2021-국가직-정보보호론-나형

총평

번호	단원	총평
1	시스템보안, 기출	해당 단원의 이론과 기출을 통해 접근하면 된다.
2	개요, 기출	해당 단원의 이론과 기출을 통해 접근하면 된다.
3	네트워크보안, 기출	해당 단원의 이론과 기출을 통해 접근하면 된다.
4	암호학, 기출	해당 단원의 이론과 기출을 통해 접근하면 된다.
5	관리체계, 기출	해당 단원의 이론과 기출을 통해 접근하면 된다.
6	어플리케이션보안, 기출	해당 단원의 이론과 기출을 통해 접근하면 된다.
7	암호학	개별적으로 알고 있던 정보를 종합하여 소거해 나가면 답을 찾을 수 있다.
8	어플리케이션보안, 기출	해당 단원의 이론과 기출을 통해 접근하면 된다.
9	암호학	ECC의 정의와 장단점을 알고 있으나 이렇게 구체적으로 구하는 문제는 예상 밖의 문제이다. 2021 국가직 정보보호론의 Killer 문항이다.
10	관련법규, 기출	해당 단원의 이론과 기출을 통해 접근하면 된다. 지문 중에 거슬리는 지문을 찾으면 된다.
11	시스템보안, 기출	해당 단원의 이론과 기출을 통해 접근하면 된다.
12	암호학, 기출	해당 단원의 이론과 기출을 통해 접근하면 된다.
13	어플리케이션보안, 기출	해당 단원의 이론과 기출을 통해 접근하면 된다.
14	관리체계	구체적으로 묻는 질문이나 “물리적 및 환경적”이라는 단어에 거슬리는 지문을 찾으면 된다.
15	암호학, 기출	해당 단원의 이론과 기출을 통해 접근하면 된다.
16	네트워크보안	헷갈릴 수는 있으나 IP 헤더는 패킷이 시작이라는 개념으로 풀면 된다.
17	관련법규	“정보통신망법”이 개정되면서 개인정보와 관련된 부분이 빠졌다는 사실로 접근하면 된다.
18	네트워크보안, 기출	해당 단원의 이론과 기출을 통해 접근하면 된다.
19	관련법규	해당 단원의 이론과 모의고사를 통해 접근하면 된다.
20	시스템보안, 기출	해당 단원의 이론과 기출을 통해 접근하면 된다.

해설

문 1. 겉으로는 유용한 프로그램으로 보이지만 사용자가 의도하지 않은 악성 루틴이 숨어 있어서 사용자가 실행시키면 동작하는 악성 소프트웨어는?

① 키로거 ② 트로이목마

③ 애드웨어 ④ 랜섬웨어

정답 체크

(2) 사용자가 의도하지 않은 코드를 정상적인 프로그램에 삽입한 형태이다.
오답 체크
(1) 사용자가 키보드로 PC에 입력하는 내용을 몰래 가로채어 기록하는 행위를 말한다. 하드웨어, 소프트웨어를 활용한 방법에서부터 전자적, 음향기술을 활용한 기법까지 다양한 키로깅 방법이 존재한다.
(3) 특정 소프트웨어를 실행할 때 또는 설치 후 자동적으로 광고가 표시되는 프로그램을 말한다. 프리웨어인 경우 불가피하게 광고 수익으로 운영되는 경우가 많으므로, 애드웨어라고 반드시 악성 소프트웨어에 속하는 것은 아니다.
(4) 컴퓨터 시스템을 감염시켜 접근을 제한하고 일종의 몸값을 요구하는 악성 소프트웨어의 한 종류이다. 컴퓨터로의 접근이 제한되기 때문에 제한을 없애려면 해당 악성 프로그램을 개발한 자에게 지불을 강요받게 된다.

문 2. 능동적 공격에 해당하는 것만을 모두 고르면?

ㄱ. 도청	ㄴ. 서비스 거부
ㄷ. 트래픽 분석	ㄹ. 메시지 변조

① ㄱ, ㄷ ② ㄴ, ㄷ
③ ㄴ, ㄹ ④ ㄷ, ㄹ

정답 체크
(3) ㄴ. 가용성을 해치는 능동적 공격이다.
ㄹ. 무결성을 해치는 능동적 공격이다.
오답 체크
(1), (2), (4) ㄱ, ㄷ은 기밀성을 해치는 수동적 공격이다.

문 3. 분산 서비스 거부(DDoS) 공격에 대한 설명으로 옳지 않은 것은?
① 하나의 공격 지점에서 대규모 공격 패킷을 발생시켜서 여러 사이트를 동시에 공격하는 방법이다.
② 가용성에 대한 공격이다.
③ 봇넷이 주로 활용된다.
④ 네트워크 대역폭이나 컴퓨터 시스템 자원을 공격 대상으로 한다.

정답 체크
(1) 여럿의 공격 지점에서 하나의 사이트를 동시에 공격한다.
오답 체크
(2) DDoS 공격을 받으면 서버는 서비스를 할 수 없다.
(3) 봇넷(좀비PC로 구성된 네트워크)이 DDoS에서 사용된다.
(4) 자원 고갈 또는 취약점 공격을 통해 공격을 수행한다.

문 4. 부인방지 서비스를 제공하기 위한 전자서명에 대한 설명으로 옳지 않은 것은?
① 서명할 문서에 의존하는 비트 패턴이어야 한다.
② 다른 문서에 사용된 서명을 재사용하는 것이 불가능해야 한다.
③ 전송자(서명자)와 수신자(검증자)가 공유한 비밀 정보를 이용하여 서명하여야 한다.
④ 서명한 문서의 내용을 임의로 변조하는 것이 불가능해야 한다.

정답 체크

(3) 대칭키를 이용하여 서명하는 것이 아니므로 비밀 정보를 공유할 필요가 없다(공개키 이용).
오답 체크
(1) 서명할 문서에 의존하여 서명이 발생한다.
(2) 서명은 재사용할 수 없다.
(4) 서명을 하면 서명자 인증, 무결성, 부인방지를 보장 받게 된다.

문 5. 다음은 IT 보안 관리를 위한 국제 표준(ISO/IEC 13335)의 위험 분석 방법에 대한 설명이다. ㉠ ~ ㉢에 들어갈 용어를 바르게 연결한 것은?

> (㉠)은 가능한 빠른 시간 내에 적정 수준의 보호를 제공한 후 시간을 두고 중요 시스템에 대한 보호 수단을 조사하고 조정하는 것을 목표로 한다. 이 방법은 모든 시스템에 대하여 (㉡)에서 제시하는 권고 사항을 구현하는 것으로 시작한다. 중요 시스템을 대상으로 위험에 즉각적으로 대응하기 위하여 비정형 접근법이 적용될 수 있다. 그리고 (㉢)에 의한 단계별 프로세스를 적절하게 수행한다. 결과적으로 시간이 흐름에 따라 비용 대비 효과적인 보안 통제가 선택되도록 할 수 있다.

	㉠	㉡	㉢
①	상세 위험 분석	기준선 접근법	복합 접근법
②	상세 위험 분석	복합 접근법	기준선 접근법
③	복합 접근법	기준선 접근법	상세 위험 분석
④	복합 접근법	상세 위험 분석	기준선 접근법

정답 체크
(3) 복합 접근법 : 먼저 조직 활동에 대한 필수적인 그리고 위험이 높은 시스템을 식별하고, 이러한 시스템에 대해서는 “상세위험 접근법”을 그렇지 않은 시스템에는 “기준선 접근법” 등을 각각 적용한다.
기준선 접근법 : 모든 시스템에 대하여 보호의 기본 수준(기준선)을 정하고, 이를 달성하기 위하여 보호대책을 선택한다.
상세 위험 분석 : 자산의 가치를 측정하고, 자산에 대한 위협의 정도와 취약점을 분석하여, 위험의 정도를 결정하는 방식이다.

문 6. 다음에서 설명하는 크로스사이트 스크립팅(XSS) 공격의 유형은?

> 공격자는 XSS 코드를 포함한 URL을 사용자에게 보낸다. 사용자가 그 URL을 요청하고 해당 웹 서버가 사용자 요청에 응답한다. 이때 XSS 코드를 포함한 스크립트가 웹 서버로부터 사용자에게 전달되고 사용자 측에서 스크립트가 실행된다.

① 세컨드 오더 XSS

② DOM 기반 XSS
③ 저장 XSS
④ 반사 XSS

정답 체크
(4) 악성 스크립트가 포함된 URL을 사용자가 클릭하도록 유도하여 URL을 클릭하면 클라이언트를 공격하는 것이다.
오답 체크
(1) 저장 또는 persistent XSS이라고 한다.
(2) DOM(Document Object Model) 환경에서 악성 URL을 통해 사용자의 브라우저를 공격하는 것이다.
(3) 접속자가 많은 웹 사이트를 대상으로 공격자가 XSS 취약점이 있는 웹 서버에 공격용 스크립트(script)를 입력시켜 놓으면, 방문자가 악성 스크립트가 삽입되어 있는 페이지를 읽는 순간 방문자의 브라우저를 공격하는 방식이다.

문 7. SHA 알고리즘에서 사용하는 블록 크기와 출력되는 해시의 길이를 바르게 연결한 것은?

	알고리즘	블록 크기	해시 길이
①	SHA-1	256비트	160비트
②	SHA-256	512비트	256비트
③	SHA-384	1024비트	256비트
④	SHA-512	512비트	512비트

정답 체크
(2) 블록 길이와 해시 길이가 정확하게 기술되어 있다.
오답 체크
(1) 블록 길이가 512이다.
(3) 해시 길이가 384이다.
(4) 블록 길이가 1024이다.

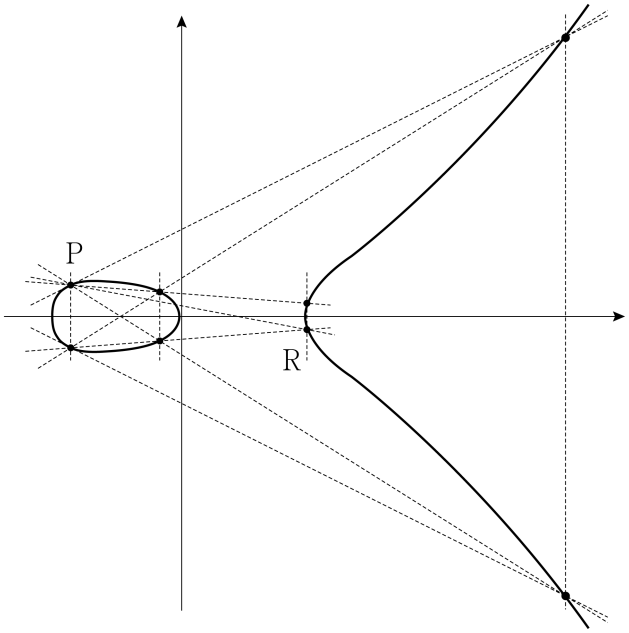
문 8. 데이터베이스 접근 권한 관리를 위한 DCL(Data Control Language)에 속하는 명령으로 그 설명이 옳은 것은?

① GRANT: 사용자가 테이블이나 뷰의 내용을 읽고 선택한다.
② REVOKE: 이미 부여된 데이터베이스 객체의 권한을 취소한다.
③ DROP: 데이터베이스 객체를 삭제한다.
④ DENY: 기존 데이터베이스 객체를 다시 정의한다.

정답 체크
(2) revoke는 권한을 취소한다.
오답 체크
(1) grant는 권한을 부여한다.
(3) drop은 ddl이다.
(4) deny는 권한을 금지한다.

문 9. 타원곡선 암호시스템(ECC)은 타원곡선 이산대수의 어려움을 이용한다. 그림과 같이 실수 위에 정의된 타원곡선과 타원곡선 상의 두 점 P와 R이 주어진 경우, $\mathrm{R}=k\mathrm{P}$를 만족하는 정수 k의 값은?

(단, 점선은 타원곡선의 접선, 점을 연결하는 직선 또는 수직선을 나타낸다)

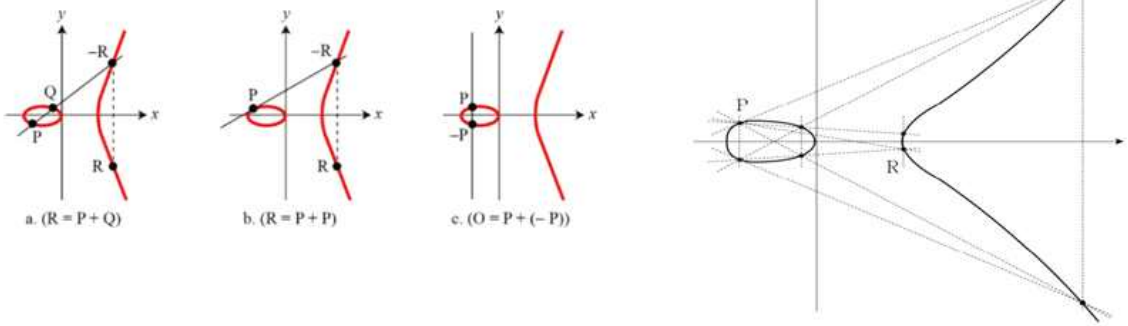


① 2 ② 3

③ 4 ④ 5

정답 체크

(3) 같은 값을 가지고 있는 P를 구하는 타원 곡선(P를 지나는 직선이 타원과 만나는 R)은 R=2P로 정의한다. 그러나 문제에서는 해당 P를 지나는 직선이 2개이므로 R=4P가 된다.



문 10. 「개인정보 보호법」상 가명정보의 처리에 관한 특례에 대한 사항으로 옳지 않은 것은?

① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.

② 개인정보처리자는 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 내부적으로 해당 정보를 처리 보관하되, 제3자에게 제공해서는 아니 된다.

③ 개인정보처리자는 가명정보를 처리하고자 하는 경우에는 가명정보의 처리 목적, 제3자 제공 시 제공받는 자 등 가명정보의 처리 내용을 관리하기 위하여 대통령령으로 정하는 사항에 대한 관련 기록을 작성하여 보관하여야 한다.

④ 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 서로 다른 개인정보처리자 간의 가명정보의 결합은 개인정보 보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 수행한다.

정답 체크
(2) 제28조의5(가명정보 처리 시 금지의무 등) ② 개인정보처리자는 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 해당 정보의 처리를 중지하고, 지체 없이 회수·파기하여야 한다.
오답 체크
(1) 제28조의2(가명정보의 처리 등) ① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.
(3) 제28조의4(가명정보에 대한 안전조치의무 등) ② 개인정보처리자는 가명정보를 처리하고자 하는 경우에는 가명정보의 처리 목적, 제3자 제공 시 제공받는 자 등 가명정보의 처리 내용을 관리하기 위하여 대통령령으로 정하는 사항에 대한 관련 기록을 작성하여 보관하여야 한다.
(4) 제28조의3(가명정보의 결합 제한) ① 제28조의2에도 불구하고 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 서로 다른 개인정보처리자 간의 가명정보의 결합은 보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 수행한다.

문 11. 시스템 내 하드웨어의 구동, 서비스의 동작, 에러 등의 다양한 이벤트를 선택·수집하여 로그로 저장하고 이를 다른 시스템에 전송할 수 있도록 해 주는 유닉스의 범용 로깅 메커니즘은?

① utmp ② syslog
③ history ④ pacct

정답 체크
(2) 시스템의 로그에 대한 정보 대부분을 수집하여 로깅한다.
오답 체크
(1) 현재 시스템에 로그인한 사용자의 상태를 출력(로깅)한다.
(3) 유닉스에서는 실행 명령에 대한 기록이 .sh_history, .csh_history, .bash_history 같이 '[셸의 종류]_history 파일' 형식으로 각 계정의 홈 디렉터리에 저장된다.
(4) 시스템에 로그인한 모든 사용자가 수행한 프로그램에 대한 정보를 저장하는 로그이다.

문 12. 공개키 암호시스템에 대한 설명으로 옳은 것만을 모두 고르면?

> ㄱ. 한 쌍의 공개키와 개인키 중에서 개인키만 비밀로 보관하면 된다.
> ㄴ. 동일한 안전성을 가정할 때 ECC는 RSA보다 더 짧은 길이의 키를 필요로 한다.
> ㄷ. 키의 분배와 관리가 대칭키 암호시스템에 비하여 어렵다.
> ㄹ. 일반적으로 암호화 및 복호화 처리 속도가 대칭키 암호시스템에 비하여 빠르다.

① ㄱ, ㄴ ② ㄱ, ㄹ
③ ㄴ, ㄷ ④ ㄷ, ㄹ

정답 체크
(1) ㄱ. 공개키는 공개하고, 개인키는 비밀로 한다.
ㄴ. ECC가 RSA에 비해 키 길이가 짧다.

오답 체크
(2), (3), (4) ㄷ. 공개키에서는 키 배송 문제가 발생하지 않는다.
ㄹ. 수학적 연산으로 인해 속도가 느리다.

문 13. 이메일의 보안을 강화하기 위한 기술이 아닌 것은?

① IMAP
② S/MIME
③ PEM
④ PGP

정답 체크
(1) 메일 클라이언트가 메일 서버로부터 메일을 내려 받을 때 사용하는 프로토콜이다(서버에 복사본 저장).
오답 체크
(2), (3), (4) 이메일 보안 프로토콜이다.

문 14. 국제 정보보호 표준(ISO 27001:2013 Annex)은 14개 통제 영역에 대하여 114개 통제 항목을 정의하고 있다. 통제 영역의 하나인 물리적 및 환경적 보안에 속하는 통제 항목에 대한 설명에 해당하지 않는 것은?

① 보안 구역은 인가된 인력만의 접근을 보장하기 위하여 적절한 출입 통제로 보호한다.
② 자연 재해, 악의적인 공격 또는 사고에 대비한 물리적 보호를 설계하고 적용한다.
③ 데이터를 전송하거나 정보 서비스를 지원하는 전력 및 통신 배선을 도청, 간섭, 파손으로부터 보호한다.
④ 정보보호에 영향을 주는 조직, 업무 프로세스, 정보 처리 시설, 시스템의 변경을 통제한다.

정답 체크
(4) 운영 보안에 해당한다.
오답 체크
(1) 물리적 출입 통제에 해당한다.
(2) 외부 및 환경 위협에 대비한 보호에 해당한다.
(3) 배선 보안에 해당한다.

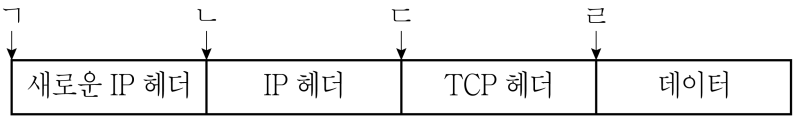
문 15. 대칭키 암호시스템에 대한 암호 분석 방법과 암호 분석가에게 필수적으로 제공되는 모든 정보를 연결한 것으로 옳지 않은 것은?

① 암호문 단독(ciphertext only) 공격 – 암호 알고리즘, 해독할 암호문
② 기지 평문(known plaintext) 공격 – 암호 알고리즘, 해독할 암호문, 임의의 평문
③ 선택 평문(chosen plaintext) 공격 – 암호 알고리즘, 해독할 암호문, 암호 분석가에 의해 선택된 평문과 해독할 암호문에 사용된 키로 생성한 해당 암호문
④ 선택 암호문(chosen ciphertext) 공격 – 암호 알고리즘, 해독할 암호문, 암호 분석가에 의해 선택된 암호문과 해독할 암호문에 사용된 키로 복호화한 해당 평문

정답 체크
(2) 암호 해독자가 일정량의 평문(P)에 대응하는 암호문(C) 쌍을 이미 알고 있는 상태에서 암호문(C)과 평문(P)의 관계로부터 키(K)나 평문(P)를 추정한다.
오답 체크

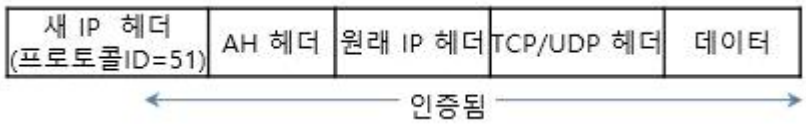
(1) 해독자가 단지 암호문 C만을 갖고 이로부터 평문(P)이나 키(K)를 찾아내는 방법이다. 평문(P)의 통계적 성질, 문장의 특성 등을 추정하여 해독하는 방법이다.
(3) 해독자가 사용된 암호화기에 접근할 수 있어 평문(P)를 선택하여 평문에 대응하는 암호문(C)를 얻어 키(K)나 평문(P)를 해독하는 방법이다.
(4) 해독자가 복호화기에 접근할 수 있어 암호문(C)에 대응하는 평문(P)를 얻어내어 해독하는 방법이다. 공격자는 해독하고자 하는 암호문을 제외한 모든 암호문에 대해 평문을 획득할 수 있는 능력을 가지고 있다고 본다.

문 16. IPv4 패킷에 대하여 터널 모드의 IPSec AH(Authentication Header) 프로토콜을 적용하여 산출된 인증 헤더가 들어갈 위치로 옳은 것은?



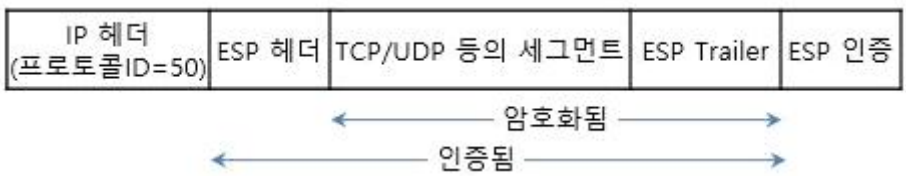
① ㄱ ② ㄴ
③ ㄷ ④ ㄹ

정답 체크
(2) AH Tunnel mode : IP 헤더는 패킷의 시작이므로 맨 앞에 와야 한다.

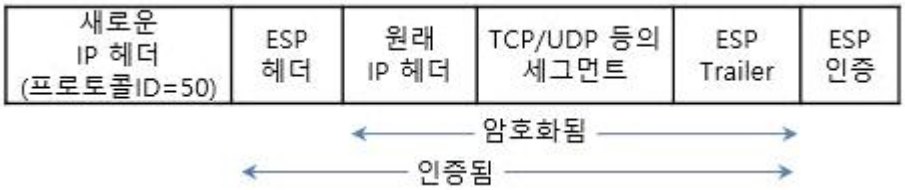


Tip!
AH Transport mode

ESP Transport mode



ESP Tunnel mode



문 17. 정보보호 관련 법률과 소관 행정기관을 잘못 짝 지은 것은?
① 「전자정부법」 – 행정안전부

② 「신용정보의 이용 및 보호에 관한 법률」 – 금융위원회
③ 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 – 개인정보보호위원회
④ 「정보통신기반 보호법」 – 과학기술정보통신부

정답 체크
(3) 소관 행정기관은 방송통신위원회, 과학기술정보통신부이다.

문 18. 침입탐지시스템의 비정상(anomaly) 탐지 기법에 대한 설명으로 옳지 않은 것은?
① 상대적으로 급격한 변화나 발생 확률이 낮은 행위를 탐지한다.
② 정상 행위를 예측하기 어렵고 오탐률이 높지만 알려지지 않은 공격에도 대응할 수 있다.
③ 수집된 다양한 정보로부터 생성한 프로파일이나 통계적 임계치를 이용한다.
④ 상태전이 분석과 패턴 매칭 방식이 주로 사용된다.

정답 체크
(4) 해당 방식은 오용 탐지 기법에 해당한다.
오답 체크
(1) 임계값을 정해놓고 임계값을 넘으면 비정상으로 탐지한다.
(2) 임계값을 이용하면 알려지지 않은 공격에도 대응할 수 있다.
(3) 통계를 이용하여 임계값을 만든다.

문 19. 「전자서명법」상 과학기술정보통신부장관이 정하여 고시하는 전자서명인증업무 운영기준에 포함되어 있는 사항이 아닌 것은?
① 전자서명 관련 기술의 연구·개발·활용 및 표준화
② 전자서명 및 전자문서의 위조·변조 방지대책
③ 전자서명인증서비스의 가입·이용 절차 및 가입자 확인방법
④ 전자서명인증업무의 휴지·폐지 절차

정답 체크
(1) 제5조(전자서명의 이용 촉진을 위한 지원) 과학기술정보통신부장관은 전자서명의 이용을 촉진하기 위하여 다음 각 호의 사항에 대한 행정적·재정적·기술적 지원을 할 수 있다.
1. 전자서명 관련 기술의 연구·개발·활용 및 표준화
2. 전자서명 관련 전문인력의 양성
3. 다양한 전자서명수단의 이용 확산을 위한 시범사업 추진
4. 전자서명의 상호연동 촉진을 위한 기술지원 및 연동설비 등의 운영
5. 제9조에 따른 인정기관 및 제10조에 따른 평가기관의 업무 수행 및 운영
6. 그 밖에 전자서명의 이용 촉진을 위하여 필요한 사항
오답 체크
(2), (3), (4) 제7조(전자서명인증업무 운영기준 등) ② 과학기술정보통신부장관은 다음 각 호의 사항이 포함된 전자서명인증업무 운영기준(이하 “운영기준”이라 한다)을 정하여 고시한다. 이 경우 운영기준은 국제적으로 인정되는 기준 등을 고려하여 정하여야 한다.
1. 전자서명 및 전자문서의 위조·변조 방지대책
2. 전자서명인증서비스의 가입·이용 절차 및 가입자 확인방법
3. 전자서명인증업무의 휴지·폐지 절차
4. 전자서명인증업무 관련 시설기준 및 자료의 보호방법

5. 가입자 및 이용자의 권익 보호대책
6. 그 밖에 전자서명인증업무의 운영·관리에 관한 사항

문 20. 안드로이드 보안 체계에 대한 설명으로 옳지 않은 것은?

① 모든 응용 프로그램은 일반 사용자 권한으로 실행된다.

② 기본적으로 안드로이드는 일반 계정으로 동작하는데 이를 루트로 바꾸면 일반 계정의 제한을 벗어나 기기에 대한 완전한 통제권을 가질 수 있다.

③ 응용 프로그램은 샌드박스 프로세스 내부에서 실행되며, 기본적으로 시스템과 다른 응용 프로그램으로의 접근이 통제된다.

④ 설치되는 응용 프로그램은 구글의 인증 기관에 의해 서명·배포된다.

정답 체크
(4) 개발자에 의해 서명 및 배포된다.
오답 체크
(1) 일반 사용자 권한으로 실행된다.
(2) 루트는 완전한 통제권을 가진다(루팅).
(3) 샌드박스를 이용하여 접근을 통제하나 iOS에 비해서는 자유로운 편이다.