카니보어 시스템을 통한 이메일 감청

범죄 예방과 사생활 침해, 가부(可否)주장 팽배

김연수 | KISA연구원 개인정보침해신고센터
저서 고도지식정보사회의 개인정보보호와 CyberLaw
E-mail kimyonsu@kisa.or.kr

Ⅰ. 카니보어의 정의 및 주요기능

1. 카니보어의 유래

카니보어는 감청용 소프트웨어들을 내장한 개인용 컴퓨터 형태로 되어 있는 장비로서 인터넷을 통하여 수없이 오가는 전자우편들 가운데 특정 범죄혐의와 직접 관련된 핵심정보들만을 잡아낸다고 하여, 육식성 동물을 뜻하는 'Carnivore' 라는 이름으로 불린다.

2. 카니보어의 개념

카니보어는, 연방수사국이 범죄수사를 위한 이메일 감청용 시스템이다. 즉, '카니보어 시스템' (Carnivore System)은 인터넷 서비스 공급업체의 네트워크에 연결해 범죄 수사의 표적과 연결되는 모든 이메일 내용을 감청 할 수 있는 장치다. 원래는 상용 이메일 검색프로그램의 일종이었으나 연방수사국의 엔지니어들에 의하여 18개월간의 작업을 통해 기능을 추가하여 완성한 것이 카니보어다.

3. 카니보어 주요기능

카니보어는 2피트자리 검정색 컴퓨터이며 윈도우 NT 운용체계를 기반으로

하고 있다.

'카니보어'는 3개 프로그램을 축으로 한 '드래곤웨어스위트'(Dragon Ware Suite)라는 이름의 거대한 비밀 감청 프로그램의 한 부분으로서, 2000년 3월부터 전 세계 인터넷서비스제공업체(ISP)를 통해 흘러 다니는 이메일을 조사하기 위하여 활용되었다.

〈http://hani.co.kr/section-007000000/2000/007000000200010192222093.html 참조〉

미국 행정부는 현재 전화 통화에 적용되고 있는 프라이버시 보호장치들을 이메일 등과 같은 전자통신수단에까지 확대하는 것을 골자로 하는 감청 관련 법령들의 정보통신법을 의회에 제안중이다.

이 정보통신법은 특히 연방수사국이 범죄수사를 위한 이메일 감청에 동원하고 있는 '카니보어 시스템'의 사용에 영향을 미칠 것으로 보고 있고 카니보어를 사용한 이메일 감청을 위하여서는 해당 수사요원들이 법원의 명령을 신청하기 전에 법무부 고위급의 승인을 받도록 했으며 이의 사용을 제한하는 더욱 엄격한 기준도 적용될 것이라고 한다.

도널드 커 연방수사국 실험실부 부장은 새로 추진되고 있는 인터넷 감청 체제가 전자우편을 포함해 인터넷으로 송수신 되는 모든 형태의 디지털 파일은 물론, 인터넷 전화를 통해 오가는 음성 메시지까지 감청 할 수 있게 할 것이라고 밝혔다.

〈http://www.hanico.kr/section-007100000/2000 참조.〉

따라서 특정인이 다른 사람들과 주고받는 전자우편의 내용을 몰래 들여다보거나 따로 복사 · 저장해 두도록 할 수 있는 카니보어 체제의 기본기능은, 새로 추진되는 광범위한 인터넷 감청체제의 부분적인 기능이 될 것으로 예상된다.

연방수사국은 특히 전화선 등을 통한 기존 전화 서비스보다 저렴하기 때문에 갈수록 많은 사람들이 이용하고 있는 인터넷 전화에 대한 감청기능을 확보하는데 주력하고 있다.

그러나 인터넷 전화 서비스 기술이 아직 표준화돼 있지 않으므로, 완전한 감청기술 확보는 어려울 것이다.

Ⅱ. 카니보어 시스템 개발과정

연방수사국은 1996년 1월, 카니보어에 앞서 2개의 이메일 감청프로그램을 보유하고 있었다.

카니보어의 바로 전 단계의 감청 프로그램인 '옴니보어(Omnivore)'는 90만달러의 비용을 들여 '선 솔라리스' 시스템에서 운용되기 위하여 개발되었으며 이보다 앞 단계의 프로그램은 비밀로 분류되어 있어 실체파악이 어렵다.

옴니보어는 이메일의 흐름을 추적하고 표적이 된 이메일을 실시간으로 출력해 내면서 다른 한편으로는 8mm 테이프 드라이브에 다른 정보를 저장하는 기능을 수행하도록 고안되었다.

그러나 옴니보어 시스템은 카니보어 시스템과 달리 전자우편들에서 대규모의 정보들을 뽑아내긴 하지만, 수사목적에 들어맞는 핵심정보들을 제대로 분별해 내지 못하는 단점을 지니고 있었다.

1999년 2월에 입안된 옴니보어는 앞단계의 프로그램이 갖는 결함 때문에 당초 계획보다 앞당겨 그 해 10월부터 베터버전 상태로 실용화되었으며 그에 따라 여러 가지 기술적인 문제들을 야기함으로 1999년 6월에 공식적으로 퇴출되었다.

결국 '솔라리스' 운영시스템이 지지부진하자 FBI는 '옴니보어'를 윈도 NT에서 구현하기 위하여 기능개선을 추진하였고, 궁극적으로 '카니보어'를 개발했으며 이후 '카니보어 1.2', '고급 카니보어' 등이 개발되어 수사에 이용되었다.

'드래곤웨어스위트'(Dragon Ware Suite)

드래곤웨어스위트를 구성하고 있는 프로그램은 카니보어(Carnivore)를 비롯하여 패킷티어(Packeteer)와 쿨마이어(Coolminer) 등이 있는데 카니보어를 제외한 이들 프로그램은 카니보어에 의하여 초기단계에서 수집된 기본 정보들을 재구성해 내는 기능을 담당한다.

드래곤웨어수위트는 연방수사국의 감청대상자가 인터넷을 통하여 웹서핑을 하는 동안 검색한 웹페이지들을 정확하게 재구성해 낼 수 있는 기능을 갖추고 있다.

현재 사용중인 '고급 카니보어' 개발에는 65만달러가 소요됐으며 이 프로그램은 2001년 1월 새로운 버전으로 대체되었다.

연방수사국은 1999년 초부터 20여개의 카니보어 시스템을 도입하고, 그때그때 연방법원 판사의 허가를 얻어 이를 실제 수사활동에 활용하였다.

즉 연방수사국은 인터넷 서비스 제공업체들의 협조를 얻어, 필요한 경우 일정기간 동안 이들 업체의 전산 네트워크에 카니보어 시스템을 연결해 놓고 이를 통해 전자우편 감청을 실시해 온 것이다. 연방수사국은 한번에 평균 45일씩, 모두 100번 정도 이 시스템을 실제 사용하였다.

연방수사국은 2000년 초 전자사생활정보센터(EPIC)가 제기한 소송으로 인해 카니보어 관련 파일중에 약 600쪽 분량의 자료를 공개하였으나 공개자료 대부분이 검정색 칠로 뒤덮여 있어 제대로 정보를 파악해낼 수 없는 상태였다고 한다.

FBI는 인터넷을 통한 전화통화의 감청기능을 가진 소프트웨어인 '드래곤 넷'를 개발중이다.

III. 미국 행정부의 동향

미국 행정부는 현재 전화통화에 적용되고 있는 프라이버시 보호 장치들을 이메일 등과 같은 전자 통신수단에까지 확대하는 것을 골자로 하는 감청 관련 법령들의 정보통신법을 2000년 7월 17일에 의회에 제안하였다.

개정법 주요내용

수사요원들이 이메일의 내용을 감청하기 위하여 법원에 감청 명령을 신청할 때에는 전화통화 감청에 준하는 법무부 고위급의 승인을 받아야 한다.

수사요원들이 하나의 '함정추적(Trap and Trace)' 명령으로 여러 통신업체와 인터넷서비스공급업체를 통한 전화통화와 이메일의 발신자를 확인할 수 있도록 허용하지만 통신 내용의 감청은 허락하지 않은 법원의 명령이다.

컴퓨터가 공격을 받을 때와 같은 긴급한 경우 사전 승인없이 전화와 이메일 등을 추적할 수 있다.

연방판사나 주판사가 통신추적 명령 신청에 대하여 독립적으로 사실관계를 파악해 허용여부를 결정할 수 있다.

이러한 개정법의 주요내용은 특히 연방수사국이 범죄 수사를 위한 이메일 감청에 동원하고 있는 카니보어 시스템의 사용에 영향을 미치게 될 것이다.

IV. 미국연방수사국 및 사법당국의 반응

아무런 제한 없이 또 적합한 승인절차 없이 카니보어 시스템을 도입, 운영한 것은 사실이나 FBI 내부, 법무부 내부 및 카니보어를 비롯한 각종 감시 장비의 운용을 감독하는 당국, 나아가 의회의 엄격한 통제하에 카니보어 시스템을 운영하고 있다.

인터넷이 보편화 된지 얼마 되지는 않으나 범죄자들이 인터넷 기술을 광범위하게 악용하고 있기 때문에 정보화 시대의 범법 행위자를 추적하기 위한 기술이 필요하였다.

일반인의 사생활을 보호하여야 하므로 사이버 범죄에 대하여 미온적으로 대응한다면 사이버 공간을 범죄자들과 테러리스트들의 천국으로 방치하게 될 것이다.

그러나 FBI 요원들이 일반국민들을 감시하기 위하여 카니보어 시스템을 사용하지는 않는다.

카니보어에는 법적으로 도청되는 통신과 그렇지 않는 것을 구별하는 독자적인 기능을 부여하고 있다.

V. 미국 시민자유주의단체 및 사생활보호 옹호론자들의 반응

미국의 소비자 인권단체들은 카니보어에 의한 감청은 사생활침해라며 반발하고 있고, 연방 수사국의 감청장비 설치 요구를 수용할 수밖에 없었던 일부 인터넷서비스 제공업체들도 자사 고객들의 사생활 정보가 누출되는데 대하여 문제를 제기하고 있다.

미국 시민자유연명(ACLU)의 배리 스타인하트 공동대표는 "카니보어 시스템은 수사요원들에게 거의 무제한으로 통신내용에 접근할 수 있도록 허용함으로써 모든 미국인들의 프라이버시를 심각하게 위협하고 있다"면서 이 시스템의 사용을 즉각 중단할 것을 촉구하였다.