

## 주요정보통신기반시설 취약점 분석·평가 점검항목(총 453개)

구분	상	중하	계	
관리적 점검항목	39	75	114	
물리적 점검항목	7	19	26	
기술적 점검항목	유닉스	43	30	73
	윈도우	45	37	82
	보안장비	16	10	26
	네트워크장비	14	24	38
	제어시스템	16	6	22
	PC	14	6	20
	DB	11	13	24
	웹	28	0	28
기술적 점검항목 소계	187	126	313	
합 계	233	220	453	

### □ 관리적 점검항목

분류	번호	취약점 점검 항목	등급
정보 보호정책	A-1	조직 전반에 적용하고 있는 정보보호 정책/지침 또는 규정이 수립되었는가?	상
	A-2	정기적으로 정보보호정책의 타당성을 검토, 평가하여 수정 보완하고 있는가?	상
	A-3	연도별 정보보안업무 세부추진 계획을 수립·시행하고 그 추진결과에 대한 심사분석·평가를 실시하는가	상
	A-4	최근 1년간 기관장에게 연간 보호대책 등의 주요 정보보안 관련 사항을 보고하였는가?	상
	A-5	정보보호정책이 문서화되어 있으며 경영자층의 승인을 받고 있는가?	중
	A-6	정보보호정책서가 모든 임직원 및 관련자에게 배포되고 모든 임직원 및 관련자가 정보보호정책을 이해하고 있는가?	중
	A-7	정보보호정책의 내용과 기관의 사업 목표 및 전략 등과의 일관성이 검토되었는가?	하
	A-8	기관의 정보보안 강화를 위한 중장기(3년 이상) 계획이 있는가?	중
정보 보호조직	A-9	보안활동을 계획, 실행, 검토하는 보안 전담조직 및 전담 보안 담당자가 구성되어 있는가?	상
	A-10	보안관련 전문가 집단으로부터 조언을 받고 해당 내용을 반영하고 있는가?	중
	A-11	정보보호 관련 주요 의사결정을 수행하는 정보보호위원회가 구성되어 있으며 위원회의 역할 및 책임이 명확히 기술되어 있는가?	하
	A-12	정보보호관리자의 역할 및 책임이 규명되어 있는가?	하
인적 보안	A-13	신원조회(민간기관 제외)가 수행되고 비밀유지서약서를 작성하고 있으며 주기적으로 갱신되고 있는가?	상
	A-14	계약직 및 임시직원은 물론 정식직원 채용 시 신원, 업무능력, 교육정도, 경력 등에 대한 적격심사가 이루어지고 있는가?	상
	A-15	민감한 직무담당자에 대해 강화된 적격심사가 수행되고 있는가?	하
	A-16	모든 인력에 대하여 정보보호의 책임과 역할을 기술하는 직무기술서가 존재하는가?	중
	A-17	정보보안정책을 불이행할 경우 이에 대한 징계가 규정에 명시되어 있는가?	중
	A-18	고용계약 만료시 자산 반납 및 접근권한을 삭제하는 절차가 있는가?	중

분류	번호	취약점 점검 항목	등급
외부자 보안	A-19	제3자(외부유지보수직원, 외부용역자포함)에 의한 정보자산 접근과 관련한 보안요구 사항을 계약에 포함하고 있는가?	상
	A-20	위탁 기관(업체) 또는 용역사업 참여 업체의 보안관련사항 위반이나 침해사고 발생 시 조치를 수행하는가?	상
	A-21	제3자의 보안요구사항 준수 검토를 위해 제3자 관리책임자로부터 보안관리 상황에 대한 주기적인 보고를 받고 수시 점검을 수행하는가?	하
	A-22	외부 관계자에게 정보나 자산에 접근할 수 있는 보안 규정을 사전 통보하고 있는가?	하
	A-23	제3자(외부유지보수직원, 외부용역자포함)에 대한 보안서약서를 가지고 있는가?	하
자산 분류	A-24	조직의 중요한 자산(인력, 시설, 장비 등)에 대한 자산분류기준이 있는가?	상
	A-25	정보자산을 보안등급과 중요도 등에 따라 분류하여 관리하고 있는가?	상
	A-26	정보자산별로 책임자가 지정되어 있으며 소유자, 관리자, 사용자들이 확인되고 있는가?	상
	A-27	조직의 주요 자산 목록을 작성하고 변경사항을 유지 관리하고 있는가?	하
	A-28	자산에 대한 등급별 보호절차, 접근제한을 실시하고 있는가?	하
매체 관리	A-29	미디어 장치의 사용 및 반출입에 대한 관리절차나 문서가 있는가?	상
	A-30	정보나 매체가 용도 폐기되기 위한 폐기 방법이 수립되고 적절하게 이행되는가?	상
	A-31	안전을 요하는 매체가 운반될 때 접근 통제가 이루어지고 있는가?	하
	A-32	노트북, USB 메모리 등 이동형 장치의 분실을 통한 자료 유출 대책이 있는가?	중
	A-33	보조기억매체의 사용을 주기적 점검을 통해 최신자료를 유지하는가?	중
교육 및 훈련	A-34	교육 훈련 대상은 관련된 모든 내외 임직원 및 외부 인력을 포함하고 있으며 정보자산에 간접적으로 접근하는 일반 외부 용역 직원에 대해서도 정보보호교육훈련을 수행하는가?	상
	A-35	정보보호 인식제고를 위한 교육 및 훈련 계획을 종합적으로 수립하여 정기적으로 실시하고 있는가?	중
	A-36	교육 및 훈련은 대상자의 직위 및 업무 특성에 따라 구분하여 실시하고 있는가?	하
	A-37	교육 훈련의 효과가 측정, 분석되어 차기 교육에 반영되는가?	하
	A-38	직원을 대상으로 사이버안전센터 보안권고문 해킹메일주의공지, 윈도우 보안업데이트 사항, 보안취약점 조치요령 등을 공지하는가?	중
접근 통제	A-39	업무 요구사항에 따라 접근통제의 방법과 범위 등을 정의하고 문서화하고 있는가?	상
	A-40	허가된 원격작업내용, 작업시간, 접근허가된 내부 시스템 및 서비스 등의 내용을 포함한 재택근무 등의 원격작업에 대한 정책, 절차가 존재하는가?	상
	A-41	스마트폰·개인휴대단말기(PDA) 전자제어장비 등 첨단 정보통신기기를 활용하는 경우, 업무자료 등 중요정보 보호 및 안전한 전송을 위한 방안이 마련되어 있는가?	상
	A-42	정보통신망에 비인가 PC·노트북 등을 연결시 차단하는가?	상
	A-43	정보시스템 및 정보보호시스템 접근기록의 비인가 열람, 훼손 등을 방지하기 위한 대책이 있는가?	상
	A-44	무선랜(Wi-Fi 등)은 국가정보원장의 보안성 검토를 필하거나 암호키 설정 등의 적절한 보안 조치를 적용하였는가?	상
	A-45	무선랜 무단 사용 여부, 비인가 무선 중계기(AP) 설치 여부, 우회 정보통신망 사용 차단 여부 등을 주기적으로 점검하는가?	상
	A-46	접근통제에 대한 주기적 검토를 통해 접근통제 정책이 적합한지를 확인하고 있는가?	중
	A-47	보안상 중요한 접근통제 규칙은 관리자의 승인을 거쳐서 설정 또는 변경하도록 하고 있는가?	하
	A-48	접근통제 방법은 내부 관련 정책 및 절차에 따라 결정되어 반영되는가?	하
	A-49	안전한 로그온 절차, 식별 및 인증관리 등과 같은 시스템 운영체제 접근 통제 방법이 존재하고 이에 따라 이행하고 있는가?	중
	A-50	외부에서의 사용자 접근에 대한 안전한 인증방식을 사용하고 있는가?	하
	A-51	외부에서 내부 시스템의 기능을 사용할 수 있다면 VPN 등 안전한 접속방법을 제공하고 있는가?	하

분류	번호	취약점 점검 항목	등급
접근 통제	A-52	제3자가 원격에서 진단, 관리 등을 위한 서비스를 제공할때 필요할 때만 연결을 허용하고 있는가?	하
	A-53	제3자외의 정보 공유, 네트워크 공유 등에 대한 보안위협에 대한 대책이 있는가?	하
	A-54	민감한 시스템에 따라 네트워크를 분리 운영하여 서로간의 접근을 막고 있는가?	하
	A-55	방화벽, 침입탐지 등 안전한 네트워크를 위한 대책을 마련하고 있는가?	중
	A-56	내부망(업무망)과 인터넷망을 분리하여 사용하는가?	중
	A-57	망분리 후 안전한 자료전송을 위한 시스템을 도입하여 사용하고 있는가?	중
	A-58	인터넷 전화망과 일반 전선망은 분리하여 운용하는가?	하
	A-59	제3자의 내부 상주 인력에 대한 네트워크를 분리 운영하고 있는가?	하
	운영 관리	A-60	개발 테스트 설비는 실제 운영설비와 분리되어 있는가?
A-61		시스템을 도입하기 전에 보안성 검토 및 호환성 검토를 실시하는가?	상
A-62		시스템 및 사용 장비에 대한 보안 취약점에 대한 주기적 검토 및 보완 프로세스가 있는가?	상
A-63		바이러스, 악성코드 등에 대한 대비책을 가지고 있는가?	상
A-64		보안규정의 이행여부를 확인하는 주기적인 보안점검 및 불시 보안점검이 이루어지고 있는가?	상
A-65		시스템 및 패스워드 관리지침을 제공하고 시스템 및 패스워드 관리책임을 주지시키고 있는가?	상
A-66		전자기록 보관을 위한 별도의 방법(아카이빙)이 존재하고, 이를 통한 관리를 하고 있는가?	상
A-67		'사이버보안진단의 날' 등과 같이 월별 보안 중점점검사항에 대해 매월 점검하고 조치하는가?	상
A-68		비밀(대외비 포함)을 비밀관리기록부에 등재하여 관리하는가?	상
A-69		출력된 비밀문서의 경우 비밀합동보관소 등에 안전하게 보관되어 있는가?	상
A-70		비밀 등 중요 정보의 안전한 처리를 위한 시스템을 도입하여 사용하고 있거나 이를 계획하고 있는가?	상
A-71		정보통신망 세부 구성현황 등을 대외비 이상으로 관리하는가?	상
A-72		정보보호시스템은 국내용 CC인증을 받았거나, 보안적합성 검증을 받았는가?	상
A-73		보안책임자는 정보자산 도입 시 보안 정책에 부합하는지 확인하고 승인하는가?	하
A-74		보안정책에 의해 정의된 운영지침과 절차는 문서화되어 관리되고 있는가?	중
A-75		정보시스템의 변경관리 절차가 존재하며 이에 따라 변경관리가 수행되는가?	중
A-76		중요 시스템 및 정보보호제품의 설정관리가 승인과정을 통해 이행되는가?	중
A-77		개발자와 운영자의 접근 권한은 분리되어 있는가?	중
A-78		중요 데이터와 일반데이터가 다른 서버에 분리되어 보관되는가?	하
A-79		장애탐지, 장애기록, 장애분석, 장애복구, 장애보고 등의 사항을 포함하는 시스템의 장애관리 지침이 존재하는가?	하
A-80		네트워크 운영 보안 유지를 위해 접근권한 통제, 원격접속 관리, 네트워크 분리 등의 내용을 포함한 네트워크 운영 보안정책이 수립되어 이행되는가?	하
A-81		시스템과 네트워크의 사용 및 접근에 대한 모니터링 절차와 책임이 정의되어 있고 이에 따라 이행하고 있는가?	하
A-82		네트워크를 통해 시스템을 운영하는 경우 원칙적으로 시스템 관리는 내부의 특정 터미널에서만 할 수 있도록 제한하고 있는가?	중
A-83		네트워크, 메신저 등으로부터의 허가되지 않았거나 불분명한 파일의 다운로드를 금지하고, 부득이 다운로드받을 경우 바이러스 검사를 받는가?	중
A-84		유지보수 도구를 사용하기 위한 사용 승인 및 통제, 감독이 이루어지는가?	하
A-85		원격 유지보수 및 진단 활동에 대한 감시가 이루어지는가?	하
A-86		암호키에 대한 관리지침이 마련되어 있고 이에 따라 관리되고 있는가?	중
A-87		암호키를 복구하기 위한 복구 절차가 수립되고 복구 내역이 확인되는가?	하
A-88		침입차단 및 탐지 도구는 조직의 보안 정책과 규칙에 적합하게 설치되어 있는가?	하
A-89		공중망 및 사설망 통신경로에 대한 신뢰성을 평가하고 있는가?	하
A-90	스팸 메일 수신을 줄이기 위한 방안(스팸차단 솔루션)이 마련되어 있는가?	하	

분류	번호	취약점 점검 항목	등급
운영 관리	A-91	홈페이지 게시 자료에 대해 게시 절차를 마련하고 시행하고 있는가?	중
	A-92	업무용 시스템 및 홈페이지 등 정보시스템의 소스코드를 관리하는가?	중
업무 연속성	A-93	업무복구목표와 요구사항에 적합한 업무연속성 전략을 수립하였는가?	상
	A-94	모의 훈련 등을 통한 업무 연속성 관리가 지속적으로 검토되고 있으며 조직내의 변경이 있을 경우 이에 대한 사항이 반영되고 있는가?	중
	A-95	보안중요성이 높은 등급의 시스템들은 이중화하여 관리하고 있는가?	중
사고 대응	A-96	백업은 정기적으로 수행하고 물리적으로 분리된 지역에 보관하는가?	중
	A-97	침해사고 발생시 신속한 보안사고보고를 위한 절차가 문서화되어 있고 이에 따라 신속한 보고가 이루어지고 있는가?	상
	A-98	DDoS 대응 체계를 수립하고 주기적인 훈련을 실시하고 있는가?	상
	A-99	개인정보보호를위해DB암호화등개인정보유출에대한방안이마련되어있는가?	상
	A-100	부정접근 사례나 보안사고 내역을 지속적으로 모니터링 하고 있는가?	하
	A-101	보안사고 유형, 범위, 영향 등을 포함한 보안사고 분석이 기록되어 관리 되는가?	중
	A-102	보안 취약점 및 사고 발생시 이에 대한 보완작업 절차를 마련하고 있는가?	중
	A-103	사이버침해사고 발생 후 재발방지 대책을 수립하고 시행하였는가?	중
	A-104	침해사고 대응계획 즉 대응범위, 역할, 임무, 대응절차 등이 문서화되어 있는가?	하
	A-105	사이버위키 '주의'이상 경보 발령 및 피해발생 등 필요시 대응할 수 있는 '긴급대응반'이 구성되어 있는가?	중
감사	A-106	침해사고시 외부기관 및 전문가들과의 대응협조체계가 구축되어 있는가?	중
	A-107	침해사고 대응절차 및 방법 숙지를 위해 정기적인 교육을 실시하는가?	중
	A-108	서비스 거부 공격에 대해 공격 정도에 따른 대응 방안이 수립되어 있는가?	하
	A-109	내부의 DDoS공격방지(그린DDoSZone)를 위한 대응방안이 있는가?	중
	A-110	정보시스템 관련 법, 규제, 계약상의 요구사항을 정의하고 문서화하고 있는가?	하
	A-111	특허권 및 저작권법, 컴퓨터프로그램보호법 등 관련 법규를 준수하고 있는가?(불법 복제 및 해킹판 소프트웨어의 사용 금지 등)	하
	A-112	보안사고 처리, 계약중빙 및 소송 등을 위한 적절한 증거자료 확보에 관한 지침이 존재하고, 이에 따라 이행되고 있는가?	하
	A-113	주기적으로 보안감사계획을 수립하고 시행하고 있는가?	하
	A-114	감사결과를 관리책임자에게 보호하여 적절한 사후관리를 시행하고 있는가?	하

## □ 물리적 점검항목

분류	번호	취약점 점검 항목	등급
접근 통제	P-1	주요 시스템에 대한 별도의 출입통제를 실시하거나 이중의 보호장치를 설치하고 있는가?	상
	P-2	보호 구역의 출입에 관한 정책과 절차가 수립되어 있으며 이에 따라 출입통제가 되고 있는가?	상
	P-3	민감한 시설에 대해 물리적으로 접근하는 사람들의 출입기록 및 허가의 타당성을 주기적으로 검토하는가?	중
감시 통제	P-4	주요시설의 출입구와 전산실 및 통신장비실 내부에 CCTV를 설치하고 있는가?	상
	P-5	CCTV 운용 시 중계 관제서버, 관리용 PC, 정보통신망 등에 대해 보안대책을 수립하는가?	상
	P-6	주요시설에 대한 출입기록은 출입일로부터 일정기간 이상 보관하고 있는가?	상
	P-7	외부인에대해서출입증을발급하고,출입권한은출입목적에필요한구역내로한정하는가?	상
	P-8	제한구역에서의 작업에 대한 추가적인 통제 수단 및 안내 지침이 존재하는가?	중
	P-9	전산 장비실에 외부협력업체 출입 시 내부 임직원이 상시 동행하는가?	중
	P-10	시각적으로 구분이 가능한 신분증을 가지고 있으며 패용하고 있는가?	하
	P-11	유리창 내 파손감지기, 진동감지기 등 침입감지와 관련된 장비를 설치하여 감시하고 있는가?	하

분류	번호	취약점 점검 항목	등급
전력 보호	P-12	전원공급 이상이나 기타 전기관련 사고로부터 장비가 보호되고 있는가? (UPS, 비상발전기, 이중전원선 등의 설비)	상
	P-13	전원공급 이상이나 기타 전기관련 사고로부터 장비를 보호하기 위해 설비 상태에 대해 정기적으로 검토하는가?	하
	P-14	전원선 및 통신선은 도청이나 손상으로부터 보호되고 있는가?	중
	P-15	누전이 발생하였을 때 이를 차단할 수 있도록 누전차단기 또는 누전경보기가 설치되어 있는가?	중
환경 통제	P-16	소방훈련과 같은 재해훈련 시 비상탈출 및 복귀절차가 확립되어 있는가?	하
	P-17	물리적 중요도에 따라 제한구역, 통제구역 등으로 분류하는 다단계 보호 대책이 있는가?	중
	P-18	제한구역의 선택, 설계시 화재, 홍수, 폭발, 폭동 혹은 다른 형태의 자연재해 또는 인재로 인한 피해가능성을 고려하였는가?	하
	P-19	데이터센터는 물리적, 환경적 위험이 적은 곳에 위치하고 건물구조가 안정성을 확보하고 있는가?	하
	P-20	주요장비, 대체시스템 및 자료들이 화재, 습도 등의 환경재해로부터 보호되는 적절한 곳에 배치되어 보호되고 있는가?	중
	P-21	전산실에 24시간 환은, 향습을 유지하기 위하여 온습도 측정이 가능하도록 환온환습기가 설치되어 있는가?	하
	P-22	전산실은 천장을 통하여 외부와의 왕래가 불가능하도록 전산실의 벽면과 접한 천장을 차단하는 조치가 되어 있는가?	하
	P-23	방재센터는 화재감지센서의 작동상황이 실시간으로 파악되도록 하고, 화재발생시에 경보신호를 통해 상황을 알 수 있도록 화재감지센서와 연동된 경보장치가 설치되어 있는가?	하
	P-24	주요시설(중앙감시실, 전산실, 전력관련시설, 통신장비실, 방재센터 등)에는 기존 조명설비의 작동이 멈추는 경우에도 작업이 가능하도록 비상조명이 설치되어 있는가?	중
	P-25	배달 및 하역구역은 비인가 지역과 격리되어 보호되고 있는가?	하
	P-26	단위면적당 규정하중을 견딜 수 있도록 설계되어 있는가?	하

## □ 기술적 점검항목

### 가. 유닉스

분류	번호	취약점 점검 항목	등급
계정 관리	U-1	root 계정 원격 접속 제한	상
	U-2	패스워드 복잡성 설정	상
	U-3	계정 잠금 임계값 설정	상
	U-4	패스워드 파일 보호	상
	U-5	root 이외의 UID가 '0' 금지	중
	U-6	root 계정 su 제한	하
	U-7	패스워드 최소 길이 설정	중
	U-8	패스워드 최대 사용 기간 설정	중
	U-9	패스워드 최소 사용기간 설정	중
	U-10	불필요한 계정 제거	하
	U-11	관리자 그룹에 최소한의 계정 포함	하

분류	번호	취약점 점검 항목	등급	
계정 관리	U-12	계정이 존재하지 않는 GID 금지	하	
	U-13	동일한 UID 금지	중	
	U-14	사용자 shell 점검	하	
	U-15	Session Timeout 설정	하	
	U-16	root 홈, 패스 디렉터리 권한 및 패스 설정	상	
파일 및 디렉토리 관리	U-17	파일 및 디렉터리 소유자 설정	상	
	U-18	/etc/passwd 파일 소유자 및 권한 설정	상	
	U-19	/etc/shadow 파일 소유자 및 권한 설정	상	
	U-20	/etc/hosts 파일 소유자 및 권한 설정	상	
	U-21	/etc/(x)inetd.conf 파일 소유자 및 권한 설정	상	
	U-22	/etc/syslog.conf 파일 소유자 및 권한 설정	상	
	U-23	/etc/services 파일 소유자 및 권한 설정	상	
	U-24	SUID, SGID, Sticky bit 설정 파일 점검	상	
	U-25	사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정	상	
	U-26	world writable 파일 점검	상	
	U-27	/dev에 존재하지 않는 device 파일 점검	상	
	U-28	\$HOME/.rhosts, hosts.equiv 사용 금지	상	
	U-29	접속 IP 및 포트 제한	상	
	U-30	hosts.lpd 파일 소유자 및 권한 설정	하	
	U-31	NIS 서비스 비활성화	중	
	U-32	UMASK 설정 관리	중	
	U-33	홈디렉토리 소유자 및 권한 설정	중	
	U-34	홈디렉토리로 지정한 디렉토리의 존재 관리	중	
	U-35	숨겨진 파일 및 디렉터리 검색 및 제거	하	
	서비스 관리	U-36	Finger 서비스 비활성화	상
		U-37	Anonymous FTP 비활성화	상
		U-38	r 계열 서비스 비활성화	상
		U-39	cron 파일 소유자 및 권한 설정	상
		U-40	DoS 공격에 취약한 서비스 비활성화	상
		U-41	NFS 서비스 비활성화	상
		U-42	NFS 접근통제	상
U-43		automountd 제거	상	
U-44		RPC 서비스 확인	상	
U-45		NIS, NIS+ 점검	상	
U-46		tftp, talk 서비스 비활성화	상	
U-47		Sendmail 버전 점검	상	
U-48		스팸 메일 릴레이 제한	상	
U-49		일반사용자의 Sendmail 실행 방지	상	
U-50		DNS 보안 버전 패치	상	
U-51		DNS ZoneTransfer 설정	상	
U-52		Apache 디렉터리 리스팅 제거	상	
U-53		Apache 웹 프로세스 권한 제한	상	
U-54		Apache 상위 디렉터리 접근 금지	상	
U-55		Apache 불필요한 파일 제거	상	
U-56		Apache 링크 사용금지	상	

분류	번호	취약점 점검 항목	등급
서비스 관리	U-57	Apache 파일 업로드 및 다운로드 제한	상
	U-58	Apache 웹 서비스 영역의 분리	상
	U-59	ssh 원격접속 허용	중
	U-60	ftp 서비스 확인	하
	U-61	ftp 계정 shell 제한	중
	U-62	Ftpusers 파일 소유자 및 권한 설정	하
	U-63	Ftpusers 파일 설정	중
	U-64	at 파일 소유자 및 권한 설정	중
	U-65	SNMP 서비스 구동 점검	중
	U-66	SNMP 서비스 커뮤니티스트링의 복잡성 설정	중
패치 관리	U-67	로그온 시 경고 메시지 제공	하
	U-68	NFS 설정 파일 접근 권한	중
	U-69	expn, vrfy 명령어 제한	중
	U-70	Apache 웹서비스 정보 숨김	중
로그 관리	U-71	최신 보안패치 및 벤더 권고사항 적용	상
	U-72	로그의 정기적 검토 및 보고	상
	U-73	정책에 따른 시스템 로깅 설정	하

## 나. 윈도우즈

점검분류	번호	취약점 점검 항목	등급
계정 관리	W-1	Administrator 계정 이름 바꾸기	상
	W-2	Guest 계정 상태	상
	W-3	불필요한 계정 제거	상
	W-4	계정 잠금 임계값 설정	상
	W-5	해독 가능한 암호화를 사용하여 암호 저장	상
	W-6	관리자 그룹에 최소한의 사용자 포함	상
	W-7	Everyone 사용 권한을 익명 사용자에게 적용	중
	W-8	계정 잠금 기간 설정	중
	W-9	패스워드 복잡성 설정	중
	W-10	패스워드 최소 암호 길이	중
	W-11	패스워드 최대 사용 기간	중
	W-12	패스워드 최소 사용 기간	중
	W-13	마지막 사용자 이름 표시 안함	중
	W-14	로컬 로그온 허용	중
	W-15	익명 SID/이름 변환 허용	중
	W-16	최근 암호 기억	중
	W-17	콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한	중
	W-18	원격터미널 접속 가능한 사용자 그룹 제한	중
서비스 관리	W-19	공유 권한 및 사용자 그룹 설정	상
	W-20	하드디스크 기본 공유 제거	상
	W-21	불필요한 서비스 제거	상
	W-22	IIS 서비스 구동 점검	상

분류	번호	취약점 점검 항목	등급	
서비스 관리	W-23	IIS 디렉토리 리스팅 제거	상	
	W-24	IIS CGI 실행 제한	상	
	W-25	IIS 상위 디렉토리 접근 금지	상	
	W-26	IIS 불필요한 파일 제거	상	
	W-27	IIS 웹 프로세스 권한 제한	상	
	W-28	IIS 링크 사용금지	상	
	W-29	IIS 파일 업로드 및 다운로드 제한	상	
	W-30	IIS DB 연결 취약점 점검	상	
	W-31	IIS 가상 디렉토리 삭제	상	
	W-32	IIS 데이터 파일 ACL 적용	상	
	W-33	IIS 미사용 스크립트 매핑 제거	상	
	W-34	IIS Exec 명령어 쉘 호출 진단	상	
	W-35	IIS WebDAV 비활성화	상	
	W-36	NetBIOS 바인딩 서비스 구동 점검	상	
	W-37	FTP 서비스 구동 점검	상	
	W-38	FTP 디렉토리 접근권한 설정	상	
	W-39	Anonymous FTP 금지	상	
	W-40	FTP 접근 제어 설정	상	
	W-41	DNS Zone Transfer 설정	상	
	W-42	RDS(RemoteDataServices)제거	상	
	W-43	최신 서비스팩 적용	상	
	W-44	터미널 서비스 암호화 수준 설정	중	
	W-45	IIS 웹서비스 정보 숨김	중	
	W-46	SNMP 서비스 구동 점검	중	
	W-47	SNMP 서비스 커뮤니티스트링의 복잡성 설정	중	
	W-48	SNMP Access control 설정	중	
	W-49	DNS 서비스 구동 점검	중	
	W-50	HTTP/FTP/SMTP 배너 차단	하	
	W-51	Telnet 보안 설정	중	
	W-52	불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거	중	
	W-53	원격터미널 접속 타임아웃 설정	중	
	W-54	예약된 작업에 의심스러운 명령이 등록되어 있는지 점검	중	
	패치 관리	W-55	최신 HOT FIX 적용	상
		W-56	백신 프로그램 업데이트	상
W-57		정책에 따른 시스템 로깅 설정	중	
로그 관리	W-58	로그의 정기적 검토 및 보고	상	
	W-59	원격으로 액세스할 수 있는 레지스트리 경로	상	
	W-60	이벤트 로그 관리 설정	하	
	W-61	원격에서 이벤트 로그 파일 접근 차단	중	
보안 관리	W-62	백신 프로그램 설치	상	
	W-63	SAM 파일 접근 통제 설정	상	
	W-64	화면보호기 설정	상	
	W-65	로그온하지 않고 시스템 종료 허용	상	
	W-66	원격 시스템에서 강제로 시스템 종료	상	

분류	번호	취약점 점검 항목	등급
보안 관리	W-67	보안 감사를 로그할 수 없는 경우 즉시 시스템 종료	상
	W-68	SAM 계정과 공유의 익명 열거 허용 안 함	상
	W-69	Autologon 기능 제어	상
	W-70	이동식 미디어 포맷 및 꺼내기 허용	상
	W-71	디스크볼륨 암호화 설정	상
	W-72	Dos공격 방어 레지스트리 설정	중
	W-73	사용자가 프린터 드라이버를 설치할 수 없게 함	중
	W-74	세션 연결을 중단하기 전에 필요한 유휴시간	중
	W-75	경고 메시지 설정	하
	W-76	사용자별 홈 디렉터리 권한 설정	중
	W-77	LAN Manager 인증 수준	중
W-78	보안 채널 데이터 디지털 암호화 또는 서명	중	
W-79	파일 및 디렉토리 보호	중	
W-80	컴퓨터 계정 암호 최대 사용 기간	중	
W-81	시작프로그램 목록 분석	중	
DB 관리	W-82	Windows 인증 모드 사용	중

#### 다. 보안 장비

분류	번호	취약점 점검 항목	등급
계정 관리	S-1	보안장비 Default 계정 변경	상
	S-2	보안장비 Default 패스워드 변경	상
	S-3	보안장비 계정별 권한 설정	상
	S-4	보안장비 계정 관리	상
	S-5	로그인 실패횟수 제한	중
접근 관리	S-6	보안장비 원격 관리 접근 통제	상
	S-7	보안장비 보안 접속	상
	S-8	Session timeout 설정	상
패치 관리	S-9	벤더에서 제공하는 최신 업데이트 적용	상
로그 관리	S-10	보안장비 로그 설정	중
	S-11	보안장비 로그 정기적 검토	중
	S-12	보안장비 로그 보관	중
	S-13	보안장비 정책 백업 설정	중
	S-14	원격 로그 서버 사용	중
	S-15	로그 서버 설정 관리	하
	S-16	NTP 서버 연동	중
기능 관리	S-17	정책 관리	상
	S-18	NAT 설정	상
	S-19	DMZ 설정	상
	S-20	최소한의 서비스만 제공	상
	S-21	이상징후 탐지 경고 기능 설정	상
	S-22	장비 사용량 검토	상
	S-23	SNMP 서비스 확인	상
	S-24	SNMP community string 복잡성 설정	상

분류	번호	취약점 점검 항목	등급
기능 관리	S-25	부가 기능 설정	중
	S-26	유해 트래픽 차단 정책 설정	중

#### 라. 네트워크 장비

분류	번호	취약점 점검 항목	등급
계정 관리	N-1	패스워드 설정	상
	N-2	패스워드 복잡성 설정	상
	N-3	암호화된 패스워드 사용	상
	N-4	사용자 · 명령어별 권한 수준 설정	중
접근 관리	N-5	VTY 접근(ACL) 설정	상
	N-6	Session Timeout 설정	상
	N-7	VTY 접속 시 안전한 프로토콜 사용	중
	N-8	불필요한 보조 입출력 포트 사용 금지	중
	N-9	로그온 시 경고 메시지 설정	중
패치 관리	N-10	최신 보안 패치 및 벤더 권고사항 적용	상
로그 관리	N-11	원격 로그서버 사용	하
	N-12	로그 버퍼 크기 설정	중
	N-13	정책에 따른 로그 설정	중
	N-14	NTP 서버 연동	중
	N-15	timestamp 로그 설정	하
기능 관리	N-16	SNMP 서비스 확인	상
	N-17	SNMP community string 복잡성 설정	상
	N-18	SNMP ACL 설정	상
	N-19	SNMP 커뮤니티 권한 설정	상
	N-20	TFTP 서비스 차단	상
	N-21	Spoofing 방지 필터링 적용	상
	N-22	DDoS 공격 방어 설정	상
	N-23	사용하지 않는 인터페이스의 shutdown 설정	상
	N-24	TCP keepalive 서비스 설정	중
	N-25	Finger 서비스 차단	중
	N-26	웹 서비스 차단	중
	N-27	TCP/UDP small 서비스 차단	중
	N-28	Bootp 서비스 차단	중
	N-29	CDP 서비스 차단	중
	N-30	Directed-broadcast 차단	중
	N-31	Source 라우팅 차단	중
	N-32	Proxy ARP 차단	중
	N-33	ICMP unreachable, Redirect 차단	중
N-34	identd 서비스 차단	중	
N-35	Domain lookup 차단	중	
N-36	pad 차단	중	
N-37	mask-rely 차단	중	
N-38	스위치 허브 보안 강화	하	

## 마. 제어시스템

분류	번호	취약점 점검 항목	등급
계정 관리	C-1	제어시스템 운영, 관리를 위한 계정이 타 사용자와 공유되지 않음	상
	C-2	ID/PW, 접속경로, 인증서 등이 하드코딩되지 않음	상
	C-3	제어시스템 운영, 관리를 위한 계정의 로그인, 사용 기록 저장	상
패치 관리	C-4	제어시스템에 대한 최신 업데이트, 보안패치를 안전하게 적용하기 위한 테스트 등의 절차 수립	상
접근 통제	C-5	제어시스템 운영자의 운영 권한은 제한된 범위 및 명령으로 제한	상
	C-6	제어시스템은 업무망, 인터넷 망과 물리적으로 분리	상
	C-7	제어 네트워크 외부와 자료연계시 물리적 일방향 환경을 구축하여 제어 네트워크로의 침입을 근본적으로 차단	상
	C-8	제어 네트워크에 무선인터넷, 테더링, 외부 유선망 연결 등의 외부망 연결을 제한하고 점검	상
	C-9	제어 네트워크에 비인가된 시스템에 대한 연결 및 접속 차단	상
보안 관리	C-10	제어시스템 구성도, 운용 매뉴얼, 비상조치 절차서 등을 작성하고 최신으로 관리	상
	C-11	제어시스템에서의 USB 사용을 금지하고, 사용시 USB 등의 이동형 저장매체 사용 통제	상
	C-12	제어명령에 대한 위변조 방지 대책 적용	상
	C-13	제어명령 replay 공격에 대한 방지 대책 적용	상
	C-14	제어시스템 개발자, 운영자, 관리자에 대한 접근권한 분리	상
	C-15	제어시스템, 제어기기에 (vendor default) 은닉서비스 및 취약한서비스가 없도록 설정	상
	C-16	제어프로그램의 입력창에 비정상적인 특장값을 입력할 시 사전에 정의한 에러 메시지가 출력되도록 하여 시스템 중요정보가 노출되지 않도록 설정	상
	C-17	정보시스템에 대한 정책과 별도로 제어시스템에 대한 정보보안 정책, 지침이 수립되어 있는가?	중
	C-18	비인가자 또는 인증과정이 없이 제어시스템, 제어기기에 대한 환경 설정이 가능하지 않도록 되어있는가?	중
	C-19	제어시스템 및 운영시스템은 제어를 위한 목적으로만 사용되도록 다른 기능 및 서비스를 제거하였는가?	중
	C-20	운영에 있어 사용가능한 제어명령 및 안전한 제어를 위한 파라미터의 범위를 제한하고 있는가?	중
	C-21	제어시스템 개선, 신규 시스템 도입, 패치 및 수정 시, 안전성을 테스트하기 위한 테스트베드 또는 시험환경을 구축하였는가?	중
	C-22	제어 네트워크는 각각의 세부망으로 세분화하고 제어시스템 운영에 필요한 네트워크, 시스템간으로 통신을 제한하고 있는가?	중

## 바. PC

분류	번호	취약점 점검 항목	등급
계정 관리	PC-1	패스워드의 주기적 변경	상
	PC-2	패스워드 정책이 해당기관의 보안정책에 적합하게 설정	상
	PC-3	복구 콘솔에서 자동 로그인을 금지하도록 설정하여 사용하고 있는가?	중
서비스 관리	PC-4	공유폴더 제거	상
	PC-5	불필요한 서비스 제거	상
	PC-6	Windows Messenger(MSN, .NET 메신저 등)와 같은 상용 메신저의 사용 금지	상
	PC-7	파일 시스템이 NTFS 포맷으로 되어 있는가?	중
	PC-8	대상 시스템이 windows 서버를 제외한 다른 OS로 멀티 부팅이 가능하지 않도록 설정하여 사용하는가?	중
	PC-9	브라우저 종료 시 임시 인터넷 파일 폴더의 내용을 삭제하도록 설정하여 사용하는가?	하

분류	번호	취약점 점검 항목	등급
패치 관리	PC-10	HOT FIX 등 최신 보안패치 적용	상
	PC-11	최신 서비스팩 적용	상
	PC-12	MS-Office, 한글, 어도브 아크로벳 등의 응용 프로그램에 대한 최신 보안 패치 및 벤더 권고사항 적용	상
보안 관리	PC-13	바이러스 백신 프로그램 설치 및 주기적 업데이트	상
	PC-14	바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화	상
	PC-15	OS에서 제공하는 침입차단 기능 활성화	상
	PC-16	화면보호기 대기 시간을 5~10분으로 설정 및 재시작시 암호로 보호하도록 설정	상
	PC-17	CD, DVD, USB메모리 등과 같은 미디어의 자동실행 방지 등 이동식 미디어에 대한 보안대책 수립	상
	PC-18	PC 내부의 미사용(3개월) ActiveX 제거	상
	PC-19	시스템 부팅 시 Windows Messenger가 자동으로 시작되지 않도록 설정되어 있는가?	중
	PC-20	원격 지원을 금지하도록 정책이 설정되어 사용되는가?	중

## 사. 데이터베이스

분류	번호	취약점 점검 항목	등급
계정 관리	D-1	기본 계정의 패스워드, 정책 등을 변경하여 사용	상
	D-2	scott 등 Demonstration 및 불필요 계정을 제거하거나 잠금설정 후 사용	상
	D-3	패스워드의 사용기간 및 복잡도를 기관의 정책에 맞도록 설정	상
	D-4	데이터베이스 관리자 권한을 꼭 필요한 계정 및 그룹에 대해서만 허용	상
	D-5	패스워드 재사용에 대한 제약이 설정되어 있는가?	중
	D-6	DB 사용자 계정을 개별적으로 부여하여 사용하고 있는가?	중
접근 관리	D-7	원격에서 DB 서버로의 접속 제한	상
	D-8	DBA이외의 인가되지 않은 사용자가 시스템 테이블에 접근할 수 없도록 설정	상
	D-9	오라클 데이터베이스의 경우 리스너의 패스워드를 설정하여 사용	상
	D-10	불필요한 ODBC/OLE-DB 데이터 소스와 드라이버를 제거하고 사용하는가?	중
	D-11	일정 횟수의 로그인 실패 시 이에 대한 잠금정책이 설정되어 있는가?	중
	D-12	데이터베이스의 주요 파일 보호 등을 위해 DB 계정의 umask를 022 이상으로 설정하여 사용하는가?	하
	D-13	데이터베이스의 주요 설정파일, 패스워드 파일 등과 같은 주요 파일들의 접근 권한이 적절하게 설정되어 있는가?	중
	D-14	관리자 이외의 사용자가 오라클 리스너의 접속을 통해 리스너 로그 및 trace 파일에 대한 변경이 가능하지 않는가?	하
옵션 관리	D-15	응용프로그램 또는 DBA 계정의 Role이 Public으로 설정되지 않도록 조정	상
	D-16	OS_ROLES, REMOTE_OS_AUTHENTICATION, REMOTE_OS_ROLES를 FALSE로 설정	상
	D-17	패스워드 확인함수가 설정되어 적용되는가?	중
	D-18	인가되지 않은 Object Owner가 존재하지 않는가?	하
	D-19	grant option이 role에 의해 부여되도록 설정되어 있는가?	중
패치 관리	D-20	데이터베이스의 자원 제한 기능을 TRUE로 설정하고 사용하는가?	하
	D-21	데이터베이스에 대해 최신 보안패치와 벤더 권고사항을 모두 적용	상
	D-22	데이터베이스의 접근, 변경, 삭제 등의 감사기록이 기관의 감사기록 정책에 적합하도록 설정	상
	D-23	보안에 취약하지 않은 버전의 데이터베이스를 사용하고 있는가?	중
로그 관리	D-24	Audit Table은 데이터베이스 관리자 계정에 속해 있도록 설정되어 있는가?	하



## 아. 웹(Web)

코드	취약점명	설 명	등급
BO	버퍼오버플로우	메모리나 버퍼의 블록 크기보다 더 많은 데이터를 넣음으로써 결함을 발생시키는 취약점	상
FS	포맷스트링	스트링을 처리하는 부분에서 메모리 공간에 접근할 수 있는 문제를 이용하는 취약점	상
LI	LDAP인젝션	LDAP(Lightweight Directory Access Protocol) 쿼리를 주입함으로써 개인정보 등의 내용이 유출될 수 있는 문제를 이용하는 취약점	상
OC	운영체제명령실행	웹사이트의 인터페이스를 통해 웹서버를 운영하는 운영체제 명령을 실행하는 취약점	상
SI	SQL인젝션	SQL문으로 해석될 수 있는 입력을 시도하여 데이터베이스에 접근할 수 있는 취약점	상
SS	SSI인젝션	SSI(Server-side Include)는 "Last modified"와 같이 서버가 HTML 문서에 입력값을 변수 값으로, 웹서버상에 있는 파일을 include 시키고, 명령문이 실행되게 하여 데이터에 접근할 수 있는 취약점	상
XI	XPath인젝션	조작된 XPath(XML Path Language) 쿼리를 보냄으로써 비정상적인 데이터를 쿼리해 올 수 있는 취약점	상
DI	디렉토리인덱싱	요청 파일이 존재하지 않을 때 자동적으로 디렉토리 리스트를 출력하는 취약점	상
IL	정보누출	웹 사이트 데이터가 노출되는 것으로 개발과정의 코멘트나 오류 메시지 등에서 중요한 정보가 노출되어 공격자에게 2차 공격을 하기 위한 중요한 정보를 제공할 수 있는 취약점	상
CS	악성콘텐츠	웹애플리케이션에 정상적인 콘텐츠 대신에 악성 콘텐츠를 주입하여 사용자에게 악의적인 영향을 미치는 취약점	상
XS	크로스사이트 크립팅	웹애플리케이션을 사용해서 다른 최종 사용자의 클라이언트에서 임의의 스크립트가 실행되는 취약점	상
BF	약한문자열강도	사용자의 이름이나 패스워드, 신용카드 정보나 암호화 키 등을 자동으로 대입하여 여러 시행착오 후에 맞는 값이 발견되는 취약점	상
IA	불충분한 인증	민감한 데이터에 접근할 수 있는 곳에 취약한 인증 메커니즘으로 구현된 취약점	상
PR	취약한 패스워드 복구	취약한 패스워드 복구 메커니즘(패스워드 찾기 등)에 대해 공격자가 불법적으로 다른 사용자의 패스워드를 획득, 변경, 복구할 수 있는 취약점	상
CF	크로스사이트 리퀘스트변조(CSRF)	CSRF 공격은 로그인한 사용자 브라우저로 하여금 사용자의 세션 쿠키와 기타 인증 정보를 포함하는 위조된 HTTP 요청을 취약한 웹애플리케이션에 전송하는 취약점	상
SE	세션 예측	단순히 숫자가 증가하는 방법 등의 취약한 특정 세션의 식별자(ID)를 예측하여 세션을 가로챌 수 있는 취약점	상
IN	불충분한 인가	민감한 데이터 또는 기능에 대한 접근권한 제한을 두지 않은 취약점	상
SC	불충분한 세션만료	세션의 만료 기간을 정하지 않거나, 만료일자를 너무 길게 설정하여 공격자가 만료되지 않은 세션 활용이 가능하게 되는 취약점	상
SF	세션고정	세션값을 고정하여 명확한 세션 식별자(ID) 값으로 사용자가 로그인하여 정의된 세션 식별자(ID)가 사용 가능하게 되는 취약점	상
AU	자동화공격	웹애플리케이션에 정해진 프로세스에 자동화된 공격을 수행함으로써 자동으로 수많은 프로세스가 진행되는 취약점	상
PV	프로세스감증누락	공격자가 응용의 계획된 플로우 통제를 우회하는 것을 허가하는 취약점	상

FU	파일업로드	파일을 업로드 할 수 있는 기능을 이용하여 시스템 명령어를 실행할 수 있는 웹 프로그램을 업로드 할 수 있는 취약점	상
FD	파일다운로드	파일 다운로드 스크립트를 이용하여 첨부된 주요 파일을 다운로드 할 수 있는 취약점	상
AE	관리자페이지 노출	단순한 관리자 페이지 이름(admin, manager 등)이나 설정, 프로그램 설계상의 오류로 인해 관리자 메뉴에 직접 접근할 수 있는 취약점	상
PT	경로추적	공격자에게 외부에서 디렉터리에 접근할 수 있는 것이 허가되는 문제점으로 웹 루트 디렉터리에서 외부의 파일까지 접근하고 실행할 수 있는 취약점	상
PL	위치공개	예측 가능한 디렉토리나 파일명을 사용하여 해당 위치가 쉽게 노출되어 공격자가 이를 악용하여 대상에 대한 정보와 민감한 정보가 담긴 데이터에 접근이 가능하게 되는 취약점	상
SN	데이터평문전송	서버와 클라이언트간 통신 시 암호화하여 전송을 하지 않아 중요 정보 등이 평문으로 전송되는 취약점	상
CC	쿠키변조	적절히 보호되지 않은 쿠키를 사용하여 쿠키 인젝션 등과 같은 쿠키 값 변조를 통한 다른 사용자의 위장 및 권한 상승 등이 가능한 취약점	상