「서울대학교 캠퍼스전산망 운영지침」 일부 개정(안)

제정 2007. 2. 5
개정 2011. 1.11
개정 2012. 6.11
개정 2013. 7.16
개정 2014. 6. 5
개정 2014.10.16.
개정 2016. 1.25.
개정 2017. 6. 9.
개정 2017.11. 1
개정 2018. 1. 10
개정 2018. 8. 1.

제1조(목적) 본 지침은 서울대학교 캠퍼스전산망을 합리적으로 관리·운영하여 서울대학교 구성원에게 원활한 교육·연구 환경을 제공하는 것을 목적으로 한다.

제2조(지원 범위) ① 서울대학교 캠퍼스전산망(이하 "캠퍼스전산망"이라 한다)은 "서울대학교 학칙"과 "서울대학교 예산·회계"에 적용 받는 관악캠퍼스, 연건캠퍼스, 수원캠퍼스에 위치한 교육조직, 관리조직, 부속시설, 연구소 등으로서 해당 기관장이 제3조에 규정된 캠퍼스전산망 장비실과 해당 장비실을 운영할 수 있는 인력을 확보하고 정보화본부장이 승인한 경우에 한하여 지원한다.

② 제1항을 제외한 지역은 정보화본부장의 승인을 얻어 본 지침을 준수하는 조건으로 캠퍼스전산망에 연결할 수 있다.

제3조(캠퍼스전산망 장비실) ① 캠퍼스전산망 장비보호 및 보안을 위하여 시건 장치가 구비되고 통풍 및 환기되는 독립 공간과 안전한 전원을 제공하여야 한다.

② 장비실 내 설치된 시설물은 요구 기관 임의로 이전할 수 없으며, 설치 장소의 용도 변경이 필요할 경우에는 요구 기관의 자체 예산으로 시설물 이전을 추진하되 정보화본부장으로부터 사전 승인을 받아야 한다.

③ 장비실 면적은 「방송통신설비의 기술기준에 관한 규정」[별표2] 업무

용 건축물의 구내통신실면적확보 기준을 준용한다.

제4조(신·증축 건물의 통신시설 및 장비) ① 건물의 신·증축으로 인해 캠퍼스 전산망 관련 시설 및 장비의 이전 혹은 설치가 필요한 경우, 소요 경비는 해당 건물 신·증축 공사의 예산에 계상하는 것을 원칙으로 한다.

② 모든 신 · 증축 건물의 시설부분에는 다음 각 호의 통신 시설이 포함되어 시공되어야 한다. 건물 설계 시 담당기관은 LAN 시설에 대하여 반드시 정보화본부와 협의하여 설계한다.

1. 광케이블은 Single-Mode 광케이블(SC타입) 8 Core 이상을 기본으로 설치하며 상위 접속지점 등 제반사항에 대하여 정보화본부와 사전 협의한다.
2. 건물 내의 모든 실에 UTP케이블 2회선 이상(2구 Outlet 포함) 설치한다. UTP 케이블은 CAT.6 이상으로 하며, 그 길이는 75m를 초과할 수 없으며, 75m를 초과하는 대형 건물에는 정보화본부와 협의하여 Multi-Mode(SC타입) 광케이블을 포설한다.
3. Rack은 FDF, Patch Panel, 장비 등을 수용 할 수 있는 크기로 한다. Rack의 전원은 단독으로 설치하며 UPS전원 활용을 권장한다.
4. 장비실에는 통풍 및 환기시설을 설치한다.
5. 준공 시 케이블(광, UTP) 도면과 시험성적서, 선번장에 대하여 서류 및 CD 각 1부씩 제출하고 정보화본부와 협의하여 Patch Panel, Outlet, 패치코드에 라벨을 부착한다.
6. 사무실 내 사용자케이블(Outlet↔PC)은 사용자가 구비한다.
7. SNU무선랜은 운영중인 관리서버(컨트롤러, 인증서버)의 수용범위 내에서 연동 가능하므로 반드시 정보화본부와 사전 협의하도록 한다.
8. 무선중계기(AP)는 정보화본부에서 지정하는 장비로 설치한다.
9. 무선중계기 컨트롤러 설치가 필요한 경우는 AP수량에 따라 정보화본부에서 지정하는 장비로 해당 기관에서 구매해야 한다.
10. 향후 원활한 운영을 위해 AP는 벽 또는 천정에 매립하지 말고 밖으로 부착하여 설치한다.

③ 신·증축 건물에 신규 설치된 장비는 정보화본부장의 승인을 얻어 정보화본부로 관리 전환할 수 있으며 다음 각 호에 따라 운영한다.

1. 관리 전환된 장비는 정보화본부의 자산으로 등재되며 정보화본부에서

유지보수를 담당한다.

2. 관리 전환하려는 기관은 대상 장비의 물품명, 수량, 가격 및 무상유지 보수 기간 등의 정보, 기술지원확약서를 정보화본부에 제공해야 한다.

제5조(네트워크 포트 관리) ① 정보화본부에서 각 호실당 1포트를 지원하며, 호실에서 2대 이상 네트워크를 접속하고자 할 경우 자체적으로 장비를 구매하여 사용한다.

② 각 호실에서 13대 이상 네트워크를 접속할 때에는 추가 포트설치에 대해 정보화본부와 협의할 수 있다.

③ 네트워크 포트가 설치된 호실의 구조가 변경될 경우, 해당 호실에서 사용 가능한 네트워크 포트는 기존과 동일하게 유지되어야 하며 포트 배치 비용은 해당 호실 구조 변경 예산에 계상한다.

제6조(무선랜 지원) ① 무선랜 장비를 추가 설치하려면 정보화본부장의 승인 하에 해당 기관에서 장비 및 설치비용을 부담하며 기술지원 및 관리 운영은 정보화본부에서 지원한다. 시설 구축 및 운영은 제4조 제2항의 제7호, 제8호, 제9호, 제10호에 따른다.

② 사용자가 직접 무선중계기(AP)를 사용할 때는 허가받지 않은 사용자가 불법으로 정보통신망을 이용하는 것을 방지할 수 있도록 인증이 가능한 장비만 사용하여야 한다.

③ 무선중계기(AP) 설치 시 주변의 무선중계기(AP)간에 간섭현상이 일어나지 않게 최대한 채널을 조정하여 설치한다. (방송통신위원회 권고사항인 1,5,9,13 채널 중에서 사용한다.)

④ 무선랜 이용 중 보안사고 및 법적분쟁 발생시 이용자에게 그 책임이 있다.

제7조(IP주소 관리) 서울대학교의 IP주소에 대한 관리 및 이용은 다음 각 호의 사항에 따른다.

1. IP주소 할당 대상자는 서울대학교 구성원으로 한다.
2. IP주소는 서울대학교 포털 사이트에서 신청한다.
3. IP주소 할당은 책임자(담당교수 및 부서 책임자)의 승낙이 있어야 한다.
4. 1개의 MAC 주소당 1개의 IP주소를 할당한다.
5. 할당된 IP주소에 대한 책임자 및 사용자, 단말기의 정보 변경에 따른 신규,

변경, 반납, 명의변경, 갱신 등은 서울대학교 포털 사이트에서 신청한다.

6. 할당된 IP주소를 이용하는 모든 시스템 및 시스템 내 운영 서비스는 ‘서울대학교 정보보안 기본지침’에 의거 해당 정보보안 사항을 이행하여야 한다.
7. 할당된 IP주소가 6개월 이상 미사용된 경우, 서울대학교 포털사이트에 게시 및 사용자에게 전자메일로 공지한 후 1개월 이내 사용자의 별도 요청이 없으면 자동 반납한다.
8. 할당된 IP주소에 대한 민원 및 보안사고 등의 법적 문제가 제기될 경우, IP주소 책임자가 책임을 진다.

제8조(도메인명 관리) 서울대학교 도메인에 대한 관리 및 이용은 다음 각 호의 사항을 따른다.

1. 도메인명은 IP주소를 할당받은 사용자가 서울대학교 포털사이트에서 신청한다.
2. 도메인명 할당은 책임자(담당교수 및 부서 책임자)의 승낙이 있어야 한다.
3. 서울대학교 도메인은 서울대학교 IP주소에 한하여 사용할 수 있다. 단, 사용할 IP주소가 서울대학교 IP주소가 아닌 경우에 기관장이 문서로 신청하고 정보화본부장이 허용 여부 및 기간을 결정하여 웹보안정책에 따라야한다.
4. 필요가 인정되는 경우 한 개의 IP주소에 대해 최대 4개까지의 도메인명(호스트) 발급을 허용한다.
5. 할당된 도메인명에 대한 책임자, 사용자, 단말기 정보(메일서버, 네임서버 운영 등) 등 정보 변경 발생시 서울대학교 포털 사이트를 통해 신청할 수 있다.
6. 사용자가 IP주소 반납 또는 갱신하지 않거나 미사용으로 인해 자동 반납된 IP주소와 연계된 도메인명, 메일서버, 네임서버는 IP주소 반납처리시 자동 반납된다.
7. 서울대학교 도메인명을 이용하는 서버는 ‘서울대학교 개인정보보호 지침 ’ 및 ‘서울대학교 정보보안 기본지침’에 의거 해당 정보보호 사항을 이행하여야 한다.

제9조(서비스 포트 관리) 방화벽에서 차단, 허용하는 서비스 포트에 대한 관리 및 이용은 다음과 같다.

① 학외에서 학내로의 주요 서비스포트 접근은 차단하며 학내에서 학외로의 모든 포트 접근은 허용한다. 단 취약한 서비스용, 일부 웜/바이러스 유포용, 데이터베이스(DB) 접속용 등의 서비스포트([별표1])는 정보화본부에서 별도 관리・차단한다.

② 차단포트를 교육・연구・업무 목적 등으로 사용하고자 하는 경우에는 다음 각 호와 같이 신청하여야 한다.

1. IP주소를 할당받은 사용자가 서울대학교 포털사이트에서 신청한다.
2. IP주소 신청시 서비스포트를 함께 신청할 수 있으며 서비스포트만 별도 신청할 수 있다.
3. 서비스포트 허용은 책임자(담당교수 및 부서 책임자)의 승낙이 있어야 한다.

③ 서비스 포트를 신청하면 정보화본부에서 제공하는 취약점 점검 절차, 방법 및 가이드라인 등을 참고하여 다음 각 호와 같이 해당 정보시스템의 취약점 점검을 실시하고 개선 결과를 제출하여야 한다.

1. 계정의 비밀번호 취약성 점검 실시
2. 정보시스템 취약점 점검 실시
3. 홈페이지(HTTP)운영 서비스포트를 신청한 경우는 웹취약점 점검 실시
4. 홈페이지에서 개인정보를 보유하는 경우는 기술적 보안조치(공공I-PIN, SSL, DB암호화 등) 및 개인정보처리방침 게재 등
5. 백신프로그램 및 자동보안패치(PMS, 윈도우만 해당) 설치

※ 윈도우, 리눅스용 V3 백신프로그램은 캠퍼스라이선스로 제공

④ 취약점 점검 및 개선 결과를 제출하면 정보화본부에서 최종 확인 후 서비스 포트 사용을 허용한다.

⑤ 서비스 포트 허용 후 다음 각 호에 해당하는 경우에는 IP신청자가 취약점 점검 및 개선을 하여 정보시스템의 안전성을 확보한 후 운영하여야 한다. 만일 안전성이 미확보된 상태로 운영하는 것이 발견될 경우, 정보화본부에서 긴급 처리를 요청할 수 있으며, 처리 완료될 때까지 서비스 포트를 차단한다.

1. 운영중인 정보시스템에 변경이 발생한 경우
   (예, 정보시스템 재구축 또는 개편, 각종 프로그램 추가 등)
2. 새로운 취약점이 발견되어 빠른 보안 업데이트가 필요한 경우
3. 그 밖에 정보시스템 보안 강화가 필요한 경우

⑥ IP 신청자는 허가받은 서비스 포트를 주기적으로 점검하고 사용하지 않는 서비스 포트는 즉시 반납하여야 한다.

⑦ 서비스 포트의 사용기간은 1년이며 연장신청하지 않은 경우에는 미사용으로 간주하여 자동 반납된다.

⑧ 운영중인 정보시스템은 1년마다 취약점 점검을 하여야 하며, 1년 이상 취약점 점검을 하지 않은 경우에는 서울대학교 포털사이트에 게시 또는 전자 메일로 공지한 후 1개월 이내 사용자의 별도 요청이 없는 한 해당 서비스포트는 자동 반납된다.

⑨ IP주소의 반납처리 시 IP주소와 연계된 서비스 포트는 자동 반납된다.

⑩ 학내망을 보호하기 위해 차단포트 목록은 조정될 수 있으며 조정 결과는 적용 전에 공지한다.

제10조(학외 메일서버 관리) ① 학내 사용자가 전자우편프로그램(Outlook 등)에서 학외 메일서버를 지정하여 메일을 송신하는 것은 원칙적으로 차단하며 신청자에 한하여 허용한다.

② 학내의 정보시스템이 학외로 대량메일을 발송하는 것은 원칙적으로 차단하며 신청자에 한해서 허용한다.

③ 학외 메일서버의 허용 신청은 IP주소를 할당받은 사용자가 서울대학교 포털사이트에서 신청한다.

④ 신청시 학외 메일서버 정보는 IP주소로만 가능하며 IP주소가 변경된 경우에는 기존 신청정보를 반납하고 신규 신청하여야 한다.

⑤ 학외 메일서버의 사용기간은 1년이며 연장신청하지 않은 경우에는 미사용으로 간주하여 자동 반납된다.

⑥ IP주소의 반납처리 시 IP주소와 연계된 학외 메일서버는 자동 반납된다.

제11조(네트워크 관리 및 정보보안) ① 캠퍼스전산망은 학칙에서 정하는 교육 · 연구 · 학술 활동에 우선 이용될 수 있도록 정보화본부에서 지원한다.

② 캠퍼스전산망 사용 주체는 '국가 정보보안 기본지침' 및 '서울대학교 정보보안 기본지침'에 의거하여 네트워크 및 관련 자료를 관리해야 한다.

③ 정보화본부는 효율적이고 안정적인 네트워크 운용을 위해 다음 각 호의 사항을 수행한다.

1. 무단 IP주소 사용자 및 영리목적 사용자는 네트워크 접근을 차단한다.
2. 트래픽 관리, 이상유·무 진단, 장애 예방 및 감지를 위해 네트워크 모니터링을 실시한다.
3. 과다한 트래픽 유발로 회선 이용을 점유하거나 장애 트래픽, 보안사고 관련 트래픽 등으로 예상되는 경우 특정 그룹 및 이용자에 대해 개별 모니터링 할 수 있으며, 다수의 이용에 피해를 줄 수 있다고 판단될 경우 네트워크 사용을 조절 할 수 있다.
4. 게임 및 증권사이트 등 학술·연구에 부적합한 사이트는 공지 후 사용을 차단 또는 조정할 수 있다.
5. 긴급히 조치가 필요하거나 보안사고가 접수된 경우 추가 피해를 막기 위해 해당 장비를 사전통보 없이 네트워크로부터 차단할 수 있으며, 해당 사고 해결 및 관련 추가 문제가 존재하지 않는 경우에만 네트워크 재접속을 허용한다.
6. 정보시스템의 보안 취약점 및 법 위반사항 조치를 고지하였음에도 불구하고, 미이행 시 네트워크를 차단할 수 있으며 해당 문제가 개선된 경우에만 네트워크 재접속을 허용한다.
7. 동일 IP주소에서 지속적인 보안사고가 발생하는 경우에는 해당 기관을 대상으로 정보보안 감사 및 교육을 실시할 수 있다.
8. 정보화본부에서는 학내 정보보안 및 불법소프트웨어 근절 등을 위해 학내 정보시스템의 정보를 수집할 수 있다.
9. 차단 및 정책 변경이 필요한 경우는 공지 후 적용할 수 있다.

제12조(사용료 과금) 정보화본부는 다음 각 호에 해당하는 서울대학교 캠퍼스전산망 자원을 사용하는 기관 또는 개인에게 자원 운영에 소요되는 비용의 전액 또는 일부를 징수할 수 있다.

1. IP 주소
2. Domain
3. 광케이블 및 LAN Port
4. 정보화본부장이 정한 기타 네트워크 자원

부 칙

제1조(시행일) ① 본 지침은 공포한 날부터 시행한다.

② 신설된 제9조(서비스 포트 관리)의 제2항, 제3항, 제4항 및 제10조(학외 메일서버 관리)의 제3항, 제4항, 제5항은 2012년 9월 1일부터 시행한다.

제2조(경과조치) 본 지침 개정 전에 서비스포트가 허용되어 사용 중인 정보시스템은 다음과 같이 조치한다.

① 정보화본부에서 제공한 “보안설정 체크리스트”에 따라 보안설정을 하고 이행결과를 2013년 2월 28일까지 제출해야 한다.

② 기한 내 이행결과를 제출하지 않을 경우에는 허용된 서비스 포트를 차단한다.

제3조(다른 지침 및 규정과의 관계) 이 지침에 명시되지 않은 사항은 다음 각 호를 준용한다.

1. 개인정보보호법 및 시행령
2. 서울대학교 정보보안기본지침
3. 서울대학교 정보화 서비스 관련 지침
4. 그 밖의 관련 법규

[별표1]

차단 서비스포트 목록

서비스 포트	서비스명	차단 방향
TCP 21	FTP(파일전송)	학외→학내
TCP 22	SSH(보안 원격접속)	
TCP 23	Telnet(원격접속)	
TCP 25	SMTP(보내는 메일)	학외↔학내 (양방향 차단)
UDP 53	DNS(도메인 서비스)	학외→학내
TCP 80	HTTP(웹서비스)	학외→학내
TCP 443	HTTPS(웹서비스)	
TCP 8080	HTTP(웹서비스)	
TCP 110	POP3(받는 메일)	
TCP 143	IMAP(받는 메일)	
TCP 1433	MS_SQL(DB접속)	학외↔학내 (양방향 차단)
TCP 1434	MS_SQL(DB접속)	
TCP 1521	Oracle(DB접속)	
TCP 3050	FireBird(DB접속)	
TCP 3306	MySQL(DB접속)	
TCP 3389	MSTSC(윈도우 원격접속)	학외→학내
TCP 5432	PostgreSQL(DB접속)	학외↔학내 (양방향 차단)
TCP 5800	VNC(윈도우 원격접속)	학외→학내
TCP 5900		
TCP 6288	V3관리(리눅스용)	학외→학내
기타	웜·바이러스 유포 의심 서비스 포트 (280여 개)	학외↔학내 (양방향 차단)

[별표2] 업무용 건축물의 구내통신실면적확보 기준(방송통신설비의 기술기준에 관한 규정)

업무용 건축물의 구내통신실면적확보 기준(제19조제1호 및 제3호 관련)

건축물 규모	확보대상	확 보 면 적
1. 6층 이상이고 연면적 5천제곱미터 이상인 업무용 건축물	가. 집중구내통신실	10.2제곱미터 이상으로 1개소 이상
	나. 층구내통신실	1) 각 층별 전용면적이 1천제곱미터 이상인 경우에는 각 층별로 10.2제곱미터 이상으로 1개소 이상 2) 각 층별 전용면적이 800제곱미터 이상인 경우에는 각 층별로 8.4제곱미터 이상으로 1개소 이상 3) 각 층별 전용면적이 500제곱미터 이상인 경우에는 각 층별로 6.6제곱미터 이상으로 1개소 이상 4) 각 층별 전용면적이 500제곱미터 미만인 경우에는 각 층별로 5.4제곱미터 이상으로 1개소 이상
2. 제1호 외의 업무용 건축물	집중구내통신실	건축물의 연면적이 500제곱미터 이상인 경우 10.2제곱미터 이상으로 1개소 이상. 다만, 500제곱미터 미만인 경우는 5.4제곱미터 이상으로 1개소 이상.

비고

1. 같은 층에 집중구내통신실과 층구내통신실을 확보하여야 하는 경우에는 집중구내통신실만을 확보할 수 있다.
2. 층별 전용면적이 500제곱미터 미만인 경우로서 각 층별로 통신실을 확보하기가 곤란한 경우에는 하나의 층구내 통신실에 2개층 이상의 통신설비를 통합하여 수용할 수 있다. 이 경우 층구내통신실 확보면적은 통합 수용된 각 층의 전용면적을 합하여 위 표 제1호 중 층구내통신실의 확보면적란의 기준을 적용한다.
3. 같은 층에 층구내통신실을 2개소 이상으로 분리 설치하려는 경우에는 층구내통신실의 면적은 최소 5.4제곱미터 이상이어야 한다.
4. 집중구내통신실은 외부환경에 영향이 적은 지상에 확보되어야 한다. 다만, 부득이한 사유로 지상확보가 곤란한 경우에는 침수우려가 없고 습기가 차지 아니하는 지하층에 설치할 수 있다.
5. 집중구내통신실에는 조명시설과 통신장비전용의 전원설비를 갖추어야 한다.
6. 각 통신실의 면적은 벽이나 기둥 등을 제외한 면적으로 한다.
7. 집중구내통신실의 출입구에는 잠금장치를 설치하여야 한다.