2017 년 지방직 9 급 정보보호론 풀이

by 호이호이꿀떡

문 1. 정보시스템의 접근제어 보안 모델로 옳지 않은 것은?

① Bell LaPadula 모델
② Biba 모델
③ Clark-Wilson 모델
④ Spiral 모델

답 ④

④ 나선형(Spiral) 모델: 소프트웨어 공학론에 나오는 소프트웨어 개발 방법론의 하나로, 점진적이고 반복적인 개발 이론 모델이다.
① 벨 라파듈라(BLP) 모델: 기밀성 중심
② 비바(Biba) 모델: 무결성 중심
③ 클락 윌슨(Clark-Wilson) 모델: 무결성 중심, 상업적 모델

- 정보흐름(Information Flow) 모델
  Biba + BLP
  은닉채널이 존재하지 않도록
- 래티스(Lattice) 모델
  격자 구조, 정보흐름을 안전하게 통제
  최소상계와 최대하계를 갖는 유한적인 반순서
- 상태기계(State Machine) 모델
  시스템이 스스로를 보호하고 불안정한 상태가 되지 않도록, 상태천이(state transition)를 통해 안전한 상태를 유지
  모든 보안 모델에 기본적으로 적용
- 비간섭(Noninterference) 모델
  한 보안 수준에서 설정된 활동은 타 보안 수준에 노출되거나 영향을 미치지 않음

문 2. 정보보안에 대한 설명으로 옳은 것은?

① 보안공격 유형 중 소극적 공격은 적극적 공격보다 탐지하기 매우 쉽다.
② 공개키 암호 시스템은 암호화 키와 복호화 키가 동일하다.
③ 정보보호의 3 대 목표는 기밀성, 무결성, 접근제어이다.
④ 부인 방지는 송신자나 수신자가 메시지를 주고받은 사실을 부인하지 못하도록 방지하는 것을 의미한다.

답 ④

① 소극적 공격은 기존의 정보 흐름이나 시스템 자원에 영향을 주지 않기 때문에 공격 발생 여부를 탐지하기 어렵다.
반면에 적극적 공격은 시스템이나 데이터 전송에 직접적인 영향을 끼치기 때문에, 공격 발생 여부를 탐지하기가 어렵지 않다.
② 공개키 암호 시스템은 비대칭키 암호화 방식라고도 하며, 암호화키와 복호화키가 다르다.
메시지를 암호화할 때 공개키를 사용하고, 복호화할 때 개인키를 사용한다.
③ 정보보호의 3 대 목표는 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)이다.
그 외 인증(Authentication), 부인방지(Nonrepudiation) 등이 있다.

문 3. 비대칭키 암호화 알고리즘으로만 묶은 것은?

① RSA, ElGamal
② DES, AES
③ RC5, Skipjack
④ 3DES, ECC

답 ①

- 대칭키 암호
  DES, 3-DES, AES, RC5, Skipjack, Blowfish
  (국산 대칭키) SEED, HIGHT, ARIA
- 비대칭키 암호(공개키 암호)
  RSA : 소인수분해
  Rabin : 소인수분해
  ElGamal : 이산대수
  ECC(타원곡선) : 이산대수
  Schnorr : 이산대수, 짧은 키 길이
  DSA : 이산대수, 전자서명 전용
  ECDSA : 내부적으로 타원곡선
  Knapsack
  KCDSA : 국산, 국내표준
  ECKDSA : 국산, 내부적으로 타원곡선, 소규모, 무선

문 4. 전자우편 서비스의 보안 기술로 옳지 않은 것은?

① PGP(Pretty Good Privacy)
② S/MIME
(Secure/Multipurpose Internet Mail Extension)
③ SET(Secure Electronic Transaction)
④ PEM(Privacy Enhanced Mail)

답 ③

③ SET 는 비자와 마스터가 함께 개발한 전자 상거래 거래 프로토콜이다.
RSA 암호화 방식과 인증을 지원. 선 압축 후 전자서명
① PGP 는 인증기관을 사용하지 않고, 개개인의 신뢰 관계를 이용하여 인증하는 방식
② S/MIME : RSA 이용, 인증기관 필요
④ PEM 은 IETF 에서 만든 암호화 방식으로, 데이터를 6 비트씩 분할하여 아스키 문자로 변환하는 Base64 변환 방식을 사용한다.
자동 암호화로 전송 중 데이터가 유출되더라도 내용을 볼 수 없어, PGP 에 비해 보안성이 뛰어나다.
다만, 중앙 집중식 키 인증 방식을 사용하기 때문에 대중적으로 널리 사용되기 어렵다는 단점이 있다.

문 5. 서비스 거부(Denial of Service) 공격기법으로 옳지 않은 것은?

① Ping Flooding 공격
② Zero Day 공격
③ Teardrop 공격
④ SYN Flooding 공격

답 ②

② 제로데이(Zero Day) 공격은 운영체제나 소프트웨어의 보안 취약점에 대한 업데이트 패치가 나오기 전에, 그 취약점을 이용하여 공격하는 방법이다.

① Ping Flooding 공격은 네트워크가 정상적으로 작동하는지 여부를 확인하게 위해서 사용하는 Ping Test 를 이용한 DoS 공격이다.
공격자가 목표 시스템에 ICMP 패킷을 계속해서 보내는데, 목표 시스템은 ICMP Request 패킷을 응답하느라 시스템 자원의 고갈되어 네트워크에 오버로드가 발생하여 서비스 불능 상태에 빠지게 된다.

③ Teardrop, Bonk, Boink 공격은 신뢰성을 제공하는 프로토콜의 취약점을 이용한 DoS 공격으로, 패킷의 순서번호를 조작하는 공격이다.
목표 대상 시스템은 이렇게 보내진 패킷들을 재조합하려고 시도하지만, 계속 실패하여 시스템 자원이 고갈되어 서비스 불능 상태에 빠진다.
• Teardrop 공격은 UDP 를 이용하여 패킷의 순서번호가 서로 중복되도록 조작하는 공격
• Bonk 공격은 패킷의 순서번호를 모두 1 로 조작하여 보내는 공격
• Boink 공격은 패킷의 순서번호를 처음에는 순서대로 보내다가 중간부터 반복되는 순서번호를 보내는 공격이다.

④ SYN Flooding
TCP 3-way hancshaking 을 이용한 DoS 공격
공격 대상 서버에 무수히 많은 SYN 패킷을 보낸 뒤, 서버로부터 오는 SYN+ACK 패킷을 무시하여, 서버가 SYN Received 상태로 끊임없이 기다리게 만드는 공격방법이다.

문 6. 해시(Hash) 함수에 대한 설명으로 옳은 것으로만 묶은 것은?

ㄱ. 입력데이터의 길이가 달라도 동일한 해시함수에서 나온 해시 결과값 길이는 동일하다.
ㄴ. 일방향 함수를 사용해서 해시함수를 구성할 수 있다.
ㄷ. 최대 128 비트까지 해시함수의 입력으로 지원한다.
ㄹ. SHA-256 의 해시 결과값 길이는 512 비트이다.

① ㄱ, ㄴ ② ㄴ, ㄷ
③ ㄷ, ㄹ ④ ㄱ, ㄹ

답 ①

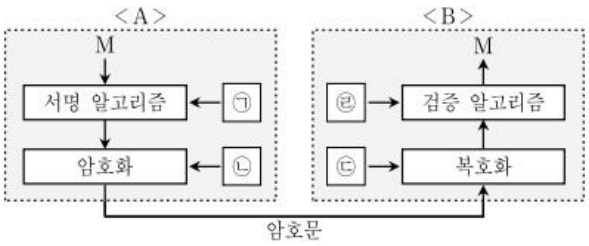
ㄱ. 대부분의 해시 함수는 가변 길이의 입력을 받아, 고정 길이의 값을 출력한다.
(해시 함수 중 HAVAL 해시 함수처럼 가변 길이 출력하는 경우도 있지만, 일반적으로 해시 함수의 특징을 얘기할 땐 고정 길이를 출력한다고 말한다.)

ㄴ. 해시 함수의 특징
• 일방향성: 역산할 수 없다. 해시값으로부터 원본 메시지를 찾을 수 없다.
• 약한 충돌내성: 주어진 해시값과 같은 해시값을 갖는 다른 메시지를 찾을 수 없다.
• 강한 충돌내성: 출력 해시값이 같은 임의의 서로 다른 두 메시지를 찾을 수 없다.

ㄷ. 해시함수 입력값의 최대 메시지 길이는 보통 $2^{64}-1$비트, $2^{128}-1$비트이다.
최대 메시지 길이가 128 비트라면 고작 16 바이트로, 텍스트 파일 하나 크기도 안 되는 크기이므로 말이 안 된다.
$2^{64}-1$: SHA-0, SHA-1, SHA-224, SSH-256, PIPEMD-160
$2^{128}-1$: SHA-384, SHA-512

ㄹ. SHA-256 의 256 은 해시값 길이 256 비트를 의미한다.
SHA-0, SHA-1: 160 비트
SHA-224: 224 비트
SHA-256: 256 비트
SHA-384: 384 비트
SHA-512: 512 비트
MD4, MD5: 128 비트
RIPEMD-128: 128 비트
RIPEMD-160: 160 비트
HAVAL: 128~256 비트의 가변 길이를 출력

문 7. A 가 B 에게 공개키 알고리즘을 사용하여 서명과 기밀성을 적용한 메시지(M)를 전송하는 그림이다. ㉠~㉣에 들어갈 용어로 옳은 것은?



㉠ ㉡ ㉢ ㉣

① A 의 공개키 B 의 공개키 A 의 개인키 B 의 개인키
② A 의 개인키 B 의 개인키 A 의 공개키 B 의 공개키
③ A 의 개인키 B 의 공개키 B 의 개인키 A 의 공개키
④ A 의 공개키 A 의 개인키 B 의 공개키 B 의 개인키

답 ③

서명은 메시지를 보내는 송신자(A)가 본인이 보냈다는 것을 확인시키기 위한 것이다. 그러므로 서명을 할 때(ㄱ)는 송신자(A)의 개인키를 사용해야 한다.
서명의 검증(ㄹ)은 송신자가 맞는지 확인하는 것이기 때문에 송신자의(A)의 공개키로 해야 한다.
암호화는 메시지를 받는 수신자(B)만 내용을 볼 수 있도록 하기 위한 것이다. 그러므로 암호를 할 땐(ㄴ) 수신자(B)의 공개키를 사용해야 한다.
메시지의 복호화(ㄷ)는 수신자만 할 수 있어야 하므로 수신자(B)의 개인키를 이용한다.

문 8. 다음에서 설명하는 패스워드 크래킹(Cracking) 공격 방법은?

> ○ 사용자가 설정하는 대부분의 패스워드에 특정 패턴이 있음을 착안한 방법으로 패스워드로 사용할 만한 것을 사전으로 만들어놓고 이를 하나씩 대입하여 일치 여부를 확인하는 방법이다.
> ○ 패스워드에 부가적인 정보(salt)를 덧붙인 후 암호화하여 저장함으로써 이 공격에 대한 내성을 향상시킬 수 있다.

① Brute Force 공격
② Rainbow Table 을 이용한 공격
③ Flooding 공격
④ Dictionary 공격

답 ④

④ 사용자가 사용하는 **패스워드에 패턴이 있는 것에 착안**하여, 미리 사용될 만한 패스워드 리스트를 사전으로 만들어 놓는다고 하였으므로, 사전 공격(Dictionary Attack)이 된다.
사람이 정해놓은 일정한 패턴의 패스워드에, 패턴이 없는 솔트(salt)를 붙이면, 패턴이 제거되는 효과가 생겨 사전 공격에 대한 내성을 높일 수 있다.

① 무차별 공격(Brute Force Attack)은 **특정 패턴을 사용하지 않고, 패스워드로 사용가능한 모든 문자열, 숫자열**을 대입해가는 공격 방법이다.
4 자리 패스워드에 대해 공격을 한다고 할 때 사람들이 의도적으로 생각해낼 수 있는 단어나 문자열 snow, bear, ABCD, 1234 등을 목록으로 만들어 대입해나가는 공격은 사전 공격이고,
qikq, md8l, zhl0 등 무작위 문자열까지 모두 대입해가며 공격하는 것은 무차별 공격이다.

② Rainbow Table 공격은 해시 함수에 대한 공격으로, 원본 문자열과 그에 대응하는 해시값을 미리 계산하여 저장해놓은 표이다. 이렇게 만들어진 Rainbow Table 은 패스워드 인증과정을 통과하거나, 해시값으로부터 원본 문자열을 찾기 위해 사용한다.
(패스워드를 데이터베이스에 저장할 땐 해시 함수로 암호화를 하여 저장하기 때문에, 실제 패스워드 문자열을 찾지 않고 그와 같은 해시값을 갖는 문자열을 찾으면 된다.)

③ Flooding 공격은, 서버에 많은 패킷을 보내 서버를 작동불능 상태에 빠뜨리게 만드는 서비스 거부 공격(DoS)이다.

문 9. 다음에서 설명하는 보안 공격 기법은?

> ○ 두 프로세스가 자원을 서로 사용하려고 하는 것을 이용한 공격이다.
> ○ 시스템 프로그램과 공격 프로그램이 서로 자원을 차지하기 위한 상태에 이르게 하여 시스템 프로그램이 갖는 권한으로 파일에 접근을 가능하게 하는 공격방법을 말한다.

① Buffer Overflow 공격
② Format String 공격
③ MITB(Man-In-The-Browser) 공격
④ Race Condition 공격

답 ④

① 버퍼 오버플로우 공격은 프로그램에 미리 할당된 버퍼보다 더 많은 양의 데이터를 집어넣어, 다른 메모리 영역을 침범하여 데이터를 변조시키는 공격이다.
② 포맷 스트링 공격은 결과를 출력하기 위하여 사용되는 printf() 함수에서 지시자를 제대로 지정하지 않아 버그를 발생시켜, 메모리의 특정 위치의 값을 다른 것으로 변경시키는 공격이다. 해커는 이렇게 포맷 스트링의 취약점을 악용해 시스템의 권한을 획득하거나 특정 동작을 수행하게 만든다.
③ MITB(Man-In-The-Browser) 공격은 웹사이트의 이용자가 브라우저를 통해 보내는 패킷을 탈취하여 변조하는 공격이다.

문 10. 다음의 내부에서 외부 네트워크 망으로 가는 방화벽 패킷 필터링 규칙에 대한 <보기>의 설명으로 옳은 것으로만 묶은 것은? (단, 방화벽을 기준으로 192.168.1.11 은 내부 네트워크에 위치한 서버 이고, 10.10.10.21 은 외부 네트워크에 위치한 서버이다)

No.	From	Service	To	Action
1	192.168.1.11	25	10.10.10.21	Allow
2	Any	21	10.10.10.21	Allow
3	Any	80	Any	Allow
4	192.168.1.11	143	10.10.10.21	Allow

< 보 기 >
ㄱ. 내부 서버(192.168.1.11)에서 외부 서버(10.10.10.21)로 가는 Telnet 패킷을 허용한다.
ㄴ. 내부 Any IP 대역에서 외부 서버(10.10.10.21)로 가는 FTP 패킷을 허용한다.
ㄷ. 내부 Any IP 대역에서 외부 Any IP 대역으로 가는 패킷 중 80번 포트를 목적지로 하는 패킷을 허용한다.
ㄹ. 내부 서버(192.168.1.11)에서 외부 서버(10.10.10.21)로 가는 POP3 패킷을 허용한다.

① ㄱ, ㄴ ② ㄴ, ㄷ
③ ㄷ, ㄹ ④ ㄱ, ㄹ

답 ②

ㄴ. **2 번** 규칙에 해당한다.
21 번 포트는 FTP 연결시 인증 제어 정보를 전송하는 포트이고, 20 번 포트는 FTP 의 실제 데이터를 전송하는 포트이다.
ㄷ. **3 번** 규칙에 해당한다.
80 번 포트는 HTTP 포트이다.
ㄱ. telnet 의 포트 번호는 23 번으로 규칙에 없다.
1 번 규칙의 25 번 포트 번호는 SMTP(간이 우편 전송 프로토콜)에서 이용한다.
ㄹ. POP3 의 포트 번호는 110 번으로 규칙에 없다.
4 번 규칙의 143 번 포트는 IMAP4 의 포트이다.

문 11. 전자서명이 제공하는 기능으로 옳지 않은 것은?

① 부인 방지(Non Repudiation)
② 변경 불가(Unalterable)
③ 서명자 인증(Authentication)
④ 재사용 가능(Reusable)

답 ④

한 문서에 대한 서명은 해당 문서에만 적용되어야 하며, 다른 문서에 재사용할 수 없어야 한다.
서명의 진짜 주인이라 할지라도 다른 문서에 서명을 할 때는 새로운 서명을 생성해야 한다.

전자서명의 특성
위조 불가(unforgeable)
서명자 인증(authentic)
부인 방지(non-repudiation)
변경 불가(unalterable)
재사용 불가(not reusable)

문 12. 위험 관리 과정에 대한 설명으로 ㉠, ㉡에 들어갈 용어로 옳은 것은?

(가) (㉠)단계는 조직의 업무와 연관된 정보, 정보시스템을 포함한 정보자산을 식별하고, 해당 자산의 보안성이 상실되었을 때의 결과가 조직에 미칠 수 있는 영향을 고려하여 가치를 평가한다.
(나) (㉡)단계는 식별된 자산, 위협 및 취약점을 기준으로 위험도를 산출하여 기존의 보호대책을 파악하고, 자산별 위협, 취약점 및 위험도를 정리하여 위험을 평가한다.

	㉠	㉡
①	자산식별 및 평가	위험 평가
②	자산식별 및 평가	취약점 분석 및 평가
③	위험 평가	가치평가 및 분석
④	가치평가 및 분석	취약점 분석 및 평가

답 ①

- 위험 분석
  위험을 분석하고 해석하는 과정으로, 자산과 취약성을 식별하고 발생 가능한 위험의 내용과 정도를 결정하는 과정, 이로 인해서 예상되는 손실을 분석하여 위험 요소를 적절하게 통제할 수 있는 수단을 구현하고 운영하는 전반적인 행위 및 절차이다.
- 위험 평가
  자산, 위협, 취약점으로부터 위험을 계산(평가)하여 발생할 수 있는 손실의 정도를 파악하여, 보안 대책에 드는 비용과 효과를 분석, 적은 비용으로 가장 효과적인 위험 관리를 수행하는 것이다.

문 13. 다음의 사이버 공격 유형과 그에 대한 <보기>의 설명을 바르게 연결한 것은?

ㄱ. 피싱(Phishing)
ㄴ. 파밍(Pharming)
ㄷ. 스미싱(Smishing)

< 보 기 >
A. 공격자가 도메인을 탈취하여 사용자가 정확한 사이트 주소를 입력해도 가짜 사이트로 연결되도록 하는 방법이다.
B. 이메일 또는 메신저를 사용해서 신뢰할 수 있는 사람 또는 기업이 보낸 메시지인 것처럼 가장하여 신용정보 등의 기밀을 부정하게 얻으려는 사회공학기법이다.
C. 문자메시지로 신뢰할 수 있는 사람이 보낸 것처럼 가장하여, 링크 접속을 유도한 뒤 개인정보를 빼내는 방법이다.

	ㄱ	ㄴ	ㄷ
①	A	B	C
②	A	C	B
③	B	A	C
④	B	C	A

답 ③

A. 정확한 주소를 입력해도 가짜 사이트로 강제 연결 -> 파밍
B. 가짜 링크를 보내 가짜 사이트로 유인 -> 피싱
C. 문자 메시지(SMS) + 피싱(Phishing) -> Smishing(스미싱)

문 14.『개인정보 보호법』상 정보주체가 자신의 개인정보 처리와 관련하여 갖는 권리로 옳지 않은 것은?

① 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리
② 개인정보의 처리 정지, 정정.삭제 및 파기를 요구할 권리
③ 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리
④ 개인정보 처리를 수반하는 정책이나 제도를 도입.변경하는 경우에 개인정보보호위원회에 개인정보 침해요인평가를 요청할 권리

답 ④

『개인정보 보호법』제 4 조(정보주체의 권리)
정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다.
1. 개인정보의 처리에 관한 정보를 제공받을 권리
2. 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리 -> ①
3. 개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람(사본의 발급을 포함한다. 이하 같다)을 요구할 권리
4. 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리 -> ②
5. 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리 -> ③

문 15. 재해복구시스템의 복구 수준별 유형에 대한 설명으로 옳은 것은?

① Warm site 는 Mirror site 에 비해 전체 데이터 복구 소요 시간이 빠르다.
② Cold site 는 Mirror site 에 비해 높은 구축 비용이 필요하다.
③ Hot site 는 Cold site 에 비해 구축 비용이 높고, 데이터의 업데이트가 많은 경우에 적합하다.
④ Mirror site 는 Cold site 에 비해 구축 비용이 저렴하고, 복구에 긴 시간이 소요된다.

답 ③

재해복구시스템(DRS, Disaster Recovery System)은 데이터센터 등 기업 IT 인프라에 장애가 발생하여 제 기능을 수행하지 못하게 됐을 때, 이를 대체하거나 복구해 제 기능을 수행할 수 있도록 기능하는 시스템을 말한다.

- Mirror Site(미러 사이트)
  원본 시스템과 동일한 데이터를 실시간으로 처리하여 **동시에 운영**되는 백업 사이트이다
- Hot Site(핫 사이트)
  원본 시스템과 동일한 장비와 데이터를 갖춘 백업 사이트지만, 평소엔 운영하지 않는다. 원본 시스템과 항상 동일한 데이터를 유지하기 때문에 백업은 실시간
- Warm Site(웜 사이트)
  핫 사이트와 콜드 사이트의 중간 단계로, 원본 시스템의 장비 일부를 백업 사이트에 설치하여 주요 업무에 대한 복구를 지원한다.
  하드웨어가 이미 연결이 되어 있으며, 직접 백업본을 갖출 수 있으나 완전하지 못할 수도 있다.
- Cold Site(콜드 사이트)
  평소에는 시스템을 사용할 수 있는 전기, 통신, 온도조절 시스템만 갖춰놓은 상태로, 재해 발생시 하드웨어와 소프트웨어를 설치하여 가동한다.
  백업 사이트 가운데 가장 값이 저렴하며, 데이터와 정보의 백업된 복사본을 거의 보유하고 있지 않다.

③ 핫 사이트는 실시간으로 백업이 이루어지기 때문에 데이터 업데이트 양이 많고 빈번한 경우에 적합
① 데이터 복구 시간은 미러 사이트가 가장 빠르다.
② 미러 사이트가 가장 많은 비용이 들고, 콜드 사이트가 가장 적은 비용이 든다.
④ 미러 사이트는 비용이 가장 많이 드는 반면, 데이터 복구에 적은 시간이 소요된다.

문 16. 무선랜의 보안 대응책으로 옳지 않은 것은?

① AP 에 접근이 가능한 기기의 MAC 주소를 등록하고, 등록된 기기의 MAC 주소만 AP 접속을 허용한다.
② AP 에 기본 계정의 패스워드를 재설정한다.
③ AP 에 대한 DHCP 를 활성화하여 AP 검색 시 SSID 가 검색 되도록 설정한다.
④ 802.1x 와 RADIUS 서버를 이용해 무선 사용자를 인증한다

답 ③

③ 자신의 기기 정보가 불필요하게 노출되지 않도록 SSID 를 변경하거나 숨기는 것이 보안에 도움이 된다.

문 17. 다음의 OSI 7 계층과 이에 대응하는 계층에서 동작하는 <보기>의 보안 프로토콜을 바르게 연결한 것은?

ㄱ. 2 계층	ㄴ. 3 계층	ㄷ. 4 계층

< 보 기 >

A. SSL/TLS B. L2TP C. IPSec

	ㄱ	ㄴ	ㄷ
①	A	B	C
②	A	C	B
③	B	C	A
④	B	A	C

답 ③

PPTP - 2 계층
L2TP - 2 계층
L2F - 2 계층
IPSec - 3 계층
SSL/TLS - 4 계층
SOCKSv5 - 5 계층
SSH(Secure Shell) - 7 계층(telnet 이나 FTP 를 암호화)

문 18.『개인정보의 기술적·관리적 보호조치 기준』상 정보통신서비스 제공자 등이 준수해야 하는 사항으로 옳지 않은 것은?

① 개인정보처리시스템에 주민번호, 계좌번호를 저장할 때 안전한 암호알고리듬으로 암호화한다.
② 개인정보처리시스템에 개인정보취급자의 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3 년간 보관한다.
③ 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취한다.
④ 이용자의 비밀번호 작성규칙은 영문, 숫자, 특수문자 중 2 종류 이상을 조합하여 최소 10 자리 이상 또는 3 종류 이상을 조합 하여 최소 8 자리 이상의 길이로 구성하도록 수립한다.

답 ②

『개인정보의 기술적·관리적 보호조치 기준』
제 4 조(접근통제)
③ 정보통신서비스 제공자등은 제 1 항 및 제 2 항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 **최소 5 년간 보관**한다.
⑧ 정보통신서비스 제공자등은 개인정보취급자를 대상으로 다음 각 호의 사항을 포함하는 비밀번호 작성규칙을 수립하고, 이를 적용·운용하여야 한다.
1. 영문, 숫자, 특수문자 중 2 종류 이상을 조합하여 최소 10 자리 이상 또는 3 종류 이상을 조합하여 최소 8 자리 이상의 길이로 구성
⑩ 정보통신서비스 제공자등은 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취하여야 한다.
제 6 조(개인정보의 암호화)
② 정보통신서비스 제공자등은 다음 각 호의 정보에 대해서는 안전한 암호알고리듬으로 암호화하여 저장한다.

『개인정보의 안전성 확보조치 기준』
제 5 조(접근 권한의 관리)
③ 개인정보처리자는 제 1 항 및 제 2 항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 **최소 3 년간 보관**하여야 한다.

※ 기술적 관리적 보호조치 기준과 안정성 확보조치 기준의 내용이 다른 걸 노려서 출제한 문제이다. 너무 자잘하다...

문 19.『정보통신망 이용촉진 및 정보보호 등에 관한 법률』상 ㉠, ㉡에 들어갈 용어로 옳은 것은?

> 제 23 조의 2(주민등록번호의 사용 제한)
> ① 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용할 수 없다.
> 1. 제 23 조의 3 에 따라 (㉠)으로 지정받은 경우
> 2. 법령에서 이용자의 주민등록번호 수집·이용을 허용 하는 경우
> 3. 영업상 목적을 위하여 이용자의 주민등록번호 수집·이용이 불가피한 정보통신서비스 제공자로서 (㉡)가 고시하는 경우

㉠	㉡
① 개인정보처리기관	개인정보보호위원회
② 개인정보처리기관	방송통신위원회
③ 본인확인기관	개인정보보호위원회
④ 본인확인기관	방송통신위원회

답 ④

『정보통신망 이용촉진 및 정보보호 등에 관한 법률』
제 23 조의 2(주민등록번호의 사용 제한)
① 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용할 수 없다.
1. 제 23 조의 3 에 따라 **본인확인기관**으로 지정받은 경우
2. 법령에서 이용자의 주민등록번호 수집·이용을 허용하는 경우
3. 영업상 목적을 위하여 이용자의 주민등록번호 수집·이용이 불가피한 정보통신서비스 제공자로서 **방송통신위원회**가 고시하는 경우

② 제 1 항제 2 호 또는 제 3 호에 따라 주민등록번호를 수집·이용할 수 있는 경우에도 이용자의 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법(이하 "대체수단"이라 한다)을 제공하여야 한다.

문 20. 다음에서 설명하는 국제공통평가기준(CC)의 구성요소는?

> ○ 정보제품이 갖추어야 할 공통적인 보안 요구사항을 모아 놓은 것이다.
> ○ 구현에 독립적인 보안 요구사항의 집합이다.

① 평가보증등급(EAL)
② 보호프로파일(PP)
③ 보안목표명세서(ST)
④ 평가대상(TOE)

답 ②

② **보호프로파일**(PP, Protection Profile)
사용자나 개발자의 보안 요구사항을 표현하기 위해 CC 를 준용하여 작성된 것으로, 보안기능을 포함한 IT 제품이 갖추어야 할 보안요구사항 집합.
제품군에 대한 보안 요구사항을 정의한 것으로, 특정 제품의 기술적인 구현에 독립적이며, 여러 제품이나 시스템이 동일한 PP 를 적용할 수 있다.

① 평가보증등급(EAL)
국제 공통평가기준(CC)에서 정의한 제품의 보증등급으로, EAL1 에서 EAL7 까지 7 단계

③ **보안목표명세서**(ST, Security Target)
개발자가 특정 IT 제품의 보안기능을 표현하기 위해 CC 를 준용하여 작성한 것으로, 제품 평가를 위한 기초자료로 사용됨
특정 제품에 대한 보안 명세를 정의한 것이기 때문에 기술적인 구현에 종속적이며, 각 제품이나 시스템은 각각의 ST 를 적용한다.
ST 는 PP 를 포함한다.

④ 평가대상(TOE(Target of Evaluation)
평가의 대상인 IT 제품이나 시스템과 이와 관련된 관리자 설명서 및 사용자 설명서