2022년 지방직,교육청 9급 정보보호론

-2022년 6월 18일 시행

1. ○△× 22.지방.9급

송수신자의 MAC 주소를 가로채 공격자의 MAC 주소로 변경하는 공격은?

① ARP spoofing
② Ping of Death
③ SYN Flooding
④ DDoS

오답피하기 ① ARP 스푸핑(Spoofing)은 공격자가 특정 호스트의 MAC 주소를 자신의 MAC 주소로 위조한 ARP Reply 패킷을 만들어 희생자에게 지속적으로 전송하면 희생자의 ARP Cache에 특정 호스트의 MAC정보가 공격자의 MAC정보로 변경이 된다는 점을 이용해 희생자에게서 특정 호스트로 나가는 패킷을 공격자가 스니핑하는 기법이다.

정답 ①

2. ○△× 22.지방.9급

스니핑 공격의 탐지 방법으로 옳지 않은 것은?

① ping을 이용한 방법
② ARP를 이용한 방법
③ DNS를 이용한 방법
④ SSID를 이용한 방법

◘ 스니핑 탐지

㉠ 핑을 이용한 방법: 대부분의 스니퍼는 일반 TCP/IP에서 동작하기 때문에 request를 받으면 response를 전달한다. 이를 이용하여 의심이 가는 호스트에 ping을 보낼 때, 네트워크에 존재하지 않는 MAC 주소로 위장하여 보낸다. 만약 ICMP Echo reply를 받으면 해당 호스트가 스니핑을 하고 있는 것이다.

㉡ ARP를 이용한 방법: ping과 유사한 방법으로 위조된 ARP request를 보냈을 때 ARP response가 오면 프러미스큐어스 모드로 설정되어 있는 것이다.

㉢ DNS 방법: 스니핑 프로그램은 스니핑한 시스템의 IP 주소에 대한 DNS 이름 해석 과정(Inverse-DNS lookup)을 수행한다. 테스트 대상 네트워크로 Ping Sweep을 보내고 들어오는 Inverse-DNS lookup을 감시하여 스니퍼를 탐지한다.

㉣ 유인(Decoy) 방법: 스니핑 공격을 하는 공격자의 주요 목적은 계정과 패스워드의 획득에 있다. 보안관리자는 이 점을 이용하여 가짜 계정과 패스워드를 네트워크에 뿌린다. 공격자는 이 계정과 패스워드를 이용하여 접속을 시도한다. 그래서 이 접속을 시도하는 시스템을 탐지한다.

㉤ ARP Watch: 초기에 MAC 주소와 IP 주소의 매칭 값을 저장한 후 ARP 트래픽을 모니터링한다. 이를 변하게 하는 패킷이 탐지되면 관리자에게 메일로 알려주는 도구이다.

오답피하기 ④ 스니핑 탐지 방법에 SSID를 이용한 방법은 없다.

정답 ④

3. ○△× 22.지방.9급

공격자가 해킹을 통해 시스템에 침입하여 루트 권한을 획득한 후, 재침입할 때 권한을 쉽게 획득하기 위하여 제작된 악성 소프트웨어는?

① 랜섬웨어
② 논리폭탄
③ 슬래머 웜
④ 백도어

◦ 슬래머 웜은 다양한 인터넷 호스트에 서비스 거부 공격(DoS)을 실시하는 웜으로, 개인컴퓨터보다는 네트워크에 더 위협적인 웜이다. 2003년 등장해 10분만에 7만 5,000대의 컴퓨터를 감염시킬 정도로 확산속도가 빨랐다.

오답피하기 ④ 백도어(backdoor)는 '뒷문이 열렸다'는 의미로 공공연히 드러내지 않고도 들락거릴 수 있음을 뜻한다. 원래는 서비스 기술자나 유지보수 프로그래머들의 다른 PC에 대한 액세스 편의를 위해 시스템 설계자가 고의적으로 만들어 놓은 것이다. 최근에는 해킹에 취약한 부분을 일컫는 용어로 쓰이고 있다.

정답 ④

4. ○△× 22.지방.9급

다음에서 설명하는 용어는?

> 보기
> ○ 한 번의 시스템 인증을 통해 다양한 정보시스템에 재인증 절차 없이 접근할 수 있다.
> ○ 이 시스템의 가장 큰 약점은 일단 최초 인증 과정을 거치면, 모든 서버나 사이트에 접속할 수 있다는 것이다.

① NAC(Network Access Control)
② SSO(Single Sign On)
③ DRM(Digital Right Management)
④ DLP(Data Leak Prevention)

◦ 데이터 유출 방지(DLP): 기업 내부자의 고의나 실수로 정보가 밖으로 새어나가는 것을 방지하는 시스템이다. 사내 직원이 사용하는 개인용 컴퓨터(PC)와 네트워크상의 모든 정보를 검색하고 사용자의 행위를 탐지, 통제해 외부로의 유출을 사전에 차단한다.

오답피하기 ② 싱글사인온(SSO, Single Sign-On)은 단 한번의 로그인만으로 기업의 각종 시스템이나 인터넷 서비스에 접속하게 해주는 보안 응용 솔루션이다. 각각의 시스템마다 인증 절차를 밟지 않고도 1개의 계정만으로 다양한 시스템에 접근할 수 있어 ID, 비밀번호에 대한 보안 위험 예방과 사용자 편의 증진, 인증 관리비용의 절감 효과가 있다.

정답 ②

5. ○△× 22.지방.9급

보안 공격 유형에는 적극적 공격과 소극적 공격이 있다. 다음 중 공격 유형이 다른 하나는?

① 메시지 내용 공개(release of message contents)
② 신분 위장(masquerade)
③ 메시지 수정(modification of message)
④ 서비스 거부(denial of service)

오답피하기 ① 메시지 내용 공개는 소극적 공격이고, 나머지는 적극적 공격이다.

정답 ①

6. ○△× 22.지방.9급

X.509 인증서 폐기 목록(Certificate Revocation List) 형식 필드에 포함되지 않는 것은?

① 발행자 이름(Issuer name)
② 사용자 이름(Subject name)
③ 폐지된 인증서(Revoked certificate)
④ 금번 업데이트 날짜(This update date)

CRL 기본 영역
- 버전(Version): 인코딩된 CRL의 버전을 기술한다.
- 서명 알고리즘 식별자(Signature Algorithm ID): CRL을 서명하기 위해 이용된 알고리즘에 대한 알고리즘 식별자를 가진다.
- 발행자 이름(Issuer name): CRL을 서명하고 발행한 엔티티를 구분한다. 발행자 신분은 발행자 이름 필드에 들어간다.
- 현재 갱신(Last update): 현 CRL의 발행일자를 나타낸다.
- 다음 갱신(Next update): 다음 CRL이 발행되는 날짜를 나타낸다. 다음 CRL은 표시된 날짜 이전에 발행될 수 있다.
- 폐지된 인증서(Revoked certificate): 유효기간은 끝나지 않았지만 폐지된 인증서의 전체 목록을 계속해서 발표한다. 각 목록은 두 부분으로 구성되는데, 하나는 사용자 인증서 순서번호이고 다른 하나는 폐지 일자이다.
- 서명(Signature): 인증서 필드와 동일하다.

오답피하기 ② 사용자 이름(Subject name)은 CRL 형식 필드에 포함되지 않고, X509v3 인증서 형식에 포함된다.

정답 ②

7. ○△× 22.지방.9급

AES 알고리즘에 대한 설명으로 옳지 않은 것은?

① 블록 암호 체제를 갖추고 있다.
② 128/192/256bit 키 길이를 제공하고 있다.
③ DES 알고리즘을 보완하기 위해 고안된 알고리즘이다.
④ 첫 번째 라운드를 수행하기 전에 먼저 초기 평문과 라운드 키의 NOR 연산을 수행한다.

오답피하기 ④ AES의 암호화 과정은 DES와 달리, 첫 번째 라운드를 수행하기 전에 먼저 초기 평문과 라운드키의 XOR연산을 수행하므로, 암호화 과정에 필요한 전체 라운드 키의 개수는 Nr+1개가 된다.(NOR 연산이 아님)

정답 ④

8. ○△× 22.지방.9급

정보기술과 보안 평가를 위한 CC(Common Criteria)의 보안 기능적 요구 조건에 해당하지 않는 것은?

① 암호 지원
② 취약점 평가
③ 사용자 데이터 보호
④ 식별과 인증

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 ② 취약점 평가는 보안 기능 요구사항이 아니고 보증 요구사항에 포함된다.

정답 ②

9. ○△× 22.지방.9급

커버로스(Kerberos) 버전 4에 대한 설명으로 옳지 않은 것은?

① 사용자를 인증하기 위해 사용자의 패스워드를 중앙집중식 DB에 저장하는 인증 서버를 사용한다.
② 사용자는 인증 서버에게 TGS(Ticket Granting Server)를 이용하기 위한 TGT(Ticket Granting Ticket)를 요청한다.
③ 인증 서버가 사용자에게 발급한 TGT는 유효기간 동안 재사용 할 수 있다.
④ 네트워크 기반 인증 시스템으로 비대칭 키를 이용하여 인증을 수행한다.

오답피하기 ④ 커버로스는 네트워크 기반 인증 시스템으로 비대칭키가 아닌 대칭키를 이용하여 인증을 수행한다.

정답 ④

10. ○△× 22.지방.9급

다음에서 설명하는 보안 공격은?

보기

○ 정상적인 HTTP GET 패킷의 헤더 부분의 마지막에 입력되는 2개의 개행 문자(\r\n\r\n) 중 하나(\r\n)를 제거한 패킷을 웹 서버에 전송할 경우, 웹 서버는 아직 HTTP 헤더 정보가 전달되지 않은 것으로 판단하여 계속 연결을 유지하게 된다.
○ 제한된 연결 수를 모두 소진하게 되어 결국 다른 클라이언트가 해당 웹 서버에 접속할 수 없게 된다.

① HTTP Cache Control
② Smurf
③ Slowloris
④ Replay

◦ GET Flooding with Cache-Control(CC Attack): 일반적으로 웹서버의 부하를 감소시키기 위해 캐싱서버를 운영하여 많이 요청받는 데이터를 웹서버가 아닌 캐싱서버를 통해 응답하도록 구축한다. 하지만 공격자는 HTTP 메시지의 캐시 옵션을 조작하여 캐싱서버가 아닌 웹서버가 직접 처리하도록 유도하여 캐싱서버의 기능을 무력화하고 웹서버의 자원을 소진시킨다.

오답피하기 ③ Slow HTTP Header DoS(Slowloris) 공격에서 웹서버는 HTTP 메시지의 헤더부분을 먼저 수신하여 이후 수신할 데이터의 종류를 판단하게 되는데, 헤더부분을 비정상적으로 조작하여 웹서버가 헤더정보를 구분할 수 없도록 하면, 웹서버는 아직 HTTP 헤더정보가 모두 전달되지 않은 것으로 판단하여 연결을 장시간 유지하게 된다.

정답 ③

11. ○△× 22.지방.9급

(가), (나)에 들어갈 접근통제 보안모델을 바르게 연결한 것은?

보기

(가)은 허가되지 않은 방식의 접근을 방지하는 모델로 정보 흐름 모델 최초의 수학적 보안모델이다.
(나)은 비즈니스 입장에서 직무분리 개념을 적용하고, 이해가 충돌되는 회사 간의 정보의 흐름이 일어나지 않도록 접근통제 기능을 제공하는 보안모델이다.

	(가)	(나)
①	Bell-LaPadula Model	Biba Integrity Model
②	Bell-LaPadula Model	Brewer-Nash Model
③	Clark-Wilson Model	Biba Integrity Model
④	Clark-Wilson Model	Brewer-Nash Model

◦ Clark and Wilson 모델: 불법수정 방지를 위해 상업 환경에 적합하게 개발된 보안 모델이다. 금융 자산의 관리나 회계 등의 내용을 담고 있는 상업 환경에서는 기밀성보다는 자료의 무결성이 더 중요하기 때문이다. 이 모델은 모든 거래 사실을 기록하여 불법 거래를 방지하며 완전하게 관리되는 자료처리(Well-formed Transactions)정책과 모든 운영과정에서 어느 한 사람만이 정보를 입력, 처리하게 하지 않고 여러 사람이 각 부문별로 나누어 처리하게 하는 임무 분리의 원칙(Separation of Duties)이 적용된다. 또한 회계거래상 이중자료 처리 시스템으로 장부를 처리하게 하는 원칙(Double-entry Bookkeeping Principle)을 적용하여 중복처리하게 함으로써 무결성을 입증한다.

오답피하기 ② (가) BLP(Bell-La Padula)모델은 허가된 비밀정보에 허가되지 않는 방식의 접근을 금지하는 기밀성을 강조한 모델로서 정보흐름 모델(Information Flow Model), 최초의 수학적 모델이다. 그리고 정보의 불법적인 파괴나 변조보다는 불법적인 비밀유출(disclosure) 방지에 중점을 두었다. 즉, 정보가 높은 보안레벨로부터 낮은 보안레벨로 흐르는 것을 방지한다. (나) Chinese Wall 모델이라고 부르는 브루어-내시 모델(Brewer and Model)은 사용자의 이전 동작에 따라 변화할 수 있는 접근 통제를 제공하기 위해 만들어졌다. 또한 이 모델은 정보 흐름 모델을 기반으로 하고 있다. 주체와 객체 사이에서 이해 충돌을 야기하는 방식으로 정보가 흐르지 않도록 한다.

정답 ②

12. ○△× 22.지방.9급

리눅스 시스템에서 umask값에 따라 새로 생성된 디렉터리의 접근 권한이 'drwxr-xr-x'일 때 기본 접근 권한을 설정하는 umask의 값은?

① 002
② 020
③ 022
④ 026

◦ 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 디렉터리의 기본 접근권한(drwxrwxrwx)에서 umask 적용 후 drwxr-xr-x가 되기 위해서는 group에서 w권한, other에서 w를 제거하는 umask 022가 되어야 한다.

정답 ③

13. ○△× 22.지방.9급

(가), (나)에 해당하는 침입차단시스템 동작 방식에 따른 분류를 바르게 연결한 것은?

보기

(가) 각 서비스별로 클라이언트와 서버 사이에 프록시가 존재하며 내부 네트워크와 외부 네트워크가 직접 연결되는 것을 허용하지 않는다.

(나) 서비스마다 개별 프록시를 둘 필요가 없고 프록시와 연결을 위한 전용 클라이언트 소프트웨어가 필요하다.

	(가)	(나)
①	응용 계층 게이트웨이 (application level gateway)	회선 계층 게이트웨이 (circuit level gateway)
②	응용 계층 게이트웨이 (application level gateway)	상태 검사 (stateful inspection)
③	네트워크 계층 패킷 필터링 (network level packet filtering)	상태 검사 (stateful inspection)
④	네트워크 계층 패킷 필터링 (network level packet filtering)	회선 계층 게이트웨이 (circuit level gateway)

오답피하기 ① (가) 응용계층 게이트웨이는 응용 서비스마다 각각 다른 응용 게이트웨이를 구현하여 보다 안전하게 내부 네트워크의 시스템을 보호할 수 있다. (나) 서킷 레벨 게이트웨이는 서비스에 대하여 유연하게 대처할 수 있으며 실제 클라이언트 요청이 전송 또는 세션 계층에서 이루어지므로 서비스마다 개별 프락시 서버를 둘 필요가 없다.

정답 ①

14. ○△× 22.지방.9급

IPSec에 대한 설명으로 옳지 않은 것은?

① AH는 인증 기능을 제공한다.
② ESP는 암호화 기능을 제공한다.
③ 전송 모드는 IP 헤더를 포함한 전체 IP 패킷을 보호한다.
④ IKE는 Diffie-Hellman 키 교환 알고리즘을 기반으로 한다.

오답피하기 ③ IP 헤더를 포함한 전체 IP 패킷을 보호하는 것은 전송 모드가 아닌 터널 모드의 특징이다.

정답 ③

15. ○△× 22.지방.9급

보안 공격에 대한 설명으로 옳지 않은 것은?

① Land 공격은 패킷을 전송할 때 출발지와 목적지 IP를 동일하게 만들어서 공격 대상에게 전송한다.
② UDP Flooding 공격은 다수의 UDP 패킷을 전송하여 공격 대상 시스템을 마비시킨다.
③ ICMP Flooding 공격은 ICMP 프로토콜의 echo 패킷에 대한 응답인 reply 패킷의 폭주를 통해 공격 대상 시스템을 마비시킨다.
④ Teardrop 공격은 공격자가 자신이 전송하는 패킷을 다른 호스트의 IP 주소로 변조하여 수신자의 패킷 조립을 방해한다.

◦ Teardrop 공격은 오프셋 값을 단편화 간에 중복되도록 고의적으로 수정하거나 정상적인 오프셋 값보다 더 큰 값을 더해 그 범위를 넘어서는 오버플로우를 일으켜 시스템의 기능을 마비시켜 버리는 DoS 공격기법의 하나이다.

오답피하기 ④ Teardrop은 중첩(Overlap) 기법을 통해 패킷 조립을 방해한다.

정답 ④

16. ○△× 22.지방.9급

다음은 「지능정보화 기본법」 제6조(지능정보사회 종합계획의 수립)의 일부이다. (가), (나)에 들어갈 내용을 바르게 연결한 것은?

보기

제6조(지능정보사회 종합계획의 수립) ① 정부는 지능정보사회 정책의 효율적체계적 추진을 위하여 지능정보사회 종합계획(이하 "종합계획"이라 한다)을 [(가)] 단위로 수립하여야 한다.

② 종합계획은 [(나)]이 관계 중앙행정기관(대통령 소속 기관 및 국무총리 소속 기관을 포함한다. 이하 같다)의 장 및 지방자치단체의 장의 의견을 들어 수립하며, 「정보통신 진흥 및 융합 활성화 등에 관한 특별법」 제7조에 따른 정보통신 전략위원회(이하 "전략위원회"라 한다)의 심의를 거쳐 수립·확정한다. 종합계획을 변경하는 경우에도 또한 같다.

	(가)	(나)
①	3년	과학기술정보통신부장관
②	3년	행정안전부장관

③ 5년 과학기술정보통신부장관
④ 5년 행정안전부장관

◘ 제6조(지능정보사회 종합계획의 수립)
① 정부는 지능정보사회 정책의 효율적·체계적 추진을 위하여 지능정보사회 종합계획을 3년 단위로 수립하여야 한다.
② 종합계획은 과학기술정보통신부장관이 관계 중앙행정기관의 장 및 지방자치단체의 장의 의견을 들어 수립하며, 정보통신 전략위원회의 심의를 거쳐 수립·확정한다. 종합계획을 변경하는 경우에도 또한 같다.
③ 과학기술정보통신부장관이 중앙행정기관의 장 및 지방자치단체의 장에게 종합계획의 수립에 필요한 자료를 요청하는 경우 해당 기관의 장은 특별한 사정이 없으면 이에 응하여야 한다.
④ 종합계획에는 다음 각 호의 사항이 포함되어야 한다.
1. 지능정보사회 정책의 기본방향 및 중장기 발전방향
2. 공공·민간·지역 등 분야별 지능정보화
3. 지능정보기술의 고도화 및 지능정보서비스의 이용촉진과 관련 과학기술 발전 지원
4. 전 산업의 지능정보화 추진, 지능정보기술 관련 산업의 육성, 규제개선 및 공정한 경쟁환경 조성 등을 통한 신산업·신서비스 창업생태계 조성
5. 정보의 공동활용·표준화 및 초연결지능정보통신망의 구축
6. 지능정보사회 관련 법·제도 개선
7. 지능정보화 및 지능정보사회 관련 교육·홍보·인력양성 및 국제협력
8. 건전한 정보문화 창달 및 지능정보사회윤리의 확립
9. 정보보호, 정보격차 해소, 제51조에 따른 기본계획의 수립에 관한 사항 등 역기능 해소, 이용자의 권익보호 및 지식재산권의 보호
10. 지능정보사회 구현을 위한 시책 추진에 필요한 재원의 조달·운용 및 인력확보 방안
11. 그 밖에 지능정보사회 구현을 위하여 필요한 사항
⑤ 중앙행정기관의 장과 지방자치단체의 장은 소관 주요 정책을 수립하고 집행을 할 때 제4항 각 호의 사항을 우선적으로 고려하여야 한다.
⑥ 과학기술정보통신부장관은 매년 종합계획의 주요 시책에 대한 추진 실적을 점검·분석하여 그 결과를 전략위원회에 보고하여야 한다.
◘ 제7조(지능정보사회 실행계획의 수립)
① 중앙행정기관의 장과 지방자치단체의 장은 종합계획에 따라 매년 지능정보사회 실행계획을 수립·시행하여야 한다.
② 중앙행정기관의 장과 지방자치단체의 장은 전년도 실행계획의 추진 실적과 다음 해의 실행계획을 과학기술정보통신부장관과 행정안전부장관에게 제출하여야 한다. 이 경우 행정안전부장관은 지방자치단체의 전년도 실행계획의 추진 실적과 다음 해의 실행계획을 종합하여 과학기술정보통신부장관에게 제출하여야 한다.
③ 중앙행정기관의 장과 지방자치단체의 장은 제출된 다음 해의 실행계획 중 대통령령으로 정하는 중요한 사항을 변경하는 경우에는 그 내용을 과학기술정보통신부장관과 행정안전부장관에게 제출하여야 한다.
④ 과학기술정보통신부장관과 행정안전부장관은 공동으로 제출된 추진 실적 및 실행계획과 제출된 실행계획을 점검·분석하고, 과학기술정보통신부장관은 행정안전부장관의 점검·분석 결과를 종합하여 그 의견을 기획재정부장관에게 제시하여야 한다.
⑤ 기획재정부장관은 실행계획에 필요한 예산을 편성할 때에는 의견을 참작하여야 한다.
⑥ 과학기술정보통신부장관은 관계 중앙행정기관의 장과 협의하여 국가기관등이 추진하는 지능정보화 사업의 중복투자 방지 등을 위한 방안을 마련할 수 있다. 다만, 「전자정부법」에 따른 사전협의 대상은 제외한다.
⑦ 실행계획의 수립 및 시행 등에 필요한 사항은 대통령령으로 정한다.

오답피하기 ① 지능정보화 기본법 상 종합계획은 3년마다 수립되고, 시행계획은 1년마다 수립된다. 종합계획은 과학기술정보통신부장관이 정보통신 전략위원회의 심의를 거쳐 수립·확정한다.

정답 ①

17. ○△× 22.지방.9급

「개인정보 영향평가에 관한 고시」상 용어의 정의로 옳지 않은 것은?

① "대상시스템"이란 「개인정보 보호법 시행령」 제35조에 해당하는 개인정보파일을 구축·운용, 변경 또는 연계하려는 정보시스템을 말한다.
② "대상기관"이란 「개인정보 보호법 시행령」 제35조에 해당하는 개인정보파일을 구축·운용, 변경 또는 연계하려는 공공기관 및 민간기관을 말한다.
③ "개인정보 영향평가 관련 분야 수행실적"이란 「개인정보 보호법 시행령」 제37조제1항제1호에 따른 영향평가 업무 또는 이와 유사한 업무, 정보보호 컨설팅 업무 등을 수행한 실적을 말한다.
④ "개인정보 영향평가"란 「개인정보 보호법」 제33조제1항에 따라 공공기관의 장이 「개인정보 보호법 시행령」 제35조에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에 그 위험요인의 분석과 개선 사항 도출을 위한 평가를 말한다.

◘ 제2조(용어의 정의)
1. "개인정보 영향평가란 법 제33조제1항에 따라 공공기관의 장이 영 제35조에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에 그 위험요인의 분석과 개선 사항 도출을 위한 평가를 말한다.
2. "대상기관"이란 영 제35조에 해당하는 개인정보파일을 구축 · 운용, 변경 또는 연계하려는 공공기관을 말한다.
3. "개인정보 영향평가기관이란 영 제37조제1항 각 호의 요건을 모두 갖춘 법인으로서 공공기관의 영향평가를 수행하기 위하여 개인정보 보호위원회가 지정한 기관을 말한다.
4. "대상시스템"이란 영 제35조에 해당하는 개인정보파일을 구축 · 운용, 변경 또는 연계하려는 정보시스템을 말한다.
5. "개인정보 영향평가 관련 분야 수행실적이란 영 제37조제1항제1호에 따른 영향평가 업무 또는 이와 유사한 업무, 정보보호 컨설팅 업무 등을 수행한 실적을 말한다.

오답피하기 ② 대상기관은 공공기관만 해당 된다.(민간기관은 포함 안됨)

정답 ②

18. ○△× 22.지방.9급

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조의4(본인확인업무의 정지 및 지정취소)상 본인확인업무에 대해 전부 또는 일부의 정지를 명하거나 본인확인기관 지정을 취소할 수 있는 사유에 해당하지 않는 것은?

① 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조의3제4항에 따른 지정기준에 적합하지 아니하게 된 경우
② 거짓이나 그 밖의 부정한 방법으로 본인확인기관의 지정을 받은 경우
③ 본인확인업무의 정지명령을 받은 자가 그 명령을 위반하여 업무를 정지하지 아니한 경우
④ 지정받은 날부터 3개월 이내에 본인확인업무를 개시하지 아니하거나 3개월 이상 계속하여 본인확인업무를 휴지한 경우

제23조의4(본인확인업무의 정지 및 지정취소)
① 방송통신위원회는 본인확인기관이 다음 각 호의 어느 하나에 해당하는 때에는 6개월 이내의 기간을 정하여 본인확인업무의 전부 또는 일부의 정지를 명하거나 지정을 취소할 수 있다. 다만, 제1호 또는 제2호에 해당하는 때에는 그 지정을 취소하여야 한다.
1. 거짓이나 그 밖의 부정한 방법으로 본인확인기관의 지정을 받은 경우
2. 본인확인업무의 정지명령을 받은 자가 그 명령을 위반하여 업무를 정지하지 아니한 경우
3. 지정받은 날부터 6개월 이내에 본인확인업무를 개시하지 아니하거나 6개월 이상 계속하여 본인확인업무를 휴지한 경우
4. 지정기준에 적합하지 아니하게 된 경우

오답피하기 ④ 3개월이 아닌 6개월이 지정 취소의 사유가 된다.

정답 ④

19. ○△× 22.지방.9급

메일 보안 기술에 대한 설명으로 옳지 않은 것은?

① PGP는 중앙 집중화된 키 인증 방식이고, PEM은 분산화된 키 인증 방식이다.
② PGP를 이용하면 수신자가 이메일을 받고서도 받지 않았다고 발뺌할 수 없다.
③ PGP는 인터넷으로 전송하는 이메일을 암호화 또는 복호화하여 제3자가 알아볼 수 없게 하는 보안 프로그램이다.
④ PEM에는 메시지를 암호화하여 통신 내용을 보호하는 기능, 메시지 위·변조, 검증 및 메시지 작성자를 인증하는 보안 기능이 있다.

오답피하기 ① PEM은 중앙 집중화된 키 인증 방식이고, PGP는 분산화된 키 인증 방식이다.

정답 ①

20. ○△× 22.지방.9급

(가) ~ (다)에 해당하는 트리형 공개키 기반 구조의 구성기관을 바르게 연결한 것은?(단, PAA는 Policy Approval Authorities, RA는 Registration Authority, PCA는 Policy Certification Authorities를 의미한다)

보기
(가) PKI에 대한 정책을 결정하고 하위 기관의 정책을 승인하는 기관
(나) Root CA 인증서를 발급하고 CA가 준수해야 할 기본 정책을 수립하는 기관
(다) CA를 대신하여 PKI 인증 요청을 확인하고, CA 간 인터페이스를 제공하는 기관

	(가)	(나)	(다)
①	PAA	RA	PCA
②	PAA	PCA	RA
③	PCA	RA	PAA
④	PCA	PAA	RA

PKI의 주요 구성요소
◦ 정책승인기관(PAA, Policy Approving Authority): PKI 전반에 사용되는 정책과 절차를 생성하고 PKI 구축의 루트 CA 역할을 수행한다.
◦ 정책인증기관(PCA, Policy Certification Authority): PAA 아래 계층으로 자신의 도메인 내의 사용자와 인증기관(CA)이 따라야 할 정책을 수립하고 인증기관의 공개키를 인증하고 인증서, 인증서 폐지 목록 등을 관리한다.
◦ 인증기관(CA, Certification Authority): 공개키 인증서를 발급하고 또 필요에 따라 취소한다. 공개키를 사용자에게 전달, 인증서/인증서 취소목록 등을 보관한다.
◦ 등록기관(RA, Registration Authority): 인증기관과 멀리 떨어져 있는 사용자들을 위해 인증기관과 사용자 사이에 등록기관을 두어 인증기관 대신 사용자들의 인증서 신청 시 그들의 신분과 소속을 확인하는 기능을 수행한다.

오답피하기 ② PKI의 주요 구성요소(구성기관)는 중요하므로 반드시 숙지해야 한다.

정답 ②

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