정보보호론

문 1. 겉으로는 유용한 프로그램으로 보이지만 사용자가 의도하지 않은 악성 루틴이 숨어 있어서 사용자가 실행시키면 동작하는 악성 소프트웨어는? 2

① 키로거 ② 트로이목마
③ 애드웨어 ④ 랜섬웨어

[해설]

- 트로이목마 프로그램 : 유용하거나 자주 사용되는 프로그램 또는 명령 수행 절차 내에 숨겨진 코드를 포함시켜 잠복하고 있다가 사용자가 프로그램을 실행할 경우 원치 않는 기능을 수행한다.
- 키로거 공격(: 컴퓨터 사용자의 키보드 움직임을 탐지해 ID나 패스워드, 계좌번호, 카드번호 등과 같은 개인의 중요한 정보를 몰래 빼가는 해킹 공격이다.
- 애드웨어 : 광고를 목적으로 설치되어 사용자의 성향을 파악하여 무분별한 광고를 제공하는 프로그램이다.
- Ransomware : 랜섬웨어는 '몸값'(Ransom)과 '소프트웨어'(Software)의 합성어다. 컴퓨터 사용자의 문서를 볼모로 잡고 돈을 요구한다고 해서'랜섬(ransom)'이란 수식어가 붙었다. 인터넷 사용자의 컴퓨터에 잠입해 내부 문서나 스프레드 시트, 그림 파일 등을 제멋대로 암호화해 열지 못하도록 만들거나 첨부된 이메일 주소로 접촉해 돈을 보내 주면 해독용 열쇠 프로그램을 전송해 준다며 금품을 요구하기도 한다.

문 2. 능동적 공격에 해당하는 것만을 모두 고르면? 3

ㄱ. 도청	ㄴ. 서비스 거부
ㄷ. 트래픽 분석	ㄹ. 메시지 변조

① ㄱ, ㄷ ② ㄴ, ㄷ
③ ㄴ, ㄹ ④ ㄷ, ㄹ

[해설]

- 적극적인(Active) 공격 : 데이터에 대한 변조를 실시하거나 직접 패킷을 보내서 시스템의 무결성, 가용성, 기밀성을 공격
- 소극적인(Passive) 공격 : 데이터를 도청하거나 수집된 데이터를 분석하는 방법 등의 공격

문 3. 분산 서비스 거부(DDoS) 공격에 대한 설명으로 옳지 않은 것은? 1

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.

[해설]

① 여러개의 공격 지점에서 대규모 공격 패킷을 발생시켜서 하나의 특정 사이트를 동시에 공격하는 방법이다.
- DDoS(Distributed Denial of Service) 공격 : 공격자, 마스터 에이전트, 공격 대상으로 구성된 메커니즘을 통해 DoS 공격을 다수의 PC에서 대규모로 수행한다.

문 4. 부인방지 서비스를 제공하기 위한 전자서명에 대한 설명으로 옳지 않은 것은? 3

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.

[해설]

※ 전자 서명은 전자 문서를 작성한 사람의 신원과 전자 문서의 변경 여부를 확인 할 수 있도록 암호화 방식을 이용하여 디지털 서명키로 전자문서에 대한 작성자의 고유 정보에 서명하는 기술을 말한다.

※ 디지털 서명의 특징

(1) 위조불가 : 서명자만이 서명문을 생성할 수 있다.
(2) 부인방지 : 서명자는 서명 후에 사실을 부인할 수 없다.
(3) 재사용 불가 : 한번 서명한 서명문은 또 다른 문서에 사용할 수 없다.
(4) 변경 불가 : 내용 변경시 서명문 자체가 변경되어 변조 사실을 확인이 가능하다.
(5) 서명자 인증 : 서명자의 서명문은 서명자의 식별이 가능하다.

문 5. 다음은 IT 보안 관리를 위한 국제 표준(ISO/IEC 13335)의 위험 분석 방법에 대한 설명이다. ㉠ ~ ㉢에 들어갈 용어를 바르게 연결한 것은? 3

> (㉠)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

[해설]

- 복합 접근법(Combined Approach) : 고위험 영역을 식별하여 상세 위험 분석을 수행하고, 다른 영역은 베이스 라인을 사용하는 방식이다. 빠르고, 비용과 자원을 효과적으로 사용할 수 있지만, 잘못된 고위험 영역을 식별 시에는 낭비가 발생할 수 있다.

문 6. 다음에서 설명하는 크로스사이트 스크립팅(XSS) 공격의 유형은? 4

> 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

[해설]
- XSS(Cross Site Scripting) : 신뢰할 수 없는 외부 값을 적절한 검증 없이 웹 브라우저로 전송하는 경우 발생하는 취약점. 사용자 세션을 가로채거나 홈페이지 변조, 악의적인 사이트 이동 등의 공격 수행
- Stored XSS : 악성 Script를 서버에 직접 올려서 공격하는 방법
- Reflective XSS : 악성 Script가 저장되어 있는 페이지의 링크를 이용하는 방법

문 7. SHA 알고리즘에서 사용하는 블록 크기와 출력되는 해시의 길이를 바르게 연결한 것은? 2

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

[해설]

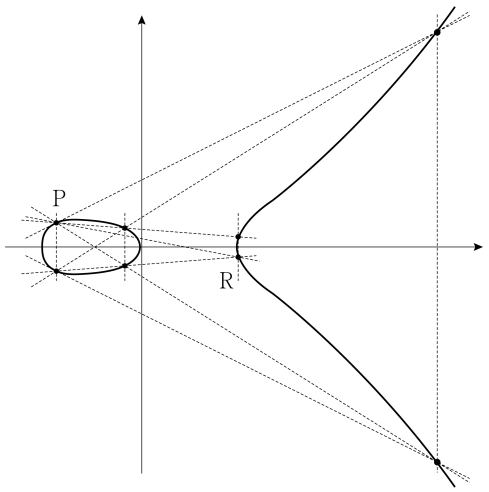
알고리즘	블록길이	해시길이	단계수
SHA-1	512	160	80
SHA-224	512	224	64
SHA-256	512	256	64
SHA-384	1024	384	80
SHA-512	1024	512	80

문 8. 데이터베이스 접근 권한 관리를 위한 DCL(Data Control Language)에 속하는 명령으로 그 설명이 옳은 것은? 2

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.

[해설]
① GRANT : 권한 부여
③ DROP : 스키마, 도메인, 테이블, 뷰, 인덱스 제거시 사용
④ DENY : 권한 거부

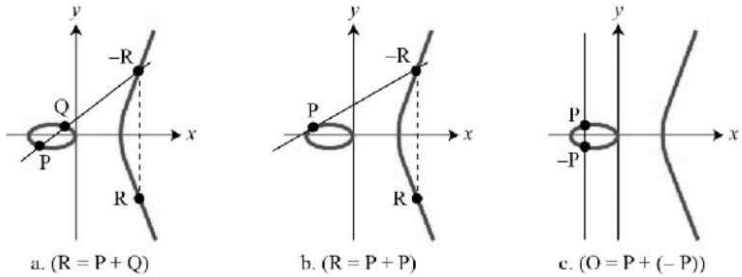
문 9. 타원곡선 암호시스템(ECC)은 타원곡선 이산대수의 어려움을 이용한다. 그림과 같이 실수 위에 정의된 타원곡선과 타원곡선상의 두 점 P 와 R이 주어진 경우, R = kP 를 만족하는 정수 k의 값은? (단, 점선은 타원곡선의 접선, 점을 연결하는 직선 또는 수직선을 나타낸다) 3



① 2 ② 3
③ 4 ④ 5

[해설]
※ 타원곡선 암호(ECC; Elliptic Curve Cryptography)
(1) 타원곡선 암호는 RSA 암호보다 짧은 키 길이로서 같은 정도의 강도를 확보하고, 암호화·복호화의 처리에 필요한 시간을 단축할 수 있다.
(2) 타원곡선상의 이산대수문제가 RSA 암호에서 사용하고 있는 소인수분해 문제보다 수학적으로 난이도가 높기 때문에 RSA 암호키 길이에서 1/6 정도로 실현할 수 있다.
(3) 타원곡선 암호가 RSA나 ElGamal과 같은 기존 공개 키 암호 방식에 비하여 갖는 가장 대표적인 장점은 보다 짧은 키를 사용하면서도 그와 비슷한 수준의 안전성을 제공한다는 것이며, 특히 무선 환경과 같이 전송량과 계산량이 상대적으로 열악한 환경에 적합하다고 할 수 있다.
(4) 타원 곡선 암호의 동작원리
① 수식공식 : 실수 위에서의 타원곡선은 a와 b가 고정된 실수일 경우에 방정식 $y^2=x^3+ax+b$ 를 만족하는 (x, y)점들의 집합이다.
② 가환군 원리 : 우변의 방정식이 중근($4a^3+27b^2\equiv 0 \pmod p$dlaus 중근 존재)을 갖지 않을 경우에, 변형된 타원 곡선 상의 점과 항등원으로 구성된 점들 사이에 적당한 덧셈 연산을 정의하면 가환군이 된다는 것을 이용한다.
- $y^2=x^3+ax+b(4a^3+27b^2\neq 0)$의 타원 x의 2점을 이용한다.
- 수식 Q=kP 에서 k와 P를 이용하여 Q를 구하는 것은 비교적 쉽지만, 알려진 Q와 P값을 통해 k값을 구하는 것은 어려운 점을 이용한다.

[타원곡선상의 3가지 덧셈]



문 10. 「개인정보 보호법」상 가명정보의 처리에 관한 특례에 대한 사항으로 옳지 않은 것은? 2

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.

[해설]

- 제28조의2(가명정보의 처리 등) ① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.
② 개인정보처리자는 제1항에 따라 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함해서는 아니 된다.[본조신설 2020. 2. 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.
② 결합을 수행한 기관 외부로 결합된 정보를 반출하려는 개인정보처리자는 가명정보 또는 제58조의2에 해당하는 정보로 처리한 뒤 전문기관의 장의 승인을 받아야 한다.
③ 제1항에 따른 결합 절차와 방법, 전문기관의 지정과 지정 취소 기준·절차, 관리·감독, 제2항에 따른 반출 및 승인 기준·절차 등 필요한 사항은 대통령령으로 정한다.[본조신설 2020. 2. 4.]

- 제28조의4(가명정보에 대한 안전조치의무 등) ① 개인정보처리자는 가명정보를 처리하는 경우에는 원래의 상태로 복원하기 위한 추가 정보를 별도로 분리하여 보관·관리하는 등 해당 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.
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.[본조신설 2020. 2. 4.]

- 제28조의5(가명정보 처리 시 금지의무 등) ① 누구든지 특정 개인을 알아보기 위한 목적으로 가명정보를 처리해서는 아니 된다.
② 개인정보처리자는 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 해당 정보의 처리를 중지하고, 지체 없이 회수·파기하여야 한다.[본조신설 2020. 2. 4.]

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? 2

① utmp ② syslog
③ history ④ pacct

[해설]

- syslog : 운영체제와 응용 프로그램의 실행 내용을 기록
- utmp : 현재 사용자의 정보를 기록
- history : 명령창에 실행했던 명령 내역
- pacct : 시스템에 로그인한 모든 사용자가 수행한 프로그램 정보

문 12. 공개키 암호시스템에 대한 설명으로 옳은 것만을 모두 고르면? 1

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

[해설]

ㄷ. 키의 분배와 관리가 대칭키 암호시스템에 비하여 용이하다.
ㄹ. 일반적으로 암호화 및 복호화 처리 속도가 대칭키 암호시스템에 비하여 느리다.

문 13. 이메일의 보안을 강화하기 위한 기술이 아닌 것은? 1

① IMAP
② S/MIME
③ PEM
④ PGP

[해설]

- IMAP(Internet Messaging Access Protocol) : 요약인터넷 메일 서버에서, 메일을 읽기 위한 인터넷 표준 통신 규약의 하나이다. 메일을 가져와서 관리하는 방식이 아닌 서버에 직접 접근하여 관리하며, 메일을 가져와도 Server에는 원본이 남아 있다.
- S/MIME, PEM, PGP은 이메일의 보안을 강화하기 위한 기술이다.

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? 4

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.

[해설]

※ 물리적 및 환경적 보안

- 보안지역 : 물리적 보안 경계, 물리적 출입 통제, 사무실/공간/시설의 보안, 외부 및 환경적 위협, 보안구역에서의 업무, 공개적 접근/인도 및 선적 지역
- 장비보안 : 장비 도입과 보호, 설비지원, 케이블 보안, 장비 유지보수, 건물 외부의 장비 보안, 장비의 안전한 처분 또는 재사용, 자산의 반출

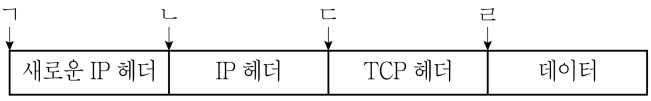
문 15. 대칭키 암호시스템에 대한 암호 분석 방법과 암호 분석가에게 필수적으로 제공되는 모든 정보를 연결한 것으로 옳지 않은 것은? 2

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

[해설]

- 기지 평문(known plaintext) 공격 : 암호 해독자는 일정량의 평문 P에 대응하는 암호문 C를 알고 있는 상태에서 해독하는 방법으로 암호문 C와 평문 P의 관계로부터 키 K나 평문 P를 추정하는 방법이다. 즉, 약간의 평문에 대응하는 암호문을 입수하고 있는 상태에서 나머지 암호문에 대한 공격을 하는 방법이다.

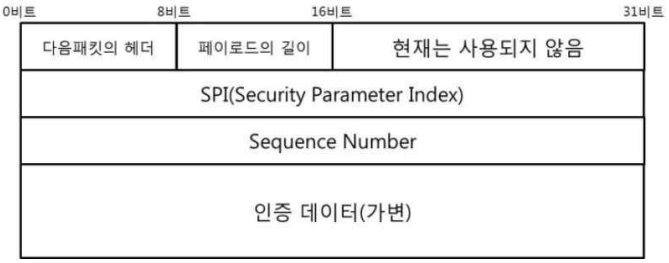
문 16. IPv4 패킷에 대하여 터널 모드의 IPSec AH(Authentication Header) 프로토콜을 적용하여 산출된 인증 헤더가 들어갈 위치로 옳은 것은? 2



① ㄱ　② ㄴ
③ ㄷ　④ ㄹ

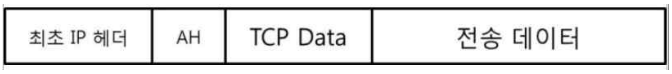
[해설]

- AH(Authentication Header) : 데이터가 전송 도중에 변조되었는지를 확인할 수 있도록 데이터의 무결성에 대해 검사하는 인증 방식



• 모드(Mode)

▌전송 모드(Transport Mode)▐



▌터널 모드(Tunnel Mode)▐

문 17. 정보보호 관련 법률과 소관 행정기관을 잘못 짝 지은 것은? 3

①「전자정부법」 – 행정안전부
②「신용정보의 이용 및 보호에 관한 법률」 – 금융위원회
③「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 – 개인정보보호위원회
④「정보통신기반 보호법」 – 과학기술정보통신부

[해설]

-「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 소관 행정기관은 과학기술정보통신부와 방송통신위원회이다.

문 18. 침입탐지시스템의 비정상(anomaly) 탐지 기법에 대한 설명으로 옳지 않은 것은? 4

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.

[해설]

※ 오용 탐지(Misuse Detection)
오용 탐지는 알려진 취약성을 통한 공격에 대한 정보를 가지고 실제적인 공격이 시도될 때 이를 탐지하는 방식이다. 비정상 행위 탐지가 침입으로 여겨지는 행위를 탐지한다면 오용 탐지는 명백한 침입을 탐지하게 된다.
- 전문가 시스템(Expert system)
- 키 모니터링(Keystroke monitoring)
- 상태 전이 분석(State transition analysis)
- 패턴 매칭(Pattern matching)

※ 비정상 행위 탐지(Anomaly Detection)
비정상 행위 탐지는 알려지지 않은 새로운 공격 기법도 탐지가 가능하다는 장점이 있지만 그에 앞서 정상적인 행위에 대한 프로파일을 구축해둬야 하기 때문에 많은 데이터의 분석이 필요하게 된다. 때문에 상대적으로 구현 비용이 큰 편이고 그만큼 어렵기 때문에 상용 제품에서는 오용 탐지를 주로 사용하고 비정상 행위 탐지는 보조하는 측면에서 사용되고 있다.
- 통계적 접근(Statistical approaches)
- 예측 가능 패턴 생성(Predictive pattern generation)
- 신경망(Neural networks)

문 19. 「전자서명법」상 과학기술정보통신부장관이 정하여 고시하는 전자서명인증업무 운영기준에 포함되어 있는 사항이 아닌 것은? 1

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

[해설]

- 제7조(전자서명인증업무 운영기준 등) ① 과학기술정보통신부장관은 전자서명의 신뢰성을 높이고 가입자 및 이용자가 합리적으로 전자서명인증서비스를 선택할 수 있도록 정보를 제공하기 위하여 필요한 조치를 마련하여야 한다.
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

- 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

문 20. 안드로이드 보안 체계에 대한 설명으로 옳지 않은 것은? 4

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.

[해설]

- 안드로이드 환경은 앱의 파일 복제가 자유롭고 마켓의 검증 과정이 철저하지 않으며, 애플리케이션에 대해 서명을 개발자가 하여 개발과 배포가 자유로운 오픈 소스 플랫폼과 오픈 마켓의 특성으로 인한 보안에 대한 본질적인 문제는 극복하기가 쉽지 않다.