

【정보보안관리 및 법규】

1. 정보보호 및 개인정보보호 관리체계(ISMS-P)에 대한 설명으로 가장 적절하지 않은 것은?

- ① ISMS-P 인증심사 종류에는 ‘최초심사’, ‘사후심사’, ‘갱신심사’가 있으며, 최초심사를 통해 인증을 취득하면 3년의 유효기간이 부여된다.
- ② 인증 의무대상자는 ISMS 인증을 받아야 하며, ISMS-P 인증을 받은 경우에도 인증의무를 이행한 것으로 본다.
- ③ 인증기관인 한국인터넷진흥원(KISA)은 금융 분야 인증위원회를 구성 및 운영하고, 인증심사 및 인증서 발급 업무를 수행한다.
- ④ 사후심사는 인증발급일 기준으로 매 1년 이전에 심사를 완료해야 하며, 인증유효기간 내 심사를 받지 않을 경우 인증이 취소된다.

2. 기술적 보호대책에 해당하는 내용으로 가장 적절한 것은?

- ① 정보시스템, 통신망, 정보를 보호하기 위한 가장 기본적인 대책
- ② 자연재해 및 권한이 없는 외부인에 의한 파괴 등으로부터 정보 시스템을 보호하기 위한 대책
- ③ 법률, 규정, 제도, 교육 등을 통한 보안계획 수립 및 운용 대책
- ④ 위험분석 및 보안감사를 통한 정보시스템의 신뢰성 확보 대책

3. 다음 국제 공통 평가기준(CC: Common Criteria)에 해당하는 EAL(Evaluation Assurance Level) 등급으로 가장 적절한 것은?

- TOE(Target of Evaluation) 명세서에 기반한 독립적인 시험 요구
- 구조적 시험(Structurally Tested)
- 낮은 수준에서 중간 수준의 보안이 필요할 경우 실시

- ① EAL1 ② EAL2 ③ EAL3 ④ EAL4

4. 정보보호 통제의 종류와 설명에 대하여 <보기 1>과 <보기 2>를 가장 적절하게 연결한 것은?

<보기 1>

- (가) 행위에 의한 통제
- (나) 보안 목표에 의한 통제
- (다) 기능에 의한 통제

<보기 2>

- ㉠ 예방적 통제, 탐지적 통제, 수정적 통제
- ㉡ 무결성 통제, 기밀성 통제, 가용성 통제
- ㉢ 관리적 통제, 기술적 통제, 운영적 통제

- | | (가) | (나) | (다) |
|---|-----|-----|-----|
| ① | ㉠ | ㉡ | ㉢ |
| ② | ㉢ | ㉡ | ㉠ |
| ③ | ㉡ | ㉠ | ㉢ |
| ④ | ㉡ | ㉠ | ㉢ |

5. 다음에서 설명하는 재해복구 시스템의 유형으로 가장 적절한 것은?

- 재해복구센터에 주 센터와 동일 수준의 시스템을 대기상태(Stand-by)로 유지
- 동기적 또는 비동기적 방식의 실시간 복제를 통하여 최신 데이터 상태 유지
- 재해 발생 시 재해복구센터의 시스템을 액티브(Active)로 전환하여 복구
- RTO(Recovery Time Objective): 수시간 이내
- 데이터의 업데이트가 많은 경우에 적합

- ① 미러 사이트(Mirror Site) ② 핫 사이트(Hot Site)
- ③ 웜 사이트(Warm Site) ④ 콜드 사이트(Cold Site)

6. 다음에서 설명하는 내용으로 가장 적절한 것은?

- 사용자에게 자신의 패스워드를 관리할 수 있는 기능을 제공한다.
- 시스템 및 각종 자원에 대하여 접근제어를 할 수 있다.
- 사용자에게 따라 권한을 차등적으로 부여할 수 있다.
- 역할 기반의 사용자 계정 솔루션이다.

- ① LBS(Location Based System)
- ② IAM(Identity and Access Management)
- ③ MPLS(Multi Protocol Label Switching)
- ④ DS(Differentiated Services)

7. <보기 1>의 위험분석 방법론 중 <보기 2>의 설명과 가장 적절하게 연결한 것은?

<보기 1>

- (가) 기준선 접근법(Baseline Approach)
- (나) 비정형화된 접근법(Informal Approach)
- (다) 상세 위험 분석 접근법(Detailed Risk Analysis Approach)
- (라) 복합 접근법(Combined Approach)

<보기 2>

㉠	· 고위험 영역을 빠르게 식별하고 처리 · 영역의 구분이 잘못 수행되었을 때, 위험분석 비용이 낭비되거나 부적절한 대응책이 선택될 수 있음
㉡	· 비용 대비 효과가 우수하며 소규모 조직에 적합 · 작은 규모의 조직에는 적합하나, 새롭거나 경험이 적은 위험 영역을 간과할 가능성이 있음
㉢	· 자산가치, 위협, 취약점의 평가에 기초한 위험을 산정하므로 경영상 허용수준까지 위험을 줄이는 근거가 명확 · 조직의 자산 및 보안 요구사항을 구체적으로 분석하여 가장 적절한 대책 수립
㉣	· 비용 및 시간 절약 · 모든 시스템에 대해 표준화된 보호 대책의 세트를 체크리스트 형태로 제공

- | | (가) | (나) | (다) | (라) |
|---|-----|-----|-----|-----|
| ① | ㉠ | ㉢ | ㉡ | ㉣ |
| ② | ㉠ | ㉣ | ㉡ | ㉢ |
| ③ | ㉡ | ㉠ | ㉢ | ㉣ |
| ④ | ㉡ | ㉡ | ㉢ | ㉠ |

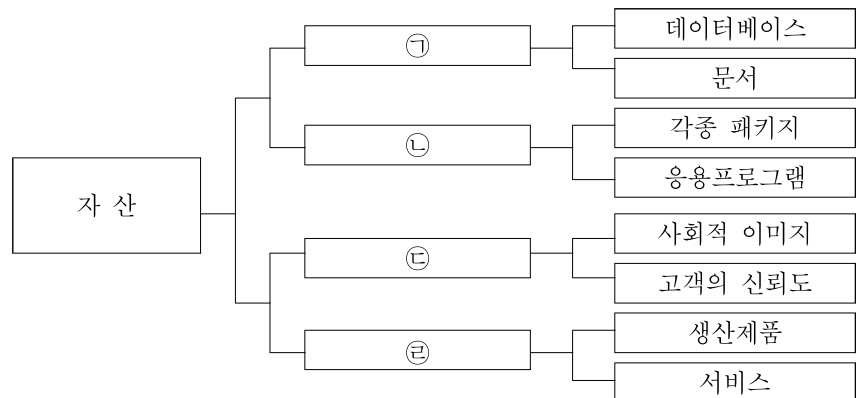
8. TCSEC(Trusted Computer System Evaluation Criteria)와 ITSEC(Information Technology Security Evaluation Criteria)의 설명으로 가장 적절하지 않은 것은?

- ① 기능성과 보증성 측면에서 ITSEC은 분리하여 평가하는 반면, TCSEC은 묶어서 평가한다.
- ② TCSEC은 ITSEC보다 나은 유연성을 제공하고, ITSEC은 기밀성에 대처하는 반면에 TCSEC은 무결성, 가용성, 기밀성에 모두 대처한다.
- ③ ITSEC은 유럽 국가들이 평가제품의 상호인정 및 평가기준이 상이함에 따른 불합리함을 보완하기 위하여 작성한 유럽형 보안기준이다.
- ④ TCSEC은 D~A1(D, C1, C2, B1, B2, B3, A1)까지 총 7개의 세부 보안등급이 있다.

9. 클라우드서비스 보안인증제에 대한 설명으로 가장 적절하지 않은 것은?

- ① IaaS, SaaS 표준등급, SaaS 간편등급, DaaS의 인증종류를 가진다.
- ② 서버 가상화 기술은 SaaS의 기술 중 하나이다.
- ③ 중요한 데이터를 다루는 SaaS 서비스는 표준등급을 받아야 한다.
- ④ DaaS 서비스는 필수 보안 요건을 만족하여야 하며, 보안장비 등의 영역에서 구성되어야 한다.

10. 자산의 종류 중 ㉠~㉣에 들어갈 내용으로 가장 적절한 것은?



- | ㉠ | ㉡ | ㉢ | ㉣ |
|------------|----------|-------|-------|
| ① 소프트웨어 자산 | 정보 자산 | 상품 자산 | 무형 자산 |
| ② 정보 자산 | 소프트웨어 자산 | 상품 자산 | 무형 자산 |
| ③ 소프트웨어 자산 | 정보 자산 | 무형 자산 | 상품 자산 |
| ④ 정보 자산 | 소프트웨어 자산 | 무형 자산 | 상품 자산 |

11. 「개인정보 보호법」상 정보주체가 자신의 개인정보 처리와 관련하여 가질 수 있는 권리로 가장 적절하지 않은 것은?
- ① 개인정보의 처리에 관한 정보를 제공받을 권리
 - ② 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리
 - ③ 개인정보의 처리 여부를 확인하고 이를 저장한 시스템의 정보를 요구할 권리
 - ④ 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리
12. 「개인정보 보호법」상 개인정보 분쟁조정위원회의 설치 및 구성에 대한 설명으로 가장 적절하지 않은 것은?
- ① 분쟁조정위원회는 위원장 1명을 포함한 20명 이내의 위원으로 구성하며, 위원은 당연직위원과 위촉위원으로 구성한다.
 - ② 위원장은 위원 중에서 공무원이 아닌 사람으로 보호위원회 위원장이 위촉한다.
 - ③ 분쟁조정위원회 또는 조정부는 재적위원 과반수의 출석으로 개의하며 출석위원 3분의 2 이상 찬성으로 의결한다.
 - ④ 위원장과 위촉위원의 임기는 2년으로 하되, 1차에 한하여 연임할 수 있다.
13. 다음은 「전자정부법」 제2조(정의)의 일부이다. <보기 1>의 뜻과 <보기 2>의 용어를 연결한 것으로 가장 적절한 것은?

—<보기 1>—

- (가)란 행정기관등이 직무상 작성하거나 취득하여 관리하고 있는 자료로서 전자적 방식으로 처리되어 부호, 문자, 음성, 음향, 영상 등으로 표현된 것을 말한다.
- (나)란 컴퓨터 등 정보처리능력을 지닌 장치에 의하여 전자적인 형태로 작성되어 송수신되거나 저장되는 표준화된 정보를 말한다.
- (다)란 종이문서와 그 밖에 전자적 형태로 작성되지 아니한 문서를 정보시스템이 처리할 수 있는 형태로 변환한 문서를 말한다.

—<보기 2>—

㉠ 행정정보	㉡ 전자문서	㉢ 전자화문서
--------	--------	---------

	(가)	(나)	(다)
①	㉠	㉡	㉢
②	㉡	㉠	㉢
③	㉡	㉢	㉠
④	㉢	㉠	㉡

14. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」상 클라우드컴퓨팅서비스의 신뢰성 향상 및 이용자 보호에 대한 설명으로 가장 적절하지 않은 것은?
- ① 클라우드컴퓨팅서비스 제공자는 이용자 정보가 유출된 때 지체 없이 그 사실을 해당 이용자에게 알려야 한다.
 - ② 이용자는 클라우드컴퓨팅서비스 제공자에게 이용자 정보가 저장되는 국가의 명칭을 알려 줄 것을 요구할 수 있다.
 - ③ 클라우드컴퓨팅서비스 제공자는 클라우드컴퓨팅서비스의 품질·성능 및 정보보호 수준을 향상시키기 위하여 노력하여야 한다.
 - ④ 클라우드컴퓨팅서비스 제공자는 이용자와의 계약이 종료되었을 때에는 이용자에게 이용자 정보를 반환하여야 하고 클라우드컴퓨팅서비스 제공자가 보유하고 있는 이용자 정보를 따로 저장하여야 한다.
15. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제46조의2(집적정보통신시설 사업자의 긴급대응)에서 집적정보통신시설 사업자가 이용약관으로 정하는 바에 따라 해당 서비스의 전부 또는 일부의 제공을 중단할 수 있는 경우로 가장 적절하지 않은 것은?
- ① 시설이용자의 정보시스템에서 발생한 이상현상으로 다른 시설 이용자의 정보통신망에 심각한 장애를 발생시킬 우려가 있다고 판단되는 경우
 - ② 중대한 침해사고가 발생하여 과학기술정보통신부장관이 요청하는 경우
 - ③ 중대한 침해사고가 발생하여 한국인터넷진흥원이 요청하는 경우
 - ④ 침해사고가 발생하지는 않았지만, 집적된 정보통신시설에 심각한 장애가 발생할 우려가 있다고 판단되어 국무총리가 요청하는 경우

16. 「전자금융거래법」 제2조(정의)에 대한 내용으로 가장 적절한 것은?
- ① 전자지급거래는 금융회사 또는 전자금융업자가 전자적 장치를 통하여 금융상품 및 서비스를 제공하고, 이용자가 금융회사 또는 전자금융업자의 종사자와 직접 대면하거나 의사소통을 하지 아니하고 자동화된 방식으로 이를 이용하는 거래를 말한다.
 - ② 전자금융거래는 자금을 주는 자가 금융회사 또는 전자금융업자로 하여금 전자지급수단을 이용하여 자금을 받는 자에게 자금을 이동하게 하는 거래를 말한다.
 - ③ 전자적 장치는 전자자금이체, 직불전자지급수단, 선불전자지급수단, 전자화폐, 신용카드, 전자채권 그 밖에 전자적 방법에 따른 지급수단을 말한다.
 - ④ 전자지급결제대행은 전자적 방법으로 재화의 구입 또는 용역의 이용에 있어서 지급결제정보를 송신하거나 수신하는 것 또는 그 대가의 정산을 대행하거나 매개하는 것을 말한다.
17. 「정보통신기반 보호법」상 정보통신기반보호위원회와 관련된 내용으로 가장 적절하지 않은 것은?
- ① 위원회의 위원은 위원장 1인을 포함한 25인 이내의 위원으로 구성한다.
 - ② 주요정보통신기반시설의 보호에 관한 사항을 심의하기 위하여 과학기술정보통신부장관 소속하에 정보통신기반보호위원회를 둔다.
 - ③ 위원회의 위원장은 국무조정실장이 된다.
 - ④ 위원회의 효율적인 운영을 위하여 위원회에 공공분야와 민간분야를 각각 담당하는 실무위원회를 둔다.
18. 「위치정보의 보호 및 이용 등에 관한 법률」 제11조(위치기반서비스사업자의 휴업·폐업 등)의 일부분이다. ㉠~㉣에 들어갈 내용으로 가장 적절한 것은?

- 위치기반서비스사업자가 사업의 전부 또는 일부를 휴업하고자 하는 때에는 휴업기간을 정하여 휴업하고자 하는 날의 (㉠)일 전까지 이를 개인위치정보주체에게 통보하고 방송통신위원회에 신고하여야 한다. 이 경우 휴업기간은 (㉡)을 초과할 수 없다.
- 위치기반서비스사업자가 사업의 전부 또는 일부를 폐업하고자 하는 때에는 폐업하고자 하는 날의 (㉢)일 전까지 이를 개인위치정보주체에게 통보하고 방송통신위원회에 신고하여야 한다.

	㉠	㉡	㉢
①	30	1년	30
②	30	2년	60
③	60	1년	30
④	60	2년	60

19. 「전자정부법」 제43조(정보주체의 열람청구권)에서 정보주체가 공동이용센터를 통하여 공동이용한 행정정보 중 본인에 관한 행정정보에 대하여 행정안전부장관 또는 해당이용기관의 장에게 신청할 수 있는 열람 사항으로 가장 적절하지 않은 것은?
- ① 공동이용센터 행정정보 책임자 정보
 - ② 공동이용의 목적
 - ③ 공동이용한 행정정보의 종류
 - ④ 이용기관
20. 경찰관 A는 불특정 다수가 이용하는 장소에 영상정보처리 기기가 설치되었다는 신고를 받고 현장에 도착하여 신고인에게 「개인정보 보호법」 제25조(영상정보처리기기의 설치·운영 제한)에 제한되지 않는 장소임을 설명하였다. 경찰관 A가 출동했었던 현장으로 가장 적절한 곳은?
- ① 목욕실
 - ② 발한실
 - ③ 정신보건 시설
 - ④ 탈의실