2019년 국가직 7급 정보보호론 풀이

by 호이호이꿀떡

정답 체크

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

문 1. Biba 보안 모델에 대한 설명으로 옳은 것은?

① 이해가 상충되는 회사들 간의 정보 흐름이 일어나지 않도록 고안되었다.
② 자신의 보안 수준보다 낮거나 같은 수준의 객체만 읽을 수 있다.
③ 자신의 보안 수준보다 높거나 같은 수준의 객체에만 쓸 수 있다.
④ 자신의 무결성 수준보다 높거나 같은 수준의 객체만 읽을 수 있다.

답 ④

④ **비바**(Biba) 모델
무결성을 중시한 모델
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> ① **Chineses Wall**(만리장성) 모델
서로 상충관계에 있는 객체간의 정보 접근을 통제하는 모델. 이익의 충돌이 많이 발생하는 금융, 회계, 투자, 광고 등의 분야에서 주로 사용된다.

②③ **벨 라파듈라**(BLP, Bell-LaPadula) 모델
기밀성을 중시한 모델
따라서 높은 등급의 데이터를 못 읽고, 낮은 등급에 쓸 수 없다.
단순 보안 속성 – NRU(No Read Up)
Star(*) 속성 – NWD(No Write Down)

문 2. IT 재해복구체계 수립 시, 업무영향분석(BIA: Business Impact Analysis) 과정에서 고려하는 항목이 아닌 것은?

① MTD(Maximum Tolerable Downtime)
② MTU(Maximum Transfer Unit)
③ RTO(Recovery Time Objective)
④ RPO(Recovery Point Objective)

답 ②

▶ 업무 영향 분석(BIA, Business Impact Analysis)
조직 내의 중요한 업무기능을 파악하고, 각종 재난·재해 등으로 인해 업무기능이 중지되었을 때를 가정하여 영향을 분석하는 것이다.
분석 과정에서 MTD, RPO, RTO를 활용한다.
▷ MTD(Maximum Tolerable Downtime, 한계복구시간)
핵심 프로세스가 정지된 후 회복 전까지 버틸 수 있는 시간
▷ RPO(Recovery Point Objective, 복구목표시점)
현재 시점을 기준으로 가장 가까운 복원지점까지의 시간 목표
수용할 수 있는 데이터 손실의 최대 허용량
▷ RTO(Recovery Time Objective, 복구재해시간)
시스템이 복구될 때까지 걸리는 목표 시간

<오답 체크> ② MTU(Maximum Transfer Unit)는 데이터 통신에서 각 프로토콜이 한 번에 데이터를 전송할 수 있는 최대 크기 단위이다.

문 3. 다음에서 설명하는 위험 분석 접근 방법은?

○ 정형화되고 구조화된 프로세스를 사용하는 대신, 분석가 개인의 지식 및 경험을 활용한다.
○ 비교적 비용대비 효과가 우수하며 중.소규모 조직에 적합하다.
○ 개인적인 경험에 의존하므로 정당성이나 일관성이 부족할 수 있다.

① 기준선 접근(Baseline Approach)
② 상세 위험 분석(Detailed Risk Analysis)
③ 비형식적 접근(Informal Approach)
④ 복합 접근(Combined Approach)

답 ③

③ **비정형 접근법**(비형식적 접근법)은 구조적인 체계 없이 컨설턴트의 경험과 지식을 이용하여 위험 분석을 하는 접근법이다.

<오답 체크> ① **기준선 접근법**(베이스라인 접근법)은 보호 대책에 대한 항목별로 체크리스트를 작성해 평가하는 방법으로, 국제정보보호관리체계, 정보보호관리체계(ISMS), 개인정보보호관리체계(PIMS) 등과 같은 인증 심사 때 많이 사용한다.

② **상세 위험 분석 접근법**은 자산 식별, 위협 분석, 취약점 분석을 단계별로 수행하여 위험을 분석하는 방법이다.

④ **복합 접근법**(통합 접근법)은 고위험 영역은 상세 위험분석을 수행하고, 그 외 영역은 기준선 접근법을 사용한다.

문 4. 다음 수식에 의해 산출되는 것은?

$$H[(K^{+} \oplus opad) \,||\, H[(K^{+} \oplus ipad) \,||\, M]]$$

H: 해시 함수
K^{+}: 비밀키 K에 0을 덧붙인 것
M: 메시지 ipad, opad: 특정 상수
⊕: XOR ||: 연결(concatenation)

① GMAC ② HMAC
③ CMAC ④ 전자 서명

답 ②

② HMAC(Hash-based MAC, 해시 기반 메시지 인증 코드)
해시값을 이용한 메시지 인증 코드로, 1997년 RFC2014로 작성되었다. 패딩 등을 이용하여 MAC보다 더 복잡하고, SHA1은 SHA1의 알고리즘을 이용한다는 걸 의미한다.

<오답 체크> ① GMAC(Galois MAC)
Galois/Counter Mode(GCM, 갈루아 카운터 모드)를 이용한 메시지 인증 코드

③ CMAC(Cipher-based MAC): AES, 3-DES를 이용한 메시지 인증 코드

◈ **HMAC 계산 과정**

1. 키에 대한 패딩 **key**
   키가 해시함수의 볼록 길이보다 짧다면 블록 길이가 될 때까지 0으로 패딩하고,
   키가 해시함수의 블록 길이보다 길다면 키의 해시값을 구해 HMAC의 키 값으로 삼는다.
2. 키와 ipad를 XOR **key ⊕ ipad**
   ipad는 00110110을 블록 길이만큼 반복한 값
3. 위의 비트열을 메시지의 앞에 붙임
   key ⊕ ipad || message
4. 3번의 결과를 일방향 해시 함수에 입력하여 해시값 계산
   hash(key ⊕ ipad || message)
5. 키와 opad를 XOR **key ⊕ opad**
   opad는 01011100을 블록 길이만큼 반복한 값
6. 위의 비트열에 4번의 해시값을 붙임
   key ⊕ opad || hash(key ⊕ ipad || message)
7. 6번의 결과를 일방행 해시 함수에 입력하여 해시값 계산
   이것이 HMAC의 값이 된다.
   hash(key ⊕ opad || hash(key ⊕ ipad || message))

문 5. 「정보보호 및 개인정보보호 관리체계(ISMS-P)의 인증 등에 관한 고시」 상의 인증심사 기준 중, '개인정보 처리 단계별 요구사항'에 포함되지 않는 것은?

① 사용자 계정 관리
② 이용자 단말기 접근 보호
③ 영상정보처리기기 설치·운영
④ 개인정보처리방침 공개

답 ①

◈ 개인정보 처리 단계별 요구사항
▶ **3.1** 개인정보 수집 시 보호조치
- 3.1.1 개인정보 수집 제한
- 3.1.2 개인정보의 수집 동의
- 3.1.3 주민등록번호 처리 제한
- 3.1.4 민감정보 및 고유식별정보의 처리 제한
- 3.1.5 간접수집 보호조치
- 3.1.6 영상정보처리기기 설치·운영
- 3.1.7 홍보 및 마케팅 목적 활용 시 조치

▶ **3.2** 개인정보 보유 및 이용 시 보호조치
- 3.2.1 개인정보 현황관리
- 3.2.2 개인정보 품질보장
- 3.2.3 개인정보 표시제한 및 이용 시 보호조치
- 3.2.4 이용자 단말기 접근 보호
- 3.2.5 개인정보 목적 외 이용 및 제공

▶ **3.3** 개인정보 제공 시 보호조치
- 3.3.1 개인정보 제3자 제공
- 3.3.2 업무 위탁에 따른 정보주체 고지
- 3.3.3 영업의 양수 등에 따른 개인정보의 이전
- 3.3.4 개인정보의 국외이전

▶ **3.4** 개인정보 파기 시 보호조치
- 3.4.1 개인정보의 파기
- 3.4.2 처리목적 달성 후 보유 시 조치
- 3.4.3 휴면 이용자 관리

▶ **3.5** 정보주체 권리보호
- 3.5.1 개인정보처리방침 공개
- 3.5.2 정보주체 권리보장
- 3.5.3 이용내역 통지

① '사용자 계정 관리'는 보호대책 요구사항 중 '2.5 인증 및 권한 관리'에 포함되는 항목이다.

문 6. 다음 리눅스 /etc/shadow 파일 항목에 대한 설명으로 옳지 않은 것은?

```
abcd:$1$qPZPGTVz$RDqazm48WaMXw3Mvy4OQb1:17562:0:99999:7:3::
```

① 계정명은 abcd이다.
② 계정 패스워드의 해시값 계산에 사용된 해시 함수는 MD-5이다.
③ 솔트(salt)값은 qPZPGTVz이다.
④ 계정 패스워드의 유효기간은 7일이다.

답 ④

abcd	사용자 이름
1qPZPGTVz$RDqazm48WaMXw3Mvy4OQb1	암호화된 패스워드 값
17562	마지막으로 패스워드를 수정한 날짜
0	패스워드 최소 사용기간(일) 패스워드 변경 후 이 기간이 지나기 전엔 다시 변경할 수 없다. 0은 언제나 바꿀 수 있다는 의미
99999	패스워드 최대 사용기간(일)
7	패스워드 만기일 전 알림을 제공하는 기간(일)
3	계정 만료 전 활성화 가능 기간(일)

그리고 그 뒤 비어있는 필드 2개는 계정 만료 기간 필드와 기타 예약 필드이다.

④ 따라서 패스워드의 유효기간은 99999일이다.
<오답 체크> ② 암호화된 패스워드 필드의 구성은
$해시 아이디(해시 계산 방식) $솔트 값 $해시 값 이다.

▷ 해시 아이디의 분류

1	MD5
2a	Blowfish
2y	Blowfish
md5	Sun MD5
5	SHA-256
6	SHA-512

문 7.「개인정보 보호법」상 개인정보처리자가 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있는 경우에 해당하지 않는 것은?

① 정보주체로부터 별도의 동의를 받은 경우
② 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우
③ 범죄의 예방을 위하여 필요한 경우
④ 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

답 ③

제18조(개인정보의 목적 외 이용 · 제공 제한)
① 개인정보처리자는 개인정보를 제15조제1항에 따른 범위를 초과하여 이용하거나 제17조제1항 및 제3항에 따른 범위를 초과하여 제3자에게 제공하여서는 아니 된다.
② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.

1. **정보주체로부터 별도의 동의를 받은 경우**
2. 다른 법률에 특별한 규정이 있는 경우
3. **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**
4. **통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우**
5. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의 · 의결을 거친 경우
6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
8. 법원의 재판업무 수행을 위하여 필요한 경우
9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

문 8.「전자정부 SW 개발·운영자를 위한 소프트웨어 개발 보안 가이드」상 분석·설계 단계 보안요구항목과 그에 대한 설명으로 옳지 않은 것은?

① 인증 수행 제한 - 인증 반복시도 제한 및 인증실패 등에 대한 인증제한 기능 설계
② 암호키 관리 - 암호키 생성, 분배, 접근, 파기 등 안전하게 암호키 생명주기를 관리할 수 있는 방법 설계
③ 예외 처리 - 보안기능 동작을 위해 사용되는 입력값과 함수의 외부입력값 및 수행결과에 대한 처리방법 설계
④ 시스템 자원 접근 및 명령어 수행 입력값 검증 - 시스템 자원접근 및 명령어 수행을 위해 사용되는 입력값에 대한 유효성 검증방법과 유효하지 않은 값에 대한 처리방법 설계

답 ③

문제에 나온 가이드 북은 한국인터넷진흥원 홈페이지 (https://www.kisa.or.kr/public/laws/laws3_View.jsp?cPage=6&mode=view&p_No=259&b_No=259&d_No=88&ST=T&SV=) 에서 다운로드나 미리보기 할 수 있다.

③ 38페이지 SR1-9 '보안기능 동작에 사용되는 입력값 검증' 항목에 대한 설명이다.
해당 항목들을 외우지 않더라도, 컴퓨터공학에서 '예외처리'는 주로 오류나 에러를 다루는 데 쓰이는 용어라는 것을 캐치하면 답을 찾을 수 있다.

문 9. 두 소수, p =13, q=11을 사용하는 RSA 시스템에서 키값 (e, d)로 사용할 수 있는 쌍은?

① **(7, 11)**
② **(7, 23)**
③ **(13, 37)**
④ **(13, 47)**

답 ③

p는 13, q는 11이므로,
오일러 함수 값 Φ(n) = (13 – 1) × (11 – 1) = 120 이다.
d는 오일러 값보다 작으며 서로소인 값이므로, 보기의 값 모두 해당하며,
e 값은 e × d mod Φ(n) = 1 을 만족해야 한다.

① 7 × 11 mod 120 = 77 mod 120 = **77**
② 7 × 23 mod 120 = 161 mod 120 = **41**
③ 13 × 37 mod 120 = 481 mod 120 = **1**
④ 13 × 47 mod 120 = 611 mod 120 = **11**

따라서 조건을 만족하는 숫자쌍은 ③번이다.

◈ RSA 알고리즘 공개키와 개인키 생성 순서
○ 단계 1: 두 소수 p, q를 선정한다.
○ 단계 2: n = p × q를 계산한다.
○ 단계 3: Φ(n) = (p – 1) × (q – 1)을 계산한다.
(단, Φ(n)은 오일러의 Totient 함수이다.)
○ 단계 4: Φ(n)보다 작고, Φ(n)과 서로소의 관계를 갖는 임의의 e 값을 선택한다.
○ 단계 5: e × d mod Φ(n) = 1의 관계를 갖는 d를 계산한다.
(단, mod는 나머지를 구하는 연산자이다.)
○ 단계 6: (e, n)을 공개키로 하고, (d, n)을 개인키로 한다.

암호문 $= (\text{평문})^{e} \bmod n$
평문 $= (\text{암호문})^{d} \bmod n$

문 10. 암호 화폐인 비트코인이 채택한 블록체인의 블록 헤더에 포함되는 구성 요소가 아닌 것은?

① 이전 블록의 헤더를 두 번 연속 해시한 값
② 해당 블록에 포함된 모든 트랜잭션의 해시로부터 추출된 merkle root 해시값
③ 작업증명(proof of work) 조건을 만족하는 nonce 값
④ 블록 생성자(miner)의 계정

답 ④

④ 블록 생성자의 계정 정보는 들어있지 않다.

◈ **비트코인 블록헤더**의 구성요소
1. **버전**(version)
2. **이전 블록 해시**(previous block hash)
이전 블록헤더를 SHA-256 해시함수를 이용하여 두 번 해싱한 해시값
3. **머클루트**(merkle root)
해당 블록에 포함된 거래정보의 거래 해시를 2진 트리 형태로 구성할 때 트리의 루트에 위치하는 해시값
4. **타임테이블**(time)
해당 블록의 생성 시간
5. **비츠**(bits)
블록의 작업증명에 대한 목표 난이도 설정값
6. **논스**(nonce)
작업증명 과정에서 구하는 값
nonce 값의 해시값은 특정 숫자보다 작아야 하며, 그 조건을 만족하기 위해 nonce 값을 1씩 증가시켜 해시값을 구하는 과정을 반복한다. 해시값이 특정 숫자보다 작아지는 nonce 값을 찾았다면, 그 nonce 값에 대한 정보를 새로운 블록 체인으로 추가한다. 이 과정을 작업증명이라고 한다.

문 11. 다음에서 설명하는 해시 함수(H)의 특성은?

> 주어진 메시지 x에 대해, H(y) = H(x)를 만족하면서 y≠x인 y를 찾는 것이 계산상 매우 어려워야 한다.

① 의사난수성(Pseudo-randomness)
② 역상 저항성(Pre-image Resistance)
③ 약한 충돌 저항성(Weak Collision Resistance)
④ 강한 충돌 저항성(Strong Collision Resistance)

답 ③

③ 주어진 메시지(x)와 같은 해시값을 갖는 다른 메시지(y)를 찾을 수 없어야 한다는 것은 약한 충돌 저항성에 대한 설명이다.
강한 충돌 저항성은 특별히 주어진 값이 아닌, 해시값이 같은 임의의 다른 두 메시지를 찾을 수 없어야 한다는 것이다.

▶ **일방향성**(onewayness)
(= **역상 저항성**(preimage resistance))
(= **약 일방향성**(weak onewayness)
역산할 수 없어야 한다.
해시값으로부터 원본 메시지를 찾을 수 없어야 한다.
▶ **약한 충돌 저항성**(weak collision resistance)
(= **제2 역상 저항성**(second preimage resistance))
(= **강 일방향성**(strong onewayness))
주어진 해시값과 같은 해시값을 갖는 다른 메시지를 찾을 수 없어야 한다.
▶ **강한 충돌 저항성**(strong collision resistance)
(= **충돌 저항성**(collision Resistance))
(= **충돌 회피성**(collision freeness))
출력 해시값이 같은 임의의 서로 다른 두 메시지를 찾을 수 없어야 한다.

<오답 체크> ① 난수는 무작위성, 예측 불가능성, 재현 불가능성의 성질을 가지며 이 세 조건을 만족하는 것을 '진정한 난수'라고 한다.
하지만 재현 불가능성은 특별한 장비가 필요하므로 일반적인 컴퓨터 환경에서는 구현이 불가능하다. 그래서 컴퓨터 환경에서 사용할 수 있도록 난수의 일부 성질만 만족하여 난수처럼 쓸 수 있게 만든 것을 '의사난수'라고 한다.
무작위성만 만족하는 난수를 '**약한 의사난수**',
무작위성과 예측 불가능성을 만족하는 난수를 '**강한 의사난수**'라고 한다.

문 12. ㉠~ ㉢에 들어갈 윈도우 운영체제 보안 컴포넌트를 모두 바르게 제시한 것은?

> (㉠)은 로컬 사용자에 관련된 보안 정보 및 계정 데이터를 저장하는 데이터베이스이다.
> (㉡)은 커널 모드에서 수행되며, 사용자나 프로세스가 어떤 객체를 열려고 시도하면, 접근 권한을 확인한다.
> (㉢)는 사용자 모드에서 수행되며, 로컬 보안 정책을 집행하는 책임이 있다.

	㉠	㉡	㉢
①	SAM	SRM	LSA
②	SRM	SAM	LSA
③	SAM	SRM	SID
④	SRM	SAM	SID

답 ①

㉠ **SAM**(Security Account Manager)
사용자/그룹 계정 정보에 대한 **데이터베이스 관리**
사용자 로그인 정보와 SAM 파일에 저장된 사용자 패스워드 정보를 비교해 인증 여부 결정
SAM 파일은 사용자, 그룹 계정 및 암호화된 패스워드 정보를 저장하고 있는 데이터베이스
㉡ **SRM**(Security Reference Monitor)
인증된 사용자에게 **SID(Security ID)를 부여**
SID를 기반으로 하여 파일이나 디렉터리에 대한 접근 허용 여부를 결정하고 이에 대한 감사 메시지를 생성
㉢ **LSA**(Local Security Authority)
모든 계정의 로그인에 대한 검증
시스템 자원(파일 등)에 대한 **접근 권한 검사**(로컬 및 원격 로그인 포함) 계정명과 SID(Security ID)를 매칭하여 SRM이 생성한 감사 로그를 기록
로컬 보안의 중심요소로, 보안 서브시스템(Security Subsystem)이라고도 함

문 13. 다음의 블록암호 운용모드 중, 암호 과정에서는 암호화 함수 E를, 복호 과정에서는 E와 다른 복호화 함수 D를 필요로 하는 것만을 모두 고르면?

ㄱ. ECB	ㄴ. CBC	ㄷ. CFB	ㄹ. OFB

① ㄱ ② ㄱ, ㄴ
③ ㄷ, ㄹ ④ ㄱ, ㄴ, ㄹ

답 ②

별도의 복호화 함수가 필요한 것은 ECB와 CBC 모드이다.
CFB, OFB, CTR 모드는 별도의 복호화 함수가 필요없이, 복호화 과정에서도 암호화 함수를 사용한다.

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

◈ **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.

◈ **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 암호와 평문 블록을 XOR하여 암호문 블록을 생성한다.

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

문 14. 「개인정보 보호법」상 '정보주체의 권리 보장'에 대한 설명으로 옳지 않은 것은?

① 정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 해당 개인정보처리자에게 요구할 수 있다.
② 자신의 개인정보를 열람한 정보주체는 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구할 수 있다. 다만, 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 개인정보 보호위원회의 심의를 거쳐 요구할 수 있다.
③ 개인정보처리자는 정보주체가 열람등요구를 할 수 있는 구체적인 방법과 절차를 마련하고, 이를 정보주체가 알 수 있도록 공개하여야 한다.
④ 개인정보처리자는 정보주체가 열람등요구에 대한 거절 등 조치에 대하여 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하여야 한다.

답 ②

② **제36조**(개인정보의 정정 · 삭제) ① 제35조에 따라 자신의 개인정보를 열람한 정보주체는 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구할 수 있다. 다만, 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 **그 삭제를 요구할 수 없다.**

<오답 체크> ① **제35조**(개인정보의 열람) ① 정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 해당 개인정보처리자에게 요구할 수 있다.

「개인정보 보호법」 제38조(권리행사의 방법 및 절차)
① 정보주체는 제35조에 따른 열람, 제36조에 따른 정정 · 삭제, 제37조에 따른 처리정지 등의 요구(이하 "열람등요구"라 한다)를 문서 등 대통령령으로 정하는 방법 · 절차에 따라 대리인에게 하게 할 수 있다.
② 만 14세 미만 아동의 법정대리인은 개인정보처리자에게 그 아동의 개인정보 열람등요구를 할 수 있다.
③ 개인정보처리자는 열람등요구를 하는 자에게 대통령령으로 정하는 바에 따라 수수료와 우송료(사본의 우송을 청구하는 경우에 한한다)를 청구할 수 있다.
④ 개인정보처리자는 정보주체가 열람등요구를 할 수 있는 구체적인 방법과 절차를 마련하고, 이를 정보주체가 알 수 있도록 공개하여야 한다.
⑤ 개인정보처리자는 정보주체가 열람등요구에 대한 거절 등 조치에 대하여 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하여야 한다.

문 15. 패스워드를 이용해서 원격 사용자를 인증하는 경우, 호스트는 비표(nonce)라는 일회성 임의 숫자 r를 생성하고 이와 함께 두 함수 h()와 f()를 사용자에게 제시한다. 사용자는 이에 대한 응답으로 f(r', h(P'))를 반환한다. 호스트는 r' =r, h(P') =h(사용자 패스워드)의 여부를 판단하여 인증을 완료한다. 이때, r를 사용하는 것은 어떤 공격에 대비하기 위한 것인가?

① 전사 공격(Brute-Force Attack)
② 트래픽 스니핑 공격(Traffic Sniffing Attack)
③ 패스워드 사전 공격(Password Dictionary Attack)
④ 재전송 공격(Replay Attack)

답 ④

문제의 설명을 요약하자면,
사용자가 호스트에 접속하려고 인증할 때, 호스트는 임의의 랜덤 값인 비표(nonce)를 사용자에게 전송하고, 사용자는 그 비표를 이용해 계산하여 그 결과값을 전송함으로써 인증하는 방식이다.
이것은 비동기식 인증 방식인 **시도-응답(Challenge-Response) 인증 방식**에 대한 설명이다.

④ 시도-응답 인증 방식은 매번 로그인시 다른 값을 사용해 인증을 하기 때문에 재전송 공격을 방지할 수 있다.

문 16. HTTP 버전 1.1에 대한 설명으로 옳지 않은 것은?

① TCP를 전송 프로토콜로 사용한다.
② 요청 메시지의 첫 줄인 요청 라인에는 메소드, URL, HTTP 버전 필드가 포함된다.
③ 요청과 그에 대한 응답이 같은 연결로 보내지는 지속 연결(persistent connection)을 기본으로 하며, 분리된 별도의 연결을 이용하는 비지속 연결(non-persistent connection)도 지원한다.
④ HTTP 서버가 클라이언트에 대한 정보를 유지하는 상태(stateful) 프로토콜이다.

답 ④

④ HTTP와 IP 등은 대표적인 무상태 프로토콜(stateless protocol)이다.
무상태 프로토콜은 여러 개의 요청/응답을 각각의 독립적인 트랜잭션으로 취급하는 통신 프로토콜 방식이다. 서버 설계가 단순해지고 현재 상태를 보존하지 않으며, 필요한 부가 정보를 요청시마다 매번 포함해야 한다.
반대로 상태 프로토콜(stateful protocol)은 통신 상태를 계속 추적하며, 상태 정보를 저장한다. 대표적으로 TCP가 있다.

문 17. 서버가 응용 메시지를 여러 개의 TCP 세그먼트로 나누어 클라이언트에게 전송하는 경우, TCP의 동작에 대한 설명으로 옳은 것은?

① 클라이언트와 서버 간의 TCP 연결 설정 후, 첫 번째 세그먼트의 순서 번호는 일반적으로 0부터 시작한다.

② 두 번째 세그먼트의 순서 번호는 첫 번째 세그먼트가 운반에 성공한 데이터의 바이트 수를 첫 번째 세그먼트의 순서 번호에 더한 것이다.

③ 일정량의 데이터를 포함한 세그먼트를 정상적으로 수신한 클라이언트는 수신한 세그먼트의 순서 번호에 1을 더한 값을 확인응답 번호로 하여 응답하고 다음 세그먼트를 기다린다.

④ 클라이언트가 FIN 세그먼트를 보내고 서버가 이에 대한 ACK 세그먼트를 보냄으로써 서버의 데이터 전송을 위한 연결이 완전히 종료된다.

답 ②

② 순서번호는 세그먼트에 포함된 데이터의 첫 번째 바이트 번호를 의미한다. 다음 순서번호는 이전의 순서번호에 전송에 성공한 데이터 크기를 더한 값이다.

예를 들어, 현재의 세그먼트 첫 번째 바이트가 1200이고 세그먼트의 크기가 500이라면, 다음 순서번호는 1700이 된다.

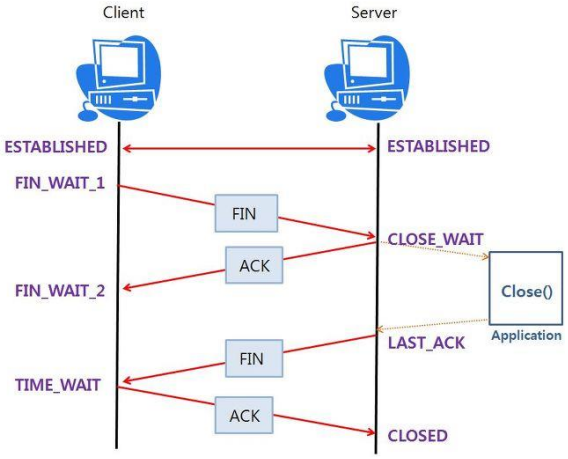
<오답 체크> ① 초기 순서번호(ISN, Initial Sequence Number)는 랜덤하게 선택된 값이다.

③ 한 번에 1바이트씩 주고 받는다면, 순서번호는 1씩 차례로 올라가지만, 일반적으로 세그먼트는 수백~수천 바이트로 이루어져 있어, 순서번호 역시 수백~수천씩 증가한다.

확인응답번호는 다음에 수신하기를 기대하는 번호이며, 크기가 100인 1200번 세그먼트(1200~1299)를 정상적으로 수신하였다면, 확인응답번호는 1300이 된다.

④ TCP 연결 종료는 FIN-ACK 패킷을 두 번씩 주고받는 4-way handshake 과정을 통해 복잡하게 진행된다.

◈ **TCP 연결 종료 과정**(4-way handshake)



1. **CLIENT ⇨ ⇨ (FIN) ⇨ ⇨ SERVER**

먼저 클라이언트는 FIN 패킷을 전송 하고 자신의 상태를 FIN_WAIT_1으로 변경한다.

2. **CLIENT ⇦ ⇦ (ACK) ⇦ ⇦ SERVER**

FIN 패킷을 받은 서버는 ACK 패킷을 클라이언트로 전송하고, 자신의 상태를 CLOSE_WAIT로 변경한다.

(이는 자신이 FIN 패킷을 잘 받았다는 의미로 응답하는 것이지, 바로 연결을 끊자는 것은 아니다.)

클라이언트로부터 종료 의사를 전달받은 서버는 서비스를 종료하기 위해 클라이언트에 연결되어 있던 어플리케이션에 close()를 요청한다.

그리고 ACK 패킷을 받은 클라이언트는 자신의 상태를 FIN_WAIT_2로 변경한다.

3. **CLIENT ⇦ ⇦ (FIN) ⇦ ⇦ SERVER**

어플리케이션이 종료된 것을 확인한 서버는 클라이언트로 FIN 패킷을 전송하고, 자신의 상태를 LAST_ACK로 변경한다.

4. **CLIENT ⇨ ⇨ (ACK) ⇨ ⇨ SERVER**

FIN 패킷을 받은 클라이언트는 ACK 패킷을 서버로 보내 응답하고, 자신의 상태를 TIME_WAIT로 변경한다. 이 상태에서 일정 시간이 지나면 CLOSED(연결 종료)가 된다.

그리고 클라이언트의 ACK 패킷을 받은 서버는 최종 의사를 확인한 것이므로 CLOSED로 연결을 종료한다.

문 18. 다음에서 설명하는 네트워크 기반 공격 방법은?

> ○ TCP 헤더 정보를 보고 패킷을 걸러내는 방화벽을 우회하기 위한 공격 방법이다.
> ○ IP 단편 옵션을 이용하여 매우 작게 패킷을 나누어서 TCP 헤더 자체가 분리되도록 만든다.
> ○ 일부 패킷 필터는 첫 번째 단편만 검사하고, 나머지 단편은 모두 통과시키기 때문에 이러한 공격 방법이 유효할 수 있다.

① Source Routing Attack
② Ping of Death
③ Trinoo
④ Tiny Fragment Attack

답 ④

◆ Tiny Fragment Attack

패킷을 작은 여러 개의 조각으로 만들어서 네트워크 침입탐지 시스템이나 패킷 필터링 장비를 우회하는 공격이다.

TCP 헤더가 2개의 패킷조각에 나뉘어 질정도로 작게 쪼개서 포트 번호가 두 번째 패킷 조각에 위치하도록 한다.

패킷 필터링 방화벽은 첫 번째 패킷 조각을 검사하여 필터링 목록에 해당하는 포트 번호를 발견할 수 없기 때문에 통과시키고, 실제 포트번호가 포함되어있는 두 번째 패킷 조각은 아예 검사도 하지 않고 통과시킨다. 그 결과 공격자가 보낸 패킷은 목적지에서 재조립되어 공격자가 원하는 공격을 수행할 수 있게 된다.

<오답 체크> ① 소스 라우팅(Source Routing)이란 패킷을 전송할 때 라우터에 의해 경로가 자동적으로 결정되는 것이 아니라, 패킷을 보내는 사람이 직접 경로를 설정하여 전송하는 기법을 의미한다.

소스 라우팅 공격은 이러한 소스 라우팅 기법을 이용하여 악의적인 공격자가 이러한 소스 라우팅 기법을 악용하여 접근이 불가능한 내부 사설망에 접근하는 프로토콜 취약점 공격이다.

② Ping of Death

icmp 패킷을 정상보다 매우 크게 만들어 공격하는 DoS 공격이다.

크게 조작된 icmp 패킷은 라우터를 통과하는 동안 매우 작은 패킷으로 조각화(fragment)되어 공격 대상에 도달하는데, 공격 대상은 조각화된 패킷을 모두 처리하느라 과부하가 걸리게 된다.

③ Trinoo(UDP Flooding)

UDP 패킷을 이용한 DoS 공격

문 19. 다음은 「정보보호산업의 진흥에 관한 법률」상 정보보호산업의 활성화를 위한 구매수요정보의 제공에 관한 조항의 일부이다. ㉠, ㉡에 들어갈 용어를 바르게 연결한 것은?

> 「전자정부법」 제2조제2호에 따른 행정기관 또는 공공기관의 장은 소관 기관·시설의 정보보호 수준을 강화하기 위하여 (㉠) 정보보호기술등에 대한 구매수요정보를 (㉡)에게 제출하여야 한다.

	㉠	㉡
①	매년	과학기술정보통신부장관
②	매년	행정안전부장관
③	2년마다	과학기술정보통신부장관
④	2년마다	행정안전부장관

답 ①

「정보보호산업의 진흥에 관한 법률」 제6조(구매수요정보의 제공)

① 「전자정부법」 제2조제2호에 따른 행정기관 또는 공공기관(이하 "공공기관등"이라 한다)의 장은 소관 기관·시설의 정보보호 수준을 강화하기 위하여 **매년** 정보보호기술등에 대한 구매수요 정보(이하 이 조에서 "구매수요정보"라 한다)를 **과학기술정보통신부장관**에게 제출하여야 한다.

② 과학기술정보통신부장관은 제1항에 따라 제출된 구매수요정보를 정보보호기업에 제공할 수 있다.

③ 과학기술정보통신부장관은 제2항에 따라 구매수요정보를 정보보호기업에 제공하는 경우 과학기술정보통신부 내에 별도의 심의위원회를 개최하여 국가안전 및 공공의 이익에 중대한 영향을 미치는 내용이 정보보호기업에 제공되지 아니하도록 하여야 한다.

④ 제1항 및 제2항에 따른 구매수요정보 제출 및 제공의 구체적인 횟수·시기·방법·절차 등에 필요한 사항은 대통령령으로 정한다.

문 20. IEEE 802.11i에서 정의한 무선 랜 데이터 보안 프로토콜로, 메시지 무결성 코드(MIC)와 RC4 암호 알고리즘을 이용하여 메시지 무결성과 데이터 기밀성을 제공하는 것은?

① EAP
② WEP
③ CCMP
④ TKIP

답 ④

▶ TKIP(Temporal Key Integrity Protocol, 임시 키 무결성 프로토콜)
데이터 필드 뒤에 MIC를 붙여 무결성을 보장하며, 데이터와 MIC를 RC4로 암호화하여 데이터 기밀성을 제공한다.
MIC(메시지 무결성 코드, Message Integrity Code)는 목적지 MAC 주소, 데이터 필드, 키 값을 입력으로 하여 생성하는 64비트 결과 값이다.

○ **WEP** 방식
암호화를 위해 RC4 사용하며(암호키 계속 사용)
암호화와 인증에 동일한 키를 사용
○ **WPA** 방식
RC4-TKIP를 통한 암호화(암호키 주기적인 변경)
EAP를 통한 사용자 인증
48비트 길이의 초기벡터(IV) 사용
○ **WPA2** 방식
AES-CCMP 사용
EAP를 통한 사용자 인증