제목 : 제로트러스트 보안 모델에서 보안관제 시스템 강화 연구

1.제로 트러스트 보안 모델

모든 통신을 의심하고, 감시하며, 접근 요청자에 대한 엄격한 인증과 최소한의 접근 권한을 부여하여 보안성을 높이는 개념

이 모델은 전통적인 경계 기반 네트워크 보안 모델의 한계를 극복하기 위해 제시

경계를 넘어 네트워크에서 발생하는 모든 행위를 믿지 않는 사상에 기반하여 보안 모델을 구축

2.주요 특징 및 목적

2-1. 신뢰하지 않음:

제로 트러스트 모델은 모든 통신을 의심하고, 기본적으로 믿음의 개념 배제

2-2. 엄격한 인증:

모든 접근 요청자에 대해 엄격한 인증 절차를 수행하여 신원을 확인

2-3. 최소한의 접근 권한:

최소한의 접근 권한만을 부여하여 민감한 자원에 대한 액세스를 제한

2-4. 네트워크 전체적인 보안 강화

:경계를 넘어 모든 행위에 대해 보안성을 강화하여 내/외부 시스템의 보안을 향상

3. 의의

이러한 제로 트러스트 모델은 보안관제 시스템의 강화를 위해 도입되었으며, 무단 접근과 데이터 유출 등의 보안 위협으로부터 기업의 보안을 강화하기 위한 방안으로 활용