2007년 제1, 2회 SIS 2급 필기시험

정보보호전문가 2급 필기 시험

필 기 시 험			
시험과목	네트워크보안/정보보호론		
시험지역		**시험시간**	
수검번호		**성 명**	

⇒ 2007년 1·2차 시험문제 중 일부를 공개합니다.

정 보 보 호 전 문 가 2 급 필 기

과 목	네트워크 보안	07년 2차

1. DHCP(Dynamic Host Configuration Protocol)는 호스트에 IP 어드레스를 부여하여 네트워크 관리를 용이하게 한다. 다음 DHCP 서버가 제공하는 것 중 틀린 것은?

   ① IP 주소
   ② 서브넷 마스크
   ③ 기본 게이트웨이
   ④ Metric
   ⑤ DNS 서버

2. 네트워크 서브넷팅의 장점이 아닌 것은?

   ① 보안성의 향상을 가져온다.
   ② 네트워크의 트래픽을 감소시킨다.
   ③ IP 손실을 줄일 수 있다.
   ④ 여러 개의 C 클래스 주소를 결합하여 하나의 네트워크 주소로 사용할 수 있다.
   ⑤ 작은 그룹으로 분리할 수 있어서 관리가 용이하다.

3. 만약 장비가 패킷을 보내고자 하는 곳의 IP 어드레스는 알고 있지만 이더넷 어드레스를 모른다면, 이더넷 어드레스를 찾기 위해 사용되는 프로토콜은 무엇인가?

   ① IP(Internet Protocol)
   ② ARP(Address Resolution Protocol)
   ③ RARP(Reverse Address Resolution Protocol)
   ④ IARP(Inverse Address Resolution Protocol)
   ⑤ DNS(Domain Name System)

4. TCP와 UDP를 비교한 것 중 잘못된 것은?

① UDP는 비연결형 서비스이고, TCP는 연결형 서비스이다.
② TCP는 수신순서가 데이터의 송신순서와 동일하지만, UDP는 송신순서와 다를 수 있다.
③ TCP는 바이트 스트림 단위로, UDP는 블록단위로 비트정보를 전송한다.
④ TCP와 UDP는 오류제어와 흐름제어 기능을 수행한다.
⑤ TCP는 양뱡향 동시 전송의 전이중방식이 가능하다.

5. 다음 중 B 클라스 IP 주소를 갖는 네트워크에서 기본으로 설정되어 있는 브로드캐스트 주소는?

① 172.16.0.0
② 172.16.255.255
③ 172.255.255.255
④ 255.255.255.255
⑤ 10.16.255.255

6. 다음 지문과 같이 NAT(Network Address Translation)를 사용할 때, 서버 B에서 보는 서버 A의 IP 주소는?

A -------- Gateway -------- {인터넷} -------- Gateway -------- B A(172.16.5.163) A의 Gateway(211.241.82.100) B(61.42.54.99) B의 Gateway(61.42.54.1)

① 172.16.5.163
② 211.241.82.100
③ 211.241.82.163
④ 61.42.54.1
⑤ 61.42.54.99

7. 다음 지문에서 설명한 내용은 TCP 필드 중 어떤 필드에 대한 것인가?

> TCP 헤더와 데이터를 포함하여 TCP 세그먼트 전체에 대한 오류를 검사하는데 사용되며 16 비트 단위로 '1의 보수' 합을 계산한다.

① Window 필드
② Control Flags 필드
③ Checksum 필드
④ Data Offset 필드
⑤ ACK Number 필드

8. 다음 지문은 어떤 종류의 ICMP 메시지를 설명하는 것인가?

> 데이터를 보내는 호스트에게 IP 데이터그램이 라우터의 집중 현상에 의해 손실되고 있음을 알리기 위해 라우터가 보내는 메시지

① Source Quench
② Echo Request
③ Echo Reply
④ Redirect
⑤ Destination Unreachable

9. STP(Spanning Tree Protocol) Switch의 포트 상태가 아닌 것은?

① Blocking
② Listening
③ Learning
④ Filtering
⑤ Forwarding

10. 시스코 라우터에서 TCP/IP 서비스를 제어하기 위해서 사용하는 명령어 중 그 사용 목적이 다른 것은?

① no service tcp-small-servers
② no ip tcp path-mtu-discovery
③ no ip redirects
④ no ip tcp selective-ack
⑤ no service udp-small-servers

11. 라우터에서 암호를 설정하는 방법 중 지정한 암호가 평문이 아닌 암호화되어 저장되도록 하는 명령어는?

① enable password
② enable secret
③ password
④ enable secret password
⑤ secret password

12. 다음 중 하드웨어 주소를 사용하여 2계층까지 트래픽을 필터링하는 장비는?

① Router
② HUB
③ Bridge
④ Repeater
⑤ L4 Switch

13. 라우터에서 Default route를 설정하는 이유는?

① 네트워크의 기본적인 구성을 위해 설정한다.
② 라우팅 테이블에 전송 경로에 대한 정보가 없는 목적지 주소의 전송을 위해 설정한다.
③ 인터넷에 연결된 스위치 포트의 효과적인 데이터 전송을 위해 설정한다.
④ Network 와 Mask에 "255"로 설정하여 브로드캐스팅의 기능을 수행하도록 설정한다.
⑤ 네트워크에 문제 발생시 관리자에게 통보하는 기능을 수행하기 위해 설정한다.

14. WTLS(Wireless Transport Layer Security)는 SSL(Secure Socket Layer)로 알려진 산업 표준인 TLS 프로토콜에 기반한다. WTLS의 특징이 아닌 것은?

① Data integrity
② RPC
③ Privacy
④ Authentication
⑤ Denial of service protection

16. 라우터에서 원격 관리를 위한 암호를 설정하는 과정이다. 밑줄에 알맞은 명령어는?

```
Router#configure terminal
Router(config)# _______
Router(config-line)#password *****
Router(config-line)#^Z
```

① line terminal 0
② line console 0
③ line vty 0 4
④ line t password 0
⑤ line virtual 0 4

17. 다음 중 허브에 대한 설명으로 적합한 것은?

① 허브는 네트워크를 분리해 주는 분산화 장비라고도 한다.
② 스위칭 허브는 CSMA/CD의 공유 방식을 사용한다.
③ 허브와 라우터는 동일한 계층의 장비이다.
④ 더미 허브와는 달리 스위칭 허브는 각 포트에 연결된 컴퓨터에 독립적인 대역폭을 제공한다.
⑤ OSI 7 계층 중 네트워크 계층에 속하는 장비로써 여러 대의 컴퓨터를 연결할 수 있는 기능을 제공한다.

18. 다음 중 Ping과 Traceroute 명령에 대한 설명으로 옳지 않은 것은?

① Ping 명령으로 네트워크 대역폭을 측정할 수 있다.
② Traceroute 명령의 응답이 '*' 인 경우는 방화벽 존재 가능성을 의미한다.
③ Ping 명령으로 상대방 시스템의 OS 종류를 유추할 수도 있다.
④ Traceroute는 패킷이 지나가는 라우터의 IP주소나 이름을 출력한다.
⑤ Traceroute는 패킷의 진행 경로를 추적함으로써 네트워크와 라우팅의 문제점을 찾아내는 목적으로 많이 사용된다.

19. 다음 중 CISCO 라우터에서 비밀번호를 잃어버렸거나 Flash의 OS가 지워지는 등의 경우에 이용하는 모드는 무엇인가?

① User Mode
② Privileged mode
③ Setup Mode
④ RXBOOT mode
⑤ Global configuration mode

20. 다음 중 스위치에 대한 설명으로 틀린 것은?

① L2 스위치는 Mac Address 기반 스위칭이다.
② L3 스위치는 IP Address 기반으로 트래픽 조절이 가능하다.
③ L4 스위치는 TCP/UDP 포트 정보를 분석해 해당 패킷이 현재 사용하는 서비스 종류별로 패킷을 처리한다.
④ L5 스위치는 트래픽의 내용, 패턴 등을 분석해 패킷을 처리한다.
⑤ 스위치는 허브와는 달리 공유방식을 사용하지 않고, 포트별로 Dedicate한 대역폭을 할당해 준다.

21. 네트워크 공격방법 중 버퍼 오버플로공격과 IP 스푸핑 공격이 각각 속하는 OSI 7 계층에 올바르게 연결된 것은?

① 물리계층 - 응용계층
② 세션계층 - 트랜스포트 계층
③ 응용계층 - 전송계층
④ 응용계층 - 네트워크 계층
⑤ 데이터링크 계층 - 네트워크 계층

22. Switched Network에서 공격자는 위조된 MAC 주소를 지속적으로 네트워크에 흘림으로서 스위칭 허브의 주소 테이블을 오버플로우시켜 허브처럼 동작하게 하여 다른 네트워크 세그먼트의 데이터를 스니핑 할 수 있게 하는 공격 방법은?

① ARP Redirect 공격
② Switch Jamming
③ ARP Spoofing 공격
④ ICMP Redirct 공격
⑤ Ping request

23. 다음 중 네트워크 기반 서비스 거부 공격이 아닌 것은?

① 버퍼 오버플로우 (Buffer Overflow)
② 스머프 (Smurf)
③ SYN 플러딩 (Flooding)
④ 티어드랍 (Teardrop)
⑤ Tiny Fragment

24. 다음 중 Spoofing, Hijacking, Sniffing 등의 방식으로 공격이 가능한 근본적인 이유는?

① TCP/IP의 개방성과 효율을 위한 단순한 설계
② 운영 체제 결함
③ 네트워크 토폴로지 구성 오류
④ 잘못된 시스템 설정
⑤ 컴퓨터 하드웨어의 구조적 결함

25. 다음 중 스텔스 스캔(Stealth scan)의 종류가 아닌 것은?

① TCP open 스캔
② TCP Half-open 스캔
③ XMAS 스캔
④ NULL 스캔
⑤ FIN 스캔

26. 다음 지문의 공격 방법을 방지하기 위한 가장 효과적인 방법은?

> Smurf 공격은 보통 라우터가 패킷을 받아서 다른 포트로 forwarding 할 때 목적지 IP 주소의 네트워크 부분만 참조하고 라우팅 테이블을 검색하여 패킷을 전달하는 점을 이용한 공격 방법이다. Source IP 주소를 자신의 IP 주소가 아닌 공격대상 시스템의 IP 주소로 변조한 후 subnet의 broadcast 주소로 ICMP Echo Request를 보내면 이 패킷은 라우터를 거쳐서 특정 네트워크에 도착하여 모든 시스템이 받게 된다. 그러면 네트워크의 모든 시스템들은 위조된 IP 주소로 ICMP Echo Reply 패킷을 전송하게 된다. 결과적으로 시스템은 Congestion 상태에 빠지게 되어 심각한 서비스 장애를 일으킨다.

① 라우터에서 Direct Broadcast를 Disable 시킨다.
② SNMP Relay 기능을 정지시킨다.
③ 디스크 자원에 쿼터를 설정한다.
④ 65,535byte보다 큰 ICMP Echo 패킷을 IP Fragmentation을 이용하여 전송한다.
⑤ 배너 그래빙을 금지시킨다.

27. 다음 중 공격 방법인 스푸핑 기법(Spoofing)에 대한 설명으로 맞는 것은?

① 네트워크 사용자의 계정을 불법적으로 획득하는 기술
② 패킷에 발신자 IP 주소를 조작하여 공격하는 기법
③ 마지막 몇 개의 숫자를 자르는 방법
④ 시스템에 과부하를 주어 작동 중지 및 서비스 거부를 하게 하는 방법
⑤ 메시지를 가로채었다가 나중에 재전송하는 방법

28. 다음 중 대표적인 네트워크 스캐닝 기능을 가진 툴이 아닌 것은?

① NMAP
② SSCAN2K
③ TRACEROUTE
④ NESSUS
⑤ SAINT

29. 분산 서비스 거부 공격으로 불리는 DDoS(Distributed Denial of Service)는 DOS 공격을 보다 효과적으로 강력하게 공격하기 위한 방법으로 사용된다. DDoS 공격이 일반 공격 방법과 구분되는 특징으로 옳지 않은 것은?

① DDOS 공격 또한 DOS 공격과 마찬가지로 서버의 시스템 장악이나 관리자 계정 획득이 목표가 된다.
② 공격 후 목표 서버는 데이터의 파괴, 삭제, 변조, 유출 등의 피해를 받지 않는다.
③ DDOS 공격 시 원할한 서비스 중단을 목표로 하기 때문에 설정 오류, 서비스 특징, 운영 소프트웨어의 특성, 운영체체의 특성, 사용 프로토콜의 단점 등을 이용하여 매우 다양한 공격의 형태를 취할 수 있다.
④ 공격의 원인 및 공격자를 추적하기 힘든 특성을 가지게 된다.
⑤ 공격 근원지인 컴퓨터의 동작 시점과 실제 공격 시점이 일치하지 않는다.

30. 세션 하이재킹 공격을 탐지하는 방법이 아닌 것은?

① 계속되는 SYN 패킷의 탐지
② Ack Storm 탐지
③ 비 동기화 상태 탐지
④ 패킷의 유실 및 재전송 증가 탐지
⑤ 기대하지 않은 접속의 리셋

31. 다음 중 DDoS 툴이 아닌 것은?

① Trinoo
② TFN
③ TFN 2K
④ Stacheldraht
⑤ Teardrop

32. 3-Way Handshaking 과정에서 Half-Open 연결 시도가 가능하다는 취약성을 이용한 공격은?

① Teardrop
② Land
③ SYN Flooding
④ Smurf
⑤ Ping of Death

33. 특정 네트워크에 대한 해킹기법은 가장 우선순위로 포트스캐닝이 이뤄졌다. 공격을 위해서는 방화벽의 설치 여부를 알 수 있어야 되는데, 방화벽의 설치 여부를 알 수 있는 명령어는?

① banner grabbing
② traceroute
③ nslookup
④ Land 공격
⑤ Smurf

34. 다음 중 허니팟의 요건이 아닌 것은?

① 쉽게 해커에게 노출되지 말아야 한다.
② 쉽게 해킹이 가능한 것처럼 취약해 보여야 한다.
③ 시스템의 모든 구성 요소를 갖추고 있어야 한다.
④ 시스템을 통과하는 모든 패킷을 감시해야 한다.
⑤ 시스템에 접속하는 모든 사람에 대한 정보를 관리자에게 알려줘야 한다.

35. 침입차단시스템(Firewall)을 지나는 패킷에 대해 출발지와 목적지의 IP 주소 및 포트 번호를 특정주소 및 포트로 매핑(Mapping)하는 기능을 무엇이라 하는가?

① Gateway
② Packet Filtering
③ NAT(Network Address Translation)
④ NAU(Network Address Unit)
⑤ VPN(Virtual Private Network)

36. 다음 중 내부 네트워크를 효과적으로 보호하기 위한 접근제어 설정으로 잘못된 것은?

① 외부 비인가자로부터 시스템의 네트워크를 분리시킨다.
② 침입차단시스템 접근제어 설정으로 외부에서 내부로 접근하는 불필요한 서비스에 대한 접근 제한 설정을 한다.
③ 내부 인가자의 부서별로 네트워크를 분리시킨다.
④ IDS(침입탐지 시스템)의 외부, 내부 인가자로 분리하여 네트워크를 단절시킨다.
⑤ 가상사설망을 사용하여 내부 네트워크에 대한 접근 제한 정책을 강화한다.

37. 다음 지문은 시스코 라우터에 설정상태를 확인한 결과로서 필요 없는 snmp 서비스가 설정되어 있다. 이를 해제하는 명령어는 ?

```
현재 설정상태
snmp-server community public RO
snmp-server community private RW

해제 명령어
(  ) snmp-server community public RO
(  ) snmp-server community private RW
```

① no
② disable
③ dis
④ not
⑤ !

38. 침입차단시스템(Firewall)을 통과하는 모든 패킷을 침입차단시스템에서 정의한 보안 정책에 따라 패킷의 통과 여부를 결정하는 역할을 수행하는 기법은?

① Packet Filtering
② NAT(Network Address Translation)
③ Proxy
④ logging
⑤ Access Control

39. 데이터수집 단계, 데이터의 가공 및 축약 단계, 침입 분석 및 탐지 단계, 그리고 보고 및 대응 단계의 4 단계 구성 요소를 갖는 시스템은?

① IDS(Intrusion Detection System)
② Firewall
③ Bridge
④ Gateway
⑤ Honeypot

40. 다음 중 방화벽의 종류에 해당하지 않는 것은?

① 패킷필터링(packet filtering) 방식
② 애플리케이션(Application) 방식
③ 서킷 게이트웨이(Circuit Gateway)
④ 하이브리드(Hybrid) 방식
⑤ 상태전이(State Transition) 방식

과 목	네트워크 보안	07년 1차

1. 서브넷팅에 대한 설명 중 틀린 것은?

① 네트워크 세그먼트로 나눈 개별 네트워크를 말한다.
② 서브넷 마스크는 네트워크 ID와 호스트 ID를 구분 짓는 역할을 한다.
③ 서브넷 마스크는 32비트의 값을 가진다.
④ 각각의 서브넷들이 모여 물리적인 네트워크를 이루어 상호 접속을 수행한다.
⑤ 각각의 서브넷간의 통신은 라우터만을 통해 가능하다.

2. 네트워크 주소변환은 IP 계층에서 동작하기 때문에 응용 프로그램 자체에서 네트워크 주소를 포함하여 전송하는 경우는 처리가 어렵게 된다. 이러한 경우 어플리케이션 게이트웨이를 사용하여 네트워크 서비스를 중계하도록 한다. 아래 보기 중 응용 프로그램 자체에서 네트워크 주소를 포함하여 전송하는 서비스가 아닌 것은?

① FTP
② NetBIOS over TCP/IP
③ RealAudio
④ SMTP
⑤ StreamWorks

3. OSI 7 Layer에서 응용 개체들 사이에 사용되는 구문을 정의하며 보안을 위한 암호화/해독, 그래픽 명령어 해석기능, 데이터 압축 등의 서비스를 제공하는 계층은?

① 세션계층(Session Layer)
② 응용계층(Application Layer)
③ 네트워크계층(Network Layer)
④ 전달계층(Transport Layer)
⑤ 표현계층(Presentation Layer)

4. 인터넷으로 잘 알려진 포트(Well-known Port)로 맞지 않는 것은?

① TFTP : 69
② FTP : 21
③ TELNET : 23
④ SMTP : 11
⑤ FINGER : 79

5. 유닉스 시스템에서 호스트 www.sis.or.kr의 IP 주소를 찾기 위하여 nslookup을 사용하였을 때 결과가 아래와 같이 나왔다. 아래의 결과를 볼 때 다음 중 맞는 설명은?

```
C:₩>nslookup www.sis.or.kr
Server:  name.host.or.kr
Address:  12.34.56.78
Non-authoritative answer:
Name:    www.sis.or.kr
Address:  211.241.82.71
```

① www.sis.or.kr의 IP주소는 211.241.82.71이다.
② nslookup을 실행한 호스트와 www.sis.or.kr은 같은 네트워크 상에 있다.
③ www.sis.or.kr과 name.host.or.kr은 동일 호스트이다.
④ 본 nslookup 결과로는 www.sis.or.kr의 IP 주소를 알 수 없다.
⑤ non-authoritative answer가 의미하는 것은 www.sis.or.kr에 대한 IP 주소 정보가 name.host.or.kr에서 보내온 것이 아님을 의미한다.

6. TCP는 주고받는 패킷의 순서를 보장하기 위하여 32 비트 크기의 순서번호(Sequence Number)를, 패킷의 상태를 나타내기 위해서 플래그를 사용한다. 다음은 TCP의 3-way handshake가 이루어지는 과정에서 오가는 패킷의 플래그와 순서번호를 나열한 것이다. 순서가 맞게 배열된 것은?

```
(1) SYN 40000
(2) ACK 3501
(3) SYN 3500, ACK 40001
```

① (1) → (2) → (3)
② (3) → (2) → (1)
③ (2) → (1) → (3)
④ (1) → (3) → (2)
⑤ (2) → (3) → (1)

7. 다음 중 C Class의 서브넷 마스크로 사용할 수 없는 것은?

① 255.255.255.0
② 255.255.255.128
③ 255.255.255.192
④ 255.255.255.224
⑤ 255.255.255.255

8. 이 프로그램은 ICMP Request 메시지를 특정 호스트에 송신하여, 이에 대한 ICMP Reply를 수신함으로서 호스트의 활성화 여부를 검사해 보고, 요청과 응답에 대한 경과 시간 RTT(Round-Trip-Time)을 알아볼 때 사용한다. 이것은 어떤 프로그램인가?

① traceroute
② ttl
③ time
④ ping
⑤ timestamp

9. 다음 BOOTP와 DHCP에 대한 설명 중 잘못된 것은 무엇인가?

① BOOTP는 RARP를 교체하는 프로토콜이다.
② BOOTP는 다른 서브 네트워크에 있는 서버로 IP주소 할당 요구가 불가능하다.
③ DHCP는 BOOTP의 확장으로 IP주소를 자동으로 할당한다.
④ DHCP는 무선환경같이 신속하게 IP주소를 할당 받기 위해 사용된다.
⑤ DHCP는 다른 서브 네트워크에 있는 서버로 IP주소 할당 요구가 가능하다.

10. 하드웨어 주소만 검사 후 프레임을 Forwarding하는 방식은?

① Cut-through
② Store-and-forward
③ Fragment Check
④ Fragment Free
⑤ Frame Forwarding

11. Traceroute를 통해 전송되는 UDP 패킷에는 불가능한 포트번호(33434)를 붙여서 전

송하는 이유는?

① 목적지에 도달했을 경우 이를 알리기 위해
② 라우터의 과부하를 알리기 위해
③ 잘못된 라우팅 정보를 알리기 위해
④ 라우팅 테이블 변경을 알리기 위해
⑤ 잘못된 정보를 패킷 필터 규칙에 걸러내기 위해

12. 다음은 네트워크 서비스 거부공격으로 인한 접속마비에 대한 현상 및 대응요령을 설명 한 것이다. 다음중 가장 부적절한 것은?

① 이상 트래픽에 의한 네트워크 속도 저하 시 서비스 거부공격을 의심하고 트래픽을 분석한다.
② 서비스 거부공격 시 라우터의 패킷 필터링 기능을 설정하여 대응한다.
③ 리눅스 시스템의 경우 iptables를 이용한 패킷 필터링을 설정한다.
④ 외부에서 들어오는 패킷의 발신지를 확인하여 공격자에게 역공격을 수행한다.
⑤ 특정 서비스(http, smtp 등) 다운 시 서비스 거부공격을 의심하고 로그를 분석한다.

13. SNMP의 매니저 및 에이전트에 있어서 관리 정보 집합을 이르는 말은?

① MIB
② Trap
③ Community
④ SMI
⑤ Device Set

14. 라우터에서 Default router를 설정하는 방법은?

① Network 와 Mask에 모두 “1”을 설정한다.
② Network 와 Mask에 모두 “0”을 설정한다.
③ 인터넷에 연결된 스위치 포트이다.
④ Network 와 Mask에 “255”로 설정한다.
⑤ router default 명령을 사용한다.

15. 컴퓨터의 열린 포트 상태 및 네트워크 상태를 보여주고, 패킷 통계 등의 정보로 활용

할 수 있는 명령어는?

① netstat
② traceroute
③ ifconfig -a
④ tcpdump
⑤ ping

16. 다음 중 반드시 Cross 케이블을 사용하여야 하는 경우에 해당하는 것은?

① 랜카드와 랜카드간 접속시
② 스위치와 랜카드간 접속시
③ 라우터와 스위치간 접속시
④ 스위치와 스위치간 접속시
⑤ 라우터와 IP공유기간 접속시

17. 이더넷(Ethernet) MAC(Media Access Control) Address를 정의하는 표준 Format은 몇 비트인가?

① 8bit
② 16bit
③ 32bit
④ 48bit
⑤ 64bit

18. 네트워크에서 루프 방지책을 고려하지 않았을 경우 발생하는 문제점이 아닌 것은?

① Broadcast storm
② 다중프레임 복제
③ 메시지 전송 시간 증가
④ 고속 패킷 스위칭
⑤ MAC 주소 테이블 안정성 저해

19. 다음 중 Ping과 Traceroute 명령에 대한 설명으로 옳지 않은 것은?

① Ping 명령으로 상대방 시스템의 활성화 여부를 파악할 수 있다.
② Traceroute 명령의 응답이 '*'인 경우는 방화벽 존재 가능성을 의미한다.
③ Ping 명령으로 상대방 시스템의 OS 종류를 파악할 수도 있다.
④ Ping 명령은 ICMP를 이용하지만 Traceroute 명령은 ICMP를 이용하지 않는다.
⑤ Traceroute는 패킷의 진행 경로를 추적함으로써 네트워크와 라우팅의 문제점을 찾아내는 목적으로 많이 사용된다.

20. MAC 주소를 사용해서 침입자를 추적할 수 있는 네트워크 환경은?

① LAN
② WAN
③ Internet
④ MAN
⑤ Extranet

21. Switched Network에서 스니핑 효과를 높이기 위해 사용되는 MAC Flooding 공격이나 MAC Spoofing 공격을 막기 위해 사용될 수 있는 방법은?

① IP Filtering
② Port Security
③ EtherChannel Security
④ Routing Security
⑤ Encryption

22. 다음은 DRDoS(Distributed Reflection Denial of Service)를 설명한 것이다. 순서대로 들어갈 내용은 무엇인가?

DDoS 공격과 달리 숙주가 되는 좀비 컴퓨터를 이용하지 않고, 공격자는 공격대상의 IP로 Spoofing 하여 서버나 라우터에게 ( ) 패킷을 보낸다. 공격대상의 IP 로부터 ( ) 패킷을 받은 라우터나 서버들은 공격대상지로 ( ) 패킷을 최대 4회까지 전송하게 된다.

① ACK - ACK - FIN
② SYN - SYN - ACK/SYN
③ ACK - ACK - RST
④ FIN - FIN - RST
⑤ SYN/ACK - SYN/ACK - RST

23. 서비스 거부 공격 중에서 공격과 해당 공격에 대한 설명이 틀린 것은?

① Land Attack - 출발지와 목적지의 IP주소를 동일시 만드는 공격이다.
② Teardrop - 헤더가 조작된 일련의 IP 패킷조각을 전송하는 공격이다.
③ Targa - 여러 DoS 공격 소스들을 사용하여 통합된 공격 도구를 만드는 것이다.
④ Boink - 패킷 시퀀스 번호를 비정상적인 상태로 보내는 공격이다.
⑤ Ping of Death - Ping를 이용하여 ICMP 패킷을 정상크기 보다 아주 작게 만들어 패킷을 전송하는 공격이다.

24. 연결의 신뢰성을 확보하기 위한 TCP 프로토콜의 시퀀스 넘버를 이용한 공격으로 클라이언트와 서버간의 통신을 관찰할 수 있을 뿐만 아니라, 트러스트를 이용한 거의 모든 세션의 갈취가 가능한 공격은 무엇인가?

① TFN
② Stacheldraht
③ TFN2K
④ IP Spoofing
⑤ Session Hijacking

25. SYN Flooding 공격에 대한 대응 방안에 대한 설명으로 가장 적절한 것은 무엇인가?

① 네트워크로 유입되는 패킷 중에서 소스 주소가 내부IP인 패킷을 차단한다.
② 이 공격에 대한 완전한 해결책은 없으며 단지 영향을 감소시키는 방법들만이 알려져 있다.
③ 사용하지 않는 UDP 서비스를 중지한다.
④ 방화벽 등을 이용하여 패킷 필터링한다.
⑤ 라우터에서 네트워크로부터 자신의 네트워크로 들어오는 IP 브로드캐스트 패킷을 막도록 설정한다.

26. Smurf 공격은 보통 라우터가 패킷을 받아서 다른 포트로 forwarding 할 때 목적지 IP 주소의 네트워크 부분만 참조하고 라우팅 테이블을 검색하여 패킷을 전달하는 점을 이용한 공격 방법이다. Source IP 주소를 자신의 IP 주소가 아닌 공격대상 시스템의 IP 주소로 변조한 후 subnet의 broadcast 주소로 ICMP Echo Request를 보내면 이 패킷은 라우터를 거쳐서 특정 네트워크에 도착하여 모든 시스템이 받게 된다. 그러면 네트워크의 모든 시스템들은 위조된 IP 주소로 ICMP Echo Reply 패킷을 전송하게 된다. 결과적으로 시스템은 Congestion 상태에 빠지게 되어 심각한 서비스 장애를 일으킨다. 이러한 공격 방법을 방지하기 위한 설명 중 내용이 적절하지 못한 것은 ?

① 라우터에서 Direct Broadcast를 Disable 시킨다.
② IP Broadcast 주소로 도착한 ICMP 패킷에 대한 Reply를 금지시킨다.
③ 라우터의 Ingress Filtering을 이용하여 Spoof된 패킷을 막는다.
④ 65,535byte보다 큰 ICMP Echo 패킷을 IP Fragmentation을 이용하여 전송한다.
⑤ 리눅스 시스템에서는 커널 설정 파일에 (net.ipv4.icmp_echo_ignore_broadcasts = 1) 와 같은 설정을 통해 브로드캐스트 주소를 갖는 ICMP Echo 요청을 무시하도록 만든다.

27. 다음은 Session Hijacking에 대한 설명이다. 아래 설명 중 틀린 것은?

① 세션 하이재킹은 TCP 프로토콜의 취약성을 이용한 적극적 공격(Active Attack)의 한 종류이다.
② 세션 하이재킹은 연결의 신뢰성을 확보하기 위한 시퀀스 넘버를 이용한 공격이다.
③ 세션 하이재킹은 TCP 접속 양단을 비동기 상태로 만들어 접속 쌍방이 더 이상 데이터 전송이 불가능 하도록 하는데 있다.
④ 세션 하이재킹은 Telnet, FTP 등 TCP를 이용한 거의 모든 세션의 갈취가 가능하다.
⑤ 세션 하이재킹의 대응방법으로는 일회용 패스워드나 티켓 기반 인증시스템 등이 있다.

28. 다음은 어떤 공격에 대한 설명인가?

보통의 프로그램에 오류를 발생시키는 프로그램 루틴을 무단으로 삽입하여 특정한 조건의 발생이나 특정한 데이터의 입력을 기폭제로 컴퓨터의 부정한 행위를 실행시키는 것이다.

① TCP SYN Flood
② Logic Bomb
③ Smurf
④ Ping of Death
⑤ DRDoS

29. 다음 중 분산서비스거부공격(DDoS)이 아닌 것은?

① Third Party Effect
② TFN 공격
③ TFN2K 공격
④ Stacheldraht 공격
⑤ Trinoo 공격

30. SSH(Secure Shell)은 네트워크 상에서 이루어지는 데이터 전송 시의 보안상 허점을 해결하고자 제시된 방법이다. SSH로 방어할 수 있는 공격은?

① IP Spoofing
② IP 소스 라우팅
③ 버퍼 오버플로우
④ 중간 경유 노드에서 데이터 가로채기
⑤ 바이러스 침해

31. 다음 설명에 해당되는 공격 유형은?

> TCP의 연결방식의 구조적 문제점을 이용한 방법이다. 특정 포트에 대해 공격자가 SYN 패킷을 보내면 대상 서버는 SYN/ACK 패킷을 보낸다. 이 때 공격자가 ACK 패킷을 보내면 TCP 연결이 완성되는데 SYN/ACK 패킷을 받은 후 ACK 패킷을 보내지 않으면 대상 서버는 ACK 패킷을 일정시간 동안 기다리다 다시 정상상태로 돌아온다. 이 때를 틈타 공격자가 계속해 SYN 패킷을 보내고 ACK패킷을 보내지 않으면, 대상 서버는 순간적으로 많은 양의 접속을 대기하다가 더 이상 해당 포트에 대해 SYN 패킷을 받지 못해 서비스를 하지 못한다.

① Hip based Buffer Overflow
② Stack based Buffer Overflow
③ Format string
④ SYN Flooding
⑤ TCP Session Hijacking

32. 네트워크를 통한 원격 공격 형태의 해킹 기법과 가장 거리가 먼 것은?

① Connection Hijacking
② SYN Floodiing
③ Race Condition Attack
④ Connection Killing by RST
⑤ IP Spoofing

33. 라우팅 루프 문제를 해결하기 위한 방법으로 네트워크에 문제가 발생하면 라우터가 네트워크 경로를 라우팅 테이블에서 지우는 것이 아니라 네트워크 도달 홉 카운트를 높여 도달 불가능한 곳으로 지정하여 라우팅 루프 문제를 해결하는 방식을 무엇이라 하는가?

① Poison Reverse
② Triggered update
③ Split horizon
④ Hop count
⑤ Hold down

34. 최근 인터넷은 침입차단시스템의 도입으로 과거와는 달리 안정화 되었다고 할 수 있다. 특정 네트워크에 대한 해킹기법은 가장 우선순위로 포트스캐닝이 이뤄졌다. 침입차단시스템에 대한 포트스캐닝 기법으로 다음 중 틀린 것은?

① 침입차단시스템은 TCP의 최초 SYN 패킷을 차단한다.
② 포트를 순차적으로 증가시키지 않고 랜덤하게 생성하여 스캐닝한다.
③ 최초 SYN 패킷을 보내지 않고 ACK, SYN/ACK 등의 패킷을 보내 반응을 본다.
④ 최초 패킷이 FIN 일 경우 침입차단시스템을 통과할 수 있다.
⑤ 패킷조작에도 반응이 없다면 해당 포트는 닫혀진 것으로 본다.

35. 다음 설명 중에서 올바른 것은?

① 라우터는 세션 계층 접속을 지원한다.
② 브리지는 네트워크 계층 접속을 지원한다.
③ 리피터는 감쇄된 신호를 재생하는 장치이다.
④ 게이트웨이는 프로토콜이 다른 네트워크들을 연결할 수 없다.
⑤ 허브는 경로선택 기능을 수행한다.

36. 다음 스니핑 도구 중 성질이 다른 하나는 ?

① airsnort
② kismet
③ airopeek
④ wireless sniffer pro
⑤ ethereal

37. 네트워크를 관리하기 위한 용도로 NMS를 도입하고자 한다. 다음 중 NMS를 이용하여 관리 가능한 것과 거리가 먼 것은 ?

① 호스트의 네트워크 연결 상태
② 네트워크 트래픽 현황
③ 호스트의 CPU 사용량
④ 네트워크 구성도
⑤ 호스트별 네트워크 트래픽 현황

38. ICMP는 호스트 서버와 인터넷 게이트웨이 사이에서 메시지를 제어하고 에러를 알려주는 프로토콜로서 RFC 792에 정의되어있다. ICMP는 IP 데이터그램을 사용하지만, 메시지는 TCP/IP 소프트웨어에 의해 처리되며, 응용프로그램 사용자에게 직접 분명하게 보이지는 않는다. 일례로서, ping 명령어는 인터넷 접속을 테스트하기 위해 ICMP를 사용한다. ICMP 스캔이나 ICMP bomb 탐지에 사용될 수 있는 리눅스 도구는 무엇인가?

① ls -als
② fstab
③ du -f
④ icmpinfo
⑤ traceroute

39. 프락시 형태의 방화벽은 OSI 7 Layer의 어느 계층에서 동작하는가?

① 4 (전송 계층)
② 5 (프레젠테이션 계층)
③ 6 (세션 계층)
④ 7 (응용 계층)
⑤ 3 (네트워크 계층)

40. 내부 네트워크와 외부 네트워크 사이에 위치하여 외부에서의 침입을 1차로 방어해 주며 불법 사용자의 침입차단을 위한 정책과 이를 지원하는 소프트웨어 및 하드웨어를 제공하는 것은?

① IDS(Intrusion Detection System)
② Firewall
③ Bridge
④ Gateway
⑤ Honeypot

정 보 보 호 전 문 가 2 급 필 기

과 목	정보보호론	07년 2차

1. 해쉬 함수의 성질 중에서 충돌 저항성(collision resistance)을 올바르게 표현한 것은?

① 동일한 해쉬 출력 값을 갖는 임의의 서로 다른 입력 x와 x'을 찾아내는 것이 계산적으로 불가능한 것을 의미한다.
② 임의의 주어진 x에 대하여 이것의 해쉬 값과 동일한 출력값을 갖는 x'을 찾는 것이 계산적으로 불가능한 것을 의미한다.
③ 임의의 해쉬출력 값에 대해서 입력을 올바르게 유추하는 것이 계산적으로 불가능한 것을 의미한다.
④ 서로 다른입력 값은 서로 다른출력 값을 가져야 함을 의미한다.
⑤ 해쉬 함수의 입력 길이와 출력 길이가 일치해야 함을 의미한다.

2. 공개키 암호 시스템의 암호학적 안정성은 적용된 수학적 문제의 해결 어려움에 기인한다. 다음 중 적용된 수학적 기반이 동일한 공개키 암호 시스템으로 짝지어진 것은?

① ECC - RSA
② ElGamal - ECC
③ RSA - ElGamal
④ Rabin - ElGamal
⑤ RSA - Rabin

3. 다음 중 최근에 소개된 Wang의 분석방법 등 다양한 해쉬함수 분석에 대하여 2^{128} 이상의 안전성을 제공하도록 설계되어 2006년 12월 27일 제정된 국내 표준번호 TTAS.KO-12.0039의 해쉬함수는?

① HAS-160
② SEED
③ TSC-4
④ HIGHT
⑤ FORK-256

4. 다음 블록 암호 사용 모드 중 초기화 벡터를 필요로 하지 않는 것은?

① 카운터 (counter) 모드
② 전자코드북 (electronic codebook) 모드
③ 암호블록 연결 (cipher block chaining) 모드
④ 암호피드백 (cipher feedback) 모드
⑤ 출력피드백 (output feedback) 모드

5. Diffe-Hellman 알고리즘은 비밀키(Secret-Key)를 공유(키 교환)하는 알고리즘이며 특정 공격에 취약한 점을 가지고 있다. Diffe-Hellman 알고리즘에 흔히 적용되는 공격은?

① 중간자공격 (man-in-the-Middle attack)
② 재전송공격 (replay attack)
③ 강제지연 공격 (forced-delay attack)
④ 반사공격 (reflection attack)
⑤ 전수조사 공격 (brute-force attack)

6. 다음 중 하드웨어 구현을 목적으로 설계된 LFSR 기반 키 스트림 생성기로 볼 수 없는 것은?

① SEAL
② MUX generator
③ BRM generator
④ Alternating step generator
⑤ Shrinking generator

7. 다음 중 두 사용자가 안전하게 비밀키를 공유하고, 이를 암호화에 이용하려는 목적으로 만든 알고리즘은?

① RSA
② Diffie-Hellman
③ ElGamal
④ DES
⑤ RIPEMD-160

8. 다음 지문에서 설명하고 있는 블록 암호 알고리즘으로 알맞은 것은?

◦ RSA와 더불어 PGP에 채택되어 사용 ◦ SPN 구조를 사용하는 알고리즘 ◦ 64비트의 평문 블록, 128비트의 키 길이, 8라운드 암호 방식 적용

① Blowfish
② IDEA
③ MISTY
④ RC5
⑤ CAST

9. 다음 중 카운터 모드의 설명으로 틀린 것은?

① 각 블록을 독립적으로 암호화 한다.
② 초기값이 바뀌면 같은 평문에 대해서도 다른 암호문을 얻을 수 있다.
③ 암호화 알고리즘과 복호화 알고리즘이 다르다.
④ 암호문의 오류는 복호화 과정에서 대응되는 한 블록에만 영향을 미친다.
⑤ 동일한 초기값과 비밀키를 반복하여 사용하면 안전성에 문제가 생긴다.

10. 다음 중 전자서명에 대한 설명으로 옳지 않은 것은?

① 수신자가 문서를 재사용 할 수 있다.
② 송신자가 문서에 대하여 부인을 할 수 없다.
③ 서명된 문서가 변형되지 않았다는 무결성(Integrity)을 보장한다.
④ 문서 내용에 대한 기밀성을 보장하지는 못한다.
⑤ 송신자의 신원을 확인할 수 있다.

11. 다음 중 해쉬함수가 아닌 것은?

① SHA-1
② MD5
③ RIPEMD-160
④ HAVAL
⑤ RC5

12. PKI 인증서 관리구조에 대한 설명 중 틀린 것은?

① 계층적 구조는 인증경로 탐색이 용이하다.
② 계층적 구조는 모든 사용자가 최상위 인증기관의 공개키를 알고 있으므로 인증서 검증이 용이하다.
③ 네트워크 구조는 서명 검증을 보장하는 단일 인증경로를 제공한다.
④ 네트워크 구조는 원격 CA 사이의 직접적인 상호인증을 통해 빈번한 사용자들에 대한 인증경로 처리 절차가 간소하다.
⑤ 혼합형 구조는 다양한 형태의 상호인증서가 필요한 단점이 있다.

13. 다음 중 비밀키(Secret-Key) 암호화 알고리즘만으로 보장하기 어려운 것은?

① 서버 인증
② 기밀성
③ 송신자 인증
④ 송신자 부인 방지
⑤ 무결성

14. 다음 중 전자서명의 특징으로 틀린 것은?

① 부인방지
② 재사용방지
③ 데이터의 무결성
④ 데이터의 가용성
⑤ 서명자 인증

15. 다음 지문에서 설명하고 기술에 해당하는 것은?

유효 기간 없이, 매 세션마다 서로 상이한 패스워드를 사용하면, 특정 세션의 개인 식별 과정에서 해당 패스워드가 노출되어도 다른 세션에 사용될 패스워드를 예측할 수 없다.

① MAC(Message Authentication Code)
② PKI(Public Key Infrastructure)
③ PMI(Privilege Management Infrastructure)
④ PAM(Pluggable Authentication Modules)
⑤ OTP(One Time Password)

16. 다음 중 공개키 암호 시스템에 대한 설명으로 틀린 것은?

① 실제로 응용되기 위해서는 인증기관이 필요하다.
② 일반적으로 속도 면에서 대칭키 암호 시스템 보다 느리다.
③ 대칭키 암호 시스템에서 필요 없는 안전한 키 분배가 필요하다.
④ 1976년 Diffie와 Hellman에 의해 공개키 암호의 개념이 소개되었다.
⑤ 암호화 함수에는 일방향성 함수의 개념이 사용된다.

17. 다음 지문은 어떤 것에 대한 설명인가?

◦ 정보보호의 목적인 정보자산의 기밀성, 무결성, 가용성을 실현하기 위한 절차와 과정을 체계적으로 수립, 문서화하고 지속적으로 관리, 운영하는 시스템이다. ◦ 2002년 4월 시행된 이후 제도의 활성화를 위해 심사, 상담, 자문, 지침배포 등에 대한 교육을 한국정보보호진흥원에서 실시하고 있다. ◦ 조직에 적합한 정보보호를 위해 정책 및 조직수립, 위험관리, 대책구현, 사후관리 등의 정보보호관리 규정을 정리하고 이를 통해 구현된 여러 정보보호 대책들이 유기적으로 통합된 체계를 갖추었는지, 제3자의 인증기관인 한국정보보호진흥원을 통해 객관적이고, 독립적으로 평가하여 인증기준에 대한 적합 여부를 주는 제도이다.

① BS7799 국제정보보호인증
② ISO27001 국제정보보호인증
③ e트러스트 인증
④ 인터넷사이트 안전마크 인증
⑤ 정보보호관리체계(ISMS) 인증

18. 정보보호관리체계에 대한 표준으로 최상의 정보보호관리를 위한 포괄적인 일련의 관리 방법에 대하여 요건 별로 해석해 놓은 규격으로 기업이 고객정보의 기밀성, 무결성, 가용성을 보장한다는 것을 공개적으로 확인하는 것이 목적인 것은?

① AS7799
② BS7799
③ ITSEC
④ TCSEC
⑤ TDI

19. 다음 중 정보시스템 보안을 위해 고려해야 할 사항으로서 적절하지 않은 것은?

① 백업데이타의 안전한 복구를 위하여 조직의 환경에 적합한 지침에 따라 하여야 한다.
② 시스템이 자연재해로 인해 피해를 보지 않도록 예방하는 등 시스템 자체의 신뢰도를 체크한다.
③ 가능한 한, 많은 사람들이 시스템에 접근할 수 있도록 하여 이를 공유한다.
④ 백업은 full backup과 incremental backup의 사본을 원격지에 소산하여 보관한다.
⑤ 사용자들의 권한은 필요한 직무수행을 위한 최소 권한으로 지정한다.

20. 다음 중 민감한 업무대상(정보 및 절차)은 오직 인가된 사람들에게만 공개되어야 한다는 것과 관계가 있는 것은?

① 무결성
② 기밀성
③ 가용성
④ 가로채기 (Interception)
⑤ 가장 (Masquerade)

21. 다음 지문이 설명하고 있는 용어는?

위험을 평가하고, 피해자가 수용할 수 있는 수준까지 위험 부담을 줄이기 위한 조치를 강구하며, 그러한 위험을 용인할 수 있는 수준으로 유지하는 것을 말한다.

① 위험 관리
② 위험 분석
③ 위험 평가
④ 위험 기준
⑤ 위험 전가

22. 다음 중 위험분석 방법론에 대한 설명으로 틀린 것은?

① 확률 분포법은 미지의 사건을 확률적 편차를 이용하여 최저, 보통, 최고의 위험평가를 예측할 수 있다.
② 과거자료 분석법은 과거의 자료를 통해 위험발생 가능성을 예측하는 방법으로서 과거 자료가 많을수록 분석의 정확도가 높아진다.
③ 수학공식 접근법은 위협의 발생빈도를 계산하는 식을 이용하여 위험을 계량하는 방법이다.
④ 순위결정법은 비교우위 순위 결정표에 위험 항목들의 서술적 순위를 결정하는 방법이다.
⑤ 델파이법은 어떤 사건도 기대대로 발생하지 않는다는 사실에 근거하여 일정 조건하에서 위협에 대한 발생 가능한 결과들을 추정하는 방법이다.

23. 다음 중 정보보호 조직 구성원의 책임에 대한 설명으로 틀린 것은?

① 최고 경영자는 정보보호를 위한 총괄책임이 있다.
② 데이터 관리자는 조직의 정보보호 정책, 표준, 대책, 실무 절차를 설계, 구현, 관리, 조사할 책임이 있다.
③ 프로세스 관리자는 해당 정보시스템에 대한 조직의 정보보호 정책에 따라 적절한 보안을 보증할 책임이 있다.
④ 기술지원 인력은 보안대책의 구현에 대하여 조언할 책임이 있다.
⑤ 정보시스템 감사자는 보안 목적이 적절하고 정보보호 정책, 표준, 대책, 실무 및 절차가 조직의 보안 목적에 따라 적절하게 이루어지고 있음을 관리자에게 보증할 책임이 있다.

24. 다음 중 프로젝트 보안 담당자와 시스템 보안 담당자의 주요 임무에 대한 내용으로 틀린 것은?

① IT 보안 프로그램 실행을 모니터링
② 정보보호 관리팀 및 조직 IT 보안 담당에 대한 연락 및 보고
③ IT 프로젝트 또는 시스템 보안 정책을 수립 및 유지
④ 정보보호 계획을 개발 및 구현
⑤ 사고 조사의 착수 및 지원

25. 정보보호관리 프로세스는 5단계로서 전체 14개의 통제사항을 필수항목으로 요구한다. 다음 중 위험관리 단계의 통제사항이 아닌 것은?

① 위험관리전략 및 계획 수립
② 정보자산의 식별
③ 위험분석
④ 위험평가
⑤ 정보보호 계획 수립

26. 다음 중 물리적 보안에서 말하는 방어의 최후에 위치하는 것으로 맞는 것은?

① 시스템
② 내부장벽
③ 사람
④ 보안 소프트웨어
⑤ 보안 운영체제

27. 다음 중 보안 관리 활동에 대한 설명으로 옳지 않은 것은?

① 사용자 계정 지침 및 절차 구성
② 파일 시스템 관리 지침 및 절차 구성
③ 보안 점검 기록관리(서버실 출입일지 구성)
④ 시스템 사용 신청
⑤ 매체의 보존 및 폐기 절차 구성

28. 자산에 대한 취약성과 위협을 분석하고 발생가능성과 그 영향에 따라 위험의 내용과 정도를 결정하는 일련의 과정을 무엇이라 하는가?

① 보안 관리
② 위험 분석
③ 정책 관리
④ 정보시스템 분석
⑤ 감사

29. 다음 지문은 네트워크 환경을 통한 일반 침입형태에 대한 설명이다. 무엇이라 하는가?

(인가받지 않은 제 3자가 통신 데이터를 수신지로 가는 도중에 몰래 sniffing기법을 활용하여 엿보거나 도청하는 행위)

① 위장(masquerade)
② 변조(modification)
③ 위조(fabrication)
④ 차단(interruption)
⑤ 가로채기(interception)

30. 다음 중 정보보호의 목적과 거리가 먼 것은?

① 기밀성 및 무결성 서비스
② 효율성 서비스
③ 인증 서비스
④ 접근제어 서비스
⑤ 부인방지 서비스

31. 다음 지문에서 설명하고 있는 정보보호 대책 활동을 무엇이라 하는가?

탐지 통제를 통해 발견된 문제들을 해결하기 위해서는 발견된 문제들의 발생 원인과 영향을 분석한다. 그리고 분석된 내용들을 바탕으로 문제의 향후 발생을 최소화하기 위하여 시스템을 변경하는 등의 일련의 활동을 수행한다.

① 예방 통제
② 위험 수용
③ 교정 통제
④ 잔류 위험
⑤ 대책 식별

32. 위험분석의 방법론 중 정량적 위험분석의 방식이 아닌 것은?

① ALE(연간예상손실)
② 과거자료 분석법
③ 수학공식 접근법
④ 확률 분포법
⑤ 델파이법

33. 개인정보분쟁조정위원회의 개인정보 관련 분쟁의 조정 등의 처리 절차에 관하여 맞지 않는 것은?

① 개인정보와 관련한 분쟁이 있으면, 반드시 분쟁조정위원회에 분쟁의 조정을 신청하여야 한다.
② 분쟁조정위원회는 분쟁조정을 위하여 필요한 자료의 제공을 분쟁당사자에게 요청할 수 있다.
③ 분쟁조정위원회는 필요하다고 인정하는 경우에는 분쟁당사자 또는 참고인으로 하여금 분쟁조정위원회에 출석하게 하여 그 의견을 들을 수 있다.
④ 분쟁조정위원회는 분쟁의 성질상 분쟁조정위원회에서 조정함이 적합하지 아니하다고 인정하거나, 부정한 목적으로 신청되었다고 인정하는 경우에는 당해 조정을 거부할 수 있다.
⑤ 분쟁조정위원회는 신청된 조정사건에 대한 처리절차를 진행 중에 일방 당사자가 소를 제기한 때에는 그 조정의 처리를 중지하고 이를 당사자에게 통보하여야 한다.

34. 전자서명법 제15조(공인인증서의 발급) 2항에서 정한 공인인증기관이 발급하는 공인인증서에 포함되어야 하는 것이 아닌 것은?

① 가입자의 이름
② 공인인증기관의 명칭
③ 인증서의 일련번호 및 유효기간
④ 가입자의 전자서명검증정보
⑤ 인증서 취소 목록 및 가입자의 전자서명 생성키

35. 정보통신서비스제공자는 이용자의 개인정보를 이용하려고 수집하는 때에는 일정한 사항에 대하여 이용자에게 알리고 동의를 얻어야 하며, 또한 이를 변경하려는 때에도 그렇게 하여야 하는 바, 여기에서 말하는 그러한 사항으로 보기 어려운 것은?

① 개인정보의 수집
② 수집하는 개인정보의 항목
③ 개인정보의 이용목적
④ 개인정보의 검색 방법
⑤ 개인정보의 보유 및 이용 기간

36. 정보통신망이용촉진및정보보호등에관한법률 제3조 제3항에 의하면 정부는 정보통신서비스제공자단체 또는 이용자단체의 (A) 및 정보통신망에서의 (B) 등을 위한 활동을 지원할 수 있다. A와 B에 적합한 단어는?

① A – 이용자 권익보호, B – 개인정보보호
② A – 개인정보보호, B – 시스템 보호
③ A – 정보자료 안정성의 보호, B – 정보통신기반보호
④ A – 정보산업보호, B – 정보통신시설의 보호
⑤ A – 개인정보보호, B – 청소년보호

37. 정보통신기반보호법상 국가안전보장에 중대한 영향을 미치는 주요정보통신기반시설로서 규정되지 아니한 것은?

① 도로·지하철·공항 시설
② 자동차·전차·철강 등 국가기간산업시설
③ 방송중계·국가지도통신망 시설
④ 원자력·국방과학 관련 정부출연연구기관의 연구시설
⑤ 첨단방위산업 관련 정부출연연구기관의 연구시설

38. 개인정보분쟁조정위원회의 조정안을 제시받은 당사자는 그 제시를 받은 날부터 몇일 이내에 그 수락여부를 개인정보분쟁조정위원회에 통보하여야 하는가?

① 7일
② 10일
③ 2주
④ 15일
⑤ 30일

39. 정보통신기반보호법 제10조 보호지침에 의하면, 관계 중앙행정기관의 장은 소관분야의 주요정보통신기반시설에 대하여 보호지침을 제정하고 해당분야의 ( )에게 이를 지키도록 ( )할 수 있다. ( ) 속에 들어갈 말을 순서대로 열거한 것은?

① 정보보호컨설팅 전문업체, 명령
② 관리기관의 장, 권고
③ 관리기관의 장, 요청
④ 사업자, 권고
⑤ 사업자, 요청

40. 아래는 정보통신망 이용촉진 및 정보보호 등에 관한 법률의 한 규정의 내용이다. (　　)안에 들어갈 말로서 바르게 나열된 것은?

> “정보통신서비스제공자는 이용자의 개인정보를 (　　)하려고 (　　)하는 때에는 다음 각 호의 (　　) 사항에 대하여 이용자에게 알리고 (　　)를 얻어야 한다. 다음 각 호의 어느 하나의 사항을 (　　)하려는 때에도 또한 같다.
> 1. 개인정보의 수집·이용 목적
> 2. 수집하는 개인정보의 항목
> 3. 개인정보의 보유 및 이용 기간

① 이용 - 수집 - 모든 - 동의 - 변경
② 보유 - 수집 - 모든 - 동의 - 변경
③ 이용 - 보유 - 개별 - 양해 - 수정
④ 사용 - 보유 - 개별 - 양해 - 수정
⑤ 이용 - 수집 - 모든 - 양해 - 변경

과 목	정보보호론	07년 1차

1. 다음 중 해쉬함수의 성질을 잘못 설명한 것은?

① 입력 값으로부터 해쉬 값을 계산하는 것은 쉬우나 역으로 해쉬 값으로부터 입력 값을 찾는 것은 계산상으로 불가능하다.
② 해쉬 값이 같은 서로 다른 두 입력 값은 반드시 존재한다.
③ n 비트 암호문을 출력하는 블록 암호 알고리즘을 사용하여 해쉬함수를 만들면 해쉬값 역시 n 비트 이다.
④ 해쉬함수는 부가형 전자서명에 사용된다.
⑤ 생일역설은 해쉬함수의 안정성을 보장하기 위한 해쉬값 길이를 결정하는데 도움을 준다.

2. 확률 공개키 암호는 동일한 평문에 대하여 암호화 수행 때 마다 다른 암호문을 생성하여 안전성을 향상시키는 방법이다. 이러한 방식의 공개키 암호가 아닌 것은?

① Goldwasser-Micali 암호
② Blum-Goldwasser 암호
③ Rabin 암호
④ ElGamal 암호
⑤ Bellare-Rogaway 암호

3. 식별(Identification) 프로토콜은 패스워드 프로토콜, 시도-응답 프로토콜, 영지식(Zero - Knowledge) 프로토콜 등으로 분류된다. 이 들을 안전성이 강한 순서대로 올바르게 나열한 것은?

① 영지식 > 패스워드 > 시도-응답
② 시도-응답 > 패스워드 > 영지식
③ 영지식 > 시도-응답 > 패스워드
④ 패스워드 > 시도-응답 > 영지식
⑤ 시도-응답 > 영지식 > 패스워드

4. 인터넷에서는 많은 공격 방법이 존재한다. 아래는 공격방법과 대처 방법을 나열한 것이다. 적절하지 않은 것은?

① 재전송 공격 : 메시지에 타임스탬프 또는 일련번호를 포함함으로써 막을 수 있다.
② 메시지의 송수신 부인 : 송수신 행위에 대해 전자서명을 삽입한다.
③ 정보의 변조 공격 : 전송 메시지에 대한 해쉬값을 같이 전송한다.
④ 중재자 공격(Middle-man attack) : 통신 당사자 인증을 사용한다.
⑤ 스니핑 공격 : 키가 있는 해쉬함수를 이용하여 메시지 출처 인증한다.

5. 인증기관(CA; Certification Authority)의 중요한 책임과 가장 거리가 먼 것은?

① 사용자 인증서 생성, 발급, 갱신
② 사용자 인증서 폐지 목록 발급
③ 사용자 신분 확인
④ 사용자 정보를 관리
⑤ 사용자 개인키 보관

6. DES 알고리즘에 대한 설명으로 옳지 않은 것은?

① 비밀키를 사용하여 데이터를 암호화하는 방법으로서 널리 사용되고 있다.
② 다른 비밀키 암호화 방법과 마찬가지로, 송신자와 수신자는 사전에 동일한 비밀키를 공유하고 사용해야만 한다.
③ 메시지를 64비트 단위의 블록으로 나누어 암호화 한다.
④ 8개의 S-박스는 선형논리로 작성되어 있다.
⑤ 복호화 연산이 암호화 연산과 동일한 파이스텔 구조로 되어 있다.

7. 전자 인증체계를 위한 구성 요소가 아닌 것은?

① 키 분배 센터 (KDC : Key Distribution Center)
② 인증기관 (CA : Certification Authority)
③ 등록기관 (RA : Registration Authority)
④ 디렉토리
⑤ 최종 개체 (사용자)

8. 단일 사용자 인증(Single Sign On : SSO)에 대한 다음 설명 중 틀린 것은?

① 한번의 로그인으로 여러 개의 시스템에 대한 사용자 인증을 할 수 있다.
② C/S환경과 legacy 시스템과의 연동도 가능하다.
③ 자원별로 권한을 부여하여 접근을 통제한다.
④ PKI 기반의 인증서를 사용할 수 있다.
⑤ SSO 지원 메커니즘으로 커버로스 프로토콜이 있다.

9. 권한 부여의 의미로서 사용자가 응용 시스템에 대한 사용 권한을 부여 받는 것을 무엇이라 하는가?

① 인증 (Authentication)
② 인가 (Authorization)
③ 전자 서명 (Digital Signature)
④ 부인 봉쇄 (Non-Repudiation)
⑤ 키 분배 (Key Distribution)

10. 다음 중 AES 알고리즘의 설명 중 틀린 것은?

① 128비트, 192비트, 256비트의 블록 단위로 암호화를 수행할 수 있다.
② 첫 라운드를 수행하기 전에 평문과 라운드 키의 XOR 연산을 한다.
③ 마지막을 뺀 각 라운드는 바이트 대치, 행 옮김, 열 조합, 라운드 키 XOR로 구성된다.
④ 마지막 라운드에서는 열 조합 연산을 수행하지 않는다.
⑤ AES는 파이스텔 구조이기 때문에 복호화 과정은 암호화 과정과 같다.

11. 암호에 관한 다음 설명 중 가장 부적절한 것은?

① 암호화 알고리즘은 기밀성을 제공하며, 무결성이나 인증 지원에는 사용하지 않는다.
② 암호화 알고리즘은 평문을 암호문으로 변환시킨다
③ 복호화 알고리즘은 암호문을 평문으로 변환시킨다.
④ 정당한 사용자가 아닌 제3자가 불법적으로 암호문으로부터 평문을 복원하는 시도를 암호해독이라고 한다.
⑤ 암호화와 복호화에 사용되는 함수를 암호 알고리즘이라고 한다.

12. 암호화와 복호화에 서로 다른 키를 사용하며, 이들 중 복호화 키만 비밀로 간직해야 하는 암호 방식은 어느 것인가?

① 고전 암호
② 관용 암호
③ 대칭 암호
④ 공개키 암호
⑤ 스트림 암호

13. 공개키 암호화 알고리즘에서 인증되지 않은 공개키를 사용한다면 이는 다양한 공격에 노출될 수 있다. 따라서 공개키에 대한 신뢰할 수 있는 인증서를 발급하는 공개키 기반구조(PKI) 시스템이 필요하다. 이 때 공개키 인증서의 형식으로 널리 사용되는 표준은 무엇인가?

① X.400
② X.409
③ X.500
④ X.509
⑤ X.25

14. 공개키 암호화는 전자상거래, 인트라넷, 엑스트라넷 및 다른 웹 기반 응용 프로그램에 있어 중요한 기술이다. 다음 중 공개키 암호화에 대한 올바른 설명이 아닌 것은?

① 암호화를 위해 공개키와 개인키를 사용한다.
② 처리 속도가 느려 대량의 데이터 암호화에는 적합하지 않다.
③ 공개키 암호화는 대칭 구조를 가진다.
④ 공개키를 사용하여 암호화하면 개인키를 이용하여 복호화한다.
⑤ 전자서명에도 사용된다.

15. 암호화에서 보는 메시지 다이제스트(Message Digest) 알고리즘에 대한 설명으로 부적절한 것은?

① 메시지 다이제스트 알고리즘은 일반적인 압축프로그램(PKxip, winZip, gzip)처럼 압축 및 복구 기능을 갖는다.
② 메시지 다이제스트 문장은 암호 응용에서 원본 데이터를 대신하는 효과를 내기도 한다.
③ 메시지 다이제스트는 전자서명의 효용성을 향상시키는데 사용된다.
④ 메시지 다이제스트 알고리즘은 체크섬(Checksum) 기능도 포함한다.
⑤ 서로 다른 메시지가 동일한 메시지 다이제스트 값을 가질 확률은 극히 낮아야 한다.

16. 다음 중 블록 암호 설계 원리인 Feistel 구조의 특징이 아닌 것은?

① 라운드 함수에 대한 제약 조건이 없다.
② 복호화시 라운드 함수의 역변환이 필요하다.
③ 3라운드 이상이며 짝수 라운드로 구성된다.
④ 2 라운드의 수행으로 블록간의 완전한 확산이 이루어진다.
⑤ 복호화시 라운드 키가 역순으로 사용된다.

17. 정보보호에 있어서의 일반적인 보안 요구사항에 관한 설명으로서 허가 되지 않는 사람에 의한 정보의 변경, 삭제, 생성 등으로부터 보호하는 조치에 해당되는 것은?

① 기밀성 (Confidentiality)
② 무결성 (Integrity)
③ 가용성 (Availability)
④ 부인방지 (Non-repudiation)
⑤ 신뢰성 (Reliability)

18. 개인정보분쟁조정위원회가 신청된 조정사건에 대한 처리절차를 진행중에 일방 당사자가 소를 제기한 때에 취하여야 하는 행위는?

① 소의 제기에 따른 법원에서의 심리와는 관계없이 조정은 진행하여야 한다.
② 조정의 처리는 진행하면서 이러한 사실을 당사자에게 통보하여야 한다.
③ 조정의 처리를 중지하고, 이를 당사자에게 통보하여야 한다.
④ 조정의 처리를 종결하고 당해 조정의 결과를 당사자에게 통보하여야 한다.
⑤ 조정의 처리를 종결하고 당해 조정의 결과를 법원에 통보하여야 한다.

19. 정보보호의 정책에 관하여 바르게 설명한 것으로 보기 어려운 것은?

① 정보보호의 정책이라 함은 특정 조직의 정보자산에 접근하려는 사람이 따라야 하는 규칙의 내용이다.
② 정보보호의 정책 목표가 결정되어야 정보보호에 관한 적절한 결정이 이루어지게 된다.
③ 정보보호의 정책을 결정함에 있어서 정보보호관리자는 시스템 사용의 용이성을 최우선의 과제로 선정하는 것이 적절하다.
④ 정보보호의 정책 내용에는 정보보호에 필요한 수준에 따른 정보 자산의 분류를 제시하여야 한다.
⑤ 정보보호의 정책 내용에는 준수해야 할 표준, 관례 및 절차와 바이러스 방지, 패스워드, 암호화 등을 포함하여야 한다.

20. 위험분석이란 정보시스템과 그 자산의 비밀성(confidentiality), 무결성(integrity), 가용성(availability), 책임추궁성(accountability)에 영향을 미칠 수 있는 다양한 위협에 대해서 정보시스템의 취약성을 인식하고, 이로 인해서 예상되는 손실을 분석하는 것인 바, 이 위험 분석에서 사용되는 핵심 요소가 아닌 것은?

① 자산
② 위협
③ 취약성
④ 규정준수
⑤ 위험 대책

21. 사후관리에 있어서의 사고 대처 능력(Incident Response Capability)과 가장 관계가 적은 것은?

① 정확한 측정을 수행하는 것을 도울 수 있도록 사고를 분석한다.
② 과거의 사고와 대처 행위에 대한 DB Repository를 개발한다.
③ 사고 관련 정보 공유를 위한 정책과 절차를 마련한다.
④ 보안 담당, IS요원, 법률 전문가 등으로 구성된 징계위원회를 설치한다.
⑤ 상세운영계획을 개발하여 사고로부터 복구하기 위한 구체적인 대처행위를 요약한다.

22. 다음에 기술되어 있는 내용의 ( )안에 들어갈 적당한 용어가 순서대로 올바르게 나열한 것은?

( )의 목적은 ( )을(를) 효율적으로 하고자 하는데 목적이 있다. 즉, 위험도가 높은 것에 대하여 우선적으로 대응하여 비용대비 효율 측면에서 가장 효과적으로 위험을 통제하고자 하는 것이다. 따라서 다양한 위험에 대하여 동일한 기준을 가지고 평가하는 것이 필요하다.

① 위험평가, 위험관리
② 위험평가, 위험조치
③ 위험기준, 위험관리
④ 위험기준, 위험분석
⑤ 위험분석, 위험평가

23. 정보보호 정책의 내용으로 최소한의 표준으로 포함되어야 할 내용으로 거리가 먼 것은?

① 모든 직원에 대한 정보화 교육
② 필요한 보호의 수준에 따른 자산의 분류
③ 준수해야 할 표준, 관례 및 절차와 바이러스 방지, 패스워드, 암호화를 포함하는 정보보호 정책 지원 수단의 구현
④ 정보시스템 보안사고에 대한 보고 및 조사
⑤ 물리적, 논리적, 환경적 보안 및 통신보안

24. 보안사고 대응팀/정보보호 위원회의 역할을 기술한 것으로 거리가 먼 것은?

① 조직 IT보안 정책의 유효성 검토
② IT보안 문제 인식 촉진
③ 조직 IT 보안 프로그램 실행을 모니터링
④ 전략적 보안계획과 관련하여 IT운영위원회에 조언
⑤ 조직 IT보안 정책과 지침의 유지

25. 다음 지문을 읽고 해당하는 서비스를 항목에서 선택하시오.

> 다음 서비스의 목적은 데이터 및 시스템을 보호하기 위함이며, 더 나아가 인가되지 않은 사람으로부터의 공격을 방어하여 전체 네트워크를 보호하고자 함이다. 사용자의 출입을 통제하기 위한 목적과 네트워크 내부의 인가된 사용자 인지의 여부를 확인하는 서비스이다. 이 서비스는 개인정보를 가공하거나, 개인만의 고유정보를 통해 인가여부를 확인하는 서비스로, 별도의 시스템에서 운용을 하며, 모든 네트워크 내의 인가된 사용자에게만 서비스를 수행한다.

① 기밀성 서비스
② 무결성 서비스
③ 인증 서비스
④ 접근제어 서비스
⑤ 부인방지 서비스

26. 정보통신부장관은 대통령령이 정하는 바에 따라 정보통신진흥기금의 운용·관리에 관한 사무의 일부를 정보통신 연구개발업무와 관련된 기관 또는 단체에 위탁할 수 있는 바, 현행 정보화촉진기본법상 이를 위탁받은 기관은?

① 한국정보보호진흥원
② 한국정보사회진흥원
③ 정보통신연구진흥원
④ 정보통신정책연구원
⑤ 한국전자통신연구소

27. 정보 자산에 대한 공격 중에 인터넷 환경에서 능동적(Active) 공격에 해당하지 않는 것은?

① 메시지의 변조
② 메시지 재전송
③ 메시지의 파괴
④ 트래픽 분석
⑤ IP 주소 도용

28. 정보시스템에 손해를 끼치는 원인이 될 수 있는 조직, 절차, 인력관리, 행정, 하드웨어와 소프트웨어의 약점을 확인하고 분류하여 위협을 감소시키는 것을 무엇이라 하는가?

① 위험 관리
② 정책 수립
③ 정책 관리
④ 취약성 분석
⑤ 감사

29. 정보 시스템을 위한 보안 운영체제의 설계원리에 적합하지 아니한 것은?

① 심층 보호의 설정
② 개방형 설계
③ 허용에 근거한 접근
④ 수평적 보안성
⑤ 보호 메커니즘 경제성

30. 정보보호의 필요성으로 보기에 부적절한 내용은?

① 전자상거래, 전자정부 등 사이버 공간에서의 활동 증가에 따른 안전성과 신뢰의 보장 및 그 해결
② 글로벌화에 따른 국내 정보 유출 우려의 불식
③ 공공기관에서 소유하고 있는 개인의 정보의 보호
④ 회사간의 각종 사업계획에 관한 정보교환 및 사업행위의 원칙적 금지를 위함.
⑤ 각종 지적소유권의 보호

31. 침해사고의 대응절차 중 가장 마지막 단계에서 이루어지는 것은?

① 사고처리 지침 및 절차, 필수적인 문서, 업무연속성 계획 등 준비
② 사고조사 및 심각성 조사를 위한 절차 및 책임
③ 사고처리, 피해제한, 사고근절, 상부보고에 대한 절차 및 책임
④ 정상 서비스 등 재구축을 위한 절차 및 책임
⑤ 법적 연투 관계에 대한 조사 및 분석을 포함한 후기사고 조치에 대한 조치 및 책임

32. 정보보호대책은 안전대책, 혹은 통제, 혹은 대응책이라고 하는 바, 이 정보보호대책은 위험을 감소시키기 위한 정보보호조치를 의미하며, 여기에는 장치, 절차, 기법, 행위 등을 포함한다. 이 경우에 탐지 통제를 통해 발견된 문제들을 해결하기 위해서 별도의 조치가 필요한 경우에 행하여지는 것은?

① 예방 통제
② 탐지통제
③ 교정 통제
④ 잔류 위험
⑤ 대책 식별

33. 전자서명법 제18조(인증서 폐지) 제1항에서는 공인인증기관은 공인인증서에 관하여 해당하는 사유가 발생한 경우에는 당해 공인인증서를 폐지하여야 하며 2항에서는 그 사실을 항상 확인할 수 있도록 지체없이 필요한 조치를 취하여야 정하고 있는 바, 법에서 정하는 해당 사유가 아닌 것은?

① 가입자 또는 그 대리인이 공인인증서의 폐지를 신청한 경우
② 가입자가 사위 또는 기타 부정한 방법으로 공인인증서를 발급받은 사실을 인지한 경우
③ 가입자가 공인인증서를 이용범위 또는 용도에서 벗어나 부정하게 사용한 경우
④ 가입자의 사망, 실종선고 또는 해산 사실을 인지한 경우
⑤ 가입자의 전자서명생성정보가 분실, 훼손 또는 도난, 유출된 사실을 인지한 경우

34. 정보통신부장관이 정보통신망이용촉진 및 정보보호 등을 위하여 강구하는 시책에 속하지 않는 것은?

① 정보통신망에 관련된 기술의 개발·보급
② 정보통신망 기술인력양성사업의 지원
③ 정보통신망의 표준화
④ 정보통신망을 이용한 정보의 공동활용 촉진
⑤ 정보통신망에서의 청소년보호

35. 전자서명법상 전자서명생성정보의 관리에 관한 규정의 내용 중 틀린 것은?

① 가입자는 자신의 전자서명생성정보가 분실·훼손 또는 도난·유출되거나 훼손될 수 있는 위험을 인지한 때에는 그 사실을 공인인증기관에 통보하여야 한다.
② ①의 경우 가입자가 공인인증서를 이용하는 자에게 공인인증기관에 통보한 내용을 고지할 필요는 없다.
③ 공인인증기관은 가입자의 신청이 있는 경우 외에는 가입자의 전자서명생성정보를 보관하여서는 아니된다.
④ 공인인증기관은 가입자의 신청에 의하여 그의 전자서명생성정보를 보관하는 경우 당해 가입자의 동의없이 이를 이용하거나 유출하여서는 아니된다.
⑤ 공인인증기관은 자신이 이용하는 전자서명생성정보가 분실·훼손 또는 도난·유출되거나 훼손될 수 있는 위험을 인지한 때에는 지체없이 그 사실을 보호진흥원에 통보하여야 한다.

36. 정보통신망이용촉진및정보보호등에관한법률 제3조 제3항에 의하면 정부는 정보통신서비스제공자 단체 또는 이용자 단체의 (A) 및 정보통신망에서의 (B) 등을 위한 활동을 지원할 수 있다. A와 B에 적합한 단어는?

① A : 권익보호, B : 개인정보보호
② A : 정보보호, B : 시스템 보호
③ A : 정보자료 안정성의 보호, B : 정보통신기반보호
④ A : 정보산업보호, B : 정보통신시설의 보호
⑤ A : 개인정보보호, B : 청소년보호

37. 정보통신망 이용촉진 및 정보보호 등에 관한법률 제22조에 의거하여 정보통신서비스 제공자는 이용자의 개인정보를 수집하는 경우 당해 이용자의 동의를 얻어야 하나, 이 규정의 예외로서 인정되는 경우는?

① 정보통신서비스 제공을 원활하게 하기 위하여 필요한 경우
② 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우
③ 정보통신서비스의 이용자가 미성년인 경우
④ 이용자의 과실로 인하여 정보통신서비스의 제공에 문제가 발생한 경우
⑤ 정보통신서비스의 제공에 관한 계약의 이행을 위하여 필요하다고 인정되는 경우

38. 정보통신기반보호법상 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 정보통신망이용촉진및정보보호등에관한법률 제2조 제1항 제1호의 규정에 의한 정보통신망을 무엇이라 하는가?

① 정보통신망
② 주요정보통신망
③ 정보통신기반시설
④ 주요정보통신기반서비스
⑤ 정보통신제어·관리시스템

39. 정보통신기반보호법 제10조 보호지침에 의하면 관계중앙행정기관의 장은 소관분야의 주요정보통신기반시설에 대하여 보호지침을 제정하고 해당분야의 (　　)에게 이를 지키도록 (　　)할 수 있다. (　　) 속에 들어갈 말을 순서대로 열거한 것은?

① 관리기관의 장, 권고
② 관리기관의 장, 명령
③ 관리기관의 장, 요청
④ 사업자, 권고
⑤ 사업자, 명령

40. 정보통신망이용촉진및정보보호등에관한법률에서 사용하는 용어를 동법 제2조에서 정의하지 아니하고 정보화촉진기본법상의 용어의 정의가 준용되는 것은?

① 정보통신망
② 전자문서
③ 개인정보
④ 정보보호
⑤ 침해사고