11.1 침입차단시스템의 필요성

정보 시스템의 진보

- 중앙집중식 데이터 처리시스템
  - 직접 연결된 여러 터미널을 지원하는 중앙 메인프레임
- LAN
  - PC와 터미널을 서로 연결하고 메인프레임과도 연결
- 댁내 네트워크(premises network)
  - 여러 개의 LAN, 연결된 PC, 서버, 한 두 개의 메인프레임으로 구성
- 기업 네트워크(enterprise-wide network)
  - 지리적으로 분산된 다수의 댁내 네트워크가 사설 광역 네트워크(WAN)에 의해 연결
- 인터넷 연결성(Internet connectivity)
  - 다양한 댁내 네트워크가 모두 인터넷에 연결

침입차단시스템 등장 배경

- 인터넷 연결성은 필수사항
  - 정보와 서비스의 가용성도 아주 중요
- 인터넷 연결로 인해 밖에서도 지역 네트워크 정보에 접근할 수 있고, 상호교환이 가능
  - 기관에 대한 위협
- 각 워크스테이션과 서버 내에 침입방지와 같은 강력한 보안장치 설치 가능
  - 현실적인 어려움
- 침입차단시스템
  - 내부적으로 제어할 수 있는 링크 구성
  - 외부로부터 보호하기 위한 보안 외벽 또는 경계선을 치기 위해 외부 인터넷과 내부 네트워크 사이에 설치

침입차단시스템

- 목적
  - 인터넷 기반 공격으로부터 댁내 네트워크를 보호하고 보안과 감사를 할 수 있는 길목(choke point)를 한군데로 모으는 것
- 단 한대의 컴퓨터 시스템일 수도 있고, 여러 대의 시스템으로 구성할 수도 있음
- 침입차단시스템은 외부 네트워크로부터 내부 네트워크를 보호하기 위한 방어층을 하나 더 보강하는 것