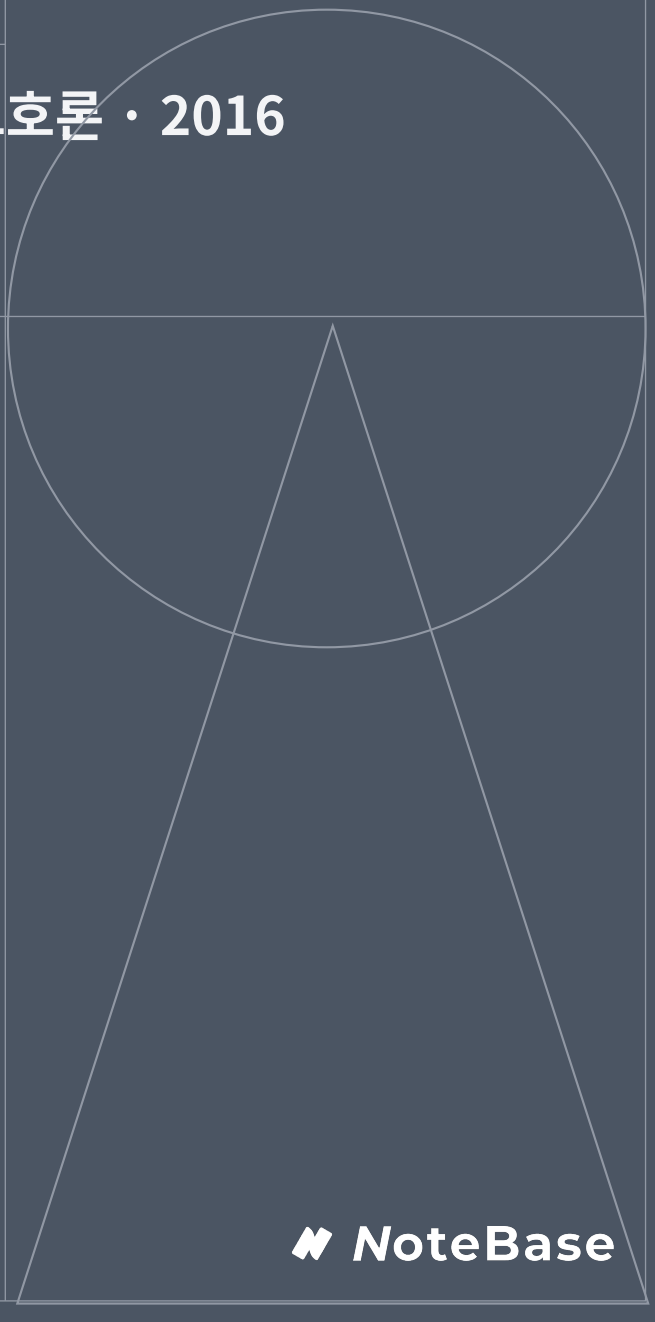
기출OX 해설집

공무원/국회직/9급 · 정보보호론 · 2016



NoteBase

기출OX 해설집

공무원/국회직/9급 · 정보보호론 · 2016

공무원/국회직/9급 · 정보보호론 · 2016

1. 정보보호시스템이 제공하는 보안서비스 개념과 그에 대한 설명으로 옳은 것은?

ㄱ. 기밀성(Confidentiality): 데이터가 위·변조되지 않아야 함
ㄴ. 무결성(Integrity): 권한이 있는 자는 서비스를 사용하여야 함
ㄷ. 인증(Authentication): 정당한 자임을 상대방에게 입증하여야 함
ㄹ. 부인방지(Nonrepudiation): 거래사실을 부인할 수 없어야 함
ㅁ. 가용성(Availability): 비인가자에게는 메시지를 숨겨야 함

① ㄱ, ㄴ
② ㄱ, ㅁ
③ ㄴ, ㄷ
④ ㄷ, ㄹ
⑤ ㄹ, ㅁ

정답 4번

출제 포인트

정보보호시스템이 제공하는 기밀성, 무결성, 인증, 부인방지, 가용성의 정의를 구별하는 문제이다.

NoteBase

기출OX 해설집 · 공무원/국회직/9급 · 정보보호론 · 2016

핵심 개념

기밀성(Confidentiality): 허가받지 않은 자가 정보에 접근하거나 정보를 알아보지 못하게 하는 성질이다. 키워드는 비밀 유지와 비인가 공개 방지이다.
무결성(Integrity): 정보가 권한 없이 위조·변조·삭제되지 않고 정확하고 완전하게 유지되는 성질이다. 키워드는 변경 방지이다.
인증(Authentication): 통신 상대방이나 사용자가 주장하는 정당한 신원인지 확인하는 기능이다. 키워드는 신원 확인이다.
부인방지(Nonrepudiation): 송신, 수신 또는 거래에 관여한 당사자가 나중에 그 사실을 부인하지 못하게 하는 기능이다. 키워드는 행위 사실의 증명이다.
가용성(Availability): 권한 있는 사용자가 필요할 때 정보와 서비스를 정상적으로 이용할 수 있는 성질이다. 키워드는 적시 이용이다.
ㄱ의 '위·변조되지 않아야 함'은 무결성, ㄴ의 '권한 있는 자가 서비스를 이용함'은 가용성, ㅁ의 '비인가자에게 메시지를 숨김'은 기밀성에 해당한다. 따라서 ㄷ과 ㄹ만 옳다.

선지별 해설

① X — ㄱ과 ㄴ은 모두 개념명이 바뀌었다. ㄱ의 '데이터가 위·변조되지 않아야 함'은 기밀성이 아니라 무결성이고, ㄴ의 '권한 있는 자가 서비스를 이용함'은 무결성이 아니라 가용성에 관한 설명이다. 올바른 조합은 ㄷ, ㄹ이다.
② X — ㄱ은 무결성의 설명이고, ㅁ은 기밀성의 설명이므로 두 문장 모두 제시된 개념명과 맞지 않는다. 올바른 조합은 ㄷ, ㄹ이다.
③ X — ㄷ은 정당한 자임을 확인하는 인증의 설명으로 옳지만, ㄴ은 무결성의 설명이 아니다. 무결성은 데이터의 비인가 위·변조를 막고 정확성과 완전성을 유지하는 성질이다. 올바른 조합은 ㄷ, ㄹ이다.
④ O — ㄷ은 상대방의 정당한 신원을 확인하는 인증이고, ㄹ은 거래 당사자가 거래 사실을 사후에 부인하지 못하게 하는 부인방지이므로 두 문장 모두 옳다.
⑤ X — ㄹ은 부인방지의 설명으로 옳지만, ㅁ의 '비인가자에게 메시지를 숨겨야 함'은 가용성이 아니라 기밀성이다. 가용성은 권한 있는 사용자가 필요할 때 정보나 서비스를 이용할 수 있는 성질이다. 올바른 조합은 ㄷ, ㄹ이다.

오답 포인트

ㄱ의 '위·변조'와 ㅁ의 '숨김'을 개념명만 보고 지나치기 쉽다. 위·변조 방지는 무결성이고 비인가자에게 내용을 숨기는 것은 기밀성이다. 또한 권한 있는 사용자의 필요 시 이용은 가용성에 연결된다.

다시 나오면 이렇게 판단

선지의 핵심 동사를 찾으면 된다. 숨기고 공개를 막으면 기밀성, 바뀌거나 훼손되지 않게 하면 무결성, 신원을 확인하면 인증, 행위 사실을 부인하지 못하게 하면 부인방지, 필요할 때 이용하게 하면 가용성으로 판단한다.

NoteBase

암기 포인트

기밀성은 숨김, 무결성은 변경 방지, 인증은 신원 확인, 부인방지는 부인 차단, 가용성은 필요할 때 이용이다.

NoteBase

2. 서버 관리자가 해커의 공격이 발생하고 있음을 감지하고 tcpdump 프로그램으로 네트워크 패킷을 캡처하였다. 다음의 요약된 캡처 정보가 나타내는 공격으로 옳은 것은?

```
13:07:13. 639870 192.168.1.73.2321 > 192.168.1.73.http ...
13:07:13. 670484 192.168.1.73.2321 > 192.168.1.73.http ...
13:07:13. 685593 192.168.1.73.2321 > 192.168.1.73.http ...
13:07:13. 693481 192.168.1.73.2321 > 192.168.1.73.http ...
13:07:13. 712833 192.168.1.73.2321 > 192.168.1.73.http ...
```

① Smudge 공격
② LAND 공격
③ Ping of Death 공격
④ Smurf 공격
⑤ Port Scan 공격

정답 2번

출제 포인트

tcpdump에 나타난 출발지 IP와 목적지 IP의 관계를 보고 LAND 공격을 식별하는 문제이다.

핵심 개념

LAND 공격은 공격 대상의 IP 주소를 출발지 주소로 위조하고 목적지도 같은 공격 대상으로 설정하여, 피해 시스템이 자기 자신에게서 온 것처럼 보이는 패킷을 처리하게 만드는 서비스 거부 공격이다.
캡처에서는 출발지와 목적지가 모두 192.168.1.73으로 같다. 이 동일한 IP 주소가 LAND 공격을 판별하는 핵심 단서이다.
Smudge 공격은 터치스크린 등에 남은 손자국으로 비밀번호나 잠금 패턴을 추정하는 공격이다. Ping of Death는 비정상적으로 큰 ICMP 패킷을 이용하며, Smurf 공격은 피해자의 IP를 출발지로 위조한 ICMP 요청을 브로드캐스트 주소로 보내 응답을 증폭한다. Port Scan은 여러 포트에 접속을 시도하여 열려 있는 서비스를 탐색한다.

NoteBase

선지별 해설

① X — Smudge 공격은 화면이나 입력 장치에 남은 흔적으로 비밀번호·잠금 패턴을 추정하는 공격이므로, 동일한 출발지·목적지 IP가 나타난 패킷 캡처와 맞지 않는다. 올바르게는 이 캡처가 LAND 공격의 특징을 나타낸다고 해야 한다.
② O — 각 패킷의 출발지 IP와 목적지 IP가 모두 192.168.1.73으로 동일하다. 공격 대상의 주소를 출발지로 위조하여 같은 주소로 보내는 LAND 공격의 특징에 해당한다.
③ X — Ping of Death 공격은 허용 범위를 넘거나 비정상적으로 조작된 큰 ICMP 패킷으로 시스템 장애를 유발하는 공격이다. 캡처에는 ICMP나 비정상적 패킷 크기에 관한 단서가 없다. 올바르게는 비정상적으로 큰 ICMP 패킷이 확인될 때 Ping of Death로 판단한다.
④ X — Smurf 공격은 피해자의 IP를 출발지로 위조한 ICMP Echo Request를 브로드캐스트 주소로 보내 다수 호스트의 응답이 피해자에게 몰리게 하는 공격이다. 캡처에는 ICMP와 브로드캐스트 목적지라는 특징이 없다. 올바르게는 위조된 피해자 출발지 IP, ICMP 요청, 브로드캐스트 목적지가 함께 나타나야 Smurf 공격으로 판단한다.
⑤ X — Port Scan 공격은 한 대상의 여러 포트에 차례로 접속하여 열린 포트와 서비스를 탐색하는 공격이다. 캡처에서는 목적지 서비스가 모두 http로 같고 여러 포트를 탐색한 흔적이 없다. 올바르게는 여러 목적지 포트에 대한 반복적인 접속 시도가 나타날 때 Port Scan으로 판단한다.

오답 포인트

짧은 시간에 패킷이 반복된다는 이유만으로 Port Scan이나 일반적인 트래픽 폭주 공격을 고르면 안 된다. 이 문항의 결정적 단서는 반복 횟수가 아니라 출발지 IP와 목적지 IP가 192.168.1.73으로 동일하다는 점이다.

다시 나오면 이렇게 판단

패킷 캡처 문제에서는 먼저 출발지와 목적지의 주소·프로토콜·포트를 비교한다. 출발지 IP와 목적지 IP가 공격 대상의 동일한 주소이면 LAND, ICMP의 비정상적 크기이면 Ping of Death, 위조 출발지와 브로드캐스트 목적지이면 Smurf, 여러 목적지 포트로의 접속이면 Port Scan으로 구분한다.

암기 포인트

LAND는 출발지와 목적지가 같은 땅, 즉 같은 IP이다.

NoteBase

3. 메시지 인증 코드와 전자서명에 대한 설명으로 옳은 것은?

① 전자서명은 대칭키가 사전에 교환되어야 사용할 수 있다.
② 메시지 인증 코드와 전자서명 모두 무결성과 부인방지 기능을 제공한다.
③ 전자서명은 서명 생성자를 인증하는 기능이 있다.
④ 메시지 인증 코드값을 검증하는 데 공개키가 필요하다.
⑤ 전자서명은 서명-후-해시(Sign-then-Hash) 방식이다.

정답 3번

출제 포인트

메시지 인증 코드와 전자서명이 사용하는 키, 제공하는 보안 기능, 생성·검증 절차의 차이를 묻는 문제이다.

핵심 개념

메시지 인증 코드(MAC): 송신자와 수신자가 공유한 비밀키와 메시지로 인증값을 만들어 메시지의 무결성과 출처 인증을 확인하는 방식이다. 양쪽이 같은 비밀키를 알기 때문에 제3자에 대한 부인방지는 제공하지 못한다.
전자서명: 서명자가 자신의 개인키로 서명하고 검증자가 서명자의 공개키로 검증하는 방식이다. 메시지의 무결성, 서명자 인증, 부인방지를 제공한다. 일반적으로 메시지를 먼저 해시하고 그 해시값에 서명하는 해시-후-서명(Hash-then-Sign) 방식이다.
핵심 차이: MAC은 공유 비밀키를 사용하고, 전자서명은 서명자의 개인키와 공개키 쌍을 사용한다.

선지별 해설

① X — 틀린 표현은 '대칭키가 사전에 교환되어야'이다. 전자서명은 대칭키를 사전 교환하는 방식이 아니라, 서명자가 개인키로 서명하고 검증자가 공개키로 검증한다.
② X — 틀린 표현은 '모두 무결성과 부인방지 기능을 제공한다'이다. 두 방식 모두 무결성을 확인할 수 있지만, 공유 비밀키를 쓰는 메시지 인증 코드는 송신자와 수신자 모두 같은 인증값을 만들 수 있으므로 부인방지를 제공하지 못한다. 부인방지는 전자서명이 제공한다.
③ O — 전자서명은 서명자의 개인키로 생성되고 그에 대응하는 공개키로 검증되므로, 서명 생성자가 해당 개인키의 소유자임을 인증하는 기능이 있다.
④ X — 틀린 표현은 '공개키가 필요하다'이다. 메시지 인증 코드값의 검증에는 송신자와 수신자가 공유한 비밀키가 필요하며, 공개키는 전자서명 검증에 사용된다.
⑤ X — 틀린 표현은 '서명-후-해시(Sign-then-Hash)'이다. 전자서명은 일반적으로 메시지를 먼저 해시한 뒤 그 해시값에 서명하는 해시-후-서명(Hash-then-Sign) 방식이다.

NoteBase

오답 포인트

②는 무결성과 부인방지를 한 묶음으로 제시해 두 방식이 같은 기능을 제공하는 것처럼 보이게 한다. MAC의 공유 비밀키는 통신 상대방도 알고 있으므로 누가 인증값을 만들었는지 제3자에게 입증하기 어렵고, 이 때문에 부인방지가 성립하지 않는다. 또한 ④의 공개키와 ⑤의 처리 순서를 전자서명의 특징과 반대로 바꾼 점이 함정이다.

다시 나오면 이렇게 판단

키의 소유 관계를 먼저 확인한다. 공유 비밀키이면 메시지 인증 코드로 보아 무결성과 출처 인증은 가능하지만 부인방지는 불가능하다고 판단한다. 개인키로 서명하고 공개키로 검증하면 전자서명으로 보아 서명자 인증과 부인방지가 가능하다고 판단한다. 서명 순서는 '메시지 해시 후 해시값에 서명'으로 판단한다.

암기 포인트

MAC은 공유키·부인방지 불가, 전자서명은 개인키 서명·공개키 검증·해시 후 서명이다.

NoteBase

4. 아래 그림은 TLS(Transport Layer Security)를 통해 쇼핑몰에 로그인하는 화면이다. 이에 대한 설명으로 옳지 않은 것은?



① TLS는 현재 1.1 버전까지 발표되었다.
② TLS는 SSL을 기반으로 한 IETF 인터넷 표준이다.
③ 서버 인증서를 통해 서버를 인증하고 키교환을 한다.
④ 상호 교환된 키로 사용자의 패스워드는 암호화된다.
⑤ 주소창에 있는 자물쇠를 클릭하면 서버 인증서를 볼 수 있다.

정답 1번

출제 포인트

TLS의 표준화 계보, 최신 버전, 서버 인증, 키 교환, 통신 암호화 및 인증서 확인 기능을 구분하는 문제이다.

핵심 개념

TLS는 인터넷 통신에서 상대방을 인증하고, 안전하게 세션 키를 합의한 뒤, 그 키로 송수신 데이터를 암호화하고 무결성을 보호하는 보안 프로토콜이다. SSL을 계승하여 IETF가 표준화했으며, 이 문항의 출제 시점인 2016년에는 TLS 1.2까지 표준화되어 있었다. TLS 1.3은 이후 2018년에 표준화되었으며, 현재 TLS 1.0과 1.1은 사용 중단이 권고된 구버전이다.

NoteBase

선지별 해설

① X
틀린 표현은 '현재 1.1 버전까지 발표되었다'이다. 이 문항의 출제 시점인 2016년에는 TLS 1.2가 이미 표준화되어 있었으므로, 올바르게는 'TLS는 1.2 버전까지 발표되었다'이다. TLS 1.3은 이후 2018년에 표준화되었으며, 현재 TLS 1.0과 1.1은 폐기된 구버전이다.

② O
TLS는 SSL을 계승해 IETF가 표준화한 인터넷 보안 프로토콜이므로 옳다.

③ O
TLS 핸드셰이크에서는 서버 인증서로 접속 대상 서버의 신원을 확인하고, 인증된 키 교환을 통해 이후 통신에 사용할 세션 키를 합의하므로 옳다.

④ O
로그인 폼에 입력한 패스워드는 HTTPS 연결에서 합의된 대칭 세션 키로 암호화되는 애플리케이션 데이터에 포함되므로 네트워크 구간에서 평문으로 전송되지 않는다.

⑤ O
브라우저의 주소창 보안 표시를 열면 해당 사이트가 제시한 서버 인증서의 발급 대상, 발급자, 유효기간 등의 정보를 확인할 수 있으므로 옳다.

오답 포인트

①의 '1.1'은 오래된 버전 정보를 이용한 함정이다. TLS 1.1이 실제로 존재한다는 사실과 TLS의 최신 표준 버전을 혼동하면 안 된다. 또한 HTTPS는 패스워드만 따로 암호화하는 것이 아니라 로그인 요청을 포함한 통신 데이터를 TLS로 보호한다.

다시 나오면 이렇게 판단

TLS 문항에서는 먼저 버전 계보를 SSL → TLS 1.0 → 1.1 → 1.2 → 1.3으로 확인한다. 이어서 서버 인증서는 서버 신원 확인과 키 교환 인증에, 합의된 세션 키는 실제 데이터의 대칭키 암호화에 쓰인다는 역할 구분으로 선지를 판단한다.

암기 포인트

TLS 1.3까지 표준화, 인증서는 서버 확인, 세션 키는 데이터 보호이다.

NoteBase

5. TPM(Trusted Platform Module)에 대한 설명으로 옳지 않은 것은?

① 하드웨어 기반으로 안전한 저장공간과 실행영역을 제공한다.
② 난수발생기, 암·복호화 엔진, RSA 키 생성기 등을 포함한다.
③ 비휘발성 메모리 영역에 최상위 루트 키가 탑재된다.
④ 단계적으로 인증된 절차로 운영체제가 부팅되도록 한다.
⑤ 국내 공인인증서 저장 시 서명키를 저장하는 표준방식이다.

정답 5번

출제 포인트

TPM이 제공하는 하드웨어 기반 신뢰 기능과 전자서명용 개인키 저장 방식에 관한 설명을 구별하는 문제이다.

핵심 개념

TPM은 암호키의 생성·보호, 안전한 저장 영역, 플랫폼 무결성 측정 등을 제공하는 하드웨어 보안 모듈이다. 비휘발성 메모리에 신뢰의 출발점이 되는 키를 보유하고, 부팅 단계의 측정값을 연쇄적으로 기록하여 신뢰된 부팅을 지원한다. 다만 특정 인증서의 서명키를 반드시 TPM에 저장해야 한다는 국내 인증서 표준방식을 뜻하지는 않는다.

선지별 해설

① O — TPM은 소프트웨어와 분리된 하드웨어 기반의 보호 영역에서 키와 보안 정보를 다루므로 안전한 저장공간과 보호된 암호 연산 환경을 제공한다.
② O — TPM에는 난수 생성 기능과 암호화·복호화 및 키 생성에 사용되는 암호 기능이 포함되며, RSA 키 생성도 지원할 수 있다.
③ O — 전원이 꺼져도 유지되는 비휘발성 메모리 영역에는 최상위 신뢰점 역할을 하는 루트 키가 저장될 수 있다.
④ O — TPM은 각 부팅 단계의 측정값을 다음 단계로 연쇄 확장하여 기록함으로써 운영체제가 단계적으로 검증된 절차에 따라 부팅되도록 지원한다.
⑤ X — 틀린 표현은 '국내 공인인증서 저장 시 서명키를 저장하는 표준방식'이다. TPM은 범용 하드웨어 보안 모듈이며, 특정 국내 인증서의 서명키 저장을 위한 표준방식 자체가 아니다. 올바르게는 'TPM은 서명키를 포함한 암호키를 하드웨어 기반으로 생성·보호하고 플랫폼 무결성을 검증하는 데 활용할 수 있다'이다.

오답 포인트

⑤는 TPM이 개인키 보호에 활용될 수 있다는 사실을 '국내 공인인증서 서명키 저장의 표준방식'이라고 과도하게 일반화한다. 활용 가능성과 특정 인증 체계의 표준방식은 서로 다른 의미이다.

NoteBase

다시 나오면 이렇게 판단

선지에 하드웨어 신뢰점, 키 생성·보호, 난수 생성, 비휘발성 저장, 부팅 무결성 측정이 나오면 TPM의 대표 기능으로 판단한다. 반대로 특정 국가의 인증서 저장 제도나 고정된 저장 방식이라고 단정하면 TPM의 범용 기능과 구별한다.

암기 포인트

TPM은 '키 보호 + 하드웨어 신뢰점 + 부팅 무결성'이며, 특정 국내 인증서 저장방식 그 자체는 아니다.

NoteBase

6. CPU의 NX(No-Execute) 비트 기술을 활용하여 효과적으로 차단할 수 있는 공격 유형으로 옳은 것은?

① Cross-Site Scripting 공격
② Denial of Service 공격
③ ARP Spoofing 공격
④ SQL Injection 공격
⑤ Buffer Overflow 공격

정답 5번

출제 포인트

CPU의 NX(No-Execute) 비트가 데이터용 메모리 영역의 명령어 실행을 금지한다는 점과, 이 기능이 코드 실행형 메모리 공격에 대응한다는 점을 묻는 문제이다.

핵심 개념

NX 비트는 스택이나 힙처럼 데이터가 저장되는 메모리 영역을 실행 불가로 표시하여, 그 영역에 주입된 공격 코드를 CPU가 명령어로 실행하지 못하게 하는 기술이다.
버퍼 오버플로 공격은 정해진 크기를 넘는 데이터를 입력하여 인접 메모리나 제어 정보를 훼손하는 공격이다. 공격자가 버퍼에 악성 코드를 넣고 실행 흐름을 그 코드로 돌리는 전통적인 코드 주입형 버퍼 오버플로는 NX 비트로 효과적으로 차단할 수 있다.

선지별 해설

① X — Cross-Site Scripting 공격은 웹 애플리케이션이 검증하지 않은 스크립트를 웹 페이지에 포함시켜 사용자의 브라우저에서 실행하게 하는 공격이다. 틀린 표현은 NX 비트로 이를 차단할 수 있다는 점이다. 올바르게는 입력값 검증, 출력 인코딩, 콘텐츠 보안 정책 등으로 대응한다.
② X — Denial of Service 공격은 과도한 요청이나 자원 고갈로 서비스의 가용성을 떨어뜨리는 공격이다. 틀린 표현은 NX 비트로 이를 차단할 수 있다는 점이다. 올바르게는 트래픽 필터링, 요청 제한, 자원 격리 등의 가용성 보호 대책으로 대응한다.
③ X — ARP Spoofing 공격은 위조된 ARP 정보를 전달하여 IP 주소와 MAC 주소의 대응 관계를 속이는 네트워크 공격이다. 틀린 표현은 NX 비트로 이를 차단할 수 있다는 점이다. 올바르게는 동적 ARP 검사, 정적 ARP 설정 등의 네트워크 계층 대책으로 대응한다.
④ X — SQL Injection 공격은 입력값을 통해 악의적인 SQL 구문이 데이터베이스 질의에 포함되게 하는 공격이다. 틀린 표현은 NX 비트로 이를 차단할 수 있다는 점이다. 올바르게는 매개변수화된 질의와 입력값 검증 등으로 대응한다.
⑤ O — Buffer Overflow 공격 중 스택이나 힙에 공격 코드를 주입한 뒤 그 영역으로 실행 흐름을 바꾸는 방식은 NX 비트가 해당 영역의 실행을 금지하므로 효과적으로 차단할 수 있다.

NoteBase

오답 포인트

NX를 모든 악성 코드나 모든 입력 공격을 막는 기술로 확대 해석하기 쉽다. NX의 차단 기준은 공격 이름 자체가 아니라 데이터 영역에 들어간 코드를 CPU가 실행하려 하는지 여부이다. 또한 NX는 코드 재사용 공격 등 모든 버퍼 오버플로 기법을 완전히 제거하는 기술은 아니다.

다시 나오면 이렇게 판단

선지의 공격이 스택·힙 같은 데이터 영역에 코드를 주입하고 그곳에서 실행하는 방식인지 확인한다. 그렇다면 NX의 직접적인 방어 대상이고, 웹 입력 검증·데이터베이스 질의·네트워크 주소 위조·서비스 가용성 문제라면 별도의 보안 대책이 필요하다.

암기 포인트

NX는 데이터 영역의 실행을 막아 코드 주입형 버퍼 오버플로를 차단한다.

NoteBase

7. IPsec에 대한 설명으로 옳지 않은 것은?

① IPsec 정책 설정 과정에서 송·수신자의 IP주소를 입력한다.
② AH(Authentication Header) 프로토콜은 무결성을 제공한다.
③ 트랜스포트(Transport) 모드에서는 IP헤더도 암호화된다.
④ 재전송 공격을 막기 위해 IP패킷별로 순서번호를 부여한다.
⑤ IKE(Internet Key Exchange) 프로토콜로 세션키를 교환한다.

정답 3번

출제 포인트

이 문제는 IPsec의 정책 설정, AH의 보안 기능, 전송 모드의 보호 범위, 재전송 공격 방지, IKE의 역할을 구분하는 문제이다.

핵심 개념

IPsec: IP 계층에서 패킷을 인증하거나 암호화하여 통신을 보호하는 보안 체계이다.
AH: 패킷의 무결성과 송신자 인증을 제공하지만 기밀성은 제공하지 않는다.
전송 모드: 원래의 IP 헤더는 유지하고 그 뒤의 상위 계층 데이터 부분을 보호하는 방식이다.
IKE: 통신 당사자를 인증하고 보안 연관을 협상하며 IPsec에 사용할 키를 교환·생성하는 프로토콜이다.

NoteBase

선지별 해설

① O
IPsec 정책은 어떤 트래픽에 보안을 적용할지를 식별해야 하므로 송신지와 수신지의 IP 주소 등을 선택 조건으로 설정한다.

② O
AH는 패킷이 전송 중 변경되지 않았는지를 확인하는 무결성 기능을 제공한다. 다만 데이터를 암호화하지 않으므로 기밀성은 제공하지 않는다.

③ X
틀린 표현은 '트랜스포트 모드에서는 IP 헤더도 암호화된다'이다. 전송 모드에서는 원래의 IP 헤더를 암호화하지 않고, ESP를 사용할 때 IP 헤더 뒤의 상위 계층 데이터가 암호화된다.

④ O
IPsec은 보안 연관별로 패킷에 증가하는 순서번호를 부여하고 수신 측의 재전송 방지 창으로 중복되거나 지나치게 오래된 패킷을 걸러 재전송 공격을 방지한다.

⑤ O
IKE는 IPsec 통신에 필요한 보안 연관을 협상하고 세션에서 사용할 키 자료를 안전하게 교환·생성한다.

오답 포인트

③은 전송 모드와 터널 모드의 보호 범위를 뒤바꾼 선지이다. 전송 모드는 원래의 IP 헤더를 그대로 두며, 터널 모드는 원래의 IP 패킷 전체를 보호한 뒤 새로운 외부 IP 헤더를 붙인다.

다시 나오면 이렇게 판단

'원래의 IP 헤더까지 암호화되는가'를 기준으로 모드를 구분한다. 전송 모드는 원래 IP 헤더를 유지하고 페이로드를 보호하며, 터널 모드는 원래 IP 패킷 전체를 캡슐화하여 보호한다.

암기 포인트

AH는 인증·무결성, ESP는 암호화, 전송 모드는 페이로드 보호, 터널 모드는 원래 IP 패킷 전체 보호, IKE는 협상·키 교환이다.

NoteBase

8. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 규정하는 정보보호 관리체계의 인증권자와 개인정보보호 관리체계의 인증권자를 순서대로 나열한 것으로 옳은 것은?

① 미래창조과학부장관, 방송통신위원회
② 미래창조과학부장관, 한국인터넷진흥원
③ 방송통신위원회, 방송통신위원회
④ 방송통신위원회, 한국인터넷진흥원
⑤ 한국인터넷진흥원, 한국인터넷진흥원

정답 1번

쟁점

이 문제는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 정한 두 관리체계의 인증권자를 구별하는 문제이다. 핵심은 정보보호 관리체계와 개인정보보호 관리체계의 담당 기관을 순서대로 정확히 연결하는 것이다.

용어 풀이

정보보호 관리체계는 정보통신망의 안정성과 신뢰성을 확보하기 위한 관리적·기술적·물리적 보호조치의 종합 체계이다. 개인정보보호 관리체계는 정보통신망에서 개인정보보호 활동을 체계적이고 지속적으로 수행하기 위한 종합 체계이다.

핵심 구분

문항에 적용되는 당시 법률의 제47조에 따른 정보보호 관리체계 인증권자는 미래창조과학부장관이고, 제47조의3에 따른 개인정보보호 관리체계 인증권자는 방송통신위원회이다. 따라서 순서는 '미래창조과학부장관 → 방송통신위원회'이다. 한국인터넷진흥원은 인증 관련 업무를 수행할 수 있는 기관이지만, 이 문항에서 묻는 두 관리체계의 법정 인증권자와는 구별된다.

NoteBase

선지별 해설

① O
정보보호 관리체계의 인증권자는 미래창조과학부장관이고, 개인정보보호 관리체계의 인증권자는 방송통신위원회이므로 두 기관의 순서가 모두 맞다.

② X
첫 번째 미래창조과학부장관은 맞지만, 두 번째 한국인터넷진흥원이 틀리다.
틀린 표현: '미래창조과학부장관, 한국인터넷진흥원'
올바른 표현: '미래창조과학부장관, 방송통신위원회'

③ X
두 번째 방송통신위원회는 맞지만, 정보보호 관리체계의 인증권자를 방송통신위원회로 제시한 첫 번째 기관이 틀리다.
틀린 표현: '방송통신위원회, 방송통신위원회'
올바른 표현: '미래창조과학부장관, 방송통신위원회'

④ X
두 기관이 모두 틀리다. 정보보호 관리체계의 인증권자는 방송통신위원회가 아니라 미래창조과학부장관이고, 개인정보보호 관리체계의 인증권자는 한국인터넷진흥원이 아니라 방송통신위원회이다.
틀린 표현: '방송통신위원회, 한국인터넷진흥원'
올바른 표현: '미래창조과학부장관, 방송통신위원회'

⑤ X
한국인터넷진흥원을 두 관리체계의 법정 인증권자로 제시한 것이 틀리다.
틀린 표현: '한국인터넷진흥원, 한국인터넷진흥원'
올바른 표현: '미래창조과학부장관, 방송통신위원회'

오답 포인트

한국인터넷진흥원이 인증 관련 실무를 수행할 수 있다는 점을 법률상 인증권자와 혼동하는 것이 함정이다. 또한 두 관리체계의 명칭이 비슷하더라도 담당 기관은 각각 달랐다는 점을 구별해야 한다.

다시 나오면 이렇게 판단

기관을 묻는 문제에서는 먼저 두 관리체계를 제시된 순서대로 나눈 뒤, 정보보호 관리체계는 미래창조과학부장관, 개인정보보호 관리체계는 방송통신위원회에 대응시킨다. 인증 업무 수행기관인 한국인터넷진흥원과 법정 인증권자를 별도로 판단한다.

NoteBase

암기 포인트

문항 당시 기준으로 정보보호는 미래창조과학부장관, 개인정보보호는 방송통신위원회이다.

NoteBase

9. 해커가 리눅스 서버에 침입 후 백도어를 설치하였다. 백도어와 연관된 포트가 열려있는지 확인하기 위해 사용할 수 있는 프로그램으로 옳은 것은?

① ps
② nmap
③ nslookup
④ traceroute
⑤ ping

정답 2번

출제 포인트

이 문제는 리눅스 서버에서 열린 포트를 탐지하는 포트 스캔 도구와 프로세스·DNS·경로·도달성 확인 도구를 구별하는 문제이다.

핵심 개념

nmap: 대상 호스트의 열린 포트와 서비스 등을 스캔하는 네트워크 탐색 도구이다. / 결정 키워드: 열린 포트, 포트 스캔
ps: 현재 실행 중인 프로세스 정보를 확인하는 명령이다.
nslookup: DNS 서버에 질의하여 도메인 이름과 IP 주소 등의 정보를 확인하는 도구이다.
traceroute: 목적지까지 패킷이 거치는 라우터 경로를 추적하는 도구이다.
ping: 대상 호스트의 네트워크 도달 가능 여부와 응답 시간을 확인하는 도구이다.

NoteBase

선지별 해설

① X — ps는 실행 중인 프로세스의 상태를 확인하는 명령이므로 열린 네트워크 포트를 검사하는 도구가 아니다. 틀린 표현은 '열린 포트를 확인하는 데 ps를 사용한다'는 것이며, 올바르게는 프로세스 목록을 확인할 때 ps를 사용한다.
② O — nmap은 대상 서버를 포트 스캔하여 어떤 TCP·UDP 포트가 열려 있는지 확인할 수 있다. 따라서 백도어와 연관된 것으로 의심되는 포트의 개방 여부를 조사하는 데 적합하다.
③ X — nslookup은 DNS 이름 해석 정보를 조회하므로 열린 포트를 스캔하지 않는다. 틀린 표현은 '열린 포트를 확인하는 데 nslookup을 사용한다'는 것이며, 올바르게는 도메인 이름과 IP 주소 등의 DNS 정보를 확인할 때 nslookup을 사용한다.
④ X — traceroute는 목적지까지의 네트워크 경로와 중간 홉을 확인하므로 포트 개방 여부를 검사하는 도구가 아니다. 틀린 표현은 '열린 포트를 확인하는 데 traceroute를 사용한다'는 것이며, 올바르게는 패킷 전달 경로를 추적할 때 traceroute를 사용한다.
⑤ X — ping은 주로 ICMP 응답을 이용하여 대상 호스트의 도달 가능 여부와 왕복 응답 시간을 확인하므로 열린 포트 목록을 보여 주지 않는다. 틀린 표현은 '열린 포트를 확인하는 데 ping을 사용한다'는 것이며, 올바르게는 호스트의 네트워크 연결 상태를 확인할 때 ping을 사용한다.

오답 포인트

ping과 traceroute도 네트워크 점검에 사용되지만, 네트워크 도구라는 이유만으로 포트 스캔 기능까지 있는 것은 아니다. 또한 ps에서 백도어로 의심되는 프로세스를 찾을 수는 있어도, 문제에서 요구한 '열린 포트' 확인 도구는 nmap이다.

다시 나오면 이렇게 판단

문제의 목적어를 기준으로 도구를 대응한다. '열린 포트·서비스 스캔'이면 nmap, '프로세스'이면 ps, 'DNS 질의'이면 nslookup, '통신 경로'이면 traceroute, '도달 여부·응답 시간'이면 ping으로 판단한다.

암기 포인트

포트는 nmap, 프로세스는 ps, DNS는 nslookup, 경로는 traceroute, 도달성은 ping이다.

NoteBase

10. 암호학적 해시함수에 대한 설명으로 옳지 않은 것은?

① MD5나 SHA-1은 취약점이 발견되어 더 이상 사용하지 않는 것이 바람직하다.

② 해시함수는 출력값에 대응하는 입력값을 구하기 어렵다.

③ 해시함수의 내부 알고리즘에 관계없이 충돌저항성을 분석하는 방법으로 생일공격(Birthday Attack)이 있다.

④ 패스워드와 난수를 해시한 값을 전송할 때, 난수가 노출되어도 사전공격(Dictionary Attack)에 안전하다.

⑤ 최근에는 가상화폐인 비트코인(Bitcoin)을 채굴하는 알고리즘에 사용된다.

정답 4번

출제 포인트

암호학적 해시함수의 일방향성·충돌저항성과 솔트의 역할 및 실제 활용을 구별하는 문제이다.

핵심 개념

암호학적 해시함수: 임의 길이의 입력을 고정 길이의 해시값으로 바꾸는 함수로, 입력 복원은 어렵고 같은 해시값을 만드는 서로 다른 입력을 찾기도 어려워야 한다.

역상저항성: 주어진 해시값에 대응하는 입력값을 찾기 어려운 성질이다.

충돌저항성: 같은 해시값을 만드는 서로 다른 두 입력을 찾기 어려운 성질이며, 생일공격은 이 성질을 분석하는 대표적 방법이다.

솔트: 패스워드마다 덧붙이는 임의의 값으로 동일 패스워드의 해시값을 다르게 하고 미리 계산한 사전·레인보 테이블의 재사용을 어렵게 한다. 솔트는 비밀값이 아니므로 노출만으로 보안이 무너지지는 않지만, 사전공격 자체를 막지는 못한다.

NoteBase

선지별 해설

① O — MD5와 SHA-1은 충돌을 찾을 수 있는 취약점이 알려져 있으므로 충돌저항성이 필요한 새로운 보안 용도에는 사용하지 않는 것이 바람직하다.
② O — 출력 해시값만 주어졌을 때 그에 대응하는 입력값을 찾기 어렵다는 것은 해시함수의 역상저항성이다.
③ O — 생일공격은 해시함수의 구체적인 내부 구조와 무관하게 출력값의 중복 가능성을 이용해 충돌을 찾는 일반적인 공격 방법이다.
④ X — 틀린 표현은 '난수가 노출되어도 사전공격에 안전하다'이다. 솔트가 노출되어도 미리 계산된 테이블의 일괄 재사용은 어렵지만, 공격자는 공개된 솔트를 각 후보 패스워드에 붙여 해시값을 계산하는 사전공격을 수행할 수 있다. 올바르게는 '솔트는 사전공격을 불가능하게 하는 것이 아니라 미리 계산한 해시 목록의 재사용과 대량 공격의 효율을 낮춘다'이다.
⑤ O — 비트코인 채굴의 작업증명에서는 블록 헤더를 반복적으로 해시하여 목표값보다 작은 결과를 찾으며, 이 과정에 암호학적 해시함수가 사용된다.

오답 포인트

④는 '솔트가 노출되어도 괜찮다'는 사실을 '사전공격에도 안전하다'로 과장한 선지이다. 솔트는 공개되어도 되는 값이지만, 공격자가 후보 패스워드를 하나씩 대입하는 일을 막는 비밀키는 아니다.

다시 나오면 이렇게 판단

해시값에서 입력을 찾는 것은 역상공격, 같은 해시값의 두 입력을 찾는 것은 충돌공격으로 구분한다. 솔트 관련 선지는 '중복 해시와 사전 계산 방지'에는 효과가 있지만 '추측 공격 자체 차단'이나 '비밀성 제공'에는 효과가 없다는 기준으로 판단한다.

암기 포인트

역상은 입력 찾기, 생일공격은 충돌 찾기, 솔트는 공개 가능하지만 사전공격의 면역 수단은 아니다.

NoteBase

11. 공개키 암호와 대칭키 암호에 대한 설명으로 옳은 것은?

① 공개키를 교환하기 위해 대칭키 암호를 이용한다.
② 128비트 RSA 공개키와 2048비트 대칭키는 안전도가 비슷하다.
③ 두 암호 모두 기밀성과 무결성을 동시에 보장한다.
④ 긴 메시지 암호화에는 하이브리드 방식의 암호가 효율적이다.
⑤ 공개키 암호는 대칭키 암호에 비해 처리속도가 빠르다.

정답 4번

출제 포인트

공개키 암호와 대칭키 암호의 키 구조, 처리 속도, 제공하는 보안 기능을 비교하고 하이브리드 암호의 쓰임을 판단하는 문제이다.

핵심 개념

대칭키 암호는 암호화와 복호화에 같은 비밀키를 사용하며 처리 속도가 빨라 대용량 데이터 암호화에 적합하다.
공개키 암호는 공개키와 개인키의 쌍을 사용하며 키 교환·전자서명 등에 유용하지만 대칭키 암호보다 처리 속도가 느리다.
하이브리드 암호는 실제 메시지는 빠른 대칭키 암호로 암호화하고, 그 대칭키는 공개키 암호로 안전하게 전달하는 방식이다.

선지별 해설

① X — 틀린 표현은 '대칭키 암호를 이용한다'이다. 공개키를 안전하게 교환하거나 배포하기 위해서는 공개키 기반의 인증 체계 등을 이용하며, 대칭키 암호는 공유 비밀키 자체를 미리 안전하게 전달해야 하는 키 분배 문제가 있다.
② X — 128비트 RSA 공개키와 2048비트 대칭키의 안전도가 비슷하다는 표현이 틀렸다. RSA와 대칭키 암호는 키 길이를 같은 숫자로 직접 비교할 수 없으며, 일반적으로 2048비트 RSA의 보안 강도는 약 112비트 대칭키 수준으로 평가된다.
③ X — 틀린 표현은 '기밀성과 무결성을 동시에 보장한다'이다. 암호화의 기본 목적은 기밀성이고, 무결성은 MAC, 전자서명 또는 인증 암호 방식 같은 별도의 기능으로 보장한다.
④ O — 긴 메시지는 처리 속도가 빠른 대칭키 암호로 암호화하고, 사용한 대칭키만 공개키 암호로 보호하는 하이브리드 방식이 효율적이다.
⑤ X — 틀린 표현은 '공개키 암호는 … 처리속도가 빠르다'이다. 공개키 암호는 복잡한 연산을 사용하므로 일반적으로 대칭키 암호보다 처리 속도가 느리다.

NoteBase

오답 포인트

③은 '암호화하면 무결성도 자동으로 보장된다'고 오해하게 만들고, ⑤는 공개키 암호의 키 관리상 장점을 처리 속도의 장점으로 바꾸어 놓았다. 또한 ②처럼 서로 구조가 다른 암호의 키 길이는 숫자만으로 직접 비교할 수 없다.

다시 나오면 이렇게 판단

대용량 메시지와 속도가 핵심이면 대칭키 암호, 키 전달·전자서명이 핵심이면 공개키 암호로 판단한다. 두 방식의 장점을 함께 묻는다면 '메시지는 대칭키, 대칭키 전달은 공개키'인 하이브리드 방식을 확인한다.

암기 포인트

대칭키는 빠른 본문 암호화, 공개키는 안전한 키 전달, 하이브리드는 두 방식의 결합이다.

NoteBase

12. 사용자 인증 방식에 대한 설명으로 옳지 않은 것은?

① 패스워드 인증은 서버 측에서 인증시스템 구축이 용이하다는 장점이 있다.

② 시각 동기화 OTP(One Time Password)는 두 사용자가 사전에 대칭키를 공유해야 한다.

③ 전자서명 방식은 도전-응답(Challenge-Response) 프로토콜과 결합하여 사용자를 인증한다.

④ 생체인증은 생체정보를 인식할 때마다 발생할 수 있는 에러처리가 중요하다.

⑤ I-PIN은 주민등록번호 대신 사용할 수 있는 일회용 사용자 식별번호이다.

정답 5번

출제 포인트

이 문제는 패스워드, OTP, 전자서명, 생체인증, I-PIN의 인증 원리와 특징을 구별하는 문제이다.

핵심 개념

패스워드 인증은 사용자가 아는 비밀정보를 서버가 확인하는 방식이며 구현이 비교적 간단하다.
시각 동기화 OTP는 사용자 측 장치와 인증 서버가 공유한 비밀키와 현재 시각을 이용해 일회용 비밀번호를 생성한다.
전자서명 기반 인증은 서버가 보낸 도전값에 사용자가 개인키로 서명하고 서버가 공개키로 검증하는 도전-응답 방식이다.
생체인증은 생체정보의 측정·비교 과정에서 오인식이 생길 수 있으므로 오류율 관리가 중요하다.
I-PIN은 인터넷에서 주민등록번호를 직접 사용하지 않고 본인을 확인하기 위한 대체 식별수단이며, 인증할 때마다 새로 생성되는 일회용 번호가 아니다.

NoteBase

선지별 해설

① O — 패스워드 인증은 서버가 등록·검증 기능을 마련하면 되는 구조이므로 다른 고급 인증 방식에 비해 구축이 비교적 용이하다.
② O — 시각 동기화 OTP는 사용자 측 장치와 인증 서버가 사전에 공유한 비밀키를 바탕으로 같은 시간대의 OTP를 계산해야 한다.
③ O — 전자서명 방식에서는 서버의 도전값에 사용자가 개인키로 서명하고 서버가 공개키로 이를 검증하므로 도전-응답 프로토콜과 결합해 사용자를 인증할 수 있다.
④ O — 생체정보는 측정할 때마다 완전히 같은 값이 나오지 않을 수 있으므로 오거부율과 오수락률 같은 오류를 적절히 처리하는 것이 중요하다.
⑤ X — 틀린 표현은 '일회용 사용자 식별번호'이다. I-PIN은 주민등록번호를 인터넷에서 직접 사용하지 않도록 마련된 대체 본인확인 수단이지, 매 인증마다 한 번만 쓰고 폐기되는 OTP형 식별번호가 아니다. 올바르게는 'I-PIN은 주민등록번호를 대신하여 인터넷상에서 본인을 확인하는 데 사용하는 대체 식별수단이다'라고 해야 한다.

오답 포인트

I-PIN의 '대체 식별수단'이라는 성격을 OTP의 '일회용 비밀번호'와 혼동하기 쉽다. '주민등록번호 대신 사용한다'는 말이 '매번 새로운 번호를 한 번만 사용한다'는 뜻은 아니다.

다시 나오면 이렇게 판단

각 인증 방식의 핵심 수단을 먼저 대응시킨다. 패스워드는 지식정보, 시각 동기화 OTP는 공유 비밀키와 시간, 전자서명은 개인키 서명과 공개키 검증, 생체인증은 오인식 관리, I-PIN은 주민등록번호 대체 본인확인 수단으로 판단한다.

암기 포인트

OTP는 일회용 비밀번호이고, I-PIN은 주민등록번호 대체 본인확인 수단이다.

NoteBase

13. DNS(Domain Name System)의 보안 위협과 DNSSEC(Domain Name System Security Extensions) 대응에 대한 설명으로 옳지 않은 것은?

① Cache Poisoning 공격은 DNS 캐시에 저장된 정보를 오염시켜 공격자가 지정한 주소로 유도한다.

② DNS Spoofing은 서버에서 응답하는 IP 주소를 변조하여 의도하지 않은 주소로 유도한다.

③ DNSSEC는 서버의 응답에 전자서명을 부가함으로써 서버인증 및 무결성을 제공한다.

④ DNSSEC는 인증체인 형태로 확장되어 계층적 구조의 DNS 서버에도 적용될 수 있다.

⑤ DNSSEC는 서버의 응답을 숨기지는 않지만, 서비스 거부 공격을 막는 효과가 있다.

정답 5번

출제 포인트

DNS 캐시 포이즈닝·DNS 스푸핑의 공격 원리와 DNSSEC가 제공하는 무결성·출처 인증의 범위를 구별하는 문제이다.

핵심 개념

DNS 캐시 포이즈닝은 DNS 캐시에 거짓 레코드를 저장시켜 이후 질의를 공격자가 정한 주소로 보내는 공격이다.
DNS 스푸핑은 위조하거나 변조한 DNS 응답으로 사용자를 의도하지 않은 주소에 접속시키는 공격이다.
DNSSEC는 DNS 레코드에 대한 전자서명을 검증하여 데이터의 출처 인증과 무결성을 제공한다. 상위 영역이 하위 영역의 키를 검증하도록 연결하는 신뢰 체인을 사용한다. 다만 DNS 응답을 암호화하지 않으므로 기밀성을 제공하지 않고, 서비스 거부 공격을 막는 가용성 보장 기술도 아니다.

NoteBase

선지별 해설

① O — 캐시 포이즈닝은 DNS 캐시에 공격자가 만든 거짓 주소 정보를 주입한다. 그 결과 이후 사용자가 정상 도메인을 질의해도 공격자가 지정한 주소로 유도될 수 있다.
② O — DNS 스푸핑은 위조·변조된 DNS 응답을 정상 응답처럼 받아들이게 하여 도메인 이름을 의도하지 않은 IP 주소와 연결한다.
③ O — DNSSEC는 DNS 응답 데이터에 대한 전자서명을 검증하게 하므로 응답 데이터의 출처 인증과 전송·저장 과정에서의 무결성을 제공한다. 여기서 서버 인증은 TLS처럼 서버 접속 주체 자체를 인증한다는 뜻이 아니라 DNS 데이터의 출처를 인증한다는 의미이다.
④ O — DNSSEC는 루트에서 최상위 도메인, 하위 도메인으로 이어지는 신뢰 체인을 형성하므로 계층적인 DNS 구조에 적용할 수 있다.
⑤ X — 틀린 부분은 '서비스 거부 공격을 막는 효과가 있다'이다. DNSSEC는 응답을 암호화하지 않아 기밀성을 제공하지 않으며, 가용성을 보장하거나 서비스 거부 공격 자체를 차단하지도 않는다. 올바르게는 'DNSSEC는 DNS 응답의 출처 인증과 무결성을 제공하지만 기밀성과 가용성은 제공하지 않는다'이다.

출제자가 노린 함정

보안 기능이라는 이유만으로 DNSSEC가 기밀성·무결성·가용성을 모두 제공한다고 생각하게 만드는 것이 함정이다. 특히 ⑤의 앞부분인 '응답을 숨기지는 않는다'는 맞지만, 뒷부분의 '서비스 거부 공격을 막는다'가 틀려 선지 전체는 옳지 않다.

다시 나오면 이렇게 판단

DNSSEC 관련 선지는 전자서명이 제공하는 속성부터 확인한다. '출처 인증·무결성·신뢰 체인'이면 DNSSEC의 기능이고, '내용 암호화·기밀성·서비스 거부 방지·가용성 보장'이면 DNSSEC의 기본 기능이 아니다.

암기 포인트

DNSSEC는 서명으로 출처와 무결성을 확인한다. 암호화와 가용성 보장은 하지 않는다.

NoteBase

14. TCSEC(Trusted Computer System Evaluation Criteria)에 따라 보안 등급을 평가할 때 보안 수준이 높은 순서대로 나열한 것으로 옳은 것은?

① Structured Protection > Labeled Security Protection > Controlled Access Protection

② Discretionary Security Protection > Controlled Access Protection > Minimal Protection

③ Minimal Protection > Structured Protection > Labeled Security Protection

④ Discretionary Security Protection > Labeled Security Protection > Minimal Protection

⑤ Controlled Access Protection > Discretionary Security Protection > Structured Protection

정답 1번

출제 포인트

TCSEC 보안 등급의 전체 서열을 알고, 제시된 등급을 보안 수준이 높은 순서로 배열할 수 있는지를 묻는 문제이다.

핵심 개념

TCSEC의 보안 수준은 높은 등급부터 A1(Verified Design) > B3(Security Domains) > B2(Structured Protection) > B1(Labeled Security Protection) > C2(Controlled Access Protection) > C1(Discretionary Security Protection) > D(Minimal Protection) 순이다.
B2는 보안 기능을 구조화하고 시스템을 보호 영역으로 나눈 단계이며, B1은 보안 레이블에 따른 강제적 접근통제를 적용하는 단계이다. C2는 사용자별 책임 추적과 더 세분화된 임의적 접근통제를 제공하고, C1은 기본적인 임의적 접근통제를 제공하며, D는 최소 보호 단계이다.

NoteBase

선지별 해설

① O — Structured Protection은 B2, Labeled Security Protection은 B1, Controlled Access Protection은 C2이므로 B2 > B1 > C2의 순서가 맞다.
② X — 'Discretionary Security Protection > Controlled Access Protection'이 틀렸다. 실제로는 C2인 Controlled Access Protection > C1인 Discretionary Security Protection > D인 Minimal Protection 순이다.
③ X — 'Minimal Protection > Structured Protection > Labeled Security Protection'이 틀렸다. 실제로는 B2인 Structured Protection > B1인 Labeled Security Protection > D인 Minimal Protection 순이다.
④ X — 'Discretionary Security Protection > Labeled Security Protection'이 틀렸다. 실제로는 B1인 Labeled Security Protection > C1인 Discretionary Security Protection > D인 Minimal Protection 순이다.
⑤ X — 'Controlled Access Protection > Discretionary Security Protection > Structured Protection'이 틀렸다. 실제로는 B2인 Structured Protection > C2인 Controlled Access Protection > C1인 Discretionary Security Protection 순이다.

오답 포인트

C1과 C2의 순서를 뒤바꾸거나 B 등급을 C·D 등급보다 낮게 놓는 것이 함정이다. 숫자가 같은 계열에서는 숫자가 클수록 보안 수준이 높으므로 C2가 C1보다 높고, 전체 계열은 A > B > C > D 순이다.

다시 나오면 이렇게 판단

먼저 전체 계열을 A > B > C > D로 놓고, 세부 등급을 B3 > B2 > B1 및 C2 > C1로 배열한다. 그다음 각 명칭을 B2=Structured, B1=Labeled, C2=Controlled, C1=Discretionary, D=Minimal에 대응시킨다.

암기 포인트

A1 > B3 > B2 > B1 > C2 > C1 > D, 그리고 B2 구조화·B1 레이블·C2 통제·C1 재량·D 최소로 기억한다.

NoteBase

15. PGP(Pretty Good Privacy)에 대한 설명으로 옳지 않은 것은?

① 이메일 보안이나 파일 암호화에 사용된다.
② 공개키 인증을 위해 PGP 인증서를 사용한다.
③ 자신의 공개키를 전달하는 데 인증기관의 서명이 필요하다.
④ 이메일에 서명할 때, 서명자의 패스워드를 요구한다.
⑤ 이메일 관리 프로그램에 플러그인도 가능하다.

정답 3번

출제 포인트

PGP의 암호화·전자서명 기능과 공개키 신뢰 방식인 신뢰망(Web of Trust)의 특징을 구별하는 문제이다.

핵심 개념

PGP는 전자우편과 파일에 기밀성·무결성·인증 기능을 제공하는 암호화 도구이다. 공개키의 신뢰성은 중앙 인증기관의 서명을 반드시 거치는 방식이 아니라, 사용자들이 서로의 공개키에 서명하여 신뢰를 형성하는 신뢰망 방식으로 확인할 수 있다. 전자서명 시에는 암호화하여 보관된 개인키를 사용하기 위해 개인키의 패스프레이즈를 입력한다.

선지별 해설

① O — PGP는 전자우편의 암호화·전자서명뿐 아니라 파일 자체의 암호화에도 사용할 수 있다.
② O — PGP 인증서는 사용자 식별정보와 공개키 및 그에 대한 서명을 결합하여 공개키의 소유자와 신뢰성을 확인하는 데 사용된다.
③ X — 틀린 표현은 '인증기관의 서명이 필요하다'이다. PGP는 중앙 인증기관의 서명을 필수로 요구하지 않으며, 사용자가 다른 사용자의 공개키에 서명하는 신뢰망 방식으로 공개키의 신뢰를 형성할 수 있다. 올바르게는 '자신의 공개키를 전달할 때 인증기관의 서명이 반드시 필요한 것은 아니다'이다.
④ O — 전자우편에 서명하려면 서명자의 개인키가 필요하며, 일반적으로 암호화되어 저장된 개인키를 해제하기 위해 서명자의 패스프레이즈를 요구한다.
⑤ O — PGP는 전자우편 관리 프로그램과 연동되는 플러그인 형태로 사용할 수 있어 암호화·복호화와 서명 기능을 메일 환경에서 수행할 수 있다.

오답 포인트

③은 공개키 기반 구조의 중앙 인증기관 방식과 PGP의 신뢰망 방식을 혼동하게 만든다. PGP에서도 공개키에 서명이 붙을 수 있지만, 그 서명이 반드시 인증기관의 서명이어야 하는 것은 아니다.

NoteBase

다시 나오면 이렇게 판단

PGP 선지에서 '인증기관이 반드시 서명한다'처럼 중앙 인증기관을 필수 조건으로 제시하면 신뢰망 방식과 충돌하는지 확인한다. 암호화는 수신자의 공개키, 복호화는 수신자의 개인키, 서명은 송신자의 개인키, 서명 검증은 송신자의 공개키를 사용한다.

암기 포인트

PGP는 중앙 인증기관 필수가 아니라 사용자 간 서명으로 이루어지는 신뢰망 방식이다.

NoteBase

16. 자원의 접근제어 방법 중 강제적 접근제어(Mandatory Access Control)에 해당하는 것으로 옳은 것은?

① 자원마다 보안등급이 부여된다.
② 사용자별로 접근권리를 이전할 수 있다.
③ UNIX 운영체제의 기본 접근제어 방식이다.
④ 조직의 역할에 따라 접근권한을 부여하는 방식이다.
⑤ 자원의 소유자가 자원에 대한 접근권한을 설정한다.

정답 1번

출제 포인트

강제적 접근제어(MAC), 임의적 접근제어(DAC), 역할 기반 접근제어(RBAC)의 권한 결정 주체와 판단 기준을 구별하는 문제이다.

핵심 개념

강제적 접근제어(MAC)는 주체의 보안허가와 객체인 자원의 보안등급을 바탕으로 시스템이 중앙의 보안정책에 따라 접근을 통제하는 방식이다. 사용자가 임의로 권한을 설정하거나 다른 사용자에게 이전할 수 없다.
임의적 접근제어(DAC)는 자원의 소유자가 신원 등을 기준으로 해당 자원의 접근권한을 정하는 방식이다.
역할 기반 접근제어(RBAC)는 조직의 직무·역할에 권한을 부여하고 사용자를 역할에 배정하는 방식이다.

선지별 해설

① O — 강제적 접근제어에서는 자원마다 보안등급을 부여하고, 주체의 보안허가와 비교하여 접근 가능 여부를 결정한다.
② X — 틀린 표현은 '사용자별로 접근권리를 이전할 수 있다'이다. 강제적 접근제어에서는 사용자가 권한을 임의로 이전할 수 없으며, 사용자나 자원 소유자가 권한을 이전할 수 있는 성격은 임의적 접근제어와 관련된다.
③ X — 틀린 표현은 'UNIX 운영체제의 기본 접근제어 방식'이다. 전통적인 UNIX의 파일 소유자와 권한 비트에 따른 기본 접근제어는 임의적 접근제어이다.
④ X — 틀린 표현은 '조직의 역할에 따라 접근권한을 부여'한다는 부분이다. 이는 역할 기반 접근제어의 설명이며, 강제적 접근제어는 보안허가와 보안등급을 기준으로 한다.
⑤ X — 틀린 표현은 '자원의 소유자가 접근권한을 설정'한다는 부분이다. 이는 임의적 접근제어의 설명이며, 강제적 접근제어에서는 중앙의 보안정책에 따라 시스템이 권한을 통제한다.

오답 포인트

②와 ⑤의 '사용자·소유자의 재량'은 임의적 접근제어, ④의 '역할'은 역할 기반 접근제어의 키워드이다. 이 표현들을 강제적 접근제어의 특징으로 혼동하기 쉽다.

NoteBase

다시 나오면 이렇게 판단

보안허가·보안등급·중앙정책이 나오면 강제적 접근제어, 소유자의 권한 설정·이전이 나오면 임의적 접근제어, 직무·역할이 나오면 역할 기반 접근제어로 판단한다.

암기 포인트

MAC는 등급과 정책, DAC는 소유자 재량, RBAC는 역할이다.

NoteBase

17. 다음 용어에 대한 설명으로 옳지 않은 것은?

① Rootkit: 시스템 침입 후의 공격을 도와주는 프로그램들의 집합
② Obfuscation: 코드를 분석하기 어렵도록 변조하는 행위
③ Ransomware: 복호화를 조건으로 금전을 요구하기 위해 피해자의 데이터를 암호화하는 악성코드
④ Cross-Site Scripting: 웹 애플리케이션의 데이터를 악성 스크립트 코드로 변조하는 공격
⑤ Sandbox: 악성코드가 시스템 자원에 쉽게 접근하도록 만든 백도어

정답 5번

출제 포인트

정보보호 용어의 정의를 구별하고, Sandbox를 백도어와 혼동한 설명을 찾는 문제이다.

핵심 개념

Rootkit은 침입 후 공격자의 권한 있는 접근을 유지하고 흔적을 숨기는 악성 프로그램의 집합이다.
Obfuscation은 코드의 기능은 유지하면서 구조나 표현을 복잡하게 바꾸어 분석을 어렵게 하는 난독화이다.
Ransomware는 피해자의 데이터나 시스템을 사용할 수 없게 만든 뒤 복구를 대가로 금전을 요구하는 악성코드이다.
Cross-Site Scripting(XSS)은 웹 페이지에 악성 스크립트를 삽입하여 그 페이지를 보는 사용자의 브라우저에서 실행되게 하는 공격이다.
Sandbox는 프로그램을 격리된 환경에서 실행하여 시스템 자원에 대한 접근과 영향을 제한하는 보안 기법이다.
Sandbox는 접근을 제한하는 격리 환경이고, 백도어는 정상 인증 절차를 우회하여 시스템에 접근하게 하는 통로라는 점에서 서로 반대되는 성격을 가진다.

선지별 해설

① O — Rootkit은 시스템 침입 후 공격자가 권한과 접근을 지속적으로 유지하도록 돕고 자신의 존재를 숨기는 프로그램의 집합이므로 옳다.
② O — Obfuscation은 동작은 유지한 채 코드를 읽고 분석하기 어렵게 변환하는 행위이므로 옳다.
③ O — Ransomware는 피해자의 데이터를 암호화하는 등의 방법으로 이용을 막고, 복구를 조건으로 금전을 요구하는 악성코드이므로 옳다.
④ O — Cross-Site Scripting은 웹 애플리케이션이 제공하는 페이지나 입력 데이터에 악성 스크립트를 삽입하여 사용자의 브라우저에서 실행되게 하는 공격이므로 옳다.
⑤ X — 틀린 표현은 '악성코드가 시스템 자원에 쉽게 접근하도록 만든 백도어'이다. Sandbox는 악성코드나 의심스러운 프로그램을 격리하여 시스템 자원에 쉽게 접근하지 못하도록 제한하는 실행 환경이다. 백도어는 정상적인 인증이나 보안 절차를 우회해 접근할 수 있게 하는 은밀한 통로이다.

NoteBase

오답 포인트

⑤는 Sandbox와 백도어의 기능을 뒤바꾸었다. Sandbox의 핵심은 '격리·접근 제한'이고, 백도어의 핵심은 '인증 우회·은밀한 접근'이다. 또한 ④의 '변조'라는 표현에만 매달리기보다 악성 스크립트를 웹 콘텐츠에 삽입하여 사용자의 브라우저에서 실행시키는 XSS의 본질을 확인해야 한다.

다시 나오면 이렇게 판단

각 용어가 공격 수단인지 방어·분석 환경인지 먼저 구분한다. 접근을 유지하면 Rootkit, 분석을 어렵게 하면 Obfuscation, 데이터를 인질로 금전을 요구하면 Ransomware, 브라우저에서 삽입된 스크립트가 실행되면 XSS, 프로그램의 자원 접근을 격리·제한하면 Sandbox로 판단한다.

암기 포인트

Rootkit은 침입 유지, Obfuscation은 난독화, Ransomware는 데이터 인질, XSS는 브라우저 스크립트 실행, Sandbox는 격리와 접근 제한이다.

NoteBase

18. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 정한 개인정보의 보호조치로 옳지 않은 것은?

① 개인정보를 안전하게 저장할 수 있는 암호화 기술 등을 이용
② 개인정보에 대한 불법적인 접근을 차단하기 위한 접근 통제장치의 설치
③ 접속기록의 변조 방지를 위한 조치
④ 개인정보를 안전하게 취급하기 위한 내부관리계획의 공개
⑤ 컴퓨터바이러스에 의한 침해 방지 조치

정답 4번

쟁점

이 문제는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 막기 위한 기술적·관리적 보호조치의 종류에 관한 문제이다. 핵심은 내부관리계획의 수립·시행과 개인정보 처리방침 등의 공개를 구별하는 것이다.

용어 풀이

내부관리계획은 개인정보를 안전하게 처리하기 위하여 조직·책임·교육·접근권한·접속기록·암호화 등의 관리 방법을 내부적으로 정한 계획이다.

핵심 구분

문항이 전제로 한 개인정보 보호조치에는 내부관리계획의 수립·시행, 접근 통제장치의 설치·운영, 접속기록의 위조·변조 방지, 암호화기술 등을 이용한 보안조치, 백신 소프트웨어의 설치·운영 등이 포함된다.
내부관리계획은 조직 내부에서 수립하고 시행하는 관리적 보호조치이며, 그 계획 자체를 공개하는 것이 보호조치로 열거된 것은 아니다.

NoteBase

선지별 해설

① O
- 개인정보를 안전하게 저장·전송할 수 있도록 암호화기술 등을 이용하는 것은 기술적 보호조치에 해당한다.

② O
- 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치를 설치·운영하는 것은 보호조치에 해당한다.

③ O
- 접속기록을 보관하고 위조·변조되지 않도록 하는 조치는 사후 추적성과 기록의 신뢰성을 확보하는 보호조치에 해당한다.

④ X
- 내부관리계획은 외부에 공개하는 것이 아니라 수립하고 시행하여야 한다.
- 틀린 표현: 내부관리계획의 공개
- 올바른 표현: 내부관리계획의 수립·시행

⑤ O
- 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치는 기술적 보호조치에 해당한다.

오답 포인트

④의 '공개'는 개인정보 처리방침의 공개와 내부관리계획을 혼동하게 만드는 표현이다. 내부관리계획은 개인정보의 안전한 처리를 위한 내부 기준이므로 '수립·시행'이 정확하다.

다시 나오면 이렇게 판단

보호조치 문제에서는 행위와 대상을 함께 확인한다. 내부관리계획은 수립·시행, 접근 통제장치는 설치·운영, 접속기록은 위조·변조 방지, 개인정보는 암호화, 컴퓨터바이러스는 백신 소프트웨어로 대응한다.

암기 포인트

내부관리계획은 공개가 아니라 수립·시행이다.

NoteBase

19. 국내 정보보호 관리체계(ISMS) 인증에 관한 평가 기준 중 시스템 개발보안에 대한 통제사항으로 옳지 않은 것은?

① 정보시스템 설계 시 사용자 인증에 관한 보안 요구사항을 고려하여야 한다.

② 알려진 기술적 보안 취약성에 대한 노출여부를 점검하고 이에 대한 보안대책을 수립하여야 한다.

③ 소스 프로그램은 운영환경에 보관하는 것을 원칙으로 하고, 인가된 사용자만 소스 프로그램에 접근하여야 한다.

④ 개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 원칙적으로 분리하여야 한다.

⑤ 운영환경으로의 이관은 통제된 절차에 따라 이루어져야 하고, 실행 코드는 시험과 사용자 인수 후 실행하여야 한다.

정답 3번

출제 포인트

시스템 개발보안 통제에서 설계·개발·시험·운영 단계별로 지켜야 할 원칙을 구별하는 문제이다.

핵심 개념

시스템 개발보안은 보안 요구사항을 설계에 반영하고, 알려진 취약점을 점검·보완하며, 개발·시험 환경과 운영환경을 분리하고, 승인·시험·사용자 인수를 거친 실행 코드만 통제된 절차로 운영환경에 이관하는 관리 활동이다. 소스 프로그램은 운영환경에 보관하는 것이 아니라 운영환경과 분리하여 접근을 통제해야 한다.

선지별 해설

① O — 정보시스템 설계 단계에서는 사용자 인증을 포함한 보안 요구사항을 식별하여 설계에 반영해야 한다.
② O — 알려진 기술적 보안 취약점에 노출되는지 점검하고, 확인된 취약점에 대한 보완대책을 마련해야 한다.
③ X — 틀린 표현은 '소스 프로그램은 운영환경에 보관하는 것을 원칙으로' 한다는 부분이다. 소스 프로그램은 운영환경과 분리된 안전한 장소에 보관하고 인가된 사용자만 접근하도록 통제해야 한다. 운영환경에는 승인된 실행 프로그램을 이관하는 것이 원칙이다.
④ O — 개발 및 시험 시스템은 운영시스템에 대한 비인가 접근이나 변경 위험을 줄이기 위해 원칙적으로 운영시스템과 분리해야 한다.
⑤ O — 운영환경으로의 이관은 승인된 통제 절차에 따라 수행하고, 실행 코드는 시험과 사용자 인수를 거친 후 운영환경에서 실행해야 한다.

오답 포인트

③은 '인가된 사용자만 접근'이라는 맞는 통제를 붙여 문장 전체가 옳아 보이게 만든다. 그러나 핵심 오류는 보관 위치이다. 소스 프로그램의 보관 장소와 운영환경에 배포되는 실행 프로그램을 구분해야 한다.

NoteBase

다시 나오면 이렇게 판단

설계 단계에서는 보안 요구사항 반영, 개발 단계에서는 취약점 점검과 환경 분리, 운영 이관 단계에서는 승인·시험·사용자 인수 여부를 확인한다. 특히 '소스 프로그램을 운영환경에 보관한다'는 표현은 잘못된 통제로 판단한다.

암기 포인트

소스는 운영환경과 분리하여 보관하고, 운영환경에는 검증·승인된 실행 코드만 이관한다.

NoteBase

20. ISO/IEC 17799와 같은 정보보호 관리체계 표준에서 나열된 보안 통제사항들을 근거로 시스템에 대한 보안 위험을 분석하는 방법으로 옳은 것은?

① 비정형화된 접근법(Informal Approach)
② 기준 접근법(Baseline Approach)
③ 상세 위험 분석(Detailed Risk Analysis)
④ 통합 접근법(Combined Approach)
⑤ 시나리오 접근법(Scenario Approach)

정답 2번

출제 포인트

이 문제는 보안 위험 분석 접근법을 구분하고, 표준에 미리 나열된 보안 통제사항을 기준으로 삼는 방법을 찾는 문제이다.

핵심 개념

기준 접근법(Baseline Approach)은 표준이나 지침에 제시된 기본 보안 통제 수준을 조직의 기준선으로 정하고, 이를 시스템에 적용하여 필요한 보호 수준을 확보하는 방법이다.
비정형화된 접근법은 전문가의 지식과 경험에 의존하고, 상세 위험 분석은 자산·위협·취약성 등을 개별적으로 정밀 분석하며, 통합 접근법은 기준 접근법과 상세 위험 분석을 함께 활용한다.

선지별 해설

① X — 비정형화된 접근법은 정해진 표준 통제 목록보다 담당자나 전문가의 지식·경험·직관에 의존하는 방법이다. 이 선지가 맞으려면 '전문가의 경험을 바탕으로 위험을 분석하는 방법'이라고 해야 한다.
② O — 기준 접근법은 ISO/IEC 17799와 같은 표준에 나열된 보안 통제사항을 기준선으로 삼아 시스템의 보안 위험에 대응하는 방법이다. 문제의 '나열된 보안 통제사항들을 근거로'라는 표현과 정확히 대응한다.
③ X — 상세 위험 분석은 각 자산의 가치와 위협·취약성·발생 가능성·영향 등을 구체적으로 분석하는 방법이다. 이 선지가 맞으려면 '자산과 위협 및 취약성을 개별적으로 상세 분석하는 방법'이라고 해야 한다.
④ X — 통합 접근법은 모든 영역에 기준 접근법을 적용한 뒤 중요하거나 위험이 큰 영역에 상세 위험 분석을 추가하는 등 두 방법을 결합한다. 이 선지가 맞으려면 '기준 접근법과 상세 위험 분석을 함께 사용하는 방법'이라고 해야 한다.
⑤ X — 시나리오 접근법은 이 문항에서 제시한 표준 통제사항 기반의 대표 위험 분석 방법에 해당하지 않는다. 올바른 표현은 '표준의 보안 통제사항을 기준으로 적용하는 기준 접근법'이다.

NoteBase

오답 포인트

‘ISO/IEC 17799’라는 표준명 자체보다 ‘나열된 보안 통제사항들을 근거로’라는 문구가 결정적이다. 표준 통제 목록을 출발점으로 삼으면 기준 접근법이며, 자산별 정밀 분석이나 전문가 경험 중심의 방법과 구별된다.

다시 나오면 이렇게 판단

표준·지침·체크리스트의 공통 통제를 적용하면 기준 접근법, 전문가 경험에 맡기면 비정형화된 접근법,
자산·위협·취약성을 개별 평가하면 상세 위험 분석, 두 방법을 섞으면 통합 접근법으로 판단한다.

암기 포인트

표준 통제 목록은 기준선(Baseline), 개별 정밀 평가는 상세 분석, 둘의 결합은 통합 접근법이다.

NoteBase