[별표 6] 보안관리실태 점검표(제18조 관련)

□ 제어시스템 보안관리 점검표

순번	점검 내용	확인
1	제어시스템은 업무망·인터넷 등 외부망과 물리적으로 분리·운영하고 외부망과 연결접점이 없는가?	
2	비인가 PC·서버 및 네트워크의 접속을 차단하였는가?	
3	제어망에서 업무망으로 자료전송을 위한 일방향 전송장비 또는 침입차단시스템 운영시 보안정책 설정이 적절한가?	
4	각종 시스템에 사용자별 또는 그룹별로 접근권한을 부여하였는가?	
5	비밀번호 사용시 숫자, 문자, 특수문자를 혼합하여 9자리 이상을 사용하고 있는가?	
6	제어시스템 및 관련 장비 도입시 보안 요구사항에 따른 검증을 실시하였는가?	
7	정보시스템 자산에 대해 최신 현황을 유지하고 있는가?	
8	중요자료는 대외비 이상으로 생산하여 독립PC 또는 보안USB 보관, 암호화 등 안전하게 관리하고 있는가?	
9	PC·서버에 불필요한 서비스 포트 제거 및 공유 금지를 하고 있는가?	
10	PC·서버에 제어시스템 운영 관련 프로그램만 설치하고 불필요한 프로그램은 제거하였는가?	
11	PC·서버에 USB 자동실행 기능을 차단하고 있는가?	
12	서버·정보보호시스템·네트워크 장비 등에 사고발생시 추적을 위한 접근기록을 1년 이상 보관하고 있는가?	
13	USB·LAN포트를 잠금장치·보안스티커 등을 사용하여 물리적으로	

	봉인하고, 봉인장치 개폐시 사용내역을 기록 유지하고 있는가?	
14	PC·서버에 최신 백신 프로그램을 설치하고 전수검사를 하였는가?	
15	백신 프로그램을 설치할 수 없는 단말기에 대해 프로세스 점검, 비인가 기기 접속여부 등을 점검하였는가?	
16	PC·서버의 운영체제 등 S/W에 대해 최신 보안패치를 하였는가?	
17	자료 전송시 광디스크를 사용하거나 지정된 전용단말기를 사용하고 있는가?	
18	'클린PC' 사용시 백신 검사, 특정사이트로 접속 제한 등 보안조치를 하였는가?	
19	제어시스템에 USB 사용을 금지하고 있는가?	
20	휴대용 저장매체 관리대장을 현행화하고 관리실태를 점검하였는가?	
21	휴대용 기기에 대한 반·출입 통제를 하고 있는가?	
22	외부에서 반입·사용하는 정보통신기기에 대해 포맷 후 필요한 프로그램만 설치 등 보안조치 하였는가?	
23	취약점 분석·평가 및 보호대책 이행여부 확인 결과 발견된 문제점을 보완조치 하였는가?	
24	사이버위기를 가정한 대응 모의훈련을 실시하고 비상대비체계의 정상작동 여부를 점검하였는가?	

□ 정보시스템 보안관리 점검표

순번	점검 내용	확인
1	웹서버 등 외부 공개용 서버는 DMZ 구간에, DB서버 등 중요 서버는 내부 구간에 위치하는 등 네트워크 구성이 적절한가?	
2	정보시스템은 다른 정보통신망(인터넷 포함)과 분리 운영하고 있는가?	
3	정보시스템 연결 업무망 PC는 인터넷과 분리되어 있는가?	
4	정보시스템과 원격지 연결은 전용회선 또는 가상사설망 구축 등 안전한 수단을 활용하고 있는가?	
5	비인가 PC·서버 및 네트워크의 접속을 차단하였는가?	
6	각종 시스템에 사용자별 또는 그룹별로 접근권한을 부여하였는가?	
7	비밀번호 사용시 숫자, 문자, 특수문자를 혼합하여 9자리 이상을 사용하고 있는가?	
8	네트워크 트래픽 보안정책이 적절하게 설정되어 있는가?	
9	정보시스템 자산에 대해 최신 현황을 유지하고 있는가?	
10	중요자료는 대외비 이상으로 생산하여 독립PC 또는 보안USB 보관. 암호화 등 안전하게 관리하고 있는가?	
11	백업시스템에 대해 보안점검을 실시하였는가?	
12	PC·서버에 정보시스템 운영 관련 프로그램만 설치하고 불필요한 프로그램은 제거하였는가?	
13	서버·정보보호시스템·네트워크 장비 등 시스템에서 불필요한 서비스 포트 및 원격연결 서비스를 통제하였는가?	
14	불필요한 공유폴더 또는 비인가 파일서버 사용을 통제하였는가?	

15	PC·서버에 USB 자동실행 기능을 차단하였는가?	
16	서버·정보보호시스템·네트워크 장비 등에 사고발생시 추적을 위한 접근기록을 1년 이상 보관하고 있는가?	
17	서버·정보보호시스템·네트워크 장비 등 시스템에 대한 접근통제 정책을 점검, 갱신하였는가?	
18	PC·서버에 최신 백신 프로그램을 설치하고 전수검사를 하였는가?	
19	PC·서버의 운영체제 등 S/W에 대해 최신 보안패치를 하였는가?	
20	백신 및 패치 관리서버에 대해 업데이트를 실시하고 악성코드 감염 여부 및 접속기록을 점검하였는가?	
21	휴대용 저장매체 관리대장을 현행화하고 관리실태를 점검하였는가?	
22	휴대용 기기에 대한 반·출입 통제를 하고 있는가?	
23	웹서버의 최신 웹 취약점을 제거하였는가?	
24	정보시스템에 대한 외부 침해시도 여부를 모니터링하고 로그자료를 분석하였는가?	
25	취약점 분석·평가 및 보호대책 이행여부 확인 결과 발견된 문제점을 보완조치 하였는가?	