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

1과목 시스템 보안

상 중 하 시스템 보안 > 리눅스 서버 보안

01 다음 보안 도구 중에서 공통적으로 제공하는 공격기능으로 올바른 것을 고르시오.

> John the Ripper
> Wfuzz
> Cain and Abel

① Brute Force 공격을 위한 도구이다.
② 시스템을 스니핑하거나 관리한다.
③ 웹취약점을 도출하고 공격한다.
④ 세션갈취를 통해서 사용자 쿠기 및 세션 정보를 획득한다.

본 문제는 John the Ripper만 보아도 **무작위 공격(Brute Force)**인 것을 식별할 수 있다. John the Ripper는 password.txt와 같은 패스워드 파일을 입력으로 해서 패스워드를 알 수 있다. 하지만 password.txt에 등록된 것이 없으면 알아낼 수 없다.

정답 ①

상 중 하 시스템 보안 > 운영체제 이해 및 관리

02 다음은 컴퓨터 시스템에서 인터럽트 처리 순서이다. 올바른 것을 고르시오.

> ㄱ. 현재 실행 중인 프로그램을 PC(Program Counter)에 저장한다.
> ㄴ. 수행했던 작업으로 복귀한다.
> ㄷ. CPU가 인터럽트를 식별한다.
> ㄹ. 인터럽트 처리 루틴을 실행한다.

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

인터럽트는 CPU가 인터럽트를 식별하면 현재 작업 중인 내용을 프로그램 카운터(Program Counter)에 저장하고 인터럽트 처리루틴을 실행 후 원래의 작업으로 복귀한다.

정답 ②

상 중 하 시스템 보안 > 윈도우 클라이언트 및 서버 보안

03 MBR(Master Boot Record)에 대한 설명으로 올바르지 않은 것은?

① MBR은 디스크에서 첫 번째 섹터에 위치한다.
② MBR은 시스템 부팅과 관련된 정보를 가지고 있다.
③ MBR은 파티션마다 존재한다.
④ MBR은 부트 로더를 포함하고 있다.

MBR은 파티션 테이블을 기점으로 부트섹터를 읽어 운영체제를 기동하는 영역으로 부트로더(Boot Loader)를 포함하고 있다.

MBR의 역할

- 부트 파티션을 파티션 테이블에서 검색한다.
- 시작 섹터(Sector)를 검색한다.
- 부트 파티션에서 시작섹터의 복사본을 메모리로 로드한다.
- 부트 섹터의 실행코드 전송을 관리한다.

MBR은 장치관리자에서 디스크 드라이브의 속성을 확인하면 되고 속성에서 볼륨, 정보표시를 클릭하면 확인할 수 있다.

정답 ③

상 중 하 시스템 보안 > 윈도우 클라이언트 및 서버 보안

04 휘발성 데이터에 대한 디지털 포렌식 수행 시 증거 데이터 수집 순서로 올바른 것을 고르시오.

① Register → 메모리 → 임시파일 → 디스크
② 메모리 → Register → 임시파일 → 디스크
③ 디스크 → 임시파일 → 메모리 → Register
④ 디스크 → 메모리 → 임시파일 → Register

운영체제 계층구조를 생각하면 답을 알 수 있다. CPU, 메모리, 디스크의 순으로 이루어진 것이 운영체제 계층구조이고 CPU 내에 있는 작고 빠른 고속의 메모리가 Register이다. 따라서 Register, 메모리(주기억장치), 임시파일, 디스크 순으로 증거를 확보해야 한다.

정답 ①

05 매일 8시 30분에 /usr/logrepost.sh를 실행하고 크론(Cron)을 설정하고자 한다. 다음 중 가장 올바른 것을 고르시오.

① * * * 08 30 /usr/logrepost.sh
② 30 08 * * * /usr/logrepost.sh
③ 08 30 * * * exec /usr/logrepost.sh
④ * 08 30 * * exec /usr/logrepost.sh

Crontab은 분, 시, 일, 월 순으로 설정하기 때문에 30분 08시를 설정하고 일과 월은 매일, 매월이므로 *로 설정한다.

crontab 설정

- crontab 파일 구문(syntax)은 "minute hour day_of_month month weekday command"
- minute(분) : 0~59 / hour(시) : 0~23 / day_of_month(일) : 1~31 / month(월) : 1~12 weekday(요일) : 일요일부터 토요일까지(0~6) / command(명령) : 실행 명령
- crontab 사용 예제(구조 : 분 시 일 월 요일 명령어)
- 30 * * * * /home/user/limbest
  (무조건 30분에 맞추어 limbest를 실행)
- */10 * * * * /home/user/limbest
  (무조건 10분마다 limbest를 실행)
- *10/ 2-5 * * * /home/user/limbest
  (2시부터 5시까지 10분마다 실행)

정답 ②

06 공격자는 시스템을 해킹한 후 백도어를 설치했다. 공격자가 설치한 백도어는 리눅스 시스템이 부팅될 때마다 자동으로 실행된다. 다음 중 어떤 파일을 변경해야 하는지 고르시오.

① /etc/inittab
② /etc/contab
③ /etc/system
④ /etc/rc.d/rc.local

부팅 시 자동으로 실행되므로 리눅스 Run Level에 설정해야 한다. Run Level 설정 파일은 /etc/rc.d/rc.local에 있다.

실행단계	내용
0	PROM 감사단계
1	관리상태의 단계로 사용자 로그인의 접근이 불가능한 단일 사용자단계로 여러 개의 파일 시스템이 로드(Load)되어 있음
2	공유된 자원을 가지지 않은 다중 사용자단계
3	기본 실행단계로 공유 자원을 가진 다중 사용자단계
4	현재 사용되지 않음
5	Run level 3로 기동되고, X-Windows를 기동함
6	재부팅 단계로 실행단계 3의 상태로 재부팅
S, s	여러 개의 파일 시스템이 로드(Load)되어 원격 사용자 로그인 접근이 불가능한 단일 사용자단계

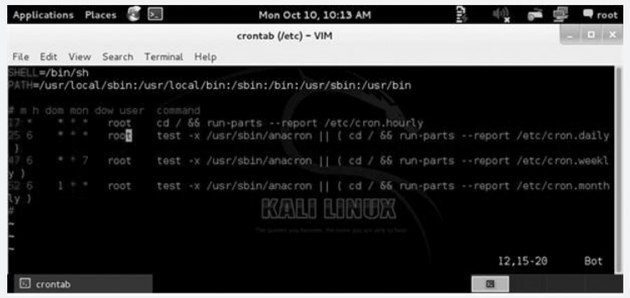
정답 ④

07 다음은 crontab에 대한 설명이다. 올바르지 않은 것을 고르시오.

① 정기적으로 작업을 실행할 수 있다.
② 주간, 월간 단위로 일자를 지정하여 실행한다.
③ crontab에 대한 로그는 /etc/default/cron 파일에 저장한다.
④ /etc/crontab 파일에 작업을 설정한다.

crontab은 정기적으로 작업을 실행하는 것이다. 그리고 crontab에 대한 로그는 /var/log/cron에 저장된다. 유닉스 및 리눅스에서 /etc 디렉터리에는 설정 파일이 있고 /var 디렉터리는 로그파일을 가지고 있다.

/etc/crontab 파일 구조



정답 ③

08 윈도우 cmd 명령으로 실행한 명령어 목록이 기록되어 있는 레지스트리 키로 올바른 것은 무엇인가?

① Favorites
② Recent File List
③ RunMRU
④ Recent Docs

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU는 실행한 명령 히스토리 정보를 가지고 있다. 위의 경로에서 Explorer는 사용자가 실행한 프로세스에 대한 정보를 가지는 것이다.

정답 ③

09 윈도우 레지스트리 중에서 실행 드라이버 설정과 관련한 레지스트리 키는 무엇인가?

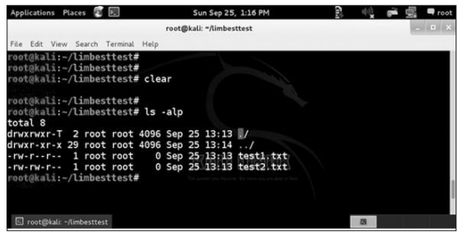
① HKEY_CURRENT_USER
② HKEY_LOCAL_MACHINE
③ HKEY_USERS
④ HKEY_CURRENT_CONFIG

HKEY_LOCAL_MACHINE는 현재 설치된 하드웨어 및 드라이버에 대한 정보를 저장하고 있는 것으로 프린터, 인터넷 시리얼 포트 설정 등에 대한 정보를 가지고 있다.

정답 ②

상 중 하 시스템 보안 > 리눅스 서버 보안

10 다음 내용을 보고 파일을 삭제할 수 없는 이유를 고르시오.



① 같은 그룹 ID를 가지고 있는 사용자라서 test2.txt 파일을 삭제할 수 없다.
② sticky bit가 설정되어 있어서 test2.txt 파일을 삭제할 수 없다.
③ test2.txt 파일에 대한 Other User의 권한은 읽기만 가능하므로 삭제할 수 없다.
④ root 사용자가 아니라서 삭제할 수 없다.

test2.txt 파일은 rw-rw-r--으로 설정되어 있어서 다른 사용자(Other User)는 파일을 읽기만 가능하고 삭제할 수는 없다.

정답 ③

상 중 하 시스템 보안 > 리눅스 서버 보안

11 다음은 xferlog 파일에 대한 설명이다. 올바르지 않은 것을 고르시오.

```
Thu Apr 8 15:40:32  2016 1 201.1.1.10  254   /usr/kisa.z  b_o r test ftp 0 *  c
```

① test 사용자로 인증받아서 ftp에 연결된 사용자이다.
② 파일 전송 크기는 254이다.
③ 전송된 파일은 /usr/kisa.z 파일이고 인증된 사용자에 의해서 전송되었다.
④ c는 전송 실패를 의미한다.

전송 상태에서 c는 전송 성공 i는 전송 실패를 의미한다.

xferlog 파일 구조

구분	설명
접근 날짜 및 시간	Thu Apr 8 15:40:32 2016 1
접속 IP	201.1.1.10
전송 파일 Size	254
전송 파일	/usr/kisa.z
파일 종류	b(Binary) 혹시 a이면 ASC II
행위	_ (아무 일도 수행하지 않음)
파일 동작	O (파일을 받았음)
사용자 접근 방식	r (인증된 사용자)
로그인 ID	test
인증 방법	0
전송 형태	c (전송 성공)

정답 ④

상 중 하 시스템 보안 > 리눅스 서버 보안

12 다음은 로그파일에 대한 설명이다. 올바르지 않은 것은?

① wtmp 로그파일은 현재 로그인한 사용자의 상태 정보를 가지고 있는 로그파일이다.
② utmp는 현재 로그인한 사용자의 정보를 기록한다.
③ pacct는 사용자가 실행한 명령 정보를 가지고 있다.
④ btmp 파일은 로그인에 성공한 정보를 가지고 있다.

btmp 파일은 **실패한 로그인 정보**를 담고 있는 파일로 /var/log/btmp에 존재한다.

정답 ④

상 중 하 시스템 보안 > 윈도우 클라이언트 및 서버 보안

13 다음 보기에서 설명하고 있는 악성코드의 종류는 무엇인가?

웹 사이트 방문 시 자동으로 다운로드되어서 감염시킨다. 사용자의 개인정보를 사용해서 금품을 요구하는 악성코드이다.

① Phishing
② 랜섬웨어
③ APT
④ Watering Hole

랜섬웨어는 사용자의 파일 및 개인정보를 암호화시켜서 금품을 갈취하는 악성코드이다.

정답 ②

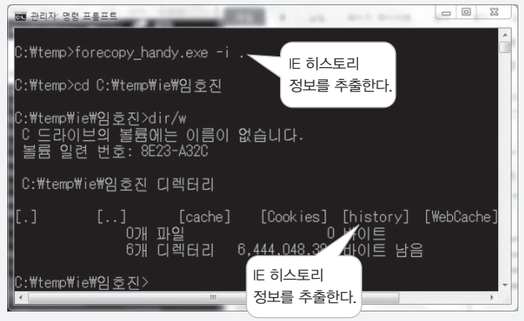
상 중 하 시스템 보안 > 윈도우 클라이언트 및 서버 보안

14 인터넷 익스플로러 History 정보는 어디에 보관되어 있는가?

① history.dat
② his.dat
③ index.dat
④ log.dat

인터넷 익스플로러 접속로그는 index.dat 파일에 존재한다.

index.dat 파일추출



정답 ③

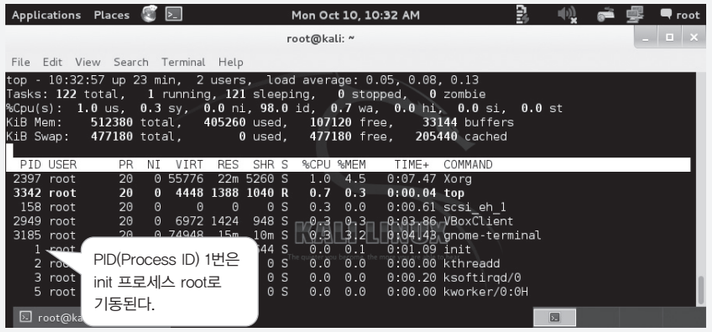
상 중 하 시스템 보안 > 리눅스 서버 보안

15 리눅스에서 PID 1을 가지고 있는 프로세스는 무엇인가?

① init
② inetd
③ cron
④ syslogd

리눅스 시스템이 부팅되면 swap 프로세스가 기동되어 디스크에 있는 리눅스 이미지를 주기억장치에 적재(Load)한다. 이후 init 프로세스가 기동되는데 init 프로세스는 프로세스 ID 1번을 가지고 자식 프로세스를 생성한다. 자식 프로세스는 fork 명령을 실행해서 inetd와 같은 프로세스를 기동한다.

top를 사용하여 init 프로세스 확인



정답 ①

상 중 하 시스템 보안 > 리눅스 서버 보안

16 다음은 백도어에 대한 대응책 설명이다. 올바르지 않은 것을 고르시오.

① 주기적으로 해시 값을 저장하여 해시 값을 확인한다.
② 네트워크 NIC 카드를 Promiscuous 모드로 변경한다.
③ 개발 보안을 준수하여 백도어가 설치될 수 없도록 한다.
④ 백도어 프로세스를 주기적으로 검사하여 확인한다.

백도어(Backdoor)는 공격자가 다음에 침입을 쉽게 하기 위해서 심어둔 악성코드이다. 주기적으로 실행 권한이 있는 파일과 특수 권한 파일을 검사하거나 파일의 해시 값을 확인해야 한다.
백도어 프로그램은 원격으로 접속하여 공격자의 명령어를 실행해야 하므로 Socket 통신 프로그램을 하나 만들어서 심어둔다. 그러면 공격자는 Backdoor 프로그램을 호출하여 시스템에 침투한다.

정답 ②

backdoor 프로그램 구조

```
if ((sockfd = socket (AF_INET, SOCK_STREAM, 0)) < 0);
  bzero (&servaddr, sizeof (servaddr));
  servaddr.sin_family = AF_INET;
  servaddr.sin_port = htons (4000);
  servaddr.sin_addr.s_addr = htonl (INADDR_ANY);

  if (bind (sockfd, (sddr *) & servaddr, sizeof (servaddr)) < 0);
  if (listen (sockfd, LOG) < 0);
  for (;;) {
    if ((connfd = accept (sockfd, (sddr *) NULL, NULL)) < 0)
      continue;
  }
```

상 중 하 시스템 보안 > 리눅스 서버 보안

17 다음은 홍길동 계정(ID hong)에 대한 정보이다. 올바르지 않은 것을 고르시오.

① 사용자 계정 ID는 hong이고 패스워드는 shadow 파일에 저장되어 있다.
② UID와 GID는 1001, 1002이다.
③ 사용자 셸(Shell)은 /bin/csh를 실행한다.
④ 사용자 디렉터리는 /home/hong이다.

/etc/passwd 필드에 대한 문제이다. hong 계층은 /bin/false로 설정되어 있어서 셸(Shell)을 실행하지 않게 되어 있다.

정답 ③

18 커널 이벤트 /var/log/emerg.log에 대해서 /etc/syslog.conf에 추가하는 것으로 올바른 것은?

① *.emerg /var/log/emerg.log
② *.* /var/log/emerg.log
③ kern.emerg /var/log/emerg.log
④ emerg – kern /var/log/emerg.log

syslog.conf에 커널 이벤트를 등록하기 위해서는 kern을 사용하고 로그 수준인 emerg 키워드를 사용해서 설정한다.

정답 ③

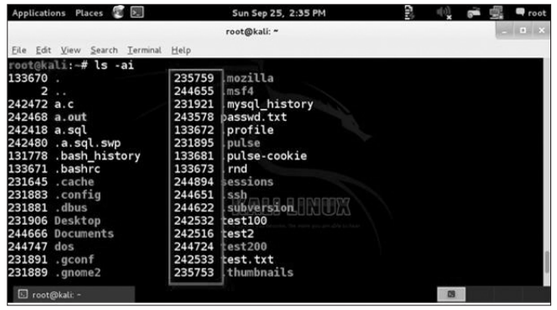
19 Ping of Death를 방지하기 위한 커널 옵션 설정으로 올바른 것은 무엇인가?

① sysctl –w netipv4.icmp_echo_ignore_all = 0
② sysctl –w netipv4.icmp_echo_ignore_all = 1
③ sysctl –w netipv4.icmp_echo_ignore_broadcast = 0
④ sysctl –w netipv4.icmp_echo_ignore_broadcast = 1

sysctl –w netipv4.icmp_echo_ignore_all = 1은 ICMP(Ping)을 차단하고 sysctl –w netipv4.icmp_echo_ignore_all = 0은 ICMP를 허용한다.

정답 ②

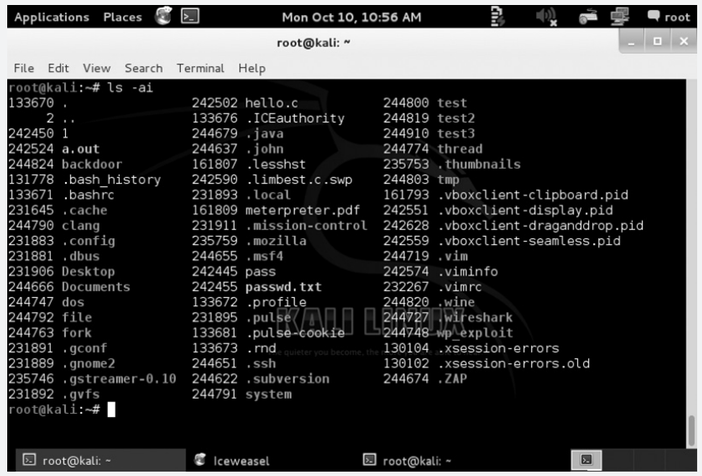
20 ls –ai를 실행한 결과이다. 체크한 부분의 의미로 올바른 것을 고르시오.



① 크기
② inode Number
③ 순서번호
④ 파일 내의 단어 수

ls 명령에서 i 옵션은 inode에 대한 정보를 확인하는 것이다.
inode는 파일에 대한 정보를 가지고 있는 것으로 파일형태, 크기, 링크 수 등의 메타데이터를 가지고 있다. Inode의 값을 유일하게 분류하기 위해서 inode number를 보유하고 있다.

ls –ai 실행



정답 ②

2과목 네트워크 보안

상 중 하 네트워크 보안 > 네트워크 활용(TCP/IP 구조)

21 TTL 값은 라우터를 통과할 때마다 감소된다. TTL 값이 0이 될 때 ICMP에서 발생되는 메시지(Message)로 올바른 것을 고르시오.

① Destination unreachable
② Time exceeded
③ Parameter problem
④ Timestamp request and reply

IP 프로토콜의 필드에는 TTL 필드가 있고 TTL은 통과할 수 있는 라우터 수를 의미하며 기본 값은 운영체제별로 다르게 설정된다. IP 패킷이 라우터를 통과하면 TTL의 값은 TTL = TTL – 1이 되어서 감소한다. 이 때 TTL이 0과 같아지면 더 이상 IP 패킷은 라우터를 통과하지 못하고 폐기된다. TTL이 0이 되어서 IP 패킷이 폐기되면 ICMP 프로토콜은 Time Exceeded(시간 초과) 오류 메시지를 송신자에게 전송한다.

정답 ②

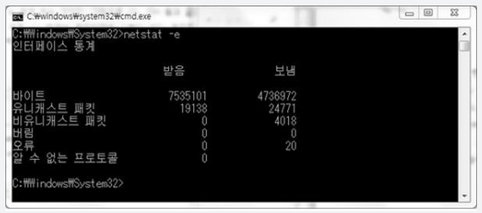
상 중 하 네트워크 보안 > 네트워크 대응 기술 및 응용

22 다음은 윈도우에서 netstat 명령을 실행한 결과이다. Netstat의 옵션으로 가장 알맞은 것은 무엇인가?

① –a
② –e
③ –f
④ –n

netstat 명령은 네트워크의 상태를 확인하는 명령어로 윈도우와 리눅스 모두에서 제공하는 명령어이다.
–e 옵션은 이더넷(Ethernet) 통계정보를 제공하는 기능과 일반적으로 –s 옵션인 프로토콜별 통계 옵션이 같이 사용된다.

netstat –e 실행



–a 옵션은 모든 연결 및 수신 대기 포트를 표시하고 –n 옵션은 주소와 포트 번호를 숫자로 표시한다.

정답 ②

상 중 하 네트워크 보안 > 네트워크 대응 기술 및 응용

23 전문가 시스템에서 사용하는 IDS 탐지 기법으로 올바른 것은 무엇인가?

① 행위기반 탐지 기법
② 상태기반 탐지 기법
③ 지식기반 탐지 기법
④ 통계기반 탐지 기법

오용탐지(Misuse)는 미리 정의된 Rule에 매칭해서 침입을 탐지하는 것으로 시그니처(Signature) 기반, 지식(Knowledge) 기반이라고도 한다. 오용탐지에 사용되는 기술은 패턴비교, 전문가 시스템(Expert System)이 있다.

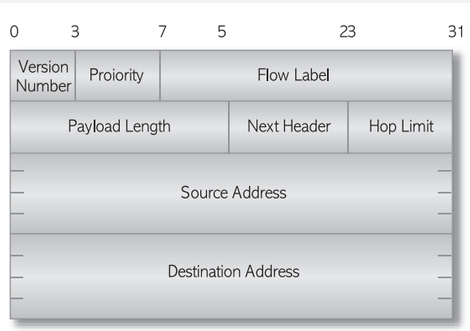
정답 ③

상 중 하 네트워크 보안 > 네트워크 활용(TCP/IP 구조)

24 다음은 IPv6에 대한 설명이다. IPv6의 특징으로 올바르지 않은 것은?

① IPv6는 IPv4의 주소부족 문제를 해결하기 위해서 주소공간을 확장했다.
② IPv4 헤더에서 4개의 헤더를 삭제하고 다른 필드를 추가해서 총 8개의 필드로 이루어져 있다.
③ IPv6는 QoS(Quality of Service) 기반으로 네트워크를 효율적으로 사용한다.
④ IPv6는 확장필드에 보안옵션을 추가할 수 있다.

IPv6 헤더는 총 8개의 필드로 구성된다.



IPv6는 보안이 옵션이 아니라 기본적으로 IPSEC을 지원한다. 옵션으로 지원한 것은 IPv4이다.

정답 ④

상 중 하 네트워크 보안 > 네트워크 활용(TCP/IP 구조)

25 다음 보기에서 설명하고 있는 네트워크 활용(TCP/IP 구조)으로 올바른 것은 무엇인가?

> 엔드포인트 보안, 접근 제어, 인증, 백신관리, 패치관리, 무결성 관리를 수행한다.

① NAC
② NMS
③ ESM
④ UTM

NAC(Network Access Control)는 엔드포인트(End Point) 보안 장치로 정당한 사용자만 네트워크에 연결되어서 네트워크를 사용할 수 있도록 하는 보안 솔루션이다. 이러한 기능을 네트워크 무결성 기능이라고 한다.

정답 ①

상 중 하 네트워크 보안 > 네트워크 대응 기술 및 응용

26 IDS 탐지 기법에서 공격자의 공격 패턴을 미리 정의하고 해당 공격과 같으면 침입을 탐지하는 기법은 무엇인가?

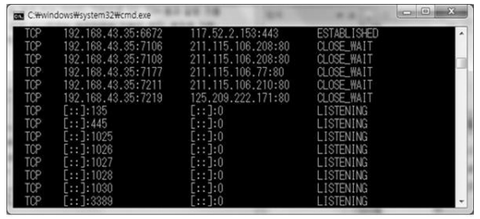
① 시그니처 기반 탐지 기법
② 이상기반 탐지 기법
③ 통계기반 탐지 기법
④ 시간기반 탐지 기법

시그니처(Signature) 기반이란 공격패턴을 저장하고 공격패턴과 동일한 것을 발견하면 침입으로 식별하는 것으로 오용탐지(Misuse Detection)라고도 한다.

정답 ①

상 중 하 네트워크 보안 > 네트워크 대응 기술 및 응용

27 Windows 7의 cmd 창에서 netstat –an을 실행한 결과이다. 다음 중 클라이언트와 연결된 IP 주소는 무엇인가?



① 192.168.43.35
② 211.115.106.208
③ 117.52.2.153
④ 125.209.222.171

TCP 상태전이 값에서 ESTABLISHED는 클라이언트와 서버 간에 연결이 확립되어 있음을 의미한다.

TCP 상태값(netstat 출력 내용)

- LISTEN : 서버 데몬(Daemon)이 실행되어서 접속을 대기하는 상태
- SYN-SENT : Local 클라이언트 애플리케이션이 원격 호스트에 연결을 요청한 상태
- SYN-RECEIVED : 서버가 원격 클라이언트로부터 접속요구를 받아 클라이언트에게 응답을 요청하였지만 확인 메시지를 받지 않은 상태
- ESTABLISHED : 3-Way Handshaking(TCP 연결방법을 의미)이 완료된 후 서로 연결된 상태
- FIN-WAIT1, CLOSE-WAIT, FIN-WAIT2 : 서버에서 연결을 종료하기 위해서 클라이언트에게 종료 요청을 하고 회신을 받아 종료하는 과정인 상태
- CLOSING : 확인 메시지가 전송 도중 분실된 상태
- TIME-WAIT : 연결은 종료되었지만 느린 메시지를 위해서 연결을 열어 둔 상태
- CLOSED : 완전히 연결이 종료된 상태

정답 ③

상 중 하 시스템 보안 > 리눅스 서버 보안

28 다음 중 무결성 검사 도구로 올바른 것은 무엇인가?

① tripwire
② tcpdump
③ Snort
④ john the ripper

정보보안기사 제1회부터 무결성 점검 도구는 꼭 출제되었다. 그 중에서 가장 많이 출제된 것은 tripwire이고 tripwire는 해시값을 저장한 후 비교하면서 변경여부를 확인하는 도구이다.

정답 ①

상 중 하 정보보안 일반 > 접근 통제

29 다음 중 인증 시스템의 구성요소가 아닌 것은?

① 인증 메커니즘
② 접근 제어 메커니즘
③ 식별 특성
④ 방화벽

방화벽(Firewall)은 특정 IP 주소, 포트, 애플리케이션 등을 등록하여 차단하는 시스템으로 외부에서 내부로 유입되는 패킷(Packet)을 차단하는 Inbound 필터링과 내부에서 외부로 유출되는 Outbound 필터링을 수행하는 보안 솔루션이다.

정답 ④

상 중 하 네트워크 보안 > 네트워크 활용(TCP/IP 구조)

30 SIEM과 관련이 없는 것을 고르시오.

① QRader
② SPLUNK
③ ArcSight
④ EnCase

- SIEM 솔루션은 IBM의 큐레이더(QRader), HP의 아크사이트(ArcSight), 스플렁크(SPLUNK) 빅데이터를 활용하여 데이터를 분석하는 솔루션이다.
- EnCase는 SIEM과 관련 없는 포렌식 분석 도구이다.

정답 ④

상 중 하 네트워크 보안 > 네트워크 대응 기술 및 응용

31 다음 중 VPN 터널링 기법이 아닌 것은 무엇인가?

① PPTP
② RTP
③ IPSEC
④ SSL

RTP(Real Time Protocol)는 UDP를 사용하여 데이터를 빠르게 전송하는 프로토콜로 VoIP에서 사용한다. RTP는 신뢰성 전송을 위해서 RTCP라는 에러 처리 프로토콜과 함께 사용되며 RTCP도 UDP로 사용해서 에러 제어를 한다.

정답 ②

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

32 다음 중 VoIP 공격으로 올바르지 않은 것을 고르시오.

① 레지스터 플러딩
② RTP 공격
③ Invite 공격
④ Get Flooding

VoIP Flooding은 VoIP 메시지인 INVITE, OPTIONS, REGISTER 등의 메시지를 사용한다. Get Flooding은 HTTP DDoS 공격 기법으로 Get 신호를 유발하여 공격을 수행한다.

VoIP 공격	설명
INVITE 서비스 거부 공격	대기 중인 상대방이 INVITE Method를 전송
BYE Method 서비스 거부 공격	• 사용자 BYE Method 패킷을 전송하여 통화를 방해하는 공격 • 통화는 끊어지지 않지만 통화품질이 저하됨

정답 ④

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

33 Syn Flooding 설명으로 올바르지 않은 것은?

① TCP의 3-Way Handshaking 기법을 사용해서 공격하는 기법이다.
② 클라이언트가 Syn 신호를 발생시킴으로써 서버 버퍼의 부하를 유발한다.
③ netstat 명령을 사용하여 특정 IP에서 발생되는 Syn 수를 분석함으로써 탐지가 가능하다.
④ SSL을 사용하면 Syn Flooding이 발생하지 않는다.

SSL은 전송구간 암호화 기법으로 전송 과정에 발생되는 데이터를 암호화하여 전송한다. 하지만 Syn Flooding은 특정 데이터 값을 변경하는 것이 아니기 때문에 암호화를 수행해도 Syn Flooding 공격은 가능하다.

정답 ④

상 중 하 네트워크 보안 > 네트워크 대응 기술 및 응용

34 다음은 IPSEC VPN에 대한 설명이다. 그 내용으로 옳은 것은?

① AH는 메시지에 대해서 암호화를 수행하여 안정적으로 데이터를 전송한다.
② ESP는 메시지에 대한 무결성과 인증 기능을 제공한다.
③ IPSEC VPN은 메시지에 대한 암호화와 인증을 수행하고 기본적으로 IPv4에 탑재되어 있다.
④ SA는 암호화 알고리즘과 매개변수를 정의한다.

SA(Security Association)는 SPI라는 SA 파라미터가 들어 있고 인덱스, 목적지 IP, 보안 프로토콜 식별자 등으로 구성된다.

정답 ④

삼 중 하 네트워크 보안 > 네트워크 대응 기술 및 응용

35 다음은 VPN 모드이다. 올바른 것은 무엇인가?

ㄱ	New IP	ESP AH	IP
ㄴ	IP	ESP AH	Payload

	ㄱ	ㄴ
①	전송모드	터널모드
②	터널모드	전송모드
③	터널모드	SA
④	IKE	전송모드

터널모드는 새로운 IP를 붙여서 **기존 IP 헤더까지 모두 보호하는 것**이고, 전송모드는 데이터는 암호화하지만 기존 IP 헤더를 그대로 사용하는 것이다.

정답 ②

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

36 다음은 DDoS 대응절차이다. 올바른 것을 고르시오.

ㄱ. 초동대응
ㄴ. 공격탐지
ㄷ. 모니터링
ㄹ. 상세분석
ㅁ. 차단

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

금융보안연구원 DDoS 공격 대응 절차
1단계(모니터링), 2단계(공격탐지), 3단계(초동조치), 4단계(공격분석), 5단계(공격차단)

정답 ①

삼 중 하 네트워크 보안 > 네트워크 대응 기술 및 응용

37 응용 게이트웨이(Application Gateway) 방화벽에 대한 설명 중 바르지 않은 것은?

① 패킷 필터링에 비해서 높은 수준의 필터링을 수행한다.
② 모든 응용 프로그램의 프록시는 한 개의 프록시만을 경유한다.
③ 프록시를 통해서 시스템에 접근 가능하게 한다.
④ 방화벽 기능이 우수하다.

프록시는 데이터베이스 및 서버 등에 접근할 때 경유하는 시스템으로 프록시에서 정당한 사용자인지를 확인하고 권한을 확인한다.

정답 ②

삼 중 하 네트워크 보안 > 네트워크 활용(TCP/IP 구조)

38 access-list 설정의 예이다. 그 해석으로 올바른 것은?

```
Router# config t
Router(config)# access-list   2  deny 130.100.0.0   0.0.255.255
Router(config)# access-list   2  permit   any
Router(config)# exit
```

① 130.100.0.0/16으로 들어오는 모든 패킷을 거부한다.
② 저장되지 않았으므로 실행되지 않는다.
③ 포트 번호를 1024 이후로 하면 연결할 수 있다.
④ 130.100.0.0으로 유입되는 패킷을 허용한다.

- 접근 통제 번호가 1~99번이면 Standard Access List를 선언하는 것으로 Source IP 주소만 확인하여 허용하거나 거부한다.
- 130.100.0.0/16으로 들어오는 모든 패킷을 거부한다.

정답 ①

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

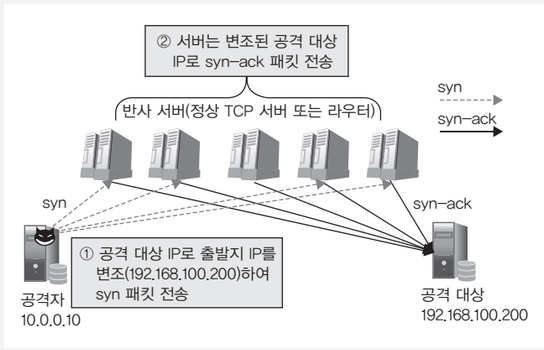
39 다음 지문에서 설명하는 DDoS 공격 기법은 무엇인가?

별도의 Agent가 필요 없이 TCP 프로토콜을 사용하여 피해자에게 TCP SYN 신호를 전송함으로써 부하를 유발하는 공격 기법이다.

① Get Flooding
② DDoS
③ DRDoS
④ HTTP Read Dos

DRDoS는 별도의 Agent를 설치하지 않고 TCP Half Open의 취약점을 이용하는 공격 기법이다.

DRDoS 진행 방법



아래의 C코드는 필자가 만든 코드이다. C언어에서 tcp.h 헤더 파일을 포함시켜서 개발한 것으로 RAW 소켓을 사용했다. 그 내용을 보면 tcpheader → dest는 목적지의 IP 주소로 syn 패킷을 전송할 IP 주소가 되고 tcpheader → src에 공격자의 IP 주소를 보내지 않고 피해자의 IP 주소를 전송하여 DRDoS 공격을 수행하는 것이다.

DRDoS 구현

```
tcpheader → src      = htons(atoi(argv[2]));
tcpheader→ dest      = htons(atoi(argv[3]));
tcpheader → seq      = htonl(0);
tcpheader → syn      = 1; // SYN 신호를 발송함
tcpheader → dof      = sizeof(struct tcphdr) >> 2;
tcpheader → windows  = htons(8192);
```

정답 ③

상 중 하 네트워크 보안 > 네트워크 대응 기술 및 응용

40 다음 중 Snort 헤더에 포함되지 않은 필드는 무엇인가?

① Direction
② Action
③ Protocol
④ 메타 데이터

Snort 헤더는 패킷을 처리하는 방법을 정의하는 action, 프로토콜의 종류를 선택하는 Protocol, 포트를 결정하는 Port, 패킷의 방향을 나타내는 Direction, 룰 옵션을 설정하는 Option으로 구성된다.

정답 ④

3과목 애플리케이션 보안

상 중 하 애플리케이션 보안 > 기타 애플리케이션 보안

41 다음 중 버퍼 오버플로(Buffer Overflow)와 관련이 없는 것을 고르시오.

① Stack
② Segment fault
③ 하트블리드
④ Open Stack

오픈스택(Open Stack)은 클라우드 운영체제의 하나로 클라우드 컴퓨팅에서 자원관리를 수행하는 Nova와 VM(Virtual Machine)을 관리하는 Glance, 파일 시스템을 관리하는 Swift, 보안 인증을 수행하는 Keystone, 스토리지 볼륨관리를 위한 Cinder, 네트워크 관리를 하는 Quantum, 인터페이스를 관리하는 Horizon으로 구성되어 있다.
Stack은 지역변수와 매개변수를 저장하고 함수 복귀주소(Return Address)를 가지고 있어서 버퍼 오버플로를 유발시키고 Segment Fault는 특정 프로세스가 메모리를 잘못 참조할 때 운영체제에서 발생시키는 인터럽트이다. 하트블리드는 OpenSSL이 가지는 보안 취약점을 사용해서 64Byte의 평문을 노출시킨다.

정답 ④

상 중 하 애플리케이션 보안 > 전자상거래 보안

42 SET에서 지불 게이트웨이(Payment Gateway) 역할을 수행하는 것은 무엇인가?

① Cardholder
② Merchant(Web Server)
③ Merchant(은행)
④ Issuer

SET의 구성은 다음과 같다. 하지만 문제에는 지불 게이트웨이가 별도로 나와 있지 않기 때문에 답이 애매하다.

구성	설명
고객(Cardholder)	물품 혹은 서비스를 구매하는 자
판매자(Merchant)	인터넷상에서 상품이나 서비스를 제공하는 자
발급사(Issuer)	고객의 카드발급 금융기관 혹은 결제카드 소지인의 계좌가 개설되어 있는 금융기관
매입사(Acquirer)	판매자의 가맹점 승인 금융기관, 판매자의 계좌가 개설되어 있는 금융기관
지급정보 중계기관 (Payment Gateway)	판매자가 요청한 고객의 지급정보를 해당 금융기관에 승인 및 결제를 요청하는 기관
인증기관 (Certification Authority)	고객 및 판매자 등의 참여기관이 신뢰할 수 있는 전자적 인증기관

정답 ②

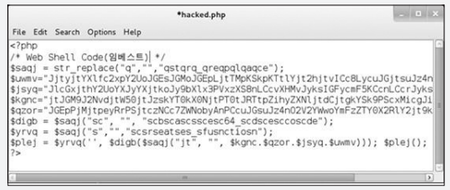
상 중 하 애플리케이션 보안 > 기타 애플리케이션 보안

43 일반적으로 업로드 취약점을 사용하는 공격형태는 무엇인가?

① CSRF
② 웹셸(Web Shell)
③ SQL Injection
④ XSS

파일 업로드 취약점이 발생되면 웹셸을 업로드하여 원격으로 시스템에게 명령을 수행할 수 있다. 그래서 업로드 취약점이 발생되는 시스템을 공격자가 통제할 수 있게 된다. 즉, 다음의 코드와 같은 형태를 게시판을 통해서 업로드하고 localhost/hack.php를 호출하여 서버에 명령을 실행시킬 수 있다.

웹셸(Web Shell)



웹셸(Web Shell) 업로드

정답 ②

삼 중 하 애플리케이션 보안 > 전자상거래 보안

44 OTP 중에서 동기화된 인증 횟수를 사용하는 OTP 인증 기법은 무엇인가?

① 시간 동기화
② 이벤트 동기화
③ S/Key 방식
④ 비동기식 기법

OTP(One Time Pad)는 난수를 생성하여 인증에 사용하는 방법으로 **동기식 방식과 비동기식 방식**으로 구분된다. 동기식 방법에는 시간 동기화와 이벤트 동기화 방법이 있다. **시간 동기화 방식은 은행(Bank)에서 사용**하는 방법으로 시간 정보를 활용해서 난수를 생성하며, 이벤트 동기화는 인증 횟수를 사용해서 인증을 수행하는 방법이다.

정답 ②

삼 중 하 애플리케이션 보안 > 기타 애플리케이션 보안

45 다음 중 웹 서비스(Web Service) 공격유형과 거리가 먼 것은?

① Blind SQL Injection
② RFI 공격
③ XSS
④ LAND Attack

- LAND Attack : 송신자의 IP와 수신자의 IP를 동일하게 하여 전송함으로써 IP 패킷이 자신에게 되돌아오는 공격 기법
- RFI(Remote File Inclusion Vulnerability) **취약점 : 악성 스크립트를 서버에 전송하여 해당 웹 페이지에서 악성코드가 실행되게 하는 것으로 자신의 코드에 악성코드를 삽입.** 즉, $_GET, $_POST, $_cookie으로 전달되는 입력 값을 검증하지 않아서 발생하는 문제점으로 전달되는 파라미터인 TEST=http://www.exmple.com/webshell.txt 등으로 전달하여 악성코드를 실행시킴

정답 ④

삼 중 하 애플리케이션 보안 > 인터넷 응용 보안

46 전자우편 보안에서 X.509 형식의 전자서명을 하는 것은 무엇인가?

① PGP
② PEM
③ MIME
④ S/MIME

S/MIME(Secure for Multipurpose Internet Mail Extensions)은 디지털 서명, 메시지 암호화를 수행하는 전자우편 보안 기술로 디지털 서명은 MIME 데이터 서명, X.509 인증서 기반의 인증, 부인방지 기능을 제공한다.

정답 ④

삼 중 하 애플리케이션 보안 > 기타 애플리케이션 보안

47 게시판에 악성 스크립트를 삽입해서 쿠키, 개인정보 전송, 악성코드 다운로드 등을 수행할 수 있는 공격 기법은 무엇인가?

① Web Shell
② XSS
③ CSRF
④ SQL Injection

XSS는 게시판에 악성스크립트를 삽입하여 공격을 수행하는 것이다.

XSS 대응 방법

1. 정규식(패턴) 데이터만 입력
2. XSS 필터링만 사용
3. 출력 값에 대해 HTML 인코딩 적용(동작하지 않도록)
4. 출력 값에 대해 XSSFilter를 적용하여 안전하지 않은 입력 값에 대해 HTML 인코딩 적용

정답 ②

삼 중 하 애플리케이션 보안 > 인터넷 응용 보안

48 다음 FTP에 대한 설명 중 올바른 것을 고르시오.

① FTP Passive Mode는 cmd 포트(21)에 PASV 명령어를 입력한다.
② FTP Passive Mode는 22번 포트를 통해서 변경한다.
③ FTP는 cmd 포트(21)번으로 데이터를 전송하고 명령을 처리한다.
④ FTP는 cmd 포트(20)번을 사용해서 명령을 전송하고 서버가 포트를 결정해주면 명령과 데이터를 송수신한다.

FTP Passive Mode는 cmd 21번 포트에 PASV 명령을 전송하여 수행된다. FTP의 Active Mode와 Passive Mode는 매번 출제되는 주제이므로 반드시 알고 있어야 한다.

정답 ①

삼 중 하 애플리케이션 보안 > 기타 애플리케이션 보안

49 소프트웨어 보안약점에서 입력 값 검증 및 표현 부분과 관련이 없는 것을 고르시오.

① SQL Injection
② 운영체제 명령어 삽입
③ XSS
④ 경쟁조건

개발보안 항목 중에서 입력 값 표현 및 검증은 SQL 삽입, 경로조작 및 자원 삽입, 운영체제 명령어 삽입, 위험한 형식 파일 업로드, 신뢰되지 않은 URL로 자동접속 연결, Xquery 삽입, Xpath 삽입, LDAP 삽입, 크로스사이트 요청 위조, HTTP 응답분할, 정수형 오버플로, 보안 기능 결정에 사용되는 부적절한 입력 값, 메모리 버퍼 오버플로, 포맷팅 스트링 공격이 있다.
시간 및 상태에는 검사시점과 종료되지 않은 반복문 또는 재귀함수 취약점이 있고 경쟁조건은 시간 및 상태 보안 취약점에 해당된다.

정답 ④

상 중 하 정보보안 일반 > 보안 요소 기술

50 다음 중 커버로스의 특징으로 올바르지 않은 것은?

① 티켓서버와 인증 서버로 구분되어서 인증을 수행한다.
② 재생공격을 방지한다.
③ 타임스탬프가 필요 없다.
④ 티켓서버는 사용자를 확인하고 인증 서버는 티켓을 통하여 인증을 수행한다.

재생공격(Replay Attack)이란 기존 티켓을 재사용해서 공격을 수행하는 것이다. 이것을 방지하기 위해서는 타임스탬프 정보가 필요하다.

정답 ③

상 중 하 애플리케이션 보안 > 기타 애플리케이션 보안

51 다음 핑거프린트에 대한 설명 중 올바르지 않은 것은?

① 구매자와 판매자 정보를 모두 디지털 콘텐츠에 삽입하여 불법유통을 방지하는 기술이다.
② 일종의 정보은닉 기술로 구매자와 판매자 정보를 분리해서 저장한다.
③ 구매자 정보와 판매자 정보를 삽입하면 구매자별로 콘텐츠가 다르다.
④ 불법유통 발생 시 디지털 콘텐츠에서 구매자 정보를 획득하여 추적할 수 있다.

핑거프린트는 워터마킹(Watermarking) 기술 중 하나로 구매자 정보와 판매자 정보를 삽입하는 Dual Watermarking을 제공하고 불법유통을 방지하기 위해서 사용된다. 구매자 정보와 판매자 정보가 삽입되었다고 구매자별로 제공받는 디지털 콘텐츠가 다른 것은 아니다.

정답 ③

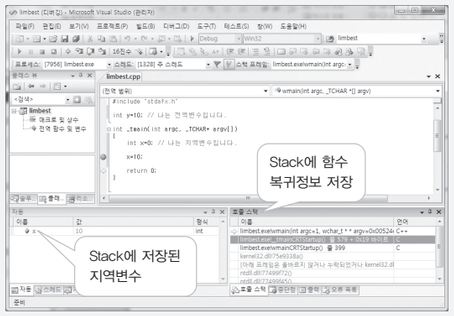
상 중 하 애플리케이션 보안 > 기타 애플리케이션 보안

52 프로세스에서 지역변수와 매개변수를 저장하는 공간은 무엇인가?

① Stack Area
② Heap Area
③ Data Area
④ Text Area

함수 내부에서 사용하는 변수가 지역변수이고 매개변수는 함수를 호출할 때 사용하는 호출 값이다. 즉, 지역변수와 매개변수는 모두 스택(Stack) 영역에 저장된다.

Stack 영역 확인



정답 ①

상 중 하 애플리케이션 보안 > 기타 애플리케이션 보안

53 다음 exploit 코드 취약점에 대한 대응방법은 무엇인가?

```
#include <stdio.h>
char buf[]=" \xec\x9a\xb0\xec\x82\xb0\xec\xa7\x80\xec\x88\x\xec\x9a\xb0\xec\x82\xb0\xec\
xa7\ x80\xec\x88\x\xec\x9a\xb0\xec\x82\xb0\xec\xa7\x80\xec\x88\x\xec\x9a\xb0\xec\x82\
xb0\xec\xa7\x80\xec\x88\x\xec\x9a\xb0\xec\x82\xb0\xec\xa7\x80\xec\x88\x\xec\x9a\xb0\
xec\x82\xb0\xec\xa7\x80\xec\x88\x\xec\x9a\xb0\xec\x82\xb0\xec\xa7\x80\xec\x88\x\xec\x9a\
xb0\xec\x82\xb0\xec\xa7\x80\xec\x88\x\xec\x9a\xb0\xec\x82\xb0\xec\xa7\x80\xec\x88\x  "
void main(void)
{
 char msg[20];
 memset(meg, 0x00, sizeof(msg));
strcpy(msg,   buf);
}
```

① memset() 함수를 삭제하여 exploit 공격을 차단할 수 있다.
② 경계 값 검사를 제공하는 컴파일러 및 링커를 사용한다.
③ char msg[20]의 버퍼 크기를 msg[30]으로 변경함으로써 예방할 수 있다.
④ 백신 프로그램을 설치하고 운영하면 발생되지 않는다.

버퍼 오버플로(Buffer Overflow) 공격은 메모리 내의 경계 값을 넘어서는 공격으로 컴파일러가 경계 값 검사를 수행함으로써 차단할 수 있다.
위의 예에서 buf 변수 내에 저장되어 있는 이상한 문자열은 무엇일까? 기계어 코드를 의미하는 셸코드(Shell code)이다.

정답 ②

삼 중 하 애플리케이션 보안 > 기타 애플리케이션 보안

54 SDLC(소프트웨어 개발 생명주기) 모델에서 원형모델에 대한 설명으로 올바르지 않은 것은?

① 소프트웨어 개발단계에서 사용자 요구사항 식별 및 검증이 가능한 장점이 있다.
② 사용자에게 사용자 요구사항이 어떻게 구현되는지 사전에 알 수 있다.
③ 제품의 일정표, 작업명세서 등을 제공하지 않는다.
④ 소프트웨어 신뢰성이 낮고 성능이 저하된다.

본 문제는 원형이라는 한글로 출제되었고 원형의 해석이 폭포수, 프로토타이핑, 나선형 모델 모두가 될 수 있다. 영문명을 주지 않아서 어느 정도 문제를 풀 때 혼동될 수는 있지만 ①번과 ②번 지문을 통해서 원형(Prototyping) 모델이라는 것을 판단해야 한다. **프로토타이핑 모델은 사전에 사용자 요구사항을 검증함으로써 소프트웨어의 신뢰성이 향상**된다.

폭포수 모델

특징	문제점
• 하향식 접근(Top-down), 순차적 모형 • 표준화 된 양식과 문서 중심 프로세스 • 정형화 된 산출물을 가장 중요시하는 모형 • 간단하며 고전적인 모형	• 사용자 요구사항에 대한 반영과 확인이 어려움 • 단계별 완전성으로 인하여 불필요한 문서작업이 많음 • 개발 도중에 변경에 대한 처리가 어려움

프로토타이핑 모형(Prototyping Mode)의 장점과 단점

구분	내용
장점	• 사용자 요구사항 도출이 용이 • 시스템에 대한 이해가 용이하고 소프트웨어 품질 향상 • 개발자와 사용자 간에 의사소통 원할 • 개발 타당성 확인 • 실행 가능한 프로토타입을 통해서 확인
단점	• 프로토타입을 최종 완제품으로 오인 • 기대심리를 유발하여 과다한 요구사항 혹은 변경이 발생 • 비경제적, 중간 단계 산출물 문서화가 어려움

정답 ④

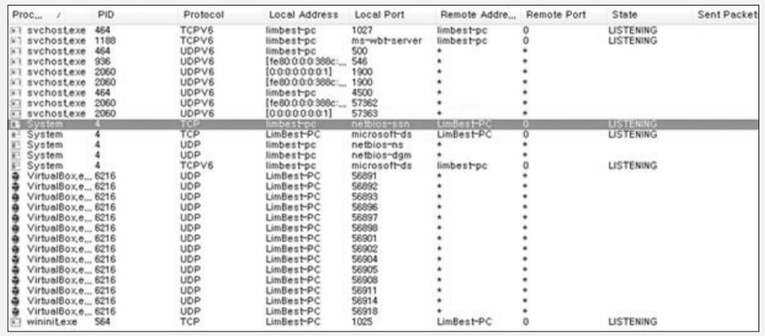
삼 중 하 네트워크 보안 > 네트워크 대응 기술 및 응용

55 다음 중 포맷 스트링과 관련이 없는 것은?

① gdb
② ltrace
③ objdump
④ tcpdump

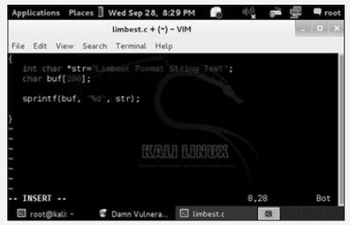
tcpdump는 스니핑 도구이고 포맷 스트링과 전혀 관련이 없다. **포맷 스트링(Format String) 공격은 printf(), sprint(), fprintf() 함수를 사용할 때 데이터 타입을 잘못 지정해서 발생되는 보안 취약점**이다.

TCP dump 실행 모습



다음과 같은 문자열을 정수형 데이터 타입으로 출력할 때 발생되는 취약점이 포맷 스트링 취약점이다. 즉, 데이터 타입이 일치하지 않을 때의 취약점이다.

포맷 스트링(Format String) 취약점



정답 ③

삼 중 하 애플리케이션 보안 > 기타 애플리케이션 보안

56 다음 HTTP 1/1 상태코드에 대한 설명으로 올바르지 않은 것은?

① 404 Forbidden
② 503 Service Unavailable
③ 302 Found
④ 204 No Content

HTTP 404는 Not Found 상태코드 값으로 클라이언트가 요청한 자원이 서버에 존재하지 않음을 의미한다.

정답 ①

삼 중 하 애플리케이션 보안 > 기타 애플리케이션 보안

57 다음 중 SSO의 장점이 아닌 것은?

① 중앙집중적인 관리와 인증을 수행한다.
② 관리비용이 절감된다.
③ 사용자 편의성이 증가한다.
④ 시스템의 부하를 발생시킨다.

- 솔루션 부분의 문제는 답이 무엇이라고 명확하게 판단하기 어렵다. 하지만 이 문제에서 답을 찾는다면 ④번으로 생각된다.
- SSO는 통합인증을 수행하며, 통합인증으로 개별 시스템에서 인증을 수행하지 않아도 되므로 사용자 편의성이 증가한다. 중앙집중적인 관리와 인증을 수행하는 것이다.

정답 ④

삼 중 하 애플리케이션 보안 > 기타 애플리케이션 보안

58 다음은 CSRF에 대한 설명이다. 괄호 안에 알맞은 것을 넣으시오.

CSRF는 (ㄱ)보다 (ㄴ) 방식을 사용하고 인증 시 서버가 클라이언트에게 (ㄷ)을 넘겨준다. 인증된 사용자가 서비스를 요청할 경우 (ㄹ)을 통해서 (ㅁ)을 수행한다.

① (ㄱ) GET (ㄴ) POST (ㄷ) 토큰 (ㄹ) 세션 (ㅁ) 재인증
② (ㄱ) POST (ㄴ) GET (ㄷ) 토큰 (ㄹ) 세션 (ㅁ) 재인증
③ (ㄱ) GET (ㄴ) POST (ㄷ) 세션 (ㄹ) 토큰 (ㅁ) 재인증
④ (ㄱ) POST (ㄴ) GET (ㄷ) 세션 (ㄹ) 재인증 (ㅁ) 토큰

CSRF는 요청에 대해 서버가 실제 페이지 서비스를 통해서 전달된 요청인지 확인하지 않고 요청을 처리하는 경우 발생한다.

CSRF 대응 방법

대응 방법	키포인트
• GET이 아닌 **POST 방식을 사용** • **CSRF 토큰**을 사용해서 URL 조작을 하지 못하도록 함 • 추가 인증 및 다중매체 인증 방식을 사용	• 서버에서 토큰을 생성해서 히든 필드로 클라이언트 전송 • **CAPTCHA를 이용**한 사용자 인증 처리(컴퓨터인지 사용자인지 확인)

CSRF 토큰

```
// Check Anti-CSRF token
// 파라미터 값을 읽기 전에 토큰을 체크함으로써 정상적인 클라이언트의 요청인지 확인한다.
   checkToken( $_REQUEST[ 'uwer_token' ],   $_SESSION[ 'session_token' ], 'limbest.php' );

// Get input
    $pass_curr = $_GET[ 'password_current' ];
      $pass_new = $_Get[    'password_new' ];
```

정답 ①

삼 중 하 애플리케이션 보안 > 기타 애플리케이션 보안

59 버퍼 오버플로 방지를 위해서 set noexec_user_stack=1, set noexec_user_stack_log=1을 설정할 수 있는 파일은 무엇인가?

① /etc/sysconf
② /etc/system
③ /etc/inetd.conf
④ /etc/services

/etc/system 파일은 시스템 관련 설정 정보를 가지고 있는 파일이며 버퍼 오버플로를 방지하기 위해서 set noexec_user_stack=1, set noexec_user_stack_log=1을 설정한다. 이 설정의 의미는 Stack 공간에서 프로그램이 실행되지 않도록 설정하는 noexec_user_stack_log라는 로그를 기록하는 것이다.

정답 ②

삼 중 하 애플리케이션 보안 > 기타 애플리케이션 보안

60 다음 중 DRM과 거리가 먼 것은?

① Watermark
② 핑거프린트
③ Watering Hole
④ DOI

Watering Hole은 APT 공격 기법 중 하나로 **신뢰한 사이트에 악성코드를 유포하고 특정 사용자가 접속했을 때 악성코드를 배포하는 공격**이다. 즉, 표적기반 공격 기법이다. Spear Phishing, Watering Hole, Drive by download 공격은 반드시 같이 학습해야 한다.

정답 ③

상 중 하 정보보안 일반 > 암호화

61 다음 중 타원곡선 암호 알고리즘(Elliptic Curve Cryptography)에 대한 설명으로 올바른 것은?

① 타원곡선 상의 점과 원점으로 구성된 점들 사이에 곱셈연산이다.
② RSA에 비해 짧은 키 길이를 사용하면서 훨씬 빠른 구현이 가능하다.
③ 곡선의 점이 크다.
④ ECC 기법은 소인수분해를 사용하여 암호화를 수행한다.

타원곡선(ECC, Elliptic Curve Cryptosgraphy)

- 타원곡선이라 불리는 곡선을 정하고, 그 곡선 상에 있는 점에 대하여 특수한 연산을 정의
- 타원곡선 암호에서는 이 연산의 역연산이 어렵다는 것을 이용
- 대개 실수와 유리수와 같은 유한대 영역에 대해 정의되고 이산대수문제에 대한 아날로그를 구현
- 하나의 곡선
- 무한한 싱글포인트 O를 갖는 = + aX + b 타원곡선의 공간들
- 덧셈은 모듈러 곱셈의 카운터파트
- 곱셈은 모듈러 멱승연산의 카운터파트
- 하나의 타원곡선 상에 주어진 두 지점 P와 R에 대해 K = PR을 만족하는 K를 찾아낸다는 것은 타원곡선 이산대수 문제로 알려진 어려운 문제임
- RSA보다 작은 키 값을 갖고도 높은 보안수준을 이룰 수 있음

정답 ②

상 중 하 정보보안 일반 > 접근 통제

62 다음 중 생체인증의 요구사항의 특성에 해당하지 않는 것은?

① 보편성
② 특수성
③ 영구성
④ 시간의존성

생체인증의 요구사항의 특성에 해당하지 않는 것은 시간의존성이다.

생체인증의 요구사항	설명
보편성	모든 대상자들이 보편적으로 지님
유일성	개개인별로 특징이 확연히 구별
지속성	발생된 특징점은 그 특성을 영속
수집성(취득용이성)	특징점의 취득용이성
성능	개인 확인 및 인식의 우수성
수용성	생체인식 대상자의 거부감이 없어야 함
위 · 변조 가능성	위조내지 변조 불가능

정답 ④

상 중 하 정보보안 일반 > 암호화

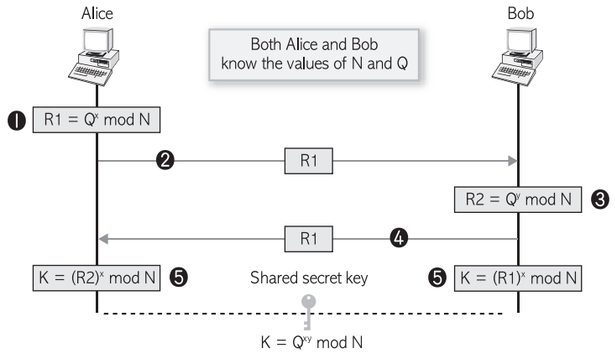
63 다음 중 3단계 정보보호와 관련하여 아래와 같은 절차로 수행되는 것은 무엇인가?

(1) 송신자 A는 소수 P, 그리고 1부터 p-1까지의 정수 q를 선택하여 사전에 수신자 B와 공유
(2) 송신자 A는 정수 a 선택(정수 a는 외부 미공개, 수신자 B도 알 수 없음)
(3) 송신자 A는 $A=q^a \bmod p$, 즉 q^a를 p 로 나눈 나머지를 계산
(4) 수신자 B도 마찬가지로 정수 b를 선택, $B=q^b \bmod p$를 계산
(5) 송신자 A와 수신자 B가 서로에게 A와 B를 전송
(6) 송신자 A가 $B^a \bmod p$, 수신자 B가 $A^b \bmod p$를 계산
(7) 마지막 단계에서 $B^a = (q^b)^a = q^{ab}$, $A^b = (q^a)^b = Q^{ab}$이며, 따라서 $K=q^{ab} \bmod p$ 라는 공통의 비밀키를 공유

① Needham-Schroeder 프로토콜
② 커버로스(Kerberos)
③ RSA(Rivest, Shamir, Adleman)
④ Diffie-Hellman

Diffe-Hellman 방법

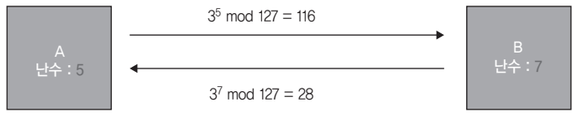
- 송/수신자를 위한 일회용 세션키를 제공
- 데이터를 교환하기 위해 세션키를 사용
- 인터넷을 통한 키 동의
- 전제 조건
  대칭키를 확립하기 이전에 송/수신자는 두 개의 수 N과 Q를 선택
  N : (N-1)/2가 소수라는 제한을 가진 큰 소수, Q : 소수
  N과 Q는 기밀성을 필요로 하지 않음
- Diffie-Hellman 키 공유 절차
  (1) 송신자 A는 소수 P, 그리고 1부터 p-1까지의 정수 q를 선택하여 사전에 수신자 B와 공유
  (2) 송신자 A는 정수 a 선택(정수 a는 외부 미공개, 수신자 B도 알 수 없음)
  (3) 송신자 A는 $A=q^a \bmod p$, 즉 q^a를 p로 나눈 나머지를 계산
  (4) 수신자 B도 마찬가지로 정수 b를 선택, $B=q^b \bmod p$를 계산
  (5) 송신자 A와 수신자 B가 서로에게 A와 B를 전송
  (6) 송신자 A가 $B^a \bmod p$, 수신자 B가 $A^b \bmod p$를 계산
  (7) 마지막 단계에서 $B^a = (q^b)^a = q^{ab}$, $A^b = (q^a)^b = Q^{ab}$이며, 따라서 $K=q^{ab} \bmod p$라는 공통의 비밀키를 공유



송신자 A : p = 127, q = 3, a = 5

수신자 B : p = 127, q = 3, b = 7

일 때 Diffie-Hellman 키공유 계산식을 다음의 그림으로 확인해 보자.

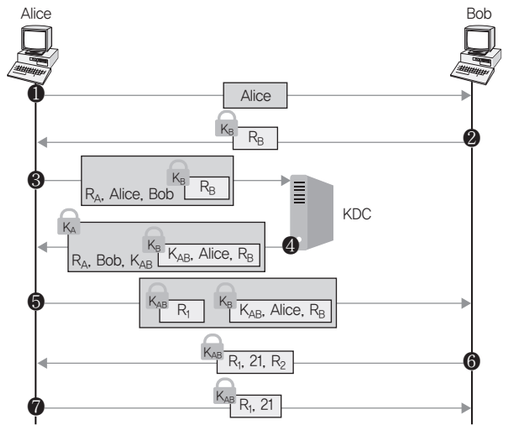


$28^5 \bmod 127$
$= (127*X+28)^5 \bmod 127$
$= (3^7)^5 \bmod 127$
$= 90$

$116^7 \bmod 127$
$= (127*X+116)^7 \bmod 127$
$= (3^5)^7 \bmod 127$
$= 90$

Needham-Schroeder 프로토콜

- 송/수신자간의 완벽한 프로토콜을 얻기 위해서 다중 챌린지-응답(challenge-response)을 사용
- Roger Needham과 Michael Schroeder가 1978년 대칭키와 Trent 개념을 사용하여 제안
- Needham-Schroeder 프로토콜 과정



- 프로토콜 define

  Trent : 인증 서버, A : Alice, B : Bob, K_A : Alice 비밀키, K_B : Bob의 비밀키

  K_S : 세션키, R_A, R_B : 랜덤 넘버
- 프로토콜 분석

  ① Alice → Trent : 앨리스가 밥과 통신하기를 원하여 A, B, R_A를 보냄

  ② Trent → Alice : EA(R_A, B, K, EB(K, A)) : Trent는 랜덤 세션키를 생성하고 그 세션키와 앨리스와 밥의 비밀키로 각각을 암호화하여 앨리스에게 보냄

  ③ EB(K, A) : 앨리스는 메세지와 세션키 k를 구하고 Trent에게 보낸 R_A를 검증한 후 Trent가 밥의 비밀키로 암호화한 메시지를 보냄

  ④ EK(R_B) : 밥은 비밀키로 메시지와 세션키 K를 구하고 또 다른 랜덤 넘버 R_B를 생성하여 세션키 K로 암호화하여 앨리스에게 보냄

(5) EK(R_B-1) : 앨리스는 세션키 K로 메시지를 구하고 R_B-1 랜덤 넘버를 생성하여 세션키 K로 암호화하고 밥에게 보냄

(6) 밥은 세션키 K로 메시지를 구하고 랜덤 넘버 R_B-1을 검증

RSA

- Rivest, Shamir, Adleman이 고안한 큰 소인수 곱 n = p * q 의 소인수 p, q를 찾는 것이 어렵다는 것을 근간으로 만들어진 알고리즘
- 공개키 암호시스템의 하나로, 암호화뿐만 아니라 전자서명이 가능한 최초의 알고리즘

구분	설명	
키쌍	공개키	수 E와 수 N
	개인키	수 D와 수 N
암호화	암호문 = (평문)^E mod N(평문을 E 제곱해서 N으로 나눈 나머지)	
복호화	평문 = (암호문)^D mod N(암호문을 D 제곱해서 N으로 나눈 나머지)	

정답 ④

상 중 하 정보보안 일반 > 암호화

64 다음 중 메시지 인증 코드에 포함되지 않은 것은 무엇인가?

① 무결성, 제3자 인증
② 기밀성, 부인방지
③ 제3자 인증, 부인방지
④ 무결성, 인증

메시지 인증 코드에 포함되지 않은 사항은 제3자에 대한 인증(증명)과 부인방지이다. 메시지 인증 코드란 메시지에 붙여지는 작은 데이터 블록을 생성하기 위해 비밀키를 이용하는 방법이다. 이 기술을 이용하면 전송되는 메시지의 무결성을 확인하여 메시지에 대한 인증을 할 수 있다.

정답 ③

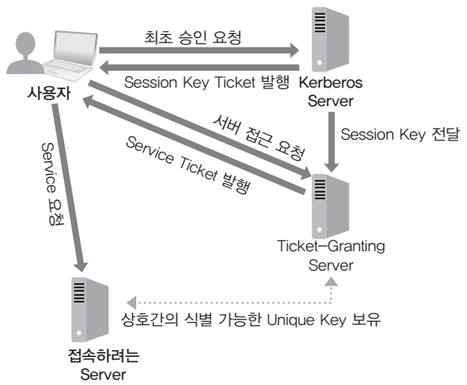
상 중 하 정보보안 일반 > 보안 요소 기술

65 다음 중 커버로스 인증 절차를 순서대로 나열한 것은 무엇인가?

A. 사용자는 User ID와 패스워드를 입력하여 Kerberos server(Active Directory)에 인증 요청을 시도한다.
B. Kerberos server는 ticket granting 서버에 사용자가 입력한 패스워드에 기반하여 만든 session key를 전달한다.
C. Kerberos server(Active Directory)는 사용자가 입력한 패스워드에 기반하여 만든 session key를 사용자에게 전달한다.
D. Kerberos server는 사용자에게 ticket granting 서버에서 발급받은 발행일자, 시간 등이 적혀 있는 ticket을 전달한다.
E. 사용자는 접속하려는 server로 service를 요청한다.

① A, B, C, D, E
② A, C, B, D, E
③ A, B, C, E, D
④ A, C, D, B, E

- 커버로스(Kerberos)는 분산컴퓨팅 환경에서 대칭키를 사용하여 사용자 인증을 제공하는 중앙집중적인 인증(Authentication) 방식으로 미국 MIT의 Athena 프로젝트에서 개발하였다.
- 보기의 커버로스 인증 절차 방식의 순서는 A, B, C, D, E에 해당하며, 인증 절차에 대한 개념도는 다음과 같다.



정답 ①

상 중 하 정보보안 일반 > 접근 통제

66 홍길동 신규 입사자는 조직업무 부서 내 프린터 담당 업무를 담당하고 있다. 기존에 업무 담당자의 권한을 그대로 받아 사용하는 최소 권한 원칙을 적용한 접근 통제 방법은 무엇인가?

① MAC(Mandatory Access Control)
② DAC(Discretionary Access Control)
③ RBAC(Role Based Access Control)
④ HMAC(Horizontal Access Control)

문제에서 설명하고 있는 접근 통제 방식은 RBAC(Role Based Access Control)이다.

역할기반 접근 통제(RBAC : Role Based Access Control)
- 다중 프로로그래밍 환경에서 사용자의 역할에 기반을 둔 접근 통제 방법
- 임의적 접근 통제와 강제적 접근 통제의 단점을 보완한 기법으로 비 임의적 접근 통제라고도 함
- 역할들을 생성해서 역할마다 권한을 준 다음 사용자들에게 각 역할을 부여함
- 규모가 큰 회사에 알맞은 시스템
- 인사이동 등이 잦아도 사용자의 역할만 변경하면 된다는 장점이 있음

정답 ③

상 중 하 정보보안 일반 > 전자서명

67 다음 중 CRL(Certificate Revocation List) 기본 확장자에 포함되지 않은 것은 무엇인가?

① CA 키 고유번호
② 일련번호
③ CRL 발급기관 대체 이름
④ 인증서 발급자

인증서 발급자는 CRL 개체 확장자 영역에 포함되지만, 기본 확장자에는 포함되지 않는다.
※ CRL의 확장자 영역 : 기본 확장자 + 개체 확장자 영역

기본 확장자
- CA키 고유 번호 : CRL에 서명한 키 번호
- 발급자 대체 이름 : CRL 발급자의 대체 이름(e-mail, IP 주소 등)
- CRL 발급자 번호 : **CRL에 대한 일련번호**
- 발급 분배점 : CRL 분배점 이름
- 델타 CRL 지시자 : 최근에 취소된 목록만을 저장한 델타 CRL 지시자

CRL 개체 확장자 영역
- 취소 이유 부호 : 인증서가 취소된 이유
- 명령 부호 : 해당 인증서를 만났을 경우 취해야 할 명령
- 무효화 날짜 : 해당 인증서가 무효화된 날짜
- 인증서 발급자 : 간접 CRL에서의 해당 인증서 발급자

정답 ④

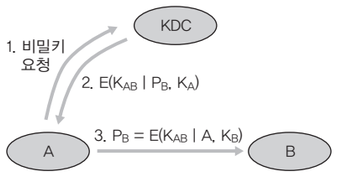
상 중 하 정보보안 일반 > 암호화

68 다음 중 세션키 공유 방법에 대한 설명으로 옳은 것은?

1. 사용자 A는 KDC에 B와 공유할 비밀키 요청
2. A의 신원을 확인한 뒤 $E(K_{AB} | P_B, K_A)$를 A에게 전송 $P_B = E(K_{AB} | A, K_B)$
3. A는 위 암호문을 K_A로 풀어서 K_{AB}를 얻고, P_B를 B에게 전송
4. B는 P_B를 K_B로 풀어서 K_{AB}를 얻음

① RSA(Rivest, Shamir, Adleman) 키 공유
② KDC(key distribution center) 키 공유
③ Diffie-Hellman 키 공유
④ Needham-Schroeder 키 공유

위의 보기는 KDC를 통한 세션키 공유 방법에 대한 설명이다.



정답 ②

상 중 하 정보보안 일반 > 암호화

69 다음 중 랜덤 오라클의 이상적인 해시함수(Hash Function) 특징에 대한 설명으로 틀린 것은?

① 역상 저항성은 h(x) = y를 만족하는 x를 찾는 것이 가능하다.
② 해시함수의 이상적인 수학적 모델이다. 결과 값이 같으면 그대로 쓴다.
③ 생일자 공격은 해시함수의 충돌저항성을 깨고자 하는 공격이다.
④ 충돌저항성은 h(x) = h(x^), x와 x^이 같지 않음을 만족하는 (x, x^)를 찾는 것이 불가능하다.

역상 저항성은 h(x) = y를 만족하는 x를 찾는 것이 불가능하다.

랜덤 오라클 모델

1. 개요 : 해시함수에 대한 이상적인 수학적 모델
2. 비둘기 집 원리
   만약 n + 1마리의 비둘기가 n개의 비둘기 집에 들어가 있다면 적어도 한 비둘기 집에는 두 마리의 비둘기가 들어가 있다는 의미이다. 일반화된 버전은 만약 kn + 1마리의 비둘기가 n개의 비둘기 집에 들어가 있다면 적어도 한 개의 비둘기 집에는 k + 1마리의 비둘기가 들어가 있어야 한다는 원리이다.
3. 생일문제(생일공격)
   특정 해시 값을 생성하는 메시지를 구하는 것이 아니라 해시 값은 뭐든지 괜찮고, 어쨌든 같은 해시 값을 생성하는 2개의 메시지를 구하는 것이다. 생일공격(birthday attack)은 일방향 해시함수의 강한 충돌내성을 깨고자 하는 공격이다.

4. 생일 패러독스
1) 생일퀴즈 : 랜덤으로 N명의 그룹을 생각한다. N명중 적어도 2명의 생일이 일치할 확률이 1/2 이상이 되도록 하기 위하여 N의 최소 숫자는?
   답 : N = 23이다. 이때 확률은 0.507297로 1/2 이상이다.
2) 특정 해시 값을 생성하는 메시지를 구하는 것이 아닌, 해시 값은 상관없이 같은 해시 값을 생성하는 2개의 메시지를 구한다. → 강한 충돌 내성을 깨고자 하는 것
3) N명의 그룹이 있을 때, 적어도 2명의 생일이 일치할 확률이 1/2가 되게 하려면 N은 최소 몇 명이 되어야 하는가?
   답 : n 비트인 h = H(x)가 있을 때, 50% 이상의 확률로 x를 찾으려면 몇 번의 횟수가 필요한가? N = 23일 때 확률이 0.507297

암호학적 해시함수 기준

1. 개요
   암호학적 해시함수는 프리이미지 저항성(preimage resistance), 제2프리이미지 저항성(second preimage resistance), 충돌저항성(collision resistence)의 3가지 기준을 충족해야 한다.
2. 프리 이미지 저항성(역상저항성)
   - 암호학적 해시함수는 프리 이미지 저항성이 있어야 한다.
   - 프리이미지
     f(x) = y에서 x는 y의 이전 이미지라고 한다. f가 일대일 대응이 아니면 하나의 y에 여러 이전 이미지가 있을 수 있다.
   - 프리이미지 저항성이란 주어진 해시함수 h와 y = h(M)에 대해 Eve가 y = h(M')를 만족하는 다른 메시지 M'을 찾아낸다는 것이 매우 힘들어야 한다는 성질이다.
3. 제2프리 이미지 저항성(역상 저항성, 약한 충돌 내성)
   - 메시지를 쉽게 위조할 수 없도록 해야 한다.
   - Eve는 메시지 M과 다이제스트 h(M)을 가로챈다. Eve는 h(M) = h(M')을 만족하는 다른 메시지를 생성한다.
4. 충돌 저항성(강한 충돌 저항성)
   Eve가 동일한 다이제스트를 가지는 2개의 메시지를 구하지 못하도록 하는 것이다. 여기서 공격자는 어떤 정보도 없는 상태에서 동일한 다이제스트를 갖는 2개의 메시지를 생성할 수 있다.

Attack	Value of k with P=1/2	Order
Preimage	$k - 0.69 \times 2^n$	2^n
Second preimage	$k - 0.69 \times 2^n + 1$	2^n
Collision	$k - 1.18 \times 2^{(n/2)}$	$2^{(n/2)}$
Alternate collision	$k - 0.83 \times 2^{(n/2)}$	$2^{(n/2)}$

정답 ①

상 중 하 정보보안 일반 > 전자서명

70 다음 보기의 빈 칸이 알맞게 짝지어진 것은?

> 전자서명과 전송할 문서를 (A)로 암호화 하고, 수신자의 (B)로 암호화한다. 중간자 공격에 대응하기 위하여 (C) 방식을 둔다.

	(A)	(B)	(C)
①	대칭키	공개키	MAC
②	대칭키	공개키	전자서명
③	공개키	대칭키	전자서명
④	공개키	대칭키	MAC

(A) 대칭키, (B) 공개키, (C) 전자서명이다.
전자서명 과정은 정보보안기사에서 가장 중요한 주제이다. 즉, 송신자의 개인키로 전자서명을 하고 송신자의 공개키로 전자서명을 확인한다. 문서(메시지)는 대칭키를 사용하여 암호화를 수행하고 대칭키는 수신자의 공개키로 암호화를 수행한다.

정답 ②

상 중 하 정보보안 일반 > 전자서명

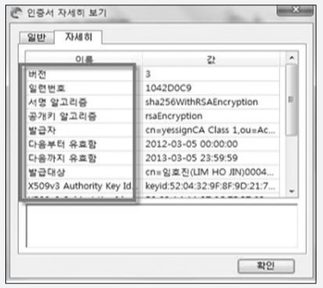
71 다음 중 X.509에 포함되지 않은 것은 무엇인가?

① 인증서 버전
② 일련번호
③ 사용자의 패스워드
④ 서명 알고리즘

X.509v3에 포함되지 않는 것은 사용자의 패스워드이다.

X.509 인증서에 포함된 내용

- 인증서 버전, 인증서 고유번호, 발급자의 서명, 발급자 정보
- 인증서 유효기간, 주체 정보, 공개키, 주체키



- 버전(Version) : X.509의 몇 번째 버전인가
- 일련번호(Serial Number) : 발행하는 CA 내부에서의 유일한 정수값
- 알고리즘 식별자(Algorithm Identifier) : 인증서를 생성하는데 필요한 알고리즘 정보
- 발행자(Issuer) : 인증서를 발행하고 표시하는 CA

정답 ③

- 유효기간(Period of Validity) : 인증서가 유효한 시작과 끝 기간
- 주체(Subject) : 인증서가 가리키는 사람
- 공개키 정보(Public-key Information) : 주체의 공개키와 이 키가 사용될 알고리즘 식별자
- 서명(Signature) : CA의 개인 서명키로 서명한 서명문

〈버전 2에서 추가된 영역〉

- 인증기관 고유 식별자 : 한 주체에 대해 둘 이상의 인증기관으로부터 인증서가 발급된 경우 인증기관 구분
- 주체 고유 식별자 : 주체를 식별하는 값, 예를 들어 같은 회사에 동명이인이 있는 경우 구분하기 위해 사용

〈버전 3에서 추가된 영역〉

- 인증기관 키 식별자 : 하나의 인증기관이 여러 개의 비밀키로 인증서를 발급한 경우 서명 검증용 공개키를 식별하기 위해 사용, SHA-1 해시 값인 KeyIdentifier, 발행기관 이름, 일련번호로 구성
- 주체 키 식별자 : 한 주체가 여러 키 쌍에 대해 발급받은 인증서를 가지고 있을 때 인증서에 포함된 공개키를 구별하는데 사용
- 키 용도 : 해당 공개키가 암호용인지 서명용인지를 해당 비트로 표시
- 비밀키 사용기간 : 인증서의 유효기간과 서명용 비밀키의 사용 시간이 다를 때 사용
- 확장 키 사용 : Key usage 항목으로 표시할 수 없는 세부적인 추가용도를 OID 형태로 표시, TLS 웹 서버 인증용, TLS 웹 클라이언트 인증용, 코드 서명용, 전자 우편용, IPSec용 등을 지시
- CRL 배포 지점 : 폐기한 인증서의 리스트가 저장되어 있는 곳의 URL
- 주체 대체 이름 : DNS 이름, IP 주소, 메일 주소, 커버로스 이름 등 주체 이름에 대한 또 다른 이름
- 발행자 대체 이름 : CA의 또 다른 이름
- 기본 제한 : {CA 플래그, pathLenConstraint로 구성}
- 기관 정보 액세스 : 인증기관이 제공하는 인증서 관련 서비스에 접근할 수 있는 URL이나 프로토콜 관련 정보
- 주체 정보 액세스 : 인증서 주체가 제공할 수 있는 정보와 서비스에 접근하는 방법 제공, 주로 CA의 루트 인증서에 사용

상 중 하 정보보안 일반 > 전자서명

72 다음 중 OCSP(Online Certificate Status Protocol) 프로토콜에 대한 설명으로 틀린 것은?

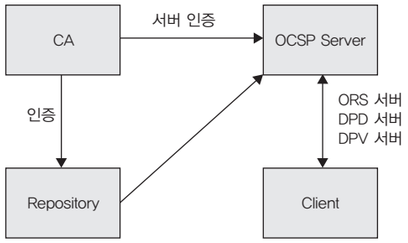
① 온라인 인증서 상태 프로토콜이다.
② 실시간 인증서를 검증할 수 있는 프로토콜이다.
③ CA가 인증서 폐기시 일정주기마다 인증서 취소목록을 생성한다.
④ OCSP 요청/응답 구조는 클라이언트/서버 모델의 정보 조회 구조이다.

③은 CRL에 대한 설명이며, OCSP는 실시간으로 인증서 유효성을 검증할 수 있는 프로토콜로 인증서가 폐기되면 바로 실시간으로 그 폐기상태가 반영된다.

OCSP(Online Certificate Status Protocol)

- **인증서에 대한 사용가능 여부를 실시간으로 검증**하기 위한 프로토콜
- 프로토콜로 인증서가 폐기되면 바로 그 폐기상태가 반영
- OCSP 요청/응답 구조는 클라이언트/서버 모델의 정보 조회 구조
- CRL보다 더 많은 정보를 전달할 수 있음
- HTTP, SMTP, LDAP와 같은 애플리케이션 프로토콜로 전달
- 어떤 인증서가 폐기되었는지에 대한 익명성 제공(CRL은 모든 리스트를 전달)

- OCSP는 RFC 2560을 따름
- OCSP는 특정 CA 기관과 사용계약을 맺어야 하고 사용량에 따라서 추가 비용을 지불
- CA 기관과 계약이 이루어지면 서버 인증서와 개인키가 발급되고, CA 기관의 OCSP Server에 인증서 유효성 요청 시 이 서버용 인증서가 사용됨
- OCSP 동작 절차



- CA 내부에 OCSP Responder가 존재
- OCSP 서버가 CA 내부의 OCSP Responder로 OCSP Request 전송
- 인증서 폐기 여부를 검증
- CA에서 OCSP Server로 OCSP Response 전송

OCSP 구성요소 [제7회 정보보안기사]

- ORS(Online Revocation Status) : OCSP는 클라이언트 온라인 취소 상태 확인 서비스
- DPD(Delegated Path Discovery) : 대리 인증 경로 발견 서비스
- DPV(Delegated Path Validation) : 대리 인증 경로 검증 서비스
- 3가지 상태 및 유효성 검증 서비스를 요구하고 서버가 이 요구 메시지에 대해 응답을 하는 프로토콜

CRL과 비교

구분	OCSP	CRL
정의	실시간 인증서 유효성 검증 프로토콜	인증서에 대한 폐지 목록
표준	RFC 2560	RFC 3280
방식	Online	Batch
정보전달	CRL보다 많은 정보 전달	제한적인 정보 전달

정답 ③

상 중 하 정보보안 일반 > 암호화

73 암호 해독자가 일정량의 평문 P에 대응하는 암호문 C를 알고 있는 상태에서 해독하는 방법이며, 암호문 C와 평문 P의 관계로부터 키 K나 평문 P를 추정하여 해독하는 공격방법은 무엇인가?

① 기지평문공격
② 선택평문공격
③ 암호문단독공격
④ 선택암호문공격

문제에서 설명하는 공격방식은 기지평문공격이다.

암호문 공격방법

암호문 공격방법	설명
암호문 단독 공격 (Ciphertext only attack)	암호 해독자가 암호문 C만을 가지고 평문 P나 키 K를 찾아내는 방법. 평문 P의 통계적 성질, 문장의 특성 등을 추정하여 해독하는 방법
기지 평문 공격 (Known plaintext attack)	암호 해독자가 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 있음. 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 ①

상 중 하 정보보안 일반 > 접근 통제

74 이것은 최초의 수학적 모델로서 보안 등급과 범주를 이용한 강제적 정책에 의한 접근 통제 모델이다. 미 국방성(DOD)의 지원을 받아 설계된 모델로서 오렌지북인 TCSEC의 근간이 되었고, 기밀성 모델로서 높은 등급의 정보가 낮은 레벨로 유출되는 것을 통제하는 접근 통제 모델은 무엇인가?

① 벨라파듈라(Bell-Lapadula) 모델
② 비바(Biba) 모델
③ 만리장성(Chinese Wall) 모델
④ 클락 윌슨(Clark and Wilson) 모델

② 비바(Biba)모델
Bell-Lapadula 모델의 단점인 무결성을 보장할 수 있도록 한 모델이다. 주체에 의한 객체 접근의 항목으로 무결성을 다룬 접근 통제 모델이다.

③ 만리장성(Chinese Wall) 모델
이해충돌(Conflict of interest)이 발생할 수 있는 상업용 응용을 위해 개발되었고, 자유재량과 강제적 접근 개념을 모두 이용한 모델이다. 주로 금융과 법 분야에서 이용된다.

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 접근 가능하다.
- 2가지 무결성 정의 : 내부 일관성(시스템 이용), 외부 일관성(감사에 활용)

클락 윌슨 모델의 무결성 3가지 메커니즘

- 완전한 처리(well-formed transaction) : 데이터는 예측가능하고 완전한 방식으로 조작되어야 함
- 직무 분리(separation of duties) : 한 사람이 모든 권한을 가지는 것을 방지하는 것으로서 정보의 입력, 처리, 확인 등 여러 사람이 나누어 각 부분별로 관리하도록 함으로써 자료의 무결성을 보장(인가자의 비인가된 행동 예방)
- 주체의 응용 프로그램 강제 사용 : 주체가 객체로 직접 접근 금지, 응용 프로그램을 강제 사용하도록 함

정답 ①

상 중 하 정보보안 일반 > 접근 통제

75 **객체의 소유자가 허가하고 싶은 사용자에게만 권한을 부여하며, 접근을 요청한 자의 신원(신분), 사용자 기반의 접근 통제 방식이며, 관리자에 의해 사용자에게 특정 역할을 부여하는 방법은?**

① MAC(Mandatory Access Control)
② DAC(Discretionary Access Control)
③ RBAC(Role Based Access Control)
④ HMAC(Horizontal Access Control)

혼합방식은 DAC와 MAC를 같이 사용하는 RBAC이다.

접근 통제 방식의 특징 비교

구분	DAC	MAC	RBAC
통제기반	주체의 신분 기반	객체에 대한 주체 권한 기반	사용자의 역할 기반
통제주체	객체의 소유자	관리자/시스템	관리자
특징	대부분 O/S 구현	강제적, 복사객체 전파	최소 권한 원칙
장점	구현 용이, 유연성	보안성 높음	그룹 단위, 변경 용이
단점	도용 시 트로이목마에 취약	성능 저하, 구현이 어려움	DAC + MAC
유형	• ACL(Access Control List) : 열 중심 • Capability List : 행중심	• CBP(Compartment Base Policy) • Multi Level Policy	핵심, 계층, 제약, RBAC

정답 ③

상 중 하 정보보안 일반 > 접근 통제

76 **A 기관은 사용자를 인증하는 과정에서 기기 사용자가 누구인가를 확인하지 않고, 해당 기기가 A 기관의 소유인 것을 확인하였다. 이와 같은 방법으로 네트워크에 접속하는 인증 기법은 무엇인가?**

① ID/PW 기반의 인증 방식
② MAC Address 기반의 인증 방식
③ SSID 기반의 인증 방식
④ 공인인증서 기반의 인증 방식

문제에서 설명하고 있는 것은 MAC Address 기반의 인증 방식이다.

정답 ②

상 중 하 애플리케이션 보안 > 전자상거래 보안

77 **SET(Secure Electronic Transaction)에서 고객의 결제정보가 판매자를 통하여 해당 지급정보중계기관(PG)으로 전송될 때 고객의 결제정보가 판매자에게 노출될 가능성과 판매자에 의한 결제 정보의 위 · 변조의 가능성을 제거하기 위하여 사용되는 서명 기법은 무엇인가?**

① 다중서명
② 이중서명
③ 은닉서명
④ 위임서명

① 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 은닉 서명 방식 : D.Chaum에 의해서 제안된 서명 방식. 서명 용지 위에 묵지를 놓아 봉투에 넣어 서명자가 서명문 내용을 알지 못하는 상태에서 서명하도록 한 방식을 수식으로 표현한 것. 즉, 서명문의 내용을 숨기는 서명 방식으로 제공자(provider : 서명을 받는 사람)의 신원과 서명문을 연결시킬 수 없는 익명성을 유지할 수 있음. 전자화폐나 전자투표에 사용

④ 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 > 암호화

78 **아래 보기에서 설명하고 있는 블록 암호화 모드는 무엇인가?**

> 비트 단위의 에러가 있는 암호문을 복호화하면, 1 블록 전체와 다음 블록의 대응하는 비트에서 에러가 발생된다. 최초 키의 생성 버퍼로 IV(Initialization Vector)가 사용되어 첫 번째 블록과 XOR 연산을 통해 암호화 되며, 두 번째 블록부터는 첫 번째 블록의 암호화된 블록과 XOR 연산을 하여 암호화가 진행된다.

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

보기의 내용은 블록 암호화 모드 중 CBC(Cipher Block Chaining)에 해당한다. CBC는 암호문 블록을 마치 체인처럼 연결시키기 때문에 붙여진 이름이다. CBC 모드에서는 1개 앞의 암호문 블록과 평문 블록의 내용을 뒤섞은 다음 암호화를 수행한다.

블록 암호화 모드의 장단점 비교

모드	장점	단점
ECB (Electric Codebook)	• 간단 • 고속 • 병렬 처리 가능(암/복호화 양쪽)	• 평문 속의 반복이 암호문에 반영 • 암호문 블록의 삭제나 교체에 의한 평문조작 가능 • 비트 단위의 에러가 있는 암호문을 복호화하면 대응하는 블록이 에러 • 재생공격 가능
CBC (Cipher Block Chaining)	• 평문의 반복은 암호문에 반영되지 않음 • 병렬 처리 가능(복호화만) • 임의의 암호문 블록을 복호화 할 수 있음	• 비트 단위의 에러가 있는 암호문을 복호화하면 1블록 전체와 다음 블록의 대응하는 비트가 에러 • 암호화에서는 병렬 처리 불가능
CFB (Cipher FeedBack)	• 패딩 불필요 • 병렬 처리 가능(복호화만) • 임의의 암호문 블록을 복호화 할 수 있음	• 비트 단위의 에러가 있는 암호문을 복호화하면 1블록 전체와 다음 블록의 대응하는 비트가 에러 • 암호화에서는 병렬 처리 불가능 • 재생공격이 가능
OFB (Output Feedback)	• 패딩이 필요 없음 • 암호화/복호화의 사전 준비가능 • 암호화와 복호화가 같은 구조를 하고 있음 • 비트 단위의 에러가 있는 암호문을 복호화하면 평문에 대응하는 비트만 에러	• 병렬 처리를 할 수 없음 • 능동적 공격자가 암호문 블록을 비트 반전시키면 대응하는 평문 블록이 비트 반전
CTR (CounTeR)	• 패딩이 필요 없음 • 암호화/복호화의 사전 준비 가능 • 암호화와 복호화가 같은 구조를 하고 있음 • 비트 단위의 에러가 있는 암호문을 복호화하면 평문의 대응하는 비트만 에러 • 병렬 처리 가능(암/복호화 양쪽)	능동적 공격자가 암호문 블록을 비트 반전시키면 대응하는 평문 블록이 비트 반전

정답 ①

상 중 하 정보보안 일반 > 암호화

79 선택 평문 공격 기법으로 두 개의 평문 블록들의 비트 차이에 대응되는 암호문 블록들의 비트 차이를 이용하여 사용된 암호키를 찾아내는 방법은 무엇인가?

① 선형공격(Linear Cryptanalysis)
② 차분공격(Differential Cryptanalysis)
③ 통계적 분석
④ 수학적 분석

1) 선형공격(Linear Cryptanalysis)
1993년 Malsu가 개발하였으며 평문 공격 기법. 알고리즘 내부의 비선형 구조를 적당히 선형화시켜 키를 찾는 방법
2) 통계적 분석(Statistical Analysis)
암호문에 대한 평문의 각 단어 빈도에 관한 자료를 포함하며 지금까지 알려진 모든 통계적인 자료를 이용하여 해독하는 방법
3) 수학적 분석(Mathematical Analysis)
통계적인 방법을 포함하며 수학적 이론을 이용하여 해독하는 방법
4) 전수키조사법(Exhaustive Key Search)
1977년 Diffile-Hellman이 제안한 방법으로 암호화할 때 일어날 수 있는 모든 가능한 경우에 대하여 조사. 경우의 수가 적을 때는 가장 정확한 방법이며 경우의 수가 많을 때는 실현 불가능

정답 ②

상 중 하 정보보안 일반 > 암호화

80 SHA(Secure Hash Algorithm)-512 암호화 과정에 대한 설명으로 괄호 안에 해당하는 것은 무엇인가?

SHA(Secure Hash Algorithm)-512는 (A)bit짜리 패딩된 메시지가 N개 있을 때 각각의 메시지를 블록으로 표현한다. 첫 번째 압축함수에는 맨 처음 블록 (A)bit와 초기 해시 값을 이용하여 512bit를 출력하고 이를 반복하여 Message Digest를 생성한다. 압축 함수의 내부에서는 512bit 초기 해시 값을 8개로 쪼개고 패딩 메시지의 (B)bit 만큼과 함께 라운드를 반복한다. 해시 결과 값 길이는 (C)이다. 이것은 정보보안의 기본 특성 중 (D)을 방지한다.

	(A)	(B)	(C)	(D)
①	1024	80	512	무결성
②	512	80	512	기밀성
③	512	64	512	기밀성
④	1024	64	512	무결성

보기에 들어갈 SHA-512의 암호화 과정은 (A) 1024, (B) 80, (C) 512, (D) 무결성이다.

해시함수 강도 비교

알고리즘	해시 값 크기	내부 상태 크기	블록 크기	길이 한계	워드 크기	과정 수	사용되는 연산	충돌
SHA-0	160	160	512	64	32	80	+, and, or, xor, rotl	발견됨
SHA-1	160	160	512	64	32	80	+, and, or, xor, rotl	공격법만 존재
SHA-256/224	256/224	256	512	64	32	64	+, and, or, xor, shr, rotr	–
SHA-512/384	512/384	512	1024	128	64	80	+, and, or, xor, shr, rotr	–

정답 ①

5과목 정보보안 관리 및 법규

상 | 중 | 하 정보보안 관리 및 법규 > 정보보호 관리

81 다음 보기에서 설명하고 있는 위험분석 기법은 무엇인가?

> 전문가 집단의 의견과 판단을 추출하고 종합하기 위해서 동일한 전문가 집단에게 설문조사를 실시하여 의견을 정리하는 분석방법이다. 짧은 시간에 결과를 도출할 수 있기 때문에 시간과 비용이 절약되지만 전문가의 추정이라 정확도가 낮다는 단점이 있다.

① 과거 자료 분석법
② 델파이 기법
③ 시나리오법
④ 순위 결정법

보기에서 설명하고 있는 위험분석 기법은 정성적 위험분석 기법 중 델파이 기법에 대한 설명이다.

위험분석 기법

1) 정성적 위험분석 기법
- **델파이법** : 전문가 집단의 의견과 판단을 추출하고 종합하기 위해서 동일한 전문가 집단에게 설문조사를 실시하여 의견을 정리하는 분석 방법. 짧은 시간에 도출할 수 있기 때문에 시간과 비용이 절약되지만 전문가의 추정이라 정확도가 낮다는 단점이 있음
- **시나리오법** : 어떠한 사실도 기대대로 발생하지 않는다는 조건 하에서 특정 시나리오를 통하여 발생 가능한 위협의 결과를 우선순위로 도출해 내는 방법. 적은 정보를 가지고 전반적인 가능성을 추론할 수 있지만 발생 가능성의 이론적 추측에 불과하여 정확성이 낮음
- **순위 결정법** : 비교 우선순위 결정표에 위험 항목들의 서술적 순위를 결정하는 방식. 위험의 추정 정확도가 낮다는 단점이 있음

2) 정량적 위험분석 기법
- **과거 자료 분석법** : 과거자료를 통하여 위험 발생 가능성을 예측하는 방법. 이는 과거에 대한 자료가 많으면 많을수록 분석의 정확도가 높아지는 반면에 과거의 사건이 미래에서 발생이 낮아질 수 있는 환경에 대해서는 적용이 어려움
- **수학 공식 접근법** : 과거 자료 분석법이 어려울 경우 사용되는 방법이며 위협 발생빈도를 계산하는 식을 이용하여 위험을 계량화 함. 기대손실을 추정하는 자료의 양이 적다는 것이 단점
- **확률 분포법** : 미지의 사건을 확률적으로 편차를 이용하여 최저/보통/최고 위험평가를 예측하는 방법. 추정하는 것이라 정확도가 낮음

정답 ②

상 중 하 정보보안 관리 및 법규 > 정보보호 관리

82 다음 보기에서 설명하고 있는 것은 무엇인가?

> 조직의 정보를 체계적으로 관리하고 정보보안 사고를 예방하기 위해 영국의 BSI(British Standards Institute ; 영국표준협회)에서 표준으로 제정하였다. 이 인증 기준은 추후 ISO 27000 시리즈로 발전되어 현재는 ISO 27000 정보보호 관리 체계를 구성하게 되었다.

① ITSEC(Information Technology Security Evaluation Criteria)
② TCSEC(Trusted Computer System Evaluation Criteria)
③ CC(Common Criteria) 인증
④ BS7799

보기에서 설명하는 것은 BS7799이다. 정보보호관리체계(ISMS)를 최초로 구축하기 시작한 영국에서 BS7799를 개발하였다. **BS7799는 BSI(British Standards Institute ; 영국표준협회)에서 1998년부터 시행한 ISMS 인증 제도**이며, 이 중에서 인증 기준인 BS 7799 Part1(실무규약)과 Part2(인증 요건)는 국제표준인 ISO 27000 시리즈로 발전되어 현재는 ISO27000 정보보호 관리체계를 구성하게 되었다.

BS7799 구성

구성	설명
BS7799 Part1	정보보안 관리에 대한 실행지침 • 참조문서로 사용할 수 있음 • 정보보안 관리에 대한 포괄적인 세트 제공 • 현 사용중인 최상의 정보보안 실행지침 • 10개의 section으로 구성 • 심사 및 인증으로의 사용은 불가
BS7799 Part2	• 정보보안 관리시스템 문서화 수립실행에 대한 요구사항 규정 : 개별 조직의 필요성에 따라 실행될 수 있는 보안관리 요건을 규정

정보보안 평가체계

평가체계	설명
ITSEC	• 1991년 5월 유럽 국가들이 발표한 공동 보안 지침서 • TCSEC이 기밀성만을 강조한 것과 달리 무결성과 가용성을 포괄하는 표준안을 제시 • TCSEC과 호환을 위한 F-C1, F-C2, F-B1, F-B2, F-B3(TCSEC의 C1, C2 등과 같음)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 평가
TCSEC	• 운영체제나 보안 솔루션이 보안 측면에서 받을 수 있는 가장 기본적인 인증 • 흔히 Orange Book이라고 부르며, Rainbow Series라는 미 국방부 문서 • 1960년대부터 시작된 컴퓨터 보안 연구를 통하여 1972년에 그 지침이 발표됨 • 1983년에 미국 정보 보안 조례로 세계에 최초로 공표되었고 1995년에 공식화
CC 인증	CCRA(CC Recognition Agreement : 상호인정 협정 국가) 가입국 간의 보안 제품에 대한 상호인증을 제공하는 보안 제품 평가 국제기준으로 TCSEC와 ITSEC를 통합한 모델

정답 ④

상 중 하 정보보안 관리 및 법규 > 정보보호 관리

83 다음 중 위험분석 기법에 대한 설명으로 틀린 것은 무엇인가?

① 기준선접근법(BaseLine approach) : 모든 시스템에 대하여 표준화된 보안대책의 세트를 체크리스트 형태로 제공하여 분석의 비용과 시간이 절약된다는 장점이 있으나 과보호 또는 부족한 보호가 될 가능성이 상존한다.
② 상세 위험분석 기법(Detail Risk analysis) : 조직의 자산 및 보안 요구사항을 구체적으로 분석하여 가장 적절한 대책을 수립할 수 있으나 시간과 노력이 많이 소요된다.
③ 복합 접근법(Combined approach) : 고위험 영역을 식별하여 이 영역의 상세 위험분석을 수행하고 다른 영역은 베이스라인 접근법을 이용하는 등 혼합형 방식을 적용한다.
④ 비공식 접근법(Informal approach) : 사전에 위험분석 방법의 선택 이전에 상위 수준의 위험 분석을 수행하여 위험분석의 방법 및 상세 위험분석의 대상이 될 영역을 식별하여야 한다.

④는 복합 접근 방법에 대한 설명이다.

비공식 접근법(Informal approach)

- 구조적인 방법론에 기반하지 않고 경험자의 지식을 사용하여 위험분석을 수행하는 것
- 이 방식은 상세 위험분석보다 빠르고 비용이 덜 듦
- 특정 위험분석 모델과 기법을 선정하여 수행하지 않고 수행자의 경험에 따라 중요 위험 중심으로 분석
- 작은 규모의 조직에는 적합할 수 있으나 새로이 나타나거나 수행자의 경험분야가 적은 위험영역을 놓칠 가능성이 있음
- 논리적이고 검증된 방법론이 아닌 검토자의 개인적 경험에 지나치게 의존하므로 사업 분야 및 보안에 전문성이 높은 인력이 참여하여 수행하지 않으면 실패할 위험이 있음

정답 ④

상 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

84 다음 중 중앙행정기관의 장이 소관분야의 정보통신기반시설 중 주요정보통신기반시설로 지정하기 위하여 고려하여야 할 사항의 연결이 올바른 것은?

1. 당해 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성
2. 기관이 수행하는 업무의 정보통신기반시설에 대한 (A)
3. 다른 정보통신기반시설과의 (B)
4. 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 (C)
5. 침해사고의 발생가능성 또는 그 복구의 (D)

	(A)	(B)	(C)	(D)
①	영향도	상호보완성	경제성	편의성
②	의존도	상호연계성	경제성	용이성
③	위험도	상호보완성	피해규모 및 범위	편의성
④	의존도	상호연계성	피해규모 및 범위	용이성

「정보통신기반보호법」(제8조)

제8조(주요정보통신기반시설의 지정 등)
1. 중앙행정기관의 장은 소관분야의 정보통신기반시설 중 다음 각호의 사항을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다.
① 당해 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성
② 제1호의 규정에 의한 기관이 수행하는 업무의 정보통신기반시설에 대한 의존도
③ 다른 정보통신기반시설과의 상호연계성
④ 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위
⑤ 침해사고의 발생가능성 또는 그 복구의 용이성

정답 ④

상 중 하 정보보안 관리 및 법규 > 정보보호 관리

85 다음 중 국내 정보보호 관리체계 인증에 대한 설명으로 틀린 것은 무엇인가?

① 정보보호 관리체계 인증기관은 정보보호 관리체계의 실효성 제고를 위하여 연 1회 이상 사후관리를 실시한다.
② 과학기술정보통신부 장관은 정보보호 관리체계의 인증을 받아야 하는 자가 과학기술정보통신부령으로 정하는 바에 따라 국제표준 정보보호 인증을 받거나 정보보호 조치를 취한 경우에는 인증 심사를 생략할 수 있다.
③ 과학기술정보통신부 장관은 인증에 관한 업무를 효율적으로 수행하기 위하여 필요한 경우 인증 심사 업무를 수행하는 기관을 지정할 수 있다.
④ 정보보호 관리체계 인증의 유효기간은 3년으로 한다.

②는 인증 심사의 일부를 생략할 수 있는 것이지 인증 심사 전체를 생략하는 것은 아니다. (『정보통신망 이용촉진 및 정보보호 등에 관한 법률』 제47조 제3항 확인)

『정보통신망 이용촉진 및 정보보호 등에 관한 법률』 제47조

제47조(정보보호 관리체계의 인증)
1. 과학기술정보통신부 장관은 정보통신망의 안정성 · 신뢰성 확보를 위하여 관리적 · 기술적 · 물리적 보호조치를 포함한 종합적 관리체계(이하 "정보보호 관리체계"라 한다)를 수립 · 운영하고 있는 자에 대하여 제4항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다. 〈개정 2012.2.17., 2013.3.23., 2015.12.1.〉
2. 「전기통신사업법」 제2조 제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다. 〈신설 2012.2.17., 2015.12.1.〉
① 「전기통신사업법」 제6조 제1항에 따른 허가를 받은 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자
② 집적정보통신시설 사업자
③ 연간 매출액 또는 세입 등이 1,500억 원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억 원 이상 또는 3개월간의 일일평균 이용자수 100만 명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자
3. 과학기술정보통신부 장관은 제2항에 따라 인증을 받아야 하는 자가 과학기술정보통신부령으로 정하는 바에 따라 국제표준 정보보호 인증을 받거나 정보보호 조치를 취한 경우에는 제1항에 따른 인증 심사의 일부를 생략할 수 있다. 이 경우 인증 심사의 세부 생략 범위에 대해서는 과학기술정보통신부 장관이 정하여 고시한다. 〈신설 2015.12.1.〉
4. 과학기술정보통신부 장관은 제1항에 따른 정보보호 관리체계 인증을 위하여 관리적 · 기술적 · 물리적 보호대책을 포함한 인증 기준 등 그 밖에 필요한 사항을 정하여 고시할 수 있다. 〈개정 2012.2.17., 2013.3.23., 2015.12.1.〉

5. 제1항에 따른 정보보호관리체계인증의 유효기간은 3년으로 한다. 다만, 제47조의5 제1항에 따라 정보보호 관리등급을 받은 경우 그 유효기간 동안 제1항의 인증을 받은 것으로 본다. 〈신설 2012.2.17., 2015.12.1.〉
6. 과학기술정보통신부 장관은 한국인터넷진흥원 또는 과학기술정보통신부 장관이 지정한 기관(이하 "정보보호 관리체계 인증기관"이라 한다)으로 하여금 제1항 및 제2항에 따른 인증에 관한 업무로서 다음 각호의 업무를 수행하게 할 수 있다. 〈신설 2012.2.17., 2013.3.23., 2015.12.1.〉
   ① 인증 신청인이 수립한 정보보호 관리체계가 제4항에 따른 인증 기준에 적합한지 여부를 확인하기 위한 심사(이하 "인증 심사"라 한다)
   ② 인증 심사 결과의 심의
   ③ 인증서 발급 · 관리
   ④ 인증의 사후관리
   ⑤ 정보보호 관리체계 인증 심사원의 양성 및 자격관리
   ⑥ 그 밖에 정보보호 관리체계 인증에 관한 업무
7. 과학기술정보통신부 장관은 인증에 관한 업무를 효율적으로 수행하기 위하여 필요한 경우 인증 심사 업무를 수행하는 기관(이하 "정보보호 관리체계 심사기관"이라 한다)을 지정할 수 있다. 〈신설 2015.12.1.〉
8. 한국인터넷진흥원, 정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관은 정보보호 관리체계의 실효성 제고를 위하여 연 1회 이상 사후관리를 실시하고 그 결과를 과학기술정보통신부 장관에게 통보하여야 한다. 〈신설 2012.2.17., 2013.3.23., 2015.12.1.〉
9. 제1항 및 제2항에 따라 정보보호 관리체계의 인증을 받은 자는 대통령령으로 정하는 바에 따라 인증의 내용을 표시하거나 홍보할 수 있다. 〈개정 2012.2.17., 2015.12.1.〉
10. 과학기술정보통신부 장관은 다음 각호의 어느 하나에 해당하는 사유를 발견한 경우에는 인증을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 인증을 취소하여야 한다. 〈신설 2012.2.17., 2013.3.23., 2015.12.1.〉
    ① 거짓이나 그 밖의 부정한 방법으로 정보보호 관리체계 인증을 받은 경우
    ② 제4항에 따른 인증 기준에 미달하게 된 경우
    ③ 제8항에 따른 사후관리를 거부 또는 방해한 경우
11. 제1항 및 제2항에 따른 인증의 방법 · 절차 · 범위 · 수수료, 제8항에 따른 사후관리의 방법 · 절차, 제10항에 따른 인증취소의 방법 · 절차, 그 밖에 필요한 사항은 대통령령으로 정한다. 〈개정 2012.2.17., 2015.12.1.〉
12. 정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관 지정의 기준 · 절차 · 유효기간 등에 필요한 사항은 대통령령으로 정한다.

정답 ②

삼 중 하 정보보안 관리 및 법규 > 정보보호 관리

86 다음 중 정량적 위험분석 기법과 정성적 위험분석 기법의 장단점에 대한 설명으로 틀린 것은?

① 정량적 위험분석 기법은 객관적 평가 기준이 적용된다.
② 정량적 위험분석 기법은 위험관리 성능 평가가 용이하다.
③ 정성적 위험분석 기법은 손실 및 위험을 개략적인 크기로 비교하여 점수화한다.
④ 정성적 위험분석 기법은 비용/가치분석이 수행될 수 있다.

위험분석 기법

구분	정량적 위험분석	정성적 위험분석
산출 개념	위험발생확률 * 손실크기 = 기대위험가치분석	• 손실 크기를 화폐가치로 표현하기 어려움 • 위험 크기는 기술 변수로 표현
접근 유형	• 수학 공식 접근법 • 확률 분포 추정법 • 확률 지배 • 몬테카를로 시뮬레이션 • 과거자료 분석법	• 델파이법, 시나리오법 • 순위 결정법, 퍼지행렬법 • 질문서법
장점	• 객관적인 평가 기준 적용 • 논리적으로 평가되어 이해가 쉬움 • 위험관리 성능평가 용이	가치평가 및 계산이 필요 없음
단점	• 많은 시간과 비용이 소요 • 자동화의 경우 정확도의 변이	• 주관적인 평가 우려 • 결과의 이해가 어려움 • 위험 관리 성능 추적이 어려움

정답 ④

삼 중 하 정보보안 관리 및 법규 > 개인정보보호법

87 다음 중 공공기관의 장이 행정자치부장관에게 등록하여야 하는 개인정보파일 등록대상이 아닌 것은?

① 개인정보파일의 명칭
② 개인정보의 처리방법
③ 개인정보를 일상적 또는 반복적으로 제공하는 경우에는 그 제공받는 자
④ 개인정보의 보유기간

『개인정보보호법』 제32조에 따라 개인정보파일 등록대상이 아닌 것은 개인정보를 일상적 또는 반복적으로 제공하는 경우에는 그 제공받는 자에 해당한다.

『개인정보보호법』 제32조

1. 공공기관의 장이 개인정보파일을 운용하는 경우에는 다음 각호의 사항을 행정자치부장관에게 등록하여야 한다. 등록한 사항이 변경된 경우에도 또한 같다. 〈개정 2013.3.23., 2014.11.19.〉
   ① 개인정보파일의 명칭
   ② 개인정보파일의 운영 근거 및 목적
   ③ 개인정보파일에 기록되는 개인정보의 항목

④ 개인정보의 처리방법
⑤ 개인정보의 보유기간
⑥ 개인정보를 통상적 또는 **반복적으로 제공하는 경우에는 그 제공받는 자**
⑦ 그 밖에 대통령령으로 정하는 사항

『개인정보보호법』 시행령 제33조(개인정보파일의 등록사항) 법 제32조 제1항 제7호에서 "대통령령으로 정하는 사항"이란 다음 각호의 사항을 말한다.
1. 개인정보파일을 운용하는 공공기관의 명칭
2. 개인정보파일로 보유하고 있는 개인정보의 정보주체 수
3. 해당 공공기관에서 개인정보처리 관련 업무를 담당하는 부서
4. 제41조에 따른 개인정보의 열람 요구를 접수 · 처리하는 부서
5. 개인정보파일의 개인정보 중 법 제35조 제4항에 따라 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 제한 또는 거절 사유

정답 ③

상 중 하 정보보안 관리 및 법규 > 정보보호 관리

88 다음 중 국내 ISMS(Information Security Management System) 인증 의무대상자에 대한 설명으로 틀린 것은?

① 「전기통신사업법」 제6조 제1항에 따른 허가를 받은 자로서 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자
② 집적정보통신시설 사업자
③ 연간 매출액 또는 세입 등이 1,500억 원 이상인 자
④ 정보통신서비스 부문 전년도 말 기준 직전 6개월간의 일일평균 이용자수 100만 명 이상인 자

『정보통신망 이용촉진 및 정보보호 등에 관한 법률』 제47조 제2항

2. 「전기통신사업법」 제2조 제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다. 〈신설 2012.2.17., 2015.12.1.〉
① 「전기통신사업법」 제6조 제1항에 따른 허가를 받은 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자
② 집적정보통신시설 사업자
③ 연간 매출액 또는 세입 등이 1,500억 원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억 원 이상 또는 3개월간의 일일평균 이용자수 100만 명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자

『정보통신망 이용촉진 및 정보보호 등에 관한 법률』 시행령 제49조

제49조(정보보호 관리체계 인증 대상자의 범위)
1. 법 제47조 제2항 제1호에서 "대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자"란 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는 자를 말한다.
2. 법 제47조 제2항 제3호에서 "대통령령으로 정하는 기준에 해당하는 자"란 다음 각호의 어느 하나에 해당하는 자를 말한다. 〈개정 2016.5.31〉
① 연간 매출액 또는 세입이 1,500억 원 이상인 자로서 다음 각 목의 어느 하나에 해당하는 자
• 「의료법」 제3조의4에 따른 상급종합병원
• 직전연도 12월 31일 기준으로 재학생 수가 1만 명 이상인 「고등교육법」 제2조에 따른 학교

② 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억 원 이상인 자. 다만, 「전자금융거래법」 제2조 제3호에 따른 금융회사는 제외한다.
③ 전년도 말 기준 직전 3개월간의 일일평균 이용자 수가 100만 명 이상인 자. 다만, 「전자금융거래법」 제2조 제3호에 따른 금융회사는 제외한다.
[본조신설 2012.8.17.]
[종전 제49조는 제53조의3으로 이동 〈2012.8.17.〉]

정답 ④

상 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

89 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 제5호에따른개인정보제공이가능한 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

상 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

90 다음 중 주요정보통신기반시설에 대한 관리기관의 장이 기술적 지원을 요청하는 경우 국가정보원장에게 우선적으로 그 지원을 요청하여야 하는 시설이 아닌 것은?

① 도로 · 철도 · 지하철 · 공항 · 항만 등 주요 교통시설
② 방송중계 · 국가지도통신망 시설
③ 금융 정보통신기반 시설
④ 원자력 · 국방과학 · 첨단방위산업관련 정부출연 연구기관의 연구시설

『정보통신기반보호법』 제7조 제3항에 따라 금융 정보통신기반시설은 국가정보원장이 금융 정보통신기반시설 등 개인정보가 저장된 모든 정보통신기반시설에 대하여 기술적 지원을 수행하여서는 아니 된다고 명시되어 있다.

『정보통신기반보호법』 제7조

제7조(주요정보통신기반시설의 보호지원)

1. 관리기관의 장이 필요하다고 인정하거나 위원회의 위원장이 특정 관리기관의 주요정보통신기반시설보호대책의 미흡으로 국가안전보장이나 경제사회전반에 피해가 우려된다고 판단하여 그 보완을 명하는 경우 해당 관리기관의 장은 **과학기술정보통신부 장관과 국가정보원장 등** 또는 필요한 경우 대통령령이 정하는 전문기관의 장(**국방부장관**)에게 다음 각호의 업무에 대한 기술적 지원을 요청할 수 있다. 〈개정 2007.12.21., 2008.2.29., 2013.3.23.〉
   ① 주요정보통신기반시설보호대책의 수립
   ② 주요정보통신기반시설의 침해사고 예방 및 복구
   ③ 제11조에 따른 보호조치 명령 · 권고의 이행
2. 국가안전보장에 중대한 영향을 미치는 다음 각호의 주요정보통신기반시설에 대한 관리기관의 장이 제1항에 따라 기술적 지원을 요청하는 경우 국가정보원장에게 우선적으로 그 지원을 요청하여야 한다. 다만, 국가안전보장에 현저하고 급박한 위험이 있고, 관리기관의 장이 요청할 때까지 기다릴 경우 그 피해를 회복할 수 없을 때에는 국가정보원장은 관계중앙행정기관의 장과 협의하여 그 지원을 할 수 있다. 〈개정 2007.12.21.〉
   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
3. 국가정보원장은 제1항 및 제2항에 불구하고 **금융정보통신 기반시설 등 개인정보가 저장된 모든 정보통신 기반시설에 대하여 기술적 지원을 수행하여서는 아니 된다.**

정답 ③

상 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

91 다음 중 통상적으로 정보보호 교육훈련 시 포함되어야 할 교육 내용에 해당하지 않는 것은 무엇인가?

① 정보보호 요구사항
② 보안사고 발생 시 사용자의 법적 책임
③ 정보보호 침해사고 사례 및 대응방안
④ 정보보호 시스템 구성도 및 운영방법

통상적인 정보보호 교육훈련 시 포함되어야 할 교육내용에 해당하지 않는 것은 정보보호 시스템 구성도 및 운영방법이라고 생각된다. 정답이 공개되지 않은 상황에서 ④번을 정답이라고 본 이유는 국내 ISMS 인증 제도 안내서의 정보보호교육이 포함된 내용을 참조하였다.

아래는 국내 ISMS 인증 시 통제항목 중 정보보호대책 5. 정보보호교육 중 5.1.3 통제항목의 정보보호교육 내용에 대한 설명을 참조하여 해설을 첨부하였다.

임직원 대상 기본 정보보호교육에 다음의 내용을 포함하였는가?
- 정보보호 및 정보보호 관리체계 개요
- 정보보호 정책, 지침, 절차 등 정보보호 관련 내부 규정
- 정보보호 관련 법률
- 침해사고 사례 및 대응방안
- 정보보호 규정 위반 시 법적 책임 등

IT 및 정보보호 조직 내 임직원은 정보보호와 관련하여 직무별 전문성 제고를 위하여 필요한 별도의 교육을 받고 있는가?
- IT 직무자(운영, 개발), 정보보호 직무자는 일반 직원과 별도로 직무별 업무 수행에 필요한 정보보호 교육을 받아야 한다. 직무별 교육은 다음과 같은 교육 과정을 활용할 수 있다.
- 정보보호 관련 컨퍼런스, 세미나, 워크샵 참가
- 정보보호 관련 교육 전문기관 내 교육 수료
- 외부 전문가 초빙을 통한 내부 교육 및 세미나

정답 ④

상 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

92 정보통신서비스 제공자 등은 개인정보의 분실 · 도난 · 유출(이하 "유출 등"이라 한다) 사실을 안 때에는 지체 없이 조치한다. 이 방법에 대한 설명으로 틀린 것을 고르시오.

① 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 한다.
② 정보통신서비스 제공자 등은 개인정보 유출 등의 사실을 안 때에는 지체 없이 신고하여야 하나, 긴급한 조치가 필요한 경우에는 그 조치를 한 후 5일 이내에 지체 없이 이용자에게 알릴 수 있다.
③ 유출 등이 된 개인정보 항목, 유출 등이 발생한 시점, 이용자가 취할 수 있는 조치 등을 이용자에게 통지한다.
④ 정보통신서비스 제공자 등은 개인정보의 유출 등에 대한 대책을 마련하고 그 피해를 최소화할 수 있는 조치를 강구하여야 한다.

정보통신서비스 제공자 등은 개인정보의 분실 · 도난 · 유출(이하 "유출 등"이라 한다) 사실을 안 때에는 지체 없이 정당한 사유 없이 그 사실을 안 때부터 24시간 내에 통지 · 신고하여야 한다.

『정보통신망 이용촉진 및 정보보호 등에 관한 법률』

제27조의3(개인정보 유출 등의 통지 · 신고)

1. 정보통신서비스 제공자 등은 개인정보의 분실 · 도난 · 유출(이하 "유출 등"이라 한다) 사실을 안 때에는 지체 없이 다음 각 호의 모든 사항을 해당 이용자에게 알리고 **방송통신위원회 또는 한국인터넷진흥원에 신고**하여야 하며, 정당한 사유 없이 그 **사실을 안 때부터 24시간을 경과하여 통지 · 신고해서는 아니 된다.** 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다. 〈개정 2014.5.28., 2016.3.22.〉
   ① 유출 등이 된 개인정보 항목
   ② 유출 등이 발생한 시점
   ③ 이용자가 취할 수 있는 조치
   ④ 정보통신서비스 제공자 등의 대응 조치
   ⑤ 이용자가 상담 등을 접수할 수 있는 부서 및 연락처
2. 제1항의 신고를 받은 한국인터넷진흥원은 지체 없이 그 사실을 방송통신위원회에 알려야 한다. 〈신설 2014.5.28.〉
3. 정보통신서비스 제공자 등은 제1항 본문 및 단서에 따른 정당한 사유를 방송통신위원회에 소명하여야 한다. 〈신설 2014.5.28.〉
4. 제1항에 따른 통지 및 신고의 방법 · 절차 등에 관하여 필요한 사항은 대통령령으로 정한다. 〈개정 2014.5.28.〉
5. 정보통신서비스 제공자 등은 개인정보의 유출 등에 대한 대책을 마련하고 그 피해를 최소화할 수 있는 조치를 강구하여야 한다. 〈개정 2014.5.28., 2016.3.22.〉
   [본조신설 2012.2.17.] [제목개정 2016.3.22.]

『정보통신망 이용촉진 및 정보보호 등에 관한 법률』

제14조의2(개인정보 유출 등의 통지 · 신고)

1. 정보통신서비스 제공자 등은 개인정보의 분실 · 도난 · 유출의 사실을 안 때에는 지체 없이 법 제27조의3 제1항 각호의 모든 사항을 전자우편 · 서면 · 모사전송 · 전화 또는 이와 유사한 방법 중 어느 하나의 방법으로 이용자에게 알리고 방송통신위원회 또는 한국인터넷진흥원에 신고하여야 한다. 〈개정 2014.11.28, 2016.9.22〉
   정보통신서비스 제공자 등은 제1항에 따른 통지 · 신고를 하려는 경우 법 제27조의3 제1항 제1호 또는 제2호의 사항에 관한 구체적인 내용이 확인되지 아니하였으면 그때까지 확인된 내용과 같은 항 제3호부터 제5호까지의 사항을 우선 통지 · 신고한 후 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지 · 신고하여야 한다.
   정보통신서비스 제공자 등은 법 제27조의3 제1항 각호 외의 부분 단서에 따른 정당한 사유가 있는 경우에는 법 제27조의3 제1항 각호의 사항을 자신의 인터넷 홈페이지에 30일 이상 게시하는 것으로 제1항의 통지를 갈음할 수 있다.
   천재지변이나 그 밖의 정당한 사유로 제3항에 따른 홈페이지 게시가 곤란한 경우에는 「신문 등의 진흥에 관한 법률」에 따른 전국을 보급지역으로 하는 둘 이상의 일반 일간신문에 1회 이상 공고하는 것으로 제3항에 따른 홈페이지 게시를 갈음할 수 있다.
   정보통신서비스 제공자 등은 법 제27조의3 제1항 각호 외의 부분 본문 및 단서에 따른 정당한 사유를 지체 없이 서면(전자문서를 포함한다)으로 방송통신위원회에 소명하여야 한다. 〈신설 2014.11.28〉 [본조신설 2012.8.17] [제목개정 2016.9.22]

『개인정보보호법』

제34조(개인정보 유출 통지 등)

1. 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각호의 사실을 알려야 한다.
   ① 유출된 개인정보의 항목
   ② 유출된 시점과 그 경위
   ③ 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
   ④ 개인정보처리자의 대응조치 및 피해 구제절차
   ⑤ 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
2. 개인정보처리자는 개인정보가 유출된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.
3. 개인정보처리자는 대통령령으로 정한 규모 이상의 개인정보가 유출된 경우에는 제1항에 따른 통지 및 제2항에 따른 조치 결과를 지체 없이 행정자치부장관 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 행정자치부장관 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다. 〈개정 2013.3.23., 2014.11.19.〉
4. 제1항에 따른 통지의 시기, 방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

『개인정보보호법』 시행령 제39조, 제40조

제39조(개인정보 유출 신고의 범위 및 기관)

1. 법 제34조 제3항 전단에서 "대통령령으로 정한 규모 이상의 개인정보"란 **1만 명 이상의 정보주체**에 관한 **개인정보**를 말한다. 법 제34조 제3항 전단 및 후단에서 "대통령령으로 정하는 전문기관"이란 각각 **한국인터넷진흥원**을 말한다. 〈개정 2015.12.30, 2016.7.22.〉

제40조(개인정보 유출 통지의 방법 및 절차)

1. 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 서면 등의 방법으로 지체 없이 법 제34조 제1항 각호의 사항을 정보주체에게 알려야 한다.
   다만, 유출된 개인정보의 확산 및 추가 유출을 방지하기 위하여 접속 경로의 차단, 취약점 점검 · 보완, 유출된 개인정보의 삭제 등 긴급한 조치가 필요한 경우에는 그 조치를 한 후 지체 없이 정보주체에게 알릴 수 있다.
   제1항에도 불구하고 개인정보처리자는 같은 항 본문에 따라 개인정보가 유출되었음을 알게 되었을 때나 같은 항 단서에 따라 유출 사실을 알고 긴급한 조치를 한 후에도 법 제34조 제1항 제1호 및 제2호의 구체적인 유출 내용을 확인하지 못한 경우에는 먼저 개인정보가 유출된 사실과 유출이 확인된 사항만을 서면 등의 방법으로 먼저 알리고 나중에 확인되는 사항을 추가로 알릴 수 있다.
   제1항과 제2항에도 불구하고 법 제34조 제3항 및 이 영 제39조 제1항에 따라 1만 명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 서면 등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 법 제34조 제1항 각호의 사항을 7일 이상 게재하여야 한다.
   다만, 인터넷 홈페이지를 운영하지 아니하는 개인정보처리자의 경우에는 서면 등의 방법과 함께 사업장 등의 보기 쉬운 장소에 법 제34조 제1항 각호의 사항을 7일 이상 게시하여야 한다.

정답 ②

상 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

93 영상정보처리기기 설치 시 정보주체가 쉽게 알아볼 수 있도록 안내판을 설치하여야 하지만, 반드시 안내판을 설치하지 않아도 되는 곳은 어디인가?

① 공공기관의 민원실
② 백화점, 대형마트, 상가, 놀이공원, 극장 등의 시설
③ 허가된 인원만이 출입할 수 있는 전산보안시설
④ 무료로 이용되는 주차장

『개인정보보호법』 시행령 제24조 안내판 설치 등

법 제25조 제4항 단서에 따라 공공기관의 장은 다음 각호의 어느 하나에 해당하는 시설에 설치하는 영상정보처리기기에 대해서는 안내판을 설치하지 아니할 수 있다. 〈개정 2015.3.11〉

1. 「군사기지 및 군사시설 보호법」 제2조 제2호에 따른 군사시설
2. 「통합방위법」 제2조 제13호에 따른 국가중요시설
3. 「보안업무규정」 제36조에 따른 국가보안시설

정답 ③

94 다음 위험관리 방법 중 위험 완화 방법에 대한 설명으로 틀린 것은?

① 위험수용(Acceptance) : 위험의 잠재 손실 비용을 감수한다.
② 위험전가(Risk Transfer) : 보험이나 외주 등으로 잠재적 비용을 제3자에게 이전하거나 할당한다.
③ 위험감소(Mitigation) : 위험을 감소시킬 수 있는 대책을 채택하여 구현하는 것으로 많은 비용이 소요되기 때문에 실제 감소되는 위험의 크기와 비교하여 비용분석을 실시한다.
④ 위험회피(Risk Avoidance) : 위험이 존재하는 프로세스나 사업을 수행하지 않고 포기하는 것을 말하며, 완전히 제거할 수 없으므로 일정수준 이하의 수준을 감수하고 사업을 진행하는 방법이다.

④는 위험회피와 위험수용에 대한 설명이 혼재되어 있다.

1. 위험수용(Acceptance)
   위험의 잠재 손실 비용을 감수하는 것으로 어떠한 대책을 도입하더라도 완전히 제거할 수 없으므로 일정수준 이하의 수준을 감수하고 사업을 진행하는 방법
2. 위험감소(Mitigation)
   • 위험을 감소시킬 수 있는 대책을 채택하여 구현하는 것
   • 많은 비용이 소요되기 때문에 실제 감소되는 위험의 크기와 비교하여 비용분석을 실시

   정보보호대책의 효과 = 원 ALE − 대책 구현 후 ALE − 연간대책비용
   양(+)의 효과를 갖는 정보보호대책을 선택
   * 연간기대손실법(ALE) − 위험 발생확률 × 손실크기를 통해 기대 위험가치를 분석
   • SLE = EF(노출계수) × AV(자산가치)
   • ALE = SLE × ARO(연간발생률)
3. 위험회피(Risk Avoidance)
   위험이 존재하는 프로세스나 사업을 수행하지 않고 포기하는 것
4. 위험전가(Risk Transfer)
   보험이나 외주 등으로 잠재적 비용을 제3자에게 이전하거나 할당하는 것

정답 ④

95 다음 보기에서 정보통신망법에 따라 개인정보를 보호하기 위한 설명 중 틀린 것을 모두 고르시오.

A. 정보통신서비스의 제공에 따른 요금정산을 위해서는 사전에 고객의 동의 없이 고객의 물품 주문내역, 서비스 이용내역, 통신사실 확인자료 등과 같이 요금을 산출하고 과금하기 위한 자료를 생성한 경우 사후에 이용자의 개인정보수집 동의를 받아야 한다.
B. 해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 사전에 동의를 받아야 한다.
C. 정보통신서비스 제공자 등은 개인정보처리위탁을 하는 경우에 수탁자가 개인정보처리위탁을 받은 업무와 관련하여 이 장의 규정을 위반하여 이용자에게 손해를 발생시키면 그 수탁자만이 손해배상책임에 있다.
D. 정보통신서비스 제공자는 영업상 목적을 위하여 이용자의 주민등록번호가 불가피하게 필요한 경우 이용자의 동의 없이 수집 · 이용이 가능하다.
E. 환자의 동의 및 개별법에 근거한 경우라면 의료정보와 관련된 개인정보수집이 가능하다.

① B, C, D
② B, E
③ A, C, D
④ A, B, D

A. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제22조 제2항에 따라 정보통신서비스의 제공에 따른 요금정산을 위해서는 개인정보를 수집 · 이용하는 경우 이용자의 동의 없이 수집이 가능하다.

제22조(개인정보의 수집 · 이용 동의 등)
1. 정보통신서비스 제공자는 이용자의 개인정보를 이용하려고 수집하는 경우 다음 각호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각호의 어느 하나의 사항을 변경하려는 경우에도 또한 같다.
   ① 개인정보의 수집 · 이용 목적
   ② 수집하는 개인정보의 항목
   ③ 개인정보의 보유 · 이용 기간
2. 정보통신서비스 제공자는 다음 각호의 어느 하나에 해당하는 경우에는 제1항에 따른 동의 없이 이용자의 개인정보를 수집 · 이용할 수 있다.
   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 [전문개정 2008.6.13.]

C. 업무위탁과 제3자 제공에 대한 책임소재에 대해서 암기할 필요가 있다.

정보통신망법 제25조 제5항에 따라 업무위탁에서 발생되는 손해배상의 책임은 위탁자에게 있으며, 제3자에게 제공 시 발생된 손해배상책임은 제3자(위탁자)에게 있다.

5. 수탁자가 개인정보처리위탁을 받은 업무와 관련하여 이 장의 규정을 위반하여 이용자에게 손해를 발생시키면 그 수탁자를 손해배상책임에 있어서 정보통신서비스 제공자 등의 소속 직원으로 본다.

정답 ③

업무 위탁과 제3자 제공의 비교

구분	업무위탁	제3자 제공
관련조항	제26조	제17조
예시	배송업무 위탁, TM 위탁 등	사업제휴, 개인정보 판매 등
이전목적	위탁자의 이익을 위해 처리	제3자의 이익을 위해 처리
이전 방법	원칙 : 위탁사실 공개 예외 : 위탁사실 고지(마케팅 업무위탁)	원칙 : 제공목적 등을 고지한 후 정보주체 동의 획득
관리 · 감독 책임	위탁자 책임	제공받는 자 책임
손해배상 책임	위탁자 부담(사용자 책임)	제공받는 자 부담

D. 모든 정보통신서비스 제공자가 아니라 전기통신사업법 제38조 제1항 또는 제2항에 따라 기간통신사업자로부터 이동통신서비스를 도매제공 받아 재판매하는 전기통신사업자만이 이용자의 주민등록번호를 수집 · 이용이 가능하다.

제23조의2(주민등록번호의 사용 제한)

1. 정보통신서비스 제공자는 다음 각호의 어느 하나에 해당하는 경우를 제외하고는 이용자의 주민등록번호를 수집 · 이용할 수 없다.
   ① 제23조의3에 따라 본인확인기관으로 지정받은 경우
   ② 법령에서 이용자의 주민등록번호 수집 · 이용을 허용하는 경우
   ③ 영업상 목적을 위하여 이용자의 주민등록번호 수집 · 이용이 불가피한 정보통신서비스 제공자로서 방송통신위원회가 고시하는 경우

   「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조의2 제1항 제3호에서 "영업상 목적을 위하여 이용자의 주민등록번호 수집 · 이용이 불가피한 정보통신서비스 제공자"라 함은 전기통신사업법 제38조 제1항 또는 제2항에 따라 기간통신사업자로부터 이동통신 서비스를 도매 제공받아 재판매하는 전기통신사업자를 말한다.
2. 제1항 제2호 또는 제3호에 따라 주민등록번호를 수집 · 이용할 수 있는 경우에도 이용자의 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법(이하 "대체수단"이라 한다)을 제공하여야 한다. [전문개정 2012.2.17.]

삼 중 하 **정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규**

96 다음 중 전자서명법의 공인인증서에 포함되는 사항이 아닌 것은?

① 공인인증서의 일련번호
② 가입자와 공인인증기관이 이용하는 전자서명 방식
③ 공인인증서의 유효기간
④ 공인인증서의 비밀번호

제15조(공인인증서의 발급)

1. 공인인증기관은 공인인증서를 발급받고자 하는 자에게 공인인증서를 발급한다. 이 경우 공인인증기관은 공인인증서를 발급받고자 하는 자의 신원을 확인하여야 한다. 〈개정 2001.12.31.〉
2. 공인인증기관이 발급하는 공인인증서에는 다음 각호의 사항이 포함되어야 한다. 〈개정 2001.12.31.〉
   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
3. 삭제 〈2001.12.31.〉
4. 공인인증기관은 공인인증서를 발급받고자 하는 자의 신청이 있는 경우에는 공인인증서의 이용범위 또는 용도를 제한하는 공인인증서를 발급할 수 있다. 〈개정 2001.12.31.〉
5. 공인인증기관은 공인인증서의 이용범위 및 용도, 이용된 기술의 안전성과 신뢰성 등을 고려하여 공인인증서의 유효기간을 적정하게 정하여야 한다. 〈개정 2001.12.31.〉
6. 공인인증서 발급에 따른 신원확인 절차 및 방법 등에 관하여 필요한 사항은 과학기술정보통신부령으로 정한다. 〈신설 2001.12.31., 2008.2.29., 2013.3.23.〉

[제목개정 2001.12.31.]

정답 ④

삼 중 하 **정보보안 관리 및 법규 > 정보보호 관리**

97 다음 보기에서 설명하고 있는 것은 무엇인가?

- 재해복구센터에 주센터와 동일한 수준의 정보기술자원을 보유하는 대신 중요성이 높은 정보기술자원만 부분적으로 재해복구센터에 보유하는 방식이다.
- 구축 및 유지비용이 저렴하나 초기의 복구수준이 완전하지 않으며, 완전한 복구까지는 다소의 시일이 소요된다.

① 중복 사이트
② 핫(Hot) 사이트
③ 웜(Warm) 사이트
④ 콜드(Cold) 사이트

1. 미러 사이트(Mirror Site)

- 주센터와 동일한 수준의 정보기술자원을 원격지에 구축하여 두고 주센터와 재해복구센터 모두 액티브 상태로(Active-Active) 실시간에 동시 서비스를 하는 방식이다(즉, 이론적인 RPO가 0임).
- 재해발생 시 복구까지의 소요시간(RTO)은 즉시(이론적으로는 0)이다.
- 초기 투자 및 유지보수에 높은 비용이 소요된다.
- 웹 애플리케이션 서비스 등 데이터의 업데이트의 빈도가 높지 않은 시스템에 적용 가능하다.
- 데이터베이스 애플리케이션 등 데이터의 업데이트 빈도가 높은 시스템의 경우 양쪽의 사이트에서 동시에 서비스를 제공하게 하는 것은 시스템의 높은 부하를 초래하여 실용적이지 않다. 이러한 경우에는 다음에서 설명하는 핫 사이트의 구축이 일반적이다.

2. 핫 사이트(Hot Site)

- 주센터와 동일한 수준의 정보기술자원을 대기상태(Standby)로 원격지 사이트에 보유하면서(Active-Standby), 동기적(Synchronous) 또는 비동기적(Asynchronous) 방식의 실시간 미러링(Mirroring)을 통하여 데이터를 최신의 상태(Up-to-date)로 유지하고 있다가(즉, RPO ≒ 0을 지향함), 주센터 재해 시 재해복구센터의 정보시스템을 액티브로 전환하여 서비스하는 방식이다.
- 일반적으로 데이터 실시간 미러링을 이용한 핫 사이트를 미러 사이트라고 하기도 한다.
- 재해발생 시 복구까지의 소요시간(RTO)은 수시간(약 4시간 이내)이다.

정답 ③

• 초기투자 및 유지보수에 높은 비용이 소요된다.
• 데이터베이스 애플리케이션 등 데이터의 업데이트 빈도가 높은 시스템의 경우, 재해복구센터는 대기상태(Standby)로 유지하다가 재해 시 액티브(Active)로 전환하는 방식이 일반적이다.

3. 웜 사이트(Warm Site)

• 핫 사이트와 유사하나 재해복구센터에 주센터와 동일한 수준의 정보기술자원을 보유하는 대신 중요성이 높은 정보기술자원만 부분적으로 재해복구센터에 보유하는 방식이다.
• 실시간 미러링을 수행하지 않으며 데이터의 백업 주기가 수시간~1일 정도로 핫 사이트에 비해 다소 길다(즉, RPO가 약 수시간~1일).
• 재해발생 시 복구까지의 소요시간(RTO)은 수일~수주이다.
• 구축 및 유지비용이 미러 사이트 및 핫 사이트에 비해 저렴하나 초기의 복구수준이 완전하지 않으며, 완전한 복구까지는 다소의 시일이 소요된다.

4. 콜드 사이트(Cold Site)

• 데이터만 원격지에 보관하고 이의 서비스를 위한 정보자원은 확보하지 않거나 장소 등만 최소한으로만 확보하고 있다가, 재해 시 데이터를 근간으로 하여 필요한 정보자원을 조달하며 정보시스템의 복구를 개시하는 방식이다.
• 주센터의 데이터는 주기적(수일~수주)으로 원격지에 백업된다(즉, RPO가 수일~수주).
• 재해발생 시 복구까지의 소요시간(RTO)은 수주~수개월이다.
• 구축 및 유지비용이 가장 저렴하나 복구소요시간이 매우 길고 복구의 신뢰성이 낮다.

98 다음은 「정보통신기반보호법」에 따라 주요정보통신기반시설 취약점의 분석 · 평가를 한 것이다. 이에 대한 설명으로 틀린 것을 고르시오.

① 관리기관의 장은 소관 정보통신기반시설이 주요정보통신기반시설로 지정된 때에는 지정 후 1년 이내에 취약점의 분석 · 평가를 실시하여야 한다.
② 관리기관의 장은 소관 주요정보통신기반시설 지정 후 취약점의 분석 · 평가를 시행하지 못할 특별한 사유가 있다고 판단되는 경우에는 관할 중앙행정기관의 장의 승인을 얻어 지정 후 9월 이내에 이를 실시하여야 한다.
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.

관리기관의 장은 소관 정보통신기반시설이 주요정보통신기반시설로 지정된 때에는 지정 후 6월 이내에 취약점의 분석 · 평가를 실시하여야 한다.

『정보통신기반보호법』

제9조(취약점의 분석 · 평가)

1. 관리기관의 장은 대통령령이 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석 · 평가하여야 한다.
2. 관리기관의 장은 제1항의 규정에 의하여 취약점을 분석 · 평가하고자 하는 경우에는 대통령령이 정하는 바에 따라 취약점을 분석 · 평가하는 전담반을 구성하여야 한다.
3. 관리기관의 장은 제1항의 규정에 의하여 취약점을 분석 · 평가하고자 하는 경우에는 다음 각호의 1에 해당하는 기관으로 하여금 소관 주요정보통신기반시설의 취약점을 분석 · 평가하게 할 수 있다. 다만, 이 경우 제2항의 규정에 의한 전담반을 구성하지 아니할 수 있다. 〈개정 2002.12.18., 2007.12.21., 2009.5.22., 2013.3.23., 2015.6.22.〉
   ① 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조의 규정에 의한 한국인터넷진흥원(이하 "인터넷진흥원"이라 함)
   ② 제16조의 규정에 의한 정보공유 · 분석센터(대통령령이 정하는 기준을 충족하는 정보공유 · 분석센터에 한함)
   ③ 「정보보호산업의 진흥에 관한 법률」 제23조에 따라 지정된 정보보호 전문서비스 기업
   ④ 「정부출연연구기관 등의 설립 · 운영 및 육성에 관한 법률」 제8조의 규정에 의한 한국전자통신연구원
4. 과학기술정보통신부 장관은 관계중앙행정기관의 장 및 국가정보원장과 협의하여 제1항의 규정에 의한 취약점 분석 · 평가에 관한 기준을 정하고 이를 관계중앙행정기관의 장에게 통보하여야 한다. 〈개정 2008.2.29., 2013.3.23.〉
5. 주요정보통신기반시설의 취약점 분석 · 평가의 방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

『정보통신기반보호법』

제17조(취약점 분석 · 평가의 시기)

1. 관리기관의 장은 소관 정보통신기반시설이 주요정보통신기반시설로 지정된 때에는 지정 후 6월 이내에 법 제9조 제1항의 규정에 의한 취약점의 분석 · 평가를 실시하여야 한다.
   다만, 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 9월 이내에 이를 실시하여야 한다.
   관리기관의 장은 제1항에 따라 소관 주요정보통신기반시설이 지정된 후 당해 주요 정보 통신기반시설에 대한 최초의 취약점 분석 · 평가를 한 후 매년 취약점의 분석 · 평가를 실시한다.
   다만, 소관 주요정보통신기반시설에 중대한 변화가 발생하였거나 관리기관의 장이 취약점 분석 · 평가가 필요하다고 판단하는 경우에는 1년이 되지 아니한 때에도 취약점의 분석 · 평가를 실시할 수 있다. 〈개정 2012.5.23〉

제18조(취약점 분석 · 평가 방법 및 절차)

1. 법 제9조 제2항의 규정에 의하여 관리 기관의 장은 취약점을 분석 · 평가하기 위한 전담반을 구성하는 때에는 별표 1의 사항을 고려하여 취약점 분석 · 평가의 객관성과 실효성을 확보할 수 있도록 하여야 한다. 관리기관의 장은 법 제9조 제3항 각호의 1에 해당하는 기관으로 하여금 소관 주요정보통신기반시설의 취약점을 분석 · 평가하게 하는 때에는 취약점 분석 · 평가 수행기관이 취득한 관리기관의 비밀정보가 외부에 유출되지 아니하도록 적정한 조치를 취하여야 한다.
   법 제9조 제3항의 규정에 의하여 관리기관의 장이 동항 각호의 1에 해당하는 기관으로 하여금 취약점을 분석 · 평가하게 하는 때에는 취약점 분석 · 평가 업무를 위탁받은 기관이 이를 직접 수행하도록 하여야 한다.
   법 제9조 제4항의 규정에 의한 취약점 분석 · 평가 기준에는 다음 각호의 사항이 포함되어야 한다
   ① 취약점 분석 · 평가의 절차
   ② 취약점 분석 · 평가의 범위 및 항목
   ③ 취약점 분석 · 평가의 방법

제19조(정보공유 · 분석센터의 취약점 분석 · 평가)

1. 법 제9조 제3항 제2호에서 "대통령령이 정하는 기준"이라 함은 별표 2의 기준을 말한다. 정보공유 · 분석센터에 가입한 복수의 관리기관이 정보통신망을 통하여 영업을 수행하는 분야에 있어서 상호 연동된 주요정보통신기반시설에 대한 취약점 분석 · 평가는 해당 관리기관의 동의를 얻어 수행하여야 한다.

정답 ①

상 중 하 정보보안 관리 및 법규 > 정보보호 관련 윤리 및 법규

99 다음 중 전자서명법에 따른 전자서명인증 업무지침에 포함되는 사항이 아닌 것은?

① 공인인증서의 관리에 관한 사항
② 전자서명 검증 정보의 파기에 관한 사항
③ 공인인증기관 시설의 보호에 관한 사항
④ 인증 업무 및 운영관리에 관한 사항

② 전자서명 검증 정보의 파기에 관한 사항은 전자서명인증 업무지침에 포함되어 있지 않고, 전자서명 생성정보의 파기에 관한 사항은 고시되어 있다.

> ※ 전자서명인증 업무지침
> 제13조(전자서명생성정보 파기)
> 공인인증기관은 관리챔임자 및 보안관리자의 입회하에 백업된 전자서명생성정보와 그 원본을 안전하게 파기하여야 한다.

『전자서명법』

제8조(공인인증기관의 업무수행)

1. 과학기술정보통신부 장관은 인증 업무의 안전성과 신뢰성 확보를 위하여 공인인증기관이 인증 업무수행에 있어 지켜야 할 구체적 사항을 전자 서명인증 업무지침으로 정하여 고시할 수 있다. 〈개정 2008.2.29., 2013.3.23.〉
2. 제1항의 규정에 의한 전자서명인증 업무지침에는 다음 각호의 사항이 포함되어야 한다. 〈신설 2005.12.30.〉
   ① 공인인증서의 관리에 관한 사항
   ② 전자서명생성정보의 관리에 관한 사항
   ③ 공인인증기관 시설의 보호에 관한 사항
   ④ 그 밖에 인증 업무 및 운영관리에 관한 사항

[전문개정 2001.12.31.]

※ 전자서명인증 업무지침 조문 목차

[시행 2014.4.24.] [과학기술정보통신부고시 제2014-30호, 2014.4.24., 일부개정]

제1장 총칙
제2장 공인인증서 관리
제3장 전자서명생성정보 및 전자서명검증정보 관리
제4장 기타 공인인증 업무
제5장 기타 운영관리

제13조(전자서명생성정보 파기)
공인인증기관은 관리책임자 및 보안관리자의 입회하에 백업된 전자서명생성정보와 그 원본을 안전하게 파기하여야 한다.

정답 ②

상 중 하 정보보안 관리 및 법규 > 정보보호 관리

100 다음 중 통상적으로 정보보호 정책서에 포함되는 내용이 아닌 것은?

① 정보보호 정책의 목적과 구성
② 정보보호 실행계획
③ 보안에 대한 역할과 책임
④ 정보보호의 선언문

통상적인 정보보안 정책서에 포함되지 않은 사항은 정보보호 실행계획이다. 정보보안 정책서는 회사에서 보호해야 할 정보자산을 정의하며, 정보보안을 실현하기 위한 기본 목표와 방향성을 설정한다.
정보보안 정책서에는 구체적인 내용뿐만 아니라 정책서의 '개정 이력', '목적', '적용 범위', '역할 및 책임', 필요 시 '주요 용어에 대한 설명' 등을 포함해야 한다.

※ 정보보호 정책서의 구성
- 정보보호 선언문 : 보통 1장에 심플하게 작성 / 정보보호전반에 대한 경영자의 의지 및 실천을 다짐하는 선언문
- 정책서 목적과 구성 / 기본 방침 / 정보보호계획수립 / 보안에 대한 역할과 책임 / 정보자산의 보안 등

정답 ②