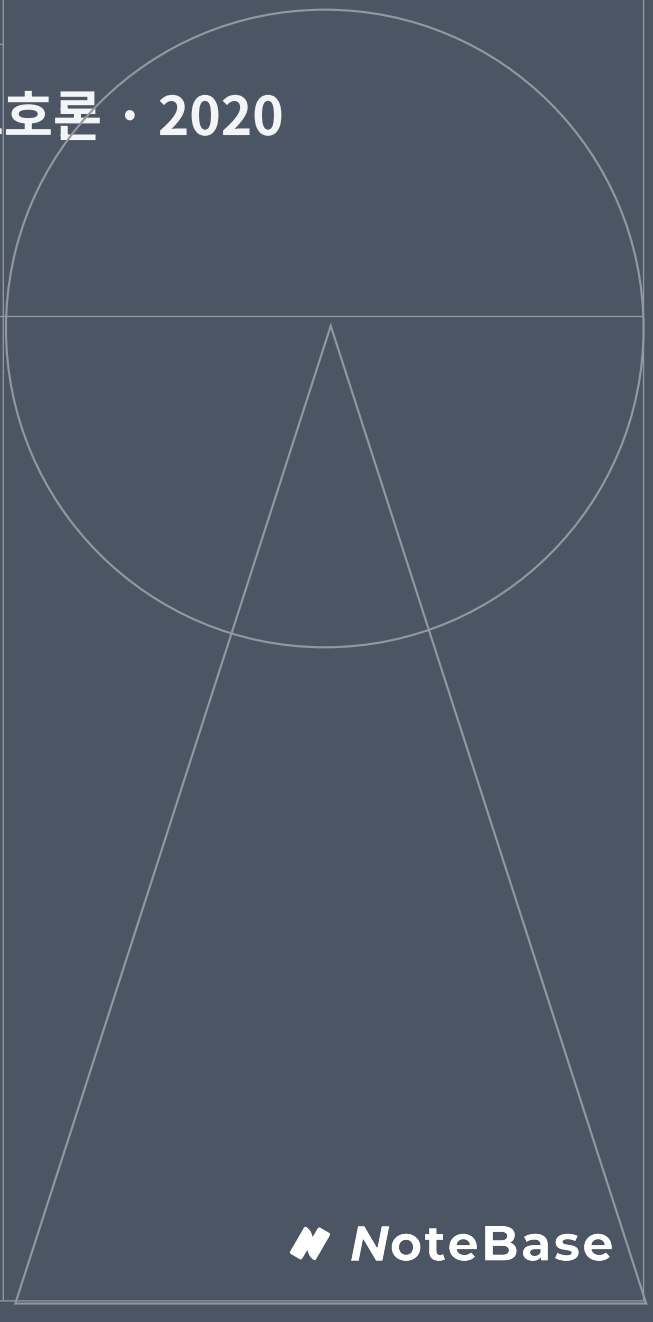
기출OX 해설집

공무원/지방직/9급 · 정보보호론 · 2020



NoteBase

기출OX 해설집

공무원/지방직/9급 · 정보보호론 · 2020

공무원/지방직/9급 · 정보보호론 · 2020

문 1. 전자 서명(digital signature) 보안 메커니즘이 제공하는 보안 서비스가 아닌 것은?

① 근원 인증

② 메시지 기밀성

③ 메시지 무결성

④ 부인 방지

정답 2번

간단한 해설

전자 서명은 메시지의 작성자와 변경 여부를 확인하는 수단이며, **메시지 내용을 숨기지는 않는다**. 메시지 기밀성을 확보하려면 별도의 **암호화**가 필요하다.

선지별 해설

① O: 근원 인증은 메시지가 누구에게서 왔는지 확인하는 서비스이다. 전자 서명은 서명자의 개인키로 생성하고 대응하는 공개키로 검증한다. 이 공개키가 실제 서명자의 것임을 신뢰할 수 있다면, 유효한 서명을 통해 **메시지의 출처**를 확인할 수 있다.

② X: 메시지 기밀성은 권한이 없는 사람이 메시지 내용을 알 수 없게 하는 성질이다. 전자 서명을 붙여도 **메시지 자체가 암호화되는 것은 아니므로** 내용을 읽는 것을 막지 못한다. 기밀성을 제공하려면 메시지를 별도로 암호화해야 한다.

③ O: 메시지 무결성은 메시지가 임의로 변경되지 않았음을 확인할 수 있는 성질이다. 전자 서명은 서명한 메시지와 연결되어 있으므로, 서명 후 메시지가 변경되면 서명 검증에 실패한다. 따라서 전자 서명은 **변조 여부를 탐지**하는 데 사용된다.

④ O: 부인 방지는 서명자가 나중에 자신이 서명한 사실을 부인하는 것에 대응하는 서비스이다. 개인키가 서명자만의 통제 아래 안전하게 관리되었다면, 대응하는 공개키로 검증되는 서명을 **서명 사실을 입증하는 증거**로 제3자에게 제시할 수 있다.

NoteBase

문 2. AES(Advanced Encryption Standard)에 대한 설명으로 옳은 것은?

① DES(Data Encryption Standard)를 대신하여 새로운 표준이 된 대칭 암호 알고리즘이다.

② Feistel 구조로 구성된다.

③ 주로 고성능의 플랫폼에서 동작하도록 복잡한 구조로 고안되었다.

④ 2001년에 국제표준화기구인 IEEE가 공표하였다.

정답 1번

간단한 해설

AES는 **DES를 대체하는 대칭키 블록 암호 표준**이다. 암호화와 복호화에 같은 비밀키를 사용하며, Rijndael 알고리즘을 기반으로 한다.

선지별 해설

① O: AES는 DES를 대체하기 위해 채택된 **대칭키 블록 암호 표준**이다. 대칭키 암호는 암호화와 복호화에 같은 비밀키를 사용하는 방식이며, AES는 Rijndael 알고리즘을 기반으로 한다.

② X: AES는 Feistel 구조가 아니라 **치환·순열 네트워크(SPN) 구조**를 사용한다. 바이트 값을 다른 값으로 바꾸는 치환과 행 이동·열 혼합 등의 변환을 반복하여 블록을 처리한다. Feistel 구조는 블록을 두 부분으로 나누고 한쪽의 연산 결과로 다른 쪽을 바꾸는 방식이라는 점에서 구별된다.

③ X: AES는 고성능 플랫폼에서만 쓰도록 복잡하게 고안된 암호가 아니다. **다양한 하드웨어·소프트웨어 환경에서 효율적으로 구현**할 수 있도록 설계되었으며, 처리 능력이나 메모리가 제한된 환경에서도 사용할 수 있다.

④ X: AES를 2001년에 공표한 기관은 IEEE가 아니라 **미국 국립표준기술연구소(NIST)**이다. NIST는 AES를 연방정보처리표준 FIPS 197로 공표하였다.

NoteBase

문 3. 침입탐지시스템(IDS)에 대한 설명으로 옳지 않은 것은?

① 호스트 기반 IDS와 네트워크 기반 IDS로 구분한다.

② 오용 탐지 방법은 알려진 공격 행위의 실행 절차 및 특징 정보를 이용하여 침입 여부를 판단한다.

③ 비정상 행위 탐지 방법은 일정 기간 동안 사용자, 그룹, 프로토콜, 시스템 등을 관찰하여 생성한 프로파일이나 통계적 임계치를 이용하여 침입 여부를 판단한다.

④ IDS는 방화벽처럼 내부와 외부 네트워크 경계에 위치해야 한다.

정답 4번

간단한 해설

IDS는 감시 대상에 따라 개별 호스트나 내부 네트워크에도 설치할 수 있으므로, **내부와 외부 네트워크의 경계에 반드시 위치해야 하는 것은 아니다**.

선지별 해설

① O: 감시 대상과 수집하는 정보를 기준으로 호스트 기반 IDS와 네트워크 기반 IDS로 구분할 수 있다. 호스트 기반 IDS는 **개별 호스트의 로그·파일 변경·시스템 활동** 등을 분석하고, 네트워크 기반 IDS는 네트워크 구간을 흐르는 패킷과 트래픽을 분석한다.

② O: 오용 탐지는 **알려진 공격의 특징과 일치하는지**를 판단하는 방식이다. 공격 행위의 실행 절차나 특징을 탐지 규칙 또는 서명으로 만들어 두고, 관찰한 활동이 이에 부합하면 침입으로 판단한다.

③ O: 비정상 행위 탐지는 일정 기간 관찰한 사용자·그룹·프로토콜·시스템 등의 정상 활동을 프로파일이나 통계적 기준으로 표현한다. 이후의 활동이 **정상 기준에서 벗어나는지**를 비교하여 침입 여부를 판단한다. 알려진 공격 특징과 대조하는 오용 탐지와 달리, 정상 행위로부터의 이탈이 판단 기준이다.

④ X: IDS의 설치 위치가 내부와 외부 네트워크의 경계로 한정되는 것은 아니다. **감시할 대상과 구간에 따라** 개별 서버나 PC에 호스트 기반 IDS를 설치하거나, 내부의 중요 네트워크 구간에 네트워크 기반 IDS를 배치할 수 있다. 따라서 '경계에 위치해야 한다'는 표현은 '감시 목적에 맞는 호스트나 네트워크 구간에 배치할 수 있다'로 고쳐야 한다.

NoteBase

문 4. RSA 암호 알고리즘에서 두 소수, $p = 17$, $q = 23$과 키 값 $e = 3$을 선택한 경우, 평문 $m = 8$에 대한 암호문 c로 옳은 것은?

① 121

② 160

③ 391

④ 512

정답 1번

간단한 해설

RSA 암호문은 평문을 공개지수만큼 거듭제곱한 뒤 **두 소수의 곱으로 나눈 나머지**이다. 이 문제에서는 $8^3 = 512$를 391로 나눈 나머지가 121이다.

계산 과정

모듈러스 계산: RSA에서 나머지 연산의 기준이 되는 모듈러스는 두 소수의 곱이다. 따라서 $n = pq = 17 \cdot 23 = 391$이다.

암호화 연산: 평문을 m, 공개지수를 e라 하면 암호문은 c=m^e n으로 구한다. 여기서 mod는 나눈 나머지를 뜻한다. 주어진 m = 8, e = 3을 대입하면 $8^3 = 512$이며, 이는 **나머지 연산 전의 중간값**이다.

나머지 계산: 512 = 391 × 1 + 121이므로 512를 391로 나눈 나머지는 121이다. 암호문은 거듭제곱한 값 자체가 아니라 **모듈러스를 기준으로 구한 나머지**이므로 c = 121이다.

계산된 암호문 121은 ①의 값과 일치한다.

NoteBase

문 5. IEEE 802.11i RSN(Robust Security Network)에 대한 설명으로 옳은 것은?

① TKIP는 확장형 인증 프레임워크이다.

② CCMP는 데이터 기밀성 보장을 위해 AES를 CTR 블록 암호 운용 모드로 이용한다.

③ EAP는 WEP로 구현된 하드웨어의 펌웨어 업데이트를 위해 사용한다.

④ 802.1X는 무결성 보장을 위해 CBC-MAC를 이용한다.

정답 2번

간단한 해설

CCMP는 AES를 **CTR 모드**로 사용하여 데이터를 암호화하고 기밀성을 보장한다. 같은 프로토콜에서 무결성 검증은 CBC-MAC가 담당한다.

선지별 해설

① X: 확장형 인증 프레임워크는 **EAP**이다. EAP는 여러 인증 방식을 수용할 수 있도록 인증 메시지 교환의 틀을 제공한다. TKIP는 기존 WEP 장비의 활용을 고려하여 설계된 데이터 기밀성·무결성 보호 프로토콜이다.

② O: CCMP는 AES를 기반으로 하며, **기밀성에는 CTR, 무결성에는 CBC-MAC**를 사용한다. CTR은 카운터 값을 AES로 암호화하여 얻은 비트열과 평문을 XOR하여 데이터를 암호화하므로, 선지의 AES와 CTR 모드의 연결이 성립한다.

③ X: EAP는 인증 프레임워크이며, WEP 장비를 펌웨어 갱신으로 보완하려는 취지에 해당하는 것은 **TKIP**이다. TKIP는 기존 WEP 장비의 암호 처리 기능을 활용하면서 보안을 강화하도록 설계되어, 이를 지원하는 장비는 펌웨어나 소프트웨어 갱신으로 적용할 수 있다.

④ X: 802.1X는 인증 결과에 따라 네트워크 이용을 제어하는 **포트 기반 접근제어** 표준이다. 인증 전에는 일반 데이터 통신을 제한하면서 인증 메시지를 교환할 수 있도록 한다. CBC-MAC로 데이터 무결성을 보호하는 것은 CCMP의 기능이다.

NoteBase

문 6. CC(Common Criteria) 인증 평가 단계를 순서대로 바르게 나열한 것은?

가. PP(Protection Profile) 평가
나. ST(Security Target) 평가
다. TOE(Target Of Evaluation) 평가

① 가→나→다
② 가→다→나
③ 나→가→다
④ 다→나→가

정답 1번

간단한 해설

PP에서 공통 보안 요구사항의 타당성을 확인한 뒤, ST에서 특정 평가 대상에 적용할 요구사항을 구체화한다. 실제 대상인 TOE는 **평가된 ST를 기준으로** 요구사항 충족 여부를 확인한다.

올바른 순서

가 → 나 → 다

가. PP(보호프로파일) 평가: PP는 특정 제품군에 공통으로 필요한 보안 요구사항을 기술한 문서이다. 요구사항이 빠짐없이 제시되고 서로 모순되지 않으며 기술적으로 타당한지 평가한다. 이 문항처럼 PP를 활용하는 평가에서는 **검증된 공통 요구사항**이 이후 ST의 기초가 된다.

나. ST(보안목표명세서) 평가: ST는 특정 평가 대상의 보안목표와 보안 요구사항 등을 기술한 문서이다. 적용하는 PP의 요구사항을 적절히 반영했는지, 문서가 완전하고 일관되며 기술적으로 타당한지 확인한다. 실제 제품을 평가하려면 **그 제품에 적용할 평가 기준**이 먼저 적절하게 정해져 있어야 하므로 TOE 평가보다 앞선다.

다. TOE(평가 대상) 평가: TOE는 평가를 받는 실제 IT 제품이나 시스템이다. 평가된 ST를 기준으로 설계·구현 자료, 시험 결과 등을 검토하여 **명시된 보안 요구사항을 충족하는지** 확인한다. 앞 단계가 요구사항을 담은 문서의 타당성을 평가했다면, 이 단계는 그 요구사항을 실제 대상이 구현했는지 평가한다.

NoteBase

문 7. SQL 삽입 공격에 대한 설명으로 옳지 않은 것은?

① 사용자 요청이 웹 서버의 애플리케이션을 거쳐 데이터베이스에 전달되고 그 결과가 반환되는 구조에서 주로 발생한다.

② 공격이 성공하면 데이터베이스에 무단 접근하여 자료를 유출하거나 변조시키는 결과가 초래될 수 있다.

③ 사용자의 입력값으로 웹 사이트의 SQL 질의가 완성되는 약점을 이용한 것이다.

④ 자바스크립트와 같은 CSS(Client Side Script) 기반 언어로 사용자 입력을 필터링하는 방법으로 공격에 대응하는 것이 바람직하다.

정답 4번

간단한 해설

브라우저에서 실행되는 자바스크립트 필터링은 우회할 수 있으므로 SQL 삽입 공격의 충분한 방어책이 되지 못한다. **서버에서 입력값을 검증**하고, **매개변수화된 질의**로 SQL 명령과 입력 데이터를 분리해야 한다.

선지별 해설

① O: 웹 애플리케이션은 사용자 요청을 받아 SQL 질의를 데이터베이스에 보내고, 처리 결과를 사용자에게 반환한다. 이 과정에서 입력값이 안전하게 처리되지 않으면 공격자가 보낸 내용이 SQL 명령의 일부로 실행될 수 있다. 따라서 **웹 애플리케이션이 데이터베이스와 연동되는 구조**는 SQL 삽입 공격이 발생하는 대표적인 환경이다.

② O: SQL 삽입 공격이 성공하면 애플리케이션이 의도하지 않은 질의가 실행될 수 있다. 이에 따라 비공개 자료를 조회·유출하거나 데이터를 수정·삭제하는 피해가 발생할 수 있다. 실제 피해 범위는 취약한 질의와 **애플리케이션의 데이터베이스 접근 권한** 등에 따라 달라진다.

③ O: 입력값을 SQL 문자열에 그대로 이어 붙여 질의를 만들면, 입력에 포함된 SQL 구문이 단순한 데이터가 아니라 **명령의 일부로 해석**될 수 있다. SQL 삽입 공격은 이 약점을 이용해 질의의 조건이나 동작을 바꾼다. 사용자 입력을 받는 것 자체가 아니라, 입력 데이터와 SQL 명령을 안전하게 구분하지 않는 것이 문제이다.

④ X: 자바스크립트 등 클라이언트 측 스크립트는 사용자의 브라우저에서 실행되므로, 공격자가 실행을 중단하거나 브라우저의 필터를 거치지 않은 요청을 서버에 직접 보내 우회할 수 있다. 따라서 클라이언트 측 필터링에 의존해서는 안 된다. **서버 측 입력값 검증**을 수행하고, 준비된 문장과 매개변수 바인딩을 사용해 **SQL 명령과 입력 데이터를 분리**하는 방식으로 대응해야 한다.

NoteBase

문 8. 유닉스/리눅스의 파일 접근 제어에 대한 설명으로 옳지 않은 것은?

① 접근 권한 유형으로 읽기, 쓰기, 실행이 있다.

② 파일에 대한 접근 권한은 소유자, 그룹, 다른 모든 사용자에 대해 각각 지정할 수 있다.

③ 파일 접근 권한 변경은 파일에 대한 쓰기 권한이 있으면 가능하다.

④ SetUID가 설정된 파일은 실행 시간 동안 그 파일의 소유자의 권한으로 실행된다.

정답 3번

간단한 해설

파일의 **쓰기 권한은 내용 수정 권한**이며, 접근 권한 자체를 바꿀 수 있다는 뜻은 아니다. 접근 권한 변경은 파일 소유자 또는 필요한 특권을 가진 사용자에게 허용된다.

선지별 해설

① O: 기본 파일 접근 권한은 읽기(r), 쓰기(w), 실행(x)이다. 일반 파일에서 읽기는 내용을 확인하는 권한, 쓰기는 내용을 수정하는 권한, 실행은 프로그램으로 실행하는 권한이다.

② O: 파일의 기본 접근 권한은 **소유자·그룹·기타 사용자**의 세 범주에 각각 지정한다. 여기서 그룹은 파일이 속한 그룹의 다른 사용자이고, 기타 사용자는 소유자도 해당 그룹의 구성원도 아닌 사용자이다. 각 범주에 읽기·쓰기·실행 권한을 다르게 부여할 수 있다.

③ X: 파일의 쓰기 권한만으로는 접근 권한을 변경할 수 없다. chmod로 접근 권한을 변경하려면 **파일 소유자이거나 필요한 특권을 가져야 한다**. 예를 들어 소유자가 아닌 일반 사용자에게 쓰기 권한을 주면 그 사용자는 파일 내용을 수정할 수 있지만, 그 사실만으로 읽기·쓰기·실행 권한의 설정까지 바꿀 수는 없다.

④ O: SetUID는 실행 파일을 실행할 때 프로세스의 **유효 사용자 ID(EUID)를 파일 소유자의 ID로 설정**하는 기능이다. 따라서 SetUID가 적용되는 실행에서는 실행한 사용자가 아니라 파일 소유자의 권한을 기준으로 접근 권한을 판단한다. 이는 실행한 사용자의 계정 자체가 파일 소유자의 계정으로 바뀐다는 뜻은 아니다.

NoteBase

문 9. IPSec에 대한 설명으로 옳지 않은 것은?

① 전송(transport) 모드에서는 전송 계층에서 온 데이터만을 보호하고 IP 헤더는 보호하지 않는다.

② 인증 헤더(Authentication Header) 프로토콜은 발신지 호스트를 인증하고 IP 패킷으로 전달되는 페이로드의 무결성을 보장하기 위해 설계되었다.

③ 보안상 안전한 채널을 만들기 위한 보안 연관(Security Association)은 양방향으로 통신하는 호스트 쌍에 하나만 존재한다.

④ 일반적으로 호스트는 보안 연관 매개변수들을 보안 연관 데이터베이스에 저장하여 사용한다.

정답 3번

간단한 해설

보안 연관(SA)은 **단방향**으로 보안 서비스를 제공하는 논리적 연결이다. 따라서 양방향 통신을 보호하려면 송신 방향과 수신 방향에 각각 SA를 설정하여 **최소 2개**가 필요하다.

선지별 해설

① O: **ESP 전송 모드를 기준으로 하면** TCP·UDP 헤더와 그 뒤의 데이터를 보호하고, 원래 IP 헤더는 보호 범위에 포함하지 않는다. IP 헤더까지 포함한 원래 IP 패킷을 감싸는 터널 모드와 구별된다. 다만 AH 전송 모드는 IP 헤더의 일부 필드도 인증하므로, 'IP 헤더는 보호하지 않는다'는 표현을 모든 전송 모드에 그대로 일반화해서는 안 된다.

② O: AH는 **데이터 출처 인증과 무결성**을 제공한다. 수신자는 인증값을 검증하여 패킷이 해당 SA의 상대방에게서 왔는지, 페이로드가 전송 중 변조되었는지 확인한다. AH 자체는 데이터를 암호화하지 않으므로 기밀성을 제공하지 않는다.

③ X: SA는 사용할 보안 알고리즘과 키 등의 매개변수를 정하여 한 방향의 트래픽에 보안 서비스를 제공하는 연결이다. A에서 B로 보내는 트래픽을 위한 SA와 B에서 A로 보내는 트래픽을 위한 SA는 별개이다. 따라서 '호스트 쌍에 하나만 존재한다'가 아니라, **양방향 통신에는 방향별 SA가 최소 2개 필요하다**고 고쳐야 한다.

④ O: 호스트는 각 SA의 매개변수를 **보안 연관 데이터베이스(SAD)**에 저장한다. SAD에는 보안 매개변수 인덱스(SPI), 적용할 암호화·인증 알고리즘과 키, 순서 번호, SA 수명 등이 포함된다. 호스트는 해당 SA의 정보를 참조하여 패킷을 암호화하거나 수신 패킷을 검증한다.

NoteBase

문 10. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제25조(침해사고 등의 통지 등), 제26조(이용자 보호 등을 위한 정보 공개), 제27조(이용자 정보의 보호)에 명시된 것으로 옳지 않은 것은?

① 클라우드컴퓨팅서비스 제공자는 이용자 정보가 유출된 때에는 즉시 그 사실을 과학기술정보통신부장관에게 알려야 한다.

② 이용자는 클라우드컴퓨팅서비스 제공자에게 이용자 정보가 저장되는 국가의 명칭을 알려 줄 것을 요구할 수 있다.

③ 클라우드컴퓨팅서비스 제공자는 법원의 제출명령이나 법관이 발부한 영장에 의하지 아니하고는 이용자의 동의 없이 이용자 정보를 제3자에게 제공하거나 서비스 제공 목적 외의 용도로 이용할 수 없다.
클라우드컴퓨팅서비스 제공자로부터 이용자 정보를 제공받은 제3자도 또한 같다.

④ 클라우드컴퓨팅서비스 제공자는 이용자와의 계약이 종료되었을 때에는 이용자에게 이용자 정보를 반환하여야 하고 클라우드컴퓨팅서비스 제공자가 보유하고 있는 이용자 정보를 파기할 수 있다.

정답 4번

①

클라우드컴퓨팅서비스 제공자는 이용자 정보가 유출되면 **즉시 과학기술정보통신부장관에게 그 사실을 알려야 한다**. 제25조 제1항 제2호가 정보 유출을 통지 사유로 정하고 제2항이 장관 통지를 연결한다. 해당 이용자에게는 '지체 없이', 장관에게는 '즉시' 알려야 한다는 점을 구별한다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제25조 제2항
클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제25조(침해사고 등의 통지 등)
② 클라우드컴퓨팅서비스 제공자는 제1항제2호에 해당하는 경우에는 즉시 그 사실을
과학기술정보통신부장관에게 알려야 한다. <개정 2017.7.26>

②

이용자는 클라우드컴퓨팅서비스 제공자에게 **이용자 정보가 저장되는 국가의 명칭을 알려 달라고 요구할 수 있다**. 제26조 제1항이 이용자에게 부여한 정보공개 요구권으로, 선지는 요구 주체인 이용자·상대방인 제공자·대상인 저장 국가명을 정확히 제시한다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제26조 제1항
클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제26조(이용자 보호 등을 위한 정보 공개)
① 이용자는 클라우드컴퓨팅서비스 제공자에게 이용자 정보가 저장되는 국가의 명칭을 알려 줄 것을 요구할 수 있다.

NoteBase

③

법원의 제출명령이나 법관이 발부한 영장에 의한 경우가 아니라면, **이용자 동의 없이 이용자 정보를 제3자에게 제공하거나 서비스 제공 목적 외로 이용할 수 없다**. 정보를 제공받은 제3자에게도 같은 제한이 적용된다. 제27조 제1항은 제공자의 정보 제공·이용 단계뿐 아니라 정보를 받은 제3자의 이후 이용에도 같은 제한을 두는 구조이다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제27조 제1항
클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제27조(이용자 정보의 보호)
① 클라우드컴퓨팅서비스 제공자는 법원의 제출명령이나 법관이 발부한 영장에 의하지 아니하고는 이용자의 동의 없이 이용자 정보를 제3자에게 제공하거나 서비스 제공 목적 외의 용도로 이용할 수 없다.
클라우드컴퓨팅서비스 제공자로부터 이용자 정보를 제공받은 제3자도 또한 같다.

④

계약으로 특별히 다르게 정한 경우를 제외하면, 계약 종료 시 이용자 정보를 반환하고 **제공자가 보유한 이용자 정보는 파기하여야 한다**. 파기는 임의사항이 아니며, 사실상 반환이 불가능한 경우에도 파기하여야 한다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제27조 제3항, 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제27조 제5항
클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제27조(이용자 정보의 보호)
③ 클라우드컴퓨팅서비스 제공자는 이용자와의 계약이 종료되었을 때에는 이용자에게 이용자 정보를 반환하여야 하고 클라우드컴퓨팅서비스 제공자가 보유하고 있는 이용자 정보를 파기하여야 한다. 다만, 이용자가 반환받지 아니하거나 반환을 원하지 아니하는 등의 이유로 사실상 반환이 불가능한 경우에는 이용자 정보를 파기하여야 한다.
⑤ 제3항 및 제4항에도 불구하고 클라우드컴퓨팅서비스 제공자와 이용자 간의 계약으로 특별히 다르게 정한 경우에는 그에 따른다.

NoteBase

문 11. 인증기관이 사용자의 공개키에 대한 인증을 수행하기 위해 X.509 형식의 인증서를 생성할 때 서명에 사용하는 키는?

① 인증기관의 공개키
② 인증기관의 개인키
③ 사용자의 개인키
④ 인증기관과 사용자 간의 세션키

정답 2번

간단한 해설

X.509 인증서에는 사용자의 공개키가 들어가지만, 이를 보증하는 서명은 **인증기관의 개인키**로 생성한다. 서명 검증에는 그와 짝을 이루는 인증기관의 공개키를 사용한다.

핵심 풀이

인증서 서명: X.509 인증서는 사용자의 신원과 공개키를 연결하는 전자문서이다. 인증기관은 사용자 공개키 등을 포함한 인증서 정보에 **자신의 개인키로 전자서명**하여 그 연결을 보증한다. 인증받는 공개키의 소유자는 사용자이지만, 인증서를 발급하고 서명하는 주체는 인증기관이다.

서명 검증: 인증서를 받은 쪽은 **인증기관의 공개키**로 서명을 검증한다. 따라서 인증기관의 개인키는 서명 생성에, 인증기관의 공개키는 서명 검증에 쓰인다는 차이가 있다.

다른 키와의 구분: 사용자의 개인키는 사용자가 자신의 전자서명을 생성할 때 쓰는 키이므로 인증기관의 인증서 서명에 사용하지 않는다. 세션키는 통신 세션에서 데이터를 암호화하는 데 쓰는 대칭키로, 인증기관의 전자서명을 생성하는 키가 아니다.

NoteBase

문 12. 하이브리드 암호 시스템에 대한 설명으로 옳지 않은 것은?

① 메시지는 대칭 암호 방식으로 암호화한다.

② 일반적으로 대칭 암호에 사용하는 세션키는 의사 난수 생성기로 생성한다.

③ 생성된 세션키는 무결성 보장을 위하여 공개키 암호 방식으로 암호화한다.

④ 메시지 송신자와 수신자가 사전에 공유하고 있는 비밀키가 없어도 사용할 수 있다.

정답 3번

간단한 해설

세션키를 공개키 암호 방식으로 암호화하는 목적은 **무결성이 아니라 기밀성**을 보장하는 데 있다. 수신자의 공개키로 암호화하면 대응하는 개인키를 가진 수신자가 세션키를 복원할 수 있다.

선지별 해설

① O: 하이브리드 암호 시스템은 대칭 암호와 공개키 암호를 결합한다. 실제 메시지는 **처리 속도가 빠른 대칭 암호**로 암호화하고, 그때 사용하는 세션키를 공개키 암호 방식으로 보호한다.

② O: 세션키는 해당 통신에서 메시지를 암호화하고 복호화하는 데 사용하는 대칭키이다. 공격자가 키를 예측하지 못하도록 일반적으로 **암호학적으로 안전한 의사 난수 생성기**로 생성한다. 단순히 난수처럼 보이는 값이 아니라 예측하기 어려운 값이어야 한다.

③ X: 세션키를 공개키 암호 방식으로 암호화하는 주된 목적은 **세션키의 기밀성 보장**이다. 송신자가 수신자의 공개키로 세션키를 암호화하면 수신자는 자신의 개인키로 이를 복호화한다. 따라서 '무결성 보장을 위하여'는 '기밀성 보장을 위하여'로 고쳐야 한다. 무결성은 데이터가 변조되지 않았는지를 확인하는 성질로, 암호화했다는 사실만으로 보장되지 않는다.

④ O: 송신자는 수신자의 공개키로 세션키를 암호화하여 전달할 수 있으므로 **사전에 공유한 비밀키 없이도** 사용할 수 있다. 수신자는 자신의 개인키로 세션키를 얻은 뒤 메시지를 복호화한다. 다만 공개키가 실제 수신자의 것인지는 신뢰할 수 있는 방법으로 확인해야 한다.

NoteBase

문 13. 해시함수의 충돌저항성을 위협하는 공격 방법은?

① 생일 공격

② 사전 공격

③ 레인보우 테이블 공격

④ 선택 평문 공격

정답 1번

간단한 해설

생일 공격은 여러 입력의 해시값을 비교하여 **같은 해시값을 갖는 서로 다른 두 입력**을 찾는다. 이는 충돌을 찾기 어려워야 한다는 **충돌저항성**을 직접 위협한다.

개념 구분

충돌저항성과 생일 공격: 충돌은 서로 다른 두 입력에서 같은 해시값이 나오는 현상이며, 충돌저항성은 이런 입력 쌍을 찾기가 계산상 어려워야 한다는 성질이다. 생일 공격은 많은 입력의 해시값을 구한 뒤 **가능한 모든 쌍 사이의 일치 여부**를 이용해 충돌을 찾는다. 입력이 늘면 비교할 쌍의 수가 빠르게 증가한다는 생일 역설을 이용하므로, 특정 해시값과 일치하는 입력 하나를 찾는 방식보다 적은 시도로 충돌을 찾을 수 있다.

사전 공격과 레인보우 테이블 공격: 사전 공격은 자주 쓰이는 비밀번호 등의 후보를 대입하여 확인하고, 레인보우 테이블 공격은 미리 계산한 해시·축약 함수의 연쇄 정보를 이용해 해시값에 대응하는 비밀번호 후보를 찾는다. 주된 목표는 **주어진 해시값에 대응하는 입력을 찾는 것**으로, 임의의 두 입력 사이에서 충돌을 찾는 생일 공격과 구별된다.

선택 평문 공격: 공격자가 선택한 평문에 대응하는 암호문을 얻어 암호체계를 분석하는 공격이다. 이는 **평문과 암호문의 대응 관계**를 이용하는 방식으로, 해시값이 같은 입력 쌍을 찾는 공격과 다르다.

NoteBase

문 14. 블록 암호 운용 모드에 대한 설명으로 옳지 않은 것은?

① CFB는 블록 암호화를 병렬로 처리할 수 없다.

② ECB는 IV(Initialization Vector)를 사용하지 않는다.

③ CBC는 암호문 블록에 오류가 발생한 경우 복호화 시 해당 블록만 영향을 받는다.

④ CTR는 평문 블록마다 서로 다른 카운터 값을 사용하여 암호문 블록을 생성한다.

정답 3번

간단한 해설

CBC에서 암호문 블록에 비트 오류가 생기면 **해당 평문 블록과 다음 평문 블록**에 영향을 준다. 해당 블록을 복호화할 때뿐 아니라 다음 블록을 복호화할 때도 그 암호문 블록을 사용하기 때문이다.

선지별 해설

① O: CFB는 생성한 암호문을 다음 암호화의 입력에 되먹임한다. 따라서 다음 암호문을 만들려면 앞선 암호문이 먼저 생성되어야 하므로 **암호화는 병렬 처리할 수 없다**. 복호화는 필요한 암호문이 이미 주어져 있으면 병렬 처리가 가능하므로 암호화와 구별해야 한다.

② O: ECB는 각 평문 블록을 같은 키로 독립적으로 암호화하며 **IV를 사용하지 않는다**. 앞선 암호문이나 별도의 초기값을 입력에 결합하지 않으므로, 같은 키로 같은 평문 블록을 암호화하면 같은 암호문 블록이 나온다.

③ X: CBC의 복호화는 현재 암호문 블록을 복호화한 결과와 직전 암호문 블록을 XOR하여 평문을 복원한다. 따라서 한 암호문 블록에 비트 오류가 생기면 해당 평문 블록에 오류가 퍼지고, 다음 평문 블록이 있다면 그 블록에서도 같은 비트 위치에 오류가 생긴다. 오류의 영향은 '해당 블록만'이 아니라 **해당 블록과 다음 블록까지**이며, 그 이후 블록에는 이 비트 오류가 전파되지 않는다.

④ O: CTR는 평문 블록마다 **서로 다른 카운터 값**을 암호화하여 키스트림을 만들고, 이를 해당 평문 블록과 XOR하여 암호문을 생성한다. 각 블록의 입력이 이전 암호문에 의존하지 않으므로 암호화를 병렬 처리할 수 있다.

NoteBase

문 15. 「개인정보 보호법」상 공개된 장소에 영상정보처리기기를 설치·운영할 수 있는 경우가 아닌 것은?

① 범죄의 예방 및 수사를 위하여 필요한 경우
② 공공기관의 장이 허가한 경우
③ 교통정보의 수집·분석 및 제공을 위하여 필요한 경우
④ 시설안전 및 화재 예방을 위하여 필요한 경우

정답 2번

①

범죄의 예방 및 수사를 위하여 필요한 경우에는 공개된 장소에 고정형 영상정보처리기기를 설치·운영할 수 있다.

개인정보 보호법 제25조 제1항 제2호
개인정보 보호법 제25조(고정형 영상정보처리기기의 설치 · 운영 제한)
① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 고정형 영상정보처리기기를 설치 · 운영하여서는 아니 된다. <개정 2023.3.14>
2. 범죄의 예방 및 수사를 위하여 필요한 경우

②

공공기관장의 허가만으로는 설치·운영할 수 없다. 범죄 예방·수사 등 법률에 열거된 허용 사유에 해당해야 한다.

개인정보 보호법 제25조 제1항
개인정보 보호법 제25조(고정형 영상정보처리기기의 설치 · 운영 제한)
① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 고정형 영상정보처리기기를 설치 · 운영하여서는 아니 된다. <개정 2023.3.14>
1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설의 안전 및 관리, 화재 예방을 위하여 정당한 권한을 가진 자가 설치 · 운영하는 경우
4. 교통단속을 위하여 정당한 권한을 가진 자가 설치 · 운영하는 경우
5. 교통정보의 수집 · 분석 및 제공을 위하여 정당한 권한을 가진 자가 설치 · 운영하는 경우
6. 촬영된 영상정보를 저장하지 아니하는 경우로서 대통령령으로 정하는 경우

NoteBase

③

교통정보의 수집·분석 및 제공은 설치·운영이 허용되는 목적이다. 이 목적으로는 **정당한 권한을 가진 자가 설치·운영해야 한다.**

개인정보 보호법 제25조 제1항 제5호
개인정보 보호법 제25조(고정형 영상정보처리기기의 설치 · 운영 제한)
① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 고정형 영상정보처리기기를 설치 · 운영하여서는 아니 된다. <개정 2023.3.14>
5. 교통정보의 수집 · 분석 및 제공을 위하여 정당한 권한을 가진 자가 설치 · 운영하는 경우

④

시설의 안전 및 관리, 화재 예방은 설치·운영이 허용되는 목적이다. 이 목적으로는 **정당한 권한을 가진 자가 설치·운영해야 한다.**

개인정보 보호법 제25조 제1항 제3호
개인정보 보호법 제25조(고정형 영상정보처리기기의 설치 · 운영 제한)
① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 고정형 영상정보처리기기를 설치 · 운영하여서는 아니 된다. <개정 2023.3.14>
3. 시설의 안전 및 관리, 화재 예방을 위하여 정당한 권한을 가진 자가 설치 · 운영하는 경우

NoteBase

문 16. SMTP 클라이언트가 SMTP 서버의 특정 사용자를 확인함으로써 계정 존재 여부를 파악하는 데 악용될 수 있는 명령어는?

① HELO

② MAIL FROM

③ RCPT TO

④ VRFY

정답 4번

간단한 해설

VRFY는 SMTP 서버에 **특정 사용자나 메일함이 존재하는지 확인**하도록 요청하는 명령어이다. 서버가 확인 결과를 알려 주면 공격자가 이를 이용해 유효한 계정을 알아낼 수 있다.

핵심 풀이

VRFY: 지정한 문자열이 사용자나 메일함을 가리키는지 서버에 확인을 요청한다. 서버가 사용자 정보나 메일 주소를 응답하면 **계정의 존재 여부가 드러날 수 있다**. 따라서 문제의 '특정 사용자를 확인'한다는 단서는 VRFY에 해당한다.

RCPT TO: 메일을 전송할 때 **수신자를 지정**하는 명령어이다. 사용자 확인 자체를 요청하는 VRFY와는 명령의 목적이 다르다.

NoteBase

문 17. 다음 법 조문의 출처는?

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.

① 국가정보화 기본법

② 개인정보 보호법

③ 정보통신망 이용촉진 및 정보보호 등에 관한 법률

④ 정보통신산업진흥법

정답 3번

공통 해설

제시된 정보보호 관리체계 인증의 근거는 **정보통신망 이용촉진 및 정보보호 등에 관한 법률**이다.
관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계가 인증기준에 적합한지를
과학기술정보통신부장관이 인증할 수 있도록 규정한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조 제1항
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. <개정 2012.2.17, 2013.3.23, 2015.12.1, 2017.7.26>

NoteBase

문 18. 위조된 출발지 주소에서 과도한 양의 TCP SYN 패킷을 공격 대상 시스템으로 전송하는 서비스 거부 공격에 대응하기 위한 방안의 하나인, SYN 쿠키 기법에 대한 설명으로 옳은 것은?

① SYN 패킷이 오면 세부 정보를 TCP 연결 테이블에 기록한다.

② 요청된 연결의 중요 정보를 암호화하고 이를 SYN-ACK 패킷의 응답(acknowledgment) 번호로 하여 클라이언트에게 전송한다.

③ 클라이언트가 SYN 쿠키가 포함된 ACK 패킷을 보내오면 서버는 세션을 다시 열고 통신을 시작한다.

④ TCP 연결 테이블에서 연결이 완성되지 않은 엔트리를 삭제하는 데까지의 대기 시간을 결정한다.

정답 3번

간단한 해설

SYN 쿠키 기법은 SYN 수신 즉시 연결 정보를 저장하지 않고, **쿠키가 반영된 ACK를 받아 유효성을 확인한 뒤** 연결 상태를 복원한다. 따라서 위조된 SYN만 대량으로 들어와도 미완성 연결 정보가 계속 쌓이는 것을 막는다.

선지별 해설

① X: 일반적인 TCP 연결 처리에서는 SYN을 받으면 미완성 연결 정보를 저장하지만, SYN 쿠키 기법은 이로 인한 자원 고갈을 막기 위해 **SYN 수신 단계에서는 연결별 상태를 저장하지 않는다**. 필요한 정보를 쿠키에 담아 보내고, 유효한 ACK가 돌아온 뒤 연결 테이블에 상태를 만든다.

② X: SYN 쿠키는 SYN-ACK 패킷의 응답 번호가 아니라 **서버의 초기 순서 번호(sequence number)**에 넣는다. SYN-ACK의 응답 번호는 클라이언트가 보낸 SYN의 순서 번호에 1을 더한 값이다. 쿠키는 연결 정보와 비밀값 등을 이용한 암호학적 해시 등의 방식으로 생성하므로, 단순히 연결 정보를 암호화하여 응답 번호에 넣는다는 설명은 부정확하다.

③ O: 클라이언트는 SYN-ACK을 받으면 서버의 순서 번호, 즉 쿠키에 1을 더한 값을 ACK의 응답 번호로 보낸다. 서버는 이 값에서 쿠키를 확인하고, **유효한 쿠키이면 연결 상태를 복원하여** TCP 연결을 완성하고 통신을 시작한다. 선지의 '세션을 다시 열고'는 이처럼 미리 저장하지 않았던 연결 상태를 구성한다는 의미이다.

④ X: 미완성 연결 엔트리를 삭제하기까지 기다리는 시간을 조정하는 것은 **미완성 연결의 타임아웃 조정**에 관한 설명이다. 대기 시간을 줄이면 해당 엔트리가 더 빨리 제거된다. SYN 쿠키 기법의 핵심은 삭제 시간을 정하는 데 있지 않고, 유효한 ACK가 오기 전에는 연결별 상태를 저장하지 않는 데 있다.

NoteBase

문 19. ISO/IEC 27001:2013 보안관리 항목을 PDCA 모델에 적용할 때, 점검(check)에 해당하는 항목은?

① 성과평가(performance evaluation)

② 개선(improvement)

③ 운영(operation)

④ 지원(support)

정답 1번

간단한 해설

점검(Check)은 정보보호 활동의 결과를 측정·분석하여 관리체계가 제대로 작동하는지 확인하는 단계이다. ISO/IEC 27001:2013의 **성과평가**가 이에 해당하며, 평가 결과에 따라 문제를 고치는 개선은 조치(Act)에 해당한다.

개념 구분

성과평가(performance evaluation): ISO/IEC 27001:2013의 9절로, 모니터링·측정·분석 및 평가, 내부감사, 경영검토를 포함한다. 정보보호 활동이 요구사항을 충족하고 관리체계가 효과적으로 작동하는지 **결과를 확인·평가**하므로 PDCA의 점검(Check)에 해당한다.

개선(improvement): 10절로, 부적합에 대한 시정조치와 지속적 개선을 다룬다. 점검에서 발견한 문제의 원인을 제거하고 관리체계를 더 나아지게 하는 **조치(Act)**에 해당한다. 성과를 평가하는 것과 그 평가를 바탕으로 바꾸는 것을 구분한다.

운영(operation): 8절로, 계획한 프로세스를 실행·통제하고 정보보호 위험평가와 위험처리를 수행한다. 계획을 실제 활동으로 옮기는 **실행(Do)**에 해당한다.

지원(support): 7절로, 자원·역량·인식·의사소통·문서화된 정보 등 관리체계를 유지하는 데 필요한 기반을 제공한다. 활동의 성과를 점검하는 항목과는 역할이 다르다.

NoteBase

문 20. 다음에서 설명하는 블록체인 합의 알고리즘은?

◯ 비트코인에서 사용하는 방식이 채굴 경쟁으로 과도한 자원 소비를 발생시킨다는 문제를 해결하기 위한 대안으로 등장하였다.
◯ 채굴 성공 기회를 참여자에 따라 차등적으로 부여한다.
◯ 다수결로 의사 결정을 해서 블록을 추가하는 방식이 아니므로 불특정 다수가 참여하는 환경에서 유효하다.

① Paxos
② PoW(Proof of Work)
③ PoS(Proof of Stake)
④ PBFT(Practical Byzantine Fault Tolerance)

정답 3번

간단한 해설

채굴을 위한 연산 경쟁 대신 **암호화폐 지분에 따라 블록 생성 기회를 부여**하는 방식은 PoS(지분 증명)이다. 연산 능력을 높이기 위한 경쟁을 줄여 PoW의 과도한 자원 소비 문제를 완화한다.

핵심 풀이

자원 소비: 비트코인의 PoW(작업 증명)는 조건을 만족하는 해시값을 찾는 연산 경쟁을 통해 블록 생성자를 정한다. 참여자는 성공 가능성을 높이려고 연산 장비와 전력을 투입하므로 자원 소비가 커진다. PoS는 이 경쟁을 **지분을 바탕으로 한 생성자 선정**으로 대체하여 에너지 소비를 줄인다.

생성 기회의 차등 부여: PoS(Proof of Stake)는 참여자가 보유하거나 예치한 암호화폐 지분을 기준으로 블록 생성 기회나 합의 영향력을 부여하는 방식이다. 따라서 제시문의 '채굴 성공 기회'는 연산 문제를 먼저 푸는 기회가 아니라 **지분에 따라 달라지는 블록 생성 기회**를 뜻한다. 이것이 PoW와 구별되는 결정적 단서이다.

불특정 다수의 참여: 참여자 수만 세어 의사 결정을 하면 한 사람이 여러 신원을 만들어 영향력을 늘릴 수 있다. PoS는 신원의 수 대신 지분을 기준으로 영향력을 부여하므로 이러한 조작을 억제하며 공개된 참여 환경에 적용할 수 있다. 제시문의 '다수결이 아니다'는 **참여자 수에 따른 단순 다수결이 아니다**라는 의미로 이해해야 한다. PoS에서도 지분 가중치를 반영한 투표 절차를 사용할 수 있으므로 투표 자체가 없다는 뜻은 아니다.

NoteBase