



정보기술자격(ITQ) 시험


한컴오피스

과 목	코드	문제유형	시험시간	수험번호	성 명
아래 한글	1111	A	60분		

수험자 유의사항

- 수험자는 문제지를 받는 즉시 문제지와 수험표상의 시험과목(프로그램)이 동일한지 반드시 확인하여야 합니다.
- 파일명은 본인의 “수험번호-성명”으로 입력하여 답안폴더(내 PCW문서WITQ)에 하나의 파일로 저장해야 하며, 답안파일을 전송하지 않아 미제출로 처리될 경우 실격 처리합니다(예:12345678-홍길동.hwp).
- 답안 작성을 마치면 파일을 저장하고, ‘답안 전송’ 버튼을 선택하여 감독위원 PC로 답안을 전송하십시오. 수험생 정보와 저장한 파일명이 다를 경우 전송되지 않으므로 주의하시기 바랍니다.
- 답안 작성 중에도 주기적으로 저장하고, ‘답안 전송’하여야 문제 발생을 줄일 수 있습니다. 작업한 내용을 저장하지 않고 전송할 경우 이전에 저장된 내용이 전송되오니 이점 유의하시기 바랍니다.
- 답안문서는 지정된 경로 외의 다른 보조기억장치에 저장하는 경우, 지정된 시험 시간 외에 작성된 파일을 활용할 경우, 기타 통신수단(이메일, 메신저, 네트워크 등)을 이용하여 타인에게 전달 또는 외부 반출하는 경우는 부정 처리합니다.
- 시험 중 부주의 또는 고의로 시스템을 파손한 경우는 수험자가 변상해야 하며, <수험자 유의사항>에 기재된 방법대로 이행하지 않아 생기는 불이익은 수험생 당사자의 책임임을 알려 드립니다.
- 문제의 조건은 한컴오피스 2022 / 2020 버전으로 설정되어 있으니 유의하시기 바랍니다.
- 시험을 완료한 수험자는 답안파일이 전송되었는지 확인한 후 감독위원의 지시에 따라 문제지를 제출하고 퇴실합니다.

답안 작성요령

- 온라인 답안 작성 절차
수험자 등록 ⇒ 시험 시작 ⇒ 답안파일 저장 ⇒ 답안 전송 ⇒ 시험 종료
- 공통 부문
 - 글꼴에 대한 기본설정은 함초롬바탕, 10포인트, 검정, 줄간격 160%, 양쪽정렬로 합니다.
 - 색상은 조건의 색을 적용하고 색의 구분이 안 될 경우에는 RGB 값을 적용하십시오.
(빨강 255,0,0 / 파랑 0,0,255 / 노랑 255,255,0).
 - 각 문항에 주어진 《조건》에 따라 작성하고 언급하지 않은 조건은 《출력형태》와 같이 작성합니다.
 - 용지여백은 왼쪽·오른쪽 11mm, 위쪽·아래쪽·머리말·꼬리말 10mm, 제본 0mm로 합니다.
 - 그림 삽입 문제의 경우 「내 PCW문서WITQWPicture」 폴더에서 지정된 파일을 선택하여 삽입하십시오.
 - 삽입한 그림은 반드시 문서에 포함하여 저장해야 합니다(미포함 시 감점 처리).
 - 각 항목은 지정된 페이지에 출력형태와 같이 정확히 작성하시기 바라며, 그렇지 않을 경우에 해당 항목은 0점 처리됩니다.
 - ※ 페이지구분 : 1페이지 - 기능평가 I (문제번호 표시 : 1. 2.),
2페이지 - 기능평가 II (문제번호 표시 : 3. 4.),
3페이지 - 문서작성 능력평가
- 기능평가
 - 문제와 《조건》은 입력하지 않으며 문제번호와 답(《출력형태》)만 작성합니다.
 - 4번 문제는 묶기를 했을 경우 0점 처리됩니다.
- 문서작성 능력평가
 - A4 용지(210mm×297mm) 1매 크기, 세로 서식 문서로 작성합니다.
 -  표시는 문서작성에 대한 지시사항이므로 작성하지 않습니다.

기능평가 I (150점)

1. 다음의 《조건》에 따라 스타일 기능을 적용하여 《출력형태》와 같이 작성하시오. (50점)

《조건》 (1) 스타일 이름 - security

(2) 문단 모양 - 왼쪽 여백 : 15pt, 문단 아래 간격 : 10pt

(3) 글자 모양 - 글꼴 : 한글(궁서)/영문(돋움), 크기 : 10pt, 장평 : 95%, 자간 : 5%

《출력형태》

With the rapid development and spread of ICT and digital technology, accessibility to cyber attacks has become easier, and a variety of more advanced attack methods have emerged as a social problem.

사이버 복원력은 전통적인 사이버 보안과의 차별성을 두고, 업무의 연속성의 유지를 위한 신속한 복원과 위협에 대한 사전 예측 기반의 예방이 핵심 목표라고 할 수 있다.

2. 다음의 《조건》에 따라 《출력형태》와 같이 표와 차트를 작성하시오. (100점)

《표 조건》 (1) 표 전체(표, 캡션) - 굴림, 10pt

(2) 정렬 - 문자 : 가운데 정렬, 숫자 : 오른쪽 정렬

(3) 셀 배경(면색) : 노랑

(4) 한글의 계산 기능을 이용하여 빈칸에 합계를 구하고, 캡션 기능 사용할 것

(5) 선 모양은 《출력형태》와 동일하게 처리할 것

《출력형태》

사이버보안 분야 연구개발 단계별 투자 동향(단위 : 백만 원)

연도	2020년	2021년	2022년	2023년	합계
기초연구	31,832	37,023	39,760	43,651	
응용연구	59,356	89,338	108,723	108,490	
개발연구	55,452	91,976	94,858	98,409	
기타	6,507	4,353	9,015	27,226	

《차트 조건》 (1) 차트 데이터는 표 내용에서 연도별 기초연구, 응용연구, 개발연구의 값만 이용할 것

(2) 종류 - <묶은 세로 막대형>으로 작업할 것

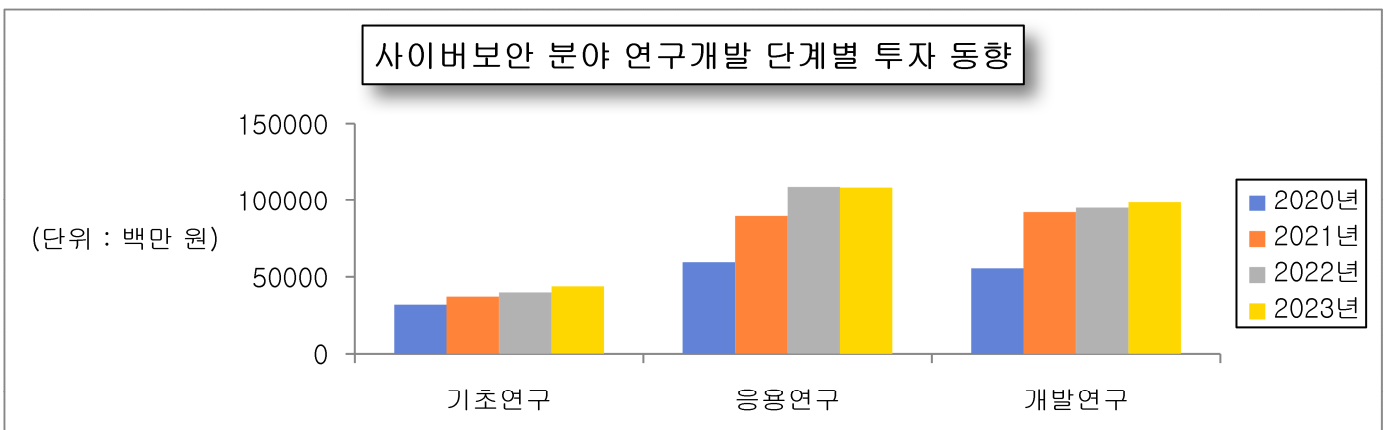
(3) 제목 - 글꼴 : 굴림, 진하게, 12pt

속성 : 채우기(밝은 색 : 하양), 테두리, 그림자(바깥쪽 : 대각선 오른쪽 아래)

(4) 제목 이외의 전체 글꼴 - 굴림, 보통, 10pt

(5) 축제목과 범례는 《출력형태》와 동일하게 처리할 것

《출력형태》



기능평가 II (150점)

3. 다음 (1), (2)의 수식을 수식 편집기로 각각 입력하시오. (40점)

《출력형태》

$$(1) \int_a^b x f(x) dx = \frac{1}{b-a} \int_a^b x dx = \frac{a+b}{2}$$

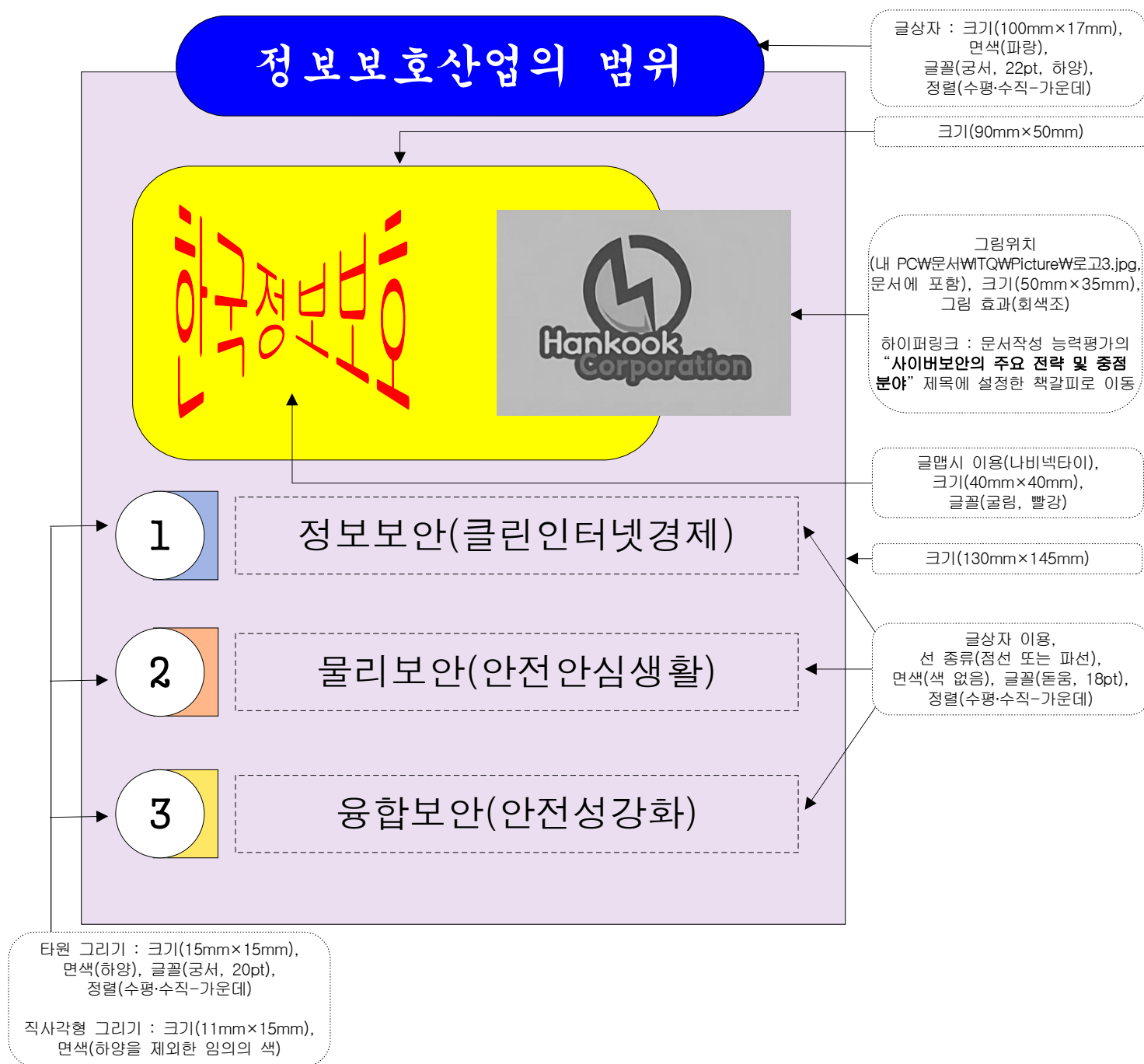
$$(2) Q = \lim_{\Delta t \rightarrow 0} \frac{\Delta s}{\Delta t} = \frac{d^2 s}{dt^2} + 1$$

4. 다음의 《조건》에 따라 《출력형태》와 같이 문서를 작성하시오. (110점)

《조건》

- (1) 그리기 도구를 이용하여 작성하고, 모든 도형(글맵시, 지정된 그림 포함)을 《출력형태》와 같이 작성하시오.
- (2) 도형의 면색은 지시사항이 없으면 색 없음을 제외하고 서로 다르게 임의로 지정하시오.

《출력형태》



문서작성 능력평가 (200점)

글꼴 : 돋움, 18pt, 진하게, 가운데 정렬
책갈피 이름 : 사이버보안
덧말 넣기

머리말 기능
궁서, 10pt, 오른쪽 정렬

기술동향브리프

성장동력사업센터 사이버보안의 주요 전략 및 중점 분야

문단 첫 글자 장식 기능
글꼴 : 굴림, 면색 : 노랑

그림위치(내 PCW문서WITQWPImageW그림4.jpg, 문서에 포함)
자르기 기능 이용, 크기(40mm×40mm), 바깥 여백 왼쪽 : 2mm

각주

사회 전 분야에 걸친 데이터와 네트워크 의존도 확대, 인공지능과 클라우드[㉠] 등 소프트웨어 신기술 등장, 해킹 조직의 전문화 등 대내외적인 변화로 사이버공격의 위험성이 점차 심화되어가고 있는 중이다. 주요 인프라의 디지털 및 인공지능 진화 가속화로 물리적 가상공간의 경계가 모호해지며, 사이버 공격의 대상 및 범위가 개인에서 산업, 사회, 국가 단위로 격상하고 있다. 사이버 공격에 최신 인공지능 기술이 접목됨과 동시에 지능형 지속 공격 등 예측하기 어려운 방식으로 진화, 소프트웨어 공급망과 클라우드 등 악성코드를 심어 공격하는 등 공격 분야 역시 확대되고 있는 중이다. 특히, 해킹 조직은 사이버공격을 고수익 창출 수단으로 인식, 특정 국가가 전문 해커조직의 배후로 밝혀지는 등 고도의 분업화 및 전문화에 따른 사이버공격 기반 생태계가 확장하고 있다.



심화하는 사이버위협에 대응한 차세대 기술개발 및 보안 패러다임 변화(變化)가 강조, 주요 기업 및 국가의 기술과 산업 경쟁력 강화를 위한 적극적인 대응 전략(戰略)을 마련하고 있다.

♣ 인공지능 보안 기술 및 특징

글꼴 : 굴림, 18pt, 하양
음영색 : 빨강

- 보안을 위한 인공지능
 - 신변종 악성코드 및 악성패턴 탐지
 - 이상징후 및 내부자 위협 탐지
- 인공지능을 위한 보안
 - 신뢰성 확보를 위한 설명 가능한 인공지능 기법 적용
 - 생성형 인공지능 모델의 환각 및 오염 여부 탐지

문단 번호 기능 사용
1수준 : 20pt, 오른쪽 정렬,
2수준 : 30pt, 오른쪽 정렬
줄 간격 : 180%

표 전체 글꼴 : 돋움, 10pt, 가운데 정렬
셀 배경(그라데이션) : 유형(가로),
시작색(노랑), 끝색(하양)

♣ 개인정보강화기술의 유형 및 특징

글꼴 : 굴림, 18pt,
기울임, 강조점

유형	주요기술	적용분야	과제 및 한계
암호화된 데이터 처리 도구	동형암호	동일 조직 내 암호화 데이터 연산	데이터 정제 문제, 정보 유출이 없음을 보장
	다자간 연산	민감하여 공개가 어려운 개인 데이터 연산	
	신뢰할 수 있는 실행환경	비공개가 필요한 모델의 연산	더 높은 연산 비용
연합 및 분산 분석	연합학습	프라이버시 보존 머신러닝	신뢰할 수 있는 연결 필요, 데이터 처리자의 모델 정보 접근 필요
	분산분석		

글꼴 : 돋움, 24pt, 진하게
장평 105%, 오른쪽 정렬

한국과학기술기획평가원

각주 구분선 : 5cm

㉠ 인터넷상에 마련한 개인용 서버에 각종 문서, 사진, 음악 따위의 파일 및 정보를 저장하여 두는 시스템

쪽 번호 매기기
5로 시작

마