# 2023년 지방직 9급 정보보호론 총평

### 1. 출제경향 분석

시험범위는 계속 넓어져 정보보호직과 정보보안기사를 따라가고 있습니다. 전면 개정 시행일을 앞둔 개인정보보호법은 생략하고, 정보통신망법과 전자서명법에서 3문제가 출제된 것이 인상적입니다. SET, ISMS-P 문제의 경우는 이론서 내용을 꼼꼼히 봐야 맞출 수 있는 문제였습니다. IPSec 터널모드, SHA-512 등은 정보보안기사에서도 출제되어 수업시간에 강조한 내용이 출제되었습니다.(알기사, 조현준 저 참조) 정보보호론은 범위는 계속 넓어지고, 향후 난이도는 계속 올라간다고 생각하시면 될 것 같습니다.

### 2. 난이도

지문이 길고, 기존 기출문제에서 한 단계 더 들어간 문제들이 있어서 가볍게 공부하신 분들은 좀 어렵게 느껴졌을 것으로 판단됩니다. 전체적인 난이도는 전년도 지방직 시험 보다 어렵고, 올해 국가직 보다 어렵게 출제되었다고 판단됩니다. 기본에 충실하고 응용문제(800제, 모의고사 등)를 많이 푸신 분들은 고득점이 나왔을 것 같습니다. 하지만 쉬운 기출문제(시중 기출문제집이 어려운 문제는 빼는 경향이 있음) 위주로만 이론정리를 하신 분들은 어렵게 느껴졌을 것으로 생각됩니다.

### 3. 향후 학습방향

다음 시험을 위해서 본인의 위치를 냉철히 판단해보고 약점을 보완하셔야 합니다. 약간은 주관적일 수 있지만 이번 시험을 기준으로 80점 이상을 받으신 분들은 그 동안의 공부의 방향이 맞다고 보여집니다. 그러나 60점이하로 받으신 분들은 공부방법을 다시 한번 생각해 볼 필요가 있습니다. 정보보호론은 암기하는 과목이 아닌 이해하는 과목입니다. 특히 법규는 범위가 워낙 넓어서 법조문을 단순 복사해서 수록한 교재나 법규는 단순 암기해야 한다는 강사는 피하시는 것이 좋습니다.



## 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

# 2023년 지방직,교육청 9급
# 정보보호론
2023년 6월 10일 시행

**1.** ○△× 23.지방9급

**데이터의 위·변조를 방어하는 기술이 목표로 하는 것은?**

① 기밀성
② 무결성
③ 가용성
④ 책임추적성

오답피하기 ② 정보는 정해진 절차에 따라, 그리고 주어진 권한에 의해서만 변경되어야 한다는 것이 무결성이다. 정보는 항상 정확성을 일정하게 유지하여야 하며, 인가받은 방법에 의해서만 변경되어야 한다. 정보보호 목표 중 무결성은 데이터의 위·변조를 방어하는데 사용할 수 있다.

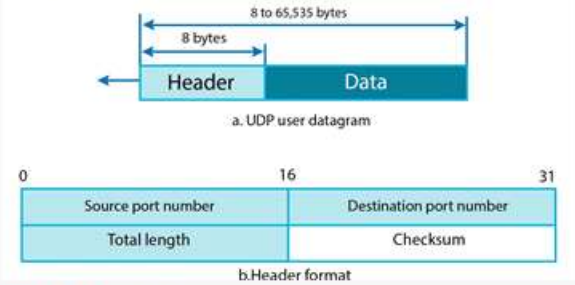
정답 ②

**2.** ○△× 23.지방9급

**UDP 헤더 포맷의 구성 요소가 아닌 것은?**

① 순서 번호
② 발신지 포트 번호
③ 목적지 포트 번호
④ 체크섬

UDP 형식




오답피하기 ① 순서 번호는 TCP 헤더에는 있지만, UDP 헤더에는 없다.

정답 ①

**3.** ○△× 23.지방9급

**논리 폭탄에 대한 설명으로 옳은 것은?**

① 사용자 동의 없이 설치되어 컴퓨터 내의 금융 정보, 신상 정보 등을 수집·전송하기 위한 것이다.
② 침입자에 의해 악성 소프트웨어에 삽입된 코드로서, 사전에 정의된 조건이 충족되기 전까지는 휴지 상태에 있다가 조건이 충족되면 의도한 동작이 트리거되도록 한다.
③ 사용자가 키보드로 PC에 입력하는 내용을 몰래 가로채어 기록한다.
④ 공격자가 언제든지 시스템에 관리자 권한으로 접근할 수 있도록 비밀 통로를 지속적으로 유지시켜 주는 일련의 프로그램 집합이다.

◦ 논리폭탄(Logic Bomb)은 보통의 프로그램에 오류를 발생시키는 프로그램 루틴을 무단으로 삽입하여 특정한 조건의 발생이나 특정한 데이터의 입력을 기폭제로 컴퓨터에 부정한 행위를 실행시키는 것이다. 프로그램이 전혀 예상하지 못한 파국적인 오류를 범하게 한다.

오답피하기 ① 스파이웨어(Spyware) ③ 키로거(Keyloggers) ④ 루트킷(Rootkit)에 대한 설명이다.

정답 ②

**4.** ○△× 23.지방9급

**대칭키 암호 알고리즘이 아닌 것은?**

① SEED
② ECC
③ IDEA
④ LEA

오답피하기 ② SEED, IDEA, LEA는 대칭키 암호 알고리즘이고, ECC는 공개키 암호 알고리즘이다.

정답 ②

**5.** ○△× 23.지방9급

**「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 규정하고 있는 사항이 아닌 것은?**

① 정보통신망의 표준화 및 인증
② 정보통신망의 안정성 확보
③ 고정형 영상정보처리기기의 설치·운영 제한
④ 집적된 정보통신시설의 보호

오답피하기 ① 정보통신망법 제8조 ② 정보통신망법 제45조 ③ 개인정보 제25조2 ④ 정보통신망법 46조에 규정하고 있다.

정답 ③

## 6. ○△× 23,지방,9급

**CSRF 공격에 대한 설명으로 옳지 않은 것은?**

① 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위를 특정 웹사이트에 요청하게 하는 공격이다.

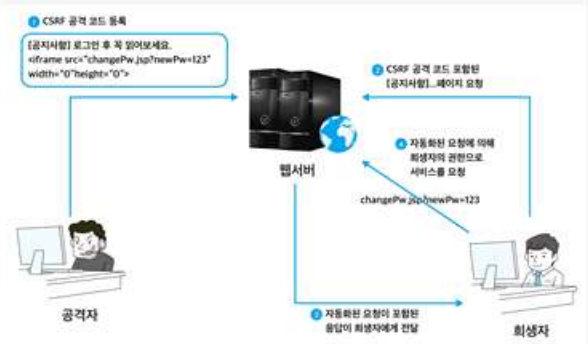
② 특정 웹사이트가 사용자의 웹 브라우저를 신뢰하는 점을 노리고 사용자의 권한을 도용하려는 것이다.

③ 사용자에게 전달된 데이터의 악성 스크립트가 사용자 브라우저에서 실행되면서 해킹을 하는 것으로, 이 악성 스크립트는 공격자가 웹 서버에 구현된 애플리케이션의 취약점을 이용하여 서버 측 또는 URL에 미리 삽입해 놓은 것이다.

④ 웹 애플리케이션의 요청 내에 세션별, 사용자별로 구별 가능한 임의의 토큰을 추가하도록 하여 서버가 정상적인 요청과 비정상적인 요청을 판별하는 방법으로 공격에 대응할 수 있다.

CSRF 공격

- 공격자는 세션탈취, XSS 등을 통해 공격자가 의도한 행위(수정, 삭제, 등록 등)를 사이트가 신뢰하는 인증된 사용자의 권한을 통해 실행하게 하는 취약점이다.
- GET 방식은 단순히 폼 데이터를 URL 뒤에 덧붙여서 전송하기 때문에 GET 방식의 폼을 사용하면 전달 값이 노출되므로 크로스사이트 요청위조 공격에 쉽게 노출될 수 있다.
- 공격 과정




오답피하기 ③ XSS는 악성 스크립트가 사용자(희생자)측에서 실행되는 반면에 CSRF는 서버쪽에서 실행된다.

정답 ③

## 7. ○△× 23,지방,9급

**IPSec의 터널 모드를 이용한 VPN에 대한 설명으로 옳지 않은 것은?**

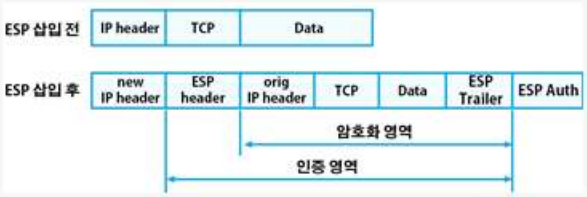
① 인터넷상에서 양측 호스트의 IP 주소를 숨기고 새로운 IP 헤더에 VPN 라우터 또는 IPSec 게이트웨이의 IP 주소를 넣는다.

② IPSec의 터널 모드는 새로운 IP 헤더를 추가하기 때문에 전송 모드 대비 전체 패킷이 길어진다.

③ ESP는 원래 IP 패킷 전부와 원래 IP 패킷 앞뒤로 붙는 ESP 헤더와 트레일러를 모두 암호화한다.

④ ESP 인증 데이터는 패킷의 끝에 추가되며, ESP 터널 모드의 경우 인증은 목적지 VPN 라우터 또는 IPSec 게이트웨이에서 이루어진다.

ESP 헤더 데이터 형식(터널 모드)




오답피하기 ③ ESP 헤더는 인증 범위에는 포함되지만, 암호화 범위에는 포함되지 않는다.

정답 ①②③④

## 8. ○△× 23,지방,9급

**「전자서명법」상 전자서명인증사업자에 대한 전자서명인증업무 운영기준 준수사실의 인정(이하 "인정"이라 한다)에 대한 설명으로 옳지 않은 것은?**

① 인정을 받으려는 전자서명인증사업자는 국가기관, 지방자치단체 또는 공공기관이어야 한다.

② 인정을 받으려는 전자서명인증사업자는 평가기관으로부터 평가를 먼저 받아야 한다.

③ 평가기관은 평가를 신청한 전자서명인증사업자의 운영기준 준수 여부에 대한 평가를 하고, 그 결과를 인정기관에 제출하여야 한다.

④ 인정기관은 평가 결과를 제출받은 경우 그 평가 결과와 인정을 받으려는 전자서명인증사업자가 법정 자격을 갖추었는지 여부를 확인하여 인정 여부를 결정하여야 한다.

제8조(운영기준 준수사실의 인정)

① 전자서명인증사업자는 인정기관으로부터 운영기준의 준수사실에 대한 인정을 받을 수 있다. 이 경우 평가기관으로부터 운영기준의 준수 여부에 대한 평가를 먼저 받아야 한다.

② 인정을 받으려는 전자서명인증사업자는 국가기관, 지방자치단체 또는 법인이어야 한다.

제9조(인정기관)

① 과학기술정보통신부장관은 한국인터넷진흥원을 운영기준 준수사실의 인정에 관한 업무를 수행하는 기관으로 지정할 수 있다.

② 인정기관은 평가 결과를 제출받은 경우 그 평가 결과와 운영기준 준수사실의 인정을 받으려는 전자서명인증사업자가 자격을 갖추었는지 여부를 확인하여 운영기준 준수사실의 인정 여부를 결정하여야 한다.

③ 인정기관은 운영기준 준수사실을 인정하는 경우 그 인정내용 및 유효기간이 기재된 증명서를 해당 전자서명인증사업자에게 발급하여야 한다. 이 경우 대통령령으로 정하는 바에 따라 증명서 발급사실을 공고하여야 한다.

제10조(평가기관)

① 과학기술정보통신부장관은 평가 업무를 수행하는 기관을 선정하여 고시할 수 있다.
② 운영기준 준수사실의 인정을 받으려는 전자서명인증사업자는 평가기관에 평가를 신청하여야 한다.
③ 평가기관은 평가를 신청한 전자서명인증사업자의 운영기준 준수 여부에 대한 평가를 하고, 그 결과를 인정기관에 제출하여야 한다.

오답피하기 ① 인정을 받으려는 전자서명인증사업자는 국가기관, 지방자치단체 또는 법인이어야 한다.(공공기관은 포함 안됨)

정답 ①

## 9. □△× 23,지방,9급

### 위험 평가 접근방법에 대한 설명으로 옳지 않은 것은?

① 기준(baseline) 접근법은 기준 문서, 실무 규약, 업계 최신 실무를 이용하여 시스템에 대한 가장 기본적이고 일반적인 수준에서의 보안 통제 사항을 구현하는 것을 목표로 한다.
② 비정형(informal) 접근법은 구조적인 방법론에 기반하지 않고 전문가의 지식과 경험에 따라 위험을 분석하는 것으로, 비교적 신속하고 저비용으로 진행할 수 있으나 특정 전문가의 견해 및 편견에 따라 왜곡될 우려가 있다.
③ 상세(detailed) 위험 분석은 정형화되고 구조화된 프로세스를 사용하여 상세한 위험 평가를 수행하는 것으로, 많은 시간과 비용이 드는 단점이 있는 반면에 위험에 따른 손실과 보안 대책의 비용 간의 적절한 균형을 이룰 수 있는 장점이 있다.
④ 복합(combined) 접근법은 상세 위험 분석을 제외한 기준 접근법과 비정형 접근법 두 가지를 조합한 것으로 저비용으로 빠른 시간 내에 필요한 통제 수단을 선택해야 하는 상황에서 제한적으로 활용된다.

오답피하기 ④ 복합 접근방법은 고위험(high risk) 영역을 식별하여 이 영역은 상세 위험분석을 수행하고 다른 영역은 베이스라인 접근법을 사용하는 방식이다.

정답 ④

## 10. □△× 23,지방,9급

### ISMS-P 인증 기준의 세 영역 중 하나인 관리체계 수립 및 운영에 해당하지 않는 것은?

① 관리체계 기반 마련
② 위험 관리
③ 관리체계 점검 및 개선
④ 정책, 조직, 자산 관리

◦ ISMS-P의 관리체계 수립 및 운영은 「관리체계 기반 마련 → 위험관리 → 관리체계 운영 → 관리체계 점검 및 개선」순으로 이루어진다.

오답피하기 ④ ISMS-P의 관리체계 수립 및 운영에 정책, 조직, 자산 관리는 포함되지 않는다.

정답 ④

## 11. □△× 23,지방,9급

### OTP 토큰이 속하는 인증 유형은?

① 정적 생체정보
② 동적 생체정보
③ 가지고 있는 것
④ 알고 있는 것

오답피하기 ③ OTP 토큰은 소유기반의 Type 2 인증 유형이다.

정답 ③

## 12. □△× 23,지방,9급

### 서비스 거부 공격에 해당하는 것은?

① 발신지 IP 주소와 목적지 IP 주소의 값을 똑같이 만든 패킷을 공격 대상에게 전송한다.
② 공격 대상에게 실제 DNS 서버보다 빨리 응답 패킷을 보내 공격 대상이 잘못된 IP 주소로 웹 접속을 하도록 유도한다.
③ LAN상에서 서버와 클라이언트의 IP 주소에 대한 MAC 주소를 위조하여 둘 사이의 패킷이 공격자에게 전달되도록 한다.
④ 네트워크 계층에서 공격 시스템을 네트워크에 존재하는 또 다른 라우터라고 속임으로써 트래픽이 공격 시스템을 거쳐가도록 흐름을 바꾼다.

오답피하기 ① Land attack으로 DoS 공격에 속한다. ② DNS Spoofing ③ ARP Spoofing ④ ICMP Redirect(스니핑 공격)에 대한 설명이다.

정답 ①

## 13. ○△× 23.지방.9급

**「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조의4(침해사고의 원인 분석 등)의 내용으로 옳지 않은 것은?**

① 정보통신서비스 제공자 등 정보통신망을 운영하는 자는 침해사고가 발생하면 침해사고의 원인을 분석하고 그 결과에 따라 피해의 확산 방지를 위하여 사고대응, 복구 및 재발 방지에 필요한 조치를 하여야 한다.

② 과학기술정보통신부장관은 정보통신서비스 제공자의 정보통신망에 침해사고가 발생하면 그 침해사고의 원인을 분석하고 피해 확산 방지, 사고대응, 복구 및 재발 방지를 위한 대책을 마련하여 해당 정보통신서비스 제공자에게 필요한 조치를 하도록 권고할 수 있다.

③ 과학기술정보통신부장관은 정보통신서비스 제공자의 정보통신망에 발생한 침해사고의 원인 분석 및 대책 마련을 위하여 필요하면 정보통신서비스 제공자에게 정보통신망의 접속기록 등 관련 자료의 보전을 명할 수 있다.

④ 과학기술정보통신부장관이나 민·관합동조사단은 관련 규정에 따라 정보통신서비스 제공자로부터 제출받은 침해사고 관련 자료와 조사를 통하여 알게 된 정보를 재발 방지 목적으로 필요한 경우 원인 분석이 끝난 후에도 보존할 수 있다.

**제48조의4(침해사고의 원인 분석 등)**

① 정보통신서비스 제공자 등 정보통신망을 운영하는 자는 침해사고가 발생하면 침해사고의 원인을 분석하고 그 결과에 따라 피해의 확산 방지를 위하여 사고대응, 복구 및 재발 방지에 필요한 조치를 하여야 한다.

② 과학기술정보통신부장관은 정보통신서비스 제공자의 정보통신망에 침해사고가 발생하면 그 침해사고의 원인을 분석하고 피해 확산 방지, 사고대응, 복구 및 재발 방지를 위한 대책을 마련하여 해당 정보통신서비스 제공자에게 필요한 조치를 하도록 권고할 수 있다.

③ 과학기술정보통신부장관은 정보통신서비스 제공자의 정보통신망에 중대한 침해사고가 발생한 경우 원인 분석 및 대책 마련을 위하여 필요하면 정보보호에 전문성을 갖춘 민·관합동조사단을 구성하여 그 침해사고의 원인 분석을 할 수 있다.

④ 과학기술정보통신부장관은 침해사고의 원인 분석 및 대책 마련을 위하여 필요하면 정보통신서비스 제공자에게 정보통신망의 접속기록 등 관련 자료의 보전을 명할 수 있다.

⑤ 과학기술정보통신부장관은 침해사고의 원인 분석 및 대책 마련을 하기 위하여 필요하면 정보통신서비스 제공자에게 침해사고 관련 자료의 제출을 요구할 수 있으며, 중대한 침해사고의 경우 소속 공무원 또는 민·관합동조사단에게 관계인의 사업장에 출입하여 침해사고 원인을 조사하도록 할 수 있다. 다만, 「통신비밀보호법」에 따른 통신사실확인자료에 해당하는 자료의 제출은 같은 법으로 정하는 바에 따른다.

⑥ 과학기술정보통신부장관이나 민·관합동조사단은 제출받은 자료와 조사를 통하여 알게 된 정보를 침해사고의 원인 분석 및 대책 마련 외의 목적으로는 사용하지 못하며, 원인 분석이 끝난 후에는 즉시 파기하여야 한다.

⑦ 민·관합동조사단의 구성·운영, 제출된 자료의 보호 및 조사의 방법·절차 등에 필요한 사항은 대통령령으로 정한다.

**오답피하기** ④ 과학기술정보통신부장관이나 민·관합동조사단은 제출받은 자료와 조사를 통하여 알게 된 정보를 침해사고의 원인 분석 및 대책 마련 외의 목적으로는 사용하지 못하며, 원인 분석이 끝난 후에는 즉시 파기하여야 한다.

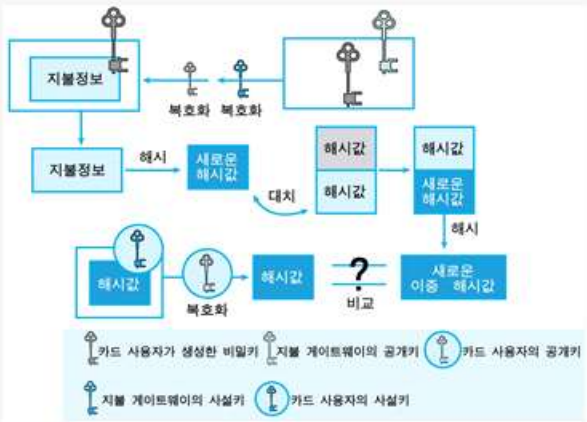
정답 ④

## 14. ○△× 23.지방.9급

**전자상거래에서 소비자의 주문 정보와 지불 정보를 보호하기 위한 SET의 이중 서명은 소비자에서 상점으로 그리고 상점에서 금융기관으로 전달된다. 금융기관에서 이중 서명을 검증하는데 필요하지 않은 것은?**

① 소비자의 공개키
② 주문 정보의 해시
③ 상점의 공개키
④ 지불 정보

**지불정보의 확인**




**오답피하기** ③ 카드사용자가 생성한 비밀키는 지불게이트웨이의 공개키로 암호화가 되어 있으므로 지불 게이트웨이의 사설키로 복호화해서 비밀키를 획득하여 지불정보를 복호화한다. 복호화한 지불정보를 해시하여 새로운 해시값을 생성한다. 이후 지불정보 해시값을 대치시켜 새로운 이중 해시값을 생성한 후 전달해온 이중해시값과 비교하여 같은지 확인한다. 구매정보와 지불정보가 포함된 이중 해시값은 카드사용자의 사설키로 암호화되어 있으므로 공개키로 복호화해서 해시값을 획득하는 과정을 거친다.

정답 ③

## 15. ○△× 23.지방.9급

**SHA-512 알고리즘의 수행 라운드 수와 처리하는 블록의 크기(비트 수)를 바르게 짝 지은 것은?**

| | 라운드 수 | 블록의 크기 |
|---|---|---|
| ① | 64 | 512 |
| ② | 64 | 1024 |
| ③ | 80 | 512 |
| ④ | 80 | 1024 |

SHA 해시 알고리즘 비교

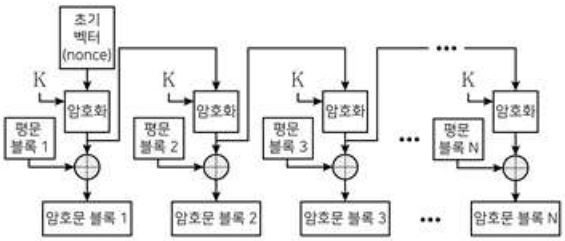
| 구분 | SHA-1 | SHA-224 | SHA-256 | SHA-384 | SHA-512 |
|---|---|---|---|---|---|
| MD 길이 | 160 | 224 | 256 | 384 | 512 |
| 블록 길이 | 512 | 512 | 512 | 1024 | 1024 |
| 워드 길이 | 32 | 32 | 32 | 64 | 64 |
| 단계 수 | 80 | 64 | 64 | 80 | 80 |

오답피하기 ④ SHA-512는 80라운드, 1024비트 블록을 처리한다.

정답 ④

## 16. ○△× 23.지방.9급

**다음 그림과 같이 암호화를 수행하는 블록 암호 운용 모드는? (단, ⊕: XOR, K: 암호키)**




① CBC
② CFB
③ OFB
④ ECB

오답피하기 ③ OFB 모드는 초기값을 암호화하고 그 결과를 다시 암호화하기를 반복하면서 생성되는 출력 블록들과 평문 블록들을 XOR하여 암호문 블록들을 생성하는 방식이다

정답 ③

## 17. ○△× 23.지방.9급

**윈도우 최상위 레지스트리에 대한 설명으로 옳지 않은 것은?**

① HKEY_LOCAL_MACHINE은 로컬 컴퓨터의 하드웨어와 소프트웨어의 설정을 저장한다.
② HKEY_CLASSES_ROOT는 파일 타입 정보와 관련된 속성을 저장하는 데 사용된다.
③ HKEY_CURRENT_USER는 현재 로그인한 사용자의 설정을 저장한다.
④ HKEY_CURRENT_CONFIG는 커널, 실행 중인 드라이버 또는 프로그램과 서비스에 의해 제공되는 성능 데이터를 실시간으로 제공한다.

◦

오답피하기 ④ HKEY_CURRENT_CONFIG(HKCC)는 시스템이 시작할 때 사용하는 하드웨어 프로파일 정보를 저장하고 있다. 하드웨어 프로파일이 컴퓨터가 부팅될 때마다 달라질 수 있지만 프로그램은 이 키를 통해서 현재 활성화되어 있는 하드웨어 프로파일 정보를 찾아 참조한다.

정답 ④

## 18. ○△× 23.지방.9급

**SSH(Secure Shell)의 전송 계층 프로토콜에 의해 제공되는 서비스가 아닌 것은?**

① 서버 인증
② 데이터 기밀성
③ 데이터 무결성
④ 논리 채널 다중화

SSH의 컴포넌트

- SSH 전송 계층 프로토콜은 서버 인증, 기밀성, 무결성 등의 보안 서비스 제공 방법, 압축, 암호 알고리즘의 협상, 키 교환 방법 등을 다루고 있다.
- SSH 인증 프로토콜은 SSH 인증 프로토콜 프레임워크, 공개키/패스워드/호스트기반 방식 등의 클라이언트 인증을 다루고 있다. SSH 인증 프로토콜은 SSH 전송 계층 프로토콜 상위에서 수행되며, SSH 접속 프로토콜을 위해 인증된 단일 터널을 제공한다.
- SSH 접속 프로토콜은 대화형 로그인 세션, 원격 명령 실행, TCP/IP 접속 전달 등의 기능을 제공하며, 이 모든 통신이 암호화된 단일 터널을 통한 다중화 채널을 사용해서 이루어진다. SSH 접속 프로토콜은 SSH 전송 계층 프로토콜과 인증 프로토콜 상위에서 수행된다.

오답피하기 ④ 논리 채널 다중화는 SSH 접속(연결) 프로토콜에서 제공한다.

정답 ④

## 19. ○△× 23.지방.9급

**리눅스 배시 셸(Bash shell) 특수 문자와 그 기능에 대한 설명이 옳지 않은 것은?**

| 특수 문자 | 기능 |
|---|---|
| ① ~ | 작업 중인 사용자의 홈 디렉터리를 나타냄 |
| ② " " | 문자(" ") 안에 있는 모든 셸 특수 문자의 기능을 무시 |
| ③ ; | 한 행의 여러 개 명령을 구분하고 왼쪽부터 차례로 실행 |
| ④ \| | 왼쪽 명령의 결과를 오른쪽 명령의 입력으로 전달 |

◘ 사전 정의된 특수 문자

| 특수 문자 | 사전 정의 | 특수 문자 | 사전 정의 |
|---|---|---|---|
| ~ | 홈 디렉터리 | * | 문자열 와일드카드 (Wildcard) |
| . | 현재 디렉터리 | ? | 한 문자 와일드카드 |
| .. | 상위 디렉터리 | ; | 셸 명령 구분자 |
| # | 주석 | \| | 파이프 |
| $ | 셸 변수 | 〈 | 입력 재지정 |
| & | 백그라운드 (Background) 작업 | 〉 | 출력 재지정 |

오답피하기 ② 배시셸의 주석 문자는 #이다. " "는 값을 출력할 때 사용한다.

정답 ②

## 20. ○△× 23.지방.9급

**ISMS-P 인증 기준 중 사고 예방 및 대응 분야의 점검 항목만을 모두 고르면?**

보기

ㄱ. 백업 및 복구 관리
ㄴ. 취약점 점검 및 조치
ㄷ. 이상행위 분석 및 모니터링
ㄹ. 재해 복구 시험 및 개선

① ㄱ, ㄴ
② ㄱ, ㄹ
③ ㄴ, ㄷ
④ ㄷ, ㄹ

◘ 사고 예방 및 대응
◦ 사고 예방 및 대응체계 구축
◦ 취약점 점검 및 조치
◦ 이상행위 분석 및 모니터링
◦ 사고 대응 훈련 및 개선
◦ 사고 대응 및 복구

오답피하기 ③ 백업 및 복구 관리 → 시스템 및 서비스 운영관리, 재해 복구 시험 및 개선 → 재해 복구에 속한다.

정답 ③