정보보안기사 필기 출제기준

직무 분야	정보통신(21)-정보기술(211)	자격 종목	정보보안기사	적용 기간	2023. 1. 1.~ 2026. 12. 31.
○직무내용 : 서버, 네트워크 장비, 응용S/W, 보안시스템 등에 대한 보안기술과 활용을 통해 보안서비스를 제공하는 직무					
필기 검정방법	객관식	문제수	100	시험시간	2시간 30분

과목명	문제수	주요항목	세부항목	세세항목
시스템 보안	20	1. 정보 시스템의 범위 및 이해	1. 단말 및 서버 시스템	1. 단말 시스템(PC, 모바일, 프린터, IoT/IIoT 등)
				2. 시스템 서버 (DB, DNS, E-mail, WEB/WAS, 파일서버, Cloud, 보안제품 등)
			2. 운영체제	1. 단말 운영체제 (Window, Linux, Android, iOS, Embeded OS 등)
				2. 서버 운영체제(Windows, Linux, Unix 등)
			3. 시스템 정보	1. 시스템 환경정보, 인증정보, 시스템/감사 로그
		2. 시스템 보안위협 및 공격기법	1. 시스템 보안위협	1. 보안설정, 권한설정, 내부자 위협 등 관리적 보안위협
				2. 보안취약점에 의한 도청, 정보유출·변조, 비인가 접근 등 기술적 보안위협
			2. 시스템 공격기법	1. APT 공격, 알려진 취약점, 취약점 스캐너, SQL Injection, Buffer overflow 등 시스템 공격기법 정의 및 특징
		3. 시스템 보안위협 및 공격에 대한 예방과 대응	1. 시스템보안 대응기술	1. 보안설정, 인증강화, 보안패치, 클라우드 보안 등 관리적 보안
				2. 시스템 파일 위·변조 방지, 유출방지, 접근통제, 접근제어, 로그분석, 이벤트 분석 등 기술적 보안

과목명	문제수	주요항목	세부항목	세세항목
			2. 시스템 분석 도구	1. 시스템 보안취약점 분석 도구(Nmap, Kali Linux, etc. 등) 기능
				2. 시스템 보안취약점 분석 도구(Nmap, Kali Linux, etc. 등) 특징 및 활용방안
			3. 시스템 보안 솔루션	1. 시스템 보호용 보안 솔루션 기능
				2. 시스템 보호용 보안 솔루션 특징 및 활용방안
네트워크 보안	20	1. 네트워크 일반	1. 네트워크 개념 이해	1. 네트워크의 개요(OSI 7 Layers 및 TCP, UDP, IP, ICMP 등 네트워크 프로토콜)
				2. 네트워크의 종류별 동작 원리 및 특징 (Ethernet, LAN, Intranet, Extranet, Internet, CAN, PAN, HAN, SDN 등)
				3. 네트워크 주소의 개요 (IPv4, IPv6 Addressing, Subnetting, CIDR, VLSM, 데이터 캡슐화, Multicast, Broadcast 등)
				4. 네트워크 주소의 종류별 동작원리 및 특징(공인주소, 사설주소, 정적주소, 동적주소, NAT 등)
			2. 네트워크의 활용	1. 네트워크 장비별 원리 및 특징 (NIC, Router, Bridge, Switch, Hub, Repeater, Gateway, VLAN 등)
				2. 네트워크 공유(Share)의 동작원리와 특징 (Netbios, Netbeui, P2P 등)
				3. 유무선 네트워크 서비스의 개요와 종류별 특징
				4. 네트워크 도구(ping, arp, rarp, traceroute, netstat, tcpdump 등)의 이해와 활용

과목명	문제수	주요항목	세부항목	세세항목
		2. 네트워크 기반 공격기술의 이해 및 대응	1. 서비스 거부(DoS), 분산 서비스 거부(DDoS) 공격	1. 서비스 거부(DoS) 공격 유형별 동작원리 및 특징
				2. 각종 서비스 거부(DoS) 공격에 대한 대응 방법
				3. 분산 서비스 거부(DDoS) 공격 유형별 동작원리 및 특징
				4. 각종 분산 서비스 거부(DDoS) 공격에 대한 대응 방법
			2. 스캐닝	1. 포트 및 취약점 스캐닝의 동작원리와 특징
				2. 포트 및 취약점 스캐닝의 대응 방법
			3. 스푸핑 공격	1. 스푸핑 공격의 동작원리 및 특징 (Spoofing)
				2. 스푸핑 공격의 대응 방법
			4. 스니핑 공격	1. 스니핑 공격의 동작원리 및 특징 (Sniffing, Session Hijacking 등)
				2. 스니핑 공격의 대응 방법
			5. 원격접속 공격	1. 원격접속 공격의 동작원리 및 특징 (Trojan, Exploit 등)
				2. 원격접속 공격의 대응 방법
		3. 네트워크 보안 기술	1. 보안 프로토콜 이해	1. 보안 프로토콜별 동작원리 및 특징
				2. 보안 프로토콜 응용 사례

과목명	문제수	주요항목	세부항목	세세항목
			2. 네트워크 보안기술 및 응용	1. 보안 솔루션의 종류별 동작원리 및 특징 (Firewall, IDS, IPS, VPN, ESM, UTM, NAC, 역추적시스템 등)
				2. 보안 솔루션의 활용(Snort, 탐지툴, Pcap 등)
				3. 로그 분석 이해 및 응용
				4. 패킷 분석 이해 및 응용
				5. 역추적 이해 및 응용
				6. 악성코드 분석 도구의 이해 및 응용
어플리케이션 보안	20	1. 인터넷 응용 보안	1. FTP 보안	1. FTP 개념
				2. FTP 서비스 운영
				3. FTP 공격 유형
				4. FTP 보안기술
			2. 메일 보안	1. 메일 개념
				2. 메일 서비스 운영
				3. 메일 서비스 공격유형(스팸 메일, 악성 메일, 웜 등) 과 대책
				4. 메일 보안 기술
			3. Web/App 보안	1. Web/App 개념
				2. Web/App 운영
				3. Web/App 장애 분석 및 대응
				4. Web/App 공격 유형
				5. Web/App 보안 기술

과목명	문제수	주요항목	세부항목	세세항목
			4. DNS 보안	1. DNS 개념
				2. DNS 서비스 운영
				3. DNS 공격유형
				4. DNS 보안 기술
			5. DB 보안	1. DB 보안 개념
				2. DB 공격 유형
				3. DB 보안 기술
		2. 전자 상거래 보안	1. 전자상거래 보안 기술	1. 전자지불 수단별 보안요소
				2. 전자상거래 보안 프로토콜
				3. 전자상거래 인증기술
				4. 무선플랫폼에서의 전자상거래 보안
		3. 어플리케이션 보안 취약점	1. 어플리케이션 보안취약점 대응	1. 어플리케이션 보안취약점 유형
				2. 어플리케이션 보안 취약점 대응 기술
			2. 어플리케이션 개발 보안	1. 소프트웨어 개발 보안 개념 및 요구사항
				2. 소스코드 개발 보안(Secure Coding)
				3. 개발보안 툴
정보보안 일반	20	1. 보안요소 기술	1. 인증	1. 사용자 인증 방식 및 원리
				2. 메시지에 대한 인증 방식 및 핵심 기술
				3. 디바이스에 대한 인증 기술의 원리

과목명	문제수	주요항목	세부항목	세세항목
			2. 접근통제	1. 접근통제 정책의 이해 및 구성 요소
				2. 접근통제 정책의 특징 및 적용 범위 (임의적, 강제적, 역할 기반 등)
				3. 접근통제 기법과 각 모델의 특징
			3. 키 분배 프로토콜	1. 대칭 키 기반 분배 방식의 원리 및 운영
				2. 공개 키 기반 분배 방식의 원리
			4. 디지털서명	1. 인증서 구조 및 주요 특징
				2. 디지털서명의 이해 (종류, 보안 요구 조건, 특징, 서명 방식 등)
				3. PKI 구성방식 및 관리(계층구조, 네트워크 구조, 복합형 구조, CRL, OCSP 등)
				4. 디지털서명 응용 원리 및 구조(은닉 서명, 이중서명 등)
		2. 암호학	1. 암호 알고리즘	1. 암호 관련 용어 및 암호 시스템의 구성
				2. 암호 공격의 유형별 특징
				3. 대칭키 암호시스템 특징 및 활용(종류, 구조, 운영 모드, 공격 기술 등)
				4. 공개키 암호시스템의 특징 및 활용 (종류, 구조, 특징)
				5. 인수분해 기반 공개키 암호방식
				6. 이산로그 기반 공개키 암호방식
			2. 해시함수	1. 해시함수의 개요 및 요구사항
				2. 해시함수별 특징 및 구조
				3. 메시지 인증 코드(MAC)의 원리 및 구조

과목명	문제수	주요항목	세부항목	세세항목
정보보안 관리 및 법규	20	1. 정보보호 관리	1. 정보보호 관리 이해	1. 정보보호의 목적 및 특성
				2. 정보보호 관리의 개념
				3. 정보보호 전략 및 조직
			2. 정보보호 위험평가	1. 위험분석 및 계획수립
				2. 정보자산 식별 및 분석
				3. 위험분석 및 평가
			3. 정보보호 대책 구현 및 사고대응	1. 정보보호 대책 선정 및 계획서 작성
				2. 관리적 보호대책 구현 및 운영(내·외부 인력보안, 교육 및 훈련, 내부감사, 침해사고 예방·대응, 업무연속성관리 등)
				3. 물리적 보호대책 구현 및 운영 (출입 통제, 개인 및 공용 환경 보안 등)
				4. 기술적 보호대책 구현 및 운영(시스템 및 SW개발 보안, 서버·네트워크·DB·어플리케이션 보안, IT 시스템 및 정보보호 시스템 운영 보안 등)
				5. 정보보호 사고대응 (디지털 포렌식 등)
			4. 정보보호 인증제도 이해	1. 정보보호 관리체계 인증의 이해
				2. 정보보호 제품인증의 이해

과목명	문제수	주요항목	세부항목	세세항목
		2. 정보보호 관련 윤리 및 법규	1. 정보보안 윤리	1. 사이버 윤리(보안윤리 개념, 디지털 저작권 침해 및 보호기술, 유해정보유통, 사이버 폭력, 사이버 사기 등 범죄행위)
				2. 정보시스템 이용자 및 개인정보취급자의 금지행위
			2. 정보보호 관련 법제	1. 정보보호 관련 법제 용어의 정의
				2. 정보통신망 이용촉진 및 정보보호 등에 관한 법률의 이해
			3. 개인정보보호 관련 법제	1. 개인정보보호 관련 용어의 정의
				2. 개인정보보호법의 이해

정보보안기사 실기 출제기준

직무 분야	정보통신(21)-정보기술(211)	자격 종목	정보보안기사	적용 기간	2023. 1. 1.~ 2026. 12. 31.

○ **직무내용** : 서버, 네트워크 장비, 응용S/W, 보안시스템 등에 대한 보안기술과 활용을 통해 보안서비스를 제공하는 직무

○ **수행준거** : 1. 보안정책 운영을 위해 운영체제별, 프로토콜별, 서비스별, 보안장비 및 네트워크 장비별 보안 특성을 파악하고 설정 및 점검 등을 수행할 수 있다.
2. 운영체제, 서비스, 보안장비 및 네트워크 장비 등의 취약점 점검을 통해 원인파악, 보완 및 이력사항을 관리할 수 있다.
3. 시스템 로그 및 패킷 로그를 분석하여 침입 원인을 파악하고 보완할 수 있다.
4. 조직의 정보자산을 식별하고 내·외부 위협요인을 분석·평가하여 적절한 정보보호대책 선정 및 이행계획을 수립할 수 있다.

실기 검정방법	필답형	시험시간	3시간

과목명	주요항목	세부항목	세세항목
정보보안 실무	1. 시스템 및 네트워크 보안 특성 파악	1. 운영체제별 보안특성 파악하기	1. IT환경을 구성하고 있는 개인용 단말 시스템 또는 서버에 설치된 운영체제 환경 및 특징을 파악할 수 있다.
			2. 서비스별 운영체제 및 버전을 파악할 수 있다.
			3. 운영체제별 식별 및 인증, 접근통제, 보안업데이트 등 보안강화 방안을 파악할 수 있다.
			4. 운영체제에서 생성되는 로그파일관리가 되고 있는지 점검할 수 있다.
		2. 프로토콜별 보안특성 파악하기	1. OSI 7계층과 TCP/IP 프로토콜의 구성 그리고 각 계층별 기능, 동작 구조를 이해할 수 있다.
			2. TCP/IP 각 계층에서 처리하는 PDU 구조 및 PDU 헤더별 필드 기능을 이해할 수 있다.
			3. IP, ARP, RARP, ICMP 그리고 각 Routing 프로토콜 동작절차 및 취약점을 이해할 수 있다.

과목명	주요항목	세부항목	세세항목
			4. TCP, UDP, SSL/TLS, IPSec 프로토콜의 동작절차와 취약점을 이해할 수 있다.
			5. 서비스 거부(DoS/DDoS 등) 공격 방식과 절차를 이해할 수 있다.
			6. 무선 프로토콜 동작 구조 및 보안 기법을 이해할 수있다.
		3. 서비스별 보안특성 파악하기	1. FTP 서비스 동작절차와 환경 설정, 보안 기법을 이해할 수 있다.
			2. 메일 서비스 동작절차와 환경 설정, 보안 기법을 이해할 수 있다.
			3. 웹 서비스 동작절차와 환경 설정, 보안 기법을 이해할 수 있다.
			4. DNS 서비스 동작절차와 환경 설정, 보안 기법을 이해할 수 있다.
			5. DB 서비스와 환경 설정, 보안 기법을 이해할 수 있다.
			6. 전자서명, 공개키 기반 구조 구성과 보안 특성을 이해할 수 있다.
		4. 보안장비 및 네트워크 장비별 보안특성 파악하기	1. 조직의 보안대상 시스템과 네트워크 장비를 파악할 수 있다.
			2. 네트워크 구성도를 분석하여 사용 중인 IP 주소, 서브넷 등의 네트워크 정보를 파악할 수 있다.
			3. SNMP를 이용한 원격관리기능과 스캐닝 도구를 이용한 관리대상시스템의 제공 서비스를 파악할 수 있다.
			4. 네트워크 장비의 역할과 동작을 이해할 수 있다.

과목명	주요항목	세부항목	세세항목
			5. VLAN 보안 서비스 및 설정 방법을 이해할 수 있다.
			6. Router 설정 절차 및 트래픽 통제 기능을 이해할 수 있다.
			7. Firewall, IPS/IDS, WAF, VPN 등 보안 장비별 특성과 설정 방법을 이해할 수 있다.
			8. NAT 종류 및 동작 절차를 이해할 수 있다.
	2. 취약점 점검 및 보완	1. 운영체제 보안설정 점검과 보완하기	1. 불필요한 계정 존재 및 악성코드 설치 여부에 대하여 점검·보완할 수 있다.
			2. 운영체제별 보호 대상 객체(파일, 폴더) 권한 설정이 보안목표에 따라 설정되어 있는지 점검·보완할 수 있다.
			3. 운영체제별 이벤트 로그정보 생성과 관리가 보안목표에 따라 설정되어 있는지 점검·보완할 수 있다.
			4. 운영체제 종류 및 버전 정보가 불필요하게 노출되어 있는지 점검·보완할 수 있다.
			5. 원격접속 및 원격관리 기능이 보안목표에 따라 설정되어 있는지 점검·보완할 수 있다.
			6. 운영체제의 패치관리가 적절히 설정되어 있는지 점검·보완할 수 있다.
		2. 서비스 보안설정 점검과 보완하기	1. 비인가된 서비스가 동작하고 있는지 점검한 후 제거 할 수 있다.
			2. 파일서버, FTP서버에 권한이 없는 사용자가 접근할 수 있게 설정되어 있는지, 각 사용자별로 접근할 수 있는 파일·폴더가 적절히 설정되어 있는지 점검할 수 있다.
			3. 공유폴더에 적절한 접근통제가 보안목표에 적합한지 점검하며, 폴더가 불필요하게 공유되어 있는지 점검·보완할 수 있다.

과목명	주요항목	세부항목	세세항목
			4. 메일 서버 설정에서 스팸메일 릴레이가 허용되어 있는지, 메일 송수신 프로토콜(SMTP, POP, IMAP) 보안 설정이 적절한지 점검할 수 있다.
			5. WEB/WAS 서버 설정에서 다양한 공격 유형들에 대비하여 보안 설정이 적절한지 점검할 수 있다.
			6. DNS 서버 설정에서 불필요한 명령어 수행이 허가되어 있지 않은지, DNS 보안 조치가 적절히 설정되어 있는지 점검할 수 있다.
			7. DB 서버 설정에서 중요 정보가 암호화되어 저장되고 있는지, DB객체(테이블, 칼럼, 뷰 등)별 접근통제가 적절히 설정되어 있는지 점검할 수 있다.
		3. 네트워크 및 보안장비 설정 점검과 보완하기	1. 네트워크 장비의 관리자 계정 보안이 적절히 설정되어 있는지 점검할 수 있다.
			2. 침입차단시스템(Firewall) 장비의 보안 설정(IP별 통제, Port별 통제, 사용자 ID별 통제 등)이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다.
			3. 침입탐지 및 방지 시스템(IDS/IPS) 보안 설정이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다.
			4. NAT 설정이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다.
			5. 무선접속 장비가 보안목표에 따라 암호화 및 접근통제가 적절히 설정되어 있는지 확인할 수 있다.
			6. WAF 보안 설정이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다.
			7. Anti-DDoS(DDOS 대응장비) 보안 설정이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다.

과목명	주요항목	세부항목	세세항목
			8. Anti-APT(APT 대응솔루션) 보안 설정이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다.
		4. 취약점 점검이력과 보완내용 관리하기	1. 운영체제별 보안점검 내용과 방법(도구), 발견된 보안취약점 및 보완 사항을 기록할 수 있다.
			2. 조직에서 사용 중인 주요 서비스에 대해 수행한 보안점검 내용과 방법(도구), 발견된 보안취약점 및 보완 사항을 기록할 수 있다.
			3. 네트워크 장비에 대해 수행한 보안점검 내용과 방법(도구), 발견된 보안취약점 및 보완사항을 기록할 수 있다.
			4. 보안장비에 대해 수행한 보안점검 내용과 방법(도구), 발견된 보안취약점 및 보완사항을 기록할 수 있다.
	3. 보안관제 및 대응	1. 정보수집 및 모니터링	1. 조직의 보안목표에 따라 운영체제 및 버전별, 서비스별(FTP, 메일, WWW, DNS, DB 등) 보안 등 생성되는 로그 정보를 파악하고 로그 내용을 모니터링 및 통제할 수 있다.
			2. 주요 보안장비(Firewall, IDS, IPS 등), 네트워크 장비(Switch, Router, 무선접속AP 등) 등에서 제공되는 로그정보 관리 도구를 이용하여 로그정보의 생성 수준, 구성요소 등을 설정 할 수 있다.
		2. 로그분석 및 대응	1. 시스템별, 주요 서비스별, 유·무선 네트워크 장비별, 보안장비별, 시간대별로 보안 로그 정보를 통합·분석할 수 있다.
			2. 통합 보안로그를 정렬하여 내·외부 공격 시도 및 침투 여부 등 관련 정보를 수집 및 분석할 수 있다.
			3. 시스템별, 주요 서비스별, 유·무선 네트워크 장비별, 보안장비별 비정상 접근과 변경 여부를 확인 및 분석할 수 있다.

과목명	주요항목	세부항목	세세항목
			4. 업무 연속성을 위한 정보 및 보안 설정 정보를 백업 및 복구 등으로 대응할 수 있다.
	4. 위험분석 및 정보보호 대책 수립	1. IT 자산 위협 분석하기	1. 조직의 IT환경의 시스템 및 네트워크 구성도 등 정보자산 현황을 파악할 수 있다.
			2. IT환경을 구성하는 서버, 어플리케이션, DBMS, WEB/WAS, PC 등으로부터의 위협 요인을 식별할 수 있다.
			3. 조직의 네트워크를 구성하는 네트워크 장비, 보안 장비로부터의 위협요인을 식별할 수 있다.
			4. 정보보호 및 개인정보보호 관련 법적 준거성 위험을 식별할 수 있다.
		2. 조직의 정보자산 위협 및 취약점 분석 정리하기	1. 조직의 H/W자산(PC, 서버, 네트워크 및 보안장비)에 대한 중요도, 내·외부위협 및 취약점분석 내용을 정리할 수 있다.
			2. 조직의 S/W자산(운영체제, 상용 및 자가개발패키지)에 대한 중요도, 내외부 위협 및 취약점분석 내용을 정리할 수 있다.
			3. 조직의 정보자산(기업정보 및 고객정보)에 대한 중요도, 내·외부 위협 및 취약점 분석 내용을 정리할 수 있다.
		3. 위험평가하기	1. 식별된 위험을 기반으로 위험도를 산정할 수 있다.
			2. 조직에서 수용 가능한 목표 위험수준을 정하고 그 수준을 초과하는 위험을 식별할 수 있다.
		4. 정보보호대책 선정 및 이행계획 수립하기	1. 식별된 위험에 대한 처리 전략(위험감소, 위험회피, 위험전가, 위험수용 등)을 수립하고 위험처리를 위한 정보보호대책을 파악할 수 있다.
			2. 정보보호대책의 우선순위를 정한 후에 일정, 예산 등을 포함하여 정보보호 대책 이행계획을 수립할 수 있다.