2016년 지방직 9급 정보보호론 풀이

by 호이호이꿀떡

정답 체크

01	02	03	04	05	06	07	08	09	10
①	③	③	④	④	①	③	④	②	③
11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
④	②	②	③	④	④	②	④	②	①

문 1. 보안 공격 유형 중 소극적 공격으로 옳은 것은?

① 트래픽 분석(traffic analysis)
② 재전송(replaying)
③ 변조(modification)
④ 신분 위장(masquerading)

답 ①

소극적 공격(수동적 공격)
- 도청(가로채기, interception)
- 트래픽 분석(traffic analysis)
- 메시지 내용 공개(release of message contents) 등

적극적 공격(능동적 공격)
- 차단(interruption)
- 변조(modification)
- 위조(fabrication)
- 신분 위장(masquerade)
- 서비스 거부 공격(Dos)
- 재전송 공격(replay attack) 등

문 2. 암호학적 해시 함수가 가져야 할 특성으로 옳지 않은 것은?

① 서로 다른 두 입력 메시지에 대해 같은 해시값이 나올 가능성은 있으나, 계산적으로 같은 해시값을 갖는 서로 다른 두 입력 메시지를 찾는 것은 불가능해야 한다.
② 해시값을 이용하여 원래의 입력 메시지를 찾는 것은 계산상으로 불가능해야 한다.
③ 입력 메시지의 길이에 따라 출력되는 해시값의 길이는 비례해야 한다.
④ 입력 메시지와 그 해시값이 주어졌을 때, 이와 동일한 해시값을 갖는 다른 메시지를 찾는 것은 계산상으로 불가능해야 한다.

답 ③

③ 대부분의 해시 함수는 입력 메시지의 길이에 상관없이 출력되는 해시값의 길이는 동일하다.

<오답 체크> ① 강한 충돌 내성(strong collision resistance)
(= 충돌 회피성(collision freeness))
출력 해시값이 같은 임의의 서로 다른 두 메시지를 찾을 수 없다.

② 일방향성(onewayness)
역산할 수 없다. 해시값으로부터 원본 메시지를 찾을 수 없다.

④ 약한 충돌 내성(weak collision resistance)
(= 제2 역상 저항성(second preimage resistance))
주어진 해시값과 같은 해시값을 갖는 다른 메시지를 찾을 수 없다.

문 3. 다음 내용에 해당하는 공개키 기반 구조(PKI)의 구성 요소로 옳은 것은?

> ○ 사용자에 대한 공개키 인증서를 생성하고 이를 발급한다.
> ○ 필요 시 사용자 인증서에 대한 갱신 및 폐기 기능을 수행한다.
> ○ 인증서 폐기 목록(certificate revocation list)을 작성한다.

① 사용자 ② 등록 기관
③ 인증 기관 ④ 디렉토리

답 ③

③ 인증 기관(CA, Certification Authority)은 공개키 인증서와 인증서 폐기목록을 생성하고 발급한다.
<오답 체크> ② 등록 기관(RA)은 인증기관과 사용자 사이에서 사용자 신분 확인, 인증서 발급을 중개, 전달한다.

문 4. ㉠과 ㉡에 들어갈 용어로 옳은 것은?

> (㉠)은(는) 디지털 콘텐츠를 구매할 때 구매자의 정보를 삽입하여 불법 배포 발견 시 최초의 배포자를 추적할 수 있게 하는 기술이다. (㉡)은(는) 원본의 내용을 왜곡하지 않는 범위 내에서 사용자가 인식하지 못하도록 저작권 정보를 디지털 콘텐츠에 삽입하는 기술이다.

	㉠	㉡
①	크래커(Cracker)	커버로스(Kerberos)
②	크래커(Cracker)	워터마킹(Watermarking)
③	핑거프린팅(Fingerprinting)	커버로스(Kerberos)
④	핑거프린팅(Fingerprinting)	워터마킹(Watermarking)

답 ④

④ 핑거프린팅(fingerprinting)
콘텐츠에 구매자의 정보를 삽입하여 불법 배포 근원지를 추적하는 기술이다.
디지털 워터마킹(digital watermarking)
저작권자의 정보를 삽입하여 원본과 출처에 대한 정보를 추적할 수 있는 기술이다.

문 5. 다음 내용에 해당하는 암호블록 운용 모드를 바르게 나열한 것은?

> ㄱ. 코드북(codebook)이라 하며, 가장 간단하게 평문을 동일한 크기의 평문블록으로 나누고 키로 암호화하여 암호블록을 생성한다.
> ㄴ. 현재의 평문블록과 바로 직전의 암호블록을 XOR한 후 그 결과를 키로 암호화하여 암호블록을 생성한다.
> ㄷ. 각 평문블록별로 증가하는 서로 다른 카운터 값을 키로 암호화하고 평문블록과 XOR하여 암호블록을 생성한다.

	ㄱ	ㄴ	ㄷ
①	CBC	ECB	OFB
②	CBC	ECB	CTR
③	ECB	CBC	OFB
④	ECB	CBC	CTR

답 ④

ㄱ. **ECB**(electronic codebook, 전자 코드북) 모드
가장 간단한 구조로, 암호화하려는 메시지를 여러 블록으로 나누어 각각 암호화하는 방식이다.

ㄴ. **CBC**(cipher-block chaining, 암호 블록 체인) 모드
평문 블록을 이전 단계의 암호문 블록과 XOR 한 후 암호화한다.
첫 번째 평문 블록의 경우에는 초기화 벡터(IV)와 XOR 한 후 암호화한다.
초기화 벡터가 같은 경우 출력 결과가 같기 때문에, 매 암호화마다 다른 초기화 벡터를 사용해야 한다.

ㄷ. **CTR**(Counter, 카운터) 모드
1씩 증가하는 카운터 값을 암호화하여 스트림 암호를 생성한 후, 생성한 스트림 암호화 평문 블록을 XOR하여 암호문 블록을 생성한다.

- **CFB**(cipher feedback, 암호 피드백) 모드
  CBC의 변형으로, 이전 단계의 암호문 블록을 암호화한 후 현재의 평문 블록과 XOR 한다.
  첫 번째 평문 블록의 경우에는 초기화 벡터(IV)를 암호화한 것과 XOR 한다.
- **OFB**(output feedback, 출력 피드백) 모드
  초기화 벡터(IV)를 매 단계마다 암호화해가며 스트림 암호를 생성한 후, 생성한 스트림 암호화 평문 블록을 XOR하여 암호문 블록을 생성한다.

문 6. 네트워크 공격에 대한 설명으로 옳지 않은 것은?

① Spoofing : 네트워크에서 송.수신되는 트래픽을 도청하는 공격이다.
② Session hijacking : 현재 연결 중인 세션을 가로채는 공격이다.
③ Teardrop : 네트워크 프로토콜 스택의 취약점을 이용한 공격 방법으로 시스템에서 패킷을 재조립할 때, 비정상 패킷이 정상 패킷의 재조립을 방해함으로써 네트워크를 마비시키는 공격이다.
④ Denial of Service : 시스템 및 네트워크의 취약점을 이용하여 사용 가능한 자원을 소비함으로써, 실제 해당 서비스를 사용하려고 요청하는 사용자들이 자원을 사용할 수 없도록 하는 공격이다.

답 ①

① 트래픽을 도청하는 공격은 **스니핑**(sniffing)이다.
스푸핑(spoofing)이란 네트워크 상에서 자신의 신분을 속이거나 다른 사용자로 위장해 공격 대상에 불법 접근하여 정보를 빼내는 것이다.

<오답 체크> ② **세션 하이재킹**(Session Hijacking) 공격
시스템에 접근할 적법한 사용자 아이디와 패스워드를 모를 때, 이미 시스템에 접속되어 세션이 연결되어 있는 사용자의 세션을 가로채기 하는 공격이다.

③ **Teardrop** 공격은 신뢰성을 제공하는 프로토콜의 취약점을 이용한 DoS공격으로, 패킷의 순서번호가 서로 중복되도록 조작하는 공격이다.
목표 대상 시스템은 이렇게 보내진 패킷들을 재조합하려고 시도하지만, 계속 실패하여 시스템 자원이 고갈되어 서비스 불능 상태에 빠진다.

- Bonk 공격은 패킷의 순서번호를 모두 1로 조작하여 보내는 공격
- Boink 공격은 패킷의 순서번호를 처음에는 순서대로 보내다가 중간부터 반복되는 순서번호를 보내는 공격이다

④ **DoS**(Denial of Service, 서비스 거부 공격)은 해당 시스템의 자원을 고갈시켜 제대로 사용하지 못하게 하는 공격이다.

문 7. 스택 버퍼 오버플로우 공격의 수행 절차를 순서대로 바르게 나열한 것은?

> ㄱ. 특정 함수의 호출이 완료되면 조작된 반환 주소인 공격 쉘 코드의 주소가 반환된다.
> ㄴ. 루트 권한으로 실행되는 프로그램 상에서 특정 함수의 스택 버퍼를 오버플로우시켜서 공격 쉘 코드가 저장되어 있는 버퍼의 주소로 반환 주소를 변경한다.
> ㄷ. 공격 쉘 코드를 버퍼에 저장한다.
> ㄹ. 공격 쉘 코드가 실행되어 루트 권한을 획득하게 된다.

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

답 ③

오버플로우(buffer overflow) 공격은 프로그램에 미리 할당된 버퍼보다 더 많은 양의 데이터를 집어넣어, 다른 메모리 영역을 침범하여 데이터를 변조시키는 공격이다.

ㄷ. 공격 쉘 코드를 버퍼에 저장한다.
↓
ㄴ. 루트 권한으로 실행되는 프로그램 상에서 특정 함수의 스택 버퍼를 오버플로우시켜서 공격 쉘 코드가 저장되어 있는 버퍼의 주소로 반환 주소를 변경한다.
↓
ㄱ. 특정 함수의 호출이 완료되면 조작된 반환 주소인 공격 쉘 코드의 주소가 반환된다.
↓
ㄹ. 공격 쉘 코드가 실행되어 루트 권한을 획득하게 된다.

문 8. 접근통제(access control) 모델에 대한 설명으로 옳지 않은 것은?

① 임의적 접근통제는 정보 소유자가 정보의 보안 레벨을 결정 하고 이에 대한 정보의 접근제어를 설정하는 모델이다.
② 강제적 접근통제는 중앙에서 정보를 수집하고 분류하여, 각각의 보안 레벨을 붙이고 이에 대해 정책적으로 접근제어를 설정하는 모델이다.
③ 역할 기반 접근통제는 사용자가 아닌 역할이나 임무에 권한을 부여하기 때문에 사용자가 자주 변경되는 환경에서 유용한 모델이다.
④ Bell-LaPadula 접근통제는 비밀노출 방지보다는 데이터의 무결성 유지에 중점을 두고 있는 모델이다.

답 ④

④ **BLP**(Bell-LaPadula, 벨 라파듈라) 모델은 **기밀성**을 중시한 모델이다.
높은 보안수준의 문서 내용이 낮은 보안수준으로 흐르는 걸 방지하는 데 중점을 둔다.
따라서 높은 등급의 데이터를 못 읽고, 낮은 등급에 쓸 수 없다.
단순 보안 속성 – NRU(No Read Up)
Star 속성 – NWD(No Write Down)

- **Biba**(비바) 모델은 **무결성**을 중시한 모델
높은 보안수준의 문서 내용이 원하지 않는 방향으로 변경되는 것을 방지하는 데 중점을 둔다.
높은 등급의 데이터에 쓸 수 없고, 낮은 등급의 데이터를 읽을 수 없다.
단순 무결성 속성 - NRD(No Read Down)
무결성 star 속성 - NWU(No Write Up)

<오답 체크> ② **강제적 접근 제어**(MAC, Mandatory Access Control)
관리자가 규칙을 작성하기 때문에 **규칙 기반 접근 제어**(Rule Based Access Control)이라고도 한다.

문 9. 개인정보 보호법령상 개인정보 영향평가에 대한 설명으로 옳지 않은 것은?

① 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인 정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려 되는 경우에는 위험요인분석과 개선 사항 도출을 위한 평가를 하고, 그 결과를 행정자치부장관에게 제출하여야 한다.

② 개인정보 영향평가의 대상에 해당하는 개인정보파일은 공공 기관이 구축·운용 또는 변경하려는 개인정보파일로서 50만명 이상의 정보주체에 관한 개인정보파일을 말한다.

③ 영향평가를 하는 경우에는 처리하는 개인정보의 수, 개인 정보의 제3자 제공 여부, 정보주체의 권리를 해할 가능성 및 그 위험정도, 그 밖에 대통령령으로 정한 사항을 고려하여야 한다.

④ 행정자치부장관은 제출받은 영향평가 결과에 대하여 보호 위원회의 심의·의결을 거쳐 의견을 제시할 수 있다.

답 ②

② 50만(X) -> 100만(○)

「개인정보 보호법」

제33조(개인정보 영향평가)

① 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가(이하 "영향평가"라 한다)를 하고 그 결과를 행정안전부장관에게 제출하여야 한다. 이 경우 공공기관의 장은 영향평가를 행정안전부장관이 지정하는 기관(이하 "평가기관"이라 한다) 중에서 의뢰하여야 한다.

② 영향평가를 하는 경우에는 다음 각 호의 사항을 고려하여야 한다.

1. 처리하는 개인정보의 수
2. 개인정보의 제3자 제공 여부
3. 정보주체의 권리를 해할 가능성 및 그 위험 정도
4. 그 밖에 대통령령으로 정한 사항

③ 행정안전부장관은 제1항에 따라 제출받은 영향평가 결과에 대하여 보호위원회의 심의·의결을 거쳐 의견을 제시할 수 있다.

④ 공공기관의 장은 제1항에 따라 영향평가를 한 개인정보파일을 제32조제1항에 따라 등록할 때에는 영향평가 결과를 함께 첨부하여야 한다.

⑤ 행정안전부장관은 영향평가의 활성화를 위하여 관계 전문가의 육성, 영향평가 기준의 개발·보급 등 필요한 조치를 마련하여야 한다.

⑥ 제1항에 따른 평가기관의 지정기준 및 지정취소, 평가기준, 영향평가의 방법·절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

⑦ 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속 기관을 포함한다)의 영향평가에 관한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙 및 중앙선거관리위원회규칙으로 정하는 바에 따른다.

⑧ 공공기관 외의 개인정보처리자는 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 영향평가를 하기 위하여 적극 노력하여야 한다.

「개인정보 보호법 시행령」

제35조(개인정보 영향평가의 대상)

법 제33조제1항에서 "대통령령으로 정하는 기준에 해당하는 개인정보파일"이란 개인정보를 전자적으로 처리할 수 있는 개인정보파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다.

1. 구축·운용 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일
2. 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일
3. 구축·운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일
4. 법 제33조제1항에 따른 개인정보 영향평가(이하 "영향평가"라 한다)를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일. 이 경우 영향평가 대상은 변경된 부분으로 한정한다.

문 10. 정보보호 시스템에서 사용된 보안 알고리즘 구현 과정에서 곱셈에 대한 역원이 사용된다. 잉여류 Z_{26}에서 법(modular) 26에 대한 7의 곱셈의 역원으로 옳은 것은?

① 11 ② 13
③ 15 ④ 17

답 ③

곱셈에 대한 역원 구하는 법은
$7 \times a \bmod 26 \equiv 1$ 이 되는 a를 찾으면 된다.
$26 \times 1 + 1 = 26 + 1 = 27$
$26 \times 2 + 1 = 52 + 1 = 53$
$26 \times 3 + 1 = 78 + 1 = 79$
$26 \times 4 + 1 = 104 + 1 = 105$(7의 15배수)
$7 \times 15 \bmod 26 \equiv 1$
∴ 26에 대한 7의 곱셈의 역원은 15이다.

문 11. 응용 계층 프로토콜에서 동작하는 서비스에 대한 설명으로 옳지 않은 것은?

① FTP : 파일전송 서비스를 제공한다.
② DNS : 도메인 이름과 IP 주소 간 변환 서비스를 제공한다.
③ POP3 : 메일 서버로 전송된 메일을 확인하는 서비스를 제공한다.
④ SNMP : 메일전송 서비스를 제공한다.

답 ④

④ **SNMP**(Simple Network Management Protocol, 간이 망 관리 프로토콜)은 IP 네트워크상의 장치로부터 정보를 수집 및 관리하며, 또한 정보를 수정하여 장치의 동작을 변경하는 데에 사용되는 인터넷 표준 프로토콜이다.
메일전송 서비스를 제공하는 프로토콜은 SMTP이다.

<오답 체크> ② **DNS**(Domain Name System, 도메인 네임 시스템) 호스트의 도메인 이름을 호스트의 네트워크 주소로 바꾸거나 그 반대의 변환을 수행한다. 특정 컴퓨터(또는 네트워크로 연결된 임의의 장치)의 주소를 찾기 위해, 사람이 이해하기 쉬운 도메인 이름을 숫자로 된 식별 번호(IP 주소)로 변환해준다.

③ 전자메일 관련 프로토콜
SMTP(Simple Mail Transfer Protocol, 간이 전자 우편 전송 프로토콜)
전자메일 송신 프로토콜
POP3(Post Office Protocol)
전자메일 수신 프로토콜, 읽으면 자동 삭제 자동 다운
IMAP(Internet Message Access Protocol, 인터넷 메시지 접속 프로토콜)
전자메일 수신 프로토콜, 읽어도 삭제되지 않음, 다운 여부 본인이 결정

문 12. 「개인정보 보호법」상 용어 정의로 옳지 않은 것은?

① 개인정보 : 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)

② 정보주체 : 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인

③ 처리 : 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위

④ 개인정보파일 : 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물

답 ②

② 개인정보처리자에 대한 설명이다.

「개인정보 보호법」 제2조(정의)

이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. "개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.
2. "처리"란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
3. "정보주체"란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
4. "개인정보파일"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
5. "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
7. "영상정보처리기기"란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치를 말한다.

문 13. 다음 설명에 해당하는 OECD 개인정보보호 8원칙으로 옳은 것은?

> 개인정보는 이용 목적상 필요한 범위 내에서 개인정보의 정확성, 완전성, 최신성이 확보되어야 한다.

① 이용 제한의 원칙(Use Limitation Principle)

② 정보 정확성의 원칙(Data Quality Principle)

③ 안전성 확보의 원칙(Security Safeguards Principle)

④ 목적 명시의 원칙(Purpose Specification Principle)

답 ②

※ OECD 개인정보보호 8원칙 ※

① 수집 제한의 법칙(Collection Limitation Principle) : 개인정보는 적법하고 공정한 방법을 통해 수집되어야 한다.

② 정보 정확성의 원칙(Data Quality Principle) : 이용 목적상 필요한 범위 내에서 개인정보의 정확성, 완전성, 최신성이 확보되어야 한다.

③ 목적 명시의 원칙(Purpose Specification Principle) : 개인정보는 수집 과정에서 수집 목적을 명시하고, 명시된 목적에 적합하게 이용되어야 한다.

④ 이용 제한의 원칙(Use Limitation Principle) : 정보 주체의 동의가 있거나, 법규정이 있는 경우를 제외하고 목적 외 이용되거나 공개될 수 없다.

⑤ 안전성 확보의 원칙(Security Safeguard Principle) : 개인정보의 침해, 누설, 도용 등을 방지하기 위한 물리적, 조직적, 기술적 안전 조치를 확보해야 한다.

⑥ 공개의 원칙(Openness Principle) : 개인정보의 처리 및 보호를 위한 정책 및 관리자에 대한 정보는 공개되어야 한다.

⑦ 개인 참가의 원칙(Individual Participation Principle) : 정보 주체의 개인정보 열람/정정/삭제 청구권은 보장되어야 한다.

⑧ 책임의 원칙(Accountability Principle) : 개인정보 관리자에게 원칙 준수 의무 및 책임을 부과해야 한다.

문 14. 현행 우리나라의 정보보호관리체계(ISMS) 인증에 대한 설명으로 옳지 않은 것은?

① 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 근거를 두고 있다.
② 인증심사의 종류에는 최초심사, 사후심사, 갱신심사가 있다.
③ 인증에 유효기간은 정해져 있지 않다.
④ 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하고 있는 자에 대하여 인증 기준에 적합한지에 관하여 인증을 부여하는 제도이다.

답 ③

③ 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」
제47조(정보보호 관리체계의 인증)
⑤ 제1항에 따른 정보보호 관리체계 **인증의 유효기간은 3년으로 한다.** 다만, 제47조의5제1항에 따라 정보보호 관리등급을 받은 경우 그 유효기간 동안 제1항의 인증을 받은 것으로 본다.

<오답 체크> ① ISMS 법적근거
「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조(정보보호 관리체계의 인증)
「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」 (제47조~제54조)
「정보보호 관리체계 인증 등에 관한 고시」(미래창조과학부 고시 제2016-59호)

② 최초심사: 정보보호 관리체계 인증 취득을 위한 심사
(범위 변경 등 중요한 변경사항 발생시에도 최초심사)
사후심사: 정보보호 관리체계를 지속적으로 유지하고 있는지에 대한 심사(연 1회 이상)
갱신심사: 유효기간(3년) 만료일 이전에 유효기간 연장을 목적으로 하는 심사

④ 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」
제47조(정보보호 관리체계의 인증)
① 과학기술정보통신부장관은 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.

문 15. 보안 서비스에 대한 설명을 바르게 나열한 것은?

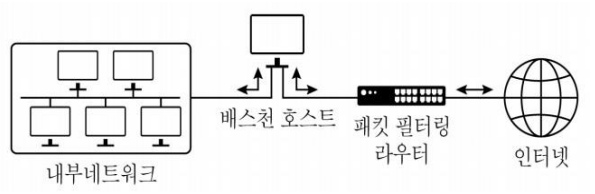
ㄱ. 메시지가 중간에서 복제·추가·수정되거나 순서가 바뀌거나 재전송됨이 없이 그대로 전송되는 것을 보장한다.
ㄴ. 비인가된 접근으로부터 데이터를 보호하고 인가된 해당 개체에 적합한 접근 권한을 부여한다.
ㄷ. 송·수신자 간에 전송된 메시지에 대해서, 송신자는 메시지 송신 사실을, 수신자는 메시지 수신 사실을 부인하지 못하도록 한다.

	ㄱ	ㄴ	ㄷ
①	데이터 무결성	부인봉쇄	인증
②	데이터 가용성	접근통제	인증
③	데이터 기밀성	인증	부인봉쇄
④	데이터 무결성	접근통제	부인봉쇄

답 ④

ㄴ. 불법적인 접근을 거부하고 정당한 사용자만 접근을 허용하는 것은 접근통제이다.
인증은 상대방이 진짜인지 아닌지 확인하는 것이다.
ㄴ을 경우에 따라서는 인증으로 볼 수도 있겠지만, ㄱ이 무결성이 확실하기 때문에 답은 ④번밖에 되지 않는다.

문 16. 다음에 해당하는 방화벽의 구축 형태로 옳은 것은?



○ 인터넷에서 내부네트워크로 전송되는 패킷을 패킷 필터링 라우터에서 필터링함으로써 1차 방어를 수행한다.
○ 배스천 호스트에서는 필터링 된 패킷을 프록시와 같은 서비스를 통해 2차 방어 후 내부네트워크로 전달한다.

① 응용 레벨 게이트웨이(Application-level gateway)
② 회로 레벨 게이트웨이(Circuit-level gateway)
③ 듀얼 홈드 게이트웨이(Dual-homed gateway)
④ 스크린 호스트 게이트웨이(Screened host gateway

답 ④

④ 스크린드 호스트 게이트웨이(Screened Host Gateway)
외부에서 내부로 들어오는 트래픽을 외부 네트워크와 연결된 스크리닝 라우터에서 패킷 필터링을 함으로써 1차 방어를 한 뒤, 내부 네트워크와 연결된 베스천 호스트에서 2차 방어를 함

<오답 체크>

① 응용레벨 게이트웨이(Application Level Gateway)
프록시(proxy) 기능을 적용하여, 내부와 외부 간의 응용 계층의 모든 트래픽에 대해 인증 기능을 제공

② 회로 레벨 게이트웨이(Circuit Level Gateway)
패킷 필터와 어플리케이션 게이트웨이 사이의 중간 솔루션으로, 모든 응용 프로그램에 대한 프록시 역할을 한다.
전체 종단 간 TCP 연결을 허용하지 않는다. 두 개의 TCP 연결을 설정한다.

③ 듀얼 홈 게이트웨이(Dual Home Gateway)
네트워크 카드가 두 개 이상 있는 방화벽으로 외부, 내부 네트워크 카드가 구별되어 운용된다.

• 스크린드 서브넷 게이트웨이(Screened Subnet Gateway)
외부 네트워크와 내부 네트워크 사이에 서브넷(Subnet)이라는 완충지대를 두며, 서브넷에는 주로 DMZ와 방화벽이 위치한다.
내부 네트워크와 서브넷 사이에 스크리닝 라우터 1개, 외부 네트워크와 서브넷 사이에도 스크리닝 라우터 1개, 총 2개의 스크리닝 라우터가 들어간다.

문 17. SSH(Secure SHell)를 구성하고 있는 프로토콜 스택으로 옳지 않은 것은?

① SSH User Authentication Protocol
② SSH Session Layer Protocol
③ SSH Connection Protocol
④ SSH Transport Layer Protocol

답 ②

※ SSH 프로토콜 스택구조
SSH 응용 프로토콜 : TELNET,RLOGIN,SMTP 등
SSH 인증 프로토콜(User Authentication Protocol) : 사용자 인증(User Authentication) 제공
SSH 연결 프로토콜(Connection Protocol) : 1개의 암호화된 터널을 통해 다수개의 논리채널 다중화
SSH 전송 프로토콜(Transport Layer Protocol) : 인증, 기밀성, 무결성, 압축(옵션) 제공

문 18. 위험분석 방법에 대한 설명을 바르게 나열한 것은?

ㄱ. 시스템에 관한 전문적인 지식을 가진 전문가 집단을 구성하고 토론을 통해 정보시스템이 직면한 다양한 위협과 취약성을 분석하는 방법이다.
ㄴ. 자산의 가치 분석, 위협 분석, 취약점 분석을 수행하여 위험을 분석하는 방법이다.
ㄷ. 표준화된 보호대책의 세트를 체크리스트 형태로 구현 하여 이를 기반으로 보호대책을 식별하는 방법이다.

	ㄱ	ㄴ	ㄷ
①	시나리오법	기준선 접근법	상세 위험 분석 접근법
②	시나리오법	상세 위험 분석 접근법	기준선 접근법
③	델파이법	기준선 접근법	상세 위험 분석 접근법
④	델파이법	상세 위험 분석 접근법	기준선 접근법

답 ④

ㄱ. 델파이법(Delphi method)은 전문가 합의법이라고도 한다.
<오답 체크> 시나리오법은 어떤 사건이 예상대로 발생하지 않는다는 사실에 근거하여 주어진 조건하에 발생 가능한 위협들을 예측하는 방법이다.

문 19.「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 개인정보 취급방침에 포함되어야 할 사항이 아닌 것은?

① 이용자 및 법정대리인의 권리와 그 행사 방법
② 개인정보에 대한 내부 관리 계획
③ 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항
④ 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목 및 수집 방법

답 ②

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」
제27조의2(개인정보 처리방침의 공개)
① 정보통신서비스 제공자등은 이용자의 개인정보를 처리하는 경우에는 개인정보 처리방침을 정하여 이용자가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.
② 제1항에 따른 개인정보 처리방침에는 다음 각 호의 사항이 모두 포함되어야 한다.
1. **개인정보의 수집·이용 목적, 수집하는 개인정보의 항목 및 수집방법**
2. 개인정보를 제3자에게 제공하는 경우 제공받는 자의 성명(법인인 경우에는 법인의 명칭을 말한다), 제공받는 자의 이용 목적과 제공하는 개인정보의 항목
3. 개인정보의 보유 및 이용 기간, 개인정보의 파기절차 및 파기방법(제29조제1항 각 호 외의 부분 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다)
4. 개인정보 처리위탁을 하는 업무의 내용 및 수탁자(해당되는 경우에만 처리방침에 포함한다)
5. **이용자 및 법정대리인의 권리와 그 행사방법**
6. **인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항**
7. 개인정보 보호책임자의 성명 또는 개인정보보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 그 전화번호 등 연락처
③ 정보통신서비스 제공자등은 제1항에 따른 개인정보 처리방침을 변경하는 경우에는 그 이유 및 변경내용을 대통령령으로 정하는 방법에 따라 지체 없이 공지하고, 이용자가 언제든지 변경된 사항을 쉽게 알아 볼 수 있도록 조치하여야 한다.

문 20. 전자서명 방식에 대한 설명으로 옳지 않은 것은?

① 은닉 서명(blind signature)은 서명자가 특정 검증자를 지정하여 서명하고, 이 검증자만이 서명을 확인할 수 있는 방식이다.
② 부인방지 서명(undeniable signature)은 서명을 검증할 때 반드시 서명자의 도움이 있어야 검증이 가능한 방식이다.
③ 위임 서명(proxy signature)은 위임 서명자로 하여금 서명자를 대신해서 대리로 서명할 수 있도록 한 방식이다.
④ 다중 서명(multisignature)은 동일한 전자문서에 여러 사람이 서명하는 방식이다.

답 ①

① 수신자지정 서명에 대한 서명이다.
수신자 지정 서명(nominative signatures)은 지정된 수신자만 서명을 확인할 수 있으며, 서명을 한 당사자도 서명 확인을 할 수 없다.
은닉 서명(blind signature)은 용어 그대로, 서명의 유효성만 확인할 뿐 서명자의 신상정보는 알 수 없도록 감춰주는 서명 방식이다. 전자투표나 비밀 자금거래 등에 이용된다.