 은행의 OTP 인증 서버 사이에 동기화되는 기준 값이 없으며 사용자가 직접 임의의 난수(질의값)를 OTP 생성 매체에 입력하여 OTP를 생성하는 방식이다.
- 사용자가 은행의 OTP 인증 서버로부터 받은 질의 값(Challenge)을 OTP 생성 매체에 직접 입력하면 응답 값(Response)이 생성된다.
- 사용자가 직접 OTP 생성 매체에 질의 값을 입력해야 응답 값인 OTP가 생성되기 때문에 전자금융 사고 발생 시 명백한 책임소재를 가릴 수 있고 보안성도 높은 방식이다.
- 직접 질의 값을 확인하여 OTP 생성 매체에 입력해야 하므로 은행이 별도의 질의 값을 관리해야 한다.

정답 ②

삼 중 하 정보보안 일반 > 암호화

80 암호 시스템의 안전성 유지 기반 이론이 같은 것끼리 짝지어진 것은?

가. RSA 암호화알고리즘
나. DSS 전자서명
다. Schnorr 서명
라. Rabin
마. ElGamal

① 가, 다 나, 라, 마
② 가, 라 나, 다, 마
③ 가, 다, 라, 나, 마
④ 가, 라, 마, 나, 다

- Rabin은 공용키 암호 방식의 하나로 2개 큰 소수 p, q의 곱 n=p−q를 계산하여 소인수 분해의 어려움을 근간으로 한다. 또한, RSA도 소인수 분해의 어려움을 근간으로 한다.
- DSS 전자서명은 미국 전자서명 표준으로 ElGamal 전자서명을 개량한 것이다.
- Schnorr 서명은 이산대수 문제의 안전성을 기반으로 하고 ElGamal도 이산대수를 기반으로 한다.

정답 ②

5과목 정보보안 관리 및 법규

삼 중 하 정보보안 관리 및 법규 > 정보보호 관리

81 다음 중 괄호 안에 들어갈 내용을 나열한 것은?

조직의 업무특성에 따라 정보자산 분류기준을 수립하고 정보보호 관리체계 범위 내 모든 정보자산을 (A)하여야 한다. 또한, 식별된 정보자산을 (B)으로 관리하여야 한다. 기밀성, 무결성, 가용성, 법적 요구사항 등을 고려하여 정보자산이 조직에 미치는 (C)를 평가하고 그 (C)에 따라 보안 등급을 부여하여야 한다.

① 식별, 목록, 중요도
② 식별, 목록, 가치
③ DOA 산정, 목록, 중요도
④ DOA 산정, 가치, 중요도

모든 자산을 식별하고 목록으로 관리한 후 중요도를 평가하여 보안 등급을 부여한다.

정답 ①

삼 중 하 정보보안 관리 및 법규 > 정보보호 관리

82 정보보호조직의 구성원 및 책임에 대한 설명으로 옳지 않은 것은?

① 최고경영자 : 조직의 규모, 업무 중요도 분석을 통해 개인정보보호 관리체계의 지속적인 운영이 가능하도록 개인정보보호 조직을 구성하고 개인정보보호 관리체계 운영 활동을 수행하는데 필요한 자원을 확보하여야 한다.
② 정보보호 관리자 : 정보보호정책 수립, 정보보호 위원회의 구성 및 운영, 위험분석 및 관리, 보안 사고 대응 및 복구 등의 정보보호에 관한 업무를 총괄 관리하여야 한다.
③ 데이터 관리자 : 정보 보안 분류 프로세스를 숙지하고 기본적인 문서 분류 기준을 사용하여 데이터의 도용 및 방지 등의 관리를 수행한다.
④ 정보보호 위원회 : 국가 및 지방자치단체, 개인정보보호단체 및 기관, 정보주체, 개인정보처리자는 정보주체의 피해 또는 권리침해에 대한 개인정보 분쟁 발생 시 조정하는 역할을 한다.

정보보호 위원회

개인정보보호와 관련된 정책, 제도개선, 권고 등에 대한 심의 의결과, 오 · 남용 감시, 이행실태 조사, 개선 방안 연구등을 독립적으로 수행한다.

정답 ④

삼 중 하 정보보안 관리 및 법규 > 정보보호 관리

83 다음 중 아래 보기에서 설명하는 것은 무엇인가?

보안 관리를 위한 관리 방향을 제시하고, 정보에 대한 보호를 지원하기 위해서 절대적으로 필요한 요소

① 정보보호 정책
② 정보보호 지침
③ 정보보호 절차
④ 정보보호 조직

정보보호 관리 체계

구분	설명
보안 정책	보안 관리를 위한 관리 방향을 제시하고, 정보에 대한 보호를 지원하기 위해서 절대적으로 필요한 요소
보안 지침	보안 정책에 근거하여 각 부서별, 담당자별로 지켜야 할 준수사항
보안 절차	보안 지침에 의거하여 보안의 적용에 대한 표준화된 순서
보안 조직	보안 정책에 의해서 보안을 관리할 조직을 구성하고, 보안 사고가 발생할 경우 신속하게 대응

정답 ①

상 중 하 정보보안 관리 및 법규 > 정보보호 관리

84 다음 중 정량적 분석과 정성적 분석으로 분류하여 올바르게 짝지어진 것은?

가. 자산의 교체비용
나. 업무기여도
다. 자산의 도입비용
라. 자산의 복구비용
마. 조직업무

	정량적 분석	정성적 분석
①	가, 나, 다	라, 마
②	나, 다, 라	가, 마
③	다, 라, 마	가, 나
④	가, 다, 라	나, 마

정량적 분석은 수치화를 통해서 분석하는 것이고 정성적 분석은 우선순위를 통해서 중요도를 산정하는 것이다.

정답 ④

상 중 하 정보보안 관리 및 법규 > 정보보호 관리

85 다음 지문이 설명하는 위험분석 기법에 해당하는 것은?

국내외 표준, 외국 컨설팅 업체의 기본 통제 등을 참조하는 위험관리 방법론으로써, 위험분석을 위한 자원이 필요하지 않고, 보호 대책 선택에 들어가는 시간과 노력이 줄어드는 장점이 있다. 만약 기업에서 선정한 기본 통제표준이 존재하고 조직의 시스템이 많은 경우 비용 대비 효과적인 선택이 될 것이다. 고려사항으로 기본적인 보호 대책이 너무 높게 설정되었다면 어떤 시스템에 대해서는 비용이 너무 많이 들고 너무 제한적이 되어 버리며 기본적인 보호 대책이 너무 낮게 설정되었다면 어떤 시스템에 대해서는 보안 결핍을 가져올 수 있다.

① 베이스라인 접근법
② 전문가 판단법
③ 상세위험분석
④ 복합적 접근법

주어진 보기의 설명은 정성적 위험분석 기법 중 베이스라인 접근법(기준선법)에 대한 설명이다.

오답 피하기

위험분석 기법	설명
기준선 접근법	• 모든 시스템에 대하여 보호의 기준 수준을 정하고 이를 달성하기 위하여 일련의 보호 대책을 선택 • 시간 및 비용이 적고 모든 조직에서 기본적으로 필요한 보호 대책 선택이 가능 • 조직의 특성을 고려하지 않기 때문에, 조직 내에 부서별로 적정 보안 수준보다도 높게 혹은 낮게 보안 통제를 적용
전문가 판단	• 정형화된 방법을 사용하지 않고 전문가의 지식과 경험에 따라서 위험을 분석 • 작은 조직에 비용 효과적이며, 구조화된 접근 방법이 없으므로 위험을 제대로 평가하기 어렵고 보호 대책의 선택 및 소요 비용을 합리적으로 도출하기 어려움 • 계속적으로 반복되는 보안 관리 및 보안 감시, 사후관리로 제한됨
상세위험분석	• 자산의 가치를 측정하고 자산에 대한 위협 정도와 취약점을 분석하여 위험 정도를 결정 • 조직 내에 적절한 보안수준 마련 가능 • 전문적인 지식과 노력이 많이 소요됨 • 정성적 분석 기법과 정량적 분석 기법이 존재함
복합적 접근법	• 먼저 조직 활동에 대한 필수적이고 위험이 높은 시스템을 식별하고 이러한 시스템은 상세위험분 석 기법을 적용 • 그렇지 않은 시스템은 기준선 접근법 등을 적용 • 보안전략을 빠르게 구축할 수 있고, 상대적으로 시간과 노력을 효율적으로 활용 가능 • 두 가지 방법의 적용 대상을 명확하게 설정하지 못함으로써 자원이 낭비될 수 있음

정답 ①

상 중 하 정보보안 관리 및 법규 > 정보보호 관리

86 다음 중 정보보호 관리체계(ISMS, Information Security Management System) 내의 인증 체계 중 정보보호 관리 과정의 단계별 절차에 대한 설명으로 옳은 것은?

① 정보보호정책 수립 및 범위설정 → 경영진 책임 및 조직구성 → 위험관리 → 정보보호대책 구현 → 사후관리
② 정보보호정책 수립 → 범위설정 → 경영진 책임 및 조직구성 → 위험관리 → 정보보호대책 구현 → 사후관리
③ 정보보호정책 수립 및 범위설정 → 위험관리 → 경영진 책임 및 조직구성 → 사후관리 → 정보보호대책 구현
④ 정보보호정책 수립 → 범위설정 → 경영진 책임 및 조직구성 → 위험관리 → 정보보호대책 → 사후관리

ISMS의 정보보호 관리 과정

관리 과정	특징	관련 문서
정보보호정책 수립 및 범위설정	• 조직 전반에 걸친 상위 수준의 정보보호정책 수립 • 정보보호 관리체계 범위 설정	• 정보보호정책서 • 정보보호 관리체계 범위서 • 정보자산 목록(정보통신설비 목록) • 네트워크 및 시스템 구성도
경영진 책임 및 조직 구성	• 정보보호를 수행하기 위한 조직 내 각 부문 의 책임 설정 • 경영진 참여할 수 있도록 보고 및 의사결정 체계 구축	정보보호조직도
위험관리	• 위험관리 방법 및 계획 수립 • 위험 식별 및 위험도 평가 • 정보보호대책 선정 • 구현 계획 수립	• 위험관리지침서 • (○○년) 위험관리 계획서 • 위험분석 · 평가 보고서
정보보호 대책 구현	• 정보보호대책 구현 및 이행 확인 • 내부 공유 및 교육	• 정보보호대책 명세서 • 정보보호계획서 • 정보보호계획 이행결과 보고서
사후관리	• 법적 요구사항 준수 검토 • 정보보호 관리체계 운영 현황 관리 • 정기적인 내부감사를 통해 정책 준수 확인	• 정보보호 관리체계, 내부감사보고서 • 정보보호 관리체계, 운영현황표

정답 ①

87 다음 중 개인정보보호법상 제 3자의 동의 없이 수집 • 이용되는 경우에 해당되는 것은?

① 경품당첨 후 참여할 수 없는 불이익 발생한 경우
② 정당한 이익을 달성하기 위하여 명백히 정보주체에 필요하다고 인정하는 경우
③ 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 정보주체 권리보다 우선한 경우
④ 정보주체와의 계약 체결 및 이행이 불가피하게 필요한 경우

개인정보보호법상 제 3자의 동의없이 수집 · 이용되는 경우에 해당하는 경우는 보기 ③이 명백하고 나머지 보기는 논란이 있다.
보기 ① 경품당첨 후 참여할 수 없는 불이익 발생한 경우 → 제15조 제 1항 제6호, 제3자 제공 사유에 해당 안 됨
보기 ② 정당한 이익을 달성하기 위하여 명백히 정보주체에 필요하다고 인정하는 경우
→ 제15조 제 1항 제6호, 제3자 제공 사유에 해당안 됨
보기 ④ 정보주체와의 계약 체결 및 이행이 불가피하게 필요한 경우
→ 제15조 제 1항 제4호, 제3자 제공 사유에 해당안 됨
개인정보보호법 제17조 (개인정보의 제공) 제1항에 따라 아래와 같은 경우에 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다.
1. 정보주체의 동의를 받은 경우
2. 제15조제1항의 제2호 · 제3호 및 제5호에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우
→ 제15조 제1항 제2호 · 제3호 및 제5호에 따른 개인정보제공이 가능한 경우

1. 정보주체의 동의를 받은 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
4. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

정답 ③

88 다음 중 아래에서 설명하는 기관에 해당하는 것은 무엇인가?

- 금융 통신 등 분야별 정보통신기반 시설을 보호하기 위한 구축운영
- 취약점 및 침해 요인과 대응 방안에 관한 정보 제공
- 정보통신망 침해사고의 처리 · 원인분석 및 대응체계 운영

① 정보공유분석센터
② 한국인터넷진흥원
③ 정보보호 관리기관
④ 지식정보보안 컨설팅 업체

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제52조에서 규정한 한국인터넷진흥원의 역할

1. 정보통신망의 이용 및 보호, 방송통신과 관련한 국제협력 · 국외진출 등을 위한 법 · 정책 및 제도의 조사 · 연구
2. 정보통신망의 이용 및 보호와 관련한 통계의 조사 · 분석
3. 정보통신망의 이용에 따른 역기능 분석 및 대책 연구
4. 정보통신망의 이용 및 보호를 위한 홍보 및 교육 · 훈련
5. 정보통신망의 정보보호 및 인터넷 주소 자원 관련 기술 개발 및 표준화
6. 정보보호산업 정책 지원 및 관련 기술 개발과 인력양성
7. 정보보호 관리체계의 인증, 정보보호시스템 평가 · 인증 등 정보보호 인증 · 평가 등의 실시 및 지원
8. 개인정보보호를 위한 대책의 연구 및 보호기술의 개발 · 보급 지원
9. 분쟁조정위원회의 운영 지원과 개인정보침해 신고센터의 운영
10. 광고성 정보 전송 및 인터넷광고와 관련한 고충의 상담 · 처리
11. 정보통신망 침해사고의 처리 · 원인분석 및 대응체계 운영
12. 「전자서명법」 제25조 제1항에 따른 전자서명인증관리
13. 인터넷의 효율적 운영과 이용 활성화를 위한 지원
14. 인터넷 이용자의 저장 정보보호 지원
15. 인터넷 관련 서비스 정책 지원
16. 인터넷상에서의 이용자 보호 및 건전 정보 유통 확산 지원
17. 「인터넷 주소 자원에 관한 법률」에 따른 인터넷 주소 자원의 관리에 관한 업무
18. 「인터넷 주소 자원에 관한 법률」 제16조에 따른 인터넷 주소분쟁조정위원회의 운영 지원
19. 「정보보호산업의 진흥에 관한 법률」 제25조 제7항에 따른 조정위원회의 운영 지원

정답 ②

89 다음 중 개인정보관리책임자의 지정 시 적합하지 않은 것은?

① 개인정보와 관련하여 이용자의 고충처리를 담당하는 부서의 장
② 사업주 또는 대표자
③ 5명 미만은 임명하지 않아도 됨
④ 임원급을 원칙으로 하되, 개인정보에 대한 전문성이 뛰어난 직원을 개인정보관리책임자로 지정할 수 있음

상시 종업원 수가 5명 미만으로 전년도 말 기준으로 직전 3개월간의 일일 평균 이용자가 1천 명 이하인 경우 별도의 개인정보관리책임자를 지정하지 않아도 되고 사업주 또는 대표자가 개인정보관리책임자가 된다.

오답 피하기

사업자는 소비자의 개인정보를 보호하고 개인정보와 관련한 소비자의 고충처리를 위해 개인정보책임자를 지정해야 한다. 고충을 처리하는 부서의 장을 부서장으로 할 수 있지만, 법률적 요건을 만족해야 한다. 즉, 회사의 임원과 사용자고충처리 담당 부서장이다. 임원이란 기업의 이사회를 구성하여 회사의 업무를 수행하고 그에 대해 책임을 지는 대표이사, 이사 및 감사를 지칭한다.

정답 ③

90 개인정보보호법에서 개인정보보호원칙에 대한 부적절한 설명은 무엇인가?

① 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.
② 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.
③ 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.
④ 개인정보 처리 시 실명 처리를 원칙으로 한다.

개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다.

오답 피하기

개인정보보호법 제3조(개인정보보호원칙)

1. 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.
2. 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.
3. 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.
4. 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.
5. 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.
6. 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.
7. 개인정보처리자는 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다.
8. 개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

정답 ④

상 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

91 다음 중 개인정보의 파기 및 보존에 대한 설명으로 틀린 것은?

① 개인정보처리자는 보유 기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때는 바로 그 개인정보를 파기하여야 한다.
② 개인정보를 파기할 때는 복구 또는 재생되지 아니하도록 조치하여야 한다.
③ 개인정보 이용 후 혹시 모를 경우 일정 기간 보관한다.
④ 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장 · 관리하여야 한다.

개인정보보호법 제21조(개인정보의 파기)

1. 개인정보처리자는 보유 기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때는 바로 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.
2. 개인정보처리자가 제1항에 따라 개인정보를 파기할 때는 복구 또는 재생되지 아니하도록 조치하여야 한다.
3. 개인정보처리자가 제1항 단서에 따라 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장 · 관리하여야 한다.
4. 개인정보의 파기 방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.
   ① 개인정보처리자는 법 제21조에 따라 개인정보를 파기할 때는 다음 각호의 구분에 따른 방법으로 하여야 한다.
      가. 전자적 파일 형태인 경우 : 복원이 불가능한 방법으로 영구 삭제
      나. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록 매체인 경우 : 파쇄 또는 소각
   ② 제1항에 따른 개인정보의 안전한 파기에 관한 세부 사항은 행정자치부장관이 정하여 고시한다.

정답 ③

상 중 하 정보보안 관리 및 법규 > 정보보호 관리

92 다음 중 BCP(Business Continuity Planning)의 6단계 절차를 순서대로 짝지은 것에 해당하는 것은?

ㄱ) 자산의중요도결정
ㄴ) 재난정책수립
ㄷ) 발생가능한재난의위험분석
ㄹ) 재난피해대책수립
ㅁ) 사업상중대업무규정
ㅂ) 테스트및수정

① ㄱ → ㄴ → ㄷ → ㄹ → ㅁ → ㅂ
② ㄴ → ㅁ → ㄱ → ㄷ → ㄹ → ㅂ
③ ㄱ → ㄷ → ㄹ → ㄴ → ㅂ → ㅁ
④ ㄱ → ㄷ → ㄹ → ㄴ → ㅂ → ㅁ

BCP는 비즈니스 연속성을 확보하기 위한 계획으로 기업 업무를 분석 및 정책을 수립하여 중요도 업무를 식별하고 중요 업무가 사용하는 자산의 중요도를 결정한다. 그리고 위험분석을 수행 후 각 위험에 따른 대책을 구현한다.

정답 ②

상 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

93 다음 중 괄호 안에 들어갈 것으로 적합한 것은?

전자문서란 컴퓨터 등 정보처리 능력을 갖춘 장치에 의하여 (A)적인 형태로 작성되어 송수신되거나 저장된 문서 형식의 자료로써 (B)된 것을 말한다.

A B
① 전기, 표준화
② 전기, 형식화
③ 전자, 표준화
④ 전자, 형식화

전자문서란 컴퓨터 등 정보처리 능력을 갖춘 장치에 의하여 **전자**적인 형태로 작성되어 송수신되거나 저장된 문서 형식의 자료로써 **표준화**된 것을 말한다.

정답 ③

상 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

94 개인정보보호법에서 제3자에게 제공할 때, 이용자에게 알려야 하는 정보에 해당하지 않는 것은?

① 개인정보 제공 계약의 내용
② 개인정보를 제공받는 자의 개인정보 이용목적
③ 제공하는 개인정보의 항목
④ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간

개인정보보호법 제17조

1. 개인정보처리자는 다음 각호의 어느 하나에 해당하는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다.
   ① 정보주체의 동의를 받은 경우
   ② 제15조 제1항 제2호 · 제3호 및 제5호에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우
2. 개인정보처리자는 제1항 제1호에 따른 동의를 받을 때는 다음 각호의 사항을 정보주체에게 알려야 한다. 다음 각호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.
   ① 개인정보를 제공받는 자
   ② 개인정보를 제공받는 자의 개인정보 이용 목적
   ③ 제공하는 개인정보의 항목
   ④ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
   ⑤ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

정답 ①

삼 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

95 다음 중 전자서명법에서 제시된 정의에 해당하지 않은 것은?

① 전자서명 : 서명자를 확인하고 서명자가 당해 전자문서에 서명을 하였음을 나타내는 데 이용하기 위하여 당해 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다.
② 전자서명 생성 정보 : 전자서명을 검증하기 위하여 이용하는 전자적 정보이다.
③ 서명자 : 전자서명 생성 정보를 보유하고 자신이 직접 또는 타인을 대리하여 서명을 하는 자이다.
④ 인증서 : 전자서명 생성 정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적정보이다.

- 전자서명 생성 정보 : 전자서명을 **생성**하기 위하여 이용하는 전자적 정보이다.
- 전자서명 검증 정보 : 전자서명을 **검증**하기 위하여 이용하는 전자적 정보이다.

정답 ②

삼 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

96 다음 중 외주 및 협력업체에 대한 인력보안에 대한 설명으로 부적절한 것은?

① 외부 위탁용역 및 협력업체 인력 계약 시 보안 관련 사항을 포함한다.
② 내부 직원과 동일한 수준으로 정보보호 정책을 준수해야 한다.
③ 외주 인력에게 회사의 중요 정보 접근을 허용하는 경우 한시적이고 제한적으로 허용하고 주기적인 점검이 이루어져야 한다.
④ 업무상 필요에 의해 협력업체 직원에게 정보시스템에 대한 접속 및 외부로의 접속을 요구하는 경우 협력업체 책임자의 승인이 필요하다.

내부 직원의 보안 정책과 협력업체 직원의 보안 정책은 다르게 관리되어야 한다

정답 ②

삼 중 하 정보보안 관리 및 법규 > 정보보호 관리

97 다음 지문이 설명하는 역할을 수행하는 사람에 해당하는 것은?

- 정보보호 정책의 수립 및 총괄 조정 승인
- 위험분석 관리 및 침해사고 예방 및 대응
- 정보보호 관련 규정 준수 관리 감독 및 효과적인 보고 절차의 수립 이행
- 보안 의식 강화 교육 및 훈련 프로그램을 위한 전략 수립 및 예산 확보
- 최고경영자, 경영진, 정보시스템 관리자 및 기업 내 중요 인적 자원들이 보안 의식 강화 및 교육 프로그램의 기본 개념과 전략을 이해하도록 보장하고 해당 프로그램의 실행 및 진행 과정을 통지
- 개인정보처리와 관련된 모든 구성원에 대한 기본적인 보안 책임 및 준수와 관련된 교육 자료 개발 및 교육

① 정보보호최고책임자
② 개인정보최고책임자
③ 개인정보관리자
④ 개인정보보호위원회

위에 제시된 역할을 수행하는 자는 정보보호 최고책임자에 대한 설명이다.

오답 피하기

개인정보보호법 제31조(개인정보보호책임자의 지정)

1. 개인정보보호계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오용 · 남용 방지를 위한 내부통제 시스템의 구축
5. 개인정보보호교육계획의 수립 및 시행
6. 개인정보 파일의 보호 및 관리 · 감독

정답 ①

상 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

98 다음 보기의 기능을 수행하고 있는 기관에 해당하는 것은?

- 개인정보보호에관한사항을심의 · 의결하기위하여대통령소속
- 개인정보침해요인평가에관한사항
- 개인정보보호기본계획및시행계획에대한심의 · 의결거쳐시행
- 개인정보보호와관련된정책, 제도및법령의개선에관한사항
- 개인정보의처리에관한공공기관간의의견조정에관한사항
- 개인정보보호에관한법령의해석 · 운용에관한사항
- 개인정보의이용 · 제공에관한사항
- 영향평가결과에관한사항
- 의견제시에관한사항
- 조치의권고에관한사항
- 처리결과의공표에관한사항

① 개인정보보호위원회
② 개인정보분쟁조정위원회
③ 개인정보보호협회
④ 명예훼손 분쟁조정

개인정보보호위원회는 개인정보보호 관련 정책과 제도 · 법령의 개선 등을 심의 · 의결하고 개인정보 처리에 관한 공공 기관과의 의견을 조정하며 정부부처, 지방자치단체, 헌법기관 등의 개인정보 침해행위의 시정 · 개선을 권고하기 위하여 설립된 대통령 소속기관이다. 개인정보보호위원회 위원장(비상임)은 대통령이 위원 중에서 공무원이 아닌 사람으로 위촉하고 장관급 예우를 받으며, 나머지 위원 14인 중 상임위원 1인은 차관급 정무직공무원으로 보한다. 위원장과 위원의 임기는 3년으로 하되, 1차에 한하여 연임할 수 있다. 위원장을 포함한 15인의 위원 중 5인은 대통령이 지명하고 5인은 국회에서 선출하며, 나머지 5인은 대법원장이 지명한다.

정답 ①

상 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

99 다음이 설명하는 개인정보처리 시 법률적 명칭에 해당하는 것은?

1. 개인정보의처리목적
2. 개인정보의처리및보유기간
3. 개인정보의제3자제공에관한사항
4. 개인정보처리의위탁에관한사항
5. 정보주체의권리 · 의무및그행사방법에관한사항
6. 그밖에개인정보의처리에관하여대통령령으로정한사항
   - 처리하는개인정보의항목
   - 개인정보의파기에관한사항
   - 개인정보의안전성확보조치에관한사항

① 개인정보보호 정책
② 표준 개인정보보호 지침
③ 개인정보보호 지침
④ 개인정보처리 방침

개인정보 처리 방침이라는 것은 개인정보의 처리목적, 처리 및 보유기간, 제3자 제공 등을 문서화한 것이다.

정답 ④

상 중 하 정보보안 관리 및 법규 > 정보보호 관리

100 다음 중 위험분석 방법에 대한 설명으로 틀린 것은?

① 과거 자료 분석법 : 과거 자료가 많을수록 분석의 정확도가 높아진다. 과거에 일어났던 사건이 미래에도 일어난다는 가정이 필요하며 과거의 사건 중 발생 빈도가 낮은 자료에 대해서는 적용이 어렵다.
② 확률 분포법 : 미지의 사건을 추정하는 데 사용되는 방법이다. 미지의 사건을 확률적(통계적) 편차를 이용하여 최저, 보통, 최고의 위험평가를 예측할 수 있다(정확성이 낮다).
③ 시나리오법 : 어떤 사건도 기대대로 발생하지 않는다는 사실에 근거하여 일정 조건하에서 위협에 대한 발생 가능한 결과들을 추정하는 방법이다.
④ 순위 결정법 : 시스템에 관한 전문적인 지식을 갖춘 전문가의 집단을 구성하고 위험을 분석 및 평가하여 정보시스템이 직면한 다양한 위협과 취약성을 토론을 통해 분석하는 방법이다.

④에 대한 설명은 순위 결정법이 아니라 전문가 판단법에 대한 설명이다

정답 ④