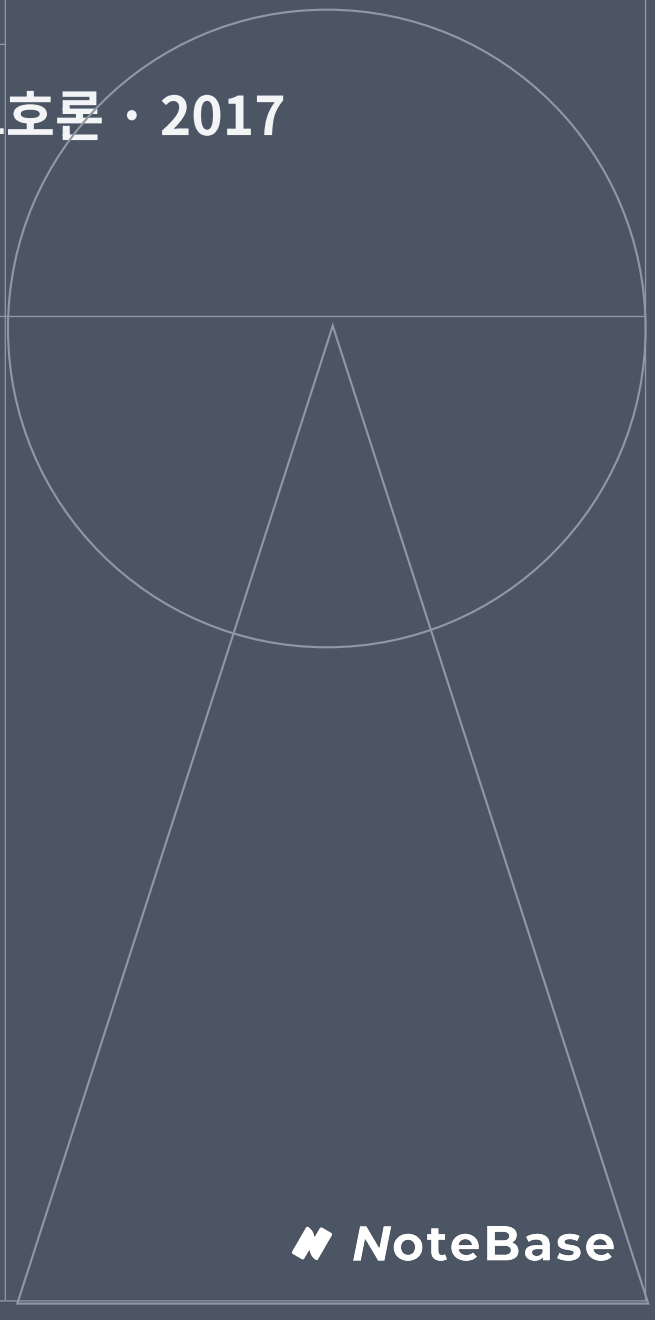
기출OX 해설집

공무원/지방직/9급 · 정보보호론 · 2017



NoteBase

기출OX 해설집

공무원/지방직/9급 · 정보보호론 · 2017

공무원/지방직/9급 · 정보보호론 · 2017

문 1. 정보시스템의 접근제어 보안 모델로 옳지 않은 것은?

① Bell LaPadula 모델

② Biba 모델

③ Clark-Wilson 모델

④ Spiral 모델

정답 4번

간단한 해설

Spiral 모델은 위험을 분석하면서 개발과 평가를 반복하는 **소프트웨어 개발 생명주기 모델**이다. 사용자나 프로그램의 데이터 접근 권한을 규정하는 접근제어 보안 모델에 해당하지 않는다.

선지별 해설

① O: Bell LaPadula 모델은 **기밀성**을 보호하는 접근제어 보안 모델이다. 주체와 객체의 보안 등급에 따라 읽기와 쓰기를 제한하여 높은 등급의 비밀정보가 낮은 등급으로 유출되는 것을 막는다.

② O: Biba 모델은 **무결성**을 보호하는 접근제어 보안 모델이다. 주체와 객체의 무결성 등급을 바탕으로 접근을 통제하여 신뢰도가 낮은 정보로 인해 신뢰도가 높은 정보가 오염되는 것을 방지한다.

③ O: Clark-Wilson 모델은 상업적 업무 환경에서 데이터의 무결성을 보호하는 보안 모델이다. 보호 대상 데이터는 **검증된 변환 절차를 통해서만 변경**하도록 하고 직무를 분리하여 부정한 변경이나 오류를 방지한다.

④ X: Spiral 모델은 **위험 분석을 중심으로 개발과 평가를 반복**하는 소프트웨어 개발 생명주기 모델이다. 주체가 객체에 어떤 연산을 수행할 수 있는지를 정하는 접근제어 보안 모델로 분류할 수 없다.

NoteBase

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 3대 목표는 기밀성, 무결성, 접근제어이다.

④ 부인 방지는 송신자나 수신자가 메시지를 주고받은 사실을 부인하지 못하도록 방지하는 것을 의미한다.

정답 4번

간단한 해설

부인 방지는 메시지를 보냈거나 받았다는 사실을 나중에 부정하지 못하도록 **송수신 사실을 입증할 증거**를 제공하는 보안 서비스이다.

선지별 해설

① X: 소극적 공격은 도청이나 트래픽 분석처럼 정보를 몰래 관찰하는 공격이다. 데이터나 시스템의 상태를 바꾸지 않아 **탐지하기 어렵다**. 적극적 공격은 메시지 변조나 서비스 방해처럼 데이터 또는 시스템 동작에 변화를 일으키므로, 소극적 공격이 적극적 공격보다 탐지하기 매우 쉽다는 설명은 잘못이다.

② X: 공개키 암호 시스템은 **서로 다른 공개키와 개인키**를 한 쌍으로 사용한다. 기밀성을 위한 암호화에서는 수신자의 공개키로 암호화하고 수신자의 개인키로 복호화한다. 암호화 키와 복호화 키가 동일한 것은 대칭키 암호 시스템의 특징이다.

③ X: 정보보호의 3대 목표는 **기밀성·무결성·가용성**이다. 기밀성은 허가받지 않은 정보 공개를 막는 것, 무결성은 허가받지 않은 변경이나 훼손을 막는 것, 가용성은 권한 있는 사용자가 필요할 때 정보와 서비스를 이용할 수 있게 하는 것이다. 접근제어는 주체의 자원 접근을 권한에 따라 허용하거나 제한하는 수단이며, 선지의 접근제어는 가용성으로 고쳐야 한다.

④ O: 부인 방지는 메시지의 송신이나 수신 사실을 입증할 증거를 제공하여 **통신 당사자가 그 사실을 나중에 부인하지 못하게 하는 것**이다. 송신자가 메시지를 보냈다는 사실을 부인하지 못하게 하는 송신 부인 방지와, 수신자가 메시지를 받았다는 사실을 부인하지 못하게 하는 수신 부인 방지가 있다.

NoteBase

문 3. 비대칭키 암호화 알고리즘으로만 묶은 것은?

① RSA, ElGamal

② DES, AES

③ RC5, Skipjack

④ 3DES, ECC

정답 1번

간단한 해설

RSA와 ElGamal은 모두 **공개키와 개인키를 구분하여 사용하는 비대칭키 암호**이다. 암호화에 사용하는 키와 복호화에 사용하는 키가 서로 다르다.

공통 해설

비대칭키 암호는 수학적으로 관련된 공개키와 개인키를 한 쌍으로 사용한다. 메시지를 보낼 때 수신자의 공개키로 암호화하면, 수신자는 자신의 개인키로 복호화한다. 이에 비해 대칭키 암호는 송신자와 수신자가 **같은 비밀키를 공유**하여 암호화와 복호화에 사용한다.

제시된 알고리즘 중 RSA·ElGamal·ECC는 비대칭키 암호에 속하고, DES·AES·RC5·Skipjack·3DES는 대칭키 암호에 속한다. 따라서 RSA와 ElGamal의 묶음은 두 알고리즘이 모두 비대칭키 암호라는 조건을 충족한다.

DES와 AES, RC5와 Skipjack은 각각 대칭키 암호끼리 묶여 있다. 3DES와 ECC의 묶음은 ECC가 비대칭키 암호이지만 **3DES가 대칭키 암호**이므로, 비대칭키 암호로만 이루어진 묶음이 아니다.

NoteBase

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)

정답 3번

간단한 해설

SET는 전자우편이 아니라 **전자상거래의 신용카드 결제**를 보호하는 보안 프로토콜이다. 전자우편 메시지의 보안에는 PGP, S/MIME, PEM이 사용된다.

공통 해설

전자우편 보안 기술은 송신자와 수신자 사이에 전달되는 메일 메시지를 보호한다. 암호화는 허가받지 않은 사람이 내용을 읽지 못하게 하는 기밀성을 제공하고, 전자서명은 발신자를 확인하고 메시지의 위변조를 탐지하는 데 쓰인다. **PGP·S/MIME·PEM**은 이러한 암호화와 인증 기능을 전자우편에 적용하는 기술이므로 전자우편 보안 기술에 해당한다.

SET는 **인터넷 신용카드 결제 거래**를 보호하는 프로토콜이다. 카드 소지자·판매자·금융기관 등 결제 참여자를 인증하고 결제 정보의 기밀성과 무결성을 보호한다. 보호 대상이 메일 메시지가 아니라 카드 결제 거래이므로 전자우편 보안 기술로 분류하지 않는다.

NoteBase

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

정답 2번

간단한 해설

Zero Day 공격은 **아직 알려지지 않았거나 패치가 제공되지 않은 취약점**을 악용하는 공격이다. 취약점의 발견·대응 상태에 따른 명칭이므로, 서비스 거부를 일으키는 특정 공격기법을 뜻하지 않는다.

선지별 해설

서비스 거부(DoS) 공격은 시스템이나 네트워크의 자원을 소모시키거나 오류를 일으켜 정상적인 이용자의 서비스 이용을 방해한다. 핵심은 서비스의 가용성을 해치는 것이다.

① O: Ping Flooding 공격은 ICMP Echo Request, 즉 ping 요청을 대량으로 보내는 공격이다. 요청과 응답에 따른 트래픽 및 처리 부담으로 **네트워크 대역폭이나 시스템 자원을 소모**시켜 정상적인 통신을 방해한다.

② X: Zero Day 공격은 아직 알려지지 않았거나 보안 패치가 제공되지 않은 취약점을 악용하는 공격이다. 이는 **취약점의 발견·대응 상태에 따른 분류**이며, DoS를 목적으로 하는 특정 기법의 명칭이 아니다. 제로데이 취약점으로 서비스 거부를 일으킬 수도 있지만, 정보 탈취나 악성코드 실행 등 다른 목적으로도 악용할 수 있다.

③ O: Teardrop 공격은 **데이터 영역이 겹치도록 조작한 IP 단편**을 보내 재조립 과정의 취약점을 공격한다. 이를 제대로 처리하지 못하는 시스템에 오류나 중단을 일으켜 정상적인 서비스를 제공하지 못하게 한다.

④ O: SYN Flooding 공격은 TCP 연결 요청인 SYN을 대량으로 보내고 연결 수립에 필요한 마지막 ACK를 보내지 않는 방식으로 **미완료 연결을 누적**시킨다. 서버가 SYN-ACK를 보낸 뒤 ACK를 기다리는 동안 연결 관리 자원이 점유되므로, 정상 이용자의 새 연결을 처리하기 어려워진다.

NoteBase

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 128비트까지 해시함수의 입력으로 지원한다.
ㄹ. SHA-256의 해시 결과값 길이는 512비트이다.

① ㄱ, ㄴ
② ㄴ, ㄷ
③ ㄷ, ㄹ
④ ㄱ, ㄹ

정답 1번

간단한 해설

해시함수는 입력 데이터의 길이가 달라도 **일정한 길이의 해시값**을 만든다. 암호학적 해시함수는 입력에서 해시값을 계산하기는 쉽지만, 해시값으로부터 대응하는 입력을 찾기는 어려운 **일방향성**을 갖도록 구성할 수 있다.

보기별 해설

ㄱ. O: 같은 해시함수의 **출력 길이는 입력 길이와 관계없이 일정**하다. 예를 들어 SHA-256은 짧은 문자열을 입력하든 긴 파일을 입력하든 256비트 해시값을 출력한다.

ㄴ. O: 일방향 함수는 입력에서 출력을 계산하기는 쉽지만, 출력으로부터 그에 대응하는 입력을 찾기는 계산상 어려운 함수이다. 이러한 **일방향성을 이용하여 암호학적 해시함수를 구성**할 수 있다.

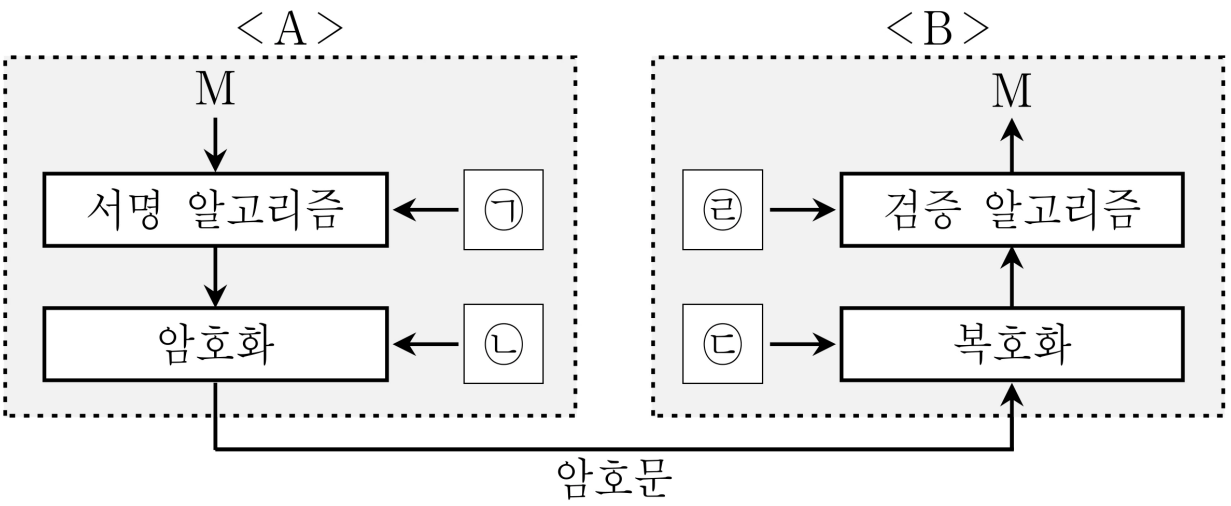
ㄷ. X: 해시함수의 최대 입력 길이가 모두 128비트로 제한되는 것은 아니다. **128비트보다 긴 데이터도 입력**할 수 있으며, 구체적인 입력 길이의 허용 범위는 알고리즘에 따라 다르다. 입력 길이와 일정하게 정해지는 출력 길이를 구별해야 한다.

ㄹ. X: SHA-256의 해시 결과값 길이는 512비트가 아니라 **256비트**이다. SHA-512의 해시 결과값 길이가 512비트이다.

옳은 보기인 ㄱ, ㄴ을 묶은 것은 ①이다.

NoteBase

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



① ㉠: A의 공개키 ㉡: B의 공개키 ㉢: A의 개인키 ㉣: B의 개인키

② ㉠: A의 개인키 ㉡: B의 개인키 ㉢: A의 공개키 ㉣: B의 공개키

③ ㉠: A의 개인키 ㉡: B의 공개키 ㉢: B의 개인키 ㉣: A의 공개키

④ ㉠: A의 공개키 ㉡: A의 개인키 ㉢: B의 공개키 ㉣: B의 개인키

정답 3번

간단한 해설

서명은 **송신자 A의 개인키**로 생성하고 A의 공개키로 검증한다. 기밀성을 위해서는 **수신자 B의 공개키**로 암호화하여 B만 자신의 개인키로 복호화할 수 있게 한다.

NoteBase

빈칸별 해설

㉠ A의 개인키: 그림에서 A가 메시지 M에 서명하는 단계에 입력되는 키이다. 전자서명은 **서명자만 보유하는 개인키**로 생성하고, 대응하는 공개키로 검증한다. 따라서 서명자인 A의 개인키를 사용한다.

㉡ B의 공개키: A가 서명한 결과를 암호화하는 단계에 입력되는 키이다. 기밀성은 전송 내용을 허가받지 않은 사람이 읽지 못하게 하는 성질이다. **수신자 B의 공개키로 암호화**하면 대응하는 개인키를 보유한 B가 복호화할 수 있으므로, 암호화에 사용하는 키는 B의 공개키이다.

㉢ B의 개인키: B가 수신한 암호문을 복호화하는 단계에 입력되는 키이다. A가 B의 공개키로 암호화했으므로, 그와 **짝을 이루는 B의 개인키**로 암호화를 해제한다. 그림에서는 복호화 결과가 서명 검증 단계로 전달된다.

㉣ A의 공개키: B가 A의 서명을 검증하는 단계에 입력되는 키이다. 서명 생성에 A의 개인키를 사용했으므로, 검증에는 **서명자 A의 공개키**를 사용한다. 이를 통해 메시지가 A의 서명에 대응하는지와 서명 후 내용이 변조되지 않았는지를 확인한다.

따라서 ㉠은 A의 개인키, ㉡은 B의 공개키, ㉢은 B의 개인키, ㉣은 A의 공개키이며, 이 대응은 ③의 구성과 일치한다.

NoteBase

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 Table을 이용한 공격
③ Flooding 공격
④ Dictionary 공격

정답 4번

간단한 해설

사람이 패스워드로 사용할 법한 단어와 패턴을 **후보 사전으로 만들어 하나씩 대입**하는 방식은 Dictionary 공격이다. 가능한 문자열을 무조건 모두 시도하는 것이 아니라, 사용 가능성이 높은 후보에 집중한다.

공통 해설

Dictionary 공격은 사용자가 선택할 가능성이 높은 단어와 그 변형을 모은 사전에서 패스워드 후보를 꺼내 일치 여부를 확인하는 방법이다. 지문의 '패스워드로 사용할 만한 것을 사전으로 만들어놓고 이를 하나씩 대입'한다는 설명이 이 정의에 해당한다. 핵심은 **후보를 사용 가능성이 높은 단어와 패턴으로 좁힌다**는 점이며, 모든 문자열 조합을 빠짐없이 시도하거나 미리 계산한 해시표를 조회한다는 뜻은 아니다.

지문의 salt는 패스워드를 해시할 때 함께 넣는 부가적인 값이다. 사용자마다 서로 다른 salt를 사용하면 같은 패스워드도 서로 다른 해시값으로 저장되므로, 공격자는 후보의 해시값을 한 번 계산해 여러 계정에 재사용하기 어렵다. 따라서 사전에 계산해 둔 해시값을 이용하는 공격의 효율을 떨어뜨린다. 다만 salt를 알아낸 공격자가 각 후보에 해당 salt를 붙여 해시값을 계산하고 비교할 수 있으므로, **salt가 사전 대입 자체를 막는 것은 아니다**.

NoteBase

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

정답 4번

간단한 해설

두 프로세스의 **자원 접근 순서와 시점**에 따라 결과가 달라지는 경쟁 상태를 악용하는 기법이 Race Condition 공격이다. 공격 프로그램이 적절한 순간에 파일의 상태나 연결 대상을 바꾸면 시스템 프로그램의 권한으로 파일에 접근하게 할 수 있다.

공통 해설

Race Condition(경쟁 상태)은 여러 프로세스나 스레드가 공유 자원에 접근할 때, 동기화가 제대로 이루어지지 않아 **실행 순서나 시점에 따라 결과가 달라지는 상태**이다. 이 틈을 악용하는 것이 Race Condition 공격이다. 지문의 두 프로세스가 자원을 서로 사용하려 한다는 설명과 시스템 프로그램의 권한으로 파일에 접근한다는 설명은 이러한 경쟁 상태를 이용한 공격을 가리킨다.

대표적인 예는 파일의 접근 권한을 검사한 뒤 실제로 파일을 열기까지의 시간 차이를 악용하는 TOCTOU(Time-of-check Time-of-use) 공격이다. 시스템 프로그램이 사용자가 접근할 수 있는 파일인지 확인한 직후, 공격 프로그램이 해당 경로를 다른 보호된 파일을 가리키는 심볼릭 링크로 바꾸면 시스템 프로그램은 자신의 권한으로 그 보호된 파일을 열 수 있다. 핵심은 **검사한 파일과 실제 사용하는 파일이 달라질 수 있다는 점**이다.

NoteBase

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

<보기>

ㄱ. 내부 서버(192.168.1.11)에서 외부 서버(10.10.10.21)로 가는 Telnet 패킷을 허용한다.

ㄴ. 내부 Any IP대역에서 외부 서버(10.10.10.21)로 가는 FTP 패킷을 허용한다.

ㄷ. 내부 Any IP대역에서 외부 Any IP대역으로 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

정답 2번

간단한 해설

2번 규칙은 출발지 제한 없이 외부 서버 10.10.10.21의 **FTP 제어 포트인 21번**으로 가는 패킷을 허용한다. 3번 규칙은 출발지와 목적지 IP에 제한 없이 **목적지 포트가 80번**인 패킷을 허용한다.

NoteBase

보기별 해설

표의 From은 출발지 IP, To는 목적지 IP, Service는 목적지 서비스 포트, Action은 처리 동작을 나타낸다. 'Any'는 해당 IP 조건에 제한이 없다는 뜻이고, 'Allow'는 규칙의 조건을 만족하는 패킷을 허용한다는 뜻이다. 이 문제에서는 내부에서 외부로 나가는 패킷에 각 규칙을 적용한다.

ㄱ. X: 1번 규칙은 192.168.1.11에서 10.10.10.21로 가는 패킷 중 목적지 포트가 25번인 패킷을 허용한다. **25번은 SMTP**에 사용하는 포트이며, Telnet의 기본 포트는 23번이다. 따라서 이 규칙은 Telnet이 아니라 SMTP 패킷의 허용을 나타낸다.

ㄴ. O: 2번 규칙은 From이 Any이고 To가 10.10.10.21이며 Service가 21번이다. 따라서 내부의 어느 IP에서든 외부 서버 10.10.10.21의 **FTP 제어 포트인 21번**으로 가는 패킷을 허용한다.

ㄷ. O: 3번 규칙은 From과 To가 모두 Any이고 Service가 80번이다. 따라서 내부 출발지 IP와 외부 목적지 IP에 관계없이 **목적지 포트가 80번인 패킷**을 허용한다. 80번은 HTTP의 기본 포트이다.

ㄹ. X: 4번 규칙은 192.168.1.11에서 10.10.10.21로 가는 패킷 중 목적지 포트가 143번인 패킷을 허용한다. **143번은 IMAP**에 사용하는 포트이며, POP3의 기본 포트는 110번이다. 따라서 이 규칙은 POP3가 아니라 IMAP 패킷의 허용을 나타낸다.

옳은 보기는 ㄴ, ㄷ이며, 이를 묶은 선택지는 ②이다.

NoteBase

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)

정답 4번

간단한 해설

전자서명은 서명한 문서의 내용에 결합되므로, 기존 서명값을 **내용이 다른 문서에 재사용할 수 없다**. 다른 내용의 문서에는 그 문서에 대한 서명을 새로 생성해야 한다.

선지별 해설

① O: 부인 방지는 서명자가 나중에 자신이 서명했다는 사실을 부정하기 어렵게 하는 기능이다. 서명자의 개인키가 안전하게 관리되고 공개키와 신원의 연결이 신뢰되는 경우, 검증 가능한 서명은 **서명 사실을 제삼자에게 입증하는 근거**가 된다.

② O: 변경 불가는 서명된 문서가 변경되지 않았음을 확인하는 무결성 기능을 뜻한다. 문서 내용이 변조되면 기존 서명으로 검증되지 않으므로 변조를 탐지할 수 있다. 파일의 수정을 물리적으로 막는다는 뜻이 아니라, **변경된 내용을 원래 서명된 내용으로 인정하지 않는 것**이다.

③ O: 서명은 서명자의 개인키로 생성하고 그에 대응하는 공개키로 검증한다. 공개키가 누구의 것인지 신뢰할 수 있게 확인되어 있다면, 서명 검증을 통해 **해당 서명자의 개인키로 서명되었음**을 확인할 수 있다. 이것이 서명자 인증 기능이다.

④ X: 전자서명은 특정 문서의 내용에 결합되므로, 한 문서의 서명값을 **내용이 다른 문서의 유효한 서명으로 재사용할 수 없다**. 예를 들어 계약 금액이 바뀐 문서에 기존 서명값만 붙이면 검증에 실패하므로 새로 서명해야 한다. 여기서 재사용 불가는 서명값에 관한 것으로, 동일한 개인키로 여러 문서에 각각 서명할 수 있다는 것과 구별해야 한다.

NoteBase

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

정답 1번

간단한 해설

정보자산을 찾아 보안성 상실이 조직에 미치는 영향에 따라 가치를 매기는 것은 **자산식별 및 평가**이다. 식별된 자산·위협·취약점을 종합하여 위험도를 산출하고 평가하는 것은 **위험 평가**이다.

빈칸별 해설

㉠ 자산식별 및 평가: (가)는 먼저 조직의 업무와 관련된 정보와 정보시스템 등 **정보자산을 식별**하고, 그 자산의 보안성이 상실될 때 조직에 미칠 영향을 바탕으로 가치를 평가하는 단계이다. 가치평가뿐 아니라 평가할 자산을 찾아내는 활동까지 포함하므로 '자산식별 및 평가'에 해당한다. 위협·취약점을 종합하여 위험도를 산출하는 위험 평가와는 구별된다.

㉡ 위험 평가: (나)는 이미 식별된 자산·위협·취약점을 기준으로 **위험도를 산출**하고, 기존 보호대책을 파악하며 자산별 위험을 평가하는 단계이다. 취약점 분석 및 평가는 위협에 악용될 수 있는 자산의 약점을 찾아 평가하는 데 초점을 둔다. (나)는 취약점뿐 아니라 자산과 위협까지 함께 고려하여 위험도를 판단하므로 '위험 평가'에 해당한다.

㉠은 자산식별 및 평가, ㉡은 위험 평가이므로 ①의 조합에 해당한다.

NoteBase

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

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

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

정답 3번

간단한 해설

신뢰할 수 있는 발신자를 사칭한 메시지로 기밀을 얻으려는 것은 **피싱**이다. **파밍**은 사용자가 사이트 주소를 정확히 입력해도 가짜 사이트로 연결되게 한다.

대응 관계 해설

ㄱ. 피싱(Phishing) → B: 이메일이나 메신저에서 믿을 만한 사람·기업을 사칭하여 신용정보 등의 기밀을 얻으려는 사회공학기법이다. B는 **발신자를 사칭한 메시지로 사용자를 속이는** 방식을 설명하므로 피싱에 대응한다.

ㄴ. 파밍(Pharming) → A: 도메인 탈취 등으로 사용자의 접속을 가짜 사이트로 돌리는 공격이다. A의 핵심은 **정확한 주소를 입력해도 가짜 사이트로 연결**된다는 점이다. 사용자를 속여 링크를 누르게 하는 메시지보다 사이트 접속 경로의 조작에 초점이 있다.

ㄷ. 스미싱(Smishing) → C: **문자메시지를 이용한 피싱**이다. C는 신뢰할 수 있는 사람이 보낸 것처럼 꾸민 문자메시지로 링크 접속을 유도하고 개인정보를 빼내므로 스미싱에 대응한다.

연결은 ㄱ: B, ㄴ: A, ㄷ: C로, ③의 조합과 일치한다.

NoteBase

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

정답 4번

간단한 해설

개인정보 침해요인 평가 요청은 정보주체의 권리가 아니라 **중앙행정기관의 장의 의무**이다. 소관 법령의 제정·개정을 통해 개인정보 처리를 수반하는 정책이나 제도를 도입·변경하는 경우 개인정보보호위원회에 평가를 요청하여야 한다.

선지별 해설

① O: 「개인정보 보호법」 제4조제2호는 정보주체가 개인정보 처리에 관한 **동의 여부와 동의 범위를 스스로 선택·결정할 권리**를 규정한다. 자신의 개인정보 처리에 동의할지, 어느 범위까지 동의할지를 결정하는 권리이다.

② O: 같은 법 제4조제4호는 개인정보의 **처리 정지, 정정·삭제 및 파기를 요구할 권리**를 규정한다. 개인정보 처리를 중단하도록 요구하거나 잘못된 정보를 바로잡고 정보를 삭제·파기하도록 요구하는 권리가 이에 해당한다.

③ O: 같은 법 제4조제5호는 개인정보 처리로 발생한 피해를 **신속하고 공정한 절차에 따라 구제받을 권리**를 규정한다. 개인정보 처리를 통제하는 권리뿐 아니라, 그 처리로 피해가 생겼을 때 구제받는 권리도 정보주체의 권리에 포함된다.

④ X: 같은 법 제8조의2제1항에 따른 개인정보 침해요인 평가 요청 주체는 **정보주체가 아니라 중앙행정기관의 장**이다. 중앙행정기관의 장은 소관 법령의 제정 또는 개정을 통하여 개인정보 처리를 수반하는 정책이나 제도를 도입·변경하는 경우 개인정보보호위원회에 평가를 요청하여야 한다. 이는 법령에 담긴 개인정보 침해요인을 검토하기 위한 절차로, 개인이 자신의 개인정보 처리에 관하여 행사하는 권리가 아니라 해당 기관장의 의무이다.

NoteBase

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

① Warm site는 Mirror site에 비해 전체 데이터 복구 소요 시간이 빠르다.

② Cold site는 Mirror site에 비해 높은 구축 비용이 필요하다.

③ Hot site는 Cold site에 비해 구축 비용이 높고, 데이터의 업데이트가 많은 경우에 적합하다.

④ Mirror site는 Cold site에 비해 구축 비용이 저렴하고, 복구에 긴 시간이 소요된다.

정답 3번

간단한 해설

Hot site는 복구용 장비를 미리 갖추고 **데이터를 최신 상태로 유지**하므로, 데이터 갱신이 잦은 시스템에 적합하다. 최소한의 자원만 확보하는 Cold site보다 구축 비용은 높다.

선지별 해설

① X: Warm site는 중요한 장비만 부분적으로 갖추고 데이터를 주기적으로 백업하므로, 전체 복구에는 장비 보완과 데이터 복원 등이 필요하다. 주센터와 같은 수준의 자원을 갖추어 실시간으로 동시 서비스를 제공하는 Mirror site보다 **전체 데이터 복구 소요 시간이 길다**.

② X: Cold site는 백업 데이터를 원격지에 보관하고 서비스용 장비는 재해 후에 조달하는 등, 사전에 확보하는 자원을 최소화한다. 따라서 주센터와 같은 수준의 시스템을 미리 구축하는 Mirror site보다 **구축 비용이 낮다**.

③ O: Hot site는 주센터와 같은 수준의 정보기술자원을 **대기 상태로 갖추고 데이터를 최신 상태로 유지**하다가, 재해가 발생하면 가동 상태로 전환한다. 장비를 최소한으로 확보하는 Cold site보다 구축 비용이 높다. 평소에는 주센터가 서비스를 담당하고 복구센터는 데이터 변경을 반영하며 대기하므로, 데이터베이스처럼 업데이트가 잦은 시스템에 적합하다.

④ X: Mirror site는 주센터와 같은 수준의 시스템을 구축하여 두 센터가 실시간으로 동시에 서비스를 제공한다. 따라서 Cold site보다 **구축 비용은 높고 복구 소요 시간은 짧다**. 비용이 저렴하지만 재해 후 장비 조달과 데이터 복원에 긴 시간이 걸리는 유형은 Cold site이다.

NoteBase

문 16. 무선랜의 보안 대응책으로 옳지 않은 것은?

① AP에 접근이 가능한 기기의 MAC 주소를 등록하고, 등록된 기기의 MAC 주소만 AP 접속을 허용한다.

② AP에 기본 계정의 패스워드를 재설정한다.

③ AP에 대한 DHCP를 활성화하여 AP 검색 시 SSID가 검색되도록 설정한다.

④ 802.1x와 RADIUS 서버를 이용해 무선 사용자를 인증한다.

정답 3번

간단한 해설

DHCP는 **IP 주소 등 네트워크 설정을 자동으로 할당**하는 기능이며, SSID를 검색되게 하는 기능이 아니다. SSID 공개 설정은 DHCP와 별개이고, 이를 공개하는 것 자체가 사용자 인증이나 암호화를 제공하지는 않는다.

선지별 해설

① O: AP는 무선 기기가 유선 네트워크 등에 접속하도록 연결하는 장치이다. 접속을 허용할 기기의 MAC 주소를 목록에 등록하고 그 주소만 허용하는 것은 **MAC 주소 기반 접근 제어**이다. 다만 MAC 주소는 위조될 수 있으므로, 이 방식만으로 강한 보안을 보장하지는 못한다.

② O: AP의 기본 계정 패스워드를 그대로 사용하면 이를 알고 있거나 쉽게 추측한 사람이 관리 기능에 접근하여 설정을 변경할 수 있다. 기본 패스워드를 **추측하기 어려운 새 패스워드로 변경**하면 이러한 무단 관리 접속의 위험을 줄일 수 있다.

③ X: DHCP는 단말에 IP 주소, 서브넷 마스크, 기본 게이트웨이 등의 네트워크 설정을 자동으로 제공하는 프로토콜이다. 무선랜을 식별하는 이름인 SSID의 공개 여부는 **DHCP가 아니라 AP의 SSID 브로드캐스트 설정**과 관련된다. 따라서 DHCP를 활성화하여 SSID가 검색되게 한다는 설명은 두 기능을 혼동한 것이다. DHCP 활성화나 SSID 공개 자체는 사용자 인증·암호화 수단이 아니며, 무선랜 보안을 위해서는 적절한 사용자 인증과 무선 구간 암호화를 적용해야 한다.

④ O: IEEE 802.1X는 네트워크 접속 전에 인증을 수행하는 포트 기반 접근 제어 방식이다. AP가 무선 단말과 인증 서버 사이의 인증 메시지를 중계하고, RADIUS 서버가 사용자 자격 증명 등을 확인하여 인증 결과를 반환하도록 구성할 수 있다. 이를 통해 **인증된 사용자에게 네트워크 접근을 허용**할 수 있다.

NoteBase

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

ㄱ. 2계층 ㄴ. 3계층 ㄷ. 4계층
<보기>
A. SSL/TLS B. L2TP C. IPSec

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

정답 3번

간단한 해설

L2TP는 **2계층 프레임**을 터널링하고, IPSec은 **3계층 IP 패킷**을 보호한다. 터널링 대상인 프레임과 보안 기능을 적용하는 IP 패킷을 구분하면 두 프로토콜의 계층을 연결할 수 있다.

대응 관계 해설

ㄱ. 2계층 — B. L2TP: OSI 2계층은 데이터링크계층이다. L2TP는 PPP 프레임을 캡슐화하여 다른 네트워크를 통해 전달하는 터널링 프로토콜이므로 **2계층 프레임의 터널링**에 대응한다. 터널링 자체가 데이터 암호화를 뜻하는 것은 아니며, 암호화 등 보안 기능은 IPSec과 결합하여 제공할 수 있다.

ㄴ. 3계층 — C. IPSec: OSI 3계층은 IP가 동작하는 네트워크계층이다. IPSec은 **IP 계층에서 패킷을 보호**하는 보안 프로토콜 체계로, 적용하는 프로토콜과 설정에 따라 인증·무결성·기밀성 등의 서비스를 제공한다. 따라서 IP 패킷을 보호하는 IPSec을 3계층에 연결한다.

ㄷ. 4계층 — A. SSL/TLS: OSI 4계층은 전송계층이다. SSL/TLS는 통신하는 응용 프로그램 사이의 데이터에 기밀성과 무결성 등을 제공하며, 이 문항에서는 **전송계층 보안 프로토콜**로 분류하여 4계층에 대응시킨다. 실제 프로토콜 구조에서는 TCP 같은 신뢰성 있는 전송 프로토콜 위에서 동작하여 응용 데이터를 보호한다.

따라서 대응은 ㄱ–B, ㄴ–C, ㄷ–A이며, 이 연결을 제시한 선택지는 ③이다.

NoteBase

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 3년간 보관한다.

③ 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취한다.

④ 이용자의 비밀번호 작성규칙은 영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성하도록 수립한다.

정답 2번

간단한 해설

권한 부여·변경·말소 내역의 보관기간은 **최소 5년**이다. ②의 '최소 3년'은 2017년 당시 「개인정보의 기술적·관리적 보호조치 기준」에서 정한 기간보다 짧다.

선지별 해설

① O: 당시 고시 제6조제2항제1호·제6호는 주민등록번호와 계좌번호를 **안전한 암호알고리듬으로 암호화하여 저장**하도록 정한다. 따라서 개인정보처리시스템에 두 정보를 저장할 때에는 암호화해야 한다.

② X: 제4조제3항에 따라 개인정보취급자의 권한 부여·변경·말소 내역을 기록하고 **최소 5년간 보관**해야 한다. 선지의 '최소 3년'을 '최소 5년'으로 고친다. 이는 누가 어떤 접근권한을 받았고 그 권한이 어떻게 바뀌었는지 확인하기 위한 이력이다.

③ O: 제4조제10항은 개인정보취급자의 접속이 **필요한 시간 동안만 유지**되도록 최대 접속시간 제한 등의 조치를 요구한다. 업무를 하지 않는데도 연결이 계속 유지되어 권한 없는 사람이 시스템을 이용하는 위험을 줄이기 위한 조치이다.

④ O: 제4조제7항은 이용자가 안전한 비밀번호를 사용하도록 작성규칙을 수립·이행하게 한다. 영문·숫자·특수문자 중 **2종류 이상이면 10자리 이상, 3종류 이상이면 8자리 이상**으로 구성하는 것은 안전한 비밀번호 작성 방식이다. 다만 당시 고시에서 이 수치를 직접 명시한 제4조제8항제1호의 대상은 개인정보취급자이다. 이용자에 관한 선지는 이러한 길이·조합 조건을 이용자의 작성규칙에도 적용하는 내용으로 이해한다.

NoteBase

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

제23조의2(주민등록번호의 사용 제한)
① 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용할 수 없다.
1. 제23조의3에 따라 (㉠)으로 지정받은 경우
2. 법령에서 이용자의 주민등록번호 수집·이용을 허용하는 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

정답 4번

간단한 해설

제시된 조문에서 주민등록번호 수집·이용의 예외가 되는 지정기관은 **본인확인기관**이다. 영업상 수집·이용이 불가피한 정보통신서비스 제공자를 고시하는 주체는 **방송통신위원회**이다.

빈칸별 해설

㉠ 본인확인기관: 제시된 구 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조의2제1항제1호는 제23조의3에 따라 본인확인기관으로 지정받은 경우를 주민등록번호 수집·이용 금지의 예외로 둔다. 제23조의3제1항의 본인확인기관은 주민등록번호를 사용하지 않고 본인을 확인하는 대체수단의 개발·제공·관리 업무를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되어 지정된 기관이다. 단순히 개인정보를 처리하는 기관이라는 사정이 아니라 **본인확인기관으로 지정받았는지**가 이 예외의 요건이다.

㉡ 방송통신위원회: 제시된 제23조의2제1항제3호에서 영업상 주민등록번호 수집·이용이 불가피한 정보통신서비스 제공자를 고시하는 주체는 방송통신위원회이다. 사업자가 영업상 필요하다고 판단하는 것만으로는 부족하고, **방송통신위원회가 고시하는 경우**에 해당해야 이 예외를 적용할 수 있다. 이 조문의 고시 주체를 개인정보보호위원회로 바꾸어서는 안 된다.

따라서 ㉠은 본인확인기관, ㉡은 방송통신위원회이며, 이 조합은 ④와 일치한다.

NoteBase

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)

정답 2번

간단한 해설

보호프로파일(PP)은 특정 제품의 구현 방식에 의존하지 않고, 같은 종류의 정보제품에 공통으로 필요한 보안 요구사항을 정리한 문서이다. 지문의 '공통적인 보안 요구사항'과 '구현에 독립적'이라는 설명이 이에 해당한다.

공통 해설

보호프로파일(PP)은 한 제품군이 공통으로 충족해야 할 보안 요구사항을 **구현에 독립적으로** 기술한 문서이다. 구현에 독립적이라는 것은 특정 제조사의 제품 구조나 구현 방법을 전제로 하지 않고, 해당 제품군에 어떤 보안이 필요한지를 규정한다는 뜻이다. 따라서 같은 종류의 여러 제품에 공통으로 적용할 수 있는 보안 요구사항의 기준이 된다.

지문의 두 설명은 이러한 보호프로파일의 정의에 해당한다. 특히 특정 평가대상의 구현을 전제로 보안 요구사항을 기술하는 보안목표명세서(ST)와 달리, 보호프로파일은 제품군 수준의 공통 요구사항을 다룬다는 점이 구별 기준이다.

NoteBase