2017-지방교행-정보보호론-A형-해설-곽후근

1. 정보보호의 목표와 그에 대한 설명 (가)~(다)를 바르게 짝지은 것은?

(가) 내부 정보 및 전송되는 정보에 대하여 허가되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 한다. (나) 정보에 대한 접근 권한이 있는 사용자가 방해받지 않고 언제든지 정보와 정보시스템을 사용할 수 있도록 보장한다. (다) 접근 권한이 없는 사용자에 의해 정보가 변경되지 않도록 보호하여 정보의 정확성과 완전성을 확보한다.

	(가)	(나)	(다)
①	기밀성	가용성	무결성
②	기밀성	무결성	가용성
③	무결성	가용성	기밀성
④	무결성	기밀성	가용성

정답 체크 :

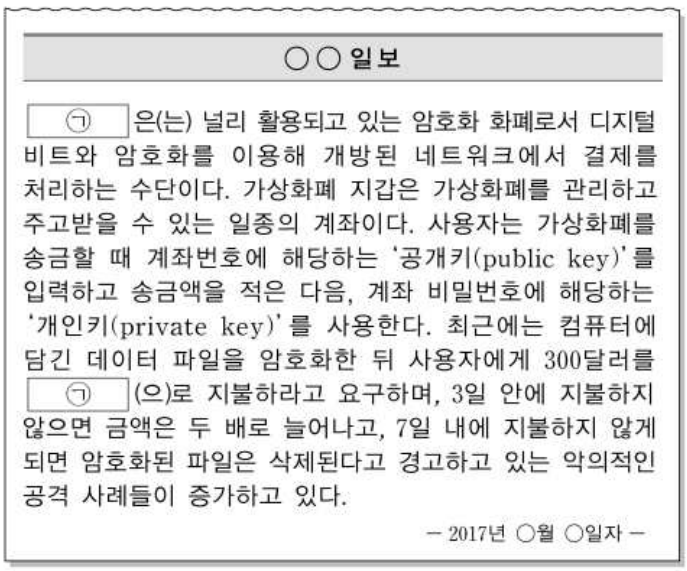
(1)

(가) 기밀성 : 인가된 사람, 인가된 프로세스, 인가된 시스템만이 알 필요성에 근거하여 시스템에 접근해야 함을 의미한다.

(나) 가용성 : 인가된 사용자가 자원이 필요할 때 지체 없이 원하는 객체 또는 자원에 접근하여 사용할 수 있어야 하는 성질을 의미한다.

(다) 무결성 : 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호되어야 하는 성질의 의미한다.

2. 다음은 신문 기사의 일부이다. 빈칸 ㉠에 공통으로 들어갈 용어로 옳은 것은?



○○ 일보

㉠ 은(는) 널리 활용되고 있는 암호화 화폐로서 디지털 비트와 암호화를 이용해 개방된 네트워크에서 결제를 처리하는 수단이다. 가상화폐 지갑은 가상화폐를 관리하고 주고받을 수 있는 일종의 계좌이다. 사용자는 가상화폐를 송금할 때 계좌번호에 해당하는 '공개키(public key)'를 입력하고 송금액을 적은 다음, 계좌 비밀번호에 해당하는 '개인키(private key)'를 사용한다. 최근에는 컴퓨터에 담긴 데이터 파일을 암호화한 뒤 사용자에게 300달러를 ㉠ (으)로 지불하라고 요구하며, 3일 안에 지불하지 않으면 금액은 두 배로 늘어나고, 7일 내에 지불하지 않게 되면 암호화된 파일은 삭제된다고 경고하고 있는 악의적인 공격 사례들이 증가하고 있다.

— 2017년 ○월 ○일자 —

① 비트코인(bitcoin)

② 허니 팟(honey pot)

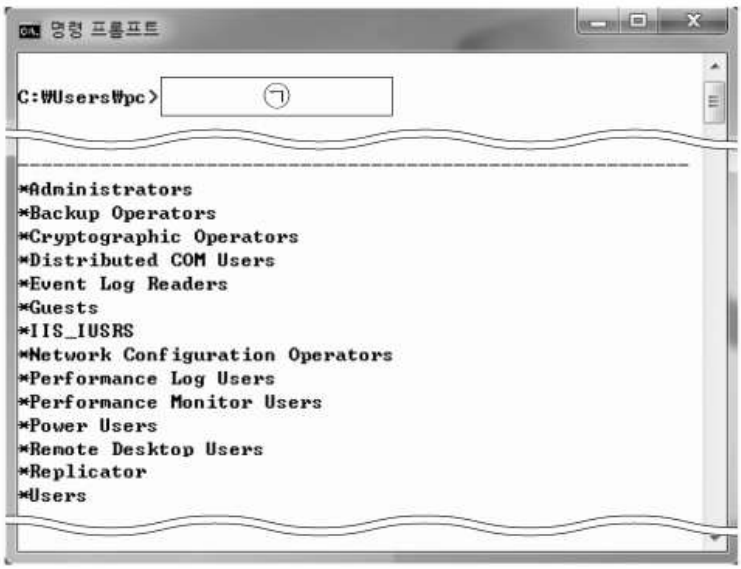
③ 랜섬웨어(ransomware)
④ 비트 채움(bit padding)
정답 체크 :
(1) 비트코인 : 가상통화 또는 암호통화라고 불리는 종류의 하나이다. 물리적으로 떨어져 있더라도 인터넷을 통해 금전의 송수신이 가능하다. 수수료가 저렴하므로 소액 결제도 편리하다. 나까모또 사토시(Nakamoto satoshi)라고 하는 정체불명의 인물이 투고한 논문으로부터 시작하였다. 2009년부터 세계 각국에서 사용하고 있다. 2015년에는 미국에서 최초의 비트코인 취급소 코인베이스(Coinbase)가 오픈되었다.
오답 체크 :
(2) 허니팟 : 크래커를 유인하는 함정을 꿀단지에 비유한 것에서 명칭이 유래한다. 마치 실제로 공격을 당하는 것처럼 보이게 하여 크래커를 추적하고 정보를 수집하는 역할을 한다. 침입자를 오래 머물게 하여 추적이 가능하므로 능동적으로 방어할 수 있고, 침입자의 공격을 차단할 수 있다. 직접적인 공격을 수행하지는 않는다.
(3) 랜섬웨어 : 컴퓨터 시스템을 감염시켜 접근을 제한하고 일종의 몸값을 요구하는 악성 소프트웨어의 한 종류이다. 컴퓨터로의 접근이 제한되기 때문에 제한을 없애려면 해당 악성 프로그램을 개발한 자에게 지불을 강요받게 된다.
(4) 비트채움 : 32비트 블록이 기본 단위이고, 메시지가 23비트일 때 블록 길이를 맞추기 위해 9비트를 0으로 비트채움한다.

3. 유닉스 시스템에 대한 설명으로 옳지 않은 것은?
① who 명령어는 utmp 로그의 내용을 사용한다.
② wtmp 로그의 내용은 ps 명령어로 확인할 수 있다.
③ 파일의 접근 권한은 ls - l 명령어로 확인할 수 있다.
④ syslog에서 서비스의 동작과 에러를 확인할 수 있다.
정답 체크 :
(2) ps는 프로세스의 상태를 확인하는 명령어로 wtmp 로그와 무관하다. wtmp 로그를 보기 위해서는 last와 같은 명령어를 사용해야 한다.
오답 체크 :
(1) utmp 로그를 보기 위해서는 w, who, users, whodo, finger 등의 명령어를 사용한다.
(3) ls -l 또는 ls -al 명령어를 사용하면 파일의 접근 권한(user/group/others)을 확인할 수 있다.
(4) syslog는 시스템의 로그에 대한 정보 대부분을 수집하여 로그를 남긴다. 해당 로그의 종류와 로깅 수준(레벨)은 설정 파일(syslog.conf)에서 확인할 수 있다.

4. 암호 시스템의 키 관리에 대한 설명으로 옳은 것은?
① X.509 인증서는 개인키를 포함한다.
② PKI(Public Key Infrastructure) 환경에서 사용자는 공개키를 생성하여 배포한다.
③ 대칭키를 사용하는 환경에서 키 배포 센터와 구성원 간의 통신은 세션키를 사용한다.
④ PKI 환경에서 공개키 암호를 이용할 경우 CA(Certification Authority)는 인증서를 발급 한다.
정답 체크 :
(4) CA는 자신의 서명을 붙여 인증서를 발급한다.

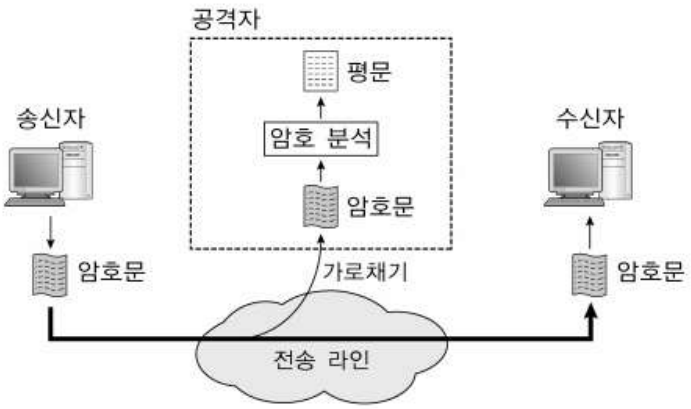
오답 체크 :
(1) X.509 인증서는 공개키를 포함한다. 개인키는 개인이 가지는 것으로 절대 인증서에 포함하면 안된다.
(2) 사용자가 공개키를 생성하지만 배포는 하지 않는다. 배포는 CA(인증기관)가 저장소를 통해 수행한다.
(3) 구성원과 구성원 간의 통신에 세션키를 사용하고, 키 배포 센터와 구성원 간의 통신에는 미리 공유하고 있던 비밀키를 사용한다.

5. 시스템 관리자는 새로운 사용자를 추가하고 권한을 부여하기 위해 현재 시스템의 그룹을 확인하고자 한다. MS 윈도 명령 프롬프트에서 시스템의 그룹을 확인하기 위한 그림의 빈칸 ㉠에 들어갈 명령어로 옳은 것은?



① net localgroup
② ping localgroup
③ netstat localgroup
④ tracert localgroup
정답 체크 :
(1) net localgroup : 컴퓨터에서 로컬 사용자 그룹을 관리하는데 사용한다.
오답 체크 :
(2) ping : IP 네트워크를 통해 특정한 호스트가 도달할 수 있는지의 여부를 테스트하는 데 쓰이는 컴퓨터 네트워크 도구의 하나이다.
(3) netstat : 컴퓨터 내에서 사용 중인 포트를 확인할 때 사용한다.
(4) tracert : 최종 목적지 컴퓨터(서버)까지 중간에 거치는 여러 개의 라우터에 대한 경로 및 응답 속도를 표시해 준다. 리눅스에서는 traceroute를 사용한다.

6. 그림에서 공격자의 암호 해독 방법으로 옳은 것은?



① 선택 평문 공격
② 선택 암호문 공격
③ 암호문 단독 공격
④ 알려진(기지) 평문 공격
정답 체크 :
(3) 암호문 단독 공격 : 해독자는 단지 암호문 C만을 갖고 이로부터 평문(P)이나 키(K)를 찾아내는 방법이다.
오답 체크 :
(1) 선택 평문 공격 : 해독자가 사용된 암호화기에 접근할 수 있어 평문(P)를 선택하여 평문에 대응하는 암호문(C)를 얻어 키(K)나 평문(P)를 해독하는 방법이다.
(2) 선택 암호문 공격 : 해독자가 암호 복호화기에 접근할 수 있어 암호문(C)에 대응하는 평문(P)를 얻어내어 해독하는 방법이다.
(4) 기지 평문 공격 : 암호 해독자는 일정량의 평문(P)에 대응하는 암호문(C) 쌍을 이미 알고 있는 상태에서 암호문(C)와 평문(P)의 관계로부터 키(K)나 평문(P)를 추정한다.

7. 네트워크 기반의 공격과 그에 대한 설명 (가)~(다)를 바르게 짝지은 것은?

〈보기〉
(가) 대량의 패킷을 이용하여 특정 서비스의 수행을 방해하는 공격
(나) 네트워크상에서 자신이 아닌 다른 상대방들의 패킷 교환을 도청하는 공격
(다) 공격자가 자신의 IP(Internet Protocol) 주소를 변조한 후 다른 사용자나 시스템처럼 위장하여 공격

(단, DoS는 Denial of Service의 약어이다.)

	(가)	(나)	(다)
①	DoS	sniffing	spoofing
②	DoS	spoofing	sniffing
③	sniffing	DoS	spoofing
④	spoofing	sniffing	DoS

정답 체크 :
(1)
(가) DoS : DoS(서버를 서비스 거부 상태로 만듦)의 공격 유형에는 취약점 공격형과 자원 고갈형

이 존재한다. 취약점 공격형은 teardrop, land attack이 해당되고, 자원 고갈형은 flooding(대량의 패킷을 이용함) 공격이 해당된다.
(나) sniffing : 패킷을 태핑(Tapping)이나 미러링(Mirroring)을 통해 도청하는 것을 의미한다. 도청만 수행하므로 소극적 공격에 해당한다.
(다) spoofing : 승인받은 사용자인 것처럼 시스템에 접근하거나 네트워크상에서 허가된 주소로 가장하여 접근 제어를 우회하는 공격 행위이다. 일례로, IP Spoofing 공격은 서버와 트러스트(Trust)로 관계를 맺고 있는 클라이언트에 DoS 공격을 수행해 클라이언트가 사용하는 IP가 네트워크에 출현하지 못하도록 한 뒤, 공격자 자신이 해당 IP로 설정을 변경한 후 서버에 접속하는 형태로 이루어진다. IP Spoofing 이외에도 ARP, Port, Content(Payload), DNS Spoofing 등이 존재한다.

8. 다음은 디지털 콘텐츠 저작권 보호에 활용되는 기술에 대한 설명이다. 빈칸 ㉠에 공통으로 들어갈 용어로 옳은 것은?

> 디지털 [㉠]은 디지털 콘텐츠를 구매할 때 구매자의 정보를 삽입하여 불법 배포 발견 시 최초의 배포자를 추적할 수 있게 하는 기술이다. 이 기술을 사용하면 판매되는 콘텐츠마다 구매자의 정보가 들어 있으므로, 불법적으로 재배포된 콘텐츠 내에서 [㉠]된 정보를 추출하여 구매자를 식별할 수 있다.

① 스미싱(smishing)
② 노마디즘(nomadism)
③ 패러다임(paradigm)
④ 핑거프린팅(fingerprinting)
정답 체크 :
(4) 핑거프린팅 : 디지털 콘텐츠를 구매할 때 구매자의 정보를 삽입하여 불법 배포 발견 시 최초의 배포자를 추적할 수 있게 하는 기술이다. 판매되는 콘텐츠마다 구매자의 정보가 들어 있으므로 불법적으로 재배포된 콘텐츠 내에서 핑거프린팅된 정보를 추출하여 구매자를 식별하고, 법적인 조치를 가할 수 있게 된다.
오답 체크 :
(1) 스미싱 : SMS(문자 메시지)와 Phishing의 약자이다. Phishing은 Private Data(개인 정보)와 Fishing(낚시)의 약자이다. 공격자가 문자 메시지에 URL을 보내고, 사용자가 이를 클릭하면 해킹 툴이 스마트폰에 설치되어 개인 정보가 탈취된다.
(2) 노마디즘 : 특정한 방식이나 삶의 가치관에 얽매이지 않고 끊임없이 새로운 자아를 찾아가는 것을 뜻하는 말로, 살 곳을 찾아 끊임없이 이동하는 유목민(노마드, Nomad)에서 나온 말이다.
(3) 패러다임 : 어떤 한 시대 사람들의 견해나 사고를 근본적으로 규정하고 있는 테두리로서의 인식의 체계, 또는 사물에 대한 이론적인 틀이나 체계를 의미하는 개념이다.

9. 다음은 SQL 삽입(injection) 공격을 위한 SQL 명령문이다. 빈칸 ㉠에 들어갈 명령어로 옳은 것은?

```
㉠ user_id FROM member WHERE
(user_id=' ' OR '1'='1') AND
(user_pw=' ' OR '1'='1');
```

∘ member: 테이블명
∘ user_id: 필드명
∘ user_pw: 필드명

① DROP
② CREATE
③ INSERT
④ SELECT

정답 체크 :
(4)
원래 코드는 사용자로부터 아이디와 비밀번호를 입력받아서 member 테이블에서 user_id와 user_pw가 일치하는 행을 선택(select)하는 것이다. SQL injection 공격을 수행하면 where 조건에 or를 추가하여 왼쪽 조건은 false(user_id=' ')로 만들고, 오른쪽 조건은 무조건 true('1'='1')가 되게 하여 일치하는 행이 있는 것처럼 만드는 것이다.

10. 메시지 인증 코드(MAC: Message Authentication Code)를 이용하여 제공할 수 있는 보안 서비스로 옳은 것을 〈보기〉에서 고른 것은?

ㄱ. 트래픽 패딩
ㄴ. 메시지 무결성
ㄷ. 메시지 복호화
ㄹ. 메시지 송신자에 대한 인증

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄹ
④ ㄷ, ㄹ

정답 체크 :
(3)
(ㄴ), (ㄹ) : MAC은 인증과 무결성을 제공한다.
오답 체크 :
(1), (2), (4)
(ㄱ) : 트래픽 패딩은 단순히 비트를 채우는 것으로 보안 서비스가 아니다.
(ㄷ) : 메시지 복호화는 기밀성인데 MAC은 기밀성을 제공하지 않는다. 기밀성은 대칭 암호 또는 공개키 암호가 제공한다.

11. 공개키를 이용하는 전자서명에 대한 설명으로 옳지 않은 것은?
① 전자서명은 위조 불가능해야 한다.

② 전자서명은 부인봉쇄(nonrepudiation)에 사용된다.
③ DSS(Digital Signature Standard)는 전자서명 알고리즘이다.
④ 한 문서에 사용한 전자서명은 다른 문서의 전자 서명으로 재사용할 수 있다.
정답 체크 :
(4) 전자서명은 재사용 불가이다. 서명문의 해시값을 전자서명에 이용하므로 한 번 생성된 서명을 다른 문서의 서명으로 사용할 수 없다.
오답 체크 :
(1) 전자서명은 위조 불가이다. 즉, 서명자만이 서명문을 생성할 수 있다.
(2) 전자서명은 인증, 무결성, 부인방지에 사용된다.
(3) DSS는 디지털 서명에 사용되는 알고리즘 모음(suite)이다. 알고리즘에는 DSA, RSA, ECC가 존재한다.

12. 침입 탐지 시스템의 탐지 단계를 순서대로 바르게 나열한 것은?

ㄱ. 데이터 수집(data collection)
ㄴ. 침입 탐지(intrusion detection)
ㄷ. 보고 및 대응(reporting and response)
ㄹ. 데이터 필터링 및 축약(data filtering and reduction)

① ㄱ-ㄴ-ㄷ-ㄹ
② ㄱ-ㄹ-ㄴ-ㄷ
③ ㄹ-ㄴ-ㄱ-ㄷ
④ ㄹ-ㄷ-ㄱ-ㄴ
정답 체크 :
(2)
(ㄱ) 데이터 수집 : HIDS(윈도우나 유닉스 등의 운영체제에 부가적으로 설치, 운용되거나 일반 클라이언트에 설치)는 호스트에서 데이터를 수집하고, NIDS(네트워크에서 하나의 독립된 시스템으로 운용)는 네트워크에서 데이터를 수집한다.
(ㄹ) 데이터 필터링 및 축약 : HIDS와 NIDS로 수집한 침입 관련 데이터를 상호 연관시켜 좀 더 효과적으로 분석하면 공격에 빠르게 대응 가능하다.
(ㄴ) 침입 탐지 : 오용 탐지 기법(이미 발견되고 정립된 공격 패턴을 미리 입력해두었다가 해당하는 패턴이 탐지되면 알려주는 것)과 이상 탐지 기법(정상적이고 평균적인 상태를 기준으로 급격한 변화를 일으키거나 확률이 낮은 일이 발생하면 알려주는 것)을 수행한다.
(ㄷ) 보고 및 대응 : 침입을 알려주거나 공격을 역추적하여 침입자의 시스템이나 네트워크를 사용하지 못하게 한다(IPS).

13. 응용 계층에서 사용되는 보안 프로토콜로 옳은 것을 〈보기〉에서 고른 것은?

〈보기〉
ㄱ. FTP
ㄴ. PGP
ㄷ. S/MIME
ㄹ. UDP

① ㄱ, ㄷ

② ㄱ, ㄹ
③ ㄴ, ㄷ
④ ㄴ, ㄹ
정답 체크 :
(3)
(ㄴ) PGP : 응용 계층에서 동작하는 이메일 보안 프로토콜이다.
(ㄷ) S/MIME : 응용 계층에서 동작하는 이메일 보안 프로토콜이다.
오답 체크 :
(1), (2), (4)
(ㄱ) FTP : 응용 계층에서 동작하나 보안 프로토콜이 아닌 파일 전송 프로토콜이다.
(ㄹ) UDP : 전송 계층에서 동작하고 보안 프로토콜이 아닌 신뢰성을 보장하지 않는 패킷 전송 프로토콜이다.

14. 일방향 해시 함수(one-way hash function)에 대한 설명으로 옳은 것은?
① 데이터 암호화에 사용된다.
② 주어진 해시값으로 원래의 입력 메시지를 구할 수 있다.
③ 임의 길이의 메시지를 입력받아 고정 길이의 해시 값을 출력한다.
④ IDEA(International Data Encryption Algorithm)는 일방향 해시 함수이다.
정답 체크 :
(3) 입력이 1bit 혹은 1Tbit라도 고정된 길이의 출력을 가진다.
오답 체크 :
(1) 해시는 무결성을 보장하나 기밀성(암호화)는 보장하지 않는다.
(2) 해시는 일방향이라 주어진 해시값으로 원래의 입력 메시지를 구할 수 없다.
(4) IDEA는 대칭키 암호 알고리즘이다.

15. 다음은 RSA 공개키 알고리즘에서 공개키와 개인키를 구하는 과정이다. 단계 4의 $^{\pm}$ 값으로 적절한 것은?

[알고리즘]
ㅇ 단계 1: 두 소수 p=5, q=11을 선정한다.
ㅇ 단계 2: n=p×q를 계산한다.
ㅇ 단계 3: $\phi(n)=(p-1)\times(q-1)$을 계산한다.(단, $\phi(n)$은 오일러의 Totient 함수이다.)
ㅇ 단계 4: $\phi(n)$과 서로소의 관계를 갖는 임의의 e 값을 선택한다.
ㅇ 단계 5: $e\times d \bmod \phi(n) = 1$의 관계를 갖는 d를 계산한다.(단, mod는 나머지를 구하는 연산자이다.)
ㅇ 단계 6: (e, n)을 공개키로 하고, (d, n)을 개인키로 한다.

① 12
② 13
③ 15
④ 18
정답 체크 :
주어진 조건으로 오일러의 Totient 함수를 구하면 다음과 같다.

40 = (5-1) x (11-1)
주어진 보기에서 40과 서로소의 관계를 갖는 수를 찾으면 된다.
(2) 13 : 공약수가 1이므로 서로소가 된다.
오답 체크 :
(1) 12 : 공약수가 1, 2, 4이므로 서로서가 아니다.
(3) 15 : 공약수가 1, 5이므로 서로서가 아니다.
(4) 18 : 공약수가 1, 2이므로 서로서가 아니다.

16. 다음의 내용을 목적으로 규정하고 있는 법은?

제1조(목적) 이 법은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 한다.

① 개인정보 보호법
② 국가인권위원회법
③ 공공기관의 정보공개에 관한 법률
④ 정보보호 산업의 진흥에 관한 법률
정답 체크 :
(1) 개인정보 보호법 : 이 법은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 한다.
오답 체크 :
(2) 국가인권위원회법 : 이 법은 국가인권위원회를 설립하여 모든 개인이 가지는 불가침의 기본적 인권을 보호하고 그 수준을 향상시킴으로써 인간으로서의 존엄과 가치를 실현하고 민주적 기본질서의 확립에 이바지함을 목적으로 한다.
(3) 공공기관의 정보공개에 관한 법률 : 이 법은 공공기관이 보유·관리하는 정보에 대한 국민의 공개 청구 및 공공기관의 공개 의무에 관하여 필요한 사항을 정함으로써 국민의 알권리를 보장하고 국정(國政)에 대한 국민의 참여와 국정 운영의 투명성을 확보함을 목적으로 한다.
(4) 정보보호 산업의 진흥에 관한 법률 : 이 법은 정보보호산업의 진흥에 필요한 사항을 정함으로써 정보보호산업의 기반을 조성하고 그 경쟁력을 강화하여 안전한 정보통신 이용환경 조성과 국민경제의 건전한 발전에 이바지함을 목적으로 한다.

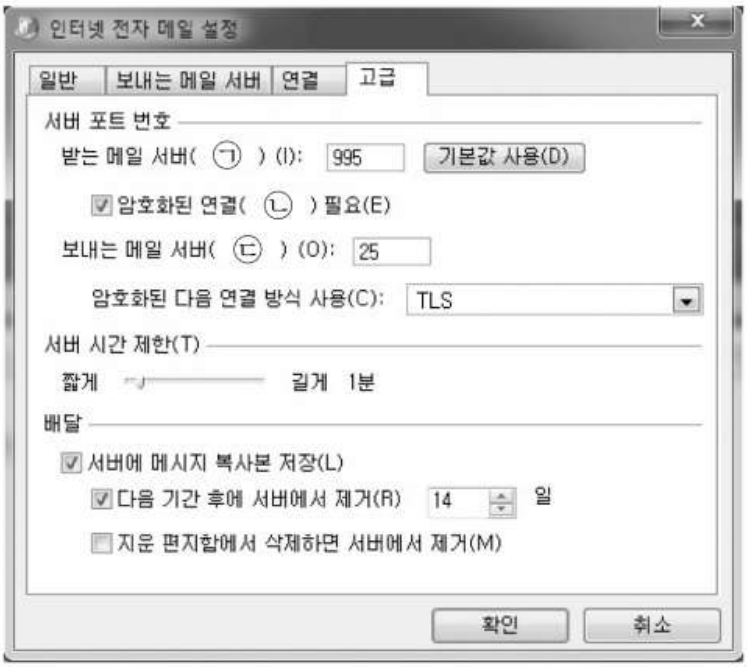
17. 다음은 방화벽 규칙 집합(rule set)이다. 이에 대한 설명으로 옳은 것은?

정책	출발지(source)		목적지(destination)		동작
	IP 주소	포트	IP 주소	포트	
1	external	any	192.168.100.100	5553	allow
2	any	any	any	any	deny

① 정책 2는 모든 접근에 대하여 허용하는 정책이다.
② 방화벽은 정책 2를 적용한 후 정책 1을 적용하게 된다.
③ 방화벽은 접근제어를 수행하기 위하여 포트만을 사용한다.
④ 외부 IP 주소를 사용하여 접근하는 경우 내부 시스템(192.168.100.100)의 5553번 포트에 접근을 허용한다.

정답 체크 :
(4) 정책 1에 해당한다.
오답 체크 :
(1) 정책 2는 모든 접근을 차단(deny)하는 정책이다.
(2) 정책 1을 적용한 후 정책 2를 적용하게 된다. 순서가 바뀌면 모든 패킷이 차단된다.
(3) 접근제어를 수행하기 위하여 IP 주소와 포트를 사용한다.

18. 그림은 인터넷 전자 메일 설정 화면이다. ㉠~㉢에 들어갈 프로토콜을 바르게 짝지은 것은?



	㉠	㉡	㉢
①	SSL	POP3	SMTP
②	POP3	SSL	SMTP
③	POP3	SMTP	SSL
④	SMTP	SSL	POP3

정답 체크 :
(2)
(ㄱ) POP3 : 메일을 받을 때는 POP3 또는 IMAP을 사용한다. POP3는 메일 서버에 메일 복사본을 남기지 않고, IMAP은 메일 서버에 메일 복사본을 남긴다(나중을 위한 백업용).
(ㄴ) SSL : 메일을 암호화하기 위해 SSL/TLS(4계층에서 암호화)를 사용한다.
(ㄷ) SMTP : 메일을 보낼 때는 SMTP를 사용한다. 메일 서버끼리 메일을 주고 받을 때도 SMTP를 사용한다.

19. 다음 설명을 모두 만족하는 암호화 알고리즘은?

o 공개키 암호 알고리즘이다. o 이산대수 문제의 어려움에 기반을 둔다.

ㅇ Diffie-Hellman 키 교환 프로토콜의 확장이다.

① SEED 암호
② Rabin 암호
③ ElGamal 암호
④ Blowfish 암호

정답 체크 :

(3) ElGamal : 이산 대수를 구하는 것이 어렵다는 것을 이용한다. 이산 대수란 g, x, p가 주어졌을 때 $y=g^x \bmod p$를 구하는 것은 쉽지만, g, y, p가 주어졌을 때 x를 구하는 것은 어렵다는 사실에 기반을 둔다. 암호문의 길이가 평문의 2배가 되어 버린다는 결점을 가진다.

오답 체크 :

(1) SEED : SEED는 전자상거래, 금융, 무선통신 등에서 전송되는 개인정보와 같은 중요한 정보를 보호하기 위해 1999년 2월 한국인터넷진흥원과 국내 암호전문가들이 순수 국내기술로 개발한 128 비트 블록 암호 알고리즘이다. 2009년 256 비트 키를 지원하는 SEED 256을 개발하였다.

(2) Rabin : 인수 분해를 하는 것이 어렵다(mod B으로 평방근(제곱근)을 구하는 것이 어렵다)는 것을 이용한다. 즉, p, q를 이용해서 N = p x q를 구하는 것은 쉽지만 N을 이용해서 p, q를 구하는 것은 어렵다는 사실에 기반을 둔다.

(4) Blowfish : 1993년 블루스 슈나이어가 설계한 키 방식의 대칭형 블록 암호이다. 기존 암호는 클로즈드 소스(특허 있음)였으나, 슈나이어는 블로피시를 오픈 소스(특허 없음)로 만들었다.

20. 다음은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의3 내용 중 일부이다. 빈칸 ㉠에 공통으로 들어갈 내용으로 옳은 것은?

> 제45조의3(㉠ 의 지정 등) ① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 임원급의 ㉠ 을(를) 지정할 수 있다. 다만, 종업원 수, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 ㉠ 을(를) 지정하고 미래창조과학부장관에게 신고하여야 한다.

① 개인정보 처리자
② 정보보호 담당관
③ 정보보호 정책관
④ 정보보호 최고책임자

정답 체크 :

(4)

"정보통신망" 제45조의3(정보보호 최고책임자의 지정 등) ① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 임원급의 정보보호 최고책임자를 지정하고 과학기술정보통신부장관에게 신고하여야 한다. 다만, 자산총액, 매출액 등이 대통령령으로 정하는 기준에

해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 지정하지 아니할 수 있다.

오답 체크 :

(1) 개인정보 처리자 : 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

(2) 정보보호 담당관 : 전산분야의 보안계획 및 운용 등의 기능을 수행하는 자로 전산업무담당 실장 본부장을 말한다.

(3) 정보보호 정책관 : 민간분야 정보보호 정책을 총괄하는 수장을 말한다.

Tip! : “미래창조과학부장관”에서 “과학기술정보통신부장관”으로 바뀐 것에 주의한다(조직이 해산되면 장관과 조직의 이름이 바뀐다).