주어진 Korealt 인력현황, 정보보호시스템목록, 시스템 구성도를 통해 현재의 상태를 파악하고 관리적, 물리적, 기술적 정보보호 목표를 새로 도입된 장비를 기준으로 설정하시오. (외부에서의 트래픽 탐지를 위한 장비(IDS)와 통합모니터링 장비가 새로 도입될 예정임)

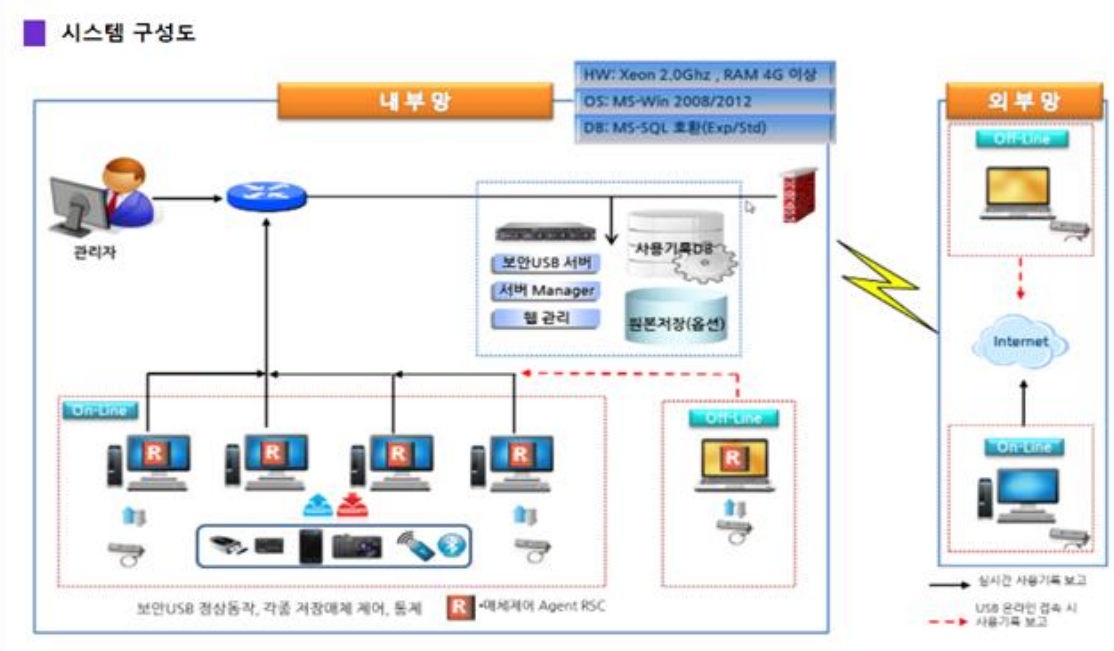
< Korealt 인력 현황 >

구분	자산명	수량	용도	자산위치	관리부서
서버	원격교육 웹서버	2	어플리케이션 관리	서버실	운영부
	원격교육 데이터서버	2	가입자 및 정보 관리	서버실	운영부
네트워크	일반스위치	1	스위칭	서버실	네트워크팀
	L4	1	로드밸런싱	서버실	네트워크팀
보안장비	통합방화벽	1	통합방화벽	서버실	보안팀
시설	에어컨	2	온도조절	서버실	운영부

< Korealt 정보보호 시스템 목록 >

업 무	부서명	내부인력	외부인력	합계
인적보안 및 교육	인사팀	2명	1명	3명
내부 보안감사	감사실	2명	1명	3명
네트워크 장비 및 보안장비 운영	네트워크관리팀	3명	2명	5명
통합보안 모니터링	정보관제실	5명	3명	8명
합 계		12명	7명	19명

< Korealt 시스템 구성도 >



▶ **관리적 물리적 기술적 정보보호 목표**

구분	항목	세부 설명
관리적	보안정책 수립 및 갱신	IDS 및 통합모니터링 장비의 운영 정책과 로그 분석 기준을 수립한다.
	관제 인력 교육	새로운 장비의 운영 방법 및 로그 분석 훈련을 통해 관리자 대응 능력을 향상시킨다.
	사고 대응 절차 마련	탐지된 이상 트래픽 발생 시 사고 대응 시나리오를 매뉴얼화한다.
	정기적 감사 및 점검 수행	IDS 및 모니터링 로그를 주기적으로 검토하고, 이상 징후를 식별한다.
물리적	장비 물리적 보안 강화	IDS 및 통합모니터링 시스템이 설치되는 장소의 출입통제를 강화한다.
	전원 및 냉각 관리	24시간 운영되는 장비 특성을 고려해 UPS 및 공조 시스템 점검을 강화한다.
	서버실 접근 통제	등록된 인력 외에는 출입 불가하게 하고 CCTV로 기록을 남긴다.
기술적	IDS 탐지정책 구성	외부에서 유입되는 비정상 트래픽에 대한 탐지 규칙을 체계화한다.
	로그 통합 및 분석 기능 강화	통합모니터링 시스템을 통해 다양한 장비의 로그를 수집·분석한다.
	자동 경보 시스템 구성	이상 행위 발생 시 관리자에게 즉각 알림이 가도록 구성한다.
	상호 연동 설정	기존 방화벽 및 보안정책 서버와의 연동을 통해 위협 정보의 실시간 공유 체계를 마련한다.

주어진 정보자산 중요도 목록 문서를 통해 추가 도입된 IDS, 통합모니터링 장비에 대해 문서화하시오.

▶ **IDS (침입탐지시스템)**

자산그룹 ID	SV-08-002	**자산그룹 이름**	IDS(침입탐지시스템)
세부자산목록	내부망 및 외부망 트래픽에 대해 이상 행위를 탐지하고 관리자에게 알림		
구분	**자산소유자**	**자산관리자**	**자산사용자**
성명	장길동 부장	최길동 팀장	네트워크관리팀

중요성 평가	**평가 등급**	**합계**	**서비스 범위**	**중요도**	**연관도**
기밀성	나	8	2	3	1
무결성	가	9	3	3	2
가용성	가	9	3	3	2

▶ **통합모니터링 장비**

자산그룹 ID	SV-08-003	**자산그룹 이름**	통합모니터링 장비
세부자산목록	전체 보안 장비 및 서버 상태를 통합 대시보드로 시각화, 이상 로그 수집 및 분석		
구분	**자산소유자**	**자산관리자**	**자산사용자**
성명	박길동 부장	황길동 팀장	정보관제실

중요성 평가	**평가 등급**	**합계**	**서비스 범위**	**중요도**	**연관도**
기밀성	나	9	3	3	2
무결성	나	9	2	3	2
가용성	가	10	3	3	2

KoreaIt 내에서의 추가 도입된 장비를 기준으로 중장기 계획을 수립하고 그에 따른 세부 실행 계획을 관리적, 물리적, 기술적 보안 영역으로 구분하여 문서화하시오.

1. 중장기 정보보호 계획

연차	주요 목표	세부 내용
1차년도 (단기)	신규 장비 구축 및 시범 운영	IDS 및 통합모니터링 장비 도입, 시범 운영 및 운영 정책 수립, 인력 교육 실시
2차년도 (중기)	연동 및 통합 보안체계 구축	방화벽, 서버, 백신, 네트워크와의 연동 구축, 통합 로그 관리 체계 수립, 자동화 경보 시스템 설정
3차년도 (장기)	고도화 및 자산 기반 보안 강화	위협 인텔리전스 연동, AI 기반 로그 분석 도입 검토, 보안운영센터(SOC) 내재화 준비

2. 세부 실행 계획

구분	실행 내용	세부 항목
관리적	보안 정책 정비	IDS/모니터링 운영지침, 이상징후 대응 매뉴얼 수립
	보안 교육	장비 운영자 대상 보안교육 및 로그분석 교육
	보안 점검 체계	로그 리뷰 및 이상행위 점검 프로세스 마련
	인증 관리 강화	장비 접근 계정의 주기적 변경 및 권한 통제
물리적	서버실 출입 통제 강화	바이오 인증 장비 도입, 출입 기록 로그 유지
	장비 전용 존 구성	IDS 및 모니터링 장비 분리 존 구성, 장애 대응 계획 수립
	영상 기록 연계	CCTV 감시 강화 및 출입과 연계된 로그 시스템 구축
기술적	IDS 탐지 정책 설정	서명 기반 및 비정상행위 탐지 규칙 설정
	통합 로그 수집 구성	방화벽, 서버, 네트워크 장비 로그 통합 수집 및 분석
	경보 및 대응 자동화	이상 트래픽 발생 시 관리자 경보 및 차단 정책 설정
	AI기반 분석 도입 검토	머신러닝 기반 이상징후 탐지 시스템 파일럿 테스트

3. 기대 효과

- 실시간 위협 대응 체계 강화 (IDS)
- 보안 운영 가시성 향상 및 업무 효율성 제고 (통합모니터링)
- 보안 사고 예방 및 내부 정보자산 보호 체계 고도화