만든이

조현준

약력

성균관대학교 정보공학 전공
前, 데카르트고시학원 전산직 전임강사
現, 지안공무원학원 전산직 전임강사
CISA, CISSP, 정보보안기사

저서

TopSpot 자료구조론 기본서,문제집
TopSpot 정보보호론 기본서,문제집
알기쉬운 정보보안기사 필기편,실기편

1. 총평(2019년 시행 지방직/교육청, 서울시)은 탑스팟 카페(http://cafe.daum.net/xotns815/DUA3/3) 또는 지안에듀 홈페이지(zianedu.com) 참고 바랍니다.

2. 전산직 공채 총정리(3년간)과 빅데이터 기반 합격 커리큘럼은 지안에듀 홈페이지을 참고 바랍니다.

2019년 지방직,교육청 9급 정보보호론

-2019년 6월 15일 시행

1. ○△× 19.지방.9급

정보통신망 등의 침해사고에 대응하기 위해 기업이나 기관의 업무 관할 지역 내에서 침해사고의 접수 및 처리 지원을 비롯해 예방, 피해 복구 등의 임무를 수행하는 조직은?

① CISO
② CERT
③ CPPG
④ CPO

◦ 정보보호 최고 책임자(CISO, Chief Information Security Officer) : 조직 내에서 보관하고 있는 모든 정보 자산에 대한 보호 업무를 총괄하는 최고 임원이다. 고객들에게 안전성과 신뢰성을 보장하기 위해 보안 정책과 보안 체계 구축에 대한 계획을 수립하고 실행하는 역할을 한다.
◦ 개인정보 관리사(CPPG, Certified Privacy Protection General) : 개인정보 보호 정책과 대처 방법론에 대한 지식이나 능력을 갖춘 사람. 개인정보 보호와 관련된 보안 정책의 수립, 기업 또는 기관의 개인 정보 보호의 이해, 개인 정보 취급자 관리, 관련 법규에 대한 지식이나 적용 같은 것에 대한 업무 능력을 보유한 사람으로서 해당 기관에서 주관하는 자격시험에 응시하여 합격한 자를 말한다.
◦ 개인정보 보호책임자(개인정보보호 최고 책임자, CPO, Chief Privacy Officer) : 개인정보를 안전하게 보호 관리하기 위해 개인정보 처리 업무를 총괄해서 관리하는 최고 책임자이다. 인터넷의 발달과 전산화로 인해 보호 · 관리해야 하는 개인정보 양이 많아져 이를 담당하는 전문 부서 및 책임자가 필요하게 되었다.

오답피하기 ② 침해사고 대응팀(CERT, Computer Emergency Response Team)은 인터넷의 보안에 관한 문제와 보고를 실시하는 공식적인 비상 대응팀. 일종의 파괴 프로그램인 웜(worm)으로부터 급습 사고가 있은 직후인 1988년 11월에 미국국방부고등연구계획국(DARPA)에서 구성되었으며, 인터넷의 보안에 관한 공동의 인식을 증진시키고 사고 처리 및 예방을 위한 정책 수립 등을 수행하는 한편, 지속적으로 공공 인식 캠페인과 보안 시스템을 개선 · 연구하고 있다. 미국 피츠버그의 카네기 멜론 대학에 있다. 이와 같은 업무를 하기 위한 우리나라의 대표적인 침해 사고 대응팀(CERT)은 인터넷 침해 사고 대응 지원 센터(KrCERT/CC)가 있다.

정답 ②

이론서 : 595p 응용(적중)

2. ○△× 19.지방.9급

OECD 개인정보보호 8개 원칙 중 다음에서 설명하는 것은?

보기

개인정보 침해, 누설, 도용을 방지하기 위한 물리적·조직적·기술적인 안전조치를 확보해야 한다.

① 수집 제한의 원칙(Collection Limitation Principle)
② 이용 제한의 원칙(Use Limitation Principle)
③ 정보 정확성의 원칙(Data Quality Principle)
④ 안전성 확보의 원칙(Security Safeguards Principle)

◘ 개인정보보호에 관한 OECD 8원칙
① 수집 제한의 법칙(Collection Limitation Principle) : 개인정보는 적법하고 공정한 방법을 통해 수집되어야 한다.
② 정보 정확성의 원칙(Data Quality Principle) : 이용 목적상 필요한 범위 내에서 개인정보의 정확성, 완전성, 최신성이 확보되어야 한다.
③ 목적 명시의 원칙(Purpose Specification Principle) : 개인정보는 수집 과정에서 수집 목적을 명시하고, 명시된 목적에 적합하게 이용되어야 한다.
④ 이용 제한의 원칙(Security Limitation Principle) : 정보 주체의 동의가 있거나, 법 규정이 있는 경우를 제외하고 목적 외로 이용되거나 공개될 수 없다.
⑤ 안전성 확보의 원칙(Security Safeguard Principle) : 개인정보의 침해, 누설, 도용 등을 방지하기 위한 물리적, 조직적, 기술적 안전 조치를 확보해야 한다.
⑥ 공개의 원칙(Openness Principle) : 개인정보의 처리 및 보호를 위한 정책 및 관리자에 대한 정보는 공개되어야 한다.
⑦ 개인 참가의 원칙(Individual Participation Principle) : 정보 주체의 개인정보 열람/정정/삭제 청구권은 보장되어야 한다.
⑧ 책임의 원칙(Accountability Principle) : 개인정보 관리자에게 원칙 준수 의무 및 책임을 부과해야 한다.

오답피하기 ④ 안전성 확보의 원칙에 대한 설명이다.

정답 ④

이론서 : 680p 응용(적중), 기출 : 647번해설 유사, 800제 : 370번 응용

3. ○△× 19.지방.9급

취약한 웹 사이트에 로그인한 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록 등)를 일으키도록 위조된 HTTP 요청을 웹 응용 프로그램에 전송하는 공격은?

① DoS 공격
② 취약한 인증 및 세션 공격
③ SQL 삽입 공격
④ CSRF 공격

오답피하기 ④ 사이트 간 요청 위조(CSRF)는 특정 웹사이트에 대해 사용자가 인지하지 못한 상황에서 사용자의 의도와는 무관하게 공격자가 의도한 행위(수정,삭제,등록 등)를 요청하게 하는 공격을 말한다. 웹 애플리케이션 사용자로부터 받은 요청에 대해서 사용자가 의도한 대로 작성되고 전송된 것인지 확인하지 않은 경우 발생 가능하고, 특히 해당 사용자가 관리자인 경우 사용자 권한관리, 게시물 삭제, 사용자 등록 등 관리자 권한으로만 수행 가능한 기능을 공격자의 의도대로 실행시킬 수 있게 된다.

정답 ④

이론서 : 552p 응용(적중), 기출 : 530번 유사

4. ○△× 19.지방.9급

스테가노그래피에 대한 설명으로 옳지 않은 것은?

① 스테가노그래피는 민감한 정보의 존재 자체를 숨기는 기술이다.
② 원문 데이터에 비해 더 많은 정보의 은닉이 가능하므로 암호화보다 공간효율성이 높다.
③ 텍스트·이미지 파일 등과 같은 디지털화된 데이터에 비밀 이진(Binary) 정보가 은닉될 수 있다.
④ 고해상도 이미지 내 각 픽셀의 최하위 비트들을 변형하여 원본의 큰 손상 없이 정보를 은닉하는 방법이 있다.

◦ 스테가노그래피 기술 : 기술은 크게 삽입기법과 수정기법으로 나뉘는데, 삽입기법은 파일 데이터를 변경하지 않고 추가 데이터를 파일 앞이나 뒤에 붙이는 방식이다. 이미지에는 영향을 주지 않는다. 수정기법은 이미지파일에서 Red, Green, Blue를 나타내는 RGB값의 최하위 비트(LSB)를 수정하는 기법이다. 최하위비트는 수정해도 육안으로 알아차리기 힘들기 때문에 많이 이용되는 방식이다.

오답피하기 ② 스테가노그래피는 전달하려는 정보를 이미지 또는 문장 등의 파일에 인간이 감지할 수 없도록 숨겨서 전달하는 기술이다. 이미지 파일의 경우 원본 이미지와 대체 이미지의 차이를 육안으로 구별하기 어려운 특징을 가지므로 원문 데이터에 비해 더 많은 정보를 은닉한다는 표현은 적절치 않다.

정답 ①②③④

이론서 : 31p 응용(적중), 기출 : 26번 유사, 800제 : 315번 응용

5. ○△× 19.지방.9급

다음 중 OSI 7계층 모델에서 동작하는 계층이 다른 것은?

① L2TP
② SYN 플러딩
③ PPTP
④ ARP 스푸핑

◘ SYN 플러딩 공격

◦ 공격자는 다량의 SYN 패킷을 서버로 전달하여 서버의 대기큐(Backlog Queue)를 가득 채워 새로운 클라이언트의 연결요청을 무시하도록 하여 장애를 유발시킨다.
◦ TCP 프로토콜이 데이터를 보내기 전에 연결을 먼저 맺어야 하는 특징을 이용한 방법이다.

오답피하기 ② L2TP, PPTP, ARP 스푸핑은 2계층과 관련되어 있고, SYN 플러딩은 4계층(전송 계층)과 관련된 공격이다.

정답 ②

이론서 : 398p, 427p, 477p 응용, 기출 : 389번 유사, 800제 : 248번 응용, 모의 : 6회/7번 응용

6. ○△× 19.지방.9급

해시 함수의 충돌에 대한 설명으로 옳은 것은?

① 해시 함수의 입력 메시지가 길어짐에 따라 생성되는 해시 값이 길어지는 것을 의미한다.
② 서로 다른 해시 함수가 서로 다른 입력 값에 대해 동일한 출력 값을 내는 것을 의미한다.
③ 동일한 해시 함수가 서로 다른 두 개의 입력 값에 대해 동일한 출력 값을 내는 것을 의미한다.
④ 동일한 해시 함수가 동일한 입력 값에 대해 다른 출력 값을 내는 것을 의미한다.

오답피하기 ③ 해시 충돌이란 해시 함수가 서로 다른 두 개의 입력값에 대해 동일한 출력값을 내는 상황을 의미한다. 이때 해시함수는 동일한 해시함수이다. 해시 함수가 무한한 가짓수의 입력값을 받아 유한한 가짓수의 출력값을 생성하는 경우, 비둘기집 원리에 의해 해시 충돌은 항상 존재한다.

정답 ③

이론서 : 93p 응용(적중), 기출 : 104번 응용, 800제 : 355번 응용

7. ○△× 19.지방.9급

암호화 기법들에 대한 설명으로 옳지 않은 것은?

① Feistel 암호는 전치(Permutation)와 대치(Substitution)를 반복시켜 암호문에 평문의 통계적인 성질이나 암호키와의 관계가 나타나지 않도록 한다.
② Kerckhoff의 원리는 암호 해독자가 현재 사용되고 있는 암호 방식을 알고 있다고 전제한다.
③ AES는 암호키의 길이를 64비트, 128비트, 256비트 중에서 선택한다.
④ 2중 DES(Double DES) 암호 방식은 외형상으로는 DES에 비해 2배의 키 길이를 갖지만, 중간일치공격 시 키의 길이가 1비트 더 늘어난 효과밖에 얻지 못한다.

중간일치공격(Meet-in-the-Middle Attack)
◦ 얼핏 보기에, 2중 DES에서는 키를 탐색하기 위한 탐색 횟수가 2^{56}번(하나의 DES)에서 2^{112}번(2중 DES)으로 증가하는 것처럼 보인다.
◦ 그러나 중간일치공격과 같은 기지평문공격을 사용하면 탐색횟수가 2^{112}가 아닌 2^{57}로 약간 증가할 뿐이다.

오답피하기 ③ AES는 10, 12, 14라운드를 사용하며, 각 라운드에 대응하는 키 크기는 128, 192, 256비트이다.

정답 ③

이론서 : 56p 응용(적중), 기출 : 42번 유사

8. ○△× 19.지방.9급

디지털 포렌식에 대한 설명에서 ㉠, ㉡에 들어갈 용어는?

보기

(㉠) 공간은 물리적으로 파일에 할당된 공간이지만 논리적으로 사용할 수 없는 낭비 공간이기 때문에, 공격자가 의도적으로 정보를 은닉할 가능성이 있다. 또한, 이전에 저장되었던 데이터가 남아 있을 가능성이 있어 파일 복구와 삭제된 파일의 파편 조사에 활용할 수 있다. 이 때, 디지털 포렌식의 파일 (㉡) 과정을 통해 디스크 내 비구조화된 데이터 스트림을 식별하고 의미 있는 내용을 추출할 수 있다.

	㉠	㉡
①	실린더(Cylinder)	역어셈블링(Disassembling)
②	MBR(Master Boot Record)	리버싱(Reversing)
③	클러스터(Cluster)	역컴파일(Decompiling)
④	슬랙(Slack)	카빙(Carving)

◦ 파일 카빙 : 저장 매체의 비할당 영역으로부터 파일을 복구하는 기법으로 저장 매체의 공간 할당에 따라 연속적인 카빙(continuous carving) 기법과 비연속적인 카빙(fragment recovery carving) 기법으로 나눌 수 있다. 연속적인 카빙 기법은 파일 내용이 저장 매체의 연속된 공간에 저장된 경우 수행하는 카빙 기법이고 비연속적인 카빙기법은 파일의 내용이 저장 매체의 여러 부분에 조각이나 저장된 경우에 수행하는 카빙 기법이다.

오답피하기 ④ 슬랙(Slack)은 저장매체의 물리적인 구조와 논리적인 구조의 차이로 발생하는 낭비 공간으로, 물리적으로 할당된 공간이지만 논리적으로는 사용할 수 없는 공간을 말한다. 램, 드라이브, 파일시스템, 볼륨 등에 나타난다.

정답 ④

이론서 : 602p 응용, 기출 : 585번, 576번 유사, 800제 : 332번 응용

9. ○△× 19.지방.9급

버퍼 오버플로우 공격 대응 방법 중 ASLR(Address Space Layout Randomization)에 대한 설명으로 옳은 것은?

① 함수의 복귀 주소 위조 시, 공격자가 원하는 메모리 공간의 주소를 지정하기 어렵게 한다.
② 함수의 복귀 주소와 버퍼 사이에 랜덤(Random) 값을 저장하여 해당 주소의 변조 여부를 탐지한다.
③ 스택에 있는 함수 복귀 주소를 실행 가능한 임의의 libc 영역 내 주소로 지정하여 공격자가 원하는 함수의 실행을 방해한다.
④ 함수 호출 시 복귀 주소를 특수 스택에 저장하고 종료 시 해당 스택에 저장된 값과 비교하여 공격을 탐지한다.

rtl 공격

◦ Non-Executable Stack에 대한 해커의 대응책은 rtl(return to libc)이다. rtl은 스택에 있는 ret 주소를 실행 가능한 임의의 주소(libc 영역의 주소)로 돌려 원하는 함수를 수행하게 만드는 기법이다. 메모리에 적재된 공유 라이브러리는 스택에 존재하는 것이 아니므로 Non-Executable Stack을 우회하는 것이 가능하다.

오답피하기 ① ASLR(Address Space Layout Randomization)은 공격을 막는 다른 실행 시간 기법으로는 프로세스 주소 공간에 있는 중요 데이터 구조의 위치를 조작하는 것이 있다. 공격자는 셸코드로 제어를 넘기기 위해 공격에 사용할 적당한 반환주소를 결정하는데 예측된 주소를 사용한다. 이 예측을 어렵게 만드는 한 가지 기법은 각 프로세스 안의 스택이 임의의 다른 곳에 위치하도록 변경하는 것이다. 따라서 스택 메모리 영역을 1메가 바이트 정도 옮긴다면 대부분의 프로그램에 미치는 영향은 적지만 타깃 버퍼의 주소 예측을 거의 불가능하게 만든다.

정답 ①

이론서 : 278p 응용(적중), 기출 : 206p 유사, 800제 : 160번 유사

10. ○△× 19.지방.9급

국내의 기관이나 기업이 정보 및 개인정보를 체계적으로 보호할 수 있도록 통합된 관리체계 인증제도는?

① PIPL-P
② ISMS-I
③ PIMS-I
④ ISMS-P

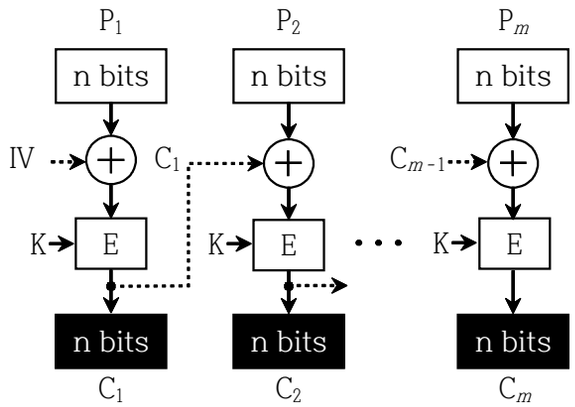
오답피하기 ④ ISMS-P 인증은 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 제도이다. 기존 정보보호 관리체계(ISMS) 인증과 개인정보보호 관리체계(PIMS) 인증을 통합하여 2018년 11월 7일부터 시행되었다.

정답 ④

모의 : 13회/3번 유사

11. ○△× 19.지방.9급

다음의 블록 암호 운용 모드는?



보기

E : 암호화 K : 암호화 키
$P_1, P_2, ..., P_m$: 평문 블록 $C_1, C_2, ..., C_m$: 암호 블록
IV : 초기화 벡터 ⊕ : XOR

① 전자 코드북 모드(Electronic Code Book Mode)
② 암호 블록 연결 모드(Cipher Block Chaining Mode)
③ 암호 피드백 모드(Cipher Feedback Mode)
④ 출력 피드백 모드(Output Feedback Mode)

오답피하기 ② CBC 모드에서는 한 단계 전에 수행되어 결과로 출력된 암호문 블록에 평문 블록을 XOR하고 나서 암호화를 수행한다. 따라서 생성되는 각각의 암호문 블록은 현재 평문 블록뿐만 아니라 그 이전의 평문 블록들의 영향도 받게 된다.

정답 ②

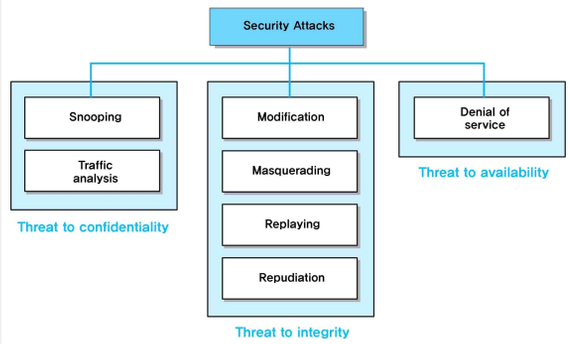
이론서 : 63p 응용(적중), 기출 : 52번 응용, 800제 : 328번 응용

12. ○△× 19.지방.9급

무결성을 위협하는 공격이 아닌 것은?

① 스누핑 공격(Snooping Attack)
② 메시지 변조 공격(Message Modification Attack)
③ 위장 공격(Masquerading Attack)
④ 재전송 공격(Replay Attack)

보안 목표와 관련된 공격의 분류



오답피하기 ① 스누핑은 기밀성을 위협하는 공격이다.

정답 ①

이론서 : 6p 응용(적중), 800제 : 793번 유사

13. ○△× 19.지방.9급

다음에서 설명하는 접근 제어 모델은?

보기

군사용 보안구조의 요구사항을 충족시키기 위해 개발된 최초의 수학적 모델로 알려져 있다. 불법적 파괴나 변조보다는 정보의 기밀성 유지에 초점을 두고 있다. '상위레벨 읽기금지 정책(No-Read-Up Policy)'을 통해 인가받은 비밀 등급이 낮은 주체는 높은 보안 등급의 정보를 열람할 수 없다. 또한, 인가받은 비밀 등급 이하의 정보 수정을 금지하는 '하위레벨 쓰기금지 정책(No-Write-Down Policy)'을 통해 비밀 정보의 유출을 차단한다.

① DAC(Discretionary Access Control) 모델
② Bell-LaPadula 모델
③ Biba 모델
④ RBAC(Role-Based Access Control) 모델

오답피하기 ② Bell-LaPadula 모델은 높은 보안 등급으로부터 낮은 보안 등급으로 정보가 유출되는 것을 방지하는 것으로, 정보의 불법적인 파괴나 변조보다는 불법적인 비밀 유출 방지에 중점을 둔 최초의 수학적 모델로 알려진 접근통제 모델

정답 ②

이론서 : 175p 응용(적중), 기출 : 174번 유사, 800제 : 97번 유사

14. ○△× 19.지방.9급

유럽의 일반개인정보보호법(GDPR)에 대한 설명으로 옳은 것은?

① EU 회원국들 간 개인정보의 자유로운 이동을 금지하기 위한 목적을 갖는다.
② 그 자체로는 EU의 모든 회원국에게 직접적인 법적 구속력을 갖지 않는다.
③ 중요한 사항 위반 시 직전 회계연도의 전 세계 매출액 4% 또는 2천만 유로 중 높은 금액이 최대한도 부과 금액이다.
④ 만 19세 미만 미성년자의 개인정보 수집 시 친권자의 동의를 얻어야 한다.

◦ GDPR 위반의 경우 전 세계 매출액 2% 또는 1천만 유로 중 더 큰 금액이, 심각한 위반의 경우 전 세계 매출액 4% 또는 2천만 유로 중 더 큰 금액의 과징금이 부과된다.
◦ GDPR에서는 one-stop-shop 메커니즘의 도입과 법적 구속력 있는 단일한 규칙을 적용함으로써 기업이 사업 수행에 따르는 필요 비용을 절약할 수 있도록 하였다.
※ one-stop-shop 메커니즘 : 처리되는 개인정보의 정보주체가 EU 내 여러 국가에 흩어져 있는 경우 주 사업장이나 단일 사업장이 소속된 국가의 감독기구가 선임 감독기구의 역할을 수행하면서 다른 회원국의 감독기구와 수시로 협력함으로써 컨트롤러·프로세서는 하나의 감독기구만을 대상으로 대응 가능한 메커니즘.)

오답피하기 ① GDPR에서는 one-stop-shop 메커니즘으로 EU 회원국들 간 단일한 규칙 적용을 목적으로 한다. ② GDPR은 EU의 모든 회원국들에게 직접적인 법적 구속력을 가지며, 무엇보다 GDPR 위반 기업에게 막중한 제재가 가해진다. 특히 GDPR의 준수 여부는 EU에 재화와 서비스를 제공하는 우리 기업들에게도 상당한 영향을 미친다. ④ 만 16세 미만의 아동에게 직접 정보사회서비스를 제공할 때 부모 등 친권을 보유하는 자의 동의를 받아야 한다. 다만 각 회원국은 개별 법률을 통하여 친권자 동의를 요하는 아동의 연령 기준을 만 13세까지 낮추어 규정할 수 있다.

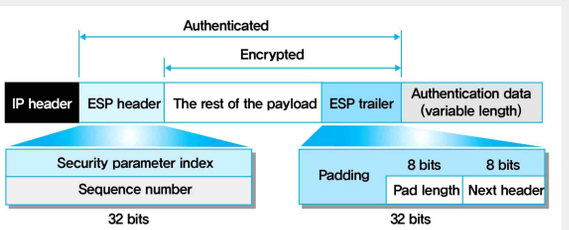
정답 ③

15. ○△× 19.지방.9급

IPsec의 캡슐화 보안 페이로드(ESP) 헤더에서 암호화되는 필드가 아닌 것은?

① SPI(Security Parameter Index)
② Payload Data
③ Padding
④ Next Header

ESP 헤더 데이터 형식



오답피하기 ① ESP Header 포함된 SPI는 인증 영역에는 포함되지만, 암호화 영역에는 포함되지 않는다.

정답 ①

이론서 : 484p 응용(적중), 800제 : 627번 응용, 모의 : 16회/11번 응용

16. ○△× 19.지방.9급

SSL 프로토콜에 대한 설명으로 옳지 않은 것은?

① 서버와 클라이언트 간 양방향 통신에 동일한 암호화 키를 사용한다.
② 웹 서비스 이외에 다른 응용 프로그램에도 적용할 수 있다.
③ 단편화, 압축, MAC 추가, 암호화, SSL 레코드 헤더 추가의 과정으로 이루어진다.
④ 암호화 기능을 사용하면 주고받는 데이터가 인터넷상에서 도청되는 위험성을 줄일 수 있다.

◦ SSL은 별도의 통신 계층으로 사용될 수도 있고, 특정 응용에 포함되어 사용될 수 있다.

오답피하기 ① 대칭 암호화는 비대칭 암호화보다 훨씬 빠르기 때문에 전송 중인 실제 데이터를 보호하는 데 사용된다. 반면에 서버와 클라이언트 간의 통신에는 RSA와 같은 공개키 암호기술이 주로 사용된다.

정답 ①

이론서 : 534p~537p 응용, 기출 : 508번 응용, 800제 : 292번 응용

17. ○△× 19.지방.9급

KCMVP에 대한 설명으로 옳은 것은?

① 보안 기능을 만족하는 신뢰도 인증 기준으로 EAL1부터 EAL7까지의 등급이 있다.
② 암호 알고리즘이 구현된 프로그램 모듈의 안전성과 구현 적합성을 검증하는 제도이다.
③ 개인정보 보호활동을 체계적·지속적으로 수행하기 위한 관리체계의 구축과 이행 여부를 평가한다.
④ 조직의 정보자산을 효과적으로 보호하고 있는지 평가하여 일정 수준 이상의 기업에 인증을 부여한다.

오답피하기 ② KCMVP(Korea Cryptographic Module Validation) 검증제도는 전자정부 법 시행령 제 69조와 [암호모듈 시험 및 검증지침]에 의거, 국가·공공기관 정보통신망에서 소통되는 자료 중에서 비밀로 분류되지 않은 중요 정보의 보호를 위해 사용되는 암호모듈의 안전성과 구현 적합성을 검증하는 제도이다. 검증대상에 해당되는 암호모듈은 소프트웨어, 하드웨어, 펌웨어 또는 이들을 조합한 형태로 구현될 수 있으며 소프트웨어 암호모듈 검증기준 또는 암호모듈 검증기준(KS X ISO/IEC 19790)을 준수하여서 시험되고 있다.

정답 ②

이론서 : 28p 응용, 기출 : 12번 유사

18. ○△× 19.지방.9급

「개인정보 보호법」상 개인정보 분쟁조정위원회에 대한 설명으로 옳지 않은 것은?

① 분쟁조정위원회는 위원장 1명을 포함한 20명 이내의 위원으로 구성한다.
② 위원장은 행정안전부·방송통신위원회·금융위원회 및 개인정보보호위원회의 고위공무원단에 속하는 일반직공무원 중에서 위촉한다.
③ 분쟁조정위원회는 재적위원 과반수의 출석으로 개의하며 출석위원 과반수의 찬성으로 의결한다.
④ 위원은 자격정지 이상의 형을 선고받거나 심신상의 장애로 직무를 수행할 수 없는 경우를 제외하고는 그의 의사에 반하여 면직되거나 해촉되지 아니한다.

➡ 제40조(설치 및 구성)
① 개인정보에 관한 분쟁의 조정을 위하여 개인정보 분쟁조정위원회를 둔다.
② 분쟁조정위원회는 위원장 1명을 포함한 20명 이내의 위원으로 구성하며, 위원은 당연직위원과 위촉위원으로 구성한다.
③ 위촉위원은 다음 각 호의 어느 하나에 해당하는 사람 중에서 보호위원회 위원장이 위촉하고, 대통령령으로 정하는 국가기관 소속 공무원은 당연직위원이 된다.
1. 개인정보 보호업무를 관장하는 중앙행정기관의 고위공무원단에 속하는 공무원으로 재직하였던 사람 또는 이에 상당하는 공공부문 및 관련 단체의 직에 재직하고 있거나 재직하였던 사람으로서 개인정보 보호업무의 경험이 있는 사람
2. 대학이나 공인된 연구기관에서 부교수 이상 또는 이에 상당하는 직에 재직하고 있거나 재직하였던 사람
3. 판사·검사 또는 변호사로 재직하고 있거나 재직하였던 사람
4. 개인정보 보호와 관련된 시민사회단체 또는 소비자단체로부터 추천을 받은 사람
5. 개인정보처리자로 구성된 사업자단체의 임원으로 재직하고 있거나 재직하였던 사람

④ 위원장은 위원 중에서 공무원이 아닌 사람으로 보호위원회 위원장이 위촉한다.
⑤ 위원장과 위촉위원의 임기는 2년으로 하되, 1차에 한하여 연임할 수 있다.
⑥ 분쟁조정위원회는 분쟁조정 업무를 효율적으로 수행하기 위하여 필요하면 대통령령으로 정하는 바에 따라 조정사건의 분야별로 5명 이내의 위원으로 구성되는 조정부를 둘 수 있다. 이 경우 조정부가 분쟁조정위원회에서 위임받아 의결한 사항은 분쟁조정위원회에서 의결한 것으로 본다.
⑦ 분쟁조정위원회 또는 조정부는 재적위원 과반수의 출석으로 개의하며 출석위원 과반수의 찬성으로 의결한다.
⑧ 보호위원회는 분쟁조정 접수, 사실 확인 등 분쟁조정에 필요한 사무를 처리할 수 있다.
⑨ 이 법에서 정한 사항 외에 분쟁조정위원회 운영에 필요한 사항은 대통령령으로 정한다.

➡ 제41조(위원의 신분보장)
위원은 자격정지 이상의 형을 선고받거나 심신상의 장애로 직무를 수행할 수 없는 경우를 제외하고는 그의 의사에 반하여 면직되거나 해촉되지 아니한다.

오답피하기 ② 위원장은 위원 중에서 공무원이 아닌 사람으로 보호위원회 위원장이 위촉한다.

정답 ②

이론서 : 699p 응용, 800제 : 379번 응용

19. ○△× 19.지방.9급

전자화폐 및 가상화폐에 대한 설명으로 옳지 않은 것은?

① 전자화폐는 전자적 매체에 화폐의 가치를 저장한 후 물품 및 서비스 구매 시 활용하는 결제 수단이며, 가상화폐는 전자화폐의 일종으로 볼 수 있다.
② 전자화폐는 발행, 사용, 교환 등의 절차에 관하여 법률에서 규정하고 있으나, 가상화폐는 별도로 규정하고 있지 않다.
③ 가상화폐인 비트코인은 분산원장기술로 알려진 블록체인을 이용한다.
④ 가상화폐인 비트코인은 전자화폐와 마찬가지로 이중 지불(Double Spending)문제가 발생하지 않는다.

◦ 전자 화폐(electronic money, e-cash, e-money) : 일정한 화폐의 가치를 IC 카드나 PC 등에 디지털 데이터 형태로 저장하였다가 온라인이나 오프라인으로 상품 구매/운임 지불을 할 수 있는 전자적인 지급 수단이다. 기본적으로 2가지 형식이 있는데, 하나는 오프라인 시장에서 현금 대신 지불하는 수단과 다른 하나는 온라인 시장에서의 지불 수단이다.
◦ 가상 화폐(virtual currency) : 컴퓨터 등에 정보 형태로 남아 실물 없이 사이버상으로만 거래되는 전자 화폐의 일종이다. 2012년 유럽 중앙은행(European Central Bank)은 가상 화폐를 '가상화폐 발행자가 발행 · 관리하고, 특정 가상 커뮤니티의 구성원들 사이에서 이용되며 대부분 법적 규제를 받지 않는 디지털 화폐'라고 정의하였다. 가상 화폐는 중앙은행이나 금융기관 등 공인기관이 관여하지 않는다. 인터넷 쿠폰, 모바일 쿠폰, 게임 머니 등과 암호 화폐인 비트코인이 가상 화폐에 해당된다.

오답피하기 ④ 이중지불(double spending)이란 원본 파일에 저장된 가치를 지불한 뒤, 해당 파일을 복사하여 다른 사람에게 또 지불하는 것을 말한다. 예를 들어, A가 B에게 1,000원이라고 기록된 파일을 전송한 후 다시 해당 파일을 복사하여 C에게 또 1,000원을 전송하는 것을 말한다. 컴퓨터와 인터넷에서 모든 파일은 복사가 가능하기 때문에 이중지불 문제를 피할 수 없다. 하지만, 전자화폐와 가상화폐에서 이런 문제가 발생하면 안 되므로 연구가 계속 이루어지고 있고 기술도 발전하고 있다.

정답 ④

이론서 : 586p 응용, 기출 : 560번 응용

20. ○△× 19.지방.9급

X.509 인증서(버전 3)의 확장(Extensions) 영역에 포함되지 않는 항목은?

① 인증서 정책(Certificate Policies)
② 기관 키 식별자(Authority Key Identifier)
③ 키 용도(Key Usage)
④ 서명 알고리즘 식별자(Signature Algorithm Identifier)

기본 영역
◦ 버전(Version)
◦ 일련번호(Serial Number)
◦ 알고리즘 식별자(Algorithm Identifier)
◦ 발행자(Issuer)
◦ 유효 개시시간(Validity From)
◦ 유효 만기시간(Validity To)
◦ 주체(Subject)
◦ 주체 공개키 정보(Subject Public-Key Information)
◦ 알고리즘(Algorithm)
◦ 서명(Signature)

확장 영역
◦ 키와 정책 정보(key and policy information)
  – 기관키 식별자(authority key identifier)
  – 사용자키 식별자(subject key identifier)
  – 키 사용(key usage)
  – 인증서 정책(certificate policies)
◦ 사용자와 발행자 속성(subject and issuer attribute)
  – 사용자 대체 이름(subject alternative name)
  – 발급자 대체 이름(issuer alternative name)
◦ 인증 경로 제약조건(certification path constraints)
  – 기본 제한(basic constraints)
  – 이름 제한(name constraints)
  – 정책 제한(policy constraints)

오답피하기 ④ 서명 알고리즘 식별자는 기본 영역에 포함된다.

정답 ④

이론서 : 130p 응용(적중), 800제 : 782번 유사, 모의 : 14회 /16번 부연설명 적중