情 報 保 護 學 會 誌
第 13 券 第 5 號, 2003. 10

사이버범죄의 암호화된 증거 수집에 관한 연구

김 소 정*, 임 종 인*, 오 일 석**

요 약

현대는 인터넷과 컴퓨터 없이는 잠시도 운용될 수 없는 사회이지만 이를 불법적으로 이용한 범죄행위도 점차 증가하고 있다. 이들 컴퓨터 범죄는 익명성에 기반한 대담성을 보이고 있으며, 개인의 사회적 존재로써의 자각에 있어서도 탈개인화됨에 따라 더 많은 우려를 낳고 있다. 이에 따라 일반 컴퓨터 사용자들의 프라이버시 보호를 위한 방법으로 암호화 방법을 점점 더 많이 사용하고 있는데, 이에 비례해 범죄자들의 암호사용도 증가하고 있다. 그렇다면, 범죄자들이 암호를 사용해 자신들의 범죄증거를 숨기고 있는 경우, 이를 수사하기 위해 공권력 및 수사기관은 어떻게 해야 될 것인가? 본 논문은 이러한 문제제기를 통해 새로운 환경에 의해 변화된 코드를 활용하는 새로운 법제도를 통한 적극적인 대비방안을 모색해 보고자 한다.

KLS와 같은 신기술을 수사기관 및 법집행기관이 신중하게 사용하여 국가의 법 집행력과 프라이버시권이라는 두 가지 근본 가치의 균형을 이룰 수 있는 방안을 고려하여야 할 것이다. PRIVACY와 SECURITY라는 동전의 양면은 현실생활의 법제도를 그대로 옮겨놓는 것만으로는 한계가 있다. 현재 암호와 관련한 모든 논의는 공론화 되지 못하고 있다. 좀 더 공개적으로 암호를 사용한 범죄 행위에 대한 현황과 또 이를 대처한 수사기관의 수사 활동에 대해 논의하고, 그 과정에서 어떤 문제점들이 발생되고 있으며, 이들 문제를 해결하기 위해 필요한 조치들이 무엇인지에 대해 논의하고, 해외 각 국은 이 문제를 해결하기 위해 어떠한 노력들을 기울이고 있는지 살펴본 후 종합적인 안목으로 시의적절한 대책을 세우는 시발점이 되었으면 한다.

Ⅰ. 서 론

나날이 발전해 가는 기술력에 따라, 이젠 인터넷과 컴퓨터를 사용하지 않고는 어떤 일도 할 수 없는 세상이 되었다. 하지만 이를 불법적으로 이용한 범죄행위도 점차 증가하는 추세이다[1]. 이들 컴퓨터 범죄인들은 인터넷의 특징인 익명성에 기반한 대담성을 보이고 있으며, 개인의 사회적 존재로써의 자각에 있어 컴퓨터를 통해 개인을 탈개인화시킴으로써 점점 더 많은 범죄를 일으키고 있다. 이러한 상황에서 사용자의 프라이버시 보호를 위해 암호화에 의존하는 경우가 빈번해지고 있는데, 이는 또한 범죄자들이 자신의 정보를 암호화하는 빈도수도 높아지고 있다는 반증이 된다. 그렇다면, 범죄자들이 암호를 사용해 자신들의 범죄증거를 숨기고 있는 경우, 이를 수사하기 위해 공권력 및 수사기관은 어떻게 해야 될 것인가?

한편으론 진보된 기술을 활용한 많은 범죄행위들에 대해 수사기관 혹은 법집행기관이 기존의 법을 적용할 수 없는 경우가 왕왕 발생하고 있다. 하지만 다른 한편에선 수사기관 및 법집행 기관이 진보된 기술을 활용해 개인의 범죄행위에 대해 프라이버시권을 침해할 여지가 많은 수사 행위를 하고 있는 것도 현실이다. 말을 바꾸어 보면, 개인의 프라이버시와 자유권적 기본권이 법집행기관의 새롭고 진보된 기술을 활용한 수사 행위에 의해 침해받지 않으면서도 법집행 기관에게

1) Pricewaterhouse Coopers의 Global Security Survey에 따르면, 국제기업의 보안부서가 2000년에만 들인 비용이 1조 5천억 달러 이상이라고 한다. Pricewaterhouse Coopers, "Global Security Survey(2000)," www.pwcglobal.com/extweb/ncpressrelease.nsf/DocID/7ABBA8E73B1E901D8525693500548A34

* 고려대학교 정보보호대학원, 정보보호기술연구센터
** 한국전자통신연구원부설 국가보안기술연구소

는 적절한 접근권을 보장할 수 있는 법제도 및 원칙이 존재할 수 있을까라는 문제에 직면하게 되는 것이다.

이러한 현실을 감안해, 진일보한 기술을 활용한 수사기관의 법집행 시, 개인의 프라이버시를 침해하지 않으면서도 법집행 기관과 수사기관의 적법한 접근권을 보장할 수 있는 법제도에 관한 외국의 사례를 분석하는 것은 큰 의의를 가질 것이다. 왜냐하면 본고에서 분석해 보고자 하는 Scarfo 사건은 개인의 프라이버시와 자유권적 기본권을 위해 사용한 암호기술에 대해 수사기관 및 법집행기관의 적법한 수사권을 보장하기 위해 최신기술인 키로그시스템(KLS : Key Logger System)을 활용한 수사 행위를 다루고 있기 때문에, 향후 컴퓨터 범죄 및 개인의 정보보호 등에 관해 많은 시사점을 던져주고 있기 때문이다. 이를 분석함으로써, 우리에게도 발생할 수 있는 문제에 대해 법제도적인 측면에서 미리 고찰해볼 수 있는 계기를 마련하고자 한다.

Ⅱ장에서는 KLS 기술에 대한 일반적으로 소개하고자 한다. 이 장에서는 소프트웨어와 하드웨어에 기반한 각 KLS의 종류 및 특징, 설치방법, 동작 원리 등에 대해 알아보고자 한다.

Ⅲ장에서는 KLS가 직접 사용된 Scarfo 판례를 분석하고자 한다. 범죄와 이에 따른 수사행위를 간략히 살펴보고, FBI의 KLS에 대한 진술서와 opinion letter를 중심으로 쌍방간의 쟁점이 무엇이었으며, 그 쟁점에 대해 각 당사자들은 어떤 의견과 근거를 주장했는지, 이에 따른 판결내용은 무엇인지 살펴보고자 한다.

끝으로 결론부분에서는 Scarfo 판례가 가져다 주는 시사점과 사회 전반에 걸쳐 제기되고 있는 프라이버시권 보호와 수사기관 혹은 법집행기관의 적법한 수사권 보장이라는 큰 주제에 대해 고찰해 보고자 한다.

Ⅱ. Key Logger System

1. 정의 및 소개

키로거는 컴퓨터를 켬과 동시에 실행되어 모든 키보드 자판을 기억하여, 일정 위치에 저장시키는 프로그램(시스템)이다. 이 프로그램을 정보를 캐내야 하는 컴퓨터에 에이전트처럼 심었다가, 키로그 된 기록을 빼냄으로써 필요한 각종 비밀정보와 중요한 사항들을 뽑아 낼 수 있다. 이 프로그램의 특징 중의 하나는 시스템의 실행 여부가 task bar에 보이지 않아 눈에 쉽게 띄지 않는다는 점이다.

〔표 1〕 Software 키로거 시스템

	프로그램명	실행 파일명	사용O/S	참고사이트 (다운로드가능)
1	Winwhat where	w3i4.exe	Windows계열	http://www.winwhatwhere.com
2	Invisible KeyLogger Stealth (IKS)	iks2k21d.exe	Win2000WinXP	http://www.keylogger.com
3		iksv12d.exe	Win95/98/ME	
4		iksnt10d.exe	WinNT4	
5	백오리피스	bo2kgui.exe	Windows계열	

2. 종 류

KLS는 크게 Software에 기반한 KLS와 Hardware에 기반한 KLS로 나뉜다. 그리고, 사용 O/S에 따라 MS Windows계열과 그 밖의 O/S계열로 나뉜다.

2.1 Software KLS

공개적으로 소개된 여러 가지 소프트웨어가 있는데, 그 중에 가장 기능과 성능이 검증된 것으로는 Winwhatwhere, IKS, 백오리피스 등이며, 주요 프로그램들을 정리하면 〔표 1〕과 같다.

2.2. Hardware KLS

하드웨어적으로 설치하는 KLS는 비교적 쉽게 설치할 수 있다. 하드웨어로 된 KLS를 컴퓨터 본체와 키보드 사이에 끼워 주기만 하면 되기 때문이다. 하드웨어에 설치하므로, O/S를 가리지 않고 모든 시스템(Windows XP, 2000, ME, NT, 98, 95, 3.1, Linux, Solaris, DOS, OS/2 and BeOS)에서 동작한다. 그리고 백신에서도 점검이 불가능하다.

3. 동작원리

일반적으로 KLS를 사용하여 정보를 수집하고 수사하는 과정을 알아보도록 하겠다. 우선 정보 수집 대상이 되는 자를 A로 놓고, 키를 확인하려는 자를 B로 설정하도록 한다. 정보수집의 방법을 간략히 정리하면 아래와 같다.

```
정보 수집 대상(A) 선정
  → 정보 수집 대상의 컴퓨터에 KLS 설치
    * 직접 대상 컴퓨터에 KLS 설치
    * 원격으로 접속하여 대상 컴퓨터에 KLS 설치
    * 대상 컴퓨터에 plug-in 형태로 접근하여 KLS 설치
  → 필요 정보 수집(확인)
    * A의 컴퓨터에서 직접 확인
    * 지정된 메일 등을 통해 확인
  → 수사에 증거로써 활용
```

〔표 2〕 KLS의 설치 방법

	방법1	방법2	방법3
설치	A 시스템에 접근, 직접 설치 (디스켓 및 저장매체)	A의 시스템에 웹을 통하여 접근, 설치 (E-mail)	A의 시스템에 plug-in의 형태로 접근, 설치 (인터넷 뱅킹 보안 모듈 다운로드식)
동작	시스템의 특정폴더에 키 정보가 파일 형태로 저장.	방법1과 같이 동작함	방법 1과 같이 동작하고, 전송 기능 포함됨.
확인	A의 시스템에서 직접확인가능.	A의 시스템에서 직접확인가능. 혹은, 메일로의 전송도 가능함.	A의 시스템에서 직접확인가능. 지정된 메일로의 전송이 가능.
비고	직접 접근하여 설치	직접 설치가 불가능할 경우 사용함. 단, 사용자가 눈치 챌 수 있음.	직접 접근한 설치가 불가능할 경우 사용, 바이러스의 전파 방법과 유사함.

이를 각 설치 방법 및 필요 정보 수집(확인) 절차 방법으로 대별해 정리하면 〔표 2〕와 같다.

4. 키로거 시스템 실행 여부의 확인

키로거 시스템의 설치 전과 설치 후에 컴퓨터에 변화된 내용은 〔그림 1〕에서 알 수 있듯이, Windows 작업관리자 화면[2]의 프로세스 중에 namebin.EXE (빨간 네모 안)가 생겼다. 따라서 이것으로부터 키로거 시스템이 작동하고 있음을 알 수 있다. 시스템 트레이에 생기지 않았다고 안전한 것이 아니므로 꼭 확인해 보아야 한다.

Ⅲ. 판례분석 : US vs. Scarfo

1. 배경

1999년 1월 15일 수색 영장을 발부 받은 FBI가 불법도박 및 고리대금업의 혐의에 관한 증거를 수집하기 위해서 Essex County에 있는 피고인 Nicodemo S. Scarfo와 Frank Paolercio의 사무실(Merchant

〔그림 1〕 설치후의 프로세스

Services)을 수색했다. FBI가 Merchant Services 사무실을 수색하는 동안 개인용 컴퓨터를 발견하고 컴퓨터 속에 있는 다양한 파일들에 접근을 시도했다. 그 와중에 "Factors."라는 암호화된 파일을 발견했으나 이 파일에는 접근하지 못했다.

수사 도중에 접근하지 못했던 "Factors."라는 파일 속에 불법도박 및 고리대금에 관한 증거가 포함되어 있을 것이라고 판단하고 철수한 FBI는 다시 영장을 발부 받았다. 새로이 발부 받은 영장에는 KLS(Key Logger System)라고 알려진 시스템을 컴퓨터나 키보드에 설치해 암호화된 파일의 비밀번호(passphrase)를 알아낼 수 있도록 하는 내용이 첨가되었다. 이를 통해 암호화된 파일에 접근해 필요한 정보를 획득하고자 하였다.

KLS는 개인용 컴퓨터의 키보드를 통해 개인이 치는 모든 keystroke을 기록한다. 하지만 미정부가 Scarfo의 컴퓨터에 설치한 KLS는 컴퓨터의 모든 모뎀통신을 점검해, 컴퓨터가 모뎀통신을 하고 있을 때에는 keystroke을 기록하지 않고, 모뎀통신을 하고 있지 않는 경우에만 keystroke을 기록하도록 고안된 시스템이었다. 미 정부는 KLS를 통해 Scarfo가 그의 개인용 컴퓨터의 키보드를 통해 암호를 치는 순간 그 passphrase를 알아내고자 했다. FBI는 암호화된 "Factors."라는 파일의 passphrase를 획득하고 이를 통해 유죄 증거라고 추정되는 자료들을 찾아냈다[3].

2) Windows 작업관리자 : 현재 시스템에서 사용중인 프로세스 정보 및 CPU, RAM 사용량 등을 보여주는 윈도우 메뉴로 〈Ctrl〉+〈Alt〉+〈Del〉를 누르면 작업관리자가 나오고 확인 가능하다(단 윈도우 NT 버전이상에서만 사용 가능함).

3) 이는 FBI가 제출한 진술서를 통해 확인할 수 있다. 진술

2000년 6월 21일, 연방 대배심은 피고인들(Scarfo, Paolercio)을 도박과 고리대금업의 혐의로 기소했다. Scarfo는 자신의 컴퓨터에서 발견된 증거의 개시 및 중지신청을 했다. 2001년 7월 30일 열린 구두심문 후, 법원은 당사자들의 브리핑이 더 필요하다고 결정했다. 2001년 8월 7일, Letter Opinion and Order에서 법원은 정부가 KLS를 Scarfo의 컴퓨터에 사용하는데 있어 도청법을 위반했는지에 대해 심각히 고려하기 시작했다. 특히, 법원은 Scarfo(혹은 그의 컴퓨터를 사용한 다른 사용자)가 전화선을 통한 모뎀을 이용해 통신을 하고 있는 동안 KLS가 작동되었는지의 여부에 관해 우려를 표명했다. 왜냐하면, Scarfo를 포함한 컴퓨터의 사용자가 통신하고 있는 동안 KLS가 작동되었다면 이는 불법적으로 통신에 대한 도청행위를 한 것이 되기 때문이다.

이러한 우려를 불식시키기 위해, 2001년 8월 7일 법원은 미정부에 KLS가 어떻게 운용되며 그 기술이 어떤 특성을 가지는지에 대해 자세한 설명을 요청했고, 특히 컴퓨터 모뎀을 통한 인터넷 통신이나 e-mail 사용을 포함한 모든 컴퓨터의 사용시 KLS가 어떻게 작동하는지에 대해 보고하라고 요청했다. 그러나 미 정부는 KLS 기술에 대한 설명이 공개되었을 때 유발될 수 있는 국가안보 위협을 표명했고, 이에 법원은 미정부에 KLS에 대한 자료의 공개가 현재 혹은 미래의 미국내 형사범죄의 수사와 국가안보에 위협이 되는지에 관한 설명자료를 제출하도록 했다.

미정부는 법원이 2001년 8월 7일 발표한 Letter Opinion and Order의 내용을 수정하여 CIPA[4]가 정한 절차를 따를 것을 요구했다.

Scarfo의 반대에 따라 미정부는 FBI의 부국장인 Neil J. Gallagher의 선서진술서(affidavit[5])를 2001년 9월 6일 제출했다. 제출된 선서진술서에서 Mr. Gallagher는 KLS의 특징 및 기능에 관한 내용은 1997년에 이미 비밀로 분류되었다고 진술했다.

법원은 2001년 9월 7일 2차 구두변론(oral argument)을 갖고 정부가 KLS를 비밀로 분류할 수 있는지에 대한 CIPA의 적용가능성을 논의했다. 비록 피고인측은 KLS가 CIPA에 의해 비밀로 분류되는 것은 인정했지만, 법원은 그 결정을 유보한 채, 미정부에 서면으로 그 내용을 제출할 것을 명령했다. 미정부는 제출된 내용의 검토를 위해서 ex parte[6]와 in camera[7]를 요청했다.

2001년 9월 26일 법원은 미 검찰청과 FBI의 고위 관리와 함께 in camera, ex parte로 심리를 진행했다. 왜냐하면 제시된 문제가 워낙에 민감한 내용이므로 CIPA에 규정된 모든 조문들을 따라야 했고, 이를 따라 비밀취급 인가자들만이 심리에 참석할 수 있었기 때문이다. CIPA 규정을 따라, 미정부는 법원에 KLS에 대한 세부사항 및 비밀사항을 제출하고, 특히 모뎀과 연결되어서 어떻게 작동하는지도 설명했다. 정부측은 또한 KLS가 어떤 방식으로 국가안보에 위협이 될 수 있는지에 대해서도 구체적으로 설명했다.

제출된 문건들을 자세히 검토한 결과, 법원은 미정부가 상기의 내용들에 대한 충분한 근거를 제시했다고 판단, 2001년 10월 2일에 Protective Order[8]를 냈다. Protective Order는 또한 피고인에게 KLS에 대한 전체적인 내용이 아닌 요약본만 제공할 수 있도록 하여, Scarfo에게는 전체내용에 대해 알려주지 않고 요약본의 내용만 알려주도록 했다. 또한 법원은 CIPA 조항에 따라 ex parte, in camera로 열린 심리 및 이때 제출된 정부의 선서진술서(affidavit) 또한 공개를 금지했다. 정부는 2001년 10월 5일, 법

서에 따르면, FBI가 Scarfo의 컴퓨터에 설치한 KLS는 설치되어 있음을 사용자가 확인할 수 없게끔 숨겨져 있으며, 디폴트로 전자통신을 하는 동안에는 기록되지 않도록 각 개별 key stroke을 식별하게 되어 있다고 한다. 특히 창을 여러 개 띄운 채로, 개별적인 작업을 하는 중에 비밀번호를 친다 할지라도 이미 통신이 되고 있는 상황에서는 key stroke을 기록하지 않도록 설계되어 있다. 또한 전송중인 데이터나 파일을 조사하거나 찾는 등의 행위도 불가능하게 설계되어 있다.
Affidavit of Randall S. Murch,
http://www.epic.org/crypto/scarfo.html참고.

4) *Classified Information Procedures Act*, Title 18, United States Code, Appendix Ⅲ, §1 et seq.

5) 법정 외에서 자발적으로 진술자가 알고 있는 사실을 기재한 진술서로서 그 진술자가 선서를 시키는 권한을 가진 직원 앞에서 선서 또는 확약을 하고 그 내용이 진실한 것임을 확인한 것. 이상도, 법률영한사전, 청림출판, 2002년 개정판, p. 25.

6) 사법절차, 재판, 유지명령 등이 일당사자만의 신청에 의하여 반대의 이해관계를 가지는 자에게 통고함이 없이 이루어진 경우에 이를 ex parte이라고 한다. 이상도, 법률영한사전, 청림출판, 2002년 개정판, p. 210.

7) 법관의 사실(私室)에서 또는 모든 방청자를 퇴정시키고 법정에서 사건을 심리하는 것으로 특별히 필요한 경우에 허용된다. Ibid., p. 278.

8) A court order prohibiting or restricting a party from engaging in conduct (esp. a legal procedure such as discovery) that unduly annoys or burdens the opposing party or a third-party witness.
Bryan A. Garner, ed., Black's Law Dictionary, 2nd pocket edition, WEST group, 2001, p. 567.

원에 요약본을 제출했으며, 이 내용이 Scarfo측에 전달되었다[9].

이러한 과정을 거쳐 법원은 피고인인 Scarfo 측이 주장한 증거의 개시 및 중지 신청에 대해, 증거의 개시는 부분적으로 인정 부분적으로 기각하고, 중지신청은 기각했다.

2. 쟁 점

피고인측은 증거의 개시 및 중지신청을 위해 이의를 제기했고, 이에 대한 공방 및 결정이 전체 사건의 판결 방향을 결정하게 되었다. 이를 좀 더 세분하여 살펴보도록 하겠다.

2.1 영장주의

컴퓨터 파일에 관한 압수·수색시에는 영장주의가 기본원칙이다. 미국의 경우 수정헌법제4조[10]에 의해 법집행기관은 상당한 이유(probable cause)를 제시하고 수색할 장소와 체포될 사람, 압수할 물품 등을 기재한 영장에 의해서만 압수·수색을 행할 수 있다.

그러나 환경의 변화에 따른 기술의 진보는 재래적인 방법과는 다른 수사방법을 필요로 하고 있다. 컴퓨터 파일은 다양한 방법으로 저장되어 있고, 암호화 등의 방법을 사용해 저장되어 있을 수도 있다. 이러한 불확실성으로 인해 수사관은 영장 청구 시 상당한 이유를 제시하기 곤란하고, 조사대상 파일을 명확히 설명할 수 없는 어려움 등에 직면하게 된다.

본 논문에서 분석하고 있는 Scarfo 사건의 경우, Scarfo 측은 정부가 암호화된 파일에 대해서만 그 passphrase와 관련된 keystrokes을 기록해야 하는데, 불필요한 자료들까지 모두 입수했으므로 정부가 발부하고 집행한 일반영장은 적법하지 않다고 주장했다.

일반적으로 증거의 사용중지 신청이 받아들여지기 위해서는 수사기관의 수사행위가 수정헌법제4조가 보장하는 권리를 침해한 경우여야 하는데, 이번 사건의 경우에 있어서는 그 근거가 없다고 판단되었다.

우선 Scarfo의 사무실을 수색하도록 했던 수색영장은 구체적으로 어떤 장소(Scarfo의 사무실)을 언제(1999년 5월 8일) 수색할 것인지에 대해 명확히 언급하고 있으며, 이는 Scarfo가 명확하게 불법도박 및 고리대금업을 하고 있다고 믿을만한 충분한 근거(probable cause)가 있었기 때문이다.

하지만 수색을 하는 동안 암호화되어 있는 파일을 발견했고, 이는 현대 수사기관이 새로운 기술을 도입하지 않고서는 그 내용을 볼 수 없었기 때문에, 다시 한번 영장에서 Scarfo의 컴퓨터에 적당한 소프트웨어나 펌웨어를 남겨 Scarfo가 타이핑하는 내용을 획득해, FBI가 관련된 자료에 접근할 수 있는 방법을 사용할 수 있도록 했던 것이다[11]. 또한 그 Order는 FBI가 수색할 수 있는 모든 서류 및 내용들을 구체적으로 명기하고 있어 Scarfo의 불법도박과 고리대금업에 관한 모든 정보를 수색할 수 있는 근거를 마련해 놓고 있다[12]. 따라서 피고측의 영장에 대한 이의는 기각되었다.

2.2 비밀로 분류된 정보의 공개 요구

두 번째 논점에 관해 Scarfo 측은 Jencks vs. United States[13]를 인용하고 있다. Jencks Argument 논쟁에서 당사자들 중 한쪽이 진술한 내용을 상대방이 모르는 경우, 심리에서 대질심문 등을 위해 그

9) Affidavit of Randall S. Murch, http://www.epic.org/crypto/scarfo.html

10) 미국의 수정헌법 제4조는 다음과 같다 : The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

11) 이에 관해 Judge Haneke의 1999년 5월 8일 Order에서는 다음과 같이 설명하고 있다. : Because the encrypted file could not be accessed via traditional investigative means, Judge Haneke's Order permitted law enforcement officers to "install and leave behind software, firmware, and/or hardware equipment which will monitor the inputted data entered on Nicodemo S. Scarfo's computer in the TARGET LOCATION so that the FBI can capture the password necessary to decrypt computer files by recording the key related information as they are entered." Judge Heneke, May 8, 1999 Order, p.4. http://www.epic.org/crypto/scarfo.html의 opinion letter 참고.

12) Judge Heneke, May 8, 1999 Order, p. 4-5. http://www.epic.org/crypto/scarfo.html의 opinion letter 참고.

13) 353 U.S. 657, 77 S.Ct. 1007, 1 L.Ed.2d 1103 (1957)

자료의 공개를 요구하는 것으로 Scarfo의 경우에는 해당되지 않는다.

왜냐하면, 원고측인 미정부가 내놓은 선서진술서의 경우(ex parte 및 in camera로 진행된 심리)는 사건 그 자체에 관한 것이었다기 보다는 KLS의 기술적인 면과 국가안보에 미치는 영향에 대해 논의한 것이기 때문에 Scarfo의 주장은 기각되었다. 또한 피고측이 간과한 점이 있다면 KLS와 관련된 부분은 CIPA의 규정에 따라 법원이 심리 진행중의 모든 정보를 공개해야 한다는 원칙의 예외조항에 해당한다는 점이다.

이번 사건에서 KLS시스템을 사용하기 위해 적용한 CIPA는 1980년 10월 15일에 이미 적용되기 시작했다. 동법은 국가안보상 중요한 기술들에 대해 형사소송 상의 사전심리, 심리에 있어서 비밀로 인가된 내용을 취급할 때는 민감한 내용의 공개를 금지하고 있다.

이에 따라 법원은 ex parte, in camera로 심리를 진행했으며, 그 결과에 대해 원고측에 요약된 내용을 피고측에 전달하도록 했다. 이는 CIPA가 인정한 정보 공개의 예외사항에 KLS에 대한 내용이 포함됨을 인정하는 것이며, 따라서 비공개 대상인 KLS에 대한 심리 및 의문점 해결을 비공개로 진행한 것이다. 따라서 피고측이 주장하는 KLS에 대한 내용의 공개는 기각되었다.

2.3 KLS의 사용과 미국의 도청관련법

이번 사건에서 가장 쟁점이 되는 부분은 Scarfo의 컴퓨터에 설치된 KLS에 의해 일반적인 통신내용이 도청되었는지의 여부이다. Scarfo의 컴퓨터는 모뎀을 통해 통신을 하고 있었고 이 경우 일어난 모든 전자통신은 미국의 도청법에 의해 보호받고 있어 적법절차에 따른 영장이 없이는 도청될 수 없는 부분이기 때문이다.

미국의 경우 법집행기관의 전통적인 전화 도청이나 현대적인 전자적 수단을 통한 전자적 감시를 합법화하는 근거로는 Pen/Trap Statute, Electronic Communication Privacy Act, Wiretap Act(Title III) 등이 있다. 예를 들어, United States v. Maxwell 사건[14]에서는 e-mail 사용자들은 서비스 제공자의 서버에 저장된 e-mail의 프라이버시에 대해 합리적인 기대를 가질 수 있다고 판시하고 있다. 즉, 영장에 의거하지 않고 통신 내용을 공개하는 것은 수정헌법제4조에 위반하는 행위로 해석될 수 있다. 왜냐하면 e-mail에 대해서는 개인의 아이디와 비밀번호 등이 다른 사람의 접근 위험을 감소시키므로 프라이버시에 대한 합리적인 기대를 갖는 것이 타당하다는 논리이다.

미국의 경우는 정보의 종류를 기본가입자 정보(basic information), 고객이나 가입자에 속하는 기록이나 다른 정보(records), 그리고 실내용(contents)로 구분해 이에 따른 수사 원칙을 개별적으로 설립해 놓고 있다.

ECPA는 ISP 사업자와 같은 네트워크 서비스 제공자가 저장하고 있는 사용자의 계정정보를 국가기관이 취득하는 경우에 대해 규제한다. 서비스 제공자의 고객이나 가입자를 위하여 법령상의 프라이버시권을 규정함으로써, 수사기관은 네트워크 서비스 제공자가 저장하고 있는 e-mail, 계정기록 또는 가입자 정보를 취득하고자 할 때마다 동 ECPA의 규정을 준수해야 한다.

Wiretap Statute(Title Ⅲ)는 국가기관이 전송중인 유선 및 전자(wire and electronic)통신의 내용을 수집하는 것을 규제하는 것을 목적으로 한다. 이와는 다르게 Pen/Trap Statute는 통신에 관련된 주소정보와 기타 내용이 아닌 정보에 실시간으로 접근하는 것을 규제하는 것을 목적으로 한다. 따라서 본 사건에서 논의되는 도청과 관련해서는 우선 Wiretap Statute에 근거해 분석해 보아야 할 것이다.

Title Ⅲ는 법에서 명시한 예외를 제외하고는 제3자가 전자적 혹은 기타 장치를 이용한 대화자 상호간의 통신내용을 도청하지 못하도록 명시하고 있다[15]. 특히 동법은 미국 전역에서 이루어지는 도청을 광범위하게 금지하고 있어 특정 사항이나 장소를 규제하는 기타 프라이버시 법률과는 차별성을 가진다.

Title Ⅲ에서 허용하는 감청은 1) 18 U.S.C. §2518의 법원명령에 의해 허용되는 감청, 2) 통신당사자의 동의에 의한 감청, 3) 서비스 제공자의 권리 또는 재산을 보호하기 위한 감청, 4) 컴퓨터 불법침입자에 대한 감청, 5) 구내전화의 감청, 6) 우연히 취득한 범죄증거의 경우 허용되는 감청, 7) 공공에게 접근 가능한 경우 허용되는 감청 등으로 명백히 한정되어 있다.

하지만 본 사건의 경우 감청인지 아닌지의 여부는 실질적으로 passphrase를 알아내는 KLS가 작동하는 동안에 컴퓨터 통신에 대한 도청행위가 일어났는지 아닌지가 논란이 되었으므로 이점에 초점을 맞춰서 고려해 보자.

법원이 ex parte, in camera로 진행된 심리에서

14) 42 M. J. 568 (A. F. Ct. Crim. App. 1995)

15) 18 U.S.C. §2511(1)

자세히 검토한 결과, KLS가 암호화된 파일의 passphrase를 찾는 동안에는 통신에 대한 어떠한 도청행위도 일어나지 않았다고 확신했다. 왜냐하면 KLS는 모뎀을 통해 통신이 일어나고 있을 때는 작동하지 않았기 때문이다.

Scarfo는 PGP(Pretty Good Privacy)라는 암호프로그램을 사용하고 있었는데 이 프로그램을 통해 암호화된 내용을 읽기 위해서는 적절한 passphrase가 필요하다[16]. PGP 프로그램을 사용한 경우 암호화된 파일에 접근하고자 할 때 passphrase를 치도록 유도하는 창이 뜨고 거기에 passphrase를 넣은 경우에만 암호화된 파일이 열리도록 되어 있다. 따라서 KLS를 활용해 사용자가 passphrase를 타이핑한 기록을 얻음으로써 특정 passphrase를 알아내려고 한다.

KLS는 FBI 기술팀에 의해 개발되었고, 오직 key 및 key와 관련된 정보만을 수집하도록 고안되었다. 즉, FBI가 설치한 KLS는 Scarfo의 컴퓨터 내의 다른 데이터나 부가정보를 수집하지 않도록 고안되었고, 오직 특정 파일(여기서는 "Factors."라는 암호화된 파일)에 대한 passphrase 만을 획득하기 위해 작동되었다. 물론 Scarfo의 컴퓨터는 파일 검색 등의 단순 문서작업과 모뎀 통신 등의 목적으로 동시에 사용되고 있기 때문에, FBI는 각 keystroke을 개별적으로 식별해 모뎀통신이 일어나지 않는 동안에만 keystroke을 기록하고, 이렇게 기록된 정보 중에서 필요한 정보만을 추출하도록 설치되었다.

이것이 가능한 이유는 Scarfo의 컴퓨터에 설치된 KLS가 모든 통신 port를 검색할 수 있어, 어떤 통신 port라도 사용되고 있는 순간에는(모뎀을 이용한 통신을 하고 있는 상황이므로), 이 때 행해지는 keystroke에 대해서는 기록하지 않고, 다만 모든 통신 port를 점검해 봤을 때, 어느 port도 사용되고 있지 않음을 확신하면(즉, 모뎀 통신을 하고 있지 않음을 확신하면) keystroke을 기록하도록 고안해, 원하는 passphrase를 획득하도록 했기 때문이다. 따라서 KLS가 Scarfo의 개인 전자통신을 도청함으로써 도청법을 위반했다는 피고측의 주장은 기각되었다.

3. 판 결

피고측이 신청한 증거의 개시는 부분적으로는 승인되었고, 부분적으로 기각되었다. 특히 법원은 피고가 요청했던 비밀로 분류된 정보의 공개(KLS에 대한내용)는 기각했으나 그 정보에 대한 요약정보를 볼 수 있도록 명령했다(이는 Murch Affidavit의 형태로 제출되었다[17]). 또한 피고측의 증거중지 신청(motion to suppress evidence)은 기각되었다.

Ⅳ. 결 론

지금 우리가 맞고 있는 21세기는 지식정보사회로 일찍이 모두가 경험하지 못했던 미지의 세계이다. 사회를 유지하는데 필수적인 기간산업인 금융, 에너지, 교통 등은 물론이고 국방 분야까지 급속히 정보화되고 있어 효율성은 크게 높아지고 있다. 하지만 지난 1월 25일 일어난 인터넷 대란이 보여주듯, 잘 갖춰진 기간망을 통한 피해의 확산속도도 걷잡을 수 없이 빨라진 것이 현실이다. 더군다나 나날이 발전하는 기술들이 범죄와 연계될 때는 미증유의 곤란과 낭패가 발생할 것이다.

기술은 눈부시게 발전하는데, 정책은 그것보다 최소 3년 이상 뒤쳐지고, 법제도는 그 기술의 발전보다 5년 이상 뒤쳐진다는 것이 일반 통설이다. 이는 신기

16) PGP(Pretty Good Privacy)는 공개키 암호시스템에 기반하고 있다. 암호 시스템은 고전적 암호시스템과 공개키 암호 시스템으로 대별할 수 있는데, 고전적 암호 시스템은 송신자와 수신자만이 알고 있는 동일한 대칭키를 이용하여 메시지를 암호화하는 방법이다. 이 암호 시스템을 사용하는 경우, 송신자와 수신자 간에 키의 사전분배(key predistribution)가 선행되어야 한다. 이는 현실세계에서 적용하기 어려운 경우가 많다.
이와 반대로, 공개키 시스템은 서로 연관이 있는 상이한 두 개의 키를 각각 암호화와 복호화에 이용하는 것이다. 즉, 송신자가 메시지를 암호화하여 수신자에게로 보내기 위해서는 먼저 공개키 디렉토리 등을 통해서 공개된 수신자의 공개키를 이용하여 암호화를 수행하고 수신자는 자신만이 알고 있는 개인키를 이용하여 복호화를 수행하는 개념이다. 모든 사용자는 자기만의 한 쌍의 공개키와 개인키를 가지며 공개키는 자기에게 메시지를 암호화하여 보내고자 하는 모든 사용자들에게 등기 우편, 온라인 또는 오프라인 공개키 서버, 공개키 인증서와 같은 안전한 공개키 분배 채널을 통해서 분배하는 것이다. 물론, 공개된 공개키로부터 복호화에 사용될 개인키를 도출하는 것은 계산적으로 불가능해야 한다는 제약조건이 따른다. 이러한 개념은 키의 사전 분배문제를 자연스럽게 해결했고, 디지털 서명과 같은 새로운 개념의 출현을 가능하게 했다.
공개키에 대해 자세히 알고 싶으면, 이만영 · 원동호 · 이민섭 · 송주석 · 임종인 · 박춘식 공저, 현대 암호학 및 응용, 생능출판사, 2002. pp. 153 - 193 참고.

17) Affidavit of Randall S. Murch, http://www.epic.org/crypto/scarfo.html

술과 접목된 범죄를 수사하는데 있어서도 예외는 아니다.

일반적인 컴퓨터 사용자들에게 있어서 신기술을 사용하여 범죄를 저지르는 측이나 그 신기술을 사용하여 수사 및 감시를 하는 측은 모두가 적(?)임에 틀림없다.

본 논문에서 살펴본 Scarfo의 경우처럼, 일면으로 가장 사적인 내용일 수도 있는 것을 보호하기 위해 암호기법을 사용했으나, 적법한 영장의 발부여부를 떠나, 사용자가 알지도 못하는 사이에 그 passphrase 등의 유출이 이루어질 수 있는 것이 현실임을 감안한다면, 일반 사용자, 수사기관 그리고 법 집행기관을 위해서 적절한 관련 법제도의 입법이 절실하다.

또한 해당 포트의 사용자가 접속하는 모든 서비스의 아이디와 비밀번호를 실시간으로 찾아주는 프로그램을 온라인상에서 손쉽게 구할 수 있고, 이 프로그램은 본 논문의 KLS와는 달리, 사용자의 컴퓨터가 아닌 감시자의 컴퓨터에 설치되므로 인식하지 못한 감시의 가능성이 극대화되고 있는 실정이다[18].

특히 이번 판례에서는 우리나라의 헌법제12조[19]가 보장하고 있는 기본권, 그리고 미국의 수정헌법 제4조 및 5조[20]가 보장하는 있는 기본권을 침해할 우려가 있기 때문에 더욱 더 그 중요성을 더한다. 예를 들어, Doe v. United States[21] 판결에서는 대법원이 비밀서류가 담긴 박스의 열쇠를 수사기관에 넘겨줘야 하지만, 그 열쇠가 만약 물리적인 것이 아니라 개인이 고유하게 알고 있는 내용일 경우 수정헌법 제5조의 내용에 따라 어떤 형태든 그 내용을 알려줄 필요가 없다는 판결을 내렸다. 하지만 Scarfo의 경우에서는 그 내용을 직접 피고인이 알려주지 않아도 수사기관의 노력으로 그 passphrase를 알아내게 되었으므로 우리에게 시사하는 바가 크다고 할 수 있다.

시각을 달리해, 수사기관 및 법집행 기관의 입장에서 보면 본 판례는 범법자의 암호사용으로 인한 수사기관의 법 집행력 약화에 대한 우려를 어느 정도 불식시켜주는 판결이다. 다만 앞서도 언급했던 것처럼, 이것이 일반인의 암호사용 위축과 프라이버시 침해가능성으로 이어진다면 OECD 암호정책 가이드라인 등 국제 조류에도 위배되는 것이다[22].

따라서 KLS와 같은 신기술을 수사기관 및 법집행기관이 신중하게 사용하여 국가의 법 집행력과 프라이버시권이라는 두 가지 근본 가치의 균형을 이룰 수 있는 방안을 고려하여야 할 것이다.

예를 들어, 호주에서 발간된 The Walsh Report[23]는 전자거래 등의 신뢰성과 프라이버시를 보호하기 위한 목적으로 사용되는 암호가 범죄의 목적으로도 사용될 수 있다는 것을 언급한 Wassenaar협정[24]의 암

18) ettercap이라는 프로그램이며, 이 프로그램은 아래 홈페이지에서 다운로드가 가능하다.
ettercap.sourceforge.net

19) 우리나라 헌법제12조는 다음과 같다. ①모든 국민은 신체의 자유를 가진다. 누구든지 법률에 의하지 아니하고는 체포·구속·압수·수색 EH는 심문을 받지 아니하며, 법률과 적법한 절차에 의하지 아니하고는 처벌·보안처분 또는 강제노역을 받지 아니한다. ②모든 국민은 고문을 받지 아니하며, 형사상 자기에게 불리한 진술을 강요당하지 아니한다. ③체포·구속·압수 또는 수색을 할 때에는 적법한 절차에 따라 검사의 신청에 의하여 법관이 발부한 영장을 제시하여야 한다. 다만, 현행범인인 경우와 장기 3년이상의 형에 해당하는 죄를 범하고 도피 또는 증거인멸의 염려가 있을 때에는 사후에 영장을 청구할 수 있다.(4항부터 7항까지는 생략)

20) 미국의 수정헌법 제5조는 다음과 같다 :
No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

21) 487 U.S. 201(1988)

22) OECD는 정보통신 인프라, 네트워크와 시스템 및 이들의 사용에 관한 신뢰성(confidence)을 조장하기 위해, 국가 및 범세계적 정보통신 인프라, 네트워크와 시스템에서 데이터의 보안성을 보장하고 프라이버시를 보호하기 위해 암호사용을 권장하고 있다. 그러나 이러한 암호사용의 권장은 부당하게 공공의 안녕, 법집행 및 국가의 안보를 저해해서는 안 된다고도 명시하고 있다. 결과적으로 암호의 효과적인 사용을 위한 국내 및 국제적 정책, 기법, 방식, 관행과 절차를 개발하고 이행함으로써 공공 및 사적 분야에서의 정책 결정을 보조하고자 노력하고 있다.
OECD Guidelines for the Security of Information Systems and Networks: Towards a culture of security 참고, www.oecd.org.

23) The Walsh Report, 호주에서 암호법을 제정하기 위한 과정에서 발간되었던 자료로 암호와 관련한 정책에 관해 매우 상세히 설명하고 있다.
http://www.efa.org.au/Issues/Crypto/Walsh/walsh.htm

24) Wassenaar 협정의 정식명칭은 The Wassenaar

호에 대한 정의(dual-use purpose)에 대해 공감하면서, 개인의 신뢰성 확보 및 프라이버시 보호를 위한 암호사용을 적극 권장하고 있다. 하지만 우리가 살펴본 Scarfo의 경우처럼, 암호를 이용한 범죄행위에 대해서는 어떻게든 처벌을 해야 하는 것이 수사당국의 입장이다. 이를 위한 적법한 접근권을 보장하는 것이 절실하다.

하지만 그렇다고 해서, 강제적인 수사권 확보는 오히려 반대 심리만 자극할 뿐이다. 그보다는 실시간 접속을 허용하는 등, 어중간한 규제와 제재로 일반인만 피해를 입는 상황은 피하도록 하는 것이 현명한 방법일 것이다[25]. 이러한 논리로 The Walsh Report는 암호를 사용한 범죄행위 적발 시 가중처벌을 하는 방안, 수사행위 및 재판 과정에 쓰이는 모든 문서를 읽을 수 있는 형태로 변환해서 제출해야만 하도록 하는 의무 규정을 설정(이를 통해, 암호화된 파일이나 문서를 근본적으로 일반인이 이해할 수 있는 내용으로 바꿈으로써 시시비비를 가릴 근거를 원천적으로 봉쇄하고자 함)하는 방안, 재래식 수사 방법과 마찬가지로 정황 증거의 인정폭을 대폭 확장하는 방안, 암호해독 원천기술 개발 기관의 역량 강화 방안 등을 제시하고 있다.

현재 암호와 관련한 모든 논의는 공론화 되어 있지 못한 실정이다. 이번 기회를 통해 좀 더 공개적으로 암호를 사용한 범죄 행위에 대한 현황과 또 이를 대처한 수사기관의 수사활동에 대해 논의하고, 그 과정에서 어떤 문제점들이 발생되고 있으며, 이들 문제를 해결하기 위해 필요한 조치들에 대해 논의하고, 해외 각국은 이 문제를 해결하기 위해 어떠한 노력들을 기울이고 있는지 살펴본 후 종합적인 안목으로 시의적절한 대책을 세울 필요가 있다.

암호가 이중으로 사용될 수 있다는 특징은 사용자의 의도와 성격에 따라 칼자루가 될 수도 있고, 방패가 될 수도 있다는 뜻이다. 이는 사용하는 사람이 어떻게 사용하느냐에 따라 판이한 결과를 야기한다. 칼자루로 사용하든 방패로 사용하든 어떤 입장의 사용자들이라도 모두 정당하고 떳떳하게 암호를 사용할 수 있는 환경을 조성하기 위한 노력이 절실히 필요한 시점에 Scarfo의 판례를 분석해 본 것은 그 의의가 상당하다고 볼 수 있다. 적절한 사용 환경을 조성할 수 있는 노력을 기울이기 위한 노력에 초석이 될 수 있기를 바란다.

Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies 이다. Wassenaar 협정은 재래식 무기와 이중-사용 제품과 기술에 대한 수출 통제를 주내용으로 한다. 조약 체결을 위한 협상은 1996년 7월 완료되었으며, 최종적으로 우리나라를 포함한 33개국이 협정 문서에 서명했다. Wassenarr 협정의 전신이 COCOM(Coordinating Committee for Multilateral Export Controls) 이다. COCOM은 Wassenaar로 자연스럽게 해체, 재조직되었다.
고려대학교 정보보호대학원, "암호기술을 통한 개인 프라이버시 보호에 있어 정책적 규제방안에 관한 연구," 최종연구보고서, 국가보안기술연구소, 2002년, pp. 45 - 54 참조.

25) 예를 들어, 인터넷 상에서의 효율성과 사생활 침해 금지를 위해 기획하는 공개키 기반 구조(PKI : Public Key Infrastructure) 또한 처음의 순수한 의도와는 다르게, 사용 과정에 있어 새로이 사용자들의 프라이버시를 침해하는 경우가 발생할 수도 있다. 이에 대한 자세한 논의는 홍창수 · 김소정 · 임종인 공저, "PKI에 잠재된 개인정보의 모호성," 개인정보연구 Vol. 1, No. 1, December 2002, KISA 참조.

참 고 문 헌

[1] 고려대학교 정보보호대학원 정책연구회, *정보보호를 위한 사이버스페이스의 법과 기술*, 북카페, 2003.

[2] 로렌스 레식, *코드 : 사이버 공간의 법이론*, 나남출판, 2000.

[3] 박창섭, *암호이론과 보안*, 대영사, 1999.

[4] 이만영 · 원동호 · 이민섭 · 송주석 · 임종인 · 박춘식 공저, *현대 암호학 및 응용*, 생능출판사, 2002.

[5] 이재상, *형사소송법(6판)*, 박영사, 2002.

[6] 홍창수 · 김소정 · 임종인 공저, "PKI에 잠재된 개인정보의 모호성," *개인정보연구 Vol. 1, No. 1*, December 2002.

[7] Harvey L. Zuckman 외 3인, *Modern Communications Law*, WEST Group, St. Paul, Minn., 1999.

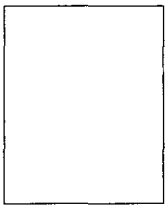
[8] Seymour Bosworth, M.E.Kabay, *Computer Security Handbook*, John Willey & Sons, Inc., 2002.

[9] Yale Kamisar 외 3인, *Basic Criminal Procedure : American Casebook Series(9th edition)*, WEST Group, St. Paul, Minn., 1999.

[10] Pricewaterhouse Coopers, "Global Security Survey(2000),"

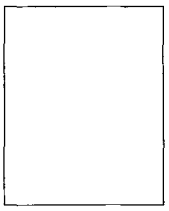
www.pwcglobal.com/extweb/ncpressrelease.nsf/DocID/7ABBA8E73B1E901D8525693500548A34
[11] Classified Information Procedures Act, Title 18, United States Code, Appendix III, §1 et seq.
[12] 미국 Wiretap Statute, Title Ⅲ, 18 U.S.C. §2510.
[13] The Walsh Report, http://www.efa.org.au/Issues/Crypto/Walsh/walsh.htm

〈著者紹介〉



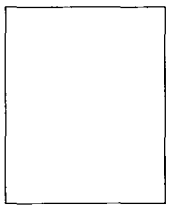
김 소 정(So-Jeong KIM)

1998년 8월 : 부산대학교 사학과 졸업(문학사)
2001년 2월 : 경희대학교 평화복지대학원 졸업(정치학 석사)
2001년 3월~2002년 9월 : 한국전파진흥협회 연구원
2002년~현재 : 고려대학교 정보보호대학원 정책박사과정 재학 중
관심분야 : 정보보호정책, e-privacy



임 종 인 (Jongin Lim)
종신회원

1980년 2월 : 고려대학교 수학과 졸업(이학사)
1982년 2월 : 고려대학교 수학과 졸업(이학석사)
1986년 2월 : 고려대학교 수학과졸업(이학박사)
1986년 9월 - 2001년 2월 : 고려대학교 수학과 교수
1999년 7월 - 현재 : 한국정보보호진흥원비상임이사
2000년 8월 - 현재 : 정보보호기술연구센터(CIST)장
2000년 8월 - 현재 : 대검 중앙수사부 컴퓨터수사 자문위원
2001년 3월 - 현재 : 고려대학교 정보보호대학원장, 정보보호기술연구센터장
관심분야 : 암호 이론 및 응용, 정보보호 정책, cyberlaw (컴퓨터 범죄수사, e-privacy)



오 일 석(Il-seok Oh)

1994년 2월 : 한국외국어대학교 영어과 졸업
1997년 2월 : 고려대학교 일반대학원 법학과 석사
1997년 3월 - 1997년 12월 : 고려대학교 비교법연구소 연구원
2001년 3월 - 현재 : 한국전자통신연구원 부설 국가보안기술연구소 연구원
관심분야 : 정보보호정책, 정보전 정책, 기본권 보장과 제한