현재의 물리적 보안 구축 상황을 파악하여 운영하고 운영 시 발생할 수 있는 문제점과 그에 대한 개선 사항을 서술하고 최근의 물리 보안과 관련된 신규 위협에 대해서 서술하시오.

1. 현재의 물리보안구축 상황 예시

- 데이터 센터의 모든 출입구에는 보안 카드 리더기와 생체 인식 장치가 설치되어 있고, 출입 기록은 자동으로 로그에 저장됨

- 중요한 서버가 있는 랙에는 시건 장치와 경고 시스템이 설정되어 있음. 랙이 무단으로 개방되면 관리자에게 알림이 감

- CCTV 카메라는 서버실과 주변을 24 시간 모니터링하고 있음

- 데이터가 저장된 서버를 물리적으로 접근할 때, 보안 카드나 생체 인식 장치 외에도 비밀번호나 일회용 -키를 추가로 요구하는 이중 인증 방식이 적용됨

- 데이터 센터 내의 일부 구역에서는 잠금 장치가 설치되어 있으며, 해당 구역은 직원들이 사용하지 않을 때 잠금 상태로 유지됨

2. 물리보안 운영 시 작업 내용 및 개선 사항 예시

- 서버실과 데이터 센터의 출입 기록을 주기적으로 점검하여 무단 출입 여부를 확인, 기기 오작동 검사

- CCTV 시스템의 영상을 정기적으로 확인해보고 혹시 사각지대가 있으면 위치를 재조정 하여야 함

- 오래되어 제대로 작동하지 않는 시건 장치가 있는지 확인 후 필요하다면 교체

- 비밀번호 및 일회용 키의 사용 이력을 점검하고, 직원들이 비밀번호를 공유하지 않도록 교육

- 잠금 장치가 설치된 구역에 대해 직원들이 실제로 사용하지 않는 경우 잠금 상태를 유지하도록 교육

3. 물리보안 신규 위협 예시

- 디지털 해킹 : CCTV 시스템에 대한 사이버 공격으로 영상 정보가 조작되거나 감시가 무력화될 가능성

- 사회적 엔지니어링 : 내부 직원의 신뢰를 이용해 보안 시스템을 우회하려는 시도. 예를 들어, 위장된 수리업체 직원이 장비 점검을 핑계로 서버실에 접근하는 시도

- 스마트 잠금 시스템 해킹 : 고급 전자식 잠금 장치를 해킹해 출입을 통제하는 공격

- 물리적 침입 : 무단 출입 시도를 방지하기 위해 보안 장치가 강화되었지만, 침입자가 물리적인 힘을 사용해 보안 시스템을 우회하려는 시도

- 내부자 위협 : 권한을 가진 직원이나 외부 협력자가 비밀 정보에 접근하거나 데이터를 유출하는 사례