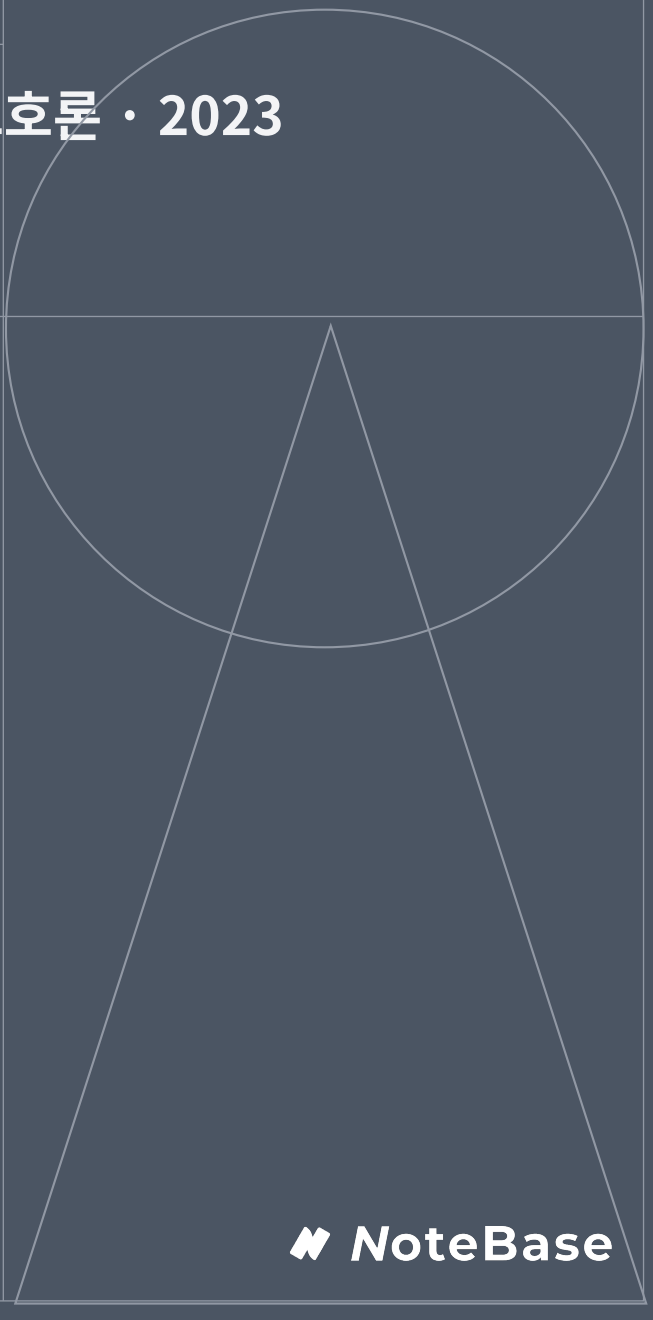
기출OX 해설집

공무원/지방직/9급 · 정보보호론 · 2023



NoteBase

기출OX 해설집

공무원/지방직/9급 · 정보보호론 · 2023

공무원/지방직/9급 · 정보보호론 · 2023

문 1. 데이터의 위·변조를 방어하는 기술이 목표로 하는 것은?

① 기밀성

② 무결성

③ 가용성

④ 책임추적성

정답 2번

간단한 해설

데이터가 허가 없이 바뀌거나 위조되지 않도록 보호하는 목표는 **무결성**이다. 핵심은 정보가 노출되는지가 아니라 내용이 부당하게 변경되는지에 있다.

개념 구분

무결성: 데이터가 **허가 없이 변경·위조·훼손되지 않도록** 보호하는 성질이다. 예를 들어 송금액을 1만 원에서 10만 원으로 몰래 바꾸는 행위는 무결성을 침해한다. 문제의 '위·변조 방어'는 이러한 부당한 변경을 막는 것이므로 무결성을 목표로 한다.

기밀성: **인가받지 않은 사람에게 정보가 공개되지 않도록** 보호하는 성질이다. 내용을 몰래 읽는 것은 기밀성 문제이고, 내용을 몰래 바꾸는 것은 무결성 문제이다.

가용성: 인가받은 사용자가 **필요할 때 정보나 서비스를 이용할 수 있도록** 하는 성질이다. 데이터 내용의 위·변조 여부보다 접근과 이용이 가능한지가 기준이다.

책임추적성: 시스템에서 발생한 행위를 **그 행위를 한 주체까지 추적할 수 있는** 성질이다. 누가 변경했는지 밝히는 것과 데이터의 부당한 변경 자체를 막는 것은 구별된다.

NoteBase

문 2. UDP 헤더 포맷의 구성 요소가 아닌 것은?

① 순서 번호

② 발신지 포트 번호

③ 목적지 포트 번호

④ 체크섬

정답 1번

간단한 해설

UDP 헤더에는 **순서 번호가 없다**. 순서 번호는 TCP에서 데이터의 순서를 관리하는 필드이며, UDP는 데이터그램의 전달 순서를 보장하지 않는다.

선지별 해설

UDP 헤더는 발신지 포트 번호, 목적지 포트 번호, 길이, 체크섬의 네 필드로 구성된다. 각 필드는 16비트이며 헤더 전체의 크기는 8바이트이다. 길이 필드는 UDP 헤더와 데이터를 합한 전체 길이를 바이트 단위로 나타낸다.

① X: 순서 번호는 **TCP 헤더의 필드**로, 전송하는 데이터의 순서를 관리하는 데 사용된다. UDP 헤더에는 순서 번호가 없으므로, UDP 자체는 데이터그램이 전송한 순서대로 도착하도록 보장하지 않는다.

② O: 발신지 포트 번호는 **데이터를 보낸 응용프로그램을 식별**하는 데 사용한다. 수신 측에서 응답할 때 목적지 포트를 정하는 데 활용할 수 있다.

③ O: 목적지 포트 번호는 **데이터를 받을 응용프로그램을 식별**하는 데 사용한다. 수신 호스트는 이를 이용해 도착한 데이터그램을 해당 응용프로그램에 전달한다.

④ O: 체크섬은 **전송 중 발생한 데이터 오류를 검출**하기 위한 필드이다. 송신 측이 계산한 검사값을 수신 측에서 확인하여 데이터가 손상되었는지 검사한다.

NoteBase

문 3. 논리 폭탄에 대한 설명으로 옳은 것은?

① 사용자 동의 없이 설치되어 컴퓨터 내의 금융 정보, 신상 정보 등을 수집·전송하기 위한 것이다.

② 침입자에 의해 악성 소프트웨어에 삽입된 코드로서, 사전에 정의된 조건이 충족되기 전까지는 휴지 상태에 있다가 조건이 충족되면 의도한 동작이 트리거되도록 한다.

③ 사용자가 키보드로 PC에 입력하는 내용을 몰래 가로채어 기록한다.

④ 공격자가 언제든지 시스템에 관리자 권한으로 접근할 수 있도록 비밀 통로를 지속적으로 유지시켜 주는 일련의 프로그램 집합이다.

정답 2번

간단한 해설

논리 폭탄은 **미리 정한 조건이 충족될 때 악성 동작을 실행**하도록 삽입한 코드이다. 조건이 충족되기 전에는 해당 악성 동작이 잠복해 있다는 점이 핵심이다.

개념 구분

논리 폭탄: ②의 '사전에 정의된 조건'과 '조건이 충족되면 동작이 트리거'된다는 표현이 결정적 단서이다. 프로그램에 삽입된 코드가 조건을 확인하고, **조건이 성립할 때 악성 동작을 실행**한다. 예를 들어 특정 날짜가 되면 파일을 삭제하도록 심어 둔 코드가 이에 해당한다. 여기서 잠복하는 것은 악성 동작이며, 그 코드가 들어 있는 프로그램 전체가 멈춰 있어야 한다는 뜻은 아니다.

스파이웨어: ①은 사용자 동의 없이 금융 정보나 신상 정보 등을 **수집·전송**하는 기능을 설명한다. 논리 폭탄을 구별하는 기준은 수집하는 정보의 종류가 아니라 악성 동작을 실행시키는 사전 조건의 존재이다.

키로거: ③은 **키보드 입력 내용을 몰래 기록**하는 기능을 설명한다. 입력 내용의 기록이 핵심이며, 특정 조건이 충족될 때까지 악성 동작이 잠복한다는 논리 폭탄의 특징과 구별된다.

루트킷: ④는 공격자의 **은밀한 관리자 권한 접근을 지속적으로 유지**하도록 돕는 프로그램 집합을 설명한다. 루트킷은 침입 흔적이나 악성 프로그램을 숨기는 데 사용되며, 논리 폭탄의 조건부 실행과는 구별된다.

NoteBase

문 4. 대칭키 암호 알고리즘이 아닌 것은?

① SEED

② ECC

③ IDEA

④ LEA

정답 2번

간단한 해설

ECC는 **공개키와 개인키를 구분하여 사용하는 공개키 암호 방식**이다. 암호화와 복호화에 같은 비밀키를 사용하는 대칭키 암호와 구별된다.

선지별 해설

대칭키 암호는 송신자와 수신자가 같은 비밀키를 공유하여 암호화와 복호화에 사용하는 방식이다. 블록 암호는 데이터를 일정한 크기의 블록으로 나누어 처리하는 대칭키 암호이다. 아래 O/X는 각 알고리즘이 대칭키 암호에 해당하는지를 나타낸다.

① O: SEED는 **대칭키 블록 암호**이다. 128비트 비밀키를 사용하여 데이터를 128비트 블록 단위로 암호화하고 복호화한다.

② X: ECC는 타원곡선의 수학적 성질을 이용하는 **공개키 암호 방식**이다. 공개키와 개인키를 구분하여 사용하므로, 대칭키 암호가 아니라 비대칭키 암호로 분류한다.

③ O: IDEA는 **대칭키 블록 암호**이다. 128비트 비밀키를 사용하며, 암호화와 복호화의 처리 단위는 64비트 블록이다.

④ O: LEA는 **대칭키 블록 암호**이다. 128비트 블록을 처리하며, 비밀키 길이는 128비트·192비트·256비트 중 하나를 사용한다.

NoteBase

문 5. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 규정하고 있는 사항이 아닌 것은?

① 정보통신망의 표준화 및 인증

② 정보통신망의 안정성 확보

③ 고정형 영상정보처리기기의 설치·운영 제한

④ 집적된 정보통신시설의 보호

정답 3번

①

정보통신망에 관한 **표준의 고시와 표준에 적합한 제품의 인증**을 규정한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제8조
정보통신망 이용촉진 및 정보보호 등에 관한 법률 제8조(정보통신망의 표준화 및 인증)
① 과학기술정보통신부장관은 정보통신망의 이용을 촉진하기 위하여 정보통신망에 관한 표준을 정하여 고시하고, 정보통신서비스 제공자 또는 정보통신망과 관련된 제품을 제조하거나 공급하는 자에게 그 표준을 사용하도록 권고할 수 있다. 다만, 「산업표준화법」 제12조에 따른 한국산업표준이 제정되어 있는 사항에 대하여는 그 표준에 따른다. <개정 2013.3.23, 2017.7.26>
② 제1항에 따라 고시된 표준에 적합한 정보통신과 관련된 제품을 제조하거나 공급하는 자는 제9조제1항에 따른 인증기관의 인증을 받아 그 제품이 표준에 적합한 것임을 나타내는 표시를 할 수 있다.
③ 제1항 단서에 해당하는 경우로서 「산업표준화법」 제15조에 따라 인증을 받은 경우에는 제2항에 따른 인증을 받은 것으로 본다.
④ 제2항에 따른 인증을 받은 자가 아니면 그 제품이 표준에 적합한 것임을 나타내는 표시를 하거나 이와 비슷한 표시를 하여서는 아니 되며, 이와 비슷한 표시를 한 제품을 판매하거나 판매할 목적으로 진열하여서는 아니 된다.
⑤ 과학기술정보통신부장관은 제4항을 위반하여 제품을 판매하거나 판매할 목적으로 진열한 자에게 그 제품을 수거 · 반품하도록 하거나 인증을 받아 그 표시를 하도록 하는 등 필요한 시정조치를 명할 수 있다. <개정 2013.3.23, 2017.7.26>
⑥ 제1항부터 제3항까지의 규정에 따른 표준화의 대상 · 방법 · 절차 및 인증표시, 제5항에 따른 수거 · 반품 · 시정 등에 필요한 사항은 과학기술정보통신부령으로 정한다. <개정 2013.3.23, 2017.7.26>

NoteBase

②

정보통신서비스 제공자 등은 **정보통신망의 안정성과 정보의 신뢰성을 확보하기 위한 보호조치**를 하여야 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조 제1항
정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조(정보통신망의 안정성 확보 등)
① 다음 각 호의 어느 하나에 해당하는 자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다. <개정 2020.6.9>
1. 정보통신서비스 제공자
2. 정보통신망에 연결되어 정보를 송 · 수신할 수 있는 기기 · 설비 · 장비 중 대통령령으로 정하는 기기 · 설비 · 장비(이하 "정보통신망연결기기등"이라 한다)를 제조하거나 수입하는 자

③

고정형 영상정보처리기기의 설치·운영 제한은 **「개인정보 보호법」에서 규정하는 사항**이다.

개인정보 보호법 제25조 제1항
개인정보 보호법 제25조(고정형 영상정보처리기기의 설치 · 운영 제한)
① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 고정형 영상정보처리기기를 설치 · 운영하여서는 아니 된다. <개정 2023.3.14>
1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설의 안전 및 관리, 화재 예방을 위하여 정당한 권한을 가진 자가 설치 · 운영하는 경우
4. 교통단속을 위하여 정당한 권한을 가진 자가 설치 · 운영하는 경우
5. 교통정보의 수집 · 분석 및 제공을 위하여 정당한 권한을 가진 자가 설치 · 운영하는 경우
6. 촬영된 영상정보를 저장하지 아니하는 경우로서 대통령령으로 정하는 경우

NoteBase

④

집적된 정보통신시설을 운영·관리하는 정보통신서비스 제공자 중 법정 기준에 해당하는 자에게 **시설의 안정적 운영을 위한 보호조치 의무**를 부과한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제46조 제1항
정보통신망 이용촉진 및 정보보호 등에 관한 법률 제46조(집적된 정보통신시설의 보호)
① 다음 각 호의 어느 하나에 해당하는 정보통신서비스 제공자 중 정보통신시설의 규모 등이 대통령령으로 정하는 기준에 해당하는 자(이하 "집적정보통신시설 사업자등"이라 한다)는 정보통신시설을 안정적으로 운영하기 위하여 대통령령으로 정하는 바에 따른 보호조치를 하여야 한다. <개정 2020.6.9, 2023.1.3>
1. 타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영 · 관리하는 자(이하 "집적정보통신시설 사업자"라 한다)
2. 자신의 정보통신서비스 제공을 위하여 직접 집적된 정보통신시설을 운영 · 관리하는 자

NoteBase

문 6. CSRF 공격에 대한 설명으로 옳지 않은 것은?

① 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위를 특정 웹사이트에 요청하게 하는 공격이다.

② 특정 웹사이트가 사용자의 웹 브라우저를 신뢰하는 점을 노리고 사용자의 권한을 도용하려는 것이다.

③ 사용자에게 전달된 데이터의 악성 스크립트가 사용자 브라우저에서 실행되면서 해킹을 하는 것으로, 이 악성 스크립트는 공격자가 웹 서버에 구현된 애플리케이션의 취약점을 이용하여 서버 측 또는 URL에 미리 삽입해 놓은 것이다.

④ 웹 애플리케이션의 요청 내에 세션별·사용자별로 구별 가능한 임의의 토큰을 추가하도록 하여 서버가 정상적인 요청과 비정상적인 요청을 판별하는 방법으로 공격에 대응할 수 있다.

정답 3번

간단한 해설

③의 '악성 스크립트가 사용자 브라우저에서 실행된다'는 **XSS(크로스 사이트 스크립팅)**의 설명이다. CSRF(크로스 사이트 요청 위조)는 사용자의 인증 상태를 악용하여 **사용자가 의도하지 않은 요청**을 웹사이트에 보내게 한다.

선지별 해설

① O: CSRF는 사용자의 의사와 무관하게 공격자가 원하는 요청을 대상 웹사이트에 보내게 하는 공격이다. 예를 들어, 해당 사이트에 로그인한 사용자가 공격자가 유도한 페이지를 열었을 때 자신의 계정에 등록된 이메일 주소를 변경하는 요청이 전송될 수 있다. 핵심은 **사용자가 요청한 것으로 처리되지만 실제로는 사용자가 의도하지 않은 행위**라는 점이다.

② O: 웹사이트는 보통 세션 쿠키 등 인증 정보를 통해 요청자의 로그인 상태와 권한을 확인한다. CSRF는 위조된 요청에도 사용자의 인증 쿠키가 함께 전송되는 경우, 서버가 이를 사용자 본인의 요청으로 받아들이는 점을 악용한다. 즉, **인증된 브라우저에서 온 요청이라는 사실만으로 사용자의 의도까지 확인할 수는 없다**.

③ X: 웹 애플리케이션의 취약점을 이용해 삽입한 악성 스크립트가 사용자 브라우저에서 실행되는 것은 **XSS**의 설명이다. 스크립트가 게시물 등 서버에 저장되었다가 전달되면 저장형 XSS, URL 등의 입력에 포함되어 서버 응답에 반영되면 반사형 XSS에 해당한다. CSRF의 핵심은 악성 스크립트의 삽입·실행 자체가 아니라, 사용자의 인증 상태를 이용해 원하지 않는 요청을 보내게 하는 데 있다.

④ O: CSRF 토큰은 정상적인 요청에 포함하도록 하는, 세션별·사용자별로 구별되는 임의의 값이다. 서버는 요청에 포함된 토큰이 해당 세션에 대해 발급한 값과 일치하는지 검사하고, 토큰이 없거나 일치하지 않으면 요청을 거부할 수 있다. 토큰은 **공격자가 예측하기 어려워야** 하며, 이 조건 아래에서 공격자가 유효한 토큰을 넣은 위조 요청을 만들기 어렵게 한다.

NoteBase

문 7. IPSec의 터널 모드를 이용한 VPN에 대한 설명으로 옳지 않은 것은?

① 인터넷상에서 양측 호스트의 IP 주소를 숨기고 새로운 IP 헤더에 VPN 라우터 또는 IPSec 게이트웨이의 IP 주소를 넣는다.

② IPSec의 터널 모드는 새로운 IP 헤더를 추가하기 때문에 전송 모드 대비 전체 패킷이 길어진다.

③ ESP는 원래 IP 패킷 전부와 원래 IP 패킷 앞뒤로 붙는 ESP 헤더와 트레일러를 모두 암호화한다.

④ ESP 인증 데이터는 패킷의 끝에 추가되며, ESP 터널 모드의 경우 인증은 목적지 VPN 라우터 또는 IPSec 게이트웨이에서 이루어진다.

정답 3번

간단한 해설

③의 'ESP 헤더와 트레일러를 모두 암호화한다'는 설명에서 **ESP 헤더는 암호화 대상이 아니다**. ESP 터널 모드는 원래 IP 패킷 전체와 ESP 트레일러를 암호화하며, ESP 헤더는 암호화하지 않는다.

선지별 해설

① O: 게이트웨이 사이에 ESP 터널을 구성하면 원래 IP 헤더를 포함한 IP 패킷 전체가 암호화되어 내부 호스트의 주소가 인터넷에 드러나지 않는다. 새로 붙이는 외부 IP 헤더에는 **터널 양 끝 VPN 라우터 또는 IPSec 게이트웨이의 주소**를 넣어 인터넷에서 패킷을 전달한다.

② O: 전송 모드는 기존 IP 헤더를 유지하면서 그 뒤에 ESP를 적용한다. 터널 모드는 기존 IP 패킷 전체를 내부에 넣고 **새로운 외부 IP 헤더를 추가**하므로, 같은 원본 데이터와 보안 알고리즘을 기준으로 전송 모드보다 패킷이 길어진다.

③ X: ESP 터널 모드의 암호화 범위는 원래 IP 헤더를 포함한 IP 패킷 전체와 ESP 트레일러이다. SPI와 순서 번호가 들어 있는 **ESP 헤더는 암호화하지 않는다**. SPI는 수신 측이 보안 연결을 식별하는 데 사용된다. ESP 인증 데이터도 암호화 범위에 포함되지 않으므로, ESP 헤더까지 모두 암호화한다는 부분을 고쳐야 한다.

④ O: ESP 인증을 사용하는 경우 무결성 검증값인 인증 데이터가 ESP 트레일러 뒤, 패킷 끝에 붙는다. 게이트웨이 사이의 터널에서는 **터널의 수신 종단인 목적지 VPN 라우터 또는 IPSec 게이트웨이**가 인증 데이터를 검증하여 패킷의 변조 여부와 송신 측의 정당성을 확인한다.

NoteBase

문 8. 「전자서명법」상 전자서명인증사업자에 대한 전자서명인증업무 운영기준 준수사실의 인정(이하 “인정”이라 한다)에 대한 설명으로 옳지 않은 것은?

① 인정을 받으려는 전자서명인증사업자는 국가기관, 지방자치단체 또는 공공기관이어야 한다.

② 인정을 받으려는 전자서명인증사업자는 평가기관으로부터 평가를 먼저 받아야 한다.

③ 평가기관은 평가를 신청한 전자서명인증사업자의 운영기준 준수 여부에 대한 평가를 하고, 그 결과를 인정기관에 제출하여야 한다.

④ 인정기관은 평가 결과를 제출받은 경우 그 평가 결과와 인정을 받으려는 전자서명인증사업자가 법정 자격을 갖추었는지 여부를 확인하여 인정 여부를 결정하여야 한다.

정답 1번

①

인정을 받으려는 전자서명인증사업자는 **국가기관, 지방자치단체 또는 법인**이어야 한다. 공공기관에 한정되지 않으며 민간 법인도 포함된다.

전자서명법 제8조 제2항
전자서명법 제8조(운영기준 준수사실의 인정)
② 제1항 전단에 따른 인정(이하 "운영기준 준수사실의 인정"이라 한다)을 받으려는 전자서명인증사업자는 국가기관, 지방자치단체 또는 법인이어야 한다.

②

인정기관의 인정을 받으려면 **평가기관으로부터 운영기준 준수 여부에 대한 평가를 먼저 받아야 한다**.

전자서명법 제8조 제1항
전자서명법 제8조(운영기준 준수사실의 인정)
① 전자서명인증사업자(전자서명인증업무를 하려는 자를 포함한다. 이하 제8조부터 제11조까지에서 같다)는 제9조에 따른 인정기관으로부터 운영기준의 준수사실에 대한 인정을 받을 수 있다. 이 경우 제10조에 따른 평가기관으로부터 운영기준의 준수 여부에 대한 평가를 먼저 받아야 한다.

NoteBase

③

평가기관은 신청한 전자서명인증사업자의 **운영기준 준수 여부를 평가하고 그 결과를 인정기관에 제출하여야 한다**.

전자서명법 제10조 제3항
전자서명법 제10조(평가기관)
③ 평가기관은 평가를 신청한 전자서명인증사업자의 운영기준 준수 여부에 대한 평가를 하고, 그 결과를 인정기관에 제출하여야 한다.

④

인정기관은 평가 결과를 제출받으면 **평가 결과와 신청 사업자의 법정 자격 충족 여부를 확인하여 인정 여부를 결정하여야 한다**.

전자서명법 제9조 제2항
전자서명법 제9조(인정기관)
② 인정기관은 제10조제3항에 따라 평가 결과를 제출받은 경우 그 평가 결과와 운영기준 준수사실의 인정을 받으려는 전자서명인증사업자가 제8조에 따른 자격을 갖추었는지 여부를 확인하여 운영기준 준수사실의 인정 여부를 결정하여야 한다.

NoteBase

문 9. 위험 평가 접근방법에 대한 설명으로 옳지 않은 것은?

① 기준(baseline) 접근법은 기준 문서, 실무 규약, 업계 최신 실무를 이용하여 시스템에 대한 가장 기본적이고 일반적인 수준에서의 보안 통제 사항을 구현하는 것을 목표로 한다.

② 비정형(informal) 접근법은 구조적인 방법론에 기반하지 않고 전문가의 지식과 경험에 따라 위험을 분석하는 것으로, 비교적 신속하고 저비용으로 진행할 수 있으나 특정 전문가의 견해 및 편견에 따라 왜곡될 우려가 있다.

③ 상세(detailed) 위험 분석은 정형화되고 구조화된 프로세스를 사용하여 상세한 위험 평가를 수행하는 것으로, 많은 시간과 비용이 드는 단점이 있는 반면에 위험에 따른 손실과 보안 대책의 비용 간의 적절한 균형을 이룰 수 있는 장점이 있다.

④ 복합(combined) 접근법은 상세 위험 분석을 제외한 기준 접근법과 비정형 접근법 두 가지를 조합한 것으로 저비용으로 빠른 시간 내에 필요한 통제 수단을 선택해야 하는 상황에서 제한적으로 활용된다.

정답 4번

간단한 해설

④의 '상세 위험 분석을 제외'한다는 설명이 잘못되었다. 복합 접근법은 먼저 시스템의 중요성과 위험을 개괄적으로 파악한 뒤, **중요하거나 위험이 높은 시스템에는 상세 위험 분석**을, 나머지에는 기준 접근법을 적용하여 분석 비용과 보호 수준의 균형을 맞춘다.

NoteBase

선지별 해설

① O: 기준 접근법은 기준 문서, 실무 규약, 업계의 우수 실무 등에서 제시하는 표준 보안 통제를 적용하여 **기본적인 보호 수준**을 확보한다. 시스템마다 자산·위협·취약점을 상세히 분석하여 통제를 새로 도출하는 부담을 줄일 수 있다.

② O: 비정형 접근법은 구조화된 분석 절차보다 **전문가 개인의 지식과 경험**에 의존한다. 절차를 정교하게 수행하는 데 드는 시간과 비용은 적지만, 전문가의 주관이나 편견이 결과에 반영되거나 중요한 위험이 누락될 수 있다.

③ O: 상세 위험 분석은 자산의 가치, 위협, 취약점 등을 체계적으로 조사하여 위험을 평가하고 그에 맞는 보안 대책을 선정한다. 분석에 많은 시간과 비용이 들지만, **위험으로 인한 손실과 대책 비용**을 함께 고려하므로 필요한 보호 수준에 맞추어 대책을 선택할 수 있다.

④ X: 복합 접근법은 상세 위험 분석을 제외하지 않는다. 먼저 전체 시스템의 업무상 중요성과 주요 위험을 개괄적으로 분석한 뒤, **중요하거나 위험이 높은 시스템에는 상세 위험 분석**을 우선 적용하고 나머지에는 기준 접근법을 적용한다. 이처럼 분석 자원을 보호 필요성이 큰 곳에 집중하여 시간·비용과 적절한 보호 수준의 균형을 맞추는 방법이므로, 저비용으로 신속하게 통제를 선택해야 하는 상황에만 제한되는 방법도 아니다.

NoteBase

문 10. ISMS-P 인증 기준의 세 영역 중 하나인 관리체계 수립 및 운영에 해당하지 않는 것은?

① 관리체계 기반 마련

② 위험 관리

③ 관리체계 점검 및 개선

④ 정책, 조직, 자산 관리

정답 4번

간단한 해설

④의 '정책, 조직, 자산 관리'는 **보호대책 요구사항** 영역의 세부 분야이다. '관리체계 수립 및 운영' 영역과는 인증기준상 소속이 다르다.

선지별 해설

① O: '관리체계 기반 마련'은 관리체계 수립 및 운영 영역의 1.1 분야이다. 경영진의 참여, 책임자 지정, 조직 구성, 관리체계 범위 설정, 정책 수립, 자원 할당 등을 통해 **관리체계를 실행할 기반**을 갖춘다.

② O: '위험 관리'는 관리체계 수립 및 운영 영역의 1.2 분야이다. 정보자산을 식별하고 업무 현황과 정보 흐름을 분석한 뒤, **위험을 평가하여 필요한 보호대책을 선정**하는 활동이다.

③ O: '관리체계 점검 및 개선'은 관리체계 수립 및 운영 영역의 1.4 분야이다. 법적 요구사항의 준수 여부와 관리체계 운영 상태를 점검하고, 발견된 문제를 개선하여 **관리체계의 효과성을 유지**한다.

④ X: '정책, 조직, 자산 관리'는 관리체계 수립 및 운영 영역이 아니라 **보호대책 요구사항 영역의 2.1 분야**이다. 정책과 조직을 유지·관리하고 정보자산을 관리하는 구체적인 보호대책을 다룬다. 관리체계 기반 마련에서 정책을 수립하고 조직을 구성하는 것과 관련은 있지만, 인증기준상 별개의 분야로 분류된다.

NoteBase

문 11. OTP 토큰이 속하는 인증 유형은?

① 정적 생체정보

② 동적 생체정보

③ 가지고 있는 것

④ 알고 있는 것

정답 3번

간단한 해설

OTP 토큰은 일회용 인증번호를 생성하는 장치를 **가지고 있음을 확인**하는 수단이므로, 소유 기반 인증에 해당한다.

개념 구분

OTP 토큰: 일회용 인증번호를 생성하는 장치이다. 사용자가 토큰에서 생성된 번호를 제출하면, 인증 시스템은 그 번호가 유효한지 확인한다. 이때 인증의 근거는 **토큰의 소유**이므로 '가지고 있는 것'으로 분류한다.

알고 있는 것과의 구분: 비밀번호처럼 사용자가 기억하는 비밀정보를 근거로 인증하는 방식이다. OTP 번호를 화면에 입력하더라도, 그 번호는 외워 둔 비밀정보가 아니라 **토큰을 통해 얻은 일회용 값**이므로 입력 행위만으로 지식 기반 인증이 되지는 않는다.

생체정보와의 구분: 정적 생체정보는 지문·홍채 같은 신체적 특징이고, 동적 생체정보는 서명 동작 같은 행동적 특징이다. OTP 토큰은 이러한 신체적·행동적 특징을 측정하는 수단이 아니므로 두 생체정보 유형에 속하지 않는다.

NoteBase

문 12. 서비스 거부 공격에 해당하는 것은?

① 발신지 IP 주소와 목적지 IP 주소의 값을 똑같이 만든 패킷을 공격 대상에게 전송한다.

② 공격 대상에게 실제 DNS 서버보다 빨리 응답 패킷을 보내 공격 대상이 잘못된 IP 주소로 웹 접속을 하도록 유도한다.

③ LAN상에서 서버와 클라이언트의 IP 주소에 대한 MAC 주소를 위조하여 둘 사이의 패킷이 공격자에게 전달되도록 한다.

④ 네트워크 계층에서 공격 시스템을 네트워크에 존재하는 또 다른 라우터라고 속임으로써 트래픽이 공격 시스템을 거쳐가도록 흐름을 바꾼다.

정답 1번

간단한 해설

발신지와 목적지 IP 주소를 공격 대상의 주소로 같게 만드는 방식은 **LAND 공격**이다. 취약한 시스템의 패킷 처리에 이상을 일으켜 정상적인 서비스 이용을 방해하므로 서비스 거부 공격에 해당한다.

선지별 해설

① O: 서비스 거부(DoS) 공격은 시스템의 정상적인 서비스 제공을 방해하여 가용성을 침해한다. 선지는 **발신지와 목적지 IP 주소를 모두 공격 대상의 주소로 위조**하는 LAND 공격을 설명한다. 전형적으로 발신지와 목적지 포트도 같게 설정한 TCP SYN 패킷을 보내며, 취약한 시스템이 이를 처리하는 과정에서 정상적인 서비스가 방해될 수 있다.

② X: 선지는 **DNS 스푸핑**을 설명한다. DNS는 도메인 이름에 대응하는 IP 주소를 알려 주는데, 공격자는 정상 응답보다 먼저 위조 응답이 받아들여지도록 하여 잘못된 IP 주소로 접속하게 만든다. 제시된 방식은 서비스 자체를 중단시키는 공격이 아니라 이름 해석 결과를 속여 접속 목적지를 바꾸는 공격이다.

③ X: 선지는 **ARP 스푸핑**을 설명한다. ARP는 LAN에서 IP 주소에 대응하는 MAC 주소를 알아내는 데 사용된다. 공격자가 서버와 클라이언트의 ARP 캐시에 상대방 IP 주소에 대응하는 MAC 주소를 공격자의 것으로 등록하게 하면, 서로에게 보낼 패킷이 공격자에게 전달된다. 제시된 방식은 통신을 가로채는 중간자 공격을 위한 것으로, 서비스 거부 공격의 설명과 구별된다.

④ X: 선지는 **ICMP 리다이렉트 공격**을 설명한다. 정상적인 ICMP 리다이렉트는 라우터가 호스트에 더 적절한 다음 경유지를 알려 주는 기능이다. 공격자는 이 메시지를 위조하여 자신의 시스템을 경유지로 사용하게 함으로써 트래픽 경로를 바꾼다. 제시된 방식의 핵심은 서비스 중단이 아니라 경로 조작을 통한 트래픽 가로채기이다.

NoteBase

문 13. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조의4 (침해사고의 원인 분석 등)의 내용으로 옳지 않은 것은?

① 정보통신서비스 제공자 등 정보통신망을 운영하는 자는 침해사고가 발생하면 침해사고의 원인을 분석하고 그 결과에 따라 피해의 확산 방지를 위하여 사고대응, 복구 및 재발 방지에 필요한 조치를 하여야 한다.

② 과학기술정보통신부장관은 정보통신서비스 제공자의 정보통신망에 침해사고가 발생하면 그 침해사고의 원인을 분석하고 피해 확산 방지, 사고대응, 복구 및 재발 방지를 위한 대책을 마련하여 해당 정보통신서비스 제공자에게 필요한 조치를 하도록 권고할 수 있다.

③ 과학기술정보통신부장관은 정보통신서비스 제공자의 정보통신망에 발생한 침해사고의 원인 분석 및 대책 마련을 위하여 필요하면 정보통신서비스 제공자에게 정보통신망의 접속기록 등 관련 자료의 보전을 명할 수 있다.

④ 과학기술정보통신부장관이나 민·관합동조사단은 관련 규정에 따라 정보통신서비스 제공자로부터 제출받은 침해사고 관련 자료와 조사를 통하여 알게 된 정보를 재발 방지 목적으로 필요한 경우 원인 분석이 끝난 후에도 보존할 수 있다.

정답 2, 4번

①

정보통신망 운영자는 침해사고가 발생하면 원인을 분석하고, 그 결과에 따라 **피해 확산 방지를 위한 사고대응·복구·재발 방지 조치를 하여야 한다**.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제48조의4 제1항
정보통신망 이용촉진 및 정보보호 등에 관한 법률 제48조의4(침해사고의 원인 분석 등)
① 정보통신서비스 제공자 등 정보통신망을 운영하는 자는 침해사고가 발생하였거나 내부 정보 유출 등 침해사고가 발생하였다고 의심할 만한 정황이 있어 제48조의2제7항에 따른 침해사고조사심의위원회가 침해사고 발생 여부에 대한 조사가 필요하다고 인정하는 경우에는 침해사고의 발생 여부 및 원인을 분석하고 그 결과에 따라 피해의 확산 방지를 위하여 사고대응, 복구 및 재발 방지에 필요한 조치를 하여야 한다. <개정 2022.6.10, 2026.3.31>

NoteBase

②

과학기술정보통신부장관은 침해사고의 원인 분석과 대책 마련을 거쳐 **공공기관등을 제외한 해당 정보통신서비스 제공자에게 필요한 조치의 이행을 명령할 수 있다**. 선지의 '권고'는 현행 규정과 다르다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제48조의4 제2항
정보통신망 이용촉진 및 정보보호 등에 관한 법률 제48조의4(침해사고의 원인 분석 등)
② 과학기술정보통신부장관은 정보통신서비스 제공자의 정보통신망에 침해사고가 발생하였거나 제48조의2제7항에 따른 침해사고조사심의위원회가 침해사고 발생 여부에 대한 조사가 필요하다고 인정하는 경우에는 그 침해사고의 발생 여부 및 원인을 분석하고 피해 확산 방지, 사고대응, 복구 및 재발 방지를 위한 대책을 마련하여 해당 정보통신서비스 제공자(공공기관등은 제외한다)에게 필요한 조치를 이행하도록 명령할 수 있다. <신설 2022.6.10, 2024.2.13, 2026.3.31>

③

과학기술정보통신부장관은 침해사고의 원인 분석과 대책 마련을 위하여 필요하면 정보통신서비스 제공자에게 **접속기록 등 관련 자료의 보전을 명할 수 있다**.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제48조의4 제5항
정보통신망 이용촉진 및 정보보호 등에 관한 법률 제48조의4(침해사고의 원인 분석 등)
⑤ 과학기술정보통신부장관은 제2항에 따른 침해사고의 발생 여부, 원인 분석 및 대책 마련을 위하여 필요하면 정보통신서비스 제공자에게 정보통신망의 접속기록 등 관련 자료의 보전을 명할 수 있다. <개정 2013.3.23, 2017.7.26, 2022.6.10, 2024.2.13, 2026.3.31>

④

제출받은 자료와 조사로 알게 된 정보는 **분석이 끝난 후 즉시 파기하여야 한다**. 재발 방지에 필요하다는 이유로 계속 보존할 수 없다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제48조의4 제7항
정보통신망 이용촉진 및 정보보호 등에 관한 법률 제48조의4(침해사고의 원인 분석 등)
⑦ 과학기술정보통신부장관이나 민 · 관합동조사단은 제6항에 따라 제출받은 자료와 조사를 통하여 알게 된 정보를 침해사고의 발생 여부 확인과 원인 분석 및 대책 마련 외의 목적으로는 사용하지 못하며, 분석이 끝난 후에는 즉시 파기하여야 한다. <개정 2013.3.23, 2017.7.26, 2022.6.10, 2024.2.13, 2026.3.31>

NoteBase

문 14. 전자상거래에서 소비자의 주문 정보와 지불 정보를 보호하기 위한 SET의 이중 서명은 소비자에서 상점으로 그리고 상점에서 금융기관으로 전달된다. 금융기관에서 이중 서명을 검증하는데 필요하지 않은 것은?

① 소비자의 공개키

② 주문 정보의 해시

③ 상점의 공개키

④ 지불 정보

정답 3번

간단한 해설

이중 서명은 소비자가 자신의 개인키로 생성하므로 검증에는 **소비자의 공개키**를 사용한다. 상점이 서명을 전달하더라도 서명자는 소비자이므로 **상점의 공개키는 필요하지 않다**.

선지별 해설

SET의 이중 서명은 주문 정보와 지불 정보 각각의 해시를 연결하고, 그 결과를 다시 해시한 뒤 소비자의 개인키로 서명한 것이다. 이를 통해 상점과 금융기관은 상대방에게만 공개되는 정보의 원문을 받지 않고도 두 정보가 같은 거래에 연결되어 있는지 확인할 수 있다.

① O: 소비자의 공개키는 이중 서명의 검증에 필요하다. 전자서명은 **서명에 사용한 개인키에 대응하는 공개키**로 검증하므로, 금융기관은 소비자의 공개키를 사용한다.

② O: 주문 정보의 해시는 이중 서명의 검증에 필요하다. 금융기관은 주문 정보 원문 대신 **주문 정보의 해시**를 전달받아, 자신이 지불 정보로부터 계산한 해시와 연결하여 검증용 해시를 만든다.

③ X: 상점의 공개키는 소비자의 이중 서명을 검증하는 데 필요하지 않다. 이중 서명의 서명자는 소비자이므로 **소비자의 공개키**가 필요하다. 상점의 공개키는 상점이 생성한 별도의 서명을 검증할 때 사용되며, 상점이 소비자의 이중 서명을 중계한다는 이유로 검증키가 바뀌지는 않는다.

④ O: 지불 정보는 이중 서명의 검증에 필요하다. 금융기관은 **지불 정보를 해시**한 뒤 주문 정보의 해시와 연결하고 다시 해시한다. 이렇게 계산한 값이 소비자의 이중 서명에 담긴 값과 일치하는지 확인하여 지불 정보의 무결성과 주문 정보와의 연결을 검증한다.

NoteBase

문 15. SHA-512 알고리즘의 수행 라운드 수와 처리하는 블록의 크기(비트 수)를 바르게 짝 지은 것은?

① 라운드 수: 64, 블록의 크기: 512

② 라운드 수: 64, 블록의 크기: 1024

③ 라운드 수: 80, 블록의 크기: 512

④ 라운드 수: 80, 블록의 크기: 1024

정답 4번

간단한 해설

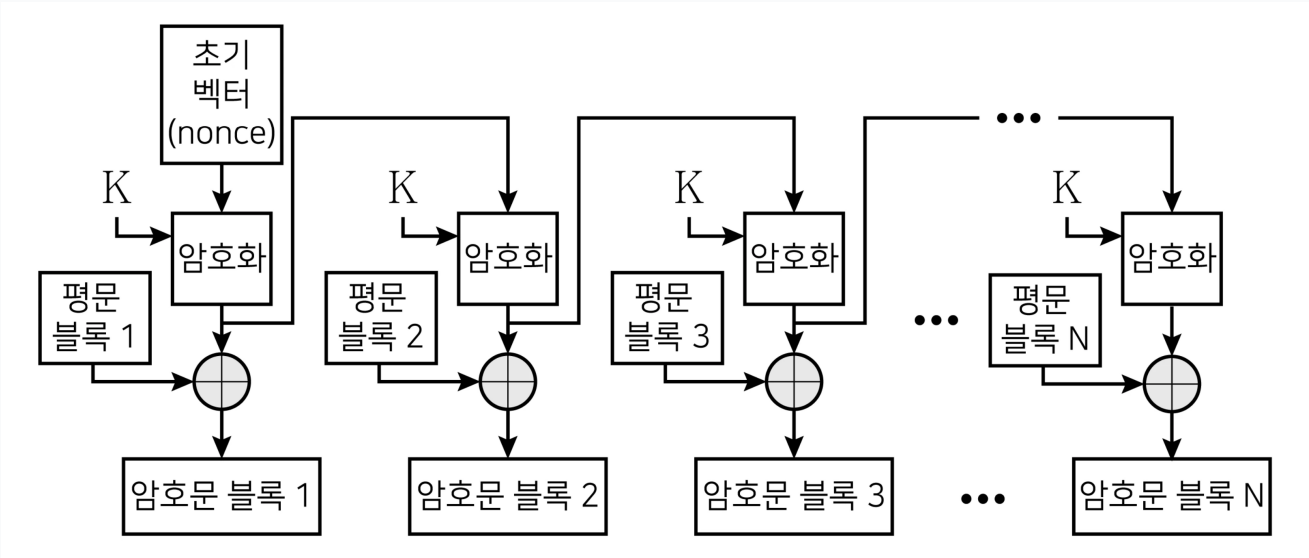
SHA-512는 **1024비트 블록**마다 **80라운드**의 압축 처리를 수행한다. 이름의 512는 입력 블록 크기가 아니라 출력 해시값의 길이이다.

공통 해설

SHA-512는 패딩을 마친 메시지를 1024비트 블록으로 나누고, 각 블록에 대해 80라운드의 압축 처리를 수행한다. 블록 크기는 한 번의 압축 처리에 들어가는 입력 단위의 길이이며, 라운드 수는 그 블록을 처리하면서 반복하는 연산 단계의 수이다. 따라서 이 알고리즘의 수행 라운드 수와 처리 블록 크기는 각각 80과 1024비트이다. SHA-512라는 이름에서 512는 **출력 해시값의 길이**를 나타내므로 **입력 블록 크기와 구별**해야 한다.

NoteBase

문 16. 다음 그림과 같이 암호화를 수행하는 블록 암호 운용 모드는? (단, ⊕: XOR, K: 암호키)



① CBC

② CFB

③ OFB

④ ECB

정답 3번

간단한 해설

그림에서 다음 암호화 단계로 이어지는 선은 **XOR 이전의 암호화 함수 출력**에서 갈라진다. 이 출력을 되먹임하여 키스트림을 만드는 방식이 OFB이다.

NoteBase

도식 해설

출력의 흐름: 초기 벡터를 암호키 K로 암호화한 출력은 두 갈래로 나뉜다. 한쪽은 평문 블록 1과 XOR되어 암호문 블록 1을 만들고, 다른 쪽은 다음 암호화 함수의 입력으로 들어간다. 이후에도 직전 암호화 함수의 출력을 다시 암호화하여 평문과 XOR할 키스트림을 만든다. 이처럼 **암호화 함수의 출력을 되먹임**하는 운용 모드가 OFB(Output Feedback)이다.

CFB와 구분: CFB(Cipher Feedback)는 평문과 XOR한 뒤 얻은 **암호문을 되먹임**한다. 그림의 되먹임 선은 아래쪽 암호문 블록에서 출발하지 않고 XOR 위쪽에서 갈라지므로 CFB와 구별된다.

CBC·ECB와 구분: CBC는 평문 블록과 이전 암호문 블록을 먼저 XOR한 뒤 그 결과를 암호화하며, 첫 블록에서는 이전 암호문 대신 초기 벡터를 사용한다. 따라서 그림처럼 암호화 함수의 출력과 평문을 XOR하는 배치와 다르다. ECB는 각 평문 블록을 독립적으로 암호화하므로 그림과 같은 블록 사이의 되먹임 연결이 없다.

NoteBase

문 17. 윈도우 최상위 레지스트리에 대한 설명으로 옳지 않은 것은?

① HKEY_LOCAL_MACHINE은 로컬 컴퓨터의 하드웨어와 소프트웨어의 설정을 저장한다.

② HKEY_CLASSES_ROOT는 파일 타입 정보와 관련된 속성을 저장하는 데 사용된다.

③ HKEY_CURRENT_USER는 현재 로그인한 사용자의 설정을 저장한다.

④ HKEY_CURRENT_CONFIG는 커널, 실행 중인 드라이버 또는 프로그램과 서비스에 의해 제공되는 성능 데이터를 실시간으로 제공한다.

정답 4번

간단한 해설

④의 '성능 데이터를 실시간으로 제공한다'는 **HKEY_PERFORMANCE_DATA**에 대한 설명이다. HKEY_CURRENT_CONFIG는 로컬 컴퓨터의 **현재 하드웨어 프로필 정보**를 제공한다.

선지별 해설

① O: HKEY_LOCAL_MACHINE은 **컴퓨터 전체에 적용되는 하드웨어·소프트웨어 설정**을 저장한다. 설치된 장치와 소프트웨어, 시스템 구성 등에 관한 정보가 포함되므로 특정 사용자의 개인 설정과 구별된다.

② O: HKEY_CLASSES_ROOT는 **파일 형식과 그 형식에 연결된 속성**을 저장한다. 예를 들어 파일 확장자에 따른 형식과 해당 파일을 여는 프로그램의 연결 정보를 관리하는 데 사용된다.

③ O: HKEY_CURRENT_USER는 **현재 로그인한 사용자에게 적용되는 설정**을 저장한다. 화면 색상, 프린터, 응용 프로그램의 개인별 환경 설정 등이 해당하므로 컴퓨터 전체의 설정을 다루는 HKEY_LOCAL_MACHINE과 구별된다.

④ X: HKEY_CURRENT_CONFIG는 로컬 컴퓨터의 **현재 하드웨어 프로필 정보**를 제공한다. 성능 데이터에 접근하는 키는 **HKEY_PERFORMANCE_DATA**이다. 성능 데이터는 일반 설정값처럼 레지스트리에 저장된 내용을 읽는 것이 아니라, 레지스트리 함수를 통해 조회할 때 시스템이 원천에서 수집하여 제공한다. 따라서 선지의 키 이름을 HKEY_PERFORMANCE_DATA로 고쳐야 한다.

NoteBase

문 18. SSH(Secure Shell)의 전송 계층 프로토콜에 의해 제공되는 서비스가 아닌 것은?

① 서버 인증

② 데이터 기밀성

③ 데이터 무결성

④ 논리 채널 다중화

정답 4번

간단한 해설

논리 채널 다중화는 하나의 암호화된 연결에서 여러 논리 채널을 함께 사용하는 기능으로, SSH의 **연결 프로토콜**이 제공한다. 전송 계층 프로토콜은 서버 인증과 데이터의 기밀성·무결성을 제공한다.

선지별 해설

① O: 서버 인증은 클라이언트가 접속 상대가 의도한 서버인지 확인하는 기능이다. SSH 전송 계층 프로토콜은 서버의 호스트 키를 이용한 암호학적 인증으로 **서버의 신원**을 확인한다.

② O: 데이터 기밀성은 통신 내용을 권한 없는 사람이 알아볼 수 없도록 보호하는 성질이다. SSH 전송 계층 프로토콜은 전송 데이터를 **암호화**하여 도청으로부터 내용을 보호한다.

③ O: 데이터 무결성은 전송 중 데이터가 무단으로 변경되었는지 확인할 수 있게 하는 성질이다. SSH 전송 계층 프로토콜은 메시지 인증 코드(MAC) 등의 무결성 보호 기법으로 **데이터 변조를 탐지**한다.

④ X: 논리 채널 다중화는 SSH 전송 계층 프로토콜이 아니라 **연결 프로토콜**이 제공한다. 하나의 암호화된 연결 위에서 원격 명령 실행이나 포트 포워딩 등의 통신을 서로 다른 논리 채널로 구분하여 함께 전송하는 기능이다.

NoteBase

문 19. 리눅스 배시 셸(Bash shell) 특수 문자와 그 기능에 대한 설명이 옳지 않은 것은?

① 특수 문자: ~, 기능: 작업 중인 사용자의 홈 디렉터리를 나타냄

② 특수 문자: " ", 기능: 문자(" ") 안에 있는 모든 셸 특수 문자의 기능을 무시

③ 특수 문자: ;, 기능: 한 행의 여러 개 명령을 구분하고 왼쪽부터 차례로 실행

④ 특수 문자: |, 기능: 왼쪽 명령의 결과를 오른쪽 명령의 입력으로 전달

정답 2번

간단한 해설

큰따옴표는 안에 있는 모든 셸 특수 문자의 기능을 없애지 않는다. 큰따옴표 안에서도 **변수 확장과 명령 치환**은 수행되므로 $로 시작하는 표현 등이 해석된다.

선지별 해설

① O: 따옴표로 감싸지 않은 ~가 단어의 맨 앞에 단독으로 쓰이거나 ~/ 형태로 쓰이면 **현재 사용자의 홈 디렉터리 경로로 확장**된다. 따라서 cd ~는 현재 사용자의 홈 디렉터리로 이동하는 명령이다.

② X: 큰따옴표는 공백을 포함한 문자열을 하나의 인수로 묶고 일부 특수 문자 해석을 막지만, **변수 확장과 명령 치환은 허용**한다. 예를 들어 echo "$HOME"은 $HOME이라는 글자를 그대로 출력하는 대신 홈 디렉터리 경로를 출력한다. $(명령) 형태의 명령 치환도 큰따옴표 안에서 수행된다. 안에 있는 문자를 모두 문자 그대로 취급하는 것은 작은따옴표이다.

③ O: 세미콜론(;)은 같은 행에 적은 여러 명령을 구분하며 **앞 명령이 끝나면 다음 명령을 실행**하게 한다. 앞 명령의 성공 여부와 관계없이 다음 명령을 실행한다는 점에서, 앞 명령이 성공했을 때만 다음 명령을 실행하는 &&와 구별된다.

④ O: 파이프(|)는 왼쪽 명령의 **표준 출력을 오른쪽 명령의 표준 입력**에 연결한다. 따라서 왼쪽 명령이 출력한 데이터를 오른쪽 명령이 받아 처리할 수 있다. 일반적인 | 연결에는 왼쪽 명령의 표준 오류가 포함되지 않는다.

NoteBase

문 20. ISMS-P 인증 기준 중 사고 예방 및 대응 분야의 점검 항목만을 모두 고르면?

ㄱ. 백업 및 복구 관리
ㄴ. 취약점 점검 및 조치
ㄷ. 이상행위 분석 및 모니터링
ㄹ. 재해 복구 시험 및 개선

① ㄱ, ㄴ
② ㄱ, ㄹ
③ ㄴ, ㄷ
④ ㄷ, ㄹ

정답 3번

간단한 해설

취약점을 찾아 조치하고 침해 징후를 탐지하는 활동은 **사고 예방 및 대응** 분야에 속한다. 반면 백업 및 복구 관리는 시스템 및 서비스 운영관리, 재해 복구 시험 및 개선은 재해 복구 분야로 구분된다.

보기별 해설

ㄱ. X: '백업 및 복구 관리'(2.9.3)는 **시스템 및 서비스 운영관리** 분야의 항목이다. 정보시스템의 가용성과 데이터 무결성을 유지하도록 백업 대상·주기·방법·보관 장소 등의 절차를 정하고, 사고 발생 시 복구할 수 있도록 관리하는 내용이다. 복구를 다룬다는 이유만으로 사고 예방 및 대응 분야에 넣지 않는다.

ㄴ. O: '취약점 점검 및 조치'(2.11.2)는 사고 예방 및 대응 분야의 항목이다. 정보시스템에 노출된 보안 취약점을 정기적으로 점검하고 발견된 취약점을 신속하게 조치하여 **침해사고에 악용될 가능성을 줄인다**. 새로 발견되는 취약점도 지속적으로 파악하고 시스템에 미치는 영향을 분석하여 조치한다.

ㄷ. O: '이상행위 분석 및 모니터링'(2.11.3)은 사고 예방 및 대응 분야의 항목이다. 네트워크와 데이터 흐름 등을 수집·분석하여 침해 시도, 개인정보 유출 시도, 부정행위 등을 **신속하게 탐지하고 대응**하며, 점검 결과에 따라 사후조치를 수행하는 내용이다.

ㄹ. X: '재해 복구 시험 및 개선'(2.12.2)은 **재해 복구** 분야의 항목이다. 재해 복구 전략과 대책이 적절한지 정기적으로 시험하고, 시험 결과와 시스템 환경·법규 등의 변화를 반영하여 보완한다. 사고 예방 및 대응 분야의 '사고 대응 훈련 및 개선'(2.11.4)과 구분해야 한다.

사고 예방 및 대응 분야에 속하는 항목은 ㄴ과 ㄷ이며, 이 조합은 ③에 해당한다.

NoteBase