2021-국가직-7급-정보보호론-가-해설-곽후근

1. 사용자 인증에 사용되는 기술로 옳지 않은 것은?
① Smart Card
② Single Sign On
③ One Time Password
④ Supervisory Control And Data Acquisition
정답 체크
(4) 산업 공정/기반 시설/설비를 바탕으로 한 작업공정을 감시하고 제어하는 컴퓨터 시스템을 말한다. 스턱스넷에 나오는 용어로 사용자 인증과 무관하다.
오답 체크
(1), (3) 소유(소지) 기반 인증에 해당된다.
(2) 모든 인증을 하나의 시스템에서 한다는 의미이다. 시스템이 몇 대가 되어도 하나의 시스템에서 인증에 성공하면, 다른 시스템에 대한 접근 권한도 모두 얻는다. 이러한 접속 형태의 대표적인 인증 방법으로는 커버로스(Kerberos)를 이용한 윈도우의 액티브 디렉토리(Active Directory)가 있다. 지식 기반 인증에 사용된다.

2. 제로 데이 공격에 대한 설명으로 옳은 것은?
① 서버의 성능을 크게 떨어뜨리거나 서버를 정지시키는 방법으로 서버의 정상적인 작동을 방해하는 공격 방법이다.
② 패스워드 사전 파일을 이용해 미리 지정한 아이디에 대입하여 접속계정을 알아내는 공격 방법이다.
③ 패치가 나오지 않은 시점에 이루어지는 공격 방법이다.
④ 버퍼에 일정 크기 이상의 데이터를 입력하여 프로그램을 공격하는 방법이다.
정답 체크
(3) 프로그램에 문제(보안취약점)가 알려지고 난 후 보안패치가 나올 때까지 시간차를 이용해 공격하는 기법을 말한다.
오답 체크
(1) 서비스 거부(DoS) 공격을 의미한다.
(2) 사전 공격을 이용한 패스워드 크래킹을 의미한다.
(4) 버퍼 오버플로우 공격을 의미한다.

3. IPSec 프로토콜의 기능이 아닌 것은?
① Pretty Good Privacy
② Authentication Header
③ Internet Key Exchange
④ Encapsulating Security Payload
정답 체크
(1) 이메일 보안이다.
오답 체크
(2) 인증, 무결성을 보장한다.

(3) SA를 협상한다.
(4) 인증, 무결성, 기밀성을 보장한다.

4. 다음 설명에 해당하는 악성코드는?

○ 사용자 동의 없이 설치되어 컴퓨터의 정보를 수집하고 전송하는 악성소프트웨어 ○ 신용카드와 같은 금융정보 및 주민등록번호와 같은 신상정보, 암호를 비롯한 각종 정보를 수집

① ransomware
② spyware
③ backdoor
④ dropper

정답 체크
(2) 사용자의 동의 없이 설치되어 컴퓨터의 정보를 수집하고 전송하는 악성 소프트웨어로, 신용 카드와 같은 금융 정보 및 주민등록번호와 같은 신상정보, 암호를 비롯한 각종 정보를 수집한다.
오답 체크
(1) 컴퓨터 시스템을 감염시켜 접근을 제한하고 일종의 몸값을 요구하는 악성 소프트웨어의 한 종류이다.
(3) 운영체제나 프로그램을 생성할 때 정상적인 인증 과정을 거치지 않고, 운영체제나 프로그램 등에 접근할 수 있도록 만든 일종의 통로이다.
(4) 대상 시스템에 악성코드를 설치하기 위해 설계된 프로그램이다. 악성코드는 드로퍼 내에 포함되어 있음으로써 바이러스 스캐너에 의한 탐지를 피하고, 실행된 이후에는 드로퍼에 의해 악성코드가 다운로드 됨으로써 설치될 수 있다.

5. 다음 설명에 해당하는 블루투스 공격을 옳게 짝지은 것은?

(가) 공격이 가능한 블루투스 장치들을 검색하고 모델을 확인하는 공격 (나) 블루투스 장치 내 저장된 데이터에 대한 접근을 허용하는 공격 (다) 블루투스 지원 장치에 대한 접근권한을 획득하는 공격

	(가)	(나)	(다)
①	bluesnarf	bluebug	blueprinting
②	bluesnarf	blueprinting	bluebug
③	blueprinting	bluebug	bluesnarf
④	blueprinting	bluesnarf	bluebug

정답 체크 (PSB)
(4) blueprinting : 블루투스 공격 장치의 검색 활동이다. 블루투스는 장치 간 종류를 식별하기 위해 서비스 발견 프로토콜(SDP: Service Discovery Protocol)을 보내고 받는다. 공격자는 이를 이용해 공격이 가능한 블루투스 장치를 검색하고 모델을 확인할 수 있다.
bluesnarf : 블루투스의 취약점을 이용하여 장비의 임의 파일에 접근한다. 공격자는 블루투스 장치끼리 인증 없이 정보를 간편하게 교환할 수 있는 OPP(OBEX Push Profile)를 사용하여 정보를 열

람할 수 있다.
bluebug : 블루투스 장비 간 취약한 연결 관리를 악용한다. 블루투스 기기는 한 번 연결되면 이후에는 다시 연결해주지 않아도 서로 연결된다. 이 인증 취약점을 이용하여 공격이다.

6. 암호화에 대한 설명으로 옳은 것은?
① 대칭키 암호 방식은 암호화 키와 복호화 키가 다른 암호화 방법으로 암호화 키는 공개되고, 복호화 키는 공개되지 않는 구조로서 다수의 정보교환자 간의 통신에 적합하다.
② 공개키 암호에는 RSA, ElGamal 등이 있으며, 처리속도가 대칭키 알고리즘에 비해 매우 느린 단점이 있으나 키 전달이 편리하여 키교환 알고리즘으로 사용되며, 전자서명을 용이하게 구현할 수 있는 특징이 있다.
③ 블록 암호는 이진화된 평문과 키 이진수열을 배타적 논리합 이진 연산으로 결합하여 암호문을 생성하고, 블록 대칭 알고리즘에는 선형 쉬프트 레지스터 등이 있다.
④ 공개키 암호 방식은 암호화 키와 복호화 키가 동일한 암호화 방법으로 두 키가 동일하게 이용되며, 데이터를 변화하는 방법에 따라서 스트림암호와 블록암호로 나누어지고 기밀성용으로만 사용된다.
정답 체크
(2) 공개키 암호에는 RSA, ElGamal, Rabin, ECC 등이 있으며, 처리속도가 수학적 연산으로 인해 느리며 키 배송 문제가 발생하지 않는다. 그리고 개인키 암호화 방식을 적용하며 디지털 서명을 할 수 있다.
오답 체크
(1) 해당 설명은 공개키 암호 방식을 의미한다.
(3) 해당 설명은 스트림 암호 방식을 의미하고, 블록 암호는 평문을 일정한 단위(블록)로 나누어서 각 단위 마다 암호화 과정을 수행하여 암호문을 얻는 방법이다.
(4) 해당 설명은 대칭키 암호 방식을 의미한다.

7. 해시에 대한 설명으로 옳지 않은 것은?
① 해시 알고리즘에는 MD5, SHA 등이 있다.
② 해시는 메시지의 무결성을 확인하기 위해서 사용한다.
③ 해시 알고리즘 SHA는 유럽 RIPE 프로젝트에 의해 개발된 해시함수이다.
④ 해시는 임의의 길이 메시지로부터 고정 길이의 해시값을 계산한다.
정답 체크
(3) 미국 국가안보국(NSA)이 개발해 미국 국립표준기술원(NIST)이 연방 표준으로 공표했다(FIPS).
오답 체크
(1) MD5, SHA, RIPEMD 등이 있다.
(2) 메시지의 무결성(변조 여부)을 확인한다.
(4) 입력 길이의 제한이 있는 해시 함수가 존재한다(SHA-1, SHA-2).

8. PPTP 프로토콜에 대한 설명으로 옳은 것은?
① 3계층인 네트워크 계층에서 동작한다.
② 마이크로소프트가 제안한 VPN 프로토콜로 PPP를 기반으로 한다.
③ 데이터를 스니핑한 뒤 해당 데이터를 다시 보내는 replay attack을 막을 수 있다.

④ 데이터가 전송 도중에 변조되었는지를 확인할 수 있도록 데이터 무결성을 검사한다.
정답 체크
(2) 마이크로소프트가 제안한 VPN 터널링 프로토콜로 PPP(1:1)을 기반으로 한다.
오답 체크
(1) 2계층인 데이터 링크 계층에서 동작한다.
(3) 2계층에서 막을 수 없고, 3계층인 IPSec에서 막을 수 있다(VPN이라면).
(4) 2계층에서 검사할 수 없고, 3계층인 IPSec에서 막을 수 있다(VPN이라면).

9.「개인정보 보호법」 제24조의2(주민등록번호 처리의 제한)에서 제24조제1항에도 불구하고 개인정보처리자가 주민등록번호를 처리할 수 있는 경우가 아닌 것은?
① 수탁자가 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하는 경우
② 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
③ 제24조의2제1항제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 개인정보 보호위원회가 고시로 정하는 경우
④ 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
정답 체크
(1) 제26조(업무위탁에 따른 개인정보의 처리 제한) 수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다.
오답 체크
(2), (3), (4)
제24조의2(주민등록번호 처리의 제한) ① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.
1. 법률 · 대통령령 · 국회규칙 · 대법원규칙 · 헌법재판소규칙 · 중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 보호위원회가 고시로 정하는 경우

10. 블록체인의 비트코인 블록헤더 구조에 대한 설명으로 옳지 않은 것은?
① Nonce는 4바이트로 구성된다.
② Timestamp는 블록을 생성한 시간이다.
③ Previous Block Hash는 32바이트로 구성된다.
④ Block Header는 5가지 필드로 구성하고 크기는 60바이트로 고정되어 있다.
정답 체크
(4) 6가지 필드(Version, Previous Block Hash, Merkle Root, Timestamp, Difficulty Target, Nonce)로 구성하고 크기는 80바이트(4, 32, 32, 4, 4, 4)이다. 여기서, Version은 비트 코인 프로토콜을 실행하는 각 노드의 버전을 의미하고, Merkly Root는 32바이트 크기의 거래가 발생할 때마다 업데이트 되는 값으로, 트랜잭션의 내용을 입력으로 해시값을 구하고 이를 트리구조로 저장한

머클트리의 루트 값이고, Difficuly Target(Bits)는 4바이트 크기의 해시 퍼즐의 난이도 조절 수치이다.
오답 체크
(1) 4바이트 크기의 다음 블록을 생성하기 위한 값으로, 이 값을 조정하여 다음 블록의 이전 블록 해시값(현재 블록 해시값)을 계산한다.
(2) 4바이트 크기의 블록이 생성되는 시간이다.
(3) 32바이트 크기의 이전 블록 헤더의 해시값(SHA-256을 두 번 적용한 값)으로 이것을 이용하여 블록을 묶는다.

11. OSI 7계층 중 각 층에 해당하는 프로토콜을 모두 옳게 짝지은 것은?
① Network – IP, NetBIOS, SMTP
② Transport – ICMP, SSL, FTP
③ Presentation – ASCII, JPEG, MPEG
④ Application – HTTP, PPP, IGMP
정답 체크
(3) 이외에도 XDR, SSL 등이 존재한다.
오답 체크
(1) IP는 Network 계층이지만, NetBIOS는 Session 계층이고, SMTP는 Application 계층이다.
(2) SSL은 Transport 계층 또는 Presentation 계층이지만, ICMP는 Network 계층이고, FTP는 Application 계층이다.
(4) HTTP는 Application 계층이지만, PPP는 Data Link 계층이고, IGMP는 Network 계층이다.

12. VPN에 대한 설명으로 옳은 것은?
① TCP, FTP는 VPN에서 사용하는 터널링 프로토콜이다.
② 공용 회선을 대신하여 저렴한 사설 임대 회선을 이용하는 공중 암호화망이다.
③ 사설 임대 회선에 터널을 형성하고 패킷을 캡슐화하지 않고 전달하는 방법을 사용한다.
④ 인터넷과 같은 공중 네트워크를 이용하여 사설망과 같은 전용선처럼 사용할 수 있는 보안 솔루션이다.
정답 체크
(4) 공중 네트워크를 이용하여 비용을 절감하고, 사설망을 사용하여 데이터를 보호할 수 있다.
오답 체크
(1) 터널링 프로토콜은 L2F, PPTP, L2TP이다.
(2) 전용 임대 회선을 대신하여 저렴한 공용 회선을 이용한다.
(3) 공용 회선에 터널을 형성하고 패킷을 캡슐화하여 전달한다.

13. 정보보호 및 개인정보보호 관리체계 인증 기준에서 정하고 있는 보호대책 요구사항은?
① 인증 및 권한관리
② 관리체계 기반 마련
③ 정보주체 권리보호
④ 관리체계 점검 및 개선
정답 체크

(1) 인증 및 권한관리는 보호대책 요구사항이다(다음 표 참조).

구분		통합인증	분야(인증기준 개수)
ISMS-P	ISMS	1. 관리체계 수립 및 운영 (16)	1.1 관리체계 기반 마련(6) 1.2 위험관리(4) 1.3 관리체계 운영(3) 1.4 관리체계 점검 및 개선(3)
		2. 보호대책 요구사항 (64)	2.1 정책, 조직, 자산 관리(3) 2.2 인적보안(6) 2.3 외부자 보안(4) 2.4 물리보안(7) 2.5 인증 및 권한 관리(6) 2.6 접근통제(7) 2.7 암호화 적용(2) 2.8 정보시스템 도입 및 개발 보안(6) 2.9 시스템 및 서비스 운영관리(7) 2.10 시스템 및 서비스 보안관리(9) 2.11 사고 예방 및 대응(5) 2.12 재해복구(2)
	-	3. 개인정보 처리단계별 요구사항(22)	3.1 개인정보 수집 시 보호조치(7) 3.2 개인정보 보유 및 이용 시 보호조치(5) 3.3 개인정보 제공 시 보호조치(3) 3.4 개인정보 파기 시 보호조치(4) 3.5 정보주체 권리보호(3)

오답 체크

(2) 관리체계 수립 및 운영이다.

(3) 개인정보 처리단계별 요구사항이다.

(4) 관리체계 수립 및 운영이다.

14. 「개인정보 보호법」 제4조(정보주체의 권리)에서 정보주체가 자신의 개인정보 처리와 관련해서 가지는 권리로 옳지 않은 것은?

① 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리

② 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리

③ 개인정보의 목적 외 수집, 오용·남용 및 무분별한 감시·추적 등에 따른 폐해를 방지하여 인간의 존엄과 개인의 사생활 보호를 도모하기 위한 시책을 강구할 권리

④ 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리

정답 체크

(3) 제5조(국가 등의 책무) ① 국가와 지방자치단체는 개인정보의 목적 외 수집, 오용·남용 및 무분별한 감시·추적 등에 따른 폐해를 방지하여 인간의 존엄과 개인의 사생활 보호를 도모하기 위한 시책을 강구하여야 한다.

오답 체크

(1), (2), (4) 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 대하여 열람(사본의 발급을 포함한다. 이하 같다)을 요구할 권리
4. 개인정보의 처리 정지, 정정 · 삭제 및 파기를 요구할 권리
5. 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리

15. 웹 해킹 공격에 대한 설명으로 옳지 않은 것은?
① Reverse Telnet은 특정 사용자를 대상으로 하지 않고 불특정 다수를 대상으로 로그인된 사용자가 자신의 의지와 무관하게 공격자가 의도한 행위를 하도록 한다.
② Cross Site Scripting은 악성스크립트를 게시판에 등록하는 글에 포함시켜, 이에 접근한 사용자 컴퓨터에서 실행하도록 한다.
③ File Upload는 첨부파일 업로드 기능을 이용해 해킹 프로그램을 업로드한 후, 웹서버의 권한 획득을 가능하도록 한다.
④ Directory Listing은 취약한 서버 설정으로 브라우징되는 디렉토리의 모든 파일이 인터넷 사용자에게 노출되어 파일의 열람을 가능하도록 한다.
정답 체크
(1) 해당 설명은 CSRF이고, Reverse Telnet은 방화벽의 아웃 바운드 정책 부재로 웹 서버에서 공격자에게 리버스 텔넷을 시도하는 것을 의미한다.
오답 체크
(2) 웹사이트 관리자가 아닌 이가 웹 페이지에 악성 스크립트를 삽입(저장)할 수 있는 취약점이다. 주로 여러 사용자가 보게 되는 전자 게시판에 악성 스크립트가 담긴 글을 올리는 형태로 이루어진다. 이 취약점은 웹 애플리케이션이 사용자로부터 입력 받은 값을 제대로 검사하지 않고 사용할 경우 나타난다.
(3) 어플리케이션 개발/운영 환경과 동일한 언어로 작성된 공격 파일을 웹 서버 측에 업로드 한 후, 원격으로 해당 파일에 접근하여 실행시키는 취약점으로, 작성된 공격 파일의 기능에 따라서 위험도가 다양해진다.
(4) 웹 브라우저에서 웹 서버의 특정 디렉토리를 열면, 그 디렉토리에 있는 파일과 디렉토리 목록이 모두 나열되는 것이다.

16. NAC에 대한 설명으로 옳지 않은 것은?
① 사용자 식별과 인증을 수행한다.
② 단말 무결성 검증을 제공한다.
③ 해커를 유인해서 정보를 얻거나 잡으려고 설치한다.
④ 802.1x 방식, VLAN 방식 등으로 구현된다.
정답 체크
(3) 해당 설명은 Honey Pot을 의미한다.
오답 체크
(1) 내부 직원에 대한 역할 기반의 접근 제어와 네트워크의 모든 IP 기반 장치 접근 제어를 수행한다.
(2) 백신 관리, 패치 관리, 자산 관리(비인가 시스템 자동 검출)를 수행한다.
(4) 이외에도 인라인 방식, ARP 방식, 소프트웨어 에이전트 설치 방식 등이 존재한다.

17. WTLS 레코드 프로토콜의 하위 프로토콜에 해당하는 것은?
① Handshake Protocol
② Change CipherSpec Protocol
③ Alert Protocol
④ Wireless Datagram Protocol
정답 체크
(4) WTLS가 적용된 WAP을 그림으로 나타내면 다음과 같다.

<table>
<tr><td>응용 계층</td><td>WAE(Wireless Application Environment)</td><td rowspan="4">기타 서비스 및
응용 기술</td></tr>
<tr><td>세션 계층</td><td>WSP(Wireless Session Protocol)</td></tr>
<tr><td>처리 계층</td><td>WTP(Wireless Transport Layer)</td></tr>
<tr><td>보안 계층</td><td>WTLS(Wireless Transport Layer Security)</td></tr>
<tr><td>전송 계층</td><td>Datagram(UDP/IP)</td><td>Datagram WDP</td></tr>
<tr><td>네트워크 계층</td><td colspan="2">Wireless Bearers(GSM, CDPD, CDMA 등)</td></tr>
</table>

오답 체크
(1), (2), (3) 해당 프로토콜은 TLS의 하위 프로토콜에 해당된다.

18. 보안 솔루션에 대한 설명으로 옳지 않은 것은?
① IPS는 유해 트래픽이나 다양한 유형의 공격을 사전에 탐지하고 자동화된 알고리즘에 의해 탐지된 공격을 차단하는 능동형 보안 기능을 제공한다.
② IDS는 전통적인 방화벽이 탐지할 수 없는 악의적인 네트워크 트래픽이나 컴퓨터 사용을 탐지하고 이를 알려 주는 역할만 한다는 점에서 공격 자체를 차단하는 방화벽과 차이가 있다.
③ DLP는 이미지 및 오디오 파일과 같은 다양한 디지털 매체를 통해 메시지를 숨겨 전송한다.
④ Firewall은 외부 네트워크에서 내부 네트워크로 유입되는 침입을 막는 역할을 한다.
정답 체크
(3) 해당 설명은 스테가노그래피를 의미하고, DLP는 기업 내에서 이용하는 다양한 주요 정보인 기술 정보, 프로젝트 계획, 사업 내용, 영업 비밀, 고객 정보 등을 보호하고 외부 유출을 방지하기 위해서 사용된다.
오답 체크
(1) 수동적인 방어 개념의 침입 차단 시스템(Firewall)이나 침입 탐지 시스템(IDS)과 달리 침입 경고 이전에 공격을 중단시키는 데 초점을 둔, 침입 유도 기능과 자동 대처 기능이 합쳐진 개념의 솔루션이다(능동적 보안 장비).
(2) passive(수동적) 보안 장비로, 네트워크상의 패킷을 7계층(payload or content) 레벨에서 분석하여 침입을 탐지한다.
(4) 인터넷과 같은 외부 네트워크로부터 기업의 내부 네트워크를 보호하는 보안 장치로, 외부 네트워크와 내부 네트워크 사이의 유일한 연결점에 위치해 트래픽(Traffic)을 제어하는 시스템을 말한다.

19. CERT에 대한 설명으로 옳은 것은?
① 컴퓨터 긴급 관리팀으로 불리며, 영국의 옥스포드대학에서 만들었다.
② 웜 사고에 대응하기 위해 만들어졌지만, 현재는 웜뿐만 아니라 해커의 침입에 대한 대응과 추적에

대한 업무까지 맡고 있다.
③ 정부에서만 CERT를 운영하고 있다.
④ CERT팀은 법률 대리인, 대외 언론 및 외부 기관 대응 전문가로만 구성된다.
정답 체크
(2) CERT 팀의 침해 대응 절차는 다음과 같다.
사전 대응 -〉 침해 사고 발생 -〉 사고 탐지 -〉 대응(단기 대응, 백업 및 증거 확보, 시스템 복구) -〉 제거 및 복구 -〉 후속 조치 및 보고
오답 체크
(1) 미 국방부 고등연구 계획국(DARPA; The Defense Advanced Research Projects Agency)은 컴퓨터와 관련한 침해 사고에 적절히 대응하고자, 피치버그의 카네기 멜론 대학 내의 소프트웨어 공학 연구소에 CERT 팀을 만들었다.
(3) 공공도 있지만 민간도 CERT를 운영한다.
(4) 시스템 운영 전문가, 대외 언론 및 외부 기관 대응 전문가, 법률팀, 인사팀으로 구성된다.

20. 정보 보안 거버넌스의 구현 요건에 대한 설명으로 옳지 않은 것은?
① 전략적 연계: 정보 보안 사고의 잠재적 위험을 줄이려면 조직에 적합한 위험 관리 체계를 수립하고 지속적으로 관리해야 한다.
② 가치 전달: 정보 보안 투자의 효과를 높이기 위해서는 구성원들에게 정보 보안의 중요성과 가치를 교육하고 국제 표준을 기준으로 정보 보안 관리 체계를 갖추어 운영해야 한다.
③ 자원 관리: 정보 보안 지식과 자원을 효율적으로 관리하기 위해 중요한 정보 자산과 인프라를 포함하는 전사적 정보 보안 아키텍처를 확보해야 한다.
④ 성과 관리: 정보 보안 거버넌스의 효과적인 운영을 위한 척도로 모니터링이나 보고 및 성과 평가 체계를 운영해야 한다.
정답 체크
(1) 해당 설명은 위험 관리이고, 전략적 연계는 비즈니스와 IT 기술의 목표, 정보 보안 전략이 서로 연계되도록 최상위 정보 보안 운영위원회의 역할과 책임을 명시하고 정보 보안 보고 체계의 합리화를 이루어야 한다.
오답 체크
(2) 구성원들에게 정보 보안의 중요성과 가치를 교육해야 한다. 국제 표준을 기준으로 정보 보안 관리 체계를 갖추어 운영하고 자본의 통제 및 투자 프로세스를 정보 보안과 통합해야 한다.
(3) 정책과 절차에 따른 정보 보안 아웃소싱을 수행하고, 아웃소싱 정보 보안 서비스의 통제와 책임을 명시 및 승인하며 기업의 정보 보안 아키텍처와 전사적 아키텍처를 연계해야 한다.
(4) 모니터링, 보고 및 평가에 따른 성과 평가 체계를 운영하고 비즈니스 측면도 고려하여 성과를 평가해야 한다.

21. 「정보통신기반 보호법」 제8조제1항에서 규정하고 있는 주요정보통신기반시설 지정 기준에 해당하지 않는 것은?
① 해당 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가 사회적 중요성
② 정보통신산업의 기반을 조성하기 위하여 산업입지의 조성 및 정보통신산업 기반시설의 지원
③ 다른 정보통신기반시설과의 상호연계성
④ 침해사고가 발생할 경우 국가안전 보장과 경제사회에 미치는 피해 규모 및 범위

정답 체크
(2) 정보통신산업 진흥법 제18조(정보통신산업진흥단지의 조성) ① 정부는 정보통신산업의 기반을 조성하기 위하여 산업입지의 조성 및 공급과 정보통신산업 기반시설의 지원 등에 필요한 시책을 마련하고, 민간인이 공동으로 정보통신산업진흥단지를 조성할 경우에는 우선 지원하여야 한다.
오답 체크
(1), (3), (4) 제8조(주요정보통신기반시설의 지정 등) ①중앙행정기관의 장은 소관분야의 정보통신기반시설중 다음 각호의 사항을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다.
1. 해당 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성
2. 제1호에 따른 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

22. TCSEC의 등급에 대한 설명으로 옳은 것은?
① C2 등급에서는 레이블된 정보보호(labeled security)를 평가한다.
② D 등급에서는 검증된 정보보호(verified design)를 평가한다.
③ A1 등급에서는 최소한의 보호(minimal protection)만 가능하다.
④ A1, B1, B2, B3, C1, C2, D 등급으로 구분된다.
정답 체크
(4) A1, B3, B2, B1, C2, C1, D 등급으로 구분된다.
오답 체크
(1) verified design은 A1 등급이다.
(2) minimal protection은 D 등급이다.
(3) labeled security는 B1 등급이고, C2는 controlled access protection이다.

23.「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제23조의3에 따라 본인확인기관 지정을 위한 심사 사항으로 옳지 않은 것은?
① 본인확인업무의 안전성 확보를 위한 물리적·기술적·관리적 조치계획
② 이동통신사업자의 본인확인업무 수행과 관련하여 이용자의 주민등록번호를 수집·이용하기 위한 계획
③ 본인확인업무 관련 설비규모의 적정성
④ 본인확인업무의 수행을 위한 기술적·재정적 능력
정답 체크
(2) 제23조의2(주민등록번호의 사용 제한) ① 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용할 수 없다.
3.「전기통신사업법」제38조제1항에 따라 기간통신사업자로부터 이동통신서비스 등을 제공받아 재판매하는 전기통신사업자가 제23조의3에 따라 본인확인기관으로 지정받은 이동통신사업자의 본인확인업무 수행과 관련하여 이용자의 주민등록번호를 수집·이용하는 경우
오답 체크
(1), (3), (4) 제23조의3(본인확인기관의 지정 등) ① 방송통신위원회는 다음 각 호의 사항을 심사

하여 대체수단의 개발 · 제공 · 관리 업무(이하 “본인확인업무”라 한다)를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되는 자를 본인확인기관으로 지정할 수 있다.
1. 본인확인업무의 안전성 확보를 위한 물리적 · 기술적 · 관리적 조치계획
2. 본인확인업무의 수행을 위한 기술적 · 재정적 능력
3. 본인확인업무 관련 설비규모의 적정성

24. RADIUS에 대한 설명으로 옳은 것은?
① 주로 서버/클라이언트 방식으로 동작한다.
② 분산형 접근 제어방식으로 인터넷을 이용하여 직접적으로 사용자를 인증하는 프로토콜이다.
③ 등록되지 않은 사용자를 인증한다.
④ 보안 강화를 위하여 TCP를 사용한다.
정답 체크
(1) 사용자와 RADIUS 서버 간에 서버/클라이언트 방식으로 동작한다.
오답 체크
(2) 중앙집중형 접근 제어 방식으로 인증 서버를 통해 간접적으로 사용자를 인증하는 프로토콜이다.
(3) 등록된 사용자를 인증한다.
(4) UDP를 사용한다.

25. 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」에서 규정하고 있는 인증 기준에 대한 설명으로 옳지 않은 것은?
① 정보자산 식별: 조직의 업무 특성에 따라 정보자산 분류기준을 수립하여 관리체계 범위 내 모든 정보자산을 식별·분류하고 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.
② 사용자 인증: 정보시스템과 개인정보 및 중요정보에 대한 사용자의 접근은 안전한 인증절차와 필요에 따라 강화된 인증방식을 적용하여야 한다. 또한 로그인 횟수 제한, 불법 로그인 시도 경고 등 비인가자 접근 통제방안을 수립·이행하여야 한다.
③ 원격접근 통제: 보호구역 이외 장소에서의 정보시스템 관리 및 개인정보 처리는 원칙으로 금지하고 재택근무·장애대응·원격협업 등 불가피한 사유로 원격접근을 허용하는 경우 책임자 승인, 접근 단말 지정, 접근 허용범위 및 기간 설정, 강화된 인증, 구간 암호화, 접속 단말 보안(백신, 패치 등) 등 보호대책을 수립·이행하여야 한다.
④ 사용자 계정 관리: 개인정보 및 주요정보 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호 강도, 암호 사용 정책을 수립하고 개인정보 및 주요정보의 저장·전송·전달 시 암호화를 적용하여야 한다.
정답 체크
(4) 해당 설명은 암호정책 적용(암호화 적용)이고, 사용자 계정 관리(인증 및 권한관리)는 정보시스템과 개인정보 및 중요정보에 대한 비인가 접근을 통제하고 업무 목적에 따른 접근권한을 최소한으로 부여할 수 있도록 사용자 등록·해지 및 접근권한 부여·변경·말소 절차를 수립·이행하고, 사용자 등록 및 권한부여 시 사용자에게 보안책임이 있음을 규정화하고 인식시켜야 한다.
오답 체크
(1) 위험 관리에 속한다.
(2) 인증 및 권한관리에 속한다.
(3) 접근 통제에 속한다.