2015년 지방직 9급 정보보호론 풀이

by 호이호이꿀떡

정답 체크

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

문 1. 인터넷 보안 프로토콜에 해당하지 않는 것은?

① SSL ② HTTPS
③ S/MIME ④ TCSEC

답 ④

④ **TCSEC**(Trusted Computer System Evaluation Criteria)
미국의 정보보호 시스템 평가 제도
컴퓨터시스템의 구축과 평가 등에 관한 지속적인 연구 결과로 미국 국방부 내 NCSC(미국 컴퓨터 보안 센터) 주도하에 1983년에 제정되었으며, 소위 'Orange Book'으로 불린다.

<오답 체크> ① **SSL**(Secure Sockets Layer, 보안 소켓 레이어) 또는 **TLS**(Transport Layer Security, 전송 계층 보안)
응용 계층과 전송 계층 사이 통신 과정에서 종단간 보안과 데이터 무결성을 제공하는 보안 프로토콜
클라이언트와 서버 간 상호 인증과 기밀성과 무결성 서비스를 제공

② **HTTPS**(Hypertext Transfer Protocol over Secure Socket Layer)
HTTP에 인증과 암호화를 사용해 보안이 강화된 버전으로 전자상거래에서 널리 쓰인다.
HTTPS는 소켓 통신에서 일반 텍스트를 이용하는 대신에, SSL이나 TLS 프로토콜을 통해 세션 데이터를 암호화한다.

③ **S/MIME**(Secure/Multipurpose Internet Mail Extension)
MIME를 보호하기 위한 보안 기술로, RSA를 이용하고 인증기관 필요로 한다.

문 2. 데이터 소유자가 다른 사용자의 식별자에 기초하여 자신의 의지대로 데이터에 대한 접근 권한을 부여하는 것은?

① 강제적 접근 제어(MAC)
② 임의적 접근 제어(DAC)
③ 규칙 기반 접근 제어(Rule-based AC)
④ 역할 기반 접근 제어(RBAC)

답 ②

② **임의적 접근 제어**(DAC, Discretionary Access Control)
정보의 소유자가 보안 등급을 결정하고 이에 대한 정보의 접근제어도 설정하는 모델이다.

<오답 체크>

①③ **강제적 접근 제어**(MAC, Mandatory Access Control)
오직 관리자만이 객체과 자원들에 대한 접근 권한을 부여할 수 있다. 자원에 대한 접근은 주어진 보안레벨에 기반한다.
관리자가 규칙을 작성하기 때문에 **규칙 기반 접근 제어**(Rule Based Access Control)이라고도 한다.

④ **역할 기반 접근 제어**(RBAC, Role Based Access Control)
정보에 대한 사용자의 접근을 개별적인 신분이 아니라 조직 내 개인 역할에 따라 허용 여부를 결정하는 모델이다.

문 3. 생체 인증 기법에 대한 설명으로 옳지 않은 것은?

① 정적인 신체적 특성 또는 동적인 행위적 특성을 이용할 수 있다.
② 인증 정보를 망각하거나 분실할 우려가 거의 없다.
③ 지식 기반이나 소유 기반의 인증 기법에 비해 일반적으로 인식 오류 발생 가능성이 매우 낮다.
④ 인증 시스템 구축 비용이 비교적 많이 든다.

답 ③

생제 인증 기술(바이오메트릭스, Biometrics)은 하나 이상의 고유한 신체적, 행동적 형질에 기반하여 사람을 인식하는 방식을 두루 가리킨다. 생체 인증 기술에 쓰이는 신체적 특성으로는 지문, 홍채, 얼굴, 정맥 등이 있으며 행동적 특성으로는 목소리, 서명 등이 있다.

③ 생체 인증 기법은 정확한 수치화가 어렵고 시간이나 환경의 변화에 따라 개인이 가진 생체 인증 정보가 변할 수 있기 때문에, 지식이나 소유 기반의 인증 기법에 비해 오류 발생 가능성이 높다.

문 4. 시스템 침투를 위한 일반적인 해킹 과정 중 마지막 순서에 해당 하는 것은?

① 공격
② 로그 기록 등의 흔적 삭제
③ 취약점 분석
④ 정보 수집

답 ②

② 해킹의 마지막 단계는 전문가에 따라 따르며,
로그 기록을 삭제한 뒤 백도어를 설치한다고 보는 견해도 있고, 백도어를 설치한 후 로그 기록을 삭제한다고 보는 견해도 있다.
따라서 선지에 로그 기록 삭제와 백도어 설치를 같이 내는 문제는 안 나올 것이다.

◈ 네트워크 해킹 과정
1. 정보 수집 단계(Foot printing)
2. 공격대상 스캔 단계(Scanning)
3. 계정 및 시스템 자원 수집 단계(Enumeration)
4. 접근 시도, 접근 권한(Gaining Access)
5. 시스템 권한 상승(Escalating Privilege)
6. 해킹에 필요한 추가적인 정보 수집(Pilfering)
7. 제어 권한 취득 후 로그 제거(Covering Track)
8. 지속적 악용을 위한 백도어 설치(Creating Backdoor)

문 5. 공개키를 사용하는 전자 서명에 대한 설명으로 옳지 않은 것은?

① 송신자는 자신의 개인키로 서명하고 수신자는 송신자의 공개키로 서명을 검증한다.
② 메시지의 무결성과 기밀성을 보장한다.
③ 신뢰할 수 있는 제3자를 이용하면 부인봉쇄를 할 수 있다.
④ 메시지로부터 얻은 일정 크기의 해시 값을 서명에 이용할 수 있다.

답 ②

② 전자 서명은 무결성만 보장할 뿐, 기밀성은 보장하지 않는다.
전사 서명은 개인키로 암호화(생성)를 하고 공개키로 복호화(검증)을 하기 때문에 누구나 복호화할 수 있으므로, 기밀성은 불가능하다.
전자 서명 문서에 기밀성을 보장받고 싶다면, 별도로 암호화를 진행해야 한다.

<오답 체크> ④ 전자 서명은 공개키 알고리즘을 이용하는데, 공개키 알고리즘은 속도가 느리다. 따라서 속도 저하를 방지하기 위해 메시지 원문이 아닌 해시값에 서명을 하는 방식이 널리 쓰인다.

문 6. 침입탐지시스템(IDS)의 탐지 기법 중 하나인 비정상행위(anomaly) 탐지 기법의 설명으로 옳지 않은 것은?

① 이전에 알려지지 않은 방식의 공격도 탐지가 가능하다.
② 통계적 분석 방법, 예측 가능한 패턴 생성 방법, 신경망 모델을 이용하는 방법 등이 있다.
③ 새로운 공격 유형이 발견될 때마다 지속적으로 해당 시그니처(signature)를 갱신해 주어야 한다.
④ 정상행위를 가려내기 위한 명확한 기준을 설정하기 어렵다.

답 ③

③ 발견된 공격 패턴을 DB에 등록해두는 건 오용 탐지에 대한 설명이다.
비정상 행위 탐지(이상 탐지)는 정상적인 패턴을 DB에 등록해둔다.

<오답 체크>

▶ **오용 탐지**(Misuse Detection)
= 시그니처 기반(Signature Base)
= 지식 기반(Knowledge Base)
이미 발견되고 정립된 공격 패턴을 미리 입력해 두고 그에 해당하는 패턴을 탐지
오탐율이 낮고 비교적 효율적이나 알려진 공격 이외는 탐지 불가능
전문가 시스템(Expert System)의 지식 DB를 이용한 IDS
Zero Day attack(제로 데이 공격)에 취약

▶ **이상 탐지**(Anomaly Detection IDS)
= 행위 기반(Behavior)
= 통계적 탐지(Statistical Detection)
정상 패턴을 DB에 등록해두고, 정상에서 벗어나는 행위를 탐지(임계치 설정)
알려지지 않은 공격인 제로 데이 공격(zero day attack) 탐지 가능
오탐율 높고, 임계치 설정이 어려움

문 7. 보안 해시 함수가 가져야 하는 성질 중 하나인 강한 충돌 저항성(strong collision resistance)에 대한 설명으로 옳은 것은?

① 주어진 해시 값에 대해, 그 해시 값을 생성하는 입력 값을 찾는 것이 어렵다.
② 주어진 입력 값과 그 입력 값에 해당하는 해시 값에 대해, 동일한 해시 값을 생성하는 다른 입력 값을 찾는 것이 어렵다.
③ 같은 해시 값을 생성하는 임의의 서로 다른 두 개의 입력 값을 찾는 것이 어렵다.
④ 해시 함수의 출력은 의사 난수이어야 한다.

답 ③

③ 강한 충돌 내성(strong collision resistance)
(= 충돌 회피성(collision freeness))
출력 해시값이 같은 임의의 서로 다른 두 메시지를 찾을 수 없다.

<오답 체크> ① 일방향성(onewayness)
② 약한 충돌 내성(weak collision resistance)
(= 제2 역상 저항성(second preimage resistance))
④ 컴퓨터에서 생성된 난수는 모두 의사 난수이다.
의사 난수는 진정한 의미에서의 난수는 아니지만 그 결과값을 추측하는 건 매우 어렵기 때문에 어느 정도 난수로 취급할 수 있는 문자열을 말한다.
의사 난수를 생성하기 위해 해시 함수 알고리즘을 이용하기도 한다.

문 8. 「전자서명법」상 공인인증기관이 발급하는 공인인증서에 포함되어야 하는 사항이 아닌 것은?

① 가입자의 전자서명검증정보
② 공인인증기관의 전자서명생성정보
③ 공인인증서의 유효기간
④ 공인인증기관의 명칭 등 공인인증기관임을 확인할 수 있는 정보

답 ②

② 전자서명생성정보는 개인키를 의미한다.
공인인증서에는 인증기관의 개인키가 포함되어 있는 것이 아니라, 인증기관의 개인키로 서명이 되어 있다.

「전자서명법」 제15조(공인인증서의 발급)
① 공인인증기관은 공인인증서를 발급받고자 하는 자에게 공인인증서를 발급한다. 이 경우 공인인증기관은 공인인증서를 발급받고자 하는 자의 신원을 확인하여야 한다.
② 공인인증기관이 발급하는 공인인증서에는 다음 각호의 사항이 포함되어야 한다.
1. 가입자의 이름(법인의 경우에는 명칭을 말한다)
2. 가입자의 전자서명검증정보
3. 가입자와 공인인증기관이 이용하는 전자서명 방식
4. 공인인증서의 일련번호
5. 공인인증서의 유효기간
6. 공인인증기관의 명칭 등 공인인증기관임을 확인할 수 있는 정보
7. 공인인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항
8. 가입자가 제3자를 위한 대리권 등을 갖는 경우 또는 직업상 자격등의 표시를 요청한 경우 이에 관한 사항
9. 공인인증서임을 나타내는 표시
③ 삭제
④ 공인인증기관은 공인인증서를 발급받고자 하는 자의 신청이 있는 경우에는 공인인증서의 이용범위 또는 용도를 제한하는 공인인증서를 발급할 수 있다.
⑤ 공인인증기관은 공인인증서의 이용범위 및 용도, 이용된 기술의 안전성과 신뢰성 등을 고려하여 공인인증서의 유효기간을 적정하게 정하여야 한다.
⑥ 공인인증서 발급에 따른 신원확인 절차 및 방법 등에 관하여 필요한 사항은 과학기술정보통신부령으로 정한다.

문 9. 사용자 A와 B가 Diffie-Hellman 키 교환 알고리즘을 이용하여 비밀키를 공유하고자 한다. A는 3을, B는 2를 각각의 개인키로 선택하고, A는 B에게 21(= 7^3 mod 23)을, B는 A에게 3(= 7^2 mod 23)을 전송한다면, A와 B가 공유하게 되는 비밀키 값은? (단, 소수 23과 그 소수의 원시근 7을 사용한다)

① 4 ② 5
③ 6 ④ 7

답 ①

A가 계산한 값 $3^3 \bmod 23 = 4$
B가 계산한 값 $21^2 \bmod 23 = 4$
공통의 비밀키 4를 갖게 된다.

◈ 디피 헬만 키 교환 순서
1. 앨리스가 충분히 큰 소수 p와 g를 선택하여 밥에게 전송한다. g는 1부터 p-1 사이의 수이다.
2. 앨리스가 정수 a를 선택한다. 이 정수는 외부에 공개되지 않으며, 밥 또한 알 수 없다.
3. 앨리스가 $A = g^a \bmod p$, 즉 g^a 를 p로 나눈 나머지를 계산한다.
4. 밥이 마찬가지로 정수 b를 선택하여 $B = g^b \bmod p$ 를 계산한다.
5. 앨리스와 밥이 서로에게A와 B를 전송한다.
6. 앨리스가 $B^a \bmod p$를, 밥이 $A^b \bmod p$를 계산한다.
   $B^a \bmod p = (g^b \bmod p)^a \bmod p = g^{ab} \bmod p$
   $A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p$ 으로 같으므로, 앨리스와 밥은 공통의 비밀키를 갖게 된다.

문 10. ISO 27001의 ISMS(Information Security Management System) 요구사항에 대한 내용으로 옳지 않은 것은?

① 자산 관리 : 정보 보호 관련 사건 및 취약점에 대한 대응
② 보안 정책 : 보안 정책, 지침, 절차의 문서화
③ 인력 자원 보안: 인력의 고용 전, 고용 중, 고용 만료 후 단계별 보안의 중요성 강조
④ 준거성 : 조직이 준수해야 할 정보 보호의 법적 요소

답 ①

① 정보보호 관련 사건과 취약점에 대한 대응은 정보보호 사고 관리 영역에 대한 설명이다.
자산 관리 영역은 조직의 자산을 파악하고 정보가 적절히 분류될 수 있도록 보장하는 단계이다.

문 11. 서비스 거부 공격 방법이 아닌 것은?

① ARP spoofing ② Smurf
③ SYN flooding ④ UDP flooding

답 ①

① **ARP spoofing**(ARP 스푸핑)
공격자가 자신의 MAC 주소를 공격 대상의 MAC 주소로 바꾸어 마치 자신이 공격 대상인 척 속이는 공격으로, 공격 대상자로 보내지는 패킷을 가로채 스니핑을 하는 것이 목적이다.
시스템 자원을 고갈시켜 정상적으로 이용하지 못하게 만드는 서비스 거부 공격(DoS, Denial of Service)과는 상관없다.

<오답 체크> ② **Smurf**(ICMP flooding)
공격대상 호스트의 IP주소로 위장된 소스 IP주소의 ICMP Echo 메시지를 브로드캐스트함으로써, 공격대상이 많은 양의 ICMP Echo 응답 패킷을 받아 시스템의 자원이 고갈되도록 만드는 공격이다.

③ **SYN Flooding**(SYN 플러딩)
TCP 3-way hancshaking을 이용한 DoS공격
공격 대상 서버에 무수히 많은 SYN패킷을 보낸 뒤, 서버로부터 오는 SYN+ACK패킷을 무시하여, 서버가 SYN Received 상태로 끊임없이 기다리게 만드는 공격방법이다.

④ **UDP Flooding**(Trinoo)
UDP 패킷을 이용한 DoS 공격

문 12. MS 오피스와 같은 응용 프로그램의 문서 파일에 삽입되어 스크립트 형태의 실행 환경을 악용하는 악성 코드는?

① 애드웨어 ② 트로이 목마
③ 백도어 ④ 매크로 바이러스

답 ④

④ **매크로 바이러스**(macro virus)
워드프로세서와 같은 응용 소프트웨어 안에서 실행되는 바이러스
일부 응용 프로그램은 작업의 편의를 위해 매크로 프로그램 기능을 포함하고 있는데, 문서가 실행될 때 매크로 바이러스도 실행될 수 있다.

<오답 체크> ① **애드웨어**(Adware)
광고를 포함한 소프트웨어를 말한다.
사용자에게 광고를 보여줌으로써 프로그래머는 소프트웨어 개발 비용을 충당할 수 있고, 사용자는 무료 또는 저렴한 가격으로 프로그램을 이용할 수 있게 만들어준다. 따라서 악성코드가 아닌 합법적인 애드웨어도 있다.
하지만 이러한 애드웨어가 무분별하게 사용자의 동의 없이 컴퓨터에 설치되어 광고 화면을 무분별하게 띄워 불편을 초래하는 악성코드가 될 수 있다.

② **트로이목마**(Trojan Horse)는 정상적인 프로그램으로 가장한 악성 프로그램으로, 다른 시스템으로 전파되지는 않는다. 트로이목마는 보통 해커들이 대상 컴퓨터의 인증이나 백신을 우회하여 시스템 내부에 침투하기 위해 사용한다.

③ **백도어**(Backdoor)는 인증 과정을 거치지 않고, 접근할 수 있도록 만든 비밀 통로이다. = 트랩도어(Trapdoor)

문 13. 데이터베이스 보안의 요구사항이 아닌 것은?

① 데이터 무결성 보장
② 기밀 데이터 관리 및 보호
③ 추론 보장
④ 사용자 인증

답 ③

③ 추론을 보장하는 게 아니고, 추론을 방지해야 한다.
추론 방지(inference control)
사용자가 외부에 보이는 일반적 데이터를 통해 숨겨둔 비밀정보를 획득하는 것을 추론이라 하는데, 이러한 추론을 불가능하도록 보호하는 것을 말한다.
<오답 체크> ① **데이터 무결성**(integrity)
부적절하게 데이터가 변경되지 않도록 하는 것
② **기밀성**(confidentiality)
부적절하게 데이터가 노출되는 것을 방지하는 것
④ **사용자 인증**(authentication)
정당한 상대방인지, 진짜인지 가짜인지를 확인하는 것
DBMS는 운영체제의 사용자 인증보다 엄격한 인증을 요구한다.

문 14. OSI 참조 모델의 제7계층의 트래픽을 감시하여 안전한 데이터만을 네트워크 중간에서 릴레이하는 유형의 방화벽은?

① 패킷 필터링(packet filtering) 방화벽
② 응용 계층 게이트웨이(application level gateway)
③ 스테이트풀 인스펙션(stateful inspection) 방화벽
④ 서킷 레벨 게이트웨이(circuit level gateway)

답 ②

② **응용 계층 게이트웨이**(Application Level Gateway)
OSI 참조 모델의 7계층 응용 계층에서 작동하는 방화벽으로, 프록시(proxy) 기능을 적용하여 내부와 외부 간의 응용 계층의 모든 트래픽에 대해 인증 기능을 제공
<오답 체크> ① **패킷 필터링 방화벽**(Packet filtering Firewall)
OSI 참조 모델 중 3계층 네트워크 계층과 4계층 전송 계층 사이에서 작동하며, 패킷의 출발지 및 목적지 IP 주소, 서비스의 포트 번호 등의 규칙을 설정하여 접속제어를 수행한다.
③ **스테이트풀 인스펙션**(stateful inspection) 방화벽
패킷 필터링 방화벽에 프로토콜의 상태정보 테이블을 유지하여, 프로토콜 특성에 따른 변화를 동적으로 대응해 주는 기능을 추가한 방화벽이다.
패킷 단위의 검사가 아닌 세션 단위의 검사를 한다.
④ **회로 레벨 게이트웨이**(Circuit Level Gateway)
패킷 필터와 어플리케이션 게이트웨이 사이의 중간 솔루션으로, 모든 응용 프로그램에 대한 프록시 역할을 한다.
전체 종단 간 TCP 연결을 허용하지 않으며, 두 개의 TCP 연결을 설정한다.

문 15. IPSec에 대한 설명으로 옳지 않은 것은?

① 네트워크 계층에서 패킷에 대한 보안을 제공하기 위한 프로토콜이다.
② 인터넷을 통해 지점들을 안전하게 연결하는 데 이용될 수 있다.
③ 전송 모드와 터널 모드를 지원한다.
④ AH(Authentication Header)는 인증 부분과 암호화 부분 모두를 포함한다.

답 ④

④ AH(인증 헤더)는 메시지 무결성과 출처 인증 기능을 하지만, 암호화는 하지 않는다.
암호화를 통해 기밀성을 제공하는 것은 ESP(Encapsulating Security Protocol, 보안 캡슐 프로토콜)이다.
<오답 체크> ③ 전송 모드에서는 IP 페이로드와 IP 헤더 일부를 인증·암호화하고,
터널 모드에서는 내부 IP 패킷 전체(헤더+페이로드)를 인증·암호화한다.

문 16. 커버로스(Kerberos)에 대한 설명으로 옳지 않은 것은?

① 네트워크 기반 인증 시스템으로 공개키 기반구조를 이용하여 사용자 인증을 수행한다.
② 인증 서버는 사용자를 인증하며 TGS(Ticket Granting Server)를 이용하기 위한 티켓을 제공한다.
③ TGS는 클라이언트가 서버로부터 서비스를 받을 수 있도록 티켓을 발급한다.
④ 인증 서버나 TGS로부터 받은 티켓은 클라이언트가 그 내용을 볼 수 없도록 암호화되어 있다.

답 ①

① 커버로스는 대칭키를 사용한다.
커버로스 버전4는 DES 알고리즘 사용
커버로스 버전5는 DES 이외의 다른 알고리즘도 사용

문 17. 사용자 패스워드의 보안을 강화하기 위한 솔트(salt)에 대한 설명으로 옳지 않은 것은?

① 여러 사용자에 의해 중복 사용된 동일한 패스워드가 서로 다르게 저장되도록 한다.
② 해시 연산 비용이 증가되어 오프라인 사전적 공격을 어렵게 한다.
③ 한 사용자가 동일한 패스워드를 두 개 이상의 시스템에 사용해도 그 사실을 알기 어렵게 한다.
④ 솔트 값은 보안 강화를 위하여 암호화된 상태로 패스워드 파일에 저장되어야 한다.

답 ④

솔트(salt)란 사용자가 설정한 패드워드에 보안성을 강화하기 위해(특히 사전 공격에 대응하기 위해) 붙이는 무작위 문자열이다.
④ 패스워드 파일에는 사용자별로 솔트값과 패스워드의 해시값이 저장되어 있다. 솔트값은 암호화되지 않은 상태로 저장되어 있다.
서버는 사용자가 입력한 패스워드와 서버에 저장되어 있는 솔트를 붙여 해시값을 계산한 뒤, 계산한 해시값을 서버에 저장되어 있던 해시값과 비교하여 로그인 성공 여부를 판단한다.
<오답 체크> ① 사용자마다 솔트값이 다르기 때문에, 여러 사용자가 동일한 패스워드를 사용하더라도 서로 다른 해시값을 갖게 된다.
② 해커는 원본 문자열과 그에 대응하는 해시값을 미리 계산하여 저장해놓은 레인보우 테이블(Rainbow Table)을 이용해 패스워드를 추론한다.
패스워드에 솔트를 사용하면 이러한 레인보우 테이블 공격이나 사전 공격(Dictionary Attack)을 어렵게 한다.
③ 한 사용자가 여러 시스템에 같은 패스워드를 사용해도 각 시스템이 사용하는 솔트값은 다르기 때문에, 각 시스템에 저장된 패스워드의 해시값은 다르다.

문 18. 스택 버퍼 오버플로(overflow) 공격에 대응하기 위한 방어 수단에 해당하지 않는 것은?

① 문자열 조작 루틴과 같은 불안전한 표준 라이브러리 루틴을 안전한 것으로 교체한다.
② 함수의 진입과 종료 코드를 조사하고 함수의 스택 프레임에 손상이 있는지를 검사한다.
③ 한 사용자가 프로그램에 제공한 입력이 다른 사용자에게 출력될 수 있도록 한다.
④ 매 실행 시마다 각 프로세스 안의 스택이 다른 곳에 위치하도록 한다.

답 ③

버퍼 오버플로우(buffer overflow) 공격은 프로그램에 미리 할당된 버퍼보다 더 많은 양의 데이터를 집어넣어, 다른 메모리 영역을 침범하여 데이터를 변조시키는 공격이다.
③ 사용자의 입력이 다른 사용자에게 출력되지 않도록 해야 한다.

문 19. 디지털 증거의 법적 효력을 인정받기 위해 포렌식 과정에서 지켜야 하는 원칙이 아닌 것은?

① 정당성의 원칙
② 무결성의 원칙
③ 재현의 원칙
④ 연계추적불가능의 원칙

답 ④

④ 증거의 정당성을 확보하기 위해 연계추적이 가능해야 한다.

◈ 포렌식의 원칙
○ 재현의 원칙: 증거를 복구하는 과정에서 똑같은 환경에서 같은 결과가 나오도록 재현할 수 있어야 함
○ 정당성의 원칙: 모든 증거는 적법한 절차를 거쳐서 획득하여야 함
○ 신속성의 원칙: 시스템 안의 디스크 또는 메모리 정보가 휘발되기 전에 빠르게 획득하여야 함
○ 연계보관성의 원칙: 증거의 이송/분석/보관/법정 제출이라는 일련의 과정에 대한 추적이 가능해야 함
○ 무결성의 원칙: 증거가 위조/변조되어서는 안 됨

문 20. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 규정하고 있는 내용이 아닌 것은?

① 주요정보통신기반시설의 보호체계
② 정보통신망에서의 이용자 보호 등
③ 정보통신망의 안정성 확보 등
④ 개인정보의 보호

답 ①

① 정보통신 시설에 대한 규정은 「정보통신기반 보호법」에서 다루는 내용이다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」
제1장 총칙
제2장 정보통신망의 이용촉진
제3장 삭제
제4장 개인정보의 보호 <---------- ④
제5장 정보통신망에서의 이용자 보호 등 <- ②
제6장 정보통신망의 안정성 확보 등 <--- ③
제7장 통신과금서비스
제8장 국제협력
제9장 보칙
제10장 벌칙