지정검사소 자동차검사장비 정보보안 준수 사항

❑ 추진 배경

○ 최근 랜섬웨어 · 해킹메일 등 보안에 취약한 인터넷 단말기(PC)를 대상으로 한 사이버 침해사고가 급격히 증가

○ 인터넷에 연결된 지정검사소 검사장비가 랜섬웨어, 악성코드 감염시 공단 자동차검사관리시스템(VIMS)로 연쇄감염으로 자동차검사업무 중단되는 국가적 보안사고 확산이 우려

○ 지정검사소 자동차검사 장비에 대한 정보보안 관리강화가 긴요

❑ 검사장비 정보보안 준수 사항

○ 검사단말기(PC)

- PC CMOS 및 윈도 로그인 비밀번호 설정 · 운영
- 화면보호기 비밀번호 설정(최대 10분 이내)
- 안전한 비밀번호 사용 및 분기별 1회 변경

※ 영문 · 특수기호 · 숫자가 포함된 9자리 이상

- 최신 백신 S/W(알약, V3 등) 설치 · 운영 및 자동 검사기능 설정 · 운영
- 보안기술 지원이 중단된 윈도XP 등 노후 운영체제 교체
- 랜섬웨어 공격에 취약한 공유폴더 사용금지 및 SMB 포트(UDP/137 · 138, TCP/139 · 445) 사용 차단
- 응용프로그램(Adobe Acrobat Reader, Flash, JAVA 등) 최신 보안 업데이트 정기적 실시

○ PC보안에 취약한 프로그램 사용

- P2P프로그램(토렌트 등), SNS(카카오톡, 라인, 밴드, 위챗, 텔레그램 등), 게임 프로그램 등
- 특별한 사유가 없는 한 아래한글 · 엑셀 · 워드 등 문서 편집프로그램을 읽기 전용으로 운용

ㅇ 검사단말기 內 자료 저장 · 관리

- 검사단말기 內 검사정보를 저장 및 관리 금지
- 검사단말기 內 개인정보 포함된 파일 저장 금지

ㅇ 개인정보보호대책 준용

- 개인정보가 저장된 PC 교체 · 반납 · 폐기 또는 외부 수리 의뢰시 하드디스크 분리 · 포맷 사전 조치
- 개인정보가 포함된 파일을 저장할 경우 암호화 저장 및 비식별화조치
- 보유 기간이 경과된 개인정보는 파기 조치

ㅇ 휴대용 저장매체 사용

- 휴대용 저장매체(USB, SD카드, 외장 하드디스크) 사용은 원천 금지
- 부득이하게 사용할 경우 검사 목적 휴대용 저장매체에 한해 관리대장에 등록하여 사용
- 개인 휴대용 저장매체를 반입 · 사용은 원천 금지

ㅇ 자동차검사관리시스템(VIMS) 이용

- 노트북 등 사전 등록되지 않은 단말기(PC)로 VIMS 연결 · 사용 금지
- VIMS 접속 비밀번호는 분기별 1회 정기적 변경

  ※ 영문 · 특수기호 · 숫자가 포함된 9자리 이상
- VIMS 제공 화면에서 검사정보 캡춰 · 저장행위 원천 금지
- 고객관리프로그램 등을 이용한 ID · 비밀번호 저장 및 VIMS 자동 로그인 금지
- 검사업무 시간 외에는 VIMS 접속 · 사용 금지

ㅇ 인터넷 사이트 접속 · 이용

- 자동차검사업무 관련 사이트 이외 접속 자제
- 보안이 취약한 웹사이트 및 불법 파일공유 사이트(웹하드 등) 방문 금지
- 인터넷 메일 사용 금지(다음, 네이버, 네이트, 구글메일(지메일) 등)

ㅇ **협회 등에서 서버를 도입·운영할 경우 자료 절취, 위·변조, 개인정보 유출 등에 대비한 보안대책을 수립·시행**

- 서버 내 저장자료 중요도에 따라 사용자 접근권한 차등 부여
- 사용자별 자료의 접근범위를 서버에 등록하여 인가여부를 식별 및 인가된 범위 이외 자료접근 통제
- 불필요한 서비스 포트 제거 및 관리용 서비스와 사용자용 서비스 분리 운용
- 서버의 관리용 서비스 접속시 특정 IP와 MAC 주소가 부여된 관리용 단말을 지정 운용
- 서버 설정 정보 및 서버에 저장된 자료에 대해서는 정기적으로 백업을 실시하여 복구 및 침해행위에 대비
- 데이터베이스에 대하여 사용자의 직접적인 접속을 차단하고 개인정보와 같은 중요정보를 암호화하는 등 데이터베이스별 보안조치를 실시
- 정보보안관리자를 지정하여 연1회 이상 서버 보안 설정, 자료 위변조 및 절취 가능성 등 보안취약점 점검

ㅇ **검사소 보안관리 전담자**

- 검사소별 보안관리 전담자 지정·운영
- 검사단말기·VPN 등 보안 준수여부 자체 점검·관리
- 개인정보가 저장된 PC 교체·반납·폐기 또는 외부 수리 의뢰시 하드디스크 분리·포맷 사전 조치

ㅇ **VPN 장비 보안관리**

- 임의로 접속 및 조작이 불가한 시건장치가 설치된 안전한 별도 장소에 설치

  ※ 별도 공간 확보가 어려울 경우, 정보통신시설 표기·시건장치 부착

ㅇ **검사장비 악성코드·랜섬웨어 감염 등 해킹 발생시 초동 조치**

- 감염 검사 장비는 인터넷 LAN선 제거 및 분리

  ※ PC 전원을 끄지 않고 유지

- 한국교통안전공단 검사운영처로 신속 통보

- 한국교통안전공단 지시에 따라 자체 후속 조치 시행

※ 해커에게 금전 지불 등 금지

❑ 위반시 제재 조치

○ VIMS 검사정보 과다 조회한 검사소에 대해 「자동차검사 전산정보 처리조직 운영지침」에 따라 적절한 조치 필요

- 해당 검사차량이외 정보 조회 및 업무목적외(검사일자 안내) 정보 이용·공개는 검사단말기 이용제한 규정(제 19조 1항)을 위반

> **제19조(단말기이용의 제한)** ① 소관부서의 장은 다음 각 호의 어느 하나에 해당하는 경우에는 단말기의 이용범위를 제한하거나 단말기의 사용 중지 또는 설치승인을 취소할 수 있다. <개정 2010.12.31, 2014.4.1>
> 1. 이용기관이 승인된 업무목적 이외의 자료를 조회·이용하거나 외부에 공개하는 경우

- VIMS 접속 ID·비밀번호를 고객관리 프로그램에 별도 저장은 공단과 체결한 「전산정보 처리조직 이용약정서」에 명시된 이용기관 준수사항(제5조 1항)을 위반

> **제5조(이용기관의 준수사항)** ①지정사업자는 전산정보처리조직을 이용하고자 할 때에는 국가전산보안기본지침(국가정보원)에 따라 보안을 유지하여야 한다.
> ② 지정사업자는 자동차 검사업무 외의 용도로 전산정보처리조직을 이용하여서는 아니 된다.
> ③ 지정사업자는 전산정보처리조직을 이용한 자료를 외부에 공개하여서는 아니 된다.

○ 보안 준수사항 위반으로 VIMS 시스템 추가 감염 등 보안사고 발생시 해당 검사소에 제재조치 이행

○ VIMS 운영 매뉴얼에 정보보안 준수사항 반영 및 개정 요청

❑ 시행 일자

○ 2019년 09월 01일부터 시행

※ 부록 : 정보통신시설 표기 안내문 및 PC 보안 설정법

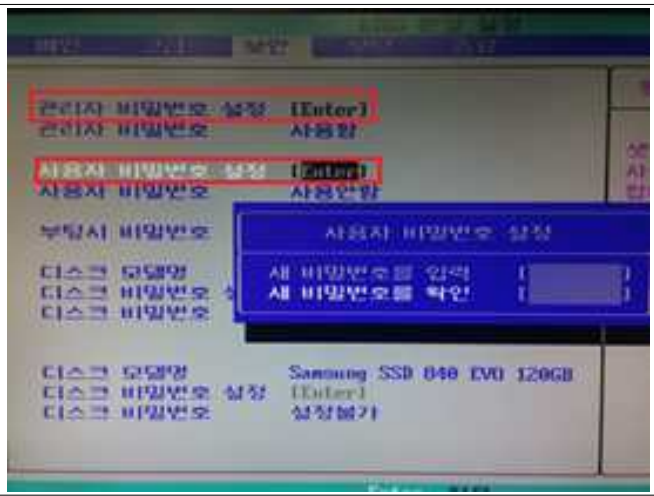
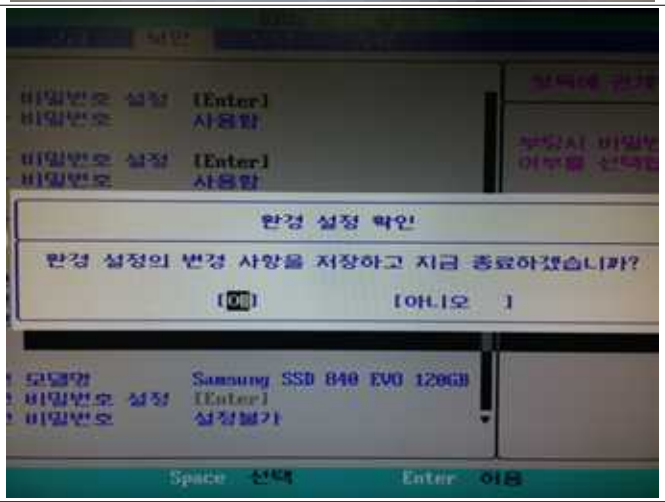
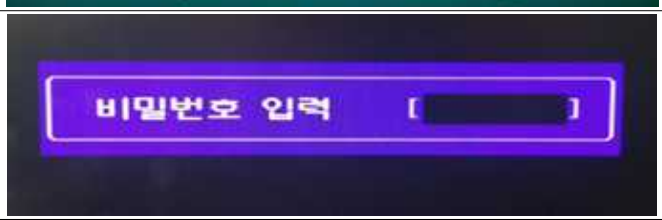
부록 1 **정보통신시설 표기 안내문**

검사소 정보통신시설임

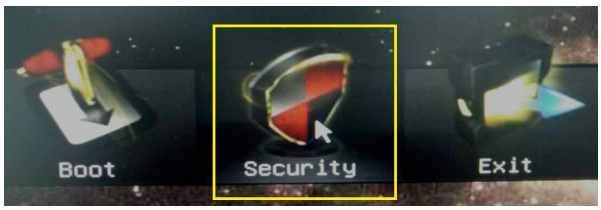
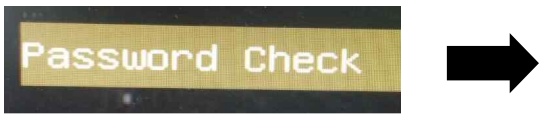
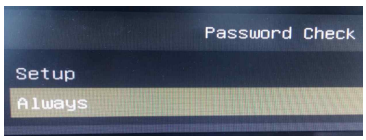
관계자 외 촉수금지

백색바탕에 적색 글씨, 적색 테두리(최대 A4사이즈)

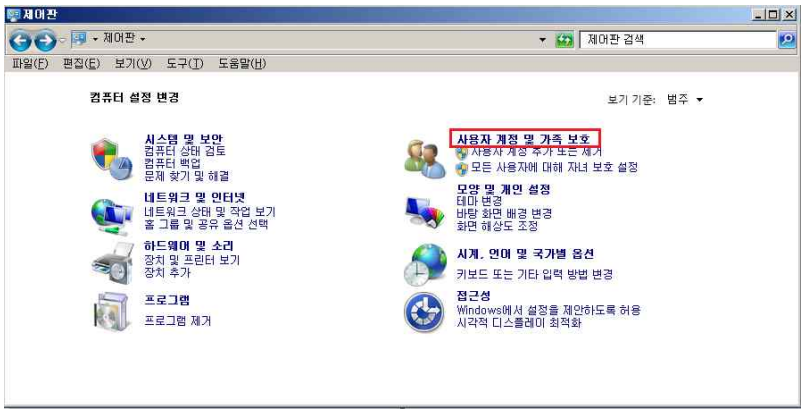
부록 2 검사 장비 PC의 CMOS 비밀번호 설정 방법(한글메뉴)

1. BIOS 환경 설정 => 부팅 직후 F2 키 클릭	
2. 사용자 비밀번호 설정 => 보안 또는 Security 탭에서 [관리자 비밀번호] 및 [사용자 비밀번호] 설정 선택 후 새 비밀번호 입력 및 확인	
3. 관리자 비밀번호, 사용자 비밀번호, 부팅시 비밀번호 : [사용함] 설정	
4. BIOS 환경 설정 확인 => ESC 또는 F10 키를 누른 후 변경 사항 저장 및 종료	
5. 사용자 비밀번호 입력 => 재부팅 후 비밀번호 입력창에 설정한 CMOS 비밀번호 입력	

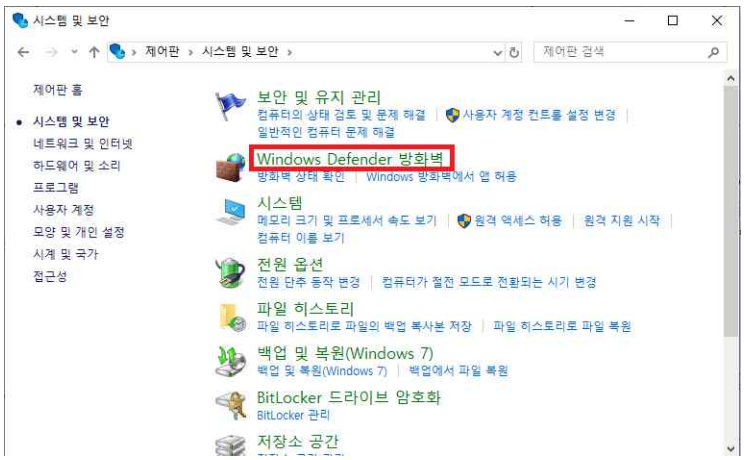
부록 3 검사 장비 PC의 CMOS 비밀번호 설정 방법(영문메뉴)

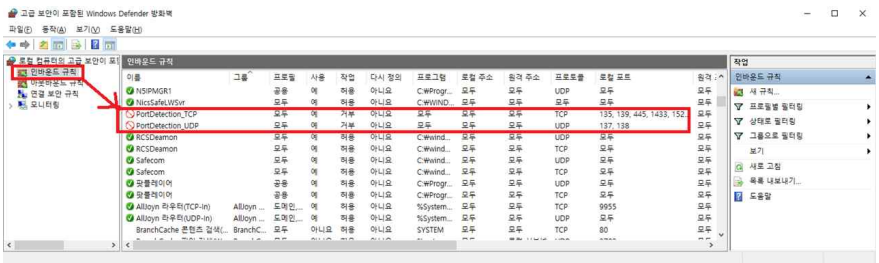
1. BIOS 환경 설정 => 부팅 직후 F2 키 클릭	
2. [Security] 탭 마우스로 클릭	
3. 키보드의 화살표 키로 Supervisor Password(관리자 비밀번호) 이동 후 엔터키 누름	
4. Supervisor Password(관리자 비밀번호) 설정 후 엔터키 눌러 저장	
5. 키보드의 커서키(화살표 키)로 User Password(사용자 비밀번호) 이동 후 엔터키 누름	
6. User Password(사용자 비밀번호) 설정 후 엔터키 눌러 저장	
7. Password Check 항목 이동 후 선택하여 [always] 선택	 
8. 메뉴에서 [Exit] 마우스 클릭	
9. [Save Changes and Exit]를 선택하여 저장 후 재부팅한다.	

부록 4 검사 장비 PC 윈도 비밀번호 설정 방법

1. 제어판 실행(시작 → 제어판)
2. 사용자 계정 및 가족 보호 선택 
3. Windows 암호 변경 선택 
4. 사용자 암호 만들기 또는 사용자 암호 변경 

부록 5 SMB 포트(UDP/137 · 138, TCP/139 · 445) 사용 차단

1. 차단 설정 파일을 검사 장비 PC에 다운로드하여 실행	
2. SMB포트 차단 설치 파일을 더블클릭하여 실행	 * 파일명 : PortBlock.bat
3. [제어판]→[시스템 및 보안]	
4. [Windows Defender 방화벽]	
5. 왼쪽 [고급설정]	

6. 왼쪽 [인바운드 규칙]	 * PortDetection_TCP 및 PortDetection_UDP 생성 확인

부록 6 검사 장비 PC에 백신 프로그램 설치·주기적 검사 설정 방법

1. 백신 설치 파일을 검사 장비 PC에 다운로드하여 설치(알약, V3 Lite 등)

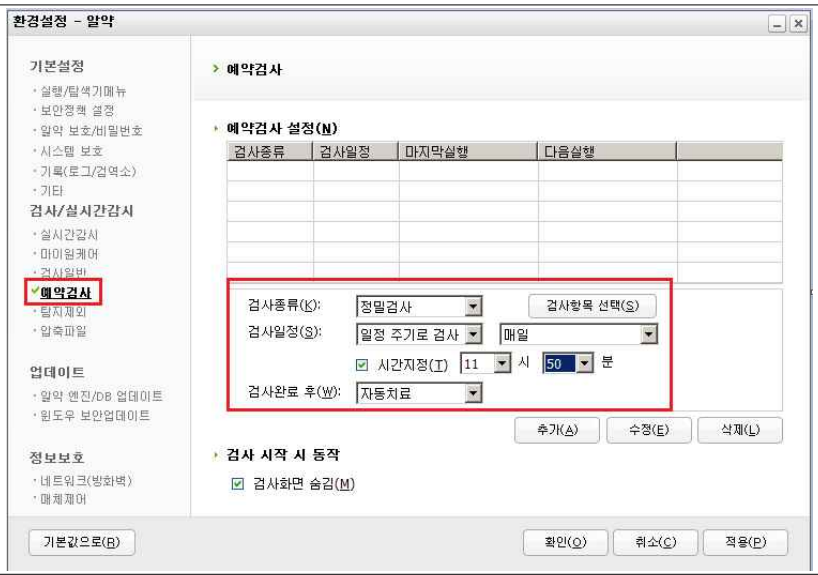
2. 백신 설치가 완료되면 [Menu]에서 [환경설정] 선택

* 예시) 알약 설치 시

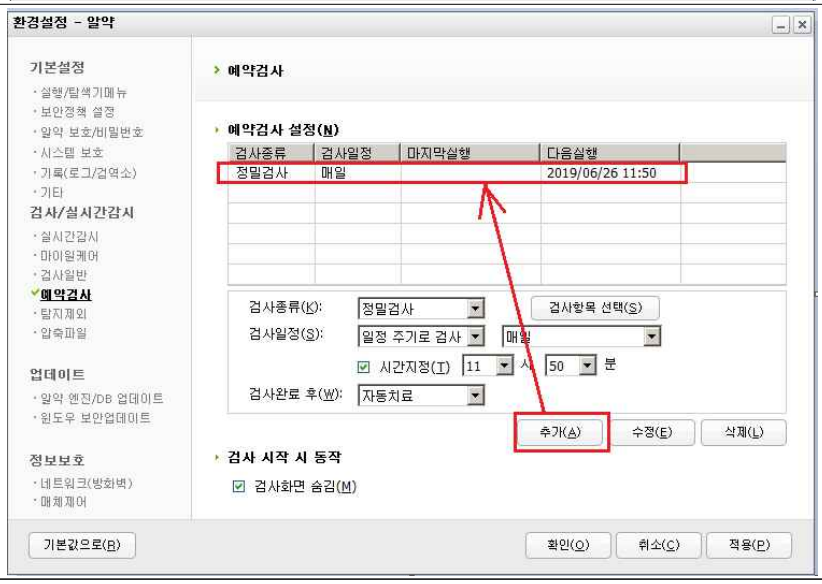
3. [예약검사]에서 우측 화면처럼

- 검사종류 : 정밀검사
- 검사일정 : 매일
- 시간 : 오전 11시50분
- 검사 완료 후 : 자동치료

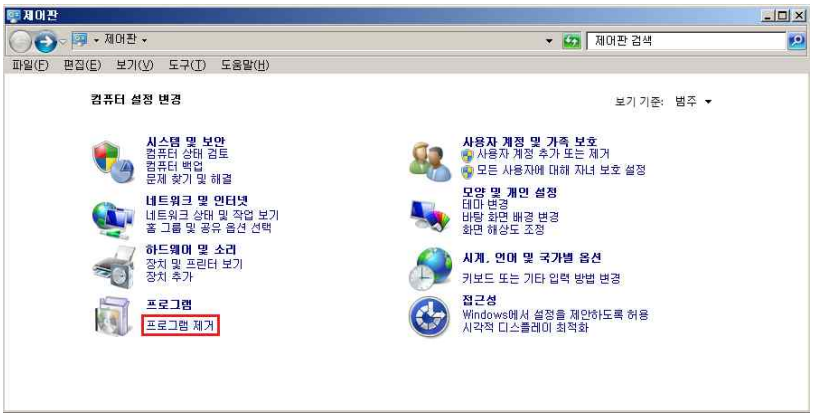
등으로 설정



4. [추가] 버튼 클릭 후 [적용]→[확인] 순으로 저장



부록 7 검사 장비 PC에서 카카오톡·라인·밴드 등 불필요 프로그램 삭제 방법

1. 제어판 실행(시작 → 제어판)	
2. [프로그램 제거] 선택	
3. 프로그램 목록에서 [카카오톡] 선택하여 제거 ※ SNS 프로그램(카카오톡, 라인, 밴드 등) 삭제