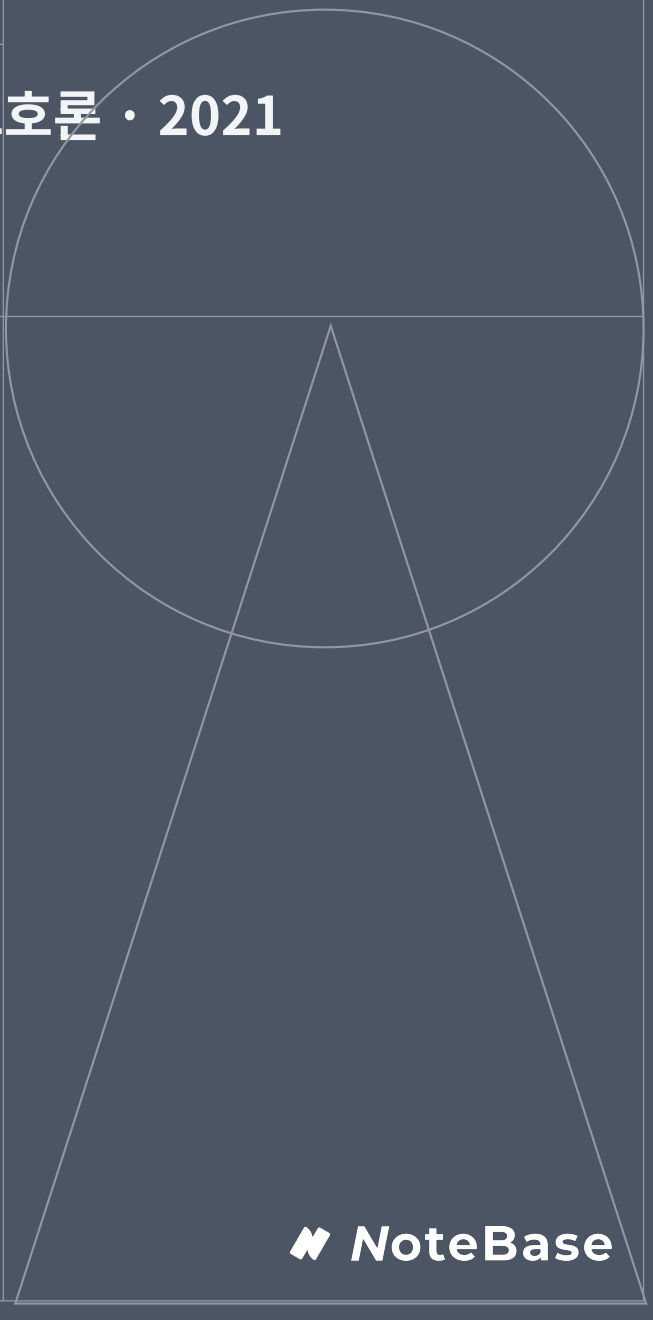
기출OX 해설집

공무원/지방직/9급 · 정보보호론 · 2021



NoteBase

기출OX 해설집

공무원/지방직/9급 · 정보보호론 · 2021

공무원/지방직/9급 · 정보보호론 · 2021

문 1. 보안의 3대 요소 중 적절한 권한을 가진 사용자가 인가한 방법으로만 정보를 변경할 수 있도록 하는 것은?

① 무결성(integrity)

② 기밀성(confidentiality)

③ 가용성(availability)

④ 접근성(accessability)

정답 1번

간단한 해설

정보를 **인가된 사용자와 방법에 의해서만 변경**할 수 있게 하여 정확성과 완전성을 유지하는 것이 무결성이다.

개념 구분

무결성: 정보가 허가 없이 변경·삭제되지 않고 정확성과 완전성을 유지하는 성질이다. 문제의 '적절한 권한을 가진 사용자'와 '인가한 방법으로만 변경'은 **정보 변경의 정당성**을 보장하는 조건이다. 예를 들어 조회 권한만 가진 사용자가 기록을 수정하지 못하게 하는 것은 무결성을 보호한다.

기밀성과의 구분: 기밀성은 인가되지 않은 사람에게 정보가 공개되지 않도록 하는 성질이다. **정보를 볼 수 있는가**가 중심이며, 정보를 변경할 수 있는가를 묻는 무결성과 구별된다.

가용성과의 구분: 가용성은 인가된 사용자가 **필요할 때 정보나 서비스를 이용**할 수 있는 성질이다. 서비스 장애를 막아 이용 가능성을 유지하는 것이 대표적인 예이며, 정보 변경의 허용 여부와는 판단 기준이 다르다.

접근성: 정보나 서비스에 접근하기 쉬운 정도를 뜻하며, 보안의 3대 요소에 해당하는 명칭은 아니다. 보안의 3대 요소는 기밀성·무결성·가용성이다.

NoteBase

문 2. 스트림 암호에 대한 설명으로 옳지 않은 것은?

① 데이터의 흐름을 순차적으로 처리해 가는 암호 알고리즘이다.

② 이진화된 평문 스트림과 이진 키스트림 수열의 XOR 연산으로 암호문을 생성하는 방식이다.

③ 스트림 암호 알고리즘으로 RC5가 널리 사용된다.

④ 구현이 용이하고 속도가 빠르다는 장점이 있다.

정답 3번

간단한 해설

RC5는 일정한 길이의 데이터 블록을 암호화하는 **블록 암호**이다. 스트림 암호의 대표적인 예로는 RC4가 있다.

선지별 해설

① O: 스트림 암호는 평문을 비트 또는 바이트 등의 단위로 **순차적으로 처리**한다. 일정한 길이의 블록을 모아 처리하는 블록 암호와 구별된다.

② O: 이진 평문과 키스트림의 각 비트를 **XOR 연산**하여 암호문을 만든다. XOR은 두 비트가 같으면 0, 다르면 1이 되는 연산이다. 암호문에 같은 키스트림을 다시 XOR하면 원래 평문이 복원된다.

③ X: RC5는 스트림 암호가 아니라 **블록 암호**이다. 스트림 암호 알고리즘의 예를 들려면 RC5 대신 RC4로 고쳐야 한다. RC4는 키스트림을 생성하여 평문과 XOR하는 방식으로 암호화한다.

④ O: 스트림 암호는 키스트림을 생성하고 평문과 XOR하는 구조로 구현할 수 있다. XOR 같은 단순한 연산으로 데이터를 연속 처리하므로 일반적으로 **구현이 비교적 간단하고 처리 속도가 빠르다**는 장점이 있다. 실제 성능은 알고리즘과 구현 환경에 따라 달라진다.

NoteBase

문 3. DES(Data Encryption Standard)에 대한 설명으로 옳지 않은 것은?

① 1977년에 미국 표준 블록 암호 알고리즘으로 채택되었다.

② 64비트 평문 블록을 64비트 암호문으로 암호화한다.

③ 페이스텔 구조(Feistel structure)로 구성된다.

④ 내부적으로 라운드(round)라는 암호화 단계를 10번 반복해서 수행한다.

정답 4번

간단한 해설

④의 '10번 반복'은 **16번 반복**으로 고쳐야 한다. DES는 16라운드의 페이스텔 구조로 암호화한다.

선지별 해설

① O: DES는 **1977년** 미국 국립표준국(NBS)에 의해 연방 정보처리표준인 FIPS 46으로 채택된 블록 암호 알고리즘이다.

② O: DES의 **블록 크기는 64비트**이다. 평문을 64비트 단위로 처리하며, 각 평문 블록을 암호화한 결과도 64비트 암호문 블록이다.

③ O: DES는 **페이스텔 구조**를 사용한다. 64비트 블록을 좌우 32비트씩 나누고, 한쪽 절반에 라운드 키와 라운드 함수를 적용한 결과를 다른 쪽 절반과 XOR하여 데이터를 변환한다.

④ X: DES의 암호화 라운드는 10회가 아니라 **16회**이다. 각 라운드에서는 해당 라운드의 키를 사용하여 데이터를 변환하며, 이 과정을 16라운드에 걸쳐 수행한다.

NoteBase

문 4. 다음 (가) ~ (다)에 해당하는 악성코드를 옳게 짝 지은 것은?

(가) 사용자의 문서와 사진 등을 암호화시켜 일정 시간 안에 일정 금액을 지불하면 암호를 풀어주는 방식으로 사용자에게 금전적인 요구를 하는 악성코드
(나) 운영체제나 특정 프로그램의 취약점을 이용하여 공격하는 악성코드
(다) 외부에서 파일을 내려받는 다운로드와 달리 내부 데이터로부터 새로운 파일을 생성하여 공격을 수행하는 악성코드

① (가): 드로퍼, (나): 익스플로잇, (다): 랜섬웨어
② (가): 드로퍼, (나): 랜섬웨어, (다): 익스플로잇
③ (가): 랜섬웨어, (나): 익스플로잇, (다): 드로퍼
④ (가): 랜섬웨어, (나): 드로퍼, (다): 익스플로잇

정답 3번

간단한 해설

(다)는 외부에서 파일을 내려받는 대신 **내부에 포함된 데이터로 악성 파일을 생성**하므로 드로퍼에 해당한다. 익스플로잇은 파일의 생성 방식이 아니라 **프로그램의 취약점을 이용한 공격**이라는 점으로 구별한다.

대응 관계 해설

(가) 랜섬웨어: 문서와 사진 등을 암호화해 사용하지 못하게 만든 뒤, 복구를 대가로 금전을 요구하는 악성코드이다. 주어진 설명에서 **암호화한 파일의 복구를 빌미로 금전을 요구**한다는 점이 랜섬웨어를 가리킨다. 돈을 내면 암호를 풀어주겠다는 것은 공격자의 요구 내용이며, 실제 복구를 보장한다는 뜻은 아니다.

(나) 익스플로잇: 운영체제나 응용 프로그램의 보안 취약점을 이용해 공격하는 코드이다. 프로그램의 결함을 악용하여 공격자가 의도한 동작을 일으킨다는 점에서, 핵심 기준은 **취약점의 악용**이다. 다른 악성 파일을 생성하는 역할을 설명한 드로퍼와 구별한다.

(다) 드로퍼: 내부에 포함된 악성코드 데이터를 파일로 생성하여 다른 악성코드를 설치하는 역할을 한다. 외부 서버에서 파일을 내려받는 방식과 달리 **자체에 포함된 데이터에서 파일을 꺼내 생성**한다는 것이 주어진 설명의 핵심이다.

(가) 랜섬웨어, (나) 익스플로잇, (다) 드로퍼의 대응은 ③의 조합과 일치한다.

NoteBase

문 5. ISO 27001의 정보보호영역(통제분야)에 해당하지 않은 것은?

① 소프트웨어 품질 보증(Software Quality Assurance)

② 접근통제(Access Control)

③ 암호화(Cryptography)

④ 정보보안 사고관리(Information Security Incident Management)

정답 1번

간단한 해설

소프트웨어 품질 보증은 개발 과정과 산출물이 **정해진 품질 요구사항을 충족하도록 보증하는 활동**이다. 보안과 관련될 수는 있지만, ISO/IEC 27001:2013 부속서 A의 **독립된 정보보호 통제분야는 아니다**.

선지별 해설

① X: 소프트웨어 품질 보증은 개발 절차와 산출물이 정해진 품질 요구사항과 표준을 따르는지 검토하는 활동이다. ISO/IEC 27001:2013 부속서 A에는 '소프트웨어 품질 보증'이라는 독립된 통제분야가 없다. 소프트웨어 개발과 관련된 보안 요구사항과 보안 시험 등은 **'정보시스템의 도입·개발·유지보수'(A.14)** 분야에서 다룬다.

② O: 접근통제는 ISO/IEC 27001:2013의 A.9 통제분야이다. 사용자에게 필요한 접근권한을 부여하고 이를 검토·회수하여 **인가되지 않은 접근을 방지**한다. 예를 들어 퇴사자의 시스템 접근권한을 제거하는 것이 이에 해당한다.

③ O: 암호화는 ISO/IEC 27001:2013의 A.10 통제분야이다. 정보의 기밀성·진정성·무결성을 보호하기 위한 암호기술의 적절한 사용을 다루며, **암호통제 사용 정책과 암호키 관리**를 포함한다. 데이터를 암호화하는 것뿐 아니라 키의 사용·보호·수명도 관리한다.

④ O: 정보보안 사고관리는 ISO/IEC 27001:2013의 A.16 통제분야이다. 보안 사건과 취약점을 보고하고, 사건이 실제 사고에 해당하는지 평가한 뒤 정해진 절차에 따라 대응한다. 사고를 신속하고 일관되게 처리하며, **사고에서 얻은 교훈을 재발 방지에 활용**하는 활동도 포함한다.

NoteBase

문 6. 암호화 알고리즘과 복호화 알고리즘에서 각각 다른 키를 사용하는 것은?

① SEED

② ECC

③ AES

④ IDEA

정답 2번

간단한 해설

ECC는 타원곡선을 이용하는 **공개키 암호 방식**이다. 이를 이용한 공개키 암호화에서는 수신자의 공개키로 암호화하고, 그와 짝을 이루는 **서로 다른 개인키**로 복호화한다.

선지별 해설

① X: SEED는 **대칭키 블록 암호**이다. 송신자와 수신자가 공유하는 같은 비밀키를 암호화와 복호화에 사용하므로, 서로 다른 공개키와 개인키를 사용하는 방식에 해당하지 않는다.

② O: ECC는 타원곡선을 이용하는 비대칭키 암호 방식으로, 공개할 수 있는 공개키와 소유자만 보관하는 개인키를 한 쌍으로 사용한다. ECC를 이용한 공개키 암호화에서는 **수신자의 공개키로 암호화하고 수신자의 개인키로 복호화**하므로, 암호화와 복호화에 서로 다른 키를 사용한다.

③ X: AES는 **대칭키 블록 암호**이다. 암호화와 복호화의 처리 절차가 달라도 사용하는 비밀키는 같으므로, 알고리즘의 절차 차이를 공개키와 개인키의 구분으로 이해해서는 안 된다.

④ X: IDEA는 **같은 비밀키를 공유하는 대칭키 블록 암호**이다. 암호화하는 사람과 복호화하는 사람이 별개의 공개키·개인키 쌍을 사용하는 것이 아니라, 공유한 비밀키로 데이터를 암호화하고 복호화한다.

NoteBase

문 7. DoS(Denial of Service)의 공격유형이 아닌 것은?

① Race Condition

② TearDrop

③ SYN Flooding

④ Land Attack

정답 1번

간단한 해설

Race Condition은 **공유 자원에 접근하는 순서와 시점의 허점**을 악용하는 방식으로, 이 문항에서는 전형적인 DoS 공격유형과 구분한다.

선지별 해설

DoS는 정상 이용자가 시스템이나 네트워크 서비스를 이용하지 못하게 하는 공격이다.

① X: Race Condition은 여러 프로세스나 스레드가 공유 자원에 접근할 때 **동기화가 제대로 이루어지지 않아 실행 순서에 따라 결과가 달라지는 취약점**이다. 예를 들어 파일의 접근 권한을 확인한 뒤 실제로 사용하기 전까지의 틈에 파일을 바꾸면, 확인했던 파일과 다른 파일에 접근하게 될 수 있다. 이 문항에서는 이러한 경쟁 상태의 악용을 전형적인 DoS 공격유형과 구분한다. 다만 경쟁 상태로 시스템이 중단될 수도 있으므로, DoS의 원인이 될 수 없다는 뜻은 아니다.

② O: TearDrop은 **서로 겹치도록 조작한 IP 조각**을 보내 재조립 과정의 취약점을 악용하는 DoS 공격이다. 취약한 시스템이 조각을 정상적으로 처리하지 못해 오류나 중단이 발생하면서 서비스 이용이 방해된다.

③ O: SYN Flooding은 TCP 연결을 요청하는 SYN 패킷을 대량으로 보내고 연결 절차를 완료하지 않아 **미완료 연결을 위한 자원**을 소진시키는 DoS 공격이다. 서버가 SYN에 대해 SYN-ACK를 보낸 뒤 마지막 ACK를 기다리는 상태가 쌓이면 정상 이용자의 새 연결을 처리하기 어려워진다.

④ O: Land Attack은 TCP SYN 패킷의 **출발지와 목적지 IP 주소 및 포트 번호를 각각 같게** 조작하여 공격 대상에게 보내는 DoS 공격이다. 취약한 TCP/IP 구현에서는 자기 자신을 상대방으로 인식해 패킷을 처리하면서 자원이 소모되거나 시스템이 중단될 수 있다.

NoteBase

문 8. 다음에서 설명하는 방화벽 구축 형태는?

◯ 배스천(Bastion) 호스트와 스크린 라우터를 혼합하여 사용한 방화벽
◯ 외부 네트워크와 내부 네트워크 사이에 스크린 라우터를 설치하고 스크린 라우터와 내부 네트워크 사이에 배스천 호스트를 설치

① Bastion Host
② Dual Homed Gateway
③ Screened Subnet Gateway
④ Screened Host Gateway

정답 4번

간단한 해설

스크린 라우터로 외부 트래픽을 먼저 걸러 내고, 그 안쪽에 배스천 호스트를 두어 서비스를 중계하는 **스크린드 호스트 게이트웨이** 구성이다. 핵심 단서는 **스크린 라우터와 배스천 호스트의 결합**이다.

핵심 풀이

제시된 구성은 Screened Host Gateway이다. 스크린 라우터는 외부·내부 네트워크의 경계에서 IP 주소와 포트 번호 등의 조건으로 패킷을 걸러 낸다. 라우터 안쪽의 배스천 호스트는 보안을 강화한 호스트로, 프록시 등을 통해 허용된 서비스를 중계한다. 즉, **라우터의 패킷 필터링과 배스천 호스트의 서비스 중계**를 결합한 구조이다. Bastion Host는 이 구성에 쓰이는 호스트 자체를 가리키므로 전체 구축 형태의 명칭과 구별한다.

Screened Subnet Gateway는 배스천 호스트를 내부망과 구분된 **별도 서브넷인 DMZ**에 배치하는 구성이다. 전형적으로 DMZ의 외부 쪽과 내부 쪽에 각각 스크린 라우터를 두어 분리한다. 제시문은 별도 서브넷을 만드는 대신 스크린 라우터 안쪽에 배스천 호스트를 배치하는 구성을 설명한다.

Dual Homed Gateway는 **두 개의 네트워크 인터페이스를 가진 호스트**가 외부망과 내부망에 각각 연결되는 구성이 핵심이다. 방화벽으로 사용할 때는 직접적인 IP 전달을 막고 호스트의 프록시 등으로 통신을 중계한다. 제시문의 결정적 단서는 인터페이스 두 개가 아니라 별도 스크린 라우터와 배스천 호스트의 결합이다.

NoteBase

문 9. 다음에서 설명하는 보안 기술은?

◯ 해시 함수를 이용하여 메시지 인증 코드를 구현한다.
◯ SHA－256을 사용할 수 있다.

① HMAC(Hash based Message Authentication Code)
② Block Chain
③ RSA(Rivest－Shamir－Adleman)
④ ARIA(Academy, Research Institute, Agency)

정답 1번

간단한 해설

해시 함수로 메시지 인증 코드를 만드는 **HMAC**은 메시지와 공유 비밀키를 이용한다. SHA-256은 HMAC 내부에서 사용할 수 있는 해시 함수이다.

핵심 풀이

HMAC은 **공유 비밀키와 해시 함수**를 이용하여 메시지 인증 코드를 생성하는 방식이다. 송신자가 메시지에 대한 인증 코드를 만들어 보내면, 수신자는 같은 비밀키와 해시 함수로 코드를 다시 계산하여 비교한다. 이를 통해 메시지의 변조 여부와 공유키를 가진 주체가 생성한 메시지인지를 확인한다.

SHA-256은 HMAC의 내부 해시 함수로 사용할 수 있으며, 이 구성을 HMAC-SHA-256이라고 한다.
SHA-256으로 메시지의 해시값만 계산하는 것과 달리, HMAC은 **비밀키를 함께 사용하여 인증**한다. 따라서 '해시 함수를 이용한 메시지 인증 코드'와 'SHA-256 사용 가능'이라는 두 단서는 HMAC을 가리킨다.

Block Chain은 블록들을 해시값으로 연결하는 기술이므로, 해시 함수를 사용한다는 점만으로 HMAC과 혼동해서는 안 된다. RSA는 공개키 암호 알고리즘이고 ARIA는 대칭키 블록 암호 알고리즘이므로, 둘 다 해시 함수 기반 메시지 인증 코드 방식이라는 설명과 구별된다.

NoteBase

문 10. 스미싱 공격에 대한 설명으로 옳지 않은 것은?

① 공격자는 주로 앱을 사용하여 공격한다.

② 스미싱은 개인 정보를 빼내는 사기 수법이다.

③ 공격자는 사용자가 제대로 된 url을 입력하여도 원래 사이트와 유사한 위장 사이트로 접속시킨다.

④ 공격자는 문자 메시지 링크를 이용한다.

정답 3번

간단한 해설

③의 '정상 URL을 입력해도 위장 사이트로 연결된다'는 **파밍**의 특징이다. 스미싱은 **문자메시지를 이용한 속임수**로 악성 앱 설치나 개인정보 입력 등을 유도하는 공격이다.

선지별 해설

① O: 전형적인 스미싱은 사용자가 문자 링크를 통해 **정상 앱으로 위장한 악성 앱**을 설치하도록 유도한다. 설치된 악성 앱은 스마트폰의 개인정보나 문자메시지 등을 빼내는 데 이용된다.

② O: 스미싱은 문자메시지(SMS)와 피싱(Phishing)의 합성어이다. 문자로 사용자를 속여 **개인정보·금융정보를 탈취**하는 사기 수법이며, 소액결제 등의 금전적 피해로도 이어질 수 있다.

③ X: 사용자가 올바른 URL을 입력해도 위장 사이트로 접속하게 만드는 것은 **파밍(Pharming)**의 특징이다. 악성코드 등으로 접속 경로를 조작하기 때문에 사용자가 주소를 정확히 입력해도 가짜 사이트로 연결된다. 스미싱의 특징으로 고치려면 '문자메시지로 악성 링크를 보내 접속이나 앱 설치를 유도한다'고 해야 한다.

④ O: 공격자는 택배 안내나 모바일 청첩장 등으로 가장한 **문자메시지 속 링크**를 이용해 사용자의 접속을 유도한다. 이 링크는 악성 앱을 내려받게 하거나 개인정보를 입력하게 하는 사이트로 연결되는 통로가 된다.

NoteBase

문 11. 디지털 포렌식을 통해 획득한 증거가 법적인 효력을 갖기 위해 만족해야 할 원칙이 아닌 것은?

① 정당성의 원칙

② 재현의 원칙

③ 무결성의 원칙

④ 기밀성의 원칙

정답 4번

간단한 해설

기밀성은 **인가받지 않은 사람에게 정보가 노출되지 않도록 하는** 정보보호 성질이다. 디지털 증거의 법적 효력을 뒷받침하는 정당성·재현성·무결성과는 구별된다.

선지별 해설

① O: 정당성의 원칙은 디지털 증거를 **적법한 절차와 방법으로 수집**해야 한다는 뜻이다. 내용이 사건과 관련되더라도 수집 과정에서 법적 절차를 위반하면 증거능력이 문제될 수 있다.

② O: 재현의 원칙은 같은 증거를 같은 조건과 절차로 분석하면 **동일한 결과를 다시 얻을 수 있어야 한다**는 뜻이다. 분석 절차와 사용한 도구 등을 기록하여 다른 분석자도 결과를 검증할 수 있도록 한다.

③ O: 무결성의 원칙은 증거를 수집한 이후 보관·분석·제출하는 과정에서 **증거의 내용이 변경되지 않았음**을 보장해야 한다는 뜻이다. 예를 들어 원본과 분석용 복제본의 해시값을 비교하여 내용의 동일성을 확인한다.

④ X: 기밀성의 원칙은 **인가된 사람만 정보에 접근**할 수 있도록 하여 정보 유출을 막는 정보보호 원칙이다. 포렌식 과정에서도 정보 유출 방지는 필요하지만, 이 문항에서 묻는 디지털 증거의 법적 효력 확보 원칙에는 해당하지 않는다. 법적 효력을 뒷받침하는 원칙으로는 정당성·재현성·무결성 등이 있다.

NoteBase

문 12. 「개인정보 보호법」 상의 개인정보에 대한 설명으로 옳지 않은 것은?

① 개인정보 보호위원회의 위원 임기는 3년이다.

② 개인정보는 가명처리를 할 수 없다.

③ 개인정보 보호위원회의 위원은 대통령이 임명 또는 위촉한다.

④ 개인정보처리자는 개인정보파일의 운용을 위하여 다른 사람을 통하여 개인정보를 처리할 수 있다.

정답 2번

①

개인정보 보호위원회 위원의 임기는 **3년**이다.

개인정보 보호법 제7조의4 제1항
개인정보 보호법 제7조의4(위원의 임기)
① 위원의 임기는 3년으로 하되, 한 차례만 연임할 수 있다.

②

개인정보를 가명으로 처리하여도 수집목적을 달성할 수 있고 익명처리로는 목적을 달성할 수 없는 경우에는 **가명으로 처리될 수 있도록 해야 한다**.

개인정보 보호법 제3조 제7항
개인정보 보호법 제3조(개인정보 보호 원칙)
⑦ 개인정보처리자는 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적을 달성할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다. <개정 2020.2.4>

NoteBase

③

개인정보 보호위원회 위원은 법정 제청·추천 절차를 거쳐 **대통령이 임명 또는 위촉한다**.

개인정보 보호법 제7조의2 제2항
개인정보 보호법 제7조의2(보호위원회의 구성 등)
② 보호위원회의 위원은 개인정보 보호에 관한 경력과 전문지식이 풍부한 다음 각 호의 사람 중에서 위원장과 부위원장은 국무총리의 제청으로, 그 외 위원 중 2명은 위원장의 제청으로, 2명은 대통령이 소속되거나 소속되었던 정당의 교섭단체 추천으로, 3명은 그 외의 교섭단체 추천으로 대통령이 임명 또는 위촉한다.
1. 개인정보 보호 업무를 담당하는 3급 이상 공무원(고위공무원단에 속하는 공무원을 포함한다)의 직에 있거나 있었던 사람
2. 판사 · 검사 · 변호사의 직에 10년 이상 있거나 있었던 사람
3. 공공기관 또는 단체(개인정보처리자로 구성된 단체를 포함한다)에 3년 이상 임원으로 재직하였거나 이들 기관 또는 단체로부터 추천받은 사람으로서 개인정보 보호 업무를 3년 이상 담당하였던 사람
4. 개인정보 관련 분야에 전문지식이 있고 「고등교육법」 제2조제1호에 따른 학교에서 부교수 이상으로 5년 이상 재직하고 있거나 재직하였던 사람

④

개인정보처리자는 업무를 목적으로 개인정보파일을 운용하기 위하여 **스스로 또는 다른 사람을 통하여 개인정보를 처리**하는 공공기관, 법인, 단체 및 개인 등을 말한다.

개인정보 보호법 제2조 제5호
개인정보 보호법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2014.3.24, 2020.2.4, 2023.3.14>
5. "개인정보처리자"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

NoteBase

문 13. DoS 및 DDoS 공격 대응책으로 옳지 않은 것은?

① 방화벽 및 침입 탐지 시스템 설치와 운영

② 시스템 패치

③ 암호화

④ 안정적인 네트워크 설계

정답 3번

간단한 해설

암호화는 정보의 내용을 알아볼 수 없게 하여 **기밀성**을 보호한다. DoS·DDoS 공격은 자원을 고갈시켜 **가용성**을 침해하므로, 암호화만으로는 과도한 요청이나 트래픽을 막을 수 없다.

선지별 해설

① O: 방화벽은 설정된 규칙에 따라 불필요하거나 의심스러운 트래픽을 차단하고, 침입 탐지 시스템은 공격 징후를 탐지하여 관리자에게 알린다. 이를 설치·운영하면 공격 트래픽을 식별하고 차단 조치를 취하는 데 도움이 된다. 다만 **침입 탐지 자체가 곧 차단을 뜻하지는 않는다**.

② O: 시스템 패치는 운영체제나 응용 프로그램의 **알려진 취약점을 보완**한다. 취약점을 악용하여 시스템을 중단시키거나 자원을 과도하게 소모하게 하는 DoS 공격을 예방하는 데 도움이 된다. 다만 대량의 트래픽으로 회선을 포화시키는 공격까지 패치만으로 막을 수 있는 것은 아니다.

③ X: 암호화는 데이터를 권한 없는 사람이 읽기 어렵게 만드는 기밀성 보호 수단이다. DoS는 시스템이나 네트워크 자원을 소모시켜 정상적인 서비스 이용을 방해하는 공격이고, DDoS는 이를 여러 공격원에서 분산하여 수행하는 공격이다. 따라서 대응에는 **공격 트래픽 차단과 자원 고갈 완화**가 필요하며, 데이터 내용을 암호화하는 것만으로는 요청량이나 트래픽이 줄어들지 않는다.

④ O: 안정적인 네트워크 설계는 충분한 처리 용량을 확보하고, 이중화나 부하 분산을 통해 **특정 장비나 경로에 부하가 집중되는 것을 완화**한다. 이에 따라 공격이 발생해도 정상적인 서비스를 유지할 가능성을 높이므로 DoS·DDoS 피해를 줄이는 대응책에 해당한다.

NoteBase

문 14. 국제 공통 평가기준(Common Criteria)에 대한 설명으로 옳지 않은 것은?

① CC는 국제적으로 평가 결과를 상호 인정한다.

② CC는 보안기능수준에 따라 평가 등급이 구분된다.

③ 보안목표명세서는 평가 대상에 해당하는 정보보호 시스템의 보안 요구 사항, 보안 기능 명세 등을 서술한 문서이다.

④ 보호프로파일은 보안 문제를 해결하기 위해 작성한 제품군별 구현에 독립적인 보안요구사항 등을 서술한 문서이다.

정답 2번

간단한 해설

CC의 평가 등급은 보안기능의 종류나 수준이 아니라, 그 기능이 요구사항을 충족하는지 얼마나 엄격하게 확인했는지를 나타내는 **보증수준**에 따라 구분된다.

선지별 해설

① O: CC에 따른 평가·인증 결과는 **국제상호인정협정(CCRA)의 참여국 사이에서 협정이 정한 범위 안에서** 상호 인정된다. 이를 통해 같은 제품에 대한 중복 평가를 줄일 수 있다.

② X: CC는 보안기능 요구사항과 보증 요구사항을 구분한다. 보안기능 요구사항은 제품이 제공해야 할 기능을 정하고, 보증 요구사항은 그 기능이 요구대로 구현되었음을 확인하는 평가 활동과 증거를 정한다.
평가보증등급(EAL1~EAL7)은 보안기능수준이 아니라 **평가의 깊이와 엄격성을 나타내는 보증수준**에 따라 구분된다. 따라서 높은 EAL이 더 많은 보안기능을 뜻하는 것은 아니다.

③ O: 보안목표명세서(ST)는 **특정 평가대상(TOE)에 대한** 보안 요구사항과 이를 충족하는 보안기능의 개요 등을 서술한 문서이다. 평가자는 이 문서에 명시된 요구사항을 기준으로 해당 제품이나 시스템을 평가한다.

④ O: 보호프로파일(PP)은 특정 제품의 구현 방법에 종속되지 않고, **제품군에 공통으로 필요한 보안 요구사항**을 서술한 문서이다. 특정 제품을 대상으로 하는 보안목표명세서와 달리, 서로 다른 구현의 제품에도 공통 요구사항을 제시할 수 있다.

NoteBase

문 15. 생체인증(Biometrics)에 대한 설명으로 옳지 않은 것은?

① 생체 인증은 불변의 신체적 특성을 활용한다.

② 생체 인증은 지문, 홍채, 망막, 정맥 등의 특징을 활용한다.

③ 얼굴은 행동적 특성을 이용한 인증 수단이다.

④ 부정허용률(false acceptance rate)은 인증되지 않아야 할 사람을 인증한 값이다.

정답 3번

간단한 해설

얼굴의 형태와 구조는 **신체적 특성**에 해당한다. 행동적 특성을 이용하는 인증은 서명 습관이나 걸음걸이처럼 사람이 행동하는 방식의 차이를 활용한다.

선지별 해설

① O: 생체 인증은 개인을 구별할 수 있고 시간이 지나도 비교적 일정하게 유지되는 신체적 특징을 본인 확인에 활용한다. 여기서 '불변'은 **쉽게 바뀌지 않는 지속성**을 뜻하며, 모든 신체적 특징이 평생 전혀 변하지 않는다는 뜻은 아니다.

② O: 지문의 무늬, 홍채의 패턴, 망막의 혈관 분포, 정맥의 패턴은 개인을 구별하는 데 활용할 수 있는 신체적 특징이다. 이러한 특징을 추출하여 미리 등록한 생체 정보와 비교함으로써 본인 여부를 판단한다.

③ X: 얼굴의 형태와 구조는 **행동적 특성이 아니라 신체적 특성**이다. 행동적 특성은 서명하는 습관, 키보드 입력 리듬, 걸음걸이처럼 개인의 행동 방식에서 나타나는 특징이다.

④ O: 부정허용률(FAR)은 인증되지 않아야 할 타인의 인증 시도 중에서 시스템이 본인으로 잘못 인정한 비율이다. 즉, **타인을 본인으로 잘못 받아들이는 오류**를 나타내며, 본인을 타인으로 잘못 판단하여 거부하는 본인거부율(FRR)과 구별한다.

NoteBase

문 16. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의3 (정보보호 최고책임자의 지정 등)에 따른 정보보호 최고책임자의 업무가 아닌 것은?

① 정보보호 사전 보안성 검토

② 정보보호 취약점 분석·평가 및 개선

③ 중요 정보의 암호화 및 보안서버 적합성 검토

④ 정보통신시설을 안정적으로 운영하기 위하여 대통령령으로 정하는 바에 따른 보호조치

정답 4번

①

정보보호 최고책임자는 **정보통신시스템 또는 정보통신서비스의 도입·개시 또는 변경 시 보안성 검토**를 총괄한다. 정보보호 사전 보안성 검토는 이 업무에 해당한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조의3 제4항 제1호 사목
④ 정보보호 최고책임자의 업무는 다음 각 호와 같다. <개정 2021.6.8, 2026.3.10, 2026.3.31>
1. 정보보호 최고책임자는 다음 각 목의 업무를 총괄한다.
사. 그 밖에 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 대통령령으로 정하는 사항

정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령 제36조의7 제7항 제1호
⑦ 법 제45조의3 제4항 제1호 사목 에서 “대통령령으로 정하는 사항”이란 다음 각 호의 사항을 말한다. <신설 2026. 9. 30.>
1. 정보통신시스템 또는 정보통신서비스의 도입 · 개시 또는 변경 시 보안성 검토

②

정보보호 최고책임자는 **정보보호 위험을 식별·평가하고 대책을 마련**하는 업무를 총괄한다. 취약점 분석·평가와 개선은 이에 해당한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조의3 제4항 제1호 다목
정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조의3(정보보호 최고책임자의 지정 등)
④ 정보보호 최고책임자의 업무는 다음 각 호와 같다. <개정 2021.6.8, 2026.3.10, 2026.3.31>
1. 정보보호 최고책임자는 다음 각 목의 업무를 총괄한다.
다. 정보보호 위험의 식별 평가 및 정보보호 대책 마련

NoteBase

③

중요 정보의 암호화와 보안서버 적합성 검토는 정보보호 위험에 대한 보호대책을 마련하는 업무로서 정보보호 최고책임자의 총괄 범위에 포함된다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조의3 제4항 제1호 다목
정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조의3(정보보호 최고책임자의 지정 등)
④ 정보보호 최고책임자의 업무는 다음 각 호와 같다. <개정 2021.6.8, 2026.3.10, 2026.3.31>
1. 정보보호 최고책임자는 다음 각 목의 업무를 총괄한다.
다. 정보보호 위험의 식별 평가 및 정보보호 대책 마련

NoteBase

④

시설의 안정적 운영을 위한 보호조치는 **일정 규모 이상의 집적정보통신시설 사업자등에게 부과되는 의무**이다. 정보보호 최고책임자의 업무를 열거한 내용과 구별된다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조의3 제4항
정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조의3(정보보호 최고책임자의 지정 등)
④ 정보보호 최고책임자의 업무는 다음 각 호와 같다. <개정 2021.6.8, 2026.3.10, 2026.3.31>
1. 정보보호 최고책임자는 다음 각 목의 업무를 총괄한다.
가. 정보보호 계획의 수립 · 시행 및 개선
나. 정보보호 실태와 관행의 정기적인 감사 및 개선
다. 정보보호 위험의 식별 평가 및 정보보호 대책 마련
라. 정보보호 교육과 모의 훈련 계획의 수립 및 시행
마. 정보보호에 필요한 인력 관리 및 예산 편성
바. 정보보호 현황 및 주요 사항의 이사회에 대한 보고
사. 그 밖에 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 대통령령으로 정하는 사항
2. 정보보호 최고책임자는 다음 각 목의 업무를 겸할 수 있다.
가. 「정보보호산업의 진흥에 관한 법률」 제13조에 따른 정보보호 공시에 관한 업무
나. 「정보통신기반 보호법」 제5조제5항에 따른 정보보호책임자의 업무
다. 「전자금융거래법」 제21조의2제4항에 따른 정보보호최고책임자의 업무
라. 「개인정보 보호법」 제31조제4항에 따른 개인정보 보호책임자의 업무
마. 그 밖에 이 법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제46조 제1항
정보통신망 이용촉진 및 정보보호 등에 관한 법률 제46조(집적된 정보통신시설의 보호)
① 다음 각 호의 어느 하나에 해당하는 정보통신서비스 제공자 중 정보통신시설의 규모 등이 대통령령으로 정하는 기준에 해당하는 자(이하 "집적정보통신시설 사업자등"이라 한다)는 정보통신시설을 안정적으로 운영하기 위하여 대통령령으로 정하는 바에 따른 보호조치를 하여야 한다. <개정 2020.6.9, 2023.1.3>
1. 타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영 · 관리하는 자(이하 "집적정보통신시설 사업자"라 한다)
2. 자신의 정보통신서비스 제공을 위하여 직접 집적된 정보통신시설을 운영 · 관리하는 자

NoteBase

문 17. 정보보호 및 개인정보보호 관리체계 인증에 대한 설명으로 옳은 것은?

① 인증기관 지정의 유효기간은 2년이다.

② 사후심사는 인증 후 매년 사후관리를 위해 실시된다.

③ 인증심사 기준은 12개 분야 92개 통제 사항이다.

④ 인증심사원은 2개 등급으로 구분된다.

정답 2번

간단한 해설

사후심사는 인증 취득 후에도 정보보호 및 개인정보보호 관리체계가 **지속적으로 유지되는지** 확인하는 절차이다. 인증 유효기간 중 **매년 1회 이상** 실시한다.

선지별 해설

① X: 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제9조제1항에 따르면 인증기관 및 심사기관 지정의 유효기간은 **3년**이다. 선지의 '2년'을 '3년'으로 고쳐야 한다. 여기서 지정의 유효기간은 인증업무를 수행할 기관으로 지정된 효력이 유지되는 기간을 뜻한다.

② O: 사후심사는 인증을 받은 기관이 정보보호 및 개인정보보호 관리체계를 계속 적절하게 운영하는지 확인하기 위한 심사이다. 인증을 취득한 뒤 인증 유효기간 중 **매년 1회 이상** 실시한다. 처음 인증기준 충족 여부를 확인하는 최초심사, 유효기간 연장을 위한 갱신심사와 목적이 구별된다.

③ X: 출제 당시 고시 제23조제1항 및 별표 7에 따른 ISMS-P 인증기준은 **3개 영역, 총 102개 인증기준**으로 구성되었다. 세 영역은 '관리체계 수립 및 운영', '보호대책 요구사항', '개인정보 처리 단계별 요구사항'이다. 따라서 '12개 분야 92개 통제 사항'이라는 설명은 당시 ISMS-P 인증기준과 맞지 않는다.

④ X: 고시 제12조 및 별표 3은 인증심사원을 **심사원보·심사원·선임심사원의 3개 등급**으로 구분한다. 각 등급에는 자격 취득과 심사경력 등에 관한 요건이 정해져 있으므로, '2개 등급'을 '3개 등급'으로 고쳐야 한다.

NoteBase

문 18. PGP(Pretty Good Privacy)에 대한 설명으로 옳지 않은 것은?

① RSA를 이용하여 메시지 다이제스트를 서명한다.

② 세션 키는 여러 번 사용된다.

③ 수신자는 자신의 개인키를 이용하여 세션 키를 복호화한다.

④ 세션 키를 이용하여 메시지를 암·복호화한다.

정답 2번

간단한 해설

PGP의 세션 키는 **메시지마다 새로 생성하여 해당 메시지에만 사용하는 대칭키**이다. 같은 세션 키를 여러 메시지에 반복해서 사용하는 것이 아니다.

선지별 해설

① O: 메시지에 해시 함수를 적용하여 메시지 다이제스트를 구한 뒤, RSA 서명 방식에서는 **송신자의 개인키**로 서명을 생성한다. 수신자는 송신자의 공개키로 서명을 검증하여 메시지의 무결성과 송신자를 확인한다.

② X: PGP는 **메시지마다 새로운 임의의 세션 키**를 생성하여 그 메시지의 암호화에만 사용한다. 따라서 '여러 번 사용된다'는 '메시지마다 새로 생성하여 해당 메시지에만 사용된다'로 고쳐야 한다. 여기서 일회성이라는 뜻은 한 메시지를 처리할 때만 쓴다는 의미이며, 수신자가 같은 키로 그 메시지를 복호화하는 것까지 금지한다는 뜻은 아니다.

③ O: 송신자는 세션 키를 **수신자의 공개키로 암호화**하여 메시지와 함께 보낸다. 수신자는 이에 대응하는 자신의 개인키로 세션 키를 복호화하므로, 개인키를 가진 수신자가 메시지 복호화에 필요한 키를 얻을 수 있다.

④ O: 메시지 본문은 **대칭키인 세션 키**로 암호화하고, 수신자도 복구한 동일한 세션 키로 복호화한다. PGP는 본문 처리에는 효율적인 대칭키 암호를, 세션 키 전달에는 공개키 암호를 결합하는 하이브리드 암호 방식이다.

NoteBase

문 19. 다음에서 설명하는 블록암호 운영 모드는?

◯ 단순한 모드로 평문이 한 번에 하나의 평문 블록으로 처리된다.
◯ 각 평문 블록은 동일한 키로 암호화된다.
◯ 주어진 하나의 키에 대하여 평문의 모든 블록에 대한 유일한 암호문이 존재한다.

① CBC(Cipher Block Chaining Mode)
② CTR(Counter Mode)
③ CFB(Cipher-Feed Back Mode)
④ ECB(Electronic Code Book Mode)

정답 4번

간단한 해설

ECB는 각 평문 블록을 같은 키로 **독립적으로 암호화**한다. 따라서 키가 같으면 동일한 평문 블록은 언제나 동일한 암호문 블록으로 변환된다.

핵심 풀이

ECB(Electronic Code Book Mode)는 평문을 블록으로 나누어 각 블록을 동일한 키로 독립적으로 암호화하는 방식이다. 앞 블록의 처리 결과나 블록의 위치가 암호화 결과에 영향을 주지 않으므로, **고정된 키에서 각 평문 블록에 대응하는 암호문 블록이 일정하다**. 예를 들어 평문 블록이 A·B·A이고 A와 B의 암호문이 각각 X와 Y라면 결과는 X·Y·X이다. 지문의 '유일한 암호문'은 이처럼 각 평문 블록의 암호문이 고정된다는 뜻이다.

CBC는 평문 블록을 **직전 암호문 블록과 XOR한 뒤 암호화**하며, 첫 블록에는 초기화 벡터(IV)를 사용한다. 따라서 현재 평문과 키만으로 암호문 블록이 결정되는 ECB와 구별된다.

CFB는 IV 또는 앞선 암호문을 반영한 값을 암호화하여 얻은 출력과 평문을 XOR하고, 생성된 암호문을 다음 처리에 피드백한다. 평문 블록을 직접 독립적으로 암호화하는 방식과 다르다.

CTR은 블록마다 서로 다른 카운터 값을 암호화한 뒤 그 출력과 평문을 XOR한다. 동일한 키를 쓰더라도 카운터 값이 결과에 관여하므로, '같은 키를 사용한다'는 조건만으로 ECB라고 판단해서는 안 된다.

NoteBase

문 20. BCP(Business Continuity Planning)에 대한 설명으로 옳지 않은 것은?

① BCP는 사업의 연속성을 유지하기 위한 업무지속성 계획과 절차이다.

② BCP는 비상시에 프로세스의 운영 재개에 필요한 조치를 정의한다.

③ BIA는 조직의 필요성에 의거하여 시스템의 중요성을 식별한다.

④ DRP(Disaster Recovery Plan)는 최대허용중단시간(Maximum Tolerable Downtime)을 산정한다.

정답 4번

간단한 해설

최대허용중단시간(MTD)은 업무 중단을 감내할 수 있는 시간의 한계로, **업무영향분석(BIA)에서 산정**한다. 재해복구계획(DRP)은 이를 바탕으로 정보시스템의 복구 방법과 절차를 정한다.

선지별 해설

① O: BCP는 재난이나 장애가 발생해도 조직의 **핵심 업무를 지속**할 수 있도록 마련하는 계획과 절차이다. 업무 중단에 대비한 운영 방법과 복구 방안을 포함하여 사업의 연속성을 확보한다.

② O: BCP는 비상시에 중단된 업무 프로세스를 다시 운영하기 위해 필요한 조치를 정한다. 담당자의 역할, 필요한 자원, 대체 업무 수행 방법과 재개 절차 등을 미리 정해 두어 **업무의 유지와 재개**가 가능하도록 한다.

③ O: BIA는 업무영향분석으로, 업무나 시스템의 중단이 조직에 미치는 영향을 분석한다. 조직의 업무상 필요와 해당 시스템이 지원하는 업무를 연결하여 **시스템의 중요성과 복구 우선순위**를 식별한다.

④ X: 최대허용중단시간(MTD)은 업무 중단으로 조직이 받아들일 수 없는 영향이 발생하기 전까지 허용할 수 있는 최대 시간이다. 이 시간은 **업무영향분석(BIA)에서 산정**하며, DRP는 분석 결과를 바탕으로 재해 시 정보시스템을 복구하는 구체적인 방법과 절차를 정하는 계획이다.

NoteBase