2018년 해경 정보보호직 정보시스템 보안

-2018년 4월 11일 시행

☑ **만든이 : 지안에듀 조현준**

- 성균관대학교 정보공학 전공
- CISA, CISSP, 정보보안기사

☑ **저서**

- TopSpot 정보보호론 이론편/문제편
- 알기쉬운 정보보안기사 필기편/실기편(알기사)
- TopSpot 자료구조론 이론편/쪽집게 기출문제

☑ **무료 동영상 안내**

- 지안에듀 홈페이지 이용(www.zianedu.com)
  - [빅데이터 3.2] 조현준 정보보호론 연도별 기출문제 풀이강의(전산 전직렬)
- 유튜브 자투리10분 기출20문항정리
  - 유튜브에서 조현준 정보보호론 검색

1. ○△× 18.해경(보).9급

OECD(경제협력개발기구) 개인정보보안 8원칙 중 정보 정확성 원칙의 구성 요소가 아닌 것은?

① 정확성
② 책임성
③ 완전성
④ 최신성

◦ 정보 정확성의 원칙(Data Quality Principle) : 이용 목적상 필요한 범위 내에서 개인정보의 정확성, 완전성, 최신성이 확보되어야 한다.

오답피하기 ② 정보 정확성 원칙에서 개인정보의 책임성이 확보되어야 하는 것은 아니다.

정답 ②

2. ○△× 18.해경(보).9급

정보보호에 대한 설명과 용어가 바르게 짝지어진 것은?

보기

ㄱ. 자산의 손실을 초래할 수 있는 원하지 않는 사건의 잠재적인 원인이나 행위자
ㄴ. 원하지 않는 사건이 발생하여 손실 또는 부정적인 영향을 미칠 가능성
ㄷ. 자신의 잠재적인 속성으로 위협의 이용 대상이 되는 것
ㄹ. 정보자산에 피해를 주는 주체

	ㄱ	ㄴ	ㄷ	ㄹ
①	위협	취약점	위험	위협원
②	위협	위험	취약점	자산
③	취약점	위험	위협	노출
④	위협	위험	취약점	위협원

◦ 위협(Threat) : 손실이나 손상의 원인이 될 가능성을 제공하는 환경의 집합이다. 보안에 해를 끼치는 행동이나 사건이다.
◦ 위험(Risk) : 위협 주체가 취약점을 이용하여 위협이라는 행동을 통해 자산에 악영향을 미치는 결과를 가져올 가능성으로, 위험은 「자산×위협×취약점」으로 표현한다.
◦ 취약점(취약성, Vulnerability) : 컴퓨터나 네트워크에 침입하여 환경 내의 리소스에 대한 허가되지 않은 접근을 시도하려는 공격자에게 열린 문을 제공할 수 있는 소프트웨어, 하드웨어, 절차 혹은 인력상의 약점을 가리킨다. 즉, 위협의 이용대상으로 관리적, 물리적, 기술적 약점이다.
◦ 위협 주체(위협원, Threat agents) : 취약점을 이용하는 존재는 위협 주체(threat agent)라고 불린다.

오답피하기 ④ 위협, 위험, 취약점, 위협원은 보안에서 자주 나오는 용어이다. 특히, 위협, 위험, 취약점의 용어는 혼동하기 쉬우므로 반드시 구별할 수 있어야 한다.

정답 ④

3. ○△× 18.해경(보).9급

중앙집중식 인증 방식인 커버로스(Kerberos)에 대한 다음 설명 중 옳지 않은 것은?

① 커버로스는 시스템을 통해 패스워드를 평문 형태로 전송한다.
② 커버로스는 네트워크 응용 프로그램이 상대방의 신분을 식별할 수 있게 한다.
③ 커버로스 방식에서는 대칭키 암호화 방식을 사용하여 세션을 통신한다.
④ Needham-Schroeder 프로토콜을 기반으로 만들어졌다.

◦ 커버로스는 대칭키 암호를 사용하고 점대점(end-to-end) 보안을 제공한다. 비록 인증을 위해 패스워드의 사용을 허용하지만, 특별히 네트워크를 통해 패스워드를 전송해야 할 필요를 제거하기 위해 설계되었다. 대부분의 커버로스 구현은 공유된 비밀키를 가지고 동작한다.

오답피하기 ① 클라이언트는 자신의 등록된 ID를 이용 평문으로 AS에 자신의 요청을 보낸다.(패스워드는 제외)

정답 ①

4. ○△× 18.해경(보).9급

UNIX 시스템에서 각 사용자가 로그인 할 때마다 시스템에 의해 자동으로 실행되어야 하는 내용(PATH 변수, 프롬프트 지정 등)을 정의해 놓은 파일은?

① /etc/inittab
② /etc/inetd.conf
③ /etc/profile
④ /etc/rc.local

◦ 각 실행 레벨의 초기화에 필요한 프로세스의 지정은 /etc/inittab 파일에서 정의한다.
◦ inetd 데몬은 최초 실행 시 /etc/inetd.conf 파일의 정보를 참조하여 서비스할 프로그램들에 대한 정보를 얻는다. 시스템 관리자는 inetd 데몬으로 서비스할 프로그램의 특징을 /etc/inetd.conf 파일에 정의해야 한다.
◦ 일반적으로 서버 부팅 시마다 매번 자동실행되길 원하는 명령어는 /etc/rc.d/rc.local에 넣어주면 된다. 리눅스에서는 실행레벨에 따라 다르게 부팅할 수 있는데 실행레벨에 따라서 설정되어 있는 모든 프로세스들을 실행하게 된다.

오답피하기 ③ 유닉스 시스템에서 각 사용자가 로그인 할 때마다 시스템에 의해 자동으로 실행되어야 하는 내용(예 변수 : PATH, 프롬프트 지정 등)을 정의해 놓는 파일은 /etc/profile이다.

정답 ③

5. ○△× 18.해경(보).9급

다음 중 SSL 프로토콜에 대한 설명으로 옳지 않은 것은?

① SSL이 적용되었다는 표시로 HTTPS를 사용한다.
② 보안성과 무결성을 유지하기 위해 마지막에는 HMAC을 붙인다.
③ SSL/TLS를 시작하기 위한 최초의 교신은 암호화와 MAC 없이 시작한다.
④ 110번 포트를 주로 사용한다.

◦ HTTPS(SSL을 이용하는 HTTP)는 웹브라우저와 웹서버 간의 안전통신을 구현하기 위한 HTTP와 SSL의 결합이다. HTTPS 기능은 현재 모든 웹브라우저에 내장되어 있다.
◦ 웹브라우저 사용자 관점에서 볼 때 URL(uniform resource locator)주소가 http://가 아니라 https://로 시작하는 점이 차이점이다.

오답피하기 ④ 정상적인 HTTP는 80번 포트를 사용하는데, HTTPS가 지정되면 443번 포트를 사용하며 SSL을 호출한다. HTTPS는 기밀성 및 클라이언트와 서버의 인증, 데이터 무결성을 제공한다.

정답 ④

6. ○△× 18.해경(보).9급

다음 서버 보안용 취약점 점검 도구에 대한 설명으로 가장 올바르지 못한 것은?

① nmap - 실시간 트래픽 분석과 패킷 로깅이 가능하다.
② SATAN - 네트워크를 통해 리모트 시스템의 보안정도를 조사하고 그 자료를 데이터베이스에 저장한다.
③ Nessus - 유닉스 플랫폼에서 동작하며 클라이언트-서버 구조로 클라이언트의 취약점을 점검한다.
④ SAINT - 유닉스 플랫폼에서 동작하는 네트워크 취약점을 분석한다.

◦ snort는 실시간 트래픽 분석과 IP 네트워크 상에서 패킷 로깅이 가능한 가벼운(lightweight) 네트워크 침입탐지시스템이다.

오답피하기 ① Nmap은 공개용 포트스캐닝 도구로 잘 알려져 있다. 윈도우용과 리눅스용 모두 지원을 하며 최근에는 윈도우용 GUI 형태로 지원하고 있어 많이 사용되고 있다.

정답 ①

7. ○△× 18.해경(보).9급

다음은 정보보호의 목표와 개념에 관한 설명으로 가장 거리가 먼 것은?

① 정보보호는 정보처리 영역에 있어서 가용성, 기밀성, 무결성을 보장하는 데 있다.
② 가용성이란 승인 또는 허가받은 사람의 경우 언제든지 접근과 이용을 보장 받는 것이다.
③ 최근에는 정보보호 영역에서 부인방지, 책임성, 진정성, 신뢰성의 중요성이 날로 커지고 있다.
④ 기밀성이란 승인 또는 허가 받지 아니한 사람이나 프로세스에 의한 데이터의 변경 또는 훼손을 방지하는 것이다.

오답피하기 ④ 승인 또는 허가 받지 아니한 사람이나 프로세스에 의한 데이터의 변경 또는 훼손을 방지하는 것은 무결성에 대한 설명이다.

정답 ④

8. ○△× 18.해경(보).9급

다음 보기의 암호 알고리즘 중 키의 길이와 라운드 수가 가장 적은 것을 고르시오?

보기

DES IDEA Rijndael SEED

① 키의 길이 : DES, 라운드 수 : Rijndael
② 키의 길이 : IDEA, 라운드 수 : DES
③ 키의 길이 : DES, 라운드 수 : SEED
④ 키의 길이 : DES, 라운드 수 : IDEA

구분	블록크기	키의 길이	라운드수
DES	64	56	16
IDEA	64	128	8
Rijndael	128	128,192,256	10,12,14
SEED	128	128	16

오답피하기 ④ DES는 키의 길이가 56비트로 보기에서 가장 적고, IDEA는 8라운드로 가장 적다.

정답 ④

9. ○△× 18.해경(보).9급

다음 중 디바이스 인증기술의 장점이 아닌 것은?

① 책임추적성
② 상호 연동성
③ 보안성
④ 경제성

기기인증 도입의 장점
- 보안성 : 기기인증서의 발급부터 이용까지의 절차적 도움을 받을 수 있고 서비스 자체의 검증된 보안 수준을 구축함으로써 보안성을 제공한다.
- 경제성 : 일관된 보안정책 및 안정성을 마련함으로써 구축 및 운영비용을 절감한다.
- 상호연동성 : 유비쿼터스 시대의 도래로 기기서비스 또한 서비스 간, 기종 간 통신 및 인증의 요구가 예측됨에 따라 단일 보안 프레임워크를 기반으로 한 상호연동성이 보장되는 기기인증체계 도입이 필요하다.

오답피하기 ① 디바이스 인증기술은 보안성, 경제성, 상호연동성의 장점을 가진다.

정답 ①

10. ○△× 18.해경(보).9급

다음 중 윈도우 운영체제의 IIS FTP 서버 설정에서 지정할 사항으로 가장 부적절한 것은?

① 운영 포트 변경 및 연결 시간의 제한
② Active/Passive 모드 지원여부
③ 보안계정 사용 및 익명 연결 허용 여부
④ 가상 디렉터리의 사용

IIS FTP 설치 및 운용
- IIS 하위 구성 요소 선택
- 운용 포트 변경
- 연결 및 연결 시간 제한
- 보안 계정 사용 및 익명 연결 허용
- FTP 메시지 지정
- 홈 디렉터리 지정 및 디렉터리 보안 설정
- 가상 디렉터리 사용

오답피하기 ② active/passive 모드 지원 여부는 FTP 클라이언트 명령에 의해서 결정이 되고, 서버에서는 passive 모드 시 허용할 포트를 방화벽에 등록해야 한다.

정답 ②

11. ○△× 18.해경(보).9급

다음 중 위험관리에 관련된 용어와 그 의미의 연결이 가장 거리가 먼 것은?

① 잔여위험 – 위험처리를 수행하기 이전에 잔여하는 위험
② 위험수준 – 결과와 가능성의 조합으로 표현되는 위험의 크기
③ 통제 – 위험을 변경시키기 위한 대책
④ 위험분석 – 위험의 본질을 이해하고 위험수준을 결정하는 과정

오답피하기 ① 기업이 대책을 마련하는 이유는 그들의 전체적인 위험을 수용할 수 있는 수준으로 감소시키는 데 있다. 100% 안전한 시스템이나 환경은 존재하지 않으며, 이는 남겨진 위험이 있음을 의미한다. 이를 잔여위험이라 부른다. 잔여위험은 정보보호 대책 적용 후에도 남아 있을 수 있는 위험을 말한다.

정답 ①

12. ○△× 18.해경(보).9급

다음 중 NTFS 파일 시스템에 대한 설명으로 가장 옳지 않은 것은?

① 이론적인 최대 NTFS 파일 크기는 16EB이다.
② 기본 NTFS 보안을 변경하면 사용자마다 각기 다른 NTFS 보안을 설정할 수 없다.
③ NTFS 구조는 크게 VBR 영역, MFT 영역, Data 영역으로 나눈다.
④ 실제 최대 NTFS 파일 크기는 16TB이다.

◦ NTFS 파일 시스템 구조

오답피하기 ② 기본 NTFS 보안을 변경하면 사용자마다 서로 다른 NTFS 보안을 적용시킬 수 있다.

정답 ②

13. ○△× 18.해경(보).9급

AES 알고리즘의 블록 크기와 키 길이에 대한 설명으로 가장 올바른 것은?

① 블록 크기는 128/192/256비트이고, 키 길이는 64비트이다.
② 블록 크기는 128비트이고, 키 길이는 56비트이다.
③ 블록 크기는 64비트이고, 키 길이는 128/192/256비트이다.
④ 블록 크기는 128비트이고, 키 길이는 128/192/256비트이다.

오답피하기 ④ AES는 128비트 평문을 128비트 암호문으로 출력하는 알고리즘으로 non-Feistel 알고리즘에 속한다. 10, 12, 14라운드를 사용하며, 각 라운드에 대응하는 키 크기는 128, 192, 256비트이다. 키 크기에 따라 AES의 세 가지 버전이 존재하며 이들은 AES-128, AES-192, AES-256으로 불린다. 그러나 어떤 경우라도 키 확장 알고리즘으로부터 생성되는 라운드 키 크기는 평문과 암호문 크기와 동일한 128비트이다.

정답 ④

14. ○△× 18.해경(보).9급

〈보기 1〉의 상황과 개인정보의 안전한 전달을 위해 제공되어야 할 〈보기 2〉의 정보보호서비스를 가장 바르게 연결한 것은?

보기1

ㄱ. 甲은 송신하는 개인정보를 도청당하는 일이 없이 乙에게 전달하기 원한다.
ㄴ. 甲은 송신하는 개인정보가 조작당하는 일이 없이 乙에게 전달되기 원한다.
ㄷ. 甲은 통신 상대의 웹 서버가 乙의 진짜 서버라는 것을 확인하고 싶다.
ㄹ. 甲은 乙의 서버에 적절한 시간에 접속하여 정상적으로 요청된 내용을 수행하고 싶다.

보기2

A. 무결성
B. 인증
C. 기밀성
D. 가용성

	ㄱ	ㄴ	ㄷ	ㄹ
①	B	A	C	D
②	A	D	C	B
③	C	A	B	D
④	B	A	D	C

정보보호의 목표

◦ 기밀성 : 인가된 자만이 접근하여 취득하여야 하는 성질이다.
◦ 무결성 : 메시지 전송 중 인가되지 않은 자 혹은 인가되지 않은 방법으로 정보가 변조되지 않아야 하는 성질이다.
◦ 가용성 : 정당한 사용자가 정보시스템의 데이터 또는 자원이 필요할 때 지체 없이 원하는 객체 또는 자원에 접근하여 사용할 수 있는 성질이다.
◦ 인증 : 정보교환에 의해 실체의 식별을 확실하게 하거나, 임의 정보에 접근할 수 있는 객체의 자격이나 객체의 내용을 검증하는 데 사용되는 성질이다.

오답피하기 ③ 보기는 정보보호서비스 중 기밀성, 무결성, 인증, 가용성에 대한 설명이다.

정답 ③

15. ○△× 18.해경(보).9급

보기에서 설명하는 특징을 가진 보안 모델은?

보기

ㄱ. 무결성 중심의 상업적 모델로 비인가자의 수정과 인가자의 부적절한 수정을 방지한다.

ㄴ. 정보의 특성에 따라 비밀 노출 방지보다 자료의 변조 방지가 더 중요할 때 적합하며 직무분리를 반영하였고, 접속에 대한 로그를 남긴다.

ㄷ. 군사적 보안 요구사항과 상용보안 요구사항 간의 차이점을 강조한다.

ㄹ. 무결성을 집행하기 위한 일반적인 메커니즘

① Clark – Wilson 모델
② Biba 모델
③ HRU(Harrison – Ruzzo – Ullman) 모델
④ BLP(Bell & La Padula) 모델

◦ HRU 모델은 Michael A. Harrison과 Walter L. Ruzzo 그리고 Jeffery D. Ullman이 개발한 모델로서 액세스 행렬모델(access matrix model)에 근간을 둔 보안 모델이다.

오답피하기 ① 클락–윌슨 모델은 접근 3요소(주체, 소프트웨어(TP), 객체), 직무분리, 감사를 통해서 무결성의 세 가지 목적을 구현한다. 세 가지 목적은 다음과 같다.

1. 허가되지 않은 사용자로부터의 수정을 예방
2. 허가된 사용자의 부적절한 수정을 예방
3. 내부 및 외부 일치성을 유지

정답 ①

16. ○△× 18.해경(보).9급

기존에 알려진 침입 방법에 기초한 오용 침입탐지(Misuse Detection)의 특징이 아닌 것은?

① 알려진 공격법이나 보안정책을 위반하는 행위에 대한 패턴을 지식데이터베이스로부터 찾아서 특정 공격들과 시스템 취약점에 기초한 계산된 지식을 적용하여 탐지해 내는 방법으로 지식 기반(Knowledge–Base)탐지라고도 한다.
② 비교적 탐지의 정확도가 높으나 알려진 공격에 대한 정보 수집이 어려우며 새로운 취약성에 대한 최신 정보를 유지하기 어렵다.
③ 정상적인 혹은 유효한 행동 모델은 다양한 방법으로 수집된 참조 정보들로부터 생성되며 현재 활동과 행동 모델을 비교하여 탐지한다.
④ 오용 침입탐지 종류로는 전문가시스템(Expert System), 시그니처 분석(Signature Analysis), 상태전이분석(State Transition Analysis)등이 있다.

규칙–기반 침입탐지(오용 침입탐지)

◦ 시스템 로그, 네트워크 입력정보, 알려진 침입방법, 비정상적인 행위 패턴 등의 특징을 비교하여 탐지하는 방법이다.
◦ 즉, 기존의 침입방법을 데이터베이스에 저장해 두었다가 사용자 행동 패턴이 기존의 침입 패턴과 일치하거나 유사한 경우에 침입이라 판단한다.
◦ 데이터베이스는 기존의 공격이나 침입 시에 나타났던 패턴의 특징을 저장하고 새로운 공격이나 침입 방법이 출현하였을 경우에는 그에 맞는 공격 패턴을 생성하여 추가한다.

오답피하기 ③ 비정상 침입탐지에 대한 설명이고, 나머지는 오용 침입탐지의 특징에 대한 설명이다.

정답 ③

17. ○△× 18.해경(보).9급

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 정보통신 서비스 제공자는 임원급의 정보보호 최고책임자를 지정할 수 있도록 정하고 있다. 이 법에서 정하고 있는 정보통신서비스 제공자의 정보보호 최고 책임자가 총괄하는 업무에 해당하지 않는 것은?

① 정보보호 관리체계 수립 및 관리·운영
② 정보보호 취약점 분석·평가 및 개선
③ 주요 정보통신 기반시설의 지정
④ 정보보호 사전 보안성 검토

제45조의3(정보보호 최고책임자의 지정 등)

③ 정보보호 최고책임자는 다음 각 호의 업무를 총괄한다.

1. 정보보호관리체계의 수립 및 관리·운영
2. 정보보호 취약점 분석·평가 및 개선
3. 침해사고의 예방 및 대응
4. 사전 정보보호대책 마련 및 보안조치 설계·구현 등
5. 정보보호 사전 보안성 검토
6. 중요 정보의 암호화 및 보안서버 적합성 검토
7. 그 밖에 이 법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행

오답피하기 ③ 주요 정보통신 기반시설의 지정은 정보통신기반보호법 제8조에 기술되어 있는 사항이다.

정답 ③

18. ○△× 18.해경(보).9급

다음 중 윈도우 로그 종류와 설명이 가장 바르게 짝지어진 것은?

① 계정 관리 감사 – 사용자 권한 할당 정책, 감사 정책, 신뢰 정책의 변경과 관련된 사항을 로깅한다.
② 정책 변경 감사 – 권한 설정 변경이나 관리자 권한이 필요한 작업을 수행할 때 로깅한다.
③ 개체 액세스 감사 – 특정 파일이나 디렉터리, 레지스트리 키 등과 같은 객체에 대한 접근을 시도하거나 속성 변경 등을 탐지한다.
④ 로그인 이벤트 감사 – 시스템의 시작과 종료, 보안 로그 삭제 등 시스템의 주요한 사항에 대한 이벤트를 남긴다.

윈도우 감사 정책

종류	설명
개체 액세스 감사	특정 파일이나 디렉터리, 레지스트리 키, 프린터 등과 같은 객체에 대하여 접근을 시도하거나 속성 변경 등을 탐지한다.
계정 관리 감사	신규 사용자, 그룹의 추가, 기존 사용자 그룹의 변경, 사용자의 활성화나 비활성화, 계정 패스워드 변경 등을 감사한다.
계정 로그인 이벤트 감사	로그인 이벤트 감사와 마찬가지로 계정의 로그인에 대한 사항을 로그로 남기는데 이 둘의 차이점은 전자는 도메인 계정의 사용으로 생성되는 것이며, 후자는 로컬 계정의 사용으로 생성되는 것이다.
권한 사용 감사	권한 설정 변경이나 관리자 권한이 필요한 작업을 수행할 때 로깅한다.
로그인 이벤트 감사	로컬 계정의 접근 시 생성되는 이벤트를 감사한다. 계정 로그인 이벤트 감사에 비해 다양한 종류의 이벤트를 확인할 수 있다.
디렉터리 서비스 액세스 감사	시스템 액세스 제어 목록(SACL)이 지정되어 있는 액티브 디렉터리(Active Directory) 개체에 접근하는 사용자에 대한 감사 로그를 제공한다.
정책 변경 감사	사용자 권한 할당 정책, 감사 정책 또는 신뢰 정책의 변경과 관련된 사항을 로깅한다.
프로세스 추적 감사	사용자 또는 응용 프로그램이 프로세스를 시작하거나 중지할 때 해당 이벤트가 발생한다.
시스템 이벤트 감사	시스템의 시동과 종료, 보안 로그 삭제 등 시스템의 주요한 사항에 대한 이벤트를 남긴다.

오답피하기 ① 정책 변경 감사, ② 권한 사용 감사, ④ 시스템 이벤트 감사에 대한 설명이다.

정답 ③

19. ○△× 18.해경(보).9급

위험분석 및 평가방법론 중 성격이 가장 다른 것은?

① 확률분포법
② 순위결정법
③ 과거자료 분석법
④ 수학공식 접근법

오답피하기 ② 과거자료 분석법, 수학공식 접근법, 확률 분포법, 점수법은 정량적 위험분석 방법이고, 순위결정법은 정성적 위험분석 방법이다.

정답 ②

20. ○△× 18.해경(보).9급

다음 중 IPSec(Internet Protocol Security)에 대한 설명으로 가장 올바르지 않은 것은?

① 네트워크 계층에서 보안성을 제공해주는 표준화된 기술로 송수신자에게 인증 및 암호화 서비스를 제공한다.
② SA(Security Association)는 보안성 있는 데이터를 교환하기 위해 암호화, 키 교환 등에 대한 합의 사항들을 담고 있다.
③ AH(Authentication Header)는 인증 부분과 암호화 부분 모두를 포함한다.
④ 보안서비스를 위하여 AH(Authentication Header)와 ESP(Encapsulating Security Payload)의 두 프로토콜을 사용한다.

AH 보안 서비스

- 무결성(Integrity) : 전달된 메시지가 중도에 변조 혹은 위조 되지 않음을 증명한다.
- 인증(Data Origin Authentication) : 전달된 메시지가 발신지로부터 온 메시지임을 증명한다.
- 재전송 공격에 대한 보호(Protection against Replay Attack) : 전달된 메시지가 재전송된 것이 아니고, 현재 발신지로부터 송신된 실제 메시지임을 증명한다.

오답피하기 ③ AH 프로토콜은 발신지 인증과 데이터 무결성을 제공하지만 프라이버시(기밀성)는 제공하지 않는다. 반면에 ESP는 발신지 인증, 데이터 무결성과 프라이버시를 제공한다.

정답 ③

2020년 빅데이터 기반 합격 커리큘럼 [정보보호론]

전산개발, 정보보호직, 경찰간부

비전공자도 합격 전략 과목으로 만들수 있는 정보보호론!

※ 공무원 시험일정과 학원사정에 의해 변경될 수 있음.

구분		2019.09~2019.10	2019.11~2019.12	2020.01~2020.02	2020.03~2020.04	2020.05~2020.06	2020.07~2020.08
전산개발	이론 1.0	기본+심화	용어+요약 1.1 + 1.2	속성이론 1.4			
	기출+적중 3.0		핵심기출 700선 3.1	최고수준 800제 3.3			
	모의고사 5.0				국가직 9급 5.1	지방직 등 9급 5.2	국가직 7급 5.3
정보보호직+경간부 7.0			정보보안기사 필기 7.1				
교재		2020 탑스팟 이론서	핵심기출 700선	·2020 탑스팟 이론서/ 최고수준 800제	프린트물	프린트물	프린트물
문제난이도		중~중상	중~중상	중상~상	중상~상	중상~상	상
비고		·이론서2권-전2권 구성 ·주3회 이론수업 ·매주 복습 퀴즈 진행	·연도별 기출문제 풀이 3.2 -교재프린트 제공, 동영상 진행 ·핵심기출 700선 (문제편/정답·해설편/용어·요약집) -전3권 구성 ·정보보안기사는 11월 개강	·최고 수준 800제 (제본, 수강생 제공)는 고득점 합격을 목표로 함	·모의고사식 실전 훈련	·모의고사식 실전 훈련 ·최신 정보보안기사 기출문제 포함 모의고사 진행	·모의고사식 실전 훈련 ·국회사무처 등 시험대비 겸합 ·최종 마무리 정리

추천과정	
전산개발(9급)	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →9급 대비 모의고사 5.1 + 5.2
군무원(9급, 7급)	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →정보보안기사 필기 7.1 →9급 대비 모의고사 5.1 + 5.2
전산개발(7급)	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →9급 대비 모의고사 5.1 + 5.2 → 7급 대비 모의고사 5.3
정보보호직	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →정보보안기사 필기 7.1
사이버, 경찰간부	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →정보보안기사 필기 7.1 →9급 대비 모의고사 5.1 + 5.2 7급 대비 모의고사 5.3

빅데이터 1.0 / 이론

- 1.1 기본+심화 통합이론
- 1.2 핵심 용어 정리 200선(용어집)
- 1.3 핵심 요약집 정리
- 1.4 속성 이론

빅데이터 3.0 / 기출+적중

- 3.1 핵심기출 700선
- 3.2 연도별 기출문제 풀이
- 3.3 최고수준 800제(학원 내부교재)

빅데이터 5.0 / 모의고사

- 5.1 국가직 9급 대비 모의고사
- 5.2 지방직, 교육청, 서울시, 군무원 대비 모의고사
- 5.3 7급 대비 모의고사

빅데이터 7.0 / 정보보호직+경간부

- 7.1 정보보안기사 필기(알기사)

기타 무료 강의

- A 정보보호론 학습 전략
- B 정보보호론 기초 입문 과정
- C 계리직 대비 정보보호론

[전산직 공채 총정리 (3년간)]

시험종류			2017년				2018년				2019년				시험과목	비고
구분	직류	급수	인원	접수기간	시험일	필기 합격선	인원	접수기간	시험일	필기 합격선	인원	접수기간	시험일	필기 합격선		
해경	정보보호	9급	2	2.8~2.22	3.11	90~	3	3.5 ~ 3.15	4.14	70점후	-				컴일,네트워크보안,시스템보안	필기 합격선이 2016년, 2017년 모두 90점이상 공무원기출+정보보안기사필기 문제집에서 다수 출제
해경	전산	7급					1	3.5 ~ 3.15	4.14	-	-				서류전형	
국가직	전산개발	9급	35	2.1 ~ 2.6	4.8	84	50	2.20 ~ 2.23	4.7	73	83	2.20~2.23	4.6	83	국,영,한,컴일,정보	전산개발, 정보보호직 동시 접수 불가
국가직	정보보호	9급	7	2.1 ~ 2.6	4.8	83	5	2.20 ~ 2.23	4.7	69	8	2.20~2.23	4.6	75	국,영,한,네트워크보안,시스템보안	전산개발, 정보보호직 동시 접수 불가
지방직	전산개발	9급	시도별	4.17~4.21	6.17	시도별	시도별	3.12 ~ 3.16	5.19	시도별	시도별	4.8~4.12	6.15	시도별	국,영,한,컴일,정보	지방직, 교육청 동시 접수 가능, 동시 응시는 불가
교육청	전산개발	9급	시도별	4.17~4.21	6.17	시도별	시도별	3.26 ~ 3.30	5.19	시도별	시도별	4.15~4.19	6.15	시도별	국,영,한,컴일,정보	거주지 제한 있음, 2019년부터 지방직과 시험지 동일
서울시	전산개발	9급	7	3.13~3.17	6.24	86	13	3.12 ~ 3.16	6.23	88	18	3.12~3.18	6.15	76	국,영,한,컴일,정보	거주지 제한 없음, 2019년부터 지방직 시험일자와 동일
군무원	국방부	7급					2	6.7 ~ 6.12	8.11	77	14	4.12~4.17	6.22	74	국,자구,DB,정보	영어와 한국사는 공인시험으로 대체 2018년부터 프로그래밍언어론→정보보호론 교체
군무원	국방부	9급	11	4.17~4.21	7.1	72	13	6.7 ~ 6.12	8.11	77.33	8	4.12~4.17	6.22	78.67	국,컴일,정보	영어와 한국사는 공인시험으로 대체 2018년부터 프로그래밍언어론→정보보호론 교체
군무원	육군	9급	24	4.24~4.28	7.1	68	18	6.7 ~ 6.12	8.11	74.67	56	4.12~4.17	6.22	77.33	국,컴일,정보	상동
군무원	해군	9급	8	4.24~4.28	7.1	67	9	6.7 ~ 6.12	8.11	73.33	19	4.12~4.17	6.22	73.33	국,컴일,정보	상동
군무원	공군	9급	2	4.24~4.28	7.1	66	3	6.7 ~ 6.12	8.11	73.33	21	4.12~4.17	6.22	76	국,컴일,정보	상동
국회사무처	전산개발	9급	1	5.8~5.15	7.22	80	1	5.21~5.25	8.25	83	3	5.20~5.24	8.24		국,영,한,컴일,정보	객관식 5지 선다형 출제
국가직	전산개발	7급	26	6.5~6.9	8.26	75.83	29	7.14~7.17	8.18	74.16	30	7.14~7.17	8.17		국,한,정보,자구,DB,소공	2017년부터 영어는 공인시험으로 대체
해경	전산	순경	14	7.31~8.11	9.2	-	10	7.11~7.30	8.11	-	10	5.24~6.3	7.2		실기시험(서술, 약술)	실기시험→서류전형→면접→최종합격, 경력채용
경찰	사이버(보안)	경장					135	7.20~7.31	9.1	시도별	79	7.12~7.22	8.10		필기(2): 정보보호론,시스템네트워크보안 선택(1): 정보보호관리및법규,디지털포렌식개론, 데이터베이스론	객관식 과목별 20문항, 경력채용 필기시험(50%)→신체,적성,체력(25%)→면접(25%)
지방직(서울)	전산개발	7급					3	3.12~3.16	6.23	80	4	8.6~8.9	10.12		국,영,한,정보,자구,DB,소공	영어는 공인시험 대체 아님, 거주지 제한 없음
지방직(경기)	전산개발	7급	2	6.26~6.29	9.23	81.42	3	7.16~7.20	10.13	76.42	2	8.5~8.7	10.12		국,영,한,정보,자구,DB,소공	영어는 공인시험 대체 아님, 거주지 제한 있음
경찰간부	사이버	간부	5	8.14~8.23	9.23	332.5(1차) 463(2차)	5	8.7~8.16	9.15	312.5(1차) 463.5(2차)	5	8.20~8.29	10.5		필수 : 정보보호론(객), 시스템네트워크보안㈜ 선택 : DB, 통신이론, 소공 중 택1	정보보호론은 전 범위에서 출제 시스템네트워크보안은 해당 범위에서만 서술식으로 출제
국가직(추가)	전산개발	9급	10	8.14~8.17	10.21	80									국,영,한,컴일,정보	2017년 하반기 추가 채용
지방직(추가)	전산개발	9급	시도별	10.20~10.26	12.16	시도별									국,영,한,컴일,정보	2017년 하반기 추가 채용

※ 만든이 : 지안에듀-조현준 선생(정보보호론, 자료구조론, 정보보안기사 담당), 최신 자료는 지안에듀(www.zianedu.com) 조현준 교수방 참조