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

1과목 시스템 보안

상 중 하 시스템 보안 > 운영체제 구조

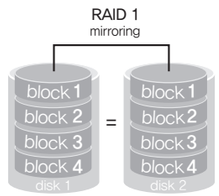
01 다음 중 RAID 레벨에 대한 설명으로 올바른 것을 고르시오.

- (ㄱ) : 저장되는 데이터를 동일한 디스크에 미러링(Mirroring)을 수행한다.
- (ㄴ) : 패리티 비트를 분산하여 저장한다.

(ㄱ)	(ㄴ)
① RAID 0	RAID 1
② RAID 0	RAID 4
③ RAID 1	RAID 5
④ RAID 1	RAID 6

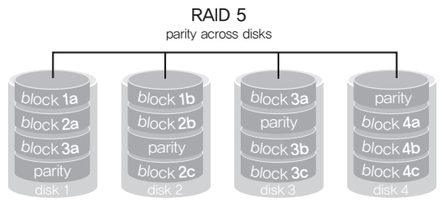
RAID 1 (Mirroring)

디스크 미러링(Disk Mirroring)은 여러 디스크에 데이터를 완전 이중화하여 저장하는 방식이다. RAID에서 가장 좋은 방식이지만 비용이 많이 발생한다. 디스크 미러링 방식은 디스크 장애 시 복구가 가능하며 디스크 Read와 Write가 병렬적으로 실행되어서 속도가 빠르다는 장점을 가진다.



RAID 5 (Parity ECC, Parity 분산 저장)

분산 패리티(Parity)를 구현하여 안정성이 향상되었으며, 최소 3개의 디스크가 요구된다(일반적으로는 4개로 구성).



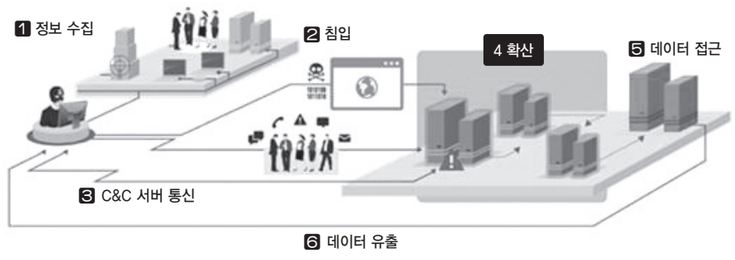
정답 ③

상 중 하 시스템 보안 > 윈도우 클라이언트 및 서버 보안

02 다음은 APT 공격절차이다. 가장 올바른 것은 무엇인가?

① 수집, 확산, 유출, 침투
② 침투, 확산, 유출, 수집
③ 수집, 침투, 확산, 유출
④ 수집, 확산, 침투, 유출

APT 공격단계는 수집, 침투, 확산, 유출단계이고 본 문제는 실기에도 자주 출제되므로 암기하기 바란다.



정답 ③

상 중 하 시스템 보안 > 윈도우 클라이언트 및 서버 보안

03 다음은 랜섬웨어 예방방법에 대한 설명이다. 가장 바르지 않은 것은?

① 랜섬과 소프트웨어의 합성어이다.
② 랜섬웨어를 예방하기 위해서 스마트카드의 데이터를 SD 카드에 저장한다.
③ 문서를 암호화하여 경제적 이득을 취한다.
④ 랜섬웨어 방법으로 크립토락커가 있다.

랜섬(Ransom, 몸값)과 ware(제품, 소프트웨어)의 합성어로 사용자의 문서를 인질로 돈을 요구하는 공격방법이다.
크립토락커(Cryptolocker)는 2013년 확산된 것으로 인질형 악성코드로 랜섬웨어이다. 즉, RSA, AES로 사용자의 문서를 암호화 시켜서 돈을 요구했다.
SD 카드에 사용자 정보를 저장해도 랜섬웨어는 모든 파일(오피스, 이미지 등)을 암호화 시킨다.

정답 ②

상 중 하 시스템 보안 > 리눅스 서버 보안

04 다음은 리눅스 명령을 실행한 결과이다. 그 내용으로 틀린 것은 무엇인가?

```
디렉터리명      권한
testuser1   rwxr-xr-x
testuser2   rwxr-xr-
testuser3   rwxr-xr-x
```

① ls testuser1
② cd testuser1
③ cd testuser2
④ ls testuser3

본 문제의 핵심은 다른 사용자(Other User)에 실행 권한이 있어야 해당 디렉터리로 이동할 수 있다는 것이다. 또한 본 문제는 제7회 정보보안산업기사에도 출제되었다. 정보보안산업기사에서는 맞는 것을 찾는 문제가 출제되었으며, 그 내용은 다른 사용자에게 Read 권한이 있다는 것이었다.

정답 ③

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

05 iptables로 192.168.1.100 IP 주소에 Port 21번 TCP를 차단하려고 한다. 다음 중 올바른 것은 무엇인가?

```
iptables -A INPUT( )  192.168.1.100 ( ) tcp ( ) 21 -j DROP
```

① -p -s --dport
② -s -p --dport
③ -d -p --dport
④ -i -p -dport

iptables에서 -s 옵션은 출발지 IP 주소, --dport는 포트 번호를 지정한다. 그리고 -p는 프로토콜이다.

• iptable
  – 패킷 필터링 도구로서 방화벽 또는 NAT에 사용된다.
• iptables 형식
  – iptables [룰] [프로토콜] [-j 허용, 거부]
• 옵션
  – 룰
  – A(--append) : 규칙을 추가함
  – INPUT : 로컬로 들어오는 패킷(입력 패킷)
  – FORWARD : INPUT과 OUTPUT 역할, 라우터에 방화벽을 적용할 때 쓰임
  – OUTPUT : 외부로 나가는 패킷(출력 패킷)
  – N(--new-chain) : 새로운 체인 생성
  – X(--delete-chain) : 체인 제거
  – P(--policy) : 체인 기본 정책 변경
  – L(--list) : 체인의 규칙상태 보기
  – F(--flush) : 체인 내의 모든 규칙 제거(방화벽 초기화)
  – Z(--zero) : 체인 내의 모든 규칙의 패킷과 바이트의 카운트를 0으로 초기화
  – D(--delete) : 규칙을 삭제
  – R(--replace) : 새로운 규칙으로 대체
  – I(--insert) : 체인의 가장 처음에 규칙을 추가
  – E(--rename-chain) : 체인의 이름을 변경
  – s : 출발지 IP
  – d : 목적지 IP
  – 프로토콜 : 각종 프로토콜을 명시함. icmp, tcp, udp 등
  – m : match를 정의. 프로토콜에 대한 특정 패킷에 대한 match
  – -dpot : 목적지의 포트를 허용하지 않음
  – j : 허용, 거부
-ACCEPT : 패킷을 허용
-DROP : 패킷을 허용하지 않으며, 허용하지 않는 메시지를 보내지 않음
  예 -A INPUT 0.0.0.0/0.0.00 -d 0.0.0.0/0.0.0.0 -p tcp -m --dport 80 -j DROP
  들어오는 모든 패킷 중 80번 포트(웹)를 이용하는 패킷은 모두 허용하지 않음

정답 ③

상 중 하 시스템 보안 > 리눅스 서버 보안

06 다음 도구 중에서 취약점 점검 도구와 거리가 먼 것은?

① SAINT
② COPS
③ NMAP
④ Tripwire

tripwire는 무결성 검사 도구이다.

보안점검 도구

도구	설명
SAINT	• 유닉스 시스템에서 작동하는 네트워크 취약점 분석 도구 • HTML 형식의 보고서 기능, 원격 취약점 점검 기능이 있음
SARA	• SATAN을 기반으로 개발된 취약점 분석 도구 • 유닉스 시스템에서 작동하며 네트워크 기반의 컴퓨터, 서버, 라우터, IDS에 대한 취약점 분석 가능 • HTML 형식의 보고서 기능이 있음
COPS	• 유닉스 시스템에서 동작하는 시스템 취약성 점검 도구 • 시스템 내부의 취약성(취약한 패스워드 체크 등) 기능이 있음
Nessus	• 유닉스 시스템에서 동작(Nessus 클라이언트는 윈도우에 설치 가능)하는 네트워크 취약점 점검 도구 • 클라이언트/서버 구조로 클라이언트의 취약점을 점검 • 약 600여 개 이상의 보안 취약점 점검 가능
NMAP	• 대표적인 포트 스캐닝 도구 • TCP connection으로 스캔뿐만 아니라 다양한 스텔스 모드로 스캔이 가능하며, 하나의 호스트뿐만 아니라 거대 네트워크의 고속 스캔도 가능

정답 ④

상 중 하 시스템 보안 > 리눅스 서버 보안

07 리눅스 커널에 내장되어 있는 Rule 기반 필터링, Connection Tracking, NAT 기능, 패킷 레벨 로깅을 제공하는 것은?

① TCP Wrapper
② netcat
③ iptables
④ xinetd

iptables는 패킷 필터링 도구로서 방화벽 또는 NAT에 사용된다.

정답 ③

상 중 하 시스템 보안 > 리눅스 서버 보안

08 재귀함수가 무한 반복될 경우 메모리의 어느 영역에 문제가 발생하는가?

① Code
② Text
③ Heap
④ Stack

Buffer Overflow는 지정된 메모리의 양보다 더 많은 양의 데이터를 쓰려는 경우 발생한다. 프로세스에서 Buffer Overflow는 Stack Buffer Overflow와 Heap Buffer Overflow가 있다. **Stack Buffer Overflow는 스택영역에 할당된 버퍼에 크기를 초과하는 데이터를 기록하고 저장된 복귀주소를 변경함으로써 임의의 코드를 실행**한다. **Heap Buffer Overflow는 힙 영역에 할당된 버퍼 크기를 초과하는 데이터를 기록하거나 저장된 데이터 및 함수의 주소를 변경하여 임의의 코드를 실행**하게 한다. 이러한 Buffer Overflow 대응방법은 **strcat, strcpy, gets, scanf, sscanf 등과 같은 취약한 함수를 사용하지 않는 방법**, 운영체제의 Buffer Overflow 취약점에 대응하기 위해서 커널 패치, 경계검사를 하는 컴파일러 및 링크 사용 등이 있다.

정답 ④

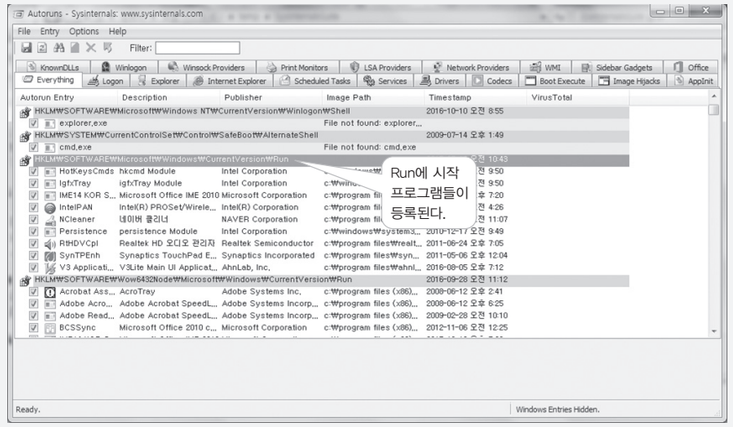
상 중 하 시스템 보안 > 윈도우 클라이언트 및 서버 보안

09 윈도우 시스템이 악성코드에 감염된 것으로 의심될 때 윈도우 부팅 시 자동 실행을 수행하는 레지스트리는 무엇인가?

① HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\AutoShareServer
② HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\NullSession
③ HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictanonymous
④ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVision\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVision\Run은 부팅 시 시작되는 프로그램이 등록된 것이다.

Autoruns 도구를 사용한 시작 프로그램 확인



정답 ④

상 중 하 시스템 보안 > 운영체제 이해 및 관리

10 다음에서 설명하는 프로세스 간 통신 기법은 무엇인가?

프로세스 간에 데이터를 송신할 때 선입선출 방법을 통하여 프로세스 간 통신을 수행한다.

① Pipe
② Socket
③ Message Queue
④ Shared Memory

선입선출을 기반으로 프로세스 간의 통신을 수행하는 것은 메시지 큐이다.

정답 ③

상 중 하 시스템 보안 > 윈도우 클라이언트 및 서버 보안

11 윈도우 시스템은 기본적인 공유를 가지고 있다. 기본 공유 중에서 admin$의 공유를 제거하는 명령으로 올바른 것을 고르시오.

① net share admin$ /del
② net share admin$ /delete
③ net user admin$ /del
④ net user admin$ /delete

net share <공유 폴더명> /delete를 이용하여 공유 폴더를 삭제한다.

공유 폴더 확인 및 제거

정답 ②

상 중 하 시스템 보안 > 윈도우 클라이언트 및 서버 보안

12 증거수집 시 휘발성 데이터와 거리가 먼 것을 고르시오.

① 시간 및 로그인 사용자 정보
② 이벤트 로그
③ 프로세스 정보
④ 클립보드 정보

윈도우는 자체적으로 로그(Log)를 기록한다. 그래서 시스템 내에서 어떤 일이 발생했는지 알 수 있도록 하여 오류를 수정하거나 보안문제 등을 식별할 수 있게 하는 것이다. 이러한 이벤트 로그는 크게 응용 프로그램, 보안, 시스템 로그로 분류되며 이벤트 로그를 보기 위해서는 윈도우 이벤트 뷰어를 실행해서 확인할 수 있다.
이벤트 로그는 메모리와 매핑된 파일을 사용하여 service.exe 프로세스에서 서비스의 하나로 Eventlog.dll을 실행시킨다. Service.exe는 이벤트 로그 기록을 위해서 모든 서비스들이 1GB의 공간을 공유하게 하고 1GB 내에 연속적으로 64KB가 할당되어 이벤트 로그를 기록한다. 만약 윈도우 시스템 사용자가 최대 이벤트 로그 크기를 설정하면, 해당 크기를 넘은 경우는 이벤트 로그가 기록되지 않게 된다.
이벤트 로그의 크기를 사용자가 정의하는 경우 64부터 4,194,240 사이의 64배수 값으로 지정할 수 있다. 또한 이벤트 로그의 보유기간도 지정할 수 있는데 이것은 1에서 356일까지 가능하다.
이벤트 로그의 저장 방법은 매일 이벤트 덮어쓰기, 필요한 경우 이벤트 덮어쓰기, 이번에 덮어쓰지 않음, 정의하지 않음으로 설정할 수 있어서 사용자가 이벤트 로그를 어떤 식으로 기록할 수 있는지 결정할 수 있다.

정답 ②

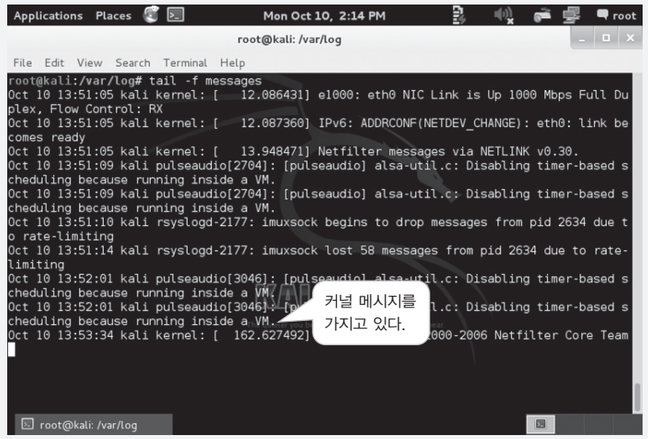
상 중 하 시스템 보안 > 리눅스 서버 보안

13 리눅스의 /var/log/messages 설명으로 가장 적정한 것을 고르시오.

① 특정 사용자의 로그를 기록한다.
② root 사용자를 위한 로그 정보를 기록한다.
③ 백업로그를 기록한다.
④ 시스템 메시지 로그이며 부트 프로세스에서 발생한 커널 메시지 및 기타 커널 상태 메시지를 저장한다.

/var/log/messages는 시스템 콘솔에서 출력된 부트 메시지 등을 기록한다.

messages 파일



정답 ④

상 중 하 시스템 보안 > 윈도우 클라이언트 및 서버 보안

14 윈도우 설정 정보는 윈도우 레지스트 파일 %SystemRoot%\System32\Config에 저장된다. 그 중 올바르지 않은 것은?

① SAM : 사용자 그룹계정 정보
② Security : 보안 및 권한 관련 정보
③ Software : 부팅에 필요한 전역 정보
④ ntuser.dat : 사용자별 설정 정보

SAM은 **사용자 그룹계정 정보**를 가지고 있는 데이터베이스이고, ntuser.dat는 **사용자 설정 정보**를 가지고 있다.

정답 ③

상 중 하 시스템 보안 > 리눅스 서버 보안

15 setuid에 대한 설명으로 옳은 것은?

① 실행자 명령어가 실행자의 ID가 아닌 명령어 파일 소유자 ID로 실행된다.
② 영문자 u로 표현된다.
③ 대표적인 명령이 /etc/passwd이다.
④ setgid와 함께 설정되지 않는다.

setuid 권한이 설정된 파일을 다른 사용자가 실행하게 되면, 해당 파일이 실행될 때 그 파일의 소유자의 권한으로 실행된다. /etc/passwd 파일은 setuid가 설정되어 있지 않고 **/usr/bin/passwd라는 실행 파일에 setuid가 설정**되어 있다.

setuid 확인

setuid가 설정된 실행 파일은 소문자 s로 권한이 조회된다.

정답 ③

상 중 하 시스템 보안 > 리눅스 서버 보안

16 공격자의 공격에 있어서 다른 곳으로 끌어내도록 설계한 유도 시스템은 무엇인가?

① Spoofing
② Honeypot
③ Sniffing
④ Switching

Honeypot은 해커가 취약성을 가진 서버에 침입하도록 유도한 뒤 해킹 수법이나 해킹 경로 등을 관찰함으로써 해커의 기술 수준과 공격 의도를 파악할 수 있도록 하는 차세대 인터넷 보안 기술이다.

정답 ②

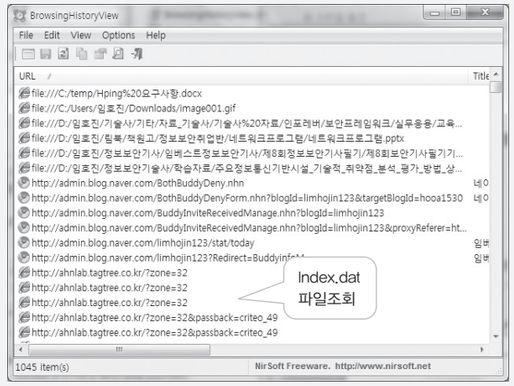
상 중 하 시스템 보안 > 윈도우 클라이언트 및 서버 보안

17 IE 기능 중 History는 index.dat 파일을 통해서 저장한다. 다음 중 History에 저장되지 않는 것은?

① 쿠키
② 접속한 URL
③ 마지막 방문시간
④ 다운로드 받은 파일

index.dat 파일은 **사용자가 방문한 웹 사이트 기록을 보관한 파일**로 웹 사이트에 대한 URL, **웹 페이지 목록, 송수신된 이메일 정보, 쿠키, 접속기록**이 남아있다.

BrowsingHistoryView로 index.dat 파일 조회



정답 ④

상 중 하 시스템 보안 > 리눅스 서버 보안

18 패스워드를 크래킹하기 위한 도구로 거리가 먼 것은?

① John the ripper
② L0phtcrack
③ pwdump
④ WinNuke

WinNuke는 DDoS 공격 도구로 청색폭탄(Blue Bomb)은 과도한 양의 네트워크에 부하를 발생시켜서 DDoS 공격을 수행한다.

정답 ④

상 중 하 시스템 보안 > 윈도우 클라이언트 및 서버 보안

19 다음 중 공유 자료관리에 관한 설명으로 옳은 내용을 모두 고르시오.

(1) 윈도우 관리 목적상 Admin$, C$, D$, IPC$ 등을 기본적으로 공유한다.
(2) IPC$ 및 nullsession 공유를 제거하는 편이 안전하다.
(3) IPC$는 윈도우 초기 버전에 해킹된 사례가 있다.
(4) 숨김 공유를 설정하면 침입을 막을 수 있다.

① (1), (2), (3), (4)
② (1), (2)
③ (1), (2), (3)
④ (4)

숨김 공유를 한다고 공유 폴더를 이용한 공격을 막을 수 있는 것은 아니다.

정답 ③

상 중 하 시스템 보안 > 리눅스 서버 보안

20 리눅스 /etc/shadow 파일을 통해서 알 수 없는 것은?

① 사용자 계정 이름
② 해시화된 패스워드
③ 패스워드 최소길이
④ 만료일 까지 남은 기간(일)

리눅스 shadow 파일은 사용자 계정명, 해시된 암호, 암호 생성일자, 암호를 변경할 수 있는 최소기간, 암호를 변경 없이 사용할 수 있는 유효기간, 만료 경고 일 수, 비활성화 일 수, 계정 만료일이 있다.

정답 ③

2과목 네트워크 보안

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

21 다음의 TCP Dump 로그는 어떤 공격의 로그인가?

```
192.168.0.10 > 192.168.0.10 ICMP echo request offset 0 seq 1000
192.168.0.10 > 192.168.0.10 ICMP echo request offset 0 seq 2232
192.168.0.10 > 192.168.0.10 ICMP echo request offset 0 seq 3332
192.168.0.10 > 192.168.0.10 ICMP echo request offset 0 seq 3333
```

① UDP Flooding
② Syn Flooding
③ Bonk Attack
④ LAND Attack

송신자의 IP 주소와 수신자의 IP 주소가 동일한 공격은 LAND Attack이며 본 문제와 동일한 문제가 제7회 정보보안산업기사 필기에서 출제되었다. 정보보안산업기사는 LAND Attack에서 변조하는 대상이 무엇인지를 물었고 답은 목적지 IP 주소였다.

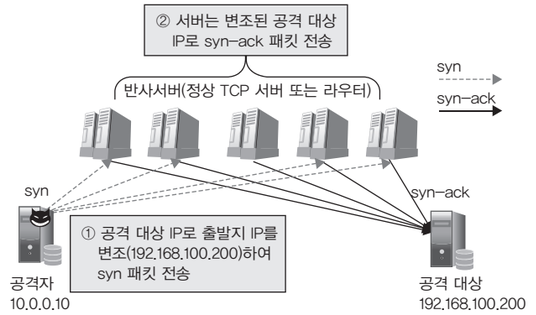
정답 ④

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

22 DRDoS의 특징으로 올바르지 않은 것은?

① IP Spoofing으로 은닉공격을 할 수 있다.
② 반사체라는 제3자를 통해서 수행한다.
③ Layer 7 공격을 수행하거나 단순 Flooding 공격이 특수 공격형태이다.
④ 3-Way Handshaking의 취약점을 이용한다.

DRDoS는 3-Way Handshaking 방식의 취약점을 이용하여 **공격자가 출발지 IP 주소를 공격 대상의 IP 주소로 위조해서 SYN 패킷을 정상적인 TCP 서버에게 전송**한다. 그러면 정상적인 TCP 서버는 SYN/ACK 패킷을 공격 대상 서버에 전송하여 DDoS 공격을 유발하는 것이다. 가장 큰 특징은 증폭의 특성을 가지고 있어서 공격자가 30Byte 정도의 패킷을 전송하면 응답으로 100Byte를 받게 된다.



정답 ③

상 중 하 네트워크 보안 > 네트워크 대응 기술 및 응용

23 Snort의 Payload를 검사하는 데 사용되는 것이 아닌 것은?

① TTL
② Content
③ Depth
④ Offset

Snort에서 Payload 탐지옵션은 content, nocase, rawbytes, depth, offset, within, uricontent, urilen, isdataat, pcre가 있다.

정답 ①

상 중 하 네트워크 보안 > 네트워크 대응 기술 및 응용

24 HIDS와 NIDS에 대한 설명으로 바르지 않은 것은?

① HIDS는 호스트에 설치되어서 시스템 침입정보를 탐지하기 때문에 별도의 하드웨어가 필요하지 않다.
② 암호화 된 트래픽 분석은 NIDS보다 HIDS가 유리하다.
③ NIDS는 네트워크 트래픽 분석에 유리하지만 별도의 하드웨어가 설치되어야 한다.
④ HIDS가 시스템 침입에 대한 로그 분석에 효용성이 높다.

네트워크 트래픽을 분석하는 것은 NIDS가 유용하고 호스트 내의 로그를 기반으로 침입을 탐지하는 것은 HIDS가 유용하다. 그리고 암호화된 트래픽은 복호화를 시켜서 탐지가 가능하기 때문에 HIDS가 암호화된 트래픽을 분석하려면 암호화키가 있어야 한다. 그러므로 IDS는 암호화된 트래픽을 분석할 수 없다. 단, 웹방화벽(Web Firewall)의 경우 SSL로 암호화된 패킷을 SSL 암호화키로 복호화한 후에 탐지할 수 있다.

정답 ②

상 중 하 네트워크 보안 > 네트워크 대응 기술 및 응용

25 IPSEC에 대한 설명으로 틀린 것은?

① AH는 무결성과 인증을 수행한다.
② ESP는 암호화를 수행하여 패킷 전체를 암호화한다.
③ 키교환을 위해서 IKE가 사용된다.
④ SA 정보는 두 통신 당사자에서 하나만 생성되고 운영된다.

SA(Security Association)는 송수신 되는 트래픽에 대해서 보안 서비스를 제공하는 것으로 양방향 서비스를 위해서 두 개의 SA가 필요하다. 또한 SA는 3개의 변수로 구분된다.
SA의 3개 변수는 SPI(Security Parameter Index), IP Destination Address, Security Protocol Identifier이며 SPI는 SA에 할당된 비트 문자열로 SPI는 AH와 ESP 헤더를 통해서 전송한다. IP Destination Address는 유니캐스트 주소만 허용하고 최종 목적지 주소이다. Security Protocol Identifier는 AH인지 ESP인지를 구분한다.

정답 ④

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

26 UDP Flooding의 대응 방법으로 옳지 않은 것은?

① 외부에서 내부로 유입되는 IP Broadcasting을 차단한다.
② 라우터 Outbound 처리에 ACL을 적용한다.
③ DDoS 대응 솔루션을 도입하여 차단한다.
④ 리눅스의 경우 chargen 또는 echo 서비스를 중지한다.

리눅스에서 echo는 TCP 버전과 UDP 버전이 존재하므로 echo를 중지한다는 것은 UDP Flooding에 대응한다고 볼 수 있다. IP Broadcasting의 경우는 255.255.255.255 주소로 패킷(Packet)을 전송하는 것으로 UDP Socket을 만들어 Broadcast를 수행한다.
라우터는 외부에서 내부로 유입되는 Inbound와 내부에서 외부로 나가는 Outbound에 ACL(Access Control List)을 설정할 수 있다. UDP Flooding은 외부에서 내부로 유입되는 공격이므로 Inbound를 차단해야 한다. 물론 내부에서 외부로 할 수도 있지만 Outound에 ACL 설정이 가장 거리가 멀다.

정답 ②

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

27 ICMP 프로토콜에 대한 설명으로 올바르지 않은 것은?

① ICMP는 네트워크 오류 상태를 확인하는 프로토콜이다.
② Destination unreachable 메시지는 TTL이 0이 되었을 때 보내준다.
③ ICMP echo request를 전송하고 그 응답으로 echo reply를 수신 받는다.
④ ICMP을 이용한 네트워크 공격이 ICMP Flooding이다.

Destination unreachable는 목적지 도착불가 메시지로 패킷이 Drop 되었을 때 송신자에게 전송되는 메시지이다.

정답 ②

상 중 하 네트워크 보안 > 네트워크 대응 기술 및 응용

28 다음의 방화벽 구축형태는 무엇인가?

외부와 내부의 완충지대에 방화벽을 설치한다.

① Screening Router
② Dual Home Gateway
③ Screened Subnet
④ Screened Host

Screened Subnet은 외부 네트워크와 내부 네트워크의 완충지대를 만드는 구축방법이다. 완충지대의 네트워크를 서브넷이라고 하며 해당 완충지대에 DMZ가 위치한다.

정답 ③

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

29 다음 중 ICMP 공격을 바르게 짝지은 것은?

① Smurf-Ping of Death
② Syn Flooing-Ping of Death
③ ICMP Flooding-Tear Drop
④ ICMP Flooding-Bonk

Smurf Attack은 ICMP Flooding이라고도 하며 ICMP echo Request에 대한 Reply 응답을 특정 호스트에 집중시켜서 공격하는 DDoS 공격 기법이다. Ping of Death는 커다란 ICMP 패킷을 전송하여 패킷 분할을 유도함으로써 피해자를 공격하는 방법이다.

정답 ①

상 중 하 네트워크 보안 > 네트워크 활용(TCP/IP 구조)

30 AS 간의 라우팅 프로토콜은 무엇인가?

① RIP
② OSPF
③ BGP
④ IS-IS

BGP(Border Gateway Protocol)는 서로 다른 종류의 자율 시스템(AS : Autonomous System) 사이에서 동작하는 라우팅 프로토콜이다. 자율 시스템이란 한 관리자에 의해서 관리되는 영역을 의미한다.

정답 ③

상 중 하 네트워크 보안 > 네트워크 일반

31 다음은 VLAN에 대한 설명이다. 괄호 안에 알맞은 것은 무엇인가?

VLAN이란 ( ) 메시지를 차단하기 위해서 ( )으로 구분된 것으로 ( )을 수행한다.

① 브로드캐스트, 물리적, 포트 모니터링
② 브로드캐스트, 논리적, 포트 모니터링
③ 유니캐스트, 논리적, 포트 필터링
④ 유니캐스트, 물리적, 포트 필터링

VLAN이란 논리적으로 분할된 스위치 네트워크로 불필요한 브로드캐스트 트래픽을 차단하고 네트워크의 보안성을 강화한다.

정답 ②

상 중 하 네트워크 보안 > 네트워크 대응 기술 및 응용

32 방화벽의 종류별 특징에 대한 설명으로 바르지 않은 것은?

① 방화벽은 외부에서 유입되는 패킷을 필터링하는 데 사용된다.
② Dual Home은 2개의 LAN 카드로 외부 망과 내부 망을 분리한다.
③ DPI(Deep Packet Interface)는 OSI 전 계층에서 필터링을 수행한다.
④ 서킷 게이트웨이는 클라이언트의 수정이 필요하다.

방화벽의 종류별 특징에 대한 설명 중 서킷 게이트웨이 부분에서 클라이언트 수정이 필요하다는 부분은 잘못된 설명이다.

서킷 게이트웨이(Circuit Gateway)

- 트랜스포트 층에서 운영되며 TCP 중계역할 수행
- TCP 포트로 연결되는 접근 통제 정책을 검사하여 허용 혹은 거부함
- 많이 사용되지 않음

정답 ④

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

33 다음 보기에서 설명하는 것은 무엇인가?

대규모 좀비 PC를 이용한 공격방법으로 좀비 PC를 하나의 네트워크로 형성하여 공격을 수행한다. 요즘은 C&C 서버 없이 좀비 PC들이 공격을 수행한다.

① DDoS
② 봇넷(Botnet)
③ DoS
④ APT

대규모의 좀비 PC들이 C&C(Command & Control) 서버의 명령을 받아서 공격하는 형태가 봇넷(Botnet)이다. 하지만 최근 공격으로 C&C 서버 없이 특정한 조건이 되면 스스로 공격을 수행하는 논리폭탄의 특성을 가진다.

정답 ②

상 중 하 네트워크 보안 > 네트워크 활용(TCP/IP 구조)

34 다음 중 인터넷 전송 방식에 대한 설명으로 틀린 것은?

① 유니 캐스트는 단말 상호 간에 데이터 전송을 수행한다.
② 멀티캐스트는 그룹에 등록된 사용자에게만 데이터를 전송한다.
③ 애니캐스트는 IPv4에서 최단노드에게만 전송하는 방법이다.
④ 브로드캐스트 IP 주소는 호스트 필드 비트 값이 모두 1인 주소를 말하며, 이러한 값을 갖는 IP 주소는 일반 호스트에 설정하여 널리 사용된다.

애니캐스트(Anycast)는 IPv6에 추가된 것으로 최단 노드에게만 데이터를 전송하는 방법이다.

데이터 전송방법

IPv4	IPv6
• Unicast • Multicast • Broadcast	• Unicast • Multicast • Anycast

정답 ③

상 중 하 네트워크 보안 > 네트워크 대응 기술 및 응용

35 SSL Handshaking에 대한 설명으로 틀린 것은?

① 서버는 클라이언트에게 Hello 메시지와 함께 클라이언트의 SSL 버전, 지원하는 암호화 알고리즘 리스트, 클라이언트 인증서 등을 전송한다.
② 서버는 Hello 메시지를 클라이언트에게 전송하며 암호화 알고리즘을 선택하여 서버 인증서를 같이 보낸다. 그리고 클라이언트가 서버 자원 접근을 요청하면 클라이언트 인증서를 요청한다.
③ 클라이언트는 서버 인증서를 확인하고 선정된 알고리즘으로 세션키를 생성하여 서버가 보내온 인증서에서 공개키를 추출하여 세션키를 암호화한 후에 서버로 전송한다.
④ 서버는 개인키로 복호화하고 종결 메시지를 클라이언트에게 보내서 서로간의 데이터 전송이 가능함을 알린다.

SSL Handshake 절차

1. 클라이언트는 서버에게 Hello 메시지와 함께 클라이언트의 SSL 버전, 지원하는 암호화 알고리즘 리스트 등을 전송한다.
2. 서버는 Hello 메시지를 클라이언트에게 전송하며 암호화 알고리즘을 선택하여 서버 인증서를 같이 보낸다. 그리고 클라이언트가 서버 자원 접근을 요청하면 클라이언트 인증서를 요청한다.
3. 클라이언트는 서버 인증서를 확인하고 선정된 알고리즘으로 세션키를 생성하여 서버가 보내온 인증서에서 공개키를 추출하여 세션키를 암호화한 후에 서버로 전송한다.
4. 서버는 개인키로 복호화하고 종결 메시지를 클라이언트에게 보내서 서로간의 데이터 전송이 가능함을 알린다.

정답 ①

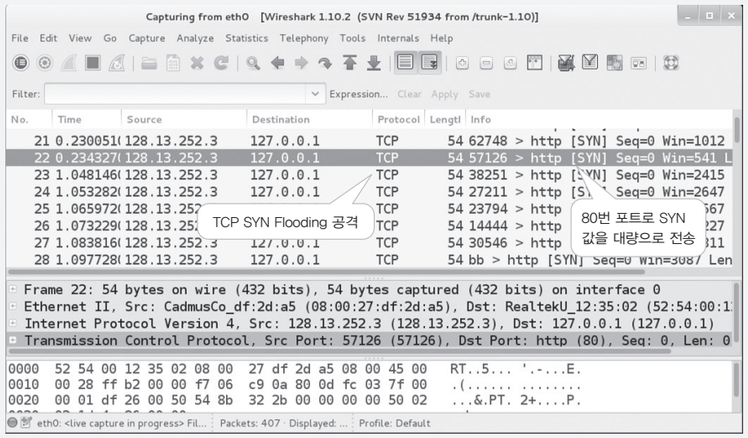
상 중 하 네트워크 보안 > 네트워크 기반 공격 기술의 이해 및 대응

36 TCP Half Open 취약점을 이용한 공격방법은 무엇인가?

① Smurf
② Syn Flooding
③ Tear Drop
④ Get Flooding

TCP Syn Flooding 공격은 TCP Half Open의 취약점을 이용한 공격으로 TCP SYN 신호를 범람시킨다.

TCP SYN Flooding 공격



정답 ②

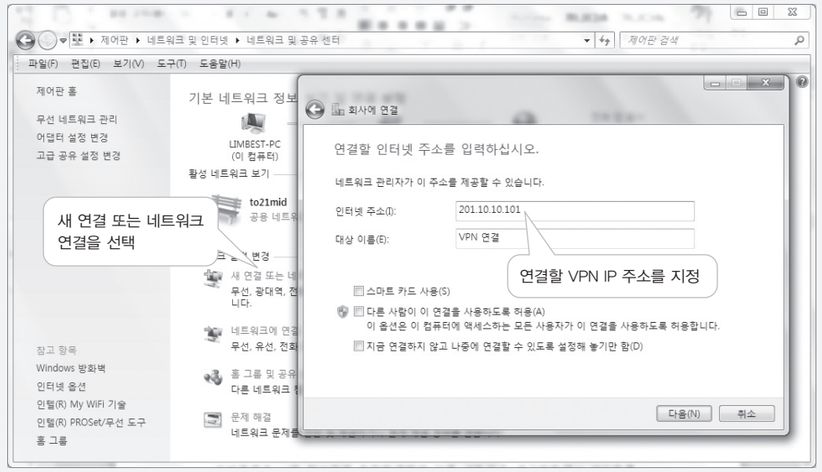
상 중 하 네트워크 보안 > 네트워크 대응 기술 및 응용

37 VPN의 기능과 거리가 먼 것은?

① 터널링
② 인증
③ 패킷 필터링
④ 암호화

VPN의 핵심 기능은 터널링이며 터널링을 실현하기 위해서 암호화를 해야 한다. 그리고 정당한 사용자만 VPN 네트워크를 사용할 수 있어야 하므로 인증 기능을 제공한다.
윈도우 제어판에서 네트워크 및 공유센터를 선택하고 새 연결 또는 네트워크 연결을 선택하면 VPN으로 연결할 수 있다. VPN 연결 설정 시 터널링 종류는 PPTP를 선택하면 된다. 물론 VPN 서버와 같은 종류의 터널링을 사용해야 한다.

윈도우에서 VPN 연결 방법



정답 ③

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

38 유도된 MAC 주소를 네트워크에 지속적으로 흘리고 스위치 허브 주소 테이블을 오버플로 시켜서 허브처럼 동작하게 하여 다른 네트워크 세그먼트에서 데이터를 스니핑하는 공격은?

① ARP Redirection
② ARP Spoofing
③ Switch Jamming
④ IP Spoofing

Switch Jamming은 Switch에서 MAC Table을 공격하는 것으로 MAC Table을 가득 차게 만드는 Flooding 공격이다. 즉, Random하게 MAC 주소를 생성하여 Frame을 Switch에 전송하면 MAC Table은 Overflow가 발생한다.

정답 ③

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

39 다음 DDoS 공격은 무엇인가?

- HTTP 서버를 공격
- 웹 서버를 공격
- 7계층을 사용

① IP Spoofing
② Syn Flooding
③ Get Flooding
④ ARP Spoofing

Get Flooding은 HTTP의 Get Method를 범람시키는 공격이고, HTTP는 OSI 7계층에서 동작한다. HTTP 프로토콜을 사용하는 것은 웹 서버이다.

정답 ③

삼 중 하 네트워크 보안 > 네트워크 대응 기술 및 응용

40 다음은 오용탐지에 대한 설명이다. 다음 중 바르지 않은 것은?

① 오용탐지는 시그니처를 등록하고 해당 시그니처와 같으면 침입으로 탐지한다.
② False Positve가 높고 False Negative가 낮은 특징이 있다.
③ 시그니처 기반, 지식기반 탐지방법으로 오탐율이 낮다.
④ 이상탐지는 False Positve가 크지만 Zeroday Attack에 대응할 수 있다.

오용탐지(Misuse)는 False Positve가 낮고 False Negative가 높다.

IDS 탐지 기법

구분	오용탐지(Misuse)	비정상탐지(Anomaly)
동작 방식	시그니처(signature) 기반 (Knowledge 기반)	프로파일(Profile) 기반(Behavior 기반, Statistical 기반)
침입 판단 방법	• 미리 정의된 Rule에 매칭 • 이미 정립된 공격패턴을 미리 입력하고 매칭	• 미리 학습된 사용자 패턴에 어긋남 • 정상적, 평균적 상태를 기준으로 하며 급격한 변화가 있을 때 침입 판단
사용 기술	패턴 비교, 전문가 시스템	신경망, 통계적 방법, 특징 추출
장점	• 빠른 속도, 구현이 쉬움, 이해가 쉬움 • False Positive가 낮음	• 알려지지 않은 공격(Zero Day Attack)에 대응 가능 • 사용자가 미리 공격패턴을 정의할 필요 없음
단점	• False Negative가 큼 • 알려지지 않은 공격탐지 불가 • 대량의 자료를 분석하기에 부적합	• 정상인지 비정상인지를 결정하는 임계치 설정이 어려움 • False Positive가 큼 • 구현이 어려움

* False Positive : false(+)로 표현, 공격이 아닌데도 공격이라고 오판하는 것
* False Negative : false(–)로 표현, 공격인데도 공격이 아니라고 오판하는 것

정답 ②

3과목 애플리케이션 보안

삼 중 하 애플리케이션 보안 > 인터넷 응용 보안

41 다음 중 PGP의 기능과 거리가 먼 것은?

① 암호화
② 인증
③ 단편화와 재조립
④ 전자서명

PGP(Pretty Good Privacy)는 전자우편 보안 기술로 필 짐머만(Phil Zimmermann)이 개발했으며 RSA와 IDEA 등의 암호화 알고리즘을 사용해서 암호화, 메시지 무결성, 전자서명을 지원한다.

정답 ③

삼 중 하 애플리케이션 보안 > 기타 애플리케이션 보안

42 HTTP Request 시 GET을 통해 메시지를 전송할 때 이를 이용한 공격방법으로, GET 메시지 전송 시 시스템의 프로세스를 실행할 수 있는 공격은 무엇인가?

① SQL Injection
② XSS
③ 운영체제 명령어 삽입
④ CSRF

개발 보안의 입력 값 검증 및 표현 부분에서 **운영체제 명령어 삽입**은 GET 방식으로 전송되는 **파라미터에 운영체제 명령을 삽입**하여 공격을 하는 방식으로 ps –ef와 같이 명령어를 덧붙이는 것이다.

운영체제 명령어 삽입

http://terms.naver.com/entry.nhn?docId=858168&cid=42346&categoryId=42346;ps –ef

정답 ③

삼 중 하 애플리케이션 보안 > 기타 애플리케이션 보안

43 파일 업로드 공격 방지를 위한 것으로 올바르지 않은 것은?

① 파일 업로드 시 파일 헤더 검사를 실행한다.
② 확장자 필터링을 수행한다.
③ 업로드된 파일에 대해서 실행 파일 속성을 제거한다.
④ 업로드할 수 있는 디렉터리를 제한한다.

파일 업로드 시 필요로 하는 디렉터리를 제한해야 한다. 즉, 상위 디렉터리로 이동할 수 없도록 해야 하며 확장자 필터링을 수행하여 실행 파일이 업로드되지 않도록 하여야 한다. 업로드된 파일의 실행 속성 제거는 유닉스 서버 상에서 실행되지 않을 수 있지만, 스크립트의 경우 클라이언트에 다운로드되어 웹브라우저에서 실행되므로 유닉스 서버 상에 실행속성 제거로 대응되지 않는다.

정답 ③

삼 중 하 애플리케이션 보안 > 전자상거래 보안

44 다음 중 SET에 대한 설명으로 바르지 않은 것은?

① 가맹점 정보와 구매자 정보를 별도로 전자서명한다.
② 전자서명 시에 가맹점과 구매자 정보를 분리해서 서명하지만 카드정보는 통합해서 서명한다.
③ 지불처리를 수행하는 프로토콜이다.
④ 암호화를 수행한다.

SET은 전자상거래 시 카드결제를 처리할 수 있는 지불 프로토콜이다. 지불처리 시 가맹점 정보와 구매자 정보를 별도로 서명하는 이중 서명을 지원한다.

정답 ②

삼 중 하 애플리케이션 보안 > 기타 애플리케이션 보안

45 버퍼 오버플로에 대한 설명으로 틀린 것은?

① 메모리 영역을 침범하는 공격이다.
② 최대 권한으로 실행한다.
③ 버퍼 오버플로 예방을 위해서 경계 값을 설정하여 컴파일을 수행한다.
④ Stack 영역의 침범으로 복귀주소를 조작한다.

정보보안에서 권한은 최대 권한이 아니라 최소 권한으로 실행한다.

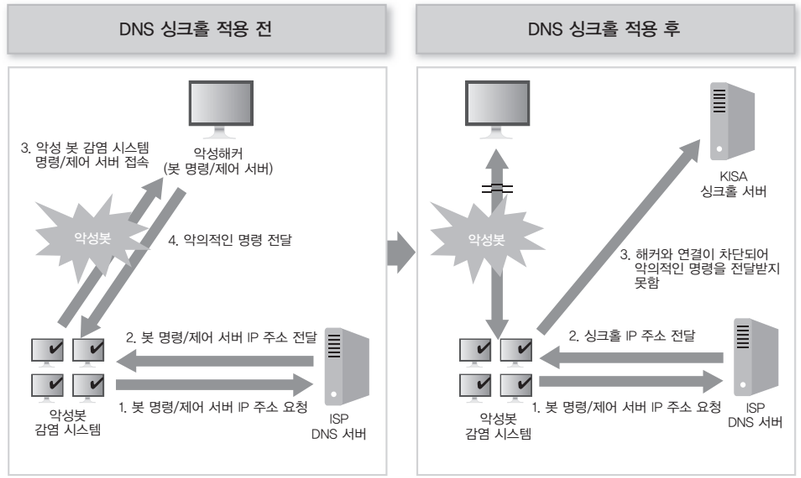
정답 ②

삼 중 하 애플리케이션 보안 > 인터넷 응용 보안

46 e메일 공격유형과 거리가 먼 것은?

① Active Contents
② 트로이 목마
③ 버퍼 오버플로
④ DNS 싱크홀

DNS 싱크홀이란 봇에 감염된 PC가 공격자와 연결을 시도할 때 싱크홀 서버에 연결하도록 하여 더 이상 공격자에게 조종당하지 않도록 해주는 시스템이다.



정답 ④

삼 중 하 애플리케이션 보안 > 인터넷 응용 보안

47 S/MIME에 대한 설명으로 틀린 것은?

① 전자서명을 지원한다.
② 전자우편에 대해서 암호화를 지원한다.
③ X.509 인증서를 사용한다.
④ X.25를 사용한다.

X.25는 백본 네트워크 기술로 회선의 상태가 좋지 않을 때 에러처리 기능을 강화하여 데이터를 송수신할 수 있는 통신기술이다.

정답 ④

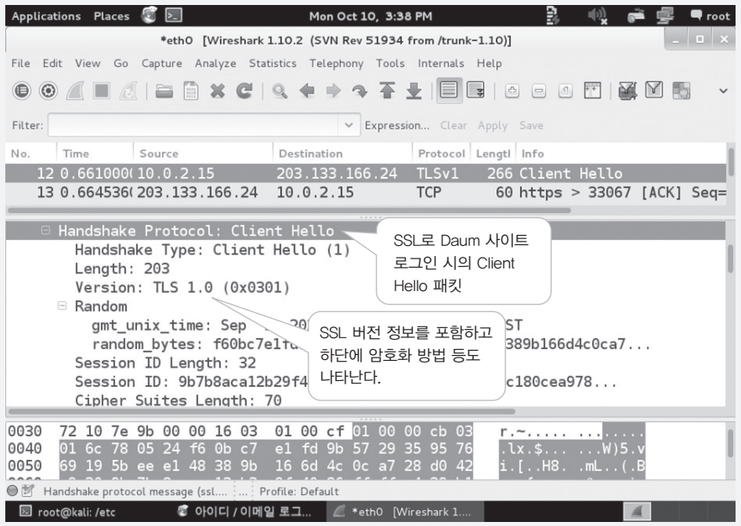
상 중 하 애플리케이션 보안 > 전자상거래 보안

48 SSL Handshake 과정에서 Client Hello에 포함되지 않은 것은?

① 클라이언트 SSL 버전
② 압축방법
③ 인증서
④ 암호화 방법

Client Hello에 포함된 것은 SSL 버전, 압축 방법, 암호화 방법을 포함하고 있다. 클라이언트 인증서는 서버의 요청 시 클라이언트가 전송한다.

SSL의 Client Hello 메시지를 Wireshark로 확인하기



정답 ③

상 중 하 정보보안 일반 > 보안 요소 기술

49 다음 중 커버로스에서 재생공격을 방지하는 방법은 무엇인가?

① 무결성 확인
② 타임스탬프
③ 암호화 키 관리
④ 전송구간 암호화

재생공격(Replay Attack)은 티켓을 복제해서 다른 사용자가 인증 서버에 접근하는 공격이다. 이러한 공격을 방지하기 위해서는 유일한 값을 부여해야 하는데 유일한 값을 부여하는 방법은 논리 계수기(Logical Counter) 혹은 타임스탬프(Timestamp) 등이 있다.

정답 ②

상 중 하 애플리케이션 보안 > 기타 애플리케이션 보안

50 다음 보기는 DRM의 구성요소에 대한 설명이다. 해당되는 것을 고르시오.

> 데이터 구조 및 정보를 일컫는 것으로 저작권 정보, 미디어 정보를 포함하고 있다.

① 패키지
② 시큐어 컨테이너
③ 메타 데이터
④ DRM 제어기

• 메타 데이터(Metadata)는 콘텐츠의 생명주기 범위 내에서 관리되어야 할 각종 데이터 구조 및 정보를 일컫는 것으로 저작권자 정보, 미디어 정보를 포함하고 있다.
• 시큐어 컨테이너는 콘텐츠 배포단위로 식별자, 암호화된 콘텐츠 메타 데이터, 전자서명 등으로 구성된다.

정답 ③

상 중 하 애플리케이션 보안 > 기타 애플리케이션 보안

51 다음 중 게시판에 악성코드를 삽입하는 공격은 무엇인가?

① XSS
② SQL Injection
③ Directory Listing
④ XPath

XSS는 게시판의 글쓰기 기능을 사용해서 악성 스크립트를 삽입하는 공격이다. 사용자가 해당 글을 클릭하면 실행되고 스크립트는 〈script〉 〈/script〉 형태로 등록한다.

정답 ①

상 중 하 애플리케이션 보안 > 기타 애플리케이션 보안

52 다음 중 SQL Injection 공격에 대한 대응방법으로 올바르지 않은 것은?

① DB 애플리케이션을 최소 권한으로 구동한다.
② 스크립트를 실행할 수 없게 한다.
③ 입력 값 검증을 수행한다.
④ PrepareStatement 함수를 사용한다.

스크립트를 실행할 수 없게 하는 것은 XSS에 대한 대응방법이고 SQL Injection은 데이터베이스를 공격 대상으로 하는 공격이라서 스크립트와는 관계가 없다.

정답 ②

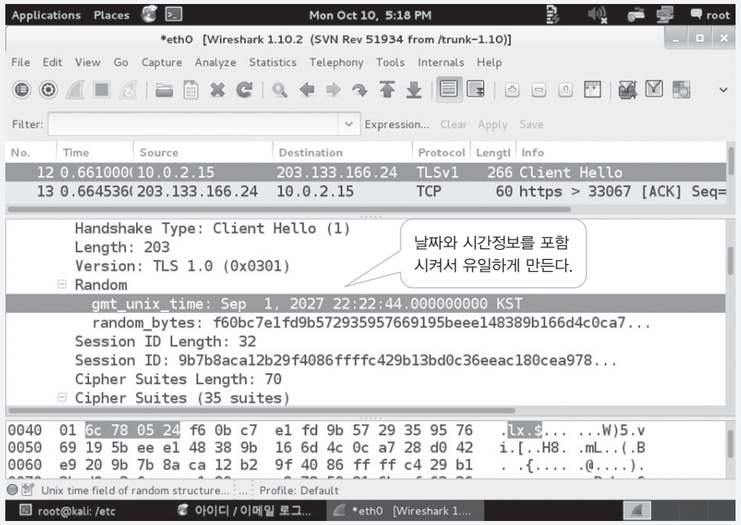
상 중 하 애플리케이션 보안 〉 전자상거래 보안

53 SSL Client Hello의 Random Number에서 날짜와 시간을 포함하도록 하는 이유는?

① 기밀성 제공
② 재생공격 방지
③ 순서제어
④ 무결성 지원

재생공격(Replay Attack)은 생성된 메시지 및 티켓 등을 복제해서 공격하는 형태로 임의의 타임스탬프, 랜덤번호 등으로 예방한다.

SSL Client Hello에 Random Number



정답 ②

상 중 하 애플리케이션 보안 〉 전자상거래 보안

54 패스워드의 안전성 확보를 위해서 매번 다른 패스워드를 사용하는 방법은 무엇인가?

① AES
② One Time Password
③ One Time Pad
④ DES

OTP(One Time Password)는 매번 다른 패스워드를 사용해서 스니핑으로 패스워드가 노출되어도 보안성을 확보할 수 있다.

정답 ②

상 중 하 애플리케이션 보안 〉 데이터베이스 보안

55 암호키 보호를 위해서 하드웨어를 사용한 기술과 거리가 먼 것은?

① 스마트카드
② HSM
③ TPM
④ SIM

스마트카드는 암호화키를 USIM에 저장하고 HSM(Hardware Security Model) 하드웨어를 기반으로 하여 관리한다. 또한 TPM(Trust Platform Module)도 암호화 모듈을 하드웨어에 저장하고 관리한다.

정답 ④

상 중 하 애플리케이션 보안 〉 기타 애플리케이션 보안

56 워터마킹의 응용분야와 거리가 먼 것은?

① 저작권 보호
② 이미지 인증
③ 데이터 은닉
④ 도청방지

워터마킹(Watermarking)은 디지털 콘텐츠에 대한 정보은닉 기술로 원저작자의 정보를 삽입함으로써 원저작자를 식별할 수 있다. 도청방지 기능은 제공하지 않는다.

정답 ④

상 중 하 애플리케이션 보안 〉 기타 애플리케이션 보안

57 〈 〉 &을 &lt, &gt, &amp, &quot로 교체하는 것은 어떠한 공격을 대비하려는 것인가?

① Buffer Overflow
② SQL Injection
③ XSS
④ Format String

〈 〉의 의미는 스크립트를 실행하기 위해서 필요한 것으로 개발 보안에서 이러한 문자를 대체해야 한다. 그리고 정보보안기사 실기를 위해서 각각의 기호가 어떤 것으로 대체되는지 확인해 두어야 한다. &lt, &gt, &amp, &quot에 대해서 알아두자.

XSS를 예방하기 위한 ReplaceAll 함수

```
replaceAll("<", "&lt;");
replaceAll(">","&gt;");
replaceAll("&","&amp;");
replaceAll("\","&quot;");
```

정답 ③

상 중 하 애플리케이션 보안 > 기타 애플리케이션 보안

58 C언어의 strcpy를 strncpy로 사용하는 것은 어떠한 공격을 대비하려는 것인가?

① 포맷 스트링
② 버퍼 오버플로
③ 경쟁조건
④ XSS

메모리를 복사할 때 길이 제한을 두는 함수가 strncpy()이다. 본 함수는 sizeof() 함수와 같이 사용해서 메모리의 크기를 먼저 확인한 후 복사하는 것이 좋다. 또한 이러한 함수를 사용하는 이유는 버퍼 오버플로 공격에 대비하기 위한 것이다.

정답 ②

상 중 하 정보보안 일반 > 접근 통제

59 생체인식 시스템의 요구사항이 아닌 것은?

① 유일성
② 획득성
③ 가변성
④ 성능

가변성은 상황 혹은 조건에 따라 변화한다는 것인데, 인증을 위해서는 변화하지 않고 유일하게 식별할 수 있는 조건이 필요하다. 그러므로 가변성은 생체인식 시스템의 요구사항과 거리가 멀다.

정답 ③

상 중 하 애플리케이션 보안 > 기타 애플리케이션 보안

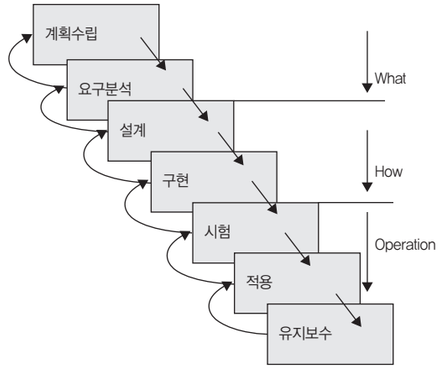
60 개발 보안 방법론에서 다음 SDLC 모형은 무엇인가?

- 개발단계별로 이전 단계를 완벽히 수행한다.
- 산출물을 중요시 한다.
- 사용자의 요구사항을 파악하기 어렵다.

① 폭포수 모델
② 나선형 모델
③ 반복형 모델
④ 프로토타이핑

폭포수 모델(Waterfall Model)은 소프트웨어 개발 생명주기 단계에서 가장 고전적이며 순차적 모델로 소프트웨어를 개발할 때 분석, 설계, 구현, 테스트의 정해진 순서로 개발하여 각 단계에서 정형화된 산출물을 강조하는 모델이다. 폭포수 모델은 아주 간단하지만 사용자 요구사항을 파악하기 어렵다. 그 이유는 사용자 요구사항에 대해서 테스트가 완료되어야 제대로 소프트웨어를 개발했는지 확인이 가능하기 때문이다.

폭포수 모델(Waterfall Model)



또한 본 문제는 향후 정보보안기사 시험의 다른 모습을 보여주는 문제이다. 즉, 지금까지의 문제에서는 개발 보안이 구현 측면에서 출제되었다면 본 문제는 개발 보안 방법론 측면에서 출제한 첫 문제이다.

정답 ①

4과목 정보보안 일반

상 중 하 정보보안 일반 > 접근 통제

61 다음 중 무결성에 중점을 둔 접근 통제 모델은 무엇인가?

① 비바(Biba) 모델
② 벨라파듈라(Bell-Lapadula) 모델
③ Non-Interference Model
④ 클락 윌슨(Clark and Wilson) 모델

1. 비바(Biba) 모델
Bell-Lapadula 모델의 단점인 무결성을 보장할 수 있도록 보장한 모델로 주체에 의한 객체 접근의 항목으로 무결성을 다룬 접근 통제 모델이다.

2. 벨라파듈라(Bell-Lapadula) 모델
- 기밀성 모델로서 높은 등급의 정보가 낮은 레벨로 유출되는 것을 통제하는 모델이다.
- 정보 구분 : Top Secret, Secret, Unclassified
- 최초의 수학적 모델로서 보안 등급과 범주를 이용한 강제적 정책에 의한 접근 통제 모델이다. 미 국방성(DOD)의 지원을 받아 설계된 모델로서 오렌지북인 TCSEC의 근간이 된다.
- 시스템의 비밀성을 보호하기 위한 보안 정책이다.

정답 ①

3. 비간섭 모델(Non-interference Model)
- 시스템 상태 또는 다른 주체의 실행에 영향을 주는 것을 방지하기 위한 보호 모델이다.
- 기본적으로 특정 주체의 실행이 다른 주체의 실행에 영향을 주지 않아야 하며, 다른 주체에 의해 인지되지 않아야 한다.
- 보안 분류의 상위 수준에 있는 특정 주체의 실행이 하위 수준에 있는 시스템 상태에 영향을 주는 것을 방지하는 것이다. 만약 그렇지 않다면 다른 주체는 안전하지 않은 상태에 놓이게 되거나 상위 수준에 대한 정보를 연역하거나 추론할 수 있게 되어 정보가 유출될 수 있다.

4. Clark and Wilson(클락 윌슨 모델)
- 무결성 중심의 상업용으로 설계한 것으로 Application의 보안 요구사항을 다룬다.
- 정보의 특성에 따라 비밀 노출 방지보다 자료의 변조 방지가 더 중요한 경우가 있다.
- 주체와 객체 사이에 프로그램이 존재하며, 객체는 항상 프로그램을 통해서만 접근한다.
- 2가지 무결성을 정의 : 내부 일관성(시스템 이용), 외부 일관성(감사에 활용)
- 클락 윌슨 모델의 무결성 3가지 메커니즘
  ① 완전한 처리(well-formed transaction) : 데이터는 예측가능하고 완전한 방식으로 조작되어야 함
  ② 직무 분리(separation of duties) : 한 사람이 모든 권한을 가지는 것을 방지하는 것. 정보의 입력, 처리, 확인 등 여러 사람이 나누어 각 부분별로 관리토록 함으로써 자료의 무결성을 보장(인가자의 비인가된 행동 예방)
  ③ 주체의 응용프로그램 강제 사용 : 주체의 객체로의 직접접근 금지, 응용 프로그램을 강제로 사용하도록 함

상 중 하 정보보안 일반 > 암호화

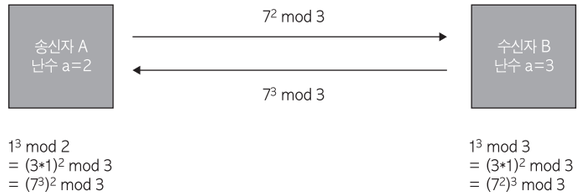
62 다음 중 디피헬만(Diffie-Hellman) 공개키 암호 알고리즘의 키교환방식에서 아래의 계산식을 확인한 후 공유키 값은 얼마인지 구하시오.

- 키 계산식: $q^{\propto} \bmod p$
- 송신자 p=3, q=7, a=2
- 수신자 p=3, q=7, a=3

① 1 ② 3
③ 5 ④ 7

Diffie-Hellman 공유키 값은 보기 ①번이다.
Diffie-Hellman 키 공유 절차는 다음과 같다.
(1) 송신자 A는 소수 P, 그리고 1부터 p-1까지의 정수 q를 선택하여 사전에 수신자 B와 공유한다.
(2) 송신자 A는 정수 a를 선택한다. (정수 a는 외부 미공개, 수신자 B도 알 수 없음)
(3) 송신자 A는 $A=q^a \bmod p$, 즉 q^a를 p로 나눈 나머지를 계산한다.
(4) 수신자 B도 마찬가지로 정수 b 를 선택, $B=q^b \bmod p$를 계산한다.
(5) 송신자 A와 수신자 B가 서로에게 A와 B를 전송한다.
(6) 송신자 A가 $B^a \bmod p$, 수신자 B가 $A^b \bmod p$를 계산한다.
(7) 마지막 단계에서 $Ba=(q^b \bmod p)^a \bmod p = q^{ab} \bmod p$, $Ab=(q^a \bmod p)^b \bmod p = q^{ab} \bmod p$이며, 따라서 공유키는 $K=q^{ab} \bmod p$를 공유하게 된다.
송신자 A p=3, q=7, a=2, 수신자 B p=3, q=7, 일때 Diffie-Hellman 키공유 계산식은 다음과 같다.

정답 ①



상 중 하 정보보안 일반 > 전자서명

63 다음 중 OCSP(Online Certificate Status Protocol)의 구성요소에 포함되지 않는 것은?

① ORS(Online Revocation Status)
② DPD(Delegated Path Discovery)
③ CRL(Certificate Revocation List)
④ DPV(Delegated Path Validation)

- OCSP(Online Certificate Status Protocol)는 인증서에 대한 사용가능여부를 실시간으로 검증하기 위한 프로토콜이다.
- OCSP는 클라이언트가 온라인 취소 상태 확인 서비스(ORS), 대리 인증 경로 발견 서비스(DPD), 그리고 대리 인증 경로 검증 서비스(DPV) 등의 3가지 상태 및 유효성 검증 서비스를 요구하고 서버가 이 요구 메시지에 대해 응답하는 프로토콜이다.
- CRL(Certificate Revocation List) : 인증서 폐기 목록

정답 ③

상 중 하 정보보안 일반 > 암호화

64 블록 암호화 모드 중 다음 보기에서 설명하고 있는 것에 해당되는 것은?

블록 암호화를 동기식 스트림 암호화로 변환한다. 블록 암호를 사용하여 블록 간의 의존 관계를 갖는 비트열 암호 이용 모드로 블록 암호의 출력 전부를 입력 레지스터 갱신에 사용하는 비트열 암호화 방법이다. 송신 측에서는 입력 레지스터에 기반을 두고 블록 암호화하여 그 출력의 비트열과 평문 비트열의 배타적 논리합을 취하여 생성한다. 수신 측에서는 송신 측의 암호화 처리와 같은 방법의 역순으로 복호한다. 영상데이터, 음성데이터와 같은 digitized analog(디지털화 된 아날로그) 신호에 주로 사용한다.

① CBC(Cipher Block Chaining)
② CFB(Cipher FeedBack)
③ OFB(Output FeedBack)
④ CTR (CounTeR) Mode

위의 보기는 OFB(Output FeedBack)에 대한 설명이다.

정답 ③

상 중 하 정보보안 일반 > 전자서명

65 다음 보기에서 설명하고 있는 서명방식은 무엇인가?

( ) 방식은 D.Chaum에 의해서 제안된 서명 방식이다. 서명용지 위에 묵지를 놓아 봉투에 넣어 서명자가 서명문 내용을 알지 못하는 상태에서 서명토록 한 방식을 수식으로 표현한 것이 은닉 서명이다. 즉, 서명문의 내용을 숨기는 서명 방식으로 제공자(provider : 서명을 받는 사람)의 신원과 서명문을 연결시킬 수 없는 익명성을 유지할 수 있다. 전자화폐나 전자투표에 사용된다.

① 이중서명 ② 은닉서명
③ 다중서명 ④ 대리서명

위의 보기에서 설명하고 있는 서명방식은 은닉서명이다.

1. 이중서명 : 사용자가 지불정보는 상점에 숨기고 주문정보는 은행에게 숨김으로써 사용자의 프라이버시가 보호되도록 함(SET)
2. 다중서명 : 전자결제시스템 혹은 전자계약시스템에 응용 가능한 방식
   - 동시 다중서명 : 전자계약시스템의 경우 동시 다중서명을 사용해서 서로 간에 안전한 계약을 수행
   - 순차 다중서명 : 전자결제의 경우 순차다중성 방식을 이용해 서명
3. 대리(위임)서명 : 본인이 부재 시에 자신을 대신하여 다른 사람이 서명을 수행
   - 제3자가 서명을 할 수 있어야 하고 검증자는 서명자의 위임사실을 확인할 수 있어야 하며 완전위임, 부분위임, 보증위임이 있음

정답 ②

상 중 하 정보보안 일반 > 접근 통제

66 다음 중 DAC(Discretionary Access Control)에 대한 특징으로 틀린 것은 무엇인가?

① 객체의 소유자가 허가하고 싶은 사용자에게만 권한 허용
② 객체의 소유자가 권한 부여
③ 접근 통제 목록(ACL, Access Control List) 사용
④ 중앙집중식 관리 환경에서 용이

- 임의적 접근 통제 모델인 DAC(Discretionary Access Control)는 중앙집중화된 환경보다는 분산형 보안관리에 더 적합한 모델로 동적(Dynamic)인 환경에서 정보 접근이 용이하다.
- 임의적 접근 통제 모델인 DAC(Discretionary Access Control)는 접근을 요청한 자의 신원(신분), 사용자 기반, 혼합 방식 접근 통제 방식이다. 객체에 접근을 하고자 하는 주체의 접근 권한에 따라 접근 통제를 적용하는 방법이다. 주체나 그들이 소속되어 있는 그룹들의 ID에 근거하여 객체에 대한 접근을 제한하는 접근 통제 방식이다.

구분	설명
통제기반	접근을 요청한 자(주체)의 신원(신분), 사용자 기반, 혼합 방식 접근 통제 방식
통제주체	객체의 소유자
특징	대부분 O/S 구현
장점	구현용이, 유연성
단점	도용 시 트로이목마에 취약
유형	• ACL(Access Control List) : 열 중심 • Capability List : 행 중심

정답 ④

상 중 하 정보보안 일반 > 보안 요소 기술

67 다음 중 커버로스(Kerberos)에 대한 설명으로 옳지 않은 것은?

① 커버로스 시스템은 인증 서버(AS), 티켓발급서버(TGS), 데이터 서버로 구성한다.
② 커버로스는 MIT에서 개발한 중앙집중적인 인증 서버이다.
③ 인증 서버에서 인증을 받은 후 티켓을 발급받아 로그인한다.
④ 티켓과 인증 서버가 분류되어 수행한다.

정답 ③

커버로스(Kerberos)

MIT의 Athena Project에 의해 개발된 **대칭키(DES) 방식에 의한 인증 시스템**. 서비스 요구를 인증하기 위한 대칭 암호기법에 바탕을 둔 **티켓을 기반으로 한 네트워크 인증 프로토콜**이다.

커버로스 구성요소

구성요소	설명
KDC	• 키분배센터(Key Distribution Sever), TGS + AS로 구성 • 사용자와 서비스 암호화키(비밀키)를 유지하고 인증 서비스를 제공하며 세션키를 만들고 분배
AS	인증 서비스(Authentication Service), 실질적 인증 수행
TGS	티켓 부여 서비스(Ticket Granting Service), 티켓을 만들고 세션키를 포함한 Principals에 티켓을 분배하는 KDC의 한 부분
Principals	인증을 위하여 커버로스 프로토콜을 사용하는 모든 시스템을 말함
Ticket	인증 토큰

커버로스의 장단점

장점	단점
• 대칭키(DES) 사용으로 데이터의 기밀성과 무결성 보장, 도청으로 보호 • 재생공격(Replay Attack) 방지 • 3A 지원 : Authentication, Accounting, Authorization • 개방된 이기종 간 시스템에서 자유로운 서비스 인증, SSO 통합인증 시 이용	• 패스워드 사전공격에 취약 • 비밀키, 세션키를 임시로 단말 저장 시 탈취가능성 존재 • 타임스탬프 시간동기화 프로토콜 필요 • SPOF(Single Point Of Failure)

상 중 하 정보보안 일반 > 접근 통제

68 다음은 특정 파일에 대한 객체의 권한 목록의 일부이다. 주체와 객체 간의 접근 통제 구조에 해당되는 것은?

File 1 user_2 : execute
File 2 user_1 : execute; user_2: execute
File 3 user_1 : execute, read; user_2: execute, read, append, write

① 접근 통제 목록(Access Control List)
② 자원 관리 목록(Resource Management List)
③ 자격 목록(Capability List)
④ 접근 통제 매트릭스(Access Control Matrix)

정답 ③

자격리스트(Capablity List)는 주체(사용자)별로 **객체(자원)를 연결 리스트로 연결한 것**이다. 객체의 수가 많으면 **탐색 속도가 느려지는 단점**이 있다. 예시를 보면 user_1, user_2의 주체가 중복되어 있는 것을 확인할 수 있다.

상 중 하 정보보안 일반 > 접근 통제

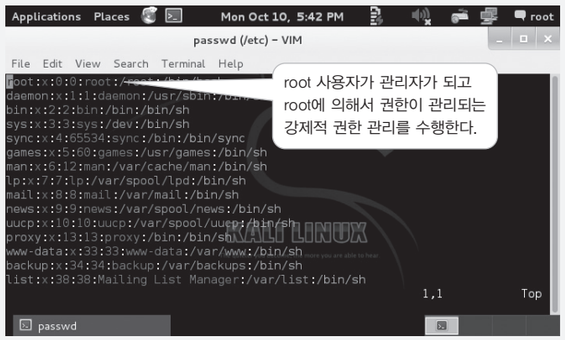
69 MAC(Mandatory Access Control)의 특징에 대한 설명으로 틀린 것은?

① 관리자에 의한 강제적 접근 통제를 수행한다.
② 객체 기밀수준과 주체 접근 근거한 보안등급(Security Class)을 할당한다.
③ 부서별, 범주별로 특성화된 접근 제어 정책을 설정하고 사용자에 의한 권한 관리를 수행한다.
④ 중앙집중식 관리 환경에서 용이하다.

정답 ③

MAC은 강제적 접근 통제로 관리자에 의한 권한 설정을 수행하고 DAC는 자율적 권한 관리로 사용자에 의한 권한 관리를 수행한다.

리눅스에서 MAC 사례



상 중 하 정보보안 일반 > 보안 요소 기술

70 다음은 OTP 일회용 패스워드 방식 중 challenge/Response에 대한 설명이다. 괄호 안에 들어갈 내용으로 알맞은 것을 고르시오.

Challenge-Response 방식은 사용자의 인증 요구와 함께 사용자 (A)를 인증 서버에게 전달한다. 인증 서버는 난수를 생성하여 challenge로 사용자에게 전달한다. 이와 동시에 인증 서버는 이용자의 사용자 (A)에 해당하는 패스워드를 키 데이터베이스에서 꺼내 이것을 이용하여 사용자와 약속된 암호 알고리즘을 통해 난수를 암호화한다.
Challenge를 받은 사용자는 그것을 자신의 패스워드를 이용하여 서버와 약속된 암호 알고리즘을 통해서 암호화하여 Response로 인증 서버에게 반환한다. 사용자로부터 Response를 받은 인증 서버는 서버 자신이 계산한 값과 수신된 Response 값을 비교하여 일치하는 경우에 사용자를 정당한 사용자로 인증한다.
Challenge-Response 방식은 입력 값이 매번 임의의 값이 된다는 측면에서는 안전성을 갖추고 있으나, 네트워크 모니터링에 의해 전송되는 값들이 노출되는 (B) 공격에 매우 취약해진다는 단점이 있다. 또 서버와 클라이언트 사이의 통신 횟수도 비교적 많이 요구된다.

① 식별번호(identification), 스니핑(sniffing)
② 인가(authorization), 재생공격(Replay Attack)
③ 인가(authorization), 스니핑(sniffing)
④ 식별번호(identification), 재생공격(Replay Attack)

Challenge-Response(시도응답)는 네트워크 사용자 인증을 위해서 기본 인증과 메시지 다이제스트 인증을 사용하는 방법이다. 사용자에게 비밀번호를 요구하고 응답받은 비밀번호가 정확하면 인증하는 방법이다.

정답 ①

상 중 하 정보보안 일반 > 전자서명

71 다음 중 공개키 기반의 인증서에 대한 설명으로 틀린 것은?

① 공개키 기반의 인증서는 공개키로 서명하고 개인키로 서명을 확인한다.
② 인증서는 인증기관이 발행한 소유자 개인키로 인증을 한다.
③ 일련번호, 유효기한을 정한 소유자 및 사용자의 알고리즘 정보를 포함한다.
④ CRL 목록을 유지하여 인증서의 유효성을 검사한다.

공개키 기반 인증서는 개인키로 전자서명을 하고 공개키로 전자서명을 확인한다.

정답 ①

상 중 하 정보보안 일반 > 암호화

72 다음 중 대칭키 문제를 해결하기 위한 방법에 해당하지 않는 것은?

① 키 배포 센터(KDC, Key Distribution Center)
② Diffie-Hellman 키 교환
③ RSA(Ron Rivest, Adi Shamir, Len Adelman)
④ 전자서명

대칭키는 키 교환의 문제가 발생하는데, 이를 해결하기 위한 방법으로 키 사전 공유 방법, 키 배포센터(KDC), Diffie-Hellman 키 교환, 공개키 암호에 의한 해결방법이 있다.

정답 ④

상 중 하 정보보안 일반 > 암호화

73 다음 중 Round 수가 가장 적은 암호화 알고리즘은 무엇인가?

① DES
② IDEA
③ AES
④ SEED

① DES : 16라운드, ② IDEA : 8라운드, ③ AES : 10, 12, 14라운드, ④ SEED : 16라운드

대칭키 암호화 기법

구분	블록크기	키 크기	Round	주요 내용
DES	64Bit	56Bit	16	키 길이가 작아 해독이 용이
3DES	64Bit	168Bit	48	DES의 Round 수를 늘려 보안성을 강화
AES	128Bit	128/192/256Bit	10/12/14	미국 표준 암호화 알고리즘
IDEA	64Bit	128Bit	8	암호화 강도가 DES보다 강하고 2배 빠름
SEED	128Bit	128Bit	16	국내에서 개발, ISO/IEC, IEFT 표준

정답 ②

상 중 하 정보보안 일반 > 암호화

74 다음 중 AES(Advanced Encryption Standard) 블록 암호화 방식에 대한 설명으로 틀린 것은?

① 블록 길이는 128비트이다.
② DES를 대신하는 미국 상무성 산하 NIST(National Institute of Standards and Technology) 표준 알고리즘이다.
③ Feistel 구조의 블록 암호 알고리즘이다.
④ 현대 암호화 기법인 혼돈(Confusion)과 확산(Diffusion)의 이론에 기반한 구조이다.

AES는 SPN 구조의 블록 암호화 알고리즘이다.

SPN(Substitution Permutation Network) 구조 특징

- 혼돈(Confusion)과 확산(Diffusion)의 이론에 기반한 구조
- 암호화 과정과 부호화 과정이 다르기 때문에 구현상 낭비가 있을 수 있음

정답 ③

상 중 하 정보보안 일반 > 암호화

75 다음 중 RSA 공개키 암호 알고리즘의 키 공유 과정에 대한 설명으로 틀린 것은 무엇인가? (①, ②, ③, ④ 순서대로 진행됨)

① 송신자 A는 개인키와 공개키를 생성한다.
② 송신자 A는 평문으로 공개키를 B에게 전송한다.
③ 수신자 B는 공유 비밀키를 생성하고, A의 공개키로 암호화하여 전송한다.
④ 송신자 A는 자신의 공개키로 공유키를 해독하고 데이터를 암호화하여 전송한다.

송신자 A는 수신자 B의 공개키로 암호화하여 수신자 B에게 전송한다. 수신자 B는 자신의 개인키로 복호화한다.

정답 ②

상 중 하 정보보안 일반 > 보안 요소 기술

76 다음 중 괄호 안에 들어갈 용어로 알맞은 것은?

- (A) : 정보 권한이 없는 사용자의 악의적 또는 비 악의적인 접근에 의해 변경되지 않는 것을 보장하는 보안 원칙
- (B) : 망을 경유해서 컴퓨터에 접속해 오는 사용자가 등록되어 있거나 정당하게 허가받은 사용자인지를 확인
- (C) : 정보가 허가되지 않은 사용자(조직)에게 노출되지 않는 것을 보장하는 보안 원칙

	(A)	(B)	(C)
①	기밀성	인증	무결성
②	무결성	책임추적성	가용성
③	식별	책임추적성	기밀성
④	무결성	인증	기밀성

- 가용성(Availability) : 인가된 사용자(조직)가 정보시스템의 데이터 또는 자원을 필요로 할 때 부당한 지체 없이 원하는 객체 또는 자원을 접근하고 사용할 수 있는 것을 보장하는 보안 원칙
- 식별(Identification) : 사용자가 시스템에 본인이 누구라는 것을 밝히는 행위(예 ID)
- 책임추적성(Accountability) : 시스템 내의 각 개인은 유일하게 식별되어야 한다는 정보보호 원칙. 이 원칙에 의해서 정보 처리 시스템은 정보보호 규칙을 위반한 개인을 추적할 수 있고, 각 개인은 자신의 행위에 대해서 책임을 짐

정답 ④

상 중 하 정보보안 일반 > 전자서명

77 다음 중 X.509 인증서 폐지에 대한 설명으로 틀린 것은?

① 인증서는 주체의 공개키 값, 이름 및 전자 메일주소, 주체 식별자, 유효기간, 발급자 식별자 정보를 보유한다.
② CRL은 인증서의 유효성을 검사하기 위해서 사용된다.
③ CA 스스로 인증서를 생성하고 자신을 스스로 인증하는 인증서를 메인 인증서라고 한다.
④ X.509 시스템에서 CA는 X.500의 규약에 따라 서로 식별되는 공개키를 가진 인증서를 발급한다.

CA 자신이 인증서를 생성하여 자신을 스스로 인증한 인증서를 루트 인증서(Self-Signed Digital Signature)라고 한다.

정답 ③

상 중 하 정보보안 일반 > 암호화

78 다음 중 해시함수의 특징에 대한 설명으로 옳지 않은 것은?

① MAC(Message Authentication Code)과 달리 키를 사용하지 않는다.
② 메시지 길이에 상관없이 적용가능하다.
③ 해시코드(Hash code) 길이는 가변이다.
④ 일방향(One-Way) 함수이다.

해시함수(Hash Funtion)

1. 임의의 길이의 메시지로부터 고정길이의 해시 값을 계산
2. 키가 없고 복호화가 불가능한 특징을 가지는 암호화 방식, 일방향 암호 기술
3. 일방향(One-Way) 함수로 주어진 임의의 출력 값에 대응하는 입력 메시지를 찾는 것이 계산적으로 불가능(Computationally Infeasible)
4. 충돌저항성(Collision free) : 동일한 출력 값을 갖는 서로 다른 메시지를 찾는 것이 어려움
   - 1st 충돌 저항 : 주어진 입력 값에 대응하는 출력 값과 동일한 출력 값을 갖는 다른 입력 값을 찾는 것이 계산적으로 불가능
   - 2nd 충돌 저항 : 임의의 두 입력 쌍에 대해 동일한 출력 값을 갖는 서로 다른 입력 값을 찾는 것이 계산적으로 불가능

정답 ③

상 중 하 정보보안 일반 > 전자서명

79 다음 중 인증 위협을 방지하기 위하여 인증 보호에 적용 가능한 기술과 관련이 없는 것은?

① 암호화
② 일방향 Hash 함수
③ MAC(Message Authentication Code)
④ 전자서명

- 메시지 인증은 수신 메시지가 송신한 메시지와 동일한 것인지 확인하는 것으로 전송 메시지 내용 변경, 순서 변경, 삭제 등의 불법행위 확인 기술이다.
- 메시지 인증 방식으로 대칭키(관용) 암호방식, 해시함수, MAC을 이용한 방법이 있다.

정답 ④

상 중 하 정보보안 일반 > 암호화

80 다음 중 암호해독을 수행하는 목적에 해당되지 않는 것은?

① 평문 데이터를 복원하기 위하여
② 암호화키 구조를 해독하기 위하여
③ 암호 알고리즘을 통하여 평문의 데이터를 추출하기 위하여
④ 암호화의 안정성 및 정량적 분석을 위하여

암호해독(cryptanalysis)이란 암호문으로부터 복호화 키를 찾아내거나 암호문을 평문으로 복원하려는 노력 또는 그에 관한 학문이다. 또한 암호화 알고리즘에서 사용되는 키에 관한 사전 지식을 갖지 않고 암호문을 평문으로 변환하기 위해 수행되는 단계 및 조작을 말한다.

암호문 공격 기법

암호문 공격 방법	설명
암호문 단독 공격 (Ciphertext only attack)	암호 해독자는 단지 암호문 C만을 갖고 이로부터 평문 P나 키 K를 찾아내는 방법으로 평문 P의 통계적 성질, 문장의 특성 등을 추정하여 해독하는 방법
기지 평문 공격 (Known plaintext attack)	암호 해독자는 일정량의 평문 P에 대응하는 암호문 C를 알고 있는 상태에서 해독하는 방법. 암호문 C와 평문 P의 관계로부터 키 K나 평문 P를 추정하여 해독하는 방법
선택 평문 공격 (Chosen plaintext attack)	암호 해독자가 사용된 암호기에 접근할 수 있어 평문 P를 선택하여 그 평문 P에 해당하는 암호문 C를 얻어 키 K나 평문 P를 추정하여 암호를 해독하는 방법
선택 암호문 공격 (Chosen ciphertext attack)	암호 해독자가 암호 복호기에 접근할 수 있어 암호문 C에 대한 평문 P를 얻어내 암호를 해독하는 방법

정답 ④

5과목 정보보안 관리 및 법규

상 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

81 다음 중 「정보통신기반보호법」의 주요정보통신기반시설의 보호 및 침해사고의 대응에 대한 설명으로 옳은 것은?

가. 소관 주요정보통신기반시설에 대한 중대한 전자적 침해사고의 발생 · 징후를 보고받거나 인지한 때에는 이를 과학기술정보통신부에 즉시 보고하고 필요한 응급조치를 하여야 한다. (보호지침 19조)
나. 관계중앙행정기관의 장은 주요정보통신기반시설보호대책을 분석 및 이행 여부를 분석하여 별도의 보호조치가 필요하다고 인정하는 경우에 해당 관리기관의 장에게 주요정보통신기반시설의 보호에 필요한 조치를 명령 또는 권고할 수 있다. (법 11조)
다. 관리기관의 장은 침해사고가 발생하여 소관 주요정보통신기반시설이 교란 · 마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관, 수사기관 또는 인터넷진흥원(이하 "관계기관등"이라 한다)에 그 사실을 통지하여야 한다. 이 경우 관계기관 등은 침해사고의 피해확산 방지와 신속한 대응을 위하여 필요한 조치를 취하여야 한다. (법 13조)
라. 주요정보통신기반시설에 대하여 침해사고가 광범위하게 발생한 경우 그에 필요한 응급대책, 기술지원 및 피해복구 등을 수행하기 위한 기간을 정하여 협회에 정보통신기반침해사고운영본부(이하 "대책본부"라 한다)를 둘 수 있다. (법 15조)

① 가, 나, 다
② 가, 나
③ 다, 라
④ 가, 라

주요정보통신기반시설에 대하여 침해사고가 광범위하게 발생한 경우 그에 필요한 응급대책, 기술지원 및 피해복구 등을 수행하기 위한 기간을 정하여 위원회에 정보통신기반침해사고대책본부(이하 "대책본부"라 한다)를 둘 수 있다. (법, 15조)

정답 ①

상 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

82 다음 중 개인정보보호법에 따라 개인정보수집 시 반드시 동의를 받아야 하는 경우는 무엇인가?

① 인터넷 홈페이지에 기재되어 있는 성명, 이메일 등의 개인정보를 수집하여 대출상담 전화 등 이벤트 광고홍보를 안내하는 경우
② 동호회에서 동호회 운영을 위하여 개인정보를 수집하는 경우
③ 자동차 구입을 목적으로 고객에게 받은 명함에 기재되어 있는 전화번호를 통하여 고객에게 구입관련 사항을 확인하는 경우
④ 소방서에서 홍수로 인하여 고립된 사람을 구조하기 위해서 연락처, 주소, 위치정보 등 개인정보를 수집하는 경우

① 개인정보보호법 제22조 제3항 개인정보처리자는 정보주체에게 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보의 처리에 대한 동의를 받으려는 때에는 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다.
② 친목단체(동창회, 동호회)의 개인정보수집 · 이용 시 반드시 동의하여야 하는 것은 아니다.
③ 제15조 제1항 제4호 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
④ 제15조 제1항 제5호 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

정답 ①

상 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

83 다음 중 주요정보통신기반시설에 해당되지 않는 것은?

① 도로 · 철도 · 지하철 · 공항 · 항만 등 주요 교통시설
② 포털 및 전자상거래 데이터를 보유한 시설
③ 전력, 가스, 석유 등 에너지 · 수자원 시설
④ 원자력 · 국방과학 · 첨단방위산업관련 정부출연연구기관의 연구시설

「정보통신기반보호법」 제7조 제2항 규정된 주요정보통신기반시설
1. 도로 · 철도 · 지하철 · 공항 · 항만 등 주요 교통시설
2. 전력, 가스, 석유 등 에너지 · 수자원 시설
3. 방송중계 · 국가지도통신망 시설
4. 원자력 · 국방과학 · 첨단방위산업관련 정부출연연구기관의 연구시설

정답 ②

상 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

84 다음 중 「정보통신기반보호법」에 따라 주요정보통신기반시설의 취약점의 분석 · 평가에 대한 설명으로 옳은 것은?

① 관리기관의 장은 소관 정보통신기반시설이 주요정보통신기반시설로 지정된 때에는 지정 후 6월 이내에 취약점의 분석 · 평가를 실시하여야 한다.
② 관리기관의 장은 소관 주요정보통신기반시설 지정 후 6월 이내에 동 시설에 대한 취약점의 분석 · 평가를 시행하지 못할 특별한 사유가 있다고 판단되는 경우에는 관할 중앙행정기관의 장의 승인을 얻어 지정 후 1월 이내에 이를 실시하여야 한다.
③ 주요정보통신기반시설에 대한 최초의 취약점 분석 · 평가를 한 후에는 3년마다 취약점의 분석 · 평가를 실시한다.
④ 소관 주요정보통신기반시설에 중대한 변화가 발생하였거나 관리기관의 장이 취약점 분석 · 평가가 필요하다고 판단하는 경우에도 1년 마다 취약점의 분석 · 평가를 실시할 수 있다.

정보통신기반보호법(제9조), 시행령(제17조)
② 관리기관의 장은 소관 주요정보통신기반시설 지정 후 6월 이내에 동시설에 대한 취약점의 분석 · 평가를 시행하지 못할 특별한 사유가 있다고 판단되는 경우에는 관할 중앙행정기관의 장의 승인을 얻어 지정 후 9월 이내에 이를 실시하여야 한다.

정보통신기반보호법 시행령(제17조 제1항)
③ 관리기관의 장은 소관 주요정보통신기반시설이 지정된 후 주요정보통신기반시설에 대한 최초의 취약점 분석 · 평가를 한 후에는 매년 취약점의 분석 · 평가를 실시한다.
④ 소관 주요정보통신기반시설에 중대한 변화가 발생하였거나 관리기관의 장이 취약점 분석 · 평가가 필요하다고 판단하는 경우에는 1년이 되지 아니한 때에도 취약점의 분석 · 평가를 실시할 수 있다.

정답 ①

상 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

85 다음 중 개인정보 분쟁조정위원회에 대한 설명으로 옳지 않은 것은?

① 분쟁조정위원회에 신청된 분쟁조정사건이 위원이 그 사건의 당사자와 친족이거나 친족이었던 경우에는 심의 · 의결에서 제척(除斥)된다
② 분쟁조정위원회는 당사자 일방으로부터 분쟁조정 신청을 받았을 때에는 그 신청내용을 상대방에게 알려야 한다.
③ 분쟁조정위원회는 분쟁조정 신청을 받은 날부터 120일 이내에 이를 심사하여 조정안을 작성하여야 한다.
④ 분쟁조정위원회는 분쟁조정 신청을 받았을 때에는 당사자에게 그 내용을 제시하고 조정 전 합의를 권고할 수 있다.

개인정보보호법
제43조(조정의 신청 등)
1. 개인정보와 관련한 분쟁의 조정을 원하는 자는 분쟁조정위원회에 분쟁조정을 신청할 수 있다.
제44조(처리기간)
① 분쟁조정위원회는 제43조 제1항에 따른 분쟁조정 신청을 받은 날부터 60일 이내에 이를 심사하여 조정안을 작성하여야 한다. 다만, 부득이한 사정이 있는 경우에는 분쟁조정위원회의 의결로 처리기간을 연장할 수 있다.

정답 ③

상 중 하 정보보안 관리 및 법규 > 정보보호 관리

86 다음 중 정보보호관리를 위한 체계와 가장 연관성이 적은 것은?

① ISMS
② ISO/IEC 27001
③ BS 7799
④ ISO/IEC 15408

영국에서 개발한 BS7799는 Part 1과 Part 2로 이루어지고 이후 BS7799를 기반으로 ISO 27000 시리즈를 표준화 했다. ISO 27000 시리즈 중에서 ISO 27001이 ISMS로 정보보호관리체계를 의미한다.
정보보호관리를 위한 체계와 가장 연관성이 적은 참조모델은 ISO/IEC 15408이다. ISO/IEC 15408은 CC(Common Criteria for security Evaluation)의 국제표준이다.

정답 ④

상 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

87 다음 중 전자서명법 인증서 소멸 사유에 해당하지 않는 것은?

① 인증 업무의 정지명령을 받은 자가 그 명령에 위반하여 인증 업무를 정지하지 아니한 경우로 공인인증기관의 지정이 취소된 경우
② 가입자의 전자서명검증정보가 분실 · 훼손 또는 도난 · 유출된 사실을 인지한 경우
③ 가입자 또는 그 대리인이 공인인증서의 폐지를 신청한 경우
④ 가입자가 사위 기타 부정한 방법으로 공인인증서를 발급받은 사실을 인지한 경우

가입자의 전자서명검증정보(×) → 전자서명생성정보(○)가 분실 · 훼손 또는 도난 · 유출된 사실을 인지한 경우(전자서명법 제18조 제1항)

제16조(공인인증서의 효력의 소멸 등)

1. 공인인증기관이 발급한 공인인증서는 다음 각호의 1에 해당하는 사유가 발생한 경우에는 그 사유가 발생한 때에 그 효력이 소멸된다.
   ① 공인인증서의 유효기간이 경과한 경우
   ② 제12조 제1항의 규정에 의하여 공인인증기관의 지정이 취소된 경우
   ③ 제17조의 규정에 의하여 공인인증서의 효력이 정지된 경우
   ④ 제18조의 규정에 의하여 공인인증서가 폐지된 경우

제12조(인증 업무의 정지 및 지정취소 등)

2. 과학기술정보통신부 장관은 공인인증기관이 6월 이내의 기간을 정하여 인증 업무의 전부 또는 일부의 정지를 명하거나 지정을 취소할 수 있다. 다만, 제1호 및 제2호의 경우에는 지정을 취소하여야 한다.
   ① 사위 기타 부정한 방법으로 제4조의 규정에 의한 지정을 받은 경우
   ② 인증 업무의 정지명령을 받은 자가 그 명령에 위반하여 인증 업무를 정지하지 아니한 경우
   ③ 제4조의 규정에 의한 지정을 받은 날부터 6월 이내에 인증 업무를 개시하지 아니하거나 6월 이상 계속하여 인증 업무를 휴지한 경우
   ④ 제6조 제4항의 규정에 의한 인증 업무준칙 변경 명령에 위반한 경우
   ⑤ 제11조의 규정에 의한 시정명령을 정당한 사유 없이 이행하지 아니한 경우

정답 ②

제17조(공인인증서의 효력정지 등)

1. 공인인증기관은 가입자 또는 그 대리인의 신청이 있는 경우에는 공인인증서의 효력을 정지하거나 정지된 공인인증서의 효력을 회복하여야 한다. 이 경우 공인인증서 효력회복의 신청은 공인인증서의 효력이 정지된 날부터 6월 이내에 하여야 한다.
2. 공인인증기관이 제1항의 규정에 의하여 공인인증서의 효력을 정지하거나 회복한 경우에는 그 사실을 항상 확인할 수 있도록 지체 없이 필요한 조치를 취하여야 한다.

제18조(공인인증서의 폐지)

1. 공인인증기관은 공인인증서에 관하여 다음 각호의 1에 해당하는 사유가 발생한 경우에는 당해 공인인증서를 폐지하여야 한다.
   ① 가입자 또는 그 대리인이 공인인증서의 폐지를 신청한 경우
   ② 가입자가 사위 기타 부정한 방법으로 공인인증서를 발급받은 사실을 인지한 경우
   ③ 가입자의 사망 · 실종선고 또는 해산 사실을 인지한 경우
   ④ 가입자의 전자서명생성정보가 분실 · 훼손 또는 도난 · 유출된 사실을 인지한 경우

상 중 하 정보보안 관리 및 법규 > 정보보호 관리

88 다음 중 보기에서 설명하고 있는 것에 해당되는 것은?

미국 국방부가 컴퓨터 보안 제품을 평가하기 위해 채택한 컴퓨터 보안 평가지침서로 흔히 오렌지 북(Orange-book)이라고도 한다.
운영체제나 보안 솔루션이 보안 측면에서 받을 수 있는 가장 기본적인 인증이 BLP(Bell-LaPadula 모델에 기반하여 기밀성만 강조한다. 보안 레벨을 A(검증된 보호), B(강제적 보호)B3 · B2 · B1, C(임의적 보호)C2 · C1, D(최소보호) 등 7단계로 분류한다.

① ITSEC(Information Technology Security Evaluation Criteria)
② TCSEC(trusted computer system evaluation criteria)
③ CC 인증(Common Criteria)
④ K- Shield certification evaluation criteria

보기의 설명은 미국의 보안평가지침서인 TCSEC에 대한 설명이다.
① ITSEC(Information Technology Security Evaluation Criteria)
- 1991년 5월 유럽 국가들이 발표한 공동 보안 지침서로 TCSEC이 기밀성만을 강조한 것과 달리 무결성과 가용성을 포괄하는 표준안을 제시하였다.
- TCSEC과 호환을 위한 F-C1, F-C2, F-B1, F-B2, F-B3(TCSEC의 C1, C2 등과 같다)와 독일의 ZSIEC의 보안 기능을 이용한 F-IN(무결성), F-AV(가용성), FDI(전송 데이터 무결성), F-DC(데이터 기밀성), F-DX(전송 데이터 기밀성) 등 총 10가지로 보안 수준을 평가한다.

③ CC 인증(Common Criteria) : 공통평가기준, ISO/IEC 15408
미국의 TCSEC와 유럽의 ITSEC의 보안표준을 기반으로 작성된 정보보호 제품의 객관적 평가를 위해 제정한 국가 간 정보보호 제품 인증 및 평가를 위한 국제공통 평가기준이다. CCRA(CC Recognition Agreement : 상호인정 협정 국가) 가입국 간의 보안 제품에 대한 상호인정을 제공하는 보안 제품 평가 국제기준이다.
④ K- Shield certification evaluation criteria

정답 ②

상 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

89 다음 중 개인정보 파기에 대한 설명으로 옳지 않은 것은?

① 다른 법령에 따라 개인정보를 파기하지 아니하고 보존하여야 하는 경우, 해당 개인정보는 다른 개인정보와 함께 저장 · 관리할 수 있다.
② 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다.
③ 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.
④ 요금정산은 완료하였으나 채권소멸시효기간 만료일이 남은 개인정보는 보존가능하다.

개인정보처리자가 법령에 따라 개인정보를 파기하지 않고 보존하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리해서 저장 · 관리하여야 한다.

개인정보보호법 제21조(개인정보의 파기)

1. 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.
2. 개인정보처리자가 제1항에 따라 개인정보를 파기할 때에는 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 파기방법 및 절차 등에 필요한 사항은 **대통령령**으로 정한다.
   • 개인정보처리자는 법 제21조에 따라 개인정보를 파기할 때에는 다음 각호의 구분에 따른 방법으로 하여야 한다.
   ① 전자적 파일 형태인 경우 : 복원이 불가능한 방법으로 영구 삭제
   ② 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 파쇄 또는 소각
   ③ 제1항에 따른 개인정보의 안전한 파기에 관한 세부 사항은 행정자치부장관이 정하여 고시한다.

정답 ①

상 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

90 다음 중 주요정보통신기반시설보호계획의 수립 등에 대한 설명으로 옳지 않은 것은?

① 제6조(주요정보통신기반시설보호계획의 수립 등) ① 관계중앙행정기관의 장은 제5조 제2항의 규정에 의하여 제출받은 주요정보통신기반시설보호대책을 종합 · 조정하여 소관분야에 대한 주요정보통신기반시설에 관한 보호계획(이하 "주요정보통신기반시설보호계획"이라 한다)을 수립 · 시행하여야 한다.
② 제5조(주요정보통신기반시설보호대책의 수립 등) ① 주요정보통신기반시설을 관리하는 기관(이하 "관리기관"이라 한다)의 장은 제9조 제1항의 규정에 의한 취약점 분석 · 평가의 결과에 따라 소관 주요정보통신기반시설 및 관리 정보를 안전하게 보호하기 위한 예방, 백업, 복구 등 물리적 · 기술적 대책을 포함한 관리대책(이하 "주요정보통신기반시설보호대책"이라 한다)을 수립 · 시행하여야 한다.
③ 3. 주요정보통신기반시설보호계획에는 다음 각호의 사항이 포함되어야 한다. ① 주요정보통신기반시설의 취약점 분석 · 평가에 관한 사항 ② 주요정보통신기반시설 및 관리 정보의 침해사고에 대한 예방, 백업, 복구대책에 관한 사항 ③ 그 밖에 주요정보통신기반시설의 보호에 관하여 필요한 사항
④ 관계중앙행정기관의 장은 소관분야의 주요정보통신기반시설의 보호에 관한 업무를 관리하는 자(이하 "정보보호관리자"이라 한다)를 지정하여야 한다.

아래의 정보통신기반보호법의 주요정보통신기반시설보호계획의 수립에 관한 법률 조항을 확인하시고 학습하시길 권고합니다.

제5조(주요정보통신기반시설보호대책의 수립 등)

1. 주요정보통신기반시설을 관리하는 기관(이하 "관리기관"이라 한다)의 장은 제9조 제1항의 규정에 의한 취약점 분석 · 평가의 결과에 따라 소관 주요정보통신기반시설 및 관리 정보를 안전하게 보호하기 위한 예방, 백업, 복구 등 물리적 · 기술적 대책을 포함한 관리대책(이하 "주요정보통신기반시설보호대책"이라 한다)을 수립 · 시행하여야 한다. 〈개정 2015.1.20.〉
2. 관리기관의 장은 제1항의 규정에 의하여 주요정보통신기반시설보호대책을 수립한 때에는 이를 주요정보통신기반시설을 관할하는 중앙행정기관(이하 "관계중앙행정기관"이라 한다)의 장에게 제출하여야 한다. 다만, 관리기관의 장이 관계중앙행정기관의 장인 경우에는 그러하지 아니하다.

제6조(주요정보통신기반시설보호계획의 수립 등)

1. 관계중앙행정기관의 장은 제5조 제2항의 규정에 의하여 제출받은 주요정보통신기반시설보호대책을 종합 · 조정하여 소관분야에 대한 주요정보통신기반시설에 관한 보호계획(이하 "주요정보통신기반시설보호계획"이라 한다)을 수립 · 시행하여야 한다.
2. 관계중앙행정기관의 장은 전년도 주요정보통신기반시설보호계획의 추진실적과 다음 연도의 주요정보통신기반시설보호계획을 위원회에 제출하여 그 심의를 받아야 한다. 다만, 위원회의 위원장이 보안이 요구된다고 인정하는 사항에 대하여는 그러하지 아니하다.
3. 주요정보통신기반시설보호계획에는 다음 각호의 사항이 포함되어야 한다. 〈개정 2015.1.20.〉
   ① 주요정보통신기반시설의 취약점 분석 · 평가에 관한 사항
   ② 주요정보통신기반시설 및 관리 정보의 침해사고에 대한 예방, 백업, 복구대책에 관한 사항
   ③ 그 밖에 주요정보통신기반시설의 보호에 관하여 필요한 사항
4. 과학기술정보통신부 장관과 국가정보원장은 협의하여 주요정보통신기반시설보호대책 및 주요정보통신기반시설보호계획의 수립지침을 정하여 이를 관계중앙행정기관의 장에게 통보할 수 있다. 〈개정 2007.12.21., 2008.2.29., 2013.3.23.〉
5. 관계중앙행정기관의 장은 소관분야의 주요정보통신기반시설의 보호에 관한 업무를 총괄하는 자(이하 "정보보호책임관"이라 한다)를 지정하여야 한다.
6. 주요정보통신기반시설보호계획의 수립 · 시행에 관한 사항과 정보보호책임관의 지정 및 업무 등에 관하여 필요한 사항은 대통령령으로 정한다.

정답 ④

91 **정보통신서비스 제공자는 정보보호 최고책임자를 지정하고 과학기술정보통신부 장관에게 신고하여야 한다. 다음 중 정보보호 최고책임자 지정 · 신고 대상자의 범위에 해당하지 않는 것은?**

① 청소년유해매체물을 제공하거나 매개하는 자
② 정보보호 관리체계 인증을 받아야 하는 자
③ 특수한 유형의 온라인서비스제공자로서 상시 종업원 수가 5명 이상이거나 전년도 말 기준 직전 3개월간의 일일평균 이용자 수가 1천 명 이상인 자
④ 상시 종업원 수가 1천 명 이상인 자

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제42조의3 제1항(청소년 보호 책임자의 지정 등)에 따라 정보통신서비스 제공자 중 일일 평균 이용자의 수, 매출액 등이 대통령령으로 정하는 기준에 해당하는 자는 정보통신망의 청소년 유해정보로부터 청소년을 보호하기 위하여 청소년 보호 책임자를 지정하여야 한다.

시행령 25조(청소년 보호 책임자 지정의무자의 범위)

1. 다음 각 목의 어느 하나에 해당하는 자
   ① 전년도말 기준 직전 3개월간의 일일평균이용자가 10만 명 이상인 자
   ② 정보통신서비스부문 전년도(법인의 경우에는 전사업연도) 매출액 10억 원 이상인 자
2. 「청소년 보호법」 제2조 제3호에 따른 청소년 유해매체물을 제공하거나 매개하는 자
   ② 청소년 보호 책임자는 해당 사업자의 임원 또는 청소년 보호와 관련된 업무를 담당하는 부서의 장에 해당하는 지위에 있는 자 중에서 지정한다.
   ③ 청소년 보호 책임자는 정보통신망의 청소년 유해정보를 차단 · 관리하고, 청소년 유해정보로부터의 청소년 보호계획을 수립하는 등 청소년 보호업무를 하여야 한다.
   ④ 제1항에 따른 청소년 보호 책임자의 지정에 필요한 사항은 대통령령으로 정한다.

정보통신망 이용촉진 및 정보보호 등에 관한 시행령 제36조의6

정보보호 최고책임자 지정 · 신고 대상자의 범위

1. 법 제41조 제1항 제1호에 따른 내용 선별 소프트웨어를 개발 및 보급하는 사업자
2. 법 제47조 제2항에 따라 정보보호 관리체계 인증을 받아야 하는 자
3. 「저작권법」 제104조 제1항에 따른 특수한 유형의 온라인서비스 제공자로서 상시 종업원 수가 5명 이상이거나 전년도 말 기준 직전 3개월간의 일일평균 이용자 수가 1천 명 이상인 자
4. 「전자상거래 등에서의 소비자보호에 관한 법률」 제2조 제3호에 따른 통신판매업자(통신판매중개업자를 포함한다)로서 상시 종업원 수가 5명 이상인 자
5. 「게임산업진흥에 관한 법률」 제2조 제7호에 따른 인터넷컴퓨터게임시설제공업을 영위하는 자에게 같은 법 제28조 제6호에 따라 고시된 음란물 및 사행성게임물 차단 프로그램을 제공하는 사업자
6. 상시 종업원 수가 1천 명 이상인 자

정답 ①

92 **다음 중 정보통신망법에 의하여 동의 없이 이용자의 개인정보를 수집 · 이용할 수 있는 사항에 해당되지 않는 것은?**

① 이 법 또는 다른 법률에 특별한 규정이 있는 경우
② 개인정보의 제3자 제공
③ 정보통신서비스 제공자 등이 영업의 전부 또는 일부의 양도 · 합병 등으로 그 이용자의 개인정보를 타인에게 이전하는 경우
④ 개인정보의 국외 처리위탁 · 보관하는 경우

1. 제22조 제2항 동의 없이 이용자의 개인정보를 수집 · 이용 가능 경우
   ① 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적 · 기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우
   ② 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우
   ③ 이 법 또는 다른 법률에 특별한 규정이 있는 경우
2. 개인정보의 제3자 제공 시 동의 필요
   • 원칙 : 동의
   • 예외조항 : 제22조 제2항 제2호(요금정산) 및 제3호(다른 법률 특별한 규정)에 해당하는 경우 외에는 동의 없이 개인정보 수집 · 이용 가능

제24조의2(개인정보의 제공 동의 등)

1. 정보통신서비스 제공자는 이용자의 개인정보를 제3자에게 제공하려면 제22조 제2항 제2호(요금정산) 및 제3호(다른 법률 특별한 규정)에 해당하는 경우 외에는 다음 각호의 모든 사항을 이용자에게 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
3. 제26조(영업의 양수 등에 따른 개인정보의 이전)
   • 원칙 : 고지(인터넷 홈페이지 게시, 전자우편 등)
   • 목적범위 초과 개인정보의 이전 시 : 별도 동의
4. 이용자의 개인정보의 국외 이전 시
   • 원칙 : 이용자 동의 (국외 제공 · 조회 이전 시)
   • 예외 : 계약을 이행하고 이용자 편의 증진 등을 위하여 이용자의 고지한 경우에는 개인정보처리위탁 · 보관에 따른 동의 절차를 거치지 아니할 수 있음

제63조(국외 이전 개인정보의 보호)

2. 정보통신서비스 제공자 등은 이용자의 개인정보를 국외에 제공(조회되는 경우를 포함한다) · 처리위탁 · 보관(이하 이 조에서 "이전"이라 한다)하려면 이용자의 동의를 받아야 한다.
   다만, 정보통신서비스의 제공에 관한 계약을 이행하고 이용자 편의 증진 등을 위하여 필요한 경우로서 제3항 각호의 사항 모두를 제27조의2 제1항에 따라 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알린 경우에는 개인정보처리위탁 · 보관에 따른 동의절차를 거치지 아니할 수 있다. 〈개정 2016.3.22.〉

정답 ②

상 중 하 정보보안 관리 및 법규 > 정보보호 관리

93 다음 중 위험관리를 수행하려고 할 때, 필요한 구성요소에 해당하지 않는 것은?

① 자산(Asset)
② 위협(Threat)
③ 취약점(Vulnerability)
④ 직원(staff)

위험관리 구성요소

위험관리	구성요소
자산(Asset)	조직에 가치가 있는 자원들
위험(Risk)	위협, 취약점을 이용하여 조직의 자산에 손실, 피해를 가져올 가능성
위협(Threat)	조직, 기업의 자산에 악영향을 끼칠 수 있는 조건, 사건, 행위
취약점(Vulnerability)	위협이 발생하기 위한 조건 및 상황

정답 ④

상 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

94 개인정보보호법 중 개인정보보호원칙에 대한 설명으로 옳지 않은 것은?

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 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.
③ 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.
④ 개인정보의 익명처리가 가능한 경우에는 실명에 의하여 처리될 수 있도록 하여야 한다.

개인정보처리 시 실명 처리를 원칙으로 한다. → ⑦ 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다.

개인정보보호법 제3조(개인정보보호 원칙)

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 개인정보의처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.
④ 개인정보처리자는 개인정보의처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.
⑤ 개인정보처리자는 개인정보처리 방침 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

95 다음 중 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립 · 시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적으로 하는 정보통신기반보호법의 일반적인 체계에 해당하지 않는 것은?

① 시스템 개발 및 관리
② 주요정보통신기반시설의 보호체계
③ 지정 및 취약점 분석
④ 보호 및 침해사고의 대응

정보통신기반보호법의 조문구성 체계는 다음과 같다.
제1장 총칙
제2장 주요정보통신기반시설의 보호체계
제3장 주요정보통신기반시설의 지정 및 취약점 분석
제4장 주요정보통신기반시설의 보호 및 침해사고의 대응
제5장 삭제
제6장 기술지원 및 민간협력 등
제7장 벌칙
부칙

정답 ①

상 중 하 정보보안 관리 및 법규 > 정보보호 관리

96 다음 중 정보보호 관리체계 인증에 대한 설명으로 옳지 않은 것은?

① 정보보호 관리체계 인증의 유효기간은 3년으로 한다.
② 인증 의무대상자는 정보통신서비스 제공자로서 정보통신망법 제47조 제2항에 따라 주요 정보통신서비스제공자로 일정 규모 이상의 정보통신서비스제공자를 말하며, 인증 의무대상자 기준에는 해당하지 않으나 자발적으로 정보보호 관리체계를 자율적으로 신청하여 인증 심사를 받을 수 있다.
③ 정보통신망의 안정성 · 신뢰성 확보를 위하여 관리적 · 기술적 · 물리적 보호조치를 포함한 종합적 관리체계(이하 "정보보호 관리체계"라 한다)를 수립 · 운영하고 있는 자에 대하여 관리적 · 기술적 · 물리적 보호대책을 포함한 인증 기준에 적합한지에 관하여 인증을 할 수 있다.
④ 정보보호 관리체계 인증을 받아야 하는 자가 국제표준 정보보호 인증을 받거나 정보보호 조치를 취한 경우에는 인증 심사의 전부를 생략할 수 있다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조 제3항
인증을 받아야 하는 자가 과학기술정보통신부령으로 정하는 바에 따라 국제표준 정보보호 인증을 받거나 정보보호 조치를 취한 경우에는 제1항에 따른 인증 심사의 일부를 생략할 수 있다.

정답 ④

상 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

97 다음 중 개인정보수집 및 이용이 가능한 경우에 해당하지 않는 것은?

① 보험회사가 계약체결을 위해 청약자의 자동차 사고 이력, 질병 정보, 다른 유사보험의 가입여부 등에 관한 정보를 수집하는 경우
② 사업자가 고객과의 소송이나 분쟁에 대비하여 요금정산자료, 고객의 민원제기내용 및 대응자료 등을 수집 · 관리하는 경우
③ 거래 체결 전에 거래상대방의 신용도 평가를 위해 정보를 수집 · 이용하는 경우
④ 입사 채용을 위한 면접단계에서 주민등록번호를 수집하는 경우

회사가 취업지원자와의 채용 및 근로계약 체결 전에 지원자의 이력서, 졸업증명서, 성적증명서 등 정보를 수집 · 이용 가능(개인정보보호법 제15조 제1항 제4호)하다. 단, 입사지원단계에 있는 주민등록번호 수집은 허용되지 않는다. 다만, 채용 여부 확정 시 주민등록번호 수집은 가능하다.

보기 ①, ③은 제15조 제1항 제4호 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우에 개인정보수집 및 이용이 가능하다.
보기 ②번은 제15조 제1항 제6호 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우이다.

정답 ④

상 중 하 정보보안 관리 및 법규 > 정보보호 관리

98 위험분석 기법은 정량적 위험분석과 정성적 위험분석으로 나뉜다. 다음 중 정량적 위험분석 방법이 아닌 것은?

① 연간기대손실법
② 과거자료분석법
③ 수학공식접근법
④ 시나리오접근법

정량적 위험분석 방법에 해당하지 않는 분석 기법은 시나리오접근법이다.

정량적 위험분석 방법

방법	설명
연간 기대 손실법(ALE)	• 위험 발생확률 * 손실 크기를 통해 기대 위험가치를 분석 • SLE = EF(노출계수) × AV(자산가치) • ALE = SLE × ARO(연간발생률)
수학공식 접근법	위의 발생빈도를 계산하는 식을 이용하여 위험을 계량하는 방법
확률 분포추정법	미지의 사건을 확률적 편차를 이용하여 위험 예측 방법
몬테카를로 시뮬레이션	확률 분포를 가정하여 모델을 만들고, 난수(Random Variable)를 발생시켜 일정/원가측면의 준수확률을 계산
과거 자료 분석법	과거의 자료를 근거로 위험을 분석하는 방법

정성적 위험분석

방법	설명
델파이법	전문적인 지식을 가진 집단을 구성하여 위험분석 및 평가하여 정보시스템이 직면한 다양한 위협과 취약성 토론을 통해 분석
시나리오법(PI Matrix)	어떤 사건이 기대대로 발생하지 않는다는 사실에 근거하여 일정조건에서 위험에 대하여 발생 가능한 결과들을 추정하는 방법
순위 결정법	위험순위 결정표에 위험항목들의 서수적 순위(Ordinal Ranking)를 결정하는 기법
퍼지행렬법	자산, 위협, 보안체계에 대해 정성적인 언어로 표현된 값을 사용하며, 자연어 표현을 수학적으로 하는 방법을 사용
질문서법	질문할 내용을 서면으로 작성하여 인터뷰 등의 방법으로 위험분석을 수행하는 방법

정답 ④

상 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

99 다음 중 개인정보보호위원회의 기능으로 옳지 않은 것은?

① 개인정보의 보호의 기본계획 및 시행계획 수립 · 시행 및 집행
② 개인정보보호와 관련된 정책, 제도 및 법령의 개선에 관한 사항
③ 개인정보의 처리에 관한 공공기관 간의 의견조정에 관한 사항
④ 개인정보 침해요인 평가에 관한 사항

제8조(보호위원회의 기능 등)

1. 보호위원회는 다음 각호의 사항을 심의 · 의결한다.
   ① 제8조의2에 따른 개인정보 침해요인 평가에 관한 사항 〈개정 2015.7.24.〉
   ①의2. 제9조에 따른 기본계획 및 제10조에 따른 시행계획
   ② 개인정보보호와 관련된 정책, 제도 및 법령의 개선에 관한 사항
   ③ 개인정보의 처리에 관한 공공기관 간의 의견조정에 관한 사항
   ④ 개인정보보호에 관한 법령의 해석 · 운용에 관한 사항
   ⑤ 제18조 제2항 제5호에 따른 개인정보의 이용 · 제공에 관한 사항
   ⑥ 제33조 제3항에 따른 영향평가 결과에 관한 사항
   ⑦ 제61조 제1항에 따른 의견제시에 관한 사항
   ⑧ 제64조 제4항에 따른 조치의 권고에 관한 사항
   ⑨ 제66조에 따른 처리 결과의 공표에 관한 사항
   ⑩ 제67조 제1항에 따른 연차보고서의 작성 · 제출에 관한 사항
   ⑪ 개인정보보호와 관련하여 대통령, 보호위원회의 위원장 또는 위원 2명 이상이 회의에 부치는 사항
   ⑫ 그 밖에 이 법 또는 다른 법령에 따라 보호위원회가 심의 · 의결하는 사항
2. 보호위원회는 제1항 각호의 사항을 심의 · 의결하기 위하여 필요한 경우 다음 각호의 조치를 할 수 있다. 〈개정 2015.7.24.〉
   ① 관계 공무원, 개인정보보호에 관한 전문 지식이 있는 사람이나 시민사회단체 및 관련 사업자로부터의 의견 청취
   ② 관계 기관 등에 대한 자료제출이나 사실조회 요구
3. 제2항 제2호에 따른 요구를 받은 관계 기관 등은 특별한 사정이 없으면 이에 응하여야 한다. 〈신설 2015.7.24.〉
4. 보호위원회는 제1항 제2호의 사항을 심의 · 의결한 경우에는 관계 기관에 그 개선을 권고할 수 있다. 〈신설 2015.7.24.〉
5. 보호위원회는 제4항에 따른 권고 내용의 이행 여부를 점검할 수 있다.
   [〈신설 2015.7.24.〉 시행일 : 2016.7.25.] 제8조 제1항

구분	2014.11.19 개정 전		2015.7.2개정 (시행일 : 2016.7.25)
제9조 기본계획	기본계획 수립	행정자치부장관은 관계 중앙행정기관의 장과 협의 하에 작성	보호위원회는 관계 중앙행정기관의 장과 협의 수립
	제출기관	보호위원회 제출	
	수립기간	3년마다	3년마다
제10조 시행계획	시행계획 수립	중앙행정기관의 장은 시행계획 작성	상동
	수립기간	매년(1년)	
제11조 자료제출요구	자료제출요청기관	행정자치부장관	보호위원회
	개인정보관리수준 및 실태파악 등을 위한 조사 실시	2015.7.24 신설항목	행정자치부장관은 개인정보보호 정책 추진, 성과평가 등을 위하여 필요한 경우 조사 실시 가능
	자료제출기관 및 실태조사실시기관	개인정보처리자, 관계 중앙행정기관의 장, 지방자치단체의 장 및 관계 기관 · 단체 등	
제12조 개인정보보호지침	작성자	행정자치부장관	
	목적	개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등 표준지침을 정하고 준수 권장	

정답 ①

삼 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

100 다음 중 전자서명법에 나온 공인인증서에 포함되는 내용이 아닌 것은?

① 가입자 및 인증기관의 전자서명 버전
② 공인인증서의 일련번호, 유효기간
③ 공인인증기관의 명칭 등 공인인증기관임을 확인할 수 있는 정보
④ 공인인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항

전자서명법 제 15조(공인인증서의 발급)

2. 공인인증기관이 발급하는 공인인증서 포함 내용
   ① 가입자의 이름(법인의 경우에는 명칭을 말한다)
   ② 가입자의 전자서명검증정보
   ③ 가입자와 공인인증기관이 이용하는 전자서명 방식
   ④ 공인인증서의 일련번호
   ⑤ 공인인증서의 유효기간
   ⑥ 공인인증기관의 명칭 등 공인인증기관임을 확인할 수 있는 정보
   ⑦ 공인인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항
   ⑧ 가입자가 제3자를 위한 대리권 등을 갖는 경우 또는 직업상 자격 등의 표시를 요청한 경우 이에 관한 사항
   ⑨ 공인인증서임을 나타내는 표시
4. 공인인증기관은 공인인증서를 발급받고자 하는 자의 신청이 있는 경우에는 공인인증서의 이용범위 또는 용도를 제한하는 공인인증서를 발급할 수 있다.
5. 공인인증기관은 공인인증서의 이용범위 및 용도, 이용된 기술의 안전성과 신뢰성 등을 고려하여 공인인증서의 유효기간을 적정하게 정하여야 한다.
6. 공인인증서 발급에 따른 신원확인 절차 및 방법 등에 관하여 필요한 사항은 과학기술정보통신부령으로 정한다.

정답 ①