2019년 국가직 9급 합격예측서비스 분석과 정보보호론 향후 학습방향 안내

1. 목적

2019년 첫 번째 시험이 4월 6일(토)에 시행되었습니다. 합격권에 들어간 수험생도 있지만, 전년도와 다른 출제 경향으로 공무원 시험에 대한 회의감을 느끼며 방황하시는 분들도 많으리라 생각됩니다. 이에 이번 시험의 객관적 분석을 통해 향후 학습에 조금이나마 도움을 드리고자 합니다.

2. 합격예측서비스 분석

가. 지안 합격예측서비스 소개

지안 합격예측서비스는 전년도에도 높은 정확도를 보였습니다. 올해도 4월16일 17:00 현재 280명 이상이 입력하여 전년도와 비슷한 수준의 표본집단을 이루고 있습니다. 입력된 자료 중에 표본과 많은 차이를 보이는 점수대는 분석에서 제외하였습니다.

나. 예상 합격선 분석(전산개발 채용인원 : 83명)

점수	2018년	누계
93	3	3
92	1	4
91	–	4
90	7	11
89	7	18
88	8	26
87	8	34
86	16	50
85	6	56
84	15	71
83	16	87
82	16	103
81	12	115
80	11	126
79	17	143

※ 2018년 필기 합격선은 73점임

나. 정보보호론 분석(오프라인 설문조사)

점수	정보보호론(2019년)	
	비율(%)	누계(%)
100	19	19
95	8	27
90	12	39
85	15	54
80	12	66
75이하	8	74
미응답	27	100

※ 2019.4.17. 무료해설 특강 참여자를 대상으로 설문조사 실시

3. 정보보호론 출제 분석

2019년 국가직 정보보호론 시험은 전년도에 비해 전체적으로 평이한 수준으로 파악이 됩니다. 이는 전년도의 수험생들의 점수분포와 비교해 봐도 바로 알 수 있습니다. 출제범위에서 특이한 것은 블록체인 관련 문제가 2문제가 출제되었고, 법규가 3문제 였는데 시행령까지 들어간 문제에서 9급에서 처음으로 출제되었습니다. 7급의 경우는 실무지침기준까지 출제되곤 합니다.

4. 정보보호론 성공 요인과 실패 요인 분석

가. 기준 점수

4월17일 14:00에 타학원 수험생을 포함하여 많은 분들이 참석하여 해설 강의 후에 상담을 진행했습니다. 매년 반복되는 패턴이긴 하지만, 시장조사를 면밀히 하지 않고 공무원 시험을 시작해서 첫 시험이 끝나고 교재와 강의 선택에 문제가 있었다는 얘기를 하곤 합니다. 정보보호론 담당 선생의 입장에서 봤을 때 만약 본인이 이번 시험에서 85점 이상을 획득했다면 공부방법이 옳다고 볼 수 있고, 그 아래 점수를 받으셨다면 원인을 분석 후에 다음 시험에 임해야 하지 않을까 생각합니다.

나. 성공 사례(주관적일 수 있음)

- 이론 수업을 충실히 반복해서 들으신 분
- 최신 탑스팟 이론서를 확실히 이해하시는 분
- 적중 800제 등을 통해 응용 훈련을 충실히 하신 분
- 이론+기출문제+적중문제+모의고사를 일관성 있게 정리하신 분

다. 실패 사례(주관적일 수 있음)

- 전공 시험과목을 과소평가 하신 분(시장조사 소홀)
- 요약집 위주로만 정리, 얇은 수험서를 선호하시는 분
- 기출문제 위주로만 문제정리 하신 분
- 학원마다 모의고사만 찾아서 공부하신 분
- 오래된 수험서와 문제집으로 공부하신 분

5. 향후 학습방향

가. 정보보호론 향후 학습방향

모든 시험은 공부한 만큼 나오긴 하지만, 어떤 도구와 방법으로 하느냐도 점수를 좌우하는 요인입니다. 이론정리 → 기출문제(700제) → 최고수준800제문제 → 모의고사 순으로 하는데 본인이 목표로 하는 시험의 남은 기간을 고려하여 보완하시길 바랍니다.[(최고수준→모의고사) or (기출→최고수준→모의고사) or (이론, 기출, 최고수준, 모의고사)]

나. 지안에듀의 향후 무료 학습지원

국가직 정보보호론은 해설자료와 함께 동영상도 업로드됩니다. 지방직 시험전까지는 로그인 없이 누구나 수강가능하오니 이용 바랍니다.(지안에듀 홈페이지에서 무료수강 가능)

6. 결언

시험을 잘 보든 못 보든 올해 첫 번째 시험이 끝났습니다. 만족할만 점수를 못 받으신 분은 냉철히 자기를 돌아보시고, 약점을 최대한 보완하셔서 원하는 시험에 합격하시길 바랍니다. 이때 주변 사람의 조언을 얻는 것도 좋은 방법일 수 있습니다.

저는 개인적으로 정보보안기사를 가장 많이 합격시키고 있고, 정보보호론을 최단 시간에 고득점을 올리는 방법과 도구를 모두 제공할 수 있는 유일한 선생이라고 자부합니다.

지안/탑스팟 가족이든 아니든 개인적으로 정보보호론 공부방법에 대해서 궁금한 내용이 있으신 분들은 kingsalt1102@naver.com으로 메일 보내시면 제가 아는 범위내에서 성심껏 답변드리도록 하겠습니다.

감사합니다.

2019년 국가직 9급 정보보호론

-2019년 4월 6일 시행

1. ○△× 19.국가.9급

쿠키(Cookie)에 대한 설명으로 옳지 않은 것은?

① 쿠키는 웹사이트를 편리하게 이용하기 위한 목적으로 만들어졌으며, 많은 웹사이트가 쿠키를 이용하여 사용자의 정보를 수집하고 있다.

② 쿠키는 실행파일로서 스스로 디렉터리를 읽거나 파일을 지우는 기능을 수행한다.

③ 쿠키에 포함되는 내용은 웹 응용프로그램 개발자가 정할 수 있다.

④ 쿠키 저장 시 타인이 임의로 쿠키를 읽어 들일 수 없도록 도메인과 경로 지정에 유의해야 한다.

◘ 쿠키에 관한 오해

◦ 바이러스 전파

– 쿠키가 위험하거나 바이러스를 전파할 거라고 생각하는 사람이 있을지 모르지만, 사실 쿠키는 텍스트 파일이기 때문에 「실행」되지는 않는다.

– 바이러스는 실행되어서 전파되는 것인데, 쿠키는 단순히 정보를 담고 있는 텍스트 파일이기 때문에 쿠키가 바이러스를 전파할 수는 없다.

– 예전에는 실행 가능한 쿠키에 바이러스를 심은 적도 있었지만, 그 역시 인터넷 익스플로러 3.0 브라우저에서만 가능했기 때문에 지금은 위험성이 없다.

◦ 사용자 컴퓨터 피해 입히기

– 쿠키는 실행 파일이 아닌 텍스트 파일이다. 쿠키에는 웹 사이트에서 만든 특정 데이터만 있을 뿐 어떠한 정보도 담겨 있지 않다.

– 더구나 실행 파일이 아니기 때문에 스스로 디렉터리를 읽거나 파일을 지우는 기능은 절대 수행할 수 없다.

◦ 다른 웹사이트에서 읽기

– 쿠키는 쿠키 안에 저장된 도메인 이름을 갖고 있는 사이트에서만 유효하다.

오답피하기 ② 쿠키(Cookie)는 1994년 넷스케이프에서 처음 사용한 기술로 사용자들이 웹 사이트를 편리하게 이용할 수 있도록 하기 위한 목적으로 만들어졌다. 쿠키는 실행 파일이 아닌 텍스트 파일로 디렉터리를 읽거나 파일을 지우는 기능을 수행할 수 없다.

정답 ②

2. ○△× 19.국가.9급

악성프로그램에 대한 설명으로 옳지 않은 것은?

① Bot – 인간의 행동을 흉내 내는 프로그램으로 DDoS 공격을 수행한다.

② Spyware – 사용자 동의 없이 설치되어 정보를 수집하고 전송하는 악성 소프트웨어로서 금융정보, 신상정보, 암호 등을 비롯한 각종 정보를 수집한다.

③ Netbus – 소프트웨어를 실행하거나 설치 후 자동적으로 광고를 표시하는 프로그램이다.

④ Keylogging – 사용자가 키보드로 PC에 입력하는 내용을 몰래 가로채 기록하는 행위이다.

◦ 넷버스(Netbus)는 원격 공격자에게 피해 시스템에 대한 전체 권한을 부여하는 원격 조정 트로이목마이다. 파일 업로드, 응용 프로그램 실행, 문서 유출, 파일 삭제 등을 수행하며, 일반적으로 일단 실행되면 특정 시스템 폴더에 자신을 복사한 후 운영체제를 시작할 때마다 트로이목마가 실행되어 레지스트리 값을 만든다. 또한, 피해 시스템에 키로거 파일을 삽입하여 사용자가 입력한 사항을 감시하고 기록한다.

오답피하기 ③ Netbus는 원격 조정 트로이목마이다. 소프트웨어를 실행하거나 설치 후 자동적으로 광고를 표시하는 프로그램은 adware이다.

정답 ③

3. ○△× 19.국가.9급

정보보호 서비스에 대한 설명으로 옳지 않은 것은?

① Authentication – 정보교환에 의해 실체의 식별을 확실하게 하거나 임의 정보에 접근할 수 있는 객체의 자격이나 객체의 내용을 검증하는 데 사용한다.

② Confidentiality – 온오프라인 환경에서 인가되지 않은 상대방에게 저장 및 전송되는 중요정보의 노출을 방지한다.

③ Integrity – 네트워크를 통하여 송수신되는 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호한다.

④ Availability – 행위나 이벤트의 발생을 증명하여 나중에 행위나 이벤트를 부인할 수 없도록 한다.

◘ 가용성(Availability)

◦ 시스템이 지체 없이 동작하도록 하고, 합법적 사용자가 서비스 사용을 거절당하지 않도록 하는 것이다.

◦ 정보는 지속적으로 변화하며, 이는 인가된 자가 접근할 수 있어야 함을 의미한다. 정보의 비가용성은 조직에 있어 기밀성이나 무결성의 부족만큼이나 해롭다.

◦ 가용성을 확보하기 위해서는 데이터의 백업, 중복성의 유지, 물리적 위협요소로부터의 보호 등의 보안 기술을 적용해야 한다.

오답피하기 ④ 행위나 이벤트의 발생을 증명하여 나중에 행위나 이벤트를 부인할 수 없도록 하는 것은 정보보호 서비스 중 부인방지에 대한 설명이다.

정답 ④

4. ○△× 19.국가.9급

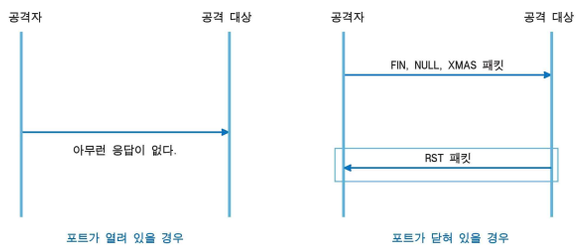
다음에서 설명하는 스캔방법은?

보기

공격자가 모든 플래그가 세트되지 않은 TCP 패킷을 보내고, 대상 호스트는 해당 포트가 닫혀 있을 경우 RST 패킷을 보내고, 열려 있을 경우 응답을 하지 않는다.

① TCP Half Open 스캔
② NULL 스캔
③ FIN 패킷을 이용한 스캔
④ 시간차를 이용한 스캔

FIN, NULL, XMAS 스캔



오답피하기 ② Null 스캔은 플래그 값을 모두 설정하지 않고(off) 스캔하는 방법을 말한다. Null 스캔은 포트가 열려있을 경우에는 응답이 없고, 닫혀있을 경우에만 RST 패킷이 되돌아온다.

정답 ②

5. ○△× 19.국가.9급

SSL(Secure Socket Layer) 프로토콜에 대한 설명으로 옳지 않은 것은?

① ChangeCipherSpec – Handshake 프로토콜에 의해 협상된 암호규격과 암호키를 이용하여 추후의 레코드 계층의 메시지를 보호할 것을 지시한다.
② Handshake – 서버와 클라이언트 간 상호인증 기능을 수행하고, 암호화 알고리즘과 이에 따른 키 교환 시 사용된다.
③ Alert – 내부적 및 외부적 보안 연관을 생성하기 위해 설계된 프로토콜이며, Peer가 IP 패킷을 송신할 필요가 있을 때, 트래픽의 유형에 해당하는 SA가 있는지를 알아보기 위해 보안 정책 데이터베이스를 조회한다.
④ Record – 상위계층으로부터(Handshake 프로토콜, ChangeCipherSpec 프로토콜, Alert 프로토콜 또는 응용층) 수신하는 메시지를 전달하며 메시지는 단편화되거나 선택적으로 압축된다.

오답피하기 ③ Alert 프로토콜은 비정상 조건을 알리는데 사용된다. 보기는 IKE 프로토콜에 대한 설명이다.

정답 ③

6. ○△× 19.국가.9급

블록체인에 대한 설명으로 옳지 않은 것은?

① 금융 분야에만 국한되지 않고 분산원장으로 각 분야에 응용할 수 있다.
② 블록체인의 한 블록에는 앞의 블록에 대한 정보가 포함되어 있다.
③ 앞 블록의 내용을 변경하면 뒤에 이어지는 블록은 변경할 필요가 없다.
④ 하나의 블록은 트랜잭션의 집합과 헤더(header)로 이루어져 있다.

블록체인

◦ 블록체인은 기존 중앙집중형 네트워크 기반의 인프라를 뛰어넘는 높은 보안성·확장성·투명성을 제공하는 분산 컴퓨팅 기술로써 4차 산업혁명의 기반 기술이자 핵심 기술이다. 블록체인은 다수의 노드들이 거래내역을 검증하여 블록 형태로 보관하기 때문에 위·변조가 매우 어렵고 데이터의 신뢰성을 기반으로 제3자 없이 거래가 가능하다.
◦ 블록체인 상의 모든 데이터는 그 이전의 데이터와 연결되어 서로 연관성을 가진다. 이 연관성 때문에 하나의 데이터만 따로 수정하는 것이 불가능하다.
◦ 블록은 헤더(HEADER)와 바디(BODY : 트랜잭션)로 이루어져 있다.

오답피하기 ③ 분산 공개 장부는 여러 개의 노드에 복사되어 있으며, 여러 개의 노드는 P2P로 연결되어 블록체인 네트워크를 형성한다. 그리고 하나의 거래 정보가 발생하면 이 거래 정보는 블록체인 네트워크에 분산되어 있는 수많은 노드에 전파되어야 한다.

정답 ③

7. ○△× 19.국가.9급

다음의 결과에 대한 명령어로 옳은 것은?

보기

Thu Feb 7 20:33:56 2019 1 198.188.2.2 861486 /tmp/12-67-ftp1.bmp b _ o r freeexam ftp 0 * c 861486 0

① cat /var/adm/messages
② cat /var/log/xferlog
③ cat /var/adm/loginlog
④ cat /etc/security/audit_event

◦ messages : 시스템의 가장 기본적인 시스템 로그파일로서 시스템 운영에 대한 전반적인 메시지를 저장한다.
◦ loginlog, btmp : 실패한 모든 로그를 남긴다.

오답피하기 ② xferlog 로그는 FTP 로그 파일로서 proftpd 또는 vsftpd 데몬들의 서비스 내역을 기록하는 파일이다. 공격자가 FTP 서비스를 이용해 시스템에서 어떤 파일을 복사했는지, 또 어떤 파일을 시스템에 복사해 두었는지 찾아내야 할 때 유용하다. 파일을 전송한 날짜와 시간, 접근 시스템의 IP, 전송한 파일을 확인할 수 있다.

정답 ②

8. ○△× 19.국가.9급

다음 설명에 해당하는 DoS 공격을 옳게 짝 지은 것은?

보기

ㄱ. 공격자가 공격대상의 IP 주소로 위장하여 중계 네트워크에 다량의 ICMP Echo Request 패킷을 전송하며, 중계 네트워크에 있는 모든 호스트는 많은 양의 ICMP Echo Reply 패킷을 공격 대상으로 전송하여 목표시스템을 다운시키는 공격

ㄴ. 공격자가 송신자 IP 주소를 존재하지 않거나 다른 시스템의 IP 주소로 위장하여 목적 시스템으로 SYN 패킷을 연속해서 보내는 공격

ㄷ. 송신자 IP 주소와 수신자 IP 주소, 송신자 포트와 수신자 포트가 동일하게 조작된 SYN 패킷을 공격 대상에 전송하는 공격

ㄱ ㄴ ㄷ

① Smurf Attack / Land Attack / SYN Flooding Attack
② Smurf Attack / SYN Flooding Attack / Land Attack
③ SYN Flooding Attack / Smurf Attack / Land Attack
④ Land Attack / Smurf Attack / SYN Flooding Attack

◦ Smurf 공격 : IP 위장과 ICMP의 특징을 이용한 공격
◦ Syn flooding 공격 : 3-Way Handshaking 과정에서 Half-Open 연결 시도가 가능하다는 취약점을 이용한 공격
◦ Land attack : 자신의 IP 어드레스와 포트를 대상 서버의 IP 어드레스 및 포트와 동일하게 하여 전송하는 공격

오답피하기 ② 각각 Smurf Attack, SYN Flooding Attack, Land Attack 공격에 대한 설명이다.

정답 ②

9. ○△× 19.국가.9급

무선 LAN 보안에 대한 설명으로 옳지 않은 것은?

① WPA2는 RC4 알고리즘을 암호화에 사용하고, 고정 암호키를 사용한다.
② WPA는 EAP 인증 프로토콜(802.1x)과 WPA-PSK를 사용한다.
③ WEP는 64비트 WEP 키가 수분 내 노출되어 보안이 매우 취약하다.
④ WPA-PSK는 WEP보다 훨씬 더 강화된 암호화 세션을 제공한다.

오답피하기 ① WPA2는 2세대 WPA로서 TKIP를 대체하기 위해 AES에 기반을 둔 CCMP(Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) 암호화 방식을 사용하며, IEEE 802.11i 수정안을 포함한 보안 기술이다.

정답 ①

10. ○△× 19.국가.9급

사용자 A가 사용자 B에게 해시함수를 이용하여 인증, 전자서명, 기밀성, 무결성이 모두 보장되는 통신을 할 때 구성해야 하는 함수로 옳은 것은?

보기

K : 사용자 A와 B가 공유하고 있는 비밀키
KS_a : 사용자 A의 개인키, KP_a : 사용자 A의 공개키
H : 해시함수, E : 암호화
M : 메시지, || : 두 메시지의 연결

① $E_K[M \| H(M)]$
② $M \| E_K[H(M)]$
③ $M \| E_{KS_a}[H(M)]$
④ $E_K[M \| E_{KS_a}[H(M)]]$

◘ 부가형 전자서명
◦ 임의의 길이로 주어진 메시지를 해시 알고리즘을 이용하여 일정한 길이로 압축하고, 해시한 결과에 서명자의 개인키를 이용하여 전자서명한 후 메시지에 덧붙여 전송한다.
◦ 전자서명의 검증은 수신된 메시지를 해시한 결과와 공개키를 이용하여 전자서명을 복호화한 값과 비교함으로써 이루어진다.

◘ 전자서명의 기밀성
◦ 전자서명을 한다고 해서 기밀성이 보장되는 통신을 할 수는 없다. 만약 기밀성이 필요하다면 메시지와 서명에 비밀키를 이용하거나 공개키를 이용해서 암호화를 해야만 한다.

오답피하기 ④ 해시함수를 이용하여 인증, 기밀성, 무결성 서비스를 모두 보장하기 위해서는 부가형 전자서명과 암호화 방법을 병행해야 한다. 보기는 해시한 결과값에 개인키로 서명한 후 메시지와 연결한

정답 ④

11. ○△× 19.국가.9급

다음 알고리즘 중 공개키 암호 알고리즘에 해당하는 것은?

① SEED 알고리즘
② RSA 알고리즘
③ DES 알고리즘
④ AES 알고리즘

오답피하기 ② SEED, DES, AES 알고리즘은 대칭키 암호 알고리즘이고, RSA 알고리즘은 공개키 암호 알고리즘이다.

정답 ②

12. ○△× 19.국가.9급

정보보안 관련 용어에 대한 설명으로 옳지 않은 것은?

① 부인방지(Non-repudiation) – 사용자가 행한 행위 또는 작업을 부인하지 못하는 것이다.
② 최소권한(Least Privilege) – 계정이 수행해야 하는 작업에 필요한 최소한의 권한만 부여한다.
③ 키 위탁(Key Escrow) – 암호화 키가 분실된 경우를 대비하여 키를 보관하는 형태를 의미한다.
④ 차분 공격(Differential Attack) – 대용량 해쉬 테이블을 이용하여 충분히 작은 크기로 줄여 크랙킹 하는 방법이다.

키 위탁(Key-Escrow) 방식

◦ 복구될 사용자의 비밀키, 비밀키의 부분 또는 키 관련 정보를 하나 이상의 신뢰 기관에 위탁하는 방식으로 위탁된 키는 사용자가 오랫동안 사용하게 되는 경우가 많다.
◦ 키 위탁 방식에서는 사용자의 비밀키를 위탁 기관에 직접 맡겨져야 하므로 개인의 프라이버시를 전적으로 위탁 기관에 의존한다는 문제점을 안고 있다.
◦ 그러므로 위탁 기관의 신뢰성이 매우 중요한 문제이며 이를 보장하기 위한 방법으로 두 개 이상의 위탁 기관을 이용하는 비밀 분산 개념이 주로 사용되고 있다.
◦ 키 위탁 방식은 유사시에 키 복구를 확실하게 할 수 있다는 장점이 있으며, 위탁 기관의 신뢰성만 보장된다면 편리하고 안전한 키 복구 방식이다.
◦ 키 위탁 방식에 속하는 키 복구 시스템들 중 가장 대표적인 것은 Clipper 키 복구 시스템이다.

레인보우 테이블을 이용한 공격

◦ 레인보우 테이블의 기본적인 개념은 패스워드별로 해시 값을 미리 생성해놓는 것이다. 즉, 크래킹 하고자 하는 해시 값을 테이블에서 검색하여, 거꾸로 원래의 패스워드를 찾는 것이다.
◦ 하지만 이런 식으로 사용 가능한 모든 패스워드에 대해 해시값을 구해놓는다면, 엄청난 용량의 파일이 필요하다. 레인보우 테이블의 또 다른 핵심 아이디어는 대용량으로 생성될 수 있는 해시 테이블을 R(Reduction) 함수를 이용해 충분히 작은 크기로 줄이는 것이다. 물론 줄이더라도 레인보우 테이블은 보통 몇십 기가 바이트 정도의 용량으로 생성된다.

오답피하기 ④ 차분 공격은 입력되는 평문이 한 비트라도 달라지면 암호문은 전혀 다른 비트 패턴으로 변화하게 된다. 그래서 암호문의 변화 형태를 조사하여 해독의 실마리를 얻는 해독 방법이다. 보기는 레인보우 테이블을 이용한 공격에 대한 설명이다.

정답 ④

13. ○△× 19.국가.9급

공통평가기준은 IT 제품이나 특정 사이트의 정보시스템의 보안성을 평가하는 기준이다. '보안기능요구사항'과 '보증요구사항'을 나타내는 보호프로파일(PP), 보호목표명세서(ST)에 대한 설명으로 옳지 않은 것은?

① 보호프로파일은 구현에 독립적이고, 보호목표명세서는 구현에 종속적이다.
② 보호프로파일은 보호목표명세서를 수용할 수 있고, 보호목표명세서는 보호프로파일을 수용할 수 있다.
③ 보호프로파일은 여러 시스템·제품을 한 개 유형의 보호프로파일로 수용할 수 있으나, 보호목표명세서는 한 개의 시스템·제품을 한 개의 보호목표명세서로 수용해야 한다.
④ 보호프로파일은 오퍼레이션이 완료되지 않을 수 있으나, 보호목표명세서는 모든 오퍼레이션이 완료되어야 한다.

PP와 ST의 비교

구분	보호 프로파일	보안 목표명세서
구현의 독립성	구현에 독립적이다.	구현에 종속적이다.
적용 제품	제품군(예 : 방화벽)	특정 제품 (예 : A사 방화벽)
오퍼레이션 종류	오퍼레이션이 완료되지 않을 수 있다.	모든 오퍼레이션이 완료되어야 한다.
시스템/제품별 적용방법	여러 시스템/제품이 하나의 동일한 유형의 보호 프로파일을 수용할 수 있다.	하나의 시스템/제품은 하나의 보안 목표명세서로 작성된다.
보호 프로파일 수용여부	보호 프로파일은 보안 목표명세서를 수용할 수 없다.	보안 목표명세서는 보호 프로파일을 수용할 수 있다.
표현 방법	「What I want?」를 표현	「What I have?」를 표현

오답피하기 ② 보호프로파일은 보호목표명세서를 수용할 수 없고, 보호목표명세서는 보호프로파일을 수용할 수 있다.

정답 ②

14. ○△× 19.국가.9급

방화벽 구축 시 내부 네트워크의 구조를 외부에 노출하지 않는 방법으로 적절한 것은?

① Network Address Translation
② System Active Request
③ Timestamp Request
④ Fragmentation Offset

오답피하기 ① 네트워크 주소 변환(NAT)은 사설 주소와 범용 주소의 매핑을 제공하고 동시에 가상 사설 네트워크를 지원하는 기술이다. 이 기술은 한곳에서 내부 통신을 위해 사설 주소를 사용하고 다른 네트워크와의 통신에는 범용 인터넷 주소를 사용할 수 있도록 해준다. 이를 통해 외부에서 내부 네트워크로 직접적인 접근이 불가능하게 되므로 네트워크 보안효과를 가져올 수 있다.

정답 ①

15. ○△× 19.국가.9급

「개인정보 보호법 시행령」상 개인정보 영향평가의 대상에 대한 규정의 일부이다. ㉠, ㉡에 들어갈 내용으로 옳은 것은?

보기

제35조(개인정보 영향평가의 대상) 「개인정보 보호법」 제33조제1항에서 "대통령령으로 정하는 기준에 해당하는 개인정보파일"이란 개인정보를 전자적으로 처리할 수 있는 개인정보파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다.

1. 구축운용 또는 변경하려는 개인정보파일로서 (㉠) 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일
2. 구축운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만 명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일
3. 구축운용 또는 변경하려는 개인정보파일로서 (㉡) 이상의 정보주체에 관한 개인정보파일

	㉠	㉡
①	5만 명	100만 명
②	10만 명	100만 명
③	5만 명	150만 명
④	10만 명	150만 명

시행령 제35조(개인정보 영향평가의 대상)

법 제33조제1항에서 "대통령령으로 정하는 기준에 해당하는 개인정보파일"이란 개인정보를 전자적으로 처리할 수 있는 개인정보파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다.

1. 구축·운용 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 법 제23조에 따른 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일
2. 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일
3. 구축·운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일
4. 법 제33조제1항에 따른 개인정보 영향평가를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일. 이 경우 영향평가 대상은 변경된 부분으로 한정한다.

오답피하기 ① 개인정보 영향평가란 개인정보 수집·활용이 수반되는 사업 추진 시 개인정보 오남용으로 인한 프라이버시 침해 위험이 잠재되어 있지 않는지를 조사·예측·검토하고 개선하는 제도로 시행령제35조에 명시된 영향평가 대상은 반드시 숙지해야 한다.

정답 ①

16. ○△× 19.국가.9급

버퍼 오버플로우(Buffer Overflow) 공격에 대한 대응으로 해당하지 않는 것은?

① 안전한 함수 사용
② Non-Executable 스택
③ 스택 가드(Stack Guard)
④ 스택 스매싱(Stack Smashing)

스택 버퍼 오버플로우(stack buffer overflow)

- 스택 버퍼 오버플로우 공격은 보통 SetUID(Set User ID)가 설정된 루트 권한의 프로그램을 공격대상으로 한다. 스택에 정해진 버퍼보다 큰 공격 코드를 삽입하여 반환주소를 변경함으로써 임의의 공격 코드를 루트 권한으로 실행하도록 하는 방법이다.
- 스택 버퍼 오버플로우는 함수의 스택 프레임 내부에 있는 지역 변수처럼 타깃 버퍼가 스택에 위치할 때 발생한다. 이런 공격 유형을 스택 스매싱(stack smashing)이라고도 부른다.

오답피하기 ④ 안전한 함수 사용, Non-Executable 스택, 스택 가드(Stack Guard)는 버퍼 오버플로우 공격에 대한 대응책인 반면에 스택 스매싱(Stack Smashing)은 공격유형이다.

정답 ④

17. ○△× 19.국가.9급

블록체인(Blockchain) 기술과 암호화폐(Cryptocurrency) 시스템에 대한 설명으로 옳지 않은 것은?

① 블록체인에서는 각 트랜잭션에 한 개씩 전자서명이 부여된다.
② 암호학적 해시를 이용한 어려운 문제의 해를 계산하여 블록체인에 새로운 블록을 추가할 수 있고 일정량의 암호화폐로 보상받을 수도 있다.
③ 블록체인의 과거 블록 내용을 조작하는 것은 쉽다.
④ 블록체인은 작업증명(Proof-of-work)과 같은 기법을 이용하여 합의에 이른다.

- 작업증명(Proof-of-Work) 방식의 합의 알고리즘은 비트코인에서 사용되는 합의 알고리즘으로써 어떤 트랜잭션이 발생했을 경우 해당 트랜잭션이 유효한 트랜잭션인지에 대한 합의 방법 및 새로운 블록이 진짜인지, 가짜인지에 대한 검증을 수행한다.

오답피하기 ③ 거래내역을 위/변조하기 위해서는 해당 블록의 해시값을 통해 연결된 모든 블록의 정보를 연쇄적으로 다 바꿔어야 한다. 그리고 일정시간마다 하나씩 생성되는 블록보다 더 빠르게 위/변조한 정보를 전파시켜야 하는데, 이는 실존하는 세계에서 가장 빠른 슈퍼컴퓨터의 성능을 넘는 연산력을 요구하기 때문에 현실적으로 실현이 불가능하다.

정답 ③

18. ○△× 19.국가.9급

「정보통신기반 보호법」상 주요정보통신기반시설의 보호체계에 대한 설명으로 옳지 않은 것은?

① 주요정보통신기반시설 관리기관의 장은 정기적으로 소관 주요정보통신시설의 취약점을 분석·평가하여야 한다.
② 중앙행정기관의 장은 소관분야의 정보통신기반시설을 필요한 경우 주요정보통신기반시설로 지정할 수 있다.
③ 지방자치단체의 장이 관리·감독하는 기관의 정보통신기반시설은 지방자치단체의 장이 주요정보통신기반시설로 지정한다.
④ 과학기술정보통신부장관과 국가정보원장등은 특정한 정보통신기반시설을 주요정보통신기반시설로 지정할 필요가 있다고 판단하면 중앙행정기관의 장에게 해당 정보통신기반시설을 주요정보통신기반시설로 지정하도록 권고할 수 있다.

◘ 제8조(주요정보통신기반시설의 지정 등)
① 중앙행정기관의 장은 소관분야의 정보통신기반시설중 다음 각호의 사항을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다.
1. 당해 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성
2. 제1호의 규정에 의한 기관이 수행하는 업무의 정보통신기반시설에 대한 의존도
3. 다른 정보통신기반시설과의 상호연계성
4. 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위
5. 침해사고의 발생가능성 또는 그 복구의 용이성
② 중앙행정기관의 장은 제1항의 규정에 의한 지정 여부를 결정하기 위하여 필요한 자료의 제출을 해당 관리기관에 요구할 수 있다.
③ 관계중앙행정기관의 장은 관리기관이 해당 업무를 폐지·정지 또는 변경하는 경우에는 직권 또는 해당 관리기관의 신청에 의하여 주요정보통신기반시설의 지정을 취소할 수 있다.
④ 지방자치단체의 장이 관리·감독하는 기관의 정보통신기반시설에 대하여는 행정안전부장관이 지방자치단체의 장과 협의하여 주요정보통신기반시설로 지정하거나 그 지정을 취소할 수 있다.
⑤ 중앙행정기관의 장이 제1항 및 제3항의 규정에 의하여 지정 또는 지정취소를 하고자 하는 경우에는 위원회의 심의를 받아야 한다. 이 경우 위원회는 제1항 및 제3항의 규정에 의하여 지정 또는 지정취소의 대상이 되는 관리기관의 장을 위원회에 출석하게 하여 그 의견을 들을 수 있다.
⑥ 중앙행정기관의 장은 제1항 및 제3항의 규정에 의하여 주요정보통신기반시설을 지정 또는 지정 취소한 때에는 이를 고시하여야 한다. 다만, 국가안전보장을 위하여 필요한 경우에는 위원회의 심의를 받아 이를 고시하지 아니할 수 있다.
⑦ 주요정보통신기반시설의 지정 및 지정취소 등에 관하여 필요한 사항은 이를 대통령령으로 정한다.

오답피하기 ③ 지방자치단체의 장이 관리·감독하는 기관의 정보통신기반시설에 대하여는 지방자치단체의 장이 아닌 행정안전부장관이 지방자치단체의 장과 협의하여 주요정보통신기반시설로 지정하거나 그 지정을 취소할 수 있다.

정답 ③

19. ○△× 19.국가.9급

업무연속성(BCP)에 대한 설명으로 옳지 않은 것은?

① 업무연속성은 장애에 대한 예방을 통한 중단 없는 서비스 체계와 재난 발생 후에 경영 유지·복구 방법을 명시해야 한다.
② 재해복구시스템의 백업센터 중 미러 사이트(Mirror Site)는 백업센터 중 가장 짧은 시간 안에 시스템을 복구한다.
③ 콜드 사이트(Cold Site)는 주전산센터의 장비와 동일한 장비를 구비한 백업 사이트이다.
④ 재난복구서비스인 웜 사이트(Warm Site)는 구축 및 유지비용이 콜드 사이트(Cold Site)에 비해서 높다.

◦ 비즈니스 연속성 계획(BCP)은 재난 발생 시 비즈니스 연속성을 유지하려는 방법을 정의하는 문서로서 재해, 재난에도 정상적인 운영이 가능하도록 데이터 백업 및 단순 복구뿐만 아니라 고객 서비스 지속성 보장, 핵심 업무 기능을 지속하는 환경 조성을 목적으로 한다.

오답피하기 ③ 주전산센터의 장비와 동일한 장비를 구비한 백업 사이트는 미러사이트 또는 핫 사이트이다.

정답 ③

20. ○△× 19.국가.9급

「개인정보 보호법 시행령」의 내용으로 옳지 않은 것은?

① 공공기관의 영상정보처리기기는 재위탁하여 운영할 수 없다.
② 개인정보처리자가 전자적 파일 형태의 개인정보를 파기하여야 하는 경우 복원이 불가능한 형태로 영구 삭제하여야 한다.
③ 개인정보처리자는 개인정보의 처리에 대해서 전화를 통하여 동의 내용을 정보주체에게 알리고 동의 의사표시를 확인하는 방법으로 동의를 받을 수 있다.
④ 공공기관이 개인정보를 목적 외의 용도로 이용하는 경우에는 '이용하거나 제공하는 개인정보 또는 개인정보파일의 명칭'을 개인정보의 목적 외 이용 및 제3자 제공 대장에 기록하고 관리하여야 한다.

◘ 시행령 제17조(동의를 받는 방법)
① 개인정보처리자는 법 제22조에 따라 개인정보의 처리에 대하여 다음 각 호의 어느 하나에 해당하는 방법으로 정보주체의 동의를 받아야 한다.
1. 동의 내용이 적힌 서면을 정보주체에게 직접 발급하거나 우편 또는 팩스 등의 방법으로 전달하고, 정보주체가 서명하거나 날인한 동의서를 받는 방법
2. 전화를 통하여 동의 내용을 정보주체에게 알리고 동의의 의사표시를 확인하는 방법
3. 전화를 통하여 동의 내용을 정보주체에게 알리고 정보주체에게 인터

넷주소 등을 통하여 동의 사항을 확인하도록 한 후 다시 전화를 통하여 그 동의 사항에 대한 동의의 의사표시를 확인하는 방법

4. 인터넷 홈페이지 등에 동의 내용을 게재하고 정보주체가 동의 여부를 표시하도록 하는 방법
5. 동의 내용이 적힌 전자우편을 발송하여 정보주체로부터 동의의 의사표시가 적힌 전자우편을 받는 방법
6. 그 밖에 제1호부터 제5호까지의 규정에 따른 방법에 준하는 방법으로 동의 내용을 알리고 동의의 의사표시를 확인하는 방법

◘ 시행령 제15조(개인정보의 목적 외 이용 또는 제3자 제공의 관리) 공공기관은 법 제18조제2항 각 호에 따라 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우에는 다음 각 호의 사항을 행정안전부령으로 정하는 개인정보의 목적 외 이용 및 제3자 제공 대장에 기록하고 관리하여야 한다.

1. 이용하거나 제공하는 개인정보 또는 개인정보파일의 명칭
2. 이용기관 또는 제공받는 기관의 명칭
3. 이용 목적 또는 제공받는 목적
4. 이용 또는 제공의 법적 근거
5. 이용하거나 제공하는 개인정보의 항목
6. 이용 또는 제공의 날짜, 주기 또는 기간
7. 이용하거나 제공하는 형태
8. 법 제18조제5항에 따라 제한을 하거나 필요한 조치를 마련할 것을 요청한 경우에는 그 내용

◘ 시행령 제26조(공공기관의 영상정보처리기기 설치 · 운영 사무의 위탁)

① 법 제25조제8항 단서에 따라 공공기관이 영상정보처리기기의 설치 · 운영에 관한 사무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서로 하여야 한다.

1. 위탁하는 사무의 목적 및 범위
2. 재위탁 제한에 관한 사항
3. 영상정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
4. 영상정보의 관리 현황 점검에 관한 사항
5. 위탁받는 자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

오답피하기 ① 영상정보처리기기운영자는 영상정보처리기기의 설치 · 운영에 관한 사무를 위탁할 수 있다. 특히, 공공기관은 사무를 위탁하는 경우 문서에 재위탁 제한에 관한 사항 등을 포함시킬 수 있으나 모든 업무의 제한으로 보기는 힘들다.

정답 ①

[정답표]

1	2	3	4	5
②	③	④	②	③
6	7	8	9	10
③	②	②	①	④
11	12	13	14	15
②	④	②	①	①
16	17	18	19	20
④	③	③	③	①