

네트워크 연계 제한장치

기술키워드	물리적 단방향 장치, 물리적 통신 모드 변경, 물리적으로 분리된 망간 자료 전송								
지식재산권	출원 3건(대한민국 1건, 미국 2건), 등록 3건(대한민국)								
기술완성도 (TRL)	기초 실험	개념 정립	기능 및 개념검증	연구실환경 테스트	시제품 제작	시제품 성능평가	시제품 신뢰성평가	시제품 인증	상용품

기술개요

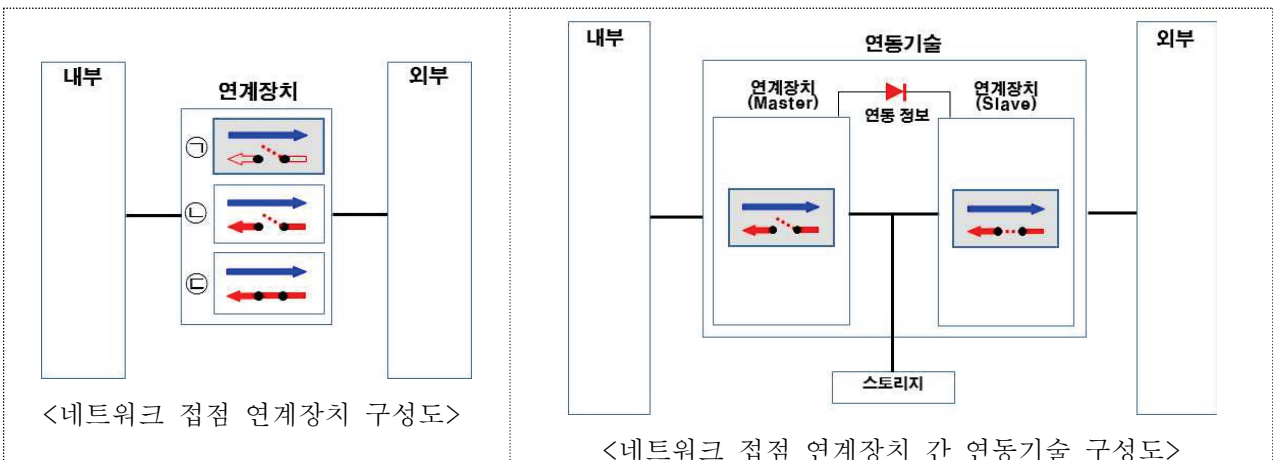
• 네트워크 연계 제한장치(세부기술 1)

- 물리적 단방향 장치는 망연계 기술의 한 종류로 보안수준이 다른 두 네트워크(내부망, 외부망) 또는 시스템(내부PC, 외부PC)에 적용하여, 내부(네트워크/시스템)→외부(네트워크/시스템)로 데이터는 전송 지원가능하나 내부←외부는 물리적으로 통신이 불가능하여, 외부에서 내부로 원격 침입이 물리적으로 불가능한 기술임
- 하지만, ①프록시 프로그램 구현의 어려움(내부 정보의 타기업 공개 꺼림, 종단간 암호화 적용 프로그램 사용 등의 원인), ②내부에서 파일 수신(백신 업데이트, 윈도우즈 업데이트)의 필요성 및 ③원격접속의 필요성으로 인해 물리적 단방향 장치만을 적용하는 것이 불가한 환경이 존재함
- 3가지 통신 모드(단방향, Outbound 양방향, 양방향)를 지원하는 제안 기술은 필요시 적절한 통신 모드를 선택하여 사용할 수 있도록 하며(평시 단방향, 비상시 양방향을 쉽게 전환 가능), 상황별 맞춤형 고수준의 보안성을 제공함
 - ㉠ 단방향 모드: 물리적 단방향 장치와 동일
 - ㉡ Outbound 양방향 모드: ①과 ②를 지원
 - ㉢ 양방향 모드: ③을 지원

• 네트워크 연계 제한장치 연동 기술(세부기술 2)

- 연동 기술은 내부(네트워크/시스템)와 외부(네트워크/시스템)간 스토리지를 경유한 데이터 교환을 지원할 수 있으나, 내부와 외부간 직접적인 양방향 통신은 물리적으로 불가능한 구조를 가짐
- 연동 기술은 내부와 외부간 실시간 양방향 연결이 필요한 백도어의 위협을 물리적으로 차단할 수 있음

• 기술 구성도



기술성

- (네트워크 연계 제한장치) 물리적 단방향 장치의 적용이 불가능한 환경에 적용하여 상황별 적절한 보안을 제공함
 - 단방향 모드: 물리적 단방향 장치와 동일한 보안성 제공(내부←외부는 물리적 연결 불가)
 - Outbound 양방향 모드: 허용된 Outbound TCP 세션이 없는 동안은 물리적 단방향 장치와 동일한 보안성 제공(Outbound TCP 세션이 있는 기간 동안에만 내부←외부를 물리적 연결 허용)
 - 양방향 모드: 정책 기반 필터링 보안성 제공(내부←외부를 물리적 연결 항상 허용)
 - * 망연계(시스템연계)시, 필요시에만 통신 모드를 변경하여 보안성 최대화 가능
- (네트워크 연계 제한장치 연동 기술) 내부/외부간 양방향 통신은 물리적으로 불가능한 독창적 구조를 지님
 - 타 네트워크연계 솔루션(물리적 양방향 연결)과 차별화된 구조를 지님

시장성

- (국내시장) 망분리 솔루션은 2017년 837억, 2020년 1,677억까지 국내 시장의 성장 예측(한국정보보호산업협회)
 - * 국내 정보보호 시장 주요 분야 중 가장 높은 폭의 성장률(26%, 업계 전체는 연평균 17% 성장률)을 보임

기술 응용 분야

- 시스템/네트워크 간 망 연계 시 보안 강화가 요구되는 분야
 - 기반시설 제어시스템 - 업무망/인터넷망 등
 - 대민지원 분야 - 민원처리 키오스크/중앙서버

기술개발 완료시기

- 2017년 11월 완료

관련 특허 세부정보

- (등록) 10-1881061(2018. 7. 17. 대한민국) "모드 변경이 가능한 양방향 통신 장치 및 방법"
- (등록) 10-1951672(2019. 2. 19. 대한민국) "조건부 양방향 통신 장치 및 방법"
- (출원) 2017-0068457(2017. 6. 1. 대한민국), 15/818908(2017. 11. 21. 미국) "단방향 통신을 이용하여 양방향 통신을 지원하는 장치 및 그 방법"
- (등록) 10-1972469(2019. 4. 19. 대한민국), (출원) 15/805292(2017. 11. 7. 미국) "분리된 망 사이의 데이터 통신을 지원하는 장치 및 그 방법"

기타

- 해당 기술은 2개의 하위 기술(네트워크 연계 제한장치, 네트워크 연계 제한장치 연동 기술)로 구분하여 기술이전 할 수 있음(기술이전 상담 시 별도 문의)