과 업 지 시 서

사업명	서정대학교 임대솔루션 시스템 관리 운영 사업

2021년 11월 12일

서정대학교
SEOJEONG UNIVERSITY

1 사업개요

가. 사업명 : 서정대학교 임대솔루션 시스템 관리 운영 및 업그레이드 사업
나. 사업기간 : 계약일로부터 5년간
다. 입찰방식 : 견적 입찰
라. 사업자 선정방식 : 제한경쟁에 의한 최저가 입찰
마. 문의처
- 입찰관련 문의 : 서정대학교 사무처, 031-860-5017
- 사업관련 문의 : 서정대학교 정보전산센터, 031-860-5024

2 사업추진 배경

가. 기존 전산 장비의 노후화로 인한 장애 발생 위험성 증가 및 성능 저하로 전산 장비 운영의 안정성, 연속성 및 신뢰성 확보 필요
나. 코로나19의 확산 및 위드코로나 시대를 대비한 비대면 온라인 교육 환경 마련을 위한 시스템 구축 필요
다. 급변하는 IT 환경 변화에 맞추어 최선 소프트웨어 버전이 적용된 대학 시스템의 성능 개선 및 확장성과 개방성을 가진 시스템 구현

3 기대 효과

가. 노후 전산 장비의 개선을 통한 안정적 운영 및 신뢰성 확보
나. 안정적인 시스템 운영을 통한 업무 연속성 보장
다. 사용자 및 운영환경 변화에 유연하게 대응할 수 있는 시스템 운영
라. 무선 음영지역 환경 개선을 통한 모바일 업무 환경 및 이용 편이성 증대
마. 대학 시스템 성능 개선 및 확장성과 개방성을 가진 시스템 확보

4 운영 및 업그레이드 내역

가. 접근통제 솔루션
나. 통합로그 솔루션
다. 스팸차단 솔루션
라. 웹 메일 솔루션
마. 차세대방화벽
바. 무선 AP 증설
사. 무선 관리시스템
아. 무선 PoE SW
자. 무선인증 솔루션
차. 무선 운영용 10G 집전스위치
카. 무선 AP 설치 및 케이블 포설

타. 기타사항
파. 국제관 무선AP 설치 위치
※ 세부사항은 규격서 항목 참조

5 운영 및 설치 장소

가. 대학교 기계실 및 각 건물 지정 장소
나. 음영지역에 대한 무선 AP 증설 및 신관 지정 위치 설치

6 입찰참가조건

가. 『국가를 당사자로 하는 계약에 관한 법률 시행령』 제12조에 따른 경쟁입찰참가 자격을 가진 업체
나. 동법 시행령 제76조(부정당업자의 입찰참가자격 제한) 규정에 따라 입찰 참가자격을 제한받지 아니한 업체
다. 입찰공고일 현재 청산, 합병, 매각 등 정리절차 중이거나 계획 중인 사업자, 법원에 화의 또는 법정관리를 신청 중인 사업자는 입찰에 참가할 수 없음.
라. 『정보통신공사업법 제14조』에 의한 정보통신공사업 등록 업체
마. 본 대학의 전반적인 네트워크 환경인 유, 무선망을 분리 관리하며, 제반 기술을 지원할 수 있는 업체
바. 원활한 납품 및 구축과 향후 유지관리를 위한 주 사업장이 서울·경기도인 업체로 기업신용등급이 BB- 이상인 업체
사. 자본금 2억 이상인 업체
아. 제조사정품공급 및 기술지원확약서

7 제출서류

가. 입찰참가 신청서(본교 양식) 1부
나. 사업자등록증 사본(원본 대조필 날인) 1부
다. 이행(입찰)보증보험증권 1부
라. 법인인감증명서 및 사용인감계 각 1부
마. 대리인 참가 시 재직증명서 및 위임장 각 1부
바. 법인등기부등본 1부
사. 국세 완납증명서 1부
아. 지방세 완납증명서 1부
자. 청렴계약이행서약서(본교 양식) 1부
차. 정보통신공사업자 등록증 1부
카. 제조사 정품공급 및 기술지원확약서 각 1부
타. 기업 신용등급확인서 1부

8 제품 공급 및 구축

가. 공급자는 본 사업의 수행을 위하여 현장 조사 및 설치, 구성 등 제반사항을 성실히 수행하며, 서정대학교에서 제시한 규격 조건에 적합한 제품을 공급 및 운영하여야 한다.

나. 본 사업에 공급되는 하드웨어 및 부품은 제조사가 인정하는 정품 및 신제품이어야 하고, 최신 기술이 제시되어야 한다.

다. 공급자는 제반 하드웨어 및 소프트웨어 설계 및 공급, 설치, 시험운영, 성능보증 등을 일괄 책임져야 한다.

라. 공급자는 제품 공급 및 설치, 구축, 시험 운영 등 작업 시 현 학사 업무에 지장이 없도록 하여야 한다.

마. 공급자는 본 사업 수행 시 서정대학교에서 제시하는 방법으로 운영될 수 있도록 설치 및 운영하여야 한다.

바. 과업지시서에서 요구하는 공급 제품의 성능 및 구축 사항에 대하여 공급자는 본 사업에 응찰 시 입찰에 필요한 모든 사항에 대해 완전히 숙지하고 입찰에 응해야 하며, 계약 후 과업지시서 내용에 대한 이의 제기를 할 수 없다.

사. 공급자는 본 사업과 관련하여 과업지시서에 언급하지 않은 서비스 및 운용상의 도움이 되는 기능이 있을 경우 이를 제시하여야 한다.

9 교육 훈련

가. 서정대학교 담당자가 공급자의 지원 없이도 시스템을 관리하고 모든 시스템의 운영 및 응급조치가 가능하도록 충분한 교육과 지식을 제공하여야 한다.

나. 운영 장비에 대한 교육 책임과 제반 비용은 공급자가 부담한다.

다. 교육 시 공급된 제품에 대한 개요, 기능, 운영방법 이해, 유지보수에 필요한 사항, 소프트웨어와 하드웨어 구성 방법 및 사용자 관리 부분 등의 내용도 포함되어야 한다.

10 유지보수

가. 유지보수 대상은 공급자가 공급한 하드웨어, 소프트웨어 일체로 한다.

나. 하자보수

(1) 공급 제품에 대한 제조사 하자보증기간은 구축 완료 후 5년간 으로 제출 한다.

(2) 장애 복구는 도착 후 4시간 이내에 착수하여 신속히 복구하며, 8시간 이내에 장애 원인과 복구 예정시간 및 조치방법 등을 제시하여야 한다. 단, 8시간 이내에 복구가 곤란한 경우에는 동급 이상의 장비(부품)로 신속히 대체하여야 한다.

(3) 정규 방문 유지보수는 매월 1회, 임대기간 종료 시 까지 방문 점검으로 한다.

- 안정적인 전산자원의 정보 서비스 제공
- 24시간 x 365일 최적 가동 상태 유지를 위한 기술 지원

- 장애 발생 시 대처 부품 수급(선 조치 후 복구 수행의 최소 제반사항 지원)
- 정기, 분기, 반기 및 수시 점검 실시에 따른 보고 및 개선방안 제출

다. 전산자원 간 복합적인 장애 발생 시 통합 운영사가 주관하여 원인파악 조치

라. 전산자원의 운영을 위한 최신 기술 제공 및 교육 지원

마. 유지보수 수행과 관련된 결과물에 대한 기록 관리

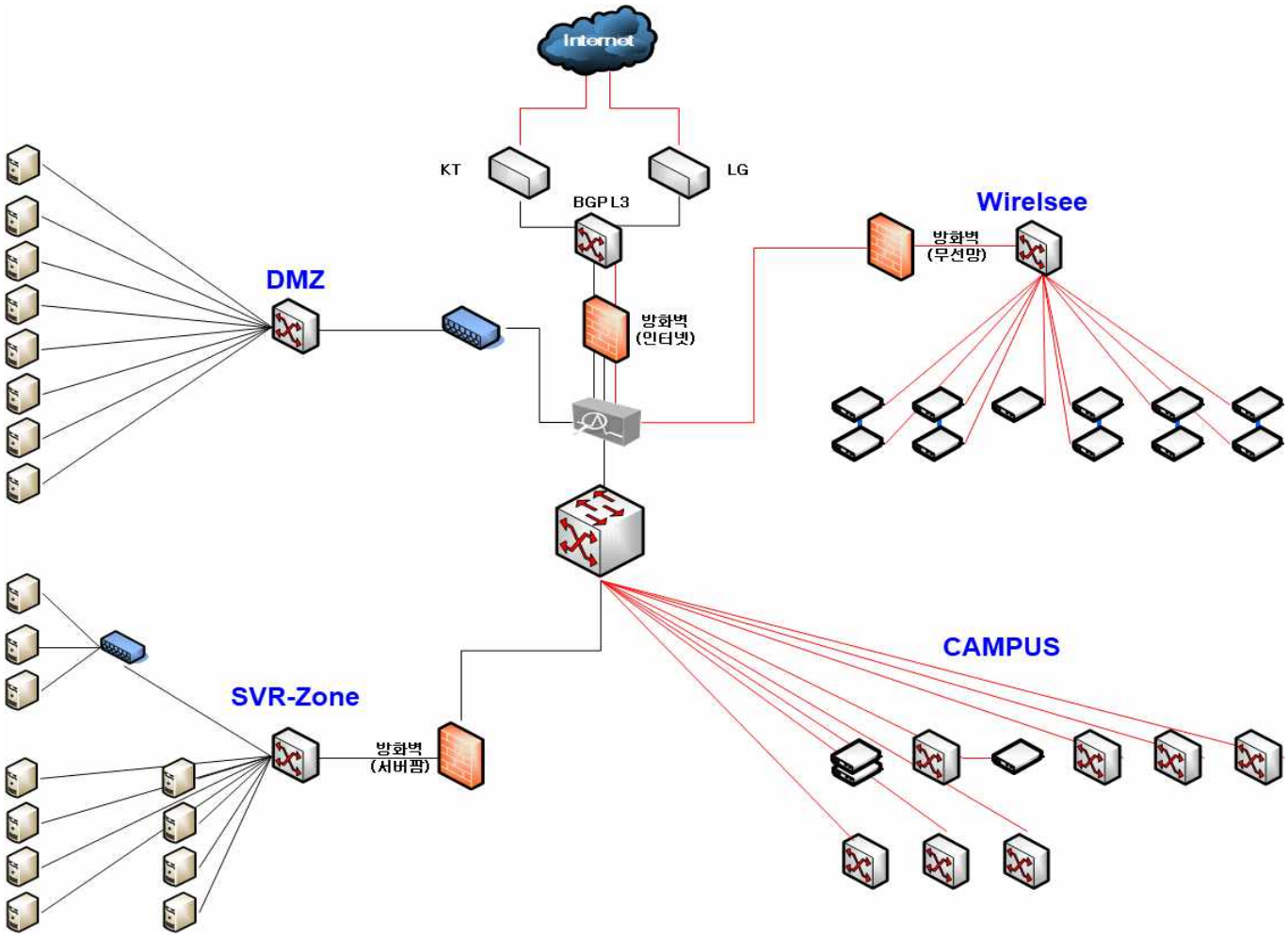
바. 사업 완료 후 전산자원 안정화를 위하여 제조사가 인정하는 엔지니어를 통하여 기술전수, 시스템 운영의 안정화 및 개선을 위하여 지속적으로 지원하여야 한다.

사. 공급자는 하자보증기간 내에 공급한 제품에 대해 최초 발생 기준 30일 이내 2회 이상 장애가 발생하였을 경우 공급한 제품의 동등 사양 이상의 제품으로 대체 지원하여야 한다.

아. 공급자는 공급된 제품에 대한 유지관리 시 서정대학교에서 요구하는 보안 관련 법규를 준수하여 보안 유지에 최선을 다하여야 한다.

자. 정해진 하자보수 기간 이후의 유상 유지보수를 서정대학교가 요구할 시 공급자는 이에 응해야 하며, 기 운영 중인 대상 품목들에 대한 유지보수 요청 시 협의 및 지원할 수 있어야 한다.

11 네트워크 구성도



12 운영 품목 세부 내용 및 규격

가. 접근통제

항목	세부 규격	수량
접근통제	[일반사항] • 기 도입 운영 중인 시스템접근제어의 정책 및 로그 데이터가 상호 호환되며 이관이 가능하여야 한다. • 교육부 정보보호 수준진단 접근 통제 관련항목에 충족하여야 한다. • EAL2 이상의 CC인증을 보유하여야 한다. • GS인증 1등급을 보유하여야 한다. • 라이선스 수량 : 150EA • 가상화 서버에 탑재하여 구동이 될 수 있도록 지원하여야 한다. (가상화 서버 탑재 적용 무상지원 포함) [접근제어] • Telnet, Ftp, SSH, SFTP, RDP, VNC 서비스에 대한 감사기능 제공하여야 한다. • CLI(Command Line Interface) 모드의 작업 환경 제공하여야 한다. • 사용자 PC와 대상 장비에 agent를 설치하지 않는 구조이어야 한다. • Mac용 client 환경을 지원해야 한다. • 로그는 암호화하여 저장되어야 한다. • 모든 로그는 중앙관리 서버에서 기록하고 보관되어야 한다. • 금지명령어 Black List / White List 기능 제공하여야 한다. • WEB 기반의 관리자 인터페이스에서 관리자가 작업한 모든 이력을 보관 관리해야 한다. • 관리자에게 모든 세션별 접근시간, 시스템명, 사용자 IP, 서비스, 사용자 아이디, 사용자 이름을 실시간 제공하여야 한다. • 패스워드 일정 횟수 오류 발생 시 계정 사용 중지해야 한다. • 패스워드는 영문자 / 숫자 / 특수문자 등의 조합과 변경주기를 사용자에게 강제 할 수 있어야 한다. • 특정 네트워크 대역이나 IP에서만 사용자 로그인, 접속을 허용해야 한다. • 사용자의 명령어뿐만 아니라 결과 값까지 로그 저장해야 한다. • 모바일 OTP 앱을 통한 2차 인증 체계 제공하여야 한다. • 작업로그의 Alias 명령어 검출기능 제공하여야 한다. • 유휴세션 화면 잠금기능 제공하여야 한다. • 동영상 로그의 효율적 관리를 위한 압축 보관해야 한다.	1식

항목	세부 규격	수량
접근통제	[계정관리] • 공유 계정의 관리체계를 제공하여야 한다. • 시스템 계정의 생성, 수정, 삭제 기능을 제공하여야 한다. • 주기적으로 시스템 계정을 수집 및 동기화 기능을 제공하여야 한다. • 계정의 수집 및 추가 / 수정 / 삭제 기능을 제공하여야 한다. • 전체 계정에 대한 계정 현황 보고서 기능(사용자 별, 호스트 별)을 제공하여야 한다. • 시스템 계정에 대한 신청 및 승인 프로세스를 제공하여야 한다. • 시스템 계정 소유자 설정 및 권한 설정 관리 기능을 제공하여야 한다. • 시스템 계정 속성(개인 / 공유 / 시스템 / APP) 관리 기능 제공하여야 한다. • 공유 계정 현황 리스트 제공(Excel)하여야 한다.	1식

나. 통합로그

항목	세부 규격	수량
통합로그	[일반사항] • 기 도입 운영 중인 통합로그 솔루션의 정책 및 로그 데이터가 상호 호환되며 이관이 가능하여야 한다. • 가상화 서버에 탑재하여 구동이 될 수 있도록 지원하여야 한다. (가상화 서버 탑재 적용 무상지원 포함) • 방화벽, 시스템접근제어, 웹 방화벽과 연동 처리하여야 하며, 대학 요구시 추가적으로 연동 지원하여야 한다. • 대시보드 1종을 지원하여야 한다. • 인증 - 로그 수집 성능을 검증할 수 있는 공인기관(TTA)의 시험성적서를 보유하고 TTA 결과 120만 EPS이상 수집하여야 한다. - EAL2 이상의 CC인증을 보유하여야 한다. - GS인증 1등급을 보유하여야 한다. • 기능 - 1일 20GB 발생 로그 기준 1년간 보관하여야 한다. - EOS(End of Service)관련 S/W(Explorer, Flash Player 등) 사용불가 - Agent, 통합로그 간 데이터 전송시 암호화 알고리즘 적용 필요 • 수집 - 보유 자원 활용의 극대화를 위하여 수집 서버 다중 구성 시 별도의 L4 스위치 없이 수집할 수 있어야 한다.	1식

항목	세부 규격	수량
통합로그	- 수집 서버들의 성능을 체크하여 확인된 서버의 성능에 따라 자동으로 로그를 분산 수집할 수 있어야 한다. - 서버별 수집 할당량을 설정하여 이에 따라 수집할 수 있어야 한다. - Agent, Agentless, DB to DB, Syslog등 다양한 수집 기능을 제공하여야 한다. - 중요 장비의 파일 시스템 감시 및 리소스 정보 수집 기능을 제공하여야 한다. • 저장 - 클러스터링 지원을 통해 다수의 서버를 단일 시스템으로 사용하여 데이터 분산 저장 후 데이터 분산 처리 기능 제공하여야 한다. - 서버 확장 시 단순 추가만으로 분산 클러스터링 환경 구성이 가능하여야 한다. - 시스템의 안정성 및 가용성 극대화를 위하여 서버간 데이터 자동 복제 (Fault Tolerance) 기능을 제공하여야 한다. • 검색 - 사용자가 자주 이용하는 검색 조건, 즐겨찾기를 UI에서 메뉴(버튼)로 제공하여야 한다. - 데이터가 많고 산만할 시 깔끔하게 정리하는 기능을 제공하여야 한다. - 단일 플랫폼에서 SQL 및 No-SQL 동시 지원하며, RDBMS에서 사용하는 표준 SQL 질의 문법을 이용하여 데이터 생성, 변경, 삭제, 조회가 가능하여야 한다. • 저장 - 클러스터링 지원을 통해 다수의 서버를 단일 시스템으로 사용하여 데이터 분산 저장 후 데이터 분산 처리 기능 제공하여야 한다. - 서버 확장 시 단순 추가만으로 분산 클러스터링 환경 구성이 가능하여야 한다. - 시스템의 안정성 및 가용성 극대화를 위하여 서버간 데이터 자동 복제 (Fault Tolerance) 기능을 제공하여야 한다. • 검색 - 사용자가 자주 이용하는 검색 조건, 즐겨찾기를 UI에서 메뉴(버튼)로 제공하여야 한다. - 데이터가 많고 산만할 시 깔끔하게 정리하는 기능을 제공하여야 한다. - 단일 플랫폼에서 SQL 및 No-SQL 동시 지원하며, RDBMS에서 사용하는 표준 SQL 질의 문법을 이용하여 데이터 생성, 변경, 삭제, 조회가 가능하여야 함. 실시간 스트리밍 데이터에 대하여 시간 윈도우를 사용하여 패턴 매칭, 데이터 연산처리, 시나리오 기반 복합 이벤트 분석을 서버간 분산 처리할 수 있는 기능을 제공하여야 한다.	1식

항목	세부 규격	수량
통합로그	- Code 및 SQL을 사용하여 엔지니어 및 담당자가 원하는 데이터를 손쉽게 검색할 수 있는 프로시져 정의 후 동작을 할 수 있는 기능을 제공하여야 한다. - 원하는 데이터를 클릭만으로 검색 가능(AND 조건)하며, 검색 결과들에 대한 추가적인 조합 검색이 가능하여야 한다. • 분석 및 모니터링 - 추가 개발 또는 3rd Party 솔루션 도입 없이 현장에서 담당자가 원하는 형식의 MS Office Word, Power Point 문서 파일을 생성하여 시스템에 - Up-load 후 즉시 보고서로 활용 가능하여야 한다. - 이상행위자가 탐지된 시나리오 탐지 내역들을 하나의 화면에서 시간의 흐름대로 보여줌으로써 이상해위자의 행동패턴을 분석하고 미래 상황에 대처할 수 있는 기능 제공하여야 한다. - 권한 통제를 위한 사용자별 메뉴 구성 기능을 제공하여야 한다. - 로그 수집현황(건수, 사이즈, EPS등)을 실시간 모니터링 가능한 종합상황판 기능을 제공하여야 한다. - 이벤트 발생 시 SMS / SMTP 서버 연동을 통한 다양한 알람 기능을 제공하여야 한다. - 사용자 정의 위젯형 대시보드 기능을 제공하여야 한다. • 감사 - 저장된 로그의 무결성 여부 체크 및 위•변조 탐지 시 관리자 알림 기능을 제공하여야 한다.	1식

다. 스팸차단 솔루션

항목	세부 규격	수량
스팸차단	[일반사항] • 라이선스 : 400 유저 • 기 운영 중인 스팸차단 솔루션에 대한 정책 및 환경이 호환, 이관되어야 한다. • 자체개발엔진을 사용한 자체개발 솔루션이어야 한다. • 멀티 OS(Windows, Linux)를 지원하여야 한다. • 멀티 백신(Cyren, Sophos)을 지원하여야 한다. • 다양한 SSP 연동을 통한 메일서버와의 스팸편지함 / 스팸설정 기능 연동이 가능하여야 한다. • 보안 GS인증을 획득한 제품(CC인증 대체 가능)이어야 한다. [메일 아카이브]	1식

항목	세부 규격	수량
스팸차단	• 메일 본문만 아니라 첨부파일 이름 및 첨부파일 내용에 대한 검색이 지원 가능하여야 한다. • 첨부파일 내용 검색 지원(Doc, txt, pdf, xls, ppt 등) • 메일 저장 시 압축저장 기능을 지원하여야 한다. [보안기능] • 랜섬웨어 차단 기능을 제공(시그니처 방식)하여야 한다. • APT 공격 차단 기능을 제공(시그니처 방식)하여야 한다. • 좀비 PC 차단 기능을 제공하여야 한다. • SSO 보안을 위하여 DES / 3DES / 허용IP 등 다양한 보안기능을 제공하여야 한다. • 접근제한 기능으로 인가되지 않은 사용자는 접근제한이 가능하여야 한다. • 자체 서버보안 기능을 통한 접근제한 및 해킹방지 기능을 제공하여야 한다. • 세션 타임아웃 기능을 제공하여야 한다. • SSL / TLS 통신을 지원하여야 한다. • 587port를 지원하여야 한다. • DDoS Attack 방어 기능을 제공하여야 한다. • RBL을 이용한 차단 및 메일내역확인을 제공하여야 한다. • SMTP AUTH 인증 후 송신자 불법 변조 메일 차단기능 제공하여야 한다. • 업데이트 설정 방법 및 예약업데이트 지정하여야 한다. (신규 스팸 메일 패턴 분석 후 패턴 업데이트를 통해 즉각 대응하여야 한다.) • RBL 소스 지원 등록 개수의 제한이 없어야 한다. • 해외 스팸메일에 대한 다국어 필터링 기능을 제공하여야 한다. • IPv6를 통한 스팸메일의 스팸차단이 가능하여야 한다. • DKIM 기능을 제공하여야 한다. • Inbound / Outbound 메일 필터링 기능을 제공하여야 한다. • 전체 / 도메인별 / 그룹별 필터와 정보 변경이 가능하여야 한다. • 이미지로 수신되는 스팸메일 차단이 가능하여야 한다. • 보내는 메일서버 인증을 통한 Relay 금지 기능을 제공하여야 한다. • 지정된 도메인만 SPF 검사 기능이 가능하여야 한다. • 스팸메일과 정상메일의 데이터 통계를 기반으로 한 스팸차단 방식을 분석하여 차단하여야 한다. • Relay 허용IP / 도메인 / 이메일 / SMTP 인증 사용자 등 필터에서 예외설정이 가능하여야 한다.	1식

항목	세부 규격	수량
스팸차단	• 메일 본문에 포함된 유해사이트, URL에 대한 스팸메일 여부 검사가 가능하여야 한다. • 한번 연결을 통해 발송하는 메일 수(수신자 수)를 제한하거나 별도의 예외설정 / 처리방법(허용, 차단, Tag, Test) / 해제시간 / 응답코드 기능을 설정 가능하여야 한다. [관리자기능] • 메일 내 개인정보 마스킹 처리가 가능하여야 한다. • 국가별 IP 허용 / 차단이 가능하여야 한다. • 송, 수신 상태별 검색이 가능하여야 한다. • SMTP 인증에 따른 사용자 계정 관리가 가능하여야 한다. • 관리자 페이지에서 Proxy / Bridge 모드 선택이 가능하여야 한다. • 바이러스 의심 메일이 수신되었을 경우 관리자를 통해 바이러스 의심 메일에 대한 제어가 가능하여야 한다. • 업데이트 설정 방법 및 예약 업데이트 지정이 가능하여야 한다. • 접속 단계에서부터 정상 / 스팸 / 바이러스 메일의 사본 저장이 가능하여야 한다. • 모든 필터에 대해 예외 설정이 가능하여야 한다. • 사본저장 기능의 대상 선택 및 송 / 수신 대상 설정이 가능하여야 한다. • 사본저장 기능을 통한 첨부파일 이름 / 확장자 검색이 가능하여야 한다. • 바이러스 발송자에 경고 메시지 발송이 가능하여야 한다. • 단일 커넥션에 대한 최대 수신자 수 제한이 가능하여야 한다. • 메일 전송 시 메일 전체 / 본문 / 첨부파일 크기 제한기능을 지원하여야 한다. • 정책, 설정 등 각종 환경설정 파일에 대한 백업과 복구 기능을 지원하여야 한다.	1식

라. 웹 메일 솔루션

항목	세부 규격	수량
웹 메일	[일반사항] • 라이선스 : 400 유저 • 업그레이드를 통한 기존메일(데이터 포함) 이관작업을 제공하여야 한다. • 대학에서 운영 중인 SSO 솔루션 연계 및 그룹웨어(전자결재) 연동을 반영하여야 한다. • 기능개선 요구사항에 대해 협의하여 진행하며, 최대한 반영하여야 한다. • 멀티 OS(Windows, Linux)를 지원하여야 한다.	각 1식

항목	세부 규격	수량
웹 메일	• 멀티 백신(Cyren, Sophos)을 지원하여야 한다. • 멀티 브라우져(익스플로어, 크롬, 사파리, 파이어폭스)를 지원하여야 한다. • 스팸메일 차단시스템을 통한 메일 수·발신을 지원하여야 한다. • 각 페이지는 3초 이내에 로딩이 완료되어야 하고, 부득이 3초 이상 소요되는 부분은 진행 상태를 알 수 있도록 표시하여야 한다. • TLS 인증서를 통한 웹 암호화 통신(Https)을 지원(TLS 1.2 이상)하여야 한다. • 조직도 연동을 통한 주소록 제공하여야 한다. • ‘전자정부 웹사이트 품질관리 지침’(행정안전부 고시 제2020-38호) [별표]의 전자정부 웹사이트 품질진단 기준을 준수하여야 한다. • 시큐어코딩 가이드를 준수하여야 한다. • 모바일 디바이스 환경에 제약받지 않는 최적화된 UI 구성하여야 한다. • 별도 설치형 프로그램(Activex 등) 없이 HTML5 호환 브라우저만으로 서비스 이용을 지원하여야 한다. - IE11, Microsoft Edge, Chrome, Safari, Firefox 최신 버전 필수 - 모바일기기 내 최신 Android 및 IOS 기본 브라우저 • 모바일 디바이스 환경에 제약받지 않는 최적화된 UI 구성을 제공하여야 한다. • 다국어지원 - 사용자 설정에 맞추어서 한국어, 영어, 일본어, 중국어로 서비스 제공하여야 한다. - 사용자 설정이 없는 경우 브라우저 언어를 참고로 기본 언어를 선택할 수 있어야 한다. - 사용자가 원하는 언어설정을 바꿀 수 있는 화면을 제공하여야 한다. [사용자인증] • SMTP 인증(SMTP Auth) - SMTP를 통한 메일 접속 시에도 계정과 비밀번호를 통해 인증 [메일기능] • 송, 수신 메일에 댓글(소셜)기능을 탑재를 지원하여야 한다. • 퀵 메뉴를 지원하여야 한다. • 묶어보기 기능을 지원하여야 한다. • 필터 기능을 지원하여야 한다. • 업무 진행상태 표시기능을 지원하여야 한다. • 회신해야 하는 메일 및 회시기간이 지난 메일 설정을 지원하여야 한다.	각 1식

항목	세부 규격	수량
웹 메일	• 새 메일, 메일용량 표시 등 메일함 정보 표시를 지원하여야 한다. • 메일 전달 시 인용, 첨부 중 선택 가능하여야 한다. • 분산저장 방식으로 설계하여 NFS 환경에서 자료 유실 현상을 방지하여야 한다. • 첨부파일 기능을 드래그 앤 드롭 첨부방식으로 제공하여야 한다. • 첨부파일만 삭제 가능하여야 한다. • 수신 구분 기능(수신, 참조, 숨은 참조)을 제공하여야 한다. • 편의기능(미리보기, 임시저장, 중요표시, 수신거부, 편지함 자동분류, 머리말, 맺음말, 휴지통 등)을 제공하여야 한다. • 다국어 인코딩(UTF-8)을 지원하여야 한다. • 메일 홈 편집기능을 드래그 앤 드롭 방식으로 지원하여야 한다. • 주소록 내보내기 / 가져오기 기능을 지원하여야 한다. • 수신처 그룹 설정 및 발송 기능을 지원하여야 한다. • 수신자 개별표시(대량메일 발송 시)를 지원하여야 한다. • 읽지 않은 메일만 필터링하여 표시 가능하여야 한다. • 읽지 않은 메일 삭제, 전체메일 삭제 기능을 지원하여야 한다. • 제목, 받은 사람, 받은 날짜로 표시하여 오름차순, 내림차순으로 정렬 기능을 지원하여야 한다. [파일관리 기능] • 상세검색(보낸 사람, 받는 사람, 검색기간, 제목 등)을 지원하여야 한다. • 이미지 첨부 파일 본문 내용에서 확인이 가능하여야 한다. • 첨부 파일만 삭제 가능하여야 한다. [관리자 기능] • 각 사용자에 대한 권한 설정(사용중지, 휴면계정)이 가능하여야 한다. • 사용자 메일용량 관리가 가능하여야 한다. • 사용자 개별등록 및 일괄등록 기능을 지원하여야 한다. • 관리자 접근제한 설정(허용IP 등록)을 지원하여야 한다. [메일기능] • 서버 부하 및 디스크 사용현황을 제공하여야 한다. • 메일 송, 수신 현황 조회 기능(일별, 주별, 월별, 년별)을 지원하여야 한다. • 로그인 로그저장 및 열람기능(사용자별 시간, 접속IP)을 지원하여야 한다. • 사용자 기본용량 제어 및 첨부파일 업로드 용량 제한 기능을 지원하여야 한다.	각 1식

마. 차세대방화벽

항목	세부 규격	수량
차세대 방화벽	[일반사항] • 기 운영중비의 운영 및 이중화 작업 시 기술지원을 하여야 한다. • 대학에서 기 운영 중인 방화벽에 대한 정책 적용, 요구하는 Zone 구성에 대하여 지원, 제안 및 반영하여야 한다. • 방화벽 및 어플리케이션 제어 - 어플리케이션의 카테고리, 특성, 리스크 등 세부 기능별 제어가 가능하여야 한다. - IP, Port등의 설정과 상관없이 모든 정책에 사용자와 어플리케이션 기반 정책 설정 및 운영이 가능하여야 한다. - Port 우회 트래픽에 대한 제어가 가능하며, 특정 Port에 종속되지 않아야 한다. - 정책 설정 시 IP, Port, 사용자, 어플리케이션 등 네 가지를 AND 조건으로 조합하여 설정 및 적용이 가능하여야 한다. - 정책별로 지정된 어플리케이션을 통해 주고받는 파일을 Type별로 업로드 / 다운로드 통제가 가능하여야 한다. - 사용자, 어플리케이션 정책별로 다른 보안(IPS, AV, URL필터, 파일 차단 등) 정책 설정이 가능하여야 한다. - 우회접속(프락시) 프로그램 탐지 및 차단이 가능하여야 한다. - SSL Decryption, SSH Decryption을 지원하여야 한다. - 특정 사용자 / 사용자 그룹의 어플리케이션별 QoS 정책 설정이 가능하여야 한다. - 시간대별, 날짜별 설정으로 스케쥴 정책 설정이 가능하여야 한다. - 정기적인 어플리케이션 Signature 업데이트를 지원하여야 한다. - Unknown 어플리케이션(어플리케이션 리스트에 존재하지 않는 어플리케이션)에 대해 허용 또는 차단 설정이 가능하여야 한다. - Custom 어플리케이션 시그니쳐 설정이 가능하여야 한다. - 새롭게 업데이트 된 어플리케이션만 Filter하여 적용을 유예시킬 수 있어야 한다. - SSL복호화 기능이 지원되어 어플리케이션 식별 및 차단이 가능하여야 한다. - 방화벽의 설정 변경 없이 외부 웹서버에서 다이나믹하게 업데이트 되는 IP, URL, Domain 정보를 정책에 적용할 수 있어야 한다. - 서비스가 아닌 어플리케이션별 Session timeout값을 변경하여 적용할 수 있어야 한다. - 사전 정의된 국가별 IP로 정책 적용이 가능하여야 한다. - Custom URL을 생성하고 정책 설정이 가능하여야 한다.	1식

항목	세부 규격	수량
차세대 방화벽	- 어플리케이션이 과다 허용된 정책에서 사용하지 않는 어플리케이션 식별이 가능하여야 한다. - 어플리케이션을 지정하지 않은 정책에서 어플리케이션 기반 정책으로 변환 가능하게 하는 분석기능이 있어야 한다. (레거시 정책을 어플리케이션 정책으로 변환) - 정책 생성 시 고유 식별 번호가 부여되어야 한다. - 개별 정책별 감사 증적(comments history, config 변경 log, rule 변경 history)을 확인할 수 있어야 한다. - Address 객체에 와일드카드 주소를 지원하여야 한다. - SSL decryption에서 HTTP/2를 지원하여야 한다. - GUI에서 보안 정책에 대한 매칭 Test 기능을 제공하여야 한다. - 정책 생성 시 관리자가 Tag, 정책 설명, 감사증적(생성, 수정 사유 작성 등)을 작성하는 기능을 지원하여야 한다. - SSL Decryption에서 TLS 1.3을 지원하여야 한다. • 사용자 기반 보안정책 - Active Directory, LDAP, eDirectory 등의 User Directory 서버와의 연동이 가능하여야 한다. - 사용자 IP 정보를 Syslog로 전달받아 사용자 기반 정책 제어가 가능하여야 한다. - Unix / Proxy / 802.1x 인증시스템, NAC 인증시스템 및 로컬 계정 관리시스템 등과 API를 통한 연동이 가능하여야 한다. - 한글 User-ID를 인지하여 사용자별 정책 설정이 가능하여야 한다. - 여러 대의 방화벽 간 사용자 정보 연동이 가능하여야 한다. • 네트워크 - Static & Dynamic Routing(OSPF, BGP) 프로토콜을 지원하여야 한다. - Route / Bridge Mode를 인터페이스별로 동시 설정이 가능하여야 한다. - Link Aggregation Control Protocol(LACP), 802.1Q(VLAN)를 지원하여야 한다. - 다양한 NAT(PAT, 1:1NAT, 1:N NAT, M:N NAT) 기능을 지원하여야 한다. - 라우팅 Next Hop에 FQDN을 지원하여야 한다. • 이중화 - Active/Passive, Active/Active Failover 기능을 지원하여야 한다. - Configuration 및 Session에 대해 동기화 기능을 지원하여야 한다. • VPN - IPSec VPN, SSLVPN을 동시 지원해야 한다. - GRE Tunneling을 지원해야 한다. - VPN 사용자 인증시 AD, LDAP, RADIUS, Local DB 등의 Authentication을 지원해야 한다.	1식

항목	세부 규격	수량
차세대 방화벽	• 관리기능 - 데이터영역과 관리영역이 분리되어 있어야 한다. (관리모듈 재시작 시 서비스에 이상이 없어야 한다.) - XML / REST API를 제공하여야 한다. - Role-based Administrator 관리 기능을 지원하여야 한다. - Syslog 및 SNMP v2, v3를 지원하여야 한다. - 한 개의 보안 정책에서 IP, 사용자, 어플리케이션, Port, URL, IPS, Antivirus, Anti-Spyware, APT 등을 설정할 수 있어야 한다. - 하나의 화면에서 어플리케이션, 사용자, IP, 공격위협, URL 필터, 데이터 필터 등을 통합 모니터링 할 수 있는 기능을 제공하여야 한다. - 설정을 적용하기 전에 유효성을 확인할 수 있어야 한다. - 설정된 Candidate config를 적용하기 전에 Revert(Rollback) 할 수 있는 기능을 제공하여야 한다. - 장비에 접속해 있는 관리자는 다른 관리자가 장비에 접속해 정책수정 및 적용을 하지 못하도록 lock을 할 수 있는 기능을 제공하여야 한다. - config “저장, 스냅샷, 적용” 단계별 작업이 가능하여야 한다. - 암호사용 기간, 대문자, 소문자, 특수문자 등 관리자 패스워드의 제약사항을 설정할 수 있어야 한다. - 관리자의 관리 콘솔의 접근 제한 설정이 가능하여야 한다. - API를 통해 방화벽 설정이 가능하여야 한다. - 세션 종료에 대한 원인을 로그를 통해 확인이 가능하여야 한다. - 사용자별 또는 기간설정을 통한 어플리케이션 및 사용량 통계에 대한 리포팅이 가능하여야 한다. - 일별, 주별, 월별, 연간 시간별 리포트를 제공하여야 한다. • 탐지 및 차단 - 지정된 어플리케이션 내부의 Contents에 대한 위협을 탐지 / 차단이 가능하여야 한다. - C&C 서버에 대한 DNS Sinkhole 기능이 제공되어야 한다. - Botnet 탐지 및 차단 기능을 지원하여야 한다. - Spyware와 Worms 탐지 차단 기능을 지원하여야 한다. - 특정한 IPS / Virus / Spyware 시그니처를 예외처리 할 수 있는 기능을 제공하여야 한다. - 압축파일을 통해 유입되는 Virus를 탐지 및 차단을 제공하여야 한다. - Signature 자동 다운로드 및 스케쥴링 기능을 제공하여야 한다. - SSL(HTTPS) 암호화 트래픽 내의 악성코드를 탐지 및 차단을 제공하여야 한다.	1식

항목	세부 규격	수량
차세대 방화벽	• 카테고리별 URL 탐지 및 차단 - 카테고리 기반 URL DB에 대해 자동 업데이트를 제공하여야 한다. - Botnet, C&C 유해사이트에 대한 DB 제공 및 탐지 / 차단이 가능하여야 한다. - URL 필터의 카테고리 별, Custom URL필터 등 정책에 탐지 및 차단이 가능하여야 한다. - 추가 보안(AV, AS, IPS) 기능과의 연동으로 가시성을 제공하여야 한다. - SSL(HTTPS) 기반의 웹 사이트 탐지 및 차단이 가능하여야 한다. • APT 탐지 및 차단 - 의심되는 Unknown & 공격성 Malware 탐지 및 차단기능을 제공하여야 한다. - 이메일에 포함된 링크 주소를 분석하여 악성URL인 경우 차단 기능을 제공하여야 한다. - 이메일에 첨부된 Malware File의 탐지 및 차단을 제공하여야 한다. - SSL(HTTPS) 암호화 트래픽내의 Unknown 악성코드의 탐지 및 차단을 제공하여야 한다. - Unknown malware 차단 시그니쳐를 5분 단위로 업데이트가 가능하여야 한다. - URL Filtering에 의한 C&C, Malware Site 접속 차단을 위한 DB를 5분 단위로 업데이트가 가능하여야 한다. [하드웨어 및 성능사항] • Interface - MGMT 10/100/1000 port 1개 / HA 10G port 1개 / Data Interface 10/100/1000 port 12개 / 1G SFP, 10G SFP+ port 8개 / 40G QSFP port 4개 • Throughput(Application) - 최대 8.7Gbps의 어플리케이션 탐지기능 포함 방화벽 성능 제공 (HTTP 트래픽 기준) • Throughput(PS / Anti-Virus / Anti Spyware+Application) - IPS / Anti-Virus / Anti Spyware 등의 기능 Enable시 최대 4.4Gbps 성능 제공(HTTP 트래픽 기준, 모든 보안기능 Enable 시) • IPSec VPN - IPSec VPN 성능 최대 4.8Gbps - IPSec VPN Tunnel 최대 6,000개 지원(site to site 기준)	1식

항목	세부 규격	수량
차세대 방화벽	• SSL VPN - SSL VPN 동시 사용자 최대 2,048개 지원 • New Sessions / SEC - 초당 처리 세션(CPS) 96,000개 • Concurrent Sessions - 최대 동시 세션(CCS) 2,200,000개 지원(IPS / Anti-Virus / Anti-Spyware / URL Filter의 모든 보안기능 Enable시) • Virtual System(base / Max) 1/6 - Virtual System Upgrade : Additional 5 추가 제공하여야 한다. • Power : Dual Power	1식

바. 무선 AP 증설

항목	세부 규격	수량
무선 AP	[일반사항] • 기 운영 중인 무선 네트워크의 일체(무선AP, POE스위치, 무선인증, 무선 네트워크관리 등)에 대하여 기술지원을 병행하여 지원하여야 한다. • 물리적 규격 - 와이파이 : Wi-Fi 6 (802.11ax) 지원 - 포트 : 2.5GbE(IEEE 10/100/100/2500Mbps, 자동 링크속도 지원, Rj45), Serial Console(four-Pin) • Wi-Fi 표준 - IEEE 802.11 a/ac/ax/b/d/e/g/h/i/k/n/r/r/u/v 지원. - VHT MCS rates, 16/64/256/1024-QAM, 20/40/80Mhz 지원. - TWT, Long OFDM Symbol, Transmit beamforming, Airtime Faimess, AMSDU, AMPDU, RJFS, STBC, LDPC, MIMO Power Save, MRC, BPSK, QPSK, CCK, DSSS, OFDM, OFDMA, UL/DL MU-MIMO 지원. • RF 규격 - 802.11 a/b/g/n/ac Wave 2/ax, 2x2:2 지원. (5GHz 802.11 a/n/ac Wave2/ax 2x2, 2.4GHz 802.11 b/g/n/ax, 2x2) - 최대 Wi-Fi Bandwidth : 1.77Gbps 속도 지원. (5GHz radio 1,201Mbps, 2.4GHz radio 573Mbps) - MiMO 안테나 지원 : 2x2 MiMO, 2 SPATIAL STREAMS 지원. - 안테나 이득 : 5GHz 6dBi Omni, 2.4GHz 5dBi Omni (최대 복사 전력 : Max EIRP 5GHz 31dBM, 2.4GHz 29dBm) • 지원 기능 - AP당 최대 접속 단말 수 : 512 Clients per AP 이상 지원하여야 한다.	50개

항목	세부 규격	수량
무선 AP	- 무선랜 관리시스템을 통한 중앙 집중관리 기능 지원 및 단독 설치 가능 제품이어야 한다. - AP 단독으로 Captive Portal 기능 제공하여야 한다. - 자동 채널설정 및 출력 조정 기능 제공하여야 한다. - NAT / DHCP 서비스 및 메시(Multi-hop, either band) 기능 제공하여야 한다. - 인증 방식 : 로컬 데이터베이스 또는 원격 인증 지원하여야 한다. (802.1x EAP-SIM/AKA, EAP-PEAP, EAP-TTLS, EAP-TLS MAC등) - Fast Roaming 지원(802.11r, OKC, Enhanced roaming) - IPv6, 사용자 부하 분산, VLAN, 원격관리, QoS 기능 지원하여야 한다. - Web, SSH, syslog, SNMP v1, v2, v3 기능 지원하여야 한다. - 최대 소비전력 : 21W(802.3at PoE) - 상태표시 : Multi-color status LEDs 기능 지원하여야 한다. • 보안 기능 - Access Control List(ACL) 기능 지원하여야 한다. - 802.1x 웹 인증 및 Radius 인증 서버와 연동 기능 지원하여야 한다. - EasyPass with Microsoft Azure and Google G Suite integration 기능 지원하여야 한다. - WPA3, WPA2(CCMP, AES, 802.11i), WPA2(802.1x/EAP), WPA PSK(TKIP), 802.11w PMF 지원하여야 한다. • 기타 사항 - 국내 형식 승인 인증 제품이어야 한다.	50개

사. 무선 관리시스템

항목	세부 규격	수량
무선 관리 시스템	[일반사항] • 수용 용량 : 단일 무선랜 관리시스템에서 최대 1,000대의 AP 관리 지원하여야 한다. • VMWare 또는 Bare Metal Hypervisor에서 지원하여야 한다. • 제어 범위 : 802.11a/b/g/n/ac/ax 실내외 AP 동시 수용 제공하여야 한다. • 서비스 관리 및 설정 지원 - 이중화(Active-Standby Layer2를 통한 High Availability) 지원 - IEEE 802.1p를 통한 QoS 설정 지원하여야 한다. - EasyPass with Microsoft Azure and Google G Suite integration 설정 기능 지원하여야 한다.	1식

항목	세부 규격	수량
무선 관리 시스템	- 별도의 비용 추가없이 AP간 Mesh 설정 지원하여야 한다. - Voice, Data, Video 서비스 트래픽 관리기능 설정 지원하여야 한다. - 지역별, 서비스 유형별 그룹 관리 기능 제공하여야 한다. - DHCP / NAT 설정 지원하여야 한다. • 보안 설정 지원 - L2, L3, L4 Access Control List(ACL) 설정 지원하여야 한다. - 보안 규정 :IEEE 802.11i 지원, WPA2, WPA3 설정 지원하여야 한다. • 관리 기능 - Web UI를 통하여 전체 무선랜 관리 기능 제공하여야 한다. - 네트워크 Discovery 기능을 제공하여야 한다. - 무선랜 관리시스템에 장애 발생하여도 원활한 Wi-Fi 서비스 제공 가능하여야 한다. - AP / Client 접속 내용 제공하여야 한다. - AP 상태(UP/Down) 관리 및 이벤트 관리 기능 제공하여야 한다. - Firmware 자동 업그레이드 및 관리 기능 제공하여야 한다. - 단말 유형에 따른 통계 및 보고서 제공하여야 한다. [기타 사항] • 국내 형식승인 인증제품이어야 한다. • 무선AP와 동일 제조사 제품이어야 한다.	1식

아. 무선 PoE SW

항목	세부 규격	수량
무선 PoE SW	[일반사항] • 안정성 - 논스톱 운용을 위하여 스위치는 모듈라 OS를 지원하여야 하며, 프로세스별 모니터, 프로세스 재시작, 개별 소프트웨어 모듈별로 스위치 운용 중에 로드할 수 있어야 한다. - OS와 config 파일의 이중 저장이 가능하여야 한다. • L2 기능 - Jumbo Frame 지원(9,000byte 이상)하여야 한다. - IEEE802.1d/W/S 지원하여야 한다. - IEEE802.3ad 표준 Link Aggregation 지원(최대 128Group)하여야 한다. - VLAN 4,000개 지원하여야 한다. - FRC3619 네트워크 Ring 토폴로지를 지원하여 50밀리 세컨드 이내의 절체(failover) 시간을 지원하여야 한다.	6식

항목	세부 규격	수량
무선 PoE SW	• 보안 기능 - Virus, 웜 등 유해트래픽 차단을 위해 스위치에 보안엔진을 탑재하여 인입 트래픽에 대한 차단, QoS, Rate Limit 적용 혹은 해당 트래픽에 대한 자동 미러링 등을 지원하여야 한다. - RADIUS 및 TACACS+ 지원하여야 한다. - Time base ACL 지원하여야 한다. - ARP Spoofing 공격 방어를 위해 ARP ACL 기능을 제공하여야 한다. - 포트 미러링 기능 지원(N:1, 1:N, remote mirroring)하여야 한다. - Multiple supplicant 기능을 지원하여 하나의 스위치 포트를 공유하는 다수 유저에 대한 각각의 보안인증(802.1x)이 가능하여야 한다. - 사용자 로그인 ID를 기반으로 스위치에서 ID를 관리 / 통제 기능을 제공하여야 한다. • 지원 기능 - LLDP 프로토콜을 지원하여야 한다. - 2개의 스위치에서 나온 다수의 물리적 링크(port)를 논리적으로 하나로 묶는 Link Agreegation 기능(Active-Active로 사용하기 위함)을 지원하여야 한다. • 관리 기능 - 웹 브라우저를 통한 관리기능을 지원하여야 한다. - NTP(Network Time Protocol) 서버 지원하여야 한다. - RFC 3176(sFlow) 기능을 지원하여야 한다. - CLI Scripting 기능을 지원하여야 한다. - XML API 및 SNMP v1/v2/v3 기능을 지원하여야 한다. [하드웨어 사양] • 물리적 사양 - 24port RJ-45 10/100/1000 Base-T PoE / PoE+ 지원하여야 한다. - 4port 100/1000 Base-X(SFP) 지원(combo)하여야 한다. - 2port 10G Base-X(SFP+) 지원(1G/10G dual speed)하여야 한다. - 콘솔port 및 10/100 Base-T 관리 port 지원하여야 한다. - DRAM : 512MB, Flash : 512MB 지원하여야 한다. - Switching capacity 88Gbps 이상 - 전송 성능 : 65Mpps 이상 - L2 MAC 주소 테이블 16,000개 지원하여야 한다. - 전원 이중화 지원하여야 한다. • 가상화 기능 - 서버의 가상머신(Virtual Machine)의 이동, 삭제, 생성 등을 추적하여	6식

항목	세부 규격	수량
무선 PoE SW	스위치에서 가상 머신의 움직임에 따라 자동으로 보안 및 QoS 기능을 적용하는 기능을 제공하여야 한다. • L3 라우팅 기능 - IPv4 L3 라우팅 지원(RIP v1/v2, OSPF)하여야 한다. - IPv6 L3 라우팅 지원(RIPng, OSPF)하여야 한다. - 멀티캐스트 라우팅 지원(PIM)하여야 한다. - 하드웨어 기반의 IPv4 및 IPv6 Layer3 Routing 지원 및 동일 성능을 제공하여야 한다.	6식

자. 무선인증 솔루션

항목	세부 규격	수량
무선인증 솔루션	[일반사항] • 인증 - 국가용 정보보호제품 보안요구사항을 준용하여 CC인증을 획득한 제품이어야 한다. • 프로토콜 - IEEE802.1x 유 / 무선 표준 인증 알고리즘을 지원하여야 한다. • 주요기능 - PEAP / EAP-TTLS / FAST 등 터널링 기반 EAP 사용 시 Fast Re-authentication 제공하여야 한다. - ID, PW 외 MAC, HW ID, HDD Volume등을 조합한 특수 인증을 지원하여야 한다. - 기존 인증체계(PKI / ESSO / EAM 등), AD / LDAP 백-엔드 인사DB 다중 연동기능(PW 컬럼, 속성 값이 Hash된 인증 체계 연동 커스터마이징)을 제공하여야 한다. - HW장비 - 장비관리자ID 그룹 인증 관리기능을 지원하여야 한다. - 프로파일 기반의 인증관리 제공 및 사설인증서 발급 / 관리기능을 제공하여야 한다. - Windows OS계열 EAP-GTC를 지원하는 Plug-In을 제공하여야 한다. - ID기반 인증 DHCP 서버(UA-DHCP)를 통한 IP당 관리기능을 제공하여야 한다. - 사용자 ID 및 MAC address 기준 고정IP 할당기능을 제공하여야 한다. - 웹 인증서버 및 Captive portal 연계기능을 제공하여야 한다. - 무선랜 통신 구간의 암호화 지원(Dynamic WEB, WPA1/2 등)을 하여야 한다	1식

항목	세부 규격	수량
무선인증 솔루션	- 사용자 ID 및 MAC address 기준 고정IP 할당기능을 제공하여야 한다. - 웹 인증서버 및 Captive portal 연계기능을 제공하여야 한다. - 무선랜 통신 구간의 암호화 지원(Dynamic WEB, WPA1/2 등)을 하여야 한다. - 암호화 터널링 Cipher suit TLS v1.2를 지원하여야 한다. - 단방향 암호화 SHA1 / SHA256 / SHA512 / NT hash Hashed PW 사용을 지원하여야 한다. - EAP-AKA, EAP-SIM 지원하여야 한다. - 사용자 및 단말별 Dynamic VLAN 설정 기능을 제공하여야 한다. - NAS 장비와 연계하여 SSID별 사용자 접속을 통제 및 정책설정 기능을 제공하여야 한다. - NAS 장비의 ACL과 연계하여 특정 네트워크로의 접속을 통제하는 접근 속성 정책기능을 제공하여야 한다. - 사용자 정의 RADIUS Attribute 부가인증 및 속성 검증기능을 지원 하여야 한다. - 인증정책 가용성 향상을 위한 가상화 계정 및 단말 인증 부가 속성 기능을 통한 사용자별 / 부서별 정책설정 기능을 제공하여야 한다. - 사용자 / 그룹 / 방문자 / 장비 / 시간, 요일 / 사용자 유형별 인증 기반 네트워크 접근제어 기능을 제공하여야 한다. - 다수의 인사DB 연동 및 각 DB별 사용자에 대한 정책설정 기능을 제공하여야 한다. • 관리기능 - 장애 대비 및 성능 향상 목적의 Active-Active HA, Procy, DB replication등 자체 이중화 기능을 제공하여야 한다. - 웹 기반(TLS)의 콘솔 관리시스템 및 MA를 위한 CLI 인터페이스를 지원하여야 한다. - 부서별 서브 관리자 지정기능과 RBAC(Role Based Access Control) 기능을 제공하여야 한다. - 사용자 단말의 MAC address 자동 수집 기능을 제공하여야 한다. - 사용자 PW 에이징 기능(PW 기간 만료 시 사용자 변경 기능)을 지원 하여야 한다. - 지역별 동일한 사설 IP를 사용하는 NAS의 그룹별 / VLAN별 DHCP 설정 기능을 제공하여야 한다. - 단말의 DHCP 강제화 기능 및 NAS의 그룹별 / VLAN별 DHCP 설정기능을 제공하여야 한다. - DHCP 기능의 Secondary IP 기능과 사용자 ID / 단말별 고정IP 할당 기능을 제공하여야 한다.	1식

항목	세부 규격	수량
무선인증 솔루션	- 해킹사고 및 감사 목적으로 사용자 IP 할당 감사 증적 로그를 제공하여야 한다. - 장애 / 성능관리 및 관리자 편의성을 고려한 다양한 로그 / 통계 / 리포트를 제공하여야 한다. [추가사항] • 기 운영 중인 무선인증 솔루션의 업그레이드를 제공하여야 한다. • 기 운영 중인 무선인증 솔루션과 완벽한 호환 및 이중화 연동을 지원하여야 한다. • 기 운영 중인 무선 네트워크의 구성 변동 없이 연동 설정 지원 제공하여야 한다. [하드웨어 사양] • 하드웨어는 전원 이중화를 지원하여야 한다. • 1,000대 이상의 무선 AP 접속 지원이 가능하여야 한다.	1식

차. 무선 운영용 10G 집전스위치

항목	세부 규격	수량
집선 스위치	[일반사항] • 기 운영 중인 무선 네트워크용 집선 스위치를 병행하여 운영 시 기술지원을 하여야 하며, 정책 및 환경이 호환되어야 한다. • 19인치 표준 랙 장착이 가능하여야 한다. • 소프트웨어를 사용한 간편 구성 및 업그레이드, 통신장비 자동설정 구성을 지원하여야 한다. • 동작상태 및 장애관제(자원 이용현황, 장애 이벤트, 전원부, I/O 등) 기능을 제공하여야 한다. • 운영 중 Power Supply를 분리하여 장애 처리가 가능하여야 한다. • 시스템 장애 시 Core-Dump 생성 및 추출 기능이 가능하여야 한다. • 포트 미러링(TX, RX, Both - 기능별 각 N:1 세션 제공) 기능을 제공하여야 한다. • 관리자 권한 별 접근제어 관리 및 관리자 접근 로긴 기능을 제공하여야 한다. • 기존 통신장비와 상호 연계하여 통신망의 안정적 운영을 위한 ICMP, UDP, TCP, HTTP 프로토콜에 대한 Packet Loss, Jitter, Delay(Round Trip Time)등의 성능을 관제하여야 하고, 기준치 초과 시 Syslog 및 snmp Trap등을 발생하여야 하며, 논리적 정책을 설정하여 구체적인	1식

항목	세부 규격	수량
집선 스위치	조건이 성립하여 통신회선 차단 등의 명령을 수행하고 그 결과를 저장하는 기능을 지원하여야 한다. • 인증 실패 시 장비 접속 제한 시간을 관리자가 설정할 수 있는 기능을 제공하여야 한다. • 지정된 횟수(기본 값 5회 이상) 이상 인증 실패 시 일정기간(기본 값 5분 이상) 장비 접속을 제한하는 기능을 제공하여야 한다. • 장비에 저장된 모든 비밀정보(비밀번호, 사전 공유키 등)를 읽거나 유추할 수 없어야 한다. • 비밀번호 암호 알고리즘(대칭키 암호, 해시함수 등)을 이용하여 안전하게 저장하여야 한다. • 위조 DHCP 서버의 서비스 방지기능을 제공(DHCP snooping)하여야 한다. • IP Source 가드 기능으로 DHCP 환경에서 IP 변조 및 임의 세팅 방지기능을 지원하여야 한다. • Non-801.1x client를 위한 MAc 인증 / WEB 인증 기능을 지원하여야 한다. • 가상화 경로 설정(Routing) 기능을 지원하여야 한다. • 운용의 효율성 향상을 위한 자동화 구현 기능을 제공하여야 한다. • 소프트웨어적 네트워크 기술을 지원하여야 한다. • 현재 운용중인 시스템과 완벽한 연결 호환성을 제공하여야 한다. • 최신 출시 제품이어야 하며, 임대 기간 동안 제조사 및 공급자기술지원이 가능하여야 한다. [하드웨어 규격] • 스위치 용량 : 최대 3.2Tbps 이상 • 포워딩 성능 : 최대 1Bpps 이상, UADP 3.0이상 • 전원 이중화 구성 • SSD storage : 최대 960G 지원 • 기본 포트 : 48port 이상의 1/10/25Gigabit Ethernet SFP28 and 4port 이상의 40/100Gigabit Ethernet QSFP28 제공 • MAC Address : 82,000개 이상 • Total number of IPv4 routes - IPv4 : 최대 212,000개의 indirect+direct routes 최대 90,000개의 host/ARP • Total number of IPv6 routes - IPv6 : 최대 212,000개의 indirect+direct routes 최대 90,000개의 host • Total number of IPv4 Multicast routes : IPv4 최대 32,000개	1식

항목	세부 규격	수량
집선 스위치	• Total number of IPv6 Multicast routes : IPv6 최대 32,000개 • QoS ACL 용량 : 최대 16,000개 이상 • Security ACL 용량 : 최대 27,000개 이상 • 패킷 버퍼 용량 : 최대 36MB 이상 • FNF entries 수 : 최대 98,000 이상의 flow • DRAM : 16GB 이상 • Flash : 16GB 이상 • VLAN ID : 최대 4,094개 이상 • Jumbo Frame : 최대 9,216bytes 이상 • Layer2 Protocol 지원 - 802.1D, 802.1S, 802.1W, 802.3ad(LACP) 지원 - 902.1x 포트 기반 인증 및 VLAN assignment 지원 - PVST+ Rapid PVST 지원 - Per-피무 Rapid Spanning Tree Plus(PVRST+) 지원 • Layer3 Protocol(Basic Routing) 지원 - BGP, EIGRP, HSRP, IS-IS, BSR, MSDP, PIM-BIDIR, IP SLA, OSPF - PVLAN, VRRP, PBR, QoS, FHS, CoPP, SXP, IP SLA Responder - IGMP v1/2/3 Snoopong 지원 • High availability and resiliency - NSF, ISSU, StackWise Virtual • Network segmentation - VRF, VXLAN, LISP, SGT, MPLS, mVPN • Automation - NETCONF, RESTCONF, gRPC, YANG, PnP Agent, ZTP/Open PnP, Guest Shell(On-Box Python) • Telemetry and visibility - Model-driven telemetry, sampled NetFlow, SPAN, RSPAN • Security - MACsec-256 지원 • 포트 수량만큼의 정품 GBIC Module을 장착하여 제공하여야 한다.	1식

카. 무선 AP 설치 및 케이블 포설

항목	세부 규격	수량
무선 설치 및 케이블 포설	[일반사항] • 기 운영 중인 무선AP 음영지역 개선을 위하여 대학이 요구하는 위치로 기존 무선AP를 이동 설치를 지원하여야 한다. • 신규 무선AP 및 무선 네트워크 구축 및 지원하여야 한다. • 선로 구성은 대학의 승인을 받은 후 작업하며, 선로작업 완료 후 선로테스트 및 케이블 포설 도면을 제출하여야 한다.	1식

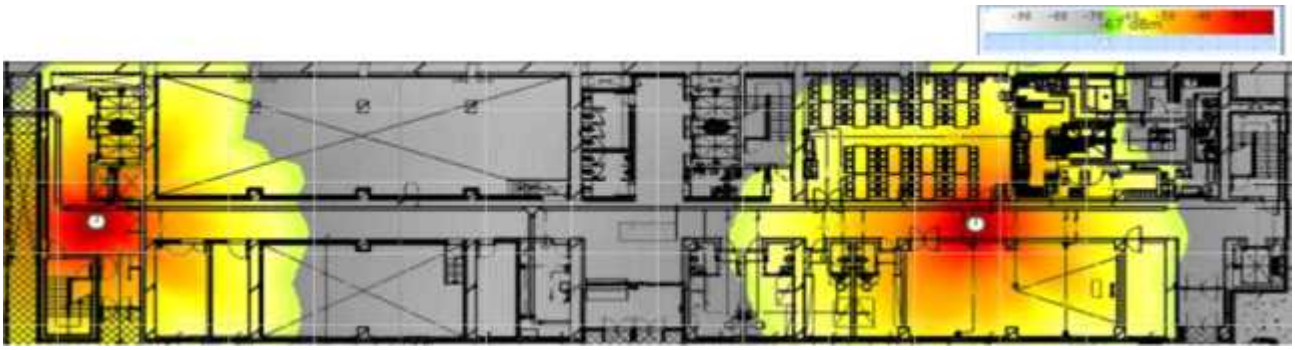
항목	세부 규격	수량
무선 설치 및 케이블 포설	• 무선AP용 케이블 포설 및 단말처리 완료 후에는 도통시험을 행하여 그 결과를 문서로 보고하여야 한다. [설치 및 케이블 포설] • 배선용 Data Cable - 종류 : UTP-4P CAT.6 Cable - 기능 : 건물 내 수평, 수직 배선망, Standard Type - 사양 : 10/100/1000 Base-T(IEEE 802.3), 도체규격 0.5mm(AWG24), 외경 5.0(Nom.), Pair 수 4개 - 특기사항 : Wireless LAN Cable 전용으로 기존 케이블과 피복 색상을 구분하며, 무선AP 1대당 2회선 사용할 수 있어야 한다. • UTP Patch Cord - 종류 : UTP-4P CAT.6 Patch Cord - 기능 : LAN HUB 장비와 Patch Panel을 연결하여야 한다. - 사양 : 규격 EIA / TIA CAT/6, 길이 3M 단선제품, 전송대역 1Gbps 이상의 네트워크 속도 지원하여야 한다. • Patch Panel - 종류 : 24 port CAT.6 Patch Panel - 기능 : Patch Cord를 사용하여 Patch Panel과 LAN 장비를 연결하고, Patch Cord를 각 port에 접속, 단락이 용이하도록 하며, Cable 인식표를 부착하여 관리가 용이하도록 하여야 한다. - 사양 : 24 port 19“ Rack Type, EIA / TIA 5688 CAT.6 규격, 각 포트와 Panel 식별이 용이하게 라벨프린트로 부착 표시하여야 한다. • Rack Box - 종류 : 네트워크 전용 랙 박스 - 기능 : LAN 장비 및 Patch Panel 등을 설치 - 사양 : 19“ Cabinet Type - 특기사항 : 각 건물 EPS실 공간을 고려하여 크기 결정 • 배관 - 종류 : 합성수지제 가요전선관(난연) - 기능 : 천정 UTP 케이블 보호용 CD관 - 사양 : 내경 22mm, 외경 27.5mm	1식

타. 기타사항

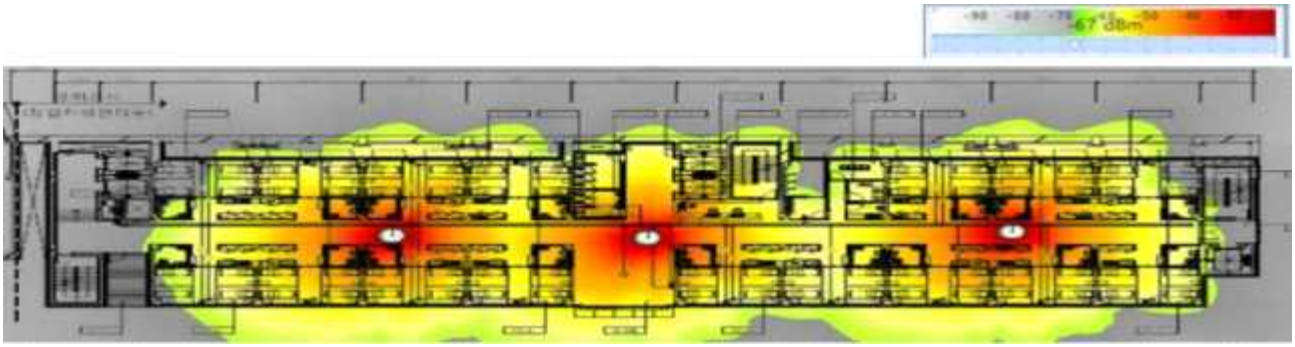
항목	세부 규격	수량
공통사항	[일반사항] • 본 사업에 해당되는 기 운영중인 모든 품목에 대하여 사업이 완료 및 검수 시점까지 무상 운영 및 유지보수를 지원하여야 한다. • 본 사업에 해당되는 도입 및 업그레이드 품목 중 대학이 지속적으로 활용하고자 할 경우 유지보수 및 기술지원을 하여야 한다. • 임대 사업 종료 시까지 매월 1회 방문 점검하여야 한다. • 정기 점검 및 수시 점검 시 보고서를 제출하여야 한다. • 최신 출시 제품이어야 하며, 제조사 정품공급 확약서를 제출하여야 함. • 임대사업 전체 기간 동안 제조사기술지원 확약서를 제출하여야 함. • 교육부 개인정보보호. 정보보호 수준진단 관련항목에 충족하여야 한다. [무선 네트워크 요구사항] • 신규 도입 무선AP와 기 운영 중인 무선AP와 효율 및 호환성 유지를 위하여 대학이 요청하는 기 운영 중인 무선AP에 대하여 층간, 건물 간 이전 설치를 지원하여야 한다. • 기 운영 중인 무선 네트워크 전체 시스템에 대하여 임대기간 동안 매월 1회 정기방문 점검을 포함하여 기술지원 및 유지보수를 시행하여야 한다. • 무선AP 서베이에 없는 무선AP 수량은 대학에서 지정하는 곳에 추가 설치를 하여야 하며, 케이블 포설을 포함한다. • 무선AP용 PoE SW는 대학에서 지정하는 곳에 설치하여야 하며, 필요한 일체의 작업을 포함한다. • 본 사업과 관련하여 임대 품목 구축 및 설치 시 기계실 내의 부대설비에 영향을 주지 않도록 하여야 하며, 부주의 등으로 인하여 부대설비를 손상시켰을 경우 즉각 원상복구 하여야 한다. • 임대 품목 구축 시 업무에 지장을 초래하지 않는 시간을 이용하여 구축하여야 하며, 구축에 필요한 각종 부대장비, 소모품 일체 등은 주 사업자가 부담하여야 하며, 무상으로 공급하여야 한다.	1식

파. 국제관 무선AP 설치 위치

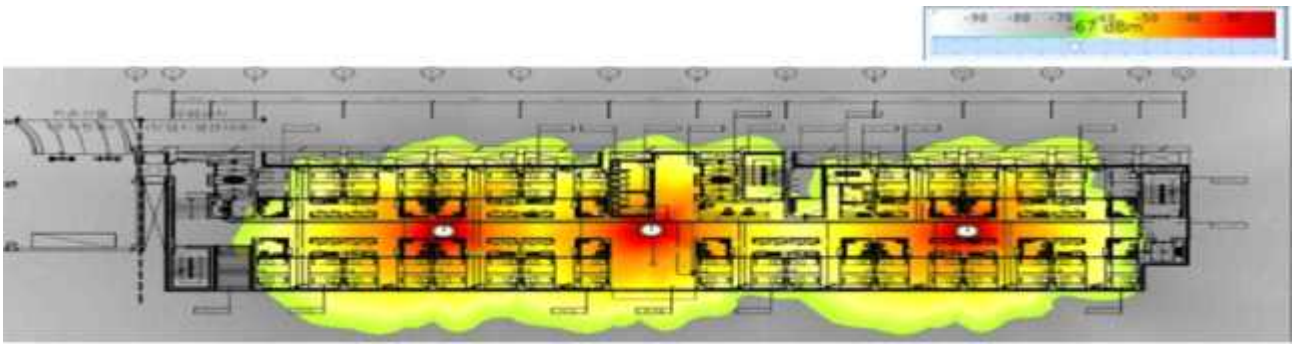
- 로비(지하) - 무선AP 설치 수량 : 2대



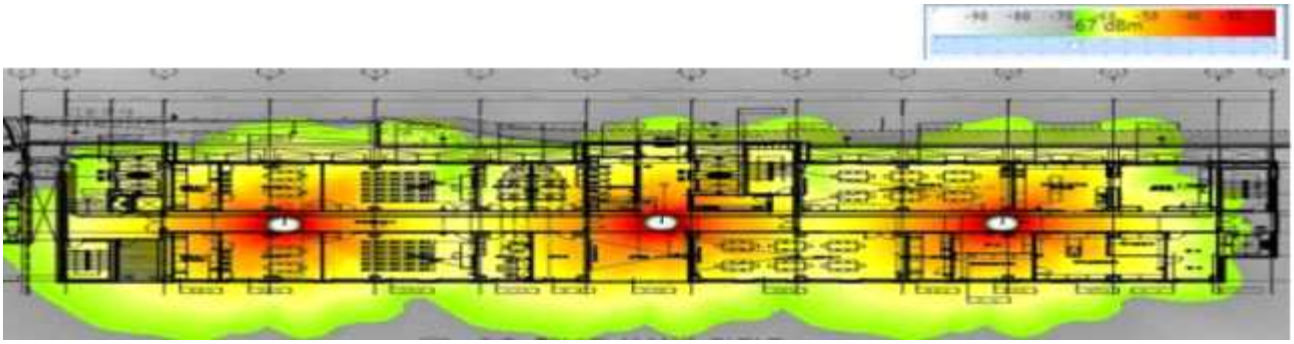
- 1층 - 무선AP 설치 수량 : 3대



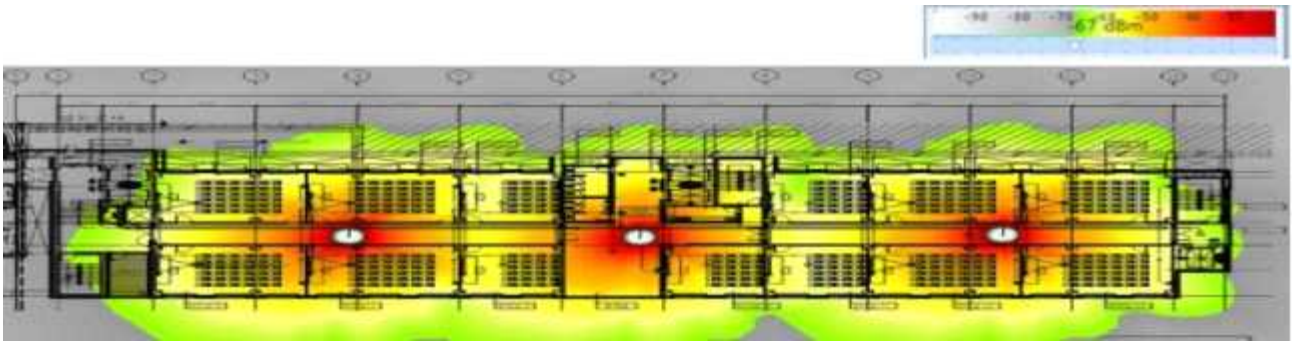
- 2층 - 무선AP 설치 수량 : 3대



- 3층 - 무선AP 설치 수량 : 3대

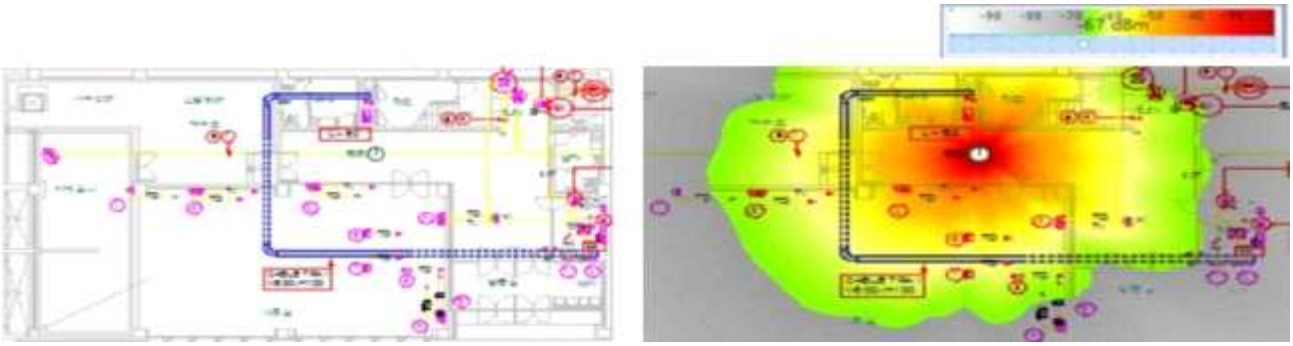


- 4층 - 무선AP 설치 수량 : 3대

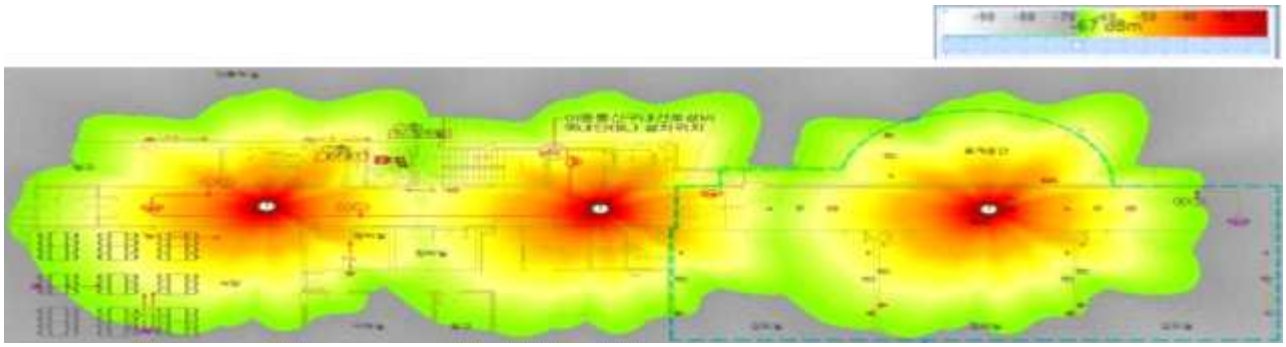


- 옥탑층(도면 없음) - 설치 무선AP 수량 : 3대

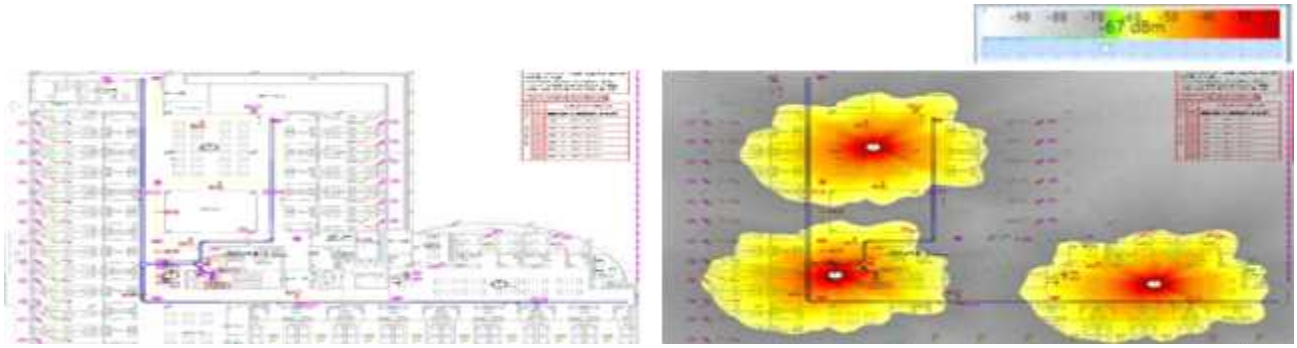
- 별관 1층 - 설치 무선AP 수량 : 1대



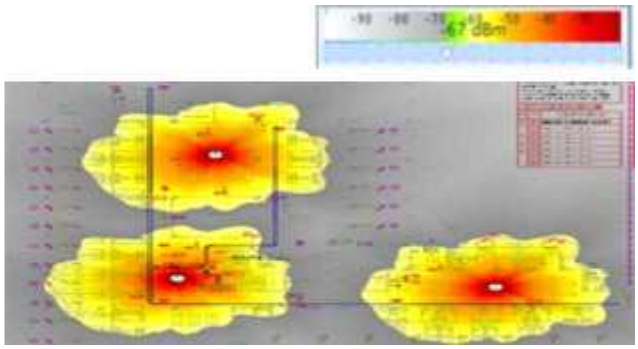
- 별관 2층 - 설치 무선AP 수량 : 3대



- 별관 3층 - 설치 무선AP 수량 : 3대



- 별관 4층 - 설치 무선AP 수량 : 3대



- 별관 옥탑층 - 설치 무선AP 수량 : 1대