2021-서울시-7급-정보보호론-해설-곽후근

1. 해시함수를 사용하여 변환 가능한 모든 해시값을 계산한 뒤, 이 정보를 사용하여 비밀번호를 공격하는 기법은?
① 무차별 대입(Brute-Force) 공격
② 퍼징(Fuzzing) 공격
③ 알려진 평문(Known Plaintext) 공격
④ 레인보우 테이블(Rainbow Table) 공격
정답 체크
(4) 패스워드의 해시값과 reduction 함수를 사용하여 패스워드를 크래킹한다.
오답 체크
(1) 가능한 모든 조합을 이용(대입)해서 공격하는 것을 의미한다.
(2) 컴퓨터 프로그램에 유효한, 예상치 않은 또는 무작위 데이터를 입력하는 것이다. 이후 프로그램은 충돌이나 잠재적인 메모리 누수 발견 등 같은 예외에 대한 감시가 이루어진다.
(3) 암호 해독자는 일정량의 평문(P)에 대응하는 암호문(C) 쌍을 이미 알고 있는 상태에서 암호문(C)과 평문(P)의 관계로부터 키(K)나 평문(P)을 추정한다.

2. 블록 암호의 운용 모드에 대한 설명으로 가장 옳은 것은?
① Electronic Codebook 모드는 초기화 벡터가 필요하다.
② Cipher Feedback 모드는 재전송 공격에 취약하다고 알려져 있다.
③ Cipher Block Chaining 모드는 복호화 과정에서도 암호화 알고리즘이 사용된다.
④ Counter 모드에서 암호문의 중간 부분을 복호화하기 위해서는 해당 부분 이전의 모든 블록들을 복호화 해야 한다.
정답 체크
(2) CFB는 재전송 공격에 취약하다.
오답 체크
(1) ECB는 초기화 벡터가 필요 없다.
(3) CBC는 복호화 과정에서 복호화 알고리즘이 사용된다.
(4) CTR은 암호문의 중간 부분을 복호화하는데 이전 블록은 필요하지 않다.

3. Single-Sign On을 실현하기에 적합한 기술로 가장 옳은 것은?
① DTLS
② TLS
③ OCSP
④ Kerberos
정답 체크
(4) Kerberos의 인증 기술을 이용하여 SSO를 실현한다.
오답 체크
(1) UDP에 TLS를 적용한 것이다(4계층 암호화).
(2) https를 실현하기에 적합한 기술이다(4계층 암호화).
(3) PKI를 실현하기에 적합한 기술이다(실시간 인증서 검증).

4. 방화벽(Firewall), 침입탐지시스템(IDS) 및 침입방지 시스템(IPS)에 대한 설명으로 가장 옳지 않은 것은?
① Shodan은 stateful inspection을 수행하는 2세대 방화벽의 일종이다.
② Snort는 대표적인 오픈소스 IPS이다.
③ IPtables는 linux의 패킷 필터 기반 방화벽의 규칙들을 관리하는 도구이다.
④ UFW는 linux에서 사용되는 방화벽 설정 툴이다.
정답 체크
(1) 쇼단은 IoT 검색 엔진이다.
오답 체크
(2) 오픈소스 IDS/IPS이다.
(3) 시스템 관리자가 리눅스 커널 방화벽이 제공하는 테이블들과 그것을 저장하는 체인, 규칙들을 구성할 수 있게 해주는 사용자 공간 응용 프로그램이다.
(4) 데비안 계열 및 다양한 리눅스 환경에서 작동되는 사용하기 쉬운 방화벽 관리 프로그램이다.

5. 〈보기〉에서 설명하는 것으로 가장 옳은 것은?

<보기>
• 공개적으로 알려진 사이버보안 취약점을 규격화된 목록으로 만들어 식별하는 체계이다.
• 목록에는 취약점의 명칭(일련 번호 포함), 취약성 및 노출 개요, 대응 참조 사항 등이 포함된다.

① Honeypot
② CVE
③ VPN
④ UTM
정답 체크
(2) CVE에서 V가 Vulnerability(취약점)를 의미한다. 이와 더불어 면접 문제에 출제된 CWE를 알아두기 바란다. 여기서, W는 Weakness(약점)를 의미한다. 약점이 큰 개념이고, 취약점이 약점 내에 포함된 개념이다.
오답 체크
(1) 크래커를 유인하는 함정을 꿀단지(곰을 유인)에 비유한 것에서 명칭이 유래한다. 마치 실제로 공격을 당하는 것처럼 보이게 하여 크래커를 추적하고 정보를 수집하는 역할을 한다. 침입자를 오래 머물게 하여 추적이 가능하므로 능동적으로 방어할 수 있고, 침입자의 공격을 차단할 수 있다. 직접적인 공격을 수행하지는 않는다.
(3) 인터넷망(public network)을 전용선(private network)처럼 사용할 수 있도록 특수 통신체계와 암호화기법을 제공하는 서비스로 기업 본사와 지사 또는 지사 간에 전용망을 설치한 것과 같은 효과를 거둘 수 있으며, 기존 사설망의 고비용 부담을 해소하기 위해 사용한다.
(4) 방화벽, 가상 전용 네트워크, 침입 차단 시스템, 웹 컨텐츠 필터링, 안티스팸 소프트웨어 등을 포함하는 여러 개의 보안 도구를 이용한 관리 시스템이다.

6. RSA에서 모듈로 연산에 사용되는 n=91이고 어떤 사용자의 비밀키에 사용되는 d=7이라고 할 때, 이 사용자의 공개키에 사용되는 e로 가장 옳은 것은?

① 13
② 31
③ 41
④ 존재하지 않는다.
정답 체크
(2) n을 소인수분해하면 13과 7로 분해된다.
오일러 피 함수를 구한다. ϕ = 12 x 6 = 72
e x 7 mod 72 = 1이 되는 e를 구하면 31이 된다.

7. IPSec에 대한 설명으로 가장 옳지 않은 것은?
① IPSec은 전송모드와 터널모드로 동작할 수 있다.
② IPSec은 데이터 송신자에 대한 인증과 재전송(Replay) 공격 방지 기능을 제공할 수 있다.
③ IPSec의 키 관리 프로토콜에서는 Diffie-Hellman 기법을 개선한 Oakley 기법을 사용하여 키 교환을 수행할 수 있다.
④ IPSec은 전송 계층인 TCP 계층의 상위 계층인 세션 계층 암호화 기법이므로, 응용 프로그램에 대한 투명성 (transparency)을 갖는다.
정답 체크
(4) 네트워크 계층 암호화 기법이다.
오답 체크
(1) 전송모드와 터널모드가 존재한다(전기터새).
(2) AH(인증, 무결성, 재전송 방지)와 ESP(인증, 무결성, 기밀성, 재전송 방지)를 제공한다.
(3) 일련의 키 교환 메커니즘들을 기반으로 한다(Diffie-Hellman 키 교환 방법을 기반으로 한다).
(IKE = ISAKMP + OAKLEY + SKEME)

8. 포맷 스트링(format string) 공격에 대한 설명으로 가장 옳지 않은 것은?
① 취약한 함수를 이용한다는 점에서 버퍼 오버플로우와 공통점이 있으나, 버퍼 오버플로우 공격이 알려지기 훨씬 이전에 발견되었다.
② C 언어의 printf 함수가 대표적인 공격 대상이다.
③ %x 토큰을 적절히 활용하면 공격자는 메모리 내용을 출력하여 확인할 수 있다.
④ %n 토큰을 적절히 활용하면 공격자는 메모리의 내용을 변경할 수 있다.
정답 체크
(1) 버퍼 오버플로우 공격이 먼저 발견되었다.
오답 체크
(2) printf의 포맷 스트링을 대상으로 한다.
(3) %x를 활용한다(메모리 내용 출력).
(4) %n, %hn을 활용한다(메모리 내용 변경).

9. AES에 대한 설명으로 가장 옳은 것은?
① AES-192는 한 번의 수행으로 192비트의 평문 블록을 암호화한다.
② Daemen과 Rijmen이 설계한 Rijndael 알고리즘에 기반한다.
③ 유한체 GF(2^{256}) 상의 연산을 이용하여 설계되었다.

④ 치환(substitution) 및 전치(permutation) 연산을 반복하는 페이스텔(Feistel) 구조를 사용한다.
정답 체크
(2) 5개의 최종 후보 중 Rijndael(라인델) 알고리즘에 기반한다.
오답 체크
(1) 128비트 블록을 암호화한다.
(3) GF(2^8) 상의 연산을 이용한다.
(4) SPN 구조를 사용한다.

10. 〈보기〉의 설명에 맞는 접근 제어 모델로 가장 옳은 것은?

<보기>
• 정보 소유자가 정보의 보안 수준을 결정하고 이에 대한 접근 권한도 설정할 수 있는 모델이다.
• 이 모델의 대표적인 사례로는 Linux 및 Windows 운영 체제에서 파일 시스템 접근 권한을 설정하는 방법이 있다.

① 임의적 접근 제어(Discretionary Access Control) 모델
② 강제적 접근 제어(Mandatory Access Control) 모델
③ 역할기반 접근 제어(Role-Based Access Control) 모델
④ 벨-라파둘라(Bell-LaPadula) 모델
정답 체크
(1) 객체에 대한 소유권(ownership)에 기초해서 소유권을 가진 주체가 객체에 대한 권한의 전부 혹은 일부를 다른 주체에게 부여한다. 유닉스 혹은 관계형 데이터베이스(RDBMS)에서 사용한다.
오답 체크
(2) 주체와 객체에 적절한 보안 등급(레이블)을 부여하고, 접근 제어시 이 등급을 비교함으로써 접근의 허용 여부를 판단하게 된다. 군사 환경과 같은 엄격한 보안이 요구되는 분야에 적합하다.
(3) 기업 환경에서는 사용자가 기업 내에서 어떤 역할(Role)을 수행하고 있는가에 따라 권한이 정해진다. 이를 모델화한 것이 역할 기반 접근 제어이다.
(4) 미 국방부 지원 보안 모델로 보안 요소 중 기밀성 강조한다. 최초의 수학적 모델로 강제적 정책에 의해 접근 통제하는 모델이다. 보안 정책은 정보가 높은 레벨에서 낮은 레벨로 흐르는 것을 방지한다. BLP의 속성은 No Read Up(보안 수준이 낮은 주체는 보안 수준이 높은 객체를 읽어서는 안되는 정책), No Write Down(보안 수준이 높은 주체는 보안 수준이 낮은 객체에 기록해서는 안됨)이다.

11. DoS공격에 대한 설명으로 가장 옳지 않은 것은?
① HTTP GET Flooding 공격: TCP 3-Way 핸드셰이킹 과정을 통해 공격 대상 시스템에 정상적으로 접속한 뒤 HTTP의 GET Method로 특정 페이지를 무한 실행 한다.
② 동적 HTTP Request Flooding 공격: 요청 페이지를 변경하여 웹 페이지를 지속적으로 요청한다.
③ Slow HTTP Header DoS(Slowloris) 공격: 웹 서버에 ID 및 Password, 게시글, 첨부 파일 등을 전송할 때 사용하는 HTTP POST 메시지에서 헤더의 Content-Length 필드에 임의의 큰 값을 설정하여 전송한다.

④ Mail Bomb: 각 사용자에게 할당된 디스크 공간 이상의 메일을 보내 더 이상 메일을 받을 수 없게 하는 공격이다.
정답 체크
(3) 해당 설명은 slow HTTP Post DoS 공격이고, Slow HTTP Header DoS 공격은 HTTP Header 정보를 비정상적으로 조작하여 웹서버가 온전한 Header정보가 올 때까지 기다리도록 한다.
오답 체크
(1) 서버에 TCP 3-웨이 핸드셰이킹 과정을 통해 정상적인 접속을 한 뒤, 특정한 페이지를 HTTP의 GET Method를 통해 무한대로 실행하는 것이다.
(2) 웹 방화벽을 통해 특징적인 HTTP 요청 패턴 차단 기법을 우회하기 위해 지속적으로 요청 페이지를 변경하여 웹 페이지를 요청하는 기법이다.
(4) 흔히 폭탄 메일이라고 하고 스팸 메일도 여기에 해당한다. 메일 서버는 각 사용자에게 일정한 양의 디스크 공간을 할당하는데, 메일이 폭주하여 디스크 공간을 가득 채우면 정작 받아야 하는 메일을 받을 수 없다. 즉 스팸 메일도 서비스 거부 공격이 될 수 있다.

12. ElGamal 등과 같이 이산 대수 문제를 기반으로 하는 암호화 기법에서 비밀키로 공개키를 계산할 때 원시근이 사용된다. 사용되는 소수가 13일 때, 원시근으로 사용될 수 있는 값은?
① 6
② 8
③ 10
④ 12
정답 체크
(1) 13의 원시근은 2, 6, 7, 11이다.
계산을 빨리 하기 위해 $6^6 \bmod 13 = 6^3 \times 6^3 \bmod 13$과 같이 계산한다.

13. SSL/TLS에서 레코드 프로토콜의 동작단계로 가장 옳은 것은?
① 압축 → 암호화 → MAC 추가 → 단편화
② 압축 → MAC 추가 → 암호화 → 단편화
③ 암호화 → 단편화 → 압축 → MAC 추가
④ 단편화 → 압축 → MAC 추가 → 암호화
정답 체크
(4) 동작 단계는 단편화 → 압축(zip) → MAC 추가 → 암호화 순이다.

14. 해시 함수에 대한 설명으로 가장 옳지 않은 것은?
① 160비트 길이의 해시 출력값을 갖는 SHA-1 해시 함수는 안전하지 않다고 알려져 있다.
② 키를 갖는 해시함수(Keyed Hash Function)는 메시지 인증 목적으로 사용될 수 있다.
③ 안전한 해시함수는 특정 해시값 h=H(x)를 갖는 x를 찾는 것이 어렵다는 충돌 회피성(collision resistance)을 가져야 한다.
④ NIST에서는 기존의 SHA-2와 원천적으로 다른 구조를 갖는 SHA-3(Keccak)를 표준화하였다.
정답 체크
(3) 해당 설명은 일방향성이고, 충돌 회피성은 약한 충돌(해시값이 주어졌을 때, 다른 메시지를 찾는 것)과 강한 충돌(해시값이 일치할 것 같은 2개의 메시지를 찾는 것)이 존재한다.

오답 체크
(1) 강한 충돌 내성이 침해되었다.
(2) HMAC을 의미한다.
(4) 기존 구조는 MD 구조이고, SHA-3은 스펀지 구조이다.

15. 디지털 서명에 대한 설명으로 가장 옳은 것은?
① 디지털 서명 기법에서 서명의 크기는 원본 데이터의 크기에 비례한다.
② RSA를 사용하는 경우 공개키로 서명하고 개인키로 서명을 검증한다.
③ X.509 인증서에는 공개키를 인증하기 위한 인증 기관의 서명이 포함되어 있다.
④ 서명 과정에서 메시지에 해시함수를 적용하면 원본으로 복구가 불가능하므로, 해시함수는 서명에 사용하지 않는 것이 좋다.
정답 체크
(3) 공개키에 인증기관의 개인키로 서명한다.
오답 체크
(1) 서명의 시간이 원본 데이터의 크기에 비례하고, 서명의 크기는 일정하다.
(2) 개인키로 서명하고 공개키로 검증한다.
(4) 서명 시간을 단축하기 위해 해시 함수를 사용한다.

16. DB 접근통제 방식 중 〈보기〉에서 설명하는 것은?

<보기>
네트워크 선로 상의 패킷들을 TAP 방식과 패킷 미러링 방식을 통해 분석 로깅하는 방식으로 사후 감사의 의미에 비중을 두는 보안 방식이다.

① 에이전트 방식
② 프록시 방식
③ 인라인 방식
④ 스니핑 방식
정답 체크
(4) 서버와 클라이언트 사이에 어떠한 에이전트의 설치나 설정변경이 필요 없으며 네트워크 부하 없이 시스템 구축 용이하다.
오답 체크
(1), (2), (3) DB 접근통제 방식을 정리하면 다음과 같다.

접근제어 방법		특성
스니핑 방식		• 네트워크 선로상의 패킷들을 TAP 방식과 패킷 미러링 방식을 통해 패킷을 분석 및 로깅하는 방법으로 사후 감사의 의미에 비중을 두는 보안 방식 • 서버와 클라이언트 사이에 어떠한 에이전트의 설치나 설정변경이 필요없으며 네트워크 부하 없이 시스템 구축 용이 • 데이터의 변조나 훼손으로 인한 무결성 유지 곤란
에이전트 방법		• 서버 자체에 접근제어 및 로깅 기능을 포함하는 에이전트 이식 • DB에 직접 접근하는 전용 클라이언트를 포함해 모든 접근 루트를 제어할 수 있는 가장 강력한 보안 방법 • DB 서버에 트래픽을 발생, DB 서버의 성능저하 우려, 시스템 정지의 리스크 내재
게이트웨이 방법	프록시 방법	• DB 서버로 접속하는 모든 IP를 DB 보안 서버(프록시 서버)를 통하도록 설정 변경 • 가장 강력한 접근제어 기능 제공 • 타깃 DBMS의 추가가 가능해 대형 시스템 환경에 유리 • 보안 서버(프록시 서버)의 장애 발생 시에도 이중화 구성이 가능하므로 온라인 업무에 지장 없이 복구 가능
	인라인 방법	• 타깃 DB 서버와 클라이언트 네트워크 사이에 인라인 보안시스템 구성 • 서버나 클라이언트에 별도의 에이전트 설치나 설정 변경 불필요 • 규모가 크지 않고 DB 서버가 한 장소에 위치하고 온라인 업무의 비중이 그다지 높지 않은 시스템에 유리 • 보안 서버 다운 시 모든 업무의 중단 우려가 있으며 타깃 DB 서버의 규모에 따라 다수의 DB 보안서버 필요. (현재는 Bypass 기능이 존재)

17. FTP 서버를 안전하게 운영하기 위한 방법으로 가장 옳은 것은?
① 파일과 사용자에 대한 보안을 위하여 익명(anonymous) FTP로 설정한다.
② 사용자가 본인의 홈디렉터리보다 상위 디렉터리에 접근할 수 있도록 설정한다.
③ 파일 내용이 인가되지 않은 방법으로 수정되지 않도록 Everyone 계정을 제거해야 한다.
④ 출장이나 재택근무 등을 대비하여 모든 IP주소 대역 에서 접근할 수 있도록 한다.
정답 체크
(3) Everyone 계정을 제거한다.
오답 체크
(1) 보안을 위해 익명 계정을 제거한다.
(2) 상위 디렉토리에 접근할 수 없어야 한다.
(4) 모든 IP 대역에서 접근할 수 없어야 한다.

18. 소프트웨어 보안 약점 유형에 대한 설명으로 가장 옳은 것은?
① 코드 오류: 의도하지 않은 방법으로 API를 사용하거나, 보안에 취약한 API를 사용하여 발생할 수 있는 보안 약점(예: DNS lookup에 의존한 보안결정)
② 에러 처리: 프로그램 입력 값에 대한 검증 누락 또는 부적절한 검증, 데이터의 잘못된 형식지정으로 인해 발생할 수 있는 보안 약점(예: SQL 삽입, XQuery 삽입, LDAP 삽입 등)
③ 시간 및 상태: 중요한 데이터 또는 기능성을 불충분하게 캡슐화하였을 때, 인가되지 않은 사용자에게 데이터 누출이 가능해지는 보안 약점(예: 잘못된 세션에 의한 데이터 또는 시스템 데이터 정보 노출 등)
④ 보안 기능: 인증, 접근제어, 암호화 등의 기능을 부적절 하게 구현 시 발생할 수 있는 보안 약점

(예: 부적절한 인가, 하드코드된 암호화키 등)
정답 체크
(4) 취약한 암호화 알고리즘 사용, 충분하지 않은 키 길이 사용 등도 포함된다.
오답 체크
(1) API 오용을 의미한다.
(2) 입력데이터 검증 및 표현을 의미한다.
(3) 캡슐화를 의미한다.
Tip! 소프트웨어 보안 약점 유형을 정리하면 다음과 같다(강의 내용).

유형	설명	취약점
1. 입력데이터 검증 및 표현	프로그램 입력 값에 대한 검증 누락 또는 부적절한 검증, 데이터의 잘못된 형식지정으로 인해 발생할 수 있는 보안 약점	• SQL 삽입 • 경로 조작 및 자원 삽입 • 크로스사이트 스크립트 • 운영체제 명령어 삽입 • 위험한 형식 파일 업로드 • 신뢰되지 않는 URL 주소로 자동접속 연결 • XQuery 삽입 • XPath 삽입 • LDAP 삽입 • 크로스사이트 요청 위조 • HTTP 응답분할 • 정수형 오버플로우 • 보안기능 결정에 사용되는 부적절한 입력 값 • 메모리 버퍼 오버플로우 • 포맷 스트링 삽입

유형	설명	취약점
2. 보안 기능	보안기능(인증, 접근제어, 기밀성, 암호화, 권한 관리 등)을 부적절하게 구현 시 발생할 수 있는 보안 약점	• 적절한 인증 없는 중요기능 허용 • 부적절한 인가 • 중요한 자원에 대한 잘못된 권한 설정 • 취약한 암호화 알고리즘 사용 • 중요정보 평문저장 • 중요정보 평문전송 • 하드코드된 비밀번호 • 충분하지 않은 키 길이 사용 • 적절하지 않은 난수 값 사용 • 하드코드된 암호화키 • 취약한 비밀번호 허용 • 사용자 하드디스크에 저장되는 쿠키를 통한 정보 노출 • 주석문 안에 포함된 시스템 주요정보 • 솔트 없이 일방향 해시 함수 사용 • 무결성 검사 없는 코드 다운로드 • 반복된 인증시도 제한 기능 부재
3. 시간 및 상태	동시 또는 거의 동시 수행을 지원하는 병렬 시스템, 하나 이상의 프로세스가 동작 되는 환경에서 시간 및 상태를 부적절하게 관리하여 발생할 수 있는 보안 약점	• 경쟁조건: 검사 시점과 사용 시점(TOCTOU) • 종료되지 않는 반복문 또는 재귀 함수
4. 에러 처리	에러를 처리하지 않거나, 불충분하게 처리하여 에러정보에 중요정보(시스템 등)가 포함될 때 발생할 수 있는 보안 약점	• 오류 메시지를 통한 정보 노출 • 오류 상황 대응 부재 • 부적절한 예외 처리
5. 코드 오류	타입 변환 오류, 자원(메모리 등)의 부적절한 반환 등과 같이 개발자가 범할 수 있는 코딩 오류로 인해 유발되는 보안 약점	• Null Pointer 역 참조 • 부적절한 자원 해제 • 해제된 자원 사용 • 초기화되지 않은 변수 사용
6. 캡슐화	중요한 데이터 또는 기능성을 불충분하게 캡슐화하였을 때, 인가되지 않은 사용자에게 데이터 누출이 가능해지는 보안 약점	• 잘못된 세션에 의한 데이터 정보 노출 • 제거되지 않고 남은 디버그 코드 • 시스템 데이터 정보노출 • Public 메소드로부터 반환된 Private 배열 • Private 배열에 Public 데이터 할당
7. API 오용	의도된 사용에 반하는 방법으로 API를 사용하거나, 보안에 취약한 API를 사용하여 발생할 수 있는 보안 약점	• DNS lookup에 의존한 보안결정 • 취약한 API 사용

19. 〈보기〉의 「 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시 」 제2조 발췌문에서 (가)에 들어갈 기관은?

<보기>

“ 정보보호 및 개인정보보호 관리체계 인증 ”이란 인증 신청인의 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 (가) 또는 인증기관이 증명하는 것을 말한다.

① 국가정보원
② 한국인터넷진흥원
③ 개인정보 보호위원회
④ 과학기술정보통신부
정답 체크
(2) 제2조(용어의 정의) 2. "정보보호 관리체계 인증"이란 인증 신청인의 정보보호 관련 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 것을 말한다.

20.「 정보통신망 이용촉진 및 정보보호 등에 관한 법률 」에 대한 설명으로 가장 옳지 않은 것은?
① 정보통신서비스 제공자는 해당 서비스를 제공하기 위하여 이용자의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 대하여 접근할 수 있는 권한(이하 “ 접근권한 ”이라 한다)이 필요한 경우, 이 접근권한이 해당 서비스를 제공하기 위하여 반드시 필요한 접근권한이 아닌 경우에는 접근권한 허용에 대하여 동의하지 아니할 수 있다는 사실을 이용자에게 알리고 이용자의 동의를 받아야 한다.
② 정보통신서비스 제공자는 해당 서비스를 제공하기 위하여 이용자의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 대하여 접근할 수 있는 권한(이하 “ 접근권한 ”이라 한다)이 필요한 경우, 이 접근권한이 해당 서비스를 제공하기 위하여 반드시 필요한 접근권한인 경우에도 접근권한이 필요한 이유를 이용자에게 알리고 이용자의 동의를 받아야 한다.
③ 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 임원급의 정보 보호 최고책임자를 지정하고 과학기술정보통신부 장관에게 신고하여야 한다. 다만, 자산총액, 매출액 등이「 전자상거래 등에서의 소비자보호에 관한 법률 」로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 지정하지 아니할 수 있다.
④ 과학기술정보통신부장관은 침해사고에 적절히 대응하기 위하여 침해사고에 대한 긴급조치를 수행할 수 있다.
정답 체크
(3) 제45조의3(정보보호 최고책임자의 지정 등) ① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 임원급의 정보보호 최고책임자를 지정하고 과학기술정보통신부장관에게 신고하여야 한다. 다만, 자산총액, 매출액 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 지정하지 아니할 수 있다.
오답 체크
(1), (2) 제22조의2(접근권한에 대한 동의) ① 정보통신서비스 제공자는 해당 서비스를 제공하기 위하여 이용자의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 대하여 접근할 수 있는 권한(이하 “접근권한”이라 한다)이 필요한 경우 다음 각 호의 사항을 이용자가 명확하게 인지할 수 있도록 알리고 이용자의 동의를 받아야 한다.
1. 해당 서비스를 제공하기 위하여 반드시 필요한 접근권한인 경우
가. 접근권한이 필요한 정보 및 기능의 항목
나. 접근권한이 필요한 이유
2. 해당 서비스를 제공하기 위하여 반드시 필요한 접근권한이 아닌 경우

가. 접근권한이 필요한 정보 및 기능의 항목
나. 접근권한이 필요한 이유
다. 접근권한 허용에 대하여 동의하지 아니할 수 있다는 사실
(4) 제48조의2(침해사고의 대응 등) ① 과학기술정보통신부장관은 침해사고에 적절히 대응하기 위하여 다음 각 호의 업무를 수행하고, 필요하면 업무의 전부 또는 일부를 한국인터넷진흥원이 수행하도록 할 수 있다.
1. 침해사고에 관한 정보의 수집·전파
2. 침해사고의 예보·경보
3. 침해사고에 대한 긴급조치
4. 그 밖에 대통령령으로 정하는 침해사고 대응조치