

정보보호론

문 1. 응용 계층 프로토콜에서 동작하는 서비스에 대한 설명으로 옳지 않은 것은?

- ① FTP: 파일전송 서비스를 제공한다.
- ② DNS: 도메인 이름과 IP 주소 간 변환 서비스를 제공한다.
- ③ POP3: 메일 서버로 전송된 메일을 확인하는 서비스를 제공한다.
- ④ SNMP: 메일전송 서비스를 제공한다.

문 2. 「개인정보 보호법」상 용어 정의로 옳지 않은 것은?

- ① 개인정보: 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)
- ② 정보주체: 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인
- ③ 처리: 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위
- ④ 개인정보파일: 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물

문 3. 다음 설명에 해당하는 OECD 개인정보보호 8원칙으로 옳은 것은?

개인정보는 이용 목적상 필요한 범위 내에서 개인정보의 정확성, 완전성, 최신성이 확보되어야 한다.

- ① 이용 제한의 원칙(Use Limitation Principle)
- ② 정보 정확성의 원칙(Data Quality Principle)
- ③ 안전성 확보의 원칙(Security Safeguards Principle)
- ④ 목적 명시 원칙(Purpose Specification Principle)

문 4. 현행 우리나라의 정보보호관리체계(ISMS) 인증에 대한 설명으로 옳지 않은 것은?

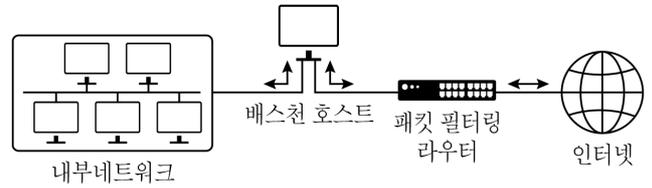
- ① 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 근거를 두고 있다.
- ② 인증심사의 종류에는 최초심사, 사후심사, 갱신심사가 있다.
- ③ 인증에 유효기간은 정해져 있지 않다.
- ④ 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하고 있는 자에 대하여 인증 기준에 적합한지에 관하여 인증을 부여하는 제도이다.

문 5. 보안 서비스에 대한 설명을 바르게 나열한 것은?

ㄱ. 메시지가 중간에서 복제·추가·수정되거나 순서가 바뀌거나 재전송됨이 없이 그대로 전송되는 것을 보장한다.
 ㄴ. 비인가된 접근으로부터 데이터를 보호하고 인가된 해당 개체에 적합한 접근 권한을 부여한다.
 ㄷ. 송·수신자 간에 전송된 메시지에 대해서, 송신자는 메시지 송신 사실을, 수신자는 메시지 수신 사실을 부인하지 못하도록 한다.

- | | | |
|-----------|------|------|
| ㄱ | ㄴ | ㄷ |
| ① 데이터 무결성 | 부인봉쇄 | 인증 |
| ② 데이터 가용성 | 접근통제 | 인증 |
| ③ 데이터 기밀성 | 인증 | 부인봉쇄 |
| ④ 데이터 무결성 | 접근통제 | 부인봉쇄 |

문 6. 다음에 해당하는 방화벽의 구축 형태로 옳은 것은?



- 인터넷에서 내부네트워크로 전송되는 패킷을 패킷 필터링 라우터에서 필터링함으로써 1차 방어를 수행한다.
- 패스천 호스트에서는 필터링 된 패킷을 프록시와 같은 서비스를 통해 2차 방어 후 내부네트워크로 전달한다.

- ① 응용 레벨 게이트웨이(Application-level gateway)
- ② 회로 레벨 게이트웨이(Circuit-level gateway)
- ③ 듀얼 홈드 게이트웨이(Dual-homed gateway)
- ④ 스크린 호스트 게이트웨이(Screened host gateway)

문 7. SSH(Secure SHell)를 구성하고 있는 프로토콜 스택으로 옳지 않은 것은?

- ① SSH User Authentication Protocol
- ② SSH Session Layer Protocol
- ③ SSH Connection Protocol
- ④ SSH Transport Layer Protocol

문 8. 위험분석 방법에 대한 설명을 바르게 나열한 것은?

ㄱ. 시스템에 관한 전문적인 지식을 가진 전문가 집단을 구성하고 토론을 통해 정보시스템이 직면한 다양한 위협과 취약성을 분석하는 방법이다.
 ㄴ. 자산의 가치 분석, 위협 분석, 취약점 분석을 수행하여 위험을 분석하는 방법이다.
 ㄷ. 표준화된 보호대책의 세트를 체크리스트 형태로 구현하여 이를 기반으로 보호대책을 식별하는 방법이다.

- | | | |
|---------|--------------|--------------|
| ㄱ | ㄴ | ㄷ |
| ① 시나리오법 | 기준선 접근법 | 상세 위험 분석 접근법 |
| ② 시나리오법 | 상세 위험 분석 접근법 | 기준선 접근법 |
| ③ 델파이법 | 기준선 접근법 | 상세 위험 분석 접근법 |
| ④ 델파이법 | 상세 위험 분석 접근법 | 기준선 접근법 |

문 9. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 개인정보 취급방침에 포함되어야 할 사항이 아닌 것은?

- ① 이용자 및 법정대리인의 권리와 그 행사 방법
- ② 개인정보에 대한 내부 관리 계획
- ③ 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항
- ④ 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목 및 수집 방법

문 10. 전자서명 방식에 대한 설명으로 옳지 않은 것은?

- ① 은닉 서명(blind signature)은 서명자가 특정 검증자를 지정하여 서명하고, 이 검증자만이 서명을 확인할 수 있는 방식이다.
- ② 부인방지 서명(undeniable signature)은 서명을 검증할 때 반드시 서명자의 도움이 있어야 검증이 가능한 방식이다.
- ③ 위임 서명(proxy signature)은 위임 서명자로 하여금 서명자를 대신해서 대리로 서명할 수 있도록 한 방식이다.
- ④ 다중 서명(multisignature)은 동일한 전자문서에 여러 사람이 서명하는 방식이다.

