2024년 국가직 9급 정보보호론 총평

1. 출제경향 분석

전반적으로 기출문제를 반복하거나 변형하는 형태의 문제가 다수 출제되었습니다. 정보보호론은 정보보호직과 정보보안기사를 따라가고 있습니다. 802.11i 키 관리의 쌍별 키 계층 관련 문제는 정보보호직에서 출제된 바 있습니다. 법규 문제는 정보보안기사(알기사, 조현준 저 참조)에서 여러 번 출제되었던 주제여서 지안 강의와 교재로 공부하신 분들은 크게 어려움이 없었을 것 같습니다.

2. 난이도

전체적인 난이도는 전년도 국가직 시험에 비해 아주 쉬웠다고 볼 수 있습니다. 당락을 결정할 난이도 있는 문제는 3문항 정도로 보입니다. 기본에 충실하고 응용문제(10년간 연도별 기출문제집, 최고수준, 모의고사 등)를 많이 푸신 분들은 만점자도 많이 있을 것 같습니다. 하지만 쉬운 기출문제(시중 기출문제집이 어려운 문제는 빼는 경향이 있음) 위주로만 이론정리를 하신 분들은 어렵게 느껴졌을 수도 있을 것 같습니다.

3. 향후 학습방향

다음 시험을 위해서 본인의 위치를 냉철히 판단해보고 약점을 보완하셔야 합니다. 약간은 주관적일 수 있지만 이번 시험을 기준으로 90점 이상을 받으신 분들은 그 동안의 공부의 방향이 맞다고 보여집니다. 그러나 70점이하로 받으신 분들은 공부방법을 다시 한번 생각해 볼 필요가 있습니다.

조 현 준

- 성균관대학교 정보공학 전공
- CISA, CISSP, 정보보안기사
- 前, 데카르트고시학원 전산직 전임강사
- 現, 지안공무원학원 전산직 전임강사
- 現, (주)지안에듀 정보보안(산업)기사 전임강사

- TopSpot 자료구조론 이론편/기출편
- TopSpot 알기사 정보보안기사(산업기사) 필기
- TopSpot 알기사 정보보안기사(산업기사) 실기
- TopSpot 정보보호론
- TopSpot 정보보호론 기출문제집

유튜브 기출해설 강의 목록(링크) : 조현준 정보보호론 검색
https://www.youtube.com/playlist?list=PLaR0eJQDBqV8Mb3h4hdxwnQ_nBhY0qCWB

2024년 국가직 9급 정보보호론

2024년 3월 23 시행

1. ○△× 24.국가.9급

사용자 A가 사용자 B에게 보낼 메시지에 대한 전자서명을 생성하는 데 필요한 키는?

① 사용자 A의 개인키
② 사용자 A의 공개키
③ 사용자 B의 개인키
④ 사용자 B의 공개키

오답피하기 ① 송신자(A)의 개인키를 사용하여 전자서명을 생성하고, 수신자(B)는 송신자의 공개키를 사용하여 검증한다.

정답 ①

2. ○△× 24.국가.9급

원본 파일에 숨기고자 하는 정보를 삽입하고 숨겨진 정보의 존재 여부를 알기 어렵게 하는 기술은?

① 퍼징(Fuzzing)
② 스캐닝(Scanning)
③ 크립토그래피(Cryptography)
④ 스테가노그래피(Steganography)

◦ 퍼징(fuzzing)은 종종 자동화 또는 반자동화된 소프트웨어 테스트 기법으로서 컴퓨터 프로그램에 유효한 예상치 않은 데이터 또는 무작위 데이터를 입력하는 것이다.

오답피하기 ④ 암호란 메시지의 내용을 읽지 못하게 하는 기법을 말하며, 영어로 크립토그래피(cryptography)라고 하는 반면, 스테가노그래피(steganography)는 읽지 못하게 하는 것이 아니라 메시지의 존재 자체를 숨기는 기법이다.

정답 ④

3. ○△× 24.국가.9급

다음에서 설명하는 공격 방법은?

보기

○ 사람의 심리를 이용하여 보안 기술을 무력화시키고 정보를 얻는 공격 방법
○ 신뢰할 수 있는 사람으로 위장하여 다른 사람의 정보에 접근하는 공격 방법

① 재전송 공격(Replay Attack)
② 무차별 대입 공격(Brute-Force Attack)
③ 사회공학 공격(Social Engineering Attack)
④ 중간자 공격(Man-in-the-Middle Attack)

오답피하기 ③ 사회공학 공격은 시스템이 아닌 사람의 취약점을 공략하여 원하는 정보를 얻는 공격 기법이다. 사회공학적 해킹은 인터넷의 발달로 이메일, 인터넷 메신저, 트위터 등을 통해 사람에게로의 접근채널이 다각화됨에 따라 지인으로 가장하여 원하는 정보를 얻어내는 공격 방법이다.

정답 ③

4. ○△× 24.국가.9급

블록 암호의 운영 모드 중 ECB 모드와 CBC 모드에 대한 설명으로 옳은 것은?

① ECB 모드는 블록의 변화가 다른 블록에 영향을 주지 않아 안전하다.
② ECB 모드는 암호화할 때, 같은 데이터 블록에 대해 같은 암호문 블록을 생성한다.
③ CBC 모드는 블록의 변화가 이전 블록에 영향을 주므로 패턴을 추적하기 어렵다.
④ CBC 모드는 암호화할 때, 이전 블록의 결과가 필요하지 않다.

◦ ECB 모드는 가장 단순한 방식으로 각 블록을 독립적으로 암호화한다. 이 방식에서 동일한 평문블록은 동일한 암호문을 생성하는데, 이런 점은 안전성에 있어서 바람직하지 않다.

오답피하기 ① ECB 모드는 블록의 변화가 다른 블록에 영향을 주지 않지만, 안전한 방법은 아니다. ③ CBC 모드는 블록의 변화가 다음 블록에 영향을 주므로 패턴을 추적하기 어렵다. ④ CBC 모드는 암호화할 때, 이전 블록의 결과가 필요하다.

정답 ②

5. ○△× 24.국가.9급

컴퓨터 보안의 3요소가 아닌 것은?

① 무결성(Integrity)
② 확장성(Scalability)
③ 가용성(Availability)
④ 기밀성(Confidentiality)

◦ 기밀성: 오직 인가된 사람만이 알 필요성에 근거하여 시스템에 접근해야 한다는 원칙
◦ 무결성: 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호되어야 하는 성질
◦ 가용성: 자원이 필요할 때 지체 없이 원하는 객체 또는 자원에 접근하여 사용할 수 있는 성질

오답피하기 ② 정보보호의 주요 목적(3원칙)에 확장성은 포함되지 않는다.

정답 ②

6. ○△× 24.국가.9급

로컬에서 통신하고 있는 서버와 클라이언트의 IP 주소에 대한 MAC 주소를 공격자의 MAC 주소로 속여, 클라이언트와 서버 간에 이동하는 패킷이 공격자로 전송되도록 하는 공격 기법은?

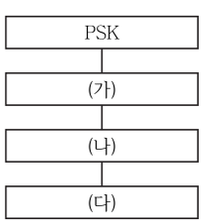
① SYN 플러딩
② DNS 스푸핑
③ ARP 스푸핑
④ ICMP 리다이렉트 공격

오답피하기 ③ ARP Spoofing은 공격자가 특정 호스트의 MAC 주소를 자신의 MAC 주소로 위조한 ARP Reply 패킷을 만들어 희생자에게 지속적으로 전송하면 희생자의 ARP Cache에 특정 호스트의 MAC 정보가 공격자의 MAC 정보로 변경이 된다는 점을 이용해 희생자에게서 특정 호스트로 나가는 패킷을 공격자가 스니핑하는 기법이다.

정답 ③

7. ○△× 24.국가.9급

IEEE 802.11i 키 관리의 쌍별 키 계층을 바르게 나열한 것은?



- TK(Temporal Key)
- PSK(Pre-Shared Key)
- PMK(Pairwise Master Key)
- PTK(Pairwise Transient Key)

	(가)	(나)	(다)
①	PMK	TK	PTK
②	PMK	PTK	TK
③	PTK	TK	PMK
④	PTK	PMK	TK

802.11i의 키 관리
◦ 사전 공유키(PSK, Pre-shared Key)
– AP와 STA가 사전 공유하는 비밀키
◦ 마스터 세션키(MSK, Master Session Key)
– AAAK(Authentication, Authorization, Accounting Key)라고도 함
– IEEE 802.1X 프로토콜이 인증단계에서 생성
◦ 쌍별 마스터키(PMK, Pairwise Master Key)
– 마스터키로 생성
– PSK를 사용한다면, PSK를 PMK로 사용
– MSK를 사용한다면, MSK의 일부로 PMK를 제작
– 마지막 인증과정이 끝나면 AP와 STA는 PMK 공유
◦ 쌍별 임시키(PTK, Pairwise Transient Key)
– PMK로 생성
– PTK는 실제로 3개의 키로 구성(EAPOL key Confirmation key, EAPOL key Encryption key, Temporal Key)
◦ TK(Temporal Key)
– 데이터 흐름 보안을 위한 임시 키

오답피하기 ② 802.11i의 키 관리 단계는 (PSK, MSK) → (PMK) → (PTK) → (KCK, KEK, TK)이다.

정답 ②

8. ○△× 24.국가.9급

CC(Common Criteria)의 보증 요구사항(Assurance Requirements)에 해당하는 것은?

① 개발
② 암호 지원
③ 식별과 인증
④ 사용자 데이터 보호

CC의 문서 구성

구성	상세 내용
CC 소개 및 일반 모델	CC에 대한 일반사항 및 모델 설명
보안 기능 요구사항	식별 및 인증, 암호지원, 보안감사, 안전한 경로/채널, 통신, 보안기능의 보호, 자원활용, 사용자 정보보호, 프라이버시, 보안관리
보증 요구사항 EAL 단계별 요구사항	생명주기, 개발, 형상관리, 시험, 설명서, 배포 및 운영, 보호 프로파일, 보안목표 명세서, 취약점 평가(보증유지)

오답피하기 ① 취약점 평가는 보증 요구사항에 해당된다.

정답 ①

9. ○△× 24.국가.9급

다음 /etc/passwd 파일 내용에 대한 설명으로 옳지 않은 것은?

보기

root x 0 0 root /root /bin/bash
㉠ ㉡ ㉢ ㉣

① ㉠은 사용자 ID이다.
② ㉡은 UID 정보이다.
③ ㉢은 사용자 홈 디렉터리 경로이다.
④ ㉣은 패스워드가 암호화되어 /bin/bash 경로에 저장되어 있음을 의미한다.

/etc/passwd 파일 필드
◦ 계정명
◦ 비밀번호
◦ 사용자 ID
◦ 그룹 ID
◦ 사용자 설명
◦ 홈 디렉터리(root)
◦ 로그인 셸

오답피하기 ④ ㉣은 로그인 셸이다.

정답 ④

10. ○△× 24.국가.9급

리눅스에서 설정된 umask 값이 027일 때, 생성된 디렉터리의 기본접근 권한으로 옳은 것은?

① drw-r-----
② d---r--rw-
③ drwxr-x---
④ d---r-xrwx

◦ UNIX 시스템에서는 각각 파일과 디렉터리를 생성할 때, 일반(정규) 파일의 경우 접근권한으로 666(rw_rw_rw_)을, 디렉터리의 경우 접근권한으로 777(rwxrwxrwx)을 디폴트(Default) 값으로 취한다.

오답피하기 ③ umask 027은 디렉터리에 대하여 Owner에게 모든 권한(rwx), Group에게는 read, execute 권한(r-x)을 준다.(750)

정답 ③

11. ○△× 24.국가.9급

역공학을 위해 로우레벨 언어에서 하이레벨 언어로 변환할 목적을 가진 도구는?

① 디버거(Debugger)
② 디컴파일러(Decompiler)
③ 패커(Packer)
④ 어셈블러(Assembler)

◦ 디버거(Debugger): 오류를 포함하고 있는 프로그램에서 그 오류의 원인을 찾기 위해서 사용할 수 있는 프로그램이다. 프로그램의 소스코드를 개별적으로 조사해서 빠르게 프로그램의 이상 동작을 검출하기 위해 사용할 수 있다.
◦ 어셈블러(assembler): 어셈블리어를 기계어 형태의 오브젝트 코드로 해석해 주는 컴퓨터 언어 번역 프로그램이다.
◦ 역어셈블러(Disassembler): 기계어를 어셈블리어로 변환하는 컴퓨터 프로그램이다. 역어셈블러는 특히 리버스 엔지니어링 도구로서 효율적으로 활용할 수 있다.
◦ 패킹(Packing): 원본 프로그램을 패킹된 형태로 압축하고 암호화하여 저장하는 기술이다.

오답피하기 ② 디컴파일러는 컴파일러와 반대의 역할을 하는 컴퓨터 프로그램이다. 이것은 상대적으로 저수준의 프로그램 코드를 고수준으로 변형한다. 역컴파일러는 보통 원본 소스코드로 완벽하게 재구성될 수 없으며, 결과가 매우 다양할 수 있다. 그럼에도 불구하고 이것은 소프트웨어 리버스 엔지니어링에서 매우 중요한 도구이다.

정답 ②

12. ○△× 24.국가.9급

위험 평가 방법에 대한 설명으로 옳지 않은 것은?

① 정성적 위험 평가는 자산에 대한 화폐가치 식별이 어려운 경우 이용한다.
② 정량적 분석법에는 델파이법, 시나리오법, 순위결정법, 브레인스토밍 등이 있다.
③ 정성적 분석법은 위험 평가 과정과 측정기준이 주관적이어서 사람에 따라 결과가 달라질 수 있다.
④ 정량적 위험 평가 방법에 의하면 연간 기대 손실은 위협이 성공했을 경우의 예상 손실액에 그 위협의 연간 발생률을 곱한 값이다.

◦ ALE = ARO × SLE(=자산가치 × 노출계수)
◦ 과거자료 분석법, 수학공식 접근법, 확률 분포법, 점수법은 정량직 위험 분석 방법이다.

오답피하기 ② 델파이기법, 시나리오법, 순위결정법, 브레인스토밍, 스토리보딩은 정성적 위험 분석 방법이다.

정답 ②

13. ○△× 24.국가.9급

「개인정보 보호법」 제30조(개인정보 처리방침의 수립 및 공개)에 따라 개인정보처리자가 정해야 하는 '개인정보 처리방침'에 포함되는 사항이 아닌 것은?

① 개인정보의 처리 목적
② 개인정보의 처리 및 보유 기간
③ 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항
④ 개인정보처리자의 성명 또는 개인정보를 활용하는 부서의 명칭과 전화번호 등 연락처

◘ 제30조(개인정보 처리방침의 수립 및 공개)
① 개인정보처리자는 다음 각 호의 사항이 포함된 개인정보의 처리 방침을 정하여야 한다. 이 경우 공공기관은 등록대상이 되는 개인정보파일에 대하여 개인정보 처리방침을 정한다.
1. 개인정보의 처리 목적
2. 개인정보의 처리 및 보유 기간
3. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)
3의2. 개인정보의 파기절차 및 파기방법(개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다)
3의3. 민감정보의 공개 가능성 및 비공개를 선택하는 방법(해당되는 경우에만 정한다)
4. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)
4의2. 가명정보의 처리 등에 관한 사항(해당되는 경우에만 정한다)
5. 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항
6. 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처
7. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치

· 운영 및 그 거부에 관한 사항(해당하는 경우에만 정한다)

8. 그 밖에 개인정보의 처리에 관하여 대통령령으로 정한 사항

② 개인정보처리자가 개인정보 처리방침을 수립하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.

오답피하기 ④ 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처가 개인정보 처리방침에 포함된다.

정답 ④

14. ○△× 24.국가.9급

「개인정보 보호법」 제4조(정보주체의 권리)에 따른 정보주체의 권리가 아닌 것은?

① 개인정보의 처리에 관한 정보를 제공받을 권리
② 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리
③ 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리
④ 완전히 자동화된 개인정보 처리에 따른 결정을 승인하거나 그에 대한 회복 등을 요구할 권리

제4조(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
3. 개인정보의 처리 여부를 확인하고 개인정보에 대한 열람(사본의 발급을 포함한다. 이하 같다) 및 전송을 요구할 권리
4. 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리
5. 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리
6. 완전히 자동화된 개인정보 처리에 따른 결정을 거부하거나 그에 대한 설명 등을 요구할 권리

오답피하기 ④ 정보주체의 권리에 완전히 자동화된 개인정보 처리에 따른 결정을 승인하거나 그에 대한 회복 등을 요구할 권리는 없다.

정답 ④

15. ○△× 24.국가.9급

증거물의 "획득→이송→분석→보관→법정 제출" 과정에 대한 추적성을 보장하기 위하여 준수해야 하는 원칙은?

① 연계 보관성의 원칙
② 정당성의 원칙
③ 재현의 원칙
④ 무결성의 원칙

오답피하기 ① 증거물 획득, 이송, 분석, 보관, 법정 제출의 각 단계에서 일련의 과정이 명확해야 하며, 이러한 과정에 대한 추적이 가능토록 책임자를 명시하는 것은 연계보관성의 원칙에 대한 설명이다.

정답 ①

16. ○△× 24.국가.9급

128비트 키를 이용한 AES 알고리즘 연산 수행에 필요한 내부 라운드 수는?

① 10
② 12
③ 14
④ 16

오답피하기 ① AES는 128비트 평문을 128비트 암호문으로 출력하는 알고리즘으로 non-Feistel 알고리즘에 속한다. 10, 12, 14라운드를 사용하며, 각 라운드에 대응하는 키 크기는 128, 192, 256비트이다. 키 크기에 따라 AES의 세 가지 버전이 존재하며 이들은 AES-128, AES-192, AES-256으로 불린다.

정답 ①

17. ○△× 24.국가.9급

SSL에서 기밀성과 메시지 무결성을 제공하기 위해 단편화, 압축, MAC 첨부, 암호화를 수행하는 프로토콜은?

① 경고 프로토콜
② 레코드 프로토콜
③ 핸드셰이크 프로토콜
④ 암호 명세 변경 프로토콜

오답피하기 ② SSL을 구성하는 프로토콜 중에서 Record 프로토콜은 상위계층에서 수신된 메시지를 전달하는 역할을 담당하며 클라이언트와 서버 간 약속된 절차에 따라 메시지에 대한 단편화, 압축, 메시지 인증 코드 생성 및 암호화 과정 등을 수행하는 프로토콜이다.

정답 ②

18. ○△× 24.국가.9급

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조(정보통신망의 안정성 확보 등)에서 정보보호지침에 포함되어야 하는 사항으로 명시적으로 규정한 것이 아닌 것은?

① 정보통신망연결기기등의 정보보호를 위한 물리적 보호조치
② 정보의 불법 유출·위조·변조·삭제 등을 방지하기 위한 기술적 보호조치
③ 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적·물리적 보호조치
④ 정보통신망의 안정 및 정보보호를 위한 인력·조직·경비의 확보 및 관련 계획수립 등 관리적 보호조치

제45조(정보통신망의 안정성 확보 등)

① 다음 각 호의 어느 하나에 해당하는 자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다.

1. 정보통신서비스 제공자
2. 정보통신망에 연결되어 정보를 송·수신할 수 있는 기기·설비·장비 중 대통령령으로 정하는 기기·설비·장비를 제조하거나 수입하는 자

② 과학기술정보통신부장관은 제1항에 따른 보호조치의 구체적 내용을 정한 정보보호조치에 관한 지침을 정하여 고시하고 제1항 각 호의 어느 하나에 해당하는 자에게 이를 지키도록 권고할 수 있다.

③ 정보보호지침에는 다음 각 호의 사항이 포함되어야 한다.

1. 정당한 권한이 없는 자가 정보통신망에 접근·침입하는 것을 방지하거나 대응하기 위한 정보보호시스템의 설치·운영 등 기술적·물리적 보호조치
2. 정보의 불법 유출·위조·변조·삭제 등을 방지하기 위한 기술적 보호조치
3. 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적·물리적 보호조치
4. 정보통신망의 안정 및 정보보호를 위한 인력·조직·경비의 확보 및 관련 계획수립 등 관리적 보호조치
5. 정보통신망연결기기등의 정보보호를 위한 기술적 보호조치

④ 과학기술정보통신부장관은 관계 중앙행정기관의 장에게 소관 분야의 정보통신망연결기기등과 관련된 시험·검사·인증 등의 기준에 정보보호지침의 내용을 반영할 것을 요청할 수 있다.

오답피하기 ① 정보통신망연결기기등의 정보보호를 위한 물리적 보호조치가 아닌 기술적 보호조치이다.

정답 ①

19. ○△× 24.국가.9급

다음에서 설명하는 ISMS-P의 단계는?

보기

- ○ 조직의 업무특성에 따라 정보자산 분류기준을 수립하여 관리체계 범위 내 모든 정보자산을 식별·분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.
- ○ 관리체계 전 영역에 대한 정보서비스 및 개인정보 처리 현황을 분석하고 업무 절차와 흐름을 파악하여 문서화하며, 이를 주기적으로 검토하여 최신성을 유지하여야 한다.
- ○ 위험 평가 결과에 따라 식별된 위험을 처리하기 위하여 조직에 적합한 보호대책을 선정하고, 보호대책의 우선순위와 일정·담당자·예산 등을 포함한 이행계획을 수립하여 경영진의 승인을 받아야 한다.

① 위험 관리
② 관리체계 운영
③ 관리체계 기반 마련
④ 관리체계 점검 및 개선

ISMS-P 관리체계 수립 및 운영

분야	항목
관리체계 기반 마련	경영진의 참여, 최고책임자의 지정, 조직 구성, 범위 설정, 정책 수립, 자원 할당
위험관리	정보자산 식별, 현황 및 흐름분석, 위험 평가, 보호대책 선정
관리체계 운영	보호대책 구현, 보호대책 공유, 운영현황 관리
관리체계 점검 및 개선	법적 요구사항 준수 검토, 관리체계 점검, 관리체계 개선

오답피하기 ① 보기는 각각 정보자산 식별, 현황 및 흐름분석, 위험 평가에 대한 설명이다.

정답 ①

20. ○△× 24.국가.9급

디지털 콘텐츠의 불법 복제와 유포를 막고 저작권 보유자의 이익과 권리를 보호해 주는 기술은?

① PGP(Pretty Good Privacy)
② IDS(Intrusion Detection System)
③ DRM(Digital Rights Management)
④ PIMS(Personal Information Management System)

오답피하기 ③ DRM(Digital Rights Management)기술은 콘텐츠의 지적 재산권이 디지털 방식에 의해서 안전하게 보호, 유지되도록 콘텐츠 창작에서부터 소비에 이르는 모든 유통과정에서 거래·분배·사용규칙이 적법하게 성취되도록 하는 기술이다. 재산권 보호 유지 이외에도 콘텐츠에 구매자 정보를 삽입하여 콘텐츠 불법 복제자를 추적하는 기능이 포함된 것이 특징이다.

정답 ③