발신: (주) 아이디스
수신: 고객님
제목: **NVR(리눅스) 제품의 보안 관리 안내**

안녕하세요 아이디스 TS팀 입니다.
당사 NVR(전제품) 녹화기의 보안 관리는 아래와 같습니다. 최근 NIS(국정원)에서 공공기간 중심으로 보안 점검 가이드 지침이 전달되었으며, 관련 자체 점검을 진행함에 있어 고객님의 문의에 대한 당사 보안장비의 구조와 이해를 돕기 위한 설명 입니다.

Q. 리눅스 시스템에서의 악성코드 감염 될 수 있는지?
A. 리눅스 시스템의 악성코드(바이너리 또는 스크립트) 감염은 주로 사용자 또는 관리자의 부주의, 실수 또는 방심으로 인해 발생합니다.
대부분 인지하지 못한 상태에서 악성 파일이 설치되거나 저장됩니다.
일반적으로 리눅스 시스템은 root 권한 없이 악성코드 설치나 실행이 불가능하나, 편의를 위해 su 또는 sudo 명령을 통해 관리자 권한을 사용할 경우 감염 위험이 커집니다.
보안이 필요한 시스템에서는 로컬 콘솔(직접 연결된 터미널)만 접근을 허용하고, 원격 접속(SSH 등)은 비활성화하는 것이 안전합니다.
또한, 사용자 및 그룹 별로 최소 권한을 할당하고 권한에 맞게 운영하는 것을 권장됩니다.

Q. IDIS 제품의 감염 가능성은?
A. IDIS 리눅스 기반 녹화기 제품의 시스템 접근 경로는 업그레이드(로컬/원격) 방식이 유일합니다.
업그레이드 파일은 암호화되어 있으며, 무결성 검증 및 비공개 보안 포맷을 통해 안전하게 처리됩니다.
또한, 아이디스 제품은 시스템(OS 및 애플리케이션) 저장소가 "읽기 전용(Read-Only)"으로 설계되어 있어 외부에서 파일을 쓸 수 없습니다.
이로 인해 악성코드 포함을 포함한 외부 코드 유입이 구조적으로 차단되어 있어 보안성이 매우 강합니다.

Q. IDIS 제품의 보안 설계 구조는?
A. 아이디스는 "KISA(한국인터넷진흥원) 및 TTA(한국정보통신기술협회)"의 보안 지침을 준수하고 있으며,TTA 검증 결과에 따라 스탠드얼론 제품에는 원격을 통한 침투 가능 서비스가 존재하지 않습니다.
일부 제품들이 TELNET, FTP, SSH 등 관리 편의 목적으로 원격 서비스를 개방하여 보안 취약점을 노출시키는 반면, IDIS는 자체 개발한 프로토콜을 사용하여 외부 접근을 엄격히 통제하고, 지속적인 보안 검증을 수행하고 있습니다.

Q. IDIS 제품에 대한 자체 보안 점검 가능 여부
A. IDIS 리눅스 OS 제품은 (물리적/논리적) 콘솔 접근(예: serial, Telnet, SSH)을 지원하지 않습니다.
이는 시스템 보안을 최우선으로 고려하여, 관리용 콘솔 접속 경로 자체를 제거한 설계 방침에 따른 것입니다. 따라서 일반적인 리눅스 시스템처럼 직접 접근하여 자체 점검을 수행하는 것은 불가능합니다.

결론
IDIS 스탠드얼론 제품은 리눅스 OS 기반으로 설계되어 있으며, 모든 외부 접근 경로와 실행 파일 쓰기 경로를 원천 차단함으로써 해킹, 악성코드 등 사이버 위협으로부터 안전합니다.
앞으로도 IDIS는 보안 중심의 제품 철학을 바탕으로, 고객의 신뢰를 지키는 안전한 시스템을 제공하겠습니다.