네트워크 트래픽 수집 · 점검 기술

기술키워드	트래픽 수집, 트래픽 점검, 네트워크 접점, 악성코드, 정보유출								
지식재산권	출원 2건(대한민국)								
기술완성도 (TRL)	기초 실험	개념 정립	기능 및 개념검증	연구실환경 테스트	시제품 제작	시제품 성능평가	**시제품 신뢰성 평가**	시제품 인증	상용품

기술개요

- 휴대용 네트워크 트래픽 수집 기술
  - · 스위치 미러링 또는 탭 장비를 통해 소형 상용 임베디드 장치를 이용하여 네트워크 트래픽을 수집하는 기술
- 네트워크 이상징후 점검 기술
  - · 수집된 네트워크 트래픽 패킷의 헤더 및 페이로드를 분석하여 네트워크 접점과 같은 비인가 연결 점검, 악성코드 점검, 정보유출 점검 등을 수행하는 기술
- 기술 구성도

기술성

- 네트워크 트래픽 수집·점검 기술 확보
  - · 제어시스템 및 정보시스템에서 네트워크 접점 탐지 등 비인가 연결 점검, 비인가 IP 점검 및 패킷 페이로드 재조합으로 잠재된 악성코드 전파, 정보유출 점검 가능
  - · 소형 상용 임베디드 장치를 활용한 네트워크 트래픽 수집 기술
  - · 트래픽 저장을 위한 저장매체를 외장매체 활용하여 보안규정 준수 용이
- 고가의 외산 네트워크 트래픽 수집 장치 국산화
  - · 외산 상용 장비 대비 단가 70% 수준, 크기 85% 수준, 무게 80% 수준 절감
- 주요 정보통신 기반시설 및 국가중앙행정기관 현장 실증을 통한 기술적 활용성 확보

시장성

- 공공/민간 영역에서 시장 규모가 크게 증가 예상
  - 사이버 침해 사례가 계속 증가하고 있음에 따라, 각 기관에서 보안 점검을 주기적 수행 필요
  - 보안 점검 시 네트워크 트래픽 점검 수행 필요
- 기술의 사업성 확보
  - 주요정보통신기반시설 및 국가중앙행정기관 수십여 기관 현장 실증 시 네트워크 접점 탐지, 비인가 인터넷 연결, 비인가 IP 탐지 등 동 기술의 성공적 활용
  - 네트워크 접점 탐지 등 트래픽 점검 서비스를 원하는 공공기관 다수 존재

기술 응용 분야

- 네트워크 트래픽 수집·점검을 통한 보안 점검
  - 제어시스템 및 정보시스템 네트워크 접점 탐지 및 비인가 인터넷 사용 점검
  - 비인가 장비 사용 점검
  - 비인가 서비스 사용 점검
  - 중요 문서 이동 등의 정보 유출 점검
  - 악성코드 전파 점검
  - 위험 제어 명령 전송 점검
  - 탐지 룰 기반 트래픽 점검

기술개발 완료시기

- 2017년 10월 완료

관련 특허 등 지식재산권

- (출원) 2017-0073928(2017. 6. 13. 대한민국) "네트워크 트래픽 관리 장치 및 방법"
- (출원) 2017-0076580(2017. 6. 16. 대한민국) "네트워크 트래픽 분석 장치 및 방법"