【정보보안관리 및 법규】

1. 사용자 인증 방식에 대한 설명으로 가장 적절하지 **않은** 것은?
① 지식기반 인증이란 사용자의 기억으로만 인증하는 방식으로 패스워드, PIN(Personal Identification Number) 등이 있으며, 패스워드 방식의 경우 전송 시 암호화하지 않으면 도청 가능성이 있다.
② 소유기반 인증은 보유하고 있는 물건으로 인증하는 방식으로 스마트카드(smart card)나 OTP(One Time Password) 등이 있으며, 스마트카드의 경우 마이크로프로세스 칩과 메모리를 내장한 일종의 소형 컴퓨터로 보안성이 요구된다.
③ 생체기반 인증은 불변의 특성을 지닌 생체적, 행동적 특징을 자동화된 수단으로 등록하여 인증하는 방식으로 존재 특징과 행동 특징으로 분류되고, 평가항목으로는 FRR(False Rejection Rate)과 FAR(False Acceptance Rate) 등이 있다.
④ 행동기반 인증은 개인의 고유한 행동적 특징을 사용해서 인증하는 방식으로 지문, 정맥, 안면, 홍채와 같은 정보를 추출하여 프로파일 정보를 구축하고, 이를 통해서 특징적이고 유일한 정보를 식별해서 인증에 사용한다.

2. 커버로스(Kerberos) 인증에 대한 설명으로 가장 적절하지 **않은** 것은?
① 대칭키 암호화 기법에 바탕을 둔 티켓(ticket) 기반 인증 프로토콜이다.
② 아이디와 패스워드를 통해서만 인증한 후 사용자에 대한 서비스를 제공한다.
③ 인증 서버(Authentication Server)는 실질적인 인증을 수행한다.
④ 재전송 공격(replay attack)을 방지하기 위해 타임스탬프(timestamp) 정보가 필요하다.

3. 다음의 접근 통제 모델(Access Control Model) 중 무결성을 보장하기 위한 모델을 모두 고른 것으로 가장 적절한 것은?

㉠ 벨라파듈라(Bell-LaPadula) 모델 ㉡ 비바(Biba) 모델 ㉢ 클락 윌슨(Clark-Wilson) 모델

① ㉠ ② ㉡ ③ ㉠㉡ ④ ㉡㉢

4. 위험분석방법에 대한 설명으로 가장 적절한 것은?
① 기준선 접근법(baseline approach): 경험자의 지식을 이용하여 위험분석을 수행하는 방법으로, 조직의 규모가 작은 경우에 적용할 수 있는 방법이다.
② 비형식적 접근법(informal approach): 고위험 영역을 식별하여 이 영역에 대해 상세위험분석을 수행하고, 다른 영역은 베이스라인 접근법을 이용하는 혼합형 방식을 적용한다.
③ 상세 위험분석 접근법(detailed risk analysis approach): 조직의 자산 및 보안 요구사항을 구체적으로 분석하여 적절한 대책을 수립할 수 있으나, 시간과 노력이 많이 소요된다.
④ 복합 접근법(combined approach): 모든 시스템에 표준화된 보안 대책을 체크리스트로 제공하여 분석의 비용과 시간이 절약되지만, 과보호 또는 부족한 보호가 될 가능성이 있다.

5. 다음에서 설명하는 재해복구 시스템의 유형으로 가장 적절한 것은?

주 센터와 동일한 수준의 정보기술 지원을 원격지에 구축하고, 상시 운영 가능한 Active-Active 운영 상태를 유지함으로써 주 센터 재해 시 실시간으로 복구가 가능하다.

① Hot Site ② Warm Site
③ Mirror Site ④ Cold Site

6. SSO(Single Sign On)에 대한 설명으로 가장 적절하지 **않은** 것은?
① 한 번의 시스템 인증을 통하여 접근하고자 하는 다양한 정보시스템에 재인증 절차 없이 접근할 수 있도록 하는 통합 로그인 솔루션이다.
② 자동 인증을 원하는 시스템에 SSO 에이전트(agent) 소프트웨어를 설치하고 SSO 서버와의 통신을 통해 자동으로 인증을 수행해 준다.
③ 인증 방식은 패스워드, 토큰 또는 공인인증서를 사용하는 PKI(Public Key Infrastructure) 기반 인증 등의 다양한 형태가 존재한다.
④ 사용자 인증 시 고정된 패스워드를 사용하는 것이 아니라 매번 패스워드를 생성하여 사용한다.

7. 위험 분석에서 위험(risk)이란 원하지 않는 사건이 발생하여 부정적인 영향을 미칠 가능성을 말한다. 위험의 유형과 규모를 확인하기 위해서는 위험에 관련된 모든 요소들과 위험의 규모에 미치는 영향을 분석해야 한다. 이러한 위험 분석에 포함되는 핵심적인 구성 요소로 가장 적절하지 **않은** 것은?
① 취약성(vulnerability) ② 손실(loss)
③ 자산(asset) ④ 위협(threat)

8. 다음에서 설명하는 내용으로 가장 적절한 것은?

각종 재해나 재난 발생에 대비하여 핵심 시스템의 가용성과 신뢰성을 회복하고 업무의 연속성을 유지하기 위한 일련의 계획과 절차를 의미한다. 단순한 데이터의 복구나 원상회복뿐만 아니라 업무의 지속성을 보장하며 이를 통해 조직의 신뢰도를 유지하고, 나아가 전체적인 신뢰성 유지와 가치를 최대화하는 방법이다.

① BCP(Business Continuity Planning)
② BIA(Business Impact Analysis)
③ DRP(Disaster Recovery Planning)
④ MTD(Maximum Tolerable Downtime)

9. OTP(One Time Password) 기법은 동기식과 비동기식 방식으로 나뉠 수 있다. 동기식 방식에 대한 설명으로 가장 적절한 것은?
① OTP 생성매체가 일정 시간마다 비밀번호를 자동으로 생성하는 형태로 시간을 기준 값으로 하여 OTP 생성매체와 OTP 인증서버가 동기화 된다.
② 사용자의 OTP 생성매체와 은행의 OTP 인증 서버 사이에 동기화되는 기준 값이 없으며 사용자가 직접 임의의 난수를 OTP 생성매체에 입력하여 생성한다.
③ 사용자가 은행의 OTP 인증 서버로부터 받은 질의 값(challenge)을 OTP 생성매체에 직접 입력하면 응답 값(response)이 생성 된다.
④ 직접 질의 값을 확인하여 OTP 생성매체에 입력해야 하므로 은행은 별도의 질의 값을 관리해야 한다.

10. 정보보호 및 개인정보보호 관리체계(ISMS-P)에 대한 설명으로 가장 적절하지 **않은** 것은?
① 기존 ISMS 인증 및 ISMS-P 인증으로 구성되며, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」과 「개인정보 보호법」을 근간으로 “정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시”를 확정했다.
② 과학기술정보통신부장관, 행정안전부장관 및 방송통신위원회는 정보보호 및 개인정보보호 관리체계 인증 운영에 관한 정책 사항을 협의하기 위하여 정보보호 및 개인정보보호 관리체계 인증 협의회를 운영한다.
③ 한국정보통신진흥협회는 인증위원회를 개최하여 최종 인증을 부여하고 인증심사원 양성을 추진하며, 심사기관은 한국인터넷진흥원이 심사를 수행한다.
④ 인증심사 기준은 관리체계 수립 및 운영과 보호대책 요구사항, 개인정보 처리 단계별 요구사항으로 각 분야별 세부항목을 정의하고 있다.

11. 「개인정보 보호법」에서 공개된 장소에 영상정보처리기기를 설치·운영할 수 있는 경우로 가장 적절하지 **않은** 것은?
① 범죄의 예방 및 수사를 위하여 필요한 경우
② 시설안전 및 화재 예방을 위하여 필요한 경우
③ 영상정보 저장과 음성 녹음이 동시에 필요한 경우
④ 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

12. 「개인정보 보호법」 및 동 시행령에서 공공기관의 장은 개인정보파일 운용으로 인하여 개인정보 침해가 우려되는 경우, 그 위험요인의 분석과 개선 사항 도출을 위한 "개인정보 영향평가"를 수행해야 한다. 해당 평가 수행에 따른 고려사항으로 가장 적절하지 **않은** 것은?

① 개인정보 처리 시스템 수
② 개인정보의 보유기간 및 제3자 제공 여부
③ 정보주체의 권리를 해할 가능성 및 그 위험 정도
④ 민감정보 또는 고유식별정보의 처리 여부

13. 「개인정보 보호법」에서 개인정보 보호위원회(이하 "보호위원회"라 한다)와 관련된 내용으로 가장 적절하지 **않은** 것은?

① 중앙행정기관의 장은 소관 법령의 제정 또는 개정을 통하여 개인정보 처리를 수반하는 정책이나 제도를 도입·변경하는 경우에는 보호위원회에 개인정보 침해요인 평가를 요청하여야 한다.
② 보호위원회는 개인정보의 보호와 정보주체의 권익 보장을 위하여 매년 개인정보 보호 내부 관리계획을 관계 중앙행정기관의 장과 협의하여 수립한다.
③ 중앙행정기관의 장은 기본계획에 따라 매년 개인정보 보호를 위한 시행계획을 작성하여 보호위원회에 제출하고, 보호위원회의 심의·의결을 거쳐 시행하여야 한다.
④ 보호위원회는 기본계획을 효율적으로 수립하기 위하여 개인정보처리자, 관계 중앙행정기관의 장, 지방자치단체의 장 및 관계기관·단체 등에 개인정보처리자의 법규 준수 현황과 개인정보 관리 실태 등에 관한 자료의 제출이나 의견의 진술 등을 요구할 수 있다.

14. 「개인정보 보호법」에서 공공기관의 장이 개인정보파일을 운용하는 경우 행정안전부장관에게 이를 제32조(개인정보파일의 등록 및 공개)에서 규정하는 바에 따라 등록하여야 한다. 동 조항에서 규정하고 있는 개인정보파일 중 등록 제외대상에 대한 내용으로 가장 적절하지 **않은** 것은?

① 국가 안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일
② 범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰처분과 출입국관리에 관한 사항을 기록한 개인정보파일
③ 「조세범처벌법」에 따른 범칙행위 조사 및 「관세법」에 따른 범칙행위 조사에 관한 사항을 기록한 개인정보파일
④ 공공기관에서 불특정 다수를 대상으로 하는 단기적 업무처리만을 위하여 사용되는 개인정보파일

15. 「개인정보 보호법」에서 개인정보 처리와 관련한 정보주체의 권리로 가장 적절하지 **않은** 것은?

① 개인정보처리자가 개인정보의 처리를 통해 취득한 이익에 관한 정보를 제공받을 권리
② 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리
③ 개인정보에 대하여 열람, 처리 정지, 정정·삭제 및 파기를 요구할 권리
④ 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리

16. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제27조의3(개인정보 유출 등의 통지·신고)의 일부내용이다. 빈칸 ㉠부터 ㉣까지 들어갈 것으로 가장 적절하게 짝지어진 것은?

> 정보통신서비스 제공자등은 개인정보의 분실·도난·유출 사실을 안 때에는 지체 없이 관련 침해사고 사항을 (㉠)에 알리고 (㉡) 또는 (㉢)에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 (㉣)을 경과하여 통지·신고해서는 아니 된다. 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.

	㉠	㉡	㉢	㉣
①	정보보호 책임자	행정안전부	국가정보원	12시간
②	해당 이용자	행정안전부	한국인터넷 진흥원	24시간
③	정보보호 책임자	방송통신 위원회	국가정보원	12시간
④	해당 이용자	방송통신 위원회	한국인터넷 진흥원	24시간

17. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 정보통신서비스 제공자등이 영업의 전부 또는 일부의 양도·합병 등으로 그 이용자의 개인정보를 타인에게 이전하는 경우에 인터넷 홈페이지 게시, 전자우편, 전화 등의 방법에 따라 서비스 이용자에게 반드시 알려야 하는 내용으로 가장 적절하지 **않은** 것은?

① 개인정보를 이전하려는 사실
② 개인정보를 이전하는 보호책임자의 성명 또는 개인정보보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 그 전화번호 등 연락처
③ 개인정보를 이전받는 자의 성명·주소·전화번호 및 그 밖의 연락처
④ 이용자가 개인정보의 이전을 원하지 아니하는 경우 그 동의를 철회할 수 있는 방법과 절차

18. 「정보통신기반 보호법」 및 동 시행령에서 정보통신기반시설에 대한 침해사고 발생에 따른 피해의 효율적인 수습을 위하여 대책본부장이 소집한 대책본부회의를 반드시 거쳐야 하는 사항이 명시되어 있다. 해당하는 사항으로 가장 적절하지 **않은** 것은?

① 피해시설에 대한 복구조치
② 피해확산 방지에 필요한 조치
③ 피해자 구제를 위한 법적 조치
④ 유사한 침해사고의 방지를 위한 예방대책

19. 「정보통신기반 보호법」 제12조(주요정보통신기반시설 침해행위 등의 금지)에서 주요정보통신기반시설을 대상으로 금지하고 있는 침해행위에 관한 일부내용이다. 빈칸 ㉠부터 ㉢까지 들어갈 것으로 ⓐ부터 ⓒ까지 내용이 가장 적절하게 짝지어진 것은?

> 1. 접근권한을 가지지 아니하는 자가 주요정보통신기반시설에 접근하거나 접근권한을 가진 자가 그 권한을 초과하여 (㉠)
> 2. 주요정보통신기반시설에 대하여 데이터를 파괴하거나 주요정보통신기반시설의 운영을 방해할 목적으로 (㉡)
> 3. 주요정보통신기반시설의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 (㉢)

> ⓐ 컴퓨터바이러스·논리폭탄 등의 프로그램을 투입하는 행위
> ⓑ 저장된 데이터를 조작·파괴·은닉 또는 유출하는 행위
> ⓒ 정보처리에 오류를 발생하게 하는 행위

	㉠	㉡	㉢
①	ⓐ	ⓑ	ⓒ
②	ⓒ	ⓑ	ⓐ
③	ⓑ	ⓐ	ⓒ
④	ⓒ	ⓐ	ⓑ

20. 「전자서명법」 제22조의2(공인인증서의 관리 등)에서 공인인증기관이 제공하는 수단을 통해 이용자가 공인인증서에 의하여 확인할 수 있는 사항으로 가장 적절하지 **않은** 것은?

① 공인인증기관의 명칭 등 공인인증기관임을 확인할 수 있는 정보
② 가입자의 의사에 반해 부정한 방법으로 자신의 공인인증서가 유출된 사실
③ 가입자가 당해 공인인증서가 발행된 당시에 전자서명생성정보를 지배·관리하고 있는 사실
④ 공인인증서의 발행 전에 전자서명생성정보가 유효한 사실

【디지털포렌식개론】

1. 디지털 포렌식의 기본 원칙으로 가장 적절하지 **않은** 것은?
① 디지털 증거의 정확성을 위해 원본을 사용하여 분석해야 한다.
② 디지털 증거는 원본을 획득하되, 특별한 환경에서는 사본을 획득할 수 있도록 하고 있다.
③ 분석도구의 신뢰성 확보를 위하여 반드시 검증된 분석도구를 사용해야 한다.
④ 적법절차를 준수하여 당사자의 프라이버시 및 인권을 최대한 보호해야 한다.

2. 디지털 데이터 사본을 만드는 방법으로 가장 적절한 것은?
① 조사대상 매체는 반드시 읽기 전용으로 조사용 시스템에 부착해야 한다.
② 원본 디스크의 저장 용량보다 반드시 적은 용량의 디스크를 사용하여 복제본을 생성해야 한다.
③ 소프트웨어를 사용한 이미징(imaging)은 하드웨어를 사용한 방법보다 이미징 시간이 단축된다.
④ 사본 이미지 생성에 LinEn, dd는 사용할 수 없다.

3. 해수욕장에서 다른 사람의 신체를 촬영하고 있는 용의자를 체포한 후 관련 사진이 저장된 것을 발견하였으나 인터넷에서 다운받은 것이라 부인할 경우, 이를 반박할 수 있는 증거를 찾는 방법 중 가장 적절한 것은?
① 이미지 파일의 확장자
② 이미지 파일들의 목록
③ 이미지 파일의 용량
④ 이미지 파일의 메타데이터

4. 포렌식 분석 기법 및 분석 도구에 대한 설명으로 가장 적절한 것은?
① 포렌식 조사 분석은 잘 알려진 파일은 검색 대상에서 제외하고, 주목해서 검색할 대상을 선정하여 검색범위를 축소하는 것이 중요하다.
② FTK(Forensic Tool Kit)의 프로그램 중 사본 이미지 생성에 사용되는 프로그램은 Registry viewer이다.
③ ProDiscover는 리눅스에서만 동작한다.
④ 해시 값을 이용하여 불필요한 파일을 조사대상에서 제외하거나 특정 파일만을 찾아내는 방법은 시그니처 분석 방법이다.

5. 디지털 증거의 특징에 대한 설명으로 가장 적절하지 **않은** 것은?
① 잠재성: 내용 확인을 위해서는 판독장치가 필요하다.
② 취약성: 위·변조 및 삭제가 용이하다.
③ 복제성: 원본과 사본의 구분이 어렵다.
④ 다양성: 자료가 방대하다.

6. 윈도우의 "Thumbs.db"에 대한 설명으로 가장 적절한 것은?
① 삭제된 이미지 파일의 존재 여부를 확인할 수는 없다.
② 기본적으로 숨김 속성으로 설정되어 있다.
③ Thumbs.db는 사용자가 직접 생성한다.
④ 사진이나 이미지를 삭제하면 Thumbs.db 파일은 삭제되므로 주기적인 백업이 필요하다.

7. 리눅스가 설치된 PC의 압수·수색 과정에서 발견된 로그파일 중 "시스템의 정기적인 작업에 대한 로그"가 기록된 것으로 가장 적절한 것은?
① secure 로그 파일 ② dmesg 로그 파일
③ xferlog 로그 파일 ④ cron 로그 파일

8. 디지털 포렌식 증거 수집에 대한 설명으로 가장 적절하지 **않은** 것은?
① 증거 수집 절차는 "증거획득→증거분석→증거보관→증거제출"이다.
② 컴퓨터시스템 전체를 확보한 경우에는 BIOS에 설정되어 있는 시스템 날짜와 시간을 조사기관의 증거분석실에서 확인할 수 있다.
③ 휘발성 정보를 수집하기 위해 PC 종료 후, 디스크 복제를 수행한다.
④ 네트워크 증거수집 시에는 반드시 소유자나 관련자의 확인을 받아야 한다.

9. 안티-포렌식에서 데이터를 식별하지 못하도록 정보를 은닉하는 방법으로 가장 적절하지 **않은** 것은?
① Safeback ② Slacker
③ Steganography ④ RuneFS

10. 디지털 포렌식에서 삭제된 파일의 복구와 관련된 설명으로 가장 적절하지 **않은** 것은?
① 파일 카빙(file carving)은 파일의 시그니처 구조, 논리구조, 형식 등에 의존하여 파일을 복구해야 한다.
② 파일이 삭제되더라도 해당 데이터 클러스터가 다른 파일로 사용되지 않았다면 복구 가능하다.
③ 복구 대상 컴퓨터에 복구 소프트웨어를 설치하여 복구한다.
④ 삭제된 파일의 속성은 다른 파일이 그 디렉토리 엔트리를 재사용하기 전까지 이름을 제외하고 대부분 보존된다.

11. 윈도우 레지스트리를 이용하여 확인할 수 있는 정보로 가장 적절하지 **않은** 것은?
① 사용한 USB 장치의 제조사, 모델명, 고유번호 정보
② 설치 후 삭제된 프로그램 정보
③ 외부 시스템 연결 정보
④ 데몬(daemon)을 관리하는 inetd 정보

12. 압수·수색 현장에서 시스템 관리자가 비협조적일 경우, 디지털 포렌식 수사관이 데이터베이스를 찾기 위한 방법으로 가장 적절하지 **않은** 것은?
① 리눅스의 경우 "ps" 명령으로 "mysql" 프로세스를 확인할 수 있다.
② MySQL, MS-SQL 등이 동작 중이라면 특정 네트워크 포트를 검색하여 존재 여부를 확인할 수 있다.
③ MS-SQL의 경우 "my.cnf"라는 환경 설정 파일을 검색하고, MySQL의 경우 파일 확장자가 ".mdf"인 파일을 검색하여 존재 여부를 확인할 수 있다.
④ 윈도우의 경우 cmd 창에서 "tasklist" 명령으로 "mysql" 프로세스를 확인할 수 있다.

13. 전체 드라이브를 암호화할 수 있으며 자신의 시스템에 인증받지 못한 변경에 대한 보호 기능을 갖는 윈도우용 안티-포렌식 응용프로그램으로 가장 적절한 것은?
① 와이핑(Wiping)
② 비트락커(BitLocker)
③ 린엔(LinEn)
④ 어뎁토(Adepto)

14. 웹 브라우저 사용 흔적의 분석을 위하여, 수집된 WebcacheV24.dat 파일에 대한 설명으로 가장 적절하지 **않은** 것은?

① ESE(Extensible Storage Engine) 라는 구조를 사용한다.
② C:\Users\<username>\AppData\Local\Microsoft\Internet Explorer\IECompatData\ 폴더에서 파일을 수집한다.
③ 인터넷 익스플로러 10 버전에서 사용한다.
④ 윈도우의 Taskhost 프로세스가 핸들링하고 있어서 일반적인 복사로 획득할 수 없다.

15. 디지털 포렌식에서 해시(hash)에 대한 설명으로 가장 적절하지 **않은** 것은?

① 해시는 일방향 알고리즘으로, 해시 값을 이용하여 본래 데이터로 복원하는 것은 원론적으로 불가능하다.
② 디지털 데이터의 무결성을 검증하기 위하여 적용하는 알고리즘이다.
③ 해시 검색은 외장장치 연결 흔적 등의 시스템 사용 흔적을 분석하기 위하여 사용한다.
④ 두 개 파일의 해시 값이 동일하다면 동일한 파일이라고 추론 가능하다.

16. 슬랙 공간(slack space)에 대한 설명으로 가장 적절하지 **않은** 것은?

① 파일 시스템 할당 크기와 볼륨 크기간의 차이로 인해 발생되는 공간을 파일 시스템 슬랙이라고 한다.
② 램 슬랙을 이용하면 파일의 끝을 알 수 있고, 삭제된 파일을 복구할 때 유용하게 사용된다.
③ 파일 슬랙을 이용하면 특정 파일이 해당 매체에 존재하였는지를 규명할 수 있다.
④ 볼륨 슬랙은 파티션 크기의 변경을 통해 임의로 생성이 불가능하다.

17. 네트워크 증거 수집 시에, 정보를 획득하기 위한 명령으로 가장 적절하지 **않은** 것은?

① netstat -r: 라우팅 테이블 정보
② net share: 외부 접속 사용자 목록
③ set user: 현재 로그인한 사용자의 도메인, 이름, 프로파일
④ ipconfig: IP 설정 정보

18. 침해 사고가 발생한 컴퓨터의 전자우편(E-mail) 분석 시, 전자우편 헤더에서 확인할 수 있는 것으로 가장 적절하지 **않은** 것은?

① 송신자가 이용한 메일 서버
② 전자우편을 보낸 시간
③ 전자우편이 경유한 라우터 목록
④ 송신자의 IP 주소

19. 디지털 포렌식에서 증거 입증을 위해서는 우선 무결성이 입증되어야 하는데, 현장에서 무결성 입증을 위한 절차 중 가장 적절하지 **않은** 것은?

① 생성된 이미지 파일에 대한 해시 값을 계산하여 피압수자가 해시 값이 기재된 서면에 서명하게 한다.
② 피압수자가 입회한 상태에서 봉인을 푼 다음, 인케이스(EnCase)와 같은 인증된 포렌식 도구를 사용하여 압수한 저장매체에 대한 이미지 파일을 생성한다.
③ 하드 디스크 등의 저장매체를 압수한 뒤, 피압수자의 서명이 없어도 봉인 후 운송할 수 있다.
④ 피의자가 공판과정에서 무결성을 부정하는 경우에는 압수한 저장장치의 해시 값과 이미지 파일의 해시 값을 비교할 수 있도록 법원에 검증을 요구한다.

20. 디지털 포렌식 조사 과정이 필요한 경우로 가장 적절하지 **않은** 것은?

① 치료 중인 환자가 잘못된 약품 투여로 사망하자, 담당 의사가 컴퓨터에 저장되어 있는 환자의 처방전 내용을 변경하였다.
② 버스 안에서 휴대폰 카메라로 옆자리에 앉은 다른 사람의 신체를 몰래 촬영한 후, 촬영한 사진 파일을 삭제하였다.
③ 검찰에서 압수·수색이 나올 것을 염려하여, 공무원에게 제공한 뇌물 내역을 정리한 엑셀 파일을 삭제하였다.
④ 타인의 주민등록증을 이용하여 스마트폰 대리점 직원을 속이고 스마트폰을 개통하였다.